総務省
MIC Ministry of Internal Affairs and Communications

総務省における情報セキュリティ政策の最新動向

情報流通行政局
情報セキュリティ対策室
課長補佐　鈴木　智晴

自己紹介

○ 平成18年4月　総務省入省　情報通信政策局（当時）　放送技術課　配属
　－ 日本の地上デジタル放送方式の海外展開などを担当

○ 平成20年7月　情報通信国際戦略局　宇宙通信政策課　衛星開発係長
　－ 準天頂衛星（日本版GPS）初号機の開発などを担当

○ 平成22年7月　総合通信基盤局　電波部　移動通信課　国際係長
　－ ITS（高度道路交通システム）の技術基準の策定などを担当

○ 平成23年11月　岩手県上閉伊郡大槌町へ出向
　－ 自治体クラウドへの移行をはじめとした情報通信施策全般を担当

○ 平成25年4月より現職

目次

情報セキュリティとは

セキュリティ　①安全。保安。防犯　②担保　③証券　（広辞苑第6版）

【英語】（英英辞典Farlex Dictionaryの「Security」を和訳）
①リスクや危険のないこと。安全、②疑いや不安のないこと。信頼、③安全を与える・保障するもの。警備。攻撃や諜報を防ぐなど・・（略）、④義務の履行を保証するもの、⑤所有や権利を表す書類。株式や債券

情報セキュリティの定義　（ISO/IEC 27001）

◆ 「情報セキュリティ」（Information Security）とは、情報の機密性、完全性及び可用性を維持すること。

・機密性（Confidentiality）	許可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。
・完全性（Integrity）	資産の正確さ及び完全さを保護する特性。
・可用性（Availability）	許可されたエンティティが要求したときに、アクセス及び使用が可能である特性。

その他、OECDの情報セキュリティ・ガイドライン（1992年）や、米国情報セキュリティ・マネジメント法（2002年）でも同様の扱い。

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。

2013年4月・・・NTTレゾナントが運営するポータルサイト「goo」が不正アクセスを受け、約3万人のアカウントに不正ログインがあったとの報道。

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。

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。

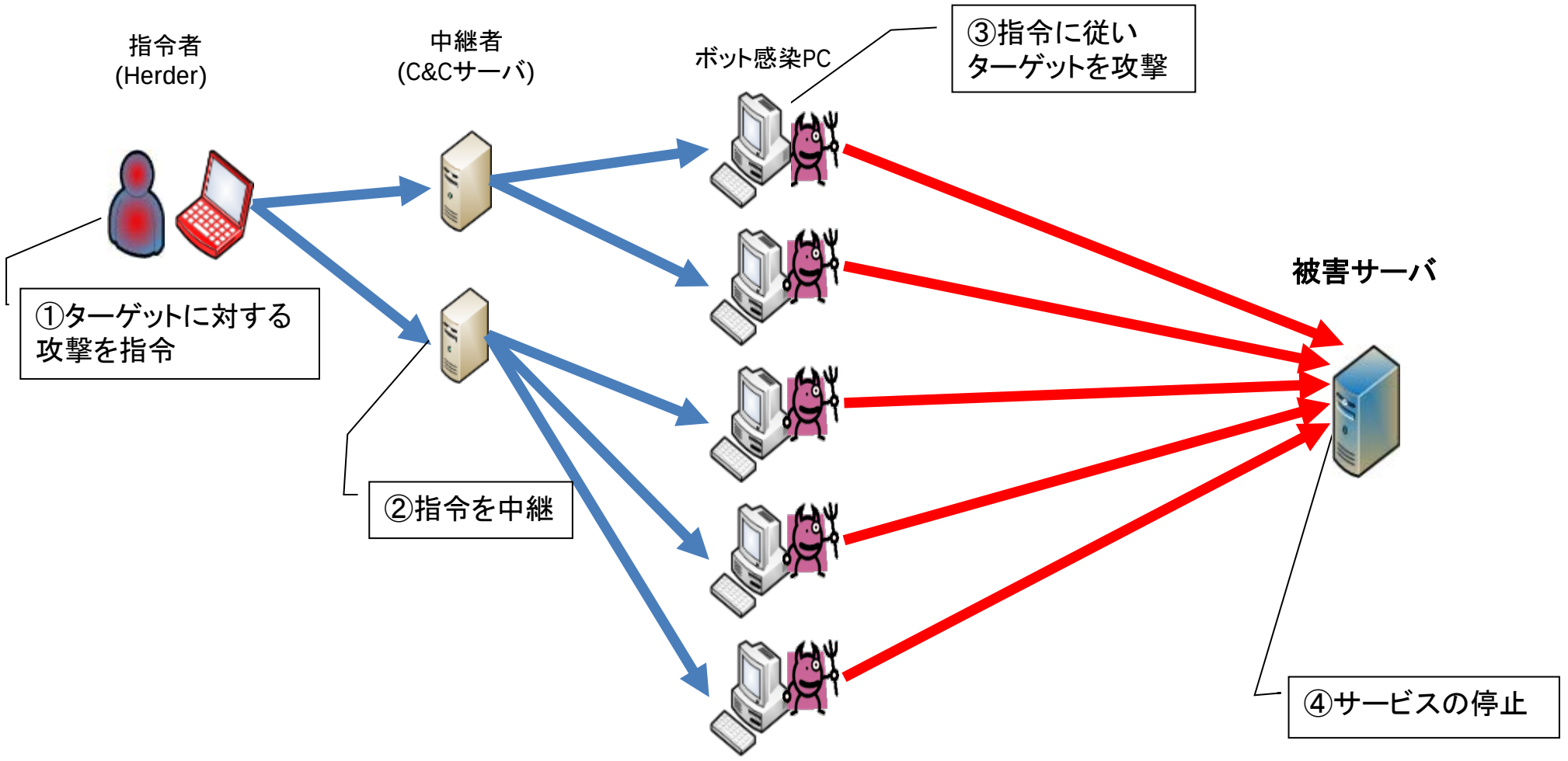
2011年11月・・**総務省**のパソコン23台が情報収集型のウイルスに感染していたことが判明、個人情報、業務上の情報が流出したおそれ。

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。

2013年3月・・・韓国において、主要放送局や金融機関のコンピュータが一斉にダウンするというサイバー攻撃が発生。

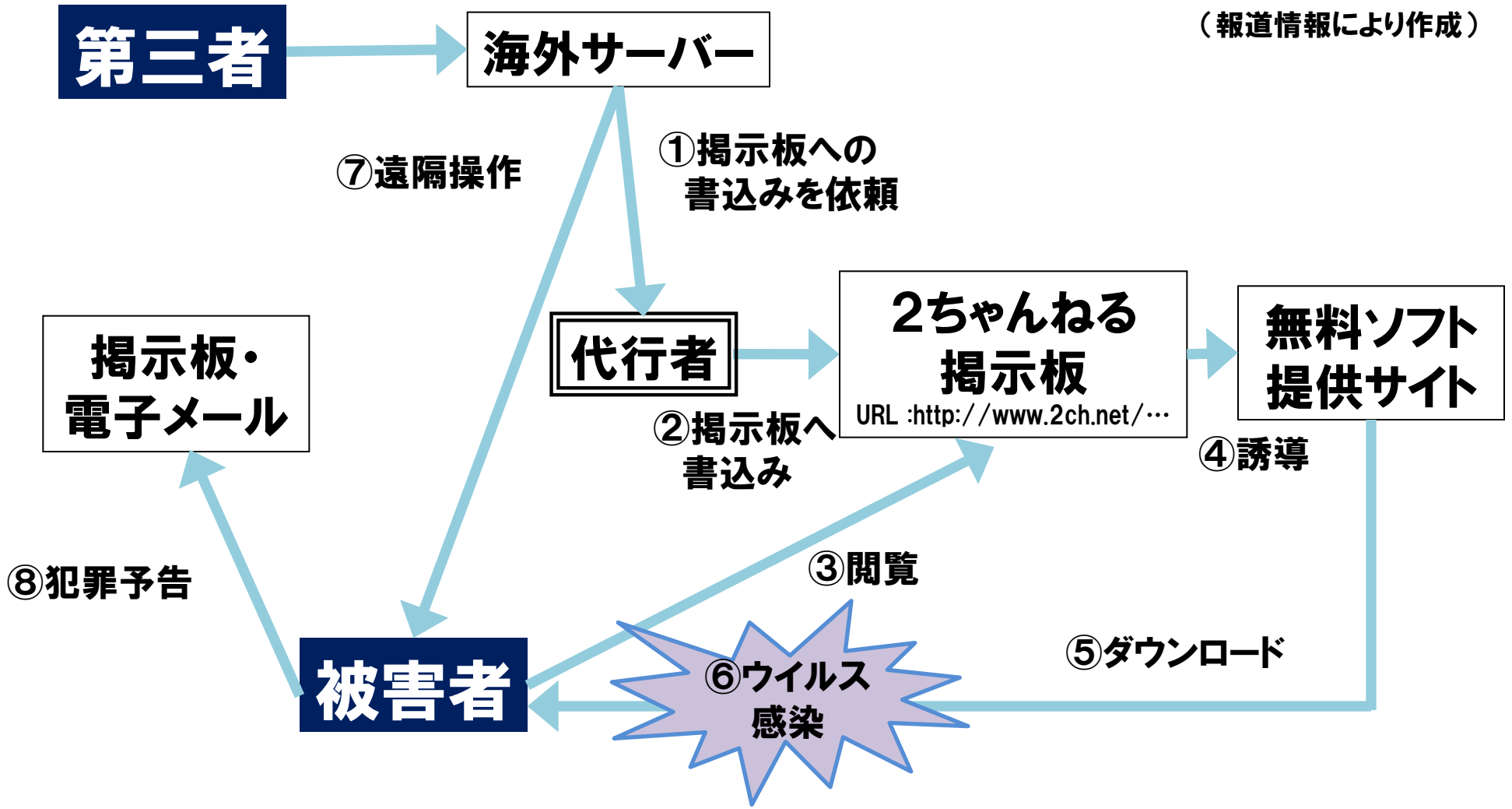
DDoS攻撃とは

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

不正アクセスの例（遠隔操作ウイルス事案の構図）



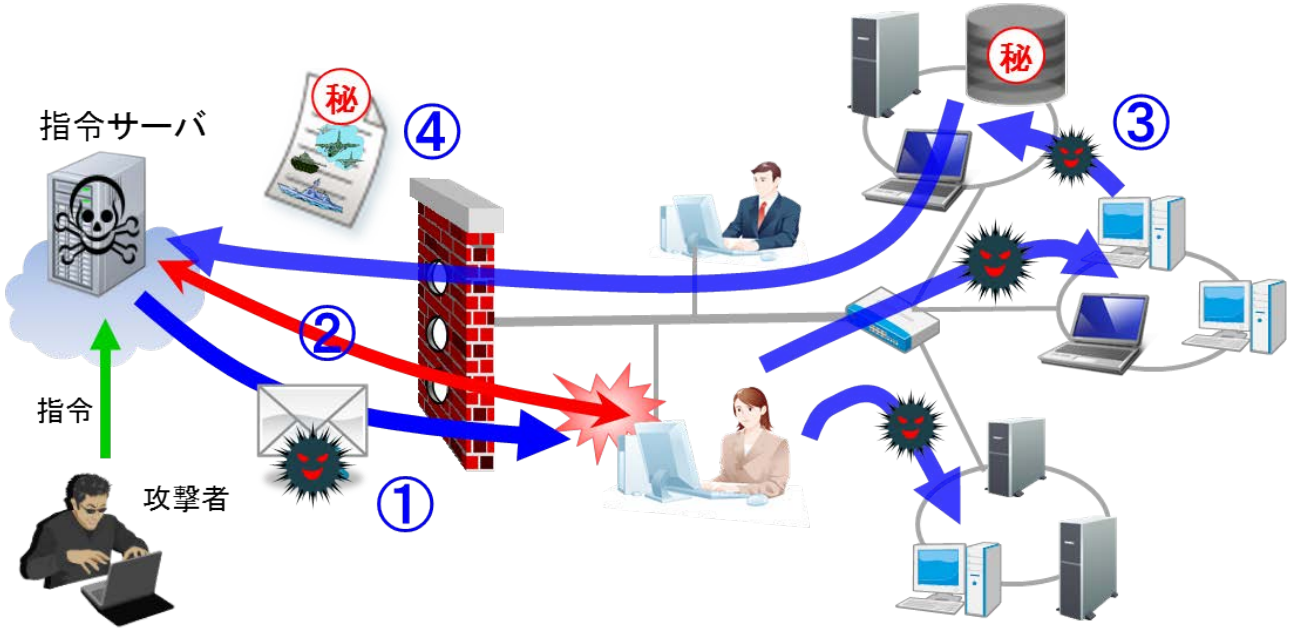
標的型サイバー攻撃とは

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。

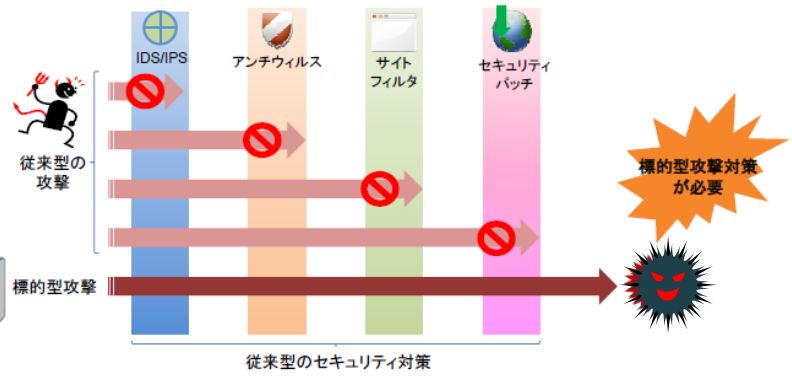
① 標的型メールにより、PCをマルウェアに感染させる。
② 当該PCと、指令サーバとを通信させる。
③ ネットワークを内偵しつつ、組織内でマルウェアの感染を拡大させる。
④ 最終目標への攻撃を遂行し、秘密情報等を手に入れる。



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。

危険度

経済犯・組織犯
金銭等の目的
計画的・悪質

愉快犯
自己顕示欲、見せしめ、嫌がらせ

メールによる感染

ネットワークによる感染

ウェブサイトによる感染

トロイの木馬

ワーム

ボット
（ロボットの略から命名）

ガンブラー

標的型サイバー攻撃

高度化
複雑化

特定の組織や個人になりすましメールを送りつけるなどして、情報窃取などを行う。

感染したPCは、遠隔操作され迷惑メール、攻撃の踏み台などに悪用。

ウェブサイトの閲覧で感染し、データの窃盗などに悪用。

一昔前のウィルス

★目立つ → 駆除しやすい

★目立たない → 駆除しにくい
感染ユーザは「少し調子がおかしいかな？」程度で、特段の不具合を感じない。

2000年　2005年　2010年

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）

目次

日本経済再生に向けた緊急経済対策（抜粋）

前文 日本経済再生に向けた取組の第１弾　　（平成２５年１月１１日閣議決定）

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

第183回国会 安倍総理所信等

【第183回国会 安倍内閣総理大臣所信表明演説（平成25年1月28日）（抄）】

＜国家としての危機管理＞

　併せて、今般のアルジェリアでのテロ事件は、国家としての危機管理の重要性について改めて警鐘を鳴らすものでした。テロやサイバー攻撃、大規模災害、重大事故などの危機管理対応について、二十四時間・三百六十五日体制で、さらなる緊張感を持って対処します。

【第183回国会 安倍内閣総理大臣施政方針演説（平成25年2月28日）（抄）】

＜世界一安全・安心な国＞

　治安に対する信頼も欠かせません。ネット社会の脅威であるサイバー犯罪・サイバー攻撃や、平穏な暮らしを脅かす暴力団やテロリストなどへの対策・取締りを徹底します。

※ICT関連は他に、クールジャパン、テレワーク、遠隔医療。

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

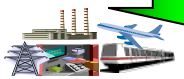
（事務局）
内閣官房情報セキュリティセンター（NISC）
センター長（官房副長官補（安危））
副センター長（内閣審議官）2名
内閣参事官6名

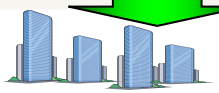
情報セキュリティ緊急支援チーム（CYMAT）

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

情報セキュリティに関する新たな基本戦略の策定について

○　情報通信技術の進展により、国民生活、社会経済、行政や安全保障・治安等のあらゆる活動がサイバー空間に依存。それに伴い、重要情報の窃取等のリスクや被害が増大するのみならず、サイバー攻撃等が国家基盤や社会基盤を揺るがすという脅威も大規模化・高度化・国際化。

○　こうした深刻化する国内外における環境変化等を踏まえ、「新たな基本戦略」の早急な策定が必要。

「新たな基本戦略」については、IT戦略本部におけるIT戦略の再構築に関する検討等と連携しつつ、平成25年夏までに、情報セキュリティ政策会議にて決定。

年度：2000 ／ 2004 ／ 2005 ／ 2006 ／ 2009 ／ 2010 ／ 2011 ／ 2012 ／ 2013 ／ 2014

各省における試行錯誤	サイバー攻撃への対応を中心とした対策実施時期	IT障害への対応も含めた総合的な対策基盤づくりの推進	サイバー攻撃事態発生を念頭、新たな環境変化対応、能動的情報セキュリティ対策 「事故前提社会」への対応力強化など成熟した情報セキュリティ先進国へ向けた取組

IT戦略

- e-Japan戦略（2001.1）
- e-Japan戦略Ⅱ（2003.7）
- IT新改革戦略（2006.1）
- i-Japan戦略2015（2009.7）
- 新たな情報通信技術戦略（2010.5）
- IT戦略の再構築（予定）

情報セキュリティ戦略

中長期計画

- 第１次情報セキュリティ基本計画 ～「セキュア・ジャパン」の実現に向けて～（2006.2）
- 第2次情報セキュリティ基本計画 ～IT時代の力強い「個」と「社会」の確立に向けて～（2009.2）
- 国民を守る情報セキュリティ戦略（2010.5　2013年度までが対象）
- **新たな基本戦略（2013年夏までに策定）**

【現行目標】
2020年までに、情報通信技術を安心して利用できる環境（高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」の実現

年度計画：2006 ／ 2007 ／ 2008 ／ 2009 ／ 2010 ／ 2011 ／ 2012 ／ 2013 ／ ・・・・・

我が国の経済発展及び国家安全保障、国民の安全・安心を確保するため、サイバー空間の持続性・発展性（「サイバーセキュリティ」）が確保された、「サイバーセキュリティ立国」の実現へ

＜第32回情報セキュリティ政策会議資料より作成＞

情報セキュリティ戦略の方向性について

環境の変化

サイバー空間と実空間の融合・一体化

- *情報通信技術の普及・高度化・利活用の進展*
  - *→ワイヤレス、クラウド、医療・就労・行政・防衛　等*
- *今後の成長による更なる進展*
  - *→ビッグデータ、M2M、IoT、ITS、スマートグリッド　等*
- *グローバルな拡大・浸透*
  - *→先進・新興・途上国等で成長のエンジンとして期待　等*

サイバー空間を取り巻くリスクの深刻化

- *甚大化するリスク*
  - *→国家・企業機密、基幹インフラ制御、医療機器　等*
- *拡散するリスク*
  - *→スマートフォン、家電、複合機、車、社会インフラ　等*
- *グローバルリスク・ボーダレスリスク*
  - *→外国からの攻撃、国内を踏み台とする外国への攻撃　等*

基本的な方針

国家の安全保障及び経済発展、国民の安全・安心を確保するため、
世界を率先する強靭で活力あるサイバー空間を実現
（「サイバーセキュリティ立国」）

① 情報の自由な流通の確保

- 管理や規制を過度に行うことなく、開放性や相互運用性を確保することにこれまで努力。
- 実空間のあらゆる活動が相互依存する神経系として、経済成長等を実現することが必要。

② リスクの深刻化への新たな対応

- リスクが甚大化、拡散し、さらに、リスクがグローバル化・ボーダレス化する状況が発生。
- 今後は、今までの取り組みとは異なる新たな対応が必要。

③ リスクベースによる対応

- サイバー攻撃の脅威が増大している状況では、全ての脅威に対応するのは不可能。
- リスクの性質を踏まえたリスクベースの対応強化が必要。

④ 社会的責務を踏まえた行動と共助

- サイバー空間に相互依存する官・公・学・産・民による社会的責務を踏まえた行動が必要。
- 社会的立場に応じた役割を発揮し、相互に、国際的にも連携しながら共助することが必要。

情報セキュリティ戦略の方向性について

各主体の役割の明確化

●サイバー空間に相互依存する官・公・学・産・民による社会的責務を踏まえた行動が必要。
●社会的立場に応じた役割を発揮し、相互に、国際的にも連携しながら共助することが必要。

① 国による積極的・先導的な役割

- 国際規範形成への積極的参画等のサイバー空間に関する外交。　サイバー空間の防衛や犯罪対策。
- 各種制度整備等による取組促進。　先端技術開発。　対策実施主体としての政府機関等における対策強化。

② 重要インフラ事業者等による安定的な役割

- 電子行政やスマートグリッド等が今後展開。サイバー攻撃等により、甚大な被害をもたらす恐れ。
- 政府機関等における対策に準じた取組。

③ 企業や教育・研究機関による協調的な役割

- 営業秘密、知的財産情報や個人情報等、競争力の源泉となる情報を保有。国際競争力の礎としても重要。
- サイバー攻撃による情報窃取等により、産業競争力を阻害する恐れ。　産業全体としての取組。

④ 一般利用者や中小企業による自律的な役割

- 全てにおいて隅々までの対応が困難。セキュリティホールとして攻撃対象となり、他者に波及する恐れ。
- リテラシー向上等の取組。

⑤ 情報通信関連事業者等による自浄的・自立的な役割

- サイバー空間を構成する技術等は民間企業が中心に提供。海外技術等への依存が高い状況。
- 情報通信関連事業者によるサイバー空間衛生確保や国内セキュリティ事業者による製品開発等の取組。

情報セキュリティ戦略の方向性について

取組分野

1. 強靱なサイバー空間 （サイバー空間の持続性）

▶インシデント情報の共有やサイバー空間の自浄機能等を通じ、攻撃等に対する防御/回復力が強化された社会

①政府・重要インフラ等対策	【例】政府システムのセキュリティ抜本的強化、重要インフラ範囲見直し、GSOC強化　等
②企業等対策	【例】企業秘密等に係るインシデント情報の共有強化、サプライチェーンセキュリティ　等
③サイバー空間の「防衛」	【例】関係主体の役割の明確化　等
④サイバー空間の犯罪対策	【例】証拠保全・フォレンジックの強化、司法・警察分野における人材育成の強化　等
⑤サイバー空間の衛生	【例】セキュリティ認証の制度整備、インシデント認知等における関連制度の弾力化　等

※GSOC（Government Security Operation Coordination team）

2. 活力あるサイバー空間 （サイバー空間の発展性）

▶高度な技術や人材の育成/蓄積等を通じ、新たなリスクに自立的に対応できる創造/知識力が強化された社会

①産業活性化	【例】サイバー空間の高度利用、政府による調達等の促進、研究開発の強化　等
②人材育成	【例】高度な資格制度の創設と政府による採用、産学連携による実践教育の強化　等
③リテラシー向上	【例】初等中等教育におけるリテラシー教育の強化、効果的な普及・啓発の推進　等

3. 世界を率先するサイバー空間 （サイバー空間のグローバル性）

▶国際的なルール形成や信頼の醸成等を通じ、グローバルな戦略空間における貢献/展開力が強化された社会

①外交	【例】共通の価値を有する国等との関係強化、国際規範形成への積極的参画　等
②国際展開	【例】ASEAN諸国等への日本企業の進出支援、国際標準化の推進　等
③国際連携	【例】海外捜査機関等との情報共有の促進、CSIRT間連携の強化　等

※CSIRT（Computer Security Incident Response Team）

体制・制度

【例】政策会議・NISCの強化、中長期目標の管理、セキュリティクリアランスによる情報共有促進　等

サイバー空間を取り巻くリスクの深刻化（例）

●：国内外で実際起こったもの、○：可能性が指摘されているもの。

甚大化するリスク

- ● 標的型攻撃により、国家機密、企業機密の窃取が発生。数年前からの窃取も発覚。
- ● 海外にて、クローズな制御系システムがウィルス感染。核関連施設が稼働不能化。
- ● 海外にて、元契約社員により、制御系システムが不正操作され、川に汚水が流入。
- ○ ITSやスマートグリッドへの攻撃による交通混乱やブラックアウトの恐れが指摘。

拡散するリスク

- ● 常時、電源ON・ネット接続で携帯されるスマートフォンから情報流出が多発。
- ● コンビニにおける防犯カメラが踏み台となり、DDoS攻撃を実施。
- ○ ネット接続の家電や自動車から生活情報や位置情報が流出する恐れが指摘。
- ○ オフィスにおけるコピー機等の複合機が情報窃取の起点となる恐れが指摘。

グローバルリスク

- ● 海外にて、外国政府の関与が疑われる政府機関等に対するDDoS攻撃が発生。
- ● 海外にて、企業秘密の窃取等を狙った外国軍隊の関与が疑われる攻撃が発生。
- ● 国内の個人PC等が踏み台となり、指令サーバとして外国にDDoS攻撃を実施。
- ○ 武力攻撃の一環としてのサイバー攻撃が国内を起点に外国へ行われる恐れが指摘。

新たな情報セキュリティ戦略のイメージ

環境の変化

サイバー空間と実空間の融合・一体化 ［普及・高度化、更なる進展、グローバルな拡大・浸透］ ▶ サイバー空間を取り巻くリスクの深刻化 ［甚大化、拡散、グローバル・ボーダレス］

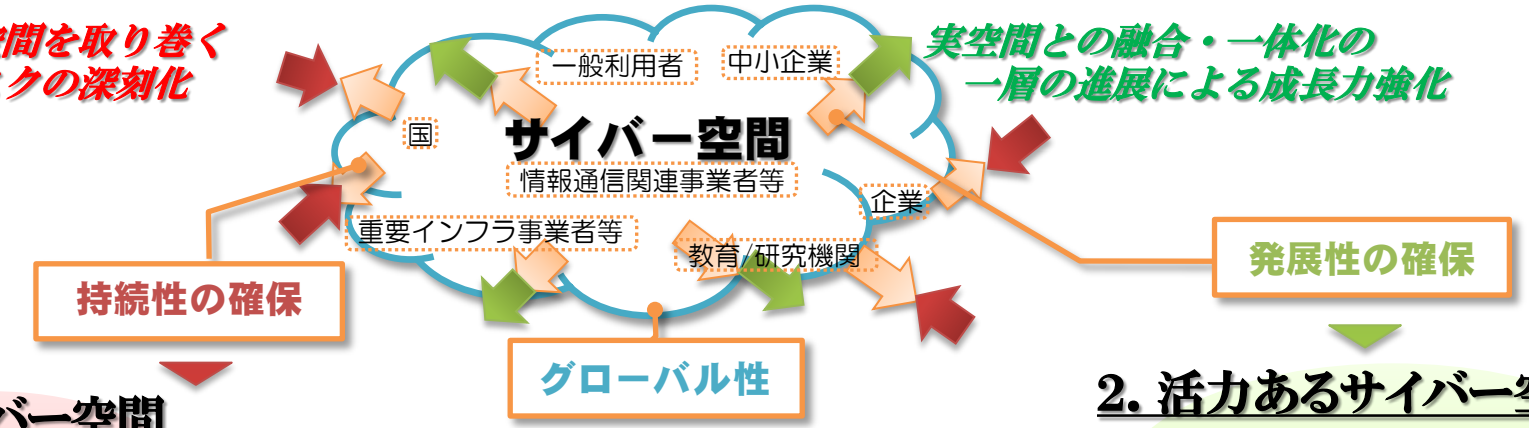
基本的な方針

国家の安全保障及び経済発展、国民の安全・安心を確保するため、世界を率先する強靭で活力あるサイバー空間を実現（「サイバーセキュリティ立国」）

① 情報の自由な流通の確保　② リスクの深刻化への新たな対応
③ リスクベースによる対応　④ 社会的責務を踏まえた行動と共助

各主体の役割の明確化

国による積極的/先導的な役割 ／ 重要インフラ事業者等による安定的な役割 ／ 企業や教育・研究機関による協調的な役割 ／ 一般利用者や中小企業による自律的な役割 ／ 情報通信関連事業者等による自浄的/自立的な役割



取組分野

1. 強靭なサイバー空間

サイバー空間の防御力・回復力の強化

①政府・重要インフラ等対策
②企業等対策
③サイバー空間の「防衛」
④サイバー空間の犯罪対策
⑤サイバー空間の衛生

3. 世界を率先するサイバー空間

サイバー空間の貢献力・展開力の強化

①外交
②国際展開
③国際連携

2. 活力あるサイバー空間

サイバー空間の創造力・知識力の強化

①産業活性化
②人材育成
③リテラシー向上

体制・制度

情報セキュリティ政策会議・ＮＩＳＣの強化、中長期目標管理、セキュリティクリアランスによる情報共有促進　等

目次

- はじめに
- 政府全体の取り組み
- **総務省の取り組み**
- おわりに

ICT成長戦略会議

- グローバル展開を視野に入れつつ、ＩＣＴを日本経済復活の切り札として活用する方策等を様々な角度から議論
- 総務大臣、副大臣、大臣政務官、１３名の有識者で構成
- 省庁の壁にとらわれず、他省庁の協力も得つつ、具体的・実践的なアウトプットを検討

社会実装戦略

超高齢社会構想会議
座長：小宮山 宏（三菱総研理事長）
座長代理：小尾 敏夫（早稲田大学教授）

街づくり推進会議
座長：岡 素之（住友商事相談役）
座長代理：小宮山 宏（三菱総研理事長）

生活資源対策会議
座長：須藤 修（東京大学大学院教授）
座長代理：山下 徹（ＮＴＴデータ相談役）

研究開発戦略

情報通信審議会 イノベーション創出委員会
主査：徳田 英幸（慶應大学教授）
主査代理：藤沢 久美（ソフィアバンク代表）

新産業創出戦略

放送サービスの高度化に関する検討会
座長：須藤 修（東京大学大学院教授）
座長代理：鈴木 陽一（東北大学教授）

放送コンテンツ流通の促進方策に関する検討会
座長：岡 素之（住友商事相談役）
座長代理：村井 純（慶應大学教授）

情報セキュリティアドバイザリーボード
座長：山口 英（奈良先端科技大学院大教授）
顧問：小野寺 正（ＫＤＤＩ会長）

ＩＣＴコトづくり検討会議
座長：三友 仁志（早稲田大学大学院教授）
座長代理：谷川 史郎（野村総研未来創発センター長）

情報セキュリティ アドバイザリーボード

情報通信分野における官民において、時々刻々と変化する情報セキュリティ上の課題に対して効果的な対策や、日本の経済成長に繋がるような有効な施策が講じられるよう、**有識者から助言を得ることを目的として設置**する。

「情報セキュリティ アドバイザリーボード」の任務

（1）**情報セキュリティ対策の在り方への助言**

情報セキュリティの推進にあたり、日本の経済成長への貢献も視野に入れつつ、情報通信分野に携わる関係者において短期的及び中長期的に講ずべき対策や既存の取組の改善などの方向性について、幅広い観点から助言を行う。

（例）・官民連携や国際連携の在り方
・情報セキュリティに係る研究開発の方向性
・DDoS攻撃や情報窃取など情報セキュリティに係るインシデント等への即応の在り方

（2）**その他**

情報セキュリティに係る諸問題への対応について、必要に応じて、提言をとりまとめる。

情報セキュリティ アドバイザリーボード

【構成員】（敬称略）

（座長）	山口 英	奈良先端科学技術大学院大学 教授
（座長代理）	林 紘一郎	情報セキュリティ大学院大学 前学長・教授
	飯塚 久夫	一般財団法人日本データ通信協会 テレコム・アイザック推進会議 会長
	岡村 久道	国立情報学研究所客員教授・弁護士
	藤沢 久美	シンクタンク・ソフィアバンク 副代表
（顧問）	小野寺 正	KDDI株式会社 代表取締役会長 ※政府の「情報セキュリティ政策会議」のメンバー

ワーキンググループ 【構成員】技術系や法律系などの有識者、電気通信事業者等

スケジュール 平成25年３月から随時開催。

「総務省における情報セキュリティ政策の推進に関する提言」について

◇　総務省では、有識者から助言を得ることを目的として、**「情報セキュリティ　アドバイザリーボード」**（座長：山口 英　奈良先端科学技術大学院大学教授）を平成25年3月から開催。

◇　本年4月、高度化・複雑化するサイバー攻撃など情報セキュリティを取り巻く環境の変化を踏まえ、**「総務省における情報セキュリティ政策の推進に関する提言」**を取りまとめ。

提言における基本的な考え方

以下の5つの基本的な考え方に立ち、総務省は、内閣官房情報セキュリティセンター等と連携しつつ、情報セキュリティ政策に取り組むことが求められる。

① 情報の自由な流通の確保

人間の尊厳、自由、民主主義など核心的な価値を推進するサイバー空間の構築による経済成長の促進。

② 過度な規制※によらない信頼できるサイバー空間の構築

イノベーションや経済成長を起こすサイバー空間の堅持。

※情報セキュリティの名の下で行われる検閲など不合理な規制

③ リスク認識に基づく対応の強化（事故前提社会）

全てのサイバー攻撃を完璧に防ぐことは困難であるという認識の下での情報セキュリティ対策の実施。

④ 動的防御プロセス連携の確立

PDCAというサイクルにとらわれることなく、常に、動的に、適時適切な意思決定を行う「動的防御プロセス連携」の確立。

⑤ 国際連携によるサイバー空間政策の推進

我が国の経済成長を見据えた戦略的な国際連携の推進。

提言のポイント

動的防御プロセス連携の確立

動的防御プロセス連携
それぞれのプロセスにおいて得られた知見を常時他のプロセスに反映

①モニタリング（検知・解析）（Observe）
◇ 継続的なモニタリングによるサイバー攻撃の検知
◇ サイバー攻撃の目的・意図を判別するための情報収集

②情勢判断（Orient）
◇ 攻撃の目的・意図を識別した上で、自組織に対する影響を把握

③意思決定（Decide）
◇ サイバー攻撃に対する措置に関する迅速かつ的確な意思決定

④行動（Act）
◇ 問題解決やリスク要因の排除の実施

総務省の取組

官民連携	悪性サイトの検知機能の強化	サイバー攻撃解析協議会による観測データ等の蓄積
国際連携	PRACTICE※1による諸外国とのサイバー攻撃情報の共有	
技術開発・人材育成	NICT「サイバー攻撃対策総合研究センター（CYREC※2）」による解析能力の向上	サイバー攻撃の防御モデルの確立・実践演習の実施※3

政府自身の防御体制の構築

・政府情報システムの情報セキュリティ対策の強化。
・職員訓練の充実。

※1 諸外国と連携してサイバー攻撃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、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及び実証実験プロジェクト。
※2 Cybersecurity Research Center
※3 演習用テストベッドを利用した官民のLAN管理者等を対象に実践的な防御演習を実施。対象やその手法の提供等は、官庁・大企業にとどまらず、地方公共団体や中小企業に拡大。

リスク認識に基づく対応の強化（事故前提社会）

個人
・ 通信事業者によるマルウェアの感染や悪性サイトへのアクセスに対する注意喚起等の実施。
・ スマホのアプリについて、個人がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みの構築。

個人や中小企業に対して自律的な対応を促す仕組みづくりの構築

中小企業
・情報セキュリティ投資促進税制等のインセンティブの検討。
・システムの共同利用など全体として低コストの情報セキュリティ対策の実現に向けた対策の推進。

国際連携によるサイバー空間政策の推進

グローバルなインターネット環境の安全の確保
共同プロジェクト推進等のASEAN諸国等との連携による情報セキュリティ環境の向上。

日本企業のグローバル展開への貢献
情報セキュリティの名の下で行われる過度な規制の撤廃に向けて省庁の枠を超えて連携。

国際的なサイバー空間の規範形成への主導的な取組
顔が見える外交を展開し、先導的に国際的なサイバー空間の規範形成をリード。

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. 利用者意識の向上

①「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。
②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。

3. 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サイバー攻撃の解析・検知に関する研究開発
・利用者の行動特性等に基づいたサイバー攻撃の解析・検知技術などの研究開発を実施。

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。

1．③ 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（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

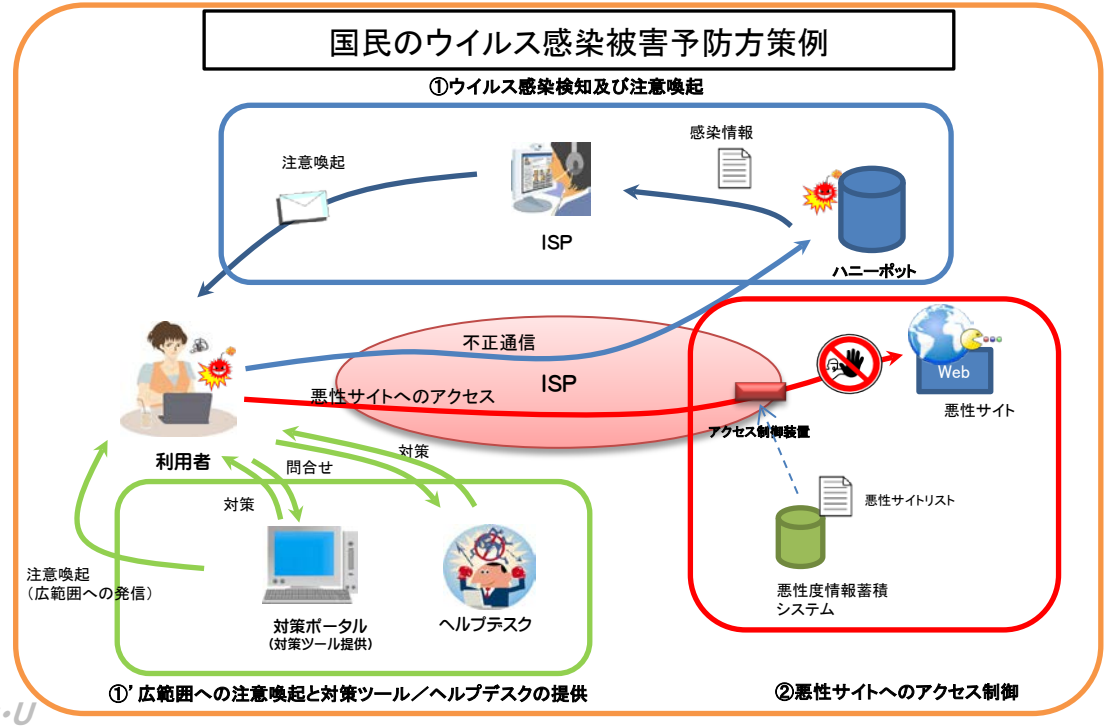
○ 個人利用者においても、ウイルス感染やID・パスワードの漏えいなどの実被害が発生していることから、インターネット利用に関する安全の確保を図るため、攻撃の解析・検知の高度化、ウイルス感染被害予防に資する研究開発・実証実験等を民間企業等への委託により実施する。

【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



2. ①『国民のための情報セキュリティサイト』のリニューアル

○「国民のための情報セキュリティサイト」は、一般利用者に情報セキュリティ対策の知識をわかりやすく提供することなどを目的として、平成15年度より運用。
○昨今、スマートフォンやSNSなどの新たな技術やサービスが登場し、情報セキュリティ対策を取り巻く環境が大きく変化していることから、近年の動向を踏まえたコンテンツの刷新を行うこととした。

（1）最近の技術動向を踏まえ、コンテンツを刷新

- 利用者が注意すべき最新の脅威と、その対策について解説
  - 携帯電話・スマートフォン・タブレット端末の注意点
  - クラウドサービスの利用上の注意点
  - SNS（ソーシャルネットワーキングサービス）利用上の注意点
  - 標的型攻撃への対策　　等


（2）親しみやすいデザインに一新

- ページ中に、親しみやすいキャラクター（盾を持った猫）を採用。

新キャラクター

現行ページ　　一般向けページ　　キッズ向けページ



（3）小学生とその保護者向けのページを新設

- 小学生がインターネットや情報機器を利用する上で注意すべきことに加え、保護者が留意すべき点も解説。

- 親と子で一緒にコンテンツを読み進めていき、共に情報セキュリティについての理解を深められる内容に。

（4）最新のウェブアクセシビリティ規格に対応

- 最新のウェブアクセシビリティ標準規格である JIS X8341-3:2010　に対応し、高齢者、障碍者を含む誰もが利用しやすい構成に改修。
  - 音声読上げブラウザでのページ読上げに対応。
  - 背景と字の色の組合せなどを色覚障碍者に配慮した構成に。

2. ② 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

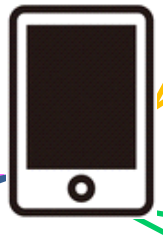
アプリケーション

○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

最終報告のフォローアップ

最終報告に掲げた情報セキュリティ対策や利用者への普及啓発策、及び当面、重点的に実施すべき事項として示された「スマートフォン情報セキュリティ行動計画」に基づき、関係事業者や政府の取組等を、事務局である総務省が調査した結果を、今後のあるべき方向性とともに公表。

ポイント

第１節　情報セキュリティ上脅威のあるアプリケーションに関する対策

〇社団法人電気通信事業者協会（TCA）において、携帯電話事業者の取組として、「アプリケーション提供サイト運営事業者向けガイドライン」を策定（平成２５年３月）。

〇一部のマルウェア対策ソフト提供事業者では、利用者情報を不適切に収集・利用するアプリケーションに対処するための機能を追加。携帯電話事業者のセキュリティサービスにも反映。

〇日本スマートフォンセキュリティ協会（JSSEC）では、Android アプリのセキュア設計・セキュアコーディングガイド」の策定・改版を行い、携帯電話事業者やアプリケーション開発企業から参照。

第２節　利用者に対する普及啓発の取組

〇総務省の取組

・「スマートフォン情報セキュリティ３か条」（平成２３年１２月）、「スマートフォン プライバシー ガイド」（平成２４年４月）、利用者向け手引書「一般利用者が安心して無線LANを利用するために」を政府広報やウェブサイト掲載、各種セミナーでの紹介等を通じて周知

〇携帯電話事業者等の取組

・TCAにおいて、スマートフォンの情報セキュリティに関する統一的啓発資料を作成。

・携帯電話事業者において、契約時配布資料や一般利用者向けの啓発教室のコンテンツにスマートフォンの情報セキュリティに関する事項を盛り込み。

フォローアップ（ｉ）:アプリケーションの可視化・制御等の取組

（１）携帯電話事業者の取組

- TCAが、平成25年3月、「アプリケーション提供サイト運営事業者向けガイドライン」を策定。アプリケーション掲載前のセキュリティ上の確認など、望まれる取組の基準を提示。
- NTTドコモでは、アプリケーションがアクセスするデータと端末機能をアイコンで表示する機能（マカフィーの「McAfee Mobile Security」）を、自社ブランドの「ドコモあんしんスキャン」として提供中。
- KDDIでは、アプリケーションによる個人情報の取扱いに応じて、漏えいの可能性を警告する「プライバシースキャン」機能（トレンドマイクロの「ウイルスバスター モバイルfor Android」）を、今後「ウイルスバスター for au」として提供を検討中。

（２）端末製造事業者の取組

- シャープ株式会社が、「電話帳アクセスモニター」として、アプリケーションから電話帳へのアクセスに関する通知・ブロック機能を導入。

（３）ＯＳ提供事業者の取組

- Android4.2以降において、危険性のあるアプリケーションをインストール前にチェックする機能や、アプリケーションが有料ＳＭＳサービスにメッセージを送ろうとしたときに利用者に通知する機能を搭載。
- iOS6において「プライバシー」セクションが設けられ、個別のアプリケーションごとに、位置情報、電話帳、カレンダー、リマインダー、写真等へのアクセスについて、利用者がインストール後に制御できる機能を搭載。

（４）その他事業者団体の取組

- 一般社団法人日本スマートフォンセキュリティ協会（JSSEC）では、「Android アプリのセキュア設計・セキュアコーディングガイド」初版を平成２４年６月に公表し、同年１１月に改訂。複数の携帯電話事業者やアプリケーション開発企業の社内教育資料として活用されているほか、平成２５年３月より、KDDIが自社アプリケーション提供サイトの掲載ガイドラインで推奨。

フォローアップ（ii）：携帯電話事業者のアプリケーション提供サイト

○情報セキュリティ上脅威のあるアプリケーションには、①マルウェアを含むアプリケーション、②ぜい弱性を含むアプリケーション、③利用者が意図しない利用者情報の外部送信を行うアプリケーションが存在。

○TCAのガイドラインを受けた取組が進展することにより、携帯電話事業者が運営するアプリケーション提供サイトが、利用者にとって一層信頼のおけるものとなることが期待。

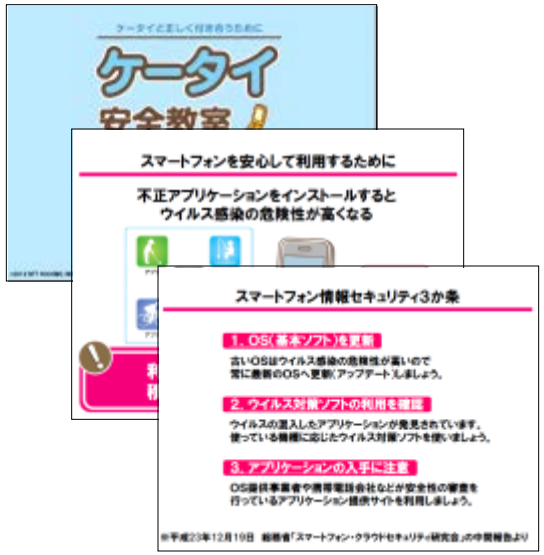
	現状	今後の方向性
①マルウェアを含むアプリケーション	・NTTドコモ及びKDDIは、必要に応じてマルウェア対策ソフト提供事業者の技術協力を受けて、事前審査を実施。	・TCAガイドラインを受け、すべてのサイトにおいて、事前審査の実施が期待。
②ぜい弱性を含むアプリケーション（現時点で大きなリスクではない）	・KDDIは平成25年3月より、JSSEC「セキュアコーディングガイド」を提携のアプリケーション開発者への推薦資料として活用。	・TCAガイドラインを受け、開発者への啓発を行うなど、アプリケーションの作成段階における対処の進展が期待。
③利用者が意図しない利用者情報の外部送信を行うアプリケーション（現時点のリスクの中心）	・KDDIにおいて、アプリケーションのパーミッション取得の理由を、開発者に申請時に申告させる取組を実施。 ・マルウェア対策ソフトの機能追加が進められ、携帯電話事業者が自社ブランドとして提供するセキュリティサービスにも追加導入していく動き。	・TCAガイドラインを受け、携帯電話事業者における審査の継続的な改善が期待。 ・マルウェア対策ソフトにおける対応等の進展が期待。

フォローアップ（iii）：携帯電話事業者等による利用者への周知啓発の取組

事業者団体で統一的
啓発資料を作成

「スマートフォン（スマホ）ご利用にあたっての注意事項」
（TCA）

青少年向け
携帯電話教室の
テキストへの
盛り込み



ケータイ安全教室資料（NTTドコモ）

契約時配布する資料に
「スマートフォン情報セキュリティ3か条」を記載

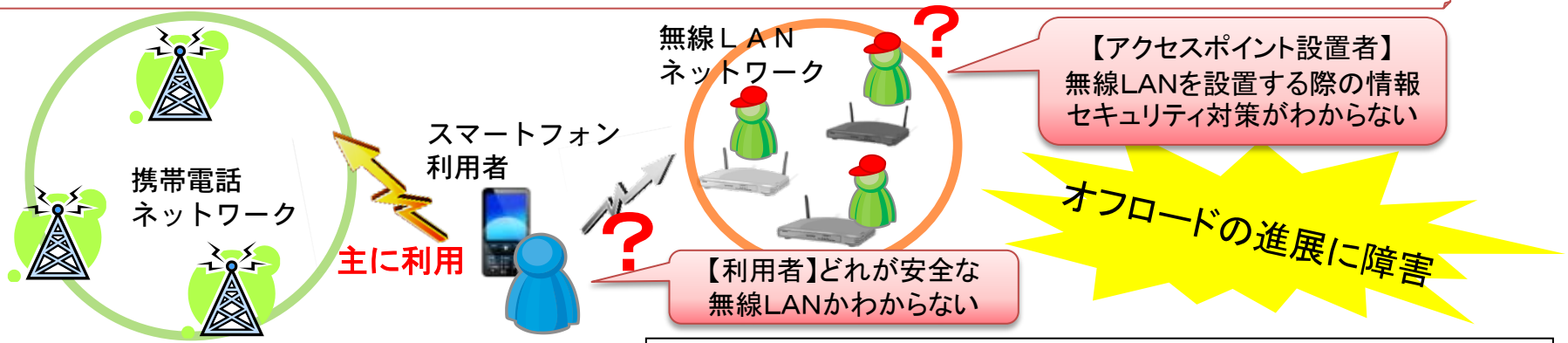
契約時配布資料（NTTドコモ）

契約時配布資料（KDDI）

フォローアップ（iv）：電波の能率的かつ安全な利用に関するリテラシー向上

現　状

・スマートフォンの急速な普及による移動体通信量の増大への対処には、携帯電話ネットワークから無線LANへのオフロード（通信の迂回）が有効。
・現状、公衆無線LANのアクセスポイントの中には、情報セキュリティ対策が不十分である等、情報漏えい等の危険性があるものが存在。
・利用者が無線LANの危険性のみを認知し、安全に利用する方策等を知らない場合、オフロードが進まず、電波の能率的利用が阻害。

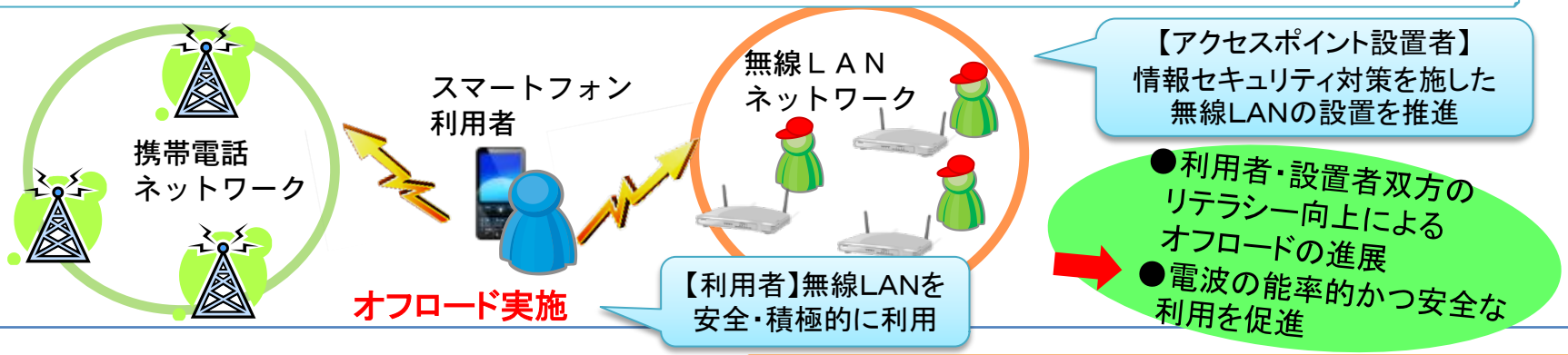


周知啓発の実施

【利用者】 無線LANの安全な利用方策、オフロードの意義・有効性
【アクセスポイント設置者】 設置者側の情報セキュリティ対策

成　果

・利用者が安心して無線LANを利用できる環境を整備するため、アクセスポイント設置者側の情報セキュリティ対策に関するリテラシーを向上。
・利用者の無線LANの安全な利用方策及びオフロードの意義に関するリテラシーを向上させることにより、オフロードを推進。



○ 実施期間：平成25年度～
○ 所 要 額：平成25年度当初予算　0.3億円（電波利用料）

2. ② 無線LANの情報セキュリティ（ｉ）

○ 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。

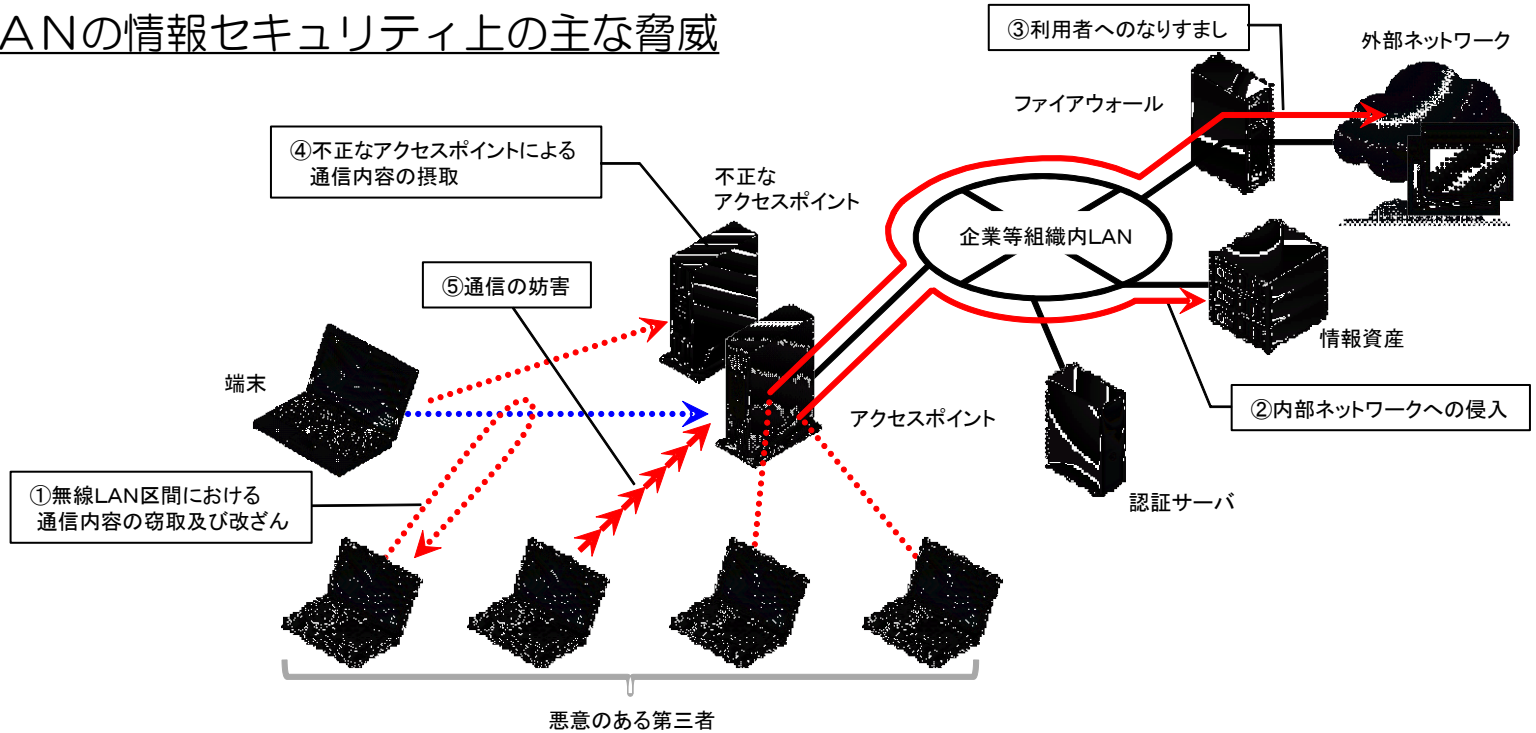
※ SSL（Secure Socket Layer）とは、信頼できるウェブサイトやサーバとの間で、データを暗号化して送受信する方法。SSLが使われていることは、URLが「https」からはじまっていることや、パソコンやスマートフォンのブラウザに「鍵マーク」が表示されることで確認。

2. ② 無線LANの情報セキュリティ（ii）

「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

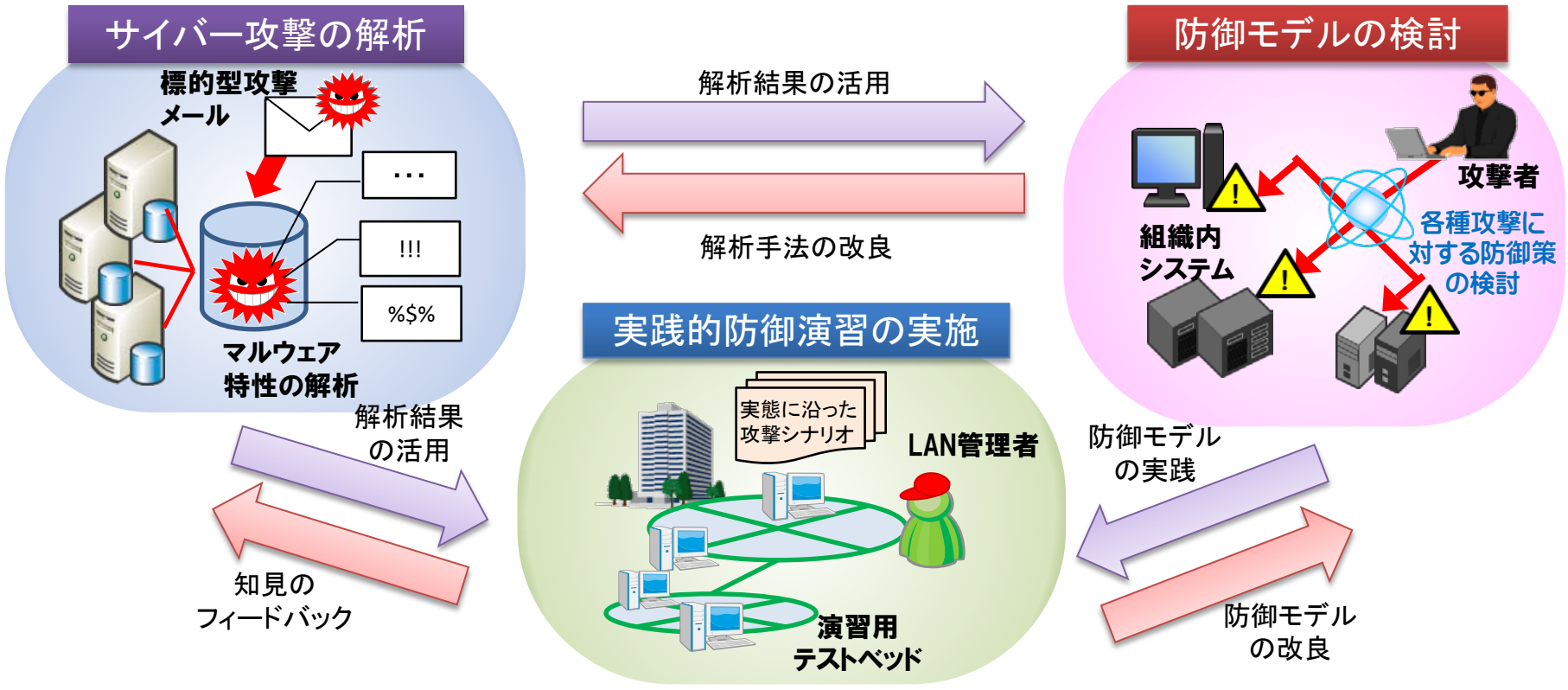
※WPA（Wi-Fi Protected Access）及びWPA2は、端末とアクセスポイントとの接続に関する認証方式（EAP等）及び通信内容の暗号化方式（CCMP等）を包含した規格の名称

3. ① 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（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

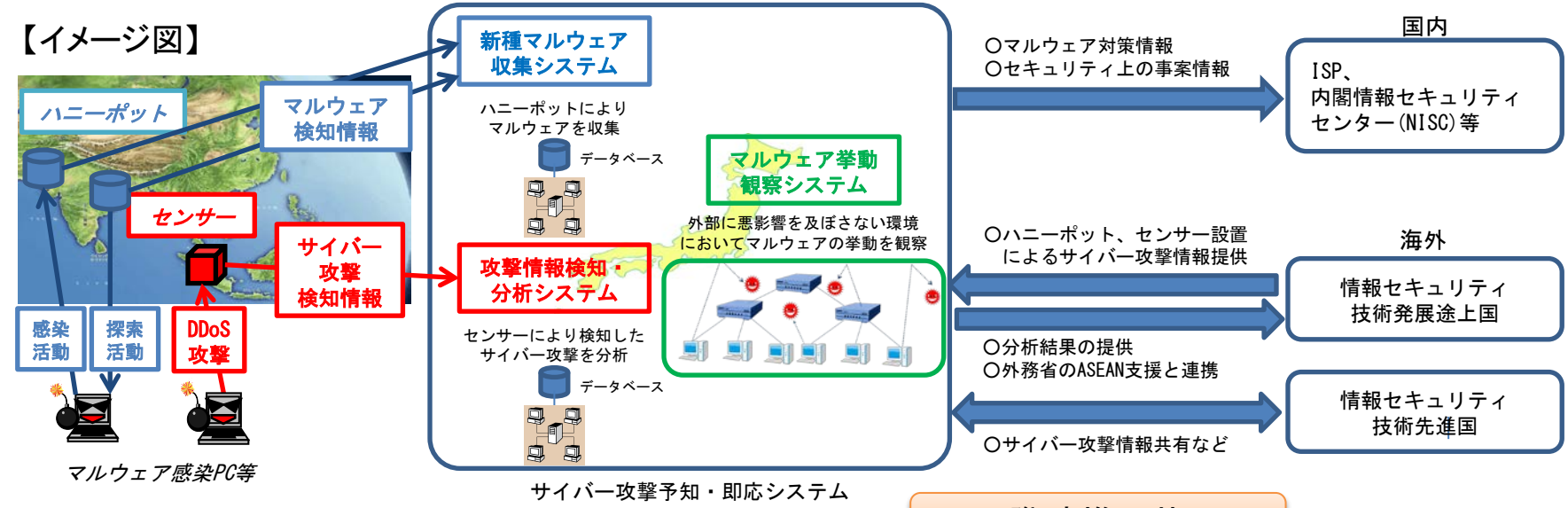
3. ② 国際連携によるサイバー攻撃予知・即応技術の研究開発

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
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。

○ そのほか、平成24年3月に**インドネシア**、4月に**モルディブ**、平成25年2月に**タイ**、3月に**マレーシア**との間で合意。

○ 現在、シンガポール等と連携に向けて協議中。

3. ③ サイバー攻撃の解析・検知に関する研究開発

目的

利用者の行動特性や環境特性等に基づいて不正な意図を検知し、侵入や感染の可能性、被害の程度、被害に至った経緯を明らかにするための技術を確立するとともに、被害拡大の防止と業務継続を両立させる組織内ネットワークを自動的に構成する技術などを開発する。

研究開発概要

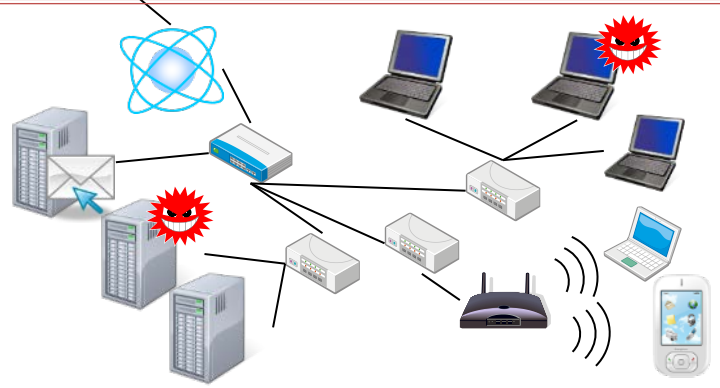
検知・解析（Observe）　情勢判断（Orient）　意思決定（Decide）　行動（Act）

Ⅰ. 行動特性

・利用者の行動特性の研究（騙され易い人、難い人の差　等）

Ⅱ. 環境特性

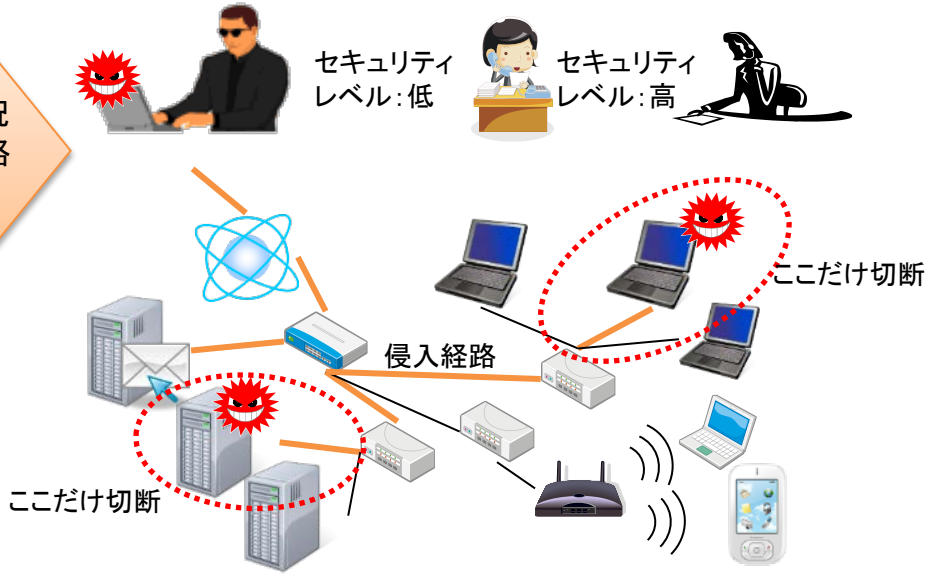
・端末情報の効果的な収集方法の研究開発
・ネットワーク状況の効率的なスキャン方法の研究開発　等



進行状況進入経路の把握

Ⅲ. 攻撃阻止と業務継続

・行動特性に応じたセキュリティレベルを適応的に設定する技術の研究開発
・進行状況や進入経路を適切に把握する技術の研究開発
・被害を拡大させずかつ業務を継続させる組織内ネットワーク構成技術の研究開発　等



<u>所要経費</u>　5．5億円　　**<u>研究開発期間</u>**　平成25年度からの5年以内

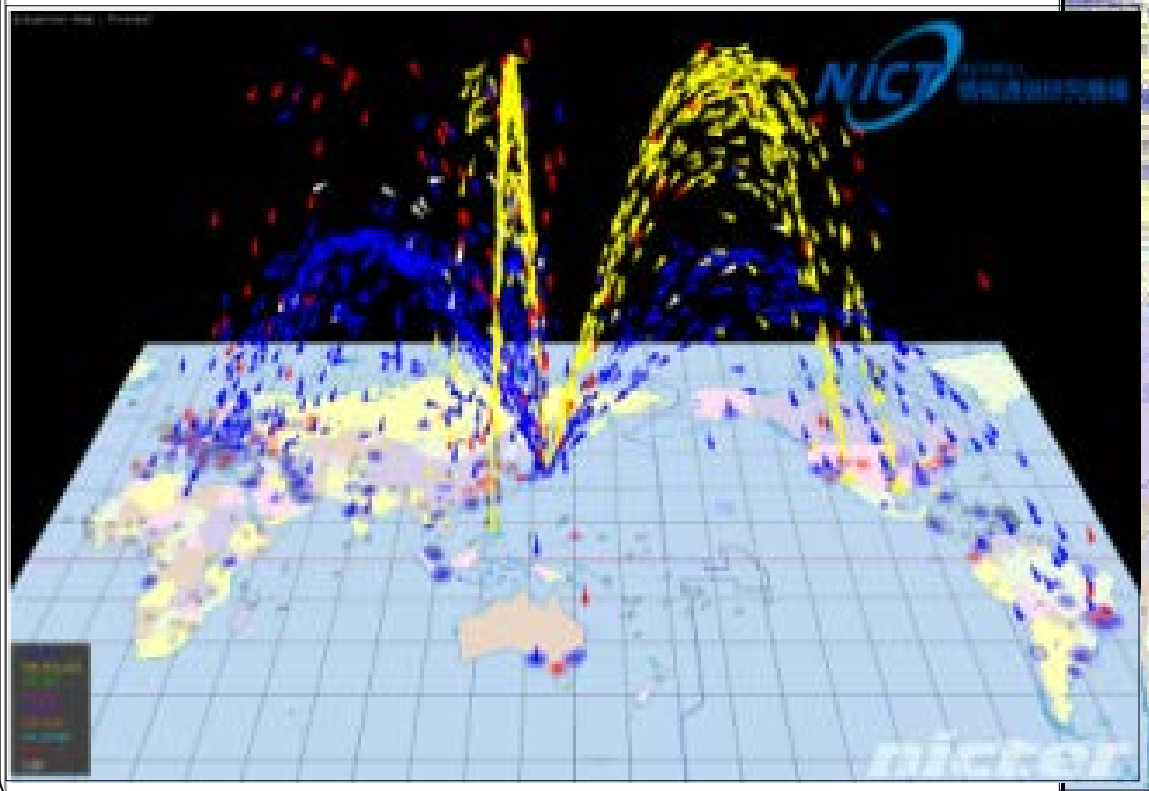
NICTによるサイバー攻撃観測（nicter）

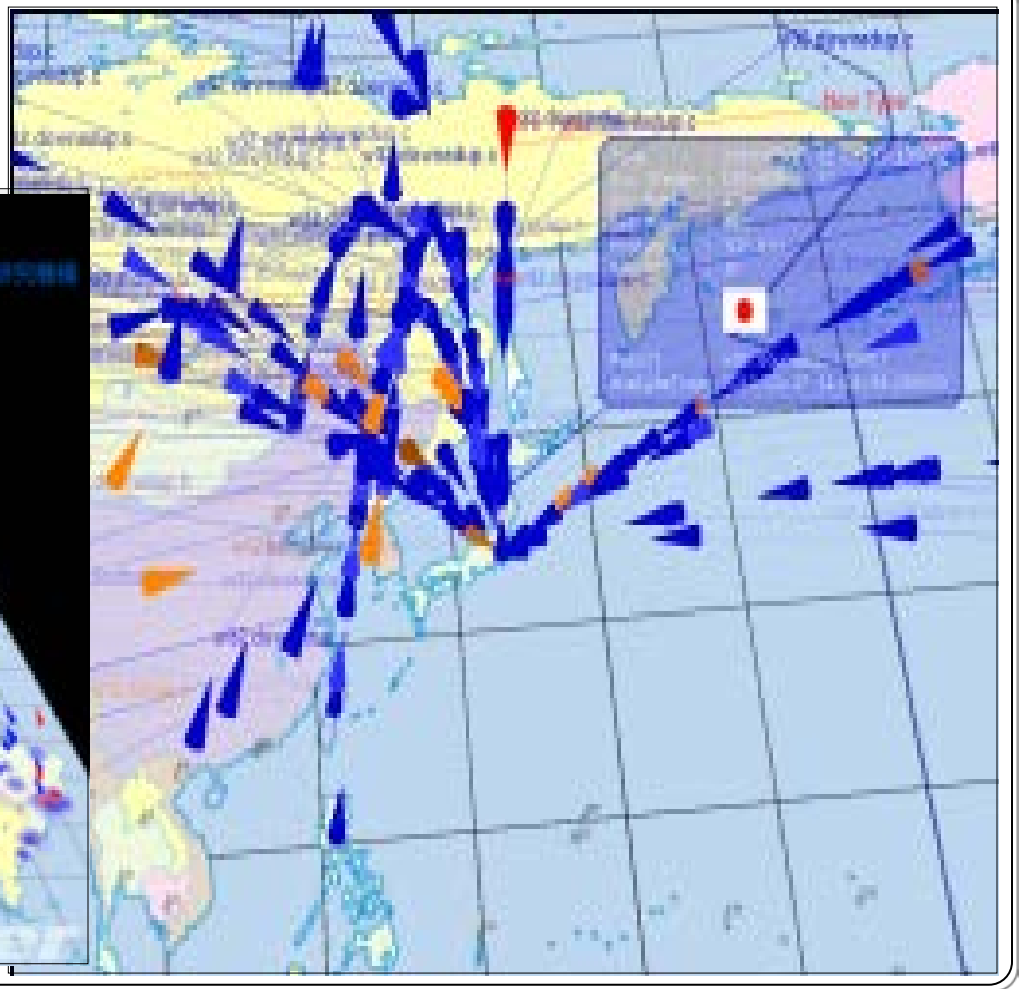
情報通信研究機構（NICT：エヌ・アイ・シー・ティー）では、インシデント分析センター（nicter）により、サイバー攻撃観測・分析網を構築して、サイバー攻撃の状況をリアルタイムで把握し、分析。

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





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。

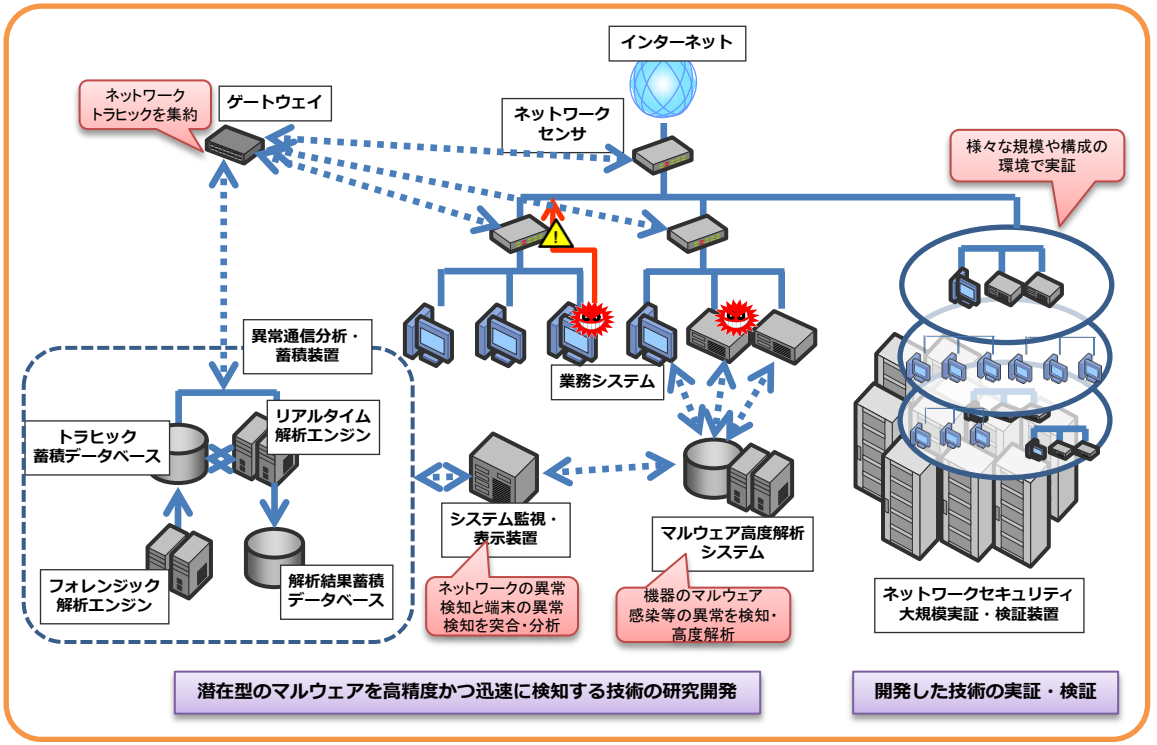
※ マルウェアとは、コンピュータウイルスのような有害なソフトウェアの総称。
潜在型のマルウェアとは、自らの挙動を正常の通信に紛れ込ませ、検知を極めて困難にしているマルウェア。

○ 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

【参考】「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

2012年11月1日に第1回会合を開催。2013年7月を目途に一定の取りまとめを行う予定。2013年4月8日に論点整理を公表。

【参考】パーソナルデータの利用・流通の促進に向けた方策

●ビッグデータを利用する際、プライバシー保護等について不明確な部分が多いため、パーソナルデータを利用する新ビジネスに支障

●個人に関する大量の情報 が集積・利用されることによるプライバシーについての不安

→ 情報の自由な流通とプライバシー保護等の調和に配慮したパーソナルデータの利活用のルールの明確化が必要

平成24年11月から「パーソナルデータの利用・流通に関する研究会」（座長：堀部政男一橋大学名誉教授）を開催して検討

論点整理の概要

○短期的な方向性

基本的な枠組み

・パーソナルデータの利活用の促進と適切な保護の調和が重要
・パーソナルデータの利活用を円滑に進めるため、その適正な取扱いについて信頼性の確保・強化が必要不可欠
・パーソナルデータの利活用に関するルールの明確化が必要

保護されるパーソナルデータの範囲

パーソナルデータの性質に応じた取扱い

✓データの取得の経緯(コンテキスト)や、プライバシー性の高低に応じた（3類型等）、パーソナルデータの取扱いのルール*

パーソナルデータの利活用のルール策定の在り方

✓「マルチステークホルダープロセス」（国、企業、消費者、有識者等、多種多様な関係者が参画するオープンな検討プロセス）によるルールの策定*

パーソナルデータの保護のための関連技術の有用性（匿名化、暗号化等）

パーソナルデータ利活用のルール遵守確保の在り方

✓プライバシーポリシーを契約約款で規定、有識者からなる専門機関の設置*

（*論点）

○中期的な方向性

・国際的に調和の取れた制度整備は不可避。
・国際的には、パーソナルデータの保護は、独立第三者機関であるプライバシーコミッショナーが行っている国が多い。
・制度的な永続性・安定性の確保のためには、個人情報保護法の在り方の見直し等、中期的な取組が必要不可欠。政府全体として速やかな検討が必要。

目次

- はじめに
- 政府全体の取り組み
- 総務省の取り組み
- **おわりに**

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