日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

日本シーサート協議会加盟組織一覧

2018 年版

1　はじめに

日本シーサート協議会への加盟組織数も、2007 年の設立発起組織数 6 組織から 310 組織(2018 年 8 月 24 日総会開催時点)となりました。このような加盟組織数の増加と共に、日本シーサート協議会の役割も、国内のシーサートコミュニティが、いざというときに協力して活動できるための場の提供と整備だけではなく、インシデント対応基礎能力の底上げや改善を図るための場として、期待に応えていく必要があります。日本シーサート協議会では、この期待に応えるべく、役割の 3 層モデル、行動指針を元に、チーム「NCA」として、ワーキンググループ、地区などの各種協議会活動において、顔の見える信頼関係と互助努力に基づいた活動を進めています。

(1)役割の 3 層モデル

役割の 3 層モデルは、Tier1 にインシデント対応基礎能力を有するシーサート、Tier2 に分野別能力を有する ISAC(Information Sharing and Analysis Center)、Tier3 に分野横断能力を有する National CSIRT を想定したモデルです。日本シーサート協議会の役割は、Tier1 のシーサートを対象に、組織自身が自主的にインシデント対応基礎能力の向上を図るための場の提供と整備であると考えています。

(2)行動指針

行動指針は、チーム「NCA」として活動するための心構え、シーサートコミュニティ活動での心構えであり、組織自身が自主的にインシデント対応基礎能力の向上を図るための場の提供と整備にあたっては、欠かせないものと考えています。

正義の味方	社会貢献、トラブルをさっそうと解決する有志による無償の提供、積極的な姿勢、強制的にさせられている訳ではない、という事を端的に示す。
自由と責務	信頼関係を築くためには積極的な連携、情報提供が必要。黙って聞いているだけでは信頼は得られない。情報を提供した分だけ、信頼感があがると考えよ。
チャレンジと自己研鑽	常に自分を自己研鑽し、プロフェッショナルであること、新しい事、だれも手をつけていない事に積極的にチャレンジすべし。そして、メンバはその人を否定するのではなく、全力でフォローする事。
Open Door	協議会内、WG 間で垣根を作らない事。どのメンバも参加、見学に対しては温かく迎える事。

サイバーセキュリティインシデントに関する緊急時対応の機能を有した専門的な部隊がシーサート(CSIRT: Computer/Cyber Security Incident Response/Readiness Team)と呼ばれていますが、日本シーサート協議会に加盟している組織を俯瞰すると、体制、対象とする分野、取りまとめる部署など、一つとして同じ形態のシーサートはありません。

日本シーサート協議会加盟組織一覧は、体制、対象とする分野、取りまとめる部署などのアンケート調査の集計結果と共に、日本シーサート協議会の Web サイト[*1]に掲載しているチーム情報をまとめたものです。これから CSIRT 構築を検討している組織、すでに CSIRT 活動を進めている組織にとって、他の組織の取組みなどを知る機会になれば幸いです。また、チーム情報には、連絡窓口(PoC: Point of Contact)となる情報も記載してあります。対外的な連絡窓口が明らかになっていることの利点は、通知側と受領側の双方が、脆弱性対策やインシデント対応の組織間連携をベストエフォートで推進できることにあると考えます。加盟組織一覧がセキュリティ対策やインシデント対応の組織間連携のための一助になることを期待しています。

2018 年 11 月 24 日

本書は、下記 URL からダウンロードできます。

日本シーサート協議会加盟組織一覧について
http://www.nca.gr.jp/member/index.html

1) 日本シーサート協議会チーム情報　http://www.nca.gr.jp/member/index.html

2　アンケート調査の集計結果

加盟組織に対するアンケートは、基本情報(業種、会社規模)、CSIRT の活動範囲(対象とする利用者、対象とする分野)、CSIRT 構築までの体制(準備期間、設立時のメンバー数)、現在の CSIRT の体制(人数、実装の形態、取り纏め部署など)、インシデント対応時の CSIRT の位置付けなどが調査項目となっています。

- 調査時期：2018 年 11 月
- 調査項目：加盟組織の業種と母体組織の規模、加盟組織の体制、加盟組織の活動範囲、インシデント対応、外部連携、PSIRT、教育／トレーニング
- アンケート回収数：215 組織

2.1　加盟組織の業種と母体組織の規模

業種については、日経業種分類[2]を用いてアンケート調査を実施しています(図 1)。『サービス業(IT 関連)』が 3 割強、続いて金融分野(銀行、証券、保険など)が 1 割強で続いています。加盟組織の母体の規模については、7 割近くが千名以上となっています(図 2)。

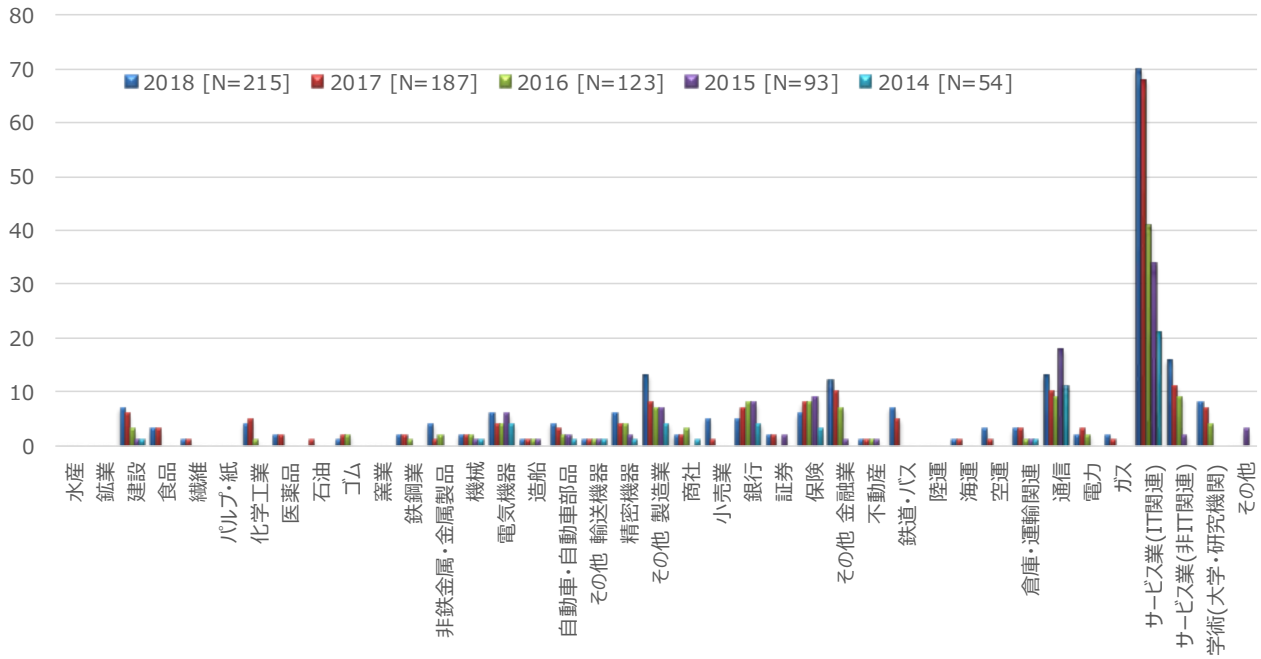


図 1：加盟組織の業種

2) 日経業種分類　http://www.nikkei.com/markets/company/gyoshu.aspx

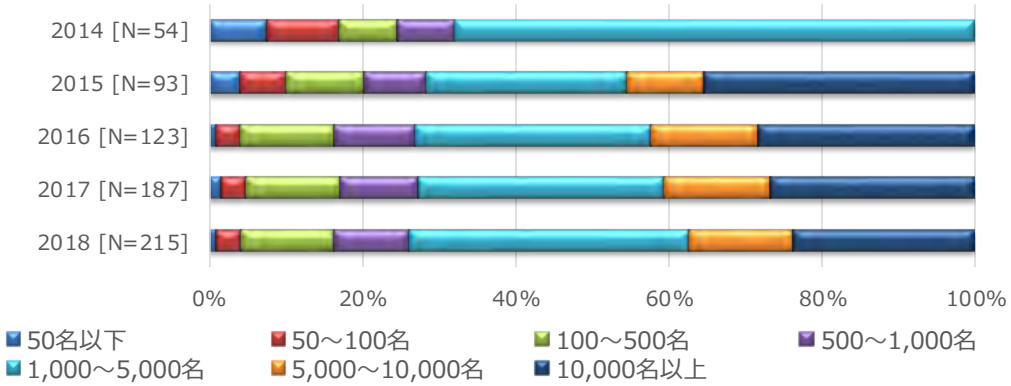
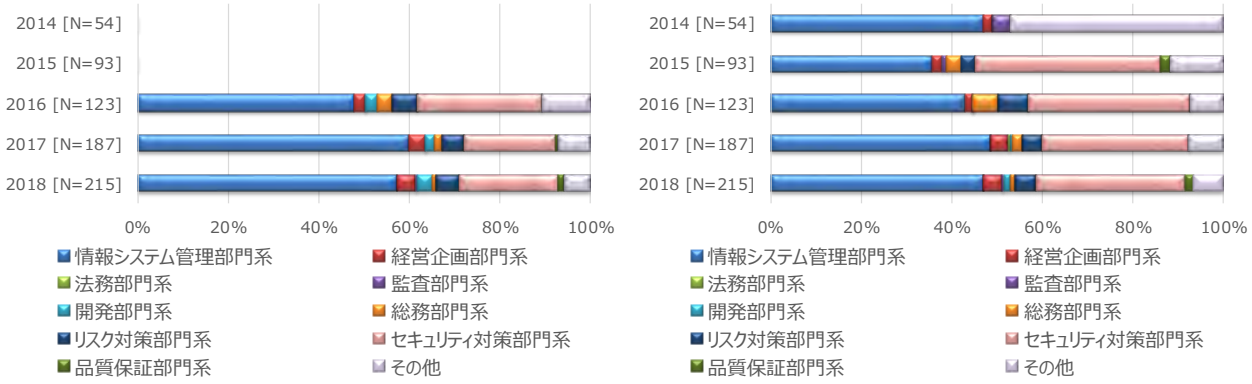


図 2：母体組織の規模

2.2 加盟組織の体制

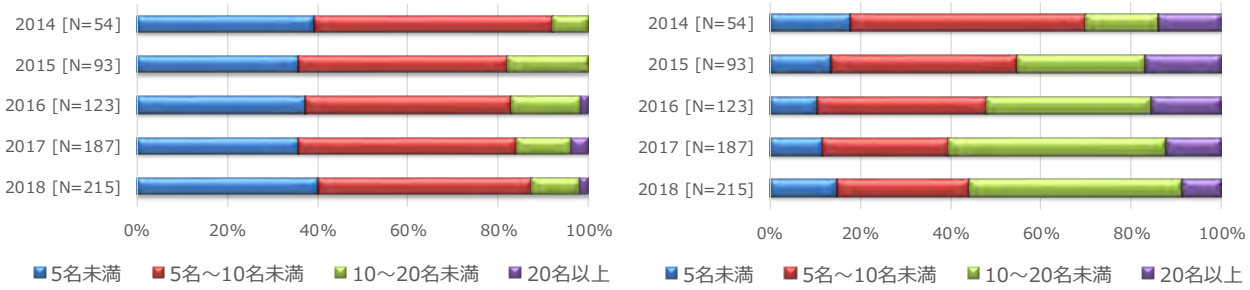
2016 年から、構築を主導した部署を調査項目に追加しました。この結果から、2018 年も『情報システム管理部門系』が CSIRT 構築を主導し、構築後は『セキュリティ対策部門系』に引き継ぐという流れがあります。また、加盟組織の多くは、『情報システム管理部門系』『セキュリティ対策部門系』が構築後の CSIRT を取り纏めています(図 3)。



(左：構築を主導した部署、右：構築後の取り纏め部署)

図 3：取り纏め部署

チーム人数は、2017 年までと同様に活動開始後に増員しており、全体としてスモールスタートです。(図 4)。その一方で、活動開始後のチーム人数は、増員傾向にあります。



(左：設立時、右：活動開始後)

図 4：チームの人数

また、加盟組織の CSIRT 実装の多くは、兼務を主体とした部署横断型です(図 5、図 6)。これは、2014 年の『専任の CSIRT 要員を抱えた部署を核とした部署横断型』が大半を占めていた状況との大きな違いです。ただし、いずれも、CSIRT 組織の実装を通した部署間を横断した組織体制の構築、すなわち、組織内の横断的な協力体制整備への期待は変わらないようです。

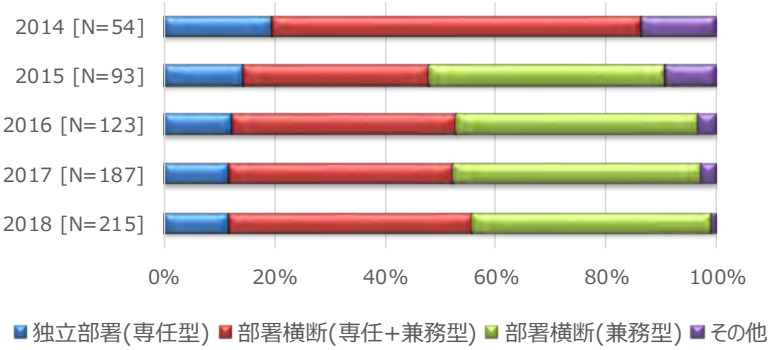


図 5：実装の形態

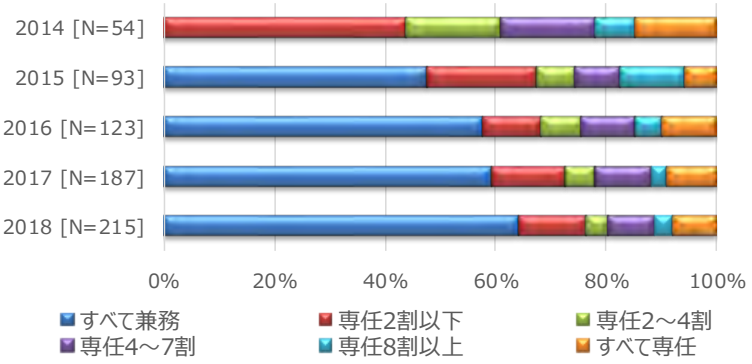


図 6：専任の割合

2.3　加盟組織の活動範囲

対象とする活動範囲については、大きな変化は見られませんでした。加盟組織が想定する活動範囲をサポート対象者視点で示したのが図 7 です。9 割以上が社員のインシデント対応、すなわち、CSIRT が所属する組織のインシデント対応を想定した活動となっています。図 8 は、活動の具体的な分野を、CSIRT が所属する組織のインシデント対応、CSIRT が所属しない組織のインシデント対応、それ以外の 3 つの分類から調査したものです。

CSIRT が所属する組織のインシデント対応としては、『社内インフラ：CSIRT が所属する組織のインシデント対応』、『顧客向けサービスのシステム：ネットワーク接続サービス、Web アプリケーションサービスなど社外の利用者に対して提供しているサービスで発生したインシデントに対応』を質問項目に、CSIRT が所属しない組織のインシデント対応については、『SI 事業など、顧客納入済システム』、『インシデントレスポンスサービスなどでの顧客サイトサポート』、それ以外では、『自社製品(ハードウェア、ソフトウェア)の脆弱性対応』、『その他』を質問項目として設定しました。

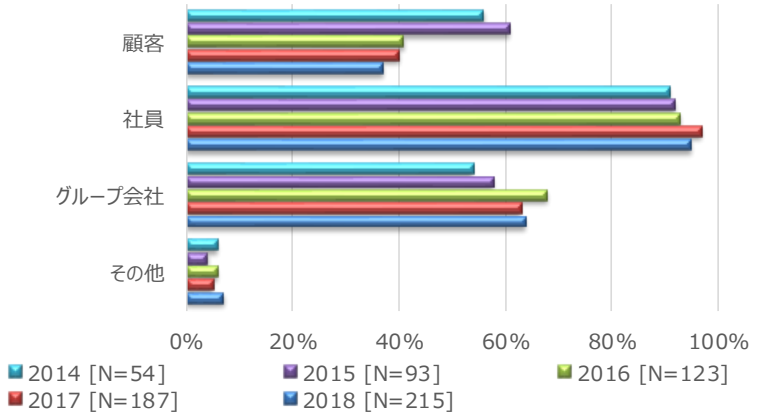


図 7：対象とするユーザ

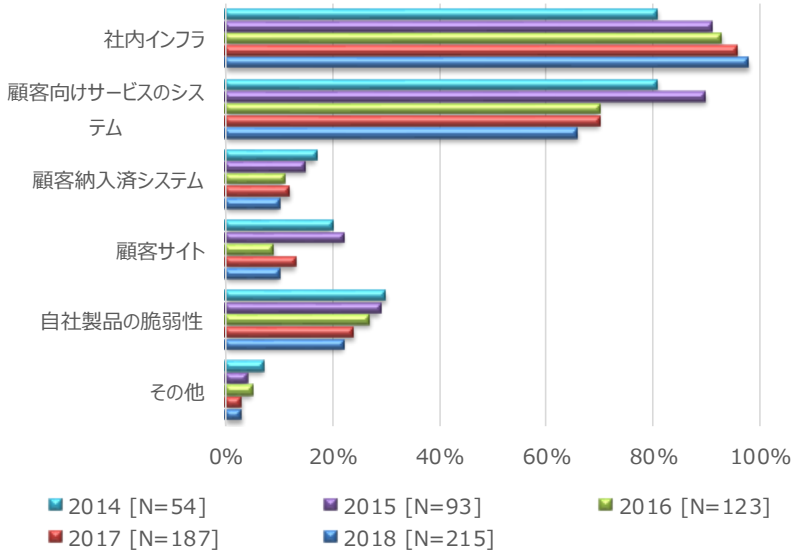


図 8：対象とする分野

図 9は、インシデント対応時のCSIRTの位置付けです。これによれば、これまでの日本企業独自の形態として紹介してきた『技術アドバイザ』という側面よりも、組織内の横断的な協力体制整備のためのコーディネーター(調整役)、現場での対応作業や支援が求められています。

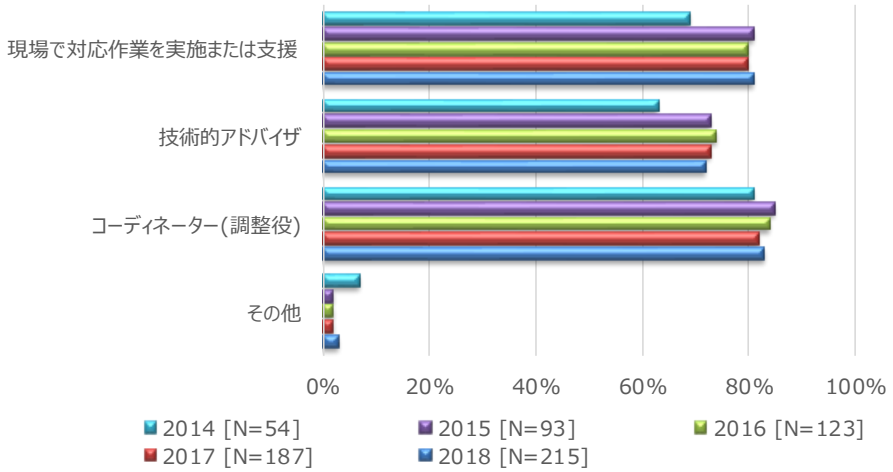


図 9：インシデント対応時の CSIRT の位置付け

2016 年から、CSIRT として実施している事前対応型、事後対応型、セキュリティ品質管理の活動分担を調査項目に追加しました。活動分担は、チーム内で実施、社内の他部署に依頼、社外に依頼という区分としています。この結果から、チーム内で実施する事後対応型の活動については、主に『脆弱性ハンドリング』、『インシデントハンドリング』、『アラートと警告』であり、『フォレンジック』、『マルウェア解析』については社外に依頼しているところが5 割近くに上ります(図 10)。

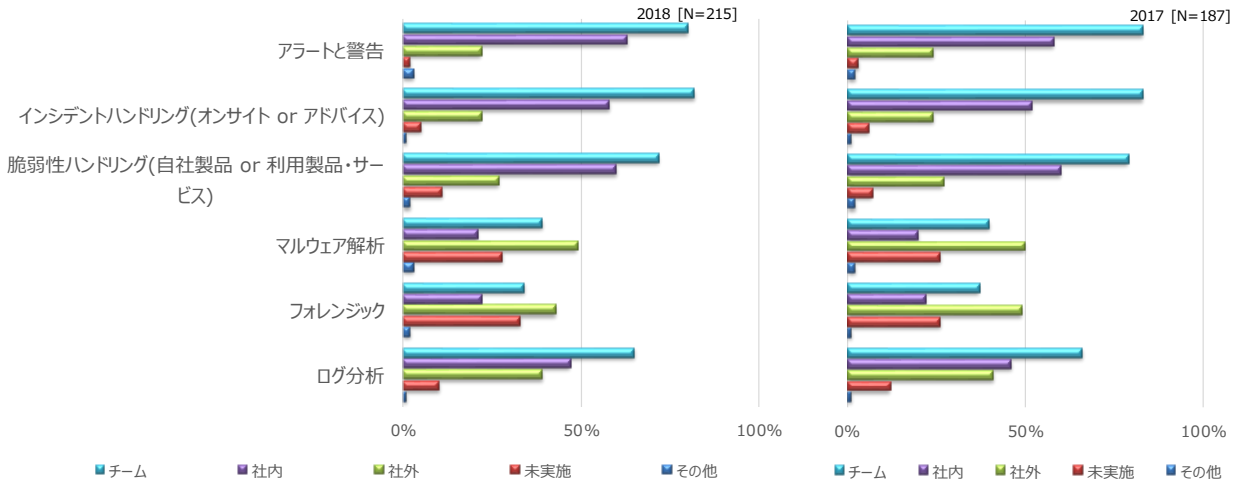


図 10：CSIRT として実施している事後対応型の活動

また、チーム内で実施する事前対応型の活動は、主に『情報収集(パブリックモニタリング、技術動向監視)』、『分析(セキュリティ動向分析)』、『展開(セキュリティ関連情報の提供、注意喚起・アナウンス)』です(図 11)。

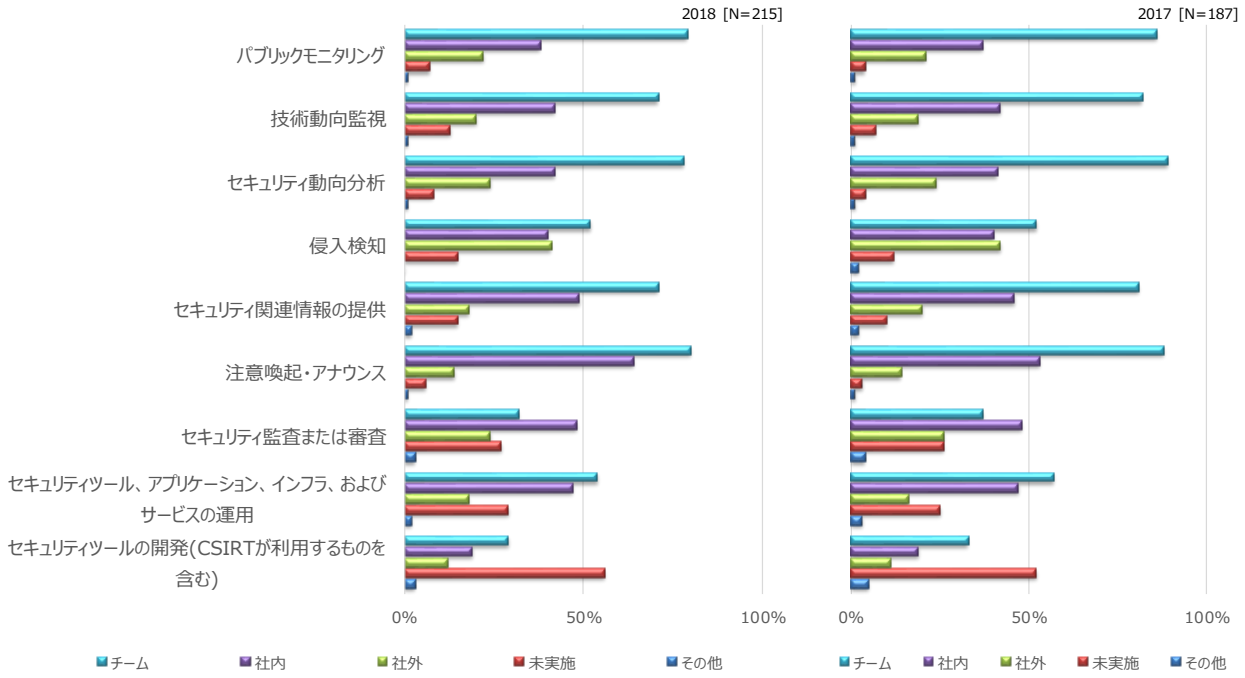


図 11：CSIRT として実施している事前対応型の活動

セキュリティ品質管理については、2017 年に教育／トレーニングをチーム内で対応するという回答が増えていました(図 24)。2018 年も、その状況は続いており、啓発・意識向上活動とあわせて、人材面での強化が求められていると言えます。また、8 割以上が各種セキュリティに関わる相談をチーム内で対応していることから、継続して CSIRT がセキュリティ相談窓口としての役割を果たしています(図 12)。

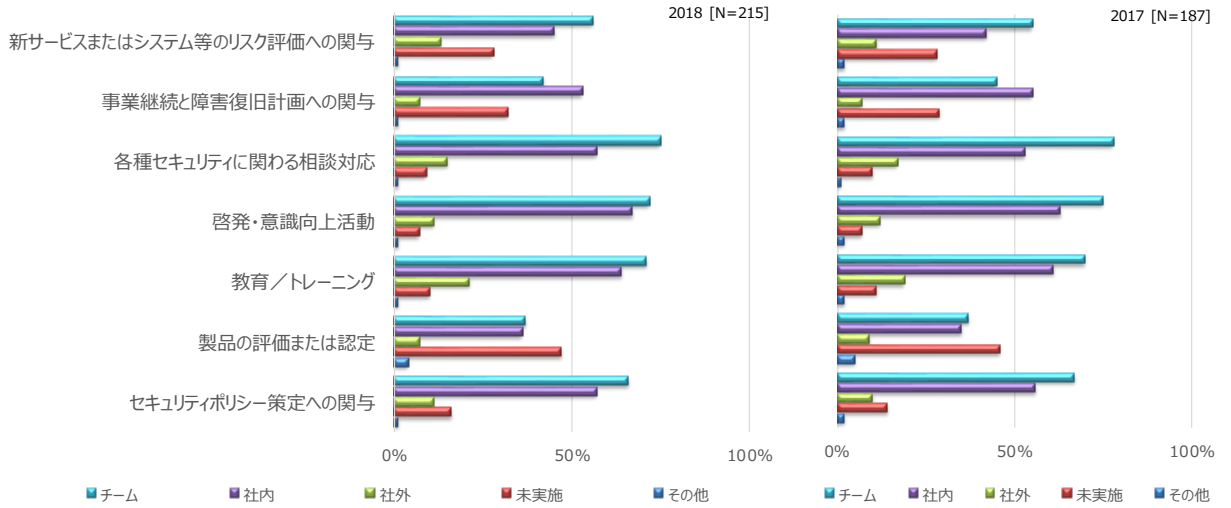


図 12：CSIRT として実施しているセキュリティ品質管理の活動

2.4　インシデント対応

2017 年から、インシデント対応に関する調査として、過去 1 年間において対応したインシデント、インシデント対応に関連する文書や手続きの整備状況、SOC(Security Operation Center)体制について調査を実施しました。

過去 1 年間において対応したインシデントについては、ランサムウェアに関連する対応件数の減少が見て取れます(図 13)。また、CSIRT 活動に関連する文書のうち、インシデント対応に関連する「インシデントの分類と定義」、「緊急時の連絡網整備」、「インシデントを防止、検知、解決するための手続き」ついては、文書化して運用しているところが 8 割を超えています。その一方、2018 年から新たに調査項目として追加したドメイン管理をみると、ドメインの取得/運用/廃棄については 6 割近くが文書化しているのに対し、類似ドメインの対処については慣習によるところが多いようです。

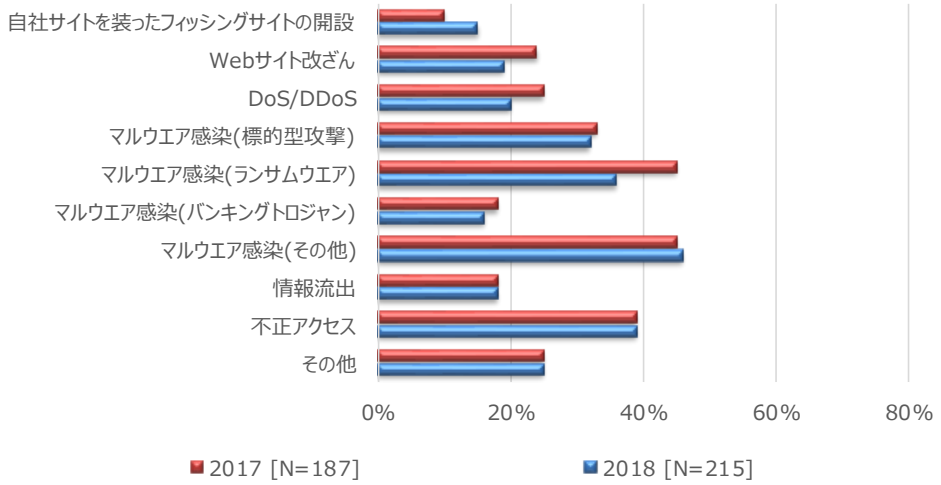


図 13：過去 1 年間において対応したインシデント

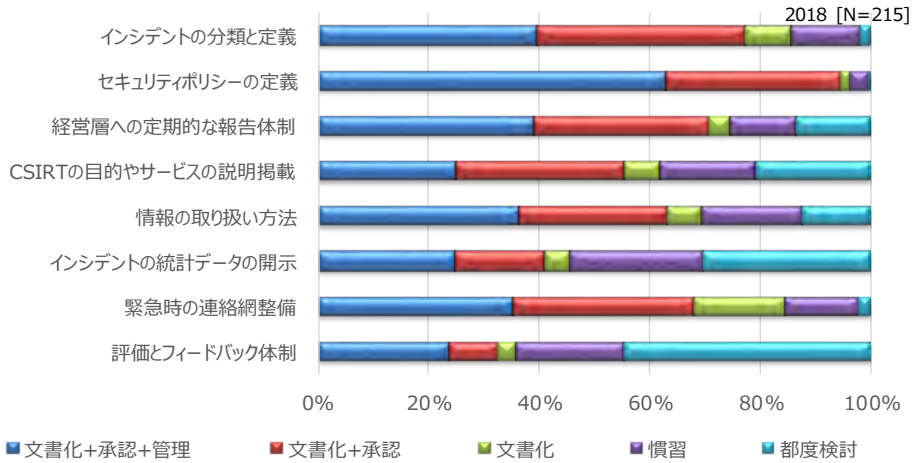


図 14：インシデント対応に関連する文書の整備状況

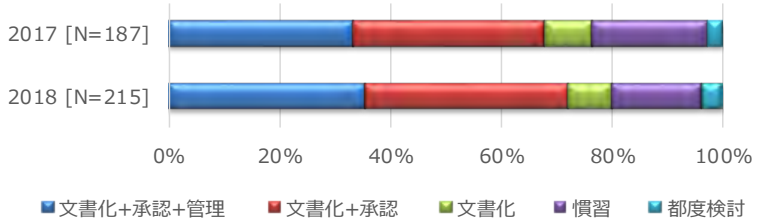


図 15：インシデントを防止、検知、解決するための手続きの整備状況

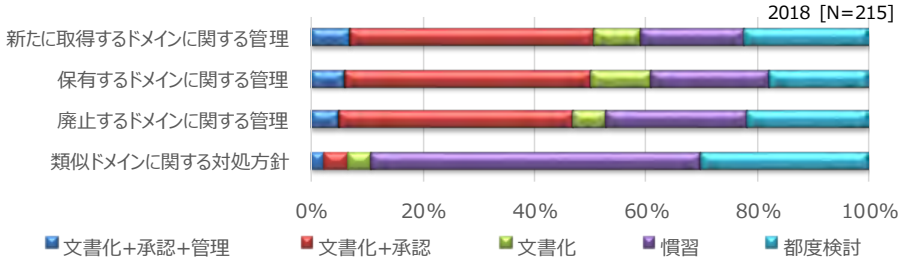


図 16：ドメイン管理に関する文書の整備状況

運用については、SOC による体制を構築している組織が 6 割近くで、約半数が他社に外注、CSIRT とは独立した形態を取っています(図 17～図 19)。

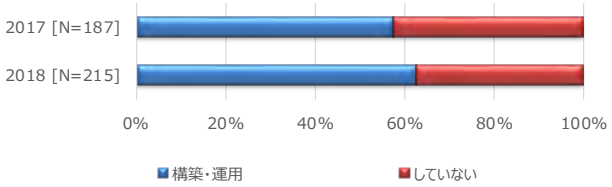


図 17：SOC による監視体制の構築・運用

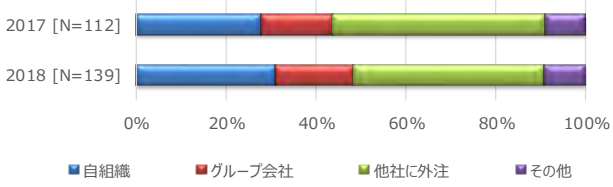


図 18：SOC の運用体制

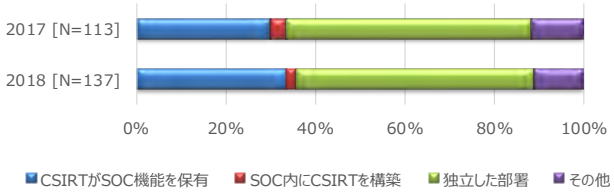


図 19：SOC と CSIRT の関係

2.5　外部連携

2017 年から、過去 1 年間に外部から CSIRT に対しての連絡や問合せの有無、CSIRT への連絡や問合せ元について調査を実施しました。この結果から、加盟組織の半数以上が、インシデントに関して外部からの連絡や問合せを受信していること(図 20)、セキュリティ研究者、一般ユーザからの連絡や問合せも増えていることがわかりました(図 21)。また、その他の連絡や問合せ元には、他組織の CSIRT、協議会加盟組織だけではなく、公的機関、顧客、グループ会社が含まれており、サイバーセキュリティに関する関心が高まっていることがみえてきました。

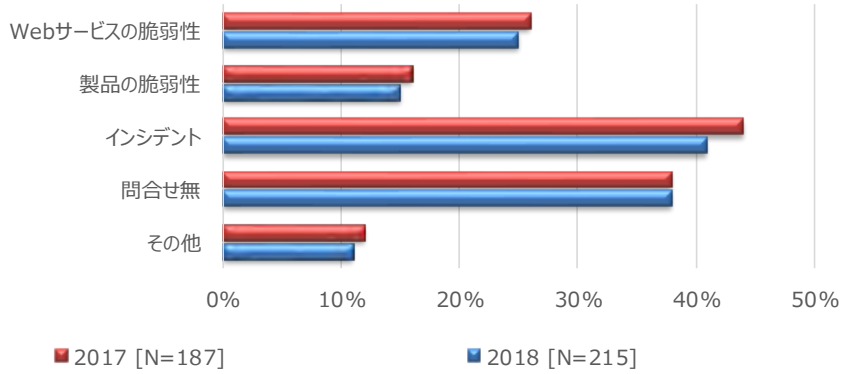


図 20：過去 1 年間に外部から CSIRT に対しての連絡や問合せ

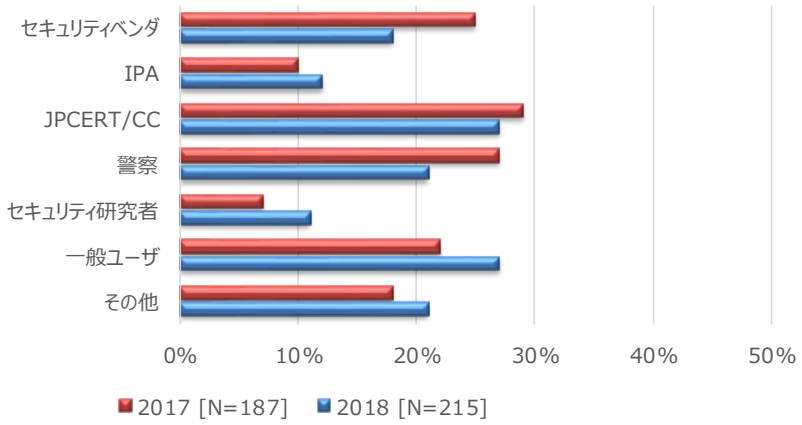


図 21：CSIRT への連絡や問合せ元

2.6 PSIRT

IoT のセキュリティ脅威が高まるにつれ、自社で製造・出荷している製品の脆弱性を取り扱う PSIRT(Product Security Incident Response Team)機能について目に触れる機会が増えています。これは、IoT のセキュリティ施策のひとつとして CSIRT が機能することへの期待ととれます。2017 年から、PSIRT 機能の有無、PSIRT の位置付けについて調査を実施しました。この結果から、PSIRT 機能を必要とする加盟組織は少ないものの(図 22)、約半数が、既存の CSIRT に、組織 CISRT と PSIRT を包含する実装を採用しています(図 23)。

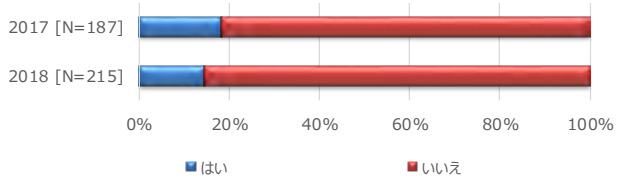


図 22：PSIRT 機能の有無

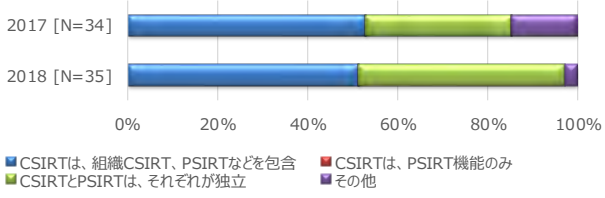


図 23：PSIRT の位置付け

2.7　教育／トレーニング

CSIRT として実施しているセキュリティ品質管理の活動項目(図 12)のひとつである「教育／トレーニング」への取組みの経年変化を図 24 に示します。チーム内で実施、社内の他部署に依頼、社外のいずれも増えており、人材面での強化を図ろうとしていることがわかります。

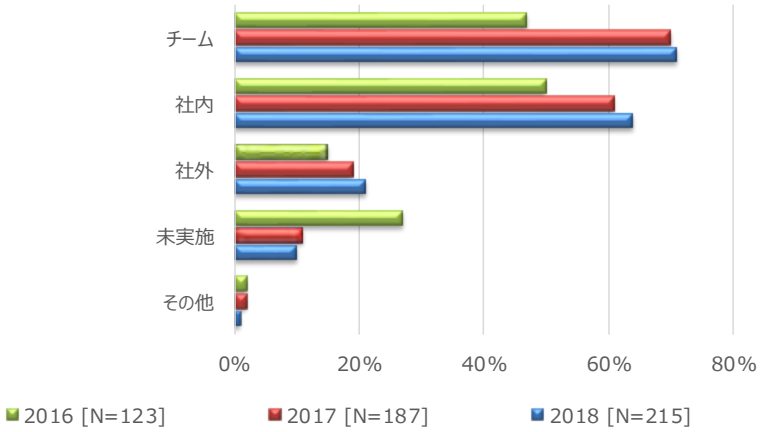


図 24：教育／トレーニングへの取組み

2018 年は、新たにメール訓練の取組みについて調査を実施しました。7 割近くがメール訓練を実施しており、5 割近くが 2015 年から 2016 年にかけてメール訓練を開始しています。年間の実施回数は、1 回と 2 回が 8 割を占めています。また、国内での実施では 8 割が全体を対象とした訓練を実施していることがわかりました。

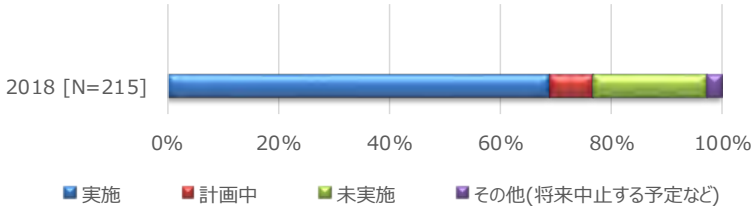


図 25 ：メール訓練の実施有無

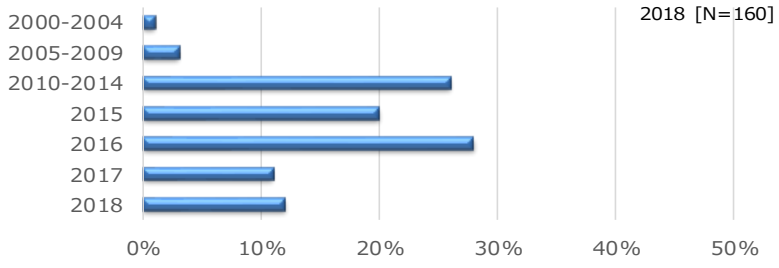


図 26：メール訓練の開始時期(年)

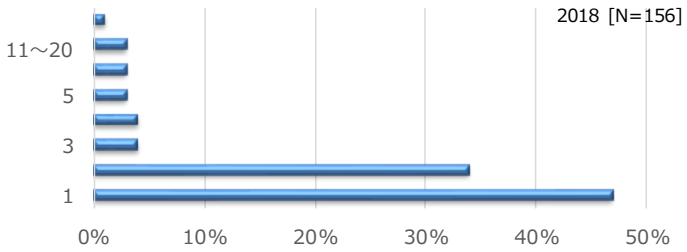


図 27：メール訓練の年間の実施回数

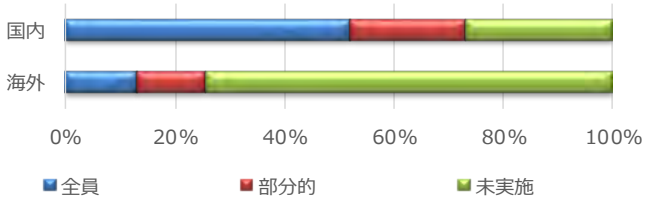


図 28：メール訓練の対象範囲

CSIRT として実施している活動の調査については、今後も調査項目を詳細化していくことで、活動実態の指標にしていきたいと考えています。

3　加盟チーム紹介

3.1　加盟数の推移

日本シーサート協議会の使命『本協議会の全会員による緊密な連携体制等の実現を追及することにより、会員間に共通する課題の解決を目指す』、『社会全体のセキュリティ向上に必要な仕組みづくりの促進を図る』に賛同し、加盟に至った組織数は、2018 年 8 月末で 310 組織となります。加盟組織の設立年と加盟数の推移を図 29に示します。2013 年以降、情報セキュリティならびにサイバーセキュリティ対策に関する必要性への高まりと共に、体制の整備が急速に進んでいると言えます。また、この傾向は、体制整備の準備期間が、1 年以内である加盟組織が 9 割近くを占めるという数値からも読み取ることができます(図 30)。

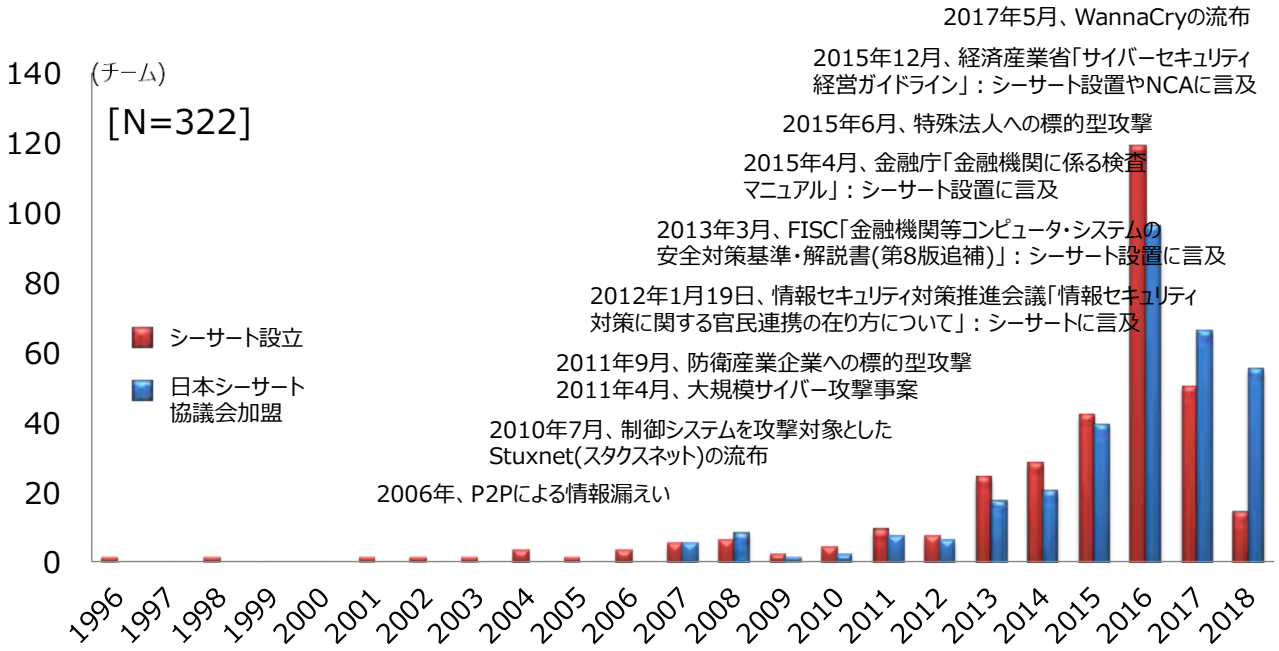


図 29：加盟組織の設立年と加盟数の推移

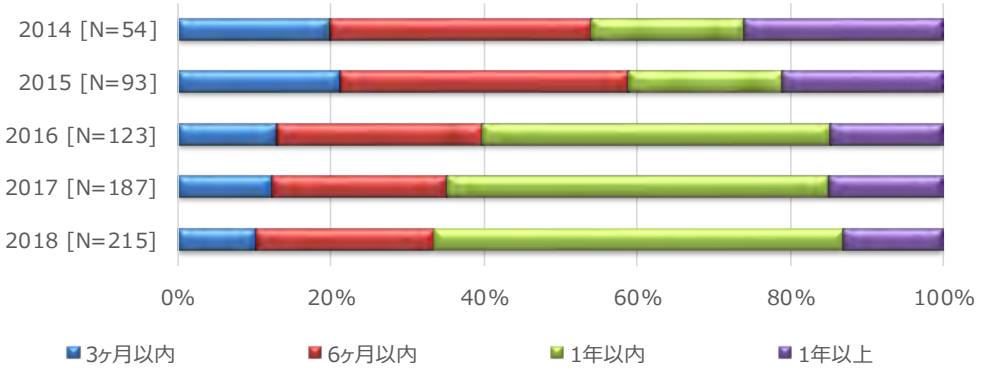


図 30：設立準備期間

3.2　加盟チーム紹介

次ページ以降は、日本シーサート協議会の Web サイトに掲載している 2018 年 8 月末までの 310 加盟組織のチーム情報をまとめたものです。最新の情報は、下記 URL を参照ください。

日本シーサート協議会チーム情報
http://www.nca.gr.jp/member/index.html

チーム連絡先情報は、インシデント対応を目的として提供しているものです。
勧誘や宣伝のために、チーム連絡先情報を使用することを禁止します。
Team contact information provided for Incident Response purposes only.
NCA strictly prohibits the use of contact information
for solicitation or marketing.

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

7&i CSIRT

チームの正式名称	Seven & i Computer Security Incident Response Team
チームの略称	7&i CSIRT
所属する組織名	株式会社セブン&アイ・ホールディングス
設立年月日	2015-10-01
チームの Email アドレス	7i-csirt@hd.7andi.co.jp
チームサイト	
所属組織サイト	http://www.7andi.com/
加盟年月	2016 年 01 月

1. 概要

株式会社セブン&アイ・ホールディングス (7&i HLDGS.) は、コンビニエンスストア・総合スーパー・百貨店・食品スーパー・フードサービス・金融サービス・通信販売・IT / サービスなど、各事業を中心とした企業グループの企画・管理・運営を事業目的としている持株会社です。

7&i CSIRT は、7&i グループの CSIRT として設置され、グループ企業に対してサービスを提供しています。

2. 設立の経緯・背景

7&i CSIRT は、昨今の情報セキュリティ脅威 (サイバーテロ・情報漏洩など) の増大に伴って、迅速かつ適切に対処するチームの必要性を強く認識する中、7&i の複数グループ企業 EC サイトを統合した新サイト (新サービス) 立上げをきっかけに、インシデント対応専門チームとして2015 年 10 月に設置されました。

3. 会社内における位置づけおよび活動内容

7&i CSIRT は、7&i HLDGS. の組織内に専任要員を以て設置され、インシデント発生時の対応だけでなく、インシデント発生の未然防止にも注力しています。
グループ企業の情報システム部門と連携し、7&i グループ内で発生するインシデントに対する未然防止のための調査・分析とリスク情報の共有、ならびにインシデント対応活動を行なっています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

7BK-CSIRT

チームの正式名称	セブン銀行 CSIRT
チームの略称	7BK-CSIRT
所属する組織名	株式会社 セブン銀行
設立年月日	2015-10-01
チームの Email アドレス	7bk-csirt@sevenbank.co.jp
チームサイト	
所属組織サイト	http://www.sevenbank.co.jp/
加盟年月	2015 年 12 月

1. 概要

7BK-CSIRT は、セブン銀行のシステムに関する攻撃について幅広く対応 (サイバー攻撃に限らず、スキミング、偽造カード、ネットバンク不正アクセスなど) するチームです。

2. 設立の経緯・背景

2013 年 7 月に「セキュリティ検討会」の名称で部署を横断した会議体を立ち上げ、サイバー攻撃に限らず、スキミング、偽造カード、ネットバンク不正アクセスなど幅広く、情報共有、対策・方針の策定等を行ってきましたが、インシデントに対する組織的な対応力強化を目的として、2015 年 10 月、金融犯罪対策部内に CSIRT 担当 (7BK-CSIRT) を設置しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
多様なインシデントに対応するため、専任者と複数の部署を横断したメンバーで構成され、当社システムへの以下のような攻撃について幅広く対応します。
・サイバー攻撃
・スキミング
・偽造カード
・インターネットネットバンキング不正アクセス
・顧客情報・機密情報の漏洩や改竄

(2)活動内容
・サイバーセキュリティインシデント等に関する情報収集・情報連携
・セキュリティ強化対策の検討
・インシデント発生時のハンドリング
・外部組織との連絡窓口
・経営層への報告など全社的な情報発信
・訓練計画の実行

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ABeam-CSIRT

チームの正式名称	ABeam Consulting CSIRT
チームの略称	ABeam-CSIRT
所属する組織名	アビームコンサルティング株式会社
設立年月日	2017 年 6 月 1 日
チームの Email アドレス	gblabcsirt@abeam.com
チームサイト	
所属組織サイト	https://www.abeam.com/jp/
加盟年月	2018年4月25日

1. 概要

アビームコンサルティングでは、次の事業を営んでいます。
【マネジメント コンサルティング】経営診断・戦略立案・M&A・アライアンス
【ビジネスプロセス コンサルティング】業務改革・組織改革・アウトソーシング
【IT コンサルティング】IT 戦略・企画立案・システム開発・パッケージ導入・保守・サイバーセキュリティ
【アウトソーシング】各種業務・システム運用の受託

2. 設立の経緯・背景

当社ではかねてより全社的な情報セキュリティ活動に取り組んでおりますが、近年の深刻化するサイバーセキュリティ脅威に対して、迅速かつ的確に対応する仕組み・体制作りが必要であると考え、ABeam-CSIRT を設立しました。

3. 会社内における位置づけおよび活動内容

情報セキュリティインシデントに対して、「検知」「対応」「予防」及び「啓発」を行います。
(1) 検知
・インシデント/セキュリティイベントの検知
・脆弱性情報、攻撃予兆情報の収集/共有
(2) 対応
・インシデントハンドリング / サポート
・コーディネーション
(3) 予防
・定期的なリスクアセスメント、セキュリティ監査
・セキュリティ技術動向調査、有効性確認
(4) 啓発
・セキュリティ教育 / トレーニング
・セキュリティ関連情報提供

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ABK-CSIRT

チームの正式名称	AEON BANK CSIRT
チームの略称	ABK-CSIRT
所属する組織名	株式会社イオン銀行
設立年月日	2016年3月1日
チームの Email アドレス	system-csirt-ml@aeonbank.co.jp
チームサイト	
所属組織サイト	http://www.aeonbank.co.jp/
加盟年月	2016 年 11 月

1. 概要

わたしたちは、商業と金融の融合により生まれた、新しい銀行です。
お客様の声を真摯に受け止め、新鮮な金融サービスの提供に努めてまいります。
休むことなく常に進化し続けることで、地域の発展に寄与してまいります。

2. 設立の経緯・背景

昨今のサイバー攻撃の高度化及び巧妙化を踏まえ、迅速に対応できる態勢を整備するためにABKーCSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
ABK-CSIRTはシステム部門内で、専任担当を中心にネットワーク、インフラストラクチャー、システム等の兼任担当で構成されています。今後はセキリュティ関係部署と連携し、部門横断型のCSIRTへ拡大予定です。

(2)活動内容
1. インシデント情報、脆弱性情報等の管理し予防措置を行う。
2. サイバー攻撃への対応を実施し、被害や損害を最小限に抑制し、収束させる。
3. 役職員への注意喚起、訓練を実施し啓蒙活動を行う。
4. セキュリティ強化対策の検討を行う。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ACS-CSIRT

チームの正式名称	AEON CREDIT SERVICE　CSIRT
チームの略称	ACS-CSIRT
所属する組織名	イオンクレジットサービス株式会社
設立年月日	2016-03-03
チームの Email アドレス	acs-csirt@aeon.co.jp
チームサイト	
所属組織サイト	http://www.aeoncredit.co.jp/
加盟年月	2016 年 06 月

1. 概要

イオンクレジットサービス株式会社は、「お客さま第一」、「生活に密着した金融サービスの提供」、「社会の信頼と期待に応える」、「活力ある社内風土の確立」を基本方針とし、金融サービスを通じたお客さまへの限りない貢献を永遠(AEON)の使命と定めております。

2. 設立の経緯・背景

昨今のサイバー攻撃が高度化・巧妙化が進む中、サイバーインシデントに対して、早期に解決するための技術的対応チームとして、ACS-CSIRTを構築しました。

3. 会社内における位置づけおよび活動内容

(1) 位置付け

ACS-CSIRTは、IT部門を中心に構成されています。

(2) 活動内容

ACS-CSIRTは、以下の活動を実施しています。

・サイバーインシデント発生時の対応支援
・最新技術動向の評価と脆弱性情報の収集
・外部機関との連絡窓口
・セキュリティ情報の配信
・技術教育・技術訓練の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ADO-CSIRT

チームの正式名称	エアドゥシーサート
チームの略称	ADO-CSIRT
所属する組織名	株式会社AIRDO
設立年月日	2016年9月1日
チームの Email アドレス	ml_itg.csirt@airdo.co.jp
チームサイト	
所属組織サイト	https://www.airdo.jp/
加盟年月	2018 年 01 月

1. 概要

ADO-CSIRT は、株式会社AIRDOに所属する組織内 CSIRT です。
株式会社AIRDOは、「北海道の翼」として札幌に本社があり、北海道内の6都市と東京・仙台・名古屋・神戸など本州間を結ぶ路線を運航する航空会社です。

2. 設立の経緯・背景

従来より情報セキュリティ委員会において情報セキュリティに係る対策の整備を進めてきましたが、サイバー攻撃が多様化・巧妙化し、セキュリティ対策がこれまでになく重要となる中、万一のインシデント発生時に社内外と連携して適切かつ迅速な対応ができるよう、ADO-CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

ADO-CSIRTは、システムを所管する企画部ITグループと情報セキュリティおよび広報活動を所管するCSR推進室CSR企画グループメンバーにより構成されるバーチャルな組織です。

主な活動内容
(1)平常時
・脅威情報、脆弱性情報の収集と関係各所への共有
・当該情報に基づいた各種対応および対策の実施
(2)緊急時
・インシデントのトリアージおよび被害の最小化のための活動
・対応後の再発防⊠対策や関係各所への報告・連絡の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

AGS-CSIRT

チームの正式名称	AGS Computer Security Incident Response Team
チームの略称	AGS-CSIRT
所属する組織名	AGS株式会社
設立年月日	2014-10-01
チームの Email アドレス	ags-csirt@ags.co.jp
チームサイト	
所属組織サイト	http://www.ags.co.jp/
加盟年月	2015 年 07 月

1. 概要

AGS-CSIRT は AGS株式会社によって運営される CSIRT です。主に AGS グループとそのお客様のセキュリティインシデントへの対応を支援します。

AGS株式会社は、金融・公共・法人の各領域でシステムコンサルティングからアウトソーシングまで幅広く情報サービスを提供しています。さらに、インターネットを活用した事業やセキュリティ対策への関心の高まりを踏まえて、本格的な設備を保有する IDC (インターネットデータセンタ) サービスや情報セキュリティサービスにも積極的に取組んでいます。

2. 設立の経緯・背景

サイバー攻撃の高度・巧妙化をふまえ、今後は被害発生の防止だけではなく、万が一の被害発生を視野に入れたセキュリティ対策が必要であるとの判断から、セキュリティインシデントの対応チームとして「AGS-CSIRT」を設立することとなりました。

3. 会社内における位置づけおよび活動内容

AGS-CSIRT は社内 IT 部門の要員と、AGS-CSIRT 運営にあたって密接な連携が必要となる部門の要員から構成されるチームです。AGS グループの情報セキュリティを統括する情報セキュリティ委員会の下部組織としてセキュリティインシデントの予防と発生時の対応を支援します。

AGS-CSIRT は主に以下の 3 つの活動を通じて、AGS グループの情報セキュリティ対策強化を支援しています。
1.セキュリティインシデント発生時の対応支援
2.ソフトウェアなどの脆弱性情報や最新のセキュリティ情報の収集とその提供 (顧客・社内向け)
3.新規・既存システムのセキュリティ対策の評価・是正勧告・対策実施支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

AHA-CSIRT

チームの正式名称	アメリカンホーム医療・損害保険CSIRT
チームの略称	AHA-CSIRT
所属する組織名	アメリカンホーム医療・損害保険株式会社
設立年月日	2015-12-01
チームの Email アドレス	AHAJapanCSIRT@aig.co.jp
チームサイト	
所属組織サイト	http://www.americanhome.co.jp/
加盟年月	2016 年 03 月

1. 概要

当社の前身であるアメリカン・ホーム・アシュアランス・カンパニー日本支店は、1960 年に日本における損害保険の事業免許を取得し、半世紀にわたり日本での事業を営んでまいりました。日本で初めての傷害保険の通信販売やリスク細分型自動車保険の開発など、通販型損害保険会社のパイオニアとしてお客様のニーズにお応えする商品やサービスを提供し続け、2014 年 4 月に日本法人「アメリカンホーム医療・損害保険株式会社」となりました。そして AIG グループ内での事業構成の簡素化を実現するため、2016 年 4 月より全ての保険商品の新規契約の販売活動を終了し、既にご加入いただいているご契約の維持・保全に特化しています。アメリカンホーム・ダイレクトはお客様のこれまでの信頼に応え、これからも「お客様に選ばれ続ける会社」であることを目指します。「アメリカンホーム保険」と「アメリカンホーム・ダイレクト」は、アメリカンホーム医療・損害保険株式会社のブランド名です。

2. 設立の経緯・背景

サイバーセキュリティの重要性は保険業界においても日々高まる一方であり、セキュリティインシデント対応態勢を強化するため、AHA-CSIRT を設置しました。

3. 会社内における位置づけおよび活動内容

AHA-CSIRT は、セキュリティインシデントが発生した際に、社内で対応をリードするチームとして位置付けられています。セキュリティインシデント対応時には、米国本社側でのセキュリティインシデント対応チームと密に連携を取り、デジタルフォレンジック等を行うほか、事後対応もリードします。
米国本社側との連携が非常に重要なので、セキュリティインシデント対応時に、いかに迅速に米国本社側にエスカレーションするかがポイントになっています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

AHIRU

チームの正式名称	Aflac Hyper Incident Rediness Unit
チームの略称	AHIRU
所属する組織名	アフラック
設立年月日	2015-10-01
チームの Email アドレス	MLT_SecurityIncident@aflac.co.jp
チームサイト	
所属組織サイト	http://www.aflac.co.jp/
加盟年月	2015 年 10 月

1. 概要

1974 年、アフラックは日本初の「がん保険」を携えて日本での事業を開始した。アフラックは、「生きるを創る」をテーマに、お客様が生きていくために本当に必要とされている保険商品とサービスを提供している。新契約件数は 155 万件、保有契約件数は 2,331 万件 (2015 年 3 月末) を保有している。日本においては、営業拠点 91 営業部・支社、アソシエーツ 14,470 店、第一生命保険会社、大同生命保険会社、日本郵政株式会社との業務提携も積極的に展開している。

2. 設立の経緯・背景

当社における危機管理の 1 つとして危機に発展する蓋然性が高いサイバーセキュリティインシデントにおける対応態勢が 9/1 付にて整備された。整備に伴い、サイバーセキュリティインシデントに平時より対応する態勢を確保し、より実効性、機動性を高めるためサイバーセキュリティインシデントレスポンスの IT 部門における実働チームとして 10/1 付にて CSIRT が設置された。

3. 会社内における位置づけおよび活動内容

当社の CSIRT は、IT 部門横断的にコンピュータやネットワーク上で、何らかの問題 (主にセキュリティ上の問題) が起きていないかどうか監視すると共に、万が一問題が発生した場合に、その原因解析や影響範囲の調査を行うチームとする。サービス対象者を「当社システムの利用者及び管理者」、活動方針を「当社の IT セキュリティにおける取組みの中核として、社内外の組織や専門家と協力し、セキュリティインシデントの検知、解決、被害局限化及び発生の予防を支援することにより、当社のセキュリティを向上すること」と定義してインシデント事前対応、事後対応を主な活動として行う。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

AIFUL-CSIRT

チームの正式名称	アイフルグループシーサート
チームの略称	AIFUL-CSIRT
所属する組織名	アイフル株式会社
設立年月日	2016年6月9日
チームの Email アドレス	csirt@aiful.co.jp
チームサイト	
所属組織サイト	http://aiful.jp
加盟年月	2017 年 01 月

1. 概要

我々は、経営理念『誠実な企業活動を通じて、社会より支持を得る』を、アイフルグループにおける最上位概念として理解し、これを達成するため、『四つの礎』『社員心得』『行動宣言10か条』の実践に努めています。
また、これらの理念のもと、全社員一丸となった企業活動を推進していくため、常に全社員がこれらの理念について確認し、行動の拠り所と出来るよう、携帯できるツールや社内環境の整備、各種勉強会を通じた意識浸透に積極的に取り組んでいます。
http://www.aiful.co.jp/topics/?cid=PFD0H010

2. 設立の経緯・背景

2015年1月のサイバーセキュリティ基本法の全面施行に伴う、2015年4月付、情報セキュリティ管理及びサイバーセキュリティ管理等に係る「貸金業者向けの総合的な監督指針」の一部改正を契機として、社内態勢の整備を実施し、標的型攻撃等のサイバー攻撃に早期警戒、解決するための技術的対応チームとして、AIFUL-CSIRTを発足するに至りました。

3. 会社内における位置づけおよび活動内容

(会社内における位置づけ)

AIFUL-CSIRT は、情報システム部門、コンプライアンス部門、広報部門を中心に構成されています。

(活動内容)

AIFUL-CSIRT は、以下の活動を実施しています。

・組織内で発生したインシデントの報告を受けるための一本化された窓口
・発生したインシデントに対応する、または、発生したインシデントへの対応に必要な技術的支援やノウハウを提供
・インシデント対応における組織としての意思決定を支援
・組織横断的に発生するインシデントにおいて、組織内の調整役として活動
・組織の情報システム管理者、ユーザ、その他の従業員に対し、セキュリティ教育と意識啓発

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

AkamaiJP-SIRT

チームの正式名称	アカマイ・テクノロジーズ合同会社セキュリティ対応チーム
チームの略称	AkamaiJP-SIRT
所属する組織名	アカマイ・テクノロジーズ合同会社
設立年月日	2016年7月14日
チームの Email アドレス	jpsirt@akamai.com
チームサイト	
所属組織サイト	https://www.akamai.com/jp/ja/
加盟年月	2016 年 12 月

1. 概要

Akamaiは企業が場所を問わず、あらゆるデバイスに安全で高パフォーマンスのユーザ体験を提供できるようサポートするクラウドサービスを代表するプロバイダーです。インターネットのWeb トラフィックの15-30%を配信するCDNプラットフォームを利用したクラウド型のWebセキュリティ、DDoS対策サービスなども提供しています。また、そのサービスの提供で得られた知見と解析されたデータをセキュリティインテリジェンスとして有し、各サービスにも反映しています。

2. 設立の経緯・背景

アカマイ・テクノロジーズ自身のセキュリティ・インシデント発生に備え、その発生時に、アカマイのセキュリティ・インシデント対応チームの一部としての迅速な対応の支援、および、問題の早期解決のために、日本シーサート協議会など外部のセキュリティコミュニティとの日本語による円滑な連絡を図るための窓口として「AkamaiJP-SIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

本チームは、以下の活動を通してアカマイ・テクノロジーズの情報セキュリティ対策強化を支援します。

1. アカマイ・テクノロジーズ自身のセキュリティ・インシデント発生時に適切な対応を実施するAkamai Infosecチームと連携した日本国内における情報共有

2. 日本国内で収集した自社に関わるインシデント情報のAkamai Infosecチームとの情報共有

3. ソフトウェアなどの脆弱性情報や最新のセキュリティインシデント情報の収集とその提供 (顧客・社内向け)

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ALSOK-CSIRT

チームの正式名称	ALSOK-CSIRT
チームの略称	ALSOK-CSIRT
所属する組織名	綜合警備保障株式会社
設立年月日	2014年4月15日
チームの Email アドレス	csirt-office@alsok.co.jp
チームサイト	
所属組織サイト	http://www.alsok.co.jp/
加盟年月	2016 年 09 月

1. 概要

ALSOKは1965年の創立以来50年にわたり、社会の安全安心の確保のために警備をはじめとするサービス・商品の提供を続けています。犯罪や自然災害などのさまざまなリスクから企業の情報を含む経営資源を守るノウハウと、全国に展開する高品質なサービス体制がALSOKグループの強みであり、これらを活用してお客様の企業秘密の管理体制を強化するなど、リスク低減に貢献していきます。

2. 設立の経緯・背景

昨今のサイバー攻撃の高度化や情報資産に関する事故が経営に与える影響が増大していることを背景に、重大な事故に対応する組織的な体制を確立するため、ALSOK-CSIRTが定義されました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
ALSOK-CSIRTは担当役員の判断により召集される直轄の組織です。

(2)活動内容
・サイバーセキュリティ関連情報収集
・社会的要請等の調査
・社内関係部署との連絡窓口
・CSIRT活動に係る訓練
・外部機関との連絡窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

AMUSE-SIRT

チームの正式名称	AMUSE-SIRT
チームの略称	AMUSE-SIRT
所属する組織名	株式会社アミューズ
設立年月日	2018 年 4 月 1 日
チームの Email アドレス	amuse-sirt@amuse.co.jp
チームサイト	
所属組織サイト	http://www.amuse.co.jp/
加盟年月	2018 年 05 月

1. 概要

AMUSE-SIRT はアミューズグループおよびサービスを提供するお客様に対し、当グループの IT セキュリティ事案の緊急時対応及び早期警戒を行うことを目的とした組織です。

アミューズグループは、コンテンツを生み出すアーティストを発掘・育成し、彼等に様々な形での創作活動を行う機会と場所を提供し、支援することでコンテンツを創出するとともに、外部の優良なコンテンツを探し出しております。そしてそのコンテンツをより多く保有し、有効に活用して事業展開することを基本方針としております。

2. 設立の経緯・背景

アミューズグループが保有する情報資産および顧客情報のセキュリティ対策に注力し、安心かつ信頼いただけるサービスの提供に努めるために 2010 年に「JIS Q 27001:2006」認証を取得し情報セキュリティマネジメントシステム活動を継続してまいりました。

ISMS 活動の中で事業継続対応訓練を実施していく上で、昨今のサイバーセキュリティインシデントにより閲覧利用者の多いファンクラブ・サイトの改ざん、ファンに提供するオンラインショップにおける不正侵入などは社会に大きな影響を及ぼすことが考えられるため、インシデントの発生時の迅速な対応、適切な判断による未然の防止が求められることを認識し、アミューズグループ全体を通しての体制づくりが必要であることを確認し CSIRT 体制を計画運用するにいたりました。

3. 会社内における位置づけおよび活動内容

AMUSE-SIRT は、CISO (情報セキュリティ統括責任者) の指揮の下、アミューズグループおよびサービスを提供するお客様に対し、次のサービスを提供する組織です。

(1) インシデント事後対応サービス
社内外の関係組織と連携し、インシデントの影響範囲・原因の特定、被害拡大防止・復旧、再発防止策の検討等の活動を行う。
(2) インシデント事前対応サービス
インシデント発生の未然防止を目的としたサービスであり、セキュリティイベントの検知やインシデント発生の可能性を減少させるための活動を行う。
(3) セキュリティ品質向上サービス
社内のセキュリティの品質を向上させることを目的としたサービスであり、AMUSE-SIRT としての視点や専門的な知見を社内外の関連組織・関連部署に提供すると共に、必要な活動を行う。
(4) 上記を実行するための仕組みを整備及び維持する。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

aratana-CSIRT

チームの正式名称	Aratana Computer Security Incident Response Team
チームの略称	aratana-CSIRT
所属する組織名	株式会社アラタナ
設立年月日	2013-06-01
チームの Email アドレス	security@aratana.jp
チームサイト	
所属組織サイト	http://www.aratana.jp/security/
加盟年月	2013 年 08 月

1. 概要

aratana-CSIRT は、ネットショップを「つくる技術」と、その運営を「サポートする技術」で、お客様のネットショップビジネス成功のためのサービスを提供している宮崎発の IT 企業である株式会社アラタナ（以下、アラタナ）の CSIRT です。

2. 設立の経緯・背景

ネットショップが取引の主要なインフラになりつつある昨今、2013 年 4 月の時点でアラタナが納品したネットショップ構築実績数は 700 を超えています。
取り扱い製品に対する社会的責任という観点から、情報セキュリティの取り組みを強化するとともに、多様化するインシデントに対応するチームの運用を開始。
2013 年 6 月に aratana-CSIRT を設置しました。

3. 会社内における位置づけおよび活動内容

aratana-CSIRT は、アラタナ経営層直轄の組織です。
アラタナが開発したサービスを契約しているお客様が、アラタナのサービスを起因とするインシデントに巻き込まれた場合、その被害の軽減と迅速な復旧に取り組みます。
また、主に国内 E コマース関連の CSIRT と連携しつつ、日本の E コマース全体における情報セキュリティの向上に取り組んでいます。

【アラタナについて】
アラタナはネットショップを『つくる技術』と、その運営を『サポートする技術』をコアコンピタンスとして、お客様の WEB ビジネス成功のためのサービスを行っています。2007 年設立から 2013 年までに 3000 社を超えるお客様にサービスをご利用頂いており、今後も当分野に特化したサービスの充実、拡大を図って参ります。

会社名 ：株式会社アラタナ（http://www.aratana.jp/）
本社所在地 ：〒880-0805 宮崎県宮崎市橘通東4丁目8番1号 カリーノ宮崎7階
代表取締役 ：濵渦伸次
事業内容 ：ネットショップ制作 他

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ASAHI-CSIRT

チームの正式名称	アサヒグループサイバーセキュリティ対応チーム
チームの略称	ASAHI-CSIRT
所属する組織名	アサヒグループホールディングス株式会社
設立年月日	2016年　8月　1日
チームの Email アドレス	asahi-csirt@asahigroup-holdings.com
チームサイト	
所属組織サイト	http://www.asahigroup-holdings.com/
加盟年月	2016 年 10 月

1. 概要

アサヒグループサイバーセキュリティ対応チーム（ASAHI-CSIRT）は、酒類事業・飲料事業・食品事業を基幹事業として展開するアサヒグループのセキュリティインシデントに対応するCSIRTです。

2. 設立の経緯・背景

近年、企業が保有する個人情報や重要な技術情報等を狙ったサイバー攻撃が増加傾向にあります。その手口も特定の組織を狙って巧妙化しており、セキュリティ対策製品等の導入だけでは防ぎきれなくなってきております。2015年12月には、経済産業省から「サイバーセキュリティ経営ガイドライン」が発表され、経営者のリーダーシップの下での体制整備と対策の推進、社会やステークホルダーに対する情報開示の在り方等についての取り組みが求められており、一年を通して、アサヒグループセキュリティポリシーに基づくPDCAマネジメントの実践を支援することにより、アサヒグループのセキュリティ対策の継続的改善を実施しております。

3. 会社内における位置づけおよび活動内容

ASAHI-CSIRTは、アサヒグループホールディングスCIO配下でグループ向けにインシデント対応等の支援を実施するアサヒグループホールディングス(株)及びアサヒプロマネジメント(株)、アサヒビジネスソリューションズ(株)の共同チームとしております。各事業会社やシステムのPoCと連携してグループで発生したインシデントの被害を低減し、平時においてもセキュリティに関する最新の脅威や脆弱性等の情報を継続的に収集・分析し、適時・適切な予防策の実施をしております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ASERT Japan

チームの正式名称	Arbor Security Engineering & Response Team Japan
チームの略称	ASERT Japan
所属する組織名	アーバーネットワークス株式会社
設立年月日	2016年9月6日
チームの Email アドレス	asert-japan@arbor.net
チームサイト	
所属組織サイト	http://jp.arbornetworks.com/
加盟年月	2017 年 07 月

1. 概要

アーバーネットワークスは、世界の主要なサービスプロバイダーとの関係構築を通して、攻撃の発生状況をグローバルなスケールでモニタリングを行い、主要なネットワークやオリンピック、ワールドカップをはじめとする代表的なイベントをサイバー攻撃（DDoS攻撃、ボットネット攻撃等）から守るテクノロジー、ソリューションを提供。

2. 設立の経緯・背景

2016年9月6日にサイバーセキュリティ調査機関ASERT（Arbor Security Engineering & Response Team）を日本に展開し、ASERT Japanを開設。その後、日本国内のいくつかのサイバーセキュリティに関連したコミュニティとの連携を強化及び貢献活動の基盤構築。

3. 会社内における位置づけおよび活動内容

• 位置づけ：
・サイバーセキュリティ調査機関としてのASERTの日本領域を担当。

• 活動内容：
・サイバー脅威に関する監視及び調査。
・サイバー脅威に関する技術的分析。
・コミュニティに対する、得られたサイバー脅威の認識共有。
・ASERTブログ（http://jp.arbornetworks.com/asert/）を通したサイバーセキュリティに関する知見の発信。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ASICS-CSIRT

チームの正式名称	ASICS Computer Security Incident Response Team
チームの略称	ASICS-CSIRT
所属する組織名	株式会社アシックス　グローバルIT統括部
設立年月日	2016年10月10日
チームの Email アドレス	AHQ-CSIRT@asics.com
チームサイト	
所属組織サイト	http://www.asics.com
加盟年月	2016 年 12 月

1. 概要

アシックスは、東京2020ゴールドパートナー（スポーツ用品）です。アシックスグループは、スポーツによる青少年の育成を通じて、社会の発展に貢献したいという思いから始まりました。私たちは、その創業の精神を受け継ぎ、60年以上にわたり、社会環境の変化を捉えながら、独自の製品とサービスを提供し、今日では、フットウエアとアパレル事業を中心に50以上の国と地域に拠点を置くまでに成長しました。今後当社は、東京2020オリンピック・パラリンピックに向けて、国内はじめ海外のアスリートならびにユーザ様へ、当社のスポーツ事業を通じ、よりさらなる貢献をしたいと思います。

2. 設立の経緯・背景

2015年に当社（本社・神戸）の情報セキュリティ委員会、ならびに情報セキュリティ事務局が発足した背景がある一方、運用フェーズに差し掛かった折、海外にあるグローバルオフィスにおいて、クリティカルかつ緊急性の高いインシデントが多発しました。現行のスタンダード文書においては、インシデント対応手順とフローは明記されているものの、情報セキュリティ委員会や事務局による運用体制では、国内外地域をカバーしつつ、迅速かつ的確な対応が難しいといった課題が発生しています。
この機会をふまえ、かつ2020年東京オリンピック・パラリンピックに向けて、国内拠点はじめ海外オフィスとの情報交換やインシデント対応のホットラインとPOC（Point of Contact）の設置の必要性があることから、当社インシデントレスポンスチームが結成された経緯があります。

3. 会社内における位置づけおよび活動内容

1. 事後対応サービス
①インシデントハンドリング
重大度（緊急・警告・注意・情報）の切り分けとリスクの優先付け
発生したインシデントの一次原因の特定とその封じ込めを実施
②インシデントレスポンス
影響ある関係子会社へのインシデントの対応支援やセキュリティアドバイザリー業務
国内CSIRTとの情報交換、ならび関係機関（地元警察）との連携・報告・調整
③脆弱性管理
当社環境（サーバ・PC）に対する脆弱性診断やハッキング手法を用いたセキュリティ監査
当社のクラウド環境やシステム基盤に対する脆弱性を低減するためのパッチ対策と運用管理の実施

2. 事前対応サービス
①アナウンスメント
マルウェア侵入時の検知レポートを元に、サイバー攻撃時における警告・注意喚起の実施
② 注意喚起と警告・通知
OSINTを情報源等を元に、サイバー攻撃に関する情報を収集し、組織内にて共有
③技術監視（モニタリング）
監視対象のネットワーク通信、不正侵入行為、関連する挙動のモニタリングの実施

3. インシデント管理サービス
①リスクマネジメント
当社の情報資産に対するリスク分析やアセスメント（影響度評価）を実施
②サイバーセキュリティ意識向上
当社情報セキュリティポリシーに準拠した情報セキュリティ教育の普及活動
当社国内拠点にある従業員の情報セキュリティに対する意識向上トレーニングの実施
③セキュリティ監査（アセスメント）

当社サービス対象に対する侵入検査（ペネトレーションテスト）の実施
当社インフラ運用上のセキュリティ監査の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Astellas-CSIRT

チームの正式名称	Astellas Cyber Security Incident Response Team
チームの略称	Astellas-CSIRT
所属する組織名	アステラス製薬株式会社
設立年月日	2017年4月1日
チームの Email アドレス	astellas-csirt@jp.astellas.com
チームサイト	
所属組織サイト	https://www.astellas.com/jp/
加盟年月	2017 年 09 月

1. 概要

アステラス製薬は、有用性と信頼性の高い医薬品で世界の人々の健康に貢献し、企業価値を持続的に向上させることを目指しています。Astellas-CSIRTはサイバー攻撃からアステラスグループを守る事で、営業秘密や個人情報等の機密情報を保護し、且つITシステムの継続的な運用により事業継続を確保する事で、薬の安定供給といった社会的責任を果たし、企業価値を維持する為に活動をしています。

2. 設立の経緯・背景

近年、サイバー攻撃はこれまで以上に技術が高度化し、攻撃手法も多様化してきました。また、サイバーインシデントは、グローバル全域にて事業に影響を及ぼすようになってきました。
当社は、従来より情報システム部門を中心にサイバー攻撃対策をグローバルで実施してきましたが、アステラスグループのビジネスをサイバー攻撃から守る為に、サイバーセキュリティ対策をより一層強化し、社内の関連職能、及び社外の専門組織との連携体制であるCSIRTを設立しました。
国内外のCSIRTメンバーと連携してグローバルで発生するサイバー・インシデントに対応をしています。

3. 会社内における位置づけおよび活動内容

1) 位置づけ
Astellas-CSIRT は、国内外の情報システム部門のセキュリティ担当、関係部門、および社外の専門組織により構成されています。

2) 活動内容
アステラスグループ内での脅威情報の共有、脆弱性管理、インシデント対応を中心に活動を行なっています

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ASY-CSIRT

チームの正式名称	ANA Systems Co., LTD. Computer Security Incident Response Team
チームの略称	ASY-CSIRT
所属する組織名	ANAシステムズ株式会社
設立年月日	2013-09-20
チームの Email アドレス	ml_oth_asycsirt@anasystems.co.jp
チームサイト	
所属組織サイト	http://www.anasystems.co.jp/
加盟年月	2013 年 09 月

1. 概要

ASY-CSIRT は、ANA システムズ株式会社 (http://www.anasystems.co.jp/) によって運営されている CSIRT です。

ANA システムズ株式会社は、ANA グループの IT 企業として、エアラインビジネスに直結した企画・提案、大型プロジェクトの受託開発、フィールドへの展開から稼働後のシステム運用ま で幅広く品質の高いトータルサービスを提供しています。

2. 設立の経緯・背景

近年、サイバー攻撃の高度化・複雑化による情報セキュリティ事件・事故が日本国内でも数多く報告されています。こうした状況を踏まえて、これまで ANA および ANA グループでは、サイバー攻撃 (情報漏えい、情報改ざん、サービス妨害など) から情報システムを守るために、セキュリティ事故の予防活動や事故発生時の早期復旧を目指した活動を様々行ってきました。しかしな がら、年々高度化・巧妙化しているサイバー攻撃に対して自社のみの活動には限界があり、情報収集面や知識面において他社や外部団体との連携の必要性から、外部組織との連携強化を目的と して ASY-CSIRT として、日本シーサート協議会に加盟いたしました。

3. 会社内における位置づけおよび活動内容

ASY-CSIRT は、ANA システムズ株式会社のセキュリティ専門部署に所属するメンバーで構成されている仮想的なチームです。当チームは、お客様に ANA 及び ANA グループが提供する情報システム (国内線・国際線の予約システム (ANA SKY WEB) など) を安心してご利用いただくために、情報システムのセキュリティ対策を強力に推進し、情報セキュリティ事故を未然に防止するための活動を継続的に図っています。

ASY-CSIRT の活動は、セキュリティ事故を未然に防止するための活動と外部団体との連絡窓口を主な活動として位置づけています。また、セキュリティ事故が発生した際には、社内の事故 対応を行うシステム運用部門と協力して、セキュリティ事故の早期復旧および影響範囲の極小化に努めています。

【ASY-CSIRT の主な活動内容】
① 情報収集・分析
コンピュータ・セキュリティ・インシデントに関連した情報の収集・分析
② インシデント事前対応
セキュリティ・インシデント発生に備えたプロセスの確立及び手順書類の作成・改訂
③ インシデント対応支援
インシデントの早期解決及び影響範囲の極小化に必要な ANA グループに対する支援
④ 外部団体との連絡窓口
日本シーサート協議会などの外部団体との連絡窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

AT-CSIRT

チームの正式名称	NTTアドバンステクノロジ　コンピュータセキュリティインシデント対応チーム
チームの略称	AT-CSIRT
所属する組織名	NTTアドバンステクノロジ株式会社
設立年月日	2016年8月1日
チームの Email アドレス	at-csirt@ml.ntt-at.co.jp
チームサイト	
所属組織サイト	http://www.ntt-at.co.jp
加盟年月	2017 年 10 月

1. 概要

AT-CSIRTはNTTアドバンステクノロジ株式会社及びNTTアドバンステクノロジグループ会社の組織内CSIRTです。

2. 設立の経緯・背景

NTT グループ各社のセキュリティ関連組織と連携し、NTTアドバンステクノロジおよび NTT アドバンステクノロジグループ各社のサイバーセキュリティ対策の推進に取り組んでいます。
NTTアドバンステクノロジでは、AT-CSIRT設立以前から情報セキュリティインシデント対応や情報セキュリティの社内統制を行ってきました。
しかし、年々、巧妙化・高度化するサイバー攻撃の脅威やその被害が増大していること、情報セキュリティインシデントが会社に与える影響度合いがますます高まっていることから、更なる社内統制とその対応の強化・迅速化を図るためにAT-CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

AT-CSIRTは NTTアドバンステクノロジの情報セキュリティを統括する情報セキュリティ推進部に設置されています。社内で発生した情報セキュリティインシデントに対し、現場の対応支援や組織間の調整を行い、被害の最小化を図っております。また、脆弱性情報等の社内展開や対処状況管理、セキュリティ関連情報の配信等を行っております。またインシデントの発生予防、発生時の対応改善の観点から社内の情報セキュリティ教育、啓発及び、幹部を含めてのインシデント対応訓練を行っております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ATENA-SIRT

チームの正式名称	株式会社アテナ　サート事務局
チームの略称	ATENA-SIRT
所属する組織名	株式会社アテナ
設立年月日	2015-10-01
チームの Email アドレス	atena-sirt@atena.co.jp
チームサイト	
所属組織サイト	http://www.atena.co.jp
加盟年月	2016 年 06 月

1. 概要

弊社は昭和43年6月にダイレクトメールの発送代行会社として設立されました。
その後、クライイアント各社様からのご要請に応じて、販売促進およびダイレクトマーケティング分野におけるトータルアウトソーサーとして成長してまいりました。現在では、メーリング、物流（3PL)、コールセンター、データ入力センター、印刷、フルフィルメント等の機能を提供できる体制を整えております。
業務の性質上、個人情報等を取り扱う事も多く、機密性の高い情報を一気通貫で取り扱えることを強味として、数多くの有力企業様からも厚い信頼を頂戴できているものと自負しております。その強味を支えるインフラとして、プライバシーマーク・QMS・ISMSといった第三者認証も取得していますが、今後更に情報セキュリティ・品質管理に万全を期してまいりたいと考えております。

＜国内拠点＞東京本社・大阪支店、東京物流センター・・大阪物流センター・名古屋物流センター、北海道IT-BPOセンター、新大阪センター
＜海外拠点＞アテナ上海(100%出資現法)

2. 設立の経緯・背景

サイバー攻撃による個人情報漏洩事件が増加している社会情勢に鑑みて、当社においても2015年にCSIRT組織(ATENA-SIRT)を発足しました。
当社は個人情報等の機密性の高い情報を大量に取り扱う業態であり、お客様からお預かりしている情報を守るという使命を果たすことが企業の存立基盤と言っても過言ではありません。
しかし、近年のサイバー攻撃は巧妙化・複雑化しており、その手法も日々変化しています。したがって、貴協議会に加盟し、様々な事例やセキュリティ対策等に関する情報を共有させて頂きたいと考えております。
また、当社からも個人情報を取り扱う事業者として長年培ってきた経験とノウハウをもって、貴協議会に微力ながら貢献できればと思っております。

3. 会社内における位置づけおよび活動内容

ATENA-SIRTは、社内及びグループ会社における情報セキュリティに関する情報収集と予防策立案・推進を日頃から実施するとともに、万一インシデントが発生した場合には緊急対応を実施するチームです。メンバーは、セキュリティインシデントに関連性の深い部署からメンバーを募り、本来業務と兼務で参画しているバーチャルチーム(専任者はいないが、システム開発部が事務局を兼務)として活動を行っています。毎月の定例ミーティングのほか、インシデントが発生時等にはメンバーを緊急招集して即座に必要な対応を実施しています。
（役割）
1. セキュリティに対する情報収集・対策立案
2. セキュリティインシデントに対する対策決定・経営への報告
3. セキュリティ対策の周知徹底、見直し・ルール化、教育訓練
4. セキュリティインシデント発生時の連絡窓口、対応策指示
5. 貴協議会への連絡窓口
（活動内容）
ATENA-SIRTメンバーの協議により、セキュリティルールの見直し・策定を行い、従業員のセキュリティ認識度向上のために社内及びグループ会社向けの情報発信を行っています。
例えば、、標的型攻撃メールに対する注意喚起後に、ダミーメールによる抜打ちテストを行ない、ミス発生者に対する対するフォロー研修も実施しました。また、新入社員研修にはSTC活動で紹介されている「スシコン」を導入し、新人教育につなげるなど、具体的な活動を実施しています。その他にも単なる注意徹底にとどまらない可視化できるレベルでの教育訓練を定期的に継続していく予定です。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

avex-sec

チームの正式名称	エイベックスグループセキュリティ事務局
チームの略称	avex-sec
所属する組織名	エイベックス株式会社
設立年月日	2013-10-01
チームの Email アドレス	avex_group_security@av.avex.co.jp
チームサイト	
所属組織サイト	http://www.avex.co.jp/
加盟年月	2016 年 05 月

1. 概要

エイベックスグループセキュリティ事務局は、エイベックス株式会社にて運営され、エイベックスグループ会社全体の情報セキュリティへの取り組みを推進しています。

2. 設立の経緯・背景

情報セキュリティを個社毎で対応していては、セキュリティ対策の抜け落ちがでる可能性があるため、グループ全体の情報セキュリティを技術面、非技術面の両側面から見る組織が必要となったためです。

3. 会社内における位置づけおよび活動内容

エイベックスグループの持ち株会社であるエイベックス株式会社内のセキュリティ専門部門が当事務局業務を担い、エイベックスグループ各社に対し、以下の活動を行っています。
・規定・ガイドラインの整備
・セキュリティ対策の企画、導入、維持運用
・インシデントレスポンス
・脆弱性情報の発信、および対応指示
・従業員教育
・セキュリティヘルプデスク

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

AXA Japan CSIRT

チームの正式名称	アクサジャパン CSIRT
チームの略称	AXA Japan CSIRT
所属する組織名	アクサ生命保険株式会社
設立年月日	2016年1月1日
チームの Email アドレス	axa-japan-csirt@axa.co.jp
チームサイト	
所属組織サイト	http://www.axa.co.jp/
加盟年月	2016 年 12 月

1. 概要

AXAグループは日本において保険事業、資産運用事業、アシスタンス事業など、多岐にわたるビジネスを展開しています。保険事業では、アクサ生命、アクサダイレクト生命、アクサ損害保険の3社が「アクサ ジャパン グループ」を形成し、相互の連携を深めるとともに、その他のAXAメンバーカンパニーと密接に連携しながら、お客さまをリスクからお守りするための商品・サービスをご提供しています。アクサジャパンCSIRTはアクサ生命保険株式会社により運営されている組織内のCSIRT（仮想組織）です。

2. 設立の経緯・背景

サイバーセキュリティ対策の重要性については、アクサグループ全社共通の経営課題として認識され情報セキュリティ戦略に組み込まれております。アクサ情報セキュリティポリシーに定める情報資産の保護及び管理に基き、認識されたサイバーリスクに関して安全管理対策の継続的な向上のための基盤としてアクサジャパン CSIRTを設置し対策強化を進めております。

3. 会社内における位置づけおよび活動内容

アクサジャパン CSIRTは、サイバーリスク及びセキュリティインシデントに関する緊急時対応及び早期警戒のための活動を行ないます。セキュリティツールによるITインフラの監視、およびアクサグループ全体でセキュリティ脆弱性情報の収集をしています。緊急時には、危機管理・事業継続部門と連携し危機管理チームを招集し、全社体制で対応を実施します。サイバーリスクの評価・管理については、統合リスク管理部門とも連携します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

B2SIRT

チームの正式名称	B2SIRT
チームの略称	B2SIRT
所属する組織名	株式会社ブロードバンドセキュリティ
設立年月日	2013-12-01
チームの Email アドレス	b2sirt@bbsec.co.jp
チームサイト	
所属組織サイト	https://www.bbsec.co.jp/
加盟年月	2015 年 07 月

1. **概要**
   株式会社ブロードバンドセキュリティ (BBSec) は企業固有のセキュリティポリシーに直結するサービスをコアサービスとし、コアサービスを実現するために必要な各種サービスをクラウドと位置づけ、IT セキュリティ全体を網羅したサービスを展開しています。
2. **設立の経緯・背景**
   24 時間 365 日稼働している当社セキュリティオペレーションセンターで検知されるインシデント対応の高度化や、その他セキュリティ事案に対応するため、2013 年 12 月に自社内の組織横断で知見を共有するチームを設立しました。
3. **会社内における位置づけおよび活動内容**
   自組織及び当社顧客のインシデントの早期解決を推進することを目的として、自社内の組織横断でチームを設立しました。インシデント発生時のインシデントレスポンス、脆弱性ハンドリング等に中心となるメンバーで構成されています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

B-EN-G CSIRT

チームの正式名称	B-EN-G CSIRT
チームの略称	B-EN-G CSIRT
所属する組織名	東洋ビジネスエンジニアリング株式会社
設立年月日	2016年7月31日
チームの Email アドレス	csirt-office@to-be.co.jp
チームサイト	
所属組織サイト	http://www.to-be.co.jp/
加盟年月	2016 年 09 月

1. 概要

1999年、東洋エンジニアリング株式会社よりシステム設計・開発・外販部門が分離・独立し開業
2014年、東京証券取引所市場第一部銘柄に指定（4月4日付）

IT 企画、システム導入などのコンサルティングサービス、企業向けシステムソリューションの開発・販売・サポート
ERP、SCM、SOA、CRM 等の SI サービス、システム運用保守サービス、クラウドサービス

2. 設立の経緯・背景

1999年の会社設立後、2002年度より情報セキュリティ委員会を設置し、社内業務において発生する様々なセキュリティインシデントへの対応や従業員の教育・啓蒙活動を行ってきた。

現在は、高度化・複雑化するセキュリティインシデントに適時・適切に対応するために、組織横断的なチームを構成し，情報収集やインシデント対応を効率的・効果的に行うことが必要となっている。
またセキュリティインシデントは外部からの連絡により顕在化することもあり、またセキュリティインシデントに関する非公知の情報や有用な対応策を得るために、体外的窓口が必要である。
経産省・IPAが策定した「サイバーセキュリティ経営ガイドライン」でCSIRTの設置が推奨されており，当社顧客を含む大手企業やCSIRTの設置が進んでいるため、顧客満足度向上のためにもCSIRTの設置が望ましいと考えた。

このような状況に鑑み、上記のインシデント対応を行い、対外窓口機能を有するCSIRTを設立することとした。

3. 会社内における位置づけおよび活動内容

位置付け：
・情報セキュリティ委員会の下部チーム（仮想的な組織）

活動内容：
・社内システム、当社のSaaS型製品・ITサービスにおけるセキュリティ担当者間の役割分担の明確化、情報共有手段の構築と維持・改善
・対外窓口の設置と維持・改善。他のCSIRTなど外部組織・団体との情報交換
・インシデント発生を前提とした事前対策、インシデント発生時の対処、インシデントの事後対応
・上記に関する社内規程類の見直し

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

BICSIRT

チームの正式名称	ビックカメラ　シーサート
チームの略称	BICSIRT
所属する組織名	株式会社　ビックカメラ
設立年月日	2016年11月15日
チームの Email アドレス	bicsirt@biccamera.com
チームサイト	
所属組織サイト	http://www.biccamera.co.jp
加盟年月	2017 年 12 月

1. 概要

「都市型」×「駅前」×「大型」を中心とした店舗出店やインターネットショッピング事業の拡大を進め、情報通信機器商品、家庭電化商品等の販売事業を行うビックカメラが母体となった、サイバーセキュリティインシデントレスポンスチーム。

2. 設立の経緯・背景

2016/7　　社長直轄のもとセキュリティ委員会設立
2016/11　CISO管理下のCSIRTを設立（主な活動はセキュリティ委員会事務局による）
情報セキュリティ上のインシデント発生時の迅速な対応を実現し、ビックカメラグループの被害を最小限に抑える事を目的に設立。

3. 会社内における位置づけおよび活動内容

情報セキュリティを脅かすインシデント発生時に、迅速かつ適切な対応を行い、早期解決を目指す。
・セキュリティインシデント情報及び脆弱性情報の収集と対応。
・組織内のセキュリティインシデント窓口として活動。
・従業員に対してのインシデント注意喚起、セキュリティ意識向上の教育、訓練。
・警視庁サイバー犯罪対策課とのサイバー犯罪に対する共同対処協定締結。
・情報セキュリティ対策全般。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

BN-CSIRT

チームの正式名称	BN-CSIRT
チームの略称	BN-CSIRT
所属する組織名	株式会社バンダイナムコホールディングス
設立年月日	2016-01-28
チームの Email アドレス	bn-csirt@bandainamco.co.jp
チームサイト	
所属組織サイト	http://www.bandainamco.co.jp/
加盟年月	2016 年 03 月

1. 概要

バンダイナムコグループは、「夢・遊び・感動」を社会に提供することをミッションとして掲げる、エンターテインメント企業グループです。
玩具製造・販売、ゲーム開発・配信、映像音楽制作・販売、アミューズメント施設運営。および、それらの事業に必要な関連事業会社で構成されており、国内社、海外社を有しています (2015 年 12 月時点)
(http://www.bandainamco.co.jp)

2. 設立の経緯・背景

バンダイナムコホールディングスはグループにおける情報セキュリティ体制を維持する為の組織として、2008 年に「グループ情報セキュリティ委員会」を設置し、2009 年から国内グループ企業に対するセキュリティーポリシーを策定しました。2011 年からは、海外グループ向けにも国内同様のセキュリティポリシーを策定しております。さらに、2012 年からはグループの公開 WEB サイトを対象とした脆弱性診断を開始し、一定の効果を上げております。

昨今、世界的な風潮である企業 WEB への執拗な攻撃や内部不正による情報漏洩事件が、一般メディアで大きく取り上げられる時代になり、当グループとして今まで以上に情報セキュリティ対策を強化する必要があると考え、2014 年頃から CSIRT について調査を行うとともに、同業他社と意見交換などしてきました。

グループ内だけでなく、グループ外企業間のコミュニケーション網を作り、お互いに有益な情報をシェアすることで、自社他社ともに情報セキュリティ能力を高めることがエンターテイメント業界の利益に繋がると期待し、その活動基盤としては日本シーサート協議会が最も適していると確信しております。

3. 会社内における位置づけおよび活動内容

【会社内における位置づけ】
グループ情報セキュリティ委員会は情報セキュリティ担当取締役 (CISO) を責任者とし、情報システム部 GM を事務局長とした管理部門横断の組織となります。専任担当者はおらず、全員が兼務となっております。
グループ内で発生した情報セキュリティインシデントに対する直接的なレスポンス (例えば顧客や従業員に対して) は現在組織として対応しておらず、グループ内外で発生したインシデントの調査や自社含めたグループ各社の CISO 及び担当者に対する情報共有を主体としております。
委員会の下には複数の分科会があり、それらの分科会にはグループ主要各社の CISO や公開 WEB 責任者等が所属し、情報連携を密にとっております。

【活動内容】
1.グループの情報セキュリティ体制に関する情報の収集・分析及び改善策の企画・提案
2.グループの情報セキュリティ体制に関する規程等の見直し
3.グループの役員及び従業員に対する教育、啓発活動に関するモニタリング並びに支援
4.グループの情報セキュリティ活動に関するモニタリング並びに支援
5.情報セキュリティ事故予防策の企画並びにモニタリング

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

BNESIRT

チームの正式名称	バンダイナムコエンターテインメント サート
チームの略称	BNESIRT
所属する組織名	株式会社バンダイナムコエンターテインメント
設立年月日	2015-08-01
チームの Email アドレス	bnesirt@bandainamcoent.co.jp
チームサイト	
所属組織サイト	http://bandainamcoent.co.jp/
加盟年月	2015 年 09 月

1. 概要

BNESIRT は、株式会社バンダイナムコエンターテインメントが運営する SIRT です。

2. 設立の経緯・背景

従来より当社 WEB サービスのセキュリティ対策を進めておりましたが、近年深刻化するセキュリティ事情に鑑み、更なる安全なセキュリティ環境を整え、より新しく、より楽しい WEB サービスを安全にお客様に提供するため、BNESIRT を設立いたしました。

3. 会社内における位置づけおよび活動内容

BNESIRT は、CISO を頂点とした社内横断型のチームであり、当社が提供する WEB サービスのセキュリティ環境を整える活動を行っております。

・各種ガイドラインの策定 / 改訂
・当社が提供する全ての WEB サービスの管理
・セキュリティ情報関連情報の提供、及び社内啓発
・インシデントレスポンス

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

C-csirt

チームの正式名称	Chiba Univercity Cyber Security Incident Response Team
チームの略称	C-csirt
所属する組織名	国立大学法人千葉大学
設立年月日	2016年4月1日
チームの Email アドレス	c-csirt@chiba-u.jp
チームサイト	http://www.chiba-u.ac.jp/general/disclosure/security/c-csirt.html
所属組織サイト	http://www.chiba-u.ac.jp
加盟年月	2016 年 12 月

1. 概要

国立大学法人千葉大学は、10学部、10研究科(院)、3学府、学生数約1万4千人、教職員数約3,500人の、4キャンパス（西千葉、亥鼻、松戸、柏の葉）からなる大規模総合大学です。「つねに、より高きものをめざして」を大学の理念とし、国内及び海外の教育研究機関、行政、地域社会、そして企業等と積極的に連携し、知の発信拠点形成を推進して、社会への貢献及び文化と科学の発展に寄与することを目標として掲げております。

千葉大学情報危機対策チーム（C-csirt（シー・シーサート））は、サイバー攻撃等から千葉大学内の情報資産を保護するため、情報漏えいやWeb改ざんにつながる不正アクセス、マルウェア感染等のセキュリティ上の問題（インシデント）に対して、早期発見・早期対処することで被害を最小化することを目的として、予防活動、発生時の対応、改善策の検討及び提案を行うチームです。

2. 設立の経緯・背景

前身である千葉大学情報危機対策チームが2009年10月に設置され、当該チームがこれまでインシデント対応にあたってきましたが、2012年から2014年までの間に学内で発生した情報漏えいなどの事案が立て続けに発生したことを受け、情報危機対策チームの体制や機能を見直し、インシデント対応のみならず、インシデントの予防やセキュリティ意識の普及啓発、人材育成にも積極的に取り組むため、新たに「千葉大学情報危機対策チーム（C-csirt）」として再出発しました。

3. 会社内における位置づけおよび活動内容

(1) 位置づけ
C-csirtは、学長直属の組織である千葉大学情報セキュリティ委員会の下に設置され、本学の情報システム部門を中心としたコアメンバーと各部局の教職員から選出された部局メンバーで構成されています。

(2) 活動内容
主な活動は以下のとおりです。
・インシデント対応
・サイバーセキュリティに係る情報収集・分析
・学内外への注意喚起
・セキュリティ人材育成（教職員・学生に対する教育・訓練等）
・情報システム調達時の支援
・脆弱性検査
・法的観点からの助言
・他組織シーサート他、関係機関との情報セキュリティにおける連携・協力

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Bridgestone CSIRT

チームの正式名称	Bridgestone CSIRT
チームの略称	Bridgestone CSIRT
所属する組織名	株式会社ブリヂストン
設立年月日	2016-01-18
チームの Email アドレス	DL-bridgestone-csirt@bridgestone.co
チームサイト	
所属組織サイト	http://www.bridgestone.co.jp/
加盟年月	2016 年 02 月

1. 概要

Bridgestone CSIRT は株式会社ブリヂストン社内および関連会社のセキュリティ関係メンバーにより構成されるセキュリティインシデント対応のための組織です。

2. 設立の経緯・背景

ブリヂストンにおいては、以前より IT セキュリティに対する脅威への対策を実施して参りましたが、近年のサイバー攻撃の高度化・常態化を受け、それらの兆候を早期に検知し、迅速に対応するための施策の一環として CSIRT を設立いたしました。

3. 会社内における位置づけおよび活動内容

Bridgestone CSIRT は、IT セキュリティに携わるメンバーを中心に構成される仮想的な組織です。セキュリティインシデント発生時は関連部署や外部機関等との連携の窓口となり、インシデントハンドリングを行い、早期の事態鎮静化を図ります。平時においても、従業員への教育訓練等、IT セキュリティ向上のための施策を推進します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Canon-CSIRT

チームの正式名称	Canon-CSIRT
チームの略称	Canon-CSIRT
所属する組織名	キヤノン株式会社
設立年月日	2014-01-01
チームの Email アドレス	canon-csirt@jp.canon.com
チームサイト	
所属組織サイト	http://canon.jp
加盟年月	2015 年 02 月

1. 概要

Canon-CSIRT は、キヤノン株式会社により運用しているセキュリティインシデントレスポンスチームです。

2. 設立の経緯・背景

当社は、従来より情報セキュリティインシデントに対する対策や対応を実施してきましたが、情報セキュリティの脅威は、年々複雑化かつ巧妙化してきています。
このような状況において、セキュリティインシデントが発生した際に速やかに状況を把握、分析し、被害の最小化・極小化を実現することができるように体制を整備し、2015 年 1 月に「Canon-CSIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

Canon-CSIRT は、キヤノングループ内で発生する情報セキュリティインシデントに対して、「監視」、「対応」、「予防」活動を行います。
(1) 監視 (検知)
・セキュリティシステムのログの収集と分析
・脆弱性情報の収集
(2) 対応
・関連部門との連携強化や体制整備
・迅速な判断と適切な対応
(3) 予防
・情報セキュリティに関する教育・啓発 / 模擬訓練
・事例の共有による再発防止

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Canon-Elec-CSIRT

チームの正式名称	Canon Electronics CSIRT
チームの略称	Canon-Elec-CSIRT
所属する組織名	キヤノン電子株式会社
設立年月日	2015-07-01
チームの Email アドレス	cel-csirt@canon-elec.co.jp
チームサイト	
所属組織サイト	https://www.canon-elec.co.jp/
加盟年月	2015 年 10 月

1. 概要

Canon Electronics CSIRT は、キヤノン電子株式会社が運用しているセキュリティインシデントレスポンスチームです。

2. 設立の経緯・背景

当社は、情報システム部門とセキュリティ研究部門が協力して、情報セキュリティインシデントへの対策、対応を実施してきましたが、情報セキュリティへの脅威はますます高度化しています。
こうした状況を受け、セキュリティインシデントに対し、より組織的に対応することを目的に、2015 年 7 月に「Canon Electronics CSIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

Canon Electronics CSIRT は、情報システム部門とセキュリティ研究部門のメンバーから構成し、次の活動を行っています。
1. セキュリティインシデントの予防
・情報セキュリティ教育、啓発
・インシデントの動向分析に基づく、最適なシステム導入と運用

2. セキュリティインシデントの監視
・セキュリティアラートの監視と、ログ収集・分析

3. セキュリティインシデントへの対処
・対処フローの作成と模擬訓練
・インシデントのトレースによる波及防止措置

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Canon MJ-CSIRT

チームの正式名称	Canon Marketing Japan Group CSIRT
チームの略称	Canon MJ-CSIRT
所属する組織名	キヤノンマーケティングジャパン株式会社
設立年月日	2016-01-01
チームの Email アドレス	canonmj-csirt@canon-mj.co.jp
チームサイト	
所属組織サイト	http://cweb.canon.jp/corporate/index.html
加盟年月	2016 年 02 月

1. 概要

Canon Marketing Japan Group CSIRT は、キヤノンマーケティングジャパン株式会社が運営しているセキュリティインシデントレスポンスチームです。

2. 設立の経緯・背景

当社では、かねてより、グループをあげた情報セキュリティ活動に取り組んでおりますが、昨今、サイバー攻撃が多様化・高度化・巧妙化してきていることから、『「グループ内インフラ」および「お客様に提供する製品・サービス」に対するサイバーセキュリティのリスク・被害を極小化すること』を目的として、2016 年 1 月に「Canon Marketing Japan Group CSIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

Canon Marketing Japan Group CSIRT は、キヤノンマーケティングジャパン株式会社の IT部門内に事務局機能を置き、情報セキュリティ部門や製品・サービスの品質管理部門のメンバーから構成された組織です。
活動内容は、次の通りです。

1.予防
・脆弱性情報の収集
・各種予防対策の実施
・教育・啓発と訓練の実施
・危機管理態勢の整備
2.監視
・ログの収集と分析
・証跡保存
3.対応
・発生時から収束、再発防止まで一連の支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

CDI-CIRT

チームの正式名称	Cyber Defense Institute Cyber Incident Response Team
チームの略称	CDI-CIRT
所属する組織名	株式会社サイバーディフェンス研究所
設立年月日	2009-02-02
チームの Email アドレス	cirt@cyberdefense.jp
チームサイト	
所属組織サイト	http://www.cirt.jp/
加盟年月	2009 年 04 月

1. 概要

CDI-CIRT は、サイバーディフェンス研究所及びそのクライアントに対して、アラート (注意喚起) 及びサイバーセキュリティに関するインシデントハンドリング及びコーディネーション等サービス提供の拠点となることミッションとした、サイバーインシデントレスポンスチームです。

特に、サービス対象が攻撃元或いは被害者に関係なく、サイバーセキュリティ関するインシデントに巻き込まれた際、その調査や情報流通の調整をします。

2. 設立の経緯・背景

CDI-CIRT は、2009 年春、政府機関や重要インフラ事業者等において発生するサイバー攻撃のうち、極めて深刻なものに対して直接的かつ包括的に対処支援ができる能力を有するべく設置されました。

その後、高い技術と豊富な経験を有する分析官が参加し、現在のマルウェア (アーティファクト) 解析、デジタル / ネットワークフォレンジック、サイバー / オープンソースインテリジェンス等の能力を有するに至っています。

並行して、海外の実力を持ったチーム (米国 ICS-CERT、NATO や ICPO 等のレスポンスチーム)、サイバー脅威対処と関係性の深い領域 (テロ対策、危機管理、外交安全保障、インテリジェンスコミュニティ等)、そして、先進的なプロジェクト (米国 DHS の PREDICT 等) との積極的な連携強化を行なっています。

3. 会社内における位置づけおよび活動内容

対応活動における意思決定は、それぞれの領域の上級分析官が独自に行ないますが、領域を横断するものについては、上級分析官間の直接的調整或いは統括担当を介した調整を行う等、目的達成 (能力発揮) を重要視した最適な意思決定プロセスで行なっています。

メンバの活動動資金については、所属組織であるサイバーディフェンス研究所から支援を受けています。

基本的な活動内容は、メンバが独自に有するスキルや能力をベースにしていますが、最近は、領域を横断する「サイバー演習」や「ネットワーク・フォレンジック」に注力しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

CEC-SIRT

チームの正式名称	シーイーシー　SIRT
チームの略称	CEC-SIRT
所属する組織名	株式会社シーイーシー
設立年月日	2015-12-01
チームの Email アドレス	CEC_SIRT@cec-ltd.co.jp
チームサイト	
所属組織サイト	http://www.cec-ltd.co.jp/
加盟年月	2016 年 03 月

1. 概要

CEC-SIRT は、セキュリティサービスの専門家としてインシデントの予防・早期解決を実施し、セキュリティ問題を起因とする有事の際には、被害の最小化を目的としたセキュリティ対策を実施します。

2. 設立の経緯・背景

当社ではセキュリティ・インシデント対応は、社内セキュリティ対応部門での方針策定・対策・対応を行ってまいりました。
また、従来から当社事業部門においてシステム運用管理サービスがあり、社内外の様々な業種のインシデント対応等を行ってまいりました。
しかしながら、昨今のサイバー攻撃 / 標的型攻撃など多様化する脅威に対し、社内外との情報共有が不可欠と判断し、事業部門と合わせてセキュリティ・インシデント対応に取り組むチームとして発足させました。

3. 会社内における位置づけおよび活動内容

(位置づけ)
当社のセキュリティ・インシデント対応等を行う、会社・部署横断したチームとなります。

(活動内容)
CEC-SIRT は、当社のセキュリティ・インシデント対応を中心に、組織体制の整備と迅速かつ適切な事後対応を行います。また、最新脅威情報、脆弱性情報の収集、管理をし、また、セキュリティに関する意識向上と教育・啓蒙活動を行い、予防にも力を入れます。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

CHUDEN-CSIRT

チームの正式名称	中部電力グループセキュリティインシデント対応チーム
チームの略称	CHUDEN-CSIRT
所属する組織名	中部電力株式会社
設立年月日	2014-10-14
チームの Email アドレス	ml-chuden.CSIRT@c-net.ne.jp
チームサイト	
所属組織サイト	http://www.chuden.co.jp/
加盟年月	2015 年 10 月

1. 概要

CHUDEN-CSIRTは、中部電力株式会社の制御系・情報系システムにおけるセキュリティインシデントへの適切な対処、およびセキュリティ事故に対するリスクの極小化を目的とするCSIRTです。

2. 設立の経緯・背景

弊社では、昨今高度化・巧妙化しているサイバー攻撃の脅威に備え、セキュリティ対策の構築やインシデントレスポンス向上等の検討を行い、日々、中電CTIとともにセキュリティ事故の防止、および発生時のリスクの極小化に努めています。今回、全社的なセキュリティマネジメント体制整備の一環で、部門横断型の対応チームとして結成しました。他社や外部機関との連携・情報共有も目的として、日本シーサート協議会へ加盟しています。

3. 会社内における位置づけおよび活動内容

CHUDEN-CSIRTは、制御系・情報系システムのセキュリティマネジメントに精通したセキュリティスペシャリストによる部門横断型のチームです。社内のセキュリティ対策・規定類の構築、社員教育やインシデント対応を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

CLP-CSIRT

チームの正式名称	cloudpack-CSIRT
チームの略称	CLP-CSIRT
所属する組織名	アイレット株式会社
設立年月日	2014-10-01
チームの Email アドレス	csirt@cloudpack.jp
チームサイト	
所属組織サイト	http://cloudpack.jp/
加盟年月	2016 年 02 月

1. 概要

cloudpack とは
Amazon Web Services (AWS) の導入設計、環境構築、運用・保守までをトータルでサポートするマネージドホスティングサービスです。
EC2 や S3 をはじめとする AWS のプロダクトを、構築はもちろんのこと、24 時間サポートや、サービス監視、バックアップなどの作業代行や技術サポートを行い、お客様の運用負荷を可能な限り軽減することを目指しています。

2. 設立の経緯・背景

近年、インターネット基盤ソフトウェアで新たな脆弱性が多く発見されていることから、cloudpack では、ソフトウェア脆弱性への対応を強化するために、cloudpack 内にコンピュータセキュリティインシデント対応チーム (CSIRT) を設置しました。

3. 会社内における位置づけおよび活動内容

ソフトウェア脆弱性情報に対する大局的な判断や指揮を行い、技術的な調査、情報共有、脆弱性 対応を統括します。具体的には、脆弱性の影響の有無・緊急度の判断、対象となるユーザー様への告知全般、脆弱性収束の判断などを行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Con-SIRT

チームの正式名称	コンシストサート
チームの略称	Con-SIRT
所属する組織名	株式会社　コンシスト
設立年月日	2017年4月1日
チームの Email アドレス	consirt@consist.jp
チームサイト	
所属組織サイト	https://www.consist.jp/
加盟年月	2017 年 08 月

1. 概要

Consist SIRTは、株式会社コンシストに所属する組織内CSIRTです。
株式会社コンシストは、コンサルティングからシステム開発・運用・保守サポートまで、一貫した高品質なソリューションサービスを提供するSI企業です。

2. 設立の経緯・背景

情報セキュリティに関する脅威は年々増加し、その方法も巧妙化しています。また一方で内部関係者による情報漏えい事件も度々報道されています。そのような内外の環境下において、サイバーセキュリティ対策は企業経営における重要テーマであるとの認識に基づき、総合的セキュリティ対策強化の一環として、2017年4月に「Consist SIRT」を設立致しました。
当社は、セキュリティインシデント発生時において、迅速な状況の把握、適切な対応の実現、また平時からの情報収集、役職員への教育・啓蒙を実施できる自組織の情報セキュリティ対策の整備を進め、当社のコンサルティングサービスにおける情報セキュリティ対策支援メニューの内容拡充を図り、顧客に対するセキュリティ対策ニーズの実現にも貢献します。

3. 会社内における位置づけおよび活動内容

「Consist SIRT」は自組織、及び顧客企業に対して、
① セキュリティ関連規程類の整備
② 情報セキュリティに関する研修等教育機会の提供
③ 脆弱性情報やセキュリティに関する最新技術の収集と提供
④ ログやイベントの管理・監視
などの活動を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

CTC-SIRT

チームの正式名称	CTC Security Incident Response Team
チームの略称	CTC-SIRT
所属する組織名	伊藤忠テクノソリューションズ株式会社
設立年月日	2016年03月15日
チームの Email アドレス	ctc-sirt@ctc-g.co.jp
チームサイト	
所属組織サイト	http://www.ctc-g.co.jp/
加盟年月	2016 年 07 月

1. 概要

CTCは、お客さまからの様々なITシステムへのご要望に対して最適なソリューションをワンストップで提供しています。CTC-SIRTはCTCによって運営されている組織内のCSIRTです。

2. 設立の経緯・背景

CTCおよびCTCグループは、かねてより情報セキュリティに関するガイドラインを定めるなど、情報管理の確立と徹底に努めてまいりました。
しかしながら、標的型攻撃をはじめとするサイバー攻撃の高度化に伴い、CTCグループ内での情報共有とセキュリティインシデント発生時の対応能力の更なる向上を図ることを目的として、「CTC-SIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

・位置づけ
CTC-SIRTは、情報セキュリティのリスク管理部門やセキュリティデバイスの管理を担当する部門、セキュリティサービスを提供する部門で構成される仮想的なチームです。

・活動内容
・社内連携の強化
・リスク管理の継続的な改善
・情報セキュリティ対策の推進
・社内外への注意喚起、啓蒙活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

CW-CSIRT

チームの正式名称	NTT Comware Computer Security Incident Response Team
チームの略称	CW-CSIRT
所属する組織名	NTTコムウェア株式会社
設立年月日	2012年4月1日
チームの Email アドレス	cw-csirt@nttcom.co.jp
チームサイト	
所属組織サイト	http://www.nttcom.co.jp/
加盟年月	2016 年 12 月

1. 概要

CW-CSIRTはNTTコムウェア株式会社及びNTTコムウェアグループ会社の組織内CSIRTです。

2. 設立の経緯・背景

NTTコムウェアでは、CW-CSIRT設立以前からコンピュータセキュリティインシデント対策として、発生したインシデントの社内統制やその対応支援を行ってきました。
しかし、年々、巧妙化・高度化するサイバー攻撃の脅威やそれによる被害が増大していることから、更なる社内統制とその対応支援及び脅威情報の収集力強化を図るためにCW-CSIRTを設立させました。

3. 会社内における位置づけおよび活動内容

CW-CSIRTはNTTコムウェアグループの情報セキュリティを統括する品質生産性技術本部内に設置されています。NTTグループ内やフィールド（世の中）で発生したコンピュータセキュリティインシデントがNTTコムウェアグループ内で拡散しないように、脆弱性情報等の全社展開や社内で発生したコンピュータセキュリティインシデントの対応を一元的に行っています。また、インシデントの発生を予防する観点から社内の情報セキュリティ教育、啓発及び開発者向けのセキュリティ研修を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Cookpad CSIRT

チームの正式名称	Cookpad Computer Security Incident Response Team
チームの略称	Cookpad CSIRT
所属する組織名	クックパッド株式会社
設立年月日	2015/04/01
チームの Email アドレス	csirt@cookpad.com
チームサイト	
所属組織サイト	https://info.cookpad.com/
加盟年月	2016 年 08 月

1. 概要

Cookpad CSIRT はクックパッド株式会社およびクックパッドグループにおけるセキュリティインシデントに対応する組織内 CSIRT です。

クックパッド株式会社は、料理レシピの投稿・検索サービスである「クックパッド」を中心とした Web サービス企業です。近年では、クックパッドを「「毎日の料理」を中心とした生活インフラ」として進化させ、またクックパッドを運営してきたノウハウを基に海外展開を開始しており、国内外に20社程度の子会社・関連会社を展開しています。

2. 設立の経緯・背景

サービス、および会社規模の拡大に伴い、増大する情報セキュリティリスクに対し、様々な視点から最適な対応を進めることを目的として設立されました。

3. 会社内における位置づけおよび活動内容

Cookpad CSIRT は、サービス・オフィスの両面から情報セキュリティ対策やインシデントハンドリングを行うことを目的とした仮想的な組織であり、複数の部署からメンバーが参加しています。
主な活動としては以下3点が挙げられます。
・ 全社的な情報セキュリティリスクアセスメント
・ 情報セキュリティインシデント発生時のハンドリング
社内における情報セキュリティ関連情報の提供、啓発

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Cy-SIRT

チームの正式名称	サイボウズ株式会社 CSIRT
チームの略称	Cy-SIRT
所属する組織名	サイボウズ株式会社
設立年月日	2011-08-04
チームの Email アドレス	security@cybozu.co.jp
チームサイト	https://www.cybozu.com/jp/features/management/cysirt.html
所属組織サイト	http://cybozu.co.jp
加盟年月	2013 年 08 月

1. 概要

サイボウズ株式会社 CSIRT は、クラウドサービスの開始を機に、従来の体制を強化する形式で設立されました。社外の組織・専門家と協力して、インシデント発生の予防、早期検知、早期解決、被害が発生した場合の最小化を主眼とした活動をすることを目的としています。

2. 設立の経緯・背景

弊社では 2002 年から、弊社製品に関する脆弱性ハンドリングを実施してきましたが、2006 年に複数の弊社製品で脆弱性が検出されたことから、PSIRT を設立し組織的に脆弱性に取り組む体制を構築いたしました。
その後 2011 年に弊社クラウドサービスをリリースすることを機に、社内の PSIRT を強化し、Cy-SIRT として全社的なセキュリティインシデントに対応する体制を構築いたしました。

2016 年には 組織全体で必要とされるセキュリティ機能を再点検し、
セキュリティに関するヘルプデスクや、教育などの機能と CSIRT の機能を併せ持つ「セキュリティ室」を設置。
「セキュリティ室」と Cy-PSIRT が協力をして Cy-SIRT の運営にあたっています。

3. 会社内における位置づけおよび活動内容

Cy-SIRT はサイボウズ株式会社の中に設置されています。弊社サービスをご利用中のお客様または、ご利用を検討いただいているお客様を主な対象とし、以下のような活動を実施しています。
・弊社製品で発生する脆弱性情報に関するサポート対応
・弊社製品および、サービスにて発生したインシデントに関する情報管理および、発信
・セキュリティインシデントを予防するための情報収集、情報発信

2014 年 6 月からは、サイボウズが提供するサービスに存在する脆弱性を早期に発見し、改修することを目的として脆弱性報奨金制度を開始いたしました。本制度の運営を Cy-SIRT にて行っております。

脆弱性報奨金制度
http://cybozu.co.jp/company/security/bug-bounty/

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

D-SIRT

チームの正式名称	Daihatsu Motor Corporation Security Incident Response Team
チームの略称	D-SIRT
所属する組織名	ダイハツ工業株式会社
設立年月日	2014-12-01
チームの Email アドレス	d-sirt@dk.daihatsu.co.jp
チームサイト	
所属組織サイト	http://www.daihatsu.co.jp/
加盟年月	2014 年 12 月

1. 概要

D-SIRT は、ダイハツ工業株式会社内の関係部署で構成するセキュリティインシデントレスポンスチームです。

2. 設立の経緯・背景

ダイハツ工業株式会社は、これまでもお客様情報や営業秘密をはじめとする情報資産に対するセキュリティ向上のため、様々な対策を講じてきました。しかしながら、近年頻発、高度化するサイバー攻撃や不正アクセスなどへの対応や営業秘密や個人情報の内部漏えい発生時の対応の迅速化が求められています。

こうした状況を踏まえ、情報セキュリティインシデントが発生した場合に、迅速に対応し、被害拡大の防止やサービスの早期復旧を実現できるよう、2014 年に CSIRT 設立を計画しました。

その後 半年以上の準備期間を経て、2014 年 12 月 1 日、「D-SIRT」を設立する運びとなりました。

3. 会社内における位置づけおよび活動内容

D-SIRT は、IT・総務部門を中心とした組織であり、インシデント内容に応じて工場、技術、広報、総務等関係部署も参画します。
なお、まずはコンピュータ関連のインシデント対応からスタートしますが、今後社内で発生した情報セキュリティインシデントに幅広く対応することを考えているため、CSIRT ではなく SIRT としました。

主な活動内容
1.インシデントの未然防止活動
・リスク情報の収集
・定期的な社内点検
・社内体制やルール、教育、システム対策等の継続的な改善
2.インシデント対応
・発生時から解決までの一連の処理
(連絡受付、対応要否判断、分析、復旧、再発防止、報告など)
ダイハツ工業では、SIRT 設立を機に、情報セキュリティレベルの向上に一層努めてまいります。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

D2C-CSIRT

チームの正式名称	ディーツーシーシーサート
チームの略称	D2C-CSIRT
所属する組織名	株式会社D2C
設立年月日	2016/10/01
チームの Email アドレス	d2c-csirt@d2c.co.jp
チームサイト	
所属組織サイト	http://www.d2c.co.jp/
加盟年月	2017 年 01 月

1. 概要

D2Cは、モバイルを中核としたデジタル全般を事業領域とし、「デジタルマーケティング事業」、「ドコモ事業」をはじめ、アジアをはじめとした世界に向けて、これまで培ってきた実績、知見、ノウハウをグループ各社を通じて展開している。

2. 設立の経緯・背景

-情報収集能力の向上
・サイバー攻撃、マルウェアの流行状況がリアルタイムに入手できる外部環境の情報源を獲得すること。
・外部からの通報等を適切に受け付ける窓口の設置
-インシデント体制の強化と実行性の向上
・インシデント対応者のノウハウ、技術力の向上
・社内のインシデントの内容、規模に合わせた体制作り
・外部への発表や、業務の停止にかかわる重大な意思決定の実施者の設定と、その意思決定が可能な基準、規程といった支援体制の確立

3. 会社内における位置づけおよび活動内容

既存のISMS、PMSの運用体制をもとに、D2Cグループすべてのコンピュータインシデントに対応する。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

CyberAgent CSIRT

チームの正式名称	CyberAgent Computer Security Incident Response Team
チームの略称	CyberAgent CSIRT
所属する組織名	株式会社サイバーエージェント
設立年月日	2014-09-01
チームの Email アドレス	ca_csirt@cyberagent.co.jp
チームサイト	
所属組織サイト	https://www.cyberagent.co.jp/
加盟年月	2011 年 10 月

1. 概要

CyberAgent CSIRT は Ameba 事業、インターネット広告事業、スマートフォンアプリ事業、スマートフォンゲーム事業を展開する株式会社サイバーエージェントの組織内 CSIRT です。

2. 設立の経緯・背景

当初は各組織毎に IT セキュリティの向上および事故対応に当たっていたメンバーが、全社的なセキュリティ向上並びにインシデント対応を目的に集まった組織です。多種多様な事業を展開するサイバーエージェントにおいてセキュリティインシデントの検知並びに情報共有を行い早期での原因究明と問題点の排除・再発防止を目的に運営されています。

3. 会社内における位置づけおよび活動内容

CyberAgent CSIRT が定義している活動内容は以下の通りです。
・社内外におけるセキュリティインシデント報告窓口
・インシデントハンドリング
・セキュリティリスク アセスメント
・セキュリティの啓発並びに人材の育成

メンバーにはサービス開発を行う事業のセキュリティ担当者に加えて社内情報システム部門、法務部門、監査部門、人事部門、広報部門の担当者がふくまれインシデント予防・対応・再発防止における全体のコーディネーションを行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DAC-CSIRT

チームの正式名称	DAC Computer Security Incident Response Team
チームの略称	DAC-CSIRT
所属する組織名	デジタル・アドバタイジング・コンソーシアム株式会社
設立年月日	2017年10月3日
チームの Email アドレス	dac_csirt@dac.co.jp
チームサイト	
所属組織サイト	http://www.dac.co.jp/
加盟年月	2017 年 10 月

1. **概要**

   DAC-CSIRT は、メディアサービス事業、ソリューションサービス事業、オペレーションサービス事業を展開するデジタル・アドバタイジング・コンソーシアム株式会社の組織内CSIRTです。

2. **設立の経緯・背景**

   弊社では、従前からCSIRT機能を複数の部門でそれぞれ保持していましたが、提供するソリューションサービスの多様化、利害関係者の増加や脅威の巧妙化等、複雑化するインシデントリスクへの対応を通して全社的なセキュリティレベルの向上を図る為、このたび新たにDAC-CSIRTを組織化しました。

3. **会社内における位置づけおよび活動内容**

   DAC-CSIRT は、セキュリティマネジメント部門、インフラ開発部門、情報システム部門、法務部門のメンバーを中心に構成されています。平時には従業員教育、脆弱性検証・改善勧告、ポリシーの整備・見直し等、セキュリティインシデントの予防活動を行います。有事の際には社内外におけるセキュリティインシデント連絡窓口となり、社内サービス主管部門と連携しながら影響低減・解決支援を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DFL-CSIRT

チームの正式名称	Dai-ichi Frontier Life Computer Security Incident Response Team
チームの略称	DFL-CSIRT
所属する組織名	第一フロンティア生命保険株式会社
設立年月日	2016年4月1日
チームの Email アドレス	DFL-CSIRT@d-frontier-life.co.jp
チームサイト	
所属組織サイト	http://www.d-frontier-life.co.jp/
加盟年月	2016 年 07 月

1. 概要

第一フロンティア生命は、第一生命グループの会社として2006年12月に設立され、一時払の終身保険や個人年金保険といった貯蓄性商品を、銀行や証券会社などの金融機関を通じて販売しています。
DFL-CSIRTは、第一フロンティア生命の組織内における、サイバー攻撃に対応するチームです。

2. 設立の経緯・背景

これまでシステムセキュリティ環境向上の一環として取り組んできた「サイバーセキュリティ攻撃対応」について、高度化、巧妙化している昨今のサイバー攻撃動向を鑑み、組織内における体制を明確化するとともに、インシデント発生時の迅速かつ確実な対応による被害拡大防止、及び、平時の情報収集・社内広報によるサイバーインシデントの発生抑止を目的に、2016年4月に設立されました。

3. 会社内における位置づけおよび活動内容

DFL-CSIRTは自組織の情報システム部門を事務局として、社内関連部門やグループ会社と連携を図りながら、以下のような活動を実施しています。

インシデント事前対応
・インシデント検知、防御環境の整備
・インシデント対応プロセス・手順の整備
・脆弱性情報や他社発生事案の入手と自社環境への影響確認

インシデント事後対応
・対外的連絡体制の整備
・インシデントハンドリング

セキュリティ品質向上
・ 訓練実施、演習参加 (標的型メール攻撃訓練、インシデント対応演習)
・ 社内セキュリティ教育
・ 他社発生事案の社内告知、注意喚起
・ CSIRTメンバーの対応能力向上（研修、セミナー参加）

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DeNA CERT

チームの正式名称	DeNA Computer Emergency Response Team
チームの略称	DeNA CERT
所属する組織名	株式会社ディー・エヌ・エー
設立年月日	2011-12-01
チームの Email アドレス	cert@dena.jp
チームサイト	
所属組織サイト	http://dena.com/jp/
加盟年月	2012 年 01 月

1. 概要

DeNA CERT は DeNA の組織内 CSIRT です。

DeNA は、モバイル端末や PC 向けにプラットフォーム、ソーシャルゲーム、e コマースなどを提供するグローバル IT 企業です。

DeNA が運営するソーシャルゲームプラットフォーム『Mobage』では現在、多数のソーシャルゲームが日本、中国、韓国、欧米のユーザネットワーク向けに提供されています。

DeNA は 1999 年に東京で設立され、現在は世界 10 カ国にオフィスおよび開発スタジオを有しています。(http://dena.com)

2. 設立の経緯・背景

DeNA CERT は 2011 年に設立されました。設立の目的は DeNA が展開するサービス及び DeNA グループ全体を含む社内システム等をセキュアに保つことと、インシデントが発生した際に適切に対応できるようにすることです。

特に 2010 年 ～ 2011 年にかけてスマートフォンが普及し始めたこと、自社の海外展開が本格的に始まったことからこれまで以上にセキュリティが重要になるとの考えの下、DeNA CERT を設立しました。

また、NCA への加盟を通じて他社との連携による一層のセキュリティ強化を期待しています。

3. 会社内における位置づけおよび活動内容

DeNA CERT は仮想的な組織で、メンバーは複数の部署からアサインされています。

中心メンバーの多くは品質管理部門、セキュリティ技術部門からアサインされており、これらの部門は特定の事業部門には属さず全社横断的に品質やセキュリティに関するミッションを負っています。

活動内容には次のようなものがあります。
・自社サービスに対する脆弱性診断とアセスメント
・セキュリティポリシーやガイドラインの策定
・社内教育
・技術調査
・各種セキュリティに関する相談窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DIR-CSIRT

チームの正式名称	DIR グループCSIRT
チームの略称	DIR-CSIRT
所属する組織名	株式会社大和総研ホールディングス
設立年月日	2015-02-01
チームの Email アドレス	dir-csirt@dir.co.jp
チームサイト	
所属組織サイト	http://www.dir.co.jp/
加盟年月	2015 年 09 月

1. 概要

DIR-CSIRT は大和総研、大和総研ビジネス・イノベーションを中核とした大和総研グループの CSIRT です。

大和総研は、平成元年の創設以来、大和証券グループの中核的な情報創出機関として、リサーチ、コンサルティング、システムの 3 つの分野において、それぞれの専門家が時代のニーズに応える独自性の高い情報サービスを提供しています。

大和総研ビジネス・イノベーションでは、証券、銀行、保険などの金融機関、ならびに通信、流通などの一般事業会社のほか、官公庁、地方公共団体など、幅広い分野のお客様に対して高品質で信頼性の高い情報システムサービスを提供しています。

2. 設立の経緯・背景

近年のサイバー攻撃手法の高度化等による、世界的規模で生じているサイバーセキュリティに対する脅威の深刻化に伴い、「サイバーセキュリティ基本法」が 2014 年 11 月に施行され、金融庁においても、「金融商品取引業者等向けの総合的な監督指針」の「システムリスク管理態勢」のカテゴリに「サイバーセキュリティ管理」が盛り込まれました。
サイバー攻撃による被害の未然防止、迅速な対処による被害の拡大防止を目的として、金融機関のシンクタンクとして、サイバーセキュリティ管理態勢を強化するため、2015 年 2 月に DIR-CSIRT を設立いたしました。

3. 会社内における位置づけおよび活動内容

(位置づけ)
大和総研グループのサイバーセキュリティ対策を行う、会社・部署横断の組織
(活動内容)
・サイバー攻撃に対する情報収集、防御、監視、回復、演習などのサイバーセキュリティ対策の実施
・サイバーインシデント発生時、迅速な対処、情報連携等による被害の拡大防止対応
・サイバーセキュリティ対策に関する信頼できる総合窓口の提供
・情報セキュリティの品質向上対策の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DENSO SIRT

チームの正式名称	DENSO Security Incident Response Team
チームの略称	DENSO SIRT
所属する組織名	株式会社デンソー
設立年月日	2017 年 11 月 9 日
チームの Email アドレス	ZN6002_CSIRT@denso.co.jp
チームサイト	
所属組織サイト	https://www.denso.com/jp/ja/
加盟年月	2018 年 04 月

1. 概要

デンソーは、先進的な自動車技術、システム・製品を提供する、グローバルな自動車部品メーカーです。世界初製品や技術の提供を通じて、企業の社会的責任を果たしていきます。

DENSO SIRT は、IT 資産のセキュリティインシデントをハンドリングする CSIRT、製品に関連する脆弱性やセキュリティインシデントをハンドリングする PSIRT から構成される組織の総称です。

2. 設立の経緯・背景

デンソーでは、予てより総務部、情報システム部門等の関係部門が連携し、情報セキュリティ対策を推進してきました。しかしながら、近年高度化しているサイバー攻撃への対応や、製品や工場等つながる社会へのセキュリティ対策強化が必要であることから、全社 CISO を設置、その配下に全社の情報セキュリティを統括する情報セキュリティ推進室を組織しました。同時に、製品や会社に関わるセキュリティインシデントが万一発生した場合に備え、DENSO SIRT を立ち上げました。

3. 会社内における位置づけおよび活動内容

DENSO SIRT は、情報セキュリティ推進室、情報システム部、製品設計部門、IT 子会社のデンソー IT ソリューションズ等からなる組織横断的な仮想組織です。平常時には脆弱性や脅威情報の収集・展開によりセキュリティインシデントの未然防止に努め、緊急時にはチーム一丸となってインシデントの早期解決にあたります。

主な活動内容
1. 平常時
・脆弱性情報や脅威情報の収集・展開
・自社製品・サービスの脆弱性対応
・体制および対応プロセスの整備
・チーム要員育成 (訓練)
・社外組織との関係構築　など

2. 緊急時
・早期警戒情報の展開
・インシデント対応全般
・外部機関との連携　など

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

dit-CSIRT

チームの正式名称	dit-CSIRT
チームの略称	dit-CSIRT
所属する組織名	株式会社ディアイティ
設立年月日	2016年4月18日
チームの Email アドレス	dit-csirt@dit.co.jp
チームサイト	
所属組織サイト	http://www.dit.co.jp/
加盟年月	2016 年 11 月

1. 概要

(株)ディアイティは、「安全・安心な高度情報通信ネットワーク社会」の実現のために、技術・製品・サービスを提供するばかりでなく、情報セキュリティと安定した情報ネットワークを、社会インフラとして確立するためのあらゆる活動を行っています。

2. 設立の経緯・背景

当社は、お客様に向けたセキュリティ支援サービスとして、インターネット監視、ログ解析、フォレンジックサービスを提供しています。それら業務を遂行する中で得た知識、技術を社内の情報セキュリティ管理に応用するための実働組織としてdit-CSIRTを設置しました。

3. 会社内における位置づけおよび活動内容

dit-CSIRTは、社内の情報システム管理と情報セキュリティ管理を分掌する委員会の管下に置き、情報セキュリティの設計、実装、運用、インシデント対応を一貫して実行できる体制としました。

dit-CSIRTは、次のような活動を行います。
・脆弱性情報の収集とハンドリング
・ネットワークのリアルタイム監視
・社内監視センターによる、インターネット上のネガティブ情報の監視と流出情報の監視
・インシデントの原因分析（ログ分析、マルウェア解析等）
・インシデントからの回復支援、再発防止の提言

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DK-SIRT

チームの正式名称	大東建託セキュリティインシデントレスポンスチーム
チームの略称	DK-SIRT
所属する組織名	大東建託株式会社　情報システム部
設立年月日	2015-04-01（ISMS適用宣言）
チームの Email アドレス	dksirt@kentaku.co.jp
チームサイト	
所属組織サイト	http://www.kentaku.co.jp/
加盟年月	2017 年 01 月

1. 概要

弊社は大地の最有効利用を掲げて創業以来、土地有効活用の専門会社として、建築営業による地主様への賃貸経営の事業提案から始まり、賃貸物件の設計・施工、入居斡旋等の不動産仲介、そして建物の管理と賃貸経営に関する業務を一環して展開しています。
約8万人の地主（オーナー）様、約170万人の入居者様の個人情報および会社の機密情報をサイバー攻撃から守るためにも、情報セキュリティの維持強化への取り組みについて、近年、重要視されています。

2. 設立の経緯・背景

必要に応じて、社内外のネットワーク機器、サーバ及びPC等、ITインフラに対する対策を実施していますが、情報セキュリティ対策は一度行ったら終わりではなく、常に積極的な対策を行っていないと、新たな脅威に対応できないという側面を持っているため、環境の変化に合わせて、見直しと改善が求められます。
そこで、情報セキュリティの国際基準であるISMS（ISO27001）を取得し、「日進月歩で進歩する脅威」に対処するために、情報セキュリティ維持及び改善のPDCAサイクルを繰り返す体制を構築しました。
ISO27001認証取得日　2015年8月24日　（適用宣言　2015年4月1日）

3. 会社内における位置づけおよび活動内容

ISMS（ISO27001）については、1部門を特定して認証できることから、情報システム部門にて認証審査を受け、取得しました。情報システム部内での情報セキュリティへの意識は高まりつつあるものの、会社全体で俯瞰して見ると、標的型攻撃メール訓練の結果などを考慮しても、意識は不足しており、研修などの啓蒙活動を継続して行っていく必要があります。また、高度化するサイバー攻撃に対応するためにも、最新の情報収集や他社との情報共有についても、今後、取り組んでいく必要があります。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DL-CSIRT

チームの正式名称	DAI-ICHI LIFE Computer Security Incident Response Team
チームの略称	DL-CSIRT
所属する組織名	第一生命ホールディングス株式会社/第一生命保険株式会社
設立年月日	2013-08-09
チームの Email アドレス	dl-csirt01@dl.dai-ichi-life.co.jp
チームサイト	
所属組織サイト	http://www.dai-ichi-life.co.jp/
加盟年月	2013 年 09 月

1. 概要

DL-CSIRT (DAI-ICHI LIFE Computer Security Incident Response Team) は第一生命ホールディングスおよび第一生命保険のサイバーインシデント対応を行うCSIRTです。

2. 設立の経緯・背景

高度化・巧妙化するサイバー攻撃により様々な被害が発生する中、企業市民として期待される責務を積極的に果たすべく、サイバーセキュリティに関する態勢強化のために設立されました。

3. 会社内における位置づけおよび活動内容

3-1）位置づけ
- DL-CSIRTは、IT部門を中心に構成されています。
- DL-CISRTは、IT担当役員を代表としています。

3-2）活動内容
- 第一生命グループ会社内での制度面／技術面でのセキュリティ対策活動の推進
- 第一生命グループ会社内の脆弱性対策とインシデント対応の実施
- CSIRT 窓口として他の組織間連携によるセキュリティ対策活動の促進

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DMM.CSIRT

チームの正式名称	DMM.CSIRT
チームの略称	DMM.CSIRT
所属する組織名	合同会社DMM.com
設立年月日	2014-10-08
チームの Email アドレス	csirt@dmm.com
チームサイト	
所属組織サイト	https://dmm-corp.com/company/com/
加盟年月	2014 年 11 月

1. 概要

合同会社DMM.com および関連会社 (以下、「DMM.com グループ」という) は、デジタルコンテンツ配信事業、通信販売事業、オンラインレンタル事業、インターネット接続事業、オンライン英会話事業、モノづくり支援事業、太陽光発電事業などを手掛けています。
DMM.CSIRT は DMM.com グループの CSIRT です。

2. 設立の経緯・背景

当社が提供するWebサービスを安全にお客様に提供するため、日々高度化していくサイバー攻撃の脅威によるインシデントに対して、情報セキュリティ侵害事故の発生による被害極小化、および情報セキュリティ侵害事故の事前予防を実行するために、DMM.CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

＜会社内における位置づけ＞
・DMM.CSIRT は合同会社 DMM.com テクノロジー本部 セキュリティ部を中心に構成されています。
＜活動内容＞
・脆弱性情報ハンドリング、サイバー攻撃によるセキュリティインシデントハンドリング

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DNP-CSIRT

チームの正式名称	DNP Group Computer Security Incident Response Team
チームの略称	DNP-CSIRT
所属する組織名	大日本印刷株式会社
設立年月日	2001-11-01
チームの Email アドレス	dnp-csirt@cansec.dnp.co.jp
チームサイト	
所属組織サイト	http://www.dnp.co.jp
加盟年月	2016 年 03 月

1. 概要

DNP-CSIRT は、DNP 大日本印刷株式会社が運営する組織内 CSIRT です

「DNP グループは、人と社会をつなぎ、新しい価値を提供する」を企業理念として掲げ、DNP グループを挙げて新しい価値の創造による事業拡大に取り組んでいます。

2. 設立の経緯・背景

2001 年 11 月より、情報セキュリティ委員会事務局として発足し、現在はDNPグループ情報セキュリティ委員会情報セキュリティ本部として情報セキュリティ活動を行っています。
サイバー攻撃が巧妙化・高度化してきており、外部機関や他社の CSIRT との情報共有や連携を通じ、自社のさらなるセキュリティ強化とインシデントの早期検知・迅速な対応を図るため、日本シーサート協議会へ加盟しました。

3. 会社内における位置づけおよび活動内容

(会社内における位置づけ)
　情報セキュリティ本部は、本社のDNPグループ情報セキュリティ委員会の下部組織として設置され、DNPグループのコンピュータ・ネットワークセキュリティを含む情報セキュリティ全般を統括しています。

(活動内容)
・情報セキュリティに関する方針・諸規程の立案
・情報セキュリティの教育・啓蒙
・各組織・グループ会社での情報セキュリティ活動の支援
・脆弱性情報などに基づく対策指示
・不測事態発生時の各組織への指示、支援

その中で、DNP-CSIRT は、情報セキュリティ本部においてコンピュータ・ネットワークセキュリティを担当しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DOCOMO-CSIRT

チームの正式名称	DOCOMO Computer Security Incident Response Team
チームの略称	DOCOMO-CSIRT
所属する組織名	株式会社 NTTドコモ
設立年月日	2008-05-13
チームの Email アドレス	csirt-ml@nttdocomo.com
チームサイト	
所属組織サイト	https://www.nttdocomo.co.jp
加盟年月	2015 年 08 月

1. 概要

NTTドコモでは、次の事業を営んでいます。
【通信事業】携帯電話サービス (LTE (Xi) サービス、FOMA サービス)、光ブロードバンドサービス、衛星電話サービス、国際サービス、各サービスの端末機器販売など。
【スマートライフ事業】動画配信・音楽配信・電子書籍サービス等の dマーケットを通じたサービス、金融・決済サービス、ショッピングサービス、生活関連サービスなど。
【その他の事業】ケータイ補償サービス、システムの開発・販売・保守受託など。

2. 設立の経緯・背景

平成 20 年 5 月にドコモ CSIRT 体制マニュアルを制定し、情報セキュリティ部を統括組織としてドコモ CSIRT の運用を開始。サイバー空間における脅威の増大に伴い、平成 24 年 5 月に情報セキュリティ部内にサイバーセキュリティ統括室を設置。現在、サイバーセキュリティ統括室を統括組織とし、ドコモグループ内のシステム部門、クライアントアプリ主管部門の POC (Point of Contact) からなる横断的組織として DOCOMO-CSIRT を形成している。

3. 会社内における位置づけおよび活動内容

自企業及びグループ企業で発生したサイバーセキュリティインシデントの迅速な解決のために、事象発生時のインシデントハンドリングと社内外のコーディネーション、および、日常的なソフトウェア脆弱性情報管理と社内教育、技術的助言、情報提供、等を行っている。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

DT-CIRT

チームの正式名称	デロイト トーマツ コンピュータインシデント対応チーム
チームの略称	DT-CIRT
所属する組織名	デロイト トーマツ リスクサービス株式会社
設立年月日	2013-04-10
チームの Email アドレス	cirt@tohmatsu.co.jp
チームサイト	
所属組織サイト	http://www2.deloitte.com/jp/ja.html
加盟年月	2013 年 07 月

1. 概要

DT-CIRT (Deloitte Tohmatsu Computer Incident Response Team) は有限責任監査法人トーマツ、デロイト トーマツ リスクサービス株式会社の 2 社で構成され、トーマツグループ内の主にコンピュータ・セキュリティ事案に関わるインシデント対応を行う組織内 CSIRT です。

2. 設立の経緯・背景

サイバーセキュリティに対する意識の高まりや、グローバルでのコンピュータ・セキュリティ事案の増加に伴い、所内及びグループ企業内での事案に対して横断的な機能が必要となったため、2013 年 4 月に設立されました。

3. 会社内における位置づけおよび活動内容

当該チームは、所内において主に次の機能を有しており、DT-CIRT 及び弊所 IT セキュリティ室が担当しています。
・コンピュータ・インシデントへの対応
・セキュリティ関連技術動向の把握
・当該チームと関連する組織へのセキュリティ教育・訓練
・日本シーサート協議会をはじめとする外部組織との正式窓口
・外部への情報発信

尚、これらの機能の一部は当該チームと関係する外部組織へ提供される場合もあります。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Entetsu-SIRT

チームの正式名称	Entetsu Security Insident Response Team
チームの略称	Entetsu-SIRT
所属する組織名	遠州鉄道株式会社、遠鉄システムサービス株式会社
設立年月日	2016/9/27
チームの Email アドレス	et-sirt@entetsu.co.jp
チームサイト	
所属組織サイト	http://www.entetsu.co.jp/
加盟年月	2017 年 04 月

1. 概要

Entetsu　Security　Insident Response Team (略称 Entetsu-SIRT)は、静岡県西部地区を中心に事業展開している遠州鉄道株式会社（http://www.entetsu.co.jp）のCSIRTで、遠州鉄道株式会社とその情報子会社である遠鉄システムサービス株式会社により運営しています。

2. 設立の経緯・背景

従来から情報セキュリティインシデント対応や脆弱性情報の収集を遠州鉄道株式会社及び遠鉄システムサービス株式会社のIT関連部門及びリスク管理部門にて対応してきましたが、近年のサイバー攻撃の頻発や国際的に組織化された高度な攻撃や計画的な攻撃の増加への対応や政府機関及びステークホルダーからの情報セキュリティ緊急時対応体制強化の要請といった状況を鑑み2016年9月、CSIRTの設置を図り、重大インシデントの発生から収束までを行う機能・体制を明確化することにより緊急時対応体制を構築しました。

3. 会社内における位置づけおよび活動内容

Entetsu-SIRTは、遠州鉄道株式会社と遠鉄システムサービス株式会社双方のメンバー（ママ）で構成される仮想的な組織体でメンバーは遠州鉄道株式会社内部統制室長の指名によります。
　Entetsu-SIRTは、遠鉄グループ各社内で発生したセキュリティインシデントに対して、直接対応を行う組織内CSIRTとしての役割を担います。

　Entetsu-SIRTの平時及び緊急時の機能は以下の通りです。
A)遠鉄グループ全体の情報セキュリティレベル向上のための施策(教育を含む)の検討・実施。
B)情報セキュリティ事故発生防止のための監視、検知及び警告。
C)セキュリティインシデントに関する情報収集機能
D)セキュリティインシデントに関する対応窓口機能
E)情報セキュリティ事故発生時における情報収集、技術対応及び指示・助言、並びに被害最小化のための施策実施。

　特に情報セキュリティに関わる重大インシデントが発生した場合、CSIRT長たる遠州鉄道株式会社の内部統制室長は遠鉄グループのリスク管理の中心的役割と権限をもってEntetsu-SIRTを指揮し、Entetsu-SIRTはインシデント解決のための可能な限りのあらゆる支援を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ExSIRT

チームの正式名称	Excite Security Incident Response Team
チームの略称	ExSIRT
所属する組織名	エキサイト株式会社
設立年月日	2017年3月13日
チームの Email アドレス	exsirt@excite.jp
チームサイト	
所属組織サイト	http://corp.excite.co.jp/
加盟年月	2017 年 10 月

1. 概要

エキサイト株式会社は、日本におけるインターネットの普及期にポータルサービスを提供する会社としてスタートし、ニュース、検索、メール、ブログなど、ネットユーザーの「便利」を追求してきました。ビジネスユーズからエンタテインメント、生活に密着したサービスまで、総合的なインターネットサービスを展開しております。ExSIRTはエキサイト株式会社により運営されている組織内CSIRTになります。

2. 設立の経緯・背景

高度化するサイバー攻撃、内部犯行等に対して予防的対策をハードウェア、ソフトウェア、ルールにて強化しておりますが、セキュリティインシデントが発生した際、迅速に対応できる体制を強化、社内、社外問わず通報、相談できる一次窓口設置とインシデントをハンドリングするチームの必要性からCSIRT設立に至りました。

3. 会社内における位置づけおよび活動内容

自社のインフラ担当を中心としたエンジニアから選抜した5名兼任チームで構成。
社員と自社サービスのシステム、業務システムを対象としており、下記役割を担っております。

1) インシデント発生時の社内への支援と伝達。
2) インシデント発生前の社内への情報提供、啓蒙、教育支援。
3) セキュリティインシデントの事例や動向、インシデント対応手法や技術に関する情報の提供。

また、社外に対しての連絡窓口として機能させます。

4) インシデントに対しての社外連絡窓口としての受付と関係機関への報告。
5) 経験から得た情報含めて、NCAへの情報の提供。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Fe-CSIRT

チームの正式名称	富士電機CSIRT
チームの略称	Fe-CSIRT
所属する組織名	富士電機株式会社
設立年月日	2017/4/3
チームの Email アドレス	fe-csirt@fujielectric.com
チームサイト	
所属組織サイト	http://www.fujielectric.co.jp/
加盟年月	2017 年 08 月

1. 概要

富士電機株式会社は、重電機メーカーとして、「エネルギー・環境事業で持続可能な社会の実現に貢献」を掲げ、事業を展開しています。Fe-CSIRTは、富士電機株式会社により運営されている組織内のCSIRTです。
参考：http://www.fujielectric.co.jp/about/company/

2. 設立の経緯・背景

当社は、かねてよりリスクマネジメントの一環として、情報セキュリティに取り組んで参りましたが、標的型サイバー攻撃、制御システムやIoTの脆弱性に対する攻撃等、多様化、高度化するセキュリティ脅威への対応力、防衛力の強化を図るため、Fe-CSIRTを設置しました。

3. 会社内における位置づけおよび活動内容

位置付け
Fe-CSIRTは、富士電機の情報システム部門の1組織として、既存の情報セキュリティマネジメント体制において、監視、監査、教育等を主導する事務局と共同して活動するチームです。

活動内容
富士電機グループ内で発生する情報セキュリティインシデントの対応、予防を担います。
1) セキュリティインシデント対応
・セキュリティイベント監視
・ログの取得、保管、分析
・セキュリティインシデントの迅速なハンドリング
・関連部門との連携
・再発防止
2) 脆弱性対応
・脆弱性による影響調査
・資産管理、バックアップの徹底
3) 品質管理
・脆弱性情報、脅威情報および最新技術動向の調査
・教育、訓練

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FEC-CSIRT

チームの正式名称	古河電工CSIRT
チームの略称	FEC-CSIRT
所属する組織名	古河電気工業株式会社
設立年月日	2018/03/08
チームの Email アドレス	fec.csirt@furukawaelectric.com
チームサイト	
所属組織サイト	https://www.furukawa.co.jp/
加盟年月	2018 年 07 月

1. 概要

古河電工CSIRT（FEC-CSIRT）は、古河電気工業株式会社によって運営されている古河電工グループの CSIRT です。

2. 設立の経緯・背景

古河電工グループでは情報セキュリティ基本方針に基づき従来より情報セキュリティ対策を行ってきましたが、
サイバー攻撃の高度化により、グループ会社内のセキュリティインシデントに従来よりも迅速に対応するため、
2018年3月8日に古河電工CSIRTを設立いたしました。

3. 会社内における位置づけおよび活動内容

＜位置づけ＞
FEC-CSIRTは古河電気工業株式会社およびFITEC株式会社で構成されており、古河電工グループのサイバー攻撃に対するインシデント対応を行います。

＜活動内容＞
古河電工グループに対して以下の活動を行います。
・CSIRT運用基準の策定と継続的な改善
・インシデントに備えた緊急連絡体制の整備と訓練
・サイバー攻撃、脆弱性情報、脅威情報の収集と情報共有

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FF-CSIRT

チームの正式名称	富士フイルム CSIRT
チームの略称	FF-CSIRT
所属する組織名	富士フイルム株式会社
設立年月日	2016-04-01
チームの Email アドレス	ff-csirt@fujifilm.com
チームサイト	
所属組織サイト	http://fujifilm.jp/
加盟年月	2016 年 05 月

1. 概要

FF-CSIRT は、富士フイルム株式会社 (http://fujifilm.jp) によって運営され、富士フイルムグループの情報セキュリティインシデントに対応する CSIRT です。

2. 設立の経緯・背景

インターネットの世界的な普及、ICT の社会インフラ化が進んでいる中、特定組織を攻撃する標的型サイバー攻撃が年々巧妙化、多様化し、情報セキュリティ対策が今まで以上に重要になってきています。
このような中、富士フイルムグループ内で発生する情報セキュリティインシデントに対し、社内外の連携や体制を強化し、今まで以上に迅速かつ適切に対応を図るため、FF-CSIRT を設立しました。

3. 会社内における位置づけおよび活動内容

FF-CSIRT は、全社的な組織横断活動として位置づけ、社内関連部門やグループ会社と連携を図りながら、以下のような活動を進めています。

インシデント事前対応
-インシデントレスポンス体制の整備
-インシデント対応プロセス・手順の整備
-脆弱性情報や脅威情報の入手と展開、分析

インシデント事後対応
-対外的セキュリティインシデント対応窓口の設置
-インシデントハンドリング
-インデントレスポンス支援
-再発防止対策検討支援

セキュリティ品質向上
-訓練 (インシデント対応訓練、標的型メール攻撃訓練)
-セキュリティ教育
-インシデント対応事例・ノウハウ蓄積

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FFRI

チームの正式名称	Fourteen Forty Reserch Institute
チームの略称	FFRI
所属する組織名	株式会社FFRI
設立年月日	2014-06-02
チームの Email アドレス	webinquiry@ffri.jp
チームサイト	
所属組織サイト	http://www.ffri.jp/
加盟年月	2014 年 06 月

1. 概要

当社のセキュリティリサーチチームは、多様化・複雑化するセキュリティ脅威に対抗するための、広範な技術力を備えた専門家チームです。脆弱性発見を中心としたセキュリティ解析・開発には多数の実績があり、様々なセキュリティコア技術の研究を行っています。

2. 設立の経緯・背景

当社は日本から世界に向けて IT セキュリティに貢献していくために、研究開発には特に力を入れています。FFRI は、社内の研究・リサーチから得られたナレッジを生かし、他の事業者様との情報共有を通して、コンピュータ社会の健全な運営に寄与するために設立に至りました。

3. 会社内における位置づけおよび活動内容

FFRI は、社内の研究・リサーチから得られたナレッジをベースに、セキュリティ情報の発信、及び対策ソリューションの紹介を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FIP-CSIRT

チームの正式名称	富士通エフ･アイ･ピー　CSIRT
チームの略称	FIP-CSIRT
所属する組織名	富士通エフ･アイ･ピー株式会社
設立年月日	2014年1月6日
チームの Email アドレス	fip-csirt@dl.jp.fujitsu.com
チームサイト	
所属組織サイト	http://www.fujitsu.com/jp/group/fip/
加盟年月	2016 年 08 月

1. 概要

富士通エフ･アイ･ピーは、「アウトソーシング」「クラウド」「ソリューション」の3つのサービスにおいて、システムの企画から設計･開発･運用･保守まで、ライフサイクル全般をLCMサービスでサポートしています。
FIP-CSIRTは、社内およびグループ会社における社内ネットワークで発生したセキュリティインシデントの対応チームです。
社内ネットワークにおけるサイバー攻撃、不審メールの対策や社員へのセキュリティ教育、訓練によるセキュリティ意識の向上により、セキュリティ維持してします。

2. 設立の経緯･背景

当社では2004年に社内セキュリティ統制部署を立ち上げ、ウイルス対策や情報漏えい対策、メール誤送信対策等に取り組んでおります。取り組みを進めていく中、従来のウイルス対策では検知できない不審メールやアドウェアが増加している傾向を脅威と考え、不正通信を監視し可視化することに取り組みました。
この不正通信の監視、可視化を契機とした新たな脅威対策をCSIRT活動と位置づけ、2014年にCSIRTチームを設立しました。

3. 会社内における位置づけおよび活動内容

FIP-CSIRTは、当社内にあるセキュリティ統括部署のメンバーにより構成されています。
社内またはグループ会社で発生したセキュリティインシデントの監視、対応と社内セキュリティ意識の向上を目的とした教育、訓練を実施しています。
＜活動内容＞
社内イントラネットワークのゲートウェイレイヤ、サーバーレイヤ、エンドポイントレイヤに導入した各セキュリティシステムを横断的に管理･監視し、発生したインシデントの調査･解析を行っています。
また、各部署に配置しているセキュリティ担当責任者に対する年2回の会議で社内セキュリティ動向の把握とセキュリティ意識の向上を図っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FJC-CERT

チームの正式名称	富士通クラウドCERT
チームの略称	FJC-CERT
所属する組織名	富士通株式会社
設立年月日	2010-09-01
チームの Email アドレス	contact-fjcc@cs.jp.fujitsu.com
チームサイト	http://jp.fujitsu.com/solutions/cloud/concept/cloud-cert/
所属組織サイト	http://jp.fujitsu.com/
加盟年月	2011 年 01 月

1. 概要

FJC-CERT は、通信システム、情報処理システムおよび電子デバイスの製造 / 販売ならびにこれらに関するサービスを提供している富士通株式会社 (http://jp.fujitsu.com/) の 提供サービスに対する CSIRT です。

2. 設立の経緯・背景

FJC-CERT は、富士通がグローバルに活用可能なパブリック型クラウドサービスを開始することに伴い、クラウドサービスにおけるセキュリティの脅威 (サイバーテロ / 不正利用 / 情報漏洩など) に対して迅速に対応する為に、2010 年 9 月に設立されました。

3. 会社内における位置づけおよび活動内容

FJC-CERT は、その正式名称が「富士通クラウド CERT」であることが示すように、富士通が提供しているクラウドサービスを主な対象にしています。

FJC-CERT の活動は、インシデント発生時の対応は当然のことながら、インシデント発生の未然防止にも注力していることが、最大の特徴です。具体的には、以下のような活動を実施しています。
1.セキュリティ脆弱性情報の収集 / 分析 / 管理
サービス基盤に関する脆弱性情報を常に収集し、インパクト (影響度) の分析を実施しています。また、分析結果を管理し、パッチマネージメントや変更管理に反映しています。
2.セキュリティ脆弱性診断
セキュリティオペレーションセンター (SOC) において、定常的に基盤環境に対し診断を実施しています。また、診断結果を管理し、パッチマネージメントや変更管理に反映しています。
3.モニタリングと検知
全世界 6 ヶ国のサービスに対する不正アクセスの 24 時間モニタリングを、日本において、集中的に実施しています。また、ログ / イベントの相関分析とレポーティングを実施しています。
4.情報セキュリティマネジメント
富士通サービスにおける「人」「モノ」「情報」を適切にマネジメントし、情報セキュリティガバナンスを実践しています。また、グローバルに共通化した情報セキュリティポリシーを適用し、サービスにおける「One Fujitsu」を実現しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FK-SIRT

チームの正式名称	藤田観光SIRT
チームの略称	FK-SIRT
所属する組織名	藤田観光株式会社
設立年月日	2017年10月1日
チームの Email アドレス	fk-sirt@fujita-kanko.co.jp
チームサイト	
所属組織サイト	https://www.fujita-kanko.co.jp/
加盟年月	2017 年 11 月29日

1. 概要

FK-SIRTは、藤田観光株式会社におけるお客様の機密情報ならびに個人情報の漏洩、不正アクセス等、情報システムに関するインシデント発生の防止、被害を最小限にすることを目的としたCSIRTです。

2. 設立の経緯・背景

サイバー攻撃の脅威の動向に合わせて、セキュリティ強化を行ってきましたが、高度化するサイバー攻撃により100%攻撃を防御する事が困難なことから、セキュリティインシデント対応に特化した組織を整備するため2017年10月にCSIRTを構築しました。

また、他社のCSIRT組織と連携を図り、密に情報共有可能な体制を作るとともに、(事前/事後)インシデント対応力強化を目的に日本シーサート協議会へ加盟しました。

3. 会社内における位置づけおよび活動内容

(1)会社内における位置づけ
FK-CSIRT は当社グループ内におけるセキュリティインシデント対応に特化した組織です。
情報システム室要員のみで構成されており、連絡窓口としてセキュリティ担当者を
配置しています。

(2) 活動内容
1. サイバー攻撃・脆弱性情報の収集
2. セキュリティインシデント発生時の対応
3. 従業員のセキュリティ意識の向上、啓蒙、教育

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FortiGuard

チームの正式名称	FortiGuard Labs
チームの略称	FortiGuard
所属する組織名	フォーティネットジャパン株式会社
設立年月日	2004-06-01
チームの Email アドレス	fortiguard_jp@fortinet.com
チームサイト	
所属組織サイト	http://www.fortinet.co.jp
加盟年月	2016 年 05 月

1. 概要

フォーティネット (Fortinet, Inc. NASDAQ：FTNT) は、ネットワークセキュリティ (ファイアウォール、次世代ファイアウォール、UTM) のマーケットリーダーで、ネットワークセキュリティアプライアンスを世界中で提供しています。フォーティネットの製品とサブスクリプションサービスは、標的型攻撃に対して IT セキュリティインフラを簡素化しながら、統合された高いパフォーマンスの保護を幅広く実現します。フォーティネットの顧客には、米フォーチュン誌が選出する 2012 Fortune Global 100 の大部分を含む世界中の大規模企業、サービスプロバイダ、政府機関が名を連ねています。

2. 設立の経緯・背景

フォーティネットでは、世界 6 カ所にセキュリティ研究センターを設置し、日々進化する脅威を世界規模で監視する、FortiGuard Labs を組織しています。世界中で発生するあらゆる脅威に対する情報を一元管理し、セキュリティのエキスパートたちがその対策のための研究と開発に日夜取り組んでいます。24 時間 365 日の運用体制で検知した脅威は、フォーティネットのネットワークを通じて、最新のシグネチャとしてお客様のフォーティネット製品に迅速に配信されます。
2015 年 12 月に FortiGuard Labs をフォーティネットジャパンオフィス内に設置し、日本に特化したセキュリティリサーチと情報発信を推進していきます。

3. 会社内における位置づけおよび活動内容

本チームは CSIRT というより、リサーチラボの意味合いのチームになります。基本的にはお客様環境や日本で広く発生したインシデントに関するリサーチを行い、弊社製品・サービスで対応できる術について、広く情報共有することや、国内情報を FortiGuard Labs の本拠地へフィードバックすることによって、我々の製品・サービスを通じて国内への脅威を軽減する活動を主なミッションとしています。

企業内 CSIRT や関連 CERT、場合によっては他のセキュリティ関連企業様との情報共有を進める事による、共有の課題となるサイバー犯罪者から日本を守るための活動を国内で推進していきます。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

freee-CSIRT

チームの正式名称	freee-CSIRT
チームの略称	freee-CSIRT
所属する組織名	freee株式会社
設立年月日	2015/7/1
チームの Email アドレス	csirt@freee.co.jp
チームサイト	
所属組織サイト	https://freee.co.jp
加盟年月	2017 年 09 月

1. 概要

freee株式会社は、「スモールビジネスに携わるすべての人が創造的な活動にフォーカスできるよう」というミッションのもと、クラウド会計ソフトや、クラウド人事労務ソフトを提供する会社です。
freeeでは、事業のほぼ全てをクラウドに依存する会社であり、またその提供サービスは財務情報や給与情報、個人番号など、非常にセキュリティレベルの高い情報を扱います。
そのため、高度なセキュリティ運用を実現する責務があります。

2. 設立の経緯・背景

当社事業活動全般におけるセキュリティ対策を向上させる専門組織とするべく、2015/7/1 に立ち上げました。立ち上げ後、兼務のメンバー中心に、社内のセキュリティ教育・啓蒙活用や、プロダクトセキュリティやオフィスセキュリティの方針検討、金融機関等の提携企業とのセキュリティ調整を担ってきました。2017/7からは、CISOを設置し、専任かつ経営の立場でセキュリティ施策をになっていくよう体制を強化しています。

3. 会社内における位置づけおよび活動内容

freee-CSIRTは経営直下組織として、以下の活動に従事しています。
- 従業員に対するセキュリティ啓蒙・教育活動
- 当社事業活動全般に関わるセキュリティ対策
- セキュリティインシデント発生時の対応
- セキュリティに関連する外部組織との窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FSAS-CSIRT

チームの正式名称	富士通エフサスCSIRT
チームの略称	FSAS-CSIRT
所属する組織名	株式会社富士通エフサス
設立年月日	2017年4月1日
チームの Email アドレス	fsas-csirt@dl.jp.fujitsu.com
チームサイト	
所属組織サイト	http://www.fujitsu.com/jp/group/fsas/
加盟年月	2017 年 07 月

1. 概要

富士通エフサスは、富士通株式会社の100%出資子会社として、主に ICT インフラの設計・構築・運用、メンテナンスサービス、機器・ソフトウェアの販売などを行っております。現在、「No.1 Service Front Company」を目指し、お客様に最も近いところで、「デジタル革命」の牽引役として、快適で安心して活用出来るICTインフラの構築・運用、サービスの提供に努めています。
FSAS-CSIRT（CSIRT室）は、関係会社9社を含む富士通エフサスグループのサイバーセキュリティ・インシデントに対応するため、専任メンバーで構成されています。

2. 設立の経緯・背景

1998年、富士通エフサスは、ネットワークセキュリティサービスを体系化して提供し、2003年にISMS認証を取得、社内の情報セキュリティの統制を開始しました。その後、2006年にプライバシーマーク、2012年に事業継続マネジメントシステムの国際規格ISO22301の認証を取得しています。
近年、巧妙かつ高度化する標的型サイバー攻撃は未然防止が難しく、またそのセキュリティリスクは未知数で、一度の被害で長時間の業務停止、大量の情報流出、サービス品質低下などの重大な経営リスクが潜んでいます。このようなサイバーセキュリティ・インシデントの早期発見と発生時の初動を組織的に行うべく、2017年4月にFSAS-CSIRTを立ち上げました。

3. 会社内における位置づけおよび活動内容

＜社内における位置づけ＞
FSAS-CSIRTは、専任メンバーと社内システム統制部門の兼任者から構成されており、サイバー攻撃に対するインシデント対応の専門組織として位置づけられています。従来からの情報セキュリティとISMS、ISOなどの統制は、他の専門組織が対応します。

＜活動内容＞
1.CSIRT運用基準の策定と、運用整備と継続的な改善
2.最新の脅威情報のタイムリーな入手によるリスク軽減のための情報発信
3.インシデント発生時の緊急対応
4.組織内リスクとセキュリティ品質の定期的な診断
5.インシデントに備えた訓練の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FSIRT

チームの正式名称	Focus Systems Insident Response Team
チームの略称	FSIRT
所属する組織名	株式会社フォーカスシステムズ
設立年月日	2007-04-01
チームの Email アドレス	irt@focus-s.com
チームサイト	
所属組織サイト	https://www.focus-s.com/
加盟年月	2012 年 05 月

1. 概要

FSIRT は SI ベンダーである株式会社フォーカスシステムズの内部で発足された CSIRT です。

2. 設立の経緯・背景

フォーカスシステムズは、2004 年頃にフォレンジックビジネスを始め、同事業の担当部署である「リスクコンサルティング部」が顧客のインシデントに対応するようになりました。FSIRT はごく稀に社内インシデントの技術的対応を行うこともありますが、社外のインシデント対応がメインです。

数年前は今よりもずっと国内におけるインシデントレスポンスに対する意識が低く、疑問と危機感を感じていました。そして、一般企業に対する CSIRT の普及・啓発活動が必要と思い、その一環として社内にも CERT チームを提案・発足しました。

3. 会社内における位置づけおよび活動内容

＜会社内における位置づけ＞
現時点で FSIRT は「リスクコンサルティング部」が母体です。会社内のインシデント対応の主体は経営システム部（一般的には情報システム部と呼ばれる部署）で、インシデント対応における実質的なマネジメントを行っています。FSIRT は社内インシデントにおける権限はありません。必要に応じて経営システム部からの依頼のもと、技術対応のみを行います。

＜活動内容＞
FSIRT が対応してきたインシデントは、過失による情報流出や背任行為、不正プログラム感染や不正アクセスなどで、特にここ数年は、サイバー攻撃に対するインシデントレスポンスやマルウェアの解析に注力しています。

1.海外や国内からの情報収集
チームの母体となる「リスクコンサルティング部」のビジネスとして、インシデントレスポンス関連製品を取り扱っています。その一環で国内のみならず海外からも様々な情報が得られる環境にいるため、FSIRT としても積極的に情報収集に取り組んでいます。

2.マルウェア分析手法の探求
マルウェア解析はもちろん、その手法についての最新情報を収集しています。

3.セミナーおよびトレーニングの実施
得た情報をセミナーやトレーニングを通して外部にも情報提供しています。

4.インシデントレスポンスのテクニカルサポート
社内・社外問わず、インシデントが起きてしまった組織からの依頼に応じて、一部もしくは全部のサポートを行っています。

上記の活動を通し、事故対応前提社会における情報セキュリティの実現に貢献していきたいと考えています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FRG ISO

チームの正式名称	ファーストリテイリンググループインフォメーションセキュリティオフィス
チームの略称	FRG ISO
所属する組織名	株式会社ファーストリテイリング
設立年月日	2016/04/01
チームの Email アドレス	FRG-ISO@fastretailing.com
チームサイト	
所属組織サイト	http://www.fastretailing.com/jp/
加盟年月	2018 年 07 月

1. 概要

ファーストリテイリングは「服を変え、常識を変え、世界を変えていく」という企業ステートメントに基づき、8つのブランドを世界中で展開する企業です。
デジタル化が進む今、私たちは、従来型のアパレル製造小売業の概念を超え、今までにない新しい産業、“情報製造小売業”に転換し、さらなる事業拡大をめざしています。
FRG ISO（Fast Retailing Group Information Security Office）は、ファーストリテイリング及びその関係会社である各ブランド・各事業国（FRG）における情報管理体制を強化している組織です。

2. 設立の経緯・背景

FRG ISOは、事業のグローバル化やEコマース事業の売上比率向上、世界の国や地域における個人情報保護関連法案の厳格化、高度化・組織化されたサイバー攻撃の高まりを受け、セキュリティへの取り組みの強化とセキュリティインシデントへの迅速な対応を目的に、2016年4月1日に設立されました。

3. 会社内における位置づけおよび活動内容

FRG ISOは、グローバル全体でのセキュリティインシデント発生時の対応やセキュリティインシデントに係る規程の整備に加え、脆弱性情報の収集・対応、従業員教育、各種システムや業務におけるリスク分析・改善等、FRGにおける情報管理体制の強化にかかる業務を専任で行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

FUJITEC-CSIRT

チームの正式名称	FUJITEC Computer Security Incident Response Team
チームの略称	FUJITEC-CSIRT
所属する組織名	フジテック株式会社 情報システム部
設立年月日	2017 年 9 月 15 日
チームの Email アドレス	csirt@fujitec.com
チームサイト	
所属組織サイト	https://www.fujitec.co.jp/
加盟年月	2018 年 04 月

1. 概要

フジテックは、エレベータ・エスカレータ・動く歩道を取り扱う、都市空間移動システムの専業メーカーです。徹底した品質管理のもと、研究・開発から販売、生産、据付、保守、そしてリニューアルまで、一貫体制で“安全・安心”な移動を実現。世界の都市機能の未来を創造します。

FUJITEC-CSIRTは、フジテックの情報セキュリティ対策の検討、立案、実行を担うための組織「情報セキュリティ委員会」を母体に設立しました。本委員会は、情報システム部門のみならず、営業、法務、広報、開発などの各機能組織から横断的にメンバーを選出し構成しております。これにより、FUJITEC-CSIRTは、ITの側面のみならず、顧客対応、コンプライアンス対応、プレス対応などの側面も十分に考慮のうえ、平常時の情報収集・教育活動 及び インシデント発生時の適切な対応を行っていきます。

2. 設立の経緯・背景

前述の「情報セキュリティ委員会」は 2006 年から活動を行っていますが、情報資産の把握、リスク評価、対策の立案・見直しといった、事件・事故を防止するための活動が主でした。
そのような中、当社において 2015 年に社外に影響が及ぶインシデントが初めて発生。またその後他社でも防止の難しいインシデントが多数発生したことから、インシデントの発生を前提として、対応を迅速かつ適切に行うことにより被害を極小化するための仕組み・体制づくりの必要性を痛感いたしました。
これを受け、2016 年より前述の情報セキュリティ委員会メンバーを中心に議論を重ね、2017 年 9 月に FUJITEC-CSIRT の役割を定義した全社規定を発行し、チームの設立に至りました。

3. 会社内における位置づけおよび活動内容

＜平常時の活動＞
(1) 情報セキュリティに関する情報収集
(2) 当社において想定されるインシデントのパターンと初動対応 (連絡先含む) の整理、社内への通知・配信
(3) 情報セキュリティ教育、インシデント発生時を想定した訓練の実施

＜インシデント発生時の活動＞
(1) インシデントの検知と対応要否判断 (影響範囲の早期確認)
(2) インシデント対応
① 初動対応 (被害拡大の防止)
② 対処 (原因の排除)
③ 終息確認
(3) 再発防止
(4) (1) ～ (3) を行う中での社内外関係者との情報連携、コントロール

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

G-CSIRT

チームの正式名称	GLORY-CSIRT
チームの略称	G-CSIRT
所属する組織名	グローリー株式会社
設立年月日	2014-04-22
チームの Email アドレス	G-CSIRT@ml.glory.co.jp
チームサイト	
所属組織サイト	http://www.glory.co.jp/
加盟年月	2014年5月

1. 概要

GLORY-CSIRT は、グローリー株式会社の関連部署で構成する組織横断的な CSIRT です。

2. 設立の経緯・背景

2011 年より情報システム部門・監査部門・法務部門・品質管理部門が連絡会を発足させ、情報セキュリティ向上のため、様々な対策・活動を実施して来ました。しかしながら、昨今の状勢を踏まえて、より迅速・効果的に対応するため GLORY-CSIRT として体制整備を行いました。

3. 会社内における位置づけおよび活動内容

(1)メンバー構成
GLORY-CSIRT は、社内に設置されている情報セキュリティ推進部会の下部組織として位置づけられ、従来の連絡会メンバーに開発部門のメンバーを加えて構成された仮想的なチームです。

(2)活動範囲
① 自社製品対応、および、社内インフラ (業務環境) 対応
② 情報セキュリティ、および、コンピュータウイルス対策

(3)活動内容
情報漏洩やウイルス感染等で全てのステークホルダーにご迷惑をかけない事を第一目標に掲げ、 セキュリティインシデントの未然防止 (情報セキュリティ向上活動の全社展開・規定類の策定・教育等) と発生時の対応を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Fuji Xerox-CERT

チームの正式名称	Fuji Xerox CERT
チームの略称	Fuji Xerox-CERT
所属する組織名	富士ゼロックス株式会社
設立年月日	2013-04-01
チームの Email アドレス	cert@fujixerox.co.jp
チームサイト	
所属組織サイト	http://www.fujixerox.co.jp/
加盟年月	2014 年 02 月

1. 概要

富士ゼロックスは 1962 年の創業以来培ってきた「紙の情報を複写する」というビジネスからの進化を図り、お客様がより効果的、効率的に価値創造するためのコミュニケーションを支援す る企業として、お客様の経営課題の解決に貢献するソリューション & サービスの提供を進めています。

Fuji Xerox CERT は、富士ゼロックスがお客様に提供するソリューション & サービスを実現する商品、および富士ゼロックスが事業継続を図るための IT 基盤に係る情報セキュリティ上のリ スクを最小化するための支援機能を有しています。社内関連部門、関連会社と協力してセキュリティインシデントの予防、検知、事後対応を図ると共に、外部 CSIRT と連携して情報化社会のセキュリティ向上に貢献します。

2. 設立の経緯・背景

当社がお客様の経営課題を解決するために提供しているソリューション&サービスは、国内のみならず、アジアパシフィック圏も含めグローバルに展開しており、これらを安全にお客様に提供するためには、情報ネットワーク上に存在するさまざまなセキュリティ上の脅威への対応が必要となります。
このため、サイバー攻撃等の脅威に対して、効果的に対応を図る専門チームとして Fuji Xerox CERT を設立しました。

3. 会社内における位置づけおよび活動内容

Fuji Xerox CERT は、全社的な組織横断活動として位置づけられ、社内関連部門や関連会社が連携を図りながら、以下のような活動を進めています。

予防
-インシデントレスポンス体制の整備
-脆弱性情報や脅威情報の入手と展開・アラート
-脆弱性検査の支援と検査スキル開発、脆弱性対応の管理
-訓練 (インシデント対応訓練、標的型メール攻撃訓練)

検知
-マルウェア感染、ウィルス感染などの異常検知
-侵入検知
-内部不正検知

事後対応
-対外的セキュリティインシデント対応窓口
-インシデント対応支援 (証拠保全、関係者とのコミュニケーションの支援等)、インシデント対応管理
-対応事例・ノウハウ蓄積と再発防止対策検討支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

GREE-IRT

チームの正式名称	GREE Incident Response Team
チームの略称	GREE-IRT
所属する組織名	グリー株式会社
設立年月日	2012-01-04
チームの Email アドレス	gree-irt@ml.gree.net
チームサイト	
所属組織サイト	http://www.gree.co.jp/
加盟年月	2012年1月

1. 概要

グリー株式会社および関連会社 (以下、「グリーグループ」という) は、「インターネットを通じて、世界をより良くする」をミッションとして、ソーシャルゲーム事業、ソーシャルメディア事業、プラットフォーム事業および広告・アドネットワーク事業等を展開しています。GREE-IRT は、グリーグループの CSIRT です。

2. 設立の経緯・背景

弊社サービスの世界展開が開始され、さらなる脅威への対策として発足致しました。単一部署で構成するのではなく、部署間を横断し、また、社を超えてセキュリティ脅威に対策する組織として位置づけられています。

3. 会社内における位置づけおよび活動内容

＜会社内における位置づけ＞
前述のとおり、単一部署で構成するのではなく、部署間を横断したバーチャル組織として位置づけられています。社内の情報セキュリティ部門や情報システム部門、開発部門、事業部門、法務や広報といったコーポレート機能にまたがった組織になっています。意思決定は担当役員主管の委員会が担っています。
＜活動内容＞
実際のインシデント対応においては、PMO 業務が中心となります。各部門との調整、調査・対応依頼、委員会事務局を担当し、インシデントの収束にあたります。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

GRS-CSIRT

チームの正式名称	グリーンシステム CSIRT
チームの略称	GRS-CSIRT
所属する組織名	グリーンシステム株式会社
設立年月日	2016年11月1日
チームの Email アドレス	grs-csirt@grs.co.jp
チームサイト	
所属組織サイト	http://www.grs.co.jp/
加盟年月	2017 年 11 月29日

1. 概要

グリーンシステム株式会社は1988年から長年、ITシステム開発を行ってまいりました。
GRS-CSIRT は グリーンシステム株式会社のシステム開発部で発足された CSIRT です。

2. 設立の経緯・背景

近年のコンピュータ・セキュリティ事案の増加に伴い、各個人や部署単位でのインシデント対応・啓蒙活動に限界を感じ、社内に CSIRT チームを提案・発足しました。

3. 会社内における位置づけおよび活動内容

＜会社内における位置づけ＞
システム開発部が主体となり、自社内の組織横断が可能なチームを設立

＜活動内容＞
①インシデント発生時のインシデントレスポンス
②セキュリティ最新脅威情報、脆弱性情報の収集、管理
③セキュリティへの意識向上の為、教育・啓蒙活動を実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

GSX-CSIRT

チームの正式名称	GSX-CSIRT
チームの略称	GSX-CSIRT
所属する組織名	グローバルセキュリティエキスパート株式会社
設立年月日	2014-04-01
チームの Email アドレス	gsx-csirt@gsx.co.jp
チームサイト	
所属組織サイト	http://www.gsx.co.jp
加盟年月	2015 年 06 月

1. 概要

当社は、情報セキュリティの確保技術に資するコンサルティング活動を通じ、わが国経済の繁栄と社会生活の安定的発展に寄与します。

今日、ネットワークを利用した電子商取引が急拡大する中で、安全な電子商取引を成立させるための社会基盤の整備が急務とされていますが、私たちは情報セキュリティの問題を人間系、技術系の両面から総合的に捉え、わが国の情報セキュリティ分野における第一人者の地位を築くことを目標とし、日々努力しています。

また職業専門家 (エキスパート) として、常に最新の情報セキュリティ技術の習得に努めつつ、ハイテク犯罪やサイバーテロに対抗しうる社会基盤の構築の実現と、企業の情報管理態勢強化の支援に取り組んでいます。

2. 設立の経緯・背景

2000 年の設立当初から、情報セキュリティポリシーの策定ならびにその定着化支援、システム監査や内部統制支援、さらにタイガーチームサービス (TTS) による質の高い脆弱性診断サービスならびにコンサルティングを提供してきました。

近年では、サイバーセキュリティサービス (CSS) 事業を強化したことにより、標的型攻撃をはじめとするサイバーセキュリティ対策に係わる課題について、ワンストップでソリューションを提供することが可能となりました。

こうしたビジネス上の経験をふまえつつ、最近では組織的なインシデント対応が経営上の重要課題ともなっていることから、当社においては BBS グループ横断のセキュリティインシデントチームとして、2014 年 4 月に情報セキュリティ委員会のメンバーを中心に、GSX-CSIRT を設立した経緯があります。

これにより今後、高度化・巧妙化するサイバー攻撃により発生した事象への対応、ならびにインシデント被害を軽減させるための対応態勢を整備することを、CSIRT チーム活動の中核としてリスクマネジメント体制の強化に努めたいと考えています。

3. 会社内における位置づけおよび活動内容

1.インシデントレスポンス (組織内ならびに関連会社組織において発生した有事対応)
2.脆弱性管理ならびに脆弱性ハンドリング
3.最新脅威情報の収集ならびにマルウェア分析やリスク評価
4.組織内ならびに関連会社組織へのサイバーセキュリティに関する意識向上と教育活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

GMO 3S

チームの正式名称	GMO System Security Support
チームの略称	GMO 3S
所属する組織名	GMO インターネット株式会社
設立年月日	2012-11-01
チームの Email アドレス	gmo-sysesu@gmo.jp
チームサイト	
所属組織サイト	http://www.gmo.jp/
加盟年月	2013 年 08 月

1. 概要

GMO 3Sは、GMOインターネットグループのCSIRTです。

GMOインターネットグループは、WEBインフラ・EC事業、
インターネットメディア事業を展開する「総合インターネットグループ」です。
企業や個人がインターネットの情報発信に必要となるサービスを、
私どもは全て一貫してご提供しております。

2. 設立の経緯・背景

CSIRT機能としましては、2006年頃に始まった、
自社内におけるインシデント管理ツールの運用開始が発端となります。

インシデント発生の都度、サービスに関連する技術者と事業責任者が集まり、
FaceToFaceで今後の対応に関して協議していく体制が確立されたのがこの頃です。

2011年には、緊急時におけるグループ横断の危機管理体制の確立を行いました。
これにより現場のみでなく、経営層までがインシデント発生に対し、
24時間365日のサポートが可能な体制となりました。

その後、2012年に「GMO 3S」として、CSIRT機能を正式にプロジェクト化させました。

この度のNCA加盟を通じて、更なるインターネット業界のセキュリティ強化に
貢献出来ればと思います。

3. 会社内における位置づけおよび活動内容

GMO 3Sは独立した組織というわけではなく、
社内での有志エンジニアを中心に構成されたプロジェクトです。

エンジニアとしての誇りを武器に、お客様の笑顔と感動を追及するべく、
GMOインターネット社における情報セキュリティ対策活動の向上に、
メンバー全員が一丸となり、切磋琢磨しながら取り組んでいます。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Hammock-CSIRT

チームの正式名称	ハンモック CSIRT
チームの略称	Hammock-CSIRT
所属する組織名	株式会社ハンモック
設立年月日	2018 年 1 月 22 日
チームの Email アドレス	Hammock-CSIRT@hammock.co.jp
チームサイト	
所属組織サイト	https://www.hammock.jp/
加盟年月	2018 年 04 月

1. 概要

ハンモック CSIRT は、株式会社ハンモックが運営する CSIRT です。
当社はパッケージソフトウェアの開発販売事業を営んでおり、さまざまなソフトウェアやソリューションの提供を通じて企業の生産性向上に貢献していきたいと考えています。

2. 設立の経緯・背景

当社は各企業のクライアント端末に対するセキュリティ対策・IT 資産管理を統合的に実現する法人向けソフトウェア「Asset View」を提供しております。
2017 年に「AssetView」の脆弱性が発見された際に行った、「セキュリティパッチ提供」「専用 Web ページの開設やメール案内」など、JPCERT/CC が公開する情報セキュリティ早期警戒パートナーシップガイドラインに基づいた対応を通じて昨今の高度なサイバーセキュリティ脅威を再認識し、当社内のセキュリティ対策においてもより迅速に情報把握および対策を実施する組織として CSIRT の体制を整備しました。

3. 会社内における位置づけおよび活動内容

【会社内における位置づけ】
ハンモック CSIRT は、当社情報システム部門および NWS 事業部の技術・営業部門を中心としながらも GLUE 事業部・DCS 事業部も含めた横断型の仮想組織として活動します。
有事の際には、ハンモック CSIRT が主体となり、製品セキュリティ運営委員会 (PSIRT) と連携し、改修要望の取りまとめやパッチ提供を受けた上で、適用作業等、終息に向けた対応を各事業部・部門へ手順の案内を含めて対応します。

【主な活動内容】
当社内システムを対象として以下の活動を実施いたします。
当社セキュリティ対策実現に活用している自社製品「AssetView」に関連する脆弱性・インシデントに関わる事項については、別途組織した製品セキュリティ運営委員会 (PSIRT) への情報連携と共に改修要望を取りまとめるなど連携して行います。

・JPCERT/CC、JVN サイト等を利用したセキュリティ情報の収集と社内システムへの影響分析
・発生インシデント時の製品セキュリティ運営委員会 (PSIRT) への連携と社内システムへの適用
・社内セキュリティレベルの向上を目的とした社員へのセキュリティ教育と啓蒙

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

HASEKO-CSIRT

チームの正式名称	HASEKO GROUP Computer Security Incident Response Team
チームの略称	HASEKO-CSIRT
所属する組織名	株式会社 長谷工コーポレーション
設立年月日	2016/04/01
チームの Email アドレス	haseko-csirt@haseko.co.jp
チームサイト	
所属組織サイト	https://www.haseko.co.jp/hc/
加盟年月	2018 年 07 月

1. 概要

長谷工コーポレーションは「都市と人間の最適な生活環境を創造し、社会に貢献する」を企業理念に、グループ一丸となってマンションに関わる様々な事業を行っております。
HASEKO-CSIRTは長谷工グループを対象範囲として活動するセキュリティインシデントレスポンスチームで、長谷工コーポレーションが運営しています。

2. 設立の経緯・背景

弊社では以前から様々な情報セキュリティ対策に取り組んでおりましたが、高度化するサイバー攻撃や、他社のインシデント事例を受け、情報セキュリティの強化が経営課題であるとの認識のもと、HASEKO-CSIRTを設立しました。
また、さらなる高度化が想定されるサイバー攻撃に対しては、自社単独の対応体制には限界があるという考えに至り、社外との情報共有、連携体制が急務であることから日本シーサート協議会への加盟を申請いたしました。

3. 会社内における位置づけおよび活動内容

(1)位置付け
HASEKO-CSIRTの中心となる長谷工コーポレーション IT推進部は当社グループ全体の情報セキュリティ対策を推進する役目を担っています。

(2)活動内容
HASEKO-CSIRTは主として以下の活動を行っています。
① 事故対応（被害の極小化、対応手順・フローの作成）
② 社内教育、訓練（不審メール訓練、事故発生時の対応訓練、情報発信、規程・ガイドラインの策定）
③ 平時の検知、警戒（セキュリティシステムのログ・アラート分析、脆弱性対応）
④ 窓口の一元化（社内相談窓口、社外連絡窓口）
⑤ 社外連携体制（日本CSIRT協議会、外部セキュリティ会社との情報連携）

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

HBA-CSIRT

チームの正式名称	HBA Computer Security Incident Response Team
チームの略称	HBA-CSIRT
所属する組織名	株式会社HBA
設立年月日	2017 年 4 月 1 日
チームの Email アドレス	hba-csirt@hba.co.jp
チームサイト	
所属組織サイト	https://www.hba.co.jp/
加盟年月	2018 年 06 月

1. 概要

HBA-CSIRT は、株式会社HBA が運営する組織内 CSIRT です。

1964 年創業の弊社は、北海道を基盤として基幹業務のシステムインテグレーション、組込み系やネットワーク分野のソフトウェア開発、データセンターを中心とするクラウドサービスや BPO を提供しています。

2. 設立の経緯・背景

従来よりセキュリティ・インシデント対応は、品質マネジメント体制により対応してきましたが、高度化するサイバー攻撃などの各種脅威に対応するため、専門組織として情報セキュリティ対策室を 2017 年 4 月に創設しました。HBA-CSIRT は情報セキュリティ対策室を母体として設立しました。

3. 会社内における位置づけおよび活動内容

HBA-CSIRT は情報セキュリティ対策室を母体としています。情報セキュリティ対策室は、専任メンバーと各部門のネットワークおよびネットワークセキュリティの管理者からなります。

主な活動内容:
・コンピュータの脆弱性対応に関する情報収集と社内へのセキュリティパッチ適用の指示
・コンピュータウイルス対策の状況把握と最新状態への設定指示
・社外関連機関との連携した脅威状況の収集と社内への情報展開
・社内ネットワーク等で発生したセキュリティインシデントへの対応

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

HIRT

チームの正式名称	Hitachi Incident Response Team
チームの略称	HIRT
所属する組織名	株式会社日立製作所
設立年月日	1998-04-01
チームの Email アドレス	hirt@hitachi.co.jp
チームサイト	http://www.hitachi.co.jp/hirt/
所属組織サイト	http://www.hitachi.co.jp/
加盟年月	2007 年 08 月

1. 概要

HIRT は、日立製作所 (http://www.hitachi.co.jp/) によって運営されている日立グループの CSIRT です。

HIRT では、4 つの IRT という組織編成モデルを採用して運用しています。日立グループの場合には、情報システム関連製品を開発する側面 (製品ベンダ IRT)、その製品を用いたシステムを構築やサービスを提供する側面 (SI ベンダ IRT)、そして、インターネットユーザとして自身の企業情報システムを運用管理していく側面 (社内ユーザ IRT) の 3 つがあります。4 つの IRT では、ここに、IRT 間の調整業務を行なう HIRT / CC (HIRT センタ) を設けることにより、各 IRT の役割を明確にしつつ、IRT 間の連携を図った効率的かつ効果的なセキュリティ対策活動を推進できると考えたモデルです。

また、HIRT という名称は、広義の意味では日立グループ全体で推進するインシデントオペレーション活動を示し、狭義の意味では、HIRT / CC (HIRT センタ) を示しています。

2. 設立の経緯・背景

4 つの IRT が整備されるまでには、4 段階ほどのステップを踏んでいます。各段階においては組織編成を後押しするトリガが存在しています。例えば、第 2 ステップの製品ベンダ IRT 立上げには CERT / CC から報告された SNMP の脆弱性が多くの製品に影響を与えたことが後押しとなっています。また、第 3 ステップの SI ベンダ IRT 立上げについては『情報セキュリティ早期警戒パートナーシップ』の運用開始が挙げられます。HIRT センタは、3 つの IRT の大枠が決まった後に、社内外の調整役を担う組織として構成されたという経緯があります。

1998 年 4 月：日立としての CSIRT 体制を整備するための研究プロジェクトとして活動を開始しました。

第 1 ステップ、社内ユーザ IRT の立上げ (1998 年 ～ 2002 年)：日立版 CSIRT を試行するために、日立グループに横断的なバーチャルチームを編成し、メーリングリストをベースに活動を開始しました。メンバ構成は主に社内セキュリティ有識者及び社内インフラ提供部門を中心に編成しました。

第2ステップ、製品ベンダ IRT の立上げ (2002 年 ～)：製品開発部門を中心に、社内セキュリティ有識者、社内インフラ提供部門、製品開発部門、品質保証部門等と共に、日立版 CSIRT としての本格活動に向け、関連事業所との体制整備を開始しました。

第 3 ステップ、SI ベンダ IRT の立上げ (2004 年 ～)：SI / サービス提供部門と共に SI ベンダ IRT の立上げを開始しました。さらに、インターネットコミュニティとの連携による迅速な脆弱性対策とインシデント対応の実現に向け、HIRT の対外窓口ならびに社内の各 IRT との調整業務を担う HIRT / CC の整備を開始しました。

3. 会社内における位置づけおよび活動内容

HIRT / CC (HIRT センタ) は、情報・通信システム社配下に設置されており、社内外の調整役だけではなく、セキュリティの技術面を牽引する役割を担っています。主な活動は、セキュリティ技術分科会活動の技術支援、IT 統括本部 / 品質保証本部との相互協力による制度面 / 技術面でのセキュリティ対策活動の推進、各事業部 / グループ会社への脆弱性対策とインシデント対応の支援、そして、日立グループの CSIRT 窓口として組織間連携によるセキュリティ対策活動の促進です。

また、HIRT / CC (HIRT センタ) の組織編成上の特徴は、縦軸の組織と横軸のコミュニティが連携するモデルを採用しているところにあります。具体的には、専属者と兼務者から構成されたバーチャルな組織体制をとることで、フラットかつ横断的な対応体制と機能分散による調整機能役を実現しています。このような組織編成の背景には、情報システムの構成品が多岐にわたっているため、セキュリティ問題解決のためには、各部署の責務推進と部署間の協力が必要であるとの考えに基づいています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

HT-CSIRT

チームの正式名称	Hokuriku Telecommunication Network Computer Security Incident Response Team
チームの略称	HT-CSIRT
所属する組織名	北陸通信ネットワーク株式会社
設立年月日	2017年10月10日
チームの Email アドレス	ht-csirt@htnet.co.jp
チームサイト	
所属組織サイト	http://www.htnet.co.jp/index.html
加盟年月	2018 年 03 月

1. 概要

弊社は、1993年の設立以来、北陸全域をカバーする光ファイバーネットワークを基盤に、万全の運用・保守・監視体制のもと、セキュリティが確保された、高品質で信頼性の高い通信サービスの提供に取り組んでおります。
HT-CSIRTは、社内で発生した情報セキュリティインシデントへの対応と、外部との連絡窓口や情報収集役として活動します。

2. 設立の経緯・背景

社外への当社CSIRT窓口を周知し、利害関係者間での信頼性を高め、セキュリティインシデント関連について社外との情報共有の活発化を目的とし、HT-CSIRTを平成29年10月に発足させました。スムーズな情報伝達ラインとセキュリティインシデント情報を収集できる体制を構築し、地域貢献を目指します。

3. 会社内における位置づけおよび活動内容

（Ⅰ）位置づけ
- 自組織外連絡窓口
- 自組織内調整からの情報発信
- 情報収集からの情報分析

（Ⅱ）活動内容
セキュリティインシデント発生前後における、迅速・的確な対処ができる社内セキュリティ体制の強化
社内外連絡窓口、インシデント対応、情報収集のため活動を行う。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

I-SIRT

チームの正式名称	帝国ホテルサート
チームの略称	I-SIRT
所属する組織名	株式会社帝国ホテル
設立年月日	2014-04-14
チームの Email アドレス	i-sirt@imperialhotel.co.jp
チームサイト	
所属組織サイト	http://www.imperialhotel.co.jp/j/
加盟年月	2014 年 05 月

1. 概要

I-SIRT は、株式会社帝国ホテルのお客様の個人情報漏洩やシステムダウン等 IT に関わるセキュリティインシデント発生の防止及び発生時のリスクの極少化を目的とする CSIRT です。

2. 設立の経緯・背景

I-SIRT 設立以前から当社の様々なリスクに対して、組織横断的な委員会により対策・活動を行っておりましたが、サイバー攻撃等のセキュリティインシデントの対応のため新たに組織を整備し、2014 年 4 月に CSIRT を構築しました。
また、昨今高度化・巧妙化しているサイバー攻撃の脅威に備え、他社や外部機関との連携・情報共有を目的として日本シーサート協議会へ加盟いたしました。

3. 会社内における位置づけおよび活動内容

(1) 会社内における位置づけ
・I-SIRT は既存の組織に新たな役割を設けた仮想の横断的組織です。本部は情報システム部の部員で構成されており、連絡窓口として各部署に IT セキュリティ担当者を配置しています。また、総務、広報、人事等の関連各部がその職掌に合わせて I-SIRT に関わる新たな役割を担うこととしております。
(2) 活動内容
1.サイバー攻撃・脆弱性情報の収集・診断
2.セキュリティインシデント発生時の対応
3.セキュリティに関する社内外への報告・相談窓口
4.セキュリティルール・規程の整備
5.従業者への研修・啓蒙

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

IBM-CSIRT

チームの正式名称	IBM Cyber Security Incident Response Team
チームの略称	IBM-CSIRT
所属する組織名	日本アイ･ビー･エム株式会社
設立年月日	2008-06-01
チームの Email アドレス	ersjapan@jp.ibm.com
チームサイト	
所属組織サイト	http://www.ibm.com/jp/
加盟年月	2008 年 06 月

1. 概要

IBM は、世界 170 カ国のお客様に対して ビジネスコンサルティングから、IT システム導入･運用管理、アウトソーシングにわたるあらゆる局面で最先端のテクノロジーやサービス等を提供しております。

IBM CSIRT は、社内でのセキュリティインシデントがお客様へ影響を及ぼすことが無いように CIO によって管理された社内の IT セキュリティおよび Data セキュリティに関するインシデント･ハンドリングのチームです。

本協議会には、IBM CSIRTに加えてIBMの顧客向けインシデント対応サービスである X-Force Incident Response and Intelligence Serviceのメンバーも参画しています。

2. 設立の経緯･背景

IBM ではIT Risk について次のように定義しています。

3. 会社内における位置づけおよび活動内容

Define :法務、人事部門 等によるポリシー、スタンダード、ガイドライン の策定
Manage :IT 部門、各事業部 による 推進と保守
Measure :管理部門、監査部門による 測定と報告また、これらを Improve するための見直しを実施し、Respond として CSIRT による事件･事故対応の実施

これらを踏まえ IBM CSIRT は CIO によって管理され、IBM 社内で発生した IT セキュリティ･インシデントと Data セキュリティ･インシデントに対して対応を行なう組織内 CSIRT としての役割を担っています。具体的には、セキュリティ･インシデント･データの解析 ･収集･分析やインシデント関連情報の周知等を行い、改善活動として社内のセキュリティを強化するための措置を検討し、実装するようにガイドをしています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

iD-SIRT

チームの正式名称	Information Development Security Incident Response Team
チームの略称	iD-SIRT
所属する組織名	株式会社インフォメーション・ディベロプメント
設立年月日	2014-06-01
チームの Email アドレス	id-sirt@idnet.co.jp
チームサイト	https://www.idnet.co.jp/contact/index.html
所属組織サイト	https://www.idnet.co.jp/
加盟年月	2014 年 07 月

1. 概要

iD-SIRT は、株式会社インフォメーション・ディベロプメントが運営する CSIRT です。
　当社グループはコンサルティングからソフトウェア開発、システム運営管理、クラウド・セキュリティ、BPO まで、トータルな IT アウトソーシングサービス「i-Bos24®」を提供しています。

2. 設立の経緯・背景

当社は 2012 年より当社のクラウドサービスである「iD-CLOUD」の提供を開始し、お客様の情報システムを運用しています。
「iD-CLOUD」では、当初から「インシデント対応サービス」を提供しておりましたが、近年の高度化したサイバーセキュリティの脅威に対しタイムリーに対応を行うため、社内のセキュリティの知見を集約する組織として CSIRT の体制を整備しました。

3. 会社内における位置づけおよび活動内容

iD-SIRT は、当社グループ会社のインシデントレスポンスチームとして発足しましたが、現時点で当社のクラウドサービスである「iD-CLOUD」および社内システムへのセキュリティインシデント対応を主な対象としています。

＜主な活動内容＞
・セキュリティ情報の収集 / 提供 / 分析
・発生インシデントの対応 / 支援
・セキュリティ技術者の育成

また、今後は提供範囲の拡大に向け準備を進めております。
＜提供拡大範囲＞
・顧客サイトのシステム
・弊社開発システムのセキュリティ対策
　等

＜活動内容の拡大＞
・セキュリティコンサルティング
・客先システムの発生インシデントに対するオンサイト対応
・国内 / 海外グループ会社との連携
　等

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

IHI-CSIRT

チームの正式名称	IHI-CSIRT
チームの略称	IHI-CSIRT
所属する組織名	株式会社IHI
設立年月日	2012-01-18
チームの Email アドレス	csirt@ihi.co.jp
チームサイト	
所属組織サイト	http://www.ihi.co.jp/
加盟年月	2016 年 04 月

1. 概要

IHI-CSIRT は、株式会社IHI のセキュリティインシデントレスポンスチームです。

2. 設立の経緯・背景

IHI は 2006 年 5 月に社内各部門のセキュリティ担当者で構成された情報セキュリティ部会を設置して以来 CSIRT 機能を含む情報セキュリティに関する幅広い活動を実施してきました。2012 年 1 月には、複雑化かつ高度化するセキュリティ脅威に対応するため、CSIRT として体制を整備しました。
2015 年 12 月、日本シーサート協議会への加盟申請を機に、IHI-CSIRT と称することにしました。

3. 会社内における位置づけおよび活動内容

IHI-CSIRT は、社内各部門のセキュリティ担当者と情報システム子会社である (株)IHIエスキューブの情報セキュリティ担当者から構成され、以下の活動を実施しています。

1)セキュリティインシデントの予防
情報セキュリティに関する社内規定の制定・改訂、情報セキュリティ教育、セキュリティツールの選定と運用、社内監査、セキュリティ関連情報の収集と対応、などのセキュリティインシデントの発生を予防するための諸活動を実施しています。

2)セキュリティインシデントへの対応
セキュリティインシデントの発生時には、インシデント発生部門と共同してインシデント対応を実施します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

IIBC-SIRT

チームの正式名称	IIBC Security Incident Response Team
チームの略称	IIBC-SIRT
所属する組織名	一般財団法人 国際ビジネスコミュニケーション協会
設立年月日	2017年8月10日
チームの Email アドレス	iibc-sirt@iibc-global.org
チームサイト	
所属組織サイト	http://www.iibc-global.org/
加盟年月	2018 年 01 月

1. 概要

一般財団法人　国際ビジネスコミュニケーション協会（以下「IIBC」という。）は、1986年の設立以来、「人と企業の国際化の推進」を基本理念に、約30年にわたり事業を展開してまいりました。その中核であるTOEIC Programは、現在では世界160カ国に広がり、英語能力を測る世界共通のモノサシとして、英語によるコミュニケーションの促進に大きな役割を果たしています。
IIBCは、英語によるコミュニケーション能力の向上とグローバル人材の育成を願い、発足以来のノウハウと経験を生かした多彩な活動を通じて、人と企業の国際化に貢献しています。

2. 設立の経緯・背景

昨今のサイバー攻撃による個人情報漏洩事件を受け、日々のセキュリティ対策を行う部署として、2017年4月に「サイバーセキュリティ対策チーム」を設立し、以下の活動を行っております。
・パブリックモニタリング
・セキュリティ動向分析や技術動向監視
・侵入検知や調査、協会内への注意喚起
・協会職員のセキュリティ耐性向上に向けた教育や啓蒙
ただし、協会が大きな損失を受けるような重大なセキュリティインシデントが発生した際、もしくはその可能性があると判断した場合に、技術的な調査、早期の対処を施すため、「IIBC-SIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

(1) 会社内における位置づけ
「IIBC-SIRT」は、情報システム部門の職員を中心としたメンバーで構成しています。

(2)活動内容
「IIBC-SIRT」は重大なセキュリティインシデントが発生、もしくはその可能性があると判断した場合に発動します。発動後は主に以下の活動を行います。
・インシデント発生時の原因解析、影響範囲調査の実行を担う
・被害拡大防止措置、復旧、事業継続の実行を担う
・JPCERT/CCやIPA、警察等、技術的なやり取りを要する対外組織との連携窓口を担う
・情報セキュリティインシデント事案について危機管理委員会、各部門への報告と支援を行う
・情報セキュリティインシデントに対して、再発防止策の策定および実行を担う

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

IIJ-SECT

チームの正式名称	IIJ group SEcurity Coordination Team
チームの略称	IIJ-SECT
所属する組織名	株式会社 インターネットイニシアティブ
設立年月日	2001-05-16
チームの Email アドレス	sect@iij.ad.jp
チームサイト	
所属組織サイト	https://sect.iij.ad.jp/
加盟年月	2007 年 08 月

1. 概要

IIJ-SECT (IIJ group Security Coordination Team) は、IIJ 及び IIJ グループにおけるインシデントに対応する CSIRT です。

2. 設立の経緯・背景

IIJ は 1992 年にインターネットの商用化を目的として設立された会社です。1994 年からセキュリティ事業を開始しています。IIJ-SECT は、1997 年に開始された IIJ のセキュリティを向上するための社内活動の延長として、特に IIJ の設備や顧客が巻き込まれた事件に対応するための組織として、2001 年に結成されました。

3. 会社内における位置づけおよび活動内容

このチームの構成員はセキュリティ情報統括室を中心として、IIJ 内部の設備運用からインテグレーションまで複数の組織のメンバから構成されています。IIJ の設備で発生した事件の発見、解析、関連各組織との連携を主なミッションとしており、セキュリティ関連情報の収集、分析、展開、インシデントハンドリングなどを通じて、IIJ のもつ基盤のセキュリティ向上を目指すとともに、お客様が安心・安全に利用できるインターネットに向けた活動を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

IL-CSIRT

チームの正式名称	Intelli-CSIRT
チームの略称	IL-CSIRT
所属する組織名	NTTデータ先端技術株式会社
設立年月日	2011-07-01
チームの Email アドレス	csirt@intellilink.co.jp
チームサイト	
所属組織サイト	http://www.intellilink.co.jp/
加盟年月	2013 年 03 月

1. 概要

NTT データ先端技術は、NTT データグループの一員としてオープン系 IT システム基盤の設計・構築サービス、ソリューション、トレーニングおよび情報セキュリティに関する各種サービスを提供しています。
「Intelli-CSIRT」はNTTデータグループにおいて、お客様向けの情報セキュリティサービスを担う、セキュリティ事業部のメンバーで構成されています。

2. 設立の経緯・背景

当初はお客様 (エンドユーザ) 向けインシデント対応サービスを提供するチームとして活動していましたが、外部組織との連携によるタイムリーな対応、CSIRT の構築・運用ノウハウもサービスとして提供するという方針から、CSIRT として組織し、活動することになりました。

「Intelli-CSIRT」の名称は、当社の英文社名が「NTT DATA INTELLILINK CORPORATION」であることと、Intelligent なサービスの提供を目指したいという思いから付けられています。

3. 会社内における位置づけおよび活動内容

(1)メンバー構成
中心となるメンバーは、セキュリティ事業部インシデントレスポンス担当に所属する社員です。
この他に、案件や内容に応じてセキュリティ事業部内のスペシャリストメンバーの支援を受けます。

(2)主なタスク
【お客様向け】
・インシデント対応サービス (初動 / 本格対応) の提供
・フォレンジックサービス、各種調査業務の実施
・CSIRT 構築支援、CSIRT 運用支援などのサービス提供
・セキュリティコンサルティング、セキュリティ設計支援の実施

【社内向け】
情報セキュリティ組織、情報システム部門、NTT-CERT、NTTDATA-CERT と連携して下記を提供します。
・セキュリティ情報の提供
・インシデント対応サービス（初動/本格対応）の提供

(3)対応範囲
・お客様サイトおよび自社内インフラで発生したインシデントに対応します。なお、当社以外の NTT データグループ各社におけるインシデントに対する CSIRT 業務は担当していません。
・お客様サイトでのインシデントについては、初動対応から本格対応 (再発防止策) まで、必要に応じたインシデント対応サービスを提供します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

INES-SIRT

チームの正式名称	INES-SIRT
チームの略称	INES-SIRT
所属する組織名	株式会社アイネス
設立年月日	2017-04-01
チームの Email アドレス	sec-service@ines.co.jp
チームサイト	
所属組織サイト	http://www.ines.co.jp/
加盟年月	2017 年 07 月

1. 概要

株式会社アイネスは、民間企業、団体、官公庁等、幅広いお客様に対して、システム構築、運用・保守、情報セキュリティ対策等のサービスを提供しています。INES-SIRTは、お客様システム及び弊社システムのセキュリティ・インシデントに対応するチームです。

2. 設立の経緯・背景

全ての企業がサイバー攻撃の被害に遭う可能性を有する現状にあって、弊社でもセキュリティ・インシデントに対応する機能を強化する必要性を認識し、2016年度より、外部コンサルタントの活用、大学院への留学生派遣等、CSIRT構築の準備を進めて参りました。その結果、2017年4月に、INES-SIRTを設立致しました。

今後、日本シーサート協議会の各種WGへの参加を通じて、CSIRT間の交流を深め、情報セキュリティに関する情報の交換を行いたいと考えています。

3. 会社内における位置づけおよび活動内容

INES-SIRTは、弊社運用部門のメンバーで構成されており、お客様システム及び弊社システムをサイバー攻撃から守る、又は被害を最小限に防ぐことを活動目的としています。主に以下の3点を主軸に活動を展開しています。
(1) 情報収集/発信
(2) インシデント対応
(3) 啓蒙活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

InfoCICSIRT

チームの正式名称	Infosec Cyber Intelligence Center Security Incident Response Team
チームの略称	InfoCICSIRT
所属する組織名	株式会社 インフォセック
設立年月日	2011-08-15
チームの Email アドレス	infocic_sirt@infosec.co.jp
チームサイト	
所属組織サイト	http://www.infosec.co.jp/
加盟年月	2011 年 09 月

1. 概要

インフォセックは、2001 年に情報セキュリティに関するトータル・ソリューションを提供する企業として設立。
　情報セキュリティをコアとし、IT システムセキュリティ、内部統制など企業が抱える課題に最適なサービスをご提供しております。

2. 設立の経緯・背景

2011 年 8 月に設立となりましたが、2010 年より InfoCIC の名にて監視センターを立ち上げました。
　この際に WEB から感染するマルウェアの対応やその他インシデントの対応が数多くあり CSIRT の必要性を感じ InfoCICSIRT (Infosec Cyber Intelligence Center Security Incident Response Team) を設立しました。

3. 会社内における位置づけおよび活動内容

InfoCICSIRT は、24 時間 365 日の監視センター内で通常分析等を行っているメンバーにて構成されております。
　社内でのインシデント、及び監視のお客様にてインシデント発生の際に対応しております。
　従いまして、監視センター責任者の管轄のもと、意思決定を行い活動しております。

　主な活動内容は、以下です。
・モニタリング
 監視している各セキュリティデバイスから送信されるログ分析
・情報収集
 セキュリティの情報収集・情報の発信
・改善活動
インシデントが発生した後のフローや監視、ルールの見直しなど

また、モニタリングからマルウェアの発見やインシデントが発生することもあるため、基本にモニタリングに関連してインシデントレスポンスも実施しております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

INTEC-SIRT

チームの正式名称	INTEC Security Incident Response Team
チームの略称	INTEC-SIRT
所属する組織名	株式会社インテック
設立年月日	2014-04-01
チームの Email アドレス	jyosec_csirt@intec.co.jp
チームサイト	
所属組織サイト	http://www.intec.co.jp
加盟年月	2014 年 07 月

1. 概要

INTEC-SIRT は、株式会社インテックのセキュリティインシデントレスポンスチームです。
　　インテックは ICT 関連の研究・開発からネットワークサービス、アウトソーシングまでの一貫した「ビジネス領域」をトータルソリューションとして提供し、企業や産業そして社会における新しい価値を創造する「社会システム企業」を目指しています。

2. 設立の経緯・背景

2012 年から社内システムにおいて、サイバー攻撃や脆弱性情報の収集 / 社内通知、社内ネットワーク上の不正パケットの調査、インシデント発生サーバ・PC のフォレンジック調査を行ってまいりましたが、最近の増加するサイバー攻撃に対して、より迅速・効果的に対応するため 2014 年に社内組織として INTEC-SIRT の体制整備を行いました。

3. 会社内における位置づけおよび活動内容

【会社内における位置づけ】
　INTEC-SIRT は、インテックの情報セキュリティ推進室に所属するメンバーを中心に構成された組織内インシデントレスポンスチームです。

【活動内容】
　社内システムおよびお客様向けのサービスやシステムに対して、セキュリティインシデント発生の予防、検知、早期解決、被害の最小化を主たる目的として活動を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Imperva JP-CSIRT

チームの正式名称	Imperva Japan CSIRT
チームの略称	Imperva JP-CSIRT
所属する組織名	株式会社Imperva Japan
設立年月日	2016年1月1日
チームの Email アドレス	Imperva-Japan-CSIRT@Imperva.com
チームサイト	
所属組織サイト	http://www.imperva.jp/Company/Contact
加盟年月	2017 年 05 月

1. 概要

Imperva は、業務上不可欠なデータやアプリケーションをクラウドかつオンプレで保護する、サイバー・セキュリティ・ソリューションの大手プロバイダです。当社は2002 年の創業以来、2015年には2億3,300万ドル、4,800以上の顧客、世界100カ国に500以上のパートナーを数えるようになり、着実に成長を続けています。

2. 設立の経緯・背景

2007年日本法人設立。
2016年重要なデータと中心としたセキュリティの脅威から顧客を守るため、Imperva Japan CSIRTを設立。

3. 会社内における位置づけおよび活動内容

本チームは CSIRT というより、お客様環境や日本で広く発生したインシデントに関するリサーチを行い、本社技術チーム・サポートチームとのプロアクティブな最新情報交換・収集し、弊社製品・サービスで対応できる術について、広く情報共有することや、緊急のインシデントに対し、日本に於ける連絡体制・緊急対応体制を整え、我々の製品・サービスを通じて国内への脅威を軽減する活動を主なミッションとしています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ISID-CSIRT

チームの正式名称	ISID Computer Security Incident Response Team
チームの略称	ISID-CSIRT
所属する組織名	株式会社　電通国際情報サービス
設立年月日	2017年1月18日
チームの Email アドレス	g-csirt@group.isid.co.jp
チームサイト	
所属組織サイト	http://www.isid.co.jp
加盟年月	2017 年 02 月

1. 概要

ISID-CSIRT（ISID Computer Security Incident Response Team）は株式会社電通国際情報サービス（ISID）の統合リスク管理委員会の下部組織である情報セキュリティ分科会事務局が中心となって構成され、ISID本社および国内・海外グループ会社におけるサイバー・インシデント対応を行う組織内CSIRTです。

2. 設立の経緯・背景

ISIDでは次世代ファイヤーウォールによる入口・出口対策、およびPCに導入しているウイルス対策ソフト等によりシステム面での多層防衛を実施しています。
しかし、近年急増している標的型攻撃では、システム面だけの対策では十分ではなく、利用者の不注意によりマルウエアに感染し、重要情報が漏えいする事象の報道がされています。
このような事象やシステムへのサイバー攻撃対策として、日本シーサート協議会へ加入することにより他社と情報共有を行い、サイバー攻撃へ迅速・効率的に対応するため、CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

【会社内における位置づけ】
ISID-CSIRTはISIDの情報セキュリティ分科会の事務局を中心に構成されるバーチャルな組織になります。

【活動内容・役割】
サイバーセキュリティに対する活動内容は、
・サイバー・インシデント発生時のインシデント対応および情報管理
・関係機関からサイバー・インシデント情報・脆弱性情報の収集および予防措置の実施
・他社とのサイバーセキュリティ情報共有
・社内へのサイバーセキュリティ情報の周知および教育

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ITS-TEA.SIRT

チームの正式名称	ITS-TEAセキュリティ対策チーム
チームの略称	ITS-TEA.SIRT
所属する組織名	一般財団法人　ITSサービス高度化機構
設立年月日	2013年2月19日
チームの Email アドレス	its-tea.sirt@its-tea.or.jp
チームサイト	
所属組織サイト	http://www.its-tea.or.jp
加盟年月	2017 年 08 月

1. 概要

一般財団法人　ITSサービス高度化機構（以下「ITS-TEA」という。）は、有料道路自動料金収受システム（ETC）に関するセキュリティを確保するための機能・役割を担う業務行っています。具体的には、ETCカードや車載器の識別処理情報の発行、車載器のセットアップに関するシステムの開発運営を行っています。

2. 設立の経緯・背景

ETCのセキュリティを確保する業務に関する主幹システムや、目的別にホームページを複数運営していることから職員のセキュリティインシデントに関して高い意識を持つ必要があります。
そのため、機構内の体制整備、セキュリティ対策の強化・推進するため設立しました。

3. 会社内における位置づけおよび活動内容

（1）位置付け
ITS-TEA.SIRTは、システム部職員が中心となり、その他部の選抜されたメンバーで構成しています。

（2）活動内容
ITS-TEA.SIRTでは、以下の活動を通してセキュリティ対策を行っています。
・ITS-TEAの情報資産を守るため必要な対策を講じることを支援する
・ITS-TEA全体の情報資産を横断的に取扱う
・各部が管理している情報資産のセキュリティ対策について助言する
・職員のセキュリティ対策意識向上のための企画・立案を支援する
・各部が管理している情報資産でセキュリティ上の課題が発生した場合は、速やかに統括者に連絡し、対策チーム全体で対応方法を検討し対処を支援する

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JACCS-CSIRT

チームの正式名称	JACCS-Computer Security Incident Response Team
チームの略称	JACCS-CSIRT
所属する組織名	株式会社ジャックス
設立年月日	2015-06-16
チームの Email アドレス	jaccs-csirt@jaccscard.co.jp
チームサイト	
所属組織サイト	http://www.jaccs.co.jp/
加盟年月	2016 年 05 月

1. 概要

株式会社ジャックスは、「日本を代表する先進的なコンシューマーファイナンスカンパニー」をビジョンに掲げ、「夢のある社会」「豊かな社会」の実現に貢献してまいります。

2. 設立の経緯・背景

サイバー攻撃の脅威から大切なお客様情報を防御するためには、いち早く情報を入手し対策を講じる必要があることから、JACCS-CSIRT を設立しました。

3. 会社内における位置づけおよび活動内容

【位置づけ】
JACCS-CSIRT は、システム部門を中心としたメンバーで構成され、サイバーセキュリティに関する実務的対応を行います。
【活動内容】
〇サイバー攻撃に対する対策の実施および防御に関する検討
〇外部 (日本シーサート協議会含む) からの情報収集・分析
〇社内各部門との連携
〇緊急時対応

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JASDEC-CSIRT

チームの正式名称	JASDEC-CSIRT
チームの略称	JASDEC-CSIRT
所属する組織名	株式会社証券保管振替機構
設立年月日	2016年8月1日
チームの Email アドレス	jasdec_csirt@jasdec.com
チームサイト	
所属組織サイト	http://www.jasdec.com/
加盟年月	2016 年 08 月

1. 概要

JASDEC−CSIRTは、株式会社証券保管振替機構の組織内CSIRTです。
弊社は、資本市場の重要な基盤である証券決済インフラとして、その公共的な役割を認識し、信頼性、利便性及び効率性の高いサービスを提供しています。

2. 設立の経緯・背景

高度化、巧妙化するサイバー攻撃によるコンピュータセキュリティインシデントへの対応を強化するため、組織内CSIRTとして、JASDEC−CSIRTを2016年8月に設立しました。

3. 会社内における位置づけおよび活動内容

■位置づけ
JASDEC−CSIRTは、リスク管理部門及びシステム部門を中心に、組織横断的に組成された仮想的なチームです。
■活動内容
(1)予防活動
・セキュリティ関連情報、技術動向情報の収集、提供
・インシデント対応訓練
・サイバーセキュリティ相談
・サイバーセキュリティに関する啓発活動
(2)インシデント対応支援活動
・インシデント報告窓口
・インシデント対応支援
(3)外部団体との連携
・他社CSIRTとの情報連携
・日本シーサート協議会との情報連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JBS-CIRT

チームの正式名称	JBS Cyber Incident Response Team
チームの略称	JBS-CIRT
所属する組織名	日本ビジネスシステムズ株式会社 SI統括本部IS本部　セキュアデザインセンター
設立年月日	2015-10-16
チームの Email アドレス	CIRT@jbs.com
チームサイト	
所属組織サイト	https://www.jbs.co.jp/
加盟年月	2016 年 02 月

1. 概要

「セキュリティエンジニア」の活躍の場として
日本ビジネスシステムズ株式会社 (JBS) は、「すべてのリソースはお客様の満足のために」の立場で、マイクロソフト社のプラットフォームをメインとした IT・クラウドソリューションを主な事業とし、シスコシステムズ社のネットワーク製品や EMC 社のストレージ製品など、今日の仮想化・クラウド基盤システム導入や環境構築にも貢献しています。
「インシデントレスポンス」の牽引役として
当社における、システムエンジニア (SE 職) においては、情報セキュリティの知識や技術スキルの向上が欠かせなくなっており、より高度な「セキュリティエンジニア」に必要な専門技術が求められています。そうした背景から、当社のインシデントレスポンスチームのメンバーとして知見を深め、かつ常に最新のサイバーセキュリティ技術の習得に努めつつ、サイバーテロ犯罪に対抗しうるインシデント体制の実現と、組織全体の有事対応の支援強化といった、経営上の課題にも取り組んでまいります。

2. 設立の経緯・背景

近年多発する組織内におけるインシデント対応が、経営上の『重要課題』であることを受け、2015 年 10 月に、JBS-CIRT (JBS Cyber Incident Response Team) として、セキュリティインシデント対応としての中心として、セキュアデザインセンター (SDC) に所属する有志メンバーを中心に、設立致しました。現在メンバー数は、常勤と非常勤を合わせ 6 名 (2016 年 2 月現在) が在籍しています。

3. 会社内における位置づけおよび活動内容

1.事後対応サービス
① 注意喚起と警告・通知
問題解決のために短期間で対応可能なインシデント対応処理の実施
② インシデントハンドリング
インシデントを検証・診断・重大度評価の検討
③ インシデントレスポンス
電話・E メールなどを通じ、有事後の影響ある部署に対する復旧サポート支援やアドバイスの実施
④ インシデントコーディネーション発生した一次原因の特定
関係する他 CSIRT 組織との情報交換ならび関係機関への報告・調整
2.事前対応サービス
① アナウンスメント
侵入検知や攻撃発生時における警告・注意喚起
② 技術監視 (モニタリング)
ネットワーク通信、不正侵入行為、関連する全ての挙動の監視の実施
③ インシデントレスポンス
電話・E メールなどを通じ、有事後の影響ある部署に対する復旧サポート支援やアドバイスの実施
④ 脆弱性管理
セキュリティ監査のための脆弱性調査と調査結果を元に、脆弱性を低減するための対策・検討
3.インシデント管理サービス
① リスクマネジメント
CSIRT 体制の成熟度を向上させるために KGI (目標達成指標) と KPI (業績評価指標) 設定
② 商用セキュリティ製品の性能評価と検証
商用ツール、アプリケーション、その他のサービスにおける製品評価や検証の実施
③ サイバーセキュリティ意識向上

最新のサイバー攻撃情報を提供するセミナーや社内外の勉強会を開催
昨年実績：サイバーセキュリティ最前線 (三菱総合研究所：MRI との共催セミナー)
～2015 年 CSIRT 元年のふり返りと今後の課題～
https://www.jbs.co.jp/event/list/2015/1209
④ サイバーセキュリティトレーニング開発
サービス対象に対して、サイバーセキュリティトレーニングの検討・実施
サイバーセキュリティアナリスト教育プログラムの研究開発

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JCB-CSIRT

チームの正式名称	JCB Computer Security Incident Response Team
チームの略称	JCB-CSIRT
所属する組織名	株式会社ジェーシービー
設立年月日	2014-05-01
チームの Email アドレス	csirt@info.jcb.co.jp
チームサイト	
所属組織サイト	http://www.jcb.co.jp/
加盟年月	2015 年 02 月

1. 概要

株式会社ジェーシービーは、国際ブランドを運営するクレジットカード会社として、世界を舞台にカード事業・加盟店事業・プロセシング事業・ブランド事業を柱とする多様な事業を展開しています。

2. 設立の経緯・背景

2014 年上期に発生した複数の深刻かつ影響範囲の大きいソフトウェア脆弱性を皮切りに、脆弱性やサイバー攻撃といったインシデントが発生した際に、迅速かつ適切に対処する必要性を強く認識し、インシデント発生後の対応策に関する検討 WG を立上げました。そして、2014 年 5 月に当社管理の Web サイトにおける脆弱性・サイバー攻撃に対し専門的に対応していくための組織として CSIRT を立ち上げました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
システムリスクを所管するシステム企画部メンバーと情報セキュリティを所管するコンプライアンス部メンバーにより構成し、社内外の情報共有・インシデント対応を担当します。

(2)活動内容
・外部専門組織との連携によるサイバー攻撃に関する早期の情報入手
・当該情報の社内展開
・事象発生時の事象管理
・事象発生の抑制
・発生時の被害拡散防止

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JFE-SIRT

チームの正式名称	JFE Security Integration and Response Team
チームの略称	JFE-SIRT
所属する組織名	JFEホールディングス株式会社
設立年月日	2015-06-22
チームの Email アドレス	jfe-sirt@jfe-gr.net
チームサイト	
所属組織サイト	http://www.jfe-holdings.co.jp/
加盟年月	2016 年 01 月

1. 概要

JFE-SIRT は JFE スチールを中心に構成される JFE グループの CSIRT です。

2. 設立の経緯・背景

留まること無く高度化していくサイバー攻撃に対して、企業内対応力強化、有事対応の迅速化と適切な社外との連携を実施するために 2015 年 6 月に JFE グループ共通の CSIRT を立ち上げました。

3. 会社内における位置づけおよび活動内容

JFE-SIRT は JFE ホールディングス以下主要グループ会社の情報システム部門によって構成される仮想チームです。平時は JFE グループ全体の情報セキュリティ対策と IT リスク管理体制の強化を継続推進しながら、インシデント発生時はリスク管理部門、情報子会社と協力して早期対応します。

具体的な活動内容
1)セキュリティ情報収集
2)インシデントレスポンス
3)自社およびグループ企業の情報セキュリティ対策・啓蒙
4)情報セキュリティに関する規程の整備・見直し
5)自社およびグループ企業のセキュリティ相談窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

J-POWER CSIRT

チームの正式名称	電源開発㈱サイバーセキュリティ推進・対応チーム
チームの略称	J-POWER CSIRT
所属する組織名	電源開発株式会社
設立年月日	2016年8月9日
チームの Email アドレス	jpower-csirt@jpower.co.jp
チームサイト	
所属組織サイト	http://www.jpower.co.jp
加盟年月	2016 年 12 月

1. 概要

電源開発㈱サイバーセキュリティ推進・対応チーム（J-POWER CSIRT）はJ-POWER（電源開発）グループにおける予防保全を含む制御システムと情報システムにおけるサイバーセキュリティインシデントへの適切・迅速な対処，及びセキュリティ事故のリスク極小化を目的に活動している。

2. 設立の経緯・背景

昨今のサイバー攻撃の高度化・巧妙化を鑑みて，サイバーセキュリティリスクの抑制を目的とした対策の強化（予防保全活動・品質改善活動）の実施，並びにサイバーセキュリティ事故発生時の影響極小化を目的に業務部門と技術部門で構成される部門横断型の対応チームとして設立しました。

3. 会社内における位置づけおよび活動内容

電源開発㈱サイバーセキュリティ推進・対応チーム（J-POWER CSIRT）は，J-POWER（電源開発）グループの制御システムと情報システムのサイバーセキュリティ統括管理の推進・対応チームとして部門横断的に下記の各種活動を主体に実施しています。

① サイバー攻撃に係る情報共有：事故事例の分析と部門横断的な情報共有
② サイバーセキュリティ対策に係る情報共有
③ サイバーセキュリティ対策に係る設計支援
④ 教育（監査教育含む）・訓練 等

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JFRIC-CSIRT

チームの正式名称	JFR情報センターシーサート
チームの略称	JFRIC-CSIRT
所属する組織名	株式会社JFR情報センター
設立年月日	2017/3/1
チームの Email アドレス	jfric-csirt@dic.daimaru.co.jp
チームサイト	
所属組織サイト	http://www.jfr-ic.jp/
加盟年月	2017 年 04 月

1. 概要

JFRIC-CSIRTは株式会社JFR情報センターの組織内CSIRTです。

JFR情報センターは大丸松坂屋百貨店を中心とするJ.フロントリテイリンググループの情報システムを担うシステム開発運営会社として設立されました。グループ内システムの企画開発・運用、システムインフラ構築、ヘルプデスク対応などを担っています。

2. 設立の経緯・背景

JFRグループには小売業以外にも割賦・信用事業、商社、建築業など様々な業態の関係会社が存在します。

昨今の社会的セキュリティ事件を受けて、2014年より社内で各部門長が参加する情報セキュリティ委員会を設立し、社内のセキュリティ対策やグループ各社へのセキュリティ啓発活動を行ってきました。高度化するサイバー攻撃に対して多様な業態が存在するグループ全体の被害を最小限に抑えるためには他社及び外部機関との連携を行い、最新の情報を収集する必要があるため、2017年3月にJFRIC-CSIRTとして発足することと致しました。

3. 会社内における位置づけおよび活動内容

＜会社内における位置づけ＞
JFRIC-CSIRTは取締役を含む各部門長をメンバーとした部門横断的な仮想組織です。

＜活動内容＞
社内のインシデント対応、対策強化、啓蒙活動に加え、グループ会社に対してグループ共通インフラに関するセキュリティ対応、セキュリティインシデントフォロー、セキュリティ提案を実施しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JINSIRT

チームの正式名称	ジンズ　セキュリティ　インシデント　レスポンス　チーム
チームの略称	JINSIRT
所属する組織名	株式会社ジンズ
設立年月日	2017 年 12 月 19 日
チームの Email アドレス	jinsirt@jins.com
チームサイト	
所属組織サイト	https://corp.jins.com/jp/ja/
加盟年月	2018 年 05 月

1. 概要

JINSIRT は株式会社ジンズとその子会社が提供するサービスおよび各店舗におけるセキュリティインシデントへの対応を行う機能です。

2. 設立の経緯・背景

サイバー攻撃の高度化・巧妙化に対するセキュリティ対策強化が急務となっています。
その中でインシデント対応能力を向上すべくシーサート機能の充実を図るため IT ガバナンス室のメンバーが中心となり JINSIRT を立ち上げることを宣言し、経営会議で承認され設立に至ったチームです。

3. 会社内における位置づけおよび活動内容

(1) 位置づけ
JISIRT はメインメンバーとサブメンバーの 2 部制で構成されています。
メインメンバーは経営直轄の組織である IT ガバナンス室のメンバーとし、外部専門機関等との連携含めセキュリティインシデント対応の舵取りを行います。
サブメンバーとして事業部門、情報システム部門、法務、カスタマーサポート、広報、総務等の各部署があり、メインメンバーは適宜必要に応じてサブメンバーと連携を行います。

(2) 活動内容
・セキュリティインシデント発生時の対応、被害規模・被害内容把握、関連部署連携
・セキュリティインシデントからの復旧および復旧支援
・セキュリティインシデントの原因究明、再発防止策の立案・実施
・セキュリティインシデントに至る可能性のある事案の受付・分析
・アイウェア業界およびその他産業におけるインシデント情報の収集・分析

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JNB-CSIRT

チームの正式名称	ジャパンネット銀行CSIRT
チームの略称	JNB-CSIRT
所属する組織名	株式会社ジャパンネット銀行
設立年月日	2013-09-18
チームの Email アドレス	jnb-csirt@japannetbank.co.jp
チームサイト	
所属組織サイト	http://www.japannetbank.co.jp/
加盟年月	2013 年 09 月

1. 概要

JNB-CSIRT はジャパンネット銀行のインターネットバンキングサービスおよび社内システム全般におけるセキュリティ・インシデント (セキュリティに関する事故や攻撃) に対応するチームです。

2. 設立の経緯・背景

インターネットにおける脅威がますます高度化、複雑化してきたことを背景に、2013 年 9 月、セキュリティ・インシデント専門チームとして JNB-CSIRT を設立しました。
これまで社内で取り組んできたサイバー攻撃や脆弱性情報の調査、セキュリティ・インシデントに対する手続きの整備などを継承するとともに、更なる体制強化を目指し、社内横断的なメンバーで構成致しました。

3. 会社内における位置づけおよび活動内容

(1)位置付け
ジャパンネット銀行の経営陣で構成するリスク管理委員会の下部に、セキュリティやシステムを担当する各部のメンバーにより構成するバーチャルな組織として設置しました。
(2)活動内容
情報収集、被害の未然防止、拡大防止、早期復旧に向けた取り組みを行っております。
・サイバー攻撃発生時のインシデントハンドリング
・セキュリティ強化策の対応推進
・新しい攻撃・防御手法や脆弱性情報の収集
・外部機関との連絡窓口 (フィッシングサイト閉鎖依頼、発生事象報告・共有)

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JOHOKU-CSIRT

チームの正式名称	城北CSIRT
チームの略称	JOHOKU-CSIRT
所属する組織名	城北信用金庫
設立年月日	2015-11-01
チームの Email アドレス	csirt@johokubank.co.jp
チームサイト	
所属組織サイト	http://www.shinkin.co.jp/johoku/
加盟年月	2016 年 03 月

1. 概要

JOHOKU-CSIRT は、城北信用金庫におけるコンピュータ・セキュリティ・インシデントの検知、解決、被害軽減、局限化および発生の予防に関する活動を行い、組織全体としての情報セキュリティの向上を図ります。

2. 設立の経緯・背景

城北信用金庫では、2004 年 9 月より情報システム部門内の会議体である「セキュリティ定例会」を開催し、コンピュータセキュリティに関する課題の解決を中心に活動しておりました。
一方で、近年の高度化・巧妙化を続ける情報セキュリティ侵害の脅威に対しては、より一層継続的・組織的な対応が必要であること、外部組織との連携が重要であるとの認識を強めておりました。
そこで、部門の枠を超えた組織横断的な活動を行うこと、また対外窓口としての機能をもって外部組織との連携を強化することを目的として、前記会議体を発展させた仮想的な組織として JOHOKU-CSIRT を設立しました。

3. 会社内における位置づけおよび活動内容

JOHOKU-CSIRT は仮想的な組織であり、システム部員を中心に複数部署の人員で構成しています。
なお、主な活動は以下の通りです。
1)組織内におけるインシデント発生抑止と被害局限化 (システム対応・啓蒙等)
2)組織内外におけるインシデント情報の収集と分析
3)外部機関との連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JPCERT/CC

チームの正式名称	JPCERT Coordination Center
チームの略称	JPCERT/CC
所属する組織名	一般社団法人JPCERTコーディネーションセンター
設立年月日	1996-10-01
チームの Email アドレス	ww-info@jpcert.or.jp
チームサイト	
所属組織サイト	https://www.jpcert.or.jp/
加盟年月	2007 年 08 月

1. 概要

JPCERT コーディネーションセンターは、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントに関する報告の受け付け、対応の支援、発生状況の 把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっています。

2. 設立の経緯・背景

JPCERT コーディネーションセンターの活動は、1992 年ころに始まった、ボランティアによるインシデントの報告対応業務まで遡ります。当時、日本国内でいくつかのネットワーク組織が活動を始めており、その運用を支援するためにネットワーク技術者たちがボランティアとして活動していたものです。また、米国ではすでに CERT / CC が活動しており、日本国内における CERT / CC のカウンターパートとなる機能が必要であるという認識もありました。

1996 年 10 月に JIPDEC (日本情報処理開発協会、現在は日本情報経済社会推進協会に改称) の一部署として定常業務を開始し、2003 年には有限責任中間法人として独立、現在は一般社団法人として活動しています。

この間、日本国内のシーサートとの連携や新たなシーサートの構築支援を行いつつ、FIRST 加盟、APCERT 設立、アフリカ諸国向けのシーサートトレーニングなど、海外の諸組織との連携強化にも努めています。

3. 会社内における位置づけおよび活動内容

JPCERT / CC は、どこかの会社の組織内シーサートというわけではなく、それ自体が独立した組織です。特定の政府機関や企業からは独立した中立の非営利組織として、国内外のシーサート組織と連携しつつ、日本における情報セキュリティ対策活動の向上に取り組んでいます。

具体的な活動内容としては、
- インシデント報告対応
- インターネット定点観測システムの運用
- 脆弱性関連情報流通
- アーティファクト分析

などがあり、これらの活動に基づいて、一般への情報提供や特定事業者向けの早期警戒情報の提供などを行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JPBank CSIRT

チームの正式名称	ゆうちょCSIRT
チームの略称	JPBank CSIRT
所属する組織名	株式会社　ゆうちょ銀行
設立年月日	2014-03-10
チームの Email アドレス	CSIRT.ii@jp-bank.jp
チームサイト	
所属組織サイト	http://www.nca.gr.jp/member/jpbankcsirt.html
加盟年月	2014 年 06 月

1. 概要

ゆうちょ CSIRT は、ゆうちょ銀行のシステムに対する、セキュリティ・インシデント発生の防止及び発生時のリスクの極少化を目的とする組織です。

2. 設立の経緯・背景

近年、金融機関をターゲットとした DoS 攻撃等のサイバー攻撃やお客さまの PC をウイルスに感染させ不正送金を行う等の事象が増加傾向にあり、当行においても上記セキュリティ・インシデント発生の防止及び発生時対応をすみやかに行うために設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置付け
ゆうちょ銀行システム部門内の IT セキュリティを担当するグループによって組織されています。
(2)活動内容
ゆうちょ CSIRT は以下の活動を実施しています。
・サイバー攻撃対策の調査・立案
・セキュリティ・インシデント発生時の対応支援
・脆弱性情報の収集
・サイバー攻撃情報収集
・システムのセキュリティ要件レビュー及び課題解決支援　等

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JPX-CSIRT

チームの正式名称	JPX-CSIRT
チームの略称	JPX-CSIRT
所属する組織名	株式会社東京証券取引所
設立年月日	2016年10月30日
チームの Email アドレス	its_csirt@jpx.co.jp
チームサイト	
所属組織サイト	http://www.jpx.co.jp/
加盟年月	2017 年 05 月

1. 概要

JPX-CSIRTは日本取引所グループ（JPX）の組織内CSIRTです。

2. 設立の経緯・背景

サイバー攻撃の手法は日々進歩しており、様々な企業・組織でホームページがダウンや情報流出などの事例が発生しています。
可能な限りマーケット運営を継続することが使命であるJPX にとっては、サイバー攻撃に対しても適切な対応が求められるため、IT を活用した入口・出口対策だけに限らず、情報管理といったルール面からの統制なども含め、継続的にセキュリティ強化策を講じていきました。
今後も、攻撃の高度化・大規模化などサイバー攻撃の脅威はますます大きくなっていくと想定されることから、これまで以上にJPX のセキュリティ態勢を強固にし、常に改善を図っていく必要があると考え、JPX-CSIRTを立ち上げることとしました。

3. 会社内における位置づけおよび活動内容

JPX-CSIRTは日本取引所グループのシステム運用部門である東京証券取引所ITサービス部及び情報システムの開発部門である、IT開発部のメンバーから構成され、情報セキュリティの統括部門、広報部門、業務部門等と連携し、インシデント対応を行います。
　また、JPX のセキュリティ態勢の継続的な改善のため、システム面でのセキュリティ対策に加え、セキュリティ診断、サイバーセキュリティ訓練等を実施しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JPHoldings CSIRT

チームの正式名称	日本郵政　CSIRT
チームの略称	JPHoldings CSIRT
所属する組織名	日本郵政株式会社
設立年月日	2015年11月1日
チームの Email アドレス	jph-irt.ii@jp-holdings.jp
チームサイト	
所属組織サイト	http://www.japanpost.jp/
加盟年月	2016 年 07 月

1. 概要

日本郵政CSIRTは、日本郵政株式会社の組織内 CSIRT です。

2. 設立の経緯・背景

近年、複雑化・巧妙化したサイバー攻撃が増加しており、日本郵政が提供するサービスについて、セキュリティイベント、及びインシデント発生時に速やかな対応を行うために設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
システム部門内の情報セキュリティ統括部署のうち、システムセキュリティを担当するグループによって構成されています。

(2)活動内容
日本郵政CSIRTは、以下の活動を実施しています。
・セキュリティイベント・インシデント発生時の対応
・脅威情報・攻撃予告の対応
・サイバー攻撃情報の収集と共有
・脆弱性情報の収集と共有
・グループ各社、社内への情報共有

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JRS-CSIRT

チームの正式名称	JRシステムシーサート
チームの略称	JRS-CSIRT
所属する組織名	鉄道情報システム株式会社
設立年月日	http://www.jrs.co.jp/
チームの Email アドレス	jrs_csirt@jrs.co.jp
チームサイト	
所属組織サイト	http://www.jrs.co.jp/
加盟年月	2017 年 08 月

1. 概要

JRS-CSIRTは、鉄道情報システム株式会社が運営するインシデント対応体制です。

鉄道情報システム株式会社は、JRグループのIT企業として『みどりの窓口』をはじめJRグループ関連情報システムおよびその他システムについて、開発から運営・管理までトータルサービスを提供しています。

2. 設立の経緯・背景

機密情報の漏えいや改ざんなどのセキュリティリスクに対し、当社では以前よりセキュリティを維持・強化するための組織および管理体制を整備し、インシデントの未然防止と早期検知に努めてきました。しかしながら、昨今のサイバー攻撃等による深刻な脅威に対し、インシデントの発生を完全に防ぐことは困難であることから、これまでの予防的な活動に加え、インシデントが発生することを前提に被害の拡散防止、対策および復旧といった一連のインシデント対応を迅速且つ確実に実施していくため、従来からのセキュリティ管理体制をCSIRTとして明確化し、活動を強化することとしました。

3. 会社内における位置づけおよび活動内容

JRS-CSIRTは、社内で発生する可能性があるインシデントの未然防止と早期検知に向けて日常的なネットワーク監視、脆弱性情報の収集・展開、定期的なセキュリティ教育、インシデント対応訓練などの予防活動を行います。インシデントが発生した際には、対応マニュアルに基づき、被害の拡散防止、原因の特定・除去、復旧といった一連のインシデント対応活動を指揮します。
また、JRシステムグループ全体として均一で高いセキュリティレベルを維持していくため、JRS-CSIRTを中心にグループ全体でセキュリティの連携を図ります。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JPLife CSIRT

チームの正式名称	かんぽCSIRT
チームの略称	JPLife CSIRT
所属する組織名	株式会社かんぽ生命保険
設立年月日	2016-01-01
チームの Email アドレス	CSIRT.ii@jp-life.jp
チームサイト	
所属組織サイト	http://www.jp-life.japanpost.jp/
加盟年月	2016 年 06 月

1. 概要

かんぽCSIRT は、当社が利用するシステムにおける情報セキュリティインシデント発生の防止策の検討及び発生時のリスクの極小化を図り、情報セキュリティ管理の高度化を目的としています。

2. 設立の経緯・背景

当社では従前から情報セキュリティに関する様々な対策を実施していますが、昨今の高度化・巧妙化するサイバー攻撃の脅威に対抗するため、組織内の態勢を強化し、統合的な管理を実現することを目的として設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置付け
かんぽCSIRTは、情報セキュリティ管理の高度化を進めていく中で、経営リスクとしてサイバーセキュリティ対策の強化、態勢整備を一段と進めることが必要であると判断し、当社コンプライアンス統括部情報セキュリティ統括室が中心となり、システム管理部と協働で、対処すべき事象に応じて、柔軟に社内外の関係者と連携して解決にあたる体制としています。

(2)活動内容
かんぽCSIRTは、自社の事業活動において利用するシステムを対象として、次の活動を実施します。
・サイバーセキュリティ事案発生時の対応
・緊急脆弱性への対応
・コンティンジェンシープランの維持管理
・社員への教育・人材育成・獲得
・サイバーセキュリティリスク評価
・サイバーセキュリティ訓練の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JRW-CSIRT

チームの正式名称	JR西日本グループCSIRT
チームの略称	JRW-CSIRT
所属する組織名	西日本旅客鉄道株式会社
設立年月日	2016年10月1日
チームの Email アドレス	jrw-csirt-secretariat@westjr.co.jp
チームサイト	
所属組織サイト	http://www.westjr.co.jp/
加盟年月	2017 年 08 月

1. 概要

JR西日本グループは2府16県を営業エリアとする鉄道事業を中心に、運輸業、流通業、不動産業など多岐にわたる事業を展開しています。
JR西日本グループCSIRT（JRW-CSIRT）は、JR西日本グループ間の情報連携により、インシデント発生時の迅速な対応および情報提供・教育等による意識向上を支援する組織です。

2. 設立の経緯・背景

昨今のサイバー攻撃の巧妙化・複雑化に伴い、情報セキュリティインシデントの発生リスクが高まる中、グループ全体の情報セキュリティレベルを向上させるべく、実効性のあるグループ共通の情報セキュリティマネジメント体制の構築が必要と考え、JR西日本グループ各社間の情報共有、情報セキュリティ事故の発生防止・被害拡大防止を目的として、JRW-CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

JRW-CSIRTはJR西日本の最高情報セキュリティ責任者（CISO）のもと、JR西日本およびJR西日本ITソリューションズを事務局とし、JR西日本およびJR西日本グループ各社をメンバーとする部門横断型の組織です。JR西日本グループにおける各種情報セキュリティインシデント発生時の初動対応サポート、各種重要情報の展開・共有、外部機関との連携、情報セキュリティ教育・研修等を実施しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JPPost CSIRT

チームの正式名称	日本郵便CSIRT
チームの略称	JPPost CSIRT
所属する組織名	日本郵便株式会社
設立年月日	2016-04-01
チームの Email アドレス	CSIRT.ii@jp-post.jp
チームサイト	
所属組織サイト	http://www.post.japanpost.jp/
加盟年月	2016 年 06 月

1. 概要

日本郵便株式会社は、日本全国に郵便局を配置して、郵便・物流サービス、ゆうちょ銀行・かんぽ生命保険等の金融代理店サービスなどを取り扱っています。
日本郵便CSIRTは、日本郵便でのセキュリティ・インシデント発生の防止及び発生時のリスクの最小化を目的として活動します。

2. 設立の経緯・背景

従来より、システムの脆弱性情報や、サイバー攻撃情報等の収集と対策、さらにインシデント発生時の対応といったセキュリティ対策を実施しておりましたが、近年のサイバー攻撃の高度化、ネット社会におけるリスクの増大を認識し、お客さまに安全・安心なサービスを継続的にお届けするため、日本郵便CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

・会社内における位置づけ
日本郵便CSIRTは、情報セキュリティ統括部署、ITガバナンス担当部署、システム管理者等によって構成された、部署横断型の組織です。

・活動内容
日本郵便CSIRTは以下の活動を実施しています。
・組織内部、外部との連絡調整
・インシデント発生時の対応支援、総合調整
・脆弱性、サイバー攻撃情報の収集及び展開
・インシデント発生防止のための総合対策推進
・セキュリティリテラシー向上の支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JTB-CSIRT

チームの正式名称	JTB-CSIRT Team
チームの略称	JTB-CSIRT
所属する組織名	株式会社JTB
設立年月日	2016年7月1日
チームの Email アドレス	itsecurity@jtb.com
チームサイト	
所属組織サイト	https://www.jtbcorp.jp/jp/
加盟年月	2017 年 08 月

1. 概要

JTB-CSIRTは、株式会社JTB（http://www.jtbcorp.jp/jp/）のCSIRTで、JTBとそのIT子会社である株式会社JTB情報システムにより運営をしています。

2. 設立の経緯・背景

JTB-CSIRTは、株式会社JTB（http://www.jtbcorp.jp/jp/）のCSIRTで、JTBとそのIT子会社である株式会社JTB情報システムにより運営をしています。

3. 会社内における位置づけおよび活動内容

JTBグループの持株会社である、株式会社JTB内のセキュリティ専門部門にて、JTBグループ各社に対し、セキュリティ対策の推進・強化の活動を行っています。
・規程、基準類の整備
・各社へのセキュリティ監査
・各社へのセキュリティ対策の企画・導入・運用のサポート
・インシデントレスポンス
・脆弱性情報や注意喚起の発信
・従業員への教育

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JRE - CSIRT

チームの正式名称	JRE - CSIRT
チームの略称	JRE - CSIRT
所属する組織名	東日本旅客鉄道株式会社
設立年月日	2016年9月1日
チームの Email アドレス	JRE-CSIRT@jreast.co.jp
チームサイト	
所属組織サイト	http://www.jreast.co.jp/
加盟年月	2016 年 12 月

1. 概要

JRE - CSIRTは、東日本旅客鉄道株式会社のセキュリティ対応や教育、セキュリティ規定類のルール整備等を行うことを目的に作られた組織体制です。

2. 設立の経緯・背景

急増するサイバー攻撃や、社会的に強化が求められる情報漏えい対策、システム障害などの、コンピュータセキュリティにかかるインシデントに対処するために、既に存在していたシステム障害時の対策本部体制を組織的に発展させCSIRT体制を構築しました。

3. 会社内における位置づけおよび活動内容

会社内の位置づけとしては、鉄道業務等に関するサイバーセキュリティ事象が発生した場合に、インシデントレスポンスチームとなる形態をとっています。
活動内容としては、迅速な初動対応により被害拡大を防ぐことや、初動対応マニュアルの策定など緊急時の対応体制を整備することや、社員へのセキュリティ教育・研修、注意喚起、セキュリティ規定類整備等を目的としています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JXTG-SEC

チームの正式名称	JXTG SECurity management group
チームの略称	JXTG-SEC
所属する組織名	JXTGホールディングス株式会社 JXアイティソリューション株式会社
設立年月日	2017年4月1日
チームの Email アドレス	jxtg_sec@jxtg.com
チームサイト	
所属組織サイト	http://www.hd.jxtg-group.co.jp/ http://www.it.jx-group.co.jp/
加盟年月	2017 年 08 月

1. 概要

当チームは顧客およびJXTGグループに対し、セキュリティインシデントに対する窓口機能を提供します。また、外部組織および専門ベンダーと連携・協業し、セキュリティインシデントの検知、解決、被害の局所化、および発生の予防を支援します。

2. 設立の経緯・背景

近年のサイバー攻撃の高度化による脅威は年々高まっており、多様化・複雑化する攻撃に対応するため、セキュリティインシデントに対する組織的対応力の強化は必要不可欠といえます。このような状況下において、重要インフラ事業者の責務を全うするため、当グループでは2016年4月より組織的インシデント対応体制の検討／整備を行い、セキュリティインシデントの発生から収束までを行う体制および対応フローを明確化し、2017年4月より正式に稼働を始めました。

3. 会社内における位置づけおよび活動内容

【会社内における位置づけ】
JXTG-SECは、JXTGグループのIT機能会社であるJXアイティソリューション株式会社のセキュリティ担当部署に設置され、専任メンバーで構成されています。

【活動内容】
JXTG-SECの平時及び緊急時の機能は以下の通りです。
1. セキュリティインシデントに関する情報収集、対応窓口機能 。
2. セキュリティインシデント発生時における情報収集、技術対応支援、被害の局所化、発生の予防を支援、および関係各所への報告。
3. 情報セキュリティレベル向上のための施策 (教育を含む) の検討・実施。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

K-SIRT

チームの正式名称	KAJIMA Security Incident Response Team
チームの略称	K-SIRT
所属する組織名	鹿島建設株式会社
設立年月日	2010-04-01
チームの Email アドレス	k-sirt@kajima.com
チームサイト	
所属組織サイト	http://www.kajima.co.jp/
加盟年月	2016 年 03 月

1. 概要

KAJIMA SIRT (K-SIRT) は、鹿島建設株式会社によって運営されている「CSIRT」です。
鹿島建設株式会社は、何もないところから、形あるものを生み出していく「建設事業」を中心とし、顧客のニーズを理想的な形で実現するための「設計・エンジニアリング」事業、土地固有のポテンシャルを引き出す「不動産開発」事業、構造技術や材料からバイオテクノロジーまで「研究開発」など、技術力と総合力を駆使し世界中で社会基盤をつくっています。

2. 設立の経緯・背景

弊社では、以前から情報セキュリティ推進部署を設置して、様々な情報セキュリティ対策を実施してきました。しかし、昨今の高度化するサイバー攻撃に対し、より迅速かつ確実に対応するため、他社や外部機関との情報連携が重要であると認識しました。情報共有を推進するために、日本シーサート協議会に加盟いたします。

3. 会社内における位置づけおよび活動内容

(1)位置付け
総務部と IT ソリューション部が合同で情報セキュリティ推進部署を設立し、情報セキュリティに関する活動及びインシデント対応にあたっています。
(1)活動内容
KAJIMA-SIRT は主に以下の活動を実施しています。
・情報セキュリティについての調査及び情報収集を行う。
・当社の情報セキュリティに関して、対策の検討、策定、周知及び指導を行う。
・外部からの当社ネットワークへの接続や新規に挿入する情報システムに対してセキュリティ対策の妥当性の審査を行う。
・情報システムのセキュリティに関する教育を実施する。
・情報セキュリティ対策の運用について、情報セキュリティ監査を実施する。
・情報セキュリティインシデントに対して、初期対策を検討・指示・実施し、被害の拡散防止、早期復旧を図る。
・情報セキュリティインシデントに対して、再発防止策を策定及び実施する。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

JT CSIRT

チームの正式名称	JT Cyber Security Incident Response Team
チームの略称	JT CSIRT
所属する組織名	日本たばこ産業株式会社
設立年月日	2016-02-25
チームの Email アドレス	jtcsirt@jt.com
チームサイト	
所属組織サイト	https://www.jti.co.jp/
加盟年月	2017 年 01 月

1. 概要

JT CSIRTは、日本たばこ産業株式会社のIT部門が運営するセキュリティインシデント対応のための組織です。

2. 設立の経緯・背景

日本たばこ産業株式会社及びグループ企業において、情報セキュリティに関係する事故が発生した場合に、その状況を正確に把握し、適切な措置を施すことで内外のステークホルダーへの影響を最小限に抑え、事態を早期に収束させることを目的として2016年2月にCSIRTを設置しました。

3. 会社内における位置づけおよび活動内容

JT CSIRTの主な活動内容は以下の通りです。
(1)インシデント発生判断
　判断基準に基づくインシデント発生有無の判断
(2)事績の記録及び関係者への連絡
　インシデント発生からの状況推移に関する記録
　インシデント発生から収束までにおける関係者への連絡
(3)分析
　インシデントの重大度の初期評価
　インシデントの詳細に関する分析
(4)封じ込め
　被害拡大を防止するための初期対応の指揮
(5)原因除去
　インシデントの原因を除去する対応の指揮

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

k.CSIRT

チームの正式名称	kabu.com Cyber Security Incident Readiness Team
チームの略称	k.CSIRT
所属する組織名	カブドットコム証券株式会社
設立年月日	2016年1月7日
チームの Email アドレス	csirt@kabu.com
チームサイト	
所属組織サイト	https://kabu.com/
加盟年月	2017 年 04 月

1. 概要

k.CSIRTは、カブドットコム証券株式会社が運営するCSIRTです。

カブドットコム証券は、「顧客投資成績重視の経営」を経営理念に掲げています。お客さまが儲かることこそが当社の成長・拡大につながると確信し、そのための経営態勢の構築やサービスの拡充などに努めています。

2. 設立の経緯・背景

昨今のサイバー攻撃の高度化・巧妙化あるいは、個人情報漏えい事案が発生していることを踏まえ、サイバーセキュリティの重要性を認識し、必要な体制を整備するため2016年1月にCSIRTを設立いたしました。

3. 会社内における位置づけおよび活動内容

(1)チーム体制
k.CSIRTは、システム部門およびリスク管理部門をメンバーとして運営しています。

(2)活動内容
k.CSIRTは主に以下の事項を実施いたします。

a.サイバーセキュリティ管理体制の強化
・サイバーセキュリティに関する社内ガイドラインの整備
・サイバー攻撃に関する訓練の起案および実施(社外の訓練参加を含む)
・人材育成計画の起案および実施

b.サイバー攻撃への事前対策
・各種サイバー攻撃対策の検討および導入
・脆弱性に関する情報収集および対策の実施
・サイバーセキュリティに関する技術動向の調査
・外部機関／グループ会社との連携および情報共有

c.サイバー攻撃発生時のインシデントハンドリング

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KADOKAWA-CSIRT

チームの正式名称	KADOKAWA Computer Security Incident Response Team
チームの略称	KADOKAWA-CSIRT
所属する組織名	株式会社KADOKAWA
設立年月日	2014-12-15
チームの Email アドレス	office@kadokawa-csirt.jp
チームサイト	https://tool.kadokawa-csirt.jp/
所属組織サイト	https://tool.kadokawa.co.jp/
加盟年月	2015 年 03 月

1. 概要

当社は 2013 年 10 月に連結子会社 9 社 (アスキー・メディアワークス、エンターブレイン、角川学芸出版、角川書店、角川マガジンズ、角川プロダクション、中経出版、富士見書房、メディアファクトリー) と合併し、One Company の KADOKAWA として新たなスタートを切りました。
優れたコンテンツを継続的に創造し、それを多様な形でメディアミックス展開していく従来の強みに加え、電子書籍ストアの BOOK☆WALKER はじめとする業界プラットフォームを自ら立ち上げ運営する、「コンテンツをベースとしたプラットフォーマー」への変貌を遂げるべく、たゆまぬ企業努力を尽くしてまいります。そして、日本市場に留まることなく、世界に展開する「グローバルエンターテインメント企業」を目指しています。

2. 設立の経緯・背景

KADOKAWA グループではプロモーションサイトやコーポレートサイト、EC サイトなど 700 サイトを超える Web サイトを運営しており、その数は日々増えております。こうした多数の Web サーバーをサイバー攻撃から防御することを目的とし、2014 年 12 月 15 日に KADOKAWA-CSIRT が設立されました。これまで、各種サーバーへの IPS および WAF の導入、脆弱性試験、セキュリティインシデントへの対応などを実施してまいりましたが、昨今のサイバー攻撃やゼロデイアタックの脅威から ICT を守るには、社内チームだけでは力不足だと判断し、日本シーサート協議に加盟することといたしました。KADOKAWA-CSIRT は、日本シーサート協議会加盟チームと連携し、インシデント防止に貢献して参りたいと考えております。

3. 会社内における位置づけおよび活動内容

社内及び、連結子会社における IT 統制と、セキュリティ向上支援、サーバーの安全性チェック、脆弱性チェック、インシデント支援等。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KAIYODAI-CSIRT

チームの正式名称	海洋大CSIRT
チームの略称	KAIYODAI-CSIRT
所属する組織名	国立大学法人東京海洋大学
設立年月日	2017年3月17日
チームの Email アドレス	csirt@o.kaiyodai.ac.jp
チームサイト	https://www.kaiyodai.ac.jp/student/ITsecurity/csirt.html
所属組織サイト	https://www.kaiyodai.ac.jp/
加盟年月	2017 年 08 月

1. 概要

海洋大CSIRT は、国立大学法人東京海洋大学の組織内 CSIRT です。
東京海洋大学は2003年10月に東京商船大学と東京水産大学が統合して誕生した新しい大学です。両大学の前身はそれぞれ1875年と1888 年に設立されており、本学は140年を越える歴史と伝統を誇っています。
東京海洋大学は両大学の伝統と個性・特徴を継承すると共に、時代の要請に応えて、新たな教育研究分野への展開を図り、国内唯一の海洋系大学として、世界最高水準の卓越した教育研究拠点の形成を目指しています。

2. 設立の経緯・背景

近年の高度化するサイバー攻撃に法人として迅速に対応し、情報セキュリティ環境の維持・向上を目的として、2017年3月17日に海洋大-CSIRTが設立されました。

3. 会社内における位置づけおよび活動内容

(会社内における位置づけ)
海洋大 CSIRTは、平成29年3月に、学内の情報セキュリティに関する部局横断的なインシデント対応チームとして、CISOの下に設置されました。国立大学法人東京海洋大学における情報セキュリティ対策基本計画に基づき、情報セキュリティ総括責任者（CISO）、情報セキュリティ実施責任者、学術情報課職員のほか、部局技術責任者等で構成されています。

情報システムの安全性維持および向上、リスク低減のために、大学として必要な対処を速やかに実施します。

(活動内容)
海洋大 CSIRTは、CISOの指示によって学内の情報セキュリティに関わる以下の業務を担当します。

セキュリティ情報のユーザへの提供（学内外への注意喚起等）
セキュリティ訓練、教育
セキュリティインシデントの検知（ログ収集、ログ分析・検索等）
インシデント対応（復旧支援）
サイバーセキュリティに係る情報収集・分析、脅威情報に基づく緊急対応
学内情報システムの構成情報の収集およびリスク分析（システム強化の提言、情報システム調達時の支援、脆弱性検査等）
外部連携（他機関との情報交換・連携強化等）
情報セキュリティに関する相談窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KB-CSIRT

チームの正式名称	京都銀行CSIRT
チームの略称	KB-CSIRT
所属する組織名	株式会社京都銀行
設立年月日	2014-10-01
チームの Email アドレス	kb-csirt@kyotobank.co.jp
チームサイト	
所属組織サイト	http://www.kyotobank.co.jp/
加盟年月	2015 年 03 月

1. 概要

京都銀行CSIRT は、京都銀行におけるサイバー攻撃等のインターネットを通じたコンピュータ・セキュリティ・インシデントに関して一元的に対応を行う組織内 CSIRT です。

2. 設立の経緯・背景

複雑化・巧妙化するサイバー攻撃等のインターネットを通じたコンピュータ・セキュリティ・インシデントに迅速に対応できるように、情報セキュリティに関する信頼できる対応窓口として、社内外の組織や専門家と協力して、コンピュータ・セキュリティ・インシデントの検知、解決、被害局限化、および発生の予防を支援することにより、自社および情報ネットワーク社会のセキュリティ向上に貢献することを目的に設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置付け
サイバーセキュリティを所管するシステム部のサイバーセキュリティ対策室によって組織されています。

(2)活動内容
京都銀行CSIRT は以下の活動を実施しています。
・インシデント発生抑制のための対応
脆弱性情報の収集・対応
セキュリティ関連の情報収集・分析、注意喚起
各種モニタリング
・インシデント発生時の対応
被害局限化・復旧のための対応 (インシデントの検知、報告受付、事実確認、対応判断、対処、報告、再発防止検討等)
・セキュリティ品質向上に向けた対応
リスク評価・分析
訓練の計画・実施
教育・啓蒙活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

K-OPT CSIRT

チームの正式名称	K-Opticom Computer Security Incident Response Team
チームの略称	K-OPT CSIRT
所属する組織名	株式会社ケイ・オプティコム
設立年月日	2015-06-24
チームの Email アドレス	csirt@k-opti.com
チームサイト	
所属組織サイト	http://www.k-opti.com/
加盟年月	2015 年 08 月

1. 概要

株式会社ケイ・オプティコム (K-OPT) は、関西電力グループの一員として、関西地域の eo光を代表とする固定通信サービスや、mineo といった全国的な MVNO 移動体通信を提供する事業会社です。K-OPT CSIRT は、K-OPT で発生したサイバーセキュリティインシデントに対応します。

2. 設立の経緯・背景

K-OPT では、サイバーセキュリティインシデントに対して、複数部門にまたがるインシデントの調整や全社展開、および、外部組織と積極的に情報交換するため、CSIRT を平成 27 年 6 月に発足させました。

3. 会社内における位置づけおよび活動内容

K-OPT CSIRT は、リスクマネジメントグループ情報セキュリティチームを中心に、K-OPT の設備運用・保守からお客様対応までの複数の組織から構成されています。K-OPT で発生したセキュリティインシデント発生時の部門横断的な対応支援だけでなく、被害が軽減されるための体制、環境および仕組みの構築を推進し、K-OPT のセキュリティ向上を行い、お客様が安心・安全に利用できるインターネットの実現を目指します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KCCS-CSIRT

チームの正式名称	KYOCERA Communication Systems Computer Security Incident Response Team
チームの略称	KCCS-CSIRT
所属する組織名	京セラコミュニケーションシステム株式会社
設立年月日	2015-10-01
チームの Email アドレス	kccs-csirt@kccs.co.jp
チームサイト	
所属組織サイト	https://www.kccs.co.jp
加盟年月	2016 年 05 月

1. 概要

KCCS-CSIRT は京セラコミュニケーションシステム株式会社が運営している組織内 CSIRT です。当社は 1995 年に京セラ株式会社経営情報システム事業部が主体となって事業を開始し、現在では企業の情報基盤 (ICT)、社会の通信基盤 (通信エンジニアリング)、環境との共生基盤 (環境・エネルギーエンジニアリング)、そして企業の経営基盤を構築・運用支援 (経営コンサルティング) する 4 事業を展開しています。それぞれを高いレベルで提供するとともに、事業がクロスする部分のシナジーにより新たな事業領域を創出し、お客様企業の収益性の向上に取り組んでいます。

2. 設立の経緯・背景

当社では情報システム部門を中心に社内の情報セキュリティ対策を推進していました。しかし、近年の高度化、巧妙化するセキュリティ脅威に対して予防的な観点だけではなく、特にセキュリティインシデント発生時の迅速な把握や対処の強化を目的として、2015 年 10 月に当社のセキュリティ部門及び社内インフラ部門も含めた横断的な組織として CSIRT を設立し、2016 年 2 月から運用を開始いたしました。

3. 会社内における位置づけおよび活動内容

KCCS-CSIRT はセキュリティインシデント発生時の検知や対応、管理等を目的とした組織であり、当社の情報セキュリティに関する決議機関である情報セキュリティ管理部会内に属する実働部隊として活動を行います。組織体制としては情報システム部門とセキュリティ部門を中心に、社内インフラ部門も含めて横断的に構成される仮想的な組織となります。
活動内容として、平時には、セキュリティインシデント情報収集、セキュリティ監視、セキュリティ情報発信などを行います。非常時には、インシデント対応の実働部隊として情報システム部門を中心に各部門が連携し、原因調査や対処、対応及び対策の実施などを行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KDDI-CSIRT

チームの正式名称	KDDI Computer Security Incident Response Team
チームの略称	KDDI-CSIRT
所属する組織名	KDDI株式会社
設立年月日	2005-10-01
チームの Email アドレス	csirt@kddi.com
チームサイト	
所属組織サイト	http://www.kddi.com/business
加盟年月	2013 年 01 月

1. 概要

KDDI-CSIRT は、スマートフォン・携帯電話サービス「au」と、インターネットサービス「au one net」、さらにパーソナル、ビジネス向けに電話、VPN 等の各種通信サービス等をグローバルに提供する KDDI 株式会社 (http://www.kddi.com) の CSIRT です。

2. 設立の経緯・背景

KDDI は 2005 年 10 月に、サービス提供用のシステム、ネットワークのサイバーセキュリティ技術課題を専門に扱う部署として「セキュリティオペレーションセンター」(SOC) を設立しました。また 2010 年には「KDDI SOC」というチーム名で FIRST に参加しました。

SOC はインシデント対応の社内調整を行う役割も担っていましたが、昨今のサイバー脅威の増大に伴い、インシデント対応の専門チームの設置が望まれる状況となり、2012 年に KDDI-CSIRT が、SOC 配下のチームとして設けられました。2013 年 4 月からは SOC の専任メンバーに加え、システム等の実対応を行う部署からの兼任メンバーを迎え体制を強化しました。

3. 会社内における位置づけおよび活動内容

KDDI-CSIRT は、KDDI のサービス提供用システム、ネットワークのインシデント対応機能・体制を維持向上し、万一の際は効率的、効果的にインシデントに対応することを通じ、お客様に安心して KDDI サービスをご利用いただく環境作りを目指しています。その活動内容は、インシデントレスポンスに係る社内コーディネーション、脆弱性ハンドリング、セキュリティ情報収集、外部機関等への参加、貢献などです。

緊急時には、CSIRT による助言、調整と役員へのエスカレーション等を通じ、事業、営業、技術、運用、管理等の社内各部門が連携・協調して対応して行きます。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KEIHAN-SIRT

チームの正式名称	京阪グループSIRT
チームの略称	KEIHAN-SIRT
所属する組織名	京阪ホールディングス株式会社
設立年月日	2017年2月1日
チームの Email アドレス	keihan-sirt@ml.keihan.co.jp
チームサイト	
所属組織サイト	http://www.keihan-holdings.co.jp/
加盟年月	2017 年 02 月

1. 概要

京阪グループは、約50社におよぶ企業で「運輸業」「不動産業」「流通業」「レジャー・サービス業」の4つの事業を営み、経営理念に掲げる「人の暮らしに夢と希望と信頼のネットワークを築いて、快適な生活環境を創造し、社会に貢献」するための取り組みを進めています。
京阪グループSIRTは、京阪グループのセキュリティインシデントに対応するCSIRTで、京阪ホールディングス株式会社とその子会社である株式会社京阪ビジネスマネジメントにより運営しています。

2. 設立の経緯・背景

京阪ホールディングスでは情報セキュリティを維持するため、2004年に「情報セキュリティ委員会」を設置し、セキュリティーポリシーを策定して対応してきましたが、近年、企業が保有する個人情報や重要情報等を狙ったサイバー攻撃が増加して、その手口も巧妙化しており、従来どおりの対応では防ぎきれなくなってきています。
そのため、情報セキュリティインシデントの発生前から準備を行い、発生の検知から収束までの機能・体制を強化することによって被害の拡大防止を図ることを目的として京阪グループSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
京阪グループSIRTは、京阪ホールディングス株式会社経営統括室IT推進部および株式会社京阪ビジネスマネジメントIT事業部のメンバーにより構成される仮想的な組織で、経営統括室IT推進部長（京阪グループSIRT代表者）がメンバーを指名します。

(2)活動内容
(ア)平常時の事前準備・予防活動
・インシデントレスポンス体制と手順の整備
・訓練・演習の実施
・セキュリティ関連情報の収集と京阪グループ内へ情報提供・ユーザ啓発
・外部組織との情報交換
・脆弱性情報・脅威情報のハンドリング
・セキュリティレポートの発行
(イ)インシデント対応
・検知・連絡受付
・トリアージ
・初動対応および復旧措置の検討と実施
・再発防止策の検討
・報告用資料の作成

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KEIO-SIRT

チームの正式名称	京王SIRT
チームの略称	KEIO-SIRT
所属する組織名	京王電鉄株式会社
設立年月日	2015-06-26
チームの Email アドレス	keio-sirt@keio.co.jp
チームサイト	
所属組織サイト	http://www.keio.co.jp
加盟年月	2016 年 03 月

1. 概要

京王SIRT (略称 KEIO-SIRT) は、京王電鉄株式会社 (http://www.keio.co.jp/) の CSIRT で、京王電鉄とその IT 子会社である株式会社京王ITソリューションズにより運営しています。

2. 設立の経緯・背景

従来から情報セキュリティインシデント対応や脆弱性情報の収集を京王電鉄内 IT 管理部を中心とする情報セキュリティ分科会 (社内委員会組織) を組織し対応してきましたが、近年のサイバー攻撃の頻発や政府及びステークホルダーからの情報セキュリティ緊急時対応体制強化の要請といった状況に鑑み、2015 年 6 月、CSIRT の設置を図り、重大インシデントの発生から収束までの機能・体制を強化することにより緊急時対応体制を構築しました。

3. 会社内における位置づけおよび活動内容

京王SIRT は京王電鉄IT管理部と京王ITソリューションズ双方のメンバーで構成される仮想的な組織体で、メンバーは IT 管理部長 の指名によります。

京王SIRT は、京王電鉄及びグループ各社内で発生した情報セキュリティインシデントに対して直接対応を行なう組織内 CSIRT としての役割を担います。

京王SIRT の平時及び事故発生時、機能は以下の通りです。
A)会社全体の情報セキュリティレベル向上のための施策 (教育含む) の検討・実施。
B)情報セキュリティ事故発生防止のための監視、検知及び警告。
C)情報セキュリティ事故発生時における技術対応及び指示・助言、並びに被害最小化のための施策実施。

特に、情報セキュリティに関わる重大インシデントが発生した場合、CSIRT 長たる IT 管理部長は会社のリスク管理体制に参画すると共に京王SIRT を指揮し、京王SIRT はインシデント解決のための技術的な支援を行います。

また、情報管理に関わる課題を検討する部門横断の組織を京王SIRT が運営することにより、会社の情報やお客様の情報の取り扱いに関わる業務手順、ICT 機器の取り扱いルール改定等の PDCA を行いインシデント発生の未然防止と被害極小化に努めています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KEYWARE-CSIRT

チームの正式名称	キーウェアシーサート
チームの略称	KEYWARE-CSIRT
所属する組織名	キーウェアサービス株式会社
設立年月日	2014-07-17
チームの Email アドレス	keyware-csirt@keyware.co.jp
チームサイト	
所属組織サイト	http://www.keyware.co.jp/keywareservice/
加盟年月	2015 年 01 月

1. 概要

弊社は平成 13 年にキーウェアソリューションズ株式会社から、サポートサービス事業を中核にグループのシステム運用・維持・保守を担う子会社として発足しました。企業スローガン【「IT can create it」 クリエイティブな発想で、IT の持つ無限の可能性を現実のものとします】を掲げ、キーウェアソリューションズ株式会社との協業でお客様システムの企画・設計から導入・運用・保守に至る一貫したサービスで、お客様システムのライフサイクルをトータルにサポートいたします。

2. 設立の経緯・背景

設立以前にも CSIRT に類する機能はあったものの、属人化された対応が散見される、社外組織と情報連携窓口がないなどの不備がありました。この不備を少しずつ改善していき、効率的にセキュリティインシデントに対応できるための体制づくりができるような活動を目指して 2014 年に 7 月にチームが設立されました。

3. 会社内における位置づけおよび活動内容

KEYWARE-CSIRT はサービス管理部門を中心に関連部署から有志が集まり構成される仮想組織で、中心となる活動は以下の 3 つの活動となります。

1.インシデント対応

キーウェアソリューションおよび関連会社にてインシデントが発生した場合、被害状況や影響範囲の分析を行い、復旧対応までを行います。今後は、事故前提の組織体制を確立し、設立以前と比較して、インシデントの発覚から収束までの期間の短縮や、被害の極小化ができるような改善提案ができることを目指します。

2.現状分析

最新のセキュリティ動向及び脆弱性情報を収集して、可能であれば自社サービスへの影響を分析します。影響が認められる場合は予防策を策定して、関係部門に予防策の実施を提案を目指します。

3.社外関連組織との協調

日本シーサート協議会加盟各組織をはじめとする社外組織と定期的にセキュリティに関する情報の連携や共有を行い、日本のインターネットサービスのセキュリティ向上に貢献します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KINDAI-CSIRT

チームの正式名称	近畿大学CSIRT
チームの略称	KINDAI-CSIRT
所属する組織名	学校法人近畿大学
設立年月日	2016年10月6日
チームの Email アドレス	csirt@ml.kindai.ac.jp
チームサイト	
所属組織サイト	http://www.kindai.ac.jp/
加盟年月	2017 年 01 月

1. 概要

近畿大学は、14学部48学科と短期大学部、法科大学院と大学院11研究科を有する「医学から芸術まで」あらゆる分野を網羅する日本屈指の総合大学です。
「実学教育」と「人格の陶冶」を建学の精神に、「人に愛され、信頼され、尊敬される人 を育成すること」を教育の目的としています。

2. 設立の経緯・背景

昨今のサイバー攻撃の高度化・巧妙化や情報セキュリティインシデントが経営に与える影響が増大していることを背景に、情報セキュリティインシデントを早期に発見・解決、事前対策、事後対応をすることを目的として、2016年10月にKINDAI-CSIRTを構築しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
KINDAI-CSIRTは、学校法人近畿大学が運用する教育、研究、事務および医療に係る情報システムを統括する総合情報システム委員会のもとに置かれ、法人全体向けに情報セキュリティインシデント対応等の支援を実施するチームです。

(2)活動内容
・情報セキュリティインシデント対応
・外部機関から提供される情報セキュリティインシデント動向の把握
・ネットワーク・サーバの脆弱性診断
・情報セキュリティインシデント情報の法人内への展開
・教職員への情報セキュリティ教育

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KJ-CSIRT

チームの正式名称	KPMG Japan Computer Security Incident Response Team
チームの略称	KJ-CSIRT
所属する組織名	有限責任 あずさ監査法人
設立年月日	2016年9月28日
チームの Email アドレス	csirt@jp.kpmg.com
チームサイト	
所属組織サイト	https://home.kpmg.com/jp/ja/home/about/azsa.html
加盟年月	2016 年 10 月

1. 概要

KJ-CSIRT は、KPMGジャパンによって運営されるCSIRT です。　KPMGジャパンは、KPMGインターナショナルの日本におけるメンバーファームの総称であり、監査、税務、アドバイザリーの3つの分野に渡る7つのプロフェッショナルファームによって構成されています。(あずさ監査法人／KPMG税理士法人／KPMGコンサルティング／KPMG FAS／KPMGあずさサステナビリティ／KPMGヘルスケアジャパン／KPMG社会保険労務士法人)

2. 設立の経緯・背景

インシデント被害の最小化を目的とし、インシデントやインシデント関連事象への対応を行うための機能・役割

サイバー攻撃に関するKPMGインターナショナルにおける監視体制GSOC(Global Security Operation Center) の構築以降、全世界のKPMGメンバーファームがワンファームとして確固たるセキュリティ基盤を整備し、インシデント発生時においてはその被害拡大の防止と早期解決を可能とする実効性ある体制を維持するため、各国におけるCSIRT活動の推進とGSOCとのより強固な連携が求められるようになりました。

3. 会社内における位置づけおよび活動内容

NITSO (National IT Security Officer)を中心に、社内IT部署と社内情報セキュリティ部署によって構成されるバーチャルチームです。　KJ-CSIRTはGSOCとの連携のもとで、次の業務を実施します。
・サイバーセキュリティに関する各種情報の収集
・サイバーセキュリティに関する啓発活動(利用者への教育訓練の実施)
・インシデント発生時の対応(GSOCとの連携含む)
・インシデントの未然防止(脆弱性管理、セキュリティモニタリング)

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KKCSIRT

チームの正式名称	カカクコムセキュリティインシデントレスポンスチーム
チームの略称	KKCSIRT
所属する組織名	株式会社カカクコム
設立年月日	2007-01-04
チームの Email アドレス	kkcsirt@kakaku.com
チームサイト	
所属組織サイト	http://corporate.kakaku.com/
加盟年月	2008 年 01 月

1. **概要**
   KKCSIRT は、消費生活サポートを提供するインターネット・メディア企業である株式会社カカクコム (http://corporate.kakaku.com/) の CSIRT です。
2. **設立の経緯・背景**
   KKCSIRT は、2005 年に発生した不正アクセスのインシデントを契機に、セキュリティインシデント対応を目的とした専門チームとして、情報セキュリティ室内に設置されました。
3. **会社内における位置づけおよび活動内容**
   KKCSIRT は、主に情報セキュリティ室のメンバーで構成され、セキュリティインシデント に関するカカクコムグループの窓口となり、当社グループ内外の組織や専門家と協力して、セキュリティインシデントの発生の予防、検知、解決、被害の最小化を支援し、当社グループのサービスを利用する全ての利用者のセキュリティ向上に取り組んでいます。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KLIRRT

チームの正式名称	Kaspersky Lab Incident Research and Response Team
チームの略称	KLIRRT
所属する組織名	株式会社Kaspersky Labs Japan
設立年月日	2004-02-01
チームの Email アドレス	klirrt@kaspersky.co.jp
チームサイト	
所属組織サイト	http://www.kaspersky.co.jp/
加盟年月	2010 年 01 月

1. 概要
2. 設立の経緯・背景
3. 会社内における位置づけおよび活動内容

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KM-CSIRT

チームの正式名称	KONICA MINOLTA Computer Security Incident Response Team
チームの略称	KM-CSIRT
所属する組織名	コニカミノルタ株式会社
設立年月日	2016-01-14
チームの Email アドレス	km-csirt@konicaminolta.jp
チームサイト	
所属組織サイト	http://www.konicaminolta.jp/
加盟年月	2016 年 04 月

1. 概要

コニカミノルタは 1873 年の創業以来培ってきた多彩な技術を活用して、情報機器や産業用光学システム、医療用画像診断システムなど、さまざまな分野の事業を展開しています。
KM-CSIRT は、サイバー攻撃などによるインシデントが発生した場合に、お客様へのサービス提供ならびに企業活動への影響が最小限になるよう活動していきます。

2. 設立の経緯・背景

企業を標的としたサイバー攻撃の増加は著しく、情報漏えい、業務妨害等による企業被害を防ぐには、防御・検知・分析・対処のコントロールが必要です。防御・検知への対策を実施していても、サイバーセキュリティ問題は発生します。その時に素早く、適切に問題対応することで企業を守ることが必要であり、KM-CSIRT を設立しました。

3. 会社内における位置づけおよび活動内容

KM-CSIRT はコニカミノルタグループ情報セキュリティ統括管理責任者の直下に属するセキュリティインシデントレスポンスチームとして位置づけられ、インシデントに対し発生部門、コーポレート部門などと連携し活動します。活動内容は以下の通りです。

□予防
-脅威・脆弱性情報の収集
-インシデント対応訓練
-ログの収集、監視
□インシデント対応
-トリアージ
-関連部門と連携したインシデント対応
□インシデント対応後
-再発防止策の検討

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KEK CSIRT

チームの正式名称	KEK 情報セキュリティインシデント対応チーム
チームの略称	KEK CSIRT
所属する組織名	高エネルギー加速器研究機構
設立年月日	2010-06-17
チームの Email アドレス	csirt@kek.jp
チームサイト	
所属組織サイト	https://www.kek.jp/
加盟年月	2012 年 05 月

1. 概要

高エネルギー加速器研究機構 (KEK) は、加速器と呼ばれる装置を使って基礎科学を推進する研究所です。

KEK CSIRT は、KEK の中で情報セキュリティ事象等が発生した場合、被害の拡大を防ぐとともに、障害・事故等からの復旧の支援、予防策の普及と実施のために設置されました。

2. 設立の経緯・背景

1998 年頃より、KEK の研究組織の一つである共通基盤研究施設 計算科学センターは攻撃の監視やインシデント対応などを行ってきました。しかし、2006 年に発生した KEK の DMZ ネットワークにある Web サーバの一つにフィッシングサイトが立てられたインシデントをきっかけに、研究の円滑な推進には国内外の大学を含む諸研究機関からの信頼にこたえる情報セキュリティの確保が必須であると考えられ、2010 年 6 月に情報セキュリティポリシーの改定と共に KEK CSIRT が設立されました。

3. 会社内における位置づけおよび活動内容

(1)位置付け
KEK CSIRT は組織横断の仮想組織です。現在、高度情報利用推進室、および計算科学センター、管理局の職員から構成されています。
(2)活動内容
主な活動は以下の通りです。
・インシデント対応
KEK CSIRT は、機構内外に対する緊急対応窓口として機能し、各組織に在籍する情報セキュリティマネージャとの連携し、インシデント対応を行っています。
また、被害に遭った機器の復旧作業に対し技術的な支援を行います。
・教育
高度情報利用推進室に所属する KEK CSIRT メンバーによる、KEK 内へ向けてのセキュリティ講習会や情報セキュリティセミナーを定期的に開催しています。
・他機関との情報交換
日本シーサート協議会、共同利用機関におけるセキュリティワークショップなどでの情報交換を通じ、脅威に備える対策の検討を行っています。
・情報セキュリティに関する相談窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Kobayashi-SIRT

チームの正式名称	Kobayashi Security Incident Response Team
チームの略称	Kobayashi-SIRT
所属する組織名	小林製薬株式会社
設立年月日	2017年3月1日
チームの Email アドレス	kobayashi-sirt@kobayashi.co.jp
チームサイト	
所属組織サイト	http://www.kobayashi.co.jp
加盟年月	2017 年 03 月

1. 概要

小林製薬グループは「“あったらいいな”をカタチにする」というブランドスローガンのもと、世の中にない新しい製品を作り続けてきました。医薬品だけにとどまらずオーラルケア・スキンケア・栄養補助食品・芳香消臭剤といった幅広い領域において製品を提供しています。

2. 設立の経緯・背景

小林製薬グループでは、常に安心・安全なサービスを提供し続け、いつまでも信頼される企業でありつづけたいとの考えのもと、取引の安全性を確保するため、種々のシステム上の対策を講じ、お客さまに安心してお取引いただくためにセキュリティ対策を実施しています。
様々なセキュリティ対策を有効に機能させるために情報セキュリティインシデントへの体制が必要であると判断し、Kobayashi-SIRTを設立しました。

3. 会社内における位置づけおよび活動内容

(1)会社内における位置づけ
Kobayashi-SIRTは、小林製薬のシステム部門と関連部門で構成しております。

(2)活動内容
インシデントハンドリング、セキュリティ関連情報提供、脆弱性情報ハンドリング、セキュリティ教育などを提供しております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KOSEN-CSIRT

チームの正式名称	高専機構CSIRT
チームの略称	KOSEN-CSIRT
所属する組織名	独立行政法人国立高等専門学校機構
設立年月日	2016年4月1日
チームの Email アドレス	csirt@kosen-k.go.jp
チームサイト	https://csirt.kosen-k.go.jp/
所属組織サイト	http://www.kosen-k.go.jp/
加盟年月	2018 年 07 月

1. 概要

KOSEN-CSIRT は、独立行政法人 国立高等専門学校機構 (高専機構) の組織内 CSIRT で、全国 51 校 55 キャンパスの国立高専と高専機構本部事務局の情報セキュリティ対策とインシデントレスポンスを主に行っています。
国立高等専門学校機構は、2004 年に設立された独立行政法人で、国立高等専門学校 (国立高専) を運営しています。国立高専は、中学校の卒業生を学生として受け入れる高等教育機関で、1962 年の 12 校からスタートし現在 51 校が設置されています。

2. 設立の経緯・背景

元々、国立高専は独立した学校で、各校で情報センタ等を設置し、個別に情報セキュリティ対策や啓発、インシデント対応を行っていました。独立行政法人化された後も、各高専や機構本部事務局の担当者間で情報共有等を行ってきましたが、近年のサイバー攻撃の増加や巧妙化に対応し、全国の国立高専の情報セキュリティ担当部署とより連携し、国立高専全体としてサイバー攻撃への対策やインシデント対応力を高めるために、2016 年 4 月に KOSEN-CSIRT を設置し、情報セキュリティ対策や啓発、インシデント対応等の活動を行っています。

3. 会社内における位置づけおよび活動内容

【組織内における位置づけ】
KOSEN-CSIRT は、情報セキュリティポリシーに基づき CISO が設置したチームで、全国の国立高専から選出された教職員と、高専機構本部事務局の情報担当・危機管理担当で構成しています。

【活動内容】
高専機構内で生じたインシデントに対して各国立高専等と連携して迅速に対応するとともに、注意喚起等の情報提供、情報セキュリティに関する研修や訓練、情報セキュリティ監査、他組織との情報交換等を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KTC-SIRT

チームの正式名称	KTCグループSIRT
チームの略称	KTC-SIRT
所属する組織名	株式会社ティーエムホールディングス
設立年月日	2015-01-01
チームの Email アドレス	sirt@ktc-group.net
チームサイト	
所属組織サイト	http://www.tmholdings.co.jp/
加盟年月	2016 年 04 月

1. 概要

KTC-SIRT は主に KTC グループを対象に、セキュリティインシデント対応や情報セキュリティに関する各種サポートを提供しています。KTC グループは教育事業を中心とした多種多様な事業体から成り立っています。

2. 設立の経緯・背景

KTC グループ内部からお客様に近いステージまで、近年情報セキュリティインシデントが多発しています。事業の多様化もあり、脅威自体も多様化しているため、グループで一貫して迅速に対応できる体制として株式会社ティーエムホールディングス内に KTC-SIRT を設立することになりました。

3. 会社内における位置づけおよび活動内容

システム部門が中心となり、広報、お客様相談室、監査、法務、マーケティング部門からメインメンバーを集めました。またグループ内の各事業部門から 1 名以上をサブメンバーとして集め、活動しています。緊急のインシデントに迅速に対応するため、一定の予算と、グループ内での指示権限を持っています。
個人情報、または社内の重要情報が漏えい、改竄、または、削除された (可能性が高い)、もしくは、お客様へのサービスが継続提供困難になった、もしくは、システムやサービスが回復困難になった、場合にチームが対応するというのが基本姿勢です。今後、インシデント対応をグループ内各部門のサブメンバーで完結できるよう、社内教育に一層力を入れていく予定です。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Kubota-CSIRT

チームの正式名称	Kubota Computer Security Incident Response Team
チームの略称	Kubota-CSIRT
所属する組織名	株式会社クボタ
設立年月日	2018年1月1日
チームの Email アドレス	kubota-csirt@kubota.com
チームサイト	
所属組織サイト	https://www.kubota.co.jp/
加盟年月	2018 年 02 月

1. 概要

Kubota-CSIRTは、クボタグループ内の主にコンピュータ・セキュリティ事故・事件に関するインシデント対応等を担う、株式会社クボタ内の関係部署で構成する組織横断的なCSIRTです。

2. 設立の経緯・背景

株式会社クボタは、これまでも全社情報セキュリティ主管部門を中心に、お客様をはじめとするステークホルダーの皆様の個人情報も含め、各種情報資産を適切に保護するために、技術的対策だけでなく、従業員の教育等も含め、様々な情報セキュリティ対策に取り組んできました。
しかしながら、サイバー攻撃が高度化・巧妙化している中、情報セキュリティ事故・事件を完全に防ぐことが困難な状況になりつつあります。
情報セキュリティ事故・事件に関し、より迅速に情報や異常を把握・共有するとともに、対策を実施し被害を最小化するため、Kubota-CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

Kubota-CSIRTは、社内に設置されている全社リスク管理委員会の下部組織として位置づけられ、全社情報セキュリティ主管部門を中心に、株式会社クボタ内の関係部署で構成する組織横断的なCSIRTです。
以下の活動を通じ、クボタグループにおける、情報セキュリティ事故・事件発生時の対応体制やプロセス等の更なる向上・改善を実現します。

・情報セキュリティ事故・事件への対応
・外部組織との連携
・脆弱性や情報セキュリティの技術動向等に関する情報収集
・社内への情報セキュリティ関連の情報発信・教育・啓蒙活動
・自社製品、サービス関連の脆弱性ハンドリング

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KYODO-CSIRT

チームの正式名称	共同通信社CSIRT
チームの略称	KYODO-CSIRT
所属する組織名	一般社団法人共同通信社
設立年月日	2013年9月1日
チームの Email アドレス	sys.soc@kyodonews.jp
チームサイト	
所属組織サイト	http://www.kyodonews.jp/
加盟年月	2016 年 07 月

1. 概要

日本全国の加盟新聞社、契約放送局、デジタルサービス向けにニュースを取材、編集、配信する一般社団法人共同通信社のICTと情報セキュリティーを守る組織です。グループ企業の情報セキュリティーも担当しています。

2. 設立の経緯・背景

2013年秋にある重大インシデントが発生して、その調査と対策のためにCSIRTを発足させました。日常の監視、インシデント・ハンドリング、外部セキュリティー団体との情報交換を受け持つ組織として活動しています。

3. 会社内における位置づけおよび活動内容

情報技術局オペレーショングループセキュリティーチームが専任でCSIRTの役割を担っています。また、兼務者の組織として、コンピューターセキュリティー対策チームのメンバーもこれを手伝う形で組織しています。上位組織として情報セキュリティー委員会を設け、その配下で活動、定期的な報告をしています。ファイアウォール監視、ログ解析、デジタルフォレンジック、インシデント・ハンドリング、セキュリティー教育などを行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KNT-CT CSIRT

チームの正式名称	KNT-CT CSIRT
チームの略称	KNT-CT CSIRT
所属する組織名	KNT-CTホールディングス株式会社
設立年月日	2017年8月1日
チームの Email アドレス	info-security@kntcthd.co.jp
チームサイト	
所属組織サイト	http://www.kntcthd.co.jp/
加盟年月	2018 年 02 月

1. 概要

KNT−CTホールディングスは、近畿日本ツーリスト各社、クラブツーリズムなど、グループ会社30社余りから成り立っており、旅を通じ世界中の人々に、夢と感動を届けられるようチャレンジしています。また、旅行業の他にも、人材派遣業務、イベント&コンベンション企画など、さまざまな事業を手がけています。

KNT-CT CSIRTは、グループ各社より選出されたメンバーが、情報セキュリティ強化推進のため、部門の枠を超えて活動しています。定期的にグループ内にてセキュリティ動向を共有し、各社内にて啓発に努めるほか、緊急事態に備え、連携強化に取り組んでいます。

2. 設立の経緯・背景

従来より、情報セキュリティ推進を実施していましたが、近年の巧妙化するサイバー攻撃の脅威に備えるべく、インシデントに迅速に対応するための組織強化に取り組みました。その一環として、2017年に立ち上げられたのが、KNT-CT CSIRTです。

さまざまな形で世界とつながる当社グループにおいて、常日頃からの情報セキュリティ強化と、万が一の際の迅速な対応を目指しています。

3. 会社内における位置づけおよび活動内容

1.位置づけ
KNT-CT CSIRT は、KNT−CTホールディングス・情報セキュリティ対策室が中心となり、当社グループのセキュリティ維持向上に取り組んでいます。

2.活動内容
主な活動内容は下記の通りです。
・サイバー攻撃及び脆弱性情報の収集と対策指示
・システムのセキュリティリスク分析
・セキュリティ教育及びインシデント対応訓練の計画立案と実施
・インシデント発生時の対応支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

LACERT

チームの正式名称	LAC Advanced Corporate Emergency Readiness Team
チームの略称	LACERT
所属する組織名	株式会社ラック
設立年月日	2003-04-07
チームの Email アドレス	lacert@lac.co.jp
チームサイト	
所属組織サイト	http://www.lac.co.jp/
加盟年月	2007 年 08 月

1. 概要

株式会社ラックでは、セキュリティ監視センターにおけるインシデント対応チームが、以前より当社の顧客および連携する企業へ、セキュリティ情報の提供やインシデント対応支援、復旧支援など、インシデントレスポンス機能を提供しています。LACERTは、当社におけるセキュリティ対策ならびにインシデント対応強化を目的に、セキュリティ監視センター含めた各事業部門と連携する仮想チームとして設置され、事後の対応のみならず、社内外の連絡窓口、セキュリティ関連情報等の収集とナレッジ共有などの活動を行っております。

2. 設立の経緯・背景

2000 年にセキュリティ監視センターが設立されて以降、さまざまなセキュリティインシデントの発生を検知できるようになりました。これに伴い、顧客へのインシデントに関連する情報提供や対応支援、対策アドバイス等を行う必要性も高まってきたことから、同センター内にインシデント対応チームを組織しました。2003 年 4 月には CSIRT の国際的コミュニティである FIRST に加盟、複雑かつ巧妙化するセキュリティインシデントに対応すべく、他組織との情報共有や連携を強化しています。
更に、2016年8月、当社におけるインシデント対応機能強化を目的に組織内CSIRTを仮想チームとして設置。2018年にはCSIRTの対象拡大に伴い、名称を「LACERT」に改称し、国内外の関連組織等との情報共有や連携を強化しています。

3. 会社内における位置づけおよび活動内容

チーム発足当初の目的は、セキュリティ監視センター内で発生したインシデントの対応支援や顧客への情報提供を行うことにありました。昨今のインシデントの発生頻度の高まりにより、現在ではサイバー攻撃や情報漏えいなどの緊急事態が発生した顧客からの直接相談・依頼の件数も年々増加傾向にあり、現在においては既存顧客への支援に限らず、緊急対応窓口に相談のあった社内外のセキュリティインシデントやセキュリティ関連情報の収集、社内外との情報連携などの事前対応についても活動範囲としています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

LINE-CSIRT

チームの正式名称	LINE コンピュータセキュリティインシデント対応チーム
チームの略称	LINE-CSIRT
所属する組織名	LINE株式会社
設立年月日	2013-04-01
チームの Email アドレス	dl_line-csirt@linecorp.com
チームサイト	
所属組織サイト	http://linecorp.com/
加盟年月	2013 年 04 月

1. 概要

LINE-CSIRT はコミュニケーションアプリ「LINE」をはじめ、キュレーションプラットフォーム「NAVERまとめ」、総合ポータルサイト「livedoor」等を展開している LINE 株式会社のインシデントレスポンスチームです。

2. 設立の経緯・背景

セキュリティ組織を中心とした CSIRT 機能は従来より存在していましたが、提供サービスの多様化、国際化、利害関係者の増加や脅威の巧妙化等、複雑化するインシデントリスクへの更なる高度化された対応を図る為、あらためて LINE-CSIRT として組織化しています。

3. 会社内における位置づけおよび活動内容

LINE-CSIRT は LINE 株式会社のみならず子会社を含め、グループ横断的にセキュリティインシデントの予防及び対応を実施するために構築された組織です。
　平時はコアメンバーである CISO 直下のセキュリティ組織により、サービス上の個人情報保護、セキュリティイベントの監視や従業員教育、脆弱性検証やポリシーの整備・見直し等、インシデントの予防活動を実施しています。
　インシデント発生時にはセキュリティ組織のほか、法務、政策、広報、カスタマーサポート、技術、インフラ部門等、部署間を横断し、対応および再発防止等の必要な措置を行います。

　世界中で利用者が増加する中、インシデントの発生はその程度や内容により社会や顧客への影響が避けられないことから、LINE-CSIRT の適切な運営は企業の社会的責任の一環と認識しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

LIXIL-CSIRT

チームの正式名称	LIXIL-CSIRT
チームの略称	LIXIL-CSIRT
所属する組織名	株式会社LIXIL
設立年月日	2017年4月1日
チームの Email アドレス	lixil-csirt@lixil.com
チームサイト	
所属組織サイト	http://www.lixil.com
加盟年月	2017 年 12 月

1. 概要

LIXILグループは、戸建住宅・マンションからオフィス・商業施設などの非住宅向けまで、多岐にわたる建材・設備機器と幅広い住関連サービスを提供するグローバル企業です。
LIXIL-CSIRTは、LIXILグループ会社の株式会社LIXILにて運営され、LIXILグループ全体の情報セキュリティへの取り組みを推進しています。

2. 設立の経緯・背景

サイバー攻撃が巧妙かつ複雑になってきた現在、100％防御するという守りのセキュリティ戦略では難しくなってきています。そこで侵入されることを前提にした攻めのセキュリティ戦略が必要と判断して検知から復旧までのインシデントハンドリングを早く判断して実施するための組織として「LIXIL-CSIRT」を2017年4月に設立しました。

3. 会社内における位置づけおよび活動内容

LIXIL-CSIRTは、株式会社LIXILの情報セキュリティ部メンバーを中心に以下の活動を行なっています。

・ガバナンス設計
　-セキュリティ戦略/計画、規程の策定
　-人材採用・教育計画を実施
　- セキュリティ委員会/セキュリティ分科会 の運営
・リスクアセスメント
　-規程および仕組み(システム)を用いたセキュリティ監査の実施
　- 情報セキュリティ規定/細則/要領 の作成
　- セキュリティに関わる問合せ対応
・管理策設計/導入
　-セキュリティ戦略/計画に基づく仕組み(システム)導入企画および導入/展開
・CSIRT業務
　-脆弱性情報収集、情報共有
　- インシデントハンドリング (受付、トリアージ、封じ込め、分析、対処、報告)
　- セキュリティインシデント対応訓練の企画、実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

KU - CSIRT

チームの正式名称	工学院大学情報セキュリティインシデント対応チーム
チームの略称	KU - CSIRT
所属する組織名	学校法人　工学院大学
設立年月日	2016年4月1日
チームの Email アドレス	poc@kogakuin.ac.jp
チームサイト	
所属組織サイト	http://www.kogakuin.ac.jp/
加盟年月	2017 年 07 月

1. 概要

KU - CSIRTは、学校法人工学院大学 (http://www.kogakuin.ac.jp/) が運営しているCSIRTです。

学校法人工学院大学（以下、「学園」という。）は、大学4学部、大学院1研究科、附属中学校・高等学校、学生数約6,500名、生徒数約1,200名、教職員数約400名、2キャンパス（東京都新宿区・八王子市）からなる工学教育の歴史と伝統を誇る学園（1887年・明治20年創立）です。「無限の可能性が開花する学園」を理念とし、建学の「社会・産業と最先端の学問を幅広くつなぐ「工」の精神」を基本に据え、「誠実、挑戦、行動、絆」のバリューに基づく、K-Mind（教育：自立した人間の育成、研究：研究を通じた教育、社会貢献：未来を創る仕組みと人材の輩出）というミッションの実践により、「多様で複雑な世の中と学問を教育で「つなぐ」ネットワークの中枢へ」というビジョンの実現を掲げています。

2. 設立の経緯・背景

学園の建学の精神を継承・発展させ、高度に情報化する社会における教育機関としての使命を果たし続けていくためには、コンピュータやネットワークなどで構成される情報処理環境を安全に運用管理し、それらを活用して重要情報を安全かつ的確に取り扱う組織能力を確保することが不可欠です。情報通信技術の進展が早く、サイバー攻撃に代表される情報セキュリティの脅威が激しく変化する中でこのような組織能力を確保していくには、学園の構成員全員が組織的に統制のとれた対応方法を身に着けるとともに、環境の変化に応じて対応策を見直していかなければなりません。

情報セキュリティの確保に向けて、学園の構成員全員が立場に応じた役割を担うことを明確にし、統一したルールで情報セキュリティリスクを未然に防ぎ、やむを得ず情報セキュリティインシデントが発生した場合の損害を最小に抑え、セキュリティ対策を環境に合わせて改善していく、などを核とするセキュリティ確保の組織能力を高めていくことを目的として、「学校法人工学院大学　情報セキュリティポリシー」（http://www.kogakuin.ac.jp/about/compliance/infopolicy/）改正（2016年4月1日）を機に、やむを得ず発生した情報セキュリティインシデント対応を行うチームとして、「KU - CSIRT」を構築しました。

3. 会社内における位置づけおよび活動内容

(1) 位置づけ
KU - CSIRTは、学校法人工学院大学情報セキュリティポリシーで規定された部署横断的なチームで、法人組織の情報システム部員（責任者、担当者）、法務、財務、広報担当等で構成され、CISO（情報担当常務理事）と密に連携し、学校法人及び全ての設置校（大学・大学院、附属中学・高等学校）を対象としています。
学園の情報セキュリティ施策は、CISO、学長、校長、総務・人事部長、情報システム部長からなる学園情報セキュリティ委員会で取り扱い、職制による推進体制を築いています。

(2) 主な活動内容
・情報セキュリティインシデントハンドリング
・情報セキュリティインシデント／情報セキュリティ事象検知
・情報セキュリティインシデント報告（月報）
・情報セキュリティ教育／啓発活動
・外部機関等（公的機関、他大学、各種団体、各PoC等）との情報交換

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

M-CSIRT

チームの正式名称	Marubeni IT Solutions Computer Security Incident Response Team
チームの略称	M-CSIRT
所属する組織名	丸紅ITソリューションズ株式会社
設立年月日	2015-08-01
チームの Email アドレス	csirt@marubeni-itsol.com
チームサイト	
所属組織サイト	http://www.marubeni-itsol.com/
加盟年月	2015 年 12 月

1. 概要

M-CSIRT は丸紅ITソリューションズ株式会社によって運営されている CSIRT です。

丸紅ITソリューションズ株式会社は、丸紅グループの IT 企業として商社・流通をはじめとする多様な業界・業務知見を活用してお客様の課題を「発見」し、分析した課題に対して最先端の IT 技術とクラウドを駆使した最適システムを「構成」、さらにシステムの提供を高品質の運用と共に確実に「実行」することで、「IT によるビジネスの革新」という使命を果たしていきます。

2. 設立の経緯・背景

近年のサイバー攻撃の高度化による脅威は更に高まっています。多様化・複雑化する攻撃に対応するためには、セキュリティ脅威に対する防御だけでなく、検知、対処、対策を一元的に実施する体制の構築が必要であり、従来の縦割り組織で個々にセキュリティに対応するのではなく、独立した専門部署設置の必要性を認識し、M-CSIRT を設立しました。

3. 会社内における位置づけおよび活動内容

M-CSIRT は丸紅ITソリューションズ株式会社の基盤インフラを担当する部署内に設置され、専任メンバーと他組織に所属するセキュリティ対応要員から構成されています。
当チームは顧客および自社に対し、情報セキュリティに関する窓口機能を提供し、外部組織および専門ベンダーと連携・協業し、セキュリティインシデントの検知、解決、被害の局所化、および発生の予防を支援する活動をしています。
主な活動内容は以下の通りです。
・インシデントに関する情報収集機能
・インシデントに関する対応窓口機能
・セキュリティに関するお問い合わせ窓口機能
・セキュリティに関する施策 / ガイドライン策定、および教育啓蒙

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Macnica-CIRT

チームの正式名称	マクニカ　サイバーインシデント対応チーム
チームの略称	Macnica-CIRT
所属する組織名	マクニカネットワークス株式会社
設立年月日	2013年4月1日
チームの Email アドレス	mcirt@macnica.co.jp
チームサイト	
所属組織サイト	http://www.macnica.net/contents/contactus.html/
加盟年月	2016 年 07 月

1. 概要

株式会社マクニカは、半導体・集積回路などの電子部品の輸出入、販売、開発、加工などを行う技術商社です。マクニカネットワークス株式会社は、マクニカグループの一員として、セキュリティ製品を中心に、最先端のテクノロジーを備えた様々なネットワーク機器・ソフトウェアなどを提供する技術商社です。

2. 設立の経緯・背景

ハイテク産業を狙った高度な標的型攻撃による脅威の高まりを受け、マクニカグループでも重要な課題と認識され、技術的な対応能力の向上を目的として設立されました。

3. 会社内における位置づけおよび活動内容

Macnica-CIRTは、マクニグループ内のセキュリティインシデントの分析やハンドリングを行うCIRTで、マクニカ株式会社本社システム部門と、マクニカネットワークス内のセキュリティ関連部署からなる横断組織です。社内システムと脅威に関する知見と専門性を共有、メンバーの能力を最大限発揮することを重視し、防御、検知、事後対応、そして予測に至るまでをスコープとしています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MB-SIRT

チームの正式名称	森ビル株式会社セキュリティインシデントレスポンスチーム
チームの略称	MB-SIRT
所属する組織名	森ビル株式会社
設立年月日	2012-04-01
チームの Email アドレス	mb-sirt@mori.co.jp
チームサイト	
所属組織サイト	http://www.mori.co.jp
加盟年月	2015 年 04 月

1. 概要

MB-SIRT は森ビル株式会社内の関連部署で構成されるセキュリティインシデントレスポンスチームです。

2. 設立の経緯・背景

昨今巧妙化・複雑化、深刻な被害が報告されているサイバー攻撃や不正アクセスに対しては、高度かつ迅速な対応が求められています。
このような脅威に対抗、セキュリティ対策を強化するためには、他社の取り組み状況、外部関連機関から発信される情報の共有が不可欠な要素です。
当社では、あるセキュリティ事故をきっかけに、JPCERT/CC 殿より日本シーサート協議会への加盟のアドバイスをいただき、社内に SIRT 設立を計画するに至りました。

3. 会社内における位置づけおよび活動内容

MB-SIRT は、情報システム部門を中心とした情報セキュリティを担当するメンバーによって構成されるチームです。
発生したセキュリティインシデントに応じて、リスク管理部門とともに対応にあたります。

主な活動内容は次の二点です。
1. セキュリティインシデント未然防止活動
1.サイバー攻撃・脆弱性情報の収集・診断
2.セキュリティルール・規程の整備
3.セキュリティレベル向上のための施策の検討・実施
4.従業者への研修・啓蒙
5.セキュリティに関する社内外への情報発信・相談窓口
2. セキュリティインシデント発生時対応
1.発生時における技術対応及び指示・助言、並びに被害最小化のための施策検討及び実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Kyutech CSIRT

チームの正式名称	九州工業大学　情報基盤運用室
チームの略称	Kyutech CSIRT
所属する組織名	国立大学法人　九州工業大学
設立年月日	2013年4月1日
チームの Email アドレス	contact@kiban.kyutech.ac.jp
チームサイト	http://www.kiban.kyutech.ac.jp/csirt/
所属組織サイト	http://www.kyutech.ac.jp/
加盟年月	2018 年 01 月

1. 概要

九州工業大学の前身は、1907 年に創設された私立明治専門学校です。明治専門学校は、1949年に国立九州工業大学となり、2004年から国立大学法人九州工業大学となりました。この間に、飯塚市に情報工学部が設置され、今年度30年目を迎え、若松の北九州学術研究都市に大学院生命体工学研究科が16年前に設置され、2学部3学府・研究科、学生数約5800名を擁する、わが国有数の個性豊かな工学系大学となり、現在に至っています。九州工業大学の理念は、「技術に堪能なる士君子の養成」という本学の基本方針として、100年以上の歴史を越えて脈々と伝えられ、現在に至っています。

2. 設立の経緯・背景

前身である九州工業大学全学情報基盤室が2006年に設置され、情報セキュリティインシデントが発生した際の緊急対応、調査等の事後対応、ファイアーウォールの維持・管理等の対応に当たってきた。2013年に全学の情報ネットワークの一体的運用、情報セキュリティ対策強化を目的に全学情報基盤室が発展的に改組し、情報基盤機構　情報基盤運用室となった。情報基盤運用室が実質的なCSIRT業務を行い安心、安全な九州工業大学のネットワーク環境の構築、維持、運営に取り組んでいます。

3. 会社内における位置づけおよび活動内容

主な業務は以下の通りです。
- 学外ネットワークへの接続及び学内情報ネットワーク並びにそれらを構成する機器等の運用管理に関すること。
- 学内情報ネットワークに係る資源割当及びサブネットワークの申請等に関すること。
- 学内サブネットワークの技術支援に関すること。
- 情報セキュリティの確保及び情報セキュリティ・インシデント対応に関すること。
- 情報セキュリティ・インシデントの発生時に初動対応として行う学内情報ネットワーク接続からの強制的な遮断に関すること。
- 情報機器のデジタル・フォレンジック（物理的なアクセス、持ち帰り、証拠保全、調査及び個人情報を含むログの解析等）の運用管理に関すること。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MBK-CSI

チームの正式名称	三井物産株式会社IT推進部サイバーセキュリティ対策室
チームの略称	MBK-CSI
所属する組織名	三井物産株式会社
設立年月日	2015-04-01
チームの Email アドレス	MBK-CSiTKACS@mitsui.com
チームサイト	
所属組織サイト	https://www.mitsui.com/jp/ja/security/contact/index.html
加盟年月	2016 年 01 月

1. 概要

三井物産は、総合商社として世界中の情報、発想、技術、資源、国をつなぎ、あらゆるビジネスを革新します。

2. 設立の経緯・背景

従来よりサイバーセキュリティ対策は推進して参りましたが、近年高まるサイバーリスクに対応する為、また三井物産グループ全体のサイバーセキュリティ対応力向上を目的として、独立した組織として 2015 年 4 月に設立致しました。

3. 会社内における位置づけおよび活動内容

三井物産本体及び三井物産関係会社を含めたサイバーセキュリティの要として、下記業務の実施を行う。
・サイバーセキュリティ啓発活動
・サイバーセキュリティ情報収集
・インシデント発生時対応

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MBSD-SIRT

チームの正式名称	Mitsui Bussan Secure Directions,Inc. Security Incident Response Team
チームの略称	MBSD-SIRT
所属する組織名	三井物産セキュアディレクション株式会社
設立年月日	2011-02-16
チームの Email アドレス	SIRT-ml@mbsd.jp
チームサイト	
所属組織サイト	http://www.mbsd.jp/
加盟年月	2011 年 02 月

1. 概要

MBSD-SIRT は、三井物産セキュアディレクション株式会社 (MBSD) 内に設立され、運営されている CSIRT です。
MBSD は、21 世紀の新しい IT リスクマネジメント・ニーズに対応するため 2001 年に設立され、以来、情報漏えい調査、脆弱性診断、不正アクセス監視、セキュリティ教育、情報セキュリティコンサルティングなどネットワークセキュリティサービスを専門とし、お客様を「安心」へと導くサイバーセキュリティ専門事業者です。

2. 設立の経緯・背景

MBSD-SIRT は、本業である情報セキュリティ専門会社として知り得たインシデント情報ならびに各種ノウハウを社内の部門間で共有し、お客様に提供する各種サービスに対し迅速に反映させるとともに、国内外のインシデント関連団体に対し情報連携及び支援を行うために設立しました。

3. 会社内における位置づけおよび活動内容

MBSD-SIRT は、自社ネットワークに対するインシデント対応以外に、各種セキュリティサービスをご契約いただいているお客様に「安心」をお届けしている情報セキュリティ専門会社として、日々インシデント情報の収集と発信を続けていることが特徴です。

チームメンバーは社内から選抜された優秀なエンジニアと、各種情報の調査・研究を行なっているスタッフから構成されています。また、MBSD-SOC (セキュリティ・オペレーション・センター) で知り得た外部攻撃の傾向や、社内エンジニアが発見したアプリケーション脆弱性の傾向などを集計し、レポートを作成しています。このレポートについては、社外公開も検討中です。

MBSD-SIRT は、サイバーセキュリティのプロフェッショナルとしての専門知識の深化と、日本シーサート協議会等の国内外のインシデント関連団体との連携を通じ、安心と安全を守るためセキュリティインシデントへの対応力強化に日々活動しております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MC-SIRT

チームの正式名称	Mitsui Chemicals Computer Security Incident Response Team
チームの略称	MC-SIRT
所属する組織名	三井化学株式会社
設立年月日	2015-04-01
チームの Email アドレス	MCSIRT@mitsuichemicals.com
チームサイト	
所属組織サイト	http://jp.mitsuichem.com/
加盟年月	2016 年 02 月加盟

1. 概要

三井化学 CSIRT は、社内でのセキュリティインシデントが社内・顧客・社会へ影響を及ぼすことがないよう、システム部門によって管理された、社内およびグループの IT セキュリティおよび 情報セキュリティに関するインシデント・ハンドリングのチームです。

2. 設立の経緯・背景

弊社は、社内情報および営業秘密をはじめとする情報資産に対するセキュリティ向上のため、様々な対策を講じてきました。
情報系システムに対するセキュリティ対策だけではなく、工場等の制御系システムへの対応も含め、近年高度化しているサイバー攻撃、不正アクセスへの対応や、情報漏えい発生時の対応の迅速化が求められています。
こうした状況を踏まえ、セキュリティインシデントが発生した場合に、迅速に対応し、影響範囲・被害の拡大防止や、サービスの早期復旧を実現できるよう、2014年にCSIRT設立を計画しました。

3. 会社内における位置づけおよび活動内容

IT 部門を中心とし、外部連携を図るための総務・広報部門、制御系に関する連携を図るためのエンジニアリング部門も参画します。まずは、従来からのシステム部門によるセキュリティ対応からスタートしますが、社内に限らず、三井化学グループにおける情報セキュリティインシデントに関する情報共有・対応を進めることとします。

主な活動内容
1. インシデントの未然防止活動
・リスク情報の収集
・定期的な社内点検
・社内体制やルール、教育、システム対策等の継続的な改善
2. インシデント対応
・発生時から解決までの一連の処理
(連絡受付、対応要否判断、分析、復旧、再発防止、報告など)

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MCDP-CSIRT

チームの正式名称	MC Data Plus Computer Security Incident Response Team
チームの略称	MCDP-CSIRT
所属する組織名	株式会社　MCデータプラス
設立年月日	2017年4月1日
チームの Email アドレス	ml.mcdp-csirt@mcdata.co.jp
チームサイト	
所属組織サイト	http://www.mcdata.co.jp/
加盟年月	2017 年 09 月

1. 概要

当社は建設業特化のクラウドサービス「建設サイト」「グリーンサイト」事業と、企業データのビジネス活用事業、特に当社は三菱商事グループの一員として、データ活用が進むリテイル分野・ヘルスケア分野等における取組みを中心とした事業展開を行っています。

2. 設立の経緯・背景

弊社は設立時からセキュリティ部門を立ち上げ、情報セキュリティリスクに対応してきたが、会社規模の拡大、サービスの増加に伴い、セキュリティリスクも増大していることから、更なるセキュリティリスクに対応する体制を構築する必要性を認識し、MCDP-CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

株式会社MCデータプラス内にMCDP-CSIRTを設置しており、ISMS事務局と併設しています。

MCDP-CSIRTでは弊社の運用するサービスで発生したセキュリティインシデントを迅速な解決するための体制を構築しています。
また、平時は日常的な社内セキュリティ教育、社内への情報提供、親会社からのソフトウェア脆弱性情報共有等を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MELCO-CSIRT

チームの正式名称	Mitsubishi Electric Corporation Computer Security Incident Response Team
チームの略称	MELCO-CSIRT
所属する組織名	三菱電機株式会社
設立年月日	2012-10-01
チームの Email アドレス	melco-csirt@mj.MitsubishiElectric.cc
チームサイト	
所属組織サイト	http://www.mitsubishielectric.co.jp/
加盟年月	2015 年 11 月

1. 概要

三菱電機グループシーサートは、三菱電機株式会社及び国内外関係会社を対象範囲として、Web サイトの閲覧やメールの送受信等により発生するセキュリティインシデントへの対応とりまとめ、発生したインシデント関係部門の技術支援、シーサート協議会を含む外部機関を通した情報収集・共有、他の外部機関との連携、及び三菱電機グループ社員への情報セキュリティ教育を行う組織です。

2. 設立の経緯・背景

世の中の標的型サイバー攻撃による被害の増加を鑑みて、JCSIP 重要インフラ製造業における重要な情報を扱う企業への高度化しているサイバー攻撃への対応強化の一環として、CSIRT 体制を構築し、2012 年に CSIRT を設立いたしました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
三菱電機本社 IT 管理部門の 1 つである IT ガバナンス方針の企画・立案・推進部門内に、専任のメンバーで CSIRT を構成しています。

(2)活動内容
・情報セキュリティシステム施策の企画・展開
・外部機関に対する窓口
・インターネット出入口におけるサイバー攻撃の監視
・三菱電機グループで発生するセキュリティインシデントの対処とりまとめ
・予防的な対策の整備

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MES-SIRT

チームの正式名称	三井E&Sシーサート
チームの略称	MES-SIRT
所属する組織名	株式会社三井E&Sホールディングス
設立年月日	2016年5月1日
チームの Email アドレス	mes-sirt@mes.co.jp
チームサイト	
所属組織サイト	http://www.mes.co.jp/
加盟年月	2016 年 09 月

1. 概要

三井E&S（旧三井造船）は、1917年の創業以来、「社会に人に信頼される　ものづくり企業であり続けます」　を企業理念とし、船舶・海洋事業、機械・システム事業、エンジニアリング事業など幅広い分野で、社会や人に役立つ製品・プラントを提供する会社です。
三井E&Sシーサート（MES-SIRT）は、三井E&SグループのCSIRTです。株式会社三井E&Sホールディングスおよび国内外の子会社・関連会社を対象範囲とし、セキュリティインシデントへの早期解決を計ります。

2. 設立の経緯・背景

当社グループは情報資産をセキュリティの脅威から守るため、今まで情報システム部門を中心に様々な対策を講じてきました。
また、近年の高度化・多様化するサイバー攻撃に迅速・適切に対応するには、外部組織との良好な関係構築、情報収集、予防対策実施、社内教育・訓練など、平常時からの組織化された活動が重要になってきました。
そのような状況を踏まえ、組織対応力強化の一環として、2016年5月に三井E&Sシーサート（MES-SIRT）を設立しました。

3. 会社内における位置づけおよび活動内容

（1）会社内の位置付け
　三井E&Sグループで発生したセキュリティインシデントに対応するため、代表取締役を責任者に、経営企画、情報セキュリティ室、総務、広報、IT部署、インシデント対応部署で構成される組織です。

（2）活動内容
　インシデント発生時は、情報セキュリティ室を事務局として、外部組織連携および社内横断的な情報収集・意思決定を行います。
　なお、通常時のセキュリティ情報の収集、予防策の実施、注意喚起・啓蒙、教育・訓練、各種ログ監視等については、情報セキュリティ室及び当社のセキュリティ・オペレーション・センター（SOC）にて日々運用しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Met-CIRT

チームの正式名称	メットライフ生命 サイバーインシデントレスポンスチーム
チームの略称	Met-CIRT
所属する組織名	メットライフ生命保険株式会社
設立年月日	2013-10-01
チームの Email アドレス	Met-CIRT@metlife.co.jp
チームサイト	
所属組織サイト	http://www.metlife.co.jp/
加盟年月	2013 年 11 月

1. 概要

Met-CIRT はメットライフ生命保険株式会社によって運営されている CSIRT です。
　メットライフ生命は、多様な販売チャネルを通して、個人・法人のお客様に革新的かつ幅広いリスクに対応できる生命保険商品を提供しております。

2. 設立の経緯・背景

サイバー攻撃発生の防止、及び発生時の対応をすみやかに行うことを目的として設立されました。
　昨今の高度化するサイバー攻撃に対し、より確実に対応するため、他社や外部機関との情報連携を目的とし、日本シーサート協議会に加盟いたしました。

3. 会社内における位置づけおよび活動内容

(1)位置付け
Met-CIRT はメットライフ生命のシステムリスク管理部門によって組織されています。
(2)活動内容
Met-CIRT は主に以下の活動を実施しています。
・サイバー攻撃に関する管理プロセスおよび手順の整備と改善
・サイバー攻撃発生時における対応のハンドリング
・サイバー攻撃に関する外部関連機関との情報窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MF-CSIRT

チームの正式名称	Money Forward Cyber Security Incident Response Team
チームの略称	MF-CSIRT
所属する組織名	株式会社マネーフォワード
設立年月日	2016年5月18日
チームの Email アドレス	mf-csirt@moneyforward.co.jp
チームサイト	
所属組織サイト	https://corp.moneyforward.com/
加盟年月	2016 年 09 月

1. 概要

MF-CSIRTは、株式会社マネーフォワード組織内のCSIRTです。

株式会社マネーフォワードは、自動家計簿・資産管理サービス「マネーフォワード」と、中小企業・個人事業主のバックオフィスをサポートするクラウドサービス「MFクラウドシリーズ」（会計、請求書、給与、経費、マイナンバー等）を提供しています。

2. 設立の経緯・背景

会社設立当初よりセキュリティ対応を行うチーム・担当は存在していましたが、社内外に対して連絡窓口の明確化、およびセキュリティインシデントに組織として高度化された対応するため、あらためてMF-CSIRTとして組織化しました。

3. 会社内における位置づけおよび活動内容

MF-CSIRTは、セキュリティインシデントの予防・事前準備・早期発見・対応最適化を推進することを目的とし、セキュリティリテラシーの啓蒙、脆弱性対応、インシデント対応時の事前準備、異常監視、インシデントレスポンスを行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MI-CSIRT

チームの正式名称	Mitsukoshi Isetan Computer Security Incident Response Team
チームの略称	MI-CSIRT
所属する組織名	株式会社　三越伊勢丹システム・ソリューションズ
設立年月日	2014-04-01
チームの Email アドレス	security-group@ims-sol.co.jp
チームサイト	
所属組織サイト	http://www.ims-sol.co.jp/
加盟年月	2014 年 08 月

1. 概要

MI-CSIRTは株式会社三越伊勢丹システム・ソリューションズによって運営されている CSIRT です。
　株式会社三越伊勢丹システム・ソリューションズは三越伊勢丹グループの IT 機能を集約したグループの情報戦略を担う企業です。

2. 設立の経緯・背景

2013 年 10 月に三越伊勢丹グループとして CSIRT 構築を目的にサイバーリスク対策 PROJ を発足し、2014 年 4 月 1 日付け組織改正にて実質的な組織として CSIRT を設置、セキュリティ専任部署として、経営管理部内に品質・リスク管理担当セキュリティ推進グループを新設いたしました。

3. 会社内における位置づけおよび活動内容

MI-CSIRT はセキュリティ推進グループのメンバーで構成されております。
　三越伊勢丹システム・ソリューションズの CSIRT は CSIRT 長である社長と関係部門責任者、セキュリティ推進グループで構成されております。
三越伊勢丹グループの顧客満足の最大化のために、三越伊勢丹グループのサイバーリスク管理体制において、危機発生時に、各部門によるインシデント対応を統括し、技術的支援、グループ内の調整、及びインシデント対応に必要な統制等を実施することで被害の局限化、及び迅速な復旧をしていきます。
■有事の活動
・インシデント分析結果に基づいてトリアージを行い、必要な対策を実施
・三越伊勢丹グループのサイバーリスク管理体制に対して、技術的観点に基づく対応策を提言
■平時の活動
・脆弱性情報のハンドリング
・セキュリティ技術動向調査
・監視情報をモニタリング (記録・調査)
・外部組織とのコミュニケーション (交流・情報交換)

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

miss-paris-CSIRT

チームの正式名称	ミス・パリグループCSIRT
チームの略称	miss-paris-CSIRT
所属する組織名	ミス・パリ・グループ
設立年月日	2018/04/01
チームの Email アドレス	miss-paris-csirt@miss-paris.com
チームサイト	
所属組織サイト	https://www.miss-paris-group.co.jp/
加盟年月	2018 年 07 月

1. 概要

「ミス・パリ・グループシーサート」は株式会社ミス・パリおよびグループ関連会社の組織内CSIRTです。
セキュリティインシデントの防止及び発生時の被害極少化を目的とする組織です。
ミス・パリ・グループは「心も体も美しく健やかな人づくり」を企業理念とし、「男のエステ ダンディハウス」,「エステティック ミス・パリ」,「Euphoria」等のエステサロンやヘアサロン、「ミスパリ エステティック専門学校」や美容業界に特化した人材派遣業務などを運営する美の総合商社です。
お客様からお預かりした大切な個人情報の保護を重要事項と捉え、最大限の努力で信頼を上げていきます。

2. 設立の経緯・背景

ミス・パリ・グループには、サロン(エステ/美容室)や専門学校を始め複数の関連法人が傘下にあります。
IT化に伴い、個人情報の管理をシステムで行う比重が増えております。
また、M&A等で関連法人も増え、管理が煩雑化しております。
個人情報を提供したお客様や社員が安心できる体制を構築するために、ミス・パリグループ各社を横断する共通的な組織として2018年4月に発足しました。

3. 会社内における位置づけおよび活動内容

① 会社内における位置づけ
1)ミス・パリ・グループ各社を横断した組織です。
2)ミス・パリ・グループ内の各部署がその職掌に合わせて、ミス・パリ・グループシーサートに関わる役割を兼務で担当します。
3)品質管理のISO事務局やプライバシーマーク事務局と密に連携を取り、相互で内容の重複や矛盾が無いように運営します。

② 活動内容
1)外部との連携窓口を担い、情報の収集や発信をします。
2)インシデントの予防施策や社員への教育・啓蒙活動を行います。
3)インシデント発生時に主導的な役割を担います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

mixirt

チームの正式名称	mixi Computer Security Incident Response Team
チームの略称	mixirt
所属する組織名	株式会社ミクシィ
設立年月日	2008-02-01
チームの Email アドレス	mixirt-contact@mixi.co.jp
チームサイト	
所属組織サイト	http://mixi.co.jp/
加盟年月	2014 年 05 月

1. 概要

株式会社ミクシィをはじめとするミクシィグループは、『新しい文化を創る』をミッションに掲げ、ソーシャル・ネットワーキング サービス「mixi」、ひっぱりハンティングRPG「モンスターストライク」等の、コミュニケーションを軸にした新しい価値の提供により、新たな市場の創造に挑戦する企業グループです。
当グループにおいて、情報セキュリティ事故への対応支援を行う組織を mixirt (ミクサート) ：mixi Computer Security Incident Response Team と言います。

2. 設立の経緯・背景

mixirt (ミクサート) は、Find Job ! が DDoS 攻撃を受け2日間サービス停止となった事故をきっかけに、その体制の検討が行われ、2008 年 2 月 1 日に、情報セキュリティに関わる事故が発生した際の速やかな対応行動と被害の最小化を目的として発足しました。

3. 会社内における位置づけおよび活動内容

mixirt (ミクサート) はグループ企業をまたいだ仮想的な組織で、事業部門のセキュリティ担当者と、社内の情報システム部門を中心に、広報、法務などのコーポレート部門の担当者などから構成される、CISO直下の組織です。
特定の中心となる部門はなく、運営事務局もグループ企業内の有志により行う形をとっています。

主な活動内容は、セキュリティインシデント対応がメインであり
・各種セキュリティインシデントが発生した際のハンドリング・技術支援・コーディネーション
・各種セキュリティインシデントに関する情報共有
が主な活動内容となっています

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Miyadai-CSIRT

チームの正式名称	宮崎大学情報セキュリティインシデント対応チーム
チームの略称	Miyadai-CSIRT
所属する組織名	国立大学法人 宮崎大学
設立年月日	2017年4月1日
チームの Email アドレス	csirt@cc.miyazaki-u.ac.jp
チームサイト	http://www.cc.miyazaki-u.ac.jp/csirt.php
所属組織サイト	http://www.miyazaki-u.ac.jp
加盟年月	2018 年 03 月

1. 概要

旧宮崎大学と宮崎医科大学とは平成15年10月に統合しました。平成16年4月からは国立大学法人宮崎大学となり、「世界を視野に地域から始めよう」のスローガンのもとに歩みを続けています。平成28年4月に地域資源創成学部を新たに設置し、現在では教育学部、医学部、工学部、農学部の5学部からなる大学として機能しています。大学院には修士課程として教育学研究科、看護学研究科、工学研究科、農学研究科があります。さらに異分野融合型のユニークな研究体制として、医学獣医学総合研究科修士・博士課程、農学工学総合研究科博士課程を備えています。

2. 設立の経緯・背景

これまでは、学内で発生した情報セキュリティインシデントへの対応は情報基盤センターが担っていた。しかし、組織内での立場や権限、連絡体制などが明確にされておらず、その場その場の判断で対応していた。近年、情報セキュリティに対する脅威が高まる中で、より迅速に情報セキュリティインシデントへ対応するためには、対応者の組織化、権限の明確化、他部署との連携の整備を行う必要性があることから、本学の情報セキュリティ基本規程に定め、2017年4月に宮崎大学情報セキュリティインシデント対応チームを設置した。

3. 会社内における位置づけおよび活動内容

Miyadai-CSIRTは、学内で情報セキュリティインシデントが発生した場合、次に掲げる対応を必要に応じて行います。
(1)被害拡大の防止
(2)原因の究明
(3)解決策の検討
(4)再発防止策の検討
(5)関係者・関係部局への指示・報告
(6)その他必要な対応
また、Miyadai-CSIRTは、情報セキュリティインシデント発生時に、学内において次に掲げる権限を持ってインシデント対応にあたります。
(1)インシデントに係わる情報機器(以下「当該機器」という。)がネットワークに接続されている場合、ネットワークを遮断することができる。
(2)当該機器が稼働し続けることにより影響が拡大すると判断した場合、当該機器を停止させることができる。
(3)当該機器の管理者及び関係部局に対して、対応を指示することができる。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Mizuho-CIRT

チームの正式名称	Mizuho Cyber Incident Response Team
チームの略称	Mizuho-CIRT
所属する組織名	株式会社みずほフィナンシャルグループ
設立年月日	2012-11-01
チームの Email アドレス	cybersecurity.dm@mizuhofg.co.jp
チームサイト	
所属組織サイト	http://www.mizuho-fg.co.jp
加盟年月	2012 年 11 月

1. 概要

みずほフィナンシャルグループは、銀行持株会社として、銀行、長期信用銀行、証券専門会社、その他銀行法により子会社とすることができる会社の経営管理ならびにこれに付帯する業務を行うことを事業目的としています。

2. 設立の経緯・背景

＜みずほ＞ではバンキング等インターネットを経由したサービスを展開しているため、最新のセキュリティ対策の維持に努めてまいりましたが、標的型攻撃やバンキングを狙うトロイの木馬等従来とは異なる事案が日本でも本格的に発生し始めたことを踏まえ、2011 年 11 月にこれらサイバー攻撃に対し適切に対応していくため検討 WG を立上げ、2012 年 11 月に同攻撃を専門的に対応していくための組織としてサイバーセキュリティチームを IT 部門内に設置しました。

3. 会社内における位置づけおよび活動内容

＜みずほ＞では、お客さまに安心して金融サービスをご利用いただくとともに、金融インフラの安定稼動と持続的発展に貢献するため、サイバー攻撃への対応を経営上の最重要課題の1つと位置づけ、Mizuho-CIRTを中心に、高度なプロフェッショナル人材を配置し、外部の専門機関とも連携したインテリジェンスや先進技術を駆使し、統合SOC等による監視、ウイルス解析、多層的防御等、戦略的なレジリエンス態勢強化に着実に取り組んでいます。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MMC-CERT

チームの正式名称	Mitsubishi Motors Corporation-CERT
チームの略称	MMC-CERT
所属する組織名	三菱自動車工業株式会社
設立年月日	2015-01-01
チームの Email アドレス	mmc.cert@mitsubishi-motors.com
チームサイト	
所属組織サイト	http://www.mitsubishi-motors.co.jp/
加盟年月	2016 年 06 月

1. 概要

三菱自動車工業株式会社は、自動車及び自動車部品の製造販売を行っている会社です。

2. 設立の経緯・背景

三菱自動車では、これまでも情報セキュリティ活動により、お客様情報や営業秘密情報の保護に務めておりましたが、近年サイバー攻撃や不正アクセスの手法が巧妙化・高度化する中で、営業秘密の漏えいだけでなく、生産系制御システムや車載ITに対するリスクが高まっております。
このような状況において、サイバーセキュリティインシデントの早期警戒や迅速な事態収束等の危機管理体制強化を目的として、2015年1月1日にMMC-CERTは設立されました。

3. 会社内における位置づけおよび活動内容

MMC-CERTは、三菱自動車工業株式会社（http://www.mitsubishi-motors.co.jp/）によって運営されているCSIRTです。

＜会社内における位置づけ＞
MMC-CERTは、IT部門の要員を中心として構成するサイバーセキュリティ事象対応を専門とした常設の組織です。事象に応じて、開発部門（車載IT）や生産部門（生産制御設備）をはじめとした関係部署と連携して対処します。

＜活動内容＞
有事、平時において主として以下の活動を行っています。
1. サイバー攻撃や脆弱性情報の収集分析および情報共有
2. サイバーセキュリティインシデント発生時の対応
3. セキュリティに関する社内外への報告・相談・連携窓口
4. 社員に対する情報セキュリティ教育や啓発活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MMJ-CSIRT

チームの正式名称	MMJ-CSIRT
チームの略称	MMJ-CSIRT
所属する組織名	マスミューチュアル生命保険株式会社
設立年月日	2017 年 12 月 21 日
チームの Email アドレス	MMJ-CSIRT.info@massmutual.co.jp
チームサイト	
所属組織サイト	http://www.massmutual.co.jp/index.html
加盟年月	2018 年 06 月

1. 概要

マスミューチュアル生命保険株式会社は、シニアマーケット、法人マーケットを中心に「お客さまの目線」を第一にした商品開発に取り組んでおり、お客さまからの安心と信頼を得られる真に社会に貢献する生命保険会社を目指しております。
MMJ-CSIRT はマスミューチュアル生命保険株式会社が運営しています。
(「マスミューチュアル」はマサチューセッツ・ミューチュアル・ライフ・インシュアランス・カンパニーの登録商標です。)

2. 設立の経緯・背景

近年、セキュリティ専門チームの設立および、サイバー攻撃を想定した事業継続計画の策定、演習を行ってきましたが、サイバー演習での反省点を踏まえると共に、常に進化し続ける攻撃手法に対してインシデント発生に備えた CSIRT の構築は不可欠であるため、2017 年 12 月に社内部門横断組織としてチームを設立しました。

3. 会社内における位置づけおよび活動内容

(会社内における位置づけ)
MMJ-CSIRT は IT 部門をはじめとして複数の管理部門、業務部門でメンバーを構成しています。サイバー攻撃により最悪の状況に陥ることを予め想定し、お客様および保険代理店に対して速やかに対応をとれるよう全社を挙げた体制にしていることが MMJ-CSIRT の特徴となっています。
(活動内容)
主な活動内容は以下の通りです。
1) サイバーインシデントの予防対策
2) サイバーインシデント発生時の対応
3) サイバー攻撃対応訓練

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MNF-CSIRT

チームの正式名称	三菱原子燃料シーサート
チームの略称	MNF-CSIRT
所属する組織名	三菱原子燃料株式会社
設立年月日	2015-10-01
チームの Email アドレス	mnf-csirt@mnf.co.jp
チームサイト	
所属組織サイト	http://www.mnf.co.jp
加盟年月	2016 年 04 月

1. 概要

当社は、安全を最優先に高品質で信頼性の高い原子燃料の設計・開発、製造、販売を行っております。

2. 設立の経緯・背景

当社は、これまでも機密情報をはじめとする情報資産に対する情報セキュリティ向上のため推進・管理体制を構築し、各種の施策を講じてきました。
しかし、急速に高度化、組織化してきているサイバー攻撃などへの対応は厳しさを増しており、またインシデント発生時の迅速な対応も不可欠になっております。

この状況も踏まえ、重大な情報セキュリティインシデントが発生した際に、速やかな状況把握、初動対応を行い、被害を最小化を図り、関係先へのスムーズな連絡対応を行うことを目的に、MNF-CSIRT を構築いたしました。

3. 会社内における位置づけおよび活動内容

MNF-CSIRT は社長、情報セキュリティ担当役員のもと、情報システム部門を中心に社外関係先との連絡窓口担当部署を加えたチーム構成としております。

主な活動内容は以下の通りです。
1.情報セキュリティインシデントが発生した際の被害の最小化・極小化のための、状況の把握と、被害拡大防止のための諸対策の迅速な実施

2.社外関係先及びマスコミへの提供情報の立案と社外関係先対応窓口部門への連絡

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MOL-CSIRT

チームの正式名称	MOL-CSIRT
チームの略称	MOL-CSIRT
所属する組織名	株式会社商船三井 商船三井システムズ株式会社
設立年月日	2017年1月18日
チームの Email アドレス	mol-csirt@molgroup.com
チームサイト	
所属組織サイト	http://www.molis.co.jp/
加盟年月	2017 年 02 月

1. 概要

株式会社商船三井（以降、商船三井）は、タンカーやLNG船、コンテナ船、自動車船、客船、フェリーなど世界有数の規模を誇る船隊を有し、多様な輸送ニーズに対応する海運会社です。年々、厳しくなるグローバル競争を勝ち抜くために、商船三井のグループ子会社である商船三井システムズ株式会社（以降、商船三井システムズ）では、グループが一体となってIT利活用を推進・強化するために活動しています。

2. 設立の経緯・背景

海運業の一端を担う商船三井グループのビジネスにおいても「サイバー攻撃」による脅威が増えつつあります。このような状況下において、国内の重要インフラ事業者としての責務を全うするために、従業員一人一人の意識・リテラシーの向上、組織内の体制整備、セキュリティ対策の推進・強化をするため設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
MOL-CSIRTは商船三井システムズのITインフラ業務を運用・保守する部門のメンバーを中心に構成し、
今後は商船三井やグループ各社と、部門横断型のCSIRTにするべく拡大を計画しています。

(2)活動内容
MOL-CSIRTでは、以下の活動を通して、MOLグループのセキュリティ対策強化を行っていきます。

・インシデント発生時の一元窓口、及び、問題収束のための支援
・インシデントやシステム脆弱性情報の収集と予防措置の情報発信
・役職員へのセキュリティ意識・リテラシーの向上のための教育・啓発
・インシデントに関する外部関係企業・団体との情報連携、合同活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Monex-CSIRT

チームの正式名称	Monex-CSIRT
チームの略称	Monex-CSIRT
所属する組織名	マネックス証券株式会社 マネックスグループ株式会社
設立年月日	2015年10月6日
チームの Email アドレス	m-csirt@monex.co.jp
チームサイト	
所属組織サイト	https://www.monex.co.jp/
加盟年月	2016 年 12 月

1. 概要

マネックスグループの中核となる、オンライン証券会社です。

2. 設立の経緯・背景

「金融分野におけるサイバーセキュリティ強化に向けた取組方針について」（金融庁）、「サイバーセキュリティ経営ガイドライン」（経済産業省・（独）情報処理推進機構）に基づき、当社ではサイバーセキュリティは経営問題であると認識し、サイバーセキュリティ対策を適切に行うため、CSO（チーフセキュリティオフィサー）を委員長とするMonex-CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

1. Monex-CSIRTは、サイバー攻撃による情報漏えいやシステム障害などコンピュータセキュリティに係るインシデントを迅速に対処するだけでなく、平時からサイバー攻撃に備えた対策を決定し、実施する。

2. 守るべき情報資産を特定し、セキュリティリスクを洗い出すとともに、そのリスクへの対処に向けたロードマップを策定する。

「基本方針」
サイバー攻撃が発生した場合、被害の極小化に努める。著しく影響を及ぼすような重大事態に至らない場合であっても、業務に影響がある場合や攻撃予告等、侵害の影響がでていない場合も迅速な対応を行う。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MOTEX-CSIRT

チームの正式名称	エムオーテックスCSIRT
チームの略称	MOTEX-CSIRT
所属する組織名	エムオーテックス株式会社
設立年月日	2017/4/1
チームの Email アドレス	MO-CSIRT@motex.co.jp
チームサイト	
所属組織サイト	http://www.motex.co.jp/
加盟年月	2017 年 10 月

1. 概要

MOTEX-CSIRTはエムオーテックス株式会社内の関係部門から参加したメンバーで構成する組織横断的なCSIRTです。

2. 設立の経緯・背景

エムオーテックス株式会社は、これまでも情報システム部門を中心に社内の情報セキュリティ対策に取り組んできました。また、事業としてユーザー企業に向けてIT資産管理・内部不正対策ソリューションの開発・提供を行ってきました。

昨今の高度化・巧妙化したサイバー攻撃への対応および、自社製品、Webサイトの脆弱性、ユーザー企業への情報共有といった多岐にわたる内容に対して、より迅速に情報の把握および対策を行う為、MOTEX-CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

1）会社内における位置づけ
MOTEX-CSIRTは経営企画、情報システム、開発部門を中心とした仮想組織であり、平時は社会動向、技術動向などの収集および、啓蒙・教育活動などインシデントの予防に向けた活動を行います。

インシデント発生時には内容によってサポート、開発、広報、総務と連携しインシデントの早期対応に向けた活動を行います。

2）MOTEX-CSIRTの活動内容

・脆弱性、セキュリティに関する情報収集
・投資したセキュリティ対策の運用状況の把握、改善案の検討
・社内へのセキュリティ教育、啓蒙活動
・外部組織との連携
・自社製品、サービスの脆弱性ハンドリング

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MUFG-CERT

チームの正式名称	三菱UFJフィナンシャル・グループCERT
チームの略称	MUFG-CERT
所属する組織名	株式会社　三菱UFJフィナンシャル・グループ
設立年月日	2009-01
チームの Email アドレス	BTMU_CERT_PF@mufg.jp
チームサイト	
所属組織サイト	http://www.mufg.jp/
加盟年月	2011 年 11 月

1. 概要

MUFG-CERT は、三菱UFJフィナンシャル・グループが運営する CSIRT です。

2. 設立の経緯・背景

2009 年 1 月に三菱東京UFJ銀行内にコンピューターウイルス対策チームを組成しました。
サイバー攻撃の危険性の増大に対応し、サイバー攻撃対策を高度化するため、2011 年 10 月に BTMU-CERT を組織しました。
その後、2012 年 3 月にカバー範囲を三菱UFJフィナンシャル・グループ全体に広げ、MUFG-CERT に改称しました。

3. 会社内における位置づけおよび活動内容

MUFG-CERT は、三菱UFJフィナンシャル・グループ各社を基盤に、主に以下の活動を実施しています。
・MUFG グループ各社内でのセキュリティインシデント対応とその支援
・セキュリティモニタリング
・脆弱性情報や攻撃情報の収集・分析・展開
・セキュリティ関連団体の活動への参加と情報交換
・セキュリティ教育・研修やセキュリティ対応訓練の実施・支援
・グループ各社のセキュリティ対策向上の推進

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MUFR-CSIRT

チームの正式名称	MUフロンティアサービサーCSIRT
チームの略称	MUFR-CSIRT
所属する組織名	エム・ユー・フロンティア債権回収株式会社
設立年月日	2015年5月25日
チームの Email アドレス	Mufr_csirt@mufr.com
チームサイト	
所属組織サイト	http://www.mufr.co.jp/
加盟年月	2016 年 09 月

1. 概要

MUFR-CSIRTはエム・ユー・フロンティア債権回収株式会社が運営するCSIRTです。

エム・ユー・フロンティア債権回収株式会社は、1999年2月に施行された「債権管理回収業に関する特別措置法（いわゆるサービサー法）」に基づき設立された、三菱UFJフィナンシャル・グループ（MUFG）のサービサーです。金融機関・投資家・公共機関・事業会社などあらゆるお客様と連携し、金融アンバンドリング戦略に貢献する会社です。

2. 設立の経緯・背景

高度化するサイバー攻撃の脅威に備え、インシデント情報の収集、インシデント対応力強化を目的に2015年5月に結成されました。

3. 会社内における位置づけおよび活動内容

＜会社内における位置づけ＞
MUFR-CSIRTは、情報システム部門内においてセキュリティマネージメントを担当するチームを中心に構成されてます。
＜活動内容＞
・インシデント関連情報の収集分析
・インシデント対応手順策定
・インシデント発生時の対応方針決定、対処
・標的型攻撃に関する社内教育（不審メール訓練、ウイルス検知、e-ラーニング）

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MUL-CSIRT

チームの正式名称	三菱UFJリースCSIRT
チームの略称	MUL-CSIRT
所属する組織名	三菱UFJリース株式会社
設立年月日	2016-01-05
チームの Email アドレス	mul-csirt@lf.mufg.jp
チームサイト	
所属組織サイト	http://www.lf.mufg.jp
加盟年月	2016 年 06 月

1. 概要

MUL-CSIRTは、三菱UFJリース株式会社が運営するCSIRTです。

2. 設立の経緯・背景

「高度化するサイバー攻撃は完全に回避することはできない」という事故前提型の考えに基づき、サイバー攻撃への対応力強化の一環として、2016年1月にMUL-CSIRTを設置しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
情報セキュリティを取り扱うリスク統括部門やシステム部門などから構成される部署横断型の仮想的な組織です。
(2)活動内容
標的型メール攻撃やWEBサイトの改ざん、通信回線を介した社内へ侵入と情報の流出など、サイバー攻撃を中心とした情報セキュリティ事案の対応を行います。

- ・情報セキュリティ事故発生時の対応
- ・世の中で発生した情報セキュリティ事故に関する情報の収集と研究
- ・外部機関や他社シーサートとの情報交換
- ・セキュリティモニタリング、ソフトウェア脆弱性対策
- ・社員への教育・啓蒙、セキュリティ対応訓練
- ・三菱UFJリースグループ子会社へのセキュリティ対応支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MY-SIRT

チームの正式名称	MEIJIYASUDA Computer Security Incident Response Team
チームの略称	MY-SIRT
所属する組織名	明治安田生命保険相互会社
設立年月日	2014-10-21
チームの Email アドレス	mysirt@meijiyasuda.co.jp
チームサイト	
所属組織サイト	http://www.meijiyasuda.co.jp/support/cc/index.html
加盟年月	2015 年 03 月

1. 概要

MY-SIRT は、明治安田生命情報システム部内の関連部署で構成された CSIRT です。

2. 設立の経緯・背景

情報セキュリティに関しては、従前よりさまざまな取組みを実施してきましたが、昨今のサイバー攻撃の高度化等の状況を踏まえ、より迅速な対応と社外との情報連携のため、MY-SIRT を設置し体制整備を行いました。

3. 会社内における位置づけおよび活動内容

(1)メンバー構成
MY-SIRTは情報システム部門および情報セキュリティ担当部門で構成する仮想的なチームです。

(2)活動範囲
明治安田生命におけるサイバーセキュリティ事案への対応、およびグループ会社に対する支援を行ないます。

(3)活動内容
サイバーセキュリティ事案の未然防止と被害極小化に関する情報の収集・共有、注意喚起、対策検討、および事案発生時の対応等を行ないます。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NB-CSIRT

チームの正式名称	農林中央金庫CSIRT
チームの略称	NB-CSIRT
所属する組織名	農林中央金庫
設立年月日	2015-03-16
チームの Email アドレス	nb-csirt@nochubank.or.jp
チームサイト	
所属組織サイト	http://www.nochubank.or.jp
加盟年月	2015 年 11 月

1. 概要

農林中央金庫 CSIRT は、農林中央金庫ならびに JA バンク (農協系統)、JF マリンバンク (漁協系統) が全国で展開するシステムを対象に、サイバーセキュリティインシデントの予防、検知、対処を行うチームです。

2. 設立の経緯・背景

日本の政府機関や重要インフラ事業者を狙ったサイバー攻撃の高度化を受け、当金庫でもサイバーセキュリティの強化に向けた取り組みを行ってきました。農林中央金庫 CSIRT はその取り組みの中核として、セキュリティインシデントの検知、分析、被害の極小化、およびセキュリティインシデントの発生防止を図ることを目的として設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
農林中央金庫IT統括部内に CSIRT の事務局を担当する専任チームを設置しています。また、総合企画、総務、コンプライアンス部門等とも連携して、緊急時の対応のみならず、サイバーセキュリティ管理態勢の維持・強化についても対応しています。

(2)活動内容
・インシデントハンドリング (受付、トリアージ、封じ込め、分析、対処、報告)
・サイバーセキュリティ関連の情報収集、情報共有
・脆弱性情報の収集、対応
・サイバー攻撃対応演習の企画、実施
・組織内の啓発活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NCiSIRT

チームの正式名称	NCiSIRT
チームの略称	NCiSIRT
所属する組織名	ニュートン・コンサルティング株式会社
設立年月日	2016年7月22日
チームの Email アドレス	csirt@newton-consulting.co.jp
チームサイト	https://www.newton-consulting.co.jp/policy/csirt.html
所属組織サイト	http://www.newton-consulting.co.jp/
加盟年月	2017 年 01 月

1. 概要

NCiSIRTは、ニュートン・コンサルティング株式会社によって運営されている「CSIRT」です。
弊社は、公共団体や民間企業のリスクマネジメント全般(ERM、BCP/BCM、サイバーセキュリティ等)の範囲選定から現状分析、構築、教育、演習・訓練の全般にわたって支援しています。また、すでに対策を実施されているお客様に対してはその運用評価や改善支援も実施しています。

2. 設立の経緯・背景

当社のビジネスにおいて、機密性の高い情報を取り扱う機会は増加する一方であり、また、情報の取り扱いのみではなく、悪意のあるハクティビストの攻撃対象となる可能性も増してきました。この状況を鑑み、情報セキュリティとサイバーセキュリティ対応の仕組みを一体化させ、コンピュータセキュリティインシデントの未然防止及び発生した場合の被害の極小化をすることを目的としてCSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
　これまで独立していたITチームとISMSチームをCSIRTメンバーと位置づけ、CISOの指揮のもと、情報セキュリティとサイバーセキュリティの両方に関わる活動を行っています。

(2)活動内容
　NCiSIRT は主に以下の活動を実施しています。

【平時の活動】
・月例勉強会当社員教育
・ユーザへのセキュリティ啓蒙活動
・インシデントの発生予防

【有事の活動】
・インシデントの発生時対応
>インシデントの分類、優先度の判断と対応方法の決定
>対応体制の決定
>被害の拡大防止の実施
>外部へ連絡・調整
>社内基準に基づく外部への公表

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

MS&AD-CSIRT

チームの正式名称	MS&ADホールディングス　CSIRT
チームの略称	MS&AD-CSIRT
所属する組織名	MS&ADホールディングスインシュアランスグループホールディングス株式会社
設立年月日	2014-07-22
チームの Email アドレス	ms_ad_csirt@ms-ad-hd.com
チームサイト	
所属組織サイト	http://www.ms-ad-hd.com/
加盟年月	2014 年 11 月

1. 概要

MS&ADホールディングスの持株会社、事業会社およびシステム開発会社等の IT 部門により運営されている CSIRT です。
MS&ADホールディングスは、グローバルな保険・金融サービス事業を通じて、安心と安全を提供し、活力ある社会の発展と地球の健やかな未来を支えることを経営理念としています。

2. 設立の経緯・背景

近年のサイバー攻撃の高度化・巧妙化、情報漏えい事故の増加に対し、組織的なインシデント対応活動が喫緊の課題となっていることから、グループ横断のセキュリティ・インシデント対応チームとして、MS&AD-CSIRT を立ち上げました。

3. 会社内における位置づけおよび活動内容

(1)チーム構成
MS&ADホールディングスの持株会社、事業会社の IT 部門およびシステム開発会社等のシステムリスク担当の兼任メンバーで構成される仮想的なチームです。

(2)活動内容
情報システムに関するセキュリティ・インシデントに関する以下の活動を行っています。
1.グループ内のセキュリティ管理態勢の強化
2.脆弱性情報 / サイバー攻撃等のセキュリティ・インシデント情報の収集、影響分析およびグループ内情報連携
3.セキュリティ・インシデントに対する影響回避・極小化に向けた対応の調整・実施・支援
4.社外のセキュリティ団体 / 他社シーサートとの連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NCSIRT

チームの正式名称	NRI SecureTechnologies Computer Security Incident Response Team
チームの略称	NCSIRT
所属する組織名	NRI セキュアテクノロジーズ株式会社
設立年月日	2007-03-01
チームの Email アドレス	ncsirt@nri-secure.co.jp
チームサイト	
所属組織サイト	http://www.nri-secure.co.jp
加盟年月	2008 年 05 月

1. 概要

NCSIRT は、NRI セキュアテクノロジーズのマネージドセキュリティサービスを母体とする、インシデントレスポンスプロバイダ型の CSIRT です。高度なセキュリティトレーニングを受けたアナリストが、日米複数拠点より 24 時間 365 日、さまざまなセキュリティデバイスの監視、管理を行いインシデントの発生を未然に防いだり、検知後の対応を支援します。

2. 設立の経緯・背景

マネージドセキュリティサービスを開始したのは 1995 年にさかのぼりますが、NCSIRT の公式な設立は 2007 年 3 月です。進化を続けるサイバー攻撃に対処していくためには、組織内 CSIRT 組織が必要となっていくものの、必要機能すべてを単独で実現するには人員・コスト等の観点から難しいと予測されます。NCSIRT は、当社のマネージドセキュリティサービスを利用頂いている企業の組織内 CSIRT のニーズにこたえていくために設立されました。

3. 会社内における位置づけおよび活動内容

Constituency を「マネージドセキュリティサービスを利用されるお客様企業」ととらえ、その企業において外部からのサイバーアタック、内部犯行といったインシデント発生した場合に、必要とされるインシデントレスポンスを有償サービスを提供しています。

インシデント時の対応フローは、内容・レベルに応じたエスカレーションフローを「お客様」毎に定義でき、NCSIRT に所属するすべてのメンバがそれらを理解し行動できるようにしています。「お客様」は、エスカレーションを受けて、NCSIRT からの技術支援、対応支援をもとに、適切なインシデントハンドリングを行うことができます。

技術支援・対応支援には、お客様に提供している、FW, IDS, IPS, Next Gen FW,WAF, AntiMalware などの様々な機器を操作しての Protection / Mitigation を含みます。また、ファイルの整合性チェックや、DDoS アタック対策といった、Integrity, Availability の観点からの Proactive な対応も行っています。

4.注力していること
メンバーへの教育、スキルアップに力を入れています。セキュリティ分野で有力な教育機関である米国 SANS Institute のセキュリティトレーニングコースを全員受講し、認定資格である GIAC の高度資格をメンバー全員が取得しています。

また、実際のインシデントを想定した運用訓練を NCSIRT で作成し、当該業務にあたるメンバー全員が消化することを義務付けています。

CSIRT は持続的な活動が求められます。このため、日本国内でも体制を、日米に分離し、さらに日本国内を東・横・阪に分離し、BCP を策定し、オペレーションを止めないようにしています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NEC-CSIRT

チームの正式名称	NEC Computer Security Incident Response Team
チームの略称	NEC-CSIRT
所属する組織名	日本電気株式会社
設立年月日	2002-07-01
チームの Email アドレス	nec-csirt@cit.jp.nec.com
チームサイト	
所属組織サイト	http://jpn.nec.com/
加盟年月	2015 年 01 月

1. 概要

NEC-CSIRT は、NEC グループでインシデント対応を行う CSIRT です。NEC グループ内やお客様で発生するインシデントに対応しています。

NEC-CSIRT では、インシデント対応と脆弱性情報ハンドリングを中心に、インシデントの発生防止と早期解決、再発防止に取り組んでいます。

2. 設立の経緯・背景

NEC-CSIRT は脆弱性情報を CERT/CC とハンドリングする目的で、2002 年 7 月 1 日に活動を開始しました。その後、セキュリティインシデントの増加に伴い、当時はビジネス部門であったインシデントレスポンスチーム (C-IRT) が合流し、2005 年 10 月以降は、NEC グループならびに当社のお客様で発生するセキュリティインシデントの緊急対応対応も行うようになりました。

3. 会社内における位置づけおよび活動内容

NEC-CSIRT は仮想的な組織であり、NEC グループの複数の部署の人間が関係しています。中心となって活動しているのは、経営システム本部と SI・サービス技術本部であり、前者 (C-IRT がコアチーム) はインシデントレスポンスを、後者 (PSIRT がコアチーム) は脆弱性情報のハンドリングの中核となっています。

NEC-CSIRT のコア機能を担うインシデント対応チーム (C-IRT) は、本社のスタッフ部門である「経営システム本部」に所属しています。インシデント発生時には、関係部門やビジネス部門の有識者などと協力して、事案の解析を行います。活動の中心は、「脅威情報の収集」「高度な脆弱性診断」「ログ解析」「フォレンジック解析」「マルウェア解析」「再発防止」等であり、2010 年頃を境に解析対象が「情報漏洩の解析」から「マルウェアを利用したサイバー攻撃の解析」へ移行いたしました。また、C-IRT で分析した脅威の傾向、攻撃に使用される手法等のノウハウは、NEC グループ内で情報共有し、ビジネスにも活用を計っています。

また NEC-CSIRT 設立当初から行っている脆弱性情報のハンドリングは、2014 年 4 月から SI・サービス技術本部に機能を移し、複数の部門が協力することで運用を行っています。ここでは、「未知脆弱性への対応」、既知の脆弱性情報の周知等を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NELCO-SIRT

チームの正式名称	NELCO セキュリティインシデント対応チーム
チームの略称	NELCO-SIRT
所属する組織名	日商エレクトロニクス株式会社
設立年月日	2016/09/01
チームの Email アドレス	nelco-sirt@nissho-ele.co.jp
チームサイト	
所属組織サイト	http://www.nissho-ele.co.jp/
加盟年月	2016 年 10 月

1. 概要

NELCO-SIRT は、日商エレクトロニクス株式会社が運営するセキュリティインシデントチームです。
主にサイバーセキュリティに関わるインシデント対応を行う組織内 SIRT です。

2. 設立の経緯・背景

NELCO-SIRTの設立は2016年9月です。NELCO-SIRT は、当社情報システム利用に関するセキュリティ環境の更なる安定運用を目指し設立しました。
当社は、全社のリスク管理、システム情報管理における体制に付随し、サイバーセキュリティにおける脆弱性情報の調査、セキュリティインシデントに対する手続きの対応等を新たに整備したく、社内横断的なメンバーで構成致しました

3. 会社内における位置づけおよび活動内容

NELCO-SIRTは、社内において、情報システム部門、リスク管理部門、セキュリティ事業部を中心とし
運営しております。

主に対応している機能:
・社内情報セキュリティのリスク管理
・セキュリティ情報関連情報の提供、及び啓発
・インシデントレスポンス(記録、収集、分析)とセキュリティイベントの管理

対応していない機能:
・各部門で判断すべきセキュリティインシデント
・各種ガイドラインの策定 / 改訂

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NetOne-CSIRT

チームの正式名称	Net One Computer Security Incident Response Team
チームの略称	NetOne-CSIRT
所属する組織名	ネットワンシステムズ株式会社
設立年月日	2015-09-01
チームの Email アドレス	CSIRT@netone.co.jp
チームサイト	
所属組織サイト	http://www.netone.co.jp
加盟年月	2016 年 02 月

1. 概要

NetOne-CSIRT (Net One Computer Security Incident Response Team) は、ネットワンシステムズ株式会社で構成され、ネットワングループ内の主にサイバーセキュリティ事案に関わるインシデント対応を行う組織内 CSIRT です。

2. 設立の経緯・背景

高度化し多発しているサイバー攻撃に起因するセキュリティインシデントに対し、被害を最小限に抑え、迅速で的確な対応を実行する事が求められる昨今の動向において、ICT ソリューションを提供するネットワングループの企業使命を鑑み、社内及びグループ内での事案に対して横断的な機能が必要となったため、2015 年 10 月に設立されました。

3. 会社内における位置づけおよび活動内容

当該チームは、社内において主に次の機能を有しており、弊社情報システム部が主管しています。
・インシデントハンドリング、コーディネーション、経営報告
・インシデント記録の収集と分析 (セキュリティイベントの管理を含む)
・インシデント対応プロセス改善及びセキュリティ対策検討
・脅威情報の収集と分析、脆弱性情報の収集と分析
・技術情報収集、インシデント対応訓練や教育の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NEXS.STC

チームの正式名称	NEC Nexsolutions Security Technical Center
チームの略称	NEXS.STC
所属する組織名	NECネクサソリューションズ株式会社
設立年月日	2006-04
チームの Email アドレス	stc@ml.nexs.nec.co.jp
チームサイト	
所属組織サイト	http://www.nec-nexs.com/
加盟年月	2008 年 09 月

1. 概要

NEXS.STC は、NEC グループのシステムインテグレータである NEC ネクサソリューションズ株式会社 (http://www.nec-nexs.com/) によって運営されている CSIRT です。

2. 設立の経緯・背景

NEC グループは、2005 年頃に相次いだセキュリティインシデント発生を機に、セキュア開発・運用の推進やセキュリティ診断などを通じてシステムの安全性、品質向上に資するための専門部署として、グループ各社にセキュリティテクニカルセンターを設立しました。

一方、NEXS.STC の前身となるグループは、テクニカルセンター設立以前から Web アプリケーションのソースコード検査などのシステム診断や Web セキュリティ製品の開発などを行なっており、また、顧客で発生したインシデント対応もグループの役割として実施していました。

NEXS.STC は両者のノウハウを融合し、全社的なインシデント対応体制の技術的中核として位置づけられた部署として 2006 年に設立されました。

3. 会社内における位置づけおよび活動内容

NEXS.STC は CSIRT としてインシデント発生の現場で実際に対応を行なう他、インシデントの発生原因、被害状況などを調査・分析する「分析センター」としての機能をもっています。NEXT.STC は、セキュリティ技術を深耕し、ここで得たノウハウを社内のエンジニア教育を通じてフィードバックし、側面から全社セキュリティ対応スキルを底上げするとともに、顧客に提供する情報システムのセキュリティ品質を向上する活動を行っています。

同時に、これらの活動を通じて培ったノウハウをもとに顧客向けのセキュリティコンサルティング事業も行っています。

また、NEC グループおよびセキュリティ事業各社との積極的な連携や情報共有を行うとともに、標準ガイドラインの策定や啓蒙のためのセミナ開催などを通じて、安心安全なシステム環境の実現に貢献しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NF-CSIRT

チームの正式名称	NTTファイナンスCSIRT
チームの略称	NF-CSIRT
所属する組織名	NTTファイナンス株式会社
設立年月日	2016年4月1日
チームの Email アドレス	nf-csirt@ntt-finance.com
チームサイト	
所属組織サイト	http://www.ntt-finance.co.jp/
加盟年月	2017 年 04 月

1. 概要

NF-CSIRTは、NTTファイナンス社として事前情報に基づく脆弱性対応、および社外からのサイバー攻撃に対し判断および対処を迅速に行い被害の拡大を最小限に食い止めるために社内組織として発足したCSIRTチームです。現在NTTグループ各社と連携しサイバーセキュリティ対策の推進に向け取り組んでいます。

2. 設立の経緯・背景

近年サイバー攻撃手法がますます高度化・巧妙化している中で、NTTグループの金融中核会社として脅威の増大に対し、サイバーセキュリティインシデントに対する取り組みを強化することを目的に、2016年4月1日から「NF-CSIRT」を立ち上げ活動を開始しました。

3. 会社内における位置づけおよび活動内容

NTTグループからの事前警戒情報などに基づき、社内での周知徹底および事前調査確認を徹底するとともに、万一社内においてサイバーインシデントが発生した場合には、迅速に被害の拡大防止に向け関連情報の収集・告知、再発防止措置を行うべく活動しています。
［活動方針］
◆日ごろからの準備と迅速な対応
日ごろから、サイバーインシデントに対する連絡体制や役割分担等を明確にしておき、対応手順の整備や訓練を実施し、インシデントが発生した場合にはNF-CSIRTが活動を開始し、迅速な対応を行います。
◆上部機関へのエスカレーション
NF-CSIRTは社内危機管理委員会の配下で活動を行い、随時委員会へ状況報告を行うとともに、必要な指示を受けながら適切な措置を実施します。
◆NTT-CERT、グループ各社との連携
インシデントの難易度に応じNTT-CERT、グループ各社と密接な連携をとり、予防保全に向けた迅速な対応、およびより高度な技術支援等を受け確実な対応を実施します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NAA CSIRT

チームの正式名称	成田国際空港コンピュータセキュリティインシデントレスポンスチーム
チームの略称	NAA CSIRT
所属する組織名	成田国際空港株式会社
設立年月日	2016年7月1日
チームの Email アドレス	naa-csirt@naa.jp
チームサイト	
所属組織サイト	http://www.naa.jp/jp/
加盟年月	2016 年 11 月

1. 概要

http://www.naa.jp/jp/
　成田国際空港株式会社(以下NAA)は、国際社会における重要な役割を担い、国際交流を活発に行えるよう邁進すると共に、施設の整備・拡充を進め、高品質なサービスの提供を目指して、空港づくりを進めています。
　成田国際空港コンピュータセキュリティインシデントレスポンスチーム（以下NAA CSIRT）は、NAA及びNAAグループ全体としてサイバーセキュリティ対応力を高め、継続して推進していくことを目的として活動しています。

2. 設立の経緯・背景

NAA CSIRTは、世界最高水準の安全性と安定運用を追及しサイバー攻撃に対するセキュリティ対策を徹底するため、サイバー攻撃に対する最新の安全対策を講じていくとともに、政府の対策基準等に準ずる形で情報セキュリティに関する体制・規程等の整備を進め、NAAグループ全体でのセキュリティ水準の向上を図り、お客様に安心して成田空港をご利用いただくため2016年7月に設立致しました。

3. 会社内における位置づけおよび活動内容

(1) 会社内における位置づけ
　NAA CSIRTは、NAAの経営企画部門　IT推進部 情報セキュリティグループとして設立し、NAA及びNAAグループ全体のサイバーセキュリティ対策を推進しています。
(2) 活動内容
・サイバー攻撃に係る対応業務（インシデント対応）
・NAAグループ全体に対するセキュリティ対策推進計画の立案・実行
・情報セキュリティ対策に関する訓練／教育
・情報セキュリティに係る社外との情報交換及び情報収集

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NFL-CSIRT

チームの正式名称	Neo First Life Computer Security Incident Response Team
チームの略称	NFL-CSIRT
所属する組織名	ネオファースト生命保険株式会社
設立年月日	2016年4月1日
チームの Email アドレス	smart_ml@neofirst.co.jp
チームサイト	
所属組織サイト	http://neofirst.co.jp/
加盟年月	2017 年 10 月

1. 概要

NFL-CSIRT(Neo First Life Computer Security Incident Response Team)は、ネオファースト生命保険のサイバーインシデント対応を行うCSIRTです。

2. 設立の経緯・背景

高度化・巧妙化するサイバー攻撃により様々な被害が発生する中、インシデント発生時の影響の最小限に抑えることを目的とし、組織内における体制を明確化するとともに、インシデント発生時の迅速かつ確実な対応による被害拡大防止、及び、平時の情報収集・社内広報によるサイバーインシデントの発生抑止を目的に、2016 年 4 月に設立されました。

3. 会社内における位置づけおよび活動内容

NFL-CSIRT は自組織の情報システム部門を事務局として、社内関連部門やグループ会社と連携を図りながら、以下のような活動を実施しています。

活動内容
1. 平常時の対応
   ・外部の情報共有機関およびグループ内CSIRTと連携し、サイバー関連の情報収集および共有
   ・各機器やウイルス対策製品のログ監視・分析
   ・サイバーセキュリティ関連教育と訓練の推進
2. インシデント発生時の対応
   ・サイバーインシデント発生（予告）の検知
   ・サイバーインシデント対応
   ・復旧作業
3. インシデント関連報告
   ・インシデント発生時の対応報告
   ・定期的なサイバーインシデントの発生件数・内容・影響度合いの報告

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NICT-CSIRT

チームの正式名称	NICT 情報セキュリティインシデント対応チーム
チームの略称	NICT-CSIRT
所属する組織名	国立研究開発法人情報通信研究機構
設立年月日	2013-04-01
チームの Email アドレス	csirt-info@ml.nict.go.jp
チームサイト	
所属組織サイト	http://www.nict.go.jp/
加盟年月	2015 年 11 月

1. 概要

NICT-CSIRT は、国立研究開発法人　情報通信研究機構（NICT）の組織内 CSIRT です。
　　NICTは、情報通信分野を専門とする唯一の公的研究機関として、2004年に発足しました。豊かで安心・安全な社会の実現や我が国の経済成長の原動力である情報通信技術（ICT）の研究開発を推進するとともに、情報通信事業の振興業務を実施しております。

2. 設立の経緯・背景

近年の高度で巧妙なサイバー攻撃に迅速に対応するため、2013 年 4 月に NICT-CSIRTが設置され、活動を開始しました。

3. 会社内における位置づけおよび活動内容

【組織内における位置づけ】
　NICT-CSIRT は、情報セキュリティ管理規程で定められた部門横断的な組織で、CIO、統括情報セキュリティ責任者、企画戦略室と情報システム室の担当職員、CIO補佐官、サイバーセキュリティ研究室長、広報担当職員で構成されています。

【活動内容】
　NICT内で生じたインシデントに迅速に対応すると共に、標的型メール訓練、情報セキュリティ自己点検、セミナー等の情報セキュリティ研修、他組織との情報交換等も行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NIKKEI-SIRT

チームの正式名称	日経セキュリティーインシデント対応チーム
チームの略称	NIKKEI-SIRT
所属する組織名	株式会社日本経済新聞社
設立年月日	2015-04-01
チームの Email アドレス	nikkei-sirt@nex.nikkei.co.jp
チームサイト	
所属組織サイト	http://www.nikkei.co.jp/nikkeiinfo/corporate/outline/
加盟年月	2015 年 12 月

1. 概要

NIKKEI-SIRT は、株式会社日本経済新聞社の組織内セキュリティーインシデント対応チームです。株式会社日本経済新聞社は、新聞発行を軸にした複合メディア企業です。

2. 設立の経緯・背景

サイバー攻撃の巧妙化、個人情報の流出・漏洩などが企業経営の大きなリスクとなっているなか、より迅速な対応と社外との情報連携のため、NIKKEI-SIRT を設置しました。

3. 会社内における位置づけおよび活動内容

NIKKEI-SIRT は社内情報システム部門である情報技術本部メンバーを中心に、社内各部門、関係機能との連携の元、セキュリティーインシデント発生時の影響低減・解決支援を軸に活動しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Nikon-CSIRT

チームの正式名称	ニコンCSIRT
チームの略称	Nikon-CSIRT
所属する組織名	株式会社ニコン
設立年月日	2012年10月15日
チームの Email アドレス	nikon.csirt@nikon.com
チームサイト	
所属組織サイト	http://www.nikon.co.jp/
加盟年月	2016 年 09 月

1. 概要

ニコンCSIRTは、株式会社ニコンにより運営されているCSIRTです。

2. 設立の経緯・背景

昨今のサイバー攻撃の高度化により、情報セキュリティの重要性がますます高まっており、これらに対して個別の部門では対応が困難になってきております。
このため、ニコングループの情報セキュリティ部門の一元化とセキュリティ対策の強化を目的として、2012年10月に設立されました。

3. 会社内における位置づけおよび活動内容

会社内の他部門とは独立した、社長直轄の組織です。
主な活動内容は、情報資産に対する脅威の最新情報の把握とそれらへの対策の立案及び実施、インシデントの監視、また、インシデント発生時の対応、などです。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NISSHIN-CSIRT

チームの正式名称	NISSHIN-Computer Security Incident Response Team
チームの略称	NISSHIN-CSIRT
所属する組織名	株式会社日清製粉グループ本社
設立年月日	2016年11月1日
チームの Email アドレス	nisshin-csirt@nisshin.com
チームサイト	
所属組織サイト	http://www.nisshin.com
加盟年月	2017 年 09 月

1. 概要

NISSHIN-CSIRT（NISSHIN-Computer Security Incident Response Team）は、日清製粉グループの情報セキュリティインシデント対応を所掌・実施する、株式会社日清製粉グループ本社の組織内CSIRTです。

2. 設立の経緯・背景

2015 年 12 月に、経済産業省から「サイバーセキュリティ経営ガイドライン」が発表され、経営者のリーダーシップの下で企業自らがサイバーセキュリティの対応強化に取り組むことが求められています。また、企業が有する個人情報や重要な機密情報を狙ったサイバー攻撃は増加傾向にあるだけでなく、手口も年々巧妙化し、その脅威は身近なものとなっています。このような状況の中、当社グループにおけるサイバーセキュリティ対策や、社員教育・訓練を継続的に実施し、脅威に対する能力を向上させ、インシデント発生時も速やかに対処するためにNISSHIN-CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

NISSHIN-CSIRT は、株式会社日清製粉グループ本社の情報システム部署メンバーで構成される組織内CSIRTです。以下の活動を通じ、日清製粉グループにおける、サイバーセキュリティ管理および態勢の維持・向上を推進します。

1) セキュリティ対策の検討・実施
2) セキュリティインシデント発生時の対応主導
3) セキュリティ教育・訓練の実施
4) 最新の脅威情報、脆弱性情報の収集と予防策の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Nitto-CSIRT

チームの正式名称	Nitto-CSIRT
チームの略称	Nitto-CSIRT
所属する組織名	日東電工株式会社
設立年月日	2017年2月1日
チームの Email アドレス	it-security-team@nitto.com
チームサイト	
所属組織サイト	http://www.nitto.com/
加盟年月	2017 年 07 月

1. 概要

日東電工株式会社は1918年に創業し、大阪市に本社を置く化学製品メーカーです。粘着、塗工、高分子機能制御、高分子分析・評価の四つの基幹技術でお客様に最適な製品を提供致します。
Nitto-CSIRTは、弊社情報セキュリティ管理体制と一体となって大切なお客様情報の保護に取り組みます。

2. 設立の経緯・背景

弊社では従来より情報セキュリティ委員会を中心にNittoグループの情報セキュリティ向上に努めてまいりました。しかし、年々高度化する外部脅威、および事業拡大によって生まれる新たなリスクに対処していくため、従来の活動に加え、レジリエンスを高めていく活動の必要性を感じておりました。そこで、事故発生に備える平時の活動を定着させ、かつ有事の際に素早く初動を行えるよう、Nitto-CSIRTを設立致しました。

3. 会社内における位置づけおよび活動内容

Nitto-CSIRTは、日東電工株式会社ITガバナンス部のメンバーによって構成されるバーチャルチームです。情報セキュリティ委員会の一員として日々のセキュリティ対策向上活動を行いつつ、情報セキュリティ事故発生時にはIT専門家として早期解決に寄与致します。主な活動内容は以下の通りです。

□予防
- 情報収集、従業員教育、経営層報告
- 情報セキュリティ対策の強化・改善・性能維持
- ログ監視およびアラートの分析

□事故対応
- 情報セキュリティ事故への初動対応
- 関連部門と連携したインシデント対応。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NLI-CSIRT

チームの正式名称	Nippon Life Insurance Company Computer Security Incident Response Team
チームの略称	NLI-CSIRT
所属する組織名	日本生命保険相互会社
設立年月日	2015-04-15
チームの Email アドレス	nli-csirt@nissay.co.jp
チームサイト	
所属組織サイト	http://www.nissay.co.jp/
加盟年月	2015 年 05 月

1. 概要

NLI-CSIRT は日本生命のシステム関連部署で構成された CSIRT です。

2. 設立の経緯・背景

従前からサイバーセキュリティに関する様々な対策を実施しておりましたが、昨今の高度化、巧妙化するサイバー攻撃の状況等をふまえ、サイバーセキュリティ事案の未然防止と検知時の迅速な対応支援を行うことを目的に設立しました。

3. 会社内における位置づけおよび活動内容

(1)メンバー構成
NLI-CSIRT は、日本生命のシステム関連部署 (システムリスク管理室、システム企画部、ニッセイ情報テクノロジー株式会社) で構成する仮想的なチームです。

(2)活動範囲
日本生命におけるサイバーセキュリティ事案の未然防止と検知時の迅速な対応を行います。

(3)活動内容
サイバーセキュリティインシデント情報の収集、調査・分析・対応、サイバーセキュリティに関する教育、啓発活動を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NSG-CSIRT

チームの正式名称	Nippon Steel & Sumitomo Metal Group. Computer Security Incident Response Team
チームの略称	NSG-CSIRT
所属する組織名	新日鐵住金株式会社
設立年月日	2013年12月1日
チームの Email アドレス	nsg-csirt@jp.nssmc.com
チームサイト	
所属組織サイト	http://www.nssmc.com/
加盟年月	2017 年 04 月

1. 概要

NSG-CSIRTは、新日鐵住金株式会社が中心となって運営している、新日鉄住金グループのCSIRTです。
新日鉄住金グループが常に世界最高の技術とものづくりの力を追求し、優れた製品・サービスの提供を通じて社会の発展に貢献し続けるために、組織横断的な情報セキュリティへの対応を実施します。

2. 設立の経緯・背景

これまで新日鐵住金および関連会社では、サイバー攻撃による事業停止・情報漏洩リスクへの対応として、
様々なセキュリティ対策を講じてきましたが、昨今の高度化・複雑化するサイバー攻撃脅威に対し、関連各社毎の個別対策ではなく、組織横断的な対策が重要であると考え設立しました。

3. 会社内における位置づけおよび活動内容

NSG-CSIRTは、新日鐵住金株式会社のセキュリティ対応部門および関連会社の情報システム部門に所属するメンバで構成されています。

NSG-CSIRTは、情報システムの継続的な安定稼働の実現を目指し、主に活動を行います。

・情報システムセキュリティに関する情報収集・分析
・セキュリティマネジメントのプロセス・手順等の整備
・脆弱性情報の収集と改善状況のモニタリング
・インシデントハンドリング
・情報システムセキュリティに関する課題・対策（管理・基盤）検討
・セキュリティ教育・啓蒙活動
・外部組織との情報連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NII CSIRT

チームの正式名称	国立情報学研究所情報セキュリティインシデント対応チーム
チームの略称	NII CSIRT
所属する組織名	国立情報学研究所
設立年月日	2014-07-10
チームの Email アドレス	nii-csirt@nii.ac.jp
チームサイト	http://www.nii.ac.jp/research/facilities/aic/nii-csirt/
所属組織サイト	http://www.nii.ac.jp
加盟年月	2015 年 02 月

1. 概要

NII CSIRT は、国立情報学研究所 (NII) の組織内 CSIRT です。

NII は、情報学の総合研究所として研究を推進すると共に、日本国内の学術ネットワーク基盤である SINET や CiNii といった学術情報サービスを大学等に提供しています。

2. 設立の経緯・背景

昨今のサイバー攻撃の高度化・巧妙化に対応するため、所内の情報セキュリティ体制についての強化、見直しが図られ、2014 年 7 月に NII CSIRT の設置が承認されました。NII CSIRT の運用規則等を定めるため、9 月に所内の情報セキュリティポリシーを改訂し、10 月から活動を開始しています。

3. 会社内における位置づけおよび活動内容

(会社内における位置づけ)
NII CSIRT は、NII 内のセキュリティ関係者・部署に所属するメンバーから新たに構成された仮想の組織横断的なチームです。教員と職員で構成されています。
(活動内容)
NII 組織内で生じたインシデント対応を集中的に行うと共に、情報セキュリティ研修の開催、脆弱性情報の提供などの事前のセキュリティ対策活動も行っています。なお、SINET や CiNii 等の学術情報サービス事業については NII CSIRT のサービスの対象外としています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NSSOL-CSIRT

チームの正式名称	新日鉄住金ソリューションズ インシデントレスポンスチーム
チームの略称	NSSOL-CSIRT
所属する組織名	新日鉄住金ソリューションズ株式会社
設立年月日	2015/4/1
チームの Email アドレス	te-nssol-csirt@jp.nssol.nssmc.com
チームサイト	
所属組織サイト	http://www.nssol.nssmc.com
加盟年月	2016 年 07 月

1. 概要

NSSOL-CSIRTは新日鉄住金ソリューションズ株式会社によって運営されるCSIRTです。

新日鉄住金ソリューションズ株式会社は、世界トップクラスの鉄鋼メーカーの複雑で高度な製鉄システムを企画・構築し、24時間、365日、約50年間運用してきました。このような大規模なシステムにおいて、長年培ってきたノウハウをベースに、製造業、金融、公共、通信といった様々な業界向けに幅広いソリューションを提供しています。

2. 設立の経緯・背景

当社では情報システムの構築・運用・ソフトウェア開発に始まり、データセンター・クラウドなど様々なサービスをお客様に提供しており、海外へも積極的に事業展開を進めています。

一方で、情報システムに対する脅威は今日急速に増加を続けており、そのリスクに直面する場面も増えてきました。
こうした環境の変化を踏まえ、当社の事業に重大な影響を与える可能性がある情報セキュリティリスクに対し、適正な対策と適切なハンドリングを行うべく、2015年4月にNSSOL-CSIRTを設置しました。

3. 会社内における位置づけおよび活動内容

■位置付け
NSSOL-CSIRTは社長をトップとしており、上流での意思決定から下流での技術対応支援までをカバーすることで組織的な活動と位置付けています。

■活動内容
当社および当社の子会社において以下の活動を行います。

1. インシデント発生時の状況確認や復旧対応についての技術支援
2. 社員に対するセキュリティ教育・啓蒙活動を含む予防策の実施
3. 脆弱性情報ならびに脅威情報の収集・分析・社内関係者への共有

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NISSAY IT CSIRT

チームの正式名称	NISSAY IT CSIRT
チームの略称	NISSAY IT CSIRT
所属する組織名	ニッセイ情報テクノロジー株式会社
設立年月日	2014-09-01
チームの Email アドレス	csirt_info@nissay-it.co.jp
チームサイト	
所属組織サイト	http://www.nissay-it.co.jp/
加盟年月	2014 年 10 月

1. 概要

NISSAY IT CSIRT は、ニッセイ情報テクノロジー株式会社の組織内コンピュータ セキュリティ インシデント レスポンスチームです。

2. 設立の経緯・背景

チーム設立以前より社内の各部門で脆弱性情報の収集や通知、外部からの攻撃の分析等を実施しておりました。昨今の脆弱性や複雑化するサイバー攻撃等、セキュリティリスクの高まりを受け、社内体制を整備・強化し、インシデント対応の更なる高度化をすべく NISSAY IT CSIRT を設立しました。

3. 会社内における位置づけおよび活動内容

会社内における位置づけ
NISSAY IT CSIRT は社内の IT 管理部門及びセキュリティ関連部門からなる仮想チームです。

活動内容
NISSAY IT CSIRT の以下の活動を実施しています。
・脆弱性情報の収集と社内への通知
・脆弱性情報への社内システムの対応検討
・各種監視状況の分析と報告
・システムセキュリティ関連動向の調査
・社内システムへのセキュリティインシデント発生時の対応・支援
・日本 CSIRT 協議会等、外部関連機関との連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NTT-CERT

チームの正式名称	NTT Computer Security Incident Response and Readiness Coordination Team
チームの略称	NTT-CERT
所属する組織名	日本電信電話株式会社
設立年月日	2003-07-01
チームの Email アドレス	cert@ntt-cert.org
チームサイト	
所属組織サイト	https://www.ntt-cert.org/
加盟年月	2007 年 11 月

1. 概要

NTT-CERT は、日本電信電話株式会社 NTT セキュアプラットフォーム研究所が中心となって運営している、NTT グループ (http://www.ntt.co.jp/) の CSIRT です。

2. 設立の経緯・背景

2003 年ごろ、NTT 情報流通プラットフォーム研究所 (当時) では、(1) インターネット・インフラの重要性の増加、(2) インシデントの多様化、(3) セキュリティ研究活動で得た諸外国の CSIRT 導入の動きを認知していました。
このことから示唆される近い将来に対応するため、それまでインシデントハンドリングにおいてボランタリーに活動していた個々の研究者が集う形で、2004 年 1 月、「先端セキュリティセンター」がオーソライズされた組織として結成されました。これが NTT-CERT の前身です。
その後、同年のうちに「NTT-CERT」と名前を改め、NTT グループの代表 CSIRT として活動するようになっています。

3. 会社内における位置づけおよび活動内容

NTT-CERT は、日本電信電話株式会社に所属する研究所 (セキュアプラットフォーム研究所) を母体としています。NTT グループ各社をサービス受給者として設定し、NTT グループの各 PoC をアドバイザーの立場で技術的に支援する「コーディネーションセンター」型の CSIRT です。以下のように幅広い活動を行っています。
・インシデント対応支援、脆弱性対応支援、再発防止策の検討のような「リアクティブな活動」
・予防・検知に関する情報発信を通した「プロアクティブな活動」
・トレーニングプログラムの開発やセキュリティ啓発活動などを通した「セキュリティ品質マネジメント活動」

また、NTT-CERT は、研究所を母体とする組織ならではの特色を持っています。普段は、専任の CSIRT メンバーが案件ハンドリングを実施していますが、状況に応じてより詳しい専門家 (研究者) と一緒になって対応をします。同時に、CSIRT の営みを通して得られた実践的な知見は、新たなセキュリティの研究開発のための原動力となります。このように研究所ならではの特色をうまく活かしながら、CSIRT 活動を維持しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NTTDATA-CERT

チームの正式名称	NTTDATA-CERT
チームの略称	NTTDATA-CERT
所属する組織名	株式会社NTTデータ
設立年月日	2010-07-01
チームの Email アドレス	nttdata-cert@kits.nttdata.co.jp
チームサイト	
所属組織サイト	http://www.nttdata.com/jp/
加盟年月	2011 年 03 月

1. 概要

NTTDATA-CERT は、NTT データグループの CSIRT です。通常はセキュリティインシデント予防のための情報収集・分析、対策実施を行っています。万が一 NTT データグループで、セキュリティインシデントが発生した際は、緊急対応を行います。緊急対応後はインシデント原因などを分析し、その結果を再発防止をはじめとする活動にフィードバックを行います。

2. 設立の経緯・背景

NTT データでの情報セキュリティインシデント対応活動は、NTTDATA-CERT が設立される前からも、全社および事業部門独自で行われてきました。これらの取組を集約し、NTT データグループとしてよりよい形での情報セキュリティインシデント予防、対応、再発防止についての取組を行えるよう、2010 年 7 月 1 日に NTTDATA-CERT が設立されました。

3. 会社内における位置づけおよび活動内容

NTTDATA-CERT は、NTT データグループの情報セキュリティに関する取組を統括する部署である「セキュリティ技術部 情報セキュリティ推進室」内に設置されており、各種セキュリティインシデントの予防に資する活動および、インシデント発生時の対応を行っています。インシデント対応によって得られた知見は、情報セキュリティ推進室内で適宜共有を行い、NTT データグループの情報セキュリティに関する取組にフィードバックを行うとともに、再発防止やインシデント検知の早期化のための取組改善に活用しています。インシデント対応以外にも、外部の知見を積極的に取り入れ、新しい脅威に対抗できるような備えを行ったり、将来的に発生しうる脅威を想定した研究開発なども行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NTTPC-CSIRT

チームの正式名称	NTTPC Communications CSIRT
チームの略称	NTTPC-CSIRT
所属する組織名	株式会社NTTPCコミュニケーションズ
設立年月日	2016年2月5日
チームの Email アドレス	nttpc-csirt@nttpc.co.jp
チームサイト	
所属組織サイト	http://www.nttpc.co.jp/
加盟年月	2016 年 09 月

1. 概要

NTTPC-CSIRTは、株式会社NTTPCコミュニケーションズの組織内CSIRTです。NTTコミュニケーションズ株式会社のグループ会社として、NTT Com-SIRTと連携し、NTTPCコミュニケーションズのサイバーセキュリティ対策の推進に取り組んでいます。

2. 設立の経緯・背景

NTTPCコミュニケーションズでは、NTTPC-CSIRT設立以前から、有志によるサイバーセキュリティ対策活動に取り組んでいましたが、今後ますます高まるであろうサイバーセキュリティの脅威に対応し、ガバナンス強化と情報収集の効率化を図るため、全社視点でサイバーセキュリティへの対応を行うことを目的とし、NTTPC-CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

NTTPC-CSIRTは、社内の技術開発／保守／運営部門の組織のメンバーから構成され、CSO職務を補佐する「CSOスタッフ」として設置し、各組織で行われているサイバーセキュリティへの取り組みを、全社に対してノウハウ共有／展開を図り、インシデントへの未然の防御の実現と発生時の適切な対応、脅威に対し社外各社と連携を図ります。

1）サイバーセキュリティインシデント対応の全社統制
2）サイバー攻撃に対応するための全社施策の立案と推進
3）社外サイバーセキュリティ関連機関との窓口

これらの活動を通じて、NTTPCコミュニケーションズのサービス全般の関連システム、ネットワーク等のサイバーセキュリティ対策を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Nomura Group CSIRT

チームの正式名称	野村グループCSIRT
チームの略称	Nomura Group CSIRT
所属する組織名	野村ホールディングス株式会社
設立年月日	2015-03-27
チームの Email アドレス	nomura-group-csirt@jp.nomura.com
チームサイト	
所属組織サイト	http://www.nomuraholdings.com/jp/
加盟年月	2015年4月

1. 概要

野村ホールディングス株式会社は、証券業を中核とする投資・金融サービス業を営む会社の株式を保有することにより、当該会社の事業活動を支配・管理する持株会社です。

2. 設立の経緯・背景

高度化・巧妙化するサイバー攻撃により発生した事象への対応、及び被害を軽減させるための態勢を整備することを目的として設置しました。

3. 会社内における位置づけおよび活動内容

1.位置づけ
・野村グループ CSIRT は、野村グループ危機管理委員会事務局 情報セキュリティ責任者の下に設置しております。
・野村グループ CSIRT は、野村ホールディングス株式会社 IT 統括部長を代表とします。
・野村グループ傘下各社の CSIRT 代表は、野村グループ CSIRT のメンバーとします。
・野村グループ CSIRT の事務局は野村ホールディングス株式会社　IT 統括部に設置します。

2.活動内容
次に掲げる活動により、野村グループ傘下各社に設置された CSIRT のガバナンスを行います。
(1)野村グループを代表して金融 ISAC や日本シーサート協議会等に加盟し、外部機関から情報収集し、野村グループ傘下各社に展開します。
(2)野村グループ傘下各社のサイバーセキュリティの対応状況等を確認し、グループベースでの連携を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

OBAYASHI-CSIRT

チームの正式名称	大林組シーサート
チームの略称	OBAYASHI-CSIRT
所属する組織名	株式会社　大林組
設立年月日	2016年12月21日
チームの Email アドレス	obayashi-csirt@ml.obayashi.co.jp
チームサイト	
所属組織サイト	http://www.obayashi.co.jp
加盟年月	2017 年 01 月

1. 概要

OBAYASHI-CSIRTは、株式会社大林組によって運営されている大林組グループのCSIRTです。

2. 設立の経緯・背景

弊社では、「平常時におけるセキュリティインシデントの未然の防止」及び「セキュリティインシデント発生時の適切な対処」のための危機管理体制及び情報セキュリティ体制を整備し対処してきました。しかし、多様化、巧妙化、複雑化する情報セキュリティリスクへの対応を強化するため、セキュリティインシデント対策の専門チームであるCSIRTを新たに組織しました。

3. 会社内における位置づけおよび活動内容

（1）位置付け
OBAYASHI-CSIRTは、グローバルICT推進室、総務部、土木・建築部門とオーク情報システムから選任されたメンバーで構成されるチームで、大林組グループのセキュリティインシデントの対応にあたっています。

（2）活動内容
OBAYASHI-CSIRTは「セキュリティインシデントの未然の防止」及び「セキュリティインシデント発生時の対処」に関し以下の活動を実施しています。
・リスク、脆弱性、情報セキュリティ動向、社内外で発生した情報セキュリティ等に関する情報の収集と分析
・情報セキュリティに関する監査の実施
・情報セキュリティインシデントに対して対応策の検討及び実施
・情報セキュリティインシデントに対して再発防止策の策定及び実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

OBC-SIRT

チームの正式名称	オービックビジネスコンサルタントSIRT
チームの略称	OBC-SIRT
所属する組織名	株式会社オービックビジネスコンサルタント
設立年月日	2015-09-01
チームの Email アドレス	obc-sirt@obc.co.jp
チームサイト	
所属組織サイト	http://www.obc.co.jp/
加盟年月	2016 年 01 月

1. 概要

OBC-SIRT は株式会社オービックビジネスコンサルタントが運用しているセキュリティインシデントレスポンスチームです。

2. 設立の経緯・背景

当社は、従来より情報セキュリティインシデントに対する対策や対応を実施してきましたが、情報セキュリティの脅威は、年々複雑化かつ巧妙化してきています。このような状況の変化と、提供サービスプラットフォームとしてのクラウドの普及を受けて、セキュリティインシデントが発生した際に速やかに状況を把握、分析し、被害の最小化・極小化を実現することができるように体制を整備し、2015 年 10 月に「OBC-SIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

OBC 提供のサービスおよびソフトウェア、そして社内で発生する情報セキュリティインシデントに対して、
・イベントの監視
・脆弱性情報の収集・連絡・対応
・インシデント発生時の原因分析、復旧対応・支援、事後対応
・情報セキュリティに関する教育・啓発、再発防止
などの活動を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

OCE-CSIRT

チームの正式名称	大崎コンピュータエンヂニアリング CSIRT
チームの略称	OCE-CSIRT
所属する組織名	株式会社大崎コンピュータエンヂニアリング
設立年月日	2015-07-01
チームの Email アドレス	oce-csirt@oce.co.jp
チームサイト	
所属組織サイト	http://www.oce.co.jp/
加盟年月	2016 年 01 月

1. 概要

OCE-CSIRT は株式会社大崎コンピュータエンヂニアリングが運営しているセキュリティインシデントレスポンスチームです。大崎コンピュータエンヂニアリングは、ICT のサービスインテグレータとして、自治体様、企業様向けの基幹情報システムやネットワークの構築・運用から、自社データセンターを活用した、お客様の情報システムの確実な運用・監視、保守サービスを提供するアウトソーシングやネットワークサービスを展開しています。

2. 設立の経緯・背景

当社は情報システム部門、ネットワーク構築部門が中心となり、情報セキュリティ対策を進めてきましたが、近年の高度化、複雑化したサイバー攻撃から情報漏洩を未然に防ぐ為には、組織内だけでの活動に限界があり、外部組織と情報交換などの連携を図り、コンピュータセキュリティの脅威を軽減する活動を強化するため、OCE-CSIRT を立ち上げ、日本シーサート協議会に加盟いたしました。

3. 会社内における位置づけおよび活動内容

OCE-CSIRT は株式会社大崎コンピュータエンヂニアリングの情報システム部門、ネットワーク基盤構築部門、データセンター運営・監視部門の要員からなる仮想的なチームです。

活動内容は以下の通りです。

-外部組織と連携を図り、コンピュータセキュリティの脅威を軽減させる情報交換の場に参加する。
-新たな脅威についての情報収集 (IPA 等) する。
-内部から外部への通信を監視して、情報漏洩インシデントの有無を判断する。
-上記インシデントが発生した場合は、関連部署と連携を図り適切に対処する。
-本ミッションで培ったノウハウを活かして、類似インシデントの防止策を検討する。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NTT Com-SIRT

チームの正式名称	NTT Communications Security Incident Response Team
チームの略称	NTT Com-SIRT
所属する組織名	NTTコミュニケーションズ株式会社
設立年月日	2015-08-03
チームの Email アドレス	NTTCom-SIRT@ntt.com
チームサイト	
所属組織サイト	http://www.ntt.com/
加盟年月	2015 年 09 月

1. 概要

NTT Com-SIRT は、NTT コミュニケーションズ株式会社の組織内 CSIRT です。

2. 設立の経緯・背景

NTT コミュニケーションズ株式会社は、今後ますます高まるであろうサイバーセキュリティの脅威に対する能力を向上させるため、この度、一元化されたわかりやすい対外的な窓口を整備することに加え、既存のセキュリティ対応機能の更なる強化を目的として NTT Com-SIRT を立ち上げることとしました。

3. 会社内における位置づけおよび活動内容

NTT Com-SIRT は情報セキュリティ部を中心とした複数の組織のメンバーから構成され、NTT コミュニケーションズグループのサービス全般の関連システム、ネットワーク等のサイバーセキュリティ対策を行います。

1)サイバーセキュリティの対外的な窓口としての情報収集及び情報発信
2)セキュリティインシデント発生時の対応主導
3)セキュリティ対策の実施

これらの活動を通じて自社や NTT グループにおけるセキュリティ基盤の向上にチャレンジし続けることで、安心・安全な情報社会の発展を目指します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

OGIS-CSIRT

チームの正式名称	株式会社オージス総研 サイバーセキュリティ対策室
チームの略称	OGIS-CSIRT
所属する組織名	株式会社オージス総研
設立年月日	2016年7月1日
チームの Email アドレス	CY_Security@ogis-ri.co.jp
チームサイト	
所属組織サイト	http://www.ogis-ri.co.jp/
加盟年月	2018 年 02 月

1. 概要

オージス総研は、大阪・東京に本社を持つ、大阪ガスグループのシステムインテグレータ（SIer）です。
大規模システムの設計、開発、運用をサポートしてきました。エネルギー、製造、金融を中心とした、多彩な業界に向けたサービス・ソリューションを展開しております。

OGIS-CSIRT は、社内でのサイバーセキュリティインシデントが、業務ひいてはお客様へ影響を及ぼすことが無いように、有事の際の対応と、その予防活動を行うサイバーセキュリティ対策に特化した、QA・セキュリティ統括を組織長とした仮想的な社内インシデントレスポンスチームです。

2. 設立の経緯・背景

オージス総研は、ISMS 認証(一部を除く)、プライバシーマークを取得しており、情報セキュリティマネジメントシステムを運用しております。
しかしながら、巧妙かつ高度化するサイバー攻撃は未然防止が難しく、その被害は、業務停止や情報流出など経営に関わるリスクがあります。
そこでサイバーセキュリティ・インシデントに特化した組織として2016年7月に OGIS-CSIRT を立ち上げました。
平時より、サイバーセキュリティインシデントによる被害を最小限にする各種活動を行うとともに、有事の際の組織的かつ迅速な対応をミッションとしています。

3. 会社内における位置づけおよび活動内容

会社内における位置づけ
全社的な対応を、迅速な判断のもと遂行するために、社長直轄組織として配置しています。
ISMS、プライバシーマークの運営部署と、社内インフラ管理部署のメンバーにより構成されています。

活動内容
OGIS-CSIRTは、以下の活動を実施しています。
・ 脆弱性情報、脅威情報の収集と社内への通知
・ 社内における脆弱性情報への対応検討と対応依頼
・ 各種の監視と検知時の対応
・ CSIRT活動に関わる訓練
・ 社内へのサイバーセキュリティインシデント発生時の対応・支援
・ サイバーセキュリティ関連の動向調査
・ 外部関連機関との連携（日本シーサート協議会、JPCERT/CC 等）

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NTT EAST-CIRT

チームの正式名称	NTT EAST Cyber Incident Response Team
チームの略称	NTT EAST-CIRT
所属する組織名	東日本電信電話株式会社
設立年月日	2013-07
チームの Email アドレス	cyber_info-gm@east.ntt.co.jp
チームサイト	
所属組織サイト	http://www.ntt-east.co.jp/
加盟年月	2013 年 07 月

1. 概要

NTT EAST-CIRT は東日本電信電話株式会社 (NTT 東日本) の組織内 CSIRT です。NTT グループ各社のセキュリティ関連組織と連携し、NTT 東日本および NTT 東日本グループ各社のサイバーセキュリティ対策の推進に取り組んでいます。

2. 設立の経緯・背景

NTT 東日本では、NTT EAST-CIRT 設立以前から、サイバー攻撃対策活動を進めていましたが、攻撃が高度化・巧妙化している実態を踏まえ、更なる対応 (意思決定) スピードの向上とガバナンスの強化を目的に、サイバー攻撃対策専門組織として NTT EAST-CIRT が設立されました。

3. 会社内における位置づけおよび活動内容

NTT 東日本には、業務運営実態に合わせて複数のサイバー攻撃対策組織がありますが、NTT EAST-CIRT は、自社の企業情報システムへのサイバー攻撃に対して、主に技術的な側面を担う組織として活動するとともに、社内のサイバー攻撃対策組織間の連携を図ることで、NTT 東日本全体のサイバー攻撃対応力強化に取り組んでいます。

以下活動のサイクルを回すことで、活動の質を継続的に向上させています。
・基準設定 ：セキュリティ対策ガイドラインの策定
・脆弱性診断 ：各システムのセキュリティ検査、システム機能の棚卸し
・脆弱性解消 ：事前のチェックに基づく適正な対策の実施
・セキュリティ監視 ：攻撃発生の早期検知
・インシデント対応 ：被害範囲や深刻度の確認、および早期解決
・情報統制 ：情報の一元的集約、および社内外組織への速やかな報告・連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

OK-CSIRT

チームの正式名称	大阪教育大学CSIRT
チームの略称	OK-CSIRT
所属する組織名	国立大学法人大阪教育大学
設立年月日	2017/04/01
チームの Email アドレス	csirt@ml.osaka-kyoiku.ac.jp
チームサイト	https://noc.cc.osaka-kyoiku.ac.jp/csirt/
所属組織サイト	https://osaka-kyoiku.ac.jp/
加盟年月	2018 年 07 月

1. 概要

国立大学法人　大阪教育大学
大阪府柏原市と大阪市天王寺に大学のキャンパスを持つほか，大阪府下に11の附属小・中・高等学校，幼稚園，特別支援学校を持っています。
https://osaka-kyoiku.ac.jp/

OK-CSIRT
学内情報システムの管理運用をおこなう情報処理センターと，事務システムの管理・運用をおこなう情報企画室をバーチャルが統合した情報基盤統括室の教職員によって構成されるチームです。
情報処理センター長を責任者として，センター教員，技術系職員，事務職がメンバーです。

2. 設立の経緯・背景

深刻化する情報セキュリティインシデントに対応するために，2017年に学内の情報セキュリティポリシーの全面改訂をおこない，同時に，学内の情報に関する組織の抜本的見直しを行いました。
その際，情報セキュリティインシデントに対応する実働組織としてOK-CSIRTを設置しました。

3. 会社内における位置づけおよび活動内容

(学内の位置づけ)
インシデント発生時，対策の遅れが被害の拡大につながるおそれがあり，緊急を要する場合は，CSIRT責任者の判断でネットワーク停止等を実施し，最高情報セキュリティ責任者へは事後報告・承認でよいと学内ルールで定めており，従来の組織にとらわれず迅速に行動できる立場です。
大学だけでなく，附属学校のインシデントにも対応します。
参考　「国立大学法人大阪教育大学情報セキュリティインシデント対応チーム要項」
http://goose.bur.osaka-kyoiku.ac.jp/doc/campus/rule/727.html
(活動内容)
インシデント対応，学内への注意喚起等
役員，教職員，学生へのセキュリティ教育等も業務内容に含まれますが，これらは情報基盤統括室で実施しており，OK-CSIRTはインシデント対応を重点的におこなっています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

NTT WEST-CIRT

チームの正式名称	NTT WEST Cybersecurity Incident Response Team
チームの略称	NTT WEST-CIRT
所属する組織名	西日本電信電話株式会社
設立年月日	2013-12-01
チームの Email アドレス	nttwest-cirt-hq@west.ntt.co.jp
チームサイト	
所属組織サイト	http://www.ntt-west.co.jp/
加盟年月	2015 年 04 月

1. 概要

西日本電信電話株式会社 (NTT西日本) は、NTTグループで西日本地域の市内通話やフレッツ光などの通信サービスを提供する事業会社です。NTT WEST-CIRT は、NTT西日本および NTT西日本のグループ会社で発生したサイバーセキュリティインシデントに対応します。

2. 設立の経緯・背景

NTT西日本における、サイバーセキュリティ対策への認識の高まりを受け、2013 年 12 月に技術革新部へ CSIRT 組織を立ち上げ、さらに 2014 年 7 月からはグループ会社である NTTネオメイトに、サイバーセキュリティオペレーションセンタ (CSOC) を発足させました。

3. 会社内における位置づけおよび活動内容

(会社内における位置づけ)
CSOC は NTT西日本グループの CSIRT 業務と SOC 業務を担っており、NTT西日本グループで発生したサイバーセキュリティインシデントを一元的に対応しています。また必要に応じて関連部署 (業務主管、システム主管、運用主管、及びネットワーク管理者など) とも協力します。NTTグループ内外の連携及び情報共有は、グループ代表 PoC である NTT 持株会社 NTT-CERT の支援を受けます。また NTTグループ各社の CSIRT および SOC 部署とも連携及び情報共有をしています。

(活動内容)
NTT西日本グループのセキュリティインシデントに関する窓口として、社内外から情報は全て受け付けています。社内で発生したサイバーセキュリティに関わるインシデントレスポンス業務のほかに、監視分析業務、脆弱性管理業務、セキュリティ技術高度化業務を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

OKI-CSIRT

チームの正式名称	OKI Computer Security Incident Response Team
チームの略称	OKI-CSIRT
所属する組織名	沖電気工業株式会社 丸紅OKIネットソリューションズ株式会社
設立年月日	2008-05
チームの Email アドレス	oki-csirt@oki.com
チームサイト	
所属組織サイト	http://www.oki.com
加盟年月	2008 年 08 月

1. 概要

OKI-CSIRT は、沖電気工業株式会社 (http://www.oki.com/jp/、以降 OKI) と丸紅 OKI ネットソリューションズ株式会社 (http://www.om-nix.com/、以降 om-nix) によって運営されている OKI グループの CSIRT です。

OKI は通信機器や現金自動預け払い機 (ATM) などの情報機器メーカーとして知られていますが、他にもシステムインテグレーションをはじめとする情報通信関連の事業も行なっています。一方、om-nix は 2005 年 ※に OKI のネットワークインテグレーション・サービス事業を行なっていた部門を独立させて設立した会社です。

※ 2005 年時点は、沖電気ネットワークインテグレーション株式会社として設立し、その後 2011 年に丸紅 OKI ネットソリューションズ株式会社に商号変更。

2. 設立の経緯・背景

OKI-CSIRT は、2007 年に発生した USB メモリを介して広まるウイルスへの感染をきっかけに、OKI の情報企画部と om-nix の「セキュリティセンタ」双方のメンバーから構成される仮想的なチームとして 2008 年に設置されました。

3. 会社内における位置づけおよび活動内容

OKI-CSIRT は OKI グループ内で発生したインシデントに対して直接対応を行なう組織内 CSIRT としての役割を担っているだけでなく、OKI グループ向けの分析センターとしての機能も有し、グループ内や顧客で発生したインシデントの原因分析やウイルスの動作解析などを行なうこともあります。

実際のインシデント対応においては、OKI-CSIRT は技術的な部分のみを担当し、発生したインシデントに対して経営層などが意思決定するために必要な情報を収集、分析、整理します。一方、情報企画部は OKI-CSIRT から得た技術情報を元にあらかじめ決められた基準に従って意思決定を行なったり、経営層の指示を仰いだ上でグループ内の該当部署に対応を指示したりします。

なお、OKI-CSIRT は、OKI グループの「品質保証」の一環として「お客様の場所にウイルスを持ち込ませない」ことを第一に活動していることから、その活動は、情報企画部だけでなく、品質保証部からも支援を受けています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

OKWAVE-CSIRT

チームの正式名称	オウケイウェイヴ CSIRT
チームの略称	OKWAVE-CSIRT
所属する組織名	株式会社オウケイウェイヴ
設立年月日	2017年4月1日
チームの Email アドレス	okwave-csirt@okwave.co.jp
チームサイト	https://www.okwave.co.jp/about/policy/#policy05
所属組織サイト	https://www.okwave.co.jp/
加盟年月	2017 年 10 月

1. 概要

株式会社オウケイウェイヴは『互い助け合いの場の創造を通して、物心両面の幸福を実現し、世界の発展に寄与する』ことを目指し、利用者同士が助け合いを行うQ&Aサイト「OKWAVE」を2000年1月より運営し、法人向けにはFAQシステム「OKBIZ. for FAQ / Helpdesk Support」、顧客参加型サポートコミュニティツール「OKBIZ. for Community Support」などを400サイト以上に導入しています。

OKWAVE-CSIRTは株式会社オウケイウェイヴの組織内CSIRTで、社内で管理するITシステム全般を活動範囲とし、
1. セキュリティインシデントが発生した際の初期消火活動
2. 社内・社外への情報共有や連絡窓口
3. セキュリティインシデントの発生を抑制するための活動
4. セキュリティ対策の考案やレビュー

を行います。

2. 設立の経緯・背景

巧妙化するサイバー攻撃に対し、従来の予防的な措置のみでは防ぎきる事はできず、有事の迅速な対応が求められる状況となっております。
そのため弊社では、サイバー攻撃を受けた際、組織としての迅速な初動対応により被害の拡大を防ぐ事を目的にとしてCSIRTを設立いたしました。

3. 会社内における位置づけおよび活動内容

OKWAVE-CSIRTは 各事業部門・管理部門のシステム運用担当を中心メンバーとして構成されており、CISO直轄の組織として設置されています。
株式会社オウケイウェイヴの提供するサービスおよび社内のシステムにおける情報セキュリティインシデントに対応します。
緊急時には経営層へのエスカレーションや関係部署との調整など、インシデント対応の中核的役割を担って被害拡大を防ぎます。
平時は、脆弱性情報の収集、各システムのセキュリティ品質向上支援、セキュリティ啓蒙活動などに努めています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

OLYMPUS-CIRT

チームの正式名称	OLYMPUS Cyber Incident Response Team
チームの略称	OLYMPUS-CIRT
所属する組織名	オリンパス株式会社
設立年月日	2015-06-01
チームの Email アドレス	olympus-cirt@ot.olympus.co.jp
チームサイト	
所属組織サイト	http://www.olympus.co.jp/
加盟年月	2015 年 09 月

1. 概要

OLYMPUS-CIRT は、オリンパス株式会社によって運営されているオリンパスグループの組織内 CSIRT です。

2. 設立の経緯・背景

弊社では、以前から様々な情報セキュリティ対策を実施してきましたが、昨今のサイバー攻撃の高度化・巧妙化に伴い、オリンパスグループ内でのインシデント情報共有と、インシデント発生時の迅速かつ適切な対応を目的として、2015 年 6 月に「OLYMPUS-CIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

会社内における位置づけ
・IT 部門内の OLYMPUS-CIRT 事務局が中心となり、インシデント発生時にはその内容に応じて IT 部門内から適切なメンバーが参画する仮想的なチームです。

活動内容
・インシデント情報の共有
・インシデント対応

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

OMRON-SIRT

チームの正式名称	OMRON-SIRT
チームの略称	OMRON-SIRT
所属する組織名	オムロン株式会社
設立年月日	2017年4月1日
チームの Email アドレス	omron-sirt@omron.com
チームサイト	
所属組織サイト	http://www.omron.co.jp/
加盟年月	2018 年 02 月

1. 概要

オムロンは、世界中の社会的課題を、事業を通して解決することで世の中の人々からその存在を必要とされ、期待される企業を目指します。

1933年の創業以来、わたしたちを取りまく社会は大きく変化してきました。オムロンは、1959年に制定した社憲「われわれの働きで　われわれの生活を向上し　よりよい社会をつくりましょう」を発展の原動力と求心力とし、よりよい社会をつくるための「ソーシャルニーズ」を世に先駆けて創造してきました。

OMRON-SIRT（OMRON Security Incident Response Team）は、オムロン株式会社によって運営される、オムロングループの情報セキュリティ体制の整備・強化を進める組織内CSIRTです。

2. 設立の経緯・背景

高度化・巧妙化するサイバーセキュリティに対し、オムロングループ全体で全社横断的な情報セキュリティ対策活動を推進する組織として、2017年4月にOMRON-SIRTを設立しました。

3. 会社内における位置づけおよび活動内容

(1) 位置づけ
OMRON-SIRTは、オムロン株式会社の情報システム統括部門内に設置された組織です。情報システムに関するセキュリティインシデント情報及び脆弱性情報の収集とインシデント対応時の窓口を担うとともに、オムロングループにおける全社横断的な情報セキュリティに関する会議体を主催し、オムロングループ全体の情報セキュリティ対策の推進に取り組んでいます。

(2) 活動内容
・セキュリティインシデント情報及び脆弱性情報の収集と、インシデント対応
・全社横断的な会議体の運営と、全社共通課題の確認及び対応方針の決定
・オムロングループ全体の情報セキュリティリスク対応策の実行指示
・情報セキュリティに関する状況レポートの取りまとめ

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ORIX-SIRT

チームの正式名称	ORIX SIRT
チームの略称	ORIX-SIRT
所属する組織名	オリックス株式会社
設立年月日	2015年10月1日
チームの Email アドレス	orix_sirt@orix.jp
チームサイト	
所属組織サイト	http://www.orix.co.jp/grp/
加盟年月	2018 年 02 月

1. 概要

オリックスグループはリースに始まり、銀行、保険、水族館さらに発電所まで、世の中の変化に対応しながら、あらたなビジネスフィールドへ常にチャレンジを続ける企業集団です。ORIX SIRTはこの多種多様な事業を展開する個社の集合体であるグループ全体をカバーするCSIRTです。

2. 設立の経緯・背景

世界的なサイバー脅威の高まり、国内での重大インシデント発生、自組織内で発生するインシデント疑い事案の増加、などを背景に、それまでIT組織内のみで対応していたインシデント対応体制の整備が経営課題として認識されるようになりました。それまでも一定のサイバーセキュリティ対応は行っていましたが、より経営的な視点からインシデント対応などを行うことを可能とするため、グループ全体を統括する本社機構として2015年10月に専任メンバーで構成されるORIX SIRTが設立されました。

3. 会社内における位置づけおよび活動内容

＜位置づけ＞
グループ全体のサイバーセキュリティを担う本社組織として設立。インシデント発生時の対応、予防活動、情報セキュリティに関する規定整備や教育啓蒙活動などについて関係各部門と連携しながら、主導的に実施していく役割を負っています。

＜活動内容＞
・脆弱性情報の収集及び対策方針の決定
・インシデント発生時のコントローラー機能、発生部門への指示、支援
・情報セキュリティに関するポリシー、規則等の立案
・情報セキュリティに関する教育・啓蒙
・各部門・グループ会社での情報セキュリティ活動の支援・組織化
・セキュリティ関連外部団体との連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Otsuka-CSIRT

チームの正式名称	大塚製薬 CSIRT
チームの略称	Otsuka-CSIRT
所属する組織名	大塚製薬株式会社
設立年月日	2016年7月26日
チームの Email アドレス	OPC-CSIRT@otsuka.jp
チームサイト	
所属組織サイト	https://www.otsuka.co.jp
加盟年月	2017 年 07 月

1. 概要

大塚製薬は「Otsuka-people creating new products for better health worldwide」の企業理念のもと、世界の人々の健康に貢献する革新的な製品を提供しています。
OTSUKA-CSIRTは大塚グループ全体での安定した製品供給に向け、サイバーテロ等のセキュリティ脅威への対策・体制の強化に努めます。

2. 設立の経緯・背景

これまでもIT部門を中心にインシデント対応を行ってきましたが、2015年12月に経済産業省より「サイバーセキュリティ経営ガイドライン」が発表され、経営の観点でサイバー攻撃から企業を守るリスク管理の必要性が高まってきました。また、欧州の一般データ保護規則（GDPR）における情報漏えい時の報告義務に対応するため、グローバルでの体制強化が求められます。それを受け、2016年7月に海外を含めた大塚グループ全体でサイバーセキュリティへの対策・体制の強化を図るべく、OTSUKA-CSIRTが設立されました。

3. 会社内における位置づけおよび活動内容

親会社の大塚ホールディングスが各社CSIRTを統制する組織としてグループ全体の運営方針やルールの策定を行っています。大塚製薬ではその運営方針に基づき、IT・コンプライアンス部門を中心にサイバーセキュリティへの対策・体制の強化に努めています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Pasona-CSIRT

チームの正式名称	Pasona Computer Security Incident Response Team
チームの略称	Pasona-CSIRT
所属する組織名	株式会社パソナグループ
設立年月日	2017年5月1日
チームの Email アドレス	csirt@pasonagroup.co.jp
チームサイト	http://www.pasonagroup.co.jp/utility/security.html
所属組織サイト	http://www.pasonagroup.co.jp/index.html
加盟年月	2017 年 06 月

1. 概要

株式会社パソナグループは人材派遣のリーディングカンパニー　パソナを中心に国内・海外で人材ビジネスを展開する会社です。　Pasona-CSIRT は、株式会社パソナグループにより運営されている CSIRT です。

2. 設立の経緯・背景

セキュリティ対策とインシデント対応について、組織的な対応の実施や現場支援を行い、外部組織とも連携をとりながら適切な危険予知を実施することを目的として設置しました。

3. 会社内における位置づけおよび活動内容

会社内における位置づけ:
Pasona-CSIRTはパソナグループ経営会議の下に設置しております。
Pasona-CSIRTはパソナグループ情報セキュリティ本部長を代表とし、事務局は情報セキュリティ本部のメンバーが兼任します。　パソナグループIT統括部のグループ長、及びパソナグループ各社のCSIRT代表はPasona-CSIRTのメンバーとします。

活動内容:
パソナグループを代表して日本シーサート協議会に加盟し、情報収集し、パソナグループ各社に展開します。
CSIRTとしての活動はセキュリティインシデント対応訓練、セキュリティインシデントの監視、セキュリティインシデント発生時の対応などインシデント対応に絞った活動を行っています。　その他、情報セキュリティ本部の活動として、グループ各社のセキュリティ対応状況を確認と教育・啓蒙活動、内部監査の活動を実施しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

PCA-CSIRT

チームの正式名称	PCA-CSIRT
チームの略称	PCA-CSIRT
所属する組織名	ピー・シー・エー株式会社
設立年月日	2015 年　7 月 21 日
チームの Email アドレス	pca-csirt@pca.co.jp
チームサイト	
所属組織サイト	http://pca.jp/
加盟年月	2017 年 01 月

1. 概要

ピー・シー・エー株式会社は、中堅・中小企業向けの会計・販売管理等業務ソフト・クラウドサービスを提供しています。PCA-CSIRT は ピー・シー・エー株式会社によって運用される組織内の CSIRT です。

2. 設立の経緯・背景

社内での情報共有、セキュリティインシデント検知能力の向上、セキュリティインシデント発生時の対応能力向上を目的として「PCA-CSIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

PCA-CSIRT は情報セキュリティインシデントに対して、社内関連部門・リスク管理委員会などと連携を図りながら部署横断的に活動するチームです。

主な活動として
・セキュリティリスク評価・分析
・セキュリティ情報の共有（脆弱性情報等）
・セキュリティ情報の提供（啓蒙、教育、注意喚起）
・セキュリティインシデントハンドリング

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

PCC-CSIRT

チームの正式名称	POCKETCARD CSIRT
チームの略称	PCC-CSIRT
所属する組織名	ポケットカード株式会社
設立年月日	2017年3月1日
チームの Email アドレス	pcc-csirt@pocketcard.co.jp
チームサイト	
所属組織サイト	http://www.pocketcard.co.jp
加盟年月	2018 年 02 月

1. 概要

ポケットカード株式会社は「暮らしに密着した付加価値の高いサービスを創造する」を企業ビジョンに掲げ、クレジットカード事業およびカード会員様向けの保険代理店事業を行っています。
PCC-CSIRT は、ポケットカード株式会社が保有する情報資産に関するインシデントの未然防止およびインシデント発生時における被害の最小化を目的とした組織内CSIRTです。

2. 設立の経緯・背景

当社が事業活動を通じてお客様等からご提供頂いた情報は、クレジットカードサービスの価値向上の礎となる最重要資産であると認識しています。その資産をサイバー攻撃から守るべく、情報システム部門にて様々なセキュリティ強化策を講じてきましたが、迅速かつ適切なインシデント対応を行うには部門横断型のチームが必要であるという考えに至り、CSIRTを設立致しました。

3. 会社内における位置づけおよび活動内容

【位置づけ】
PCC-CSIRTは情報システム部門を中心としたメンバーで構成され、社内外の情報共有・インシデント対応を担当します。

【活動内容】
・外部機関との連絡窓口
・セキュリティ関連情報の収集・社内展開
・セキュリティインシデント発生時の初動対応
・脆弱性情報の収集・モニタリング
・情報セキュリティ教育、セキュリティ対応訓練の実施
・セキュリティ関連団体の活動への参加と情報交換

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

PERSOL-SIRT

チームの正式名称	パーソルグループSIRT
チームの略称	PERSOL-SIRT
所属する組織名	パーソルホールディングス株式会社
設立年月日	2015-10-01
チームの Email アドレス	cybersecurity@persol.co.jp
チームサイト	
所属組織サイト	https://www.persol-group.co.jp
加盟年月	2016 年 03 月

1. 概要

パーソルグループ SIRT (PERSOL-SIRT) はパーソルホールディングス株式会社が運営する組織内 CSIRT です。

2. 設立の経緯・背景

従来より、セキュリティインシデント対策についておこなってきましたが、2015 年 5 月よりパーソルグループとしてのインフラ共通基盤の稼働や基幹システムの統合などが始まり、部署間だけでなく各グループ会社間でのインシデント対応や情報共有が求められるようになりました。
そのような状況の中、グループ IT インフラを統括するメンバーを中心に 2015 年 10 月よりセキュリティインシデントを一元的に管理し始め、CSIRT (PERSOL-SIRT) の設立となりました。
昨今のサイバー攻撃をはじめとした巧妙化・複雑化するセキュリティインシデントへの対応をするうえで、情報収集面や知識面で他社との連携、情報共有は欠かせないと考え、日本シーサート協議会への加盟を通じ、よりセキュリティ強化につながることを期待しています。

3. 会社内における位置づけおよび活動内容

【会社内における位置づけ】
PERSOL-SIRT は、パーソルホールディングス株式会社グループ IT 本部サイバーセキュリティ部の統制下の組織横断の仮想組織と位置付けられています。

【活動内容】
PERSOL-SIRT は、NIST サイバーセキュリティフレームワークをもとに策定した対応ガイドラインに準拠した対応をおこない、その判定結果をもとに以下の項目について支援します。
・インシデント分類と分析
・インシデント初期対応
・インシデント解決
・対応フローの改善

「サイバー空間」において、システム内に存在する情報資産の脅威が発生している、もしくは、脅威につながる可能性がある事象をセキュリティインシデントと定義します。PERSOL-SIRT が対応するセキュリティインシデントを以下の 7 領域に分類しています。
1.サイバー侵入
2.サービス拒否 (DoS 攻撃)
3.内部犯行
4.マルウェア感染
5.ソーシャルエンジニアリング
6.ウェブサイト改ざん
7.その他 (発生理由不明)

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

PH-CSIRT

チームの正式名称	PHC Cyber Security Incident Response Team
チームの略称	PH-CSIRT
所属する組織名	PHCホールディングス株式会社
設立年月日	2015年4月1日
チームの Email アドレス	phcsirt@ml.phchd.com
チームサイト	
所属組織サイト	https://www.phchd.com/jp/
加盟年月	2016 年 09 月

1. **概要**
   PH-CSIRTは、PHCホールディングス株式会社により運営されている、PHCホールディングスグループを対象とした組織内CSIRTです。
2. **設立の経緯・背景**
   PHCホールディングスグループは、これまでも情報セキュリティ活動を実施してきましたが、サイバー攻撃の高度化・巧妙化に伴い、事故発生時に迅速に対応しリスクを極小化する事を目的として、2015年4月にCSIRTの組織を設置しました。(2018年4月にパナソニックヘルスケアホールディングス株式会社からPHCホールディングス株式会社に社名変更)
3. **会社内における位置づけおよび活動内容**
   PH-CSIRTは、PHCホールディングスグループ内　脅威情報の共有・脆弱性管理・インシデント対応を中心に活動を行なっています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

QSIRT

チームの正式名称	QualitySoft Security Incident Response Team
チームの略称	QSIRT
所属する組織名	クオリティソフト株式会社
設立年月日	2017 年 5 月 1 日
チームの Email アドレス	csirt@qualitysoft.com
チームサイト	
所属組織サイト	https://www.qualitysoft.com
加盟年月	2018 年 05 月

1. 概要

クオリティソフト株式会社では、IT 資産管理・エンドポイントセキュリティなどの、パッケージソフトウェアとクラウドサービス及びアプライアンス製品の開発及び販売業務を行っています。
QSIRT は、クオリティソフト社内のセキュリティ管理体制をベースとした、組織横断的な CSIRT で、自組織のインシデントの防止や、発生時の対応を実施しています。

2. 設立の経緯・背景

これまでは情報システム部門を中心としたインシデント対応が実施されていましたが、サイバー攻撃の巧妙化や、大規模化により、単独部門での対応が困難になることが考えられます。
ISO27001 認証取得に合わせ、組織としてのインシデント対応体制を構築し、あわせて CSIRT を設立しました。

3. 会社内における位置づけおよび活動内容

情報セキュリティ管理責任者を中心とした、情報システム部門、人事総務部門などを含む、組織横断型の CSIRT で、社内の各部署に配置された ISMS 推進担当者との連携を持ちます。
通常時の活動は、脆弱性やセキュリティインシデントの情報収集や社内共有、社内の脆弱性への対策、セキュリティに関する社内教育などを実施しています。
また、これらの情報を自社製品の企画部門や開発部門にフィードバックする活動なども行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Panasonic CSIRT

チームの正式名称	Panasonic Cyber Security Incident Response Team
チームの略称	Panasonic CSIRT
所属する組織名	パナソニック株式会社
設立年月日	2014-01-01
チームの Email アドレス	Panasonic_CSIRT@gg.jp.panasonic.c
チームサイト	
所属組織サイト	http://www.panasonic.com/jp/home.html
加盟年月	2014 年 09 月

1. 概要

Panasonic CSIRT は、パナソニック株式会社によって運営されているパナソニックグループの CSIRT です。

当社は 1918 年の創業以来、事業を通じて世界中の皆様の「くらし」の向上と社会の発展に貢献することを基本理念とし、あらゆる活動を行ってまいりました。

常に「人」を中心に置き、その「くらし」をみつめ、より良いものにしていく
— それが今も昔も変わらないパナソニックの原点です。
そして今、私たちが目指すのは、お客様にとっての「いいくらし」をあらゆる空間に拡げていくことです。

家の中から、オフィス、店舗、自動車、航空機、さらに街まで、お客様が活動する様々な空間において、ハードウェア単品だけでなく、ソフト、サービスを含めたトータルソリューションを提供し、お客様一人ひとりにとってのより良いくらし、より良い世界 ～「A Better Life, A Better World」を追求してまいります。

2. 設立の経緯・背景

社内外からのセキュリティ脅威が年々増加し、かつ高度化する状況の中、Panasonic CSIRT は、情報システム部門のメンバーから構成されるチームとして 2014 年に設置されました。

3. 会社内における位置づけおよび活動内容

Panasonic CSIRT は、社内各事業場、関係機能との連携の元、パナソニックグループ内で発生する情報システムへのインシデントに対する未然防止のための調査・分析とリスク情報の共有、ならびにインシデント解決支援を軸に活動を行なっています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Rakuten-CERT

チームの正式名称	Rakuten Computer Emergency Response Team
チームの略称	Rakuten-CERT
所属する組織名	楽天株式会社
設立年月日	2007-11-15
チームの Email アドレス	rakuten-cert@mail.rakuten.com
チームサイト	
所属組織サイト	https://www.rakuten.co.jp/
加盟年月	2007年12月

1. 概要

Rakuten-CERT は、ネットショッピングをはじめとするインターネット総合サービスを提供している楽天株式会社 (https://www.rakuten.co.jp/) の CSIRT です。

2. 設立の経緯・背景

Rakuten-CERT が正式に活動を開始したのは 2007 年末ですが、それ以前から CSIRT のようなセキュリティ対応体制は整備されていました。その一方で、楽天のセキュリティ対応体制の中心にある「開発部システムセキュリティグループ (現：IT Security Engineering Office)」では、不審なアクセスを行なっているアクセス元の ISP に対応を依頼しなければならない事態など、自社単独での対応が難しいインシデントが今後増加していくであろうとの予想の下、そのようなインシデントに対応するための方策を検討していました。

3. 会社内における位置づけおよび活動内容

Rakuten-CERT の特徴は、その中心となる部署が「IT Security Engineering Office」であることが示すように、楽天グループが提供している自社開発の Web サービスを主な対象にしている点です。

具体的には、楽天グループ内で開発した Web サービスシステムの脆弱性などに起因するインシデントに対して、発生の未然防止、被害拡大の抑止、再発防止などを目的とし、楽天グループ内の開発部門をセキュリティの面で統括しています。このように Rakuten-CERT は楽天グループ内の「コーディネーションセンター」としての役割を果たす一方、自社開発の Web アプリケーションの脆弱性に対応するという点では、メーカーにおいて自社製品の脆弱性対応を行なう CSIRT である「ベンダチーム」のような機能も有しています。

Rakuten-CERT は「IT Security Engineering Office」の常勤メンバーを中心に、楽天グループの様々なサービスの開発を担当する Development Unit のメンバーによって構成されています。また、緊急時には Development Unit の取締役と連携し、リスク情報がエスカレーションされ、意思決定される形になっていますが、あらかじめ決められた基準に従い、Rakuten-CERT 自身の意思決定によって作業指示が行なわれることもあります。

一方、Rakuten-CERT は社内教育に特に力を入れており、ものづくりの部署には脆弱性を作りこませないための厳しい教育を行なっています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Recruit-CSIRT

チームの正式名称	Recruit Cyber Security Incident Response Team
チームの略称	Recruit-CSIRT
所属する組織名	株式会社リクルート
設立年月日	2013-08-01
チームの Email アドレス	csirt@r.recruit.co.jp
チームサイト	
所属組織サイト	http://www.recruit.jp/
加盟年月	2014 年 05 月

1. 概要

Recruit-CSIRT は、販促メディア事業、人材メディア事業など幅広い事業領域でサービスを提供するリクルートの CSIRT です。

2. 設立の経緯・背景

リクルートグループの共通インフラの構築・運用を担うリクルートテクノロジーズは、サイバー攻撃への対応能力向上を目的として、自社の CSIRT である R-tech Cyber Incident Team を 2013 年 8 月に設立し、2014 年 6 月に日本シーサート協議会に加盟しました。

その後、リクルートホールディングスが中心となったグループ全体のサイバー攻撃対応およびインシデント対応を推進する体制が整ったため、2015 年 4 月にリクルートグループ全体の CSIRT である Recruit-CSIRT として再出発することになりました。

2018年4月のグループ組織再編にともない、メディア&ソリューション事業の統括会社であるリクルートのCSIRTと位置づけられることになりました。

3. 会社内における位置づけおよび活動内容

Recruit-CSIRT は、リクルートセキュリティマネジメント部ソリューションマネジメントGおよびリクルートテクノロジーズサイバーセキュリティエンジニアリング部からなる、リクルート配下の事業会社・機能会社へのセキュリティ支援のための仮想組織です。

Recruit-CSIRT の主な活動は以下の通りです。

(1)セキュリティインシデント対応支援
-インシデント発生時の技術支援
-社外関連組織との連携
-早期警戒
など

(2)グループ共通インフラのセキュリティ監視
-不正アクセスの検知、遮断
-イベントの詳細分析
-フォレンジック
など

(3)平時のセキュリティ品質向上
-脆弱性診断
-脆弱性情報の収集および展開
-開発者教育
など

リクルート配下の国内外の事業会社・機能会社に加えて、株式会社スタッフサービス・ホールディングスおよび株式会社リクルートスタッフィングが支援の対象となります。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Resona-CSIRT

チームの正式名称	Resona-CSIRT
チームの略称	Resona-CSIRT
所属する組織名	株式会社りそなホールディングス
設立年月日	2014-03-17
チームの Email アドレス	Resona.CSIRT@resona-hd.co.jp
チームサイト	
所属組織サイト	http://www.resona-gr.co.jp/
加盟年月	2014 年 03 月

1. 概要

りそなホールディングスは、銀行持株会社として、銀行その他銀行法により子会社とすることができる会社の経営管理ならびにこれに付帯する業務を行うことを事業目的としています。

2. 設立の経緯・背景

高度化・巧妙化しているサイバー攻撃やセキュリティインシデントに対して早期に解決するための組織として、CSIRT グループを設置しました。

3. 会社内における位置づけおよび活動内容

IT 企画部に設置した CSIRT グループがセキュリティインシデント対応を担当します。
【活動内容】
・発生したインシデントの被害極小化
・インシデントの発生抑制
・社内セキュリティ品質の向上
・外部機関との連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Rohto-SIRT

チームの正式名称	Rohto Security Incident Response Team
チームの略称	Rohto-SIRT
所属する組織名	ロート製薬株式会社
設立年月日	2013/11/01
チームの Email アドレス	Rohto-sirt@rohto.co.jp
チームサイト	
所属組織サイト	http://www.rohto.co.jp
加盟年月	2018 年 07 月

1. 概要

正式社名「ロート製薬株式会社」。英文社名「ROHTO PHARMACEUTICAL CO., LTD.」。製薬業。明治32年(1899)「信天堂山田安民薬房」創業。昭和24年(1949)設立。本社は大阪市生野区巽西。大衆向け目薬のシェアトップクラス。子会社に米国メンソレータムなど。東京証券取引所第1部上場。証券コード4527。現在はスキンケア製品を中心に中国、ベトナム、インドネシアなどアジアを中心に海外展開もしております。

2. 設立の経緯・背景

増え続ける脅威への対策、セキュリティ事故発生時の被害を最小減にとどめるために「CSIRT（Computer Security Incident Response Team）を社内に設置しました。
2017年9月にココロートパークという会員制WEBサイトがパスワードリストアタックを受け個人情報が漏えいしてしまい、従来の情報セキュリティ委員会がCSIRTとして活動することを宣言して窓口を設けております。

3. 会社内における位置づけおよび活動内容

通常時にセキュリティの品質向上や従業員のセキュリティ意識向上教育を行う「セキュリティ委員会」が、有事の折に「CSIRT」として機能する。
危機管理の最高責任者をトップに、経営企画部長、人事部長、お客様対応の部門長、情報システム部長、情報セキュリティ委員会事務局から構成されます
CSIRTの下位組織としてSOC（セキュリティオペレーションセンター）が存在しておりまして、実務的なインシデント対応、脆弱性情報の共有、教育などの施策を行っております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

RS-CIRT

チームの正式名称	Risk Solutions - Cybersecurity Incident Response Team
チームの略称	RS-CIRT
所属する組織名	株式会社JMCリスクソリューションズ
設立年月日	2016/04/01
チームの Email アドレス	rs-cirt@jmc.ne.jp
チームサイト	
所属組織サイト	http://rs.jmc.ne.jp/
加盟年月	2018 年 07 月

1. 概要

株式会社JMCリスクソリューションズのRS-CIRTは、情報セキュリティコンサルティングやセキュリティ診断の経験を基に、お客様のCSIRTと連携することで、ひとつ先を予測するオーダーメイド対策をご提供しております。

2. 設立の経緯・背景

甚大な被害のインシデントを目の当たりにして常に痛感することは、「予測していたことにもっと早く手を打てていれば、被害が最小限に抑えられていたかもしれない・・」ということです。
高度化するサイバー攻撃に対し単独のCSIRTではインシデントの早期発見及び兆候の検知が困難な状況になってきました。
そこで、弊社を媒介として、お客様のCSIRT間の連携を強めることで、「ひとつ前へ、一歩先へ」手を打つ、攻めのセキュリティ実現のため、RS-CIRTを設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置付け
・社内のCSIRT機能
・RS-CIRTが連携するお客様CSIRTへの情報発信、体制整備、教育訓練等のサービス提供

(2)活動内容
・平常時
お客様CSIRTの体制整備を中心に、現場で起こっている様々な事象を弊社RS-CIRTをハブとして集約することで、連携する全てのお客様CSIRTへ横展開を図り、インシデントの兆候を早期に捉え情報共有を行っております。
またRS-CIRTでは、自社で収集している定点観測データを分析し、先の攻撃予測を月例で行うことで、お客様への情報発信に加え教育訓練支援へ活用しております。
・緊急時
インシデント発生後の対応フォローも必要に応じて行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

S2SIRT

チームの正式名称	セガサミーサート
チームの略称	S2SIRT
所属する組織名	株式会社　セガホールディングス
設立年月日	2015年1月1日
チームの Email アドレス	S2SIRT@sega.com
チームサイト	
所属組織サイト	http://sega.co.jp/
加盟年月	2017年11月29日

1. 概要

(1)会社概要
セガグループは、コンシューマ事業、アミューズメント機器事業、トイ・映像事業、アミューズメント施設事業の4つの事業グループを手掛け、様々なエンタテインメントを通じて世界中のお客様に感動体験をお届けしています。(株)セガホールディングスは、セガグループを統括する中間持株会社です。

(2)会社沿革
1960年(昭和35年):セガの前身となる日本娯楽物産(株)設立
1965年(昭和40年):(株)セガ・エンタープライゼスに商号変更
2000年(平成12年):(株)セガに商号変更
2015年(平成27年):セガグループ再編に伴い、(株)セガホールディングス設立

2. 設立の経緯・背景

(1)CSIRT設立日
2015年1月1日

(2)CSIRT設立経緯
2011年6月の欧州子会社における個人情報漏えい事故を機に、国内子会社/海外子会社を含むセガグループ全社を対象としたセキュリティルールを策定し、情報セキュリティに対する本格的な取り組みを開始しました。
その後は兼任体制にて、情報セキュリティに関する活動を推進してきましたが、セガグループ再編に伴い、対象範囲の拡大や体制・対応等の強化を目的として、情報セキュリティに特化した専門組織を2015年1月に設立しました。

3. 会社内における位置づけおよび活動内容

セガグループにおける唯一の情報セキュリティ専門組織として、セガグループ全社を対象に以下に代表する推進活動を行っています。

(1)インシデントの事前予防
脆弱性情報の収集/展開、機器のログ収集/解析、監視/モニタリング

(2)インシデントの事後対策
受付/優先度付、担当決定/コントロール、レポーティング、再発防止検討

(3)体制強化
審査/承認、教育/啓蒙活動、規程類/ルール整備、脆弱性診断/自己診断

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

PwC Japan CSIRT

チームの正式名称	PwC Japan Computer Security Incident Response Team
チームの略称	PwC Japan CSIRT
所属する組織名	PwCコンサルティング合同会社 PwCあらた有限責任監査法人
設立年月日	2014-08-01
チームの Email アドレス	pwc.jp.csirt@jp.pwc.com
チームサイト	
所属組織サイト	http://www.pwc.com/jp/ja/advisory/index.jhtml
加盟年月	

1. **概要**

   PwC Japan CSIRT は、日本における PwC メンバーファームおよびその関連法人に対し情報セキュリティに関するさまざまな支援やインシデント対応を実施する専門チームです。

2. **設立の経緯・背景**

   PwC メンバーファームおよびその関連法人は、会計監査ならびにアドバイザリーサービスを提供するなかで、クライアント企業の機密情報を扱う場面も少なくありません。プロフェッショナル・サービス・ファームとして求められる高い業務品質を維持し、社会からの要請に応え信頼される存在であり続けるために、「リスク管理・コンプライアンス室」に情報セキュリティの専門チームを設置し、情報セキュリティの確保に努めてきました。そして 2014 年 8 月、同じ課題を持つ企業との情報共有を図るため、”PwC Japan CSIRT” のチーム名称にて、対外的な活動を開始しました。

3. **会社内における位置づけおよび活動内容**

   PwC がグローバルに展開する「サイバーセキュリティサービス」を提供するチームと連携し最新のベストプラクティスを活用することで、情報セキュリティ・インシデントへの対応、セキュリティ対策の導入やデータ管理支援、および事業継続管理について実施しています。また、PwC のスタッフが情報セキュリティ管理について高い意識を持ち基本的な行動様式を日々の業務において体現できるよう、情報セキュリティに関する注意喚起や最新情報の提供などを行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SAKURA.CSIRT

チームの正式名称	SAKURA Internet CSIRT
チームの略称	SAKURA.CSIRT
所属する組織名	さくらインターネット株式会社
設立年月日	2015-05-01
チームの Email アドレス	csirt-ml@sakura.ad.jp
チームサイト	
所属組織サイト	https://www.sakura.ad.jp/corporate/
加盟年月	2015年7月

1. 概要

さくらインターネット株式会社は、ホスティングサーバーを中心とするデータセンター事業およびインターネットサービス事業を行っています。法人のお客様向けには、データセンターのハウジングサービス、専用サーバ、レンタルサーバ、さくらの VPS、さくらのクラウドを提供しています。個人のお客様向けには、専用サーバ、レンタルサーバ、さくらのメールボックス、ドメインの取得、さくらの VPS、さくらのクラウドのサービスを提供しています。

2. 設立の経緯・背景

これまでも外部からの攻撃の対処を日々実施してきたが、対処活動を集約することによってそれらを効率化し、レベルを上げていくニーズが出てきました。社内の対処活動や収集されている情報を集約することで知見を集約し、ノウハウをより良いインターネット社会への貢献に活用して行くために設立しました。

3. 会社内における位置づけおよび活動内容

SAKURA.CSIRT は、リスクマネジメント室の一部として設立しました。現在は総務部　内部統制・情報セキュリティグループ内において専任者を立て、さくらインターネットのサービスを開発・運用している部門と連携し、対処活動の「ハブ」のような役割を担っている。

SAKURA.CSIRT では、次のサービスを提供しています。
【社内及び技術的な活動】
① 事後対応サービス
・注意喚起
・脆弱性ハンドリング
・インシデントハンドリング
② 事前対応サービス
・技術動向の把握、アナウンス
・セキュリティに関する普及啓発
③ リリース前のセキュリティ診断などの品質関連の支援
④ 技術者およびその他の社内リソースのセキュリティ啓発/教育活動
【お客様側への対応】
① Abuse/カスタマサポートの支援
② 外部機関との連携
③ セキュリティ関連情報や情勢の把握と共有/活用

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Qdai CSIRT

チームの正式名称	情報統括本部　九大CSIRT
チームの略称	Qdai CSIRT
所属する組織名	国立大学法人　九州大学
設立年月日	2016年 9月30日
チームの Email アドレス	security-room@iii.kyushu-u.ac.jp
チームサイト	http://www.sec.kyushu-u.ac.jp/
所属組織サイト	https://www.kyushu-u.ac.jp/
加盟年月	2017 年 05 月

1. 概要

国立大学法人　九州大学は、1911年（明治44年）に4番目の帝国大学として創立され、18学府、18研究院、4研究所、11学部、学生数約1万9千人、教職員総数約8千人、6つの主要キャンパス（伊都、箱崎、病院、筑紫、大橋、別府）からなる大規模総合大学です。
2011年の創立百周年を機に、新たな百年に向けて、すべての分野において世界のトップ百大学に躍進する、「躍進百大」というスローガンを掲げ、「自律的に改革を続け、教育の質を国際的に保証するとともに、常に未来の課題に挑戦する活力に満ちた最高水準の研究・教育拠点となる」を基本理念としています。

2. 設立の経緯・背景

前身である情報セキュリティ対策室が2007年に設置され、情報セキュリティインシデント等が発生した際の応急対応、調査等の事後対策並びに日々の情報セキュリティ状況の把握と情報インシデントの事前防止などの対応に当たってきましたが、九州大学の情報セキュリティの保全のさらなる強化を目的に、情報セキュリティ対策室を発展的に改組し、2016年9月30日に九大CSIRTを設置し、安全な九州大学サイバー空間の維持・強化に取り組んでいます。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
九大CSIRTは、情報政策担当理事・副学長（CIO、CISO）のもとの情報統括本部に所属する一組織として設置され、リーダーのCISOのもと副リーダー3名、メンバー8名で構成されており、各部局の情報セキュリティ責任者（部局長）と連携して全学体制で対応しています。

(2)活動内容
主な業務は以下のとおりです。
- 情報インシデントの応急対応
- 情報インシデントの調査、事後対策
- 情報インシデントの事前防止
- ファイアウォールの運用・管理
- 情報インシデント対策に関する広報や文書作成

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SANKEI-CSIRT

チームの正式名称	産経新聞 コンピュータセキュリティ対策チーム
チームの略称	SANKEI-CSIRT
所属する組織名	株式会社産業経済新聞社
設立年月日	2016-02-01
チームの Email アドレス	ml.sankei-csirt@sankei.co.jp
チームサイト	
所属組織サイト	https://sankei.jp/
加盟年月	2016 年 06 月

1. 概要

株式会社産業経済新聞社は、全国紙の産経新聞、およびサンケイスポーツ、夕刊フジ、フジサンケイビジネスアイ、競馬エイト、週間Gallopをはじめとし、他にも多数の紙媒体を発行しています。また、株式会社産経デジタル（グループ会社）へも常時コンテンツを提供し、紙面・WEBの両面から報道・情報を発信しています。

2. 設立の経緯・背景

昨今のサイバー攻撃の激化に伴い、弊社でも対策を検討しました。インシデントの早期発見、被害を最小限にとどめる、日々の社内啓蒙活動などにおいて、組織的に態勢を整える必要があると会社が判断したため、SANKEI-CSIRTを立ち上げることになりました。

3. 会社内における位置づけおよび活動内容

SANKEI-CSIRTは、基幹システムを担うシステム本部、産経デジタルの情報システム部、また外部委託SOCと連携の元、コンピュータセキュリティインシデントの早期覚知・対応、被害の最小化、日々の啓蒙に努めることで、安定した新聞発行、デジタルコンテンツ配信を支える活動をしています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Sansan-CSIRT

チームの正式名称	Sansan Computer Security Incident Response Team
チームの略称	Sansan-CSIRT
所属する組織名	Sansan株式会社
設立年月日	2015-05-19
チームの Email アドレス	csrit@sansan.com
チームサイト	
所属組織サイト	http://jp.corp-sansan.com/
加盟年月	2016 年 04 月

1. **概要**
   Sansan-CSIRT は「ビジネスの出会いを資産に変え、働き方を革新する」を Mission に掲げ、法人向けクラウド名刺管理サービスの「Sansan」、個人向けアプリ「Eight」を提供する Sansan株式会社の CSIRT です。

2. **設立の経緯・背景**
   Sansan は名刺という個人情報を扱うサービスを運営しています。取り込まれる名刺枚数は日々増えセキュリティの重要性は高まるばかりです。さらに、組織内の部門間での調整、世の中で発生するセキュリティインシデントの情報収集と蓄積、対応ノウハウの蓄積の必要性から 2015 年 5 月に発足しました。

3. **会社内における位置づけおよび活動内容**
   Sansan-CSIRT は CISO 直轄の組織です。
   自社で発生したセキュリティインシデントの迅速な解決のために、事象発生時のインシデントハンドリングと社内の社内外の取りまとめ、情報提供を行っています。また、日々脆弱性情報の収集、社員への教育と外部有識者との定期的な打ち合わせを行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

QTnet CSIRT

チームの正式名称	QTnet CSIRT
チームの略称	QTnet CSIRT
所属する組織名	株式会社QTnet
設立年月日	2016年10月1日
チームの Email アドレス	qtnet_csirt@qtnet.co.jp
チームサイト	
所属組織サイト	http://www.qtnet.co.jp/
加盟年月	2017 年 01 月

1. 概要

株式会社QTnetは、1987年の設立以来、九州電力グループの情報通信事業者として、お客さまの生活や事業活動に欠かせない情報・サービスを、安全・便利・快適にご利用いただくことにより、九州の発展に貢献できるよう努めてきました。
　QTnet CSIRTはお客さま向けの事業用設備や、社内業務用設備のサイバーセキュリティリスク対策の検討・指示、情報収集・展開などを役割として活動します。

2. 設立の経緯・背景

株式会社QTnetでは各部署でサイバーセキュリティに関わるリスク対策を行っていましたが、全社でリスク対策推進を行う体制が必要との考えから、2016年10月1日QTnet CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

サイバーセキュリティリスク対策の検討・指示、情報収集・展開を行います。
(1) サイバーセキュリティリスクに対する管理方針及び予防対策の検討・指示
・管理方針及び予防対策の検討、対策実施部署への指示
・脆弱性情報の収集、関連部署への展開・対策指示、実施状況管理
・標的型攻撃メール訓練などセキュリティ意識向上対策の検討・指示
(2) サイバー攻撃が発生、又は疑われる事象が発生した場合の
・被害拡大防止のために必要な措置の検討・指示(事業用・業務用設備の停止など)
・被害復旧及び対策措置、その他必要事項の検討・指示
・社外公表の決定、公表内容・方法の検討・指示
(3) 社外サイバーセキュリティ関係者からの情報収集、社内関係部署への情報展開
(4) サイバーセキュリティリスクに対する社員教育の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SB-CSIRT

チームの正式名称	ソニー銀行CSIRT
チームの略称	SB-CSIRT
所属する組織名	ソニー銀行株式会社
設立年月日	2016-03-01
チームの Email アドレス	sb-csirt@sonybank.co.jp
チームサイト	
所属組織サイト	http://sonybank.net/
加盟年月	2016 年 06 月

1. 概要

ソニー銀行CSIRTは、ソニー銀行株式会社の組織内における、サイバー攻撃に対応するチームです。

2. 設立の経緯・背景

昨今のサイバーセキュリティに関する動向を踏まえ、ソニー銀行におけるサイバー攻撃対応対応態勢の整備を行い、ソニー銀行CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

位置づけ
ソニー銀行CSIRTは、システム部門を中心として、活動を行います。
なお、有事の際には各部門と連携をした上で、対応にあたります。

活動内容
(1) サイバー攻撃の未然防止対策・事前対策
・脆弱性に係る情報収集および対策の実施
・サイバー攻撃の動向に係る情報の収集および共有
・セキュリティ対策技術の動向に係る調査
・サイバー攻撃に係る対応態勢の評価および改善　など
(2) サイバー攻撃発生時の対応全般
(3) サイバー攻撃対応訓練の立案および実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SBILIFE-CSIRT

チームの正式名称	SBI生命 CSIRT
チームの略称	SBILIFE-CSIRT
所属する組織名	SBI生命保険株式会社
設立年月日	2017/10/01
チームの Email アドレス	life_csirt_admin@sbilife.co.jp
チームサイト	
所属組織サイト	https://www.sbilife.co.jp/
加盟年月	2018 年 07 月

1. 概要

SBI生命は、2015年2月にSBIグループの一員となり、2016年2月より時代のニーズに応える保険商品を販売しています。SBI生命CSIRTは、SBI生命のセキュリティインシデント対応を行うための社内横断組織です。

2. 設立の経緯・背景

SBI生命では、情報セキュリティ対策を経営の重要課題として位置づけ、様々な取組みを継続的に実施していますが、昨今の高度化・巧妙化するサイバー攻撃への危機管理態勢をさらに強化するため、2017年10月にSBI生命CSIRTを設立いたしました。

3. 会社内における位置づけおよび活動内容

(1)社内における位置づけ
SBI生命CSIRTはセキュリティインシデントに対して社内外へ迅速な対応ができるよう、IT部門だけでなく経営層を含む複数の部署のメンバーから構成されています。

(2)活動内容
以下のような活動を実施しています。
・セキュリティインシデントや脆弱性に関する情報収集・全社的な情報連携
・セキュリティインシデント事案発生時のハンドリング
・全従業員へのセキュリティ教育・啓蒙活動
・サイバー攻撃を想定した演習の実施
・セキュリティ対策の提案・推進

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SBT-CSIRT

チームの正式名称	SoftBank Technology Computer Security Incident Response Team
チームの略称	SBT-CSIRT
所属する組織名	ソフトバンク･テクノロジー株式会社
設立年月日	2016年6月21日
チームの Email アドレス	sbt-csirt@tech.softbank.co.jp
チームサイト	
所属組織サイト	http://www.softbanktech.co.jp/
加盟年月	2017 年 02 月

1. 概要

SBT-CSIRT（SoftBank Technology Computer Security Incident Response Team）は、ソフトバンク･テクノロジー株式会社が運営する組織内 CSIRT です。
ソフトバンク･テクノロジー株式会社は「情報革命で人々を幸せに ～技術の力で、未来をつくる」を経営理念とし、ICTサービスの提供を通じて、豊かな情報化社会の実現に貢献してまいります。

2. 設立の経緯･背景

ソフトバンク･テクノロジー株式会社は、2004年に情報セキュリティマネジメントシステムを構築して以来、様々な情報セキュリティ対策を推進し、社内セキュリティ対応部門での方針策定や対応を実施してきましたが、昨今高度化･巧妙化しているサイバーセキュリティの脅威に対し、セキュリティインシデントに対する組織的対応力と外部組織との連携を強化するためにセキュリティインシデント対応を専門とする組織内CSIRTを設立しました。
（ISMS取得年：2004年）

3. 会社内における位置づけおよび活動内容

（位置付け）
SBT-CSIRT は情報セキュリティ部門を中心とした複数の組織のメンバーから構成されるチームです。

（活動内容）
・ セキュリティ関連情報の収集
・ セキュリティインシデント発生時の対応
・ 対外的な連絡窓口
・ セキュリティ対策の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SC-CSIRT

チームの正式名称	Sumitomo Chemical Computer Security Incident Response Team
チームの略称	SC-CSIRT
所属する組織名	住友化学株式会社
設立年月日	2016年2月10日
チームの Email アドレス	scc-csirt@ya.sumitomo-chem.co.jp
チームサイト	
所属組織サイト	http://www.sumitomo-chem.co.jp/
加盟年月	2016 年 11 月

1. 概要

SC-CSIRTは、住友化学、および、住友化学グループにおける情報システムセキュリティ・インシデントの発生を速やかに検知し、迅速かつ適切に対応することで被害の拡大を最小限に抑えることを目的に設立されました。

2. 設立の経緯・背景

・これまで弊社では、多層防御の考え方に基づき、種々のセキュリティ対策を講じてきました。
・しかしながら、標的型攻撃に代表されるように、セキュリティ・インシデントを完全に防ぐことは難しく、セキュリティ・インシデントが発生したとしてもその被害を最小限に抑えることの重要性が益々増えてきていると弊社では認識しています。
・また、2014年に化学が重要インフラに指定されたことや、制御システムにおいて、IP通信の普及と汎用OSの拡大やUSBを介したマルウェア感染事例が実際に発生していること等から、業界団体（石油化学工業協会、日本化学工業協会）とも連携しながら、制御システムセキュリティへの取組みを当社ではここ数年強化してきました。
・こういった経緯・背景から、2015年12月に公表された経営セキュリティガイドラインでも述べられているCSIRTを2016年2月に住友化学内に設立し、住友化学グループにおけるCSIRT活動を制御システムも含めて、実施していくことになりました。

3. 会社内における位置づけおよび活動内容

住友化学のIT部門内にCSIRTを設立し、社外（経済産業省、NISC、JPCERT/CC、IPA、警視庁等）や弊社内の本社（総務部門、広報部門、人事部門、生産技術部門、安全部門）や各工場（工務部門、IT部門）、各グループ会社の窓口と連携しながら、以下のような活動を実施していこうとしています。

主な活動内容
1. 事前対応
・社内外との情報共有体制構築
・検知・対応プロセスの整備・改善
・注意喚起等

2. 事後対応
・インシデント対応状況把握
・大規模インシデント対応リーディング

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SCSK-CSIRT

チームの正式名称	SCSK-CSIRT
チームの略称	SCSK-CSIRT
所属する組織名	SCSK 株式会社
設立年月日	2012-03
チームの Email アドレス	nca-staff@ml.scsk.jp
チームサイト	http://www.scsk.jp/sp/sys/service/soc-csirt/index.html
所属組織サイト	http://www.scsk.jp/
加盟年月	2012 年 08 月

1. 概要

SCSK CSIRT は、監視サービスや SOC 構築を提供している顧客システムにおいて、インシデント検知、分析を行い、最適なセキュリティ対策を提供する。

2. 設立の経緯・背景

2011年当初、SCSK では顧客システムにセキュリティ監視サービスを提供し、有事の際に顧客にインシデントレスポンス対応を実施するなど、CSIRT の機能は提供していたが明確な組織としては存在しなかった。
昨今は巧妙なサイバー攻撃、特に標的型攻撃が頻発し、社外との情報共有・情報交換が不可欠と判断。以前より脆弱性対応の面で連携していた JPCERT/CC から NCA を紹介されたことをきっかけに、既に顧客向けサービスとして提供していた機能を明確に CSIRT として定義。

2012 年 3 月に『SCSK CSIRT』が正式に発足した。

3. 会社内における位置づけおよび活動内容

[体制]
SCSK CSIRT は、セキュリティコンサルティング、脆弱性診断、セキュリティ監視、SOC 構築支援等、各種セキュリティサービス・ソリューションを提供している部署のメンバーで構成されている。同部には渉外担当も含まれる。

[活動内容]
主な活動として、セキュリティ監視サービスを提供している顧客システムで発生したインシデントの対応、対応依頼を受けた顧客に対するログフォレンジック、SOC の構築支援、顧客常駐メンバーと連携したインシデント対応・対策等を実施する。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SECOM-CSIRT

チームの正式名称	SECOM Computer Security Incident Response Team
チームの略称	SECOM-CSIRT
所属する組織名	セコムトラストシステムズ株式会社
設立年月日	2004年4月1日
チームの Email アドレス	secom-csirt@ml.secom-sts.co.jp
チームサイト	
所属組織サイト	http://www.secomtrust.net/
加盟年月	2016 年 07 月

1. 概要

セコムは、「安全・安心」で「快適・便利」な社会を実現するために、セキュリティ、防災、メディカル、保険、地理情報サービス、情報通信、不動産などの事業を融合させた「社会システム産業」を事業展開しております。
情報セキュリティの分野では、セコムは、1975年に、世界で初めて、コンピュータを警備業務に導入し、安全性向上と業務合理化を飛躍的に進展させましたが、一方で、コンピュータを使用することによるリスクに着目して、コンピュータ犯罪や事故を防ぐため、セコムの情報系子会社であるセコムトラストシステムズよりシステム監査・診断、情報セキュリティシステムの設計、構築、保守、コンサルティング業務などトータルな情報セキュリティサービスをお客様に提供しております。
それらの情報セキュリティサービスに携わる専門家が、セコムグループ全体の情報セキュリティ強化を担当するシーサートとして活動しています。

2. 設立の経緯・背景

セコムは、設立以来、セキュリティ（警備）を提供する業務の一環として、情報セキュリティに関して、厳しい基準で運営していますが、お客様の生命・財産を守るには、個人情報や機密情報などの情報セキュリティは必要不可欠であり、情報セキュリティはセコムの事業そのものであると言えます。
そのような背景からセコムでは、現場で発生した事案については、経営層を含む関係者に即時に情報が伝達される重要事項報告という仕組みを運用してきました。即ちシーサートという言葉が一般的になる前から事案発生時の体制、対応、更に重要事項が発生しないよう平時の対応を行うチームを立ち上げており、それをベースとしてシーサートを発足しました。

3. 会社内における位置づけおよび活動内容

SECOM-CSIRTはセコムトラストシステムズのメンバで運営されており、セコムグループ全体の情報セキュリティインシデントに対応します。
SECOM-CSIRTは事案発生の際の緊急出動、事案対処は勿論のこと、経営層へのエスカレーションや関係部署との調整を行い、被害拡大を防ぎます。又、平時は脆弱性情報の収集、パッチ適用、全セコムグループの脆弱性有無の管理などを行っており、毎月定例会を開催して24時間365日、セコムグループの情報資産の保護活動の向上を図っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SecureBrain-ARL

チームの正式名称	SecureBrain Advanced Research Laboratory
チームの略称	SecureBrain-ARL
所属する組織名	株式会社セキュアブレイン
設立年月日	2012-10-05
チームの Email アドレス	ml-nca-sbarl@securebrain.co.jp
チームサイト	
所属組織サイト	http://www.securebrain.co.jp/about/security.html
加盟年月	2013 年 07 月

1. 概要

セキュアブレインは、日本発のセキュリティの専門企業として、企業や官公庁へ信頼性の高いセキュリティ情報と、独自開発した高品質なセキュリティ製品・サービスを提供しています。

2. 設立の経緯・背景

会社設立以降、主にウェブセキュリティ対策、マルウェア対策の各種製品開発やセキュリティ分析を行ってきました。しかし近年、コンピュータのインシデントやフォレンジックの増加や巧妙化に伴い、より迅速かつ的確な分析と封じ込め、情報提供を実現するために、2012 年ころより、弊社内のシーサート活動の強化などを今まで以上に推進しており、多くの事業者様との連携や情報交換の場に積極的に加わることで、より快適で安心できるネットワーク社会への貢献を目指すために、設立しました。

3. 会社内における位置づけおよび活動内容

SecureBrain-ARL では、特にマルウェアに起因するインシデントやフォレンジックについて、具体的な原因調査や対策に取り組んでおります。また、近年の様々な脅威に速やかに対応するために、弊社独自のフレームワークで得た情報を基に、日々研究及び技術開発などを行っております。

弊社では、これらの活動を通じて、全てのインターネットユーザに安心を届けられるように、セキュリティ情報やソリューション提供を続けております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SEI-CSIRT

チームの正式名称	SEI-CSIRT
チームの略称	SEI-CSIRT
所属する組織名	住友電気工業株式会社
設立年月日	2016年4月16日
チームの Email アドレス	csirt-sml@list.sei.jp
チームサイト	
所属組織サイト	http://www.sei.co.jp/
加盟年月	2016 年 07 月

1. 概要

SEI-CSIRT は、住友電気工業株式会社（以下、住友電工）によって運営されている住友電工グループの CSIRT です。

住友電工グループは、400年に亘り受け継がれる「住友事業精神」と「住友電工グループ経営理念」のもと、公正な事業活動を通じて社会に貢献していくことを不変の基本方針としています。1897年の創業以来、電線・ケーブルの製造技術をベースに、独創的な研究開発とあくなき新規事業への挑戦を通じ、新製品・新技術を創出し、事業領域を拡大してきました。現在では、自動車、情報通信、エレクトロニクス、環境エネルギー、産業素材の5つのセグメントで、グローバルに事業を展開しています。

2. 設立の経緯・背景

住友電工は、モビリティ・エネルギー・コミュニケーション分野といった先進社会の維持・安定に不可欠な領域の製品を多く製造しています。社内情報システムのセキュリティについては、以前から対応チームを有していましたが、IoTの進展に伴い、これらの製品群がネットワークと繋がる際にも高いセキュリティ品質を維持することが社会的な責務であると考え、　製品・生産設備のセキュリティまでカバーするための対応チームを2016年に立ち上げました。

3. 会社内における位置づけおよび活動内容

SEI-CSIRTは、住友電工グループ内の各部門と連携して、下記の業務を遂行します。
① セキュリティ方針の策定・展開・維持
② サイバーセキュリティ対策状況の管理・経営層への報告
③ サイバーセキュリティインシデント対応状況の管理・経営層への報告/社外への公表支援
④ サイバーセキュリティ情報の収集・配信（脅威・脆弱性情報）/ シーサート協議会との連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SEIBU-CSIRT

チームの正式名称	西武CSIRT
チームの略称	SEIBU-CSIRT
所属する組織名	株式会社 西武ホールディングス
設立年月日	2017年11月16日
チームの Email アドレス	seibu-csirt@seibu-group.co.jp
チームサイト	
所属組織サイト	http://www.seibuholdings.co.jp/
加盟年月	2018 年 03 月

1. 概要

当社は、西武グループの持株会社として2006年に設立し、グループの中核事業を担う「西武鉄道」及び「プリンスホテル」などの事業会社を統括するグループガバナンス体制を構築、運用しており、「グループビジョン」に基づき、皆さまの「安全で快適な暮らし」に貢献できる企業グループを目指しております。
西武CSIRTは、西武グループ各社のサイバーセキュリティインシデントに対応するCSIRTで、西武ホールディングスが運営しています。

2. 設立の経緯・背景

当社グループでは「西武グループIT基本方針」、「西武グループIT戦略」等の規程類に基づき、セキュリティ対策を実施してきましたが、昨今のセキュリティリスクの高まりを受け、またサイバーセキュリティ対策を経営に関する重要事項として捉え、当社グループ内のサイバーセキュリティに関する情報管理・対策を推進する組織として2017年11月に対策チーム（西武CSIRT）を設立しました。

3. 会社内における位置づけおよび活動内容

西武CSIRTは、当社および当社グループ各社内で発生したサイバーセキュリティインシデント対応を行う組織内CSIRTとしての役割を担います。
西武CSIRT の平常時およびインシデント発生時の機能は以下の通りです。
(1)グループ全体のサイバーセキュリティレベル向上のための全社的な施策 (危機管理対応・教育・訓練など) の検討・実施。
(2)サイバーセキュリティインシデントの未然防止と早期検知に向けての日々の脆弱性情報の収集・グループ展開、およびその対応管理。
(3)サイバーセキュリティインシデント発生時における被害の拡散防止、お客さま対応、原因の特定および対策（グループ展開含む）の実施またはその支援。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Sep-CIRT

チームの正式名称	Septeni Computer Incident Response Team
チームの略称	Sep-CIRT
所属する組織名	株式会社セプテーニ・ホールディングス
設立年月日	2015-10-01
チームの Email アドレス	sep-cirt@septeni-holdings.co.jp
チームサイト	
所属組織サイト	https://www.septeni-holdings.co.jp/
加盟年月	2015 年 12 月

1. 概要

Sep-CIRT は、株式会社セプテーニ・ホールディングスが運営するセプテーニグループの組織内 CSIRT です。
セプテーニグループは、主に次の事業を手がけております。
・ネットマーケティング事業
インターネット広告を軸としたマーケティング支援サービス
・メディアコンテンツ事業
ソーシャルゲームを中心とした各種デジタルコンテンツの提供
マンガ家の育成・輩出、マンガ配信サービスの運営

2. 設立の経緯・背景

昨今のサイバー攻撃の高度化、巧妙化に伴い、セプテーニグループ内でのコンピュータインシデント発生時の迅速かつ適切な対応、および脆弱性ハンドリングを目的として、2015 年 10 月に「Sep-CIRT」を設立しました。

3. 会社内における位置づけおよび活動内容

Sep-CIRT は仮想的な組織で、セプテーニ・ホールディングス　情報システム部のメンバーを中心に構成されています。
セプテーニグループ内における情報セキュリティ分野において、次の事項を行います。
(1)情報セキュリティに関する相談受付、指導及び助言
(2)会社内外の組織や専門家と協力して、インシデントの検知、解決、及び被害発生の予防支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SG-CSIRT

チームの正式名称	静岡ガス-CSIRT
チームの略称	SG-CSIRT
所属する組織名	静岡ガス株式会社 事業推進部 ICT企画
設立年月日	2016 年 4 月 1 日
チームの Email アドレス	sg-csirt@shizuokagas.co.jp
チームサイト	
所属組織サイト	http://www.shizuokagas.co.jp/
加盟年月	2018 年 04 月

1. 概要

静岡ガスグループは 1910 (明治 43) 年の創立以来、地域の皆さまに都市ガスを広く安全に安定してお届けすることを使命に事業を進めてまいりました。現在では、静岡県を中心に約 30 万件のお客さまにクリーンエネルギー天然ガスをお届けしています。
今日、エネルギー環境が大きく変化する中、ガス事業のみならず電力事業にも参入し、お客さまへ最適なエネルギー利用のご提案をしています。これまでの延長線上にない新たな分野への取り組みを積極的に進め、新しい時代を担う「地域 No.1 ソリューション企業」を目指し、これからも常に努力と挑戦を続けていきます。

2. 設立の経緯・背景

静岡ガス-CSIRT は、静岡ガスグループのお客様の「安心、安全、信頼」を守り、インシデント発生時においても、その被害を極小化することを目的に、2016 年 4 月に設立されました。

3. 会社内における位置づけおよび活動内容

(1) 会社内における位置づけ
静岡ガス-CSIRT は、静岡ガスのシステム部門である事業推進部 ICT 企画担当およびシステム子会社である静岡ガス・システムソリューションを中心に、グループ内の複数部門が参画する仮想的な組織です。
(2) 活動内容
静岡ガスグループを対象に、情報系および制御系システムに関わるインシデント対応、脆弱性ハンドリング、社員へのセキュリティ教育、および外部組織との情報連携を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SGH-CSIRT

チームの正式名称	SGホールディングスグループCSIRT
チームの略称	SGH-CSIRT
所属する組織名	SGホールディングス株式会社
設立年月日	2016年3月21日
チームの Email アドレス	csirt_poc_sgh@ml.sg-hldgs.co.jp
チームサイト	
所属組織サイト	http://www.sg-hldgs.co.jp/
加盟年月	2017 年 04 月

1. 概要

SGH-CSIRTは、SGホールディングスグループの事業会社に対して、情報セキュリティに関するインシデント対応を行うCSIRTです。

2. 設立の経緯・背景

SGホールディングスグループは、外部からの攻撃に対して対処できるよう対応策を実施してきました。
しかし、近年、標的型攻撃を代表とした攻撃手法の高度化により、いままで対応していた方法での限界を感じ、情報セキュリティインシデントに対応する専門チームとして、CSIRTを構築いたしました。

3. 会社内における位置づけおよび活動内容

1.位置づけ
情報セキュリティインシデント発生時に、仮想的な組織として活動し、メンバーとして、SGホールディングスを中心に、SGシステム、および各事業会社の担当者によって構成されます。

2.活動内容
情報セキュリティインシデントが発生した場合に、被害を最小限に抑えるため組織的に行動し、初動対応～インシデント対応～事後対応、情報の管理や指示、関係各社への報告などインシデント対応を主導する役割を担います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Shimadai-CSIRT

チームの正式名称	島根大学コンピューターセキュリティインシデント対応チーム
チームの略称	Shimadai-CSIRT
所属する組織名	島根大学
設立年月日	2016年10月1日
チームの Email アドレス	csirt@ipc.shimane-u.ac.jp
チームサイト	https://www.csirt.shimane-u.ac.jp
所属組織サイト	http://www.shimane-u.ac.jp/
加盟年月	2017 年 11月29日

1. 概要

島根大学は、松江高等学校、島根師範学校など3校を統合し、1949（昭和24）年に設置し、2003（平成15）年に島根医科大学と統合しました。現在法文学部、教育学部、医学部、総合理工学部、生物資源科学部、さらに、2017年度から人間科学部を開設しました。近年では、大学にある最先端の研究に関する機密情報を狙った標的型のサイバー攻撃が多数報告されています。そこで、島根大学が所有する情報資産の管理、被害拡大防止、原因の追究、システム監視、インシデントの分析、セキュリティ管理、再発防止策の検討し、大学内の研究、教育を支援するために取り組みとして、2016年10月に島根大学コンピューターセキュリティインシデント対応チーム（以下：島根大学CSIRTと明記する）の運用が始まりました。

2. 設立の経緯・背景

平成25年度1月9日文部科学省主催の文部科学省関係者機関における情報セキュリティ対策に関する会議に参加し、大学内におけるCSIRT立ち上げを検討し、平成27年7月にCSIRTフォーラムに参加し、本格的に立ち上げ準備に取り掛かかりました。島根大学（以下「本学」という。）では、本学の情報セキュリティ確保のため、情報セキュリティ委員会の配下に、島根大学CSIRTに設置しています。さらに、2017年6月より週1回を基本にCSIRT連絡会議を設け（研究・学術情報機構総合情報処理センター長、技術職員、CSIRTチームリーダ補佐）さまざまな学内における情報セキュリティインシデント対応に対して、トリアージや再発防止策、ネットワーク遮断、復旧の可否などを協議を行い、インシデントの対応の振り返りによる問題点の洗い出しなどを実施しています。

3. 会社内における位置づけおよび活動内容

島根大学における情報セキュリティ確保のため，島根大学情報セキュリティ委員会を設置し、島根大学CSIRTを設置しています。島根大学CSIRT2016年10月より活動を開始し、さらに、2017年6月よりCSIRT連絡会議を設け、個々の情報セキュリティインシデントに対する対応、原因の究明、再発防止先の検討を行っています。
☒ 情報セキュリティインシデント管理台帳を作成し、一目でインシデントの対応状況を把握できる仕組みの構築
☒ チームメンバーで情報共有できるシステム
☒ 構成員から情報セキュリティインシデントが発生した際に、すぐに連絡してもらえるように学内周知の取り組みとして、島根大学CSIRTのウェブサイトの構築、情報発信、多言語（英語、日本語、中国語、韓国語）のパンフレット、新入生向け情報セキュリティハンドブックの作成、留学生向け情報セキュリティハンドブックを作成し、配布
☒ 適時一斉メール等で注意喚起
☒ 情報セキュリティポリシーの見直し

今後の活動は、情報セキュリティ事故のその多くは (約8割) 人による誤操作や紛失などのヒューマンエラーを含む内部要因が影響しています。島根大学CSIRTは人的なヒューマンエラーを含む個人情報流出事故が発生しないためにも構成員の意識向上、知識向上を目指していきます。
☒ 情報セキュリティ向上として集合研修やe-learning講習などを実施すると共に、講習会の流れを体系的に構築し、重複した内容、構成員の立場に即した内容を学習させるためのフローチャート図を作成し、無駄のない講習会の実施

最後に、チームメンバーは、CISOである秋重幸邦、CISO補佐松本多恵、総合情報処理センターのメンバーと医学部情報ネットワークセンターのメンバーで構成しています。情報インシデントの内容によっては、他部署間と連携し、情報セキュリティインシデント対応と原因追及、再発防止に取り組んでおります。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Shimz-SIRT

チームの正式名称	SHIMIZU CORPORATION Security Incident Response Team
チームの略称	Shimz-SIRT
所属する組織名	清水建設株式会社 情報システム部
設立年月日	2008年7月1日
チームの Email アドレス	Shimz-SIRT@shimz.co.jp
チームサイト	
所属組織サイト	http://www.shimz.co.jp
加盟年月	2017 年 03 月

1. 概要

Shimz-SIRT はシミズグループを対象範囲として活動するセキュリティインシデントレスポンスチームで、清水建設株式会社が運営しています。

2. 設立の経緯・背景

当社では情報セキュリティマネジメント体制のもと、2002年に電子情報セキュリティガイドラインを制定し社内への定着を図るとともに、2003年には情報ソリューション事業部でISMSの認証を取得し、
セキュリティの向上に取り組んできました。
2008 年には全社のセキュリティインシデントへの対応体制を整備し、セキュリティの強化を継続的に進めてきましたが、近年のサイバー攻撃や不正アクセスの高度化を受けて、他社や外部機関との情報連携を図って対応するために、2017年3月に日本シーサート協議会に加盟しました。

3. 会社内における位置づけおよび活動内容

(1) 位置付け
Shimz-SIRTは情報システム部門を中心とした関係部署で構成される仮想的な組織です。グループ各社と連携して情報セキュリティに関する活動を行っています。

(2) 活動内容
Shimz-SIRTの活動内容は以下のとおりです。

1. 情報セキュリティインシデントの未然防止活動
・情報セキュリティに関する情報収集、技術調査
・情報セキュリティルールの制定、対策の立案
・情報セキュリティ教育、啓発活動
・情報セキュリティに関する運用状況チェック

2. 情報セキュリティインシデント対応活動
・インシデント検知、連絡受付
・被害の拡大防止と早期復旧に向けた活動、及び再発防止策の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SHIZUGIN-CSIRT

チームの正式名称	静岡銀行CSIRT
チームの略称	SHIZUGIN-CSIRT
所属する組織名	株式会社静岡銀行
設立年月日	2014-12-18
チームの Email アドレス	shizubank_csirt@jp.shizugin.com
チームサイト	
所属組織サイト	http://www.shizuokabank.co.jp/
加盟年月	2016 年 03 月

1. 概要

静岡銀行 CSIRT は、静岡銀行グループの CSIRT です。
静岡銀行グループは、グループの金融機能を融合した最適な金融サービスを提供する地域の総合金融機関です。

2. 設立の経緯・背景

日本全体でインターネットを利用したシステムに対する脅威 (不正送金、ホームページ改ざん、標的型メール攻撃、DDoS 攻撃等) が増大するなか、同脅威に対して組織横断的に活動し対応力を強化することを目的として 2014 年 12 月に設立しました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
静岡銀行 CSIRT は、サイバー攻撃に対応する組織横断的な組織で、リスク統括部門、システム統括・開発部門、インターネットバンキング提供部門、情報管理部門から構成されています。
(2)活動内容
静岡銀行 CSIRT は、主に以下の活動を実施しています。
1.サイバーセキュリティに関する対応方針の策定
2.インターネットバンキングのセキュリティ強化、および利用者への継続的な注意喚起
3.サイバー攻撃情報について外部機関や他社 CSIRT との共有
4.対応訓練の企画・運営
5.脆弱性情報の収集・対応
6.職員教育　等

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Shochu-SIRT

チームの正式名称	商工中金Security Incident Response Team
チームの略称	Shochu-SIRT
所属する組織名	株式会社 商工組合中央金庫
設立年月日	2015-10-05
チームの Email アドレス	shochu-sirt01@gm.shokochukin.co.jp
チームサイト	
所属組織サイト	http://www.shokochukin.co.jp
加盟年月	2015 年 12 月

1. 概要

【商工中金の概要】
名称：株式会社商工組合中央金庫（略称 / 商工中金）
＜英語表記：The Shoko Chukin Bank, Ltd.＞
会社成立：昭和 11 年 10 月 8 日
目的：中小企業等協同組合その他主として中小規模の事業者を構成員とする団体及びその構成員に対する金融の円滑化を図るために必要な業務を営むことを目的とする。

2. 設立の経緯・背景

2014 年 10 月に当金庫システム部内にサイバーセキュリティ対策ワーキンググループを立ち上げ、セキュリティの高度化を図って参りました。その後、世界規模で生じているサイバーセキュリティ事案への迅速な対応やインターネットバンキング等を利用する顧客保護等を目的に、子会社等を含む当金庫グループ全体の管理・対応を行う全社横断的な Shochu-SIRT を 2015 年 10 月に組織しました。

3. 会社内における位置づけおよび活動内容

位置づけ
(1)位置づけ
当金庫システム部内に SIRT 事務局を設置し、経営企画部及びその他の関係部室も参画して、当金庫グループすべてのシステムを管理対象としたサイバーセキュリティ管理体制整備を行い、平常時の管理からインシデント発生時の対応を図っています。

(2)活動内容
・サイバーセキュリティに関連する情報収集・情報共有・分析
・グループ各社含めたセキュリティ高度化の推進
・サイバーインシデントを想定した訓練の企画・実施
・サイバーセキュリティ人材の育成
・サイバーセキュリティに関する社内外への注意喚起、啓蒙活動
・インシデント対応 (検知、初動対応、顧客対応、対外公表、報告)

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Simplex-CSIRT

チームの正式名称	Simplex-CSIRT
チームの略称	Simplex-CSIRT
所属する組織名	シンプレクス・ホールディングス株式会社
設立年月日	2017/11/01
チームの Email アドレス	sxi-csirt@simplex.ne.jp
チームサイト	
所属組織サイト	http://www.simplex.ne.jp/
加盟年月	2018 年 07 月

1. 概要

シンプレクスは、1997年の創業以来、メガバンクや大手証券、大手FX会社を筆頭に、日本を代表する金融機関に向けて、収益業務に特化した金融フロントソリューションを提供しています。

Simplex-CSIRTはシンプレクス・ホールディングス株式会社のCSIRTです。

2. 設立の経緯・背景

昨今の多様化する脅威に対して、組織的なセキュリティ強化および実効性を有したセキュリティ実現の必要性から、セキュリティ対策/対応の専門チームであるCSIRTを設立するに至りました。

3. 会社内における位置づけおよび活動内容

概ね下記のように定義しています。関連チームとして、セキュリティオペレーションチームがおり、設定変更作業や傾向分析はそちらが担当し、CSIRTが監修しています。

事業会社側へのPoCチームの設置を推進しています。現場に近い窓口やセキュリティ関連案件の対応を協働で行います。

【定常サービス】
セキュリティ情報収集/共有活動
セキュリティ啓蒙教育活動
セキュリティサービスデスク(社内窓口)
リスクアセスメント支援
セキュリティ関連社外協働窓口

【緊急サービス】
セキュリティインシデントハンドリング
社内外関係者間連絡窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SJ-CSIRT

チームの正式名称	SJ-CSIRT
チームの略称	SJ-CSIRT
所属する組織名	スカパーJSAT 株式会社
設立年月日	2015-04-01
チームの Email アドレス	sj-csirt@sptvjsat.com
チームサイト	
所属組織サイト	https://www.sptvjsat.com/
加盟年月	2015 年 08 月

1. 概要

SJ-CSIRT はスカパーJSAT グループ内の各社におけるセキュリティインシデントによる被害の未然防止あるいは被害の極小化に迅速に対応するために設立されました。

2. 設立の経緯・背景

昨今の年々複雑化、高度化し増大する情報セキュリティの脅威に対し、スカパーJSAT グループ内や取引先においてもセキュリティインシデントが発生し、業務に支障をきたす事態となっています。
このような状況を鑑み、未然に予防する活動を含め、セキュリティインシデントに迅速に組織的に対応できる体制として、スカパーJSAT グループ内において CSIRT (Computer Security Incident Response Team) を立ち上げることになりました。

3. 会社内における位置づけおよび活動内容

SJ-CSIRT は、事務局機能を担う内部統制推進部、技術的な中核部分を担う情報システム部およびグループ各社内の各システムとのリエゾンの役割を担うシステム管理責任者によって構成され、情報統括管理責任者の指示に基づき業務を遂行します。

主たる活動内容は下記です。

(1)事後対応
社内、スカパーJSAT グループ内からのインシデントやその予兆の報告、また不正検知システムなどからの情報に基づき、インシデントの内容や被害範囲などの特定、対応方法の策定などを行い、侵入被害の拡大を防ぐ。

(2)事前対応
技術動向の監視、脆弱性情報、脅威情報などの情報収集の提供や、セキュリティシステムを適切に運用することにより、インシデント発生の抑制を図る。

(3)セキュリティ品質管理
会社全体、グループ全体としてのセキュリティレベルの向上に資する活動を行う。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SL-CSIRT

チームの正式名称	SonyLife Computer Security Incident Response Team
チームの略称	SL-CSIRT
所属する組織名	ソニー生命保険株式会社
設立年月日	2015-05-01
チームの Email アドレス	all-sl-csirt@sonylife.co.jp
チームサイト	
所属組織サイト	http://www.sonylife.co.jp/
加盟年月	2015年7月

1. 概要

SL-CSIRT は、ソニー生命保険株式会社のシステム部門である、IT 戦略本部内に設置された CSIRT です。
当社は合理的な生命保険と質の高いサービスを提供することによって、顧客の経済的保障と安定を図ることを基本的な使命としております。

2. 設立の経緯・背景

近年のサイバー攻撃の増大、手段の高度化に対して、金融機関として適切に対応して社会的要請にこたえる必要が高まりました。
当社は、営業職員であるライフプランナーを通して、あるいはインターネット経由でダイレクトに多くの IT サービスを顧客に提供しています。顧客保護と顧客サービスの提供に万全を期するために、従来のシステム部門内での対応体制を一層強化し、社会的要請にこたえるため、SL-CSIRT は設立されました。

3. 会社内における位置づけおよび活動内容

SL-CSIRT はサイバーセキュリティマネージメントを専門に行う組織であり、インシデント発生時の迅速な復旧対応を担います。外部との窓口として的確な対応を取ることを重視し、システム部門内に専従要員を配置しております。
また、サイバーセキュリティリスク管理におけるヘッドクオーター機能を担っており、当社内での各種リスク管理の一環を担っています。
SL-CSIRT の主要な役割は下記の通りです。
1.サイバーセキュリティインシデントの監視・分析 ・報告
2.有事 (BCP 含む) 緊急対応
-ルール整備と維持
-検知、確認、対応、関係部門への連絡、対策会議の招集、進捗管理、再発防止策策定
3.外部機関 (監督省庁、他社等) との連携
4.サイバーセキュリティ事案に関する社員教育
5.サイバーセキュリティ専門家の育成
-外部専門家をグリップできる内部人材の育成
6.サイバーセキュリティ改善計画の策定

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SMAC

チームの正式名称	JBサービス　ソリューションマネジメントアンドアクセスセンター
チームの略称	SMAC
所属する組織名	JBサービス株式会社
設立年月日	2015-08-01
チームの Email アドレス	jbs-sirt@jbsvc.co.jp
チームサイト	
所属組織サイト	http://www.jbsvc.co.jp/products/smac/index.html
加盟年月	2016 年 03 月

1. 概要

JBS-SIRT は JB サービス株式会社の運用センター SMAC のメンバーが中心となって運営している CSIRT です。

2. 設立の経緯・背景

JBグループとしては情報セキュリティポリシーの策定や 2004 年に情報セキュリティ委員会を発足させるなど、これまで主に内部脅威に対して情報資産を保護するよう務めてきました。しかしながら昨今、標的型攻撃をはじめとした外部脅威が増加している為、それらによるインシデント発生時にも迅速な対応が可能となるように、JBグループ内でセキュリティ運用などを手掛けているJBサービスにて CSIRT 組織をたちあげました。

3. 会社内における位置づけおよび活動内容

【会社内における位置づけ】
JBサービスの CSIRT は運用センター SMAC を中心とした組織であり、インシデント内容に応じて自社の事業管理部門・営業部門・グループ会社の情報システム部門・広報部門・経営層などと連携しています。

【活動内容】
社内への注意喚起によるインシデント発生の未然防止や、インシデント発生時の事後対応などを行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Shiseido CSIRT

チームの正式名称	資生堂シーサート
チームの略称	Shiseido CSIRT
所属する組織名	株式会社 資生堂
設立年月日	2016年7月1日
チームの Email アドレス	nca.shiseido.csirt@to.shiseido.co.jp
チームサイト	
所属組織サイト	http://www.shiseidogroup.jp/inquiry/?rt_bt=manu-inquiry_001
加盟年月	2017 年 03 月

1. 概要

Shiseido CSIRT は、資生堂グループのグローバル各地域のセキュリティ組織と連携を取りながら、サイバーインシデントに対応するチームです。

2. 設立の経緯・背景

昨今のサイバーセキュリティ事案を鑑み、未然防止策だけでなく、インシデントが発生することを前提とした監視体制および対応体制の整備を目的とし2016年7月5日に設立を宣言しました。(開始は2016年7月1日～)

3. 会社内における位置づけおよび活動内容

Shiseido CSIRTは、インシデント事後対応サービスを中心にコンプライアンス部門(総合調整)およびICT部門(技術情報支援)をコアメンバーとして必要に応じて関係部門と連携を取りながら、検知したインシデントに対するレスポンス・ハンドリングを実施しています。またグローバル各地域拠点のコンプライアンス/ICT部門とも連携し、必要に応じてCSIRTによるサイバーインシデント対応体制を発動させています。

現在、チームは成長段階にあり、インシデント判断基準、対応フローやガイドラインを再整備しました。
今後は、再整備した各管理コンテンツの効果的運用を目指し、各地域拠点のセキュリティ組織へも紹介・展開し、インシデント対応判断の更なる明確化やインシデントレスポンスに対するグローバル連携および各地域セキュリティ組織それぞれの更なる強化に繋げられるよう活動していきます。

また、様々なインシデント事案を教訓に、資生堂グループ全体のセキュリティ対応体制を技術・運用の両側面で順次見直していき、インシデントに対する事前対応・品質管理の各機能(防御技術基盤、SOC、監査、教育など)とも連携させながらセキュリティPDCA活動を向上させていけるCSIRTチームとして成長を目指します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Soliton-CSIRT

チームの正式名称	Soliton-CSIRT
チームの略称	Soliton-CSIRT
所属する組織名	株式会社ソリトンシステムズ
設立年月日	2016/4/5
チームの Email アドレス	Soliton-CSIRT@list.soliton.co.jp
チームサイト	
所属組織サイト	http://www.soliton.co.jp
加盟年月	2017 年 01 月

1. 概要

Soliton-CSIRTは、株式会社ソリトンシステムズが運営する組織内CSIRTです。
ソリトンシステムズは、ITセキュリティおよびクラウド事業を基幹とする情報セキュリティ製品の開発、販売ならびに、クラウドサービス、ネットワークインテグレーション等を提供しています。

2. 設立の経緯・背景

近年増大化するサイバーセキュリティインシデントの防御に向けて、従来の情報システム部門が単独でカバーできないインシデントを、全社の人的リソースを活用して速やかに対処し、被害の甚大化を防ぎ、かつ原因を排除するためCSIRT組織を設立しました。

3. 会社内における位置づけおよび活動内容

Soliton-CSIRTは、社内各部門の情報セキュリティ技術者(実行部隊)および情報システム部(事務局)をメンバーとする仮想組織です。ソリトンシステムズ本社および国内拠点において保有する業務基盤、顧客向けのサービス基盤を対象に、以下のような活動を実施しています。
・平時における情報セキュリティシステム・検知システム・解析システム等の構築や改善、および社内教育、啓蒙活動等
・インシデント発生時の即時対応、原因分析、除去、修復作業等
また、外部団体や他社CSIRTより得られた知見を活用するとともに、Soliton-CSIRTからも情報発信を行ってまいります。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SIG CSIRT

チームの正式名称	SIG Computer Security Incident Response Team
チームの略称	SIG CSIRT
所属する組織名	株式会社　SIG
設立年月日	2016/6/1
チームの Email アドレス	csirt@sig-c.co.jp
チームサイト	
所属組織サイト	http://www.sig-c.co.jp/
加盟年月	2017 年 01 月

1. 概要

SIGは、ITシステムのインテグレーションを中心とした会社です。
SIG CSIRTは、社内及び関連会社で発生したコンピュータ・インシデントに対し、調査、対処、被害軽減のための活動や、未然防止のためのセキュリティ体制の見直し、提案、構築を行うことを目的としています。

2. 設立の経緯・背景

ITシステムのインテグレータとして事業を行ってきましたが、社会の醸成や顧客からの要望を通じて、日々厳しくなっていくセキュリティの状況を認識していました。
このため、内部対策を行う体制を明確にし、効果的に対処できる組織を持つ必要から、SIG CSIRTが設立されました。

3. 会社内における位置づけおよび活動内容

SIG CSIRTは株式会社SIGに属し、以下の活動を行います。

(1) インシデント対応サービス
・インシデントレスポンス
・フォレンジック調査
(2) 運用サービス
・インシデント/セキュリティイベント検知
・技術動向調査
・セキュリティ監査
(3) セキュリティ品質向上サービス
・リスク評価分析
・セキュリティコンサルティング
・セキュリティ教育/トレーニング/啓発活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SONY-JP-SIRT

チームの正式名称	SONY Japan Security Incident Response Team
チームの略称	SONY-JP-SIRT
所属する組織名	ソニー株式会社
設立年月日	2011年9月6日
チームの Email アドレス	sonyjp-sirt@jp.sony.com
チームサイト	
所属組織サイト	http://www.sony.co.jp/
加盟年月	2016 年 09 月

1. 概要

SONY-JP-SIRTは、ソニー株式会社によって運営されているソニーグループの日本国内のセキュリティインシデントレスポンスチームです。

井深大・盛田昭夫の二人が"自由闊達にして愉快なる理想工場"を目指して創業したソニー は、グループ全体で13万人規模の日本を代表するグローバル企業となりました。
エレクトロニクスから始まり、音楽、映画、ゲーム、ネットワークサービス、金融と事業領域を拡大しながら、世界に先駆けた商品やサービス、新しい文化を生み出してきました。これからも、お客様に感動をもたらし、好奇心を刺激する会社であり続けることをミッションとし、成長を加速させていきます。

2. 設立の経緯・背景

ソニーは情報セキュリティの領域において、急速に高度化する脅威に直面しています。グローバル企業が保有する情報を狙う攻撃者の数は増え続け、より高い能力を用いて、これまで以上に継続的な攻撃が行われています。このような状況に対応するため、ソニーはチーフ・インフォメーション・セキュリティ・オフィサー(CISO)を長とした情報セキュリティおよびプライバシー組織を設置しました。

3. 会社内における位置づけおよび活動内容

(位置付け)
ソニー(株)本社情報セキュリティ部門内に、専任のメンバーによってSIRT(セキュリティインシデントレスポンスチーム)を構成しています。このSIRTはIT関連に限らず、ソニーグループ内で発生した情報セキュリティインシデントに幅広く対応します。

(活動内容)
・セキュリティインシデントの分析を行い、アメリカ側のセキュリティ事故対応チームと連携し、対応策の検討、支援を行う。
・アメリカ側の方針に対する検証／評価を行い、意思決定プロセスに関わる体制を構築する。
・社内外の関係各所とセキュリティ対策のコミュニケーションをとり、今後のインシデント防止に向けた体制、情報基盤の構築を図る。
・社内セキュリティ人材の育成、知識やノウハウの蓄積と底上げを行う。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SPSV-CSIRT

チームの正式名称	ソニーペイメントサービスCSIRT
チームの略称	SPSV-CSIRT
所属する組織名	ソニーペイメントサービス株式会社
設立年月日	2017年2月22日
チームの Email アドレス	spsv-csirt-ml@sonypayment.co.jp
チームサイト	
所属組織サイト	http://www.sonypaymentservices.jp/
加盟年月	2017 年 04 月

1. 概要

ソニーペイメントサービスCSIRTは、ソニーペイメントサービス株式会社の組織内におけるサイバー攻撃などのセキュリティインシデントに対応するチームです。
当社は安心・安全・スピーディーな決済サービスを提供し決済市場の健全な発展を使命としております。

2. 設立の経緯・背景

当社はカード情報など重要な情報を取り扱う決済代行事業者として、信用力・安全性を確保するためセキュリティ対策機器の導入やインシデント対応体制の強化に取り組んでまいりました。
しかしながら、近年の標的型サイバー攻撃においては、セキュリティツールなどによる検知をかいくぐるなど攻撃が高度化・巧妙化しております。
このような状況を踏まえ、情報セキュリティの更なる強化の観点から、他社や外部組織との連携を強化し幅広く情報収集や対策検討を行うため、ソニーペイメントサービスCSIRTを設立し、日本シーサート協議会に加盟いたしました。

3. 会社内における位置づけおよび活動内容

ソニーペイメントサービスCSIRTは、システム部門に所属するメンバーを中心に構成されており、インシデント発生時の早期復旧および被害の拡大防止を行います。
平時においても情報セキュリティに関する動向・傾向、脅威・脆弱性等の情報を収集・分析し、セキュリティ対策の推進とセキュリティインシデントの未然防止を図ります。

【ソニーペイメントサービスCSIRTの主な活動内容】
予防
・サイバー攻撃に関する早期の情報入手
・脆弱性情報の収集と評価
・ルール整備と維持
・訓練
検知
・各種ログのモニタリング
・侵入検知
・内部不正検知
有事対応
・社内外の連絡窓口
・インシデント発生時のとりまとめや対応支援
・再発防止対策検討支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SRIG-CSIRT

チームの正式名称	住友ゴムグループシーサート
チームの略称	SRIG-CSIRT
所属する組織名	住友ゴム工業株式会社
設立年月日	2014-10-01
チームの Email アドレス	srig-csirt@srigroup.co.jp
チームサイト	
所属組織サイト	http://www.srigroup.co.jp
加盟年月	2016 年 01 月

1. 概要

SRIG-CSIRTはダンロップ・ファルケンをメインブランドとする、タイヤの製造・販売事業、ゴム手袋から制振ダンパーまで様々な製品の開発・製造を行う産業品事業、ゴルフやテニスなどのスポーツ事業を基幹事業とする、住友ゴムグループの関係部署と関係会社から構成、運営されるCSIRTです。
住友ゴムグループ国内関連企業を中心にコンピュータセキュリティインシデントの対応や、教育、啓蒙活動を実施しています。

2. 設立の経緯・背景

2014年にDDOS攻撃を受け、その対応に非常に多くの時間を要し、業務影響が出た事を切っ掛けに、
セキュリティ対策、体制整備を急務として進めてきました。
その一環として、グループ会社内のセキュリティインシデントに迅速に対応するため、2014年10月1日に社内にサートを設立、2016年2月にNCAへ正式に加盟致しました。同年、社内の危機理本部と連携する形社内での位置付けを変更したことに伴い、名称を【SRIG-CSIRT】に変更致しました。

3. 会社内における位置づけおよび活動内容

SRIG-CSIRTは住友ゴム工業IT企画部と、システム子会社であるSRIシステムズのセキュリティ担当者
を中心に構成されています。コンピュータインシデントに対応していくためのチームとして設立し、近年はセキュリティ関連の記事がメディアに取り上げられる機会も増え、活動の幅が拡がっています。
活動内容は、平時はユーザ教育や啓蒙活動、ITセキュリティ関連の情報収集、作業計画立案、各種監視活動を行っており、有事にはインシデント対応を実施、被害の極小化に努めています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SSNB-CSIRT

チームの正式名称	住信SBIネット銀行CSIRT
チームの略称	SSNB-CSIRT
所属する組織名	住信SBIネット銀行株式会社
設立年月日	2015-07-01
チームの Email アドレス	Sec_post@netbk.co.jp
チームサイト	
所属組織サイト	https://www.netbk.co.jp/
加盟年月	2016 年 01 月

1. 概要

住信SBIネット銀行は、経営理念である「お客さまや社会の発展に貢献する新しい価値の創造」の下、お客さまにとっての「レギュラーバンク」を目指し、更なる利便性の向上と商品・サービスの開発・改善を進めてまいります。

2. 設立の経緯・背景

近年、インターネット環境を利用した大規模なサイバー攻撃が発生しており、今後もサイバー攻撃は拡大する可能性が高く、特にインターネット専業銀行という特性を持つ弊社においてはセキュリティ対策及びインシデント対応の一層の強化が求められることを背景に、2014 年度から設立準備活動を開始、2015 年 7 月 1 日に専門組織である CSIRT チームを立ち上げました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
セキュリティ・インシデントへの対応を効果的に行うための専任チームとして設置しました。

(2)位置づけ
以下の活動を行っています。
・CSIRT 活動方針案の策定
・セキュリティ・インシデント発生時の対応推進
・訓練の企画と実施
・セキュリティに関する情報発信
・セキュリティ啓蒙活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

START

チームの正式名称	Symantec Tactical and Advanced incident Response Team
チームの略称	START
所属する組織名	株式会社シマンテック
設立年月日	2016-03-01
チームの Email アドレス	DL-MSS-START@symantec.com
チームサイト	
所属組織サイト	https://www.symantec.com/ja/jp/index.jsp
加盟年月	2016 年 04 月

1. **概要**
   シマンテック株式会社のサイバーセキュリティ情報の発信と対外的な窓口組織です。
2. **設立の経緯・背景**
   コンピューターセキュリティインシデントが複雑・高度化し対応の難易度が上がる中、外部組織連携をするための窓口の明示および、シマンテックが収集した情報を発信する窓口として設立
3. **会社内における位置づけおよび活動内容**
   シマンテックがグローバルに展開するサイバーセキュリティサービスを活用頂いているお客さまで発生したセキュリティインシデントへの事後対応に加えて、情報収集・発信・研究を実施しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SMBC Group CSIRT

チームの正式名称	SMBCグループCSIRT
チームの略称	SMBC Group CSIRT
所属する組織名	株式会社三井住友フィナンシャルグループ
設立年月日	2013-09-10
チームの Email アドレス	smfg_csirt@ea.smbc.co.jp
チームサイト	
所属組織サイト	http://www.smfg.co.jp/
加盟年月	2013 年 09 月

1. **概要**

   SMBCグループは、銀行業務を中心に、クレジットカード業務、リース業務、情報サービス業務、証券業務などの様々な金融サービスにかかわる事業を行っています。

2. **設立の経緯・背景**

   手口が高度化し、脅威が増しているサイバー攻撃に対し、幅広い情報共有および各社との協働による早期のインシデント解決を目的とします。

3. **会社内における位置づけおよび活動内容**

   サイバーセキュリティを所管する三井住友フィナンシャルグループ IT企画部 システムリスク統括室 サイバーセキュリティ管理グループが社内外の情報共有・インシデント対応を担当します。

   活動内容
   ・外部機関との連絡窓口
   ・外部からの情報収集・グループ内連係
   ・SMBCグループのインシデント情報集約・連携
   ・SMBC内のインシデント対応(SMBC-CSIRTとしての活動)

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

STARTIA-CSIRT

チームの正式名称	STARTIA GROUP Computer Security Incident Response Team
チームの略称	STARTIA-CSIRT
所属する組織名	スターティアホールディングス株式会社
設立年月日	2014-10-01
チームの Email アドレス	startia-csirt@startiaholdings.com
チームサイト	
所属組織サイト	https://www.startiaholdings.com/
加盟年月	2014 年 11 月

1. 概要

スターティアグループは電子ブック作成ソフトを中心とした Web アプリケーションと、クラウドソリューションをはじめとした IT インフラを中堅・中小企業を主な顧客として提供をしています。

STARTIA-CSIRT はスターティアグループのコンピュータセキュリティにかかわるインシデントに対処するための組織内 CSIRT です。

2. 設立の経緯・背景

コンピュータセキュリティインシデントが複雑化・高度化するにともない、グループを統括する、より高いレベルの組織が必要となり、STARTIA-CSIRT の設立にいたりました。

3. 会社内における位置づけおよび活動内容

＜会社内における位置づけ＞
・STARTIA-CSIRT はスターティアグループの認証グループを母体に機能を拡大させた組織内レスポンスチーム
＜活動内容＞
・社内情報システムおよびお客様向け IT サービスにおけるセキュリティインシデントの検知、解決、被害局限化および、発生の予防、再発の防止
・事後対応・事前対応・セキュリティ品質向上へ向けた加盟企業との連携

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SMCC CSIRT

チームの正式名称	三井住友カード CSIRT
チームの略称	SMCC CSIRT
所属する組織名	三井住友カード株式会社
設立年月日	2016/08/01
チームの Email アドレス	smcc-csirt@smbc-card.com
チームサイト	
所属組織サイト	https://www.smbc-card.com/mem/company/info/outline.jsp
加盟年月	2016 年 12 月

1. **概要**
   三井住友カードは1967年に発足以来、日本におけるVisaのパイオニアとして、またキャッシュレス化を先導する総合決済事業者として、国内外のFinTech企業との連携しています。

2. **設立の経緯・背景**
   クレジットカードはもとより、プリペイドカード、デビットカード、電子マネーなど様々な電子決済へのニーズを踏まえ、情報技術と決済を融合した新しいサービスをより安全に提供するため、『三井住友カード CSIRT』を発足致しました。

3. **会社内における位置づけおよび活動内容**
   システムリスクを所管するシステム企画部と情報セキュリティ企画部が連携し社内外の情報共有・インシデント対応を対応します。

   活動内容
   ・ 外部機関との連絡窓口
   ・ 外部からの情報収集・グループ内連携
   ・ インシデント発生時の対応、インシデント管理
   ・ セキュリティ関連団体の活動への参加と情報交換

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SUMIBE-CSIRT

チームの正式名称	Computer Security Incident Response Team of Sumitomo Bakelite Co.,Ltd.
チームの略称	SUMIBE-CSIRT
所属する組織名	住友ベークライト株式会社
設立年月日	2016年8月1日
チームの Email アドレス	sumibe-csirt@ml.sumibe.co.jp
チームサイト	
所属組織サイト	http://www.sumibe.co.jp
加盟年月	2017 年 08 月

1. 概要

SUMIBE-CSIRTは、半導体、電子部品、自動車、建材、包装、医療などの分野で利用される
プラスチック製品の総合メーカー住友ベークライト株式会社、およびグループ会社の
セキュリティインシデントに対応するためのチームとなります。

2. 設立の経緯・背景

サイバー攻撃は、複雑化、巧妙化してきており、被害を完全に防ぐことは、今や不可能であり、セキュリティインシデント発生を前提とした備えが必要な状況です。そうした状況下、当社では情報システム部門が中心となり、予防、被害の最小化等の対応にあたってきましたが、予防強化や重大なインシデント発生時の
対応強化のためには、組織横断的な活動が必要と捉え2016年8月に、SUMIBE-CSIRTを発足しました。

3. 会社内における位置づけおよび活動内容

平常時には、個別リスクを主管する組織として、情報セキュリティ事故発生を未然に防ぐための対策策定、事故発生時の対応手順の整備を行います。

セキュリティインシデント発生時には、緊急時対策本部の下部組織として、被害の最小化、社内関係部署との連携、社外対応、復旧対応、再発防止策の策定を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SNC SIRT

チームの正式名称	ソニーネットワークコミュニケーションズセキュリティインシデントレスポンスチーム
チームの略称	SNC SIRT
所属する組織名	ソニーネットワークコミュニケーションズ株式会社
設立年月日	2016-05-01
チームの Email アドレス	snc-sirt@sony.com
チームサイト	
所属組織サイト	http://www.sonynetwork.co.jp/
加盟年月	2016 年 06 月

1. **概要**
   SNC SIRTは、ソニーネットワークコミュニケーションズ株式会社のリスク管理部門メンバーが中心となって運営しているCSIRTです。
2. **設立の経緯・背景**
   ソニーネットワークコミュニケーションズ株式会社ではこれまでもインシデント対応を行ってきていますが、セキュリティ脅威の多様化や組織、システムが複雑化する中、より効率的かつ合理的な対応ができるよう体制を強化するため、2016年5月にSo-net SIRTが設立され、2016年7月1日、所属組織の商号変更に伴い名称がSNC SIRTに変更されました。
3. **会社内における位置づけおよび活動内容**
   SNC SIRTでは、現在リスク管理部門メンバーを中心に、ソニーネットワークコミュニケーションズ株式会社および関連組織を対象としたセキュリティ監視、セキュリティ診断、セキュリティ教育、およびインシデントレスポンス等の活動をしています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SUMISEI-CSIRT

チームの正式名称	SUMISEI Computer Security Incident Response Team
チームの略称	SUMISEI-CSIRT
所属する組織名	住友生命保険相互会社
設立年月日	2015-03-03
チームの Email アドレス	sumisei_csirt@am.sumitomolife.co.jp
チームサイト	
所属組織サイト	http://www.sumitomolife.co.jp/
加盟年月	2015 年 03 月

1. 概要

SUMISEI-CSIRT は、住友生命保険相互会社の CSIRT です。
　住友生命保険は、超高齢社会が到来する中、医療や介護の保障、老後の生活への備えなどますます多様化する生命保険へのニーズに対して、お客さまお一人おひとりのニーズにしっかりとお応えした最適な保障を提供する生命保険会社です。

2. 設立の経緯・背景

高度化、巧妙化するサイバー攻撃に対し、有事の迅速かつ的確な対応による被害拡大防止と、平時の情報収集・共有によるサイバーインシデントの発生抑止を目的に、2015 年 3 月に設立されました。

3. 会社内における位置づけおよび活動内容

SUMISEI-CSIRT は、サイバーセキュリティ事象に対応する部門横断的な仮想組織です。情報システム部門 (情報システム部およびスミセイ情報システム株式会社) を中心に、サイバー攻撃対応に関係の深い広報、お客さまサービス部門等の関係各部から構成される CSIRT です。

有事、平時において主に以下の活動を実施します。
・サイバーセキュリティに関する情報収集・共有
・インシデント発生時の対応
・有事、平時の外部機関、他社 CSIRT との情報共有
・サイバーセキュリティに関する対応方針の検討
・従業員教育

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SoftBank CSIRT

チームの正式名称	ソフトバンクコンピューターセキュリティインシデント対応組織
チームの略称	SoftBank CSIRT
所属する組織名	ソフトバンク株式会社 Wireless City Planning株式会社
設立年月日	2004-09-01
チームの Email アドレス	SBBGRP-SBCSIRT@g.softbank.co.jp
チームサイト	
所属組織サイト	https://www.softbank.jp/
加盟年月	2007 年 08 月

1. 概要

SoftBank CSIRT (SoftBank Computer Security Incident Response Team) は、ソフトバンク株式会社、及び Wireless City Planning 株式会社で構成される、主に通信サービスに関するインシデントに対応する CSIRT です。

2. 設立の経緯・背景

SoftBank CSIRT の前々身である SBB-SIRT は 2004 年 9 月に設立されました。当時はソフトバンク BB 株式会社 (現ソフトバンク株式会社) のインシデント対応を行う組織でしたが、脅威の変遷やグループの規模拡大に合わせて体制を変更し、2008 年 8 月にはソフトバンク BB 株式会社 (現ソフトバンク株式会社)、ソフトバンクテレコム株式会社 (現ソフトバンク株式会社)、ソフトバンクモバイル株式会社 (現ソフトバンク株式会社) の 3 社で構成される CSIRT になりました。その際、名称を SB CSIRT に変更しました。

その後、2012 年 10 月には株式会社ウィルコム (現ソフトバンク株式会社)、2013 年 4 月には Wireless City Planning 株式会社も加わりました。

また、2015年9月1日に名称をSoftBank CSIRTに変更しました。

3. 会社内における位置づけおよび活動内容

SoftBank CSIRT はセキュリティ部門のメンバーを中心として、関連部門からの参加者で構成されています。参加者は所属する各部門の部門長により任命され、その責任の下で業務を行っています。

SoftBank CSIRT の活動は、インシデント発生の未然防止、インシデント発生時の対応準備、インシデント発生時の対応等に区分されます。とりわけ、未然防止、対応準備に多くの時間を割いています。未然防止や対応準備として行っていることは以下の通りです。
・セキュリティ関連情報 (脆弱性の情報や攻撃予告など) の収集、現場への展開、対応の促進
・公開前の脆弱性情報への対応
・インシデント発生に備えた訓練、対応手順の確立
・セキュリティルールの見直し

実際のインシデント発生時の対応については迅速な復旧を実現するために各部門へ権限を委譲し、現場で対応可能なインシデントについては極力現場で対応できる体制を構築しています。一方で、現場だけで対応することが難しい複雑なインシデント、あるいは一通信事業者だけでは解決できない大規模 DDoS などのインシデントについては SoftBank CSIRT の中心メンバーが対応することにしています。

なお、開発したシステムのセキュリティチェックなどは SoftBank CSIRT の活動には含まれず、別のセキュリティ担当が実施しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SUMITEM-CSIRT

チームの正式名称	SUMITEM Computer Security Incident Response Team
チームの略称	SUMITEM-CSIRT
所属する組織名	住友セメントシステム開発株式会社
設立年月日	2015-06-29
チームの Email アドレス	csirt@sumitem.co.jp
チームサイト	
所属組織サイト	https://www.sumitem.co.jp/
加盟年月	2015 年 08 月

1. 概要

SUMITEM-CSIRT は、住友セメントシステム開発株式会社が運営する CSIRT 組織です。住友セメントシステム開発株式会社は、住友大阪セメント株式会社の情報システム運用を行なうと共に、自社開発の IT サービスを展開しています。

2. 設立の経緯・背景

弊社では、2012 年の ISMS 認証取得より、社内横断で情報セキュリティを推進する委員会活動を行っています。社内に於いては委員会にてインシデント情報の掌握、インシデント対応、情報セキュリティ教育などを推進しておりますが、対外的な窓口として CSIRT を設立することになりました。

3. 会社内における位置づけおよび活動内容

(会社内における位置づけ)
SUMITEM-CSIRT は、社内横断組織として存在する情報セキュリティ委員会の対外的呼称です。
情報セキュリティ委員会は、全社部門の代表により組織されています。情報セキュリティ委員会の事務局は、社内情報セキュリティ専任部署が担っています。従って、SUMITEM-CSIRT の窓口は、情報セキュリティ委員会の事務局となります。

(活動内容)
対外的窓口として、日本 CSIRT 協議会等、外部関連機関との連携
脆弱性情報の収集と周知、対策
インシデント発生時の対応
情報セキュリティ教育

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SOGO SIRT

チームの正式名称	総合メディカルサート
チームの略称	SOGO SIRT
所属する組織名	総合メディカル株式会社
設立年月日	2016-04-01
チームの Email アドレス	sirt@sogo-medical.co.jp
チームサイト	
所属組織サイト	http://www.sogo-medical.co.jp/
加盟年月	2016 年 04 月

1. 概要

総合メディカルは、「よい医療はよい経営から」をコンセプトに、医療機関が効率的で質の高い医療を提供できるよう、コンサルティングをベースに医療機関経営のトータルサポートをおこなっています。
医師の紹介や医業継承、医療連携を通じて、地域医療の活性化をお手伝いする DtoD、全国に 570 店舗以上を展開する調剤薬局、アメニティの向上をお手伝いするリース・レンタルをはじめ、在宅・介護まで多角的な事業を展開しています。

2. 設立の経緯・背景

増加するサイバー攻撃やセキュリティの脆弱性に起因する情報セキュリティインシデントに的確かつ迅速に対応するための体制作りと、発生抑止を目的とし 2016 年 4 月に設立しました。

3. 会社内における位置づけおよび活動内容

総合メディカルサートは自社及びグループ会社で発生した情報セキュリティインシデントのハンドリングと社内外のコーディネーションを行う部門横断型の仮想組織です。
平時の活動はセキュリティ監視と分析、従業員教育、訓練を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SuMiTPFC-CSIRT

チームの正式名称	三井住友トラスト・パナソニックファイナンス CSIRT
チームの略称	SuMiTPFC-CSIRT
所属する組織名	三井住友トラスト・パナソニックファイナンス株式会社
設立年月日	2016-01-29
チームの Email アドレス	sumitpfc_csirt_ml@smtpfc.jp
チームサイト	
所属組織サイト	https://www.smtpfc.jp/
加盟年月	2016 年 04 月

1. 概要

SuMiTPFC-CSIRT は、三井住友トラスト・パナソニックファイナンス株式会社 (以下、「当社」) によって運営されている CSIRT です。

当社は、三井住友信託銀行とパナソニック株式会社を株主に持ち、歴史的に銀行系リース会社とメーカー系クレジット会社の系譜を受け継ぎ、双方の特徴を併せ持つ総合ファイナンス会社です。

2. 設立の経緯・背景

国内外での大規模なセキュリティ・インシデントの発生状況を踏まえ、セキュリティ対策、インシデント対応力の強化が企業としての急務であるとの認識のもと、当社では 2015 年度から設立準備活動を開始し、社内横断的なメンバーから構成されるチームとして 2016 年 1 月に設置されました。

3. 会社内における位置づけおよび活動内容

SuMiTPFC-CSIRT は、セキュリティ・インシデントへの対応を、情報システム部門と連携して効果的に行うための社内横断的なチームとして設置されました。

主な活動内容は下記の通りです。
・CSIRT 活動計画の策定、実行
・セキュリティに関する情報収集、情報発信
・社内へのセキュリティ啓蒙活動
・インシデント発生時の情報システム部門による対応の支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SOMPO HD CSIRT

チームの正式名称	SOMPOホールディングス CSIRT
チームの略称	SOMPO HD CSIRT
所属する組織名	SOMPOホールディングス株式会社
設立年月日	2015-01-01
チームの Email アドレス	10_csirt-member@sompo-hd.com
チームサイト	
所属組織サイト	http://www.sompo-hd.com/
加盟年月	2015 年 04 月

1. 概要

SOMPO ホールディングス CSIRTは、SOMPO ホールディングスグループで発生するセキュリティインシデントに対応するためのインシデントレスポンスチームです。

2. 設立の経緯・背景

サイバー攻撃の脅威が年々増加し、高度化する中で、組織的なインシデンと対応が喫緊の課題となっていることから、グループ横断のセキュリティインシデントチームとして SOMPO ホールディングス CSIRT を立ち上げました。

3. 会社内における位置づけおよび活動内容

位置づけ

SOMPOホールディングスグループの持株会社、事業会社のシステム部門、システム開発会社の兼任メンバーで構成される仮想チームです。

活動内容

SOMPO ホールディングスグループの情報システムや通信ネットワークでウイルス感染や不正アクセス、サービス拒否攻撃 (DoS 攻撃) などセキュリティ上の脅威となる現象や行為が発生した際に、被害の拡大防止や関連情報の収集・告知、再発防止策の策定などの活動を行います。また、SOMPOグループ以外の事件・事故の被害情報やシステムの脆弱性についての情報を収集し、SOMPOグループとして必要な対策を検討し、SOMPO ホールディングスグループ各社に対策指示を行います。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SWC-CSIRT

チームの正式名称	住友倉庫CSIRT
チームの略称	SWC-CSIRT
所属する組織名	株式会社住友倉庫
設立年月日	2015-11-01
チームの Email アドレス	csirt@sumitomo-soko.co.jp
チームサイト	
所属組織サイト	http://www.sumitomo-soko.co.jp/
加盟年月	2016 年 03 月

1. 概要

住友倉庫 CSIRT は、物流事業・海運事業・不動産事業を展開する住友倉庫グループ各社を対象とする情報セキュリティ・インシデント対応チームであり、株式会社住友倉庫によって運営されています。

2. 設立の経緯・背景

近年、サイバー攻撃が高度化かつ巧妙化する中、住友倉庫グループ各社における情報セキュリティ事案の抑止及び事案発生時の被害最小化を図る体制を整備するため、株式会社住友倉庫は 2015 年 11 月 1 日付で社内横断組織「住友倉庫 CSIRT」を設置しました。

3. 会社内における位置づけおよび活動内容

住友倉庫 CSIRT は、株式会社住友倉庫の CSR 委員会 (内部統制部会) 内に設置された社内横断組織です。
平時は情報セキュリティに関する情報収集、住友倉庫グループ従業者への注意喚起、教育・研修、啓蒙活動等を行い、有事には外部機関からの連絡受付をはじめ、インシデントハンドリング全般を行うこととしています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

T-SIRT

チームの正式名称	Taisei-SIRT
チームの略称	T-SIRT
所属する組織名	大成建設株式会社
設立年月日	2013-01-01
チームの Email アドレス	t-sirt@taisei.co.jp
チームサイト	
所属組織サイト	http://www.taisei.co.jp/
加盟年月	2013 年 03 月

1. 概要

Taisei-SIRT (略称 T-SIRT) は、総合建設会社である大成建設株式会社 (http://www.taisei.co.jp/) の CSIRT で、大成建設とその情報子会社である株式会社大成情報システムにより運営しています。

2. 設立の経緯・背景

従来から電子情報セキュリティインシデント対応や脆弱性情報の収集を情報企画部の役割として運用してきましたが、近年の高度なサイバー攻撃の頻発や政府及び顧客企業からの情報セキュリティ緊急時対応体制強化の要請といった状況に鑑み、2013 年 1 月、情報管理関連規程に CSIRT の設置を明示し、重大インシデントの定義、報告ルール、CSIRT の機能を明確にして緊急時対応体制を強化しました。

3. 会社内における位置づけおよび活動内容

T-SIRT は大成建設社長室情報企画部と大成情報システム双方のメンバーで構成される仮想的な組織体で、メンバーは情報企画部長 (大成情報システム 社長を兼務) の指名により決まります。

T-SIRT は、大成建設内で発生したインシデントに対して直接対応を行なう組織内 CSIRT としての役割を担うだけでなく、大成建設グループ、及び図面や企画書・計画書などのお客様の情報を共有する JV 工事作業所を構成する協力会社、専門工事業者を Constituency の対象に含め技術的な支援や調整を行います。

平時及び事故発生時、T-SIRT は以下の機能を果たします。
a)会社全体の電子情報セキュリティレベル向上のための施策 (教育含む) の検討・実施。
b)電子情報セキュリティ事故発生防止のための監視、検知及び警告。
c)事故発生時における技術対応及び指示・助言、並びに被害最小化のための施策実施。

特に、電子情報セキュリティに関わる重大インシデントが発生した場合、情報企画部長は会社のリスク管理体制に参画すると共に T-SIRT に対応を指示し、T-SIRT はインシデント解決のための技術的な支援を行います。

また、情報管理に関わる課題を検討する部門横断の組織を T-SIRT が運営することにより、会社の情報やお客様の情報の取り扱いに関わる業務手順、ICT 機器の取り扱いルール等の改善を行いインシデント発生の予防や再発防止に努めています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TAKENAKA-SIRT

チームの正式名称	TAKENAKA Security Incident Response Team
チームの略称	TAKENAKA-SIRT
所属する組織名	株式会社竹中工務店
設立年月日	2006年4月1日
チームの Email アドレス	Takenaka-sirt@takenaka.co.jp
チームサイト	
所属組織サイト	http://www.takenaka.co.jp/
加盟年月	2016 年 07 月

1. 概要

TAKENAKA-SIRTは、総合建設会社である株式会社竹中工務店によって運営されているCSIRTで、竹中グループを活動範囲としています。

2. 設立の経緯・背景

弊社では、2006年にセキュリティグループを設置して、CSIRTに関する業務を実施してきました。グループ全体を対象として昨今の高度化するサイバー攻撃に対し、被害の最小化を図るためには、他社や外部機関との情報連携が重要であるため、TAKENAKA-SIRTとして新たに発足いたしました。

3. 会社内における位置づけおよび活動内容

(1)位置付け
　情報セキュリティ主管部門の総務室とグループICT推進室のメンバーで、インシデント対応を含む情報セキュリティに関する活動を行っています。

(2)活動内容
　竹中グループにおいて主に以下の活動を実施しています。
① 情報セキュリティインシデントに対する未然防止
　・社会動向、技術動向調査
・セキュリティルールの制定、対策の立案
・セキュリティ関連情報の提供及び教育・啓蒙
・セキュリティ対策実施状況チェック
・インシデント検知、連絡受付
② 情報セキュリティインシデントの早期復旧、被害の拡大防止及び再発防止
・インシデント対応

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TC-CSIRT

チームの正式名称	Tokyo Century Computer Security Incident Response Team
チームの略称	TC-CSIRT
所属する組織名	東京センチュリー株式会社
設立年月日	2016/4/1
チームの Email アドレス	tc-csirt@tokyocentury.co.jp
チームサイト	
所属組織サイト	https://www.tokyocentury.co.jp
加盟年月	2016 年 08 月

1. 概要

TC-CSIRT は、東京センチュリー株式会社内の関係部署で構成する CSIRT です。

2. 設立の経緯・背景

当社では、従来より情報セキュリティに対して様々な取組を実施してきましたが、高度化・巧妙化するサイバー攻撃や情報セキュリティインシデント対して組織横断的に迅速に対応するため、2016年4月1日にCSIRTチームを設立致しました。

3. 会社内における位置づけおよび活動内容

(1)会社における位置づけ
TC-CSIRT は、東京センチュリーのシステム部門を中心として、IT 推進部内に設置する仮想的な組織です。

(2)活動内容
①インシデント対応
・サイバー攻撃に起因するコンピュータセキュリティインシデントに対し、社内関係部署や社外組織との連携により被害拡大防止を図る。
② 予防的活動
・外部CSIRTとのインシデントや脆弱性等の情報交換
・インターネットでの脆弱性情報検索
・社内およびグループ会社向け情報発信
・教育訓練（標的型攻撃メール訓練等）の実施
・脆弱性診断・対応
・通信の監視・遮断

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TC-SIRT

チームの正式名称	トヨタコネクティッドサート
チームの略称	TC-SIRT
所属する組織名	トヨタコネクティッド株式会社
設立年月日	2017年1月1日
チームの Email アドレス	list-tc-sirt@mail.toyotaconnected.co.
チームサイト	
所属組織サイト	http://www.toyotaconnected.co.jp/
加盟年月	2017 年 12 月

1. 概要

当社は、トヨタ自動車のコネクティッド戦略の中核的な役割を担い、テレマティクスサービス「G-BOOK」「T-Connect」など、さまざまなコネクテッドサービスを提供しています。「ITによってお客様との接点を作る」ことを基本とし、新しいモビリティ社会の発展と自動車ビジネスの変革を目指します。

2. 設立の経緯・背景

近年高度な攻撃手法を用いて継続的・組織的に行われるサイバー攻撃に対して、従来の予防に軸足を置いた対策では限界があるため、インシデント発生を前提とした早期発見・被害拡大防止の機能や体制であるTC-SIRTを構築しました。

3. 会社内における位置づけおよび活動内容

TC-SIRTは、代表取締役 副社長直属で、「セキュリティ」に関することは全社横断的に対応する組織です。

平時は、未然防止や各種実施策の品質向上を行いながら、インシデントの早期検出・被害拡大防止に努めます。

有事の際は、TC-SIRTが情報を集め一元管理し、発生部門やシステム管理部門などと連携してインシデント対応を指揮します。また、予め定義したインシデントレベルに応じて、社内マネジメント層、関連企業、および外部機関などに報告、連絡を行ないます。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TDC-CSIRT

チームの正式名称	TDC-CSIRT
チームの略称	TDC-CSIRT
所属する組織名	TDCソフト株式会社
設立年月日	2015-01-06
チームの Email アドレス	tdc_csirt@tdc.co.jp
チームサイト	
所属組織サイト	https://www.tdc.co.jp/
加盟年月	2015 年 03 月

1. 概要

TDC-CSIRT は TDCソフト株式会社が運営する CSIRT 組織です。

弊社は 1962 年に創業し、独立系 SI 企業としてお客様のビジネスニーズに IT の力で貢献してきました。
詳細は弊社ウェップサイト (http://www.tdc.co.jp/) をご覧ください。

2. 設立の経緯・背景

弊社では、従前より情報システム部門及び品質保証部門主導によりセキュリティ対策を実施してきました。しかしながら昨今のセキュリティ状況を踏まえ、社内においてはより迅速なセキュリティレスポンス活動を目指すと共に、社外の CSIRT 組織との情報共有と相互貢献を行うために CSIRT を設立いたしました。

3. 会社内における位置づけおよび活動内容

TDC-CSIRT は全社横断組織として、弊社グループ企業全体をサービス対象としています。
2015 年 4 月現在では主に以下のサービスを情報セキュリティの専門知識を有するメンバーが提供しています。
・脆弱性情報の収集と周知及び対策支援
・インシデント発生時の対応支援

また、今後は以下のセキュリティ品質向上に資するサービスを提供する予定です。
・セキュアプログラミング教育
・脆弱性診断 / ペネトレーション試験

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TDU-CSIRT

チームの正式名称	東京電機大学シーサート
チームの略称	TDU-CSIRT
所属する組織名	東京電機大学総合メディアセンター
設立年月日	2016-06-14
チームの Email アドレス	tdu-csirt@csirt.dendai.ac.jp
チームサイト	
所属組織サイト	http://www.dendai.ac.jp/
加盟年月	2016 年 06 月

1. 概要

本学は、1907年に創立した理工系総合大学です。「技術で社会に貢献する人材の育成」を使命とし、建学の精神「実学尊重」、教育・研究理念「技術は人なり」を掲げ、有為な人材を輩出しています。

TDU-CSIRTは、大学と大学のブランド価値を守るために必要なインシデント対応および発生の予防を行う組織として活動しています。

2. 設立の経緯・背景

情報セキュリティ対策は、大学組織でも喫緊の課題であり、特に本学の「顔」の一つであるセキュリティ関連の体制強化・構築は急務です。
そのため、情報セキュリティマネジメントおよび事業継続計画の立案等を行うことを目的としてCISOを設置し、その配下でインシデント対応を図る組織としてTDU-CSIRTを構築しました。

3. 会社内における位置づけおよび活動内容

TDU-CSIRTは、学内の情報セキュリティに関する信頼できる対応・対策窓口として設置しています。学内の情報基盤であるインフラを担当する総合メディアセンターが中心となり、体制を構築しています。学科・他部署の担当もCSIRTの一員となることを検討しています。

主な活動内容は、以下の通りです。
- ・セキュリティインシデントの検知、解決、迅速な復旧
- ・学内（学外）への適切な情報提供
- ・セキュリティに対する意識向上の啓発活動
- ・日常訓練の実施
- ・学外組織との連携強化

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TEIJIN-CSIRT

チームの正式名称	TEIJIN Computer Security Incident Response Team
チームの略称	TEIJIN-CSIRT
所属する組織名	帝人株式会社
設立年月日	2016/4/1
チームの Email アドレス	teijin-csirt@teijin.co.jp
チームサイト	
所属組織サイト	http://www.teijin.co.jp/
加盟年月	2016 年 11 月

1. 概要

帝人株式会社および帝人グループの情報資産、情報システムをセキュリティリスクから守るために結成されたファンクションチームです。
グループ内の情報システム組織や社内外の部門・組織と連携を取りながら活動を行います。

2. 設立の経緯・背景

帝人グループでは技術情報や顧客情報を防衛することを目的とし、情報セキュリティの強化に努めてきました。
しかしながら、サイバー攻撃は高度化、複雑化してきており、防衛のみならずセキュリティインシデントの発生も想定し、社内外への影響を極小化する為2016年にCSIRT体制を設立しました。

3. 会社内における位置づけおよび活動内容

本CSIRTは、セキュリティ専任部隊として帝人株式会社を含む帝人グループにおいて、以下の活動を目的としています。
・セキュリティインシデントを迅速に把握し、被害の拡大を防ぐ。
・セキュリティインシデントの早期解決を支援する。
・セキュリティインシデントの発生を予防する。
・セキュリティインシデントに関する情報、対応のノウハウを蓄積し、グループ全体のセキュリティレベル向上に貢献する。
・帝人グループ内の関係者、および社外の専門家・関係者と連携し、情報セキュリティに関する統一的な窓口となる。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TEPCO-SIRT

チームの正式名称	東京電力セキュリティインシデントレスポンスチーム
チームの略称	TEPCO-SIRT
所属する組織名	東京電力ホールディングス株式会社
設立年月日	2015-07-01
チームの Email アドレス	tepco-sirt@tepco.co.jp
チームサイト	
所属組織サイト	http://www.tepco.co.jp/index-j.html
加盟年月	2015 年 12 月

1. 概要

TEPCO-SIRTは、東京電力グループにおけるセキュリティインシデントの予防と、発生時の迅速な対応を目的としています。

2. 設立の経緯・背景

サイバー攻撃手法の複雑・巧妙化をはじめとして、サイバーセキュリティリスクが深刻化しています。この状況を踏まえ、東京電力グループとしてのセキュリティ管理水準向上を目指すために設立しました。

3. 会社内における位置づけおよび活動内容

(会社内における位置づけ)
TEPCO-SIRTは、東京電力グループのセキュリティ管理機能全体を統括する組織として、各種活動を行っています。

(活動内容)
・セキュリティ関連情報収集
・セキュリティリスク管理
・システム開発に関わるセキュリティ設計支援
・セキュリティインシデント対応

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Suntory CSIRT

チームの正式名称	Suntory Computer Security Incident Response Team
チームの略称	Suntory CSIRT
所属する組織名	サントリーシステムテクノロジー株式会社
設立年月日	2016年1月4日
チームの Email アドレス	csirt@ml.suntory.co.jp
チームサイト	
所属組織サイト	http://www.suntory.co.jp/sst/
加盟年月	2017 年 11 月29日

1. 概要

サントリービジネスシステム株式会社（SBU）の情報システム部門およびその子会社のサントリーシステムテクノロジー株式会社（SST）は、酒類や飲料を中心に様々な事業を国内外に展開しているサントリーグループ全体の情報化戦略の策定・推進および情報システムの企画・構築・運用を担っています。

2. 設立の経緯・背景

Suntory CSIRTは情報セキュリティの脅威（サイバーテロ・不正利用・情報漏洩など）に対して迅速に対応するため、2016年1月4日に専門チームとして、設立しました。

3. 会社内における位置づけおよび活動内容

Suntory CSIRTはSBUとSSTのセキュリティ担当からなるバーチャル組織です。
サントリーグループにおけるセキュリティインシデントの
・発生を予防する
・万一発生した場合は「もれなく」「迅速」「正確」に対処する。
ことを組織目標として、日々活動を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TEPSYS-SIRT

チームの正式名称	テプコシステムズセキュリティインシデントレスポンスチーム
チームの略称	TEPSYS-SIRT
所属する組織名	株式会社テプコシステムズ
設立年月日	2017年4月1日
チームの Email アドレス	tepsys-sirt@tepsys.co.jp
チームサイト	
所属組織サイト	http://www.tepsys.co.jp
加盟年月	2017 年 10 月

1. 概要

TEPSYS-SIRTは、東京電力ホールディングスの情報子会社であるテプコシステムズにおけるセキュリティインシデントへの適切な対処及びセキュリティ事故に対するリスクの極小化を目的とするSIRTです。

2. 設立の経緯・背景

弊社では、東京電力ホールディングスの情報子会社として、セキュリティ対策の構築やインシデントレスポンス向上等の検討を行い、セキュリティ事故の防止及び発生時のリスクの極小化に努めています。
今回、全社的なセキュリティマネジメント体制整備の一環として、部門横断型の対応チームとして結成しました。
また、東京電力ホールディングスのTEPCO-SIRTとの連携を行い、グループ全体のセキュリティレベル向上に貢献します。

3. 会社内における位置づけおよび活動内容

TEPSYS-SIRTは、セキュリティマネジメントや個人情報の扱いに精通したセキュリティスペシャリストによる部門横断型のチームとして、社内のセキュリティ対策、規程類の構築、社員教育及びインシデント対応を行っています。
対象範囲がH／W、S／W、N／Wなどの技術的な内容にとどまらず、物理的・人的・組織的セキュリティ全般の対策を行うことから「SIRT」と称しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

SURUGA CSIRT

チームの正式名称	スルガ銀行CSIRT
チームの略称	SURUGA CSIRT
所属する組織名	スルガ銀行株式会社
設立年月日	2014-04-01
チームの Email アドレス	csirt@surugabank.co.jp
チームサイト	
所属組織サイト	https://www.surugabank.co.jp/surugabank/index.html
加盟年月	2015 年 03 月

1. 概要

SURUGA CSIRT は、スルガ銀行グループ全企業のシステムに関するセキュリティインシデントに対応し、リスクを極小化することを目的とした組織です。

2. 設立の経緯・背景

年々増加する情報セキュリティリスクにスルガ銀行グループ一体で対応するため、専門チームとして設置されました。

3. 会社内における位置づけおよび活動内容

1.位置づけ
システム部内の運用グループ内に情報セキュリティ担当専門チームとして設置。セキュリティオペレーションセンターを兼務します。

2.活動内容
(1)グループ企業内インフラに対するセキュリティ対応
・セキュリティインシデント発生時のハンドリング
・脆弱性情報の収集
・脆弱性改善状況のモニタリング
・セキュリティ対策の立案　等
(2)インターネットバンキングに対するセキュリティ対応
・脆弱性情報の収集
・攻撃情報の収集
・対応策策定および実施　等

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TIS-CSIRT

チームの正式名称	TISシーサート
チームの略称	TIS-CSIRT
所属する組織名	TIS株式会社
設立年月日	2016年4月1日
チームの Email アドレス	tis-csirt@ml.tis.co.jp
チームサイト	
所属組織サイト	http://www.tis.co.jp/
加盟年月	2016 年 07 月

1. 概要

TIS-CSIRT は、TIS株式会社が運営する組織内 CSIRT です

TISは、「情報の価値を高めるサービス」を提供し続けることで、
知的で感性豊かな「ゆとりある生活」を実感できる社会の創造に貢献します。

2. 設立の経緯・背景

TISでは、2004年より、社内のSIRT運営を実施していましたが、
個々の企業のみならず日本企業を幅広く攻撃するような
サイバー攻撃が多発している状況から自社内の管理に閉じ、
インシデント発生後の事後対応を中心とするのではなく、
他社との情報共有、意見交換による未然防止策の検討、実施の重要性を感じ
2016年4月1日に設立されました。

3. 会社内における位置づけおよび活動内容

(1)位置づけ
弊社総務部セキュリティ管理グループが社内外との情報共有、意見交換窓口として活動し
インシデント発生後対応、拡散防止を実施しています。

(2)活動内容
サイバー攻撃に関する早期の情報入手
未然防止策の検討、実施
インシデント発生後対応、拡散防止

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TKK-CSIRT

チームの正式名称	東急電鉄CSIRT
チームの略称	TKK-CSIRT
所属する組織名	東京急行電鉄株式会社
設立年月日	2016年4月1日
チームの Email アドレス	tkk-csirt@tkk.tokyu.co.jp
チームサイト	
所属組織サイト	http://www.tokyu.co.jp
加盟年月	2017 年 04 月

1. 概要

TKK-CSIRTは、東京急行電鉄（株）のシステム部門により運営されているCSIRTです。

東急グループは、1922年の「目黒蒲田電鉄株式会社」設立に始まり、2016年9月末現在、218社8法人（株式上場会社6社）で構成され、交通事業、不動産事業、生活サービス事業、ホテル・リゾート事業を事業分野としています。弊社は、その中核企業として、鉄道事業を基盤とした「街づくり」を事業の根幹に置きつつ、長年にわたって、皆さまの日々の生活に密着したさまざまな領域で事業を進めています。

2. 設立の経緯・背景

情報セキュリティ対策に関し、これまで弊社では基本的セキュリティルールは存在していたものの、実際のセキュリティ対策の実施は社内の各部門および東急電鉄グループ各社の裁量による部分が多く、また体制も不明確でした。しかしながら、昨今の脆弱性の発見やサイバー攻撃に伴うセキュリティリスクの高まりを受け、東急電鉄グループ各社も巻き込んだ体制の整備・強化をはかり、セキュリティインシデントへの対応を迅速に行う必要性を感じたことから、TKK-CSIRTを設立いたしました。

3. 会社内における位置づけおよび活動内容

TKK-CSIRTは東京急行電鉄の情報システム部門に設置されるバーチャルチームです。

チームメンバーは東京急行電鉄の情報システム部門の社員を中心とし、情報子会社および情報セキュリティベンダとともに日々のインシデント予防業務を推進するとともに、インシデント発生時には関係部門および東急電鉄グループ各社と連携をとりつつ対応を行います。

TKK-CSIRTの活動範囲は、弊社社内の各部門および東急電鉄グループ各社を対象とします。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

T2 CERT

チームの正式名称	東京工業大学 情報システム緊急対応チーム
チームの略称	T2 CERT
所属する組織名	国立大学法人　東京工業大学
設立年月日	2014年10月3日
チームの Email アドレス	contact@cert.titech.ac.jp
チームサイト	http://cert.titech.ac.jp
所属組織サイト	http://www.titech.ac.jp
加盟年月	2017 年 02 月

1. 概要

東工大CERT(T2 CERT)は、国立大学法人東京工業大学（http://www.titech.ac.jp/）によって運営されているCSIRTです。

東京工業大学は、創立から130年を越える歴史をもつ国立大学であり、日本最高の理工系総合大学です。世界を舞台に科学技術の分野で活躍できる人材の輩出と地球規模の課題を解決する研究成果によって社会に寄与し、長期目標である「世界最高の理工系総合大学」の実現を目指します。

2. 設立の経緯・背景

本学を脅かすサイバー攻撃に対し、本学では情報セキュリティ確保のため様々な対策を実施してきました。
しかし、2012年9月に発生したセキュリティ事案においては、WEBサイトを外部業者へ委託管理していたことが災いし、本学の情報セキュリティ対策が及ばないケースでありました。このような実質的に本学の管理下にない情報システムを含めた全学の情報セキュリティ対策を実施できる権限を有する組織が強く求められ、東工大CERT(T2 CERT)が設立されました。

3. 会社内における位置づけおよび活動内容

東工大CERT(T2 CERT)は本学の情報セキュリティ監査・危機管理専門委員会内に設置され、CISOから権限を任された独立性の高い組織です。学術国際情報センターの教員に加え、情報基盤課の事務職員・技術職員により構成されています。また、学術国際情報センターのネットワーク/認証基盤担当であるNOC/NAPのメンバーの一部が部分的に東工大CERTに加わり、普段から連携のとれた体制を築いています。
東工大CERTは、本学における研究/教育/事務活動等を促進させるため、安全な計算機環境を提供する事を役割としています。

主な活動は以下の通りです。

・インシデントハンドリング
・インシデント/セキュリティイベント検知
・セキュリティ情報の発信
・脆弱性調査
・セキュリティ教育/啓発活動

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TM-SIRT

チームの正式名称	Trend Micro Security Incident Response Team
チームの略称	TM-SIRT
所属する組織名	トレンドマイクロ株式会社
設立年月日	2013-01-07
チームの Email アドレス	TrendMicro-SIRT_Japan@trendmicro.
チームサイト	http://www.trendmicro.co.jp/jp/about-us/csr/for-society/tm-sirt/index.html
所属組織サイト	http://www.trendmicro.co.jp/jp/index.html
加盟年月	2013 年 02 月

1. 概要

トレンドマイクロはコンピュータ及びインターネット用の情報セキュリティ対策製品・サービスなどを開発し、情報セキュリティソリューションの提供を行っております。

2. 設立の経緯・背景

2005 年から全社的なインシデントに対応するインシデントレスポンスチームを構築致しました。ここでは人・物理・技術いずれのセキュリティ事案も取り扱ってきました。

しかし、コンピュータセキュリティインシデントの取り扱いが増加し、コンピュータセキュリティインシデントを取り扱うチームを独立・専門化させ、Trend Micro Security Incident Response Team (TM-SIRT) を構築いたしました。

3. 会社内における位置づけおよび活動内容

＜会社内における位置づけ＞
－中心部署・メンバーについて
解析 (TrendLabs) 部門や調査 (Forward looking Threat Research) 部門や監視部門 (Threat Monitoring Center) を中心に、サポート関連部門、マーケティング関連部門、IS 部門などから主要となるメンバーを「人数を限定」且「管理職以上」の人員を参画させ、仮想組織として社内で位置づけられております。
－予算の出所
必要性の高い部門において計上を行っております。
－対応に必要な意思決定のフロー
基本的には TM-SIRT 内で即座に判断が出来るように体制を取っております。TM-SIRT で判断が出来ない場合は直接経営層との意思決定を行う形になります。
－インシデント対応体制概要
「TM-SIRT 窓口への問い合わせ」→「所属メンバーいずれかから初期回答」→「 (クローズ出来ない場合) 調査」→「緊急会議の招集 (今後の対応方針の検討) 」→「 (緊急会議で定められた) アクションの実施」→「レビュー会議の実施 (緊急または月例) 」

＜活動内容＞
－対応しているインシデントなど CSIRT が実際に行なっている活動
(前提：社内 / 外部 (公的機関や CSIRT) からの問い合わせ対応)

事前対応：技術・セキュリティ動向調査、解析・調査・監視部門から出てくる情報の集約・通知等
事後対応：インシデントハンドリング、コーディネーション、情報統制等
品質向上：ポリシーからアクションへの落とし込みと見直し、社内勉強会の実施等
－主に対応していること
昨今のサイバー攻撃に関する全般的な情報収集と対応
－対応していないこと
・各部門で判断すべきコンピュータセキュリティインシデント
・コンピュータセキュリティインシデント以外のインシデント
・情報漏えいにつながるコンピュータセキュリティインシデント

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TMC-SIRT

チームの正式名称	Toyota Motor Corporation Security Incident Response Team
チームの略称	TMC-SIRT
所属する組織名	トヨタ自動車株式会社
設立年月日	2013-11-01
チームの Email アドレス	TMC-SIRT@mail.toyota.co.jp
チームサイト	
所属組織サイト	http://www.toyota.co.jp
加盟年月	2013 年 10 月

1. 概要

TMC-SIRT は、トヨタ自動車株式会社内の関係部署で構成する、セキュリティインシデントレスポンスチームです。

2. 設立の経緯・背景

トヨタでは、これまでもお客様情報や営業秘密をはじめとする情報資産に対するセキュリティ向上のため、様々な対策を講じてきました。しかしながら、近年のサイバー攻撃や不正アクセスなど、情報流出やシステム障害につながる脅威は一層高度化・複雑化しています。

こうした状況を踏まえ、情報セキュリティインシデントが発生した場合に、迅速に対応し、被害拡大の防止やサービスの早期復旧を実現できるよう、2012 年に CSIRT 設立を計画しました。

その後 1 年以上に亘る準備期間を経て、2013 年 11 月 1 日、「TMC-SIRT」を設立する運びとなりました。

3. 会社内における位置づけおよび活動内容

TMC-SIRT は、総務部門・IT 部門を中心とした関係部署で構成される、仮想的な組織です。発生事案に応じて、広報機能、法務機能なども参画して、対応にあたります。なお、コンピュータ関連に限らず社内で発生した情報セキュリティインシデントに幅広く対応する、という意思を込めて、CSIRT ではなく SIRT としました。

活動内容は、主に以下の二点です。
(1)インシデントの未然防止活動
・リスク情報の収集
・定期的な社内点検
・社内体制の継続的な改善
(2)インシデント対応
・発生時から解決までの一連の処理
(連絡受付、対応要否判断、分析、復旧、再発防止、報告など)
トヨタでは、SIRT 設立を機に、情報セキュリティレベルの向上に一層努めてまいります。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TMHD-CSIRT

チームの正式名称	東京海上ホールディングス　シーサート
チームの略称	TMHD-CSIRT
所属する組織名	東京海上ホールディングス株式会社
設立年月日	2013-06-01
チームの Email アドレス	tmhd-csirt@tokiomarinehd.com
チームサイト	
所属組織サイト	http://www.tokiomarinehd.com/
加盟年月	2014 年 07 月

1. 概要

TMHD-CSIRTは、東京海上ホールディングスが運営するCSIRTです。

2. 設立の経緯・背景

TMHD-CSIRTは、東京海上グループにおけるセキュリティ管理態勢の強化をミッションとしています。

3. 会社内における位置づけおよび活動内容

TMHD-CSIRTは、主に以下の活動を実施しています。
・グループ会社におけるセキュリティ強化の支援
・外部関連機関との連携窓口
・国内グループ会社におけるセキュリティインシデント発生時の対応支援

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TMHH-CSIRT

チームの正式名称	東京都保健医療公社　シーサート
チームの略称	TMHH-CSIRT
所属する組織名	公益財団法人東京都保健医療公社　事務局
設立年月日	2017 年 3 月 2 日
チームの Email アドレス	csirt@tokyo-hmt.jp
チームサイト	
所属組織サイト	http://www.tokyo-hmt.jp/
加盟年月	2018 年 05 月

1. 概要

私たち東京都保健医療公社は 6 病院と 1 検診センターを有する公益財団法人です。
昭和 63 年に東京都の地域医療を推進するために設立した東京都の管理団体となります。
6 病院合計の病床数は 2225 床、1 日の平均外来患者数は約 3,000 人、平均入院患者数は約 1,600 人となっており東京都の地域医療支援病院として日々医療を提供しております。

2. 設立の経緯・背景

東京都は総務局に平成 28 年に今後増え続けるサイバー攻撃への対処を専門的に行う東京都 CSIRT を設置しました。一方で、「東京都サイバーセキュリティ基本方針」によって、東京都の管理団体は東京都に準じた情報セキュリティ対策を講じることとなっています。その為、当該方針に則った上で、多くの要配慮個人情報を扱う医療機関として情報セキュリティサイバー攻撃や過失による事故から患者情報を守ることを第一に、サイバーセキュリティの予防及び重大な事故に組織的な対応を行うため、THMM-CSIRT を設置しました。

3. 会社内における位置づけおよび活動内容

(1) 位置づけ
THMM-CSIRT は常務の判断により召集される各病院を統括する組織です。

(2) 活動内容
・サイバーセキュリティ関連情報収集
・東京都 CSIRT との連携
・社内関係部署とのセキュリティに関する窓口
・各種訓練及び内部監査の実施

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TOMOWEL-CSIRT

チームの正式名称	TOMOWEL Computer Security Incident Response Team
チームの略称	TOMOWEL-CSIRT
所属する組織名	共同印刷株式会社
設立年月日	2017年10月3日
チームの Email アドレス	csirt@kyodoprinting.co.jp
チームサイト	
所属組織サイト	https://www.kyodoprinting.co.jp/
加盟年月	2017 年 12 月

1. 概要

TOMOWEL-CSIRTは、共同印刷株式会社が運営するCSIRTです。

共同印刷グループは、出版物や商業印刷物などの印刷事業を核とし、交通ICカード、パッケージ、プロモーションやITソリューション等、幅広い分野のサービスを手掛けており、社会への新たな価値の提供および社会・文化の発展に力を尽くしております。

2. 設立の経緯・背景

近年、個人情報保護をはじめとする情報セキュリティの重要性が高まる一方、サイバー攻撃の高度化など企業を取り巻く事業リスクは飛躍的に増加しています。従来の枠組みにとらわれない情報機器特有のインシデントに対応する専門組織や部門横断的な情報連携の必要性の高まりをうけ、2017年に組織内CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

TOMOWEL-CSIRTは、「危機管理委員会」のもとで、コンピュータ、ネットワーク等、情報機器が関るインシデントが発生した際、各部門よりメンバーが集結し対応にあたる仮想的組織です。
緊急事態での対応指揮および技術的な対策のほか、平時には啓蒙活動など、既存の情報セキュリティ体制と連携しながら事前予防に取り組むことで緊急事態を未然に防止する活動を実施します。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TOPPAN-CERT

チームの正式名称	TOPPAN Computer Emergency Response Team
チームの略称	TOPPAN-CERT
所属する組織名	凸版印刷株式会社
設立年月日	2010-08-01
チームの Email アドレス	cert@toppan.co.jp
チームサイト	
所属組織サイト	http://www.toppan.co.jp/
加盟年月	2011 年 06 月

1. 概要

TOPPAN-CERT は、凸版印刷株式会社 (http://www.toppan.co.jp/) によって運営されている CSIRT です。

トッパングループ各社は、「印刷テクノロジー (http://www.toppan.co.jp/print_technology/index.html)」を核に、情報コミュニケーション事業、生活環境事業、マテリアルソリューション事業の分野にわたり、新たな技術やビジネスモデルを創出し、お客さまや社会の課題解決につながるトータルソリューションをグローバルに展開しています。

2. 設立の経緯・背景

社内外における情報セキュリティに対する意識の高まりや、サイバー攻撃等の増加に伴うセキュリティインシデント対応技術の高度化などを受け、全社横断的に必要な機能として、2010 年 8 月に設立されました。

3. 会社内における位置づけおよび活動内容

TOPPAN-CERT は、社内に設置されている情報セキュリティ管理推進部会の下部組織として位置づけられ、主にセキュリティインシデントが社内で発生した際に技術的な対応を迅速に行うべく、本社スタッフをメンバーとして仮想的に構成された専門チームです。

当該チームは、セキュリティインシデントに対する事後対応のみではなく、関連技術動向の把握や社内セキュリティ教育の支援などによるセキュリティインシデントの未然防止活動、日本シーサート協議会等外部との正式窓口として相互協力関係の確保などの施策を実施いたしております。

なお、コンピュータウイルス対策については、同じく情報セキュリティ管理推進部会の下部組織として、本社スタッフに加え事業部門からもメンバーが参加する形での仮想的な専門チームが実施しているため、TOPPAN-CERT としては、スコープ外としております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

ToppanForms-CERT

チームの正式名称	TOPPAN FORMS CERT
チームの略称	ToppanForms-CERT
所属する組織名	トッパン・フォームズ株式会社
設立年月日	2015-09-15
チームの Email アドレス	tf-cert@toppan-f.co.jp
チームサイト	
所属組織サイト	http://www.toppan-f.co.jp/
加盟年月	2015 年 09 月

1. 概要

TOPPAN FORMS CERT は、トッパン・フォームズ株式会社 (http://www.toppan-f.co.jp/) によって運営されている CSIRT です。

トッパンフォームズは、ビジネスフォームやデータ・プリント・サービスなどの分野で培ってきた技術やノウハウをベースに、お客様の情報伝達を最適化する情報ソリューションカンパニーです。印刷物と電子ドキュメントの融合や、RFID・IC などの情報メディア、プリンテッド・エレクトロニクス技術を応用した製品開発など、「情報」を核としたさまざまな事業を展開しています。

2. 設立の経緯・背景

社内外における情報セキュリティに対する意識の高まりや、サイバー攻撃等の増加に伴うセキュリティインシデント対応技術の高度化などを受け、問題発生を前提とした、セキュリティインシデントに対応する専門チームとして、2015 年 9 月に設立されました。

3. 会社内における位置づけおよび活動内容

TOPPAN FORMS CERT は、社内に設置されている全社情報セキュリティ管理委員会の下部組織として位置づけられ、主にセキュリティインシデントが社内で発生した際に技術的な対応を迅速に行うべく、本社スタッフをメンバーとして仮想的に構成された専門チームです。

当該チームは、セキュリティインシデントに対する事後対応のみではなく、関連技術動向の把握や社内セキュリティ教育の支援などによるセキュリティインシデントの未然防止活動、日本シーサート協議会等外部との正式窓口として相互協力関係の確保などの施策を実施いたしております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TOSHIBA-CSIRT

チームの正式名称	TOSHIBA Computer Security Incident Response Team
チームの略称	TOSHIBA-CSIRT
所属する組織名	株式会社東芝
設立年月日	2012-04-01
チームの Email アドレス	csirt@ml.toshiba.co.jp
チームサイト	
所属組織サイト	http://www.toshiba.co.jp/
加盟年月	2015 年 08 月

1. 概要

TOSHIBA-CSIRT は、株式会社東芝が運営する東芝グループの CSIRT です。

2. 設立の経緯・背景

2004 年に発足した情報セキュリティの専任組織のもと、東芝グループの情報セキュリティ管理体制を整備し、情報セキュリティの管理強化に取り組んできました。2012 年には、高度化・巧妙化するサイバー攻撃への対応力を強化するため、情報セキュリティ専任組織内にインシデント対応等を専門とするグループを立ち上げ、情報システム部門や情報セキュリティ管理体制と連携した TOSHIBA-CSIRT を設置しました。

3. 会社内における位置づけおよび活動内容

TOSHIBA-CSIRT の活動は、イベントの監視、脆弱性情報の収集・連絡・適用、セキュリティ診断等のインシデント抑制から、インシデント発生時の原因分析、復旧対応・支援等の事後対応、教育、監査等の品質管理と CSIRT サービス全般に渡ります。東芝グループ内の情報通信システムを主な対象とし、製品管理部門との連携など活動範囲を広げています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TOYAL-CSIRT

チームの正式名称	TOYAL-CSIRT
チームの略称	TOYAL-CSIRT
所属する組織名	東洋アルミニウム株式会社
設立年月日	2017 年 4 月 3 日
チームの Email アドレス	toyal-csirt@toyal.co.jp
チームサイト	
所属組織サイト	http://www.toyal.co.jp
加盟年月	2018 年 06 月

1. 概要

東洋アルミニウム株式会社は、アルミニウム箔事業、パウダー・ペースト事業、ソーラー事業、日用品事業を展開しています。TOYAL-CSIRT は、東洋アルミニウム株式会社によって運営され、サイバー攻撃対策を中心に、社内のセキュリティインシデントの早期解決を推進するための組織です。

2. 設立の経緯・背景

TOYAL-CSIRT は、サイバー攻撃の高度化、巧妙化という背景を受け、サイバー攻撃に対する当社の抵抗力を高めるため、既存の ISMS 活動におけるサイバーセキュリティ対策部分について、インシデント発生時の対策を中心に、補完的に強化することを目的に、2017 年 4 月に設立致しました。

3. 会社内における位置づけおよび活動内容

TOYAL-CSIRT は ISMS 活動を中心的に担ってきた ISMS 中央事務局の内部に設置されており、ISMS 中央事務局メンバ並びに、情報システム部門のメンバから構成されています。
＜活動内容＞
・サイバーセキュリティリスクの「特定」
・サイバーセキュリティリスクに対する「防御」
・脅威の「監視と検知」
・インシデントが発生したときの「対応と復旧」
・サイバーセキュリティに関する「教育」

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TG CSIRT

チームの正式名称	東京ガスシーサート
チームの略称	TG CSIRT
所属する組織名	東京ガス株式会社
設立年月日	2015-07-01
チームの Email アドレス	tgcsirt@tokyo-gas.co.jp
チームサイト	
所属組織サイト	http://www.tokyo-gas.co.jp
加盟年月	2016 年 01 月

1. 概要

東京ガスグループは、半世紀近くにわたり「LNG のパイオニア、天然ガスのトップランナー」として、LNG バリューチェーンの確立・強化と天然ガスの普及・拡大に努めてきました。
弊社グループは日本で最もエネルギー需要が集積している関東圏を事業基盤とし、日本国内の都市ガス販売量の約 4 割を供給しています。
また、安全かつ安定的な供給をベースに、競争力ある電源の拡充・電力販売の拡大にも努め、ガスと電気および付加価値を組み合わせた最適なエネルギーソリューションを提供しています。

2. 設立の経緯・背景

TG CSIRT は、東京ガスグループのお客様の「安心、安全、信頼」を守り、インシデント発生時においても、その被害を極小化することを目的に、東京ガスのIT監理部門が主導し、2015 年 7 月に設立されました。

3. 会社内における位置づけおよび活動内容

(1)会社内における位置づけ
TG CSIRTは、東京ガスのIT監理部門を中心に、システム子会社である東京ガスiネット（株）の複数の情報セキュリティ関連部門が参画する仮想的な組織です。
(2)活動内容
東京ガスグループを対象に、情報システムに関わるインシデント対応、脆弱性ハンドリング、および外部組織との情報連携を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

transcosmos-CSIRT

チームの正式名称	トランスコスモス シーサート
チームの略称	transcosmos-CSIRT
所属する組織名	トランスコスモス株式会社
設立年月日	2016-04-01
チームの Email アドレス	transcosmos_csirt@trans-cosmos.co
チームサイト	
所属組織サイト	http://www.trans-cosmos.co.jp/
加盟年月	2016 年 06 月

1. 概要

transcosmos-CSIRTは、トランスコスモス株式会社および関連会社でのサイバーインシデント発生時の対応に関する取り決め策定、および周知徹底を行うこと、およびインシデント発生時の原因究明に必要となる仕掛けや仕組みを検討し、関連システムへの摘要を推進/監査することを目的とした組織です。

2. 設立の経緯・背景

従来より行ってきた情報セキュリティ対策だけでは対応しきれないサイバー攻撃などへの対応、対策の取り組みが必要であること、および実際のセキュリティインシデント発生体験を踏まえた、速やかなる対応体制および対応オペレーションの策定とその徹底を全社組織として束ねる部署が必要である、との判断の下に組成されたものとなります。

3. 会社内における位置づけおよび活動内容

従来より情報セキュリティ関連インシデント発生時のコーディネーションなどを行っていた、全社コンプライアンス対応を管理するコンプライアンス推進部門と連携し、よりシステム的な知識が必要となるサイバーインシデント対応に関する対策検討部分を担当する位置づけとなります。
主な活動としては、サイバーインシデント発生時に、より迅速かつ的確に情報収集が行えるよう、調査に必要となるデータやログが取得できるような仕掛けなどを定義したガイドラインの策定、および擬似的なインシデントの発生を想定した対応シミュレーション訓練を通しての、問題点や不足部分の洗い出しを定期的、かつ経営層も含めた全社的なものとして推進していくことを予定しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TSUTAYA-SIRT

チームの正式名称	TSUTAYA Security Incident Response Team
チームの略称	TSUTAYA-SIRT
所属する組織名	株式会社TSUTAYA
設立年月日	2018 年 2 月 1 日
チームの Email アドレス	tsutaya-sirt@ccc.co.jp
チームサイト	
所属組織サイト	https://www.tsutaya-ltd.co.jp/
加盟年月	2018 年 05 月

1. 概要

株式会社 TSUTAYA は、生活提案の場としての「TSUTAYA」の企画ならびにFC展開事業、ネット分野における生活提案プラットフォーム企画・運営事業を手掛けています。TSUTAYA-SIRT は、自社で運用するサービスで発生するセキュリティインシデントに対し、緊急対応を行います。

2. 設立の経緯・背景

当社は、社内の IT 部門にて独自にセキュリティ対策や対応を実施してきました。しかしながら、昨今のサイバー攻撃が巧妙化され、大規模なセキュリティインシデントが頻発する脅威に対し自社のみでの対応は難しく、インシデント検知から迅速な分析 / 対応する体制ならびに社内外との情報共有が不可欠と判断し、2018 年 2 月に「TSUTAYA-SIRT」を設立いたしました。

3. 会社内における位置づけおよび活動内容

(1) 位置付け
TSUTAYA-SIRT は、各 IT 部門からの兼務メンバーで構成されるチームで、株式会社 TSUTAYA 内で発生するセキュリティインシデントの対応を行います。

(2) 活動内容
TSUTAYA-SIRT は、セキュリティインシデントの予防および、セキュリティインシデント発生時の対応を中心に、以下の活動を実施しています。

- ・セキュリティ関連情報の収集
- ・セキュリティインシデント検知
- ・セキュリティインシデント発生時の対応

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TSUZUKI-CSIRT

チームの正式名称	都築CSIRT
チームの略称	TSUZUKI-CSIRT
所属する組織名	都築電気株式会社
設立年月日	2018年1月1日
チームの Email アドレス	tsuzuki-csirt@tsuzuki.co.jp
チームサイト	
所属組織サイト	http://www.tsuzuki.co.jp
加盟年月	2018 年 02 月

1. 概要

都築電気株式会社は、ICT企業です。メーカーや流通・サービス業から、金融業、医療・福祉、公共機関に至るまで、20,000社を超えるお客様との取引実績を誇る、システムコンサルティング・開発のトータルソリューションプロバイダです。

都築CSIRTは、顧客システムを対象としたセキュリティインシデントの対応を行います。
＊顧客システム：当社がお客様へ納品したシステムや機器など

2. 設立の経緯・背景

近年、サイバー攻撃による当社顧客システムへの不正アクセス被害が多発し、深刻な課題となっています。これをうけ、当社ではセキュリティインシデントへの対応能力強化および顧客システムの情報セキュリティ対策レベル向上を図るべく、「都築CSIRT」を立ち上げました。
2017年4月からセキュリティ整備WGを立ち上げ、
・インシデント対応計画の策定・セキュリティ開発ガイドラインの整備・インシデント対応ガイドラインの策定・エスカレーションプロセスの明確化・ログ取得・保管基準の定義など
重要なアクションプランとして14のタスクを設立へ向けて取り組みました。

3. 会社内における位置づけおよび活動内容

・会社内における位置づけ
都築CSIRTは、仮想組織です。情報システム部門、法的対応部門、顧客システムプロジェクト管理部門、顧客システム構築を担うSE・NEからの選抜メンバーにより構成されています。

・活動内容
都築CSIRTは、顧客システムで発生した情報セキュリティインシデントの対応や平時の予防対応を行います。＊社内システムは対象外です。

主な活動は、有事対応及び平時での予防対応や訓練を行い、それらから発生した課題を定期的に見直し（PDCAサイクルでの見直し）、インシデント対応能力強化および下記項目の質の向上に取り組みます。
・セキュリティ人材の育成
・顧客システム　セキュリティ維持管理
・インシデント対応ポリシー策定維持管理
・インシデント対応ガイドライン策定維持管理
・リスク分析/評価の実施
・脆弱性情報の収集・管理
・ナレッジの管理・共有　維持管理
・封じ込め手順の維持管理
・証拠保全手順の維持管理
・ログ取得、保管基準の維持管理

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TSYS-CSIRT

チームの正式名称	Toyotsu Syscom Corporation Computer Security Incident Response Team
チームの略称	TSYS-CSIRT
所属する組織名	株式会社 豊通シスコム
設立年月日	2015/8/1
チームの Email アドレス	tsys-csirt@tsyscom.co.jp
チームサイト	
所属組織サイト	https://www.tsyscom.co.jp/
加盟年月	2016 年 07 月

1. 概要

豊通シスコムは、豊田通商グループのシステムインテグレーターして、コンピュータ及びインターネット用のセキュリティ対策製品・サービスをビジネス展開し、総合セキュリティサービスの提供を行っております。

2. 設立の経緯・背景

2014年、過去の情報セキュリティソリューションの取り扱い実績を踏まえて、総合セキュリティサービスの提供を開始しました。
また、近年多発し、高度化するサイバー攻撃や不正アクセスへの迅速な対応が求められています。
こうした状況を踏まえて、2015年、当社としても社内外のインシデントに対するインシデントレスポンス体制を設立しました。

3. 会社内における位置づけおよび活動内容

社内インフラ組織、顧客サービスを提供する部門および社内外への広報部門間の連携組織を
TSYS-CSIRTと位置付けし、
・インシデントレスポンス支援
・組織内への意識向上教育・訓練の定期実施
を提供しております。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

TX-CSIRT

チームの正式名称	NTTテクノクロスシーサート
チームの略称	TX-CSIRT
所属する組織名	NTTテクノクロス株式会社
設立年月日	2016年7月1日
チームの Email アドレス	tx-csirt@cs.ntt-tx.co.jp
チームサイト	
所属組織サイト	https://www.ntt-tx.co.jp/
加盟年月	2017 年 12 月

1. 概要

当社は、旧NTTソフトウェア株式会社と旧NTTアイティ株式会社が合併し、NTTアドバンステクノロジ株式会社からメディア系技術の事業を譲受して2017年4月に誕生しました。NTTテクノクロスの「クロス」には、最先端技術を横断的に掛け合わせ、すなわちクロスさせることで、社会やお客さまの課題にあわせて応用し、ビジネス向上のお役に立ちたいという思いを込めています。NTT研究所の先進技術を活用し、皆さまに役立つソリューションを創出して、お客さまとともにその先の社会に貢献してまいります。

2. 設立の経緯・背景

サイバー攻撃が巧妙化、悪質化する中、NTTグループ内におけるサイバーセキュリティ態勢の益々の強化、信頼の確保が求められており、サイバーセキュリティインシデントの未然防止、被害局限化を目的に、2016年7月、旧NTTソフトウェア内に前身である「NS-CSIRT」を立ち上げ、活動を開始しました。2017年4月には、会社統合による社名変更により、名称も「TX-CSIRT」に改め、活動を継続しております。

3. 会社内における位置づけおよび活動内容

(1) 位置づけ
社内のセキュリティマネジメントを統括する「統合マネジメントシステム推進室（TMS室）」内に専担チームを配置し、高度な技術支援が必要な場合は、事業部に所属するセキュリティ技術者が支援する組織横断的なバーチャル体制で運営しています。

(2) 活動内容
主に、以下の活動を実施しています。
・セキュリティ関連情報提供
　脆弱性情報、インシデント事例、セキュリティ関連ニュース等のセキュリティ関連情報を社内に提供
・脆弱性情報ハンドリング
　ツールを活用して、脆弱性情報の収集と影響する機器、影響度を自動的に識別し、社内に情報配信するとともに、対応状況を把握、管理。
・インシデントハンドリング
　インシデントの検知・受付、トリアージュ、原因究明、対策支援、レポーティング、再発防止策検討等のハンドリング　業務。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

UCSIRT

チームの正式名称	Nihon Unisys Group Computer Security Incident Response Team
チームの略称	UCSIRT
所属する組織名	日本ユニシス株式会社
設立年月日	2009-01
チームの Email アドレス	ucsirt@ml.unisys.co.jp
チームサイト	
所属組織サイト	http://www.unisys.co.jp
加盟年月	2015 年 03 月

1. 概要

UCSIRT は、日本ユニシスグループ総合セキュリティ委員会に設けられた組織で、脆弱性情報のハンドリングと、日本ユニシスグループ内およびお客様で発生したセキュリティインシデントに対応することを目的としています。

2. 設立の経緯・背景

複雑化するコンピュータインシデントに対し、迅速な対応、および情報収集や予防策が重要となってきたことから、日本ユニシスグループでも組織内 CSIRT の構築がセキュリティ戦略の重要な課題と認識され、2009 年 1 月に設立しました。
当初は、グループ内およびお客様で発生したインシデントに速やかに対応するための、事後対応型チームとして組織化されましたが、後に、脆弱性情報のハンドリングを開始し、事前対応型の役割も担うようになりました。

3. 会社内における位置づけおよび活動内容

会社内における位置づけ
UCSIRT は、日本ユニシスグループ総合セキュリティ委員会内に設けられており、グループ内セキュリティ関連部門に所属するセキュリティスペシャリストを中心に組織されています。

活動内容
UCSIRT では、次の2つの活動を行っています。
(1)脆弱性情報ハンドリング
収集した脆弱性情報の内容を確認し、関連性・影響度に応じ、グループ従業員へ配信しています。

(2)インシデント対応
グループ内およびお客様で発生したセキュリティインシデントへの対応を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

URS-CSIRT

チームの正式名称	URシステムズ Computer Security Incident Response Team
チームの略称	URS-CSIRT
所属する組織名	株式会社　URシステムズ
設立年月日	2016年10月1日
チームの Email アドレス	urs-csirt@ur-systems.co.jp
チームサイト	
所属組織サイト	http://www.ur-systems.co.jp/
加盟年月	2017 年 04 月

1. 概要

株式会社URシステムズは、情報通信技術を活用した課題解決力と技術力により、お客様の新たなビジネス創造と発展に貢献します。

URS-CSIRTは、株式会社URシステムズが運営する組織内CSIRT です。

2. 設立の経緯・背景

当社は、2005年のPMS導入と2009年のISMS導入を契機に個人情報を含む情報資産に対して様々なセキュリティ対策を行ってきました。
また、近年のサイバー攻撃の高度化・複雑化による情報セキュリティ事件・事故が日本国内でも数多く報告されている状況を踏まえて、2016年10月にURS-CSIRTを設置しました。

3. 会社内における位置づけおよび活動内容

(1)会社内における位置づけ
URS-CSIRTは、社内の情報システムに関する企画部門を中心に、各部門から情報セキュリティに関する能力に長けたメンバを選抜して構成したチームです。

(2)活動内容
活動内容は以下の通りです。
・脆弱性情報の収集・評価・対策
・イベントの監視・検知
・インシデント発生時の原因分析、復旧対応・支援・事後対応
・情報セキュリティに関する教育・訓練

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

VZJ-CSIRT

チームの正式名称	VZJ-CSIRT
チームの略称	VZJ-CSIRT
所属する組織名	ベライゾンジャパン合同会社
設立年月日	2012-01
チームの Email アドレス	vzj-CSIRT@one.verizon.com
チームサイト	
所属組織サイト	http://www.verizonenterprise.com/jp/
加盟年月	2013 年 01 月

1. 概要

VZJ-CSIRT は、ベライゾンジャパン合同会社 (http://www.verizonenterprise.com/jp/) の CSIRT です。

2. 設立の経緯・背景

VZJ-CSIRT の設立は 2013 年 2 月です。

ダウ工業株 30 銘柄企業の一社であるベライゾンは、世界 150 ヶ国に通信、IT ソリューションを提供し、ネットワークの運用監視から万が一の情報漏洩事故発生時の対応に至るまで、総合的なセキュリティサービスを提供しています。国際カード会社認定 PCI Forensic Investigator (PFI) 機関でもあります。

ベライゾンは 2004 年より世界各国で発生した実際の企業漏洩インシデントの調査結果を分析し、集計結果を「データ漏洩・侵害調査報告書」として無料で公開し、企業が効果的な対策・対応がおこなえるよう、被害企業の共通項と推奨対策の提言を行っています。ベライゾンジャパンは、ベライゾンの日本法人として日本市場においても同様の活動を行うために、CSIRT を設立しました。

3. 会社内における位置づけおよび活動内容

フォレンジック調査対応部が中心となり、セキュリティコンサルとマーケティング部などをメンバー加えて VZJ-CSIRT を運営しています。

VZJ-CSIRT は、外部への情報展開を主眼に置いた組織です。ベライゾンが毎年公開している「データ漏洩・侵害調査報告書」には、ベライゾンのフォレンジック調査チームが対応したケースと、米国のセキュリティサービスやオーストラリアの連邦警察といった法執行機関や、2013 年版より US-CERT や各組織の CERT を含む計 19 の世界的セキュリティ機関が対応したインシデントを分析した統計情報がまとめられています。

VZJ-CERT では、データ漏洩・侵害調査報告書とフォレンジック調査対応部が調査した案件などから外部に提供可能な情報を展開していきます。また、4 半期に一度程度、セキュリティセミナーとして、セキュリティコンサルによる昨今のコンピューティングアタックの傾向とその対策を紹介しています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

W-CSIRT

チームの正式名称	ワンビシアーカイブズCSIRT
チームの略称	W-CSIRT
所属する組織名	株式会社ワンビシアーカイブズ
設立年月日	2016年7月1日
チームの Email アドレス	w-csirt@wanbishi.co.jp
チームサイト	
所属組織サイト	http://www.wanbishi.co.jp
加盟年月	2017 年 03 月

1. 概要

ワンビシアーカイブズはリスクマネジメントの一翼を担う企業として、企業情報の安全保管と管理の効率化をお手伝いする「情報資産管理事業」、個人のお客様が安心して生活していただけるよう、様々な生命・損害保険をご提案する「保険代理店事業」を行っております。

2. 設立の経緯・背景

近年、サイバー攻撃の急増により、情報漏洩やWebサイト改ざん、コンピュータウイルスなどのマルウエア（悪意のあるソフトウエア）感染といったサイバー空間でのセキュリティインシデントが後を絶ちません。
いざサイバーセキュリティインシデントが発生した際には経営の根幹を揺るがすものへと波及する可能性もあり、予防対策だけでなく、発生することを前提とした専門の組織体制を構築する企業が増えてきています。
当社でも身近に迫ってきている脅威に対応するため、また、事業の性質上の必要性、顧客からの要請が高まりつつあるため、W-CSIRTを設立いたしました。

3. 会社内における位置づけおよび活動内容

W-CSIRTはサイバーセキュリティインシデント対応の司令塔となる組織として社内関係部署との連携を行いつつ、以下の4つの業務を行っています。

1. サイバーセキュリティインシデントが発生した際の事後対応
2. 発生を未然に防ぐ事前対応
3. 会社組織としてのレベルアップを図るための品質向上
4. 社内外の関係者との一元的な連絡窓口

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

Wacoal-SIRT

チームの正式名称	Wacoal Security Incident Response Team
チームの略称	Wacoal-SIRT
所属する組織名	株式会社ワコール ホールディングス 株式会社ワコール
設立年月日	2017年10月26日
チームの Email アドレス	wacoal-sirt-ml@wacoal.co.jp
チームサイト	
所属組織サイト	http://www.wacoal.co.jp/
加盟年月	2018 年 01月

1. 概要

株式会社ワコールは、株式会社ワコールホールディングスの100%子会社で、インナーウェア（主に婦人のファンデーション、ランジェリー、ナイトウェアおよびリトルインナー）、アウターウェア、スポーツウェア、その他の繊維製品および関連製品の製造、卸売販売および一部製品の消費者への直接販売を主な事業としています。
Wacoal-SIRT（ワコールサート） は、ワコールグループにおけるセキュリティインシデントに対応する組織内 CSIRT です。その母体は、2005年ワコールグループ内組織「情報セキュリティ対策委員会（2012年、コンプライアンス委員会に統合）」のワーキンググループの一つとして、「ITセキュリティ分科会」という名称で組織横断的なメンバー10名程度で発足しました。以降同分科会は、毎年度メンバーの見直しを行って現在に至るまで活動を継続しています。

2. 設立の経緯・背景

いつでもどこでも商品が購入できる環境となった昨今、商品を販売するにあたり様々な情報を取り扱い、守らなければなりません。ワコールグループもそのような環境の中で外的・内的要因によるセキュリティ脅威から自己防衛するために日々対策、対応を実施しています。
近年、多種多様な脅威が企業を取り巻き1企業だけで対応していくことが困難な状況です。この度、NCA加盟各チームと連携を深め、セキュリティインシデントに対する効果的・迅速な対応を行うための情報を共有し、一丸となってセキュリティ脅威へ対応していくため、Wacoal-SIRTを設立しました。

3. 会社内における位置づけおよび活動内容

＜社内における位置づけ＞
Wacoal-SIRT は、ワコールホールディングス／ワコール社内のITセキュリティ分科会メンバー（経営企画部、情報システム部、WEB・通販関連管理部門からの選任社員）で構成されており、コンピュータに限らずセキュリティ全般に関するインシデントの対応チームとして位置づけています。

＜活動内容＞
(1)セキュリティ規程等の整備
(2)インシデントレスポンス
(3)インシデント予防策の実施
(4)組織内リスク分析とリスク低減のための対策実施
(5)従業員への脆弱性情報や注意喚起及びセキュリティ教育

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

WIRT

チームの正式名称	WIDE Incident Response Team
チームの略称	WIRT
所属する組織名	慶応義塾大学（WIDE プロジェクト）
設立年月日	2017年9月1日
チームの Email アドレス	csirt@wide.ad.jp
チームサイト	https://wirt.wide.ad.jp/
所属組織サイト	http://www.wide.ad.jp/
加盟年月	2018 年 01 月

1. 概要

WIDEプロジェクトは, インターネット技術の研究開発を目的とした産官学連携コンソーシアムであり, 1980年代後半より日本国内のバックボーン・ネットワークの構築, 及び国際接続を行っており, 国内の様々なISPと連携しながらインターネットの運用を行っています.
WIRTはWIDEプロジェクトが運用するバックボーン・ネットワーク (WIDE-BB) における組織内CSIRTです.

2. 設立の経緯・背景

WIDEプロジェクトではこれまでWIDE-BB内部でのインシデント対応やWIDE-BBに接続する下位組織でのインシデント対応状況の管理をWIDE-BBの運用メンバを中心に行ってきました. しかし, 昨今のサイバーセキュリティ脅威の高度化に対応して, 特にセキュリティインシデントに関する対外的な窓口機能の統合や組織間に跨がったCSIRTの交流が必要との認識にいたり, WIRTの設立に至りました.

3. 会社内における位置づけおよび活動内容

WIRTはWIDE-BBの運用チームに所属するメンバを中心に構成された組織内CSIRTです. WIRTはセキュリティインシデントに関するWIDEプロジェクトの対外的な窓口機能, WIDE-BB内部のインシデント対応機能, WIDE-BBに接続する下位組織でのインシデント対応状況の管理機能を主に担います

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

YAMATO-CSIRT

チームの正式名称	YAMATO Group Computer Security Incident Response Team
チームの略称	YAMATO-CSIRT
所属する組織名	ヤマトホールディングス株式会社
設立年月日	2014-06-16
チームの Email アドレス	yamato-csirt@kuronekoyamato.co.jp
チームサイト	
所属組織サイト	http://www.yamato-hd.co.jp/
加盟年月	2014 年 08 月

1. 概要

YAMATO-CSIRT は、国内のヤマトグループを横断した CSIRT です。
宅急便やメール便に代表されるヤマトグループの情報システムに対して、より巧妙化するサイバー攻撃へのセキュリティ対策を高度化していくために結成されました。
外部との情報連携による情報収集力の強化、収集した情報の内部活用による事故前提の対策強化を目的に活動しています。

2. 設立の経緯・背景

ヤマトグループでは、これまではサイバー攻撃による被害を受けないための「防御」をする技術的対策に比重を置いてきました。しかしながら、昨今のサイバー攻撃の高度化から、システム面の対策のみでは対応が難しく、事故前提での対策の強化が必要であると考えました。
そこで、ヤマトグループを横断した CSIRT を立ち上げ、外部協力組織やグループ各社の CSIRT 担当者と情報連携することで、単独では解決が困難な事態に対して、迅速かつ最適な対応を実施するための体制を整えることにしました。

3. 会社内における位置づけおよび活動内容

YAMATO-CSIRT は、国内のヤマトグループ各社の IT 責任者によって構成された、バーチャルな組織です。以前よりグループセキュリティを強化する活動を推進していた、持株会社であるヤマトホールディングスとヤマト運輸、ヤマトシステム開発の 3 社が本部となって活動しています。

＜具体的な活動内容＞
・外部との情報連携窓口
外部との情報連携を強化することにより、想定外のインシデントに対しても柔軟な対応をすることができます。

・情報セキュリティ事故発生時の解決提案 (インシデント対応)
情報セキュリティ事故が発生した際に必要な、「グループを横断した情報連携」や「意思決定機関に対する対応策実施のための情報提供」をすることで、インシデントを迅速に解決し被害を最小限にとどめることができます。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

YJ-CSIRT

チームの正式名称	Yahoo Japan Corp. Computer Security Incident Response Team
チームの略称	YJ-CSIRT
所属する組織名	ヤフー株式会社
設立年月日	2006-12-01
チームの Email アドレス	yj-csirt@mail.yahoo.co.jp
チームサイト	
所属組織サイト	https://www.yahoo.co.jp/
加盟年月	2008 年 07 月

1. 概要

Yahoo Japan Corp. CSIRT(略称:YJ-CSIRT)は、インターネット広告事業やイーコマース事業などを展開するヤフー株式会社の CSIRT です。

2. 設立の経緯・背景

社内CSIRT設立以前にも CSIRTに類する機能はあったものの、属人化された対応が散見される、社外組織と情報連携窓口が一元化できていないなどの不備がありました。
この不備を解消し、迅速かつ効率的にセキュリティインシデント (以降、インシデント) に対応する為、体制ならびにルールを整備して、YJ-CSIRTの前身となるYIRDが正式な社内CSIRTとして2006年に設立されました。
また、2017年7月1日に名称をYIRDから、Yahoo Japan Corp. CSIRT (略称:YJ-CSIRT)に変更しました。

3. 会社内における位置づけおよび活動内容

YJ-CSIRT は CISO 室を中心に広報や法務などの関連部署から選抜されたメンバーにて構成される仮想組織で、中心となる活動は以下の 3 つの活動となります。

■インシデント対応支援
ヤフーおよび関連会社が提供するサービス (以降、ヤフーサービス)にてインシデントが発生した場合、被害状況や影響範囲の分析を行い、サービス管轄部門に復旧対応をエスカレーションする。
管轄部門が復旧対応を行う際には、技術的なアドバイスや関連部門、社外関連組織との調整などの後方支援を行う。
社内CSIRT設立以前と比較して、インシデントの発覚から収束までの期間を短縮され、被害の拡大防止に効果を発揮。

■予防と啓蒙
最新のセキュリティ動向及び脆弱性情報を収集して、ヤフーサービスへの影響を分析する。
影響が認められる場合は予防策を策定して、サービス管轄部門に予防策の実施を指示する。
また、セキュリティに関する教育や情報発信にも注力し、サービス開発に際して安心・安全なサービスの提供を第一とする意識の啓蒙に務める。

■社外関連組織との協調
ヤフーサービスにて発見されたインシデントに関する報告を受ける為の窓口機関として機能する。
また、日本シーサート協議会加盟各組織をはじめとする社外組織と定期的にセキュリティに関する情報の連携や共有を行い、日本のインターネットサービスのセキュリティ向上に貢献する。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

YKK-CSIRT

チームの正式名称	YKK CSIRT
チームの略称	YKK-CSIRT
所属する組織名	YKK株式会社
設立年月日	2017-04-01
チームの Email アドレス	csirt-ykk-japan@ykk.co.jp
チームサイト	
所属組織サイト	http://www.ykk.co.jp/
加盟年月	2017 年 07 月

1. 概要

YKK株式会社は、ファスニング事業本部（ファスナーの製造販売）とその一貫生産を支える工機技術本部、グローバル事業経営と世界6極による地域経営を基本とするYKKグループを支える本社機能から成ります。

2. 設立の経緯・背景

これまでもサイバーセキュリティ・インシデントに対応する情報システム部門やリスクマネジメント部門の担当者は存在し“暗黙の了解”のうちに行動していましたが、昨今のさらなる情報セキュリティ・リスクの高まり・攻撃の巧妙化に対応し、万が一サイバー・セキュリティ事件・事故が発現・現実化した場合の対応をさらにレベルアップするためには、継続的な活動ができる体制を社内外に向けて明確にし、必要な人材・スキルの確認・確保・維持更新の仕組みが必要だと考え、CSIRTを設立しました。

3. 会社内における位置づけおよび活動内容

≪組織の位置づけ≫
YKK株式会社のシーサートとして、国内関連部門、関係会社にまつわるサイバーセキュリティ・インシデントの対応として以下の活動を行います。　メンバーは、グループの情報セキュリティ委員会の委員長、事務局である総務部リスクマネジメントグループと情報システム部IT基盤グループから成ります。
≪活動内容≫
脆弱に関する情報収集とグループ内への共有。　サイバーセキュリティ・インシデント発生の検知と初動対応、影響範囲の特定、原因分析、被害拡大・再発防止策の立案とグループ内への展開。　情報セキュリティ委員会への報告。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

YMC-CSIRT

チームの正式名称	Yamaha Motor Corpolation Computer Security Incident Response Team
チームの略称	YMC-CSIRT
所属する組織名	ヤマハ発動機株式会社
設立年月日	2013-11-01
チームの Email アドレス	ymc-csirt@yamaha-motor.co.jp
チームサイト	
所属組織サイト	http://global.yamaha-motor.com/
加盟年月	2014 年 05 月

1. 概要

YMC-CSIRT は、ヤマハ発動機株式会社国内・海外グループの主に Web サイト、インターネットを介して発生するセキュリティ対策や、協議会を通した情報収集、共有、連携を行う組織になります。

2. 設立の経緯・背景

ヤマハ発動機グループのお客様に安全で安心な Web サイト、システムを提供する目的で、早期警戒・情報共有等の活動を通して情報セキュリティ緊急時対応体制の強化を図るために設立に至りました。

3. 会社内における位置づけおよび活動内容

■位置づけ
ヤマハ発動機株式会社の情報システム部門であるプロセス・IT 部と情報システム子会社であるヤマハモーターソリューション株式会社の IT サービス事業部のインターネット、Web サイトインフラを管轄するメンバーが中心となり、国内外各グループ会社の IT 部門、Web マスターと連携した仮想組織です。
■活動内容
ヤマハ発動機グループにおける Web サイト (一般に公開されたシステム) について、インターネット、Web システムに関するセキュリティ情報の収集、早期警戒、共有及び、インシデント対応を行っています。

日本コンピュータセキュリティインシデント対応チーム協議会
Nippon CSIRT Association

YOMIURI-SIRT

チームの正式名称	読売新聞SIRT
チームの略称	YOMIURI-SIRT
所属する組織名	株式会社　読売新聞東京本社
設立年月日	2016年12月1日
チームの Email アドレス	y-sirt@yomiuri.com
チームサイト	
所属組織サイト	https://info.yomiuri.co.jp/group/about/data/index.html
加盟年月	2017 年 02 月

1. 概要

読売新聞社のグループ本社と東京・大阪・西部の3本社を中心とした情報セキュリティーを守る組織で、グループ関連会社のインシデントについても適宜、対応します。

2. 設立の経緯・背景

サイバー攻撃の巧妙化や個人情報流出などが大きなリスクとなる中、2016年1月、グループ本社情報管理委員会事務局内にセキュリティー事案対応チームを発足。同チームを中心に情報セキュリティーの早期対応体制を整備する過程で同年9月末、本社のニュースサイトの偽サイトの存在が明らかになり、同チームで迅速に一元対応し早期収束につなげた。その結果も受け、正式にCSIRT体制として発足しました。

3. 会社内における位置づけおよび活動内容

セキュリティー事案については、情報セキュリティー部門と広報、法務などを含めた関係部署で迅速な一元対応で早期収束を目指す一方、JPCERT/CCなどとの社外連携、インシデント発生時の影響や被害を低減させるための社内での教育や啓発、グループ関連会社への解決支援などに取り組みます。