経済産業省

産業サイバーセキュリティ強化へ向けた経済産業省の取組の紹介

経済産業省

商務情報政策局

サイバーセキュリティ課

１．サイバー攻撃の脅威レベルの向上と海外の動き

２．産業サイバーセキュリティ研究会

３．経済産業省のサイバーセキュリティ政策動向

サイバー攻撃の脅威レベルの向上の例①：ランサムウェア"WannaCry"の猛威

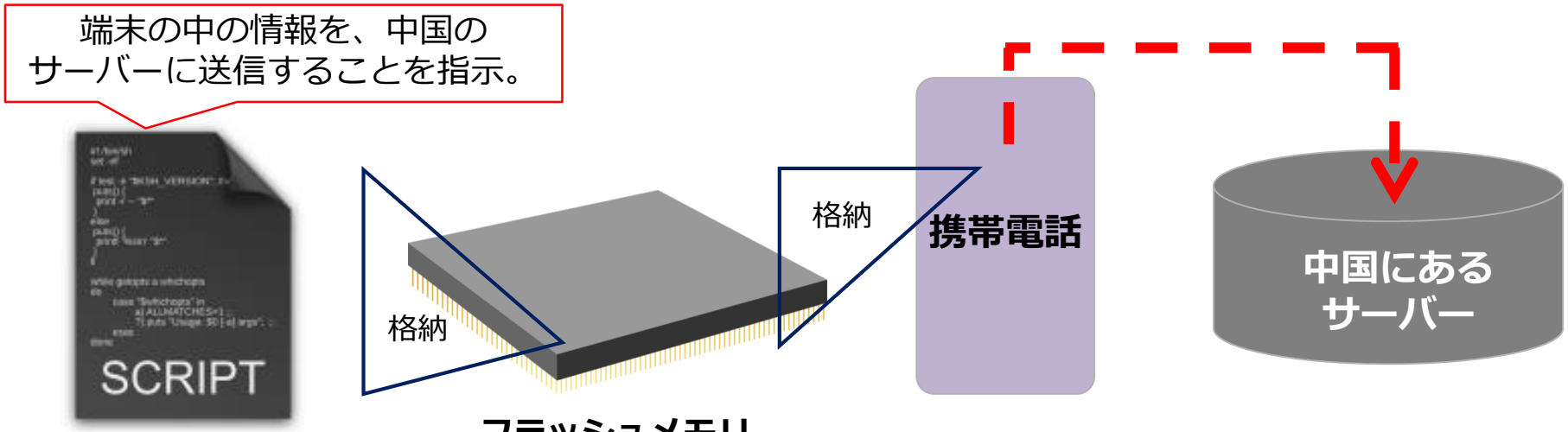
- 平成29年５月、世界の少なくとも約150か国において、Windowsの脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。
- **感染した欧州企業から、サプライチェーン経由で国内企業も感染。**

サイバー攻撃の脅威レベルの向上の例②：
携帯端末に不正プログラムが仕掛けられた事例

- メモリに不正プログラムが仕掛けられ、保存されている情報の不正送信や改ざんを受けるリスクが顕在化。
- **製造時に物理的に組み込まれた不正プログラムは検知や削除が容易ではない。**

フラッシュメモリに不正プログラムが仕掛けられた事例

- 2016年、**米国セキュリティ会社が携帯電話のフラッシュメモリのファームウェアに仕込まれている不正プログラムを発見**。
- 中国企業が開発・製造したもので、ユーザーの同意なしに、72時間おきに携帯電話内の情報が中国のサーバーに送信される。



不正プログラム（イメージ）　フラッシュメモリ

サイバー攻撃の脅威レベルの向上の例③：制御系にまで影響が波及

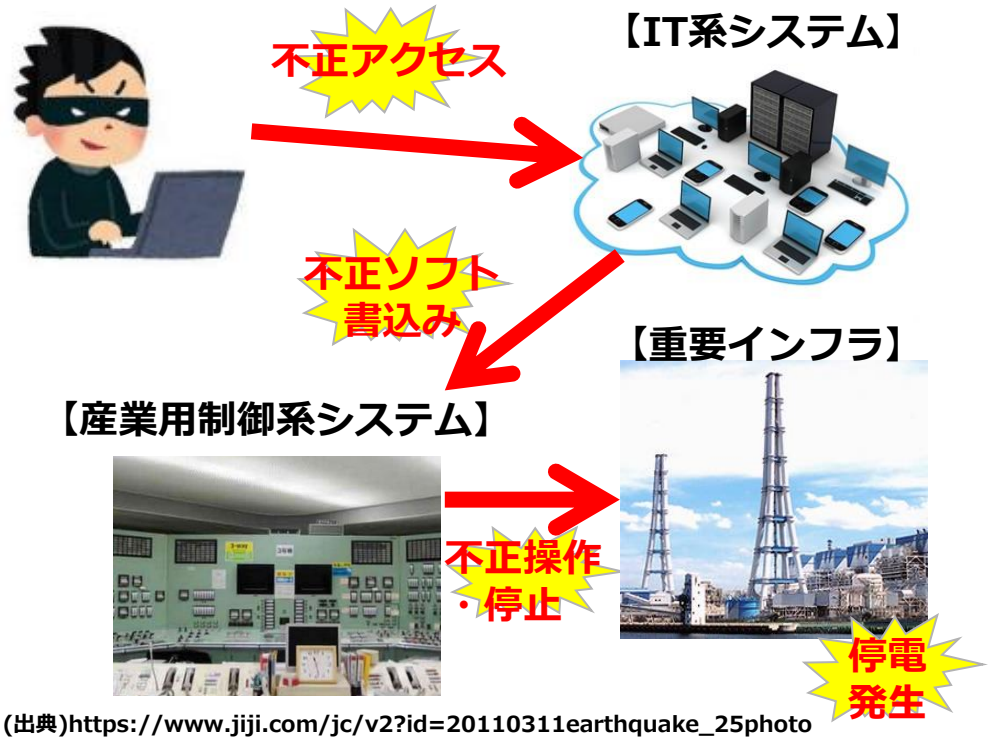
- 米国ICS-CERTの報告では、**重要インフラ事業者等において、制御系にも被害が生じている**。
- ウクライナでは、2015年と2016年にサイバー攻撃による停電が発生。**2016年の攻撃(CrashOverRide)**では、**サイバー攻撃のみで、停電が起こされた**。

米国の重要インフラへのサイバー攻撃の深さ

攻撃のうち約一割は、制御系までサイバー攻撃が到達

（出典）NCCIC/ICS-CERT Year in Review FY2015
Homeland Security より経済産業省作成

2016年に発生したウクライナの停電に係る攻撃（CrashOverRide(Industryoyer)）



(出典)https://www.jiji.com/jc/v2?id=20110311earthquake_25photo
(出典)www.chuden.co.jp/hekinan-pr/guide/facilities/thermalpower.html

米国電力事業者を標的とした北朝鮮によるサイバー攻撃

- 2017年9月22日、北朝鮮のハッカー集団「TEMP.Hermit」が複数の米電力事業者を標的にスピアフィッシングメール攻撃を行った（FireEye報告書より）。
- 今回の攻撃は、検知・阻止されたものの、電力事業者のシステムに致命的な打撃を与えるための偵察活動であったと見られている。

本攻撃による脅威の詳細

偵察活動

① 資金調達パーティへの招待状を偽装したメールが複数の米電力事業者宛に届く
② マクロが含まれている添付ファイルを開封すると、バックドア型マルウェア「PEACECOFFEE」がインストールされ、ポート443を通じてC&Cサーバとの通信を開始
③ 攻撃者は、 C&Cサーバを介し、ファイルのアップロードやダウンロード、ファイルリストの作成等、任意のコマンドを実行

電力制御系システムの防御対策等の情報漏えい → さらなる攻撃による電力供給停止

ビル分野のセキュリティ事故事例：病院

● 警備員による病院のHVACシステムのハッキング（内部犯行による空調システムへのハッキング）

日時	2009年4月～6月
攻撃対象	米国テキサス州ダラス W.B. Carrell Memorial Clinic
侵入経路	病院のHVACシステム（暖房換気空調システム）、患者情報を扱うコンピュータ等の不正アクセス
被害	**システムへの侵入、システム画面のオンライン上での公開、未遂だがDDoS攻撃の計画あり**

TimeLine	経緯・概要
（背景）	同病院の夜勤の契約警備員（当時25）は、オンライン上で“Ghost Exodus”という名前で活動し、ハッカーグループ“Electronik Tribulation Army” のリーダも務めていた。
攻撃 *2009.4-6*	警備員は同病院のHVACシステムや顧客情報のコンピュータに侵入し、HVACシステムのHMI画面のスクリーンショットをオンラインで公開。公開された画面では、手術室のポンプや冷却装置を含め、病院の様々な機能のメニューが確認できる。さらに、病院内のPCにマルウエアをインストールする（DDoS攻撃のため、PCをボットネット化したものとみられる）様子なども動画に撮って公開している。
―	一方、病院の職員はアラーム設定が停止されたことで、HVACシステムのアラームがプログラム通りに機能せず、不思議に思っていたが、内部から発覚することはなかった。
発覚・逮捕 *2009.6*	SCADAセキュリティの専門家がハッカーの知り合いからの情報を得て調査し、FBI及びテキサス州検察局に報告したことで発覚し、2009年6月26日警備員は逮捕された。（連邦刑務所への9年の禁固刑を受ける。）
攻撃計画（未遂） *2009.7*	逮捕により未遂に終わったものの、警備員は、乗っ取られた病院のシステムを使って2009年7月4日（独立記念日）に大規模なDDoS攻撃を仕掛ける計画を立てており、インターネット上で協力してくれるハッカー仲間を募っていた。また、既に攻撃予定日の前日に辞職する旨を所属する警備会社に伝えていた。

出典：DOJプレスリリース (https://www.justice.gov/archive/usao/txn/PressRel09/mcgraw_cyber_compl_arrest_pr.html)

(写真出典) http://www.gsr-andrade.com/#!/page/118644/healthcare

その他ビル分野のセキュリティ事故事例

- 海外を中心に多くの実際の事件や脆弱性の発見事例が見られる。

時期	内容
2011年11月	コロンビア大の研究者がオフィス等に導入されているLaserJetプリンターに脆弱性があり、ハッカーからのアップデート指示により過剰な運転状態となって、最終的には発火することを証明した。対象は何百万台にもおよぶ。
2012年4月	MITの学生が同大学グリーン棟の照明システムをハッキングし、ビルの窓照明を巨大なテトリスゲームにしてしまった。
2013年8月	フロリダ州マイアミのターナー・ギルフォード・ナイト矯正センターの警備システムが何者かにハックされ、収容房の扉のロックをリモート解除し、受刑者が敵対ギャングに属する別の受刑者を襲う事件が発生。
2013年5月	米セキュリティ企業が、オーストラリア・シドニーのオフィスのビル管理システムへの侵入テストを実施し、フロア空調やエネルギーメーター、アラームといったビル管理機能への侵入を実現。同ビルの設備管理に使われているデバイスは、世界中で数十万個利用されている。
2014年12月	ドイツの製鋼所のネットワークが標的型メールによるサイバー攻撃を受け、制御システムを乗っ取られた。その結果、プラントの各所に障害が発生し、溶鉱炉が制御不能となり、最終的に停止不能となった。
2016年1月	IBMのチームが商業オフィスのBASに対するペネトレーションテストを実施し、複数のビルを遠隔のBASで管理しているようなケースにおいて、全米の複数のビルの自動コントローラに対する完全な指揮権を入手出来ることを明らかにした。
2016年11月	フィンランド南東部の都市・ラッペーンランタのビルがDDos攻撃を受け、空調や温水管理をしていたコンピュータが不調をきたし、暖房が停止した。比較的早急に回復出来たが、外気温マイナス2度の環境で、しばらく暖房を利用できない状況となった。

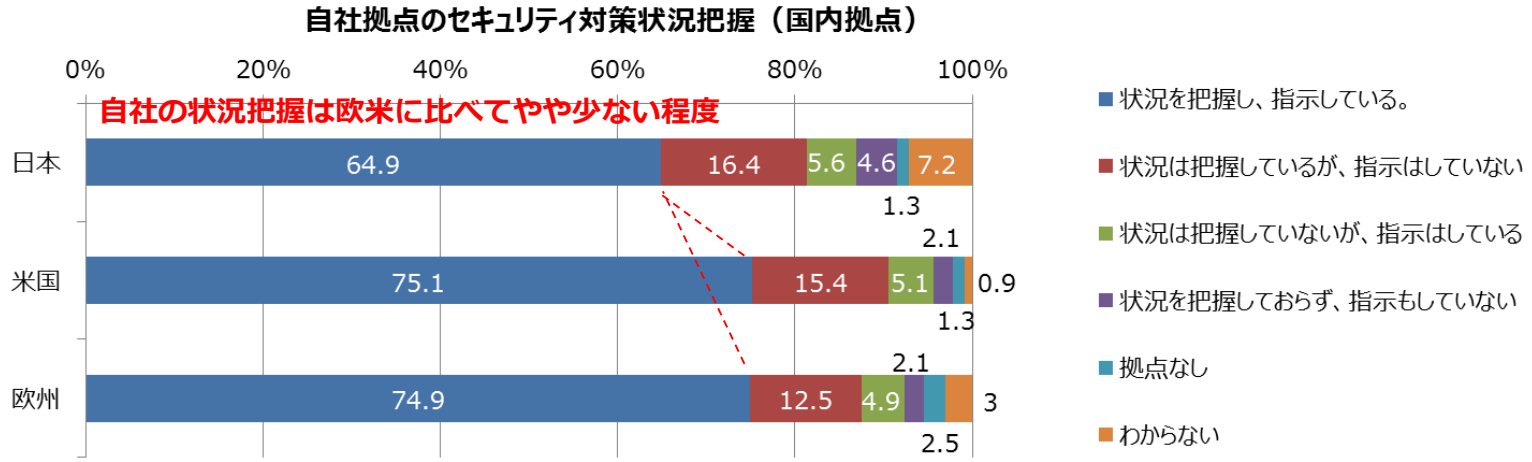
中小企業の被害事例

- 重要インフラや大企業だけでなく、中小企業においてもサイバー攻撃の被害は発生

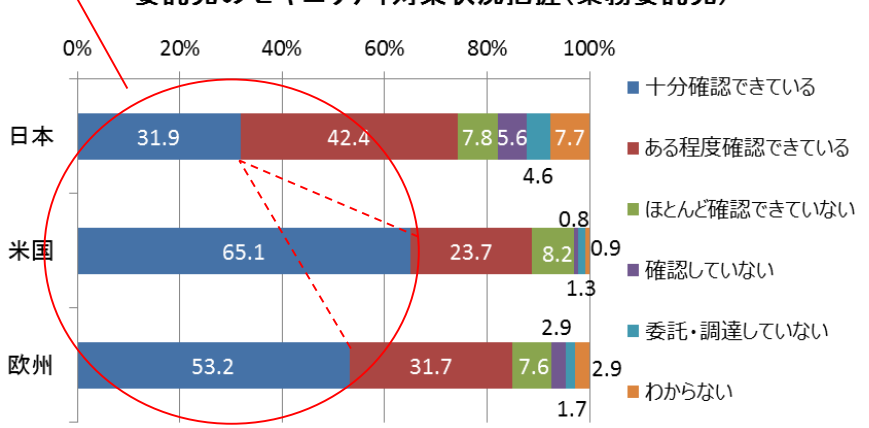
事例	業種	所在地	従業員規模
役員のパソコンが**ウイルスに感染**し、保存されていた過去の電子メールが、これまでの送受信先などに大量に送信され、自社および取引先の**重要な情報が漏えい**してしまった。取引先からはクレームが上がり、謝罪をしたものの**信頼を失墜**することとなった。 ウイルス対策ソフトのアップデートが実施されていなかった。	製造業	栃木県	51～100名
ウイルス対策ソフトの契約更新を失念し、数日間サポートが切れた。そのわずかの間に、インターネットに繋がっていたパソコンが**「トロイの木馬」に感染**した。 急ぎアプリケーションを停止し、自社でリカバリーしたが、**復旧までに約2か月**を要し、その間、仕事にも支障をきたした。	卸売業	福岡県	21～50名
メールサーバが不正アクセスを受け、**電子メールの不正送信の踏み台**にされていた。自社に実害は生じていないものの、**知らない間に攻撃の一端を担う**こととなった。	情報通信業	奈良県	5名以下
オフライン運用していたWindowsXPパソコンを不注意でネットワーク接続したところ**ウェブサイトの閲覧を通じて**ランサムウェアに感染し、**ファイルが暗号化された**。 **バックアップファイルからデータを復元**できたため被害は最小限で済んだ。	製造業	新潟県	21～50名

取引先へのサイバーセキュリティ対策の遅れ

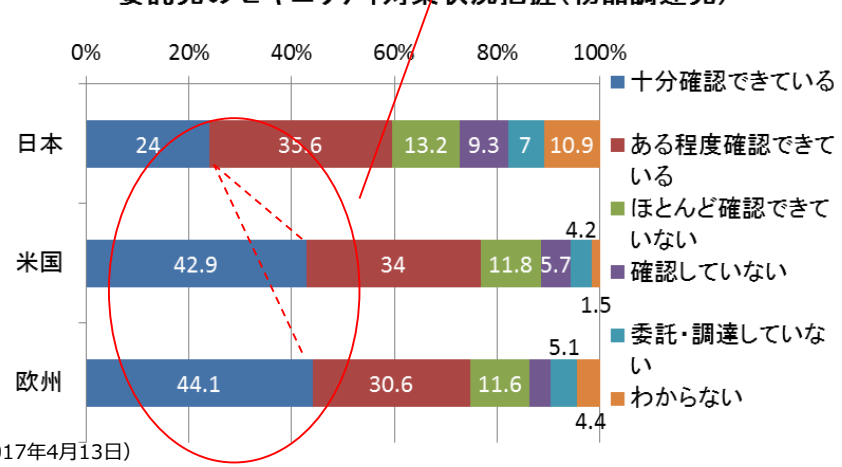
- **日本企業では、委託先等の取引先への対応が大幅に遅れている。**



委託先の状況把握は米国の半分以下、欧州の2/3



調達先の状況把握は欧米の6割以下



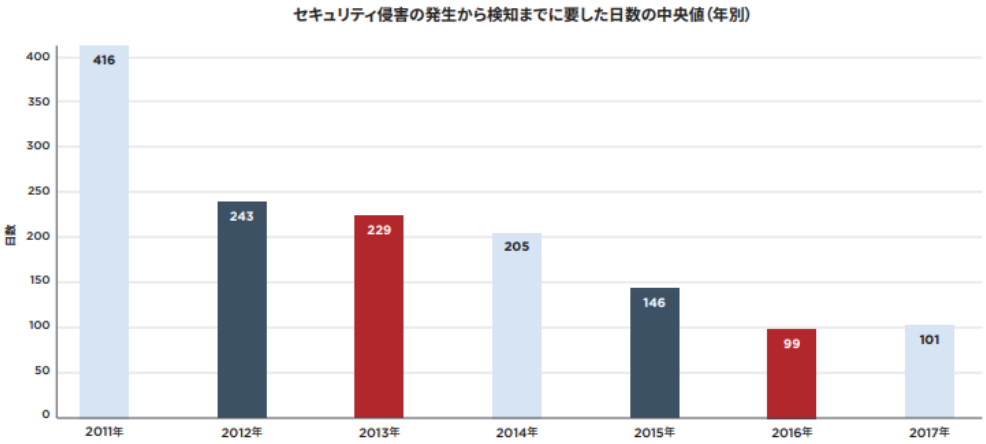
出典：独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017-調査報告書-」（2017年4月13日）

＊ 日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10～11月）

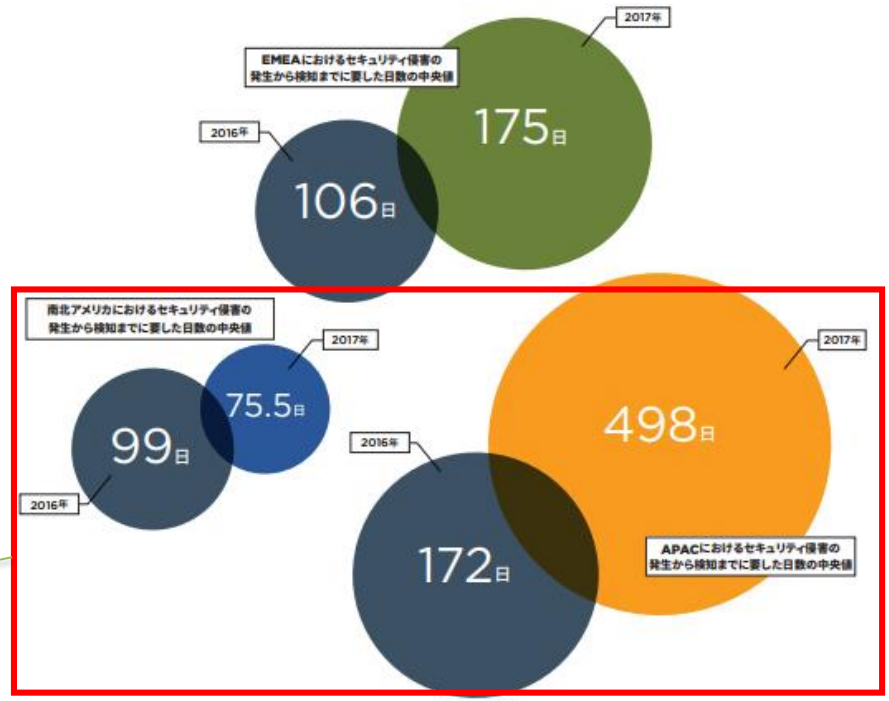
＊ 回収は日本755件、米国527件、欧州526件

セキュリティインシデントの検知に要する日数

- 世界的な動向を見ると、セキュリティインシデントの検知に要する日数は年々減少傾向にある。
- 一方で、APACに目を向けると、昨年と比較して検知に要する日数が遅くなっており、欧米と比較しても大幅に遅いという傾向にある。



南北アメリカでは検知日数が減少しているが、APACでは大幅に悪化。
APAC地域で活動する攻撃者は長い期間、攻撃対象の組織でアクセス権を保持できることになる。

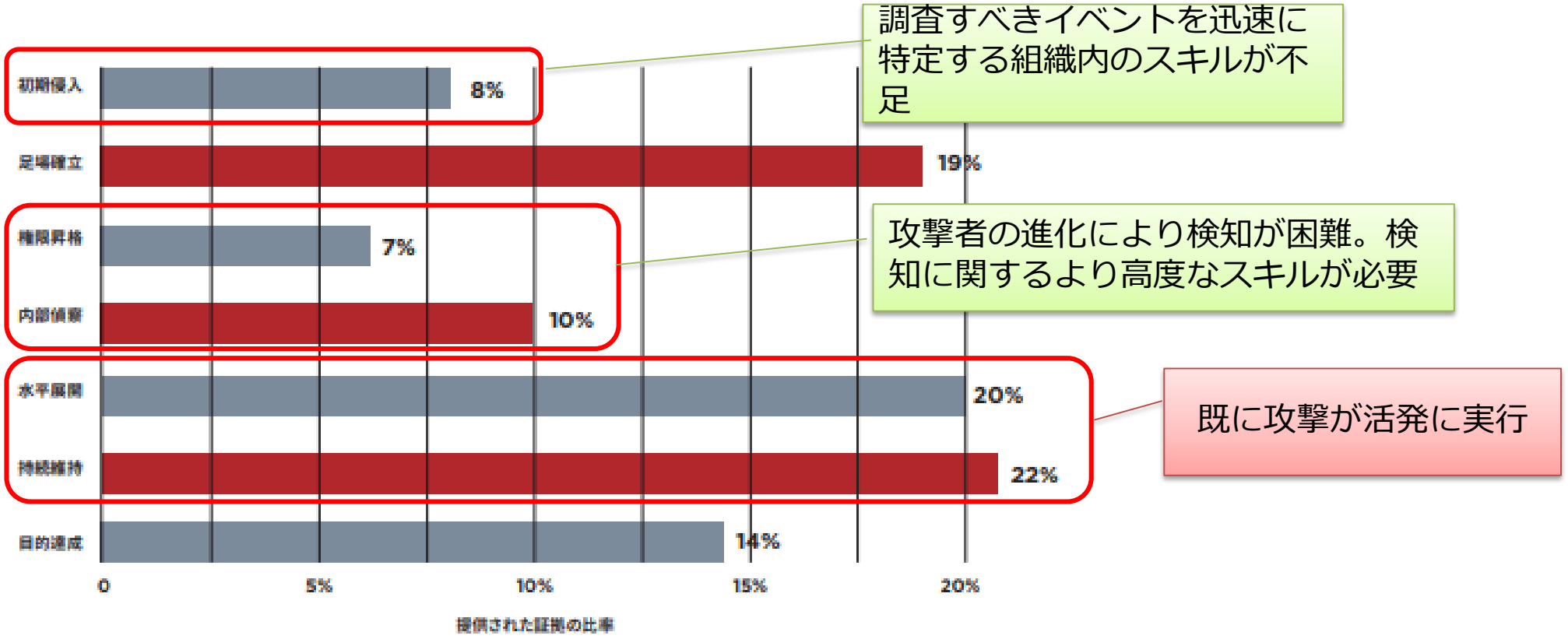


セキュリティ侵害の発生から検知に要した日数（地域別）

（出典）m-TREND2018（FireEye, Inc）

攻撃ライフサイクルの段階毎の検知状況

- 攻撃ライフサイクルの段階毎の検知状況を見ると、多くは「水平展開」、「持続維持」といった既に攻撃が活発化している段階で検知されている。
- 検知の仕組みを活用できる人材（スキル）が不足していることにより、早期の段階で攻撃の兆しを見逃している可能性がある。



（出典）m-TREND2018（FireEye, Inc）

欧米において強化される『サプライチェーン』 サイバーセキュリティへの要求

- **米国、欧州は、サプライチェーン全体に及ぶサイバーセキュリティ対策を模索。**

【米国】

- 2018年4月16日、**サイバーセキュリティフレームワーク**（NIST策定のガイドライン）**に、『サプライチェーンのリスク管理』及び『サイバーセキュリティリスクの自己評価』を追記**
- 2017年末、**防衛調達に参加する全ての企業に対してセキュリティ対策（SP800-171の遵守）を義務化**

【欧州】

- 2018年5月10日、**エネルギー等の重要インフラ事業者に、セキュリティ対策を義務化（NIS Directive）を施行**
- 2017年、**単一サイバーセキュリティ市場を目指し、ネットワークに繋がる機器の認証フレームの導入検討を発表**
- 2018年5月25日、**EUの顧客データを扱う企業に対するデータ処理制限等の新たな義務（GDPR）を施行**
- **ドイツにおいてルーターのテクニカルガイドラインを作成中**

セキュリティ要件を満たさない事業者、製品、サービスは

グローバルサプライチェーンからはじき出されるおそれ

１．サイバー攻撃の脅威レベルの向上と海外の動き

２．産業サイバーセキュリティ研究会

３．経済産業省のサイバーセキュリティ政策動向

サイバーセキュリティ政策の方向性

1．産業政策と連動した政策展開

① 重要インフラの対策強化
－情報共有体制強化　等

② IoTの進展を踏まえたサプライチェーン毎の対策強化 (Industry by industry)
－防衛関係、自動車、電力、スマートホーム等の分野別検討と技術開発・実証の推進

③ 中小企業のサイバーセキュリティ対策強化

2．国際ハーモナイゼーション

① 日米欧間での相互承認の仕組みの構築

② 民間主体の産業活動をゆがめる独自ルールの広がり阻止

3．サイバーセキュリティビジネスの創出支援

① 産業サイバーセキュリティシステムを海外に展開

② サービス認定創設、政府調達などの活用

4．基盤の整備

① 経営者の意識喚起

② 多様なサイバーセキュリティ人材の育成（ICSCoE等）

③ サイバーセキュリティへの過少投資解決策の検討

産業サイバーセキュリティ研究会

- サイバーセキュリティに関し、大所高所の観点から議論し、メッセージを強く発信。
- 政府の政策や、研究会の下に設置するWGの具体的アクションについて方向を提示。

＜構成員＞

※肩書等は平成30年5月30日時点

石原　邦夫　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、東京海上日動火災保険株式会社相談役

鵜浦　博夫　日本電信電話株式会社代表取締役社長

遠藤　信博　日本経済団体連合会情報通信委員長、日本電気株式会社会長、サイバーセキュリティ戦略本部員

小林　喜光　経済同友会代表幹事、株式会社三菱ケミカルホールディングス取締役会長

中西　宏明　日本経済団体連合会副会長・情報通信委員長、株式会社日立製作所会長

船橋　洋一　アジア・パシフィック・イニシアティブ理事長

宮永　俊一　三菱重工業株式会社社長

座長　村井　純　慶應義塾大学教授、サイバーセキュリティ戦略本部員

渡辺　佳英　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

（オブザーバー）

NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

サイバーセキュリティ政策の課題とWG等における対応状況

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催

→ 産業サイバーセキュリティ強化へ向けた**アクションプラン**を提示

- 重要インフラ分野における情報共有体制の構築

→ サイバーセキュリティ基本法改正（NISC）にて対応　　3/9 閣議決定

- 「Society5.0」におけるサプライチェーン全体のセキュリティ確保

→ WG１（制度・技術・標準化）　　第１回　2/7
第２回　3/29
第３回　8/3

- 経営者のサイバーセキュリティに関する意識喚起
- セキュリティ人材の育成
- 日米欧三極の連携強化

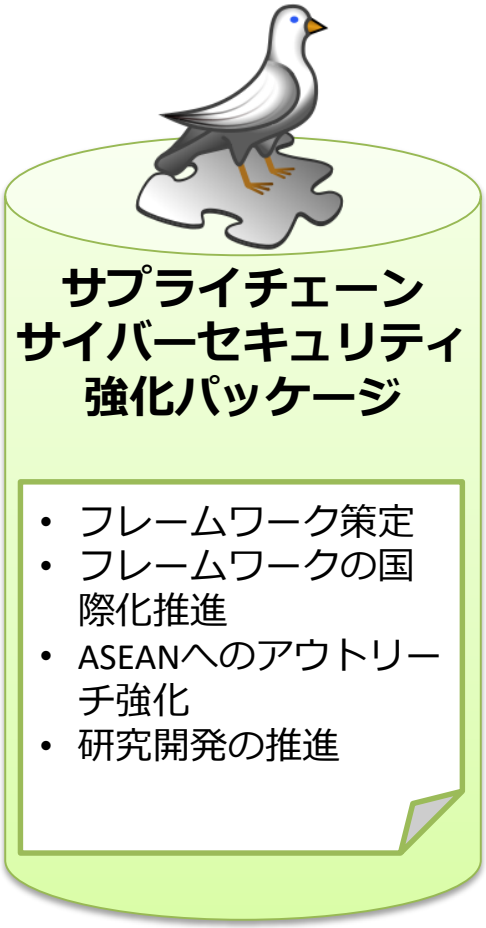
→ WG２（経営・人材・国際）　　第１回　3/16
第２回　5/22

- サイバーセキュリティのビジネス化

→ WG３（サイバーセキュリティビジネス化）　　第１回　4/4
第２回　8/9

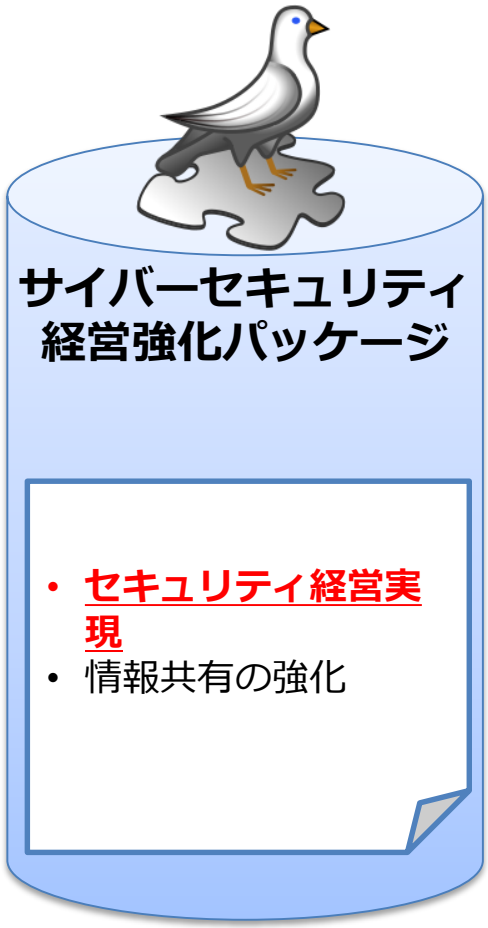
産業サイバーセキュリティ強化へ向けたアクションプラン

- 経済産業省は、産業サイバーセキュリティ強化に向けて、関係省庁と連携しつつ、以下の４つの政策パッケージの実施に取り組む。



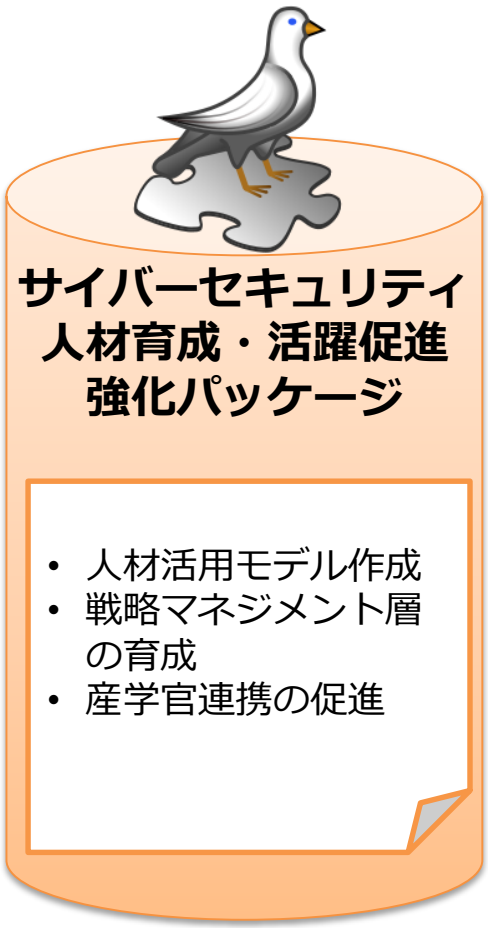
サプライチェーン サイバーセキュリティ 強化パッケージ

- フレームワーク策定
- フレームワークの国際化推進
- ASEANへのアウトリーチ強化
- 研究開発の推進



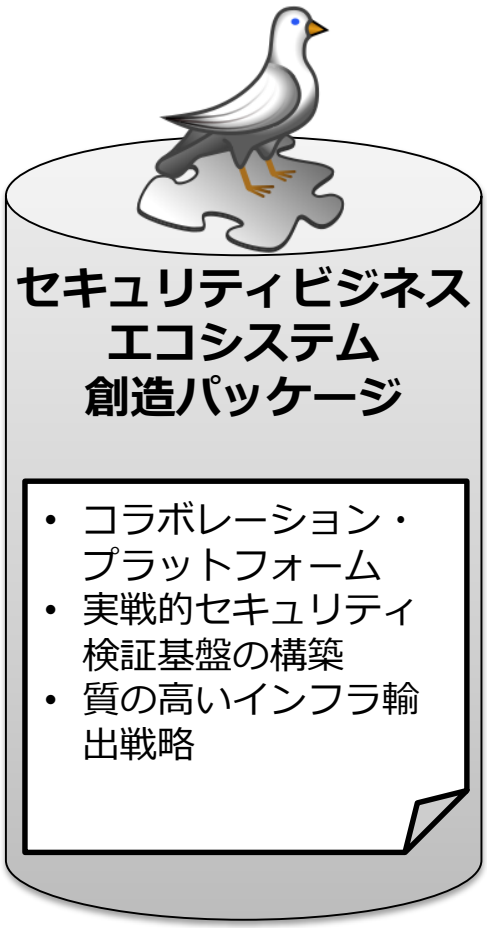
サイバーセキュリティ 経営強化パッケージ

- **セキュリティ経営実現**
- 情報共有の強化



サイバーセキュリティ 人材育成・活躍促進 強化パッケージ

- 人材活用モデル作成
- 戦略マネジメント層の育成
- 産学官連携の促進

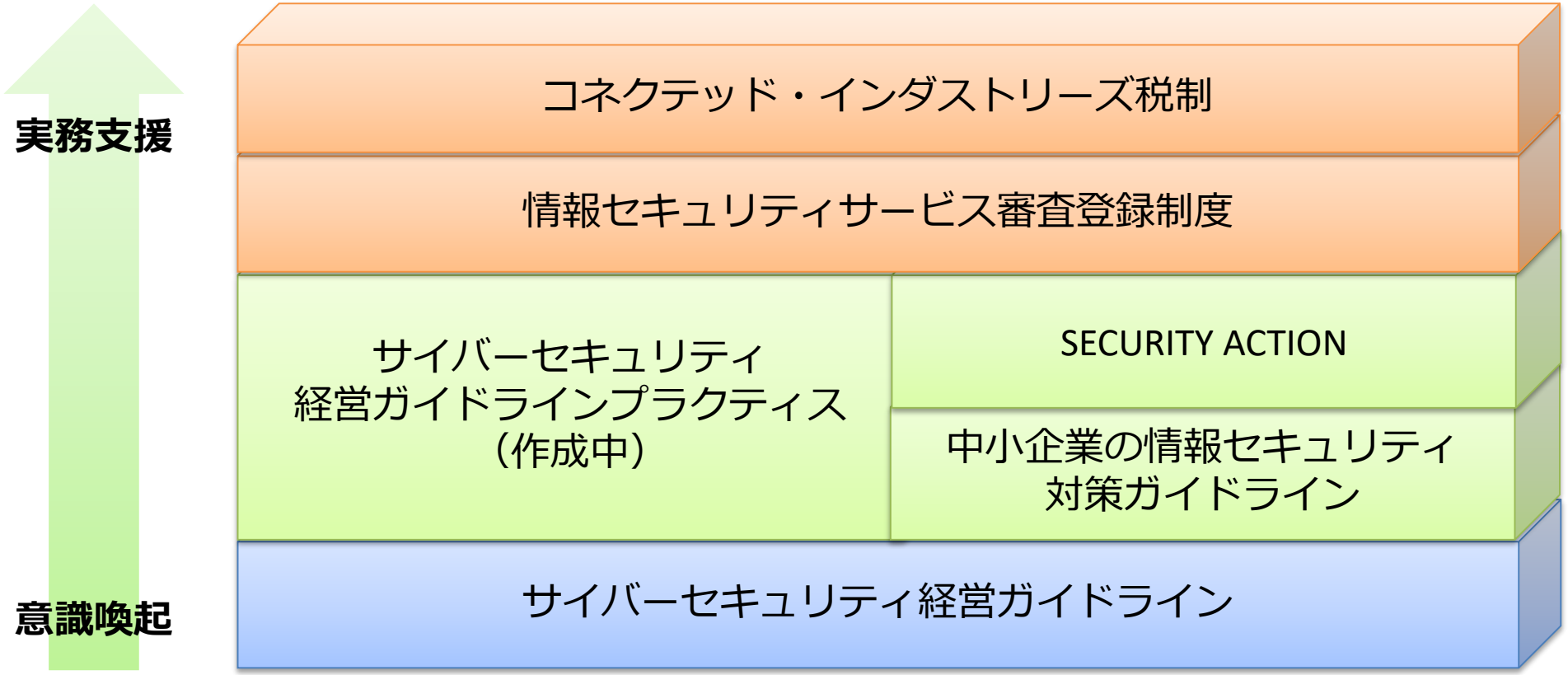


セキュリティビジネス エコシステム 創造パッケージ

- コラボレーション・プラットフォーム
- 実戦的セキュリティ検証基盤の構築
- 質の高いインフラ輸出戦略

サイバーセキュリティ経営の実現

- サイバーセキュリティ経営の実現に向けて、サイバーセキュリティ経営ガイドラインを軸として経営者の意識を喚起。
- 税制やサービス審査登録制度等、経営者からの指示に基づき実務を行う上での支援策も実施。



１．サイバー攻撃の脅威レベルの向上と海外の動き

２．産業サイバーセキュリティ研究会

３．経済産業省のサイバーセキュリティ政策動向

サイバーセキュリティ経営ガイドライン

サイバーセキュリティ対策における経営者の役割

- 企業戦略として、どの程度ITに対する投資やセキュリティ投資を行うかは経営判断。
- 場合によっては経営者責任を問われる恐れ。

経営判断が必要

- 企業戦略として、どの程度IT投資を行うか
  （生産性向上、ビジネス拡大）
- その中で、どの程度セキュリティ投資を行うか
  （企業価値向上）

経営者のリスク対応の是非、経営者責任について社会から問われる恐れ

例えば、以下のような時に問われる恐れがある

- サイバー攻撃により個人情報や秘密情報が漏洩した場合
- インフラの供給停止など、社会に損害を与えてしまった場合

セキュリティに関する経営層の関わり

- 海外と比較すると日本の企業は情報セキュリティに関する意思決定において経営層の関わりが薄い。

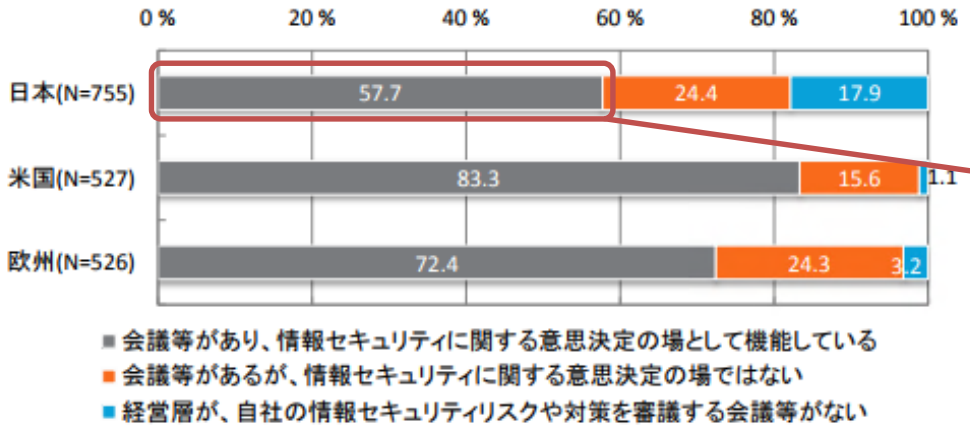


図 5.3-2 経営層の情報セキュリティに対する関与

経営層が積極的にセキュリティに関与している企業は6割弱

セキュリティが経営上のリスクの1つであることを上司から説明を受けている企業は7割弱
（米国は9割強）

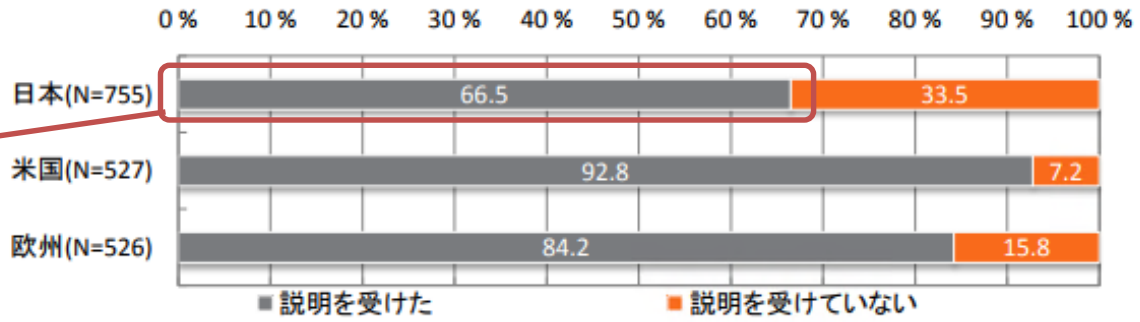


図 5.3-1 経営層または上司からの説明状況

出典：企業のCISOやCSIRTに関する実態調査2017(IPA)

セキュリティ対策に関する責任者（CISO等）の設置状況

- 欧米ではCISOは経営層、又は経営層直下に設置されており、スピード感を持った対応を実施できている。一方で、日本企業は情報システム部門のトップをCISOに任命しているケースが多く、ボトムアップで対策が取られている。

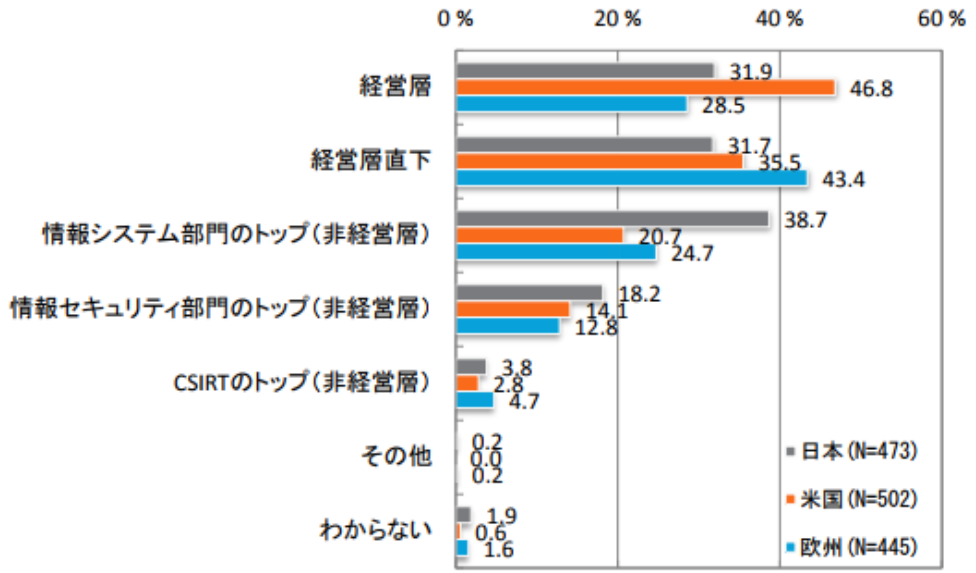


図 5.6-3　CISO 等の組織内の位置づけ

出典：企業のCISOやCSIRTに関する実態調査2017(IPA)

【現場の声】(経済産業省ヒアリングによる)

- 経営層が積極的な関与をしていないため、セキュリティ担当者が会社から評価されにくい
- 企業のセキュリティ担当者はモチベーションが上がらない

➡ セキュリティ人材を育成する上でも経営層が積極的に関与し、会社から評価される体制が必要

サイバーセキュリティ経営ガイドライン

- 経営者のリーダーシップによってサイバーセキュリティ対策を推進するため、**経営者が認識すべき3原則**と、**経営者がセキュリティの担当幹部（CISO等)に指示すべき重要10項目**を提示。

1．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**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等に指示すべき１０の重要事項

リスク管理体制の構築

（１）組織全体での対策方針の策定
（２）方針を実装するための体制の構築
（３）予算・人材等のリソース確保

リスクの特定と対策の実装

（４）リスクを洗い出し、計画の策定
（５）リスクへの対応
（６）PDCAの実施

インシデントに備えた体制構築

（７）緊急対応体制の構築
（８）復旧体制の構築

サプライチェーンセキュリティ

（９）サプライチェーンセキュリティの確保

関係者とのコミュニケーション

（10）情報共有活動への参加

経営者が認識すべき３原則（サイバーセキュリティ経営の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、系列企業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

経営者がCISO等に指示をすべき１０の重要事項 －全体像－

経営者

【３原則】
１．経営者のリーダーシップが重要
２．自社以外（ビジネスパートナー等）にも配慮
３．平時からのコミュニケーション・情報共有

ACT

CHECK

PLAN

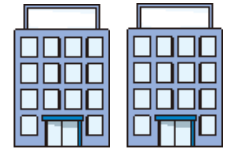
DO

指示

報告

①サイバーセキュリティ対応方針策定

内外に宣言・開示



ステークホルダー
（株主、顧客、取引先等）

②リスク管理体制の構築

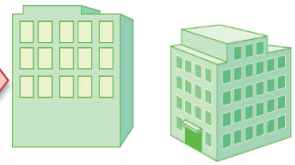
サイバーセキュリティリスク管理体制

◆経営リスク委員会等
他の体制と整合
（ex.内部統制、災害対策）

CISO等の担当幹部

③資源(予算、人材等)の確保

⑨サプライチェーンセキュリティ対策



ビジネスパートナー

セキュリティ担当、CSIRT等

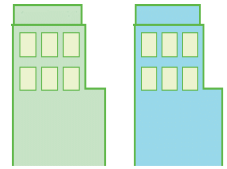
④リスクの把握と対応計画策定

⑤保護対策(防御・検知・分析)の実施

⑦緊急対応体制の整備

⑧復旧体制の整備

⑩情報共有活動への参加



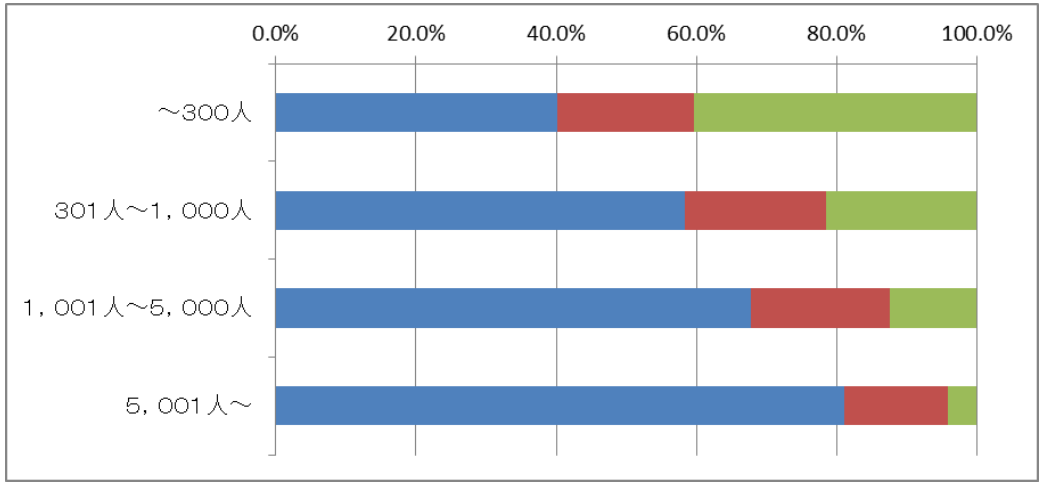
情報共有団体・コミュニティ

⑥PDCAの実施

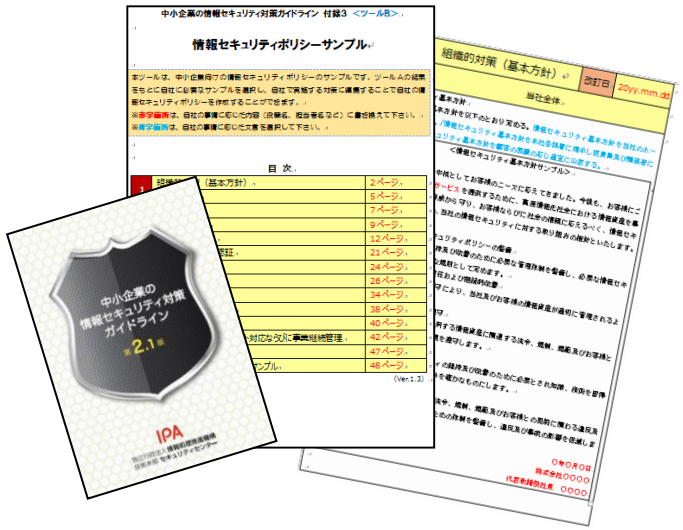
経営者がCISO等に指示をすべき１０の重要事項
(1)サイバーセキュリティリスクの認識、組織全体での対応の策定

サイバーセキュリティリスクへの対応について、組織の内外に示すための方針（セキュリティポリシー）を策定させること。

セキュリティポリシーの策定・社内外への宣言・公表（従業員数別）



参考

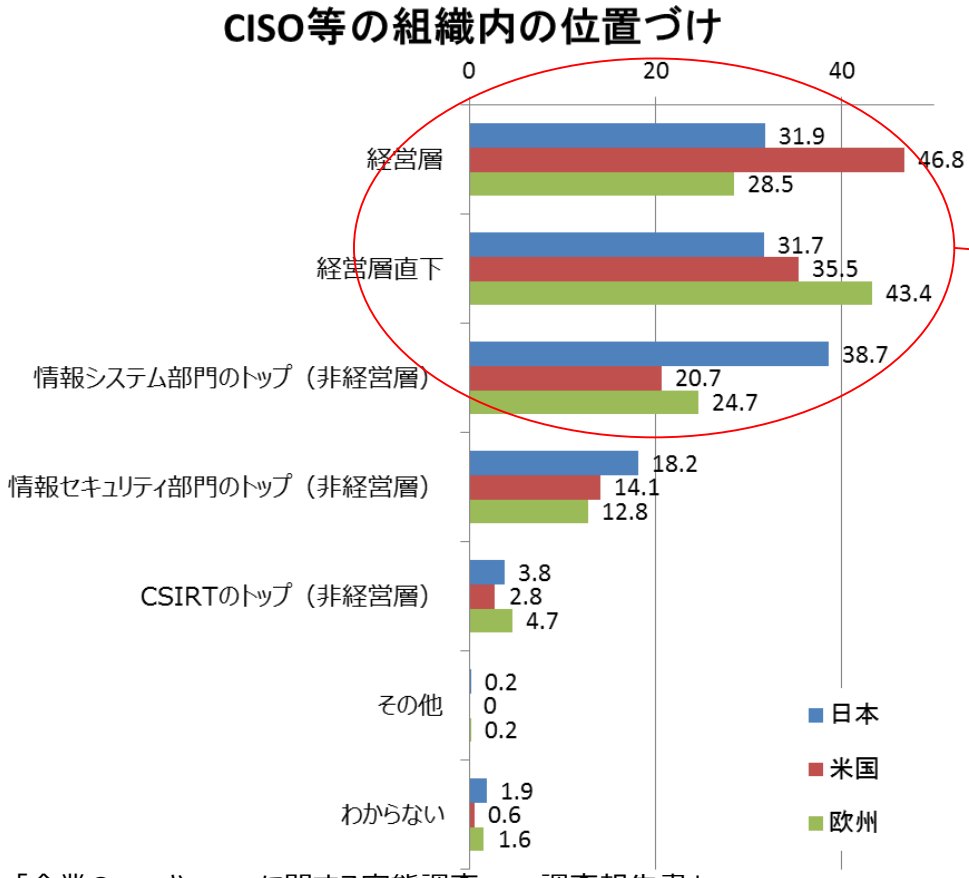


情報セキュリティポリシーサンプル（IPA）
- 中小企業の情報セキュリティ対策ガイドライン 付録３

(*)平成28年度我が国におけるデータ駆動型社会に係る基盤整備（情報処理実態調査の分析及び調査設計等事業）調査報告書（経済産業省）のデータを元に作成
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H28_report.pdf

経営者がCISO等に指示をすべき１０の重要事項
(2)サイバーセキュリティリスク管理体制の構築

方針に基づく対応策を実装できるよう、経営者とセキュリティ担当者、両者をつなぐ仲介者としてのCISO等からなる適切な管理体制を構築すること。



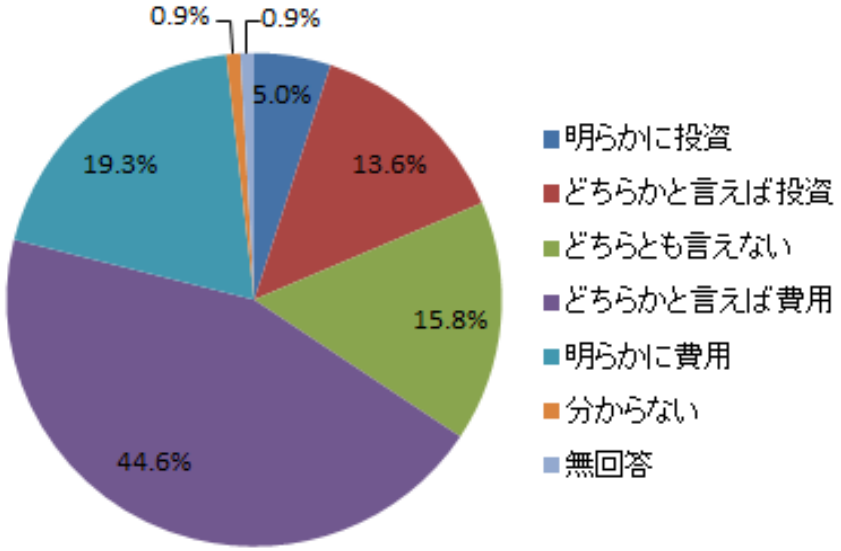
欧米は経営層に紐づくCISOが多い

（出典）IPA「企業のCISOやCSIRTに関する実態調査2017調査報告書」

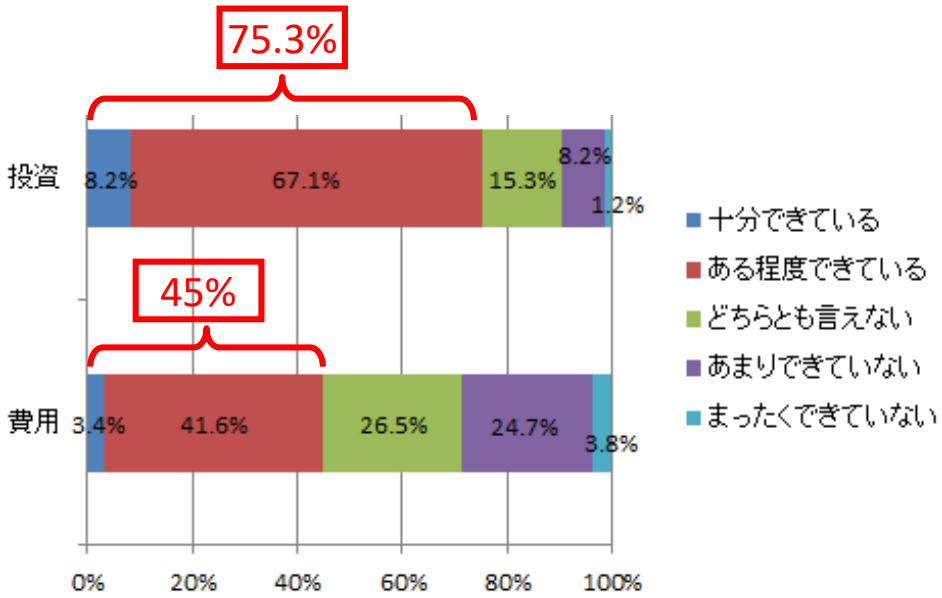
経営者がCISO等に指示をすべき１０の重要事項
(3)サイバーセキュリティ対策のための資源(予算、人材等)確保

サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させること。

【セキュリティ対策の支出の位置づけ】



【必要なセキュリティ予算の確保】



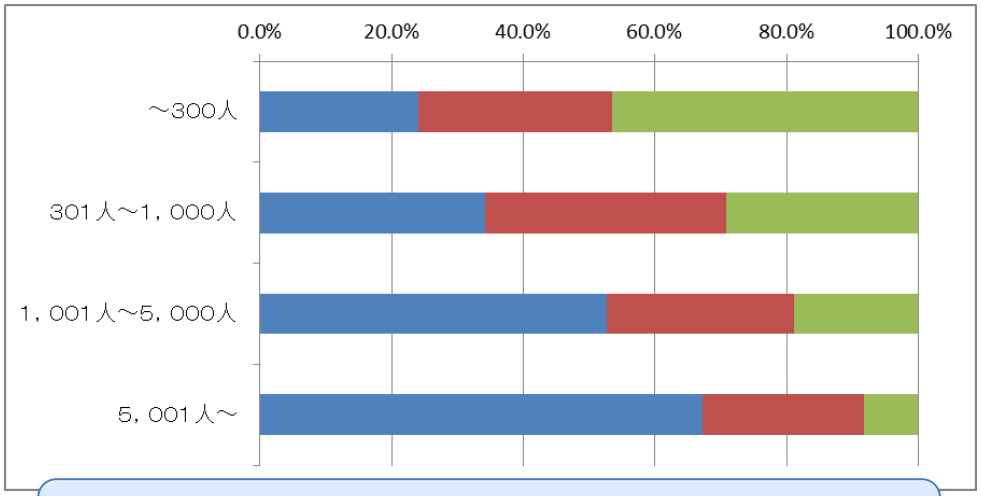
（出典） KPGコンサルティング「セキュリティサーベイ2017」より経済産業省作成

セキュリティ投資を「コスト」ではなく「投資」と位置づける

経営者がCISO等に指示をすべき１０の重要事項
(4)サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

経営戦略を踏まえて守るべき資産を特定し、セキュリティリスクを洗い出すとともに、そのリスクへの対処に向けた計画を策定させること。

社内情報資産に対するリスク分析の実施状況（従業員数別）



5,001人以上の大企業でも実施率67%

■実施している
■検討中、または今後実施予定
■実施していない

参考

リスク分析シート（IPA）

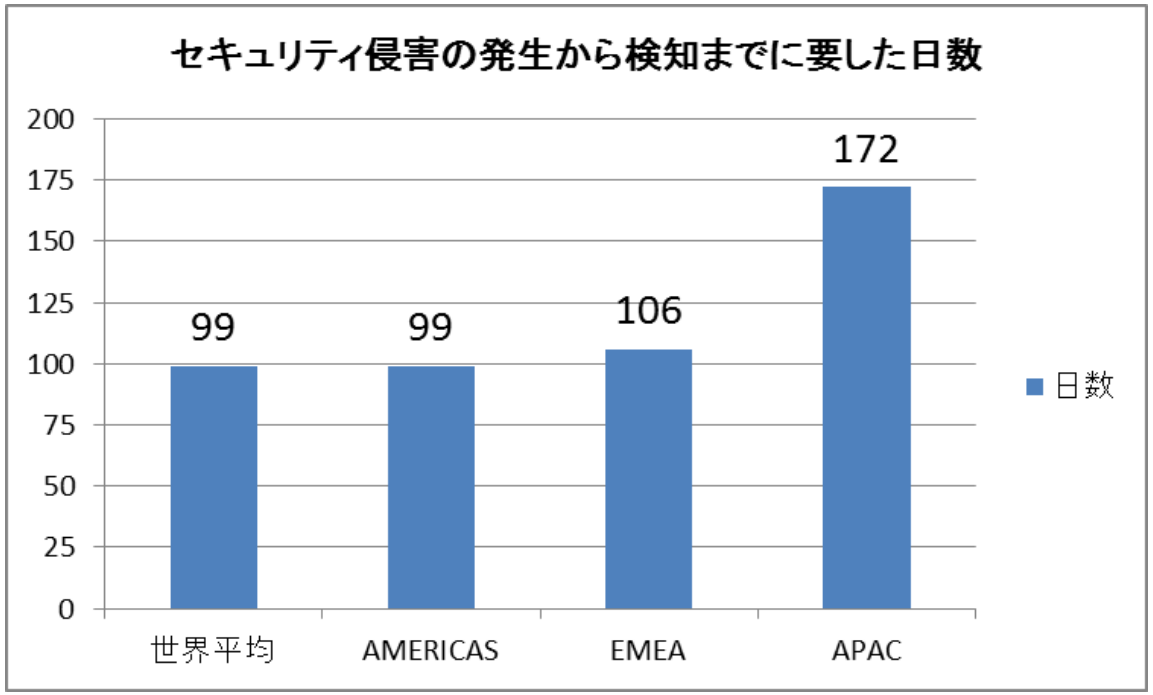
- 中小企業の情報セキュリティ対策ガイドライン 付録３－ツールA

(*)平成28年度我が国におけるデータ駆動型社会に係る基盤整備（情報処理実態調査の分析及び調査設計等事業）調査報告書（経済産業省）のデータを元に作成
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H28_report.pdf

経営者がCISO等に指示をすべき１０の重要事項
(5)サイバーセキュリティリスクに対応するための仕組みの構築

- サイバーセキュリティリスクに対応するために、「防御」、「検知」、「分析」に関する対策を実施させること。

- 「防御」の対策ももちろん重要ではあるが、サイバー攻撃による被害を最小限にするためには早期に「検知」、「分析」を行うための仕組みも重要。

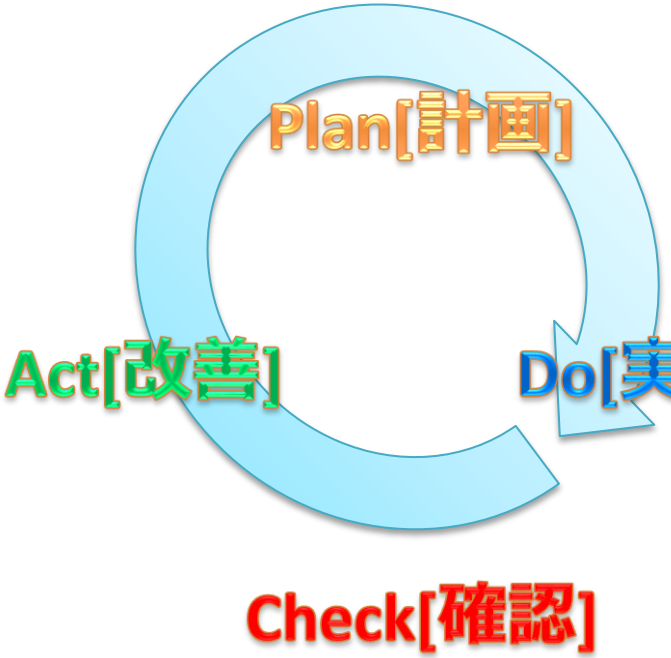


APAC（アジア太平洋）
EMEA（欧州、中東及びアフリカ）

（出典）FireEye. Inc.「M-trends2017：セキュリティ最前線からの視点」より経済産業省作成

経営者がCISO等に指示をすべき１０の重要事項
(6)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

計画が確実に実施され、改善が図られるよう、PDCAを実施させること。



計画の確実な実施と、改善

経営者への
報告

KPIの設定など、
経営者が把握できるよう
可視化して報告

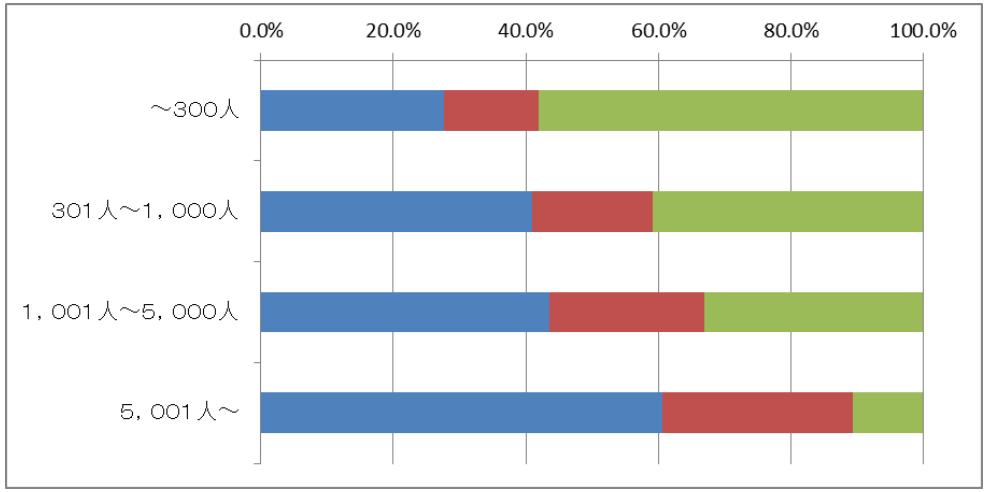
KPIの例

- セキュリティ投資額
- リスク分析の実施回数
- リスクアセスメントの指摘事項数
- セキュリティ教育受講率

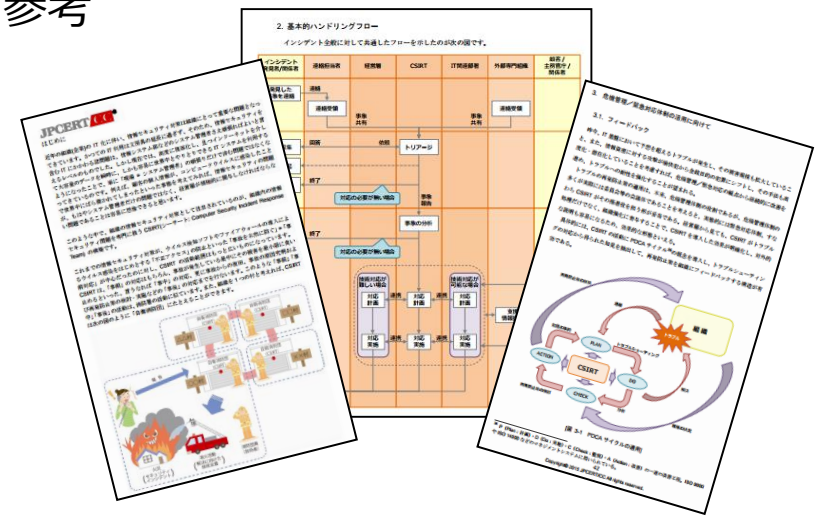
経営者がCISO等に指示をすべき１０の重要事項
(7)インシデント発生時の緊急対応体制の整備

インシデントが発生した場合、「影響範囲や損害の特定」、「被害拡大防止のための初動対応」、「再発防止策の検討」等を実施するための体制（CSIRT等）を構築させること。

インシデント対応のためのチーム、窓口の設置状況（従業員数別）



参考

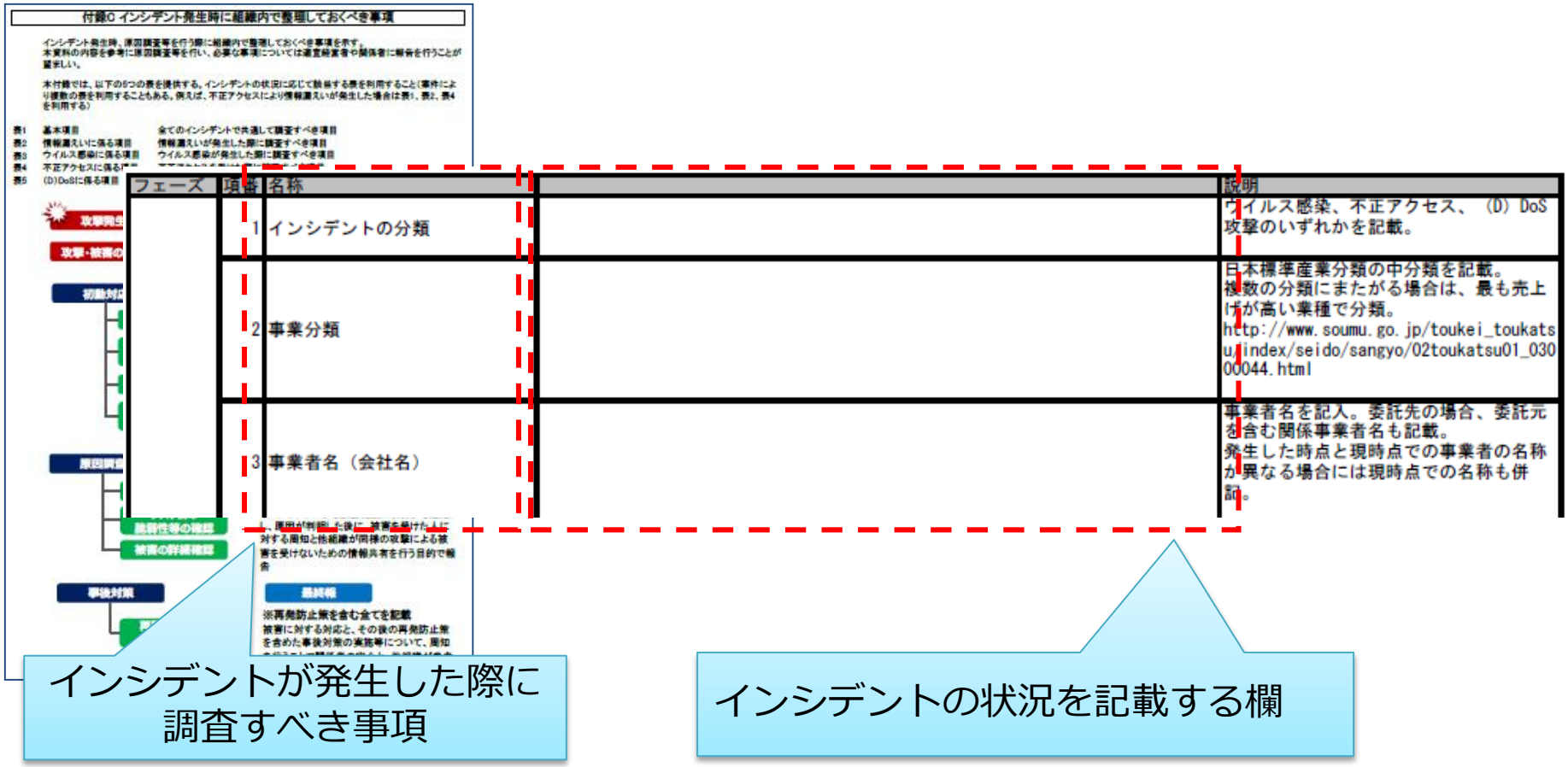


CSIRTマテリアル（JPCERT/CC）

(*)平成28年度我が国におけるデータ駆動型社会に係る基盤整備（情報処理実態調査の分析及び調査設計等事業）調査報告書（経済産業省）のデータを元に作成
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H28_report.pdf

（参考）付録C インシデント発生時に組織内で整理しておくべき事項

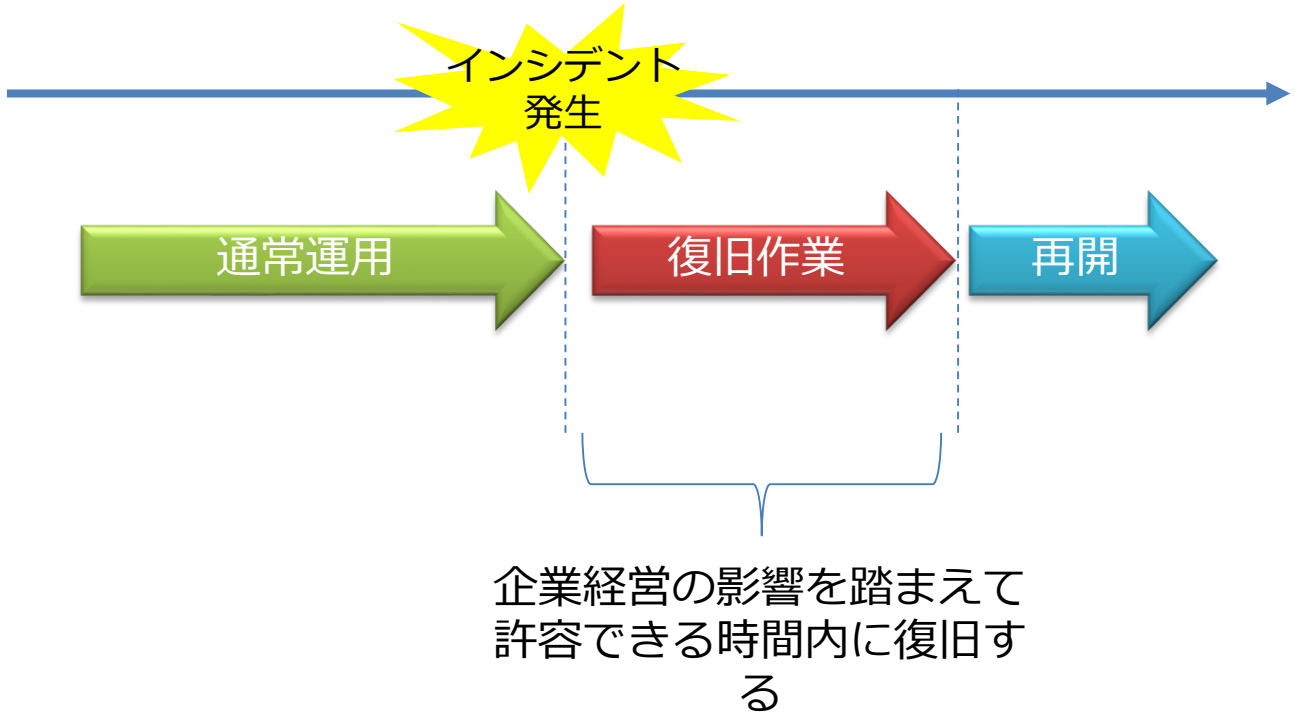
- 事後対策の対応力を強化するために、インシデント発生時に組織として整理しておくべき事項を付録Cで提示。



経営者がCISO等に指示をすべき１０の重要事項
(8)インシデントによる被害に備えた復旧体制の整備

- セキュリティインシデントにより業務停止等に至った場合に、企業経営への影響を最小限にするための復旧計画、復旧手順書、復旧体制等を整備する。

- ランサムウェアやDDoS攻撃等、可用性を損なわせることを目的としたサイバー攻撃も多発している。



経営者がCISO等に指示をすべき１０の重要事項
(9)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・状況把握

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、自社同様にPDCAの運用を含むサイバーセキュリティ対策を行わせること。

◎委託先が標的型サイバー攻撃を受けた事例

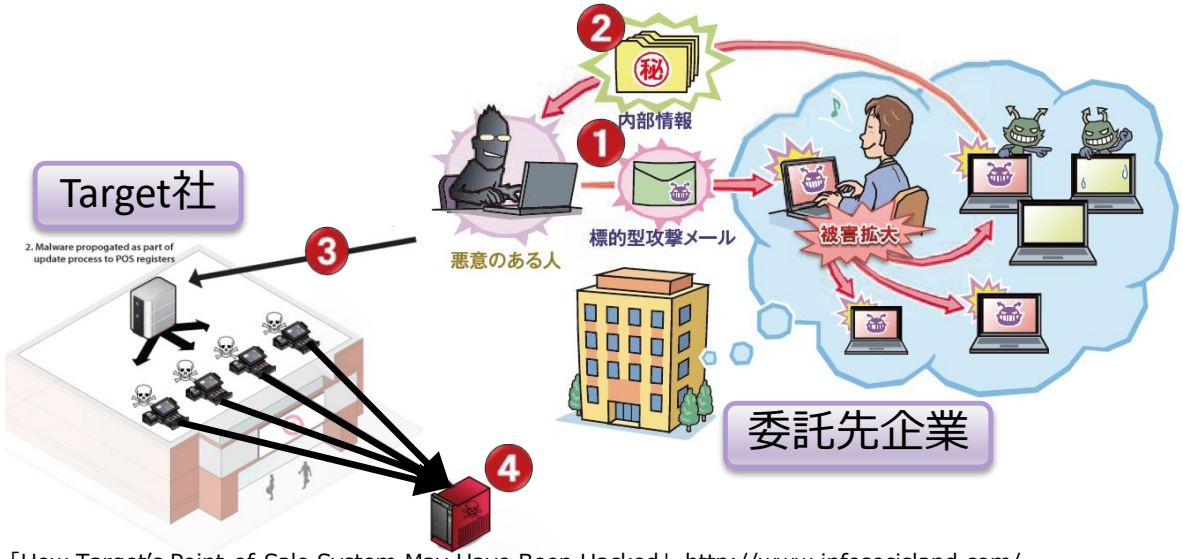
米売上高第５位の小売業者であるTarget社のPOS端末を狙った攻撃により、4,000万件のクレジットカード情報と約7,000万件の個人情報が漏えいした。

①Target社に空調機器システムを提供していた会社にフィッシングメールを送付

②Target社のネットワークに侵入できる暗証番号を不正入手

③Target社のネットワークへ侵入し、マルウェアをPOS端末に送り込む

④情報を外部サーバに送信



出典：「How Target's Point-of-Sale System May Have Been Hacked」 http://www.infosecisland.com/
：日経ビジネスオンライン「セキュリティ対策はコストではない～米国で起きた「ターゲットの悲劇」の教訓～」
http://business.nikkeibp.co.jp/article/opinion/20140604/266189/?rt=nocnt

経営者がCISO等に指示をすべき１０の重要事項
(10)情報共有活動への参加、入手情報の有効活用のための環境整備

攻撃側のレベルは常に向上することから、情報共有活動に参加し、最新の状況を自社の対策に反映すること。また、可能な限り、自社への攻撃情報を公的な情報共有活動に提供するなどにより、同様の被害が社会全体に広がることの未然防止に貢献すること。

情報共有に関する相談先や報告先機関等の例

	名称	概要	運営機関
情報入手	注意喚起情報	深刻かつ影響範囲の広い脆弱性などに関する情報を告知する	JPCERT/CC
	サイバーセキュリティ注意喚起サービスicat	重要なセキュリティ情報を配信するサービス	IPA
情報提供相談	インシデントの対応依頼・情報提供	インシデントに関する報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための助言を行う	JPCERT/CC
	情報セキュリティ安心相談窓口	マルウェア及び不正アクセスに関する技術的なご相談を受け付ける窓口	IPA
	標的型サイバー攻撃の特別相談窓口	標的型サイバー攻撃を受けた際に、専門的知見を有する相談員が対応する窓口	
情報共有	日本シーサート協議会	日本で活動するCSIRT間の情報共有及び連携を図るとともに、組織内CSIRTの構築を促進、支援するコミュニティ	日本シーサート協議会

段階的なサイバーセキュリティ経営の実現

- 以下の3Stepにより、サイバーセキュリティ経営の定着を目指す。

1st Step

サイバーセキュリティ経営の明確化

- サイバーセキュリティ経営ガイドラインの普及・定着

2nd Step

サイバーセキュリティ経営の実践

- CGSガイドラインにサイバーセキュリティを反映
- IRの観点から、サイバーリスクを経営リスクとして認識・自己確認することの重要性を啓発
- 取締役会実効性評価の項目にサイバーリスクを位置づけ
- 投資家に対してもサイバーセキュリティの重要性を啓発

3rd Step

セキュリティの高い企業であることの可視化

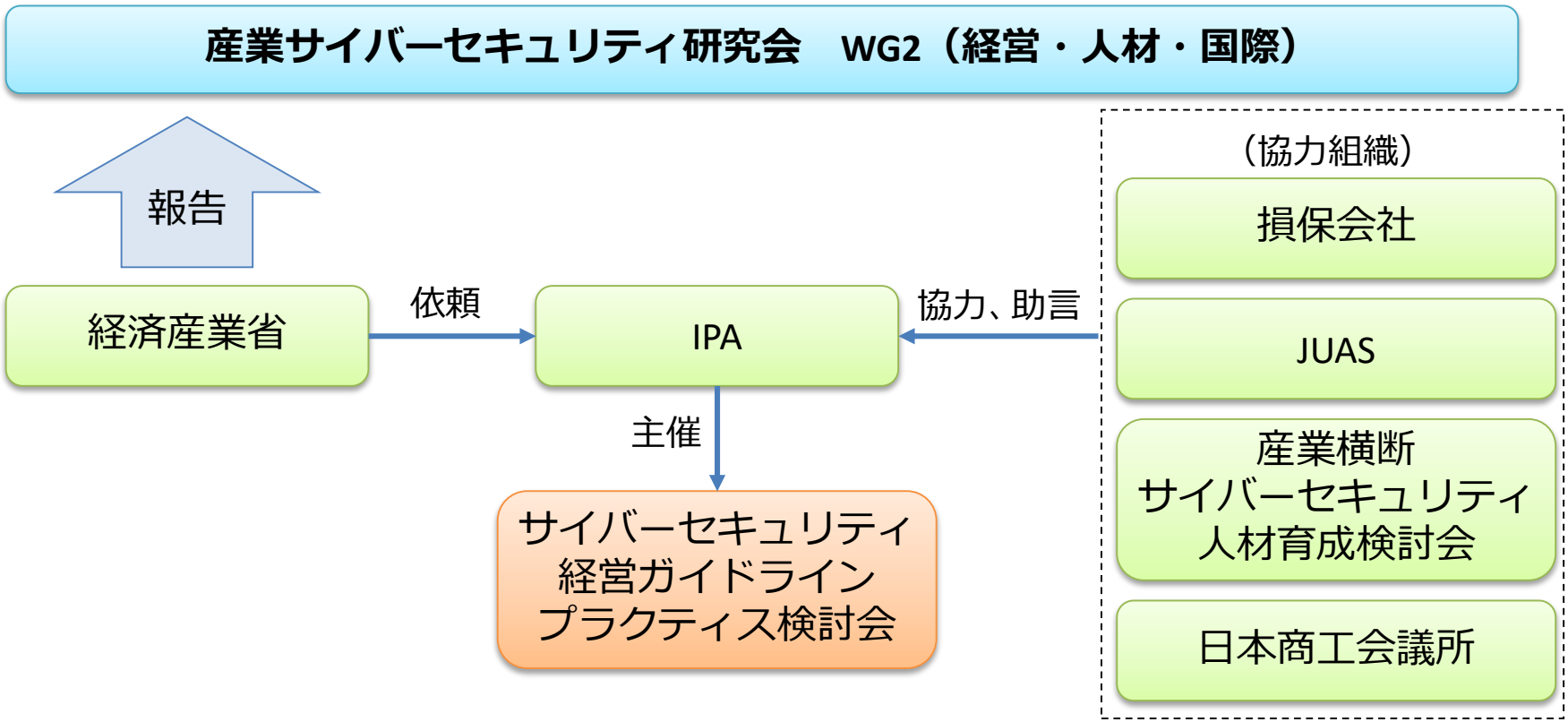
- セキュリティの高い企業であることを投資家が評価できるようにするための、サイバーセキュリティ経営に関する情報の開示の在り方の検討

サイバーセキュリティ経営ガイドラインプラクティスと可視化ツールの作成

- サイバーセキュリティ経営ガイドラインのプラクティスと、セキュリティ対策の実施状況を可視化するツールを作成（平成３０年度中に公開予定）する体制をIPAにて構築。

  ＊ユーザー企業の活動の多様性を踏まえ、多数のセキュリティの実践事例を収集し、体系化する。

＜作成体制＞



企業経営におけるサイバーセキュリティの位置付け強化

- 企業の経営にとって、サイバーセキュリティは重要なリスク管理の一部であり、グループ内企業におけるセキュリティ確保も含め、適切な体制整備が必要。
- また、中小企業をはじめとする取引先も含め、サプライチェーン全体でセキュリティ意識を向上していくことも重要。
- コーポレート・ガバナンス・システムに関する議論において、「守り」のリスク管理の一環としてサイバーセキュリティ対策を位置付けることについて検討が必要ではないか。

＜参考＞「コーポレート・ガバナンス・システムに関する実務指針（CGSガイドライン）」（平成29年3月）の内容

1. 形骸化した取締役会の経営機能・監督機能の強化

- **中長期の経営戦略、経営トップの後継者計画**の審議・策定
- 個別業務の執行決定は対象を絞り込み、CEO以下の**執行部門に権限委譲**

2. 社外取締役は数合わせでなく、経営経験等の特性を重視

- 人選理由を後付けで考えるのではなく、最初に必要な社外取締役の**資質、役割を決定した上で人選**
- 社外取締役のうち**少なくとも１名は企業経営経験者**を選任（逆に、経営経験者は他社の社外取を積極的に引受け）

3. 役員人事プロセスの客観性向上とシステム化

- CEO・経営陣の選解任や評価、報酬に関する**基準及びプロセスを明確化**
- 基準作成やプロセス管理のため、**社外者中心の指名・報酬委員会を設置・活用**（過半数が社外、半々なら委員長が社外）

4. CEOのリーダーシップ強化のための環境整備

- 取締役会機能強化により、CEOから各部門（事業部、海外・地域拠点等）への**トップダウンをやりやすく**
- **退任CEOが相談役・顧問**に就任する際の**役割・処遇の明確化**
- 退任CEOの就任慣行に係る積極的な**情報開示**

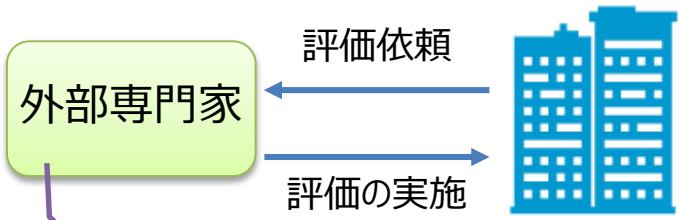
取締役会の実効性評価及び外部専門家との連携による実効性評価の強化

- コーポレートガバナンス・コードでも求められている取締役会の実効性評価（原則４－１１）に、サイバーセキュリティへの関与も評価項目として組み込むことを促進。
- 評価結果の信頼性を向上させる**外部専門家と連携し、サイバーセキュリティへの関与状況も考慮した実効性評価を促進**するとともに、**投資家に対するサイバーセキュリティの教育を実施**。

コーポレートガバナンス・コード
（株式会社東京証券取引所）

【原則４－１１．取締役会・監査役会の実効性確保のための前提条件】
（中略）
取締役会は、**取締役会全体としての実効性に関する分析・評価を行う**ことなどにより、その機能の向上を図るべきである。

補充原則
４－１１③　取締役会は、毎年、各取締役の自己評価なども参考にしつつ、取締役会全体の実効性について分析・評価を行い、**その結果の概要を開示すべき**である。
（コーポレートガバナンス・コードより抜粋）



実効性評価のコンサルティングメニューに「サイバーセキュリティへの関与」を追加

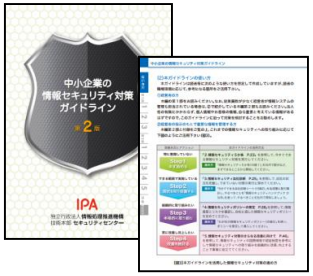
（参考）　英国における実効性評価の位置づけ
2010年に制定された英国コーポレートガバナンス・コードにおいて、主要な上場企業（FTSE350企業）には**外部の専門家を関与させた評価を少なくとも3年ごとに実施することを要求**。

B.6.2. Evaluation of the board of FTSE 350 companies should be externally facilitated at least every three years. The external facilitator should be identified in the annual report and a statement made as to whether they have any other connection with the company.
（The UK Corporate Governance Code（Financial Reporting Council）より抜粋）

中小企業の
情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策ガイドライン（平成28年11月15日公開）

- 中小企業向けのガイドラインをIPAにて公開。
- これまでセキュリティ対策を実施していなかった企業向けの対策や、ある程度対策の進んでいる企業向けの対策の提示など、企業のレベルに合わせてステップアップできるような構成としている。



ガイドライン本体

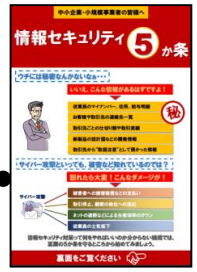
経営者向けの解説

サイバーセキュリティ経営ガイドラインの内容を中小企業向けに整理し、
経営者が認識すべき３原則と実施すべき重要７項目を解説

管理者向けの解説

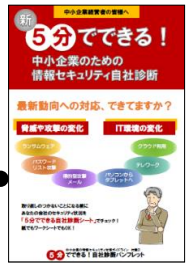
管理者が具体的にセキュリティ対策を実施していくための方法を、
企業のレベルに合わせて段階的にステップアップできるような構成で解説

Step1 まず始める



最低限実施すべき
セキュリティ対策の5箇条

Step2 現状を知り改善する



簡易的な
セキュリティ対策の25項目

Step3 本格的に取り組む

セキュリティポリシーを策定し、
組織的な対策の取り組み

Step4 改善を続ける

第三者認証(ISMS)の取得を
目指した取り組み

セキュリティ対策自己宣言「SECURITY ACTION」

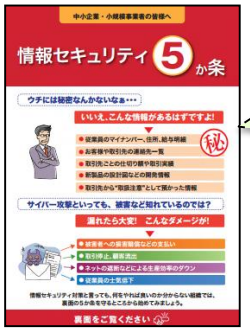
- 中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度をIPAにて開始(*)。
- 二つ星を宣言した企業には、サイバー保険の保険料を割り引く制度も損保会社（損保ジャパン）より提供。

★ 一つ星

SECURITY ACTION ★

セキュリティ対策自己宣言

情報セキュリティ5か条に取り組む企業



① OS・ソフトウェアの最新化
（パッチ適用、バージョンアップ）
② ウイルス対策ソフトの導入
③ 強固なパスワード設定
④ データ等は必要最低限の人のみに共有
⑤ 攻撃の手口の把握

★★ 二つ星

SECURITY ACTION ★★

セキュリティ対策自己宣言

情報セキュリティ自社診断により自社の状況を把握し、セキュリティポリシーを策定する企業

25の診断項目により
自社の対策状況を把握

セキュリティポリシー
策定のためのひな形も提供

(*) https://www.ipa.go.jp/security/security-action/

コネクテッド・インダストリーズ税制

コネクテッド・インダストリーズ税制

（所得税・法人税・法人住民税・事業税）

- **一定のサイバーセキュリティ対策**が講じられた**データ連携・利活用**により、**生産性を向上させる取組**について、それに必要となる**システムや、センサー・ロボット等の導入**に対して、**特別償却30%又は税額控除3%（賃上げを伴う場合は5%）**を措置。
- 事業者は当該取組内容に関する**事業計画を作成**し、**主務大臣が認定**。**認定計画に含まれる設備に対して、税制措置を適用（適用期限は、平成32年度末まで）。**

【計画認定の要件】

①データ連携・利活用の内容

・社外データやこれまで取得したことのないデータを社内データと連携

・企業の競争力上重要なデータをグループ企業間や事業所間で連携

②セキュリティ面

必要なセキュリティ対策が講じられていることをセキュリティの専門家(登録セキスペ等)が担保

③生産性向上目標

投資年度から一定期間において、以下のいずれも達成見込みがあること

・労働生産性：年平均伸率２%以上

・投資利益率：年平均15%以上

課税の特例の内容

➢ 認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% （法人税額の15%を限度）
		5％ ※ （法人税額の20%を限度）

【対象設備の例】
データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、ＡＩ、ソフトウェア等）、サイバーセキュリティ対策製品　　等

最低投資合計額：5,000万円

※ 計画の認定に加え、継続雇用者給与等支給額の対前年度増加率≧３％を満たした場合。

データの安全管理に関する要求事項

- 様々なモノがつながることにより、サイバー攻撃によるリスクの増大も懸念されるため、本税制では必要なセキュリティ対策（以下７項目）を講じていることを要求。
- セキュリティ対策の妥当性については専門家（登録セキスペ等）による確認が必要。
- 制度上、専門家が申請書に署名を行ったこと自体で、インシデント発生時の損害賠償責任等を追うことは特段定めていない(*)。

① データにアクセスできる組織又は個人を必要最小限に制限する機能

② データ連係を行うシステム間の通信経路から盗取されないような機能

③ データに対する外部からの不正なアクセスに対する防御に必要な機能

④ データを連係させるシステムに対する不正なアクセス等を検知する体制

⑤ 不正なアクセス等により被害が生じた場合の対処方針

⑥ データの提供を受ける法人又は個人における安全確保対策

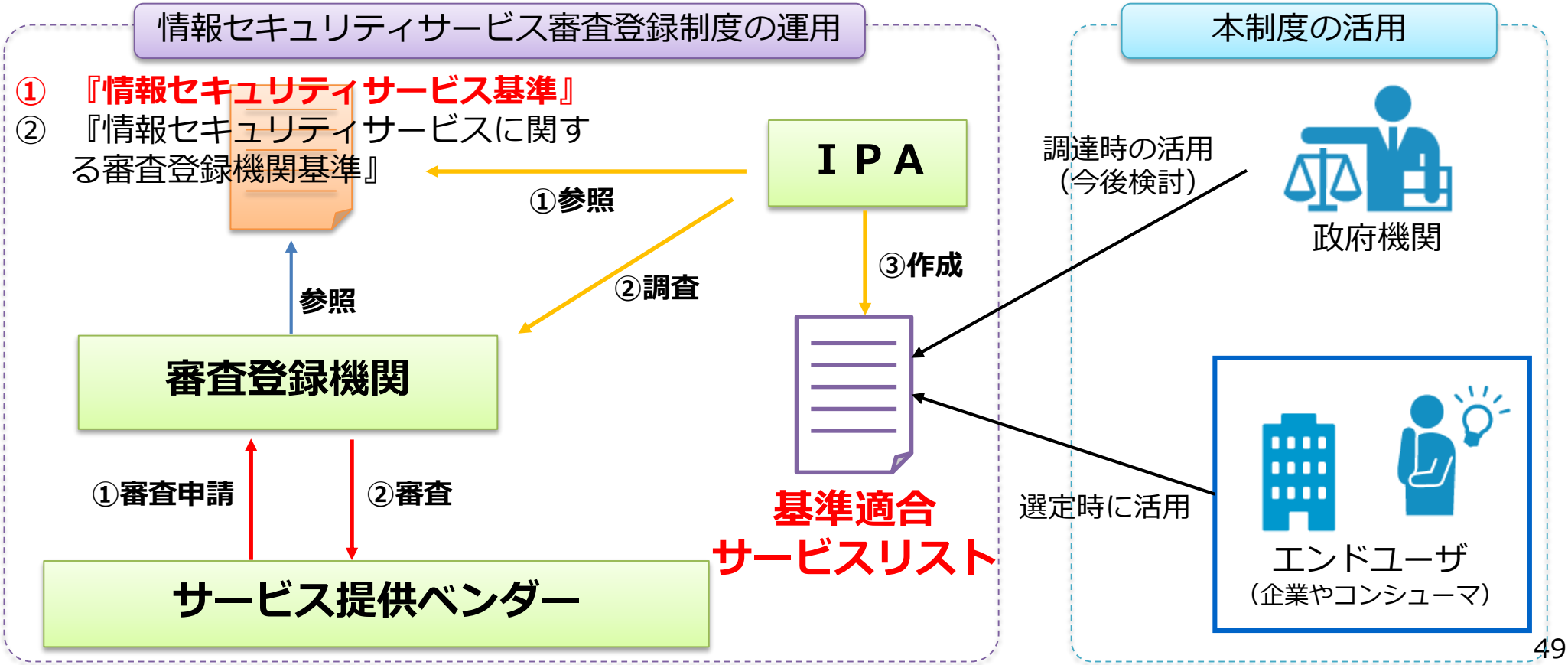
⑦ データを連携させるシステムについての定期的な脆弱性確認の方法

(*)但し、署名を行うにあたって事業者と何らかの契約を行っている場合、当該契約に定められた範囲で責任を負うことはあり得る。

情報セキュリティサービス審査登録制度

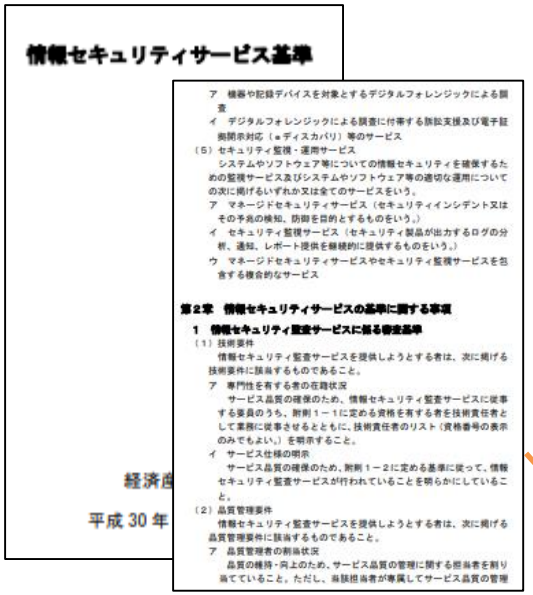
情報セキュリティサービス審査登録制度の概要

- **セキュリティサービスが最低限の品質を維持するために満たすべき『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基準に関する審査登録機関基準』を公表（平成30年2月）。
- 台帳を利用することで、**中小企業は一定の品質維持向上が図られているサービスを使うことが可能になる**。



情報セキュリティサービス基準等の策定

- IPAから情報セキュリティサービス基準に適合するサービスのリストを公開（平成30年7月）。



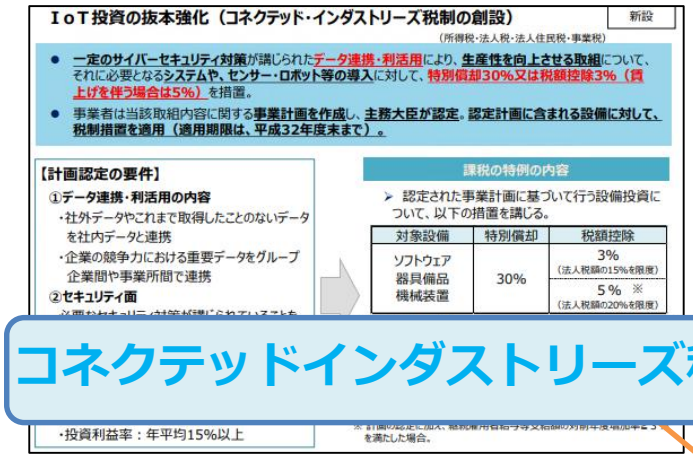
情報セキュリティサービス基準

以下の4サービスに関する基準を定める
- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタルフォレンジックサービス
- セキュリティ監視・運用サービス

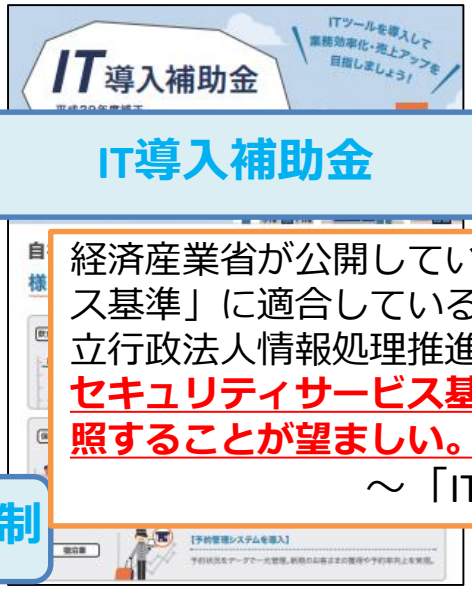
47サービスが掲載（7/5時点）
- 情報セキュリティ監査（12サービス）
- 脆弱性診断（14サービス）
- デジタルフォレンジック（10サービス）
- セキュリティ監視・運用（11サービス）

基準を満たした情報セキュリティサービスの利用促進

- 情報セキュリティサービスの利用を促進するため、政府調達や、税制・補助金における「情報セキュリティサービス基準適合サービスリスト」の推奨を実施。



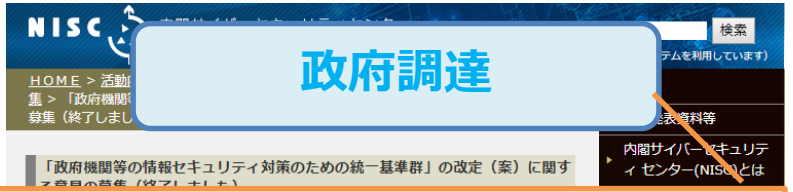
コネクテッドインダストリーズ税制



IT導入補助金

経済産業省が公開している「情報セキュリティサービス基準」に適合しているサービスのリストとして、独立行政法人情報処理推進機構（IPA）が公表する**「情報セキュリティサービス基準適合サービスリスト」を参照することが望ましい。**

～「ITツール登録要領」より抜粋



政府調達

セキュリティ監視・運用サービスを利用する場合、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を記載した**「情報セキュリティサービス基準適合サービスリスト」に記載があるサービスを利用している**。

～「認定申請書記入方法」より抜粋

※情報セキュリティ監査、脆弱性診断についても同様に記載。

経済 産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた 企業を記載した**「情報セキュリティサービス基準適合サービスリスト」（うちセキュリ ティ監査サービスに係る部分）を活用**するほか、（中略）～参照することも考えられる。

～「政府機関等の対策基準策定のためのガイドライン」より抜粋