総務省
MIC Ministry of Internal Affairs and Communications

参考1－1

政府の情報セキュリティ政策の動向

平成２５年３月５日
総　　務　　省
情報セキュリティ対策室

政府の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

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

閣僚が参画

（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）

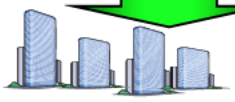
協力

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

重要インフラ事業者　等



政府機関（各府省庁）

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）

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

新たな基本戦略
（2013年夏までに策定）

中長期計画

- 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）
- 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

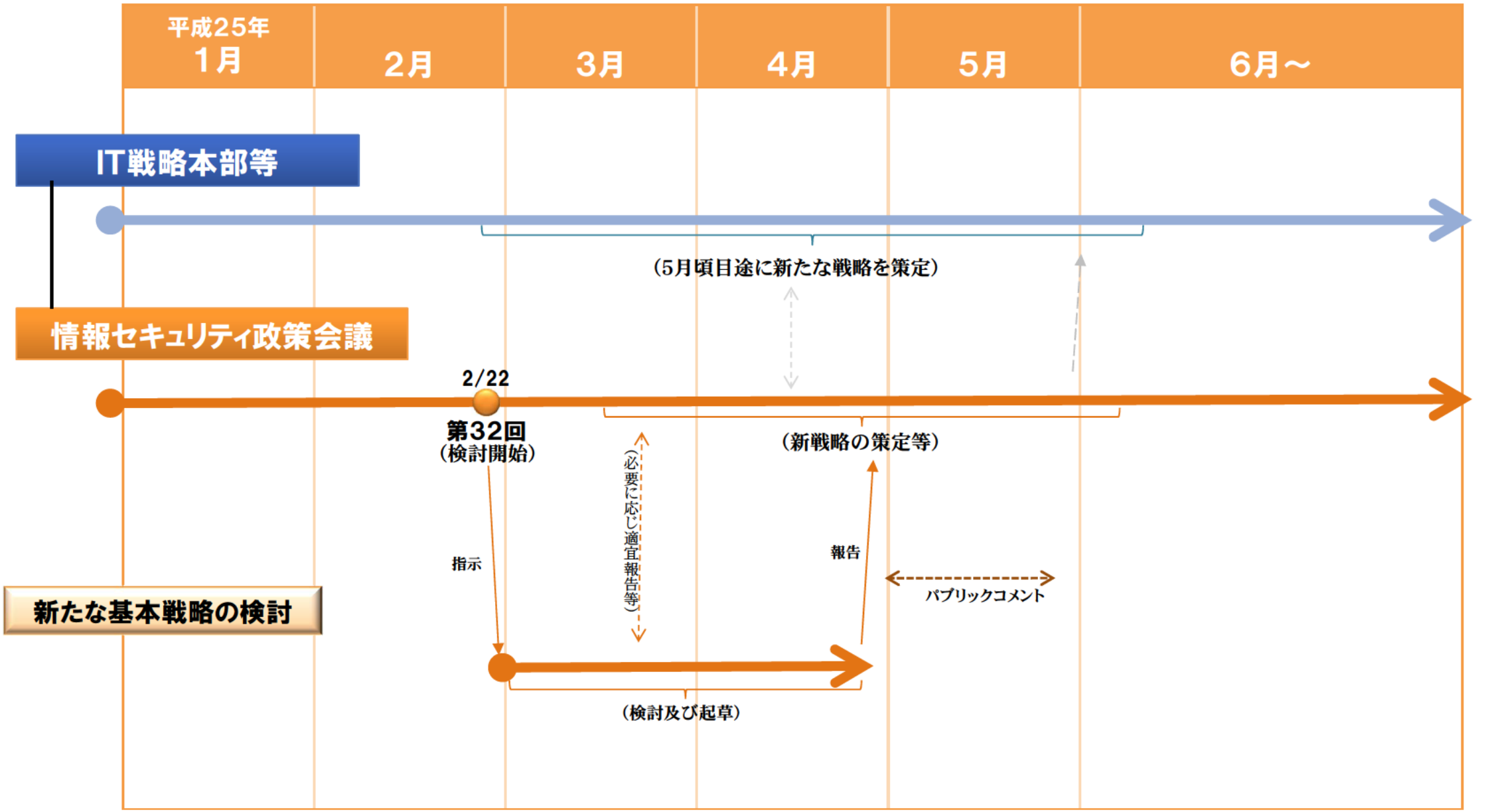
【現行目標】
2020年までに、情報通信技術を安心して利用できる環境（高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」の実現

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＞

「新たな基本戦略」の策定スケジュール



＜第32回情報セキュリティ政策会議資料より作成＞

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）

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)。

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普及啓発活動。
・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普及啓発活動。

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. パーソナルデータの利用・流通の促進

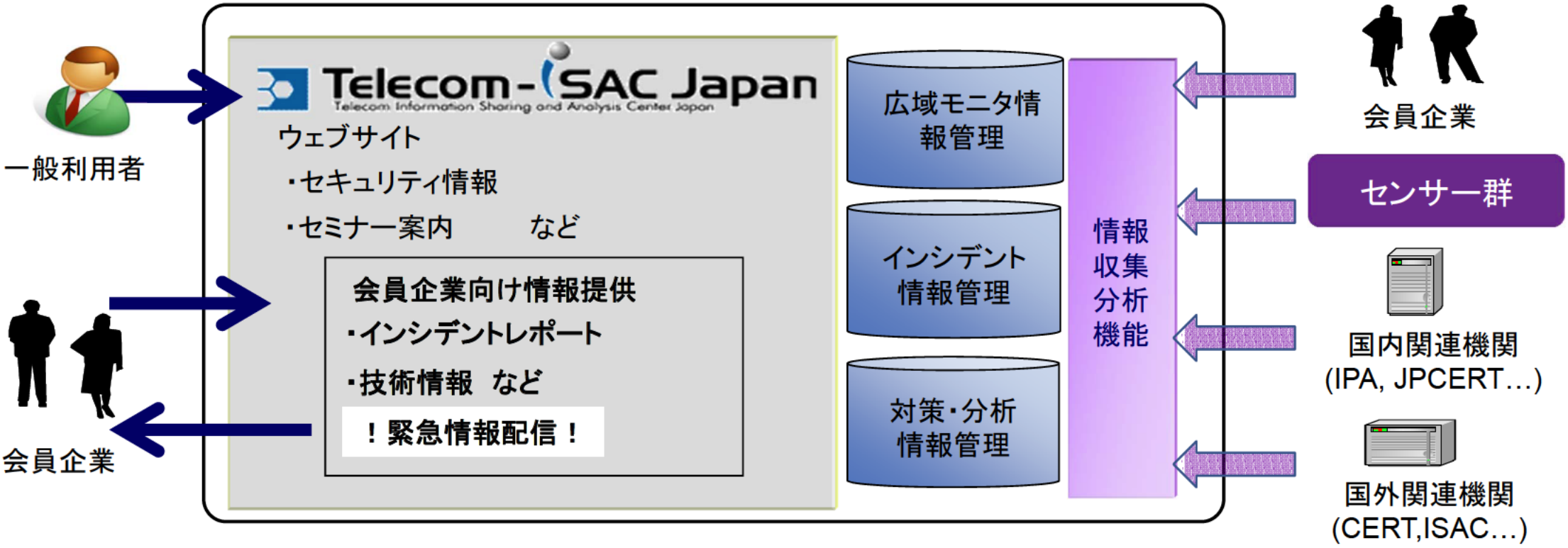
・プライバシー保護等に配慮したパーソナルデータ(個人に関する情報)のネットワーク上での利用・流通の促進に向けた方策について検討するため、「パーソナルデータの利用・流通に関する研究会」を開催。

Telecom-ISAC Japanとの連携

◆国内の主要なインターネットサービスプロバイダ（ISP）により構成

◆情報セキュリティインシデント情報等を収集・分析し、業界内で共有することが目的

共有・分析する情報：　①システムの脆弱性、②対抗策・ベストプラクティス、③サイバー攻撃・犯罪、等



〈正式名称〉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

〈会員企業〉日本電気、エヌ・ティ・ティ・コミュニケーションズ、KDDI、インターネットイニシアティブ、ニフティ、日立製作所、沖電気工業、ソフトバンクBB、東日本電信電話、西日本電信電話、日本電信電話、KDDI研究所、NECビッグローブ、富士通、インターネットマルチフィード、エヌ・ティ・ティ・コムテクノロジー株式会社、エヌ・ティ・ティ・ドコモ、エヌ・ティ・ティ・データ先端技術、ソネットエンタテインメント株式会社

情報セキュリティに関する予算施策（H24補正及びH25当初）

課題

標的型攻撃

昨今、標的型攻撃等の巧妙化するサイバー攻撃により、我が国政府機関、民間企業等において機密情報漏えい等の被害が発生する事態が頻発。

個人のマルウェア感染

個人利用者においても、ウイルス感染の拡大や、オンラインバンキングにおけるID・パスワードの漏えいなどの実被害が発生。

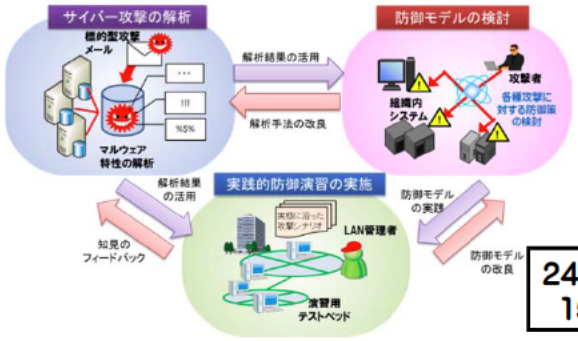
分散型サービス妨害攻撃（DDoS攻撃）

海外を主な発信源とするDDoS攻撃等により、政府機関等のウェブサイトのアクセス障害や改ざん等が頻発。

実証実験

サイバー攻撃解析・防御モデル実践演習

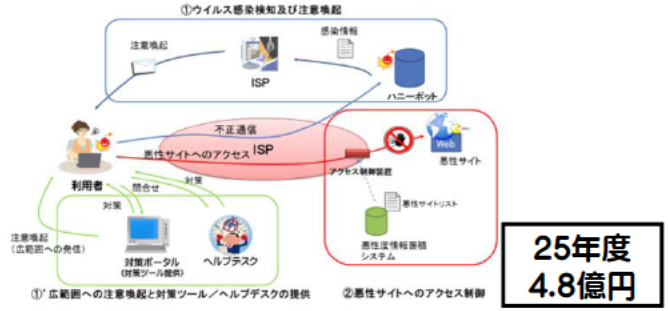
標的型攻撃の解析による実態把握、防御モデルの検討、官民参加型の実践的な防御演習による人材育成を実施。



24年度補正
15.2億円

国民のウイルス感染被害予防に関する実証実験

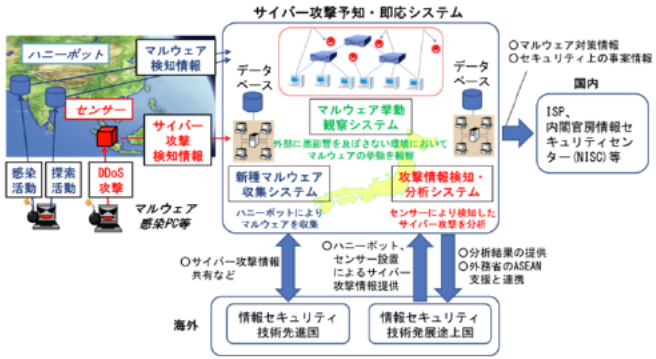
①PCがウイルス感染した個人利用者にISP等を通じて注意喚起。
②個人利用者がウイルス感染元等の悪性ウェブサイトにアクセスしようとした際に注意喚起。



25年度
4.8億円

国際連携によるサイバー攻撃予知・即応技術の研究開発

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を実施。



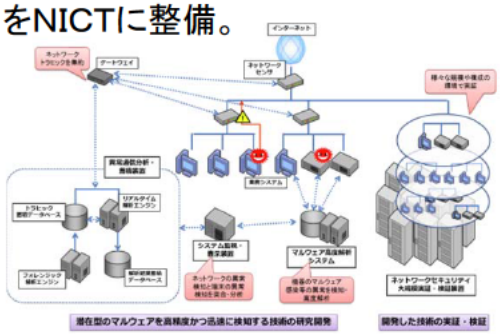
◇ 平成24年３月に、サイバー攻撃の予知のための研究開発の協力について、**米国と合意**。
◇ 平成24年４月に**モルディブ**、平成24年５月に**インドネシア**との間で情報共有を開始。平成25年２月に**タイ**と、連携について合意。
◇ 現在、欧州諸国、マレーシア、シンガポール等と連携に向けて協議中。

23年度　6.3 億円
23年度補正　5.6 億円
25年度　5.8 億円

研究開発

NICT施設整備補助金

潜在型マルウェアの検知技術等、革新的な情報セキュリティ技術の研究開発・実証実験施設をNICTに整備。



24年度補正
100億円

サイバー攻撃の解析・検知に関する研究開発

①サイバー攻撃の存在に気づいた後、攻撃の侵入経路や進行状況を過去に遡って解析する技術の研究開発。
②サイバー攻撃が仕掛けられていることを早期に検出する不正検知技術の研究開発。
③これらの解析・検知を行うために有効なログの取得・縮退方法の研究開発。

25年度
5.5億円

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対策の推進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。（http://www.soumu.go.jp/main_content/000199322.pdf ）

○　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。（http://www.soumu.go.jp/main_content/000199323.pdf ）

「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。

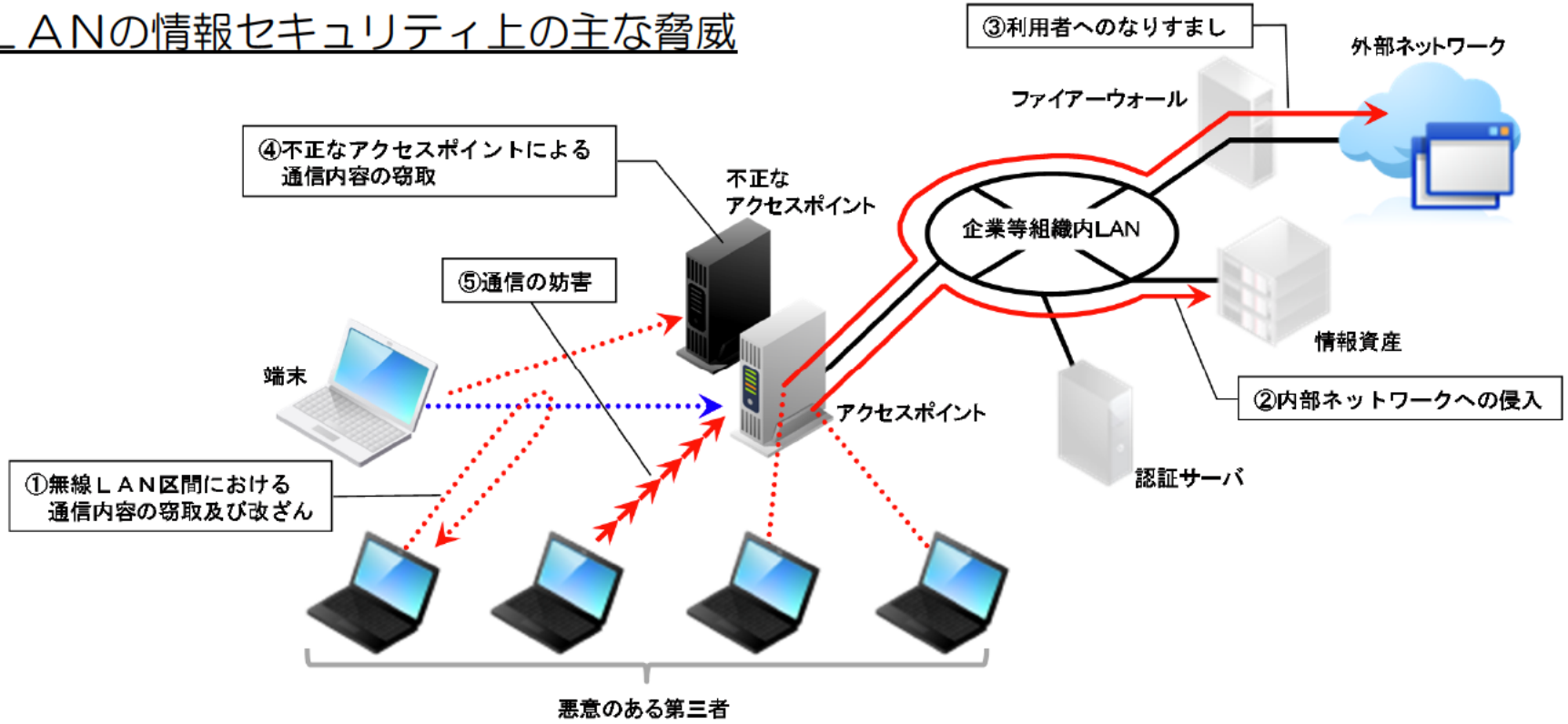
※ SSL（Secure Socket Layer）とは、信頼できるウェブサイトやサーバとの間で、データを暗号化して送受信する方法。SSLが使われていることは、URLが「https」からはじまっていることや、パソコンやスマートフォンのブラウザに「鍵マーク」が表示されることで確認。

無線LANの情報セキュリティ対策の推進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

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は、平成25年3月1日に、「電子政府推奨暗号リスト」（平成15年2月20日公表）を改定した「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」を策定。

◇ 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：
・「CRYPTREC暗号リスト」※の公表。
・暗号技術の安全性等の監視活動及び評価を実施。

※「CRYPTREC暗号リスト」は、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」、「運用監視暗号リスト」から構成される。

※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。

◇ CRYPTREC暗号リストの策定について

○ 暗号に対する解析・攻撃技術の高度化や新たな暗号技術の開発を踏まえ、10年振りにリストを改定。
○ 改定にあたっては、安全性だけでなく、調達の容易性、国産暗号の普及促進といった様々な視点で検討。

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

平成25年3月1日
総務省
経済産業省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するものの一覧。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS[13]
		RSASSA-PKCS1-v1_5[13]
	守秘	RSA-OAEP[13]
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号[152]	3-key Triple DES[13]
	128ビットブロック暗号	AES

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

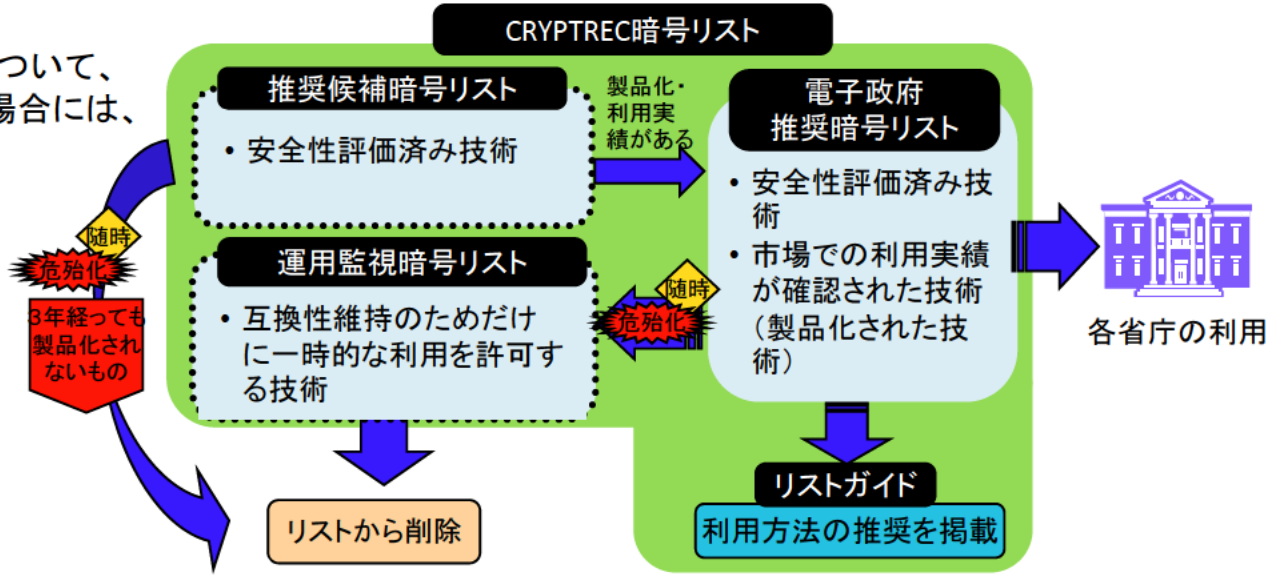
技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM[135]
	64ビットブロック暗号[136]	CIPHERLUNICORN-E
		Hierocrypt-L1
		MISTY1

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5[136][139]
	鍵共有	該当なし
	64ビットブロック暗号	該当なし

CRYPTREC暗号リスト



電子政府推奨暗号リスト改定の流れ

不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）

○「不正アクセス防止対策に関する行動計画」を受け、平成24年2月、警察庁、総務省、経済産業省が共同で不正アクセス禁止法改正法案を国会提出。
○平成24年3月、不正アクセス禁止法改正法が成立。同年5月1日施行。

改正前の法律概要

（1）不正アクセス行為※の禁止・処罰

※識別符号（ID・パスワード等）により利用が制限・管理されている特定電子計算機（ネットワークに接続されたコンピュータ）に対し、ネットワークを経由して他人の識別符号を入力すること等により、本来は制限されている利用を可能にする行為

（2）不正アクセス行為を助長する行為の禁止・処罰

（3）アクセス管理者による防御措置の努力規定

（4）国及び都道府県公安委員会によるアクセス管理者への援助等

主な改正点

（1）フィッシング行為※の禁止・処罰 新設

※企業等になりすまして偽のウェブサイトを構築する、偽のメールを送信する等の手段により、ＩＤ・パスワードをだまし取る行為。

（2）ID・パスワードの不正取得・不正保管の禁止・処罰 新設

（3）ID・パスワードの提供行為の禁止・処罰範囲の拡張 改正

ID・パスワードを提供する際、これらの利用先を特定しなくても可罰対象に改正。

（4）不正アクセス行為に係る法定刑の引上げ 改正

○不正アクセス行為：
　１年以下の懲役又は50万円以下の罰金　→　３年以下の懲役又は100万円以下の罰金
○相手方に不正アクセス目的があることを知ってID・パスワードを提供する行為：
　30万円以下の罰金　→　１年以下の懲役又は50万円以下の罰金

（5）アクセス制御の高度化に係る事業を行う団体への国の援助 新設

アクセス管理者の支援団体(現在、日本セキュリティオペレーション事業者協議会など)に対し、不正アクセスに関する動向などの情報提供等を行う努力義務。

パーソナルデータの利用・流通に関する研究会

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。