総務省
MIC Ministry of Internal Affairs and Communications

総務省の情報セキュリティ政策

情報流通行政局 情報セキュリティ対策室長
山碕　良志

はじめに

- ☑ はじめに
- ☐ サイバー攻撃の動向
- ☐ 情報セキュリティ政策の動向
- ☐ 終わりに

日本経済再生に向けた緊急経済対策（抜粋）（平成25年1月11日閣議決定）

前文 日本経済再生に向けた取組の第１弾

第1章 景気の現状

第2章 日本経済再生に向けての考え方

第3章 具体的施策

Ⅱ．成長による富の創出

１．民間投資の喚起による成長力強化

（２）研究開発、イノベーション推進

①研究開発プロジェクトの推進

・イノベーションを創出する情報通信技術の利活用推進・強固な基盤整備（総務省）

３．日本企業の海外展開支援等

②クール・ジャパンの推進、訪日外国人旅行者の増大に向けた取組等

・クールジャパン・コンテンツの海外展開等の促進（経済産業省、総務省）

Ⅲ．暮らしの安心・地域活性化

１．暮らしの安心の確保

（４）安心の確保

国民の暮らしと命を守るため緊急に必要な不測の事態等に対処する能力を強化し安心を確保する。

・警察機動力及び装備資機材の整備（警察庁）

・変化する安全保障環境への適応（防衛省）

・領海警備体制の強化等（国土交通省、農林水産省）

・サイバーセキュリティ対策の強化（内閣官房、警察庁、総務省、経済産業省）

第4章 本対策の規模と効果

ICTは時代を支える土台

○ICTは民主主義の生命線：「アラブの春」（ソーシャルメディア）、ネット署名
サイバー空間の在り方の議論

○ICTは経済成長の原動力：提供主体と利用主体
新サービス（スマホ、ビッグデータ）

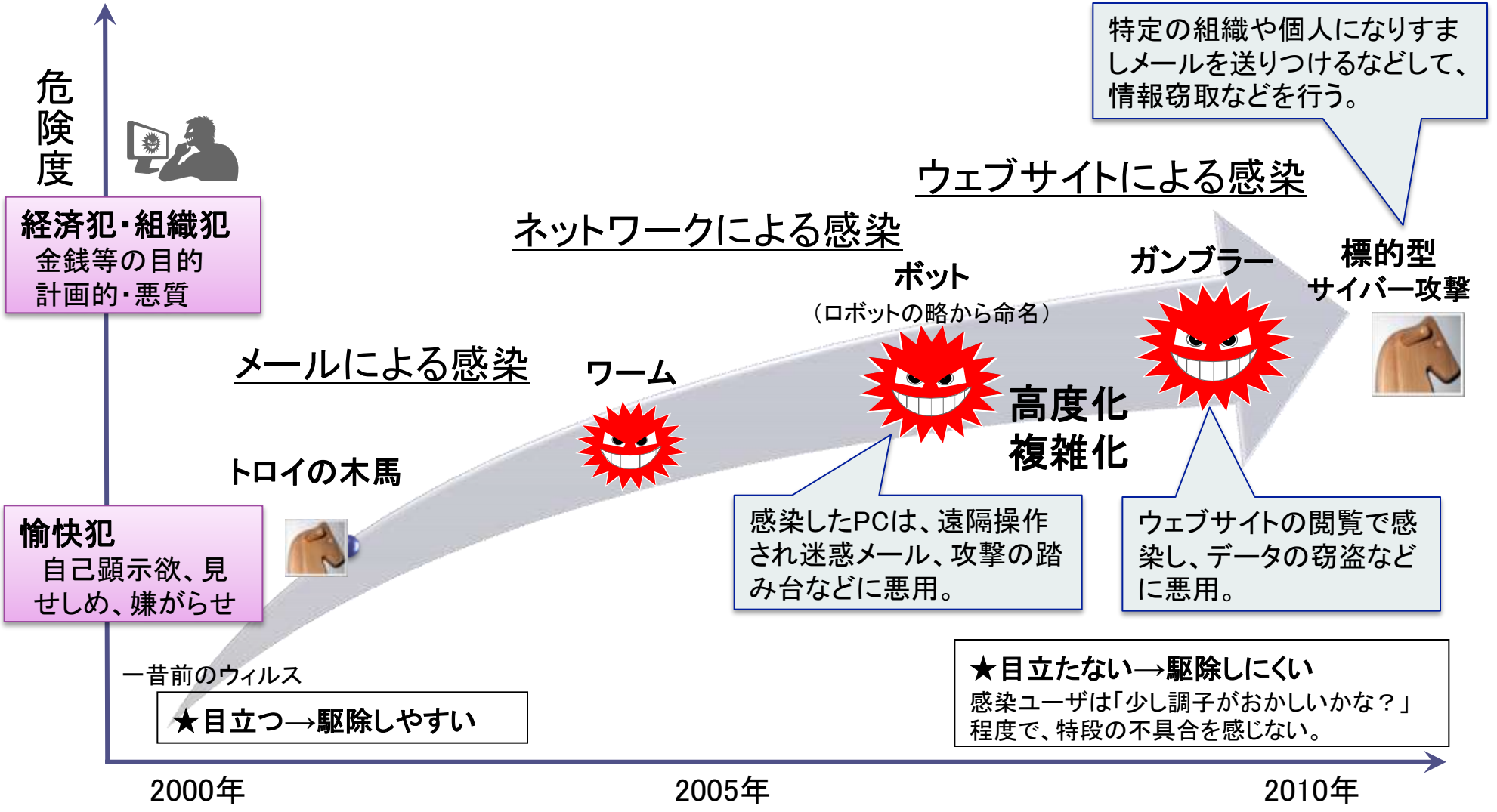
○ICTは国民生活の必需品：時間と空間の制約を克服する手段

サイバー攻撃の動向

- ☐ はじめに
- ☑ サイバー攻撃の動向
- ☐ 情報セキュリティ政策の動向
- ☐ 終わりに

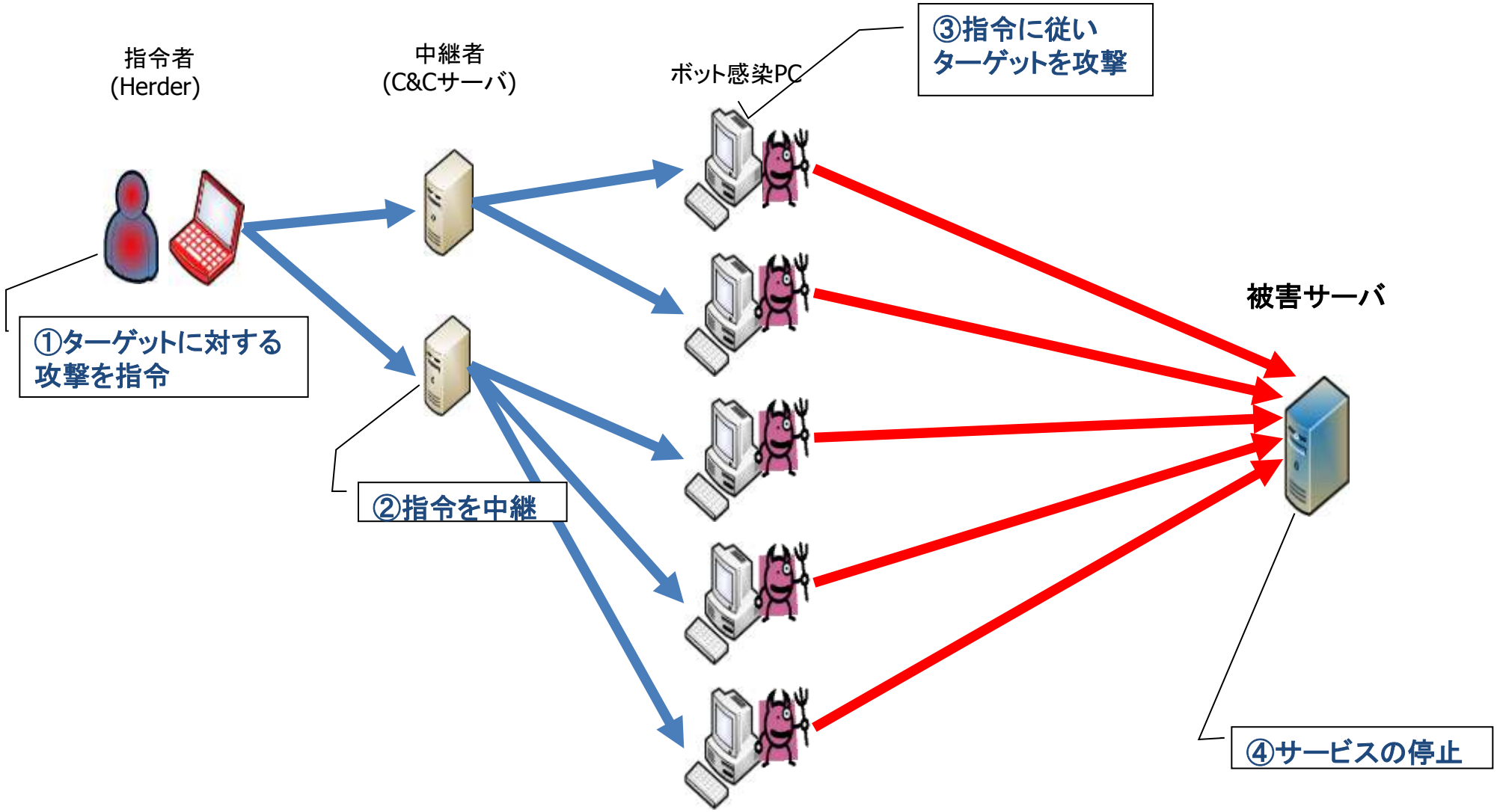
脅威の変遷

ICTは社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、情報セキュリティ上の脅威の多様化・悪質化により、その被害が深刻化している。



DDoS攻撃とは

DDoS：Distributed Denial of Service（分散型サービス妨害攻撃）



出典：内閣官房情報セキュリティセンター

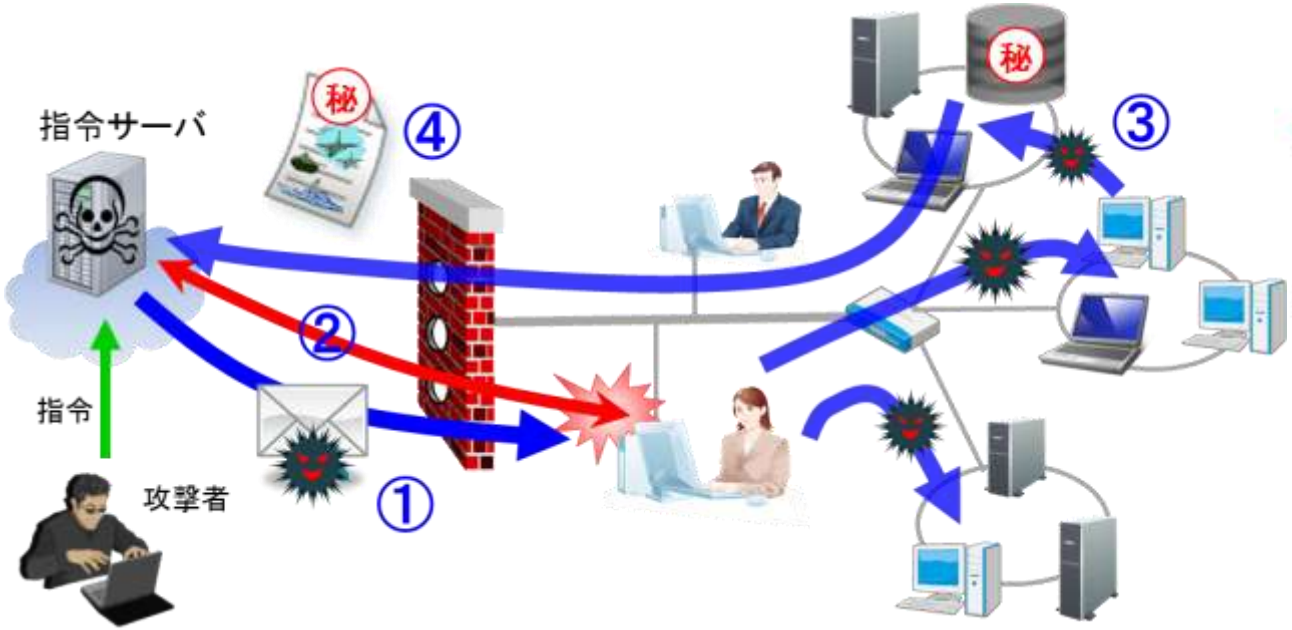
標的型攻撃とは

標的型攻撃とは、特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃。攻撃が巧妙化・複合化しており、検出・防御が困難。

標的型攻撃の代表的な手順

攻撃の標的となる組織について、事前にLAN環境に関する調査、SNSや社会的な手段により、攻撃の標的となる組織に関する調査を行った上で、次のような段階を踏んで攻撃を行う。

① 標的型メールにより、PCをマルウェアに感染させる。
② 当該PCと、指令サーバとを通信させる。
③ ネットワークを内偵しつつ、組織内でマルウェアの感染を拡大させる。
④ 最終目標への攻撃を遂行し、秘密情報等を手に入れる。



現状の課題

標的型攻撃は、未知のぜい弱性（ゼロデイ）を突くマルウェアを利用して攻撃が行われることもあるため、従来型の情報セキュリティ対策では検出・防御ができない。また、その被害や攻撃されていること自体に気づくのが事後、又は困難である場合もある。

情報セキュリティ上の事案

分散型サービス妨害(DDoS)攻撃

2009年7月・・・韓国、米国の金融機関や政府機関等のシステムが攻撃を受け、数日間に亘りウェブサイトへのアクセス不能な状態に陥ったことに加え、推定で27～41億円の経済的な被害が発生。

2010年9月・・・中国のハッカー組織が、日本政府機関のウェブサイトを攻撃すると表明した後、防衛省及び警察庁等のウェブサイトが攻撃を受け、3日間に亘りアクセスしづらい状態が継続。

2012年6月・・・国際ハッカー集団アノニマスが、ネット上の違法ダウンロード行為に刑事罰を導入する改正著作権法の成立に反発し、日本政府等に攻撃予告。**財務省、国交省**のウェブサイトが改ざんされたほか、最高裁、自民党、民主党のウェブサイトが一時アクセスしづらい状態が発生。

2012年9月・・・中国からのサイバー攻撃により、**最高裁判所、文化庁**等のウェブサイトが改ざん。

クラウドサービスの障害事例

2012年6月・・・ファーストサーバ(ヤフー子会社のレンタルサーバ事業者)が保有する共有サーバ・クラウドサーバにおいて、保守作業で使用した更新プログラムの不備により、約5000の企業・団体顧客のメールデータ等が消失

不正アクセス

2011年4月・・・**ソニーの子会社**(ソニー・コンピュータエンタテイメント及び米国法人)のシステムに対する不正アクセスにより、個人情報(氏名・住所、電子メールアドレス、クレジットカード番号等)約1億人分が窃取。

2012年9月・・・ウイルスに感染したPCが第三者により**遠隔操作**され、掲示板に違法な書込みが行われたことから、当該PCの所有者が誤認逮捕。

2012年10月・・ウイルス感染により、ネットバンキングにログインした利用者のPCの画面に偽画面が表示され、ID・パスワードが窃取。これにより、数百万円の不正送金が発生。

標的型サイバー攻撃

2010年9月・・・イランの原子力発電所の制御システムにおいて、USB経由でスタックスネットと呼ばれるマルウェア感染が確認されたとの報道。(我が国のパソコンでも、スタックスネット感染パソコンが発見された旨の報道。)

2011年8月・・・**三菱重工業**の社内サーバやパソコン約80台が情報収集型のウイルスに感染し、コンピュータのシステム情報が流出したおそれ。

2011年10～11月・・・**衆参両院**のサーバやパソコンが情報収集型のウイルスに感染していたことが報道、ID・パスワードが流出したおそれ。

2011年11月・・**総務省**のパソコン23台が情報収集型のウイルスに感染していたことが判明、個人情報、業務上の情報が流出したおそれ。

2013年1月・・・**農林水産省**のPCが遠隔操作型のウイルスに感染し、TPPに関する機密文書が窃取されたおそれがあることが報道。

情報セキュリティこの10年

○　利用者の拡大：ICT（情報通信技術）の浸透

ケータイ・PC⇒スマホ・ソーシャルメディア（フェイスブック・ツイッター）

○　利用国の拡大：先進国から途上国へ（「ネットは世界につながっている」が具現化）

○　サイバー攻撃：手段⇒高度化・複雑化（標的型攻撃）

目的⇒愉快犯から経済犯・組織犯へ悪質化

○　安全保障分野：「サイバー空間は第五の戦場」（米大統領選、防衛省動向）

情報セキュリティ政策の動向

- ☐ はじめに
- ☐ サイバー攻撃の動向
- ☑ 情報セキュリティ政策の動向
- ☐ 終わりに

政府における情報セキュリティ政策の推進体制

内閣官房を中心に関係省庁も含めた横断的な体制を整備

高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）

本部長　内閣総理大臣
副本部長　情報通信技術（IT）政策担当大臣
内閣官房長官
総務大臣
経済産業大臣
本部員　本部長及び副本部長以外のすべての国務大臣
民間有識者（10人）

（事務局）
内閣官房IT担当室
室長（政府CIO）

情報セキュリティ政策会議　（平成17年5月30日　IT戦略本部長決定により設置）

議長　内閣官房長官
議長代理　情報通信技術（ＩＴ）政策担当大臣
構成員　国家公安委員会委員長
総務大臣
経済産業大臣
防衛大臣

閣僚が参画

遠藤　信博	日本電気株式会社代表取役執行役員社長
小野寺　正	KDDI株式会社代表取締役会長
土屋　大洋	慶應義塾大学大学院教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	首都大学東京法科大学院教授
村井　純	慶應義塾大学教授

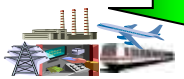
（事務局）
内閣官房情報セキュリティセンター（NISC）
センター長（官房副長官補（安危））
副センター長（内閣審議官）2名
内閣参事官6名

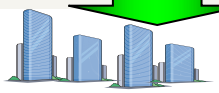
情報セキュリティ緊急支援チーム（CYMAT）

協力

その他の関係省庁
重要インフラ所管省庁
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス）
国土交通省（鉄道、航空、物流）
その他
文部科学省（セキュリティ教育）　等

協力4省庁
警察庁（サイバー犯罪の取締り）
総務省（通信・ネットワーク政策）
経済産業省（情報政策）
防衛省（国の安全保障）


重要インフラ事業者　等


政府機関（各府省庁）


企業


個人

総務省の情報セキュリティ政策の概要

1. 安心なネットワーク環境の整備

①事業者との情報共有

・テレコム・アイザック推進会議等の所管事業者や(独)情報通信研究機構と情報共有し、被害の拡大防止等に寄与。

②サイバー攻撃対処に向けた官民連携の強化

・経済産業省及び関連4団体と、各機関が保有する情報を高度解析し、サイバー攻撃の実態等を把握(サイバー攻撃解析協議会)。

③ＩＣＴ環境の変化に応じた情報セキュリティ対応方策の推進事業（平成25～29年度）

・国民のウイルス感染被害予防に資する研究開発・実証実験等を実施。

2. 技術開発の推進

①サイバー攻撃解析・防御モデル実践演習（平成24～29年度）

・サイバー攻撃への防御モデルの検討を行うとともに、官民参加型の実践的な防御演習を実施。

②国際連携によるサイバー攻撃予知・即応技術の研究開発（平成23～27年度）

・諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術の研究開発を実施。

3. 利用者意識の向上

・「国民のための情報セキュリティサイト」による情報提供、セミナー開催による周知啓発活動。

・スマートフォン、無線LAN等の情報セキュリティに関する様々なメディアを活用した周知啓発活動。

4. 国際連携の推進

・米国、ASEAN等の海外諸国と情報セキュリティ対策に関する取組を共有し、国際的な連携を推進。

5. プライバシーの保護

・プライバシー保護等に配慮したパーソナルデータ(個人に関する情報)のネットワーク上での利用・流通の促進に向けた方策について検討するため、「パーソナルデータの利用・流通に関する研究会」を開催。

スマートフォンの情報セキュリティ対策について

スマートフォン・クラウドセキュリティ研究会

【問題意識】

✓ 近年、スマートフォンの急速な普及が進む一方、スマートフォンを対象としたマルウェアの出現・増加が報告されるなど、情報セキュリティ上の脅威が高まっている。

【検討の経緯】

✓ 平成23年10月、有識者、携帯電話事業者、端末製造事業者等を構成員として設置

✓ 座長： 山口　英　奈良先端科学技術大学院大学教授

✓ 平成23年12月に中間報告、平成24年6月に最終報告をとりまとめ。

最終報告の概要

事業者・政府等における対策及び利用者への普及啓発方策を提言

事業者等における対策

アプリケーション

○マルウェアを含むアプリケーションの作成・流通・インストール防止対策
○アプリケーション提供サイトの運営方針開示等、利用者が自衛できる環境の構築

通信路

○安全性の高い暗号化・認証方式等の無線LANの情報セキュリティ対策

OS

○事業者間での情報共有など、OSのぜい弱性対策

データ

○端末の紛失・盗難に備えた対策

利用者への普及啓発

○政府、事業者等が利用者啓発を推進

スマートフォン情報セキュリティ３か条
１．ＯＳ（基本ソフト）を更新
２．ウイルス対策ソフトの利用を確認
３．アプリケーションの入手に注意

政府における対策

○事業者等と連携しアプリケーションの性質の可視化の枠組みを整備
○利用者保護のための技術の研究開発
○利用者への総合的な普及啓発の実施
○国際連携の推進

＊今後、事業者・政府等の取組を定期的にフォローアップし公表

無線LANの情報セキュリティ ①

○ 一般利用者が安心して無線LANを利用するための方策や、無線LANの情報セキュリティ上の脅威についてとりまとめた手引書「一般利用者が安心して無線LANを利用するために」を平成24年11月2日に策定。

○ 企業等が無線LANを導入・運用する際の手引書は「企業等が安心して無線LANを導入・運用するために」は、平成25年1月30日に策定。

「一般利用者が安心して無線LANを利用するために」の概要

Ⅰ. 無線ＬＡＮ情報セキュリティ３つの約束

～パソコンやスマートフォンの一般利用者が最低限取るべき対策～

約束1. 無線LANを利用するときは、大事な情報はSSL※でやりとり

約束2. 無線LANを公共の場で利用するときは、ファイル共有機能を解除

約束3. 自分でアクセスポイントを設置する場合には、適切な暗号化方式を設定

約束1. SSLの利用例

Ⅱ . 一般利用者が安心・安全に利用するためのガイドライン

利用者のリテラシーや重要度に応じた対策を段階的に、「Ⅰ. 無線ＬＡＮ情報セキュリティ３つの約束」を含め総合的に提示。

Ⅲ . 無線LANを適切に利用しないと生じる危険性の具体例と解決策

危険性について具体的な事例を交え解説し、それぞれの事例における問題点の解決法を解説。

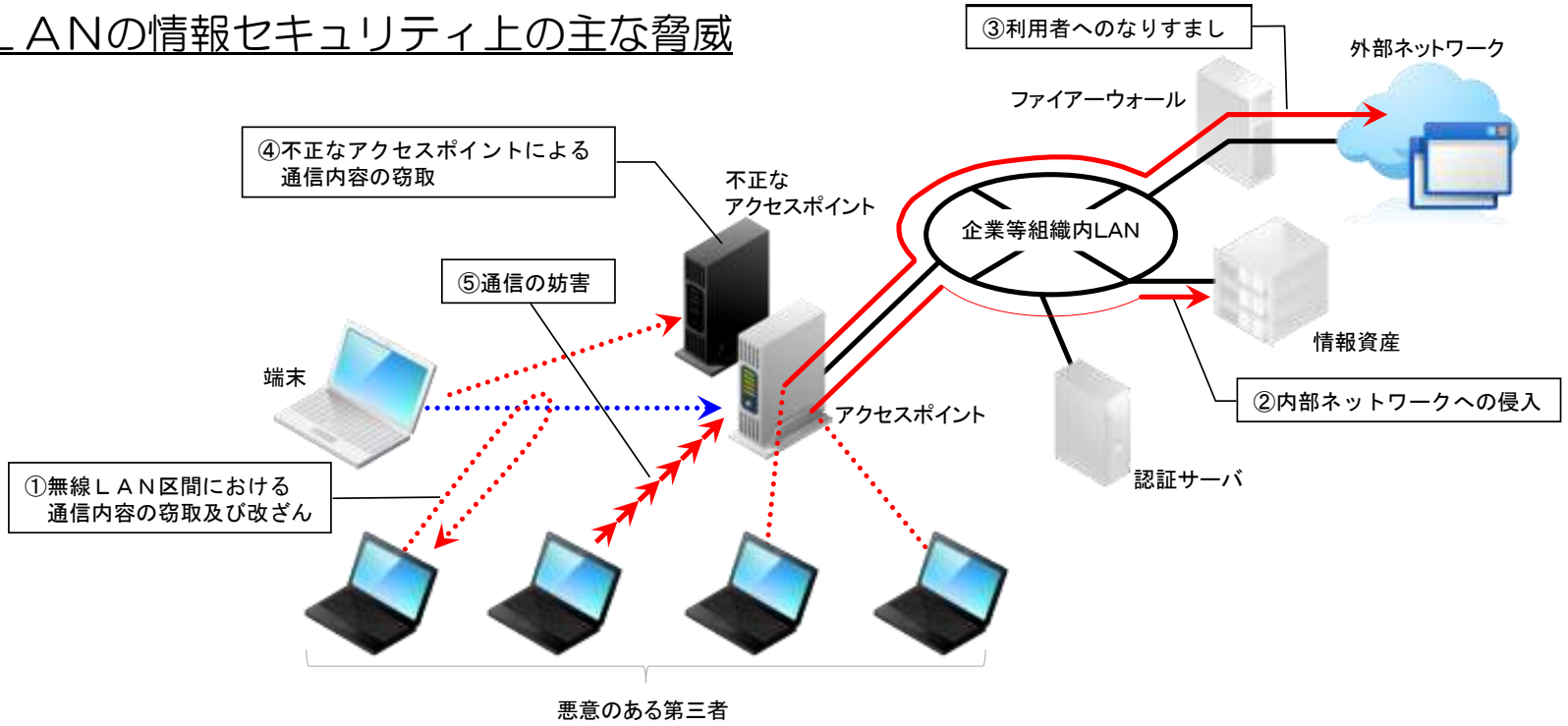
※ SSL（Secure Socket Layer）とは、信頼できるウェブサイトやサーバとの間で、データを暗号化して送受信する方法。SSLが使われていることは、URLが「https」からはじまっていることや、パソコンやスマートフォンのブラウザに「鍵マーク」が表示されることで確認。

無線LANの情報セキュリティ ②

「企業等が安心して無線LANを導入・運用するために」の概要

○　無線ＬＡＮにおいて想定される情報セキュリティ上の脅威、及び企業等の組織のＬＡＮ管理者が取るべき情報セキュリティ対策を提示。また、無線ＬＡＮの導入・運用の各段階において実施すべき事項についても提示。

無線ＬＡＮの情報セキュリティ上の主な脅威



想定される脅威	脅威への主な情報セキュリティ対策	
①無線ＬＡＮ区間における通信内容の窃取及び改ざん	◎	ＷＰＡ／ＷＰＡ２（ＣＣＭＰ）の採用と適切な設定
	◎	アクセスポイントの管理者パスワードの適切な設定
②内部ネットワークへの侵入	◎	ＷＰＡ／ＷＰＡ２－ＥＡＰの採用と適切な設定
③利用者へのなりすまし	◎	アクセスポイントの管理者パスワードの適切な設定
④不正なアクセスポイントの設置による通信内容の窃取	◎	ＷＰＡ／ＷＰＡ２－ＥＡＰの採用及び適切な設定
⑤通信の妨害	○	ログの収集・保存

※WPA（Wi-Fi Protected Access）及びWPA2は、端末とアクセスポイントとの接続に関する認証方式（EAP等）及び通信内容の暗号化方式（CCMP等）を包含した規格の名称

ICT環境の変化に応じた情報セキュリティ対応方策の推進事業①（国民のウイルス感染被害予防方策）

施策概要

○ 昨今、国会、政府機関、民間企業等がネットワークを通じたサイバー攻撃を受け、情報漏えい等の被害が発生する事態が頻発している。ICT環境が変化する中、サイバー攻撃が標的型攻撃※をはじめ巧妙化・複合化するなど、我が国における情報セキュリティ対策基盤の強化が喫緊の課題となっている。

※ 標的型攻撃：特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃

○ 個人利用者においても、ウイルス感染やID・パスワードの漏えいなどの実被害が発生していることから、インターネット利用に関する安全の確保を図るため、攻撃の解析・検知の高度化、ウイルス感染被害予防に資する研究開発・実証実験等を民間企業等への委託により実施する。

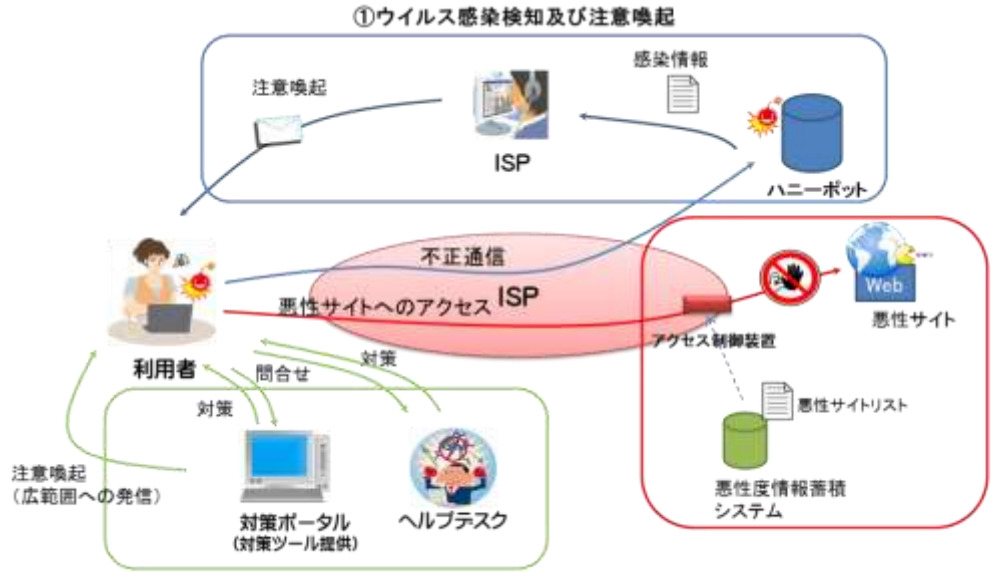
【国民のウイルス感染被害予防方策例】

①ウイルス感染した個人利用者のPCによる不正通信を自動的に検知。利用者にインターネットサービスプロバイダ（ISP）等を通じて注意喚起情報を送付し、駆除等の対策を促す。

②ウイルス感染元等、ウェブサイトの悪性度の情報を蓄積したシステムを構築し、個人利用者がアクセスしようとした場合に、当該システムにより検知し、注意喚起等を行う。

○ 実施期間：平成25～29年度
○ 所 要 額：平成25年度当初予算 10億円

国民のウイルス感染被害予防方策例



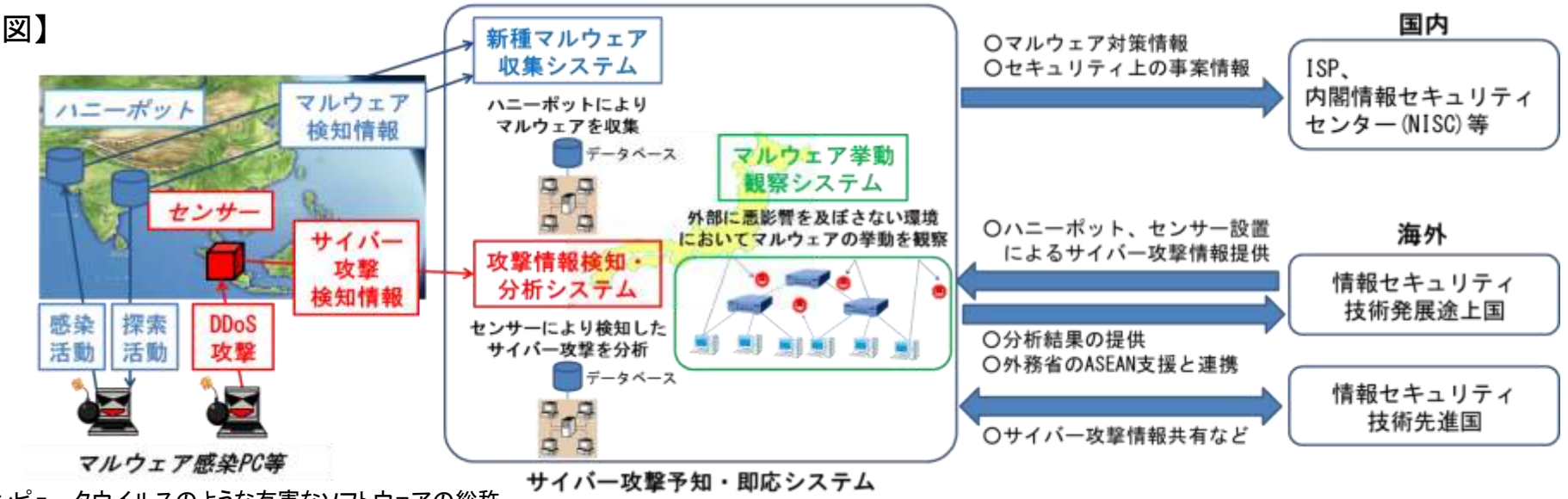
国際連携によるサイバー攻撃予知・即応技術の研究開発

プロジェクト略称：PRACTICE：Proactive Response Against Cyber-attacks Through International Collaborative Exchange

○目的：
近年、被害が拡大しているサイバー攻撃（分散型サービス妨害攻撃、マルウェアの感染活動等）に対処し、我が国におけるサイバー攻撃のリスクを軽減。

○概要：
国内外のインターネットサービスプロバイダ（ISP）、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術について、その研究開発及び実証実験を実施。

【イメージ図】



○マルウェア：コンピュータウイルスのような有害なソフトウェアの総称。
○DDoS（Distributed Denial of Service）攻撃：分散型サービス妨害攻撃。多数のPCから一斉に大量のデータを特定宛先に送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃。
○ハニーポット：故意に外部からの進入を容易にした囮のネットワーク機器。マルウェアの感染活動等の検知を目的にネットワーク上に設置。

○ 実施期間：平成23～27年度
○ 予 算 額：平成23年度当初予算　6.3 億円
　　平成23年度補正予算（第４号）　5.6 億円
○ 所 要 額：平成25年度当初予算　5.8 億円

国際連携の状況

○ 平成23年11月、「第4回日・ASEAN情報セキュリティ政策会議」において、ASEAN各国に連携を呼びかけ。
○ 平成24年3月には、サイバー攻撃の予知のための研究開発の協力について、**米国と合意**。6月に研究者中心の日米会合を実施。
○ 平成24年4月に**モルディブ**と、平成24年5月に**インドネシア**との間でデータ共有システムを稼働させ、実際に日本との情報共有を開始。
○ 現在、タイ、マレーシア、シンガポール等と連携に向けて協議中。

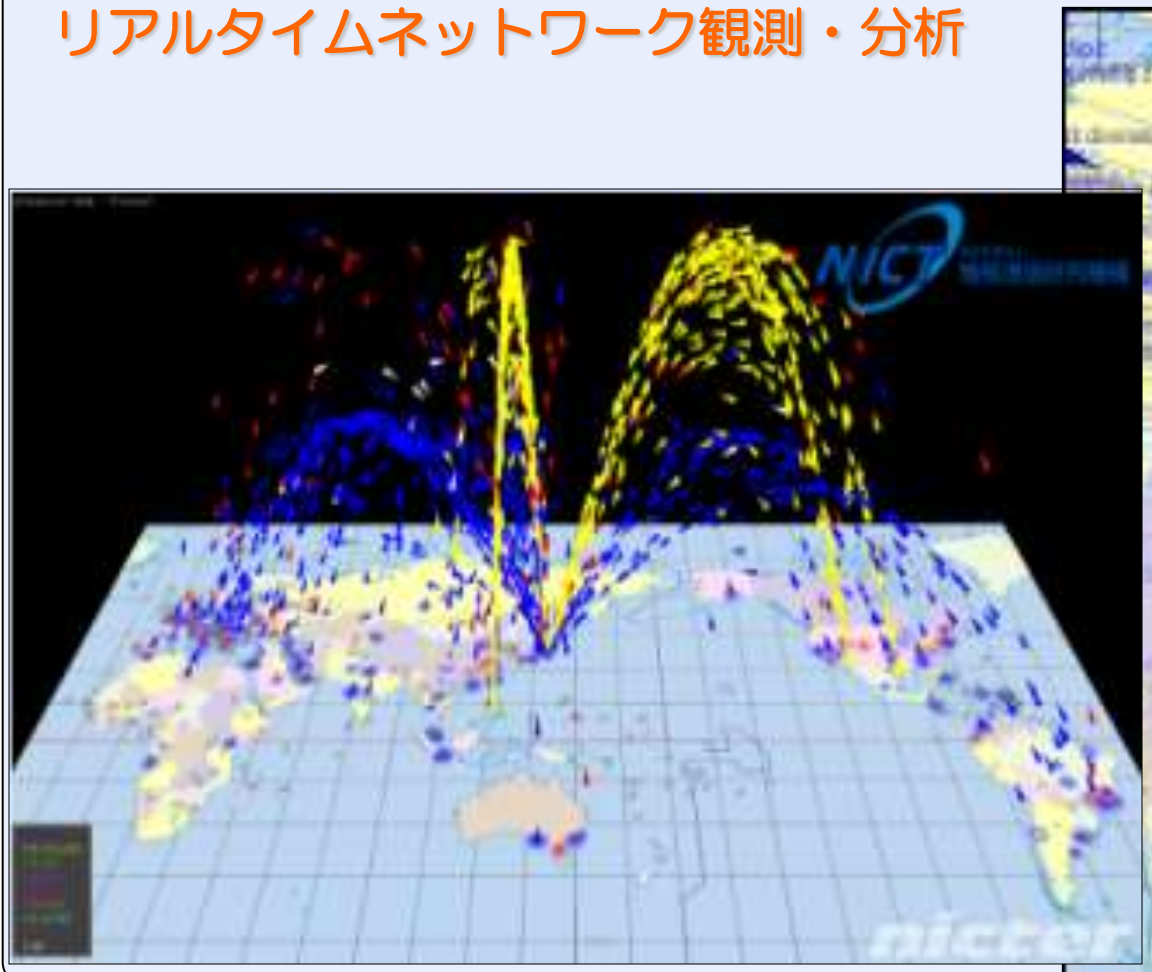
NICTによるサイバー攻撃観測（nicter）

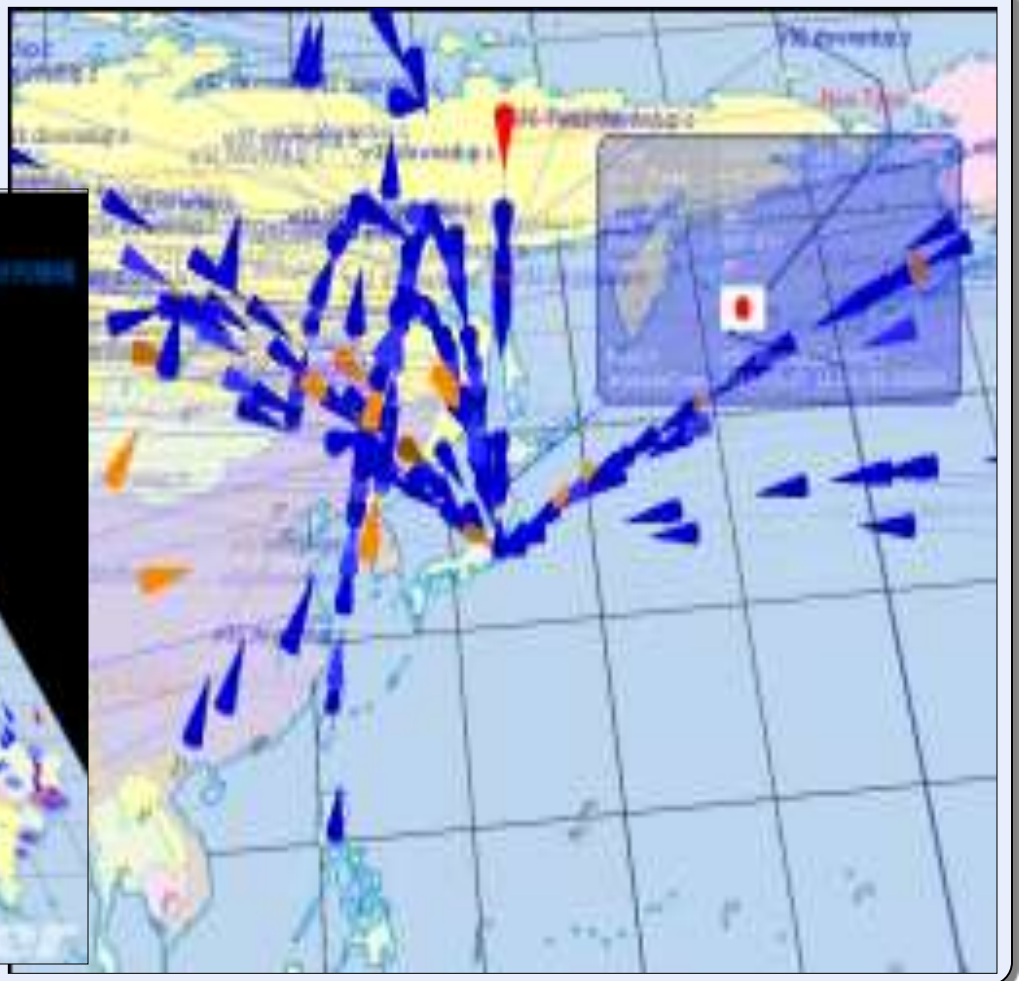
情報通信研究機構（NICT：エヌ・アイ・シー・ティー）では、インシデント分析センター（nicter）により、サイバー攻撃観測・分析網を構築して、サイバー攻撃の状況をリアルタイムで把握し、分析。

nicter

Network Incident analysis Center for Tactical Emergency Response

リアルタイムネットワーク観測・分析



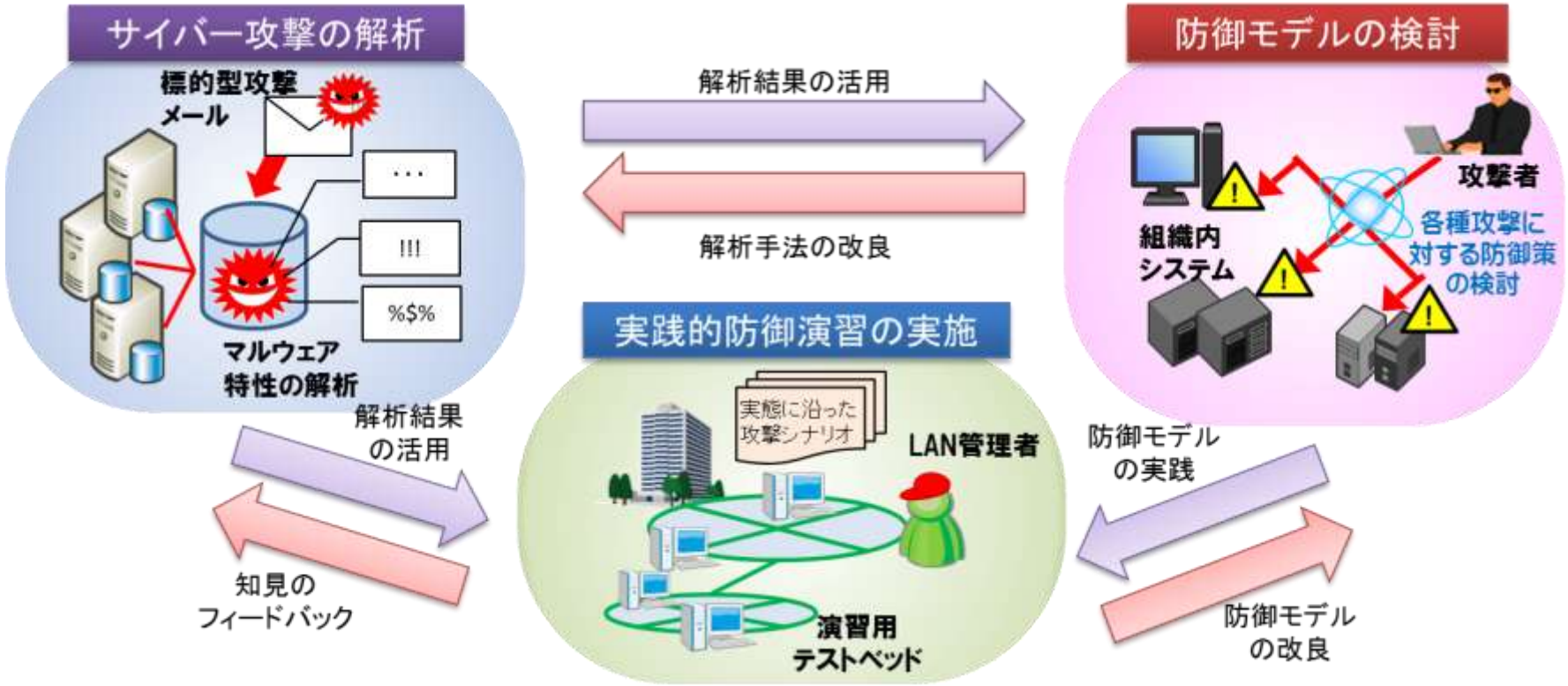


ICT環境の変化に応じた情報セキュリティ対応方策の推進事業②（サイバー攻撃解析・防御モデル実践演習）

昨今、国会、政府機関、民間企業等がネットワークを通じたサイバー攻撃を受け、情報漏えい等の被害が発生する事態が頻発している。サイバー攻撃が標的型攻撃※をはじめ巧妙化・複合化するなど、ICT環境が変化する中、我が国における情報セキュリティ対策基盤の強化が喫緊の課題となっている。

新たなサイバー攻撃に対応可能な環境を実現するため、攻撃の解析及び防御モデルの検討を行い、官民参加型のサイバー攻撃に対する実践的な防御演習を実施する。

標的型攻撃：特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃。



○ 実施期間：平成24～29年度
○ 所 要 額：平成24年度補正予算 15億円

情報セキュリティ技術の研究開発・実証実験施設の整備

施策概要

○ 政府機関、民間企業等を狙った近時のサイバー攻撃では、技術的に高度な潜在型のマルウェア※等が使用されており、既存の技術では対処が極めて困難。

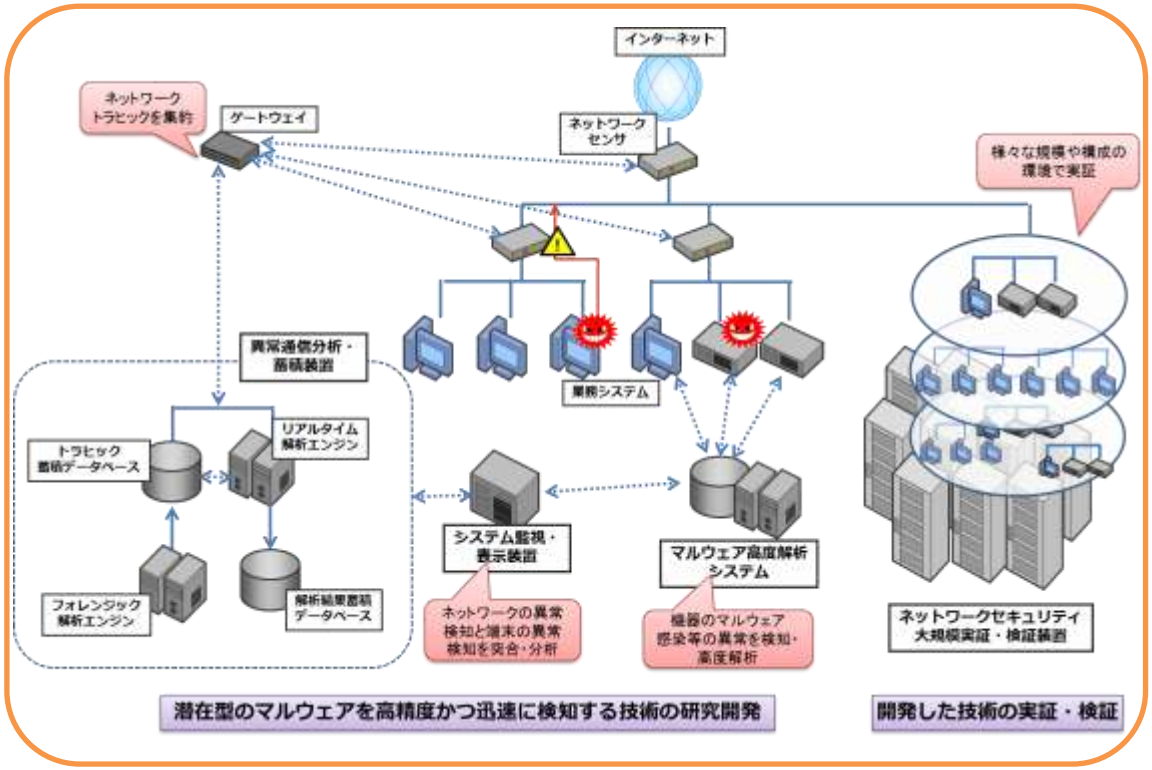
※ マルウェアとは、コンピュータウイルスのような有害なソフトウェアの総称。
潜在型のマルウェアとは、自らの挙動を正常の通信に紛れ込ませ、検知を極めて困難にしているマルウェア。

○ 潜在型のマルウェアへの感染を高精度かつ迅速に検知する技術等、革新的な情報セキュリティ技術の研究開発・実証実験を実施するための施設を、(独)情報通信研究機構(NICT)に整備する。

＜整備対象＞

①潜在型のマルウェアを高精度かつ迅速に検知する技術の研究開発環境

②様々な規模や構成のネットワークを模擬し、開発した技術の実証・検証を行うための環境



○ 所 要 額：平成24年度補正予算 100億円

安全な暗号利用の推進

○　総務省では、電子政府等の安全性及び信頼性の確保を目的として、経済産業省と共同で暗号評価プロジェクトCRYPTREC（Cryptography Research and Evaluation Committees）を実施。
○　CRYPTRECでは、安全性に優れる暗号技術を「電子政府推奨暗号リスト」としてリスト化し、各府省に対して、その利用を推奨。現在、同リストの改訂に向け作業中

◇ CRYPTRECの概要

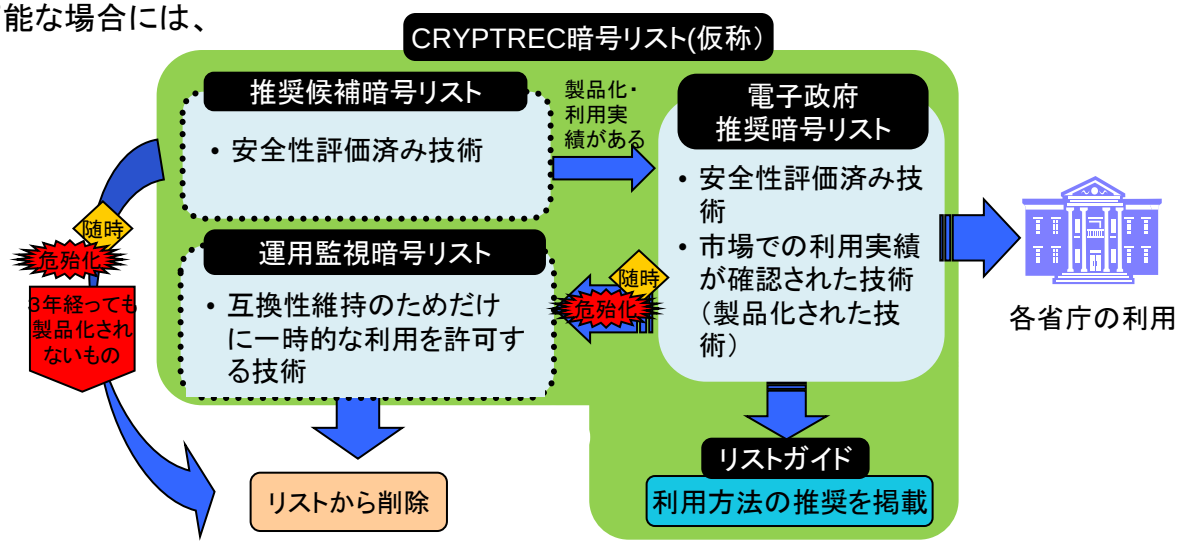
○ 構成：
・暗号技術に関する専門家で構成。（座長：今井 秀樹 中央大学教授）
○ 活動内容：
・「電子政府推奨暗号リスト」の公表。
・暗号技術の安全性の監視活動及び評価を実施。

※各府省庁における暗号化及び電子署名のアルゴリズムについて、「電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること」が定められている。

電子政府推奨暗号リスト

◇ 電子政府推奨暗号リストの改訂について

○　新たな暗号技術の開発や暗号に対する解析・攻撃技術の高度化を踏まえ、現リストを平成24年度末までに改訂。
○　改訂に当たっては、安全性に加え、調達の容易性、普及度合い等の運用性を評価。
○　本改訂により、国産暗号技術の選択と集中を図り、国産暗号の普及を促進。

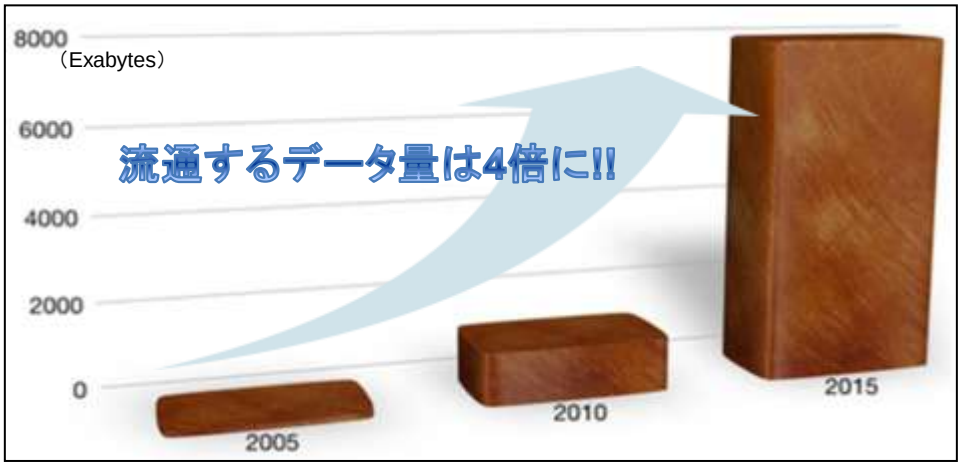


電子政府推奨暗号リスト改訂の流れ

安全と確認された暗号のみが推奨候補暗号となる。さらに、製品化が進んでいる暗号及び将来性が見込まれる暗号に絞り込み、電子政府推奨暗号リストに掲載。

プライバシーの保護

ICTの普及発達

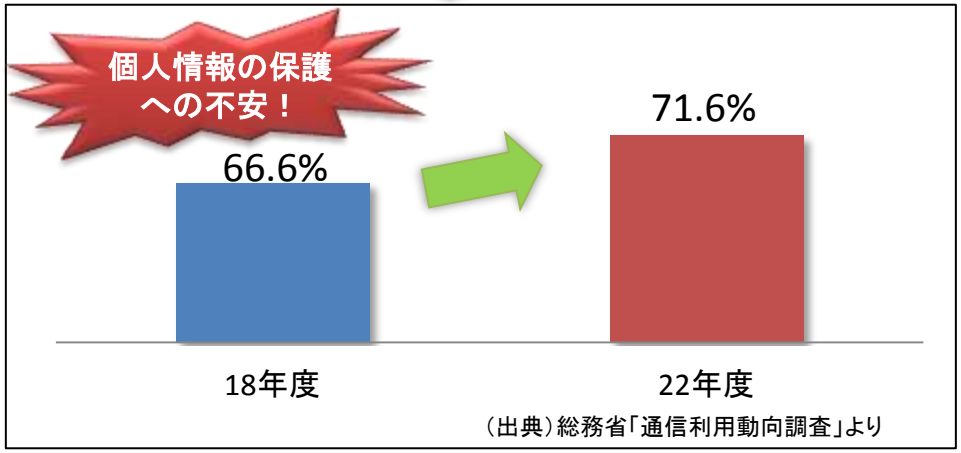


・新ビジネス・利便性の増大

・多種多様な大量の情報の利用が可能に

・ネットワークを通じた国境を越える情報の利用・流通の拡大

その一方で



海外でも活発な議論

〇EU：個人データ保護規則案の提案

・2012年1月
・急速なICTの進歩とグローバル化の進展，個人データ保護に対するリスクの拡大，等
・域内の規制の単一化・簡素化，より強固な個人データ保護ルールの整備，等
・本年内の合意、2年後の発効を目指す

〇米国：プライバシー権利章典の公表

・2012年2月
・プライバシー保護は、デジタル経済をドライブする上での基本要件
・消費者が自身のプライバシー情報をコントロールできること，同情報の取り扱いの透明性確保，同情報のセキュアな取り扱い，等

パーソナルデータ（個人に関する情報）の保護に配慮しつつ
様々なデータのネットワーク上での利用・流通を促進する新たなルールについて検討

パーソナルデータの利用・流通に関する研究会

開催趣旨

ICTの普及発達により、ライフログなど多種多様な大量の情報（いわゆるビッグデータ）がネットワークを通じ流通する社会を迎えている。 これにより、新ビジネスの創出、国民の利便性の増大、より安心安全な社会の実現などが期待されている一方、個人に関する大量の情報が集積・利用されることによる個人情報・プライバシー等についての不安も生じている。

また、ICTの普及発達は、クラウドサービスなど国境を越えた情報の流通を極めて容易としており、国際的な調和の取れた、自由な情報の流通とプライバシー保護等の双方を確保する必要性が高まっている。海外でもEUでデータ保護規則案の提案、米国でプライバシー権利章典の公表がなされるなど活発な議論が行われている。

これらを踏まえ、プライバシー保護等に配慮したパーソナルデータ（個人に関する情報）のネットワーク上での利用・流通の促進に向けた方策について検討する。

主な検討事項

○ 適切な流通に向けた、パーソナルデータの取扱いについての基本的な考え方

情報の自由な流通とプライバシー保護等の関係、パーソナルデータの性質に応じた適切な取扱い　等

○ 適切な流通に向けた、パーソナルデータの具体的な取扱いの在り方

パーソナルデータの性質に応じた適切な具体的な取扱い、 匿名化、暗号化などの技術の利用　　等

○ 適切な流通に向けた、安心安全なパーソナルデータの取扱いの確保に向けた方策

プライバシーの保護等について国民の信頼や安心を確保するための方策、国際的なハーモナイゼーション　等

構成員

有識者（法学系、工学系）、弁護士、消費者団体、コンサル、通信事業者、国内外ベンダー、自治体、研究機関　等

（座長　堀部 政男　一橋大学名誉教授）

開催期間

平成24年11月1日に第1回会合を開催。平成25年7月を目途に一定の取りまとめを行う予定。

終わりに

- ☐ はじめに
- ☐ サイバー攻撃の動向
- ☐ 情報セキュリティ政策の動向
- ☑ 終わりに

情報セキュリティ月間（２月）について

情報セキュリティに関する意識の向上のため、官民連携を図りつつ、行事の開催や広報等の普及啓発活動を集中実施。

イベントの開催

●**キックオフ・シンポジウム（2/1）**

月間のキックオフイベントとして、情報セキュリティの現状と対策等に関するシンポジウムを開催し、その模様を**インターネットで配信**

●**情報セキュリティ勉強会（2/20）**

最新の情報セキュリティ脅威を踏まえた政府職員向けの勉強会を開催

全国ブロック別イベント

全国８ブロックにおいて各ブロックにおける基軸となる講演会等を開催

その他官民による関連行事

様々な関連行事を集中的に開催

【主な行事】

●**情報セキュリティに関する講習等（都道府県警察）**
小中高校等を対象に、サイバー犯罪の現状、検挙事例等を説明

●**e-ネット安心講座（総務省、文部科学省等）**
保護者等を対象とした子供たちをネットトラブルから守るための講座

●**インターネット安全教室（経済産業省等）**
家庭や学校におけるインターネット利用の基礎知識を学習

官民連携の推進

様々な手法により官民連携を推進

【主な連携の例】

●民間イベントへの後援、講師派遣

●ホームページやメールマガジン等において、相互の取組等を紹介

トップからのメッセージ発信

月間に関するトップメッセージを、記者会見、ＨＰへの掲載を通じ周知

※イメージ

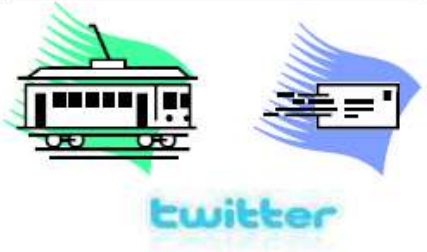
専用ＨＰの更新

「国民を守る情報セキュリティサイト」に、**スマートフォンのセキュリティ対策に関するページ**を開設、**日替わり川柳**を掲載

※イメージ

各種媒体の活用

電車広告、メールマガジン、Twitter、政府広報等を通じ各種情報を提供



周知用素材の作成・配布

月間周知用のポスター、名刺用ステッカー、バナーを作成、配布

ご清聴ありがとうございました。

（参考） 総務省　国民のための情報セキュリティサイト

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm