経済産業省

産業分野におけるサイバーセキュリティ

～サイバー・フィジカル・セキュリティ対策フレームワークを中心に～

経済産業省　商務情報政策局

サイバーセキュリティ課長

奥家 敏和

１．はじめに
~サイバー攻撃の脅威レベルの向上と海外の動き

２．産学官の検討体制の構築
~産業サイバーセキュリティ研究会

３．「Society5.0」において必要なセキュリティ対策
~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

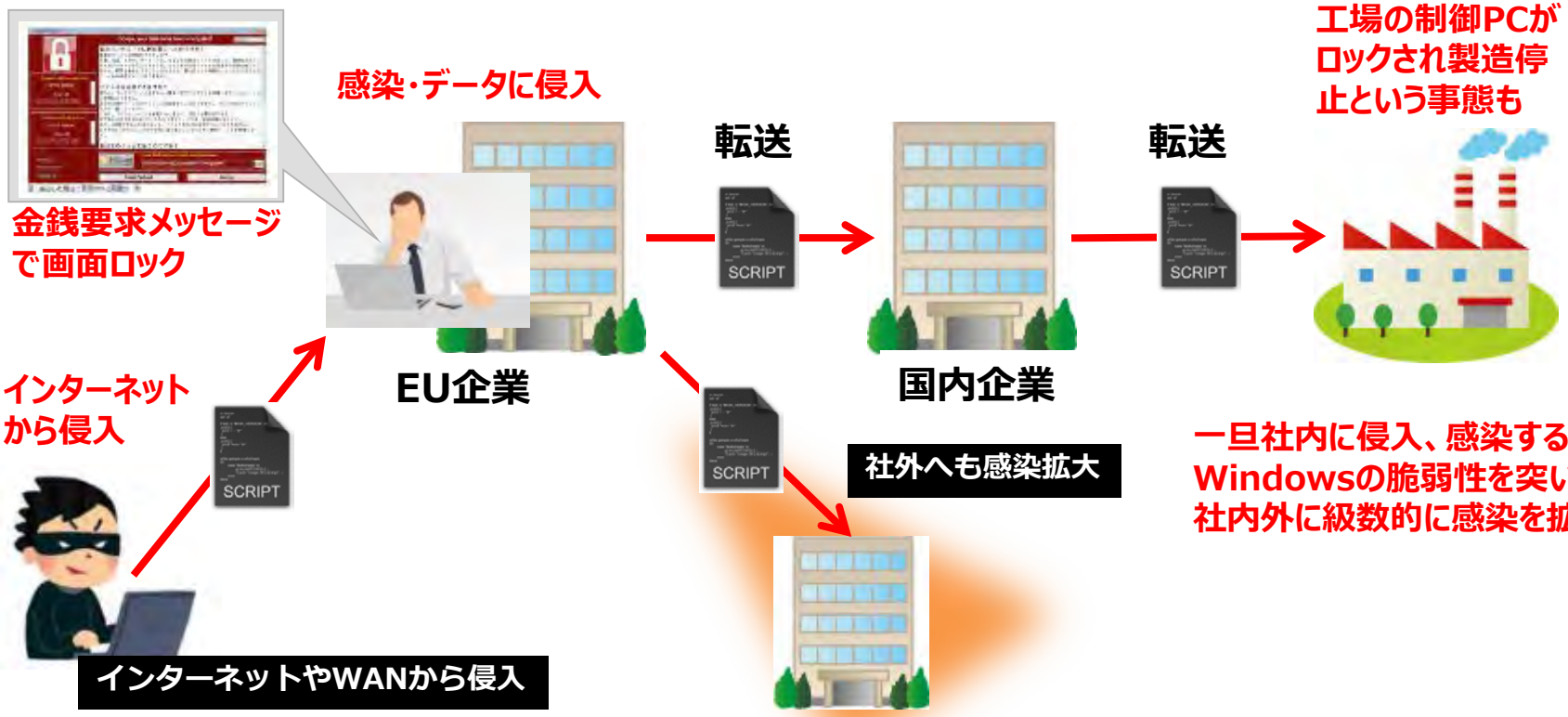
４．海外のサプライチェーンの強化

５．サイバーセキュリティ対策の基盤整備
~経営者の意識喚起、人材育成

６．サイバーセキュリティビジネスの創出
~エコシステムの構築

サイバー攻撃の脅威レベルの増大（サプライチェーンを通じた攻撃（水平的脅威））
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増大（サプライチェーンを通じた攻撃（水平的脅威））
台湾積体電路製造（TSMC）のランサムウェア感染事案

- 2018年8月3日、半導体受託生産の世界最大手である**台湾積体電路製造（TSMC）※において、主力工場内ネットワーク機器がマルウェア感染**。6日午後に復旧するまでの間、**生産が一時停止**。
- 生産停止による**損害額は最大190億円**（営業利益ベース）。

※台湾TSMC社：台湾新竹市に本拠を置く世界最大の半導体製造企業。2014年の市場シェアは53.1%。
顧客企業は米アップル、クアルコム、NVIDIA等、数百社に上る。

本事案の詳細（原因等）

- 感染したマルウェアは、2017年5月に世界中で猛威を振るった「WannaCry」の亜種（金銭要求画面が出ずに機器を停止）。
- 感染した新規追加機器を工場内ネットワークに接続したことで、ネットワーク内感染が発生。
- 本来、接続前に閉鎖環境でウィルススキャンする手順であったが、内部の作業ミスにより実施されなかった。
- 加えて、ネットワーク内機器がWindows7端末であったため、ネットワーク内で感染が拡大。

３日間の生産停止により、損害額１９０億円

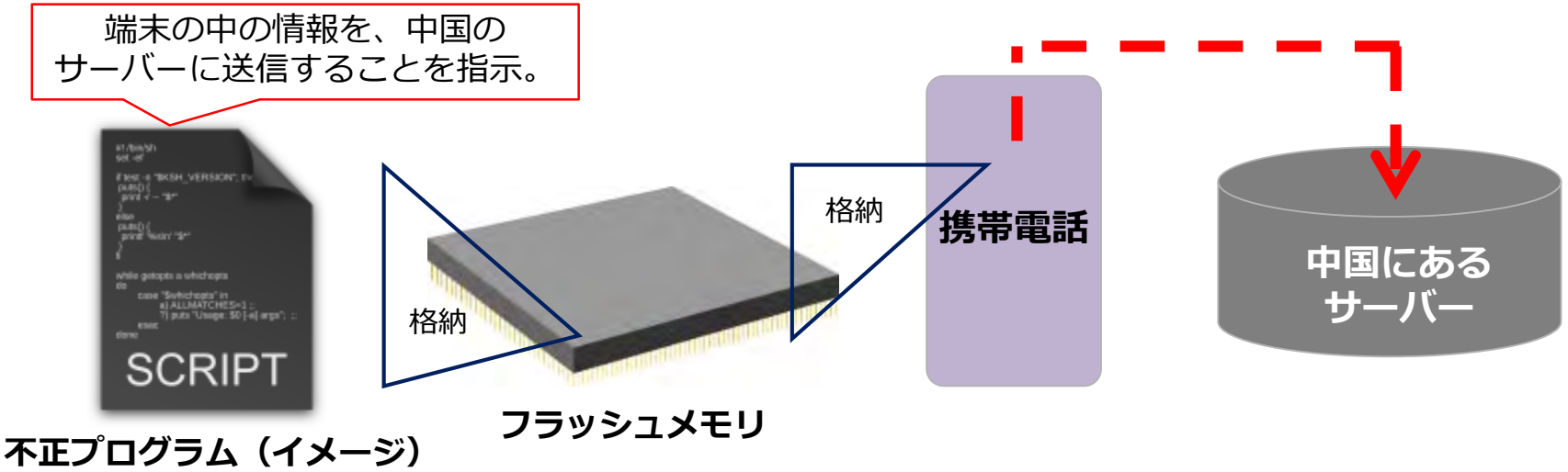
感染イメージ

サイバー攻撃の脅威レベルの増大（サプライチェーンを通じた攻撃（水平的脅威））
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。



サイバー攻撃の脅威レベルの増大
（情報システムを越えて制御システムに達する攻撃（垂直的脅威））
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

（参考）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

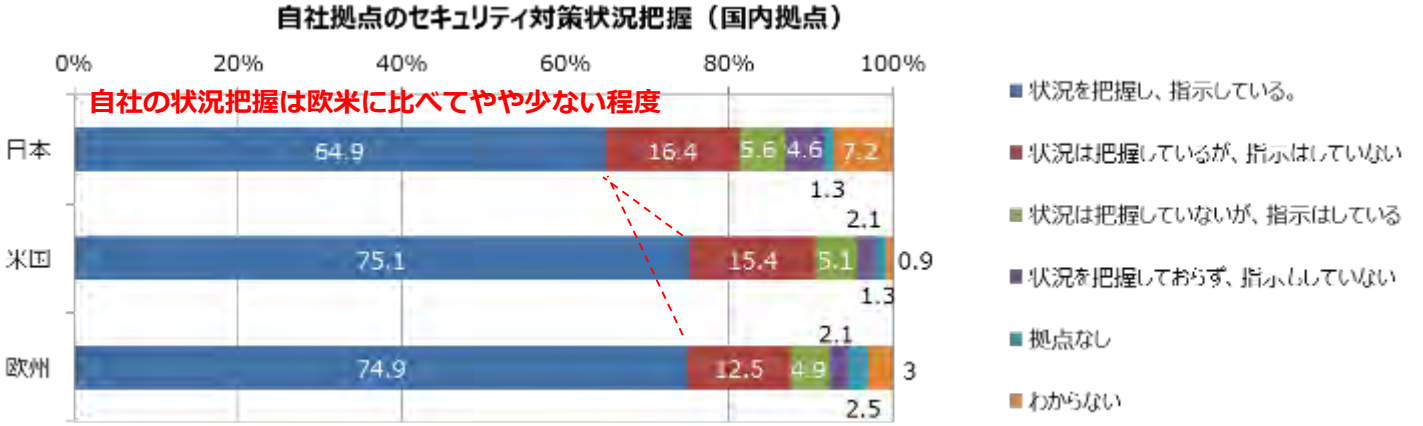
偵察活動

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

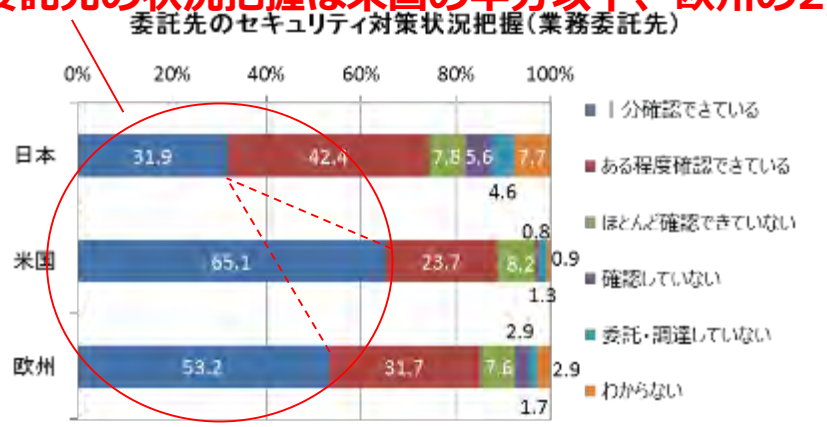
電力制御系システムの防御対策等の情報漏えい　→　さらなる攻撃による電力供給停止

取引先へのサイバーセキュリティ対策の遅れ

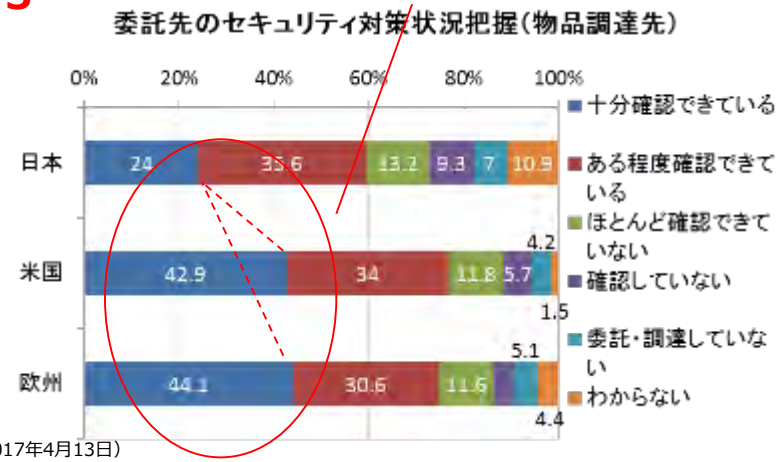
- **日本企業では、委託先等の取引先への対応が大幅に遅れている。**



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）

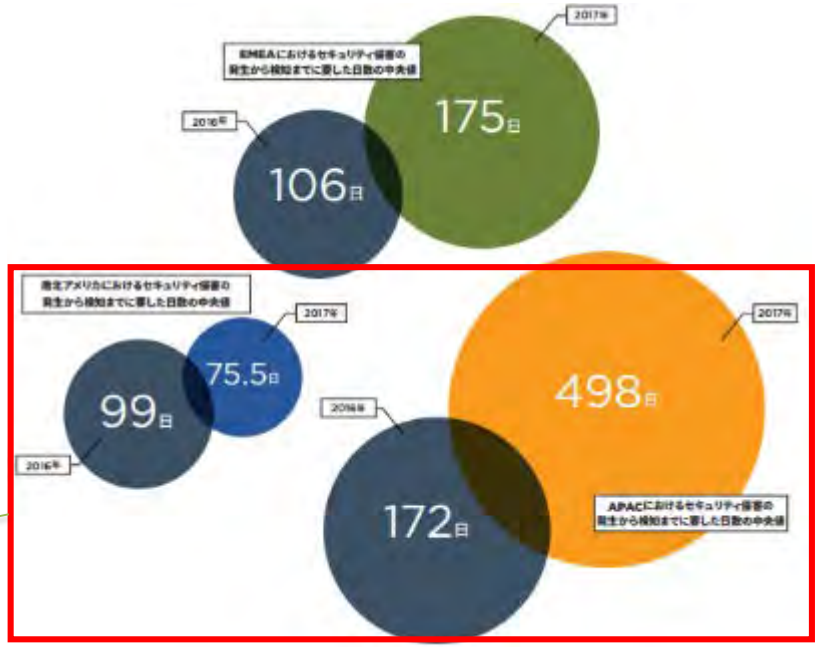
＊ 日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10～11月）

＊ 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。

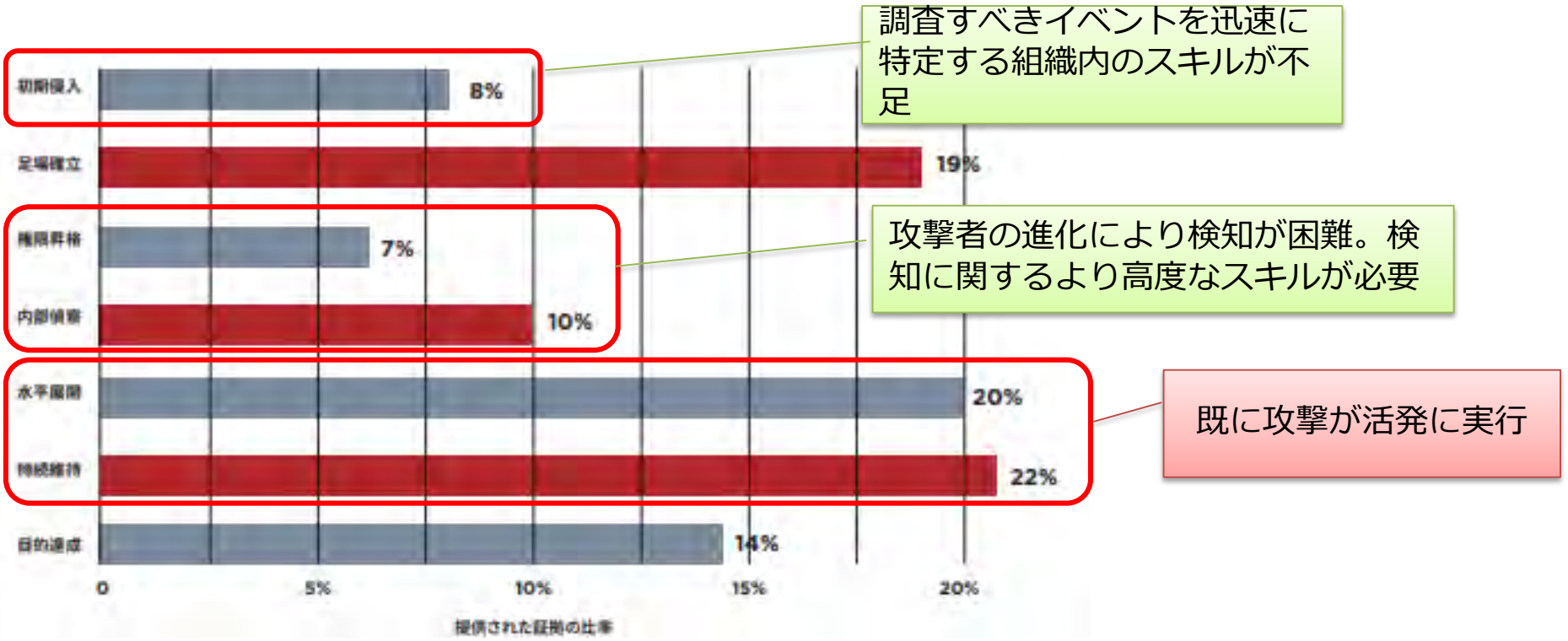


セキュリティ侵害の発生から検知に要した日数（地域別）

（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．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．「Society5.0」において必要なセキュリティ対策
～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

４．海外のサプライチェーンの強化

５．サイバーセキュリティ対策の基盤整備
～経営者の意識喚起、人材育成

６．サイバーセキュリティビジネスの創出
～エコシステムの構築

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とWGの設置による検討体制

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（４つの柱）を提示

構成員

※第2回開催時点

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　株式会社日立製作所会長、
(日本経済団体連合会会長)

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

村井　純(座長)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基本法改正（NISC）にて対応　3/9 閣議決定

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

１．サプライチェーン強化パッケージ

WG２（経営･人材･国際）　第１回 3/16 / 第２回 5/22

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

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

４．ビジネスエコシステム創造パッケージ

１．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．「Society5.0」において必要なセキュリティ対策
～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

４．海外のサプライチェーンの強化

５．サイバーセキュリティ対策の基盤整備
～経営者の意識喚起、人材育成、情報共有、初動対応、
重要インフラ支援

６．サイバーセキュリティビジネスの創出
～エコシステムの構築

サイバー・フィジカル・セキュリティ対策フレームワークを策定する目的

- 「Society5.0」、「Connected Industries」の実現へ向けて、**産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応することが必要**。
- **このため、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』の策定**を進めている。

１．各事業者がフレームワークを活用することで期待される効果

- **「Society5.0」、「Connected Industries」の実現に求められるセキュリティの確保**
- **製品・サービスのセキュリティ品質を差別化要因（価値）にまで高めることによる競争力の強化**

２．フレームワークの特徴

① 各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる
- 社会として目指すべき概念だけではなく、各事業者が実際にセキュリティ対策を実施するうえで活用できる内容にする。

② セキュリティ対策の必要性とコストの関係を把握できる
- サプライチェーン全体を構成する中小企業を含めた事業者が、実際に対策を行えるよう、想定されるリスクと必要な対策のコストのバランスをイメージできるような内容にする。
- セキュリティレベルを保ったままでコストを圧縮できるような内容にする。
- リスクシナリオベースの考え方も考慮した内容にする。

③ グローバルハーモナイゼーションを実現する。
- グローバルサプライチェーンの中で、日本における製品・サービスのセキュリティ対策が海外からも認められるよう、諸外国の動きをよく取り入れ、ISMSやNIST Cybersecurity Frameworkなど米欧などの主要な認証制度との整合性を確保し、相互承認を進めていくことができる内容にする。

フレームワークの構造～「Society5.0」型サプライチェーン“価値創造過程”への対応

- あらゆるものがつながるIoT、データがインテリジェンスを生み出すAIなどによって実現される**「Society5.0」（人間中心の社会）、「Connected Industries」では、製品/サービスを生み出す工程（サプライチェーン） も従来の定型的・直線的なものとは異なる、多様なつながりによる非定型の形態を取る**ことになる。
- 本フレームワークでは、このような**「Society5.0」型サプライチェーンを**これまでのサプライチェーンとは区別して認識するため、**価値創造過程（バリュークリエイションプロセス）と定義**し、「Society5.0」、「Connected Industries」によって拡張したサプライチェーンの概念に求められるセキュリティへの対応指針を示す。

- 本フレームワークは、価値創造のための活動が営まれる産業社会を、下記の**三層構造**と**6つの構成要素**で捉え、包括的にセキュリティポイントを整理し、それらに対応するための指針となるものである。　⇒　**詳細は次頁以降参照**

◆三層構造

第3層－　サイバー空間におけるつながり

第2層－　フィジカル空間とサイバー空間のつながり

第1層－　企業間のつながり（従来型サプライチェーン）

◆６つの構成要素

－組織、ヒト、モノ、データ、プロシージャ、システム

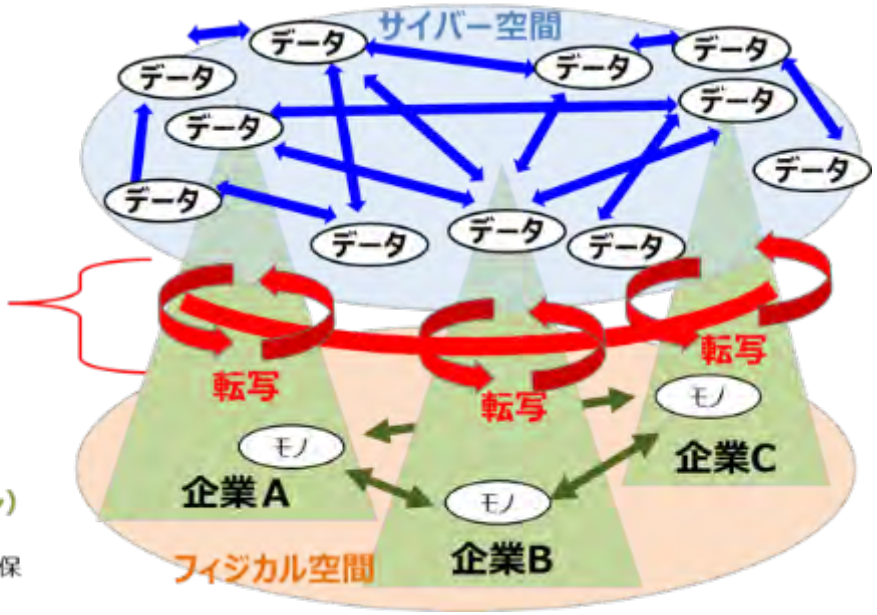
三層構造アプローチの意義

- 3つの層には、価値創造過程において確保されなければならない機能・役割が存在する。
- 例えば、各層において以下で示すようなことが確保されていなければ、価値創造過程は成立をしないことになる。
  - 第１層では生産された製品等－信頼できる企業が信頼できる生産活動によって仕様どおりの製品やサービスを供給しているか否か
  - 第２層ではセンサーで読み込まれたデータ等－フィジカル空間における情報を、センサーなどのIoT機器が正確にデジタル化し、サイバー空間に“転写”しているか否か
  - 第３層ではデータ分析で得られたデータ等－収集する過程で改ざんされていないデータを適切な方法で加工した、信頼できるデータを活用できるか否か
- 本フレームワークでは、各層で創造される価値の持つ特徴を踏まえた対応の方針を示す。

サイバー空間におけるつながり
【第３層】
- 自由に流通し、加工・創造されるサービスを創造するためのデータの信頼を確保

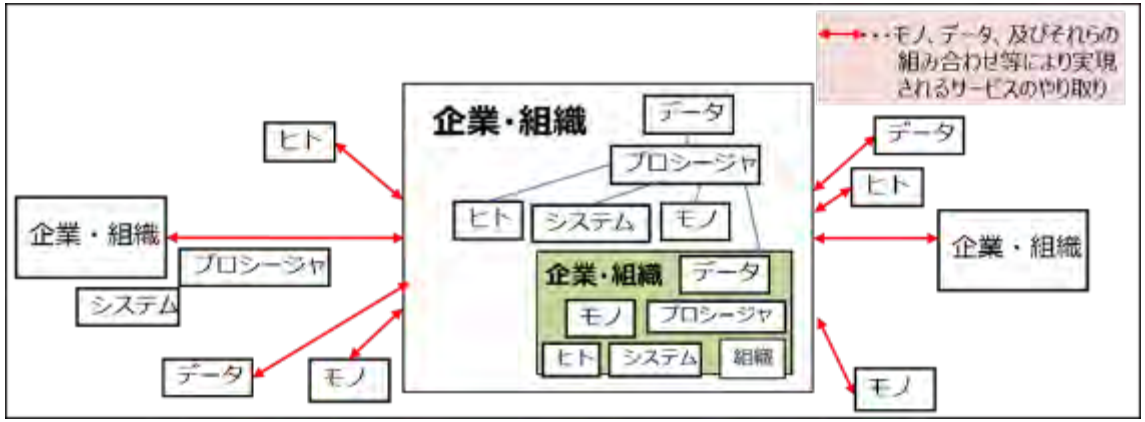
フィジカル空間とサイバー空間のつながり
【第２層】
- フィジカル・サイバー間を正確に“転写”し、機能の信頼を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり（従来型サプライチェーン）
【第１層】
- 適切なマネジメントを基盤に各主体の信頼を確保

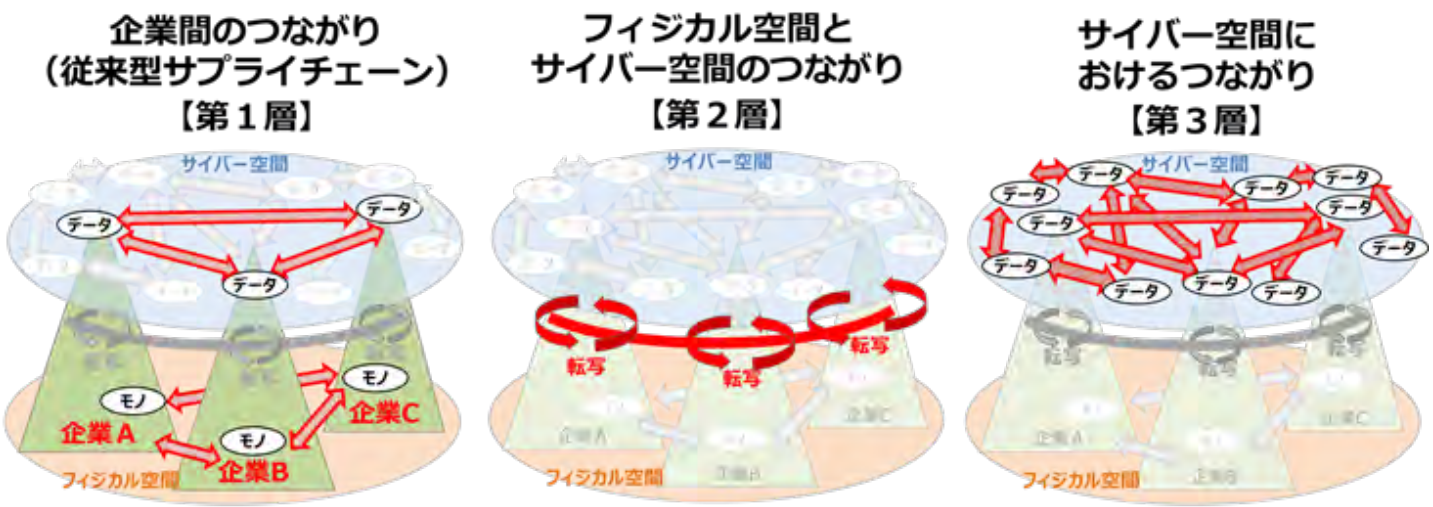


価値創造過程に関わる６つの要素と構成要素の関係

構成要素	定義
組織	価値創造過程（特に、従来型サプライチェーン）に参加する企業・団体
ヒト	組織に属する人、及び価値創造過程に直接参加する人
モノ	ハードウェア、ソフトウェア、及びそれらの部品
データ	フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するために要求される定型化された一連の活動
システム	サービスを実現するためにモノで構成される仕組み・インフラ



各層におけるセキュリティ対策の概要



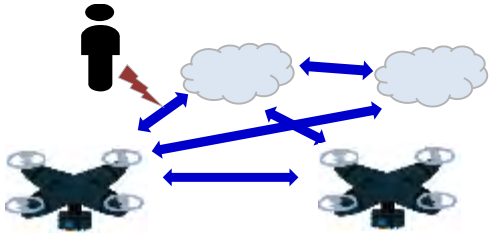
新たなサプライチェーン構造の整理			
守るべきもの	・仕様どおりの製品、サービス ・組織の信頼	・正確な転写機能 ・レジリエンス	・セキュアなデータ流通 ・サイバー上での信頼あるデータサービス
セキュリティリスクの洗い出し	・製品へのマルウェア混入 ・組織からの情報漏えい	互いに関係 ・計測データの改ざん ・制御機能への攻撃	互いに関係 ・ネットワーク上でのデータ改ざん ・偽称されたデータサービス
具体的な対策の提示（構成要素ごとに整理）	■納品されたモノの検証 ■マネジメントルールの徹底	■セキュリティバイデザイン ■セキュアなIoT機器等の導入 ■安全とセキュリティのためのシステム運用	■暗号化によるデータ保護 ■データ提供者の信頼性確認

（参考）フレームワーク活用例：リスクベース

【第３層】

機器が盗難にあい、情報が不正閲覧される。

不正アクセスにより情報が漏えいする。



サイバー空間にて送受信する情報が盗聴される。

廃棄した機器から情報が漏洩する。

【第２層】

セキュリティを考慮しない設計で、結果としてコストがかさむ。

模造品を利用することで、不正データが混入する。

機器が不正に操作される。

ウイルスに感染し、誤動作する。

廃棄した機器が悪用される。

【第１層】

セキュリティを考慮しない生産体制・管理により、被害発生のおそれが増大する。

生産記録をきちんと管理しないことにより、問題の部品の特定ができない。

管理が漏れた機器がマルウェアに感染する。

セキュリティポリシーや体制が不十分で、セキュリティ被害が拡大する。

設計 | 調達 | 製造 | 運用 | 廃棄

フレームワークにおける信頼の確保の考え方

- サイバーフィジカルシステムのセキュリティを確保するため、それぞれの構成要素についての**セキュリティの確保(信頼の創出)とその確認(信頼の証明)を繰り返し行い、信頼のチェーンを構築、維持することで、価値創造過程全体のセキュリティを実現**。

1．信頼の創出

・セキュリティ要件を満たすモノ・データ等の生成
・対象のモノ・データ等が要件を満たした形で生成されたことの確認

2．信頼の証明

・対象のモノ・データ等が正常に生成されたものであることを確認できるリスト(トラストリスト)の作成と管理
・トラストリストを参照することで対象のモノ・データ等が信頼できるものであることの確認

3．信頼のチェーンの構築と維持

・信頼の創出と証明を繰り返すことで信頼のチェーンの構築(トレーサビリティの確保)
・信頼のチェーンに対する外部からの攻撃等の検知・防御
・攻撃に対するレジリエンスの強化

産業分野ごとの検討の促進：分野別のSWGの設置

- WG1で検討する『サイバー・フィジカル・セキュリティ対策フレームワーク』を、産業分野別に順次展開し、具体的適用のためのセキュリティポリシーを検討。

（参考）ビルSWG（座長：江崎 浩 東京大学 教授）

- ビルの管理・制御システムに係る各種サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理し、ビルに関わるステークホルダーが活用できる**ガイドラインをとりまとめる**。
- オリパラに向けて、**各事業者において実施できる分野から実装**を目指す。

＜構成員＞

有識者、ビルオーナー、ゼネコン、サブコン、設計事務所、個別システム事業者（ビル管理、空調、エレベーター、ビデオ監視、電力・熱供給 等）、自治体、関係省庁 等

＜ガイドラインのとりまとめイメージ＞

- ビルシステム全体に**共通する最低限の要求**をまとめたもの＋**より詳細な方策**を示したものの二階建て構成
- ガイドラインでは、多くの事業者の取組の参考となるよう**優先順位を示した選択肢を提供**

内容項目例

・ビルに係わるサイバーセキュリティ上の脅威の現状
・ビルシステムに対して起こりえる攻撃とその影響の予測
・サイバーセキュリティ確保のための対策の概要
・対策の具体的内容
・対策実施に向けたチェックリスト

フェーズ	主な要求概要	関係するステークホルダー
設計	機器、ネットワーク、物理セキュリティへの要求	設計事務所、オーナー、ゼネコン、サブコン、ベンダー
施工／建築	機器単位、システム単位の施工プロセスへの要求	ゼネコン、サブコン、ベンダー
竣工検査	全体管理体制、管理結果、受入検査への要求	ベンダー、ゼネコン、サブコン、オーナー、設計事務所
運用・保守	管理体制への要求	オーナー、サブコン、ベンダー

＜検討スケジュールイメージ＞

- **2018年夏：ガイドライン共通編（骨子）を作成**
- 2018年度中：骨子を用いたモデル評価（2サンプル程度）とフィードバック、ガイドライン共通編の完成
- 2019年度以降：ガイドライン共通編（完成版）の本格活用開始、個別編のモデル評価とフィードバック、完成

（参考）電力SWG（座長：渡辺 研司 名古屋工業大学大学院 教授）

- 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、**官民が取り組むべき課題と方向性**について、**短期・中長期という時間軸を加味**しつつ、広く検討。
- **サイバー・フィジカル・セキュリティ対策フレームワークを踏まえ、電力分野におけるセキュリティ向上を目指す**。

＜構成員＞

有識者（大学教授、弁護士等）、電力事業者、業界団体

＜検討項目＞

- 電力制御系システムに関するセキュリティ向上策
  → **「電力制御システムセキュリティガイドライン」への提言**（サプライチェーンのリスクマネジメントや緊急時対応の強化）
  →2020年**東京オリパラへの対応を視野に、短期的に対応すべき事項と、より中長期で見て対応すべき事項を整理**して検討

- 電力自由化等に伴う多種多様なプレイヤー参入による、制御系システム周辺に拡がりつつあるサイバーセキュリティリスクへの対応策
  →**制御系システムに関連した分野・事業者におけるセキュリティ向上**のあり方を検討

- 業界全体の取組向上に資する基盤整備
  → **情報共有の更なる強化、諸外国との連携強化、人材育成基盤の強化** 等

グローバルサプライチェーンに対応するため
『サイバー・フィジカル・セキュリティ対策フレームワーク』の国際化を推進

- グローバルサプライチェーンにそのまま適用できるフレームワークとするため、国際標準（ISO27001等）や米国規格（NIST Cybersecurity Framework等）と連動。
- 国外からも積極的に意見を募るため、**英語版パブリックコメントを実施**。
- **国外の会議などでフレームワークを積極的に紹介**。今後、国際標準化についても検討。

パブリックコメント（4/27-5/28）

■ 国内23、海外10の組織・個人より300件強の意見提出あり。肯定的な意見が9割弱。

■ 海外からの主なコメント

- 各産業への「行動の呼びかけ」として有用（米国企業）
- 中小企業でも利用しやすいフレームワークとすると良い（米国産業団体）
- 国際標準や海外規格に留意して進めてほしい（欧州企業 他）

海外における周知活動

- TechGlobal (米国・ワシントンDC）4月
- 日ASEANサイバーセキュリティＷＧ（インドネシア・バリ）5月
- Securing Global Industrial Value Networks（ドイツ・ベルリン）5月
- OECD・SPDE（フランス・パリ）5月

マルチ・バイを通じた国際協調への取り組み①

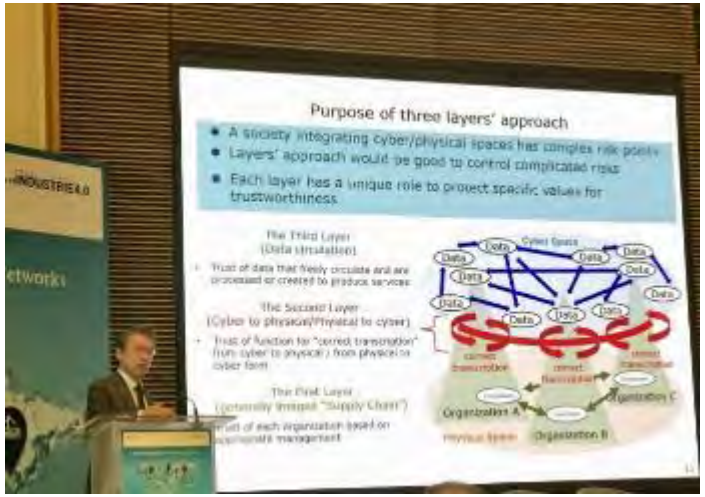
- **「サイバー・フィジカル・セキュリティ対策フレームワーク」**を軸に、各国のステークホルダーと議論、マルチの会議で紹介し、サイバー・フィジカル・セキュリティに関する共通の認識を醸成。
- **安全なサプライチェーンの実現**には関係する者の信頼性の確保について、各国と意見交換。

【ドイツ】

- **Securing Global Industrial Value Networks （2018年5月@ベルリン）**

➢ ドイツを中心とした各国の官民の関係者にむけて、Society5.0時代のサイバーセキュリティについてフレームワークや標準化活動等、日本の取組を説明。

➢ 日独連携の取組の成果として、2017年に引き続き2018年5月に産業サイバーセキュリティに関する共同ポジションペーパーを発出。カンファレンスの講演内で日独双方から披露・解説。



マルチ・バイを通じた国際協調への取り組み②

【EU・OECD】

- **<u>日EUデータエコノミー対話 政府間会合（2018年4月@東京）</u>**

➢ EUでサイバーセキュリティを所掌する通信総局（DG CONNECT）へフレームワークを紹介。
日欧は協調してセキュリティに関する国際的なルール構築に当たっていくとの認識を共有。

- **<u>OECD／CDEP（デジタル経済政策委員会）会合（2018年5月@パリ）</u>**

➢ セキュリティ・プライバシーに関する作業部会（SPDE）にてフレームワークを紹介。

マルチ・バイを通じた国際協調への取り組み③

【アメリカ】

- **TecGlobal （米国商工会議所主催）（2018年４月@ワシントンDC）**
  - 米国国土安全保障省（DHS）、アメリカ民間企業等に、現在日本で検討を進めているフレームワークについて、基本的な考え方や検討状況を共有し、お互いのサイバーセキュリティの取組を協調しながら進めていく環境を整備。

米国商工会議所のHPより引用

- **Industrial Control Systems Joint Working Group (ICSJWG)（2018年４月@アルバカーキ）**
  - DHS傘下の国家サイバーセキュリティ通信総合センター（NCCIC）が、重要インフラ防護に向けて官民関係者の連携を深めるべく、関係者で情報共有を図る会議において「サイバー・フィジカル・セキュリティ対策フレームワーク」を初めとする経産省のサイバーセキュリティ政策について紹介。

- **2nd Global Cyber Dialogue（米国商工会議所主催）（2018年10月@ワシントンDC）**
  - 米（DHS、NIST、国務省、商務省）、英、仏、EC等における影響力のある政策担当者や代表的な民間企業と、サイバーセキュリティ政策について議論。

マルチ・バイを通じた国際協調への取り組み④

【ASEAN】

- **第2回日・ASEANサイバーセキュリティWG（2018年５月@インドネシア・バリ）**

➢ 情報セキュリティ分野において、我が国とASEAN諸国との国際的な連携・取組を強化することを目指す会議において、日本のサプライチェーンセキュリティの取組、フレームワークについて紹介。域内の情報セキュリティ水準向上のための意識啓発を実施。

➢ 日米共同演習への参加を呼びかけ。

マルチ・バイを通じた国際協調への取り組み⑤

【APEC】

- **APEC TEL57（第57回電気通信・情報作業部会）（2018年6月@パプアニューギニア・ポートモレスビー）**
  - Security and Prosperity Steering Group (SPSG)において中国のサイバーセキュリティ関連組織であるCNCERT/CCが主催した「IoT Security Workshop」で、「サイバー・フィジカル・セキュリティ対策フレームワーク」について紹介。
  - 華為技術（Huawei）、カスペルスキー研究所、UL等の民間企業やIntermet Society(ISOC)、Asia-Pacific Network Information Centre（APNIC）等の国際団体も参加。

- **APEC TEL58（第58回電気通信・情報作業部会）（2018年10月@台湾・台北）**
  - シンガポールが主催したWS “Digital Economy: Strategies and Measurements”で、「Japan’s Initiative and measurements towards “Connected Industries”」のテーマで発表。「サイバー・フィジカル・セキュリティ対策フレームワーク」について紹介。
  - Intermet Society(ISOC)、Asia-Pacific Network Information Centre（APNIC）等の国際団体も参加。

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見直し方針

- 国内外からのパブリックコメントの意見を踏まえ「サイバー・フィジカル・セキュリティ対策フレームワーク」（案）の記載・構成を以下の観点から見直す。

フレームワークの考え方の明確化

- 目的、適用範囲、対象、想定する読者等を冒頭で明示
- 価値創造過程の定義や信頼の確保の考え方の記載位置を変更（前方に移動）
- 6つの構成要素で整理する根拠、目的を追記
- マルチステークホルダーの考え方を明記

国際規格等との対応関係の整理

セキュリティ対策例のレベル分け

国際規格等との対応関係の整理

- グローバルハーモナイゼーションの観点から、各対策項目と、既存の海外主要規格等との対応関係を明確にする。
- 特に、**米国政府が国際標準化を推進する『NIST Cybersecurity Framework』の機能分類と対比**した上で、**対策項目の整序や統合を含む再構成を実施**する。

対応する海外主要規格等の記載（案）

- 『サイバー・フィジカル・セキュリティ対策フレームワーク』の各対策項目に、海外主要規格等の対応するサブカテゴリーを記載
- 海外主要規格等のサブカテゴリーを基準として、対応する各対策項目を整理

NIST CSFの機能分類との対比（案）

- NIST CSFの5つの機能分類にあわせて、本フレームワークの対策項目をマッピング
- 各層内の対策項目を分類するカテゴリーを追加し、対策項目を整序

	識別(ID)	防御(PR)	検知(DE)	対応(RS)	復旧(RC)
第1層	L1.001 L1.002 L1.003 ⋮	L1.005 L1.006 L1.012 ⋮	L1.003 L1.004 L1.010 ⋮	L1.003 L1.008 L1.013 ⋮	L1.002 L1.008 L1.009
第2層	L2.001 L2.003 L2.010 ⋮	L2.002 L2.013 L2.014 ⋮	L2.007 L2.008 L2.015 ⋮	L2.006 L2.009 L2.018 ⋮	(第1層の上記項目を参照)
第3層	L3.001 L3.008 L3.022	L3.002 L3.011 L3.017 ⋮	L3.001 L3.006 L3.015 ⋮	L3.004 L3.008 L3.015 ⋮	(第1層の上記項目を参照)

セキュリティ対策例のレベル分け

- 「各事業者がオペレーションレベルで活用できる」「セキュリティ対策の必要性とコストの関係を把握できるようにする」ことを目標として、**対策による効果やコスト等を考慮しながら、具体的な対策例を示す。**
- なお、産業分野ごとに守るべきものやリスクは異なる場合があるため、詳細な検討については各SWGにおいて検討する。

対策例の記載イメージ

現状の記載例

…

■構成要素毎の対策例

〇組織

- IoT機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。
- IoT機器やソフトウェアのサプライヤーを特定し、そのサプライヤーから正規品を導入する。

〇ヒト

…

各対策例に、効果やコスト等による重み付けがなされていない

対策例のレベル分け

分類後のイメージ（案）

…

■構成要素毎の対策例

〇組織

【レベル３】

- 製造システムの仕様、設計、開発、実装及び変更にセキュリティエンジニアリングの原則を適用する。開発過程におけるバグや脆弱性の修正課程が追跡可能な状態を維持する。

【レベル１】

- システム開発時にセキュリティの考慮事項を明確に含むライフサイクルが考慮されており、外部コンポーネントの導入時にはセキュリテ

…

〇ヒト

…

【レベル分けの例】
レベル３：高いセキュリティ水準、国際規格等（ISO/IEC27002, SP800-171等）への対応
レベル２　　〃
レベル１：セキュリティ対策として最低減求めたい事項

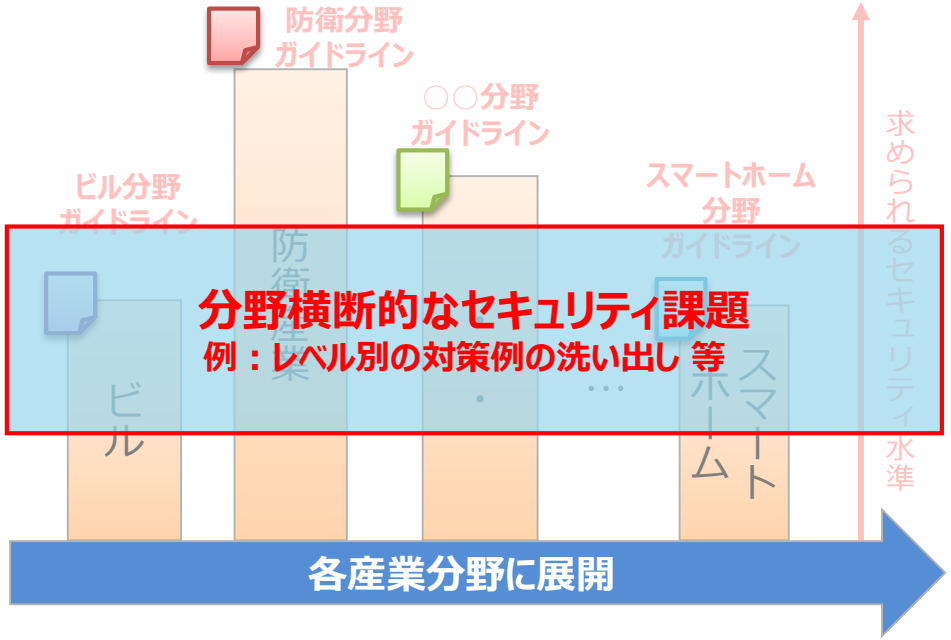
分野を横断して共通するセキュリティ課題への対応

- サイバー空間とフィジカル空間が高度に融合する「Society5.0」では、産業分野を横断した企業間のつながりやデータの流通、サービスの提供がなされることも事実。
- 産業分野別の課題や対策等を相互に持ち寄り、**分野を横断して共通するセキュリティ課題の洗い出しやその対策について検討するSWGを設置**。
- 検討結果は、**産業分野別の検討にフィードバックする**とともに、**「サイバー・フィジカル・セキュリティ対策フレームワーク」へ反映する等の取組を進める**。

サイバー・フィジカル・セキュリティ対策フレームワーク

三層別アプローチ	必要な対策のポイント
1. 企業間のつながり (主体の信頼)	セキュリティポリシーの策定、体制の整備
	事業継続計画又はコンティンジェンシープランへの反映
	…
2. フィジカル空間とサイバー空間のつながり (機能の信頼)	セキュリティ対策が施されたIoT機器の導入
	セキュリティバイデザインの実践
	…
3. サイバー空間におけるつながり (データの信頼)	信頼できるサービスサプライヤーの選定
	サイバー空間における接続相手の認証
	…

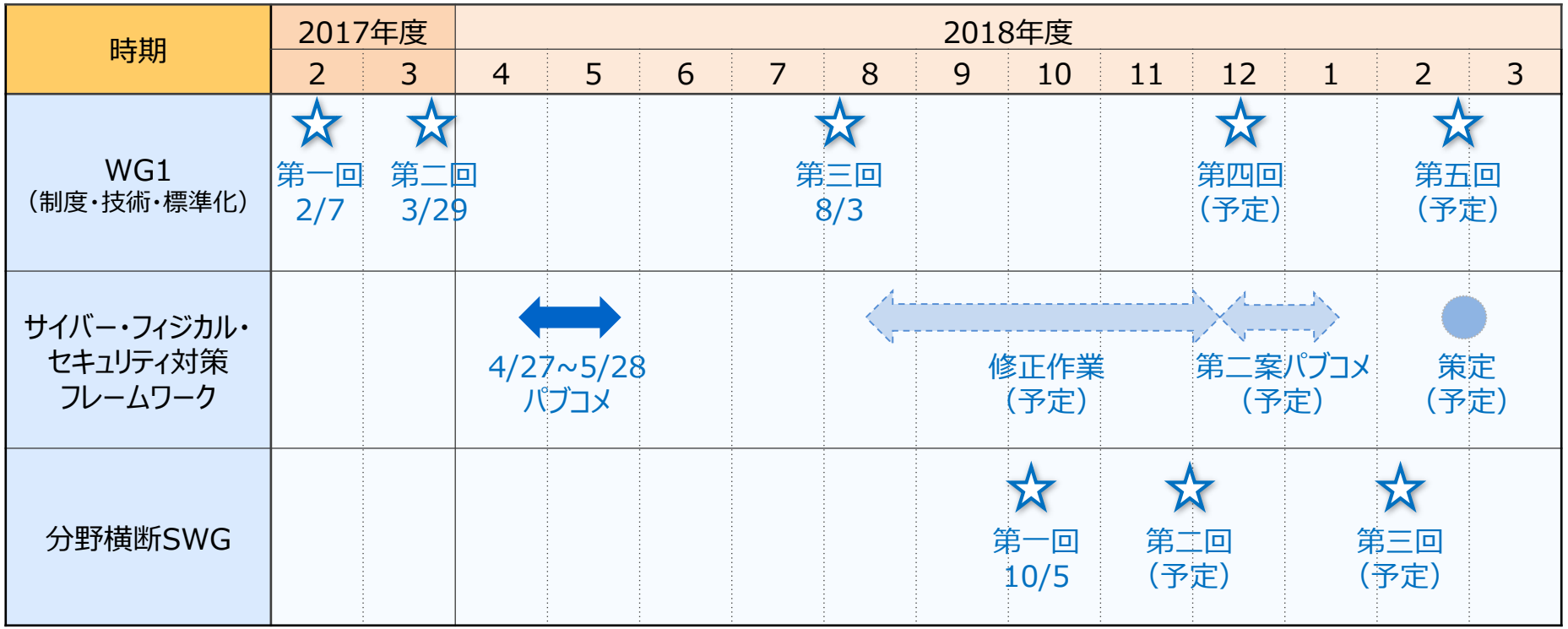
産業分野別のサイバー・フィジカル・セキュリティ対策



今後のスケジュール（案）

- **『サイバー・フィジカル・セキュリティ対策フレームワーク』（第二案）**に向けた修正を実施。第二案についてもパブリック・コメントを実施し、国内外から広く意見を募る。
- 並行して、分野横断SWGを設置し、分野横断的なセキュリティ対策の議論を進める。

今後のスケジュールのイメージ



１．はじめに
　～サイバー攻撃の脅威レベルの向上と海外の動き

２．産学官の検討体制の構築
　～産業サイバーセキュリティ研究会

３．「Society5.0」において必要なセキュリティ対策
　～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

４．海外のサプライチェーンの強化

５．サイバーセキュリティ対策の基盤整備
　～経営者の意識喚起、人材育成

６．サイバーセキュリティビジネスの創出
　～エコシステムの構築

サプライチェーンを共有するASEANへのアウトリーチの強化

- 多くの日本企業がサプライチェーンを共有するASEAN各国等のサイバーセキュリティ対応能力の向上のため、**米国国土安全保障省（DHS）と連携**し、**ASEAN等向けの日米共同演習を今年初めて開催**。

■**開催日時**：2018年9月10～14日(以降毎年9月に開催)

■**開催場所**：東京

■**内　　容**：重要インフラにおける制御システムのセキュリティに関する5日間の講義・演習

■**参 加 者**：IPA産業サイバーセキュリティセンター（ICSCoE）中核人材育成プログラム 83名
ASEAN10ヶ国、韓、台、印、豪、NZ 36名
DHS/NCCIC 講師5名　ほか

■**開講挨拶**：武藤容治　前経済産業副大臣
ウィリアム・F・ハガティ 駐日米国大使
富田達夫 IPA理事長

<日米以外の参加国>

武藤前副大臣ご挨拶（フジTVより）

ハガティ大使ご挨拶（大使のTwitterより）

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。

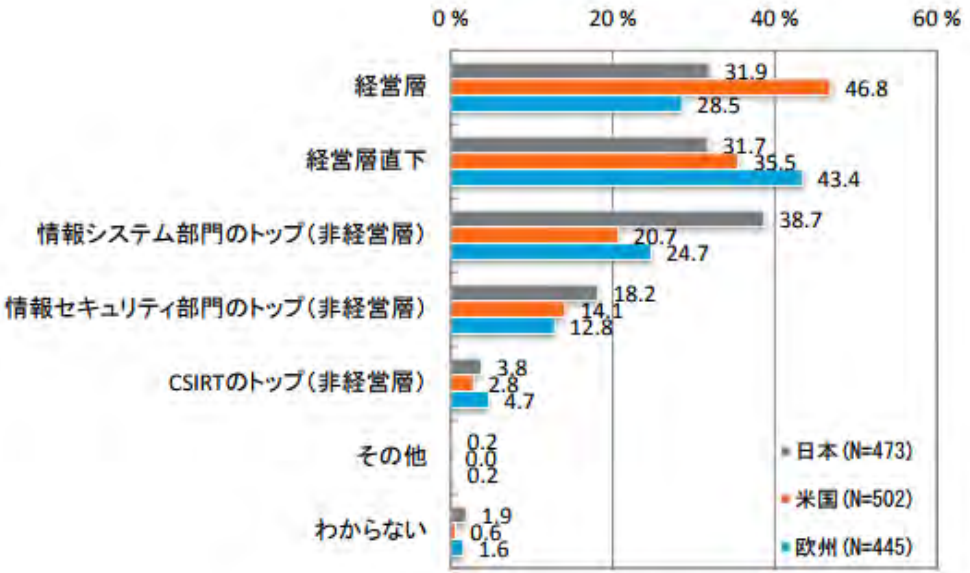


図 5.6-3　CISO 等の組織内の位置づけ

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

①経営層向け：
経営者にサイバーセキュリティ経営を促す仕組み『３STEPアプローチ』

1st Step

サイバーセキュリティ経営の在り方の明確化

- **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を求める仕組みの構築

- **コーポレート・ガバナンス・システム（CGS)に関するガイドラインのとりまとめに向け、サイバーセキュリティを位置付け**
- **『取締役会実効性評価』の項目にサイバーリスクを組み込むことを促進**
- サイバーセキュリティが経営リスクであることの投資家に対する啓発

3rd Step

市場（投資家）に対するサイバーセキュリティ経営の可視化

- 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

平成27年12月28日策定
平成28年12月8日改訂（Ver.1.1）
平成29年11月16日改訂（Ver2.0）

- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドラインを公表

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

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

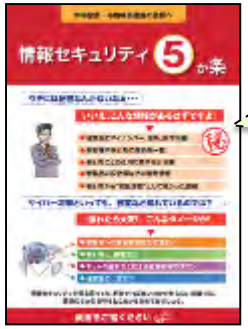
セキュリティ対策自己宣言「SECURITY ACTION」

- 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

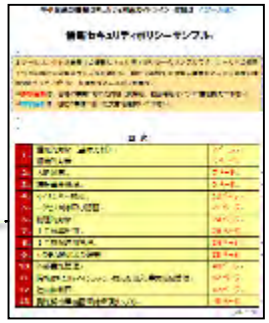
★★ 二つ星

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/

②現場の実務者向け：
サイバーセキュリティ対策の導入を促す対策事例集と可視化ツールの作成

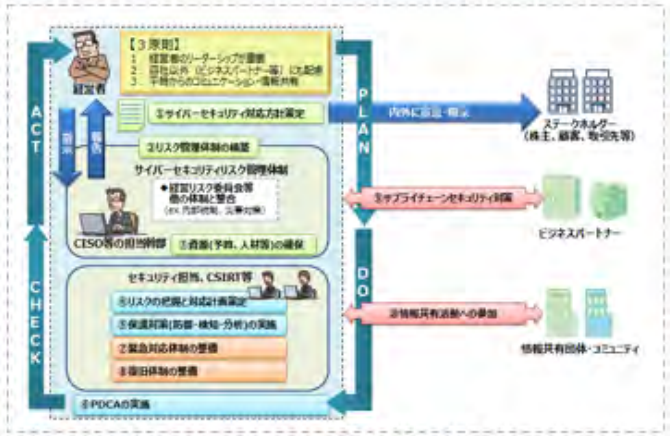
- 企業現場での対策導入を促すべく、**具体的な対策の参考となる『対策事例集』**と**自社の状況（成熟度）を把握するための『可視化ツール』**の整備に着手。
- ツール整備・活用推進のため、**『サイバーセキュリティ経営プラクティス検討会』を発足**。

サイバーセキュリティ経営プラクティス検討会(本年7月設置)

(事務局：IPA、経産省)

損保会社 | 産業横断サイバーセキュリティ人材育成検討会 | JUAS | 日本商工会議所

「対策事例集」の作成



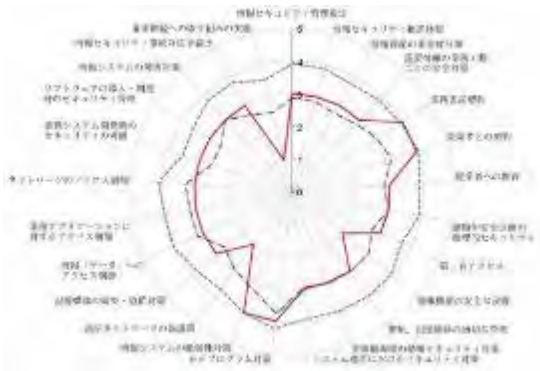
サイバーセキュリティ経営ガイドライン

連携 業界団体（ユーザ企業）

作成

重要１０項目ごとのプラクティス

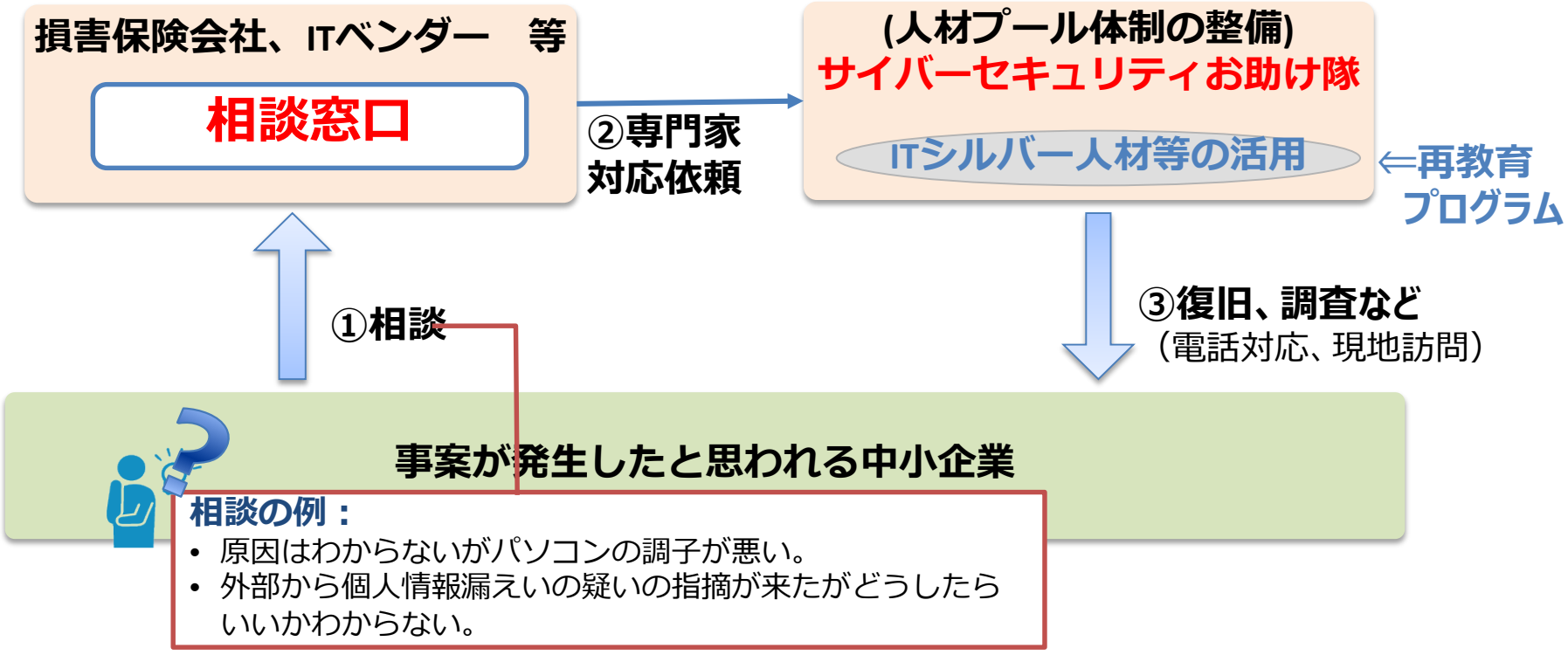
『可視化ツール』のイメージ (米国NPOとも協力)



③中小企業向け：
サイバー保険等と連携して中小企業を支援する『サイバーセキュリティお助け隊』の創設

- 24時間相談窓口などの体制を持つ損保会社等と連携して、中小企業のサイバーセキュリティに関するトラブル対応を支援する**『サイバーセキュリティお助け隊』を創設**。
- ITに従事してきたシルバー人材の再教育などを通じて人的リソースを確保。

サイバーセキュリティ保険等と連携した『サイバーセキュリティお助け隊』のイメージ



１．はじめに
　～サイバー攻撃の脅威レベルの向上と海外の動き
２．産学官の検討体制の構築
　～産業サイバーセキュリティ研究会
３．「Society5.0」において必要なセキュリティ対策
　～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
４．海外のサプライチェーンの強化

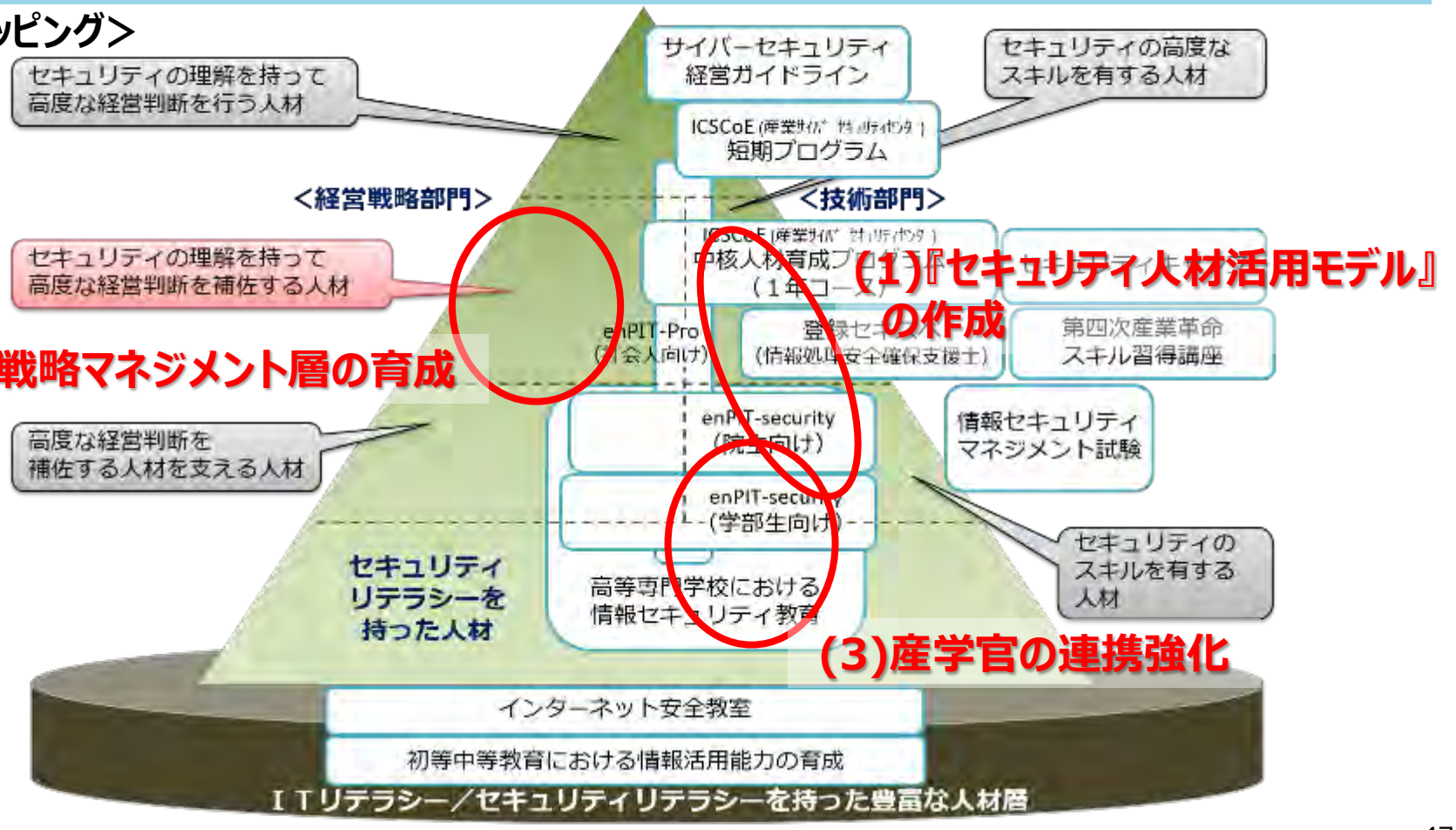
５．サイバーセキュリティ対策の基盤整備
　～経営者の意識喚起、人材育成
　①経営
　②人材

６．サイバーセキュリティビジネスの創出
　～エコシステムの構築

サイバーセキュリティ人材育成・活躍促進パッケージの全体像

- ユーザー企業において必要となる**セキュリティ人材の定義、評価指標が不明確**。
- **「セキュリティの理解を持って高度な経営判断を補佐する人材」の育成が不十分**。
- 教育プログラム策定への貢献など、**産業界の教育への取組の強化が期待される**。

＜政策マッピング＞



サイバーセキュリティ経営を進める戦略マネジメント層の育成

- セキュリティの理解を持って高度な経営判断を補佐する人材『**戦略マネジメント層**』を育成するために、**産学官連携やICSCoEを拠点としたプログラムを開始**。

サイバーセキュリティ経営を含む『次世代経営人材の育成プログラム』の開始 ＜産学官連携＞

- 次世代の経営人材を集中的に育成するプログラム**(2018年9月開講)**の中で、**経営視点で見たサイバーセキュリティ課題の講義も実施**予定。

CISO人材の育成プログラムの開始 ＜IPA産業サイバーセキュリティセンター＞

- **CISOや戦略マネジメント機能を担う人材に必要なセキュリティ対策に関するトレーニング**を行うプログラムを**2018年11月から開始**。

対象人材像

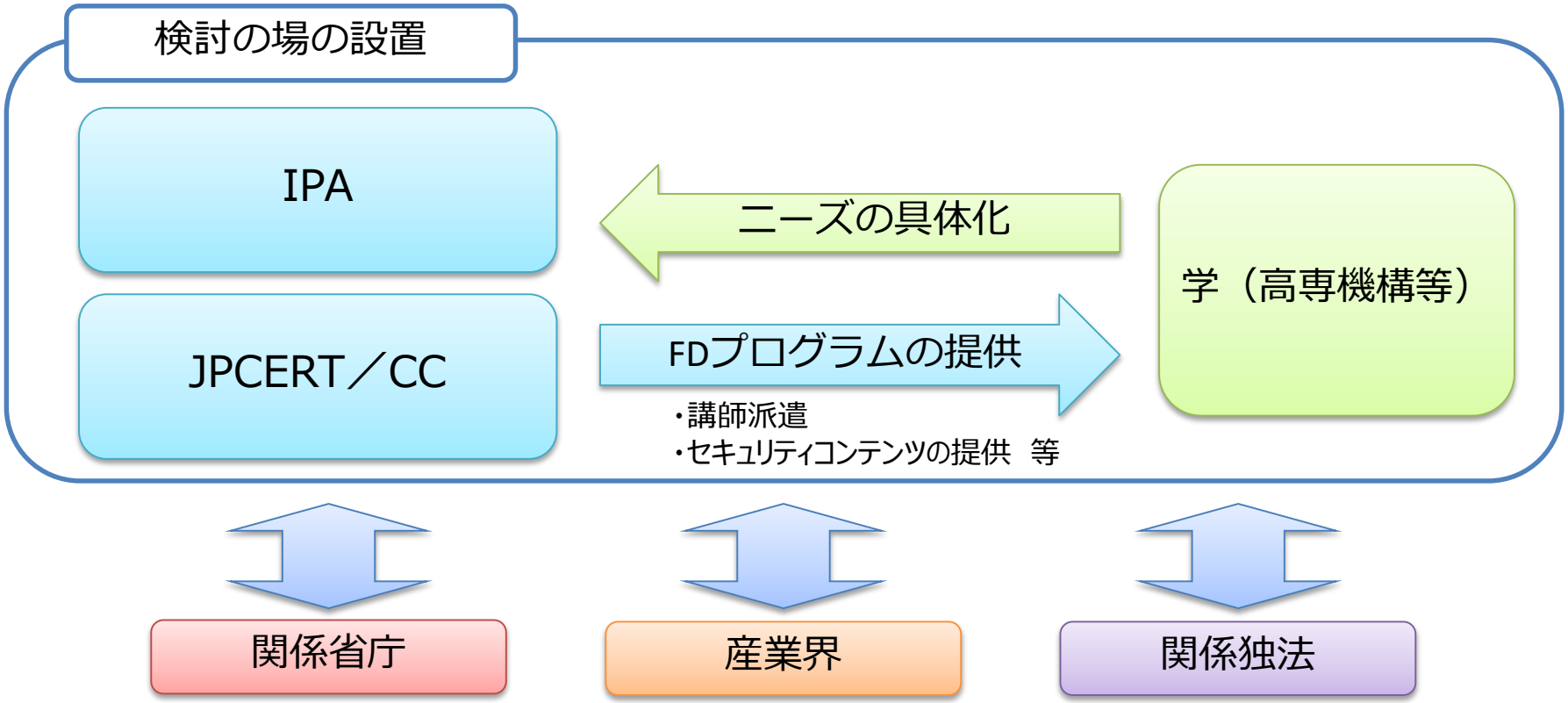
- **次世代の経営を担うことを期待**されている**戦略企画層の方**
- **現在CISOやその補佐を務めている方や、戦略企画層の方**

カリキュラム・期間

- **デジタル経営の講義を、4か月程度かけて実施。**
- その中で、**サイバーセキュリティの必要性・位置づけ**についても講義を実施。
- **サイバーセキュリティのリスク管理や、インシデント対応等**のプログラムを、**2か月の間集中して実施。**
- 「中核人材育成プログラム」の受講者80名に、**戦略マネジメント層20名を加え、合計100名程度を対象として開始予定。**

産学官連携の促進　「学」向けのトレーニングの提供

- セキュリティ教育の機会を提供するため、教える側の質的向上・量的拡充が必要。**「学」の教員向けにIPA、JPCERT/CCにより、FD（Faculty Development）等の研修機会を提供**。
- 当初は、IPA、JPCERT/CC、高専機構等の「学」による検討の場を設置し、今後、産業界、関係省庁、関係独法等の参画を求めながら課題の洗い出し・解決を図る。



（参考）産業サイバーセキュリティセンター（ICSCoE）

- 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
- 第１期（平成29年7月～平成30年6月）では、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った。
- 2017年9月、**米国・国土安全保障省（DHS）及びNCCIC（旧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

模擬プラント
全景

機械製造設備プラント

発電模擬プラント

（参考）セキュリティ・キャンプ

- 複雑かつ高度化しているサイバー攻撃に適切に対応するため、**若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラス人材を創出**することが必要。
- 民間企業と一丸となって、若年層(22歳以下)セキュリティ人材の育成合宿を開催し、**倫理面も含めたセキュリティ技術と、最新ノウハウを、第一線の技術者から伝授する場を創出**。これまでの**セキュリティ・キャンプ全国大会(2004年より開始,計15回開催)**については累計で**748名**が受講。
- 更に、地方における**セキュリティ・キャンプ地方大会**(2013年より開始)も併せて実施することにより、セキュリティ人材の裾野と輪を広げている。

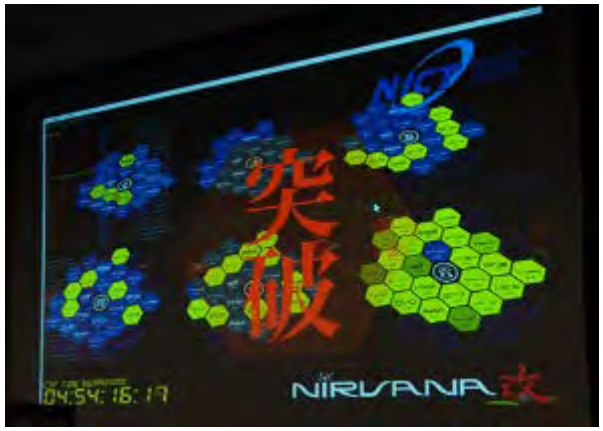
セキュリティ・キャンプ卒業生の例

清水郁実さん
2015年修了（当時15歳）

毎年夏に、米国ラスベガスで開催される世界最大のハッカーの祭典「DEFCON(デフコン)」その目玉イベントのハッカー大会において、３位入賞を果たした。プログラミングや暗号解読をはじめとしたサイバーセキュリティ分野の技術力と知識を武器に、大人達に交じって勝ち抜き、セキュリティ・キャンプ修了生が有する高い技術力を発揮した。

（参考）SECCON　（セキュリティ・コンテスト）について

- SECCON（SECurity CONtest）とは、2012年度から開催されている、実験ネットワーク内で行う疑似的な攻防戦などを通じてセキュリティ技術を競うコンテスト。
- 2011年度に経済産業省でセキュリティコンテストの実証事業を行い、同事業の成果を引継ぎ、2012年度からJNSA（NPO法人日本ネットワークセキュリティ協会）が実施している。2018年度で７回目。
- 2016年には世界99カ国、4,349人、2017年には世界102カ国、4,347人が予選参加する日本最大の国際競技大会に成長。



■SECCON2016
１位　CyKor(韓国)
２位　PwnPineappleApplePwn(韓国)
３位　eee（中国）
４位　２１７（台湾）
５位　binja（日本）

■SECCON2017
１位　CyKor(韓国)
２位　PPP(韓国)
３位　dododododo（日本）
４位　HITCON（台湾）
５位　２１７（日本）

画像は@ITから引用　http://www.atmarkit.co.jp/ait/articles/1702/07/news049.html

（参考）情報処理安全確保支援士（登録セキスペ）制度

- 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。
- 平成30年10月1日時点での登録人数は17,000名を超過する見込み。

◆ 政府機関や企業等のサイバーセキュリティ対策を強化するため、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。**

◆ 技術進歩等が早いサイバーセキュリティ分野においては、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。**

◆ 民間企業等が安心して人材を活用できるようにするには、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。**

（参考）第四次産業革命スキル習得講座認定制度

- 社会人向けの**ＩＴ・データ分野の専門性・実践性の高い教育訓練講座を経済産業大臣が認定**する「第四次産業革命スキル習得講座認定制度」を創設。
- 2018年1月にAI・データサイエンス分野を含む**23講座（16事業者）を初回認定し、４月から開講中。**また、**今年7月**には**21講座（15事業者）を認定し、10月以降に開講。**

※ 経済産業大臣が認定した教育訓練講座のうち、厚生労働省が定める一定の要件を満たし、厚生労働大臣の指定を受けたものは、「専門実践教育訓練給付」の対象となる。

＜認定対象分野＞

①ＩＴ分野

⇒ **ＡＩ**、**データサイエンス**、ＩｏＴ、クラウド 【将来成長が見込める新技術・システムの習得】
（デザイン思考、アジャイル開発等の新たな開発手法との組み合わせを含む）

⇒ 高度なセキュリティ、ネットワーク 【必須スキルの習得】

② IT利活用分野（今後、拡大の予定）

⇒ 自動車分野のモデルベース開発　等 【(製造業向け等の)ITによる高度化対応】

Reスキル

初回認定講座事業者と世耕大臣との意見交換

講座の特徴

- ✓ 民間事業者による資格とヒモ付かない講座、120時間以下（30時間以上）の講座でも対象
- ✓ 実習、実技、演習又は発表などが含まれる実践的な講座がカリキュラムの半分以上
- ✓ 審査、試験等により訓練の成果を評価
- ✓ 社会人が受けやすい工夫（e-ラーニング等）

１．はじめに
～サイバー攻撃の脅威レベルの向上と海外の動き

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．「Society5.0」において必要なセキュリティ対策
～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

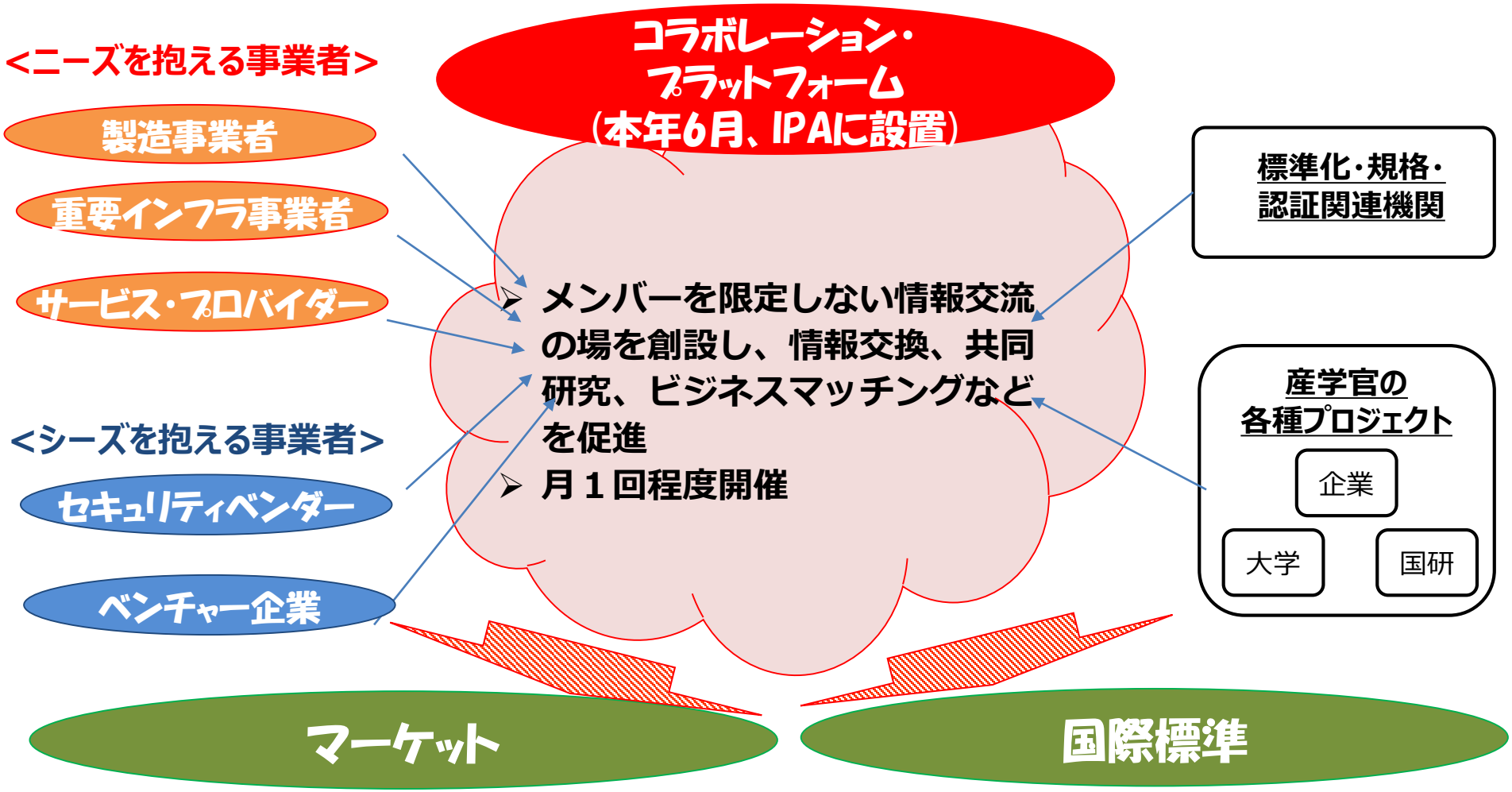
４．海外のサプライチェーンの強化

５．サイバーセキュリティ対策の基盤整備
～経営者の意識喚起、人材育成

６．サイバーセキュリティビジネスの創出
～エコシステムの構築

ニーズとシーズをマッチングする『コラボレーション・プラットフォーム』の設置

- 各WGの活動などを通じて顕在化したニーズとシーズをマッチングする“場”となる**『コラボレーション・プラットフォーム』をIPAに設置し、6月から活動を開始**。



コラボレーション・プラットフォームの開催状況

- 各回、予定定員以上の申込みがあり、参加者からは政府との意見交換、最新動向の情報収集、人脈形成等、様々な視点で有益との声。

	日にち	参加人数(*)	主なテーマ
第一回	6月13日	179名（99名）	経済産業省の政策動向、パネルディスカッション（サイバーセキュリティビジネス、サプライチェーンセキュリティ）
第二回	7月23日	104名（74名）	IoTの発展に潜むリスクと対策、グループディスカッション（サプライチェーン、人材、つながる世界の脅威と対策）
第三回	9月3日	132名（69名）	経済産業省の新政策、企業の取り組み事例（資生堂）、グループディスカッション（業界別セキュリティ対策、セキュリティ検証基盤、サイバーセキュリティ経営）
第四回	**10月16日**	**151名（56名）**	**中小企業におけるサイバーセキュリティリスク、ウイルス感染デモ、中小企業向けサイバーセキュリティ対策**

(*)括弧内の人数はコラボレーション・プラットフォーム後に開催した情報交換会の出席者数


富田理事長(IPA)ご挨拶


三角審議官(経済産業省)ご挨拶


パネルディスカッション(第一回)


グループディスカッション(第二回)

日本特有のセキュリティ要求に応えた製品・サービスの活用を進める『実戦的サイバーセキュリティ検証基盤』の構築

- 日本のセキュリティニーズに応じた日本発の**サイバーセキュリティ製品の有効性等を実機を通じて検証するための『実戦的サイバーセキュリティ検証基盤』**を構築。

実戦的サイバーセキュリティ検証基盤の全体像

1．セキュリティ製品の有効性検証 ＜性能評価＞

＜イメージ＞

・検証機関が、**セキュリティ製品の有効性を検証し、お墨付きを与えることで、マーケットインを促進。**

2．実環境における試行検証 ＜信頼性評価＞

＜イメージ＞

・ベンチャー等が、**製品の信頼性等を検証するために、製品を民間事業者等へ提供し、実績を作る。**

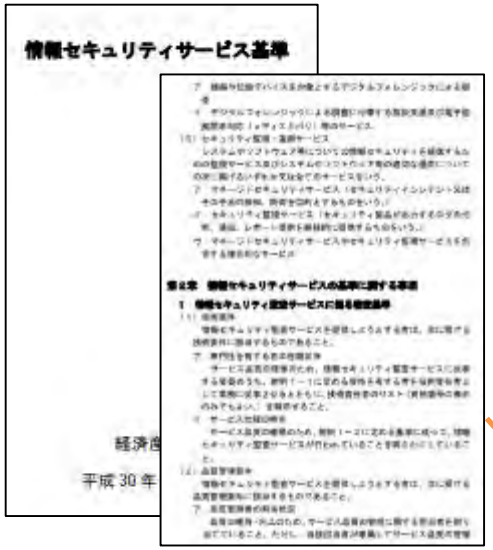
3．ホワイトハッカーの実攻撃検証 ＜ハイレベルなリスク評価＞

＜イメージ＞

・**ホワイトハッカーによる自由な攻撃**を通じて、**実際の制御系システムのセキュリティを検証。**

情報セキュリティサービス基準等の策定

- 経済産業省にて、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を策定（平成30年2月28日）。
- IPAより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。



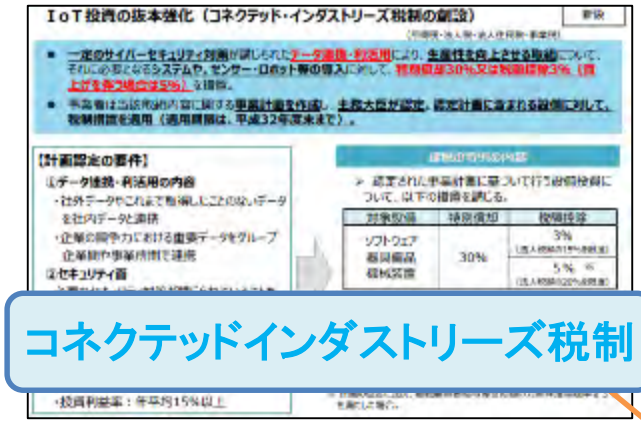
情報セキュリティサービス基準

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）

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措置として、政府調達での活用、税制・補助金における要件化を実施。

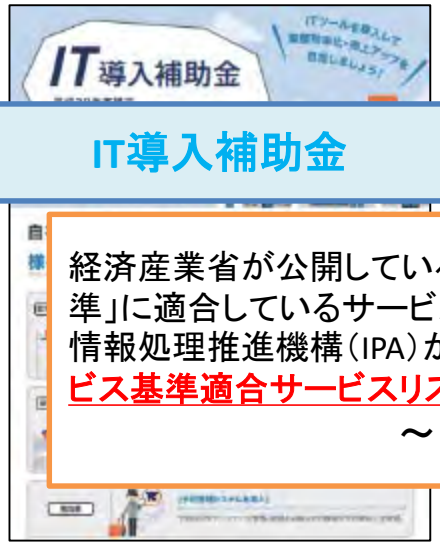


コネクテッドインダストリーズ税制

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。



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

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