JPCERT/CC の国際連携について

～International Coordination in CSIRTs network～

JPCERT コーディネーションセンター

鎌田 敬介

KAMATA Keisuke

CSIRTとは?

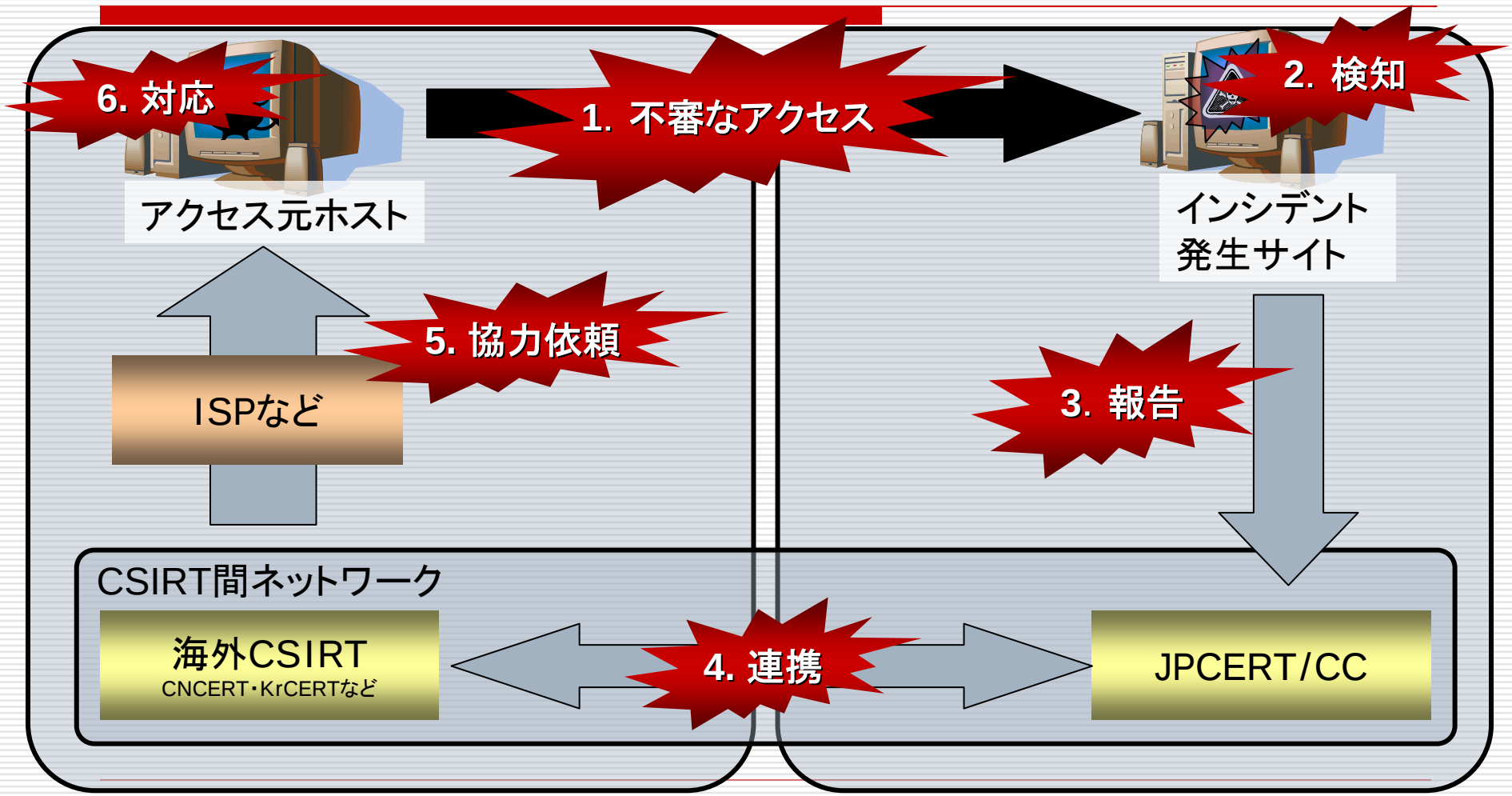
- CSIRTはComputer Security Incident Response Teamの略
  - インシデントへの対応を主な目的とした組織体の一般名称
  - 1988年に設立された世界初の CSIRT が米国 CERT/CC

- JPCERT/CCのような、政府からも、業界からも中立なインシデント対応調整組織は、世界中に存在する
  - KrCERT(韓国)、CNCERT(中国)、AusCERT(豪)など多数
- 政治的、市場からも独立した、テクニカルで、中立な調整機関間で、共通する方針を持って協力し、インシデント対応を行うコミュニティ
  - My security is Depending on your security
  - Web of Trust
- 実績と、信頼関係でつながるCSIRT
  - 繰り返し行うハンドリング手順によって、確実でスピードの速いインシデント対応を行う

CSIRT の分類
http://www.cert.org/csirts/csirt_faq.html

- constituency と呼ばれる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
    - national = 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」など

インシデント対応の国際連携



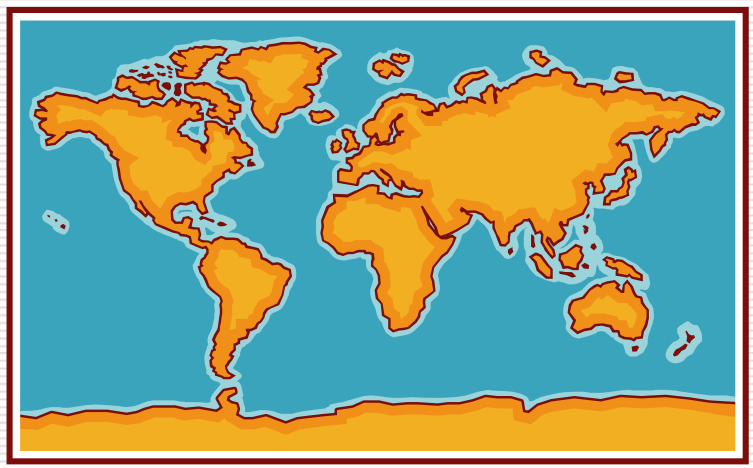
某国

日本

インシデントハンドリングの国際連携

- 国際連携によって越えられる壁
  - 言語の違い
  - 文化の違い
  - 法律・制度の違い

- 各国CSIRT間の
  連携・協調活動として
  最も進んでいる



phishing サイトでの例…

1. 株式会社EXAMPLE の社員が自社ドメイン example.com を真似したexamp1e.com を利用した phishing サイトを発見、IP アドレスから南米の某国であるとわかる
2. 担当者→JPCERT/CC に連絡の仲介を依頼
3. JPCERT/CC→某国CSIRT に連絡
4. 某国CSIRT→phishingサイトのIPアドレス管理者に連絡(whois などを活用)
5. IPアドレス管理者にてサイトが閉鎖

参考

- インシデント対応(レスポンス)概要

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

- 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

- 関係サイトとの情報交換

  http://www.jpcert.or.jp/ed/2002/ed020001.txt

JPCERT CC

ありがとうございました