経済産業省

サイバーセキュリティの現状と経済産業省としての取組

経済産業省

サイバーセキュリティ・情報化審議官

伊東 寛

１．サイバー攻撃の現状

２．経済産業省の取組

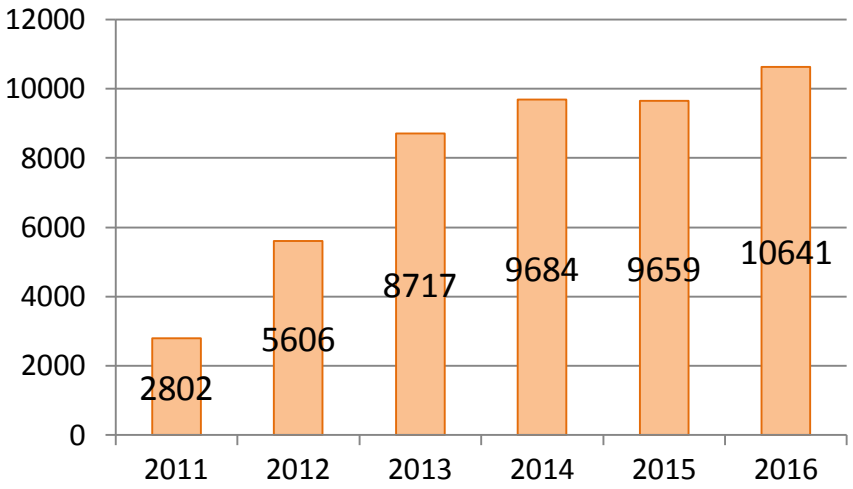
３．サイバーセキュリティ政策の方向性

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 2018	2017 順位	2016 順位
1位	**標的型攻撃による情報流出**	**1位**	**1位**
2位	**ランサムウェアによる被害**	**2位**	**7位**
3位	ビジネスメール詐欺	圏外	圏外
4位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	圏外	6位
5位	セキュリティ人材の不足	圏外	圏外
6位	ウェブサービスからの個人情報の窃取	3位	3位
7位	**IoT機器の脆弱性の顕在化**	**8位**	**圏外**
8位	内部不正による情報漏えいとそれに伴う業務停止	5位	2位
9位	サービス妨害攻撃によるサービス停止	4位	4位
10位	攻撃のビジネス化（アンダーグラウンドサービス）	9位	圏外

（出典）IPAウェブサイトより経済産業省作成

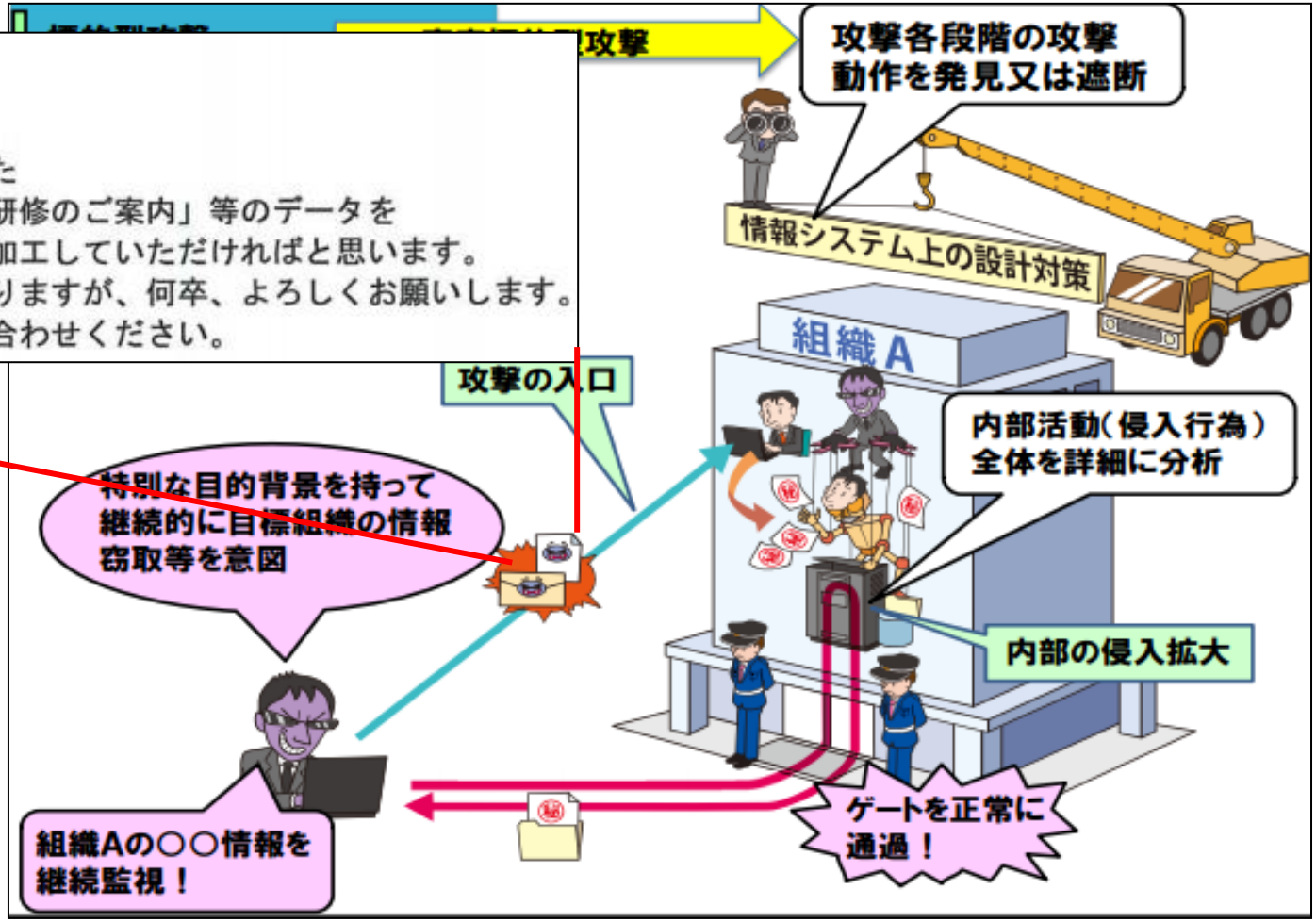
標的型攻撃による情報流出

- 特定の組織（政府関係機関や企業）を狙った標的型攻撃により、個人情報や重要技術等の情報が漏えいするインシデントが多発。

標的型メールの例

○○　○○　様

いつもお世話なっております。
遅くなりましたが、先日、お話しした
第１回養成研修のときに使用した「研修のご案内」等のデータを
送付します。これらを参考にして、加工していただければと思います。
お忙しい中、ご負担をおかけしておりますが、何卒、よろしくお願いします。
何かありましたら、何なりとお問い合わせください。



（出典）「高度標的型攻撃対策に向けたシステム設計ガイド（IPA）」、「不正アクセスによる情報流出事案に関する調査結果報告について（日本年金機構）」より経済産業省作成

ランサムウェアによる被害

- PCをロックしたり、ファイルを暗号化したりしてシステムへのアクセスを制限する。
- アクセス制限の解除を行うために身代金の支払を要求される。
- 2017年5月には世界中で大規模なランサムウェア感染被害も発生した(WannaCry)

料金収納システムがダウン
(アメリカの市営鉄道：2016/11)

客室の開錠システムがダウン
(オーストリアのホテル：2017/01)

国民保険サービスシステムがダウン
(イギリスの医療機関：2017/05)

同様のランサムウェアによりアメリカ、日本、ロシア、中国、ドイツ等多くの国で被害が発生

ランサムウェア”WannaCry”について

- 平成29年５月、世界の少なくとも約150か国において、ソフトウェア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。**

社会インフラを狙ったサイバー攻撃の増加

- 近年は社会インフラに物理的なダメージを与えるサイバー攻撃のリスクが増大。テロリストや他国家によるサイバー攻撃には、大規模停電のように生命・財産を脅かすものがある。
- このため、国民の安全に責任を持つ政府と、インフラの安定的な運用に責任を持つ事業者が連携し、対策に取り組む必要がある。

原発の制御システム停止（米国、2003年）

発電所の制御システムがウィルスに感染。制御システムが約５時間にわたって停止。

製鉄所の溶鉱炉損傷（ドイツ、2014年）

何者かが製鉄所の制御システムに侵入し、不正操作をしたため、生産設備が損傷。

ロンドン五輪への攻撃（イギリス、2012年）

毎秒約１万件の不正通信。開会式会場の電力システムへの攻撃情報。手動への切り替えを準備。

変電所へのサイバー攻撃（ウクライナ、2015年、2016年）

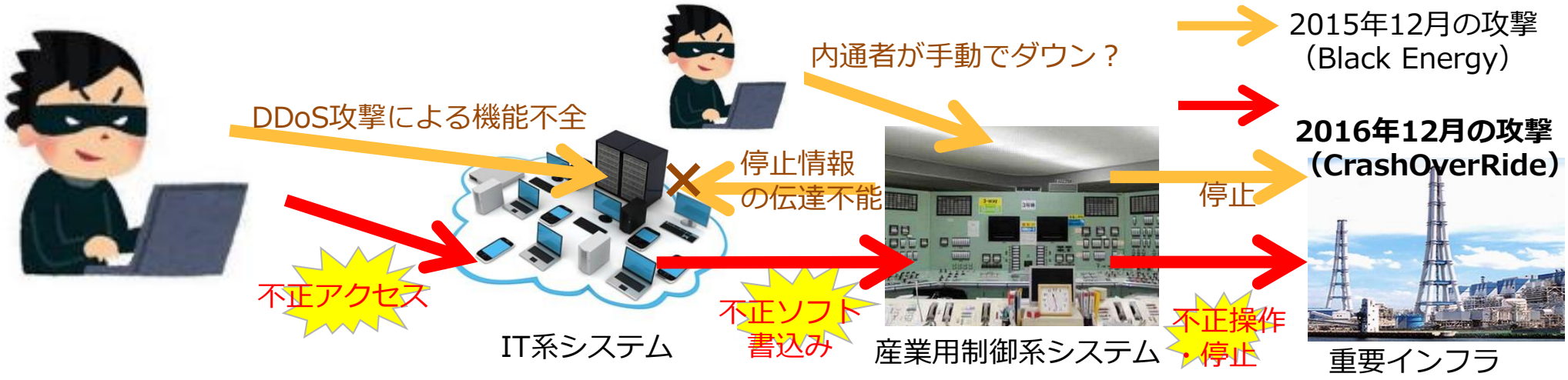
2015年と2016年の12月に発生。マルウェアの感染により、変電所が遠隔制御された結果、数万世帯で停電が発生。

ウクライナにおける2度の停電

- 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。

- **2015年12月（Black Energy・KillDisk）**
  サイバー攻撃だけで電力を直接コントロールするには至っていない。

- **2016年12月（CrashOverRide（Industroyer））**
  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**。



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

１．サイバー攻撃の現状

２．経済産業省の取組

３．サイバーセキュリティ政策の方向性

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（ジェイピーサートコーデ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。

企業が取り組むサイバーセキュリティ対策の推進

- 自然災害等の脅威に比べ、サイバー攻撃の脅威は肌感覚では認識しがたいもの。
- このため、経営者において、①リスク分析によりサイバー攻撃の脅威を正しく認識し、②システム更新・人材育成等のセキュリティを高めるための投資を行い、さらに、③これらを企業活動における継続的サイクルとして根付かせていく、というアプローチが有効である。
- 我が国において、こうした企業活動を定着させ、経済活動として循環させていくことにより、産業を振興・強化していく。

【サイバーセキュリティ対策を実装するためのプロセス】

①サイバー攻撃の脅威の認識

- 情報共有
- リスク分析・評価

②セキュリティ投資の実施

- ◆ 社内システム等へのセキュリティ投資
  - 社内システムの改善
  - 各種ガイドライン
- ◆ 対策の中核を担う人材の育成・配置
  - 産業サイバーセキュリティセンターの活用
  - セキュリティ人材のキャリアパス構築

③ 継続的サイクルとして定着

産業の振興・強化

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、事業継続性の確保やサイバー攻撃に対する防衛力の向上のために、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

サイバーセキュリティ経営ガイドライン Ver2.0

- ３原則を維持しつつ、基本構成を見直し(平成29年11月改訂)

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

サイバーセキュリティ経営ガイドライン Ver2.0

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

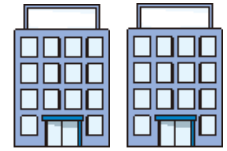
指示

報告

①サイバーセキュリティ対応方針策定

PLAN

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

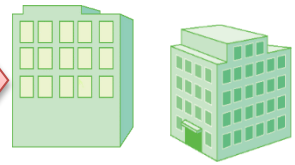
サイバーセキュリティリスク管理体制

◆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

DO

セキュリティ担当、CSIRT等

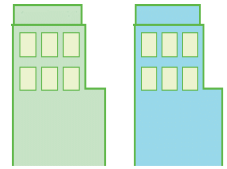
④リスクの把握と対応計画策定

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



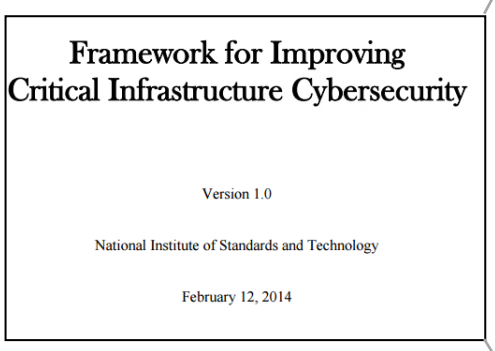
情報共有団体・コミュニティ

CHECK

⑥PDCAの実施

ガイドライン改訂前の主な課題

- 昨今のサイバー攻撃の巧妙化により入口出口対策などの事前対策だけでは対処が困難。
- 米国のサイバーセキュリティフレームワークでも事前対策だけでなく、事後（**検知、対応、復旧**）対策を要求。
- 一方で従来のガイドラインはCSIRTの構築などの「対応」に関する項目はあるものの、「検知」や「復旧」に関する内容が弱く、**国際的な状況を踏まえるとガイドラインとの整合性が不十分**。

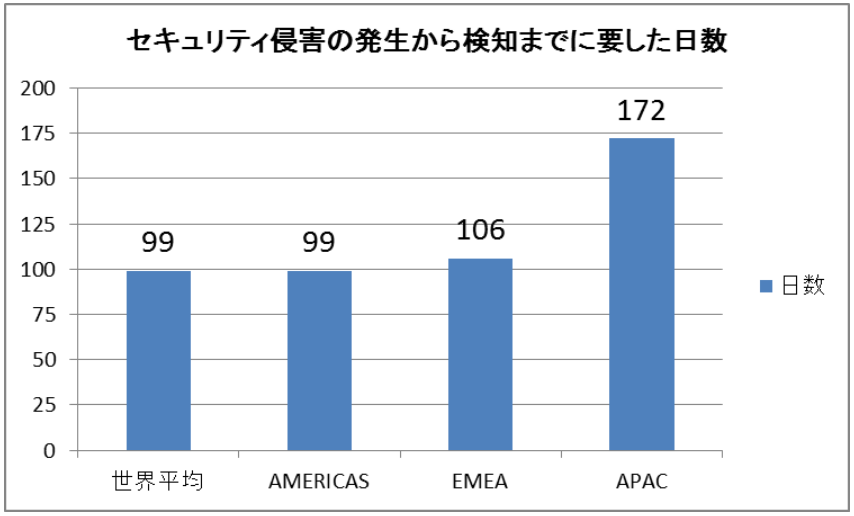


	重要10項目の項番（Ver1.1）
特定	1、2、3、5、7、8
防御	3、6
検知	–
対応	9、10
復旧	–

事後対策の強化　～検知･復旧対策の実施～

- 重要項目　指示5として「攻撃の検知」に関する、「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」を追加

- 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することが重要。
- 約半数の企業が外部からの指摘によりサイバー攻撃による被害が発覚している状況であり、**<u>サイバー攻撃を自分たちで気づけていない</u>**ケースが多い。



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

- 重要項目　指示8 として「復旧」に関する、「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」を追加

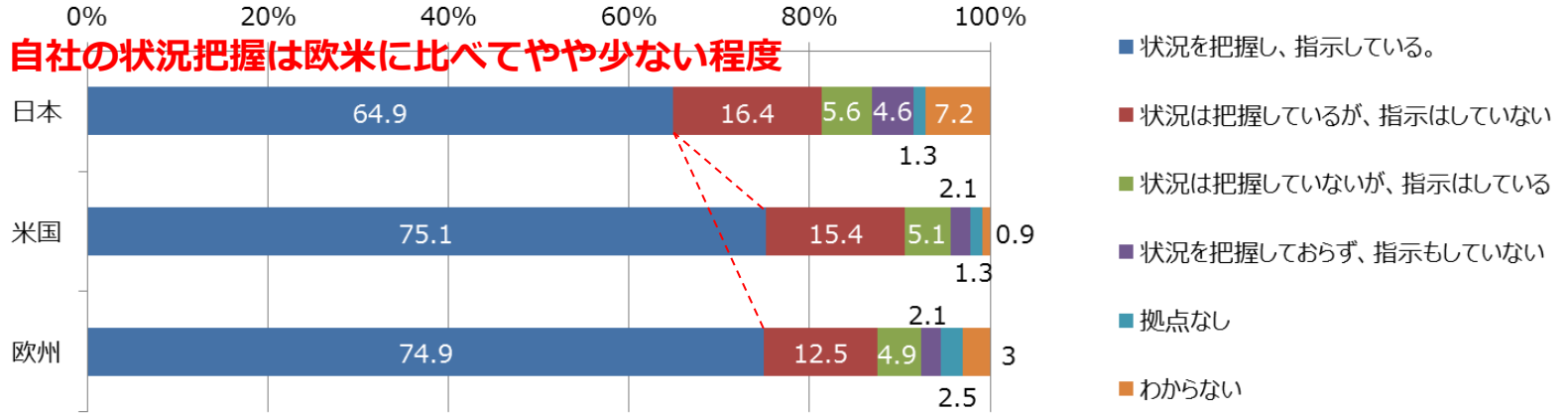
- 企業においてBCPの策定・訓練の実施が進んでいるが、自然災害対策等を想定しており、**<u>サイバー攻撃についての復旧が意識されていない</u>**ケースが多い。

サプライチェーン対策の強化

- 重要項目　指示9の「サプライチェーンのビジネスパートナーや委託先等を含めたサイバーセキュリティ対策の実施及び状況把握」において、委託先におけるリスクマネーの確保や委託先の組織としての活用の把握（ISMSやSECURITY ACTION）等の留意点を追記

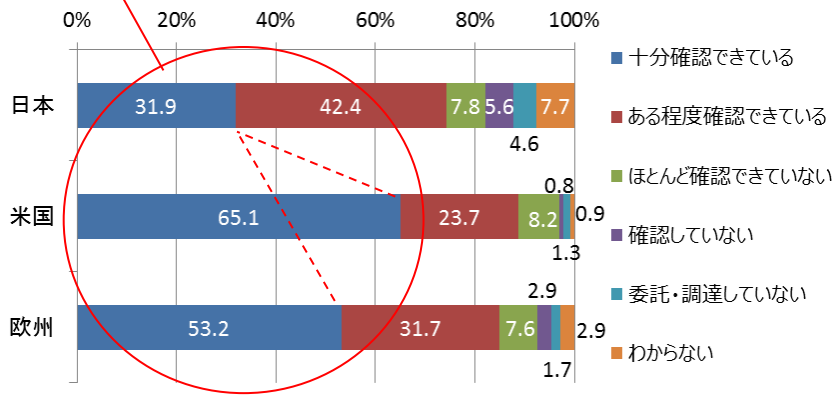
日本企業の自社のセキュリティ点検は欧米にやや遅れる程度だが、委託先等へのケアは大幅に遅れている。

自社拠点のセキュリティ対策状況把握（国内拠点）



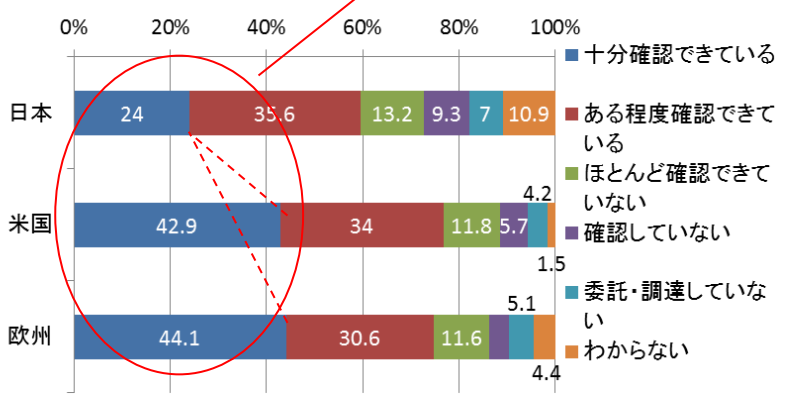
委託先の状況把握は米国の半分以下、欧州の2/3

委託先のセキュリティ対策状況把握（業務委託先）



調達先の状況把握は欧米の6割以下

委託先のセキュリティ対策状況把握（物品調達先）



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

（参考）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

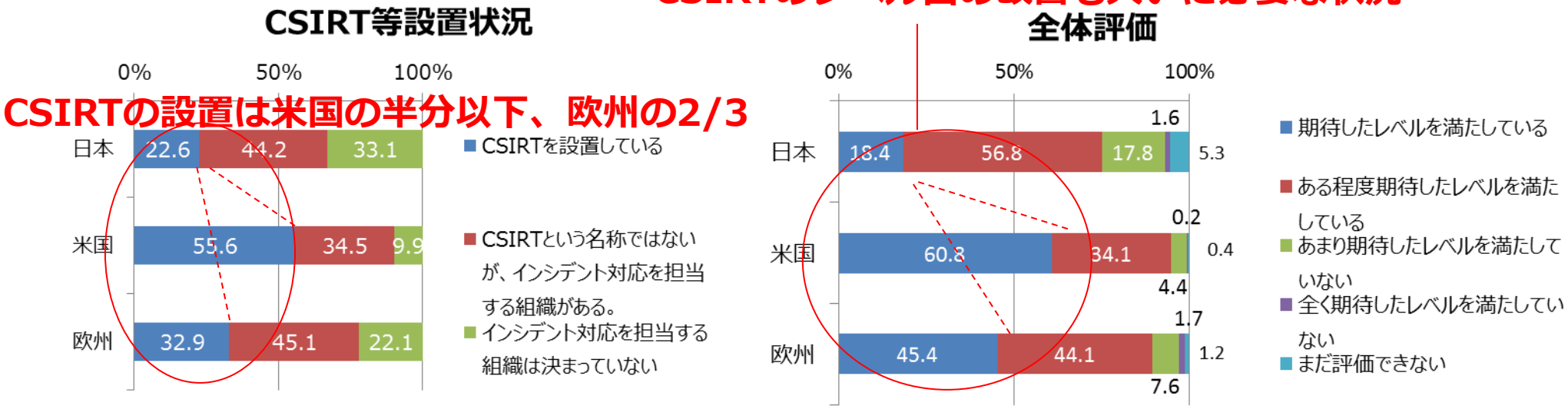
- 「つながる」ことを前提とするコネクテッドインダストリーにおいて、サイバーセキュリティの確保は必要条件
- 2020年東京オリパラに向けて、ボットネット撲滅の推進を決定

事後対策の強化　～インシデント発生時の対応～

- インシデント発生時に組織として調査しておくべき事項をまとめた付録Cを追加

CSIRTの設置が海外よりも遅れており、設置できていても実際にインシデントが発生したときにどのような対処をすべきかについての不安を抱えている企業も多い。

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

重要１０項目の整理

- 新規に２項目（(5)対策実施と(8)復旧）追加するとともに、既存の項目を再整理。
- 重要１０項目の並びについても、３原則、及び作業の時系列を意識して再整理。
- (7)の参考資料として付録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」を新規に追加。

1.リーダーシップの表明と体制の構築	
(1)	セキュリティポリシーの策定
(2)	サイバーセキュリティリスク管理体制の構築
2.サイバーセキュリティリスク管理の枠組み決定	
(3)	リスクの把握、対策目標と計画の策定
(4)	PDCAの実施と対策の開示
(5)	サプライチェーンセキュリティ対策の実施
3.サイバー攻撃を防ぐための事前対策	
(6)	セキュリティ対策のための資源確保
(7)	ITシステム管理の委託範囲の特定
(8)	情報共有活動への参加
4.サイバー攻撃を受けた場合に備えた準備	
(9)	緊急時の対応体制の整備
(10)	被害発覚後の準備

＜経営者がリーダーシップをとった対策の推進＞	
セキュリティマネジメント体制の構築	
(1)	セキュリティポリシーの策定
(2)	サイバーセキュリティリスク管理体制の構築
(3)	セキュリティ対策のための資源確保
セキュリティリスクの特定と対策の実装	
(4)	リスクの把握、対策目標と計画の策定
(5)	リスク対応策（防御・検知・分析）の実施
(6)	PDCAの実施と対策の開示
サイバー攻撃を受けた場合に備えた体制構築	
(7)	緊急時の対応体制の整備
(8)	復旧体制の整備
＜サプライチェーンセキュリティ対策の推進＞	
(9)	サプライチェーンセキュリティ対策の実施
＜関係者とのコミュニケーションの推進＞	
(10)	情報共有活動への参加

新規追加項目　類似項目をマージ

その他の改訂ポイント

＜NISTのサイバーセキュリティフレーワークとの対応関係の提示＞

- 付録Aの各チェック項目について、NISTのサイバーセキュリティフレームワークと対応する項目を提示。

＜冒頭の説明の見直し＞

- 「サイバーセキュリティ経営ガイドライン・概要＞の説明を全体的に修正。
- IoTやAIの活用といった最近の情勢をふまえるとともに、サプライチェーンセキュリティの必要性が高まっていることや、セキュリティ対策を怠ると他社に迷惑をかけることもある等についても言及。

＜統計データのアップデート＞

- １．１節「サイバーセキュリティ経営ガイドラインの背景と位置づけ」で参照している統計データをアップデート。それに伴い説明文も修正。

＜情報共有活動における情報提供の記載を強調＞

- 重要１０項目の（１０）において、従来は「情報の入手とその有効活用」となっていた部分を「情報の提供、及び入手とその有効活用」に修正。

＜その他＞

- 経営者、CISOを対象読者としていることから、冗長な表現を見直し、全体の記載を簡素化。

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

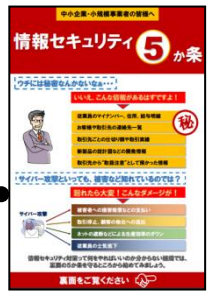
経営者向けの解説

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

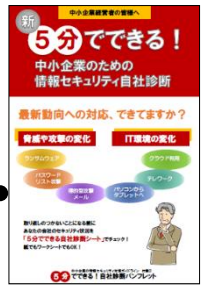
管理者が具体的にセキュリティ対策を実施していくための方法を、**企業のレベルに合わせて段階的にステップアップできる**ような構成で解説

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

（参考）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

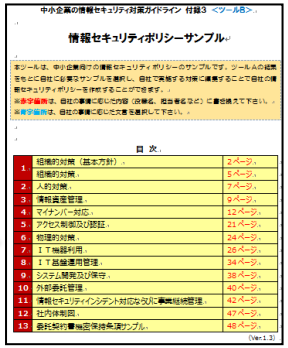
★★ 二つ星

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


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B>
情報セキュリティポリシーサンプル
目 次

1	組織的対策（基本方針）	2ページ
	組織的対策	5ページ
2	人的対策	7ページ
3	情報資産管理	9ページ
4	マイナンバー対応	12ページ
5	アクセス制御及び認証	21ページ
6	物理的対策	24ページ
7	ＩＴ機器利用	26ページ
8	ＩＴ基盤運用管理	34ページ
9	システム開発及び保守	38ページ
10	外部委託管理	40ページ
11	情報セキュリティインシデント対応ならびに事業継続管理	42ページ
12	社内体制図	47ページ
13	委託契約書雛型(保持義務)サンプル	48ページ

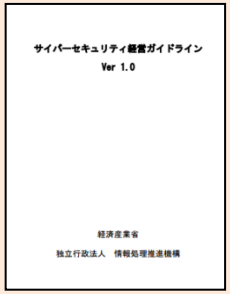
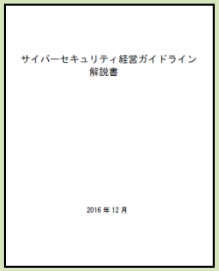
(Ver1.3)

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

（参考）サイバーセキュリティ経営ガイドラインとの関係性

経営者が認識すべき「3原則」とCISO等に指示すべき「重要10項目」を説明。

「3原則」で考慮すべきポイントや、「重要10項目」を実施するための具体的な手順を説明。

企業規模	全体指針	具体的対策
大企業	 サイバーセキュリティ経営ガイドライン（経済産業省、IPA）	 サイバーセキュリティ経営ガイドライン解説書（IPA）
中小企業（セキュリティ対策が進んでいる企業）		
中小企業（セキュリティ対策にこれから着手する企業）		 中小企業の情報セキュリティ対策ガイドライン（IPA）
小規模事業者		

- 「3原則」・「重要10項目」を中小企業向けにかみ砕いて「3原則」・「重要7項目」として説明。
- 対象としては情報セキュリティのみでなく、サイバーセキュリティも含む。

IoTセキュリティガイドライン

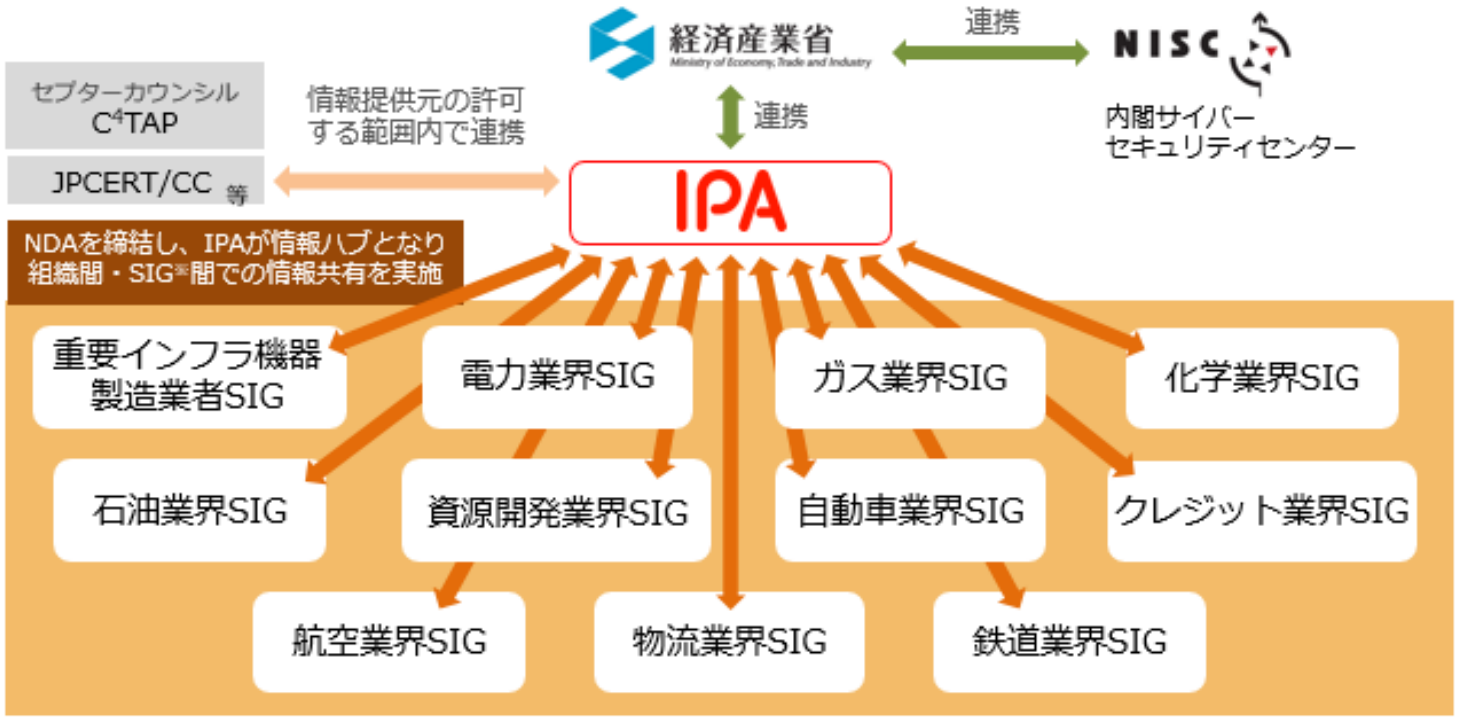
（IoTセキュリティWGにおいて策定：総務省・経済産業省共同事務局）

- 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。
- 日本が主体となって、ISO/IEC JTC1 SC27/WG4に、本ガイドラインをベースとしたIoTセキュリティ規格の提案を行い、標準化活動を推進中。

	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

重要インフラ事業者に対するサイバー攻撃情報共有体制（J-CSIP）

- 電力・ガス等の重要インフラ企業に対するサイバー攻撃の情報共有が、組織的な防御力向上に不可欠。
- IPAは、重要インフラ事業者に対するサイバー攻撃情報共有体制（J-CSIP（ジェイシップ）：Initiative for **C**yber **S**ecurity **I**nformation sharing **P**artnership of **J**apan、11業種、190組織が参加）を構築。
- 公的機関としての信頼性を基に、秘密保持等契約を結び、企業から情報を収集、解析、秘匿化し、迅速に共有することにより被害拡大を防止。



J-CSIP
Initiative for Cyber Security Information sharing Partnership of Japan

攻撃手口を解析し、提供者の営業秘密等保護のための匿名化を行った上で共有。

共有件数
（800件以上）
（2012年5月からの累計）

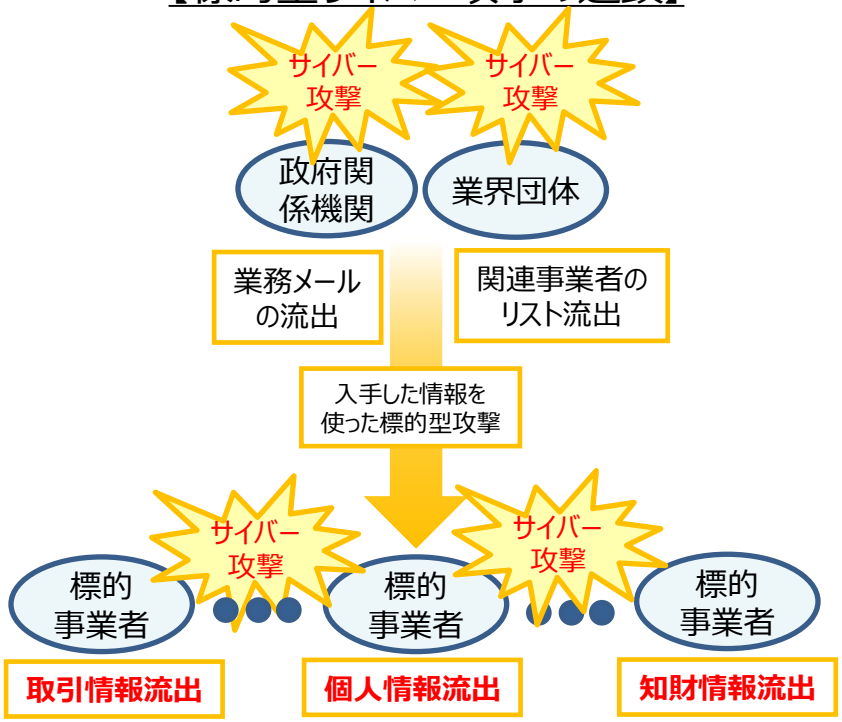
高度標的型サイバー攻撃を受けた組織への初動対応支援

●平成26年7月、IPAに、個々の組織の能力では対処困難な、高度標的型サイバー攻撃を受けた組織に対する初動対応を行う「サイバーレスキュー隊(J-CRAT)」を立ち上げ。

（J-CRAT（ジェイ・クラート）：**C**yber **R**escue and **A**dvice **T**eam against targeted attack of **J**apan）

●最初の標的となり、対応遅延が社会や産業に重大な影響を及ぼすと判断される組織（主として、重要インフラ事業者、業界団体・独法等）に対して支援を実施。

【標的型サイバー攻撃の連鎖】



【サイバーレスキュー隊の活動】

政府関係機関、業界団体等

経済社会に被害が拡大するおそれが強く、一組織で対処が困難な深刻なサイバー攻撃の発生

初動時の緊急処置の助言、被害状況の理解促進、対応体制の早急な立ち上げの支援

支援数
406件（累計）
※2017年度９月末時点

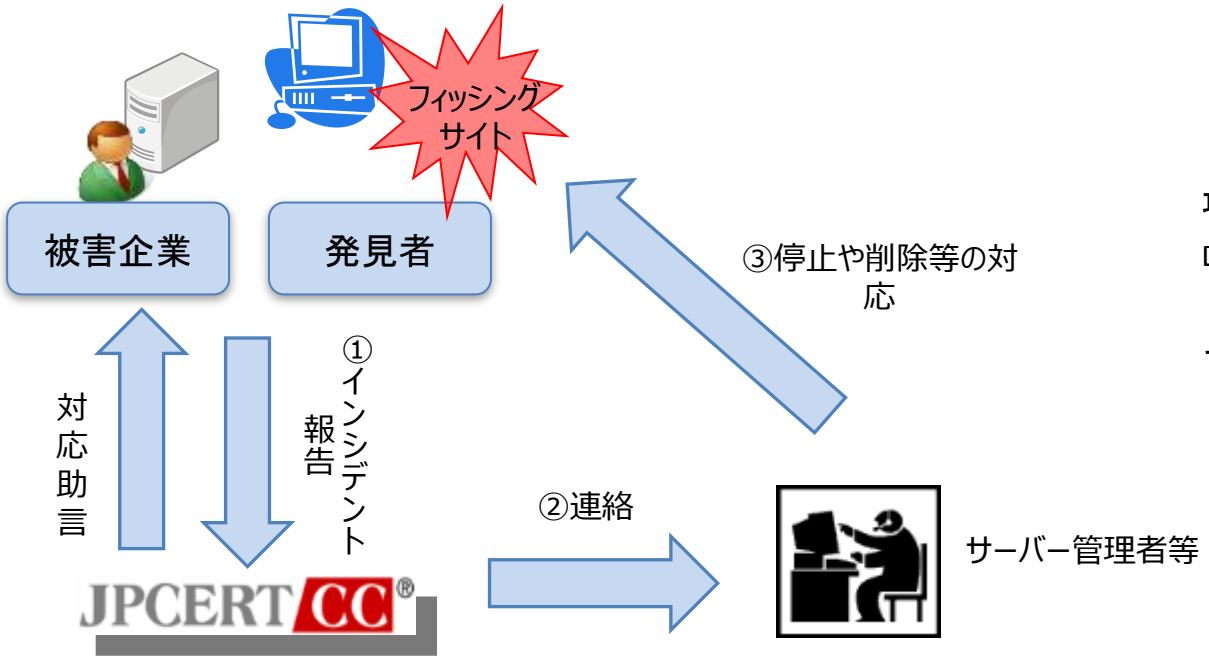
サイバーレスキュー隊

インシデントへの対応支援

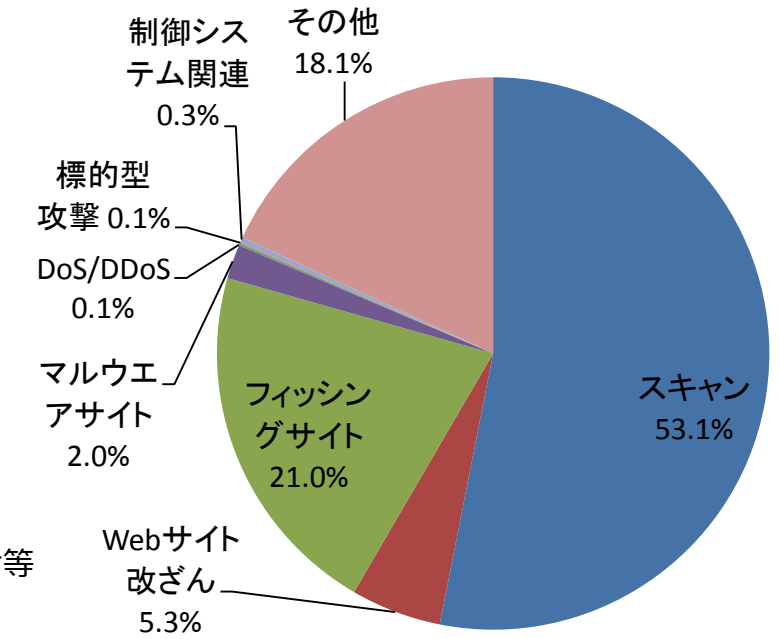
- 一般社団法人JPCERT/CCは、国内におけるインシデントへの対応支援も実施。
- 例えば、被害者や発見者から、ウェブサイト改ざん、DoS・DDoS等のサービス妨害攻撃、マルウエア配付サイトや、マルウエア添付メール等によるシステムへの不正侵入などのインシデント報告を受けて、ISP・ASP事業者やシステム管理者等に連絡し、インシデント発生元への対応依頼など、被害拡大の抑止を実施。

※ISP:インターネットサービスプロバイダ。ASP：アプリケーションサービスプロバイダ

【インシデント対応のイメージ】



【JPCERT/CCが報告を受けたインシデント件数の割合】



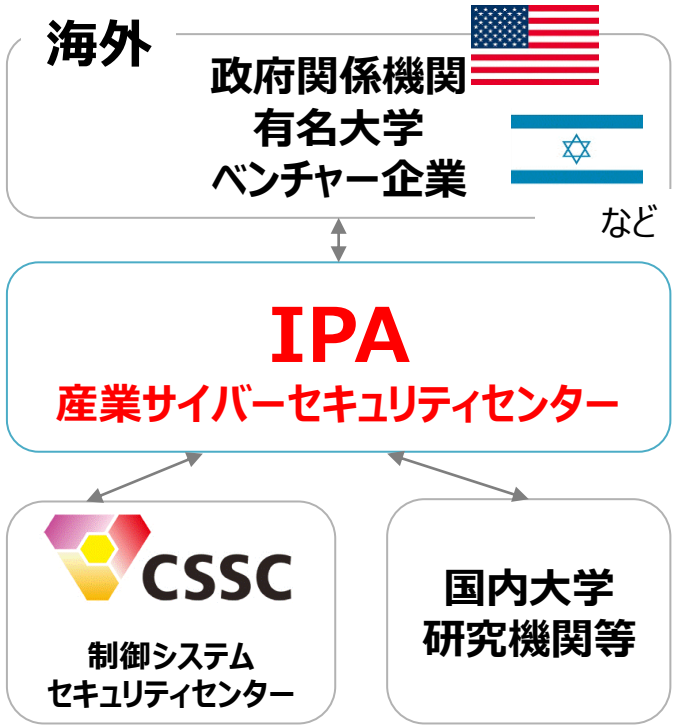
（出典）JPCERT/CCインシデント報告対応レポート (2017年7月1日～9月30日)より作成

産業サイバーセキュリティセンター

- 2017年4月、IPAに産業サイバーセキュリティセンターを設置
- 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
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

現場を指揮・指導するリーダーを育成



１．サイバー攻撃の現状

２．経済産業省の取組

３．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及びWGの全体構成

- 産業サイバーセキュリティの旗を掲げた研究会及びテーマ毎のＷＧを設置し、我が国の産業がサイバーセキュリティに関して直面する課題に対応していく。

産業サイバーセキュリティ研究会　平成29年12月設置

■政策の方向性を提示

ＷＧ１　制度･技術･標準化　平成30年2月設置

■制度・技術・標準化を一体的に政策展開する戦略を議論

ＷＧ２　経営･人材･国際

■サイバーセキュリティ政策全体の共通基盤となる経営・人材・国際戦略を検討

ＷＧ３　サイバーセキュリティビジネス化

■セキュリティサービス品質向上と国際プレーヤー創出に係る政策を検討

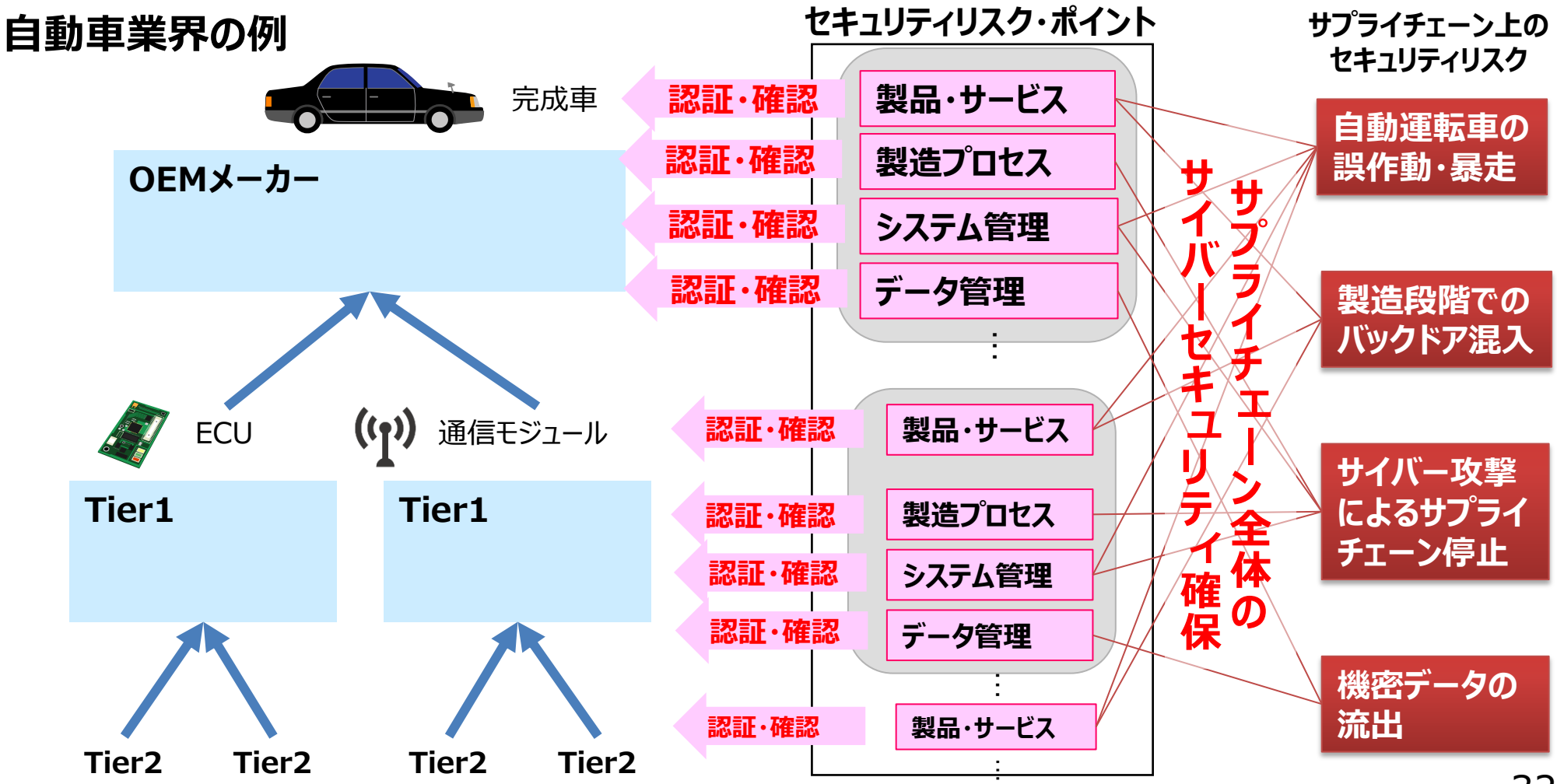
連携

中小企業政策審議会基本問題小委員会等

■中小企業の生産性向上に資するIT利活用支援策とともに検討

（参考）サイバー・フィジカル・セキュリティ対策フレームワークの策定

- **産業に求められるセキュリティ対策の全体像を整理**し、**産業界が活用できる『サイバー・フィジカル・セキュリティ対策フレームワーク』の作成**を目指す



（参考）『サイバー・フィジカル・セキュリティ対策フレームワーク』のイメージ

WG1において検討を進め、年度内に大枠を整理することを目指す

来年度以降SWGにおいて具体を検討

3つの切り口	脅威が守るべきものへ与える影響(リスク分析) **守るべきもの**	**脅威**	**具体的な対応策（構成要素ごとに整理）**
企業と企業の繋がり	・仕様通りの製品、サービス ・情報の秘密保持 ・安全な取引	■マルウェアの混入 ■不正な機器の混入(調達段階)	**セキュアなサプライチェーン構築のために取引先に確認すべき項目** ■納入されるモノのセキュリティ確保 ■取引先のセキュリティ状況の確認 ■取引先とのやり取りのセキュリティ確保
フィジカル空間とサイバー空間の繋がり	・実現したい機能 ・レジリエンス ・セキュリティ ・セーフティー　等	■不正な機器の混入(設置段階) ■計測データの改ざん ■制御機能への攻撃	**セキュアなCPS構築に向けて必要な対策の項目** ■安全なIoTシステムの導入 ■CPS/IoTの構築と運用 ■組織文化の醸成　等
サイバー空間とサイバー空間の繋がり	・セキュアなデータ流通 ・サイバー上でのサービス利用	■データベースに格納されるデータの信ぴょう性 ■データプラットフォームへの攻撃 ■ネットワーク上での攻撃	**セキュアなデータ連携・活用に必要な対策の項目** ■データプラットフォームのセキュリティ ■データ品質の確認 ■データプラットフォームに参加する企業のセキュリティの確認　等

互いに関係

互いに関係

各分野のライフサイクルや求められる機能を踏まえたセキュリティ対策ガイドライン

ご清聴ありがとうございました