

一般的なCSIRT実装モデルの紹介

CSIRT研究者・日本シーサート協議会

山賀正人

自己紹介

- フリーライター/コンサルタント

- Internet Watch連載「海の向こうのセキュリティ」

- JPCERT/CC専門委員

- 日本シーサート協議会専門委員

- CSIRT研究家

- 明治大学客員研究員

- 2001年から2006年までJPCERT/CCに勤務



はじめに

■ CSIRTに規格はない

- RFC 2350

- Expectations for Computer Security Incident Response

- 各企業の実情・現状に即したCSIRTの実装

- 二つとして同じCSIRTは存在しない

■ 実例を参考に

- ここで紹介する事例は取材当時(2009年－2010年)のもの

参考資料

日経NETWORK「CSIRT奮闘記」

<http://itpro.nikkeibp.co.jp/article/COLUMN/20091120/340847/>

CSIRTは機能である

■ CSIRT

- Computer Security Incident Response Team

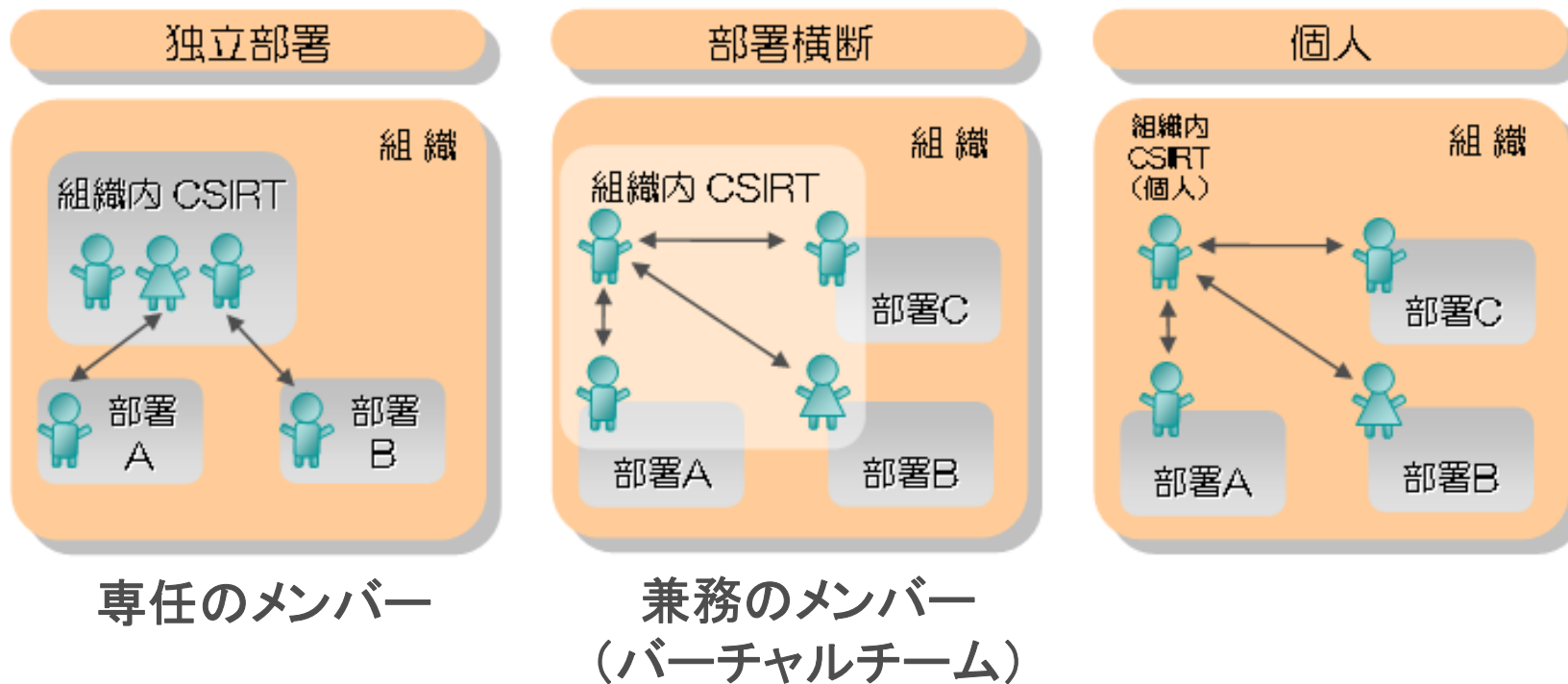
■ CSIRC

- Computer Security Incident Response Capability

現在、CSIRTという単語は
実質的にCSIRCの意味を含んでいる。

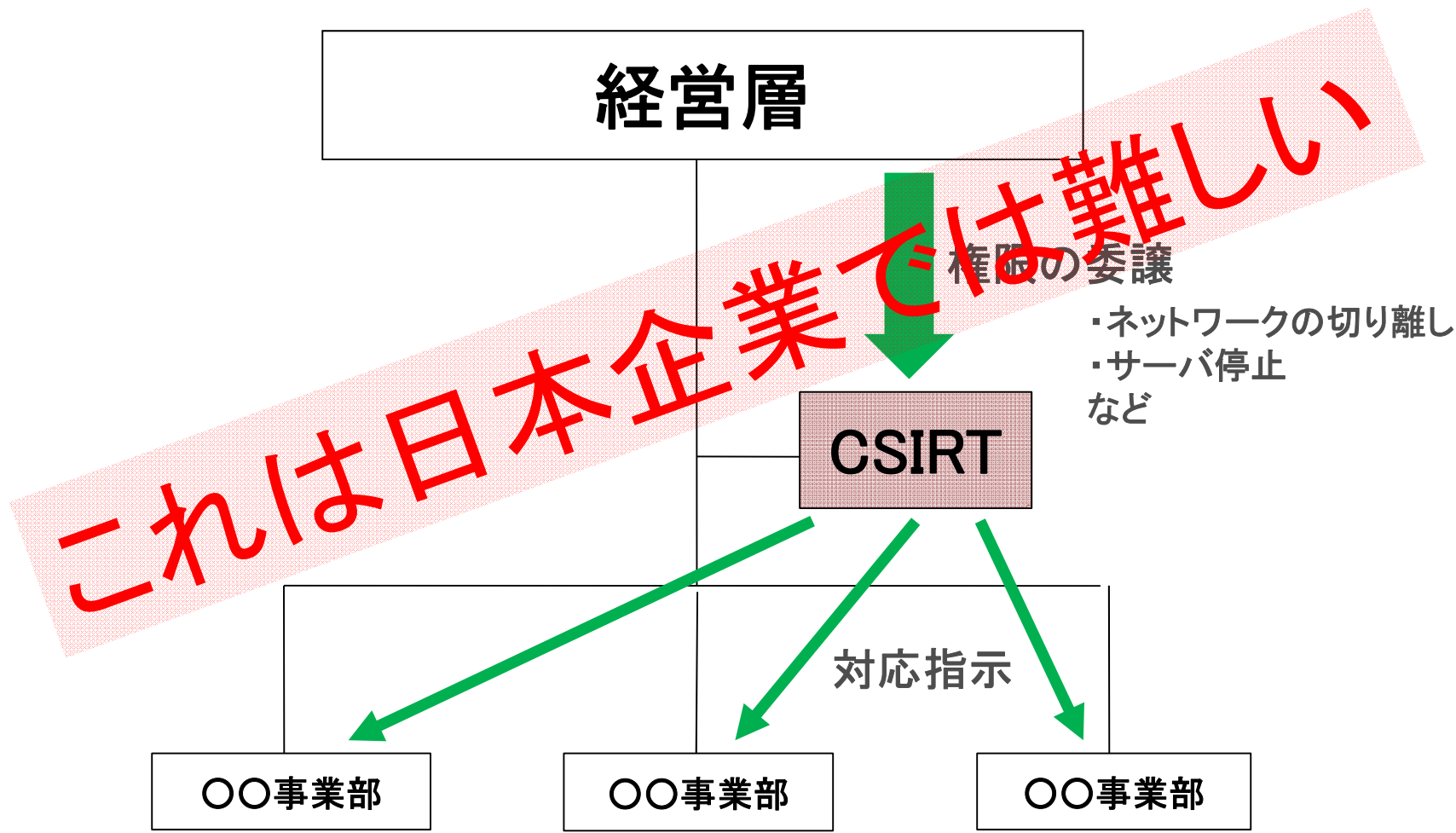
CSIRTの実装形態の例

大きく分けて以下の3種類



出典: JPCERT/CC「CSIRTガイド」
http://www.jpccert.or.jp/csirt_material/files/guide_ver1.0.pdf

代表的実装例



何故日本の企業では難しいのか？

■ 委譲すべき「権限」の存在がそもそも曖昧

- 取締役会での合議制
- 名前だけのCIO, CSO, CISO
 - 実際には権限がない
 - 意思決定ができない
- 歴史的背景に起因する微妙な社内パワーバランス

■ 社内での協力関係が成立しにくい

- 管理・監視の組織と見なされ、社員が情報を提供・報告しようとしていない

■ 定期的な人事異動によるゼロリセット

日本でも「権限委譲型」はある

- 楽天のRakuten-CERT
 - ミクシィのmixirt(ミクサート)
- など

IT系をはじめとする新しい企業では可能かもしれない

「権限委譲型」とは異なる日本企業独自の形態

- OKIグループのOKI-CSIRT
- NTTグループのNTT-CERT
- HITACHIグループのHIRT(ハート)

各社独自の形態で実装

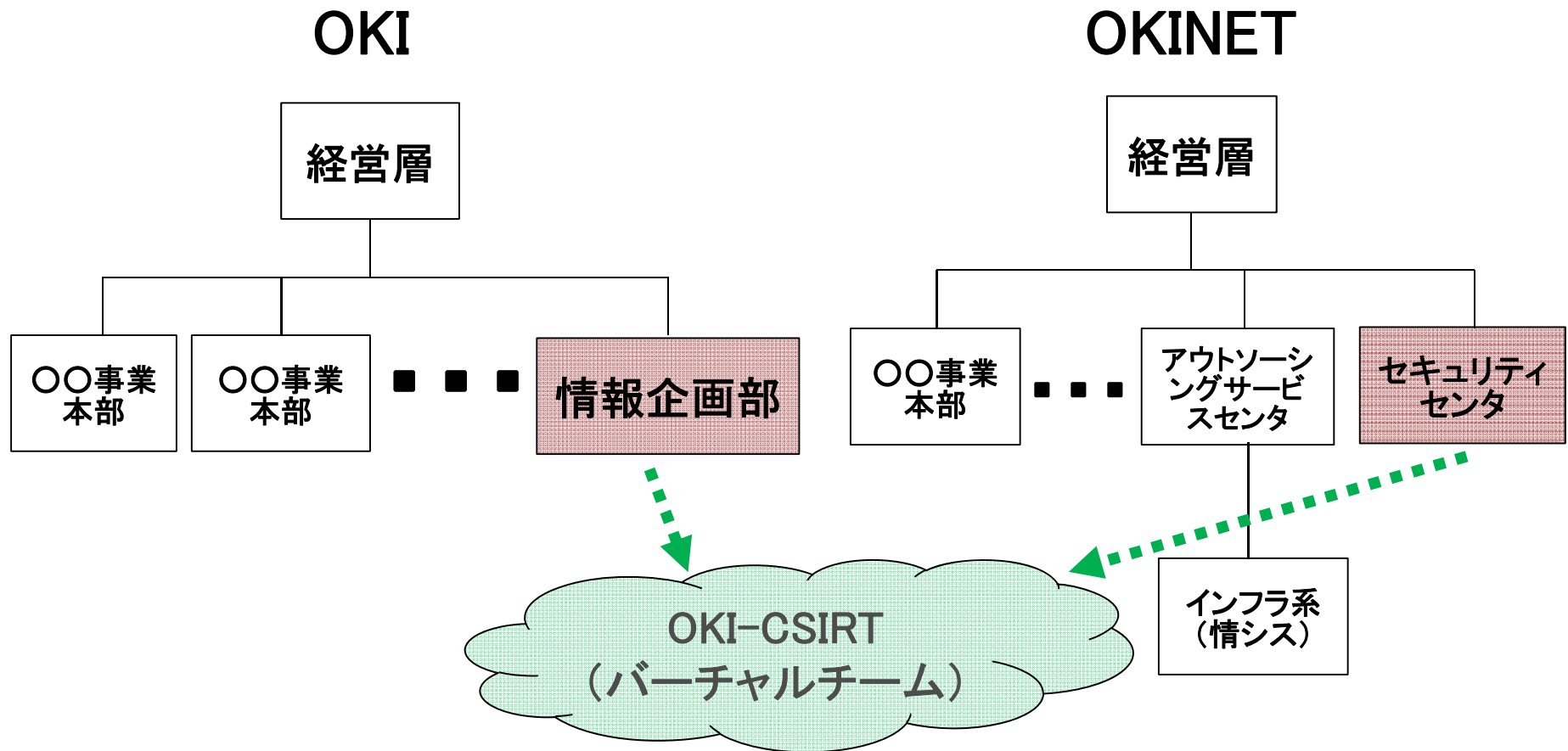
- 共通して見られるポイント
 - CSIRTとしては権限を持たず技術的対応に専念
 - 権限は既存の体制をそのまま使い、権限執行者(部署)と連携

OKIの場合

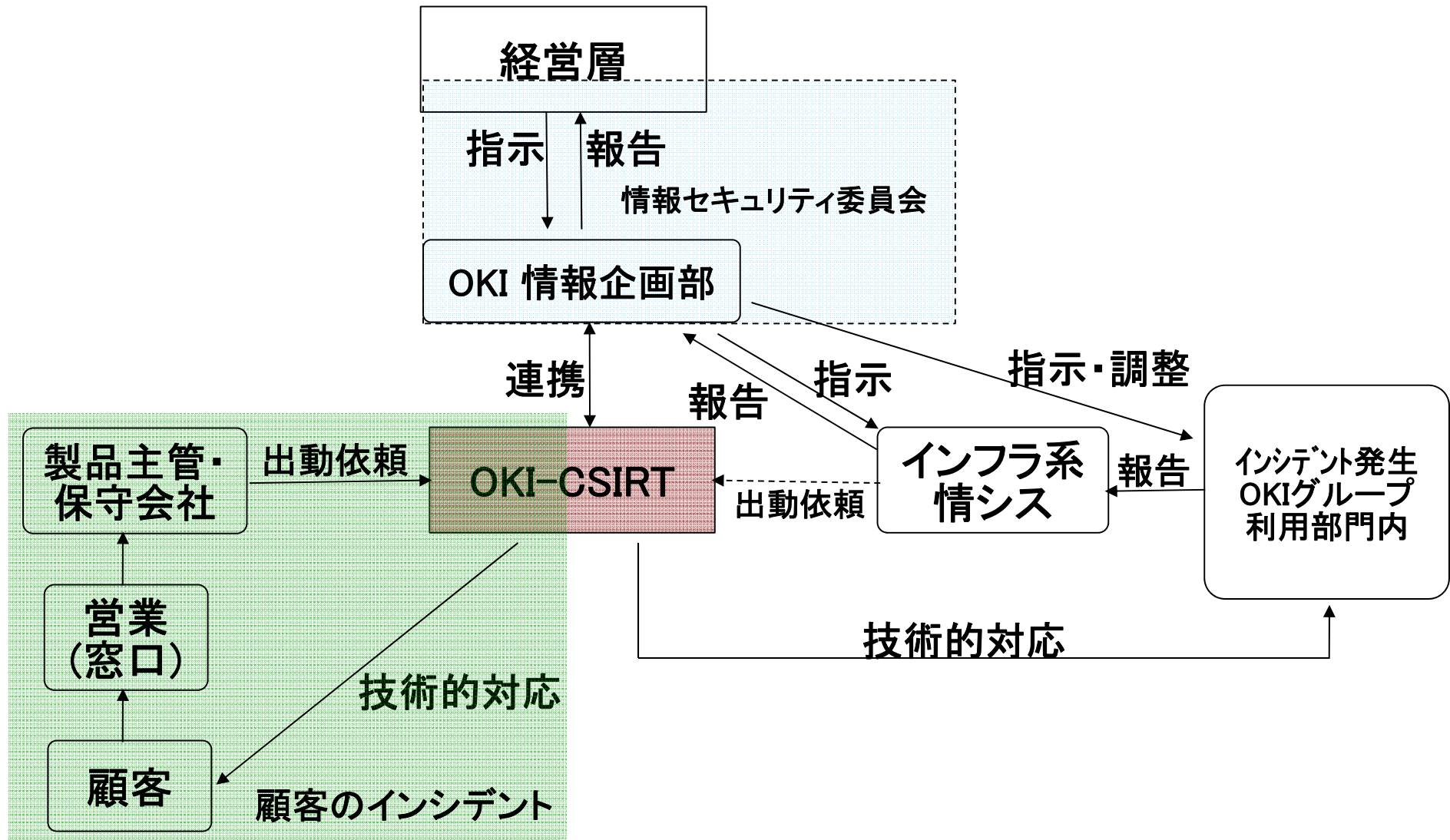
OKI-CSIRT

- OKIグループのCSIRT
 - OKI Computer Security Incident Response Team
 - 沖電気工業(OKI)と沖電気ネットワークインテグレーション(OKINET、現:丸紅OKIネットソリューションズ)が運営
- 2008年5月に正式に活動開始
- OKI情報企画部とOKINETセキュリティセンタのメンバーからなるバーチャルチーム
- 権限を持たず、技術的対応に専念
 - 権限を持つOKI情報企画部との連携
 - 「帽子」の使い分け
- IT運営(共通経費)と品質保証の予算で運営
 - 別途経費を請求することも

OKI情報企画部とOKINETセキュリティセンタの位置づけ



OKIグループのインシデント対応体制



NTTの場合

NTT-CERT

■ NTTグループのCSIRT

- NTT Computer Security Incident Response and Readiness Coordination Team

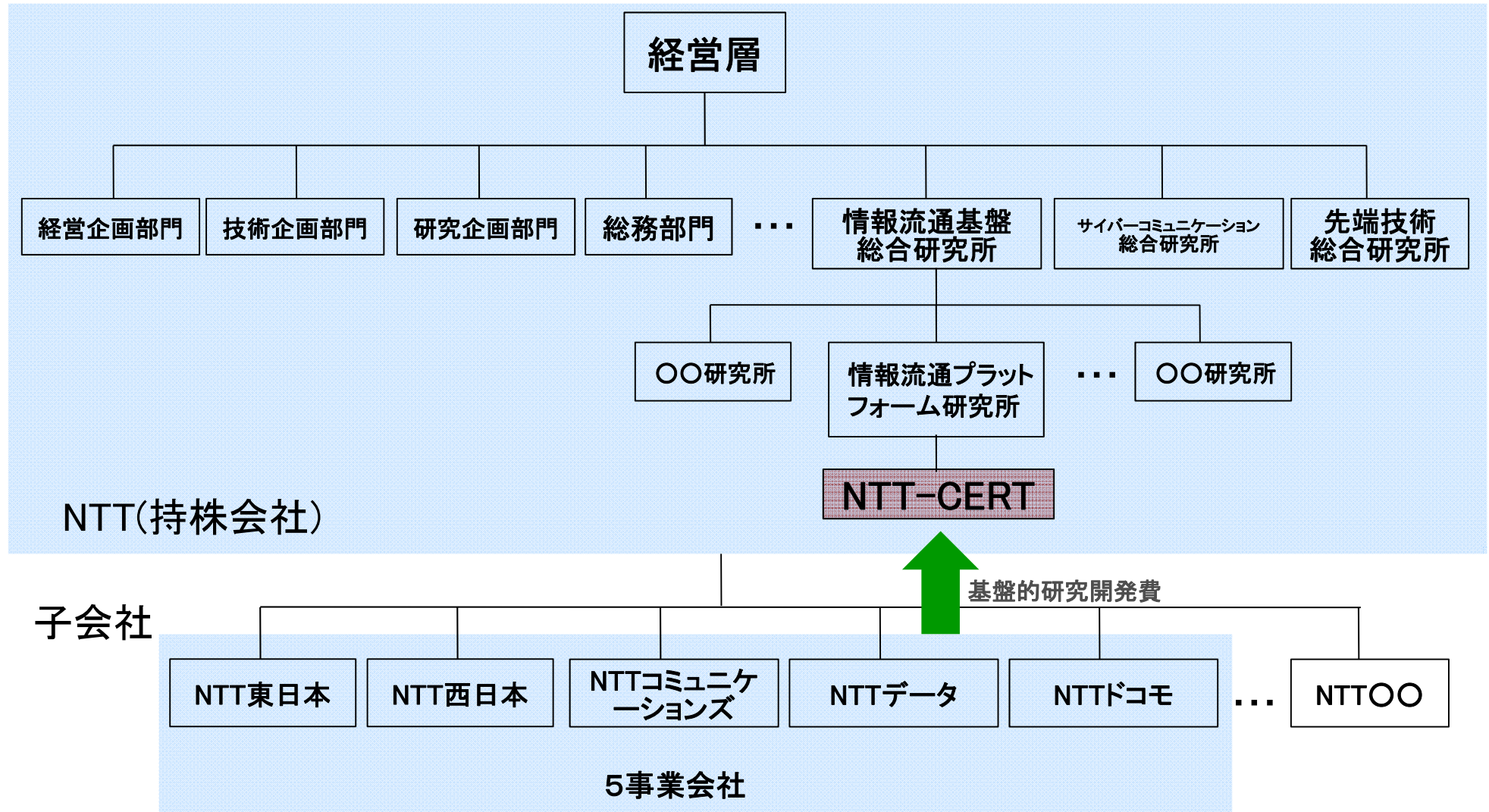
■ 2004年10月に正式に活動開始

■ 持株会社にある情報流通プラットフォーム研究所(PF研)の1研究グループからなるチーム

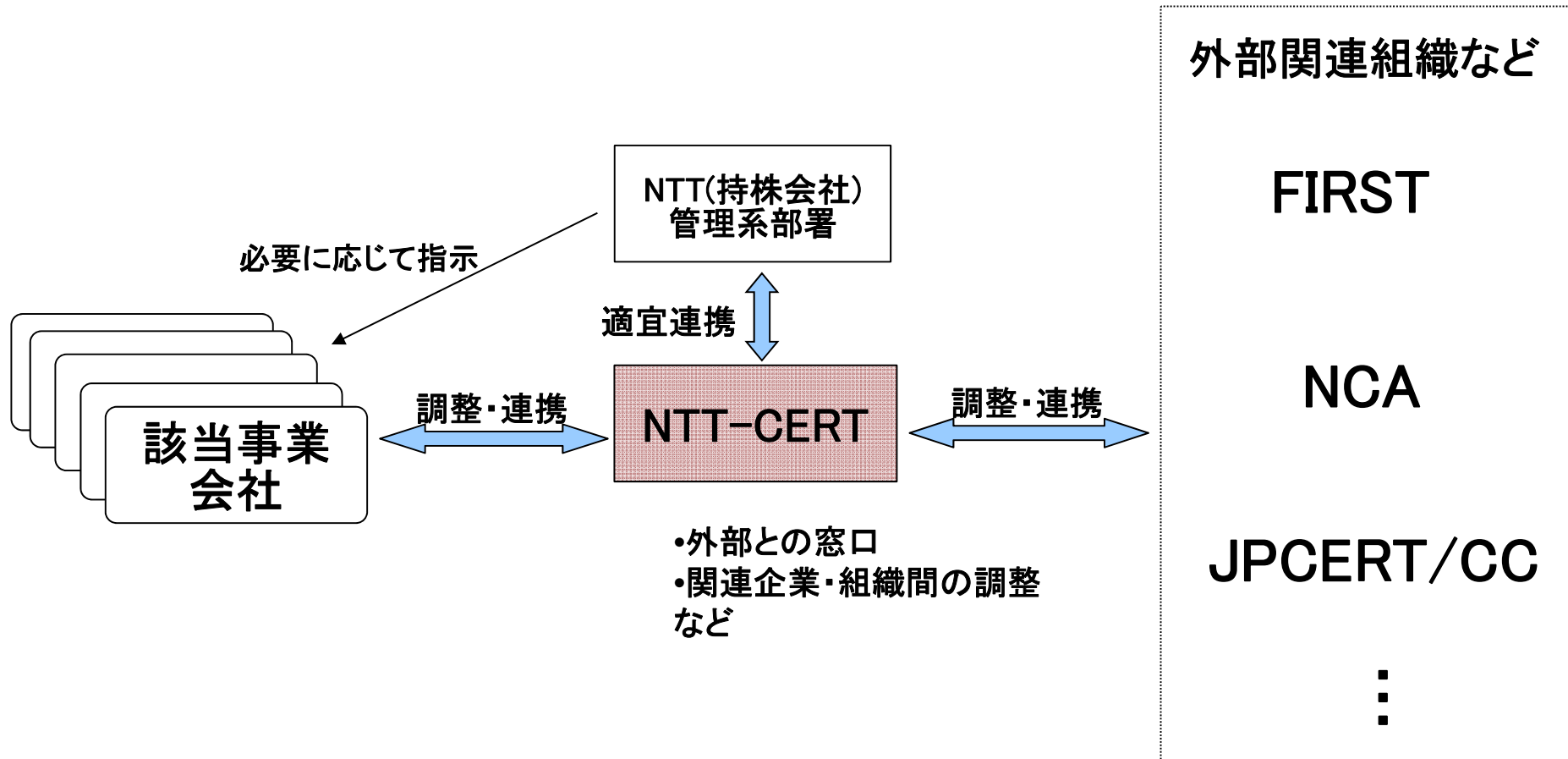
■ 権限を持たず、技術的対応(の支援)に専念

- 研究所に設置されたことで技術的に信頼できる高品質のサービスを提供してくれる組織と受け取ってもらえる
- グループ企業間の「コーディネーション(調整)」を担う
- NTTグループにおけるセキュリティ関連の対外窓口
 - 他の関連企業・組織との連携窓口

NTTグループにおけるNTT-CERTの位置づけ



NTT-CERTを中心としたインシデント対応体制



HITACHIの場合

HIRT

■ HITACHIグループのCSIRT

- Hitachi Incident Response Team

■ 1998年に研究プロジェクトとして活動開始

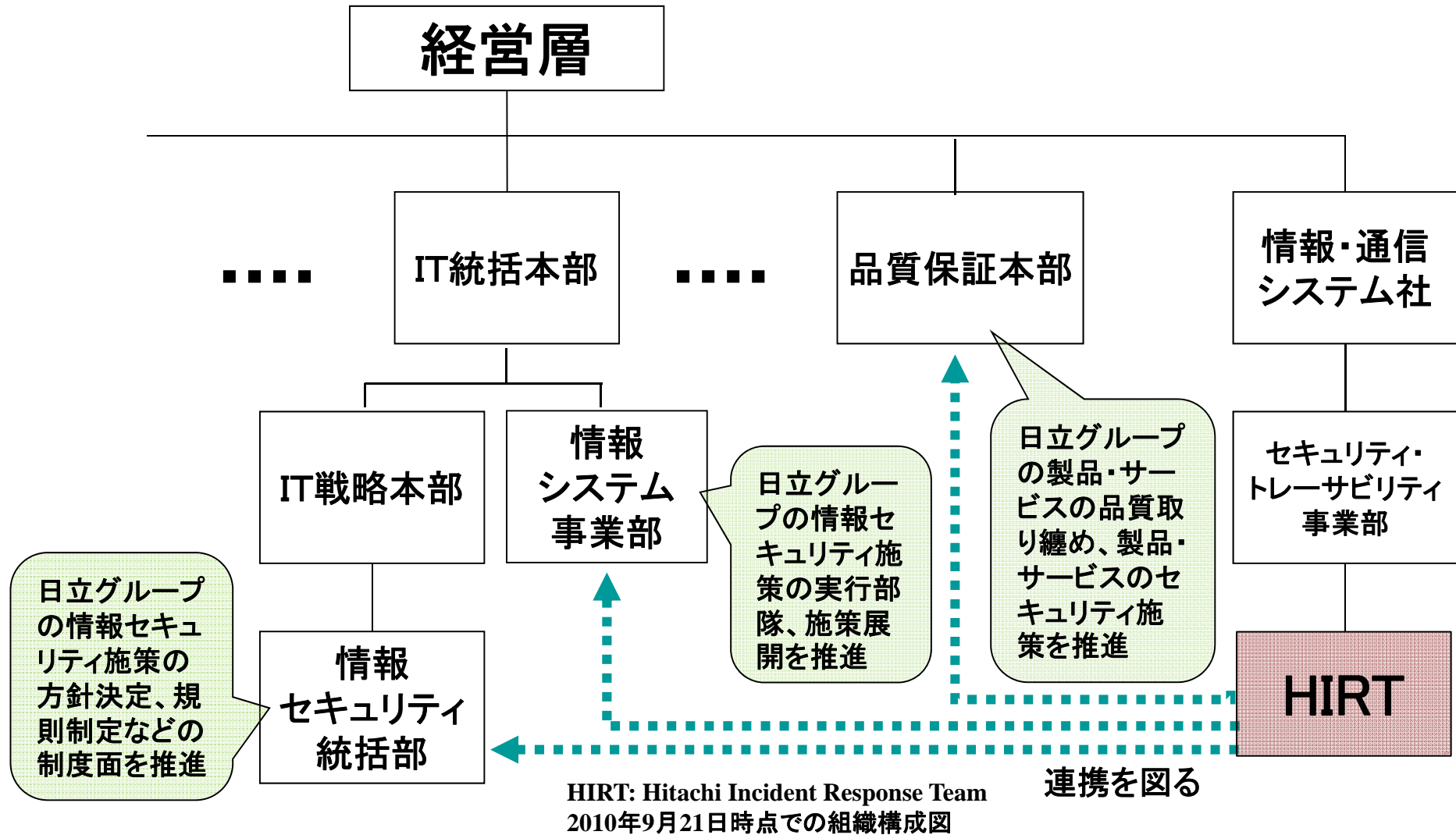
- 研究所のメンバーをはじめとするボランティアグループとして地道に実績を積み上げ信頼を獲得、認められるように

■ 2004年にほぼ今の形態に(次スライド参照)

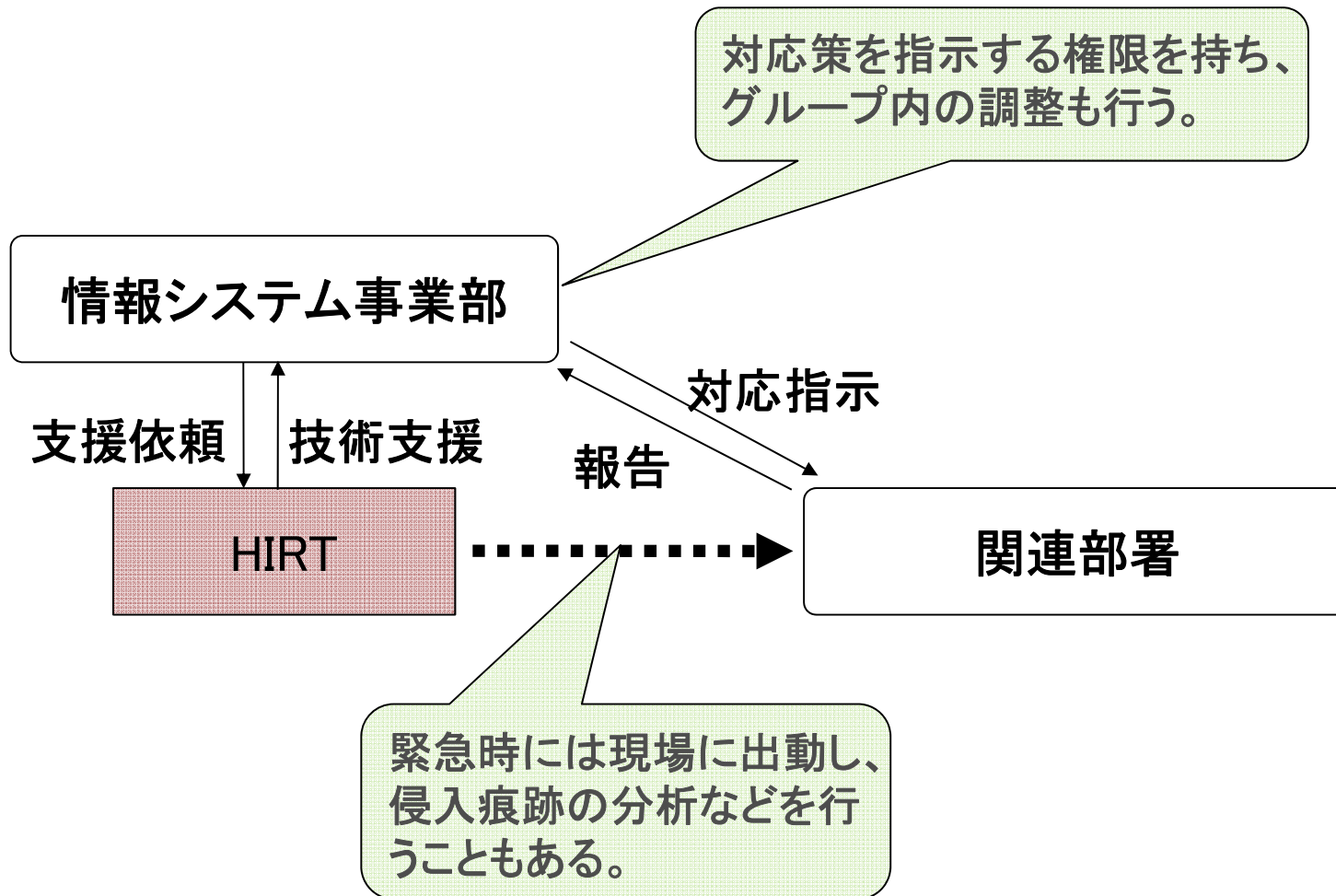
■ 権限を持たず、技術的対応(の支援)に専念

- 権限の執行、実対応、調整は情報システム事業部で
- HITACHIグループにおけるセキュリティ関連の対外窓口
 - 他の関連企業・組織との連携窓口

HITACHIにおけるHIRTの位置づけ



HITACHIのインシデント対応体制



まとめ

- CSIRTに特定の規格はない。
- 日本企業の場合、技術対応に特化した形でCSIRTを構築し、インシデント対応に必要な権限は既存の体制を利用し、連携するケースが多い。
- 既存CSIRTの実例をCSIRT構築の参考に

参考資料

日経NETWORK「CSIRT奮闘記」

<http://itpro.nikkeibp.co.jp/article/COLUMN/20091120/340847/>

ご清聴ありがとうございました。

CSIRTに関して: csirt-pr@nca.gr.jp

NCAおよび加盟に関して: nca-sec@nca.gr.jp



<http://www.nca.gr.jp/>