

情報セキュリティ白書2015

サイバーセキュリティ新時代：あらゆる変化へ柔軟な対応を

概要説明資料

2015年7月1日

独立行政法人情報処理推進機構
技術本部セキュリティセンター
情報セキュリティ分析ラボラトリー

情報セキュリティ白書2015

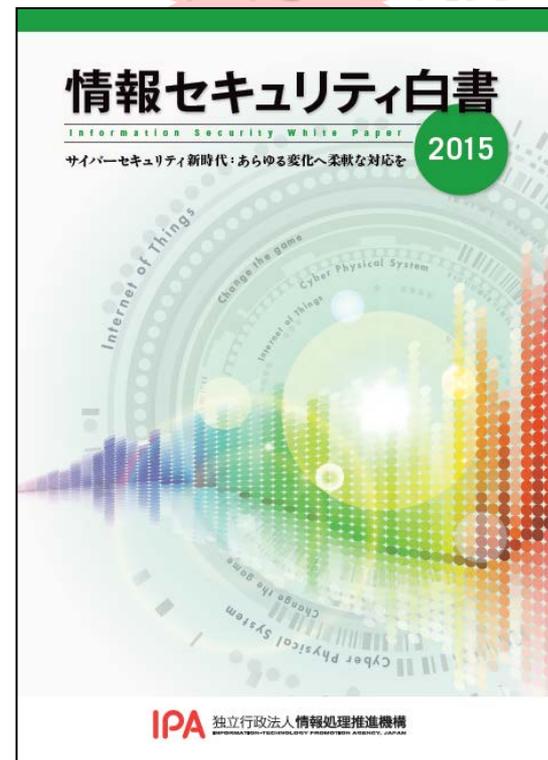
サイバーセキュリティ新時代：あらゆる変化へ柔軟な対応を

情報セキュリティの動向を広くカバーした一冊

- 2014年度に情報セキュリティの分野で起きた注目すべき10の出来事を分かりやすく解説
- 国内外における情報セキュリティインシデントの状況や事例、攻撃の手口や脆弱性の動向、企業や政府等における情報セキュリティ対策の状況を掲載
- 情報セキュリティを支える基盤の動向として、国内外における情報セキュリティ政策や関連法の整備状況、情報セキュリティ人材の現状、組織の情報セキュリティマネジメントの状況、国際標準化活動の動向を掲載
- 近年注目されている内部不正対策や高度化する標的型攻撃に対する取り組みの動向、IoTの情報セキュリティ、マイナンバー制度等の主要なテーマを解説

◆ 入手先：Amazon(<http://www.amazon.co.jp>)
全国官報販売組合(<http://www.gov-book.or.jp>)
IPA ※全国の書店からも購入できます
電子書籍版はAmazon Kindleストア、
楽天Kobo(<http://books.rakuten.co.jp/e-book/>)より発売

2015年7月1日発売



発行：IPA

ISBN：978-4-905318-31-6

ソフトカバー / A4判

定価 2,000円（税別）

電子書籍版 定価1,600円（税別）

全体構成

- **第Ⅰ部 情報セキュリティの概要と分析**
 - 序章 2014年度の情報セキュリティの概況～10の主な出来事～
 - 第1章 情報セキュリティインシデント・脆弱性の現状と対策
 - 第2章 情報セキュリティを支える基盤の動向
 - 第3章 個別テーマ
- **第Ⅱ部 情報セキュリティ10大脅威2015 ～被害に遭わないために実施すべき対策は？～**
- 付録 資料・ツール
- 第10回 IPA「ひろげよう情報モラル・セキュリティコンクール」
2014 受賞作品
- コラム

2014年度に観測されたインシデント状況

情報漏えいインシデント

データ漏えい／侵害事例では外部からの攻撃が15%増加、内部犯行によるものが2%増加。データ侵害の件数は2013年から23%増加。

マルウェア遭遇

標的型攻撃が前年比8%増で過去最多を記録。水飲み場型攻撃も増加。

スパムメール発信源

「スパム配信国ワースト12」の2014年10～12月期で日本が初めて5位にランクイン。送信にはボットウイルスに感染したパソコンが悪用されている。

序章 2014年度の情報セキュリティの概況～10の主な出来事～

2014年4月から2015年3月を対象に、本書の全体を表すトピックスを10個選定

- ① インターネットバンキングの不正送金被害、過去最悪を更新（1.2.3）（1.3.5）
- ② 止まらないパスワードリスト攻撃による不正ログイン（1.2.4）（1.3.7）
- ③ 内部不正による被害が相次ぎ表面化（1.2.8）（2.1.2）（3.1）
- ④ インターネット基盤を揺るがす脆弱性が多発（1.2.1）（1.3.1）
- ⑤ 日々巧妙化する標的型攻撃による諜報活動（1.2.5）（1.3.2）
- ⑥ サイバー攻撃対処のための「通信の秘密」の解釈を明確化（2.1.3）
- ⑦ サイバーセキュリティ基本法の成立に伴うNISCの体制強化（2.1.1）（2.2.1）
- ⑧ J-CRAT（サイバーレスキュー隊）の正式発足、日本サイバー犯罪対策センター（JC3）の稼働等、サイバー攻撃への対応体制を整備（2.1.2）（2.1.4）（3.3）
- ⑨ パーソナルデータ保護と利活用への取り組み、マイナンバー制度の準備が本格化（2.2.2）（3.2）
- ⑩ IoTの情報セキュリティ（3.7）

※末尾の項番号は、「情報セキュリティ白書2015」のもの。

①インターネットバンキングの不正送金被害、過去最悪を更新

2014年は、国内のインターネットバンキングを狙った不正送金の年間被害額が過去最大。これまで過去最悪だった2013年と比較して被害件数は約1.4倍、被害額は約2倍。インターネットバンキングの個人口座だけでなく、振込み上限額が大きい法人口座も狙われ、被害額が急増。ワンタイムパスワードや電子証明書等の銀行側の対策に対応した新しい手口のウイルスが登場するなど、更に注意が必要である。

不正送金の被害件数と被害額

2013年と比較し被害総額は約2倍

年	被害件数	被害額 (約)
2011年	165件	3億800万円
2012年	64件	4,800万円
2013年	1,315件	14億600万円
2014年	1,876件	29億1,000万円
		上半期：18億5,100万円 下半期：10億5,800万円

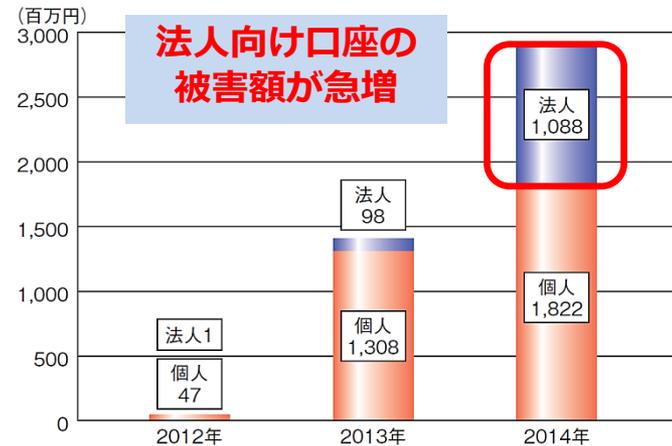
約2倍

約1.4倍

■表 1-2-2 不正送金の被害件数と被害額

(出典)警察庁「平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」⁵²「平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」を基に IPA が作成

口座種別ごとの被害額



■図 1-2-3 口座種別ごとの被害額

(出典)警察庁「平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」を基に IPA が編集

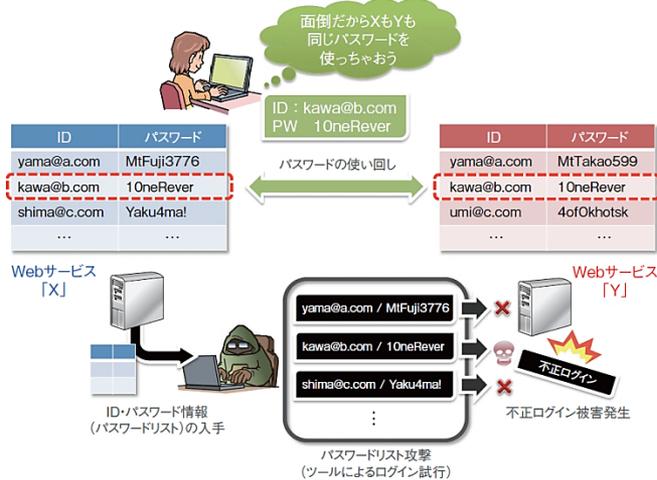
▲不正送金被害の主な原因

- ・フィッシングやログイン情報窃取のウイルスの他、新たなウイルスが登場
→送金に必要なID等の情報を入力すると、それらが即座にウイルスによって悪用され、リアルタイムに第三者の口座へ不正送金されてしまう、等

②止まらないパスワードリスト攻撃による不正ログイン

2014年度は、2013年度と同様、IDとパスワードを使いまわしている利用者を狙った**パスワードリスト攻撃による被害が多発**。パスワードリスト攻撃は、脆弱なサイトからアカウント情報が盗まれ、同じID・パスワードを使用している他のサイトに次々と不正にログインし、**情報の窃取や不正利用等の被害を引き起こす**。

パスワードリスト攻撃のイメージ



■ 図 1-3-20 パスワードリスト攻撃の例

▲パスワードリスト攻撃被害の主な原因

- ・IDとパスワードの使い回し

不正ログインのあったサービスとその概要

公表日	対象サービス	運営会社	攻撃期間	被害件数	ログイン試行回数
2014年4月4日	個人向けインターネットバンキング	足利銀行	2014年4月4日9:00頃～19:00頃	15	7万7,966
2014年4月23日	CLUB Panasonic	パナソニック株式会社	2014年3月23日～4月21日	7万8,361	460万超
2014年4月30日	My SoftBank	ソフトバンクモバイル株式会社	2014年4月14日～4月28日	724	公表なし
2014年5月2日	ソニーポイントサービス	ソニーマーケティング株式会社	2014年4月19日～4月29日	273	公表なし
2014年6月10日	niconico	株式会社ニワンゴ	2014年5月27日～6月4日	29万5,109	355万1,370
2014年6月12日	LINE	LINE 株式会社	公表なし	公表なし	公表なし
2014年6月17日	mixi	株式会社ミクシィ	2014年5月20日～6月16日		
2014年6月20日	はてな	株式会社はてな	2014年6月6日～6月19日		
2014年6月23日	Ameba	株式会社サイバーエージェント	2014年6月19日17:27～6月23日8:36	3万8,280	229万3,543
2014年6月26日	CAPAT	株式会社クリエイティブ・プランニング・アンド・プロモーション	2014年6月23日～6月24日	最大1万1,502	公表なし
2014年6月30日	バンダイナムコID	株式会社バンダイナムコゲームス	2014年6月28日～6月29日	1万4,399	179万6,629
2014年7月4日	あんぱら	株式会社イード	2014年6月25日～7月1日	1万5,092	342万
2014年8月13日	無印良品ネットストア	株式会社良品計画	2014年8月7日16:34～8月12日10:52	2万957	422万382
2014年8月18日	Suica ポイントクラブ	JR 東日本	2014年8月15日1:29～5:35	756	約29万6,000
2014年9月8日	ボンバレモール	株式会社リクルートホールディングス	2014年9月6日～9月7日	9,749	3万1,660 (リクルートIDと一致した件数)
2014年9月12日	My JR-EAST	JR 東日本	2014年9月10日2:59～9月11日10:55	約2万1,000	約1,152万
2014年9月23日	無印良品ネットストア	株式会社良品計画	2014年9月22日21:29～9月23日0:04	19	1万8,663
2014年9月26日	クロネコメンバーズ	ヤマト運輸株式会社	2014年9月25日～9月26日17:00	1万589	約19万
2014年9月29日	WEBトータル	佐川急便株式会社	公表なし	3万4,161	公表なし
2014年9月				6,072	公表なし
2014年11月				10万8,185	公表なし
2014年12月				1,320	316万1,872
2015年1月9日	モラッポ、mixi アンケート	株式会社ミクシィ	2014年12月23日	4,536	1,960万
2015年2月4日	So-netメールサービス	ソネット株式会社	2014年9月1日～2015年1月20日	3万1,529	公表なし

被害件数約30万件

1日で1,900万回の不正なログインの試行もあり

③内部不正による被害が相次ぎ表面化

内部者の不正行為による被害の報道が相次いだ。2014年7月、株式会社ベネッセコーポレーションのグループ会社が業務を委託した企業の社員が、顧客情報を漏えいさせたとして不正競争防止法違反の容疑で逮捕された。漏えいした顧客情報は、国内史上最悪の**約3,504万件**に上った。**内部不正の解決に要する時間は平均39.5日と最長。**

技術情報等の営業秘密の流出は、組織における内部者によるものが多いことから、内部不正対策及び営業秘密の保護対策を見直す気運が高まっている。

内部者による犯行事例※

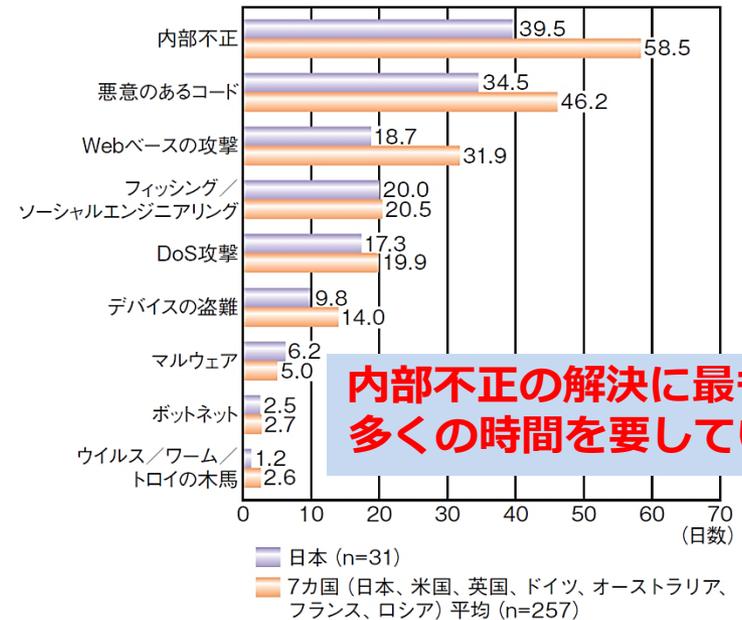
報道年月	事件の概要	不正行為者	動機
2014年7月	株式会社ベネッセコーポレーションの顧客データベースを保守管理するグループ会社の業務委託先の元社員が、大量の個人情報流出させたとして逮捕された。	委託先元社員	金銭の取得
2015年1月	家電量販大手エディオンの子会社の元役員が遠隔操作ソフトを使い、エディオンの営業秘密に当たる4件のデータを不正に入手したとして逮捕された。	退職者	転職先で役立てたかった

※本誌に掲載されている事例の一部

▲内部者による情報漏えいの主な原因

- 処遇への不満等の動機
- 機密情報へのアクセス権限の悪用
- 監視体制が不十分

サイバー攻撃別の平均解決日数



内部不正の解決に最も多くの時間を要している

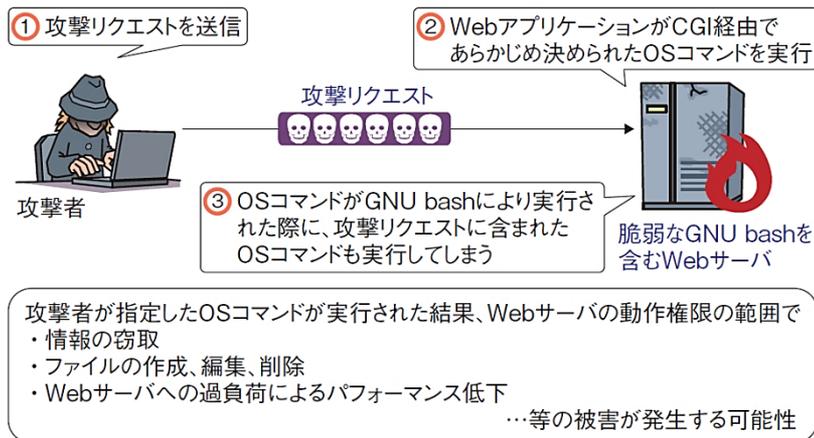
図 3-1-1 サイバー攻撃別の平均解決日数
(出典) Ponemon「2014 Global Report on the Cost of Cyber Crime」
「2014 Cost of Cyber Crime Study: Japan」(提供: HP Enterprise Security)^{*9}を基に IPA が編集

④インターネット基盤を揺るがす脆弱性が多発

2014年度はクライアントのブラウザやサーバで利用されているソフトウェアまで、広く普及しているソフトウェアに**深刻な脆弱性**が多数公開された。

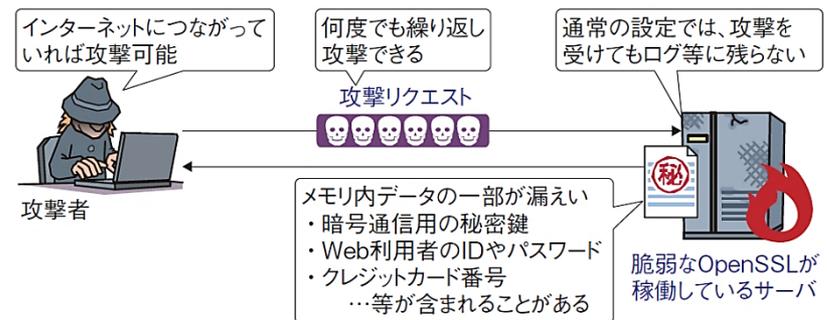
特に、Windowsの標準ブラウザであるInternet Explorerの脆弱性や、OpenSSLの脆弱性（通称HeartBleed）、Linux系OSのGNU bashの脆弱性（通称ShellShock）、Webアプリケーション開発で広く利用されているApache Struts2の脆弱性など、**インターネット基盤に大きな影響を与える脆弱性が相次いで公開され**、企業は対応に追われることとなった。

GNU bashの脆弱性の悪用イメージ



■ 図 1-3-1 GNU bash の脆弱性の悪用イメージ

OpenSSLの脆弱性の悪用イメージ



■ 図 1-3-2 HeartBleed の悪用イメージ

- ▼ 広く普及しているソフトウェアの脆弱性対策
- OS やアプリケーションのアップデートが基本
- ソフトウェアの公式サイトからの情報収集

⑤日々巧妙化する標的型攻撃による諜報活動

世界各地で、政府機関や重要インフラ企業の機密情報を狙った標的型攻撃が多発している。政府機関情報セキュリティ横断監視・即応チーム(GSOC)によると、2013年の政府機関への脅威の件数は**約508万件**と、2012年比のおよそ**5倍**となっている。

国内でも、2014年6月には国産ワープロソフト「一太郎」の脆弱性を悪用したウイルスを送付する攻撃、9月には医療費通知や健康保険のお知らせメールを装い、**Word文書に偽装したウイルス**を送付する攻撃が報告されている。

その他にも、Webサイトを使った標的型攻撃である**水飲み場型攻撃**や、やり取りを通してウイルス入りの添付ファイルを開かせる**やり取り型攻撃**等、標的型攻撃の手法が日々巧妙化している。

GSOCセンサーで認知された政府機関への脅威の件数の推移



■ 図 1-2-5 GSOC センサーで認知された政府機関への脅威の件数の推移

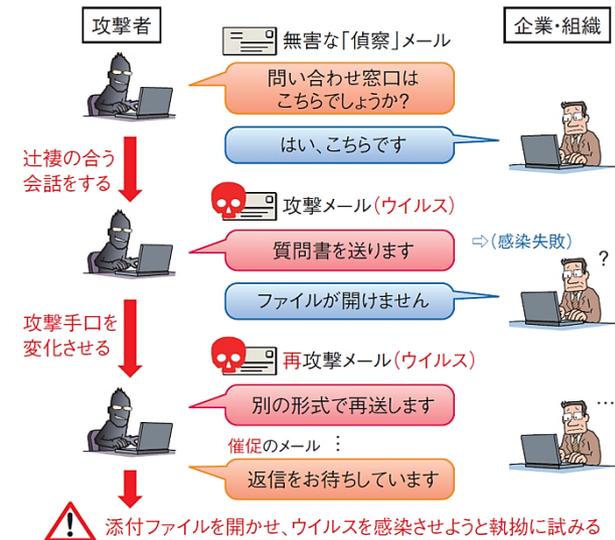
(出典) NISC^{*71}「サイバーセキュリティ政策に係る年次報告(2013年度)」^{*72}「政府機関における情報セキュリティに係る年次報告(平成24年度)」^{*73}を基に IPA が作成

Word文書に偽装したウイルスのイメージ



■ 図 1-3-7 拡張子が表示されないショートカットファイルの例

やり取り型攻撃のイメージ



■ 図 1-3-4 「やり取り型」攻撃のイメージ

⑥サイバー攻撃対処のための「通信の秘密」の解釈を明確化

総務省は、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ」を2014年4月に公表した。サイバー攻撃への対処において、IPアドレスやタイムスタンプ等の情報を知り、該当する利用者を割り出すことは通信の秘密を侵す行為だと考えられてきたが、「**利用者の有効な同意**」「**正当防衛**」「**緊急避難**」「**正当行為**」にあたるものについては、通信の秘密を侵す行為ではないと解釈を明確化した。

これを踏まえ、同年7月に「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」の修正を行い、第3版を公開した。

「通信の秘密」に関する課題と明確化した対処方法の例※

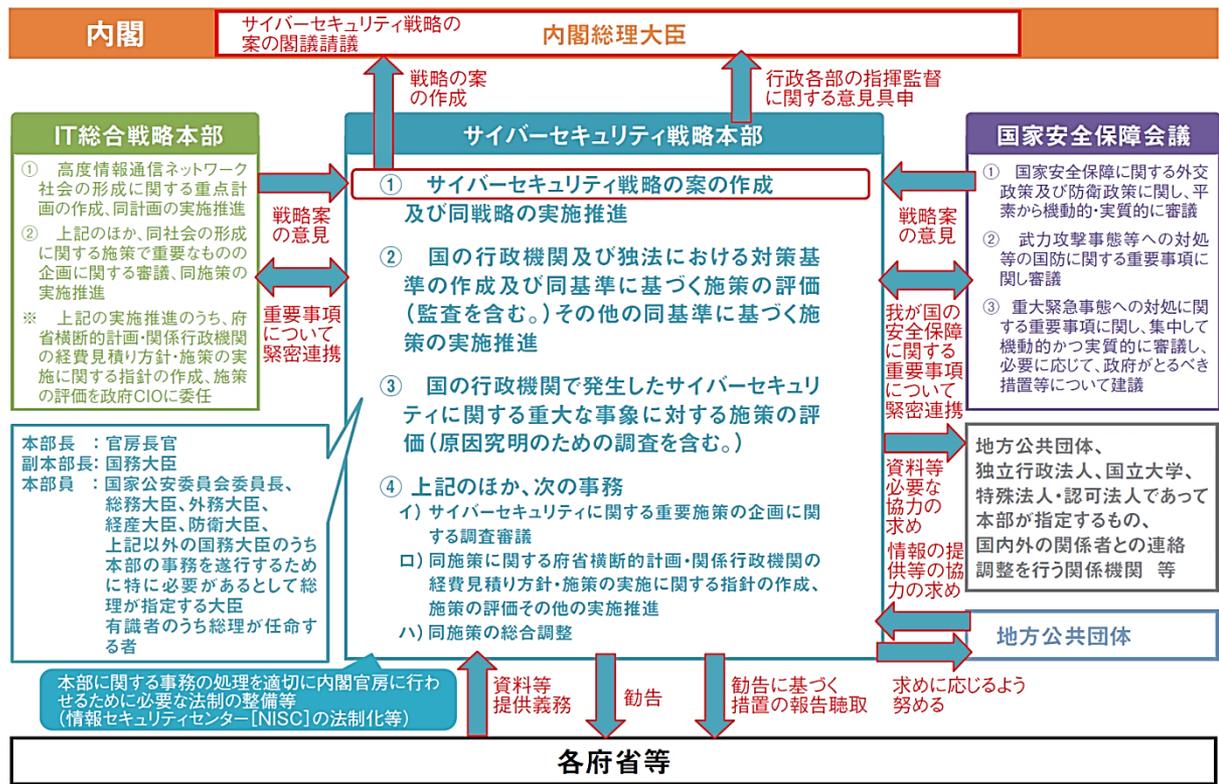
通信の秘密に関して解決すべき課題 (不明確だった点)	明確化した対処方法
利用者の通信先をチェックし、ウイルス配布サイトに接続しようとした場合に注意喚起しても良いかどうか	約款による事前の包括的な同意を得ることにより、利用者のアクセス先URL またはIP アドレスを確認することが可能
摘発した不正サーバに残った通信履歴を基にウイルス感染者に注意喚起することは可能かどうか	ウイルスを駆除するための「緊急避難」にあたり、通信の発信元IPアドレス及びタイムスタンプから利用者を割り出すことが可能
特定の条件の通信を検知して遮断することで、DNSAmP攻撃を予防することは可能かどうか	サービスを安定して提供するための「正当業務行為」にあたり、通信の宛先IP アドレス及びポート番号を常時確認することが可能

※本誌に掲載されている例の一部

⑦サイバーセキュリティ基本法の成立に伴うNISCの体制強化

2014年11月、日本においてサイバーセキュリティ基本法が成立した。同法に基づき2015年1月、国のサイバーセキュリティ戦略の策定・実施の司令塔として「**サイバーセキュリティ戦略本部**」が内閣に設置された。また、これまで実務を担ってきた「内閣官房情報セキュリティセンター」が、「**内閣サイバーセキュリティセンター**」(NISC)に改組され、機能が強化された。

サイバーセキュリティ戦略本部の機能・権限(イメージ)



■ 図 2-1-1 サイバーセキュリティ戦略本部の機能・権限(イメージ)
 (出典) NISC「[サイバーセキュリティ基本法]の概要^{*1)}」

⑧ J-CRAT（サイバーレスキュー隊）の正式発足、日本サイバー犯罪対策センター(JC3)の稼働等、サイバー攻撃への対応体制を整備

経済産業省は2014年7月、サイバー攻撃に気付いた組織に対する被害拡大と再発の防止・低減、標的型攻撃による謀報活動等の連鎖の遮断を図ることを主な目的として、**J-CRAT(サイバーレスキュー隊)**をIPAに発足させた。

また、2014年11月、サイバー空間の脅威に対処するため、**一般財団法人日本サイバー犯罪対策センター(JC3)**が業務を開始した。JC3は産業界、学術研究機関、捜査機関の間で、情報や知識・経験、ノウハウを共有し、協力を促進する。

JC3の活動概要

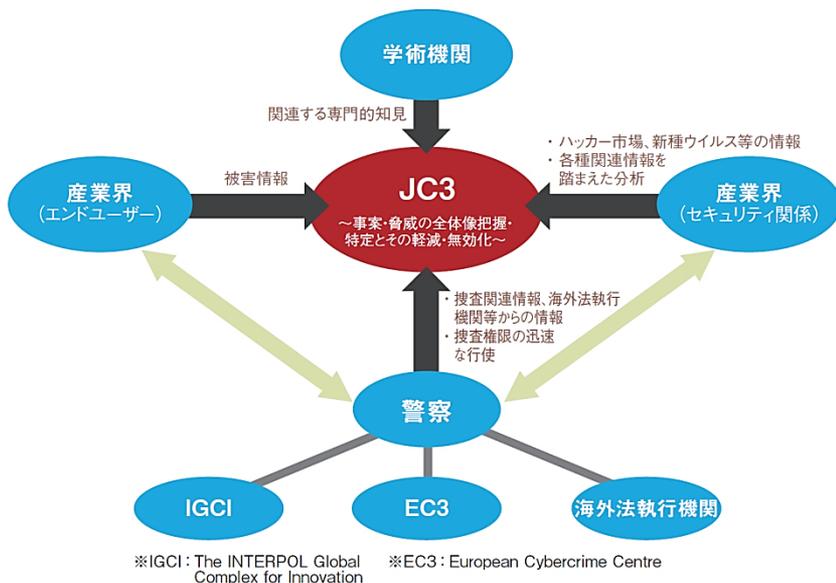


図 2-1-6 JC3 のスキームによる脅威への対応
 (出典)JC3「JC3のスキームによる脅威への対応」³⁷⁾

J-CRATの活動概要

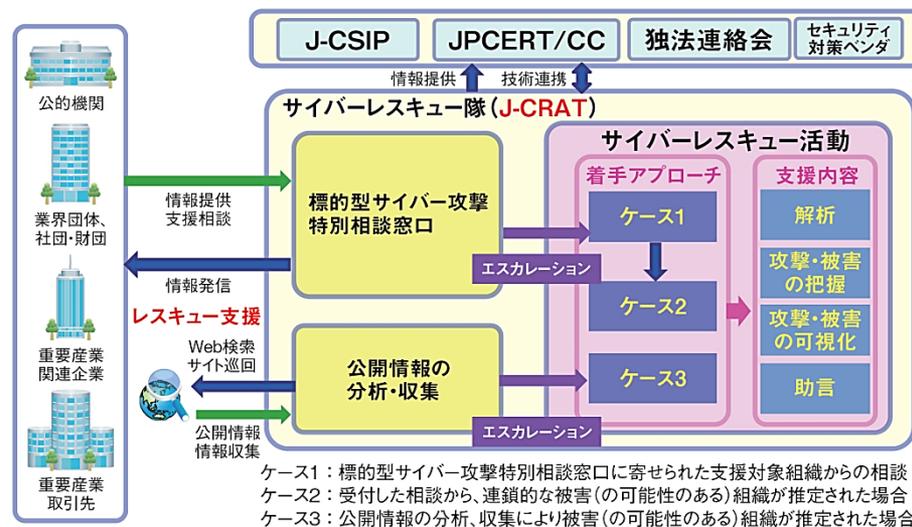
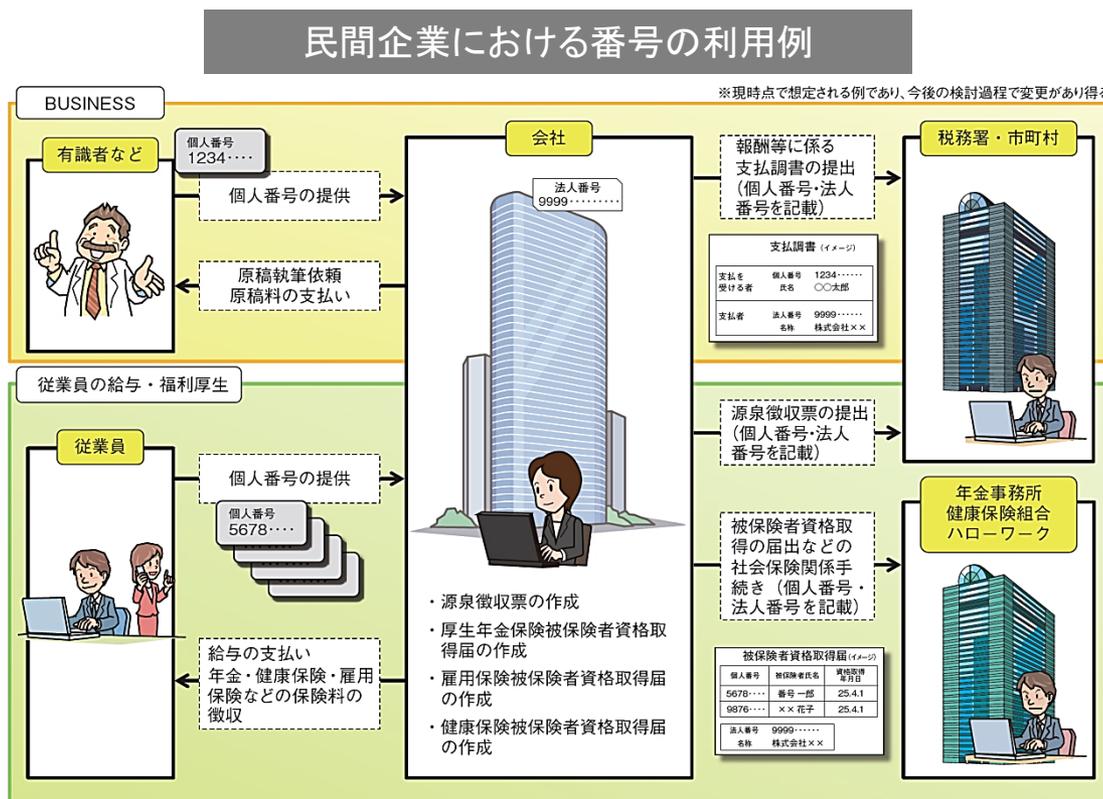


図 3-3-3 J-CRAT の活動概要

⑨ パーソナルデータ保護と利活用への取り組み、マイナンバー制度の準備が本格化

ビッグデータ活用による新たなビジネス創出が期待される中、2014年6月「パーソナルデータの利活用に関する制度改正大綱」で基本的な枠組みが公開されたが、その後多くの意見・提言を受けて、**2015年3月「個人情報保護法案」が国会に提出された。**

行政手続きのワンストップ化や効率性向上の実現に活用される**マイナンバー制度**については、**2015年10月より個人番号の通知、2016年1月から個人番号の行政による利用**を目指して、制度の整備、システムの構築が進んでいる。



■ 図 3-2-2 民間企業における番号の利用例

(出典) 内閣官房社会保障改革担当室、内閣府大臣官房番号制度担当室「マイナンバー-社会保障・税番号制度概要資料^{※41)}」を基に IPA が編集

⑩ IoTの情報セキュリティ

インターネットやモバイル通信等に関連する様々な機器が小型化・高性能化してきたことによって、あらゆるモノがネットワークに接続する「モノのインターネット」(Internet of Things : IoT)の時代が到来している。

IoTの普及には、攻撃にさらされる機会の増加、セキュリティが考慮されていない機器やアップデートされない機器の存在、セキュリティレベルの不統一といった**数々の問題点が認識**されている。IoTは、人の生命や財産に関わるサービスにも拡大していく可能性があるため、社会基盤として安全・安心に利用できる環境が求められている。

IoTとビッグデータが実現する様々なサービス

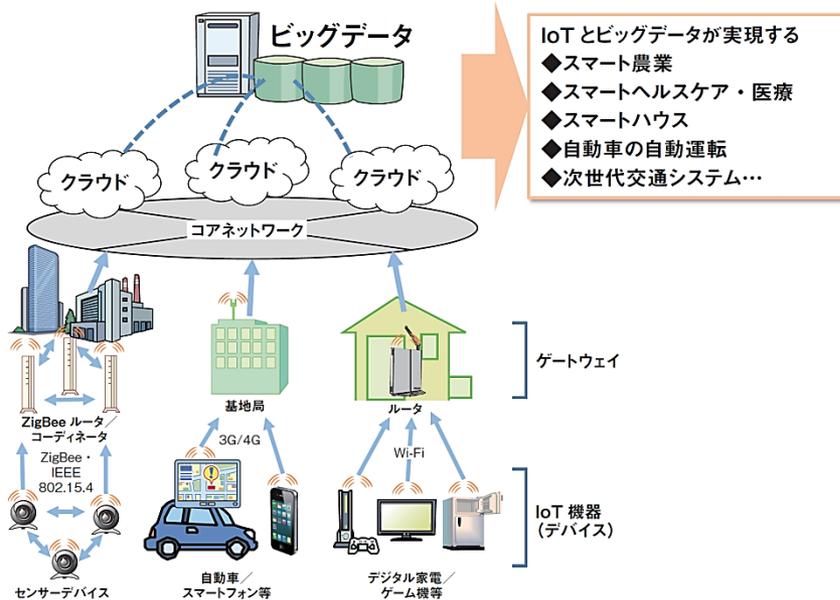


図 3-7-1 IoTとビッグデータが実現する様々なサービス

想定されるIoTのセキュリティ上の問題点

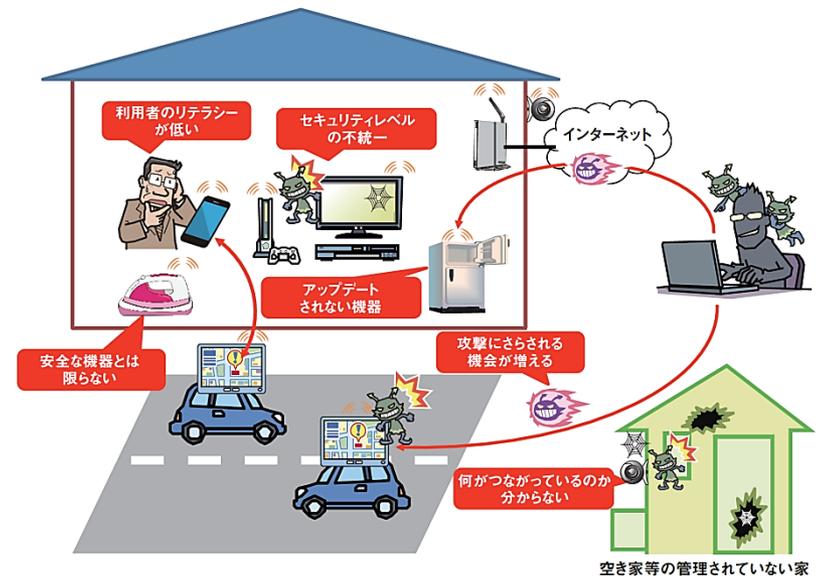


図 3-7-2 想定されるIoTのセキュリティ上の問題点

● 目次構成

1.1 2014年度に観測されたインシデント状況

- 1.1.1 世界における情報セキュリティインシデント状況
- 1.1.2 国内における情報セキュリティインシデント状況

1.2 情報セキュリティインシデント別の状況と事例

- 1.2.1 広く普及しているソフトウェアの脆弱性
- 1.2.2 活動妨害を狙った攻撃
- 1.2.3 インターネットバンキングを狙った攻撃
- 1.2.4 個人情報の大量取得を狙った攻撃
- 1.2.5 政府関連・重要インフラの機密情報を狙った攻撃
- 1.2.6 オンライン詐欺
- 1.2.7 アップデートを悪用した攻撃
- 1.2.8 内部者による情報の流出

1.3 攻撃・手口の動向と対策

- 1.3.1 広く普及しているソフトウェアの脆弱性を悪用する攻撃
- 1.3.2 巧妙化する標的型攻撃
- 1.3.3 ゼロデイ攻撃

1.3.4 DDoS攻撃

1.3.5 インターネットバンキングを狙った攻撃

1.3.6 オンライン詐欺

1.3.7 パスワードリスト攻撃

1.3.8 アップデートを悪用した攻撃

1.4 情報システムの脆弱性の動向

1.4.1 脆弱性対策情報の登録状況

1.4.2 脆弱性の状況

1.5 情報セキュリティ対策の状況

1.5.1 企業における対策状況

1.5.2 政府における対策状況

1.5.3 地方公共団体における対策状況

1.5.4 教育機関における対策状況

1.5.5 一般利用者における対策状況

● 目次構成

2.1 日本の情報セキュリティ政策の状況

- 2.1.1 政府全体の政策動向
- 2.1.2 経済産業省の政策
- 2.1.3 総務省の政策
- 2.1.4 警察におけるサイバー犯罪対策
- 2.1.5 電子政府システムの安全性確保への取り組み
- 2.1.6 防衛省のサイバー空間での取り組み

2.2 情報セキュリティ関連法の整備状況

- 2.2.1 サイバーセキュリティ基本法の成立
- 2.2.2 個人情報保護に関する法律の改正
- 2.2.3 不正競争防止法の改正
- 2.2.4 サイバーセキュリティ関連の輸出規制

2.3 国別・地域別の情報セキュリティ政策の状況

- 2.3.1 国際社会と連携した取り組み
- 2.3.2 米国のセキュリティ政策
- 2.3.3 欧州のセキュリティ政策
- 2.3.4 アジア各国におけるセキュリティへの取り組み

2.4 情報セキュリティ人材の現状と育成

- 2.4.1 情報セキュリティ人材の育成に関する政策と取り組み事例
- 2.4.2 情報セキュリティ人材に求められるスキル
- 2.4.3 情報セキュリティ人材育成のための活動
- 2.4.4 大学を中心とした取り組み
- 2.4.5 各国における人材育成の動向

2.5 情報セキュリティマネジメント

- 2.5.1 情報セキュリティマネジメント対策の実施状況
- 2.5.2 情報セキュリティマネジメントの制度と規格
- 2.5.3 米国サイバーセキュリティフレームワークの状況
- 2.5.4 その他の情報セキュリティマネジメント関連規格

● 目次構成

2.6 国際標準化活動

- 2.6.1 様々な標準化団体の活動
- 2.6.2 情報処理関係の規格の標準化（ISO/IEC JTC 1/SC 27）
- 2.6.3 工業通信ネットワーク-ネットワーク及びシステムセキュリティ（IEC 62443）
- 2.6.4 インターネットコミュニティによる標準化（IETF）
- 2.6.5 信頼性の高いコンピューティング環境の実現に向けたセキュリティ標準（TCG）

2.7 評価認証制度

- 2.7.1 ITセキュリティ評価及び認証制度
- 2.7.2 スマートカードの評価認証
- 2.7.3 暗号モジュール試験及び評価認証制度

2.8 情報セキュリティの普及啓発活動

- 2.8.1 政府の普及啓発活動
- 2.8.2 一般国民向けの普及啓発活動
- 2.8.3 企業・組織に対する普及啓発活動
- 2.8.4 児童生徒向けの普及啓発活動

2.9 情報セキュリティ産業の規模と成長の動向

- 2.9.1 日本の情報セキュリティ産業の規模
- 2.9.2 サイバー保険

2.10 その他の情報セキュリティの状況

- 2.10.1 デジタル・フォレンジック
- 2.10.2 クラウドコンピューティングのセキュリティ
- 2.10.3 暗号技術の動向

● 目次構成

3.1 組織における内部不正の現状と対策の動向

- 3.1.1 海外の内部不正の動向
- 3.1.2 国内の内部不正の動向
- 3.1.3 内部不正防止への取り組み
- 3.1.4 営業秘密保護に関する取り組み

3.2 個人情報保護法改正とマイナンバー制度

- 3.2.1 パーソナルデータ保護
- 3.2.2 社会保障・税番号（マイナンバー）制度
- 3.2.3 まとめ

3.3 深刻化する標的型攻撃に対抗する取り組み

- 3.3.1 J-CSIP（サイバー情報共有イニシアティブ）
- 3.3.2 脅威と対策研究会
- 3.3.3 J-CRAT（サイバーレスキュー隊）

3.4 スマートデバイスの情報セキュリティ

- 3.4.1 スマートデバイスの普及状況
- 3.4.2 スマートデバイス利用時の被害事例
- 3.4.3 スマートフォン上でのワンクリック請求
- 3.4.4 スマートフォンのセキュリティに関する取り組み
- 3.4.5 「SIMロック解除」の義務化に関する動向

3.5 自動車の情報セキュリティ

- 3.5.1 2014年度の研究事例
- 3.5.2 英国におけるイモビライザのハッキング
- 3.5.3 米国における自動車の脅威情報共有の取り組み
- 3.5.4 日本における運転支援システムへのセキュリティの取り組み
- 3.5.5 自動車セキュリティ専門会議の広がり
- 3.5.6 今後の見通し

3.6 制御システムの情報セキュリティ

- 3.6.1 制御システムの概要
- 3.6.2 制御システムの脆弱性とインシデント事例
- 3.6.3 米国における制御システムセキュリティの動向
- 3.6.4 国内における制御システムセキュリティの動向

3.7 IoTの情報セキュリティ

- 3.7.1 IoTでつながる世界
- 3.7.2 IoTのセキュリティ
- 3.7.3 標準化に向けた取り組み
- 3.7.4 安全なIoTを使ったサービスの活用に向けて