IPA Better Life with IT

情報セキュリティ白書2018

深刻化する事業への影響：つながる社会で立ち向かえ

概要説明資料

2018年7月17日

独立行政法人情報処理推進機構
セキュリティセンター　セキュリティ対策推進部
セキュリティ分析グループ

情報セキュリティ白書2018
深刻化する事業への影響：つながる社会で立ち向かえ

情報セキュリティの動向を広くカバーした一冊

■2017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

■IoT、仮想通貨、スマートフォン、制御システム、
中小企業での対策など、2017年度に注目された
出来事、分野の情報セキュリティについて解説

2018年7月17日発行

◆製本版入手先：Amazon
全国官報販売協同組合
IPA　※全国の書店からお取り寄せができます

◆PDF版入手先：IPAのHPから、アンケートにお答え
いただくとダウンロード可能です。
https://www.ipa.go.jp/security/publications/hakusyo/2018.html

発行：IPA
ISBN：978-4-905318-63-7
ソフトカバー/A4判　240頁
製本版価格　2,000円（税別）

全体構成

- 情報セキュリティの概要と分析
  - 序章 2017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（IoT、仮想通貨、スマートフォン、制御システム、中小企業）

- **付録　情報セキュリティ10大脅威2018・資料・ツール**
  - 情報セキュリティ10大脅威2018
  - 資料A 2017年のコンピュータウイルス届出状況
  - 資料B 2017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13回 IPA「ひろげよう情報モラル・セキュリティコンクール」2017 受賞作品**

2017年度の情報セキュリティの概況

2017年4月から2018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。

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

2017年度の主な情報セキュリティインシデント・事件

	主な情報セキュリティインシデント・事件
2017年　4月	Apache Struts2の脆弱性を悪用した不正アクセスによる情報流出が相次ぐ（1.2.4(1)、1.3.3(1)）
5月	世界各国でWanna Cryptorによる被害が相次ぐ（1.2.1、1.3.1）
6月	ランサムウェアを自作したとして、中学3年の男子生徒を、不正指令電磁的記録作成等の疑いで逮捕(2.1.4)
9月	国内航空会社でビジネスメール詐欺による3億円を超える被害発生(1.2.5(1)、1.3.6) 米国の大手信用情報会社が1億4,300万人の米国顧客の個人情報が流出可能性を公表(1.1.1,1.4.1(2))
10月	コミュニティサイトを通じて知り合った男女9名が殺害される事件が発生（2.1.4） 仮想通貨のマイニングツールが確認される（3.1、3.3） 無線LANの暗号化規格であるWPA2の脆弱性（KRACK / KRACKs）が発見される(1.4.1)
11月	国内におけるIoT機器のウイルス感染の急増(3.1.2)
2018年　1月	仮想通貨交換取引所から約580億円相当の仮想通貨が不正流出(3.2.1)
2月	平昌冬期オリンピック・パラリンピック競技大会の妨害を目的としたサイバー攻撃
3月	日本年金機構の業務委託先が無断で海外事業者に再委託していたことが発覚（1.2.4(3)） SNS上で取得された最大8,700万人の個人情報が米国選挙工作のため不正利用されていたことが発覚（1.2.4(3) 2.3.2(7)）

※末尾の項番号は、「情報セキュリティ白書2018」の該当箇所

2017年度の情報セキュリティの概況

2017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
2017年　4月	情報処理安全確保支援士（登録セキスペ）登録開始(2.4.2) 「重要インフラの情報セキュリティ対策に係る第4次行動計画」決定(2.1.1) 産業サイバーセキュリティセンター発足（2.4.1） 「サイバーセキュリティ人材育成プログラム」公表（2.4.1） SECURITY ACTIONの創設（3.5）
5月	改正個人情報保護法の全面施行 「知的財産推進計画2017」決定(2.2.2) 米国でサイバーセキュリティ強化に関する大統領令の発効（2.3.2）
6月	「科学技術イノベーション総合戦略2017 」「未来投資戦略2017」決定(2.1.1、2.2.2) 中国でネットワーク安全法の施行（2.3.4）
7月	「サイバーセキュリティ研究開発戦略 」公表(2.1.1) ドイツで一般データ保護規則（GDPR）に対応した新ドイツ連邦データ保護法の成立（2.3.3）
8月	「サイバーセキュリティ2017」公表(2.1.1)
9月	欧州委員会がサイバーセキュリティ法案を発表（2.3.3）
10月	「IoTセキュリティ総合対策」公表（2.1.3） 「Connected Industries」東京イニシアティブ2017 発表(2.1.2) 「サイバーセキュリティ国際キャンペーン」月間実施（2.1.1）
11月	「サイバーセキュリティ経営ガイドラインVer.2.0」の公開（2.1.2、2.5.1）
12月	「分野横断的演習」の実施（2.1.1） 産業サイバーセキュリティ研究会設置（2.1.2） 個人情報保護マネジメントシステムJIS Q 15001 改訂（2.5.2）
2018年　2月	サイバーセキュリティ月間(2.8.1) 「不正競争防止法等の一部を改正する法律案」の閣議決定(2018年5月30日公布)(2.2.2) 「情報セキュリティサービス基準」及び「情報セキュリティサービスに関する審査登録機関基準」公表(2.1.2)
3月	「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律案」の閣議決定(2018年5月23日公布)(2.1.3)

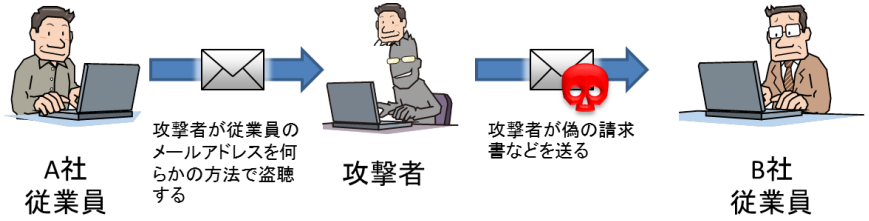
※末尾の項番号は、「情報セキュリティ白書2018」の該当箇所

① 詐欺による金銭被害の増加

偽の画面を表示させ利用者の不安や焦りに付け込んで金銭や情報を騙し取る**偽警告・偽サイト等の詐欺**や、偽の電子メールを組織・企業に送り付け従業員を騙して送金取り引きに関わる資金を詐取しようとする**ビジネスメール詐欺**（Business E-mail Compromise：BEC）、等巧妙な騙しの手口を駆使した詐欺による**金銭被害が増加**している。

2017年12月、日本航空株式会社（JAL）が、ビジネスメール詐欺により、2件で総額約3億8,400万円（347万880.64米ドル）の被害を受けたことを発表し、注目された。ビジネスメール詐欺は攻撃者にとって多額の収益が見込めることから、今後も脅威は続くと思われ、注意が必要である。

ビジネスメール詐欺の手口



■図1-3-14　取引先との請求書の偽装の例
（出典）IPA「【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口」

狡猾な細工がされている偽警告

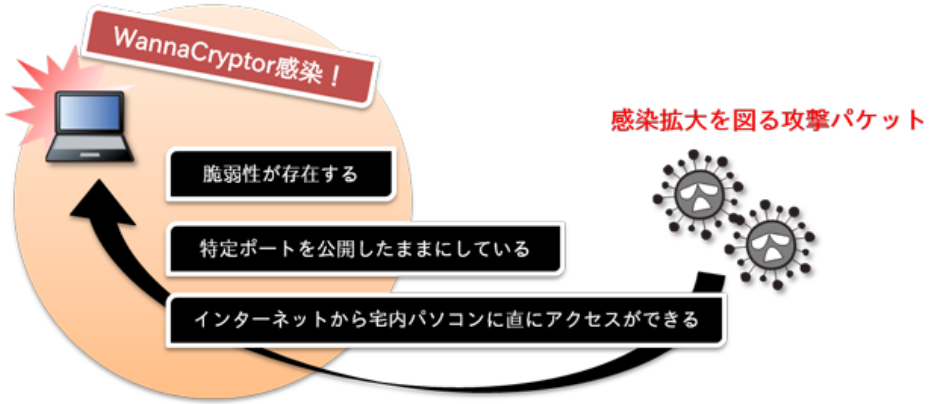
■図1-3-22　狡猾な細工がされている偽警告画面の例

② ランサムウェア被害件数が過去最多に

2017年は**自己増殖機能を持ったランサムウェア**が大きな話題となった。そのような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やソフトウェアの最新化、不審なメールへの注意、通信制御**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。

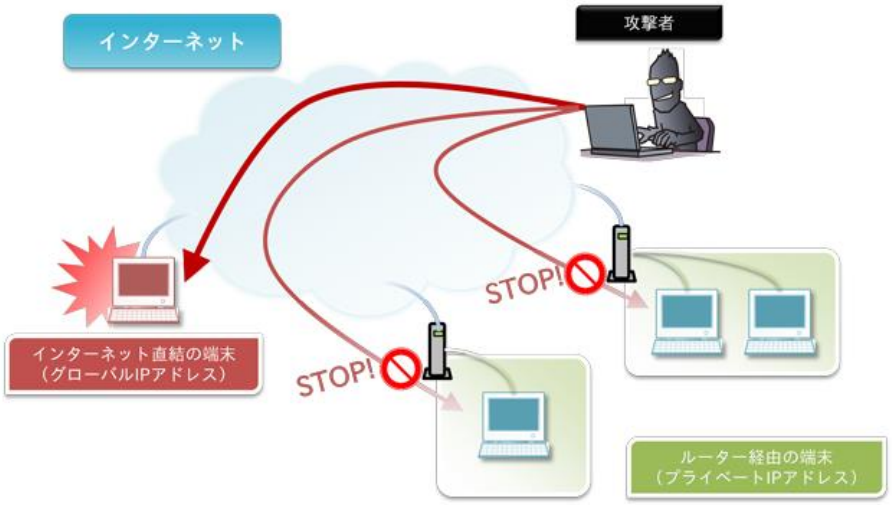
また、Microsoft Internet Explorer やAdobe Flash Player の脆弱性を悪用した攻撃でランサムウェアが拡散されたり、従来のランサムウェアに仮想通貨を窃取する目的の機能が追加されたりする等、ランサムウェアの多様化やバージョンアップは続いている。
今後もランサムウェアに対する警戒が引き続き必要である。

WannaCryptorに感染してしまう原因



■図1-3-1　Wanna Cryptor に感染してしまう三つの環境要因
（出典）IPA「Wanna Cryptorの相談事例から学ぶ一般利用者が注意すべきセキュリティ環境」

宅内パソコンに必要な対策

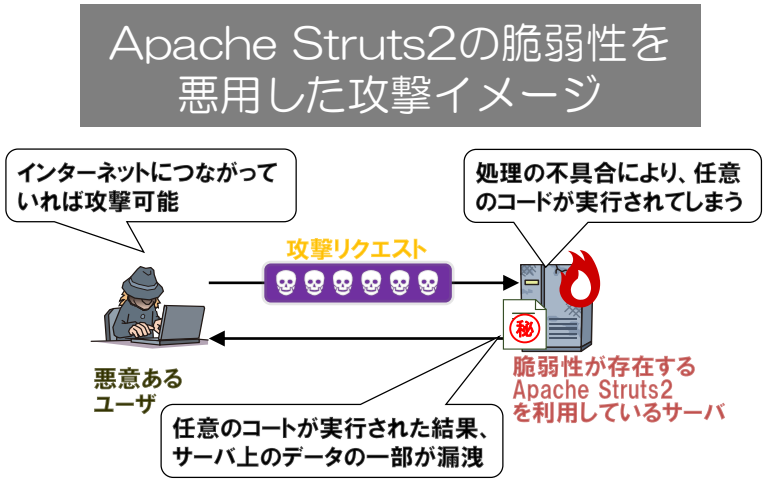


■図1-3-2　ルータ経由でインターネットに接続することでパソコンを外部の攻撃から守る
（出典）IPA「Wanna Cryptor の相談事例から学ぶ一般利用者が注意すべきセキュリティ環境」

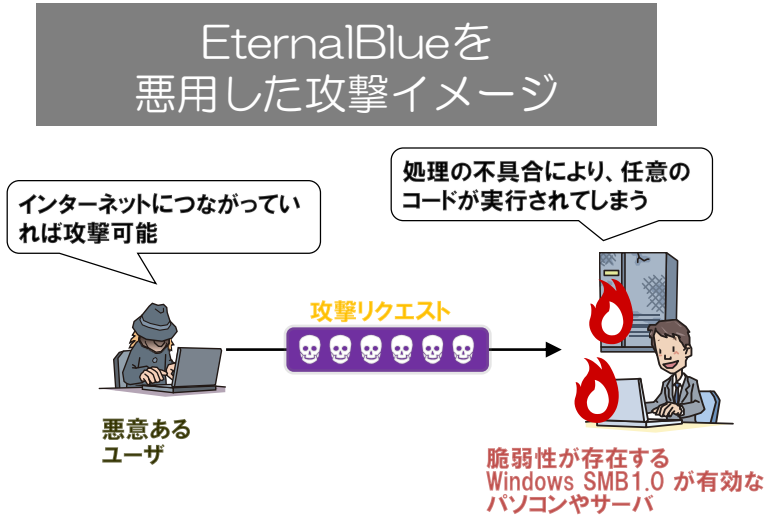
③ 広く普及しているソフトウェアの脆弱性の問題

2017年は、多くのWeb サーバで使われている**Apache Struts2** や、多くの利用者を持つ**Windows に存在する既知の脆弱性**を狙った攻撃が報告された。Apache Struts2 の脆弱性を悪用する攻撃では、総務省やB.LEAGUEサイト等、多くの個人情報を保有するWeb サイトが攻撃に遭い、個人情報が漏えいした可能性があると報告された。

Wanna Cryptor 等の数多くのウイルスで悪用された攻撃ツール「**EternalBlue**」は、Windows SMBv1 サーバの脆弱性を狙ったものであった。対策としては脆弱性を解消するアップデートや修正プログラムの速やかな適用が有効であるが、何らかの理由により時間を有する場合は、一時的にIPSやWAF等で防御する方法もある。



■図1-3-6　Apache Struts2 の脆弱性を悪用した攻撃イメージ



■図1-3-7　EternalBlue を悪用した攻撃イメージ

④ 仮想通貨の脅威の顕在化

一般社団法人日本仮想通貨事業者協会（JCBA）は、2017年1月1日を「**仮想通貨元年の幕開け**」と表現し、仮想通貨に関わる業者が連携してガイドラインや自主規制の策定に取り組むとした。金融業界でも、独自仮想通貨の発行や、ブロックチェーン技術応用のための各種実証研究等が進められている。一方で2018年1月、**仮想通貨「NEM」**の不正流出（不正移転）が発生し、仮想通貨交換業のセキュリティ上の問題点等が浮き彫りとなった（仮想通貨不正移転問題）。様々な問題やインシデントが発生した原因としては、ブロックチェーン技術等の仮想通貨固有の課題（ファイナリティ問題等）もあるが、事業者や政府の対応が急速に拡大するビジネスに追いつかなかったことも大きいと考えられる。問題分野や課題等を正確に把握し、対策を検討・実施していく必要がある。

仮想通貨に関する脅威と対策

	脅威	問題分野	主な対策	課題
仮想通貨固有の問題	仮想通貨不正移転	秘密鍵等管理方法	コールドウォレット、マルチシグネチャ、権限管理	開発不備、取引利便性への障害、コスト過大等を考慮したリスク分析
			分散型取引所	資金決済法との整合性
			事後追跡機能	本人確認不十分な取引所、匿名通貨との交換
	ネットワークリスク（ブロックチェーンの分岐、取引遅延等）	コンセンサスアルゴリズム	マイナー等の動向注視、オフチェーン技術等の実装	マイナー勢力等の意向の影響が大きく、予想が困難。新技術の実装研究は未だ発展途上
			PBTF等集中管理型コンセンサスアルゴリズムの採用	限定ノードに対する攻撃の危険、パブリックシステムへの適用困難
	不正プログラム	各仮想通貨のOSS	十分な検証、安全性確認	信頼性の保証のある基準の確立
一般的問題	その他サイバー攻撃	各取引所、個人のセキュリティー般	パッチ適用、通信暗号化、サーバ冗長化、2段階認証等	統一的な安全性基準の確立、情報リテラシーの向上
	詐欺（ICO詐欺含む）	取引関係者の説明義務、財政基盤の有無	消費者対策、取引業者に対する監視・監督	国際的取り引きが容易に行われ、我が国の監視が及ばない場合

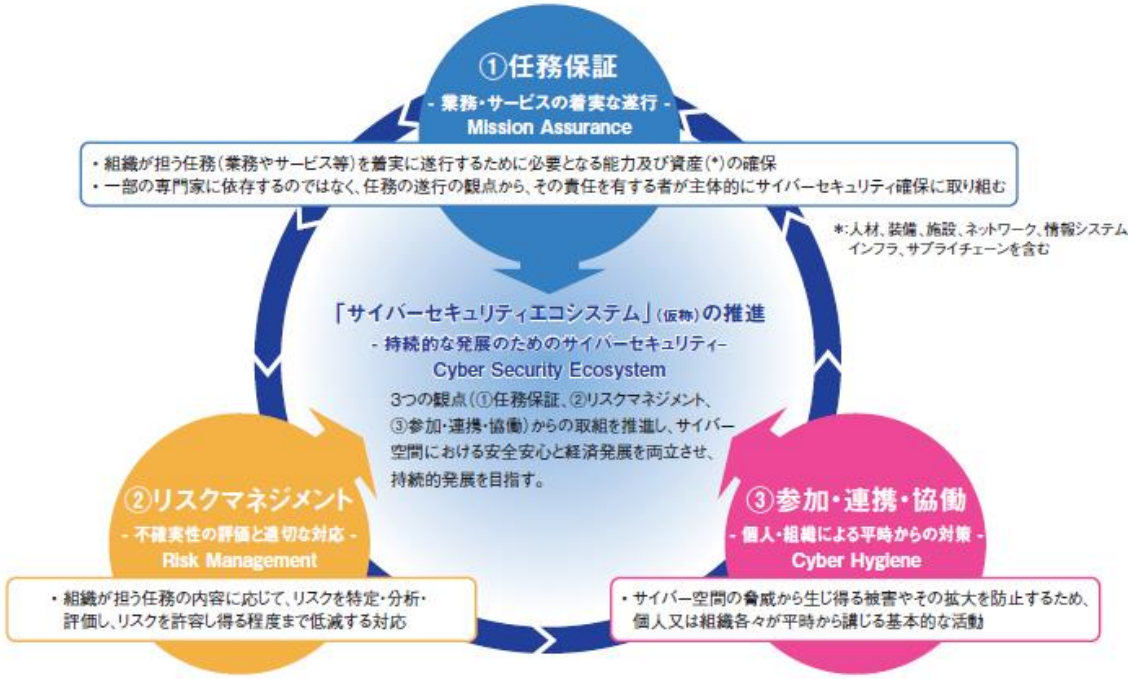
■表3-2-1　仮想通貨の問題分野別検討表

⑤ セキュリティ対策を強化する国内の取り組み

政府は「サイバーセキュリティ戦略」に基づき、「サイバーセキュリティ2017」を策定し実施した。また「重要インフラの情報セキュリティ対策に係る第4 次行動計画」を策定し、リスクアセスメント手引書の公表、分野横断的演習やセプター訓練の実施等、情報セキュリティ対策強化を行っている。

「『次期サイバーセキュリティ戦略』の骨子」では、「サイバーセキュリティエコシステム」（仮称）を目指して、「任務保証」「リスクマネジメント」「参加・連携・協働」の観点から、官民のサイバーセキュリティに関する取り組みを推進することを示した。

次期サイバーセキュリティ戦略

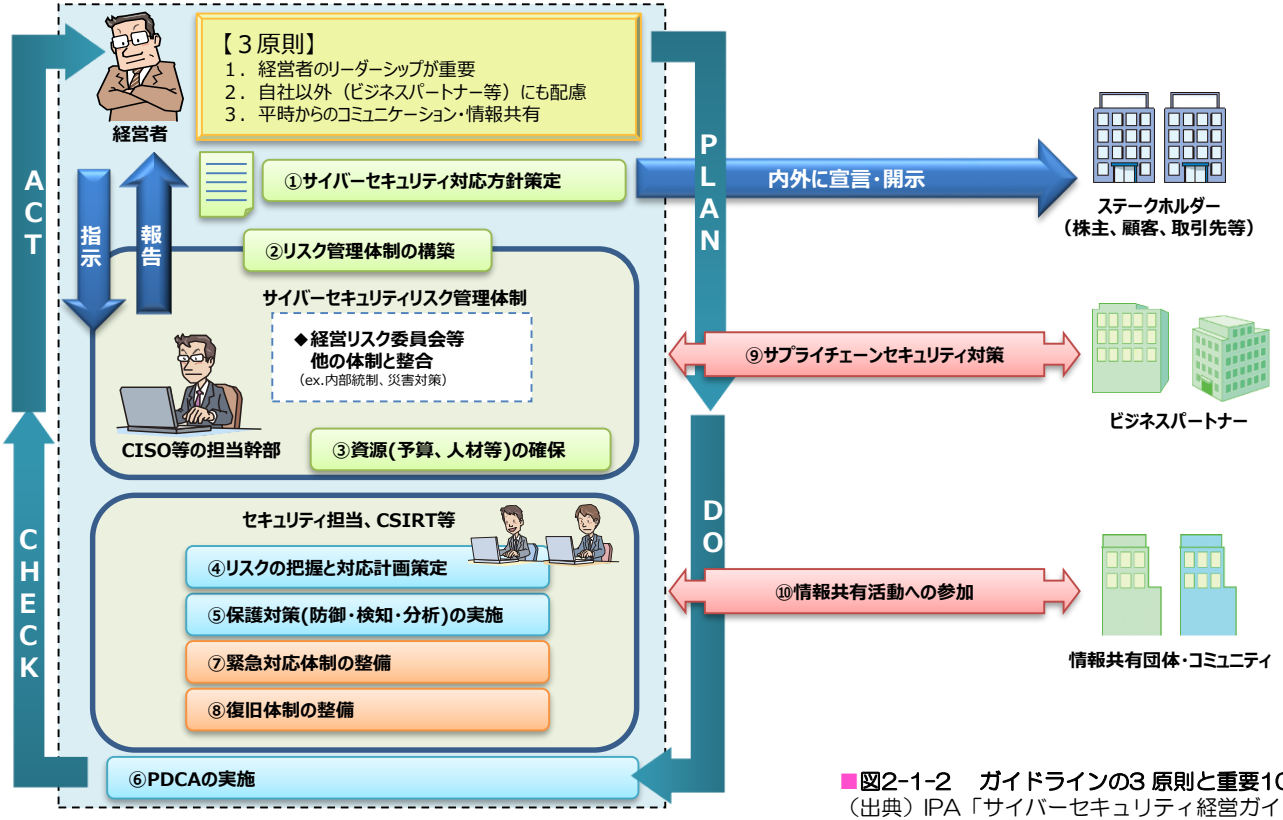


■図2-1-1　次期戦略におけるサイバーセキュリティの基本的な在り方のイメージ
（出典）サイバーセキュリティ戦略本部「『次期サイバーセキュリティ戦略』の骨子」を基にIPA が編集

⑥ サイバーセキュリティ経営ガイドラインVer2.0の発行

2017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、重要項目の中に“攻撃の検知”“サイバー攻撃を受けた場合の復旧への備え”が新たに追記され“サプライチェーン対策の強化”が強調された

サイバーセキュリティ経営ガイドラインの全体像



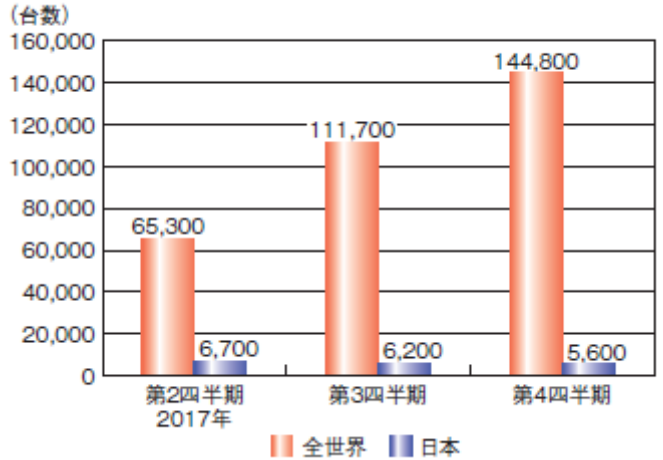
■図2-1-2　ガイドラインの3 原則と重要10 項目の概要
（出典）IPA「サイバーセキュリティ経営ガイドラインVer2.0」

⑦ 国外のセキュリティ動向

日本政府は2017年度も米国、欧州、イスラエル、アジア諸国とのサイバーセキュリティに関する**連携協議や演習を実施**した。米国では、5 月に発効した**大統領令**に基づき連邦政府のセキュリティ政策見直し及び権限集約等によるナショナルセキュリティ戦略の強化を行った。欧州各国では、**NIS 指令**に基づき **GDPR** 発効に向けた国内法制の整備を行った。中国では、2017年6 月中華人民共和国網絡安全法（「**ネットワーク安全法**」）が施行された。

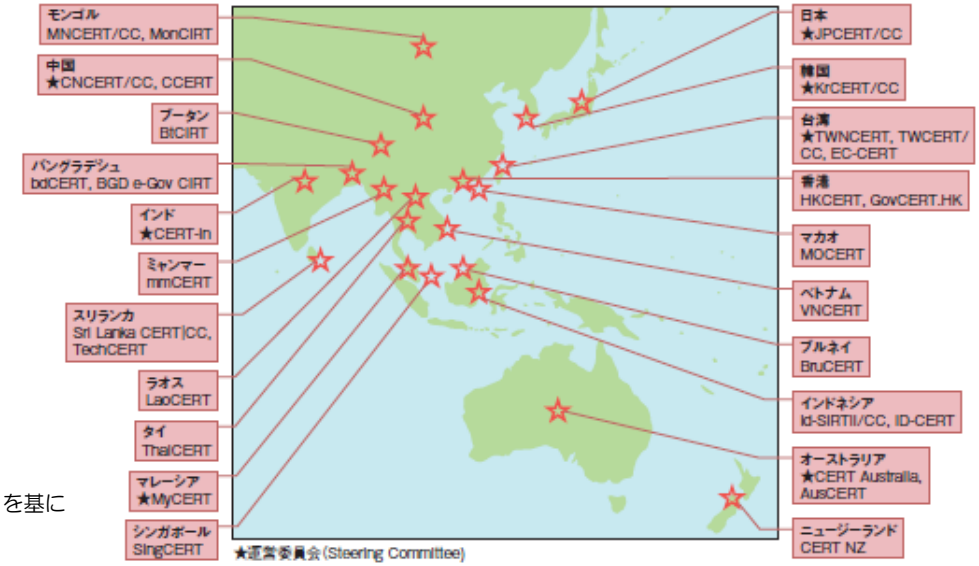
2017年5 月にランサムウェアWanna Cryptorにより引き起こされた大規模サイバー攻撃では、アジア太平洋地域の国々でも広範囲にわたって感染事例が報告された。こうした同時多発的なインシデントへの対応においては、個々のCSIRT が役割を発揮すること、また各国及び地域全体においてCSIRT 間で連携をとることが一層重要となる。そのため、アジアでは、各国の**CSIRT**が連携して演習や情報共有を行っており、連携が進んでいる。

増加するランサムウェアの脅威



■図1-1-1　日本と世界におけるWanna Cryptor の検出台数推移
（出典）トレンドマイクロ社「2017 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



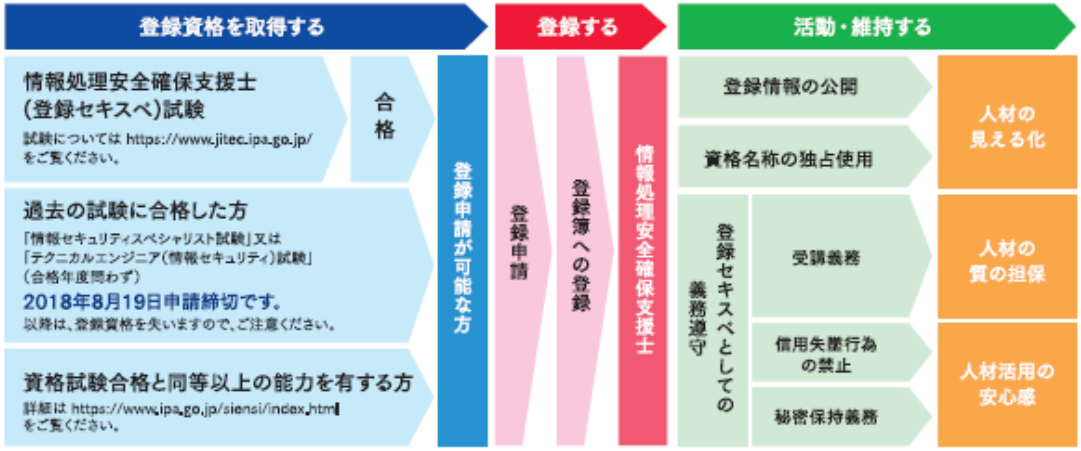
■図2-3-1　APCERT オペレーショナルメンバー（2018 年5 月末現在）

⑧セキュリティ人材育成のための取り組み

2017年4 月、IPA は、制御技術（OT）と情報技術（IT）の知見を結集させたサイバーセキュリティ対策の中核拠点として、産業サイバーセキュリティセンター（ICSCoE）を発足させた。社会インフラや産業基盤の運用の鍵となるOTとITの双方のスキルを核とした産業サイバーセキュリティ人材育成のトレーニングを開始した。

また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、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」の登録を開始した。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。

情報処理安全確保支援士制度の全体像



■図2-4-6　情報処理安全確保支援士制度の全体像
（出典）IPA「制度について」を基に編集

産業サイバーセキュリティ人材像

■図2-4-4　目指すべき産業サイバーセキュリティ人材像
（出典）IPA の事業案内パンフレット

⑨「制御システムのセキュリティリスク分析ガイド」公開

制御システムのセキュリティ対策としてリスク分析は重要であるが、「具体的な方法論や手順が分からない。」「従来のリスク分析は膨大な工数を要することが多い。」といったことから、十分浸透していない。重要インフラの情報セキュリティ対策に係る第4次行動計画で掲げられている「リスクアセスメントの浸透」を支援するため、IPA は2017年10 月に「制御システムのセキュリティリスク分析ガイド」を公開した。

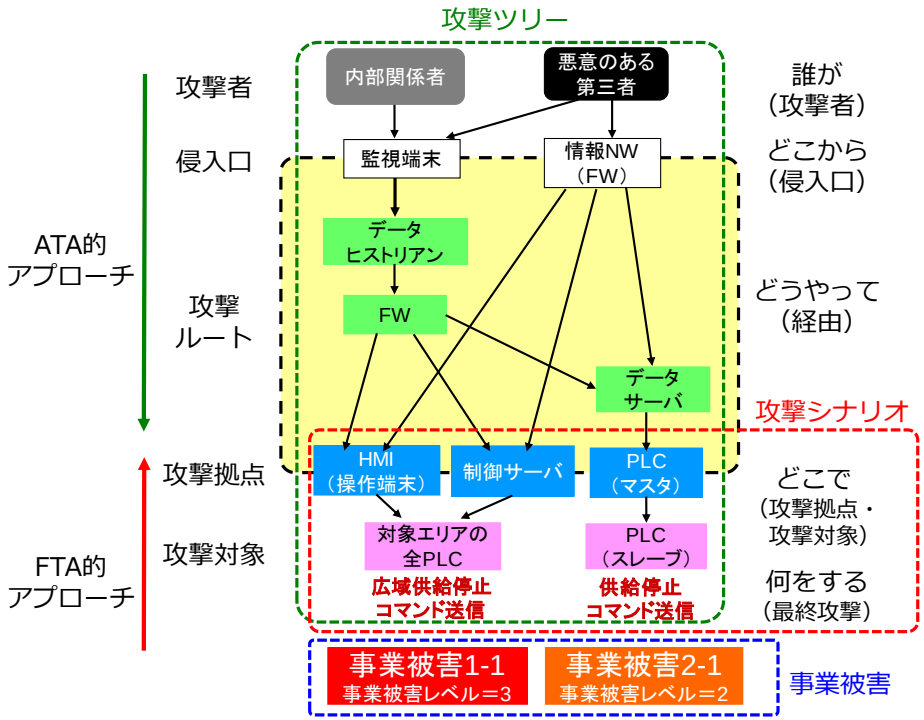
リスク分析に用いる評価指標

評価指標		ガイドで提供している検討例（各事業者で定義または例をカスタマイズ）
脅威（資産ベース・事業被害ベース共通）	脅威	「資産に対する脅威（攻撃手法）」「資産（通信経路）に対する脅威（攻撃手法）」
	脅威レベル	－
	判断基準	「脅威レベルの判断基準の定義例」
脆弱性（資産ベース・事業被害ベース共通）	脆弱性	「セキュリティ対策項目一覧」
	脆弱性レベル（対策レベル）	－
	判断基準	「脆弱性レベルと対策レベルの定義（評価点と判断基準）」
資産の重要度（資産ベース）	資産の重要度	「CIA要件及びHSE要件を考慮した資産の重要度の評価例」
	資産の重要度（レベル）	－
	判断基準	「資産の重要度の判断基準の定義例」
事業被害（事業被害ベース）	事業被害	「事業被害の定義例」
	事業被害レベル	－
	判断基準	「事業被害レベルの判断基準の定義例」

※レベルはそれぞれ「1：低」～「3：高」で評価

■表3-4-2(一部抜粋)　ガイドにおけるリスク分析で用いている評価指標

事業被害ベースのリスク分析



■図3-4-1　事業被害、攻撃シナリオ、攻撃ツリーの関係

⑩ 中小企業のセキュリティ対策「SECURITY ACTION」

SECURITY ACTIONとは、**中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度**である。IPAが公開している「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに、2 段階の取組目標を設定している。第1 段階では、付録「**情報セキュリティ5 か条**」に取り組むことを宣言することで、宣言企業であることを示す一つ星のロゴマークを使用できる。第2段階では、付録「**5 分でできる！情報セキュリティ自社診断**」で自社の状況を把握した上で、「**情報セキュリティポリシー（基本方針）**」を定め、外部に公開したことを宣言することで、ステップアップした二つ星のロゴマークを使用できる。

SECURITY ACTION は、政府が2017年度補正予算として措置した経済産業省の「サービス等生産性向上IT 導入支援事業」の申請要件となった。中小企業へのIT 利活用の拡大とあわせて同制度が広く普及していくことが見込まれる。

中小企業の情報セキュリティ対策ガイドライン

第1部　経営者編
第2部　管理実践編
付録1　情報セキュリティ５か条
付録2　５分でできる！
　　情報セキュリティ自社診断
付録3　わが社の情報セキュリティポリシー
ツールA　リスク分析シート
ツールB　情報セキュリティポリシーサンプル

■図3-5-3　中小企業の情報セキュリティ対策ガイドライン第2.1 版

SECURITY ACTIONのロゴマーク

■図3-5-2　一つ星（左）と二つ星（右）のロゴマーク

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（１／２）

目次

第2章 情報セキュリティを支える基盤の動向（2／2）

目次

第3章 個別テーマ

目次