インシデントレスポンスに係る情報共有の現状と課題

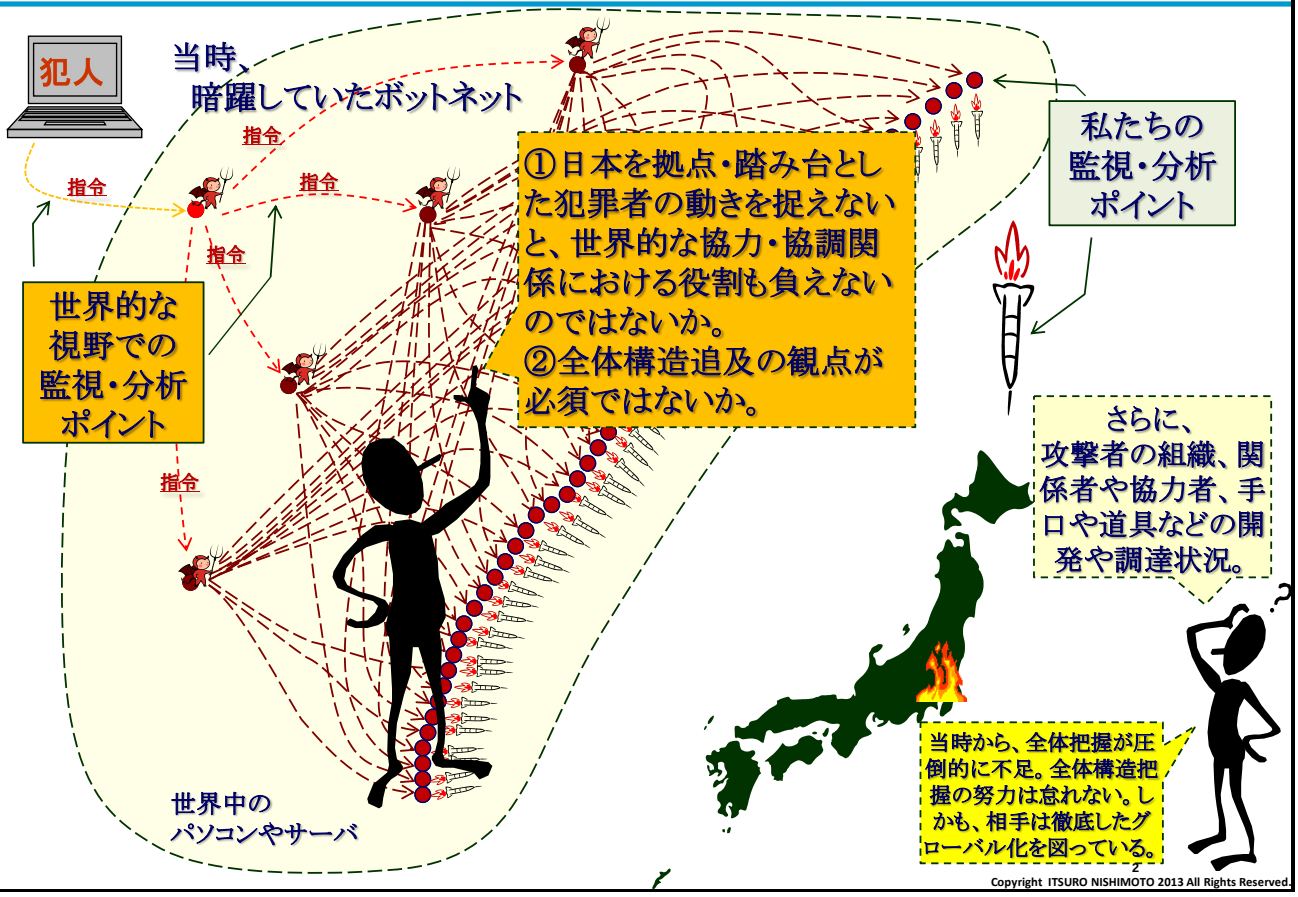
～周回遅れの対策～

2013年8月6日
株式会社ラック
CTO 西本 逸郎
http://www.lac.co.jp/

本書は、西本逸郎個人の意見であり、株式会社ラックや、所属・関係している団体等の意見を代表したものではありません。

また、内容も社会一般に対するものではなく、趣旨と背景をご理解頂いている範囲でのお取扱を、お願いいたします。

1. そもそも 2007年頃の話題。



2. 緊急対応事案でおきること

1）証拠保持に関して

2）調査における基本姿勢

3）他組織との連携や相談

4）情報や対策の共有、及び協調と連携

5）事故現場で耳にすること

2. 緊急対応事案でおきること・・・ 1）

1）証拠保持に関して

→ 証拠消失

→ 調査拒否

→ 自己過剰調査

① 訓練の実施

事件発生時のプロセスと必要対策を意識した訓練が必要

② 演習の実施

同時に、現状の実態確認を兼ねての演習は有効的

③重過失や故意の消失

証拠保持重要性の訴追だけでは足りないのではないか。

4

2. 緊急対応事案でおきること・・・ 2）

2）調査における基本姿勢

→ 個人情報流出は意識が高い。

→ 逆に、他への興味は薄い。

→ 多くは最低限。事業再開がポイント。

① 概ね複数の事案が複合

ログがある限りは調査する。

② 原因把握と再発防止優先

原因を把握できると、再発防止策への切り替えが一般的。

被害範囲の把握は、内部と外部では対応が違う。

③ 拡散防止や社会的封じ込め

あまり興味がない。

5

2. 緊急対応事案でおきること・・・ 3)

3) 他組織との連携や相談
→ 監督官庁、警察、業界団体
→ IPA、JPCERT

① 有効性

民は、法律上の縛りが無ければ、まずやらない

② メリットより、まずはデメリットを考慮

情報流出。メディアなどに叩かれるリスク
やはり、情報共有のガイドが必要か

③ 仕事が増える。

再開が遅くなる。費用負担。

6

2. 緊急対応事案でおきること・・・ 4)

4) 情報や対策の共有、及び協調と連携
→ もちろん、他での情報は欲しい。
→ やはり、情報活用と情報管理。

① 単独で、組織犯への対抗は困難

相手のグローバル化は常態化

② 縦割り・業界割りの弊害

攻撃側には、基本的に監督官庁や業界の意識はない。

③ 点としての事件対応では追いつかない

④ 点(通常の対応)を線へ

努力は必須だが。誰が、どこでやる？

7

2. 緊急対応事案でおきること・・・ 5)

5)事故現場で耳にすること

→ 子会社、委託先に任せている。
→ 何故か、事件後は慎重に。
→ 対策は理解したが運用できない。
→ ※ 内部ヒアリング中

国としてのサービス

時折、組織犯や国家レベルの攻撃に対して、普通の会社が自分の経費で対策が必要なのか意味が分からない。国としてのサービスをどう考えているのか等の声はよく耳にする。

2. 緊急対応事案でおきること・・・ 6)

6)事故現場で遭遇する種々の壁

① 契約の壁:「契約がないと、、、」
② 組織の壁:「うちの担当では、、」
③ 業者の壁:「うちの契約では、、」
④ 会議の壁:「関係会社10社、参加者30名、3時間」
⑤ 仕切の壁:「インシデントの仕切はラックさんで、、」
⑥ 技術の壁:「話が専門過ぎて、、」
⑦ 運用の壁:「知識のある人間をアサインできません」
⑧ 継続の壁:「喉もと過ぎれば、、」
⑨ 予算の壁:「・・・」

3. 恐らくは必要なこと 1)

1)フォレンジック

→ PC、サーバ、スマホ、タブレット
→ 組み込み、制御機器
→ 仮想環境、ファームの乗った機器

① 証拠保全 手順確立、決裁、監査
② 一次フォレンジック(マニュアル的)
③ 二次フォレンジック(腕、ビッグデータ)
④ マルウェアの取り出し
⑤ 対象デバイス、新デバイスへ
⑥ 質と規模への対応。教育、訓練、演習。

3. 恐らくは必要なこと 2)

2)マルウェア、プログラム解析

① 検体の一次解析(動的解析)
→ 判定、接続先など、基本機能、AV
② 検体解析(静的解析)
→ 機能解析
③ 対象デバイス、新デバイス
④ 質と規模への対応。教育、訓練、演習。

3. 恐らくは必要なこと 3)

3)道具や手口

→ 脆弱性、POCなどの収集(既)

→ ツールや情報サイトの調査(既)

→ 汚染サイトや汚染PCの情報収集

① 攻撃検出と防御方法

② 痕跡研究

③ 攻撃や痕跡からの逆引き

3. 恐らくは必要なこと 4)

4)攻撃者のモニタリング・プロファイリング

→ 使用道具、手口

→ 汚染されたサイトやPCへの使用動向

→ 状態や動向の追跡

① 民でやるとすれば研究機関

一般的には動機はない。

情報提供サービス？？？

3. 恐らくは必要なこと 5)

5)匿名化システムへの対抗
→ TORノード調査、動向把握
→ TORシステム調査
→ ログ解析、ビッグデータなど

① 少なくとも民には調査動機はない

少なくともビジネスにはならない

3. 恐らくは必要なこと 6)

6)全体構造の把握と整備への模索
→ ボトムアップ。事件捜査、事件対応
→ トップダウン。全体把握。
→ 点と線を繋ぐ。インテリジェンス？

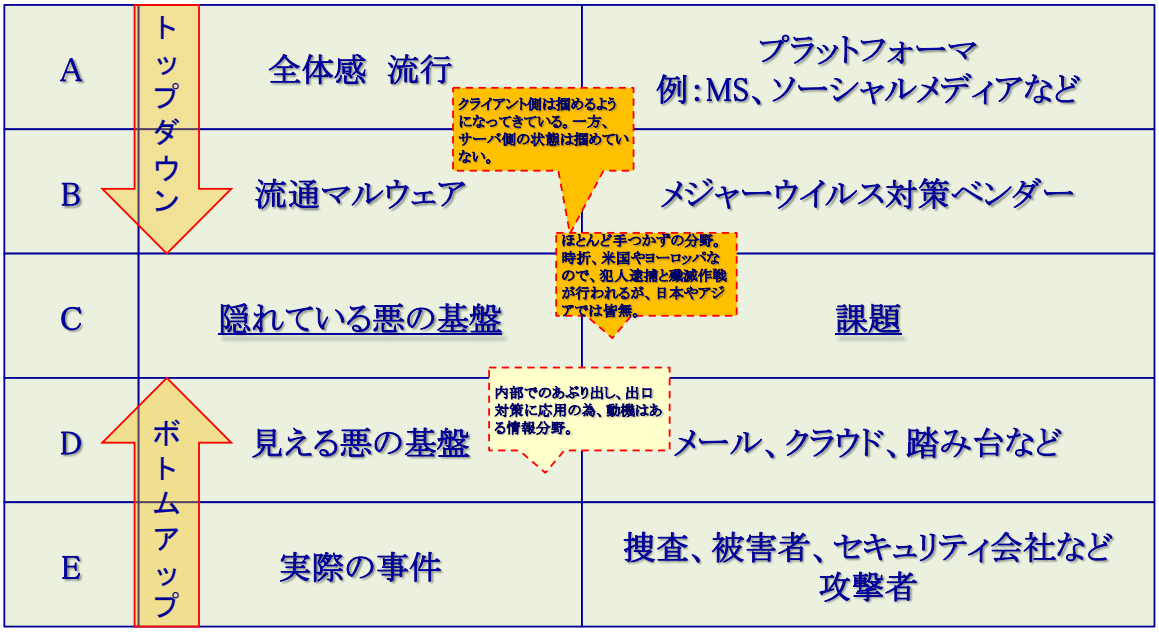
① 影響ある事件が起きれば動く

そこからのキックオフでは間に合わない。対症療法

② 事件にならないことは誰も動かない

官レベルだけではなく民レベルでの国際連携は必要
他国への影響、攻撃への準備、狙いなどは追えないと

3. 恐らくは必要なこと 6)



4. 恐らくは必要なこと 7)

7) 実証実験が必要では。例えば、、
- → 大規模改ざんの全体把握
- → オンラインバンキングの背後調査
- → リスト攻撃の実態把握

① 民間主導

② 全ページのA～Eでの協調・連携模索

③ 活動母体をどうするか
- → 学、中立専門団体？
- → 小さく始めたほうが良い。
- → いずれにせよ、一流人材をひきつける活動は必須では。

④ メディア連携しても良いかも。

ありがとうございました。

Any question ?

1

産官学の連携について

- 東京工業大学　尾形わかは
- 教育機関からの要望
- 研究機関として、今後の可能性と課題

2013/8/6

2

教育機関として望むこと

- 情報セキュリティ
  - サイバーテロなどの外部脅威
  - 内部の脅威
- 情報セキュリテイ教育には、過去の攻撃事例・事故事例の詳細が不可欠
- 現状では、公表されている情報から対策を議論するのは難しい

2013/8/6 3

研究機関として、今後の可能性
（暗号理論の場合）

暗号理論

- 基本：暗号化・メッセージ認証・本人認証・ディジタル署名
- 応用：暗号プトロコル

暗号プトロコルとは

- 基本ツールを組み合わせることで、様々なサービスを実現
- 複数組織が、それぞれの秘密情報を秘密に保ったまま、それらの情報から導かれる値を計算する

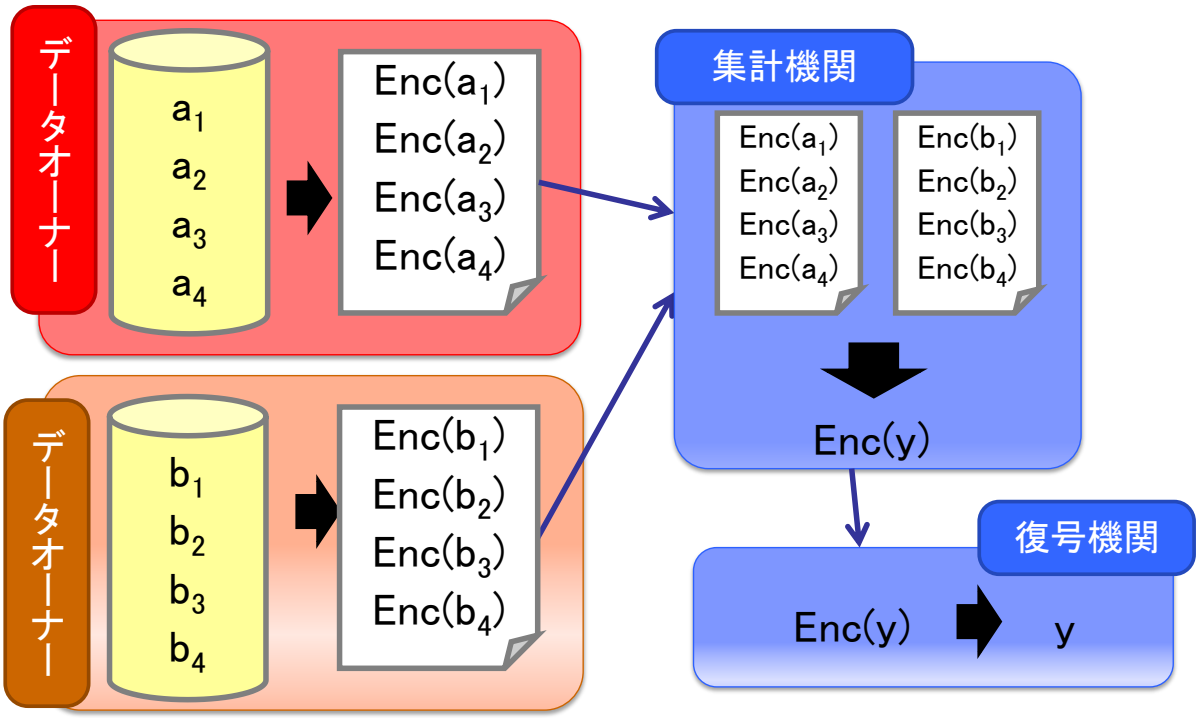
問題点

- 社会でのニーズが把握できていない

2013/8/6 4

準同型暗号を利用した暗号プロトコルの例

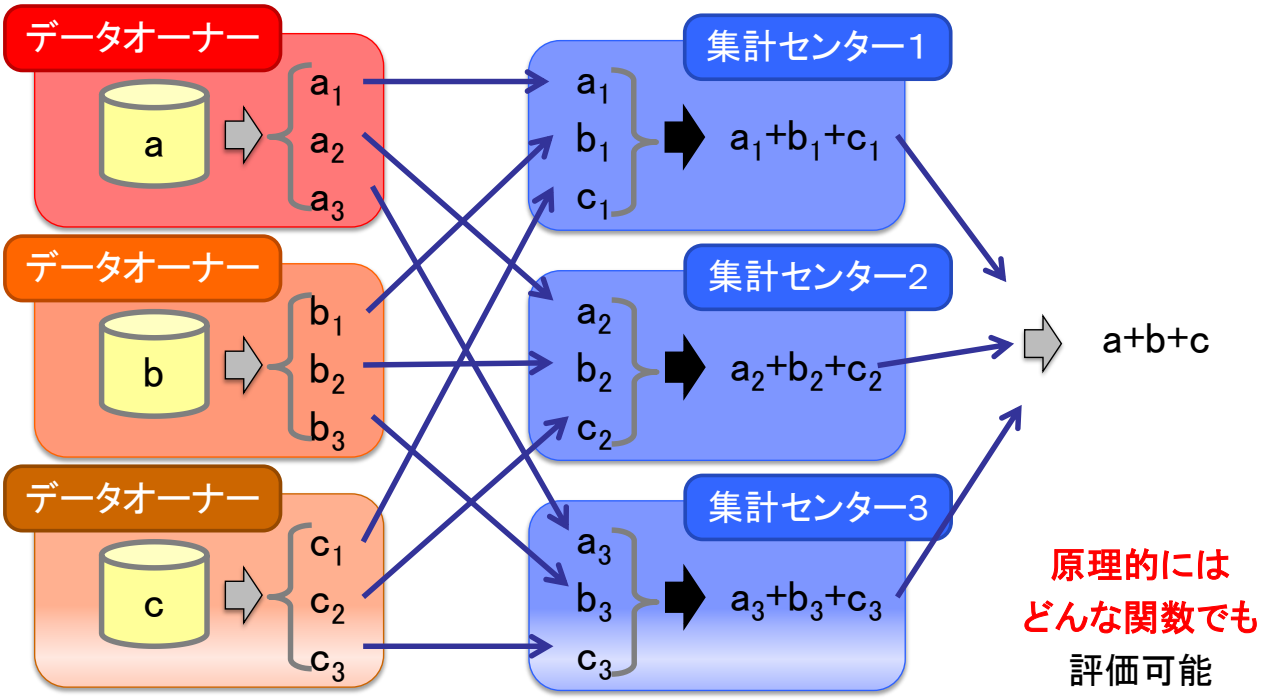
データ a1,...,a4, b1,...,b4 の統計量 y を得たい場合



2013/8/6 5

秘密分散を利用した暗号プロトコルの例

データ a, b, c の合計のみを知りたい場合



原理的には
どんな関数でも
評価可能

2013/8/6 6

課題

原理的には

- 準同型暗号を用いる場合も、秘密分散法を応用する場合も、どんな関数でも評価可能

現実的には

- 複雑な計算式の場合、計算処理が重く、非現実的

ニーズ把握の必要

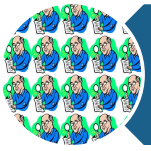
- 実際にどのようなデータからどのような値を抽出したいのか、要求に応じて効率化できれば、実用化できる

技術系職種

- ウイルス解析者
  - ウイルス解析及びパターンファイル作成・テスト等
- 脅威リサーチャー
  - 特定脅威に対する調査、監視、情報収集
- セキュリティコンサルタント
  - **コンサルティング、データ分析、セールスツール作成**
- System　Engineer
  - 製品実装設計・支援、セールスツール作成、データ分析
- テクニカルサポートスタッフ
  - 製品技術アフターサポート、製品仕様フィードバック
- プログラム開発者
  - 製品仕様設計、コーディング、QA

抱える課題

スペシャリストと言う事

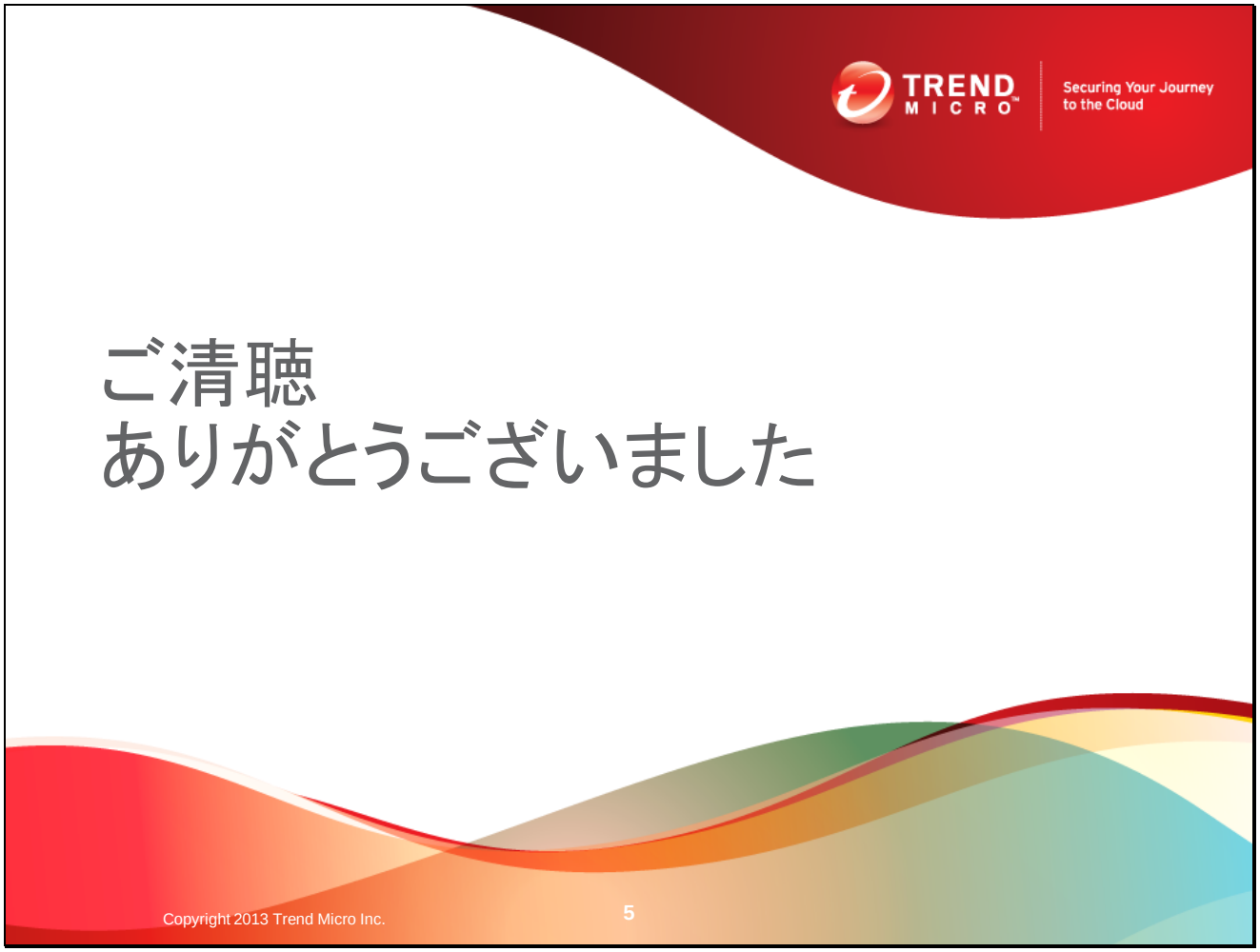


年をとると言う事

新卒採用において

国際化（Globalization）

NCFTAに掛ける期待


TREND MICRO
Securing Your Journey to the Cloud
ご清聴
ありがとうございました
Copyright 2013 Trend Micro Inc.
5

HITACHI
Inspire the Next

日立グループのCSIRT活動における海外の関係機関等との連携

2013/09/06

寺田真敏
Hitachi Incident Response Team
http://www.hitachi.co.jp/hirt/

1 日立グループのCSIRT活動 ～コンセプト～

Hitachi Incident Response Team

HIRTとは

- HIRT (Hitachi Incident Response Team) は、インターネットコミュニティとの連携による迅速なインシデントオペレーション (脆弱性対策ならびにインシデント対応) を通して、**安心かつ安全なネットワーク環境の実現に寄与することを目的とした活動**である。

脆弱性対策：セキュリティに関する脆弱性除去のための早期解決活動
日立製品ならびに日立関連サイトに関連する脆弱性の存在を指摘された場合、外部の製品ならびにサイトに脆弱性を発見した場合など

インシデント対応：実際に発生している侵害活動を回避するための早期解決活動
侵害活動の要因ならびに助長する痕跡が指摘された場合、侵害活動の脅威を除去するための協力を依頼された場合、外部のサイトに侵害活動の要因ならびに助長する痕跡を発見した場合など

シーサート (CSIRT)
Computer Security Incident Response Team
コンピュータセキュリティにかかるインシデントに対処するための組織の総称 (機能)

 2

1 日立グループのCSIRT活動 ～コンセプト～

Hitachi Incident Response Team

HIRTセンタとは

- HIRTセンタは、情報セキュリティのインシデントオペレーションの企画・調整部門であり、社外IRT組織との連携を図りながら、日立グループの各部門に対し、脆弱性対策情報とインシデント対応情報を効率的に流通させることで、社内外のシステムを脆弱性ならびにインシデントから守るための対策推進を支援する組織である。
- 1998年に開始したHIRTプロジェクトを引き継ぎ、HIRTの実行的な組織として、2004年10月に設立された。

広義のHIRTとは、
＝HIRTセンタ＋製品ベンダIRT＋SIベンダIRT＋社内ユーザIRT
＝日立グループ全体で推進するIRT活動

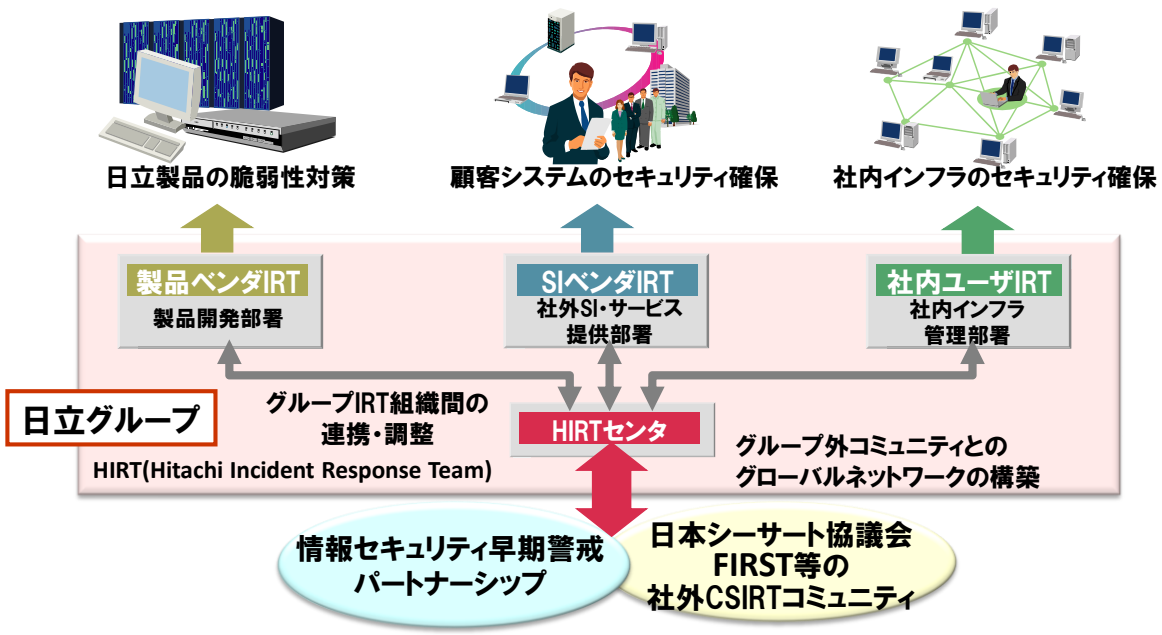
狭義のHIRTとは、
＝HIRTセンタ
＝日立グループにおけるIRTの実行的な組織

2 日立グループのCSIRT活動 ～モデル化～

Hitachi Incident Response Team

CSIRT活動体制のモデル化

- 脆弱性対策とインシデント対応活動を支える4つのIRT（2001年）



3 日立グループのCSIRT活動 ～マイルストーン～

Hitachi Incident Response Team

CSIRT活動のマイルストーン

▼HIRTプロジェクト始動　▼HIRTセンタ開設

1998-2003	2004-2009	2010-2015
脆弱性対策・インシデント対応認知期	脆弱性対策・インシデント対応黎明期	脆弱性対策・インシデント対応定着期
均一的かつ広範囲に渡る単発被害 Webサイトのページ書き換え	均一的かつ広範囲に渡る連鎖型被害 ウイルス添付型メールの流布 ネットワーク型ワームの流布	すべてが異なる局所的な被害 標的型攻撃 戦術型攻撃
オペレーティングシステムの脆弱性	アプリケーションの脆弱性	ユーザの脆弱性
● 脆弱性対策・インシデント対応情報発信を通したIRT活動モデルの構築	● 4つのIRTをコンセプトとした仮想組織体制の整備による情報セキュリティ早期警戒パートナーシップへの対応 ● 海外IRT活動（FIRST、WARP）、国内IRT活動（日本シーサート協議会）参画を通した連携モデルの構築	● 技術、コンテンツ、管理連携による、ユーザエリア、製品・サービスエリアの一体化と脆弱性対策・インシデント対応に関する問題の低減 ● 海外ならびに国内IRT連携活動を通したトラストモデルの構築

4 日立グループのCSIRT活動 ～組織間連携～

Hitachi Incident Response Team

IRT活動の国内＆海外連携（組織間連携による問題の早期解決）

脆弱性情報の流通基盤の整備
- JPCERT/CC（2002～）JVN活動
- IPA（2004～）MyJVN活動

脆弱性ハンドリング
- JPCERT/CC（2002～）
- CERT/CC（米）（2002～）
- CPNI（英）（2003～）

インシデント観測／分析環境の整備
- Telecom-ISAC Japan（2005～）
- 東海大学、中央大学（2006～）共同研究
- MWS（マルウェア対策研究人材育成ワークショップ）（2008～）立上げ支援

インシデントハンドリング
- JPCERT/CC（2000～）
- FIRST（海外）（2005～）加盟
- 日本シーサート協議会（2007～）加盟

FIRST: Forum of Incident Response and Security Teams

脆弱性対策・インシデント対応のための体制強化

業種別
- 金融分野における先行的な取り組みとして、HIRT-FIS(Financial Industry Information Systems HIRT) を設置し、連携活動を開始（2012～）

ISP・セキュリティ・製品ベンダ
- NTT-CERT（2005～）定期会合
- TM-SIRT（トレンドマイクロ）（2012～）

海外組織
- WARP（英）（2007～）加盟
- Academy CERT（インドネシア）（2010～）立上げ支援

WARP: Warning, Advice and Reporting Point

●セキュリティ情報流通（コミュニティとの連携、協力関係の構築）
●信頼関係のあるコンタクトパスの確立

日立グループ窓口一本化による連携体制

HIRT センタ

日立グループへの／からのフィードバック

5 日立グループのCSIRT活動 ～脆弱性対策～

Hitachi Incident Response Team

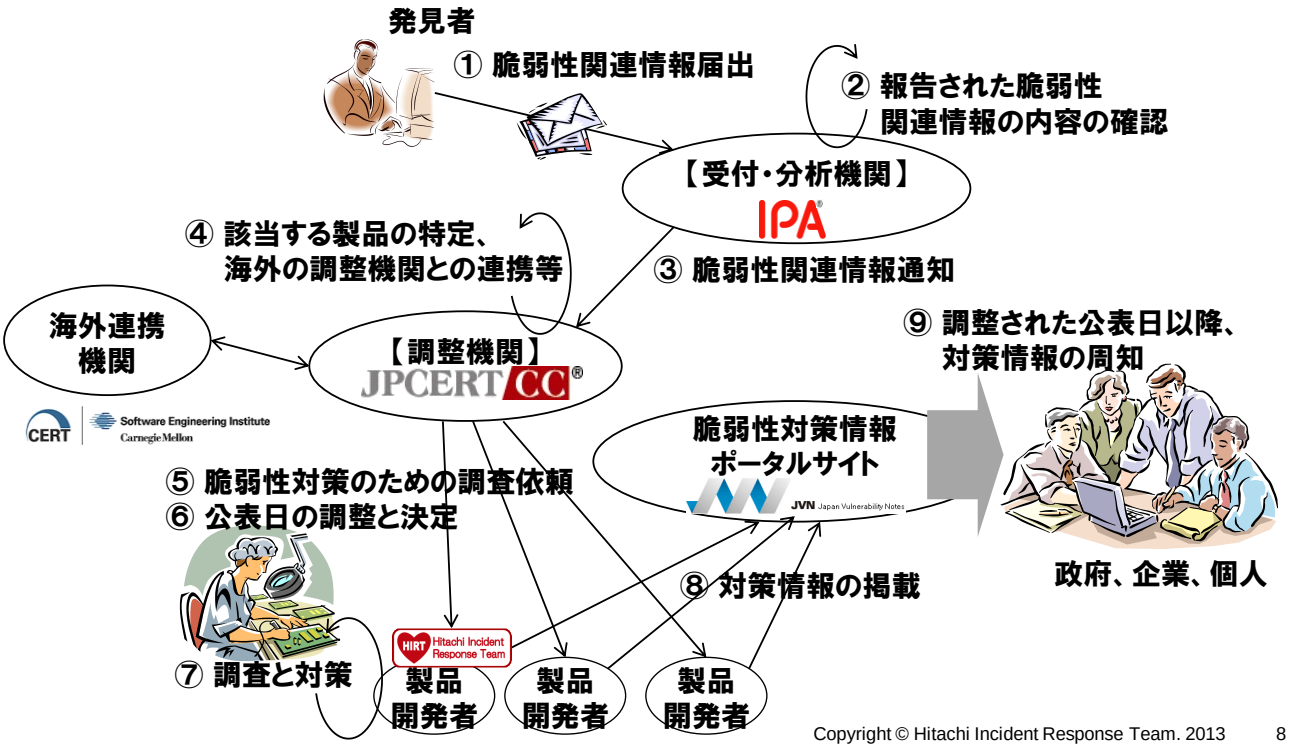
脆弱性ハンドリング

- 脆弱性情報の受信、脆弱性対策情報の発信
  - 2002 年10月～ CERT/CCとの連携
    CERT/CC Vulnerability Disclosure Policy に基づく情報入手
    CERT Vulnerability Notes Databaseへの日立対応情報の掲載
  - 2003年9月～ NISCC (現CPNI) との連携
    NISCC Vulnerability Disclosure Policy に基づく情報入手
    NISCC Vulnerability Advisoryへの日立対応情報の掲載
  - 2004年7月～ 情報セキュリティ早期警戒パートナーシップへの参画
    パートナーシップに基づくIPA/JPCERT, CERT/CC, NISCCの情報入手
    Japan Vulnerability Notes (JVN) サイトへの日立対応情報の掲載
- 脆弱性除去の推進＝＞インターネットコミュニティへの貢献
  - 2003年07月21日 CERT/CC に報告 ⇒ Vulnerability Note VU#694428
    Apache stops writing access/error logs after processing "Request-URI" containing "0x1A" characters
  - 2005年03月14日 IPA/JPCERTに報告 ⇒ JVN#DD18AD07
    Tomcat におけるサービス拒否の脆弱性

5 日立グループのCSIRT活動 ～脆弱性対策～

Hitachi Incident Response Team

参考：情報セキュリティ早期警戒パートナーシップ



6 日立グループのCSIRT活動 ～インシデント対応～

Hitachi Incident Response Team

海外の関係機関等との連携における日本版NCFTAへの期待

- 情報セキュリティ早期警戒パートナーシップは、脆弱性ハンドリングを、仕組みという形で実現した。
  - 脆弱性ハンドリングを仕組みとして説明できる。
    ⇒シーサート関係者以外の方も理解しやすい。
  - 直接コンタクトパスを持っていない海外の関係組織にリーチできる。

- 日本版NCFTAは、インシデントハンドリングのうち、サイバー犯罪ハンドリング（公共の秩序・治安という観点が必要なハンドリングと定義）を、仕組みという形で実現できる、と想定した場合、
  - サイバー犯罪ハンドリングを仕組みとして説明できる。
    ⇒シーサート関係者、シーサート関係者以外の方も理解しやすい。
  - 直接コンタクトパスを持っていない海外の関係組織にリーチできる。
    ⇒海外進出した地域で発生したサイバー犯罪ハンドリングの支援施策として活用できる。

 9

HITACHI
Inspire the Next