経済産業省

資料３

IoT機器に求められるセキュリティについて

経済産業省

商務情報政策局

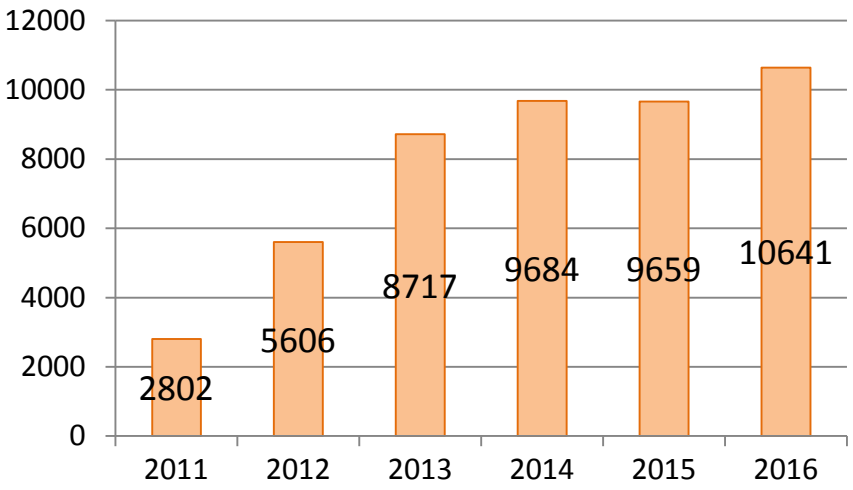
サイバーセキュリティ課

サイバー攻撃の脅威

- IT利活用の拡大に伴い、サイバー攻撃の脅威も増大。
- JPCERT/CCのインシデント調整件数は、2011年と比較し、4倍近くまで増加。
- （独）情報処理推進機構（IPA）が毎年公表する「情報セキュリティ10大脅威」の順位も大きく変化。

JPCERT/CC（※）のインシデント調整件数

JPCERT/CC（ｼﾞｪｲﾋﾟｰｻｰﾄｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ）は、海外機関との国際連携によりインシデント対応等を実施する一般社団法人



順位	組織における10大脅威	昨年順位
１位	標的型攻撃による情報流出	１位
２位	ランサムウェアによる被害	７位
３位	ウェブサービスからの個人情報の窃取	３位
４位	サービス妨害攻撃によるサービス停止	４位
５位	内部不正による情報漏えいとそれに伴う業務停止	２位
６位	ウェブサイトの改ざん	５位
７位	ウェブサービスへの不正ログイン	９位
８位	IoT機器の脆弱性の顕在化	圏外
９位	攻撃のビジネス化（アンダーグラウンドサービス）	圏外
１０位	インターネットバンキングやクレジットカード情報の不正利用	８位

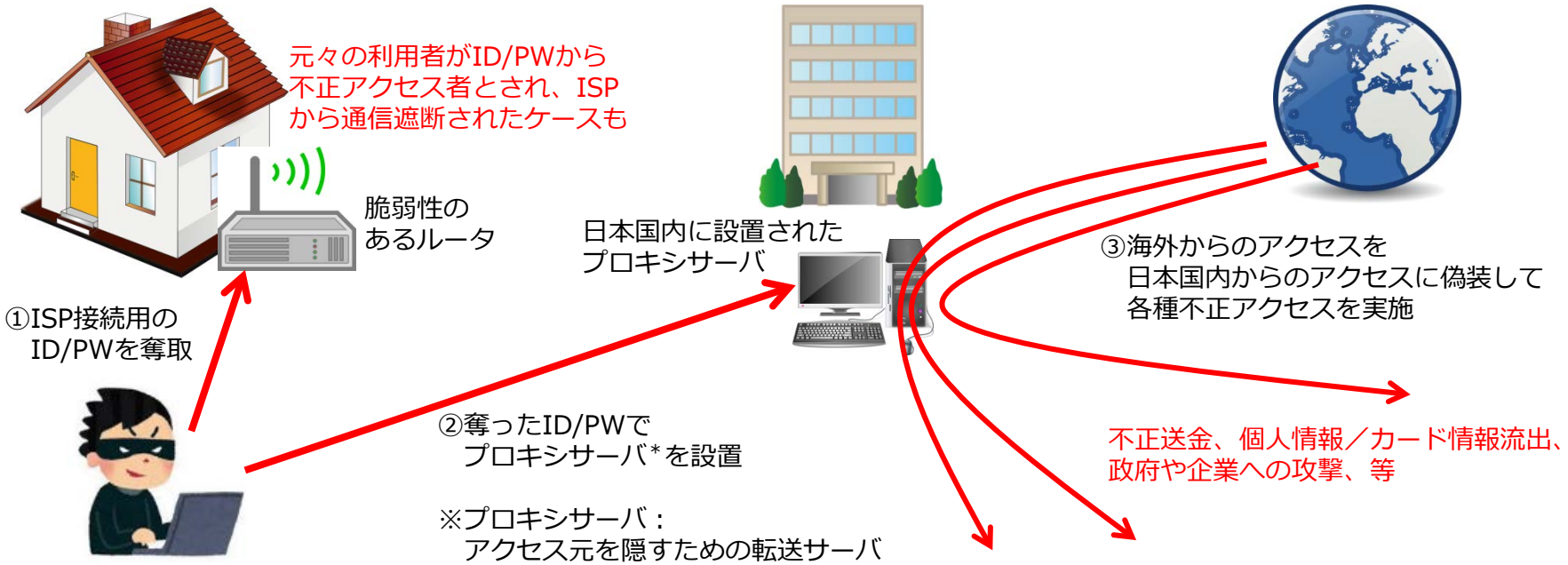
（出典）IPAウェブサイトより経済産業省作成

IoT機器の急増に伴い、サイバー攻撃の起点が急激に拡散

- 英調査会社によれば、**ネットに繋がる機器は2020年には300億個まで増加**。（現在の1.7倍）
- **IoT機器が乗っ取られる懸念など、ネットワーク全体のセキュリティリスクも上昇**。

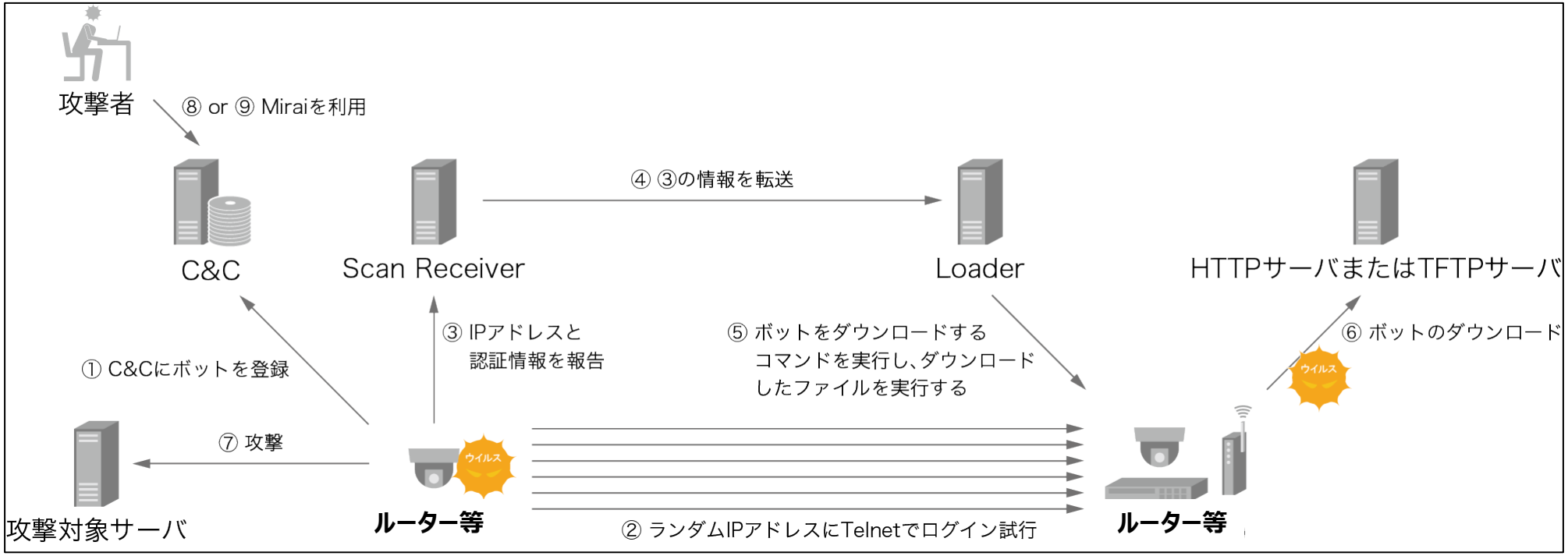
（参考）ブロードバンドルータの脆弱性を使ったケース

- 一般向けブロードバンドルータに脆弱性があり、ISP接続用のID/PWが奪取される危険性があることが判明、2012年5月に対策用のアップデートを公開。
- しかしながら、アップデートをしない個人ユーザが多く、メーカや警視庁等による複数回の注意喚起にも関わらず、数年にわたって乗っ取り被害が発生。



（参考）Miraiのケース①

- 2016年、23/tcp（telnet）2323/tcp で接続し、「ユーザ名とパスワード」がデフォルトだったり、固定された設定のルータやウェブカメラがマルウェア「Mirai」に感染しているケースが発覚。
- 「Mirai」に感染した機器から、同様に感染可能なルータ等の探索活動が行われたことから感染が拡大。感染したルータ等は、C＆Cサーバからの攻撃命令によって攻撃対象にDDoS攻撃を実施。



図： Mirai Botnetのシステム構成（出典：Internet Infrastructure Review「IIR]）

（参考）Miraiのケース②（ドイツテレコム）

- 2016年11月、ドイツで90万人以上が被害を受けた事例が発生。
- 大規模なサイバー攻撃用ボットネットの構築を狙ったMirai亜種の感染活動により、アクセスを受けた一部のルータがダウン。
- この事例を受け、現在、ドイツにおいて、テクニカルガイドラインを作成中。

【ドイツにおけるルータ向けテクニカルガイドラインの検討状況】

- ドイツテレコムの事案を受け、小規模オフィスや家庭用のルータのテクニカルガイドラインの作成に着手。
- パスワード設定機能（8字以上、大小文字の組み合わせを要求）、ファームウェアのアップデート機能、ファイアウォール機能が盛り込まれる見込み。
- 任意のガイドラインであって、強制認証ではない。産業界と連携し、年内に取りまとめる予定。

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。**

金銭要求メッセージで画面ロック

社内へ感染拡大

悪意のあるコード

工場の制御PCがロックされ製造停止という事態も

インターネットから侵入

海外工場のPCが乗っ取られWAN経由で侵入

インターネットやWANから侵入

社外へも感染拡大

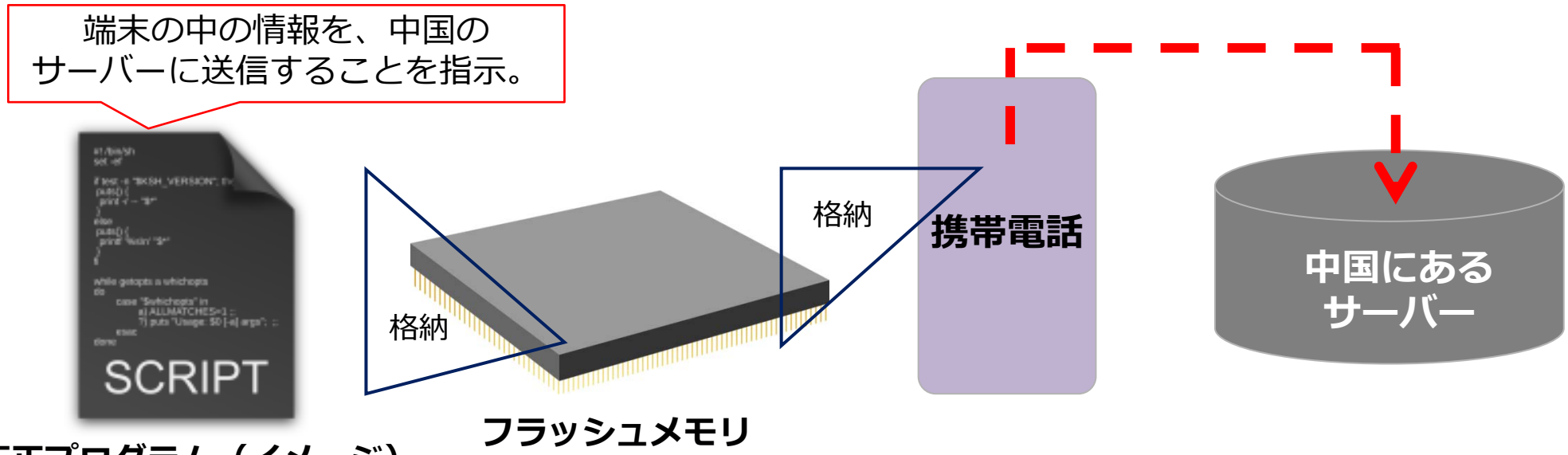
一旦社内に侵入、感染すると、Windowsの脆弱性を突いて、社内外に級数的に感染を拡大

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困難。

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

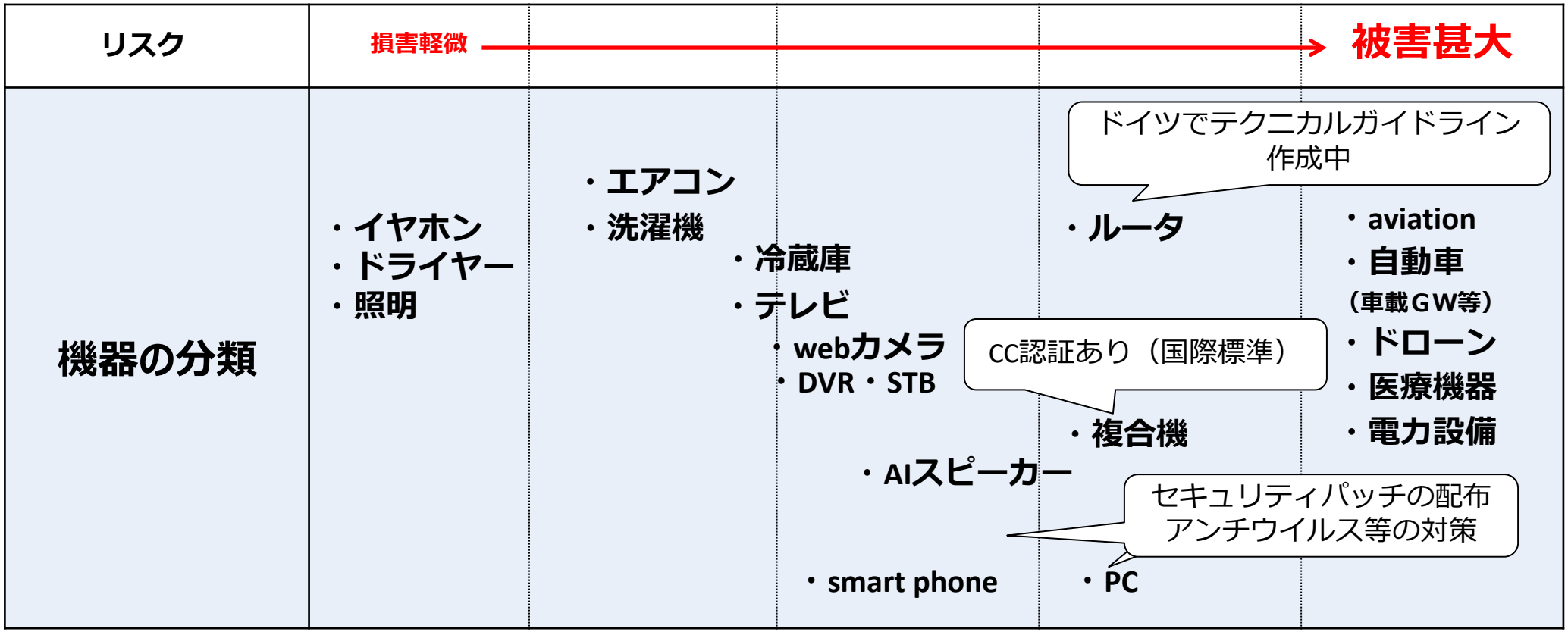
- 2016年、米国セキュリティ会社が携帯電話のフラッシュメモリのファームウェアに仕込まれている不正プログラムを発見。
- 中国企業が開発・製造したもので、ユーザーの同意なしに、72時間おきに携帯電話内の情報が中国のサーバーに送信される。



不正プログラム（イメージ）　フラッシュメモリ

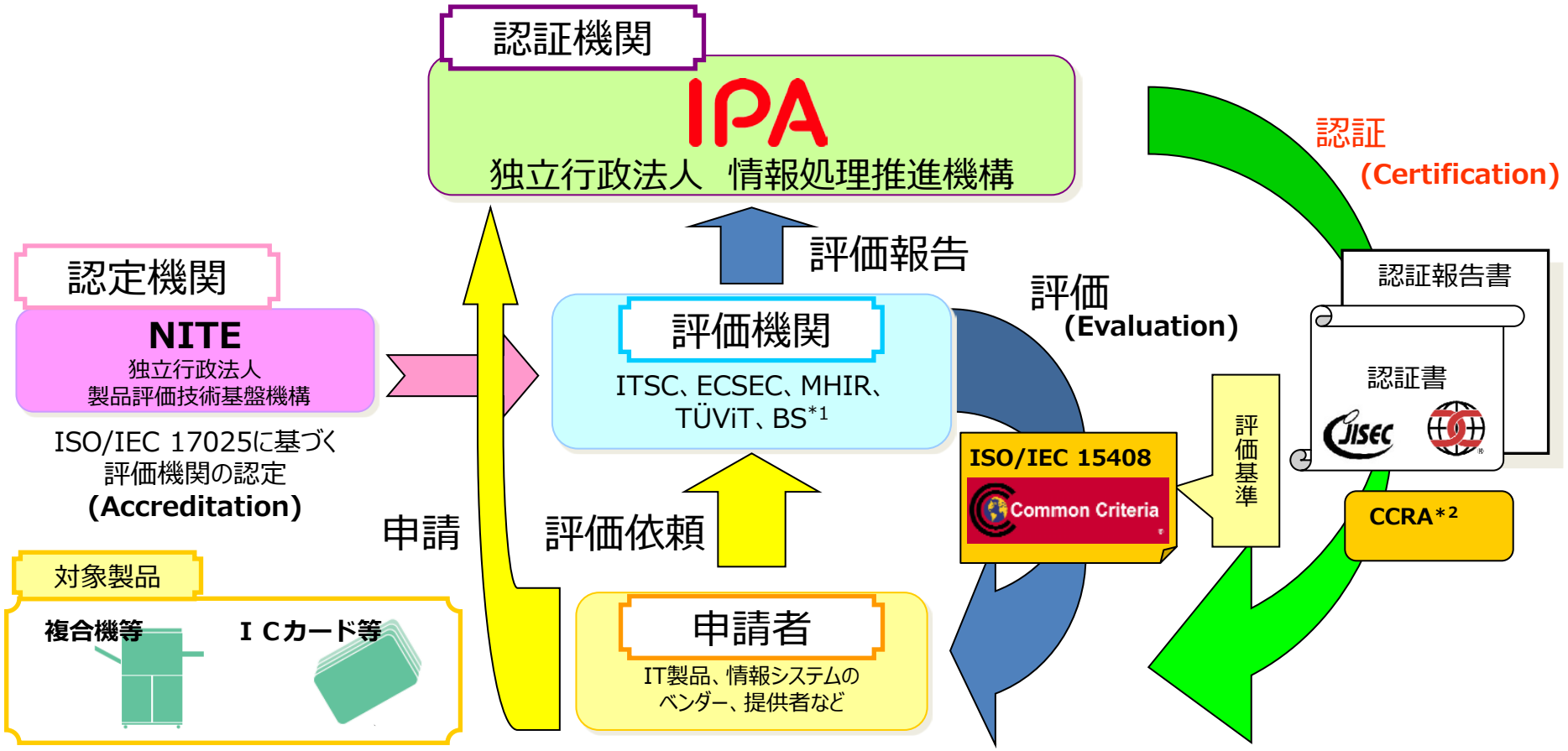
IoT機器とリスク

- 一口に『**IoT機器**』**と言っても、多様な種類が存在**。
- 各機器の用途、利用方法、コンピューティングパワー等が大きく異なるため、**サイバー攻撃を受けた場合のリスクの大きさもそれぞれ異なる**。



ITセキュリティ評価及び認証制度（JISEC）

- ネットワークにつながる機器のセキュリティに関する国際標準に基づく認証制度も存在しており、複合機等は既に対象になっている。



*1　ITSC：一般社団法人ITセキュリティセンター、ECSEC：株式会社ECSEC Laboratory、MHIR：みずほ情報総研株式会社
TÜViT：TÜV Informationstechnik GmbH、BS：Brightsight bv

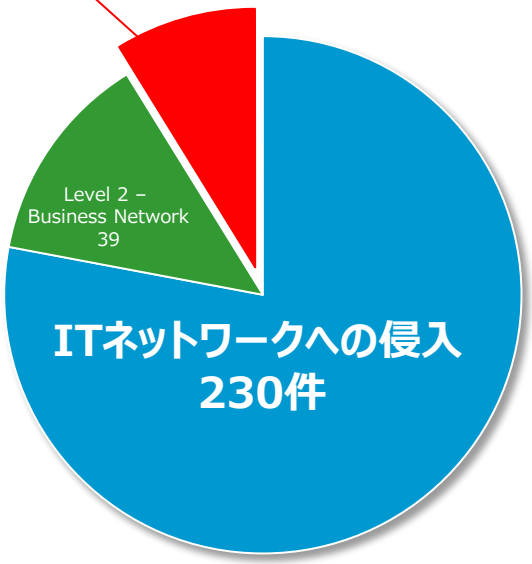
*2　Common Criteria Recognition Arrangement：国際相互承認協定

サイバー攻撃のレベルが上がり、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**。

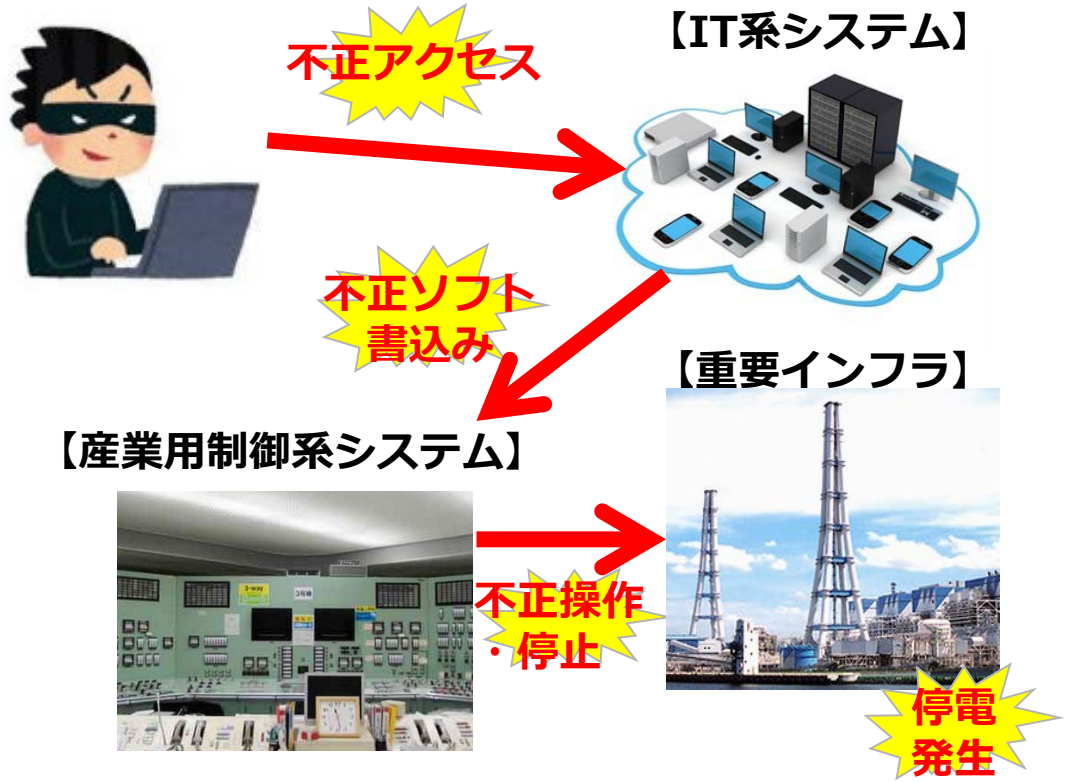
米国の重要インフラへのサイバー攻撃の深さ

攻撃のうち約一割は、制御系までサイバー攻撃が到達



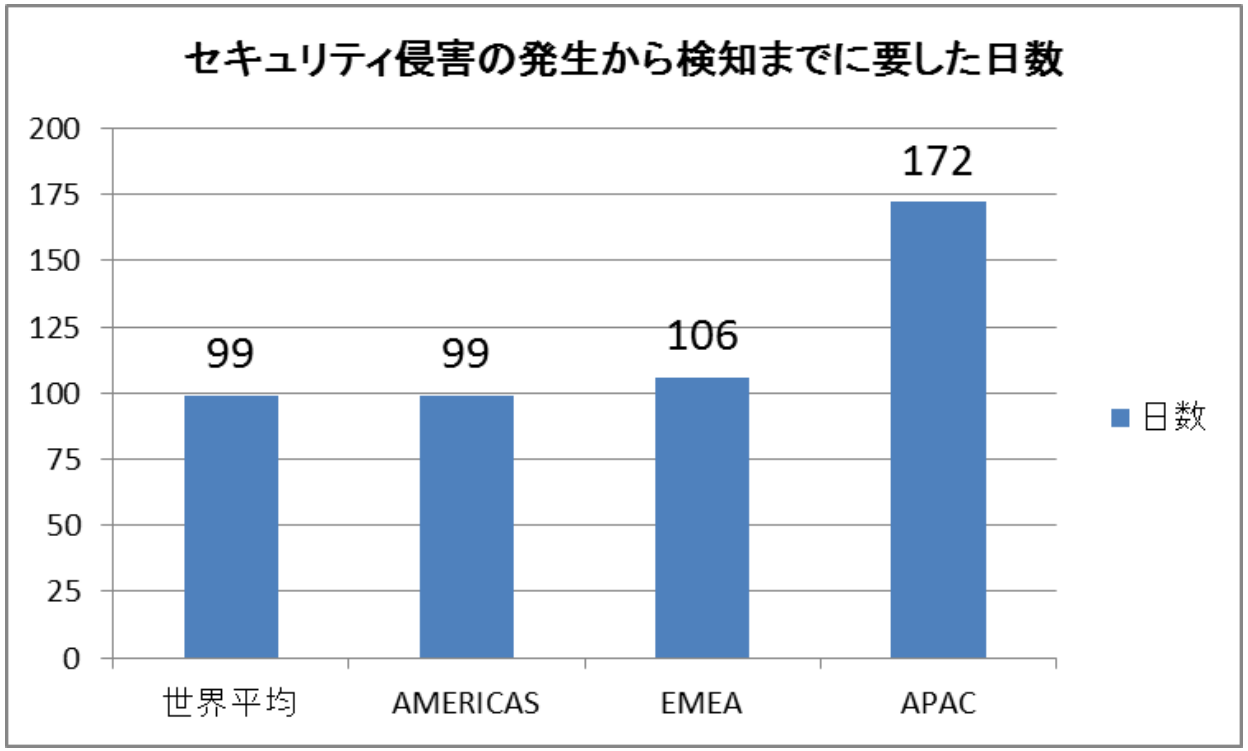
（出典）NCCIC/ICS-CERT Year in Review FY2015 Homeland Security より経済産業省作成

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



（参考）サイバー攻撃を検知するまでに要している日数

- サイバー攻撃を受けてから、その事実を検知するまでに平均99日かかっている。
- 検知までに1年以上かかっているケースもあり、その間攻撃者は自由に探索活動や情報窃取を行っている。



（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

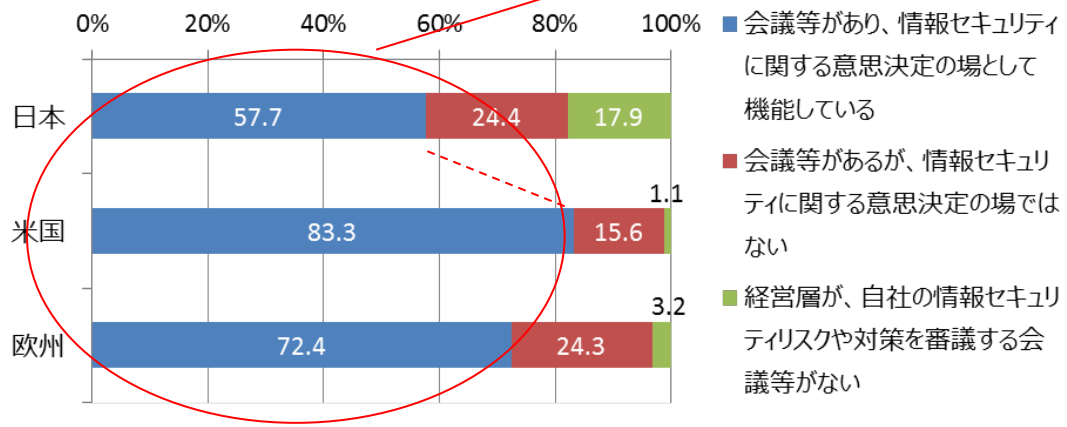
サイバーセキュリティに関する経営の意識、体制の整備も十分ではない。

民間セクターのセキュリティ責任体制（日米欧）

- 日本では、経営のサイバーセキュリティへの関わりが弱い。

情報セキュリティの意思決定に経営層が関わるのは米国の2/3

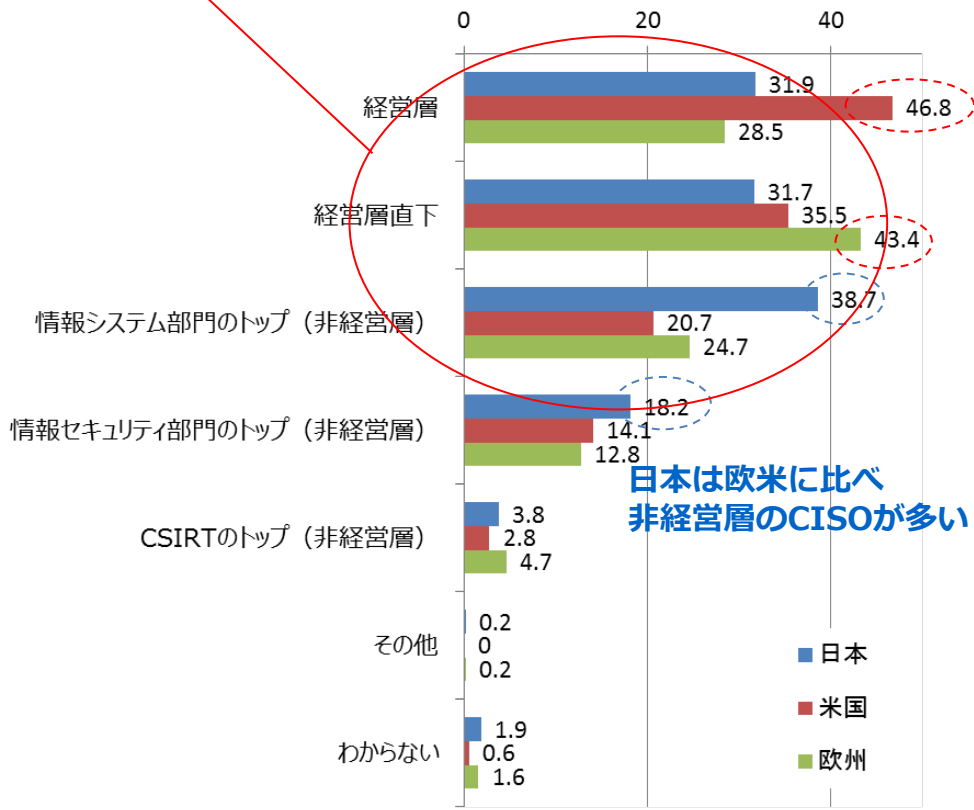
経営層の情報セキュリティに対する関与



欧米は経営層に紐づくCISO※が多い

※Chief Information Security Officer（シーアイエスオー、シーソ）

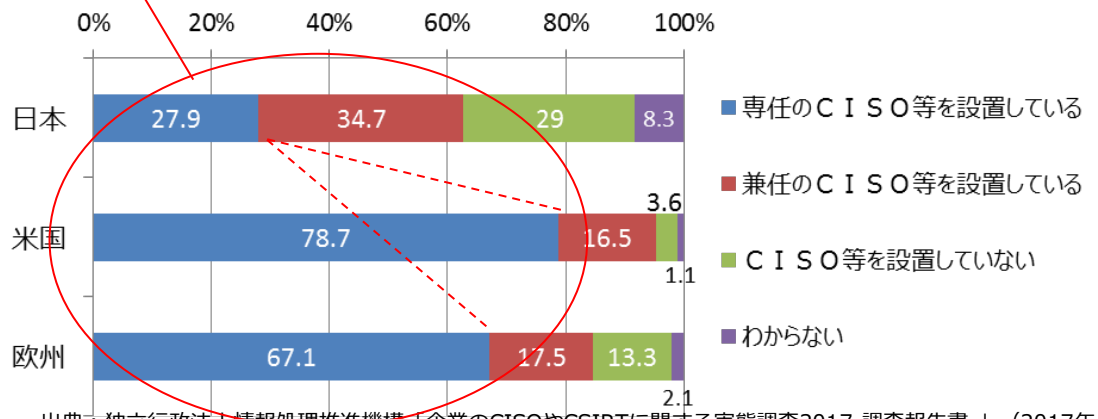
CISO等の組織内の位置づけ



日本は欧米に比べ
非経営層のCISOが多い

日本の専任CISOは欧米の半分以下

CISO等設置状況



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）

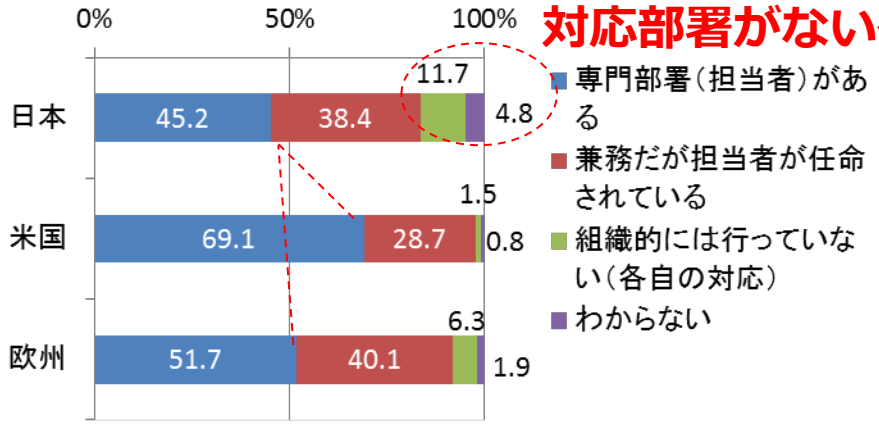
＊ 日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10～11月）

＊ 回収は日本755件、米国527件、欧州526件

民間セクターのセキュリティ対応体制（日米欧）

- 情報セキュリティの対応体制も日本は欧米に比べて脆弱。

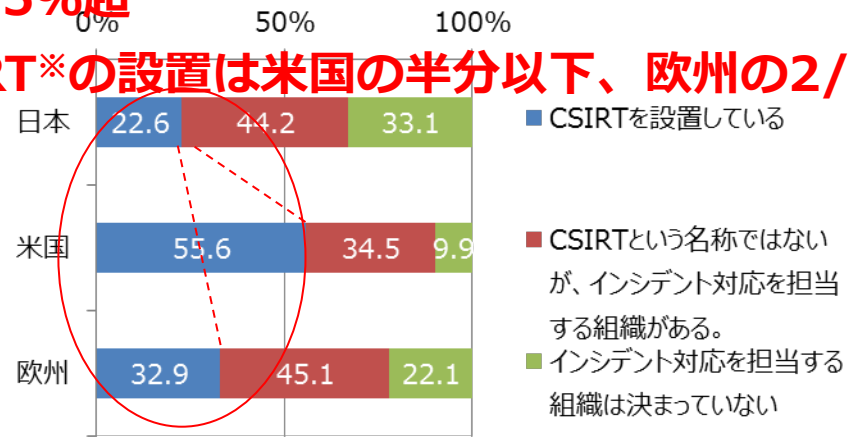
情報セキュリティ対策の体制



対応部署がないケースも15%超

日本は専門部署の設置が少ない

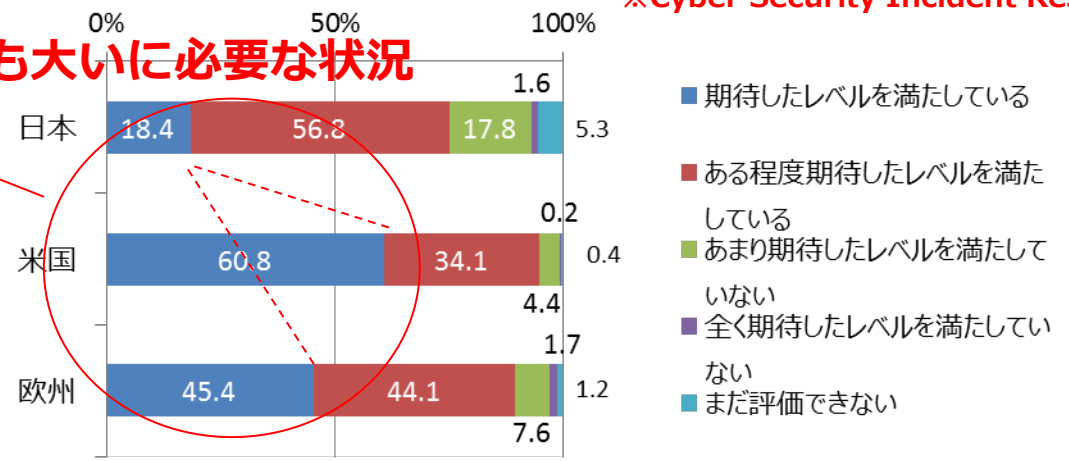
CSIRT等設置状況



CSIRT※の設置は米国の半分以下、欧州の2/3

※Cyber Security Incident Response Team（シーサート）

全体評価



CSIRTのレベル面の改善も大いに必要な状況

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

サイバーセキュリティに関してサプライチェーン全体で対応する国際的な動きが強まっている。

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。**
- 国内でも、**Connected Industriesの進展、ボットネット対策から、製品・サービスに対する、より一層のサイバーセキュリティ対策の推進が求められる。**

【米国】

- **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、『サイバーサプライチェーンリスクマネジメント』を明記へ**
- **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】

- **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を検討**
- 既に、**エネルギー等の重要インフラ事業者は、セキュリティ対策が義務化（NIS Directive）**

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、国内サプライチェーンからはじき出されるおそれ

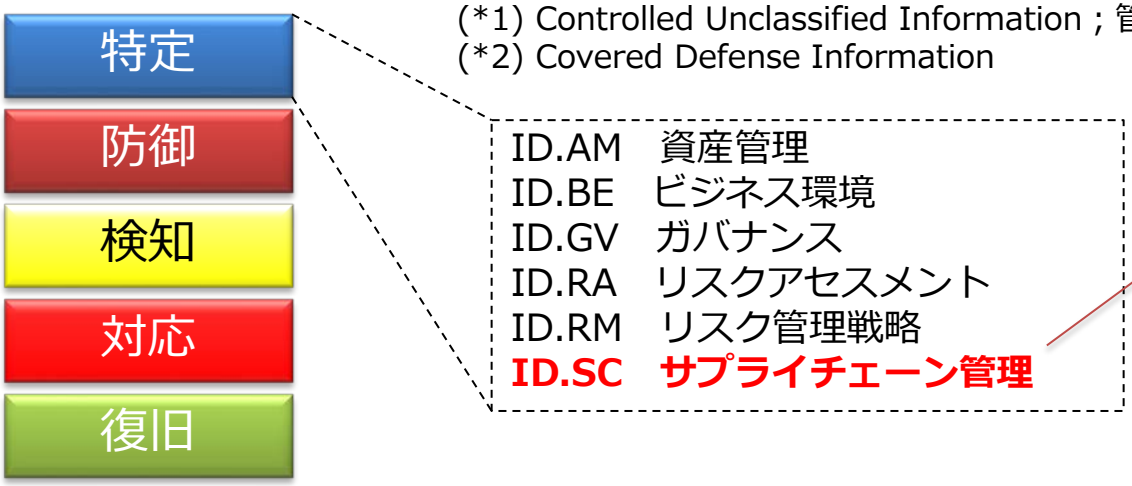
【国内】Connected Industriesの推進、ボットネット対策

- 「つながる」ことを前提とするコネクテッドインダストリーにおいて、サイバーセキュリティの確保は必要条件
- 2020年東京オリパラに向けて、ボットネット撲滅の推進を決定

米国の動き

- **サイバーセキュリティの視野は、『特定機能の防御（重要インフラ中心）』から『サプライチェーン管理』へ拡大。**

2010.11	米国大統領令(E.O.13556)発出	米国政府全体として、CUI(*1)のセキュリティ強化の取組を開始
2014.02	**Cybersecurity Framework vesion1.0公表**	サイバーセキュリティ対策の全体像を示し、「特定」、「防御」、「検知」、「対応」、「復旧」に分類して対策を記載
2015.06	**NIST SP800-171策定**	非政府機関の情報システム等におけるCUIの保護を目的としたサイバーセキュリティ対策の要件を規定
2016.10	**DFARS Clause252.204-7012 発行**	CDI(*2)を保護対象とし、米国防衛省と契約する者に対し、2017年12月31日までにSP800-171相当のサイバーセキュリティの対応を要求。
2017.01	**Cybersecurity Framework version1.1 draft公表**	サプライチェーンのリスク管理やサイバーセキュリティの評価方法などを追記



Cybersecurity Frameworkにおける5つの分類

DFARS Clause 252.204-7012において要求されていること

- **米国の防衛装備品調達では、本年末からSP800-171※に対応することが求められる。**

※ 非政府機関の情報システム等におけるCUIの保護を目的とした
サイバーセキュリティ対策の要件を規定したもの

（1）主なセキュリティ要求事項

- **NIST SP800-171※のセキュリティ要求事項を満たすこと。**
- **外部サービスとプロバイダ**を利用して保護対象防衛情報を保存・処理・送信する場合には、米国のクラウドの基準Fed RAMP（NIST SP800-53を満たした事業者が提供するクラウドサービス）の要求事項と**同等の基準**を満たし、そのサービスプロバイダが、サイバー事案報告等の要求事項を満たしていること。

（2）サイバー事案報告の要求

- 契約業者が、保護対象防衛情報に影響を及ぼす等のサイバー事案を発見した場合には、国防省にサイバー事案を**速やかに報告**し、調査等を受け入れること。

（3）下請け契約の扱い

- 契約業者が、**下請け業者と共有する情報が保護対象防衛情報である場合には、下請け業者にもDFARS Clause 252.204-7012に基づく保護を要求**する。

欧州の動き

- 欧州では、**重要インフラは最新のサイバーセキュリティ対応を実装することが求められ**（NIS Directive）、**ネットワークに接続する機器のセキュリティに関して認証・確認のための自主的フレームワーク（Cybersecurity Certification Framework）を整備**することを掲げている

【欧州】

- **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を検討**。

  ⇒方向性：規制ではなく、自主的な仕組み　産業界：国際標準に基づく自己適合宣言を主張している。

- 2016年、ＥＵ各国の重要インフラ事業者（エネルギー、交通、銀行、金融等）に対して、**セキュリティ対策を義務化。その際セキュリティ関連国際標準を考慮することを指示（NIS 指令）**。
- EUの顧客データを扱う企業に対して、データ処理制限、流出などの際の通知義務などをEU域外においても義務化。（EU一般データ保護規則：GDPR）

【ドイツ】

- ＮＩＳ指令に先立ち、2015年にＩＴセキュリティ法を制定し、重要インフラ事業者（エネルギー、交通、ICTs、交通、金融・保険、健康、水、食糧）に対して以下を要求。

  ①サイバーセキュリティに係る**最低限の基準を満たしていることについて情報セキュリティ庁の証明を得ること**
  ②**２年ごとにセキュリティ監査等を受けること**
  ③**サイバー攻撃と思われる事象が発生した場合に情報セキュリティ庁へ報告すること**

- 現在、small office and homes のルーターのテクニカルガイドラインを作成中（任意制度）。

政策の方向の整理

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

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

経済産業省におけるサイバーセキュリティの主な取組

政府機関を守る取組

IPA（独立行政法人情報処理推進機構）が独法等の監査、監視を実施。

【平成28年4月、サイバーセキュリティ基本法と情報処理促進法を改正】

Industry by Industry の取組

サイバーセキュリティに対応した産業活動基盤の構築：産業分野別にセキュリティポリシー（基準・規格）を設定、国際標準化。

企業を守る取組

サイバーセキュリティ経営ガイドラインの策定：
経営者のリーダーシップにより、サイバーセキュリティ対策等をとりまとめ。

中小企業の情報セキュリティ対策ガイドラインの策定：
「サイバーセキュリティ経営ガイドライン」を中小企業向けに編集。

IoTセキュリティガイドラインの策定：
IoT機器等のサイバーセキュリティ対策をまとめたもの。

重要インフラを守る取組

重要インフラ事業者のリスク評価事業：
2020年東京オリンピック・パラリンピック等も踏まえ、電気・ガス・水道等の重要インフラのリスク評価を実施。

情報共有・初動対応支援体制の強化：
IPA、JPCERT/CC※による情報共有体制の構築・緊急時の初動対応支援等の実施。

基盤整備のための取組

人材育成：若年層の優秀なセキュリティ人材の早期発掘（**未踏IT人材発掘・育成事業等**）。
情報処理安全確保支援士の資格創設。【平成28年4月、情報処理促進法を改正】
産業サイバーセキュリティセンターを設置し、セキュリティ対策の中核人材を育成。

国際連携：サイバー攻撃は国境をまたぐ問題であり、米欧イスラエル等との国際連携を推進。

※JPCERT/CC（ｼﾞｪｲﾋﾟｰｻｰﾄｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ）は、海外機関との国際　連携によりインシデント対応等を実施する一般社団法人。

（参考）IoTセキュリティガイドライン

（IoTセキュリティWGにおいて策定：
総務省・経済産業省共同事務局）

- 本ガイドラインは、IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの（平成28年7月5日公開）。
- 各指針等においては、具体的な対策を要点としてまとめている。

	指針	主な要点
方針	**IoTの性質を考慮した基本方針を定める**	• 経営者がIoTセキュリティにコミットする • 内部不正やミスに備える
分析	**IoTのリスクを認識する**	• 守るべきものを特定する • つながることによるリスクを想定する
設計	**守るべきものを守る設計を考える**	• つながる相手に迷惑をかけない設計をする • 不特定の相手とつなげられても安全安心を確保できる設計をする • 安全安心を実現する設計の評価・検証を行う
構築・接続	**ネットワーク上での対策を考える**	• 機能及び用途に応じて適切にネットワーク接続する • 初期設定に留意する • 認証機能を導入する
運用・保守	**安全安心な状態を維持し、情報発信・共有を行う**	• 出荷・リリース後も安全安心な状態を維持する • 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える • IoTシステム・サービスにおける関係者の役割を認識する • 脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		• 問合せ窓口やサポートがない機器やサービスの購入・利用を控える • 初期設定に気をつける • 使用しなくなった機器については電源を切る • 機器を手放す時はデータを消す