あなたの会社の情報セキュリティ対応体制は大丈夫? ～CSIRT入門～

CSIRTとは

日本シーサート協議会　運営委員

杉浦芳樹

日本シーサート協議会（NTT-CERT）

林　郁也

CSIRTとは（目次）

- イントロダクション
  - ～　CSIRTの起源
- こんなことに困っていませんか
  - ～　なぜCSIRTが必要なのか
- CSIRTの発展と連携

あなたの会社の情報セキュリティ対応体制は大丈夫? ～CSIRT入門～

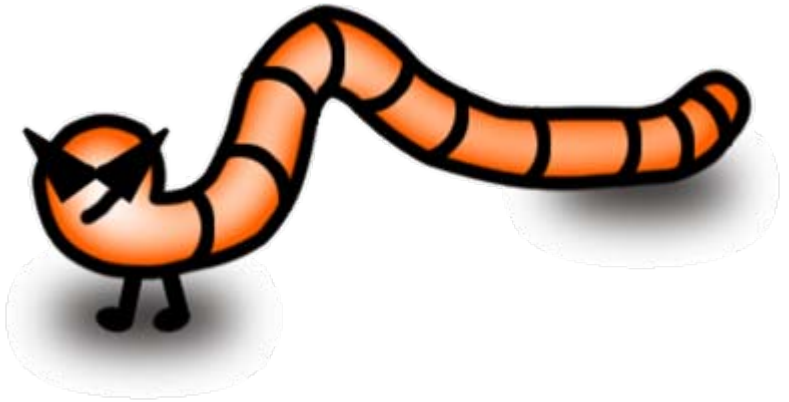
イントロダクション
～　CSIRTの起源

CSIRT
日本シーサート協議会

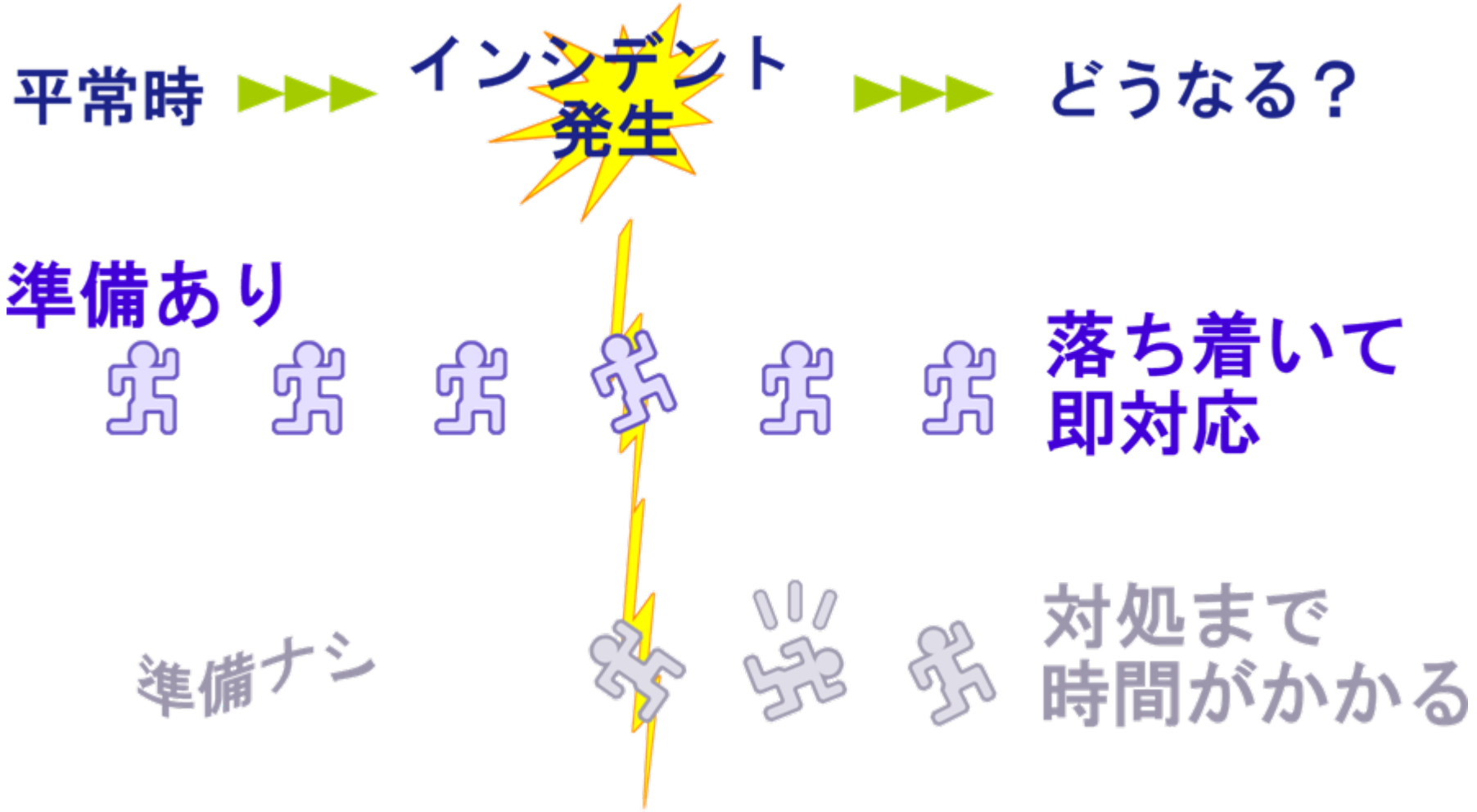
黎明期　－ CSIRTの起源 －

1988年CERT/CC

1991年FIRST

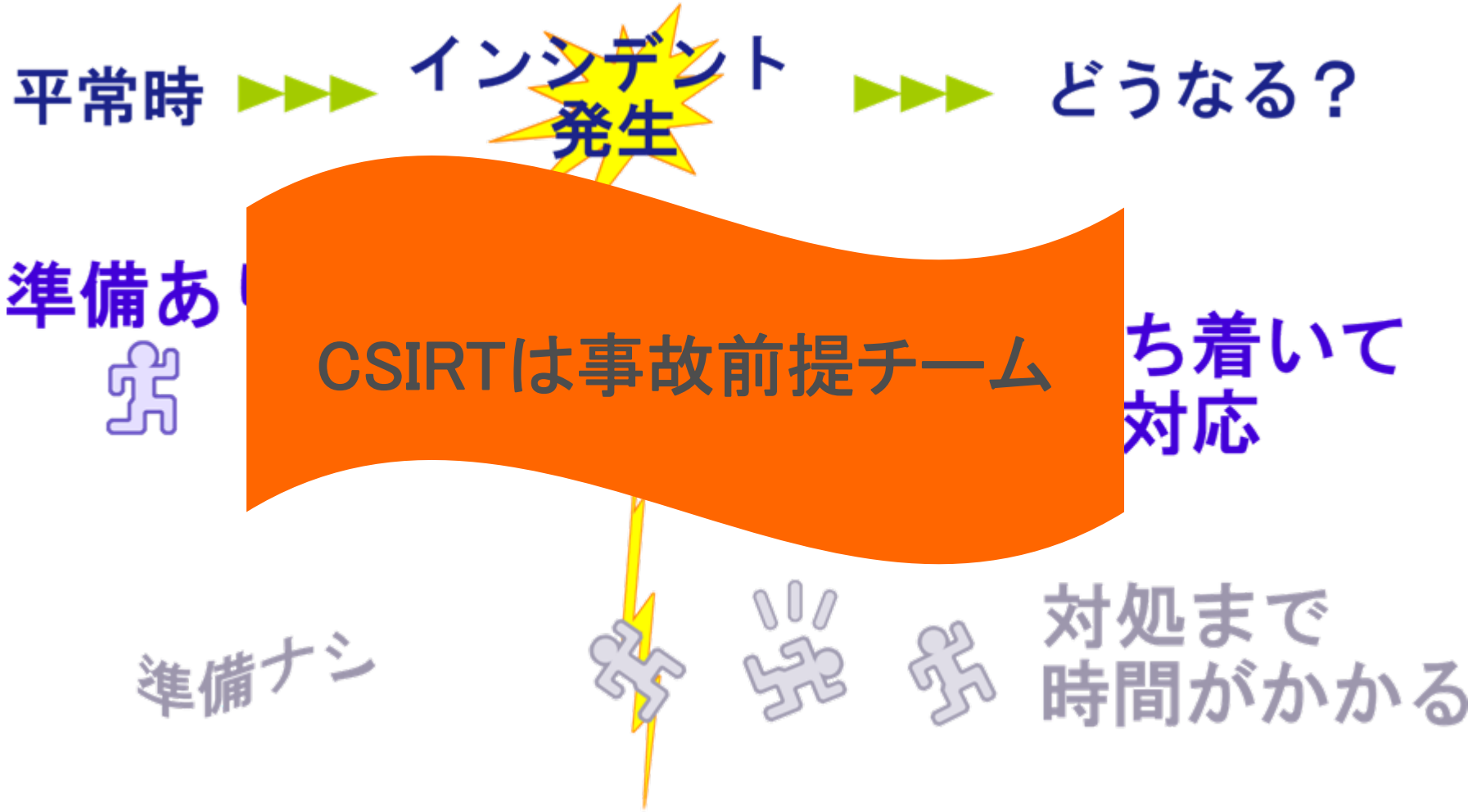


いざ事故が起きたら



CSIRT 日本シーサート協議会

いざ事故が起きたら



CSIRT 日本シーサート協議会

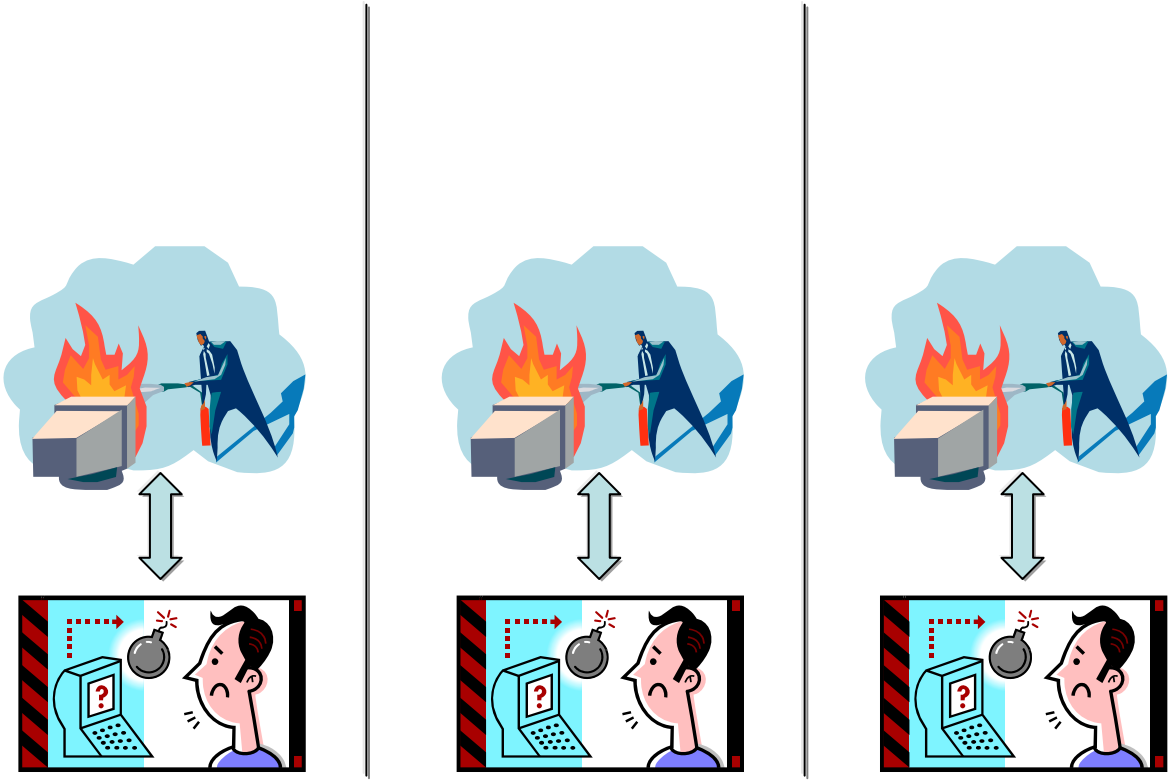
あなたの会社の情報セキュリティ対応体制は大丈夫? ～CSIRT入門～

こんなことに困っていませんか
～　なぜCSIRTが必要なのか

CSIRT
日本シーサート協議会

Question 1

- 同じようなトラブルに悩んでいませんか

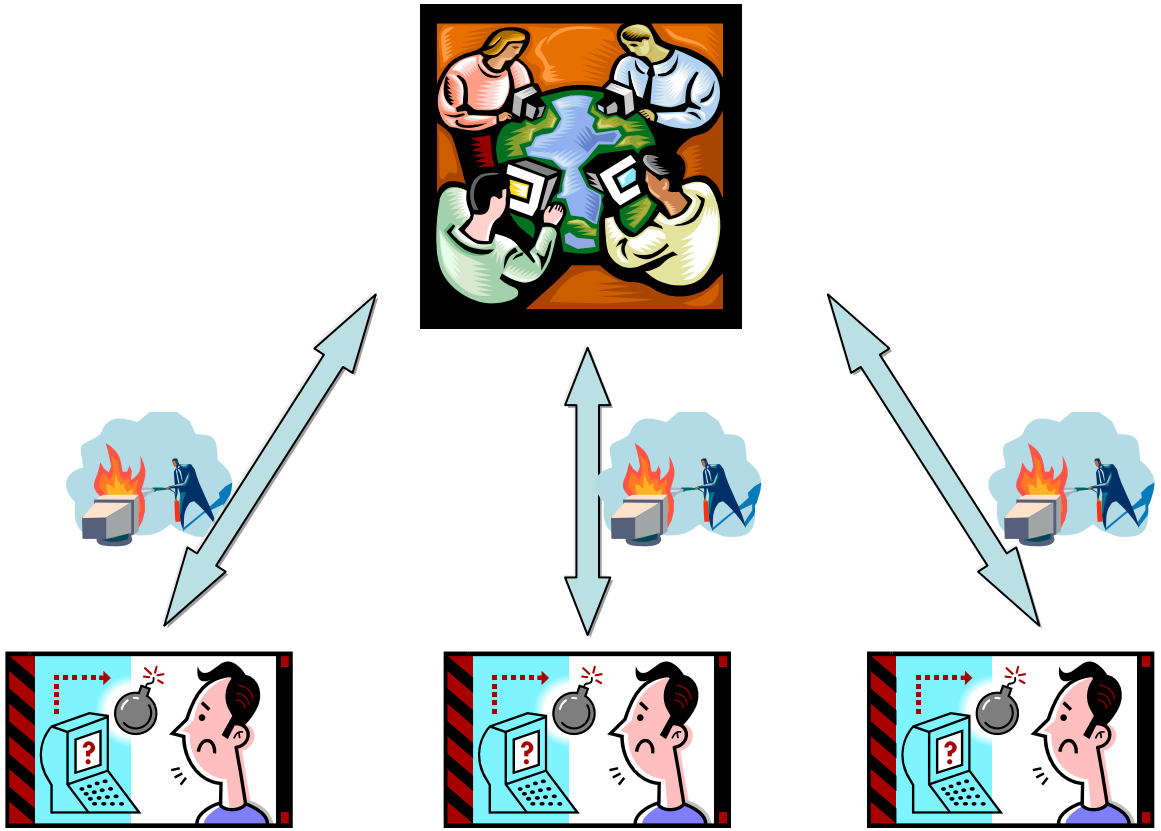


Question 1

■ 同じようなトラブルに悩んでいませんか

ベストプラクティス
集中と適用

センシティブな状況
→難しい判断



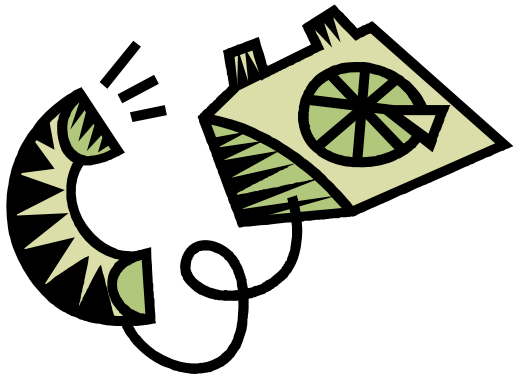
CSIRT
日本シーサート協議会

Question2

- インシデントが起こったときにすぐに動けますか
  - 体制 （誰が動く？誰に動いてもらう？）
  - やるべきこと （またはその反対）
  - エスカレーション
  - 訓練・演習

Question3

- 情報が必要なところに伝わりますか
  - １組織だけでなく、会社全体として・・・
    - やれること、やるべきこと （またはその反対）
    - 体制
    - エスカレーション
    - 訓練・演習
  - 縦横の連携



  - 何を扱うかを事前に決めておく必要がある

振り返り（組織内の活動）

- 同じようなトラブルに悩んでいませんか
- インシデントが起こったときにすぐに動けますか
- 情報が必要なところに伝わっていますか

これらは、組織内において予め対応体制を定めておくことで、解決できる。

Question4

- 自分達の施策に自信が持てますか
- 自分達の不得意はどのようにカバーしていますか

レビューと修正

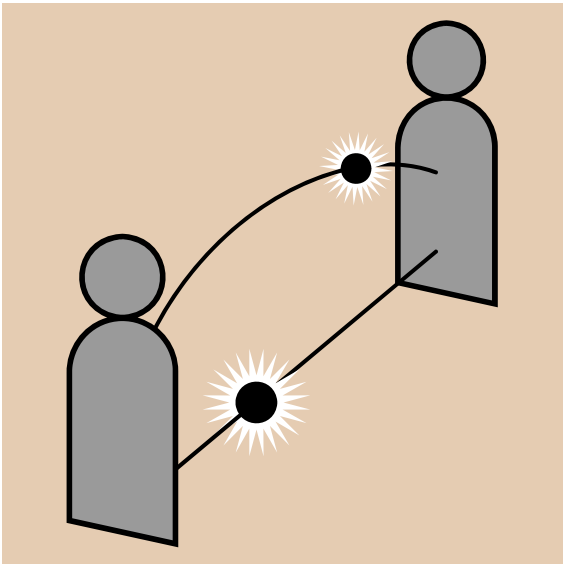
Question5

■ 情報はどこからもらえますか

たくさんの窓口があると迷惑・混乱を招く

コミュニティの話題で初めて気づく何かもある

自分自身の存在を知ってもらっていないと・・・
信頼されていないと・・・



CSIRT
日本シーサート協議会

振り返り（外との連携）

- 自分達の施策に自信が持てますか
- 自分達の不得意はどのようにカバーしていますか
- 情報はどこからもらえますか

これらは、対応体制があることを組織外に宣言・周知し、普段から連携しておくことで、解決できる。

まとめ

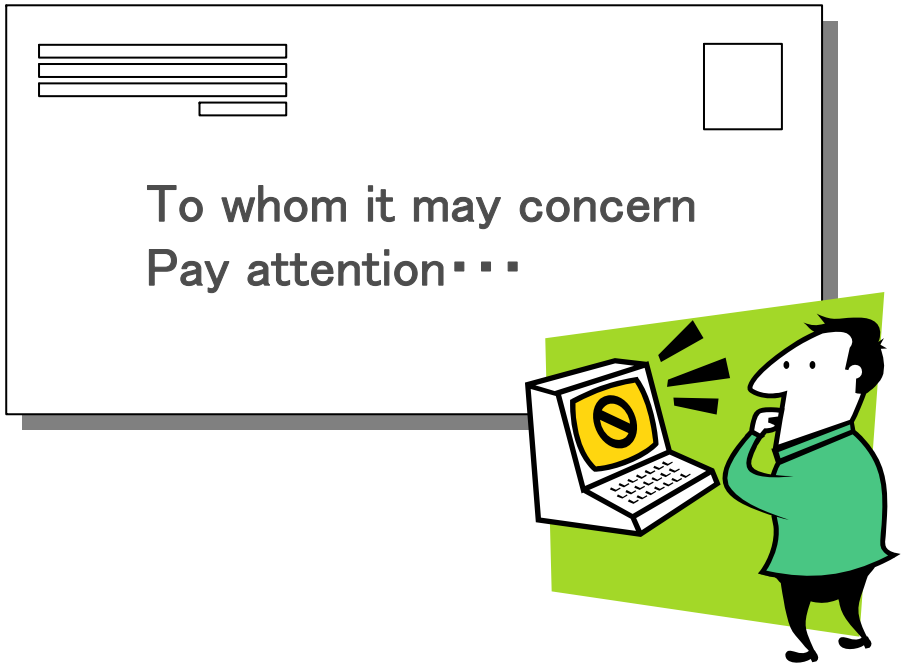
- 事故前提における、準備が大切
  - 起こってしまうものにどう対応するか
  - 取り扱いの難しい情報・状況がある
  - 頼られる存在
- 一人よりみんな（一組織では対応しきれない）
  - 信頼できるスジからの情報
  - 他社との比較、たな卸し
  - 得意分野の相互補完
  - 業界の問題への対応
  - 事例の共有
    - 対応の参考、未来の被害者を出さない

ケーススタディ（Spamメール？）

■ 海外からのメール

受け手）
　英語なので見なかった
　Spamかと思った

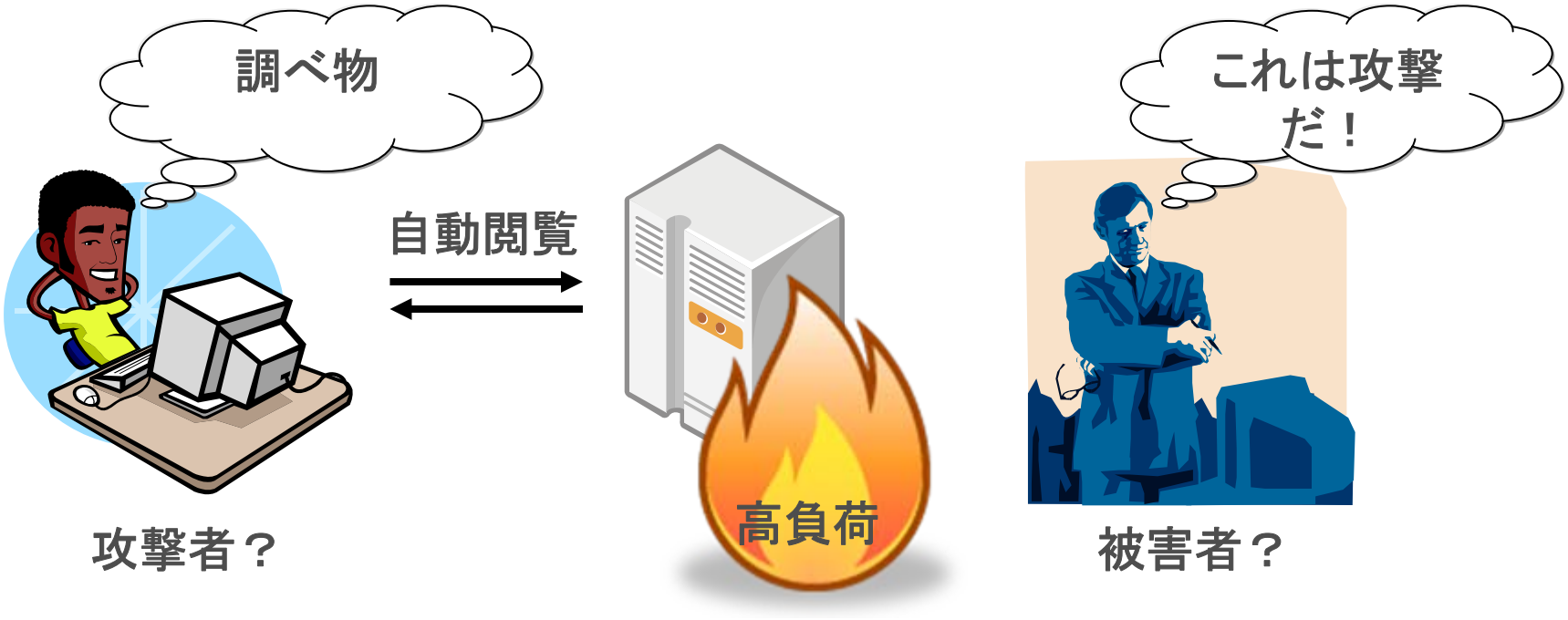
送り手）
　どこに送るかわからない



CSIRT
日本シーサート協議会

ケーススタディ(攻撃か？被害か？)

■ どうやら攻撃を受けたらしい・・・？



CSIRT 日本シーサート協議会

CSIRTとは

- インシデント対応の中核を担う部署（チーム）または機能
  - インシデント対応機能の実装
  - CSIRTであることの宣言（社内的、社外的、両方ある）

    社内：　情報の集約・・

    社外：　連携・・

- 抽象的概念である
  - 決まった実装形態はない

    求められるのは機能

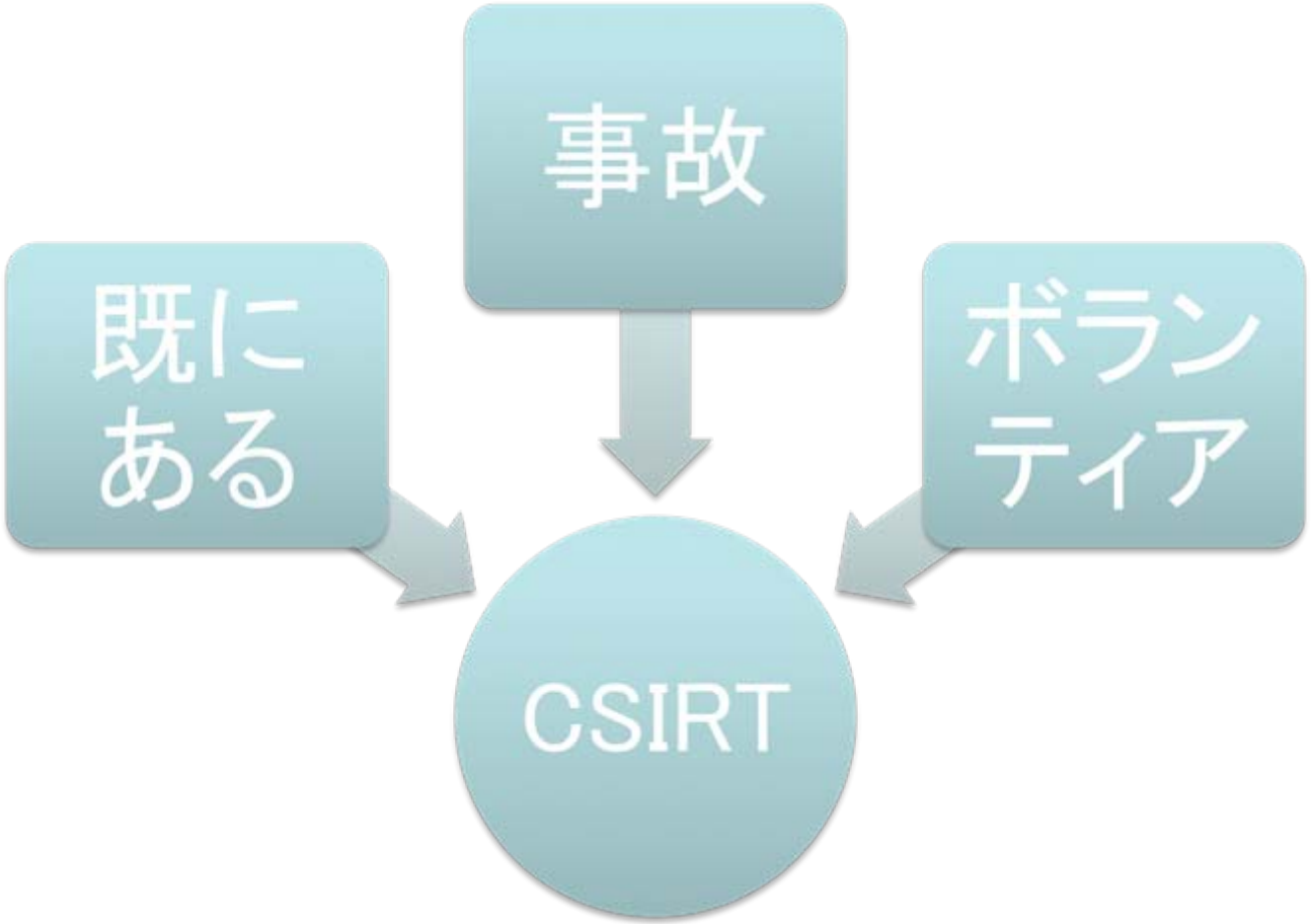
あなたの会社の情報セキュリティ対応体制は大丈夫? ～CSIRT入門～

CSIRTの発展と連携

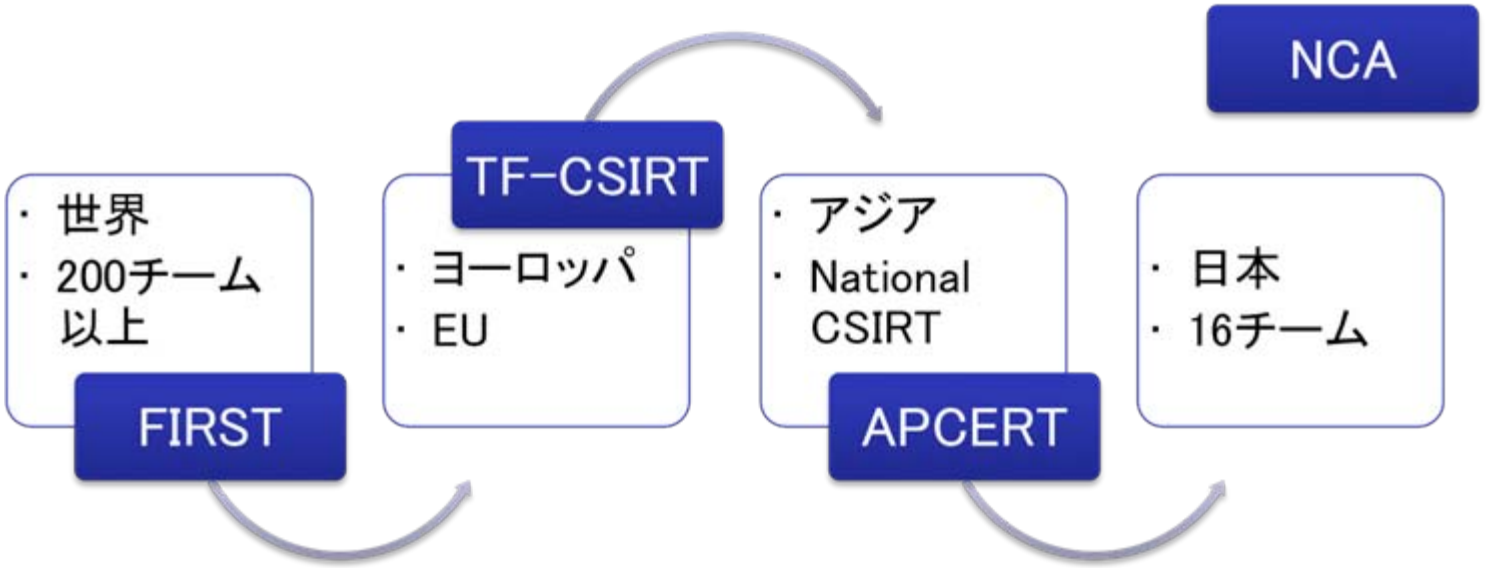
日本のCSIRTの歴史

CSIRT 日本シーサート協議会

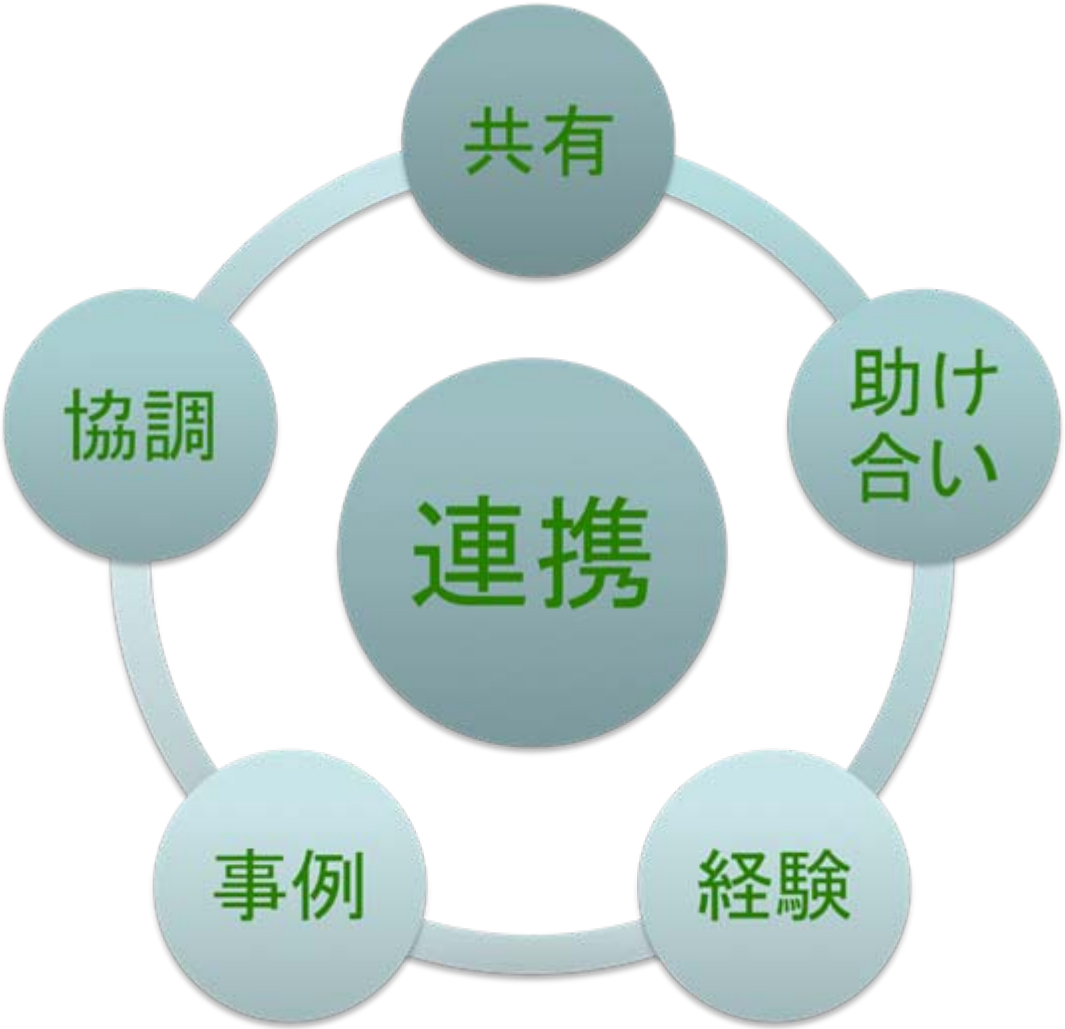
CSIRTのパターン



様々な協力関係



連携の意義



CSIRT 日本シーサート協議会

ご清聴ありがとうございました。

以下お気軽に相談ください。

CSIRTに関する相談: csirt@nca.gr.jp

NCAおよび加盟に関して: nca-sec@nca.gr.jp

CSIRT
日本シーサート協議会

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

補足:リファレンス

- History of JPCERT/CC
  - http://www.jpcert.or.jp/magazine/10th/index.html
- 立ち上げの頃の話(JPCERT/CC)
  - http://www.jpcert.or.jp/magazine/10th/beginning.html