NTTグループが考えるセキュリティ対応の在り方

～CSIRTと法執行機関の連携に関する法的課題～

2012年5月25日

日本電信電話㈱　セキュアプラットフォーム研究所　山川智彦
㈱情報通信総合研究所　法制度研究グループ　小向太郎

項目

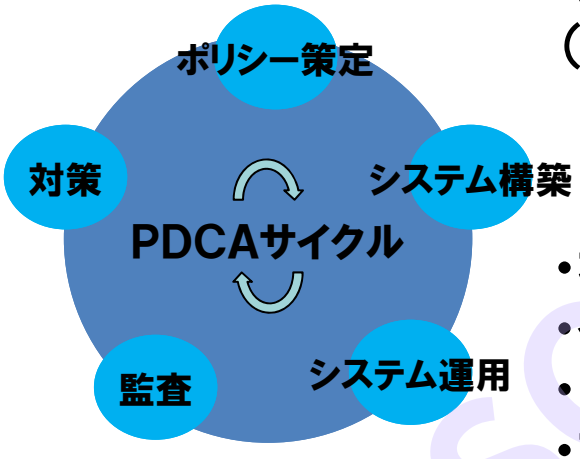
- コンピュータセキュリティインシデント対応の在り方
  ～CSIRT活動の紹介～
- NTT-CERTの紹介
- NTT西日本の展開事例
- CSIRTと法執行機関の連携に関する法的課題

1. コンピュータセキュリティインシデント対応の在り方
～CSIRT活動の紹介～

1.1　インシデントへの取り組みスタンス

・十分なセキュリティ対策を実施していてもインシデントは発生します。インシデント発生時に、落ち着いて迅速な対応をすることで被害を限定的にすることができます。

セキュリティ対策の基本



セキュリティ対策を継続的に実施していても
それでもインシデントは起こってしまう・・・
（対策範囲が広く、脅威が複雑化、高度化しています。）

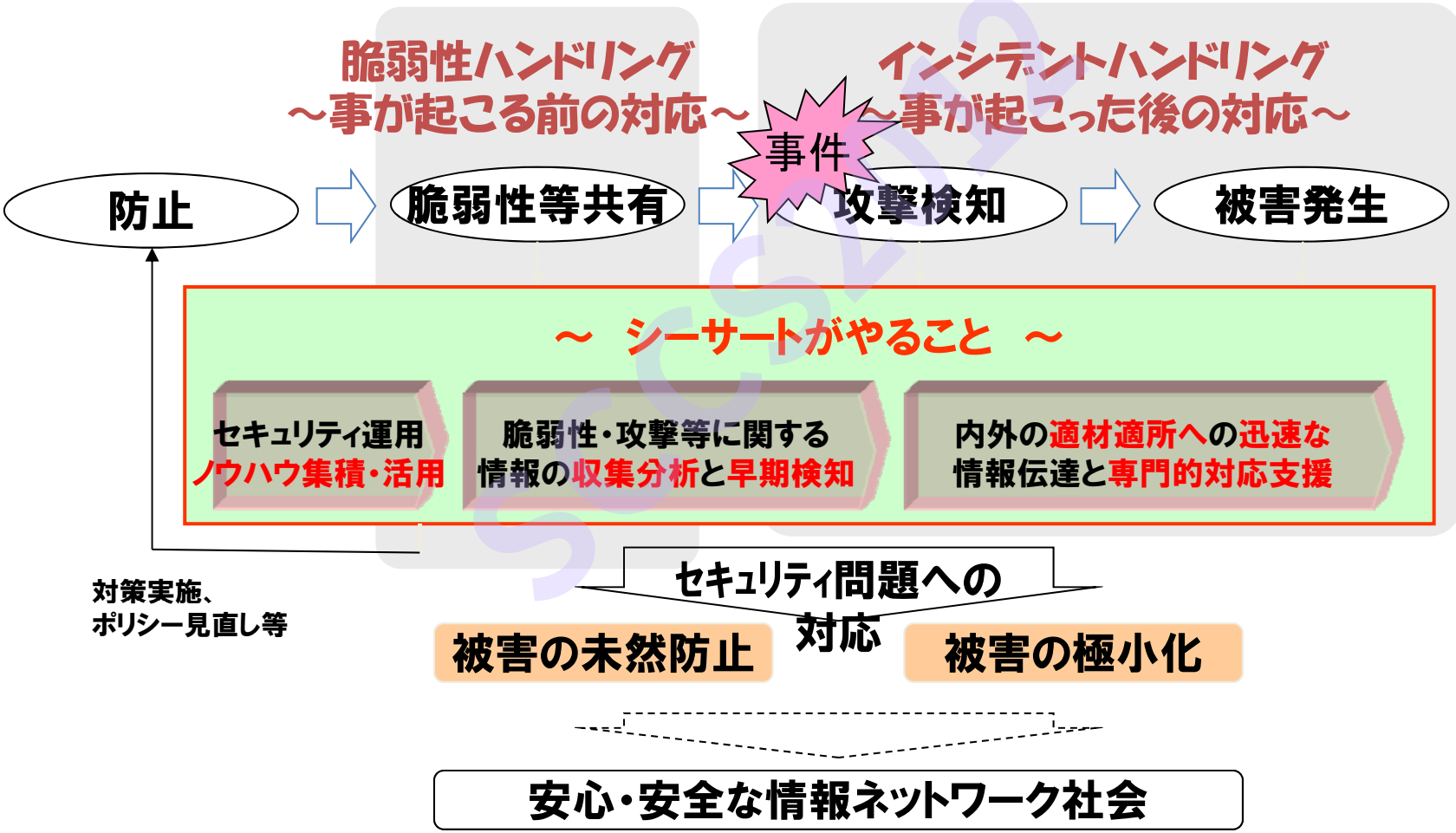
・社内で同じようなトラブルに悩んでいませんか？
・インシデントが発生したらすぐに動けますか？
・自社の対応に自信が持てますか？
・対応に必要な情報はもらえますか？

POINT！ CSIRTという事故前提組織が注目されています！

消防署

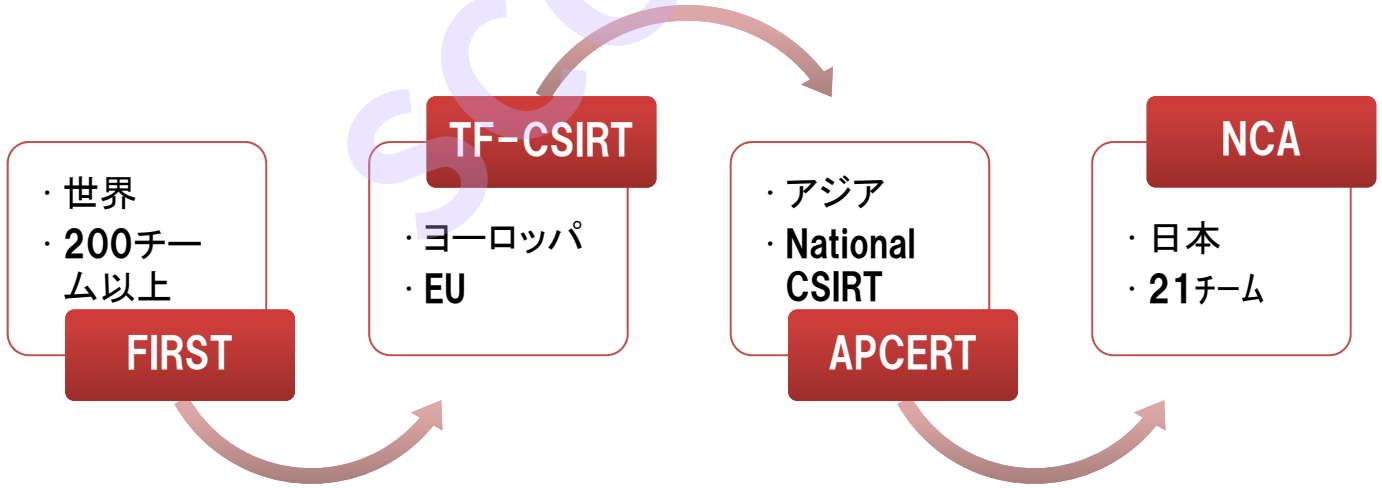
1.2　CSIRT(シーサート)のミッション

・シーサートは、組織内のインシデント・脆弱性について、セキュリティ管理者、システム運用者、外部のシーサート等と連携して、専門的に対応支援するチーム。



1.3 CSIRTの歴史と連携

・1996年にJPCERT/CCが誕生し、2012年4月現在、日本で27チームが連携しています。
・また世界で200チーム以上が活動しており、定期的に情報交換しています。



2. NTT-CERTの紹介

2.1.1. NTTグループのCSRと情報セキュリティ

*NTTグループウェブサイトより

2.1.2. NTTグループCSR憲章（2006年6月制定、2011年6月改定）

【CSR報告書　P21】

CSRメッセージ

私たちNTTグループは、情報通信産業の責任ある担い手として、最高のサービスと信頼を提供し、
“コミュニケーション”を通じて、人と社会と地球がつながる安心・安全で豊かな社会の実現に貢献します

CSRテーマ

■人と社会の コミュニケーション

①私たちは、より豊かで便利なコミュニケーション環境を実現するとともに、情報通信技術を活用し、
人口減少・高齢化社会におけるさまざまな課題解決に貢献します

■人と地球のコミュニケーション

②私たちは、自らの環境負荷を低減し、地球にやさしいコミュニケーション環境を構築するとともに、
情報通信サービスの提供を通じて社会全体の環境負荷低減に取り組みます

■安心・安全なコミュニケーション

③私たちは、情報セキュリティの確保や通信の利用に関する社会的な課題に真摯に取り組み、
安心・安全な利用環境と新しいコミュニケーション文化の創造・発展に尽くします

④私たちは、社会を支え生活を守る重要なインフラとして、災害時にも強い情報通信サービスの
提供に努め、いつでも、どこでも、だれとでもつながる安心と信頼を提供します

■ チームNTTのコミュニケーション

⑤私たちは、“チームNTT”として、高い倫理観と人権意識を持って事業に取り組み、働きやすい職場環境の整備や個の成長・多様性の尊重に努めるとともに豊かな地域社会づくりを推進し、社会的使命を果して行きます

※チームNTTは、派遣社員・契約社員も含めたNTTグループで働く社員、パートナーの皆さま、NTTグループのCSRに
賛同する退職した方々で構成されています。

2.1.3. 安心・安全なコミュニケーション

情報セキュリティの確保

・*情報セキュリティの確保・向上の研究・技術開発*
- 究極のセキュリティ「量子暗号」の実現に向けた研究 NTT
- クラウド時代のセキュリティ課題を解決する「インテリジェント暗号」を開発 NTT
- インターネットの脅威である、ボットウィルスなどマルウェアの撲滅・回避 NTT Communications
- 情報漏えいの防止を目的に、3ヵ年計画で大規模なセキュリティ対策を導入 NTTコムウェア
- 送信内容確認や上長承認機能を電子化した「FAX誤送信防止ソリューション」を開発 NTTソフトウェア

情報セキュリティマネジメントの推進・支援 NTTグループ
- NTT-CERTがNTTグループ内各社のセキュリティを支援
- 電気通信事業者向けのセキュリティ基準「ISO/IEC27011」を国内で初めて認証取得 docomo
- 「PDCAダブルループ」を実現し、グループ全体で情報セキュリティを推進 NTT DATA
- 「指紋認証」で「自動接続」できる情報漏えい対策に優れたリモートアクセスを発売 NTTIT

お客さまの個人情報の保護
- お客さまの個人情報保護 NTTグループ

重要インフラとして高い安定性と信頼性の確保

・*通信サービスの維持・管理*
・*災害への備え*
・*さまざまな安否確認手段*
・*通信サービスに関するさまざまな訓練*
・*お客さまの防災・災害対策の支援*

健全な利用環境の実現

・*安心・安全な利用のための知識とマナーの啓発活動*
・*子どもの安全確保のためのサービス提供*

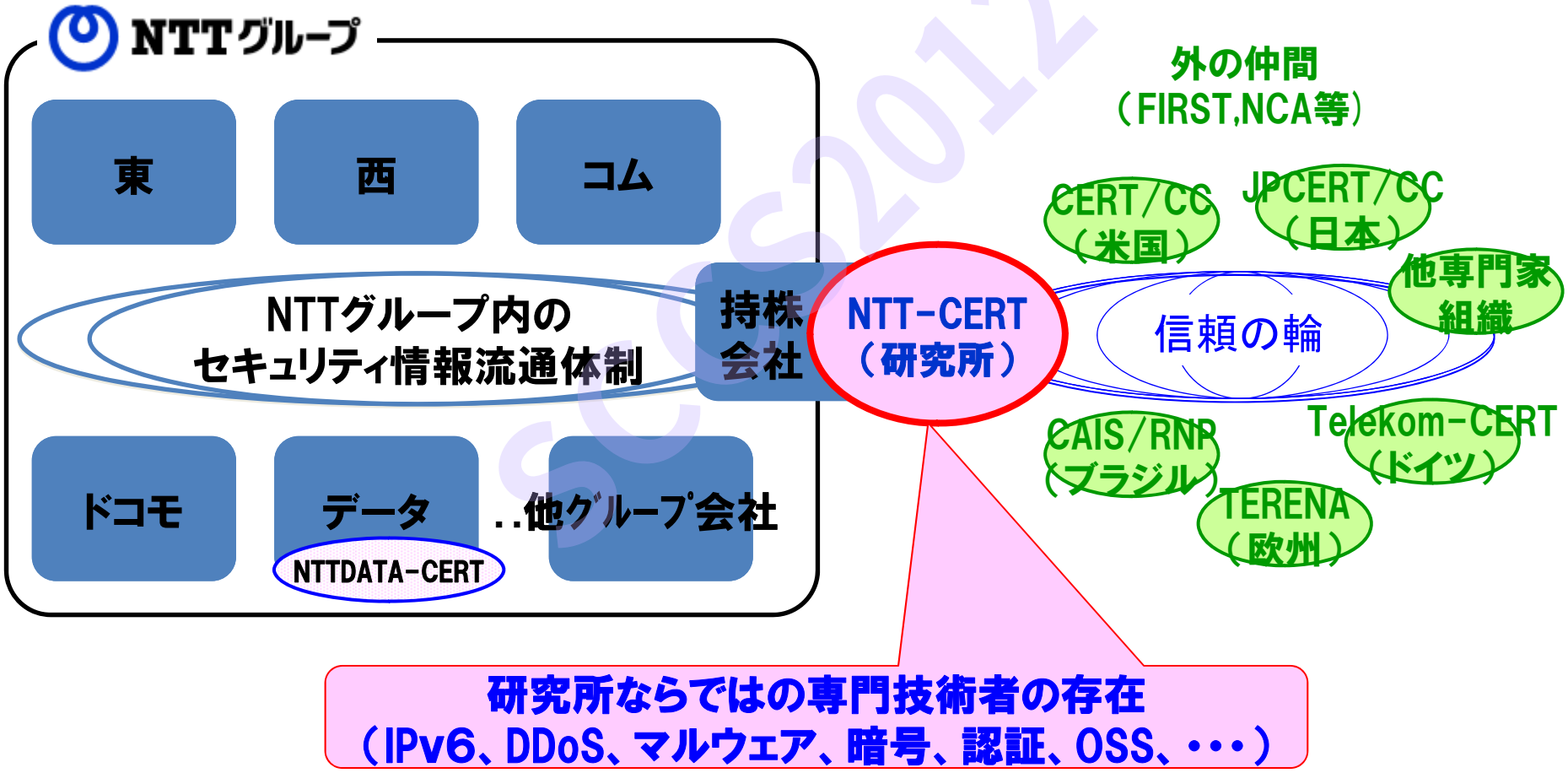
お客さまの満足に向けた取り組み

・*お客さま満足の追求*
・*品質マネジメント体制の構築とさまざまな品質向上の取り組み*
・*ユニバーサルデザインの推進*

*NTTグループウェブサイトより

2.2 NTTグループの連携体制について

- 外の仲間との信頼の輪を強化し、研究所内専門技術者との連携を図りつつ、セキュリティ強化や関連技術のノウハウを蓄積しています。
- NTTグループ各社に、蓄積したノウハウをナレッジ提供しています。



2.3 NTT-CERTの業務概要

・NTTグループのインシデント対応窓口として活動しています。
・インシデントの予防措置、早期発見、迅速な事後対応を目的として様々な情報収集活動をしています。

●事前対応

セキュリティ-レポーティング	・・・ 調査・入手した情報（最新動向、技術情報、トピック記事等）の配信
セキュリティ-アラート	・・・ 脆弱性の情報を事業会社に報告。適宜、外部機関との調整を実施
インシデント検知・報告	・・・ 自前の／外部からの情報を元に、インシデントをいち早く検知・報告

●事後対応

脆弱性ハンドリング	・・・ 確認された脆弱性に対し、事業会社での対応をサポート
インシデントハンドリング	・・・ 検知されたインシデント（情報漏えい、不審アクセス、侵入改竄等）に対し、事業会社での対応をサポート。
フォレンジック	・・・ デジタル鑑識の実施（インシデントの原因究明に際し、機器やデータを分析し、法的な証拠性を明らかにする）

●セキュリティ品質向上

セキュリティ-コンサル	製品・方式評価	・・・ 開発中後の製品・方式のセキュリティ評価支援等
セキュリティ-啓発	セキュリティ-教育	・・・ ポータルや各種トレーニング等を通じたグループ全体のセキュリティ底上げに寄与

2.4 NTT-CERT活動(インシデント検知・報告)

・様々な情報を日々点検確認し、インシデントの早期発見に努め、被害の拡大を予防しています。

パブリックモニタリング

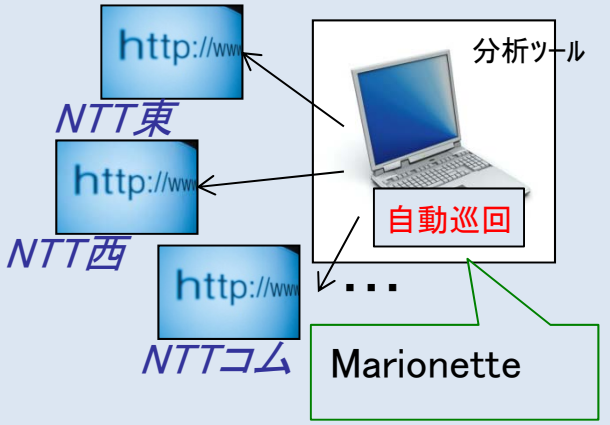
Black-list掲載サイト調査

掲示板書き込み調査

情報拡散調査

マルウェア被疑サイト調査

グループのWebサイト改ざん調査



3.NTT西日本の展開事例

3.1　CSIRT(NTT-CERT)ノウハウを活かした活動

・NTT西日本では、NTT-CERT活動(NTTグループを脅威から守る)で蓄積した技術ノウハウをお客様のセキュリティー品質向上に役立てています。

セキュリティ事故の未然防止

- **セキュリティー診断サービス**
  - サーバーセキュリティーチェックサービス　・・・　事例①
    （サーバーやネットワーク機器の脆弱性を検査し、分析結果を報告）
  - Webアプリケーションセキュリティーチェックサービス
    （Webサイトに潜む脆弱性などを検査し、分析結果を報告）
- **不正アクセス防御ソリューション**
  （IDS/IPS、UTM、WAFの導入から監視、運用までをサポート）

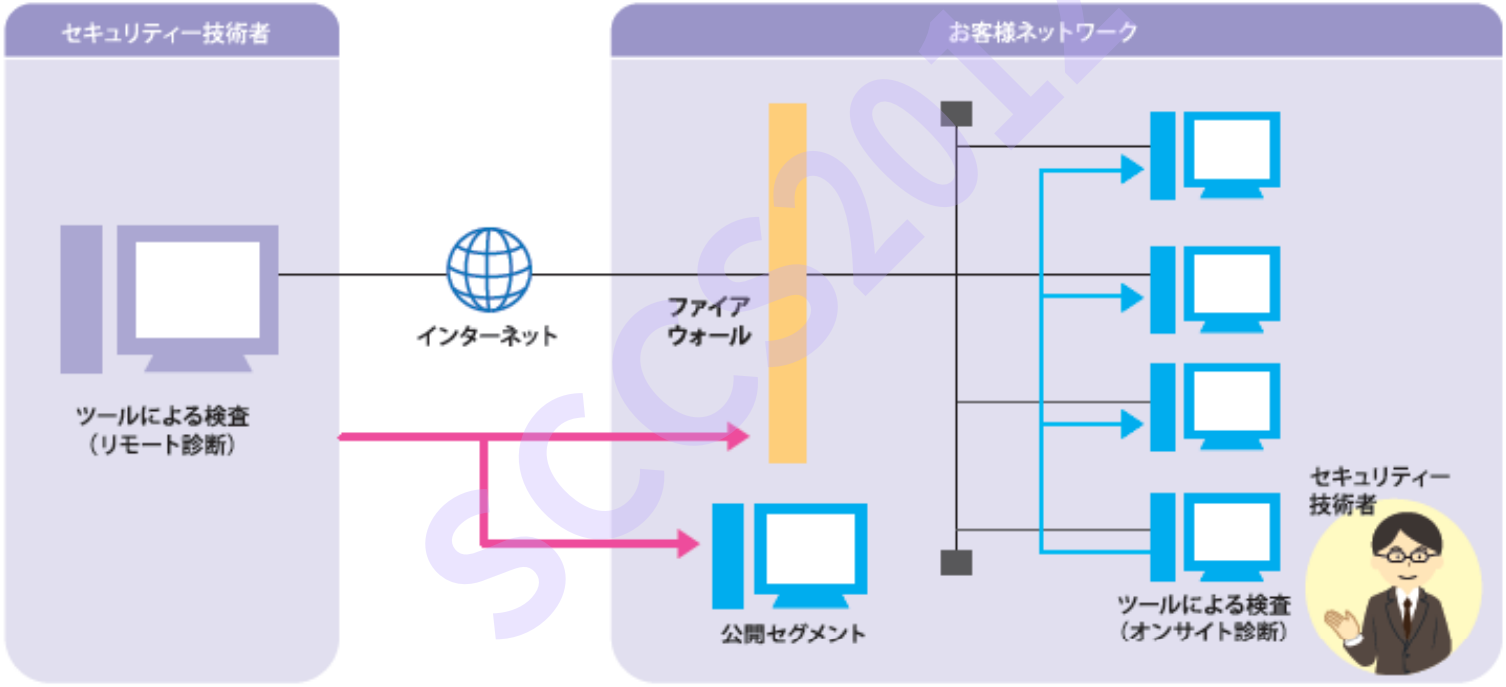
セキュリティ事故の再発防止

- **情報セキュリティーインシデント対応サービス**　・・・　事例②
  （不正アクセスなどによるセキュリティ事故に対し、原因分析、再発防止策を提案）

※詳細は、お配りしているセキュリティサービスカタログをご確認ください。

3.2.1　セキュリティー診断サービス（概要）
サーバーセキュリティーチェックサービス

サーバーやルーター等のネットワーク機器における脆弱性は、そのままにしておくと不正アクセスや情報漏えい等の被害にあってしまう恐れがあります。
このサービスでは、お客様の環境に対し、セキュリティ技術者が脆弱性を検査・分析し、分析結果および具体的な改善策を報告します。



【検査方法】

◎リモート診断
インターネット経由のセキュリティー検査を実施。グローバルIPアドレスを持つサーバーやネットワーク機器に対して検査が可能です。

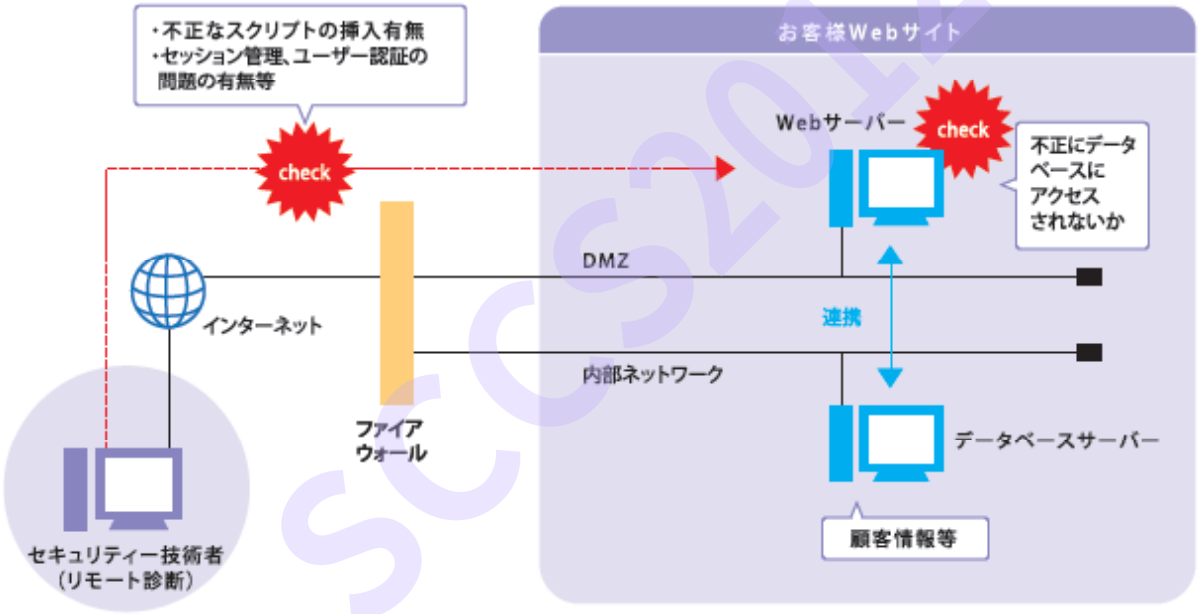
◎オンサイト診断
お客様の社内ネットワーク内部から、セキュリティー検査を実施。IPアドレスを持つすべてのサーバーやネットワーク機器に対して検査可能です。

【主な検査内容】

- OS脆弱性
- DoS脆弱性
- バックドア検知
- ID/パスワード
- ポートスキャン 等

3.2.2　セキュリティー診断サービス（概要）
Webアプリケーションセキュリティーチェックサービス

重要な情報や個人情報等を扱うWebアプリケーションの脆弱性は、そのままにしておくと情報漏えいやWebサイト改ざん等の被害にあってしまう恐れがあります。
このサービスでは、お客様のWebアプリケーションに対して、セキュリティ技術者が脆弱性を検査・分析し、分析結果及び具体的な改善策をご報告します。



【診断対象となるWebアプリケーション】

オンラインショッピングや会員向けサイト等、重要な情報（クレジットカード情報や、会員ID/パスワード等）を取り扱うWebアプリケーションが対象となります。また、資料の請求フォームや問合せフォームといった個人情報の入力可能なWebアプリケーションも対象となります。

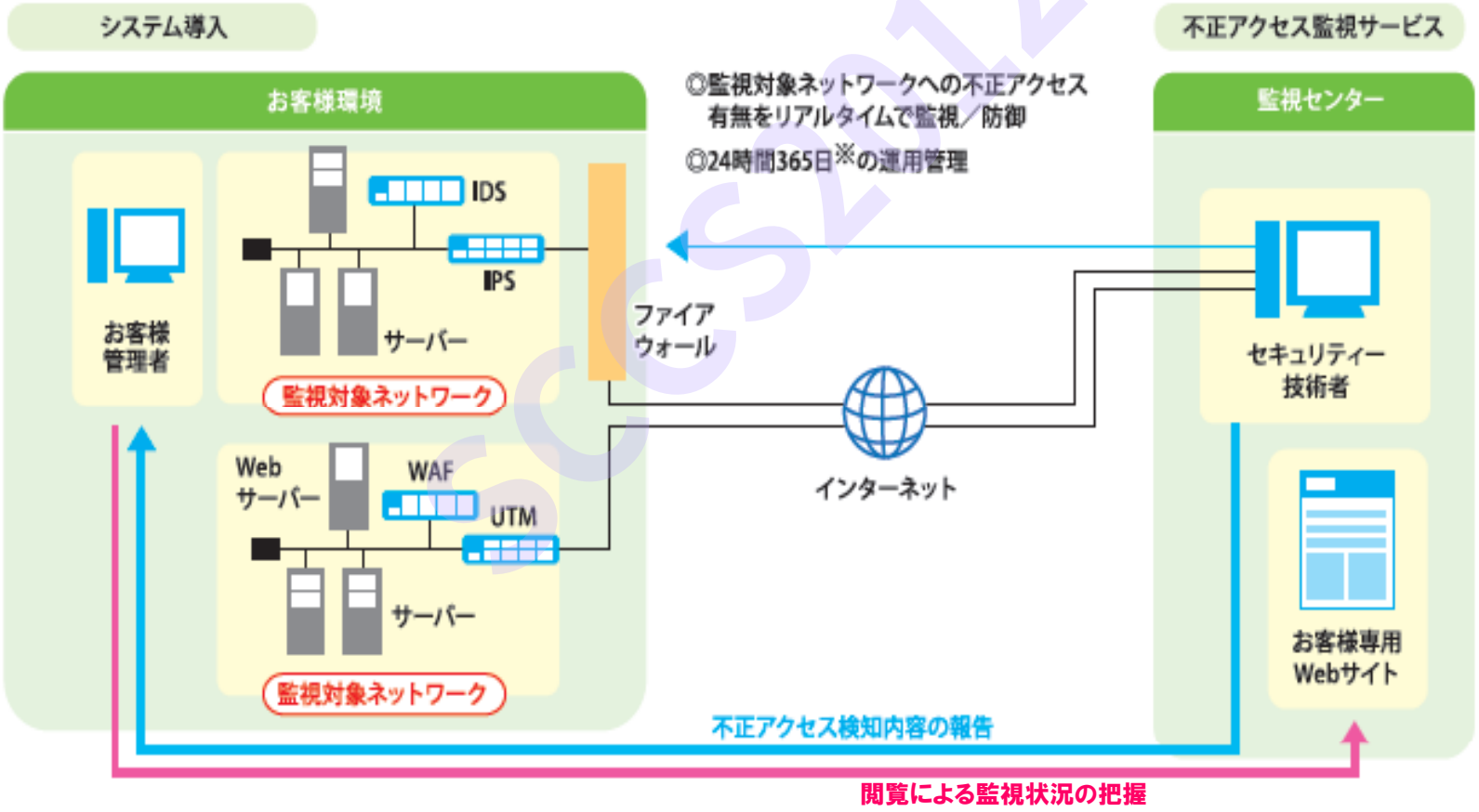
<診断対象イメージ>

【主な検査内容】

・クロスサイトスクリプティング
・SQLインジェクション
・セッション管理
・認証
・ファイル拡張子 等

3.2.3　不正アクセス防御ソリューション（概要）

IDS/IPS、UTM、WAFの導入により、不正アクセス対策を行い、お客様システムの更なるセキュリティ強化をサポートします。また、監視サービスの追加によりお客様に代わって専門家が、運用や攻撃の分析を実施するので、高度な防御品質を維持しながら、専任担当者雇用などのコスト削減が期待できます。



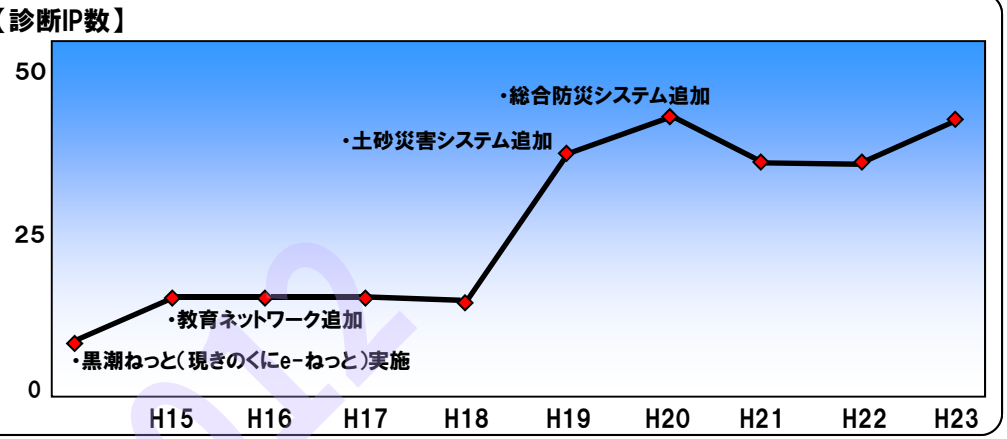
3.2.4　情報セキュリティーインシデント対応サービス（概要）

昨今、インターネットが企業や自治体におけるビジネスのインフラとして重要度を増す一方で、不正アクセスの手口は複雑化し、ホームページの改ざんや情報漏えい等が後を絶ちません。
このサービスでは、NTTが有するこれまでの実績やノウハウ、インシデントに対する高度な分析技術などを活用し、事故発生時に、証拠データの保全から原因分析、被害状況の確認、適切な再発防止策を提案します。

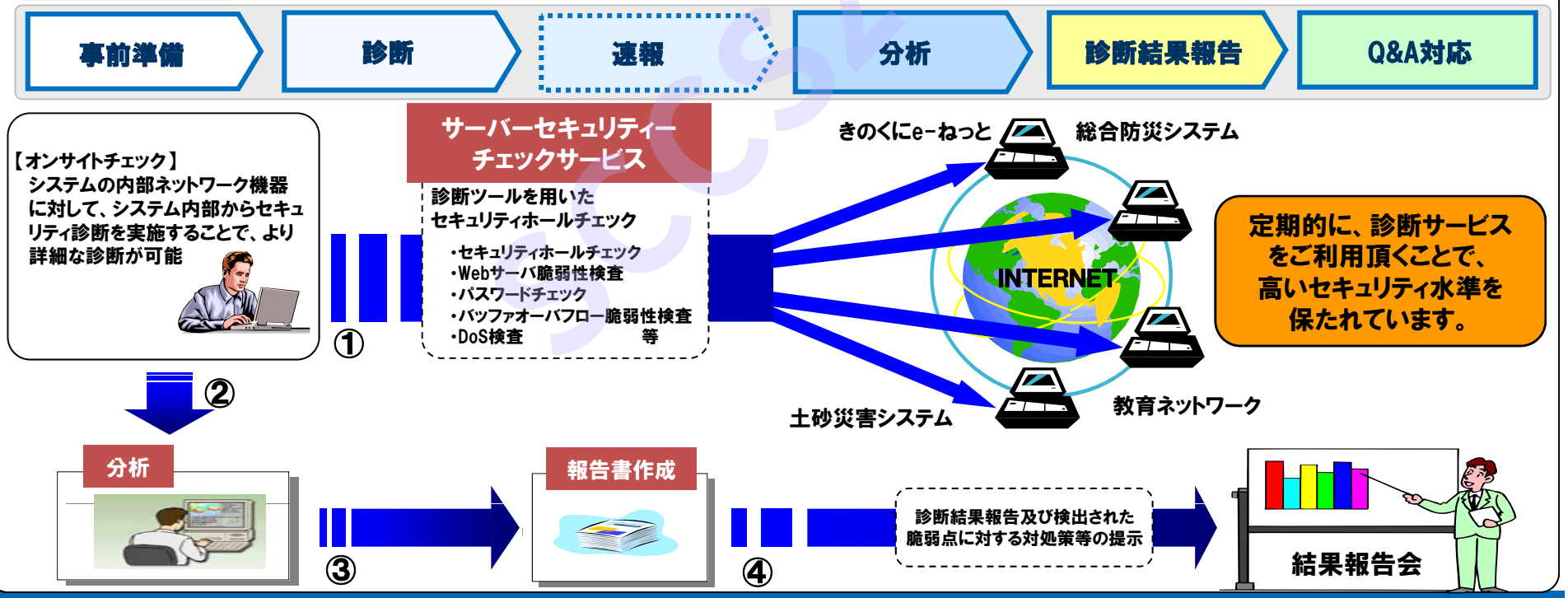
3.3.1 事例1　和歌山県庁様へのセキュリティー診断の取組について

背景・経緯

H14年度の初診断において、事前調査・ヒヤリングから確実な診断の実施、分析結果に基づく適切な対処策の提示・説明等、お客様目線に合わせた判り易い報告等により、高い評価をいただき、新システム増設や県庁内他部署並びに関連組織へのご紹介等により対象設備を拡大するなど、継続して高い評価をいただいております。



実施概要



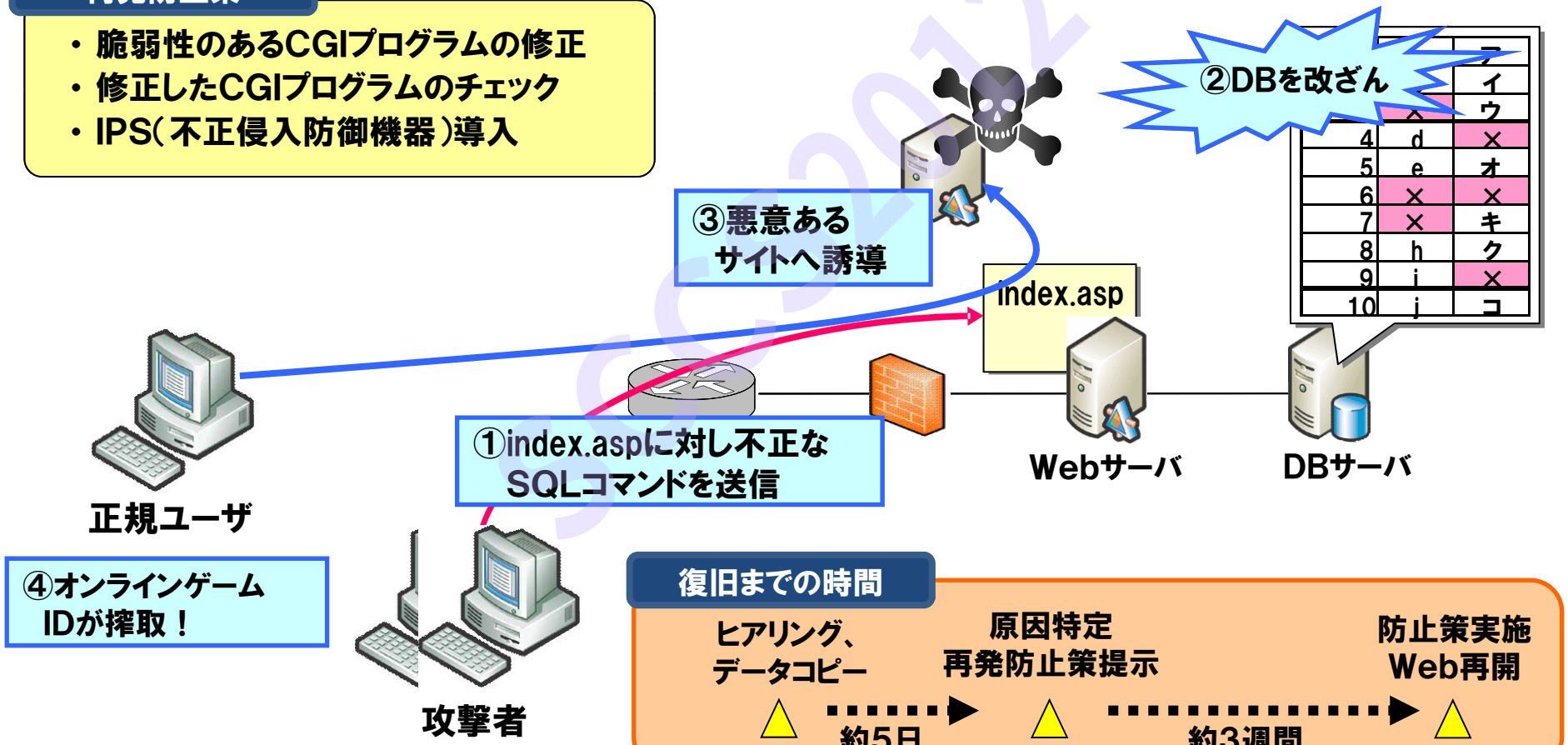
3.3.2 事例2　公開Webサーバーの改ざん事件

確認された事象

- 攻撃者がSQLインジェクションにより、DBサーバ上の情報を不正に改ざん
- 正規ユーザがアクセスした際、不正なJavaスクリプトにより悪意あるサイトへ誘導
- 悪意あるサイトでウイルス感染し、端末のオンラインゲームIDを搾取される

再発防止策

- 脆弱性のあるCGIプログラムの修正
- 修正したCGIプログラムのチェック
- IPS（不正侵入防御機器）導入



復旧までの時間

ヒアリング、データコピー　→（約5日）→　原因特定 再発防止策提示　→（約3週間）→　防止策実施 Web再開

閑話休題

政策の視点から「サイバーセキュリティ」を
あらためて考えてみる

ジョセフ・ナイ教授の著作「スマート・パワー」より

第5章　力の拡散とサイバー・パワー

【情報革命】

- 情報革命＝コンピュータ、通信、ソフトウェアの技術が急速に進展。それにより情報の作成、処理、伝達、検索のコストが劇的に低下。
- インターネットは多彩なコミュニケーションが可能で、一元的管理がないため、「1984」とは逆に、力の分散が起きている。
- 政府は国際政治を一元的に管理できなくなる。

【政府と国際主体】

- サイバー社会における主体の多様化
  - 力の拡散の観点→主権国家がどう機能するのか
  - 多国籍企業
  - 国際非政府組織：情報革命によるソフト・パワーが拡大
  - テロリスト集団

【サイバーパワー】

- サイバー空間＝物理的資産と仮想的資産の独特の組み合わせ
  - 物理的資産の層=インフラ。経済法則と政治法則
  - 仮想的資産の層＝情報。ネットワーク経済。国家による支配の困難
- 人口の空間。ほかの領域より変化が速い。

「スマート・パワー」（続）

【行為主体とそれぞれの力の源泉】

主要国政府

1. インフラ、教育、知的財産の開発と支援
2. 領土内の個人と仲介企業に対する法的、物理的な強制
3. 国内市場の規模と市場参入の規制（EU、中国、アメリカ）
4. サイバー攻撃とサイバー防衛（政府組織、予算、情報機関）
5. 公共財の提供（経済活動に必要な法規など）
6. 正当性、善意、有能さに関する評価（ソフトパワーの源泉）

大規模な組織と高度に組織化されたネットワーク

1. 巨額の予算、人材、規模の経済
2. 各国で活動できる柔軟性
3. 独自ソフトと製品開発の管理、アプリケーションの自己増殖
4. ブランドと名声

多国籍企業、犯罪組織、テロリスト

結びつきが緩いネットワークと個人

1. 参入コストの低さ
2. 事実上の匿名性と退出の容易さ
3. 政府や大組織と比較したときの脆弱性の低さ

Hactivist

脆弱性

- 攻撃に弱い複雑なシステムへの依存
- 政治的な不安定性
- 名声が失われる可能性

- 訴追
- 知的財産窃盗
- システム障害
- 名声が失われる可能性

- 捕らえられたときに政府と組織から受ける合法的、非合法的な強制力の行使

（出典）「スマート・パワー」P174に加筆・修正

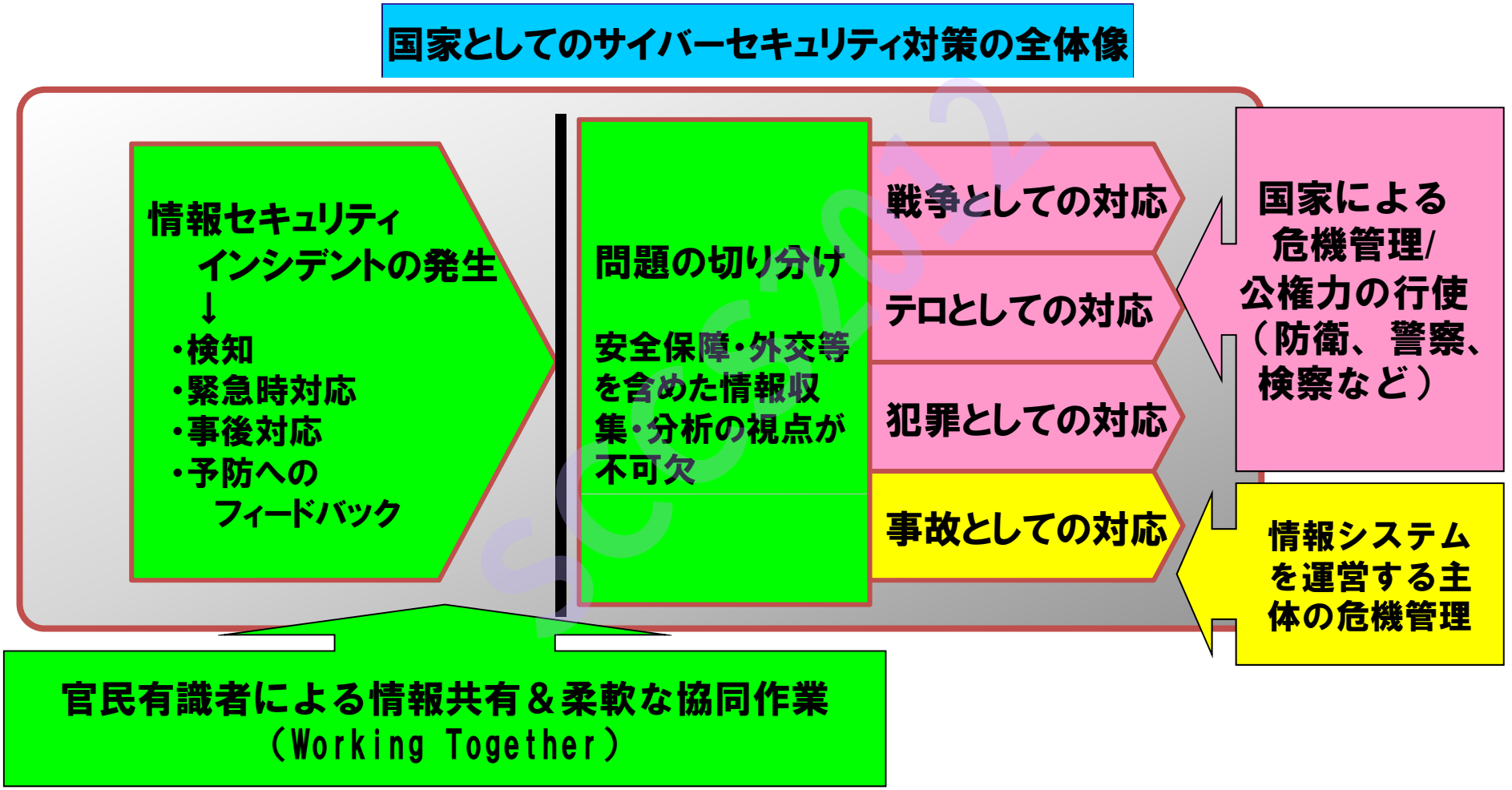
「スマート・パワー」（続）

【政府と統治】

- 主権国家はサイバー空間をどうやって統治するか？
- 主権国家にとっての国家安全保障への脅威。それぞれ解決方法が違う
  - ①　経済スパイ
  - ②　犯罪
  - ③　サイバー戦争
  - ④　サイバーテロ
- 現在被害が最も大きいのは「経済スパイ」と「犯罪」だが、今後十年で順位が変わる可能性がある
- 潜在的脅威の中で最も劇的なのが「サイバー戦争」

サイバーセキュリティ対策の全体像

国家としてサイバーセキュリティ対策を見直すには、安全保障・外交等を含めた情報収集・分析の視点が不可欠である。一方、限られたリソースの中で最大の効果を得るためには、国家として取り組むべき領域の明確化と、民間の力を活用可能なスキームを整理する必要がある。



「問題の切り分け」と「その後の対応」に関する法整備が必要

（参考）RSA Conference 2012キーノートより

国防総省次官　Ashton Carter

*国防総省
ウェブサイトより

- 国家、犯罪者によるサイバー攻撃に対応するため、先端的技術開発と合衆国官民レベルでの能力向上が必須。
- 脅威のターゲットとなるのは、軍事ネットワークだけでなく、DoDが依存する重要インフラ。DHSだけでなく、DoDもセキュリティの責任の一端を担う必要がある。特にNSAのセキュリティインテリジェンスを民間に転用することは、DHSにとっても意義は大きい。
- セキュリティニーズにあわせた官民情報共有の進め方が重要。DoDとしては、先進的な民間技術への期待が大きい。DoDとしてはサイバーセキュリティ分野への支出を拡大していく。

FBI長官　Robert S. Mueller, III

*FBI
ウェブサイトより

- インターネットの先端的技術は、犯罪者や国家にもサイバー攻撃の手段として利用される。未だフルスケールのサイバー攻撃に使われたことはないが、その能力は過小評価されるべきではない。
- 法執行機関と民間企業が協力して市民の安全、安心を守ることが必須。昨年度は民間と協力して大規模なBot net（Coreflood）を防いだが、それもタイムリーな情報共有が重要であった。
- サイバーの脅威に対応するには、リアルタイム情報共有が必須であり、政府と民間セクターで共有されるべきである。一度攻撃されたとしても、その教訓を生かして事故再発を防ぐ企業と、同じ過ちを繰り返す企業が存在する。

最近の傾向をまとめると

- アメリカ型
  - テロ、犯罪、Cyber Espionage・・・
  - SOCとCSIRTの連携
    - SOC=Security Operation Center。ネットワーク機器、サーバなどのログ、データを収集・分析→脅威からの監視
    - CSIRT＝セキュリティインシデント対応

- 欧州型
  - サイバー犯罪対応がホットイシュー
  - サイバー犯罪対応を語る文脈ではPrivate Sector=CSIRTまたはCERTを意味する

    （例）欧州評議会　サイバー犯罪に対する法執行機関とISPの協力についてのガイドライン
  - SOCのような大規模ビジネス市場は未成熟？

- 日本型？？

企業としての問題意識

- 「情報セキュリティ」で、複数の目的に対応する必要
  - サイバー犯罪
  - 重要インフラ防護
  - 情報の保護（財産的情報、個人情報の保護）
  - コンプライアンス、CSR

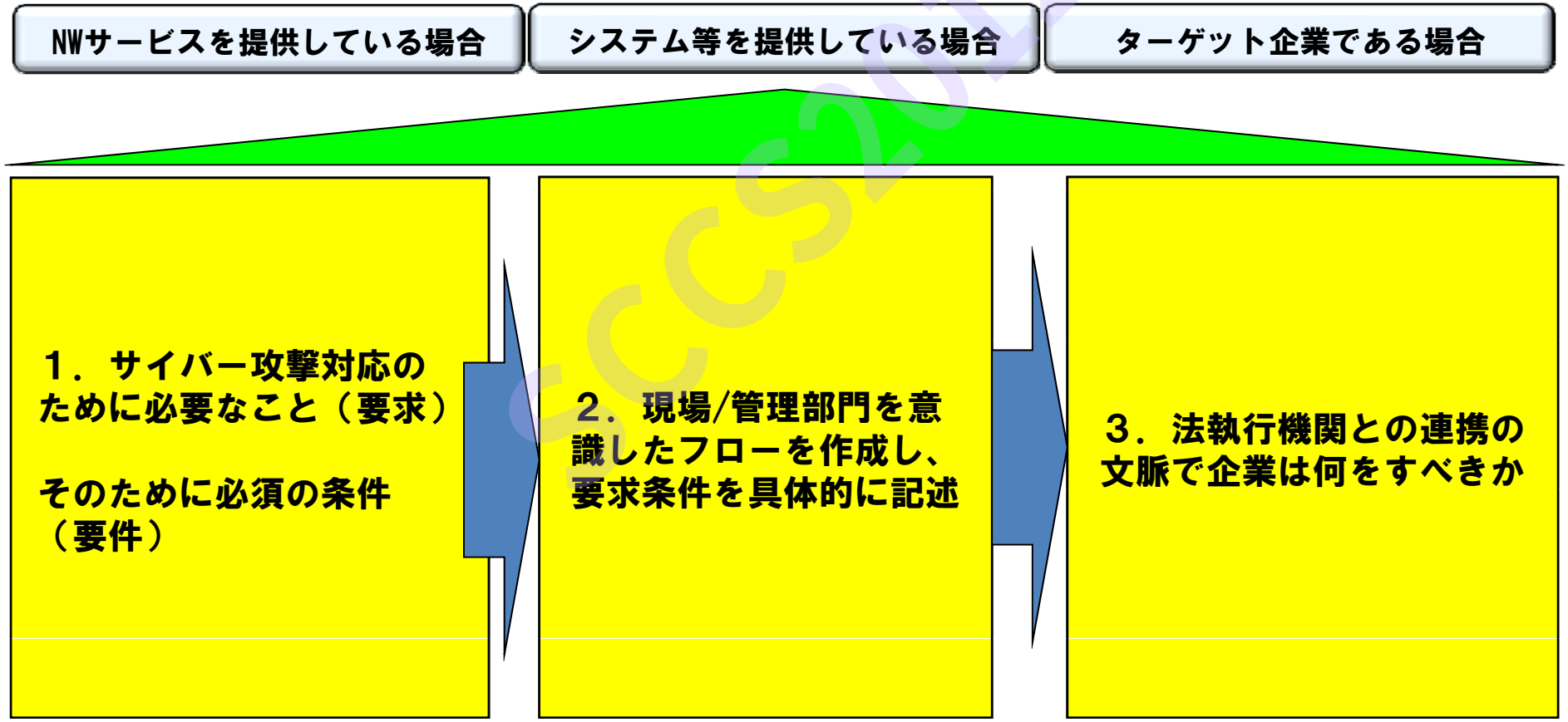
- 事後対応（万が一、インシデントが発生したら）
  - 早急なサービス復旧、被害拡大の阻止

- 事前対応（インシデント発生の前に）
  - ほかでの攻撃事例を分析することで、事前の対策策定・実施

- 法執行機関との連携
  - 犯人逮捕による再発防止
  - 法の手続きに則って実施
  - 緊急時の対応だけでなく、平時のセキュリティレベル底上げにも役立つ？

NTT-CERTとしてのリサーチ＝サイバーディフェンス標準モデル

- H22年度：インシデントマネジメントモデル
  - CSIRT等のインシデントマネジメント体制に関する調査
    - NTTグループのほか、他社の先進的CSIRTにヒアリング
    - 企業のガバナンスの観点からCSIRTに求められる役割
- H23年度：サイバーディフェンス標準モデル
  - CSIRTマネジメント体制に関する調査結果をふまえつつ、以下の3つの場合について、サイバー攻撃対応を意識したフローを作成



4. CSIRTと法執行機関の連携に関する法的課題

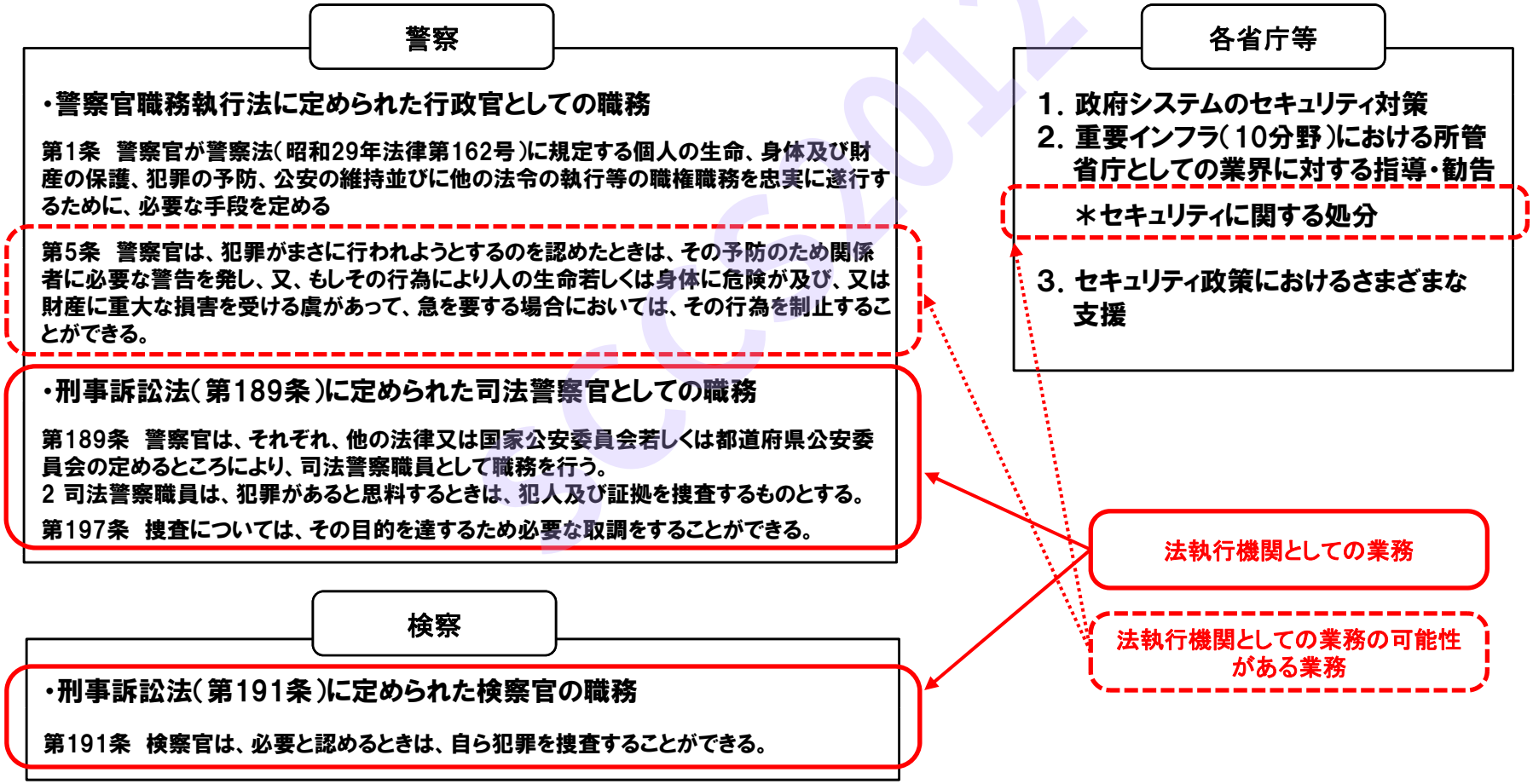
㈱情報通信総合研究所
法制度研究グループ
小向主席研究員

目　次

1-1. 法執行機関の定義(1/2)

*NTT研究企画部門、㈱情報通信総合研究所調査

・法執行機関とは、被疑者やNW等の関連事業者、攻撃対象となった機関に対して、『行政上の強制執行又は即時強制を職務とする行政機関』(法律学小辞典[有斐閣]による)と定義することができる。
・したがって日本において、サイバーディフェンスにおける法執行機関の代表とは、強制力を伴う犯罪捜査を行う 警察等の捜査機関のことであり、各省庁等のセキュリティ対策に取り組む公的機関が実施している支援業務は、法執行機関の業務には含まれないと考えられる。



1-1. 法執行機関の定義(2/2)

*NTT研究企画部門、㈱情報通信総合研究所調査

・日本においては、法執行機関として検察や警察、自衛隊などが挙げられるが、どの機関が関わるかは、対象となる脅威によって異なると考えられる。

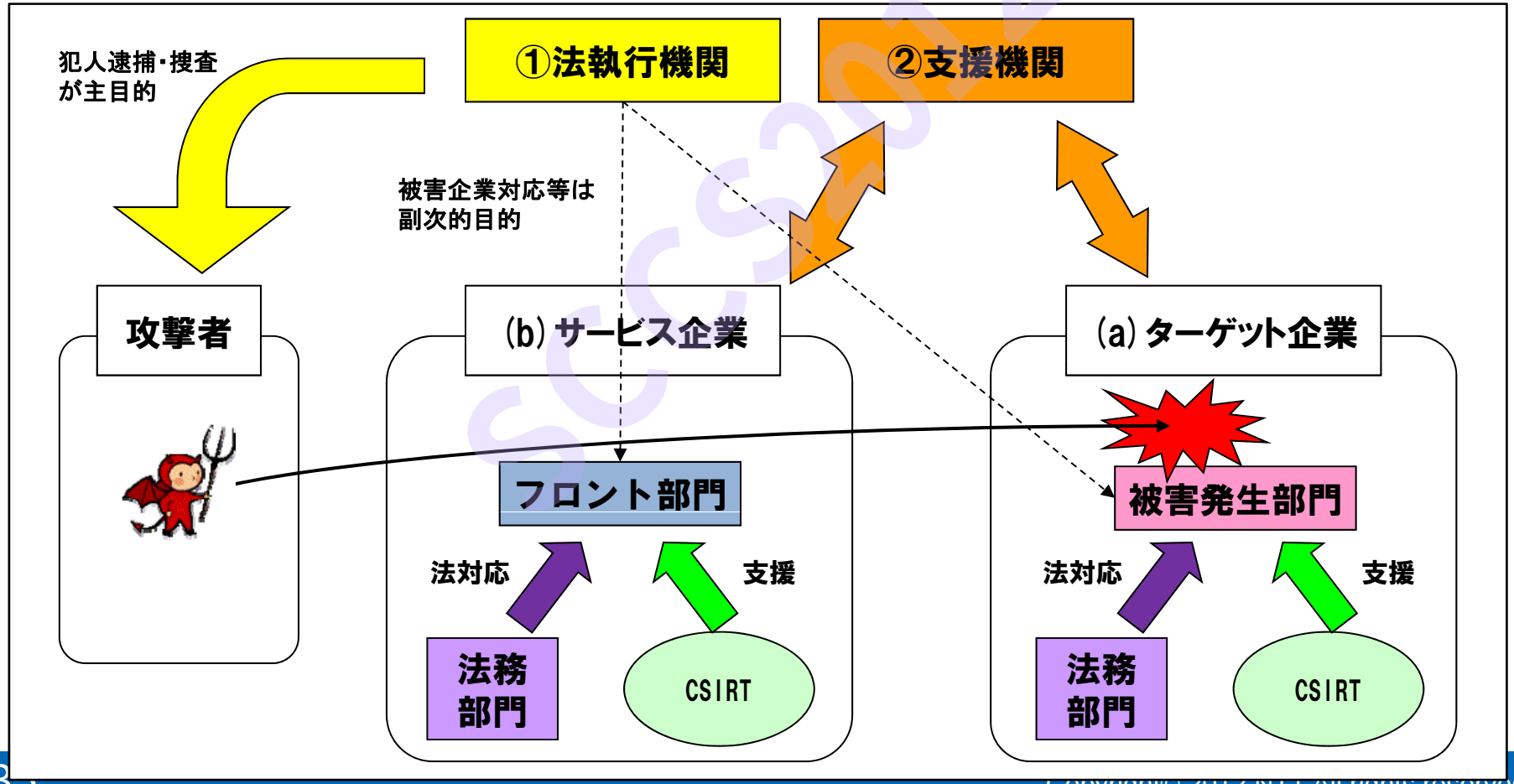
対象となる脅威		法執行機関	セキュリティ対策に取り組む公的機関		所管省庁
		犯罪関連	セキュリティ政策における支援		対策・指導等
●政府機関に対する攻撃		警察 (サイバー犯罪の取締り) 検察 (刑事事件の起訴)	内閣官房 (政府横断的な情報収集・分析、安全な暗号利用の推進など)	防衛省 (国の安全保障関係) 総務省 (通信・ネットワーク政策) 経済産業省 (情報政策)	各府省庁
●重要インフラ(10分野)に対する攻撃	・情報通信		内閣官房 (情報共有の推進、安全基準等の整備浸透、防護対策の向上など)		総務省
	・金融				金融庁
	・航空 ・鉄道 ・物流				国土交通省
	・電力 ・ガス				経済産業省
	・政府、行政サービス				総務省
	・医療 ・水道				厚生労働省
●民間企業に対する攻撃			内閣官房 (安全性・信頼性の高いIT製品等の利用促進など)		(主務官庁)(注)

(注)迷惑メールの場合、総務大臣が電子メールの送信上の支障を是正するよう措置命令を実施でき、経済産業大臣が規制内容に従わない事業者等に対して、指示・業務停止命令を実施できる。

1-2. CSIRTと法執行機関の連携イメージ

*NTT研究企画部門、㈱情報通信総合研究所調査

・攻撃者がターゲット企業に攻撃を仕掛けた場合、①法執行機関 や ②支援機関が、(a) ターゲット企業 や (b) サービス企業(ターゲットにNWなどのサービスなどを提供している企業)との連携をどう考えるかが課題である。
・CSIRTは、(a) ターゲット企業の被害発生部門、(b) サービス企業のフロント部門の背後にいて、彼らが、①法執行機関と対応するのを支援する。ただし、法務対応とは別ラインであると考えられる。
・特にクラウドサービスの場合は、サービスを提供している企業が攻撃を受けた場合に、サービスを提供している顧客企業が攻撃を受けているのか、自社が攻撃を受けているのか、明確に区分できない場合がある。



1-3. 米国における取り組み状況

*NTT研究企画部門、㈱情報通信総合研究所調査

・米国においては、国防総省(DOD)が2011年7月、外国からのサイバー攻撃への対応方針となる「サイバー軍事戦略」を発表し、サイバー空間における攻撃に対応する戦略を強化することを明確にしたところである。

・米国におけるサイバーセキュリティ政策は、クリントン政権において重要インフラ保護のための政策を打ち出したことに端を発するが、オバマ政権においては様々な連邦省庁や民間も含めた体制の構築を目指している。

連邦政府におけるサイバーセキュリティ政策の経緯

・1996年 6月　クリントン政権において、大統領令13010号を発令　⇒重要インフラ保護のための政策を打ち出す
--2001年9月　同時多発テロ発生--
・2001年10月　ブッシュ政権において、大統領令13231を発令
・2001年10月　USAパトリオット法成立　⇒電話及びインターネット等の通信内容の傍受などが米国の捜査当局に認められた
--2001年11月　サイバー犯罪に関する条約成立--
・2003年 1月　サイバーセキュリティ政策に係る権限を、新たに設置された国土安全保障省(DHS)に移管
・2003年 2月　National Strategy to Secure Cyberspaceを発表
＊2006年 8月　米国連邦捜査局(FBI)は、オンライン詐欺の取締り強化に向けて、「Operation Identity Shield」と呼ばれる新たな捜査班を設置し、民間企業との連携を強化した。
・2008年 1月　包括的サイバーセキュリティ・イニシアティブ(NSPD54/HDPD23)策定
⇒DODのNSA(National Security Agency)等諜報機関における侵入等に係るモニタリング等を強化した。
・2009年 1月　オバマ政権において、Homeland Securityに係るアジェンダにおいて、情報セキュリティに係る6項目の中で、サイバーインフラが戦略的資産であると宣言
・2009年 2月　サイバーセキュリティ政策の60日間での見直しを開始　⇒サイバーセキュリティに関する議論が活発化した
・2009年 5月　Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure発表
⇒サイバーセキュリティを経済繁栄・安全保障の基盤と位置付けた
・2009年12月　国家のサイバーセキュリティ政策・活動の調整に責任を有する担当者(Cyber Security Coordinator)を新設
・2010年 7月　サイバースペースにおける個人アイデンティティの信頼性向上を目指すための戦略のドラフト公表
・2011年 1月　DHSの権限強化等により、サイバー及び物理的インフラを保護するための法案(Homeland Security Cyber and Physical Infrastructure Protection Act)議会に提出
・2011年 7月　DODがサイバー軍事戦略を発表
⇒サイバー空間を、陸・海・空・宇宙空間に次ぐ第5の軍事領域と位置付け、サイバー空間における攻撃に対応する戦略を強化することを明確にした

1-4. 欧州における取り組み状況

*NTT研究企画部門、㈱情報通信総合研究所調査

・欧州においては、2007年に起きたエストニアにおける大規模なサイバー攻撃や中国が起源とされるサイバー攻撃により、サイバーセキュリティに関する意識がますます高まっている。

・欧州におけるこれまでの取り組み状況は、次のとおりである。

EUにおける取り組みの経緯

・2004年　サイバーセキュリティ対策の専門機関である「欧州ネットワーク・情報安全庁（European Network and Information Security Agency：ENISA）」を設立
　⇒ICTインフラの保護に関する政策及び法整備が大きく進められることになった
・2006年　ICTインフラセキュリティ戦略「安全情報社会のための戦略―対話、パートナーシップ、強化―」を打ち出す
・2009年　「重要情報インフラ防護」プログラムおよび2009年電子通信規制改革パッケージ
　⇒2002年に成立した「電子通信ネットワークとサービスのための共通規制枠組に係る指令」が改正された
・2010年5月　ICT政策パッケージ「デジタル・アジェンダ」
　⇒ICTインフラ保護に関する政策を打ち出す

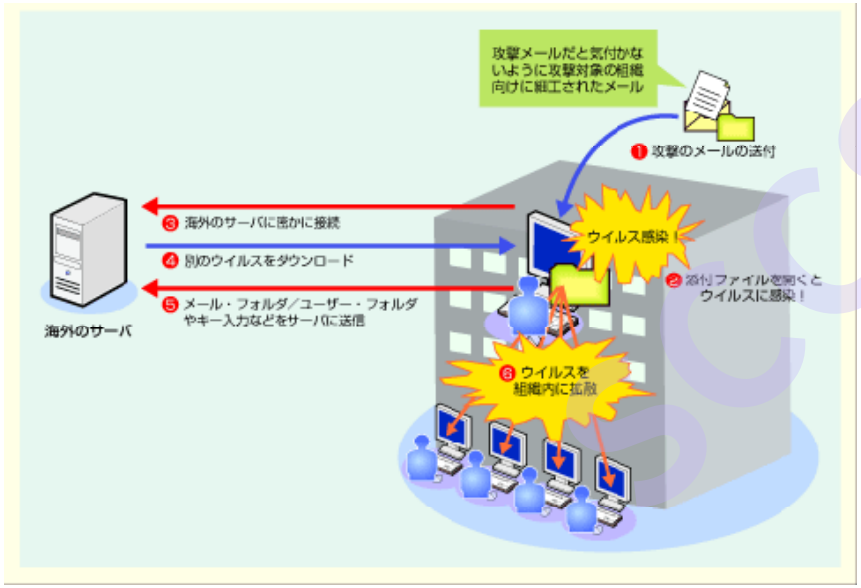
欧州評議会における取り組みの経緯

＜2001年11月、サイバー犯罪に関する条約採択＞
・2005年末　司法・内務閣僚理事会の要請を受けて、「欧州重要インフラ防護プログラム」の策定を開始し、2006年末に同プログラムを発表
・2009年3月　「重要情報インフラ防護についての通達書」を発表
・2010年　EUの新しい通信網および情報セキュリティ方針を策定
・2013年までに、EUおよび全世界レベルでのサイバー空間上の規則を制定する予定

2-1-1. 法執行機関との連携の必要性(1/4)

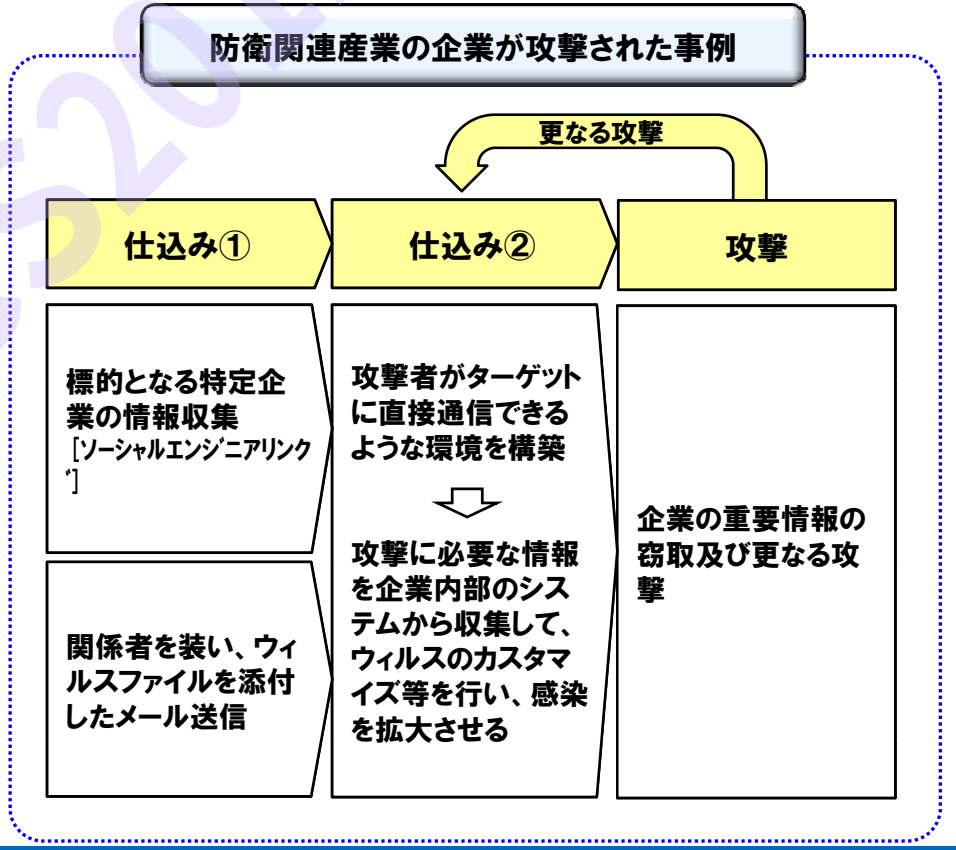
・最近増加している標的型サイバー攻撃は、既存の複数の手法を駆使して、標的企業の重要情報の窃取や破壊、停止活動を行う「攻撃」と、攻撃のために事前に行う「仕込み」を、複雑に組み合わせた巧妙な手口が特徴的である。特に「仕込み」の段階における手法が、従来より執拗で高度化していると言われている。脅威の深刻さが増す中で今後、「攻撃」だけでなく「仕込み」の段階まで、法執行機関との連携が求められる可能性もあると考えられる。

・日本の防衛関連産業の企業がサイバー攻撃を受けた事例において、この場合の標的型サイバー攻撃の手法を要素ごとに分析したものが以下の図である。



〔出所： @IT「標的型攻撃の攻撃例」(H23.11.14)〕

*NTT研究企画部門、㈱情報通信総合研究所調査



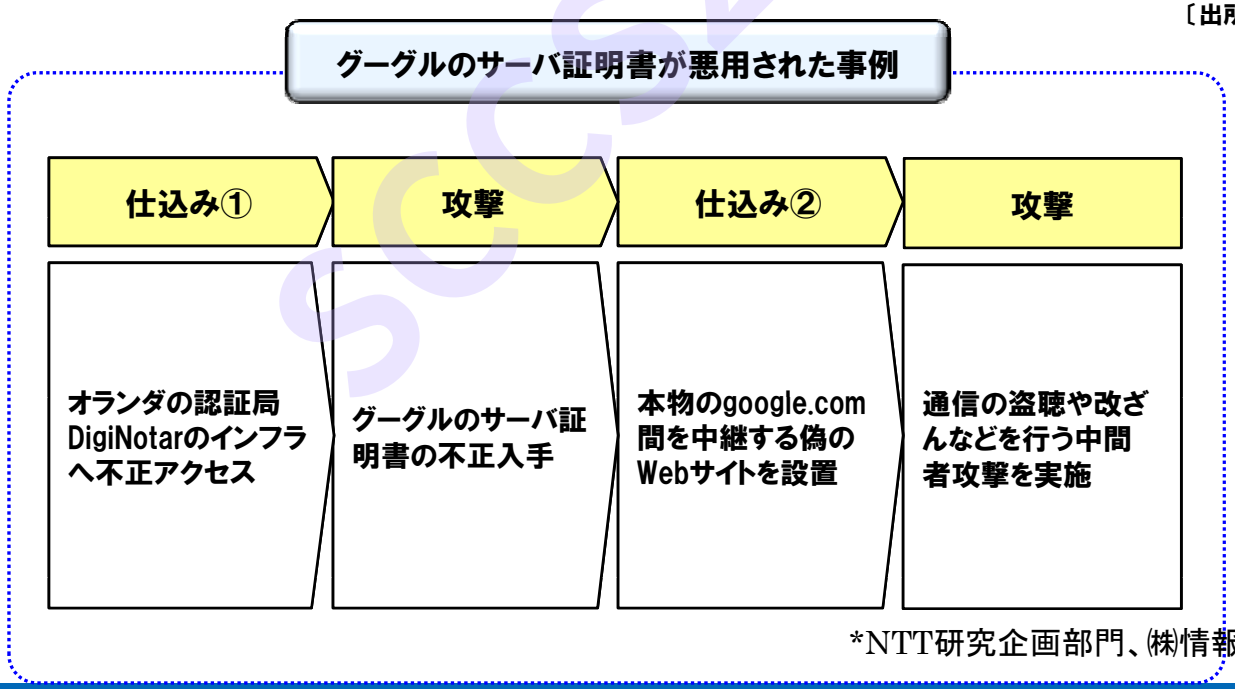
2-1-1. 法執行機関との連携の必要性(2/4)

・2011年8月にグーグルのサーバ証明書が不正発行され、悪用された事例が発生したが、この場合の標的型サイバー攻撃の手法を要素ごとに分析したものが以下の図である。

■ 米VASCOデータ・セキュリティ・インターナショナル(VASCO)は2011年8月30日(米国時間)、オランダ子会社の大手SSL認証局であるDigiNotarの認証システムが7月19日に侵入され、google.comを含む多数のドメインのSSL証明書が不正発行されたと発表した。SSL証明書はWebブラウザーで表示しているWebサイトが本物であることを証明する電子的な仕組みで、この証明書が不正発行されれば、偽のWebサイトが本物であると自称することが可能になる。すでに、不正発行されたgoogle.comのSSL証明書を悪用した攻撃も発生している。フィンランドのエフセキュアによると、 DigiNotarは数年前からハッキング攻撃を受けていたとのことである。

■ グーグルのセキュリティ・ブログも、8月29日(米国時間)に攻撃を受けていることを明らかにした。グーグルでは、同社のWebブラウザーであるChromeには不正証明書を検出する機能があるので、現状の利用のままでも攻撃からは守られているが、事件の調査が終わるまでDigiNotarが発行した証明書は無効にするとしている。

〔出所: PC Online(H23.9.6)〕



*NTT研究企画部門、㈱情報通信総合研究所調査

2-1-1. 法執行機関との連携の必要性(3/4)

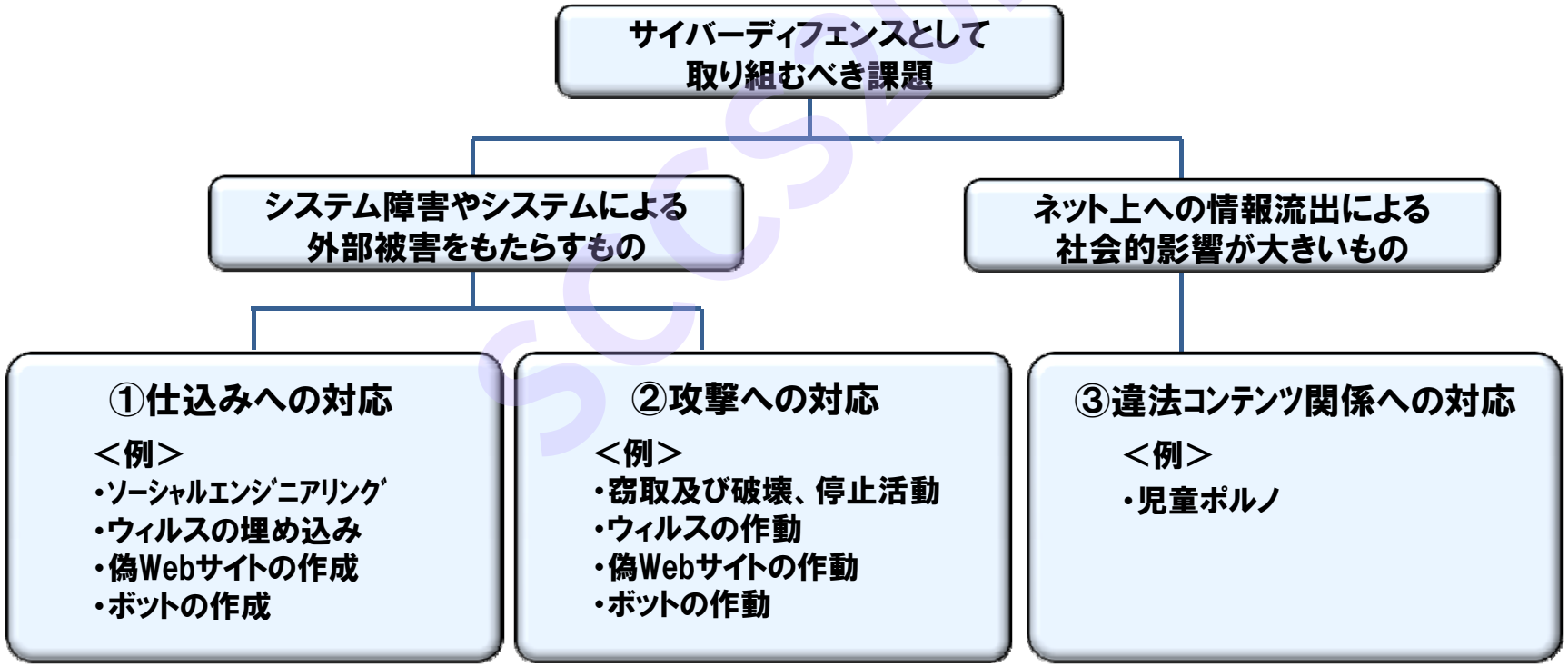
・サイバーディフェンスに関する法執行機関との連携において、取り組むべき課題として、次の3つの要素が考えられる。

①仕込み:標的に対して重要情報の窃取や破壊、停止活動を行うために、事前に行うものへの対応

②攻　撃:標的に対して直接的に行われる重要情報の窃取や破壊活動への対応

③違法コンテンツ関係:児童ポルノなどのように、ネット上への情報流出による社会的影響が大きく、ネットワークやサーバでの対処が求められる違法コンテンツへの対応

*NTT研究企画部門、㈱情報通信総合研究所調査



2-1-1. 法執行機関との連携の必要性(4/4)

*NTT研究企画部門、㈱情報通信総合研究所調査

・「仕込み」「攻撃」「違法コンテンツ関係」の3つの要素における法執行機関との連携を示したものが、次の図の［　　］で示す部分である。被害が顕在化している「攻撃」と異なり、「仕込み」の段階では被害が顕在化していない場合が多いために、法執行機関が捜査を行わないことが想定される。しかし、脅威が深刻さを増しているボットネット等については、今後「仕込み」の段階まで捜査機関と連携を行うか、という課題が浮き彫りになっている。

・ 法執行機関との連携において、海外での取り組みと差があり日本における対策が十分ではないのではないかと考えられるのは、サービス企業としてのボットネット等の遮断や違法コンテンツ関係の対応であると考えられる。

		サービス企業である場合		ターゲット企業である場合
		システム等を提供している場合	NWサービスを提供している場合	
仕込み	予防・検知	・ウィルスチェックやスパムフィルタ等の実装 ・捜査機関との情報共有	・ウィルスチェックやスパムフィルタ等の提供 ・捜査機関との情報共有	・入口対策(ウィルスチェック等)と出口対策 (外部通信の検知と遮断、ウィルスのシステム内拡散防止等)の実施 ・捜査機関との情報共有
	事後対応	・アクセスの遮断、ウィルス等の除去* ・捜査機関からの協力依頼 ⇒ユーザとの守秘等確認	・ボットネット等の遮断* 捜査機関との連携の可能性	・アクセスの遮断、ウィルス等の除去* ・捜査機関からの協力依頼 ⇒捜査協力
攻撃	予防・検知	・モニタリング ・捜査機関との情報共有	・(モニタリング) ・捜査機関との情報共有	・モニタリング ・捜査機関との情報共有
	事後対応	・アクセスの遮断、システムの分離 ・攻撃者情報や攻撃手法の調査、分析* ・捜査機関からの協力依頼 ⇒ユーザとの協議・守秘等確認 ・ユーザからの協力依頼 ⇒捜査機関へ協力要請検討	・自ら発見 ⇒静観か対応かの判断 ・捜査機関からの協力依頼 ⇒通信の秘密の問題 ・ユーザからの協力依頼 ⇒捜査機関へ協力要請検討	・アクセスの遮断、システムの分離 ・攻撃者情報や攻撃手法の調査、分析* ・捜査機関からの協力依頼 ⇒捜査協力 ・自らの発見 ⇒必要に応じて捜査機関へ協力要請
違法コンテンツ関係	予防・検知	・(モニタリング) ・捜査機関との情報共有	・(モニタリング) ・捜査機関との情報共有	・モニタリング ・捜査機関との情報共有
	事後対応	・遮断、除去	・遮断、除去 ・捜査機関へリスト作成等の協力要請	・遮断、除去

* 攻撃者を特定する法的手段をとれない場合が多い。

2-1-2. 海外における事例(1/2)

*NTT研究企画部門、㈱情報通信総合研究所調査

案件	被害内容	技術的対応	法的対応
米国・韓国への大規模DDos攻撃(2009.7)	乗っ取られた約5万台のPCから成るボットネットが米国政府のWebサイトを攻撃し、米国と韓国の民間企業も巻き添えとなった	標的となったWebサイトへソリューションを提供するAkamaiが、エッジサーバで攻撃をブロックしつつ、告訴に必要な情報を収集し、捜査機関へ提供	FBI等が詳細調査
大規模DDos攻撃(2011.3)	韓国国外を拠点とするボットネットにより、DDoS攻撃が約10日間継続的に仕掛けられ、サイト閲覧に支障が生じた	詳細は不明	韓国警察当局からICPOを通じ、各国の捜査機関に攻撃元の特定について協力要請
Botnet "Waledac"(2010.2)	米国を含む39ヵ国でスパムメールの送信やDDos攻撃などの活動を行い、感染したPCは7万~9万台と言われていた	①P2P遮断、②DNS/HTTP遮断、③上位2層遮断によりBotnet遮断	①ex parte TRO、②匿名訴訟による悪意のないドメイン登録者保護、 ③中国のレジストラに登録されたドメインの対処、④本来被告となるべき相手(ハーダー)への通知、⑤ex parte TRO(一方的な仮処分)への応答がないことから、ドメイン所有権の移管
Botnet "Bredolab"(2010.10)	2009年7月以降、全世界で3,000万台のPCを感染させ、感染した Web サイトを通じてトロイの木馬「Bredolab」を仕掛け、ボット化したPCを通じてさらに大量の別のウイルスを拡散させ、新たなボットネットを作り上げていた	オランダの国家犯罪対策局ハイテク犯罪チームが、ホスティングプロバイダ「LeaseWeb」社の協力を得て、悪用されていた同社配下の143台のサーバをインターネットから切断	当局が、同ボットネットの感染者に対し、次回のログイン時に感染を知らせる通知を送り、駆除方法をアドバイスする方法がとられた。 ※NFI(オランダ犯罪科学研究所)、Fox-IT(ネットセキュリティ会社)、GOVCERT.NL,(オランダのコンピュータ緊急対応チーム)等が協力
Botnet "Rustock"(2011.3)	100万台にものぼる感染PCを通じてWeb上にマルウェアを拡散させ、偽のMicrosoftくじや、偽の(危険性のある)処方薬を売り込むものなど、毎日数十億件ものスパムメールを送信	Waledacと同様のスキームでC&Cサーバ全てを遮断	商標不正使用に基づき、Botnet匿名オペレータを相手どり、被告人不詳訴訟を提起。ワシントン州西部地区連邦地方裁判所の決定により、複数の場所にあった C&C サーバを押収

2-1-2. 海外における事例(2/2)

*NTT研究企画部門、㈱情報通信総合研究所調査

案件	被害内容	技術的対応	法的対応
Botnet“CoreFlood” (2011.4)	Windows PCの脆弱性を突いて侵入し、個人情報や銀行関連の機密情報等を盗み出す。感染PCは200万台を超える	オランダ当局が「Bredolab」ボットネットを遮断する際に用いた手段と同様、	当局は犯罪者グループの13人を詐欺などに関与した疑いで民事提訴したほか、米国内に置かれている5台のC＆Cサーバ及びその通信に使われていた29のドメイン名を差し押さえた。また保全命令を取得した上で、C＆Cサーバを代用サーバに置き換え、感染したコンピュータにマルウエアを停止するコマンドを送信して攻撃拡大の阻止を図った。
Botnet “Kelihos” (2011.9)	マルウエアを感染させ、大量のスパムメッセージの送信、個人情報の収集、児童ポルノサイトの宣伝等の活動に悪用。感染PCは約4万1000台。1日あたり38億通のスパムメールを送信	Microsoftは当局の承認を得てKelihosとゾンビマシン(感染したコンピュータ)を切り離し、Kelihosを停止させた。	被告に訴訟の通知を送付し、詳細を追求するために調査を継続するとしている。 ※MSは、初めてボットネットに関わった被告を民事訴訟で名指しした。
Botnet “Operation Ghost Click” (2011.11)	トロイの木馬型不正プログラム(DNSチェンジャー)を利用し、400万以上の巨大ボットネットで、被害ユーザは全く異なるDNSサーバを使わされ、気付かないまま不正なWebサイトに誘導されていた。	C&Cサーバ閉鎖	FBI:NYとChicagoのDCに強制捜査を実施し、100台以上のC&Cサーバを閉鎖。様々な場所にあるPCや不正なDNSサーバを押収。 エストニア警察:世界規模で感染させた膨大な数のボットをコントロールし、莫大な金銭的利益を不正に得ていたエストニア人主犯グループ6人を逮捕。 トレンドマイクロ、ISC等業界関係者による協力

2-1-3. ボットネット遮断等における海外との比較(1/2)

Waledac Takedown Case Study

対応	USA
技術的アプローチ	・Waledacの制御用サーバと支配下のゾンビPC間の通信を遮断し、活動停止に追い込む。 ・具体的には、以下の3段階からなる計画によりBotnetを遮断 ①P2P遮断 ②DNS/HTTP遮断 ③上位2層遮断によりBotnet遮断 ＜登場人物＞ Microsoft、Trendmicro、iDEFNSE、University of Washington、Shadowserver Foundation、Vienna University of Technology、
法的アプローチ	上記を可能にするための法的措置として、以下を実施。 ①連邦裁判所に対する一方的な仮処分(ex parte TRO)を請求し、Waledacとの関係が疑われるドメインの通信を一時遮断する許可を得る ②ドメインが乗っ取られているケースへの対処として、匿名訴訟(John Doe Lawsuit)による悪意のないドメイン登録者を保護 ③中国のレジストラを通じて登録されたドメインへの対処として、連邦原則、米国憲法、中国法を確認し、ハーグ条約に基づき中国法務省に依頼 ④本来被告となるべき相手(ハーダー)への通知(訴状、電子メール、FAX、書簡、訴訟に関する書面のサイト掲載、メディア周知等) ⑤ex parte TRO(一方的な仮処分)に対する応答がないことから、処分の不履行(Default)を申請し、救済策としてドメイン所有権をマイクロソフトに移管 ＜登場人物＞ Microsoft、米バージニア州東地区連邦地方裁判所、中国法務省、ドメイン登録者、レジストラ、ハーダー、

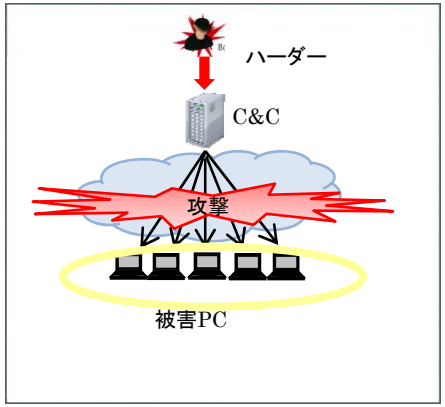
	米国	日本
匿名訴訟	John Doe Lawsuit	民事裁判では被告不詳は提起できない。
発信者情報開示	Discovery請求	・通信の秘密 ・プロバイダー責任法により、ISPが応じられない場合が多い。

*NTT研究企画部門、㈱情報通信総合研究所調査

2-1-3. ボットネット遮断等における海外との比較(2/2)

・海外では、業界や学術機関が法執行機関と連携し、巨大Botnetの遮断に成功した事例がある。

・具体的には、攻撃に使用されたコマンド&コントロールサーバ(C&C)やドメインを差押え、攻撃元とゾンビPCを切断し、ハーダーに対する責任を問う方法である。



Action	被害者	対応企業	法執行機関*	ゾンビPC	ハーダー
感染PCの確認とユーザへの通知	○	○	○		
攻撃元とゾンビPCの切断					
C&Cサーバの閉鎖のための差止		○	○ 請求		△
攻撃に利用されたドメインの差押		○	○ 請求		△
ハーダーへの責任追及		○ (民事責任)	○ (刑事訴追		△

※法執行機関:裁判所も含まれる。

・日本で同様の手法をとる場合、感染PCのIPアドレスから上位層のノードを辿り、ハーダーが操作するC&C等の発信者情報開示をISPに求め、ハーダーを特定していくこと等が必要となる。その際の課題は以下のとおりである。

前提条件	民間企業が実施する場合	公権力が執行する場合
・日本国憲法第21条2項は、検閲の禁止と通信の秘密を保障する規定であり、政府など公権力に対する義務として課せられ、表現の自由を保障するため一つの施策として憲法上確保されている。 ・また、ISPは、電気通信事業法第4条第1項で、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない」とされている。	・ISPに対し、情報開示を任意で求めることが出来る可能性はあるが、通信の秘密に抵触するため、ISPが応じられない場合が多い。 ・プロバイダー責任法による発信者情報の開示を請求できるのは、特定電気通信による情報の流通によって自己の権利を侵害された者のみであり、侵害されているとする権利及び権利侵害の態様を示す必要がある。	・公権力が情報開示を求める場合は、「通信の秘密」があるため、犯罪事実が認められ、かつ、法定による手続きによらなければならない。 ・捜査対象となる場合、業務妨害罪や2011年に新設された「不正指令電磁的記録に関する罪(コンピュータ・ウイルスの作成・供用等の罪)」により処罰の対象となる。

*NTT研究企画部門、㈱情報通信総合研究所調査

2-1-4. 違法コンテンツ関係への対応における海外との比較(1/2)

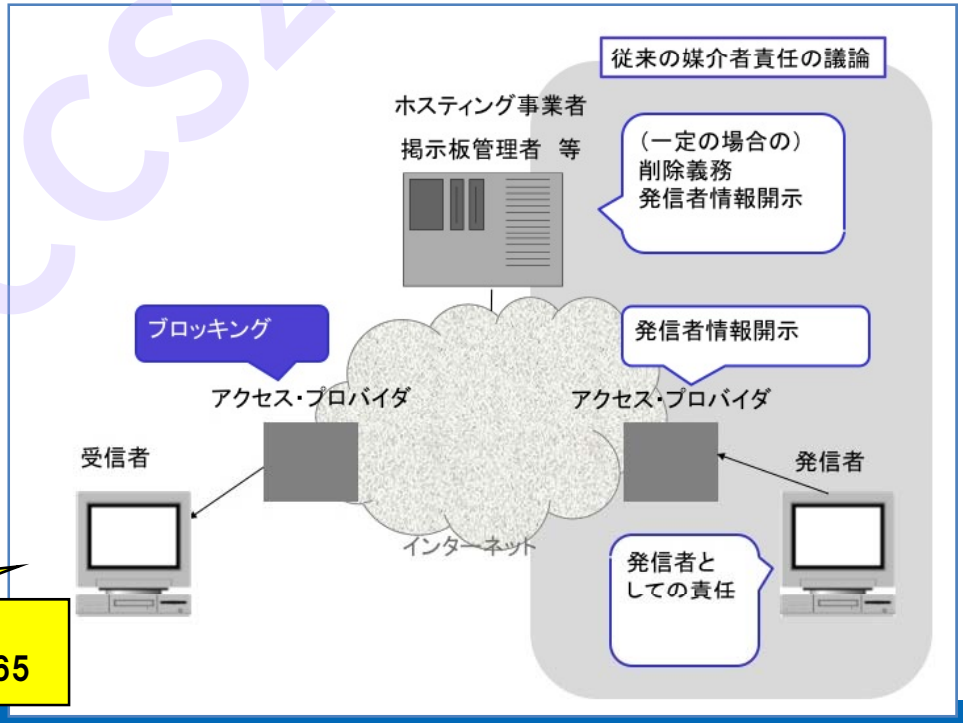
日本における対応

*NTT研究企画部門、㈱情報通信総合研究所調査

・2011年4月に、インターネット上における児童ポルノの流通防止に向けて、大手ISPなどの自主的な取り組みとしてブロッキングが導入されたところであるが、国内発も含めてブロッキングを徹底すべきだという意見もある。一方で、ブロッキングという手段について、検閲につながる危険性もはらんでいるとして、慎重な運用を呼び掛ける声や、ブロッキング導入前は、通信の秘密や表現の自由の観点からマスコミなどの関心も高かったが、関心が薄れてきたのではないかと指摘する声もある。

・違法コンテンツ関係への対応として、ブロッキング対象の安易な増加を許せば、他の著作権侵害コンテンツなどへの適用に発展する危険性を懸念する声も聞かれる。今後、違法コンテンツの定義の明確化や、電気通信事業者等が自主的にブロッキングを実施する際には、その対象や手法の明確性と透明性が確保されることが期待される。

ブロッキングとは、インターネットへの接続を提供するISPなどが、利用者がアクセスしようとしたサイトが児童ポルノサイトである場合に、そのアクセスを強制的に遮断することである。
児童ポルノサイトをあらかじめリストアップしておき、利用者のアクセス先と機械的に照合して、特定サイトへのアクセスを防止する。
従来のISPの対応が、主に情報発信者側のISPによって行われていたのに対して、ブロッキングでは情報受信者のアクセスを、**本人の同意を得ることなく**制限することになる。



＜出典＞　小向太郎
「情報法入門【第2版】デジタル・ネットワークの法律」P165

2-1-4. 違法コンテンツ関係への対応における海外との比較(2/2)

海外との比較

*NTT研究企画部門、㈱情報通信総合研究所調査

・イギリスやノルウェーでは、児童ポルノのブロッキングを2004年から実施している。各国における児童ポルノを規制する法律等と、日本における法制度の違いは、次のとおりである。

		イギリス	ノルウェー	日本
ブロッキング開始時期		2004年 [各ISPが自主的に実施(警察からの強い要請があったと言われている)]	2004年 [警察機関と各ISPが契約書を交わすことで自主的に実施]	2011年 [各ISP等が自主的に実施]
ブロッキングに関する法律等		なし	なし	なし
児童ポルノを禁止する法律関係	児童ポルノの定義	18歳未満。18歳未満のように見える人物も含む	18歳未満、及び18歳未満に見える人物	18歳未満
	対象コンテンツ	児童のみだらな写真・映像・疑似写真、写実的に描かれた絵	写真・映像・絵(実写性があるもの)	実在の児童
	禁止行為	製造、領布、展示、出版、 単純所持等	製造、取得、輸入、所持、 領布・販売、単純所持等	製造、提供・領布、運搬、 輸入・輸出、上映・公然陳列 (*単純所持は禁止されていない)
	違反した場合	10年以下の拘禁刑、又は罰金刑、 もしくはそれらの併科	罰金、もしくは3年以下の懲役	3年以下の懲役、又は300万円以下の罰金
	例外規定	単純所持において、本人又は代理人があらかじめ要求しないにもかかわらず送付され、かつ合理的な期間内でその保有をやめたことなどが証明できれば処罰の対象外	芸術的、科学的等、正当に認められる性的描写	なし

2-2. 主な法的課題

・情報セキュリティの高度化により、情報システムを取り巻く脅威の深刻さが増す中で、サイバーセキュリティの領域における法制度の果たすべき役割が急速に増大している。そのため、我が国において法整備も含めた情報セキュリティ政策の検討がなされているが、法制度の側面から見た検討は、必ずしも十分とは言えない部分がある。

・現時点では、我が国において情報セキュリティ全体を包括的に保護するための法令は制定されていない。そこで、現時点におけるサイバーセキュリティの領域における主な法的課題を挙げたものが次の図である。

	実体法	手続法
民事	・情報の不正な取得等については、財産的被害を主張・立証することが必ずしも容易ではない ・情報に関わる損害については、差止請求等で損害を回復することが難しい ・製造物責任法のように、動産に限定し、ソフトウェアプログラムを対象外としているものがある	・電気通信事業者等は「通信の秘密」を保護することが厳格に定められているため、電気通信事業者等が保有する情報について、法的に請求することが難しい場合がある ・責任の追及には、相手方の氏名・住所等の情報が必要になる　（民事訴訟規則第二条＊） ・情報の流通によって自己の権利が侵害された者が、プロバイダ等に発信者情報の開示を請求した場合に、その開示に時間を要する
刑事	・情報の不正な取得一般は、刑事罰の対象となっていないので、情報の不正取得が処罰の対象とならない場合がある ・国内犯の処罰を原則としているため、国外犯処罰規定の対象となっていないものがある 例：電子計算機損壊等業務妨害罪（刑法234条の2）	・国際的な行為に対して、捜査共助・犯罪人身柄引き渡し等の捜査機関の間の協力が、有効に機能しない場合がある ・国により規定が異なり、裁判管轄や適応法が明確でない場合がある

＊民事訴訟規則第二条
訴状、準備書面その他の当事者又は代理人が裁判所に提出すべき書面には、次に掲げる事項を記載し、当事者又は代理人が記名押印するものとする。
一　当事者の氏名又は名称及び住所並びに代理人の氏名及び住所

Thank you !

NTT