CSIRTスタータキット

Ver 3.0

一般社団法人 日本シーサート協議会
2025年10月9日

連絡先:https://www.nca.gr.jp/contact/index.html

本文書の取り扱いは **TLP:CLEAR** でお願いします。TLPについては次を参照してください。

FIRST: TLP Standards Definitions and Usage Guidance - Version 2.0
https://www.first.org/tlp/docs/v2/tlp-v2_ja.pdf（日本語版）

もくじ

はじめに **3**
CSIRTの概要 **4**
昨今の CSIRT 4
CSIRT小史 4
インシデントとは 4
インシデントに関連する言葉 5
CSIRTとは 6
CSIRTのメリット 6
CSIRT構築のポイント **8**
まずは始めましょう 8
経営層の理解 8
CSIRTはセキュリティインシデント対応の統括機能 8
セキュリティインシデント対応の検討から始めることを推奨 8
インシデントはそれぞれの組織で違う 9
CSIRTの型 9
CSIRT構築のためのステップ **12**
CSIRT構築フェーズ 13
CSIRT運用フェーズ 14
STEP 0　CSIRT構築プロジェクトの立ち上げ 14
STEP 1　情報収集と現状把握・問題把握 17
STEP 2　CSIRT 企画立案 23
STEP 3　CSIRT構築 33
STEP 4　CSIRT運用 37
STEP 5　CSIRT再検討 39
最後に：**SIM3** **41**
改訂履歴 42

はじめに

本文書であるCSIRTスタータキットは、V1.0を2007年、V2.0を2011年に公開しました。CSIRT の構築に関する文書でわかりやすいものが少ないとの思いもあり、日本シーサート協議会の有志で作成しました。これまでの間にも、ベトナム語や英語、インドネシア語などへの翻訳も作成され、その必要性は必ずしも日本だけではないということが分かってきました。現状でも十分に参考になる文書と自負していますが、V2.0の公開から10年以上がたち、今の状況に合わせて更新が必要だと感じました。

本V3.0は最近の状況を取り込み、より読みやすくなるように書き直しました。CSIRTを構築するのは簡単ではありません。また、その後の運用も決して楽ではないでしょう。何かさらに支援できないかと考え、特に最新の情報と、CSIRT の運用で苦労してきた筆者たちの CSIRT のノウハウを込める必要があると考えました。

本文書はこれから CSIRT を構築する、始める方向けに記載しています。IT系の企業だけではなくユーザ系の CSIRT の方でも理解できるように心がけ、必要に応じて用語の説明を行っています。また、コラムなども挿入することにより、理解を助けるようにしました。ただし、セキュリティの基本レベル、例えば CIA がなんであるかなどの単語は知っていることを前提としています。

構築やこれから開始する方向けのガイドではありますが、運用に悩んでいる方が基本的な考え方や概念を確認する際の参考になると考えています。

本文書が皆様のCSIRT 活動の発展に少しでも寄与できればと思います。

CSIRTの概要

昨今のCSIRT

CSIRT を取り巻く状況は大きく変化しています。世界的なセキュリティチームのコミュニティである FIRST でも、600以上のチームが加盟しています。その加盟チームはアフリカなども含む四大陸からとなっています。世界的に見ても CSIRT は注目されています。また、アフリカやアジアの方々とお話をすると、企業のCSIRT 構築の必要性がよく聞かれます。

日本シーサート協議会は2007年に開始しましたが、そのときには6チームでした。以前は任意団体として活動していましたが、2020年より社団法人となりました。現在は500以上の加盟組織からなり、世界的に見てもここまで企業の CSIRT が連携するコミュニティは存在しません。しかしながら、多くのチームは立ち上げたあとも CSIRT 自体の運用で悩まれていることも多いようです。

CSIRT を構築するための資料は引き続きニーズが高いと思われます。

CSIRT 小史

CSIRT はいつから始まったのでしょう。1988年CERT/CCの設立からと言えるのではないかと思います。 まだ、歴史というほどの年月はたっていません。しかしながら、その小史とも言える歴史をたどることはCSIRTの構築・運用においても参考になると思います。そこで、以下のリンクよりCSIRT小史としてまとめました。

CSIRT小史: https://www.nca.gr.jp/activity/pub_doc/csirt.html

インシデントとは

ここからは代表的な用語を解説していきます。まずはインシデント（incident）です。
CSIRT（Computer Security Incident Response Team）とはその略語からわかるように、コンピュータに関わるセキュリティ上のインシデントを扱う組織です。最近であれば、コンピュータに関わるというよりもサイバーセキュリティと言った方がわかりやすいかもしれません。

まず、ここではCSIRT の世界で使用されているインシデントという言葉について解説します。
ISO22300（JIS22300）「社会セキュリティ—用語」では、インシデントは次のように定

義されています。
''「中断・阻害，損失，緊急事態又は危機になり得る又はそれらを引き起こし得る状況」''
「なり得るまたは引き起こし得る状況」と記載のとおり、可能性まで含めて発生したものです。CSIRT はコンピュータ、もしくはサイバーセキュリティに特化したインシデントを扱う組織と言ってよいでしょう。

インシデントに関連する言葉

インシデントの他にも CSIRT が活動するにあたって様々な用語が使われます。
以下に CSIRT の視点で整理してみます。

インシデント

組織における出来事のうち、事件・事故、もしくはそれらになり得るものも含みます。

- 重大インシデント
組織に重大な影響を及ぼすインシデント、BCM や危機管理の領域で扱うべきものです（CSIRT によってはこれらも主体で動く組織もあります）。

イベント

本来のイベントという言葉からはずれてしまいますが CSIRT の世界では、組織に関係する出来事のことです。Firewall からの警告や SOCなどからの通知などがあり得ます。この中にはインシデントとまでは言えないものも含まれます。

インテリジェンス

様々な情報を分析し、知見として共有する情報です。場合によってはインシデントとなる場合もあります。

CSIRT について「コンピュータ、もしくはサイバーに関わるセキュリティに特化したインシデントを扱う」と述べましたが、情報システムは瞬く間に社会に浸透しました。また、IoT（Internet of Things）も普及しつつあります。このような中、対応するインシデントの対象を広げている CSIRT もあります。
「インシデント」という曖昧な言葉をきちんと定義することは、CSIRT にとって重要です。情報システムは社会に浸透し、組織にとっても必須の存在になっていますが、まだ十分に理解されていないのが現状です。また、お金や人手などのリソースを

CSIRT に手厚く投入できる組織は限られています。このような理由から、CSIRT を立ち上げると、セキュリティばかりでなく、情報システムに関わる諸事への対応が求められることがしばしばあります。つまり、CSIRT が「なんでも屋」にならざるを得ないのです。そのような CSIRT では、本来の活動が滞ってしまう恐れがあります。そうならないためにも、自分たちの CSIRT が扱うインシデントを定義することはとても重要です。

CSIRT とは

インシデントへの対応を行う組織が CSIRT です。日本シーサート協議会（以下、NCA）では、CSIRT を次のように定義しています。
「CSIRT とは、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の組織の総称です。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をします。」
この定義にあるように、CSIRT は情報漏えいなどの大きな事故などを含めて、インシデントにも対応する組織です。

CSIRTのメリット

CSIRT として活動するメリットは何でしょうか。

毎回同じようなインシデントに悩んでいませんか

「先月総務部で起こった類似のインシデントが企画部でも起こってしまった。」
「企画部は大変だったらしい。せめて SI 部と連携できていれば……。」
↓
「先月のインシデントをみんなに共有しよう。」（事前予防）
「万一インシデントが発生しても、前の経験を活かせるから早期解決だ。」（被害低減）

あなただけの力で十分ですか（外部との連携）

「A国で同じような事例が3か月も前にあったのか……。もし知っていれば手が打てたかもしれない。」
「私の会社は、解析は得意だが、情報収集は苦手だな……。」
↓
「NCA で脅威情報をもらった。私たちも警戒しよう。」（他山の石）
「他の会社ではこんなふうに情報収集を強化しているのか。参考にしよう。」（事例共有）

「私たちの解析結果を外に共有して役立ててもらおう。」（補完）

*CSIRT*は、企業内の「セキュリティインシデント消防署」

CSIRT はセキュリティインシデントの窓口となり、情報が集まり、経験が蓄積します。ノウハウを活かしその経験から消防署員として振る舞えます。いざというときに集まるのであれば、消防団に例えることもできるでしょう。

*CSIRT*は体外的な名刺になる

CSIRT と名乗ることで他のCSIRTとの情報交換や協力を可能にします。この関係は、あなたの企業のセキュリティに寄与する可能性があります。
CSIRT にはコミュニティがいくつかあります。
日本シーサート協議会（国内 CSIRT コミュニティ）
FIRST（CSIRT の国際的コミュニティ）

以下の文書も参考になります。
『What's CSIRT ?』

CSIRT 構築のポイント

まずは始めましょう

本文書はCSIRT 構築をステップごとに解説しています。しかしながらそのステップにきっちりと従って作る必要はありません。自組織の事情に合わせて構築してください。また、各ステップの検討段階で先に進むことが難しくなるかもしれません。そのときは課題として残し、まずは CSIRT を始めることを優先しましょう。
既にある巨大企業の CSIRT も最初は小さなものでした。まずは、スモールスタートで始めることが重要です。

経営層の理解

サイバーセキュリティは組織の経営課題として対応すべきです。経済産業省ではサイバーセキュリティ経営ガイドラインを作成しています。この中でも CSIRT の機能を構築し、セキュリティインシデントが発生したときに対応してくださいと記載されています。このことからも CSIRT の活動は経営層からの指示で実施すべきです。CSIRT を始めることの重要性およびその活動の支援を得るようにしてください。

参考）
『経済産業省「サイバーセキュリティ経営ガイドライン」』

CSIRT はセキュリティインシデント対応の統括機能

CSIRT はセキュリティインシデント対応組織ではあるものの、その範囲はセキュリティ対応全体に及びます。CSIRT が組織におけるセキュリティ対応の統括機能を果たせるように活動してください。

セキュリティインシデント対応の検討から始めることを推奨

まずはセキュリティインシデント対応の検討から始めることを推奨します。そうすることにより他の機能の必要性が見えてくることがあります。

インシデントはそれぞれの組織で違う

本文書でも「インシデントとは」と解説していますが、組織ごとに対応が変わります。自分たちの CSIRT が扱うインシデントは何かということを決めてください。

CSIRT の型

本文書ではこの後、構築方法、チームの体制、位置づけなどが出てきます。それらはみなさんが作ろうとする CSIRT の型を決める上で参考になると思います。自身の CSIRT をどのような型で作るかは、組織の全体の体制や要員、予算など様々な課題があり、理想の形で作ることは難しいでしょう。どんな型で作るにせよ重要なポイントを以下に上げます。

*1*つのチームとして

1つのチームとして動けるように、信頼を確立してください。

経営層を含めた各部署からの信頼を得てください

最初から信頼を得るのは無理かもしれません。各所の課題や問題に耳を傾けたり、セキュリティの勉強会などを提供したりして、徐々に信頼の輪を広げるよう尽力してください。

チームが組織の中で自由に動き回れるようにしましょう

各組織には体制があり、命令系統があるでしょう。組織のラインを使った連絡手段は当然必要ですが、部署に関わらず、組織内を自由に動き回れるようにすることが重要です。

多くの組織では部署があり、それぞれの利益を追求しています。また、部署間の確執などもあり、縦割りになっているところも多いでしょう。そのためには、各部署にはセキュリティに詳しいキーパーソンがいるかもしれません。それらのキーパーソンを見つけ、その人たちとの連携を確立してください。

コラム：チャタムハウスルール

チャタムハウスルールとは、イギリスのシンクタンクであるチャタムハウス（王立国際問題研究所）で 採用されたことに由来して名づけられたルールです。

参加者は会議中に得た情報を自由に使用できますが、その発言者や所属を特定したり、他の参加者を特定したりする情報は伏せなければなりません。このルールを適用することで、活発な CSIRT 間の情報共有、連携を通した事例などの情報活用が可能となります。

コラム：**TLP**

TLP（トラフィックライトプロトコル）は、機密情報を確実に、適切な組織または人に共有するために使われる、一連の標示です。

情報の受信者に求められる情報共有の境界を示すために、情報の発信者が4つの色を用いて標示します。

TLP の指定より広い範囲にその情報を共有する必要がある場合は、情報の受信者は発信者の明示的な許可を得なければなりません。

以下に FIRST のTLPv2.0の概要を記します。

TLP:RED = 公開不可、関係者限定

情報が初めて公開された会議・会話に含まれない、いかなる第三者とも共有してはならない。

TLP:AMBER = 限定公開、関係者が所属する組織内で共有可能

情報を関係者が所属する組織の構成員、および自組織を保護したりさらなる被害を防止したりするために情報を必要とするクライアントや顧客のみに共有できる。情報の発信者は、対象とする公開範囲の制限を自由に指定でき、この公開範囲は遵守されなくてはならない。

TLP:AMBER+STRICT

組織内のみに共有が制限される。

TLP:GREEN = 限定公開、コミュニティ内で共有可能

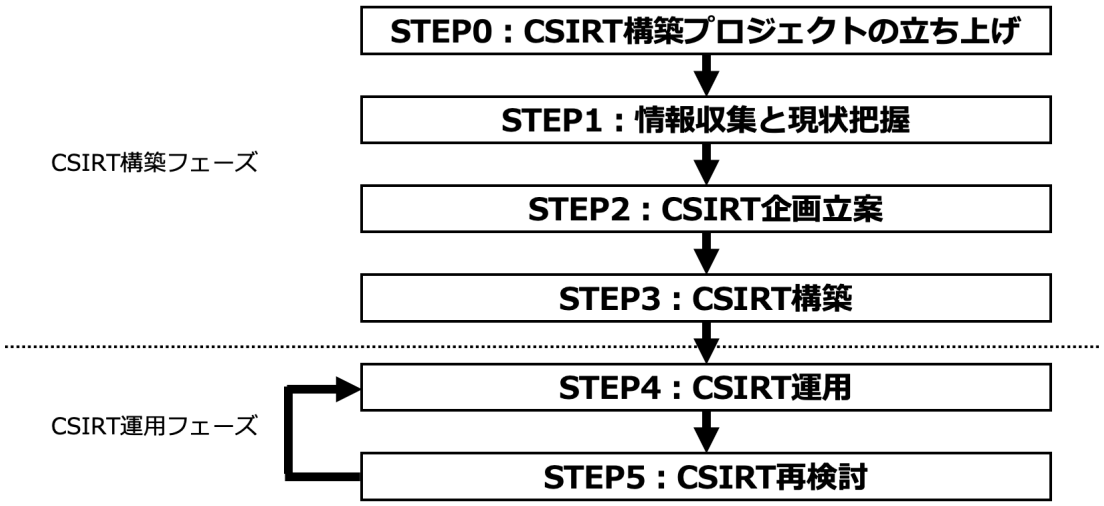
自組織の構成員およびコミュニティやセクター内のパートナー組織に共有してもよいが、誰もがアクセス可能な手段を介してはならない。

TLP:CLEAR = 制限なく共有可能

標準的な著作権保護の規定にのっとり、制限なく配布可能。

CSIRT 構築のためのステップ

ここでは、CSIRT 構築のためのステップについて解説します。
CSIRT にはセキュリティインシデントへの対策という共通の目的があったとしても CSIRT は百社百様であり、一つとして同じ CSIRT は存在しません。それは、自組織の組織形態やセキュリティポリシー、スタッフの専門知識や予算などの組織固有の環境に依存しているためです。このことは、「同業他社の CSIRT を参考にしながら CSIRT を構築すればよい」ということが難しいことを意味します。自組織において最適な CSIRT を検討しなければなりません。
自組織において最適な CSIRT を検討する際には、ベースとなる考え方を踏襲することが効率的です。基本的なステップ（図1）を以下に示します。



(図1)

各ステップについて詳細は本書にて解説を行うものとして、以下に概要を記載します。
本書で記載するステップはSTEP0～ STEP5で構成されます。また、このステップはSTEP0～ STEP3までのCSIRT 構築フェーズと、STEP4～ STEP5までのCSIRT 運用フェーズに大別されます。

CSIRT 構築フェーズ

CSIRT 構築フェーズとは CSIRT がない状態から CSIRT の検討を始めるフェーズです。

STEP 0: CSIRT 構築プロジェクトの立ち上げ

CSIRT の構築を始めるにあたっては、CSIRT を構築し運用開始するまでをゴールとしたプロジェクトを立ち上げて、集中的に検討することが効率的です。ここでは、プロジェクトメンバーの選定やプロジェクト運営方法の決定、スケジュールの検討などを実施します。

STEP 1: 情報収集と現状把握

自組織がセキュリティインシデントにおいてどのような対応ができているかを正確に把握するために情報収集を行います。その後、収集した情報を分析し、自組織の強み、弱み、機会、脅威などを明確化します。これにより、現状（AS-IS）を把握し、CSIRT 構築後（TO-BE）のブループリントを描くことが可能となります。

STEP 2: CSIRT企画立案

STEP 1で描かれたブループリントを具体化するために、現状分析を元にCSIRT 企画立案を実施します。ミッションの定義、サービスの定義、コンスティチュエンシーの定義や、セキュリティインシデント対応フローの作成および、アウトソーシングの検討を行います。また、中長期計画もこのステップで立案します。

STEP 3: CSIRT構築

STEP 2で検討した CSIRT の企画を組織に実装します。CSIRT 記述書を作成し、CSIRT の具体的内容のドキュメント化を行います。CSIRT 記述書をステークホルダから承認を得ることにより、組織内の正式な組織として発足させます。CSIRT運用のために、予算、リソースの準備を行います。また組織内の関連する部門との調整や、CSIRT 活動を実施するための具体的な手順書などの準備を行います。

CSIRT 運用フェーズ

CSIRT 運用フェーズとは CSIRT を立ち上げ、運用を行うフェーズです。CSIRT 運用開始時に実施することや、中期的な活動計画の立案と実行などが含まれます。既に運用開始している CSIRT にとっては、STEP 4 ～ 5を検討することによって、手順の整備・改善や課題の解決が図れます。

なお、「運用」としていますが、セキュリティインシデント対応の内容などといった、CSIRT の運用そのものに関してはここでは記載しません。

STEP 4: CSIRT 運用

CSIRT 運用開始時や運用中に実施することがあります。CSIRT 運用開始の組織内周知や社外連携体制の確立などを運用開始時に実施します。また、CSIRT 活動をアピールするために、レポートの作成が重要です。

STEP 5: CSIRT 再検討

CSIRT を運用していくにあたって、CSIRT 構築フェーズでは見えていなかった課題がでてきます。また、CSIRT 活動の中長期計画をたてる必要があります。CSIRT の再検討においては、短期的なCSIRT 再検討と中長期的なCSIRT 再検討が重要です。

STEP 0　CSIRT 構築プロジェクトの立ち上げ

STEP 0 では、CSIRT を構築する活動を実践するための「CSIRT 構築プロジェクト」を立ち上げます。プロジェクトの円滑な進行のために考慮すべき点を以下に示します。

目標

CSIRT 構築のきっかけを明確に示します。
- 「外部のステークホルダーとのコミュニケーションを推進するため」など

プロジェクト構成メンバー

プロジェクトの構成メンバーを定義します。

- コアメンバー（セキュリティインシデントに関連するメンバーで構成します
- ステークホルダ（利害関係を明確にします）
- 関連する部門（必要に応じて専門知識や意見を取り入れられる体制を確立します）

スケジューリング

時間的制約事項を確認します。

- CSIRT 構築プロジェクトのWBS（マイルストーンを明確にします）など

プロジェクト運営

プロジェクトの運営ルールを明確化します。

- 物理的に離れているメンバーのコミュニケーション手段を確保します
- プロジェクト内の意思決定フローを確認します
- その他の制約事項を確認します

セキュリティインシデント対応に関連する部門は多岐に渡り、ミッションやモチベーションが異なる複数の部門を巻き込んでいく必要性があります。プロジェクト立ち上げの段階で、コアメンバーで上記の考慮すべき点について議論してリスクを事前に洗い出し、対策することが効果的です。

CSIRT 構築プロジェクトの立ち上げ期に活用できる資料を以下に示します。

『CSIRT構築に悩まれている担当者の皆様へ』

これから CSIRT を立ち上げる方に向けて適切な CSIRT の構築を支援する目的で参考資料がまとめられています。

『What’s CSIRT ？ ～CSIRTのススメ～』

CSIRT の必要性を1枚のスライドにまとめた文書です。

『サイバーセキュリティ経営ガイドライン Ver2.0 付録F サイバーセキュリティ体制構築・人材確保の手引き（経済産業省）』

企業経営の観点から、自社に最適な体制や資源確保に関する適切な判断を行うためのポイントについて解説されています。

『構築活動のためのプロジェクト憲章（JPCERT/CC）』
構築活動を開始するにあたって、構築活動全体の定義について明記する文書です。

『CSIRT構築活動のためのスコープ記述書（JPCERT/CC）』
構築活動を進めるにあたって必要なマイルストーン、見積もり、制限などを記述する文書です。

関連する部門の例

関連する部門の例を以下に示します。CSIRT 構築プロジェクトにおけるアウトプットの報告会などを通して、関連する部門の CSIRT に関する理解を深め、フィードバックを受けながらプロジェクトを進めていくことが肝要です。

経営者・意思決定層

CSIRT 構築の承認によるリソースの確保や、CSIRT に必要な責務と権限の関係を社内体制に反映する責任を持ちます。また、セキュリティインシデントの最終報告先を担います。

情報システムの主幹・運用部門

CSIRT活動に深く関連します。セキュリティインシデント対応機能を持つ場合もあります。

内部統制部門

セキュリティインシデント対応と内部統制活動との連携を担います。（CSIRT 活動は内部統制的な活動ではなく、あくまでもセキュリティインシデント対応にあることを念頭に置いてください。）

法務部門

セキュリティインシデント対応における法的対応を担います。

広報部門

セキュリティインシデント対応における広報対応を担います。

人事部門

CSIRT スタッフの配置・雇用を主管します。また、セキュリティインシデント発生元の人事的処置を実施します。（CSIRT 活動は人事的処置のためではなく、あくまでもセキュリティインシデント対応にあることを念頭に置いてください。）

人材開発部門

セキュリティのノウハウ、ポリシー、セミナー、ワークショップ、教材などを通してサービス対象に教育や啓発活動を行います。

経営企画部門

事業継続計画および、災害復旧計画とセキュリティインシデント対応の連係を担います。

ヘルプデスク部門

セキュリティインシデントへの対応時の一次窓口を担います。

物理セキュリティ部門

物品（特にPC）の盗難対策や、入退室制限の管理を担います。

STEP 1　情報収集と現状把握・問題把握

STEP 0でCSIRT 構築プロジェクトの立ち上げが完了したら、そのプロジェクトで CSIRT 構築に向けて具体的な活動を始めます。STEP 1では、CSIRT 構築前の段階における現状を把握し、問題を洗い出します（AS-IS）。更に、そこからどのような CSIRT とするかの検討（TO-BE）を行います。

1. 情報収集

ほとんどの組織において、様々なセキュリティ対策に関連する既存の情報があると思われます。プロジェクトで、既存の自組織の正確な現状を把握するために、まずは CSIRT 構築に関連すると思われる情報を収集していくことが必要です。収集する情報の一覧を以下に示します。これらの文書は既存であるものを収集する必要があり

ますが、CSIRT 構築のために新規に作成する必要性までは想定していません。
また、これらの情報は全てそろわなければならないというわけではありません。「情報がない」ということも一つの情報です。下記以外でもCSIRT 構築にあたって有用な情報があれば、積極的に情報収集を行うことを推奨します。

既存セキュリティポリシー群

既存のセキュリティポリシー群を把握します。既存のセキュリティ関連の基本的な遵守事項や制約事項などが記載されていますので、CSIRT 構築の際の基本的な情報となります。CSIRT も既存のセキュリティポリシー群に記載されている内容に準拠できるように設計していくことが求められます。

IT に限定しないセキュリティ関連文書

IT に限定しないセキュリティ関連文書がある場合、その内容を把握しておく必要があります。CSIRT 構築には直接的には関係しない場合もありますが、参考となる情報が含まれている場合があります。例えば、IT に関連しないセキュリティインシデントのエスカレーションフローやセキュリティインシデントに対応する組織などです。

既存のインシデントの重大度を判定するための基準

CSIRT はセキュリティインシデント対応において、トリアージを実施します。セキュリティインシデントのトリアージ基準をCSIRT 構築時に検討することが必要です。トリアージ基準の検討の参考資料として、既存のインシデントの重要度を判定するための基準を収集しておく必要があります。

CIA 基準

CIA とは情報セキュリティの3要素であり、「機密性」（Confidentiality）、「完全性」（Integrity）、「可用性」（Availability）の頭文字から略されています。組織に CIA 基準があれば、把握しておく必要があります。トリアージ基準作成のために利用できる可能性があります。

個人情報保護に関する文書

個人情報保護に関する文書は、個人情報漏えいが発生した場合に必要な対応が記載されています。CSIRT が個人情報漏えいを伴うセキュリティインシデント対応の実施事項や連携する社内外の組織に関しての記述がされています。

BCP 関連文書

BCP とは災害などの緊急事態における組織の事業継続計画（Business Continuity Planning）のことです。セキュリティインシデントにおいて事業継続が困難になる場合において、BCP にのっとって CSIRT が活動することが想定されます。CSIRT 構築にあたっては、BCP を考慮して組織を設計したり、BCP 発動の基準とトリアージ基準との整合性を取ったりする必要があります。

リスクアセスメント結果

リスクアセスメントの結果はCSIRT 構築の必要性の論拠として説得力があります。セキュリティインシデントへの対応能力の低さがリスクアセスメントによって示唆されているならば、そのリスクへの対応としてのCSIRT 構築が求められてきます。

セキュリティ関連の認証情報

ISMS やプライバシーマークなどのセキュリティ関連の認証情報に関して、情報収集しておく必要があります。CSIRT の組織設計や制約事項の参考になる可能性があります。

*IT*資産リスト/情報資産リスト

組織の持っているIT資産や情報資産を把握する必要があります。セキュリティインシデント対応やトリアージ実施に参考になる情報です。

セキュリティインシデント検知ツール/対応ツール

既存でどのようなセキュリティインシデント検知ツール/対応ツールがあるかを把握しておく必要があります。またセキュリティインシデント検知にあたっては、その検知ツールやログの運用状況や運用体制も合わせて把握しておく必要があります。

システム運用体制

既存システムの運用体制を把握しておく必要があります。セキュリティインシデント対応において、システム運用体制とCSIRT との連携は非常に重要です。セキュリティインシデント対応プロセス検討時のインプットとしても重要な情報です。

ログ管理状況の把握

既存のログ運用がどのようにされているかを把握する必要があります。セキュリティインシデント対応においてログは非常に重要な要素であり、誰がどのようなポリシーでどのように運用しているかを正確に把握しておく必要があります。

既存のシステムの脆弱性対応プロセス

脆弱性対応はセキュリティ対策として重要なプロセスです。現在、どのような脆弱性対応を行っているかを CSIRT は把握しておく必要があります。また、CSIRT が脆弱性対応を実施する場合には、既存の脆弱性対応プロセスを把握したうえで、CSIRT のサービスの設計をする必要があります。

既存のセキュリティインシデント対応フロー

既存でセキュリティインシデント対応フローがある場合には、CSIRT構築にあたっての重要なインプットです。既存のセキュリティインシデント対応フローを、組織的で効果的なフローとしてアップデートしていくことが求められます。

既存のインシデントレポートフォーマット

既存のインシデントレポートフォーマットは、CSIRT がセキュリティインシデント対応を行うにあたっての重要な参考情報です。インシデントレポートフォーマットによって、「誰が」「誰に対して」「いつ」「どのような」レポートを行うかを把握できます。また、CSIRT 構築によって、このレポートフォーマットをアップデートする必要性があるかもしれません。

セキュリティインシデント対応に関連する組織内外の組織の洗い出し

セキュリティインシデント対応は CSIRT だけで完結するものではなく、組織内外の組織との連携が不可欠です。組織内外の連携を洗い出す必要があります。代表的な例として、組織内としては、情報セキュリティ委員会、法務部門、総務部門、広報部門、IT部門、内部統制部門、人事部門などがあげられます。組織外の部門としては、監督官庁、法執行機関、マスコミ、セキュリティベンダ、ITベンダ、他組織の CSIRT などがあります。

監督官庁からの指示文書

セキュリティインシデントにおける監督官庁からの指示文書があれば、把握しなければなりません。CSIRT のセキュリティインシデント対応における必須要件として盛り込む必要があります。

2. 現状分析・問題把握

収集した情報を元に、現状分析・問題把握を開始します。収集した情報から、自組織で何ができていて、何ができていないかを明確にしていく必要があります。さらに、CSIRT 構築後は課題点をどう改善できるようになるかを説明可能な状況にすることが求められます。
以下の観点で情報を分析することが効率的です。これらの分析により、現状(AS-IS)を正確に把握し、CSIRT 構築後（TO-BE）の将来の計画を立てられます。STEP 1での分析結果が「STEP 2：CSIRT 企画立案」のインプットとなり得ます。

現状のセキュリティインシデント対応における各組織の役割

既存の組織がセキュリティインシデント発生時に何を実施する事となっているかを確認します。また、セキュリティインシデント対応において、ボトルネックとなるような組織間連携がどこかを洗い出します。既存の組織間連携を（ボトルネックとなる箇所も含めて）組織間連携図としてまとめることが望まれます。CSIRT 構築後は、各組織が何を行う必要があり、CSIRT との連携はどうすべきかを検討する材料となります。

既存の権限

セキュリティインシデント対応において、ビジネスを止める意思決定ができる権限は誰が持っているか（もしくは誰も持っていないか）を確認します。CSIRT 構築後は、その権限は誰が持つべきかを検討する材料となります。

既存のセキュリティインシデント検知システム

セキュリティインシデントを検知するシステムを明確にします。IDS/IPS、SIEM、EDR、WAF などが代表的な検知システムです。また、SOC などに一元的にアウトソーシングしている場合は、どのようなスコープでどのようなサービスを受けているかを確認します。また、検知システムの運用状況や運用者、検知通知の受取先が誰になるのかなども合わせて確認していく必要があります。CSIRT 構築後は、検知システムの運用者や検知通知の受取先をどうするかを検討する材料となります。

セキュリティインシデント対応の管理方法

セキュリティインシデントを現状でどのように管理しているかを確認します。管理表、チケットシステム、セキュリティインシデント報告フォーマット、報告基準などを明確にします。CSIRT 構築後はどのような管理とすべきかを検討する材料となります。

既存のセキュリティインシデント発生時のトリアージ基準

セキュリティインシデント発生時のトリアージ基準や、関連する基準を確認します。CIA、BCP 発動時の基準など、関連する基準を整理し、CSIRT が用いるトリアージ基準を作成するための基本情報として取りまとめます。

監督官庁からの指示文書への対応状況

セキュリティインシデント発生時の監督官庁への報告の指示文書があれば、それが何かを明確にしておく必要があります。また、報告元が誰となっているかを確認します。

過去のセキュリティインシデント分析

過去に発生したセキュリティインシデントを分析し、セキュリティインシデント対応において良かった点と悪かった点を洗い出します。良かった点は再現性があるかを確認し、悪かった点はなぜ悪かったのかを確認します。CSIRT 構築後は、良かった点を組織的に再現性があるように組み込み、悪かった点に関しては CSIRT にて解決できるようにするためにはどうしたらよいかを検討します。

ユースケースにおけるセキュリティインシデント対応のシミュレーション

セキュリティインシデントのユースケースを想定し、現在セキュリティインシデントが発生したら、どのようになるかを確認します。セキュリティインシデント対応の現状の課題点を洗い出します。

*SWOT*分析

SWOT分析とは、自組織の外部環境と内部環境を Strength（強み）、Weakness（弱み）、Opportunity（機会）、Threat（脅威）の4つの要素で要因分析することで、戦略を策定するためのフレームワークです。セキュリティインシデント対応におけるSWOT分析を実施します。セキュリティインシデント対応における現状分析・問題把握を明確にし、CSIRT 構築にあたっての戦略を練られます。

コラム：トリアージ

トリアージ（Triage）という言葉は、一般的には医学で用いられている用語です。限られたリソースの中で、できるだけ多くの人々の命を救うため、優先的に緊急度の高い患者に対応するという意味で用いられています。セキュリティインシデント対応におけるトリアージとは、セキュリティイベントがインシデントか否かの判断と、セキュリティイ

ンシデントの優先順位付けを実施することです。
トリアージは、その基準を作成し CSIRT として常に同じ基準で実施しなければなりません。ただし、コンピュータセキュリティを取り巻く環境はめまぐるしく進歩しており、基準となる要素は常に変化するので定期的な見直しを行っていくべきです。

STEP 2　CSIRT 企画立案

STEP 2では、CSIRT の企画立案を行い、どのような CSIRT を構築するかの骨子を確定させます。STEP 1で現状の課題の洗い出しや、CSIRT の方向性を検討した内容をインプットとしてSTEP 2の検討を進めていきます。
検討する項目を以下に示します。

CSIRT の定義

CSIRT 名の定義

CSIRT の名称を決定します。自組織の CSIRT であることを明確に示す名称をつけることを推奨します。CSIRT の国際的な連携を行う必要が出てくる場合があるため、多くの CSIRT がアルファベットで命名しています。

- 一般的な名称例:「自組織名」-CSIRT

ミッションの定義

「なぜ CSIRT が必要なのか」「CSIRT は何を行うのか」といった活動の軸となるミッションはとても重要です。ミッションを定め、目標や目的を明確にすることで CSIRT 活動に迷いや停滞が生じた時に立ち返ることができ、CSIRT 活動の大きな助けとなります。ミッションは CSIRT が何を目的とした組織であり、何を行うかを端的に短文で記載することが求められます。
- ミッションの例:〇〇〇-CSIRTは、セキュリティインシデントに組織的かつ迅速に対応する体制である。セキュリティインシデントによる情報漏えいなどの未然の防止と、発生した際の被害を最小化のための活動を行い、〇〇〇事業継続性を確保するとともに社会的信頼を発展させる。

行動指針・倫理規範の定義

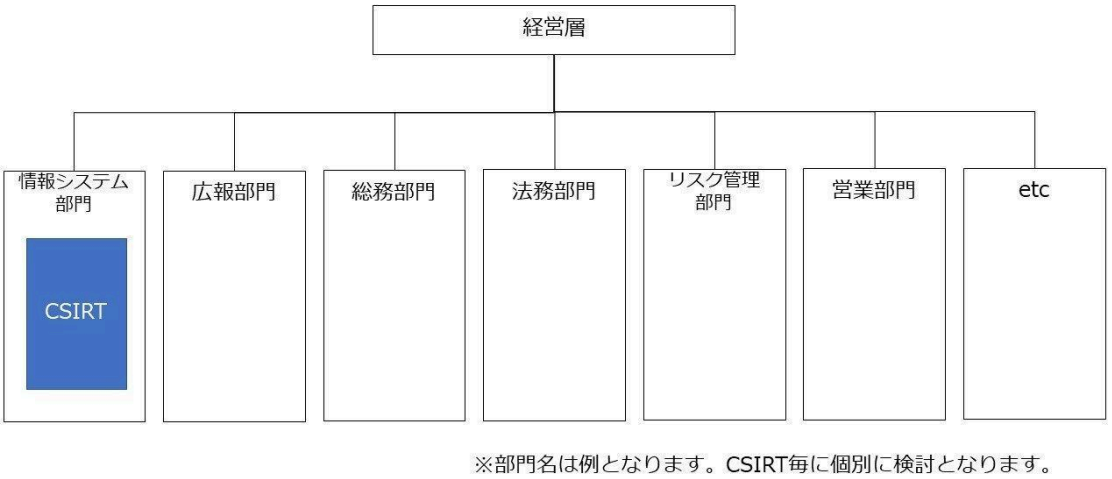
CSIRT のメンバーは、多くのシステムや機微な情報にアクセスできるため、そのメンバーの行動は責任が重いものだと認識しなければなりません。
CSIRT はメンバーへの倫理的行動を喚起し、かつガイドすることを目的とした行動指針を定義する必要があります。
マニュアル通りにはいかない不測の事態に対応しなければならないことが多い CSIRT にとって、行動指針を定めることはとても意味のあることです。FIRST が作成した『EthicsfIRST』が参考となります。

*CSIRT*体制定義

CSIRT の体制と組織内の位置づけを定義します。CSIRT 体制図を図示するとよりよいでしょう。CSIRT 体制図には、CSIRT だけでなくセキュリティインシデント対応に関連する組織内の全部門や連携する組織が記載されていることが求められます。組織内部門や他組織との連携の曖昧さを排除し、コミュニケーションパスを全て体制図内に記載することにより、より精度の高いCSIRT 体制図を描写できます。
CSIRT は二つとして同じものは存在しませんが、基本的なモデルに関して以下に示します。

モデル1　部門内モデル

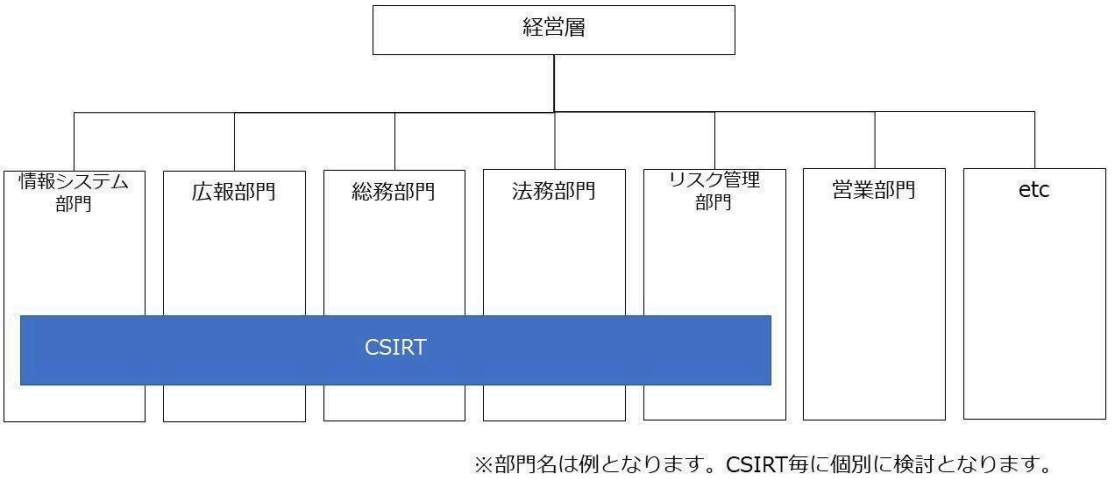
このモデルは、組織内のある特定の部門内に設置される CSIRT です。部門内のセキュリティ業務の一環として CSIRT が設置される場合が多く見られます。この CSIRT の活動内容はその部門の活動の範囲内として実施することとなります。主に、情報システム部門、総務部門、リスク管理部門内に設置されることが多いモデルです。また、セキュリティインシデント対応には、広報対応、法務対応などの他部門との協力が必要となります。



(図2)

モデル2　バーチャル組織モデル

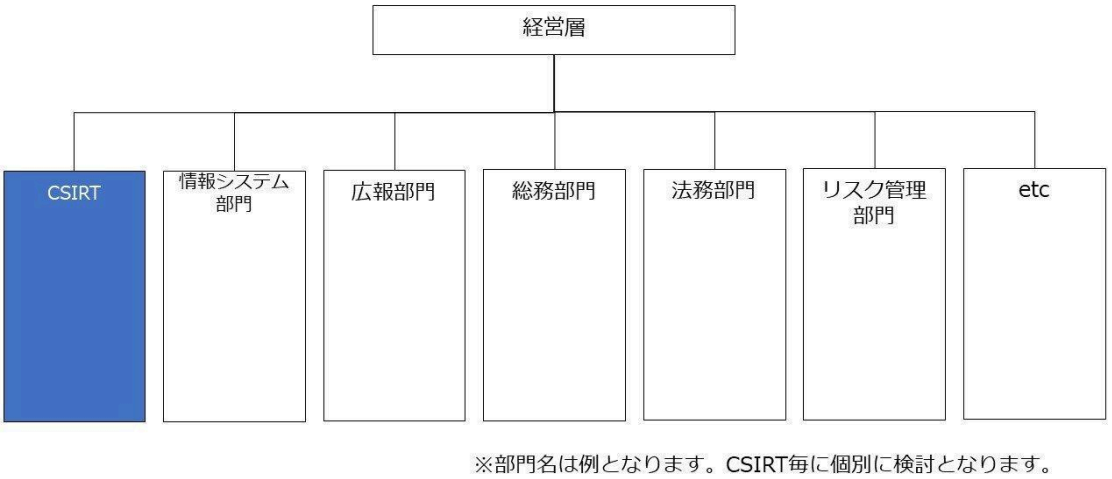
このモデルは、組織内の複数の部門から構成される CSIRT です。CSIRT の業務は多岐にわたるため、単独の部門の業務範疇だけでは収まりません。例えば、技術的な対応だけでなく、広報対応、法務対応、監督官庁対応、組織内調整など様々な対応が求められます。CSIRT がバーチャル組織として構成されることにより、様々な部門の能力を有機的に結合し、効果的なセキュリティインシデント対応を実現します。主に、情報システム部門、法務部門、総務部門、広報部門、リスク管理部門などで CSIRT が構成されることが多いモデルです。



(図3)

モデル3　独立組織モデル

このモデルは、組織内で CSIRT が独立した部門として構成されるモデルです。CSIRT が独立した部門として構成されることにより、他のモデルのように母体となる組織の能力やミッションに縛られることなく、その組織内で最適化されたサービスを提供できる CSIRT として構成することが可能です。また、経営層の意見をダイレクトに反映することも可能です。適切な権限を設定することにより、他の部門への影響力を持てます。セキュリティインシデント対応には、広報対応、法務対応などの他部門との協力が必要となります。



(図4)

CSIRT の権限の定義

CSIRT の権限に関して定義する必要があります。CSIRT は、サービスにおいて様々な権限を持つことになります。その中でも特に、ネットワーク切断やシステム停止などの、業務に多大な影響を及ぼすセキュリティインシデントの封じ込め策実施判断の権限の所在は明確に定義しておく必要があります。
具体的には、CSIRT がその権限を持つか、CSIRT の上位組織もしくは経営層がその権限を持つかの検討になります。

経営層へのエスカレーションの定義

重大システムのランサムウェア感染による事業停止や大規模な情報漏洩などのセキュリティインシデントは CSIRT の範疇を超えることもあるでしょう。そのためにも経営層へのエスカレーションパスを必ず構築しましょう。

サービスの定義

CSIRT が提供するサービスを検討する必要があります。CSIRT の「サービス」とは「業務」や「役務」ととらえて問題ありません。CSIRT のサービスを定義することにより、CSIRT が何を実施するかを明確にし、CSIRT を具体化させていきます。
CSIRT のサービスとしては FIRST（Forum of Incident Response and Security Teams）の Education Advisory Board がまとめた『FIRST CSIRT Services Framework』が参考になります。FIRST CSIRT Services Frameworkでは、「CSIRT が提供するサービスの一覧」がまとめられており、サービスポートフォリオを

選択、拡張、または改善するために使用できます。CSIRT はこのフレームワークのサービスを全て実装する必要はありません。また、このフレームワーク以外のサービスを提供しても問題ありません。CSIRT 構築の段階では、スモールスタートとして、自組織において最小限で必須のサービスから開始することが望まれます。CSIRT の運用開始後に、サービス拡大を検討していくことで、より強力な CSIRT として定義されます。

コンスティチュエンシー（*Constituency*）の定義

コンスティチュエンシーとは、CSIRT が提供するサービスのスコープに該当します。コンスティチュエンシーの定義を行うことにより、CSIRT のスコープを定義し、活動範囲を明確にします。
コンスティチュエンシーを定義するには、以下の2軸で検討することが効果的です。

- 組織的観点：どの組織に対してサービスを提供するかを検討します。例えば、「国内の組織」や「本社」などです。

- システム的観点：どのシステムに対してサービスを提供するかを検討します。例えば「OAシステム」や「オンプレミスのシステム」などです。

サービスと同様に、コンスティチュエンシーもスモールスタートすることが求められます。例えば、“「本社」の「オンプレミスのシステム」のみをCSIRT 構築当初のコンスティチュエンシーとして、「子会社」「グローバル」「クラウド」「OT」などはCSIRT 運用開始後にコンスティチュエンシーの拡張検討とする”などです。

人的リソースの検討

「CSIRT 体制の定義」「サービスの定義」「コンスティチュエンシーの定義」より、CSIRT に必要な人的リソースの確保を行います。
どのような人的リソースが必要かに関しては、『CSIRT人材の定義と確保』が参考となります。
CSIRT人材の定義と確保では CSIRT に求められる役割と実現に必要な人材のスキルがまとめられており、人的リソースの検討の参考となります。

アウトソーシング検討

CSIRT は、自組織の人的リソースなどの制約により、自組織だけではサービス提供できない場合が想定されます。そのような場合には外部専門組織へのアウトソーシングを検討する必要があります。
幸いなことに、昨今では多数のセキュリティベンダから高い品質のセキュリティサービスが提供されているので、それを活用することで高品質のサービスを自組織に提供

できることがあります。
ただし、CSIRT のサービスにおいては、アウトソーシングの向き不向きがある点に留意する必要があります。
アウトソーシングに向くサービスとしては、SOC やフォレンジックスなどのセキュリティインシデント分析、リスクアセスメント、OSINT 調査など、高い技術力や専門知識が求められ、定められたスコープにおいて高品質のアウトプットが要求されるものです。
一方、コーディネーション業務や意思決定など、自組織内でないと実施できない業務はアウトソーシングに向きません。

*CSIRT*が取り扱うインシデントの定義と分類

「はじめに」でも述べたように、自組織の CSIRT で取り扱うインシデントを定義することが肝要です。インシデントには様々な分類があります。以下、具体的なインシデントとなる事例をあげます。

不審なアクセス

ポートスキャン、何らかの不審な動向。組織の弱点を探る、侵入を試みるような動き

ウイルス感染を意図した行為

送信ヘッダを詐称した電子メールの配送From:（送信元）の詐称など

システムへの侵入

システムへの侵入・改ざん。踏み台にするための侵入。攻撃用プログラムの設置

ネットワークサービスなどの利用

管理者が意図しない、第三者によるメールサーバ、プロキシサーバなどの使用。仮想通貨の採掘（マイニング）利用

サービス運用妨害につながる攻撃

ネットワークの輻輳による妨害。サーバプログラムの停止。システムの停止・再起動

ビジネスメール詐欺（BEC（Business E-mail Compromise））

電子メールを使用し実在の組織や人物を騙り、口座にお金を振り込ませたり、特定の情報を取得したりする

その他

コンピュータウイルス感染。スパムメールの受信

トリアージ基準の定義

トリアージは、セキュリティイベント受付時にセキュリティインシデントにラベリングしたり、重大度を判断したりするために用いられます。トリアージ結果に伴って、個々のアクションを変えていく必要があります。アクションに影響を与えるものとしては、重大度、優先順位、対応体制、エスカレーション対象、様々なタイミングなどが挙げられます。重大度やラベリングのためにはトリアージ基準を作成する必要があります。

インシデントレベルの定義

インシデントレベルは、セキュリティインシデントによってもたらされる事業影響度などを鑑みてレベル付けを行う必要があります。このレベルはトリアージ時点で判明するものもあれば、インシデント対応を進めていくうえで明確化されていくものもあります。また、インシデント対応が進むによってインシデントレベルが変更されていく場合もあります。インシデントレベルの定義を検討するにあたっては、STEP 1で収集した要素を参考にして整合性を取りながら、CSIRT としての基準を作成していく必要があります。また、レベルごとに「経営層へのエスカレーションの定義」や「広報方針の定義」と組み合わせて検討していくことで、整合性のとれた意思決定方針を定義できます。
以下にインシデントレベルの定義の参考となる事例をあげます。

(表1)

文書	基準への反映
既存のインシデントの重大度を判定する基準	組織内に既存のインシデントの重大度を判定するための基準がある場合、それに準拠してセキュリティインシデントに関するトリアージ基準を作成すると、組織内で整合性のとれた判断が可能となります。
CIA基準	CIA基準はトリアージ基準に活用できる場合があります。例えば、機密性の基準

	が「A：厳秘」「B：社内秘」「C：公開情報」となっていた場合、情報漏えいに関するトリアージ基準を機密性基準に合わせて「A」「B」「C」と区分し整合性を取ることにより、組織内で整合性のとれた判断が可能となります。
個人情報保護に関する文書	個人情報漏えいは個人情報保護法やGDPR などの法令にのっとった対応を行う必要があることから、個人情報漏えいをトリアージ基準として含めておく必要があります。

セキュリティインシデント対応フローの定義

CSIRT をセキュリティインシデント対応の中核組織として位置づけ、セキュリティインシデント対応フローを定義する必要があります。またセキュリティインシデント対応フローは組織内へ周知徹底する必要があります。
セキュリティインシデント対応フローにおける実施事項を検討するにあたっては、『NIST SP800-61 コンピュータセキュリティインシデント対応ガイド』が参考になります。

ここでは、セキュリティインシデント対応として「検知」「分析」「封じ込め」「根絶」「復旧」「インシデント後の対応」としてプロセスが定義されています。このNIST SP800-61の概念、「CSIRT 体制定義」によるアクター、コミュニケーションパスの定義および、「CSIRT の権限の定義」「トリアージ基準の定義」を組み合わせることにより、セキュリティインシデント対応フローを作成できます。
ただし、実際にセキュリティインシデントが発生した際には、セキュリティインシデント対応フローに忠実に従ったアクションを行うことは難しい、ということは留意しておく必要があります。
実際のセキュリティインシデント対応においては、個々のセキュリティインシデントごとに状況が異なり、セキュリティインシデント対応フローを超越した高いレベルでの意思決定やアクションの実行、コミュニケーションが行われます。
つまり、セキュリティインシデント対応フローは、セキュリティインシデントごとの臨機応変な対応を網羅するものではなく、モデル化されたセキュリティインシデント対応の行動原則を定義したドキュメントであるということを意識して記載することが求められます。

広報方針の定義

セキュリティインシデント対応において、発生したセキュリティインシデントの広報活動は重要です。必要な情報を必要なタイミングで広報できるかどうかで、発生したセキュリティインシデントに対する世間からの印象は異なります。同様のセキュリティインシデントだったとしても、一方ではセキュリティインシデント対応を称賛され、他方では風評被害で炎上するということもあり得ます。CSIRT は広報部門と連携を行い、広報方針を定義しておく必要があります。

コラム：**CSIRT** の名称

名称検討の参考として、CSIRT に関係する名称に関して、以下に記載します。

CSIRT：

「Computer Security Incident Response Team」の略称です。

SIRT：

「Security Incident Response Team」の略称です。CSIRT から Computer を外すことによって、幅広いセキュリティインシデント対応を行うことで CSIRT との差別化を行おうとする意図を含む場合もありますが、CSIRT と明確に差異がある単語ではありません。

IRT ：

「Incident Response Team」の略称です。CSIRT からComputer Securityを外すことによって、更に広範囲でのセキュリティインシデントに対応する意図を含む場合がありますが、CSIRT と明確に差異がある単語ではありません。

CERT：

「CERT」はカーネギーメロン大学（CMU）が所有する登録商標です。インターネットに接続されたネットワークのセキュリティを向上させるというカーネギーメロン大学ソフトウェア工学研究所（SEI）のコミットメントを共有する米国内のCSIRTは、その名称に「CERT」マークを使用する認可を CMU に申請することができます。米国外の CSIRT は（米国ではなく）所在国において「CERT」を含む独自の名称を名乗ることができます。

参考）
Authorized Users of the CERT Mark

コラム：バーチャル組織モデルの苦悩

バーチャルモデルは複数の部門にまたがり、組織内連携を取りながら効率的にセキュリティインシデント対応を行うことを目指すモデルです。しかし、CSIRT にアサインされたメンバーは、もともと自部門のミッションに乗っ取って活動しているメンバーであり、その自組織の業務を優先する場合もあるため、CSIRT 活動への理解が乏しかったり、CSIRT活動へのモチベーションがなかったりする場合が多く見られます。バーチャル組織モデルをうまく機能させるためには、平時の活動における CSIRT 内連携を実施し、CSIRT 活動への理解促進と、メンバー間の密なコミュニケーションによる連携体制の構築が重要です。また、自部門の活動だけでなく、CSIRT 活動にも KPI を設定し、メンバーの評価項目とすることもモチベーションの維持に有効です。

STEP 3　CSIRT 構築

STEP 2で定義した CSIRT 企画立案を実行しCSIRT 構築を実現します。CSIRT 構築には以下の実施事項があります。

CSIRT 記述書作成

STEP 2で定義したCSIRT 企画立案の内容をCSIRT 記述書として取りまとめます。
CSIRT 記述書作成のための参考となるフォーマットとしては、『RFC 2350』の
CSIRT テンプレートに準拠した『CSIRT記述書』などがあります。
自組織のセキュリティポリシーなどのフォーマットにのっとってCSIRT 記述書（もしくは、自組織のセキュリティポリシーに準じたドキュメント名）を作成し、自組織のセキュリティポリシー群に組み込むと、より自組織の状況に応じたドキュメントとなります。

CSIRT 構築調整

CSIRT 構築にあたっての組織内調整を実施します。組織内の関係者やサービス対象への調整を実施します。CSIRT 体制定義で定義したセキュリティインシデント対応に関連する組織に関して、CSIRT に関することやセキュリティインシデント対応フローでの実施事項などの調整を実施する必要があります。

経営層/意思決定層の承認

CSIRT 記述書にまとめた内容について経営層/意思決定層の承認を取得します。
CSIRT 企画立案から構築へと進むことが可能となります。

手順書や関連文書の整備

CSIRT のサービス実現に向けた、個別の業務内容の手順書や関連文書を準備します。手順書としては、システム操作手順書など、CSIRT メンバーが同様のオペレーションを実施できるための手順書を作成する必要があります。
関連文書として、ITリソースリスト、情報収集先のリスト、連絡先一覧などがあります。

リソース調達

CSIRT 活動を実施するために必要なリソースを調達します。

(表2)

リソース	説明
人的リソース	STEP 2で検討した人的リソースの調達を行います。自組織内に検討したスキルセットを持つ人材がいるとは限らないので、外部からの人的リソースの調達を視野に入れる必要があるかもしれません。また、人材育成としてのトレーニングや CSIRT 人材としてのロールモデルの実装を行うことにより、人材の定着に繋がります。
システムリソース	CSIRT の運用やサービス実現のためのシステムリソースを調達します。代表的なシステムの例としては、インシデントチケット管理システム、セキュリティインシデント検知/防御システム、セキュリティインシデント分析システムなどがあります。CSIRT が提供するサービスに必要なシステムを検討することが重要です。

トレーニング	CSIRT のトレーニングは、組織内や CSIRT 内に関する事項を訓練する内部トレーニング、外部のセキュリティの専門知識を習得するための外部トレーニング、円滑なコミュニケーション実現のためのコミュニケーショントレーニングに大別されます。CSIRT としてトレーニングメニューを検討しておくことが必要です。

コラム：1人CSIRT

CSIRT の最小単位は「1人CSIRT」と呼ばれるようなCSIRT 業務を1人で実施するモデルです。「1人CSIRT」は本書でのCSIRT 体制定義における「モデル1 部門内モデル」の最小単位と位置付けられます。業務上セキュリティインシデント対応の必要性に駆られて、いつのまにかCSIRT 業務を実施している場合などがよくある例です。「1人CSIRT」のメリットは、スモールスタートで開始できることです。また、セキュリティインシデント対応などのCSIRT 活動においてCSIRT 内調整が不要で迅速に対応できることもメリットです。その一方で、リソースの限界により活動内容が制限されてしまいます。また、組織内でのCSIRT 活動が経営層に承認されていなかったり、活動内容が属人的で組織的に対応できなかったりする場合があります。「1人CSIRT」にてCSIRT 業務を実施している場合には、本書に乗っ取って CSIRT の再定義を行い、組織的な対応を実施できる体制とすることが求められます。

コラム：CSIRT 活動における例外規定

CSIRT 活動の中で、定義したセキュリティポリシーの例外にあたることを行う可能性があります。
- 独自の設備
- マルウェアの取り扱い
- ポートスキャン
- ハニーポットの運用
- 緊急対応

などです。前もって例外規定を定め、経営層/意思決定層からの承認を得ておくのがよいでしょう。

コラム：**TRANSITS**

日本シーサート協議会では、CSIRT 対応能力向上トレーニング TRANSITS Workshopを開催しています。

TRANSITS Workshopとは、ヨーロッパの学術ネットワークであるGÉANTが提供する教育コースで、TRANSITS-IとTRANSITS-IIの2つがあります。日本シーサート協議会ではTRANSITS-Iを日本語化して提供しています。
オペレーション、組織、技術、法律の4モジュールで構成され、講師による講義と、CSIRT に関わる課題についての議論を中心とした内容になっています。

『CSIRT 対応能力向上トレーニング「TRANSITS」の紹介』

TRANSITS Workshopは CSIRT の知識を習得することはもちろんのこと、他組織の方々とのネットワークを構築する絶好の機会となります。

STEP 4　CSIRT 運用

STEP 4では STEP 3までの構築準備を経てCSIRT 運用を開始します。

1.周知

CSIRT 運用を開始するためには、サービス対象に CSIRT の連絡先の周知徹底を行わなければなりません。社外への周知にはニュースリリースを利用することが1つの効果的な方法です。
発足当初は CSIRT が提供するサービスのケイパビリティをサービス対象に周知することも重要です。サービス対象の期待を満たさない場合には、STEP 5 CSIRT 再検討にて計画的に改善します。

2.社外連携体制の確立

STEP 2で検討した社外連携体制を確立していきます。すべてのセキュリティインシデントを1つの CSIRT のみで解決できるとは限りません。他の CSIRT との積極的なコミュニケーションを図り、事業リスク軽減のための効果的な連携方法を確立することが望まれます。日本シーサート協議会などのコミュニティに加盟することは1つの効果的な方法です。

3.サービス対象へのサービス提供

STEP 2で定義したサービスをサービス対象に提供します。活動状況について、経営層に対するレポートを行うことが重要です。

コラム：運用開始時の演習について

可能であればこの段階で、今まで発生したセキュリティインシデントや想定したセキュリティインシデントを元にシナリオを作成し、CSIRT活動の机上演習を実施するのもよいでしょう。演習を実施することで、構築した CSIRT の有用性を確認したり、社内連携体制、情報の伝達経路および、責任分解点を明確にしたりするなど課題を洗い出せます。
効果的に実施するために、セキュリティインシデント対応に関連する部門から参加者を集め、ワークショップ形式で演習を行います。ワークショップとは、一方向のセミナーとは異なり、参加者全員が主体的に作業や発表を行う、体験する場として運営されるものです。
演習の実施後は改善点を検討し、成果としてレポートを作成しましょう。また STEP 3 で作成した資料に反映しましょう。

コラム：アドバイザリについて

コンスティチュエンシーに理解をしてもらうため、アドバイザリを書きましょう。
収集した脅威情報や脆弱性情報、自組織でどのような問題が発生していてどのような対策が必要なのかを記載し、対策を実施してもらいます。
また、経営層向けにもレポートを作成し、CSIRT活動の内容や存在意義を理解してもらい、予算や人員の確保につなげるようにしていくことが重要です。

STEP 5　CSIRT 再検討

CSIRT の運用を開始すると、CSIRT の改善点などが把握出来てきます。また、新規サービス開発のニーズも生まれてきます。
改善だけでなく、セキュリティへの対応は日進月歩の技術力の変化に追随する必要もあります。適宜 CSIRT の再検討を行うことが有効です。
CSIRT の再検討は、短期的な再検討と中長期的な再検討とに分類できます。

短期的な再検討

短期的な再検討は、日々のCSIRT 運用からのフィードバックによる改善業務です。
CSIRT メンバーでできることから改善を行っていきます。具体的には、手順書のアッ

プデート、業務の自動化検討、チェックシート作成、セキュリティインシデント対応フロー改善、新規実装サービスの検討などです。CSIRT 運用からのフィードバックにおいて、大規模な改善が必要なものは中長期的な再検討項目へ移管します。

中長期的な再検討

中長期的な再検討は、CSIRT の拡大展開や成熟度向上を実現し、組織全体の一層のセキュリティ向上に貢献できる CSIRT となるためのアプローチです。 具体的な検討項目を以下に示します。

中長期計画にのっとった **CSIRT** 拡大検討

CSIRT 企画立案で作成した中長期計画にのっとった CSIRT の拡大展開を実現します。具体的には「コンスティチュエンシーの拡大」と「サービスの拡大」です。スモールスタートでの経験を活かし、CSIRT の拡大展開をしていきます。「コンスティチュエンシーの拡大」に関しては、今までスコープとしてカバーできていなかった組織やシステムに、既存の CSIRT のサービスを提供することです。「サービスの拡大」は CSIRT の新規サービスの実装です。中長期計画において検討してきたものもあれば、CSIRT を運用する中で生まれたものも含まれます。

成熟度向上

CSIRT 自身や CSIRT で提供しているサービスに関して、必要な文書化を実施し、内容の再評価を継続的に行い、より高い品質で効率的なCSIRT 運用を実現することにより、CSIRT の成熟度の向上を目指します。成熟度の向上に関しては、以下の内容で実施します。

アセスメント

CSIRT のアセスメントを実施し、評価を行います。CSIRT の弱点や改善点を洗い出し、更なる拡大展開や品質向上に向けたアクションを定義します。

演習

セキュリティインシデント対応力をつけていくためには、継続的な演習の実施が必要です。また、演習を通して気づいた点や反省点を振り返り、課題を抽出します。課題への改善活動を通じて成熟度の向上を実現します。

人的リソースの拡充

CSIRT の拡大展開を実現するためには人的リソースの拡充は必要です。CSIRT 拡大展開に伴う稼働の弾力性の向上や追加サービスに伴う、人材（スキル）の追加と、育成など、中長期的なアプローチが必要です。

最後に：SIM3

『SIM3』はヨーロッパで開発された CSIRT の成熟度評価のモデルです。
CSIRT が適切に活動し、社会や組織の変化に追随して改善するために検討・整理すべき項目が含まれています。CSIRT を開始したら、まず SIM3 で評価してみることをお勧めします。Open CSIRT Foundationは自組織で評価するためのツールを準備しています。

『SIM3 Online Tool』

本ツールを使って是非自身を評価してみてください。FIRST Baseline のプロファイルを選択するとよいでしょう。

改訂履歴

Ver 3.0 2025年9月30日 Ver3用に全面書き直し
Ver 2.0 2011年8月1日 NCA版作成
Ver1.0 2007年2月5日 新規作成