JPCERT CC®

企業における情報セキュリティ緊急対応体制
～組織内 CSIRT の必要性～

JPCERT コーディネーションセンター
早期警戒グループ マネージャ
満永　拓邦

目 次

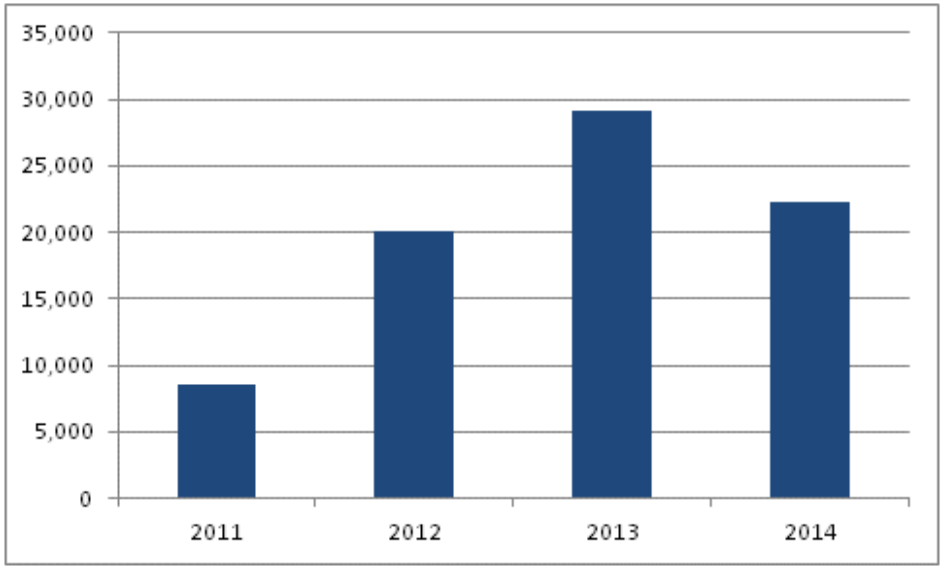
- 情報セキュリティを取り巻く現状と、情報セキュリティ緊急対応体制 (CSIRT*)
- CSIRT構築前の検討事項など
- CSIRT構築パッケージ

- CSIRT・・Computer Security Incident Response Team
  (コンピュータセキュリティインシデント緊急対応チーム)

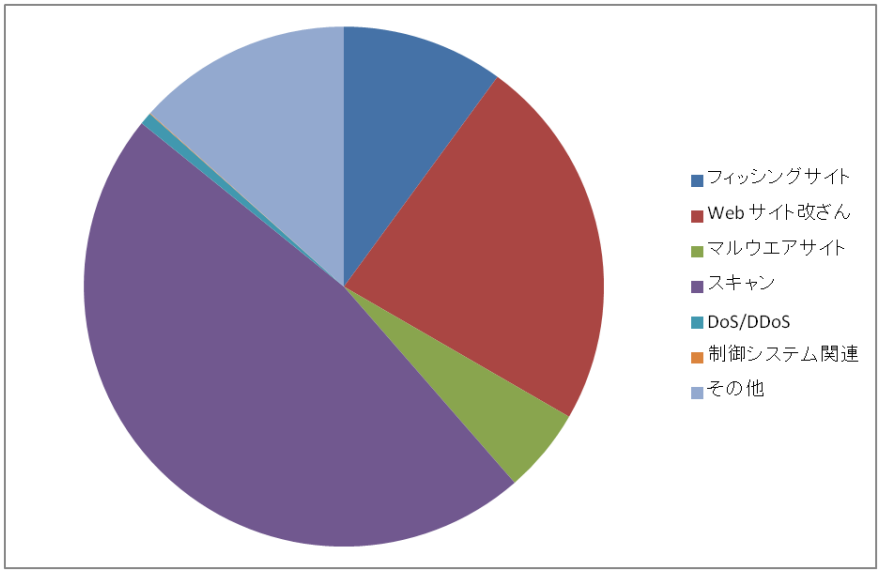
情報セキュリティを取り巻く現状と
情報セキュリティ緊急対応体制 (CSIRT)

JPCERT/CC が受領したインシデント報告件数

年	件数
２０１４年	２２,２５５件
２０１３年	２９,１９１件



報告件数の推移



2014年に受領した報告の内訳

JPCERT CC®

一般社団法人JPCERTコーディネーションセンター
（JPCERT/CC (ジェーピーサート・コーディネーションセンター)）

・経済産業省からの委託事業として、コンピュータセキュリティインシデントへの対応支援、国内外にセンサをおいた
インターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
・インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、我が国の窓口となる　CSIRT

インシデント数増加の背景

ITの社会インフラ化

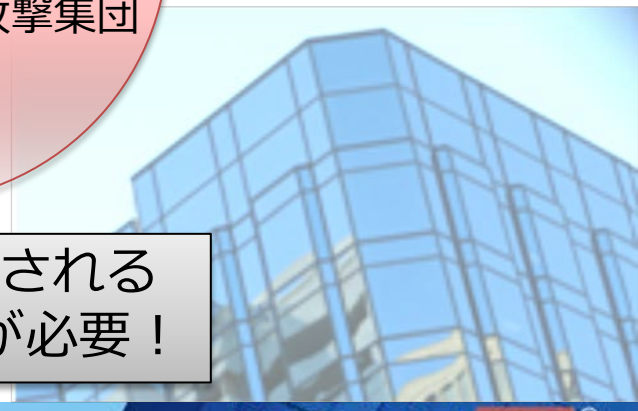
- 企業活動のIT化
- 電子商取引の発展
- 制御系システムへの利用

インターネットの世界的な普及

- ボーダレスの通信
- 物理的な追跡困難性

攻撃用インフラの整備

- 攻撃ツールの進歩
- 分業化された攻撃集団

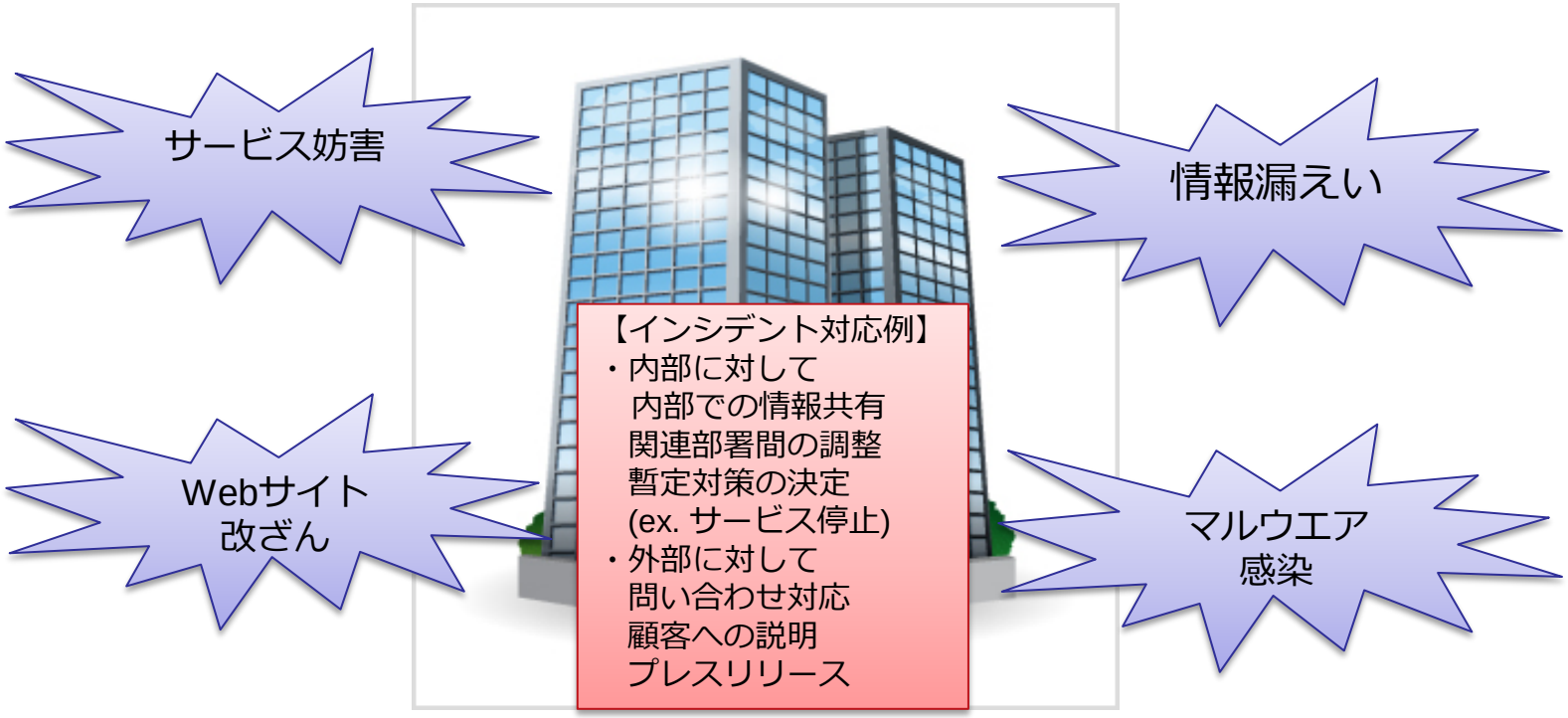


今後、サイバー攻撃の増加が予想されるため、各組織においても対応体制が必要！

セキュリティに関する対応体制

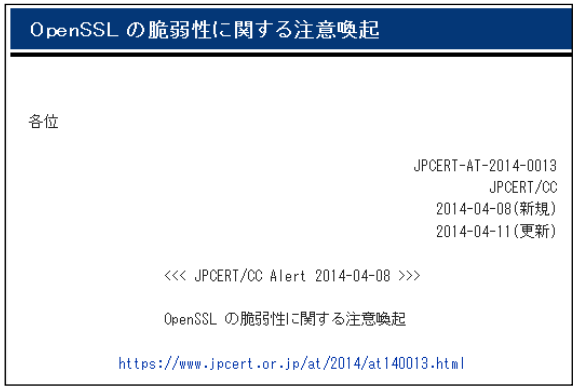
- インシデント(*)発生時の対応体制
  - ユーザ部門、システム管理、営業、法務、広報などの関連部署間で情報の共有および対策の一元化
  - システム責任者、対応フローの明確化(ex. 誰がサーバを止めれるか？)

インシデント(*)・・IT システムの正常な運用または利用を阻害するウィルス感染、不正アクセス、情報漏えい、DoS 攻撃などの事案や現象の発生をいう



例えば・・・

- 先月、 SSL等を利用するためのライブラリ「OpenSSL」に関する情報漏えいの脆弱性が公開された。攻撃手法も公開されており、いつ攻撃を受けてもおかしくない状況であった。緊急度が高い状況で、例えば以下の様な対応体制を事前に関係者間で確認しておく事で、迅速な対応が可能になる。
  - 管理サーバが、当該脆弱性の影響を受けるかの確認フローと担当
  - もし影響を受ける場合、サービス停止を決定する社内プロセス
  - 脆弱性や対応に関する社内の情報共有体制
  - 被害を受けた場合の対応手順、顧客への連絡、プレスリリースについて



OpenSSL の脆弱性に関する注意喚起

各位

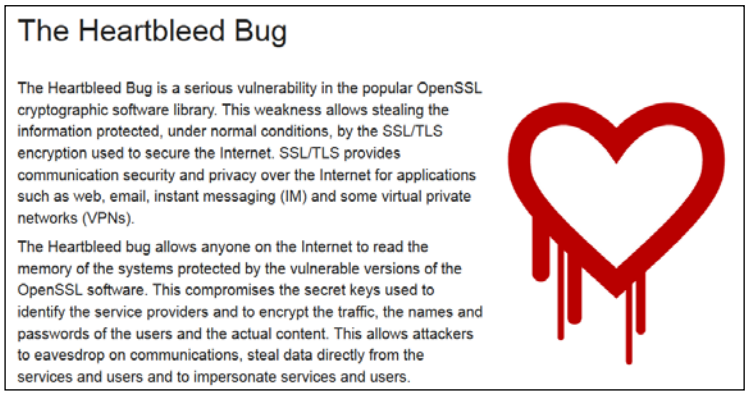
JPCERT-AT-2014-0013
JPCERT/CC
2014-04-08(新規)
2014-04-11(更新)

<<< JPCERT/CC Alert 2014-04-08 >>>

OpenSSL の脆弱性に関する注意喚起

https://www.jpcert.or.jp/at/2014/at140013.html

OpenSSL の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140013.html



The Heartbleed Bug

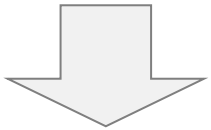
The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

The Heartbleed Bug
http://heartbleed.com/

完全なセキュリティ予防策はない

- インシデント対応活動
  - インシデントを検知し、或いはその報告を受けることにより認知し、影響の拡大を防ぐとともに、情報を収集して分析を加え、インシデントの全体像や原因について把握し、復旧措置や再発防止のための措置を取る
- 「コンピュータセキュリティ」で思い描くイメージ
  - 「いかにしてインシデントの発生を未然に防ぐか」を主眼に置かれることが多い
- コンピュータセキュリティを取り巻く状況を見ると．．．
  - 人為的ミス（パッチの適用忘れなど）
  - 未知（公知になっていない）の脆弱性の悪用
  - 技術的な対応の限界　等

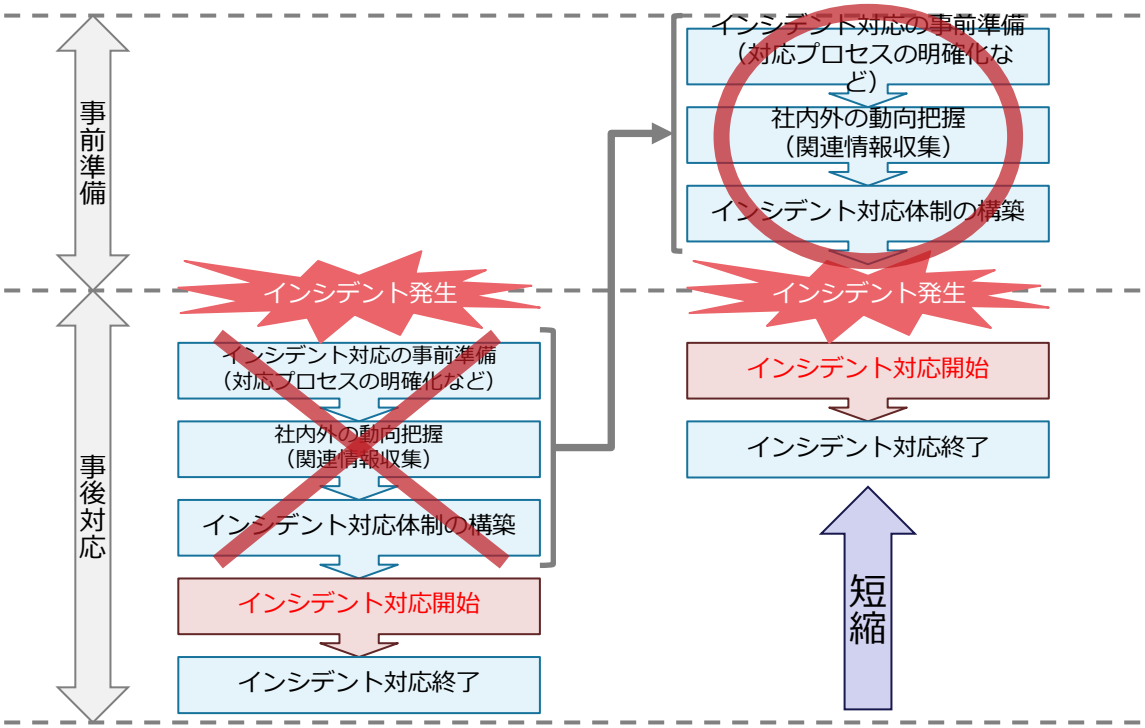


インシデントの発生を「完全に回避する」ための予防策はない
（事故前提の対応体制が必要）

（発生確率を低下させ、発生時の影響や被害を低減するための予防策はある）

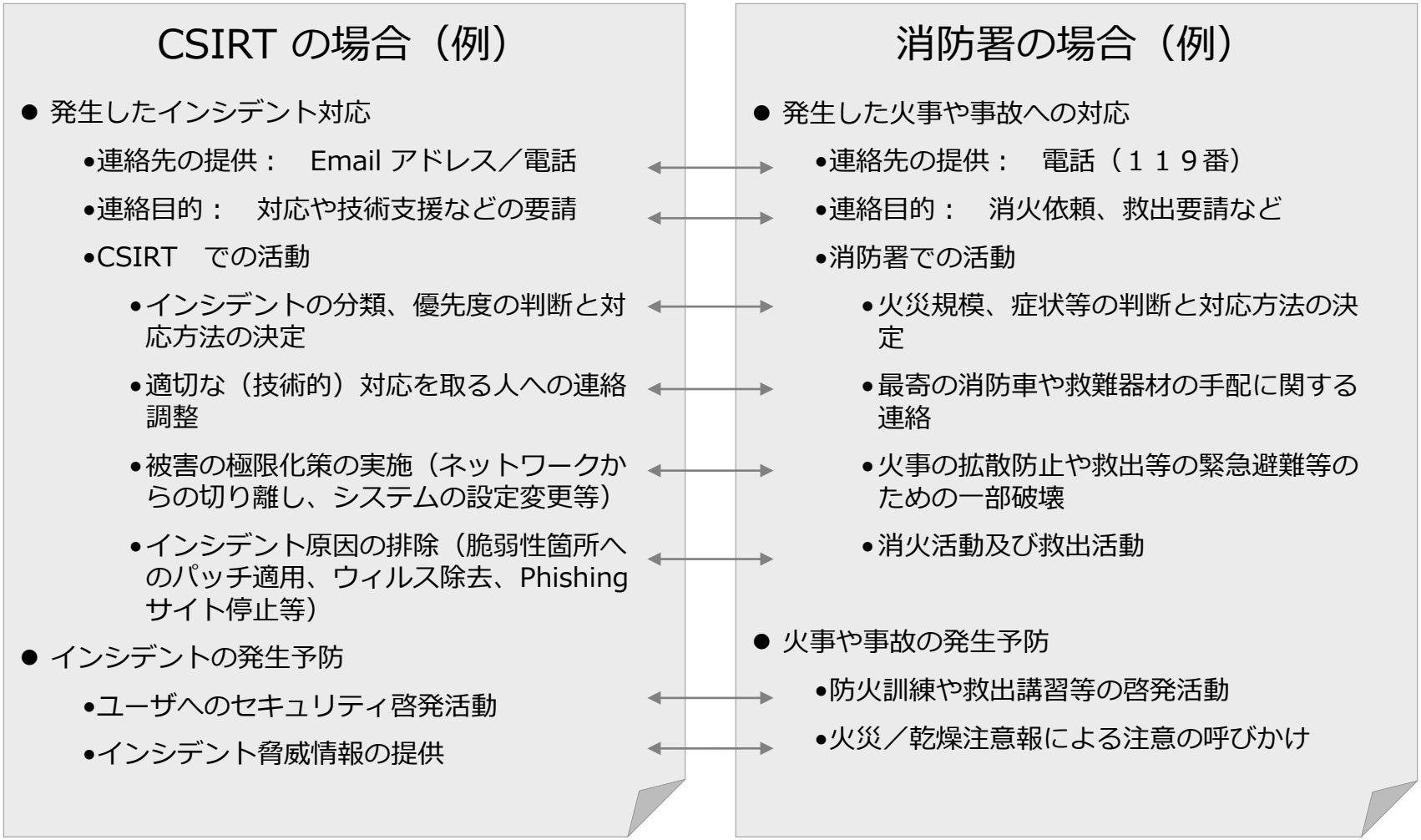
事前準備の重要性

- インシデント発生後、その対応方法を考え始め、対応体制をとるのは、被害を拡大させる一因となるため、<u>できるだけ**事前に**</u> 対応体制等を整えておく必要がある



対応体制構築、マニュアル整備に加え、
情報セキュリティに関する”避難訓練(対応訓練)”を実施してみる

CSIRT と消防署の役割の比較例



CSIRT構築前の検討事項など

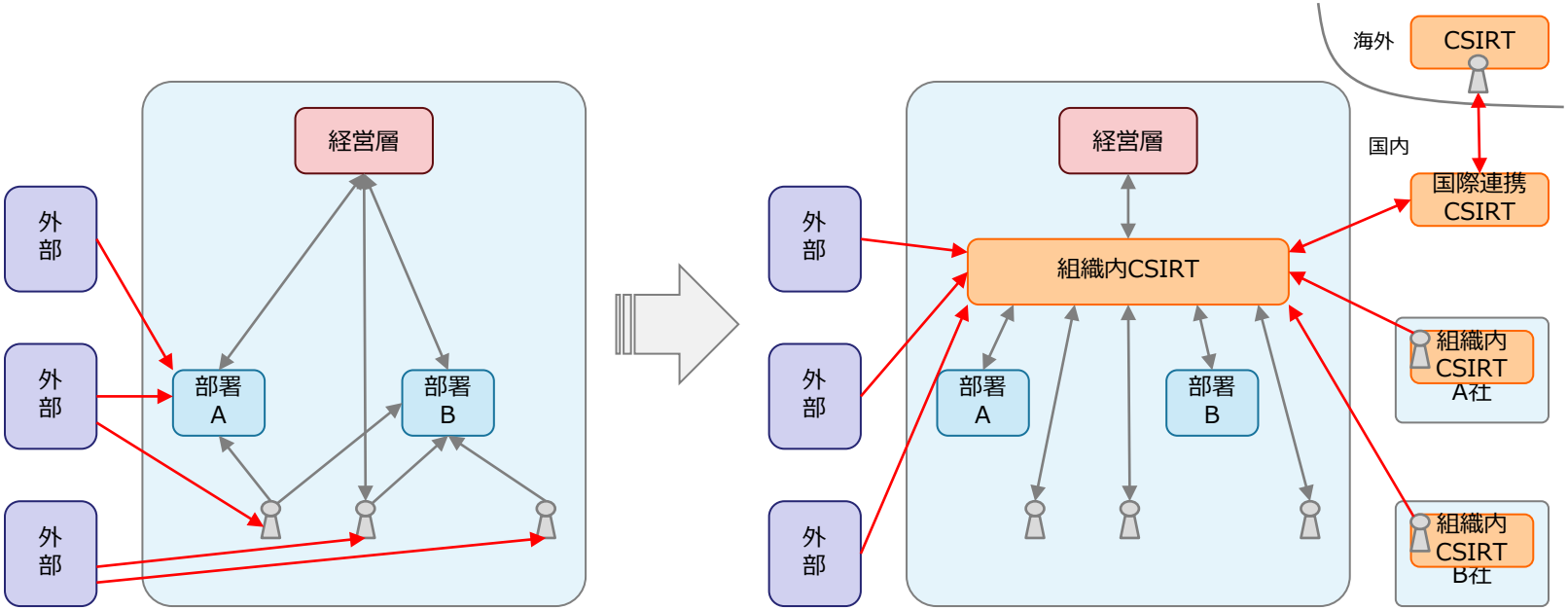
事前のインシデント対応計画の策定

- インシデント対応体制の構築には、事前の インシデント対応計画の策定が重要である

- 組織的なインシデント対応計画を策定するためのポイント
  - 複雑化する**ネットワーク及びシステムの把握**
  - インシデント対応の**担当者／責任者の明確化**
  - インシデント発生時の報告**窓口の一元化**
  - インシデント対応に必要な技術的支援、ノウハウ、関連情報の入手を支援する人／チーム／部署の設置
  - インシデント対応に必要なポリシー及びマニュアル等の整備
  - 外部組織に依頼する場合の、外部の対応能力の把握と適切な報告
  - リスク評価の実施と**リスク許容度**の設定

組織内 CSIRT のメリットのイメージ

- 組織の内外に対し、インシデントに関する一元的な対応窓口であるCSIRTを構築する



メリットの例：

①社内セキュリティ情報の共有、集中管理の実現
②セキュリティ対応にかかる指示系統の迅速化（ダイレクトリーチ
③外部に対して信頼性のある窓口先の提供
④外部からの情報の一元管理の実現
⑤インシデントレスポンスに必要な情報量の向上
⑥想定外（予想外）のインシデントへの柔軟な対応

組織内 CSIRT の機能

- 組織内 CSIRT の内部に対する側面
  - 組織内で発生したインシデントを報告するための、一本化された窓口を提供する
  - 発生したインシデントに対応する、或いはその対応に必要な技術的支援及びノウハウを提供する
  - インシデント対応に必要な、組織としての意思決定を支援する
  - 部署間で発生するインシデントの調整役として活動する
  - 組織内の業務システムのユーザに対するセキュリティ意識を啓発する
- 組織内 CSIRT の外部に対する側面
  - 外部のインシデント対応組織との連絡調整をする
  - 最近のインシデント動向及びインシデント対応手法・技術に関する情報を外部から収集し、必要なところに提供する
  - 従業員・報道・国民へ適切な情報を提供する

組織内 CSIRT の活動設定のポイント 1

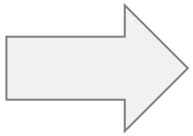
- 次のような求められる役割が示された場合

> 組織内において、発生した インシデント に対して、
> 適切な対応 活動を実施し、速やかな復旧の支援をする。

- 考察すべきポイント 1
  - この組織における「インシデント」の定義
    - これまで発生したインシデントの把握及び傾向分析
    - 同業他社で発生しているインシデントの把握及び発生可能性
    - 予測されるインシデント発生場所の把握及び傾向分析
    - 経営層及び現場の社員が認識しているインシデントの把握及び傾向分析
    - 可能であれば、インシデントの分類を検討

定義の策定

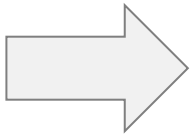
コストとプロフィットの見える化



「インシデント」が定義されることによって、組織内 CSIRT の活動の基本方針が決まる。極めて重要な定義である。

組織内 CSIRT の活動設定のポイント 2

- 考察すべきポイント 2
  - 「適切な対応」をする手段及び事前準備の定義
    - インシデント対応をする前に、発生したインシデントがきちんと報告されるかどうかの確認
      - サービス対象へのインシデント報告窓口の周知徹底を事前に行う
    - 組織内でのみ対応ができないものがあるかどうかの把握と検討
      - 組織内のみでできない場合は、事前に外部の連携について検討する
    - 経営層及びサービス対象が、どのような「適切な対応」を期待しているのか把握及び検討する
    - インシデントが発生した際、「直ちに排除する」か「範囲を特定する」かの判断ができるように、組織のリスク許容度を評価する



「適切な対応」の活動リストと、それらを実現するため、事前にしておかなければならない活動のリストも得られる。

(参考)CERT/CC におけるサービスの分類の例

事後対応型サービス	事前対応型サービス	セキュリティ品質管理サービス
・アラートと警告 ・インシデントハンドリング - インシデント分析 - オンサイトでのインシデント対応 - インシデント対応支援 - インシデント対応調整 ・脆弱性ハンドリング - 脆弱性分析 - 脆弱性対応 - 脆弱性対応調整 ・アーティファクトハンドリング - アーティファクト分析 - アーティファクト対応 - アーティファクト対応調整	・告知 ・技術動向監視 ・セキュリティ監査または審査 ・セキュリティツール、 アプリケーション、インフラ、 およびサービスの設定と保守 ・セキュリティツールの開発 ・侵入検知サービス ・セキュリティ関連情報の提供	・リスク分析 ・ビジネス継続性と障害回復計画 ・セキュリティコンサルティング ・意識向上 ・教育 / トレーニング ・製品の評価または認定

（参考） 組織内 CSIRT の活動の分類について

- 組織内 CSIRT 活動は、以下のように分類できる
  - 事後対応型の活動
    - Reactive Service
    - 各インシデント報告や不正検知システムなどからの情報による活動
    - CSIRT の基本的な活動
  - 事前対応型の活動
    - Proactive Service
    - 事前にソフトウェアなどの脆弱性、脅威情報、攻撃予測情報などを提供する活動
    - 直接的にインシデント発生の抑制を図る
  - セキュリティ品質マネージメントに関する活動
    - セキュリティコンサルタント、教育など
    - 他のセキュリティ会社がすでに提供済みだが、CSIRT としての視点や専門知識での見識を提供できる。
    - 間接的にインシデント発生の抑制を図る

CSIRT構築フレームワーク

組織内 CSIRT の活動のフレームワーク

- 組織内 CSIRT の活動のフレームワークを整えるためには、以下の基本骨子を確実に定義しなければならない
  - ミッションステートメント
    - 大局的な目標、目的 – 何を果たすべきなのか
  - サービス対象（Constituency）
    - 誰のために活動するのか
    - サービス対象と、どのような関係なのか
    - サービス対象から、どのくらい認識されているのか
    - サービス対象との信頼関係
  - 組織内の 位置づけ
    - 組織内における CSIRT の位置
    - 組織内における CSIRT の役割
    - 各部署との相互関係
  - 他のチームとの関係
    - 他の CSIRT との協力及び連携

組織内 CSIRT の活動のフレームワーク
「ミッションステートメント」の定義方法

- 組織から求められる役割（インシデント対応など）を明確にする

- 組織内 CSIRT に対する期待として多く見られるものは以下のとおり
  - 組織内に「インシデント対応能力をつける」こと
    - 組織内においてインシデントに対応する部門や人が決まっていないため、インシデントに**「直接」対応**するチームを設けたいという期待
  - 「組織的なインシデント対応能力」を向上させること
    - 特定の部門でインシデント対応するところはあるが、必ずしも組織全体としてのインシデント対応に結びついていないため、部門によるインシデント**対応を「支援」**しながら、組織全体としての統制をとるチーム設けたいという期待
  - 「外的要因のインシデント」への対応能力をつけること
    - DoS 攻撃や Phishing 詐欺のような外部要因のインシデントに対応する部門が決まっていないため、外部及び内部の部門と**「調整して」対応**する部門を設けたいという期待

組織内 CSIRT の活動のフレームワーク
「サービス対象」の定義方法

- 組織内 CSIRT がどの範囲を対象として活動するかを設定する
  - 「組織内 CSIRT が提供するサービスの対象範囲を設定する」と言い換えることができる
- 組織内 CSIRT がサービス対象に対してどの程度の権限を持つのか設定する
  - 強制的な権限があるのか、ないのか？
- サービス対象者に対して、組織内 CSIRT が何をするのかを周知する
  - インシデントの報告先として認知してもらう
- サービス対象者から信頼を得る
  - 信頼がなければ、インシデントは報告されない

組織内 CSIRT の活動のフレームワーク
「組織内の位置づけ」の定義方法

- 組織内 CSIRT が組織におけるリスク管理全体において求められている役割を明確にする
  - 主に、情報セキュリティ基盤に起因するリスクを管理する役割が多い
- 組織内に既に他のインシデント対応チームが存在している場合は、それぞれのミッションステートメント及びサービス対象の定義の区別を明確にする
- 組織における組織内 CSIRT の責任を明確にする

組織内 CSIRT の活動のフレームワーク
「他のチームとの関係」の定義方法

- 組織内 CSIRT が他の（外部の） CSIRT との調整及び連携するという役割を明確する
- 他の CSIRT が何ができ、どんな調整及び連携ができるのかを把握する
  - 逆に、みずからできることを、他の CSIRT に伝えることも重要である
- 他の CSIRT との連携に必要なことを定義する
  - 他の CSIRT に対する対応依頼は、自発的で非公式な場合が多いため、信頼関係の構築が必要となる

他組織との連携

- 情報共有の枠組み
  - 信頼に基づく組織間において、セキュリティに関連する情報の共有を行う事で、全体的なセキュリティ対策の向上に繋げる
- FIRST(Forum of Incident Response and Security Teams)
  - インシデント対応チーム 289組織(2014/05/12現在)で構成される国際的なフォーラム
- 日本シーサート協議会
  - 情報共有などのCSIRT間の緊密な連携体制の実現と、CSIRTが共通して抱える課題の解決を目指す協議会

FIRST http://www.first.org/

日本シーサート協議会 http://www.nca.gr.jp/

（参考）組織内 CSIRT の構築に役立つ資料

- JPCERT/CC　における関連文書
  - 組織内 CSIRT 構築支援マテリアル
    - https://www.jpcert.or.jp/csirt_material/
  - コンピュータセキュリティインシデント対応チーム（CSIRT）のためのハンドブック
    - https://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf

- その他の参考資料
  - CERT/CC – “Creating a Computer Security Incident Response Team: A Process for Getting Started”
    - http://www.cert.org/csirts/Creating-A-CSIRT.html
  - TERENA – “CSIRT Starter Kit”
    - http://www.cert.org/csirts/Creating-A-CSIRT.html
  - AusCERT – “Forming an Incident Response Team”
    - http://www.auscert.org.au/render.html?it=2252
  - RFC 2350 – “Expectations for Computer Security Incident Response”
    - http://www.ietf.org/rfc/rfc2350.txt

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：office@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form