IPA Better Life with IT

情報セキュリティ白書2016

今そこにある脅威：意識を高め実践的な取り組みを

概要説明資料

2016年7月14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2016

今そこにある脅威：意識を高め実践的な取り組みを

情報セキュリティの動向を広くカバーした一冊

■2015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

■重要インフラやサイバー・フィジカル・システムの安全性、自動車・制御システム・IoT・スマートデバイスの情報セキュリティ等の重要なテーマを解説

2016年7月15日発売

◆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

発行：IPA
ISBN：978-4-905318-41-5
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）

IPA

全体構成

- **第Ⅰ部　情報セキュリティの概要と分析**
  - 序章　2015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2016** ～個人と組織で異なる脅威、立場ごとに適切な対応を～

- 付録　資料・ツール
- 第11回 IPA「ひろげよう情報モラル・セキュリティコンクール」2015 受賞作品
- コラム

2015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
データ侵害の件数は2014年と同水準の推移。個人情報の漏えい件数は前年比23%増の4億2,900万件。過去最多となる9件の大規模漏えい事件が発生。

ゼロデイ脆弱性
攻撃者に悪用されるゼロデイ脆弱性が2014年の2倍以上の54件と過去最多。

ランサムウェアの増加
パソコンやスマートフォンなどのデータを人質に身代金を要求するランサムウェアが2014年の1.5倍に増加。暗号化型のランサムウェアの割合が73%に急増。

序章　2015年度の情報セキュリティの概況～10の主な出来事～

2015年4月から2016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 標的型攻撃により日本年金機構から個人情報が流出（1.2.5）（1.3.2）
② インターネットバンキングの不正送金、被害額は過去最悪を更新（1.2.3）（1.3.5）
③ オンライン詐欺・脅迫被害が拡大（1.2.6）（1.2.7）（1.3.6）（1.3.7）
④ 広く普及しているソフトウェアの脆弱性が今年も問題に（1.2.1）（1.3.1）
⑤ DDoS攻撃の被害が拡大、IoT端末が狙われる（1.2.2）（1.3.4）
⑥ 重要インフラへの攻撃と重要インフラのセキュリティを強化する国内の取り組み（2.1.1）（2.1.2）（3.3）
⑦ 法改正による政府機関のセキュリティ強化（2.2.2）
⑧ 企業のセキュリティ強化に経営層の参画が重要（1.5.1）（2.1.2）
⑨ セキュリティ人材育成への取り組み（2.4）
⑩ 自動車・IoTのセキュリティ脅威が高まる（3.2）（3.4）

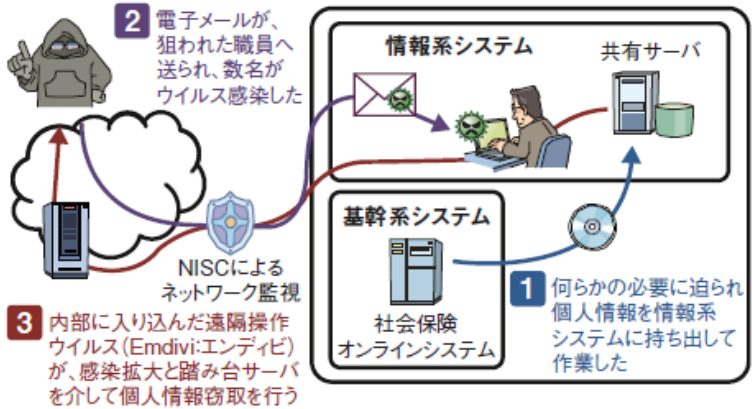
※末尾の項番号は、「情報セキュリティ白書2016」のもの。

①標的型攻撃により日本年金機構から個人情報が流出

2015年6月、日本年金機構の職員が利用する複数の端末がウイルスに感染し、**約125万件の個人情報の流出が発覚**。複数回に分けて添付ファイル付きのメールや外部URLが記されたメールが送付され、これらのメールを職員が開封、実行したことが感染の原因とされた。

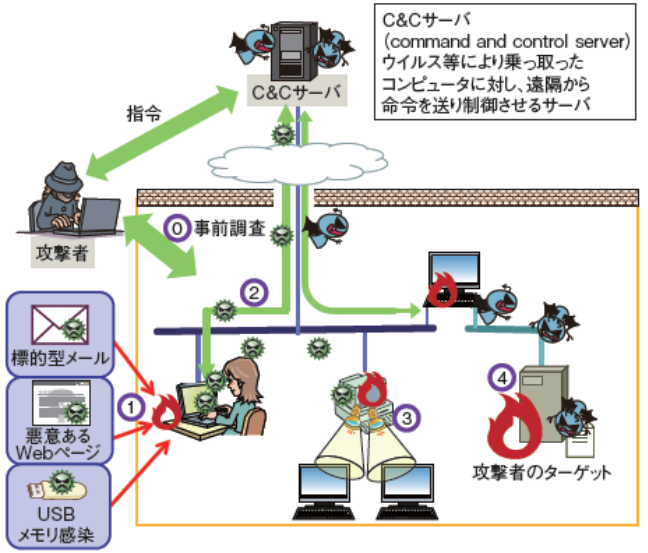
同時期に、**外部組織からの指摘**により類似したウイルスの感染が発覚した事例が多数公表された。標的型攻撃は**ますます巧妙化**しており、有効な対策の導入やインシデントの発覚時に適切に対応可能な体制が求められている。

日本年金機構の情報流出経路



■図 1-2-7　情報の流出経路
(出典)株式会社ラック「日本年金機構の情報漏えい事件から、我々が得られる教訓※93」を基に IPA が編集

標的型攻撃の流れ※



※本誌図1-3-3より一部抜粋

②インターネットバンキングの不正送金、被害額は過去最悪を更新

インターネットバンキングを狙った攻撃による不正送金の被害件数は減少したが、**被害額は過去最悪の約30億7,300万円に達した**。2015年の被害金融機関は、**信用金庫や信用組合等に拡大している**。原因の一つとして、警察庁が一般社団法人全国銀行協会等、金融関係の9団体に対策強化を要請したことで、対策を強化した地方銀行から標的が移ったものと推測される。

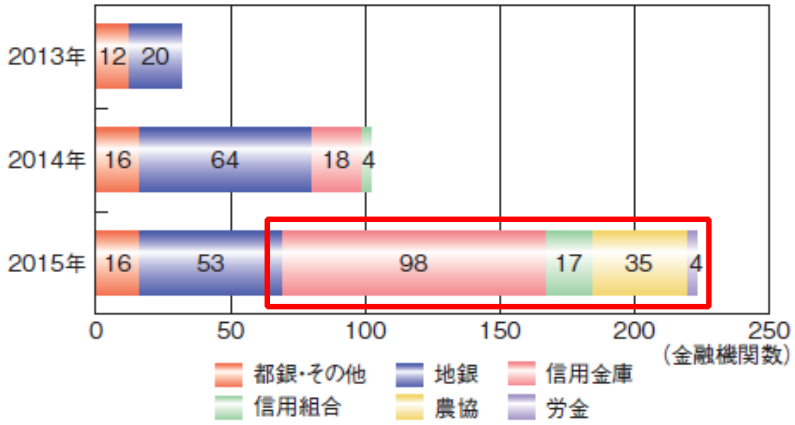
インターネットバンキングを狙った「WERDLOD」等のウイルスは引き続き検出されており、継続的なウイルス対策が必要である。

不正送金の被害件数と被害額

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
2015 年	1,495 件	30 億 7,300 万円

■表 1-2-2　不正送金の被害件数と被害額
（出典）警察庁発表※58 を基に IPA が作成

被害金融機関数の推移



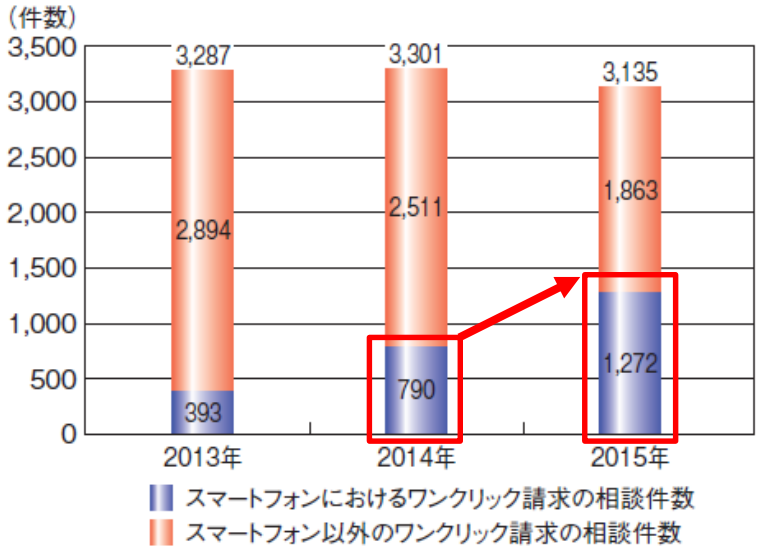
■図 1-2-5　被害金融機関数の推移
（出典）警察庁「平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」を基に IPA が編集

③オンライン詐欺・脅迫被害が拡大

2015年も引き続き「ワンクリック請求」についての相談が多く寄せられ、特に**スマートフォンにおける被害相談が増加傾向**にある。

感染すると画面ロックやデータを暗号化することでパソコン等を使用不可にし、復旧のために身代金を支払うように脅迫する**ランサムウェアの被害も拡大**している。これまでは海外での感染が多く報告されていたが、2016年3月には**前月の約5.6倍もの相談**がIPAに寄せられており、日本国内での被害の増加が懸念される。

ワンクリック請求の相談件数



■図 1-2-9　IPA に寄せられたワンクリック請求の相談件数

ランサムウェアの画面例

■図 3-5-3　日本語表示に対応した Android 版ランサムウェア
(出典)トレンドマイクロ株式会社「日本語表示に対応したモバイル版ランサムウェアを初確認、既に国内でも被害[※68]」

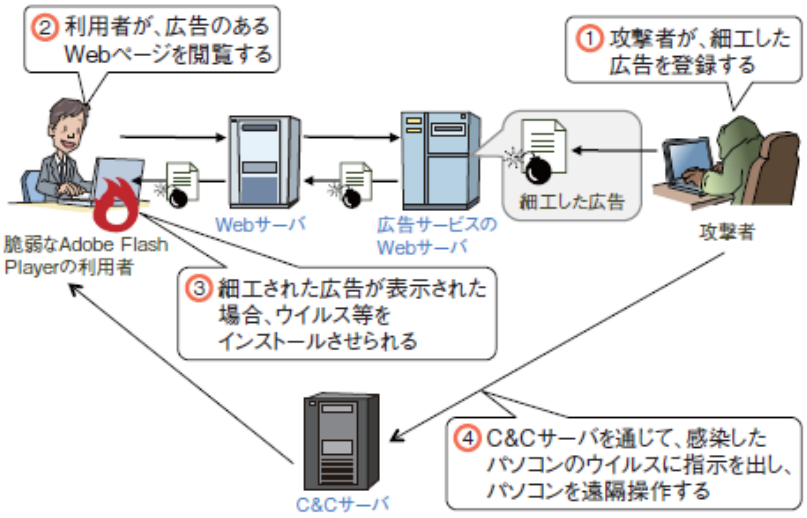
④広く普及しているソフトウェアの脆弱性が今年も問題に

2015年度はAdobe Flash PlayerやWordPress等の広く普及しているソフトウェアで多数の脆弱性が発見・公開された。

特に、Adobe Flash Playerは2015年に**339件もの脆弱性が公開された**。そのうち10件は修正プログラムが公開されておらず、**実際にゼロデイ攻撃で悪用された**。CMS※の一つであるWordPressも世界中のWebサイトで数多く利用されており、脆弱性が発見されたために多くのWebサイトが影響を受けた。利用者やWebサイトの管理者は最新の脆弱性情報を入手し、対策を講じる必要がある。

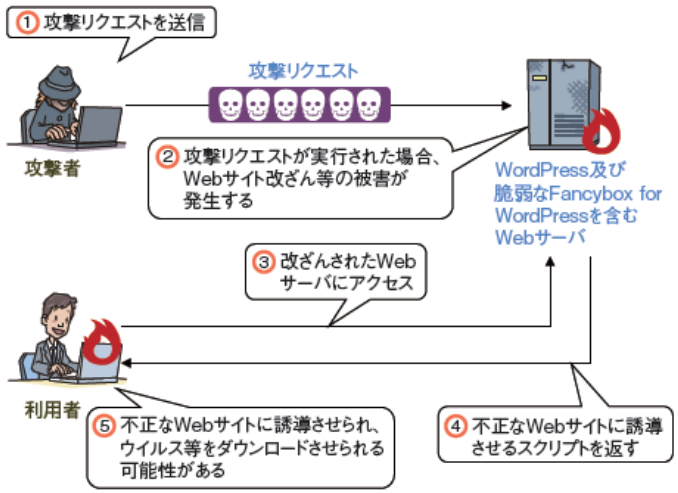
※CMS（Content Management System）

Adobe Flash Playerの脆弱性の悪用イメージ



■図 1-3-1　Adobe Flash Player の脆弱性を悪用した攻撃のイメージ

WordPressの脆弱性の悪用イメージ



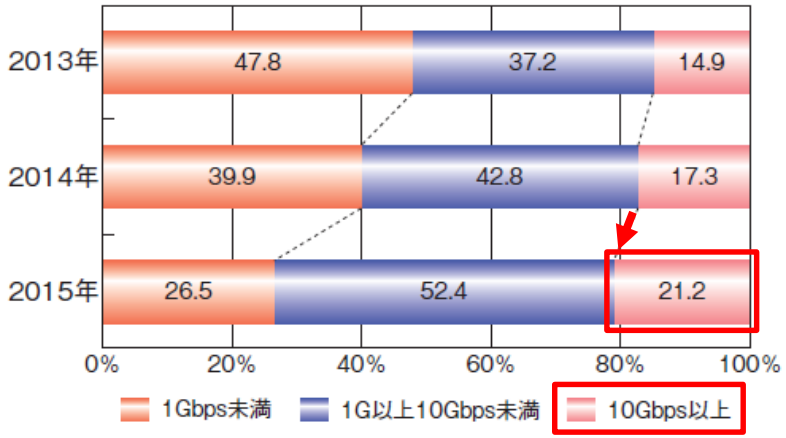
■図 1-3-2　Fancybox for WordPress の脆弱性を悪用した攻撃のイメージ

⑤DDoS攻撃の被害が拡大、IoT端末が狙われる

2015 年は、2014 年に比べ**2 倍近くのDDoS 攻撃が観測された**。 DDoS攻撃の攻撃規模は年々増加傾向にあり、10Gbps を超える通信量の攻撃が全体の20% 以上にまで増加している。アノニマスは、世界中の様々な組織に対しDDoS攻撃を仕掛けており、国内の複数の機関がその被害に遭っている。

2015 年10 月、ネットワークに接続された**監視カメラがボットネットを形成し、クラウドサービスにDDoS攻撃を行っていた**ことが確認された。 IoT 機器やスマートフォン等のデバイスを悪用した大規模なDDoS 攻撃が今後想定される。対策の検討が急務である。

DDoS攻撃の攻撃規模



■図 1-2-1　DDoS 攻撃の攻撃規模
(出典)CDNetworks「2016年度版DDoS攻撃の動向と今後の見通し※46」を基に IPA が編集

アノニマスによるDDoS攻撃の被害にあったWebサイト

日時	被害に遭った Web サイト
2015 年 9 月	和歌山県太地町
2015 年 10 月	成田空港、中部空港
2016 年 1 月	日産自動車株式会社
2016 年 1 月	警察庁
2016 年 2 月	国税庁

■表 1-2-1　アノニマスにより被害に遭ったと報じられた組織(一部)※50

⑥重要インフラへの攻撃と重要インフラのセキュリティを強化する国内の取り組み

重要インフラを狙う攻撃が世界各国で観測された。例えば、2015年12月、ウクライナで複数の電力事業者がサイバー攻撃を受け、**3～6時間にわたり電力供給が停止**した。

重要インフラのセキュリティを強化するためには**ガイドラインや情報連携の仕組み**を整備し、**官民連携**で具体的なセキュリティ対策を迅速に進める必要がある。

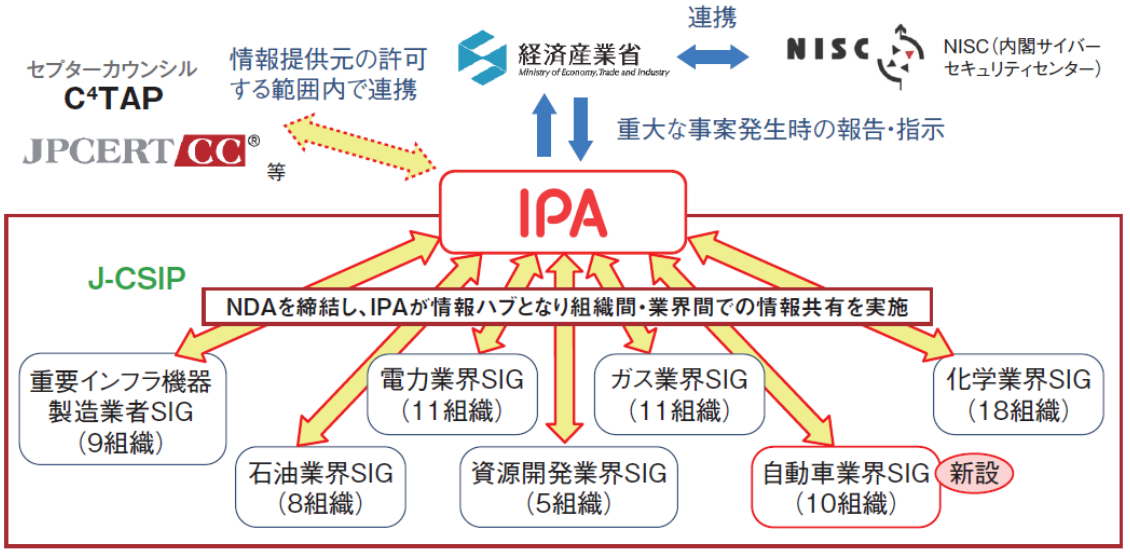
国内では、**J-CSIP※により重要インフラに関する標的型攻撃の情報共有**が行われている。

※J-CSIP（Initiative for Cyber Security Information Sharing Partnership of Japan：サイバー情報共有イニシアティブ）

政府機関による重要インフラのセキュリティを強化するための施策

策定機関	策定した指針、対策名	策定時期
サイバーセキュリティ戦略本部	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第4版）	2015 年 5 月
資源エネルギー庁（経済産業省）	電力分野のサイバーセキュリティ対策について	2016 年 2 月

J-CSIP（サイバー情報共有イニシアティブ）：官民連携による標的型攻撃への対策

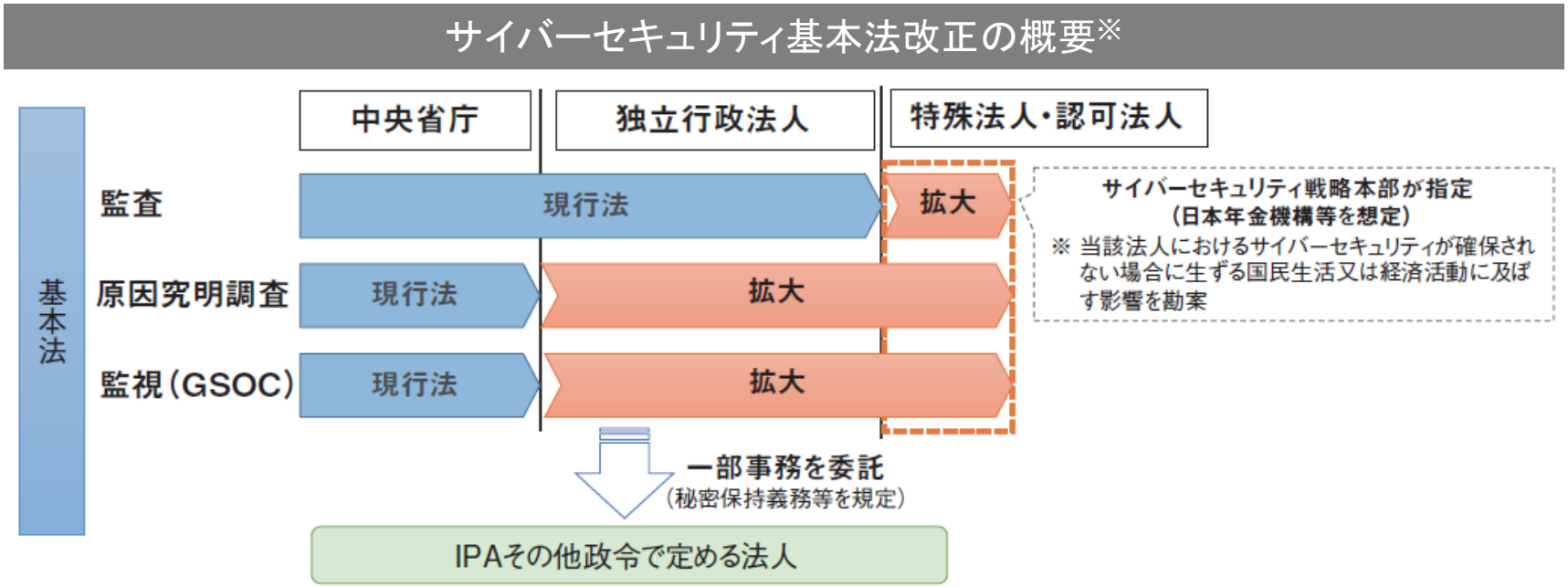


■図 2-1-5　J-CSIP の体制全体図

⑦法改正による政府機関のセキュリティ強化

日本年金機構における個人情報の漏えい等を受け、政府は、サイバーセキュリティ基本法及び情報処理の促進に関する法律の改正案を国会に提出し、2016 年4 月、同法が成立した。

同改正により、政府機関に対する**監視及び調査等の対象範囲が独立行政法人及び指定法人に拡大され、監査等の対象範囲が指定法人に拡大された**。深刻化するサイバー攻撃等に備え、政府機関のサイバーセキュリティ対策の強化が期待される。



■図 2-2-1　サイバーセキュリティ基本法及び情報処理の促進に関する法律の改正の概要
（出典）NISC「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案の概要※61」

※本誌図2-2-1より一部抜粋

⑧ 企業のセキュリティ強化に経営層の参画が重要

企業の経営層が経営課題としてサイバーセキュリティ強化に取り組む必要がある中、経済産業省とIPAは、**経営層がCISO※等に指示すべきセキュリティ対策**をまとめ、「**サイバーセキュリティ経営ガイドライン**」として2015 年12 月に公開した。

IPA の調査によれば、日本の**CISO 設置企業の割合は欧米と比較して低く**、CISO の任命やその社内認知について、欧米企業の水準に及んでいない状況である。

※CISO（Chief Information Security Officer：最高情報セキュリティ責任者）

サイバーセキュリティ経営ガイドラインの構成

1. 経営者が認識すべき3原則

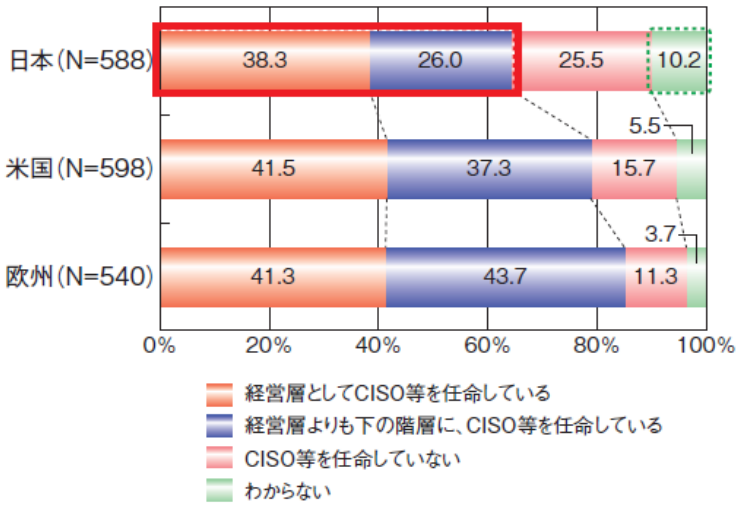
（1）経営者は、IT 活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
（2）自社は勿論のこと、系列会社やサプライチェーンのビジネスパートナー、IT システム管理の委託先を含めたセキュリティ対策が必要
（3）平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

2. 経営者がCISO等に指示をすべき10の重要事項

リーダーシップの表明と体制の構築	（1）サイバーセキュリティリスクの認識、組織全体での対応の策定
	（2）サイバーセキュリティリスク管理体制の構築
サイバーセキュリティリスク管理の枠組み決定	（3）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
	（4）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
	（5）系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握
リスクを踏まえた攻撃を防ぐための事前対策	（6）サイバーセキュリティ対策のための資源（予算、人材等）確保
	（7）ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
	（8）情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
サイバー攻撃を受けた場合に備えた準備	（9）緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
	（10）被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

■図 2-1-3　サイバーセキュリティ経営ガイドラインの構成
（出典）経済産業省／ IPA「サイバーセキュリティ経営ガイドライン」を基に IPA が作成

CISO等の任命状況



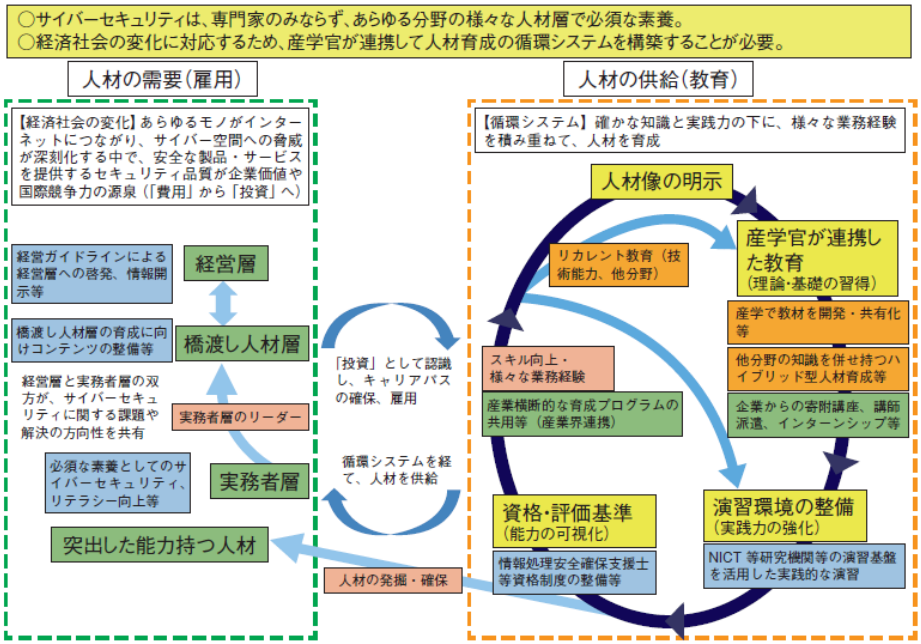
■図 1-5-4　CISO 等の任命状況
（出典）IPA「企業の CISO や CSIRT に関する実態調査 2016」を基に作成

⑨セキュリティ人材育成への取り組み

サイバーセキュリティ戦略本部は「**サイバーセキュリティ人材育成総合強化方針**」を2016年3月に決定した。

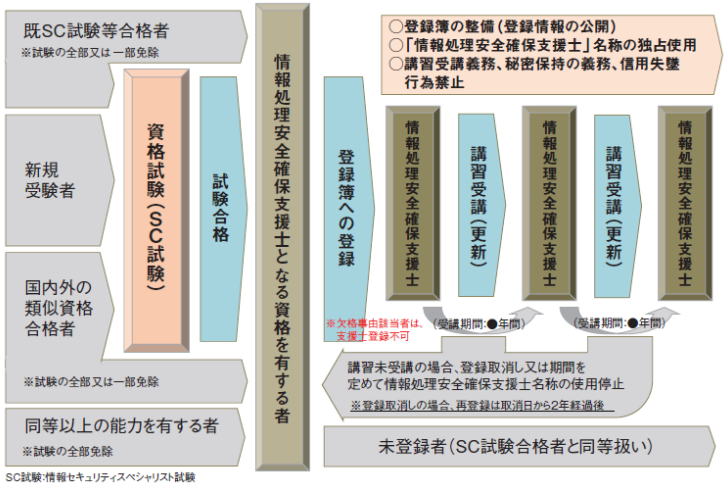
また、企業における情報セキュリティマネジメント人材を育成するため、2015 年10月に「**情報セキュリティマネジメント試験**」が創設された。さらに2016 年4 月の情報処理の促進に関する法律の改正により、サイバーセキュリティへの助言を行う国家資格「**情報処理安全確保支援士**」の新設が決定した。

サイバーセキュリティ人材育成総合強化方針



■図 2-4-2　社会で活躍できる人材の育成
(出典)NISC「サイバーセキュリティ人材育成総合強化方針」

情報処理安全確保支援士制度



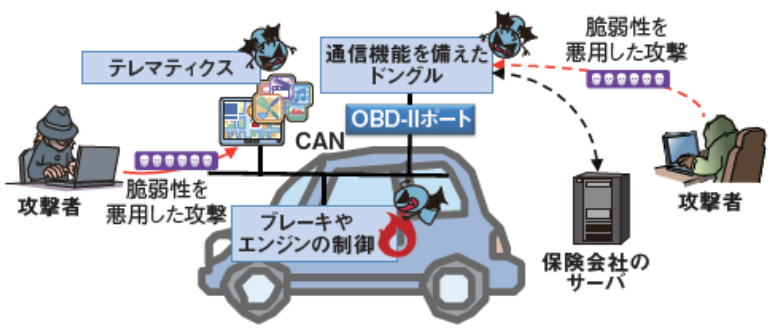
■図 2-4-4　情報処理安全確保支援士（情確士）制度の全体像
(出典)経済産業省「情報処理安全確保支援士制度（案）[※126]」

⑩ 自動車・IoTのセキュリティ脅威が高まる

2015 年度は、**自動車の遠隔操作が可能となる脆弱性や攻撃手法**がBlack Hat USA 2015及びDEF CON 23 において報告された。今後自動運転の技術開発が進み、自動車がソフトウェアにより制御されるようになれば、自動車を標的にした攻撃の増加が予想される。

IoT（Internet of Things）の利活用に向けては、官民を挙げた取り組みが始まっている。2015年10月には**IoT推進コンソーシアム**が設立され、**IoTセキュリティガイドライン**を策定中である。IoT機器は**設定不備のままで運用**されることも多く、ガイドラインを適切に策定・周知し、遵守状況をチェックする体制の構築が必要である。

自動車のセキュリティ脅威



■図 3-2-1　自動車への攻撃のイメージ

IoTセキュリティガイドラインの対象と内容

		供給者		利用者	
		機器メーカ	サービス提供者（SIer、インストーラ）	企業利用者	一般利用者
プラットフォーム（データセンタ、データ分析）		総務省ガイドライン／経産省ガイドライン クラウドセキュリティガイドラインと連携			
ネットワーク	インターネット	【議題2】IoT サービスの提供者・利用者が機器をネットワークに接続する際、遵守もしくは留意すべき事項		【議題1】セキュリティ対策を行う上での、組織的改善事項（CSMS をベースに検討）	【議題2】一般利用者がIoT サービス・機器を利用する際に最低限留意すべき事項
	狭域ネットワーク				
機器	通信機能	【議題1】IoT 機器が満たすべきセキュリティ・セーフティ・リライアビリティに関して、設計・開発時に留意すべき推奨事項			
	ハードウェア				
	ソフトウェア（OS、ミドルウェア、アプリ等）				
	本来機能				

■表 3-4-2　IoT セキュリティガイドラインの内容と対応
（出典）IoT 推進コンソーシアム「IoT セキュリティワーキンググループで検討するガイドラインの対象と内容について※43」

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

目次構成

第2章 情報セキュリティを支える基盤の動向

目次構成

第2章 情報セキュリティを支える基盤の動向

目次構成

第3章 個別テーマ

目次構成