IPA Better Life with IT

# 情報セキュリティ白書2017

## 広がる利用、見えてきた脅威：つながる社会へ着実な備えを

概要説明資料

2017年8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2017

## 広がる利用、見えてきた脅威：つながる社会へ着実な備えを

## 情報セキュリティの動向を広くカバーした一冊

■2016年度に情報セキュリティの分野で起きた
注目すべき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

■制御システム、IoT、スマートデバイス、Fintech、
オリンピックなど、2016年に注目された出来事、
分野の情報セキュリティについて解説

2017年7月1日発売


◆入手先：Amazon
全国官報販売組合
IPA　※全国の書店からも購入できます
電子書籍版は2017年8月、Amazon Kindleストア、
楽天Kobo等より発売

発行：IPA
ISBN：978-4-905318-53-8
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

- 情報セキュリティの概要と分析
  - 序章 2016年度の情報セキュリティの概況（年表）
  - 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

- 付録　情報セキュリティ10大脅威2017・資料・ツール
  - 情報セキュリティ10大脅威2017
  - 資料A 2016年のコンピュータウイルス届出状況
  - 資料B 2016年のコンピュータ不正アクセス届出状況
  - 資料C ソフトウェア等の脆弱性関連情報に関する届出状況
  - ツール

- 第12回 IPA「ひろげよう情報モラル・セキュリティコンクール」2016 受賞作品

# 序章　2016年度の情報セキュリティの概況

2016年4月から2017年3月を対象に、情報セキュリティに関する主なインシデントや実施された政策・制度について年表を示すとともに、概況を述べる。

## 参考：2016年度の主な情報セキュリティインシデント・事件

標的型攻撃、ランサムウェア被害、DDoS攻撃、Web改ざん等の攻撃は通年で発生

| | 主な情報セキュリティインシデント・事件 |
|---|---|
| 2016年　6月 | 旅行会社グループ企業に標的型攻撃（1.2.3（4））|
| 7月 | ランサムウェアの被害相次ぐ（1.2.9、1.3.6） |
| 8月 | リオデジャネイロオリンピック開催への抗議活動（1.2.1（2））<br>家電量販店運営のECサイトへのDDoS攻撃（1.2.1（2）） |
| 9月 | Miraiによる大規模なDDoS攻撃が発生（1.2.1（1）、1.3.2（3）、3.2.1（1）） |
| 10月 | 大学関連施設が標的型攻撃の被害を公表（1.2.4（1）、1.5.4（1）） |
| 11月 | 経団連が標的型攻撃の被害を公表（1.2.4（2）） <br>米国大統領選挙においてロシアが選挙妨害（2.3.2（4）） |
| 12月 | ウクライナ、キエフ北部でサイバー攻撃による大規模停電が発生（3.1.2） |
| 2017年　2月 | WordPressの脆弱性を悪用したWeb改ざんが多発（1.2.2、1.3.2（2）） |
| 3月 | Apache Struts2の脆弱性を悪用した攻撃が多発（1.2.3（1）、1.3.2（2）） |

※末尾の項番号は、「情報セキュリティ白書2017」のもの。

# 序章　2016年度の情報セキュリティの概況

## 参考：2016年度の主な情報セキュリティ政策・イベント

| | 主な情報セキュリティ政策・イベント |
|---|---|
| 2016年　5月 | 伊勢志摩サミット共同宣言（2.3.1（4））|
| 8月 | リオデジャネイロオリンピック開催（3.5）<br>サイバーセキュリティ戦略の年次計画「サイバーセキュリティ2016」の公開（2.1.1（1））<br>「安全なIoTシステムのためのセキュリティに関する一般的枠組」の発表（2.1.1（1）、3.2.2（1））<br>EUで重要インフラ保護のためのNIS指令の施行（2.3.3（2））|
| 10月 | 情報処理安全確保支援士制度開始（2.4.2（2））<br>改正サイバーセキュリティ基本法の施行（1.5.2、2.4.2（2）、2.5.3（3））|
| 11月 | 個人情報の保護に関する法律についてのガイドラインの公開（2.2.1（2））|
| 12月 | EUで一般データ保護規則（GDPR）ガイドライン公開（2.2.1（3）、2.3.3（3）（4））<br>「サイバーセキュリティ経営ガイドラインVer1.1」及び解説書の公開（2.1.2（1）（2））|
| 2017年　1月 | 米国トランプ政権成立（2.3.2（5））|
| 2月 | 中小企業の情報セキュリティ対策普及の加速化に向けた共同宣言（2.8.2）|
| 3月 | 第四次産業革命に関する日独共同宣言（ハノーバー宣言）の発表（2.3.1（2））|

※NIS指令：The Directive on security of network and information systems.

※末尾の項番号は、「情報セキュリティ白書2017」のもの。

# ① 標的型攻撃による被害が継続

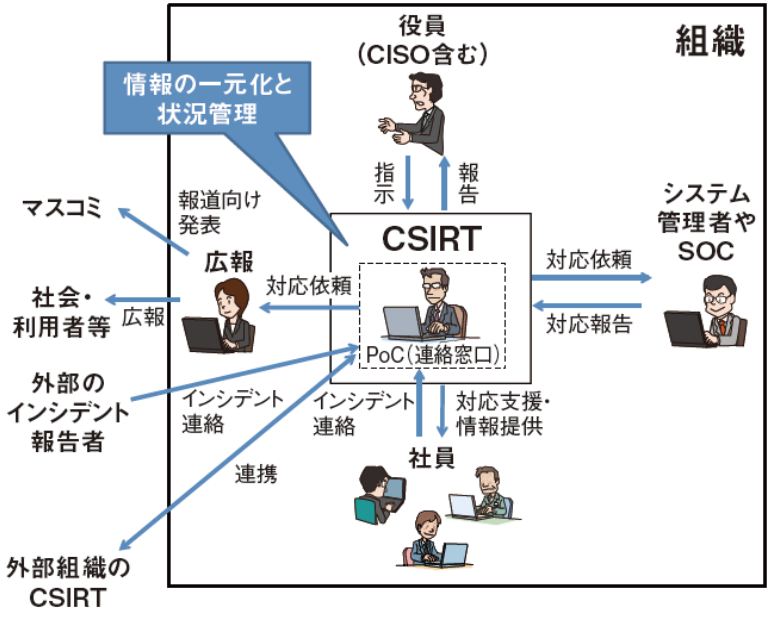
2015年6月の日本年金機構での個人情報の流出事件以降も、**標的型攻撃による被害が継続**している。複数回に分けて添付ファイル付きのメールや外部URLが記されたメールが送付され、これらのメールを受信者が開封、実行したことによる感染が原因と考えられる。

標的型攻撃は**ますます巧妙化**しており、業務によってはメールの開封を回避することが困難であるため、不審なメールを開封してしまったことに**気付いたらすぐに報告**すること、**不審な外部との通信を監視**することなど、被害を最小化する組織的な取り組みが求められている。そのためには、組織外との連絡窓口、組織内の適切な連絡体制の整備等、**セキュリティインシデントを組織として受け止める体制**を構築しておくことが重要である。

## 主な被害事例

| 組織名 | 発覚時期 | 被害内容 |
|---|---|---|
| 株式会社i.JTB<br>（JTBグループ） | 2016年6月 | 約678万人分の利用者の氏名、生年月日、住所、電話番号、メールアドレス、パスポート番号等が漏えいの可能性あり。 |
| 国立大学法人<br>富山大学<br>研究推進機構<br>水素同位体科学<br>研究センター | 2016年10月 | 1,492 名分の個人情報、放射性汚染水の処理をテーマとした研究に関する情報が漏えい。 |
| 一般財団法人<br>日本経済団体<br>連合会 | 2016年11月 | 事務局のパソコン17台がウイルス（遠隔操作ツール）に感染し、外部への不審な通信が発生していた。 |

## CSIRTを中心とした組織体制の整備

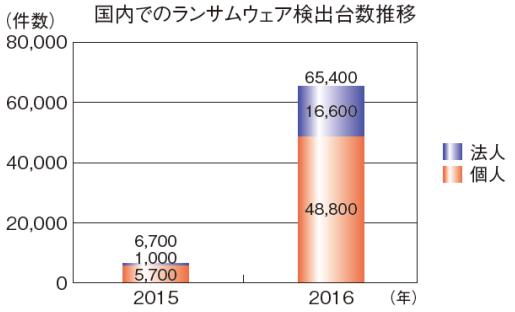


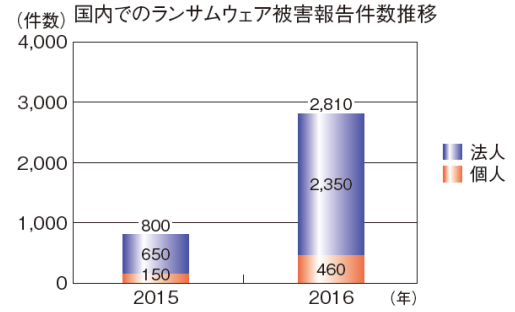

■図 1-3-13　CSIRT を中心とした組織体制の整備※211

# ② ランサムウェア被害件数が過去最多に

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について、**2016年は国内での検出台数、被害報告件数が過去最多**となった。ランサムウェアに感染した場合の影響範囲は、感染したパソコンのみにとどまらず、ネットワーク経由でアクセス可能な端末へも影響を及ぼす可能性がある。ランサムウェアに感染しないための対策（**OS、 ソフトウェアの最新化**や不審なメールへの注意等）と感染に備えた対策（**バックアップ**の取得等）が求められている。

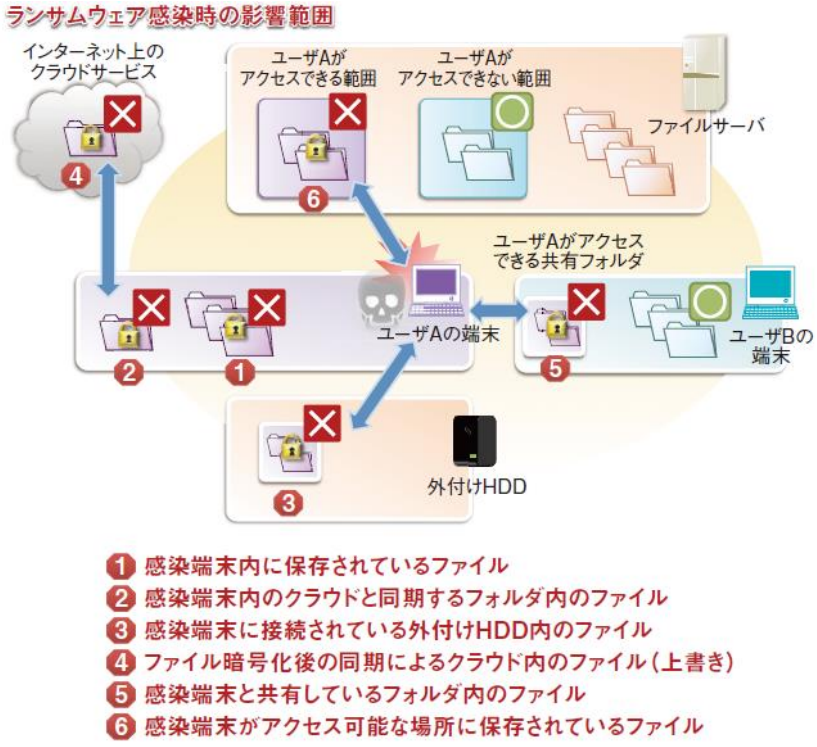
## 国内でのランサムウェアの検出台数と被害報告件数の推移




■図 1-1-8　国内でのランサムウェアの検出台数と被害報告件数の推移
（出典）トレンドマイクロ社「2016 年 年間セキュリティラウンドアップ」を基に IPA が編集

## ランサムウェア感染時の影響範囲




■図 1-3-23　ファイル暗号化型のランサムウェア感染時の影響範囲
（出典）IPA「ランサムウェアの脅威と対策」を基に編集

# ③ 広く普及しているソフトウェアの脆弱性の問題

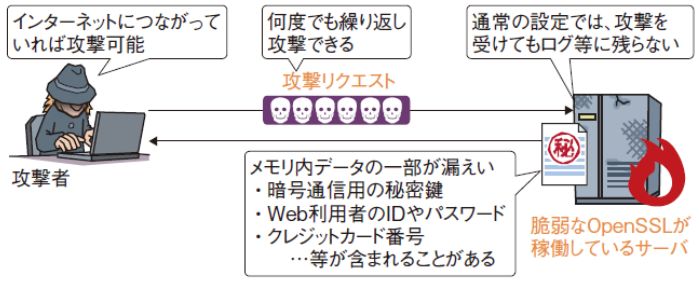
OpenSSL、WordPress、Apache Struts2といった、広く普及しているソフトウェアの脆弱性を悪用した攻撃が多発した。

古いバージョンのOpenSSLには「Heartbleed」と呼ばれる深刻な脆弱性が存在する。2014年4月に修正プログラムが公開されており、アップデートで問題を解消できるにもかかわらず、2016年にも同じ脆弱性を悪用した攻撃による被害が報告されている。**脆弱性が放置されている**ことが原因と考えられる。

2017年2月にはWebサイト構築・編集に利用されているWordPress、3月にはWebアプリケーションフレームワークApache Struts2の深刻な脆弱性が公表された。どちらも、脆弱性を修正するバージョンアップが公表されていたが、**脆弱性の公表直後に、対応が遅れているWebサイトを狙った攻撃が発生**した。その結果、**改ざんや個人情報漏えいの被害**が報告された。

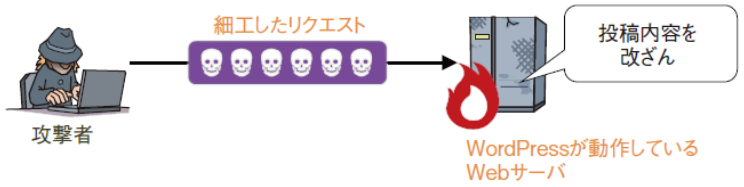
システム管理者は、どのようなソフトウェアが利用されているか把握しておき、**最新の脆弱性情報**を入手し、対策を講じる必要がある。

OpenSSLの脆弱性の悪用イメージ




■図 1-3-6　Heartbleed 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 1-3-7　WordPress の脆弱性を悪用した攻撃のイメージ

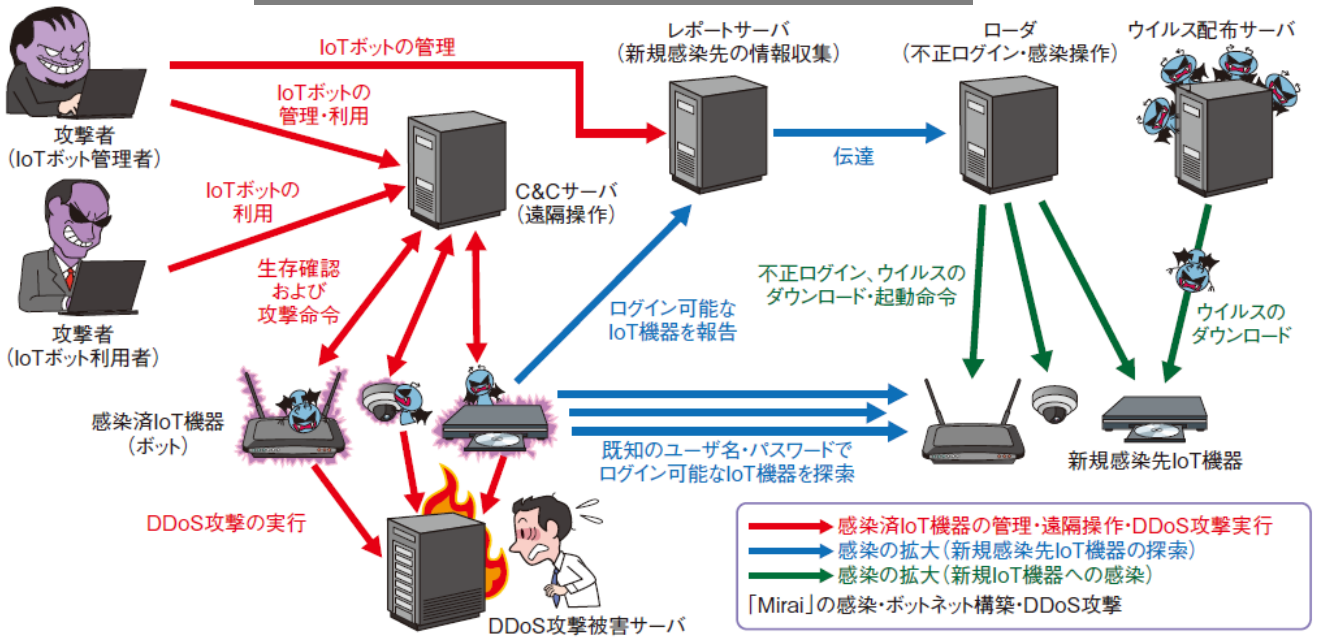
# ④ IoT機器の脅威の顕在化

2016年9月、「**Mirai**」と呼ばれるウイルスに感染した**15万台以上のネットワークカメラやホームルータ**等で構成されるボットネットによる**大規模DDoS攻撃**が行われた。ピーク時に1Tbpsを超える攻撃トラフィックを観測したという。

Miraiは**初期設定のユーザ名とパスワード**を用いて**Telnet**でログイン可能なIoT機器に感染し、定期的にC&Cサーバと通信し、攻撃命令を受信すると指定された攻撃対象にDDoS攻撃を行う。

IoT機器の利用者は、気が付かないうちに加害者になってしまうリスクを認識し、**不要な機能の無効化**や**初期パスワードの変更**などの対策を実施することが望まれる。

「Mirai」の感染からDDoS攻撃まで




■図 3-2-1 「Mirai」の感染・ボットネット構築・DDoS 攻撃
(出典)セキュリティベンダの調査結果※64 を基に IPA が作成

# ⑤ IoTに対する取り組みの強化と国際連携

IoT機器に対するセキュリティ対策の必要性の認識が高まる中、2016年には、政府が本格的な取り組みの方針を表明し、国内外において**IoTセキュリティに関する様々なガイドライン等が公開**された。

また、米国や欧州と国家レベル、企業レベルで連携することを表明した。

- 2016年4月、経済産業省とドイツ経済エネルギー省との間で「日独IoT/インダストリー4.0協力に係る共同声明」への署名
- 2016年10月、産学官連携のIoT推進コンソーシアムと、IIC及びOpenFogコンソーシアムとの間で、IoT分野の協力に係る署名

## 国内で公開されたIoT関連ガイドライン

| 公開機関 | 公開資料名 | 公開年月 |
|---|---|---|
| IPA | IoT開発におけるセキュリティ設計の手引き | 2016年5月 |
| 経済産業省、総務省、IoT推進コンソーシアム | IoTセキュリティガイドラインver1.0 | 2016年7月 |
| NISC | 安全なIoTシステムのためのセキュリティに関する一般的枠組 | 2016年8月 |
| 日本クラウドセキュリティアライアンス | Internet of Things(IoT)インシデントの影響評価に関する考察 | 2016年4月 |
| 重要生活機器連携セキュリティ協議会 | 製品別セキュリティガイドライン 車載器編/IoT-GW編/ATM編/POS編 | 2016年6月 |
| 日本ネットワークセキュリティ協会 | コンシューマ向けIoTセキュリティガイド | 2016年6月 |

■表3-2-2　国内で公開されたIoT関連のガイドライン等　より2016年度発行のものを抜粋

## 国外で公開されたIoT関連ガイドライン

| 公開機関 | 公開資料名 | 公開年月 |
|---|---|---|
| NIST | NIST Special Publication 800-183 Networks of 'Things' | 2016年7月 |
| IIC (Industrial Internet Consortium) | Industrial Internet of ThingsVolume G4: Security Framework | 2016年9月 |
| DHS | Strategic Principles for Securing the Internet of Things | 2016年11月 |
| IoT Security Foundation | IoT Security Compliance Framework | 2016年12月 |

■表3-2-3　海外で公開されたIoT関連のガイドライン等　より2016年度発行のものを抜粋

# ⑥ 重要インフラのセキュリティ対策を強化する国内の取り組み

「重要インフラの情報セキュリティ対策に係る第3次行動計画」に基づき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進めた。

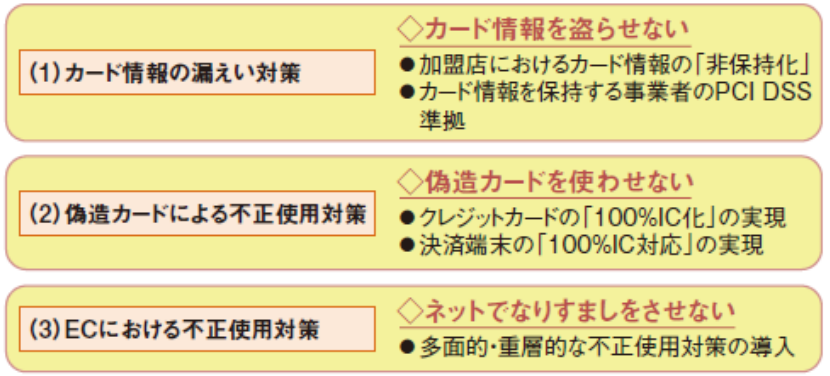
電力業界では、2016年4月の電力自由化をきっかけにサイバーセキュリティ対策が検討され、関連ガイドラインの策定、及びガイドラインに基づく情報セキュリティ監査を実施した。

クレジット業界では、セキュリティ環境を整備するため、クレジットカード会社や加盟店棟の各主体が取り組むべき事項をまとめた「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」を策定した。また、2017年4月には、J-CSIPにクレジット業界SIGが発足し、標的型攻撃の情報共有を開始した。

## 電力業界のセキュリティ対策強化

| 公開機関 | 公開資料名 | 公開年月 |
|---|---|---|
| 日本電気技術規格委員会（JESC） | スマートメーターシステムセキュリティガイドライン | 2016年3月 |
| | 電力制御システムセキュリティガイドライン | 2016年5 月 |
| 経済産業省 | 「電気設備に関する技術基準を定める省令」の一部改正<br>電気事業法で定めている技術基準及び保安規定内規に上記ガイドラインを組み込んだ | 2016年5月 |

## クレジットカード取引におけるセキュリティ対策強化



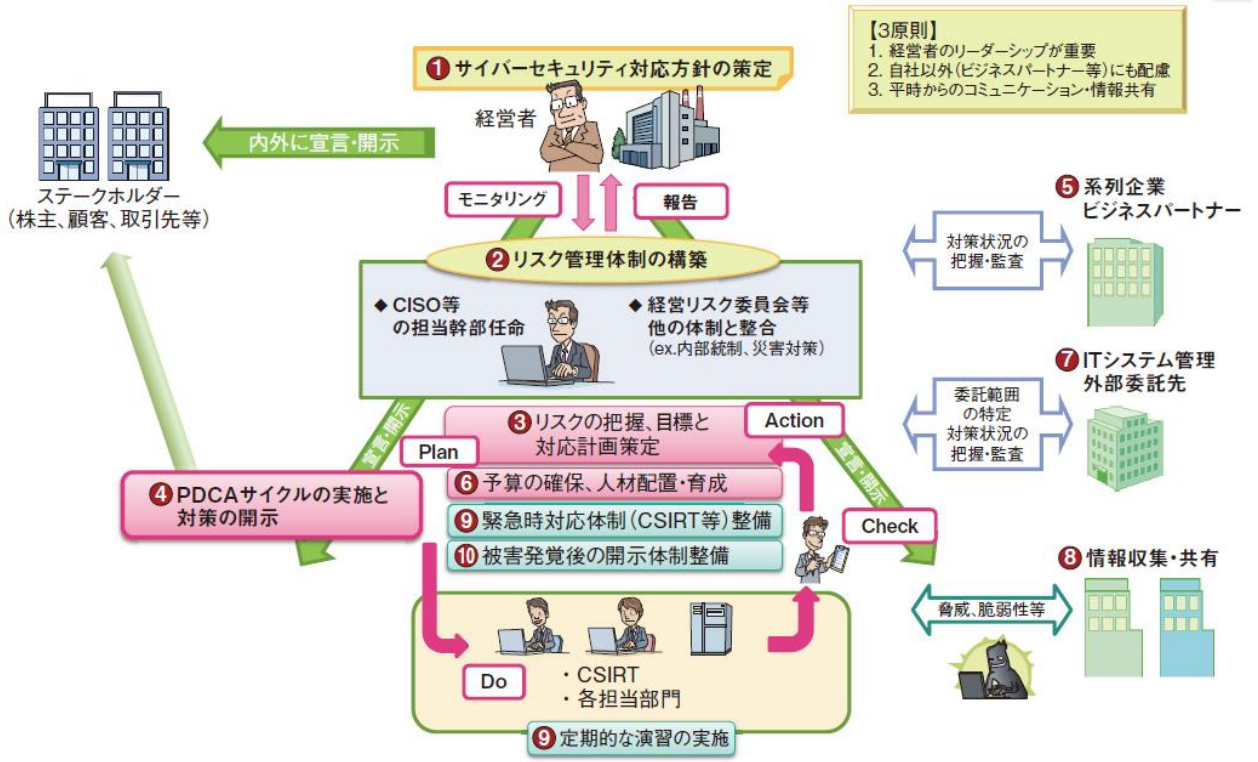

■図 2-1-7 「実行計画」における対策の３本柱
（出典）一般社団法人日本クレジット協会「クレジット取引セキュリティ対策協議会 実行計画 -2017- の概要について※39」を基に IPA が編集

# ⑦ サイバーセキュリティ経営ガイドラインの改訂

2016年12月、経済産業省とIPAは「サイバーセキュリティ経営ガイドライン」を改訂した。同ガイドラインは、2015年12月に初版が策定され、経営者が認識すべき原則とCISO等に指示すべき対策等がまとめられている。この改訂で、“経営戦略としてセキュリティ投資は必要不可欠かつ経営者としての責務である”という表現が明記された。

また、「サイバーセキュリティ経営ガイドライン解説書」を作成し、同ガイドラインにおける重要な対策の実施手順や検討ポイント等を示した。

**サイバーセキュリティ経営ガイドラインの全体像**

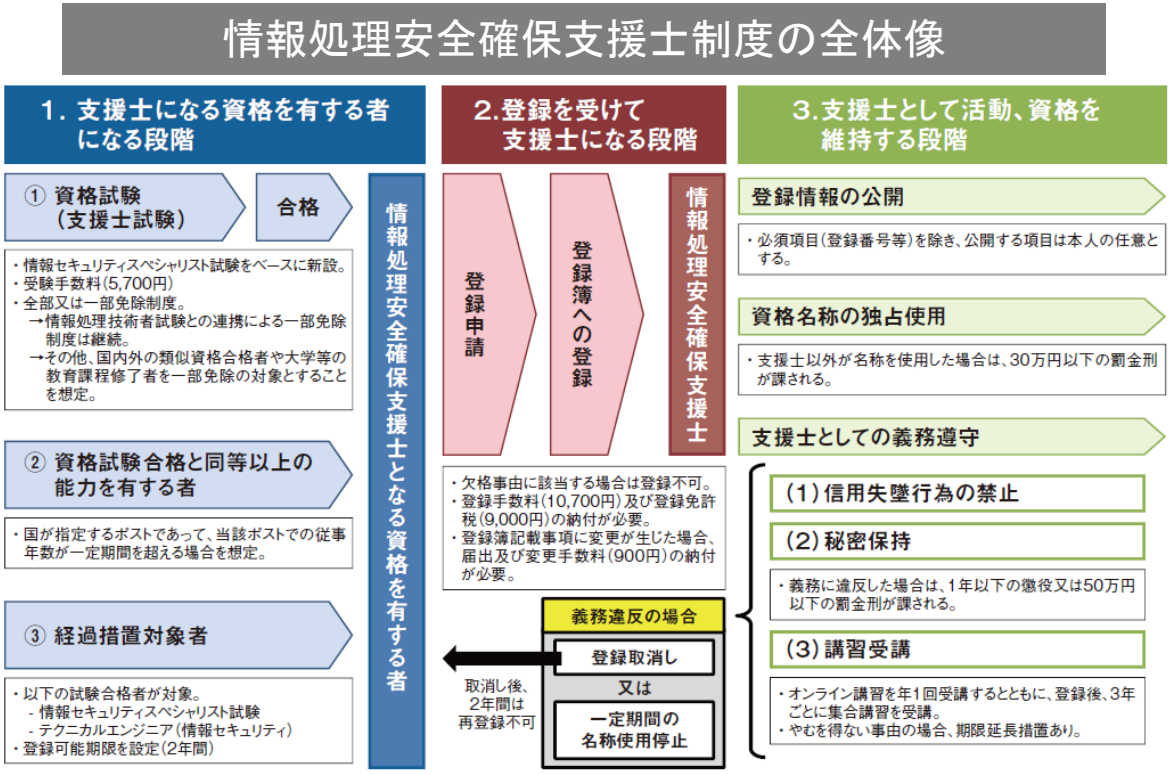



■図 2-1-6　ガイドラインの 3 原則と重要 10 項目
(出典)IPA「サイバーセキュリティ経営ガイドライン解説書」

# ⑧情報セキュリティ人材育成のための資格制度を新設

サイバーセキュリティに関する実践的な知識・技能を有する専門人材の育成と確保を目指し、2016年10月、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**」（通称：登録セキスペ）制度が新設された。2017年4月1日付の初回登録では、4,172名が登録された。経済産業省及びIPAは、**2020年までに3万人の登録**を目標としている。

今後、組織における情報セキュリティ確保、及び情報セキュリティ人材の育成・強化への活用が期待される。



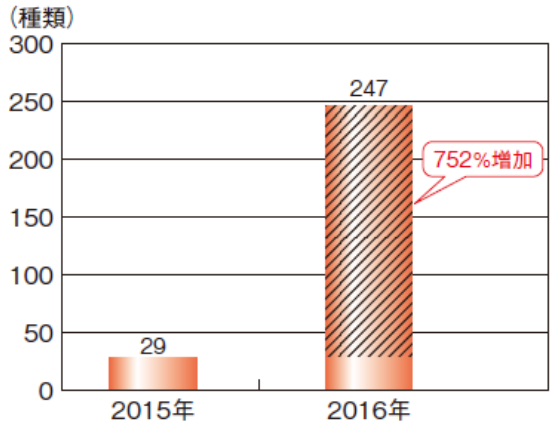

■図 2-4-4　情報処理安全確保支援士制度の全体像
(出典)経済産業省「支援士制度概要※202」

# ⑨ 国外のセキュリティ動向

2016年度は、全世界的にランサムウェアが猛威を振るい過去最大の被害が報告された。8月にはリオデジャネイロオリンピック開催への抗議活動として、オリンピックに関連したWebサイトやブラジル政府機関への攻撃が観測された。11月にはロシア政府による米国大統領選挙妨害のためのハッキングなどの国家レベルの攻撃があった。

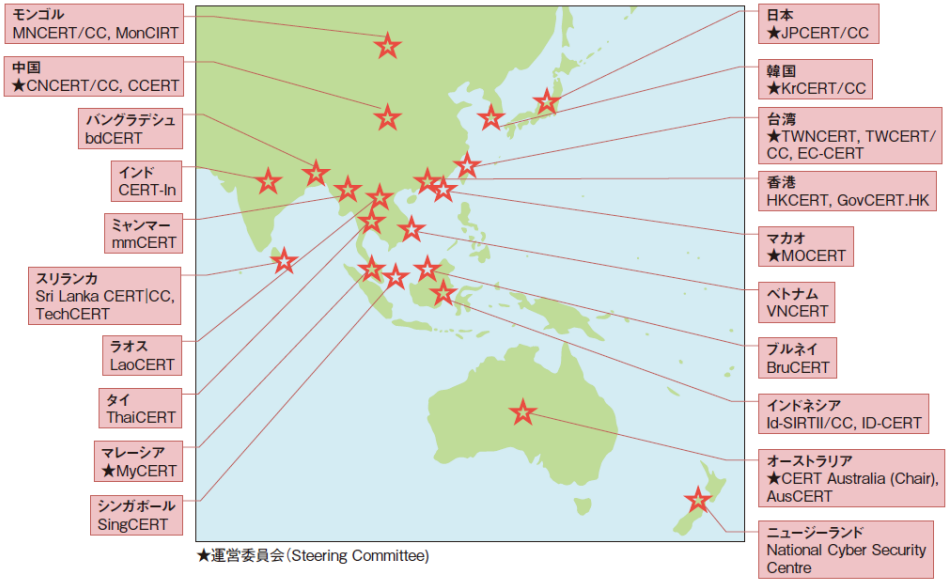
政策面では、8月にはEU 域内においてNIS 指令が施行され、重要インフラ防御の政策が進展した。2017年1月には、米国のサイバーセキュリティフレームワークが改訂される等、各国でセキュリティ対策強化のための施策が発表された。2016年12月にガイドラインが公開されたEUの一般データ保護規制（GDPR）は日本企業でも対応の必要があり、早急な準備が望まれる。また、アジアでは、各国のCSIRTが連携して演習や情報共有を行っており、連携が進んでいる。

## 増大するランサムウェアの脅威




■図 1-1-4　新種のランサムウェア数（新ファミリー数）
（出典）トレンドマイクロ社「2016 年 年間セキュリティラウンドアップ」を基に IPA が編集

## アジア太平洋地域のCSIRT 間連携




■図 2-3-2　APCERT オペレーショナルメンバー（2017 年 3 月末現在）

# 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

# 第2章 情報セキュリティを支える基盤の動向

## 目次

# 第2章 情報セキュリティを支える基盤の動向

## 目次

# 第3章 個別テーマ

## 目次