応：～インシデントに対応する（発見と調整）～

# インシデントレスポンス概論

JPCERTコーディネーションセンター
細野　英朋
office@jpcert.or.jp

# 本講演の流れ

1. インシデントレスポンス
   - インシデントとは? インシデントレスポンスとは?
   - インシデントレスポンスはなぜ必要か?
2. インシデント対応手順
   - インシデントレスポンスに必要なもの、対応手順
3. CSIRT
   - CSIRTとは?

Appendix:
   - 1. CSIRTとJPCERT/CCのあゆみ
   - 2. 参考資料など

# 1. インシデントレスポンス

# インシデントとは

## コンピュータセキュリティ・インシデントとは

**コンピュータセキュリティに関係する人為的事象で**
**意図的および偶発的なもの（その疑いがある場合）**

「インシデント」は「不正アクセス」と違い世界的に広く使われている用語
– RFC（Request For Comments）でも用いられている

# インシデントの分類（一例）

- スキャン
  - 脆弱なアカウントの探索、侵入未遂など
- システムへの侵入
- DoS（Denial Of Service）
  - サーバプログラムの停止、再起動
- **Web偽装詐欺（phishing）**
  - 銀行などのサイトを装ったページをつくり、個人情報を盗む
- インシデントではないもの
  - いわゆるspamメールの配信、ワンクリック詐欺など

# インシデント発生時最大の問題

- 最大の問題は?
  - インシデントの発生に気が付かず、放置
  - その結果、踏み台に…

…踏み台にならないようにするためには

いかにインシデントの発生に
**すばやく気付く**か
いかに**適切に連絡・調整を行なう**か

が重要

# インシデントレスポンスとは

「インシデントは起こる」
という前提に基づきインシデントの拡大を
防ぐための

**事後の対応**

「事後の対応」を検討および確認するための
「**事前の対応**」も含まれる

# インシデントレスポンスの必要性

守るだけがセキュリティではない

人間が扱うものに「完璧」はない!

例えば…

ミスや制御不可能な事由

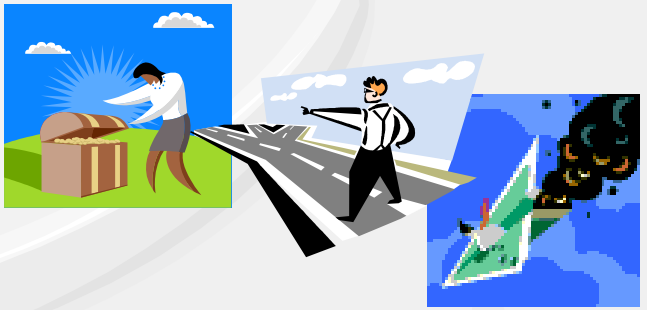
- 修正プログラムの適用忘れ
- 設定更新時の作業漏れ
- 未知の脆弱性を突かれる
- 修正プログラムの提供が間に合わない

など

# まず、ポリシーの策定

あなたの組織にとっての「インシデント」とは?

- 守るべきもの
- 優先すべきもの
- 想定されるダメージ…



システム設計時に考慮・整理しておく項目

- 提供するサービス
- アクセス制御・認証
- 保守・管理体制

# インシデント発見・対応手順の明確化

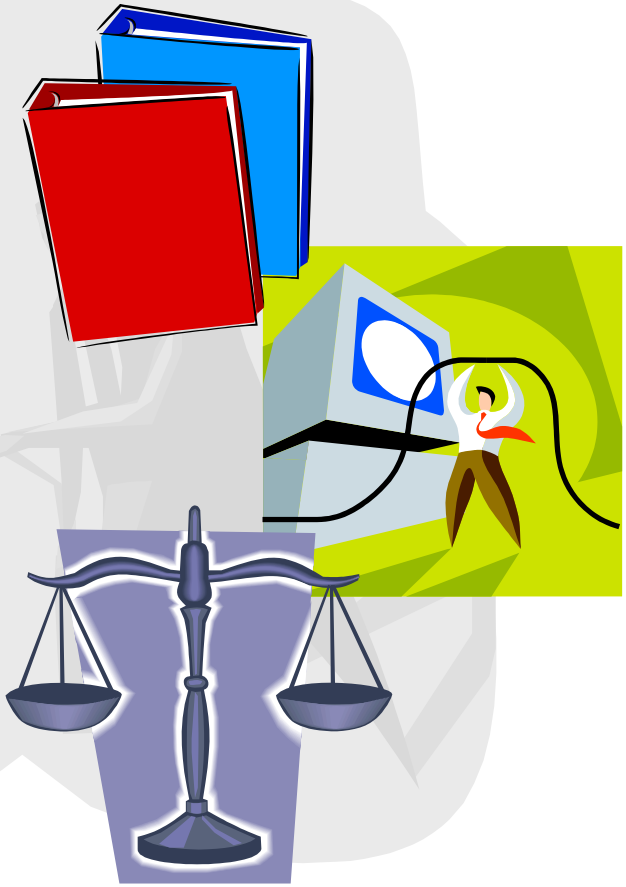
事前に明確にしておくべき項目の一例

- ログの取得内容、確認手順
- 不審なプロセスや通信、改ざんの検知
- 異常事態発生時の報告の仕組み
- whois情報などの公開連絡先
  - 公開連絡先を通して
    インシデント通知連絡を受けることもある
    - 不要なメールも届くことを覚悟する

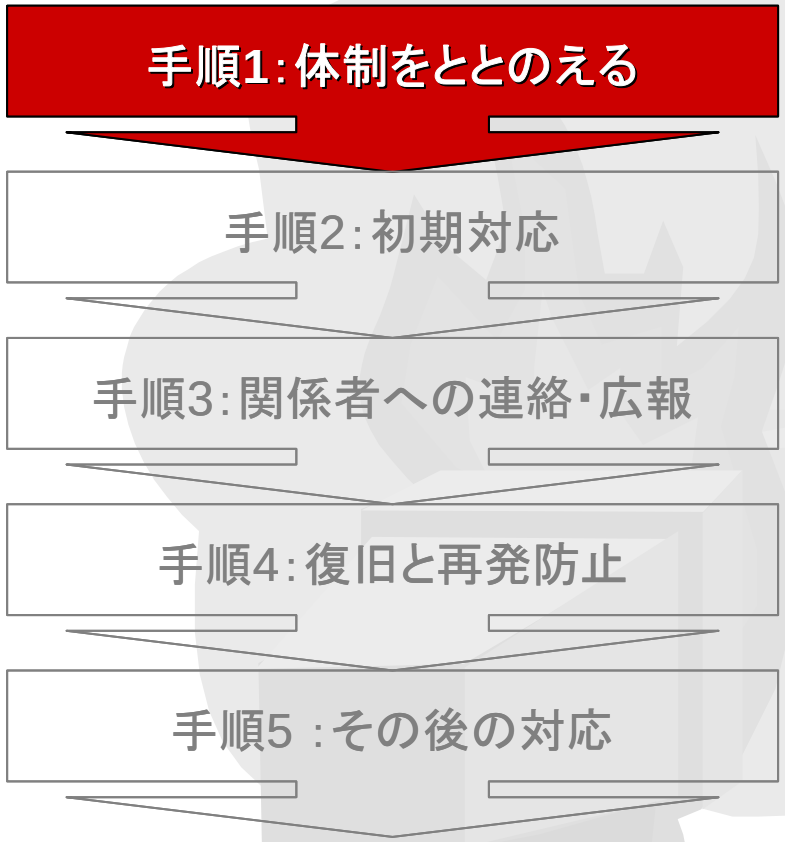
# 2. インシデント対応手順

# インシデントレスポンスに必要なもの

- 組織の体制
  - 対応手順
  - 予行演習
  - 専門のチーム（CSIRT）
- スタッフの資質
  - 知識・技術
  - 想定外の事態への対応能力
    - 柔軟性、冷静さ…
  - モラル

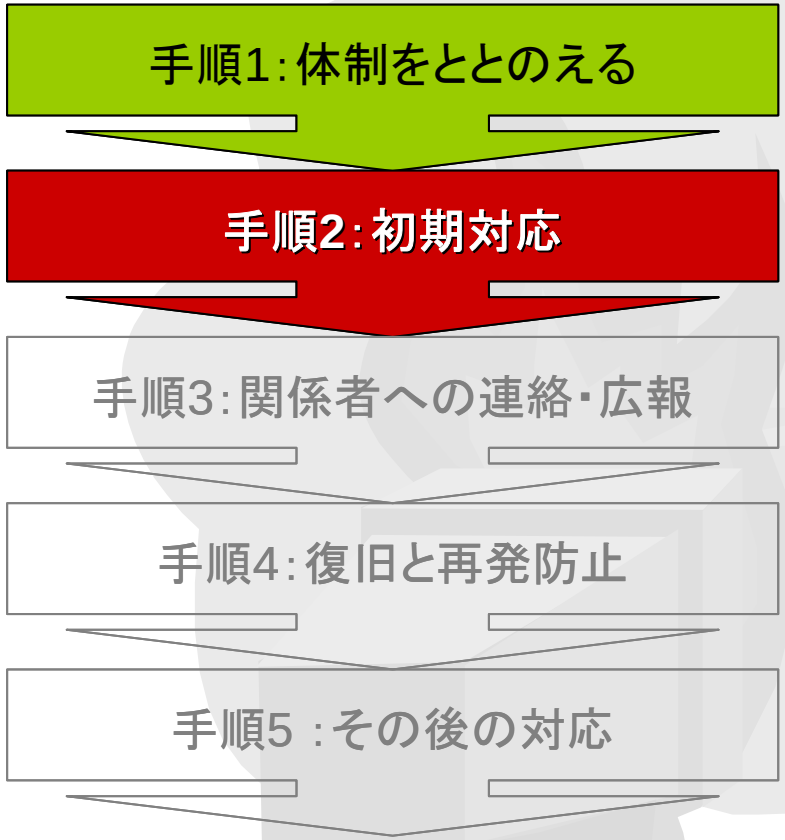


# 手順1:体制をととのえる



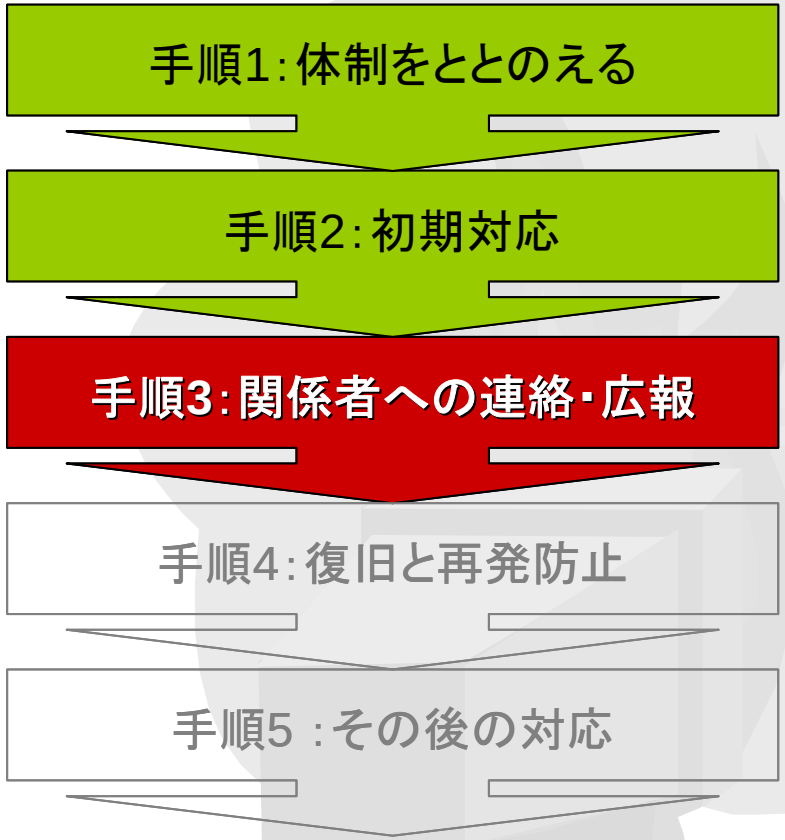

- インシデントが発生した? と思ったら
  - まずは深呼吸
    (冷静になりましょう)
  - 手順の確認
    - セキュリティポリシー
    - 作業マニュアル
  - 作業記録の作成
    - 対応時刻・対応者・対応内容を簡潔に
  - 責任者、担当者への連絡
    - 連絡体制の整備
    - インシデント対応の担当者への連絡

# 手順2：初期対応



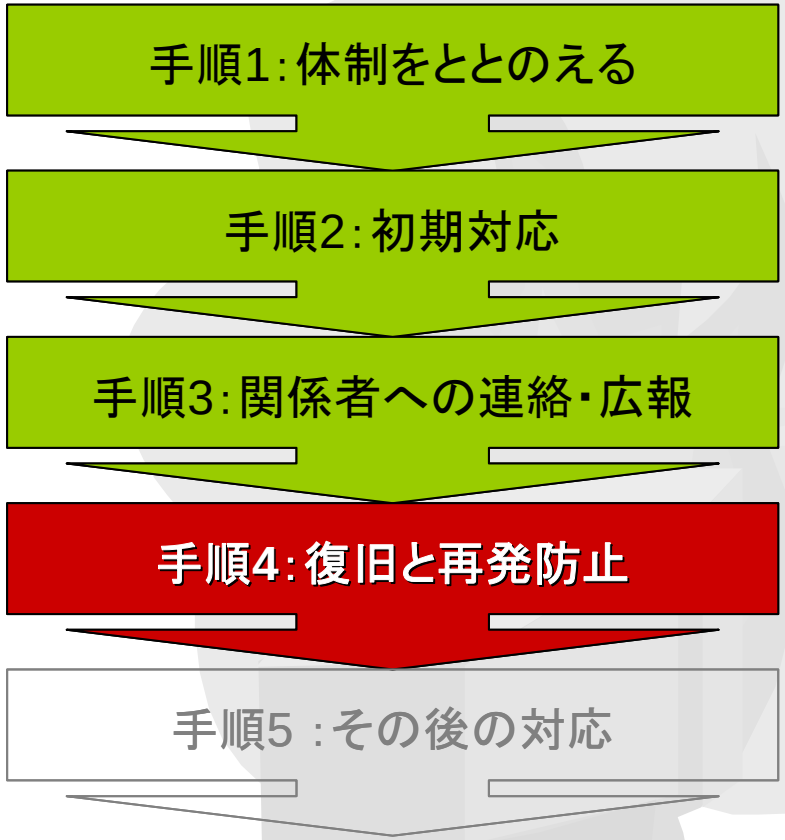

- 事実の確認
  - 本当にインシデントなのか？
    （正当なアクセスもある）
- ログなどの保全
  - 調査や分析、
    連絡などに必要
  - 提出を求められることもある
- ネットワーク接続や
  システムの遮断・停止

# 手順3:関係者への連絡・広報



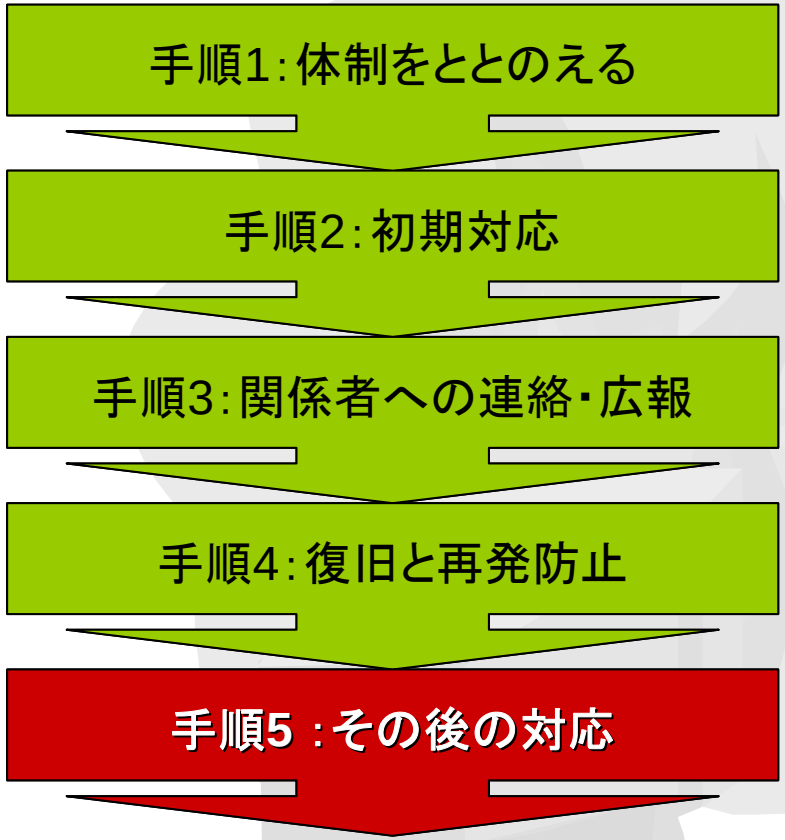

- 影響範囲の特定
- 関係サイトへの
  連絡、謝罪、情報提供
- インシデントの事実の公表
  - 公表の是非を含めて検討
  - 公表する範囲に注意
- アクセス元などへの通知連絡
  - JPCERT/CC経由でも可能

# 手順4：復旧と再発防止




- 要因の特定
  - 脆弱性？ 運用体制？
    あるいは複数の要因？
- システムの復旧
  - バックアップメディアからの復旧
- 再発防止策の検討、実施

# 手順5:その後の対応




- 作業結果の報告と
  作業の評価
  ↑ ↑ 忘れずに!
- ポリシー、
  運用・監視体制、
  運用手順の見直し
  - 上位部署や
    トップも巻き込む
- JPCERT/CCなどへ報告

# 3. CSIRT

# CSIRTとは

## ➢コンピュータセキュリティ・インシデントに対応する組織体

- 報告を受け取る
- 調査する
- 対応活動を行う・他

すべてのCSIRTがすべてを行うわけではない

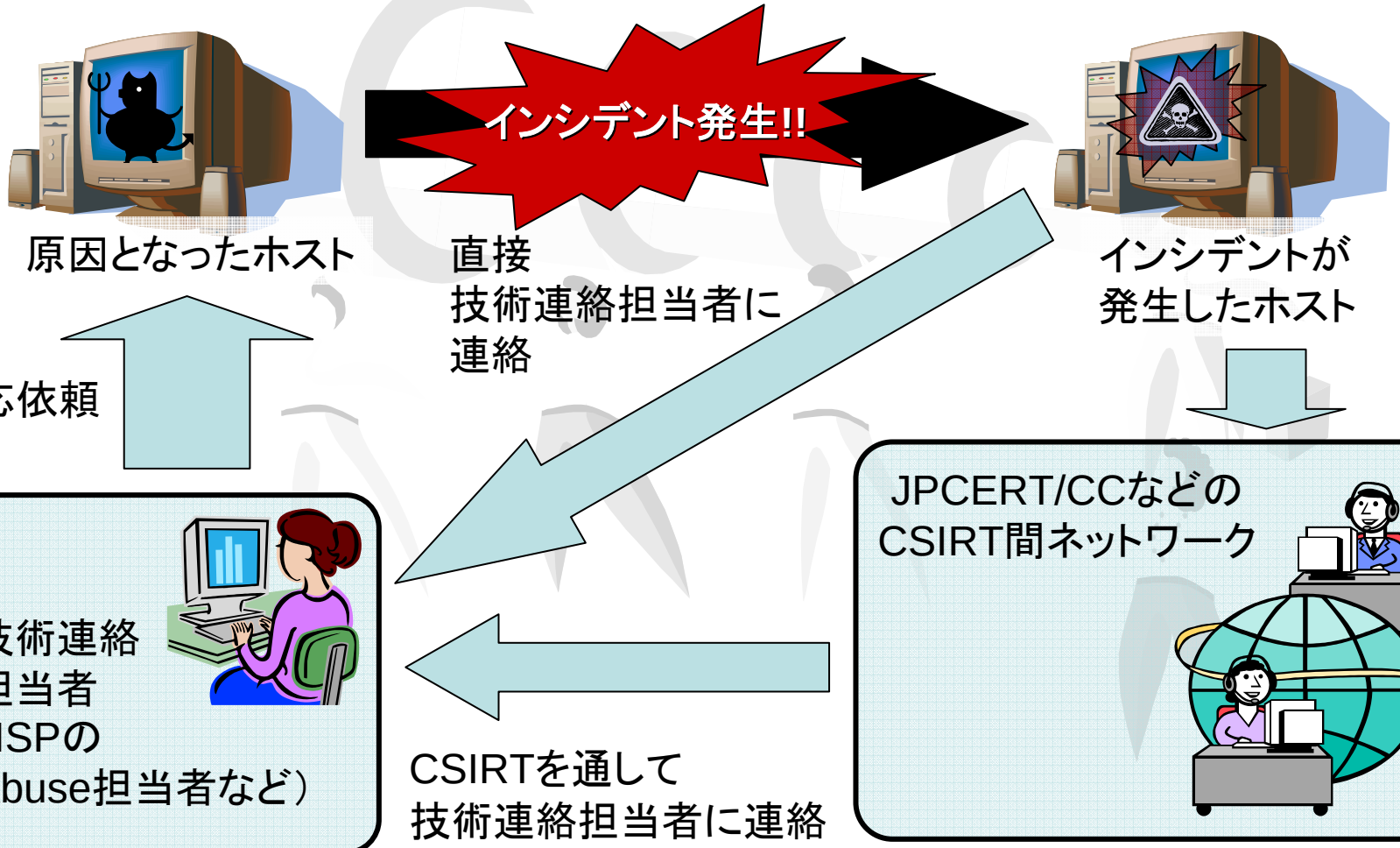
※一般名詞は「CSIRT」（Computer Security Incident Responce Team）
単語「CERT」（Computer Emergency Response Team）は米国CERT/CCの登録商標

# CSIRTの分類

**constituency（サービス対象）によって分類**

- **Internal CSIRTs**
  - 自組織や顧客が関わるインシデントに対応
- **National CSIRTs**
  - 国・地域のコンタクトポイント
- **Coordination Centers**
- **Analysis Centers**
- **Vendor Teams**
  - 自社製品の脆弱性について対応
- **Incident Response Providers**
  - いわゆる「セキュリティベンダ」

# CSIRTと連絡スキームの関係



# 他のCSIRTやxSPとの連携

- **速やかで効率的、効果的な通知、連絡　が可能**

- xSPや別のCSIRTがより適切な通知連絡先を知っている場合がある
- xSPの顧客対応窓口はもっとも「ユーザ」に近いところにいるCSIRT
  のひとつ
  - 技術的なアドバイス、非技術的なアドバイス
    （何をすべきか、何をしてもいいか、何をしてはいけないか、など）
  - （お勧めはしませんが）
    約款などを根拠にサービスを停止できる

# 情報の収集と流通

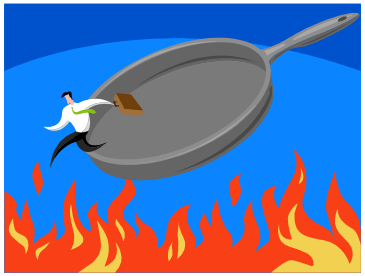
## 情報収集と流通もCSIRTの大切な業務

活動例

- 脆弱性情報流通
  - さまざまなCSIRTが脆弱性情報（有料・無料）を発信
    →比較・検討のうえ活用
- インシデント傾向の把握
  - さまざまなCSIRTが公開する注意喚起、定点観測のデータを活用
- 啓発活動
  - 講演の聴講、カンファレンスやワークショップへの参加
  - 自身のconstituencyへ知識・技術などをフィードバック

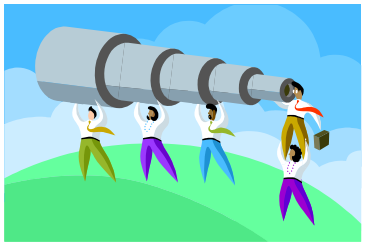
# まとめ

- インシデントは**いつかは起こる**
  - 事後対応と、そのための事前対応が不可欠



- インシデントレスポンスに必要なもの
  - 体制
    （対応手順の整備、予行演習、CSIRT）
  - 資質（知識・技術、柔軟性、冷静さ、モラル）

- インシデントレスポンスでのCSIRTの重要性
  - CSIRT間の**連携**によって
    速やかで効率的、効果的な通知、連絡が可能
  - 普段からの**情報収集と流通**もCSIRTの大切な業務



# Appendix 1.
# CSIRTとJPCERT/CCのあゆみ

# CSIRT・JPCERT/CC関連年表

1988 1990 1992 1994 1996 1998 2000 2002 2004 2006

JPCERT活動
1992頃～1996

JPCERT/CC第一期
（任意団体時代）
1996～2003

JPCERT/CC
（中間法人化）
2003～

▲Morris Worm事件（1988）
▲米国CERT/CC設立（1988）
▲FIRST発足（1990）

▲JPCERT/CC
FIRST加盟（1998）

▲JPCERT/CC
定点観測事業開始（2003）

▲JPCERT/CC
脆弱性情報流通開始（2004）

▲FIRST加盟CSIRT
170チームを突破（2005）

商用インターネット 1995頃～

# Appendix 2. 参考資料

# 参考URL（JPCERT/CC発行）

- 技術メモ

  http://www.jpcert.or.jp/ed/

  - コンピュータセキュリティインシデントへの対応

    http://www.jpcert.or.jp/ed/2002/ed020002.txt

- 管理者のためのセキュリティ推進室
  インシデントレスポンス入門

  http://www.jpcert.or.jp/magazine/atmarkit/
  （@IT連載記事）

# 参考URL（他組織発行）

- インシデントの分類
  米国Sandia National Laboratoriesの報告書
  “A Common Language for Computer Security Incidents”
  http://www.cert.org/research/taxonomy_988667.pdf
- CSIRTの分類
  http://www.cert.org/csirts/csirt_faq.html
- RFC2350
  “Expectations for Computer Security Incident Response”
  http://www.ietf.org/rfc/rfc2350.txt（原文）
  http://www.ipa.go.jp/security/rfc/RFC2350JA.html
  （IPAによる日本語訳）
- FIRST（Forum of Incident Response and Security Teams）
  http://www.first.org/
  メンバー一覧
  http://www.first.org/about/organization/teams/

# 参考文献(書籍)

- Kevin Mandia・Chris Prosise

『インシデントレスポンス』

訳　:エクストランス

監修:坂井順行・新井悠

翔泳社

ISBN4-7981-0295-4

# JPCERT/CCへのアクセス

- Web
  http://www.jpcert.or.jp/
- メーリングリスト
  http://www.jpcert.or.jp/announce.html
- インシデント報告
  - E-mail
    info@jpcert.or.jp
    PGP：BA F4 D9 FA B8 FB F0 73  57 EE 3C 2B 13 F0 48 B8
  - 報告様式
    http://www.jpcert.or.jp/form/（インシデント報告の際はお使いください）
  - インシデント報告専用ファックス
    03-3518-2177（電話ではインシデント報告を受け付けておりません）

# Thank you