CSIRT スタータキット

Ver 2.0

日本コンピュータセキュリティインシデント対応チーム協議会

目　次

文書更新履歴

版	日付	内容
2.0	2011 年 8 月 1 日	NCA 版作成
1.0	2007 年 2 月 5 日	新規作成

1　はじめに

本書は、日本において CSIRT を構築する際に注意し取り組むべき課題や定義すべき事項について説明している文書である。また、組織におけるインシデントレスポンスの計画を構築する際に取るべき手順についても言及し、CSIRT を構築する上での一般的なガイドとしても役に立つように記述されている。

CSIRT はその目的や組織の背景により、一つとして同じモデルは存在し得ない。結果として、まったく同じ方法で運用されるチームは存在しない。そのため組織にとって、なぜ CSIRT を作るのか、CSIRT が達成すべき事項は何かを判断した上で、CSIRT が最も効果的な役割を担うように構成される必要がある。本書は、日本で CSIRT の構築に関わるすべての人々が、各々の組織で適切に検討する際の材料として利用されることを目的としている。

本書が想定している読者は、日本国内で、コンピュータセキュリティインシデントの再発防止・被害局限化を目的とした組織的な対策の実施における、実施責任者及び担当者である。本書がセキュリティ向上に向けて効果的に利用されることを期待する。

2　コンピュータセキュリティインシデントの対応と CSIRT

昨今の情報化の目覚ましい進展に伴い、情報システムの果たす役割はますます重要になり、かつそれらが処理する情報は企業の活動にとってなくてはならないものとなっている。そのため、コンピュータセキュリティインシデント（以下、インシデントと表記）の原因を突き止めるための仕組みや、適切なシステムの改善計画を有していない組織においては、インシデントの発生による業務への多大な影響により、生産性の減少や、社会的信用の失墜、場合によっては社外に与えた損害による多額の賠償の支払いが生じるなど、組織の存続が危ぶまれる事態を招いてしまう。

あらゆるインシデントの可能性を未然に防ぐために必要なすべてのセキュリティ対策を実践できる組織は恐らく存在しないだろう。また、システムの複雑化が加速している現状においては、情報システムをどんなにセキュアに構築・運用したとしても、インシデントが発生する可能性を排除することはできない。

Computer Security Incident Response Team（CSIRT・シーサート）は、発生したインシデントに関する分析、対応を行うだけでなく、セキュリティ品質を向上するための教育、監査などの活動を行う組織である。その活動の目的は、効果的なインシデントレスポンス[1]を実践し、上記のような事業リスクを軽減することである。

CSIRT を構築することにより、以下のメリットを享受できる。

- ✓ インシデントやセキュリティイベント[2]の検知と的確な組織への迅速な情報伝達
- ✓ インシデントレスポンスの実践によるノウハウの蓄積と共有
- ✓ インシデントの再発防止を目的としたセキュリティ品質の向上

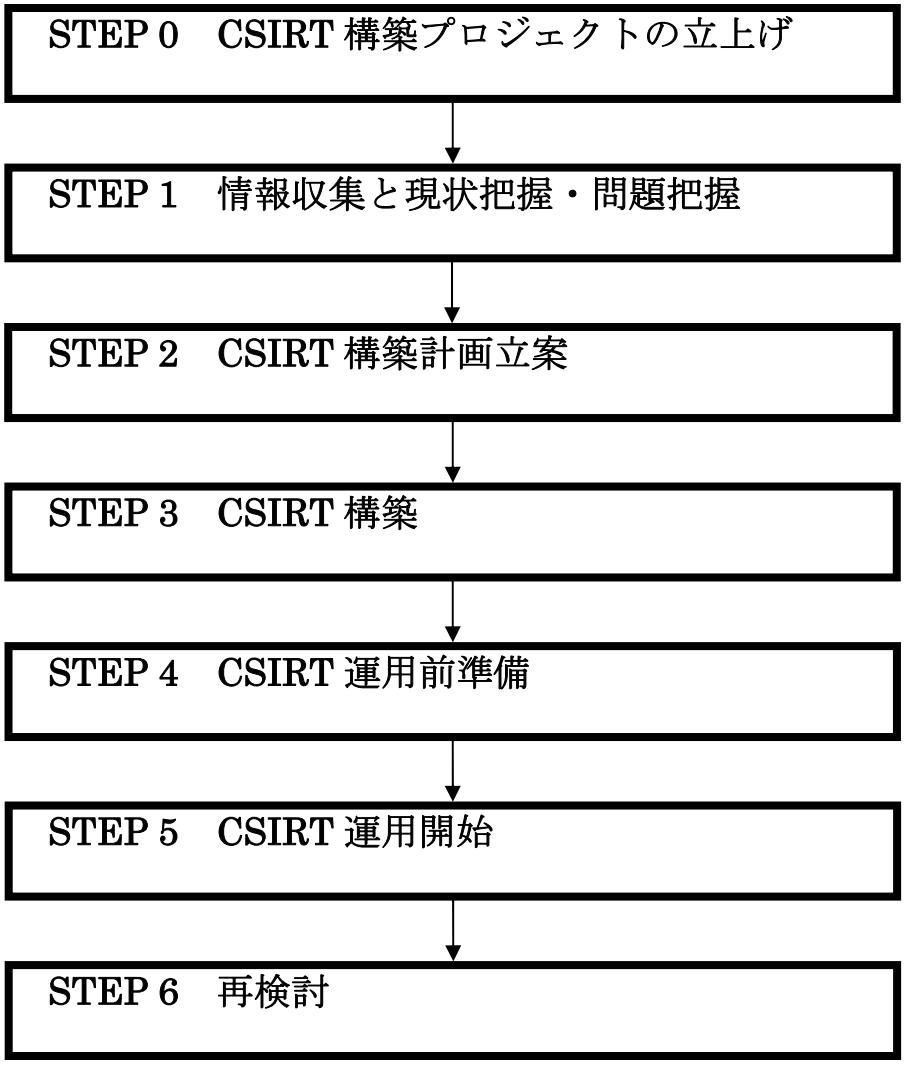
インシデントへの対応は、すでに多くの企業が何らかの対策に取り組んでいることであろう。しかし、それは組織の一部であり、全体として実際にインシデントレスポンスの体制が整備されている企業はほんの一握りでしかない。既存のインシデントレスポンスのためのリソースを有効に利用しながら、社内全体で適切なインシデントレスポンスを実践する CSIRT の構築が急務となっているのである。

インシデントは企業の存続をも脅かす事態であり、必ず対策すべきである。CSIRT を構築し、適切なインシデントレスポンスを実践する体制を確立することによって、企業活動を脅かす重大な事態を回避することが各企業の生産性の向上につながり、結果として、社会的信頼の向上・事業目標の達成が実現されるのである。

1　インシデントに対応するための事前もしくは事後の対応
2　本書では、インシデントと思われるが、インシデントとは確定していない事象をセキュリティイベントと定義する。

3　CSIRT 構築のためのステップ

CSIRT がどのように構築されるかについては、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が、すべての CSIRT に適用する基本的なステップがある。CSIRT を構築することに関連するステップについて、以下に図示する。



4　CSIRT 構築のための詳細プロセス

「**3 CSIRT 構築のためのステップ**」で記載した各項目に関しての詳細を以下に示す。

STEP 0　CSIRT 構築プロジェクトの立上げ

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」を立ち上げる。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す。

① 目標（CSIRT を構築すること）
- CSIRT 構築のきっかけの明確化

② プロジェクトの構成メンバ
- セキュリティインシデントに関連するメンバで構成
- メンバの利害関係の明確化
- 物理的に離れているメンバのコミュニケーション手段の確保
- 必要時に応じて専門知識や意見を取り入れられる体制の確立

③ スケジューリング
- 時間的制約事項の確認

④ プロジェクト運営
- 運用ルールの明確化
- プロジェクト内の意思決定フローの確認
- 制約事項

CSIRT 構築プロジェクトの立ち上げにあたって、経営者/意思決定者の合意を得る必要がある。

STEP 1　情報収集と現状把握・問題把握

STEP 1 では、構築する CSIRT の組織的背景を含め、まず始めに組織が置かれている現状を調査する。これらの調査結果から、CSIRT を構築することにより達成すべき事柄が何であるのか、そして CSIRT を構築する上での課題が何であるかを抽出する。

収集すべき組織の現状を表す情報の例を以下に示す。なお、これらの情報の詳細については、「＜別紙＞CSIRT スタータキット（1）情報収集と現状把握・問題把握すべき内容」からも参照可能である。

- ✓ 守るべき情報資産と脅威の把握
- ✓ 既存のインシデントレスポンス体制
- ✓ 既存のセキュリティポリシーおよびセキュリティ関連文書
- ✓ 参考情報

その後、収集した情報を基に現状の問題点の洗い出しと CSIRT の構築のための検討を行う。以下に、CSIRT を構築する上で検討すべき課題の例を示す。

- ✓ CSIRT を設立するための基本となる要求は何であるのか
- ✓ どんなサービスを提供するべきか
- ✓ 組織のどこに CSIRT が配置されるべきか
- ✓ どの程度の規模の CSIRT が必要なのか
- ✓ CSIRT を構築するのにどのくらいのコストがかかるか

これらの検討結果を元に、次の STEP 2 では CSIRT 構築のための計画を立案していくこととなる。

STEP 2　CSIRT 構築計画立案

① CSIRT基本構想の検討
② サービスの検討
③ 社内体制の検討
④ 社外連携体制の検討
⑤ リソースの検討
⑥ 理想像とのギャップ考察
⑦ 構築スケジュールの検討

STEP 2 では、STEP 1 で抽出した課題・問題を解決するために、どのような CSIRT を構築するのか、CSIRT 構築計画を作成する。CSIRT の構築計画には、以下に示す手順がある。

① CSIRT 基本構想の検討

CSIRT 基本構想の立案により、構築する CSIRT の方向性の明確化を行い、達成する目的の基礎的な理解を得るために、CSIRT 基本構想を検討する。

- **サービス対象の定義**

サービス対象とは、CISRT が提供する特定のサービスを利用できる、グループや組織のことである。サービス対象を定義することは、構築する CSIRT の方向性を定める大きな要因である。

以下に参考として、サービス対象を例示する。

ABC-CSIRTのサービス対象
ABC社の業務に従事する情報システム管理者、運用担当者、利用者、およびセキュリティ管理者

- **ミッションの定義**

CSIRT を構築することによって達成すべきミッションを定義する。ミッションには、以下の内容が含まれることが望ましい。

- 組織が置かれている立場・状況
- 目標を達成するために遂行する手段
- 達成すべき目標

なお、CSIRT が達成すべき大きな目標は、構築する CSIRT の組織的背景によって変化するが、主に以下に示す内容に集約される。

- インシデントの発生・再発を予防するための活動を行うこと
- 適切なレスポンスと有効な対策を実施することにより、インシデントの被害を抑制し損害を最小限にすること

各組織において定義するミッションについては、実現するための具体的な手順や実現すべき具体的な目標について、明確かつ簡潔な表現が望ましい。また、サービス対象との係わり合いについて示されていることが望ましい。

以下に参考として、ミッションを例示する。

ABC-CSIRTのミッション
ABC社のセキュリティ分野における取組みの中核として、情報セキュリティに関する信頼できる相談窓口を提供し、ABC社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検知、解決、被害局限化、および発生の予防を支援することにより、ABC社および情報ネットワーク社会のセキュリティ向上に貢献します。

- **取扱うインシデントの定義**

STEP 1 で把握した問題のうち、CSIRT により解決すべき対象を定め、取扱うインシデントの定義を行う。CSIRT で取扱うインシデントを定義することにより、CSIRT の機能として持つべきサービス・リソース等について検討することができる。

取扱うインシデントを分類するための参考として、「＜別紙＞CSIRT スタータキット(2) インシデントの分類」を示す。しかし、これらは、システム的側面からの分類であり、同じ分類に属するインシデントでも、実質的被害は情報システムの性質により多種多様となることに注意しなければならない。

② サービスの検討

サービスとは、構築する CSIRT が行うインシデントレスポンスの具体的内容である。以下に一般的な CSIRT のサービス概要を示すが、この全てを CSIRT が実装する必要はない。どのようなサービスを実装するかは、サービス対象、ミッション、取扱うインシデントによって CSIRT ごとに検討する。

CSIRT のサービスは大きく 3 つのカテゴリに分類できる。

- **インシデント事後対応サービス**
  インシデントの被害局限化を目的とした、インシデントやインシデントに関連する事象への対応を行うためのサービス。
- **インシデント事前対応サービス**
  インシデントの発生抑制を目的とした、インシデントやセキュリティイベント

の検知や、発生の可能性を減少させるためのサービス。

- **セキュリティ品質向上サービス**
  社内セキュリティの品質を向上させることを目的としたサービス。CSIRT としての視点や専門知識での見識を提供し、社内組織と連携することにより効果的な活動を実施できる。間接的にインシデントの発生抑制をすることが可能。

表 1 に、代表的なサービスの一覧を示す。これはあくまで代表的な CSIRT のサービスであり、全てを網羅する必要はなく、これ以外のサービスを提供する場合もある。（サービスの詳細は「＜別紙＞CSIRT スタータキット （3） サービス」を参照。）

インシデント 事後対応サービス	インシデント 事前対応サービス	セキュリティ品質向上 サービス
・ インシデントハンドリング ・ コーディネーション ・ コンピュータ・フォレンジックス ・ オンサイトインシデントレスポンス ・ インシデントレスポンスサポート ・ アーティファクトハンドリング ・ 脆弱性情報ハンドリング	・ セキュリティ関連情報提供 ・ インシデント/セキュリティイベント検知 ・ 技術動向調査 ・ セキュリティ監査/査定 ・ セキュリティツールの管理 ・ セキュリティツールの開発	・ リスク評価分析 ・ 事業継続性、災害復旧計画作成・改変 ・ セキュリティコンサルティング ・ セキュリティ教育/トレーニング/啓発活動 ・ 製品評価・認定

表 1 CSIRT のサービス概要

提供するサービスを検討すると共に、サービスを提供するための CSIRT に必要な権限についても検討を行う。特にインシデントハンドリング[3]は重要であり、CSIRT として実装しなければならない。インシデントハンドリングには、そのプロシージャを CSIRT として定める必要がある。

また、社内において既存で提供しているインシデントレスポンス機能があれば、その既存の機能を有効に利用すべきであり、CSIRT との連携関係について検討を行う。必要に応じて、既存のインシデントレスポンス機能を CSIRT に移管することも考慮に入れる。

③ 社内体制の検討

CSIRT が社内で機能するために、社内における体制の検討を行う。社内の体制

[3] 発生したインシデントへの対応を行い、被害局限化・復旧のための活動

を整備すべき対象の部門は、「＜別紙＞CSIRT スタータキット（4）インシデントレスポンスに関連する部門」に一覧を示す。

例えば、ある CSIRT においてサービス対象が社内システム全般・全社員である場合、そのサービス対象にサービスを提供できる社内体制でなければならない。上記を実現するためには、図 1 のようなイメージの体制が有効に機能する場合がある。

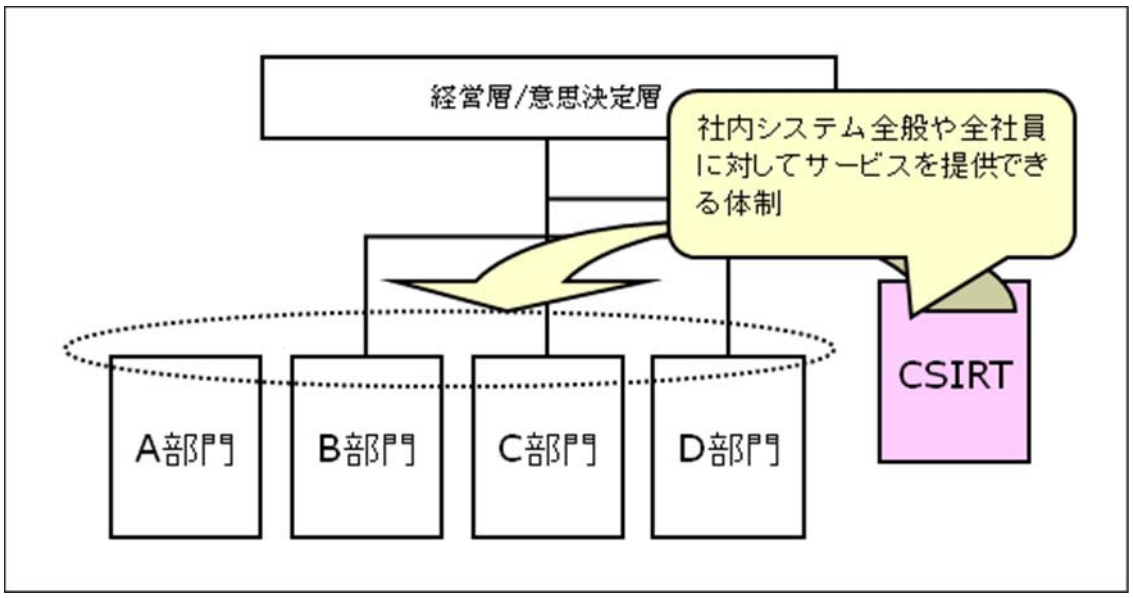


図 1　サービス対象が社内システム全般や全社員の場合の体制イメージ

また、企業体が大きく、1 つの CSIRT では社内システム全般・全社員へのサービスの提供が難しい場合には、図 2 のように、部門ごとの CSIRT を構築し、全社的な調整を行う CSIRT を構築するという体制が有効に機能する場合がある。

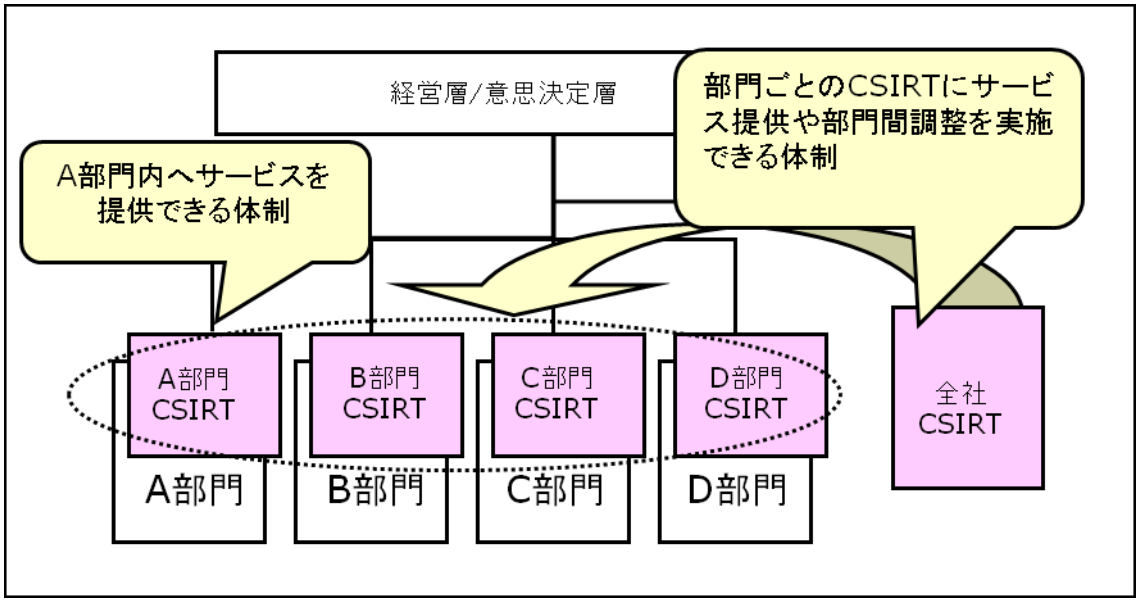


図 2 サービス対象が社内システム全般や全社員の大企業の場合の体制イメージ

図 2 のような階層的な CSIRT の体制は、グループ企業を傘下に持ち、サービス対象がグループ会社全般の CSIRT でも有用に機能する場合がある。このような場合の体制イメージを図 3 に示す。

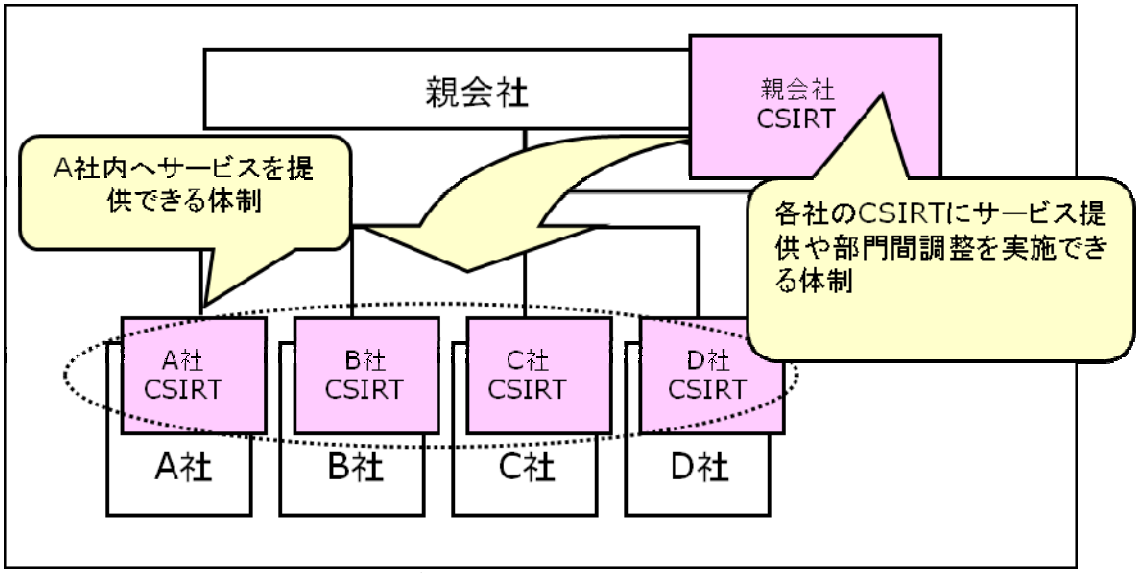


図 3 サービス対象がグループ会社全般の場合の体制イメージ

また、社内体制を検討するにあたり、CSIRT に必要な権限と、既存でのインシデントレスポンス機能を持つ部門と CSIRT との連携体制と責任分解点を、体制検討の内容に反映させる。

併せて、CSIRT の設置場所についての検討を行う。

④ 社外連携の検討

インシデントレスポンスは社内だけでなく、社外と連携した活動が必要となるケースがある。よって、外部組織との連携体制について検討を行う。

- **外部 CSIRT との連携**

  外部 CSIRT との連携によって、インシデントの早期検知やインシデントレスポンスノウハウの共有、組織間をまたがるインシデントハンドリングの実施など、CSIRT の活動をより効果的に実施することができる。効果的な CSIRT 間連携を実現するために、どのような外部 CSIRT と連携を行い、何を実現するかの検討が必要である。

  代表的な CSIRT 間連携のフレームワークの例として、FIRST[4]や APCERT[5]などがあげられる。また、日本の CSIRT 間連携のためのコミュニ

[4] Forum of Incident Response and Security Teams の略で、世界中の CSIRT で構成される組織。(http://www.first.org/)

[5] Asia Pacific Computer Emergency Response Team の略で、アジア太平洋地域の CSIRT で構成される

ティとして、日本シーサート協議会[6]が存在している。

- **外部組織との連携**

  インシデントレスポンスにおいて、法執行機関(警察など)や報道機関、製品ベンダーとの対応・連携が必要な場合もある。それらの外部組織との対応方針について事前に定めておくべきである。

⑤ リソースの検討

CSIRT 内に必要なリソースを検討する。サービスの提供や社内外体制の確立のために必要となるリソースを検討することが望ましいが、組織内でのリソースの制限も考慮する。どのような人的リソースが必要かは、「＜別紙＞CSIRT スタータキット(5)リソース」に概要を示す。

- **人的リソースの検討**

  CSIRT の活動に必要なスキルを持つスタッフを何名体制で実現するかを検討する。インシデントレスポンスに即戦力となるリソースが確保できない場合には、スタッフの育成に関しても検討する。育成を行うにあたっては、社内での育成だけでなく、インシデントレスポンス用の商用のトレーニングを利用することにより効率的に育成を行うことも可能である。

- **設備的リソースの検討**

  CSIRT として運営するための必要な設備を検討する。CSIRT が取扱うインシデント情報は機密情報である場合がほとんどであるため、同じ社内であっても不必要に情報が開示されないような設備を整える。

- **予算**

  人的リソースや、設備的リソースの規模とその維持・運用管理にかかる費用より、CSIRT の活動に必要な予算を割り出す。初期経費と維持経費を検討する。

⑥ 比較検討

“現状”、“構築する CSIRT”、“インシデントレスポンスの理想像”を比較することにより、CSIRT 構築時の実施内容の洗い出しと、運用開始後の CSIRT の発展の構想を持つことができる。

- **現状と CSIRT 構築後の比較による、CSIRT 構築時の洗い出し**

組織(http://www.apcert.org/)

[6] 日本シーサート協議会(正式名称:日本コンピュータセキュリティインシデント対応チーム協議会、NCA と略される場合も)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行っている(http://www.nca.gr.jp/)

現状と、CSIRT 構築後の比較を行い、CSIRT 構築時の具体的実施内容の洗い出しと実施内容の優先度付けを行うことができる。

今まで発生したインシデントなどからインシデントシナリオを作成し、インシデントレスポンスのシミュレーションを実施することにより、現状とCSIRT構築後との効果的な実施内容の洗い出しを行うことが可能である。また、シミュレーションにより計画の不備が見つかれば、計画の再検討を行うことも可能である。

● 構築する CSIRT と理想像とのギャップ考察

リソースの制限や社内の制限事項などにより、構築時の CSIRT がインシデントレスポンスの理想像となっていない場合には、理想像との乖離を課題点として整理をしておく。その課題点を CSIRT 運用開始後の改善内容とし、理想像に近づけるための中長期的な活動指針を得ることができる。

⑦ CSIRT 構築スケジュール検討

これまで検討してきた内容を整理し、CSIRT の活動のメリットを示すことにより、社内に CSIRT 必要性を認識してもらうために CSIRT 構築計画説明資料の作成を行う。

以下の対象者ごとに資料を作成する。

● 経営層/意思決定層

- CSIRT 構築の承認のための資料

● インシデントレスポンスに関連する部門

- 社内調整のための資料

● サービス対象

- CSIRT 説明用資料

● CSIRT 内資料

- CSIRT 内体制整備のための資料

STEP 3　CSIRT 構築

① 経営層/意思決定層の承認とリソースの確保
② 社内調整の実施
③ サービス対象への説明
④ CSIRT体制整備
⑤ 必要文書の作成

STEP 3 では、STEP 2 で作成した CSIRT 構築計画を基に、CSIRT を構築する。

① 経営層/意思決定層の承認とリソースの確保

STEP 2 で作成した CSIRT 構築計画について、経営層/意思決定層からの承認を得る。併せて、CSIRT 構築のためのリソースの確保を行う。

② 社内調整の実施

インシデントレスポンスに関連する社内の様々な部門との調整を行い、CSIRT が機能できる体制を整える。

③ サービス対象への説明

CSIRT 構築に関してサービス対象に説明を実施し、CSIRT に関しての理解を得る。また、サービス対象のニーズを把握し、CISRT 構築の活動の方向性に反映すべきかの検討の要因とする。

④ CSIRT 体制整備

構築する CSIRT 自体の体制整備を行う。リソースの調達やスタッフへのトレーニングの実施を行う。

⑤ 必要文書の作成

CSIRT の活動のための資料作成を行う。CSIRT 構築計画説明資料の内容を利用し、CSIRT 内の文書とする。文書は CSIRT の概要を示す文書と、CSIRT の運用に必要な文書を作成する。CSIRT の概要を示す文書に関しては、「＜別紙＞CSIRT スタータキット (6) 文書」に示す。

CSIRT の運用に必要な文書に関しては、CSIRT 内体制の文書や、インシデントレスポンスフロー、業務上の規則・注意事項、連絡先一覧など、より実務的なドキュメントである。

CSIRT 構築するにあたっての障害があるようならば、計画の再度見直しを行い、組織にとって最適な CSIRT とする。

STEP 4 CSIRT 運用前準備

✓ シミュレーションの実施

STEP 4 では、今まで発生したインシデントや、想定したインシデントより、インシデントシナリオを作成し、机上で CSIRT の活動のシミュレーションの実施を行う。シミュレーションの実施により、構築した CSIRT の有用性を確認し、運用開始前に問題点を洗い出すことができる。洗い出せる問題としては、社内連携体制や情報の伝達経路、責任分解点の明確化などである。シミュレーションを効果的に実施するために、インシデントレスポンスに関連する組織の代表者が出席するべきである。

シミュレーション実施後は必ず改善点に関する検討を実施し、結果を STEP 3 で作成した資料に反映させる。

STEP 5　CSIRT 運用開始

① 周知
② CSIRTのサービスをサービス対象へ提供
③ 社外連携体制の確立

STEP 5 では、STEP 4 までの構築手順を経て CSIRT の運用を開始する。

① 周知

サービス対象や社外へ CSIRT の存在をアピールすることが必要である。また、CSIRT の運用を開始するためには、CSIRT の連絡先をサービス対象に周知徹底を行わなければならない。社外への周知にはニュースリリースを利用することが一つの効果的な方法である。

② CSIRT のサービスをサービス対象へ提供

CSIRT のサービスをサービス対象へ提供を行うことにより、実質的に CSIRT の運用が始まる。インシデントレスポンスを行い、事業リスクの軽減に努めていくこととなる。

③ 社外連携体制の確立

STEP 2 で検討した社外連携体制の確立を行っていく。事業リスク軽減のための効果的な連携の確立を実施する。

CSIRT が運用を開始した時点で、「CSIRT 構築プロジェクト」は目的の達成となる。次の STEP 6 からは、実際の CSIRT の運用となる。

STEP 6　再検討

STEP 6 では、STEP 5 で運用を開始した CSIRT の組織的機能の再検討を実施する。再検討は運用開始後に定期的に行い、品質向上や機能拡充に努めていく必要がある。再検討では、CSIRT での活動自体の分析や、サービス対象のニーズの把握、シミュレーションの実施など結果を基に行うとよい。また、コンピュータセキュリティを取巻く環境は日進月歩で進化しており、CSIRT も進化させなければならないということを常に念頭においておく必要がある。更に、継続的に社外との有用な連携体制を模索していく必要がある。

5　終わりに

コンピュータセキュリティには、これで十分ということはない。CSIRT の構築はインシデントのリスクを軽減させるための手段の一つにすぎない。しかし、CSIRT の構築は組織にとって有効なインシデントへの対抗策である。日本シーサート協議会では、日本の CSIRT 構築活動支援をミッションとしている。不明点等があれば、以下へ問合せを実施してほしい。

＜日本シーサート協議会の連絡先＞

〒101-0054
東京都千代田区神田錦町 3-17 廣瀬ビル 11 階
一般社団法人 JPCERT コーディネーションセンター内

Email：nca-sec@nca.gr.jp
Tel：03-3518-4600
（日本シーサート協議会事務局担当を呼び出してください）

執筆および協力者一覧

石塚　元	NTT Com
佐久間　邦彦	株式会社 JSOL
佐川　香織	KLIRRT
曽根　基樹	シャープ株式会社
山賀　正人	NCA 専門委員
庄司　朋隆	TOPPAN-CERT
福本　佳成	Rakuten-CERT
軍司　祐介	Rakuten-CERT
橘　喜胤	OKI-CSIRT
沼田　亜希子	HIRT
寺田　真敏	HIRT
茂岩　祐樹	DeNA システム統括本部 IT 基盤部
杉浦　芳樹	NTT-CERT
林　郁也	NTT-CERT
吉田　尊彦	NTT-CERT

＜別紙＞ CSIRT スタータキット

(1) 情報収集と現状把握・問題把握すべき内容

大項目	小項目	情報の利用目的
守るべき対象と脅威の把握	社内システム・ネットワーク － 運用主管 － 重要なシステム － 情報資産	CSIRT が取扱うインシデントの定義の判断材料
	過去のインシデント情報 － 発生した重大なインシデント － 再発傾向にあるインシデント	
	既存のリスク分析結果	
既存のインシデントレスポンス体制	既存のインシデントへの事前対応 － 実施主管組織/部門間連携体制/手順	既存インシデントレスポンスの機能面・体制面からの問題点・改善点の洗い出し
	既存のインシデントへの事後対応 － 実施主管組織/部門間連携体制/手順	
	既存のセキュリティ向上に向けた取り組み － 実施主管組織/部門間連携体制/手順	
	既存のインシデントレスポンスに関連する社外組織	インシデントレスポンスに有効な社外連携体制の確立
	インシデントレスポンスに有効な社外連携体制の確立	
既存のセキュリティポリシーおよびセキュリティ関連文書	セキュリティポリシー	インシデントレスポンス時の制約の把握
	災害復旧計画・事業継続性計画	
	セキュリティに関連する制約事項や規制	
	物理セキュリティに関する制限事項	
参考情報	他の CSIRT の情報[7]	CSIRT 構築にあたっての参考情報

表 2 STEP1 での収集すべき情報

[7] 日本シーサート協議会（http://www.nca.gr.jp/）、FIRST(http://www.first.org/)や APCERT(http://www.apcert.org/)より世界の代表的な CSIRT の情報を収集することができる。

(2) インシデントの分類

プローブ、スキャン、そのほか不審なアクセス	- 弱点探索（サーバプログラムのバージョンのチェックなど） - 侵入行為の試み（未遂に終わったもの） - ワームの感染の試み（未遂に終わったもの）
サーバプログラムの不正中継	- メールサーバやプロキシサーバなどの、管理者が意図しない第三者による使用
不審なアクセス	- From: 欄などの詐称
システムへの侵入	- システムへの侵入、改ざん（root kit などの専用ツールによるものも含む） - DDoS 攻撃用プログラムの設置（踏み台）
サービス運用妨害につながる攻撃（DoS）	- ネットワークの輻輳（混雑）による妨害 - サーバプログラムの停止 - サーバ OS の停止や再起動
コンピュータウイルス・ワームへの感染	
その他	- UCE(いわゆるスパムメール)の受信

表 3 一般的なインシデントの大別

(3) サービス

CSIRT のサービスは大きく 3 つのカテゴリに分類できる。

1) インシデント事後対応サービス

インシデントの被害局限化を目的とした、インシデントハンドリング。

2) インシデント事前対応サービス

インシデントの発生抑制を目的とした、インシデントやセキュリティイベント[8]の検知や、発生の可能性を減少させるためのサービス。

3) セキュリティ品質向上サービス

社内セキュリティの品質を向上させることを目的としたサービス。CSIRT としての視点や専門知識での見識を提供し、社内組織と連携することにより効果的な活動を実施できる。間接的にインシデントの発生抑制をすることが可能。

表 1 に、代表的なサービスの一覧を示す。これはあくまで代表的な CSIRT のサービスであり、全てを網羅する必要もなく、これ以外のサービスを提供する場合もある。

インシデント 事後対応サービス	インシデント 事前対応サービス	セキュリティ品質向上 サービス
・ インシデントハンドリング ・ コーディネーション ・ オンサイトインシデントハンドリング ・ インシデントハンドリングサポート ・ コンピュータ・フォレンジックス ・ アーティファクトハンドリング	・ セキュリティ関連情報提 ・ 脆弱性情報ハンドリング ・ インシデント/セキュリティイベント検知 ・ 技術動向調査 ・ セキュリティ監査/査定 ・ セキュリティツールの開発	・ リスク評価・分析 ・ 事業継続性、災害復旧計画作成・改変 ・ セキュリティコンサルティング ・ セキュリティ教育/トレーニング/啓発活動 ・ 製品評価・認定

表 1 CSIRT のサービス概要

以下、サービスの詳細を示す。

1) インシデント事後対応サービス

- インシデントハンドリング

  インシデントハンドリングは、CSIRT の基本的な機能であり、必ず実装すべきサービスである。インシデントハンドリングとは発生したインシデントへの対応を行い、被害局限化・復旧のための活動である。

[8] 本書では、インシデントと思われるが、インシデントとは確定していない事象をセキュリティイベントと定義する。

インシデントハンドリングはそのプロシージャを CSIRT として定める必要がある。

プロシージャを作成するための基となる情報として、インシデントハンドリングの一般的なフローを以下に図示する。

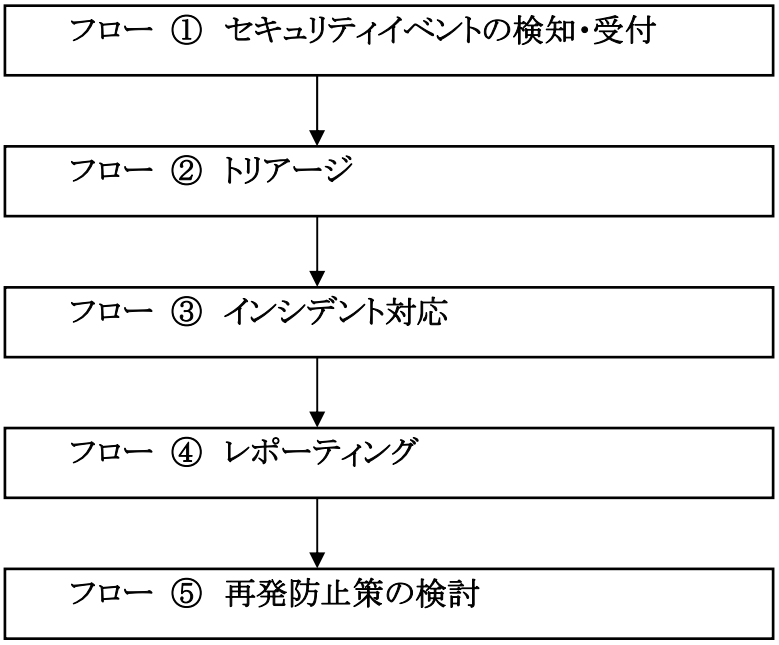


図 4 インシデントハンドリングの基本的な流れ

フローに記載してある内容を以下に示す。

① セキュリティイベント[9]の検知・受付

セキュリティイベントの報告の受付を行い、管理を行うことである。

② トリアージ[10]

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、インシデントの優先順位付けの実施のことである。

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らない。ただ、コンピュータセキュリティを取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ある。

---

9 本書では、インシデントと思われるが、インシデントとは確定していない事象をセキュリティイベントと定義する。

10 トリアージという言葉は、一般的には医学で用いられている用語として用いられる。医学用語としては、限られたリソース中で、できるだけ多くの人々を救命するため、緊急度の高い患者を優先的に対応するという意味で用いられている。

トリアージは、以下の点を考慮し、作成した基準を元に実施する。

- 内容の事実確認
- 影響範囲の検討

一旦、トリアージを行ったインシデントに対しては、後から容易に参照できるようにするため識別子を付与することが望ましい。

③ インシデント対応

インシデントの原因究明や復旧対応のための活動である。トリアージされたインシデントの分析を実施し、インシデントがどのような性質を持っているか見極めなければならない。

インシデントを特徴づける要素としては、以下の項目が考えられる。

- 攻撃元
- 攻撃先
- インシデントが発生した日時
- 攻撃手法
- 影響範囲
- 被害発生の要因
- 講じうる対応策
- 被害拡大の可能性

上記の要因から、対応策を決定し、実施する。

インシデント対応時の CSIRT の機能としては、以下が代表的なものである。

- コーディネーション

  社内外問わず、複数の組織にて、それぞれの責任の下でインシデントハンドリングを行うことが必要となってくる場合がある。一貫した効果的なインシデントハンドリングを行うためには、CSIRT がインシデント全体を把握したコーディネータの役割を果たすことが求められる。インシデンハンドリングを迅速に進める上では、即時性のあるコーディネーションが必要とされる。

- オンサイトインシデントハンドリング

  インシデントが発生したシステムやネットワークに対して、CSIRT が直接復旧作業を行う。システムの運用担当者との責任分解点を定めておく必要がある。

- インシデントハンドリングサポート

  CSIRT がメール・電話・ドキュメントの提供等を行うことによるインシ

デントハンドリングを行う。

- **コンピュータ・フォレンジックス**
  インシデントが発生したコンピュータから、証拠となりうるデータを保存し、(1)どのような被害を受けたか、(2)どこから侵入を受けたか、(3)誰が侵入者かなどを分析し、インシデントハンドリングを行う。コンピュータ・フォレンジックスを実施するためには、専門のスキルを持ったメンバの CSIRT への配置とコンピュータ・フォレンジックス専用ツールの準備も必要である。また、コンピュータ・フォレンジックスでは機密情報を取り扱う可能性が大きいため CSIRT 内の情報管理を徹底する必要がある。

- **アーティファクトハンドリング**
  インシデントハンドリング時に発見された不審なプログラムを解析するサービスである。不審なプログラムのソースコードの解析や、隔離した環境でのプログラムの挙動解析を実施し、不審なプログラムがインシデントの原因であるかどうかの調査を行う。専門のスキルを持ったメンバの CSIRT への配置や、他のネットワークから隔離されたアーティファクトハンドリング専用の設備が必要である。

④ レポーティング

インシデント原因究明や、復旧対応等が行われた後に、インシデントハンドリングの結果のレポーティングを行う。CSIRT 内部でのインシデントハンドリングのノウハウの蓄積や、インシデントオーナー[11]や社内の報告先への報告書等の目的によって利用できる。

⑤ 再発防止策の検討

収束したインシデントの原因を分析し、再発防止策を講じる必要がある。
インシデント分析にあたっては、以下の項目を再整理する必要がある。

- インシデント詳細内容
  - 原因
  - 被害状況
  - インシデントンシデント検知の契機
  - 初動対応・暫定対応
  - 恒久対応
- インシデントハンドリングに関わった組織

[11] インシデント発生元の組織や人物

- インシデントハンドリングの良かった/悪かった点

分析した結果を元に、再発防止のための対策を実施する必要がある。

2) インシデント事前対応サービス

- **セキュリティ関連情報提供・アナウンスメント**

  セキュリティ情報をサービス対象に情報提供するサービスである。提供する情報を以下に例示する。

  - CSIRT の活動内容周知/連絡先周知
  - ポリシー/プロシージャ/セキュリティ関連のチェックリスト
  - 流行しているウイルス/ワーム情報や攻撃手法
  - インシデントレスポンスの一般的手法
  - インシデント統計情報

- **脆弱性情報ハンドリング**[12]

  ソフトウェアやハードウェアの脆弱性関連情報を分析し、サービス対象へ情報を伝達するサービスである。サービス対象はその脆弱性に対応したパッチの適応や、回避策の実施の管理を行わなければならない。脆弱性情報ハンドリングでは、サービス対象がどのようなソフトウェアやハードウェアを利用しているか把握しておかなければならない。

  また、自社にて開発した製品の脆弱性の場合には、その対応などもこのサービスに含まれる。

- **インシデント/セキュリティイベントの検知**

  インシデント/セキュリティイベントなどを検知するサービスである。検知する方法としては、IDS やハニーポットの設置、各種サーバ群のログの解析、P2P ファイル共有アプリケーションを経由した情報漏えい検知のための専用環境等がある。

- **技術動向調査**

  セキュリティ向上のための技術やインシデント検知技術、もしくは侵入技術等の最新のセキュリティ技術動向調査や目利きを実施し、サービス対象への有用性を確認するサービスである。有用な技術は

12　脆弱性情報の収集に参考となる URL の例を以下に挙げる。

- Security Focus (http://securityfocus.com/)
- Secunia (http://secunia.com/)
- SANS Handler's Diary (http://isc.sans.org/diary.php)
- FrSIRT (http://www.frsirt.com/english/)
- JVN (http://jvn.jp/index.html)

CSIRT に実装や、サービス対象へ情報提供などに利用する。

- セキュリティ監査/査定
  ドキュメントの確認やペネトレーションテストを通じて、監査/査定するサービスである。
- セキュリティツールの開発
  CSIRT やサービス対象が利用するセキュリティツールを開発するサービスである。例えば、新しいインシデント検知ツールや、暗号化技術を容易に利用することのできるスクリプトや、自動化されたパッチ配信の開発などである。

3) セキュリティ品質向上サービス

- **リスク評価・分析**
  企業や対象となる情報システムの機密性、完全性、可用性を阻害する様々なリスクを洗い出し、その影響度を分析するサービスである。目的としては、現状のリスクの認識と、リスクを減少させることである。一般的には以下の項目で行う。
  - 情報資産の洗い出し(プライオリティの設定)
  - 洗い出された資産に対するリスク分析
    リスク分析をもとにセキュリティポリシーや CSIRT のサービス、インシデントハンドリングのプロシージャなどに反映させることにより、リスクを低減できる。
- **事業継続性、災害復旧計画　作成・改変**
  大規模なインシデントが発生したとしても重要事業を中断させず、中断しても可能な限り短期間で再開させ、 中断に伴う顧客取引の競合他社への流出、マーケットシェアの低下、企業評価の低下などから企業を守るための経営戦略に CSIRT としてのインシデントレスポンス機能を事業継続性、災害復旧計画として反映させるサービスである。
- **セキュリティコンサルティング**
  CSIRT としてのノウハウをサービス対象の事業へ反映させるためのコンサルティングを行うサービスである。そのノウハウは、ビジネスにおいてセキュリティ要件を満たすための利用や、ノウハウ自体がビジネス化することなど、企業の持つビジネスにより利用形態は様々である。
- **セキュリティ教育/トレーニング/啓発活動**
  CSIRT でのノウハウや、そのノウハウを反映させたポリシー・プロシ

ージャ等を、セミナー・ワークショップ・コース・教材等を通じてサービス対象に教育やトレーニング、啓発活動を行うサービスである。人材開発部門等と連携して実施する場合が多い。

- **製品評価・認定**

  製品・ツール・プロダクト・サービス等に関して、それらをサービス対象がセキュアに利用できるものかどうかを CSIRT が評価・認定するサービスである。CSIRT にて、その組織に応じた評価・認定基準を作成する必要がある。

(4) CSIRT の活動に関連する部門

経営層/意思決定層	CSIRT 構築の承認による、資金やリソースの確保や、CSIRT に必要な責務と権限の社内の体制への反映。また、インシデントの最終報告先
情報システムの主幹・運用部門	サービス対象に位置付けられることもあり、インシデントハンドリング機能を持っている場合もあり、CSIRT の活動に深く関連
内部統制部門	インシデントレスポンスと内部統制的活動との連携（CSIRT の活動は内部統制的な活動ではなく、あくまでインシデントレスポンスであることを念頭に置いておく必要がある。）
法務部門	インシデントレスポンスにおける法的対応時
広報部門	インシデントレスポンスにおけるマスコミ対応時
人事部門	CSIRT のスタッフの配置・雇用。インシデント発生元の人事的処置実施時（CSIRT の活動は人事的処置のためではなく、あくまでインシデントレスポンスであることを念頭に置いておく必要がある。）
人材開発部門	セキュリティのノウハウやポリシー、セミナー・ワークショップ・コース・教材等を通じてサービス対象に教育やトレーニング、啓発活動
経営企画部門	事業継続性計画・災害復旧計画とインシデントレスポンスの反映
ヘルプデスク	インシデントへの対応時の一次窓口
物理セキュリティ部門	物品(特に PC)の盗難。入退出制限の管理・実施

表 4 CSIRT の活動に関連する部門の例

(5) リソース

必要なリソースの概要に関して、以下に示す。

- **人的リソース**

  CSIRT には以下の役割を持つ人的リソースが必要である。

  - マネージャー/チームリーダー/グループリーダー
    チームやグループの責任者。チームやグループの意思決定を行う。
  - トリアージスタッフ
    インシデントのトリアージを司るスタッフ。設定したトリアージ基準に則り、トリアージを実施し、インシデントの優先順位付けを行い、そのインシデントに対してのハンドラーを割り当てる。
  - インシデントハンドラー
    トリアージしたインシデントに対してのインシデントハンドリングを実施するスタッフ。CSIRT のメンバとしての中核を支える。
  - その他、提供するサービスのスタッフ
    提供するサービスの活動を実施するスタッフ。

また、以下にスタッフに要求されるスキルの例を示す。

- 基本的技術スキル
  - OS(Windows, UNIX 等)のスキル
  - ネットワークスキル
  - プログラミングスキル
  - PGP 暗号の利用スキル
- セキュリティスキル
  - コンピュータへの攻撃に関するスキル/脆弱性に関するスキル
  - インシデントハンドリングの経験・スキル
- パーソナルスキル
  - コーディネーションスキル
  - コミュニケーションスキル
  - 問題解決能力

これらのスキルはあくまで基本的なスキルであり、それだけでは十分ではない。特に、CSIRT にて提供するサービスごとに必要となるスキルを持つスタッフが必要である。

- **設備リソース**

以下に必要な設備の例を示す。

- 基本的オフィス用品基本的技術スキル
    - CSIRT 用専用電話
    - スタッフ用コンピュータ（PGP 暗号などのセキュアなコミュニケーションを行うことができる環境）
    - スタッフ用携帯電話
    - 専用プリンタ
    - 専用シュレッダー　等々
- CSIRT 用インフラ
    - 入退出管理ができる CSIRT 用居室
    - CSIRT 用ネットワーク環境
    - 金庫
    - インシデントハンドリングシステム[13]
    - インシデントハンドリング用持出し PC
    - サービスを提供するのに必要となるインフラ　等々

[13] インシデントハンドリングシステムとは、インシデント情報の収集・分析・共有などを行うツールの総称である。

(6) 文書

CSIRT の概要を示す文書のテンプレートは RFC2350[14]に定義されている。このテンプレートに則って文書を作成することを推奨する。

1　文書情報
1.1　最終更新日
1.2　通知のための配布リスト
1.3　本書がある場所
2　連絡先情報
2.1　チームの名前
2.2　所在地
2.3　時間帯
2.4　電話番号
2.5　ファクシミリ番号
2.6　他の遠隔コミュニケーション
2.7　電子メールアドレス
2.8　公開鍵と他の暗号化情報
2.9　チームメンバ
2.10 他の情報
2.11 顧客連絡先
3　憲章
3.1　使命表明
3.2　構成員
3.3　スポンサーシップ、かつ／または提携
3.4　オーソリティ
4　ポリシー
4.1　インシデントの種類とサポートのレベル
4.2　協力、相互活動および情報の開示
4.3　コミュニケーションと本人認証
5　サービス
5.1　インシデント対応
5.1.1. インシデントトリアージ
5.1.2. インシデントコーディネーション
5.1.3. インシデント解決
5.2　予防的活動
6　インシデント報告フォーム
7　免責事項

---

[14] http://www.ietf.org/rfc/rfc2350.txt（英語）
http://www.ipa.go.jp/security/rfc/RFC2350JA.html（日本語）