日本コンピュー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

2014 年版

1　はじめに

関連情報誌や官公庁におけるセキュリティ対策関連文書等においても CSIRT(シーサート)という用語が記載されるようになり、多くの方々に CSIRT が知られるようになりました。CSIRT の認知度向上と共に、日本シーサート協議会への加盟組織数も、2007 年からの設立発起組織数 6 組織から 2014 年の設立 7 年目にして 59 組織(2014 年 8 月 21 日総会開催時点)となっています。

情報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 CSIRT 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 CSIRT はなく、百社百様です。

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。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きっかけになることを期待しております。

2015 年 3 月 6 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 の位置付けが調査項目となっています。

- 調査時期：2014 年 8 月～12 月
- アンケート回収数：54 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』のなかを細分化しますと、セキュリティベンダ系、Web サイト運営などのオンラインサービス系の 2 業種に分けることができます。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。

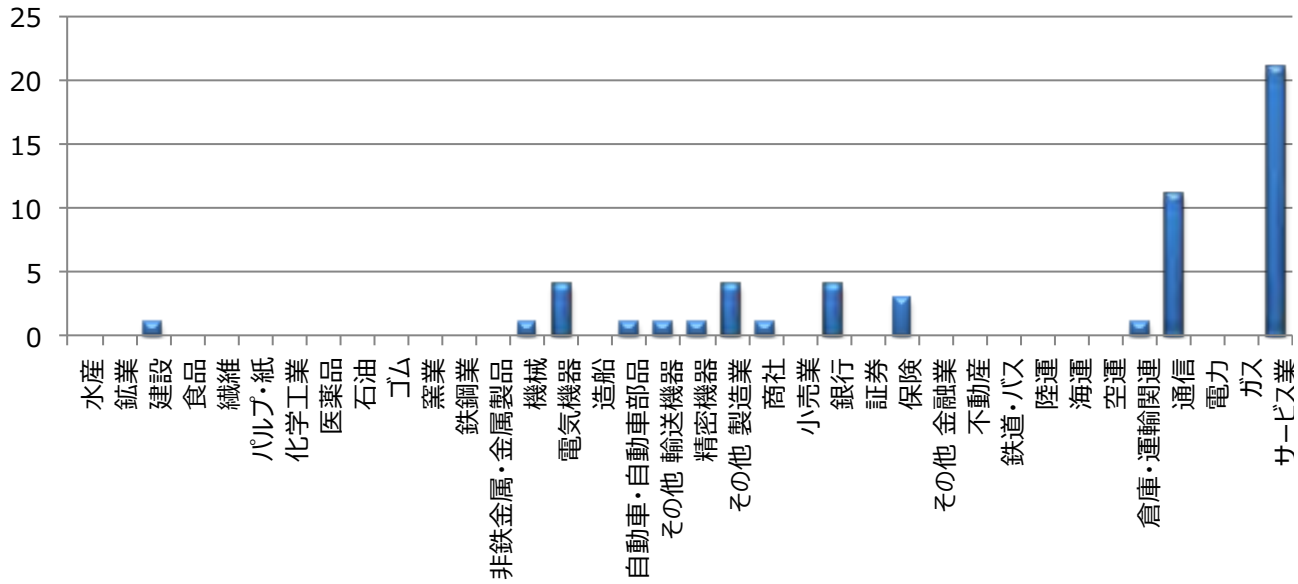

図 1：加盟組織の業種

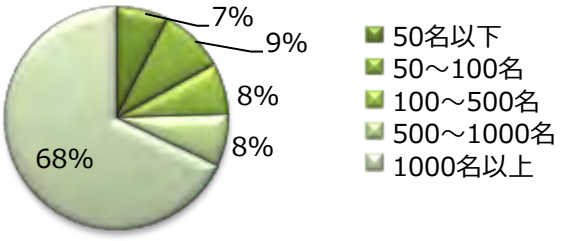

図 2：母体組織の規模

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

2.2　加盟組織の体制

加盟組織の多くは、『情報システム管理部門系』が取り纏め部署となっています。『その他』の中には、セキュリティ専門部門、商品・サービス開発提供部門、品質保証部門などが含まれています(図 3)。チーム人数は、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と言えます(図 4)。

また、加盟組織の CSIRT 実装の多くは、専任の CSIRT 要員を抱えた部署を核とした部署横断型です(図 5、図 6)。このことから、CSIRT 組織の実装を通して、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を読み取ることができます。

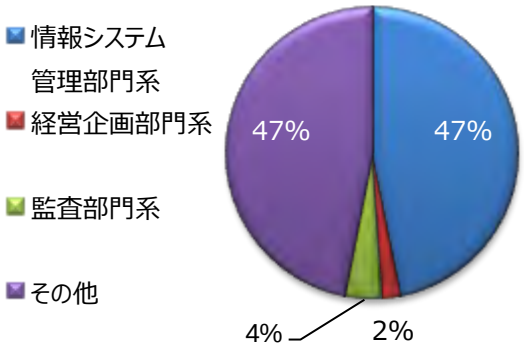

図 3：取り纏め部署

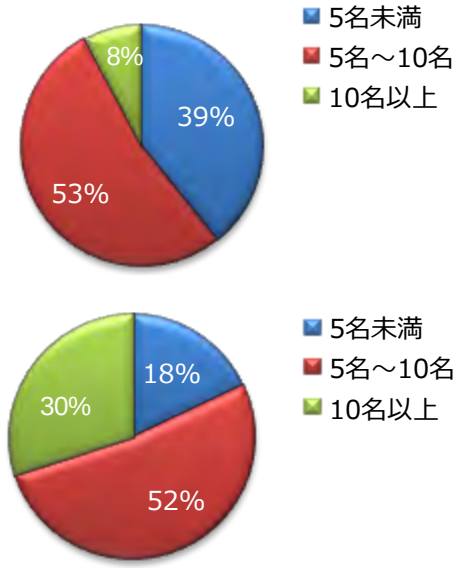

図 4：チームの人数
(上：設立時、下：活動開始後)

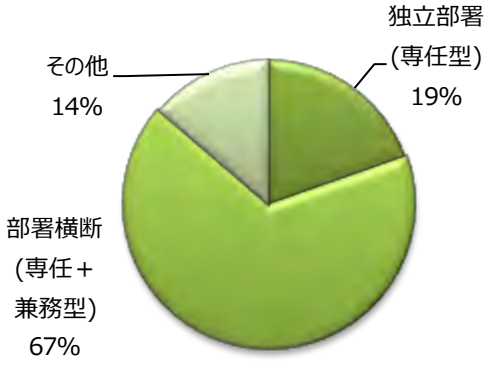

図 5：実装の形態

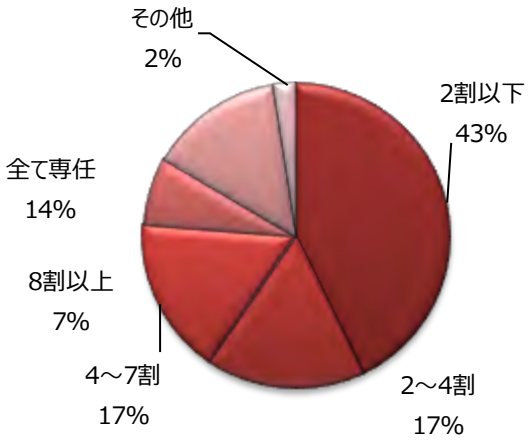

図 6：専任の割合

2.3　加盟組織のサービス

加盟組織が想定するサービスの対象者を示したのが図 7 で、7 割近くが、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。

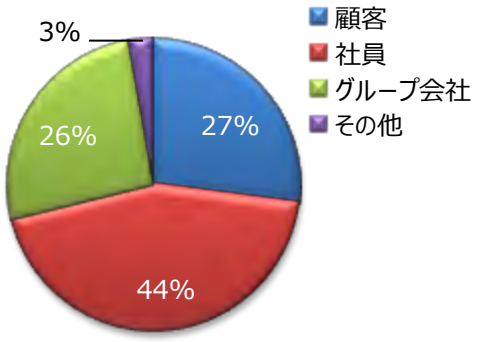

図 7：対象とする利用者

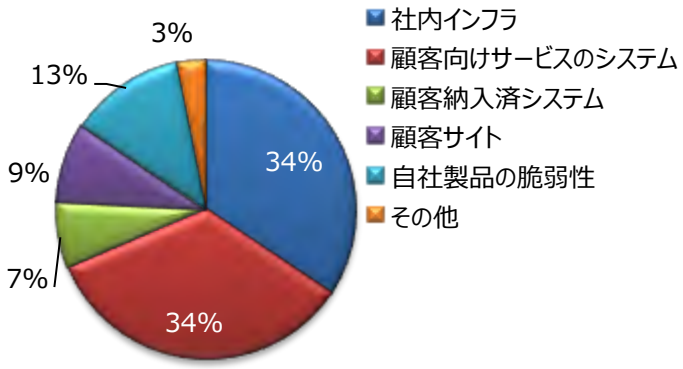

図 8：対象とする分野

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』という側面だけではなく、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)の側面が見えてきました。

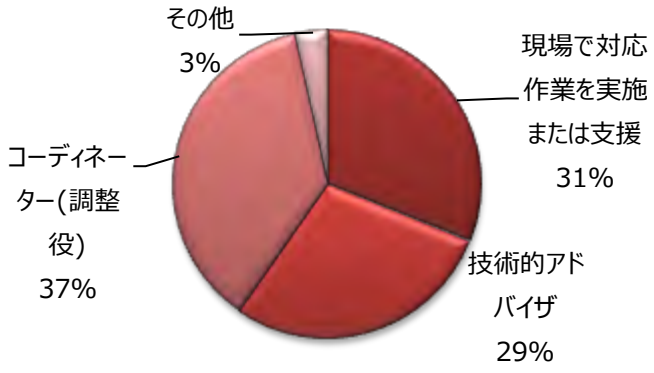

図 9：インシデント対応時の CSIRT の位置付け

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、2014 年 12 月末で 69 組織となります。加盟数の推移を図 10 に示します。

図 11 は、加盟組織の設立年の分布です。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、体制の整備が進められています。

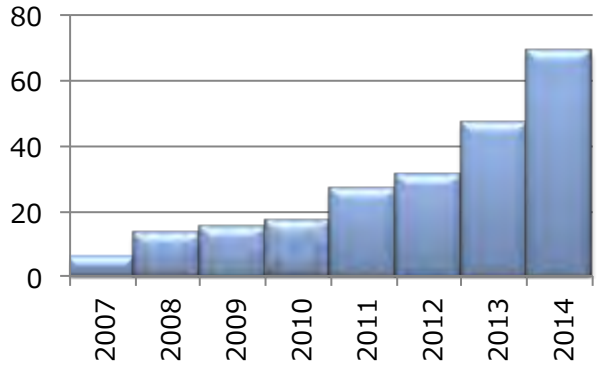

図 10：加盟数の推移

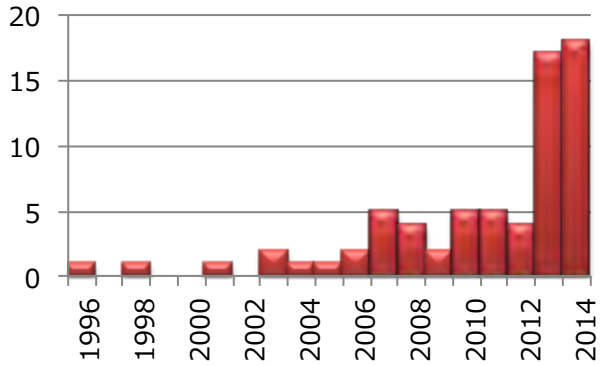

図 11：設立年の分布

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 2014 年 12 月末までの計 69 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.

CSIRT
日本シーサート協議会

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

会員一覧 – Member summary

会員（チーム）情報

AhnLab CIRT

チームの正式名称	AhnLab Computer Incident Response Team
チームの略称	AhnLab CIRT
所属する組織名	株式会社アンラボ
設立年月日	2009-07-07
チームの Email アドレス	cirt@ahnlab.co.jp
Web サイト	http://www.ahnlab.co.jp/

1. 概要

AhnLab CIRT は、マネージドセキュリティサービスを中心に、インシデント対応・支援、教育やコンサルティングなど、多角度的にセキュリティ脅威に対応。

2. 設立の経緯・背景

当社は 1995 年、韓国でウイルス対策ソフト開発会社として設立。2002 年、日本法人設立。セキュリティ脅威からより強固に顧客を守る為、当社のウイルス解析技術とノウハウを元に、AhnLab CIRT を設立。

3. 会社内における位置づけおよび活動内容

日本国内にある SOC にて 24 時間監視体制を実施するとともに、韓国本社での SOC 24 時間体制、ウイルス解析を行う ASEC (AhnLab Security Emergency Response Center) が悪性コード分析・緊急対応を実施し、通常の監視体制から緊急時の診断・分析まで、ワンストップで迅速かつ効果的な対応を行う体制を有する。

主には、セキュリティマネージドサービスを提供、ライブフォレンジックなど、顧客の求めるセキュリティ対策にフィットしたサービス内容を提供、緊急時の早期診断・分析が主な活動。自社内 SOC (Private SOC) 構築やネットワーク・セキュリティコンサルティング、セキュリティ教育など、総合的なセキュリティ対策支援を行う。

4. 当社ならではの強み

ウイルス対策ソフトウェアのベンダーとして出発し、マルウェア解析～セキュリティマネージドサービスを行っている為、ワンストップで顧客の様々なセキュリティ脅威に対して迅速に対応が可能。また、インターネット先進国の韓国だからこそ分かる、最新のセキュリティインシデントに対する情報、研究、対策、ノウハウをいち早く日本国内の顧客により良いサービスとして提供できる点が、大きな強みである。

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.aratana.jp/security/

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 :宮崎県宮崎市錦町 1-10 宮崎グリーンスフィア壱番館 5 階
代表取締役 :濵渦伸次
事業内容 :ネットショップ制作 他

サイトマップ ｜ プライバシーポリシー

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.cirt.jp

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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	productsecurity@cybozu.co.jp
Web サイト	https://www.cybozu.com/jp/features/management/cysirt.html

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。

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

この他、セキュリティインシデントの発生を予防するための活動として、定期的に弊社サービスに対する脆弱性検証を実施しています。

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

会員一覧 – Member summary

会員（チーム）情報

DeNA CERT

チームの正式名称	DeNA CERT
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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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	第一生命保険株式会社
設立年月日	2013-08-09
チームの Email アドレス	
Web サイト	http://www.dai-ichi-life.co.jp/

CSIRT
日本シーサート協議会

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

会員一覧 – Member summary

会員（チーム）情報

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	株式会社 DMM.com ラボ
設立年月日	2014-10-08
チームの Email アドレス	csirt@dmm.com
Web サイト	http://www.dmm.com/

1. 概要

株式会社 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、通信販売、レンタル、電子書籍、オンラインゲーム、英会話、3D プリント、Fx / CFD、ソーラーパネル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

PCIDSS 準拠後に個人情報保護の観点から自社サービスに対する脆弱性診断、開発ガイドラインの策定、社内教育、各種セキュリティに関する相談窓口などを行っております。

3. 会社内における位置づけおよび活動内容

＜会社内における位置づけ＞

・DMM.CSIRT は株式会社 DMM.com ラボ システム本部 セキュリティチームを中心に構成されています。

＜活動内容＞

・脆弱性情報共有と対応の進捗管理、自社サービスに対する脆弱性診断、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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.daihatsu.co.jp/

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

会員一覧 – Member summary

会員（チーム）情報

DT-CIRT

チームの正式名称	Deloitte Tohmatsu Computer Incident Response Team
チームの略称	DT-CIRT
所属する組織名	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
設立年月日	2013-04-10
チームの Email アドレス	cirt@tohmatsu.co.jp
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

FFRI

チームの正式名称	Fourteen Forty Research 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
Web サイト	http://www.ffri.jp/

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

会員一覧 – Member summary

会員（チーム）情報

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	
Web サイト	http://jp.fujitsu.com/solutions/cloud/concept/cloud-cert/

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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	
Web サイト	

1. 概要

富士ゼロックス株式会社は、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パートナーとして、お客様の経営課題の解決に貢献するためのソリューションおよび商品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および商品に関する情報セキュリティ上のリスクを極小化するための社内向け支援窓口機能を有し、社内関連部門、関連会社と協力して情報セキュリティ上の侵害事故の検知、解決、被害極小化、及び発生の予防を行うと共に、外部 CSIRT と連携して情報ネットワーク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

お客様の経営課題を解決するために当社が提供するソリューションと商品は、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、これらのサービス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、予防・検知・迅速な事後対応を図るための専門チームとして Fuji Xerox 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

Fuji Xerox CERT は、R&D 部門における横断活動として位置づけられ、社内の関連部門や関連会社との連携を図りながら、以下のような活動を進めています。

予防

- 初動エスカレーション体制の整備
- 早期警戒情報の入手と展開・アラート
- 脆弱性検査の支援と検査スキル開発
- 模擬訓練 (初動エスカレーション訓練、標的型攻撃訓練)
- セキュア設計開発支援/リスクアセス

検知

- 侵入検知環境の整備

迅速な事後対応

- 初動対応支援 (証拠保全等)
- 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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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

会員一覧 - Member summary

会員（チーム）情報

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
Web サイト	http://www.gmo.jp/

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.gree.co.jp/

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.hitachi.com/hirt/

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、製品 / サービスセキュリティ委員会活動の技術支援、IT 戦略本部 / 情報システム事業部 / 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

会員一覧 – Member summary

会員（チーム）情報

IBM-CSIRT

チームの正式名称	IBM Computer 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	
Web サイト	http://www.ibm.com/ibm/jp/security/

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。

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・事故対応を実施する。

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。

CSIRT
日本シーサート協議会

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.idnet.co.jp

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」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 / 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

・社内システム

等

＜活動内容の拡大＞

・セキュリティコンサルティング

・セキュリティ情報の提供

・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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	https://sect.iij.ad.jp/

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.intellilink.co.jp/

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セキュリティソリューション BU セキュリティアーキテクチャグループ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

会員一覧 – Member summary

会員（チーム）情報

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	
Web サイト	

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

会員一覧 - Member summary

会員（チーム）情報

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	
Web サイト	http://www.intec.co.jp

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.japannetbank.co.jp/

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)

CSIRT
日本シーサート協議会

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

会員一覧 - Member summary

会員（チーム）情報

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
Web サイト	http://www.jp-bank.japanpost.jp/

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

会員一覧 – Member summary

会員（チーム）情報

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	office@jpcert.or.jp
Web サイト	https://www.jpcert.or.jp/

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

会員一覧 - Member summary

会員（チーム）情報

JSOC

チームの正式名称	Japan Security Operation Center
チームの略称	JSOC
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	jsoc-irt@lac.co.jp
Web サイト	http://www.lac.co.jp/

1. 概要

株式会社ラックのセキュリティ監視センター JSOC におけるインシデント対応チームは、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。

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、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、JSOC 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。

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 JSOC 内で発生したインシデントの対応支援や JSOC 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 JSOC 顧客の支援に限らず、緊急対応窓口に相談のあったセキュリティインシデント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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.kddi.com/business

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

会員一覧 – Member summary

会員（チーム）情報

KEK CSIRT

チームの正式名称	KEK Computer Security Incident Response Team
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
Web サイト	http://www.kek.jp/

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.keyware.co.jp/keywareservice/

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

会員一覧 – Member summary

会員（チーム）情報

KKCSIRT

チームの正式名称	Kakaku.com Security Incident Response Team
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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.kaspersky.co.jp/

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

1. 概要

   LINE-CSIRT はコミュニケーションアプリサービスの LINE をはじめネット上のまとめサービス等が中心の NAVER、ブログやポータル・ニュース事業等を行う livedoor をサービスに持つ 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

   CSIRT 機能のルーツはオンラインゲームが事業の中心だった旧社名 NHN Japan の時に数々のインシデントへの対応を行なっていた 2005 年にまで遡ります。
   インシデント発生の都度、関係部門が集い、セキュリティ管理組織が旗振りととりまとめを行いながらその対処をしていたことから実質上 CSIRT 機能は存在していました。
   LINE サービスがグローバルに展開されていく中、CSIRT と正式に冠を付け内外に対応機能の存在をアピールすることで適切なインシデント体制の更なる充実を図ることから LINE-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

LINE-CSIRT は全社のセキュリティ管理を行う情報セキュリティ組織と同じく全社の技術的なセキュリティ対応を行う IT セキュリティ組織とで構成されています。
両組織はそれぞれを掌握する執行役員の元で機能しており、インシデントの発生内容に応じ協業をして対処しています。
対処における意思決定は再発防止策の立案含め事業部門やサービスの技術部門、広報組織、法務組織も交えた形で各責任者が一同に介し行われ、その経緯および結果は掌握する執行役員により代表取締役に報告されます。
再発防止策の実行またはインシデント発生予防のための投資予算は年度始めに両組織により提案され、財務組織の承認を得た上で予算化されます。

発生するインシデントは様々ですが、外部攻撃に関しては擬似メールの全社送付により開封率を測定する等してトレーニングを繰り返しています。また、ハード面では侵入検知を早期に把握出来るべく監視や装置の設置を以って対処出来るようにしています。
またサービス上は脆弱性等のインシデントの元に成り得るものを最初から除去すべく、ローンチ前に IT セキュリティ組織の専門人員による詳細なチェックが行われています。

グローバルな展開と利用するユーザー数の増加に伴い、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

会員一覧 – Member summary

会員（チーム）情報

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@mbsd.jp
Web サイト	http://www.mbsd.jp/

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

会員一覧 – Member summary

会員（チーム）情報

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	ncaMet-CIRT@metlife.co.jp
Web サイト	http://www.metlife.co.jp/

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

会員一覧 – Member summary

会員（チーム）情報

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	
Web サイト	

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

会員一覧 - Member summary

会員（チーム）情報

mixirt

チームの正式名称	mixi 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
Web サイト	

1. 概要

株式会社ミクシィは、ソーシャル・ネットワーキング サービス (SNS) mixi をはじめ、「すべての人に心地良いつながりを」をミッションとして、新たなチャレンジを続けている会社です。
当社において、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 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、常設の組織ではなく、事故が発生した際にセキュリティ部門を中心に各部門を横断したメンバーで編成されます。

通常は、セキュリティ部門が、社内教育を通じて、事故報告窓口の周知や、規程の整備を行っています。
mixirt 宛に事故報告が届き、その事故の重大度が高いと判断された場合に、セキュリティ部門が中心となり、すみやかに mixirt の体制が整えられます。

全ての事故は、対応履歴を残し、その記録を社員に公開しています。
こうして蓄積されたノウハウは、再発防止へと役立てられています。

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

会員一覧 – Member summary

会員（チーム）情報

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	株式会社みずほファイ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	
Web サイト	http://www.mizuho-fg.co.jp

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

(1) チーム構成

IT・システム企画部に設置したサイバーセキュリティチームを事務局として活動。

【役割】

- 標的型攻撃等、高度化していくサイバー攻撃に対する対策の企画 / 推進
- 侵害発生時のシステム / サービス所管部署と協働した攻撃分析・攻撃元サイト停止等の被害軽減対応
- 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確保、最先端の情報収集、及びグループ内への情報発信

(2) 活動内容

主な活動は以下の通りです。

- インターネットバンキングへの攻撃対応：フィッシング、Banking Trojan
- イントラ標的型攻撃への対応
- 9 月 18 日攻撃への対応：Web システム全体の脆弱性対応

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

会員一覧 – Member summary

会員（チーム）情報

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 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
Web サイト	http://www.ms-ad-hd.com/

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

会員一覧 - Member summary

会員（チーム）情報

MUFG-CERT

チームの正式名称	Mitsubishi UFJ Financial Group - 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	MUFG_CERT@hd.mufg.jp
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.nri-secure.co.jp

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。

CSIRT
日本シーサート協議会

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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	Security_info@nissay-it.co.jp
Web サイト	

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

これまで実施していた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いました。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て、社内体制を整備・強化して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

会員一覧 – Member summary

会員（チーム）情報

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@ml.east.ntt.co.jp
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.ntt-cert.org/

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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「品質保証部 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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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.com
Web サイト	

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

会員一覧 - Member summary

会員（チーム）情報

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	プライスウォーターハウスクーパース株式会社 あらた監査法人
設立年月日	2014-08-01
チームの Email アドレス	pwc.jp.csirt@jp.pwc.com
Web サイト	http://www.pwc.com/jp/ja/advisory/index.jhtml

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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 (http://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：System Security 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「System Security 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「System Security 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

会員一覧 – Member summary

会員（チーム）情報

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	
Web サイト	

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

会員一覧 - Member summary

会員(チーム)情報

R-tech Cyber Incident Team

チームの正式名称	リクルートテクノロジーズ サイバーインシデントレスポンスチーム
チームの略称	R-tech Cyber Incident Team
所属する組織名	株式会社リクルートテクノロジーズ
設立年月日	2013-08-01
チームの Email アドレス	
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

SBCSIRT

チームの正式名称	Softbank Telecommunications Security Incident Response Team
チームの略称	SBCSIRT
所属する組織名	ソフトバンク BB 株式会社 ソフトバンクテレコム 株式会社 ソフトバンクモバイル 株式会社 ワイモバイル株式会社 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
Web サイト	

1. 概要

SBCSIRT (SoftBank teleCommunications Security Incident Response Team) は、ソフトバンク BB 株式会社、ソフトバンクテレコム株式会社、ソフトバンクモバイル株式会社、ワイモバイル株式会社、Wireless City Planning 株式会社の 5 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

SBCSIRT の前身である 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、ソフトバンクテレコム株式会社、ソフトバンクモバイル株式会社の 3 社で構成される CSIRT になりました。その際、名称を現在の SBCSIRT に変更しました。

2012 年 10 月には株式会社ウィルコム (現ワイモバイル株式会社)、2013 年 4 月には Wireless City Planning 株式会社も加わり、現在では 5 社の CSIRT となっています。

3. 会社内における位置づけおよび活動内容

SBCSIRT はセキュリティー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。

SBCSIRT 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。

- セキュリティー関連情報 (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
- セキュリティールールの見直し

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 SBCSIRT 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ーチェックなどは SBCSIRT の活動には含まれず、別のセキュリティー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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.scsk.jp/sp/sys/

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。

2. 設立の経緯・背景

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 構築支援を提供しているグローバルセキュリティソリューション部のメンバーで構成。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フォレンジック、SOC の構築支援、SCSK CSIRT メンバー常駐による内部犯行対策等を実施。

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

会員一覧 - Member summary

会員（チーム）情報

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-antimalware-unit@securebrain.co.jp
Web サイト	http://www.securebrain.co.jp/about/security.html

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

会員一覧 - Member summary

会員（チーム）情報

SMFG-CSIRT

チームの正式名称	Sumitomo Mitsui Financial Group - CSIRT
チームの略称	SMFG-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
Web サイト	

1. 概要

三井住友フィナンシャルグループは、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、証券業務などのさまざま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IT企画部のシステムリスク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・グループ内連携
- SMFG 各社・SMBC 内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

会員一覧 - Member summary

会員（チーム）情報

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	スターティア株式会社
設立年月日	2014-10-01
チームの Email アドレス	startia-csirt@startia.co.jp
Web サイト	http://www.startia.co.jp/

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情報システム委員会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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	http://www.toyota.co.jp

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

会員一覧 – Member summary

会員（チーム）情報

TMNS-CSIRT

チームの正式名称	Tokio Marine & Nichido Systems Computer Security Incident Response Team
チームの略称	TMNS-CSIRT
所属する組織名	東京海上日動システムズ株式会社
設立年月日	2013-06-01
チームの Email アドレス	tmns-csirt@grp.tmnf.jp
Web サイト	

1. 概要

TMNS-CSIRT は、東京海上日動システムズ株式会社 によって運営されている CSIRT です。

東京海上日動システムズは、東京海上日動火災保険株式会社の IT グループ会社として、「技術に心を乗せて世界中にお届けします」という企業コンセプトのもと、業務分析からビジネスプロセスの構築、幅広いソリューションの提案によって最適なシステムをつくり上げ、安定稼働させることをミッションとしています。

2. 設立の経緯・背景

近年の大規模な情報流出事件等を契機に、当社が東京海上日動火災保険株式会社に提供する情報システムをサイバー攻撃から守ることを目的に専任者を設置してセキュリティ対策の強化を図ってきましたが、組織的な対策の必要性を感じ、CSIRT チームを設立しました。しかしながら自社のみでは年々高度化・巧妙化するサイバー攻撃に対応するには限界があり、他社や外部組織との連携強化を目的に、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

TMNS-CSIRT は、IT 管理部門内の専任メンバーと、実際にシステムを構築・運用する兼任メンバーで構成する仮想的なチームです。

主な活動内容は次の通りです。

(1) 情報収集及び影響分析
コンピュータ・セキュリティ・インシデントや脆弱性に関連した情報の収集と当社における影響の分析及びトリアージ

(2) インシデント対応
コンピュータ・セキュリティ・インシデント検知から影響の極小化、解決のための活動

(3) セキュリティ強化対策の推進
コンピュータ・セキュリティ・インシデント発生に備えたソリューション導入および態勢構築、プロセスの確立

(4) 外部団体との連絡窓口
日本シーサート協議会等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

会員一覧 – Member summary

会員（チーム）情報

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.co.jp
Web サイト	http://www.trendmicro.co.jp/jp/about-us/csr/security-action/#tm-sirt

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＞

ー 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。

ー 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。

ー 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。

ー 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＞

ー 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

ー 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

ー 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

会員一覧 – Member summary

会員（チーム）情報

TOPPAN-CERT

チームの正式名称	TOPPAN-CERT
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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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。

   ダウエ業株 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

会員一覧 – Member summary

会員（チーム）情報

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
Web サイト	

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

会員一覧 – Member summary

会員（チーム）情報

YIRD

チームの正式名称	Yahoo Incident Response Division
チームの略称	YIRD
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	yird-contact@mail.yahoo.co.jp
Web サイト	http://www.yahoo.co.jp/

1. 概要

YIRD (Yahoo Incident Response Division) 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

YIRD 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、正式な社内 CISRT 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

YIRD は CSO 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。YIRD 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

会員一覧 - Member summary

会員（チーム）情報

YMC-CSIRT

チームの正式名称	Yamaha Motor Corporation 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
Web サイト	http://global.yamaha-motor.com

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。