NTTグループの情報セキュリティリスクに対する取り組み

～ R&Dの視点から ～

2008年2月20日

NTT情報流通プラットフォーム研究所

大久保 一彦

<Table of Contents>

１．はじめに

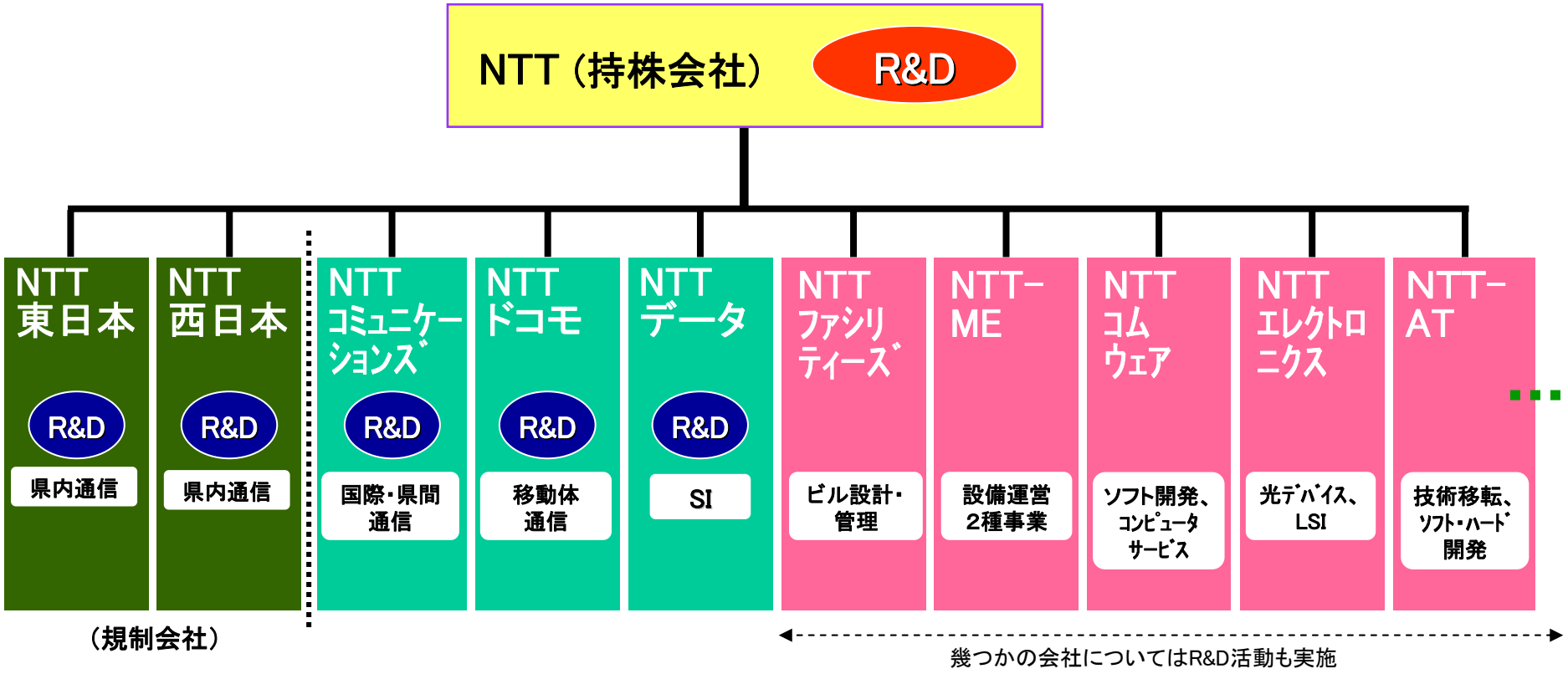
～NTT研究所について～

NTTグループにおけるR&Dのフォーメーション

R&D **基盤的研究開発**
- ●新サービス実現のための共通基盤技術
- ●新原理、新部品等を生み出す基礎・要素技術

R&D **応用的研究開発**
- ●システム改良
- ●カスタマイズ等

人員：約6,000名
費用：約3,000億円



NTT研究所の拠点

（★:研究所企画部の所在地）

京阪奈

★コミュニケーション科学基礎研究所

武蔵野研究開発センタ

■情報流通基盤総合研究所
- ★サービスインテグレーション基盤研究所
- ★情報流通プラットフォーム研究所
- ★ネットワークサービスシステム研究所
- ☆環境エネルギー研究所
- ☆サイバーソリューション研究所
- ☆サイバースペース研究所
- ☆未来ねっと研究所

大手町（東京）

・持株スタッフ部門
（研究企画部門）

筑波研究開発センタ

★アクセスサービスシステム研究所

幕張

☆アクセスサービスシステム研究所

横須賀研究開発センタ

■サイバーコミュニケーション総合研究所
- ★サイバーソリューション研究所
- ★サイバースペース研究所
- ☆ネットワークサービスシステム研究所
- ☆アクセスサービスシステム研究所
- ★未来ねっと研究所

厚木研究開発センタ

■先端技術総合研究所
- ★マイクロシステムインテグレーション研究所
- ★フォトニクス研究所
- ★物性科学基礎研究所
- ☆コミュニケーション科学基礎研究所
- ★環境エネルギー研究所

NTT研究所の構成

サイバーコミュニーケーション総合研究所

サイバーソリューション研究所	情報流通ビジネスのための共通プロダクトとサービス基盤の研究開発等
サイバースペース研究所	情報流通ビジネスの発展に資するコンテンツ流通要素技術の研究開発等

情報流通ビジネスアプリケーション用の新たなプロダクトの創出

情報流通基盤総合研究所

サービスインテグレーション基盤研究所	戦略的企画、NWアーキテクチャ及び通信トラヒック・品質技術の研究開発、研究所横断的な研究開発推進等
情報流通プラットフォーム研究所	各種情報流通ネットワークサービスにおいて、共通的な構成要素となるプラットフォームの研究開発等
ネットワークサービスシステム研究所	ネットワークサービス及びそれらを実現するネットワークの高度化の研究開発等
アクセスサービスシステム研究所	情報流通ビジネスの基盤となる新たなアクセスサービスの創出とそれを支えるアクセスネットワークの実現等
環境エネルギー研究所	環境情報技術（環境IT）、環境を考慮したエネルギーシステムの研究開発等

グループの情報流通ネットワークサービスの創出

先端技術総合研究所

未来ねっと研究所	革新的通信方式に基づくネットワークシステムの研究開発等
マイクロシステムインテグレーション研究所	ユビキタスサービスに革新をもたらすデバイス、モジュール、サブシステムの研究開発等
フォトニクス研究所	通信・情報分野に大きな技術革新をもたらす光・電子部品、モジュール及び材料の研究開発等
コミュニケーション科学基礎研究所	情報通信に変革をもたらす知識処理、メディア処理など新しい知見や概念の創出等
物性科学基礎研究所	速度・容量・サイズなどネットワーク技術の壁を越える新原理・新コンセプトの創出等

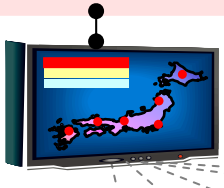
情報通信に全面変革をもたらす新原理・新コンセプトの創出、及び5～10年先の事業領域拡大につながる先端技術の研究開発

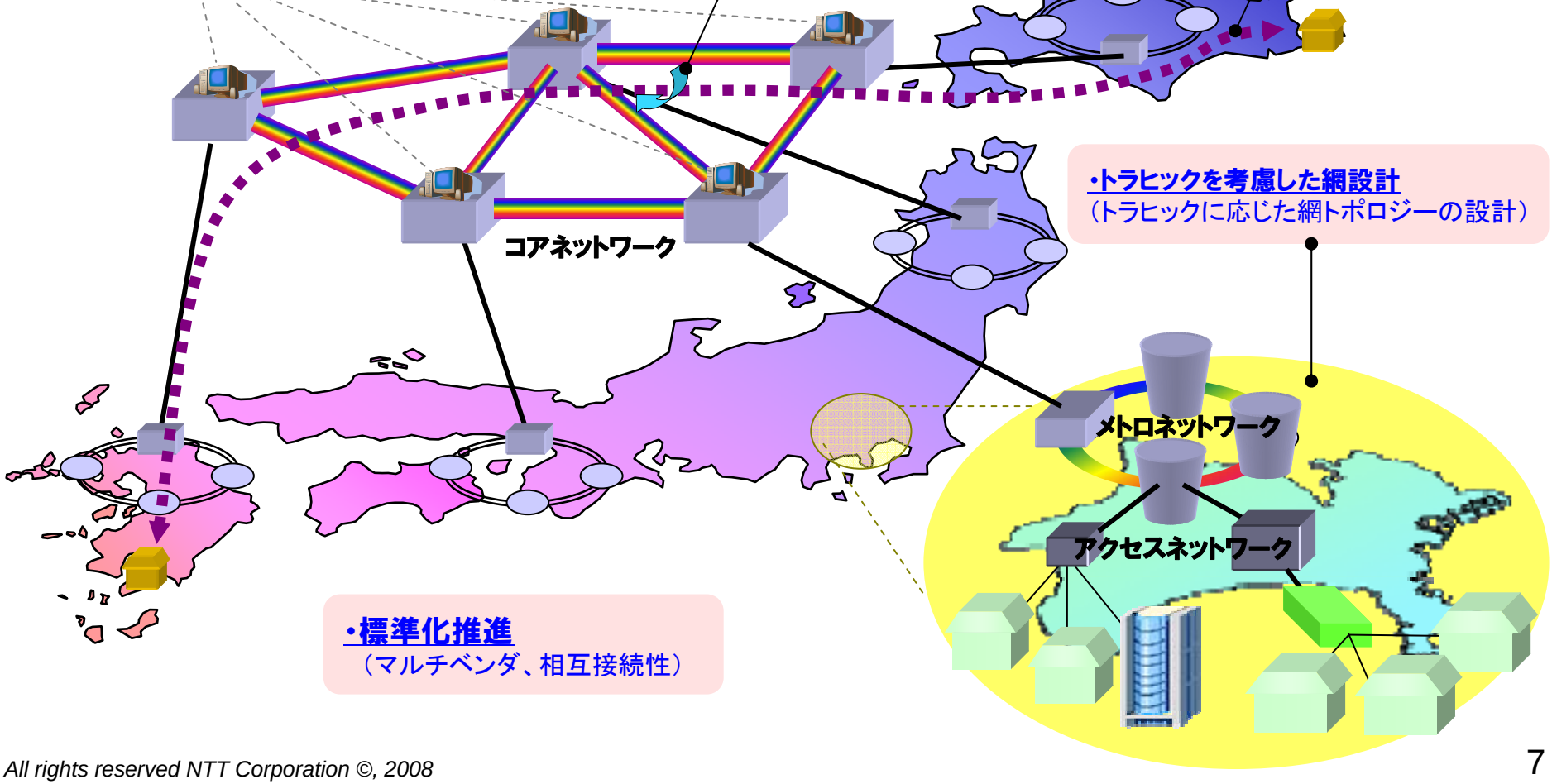
NTT研究所における“全体最適”を目指した研究

・ネットワークの一元的保守／運用
（ネットワーク、システムの監視／運用）

・ライフラインとしての接続性保証
（故障時の無瞬断切り替え／
サービス無中断ファイル更新）

・End-Endの品質保証
（ネットワークレベルでの
サービス品質[QoS]制御）



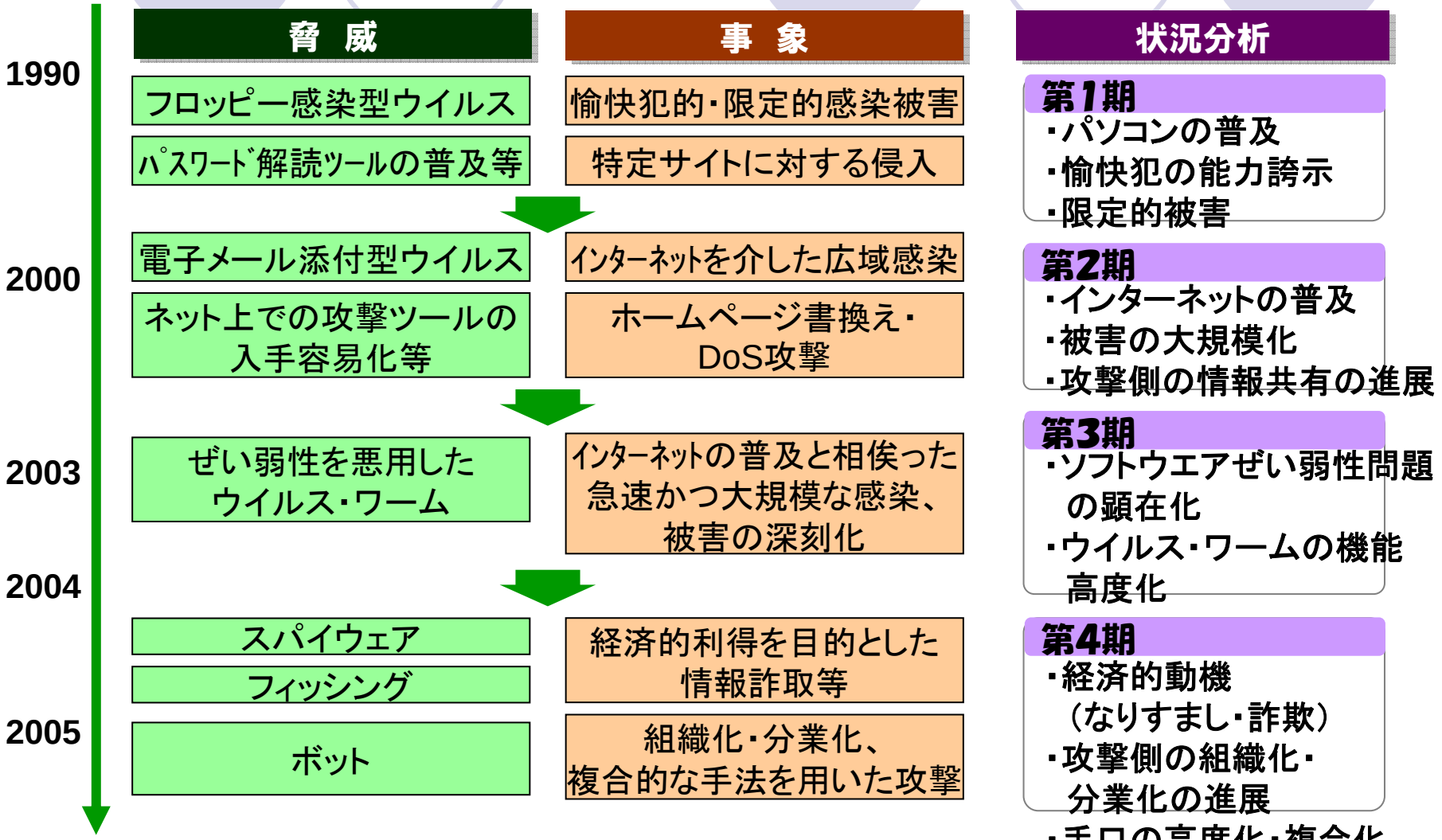


・トラヒックを考慮した網設計
（トラヒックに応じた網トポロジーの設計）

・標準化推進
（マルチベンダ、相互接続性）

2．情報セキュリティリスクへの取り組み

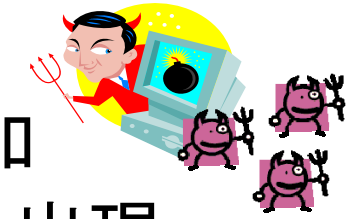
セキュリティ脅威の変遷



出典：「情報セキュリティの最新動向」, IPAX2007（2007.6.28）
http://www.ipa.go.jp/security/event/2007/ipax/IPAX2007-0628-11-Nakata.pdf

脅威と対策

- **最近のサイバー攻撃では、攻撃者は技術を駆使し、ますます巧妙になってきている・・・**
  - ○愉快犯から利益目的の窃盗団型に
  - ○Webアプリを媒体にするウィルスの増加
  - ○自らをアップデートして進化するボットも出現



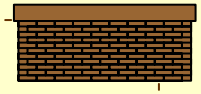
- **攻撃側の“分業化”や“プロ化”が進む中で、防御側も検知・分析技術を磨くとともに、組織連携して継続的にセキュリティ対策に取り組む必要がある。**

セキュリティリスクに対する取り組み

●セキュリティの視点では、システム等の構築時のみならず、システム構築後の**継続的な監視・対応**が肝要。

システムのセキュア化

- **システム要塞化**

例）防火壁 

- **検知から対策までの自動化**

例）スプリンクラー

リスクの更なる低減

セキュリティ運用の強化

- **事前対応** ⇒未然防止

例）夜番「火の用心」

- **事後対応** ⇒被害極小化

例）消火活動 

：アナロジー（火災を例に） 

システムのセキュア化に向けたR&D

- **システム要塞化**
  - 暗号アルゴリズム及び、ライブラリ
  - NGN構成要素のセキュア化
  - 各種認証機能の強化
    - ユーザ認証、サービス認証、時刻認証　等
- **検知から対策までの自動化**
  - 異常トラヒック対策技術
  - ボットネット対策技術
  - Webセキュリティ対策技術　等

NTT暗号・研究開発の歴史

暗号の社会的位置づけの変化

NTTでの暗号R&D

- 1985年　FEAL（共通鍵暗号）
  - 国内初の64ビット共通鍵ブロック暗号
  - DESよりも高速
- 1985年　ESIGN（署名）
  - 国内初のデジタル署名
  - RSAよりも高速
- 1998年　E2（共通鍵暗号）
  - 国内初の商用128ビット共通鍵ブロック暗号
  - 日本から唯一のAES暗号プロジェクトに応募
- 1999年　PSEC（鍵配送）、ECAO（署名）
  - 国内初の証明可能安全な楕円暗号
- 2000年　Camellia（共通鍵暗号）
  - 128ビット共通鍵暗号を三菱電機と共同開発
  - NTTの高速ソフトウェア実装技術と三菱電機の小型高速ハードウェア実装技術を融合
- 2003年　CRESERC（署名；仕様）
  - 三菱電機と日立製作所と共同で楕円デジタル署名ECDSAの実装仕様を規定

「規制すべき武器」

↓

「標準化すべき社会基盤技術」

NTT単独での高度な技術追求

↓

仲間作りを通じた競争力強化

NEWS RELEASE

NTT
日本電信電話株式会社

2006年4月13日

128ビットブロック暗号「Camellia」のオープンソースを公開
～多くの国際標準規格に採用された次世代国産暗号を広く使いやすいものに～

日本電信電話株式会社（本社：東京都千代田区、代表取締役社長：和田 紀夫、以下「NTT」）は、2000年に三菱電機株式会社（本社：東京都千代田区、執行役社長：下村 節宏、以下「三菱電機」）と共同開発した128ビットブロック暗号※1アルゴリズム「Camellia（カメリア）」のNTT製ソースコード（C言語版・Java版）を、オープンソースとして、本日（2006年4月13日）よりホームページ上にて公開いたします。主要な国際標準暗号・推奨暗号に選定された国産暗号がオープンソースとして提供されることは初めてのことであり、Camelliaを、日本発の暗号技術として安全な高度情報流通社会を支える国際的な基盤技術に広めていくとのNTTの方針に基づいて実施するものです。

なお、このソースコードは、従来ホームページ上で公開していた参照コードよりも約3倍（当社比）高速なものであり、オープンソースコミュニティに対して順次提供していく暗号エンジンとなる予定のものです。

Camelliaホームページ　：http://info.isl.ntt.co.jp/crypt/camellia/index.html
オープンソース掲載ページ：
http://info.isl.ntt.co.jp/crypt/camellia/source.html

NEWS RELEASE

NTT
日本電信電話株式会社

2006年11月8日

国産唯一の次世代国際標準暗号「Camellia」を オープンソースコミュニティOpenSSL Projectが採用

～ オープンソースライブラリとして組込・配布も自由にでき 世界的な普及促進に弾み ～

日本電信電話株式会社（本社：東京都千代田区、代表取締役社長：和田　紀夫、以下「NTT」）が2000年に三菱電機株式会社（本社：東京都千代田区、執行役社長：下村　節宏、以下「三菱電機」）と共同開発した128ビットブロック暗号※1アルゴリズム「Camellia（カメリア）」が、国際的なオープンソースコミュニティであるOpenSSL Projectが開発するSSL/TLS※2プロトコル用暗号ツールキットOpenSSL toolkitに採用されました。

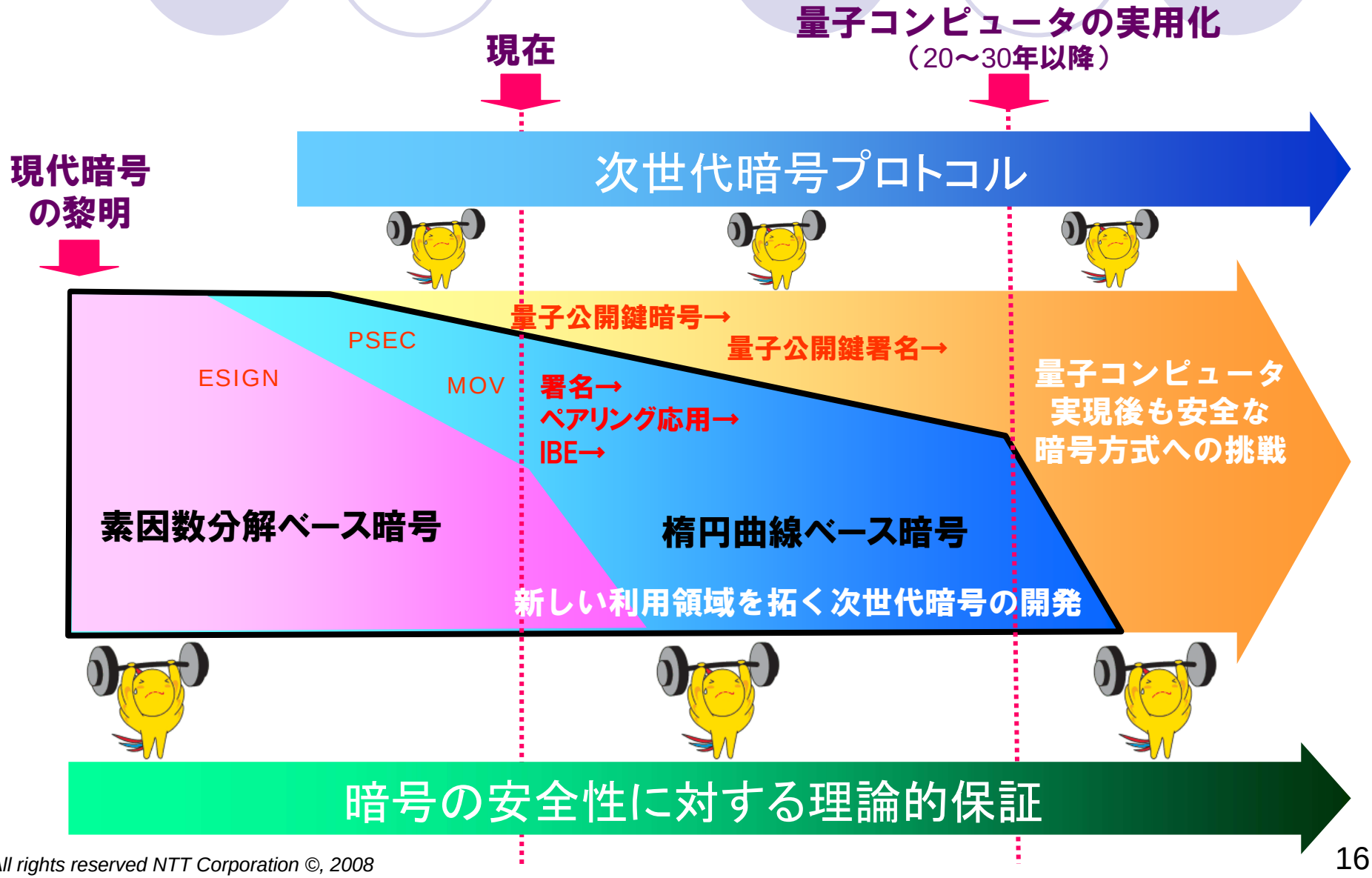
NTTでは、安心・安全な高度情報化社会を支えるために、主要な国際標準暗号・推奨暗号に選定されたCamelliaを国際的な基盤技術として広めていくとの方針のもと、2006年4月13日にオープンソース化を実施してCamelliaを自由に利用できる環境を提供するとともに、オープンソースコミュニティに対してもCamelliaのソースコードを提供するなど、採用に向けた活動を行ってまいりました。

その結果、本年9月にリリースされたOpenSSL 0.9.8c版にCamelliaが搭載されました。

OpenSSL toolkitにCamelliaが採用されたことは、米国政府標準暗号AES※3と同等の安全性と処理性能を有する世界唯一の暗号方式としてのCamelliaの位置づけがより確かなものになったものといえます。今後、Camelliaが搭載されたOpenSSL toolkitが世界中のWWWサーバなどに組み込まれ、また世界有数のオープンな暗号ライブラリとしても利用されるようになることによって、Camelliaの利用や製品開発が世界規模でより一層広がるものと期待しております。

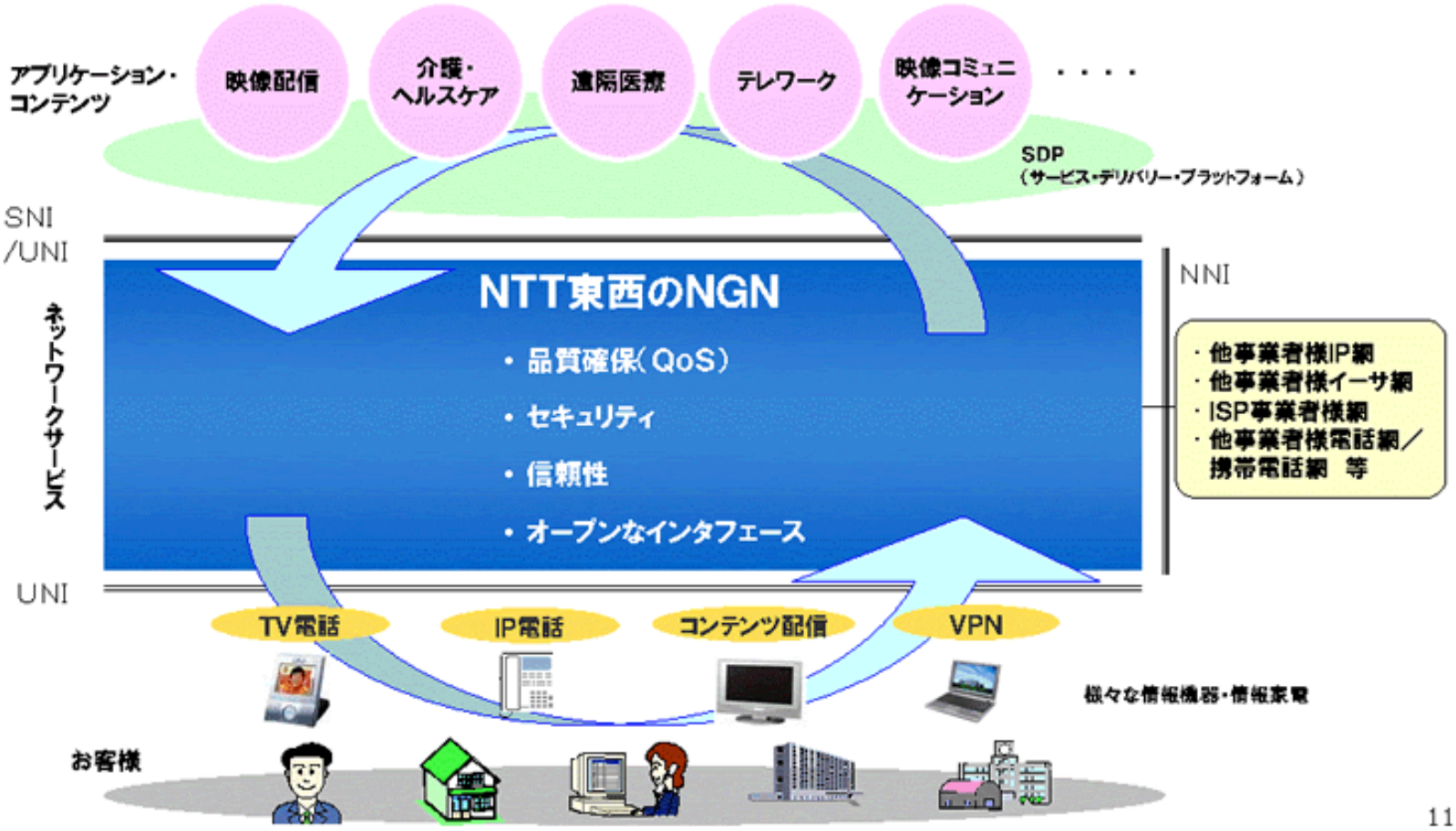
Camelliaホームページ　：http://info.isl.ntt.co.jp/crypt/camellia/index.html
オープンソース掲載ページ：http://info.isl.ntt.co.jp/crypt/camellia/source.html
OpenSSL Projectページ　：http://www.openssl.org/

更なる先端研究へ



NGNの概要

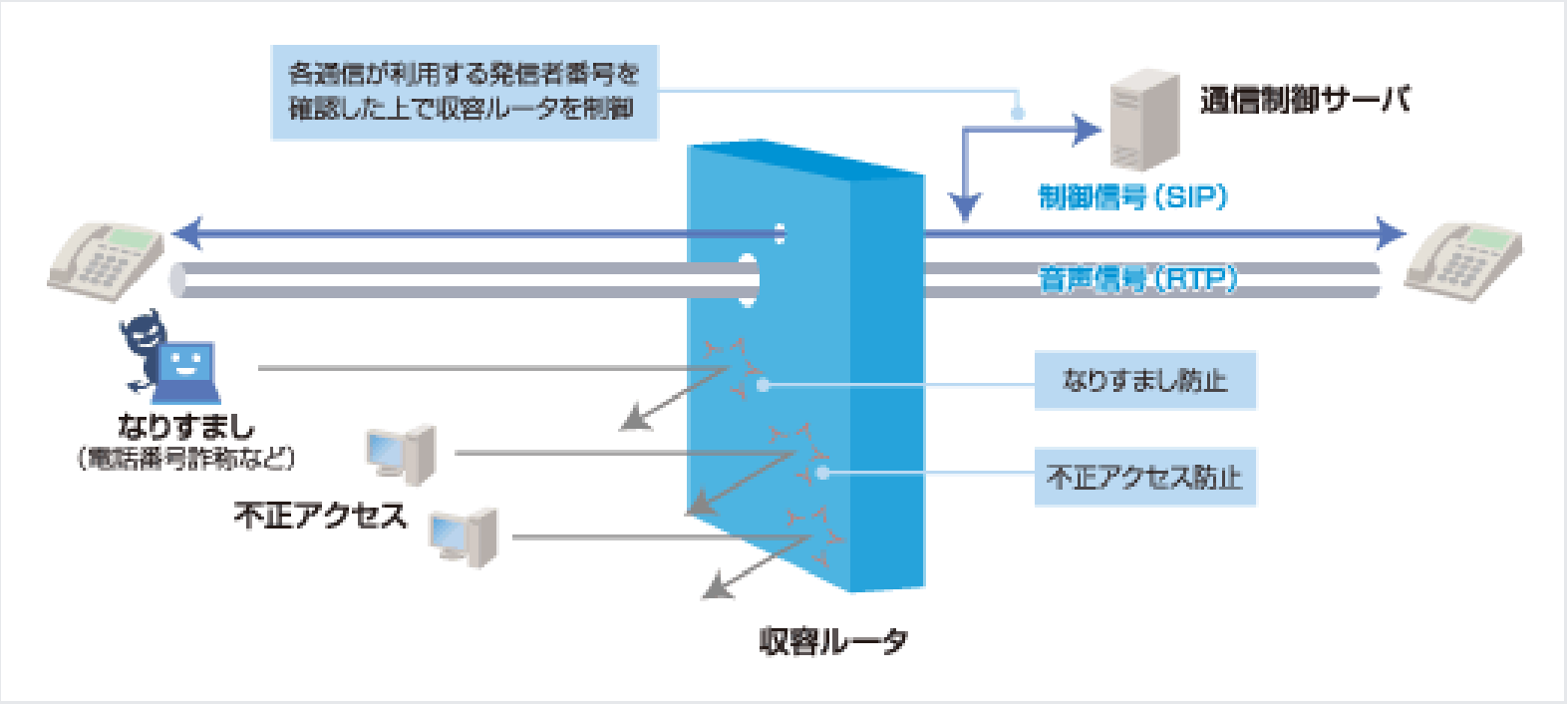
■ 最新かつ高度な技術による高い信頼性・安全性およびエンド・トゥ・エンドでの品質確保されたネットワークサービスをベースに、「オープン」と「コラボレーション」をキーワードとした、ビジネスパートナーの皆様との「サービスの共創」により、多彩なサービス展開を推進



出典： NTT東日本・平成19年度（第9期）中間決算について（http://www.ntt-east.co.jp/release/0711plhw/bmzk071109a_13.html）

NGNのセキュリティ

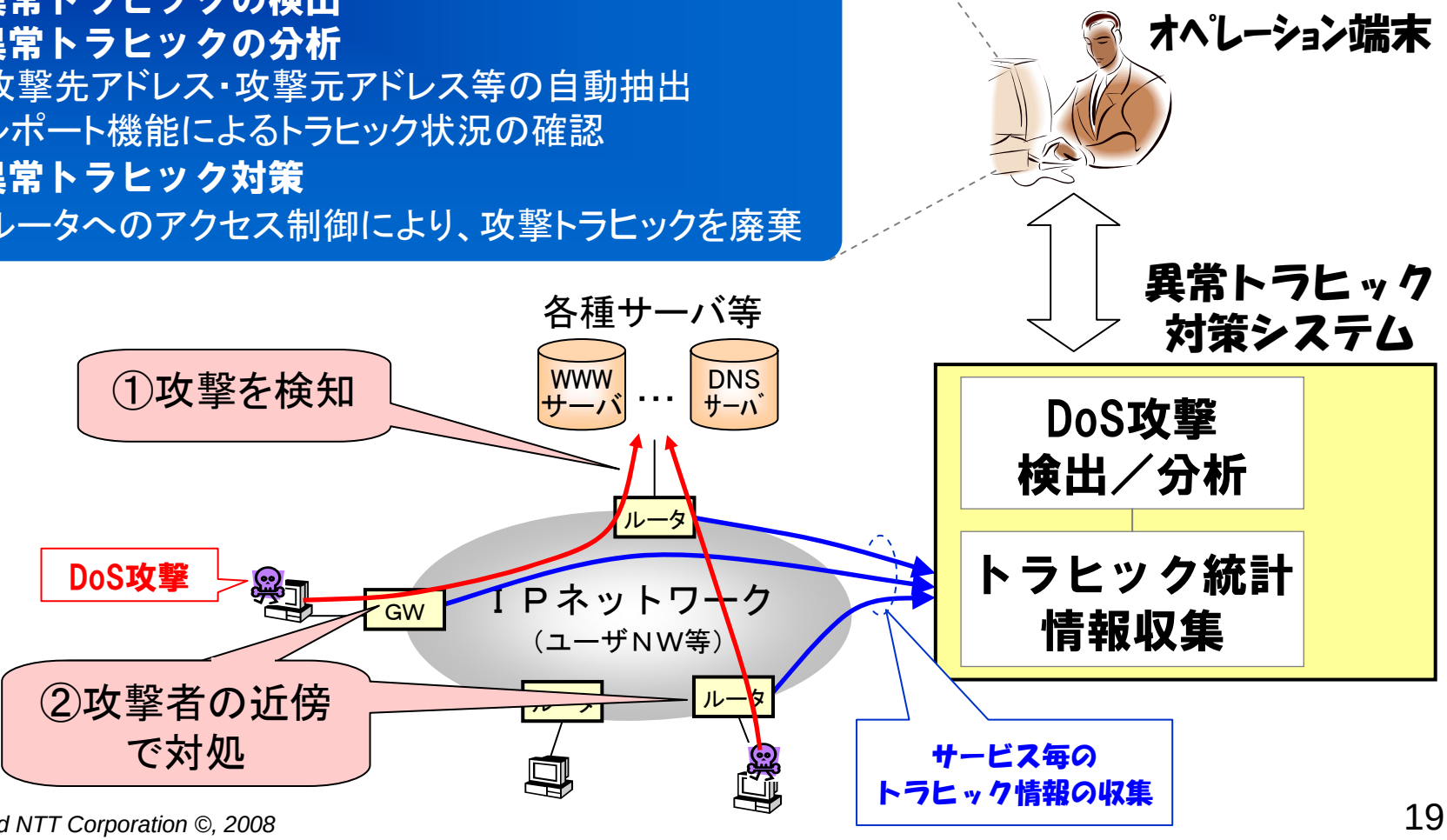
■NGNでは、回線ごとに割り当てられた発信者IDをチェックし、なりすましを防止します。また、ネットワークの入り口で、不正なアクセスやなりすましをブロックする機能等を具備しています。



出典： http://www.ntt-east.co.jp/ngn/about/index.html

サイバー攻撃対策技術

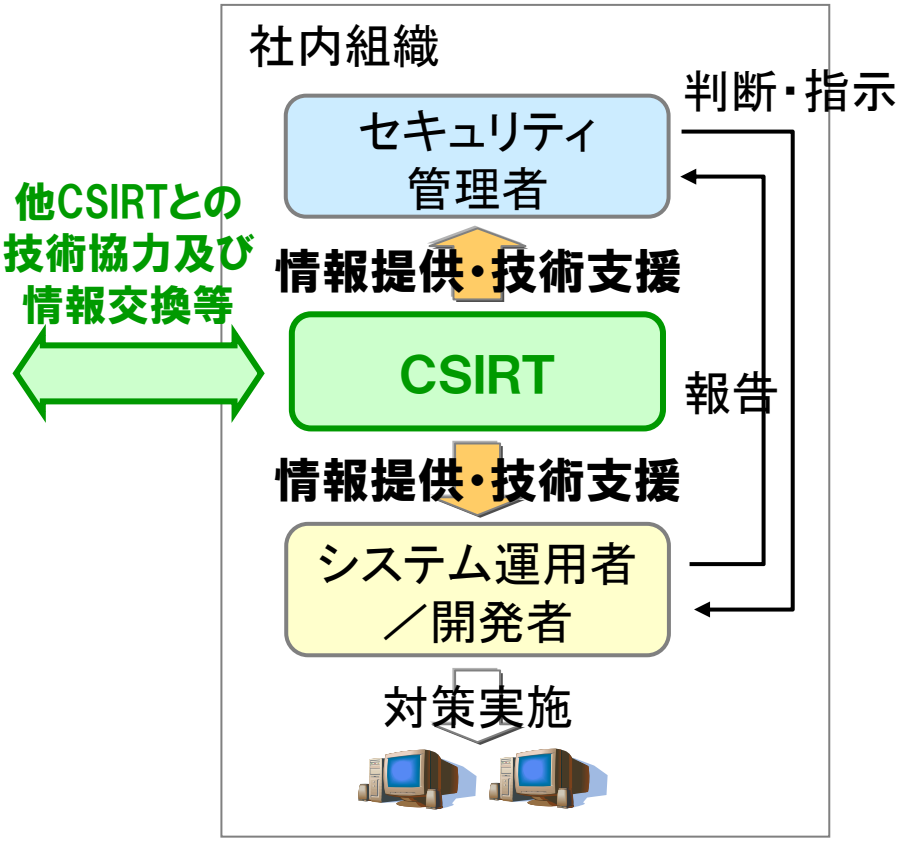
(1) トラヒック監視設定
(2) 正常状態の確認
- レポート機能によるトラヒック状況の確認
(3) 異常トラヒックの検出
(4) 異常トラヒックの分析
- 攻撃先アドレス・攻撃元アドレス等の自動抽出
- レポート機能によるトラヒック状況の確認
(5) 異常トラヒック対策
- ルータへのアクセス制御により、攻撃トラヒックを廃棄



セキュリティ運用の強化

◆セキュリティ運用の強化に向けては、専門家による組織的な活動を行う部隊であるCSIRT※と呼ばれる形態が注目されている。

※CSIRT：Computer Security Incident Response Team



機能	主な役割
セキュリティ管理者	対応の判断・指示、対策実施の管理
CSIRT	**対応の調整、技術支援、情報収集・分析・提供**
システム運用者／開発者	対策実施（パッチ適用、バージョンアップ、設定変更等）

CSIRT業務の概要

1．事後対応型サービス	2．事前対応型サービス	3．セキュリティ品質管理サービス
◆アラートと警告 ◆インシデントハンドリング ・インシデント分析 ・オンサイトでのインシデント対応 ・インシデント対応支援 ・インシデント対応調整 ◆脆弱性ハンドリング ・脆弱性分析 ・脆弱性対応 ・脆弱性対応調整 ◆アーティファクトハンドリング ・アーティファクト分析 ・アーティファクト対応 ・アーティファクト対応調整	◆告知 ◆技術動向監視 ◆セキュリティ監査又は審査 ◆セキュリティツール、アプリケーション、インフラ及びサービスの設定と保守 ◆セキュリティツールの開発 ◆侵入検知サービス ◆セキュリティ関連情報の提供	◆リスク分析 ◆ビジネス継続性と障害回復計画 ◆セキュリティ・コンサルティング ◆意識向上 ◆教育・トレーニング ◆製品の評価又は認定

出典：http://www.jpcert.or.jp/csirt_material/files/03_activities_of_csirt.pdf

NTT-CERTについて

●NTTグループのCSIRTとして、2004年10月に発足（情報流通プラットフォーム研究所に設置）

●FIRST※に加盟（2005年1月）

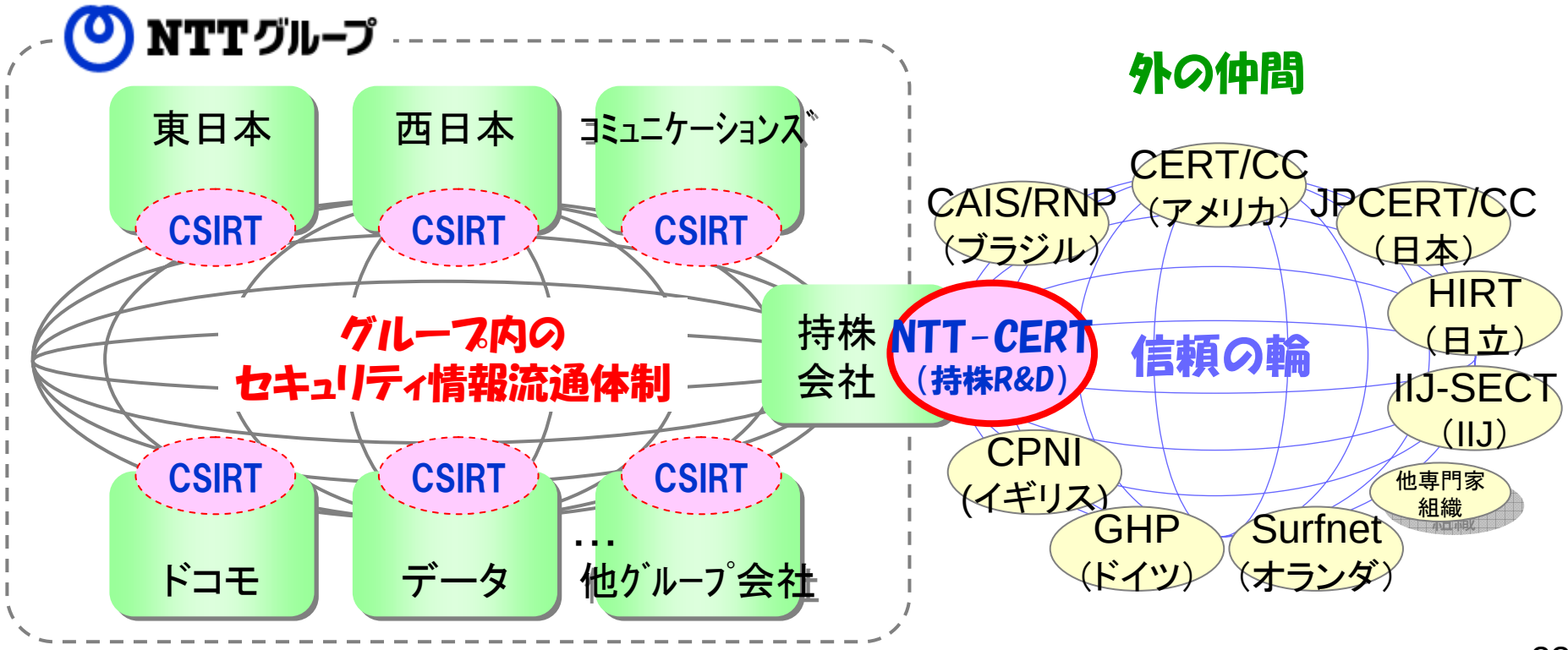
●NTT Computer Security Incident Response and Readiness Coordination Team の略称

※FIRSTとは・・・
Forum of Incident Response and Security Teamsの略。
1990年に設立された世界中のCSIRTの集まり（2007年現在で190チーム以上）。

NTTグループのセキュリティ強化に向けて

●**NTT-CERT**（セキュリティ運用チーム）は、NTTグループのセキュリティ関係者による技術連携を推進し、関連ノウハウの蓄積を図るとともに、NTTグループの**安心・安全なサービス提供、安心・安全のブランド向上**に貢献しています。

●**世界中の専門家組織と協調**して、セキュリティ上の諸問題を解決することで、**お客様の個人情報の保護、企業等の事業継続性の確保**に努めています。

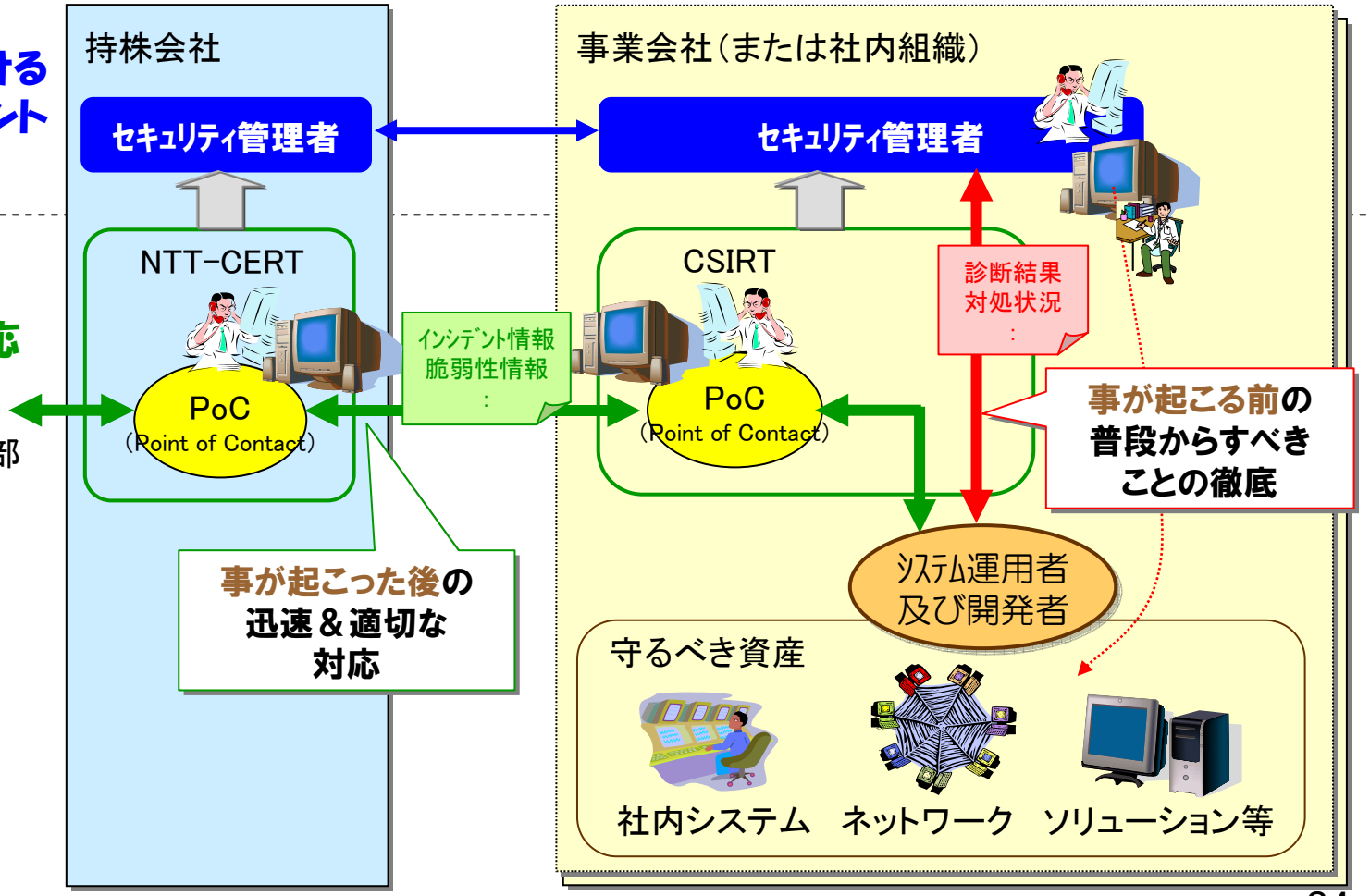


組織連携を機軸としたセキュリティ運用強化

■効果的な対策を立案・実施するためには、素早い状況把握や情報の共有等、組織（or 会社）間の連携が重要。
■組織を跨る、**１）セキュリティマネジメントの連携**、**２）セキュリティ情報・対応支援（CSIRT）の連携**の両輪によって、セキュリティリスクへの対応が強化できる。

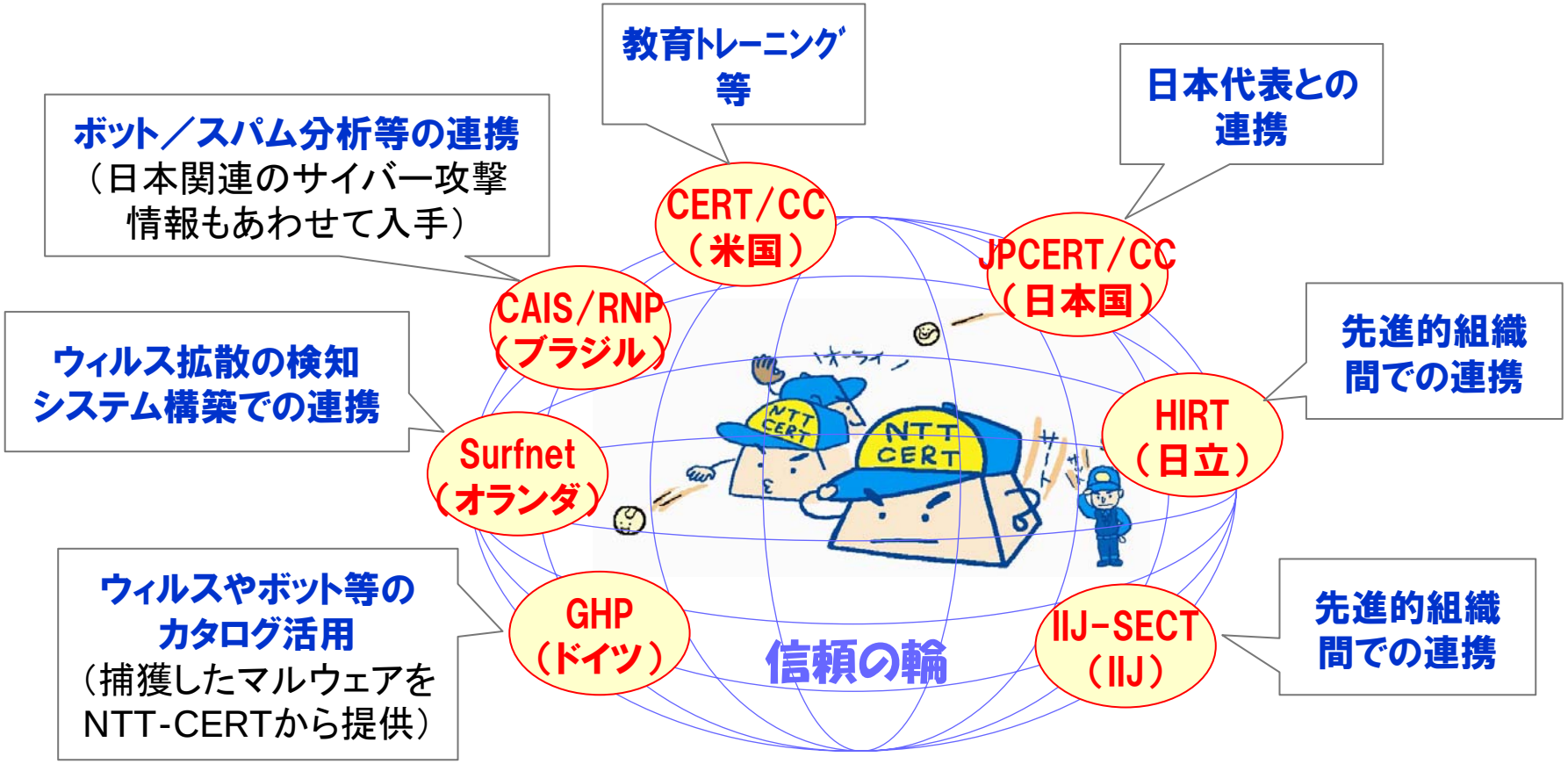
１）グループ企業におけるセキュリティマネジメントの連携

２）グループ内外のセキュリティ情報・対応支援の連携（CSIRT連携）



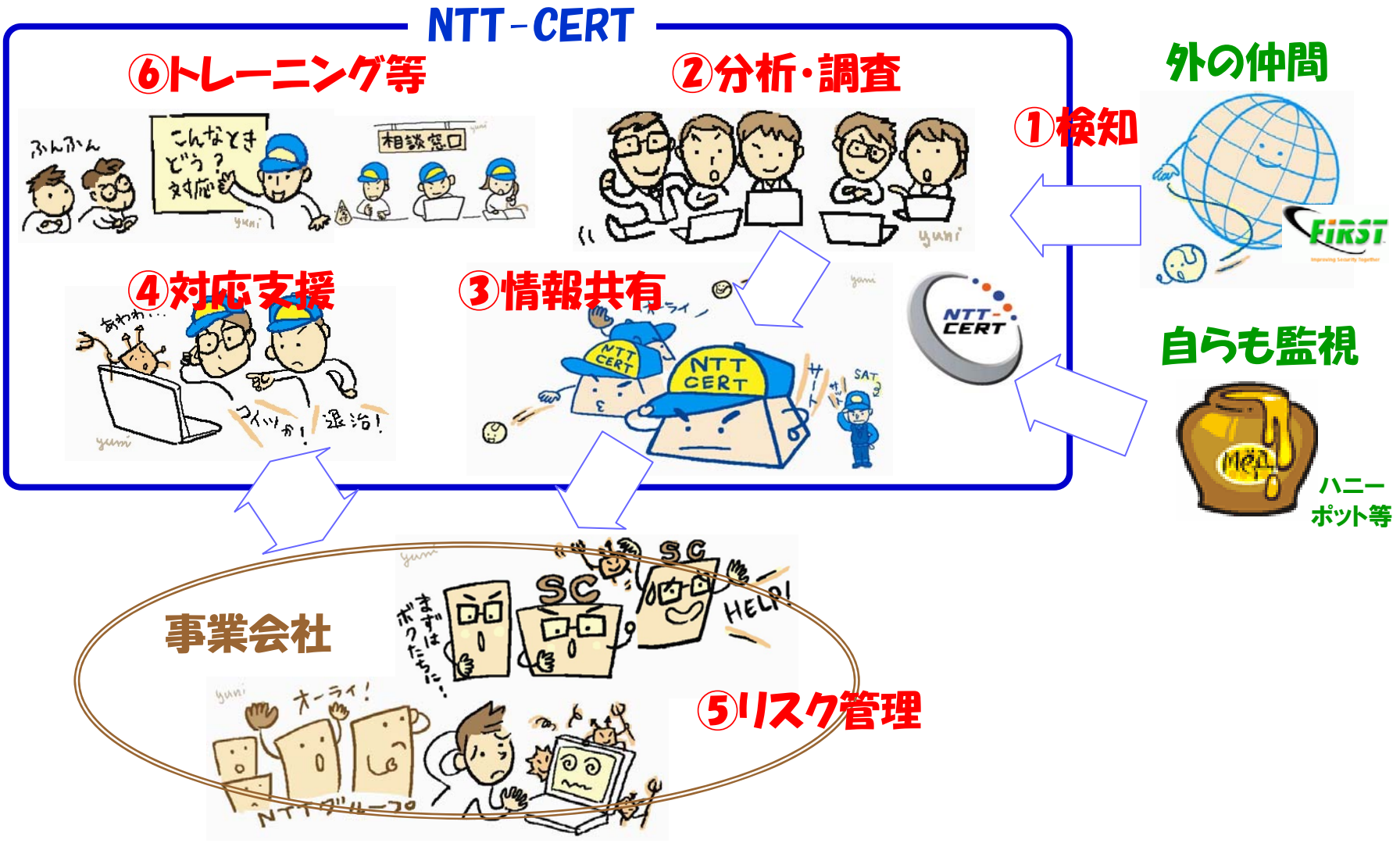
外の仲間との連携

◆Give&Takeにより信頼の輪を強化しつつ、セキュリティ情報の共有や関連技術の高度化を図っている・・・



3. セキュリティ運用強化に向けたR&D

NTT-CERTの取り組み



NTT-CERTの業務概要

セキュリティ運用業務の概要	
①検知	ハニーポット等を用いたインシデントの発見や攻撃傾向の把握
②分析・調査	インシデントや脆弱性、マルウェア等の分析・調査
③情報共有	インシデント発生／脆弱性発覚時の案件ハンドリング
	セキュリティ関連情報のモニタリング、レポーティング
④対応支援	事業会社におけるインシデント発生時の対応サポート
⑤リスク管理	事業会社にて普段から実施するセキュリティリスク診断や対応管理に関わる支援
⑥トレーニング等	一般／専門家向けのセキュリティ教育コース及び、草の根活動としてのワークショップの開催

検知・分析の支援システム

【目的】

・インシデントの発見や攻撃傾向の把握
（これをいち早く行うことで、被害の未然防止、極小化に繋げる）

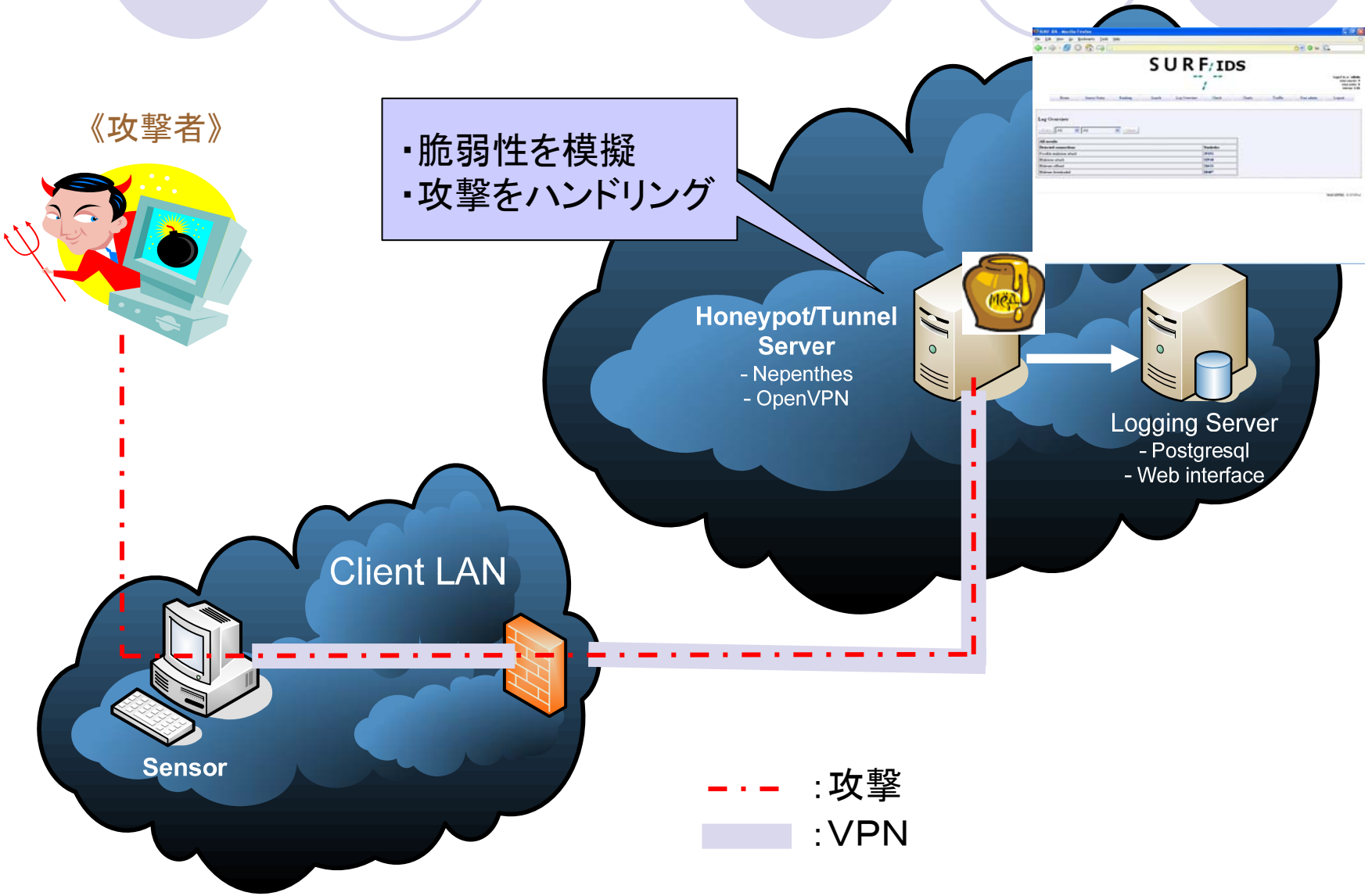
【アプローチ】

・ひとつの手段として、nepenthes等のlow-interaction honeypotを用いた
イベント検知システム（SURFnet IDS）を利用し、攻撃情報を収集・・・

《SURFnet IDS》

- SURFnet（オランダ）が提供する侵入検知システム(IDS)
- Sensor、Honeypot/Tunnelサーバ、Loggingサーバによる構成
- 攻撃者（主にworm、virusが対象）の挙動の記録やmalwareの収集が可能
- 異なるネットワークに複数のSensorを配置することにより、分散型IDSとして機能

SURFnet IDS



https://dids.ntt-cert.org/index.php

SURFnet IDS

logged in as: admin
total sensors: 5
total active: 4
version: 1.04

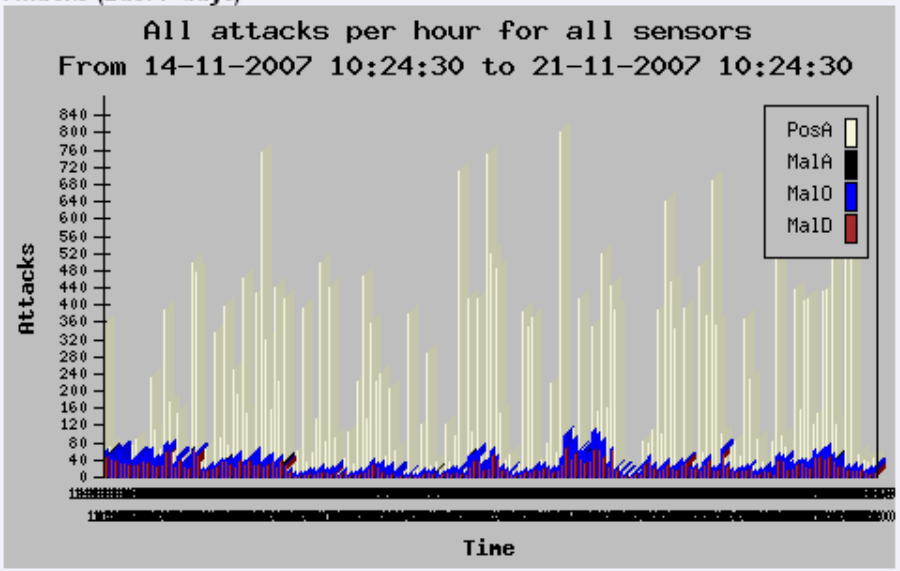
Home | Sensor Status | Ranking | Search | Log Overview | Check | Traffic | Plotter | Map | Logout

User Admin | Mail Admin | Organisation Admin | Server Info

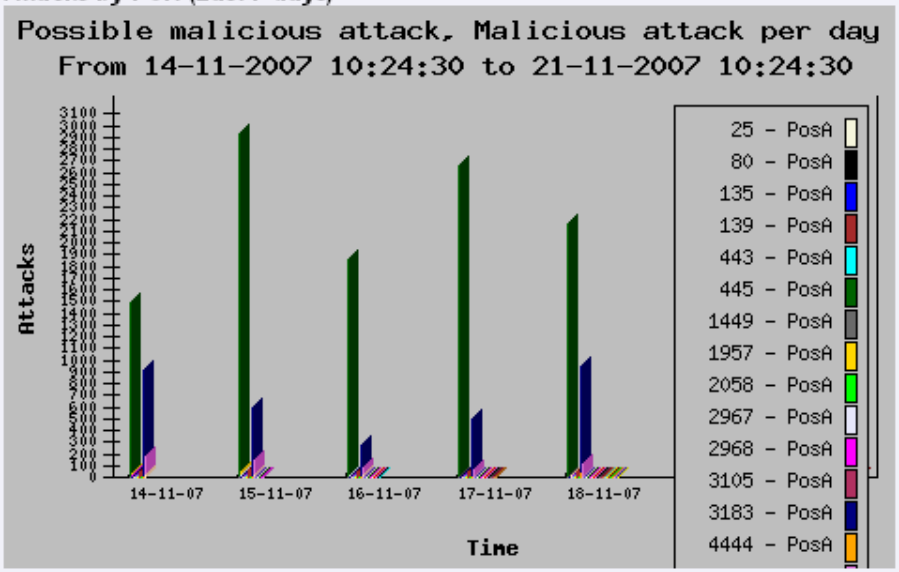
SURFnet IDS 1.04

Last 7 days

Attacks (Last 7 days)



Attacks by Port (Last 7 days)



Attackers (Last 7 days)

Today — 6 days ago

IP Address	Last Seen	Total Hits
2 .43.117	16-11-2007 03:08:27	414
1 .107.234	21-11-2007 09:56:49	392
6 143.55	20-11-2007 05:28:23	382
1 70.90	20-11-2007 19:02:25	364
8 94.217	17-11-2007 18:02:18	363

Ports (Last 7 days)

Destination Ports	Description	Total Hits
445	microsoft-ds	17432
139	netbios-ssn	13287
0	Port could not be determined	8737
135	msrpc	6780
44445	Port could not be determined	323
80	http	279

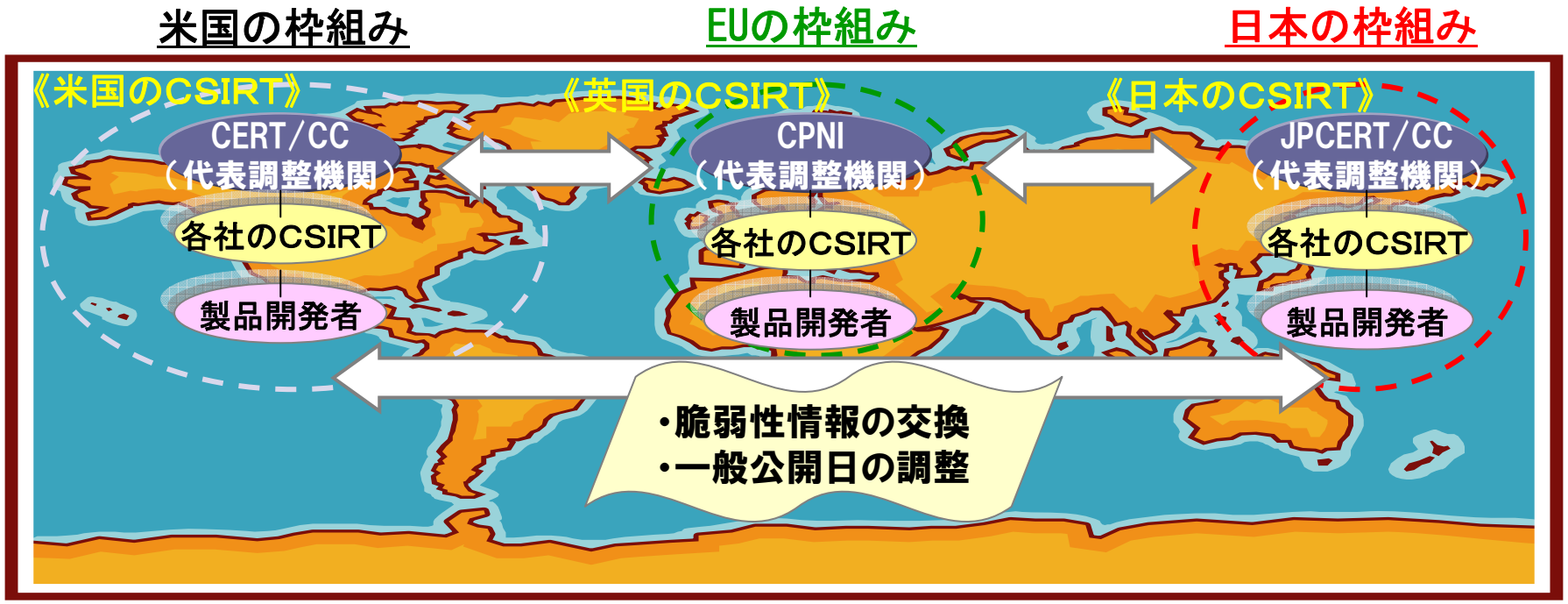
NTT-CERTの業務概要

セキュリティ運用業務の概要	
①検知	ハニーポット等を用いたインシデントの発見や攻撃傾向の把握
②分析・調査	インシデントや脆弱性、マルウェア等の分析・調査
③情報共有	インシデント発生／脆弱性発覚時の案件ハンドリング
	セキュリティ関連情報のモニタリング、レポーティング
④対応支援	事業会社におけるインシデント発生時の対応サポート
⑤リスク管理	事業会社にて普段から実施するセキュリティリスク診断や対応管理に関わる支援
⑥トレーニング等	一般／専門家向けのセキュリティ教育コース及び、草の根活動としてのワークショップの開催

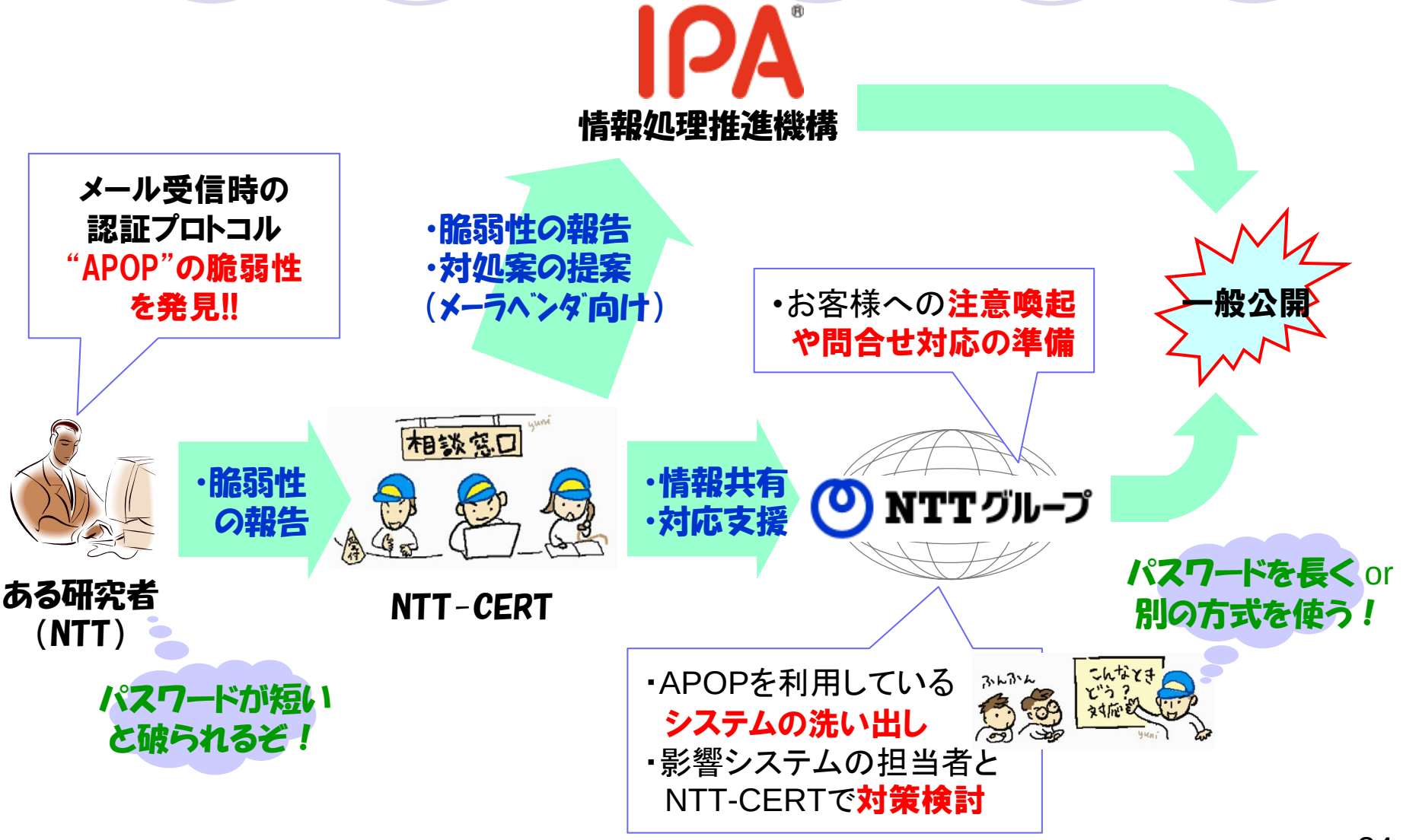
早期警戒パートナーシップ

◆経産省が「ソフトウエア等脆弱性関連情報取得基準」を告示し（2004年7月）、IPAが受付機関として、「情報セキュリティ早期警戒パートナーシップ」を開始。
◆国際的には、市中製品※に影響を与え、インターネットの安全を大きく脅かす脆弱性について、各国を代表するCSIRT（調整機関）が協力して一般公開前の脆弱性情報を関連製品の開発者間で共有し、更新ソフトウェアの公開日を一致させながら対処していく取り組みが展開されている。

※ソフトウェア製品及び、ソフトウェアを組み込んだハードウェア製品

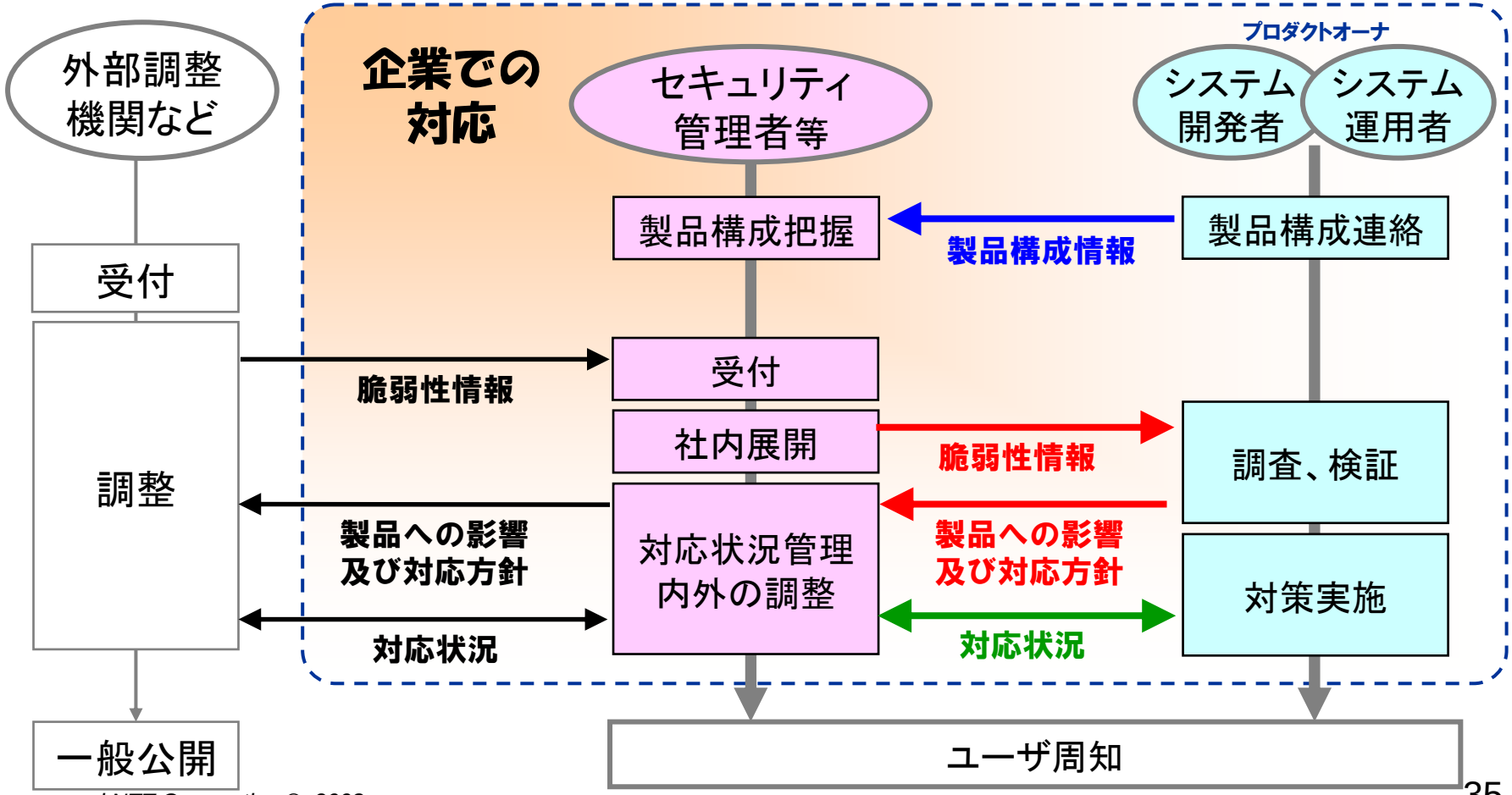


非公開脆弱性への対応の事例



脆弱性ハンドリングの流れ

●**いち早く、適材適所にかつ、セキュアに**実施するためには・・・
（1）特定の脆弱性の影響を受ける製品の網羅的な調査と対策の提供
（2）一般公開前の脆弱性情報の漏洩の防止
（3）対応状況管理及び、調整機関との公開スケジュール調整



案件ハンドリングの支援システム要件

案件ﾊﾝﾄﾞﾘﾝｸﾞの流れ

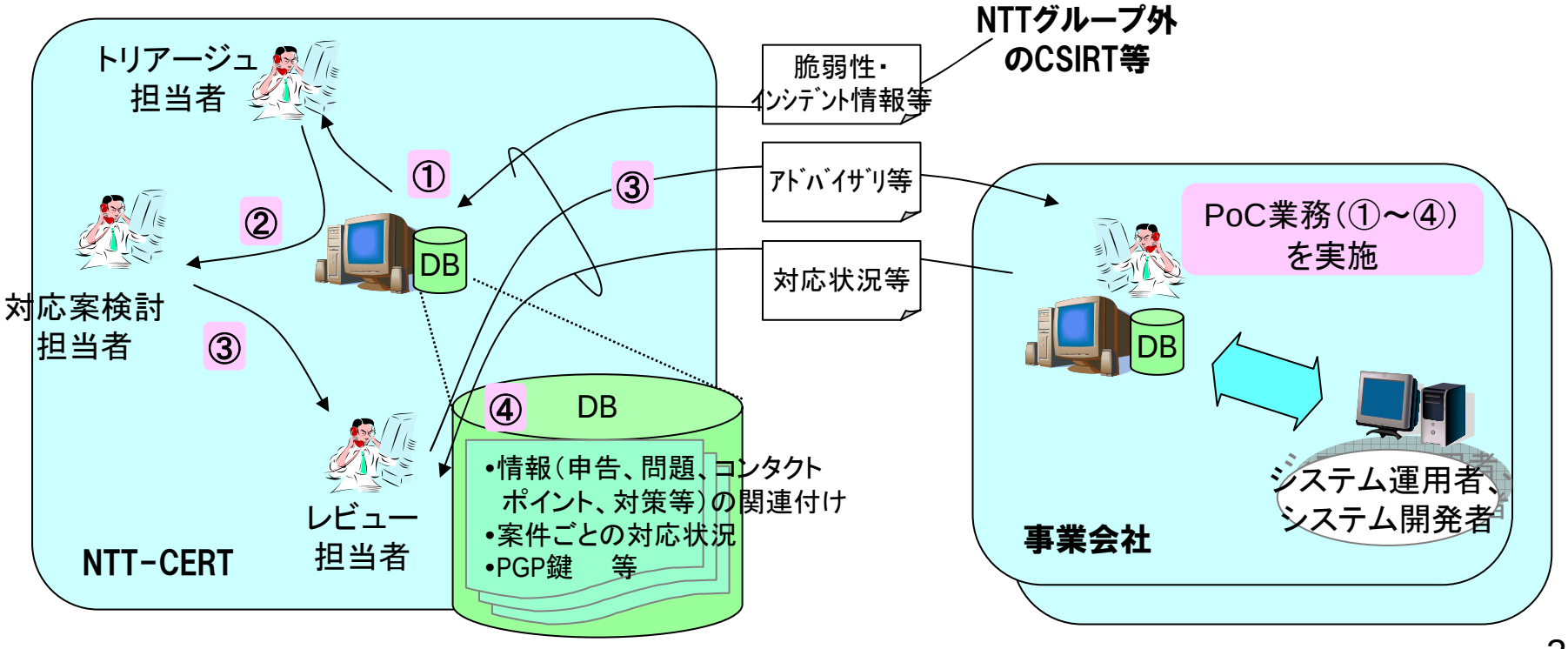
①脆弱性・ｲﾝｼﾃﾞﾝﾄ情報等の受付 → ②ﾄﾘｱｰｼﾞｭ(関係者特定・優先ﾚﾍﾞﾙ付け) → ③対応策定/送付(ｱﾄﾞﾊﾞｲｻﾞﾘ・技術情報等) → ④各案件の対応状況を一元的に把握

＜情報の階層化管理と暗号化＞
- ・復号／署名検証機能(PGP)
- ・送受信文書の関連付け管理の高度化(ソート・絞込み等)
- ・全文検索機能
- ・インデックス機能等

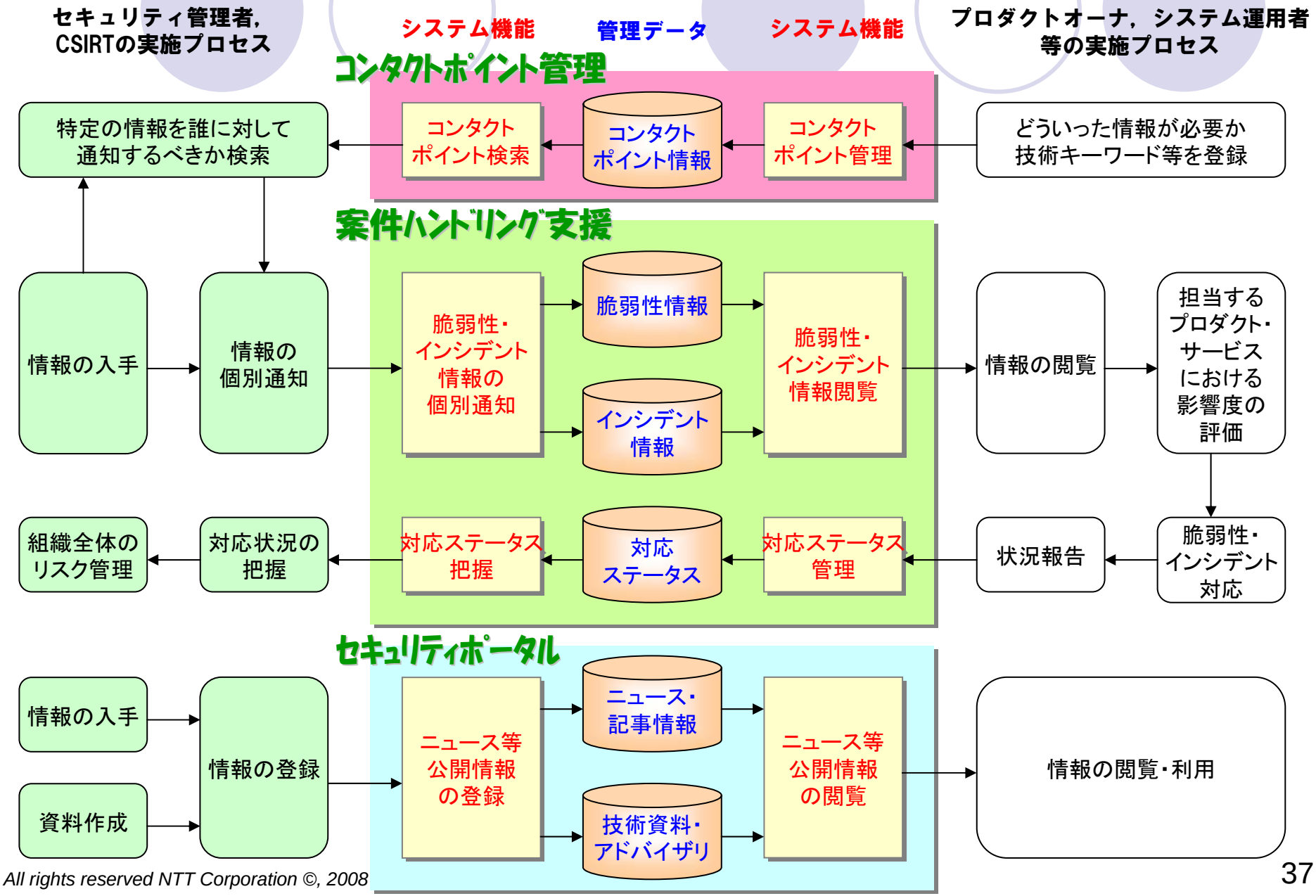
＜コンタクトポイント管理＞
- ・コンタクトポイント管理機能(PoC情報登録、検索及び、参照)
- ・対応案件毎の伝達先に応じた階層化

＜文書作成支援＞
- ・ユーザ操作履歴機能
- ・文書作成履歴機能
- ・暗号化／署名機能(PGP)

＜PoC業務フロー関連＞
- ・案件のｽﾃｰﾀｽ管理に基く進捗状況管理機能
- ・優先ﾚﾍﾞﾙに基づく対応期限通知機能



セキュリティ情報共有を支えるシステムの全体像

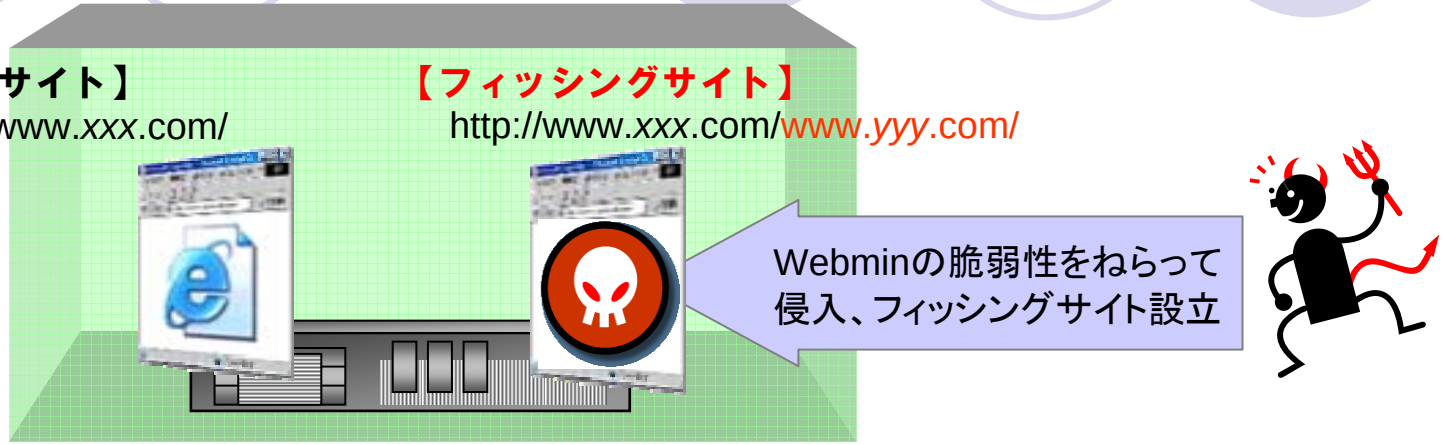


NTT-CERTの業務概要

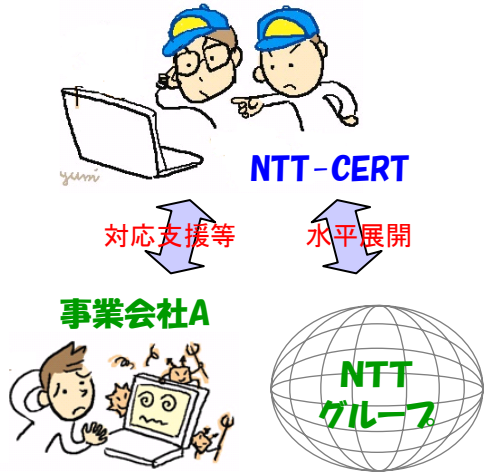
セキュリティ運用業務の概要	
①検知	ハニーポット等を用いたインシデントの発見や攻撃傾向の把握
②分析・調査	インシデントや脆弱性、マルウェア等の分析・調査
③情報共有	インシデント発生／脆弱性発覚時の案件ハンドリング
	セキュリティ関連情報のモニタリング、レポーティング
④対応支援	事業会社におけるインシデント発生時の対応サポート
⑤リスク管理	事業会社にて普段から実施するセキュリティリスク診断や対応管理に関わる支援
⑥トレーニング等	一般／専門家向けのセキュリティ教育コース及び、草の根活動としてのワークショップの開催

インシデント(侵入・改竄)対応の事例

某金融機関のフィッシングサイトが立てられてしまった・・・



インシデント対応支援



①海外のある組織からメールによりインシデントの連絡

②初動対応支援

フィッシングサイトのコンテンツを外部からアクセスできない場所に移動

③原因分析(フォレンジック)

某国からWebmin経由で侵入し、フィッシングサイトを立てた可能性を発見

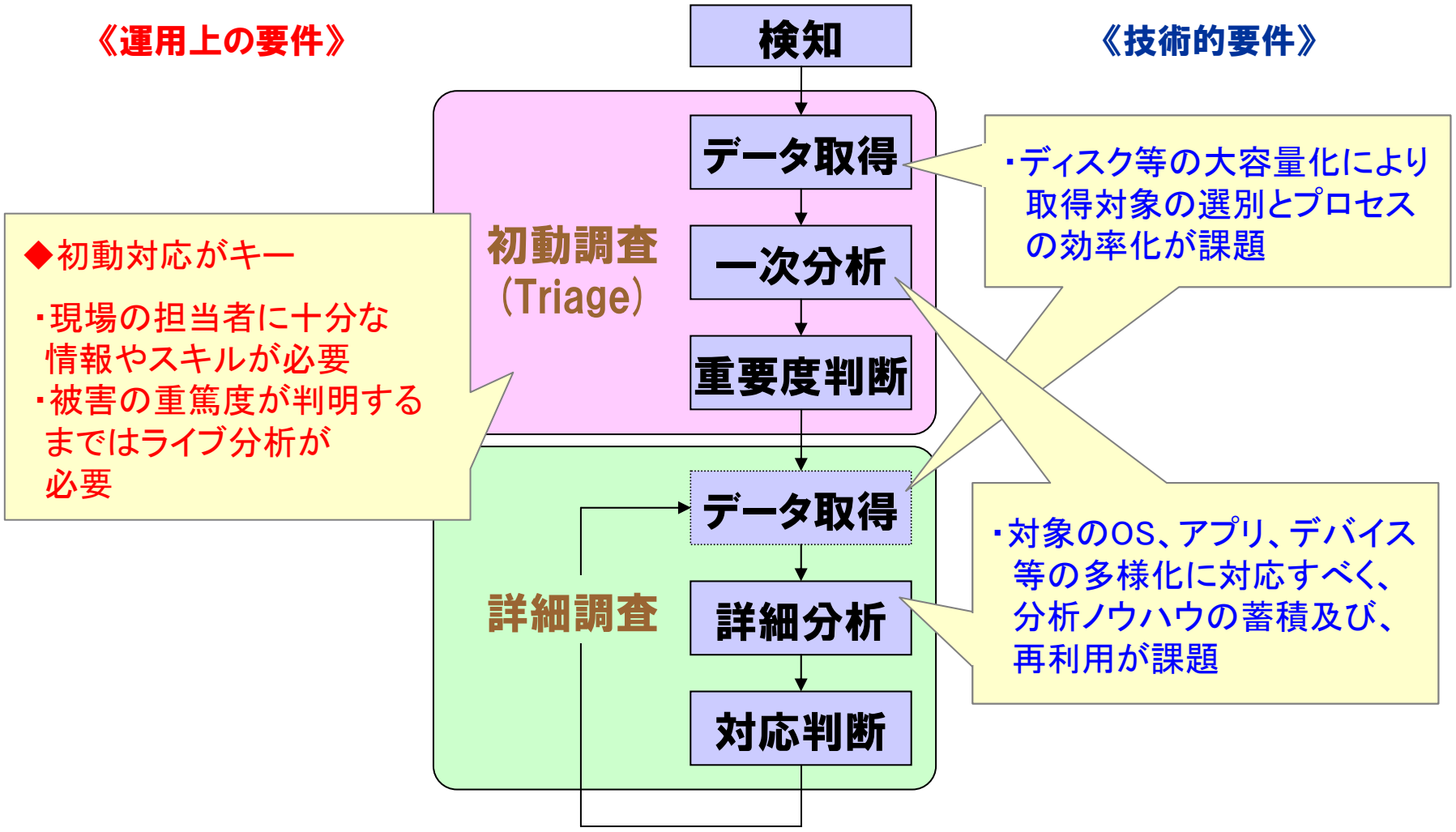
④被害状況の分析

DBサーバに格納された個人情報の漏えいがないことを確認

⑤NTTグループ内に注意喚起と未然防止策を水平展開

類似インシデントの未然防止

インシデント・レスポンスにおける課題



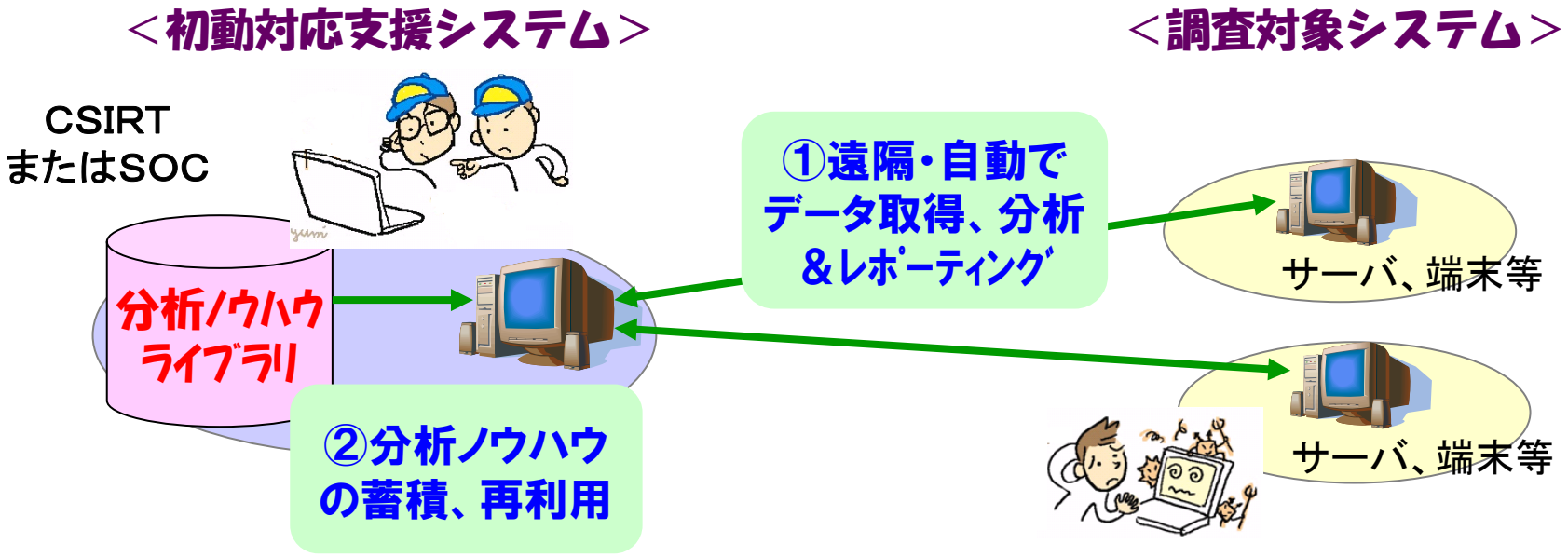
フォレンジックの支援システム（1）

①初動対応のシステム化

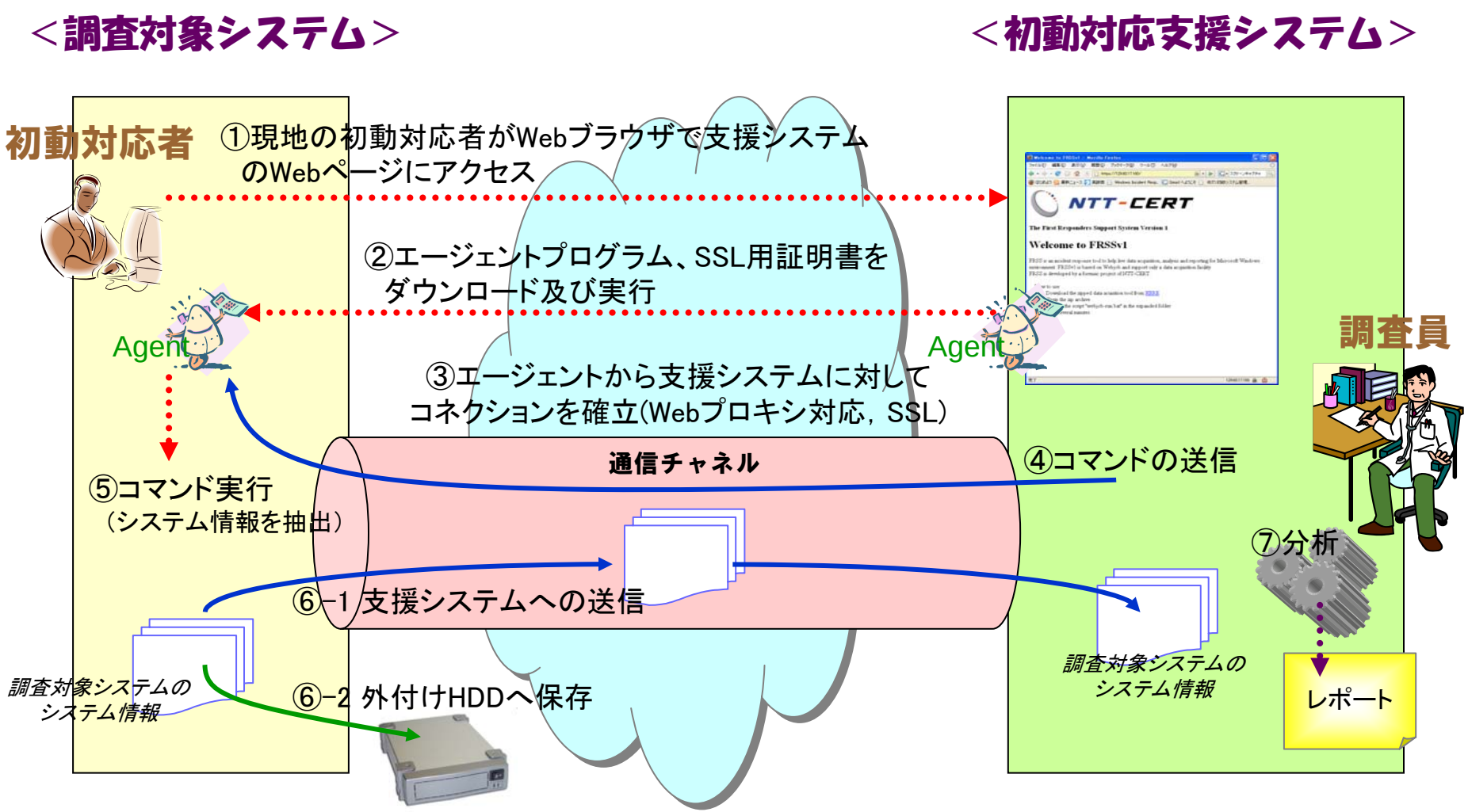
◆リモートから自動で問題のサーバや端末のデータを取得
◆自動による一次分析および結果のレポーティング

②分析ノウハウの蓄積および再利用

◆アプリケーション・スペシフィックな分析ノウハウの蓄積
◆自動分析モジュールから利用可能な形態でのライブラリ化



フォレンジックの支援システム（2）



NTT-CERTの業務概要

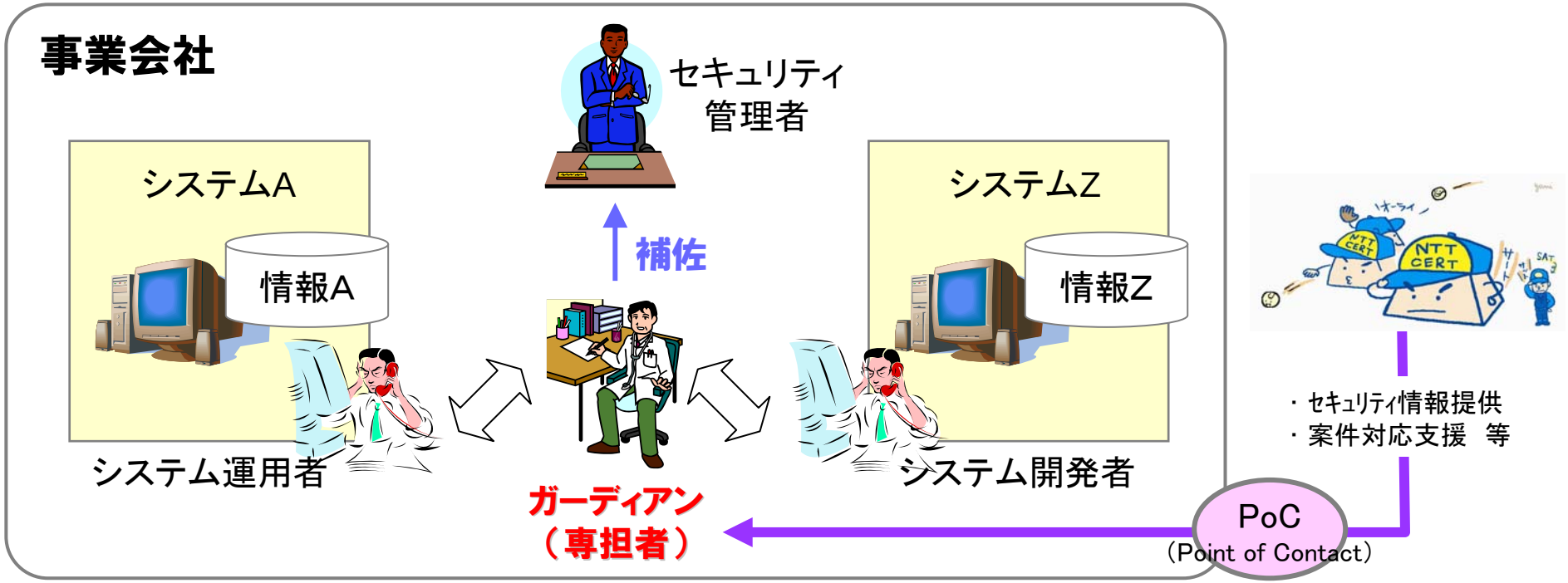
セキュリティ運用業務の概要	
①検知	ハニーポット等を用いたインシデントの発見や攻撃傾向の把握
②分析・調査	インシデントや脆弱性、マルウェア等の分析・調査
③情報共有	インシデント発生／脆弱性発覚時の案件ハンドリング
	セキュリティ関連情報のモニタリング、レポーティング
④対応支援	事業会社におけるインシデント発生時の対応サポート
⑤リスク管理	事業会社にて普段から実施するセキュリティリスク診断や対応管理に関わる支援
⑥トレーニング等	一般／専門家向けのセキュリティ教育コース及び、草の根活動としてのワークショップの開催

ガーディアンによるセキュリティ管理体制の補強

◆セキュリティ管理者の補佐となり、セキュリティ状況を一元的に把握し、システム運用者等と連携して問題解決にあたる**“ガーディアン”の導入によりセキュリティ管理体制を補強**。

- ●守るべき資産の一元管理、定常的なセキュリティチェック
- ●脆弱性情報の通知・対処勧告及び、システム運用者支援
- ●リスク情報の把握、対処状況の追跡・管理
- ●セキュリティ管理者への定期／随時レポーティング

ガーディアンによる対応



リスク診断・管理のシステム要件

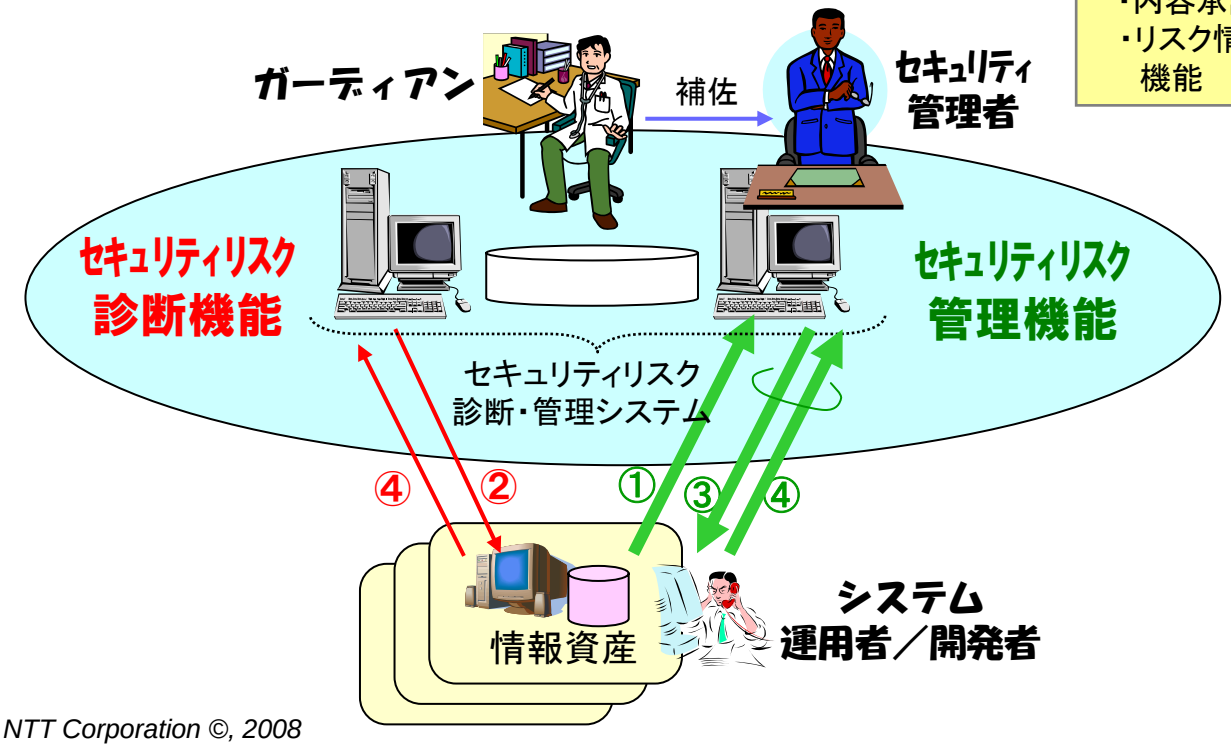
セキュリティ診断
管理業務の流れ

①情報資産(情報、サーバ等)を登録 → ②情報資産のセキュリティ状況を定常的に診断 → ③問題を一元的に把握し対応判断・勧告 → ④対応状況を一元把握、ノウハウとして蓄積

＜情報資産管理＞
- 管理対象システムの情報登録、更新、削除機能
- 登録した情報資産の有効期限確認機能

＜セキュリティリスク診断＞
- ネットワーク診断機能
- Web診断機能
- サーバ監査機能
- 診断スケジューリング機能

＜リスク情報管理、レポーティング＞
- リスク情報の登録、更新、検索、削除機能
- 対応状況監視／通知、役割別メニュー表示機能
- 内容承認機能
- リスク情報・対応状況の外部出力機能



NTT-CERTの業務概要

セキュリティ運用業務の概要	
①検知	ハニーポット等を用いたインシデントの発見や攻撃傾向の把握
②分析・調査	インシデントや脆弱性、マルウェア等の分析・調査
③情報共有	インシデント発生／脆弱性発覚時の案件ハンドリング
	セキュリティ関連情報のモニタリング、レポーティング
④対応支援	事業会社におけるインシデント発生時の対応サポート
⑤リスク管理	事業会社にて普段から実施するセキュリティリスク診断や対応管理に関わる支援
⑥トレーニング等	一般／専門家向けのセキュリティ教育コース及び、草の根活動としてのワークショップの開催

草の根活動によるスキル底上げ

◆「人は石垣、人は城」
◆セキュリティワークショップの定期的な開催

情報、ノウハウ、ベストプラクティスの共有

参加者各自のスキル、経験、ノウハウ、苦労話、工夫点の共有とディスカッション

人脈形成

グループ内セキュリティ実務担当者間で「信頼できる人的ネットワーク」を構築（Web of Trust）

セキュリティ実務者のスキル向上

最新のトピック、対策技術に関する講義、実習型トレーニング（外部講師もあり）

4. 日本の情報セキュリティ向上を目指して

通信事業者が立ち向かう新たな脅威

①サイバーテロ・組織化されたサイバー攻撃

- インフラに破壊的な被害をもたらす
- 設備の処理能力を超えてしまう

②サイバー犯罪

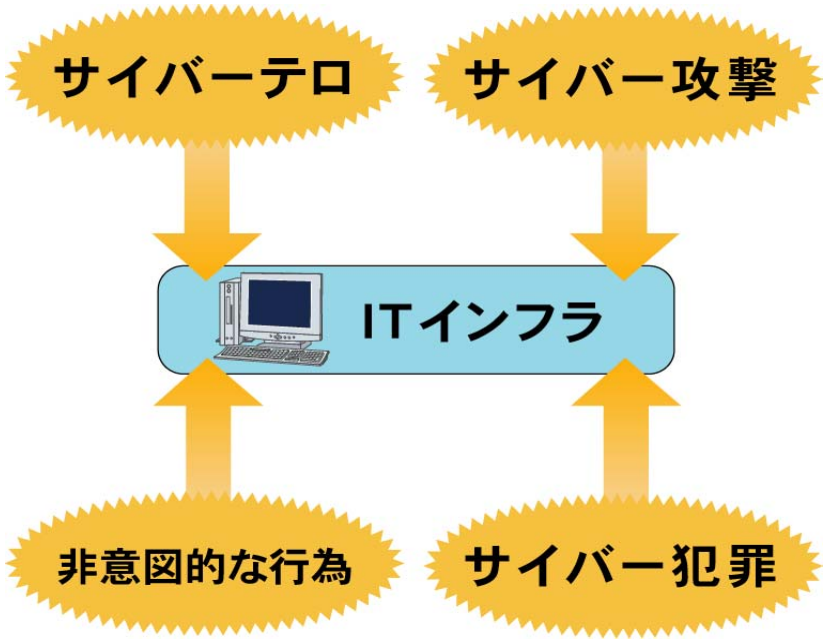
- 営利目的
- ユーザに迷惑や経済的被害をもたらす

③非意図的な行為

- 誤設定・誤操作
- ソフトウェアの不具合

④その他の意図的な行為

- 内部脅威



※NTTラーニングシステムズの調査結果より

世界で初めて発生したサイバーテロとは？

- 2007年4月下旬にバルト海沿岸の国エストニアで大規模なサイバーテロ攻撃が発生

（出典）外務省ホームページ

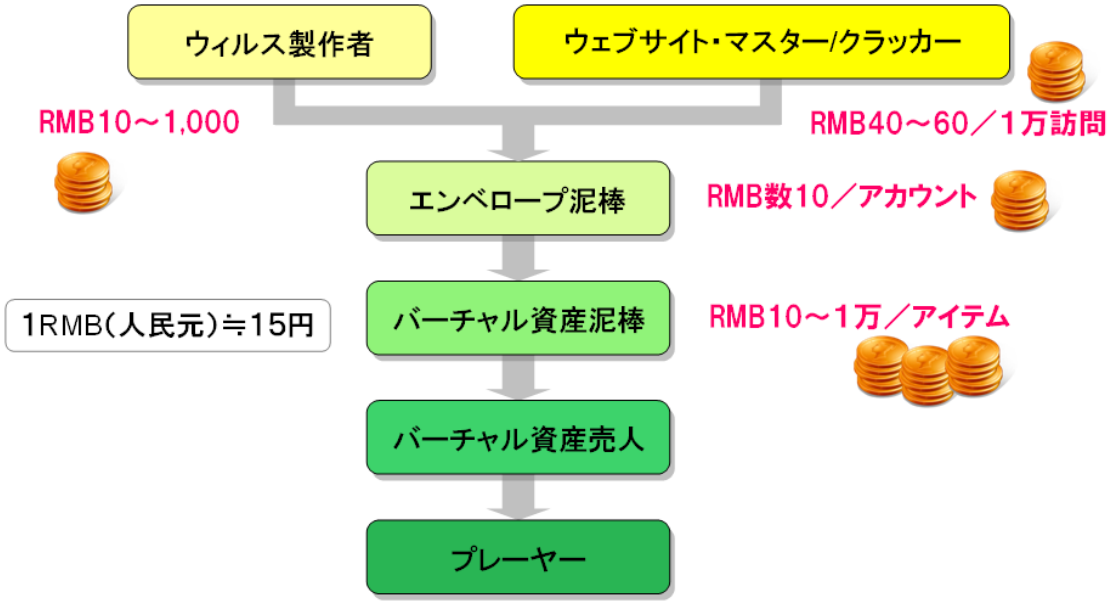
- エストニア
  - 1940年　ソ連に編入、1990年　ソ連から独立
  - IT国家として名高い、NATO加盟国（2004年）
- 経緯
  - 2007年4月26日、ソ連時代に設置された記念銅像を撤去
  - 翌日から大量のトラヒックが国外から流入
  - 政府、大統領府、省庁、大手銀行、新聞社、ISPに被害が発生
  - ATMや固定電話も使いづらくなった
  - 5月中旬に攻撃が突如停止した
- 「偵察活動」との見方もあり

※NTTラーニングシステムズの調査結果より

経済的被害をもたらすサイバー犯罪

●盗んだアカウント・パスワードやアイテムを取り引きする闇市場が形成されている
●犯罪を幇助しないよう、通信事業者が対応措置を取らされる事例が増加している

■中国のアンダーグラウンド・エコノミー



■ヤミ市場における販売価格

商　品	価格(ドル)
クレジットカード(米国)	1～6
銀行口座	14～18
メールアドレス(2万9千件)	5
Skypeアカウント	12
PayPalアカウント	10～500

(出典)シマンテック

※NTTラーニングシステムズの調査結果より

災害対応

●自然災害の対応では、被災地の支店が復興の主役となり、本社は後方支援を実施
●インバウンド情報を集約して、関係者への報告やロジスティクス支援を実施

地震、台風など

災害発生！

稼動/物資応援

他支店

被災地支店

状況報告

•設備状況の把握
•復興作業

復旧の支援

本社（後方支援）

•被災規模の把握
•ロジスティクスの支援
•関係者への報告

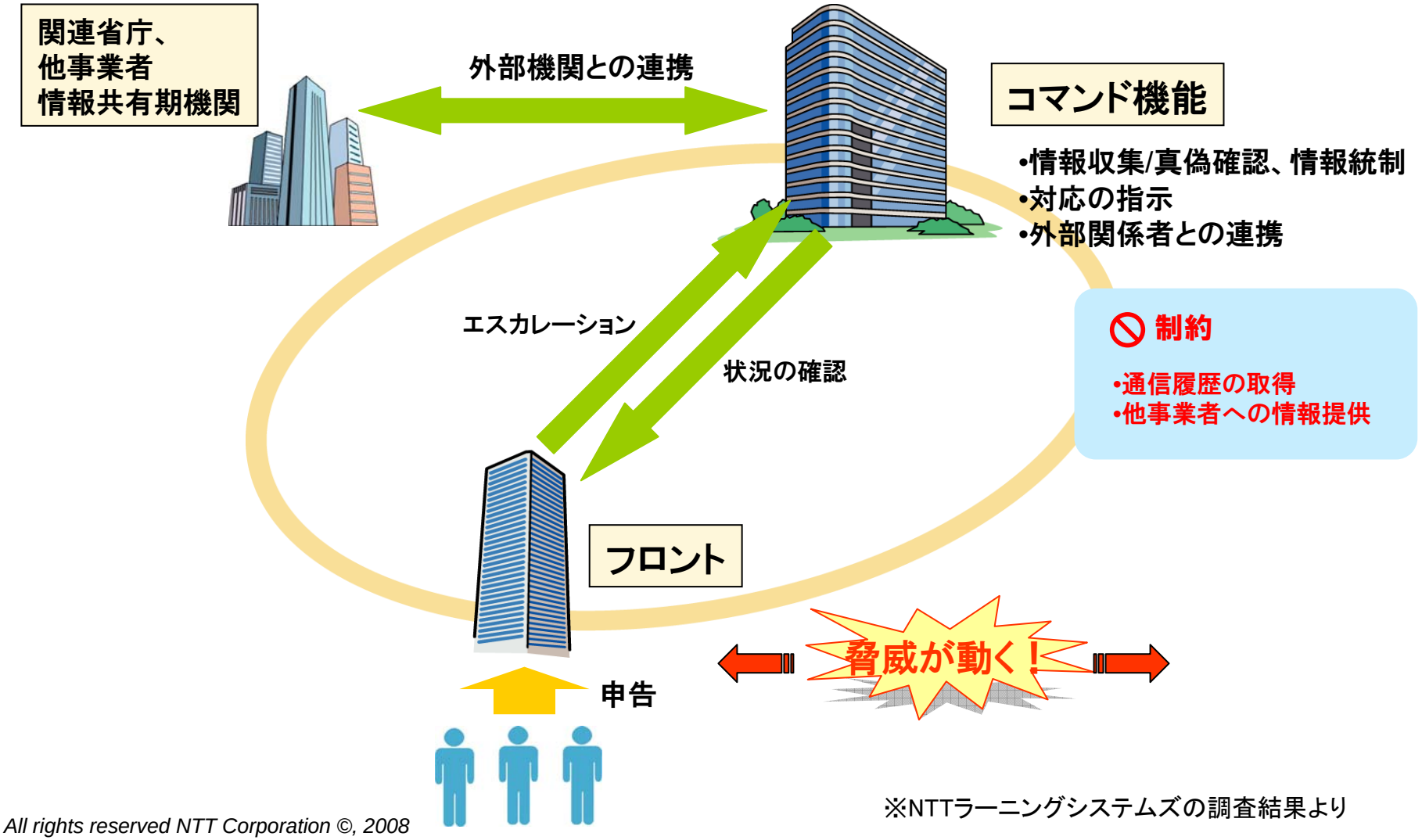
制約
・危険地域への立ち入り

テレビ報道
気象情報

※NTTラーニングシステムズの調査結果より

セキュリティ・インシデント対応

●アウトバウンドで情報を収集し、被害拡大の抑止と根本解決につなげる



※NTTラーニングシステムズの調査結果より

従来の災害対応と
セキュリティ・インシデント対応の比較

比較項目	自然災害	セキュリティ・インシデント
脅威	動かない	動く
災害・インシデントの発生場所	限定的（地理的に特定可能）	特定不可能
災害・インシデントの終息宣言	第三者（気象庁など）が判断	自ら情報を集めて、自らが判断
復旧時の制約	危険地域への立ち入り ロジスティクス （稼動応援、予算）	真の原因究明、 憲法・法律 （通信の秘密、個人情報）
回復方法	NTT設備の復旧	場合により異なる
他事業者との連携	NTT伝送路を使っている場合は連携もあり	犯人特定やインシデント情報共有で連携は必須
世間の反応	同情的	批判的

※NTTラーニングシステムズの調査結果より

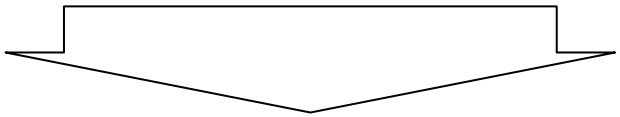
取り組みのスタンス

●NTT-CERTは、電気通信インフラ分野における情報分析・共有機能の取り組み（T-CERTOAR）を推進。

●この取り組みをより効果的に進めるため、日本シーサート協議会の個別企業等におけるCSIRT構築・運用支援の活動にも協力。

日本のCSIRT事情

- セキュリティ・インシデントへの迅速な対応が単独のCSIRTでは困難になってきている・・・
  - 日本国内の企業事情を巧みに利用する攻撃
  - 対応ノウハウの蓄積が難しいターゲット型攻撃
- 国内CSIRTの活動も活発化し、個々のチーム同士での連携が進んできている



これ迄にない高いレベルの緊密な連携体制で、共通の問題を解決していく場が必要！

日本シーサート協議会

■**日本シーサート協議会**が設立・始動（2007.4～）。
■初期メンバ：JPCERT/CC, IIJ-SECT, HIRT,
SBB-SIRT, JSOC, NTT-CERT

【主な活動】

- ○インシデント情報、対応手法等の情報共有
- ○国内のCSIRT構築等の支援
- ○社会的かつ、CSIRT間に共通する課題解決に向けたワークグループ（WG）活動
- ○様々な場の提供
  - ●異なるCSIRT同士の交流の場
  - ●CSIRTのあり方に関する議論の場

CSIRT
日本シーサート協議会

日本シーサート協議会のWG活動

＜組織内シーサート課題検討 WG＞

シーサート協議会のメンバー、及び組織内シーサートの構築や運用を考えている方々とのディスカッションを通じ、組織内シーサートの構築や運用に必要な課題を抽出する。その上で、それらの課題に対応した、各シーサートの活動の一助ともなる、シーサート構築及び運用に必要なマテリアル等の作成を目指す。

＜脅威情報共有 WG＞

緊密かつ信頼関係のあるシーサート間においてコンピュータセキュリティインシデントに関する脅威情報を共有する。

＜CSIRT FACT SHEET WG＞

日本国内の各シーサートの活動の背景情報(目的、組織内での位置、権限、人員、予算など)を整理して共有することで、既存のチームの改善や、新しいシーサート構築の支援に役立つ資料の作成を目指す。

出典：http://www.nca.gr.jp/activity/index.html

<Conclusions>

●「システム・セキュア化」と「セキュリティ運用強化」の両輪で・・・

攻撃側の“プロ化”や分業化”に対し、防御側は技術（検知・分析・対策）の高度化、内外の組織連携を機軸とした継続的な対応で迎え撃つ！

●信頼の輪を通じて、「いち早く、適材適所かつ、セキュア」に・・・

《組織の内》セキュリティ関係者による連携プレイ、関連ノウハウの蓄積
《組織の外》世界中のセキュリティ専門家組織と協調して諸問題を解決

●「人は石垣、人は城！」

【連絡先】

cert@ntt-cert.org

0422-59-7800

https://www.ntt-cert.org/