第2節　情報セキュリティと安心・安全な利用

ICTの普及・発達により、国民生活、社会経済、安全保障・治安確保等のあらゆる活動がサイバー空間に依拠している中、サイバー空間を対象とした攻撃は、近年、高度化・複雑化するとともに、愉快犯から経済犯・組織犯的なものに移行しており、社会的な脅威が高まっている。また、スマートフォン、タブレット端末等の急速な普及、ソーシャルメディア、クラウドサービス等の利用の拡大に伴い、これらを狙ったマルウェア（malware）*1の増加など、新たな脅威も表面化しているところである。

今後、ICTの更なる高度化及び利活用の進展により、サイバー攻撃の被害の深刻化及び広域化が懸念されるところであり、このような情報セキュリティ上の脅威は、我が国の経済活動の阻害要因及び国家の安全保障の脅威となることから、安心・安全な情報通信ネットワークの確保に向け、官民一体となった対策の強化が必要となっている。本節では、情報セキュリティをめぐる動向として、最近の脅威の動向や特徴的な事例について紹介するとともに、諸外国及び我が国における情報セキュリティに係る政策動向について紹介する。また、情報セキュリティに係る利用者意識について、6か国（日本・米国・英国・フランス・韓国・シンガポール）の比較調査を行ったところ、その結果についても併せて紹介する。

1　高度化・複雑化するサイバー攻撃

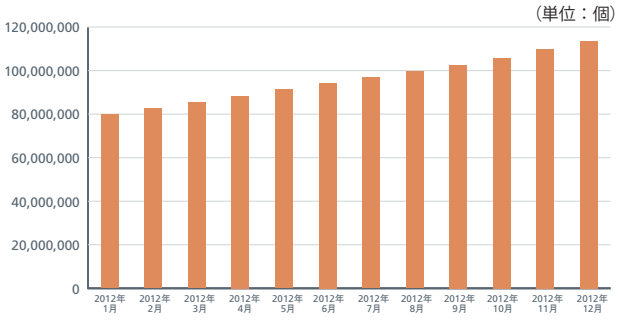
（1）情報セキュリティに関する脅威の動向

現在、情報セキュリティベンダのMcAfee社のデータベースに登録されるマルウェアの種類は、1月あたり約300万検体のペースで増加している（図表3-2-1-1）。また、近年発生した情報漏えい／侵害事例の原因としてマルウェア感染、ハッキング等の外部からの攻撃によるものが高い割合を占める傾向にある（図表3-2-1-2）など、我々を取り巻く情報セキュリティに関する脅威はますます深刻化している。

近年のサイバー攻撃は、国家機密を標的とした攻撃から個人の情報・金銭を標的とした攻撃まで多岐にわたっており、政府機関及び企業のみならず、スマートフォン等の普及により、個人においても一層の情報セキュリティ対策を事業者任せではなく、利用者自身で講じることが求められる時代になったといえる。

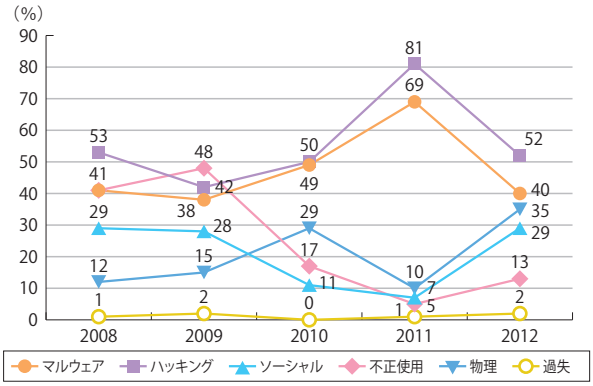
以下、図表3-2-1-3において、2012年（平成24年）から2013年（平成25年）にかけて国内外で発生した主な最近のサイバー攻撃から特徴的な事例を紹介する。

図表3-2-1-1　マルウェア検体の増加状況（データベースに登録されたマルウェア検体の合計）



（出典）McAfee社脅威レポート（2012年第4四半期）

図表3-2-1-2　脅威の種類別のデータ漏えい／侵害事例



※合計値が100%を超えるのは、原因が複数にまたがる事例が多く存在するため。
＊2010年の「過失」は、厳密には「1%未満」である。

（出典）Verizon社　2013 DATA BREACH INVESTIGATIONS REPORT

＊1　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

図表3-2-1-3　2012年4月～2013年3月の間に明らかになった主なサイバー攻撃

時期	業種（国）	攻撃概要
2012年4月	政府等（中国）	「アノニマス」を名乗るハッカー集団が中国を攻撃の標的に定め、数百に及ぶウェブサイトを改ざんした。
2012年4月	個人（日本）	スマートフォンに登録された電話番号等を無断で外部に送信するアプリが出回り、これまでに数百万人の個人情報が流出したおそれがあることが判明した。
2012年4月	企業（日本）	顧客情報等の様々な情報を管理しているコンピューターネットワークに対し、サイバー攻撃を受けていたことが判明した。
2012年5月	政府（日本）	独立行政法人のウェブサイトの一部が不正アクセスにより改ざんされた。
2012年6月	政府（日本）	独立行政法人の業務用パソコン19台がマルウェアに感染し、外部に情報を送った可能性があることが判明した。
2012年6月	地方自治体（日本）	地方自治体のTwitterアカウントが乗っ取られ、悪意の第三者がログインしていることが判明した。
2012年6月	政府等（日本）	「アノニマス」を名乗るハッカー集団が日本の政府機関等のウェブサイトに対して、DDoS攻撃やホームページの改ざんを行った。
2012年6月～9月	地方自治体等（日本）	大量殺人予告や爆破予告が地方自治体のサイトに書き込まれたりメールで送り付けられた。その後、マルウェアに感染したパソコンが外部から遠隔操作された結果であることが判明した。
2012年7月	政府（日本）	中央省庁の職員が使用するパソコン123台がマルウェアに感染し、外部サイトに向けて不審な通信を行っていたことが判明した。
2012年7月	企業（韓国）	韓国の通信会社のネットワークがハッキングされ、携帯電話契約書877万人の個人情報が流出したことが判明した。
2012年8月	企業（サウジアラビア）	石油会社が、およそ30,000台にのぼる同社のワークステーションがサイバー攻撃の被害を受けたと認める声明を出した。
2012年9月	政府等（日本）	日本の公的機関や企業のウェブサイトがサイバー攻撃を受け、計19のサイトで閲覧障害や改ざんが確認された。
2012年10月	大学（各国）	「GhostShell」を名乗るハッカー集団が、日本の5大学を含む世界の有力100大学のサーバから盗んだ情報12万件を、インターネットに掲載したと公言した。
2012年10月	金融（日本）	各銀行のインターネットバンキングのウェブサイト上で、顧客の暗証番号などの入力を求める偽の画面が表示され、不正送金が行われるケースが判明した。
2012年11月	企業（米国）	テレビ局のウェブサイトが「pyknik」と称するハッカーにより侵入され、コンテンツが改ざんされた。
2012年11月	金融（日本）	生命保険会社を退職した社員や代理店の保険販売員が同社のシステムに不正にアクセスしていたとの発表があった。
2012年11月	政府（日本）	独立行政法人のコンピューターがマルウェアに感染し、外部コンピューターに向けてデータを送信したことが判明した。
2012年11月	国際機関	国際機関のサーバが何者かにハッキングされ、同機関とともに働いている専門家の連絡先などの情報が盗まれたと明らかにした。
2012年12月	企業（日本）	製造業で業務用パソコン4台が新種のマルウェアに感染したとの発表があった。
2012年12月	政府（日本）	独立行政法人が保有する端末がマルウェアに感染し、外部のサイトへ通信が行われていた旨発表した。
2012年12月	企業（日本）	マスコミの社内システムが不正アクセスを受け、同社が試験的に作成したデータが一時、閲覧できる状態にあった。
2012年12月	企業（日本）	マスコミの社員が利用するパソコンがマルウェアに感染し、社員のメールの一部が外部に流出した可能性があると発表した。
2013年1月	政府（日本）	中央省庁の職員が使用するパソコンがサイバー攻撃を受け、機密文書が外部に流出した疑いがあることがわかった。
2013年1月	政府（米国）	「NullCrew」を名乗るハッカー集団が、政府機関などのウェブサイトに不正アクセスした。
2013年1月	企業（日本）	企業のウェブサイトの一部に不正アクセスがあり、会員約47万人分の個人情報を改ざんされたと発表した。
2013年1月	政府（日本）	独立行政法人が運用している ウェブサイトが外部からの不正アクセスによるサイバー攻撃を受け、一部のページが改ざんされた。
2013年1月	地方自治体（日本）	地方自治体でウェブサイトの更新に必要なIDとパスワードが何らかの方法で盗まれ、海外のサーバーから不正アクセスを受けた。
2013年1月	政府（米国）	政府機関のウェブサイトに対してアノニマスがサイバー攻撃を行った。
2013年1月	企業（米国）	マスコミ各社が、中国からサイバー攻撃を受け続けていた旨、相次いで公表した。
2013年1月	政府（日本）	中央省庁のパソコンからインターネット上の外部サーバへの不審な通信が確認され、パソコンから文書が流出した疑いがあることが判明した。
2013年2月	企業（米国）	Twitterで利用者情報を狙った不正アクセスが検出された。攻撃者はおよそ25万人分の利用者のメールアドレス、セッショントークン、暗号化したパスワードにアクセスした可能性があることが判明した。
2013年2月	政府（米国）	政府機関のサーバ14台とワークステーション20台が不正侵入され、職員数百人の個人情報が流出した。
2013年2月	政府（米国）	政府機関がサイバー攻撃を受け、個人情報が流出した。
2013年2月	企業（日本）	企業のサーバおよびパソコン端末17台がマルウェアに感染し、個人情報を含む営業情報と関連する技術情報が外部に漏えいした可能性があることが判明した。
2013年3月	企業（米国）	企業は外部からサーバに不正アクセスを受け、利用者のIDやパスワード、メールアドレスなどが盗まれたおそれがあると発表した。
2013年3月	企業（日本）	電子商取引サイトが不正アクセスを受け、最大1万2036件のクレジットカード情報が流出した可能性があると発表した。
2013年3月	政府（日本）	中央省庁が運営するウェブサイトが改ざんされた。閲覧者のパソコン内の情報が盗まれた可能性があるとのこと。
2013年3月	企業（韓国）	銀行や放送局など複数のコンピュータネットワークがサイバー攻撃とみられる攻撃を受けた。
2013年3月	地方自治体（日本）	地方自治体で学校や文化施設など計53のウェブサイトを管理するサーバが外部から改ざんされた。
2013年3月	民間（欧州）	非営利団体のウェブサイトにDDoS攻撃が行われ、同団体はウェブサイトを停止した。

（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

ア　国家・企業の機密情報を狙った標的型攻撃

2012年（平成24年）も前年に引き続き、標的型攻撃は情報セキュリティ上の大きな脅威となっている。標的型攻撃とは、一般に情報窃取等を目的として攻撃対象に潜入し、情報システム内部から有益と思われる情報を窃取するものである。一口に標的型攻撃と言っても、単純に電子メールにマルウェアを添付したものから、巧妙に攻撃シナリオを練ったもの（例えば、攻撃者が攻撃対象者との間で電子メールのやりとりを数回行い、相手の警戒が解けた頃を見計らってマルウェアを添付した電子メールを送信するといった、ソーシャルエンジニアリングを活用した手法など）まで、多種多様である。2012年度（平成24年度）には、我が国の独立行政法人において、職員のパソコンがマルウェアに感染した結果、当該パソコン内に保存されていた情報が外部に漏えいしたおそれがあることが明らかになったほか、中央省庁においても外部への情報漏えいが疑われる通信が確認されたところである。

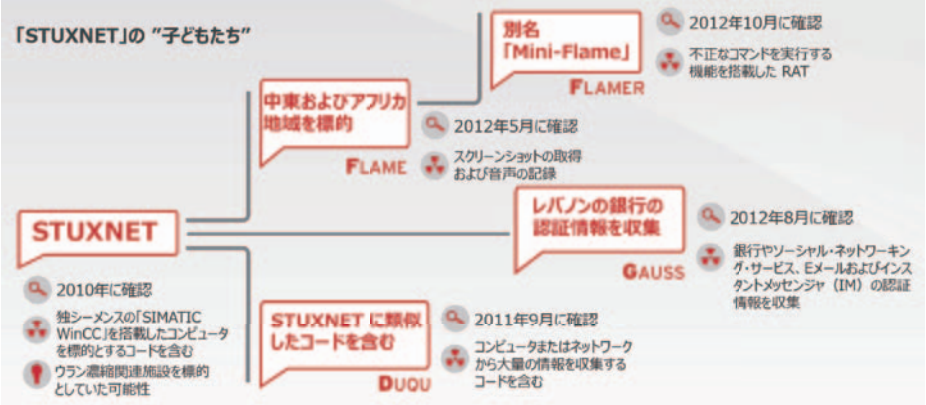
また、民間企業等における標的型攻撃の被害や脅威についても報じられており、通信、電力等の重要インフラ分野も例外ではない。制御系システムを狙った不正プログラムの代表例として、2010年（平成22年）にイラ

ンにおいて確認された「Stuxnet」[*2]があるが、それと関連している不正プログラムは2012年（平成24年）も確認されており、官民及び国内外を問わず、標的型攻撃の脅威に引き続きさらされている状況にある（図表3-2-1-4）。

なお、情報セキュリティベンダのシマンテック社が2013年（平成25年）4月に公表したレポートによると、2012年（平成24年）に発生した標的型攻撃は一日平均116件と前年より大幅に増加している。ただし、2012年（平成24年）上半期までは件数が伸長傾向だったのに対し、下半期には沈静化している状況にある。

また、攻撃対象を従業員規模別及び役職別でみると、より小規模の企業、研究開発及び営業等の機微な情報を取り扱う部署を標的とする傾向にあることがわかる（図表3-2-1-5）。

図表3-2-1-4　Stuxnetと関連する不正プログラム

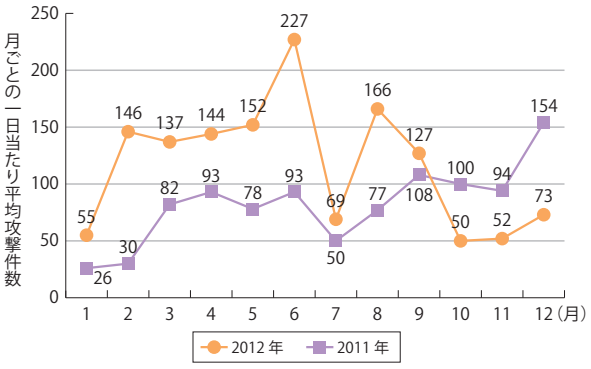


（出典）トレンドマイクロ

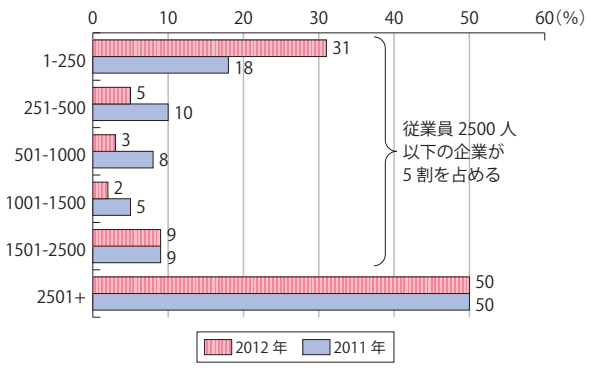
図表3-2-1-5　世界における標的型攻撃の増加

●標的型攻撃の増加　1日当たり平均82件（2011年）→116件（2012年）

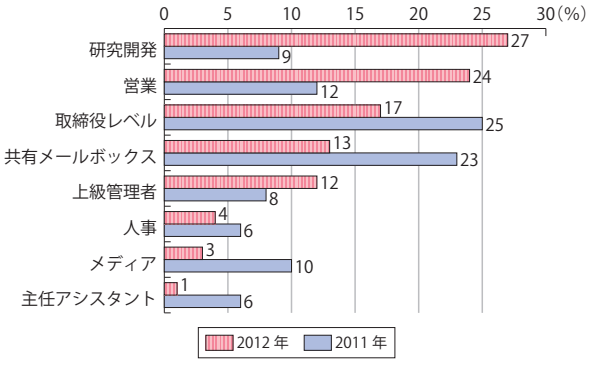
●月ごとの標的型攻撃の件数（1日当たり平均）



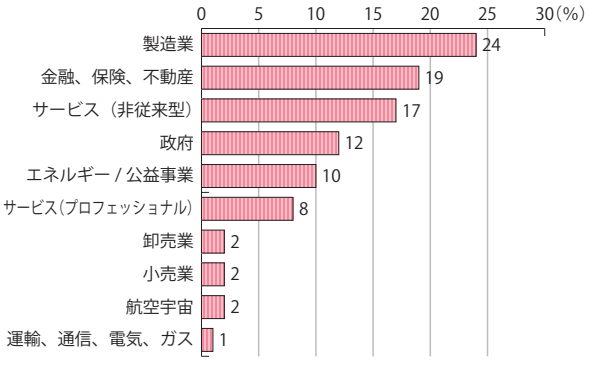
●従業員規模別の標的型攻撃の比率



●役職等別の標的型攻撃の比率



●部門別の標的型攻撃の比率（2012年）



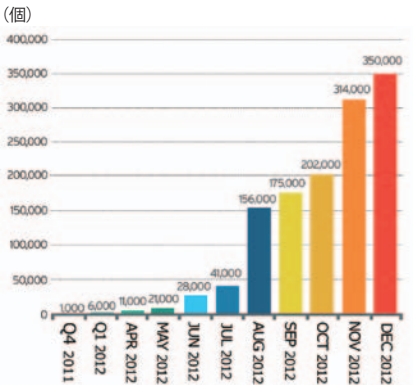
（出典）シマンテックインターネットセキュリティ脅威レポート第17号及び第18号より作成

＊2　Stuxnet（スタックスネット）とは、ドイツのシーメンス社が開発した産業用機器の制御システムを攻撃対象とし、インターネット及びUSBフラッシュメモリー等を媒介して感染活動を行うマルウェア。物理的な機器破損・稼動停止を引き起こした初めてのマルウェアであるとされており、実際にイランの原子力施設における1,000台近くの遠心分離機がStuxnetの侵入を受けて稼動停止に陥った。Stuxnetは、Windowsの未知のぜい弱性を複数利用しており、コードの分量が一般的なマルウェアの数十倍に及ぶなど、複雑・高度な技術によって作られているとされている。

イ　スマートフォン等を標的としたマルウェアの急増

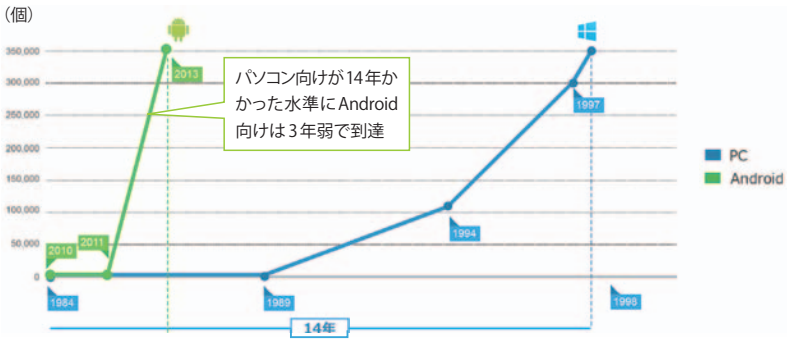
スマートフォン、タブレット端末の普及に伴い、これらを標的としてマルウェアが急速に増加している。情報セキュリティベンダのトレンドマイクロ社が2013年（平成25年）2月に公表したレポートによれば、2012年（平成24年）末には、Android端末向けマルウェアは累計で35万個に達した（図表3-2-1-6）。これは、パソコン向け不正マルウェアが約14年かけて到達した数を、3年かからずに到達したことになる（図表3-2-1-7）。

図表3-2-1-6　Android向けマルウェアの増加



（出典）トレンドマイクロ

図表3-2-1-7　Android及びパソコンにおけるマルウェアの増加



（出典）トレンドマイクロ

2012年（平成24年）4月には、「the Movie」という文字を含むスマートフォン向けアプリが、電話帳データを収集していると大きく報道された。動画コンテンツを閲覧できることを謳い文句に、Google社が運営する公式マーケット上で配布したところ、多くのスマートフォンの利用者がアプリをインストールし、その結果、約1,000万件の個人情報が窃取されたといわれている。

また、ウェブサイトの閲覧中に年齢認証等を求められ、クリックすると会員登録画面が表示され高額な利用料金を請求される「ワンクリック詐欺」についても、スマートフォン等を標的としたものが登場している。利用者の不安をあおり、画面に表示された連絡先に問い合わせるよう仕向けることにより、当該利用者の個人情報を窃取し、執拗な料金請求等につながるといった被害が発生している。

スマートフォン等は従前の携帯電話とは異なり、端末内には多種多様なデータを格納しているほか、最近では、個人の私物端末を業務に持ち込んで利用するBYOD（Bring Your Own Device）の浸透により、利用者本人だけでなく知人、所属する組織、取引先等に関係する情報まですべて窃取されるおそれがあるなど、新たな情報セキュリティ上の脅威となっている。

ウ　ソーシャルメディア上における脅威

FacebookやTwitterに代表されるソーシャルメディアの急速な普及に伴い、これらの利用者を標的とした攻撃も登場している。例えば、Facebookの「いいね！」ボタンを悪用することで、プライバシー情報の非公開設定を公開設定に変更されるなどのクリックジャック攻撃やTwitterの公式アカウントの乗っ取り、偽のアプリケーションの配布など、ソーシャルメディアの機能を悪用した攻撃が相次いで出現している。

エ　いわゆる「ハクティビズム」の我が国での顕在化

政治的な活動、企業への抗議活動等の手段としてサイバー攻撃を行う、いわゆる「ハクティビズム」も活発となっている。「インターネットの世界」の自由を掲げ、規制反対の立場からサイバー攻撃を行う集団「アノニマス」は、その代表例であり、海外の政府機関、企業等に対し、DDoS（Distributed Denial of Service）攻撃*3、個人情報の漏えいにつながるサイバー攻撃等を行っている。2012年（平成24年）6月には我が国の政府機関等に対し、DDoS攻撃及びウェブサイトの改ざんを行った。攻撃と前後して、「アノニマス」は改正著作権法*4の内容に抗議し、政府機関等へ攻撃を行う旨の声明をインターネット上に掲載するなど、我が国においても「ハクティビズム」がクローズアップされた年でもあった

オ　遠隔操作型マルウェアによる攻撃

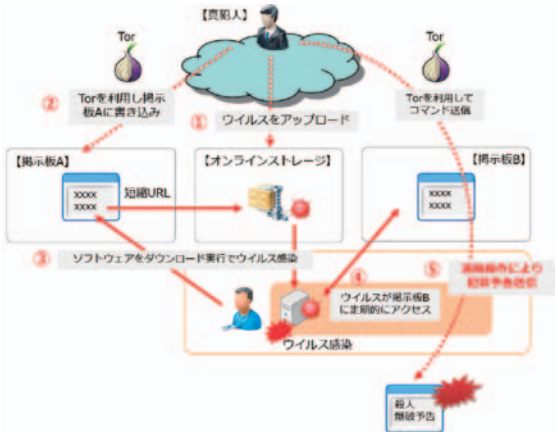
2012年（平成24年）に個人を標的としたマルウェアで大きな注目を集めたのが、いわゆる「遠隔操作型マルウェア」事件である。本件では、マルウェアに感染した第三者のパソコンを遠隔操作することにより、公共機

＊3　分散型サービス妨害攻撃。多数のパソコン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、当該あて先のネットワークやサーバを動作不能にする攻撃。
＊4　著作権法の一部を改正する法律（平成24年法律第43号）

関のウェブサイト及び掲示板に犯行予告を書き込んだものであり、マルウェアに感染したパソコンの所有者が逮捕される結果となった。

本件では、掲示板への書込み及びマルウェアに感染したパソコンに対する命令の送信等について、発信元を隠ぺいする匿名化技術[*5]が使われていることが特徴であり、送信元及び通信経路を追跡することが非常に困難な要因となっている（図表3-2-1-8）。

図表3-2-1-8　遠隔操作ウイルス事案の構図



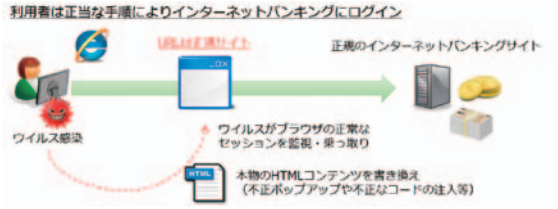
（出典）「個人を狙ったウイルスの最新動向」（ITUジャーナル　2013年3月号）

カ　インターネットバンキングを狙った情報窃取

個人を標的とした攻撃でもう一つ特徴的な事例として、利用者がインターネットバンキングサイトにログインした際、偽装したポップアップ画面を表示し、第二暗証番号、秘密の質問等を窃取するものがある。その結果、一部の金融機関においては、顧客の口座から別口座に対して不正送金・出金が行われていたことが確認されている。

従来のフィッシングとは異なり、マルウェアにより利用者が正当な手順でインターネットバンキングサイトにログインしたにも関わらず、不正なポップアップが表示される点が本事例の特徴である（図表3-2-1-9）。

図表3-2-1-9　インターネットバンキング情報窃取事案で取られた手法



（出典）「個人を狙ったウイルスの最新動向」（ITUジャーナル　2013年3月号）

（2）諸外国における情報セキュリティに係る最新動向

ア　米国における動向

米国では、2013年（平成25年）2月12日、オバマ大統領は「重要インフラのサイバーセキュリティ強化に関する大統領令（Executive Order：Improving Critical Infrastructure Cybersecurity）」[*6]への署名を行った。命令には、サイバー攻撃に係る情報の共有を軍需産業からすべての重要インフラ事業者に拡大する手続きを確立することや重要インフラに対する情報セキュリティ上のリスクを軽減する枠組の策定等が盛り込まれている（図表3-2-1-10）。

また、同日の一般教書演説[*7]において、オバマ大統領は、「外国による企業機密の窃取や、電力、金融、航空制御システムへの攻撃の発生など、国家安全保障と経済にとっての本当の危機に直面していること」、「情報共有の強化等に関する新しい大統領令に署名したが、それにも関わらず、ネットワークの強靱化と攻撃の阻害を強化するためには、サイバーセキュリティを強化する法整備が必要である」とした。

図表3-2-1-10　重要インフラのサイバーセキュリティの強化に関する米大統領令の概要

【基本方針】（第1条関係）
国家の重要インフラのセキュリティの向上や、プライバシーの保護を促しつつイノベーションや経済成長を起こすサイバー空間の維持。

【情報共有の促進】（第4条関係）
- 政府と民間セクターが共有するサイバー攻撃情報の量、適時性、質を向上させなければならない。
- 司法長官、国土安全保障長官、国家情報長官は、標的となっている企業を特定するレポートを適時に作成するためのガイドラインを発行。
- 国土安全保障長官は、「強化されたサイバーセキュリティサービスプログラム」（政府からの機密情報も含めた、悪意のあるサイバー攻撃の情報共有を図る自発的プログラム）を軍需産業から全ての重要インフラ事業者に拡大する手続を確立。

【プライバシーへの配慮】（第5条関係）
- 本命令に基づく活動は、プライバシーと市民の自由権が確保しつつ、実施。

【重要インフラに対するサイバーリスクを減らすための基本枠組（Cybersecurity Framework）】（第7条・第8条関係）
- 商務長官は、米国標準技術研究所（NIST）に対して、重要インフラへのサイバーリスクを軽減する枠組（Cybersecurity Framework）を策定するよう命令。
- NIST所長はパブリックコメントを経て、大統領命令から240日以内に暫定版を公表し、1年以内に最終版を公表。

【最もリスクにさらされている重要インフラの特定】（第9条関係）
国土安全保障長官は、サイバーセキュリティ上の大惨事を招く可能性のある重要インフラを特定し、事業者へ通知。

【基本枠組の採択】（第10条関係）
重要インフラを所管している連邦機関は、Cybersecurity Frameworkの暫定版を参照し、現行のサイバーセキュリティに関する義務付けが十分か判断。不十分である場合は、必要な措置を実施。

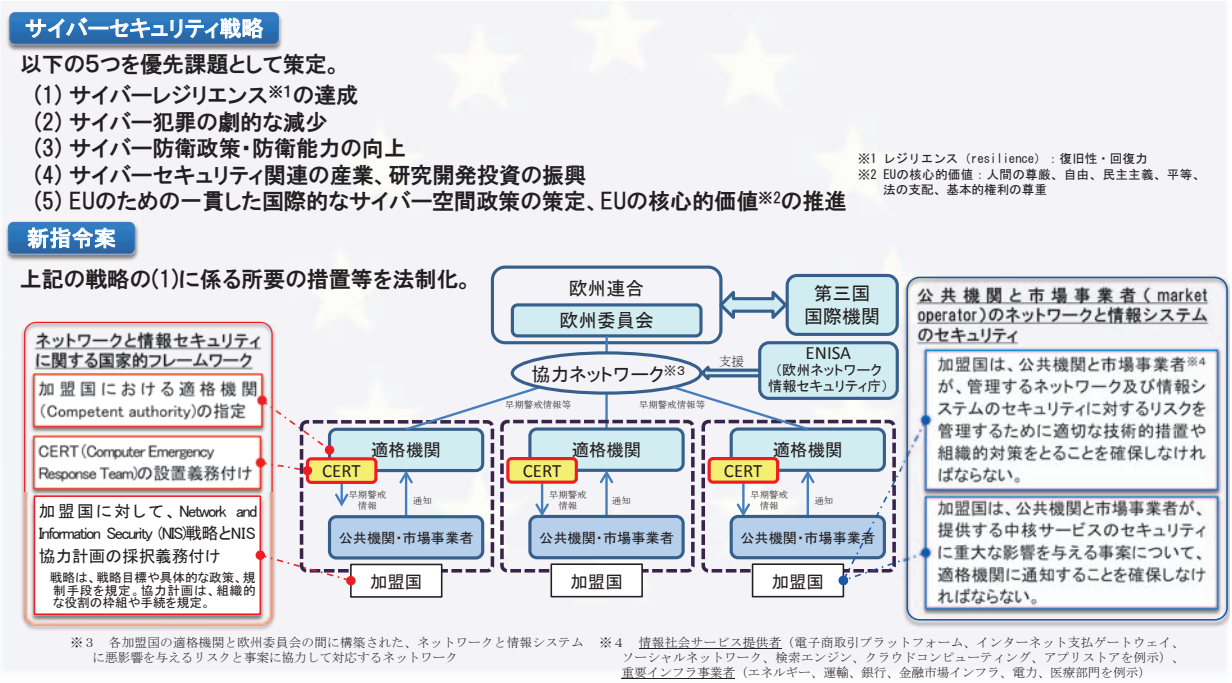
（出典）米国政府公表資料より作成

＊5　Tor（The Onion Router）と呼ばれる接続経路の匿名化を行うフリーのソフトウェアを利用していたとされる。Torは、無作為に選ばれた複数の中継ノードを経由してあて先との通信を行うが、中継ノード上にログを残す機能がない、出口以外の通信路が暗号化される、一定時間ごとに通信経路も変更されるなどの特徴より、発信者の特定は困難となっている。
＊6　http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
＊7　http://www.whitehouse.gov/state-of-the-union-2013

イ　EUにおける動向

2013年2月7日に欧州委員会通信ネットワーク・コンテンツ・技術総局及び内務総局は、欧州連合外務・安全保障政策上級代表と合同で、サイバーセキュリティ戦略及びネットワーク・情報セキュリティに関する指令案*8を公表した（図表3-2-1-11）。

図表3-2-1-11　欧州委員会サイバーセキュリティ戦略及び新指令案の概要



（出典）欧州委員会公表資料より作成

同戦略では、サイバー攻撃への対応に関するEUの包括的なビジョンとして、①サイバーレジリエンスの達成、②サイバー犯罪の劇的な減少、③サイバー防衛政策・防衛能力の向上、④サイバーセキュリティ関連の産業、研究開発投資の振興、⑤EUのための一貫した国際的なサイバー空間政策の策定、EUの核心的価値の推進、を優先的な課題として示している。また、指令案では、サイバーレジリエンスの達成のために必要な措置の法制化を行っている。

なお、英国では、サイバーセキュリティに係る情報を官民で豊富かつ迅速に共有するための枠組として、「サイバー・セキュリティ情報共有パートナーシップ（CSIP：Cyber Security Information sharing Partnership）」を立ち上げることを2013年3月に発表した*9。

*8　http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
*9　http://www.chathamhouse.org/sites/default/files/home/chatham/public_html/sites/default/files/270313maude.pdf

2 情報セキュリティに係る利用者の意識

総務省では、情報セキュリティに係る利用者の意識について、各国で違いがあるか実態を把握するため、日本・米国・英国・フランス・韓国及びシンガポールの利用者を対象としたアンケート調査*10を実施した。また、日本国内については、毎年実施している通信利用動向調査においても、情報セキュリティに係る設問を設けているところ、これらの結果を基に利用者の意識について分析を行った。

我が国の利用者の傾向としては、①情報セキュリティの被害に遭った経験はそれほど高くないものの、インターネット利用に対する不安意識は高い。②インターネット上の脅威（マルウェア、フィッシング、架空請求等）に関する知識も有しているが、特定の脅威を念頭に置いたものではなく漠然としており、そのためか、一定の情報セキュリティ対策はスマートフォンを含めて実施しているものの、それだけで不安感を払拭するには至らず、また、情報セキュリティに関するリテラシーも十分には得られていないと感じている、といった結果が得られた。

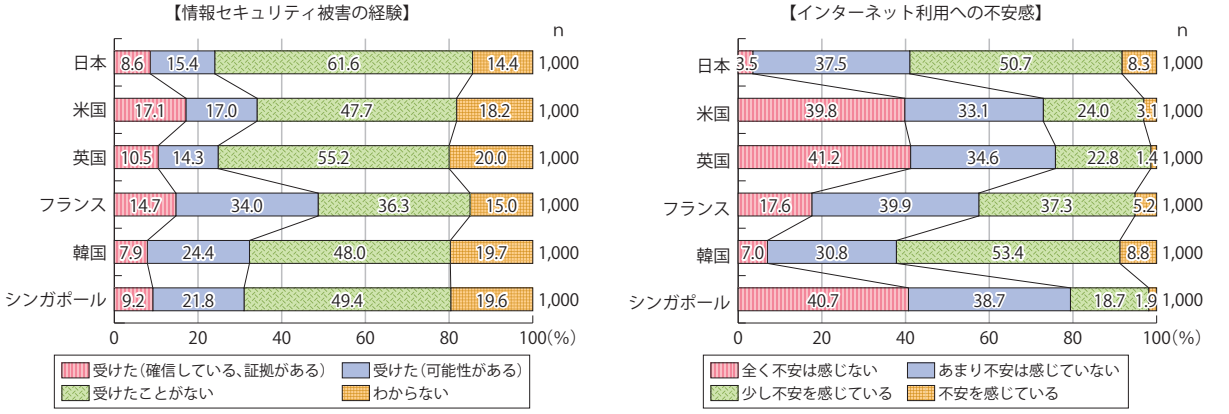
（1）情報セキュリティ被害の経験とインターネット利用への不安感

インターネットを利用していて情報セキュリティ被害にあった経験の有無を尋ねたところ、「被害を受けた」（＝「受けた（確信している、証拠がある）」と「受けた（可能性がある）」の合計）を見ると、フランスが48.7%と最も高く、次いで、米国（34.1%）、韓国（32.3%）の順となった。他方、日本は、「受けたことがない」の回答が61.6%と6か国中最も高い結果となった。

また、インターネット利用時における不安の有無について6か国の利用者に尋ねたところ、不安（「不安を感じている」＋「少し不安を感じている」）と回答した利用者は韓国が62.2%と最も高く、次いで日本（59.0%）、フランス（42.5%）と続いた。

韓国やフランスは「被害を受けた」との回答が多く、かつ、「不安を感じる」との回答が多かったのに対し、日本は「被害を受けていない」との回答が多いにも関わらず、「不安を感じる」との回答が多い点が特徴的である。ちなみに、他の3か国（米国、英国及びシンガポール）では、「全く不安を感じない」との回答が一番多い結果となった（図表3-2-2-1）。

図表3-2-2-1 情報セキュリティに関する被害の経験とインターネット利用への不安感

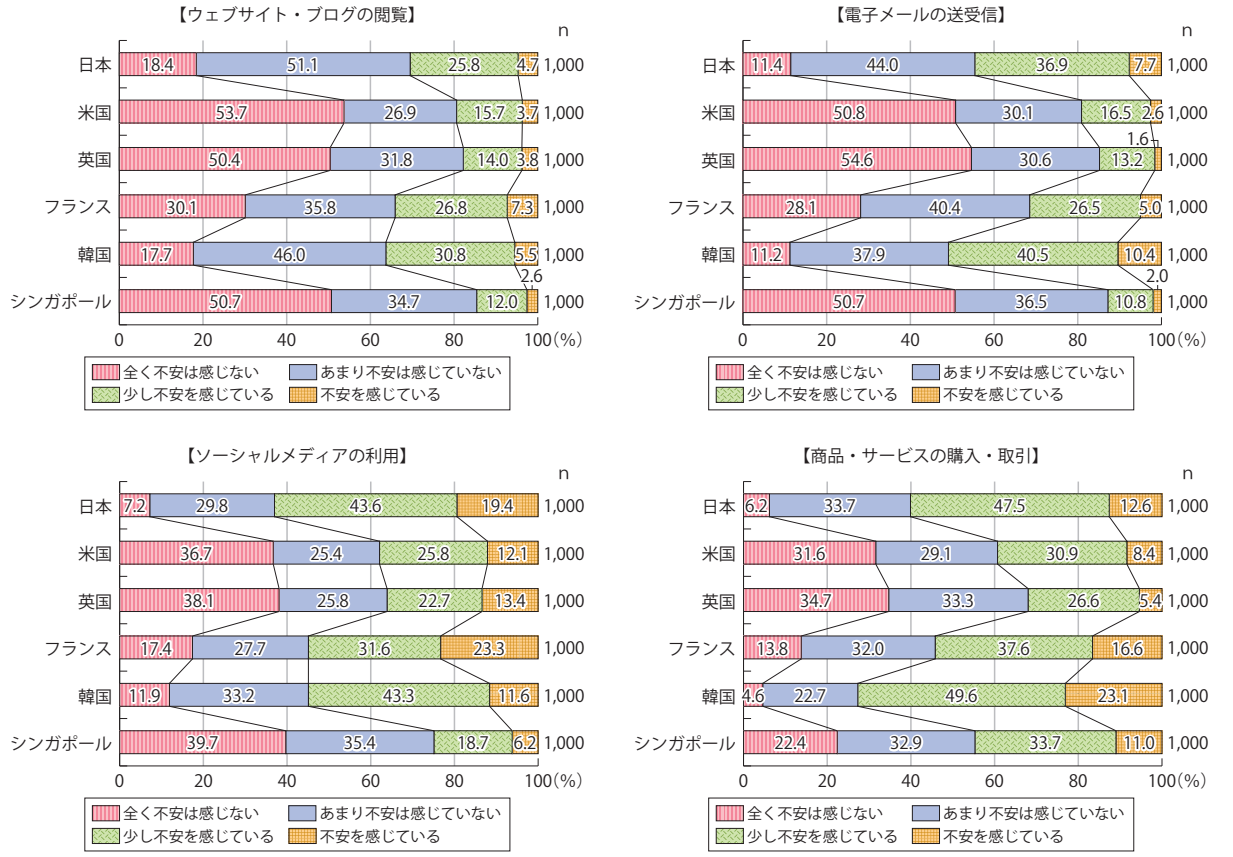


（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

続いて、サービス別に利用時の不安の有無について尋ねたところ、「ホームページ（ウェブ）・ブログの閲覧」や「電子メールの送受信」といった基本的な機能においては、不安を感じる利用者はあまり多くないが、「ソーシャルメディアの利用」や「商品・サービスの購入・取引」の利用となると、インターネット利用について「不安を感じる」との回答が多かった3か国（日本・フランス・韓国）では、「不安を感じる」との回答が高くなった（図表3-2-2-2）。

*10 調査概要は第3章第1節第2項（パーソナルデータの取扱いに関する利用者意識の国際比較）を参照のこと。

図表3-2-2-2　インターネット利用時における不安感（サービス別）



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

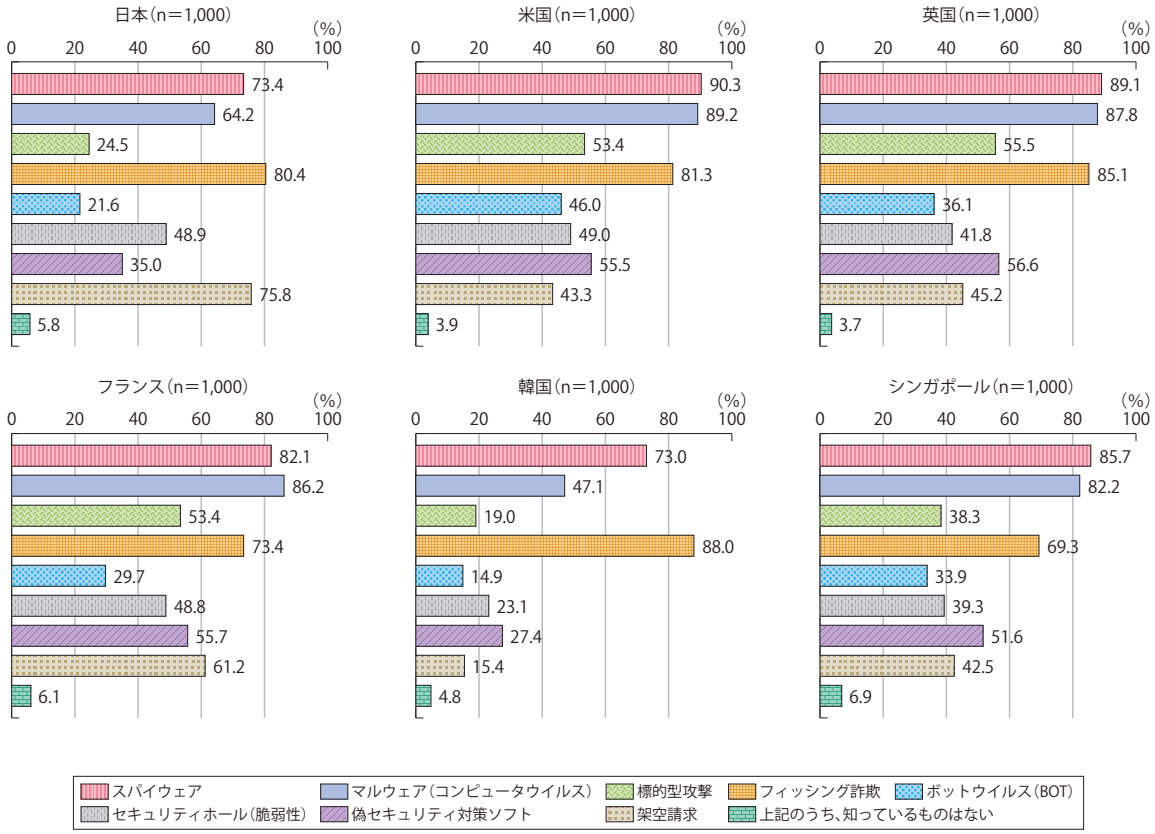
（2）インターネット上の脅威への認知度

インターネット上の脅威に対する認知度について６か国の利用者に尋ねたところ、順位の上下はあるが、「スパイウェア*11」、「マルウェア（コンピュータウイルス）」及び「フィッシング詐欺」についての認知度が高い点では共通している。

そのほかの特徴として、日本では「フィッシング詐欺」に次いで「架空請求」の認知度が高い反面、「標的型攻撃」の認知度があまり高くないこと、韓国では「フィッシング詐欺」を除き、インターネット上の脅威への認知度が他の５か国より全体的に低いことなどが言える（図表3-2-2-3）。

＊11　スパイウェアとは、パソコン内のアクセス履歴等の個人情報の収集等を行うプログラムを意味する。

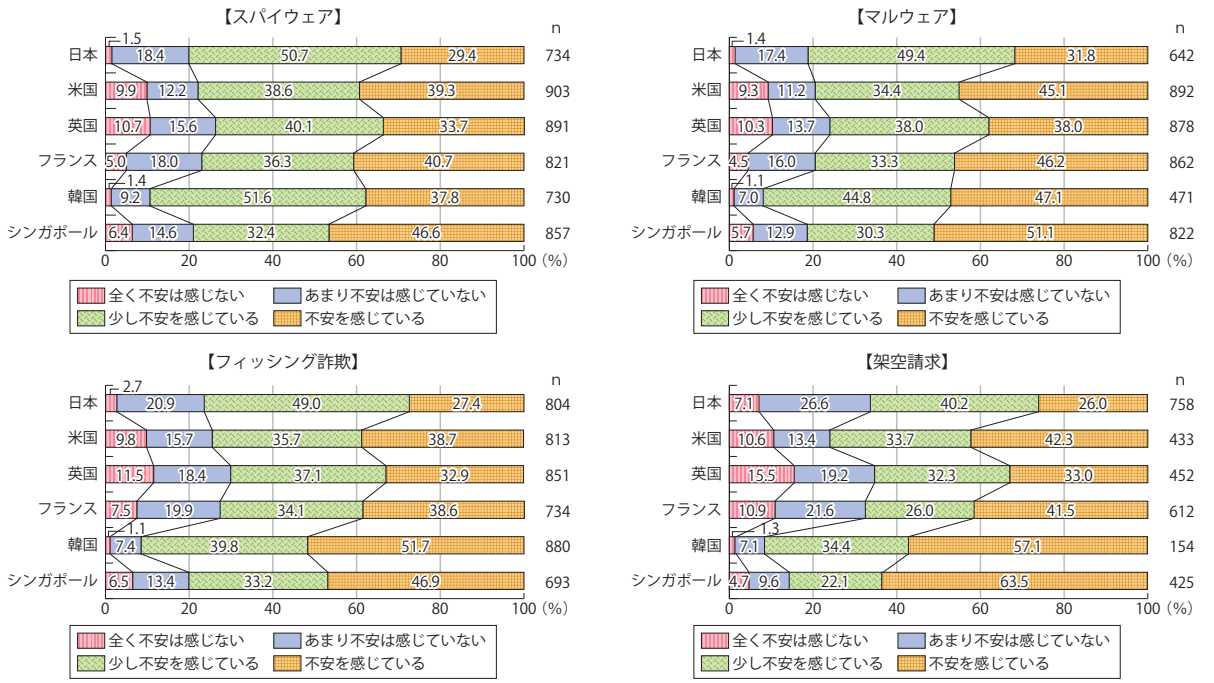
図表3-2-2-3 インターネット上の脅威への認知度



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

続いて、それぞれ認知している脅威に対する不安に関し、各国で認知度が高かった「スパイウェア」、「マルウェア」、「フィッシング詐欺」及び日本で認知度が高かった「架空請求」について尋ねたところ、全体的に脅威として認知しているものに対する不安感は高い結果となっているが、特にシンガポールにおいては「不安を感じている」との回答が他国より高く出る結果となった。シンガポールでは情報セキュリティに対して漠然とした不安ではなく、具体的な脅威を念頭に置いた上で不安を感じている可能性が高いことがうかがえる（図表3-2-2-4）。

図表3-2-2-4 インターネット上の脅威に対する不安感

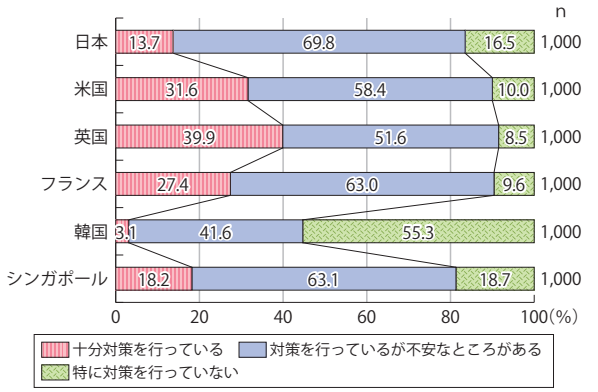


（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

(3) 情報セキュリティ対策の実施状況

情報セキュリティ対策の実施状況を6か国の利用者に尋ねたところ、韓国では「特に対策を行っていない」が55.3%と回答の過半数を占めたのに対し、他の5か国では「対策を行っているが不安なところがある」が回答の過半数を占める結果となった。特に日本では約7割の利用者が「対策を行っているが不安なところがある」と回答した。他方、米国や英国では「十分対策を行っている」と回答した利用者が3割以上存在している（図表3-2-2-5）。

図表3-2-2-5　情報セキュリティ対策の実施状況

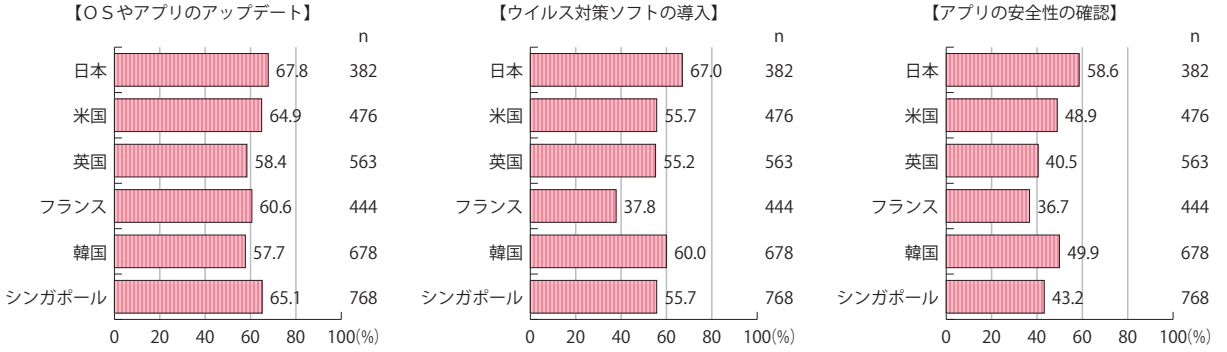


（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

(4) スマートフォンの情報セキュリティ

スマートフォンにおける情報セキュリティ対策については、我が国では「スマートフォンセキュリティ3か条」[*12]を公表し、啓発に努めているところであるが、3か条に該当する「OSやアプリケーションのアップデート」、「ウイルス対策ソフトの導入」及び「インストールするアプリの安全性の確認」の認知度について、6か国の利用者に尋ねた。その結果、日本は3項目すべてにおいて他国より認知度が高い結果となった（図表3-2-2-6）。

図表3-2-2-6　スマートフォンのセキュリティ対策の認知度



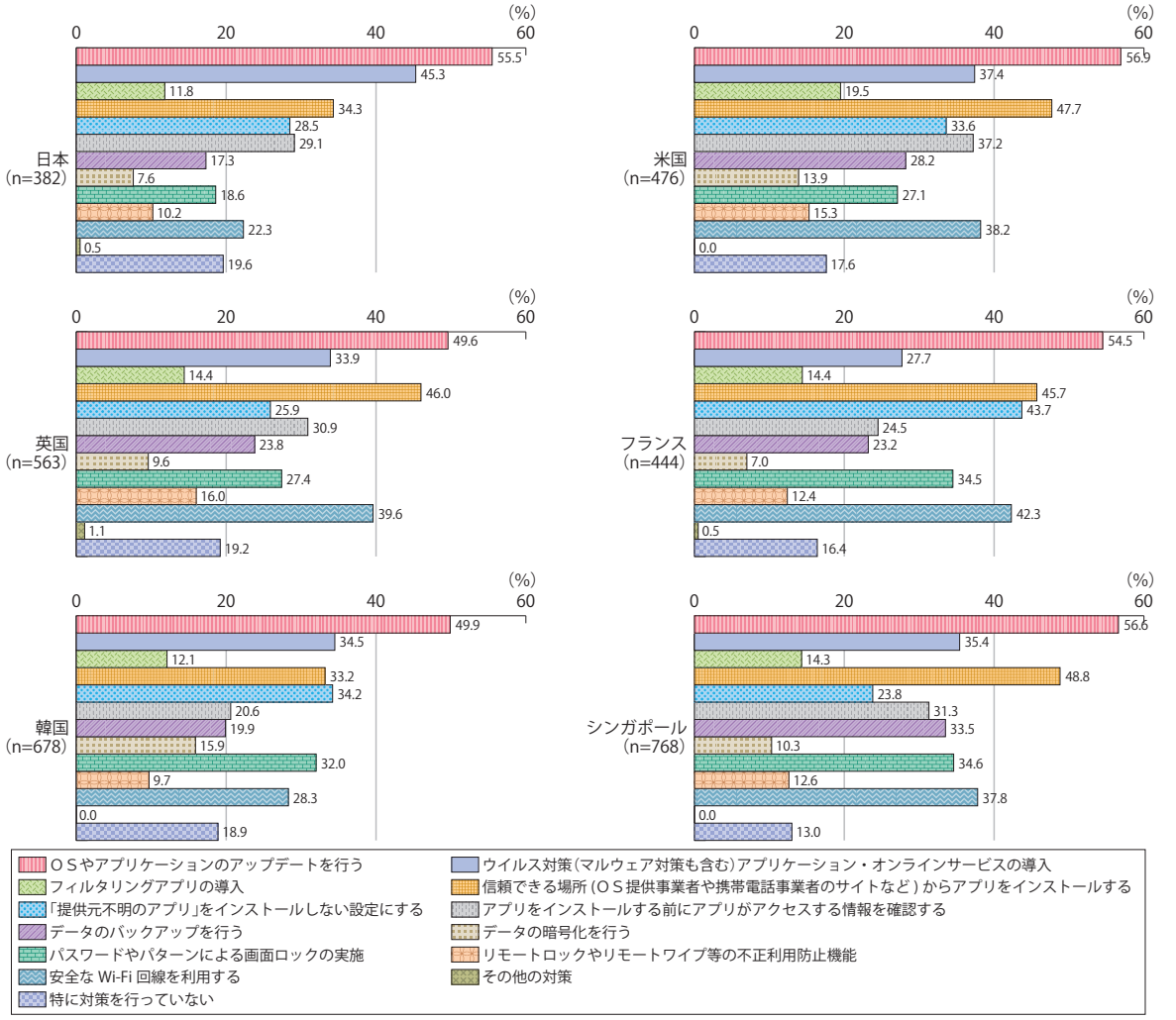
（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

続いて、実際にスマートフォンに行っている情報セキュリティ対策について、スマートフォンセキュリティ3か条以外の対策も含めて尋ねた。まず、3か条の実施状況については、認知度におおむね沿う形で対策が行われているが、日本では、「信頼できる場所（OS提供事業者や携帯電話事業者のサイトなど）からアプリをインストールする」について、その認知度が高い割には、対策の実施状況はそれほど高くないとの結果が出ている。

スマートフォンセキュリティ3か条以外の項目では、「画面ロックの実施」や「安全なWi-Fi回線の利用」についても、日本は他の5か国に比べ、実施状況が低く出る結果となっている（図表3-2-2-7）。

＊12 総務省では、一般の利用者向けに、情報セキュリティの知識に関するさまざまな教材や啓発資料を公開している。平成24年6月に最終報告をとりまとめた「スマートフォン・クラウドセキュリティ研究会」では、スマートフォンの利用者が最低限取るべき対策として、「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」の3つを「スマートフォン情報セキュリティ3か条」として推奨している。

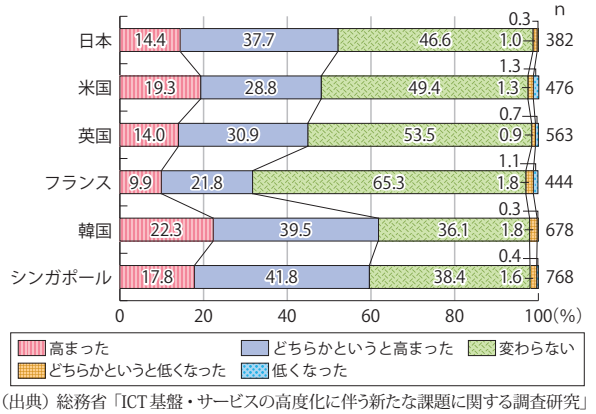
図表3-2-2-7　スマートフォンのセキュリティ対策の実施状況



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

なお、スマートフォンを利用するようになってから、情報セキュリティへの不安が高まったか否かについて尋ねたところ、韓国やシンガポールでは「不安が高まった（どちらかというとを含む）」との回答が約6割に達している。ちなみに、日本では約5割の利用者が「不安が高まった（どちらかというとを含む）」と回答している（図表3-2-2-8）。

図表3-2-2-8　スマートフォンを利用するようになってからの情報セキュリティへの不安



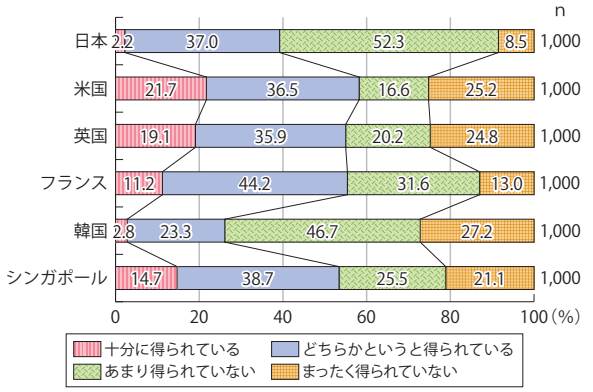
（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

(5) 情報セキュリティに係るリテラシー

情報セキュリティ対策に係る情報を得られているかについて尋ねたところ、米国、英国、フランス及びシンガポールでは得られているとの回答が5割を超えたのに対し、日本及び韓国では4割を下回るという対照的な結果となった（図表3-2-2-9）。

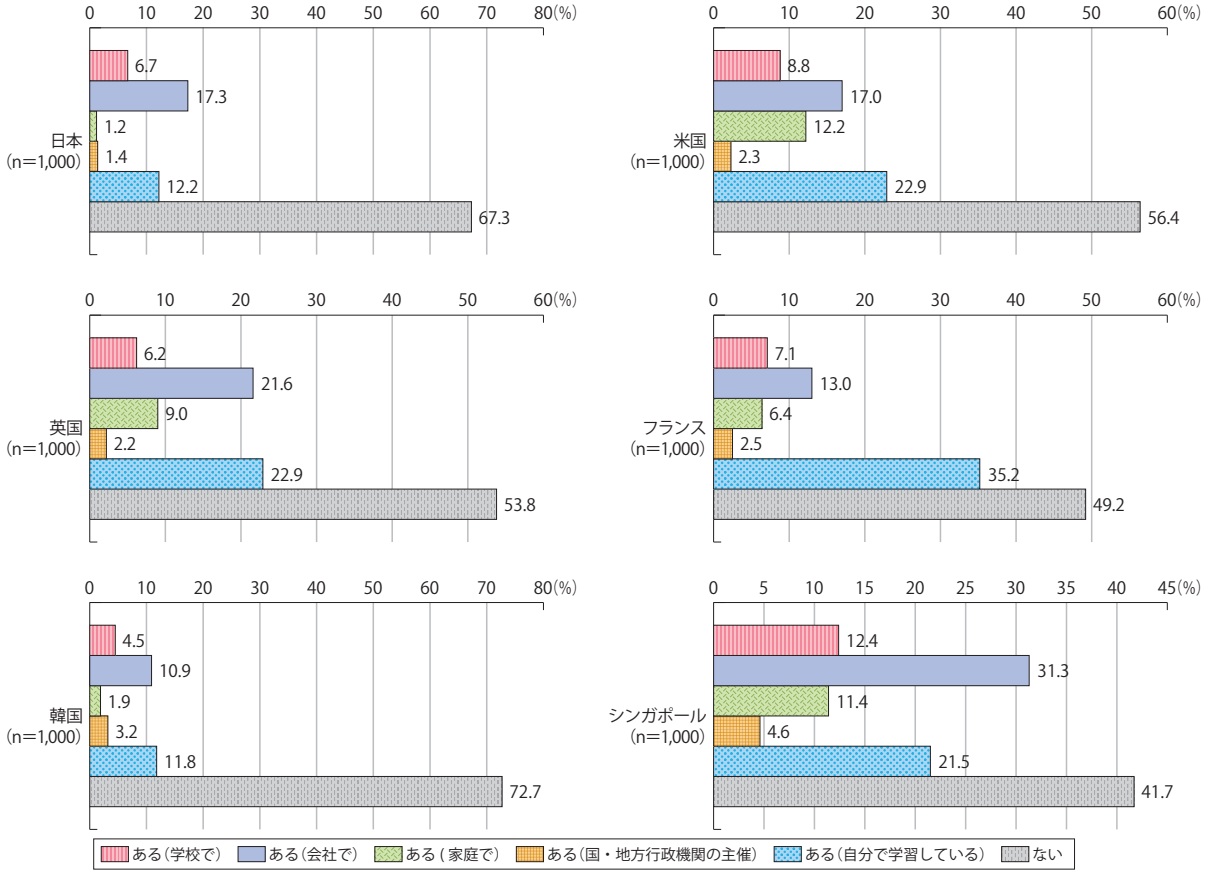
なお、情報セキュリティに関する教育・研修を学校や職場で受けた経験について尋ねたところ、日本や韓国では「ない」との回答が6割を超える結果となった。なお、フランスでは「自分で学習している」との回答が3割を超え、シンガポールでは「会社で受講したことがある」との回答が3割を超えている（図表3-2-2-10）。

図表3-2-2-9　情報セキュリティ対策に関する情報の入手



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

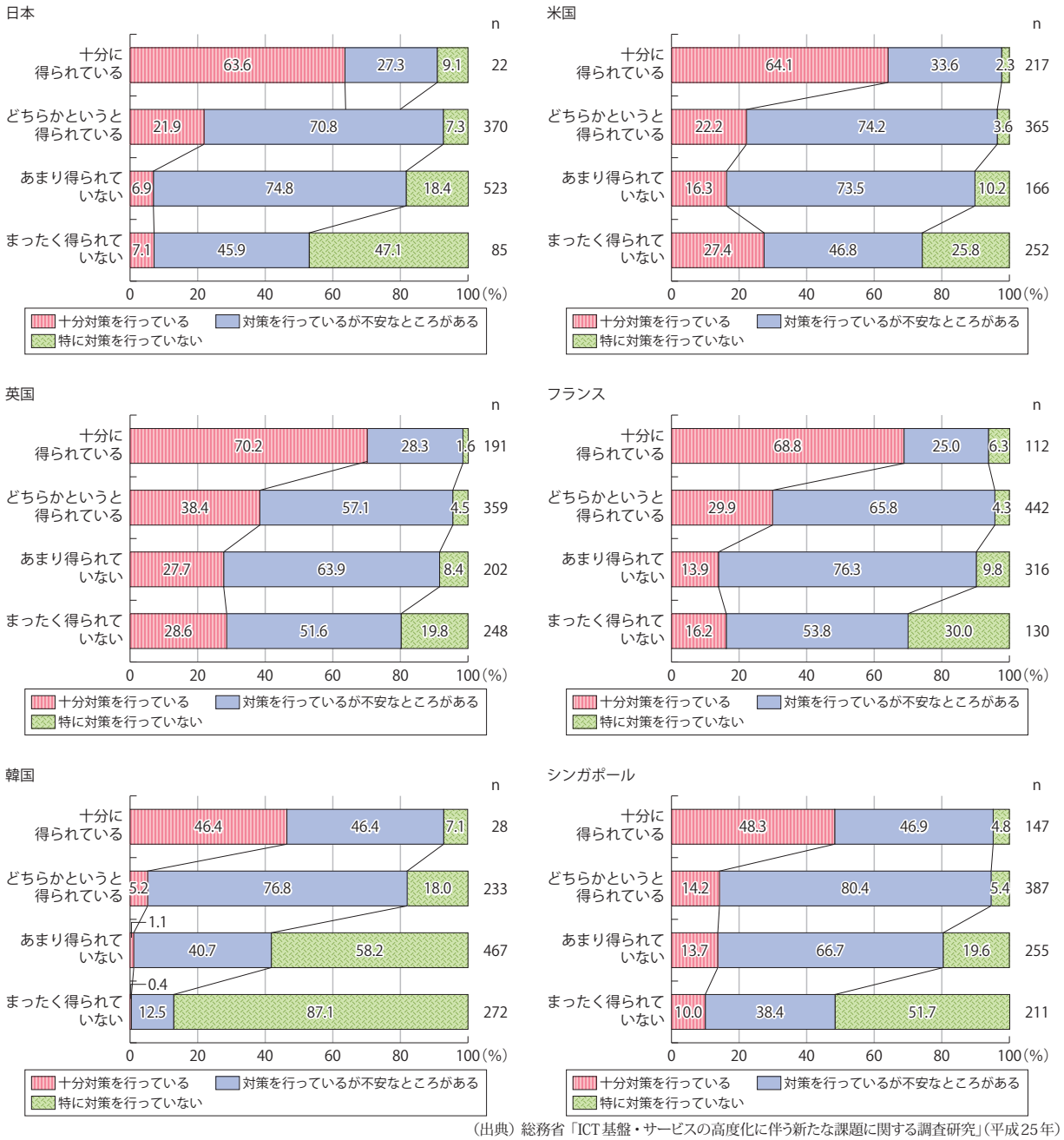
図表3-2-2-10　情報セキュリティの教育・研修を受けた経験



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

さらに、情報セキュリティ対策の実施状況と情報セキュリティ対策に関する情報の入手状況の関連性についても分析したところ、各国とも情報を得ていない人ほど、対策を行っていないという結果が出た。日本、韓国及びシンガポールでは、「十分に得ている」利用者と「まったく得られていない」利用者の間での「対策を行っていない」割合の開きが大きく出ている（図表3-2-2-11）。

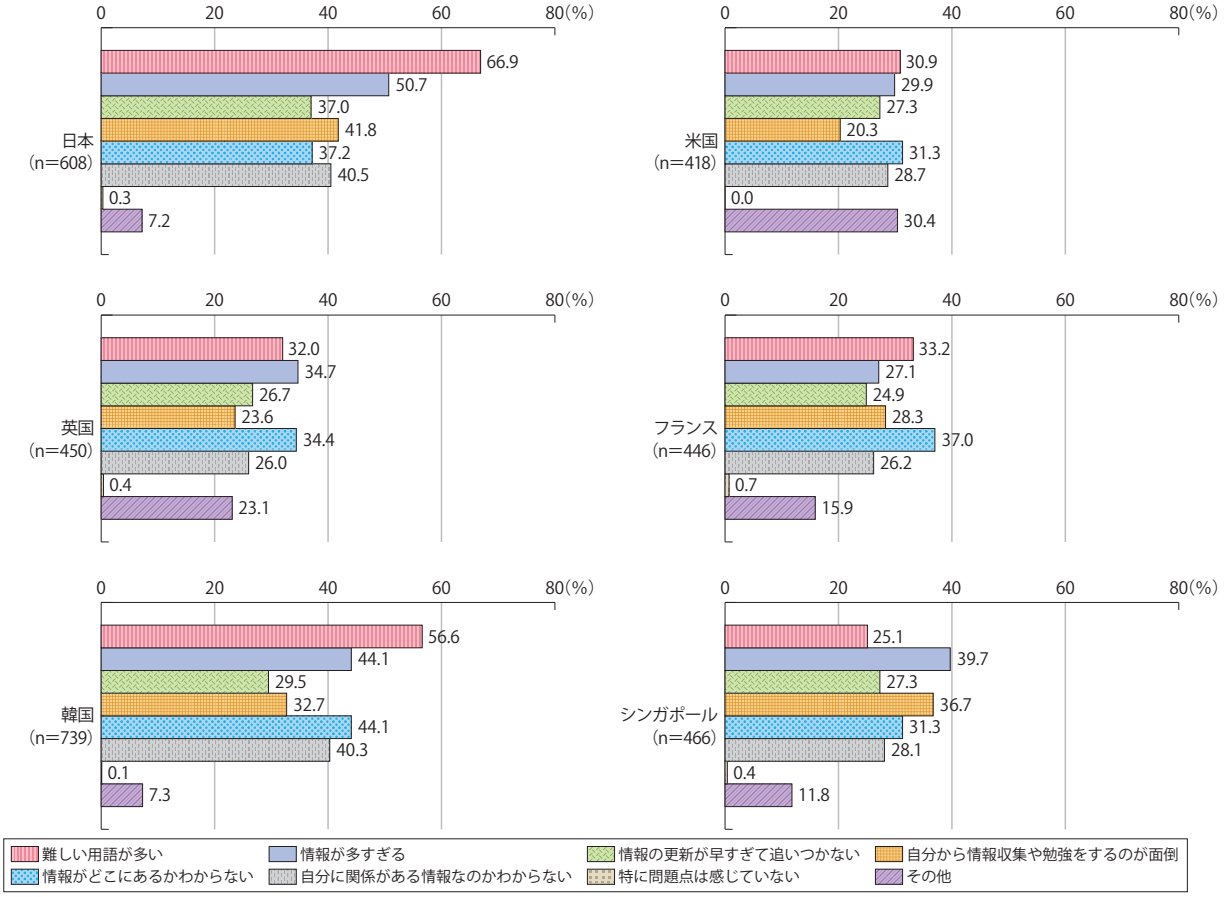
図表3-2-2-11　情報セキュリティ対策の実施状況（情報セキュリティ対策情報の入手状況別）



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

情報セキュリティ対策情報を「あまり得られていない」または「まったく得られていない」と回答した利用者に対して、情報セキュリティ対策情報を入手するにあたって感じている問題について尋ねたところ、大きく３つに分かれた。日本や韓国では利用者の６割前後が「難しい用語が多い」と回答した。他方、英国やシンガポールは「情報が多すぎる」という回答が最も多く、米国やフランスでは「情報がどこにあるか分からない」との回答が最も多かったが、いずれも４割を下回る結果であった（図表3-2-2-12）。

図表3-2-2-12　情報セキュリティ対策情報の入手にあたって感じる問題



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

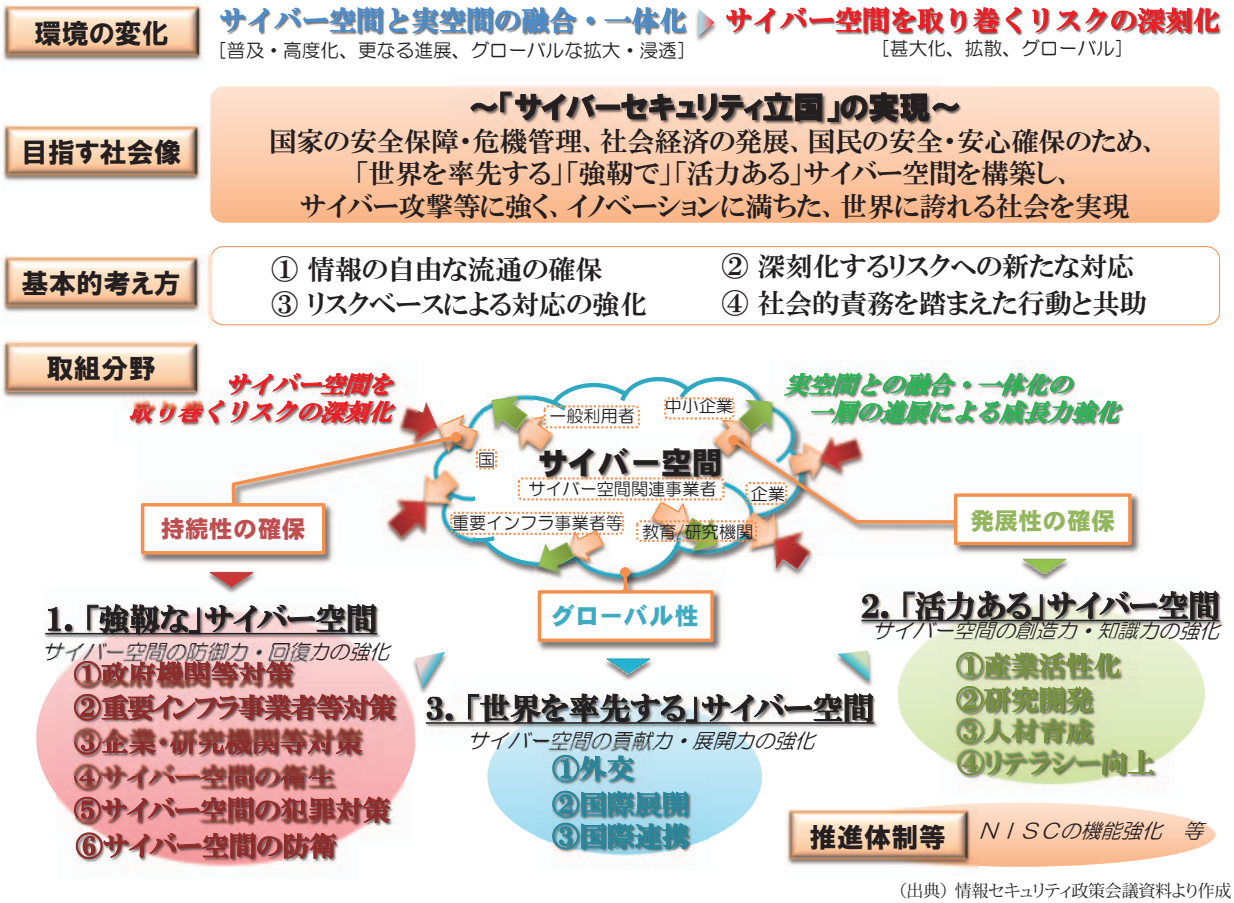
3 我が国における情報セキュリティに係る取組

(1) 新たな情報セキュリティ戦略の策定

我が国では、2005年（平成17年）に、高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）の下に情報セキュリティ政策会議が、また、内閣官房に情報セキュリティセンター（NISC：National Information Security Center）がそれぞれ設置された。これまで同会議においては、情報セキュリティ分野における基本戦略として、「第1次情報セキュリティ基本計画」（2006年（平成18年）2月）、「第2次情報セキュリティ基本計画」（2009年（平成21年）2月）及び「国民を守る情報セキュリティ戦略」（2010年（平成22年）5月）が策定され、官民が連携して情報セキュリティ対策の強化に関する取組が進められてきた。

この間、我が国の情報セキュリティを取り巻く環境が急速に変化し、サイバー空間と実空間の融合・一体化が進展するとともに、サイバー空間を取り巻くリスクが甚大化し、拡散し、グローバルレベルのものとなった。こうした深刻化する環境変化を踏まえ、現在、同会議においては、国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、新たな情報セキュリティ戦略として、世界を率先する強靱で活力あるサイバー空間を構築し、「サイバーセキュリティ立国」を実現することを基本的な方針とする「サイバーセキュリティ戦略」を検討し、本年6月に決定した（図表3-2-3-1）。

図表3-2-3-1 「サイバーセキュリティ戦略」の概要



（出典）情報セキュリティ政策会議資料より作成

(2) 情報セキュリティ分野における各国・地域との協議

我が国はこの間、情報セキュリティ分野における二国間会合において、活発に議論を行っている。

ア　米国

米国との間では、2012年（平成24年）10月に行われた「インターネットエコノミーに関する日米政策協力対話（第4回局長級会合）」において、サイバー攻撃への対応に関する研究開発協力として、総務省（PRACTICE

プロジェクト*13）と国土安全保障省（PREDICTプロジェクト*14）との間でサイバーセキュリティ研究開発に関するネットワーク運用のデータ共有の開始を確認したほか、スマートフォンやクラウドコンピューティングサービスのセキュリティの確保の重要性を認識し、ベストプラクティスと現状のアップデートに関する情報共有の継続で一致した。なお、米国とは2013年（平成25年）5月にサイバーセキュリティに関する初の包括的な対話である「日米サイバー対話」を開催した。

イ　英国

英国とは、2012年（平成24年）6月に「日英サイバー協議」を開催し、サイバーセキュリティにおける国際的な規範作り、安全保障面における課題、サイバー犯罪への取組、情報セキュリティ・システム防護、経済的・社会的側面における両国の取組についての紹介や協力の可能性等について意見交換を行った。

ウ　EU

欧州委員会とは、2012年（平成24年）11月に「日EUインターネット・セキュリティフォーラム」を開催し、情報セキュリティに関する政策動向についての意見交換、情報セキュリティに関するグッド・プラクティス（PRACTICEプロジェクト、スマートフォンのセキュリティ対策等）の共有、重要インフラ防護や官民の情報共有のあり方についての取組の共有、情報セキュリティに関する意識啓発活動についての意見交換が行われた。

エ　ASEAN諸国

ASEAN（東南アジア諸国連合）とは、2012年（平成24年）10月に「第5回日・ASEAN情報セキュリティ政策会議」を開催し、情報セキュリティ意識啓発に関する取組の推進、情報セキュリティ関連情報共有体制の検討と連絡窓口確認の実施、その他情報セキュリティにおける一層の連携強化について合意した。また、2013年（平成25年）9月には「日ASEANサイバーセキュリティ協力に関する閣僚政策会議」を開催する予定である。

オ　インド

インドとは、2012年（平成24年）11月に「第1回日インド・サイバー協議」を開催し、安全保障面における課題、サイバー犯罪への取組、情報セキュリティ・システム防護、経済的・社会的側面における両国の取組についての情報交換や両国間での協力の可能性等について意見交換を行った。

（3）総務省の取組

総務省では、情報セキュリティ対策について、関係府省及び民間事業者等との連携の下、以下の取組を実施している。

ア　情報セキュリティ　アドバイザリーボードの開催

情報通信分野における官民それぞれが、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、我が国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に平成25年3月に情報セキュリティ　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）を設置*15して今後の情報セキュリティ政策のあり方について検討を行い、同年4月に「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」を取りまとめた（図表3-2-3-2）。

本提言を踏まえ、総務省では以下の取組を進めていく予定である。

①「動的防御プロセス連携」の確立

・独立行政法人情報通信研究機構（NICT）は、解析能力等の向上に向けて、平成25年4月、「CYREC(サイレック)*16」という愛称でオール・ジャパンの英知を結集したサイバーセキュリティ研究開発拠点を構築。

・演習用テストベッドを利用した官民のLAN管理者等の参加によるサイバー攻撃の実践的な防御演習を実施し、対象を官庁・大企業から地方公共団体・中小企業に拡大。

②利用者に自律的な対応を促す仕組づくり

【個人利用者】

・通信事業者によるマルウェア感染、悪性サイトへのアクセスに対する注意喚起等の実施。

＊13 Proactive Response Against Cyber-attacks Through International Collaborative Exchange。総務省が平成23年度から実施している研究開発の一つ。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6月現在、米国、インドネシア、タイ、マレーシア等と連携。

＊14 Protected REpository for Defense of Infrastructure against Cyber Threats。米 国土安全保障省のサイバーセキュリティ技術開発プロジェクト。

＊15 http://www.soumu.go.jp/menu_seisaku/ictseisaku/securityadvisory/index.html

＊16 Cybersecurity Research Center

・スマートフォンのアプリについて、個人がリスクを認識し、利用などの判断を自ら行うことが可能な仕組の構築。

【中小企業】

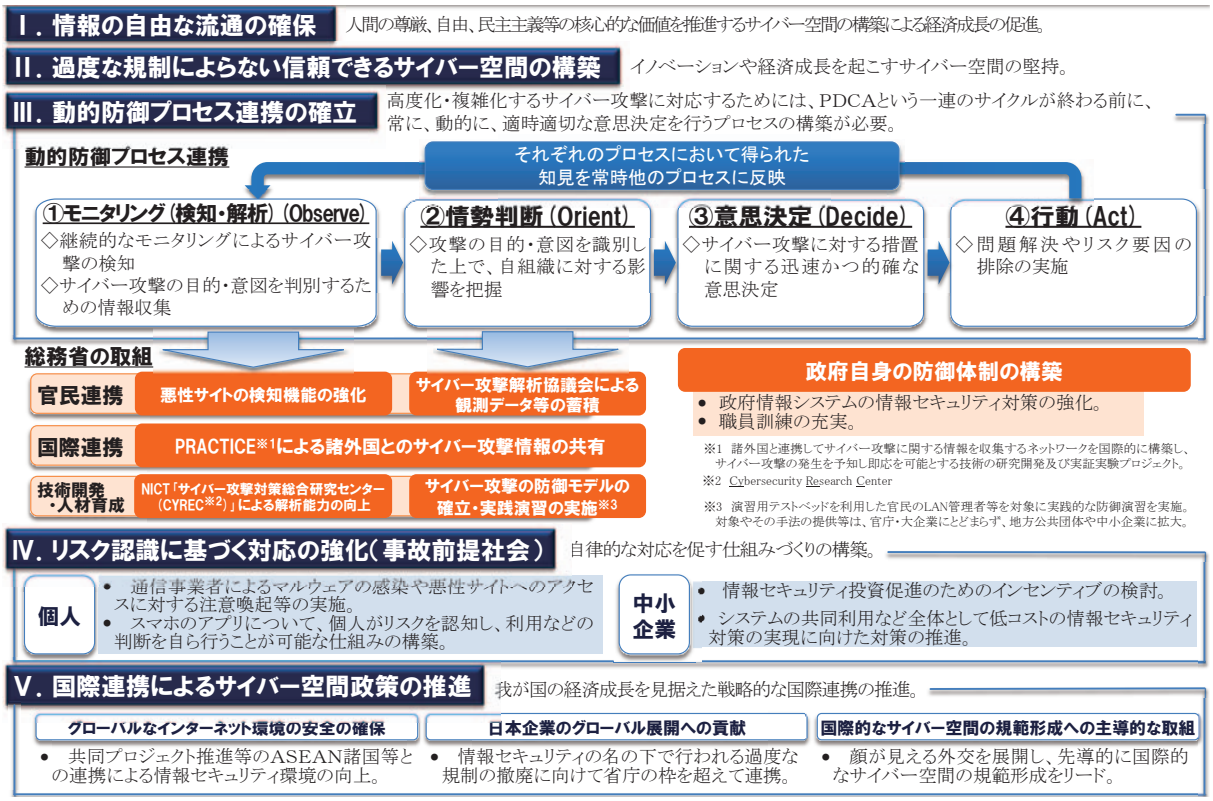
・情報セキュリティ投資促進のためのインセンティブの検討。

③多様な国際協力の推進

・サイバー攻撃に関する情報共有の枠組を米国、インドネシア等から欧州、ASEAN諸国に拡大し、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・実証実験を実施。

・ASEAN諸国の情報セキュリティ環境の高度化を支援するため、「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」を2013年（平成25年）9月に開催。

図表3-2-3-2　「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」の概要



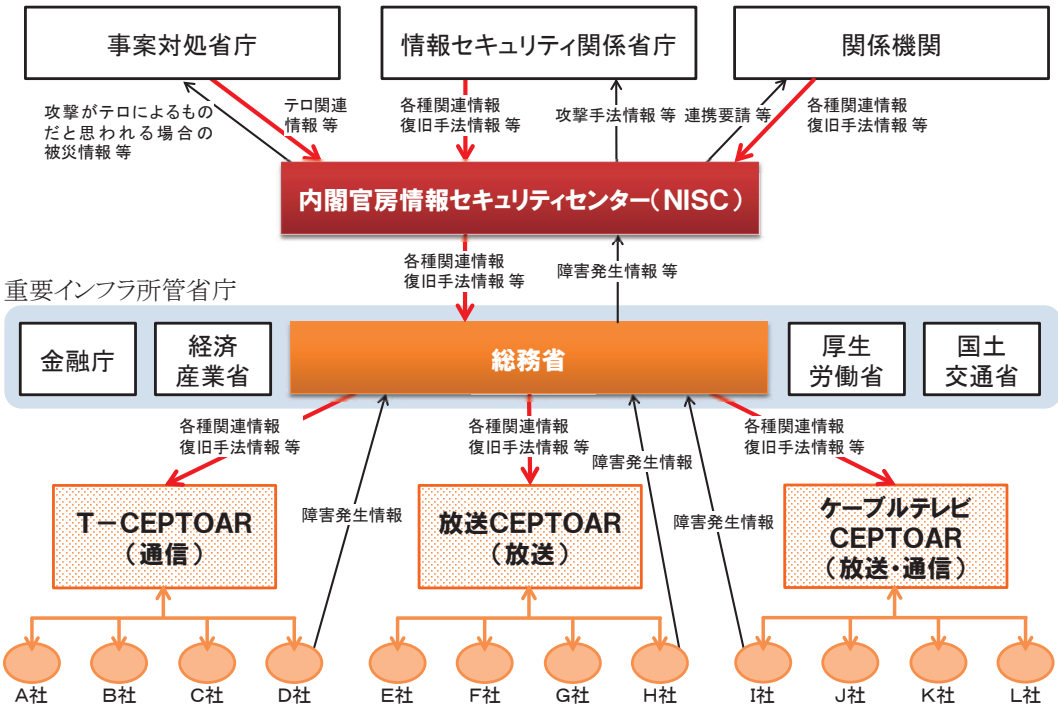
イ　官民連携

サイバー攻撃による被害の拡大防止等に寄与すべく、政府全体としては、セプター*17を通じた重要インフラ事業者*18との情報共有体制を構築している。総務省では、重要インフラである情報通信及び地方自治体を所管しており、これらの関係者または、NICTとの間で、情報共有及び対応策の強化に向けた連携を進めている（図表3-2-3-3）。

*17 CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response）。重要インフラ分野における情報共有・分析を行う体制。

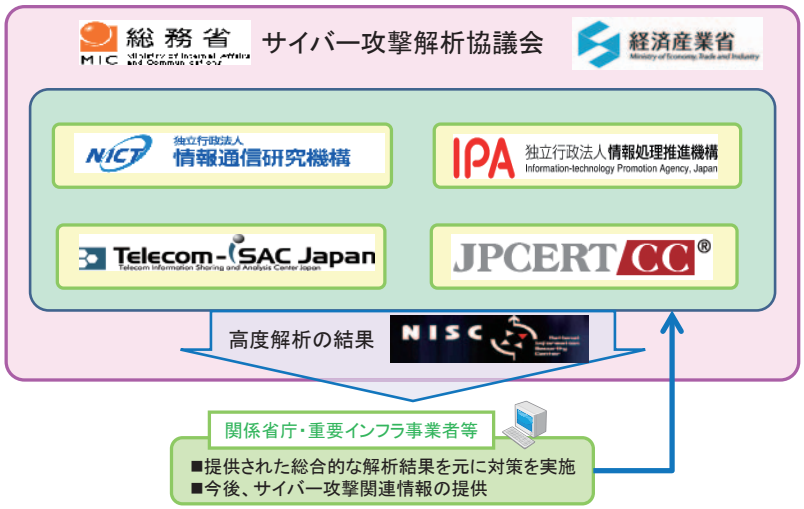
*18 「重要インフラの情報セキュリティ対策に係る第２次行動計画」（ＩＴ戦略本部情報セキュリティ政策会議 2009年２月決定、2012年４月改定）では、「重要インフラ」を他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状況に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものとしており、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む。）」、「医療」、「水道」及び「物流」の10分野としている。

図表3-2-3-3　情報通信分野のサイバー攻撃等の情報共有体制



また、高度なサイバー攻撃は、その実態を把握することが困難であることから、平成24年7月、総務省及び経済産業省は、サイバー攻撃に関する情報共有と高度解析を進めるため、NICT、独立行政法人情報処理推進機構（IPA：Information-technology Promotion Agency）、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*19及び一般社団法人JPCERTコーディネーションセンターの関係4団体とともに「サイバー攻撃解析協議会」を発足させた。平成25年4月、同協議会は平成24年度活動成果と今後の活動方針を取りまとめ、今後、協議会参加の各団体において、解析の精度及び適時性の向上を図り、その成果を各団体の活動の中で活かすとともに、NISCや重要インフラ事業者等への情報提供も順次図っていくこととしている（図表3-2-3-4）。

図表3-2-3-4　サイバー攻撃解析協議会の構成図



さらに、機密情報等を有する特定の対象を狙った高度なサイバー攻撃（標的型攻撃）が依然として発生しており、政府機関、民間企業等から機密情報が漏えいする事態が生じている。このため、技術的な対策のほか、実際のLAN管理者の対処能力を向上させることがますます重要となっている。そこで、総務省では、サイバー攻撃関連情報を収集・解析し、解析結果に基づく組織ネットワークの防御モデルを構築した上で、官民参加型のサイ

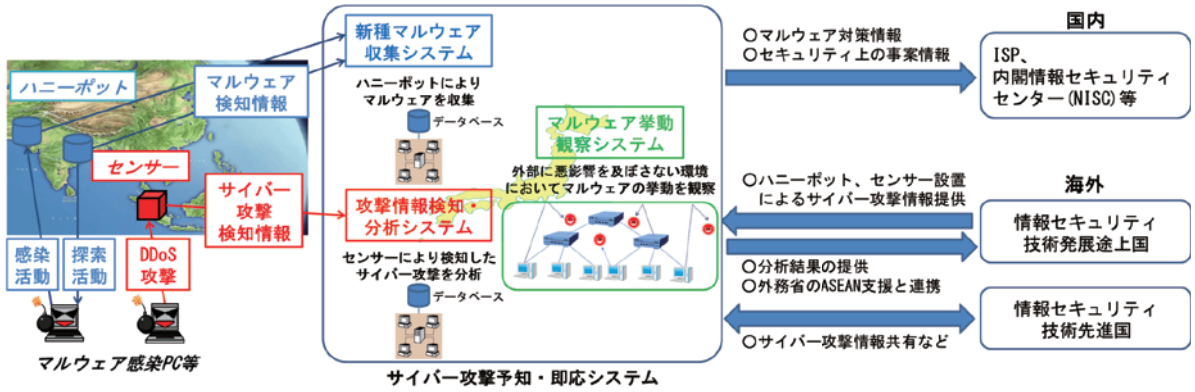
＊19 国内の主要なインターネットサービスプロバイダ（ＩＳＰ）により構成され、情報セキュリティインシデント情報等を収集・分析し、業界内で共有することを目的としている。

バー攻撃に対する実践的な防御演習を実施する施策を開始している。

ウ　国際連携

国境を越えたサイバー攻撃の増加を踏まえると、一国・一組織による対応では難しい状況となっていることから、国際連携が重要なポイントとなる。このため、総務省では、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、DDoS攻撃などのサイバー攻撃、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（PRACTICEプロジェクト）を実施している。これまで、米国、ASEAN等の海外諸国と連携を開始している（図表3-2-3-5）。

図表3-2-3-5　PRACTICEプロジェクトの概要



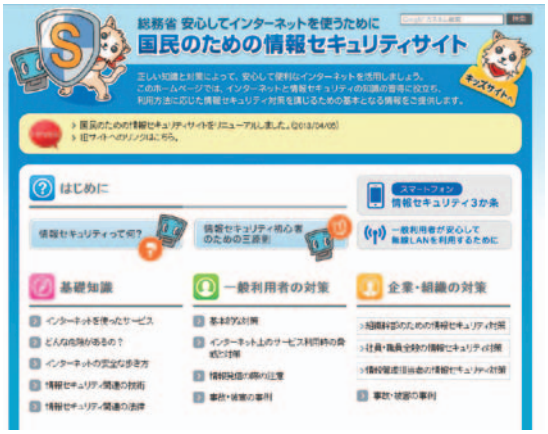
エ　普及啓発

スマートフォン、SNS、無線LANなど、新たな情報通信サービスが国民生活に浸透する一方で、それらのサービスの性質を悪用した詐欺などによる被害も発生している。このため、利用者一人一人が、これらのサービスの性質を理解し、安心・安全に使うための知識（情報セキュリティ・リテラシー）を身につけることが重要となる。

また、総務省は、情報セキュリティに関する知識をわかりやすく解説した「国民のための情報セキュリティサイト[*20]」を、平成15年度から運営している。平成24年度には、最新のサービス動向や情報セキュリティ上の脅威の動向を踏まえ、同サイトのコンテンツの刷新・拡充を行い、平成25年4月にリニューアルしたサイトを公開した。

さらに、一般及び企業において利用が拡大している無線LANについては、情報窃取等の情報セキュリティ上の課題が指摘されている。このため、無線LANの安心・安全な利用を促進することを目的に、手引書「一般利用者が安心して無線LANを利用するために」[*21]（平成24年4月）及び「企業等が安心して無線LANを導入・運用するために」[*22]（平成25年1月）を策定・公表したところである（図表3-2-3-6）。

図表3-2-3-6　「国民のための情報セキュリティサイト」及び「一般利用者が安心して無線LANを利用するために」



*20 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html
*21 http://www.soumu.go.jp/main_content/000199322.pdf
*22 http://www.soumu.go.jp/main_content/000199323.pdf

オ　暗号技術の安全性評価と高度化の推進

総務省では、経済産業省と共同で暗号評価プロジェクトCRYPTREC（Cryptography Research and Evaluation Committee）*23を開催し、NICT及びIPAの知見を得ながら、電子政府推奨暗号等の安全性の評価・監視や、暗号技術の適切な実装方法・運用方法の調査・検討を実施している。

近年の技術の進展により「電子政府推奨暗号リスト」掲載暗号の危殆化が懸念されていることから、CRYPTRECにおいて、安全性、実装性、運用性等の様々な観点から掲載候補の暗号の評価を実施し、「電子政府推奨暗号リスト」（平成15年2月20日公表）*24を改定して「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日公表）*25を策定した。

カ　電子署名・認証業務の普及促進

電子商取引等のネットワークを介した社会経済活動を安全に行うため、「電子署名及び認証業務に関する法律」（平成12年法律第102号）では、安全性の高い電子署名について行われる認証業務を「特定認証業務」と定義し、電子署名の真正性を担保している。平成25年4月末現在、11件の特定認証業務が認定を受けており、電子署名・認証業務の普及促進を図っている。

＊23 http://www.cryptrec.go.jp/index.html
＊24 http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_fy2005.pdf
＊25 http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf