経済産業省

参考資料

経済産業省

商務情報政策局

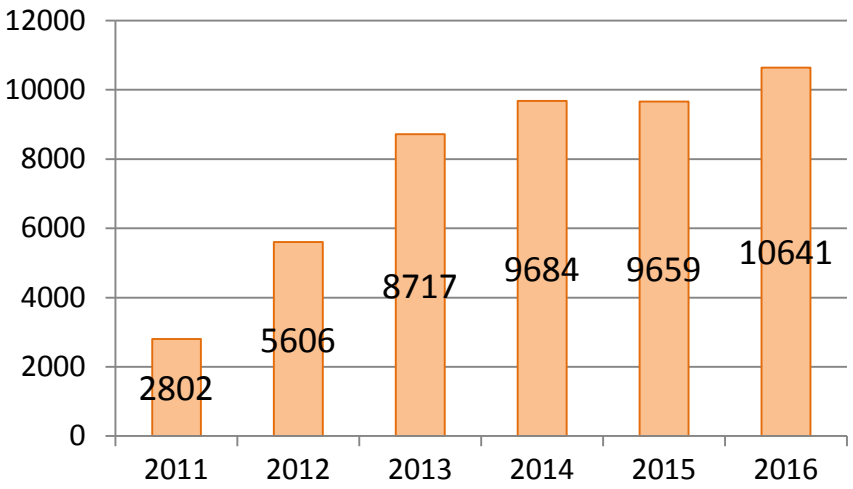
サイバー攻撃の拡大と深刻化

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

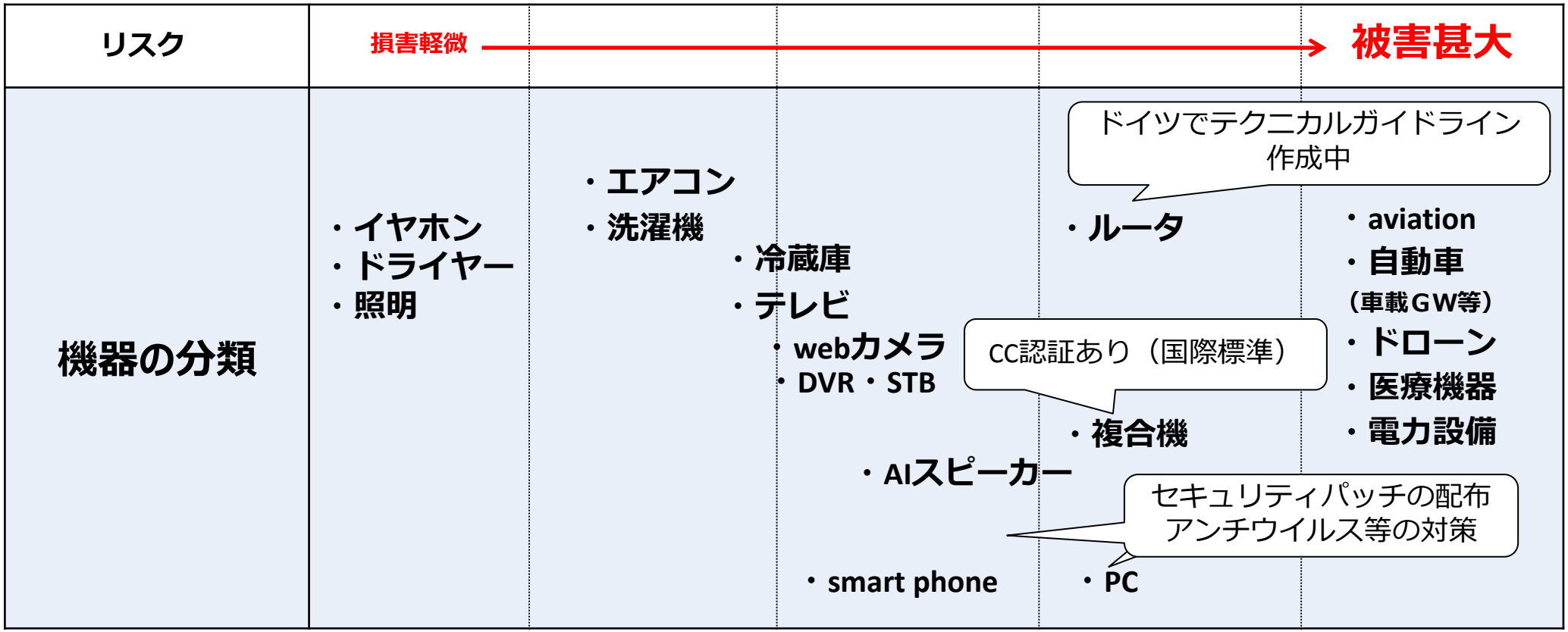


順位	組織における10大脅威	昨年順位
１位	標的型攻撃による情報流出	１位
２位	ランサムウェアによる被害	７位
３位	ウェブサービスからの個人情報の窃取	３位
４位	サービス妨害攻撃によるサービス停止	４位
５位	内部不正による情報漏えいとそれに伴う業務停止	２位
６位	ウェブサイトの改ざん	５位
７位	ウェブサービスへの不正ログイン	９位
８位	IoT機器の脆弱性の顕在化	圏外
９位	攻撃のビジネス化（アンダーグラウンドサービス）	圏外
１０位	インターネットバンキングやクレジットカード情報の不正利用	８位

（出典）IPAウェブサイトより経済産業省作成

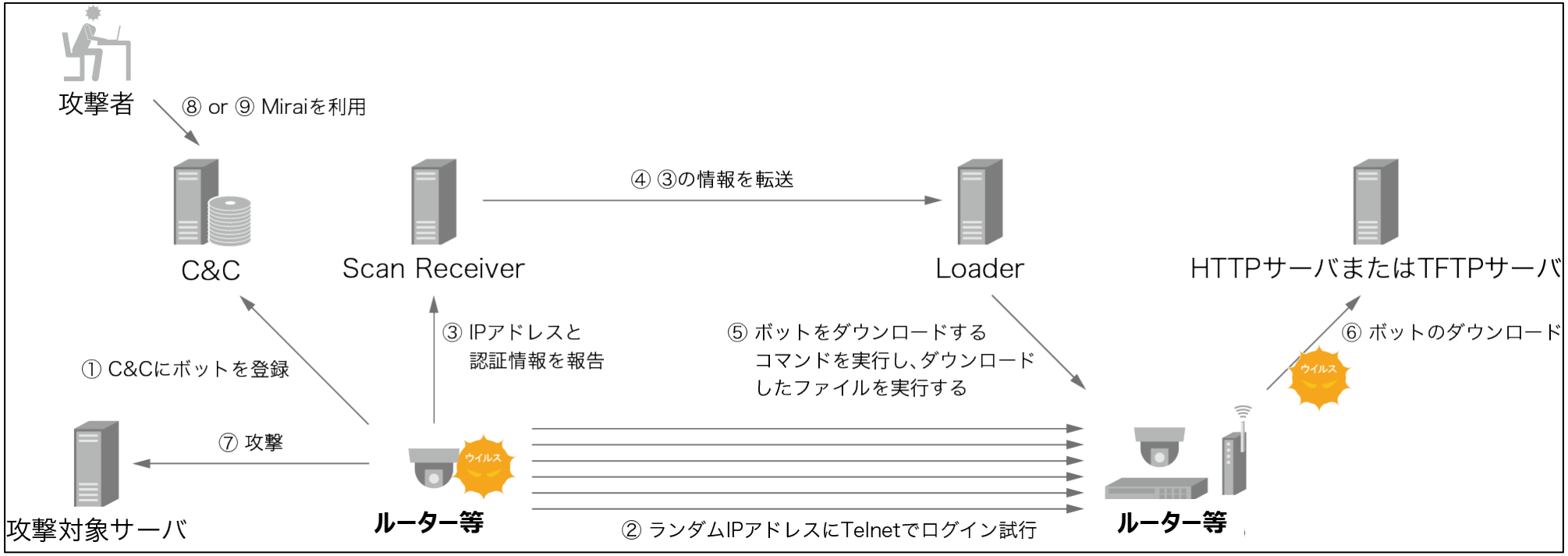
IoT機器とリスク

- 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**。



（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サーバからの命令によって攻撃対象にDDoS攻撃を実施。**



Mirai Botnetのシステム構成（出典：Internet Infrastructure Review「IIR])より経済産業省にて一部修正

（参考）Miraiのケース②（ドイツテレコム）

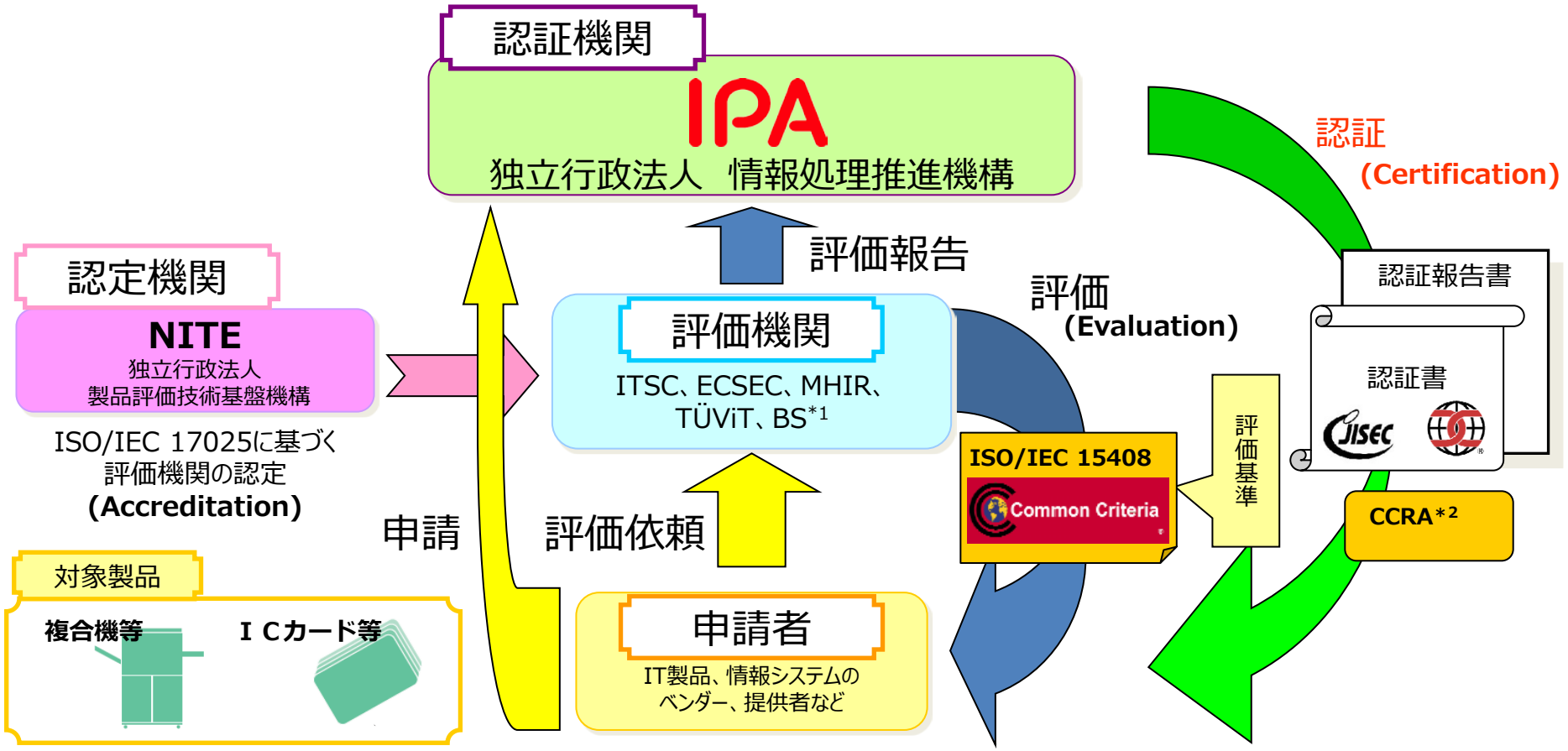
- 2016年11月、**ドイツで90万人以上が被害を受けた事例**が発生。
- 大規模なサイバー攻撃用ボットネットの構築を狙ったMirai亜種の感染活動により、**アクセスを受けた一部のルータがダウン**。
- この事例を受け、**現在、ドイツにおいて、テクニカルガイドラインを作成中**。

【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。

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**。
- 複合機等は既に対象。



*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

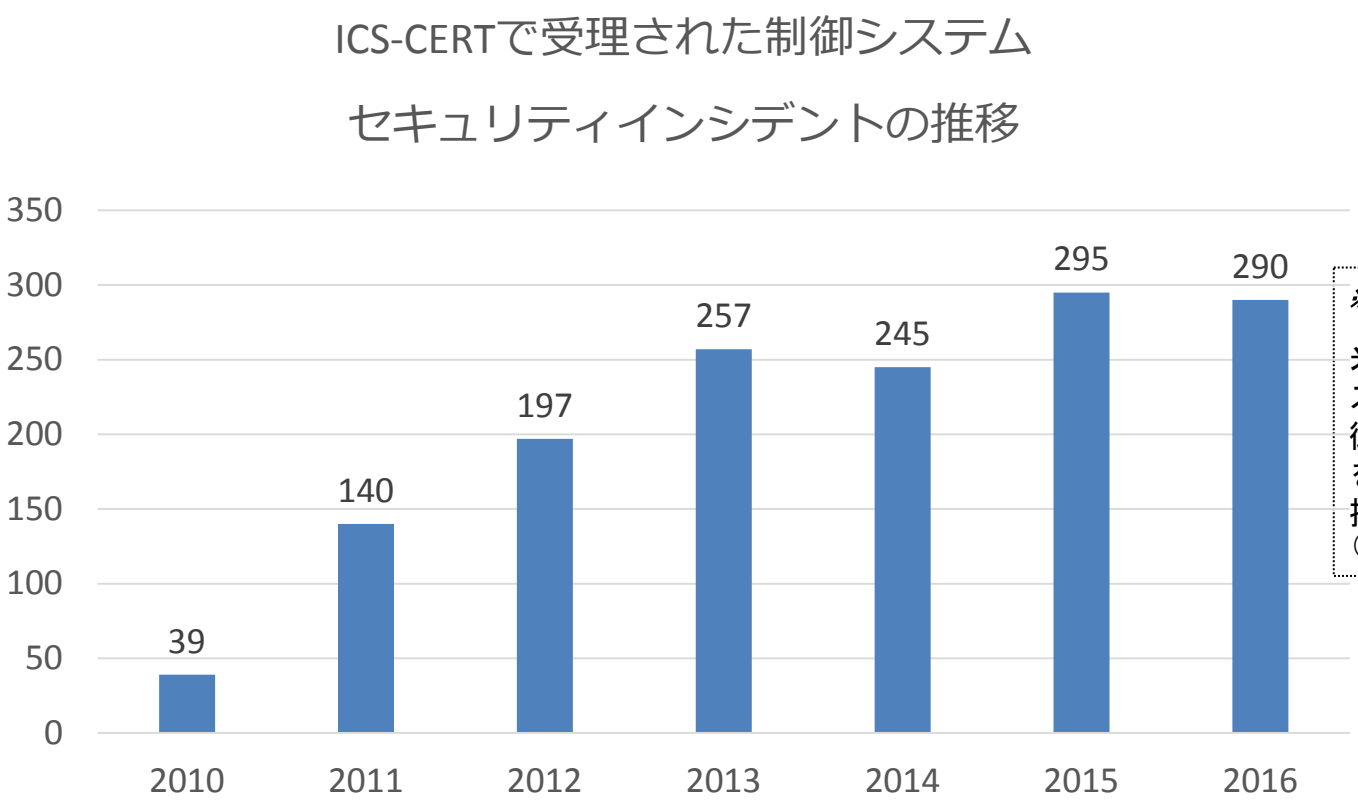
*2　Common Criteria Recognition Arrangement：国際相互承認協定

制御システムのセキュリティインシデントの動向

- **<u>制御システムにおけるインシデントは世界的に増加傾向</u>**。
- 2010年度にStuxnetによって制御システムへの攻撃が顕在化。

2015年度：1位　工場(97)、2位　電力(46)、3位　水道(25)、4位　化学(4)

2016年度：1位　工場(63)、2位　通信(62)、3位　電力(59)、4位　水道(18)



出典：ICS-CERT, “ICS-CERT Year in Review FY2015_Final“ に基づき作成

※ICS-CERTとは

米国国土安全保障省（DHS）が運営する制御システムに特化したインシデント対応機関。制御システムに関する国内のインシデント報告を受け、専門家による分析・対応サービスを提供する。
(http://www.us-cert.gov/control_systems/ics-cert/)

サイバー攻撃の脅威レベルの高度化　－ウクライナにおける2度の停電の教訓－

- ウクライナでは、 2015年12月と2016年12月に、サイバー攻撃による停電が発生。
- **2回のサイバー攻撃の手法には、大きな違い**が存在。
- **2015年12月の攻撃（Black Energy・KillDisk）**では、サイバー攻撃だけでは、電力を直接コントロールするには至っていない。

※インターネットと繋がっているＩＴ系から産業用制御系への通信を停止させただけであり、停電の原因は、手動で停電をさせた内通者がいたのではないかといわれている。

- **2016年12月の攻撃（CrashOverRide（Industroyer））**では、IT系から侵入して、産業用制御系システムに産業用通信プロトコルが標的としたソフトウェアを埋め込み、制御系が外部から操作された。つまり**サイバー攻撃のみで、停電が起こされた**。

※攻撃手法には汎用性があり、他のシステムへも適用が可能であると言われる。

- CrashOverRideは産業用制御システムに関する深い知識と理解に基づいて開発されたと見られ、電力システム向けに作られたマルウェアだが、**〝モジュールを加えることで、他分野の重要インフラに被害をもたらす可能性〟**があるという分析もある。

ビル分野のセキュリティ事故事例

- 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）


W.B. Carrell Memorial Clinic

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）、患者情報の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（次頁参照）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（後述の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り公開している。
ー	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どおりに機能せず、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 (http://www.justice.gov/usao/txn/PressRel09/mcgraw_cyber_compl_arrest_pr.html)

ビル･工場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**。

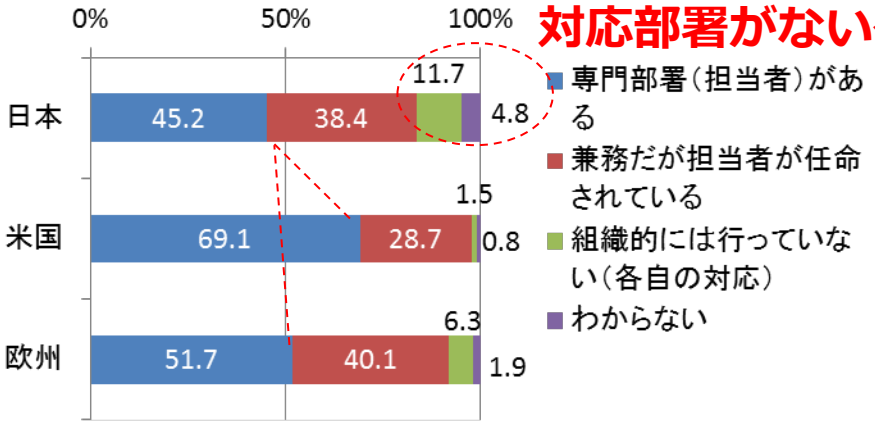
時期	内容
2011年11月	コロンビア大の研究者が**オフィス等**に導入されているHPのLaserJet**プリンターに脆弱性**があり、ハッカーからのアップデート指示により過剰な運転状態となって、**最終的には発火することを証明**した。対象は何百万台にもおよぶ。
2012年4月	MITの学生が同大学グリーン棟の**照明システムをハッキング**し、**ビルの窓照明を巨大なテトリスゲーム**にしてしまった。
2013年8月	フロリダ州マイアミのターナー・ギルフォード・ナイト**矯正センターの警備システムが何者かにハックされ**、収容房の**扉のロックをリモート解除**し、受刑者が**敵対ギ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のCylanceは、オーストラリア・シドニーの**Googleビルの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Tridium Niagara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電子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、プラントの各所に頻繁な障害が発生、溶鉱炉が制御不能となり、**最終的に停止不能となり、破壊**させられた。
2016年1月	IBMのX-Force Security Research and Development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。

サイバーセキュリティに対する経営の意識

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について、日本は欧米に比べて脆弱

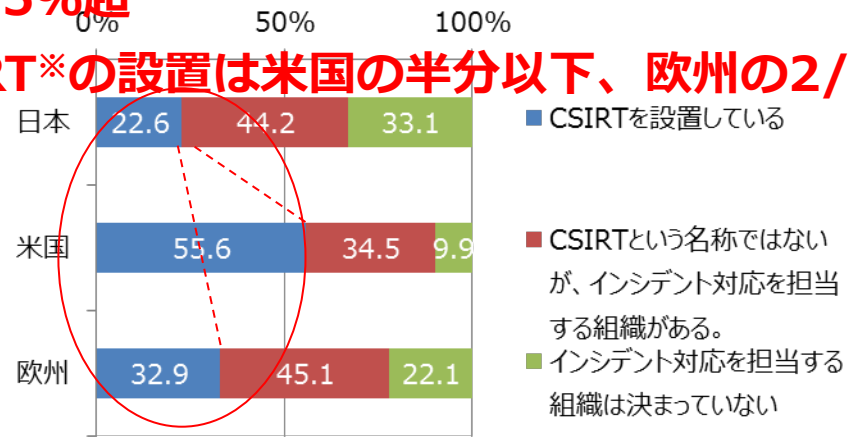
情報セキュリティ対策の体制



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

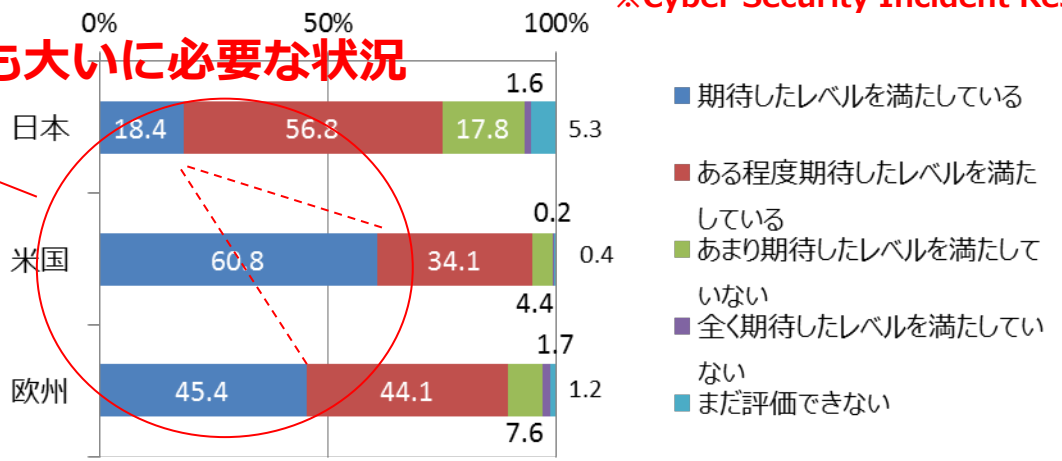


CSIRT※の設置は米国の半分以下、欧州の2/3

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

CSIRTのレベル面の改善も大いに必要な状況

全体評価



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）

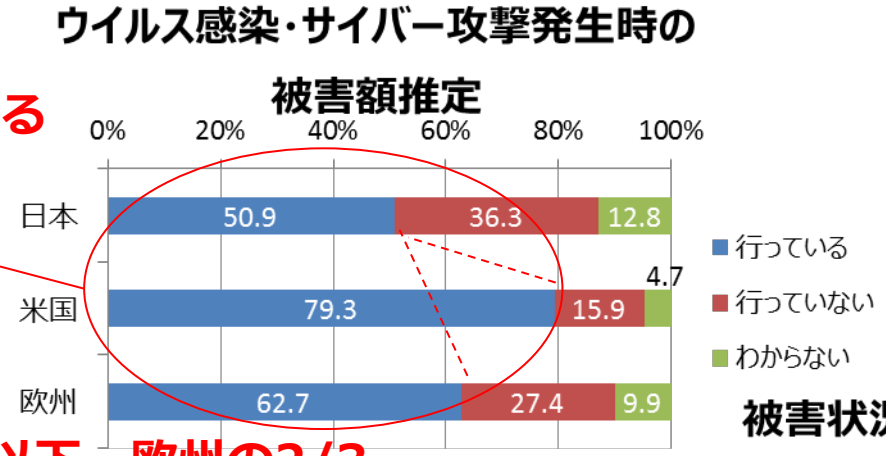
＊ 日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10～11月）

＊ 回収は日本755件、米国527件、欧州526件

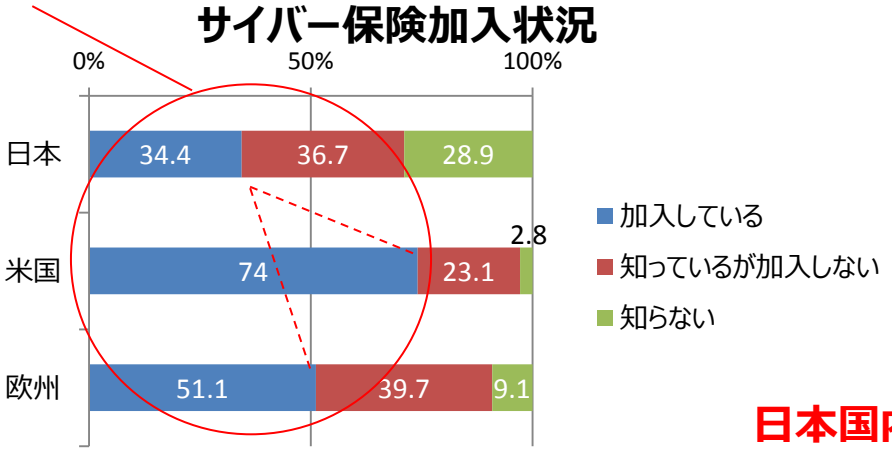
民間セクターのセキュリティリスクへの準備と被害実態（日米欧）

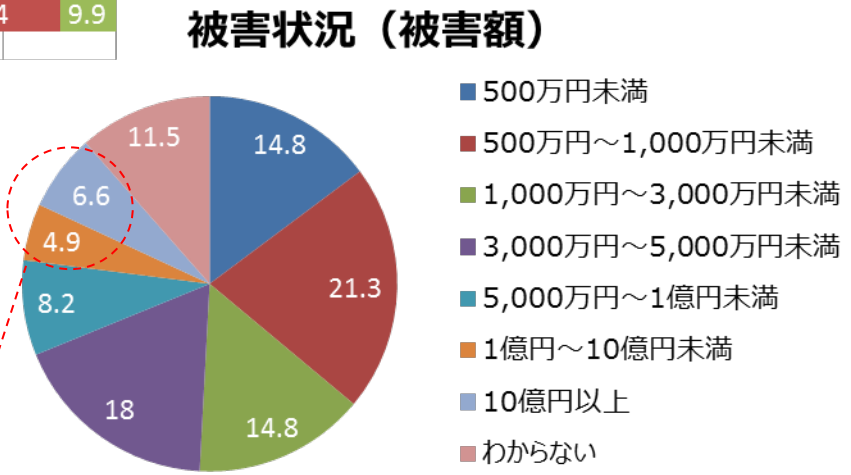
- 日本企業のサイバー攻撃等への事前対策の実施状況は欧米に比べて低調
- 一方、日本企業も1億円を超える被害が発生している

事前に被害推定を行っているケースは少ない



保険の加入は米国の半分以下、欧州の2/3





日本国内でも1億円、10億円を超える被害は既に発生

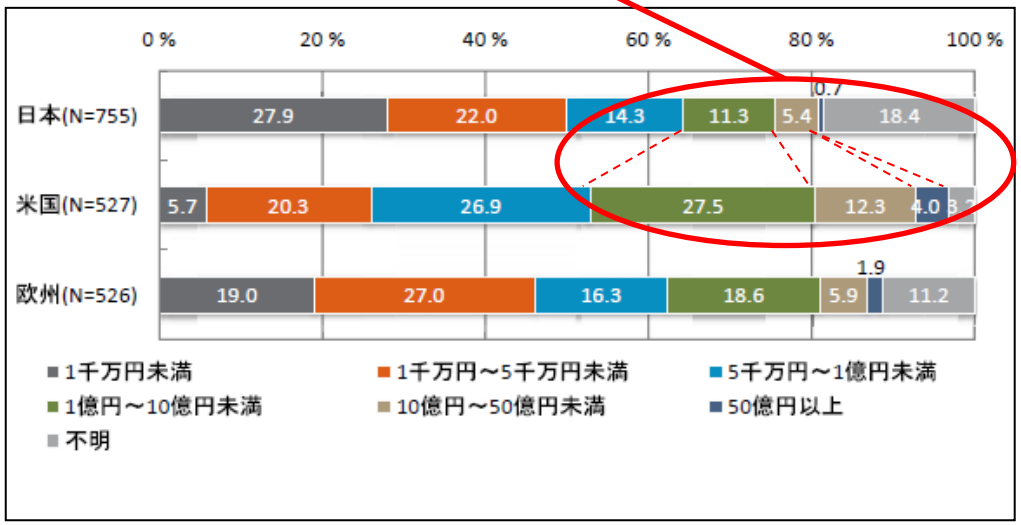
出典：独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017-調査報告書-」（2017年4月13日）
＊日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10～11月）
＊回収は日本755件、米国527件、欧州526件

日本は、サイバーセキュリティ投資が不足

- **日本の一社当たりのセキュリティ投資額は米国等よりも大幅に低い。**
- 国のセキュリティ投資も、**日本は対GDP比で米国よりも1桁少ない。**

民間企業のサイバーセキュリティ投資額

高額投資企業はそれぞれ半分以下



出典：ＩＰＡ「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

日米政府のサイバーセキュリティ予算

国	サイバーセキュリティ予算		GDP比
日本	598.9億円	2017年度予算	0.0098%
米国	約2兆円（190億ドル）	2017年度予算案	0.1020%

データ出典：NISC、米CANP(Cybersecurity National Action Plan)、米NITRD
予算額はCANPによる
何れも三菱総合研究所とりまとめ

うち、研究開発予算（参考）

国	研究開発予算
日本	**約20億円（2014年）** ※サイバー研究開発予算
米国	**約800億円（2014年）** ※情報セキュリティ研究開発予算 ※研究開発予算を通じて人材育成も実施

データ出典：「情報セキュリティ研究開発戦略（改訂版）」2014/7（NISC）

サイバーセキュリティ経営ガイドライン（平成27年12月28日公開、平成29年11月16日改訂）

- 経済産業省と（独）情報処理推進機構（IPA）にて策定。
- 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）経営者は、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、ビジネスパートナーや委託先も含めた**サプライチェーンに対する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に係る情報開示など、**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等に指示すべき１０の重要事項

リスク管理体制の構築

（指示１）サイバーセキュリティリスクの認識、組織全体での対応方針の策定
（指示２）サイバーセキュリティリスク管理体制の構築
（指示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

インシデントに備えた体制構築

（指示７）**インシデント発生時の緊急対応体制の整備**
（指示８）**インシデントによる被害に備えた復旧体制の整備**

リスクの特定と対策の実装

（指示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
（指示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**
（指示６）サイバーセキュリティ対策におけるPDCAサイクルの実施

サプライチェーンセキュリティ

（指示９）**ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握**

関係者とのコミュニケーション

（指示10）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及び提供

※赤字及び太字は平成29年度11月16日改訂部分

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

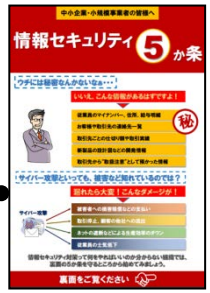
経営者向けの解説

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

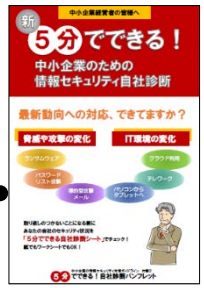
管理者が具体的にセキュリティ対策を実施していくための方法を、**企業のレベルに合わせて段階的にステップアップできる**ような構成で解説

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

サイバーセキュリティ保険について

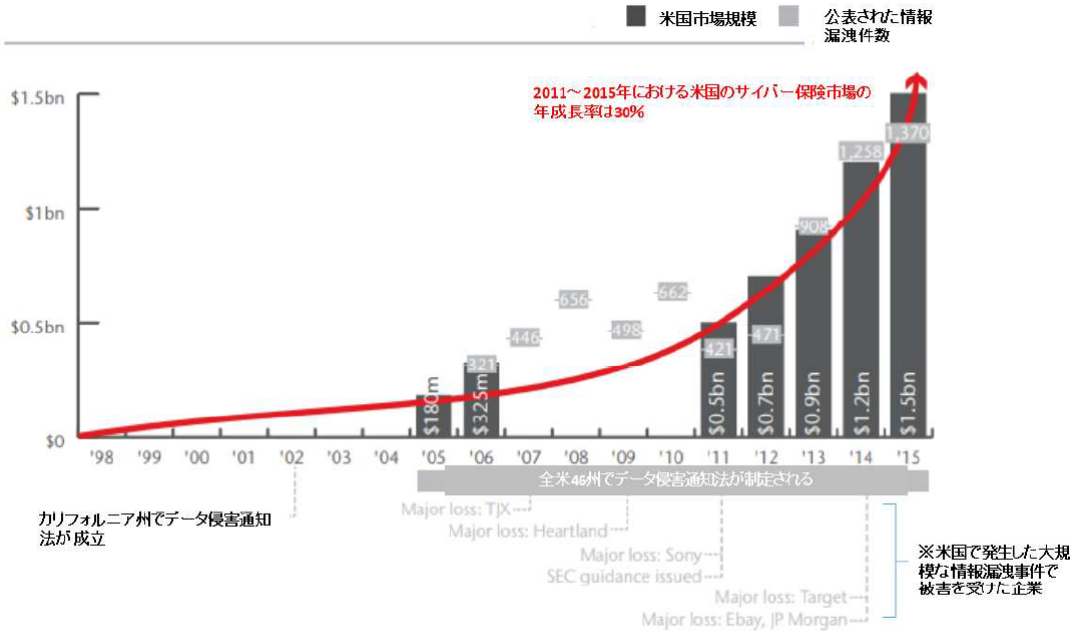
サイバー保険の状況

- 米国と比較すると、**我が国では、サイバーセキュリティ保険市場が小さい**。
- 2015年度時点で、**米国は約1500億円**、**日本は135億円**。

日本のサイバーセキュリティ保険市場規模
（2017年度は予測）

出典：ＪＮＳＡ　2016年度　情報セキュリティ市場調査

米国におけるサイバー保険の推定市場規模推移



※サイバー保険は単独商品として提供されている保険を対象とする。
出典：Aon

サイバーセキュリティリスク評価指標の策定

- 『サイバーセキュリティ経営ガイドライン』と連動した、**サイバー保険の査定にも活用できる『サイバーセキュリティリスク評価指標』を整備する**。

サイバーセキュリティ経営ガイドラインを踏まえた
『サイバーセキュリティリスク評価指標』のイメージ

	サイバーセキュリティ経営の重要10項目	ベストプラクティス（指標）	各社の取組
管理体制構築	サイバーセキュリティリスクの認識、組織全体での対応方針の策定	①実施すべき対策についてベストプラクティスを整理し、 ②評価指標として一般化を目指す	
	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対策のための資源（予算、人材等）確保		
リスクの特定と対策の実装	・・・		
	・・・		
	・・・		
インシデント発生に備えた体制構築	・・・		
	・・・		
サプライチェーンセキュリティ対策の推進	・・・		
関係者とのコミュニケーション	・・・		

■ベストプラクティス・評価指標と比較することで、各社の取組の評価が可能に

■保険会社はサイバー保険の査定に活用

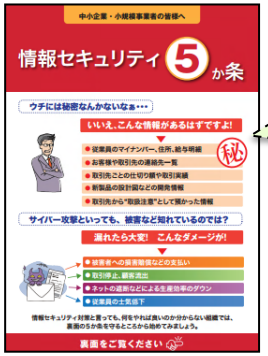
セキュリティ対策自己宣言「SECURITY ACTION」

- 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

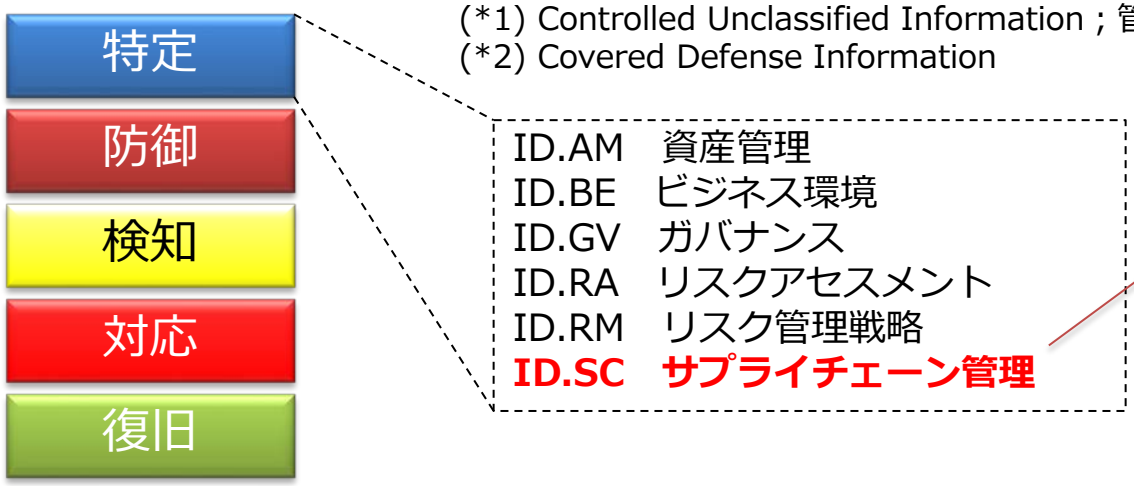
(*) https://www.ipa.go.jp/security/security-action/

米欧の動き

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）**
- 2018年から、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**

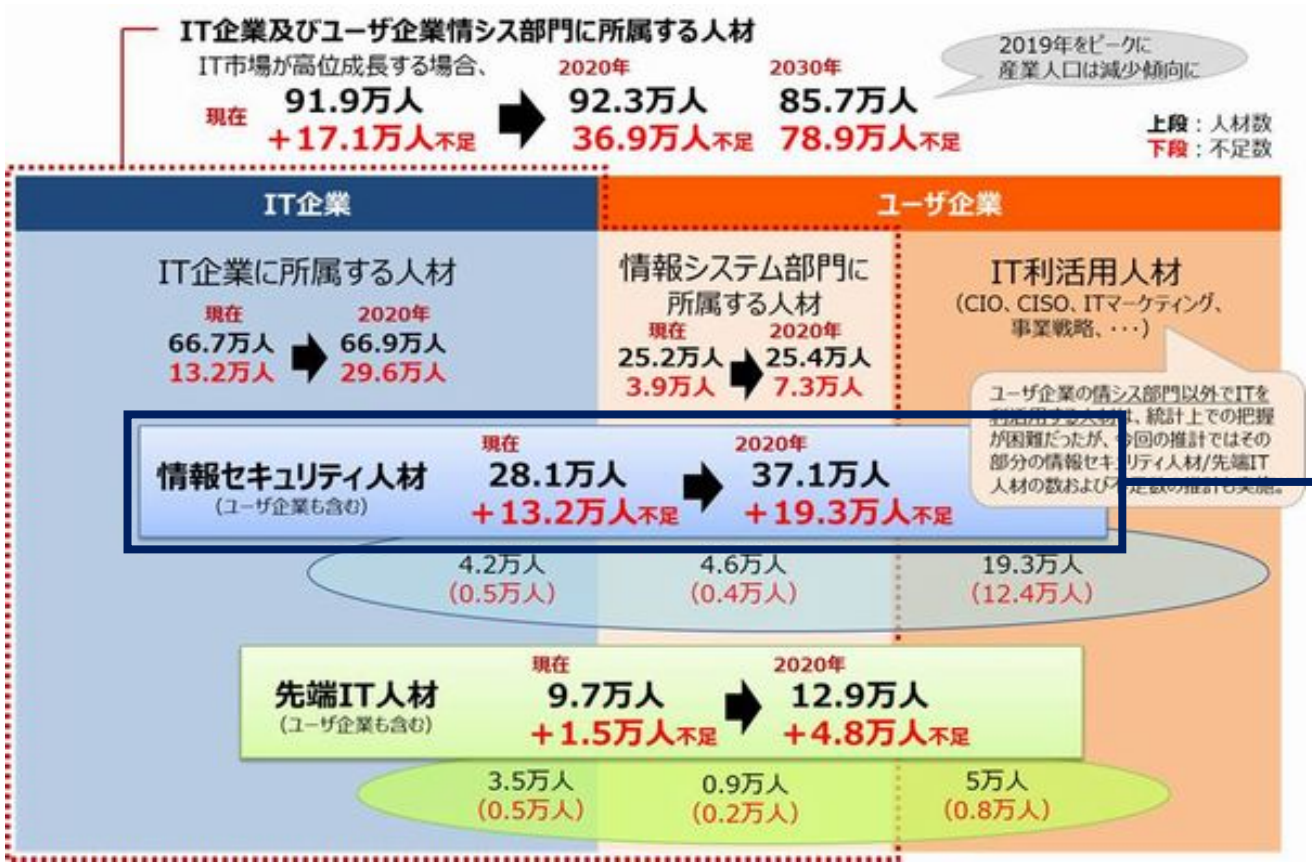
- 現在、small office and homes のルーターのテクニカルガイドラインを作成中（任意制度）

サイバーセキュリティ人材

日本のサイバーセキュリティ人材の需要

- **<u>情報セキュリティ人材は、現在13.2万人不足、特にユーザー企業で大きな不足感。</u>**
- 我が国産業のサイバーセキュリティ対策をけん引するトップ人材は、海外の知見を積極的に活用して育成し、国際的なネットワークを形成していくことが重要。

IT・データ人材の需給に関する推計



海外の知見も習得する高度な人材
全体の1～2割

セキュリティ人材
50万人超（37.1万人＋19.3万人）
（2020年時点）

（資料）経済産業省平成26年度補正先端課題に対応したベンチャー事業化支援等事業「IT人材の最新動向と将来推計に関する調査結果（報告書概要版）」より

重要インフラ・産業基盤のサイバーセキュリティ対策を担う人材の育成

- 2017年4月、IPAに産業サイバーセキュリティセンター(Industrial Cyber Security Center of Excellence, ICSCoE)を設置。電力、ガス、鉄鋼、石油、化学、自動車、鉄道、ビル、空港、放送、通信、住宅等の各業界60社以上から約80名の研修生を受け入れ、実践的な演習・対策立案等のトレーニングを行う。
- 2017年9月、米国・国土安全保障省（DHS）及びICS-CERTから専門家を招聘し、「産業分野におけるサイバーセキュリティの日米共同演習」を実施。
- 2017年11月、イスラエルから複数の有識者を招聘し、世界の最新動向を踏まえた特別講義の開催。

IT系・制御系に精通した専門人材の育成

模擬プラントを用いた対策立案

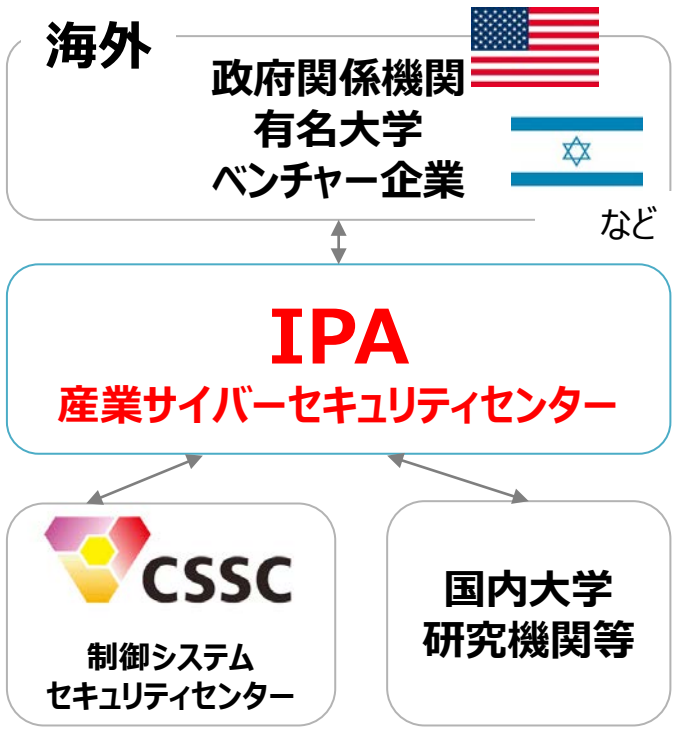
- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家とともに安全性・信頼性の検証や早期復旧の演習を行う。
- 海外との連携も積極的に実施。

実際の制御システムの安全性・信頼性検証等

- ユーザーからの依頼に基づき、実際の制御システムやIoT機器の安全性・信頼性を検証。
- あらゆる攻撃可能性を検証し、必要な対策立案を行う。

攻撃情報の調査・分析

- おとりシステムの観察や民間専門機関が持つ攻撃情報を収集。新たな攻撃手法等を調査・分析。



登録セキスペ（情報処理安全確保支援士）制度の創設

- 情報セキュリティの専門人材を確保できるよう、人材の識別を容易にするとともに、専門人材へのアクセスを確保するため、国家資格「情報処理安全確保支援士」（通称：登録セキスペ）制度を創設。2020年までに登録者3万人超を目指す。

◆ 専門人材を見える化し、活用できる環境を整備することが必要。

➡ **情報処理安全支援士の名称を有資格者に独占的に使用させることとし、さらに民間企業等が人材を活用できるよう登録簿を整備。**

◆ 技術進歩等が早いため、知識等が陳腐化するおそれ。

➡ **有資格者の継続的な知識・技能の向上を図るため、講習の受講を義務化。義務に違反した者は登録を取り消される更新制を導入。**

◆ 専門人材に厳格な秘密保持が確保されていることが必要。

➡ **業務上知り得た秘密の保持義務を措置。**

情報処理安全確保支援士
（登録セキスペ）

2016年

10月21日　情報処理の促進に関する法律施行

2017年

4月　1日　経過措置対象者を対象とした第1回登録により、4,172名の登録セキスペが誕生
4月16日　第1回試験（25,130名応募）
6月21日　第1回試験合格発表(2,822名合格)
10月　1日　第2回登録により、新たに2,822名の登録セキスペが誕生（計6,994名）
10月15日　第2回試験（予定。23,245名が応募）