NTT Secure Platform Laboratories
NTT セキュアプラットフォーム研究所

Network Security Forum 2013パネルテーマ「最近のサイバー攻撃に対する企業の自己防衛策」NTT-CERTにおける現状および課題

2013年1月25日

NTT-CERT 仁佐瀬剛美

アジェンダ

- NTT-CERTについて
  - 組織の紹介、活動概要
- NTT-CERTにとってのサイバー攻撃の意味
  - 一企業のインシデント対応支援組織としての現状および課題
  - インフラ会社のインシデント対応支援組織としての現状および課題
- あると嬉しいもの

NTT-CERTについて

・NTT-CERTは、

-NTTグループのCSIRT(Computer Security Incident Response Team)として、以下を実施

- 国内外のCSIRTやセキュリティ専門家との連携
- NTTグループに関連するセキュリティインシデント情報受付やインシデント対応支援
- その他、NTTグループのセキュリティレベル向上の支援

-NTT持株会社 NTTセキュアプラットフォーム研究所が中心となって運営(2004年～)

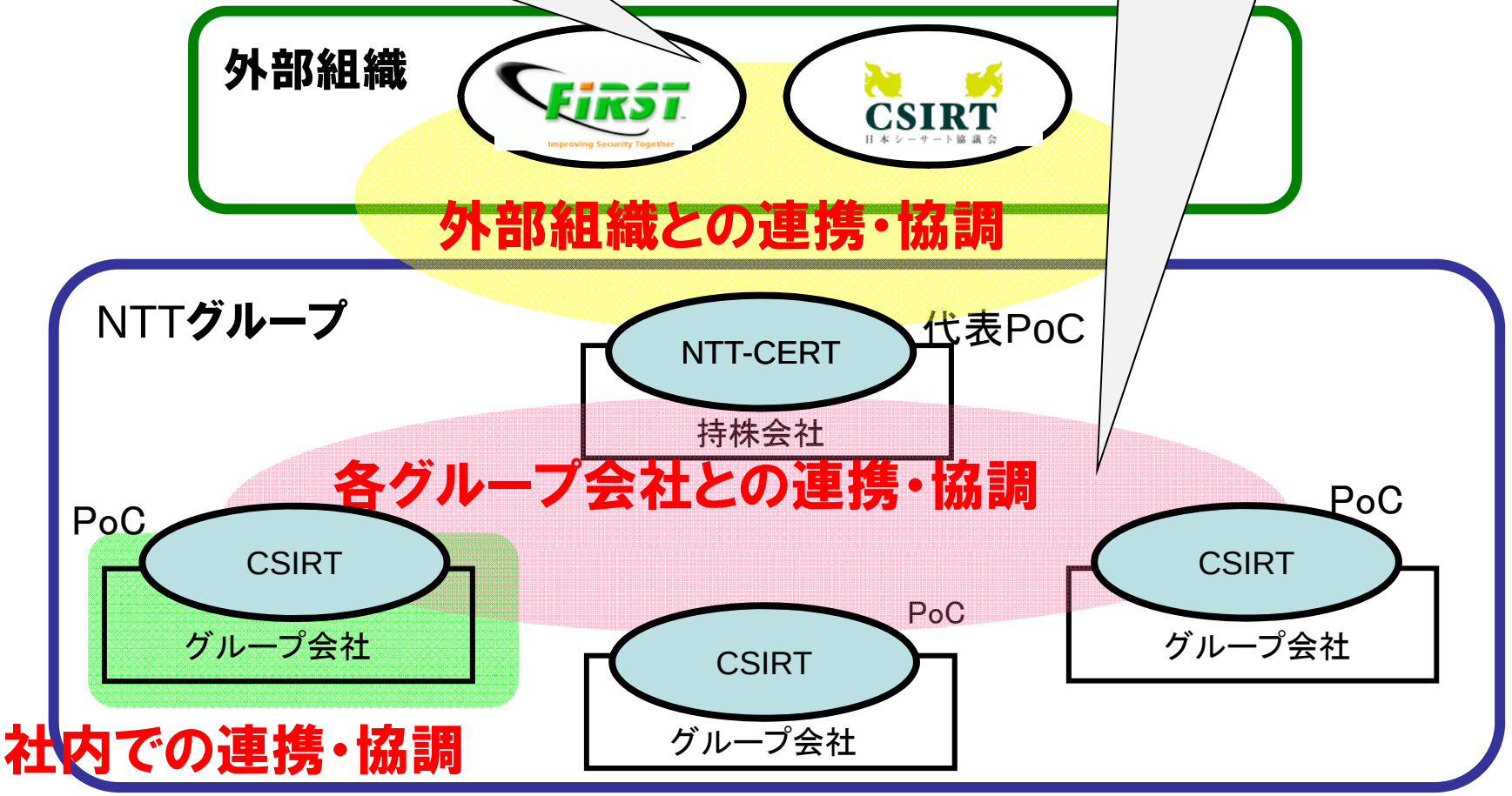
→企業内のCSIRT組織によるセキュリティの取り組み、インシデント対応支援が「自己防衛策」の一つ

参考： 外部向けサイト http://www.ntt-cert.org/

NTT-CERT活動概要 内外の連携

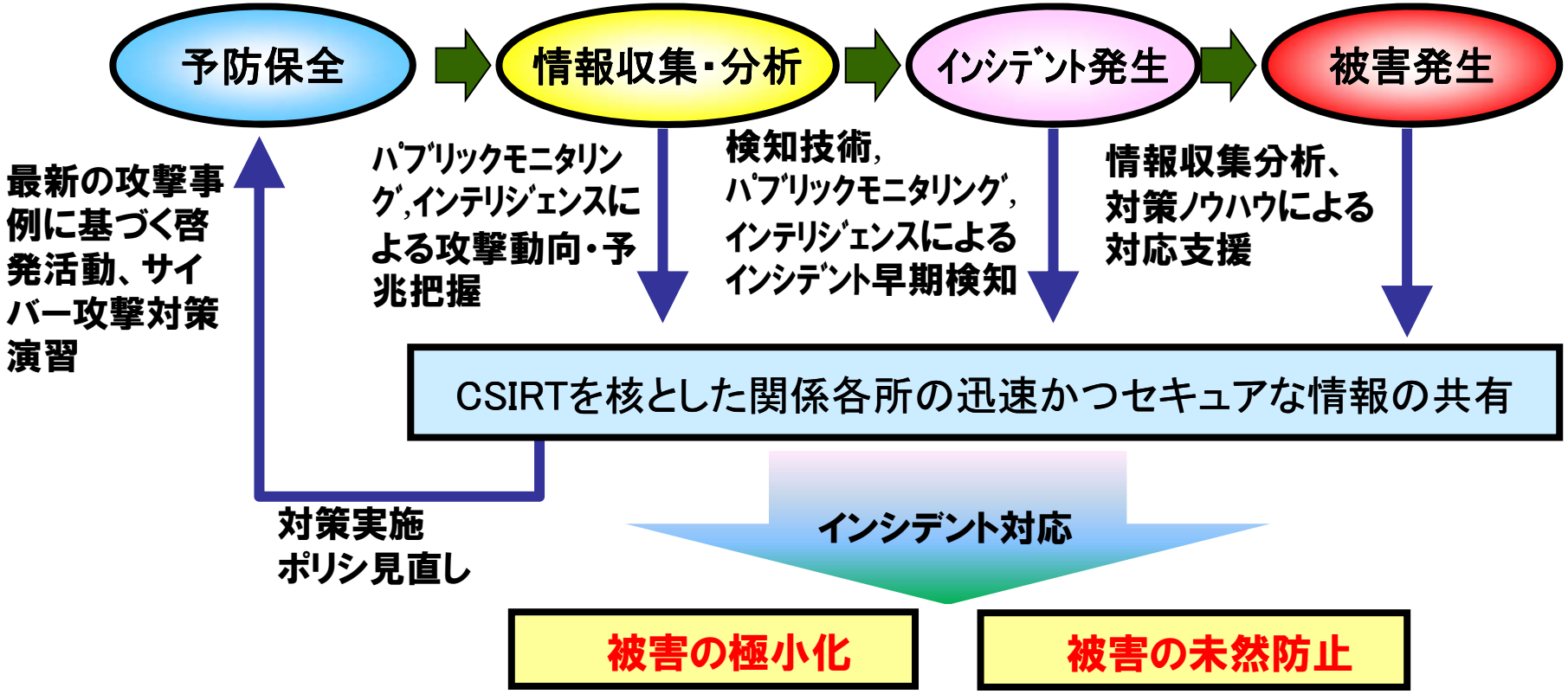
・協力関係の形成。
・最新情報の流通と情報の共有。
・ノウハウの吸収。

・インシデント対応支援。
・セキュリティ情報、ノウハウの蓄積・提供。
・研究開発（セキュリティ技術、インシデント分析、運用技術等）



NTT-CERT活動内容

- セキュリティマネジメントサイクルの各フェーズで、被害の極小化と未然防止に向けて取り組み中
- 研究所のセキュリティ研究成果、ノウハウを適用するとともに、得られた知見をセキュリティ研究にフィードバック



NTT-CERTにとってのサイバー攻撃の意味

- NTT-CERTは以下のような複数の側面を持ち、それぞれの立場でサイバー攻撃対応上の課題が存在
  - 一企業のCSIRT：NTTグループ内で発生したインシデント対応支援、セキュリティ相談対応のための組織
  - インフラ会社のCSIRT：NTTグループが提供するNWインフラサービスで発生したインシデント対応支援組織
  - NTT持株研究所内のセキュリティ研究組織：セキュリティ対策技術やマルウェア分析技術の研究ネタの実践の場、情報収集の場（今回の議論の対象外）

一企業のCSIRTとして 1/2

・対処方針：基本に忠実であること（近道はない）
  - パッチの徹底、危険なアプリの禁止
  - 不要な入口を塞ぐ
  - 最も脆弱な「人」に対する訓練、啓発活動
  - インシデントを検知した際の速やかなエスカレーション
  - 脆弱性、攻撃情報の収集分析、関係者への共有
  - 定期的なチェックの徹底
  - ・・・

一企業のCSIRTとして 2/2

- 課題
  - 複雑化する様々な攻撃への対応(0-day攻撃、標的型攻撃)
    - →出口対策、ログ分析体制の強化を図っているが、攻撃の高度化に対応しきれているか、発生しているかもしれないインシデントを見つけることができるのか、常に不安・・・
  - スマートフォン、BYOD、クラウド、SNSなどの新たなICT環境への対応
    - →入口、出口の増大に合わせたルールの強化/見直しは図っているが、確実にルールを守ってもらえるか、入口、出口の見落としはないか・・・

インフラ会社のCSIRTとして 1/2

- 対処方針: 以下の二つのインフラへの脅威に対してNTTグループ内のCSIRT連携を進め、被害・影響を少しでも低減する体制を強化
  - 大規模サイバー攻撃などに伴うインフラへの影響
    - インターネット上のサイバー攻撃情報や、トラヒック情報などからの攻撃予兆の把握
    - 発生したインシデントに対する対応支援、分析支援
    - 上記を実現するための、NWセキュリティ技術の研究開発
  - インフラ自身への攻撃
    - 電気通信事業者向けのガイドラインに基づくNW機器、サーバ類のセキュリティ強化支援
    - インターネット上の情報や、トラヒック情報などからの攻撃予兆の把握
    - 発生したインシデントに対する対応支援、分析支援
    - 上記を実現するための、NWセキュリティ技術の研究開発

インフラ会社のCSIRTとして 2/2

- 課題
  - インフラ固有の課題
    - 攻撃成功時の影響の大きさ、他のインフラへの影響・・・
  - 大規模サイバー攻撃リスクの増大
    - ハクティビストによるサイバー攻撃が増大し、常に世界中でサイバー攻撃が発生し情報が氾濫している状態で、狼少年にならずに攻撃の予兆を把握できるか・・・
  - インフラへの攻撃手法の高度化
    - 制御系システム固有の構成、運用を狙った攻撃手法への耐力向上、検知・遮断技術の導入がタイムリーに実施できるか、それらを支援できるか・・・

あると嬉しいもの

- 様々な課題はありますが、迅速かつ適切に関係各位と調整を進めていくためにあると嬉しいもの
  - 脅威情報、対策情報の信ぴょう性の確保：いわゆるお墨付き
  - 日々状況が変化していく中での、脅威レベルの定量性の確保： 最低限、これだけは対処すべきという目安、そのためのインシデント情報の共有の推進

以上