CSIRTについて

～Computer Security Incident Response Team～

2006年3月3日（金）

JPCERT コーディネーションセンター

名和 利男

Copyright© 2006 JPCERT/CC
All rights reserved.

アジェンダ

1. CSIRTの発足
2. CSIRTとは
3. CSIRTのサービス対象
4. CSIRTのサービス
5. CSIRTの組織モデル
6. JPCERT/CCについて

Copyright© 2006 JPCERT/CC
All rights reserved.

1. CSIRTの発足

Copyright© 2006 JPCERT/CC
All rights reserved.

1988年11月

		1	2	3	4	5
6	7	8	9			12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

ワーム攻撃
（モリスワーム）

Copyright© 2006 JPCERT/CC
All rights reserved.

モリスワーム発生！

- 1988年11月2日発生
- 米国の23歳の大学生が作成した不正プログラムで、さまざまな脆弱性を利用しながら、自発的に繁殖し、APPANET の上の60,000～80,000のホスト（全体の約10%）に影響が出た
- 多くのホストが通信線を抜いたので、インターネットの通信リレーが機能しなくなった

Copyright© 2006 JPCERT/CC
All rights reserved.

1988年11月

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

ワーム攻撃
（モリスワーム）

対策会議

Copyright© 2006 JPCERT/CC
All rights reserved.

モリスワーム対策会議にて

- 1988年11月8日開催
  - Defense Advanced Research Projects Agency（DARPA）により構成
- 不十分な協力体制
  - 研究機関やコンピューターセンターにおいて、それぞれ重複した分析作業をしていた
- 連絡体制の未整備
  - 多くのサイトが最新の有効な対策情報をタイムリーに入手することができなかった

コンピュータインシデントの分析／対処をハンドリングする（取扱う）正式な手段がなかったという問題点が明確になる

Copyright© 2006 JPCERT/CC
All rights reserved.

1988年11月

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

ワーム攻撃
（モリスワーム）

対策会議

CERT/CC発足

Copyright© 2006 JPCERT/CC
All rights reserved.

最初のCSIRT

- 1988年11月24日発足
- コンピュータ（**C**omputer）の緊急事態に（**E**mergency）を対応（**R**esponse）する組織（**T**eam）の構築へ
- 単独のCSIRTのみで、すべての業種や組織体に対して対応をとることは大変難しいため、1989年以降、各政府機関においても同様な組織（チーム）が構築されていくことに

Copyright© 2006 JPCERT/CC
All rights reserved.

2. CSIRTとは

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの基本的な役割
レスポンス（例）

消防署と消火活動

- 火事発生
- 消防署に火事情報を報告
- 現場に到着後、被害状況把握と火事の種類の見極め
- 消火行動の決心
- 火事の抑制と消火

CSIRTとインシデント報告

- コンピュータに関するインシデント発生
- CSIRTにインシデント情報を報告／連絡
- インシデントの把握と分析
- 被害抑制のための方策の決定
- 問題解決に向けた行動

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの基本的な役割
事前行動（例）

消防署の事前行動	CSIRTの事前行動
防火訓練	セキュリティ教育
避難訓練	セキュリティコンサルティング
火災検知器の設置	運用の維持管理
非難設備（はしご）の設置	技術文書やアドバイザリーの提供

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの一般的な目的と活動

目 的

- セキュリティインシデントなどによる被害を抑制し、損害を最小限にすること
- 適切なレスポンスと有効な対策を提供すること
- 将来発生するインシデントに対する予防をすること

活 動

- 担当する対象範囲内のインフラなどに関する以下の情報を収集する
  - インシデント情報
  - セキュリティーホール情報
  - ソフトウェア及びシステムの脆弱性情報
- 配下のセキュリティー対策組織間の情報共有と連絡調整
- 他のCSIRTとの連携による情報共有と連絡調整

Copyright© 2006 JPCERT/CC
All rights reserved.

3. CSIRTのサービス対象

Copyright© 2006 JPCERT/CC
All rights reserved.

サービス対象について

- サービス対象（Constituency）及びその関係の定義
- CSIRTをサービス対象に周知
- “doing the job right（仕事を適切にこなす）”により、サービス対象から信頼獲得

Copyright© 2006 JPCERT/CC
All rights reserved.

サービス対象について
ミッションステートメント

- ミッションは、所属している組織及びサービス対象者が期待するものに強く影響される

- 一般的なCSIRTのミッションは以下のとおり
  - 構成システムのセキュリティの保守と維持管理
  - インシデントレスポンス活動の統制及び調整
  - セキュリティインシデントによる被害の最小化
  - サービス対象者に対するセキュリティ関連の教育及び啓蒙と最善策(”best practice”)の提供

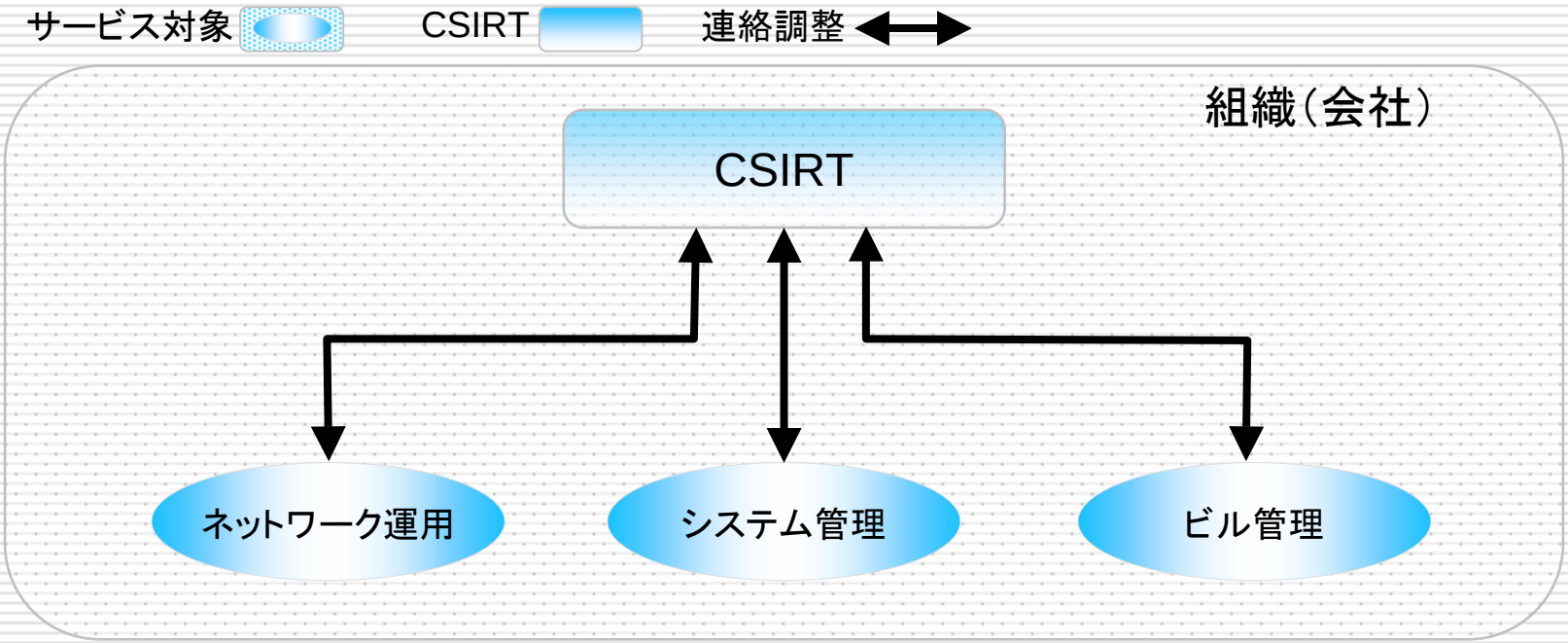
Copyright© 2006 JPCERT/CC
All rights reserved.

サービス対象について
ミッションの特徴とCSIRTのタイプ

CSIRTのタイプ	ミッションの特徴	サービス対象のタイプ
International Coordination Center	・他国のCSIRTと連携をすることにより、コンピュータセキュリティーのグローバルな観点でのナレッジベースを獲得できる。 ・CSIRT間での「信頼の輪」(web of trust)の構築	世界各国のCSIRT
Corporation	組織の情報基盤のセキュリティーを向上させ、侵入による被害の脅威を最小限にする。	システム管理者やネットワーク管理者、組織内のシステムユーザ
Technical	既存のIT製品のセキュリティ向上	製品ユーザ

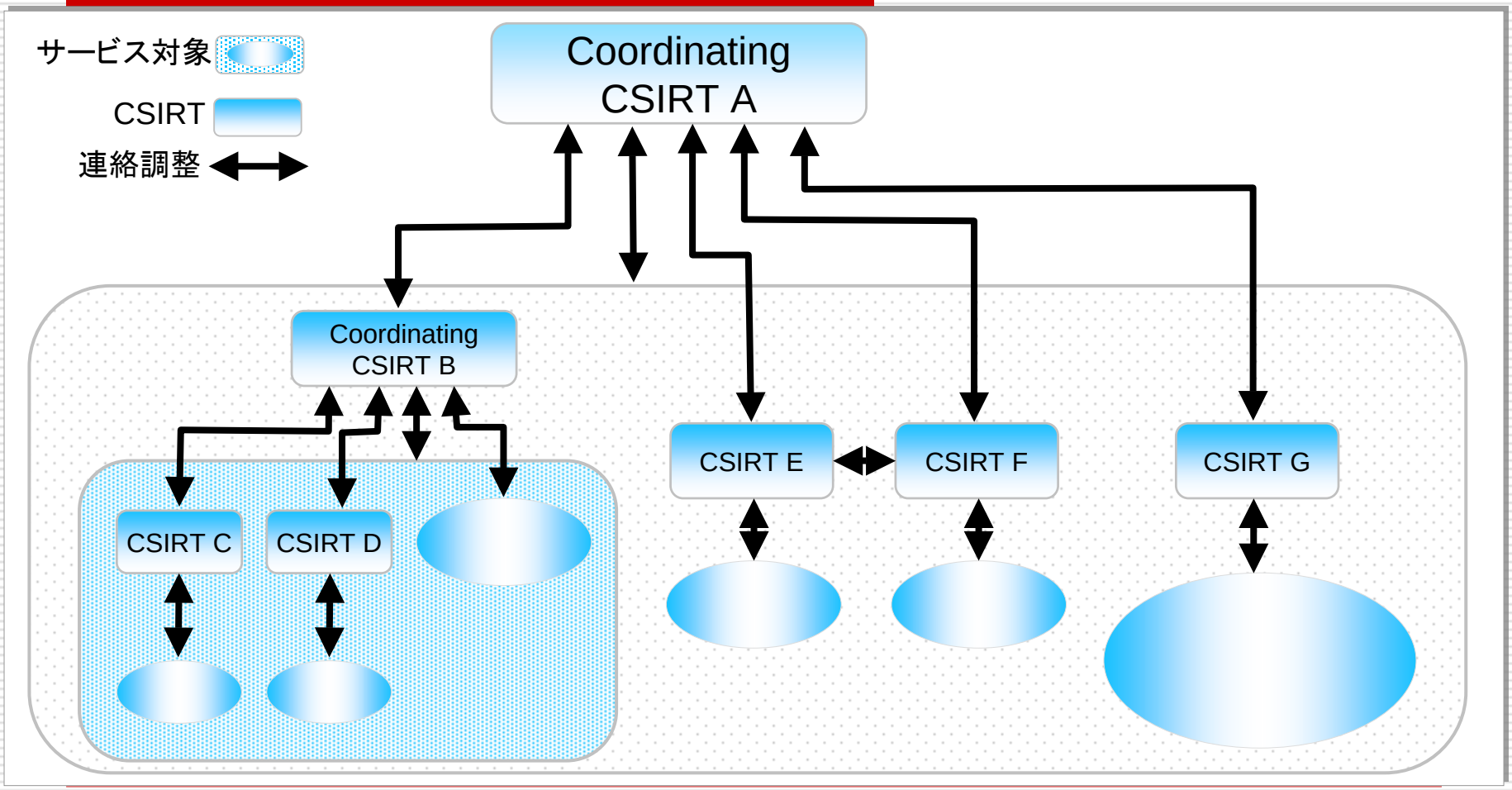
Copyright© 2006 JPCERT/CC
All rights reserved.

サービス対象について
組織内CSIRTの位置



Copyright© 2006 JPCERT/CC
All rights reserved.

サービス対象について
CSIRT間連携



Copyright© 2006 JPCERT/CC
All rights reserved.

4. CSIRTのサービス

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTのサービスについて
種類

- Reactive Service
  - Reactive: 反応
  - 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のもっともコアな活動
- Proactive Service
  - Proactive: 先を見越す
  - 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
- Security quality management service
  - セキュリティコンサルタント、教育など
  - 他のセキュリティー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

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTのサービスについて リスト

Reactive Service	Proactive Service	Security Quality Management Service
+アラート及び警告 +インシデントハンドリング -インシデント分析 -現場でのｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽ -ｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽｻﾎﾟｰﾄ -インシデントレスポンス調整 +脆弱性ハンドリング -脆弱性分析 -脆弱性レスポンス -脆弱性レスポンス調整 +アーティファクトハンドリング -アーティファクト分析 -アーティファクトレスポンス -ｱｰﾃｨﾌｧｸﾄﾚｽﾎﾟﾝｽ調整	○アナウンスメント ○技術動向監視 ○セキュリティ監査 或いはアセスメント ○調整、セキュリティツール／アプリケーションメンテナンス、インフラ整備 ○セキュリティツールの構築 ○不正検知サービス ○セキュリティ関連情報の提供	✓リスク分析 ✓事業継続及び災害復旧計画 ✓セキュリティコンサルタント ✓セキュリティ意識啓発 ✓教育／トレーニング ✓製品の評価及び検証

Copyright© 2006 JPCERT/CC
All rights reserved.

5. CSIRTの組織モデル

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル

- Security Team
  - セキュリティーチーム
- Internal Distributed CSIRT
  - 内部における分配型CSIRT
- Internal Centralized CSIRT
  - 内部における集中型CSIRT
- Internal Combined Distributed and Centralized CSIRT
  - 内部における統合（分配/集中）型CSIRT
- Coordinating CSIRT
  - 連絡調整としてのCSIRT

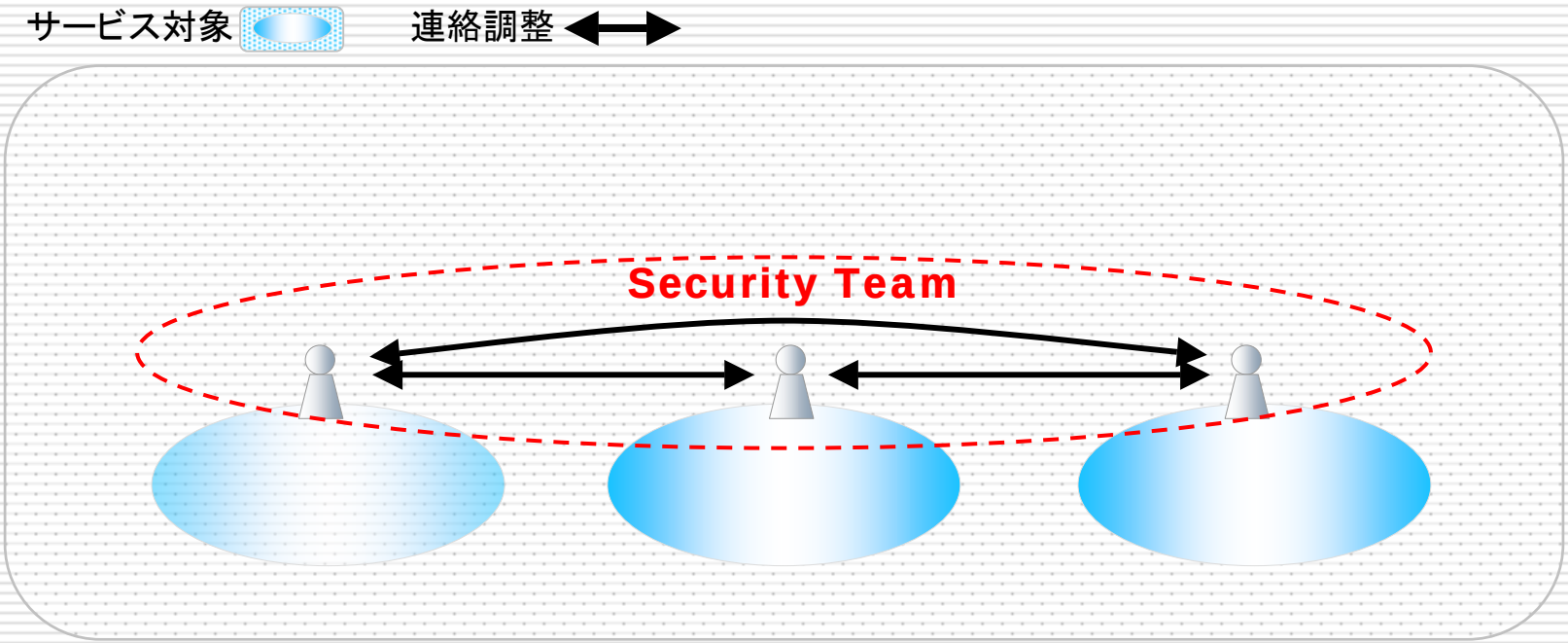
Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル
Security Team

- 正式なCSIRTの組織体ではない（既存のITエンジニアを活用）
- システム管理者、ネットワーク管理者、セキュリティ管理者などの職務の一部として、セキュリティインシデントに関する対応をとる
- 組織全体へのインシデントレスポンス事がしにくい
- 復旧のために組織全体から情報を集めたり、最新の脅威情報を収集し、所属組織への影響度を考察し、報告するような組織ではない
- “Business as usual”（いつもどおり）のアプローチであり、インシデント対応としては極めて限定的な活動となる

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル
Security Team



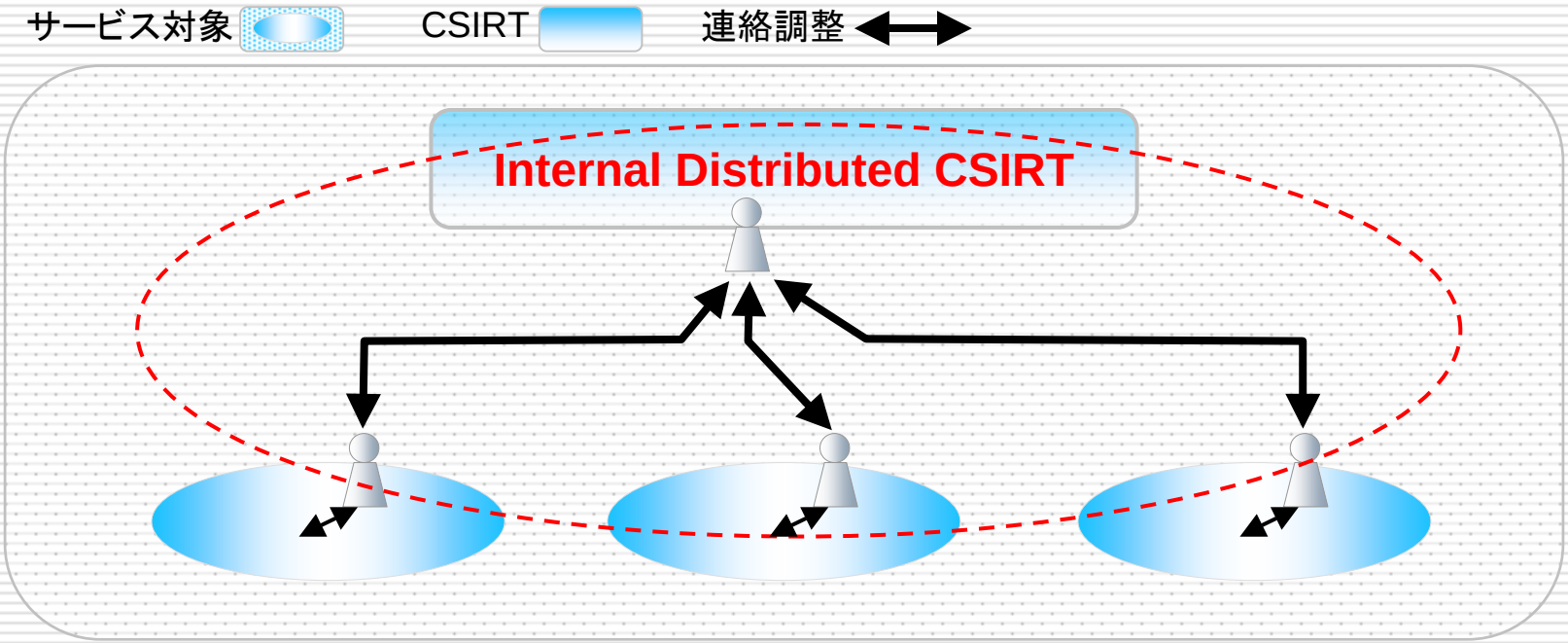
Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル
Internal Distributed CSIRT

- それぞれの下位組織の中に、仮想的に（兼務で）CSIRTのスタッフを指定する
- 一人の責任者（マネージャ）が、監督及び調整をする
- スタッフは、それぞれのエリアを担当をベースにしながら、インシデント発生時には、CSIRTのスタッフして活動をする。また、幾人かは、CSIRTのみの業務を専門にする
- このCSIRTは、その組織に対するPOC（Point of Contact：連絡窓口）としての機能を持つ

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル
Internal Distributed CSIRT



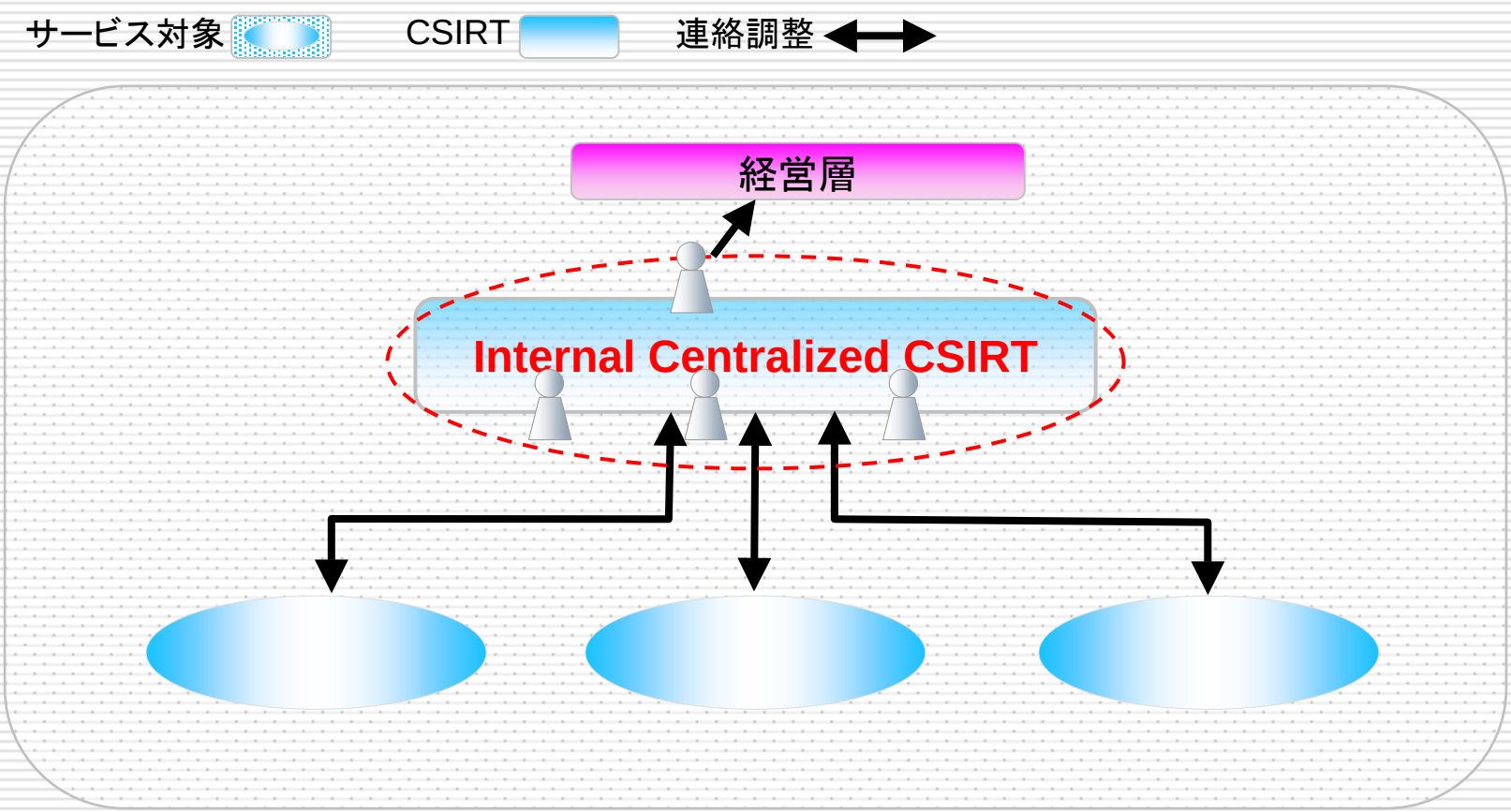
Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル
Internal Centralized CSIRT

- 専属のスタッフで構成されているが、幾人かは、パートタイムやローテーションで活動する場合がある
- 責任者（マネージャ）、組織のトップ層（CIOなど）に対する報告義務が伴う
- 正式に組織されており、組織内で発生するすべてのインシデントレスポンスへの責任がある
- このCSIRTは、この組織に対するPOCとしての機能を持つ

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル
Internal Centralized CSIRT



Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル

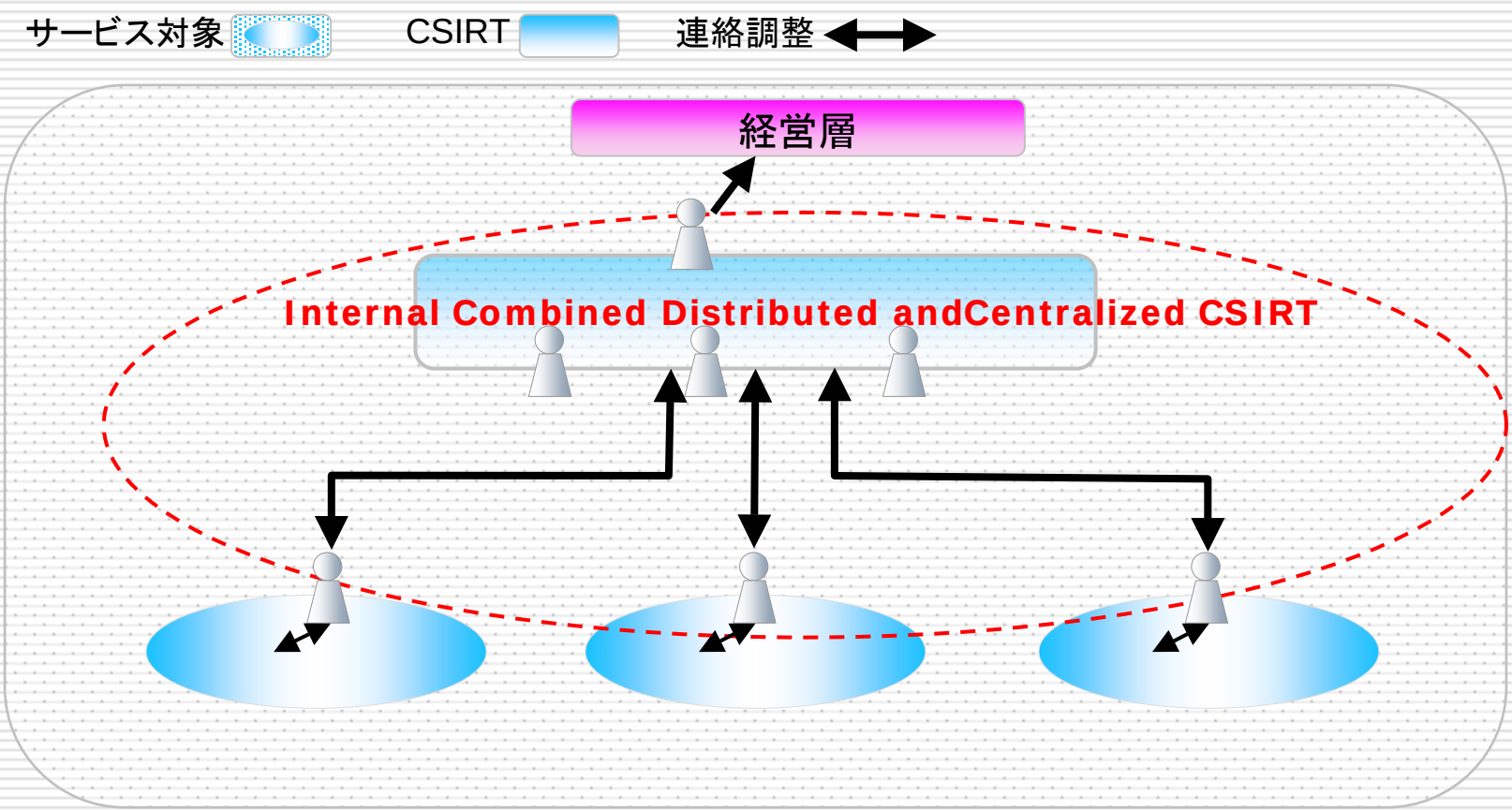
Internal Combined Distributed and Centralized CSIRT

- Distributed（分配型）とCentralized（集中型）のCSIRT
- 組織内全体にセキュリティインシデントに対応できる体制を整えるため、既存の社員を最大限に活用する
- 組織の中心に、下位組織のCSIRTを調整できる能力を持たせる
- そのCSIRTは、この組織に対するPOCとしての機能を持つ

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル

Internal Combined Distributed and Centralized CSIRT



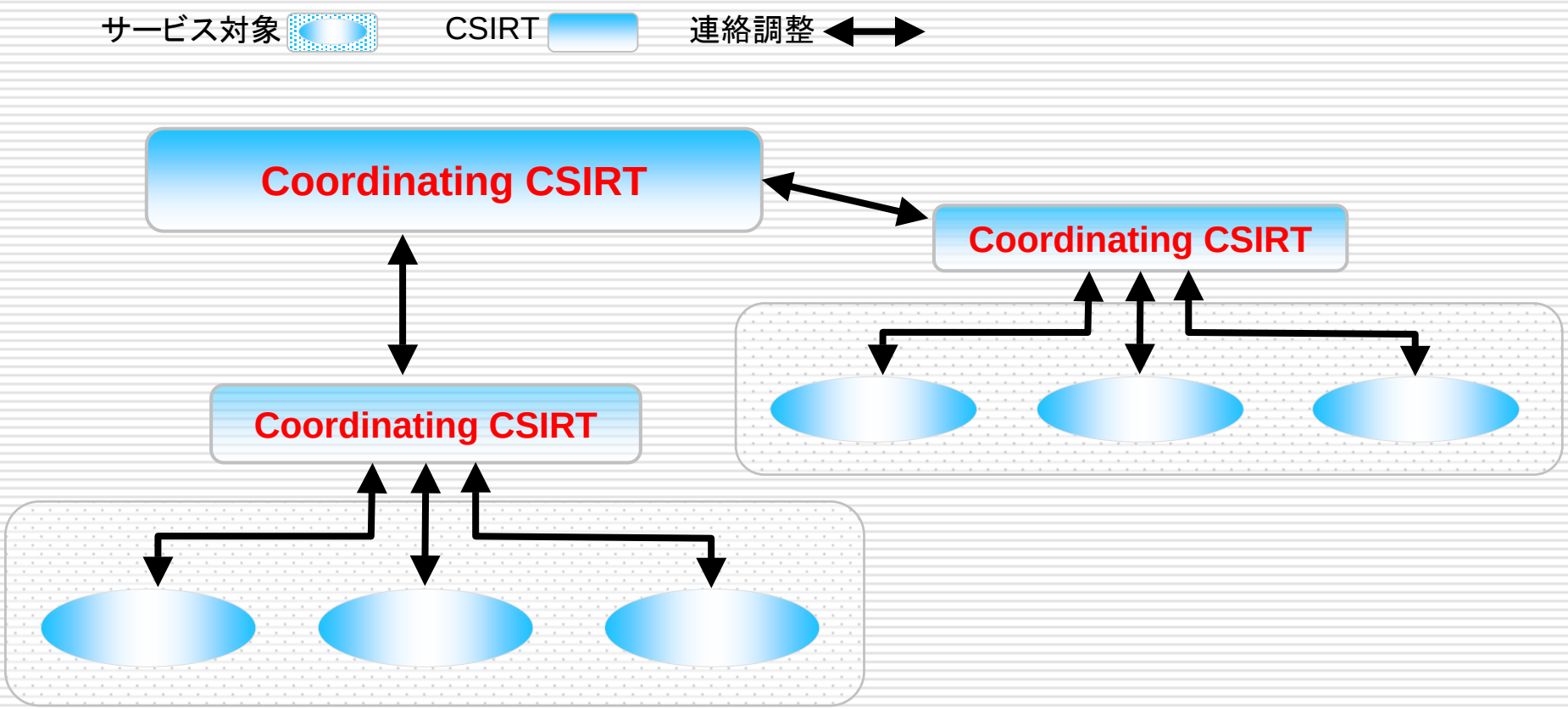
Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル
Coordinating CSIRT

- 組織の内外に対するインシデントレスポンスを調整をしたり、その環境を構築する。（組織外に関しては、他の組織のCSIRTとの連携を指す）
- このCSIRTは広い範囲を対象とし、さまざまなサービス対象を持つ
- 他の組織のインシデントレスポンスを助けるための連絡調整もする

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデル
Coordinating CSIRT



Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデルとサービス

サービス種類	サービス		Security Team	Distributed	Centralized	Combined	Coordinating
Reactive	アラート及び警告		△	○	○	○	○
	インシデントハンドリング	インシデント分析	○	○	○	○	○
		現場での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	×	○	○	○	○
		インシデントレスポンス調整	○	○	○	○	○
	脆弱性ハンドリング	脆弱性分析	△	△	△	△	△
		脆弱性レスポンス	○	△	×	△	△
		脆弱性レスポンス	△	○	○	○	○
	アーティファクトハンドリング	アーティファクト分析	△	△	△	△	△
		アーティファクトレスポンス	○	△	×	△	△
		アーティファクトレスポンス調整	△	△	○	○	○

Copyright© 2006 JPCERT/CC
All rights reserved.

CSIRTの組織モデルとサービス

サービス種類	サービス	Security Team	Distributed	Centralized	Combined	Coordinating
Proactive	アナウンスメント	×	○	○	○	○
	技術動向監視	×	△	○	○	○
	セキュリティ監査或いはアセスメント	×	△	△	△	×
	調整、セキュリティツール／アプリケーションメンテナンス、インフラ整備	○	△	△	△	×
	セキュリティツールの構築	△	△	△	△	△
	不正検知サービス	○	△	△	△	×
	セキュリティ関連情報の提供	×	△	○	○	○
Security Quality Manage-ment	リスク分析	×	△	△	△	△
	事業継続及び災害復旧計画	×	△	△	△	△
	セキュリティコンサルタント	×	△	△	△	△
	セキュリティ啓発活動	×	△	△	△	○
	教育／トレーニング	×	△	△	△	○
	製品の評価及び検証	×	△	△	△	△

Copyright© 2006 JPCERT/CC
All rights reserved.

6. JPCERT/CCについて

Copyright© 2006 JPCERT/CC
All rights reserved.

JPCERT/CCの概要

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

- 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、連携などの活動をおこなっている
    - 緊急事態 (Emergency) への対応 (Response)

※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、
意図的及び偶発的なもの

Copyright© 2006 JPCERT/CC
All rights reserved.

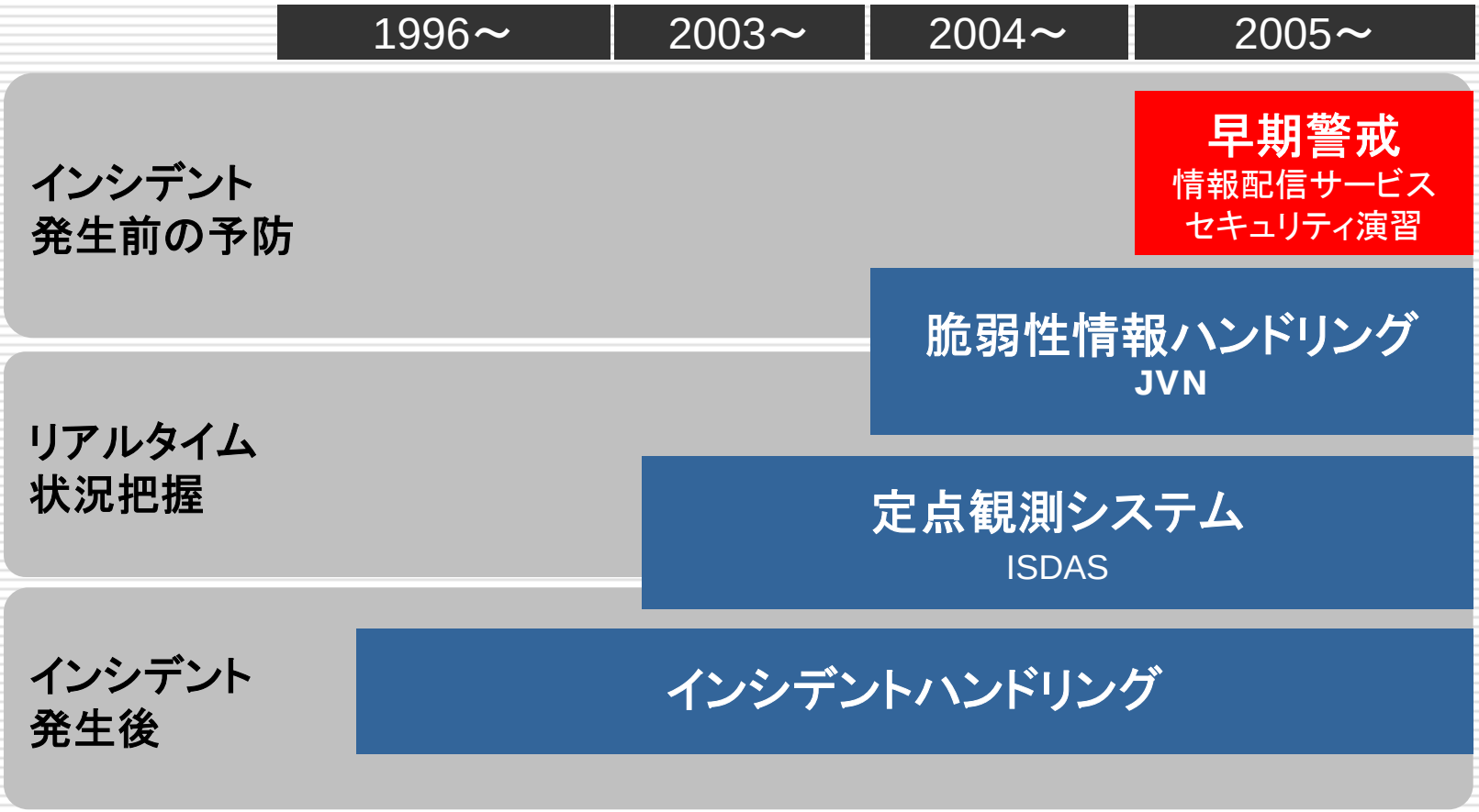
JPCERT/CCの略歴

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	任意団体として発足
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	有限責任中間法人格取得
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

※CSIRTとはコンピュータセキュリティインシデント対応組織の略称
※FIRSTとは世界的な、コンピュータセキュリティインシデント対応組織の協力体制を構築する目的で設立されたフォーラム

Copyright© 2006 JPCERT/CC
All rights reserved.

JPCERT/CC活動内容



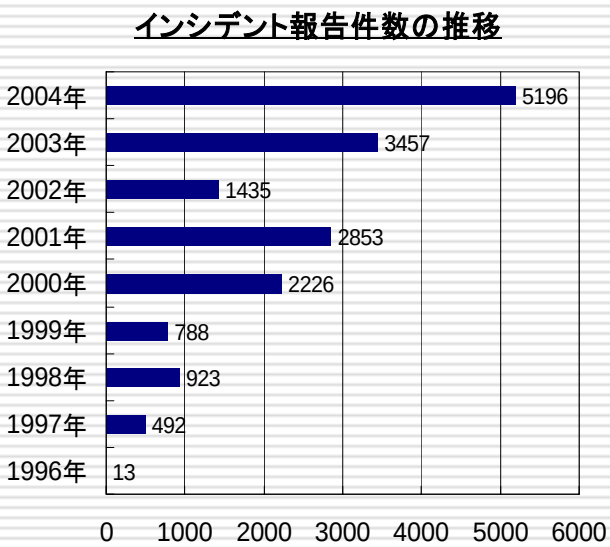
Copyright© 2006 JPCERT/CC
All rights reserved.

インシデントハンドリング

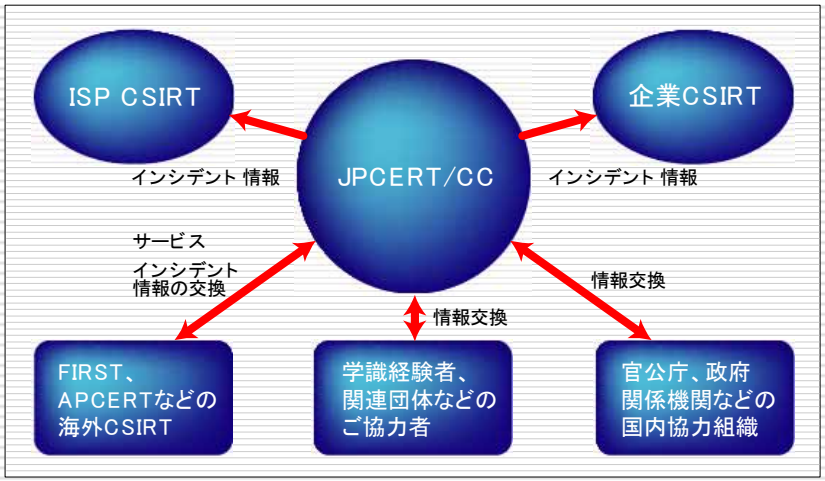
「CSIRT of CSIRTs」

CSIRT (Computer Security Incident Response Team)間の連携をコーディネート

- インシデントレスポンスの時間短縮による被害最小化
- 再発防止に向けた関係各機関の情報交換および情報共有

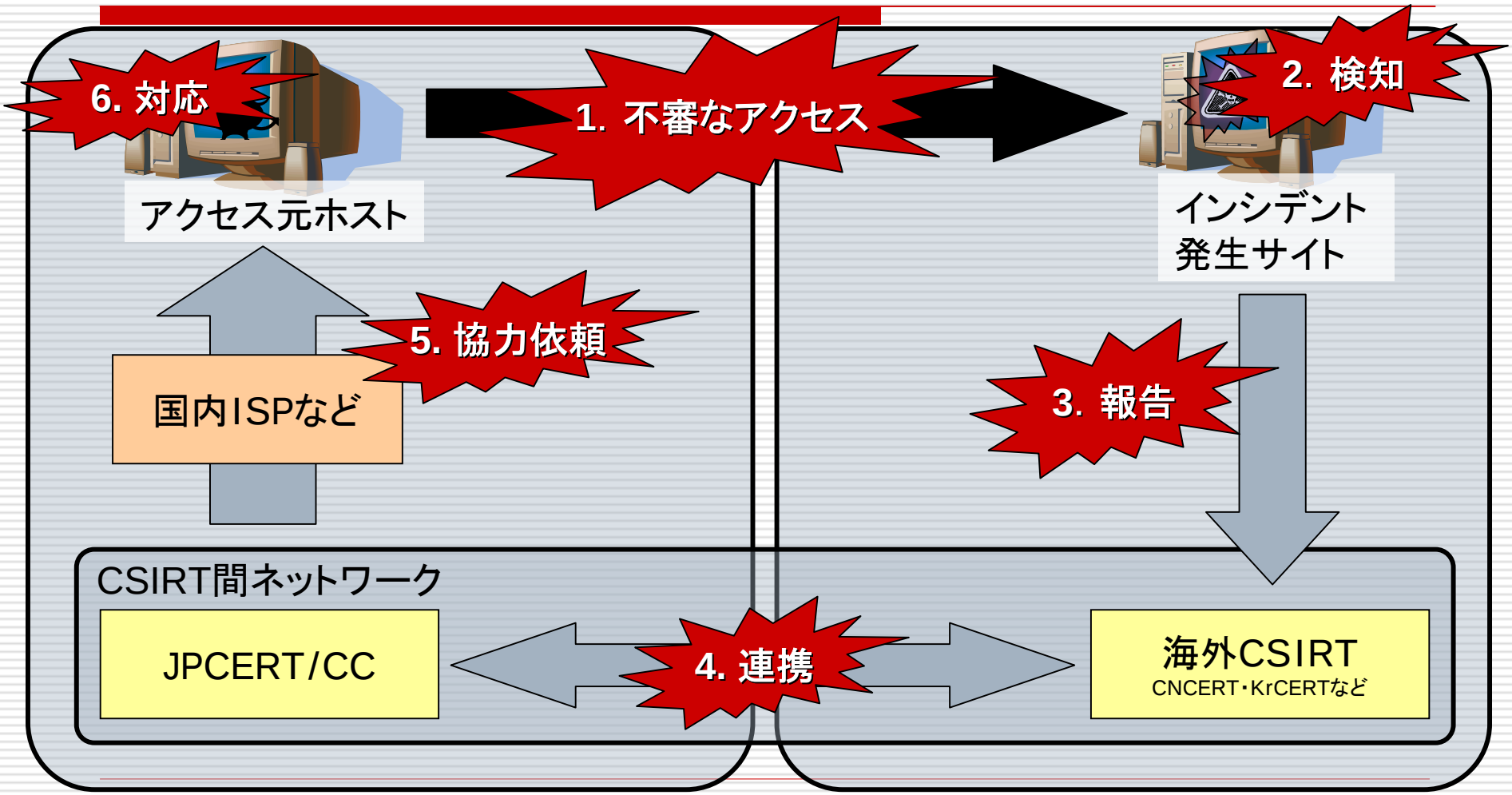


※JPCERT/CC が1996年から2004年に受領したインシデント報告



Copyright© 2006 JPCERT/CC
All rights reserved.

インシデントハンドリングの国際連携



Copyright© 2006 JPCERT/CC
All rights reserved.

連絡先

- JPCERTコーディネーションセンター
  - Email: office@jpcert.or.jp
  - Tel:03-3518-4600
  - http://www.jpcert.or.jp

  - 早期警戒グループ
    - Email: ww-info@jpcert.or.jp

Copyright© 2006 JPCERT/CC
All rights reserved.