JPCERT CC®

組織内 CSIRT の重要性

2007.2.14（水）

JPCERT コーディネーションセンター
経営企画室　業務統括　伊藤　友里恵

目次

- JPCERT コーディネーションセンターについて
- 最近のセキュリティ動向について
- 求められる対策について
- CSIRT という概念
  - 情報セキュリティのガバナンスとして
  - 統一された窓口として

JPCERT コーディネーションセンターについて

JPCERT コーディネーションセンターについて

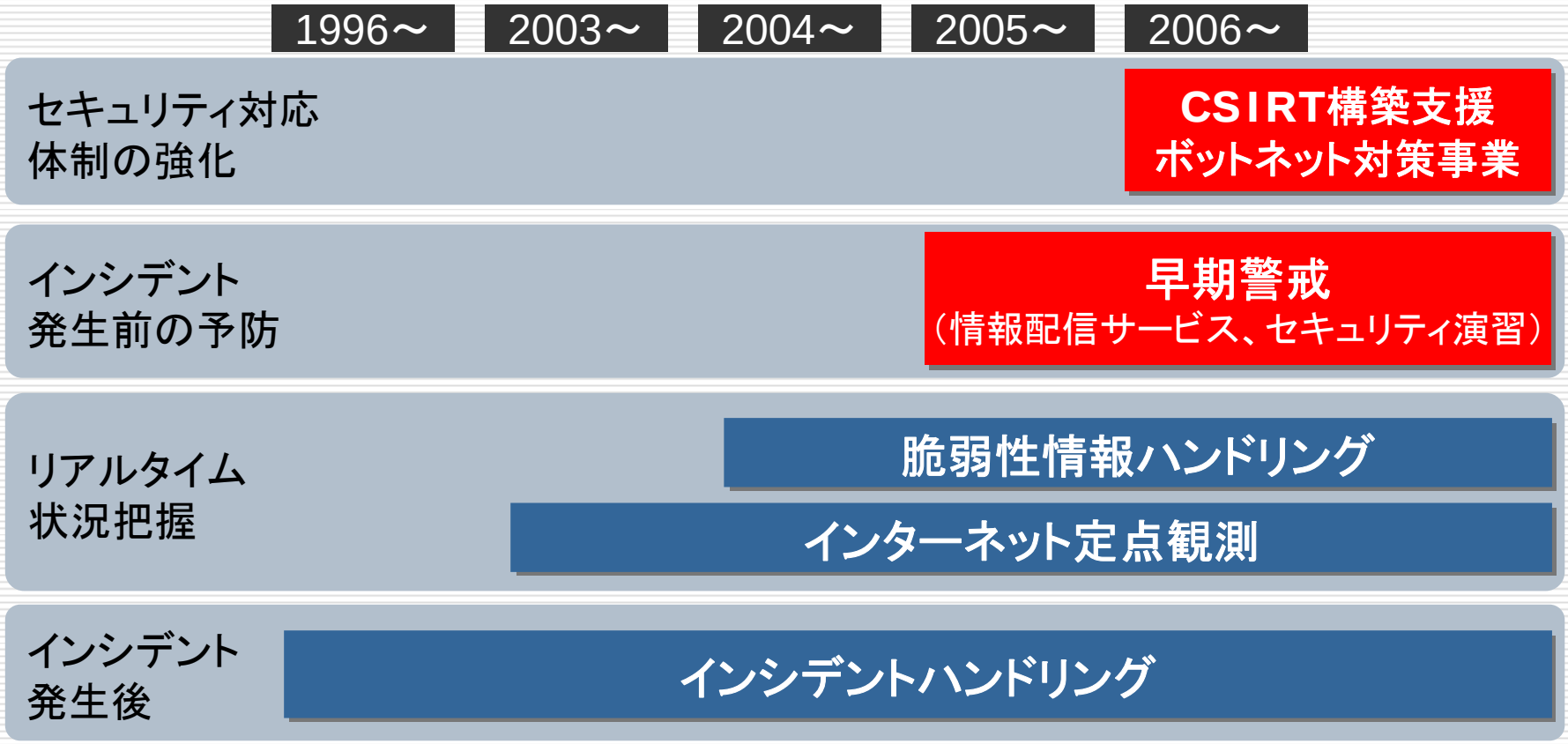
- **JPCERT/CC**
  - **Japan Computer Emergency Response Team Coordination Center**
  - ジェーピーサート・コーディネーションセンター
    - コンピュータセキュリティインシデントに関する調整、連携などの活動を行っている
    - 緊急事態 (Emergency) への対応 (Response)

JPCERT コーディネーションセンター(**JPCERT/CC**) は、国境を越えて広がるセキュリティインシデントに対するため、我が国の窓口となる CSIRT (**Computer Security Incident Response Team**) として、**インシデントレスポンスや脆弱性情報に係る国際コーディネーション**、情報セキュリティインシデントの予防・対策・対処の支援、ネットワークモニタリングを行い、我が国の組織内 **CSIRT** の活動を支援しています。

JPCERT コーディネーションセンターについて
JPCERT/CC の沿革

1992年	ボランティアベースの活動開始 コンピュータセキュリティインシデント報告対応業務開始
1996年10月	「コンピュータ緊急対応センター」として発足
1998年8月	CSIRTとして日本で最初に **FIRST** に加盟 -日本のPOC(窓口)CSIRTとして国際的に認知
2003年2月	**APCERT(アジア太平洋コンピュータ緊急対応チーム)**フォーラム発足
2003年3月	有限責任中間法人としての法人格を取得
2003年12月	**インターネット定点観測システム(ISDAS)** 公開
2004年7月	経済産業省告示にて「**脆弱性情報流通調整機関**」として指定
2005年8月	FIRST運営委員および理事就任
2006年10月	JPCERT/CC 創立10周年

JPCERT コーディネーションセンターについて
JPCERT/CC の活動内容



最近のセキュリティ動向について

近日のサイバーインシデントトピック

- 非常に多数の脆弱性が発見、報告される
  - – 2006'の報告数8,046 (CMU－CERT/CC統計情報)
- 悪意のあるソフトウェアによって引き起こされるインシデントの増加
- ボットネットの問題はよりいっそう深刻に
- AP地域間の経済地域間における攻撃
- オンライン・サイバー犯罪
- ソーシャルエンジニアリング手法の高度化
- ターゲット攻撃
- ゼロデイ攻撃
- クライアントアプリケーションを対象とした攻撃
  - オフィスクライアントアプリケーションが攻撃対象に
- DNSサーバーのようなインターネットインフラ自体への攻撃
- 制御、コントロールシステム (SCADA) への注目
- 初歩的な攻撃手法も引き続き発生—辞書攻撃、パスワード攻撃
- P2Pファイル共有ソフトネットワークにおける情報漏えいは引き続き深刻

最近のセキュリティ動向について(1)

- 経済的な利益を目的とする攻撃が組織化・高度化
  - 価値のある情報資産(情報そのもの、機器等のリソース)を狙い撃ちにする攻撃(ターゲテッド・アタック)
  - 攻撃対象数は限られているが被害は甚大
  - 多目的に利用できるように構築されたボットネットワークを利用する。経済的な利益を得ようとする者に対して攻撃ツールを提供すること自体がビジネス

最近のセキュリティ動向について(2)

- 脅威の潜在化
  - 攻撃・被害が認識されにくい方法を用いて行われている(潜行化、プロ化)傾向
    - 例:ソーシャルエンジニアリングを使ったメール添付型 Exploit コード
      - Exploit コードにプログラムされたウェブサイトにアクセスさせる。
      - ウェブサービスを使う、通信の暗号化、ルートキットなど
- 攻撃手法の巧妙化と攻撃の迅速化
  - 脆弱性の悪用
  - ゼロディアタック

最近のセキュリティ動向について(3)

- 原因追求の困難化
  - システムに特化した仕組みの理解
  - 最新のセキュリティ関連情報の把握の必要性
- 企業情報窃取
  - 特許、市場戦略、プロセス、デザイン、開発啓発…
  - 産業スパイ

求められる対策について

求められる対策について

- 組織内におけるセキュリティ情報の統制
  - 各部署／各事業部のセキュリティ情報の収集・共有
  - 外注先（SIer等）とのセキュリティ情報共有の一元化
  - 部署／事業部をまたいだインシデント対応（調整）
  - 経営層に対する一元化した報告及び指示受けの体制、権限委譲の明文化
- 対外窓口の一本化
  - 外部からのインシデント受付する「信頼ある」窓口の設置
  - 情報提供としての窓口として
- 現実的な対応体制の構築
  - 発生したインシデントによる「被害の極限化と迅速な復旧」の活動が有効に働くための必要条件の整備

CSIRT という概念について

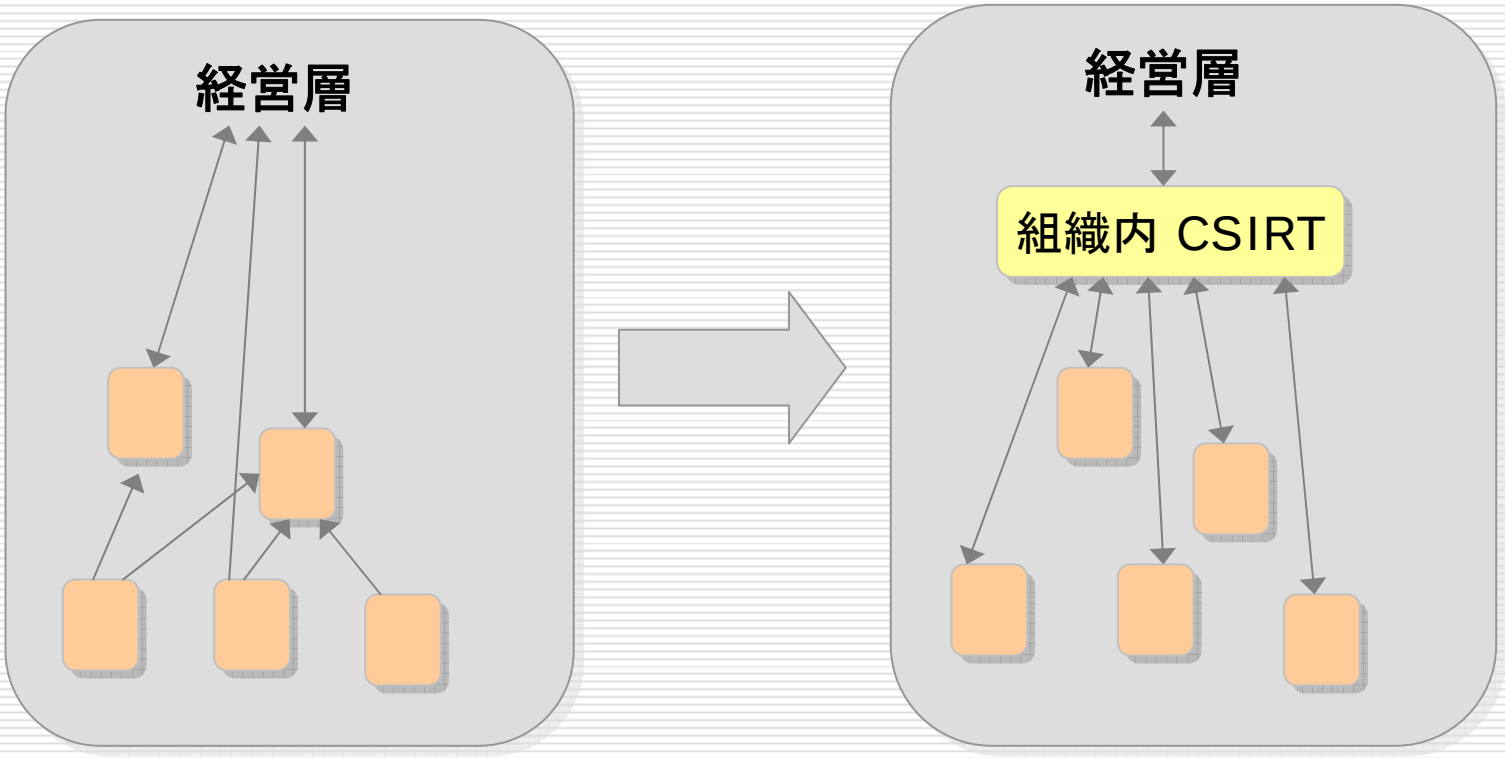
CSIRT という概念について

- Computer Security Incident Response Team
  - コンピュータセキュリティインシデントに関わる（インシデント対応，分析，教育や監査，研究開発など）活動を行っている組織

- インシデント対応のフレームワークの基礎
  - 汎用技術の導入に伴い、それにかかるインシデント対応は連携した対応が必要となる。

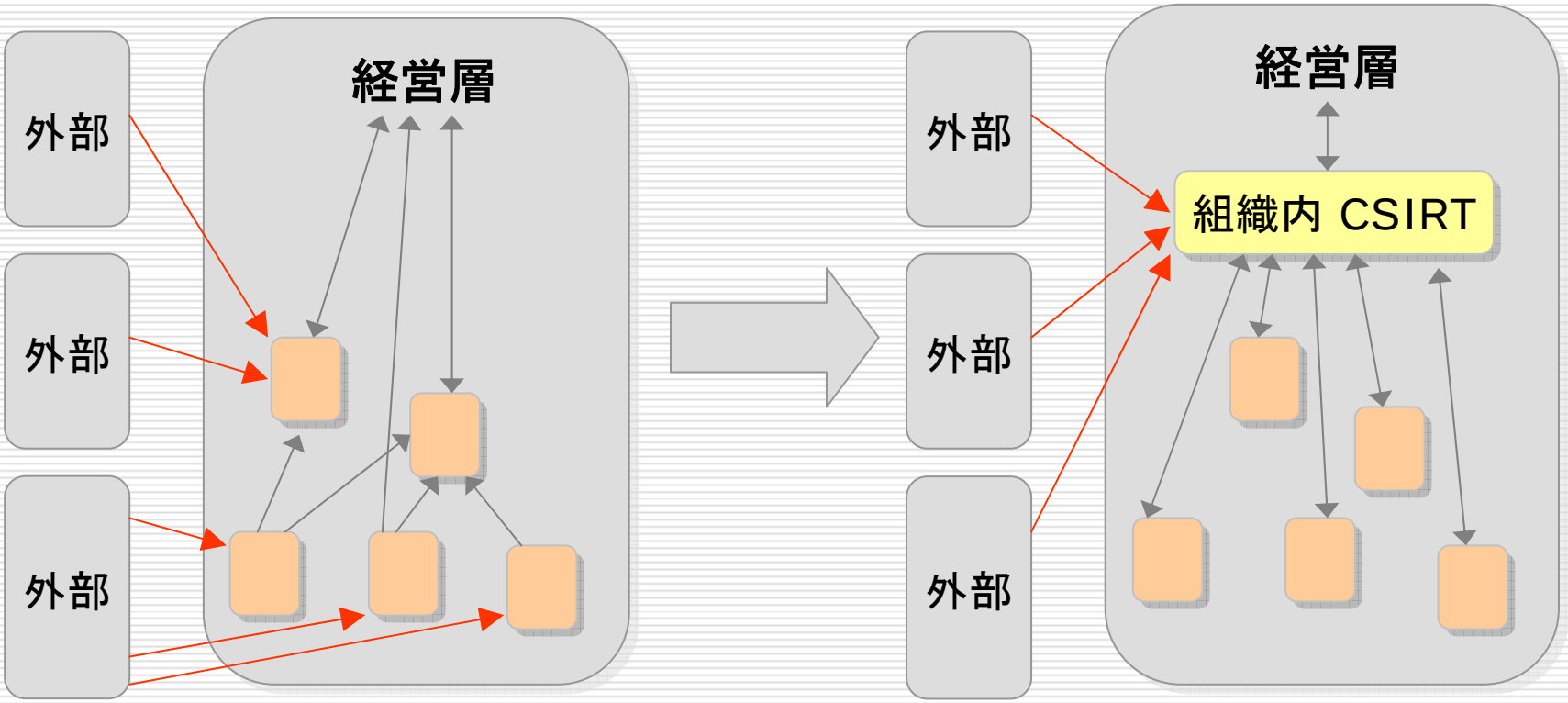
- インシデントの防止および沈静化、復旧の支援、再発防止のための活動
  - 情報セキュリティにかかるインシデントは、他のインシデントと異なり、専門的な知識、経験そして最新動向（対策を含めて）などを把握する必要がある。

CSIRT という概念について
情報セキュリティのガバナンスとして



メリット：①社内セキュリティ情報共有及び集中管理の実現
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）

CSIRT という概念について
統一された窓口として



メリット：①外部に対する信頼性のある窓口先の提供
②外部からの情報の一元管理の実現

CSIRTの重要な役割 (1)

- 攻撃は、ますます検知が困難に
  - 新種が数多く発生するマルウェアにAVソフトのパターンファイルが追いつかない状況
  - 悪意のある通信や行為を、暗号化したり、見えなくさせる攻撃手法
- インシデント情報は、共有しにくい傾向
- 企業におけるサイバー攻撃、インシデント情報はほとんど報告されない
  - 企業のセキュリティポリシーなど
- **何が起きているか分からなくなる状況が非常に危険**
- 重要な CSIRT 役割;
  - インシデント情報を収集、分析し、匿名化できるような形で、必要な関係者で共有できるようにする。
  - 同じ手法の攻撃があった場合、次はより効果的なインシデント対応ができるようになる。
  - 再発防止

CSIRTの連携枠組み

- FIRST
  - Forum of the Incident Response Security Teams
  - http://www.first.org
  - 世界各国から200チーム以上のCSIRTがメンバーとして参加
  - インシデント対応、脅威情報対応を目的として、またベストプラクティスの共有といった情報共有を行う。
- APCERT
  - Asia Pacific Computer Emergency Response Teams
  - http://www.apcert.org
  - アジア環太平洋地域 15カ国から、計18チームがメンバー
  - インシデント対応、脅威情報対応を目的として、またベストプラクティスの共有といった情報共有を行う。
- 日本において
  - CSIRT間の連携枠組みを構想中

CSIRTの重要な役割 (2)

- Know Your System!!!

- 組織内のシステムについて把握すること
  - 脅威度の把握
  - 対策の必要性、優先順位