経済産業省

資料4

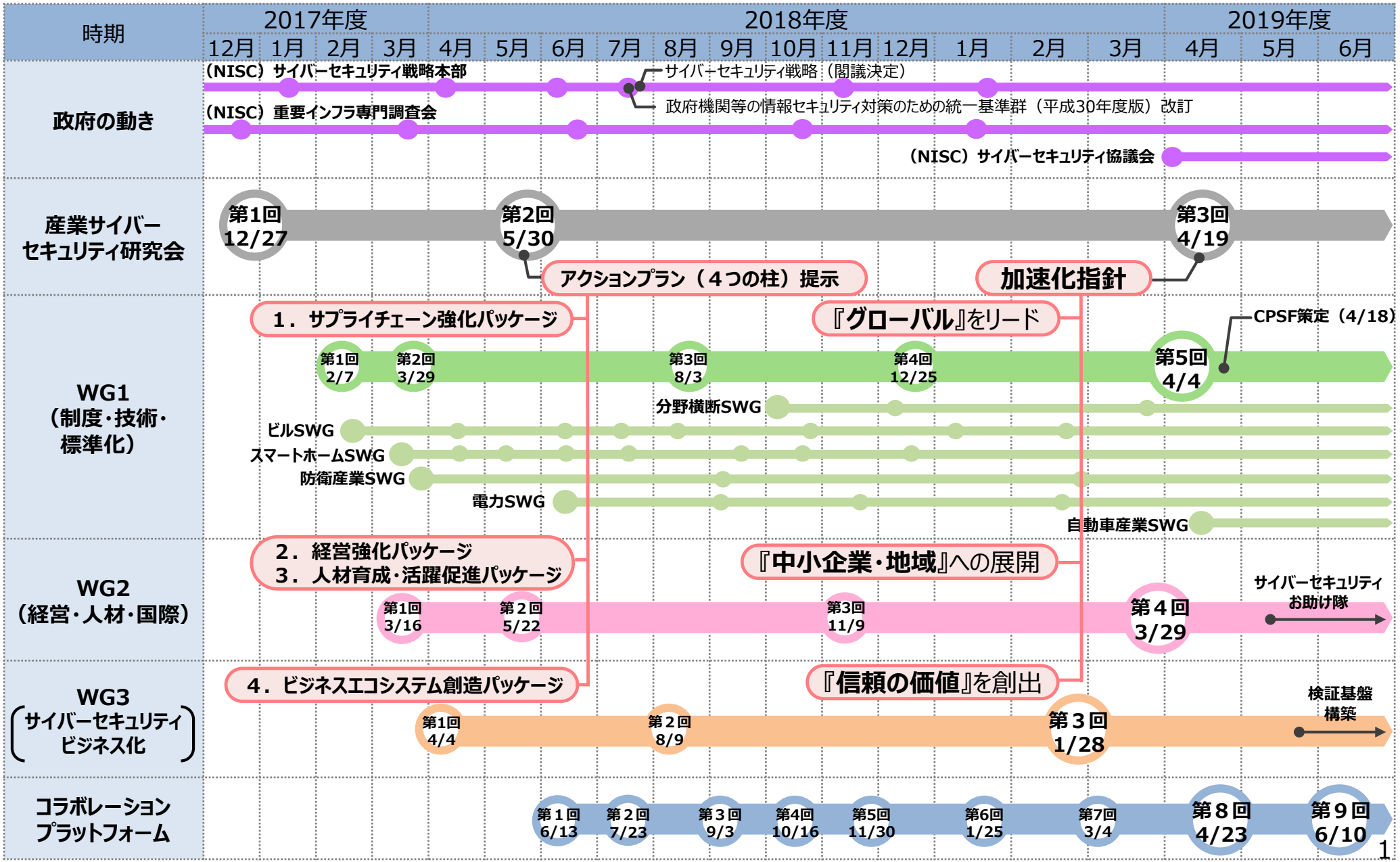
産業サイバーセキュリティの加速化指針
~アクションプランの深化・拡大~

2019年4月19日

経済産業省

商務情報政策局

産業サイバーセキュリティ研究会関連の動き



昨年5月に提示した、4つの政策パッケージから成る「アクションプラン」の取組は大きく前進。

1．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

・**サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）**策定（2019年4月18日）
・ASEAN等に向け米国DHSと連携した**日米共同演習を東京で初開催**（2018年9月）
・産総研に**サイバーフィジカルセキュリティ研究センター**を設置（2018年11月）

2．サイバーセキュリティ経営強化パッケージ

・**グループ経営におけるコーポレートガバナンスの指針（案）に位置づけ**（2019年４月）
・**サイバーセキュリティ経営プラクティス集**の公表（2019年3月25日）
・**サイバーセキュリティお助け隊**の地域実証事業を開始（2019年3月26日公募開始）

3．サイバーセキュリティ人材育成・活躍促進パッケージ

・**戦略マネジメント層向け講習**開始（一橋大学、ICSCoE）（2018年秋～）
・**高専機構との連携開始**　JPCERT/CCによる講師派遣（2018年11月15日）

4．セキュリティビジネスエコシステム創造パッケージ

・官民の意見交換の場となる**コラボレーション・プラットフォーム**を開催（これまで計7回）
・セキュリティビジネスの信頼性可視化のための**審査登録制度**開始（2018年7月）

アクションプランを中心とした取組を更に加速していくため、以下の3つの視点から重点施策を強化する。

１．『グローバル』をリードする

－G20等を視野に、サイバーセキュリティの取組をリードする

２．『信頼の価値』を創出する~Checked by Japan~

－「検証」を信頼につなげ、ビジネスにする（Proved by Japan）

３．『中小企業・地域』まで展開する

－社会全体、中小企業・地域までサイバーセキュリティを浸透させる

1．『グローバル』をリードする

- 本年6月に大阪で開催されるG20首脳会合に先立ち、**2019年3月15日にB20東京サミットの共同宣言において、サイバーセキュリティの枠組み構築が提言**された。
- G20に向けて、サプライチェーン全体のサイバーセキュリティ対策を確保ための『**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、デジタル革新へ向けたグローバルな動きをリード**していく。

B20 東京サミット共同提言（関連部分抜粋）

II. Society 5.0を通じたSDGs実現に向けた政策提言

1. **すべての人々のためのデジタル革新**

(1) データ活用のための政策枠組みの整備

A) **次世代データ・ガバナンス枠組みの確立**

- **リスクに基づくセキュリティとプライバシー保護の基準について、法域を越えた国際的な相互運用性を推進することによって、各国のプライバシーやデータ保護、知的財産権に関する法的枠組みを尊重しつつ、国境を越えたデータ、情報、アイデア、知識の自由な流通を確保**

(2) **サイバーセキュリティ分野の国際協力の推進**

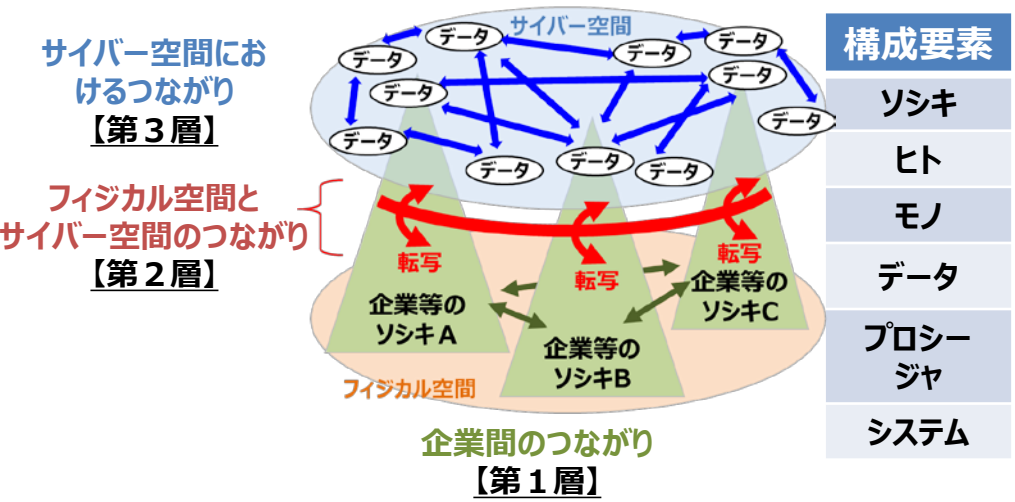
- イノベーションを阻害せず、企業に不要な負担も課さない規制的アプローチによって補完された、**リスクに基づく自主的なサイバー・セキュリティ枠組みの採用**
- **グローバルなサプライチェーン全体のICTリスクを管理する、一貫性のある、または相互運用可能な枠組みの開発・運用。**
  自主的なグローバル・セキュリティ基準（例：ISO基準等）の利用を通じた相互運用可能なサイバー・セキュリティ対策の実施の支援

グローバルをリードするための指針となる

『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）』の策定・公表

- 2019年4月18日、**『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver1.0』を策定・公表。**
- 2度にわたる英文パブコメに対して**海外からも多数のコメントが寄せられ、国際的認知も進展。**
- **CPSFで示した『3層構造モデル』、『リスクベースアプローチ』、『マルチステークホルダーアプローチ』**に対する期待が大きい。

CPSFが示した『3層構造』、『6つの構成要素』



CPSFにおけるリスク管理の考え方

機能（守るべきもの） ⇒ セキュリティインシデント ⇒ リスク源（構成要素ごとに整理） ⇒ 対策要件

第2回パブリックコメント（英語表記含む）の結果

期間　：本年1月9日～2月28日
意見数：**国内27、海外13（米国7、欧州6）**から、**約500件**

＜主な意見＞

- CPSFの**3層構造モデル、リスクベースアプローチ、マルチステークホルダーアプローチ**等に対する**肯定的な意見。**
- データ保護、ソフトウェアセキュリティ等、**CPSFのより具体的な活用方法を求める**意見。

CPSFも活用し、データ流通を加速する
データフリーフローwithトラスト（DFFT）を我が国から世界へ発信

- 依然として組織・企業・国境内に抱え込まれている**価値の高いデータや、慎重な扱いを求められるデータの流通を促し、真にデータ連携による新たな付加価値を生み出す社会を目指す。**
- **データ主導による「新たな付加価値」を生み出すためのコンセプトとして、DFFTを世界へ発信。**
- **CPSFの国際化等で、DFFTの基盤を整備。**

Trustを基盤とすることで
より多くのデータが流通

Data Free Flow

従前からサイバー空間で
流通しているデータ

＜現状＞

Data Free Flow with Trust (DFFT)

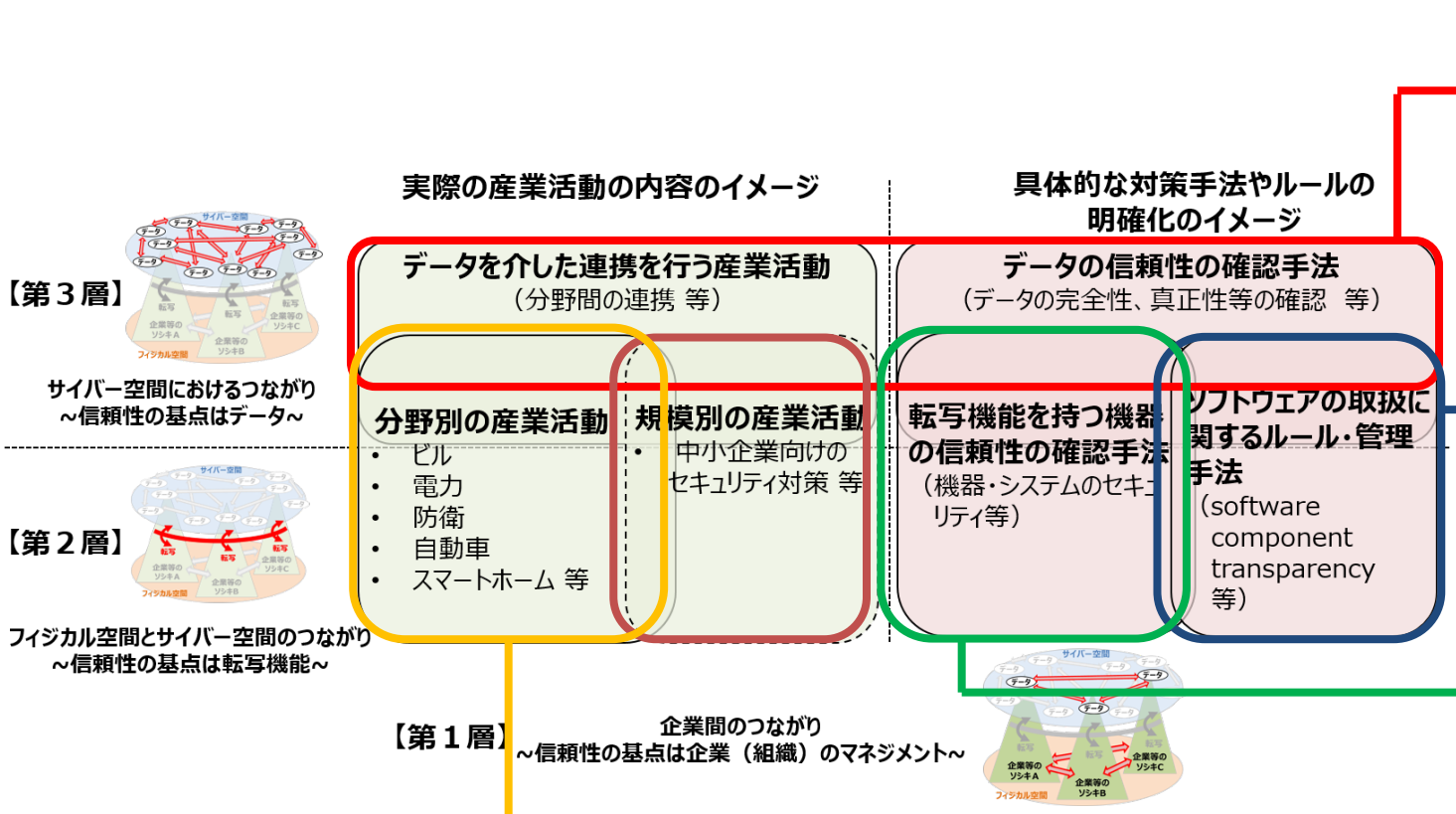
組織・企業・国境内に抱え込まれている価値の高いデータや、慎重な扱いを求められるデータの流通

サイバー・フィジカル一体型社会における信頼性を
確保するためのセキュリティ対策　等
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）　等

＜目指すべき方向性＞

CPSFの具体化・実装の推進

- CPSFの具体的適用に向け、**『データ区分に応じたセキュリティ対策』**、**『転写機能を持つ機器・システムに求められるセキュリティ対策』**、**『OSSを含むソフトウェアの管理手法等』**について、分野横断的な議論を行うタスクフォース(TF)を設置。
- **分野別サブワーキンググループ(SWG)の議論と連携し、CPSFの産業界における実装を推進。**



データ区分に応じたセキュリティ対策要件の作成
⇒**『第3層』TF**

OSSを含むソフトウェアの管理手法等の検討
⇒**ソフトウェア管理手法等TF**

転写機能を持つ機器等に求められるセキュリティ対策要件の作成
⇒**『第２層』TF**

連携

産業分野別ガイドライン等の作成
⇒**産業分野別SWG**

グローバルサプライチェーンを支えるASEAN等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諸国等の対応能力向上のため、**ASEAN等向け日米共同演習**の実施や、**ASEAN諸国のインターネットの健康状態を可視化・比較するカントリー・レポートの作成**を推進。

1．ASEAN等向け日米サイバー共同演習（2018年9月）

- 制御システムのサイバーセキュリティに関する日米専門家による講義・演習を実施。
- 多国間連携のシンボル事業として、2019年度も開催に向けて準備中。

＜昨年度の例＞

OTセキュリティの基礎を学習

制御システムを用いた演習

模擬プラントを用いた講義

プラクティス共有等

2．ASEAN諸国サイバーエコシステム健全性分析調査

- 東アジア・ASEAN経済研究センター（ERIA）が中心となり、米国のNPOとも連携し、ASEAN各国のネットワークやサーバー等のインターネットインフラの健全性やセキュリティ状況に関する分析レポートを作成。

2．『信頼の価値』を創出する~Checked by Japan~
（Proved by Japan）

- スマート工場や自動運転等を実現するためには、そこで駆使される**IoT、AI等の信頼の確保が必要。**
- Society5.0は、**“開発のための投資”＜“検証のための投資”**の時代へ。
- 信頼を確認するための検証技術・サービスを成長分野に位置づけ、**“Checked by Japan”を推進。**
（Proved by Japan）

サイバーセキュリティ戦略（平成30年7月27日閣議決定）（関連部分抜粋）

4.4.1. 新たな価値創出を支えるサイバーセキュリティの推進

(3) 先端技術を利活用したイノベーションを支えるサイバーセキュリティビジネスの強化

- ・・・**国際競争力の強化や真正性・信頼性の検証が困難なセキュリティ製品・サービスへの依存を回避する観点から、我が国において具体的な解決策を提供できるサイバーセキュリティビジネスの強化が必要**である。
- ・・・**先端技術による新たな価値創出を目指す企業と、その先端技術の利用 を支えるためのサイバーセキュリティ技術・サービスの供給者とのマッチングやサイバーセキュリティ技術・サービスの適切な評価に係る仕組みの構築等**に向けた検討を行う。

4.4.2. 研究開発の推進

(1) 実戦的な研究開発の促進

- **政府機関や重要インフラ事業者等のシステムに組み込まれている機器やソ フトウェアについて、必要に応じて、不正なプログラムや回路が仕込まれていないことを検証できる手段を確保**することが重要である。このため、**国が中心となって、必要な技術的検証を行うための体制の整備を図る**とともに、そのために必要となる研究開発に取り組む。

包括的なサイバーセキュリティ検証基盤を構築し、『Checked by Japan（Proved by Japan）』を促進

- 「**Checked by Japan**」では、2つの方向を追求し、**セキュリティビジネスの成長を促進**。

① 有効性確認等を通じ、日本発のサイバーセキュリティ製品のマーケット・インを促進

② IoT機器等の信頼性を高度に検証するハイレベル検証サービスの拡大

1．セキュリティ製品の有効性検証

2．実環境における試行検証

3．攻撃型を含めたハイレベルな検証サービス

信頼できるセキュリティ製品・サービス

世界に貢献する高水準・高信頼の検証サービス

我が国発のセキュリティ製品の普及展開へつなげるため

重要分野のセキュリティ製品の有効性を確認し、発信する仕組みの構築

- 成熟したセキュリティ製品市場では、海外製の製品が高いシェア。
- **我が国発の新たなセキュリティ製品の市場参入を促進する**ため、サイバー攻撃の脅威や対策動向等を踏まえ、**これから重要性が高くなると考えられる製品分野を公表。**
- その**分野に該当する我が国製品について、専門家による有効性確認を実施**し、その**内容を発信**することで、**ユーザーが我が国発の製品を選定しやすい環境を構築。**

重要分野予測

脅威、市場動向等を分析し、**これから重要となる分野の予測をIPAが公開**

重要分野に該当するセキュリティ製品

製品A

製品Aの評価

・使いやすさ
・技術的な革新性
・コスト
（管理含む）
等

導入選定時に参照

有識者による評価

重要分野に関連するセキュリティ技術・製品について、**有識者が率直な評価を行い、その内容を公表**

ユーザー企業

我が国発のセキュリティ製品の普及展開へつなげるため

セキュリティ製品の実環境への試行導入と実績公表を進める仕組みの構築

- セキュリティ製品等の**選定の決め手の一つは、実環境への導入実績。**
- 実環境への**試行導入・実績公表を行う企業向けの手引きを作成**するとともに、試行導入に関心がある**ユーザーとベンダーをマッチング**し、**我が国発のセキュリティ製品の試行導入・実績公表を促進。**

＜ベンダー側の課題＞

・良い製品を作っても、実績が示せず、利用者が試さない。

＜重要分野のセキュリティ製品評価のイメージ＞

・重要となる分野の予測をIPAが公開。
・当該分野に関連するセキュリティ技術・製品について、有識者による率直な評価を頂き、その内容を公表。

＜ユーザー側の不安＞

・セキュリティ製品の導入が既存システムへ影響を与えないか。
・導入事例を公表することでリスクが高まらないか。

＜試行導入・導入事例公表の手引きのイメージ＞

・どのようなプロセスでセキュリティ製品の導入対象システムを選定したのか、事例公表に踏み切った理由等を紹介。

支援

ベンダー企業

マッチングの機会を創出

コラボレーション・プラットフォーム

支援

ユーザー企業

セキュリティ製品の実環境への試行導入と実績公表

Society5.0時代の信頼性確保のために必要となる
攻撃型手法を含むハイレベルな検証サービスの普及展開へ向けた実証

- IoT機器・システムを中心に、**ホワイトハッカー等を有する事業者による攻撃的手法を含むハイレベルな検証を実施**。
- 実証を通じ、**信頼できる検証主体を確認する仕組み**や、**機器毎に効果的な検証手法等の考え方を整理**し、検証サービスの効果・信頼性を向上させ、ビジネスとして普及展開。

実証

検証対象

・ネットワークに常時接続する端末機器
・サイバー攻撃を受けることにより事故に繋がる可能性があるもの　等

検証事業

検証手法・検証ツール
（リバースエンジニアリング、ネットワークキャプチャ　等）

＋

検証事業者
（ホワイトハッカー　等）

検証技術等の技術開発
（内閣府SIPプロジェクト、AIチッププロジェクト　等）

実証の成果と活用のイメージ

①各検証手法を用いた、対象機器・システムごとの検証結果

⇒IoT機器等毎の効果的な検証手法の考え方を整理

②検証事業者に求められる、情報管理体制等の考え方の整理

⇒信頼できる検証主体を確認する仕組みの検討

③技術開発支援などにより、我が国の検証技術の高度化

⇒検証サービスの効果向上

期待される効果

検証サービスの効果・信頼性向上

検証ビジネスの普及展開

３．『中小企業・地域』まで展開する

- 危機意識が十分でない中小企業も少なくないが、地域の中小企業であっても、例外なくサイバー攻撃の脅威にさらされている実情が徐々に明らかになっている。
- 中小企業・地域におけるサイバーセキュリティの取組は、日本の産業に対する世界の信頼に直結する重要な課題。
- サイバーセキュリティ対策強化を中小企業・地域まで展開するため、中小企業・地域の更なる実態把握、徹底した中小企業の現場支援、地域を支えるコミュニティ形成を進めていく。

（参考）中小企業・地域の実態　～大阪商工会議所における調査

調査内容

- 実証期間：平成30年9月～平成31年1月
- 実証内容：中小企業30社を対象に、ネットワーク上の通信データ等を一定期間にわたり収集し、サイバー攻撃に関する調査、分析を行う。

調査結果（中間報告）

- **調査した30社全てでサイバー攻撃を受けていたことを示す不審な通信が記録**されていた。
- 少なくとも5社ではコンピューターウイルスに感染するなどして、情報が外部に流出したおそれがあることが分かった。
- 今後さらに調査を進め、最終的な調査結果を今年４月頃に公表する。

中小企業・地域のセキュリティ対策強化に向けて

- サイバー攻撃の脅威は、資源・人材の限られる中小企業・地域も例外でない。
- サプライチェーン全体での対策を進めていくためには、各中小企業・地域の実態に応じた、**徹底した中小企業の現場支援**と、**地域を支えるコミュニティ形成**が必要。

商工会議所等と連携した実態把握

徹底した中小企業の現場支援

【事前支援】
- 中小企業ガイドラインやセキュリティアクション（6.7万社が自己宣言※）※2019年2月時点
- 登録セキスペの企業派遣・マネジメント支援

【事後支援】
- サイバーセキュリティお助け隊

地域での人材育成・コミュニティ形成促進

【地域を支える人材の育成】
- 高専機構等との産学官連携による人材育成推進
- 産業サイバーセキュリティセンター（ICSCoE）の地域へのアウトリーチ

【地域コミュニティの形成】
- コラボレーションプラットフォームの地域展開
- 地域の登録セキスペやICSCoE修了生との連携

各地域の実態に応じた取組の推進

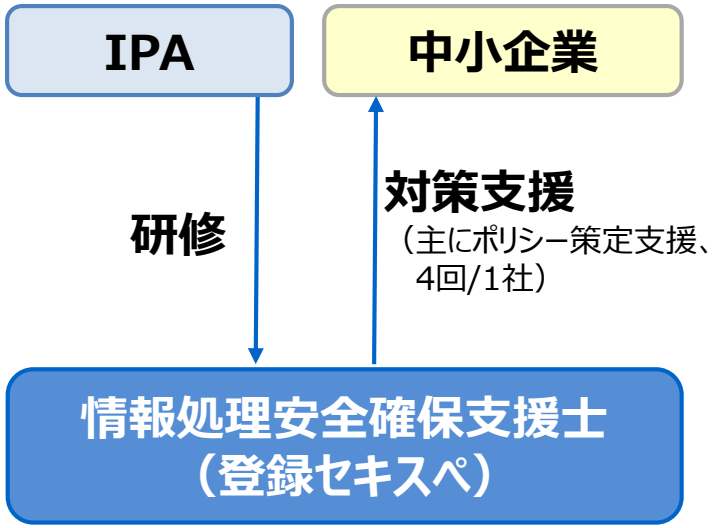
中小企業における現場対応の徹底支援
～事前の備えから、インシデントが発生してしまった後の対応・復旧支援まで

- セキュリティ対策を始めるに当たって何をやればいいのかわからない、そういった悩みをもつ中小企業に対し、**専門家を派遣し、セキュリティポリシーの策定を支援。**
- インシデントが発生してしまったが対処方法がわからない、そんな中小企業の事後対応を支援する簡易保険の実現を目指し、**サイバーセキュリティお助け隊による支援体制を構築。**

特定 → 防御 → 検知 → 対応 → 復旧

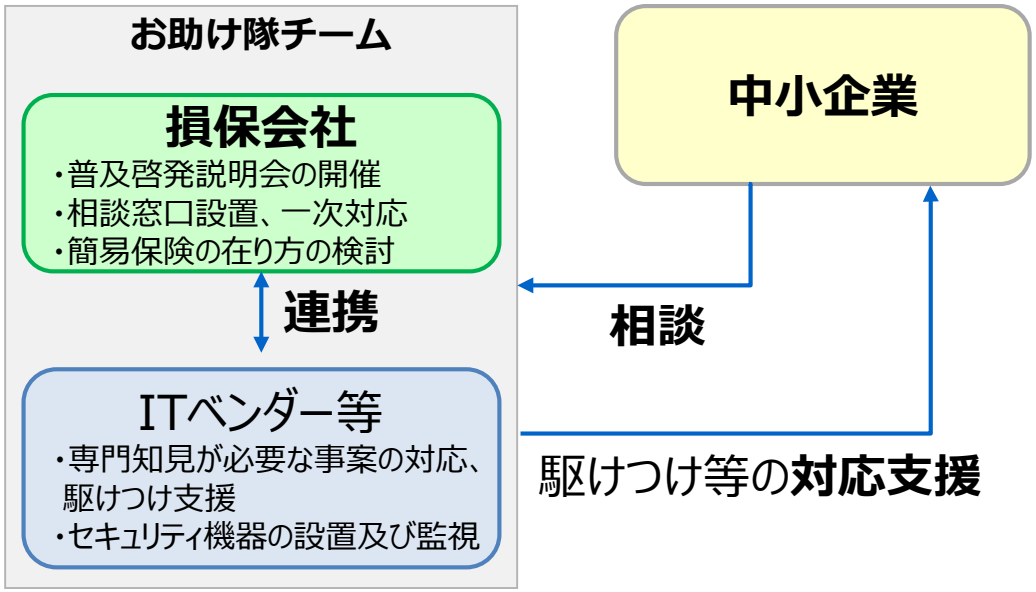
主に事前支援（セキュリティ専門家派遣）

・中小企業に専門家を派遣し、実践的なセキュリティ対策の定着につなげる。



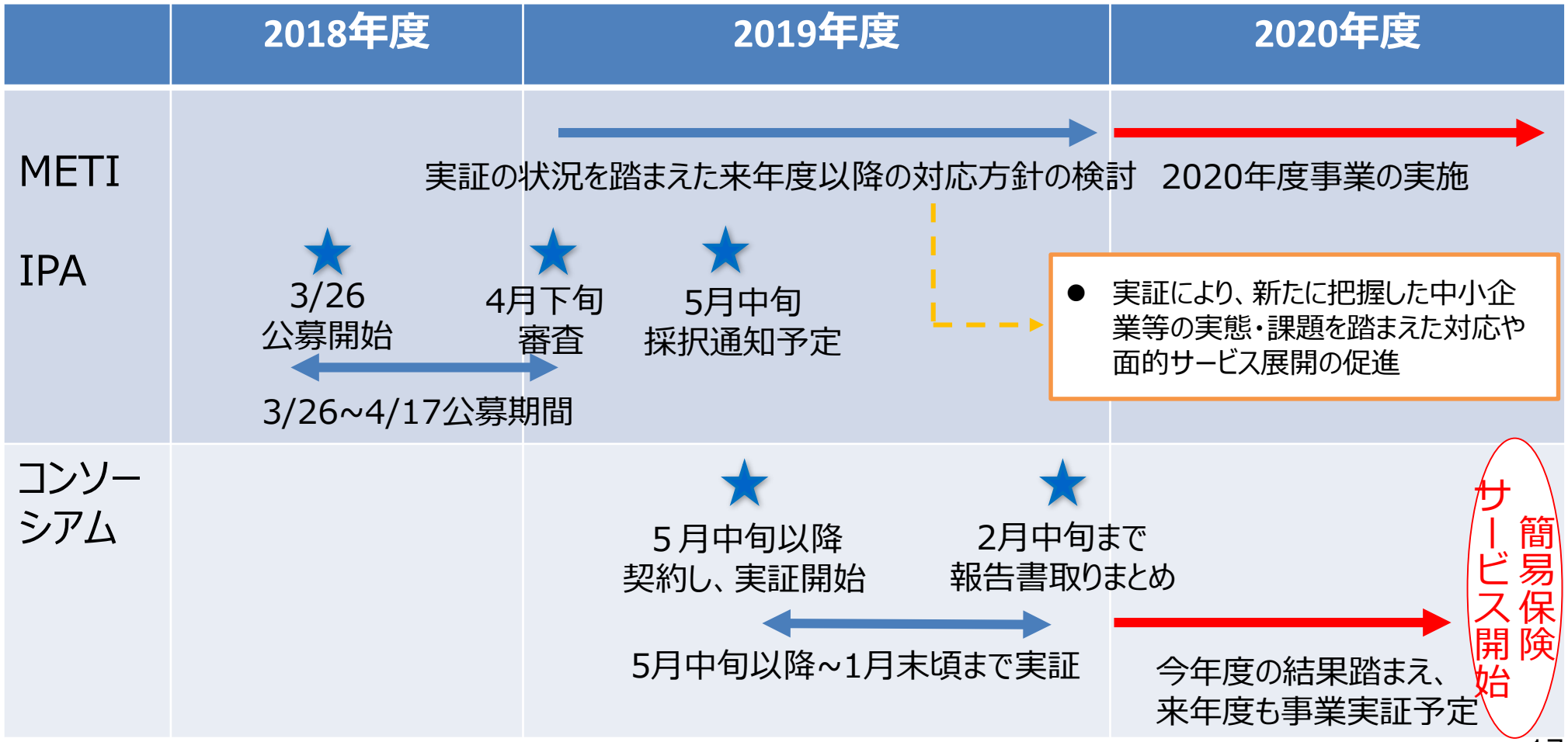
主に事後支援（サイバーセキュリティお助け隊）

・中小企業がサイバー攻撃等で困った時の**相談窓口、駆けつけ支援体制**を構築。
・**将来的な民間サービスとしての自走を目指し、今年度は８地域で実証。**
・今年度の結果を踏まえ、来年度以降、**全国展開を目指すための方策を実施。**



サイバーセキュリティお助け隊の実証のスケジュール

- 2019年3月26日から公募を開始。**5月中旬以降事業開始**。
- 全国8か所で実証事業を行う。あわせて、実証を通じ中小企業の実態把握を進め、実態に応じた効果的な取組も検討していく。



地域での産学官連携による人材育成・コミュニティ形成の促進

- 各地域で不足しがちな**地域を支えるセキュリティ人材の育成**や、実務担当者間の情報交換や相互扶助の基盤となる**地域に根差したコミュニティ形成**のための産学官連携の取組を促す。

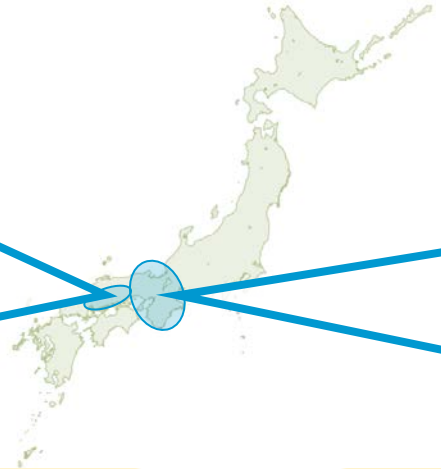
＜各地域の取組の例＞

サイバーセキュリティセミナー広島・岡山

・平成31年2月20日@広島（中国経産局、中国総通局）

・平成31年3月5日@岡山（中国経産局、中国総通局）

※中国経産局を中心としてイベント開催等の体制強化を検討中（平成31年度）



関西サイバーセキュリティ・ネットワーク
（近畿経産局、近畿総通局、KIIS※1）

平成30年11月12日 キックオフフォーラム

リレー講義の様子（計7回実施）

＜取組の方向性＞

1．地域を支える人材の育成

- **産学官連携によるセキュリティ教育の充実**
  - ・国立高専機構と産（JNSA※2、CRIC CSF※3 等）や官（IPA、地方局 等）との更なる連携強化　等
- **ICSCoEの地域へのアウトリーチ**
  - ・各地域への出張講義　等

両輪で促進

2．地域に根差したコミュニティの形成

- **コミュニティ形成のための働きかけ**
  - ・地方版コラボレーションプラットフォームや、シンポジウム（5月28日@大阪）の開催 等
- **ハブとなる人材の活躍促進**
  - ・各地域の登録セキスペやICSCoE修了生等との連携強化　等

産	学	官
企業・業界団体等 ■CRIC CSF、JUAS、JNSA ■ユーザー企業、ベンダー企業　等	**大学・高専等** ■情報系の学生 ■研究者・教員　等	**関係省庁・独法・自治体等** ■都道府県警、地方局 ■IPA、JPCERT/CC　等

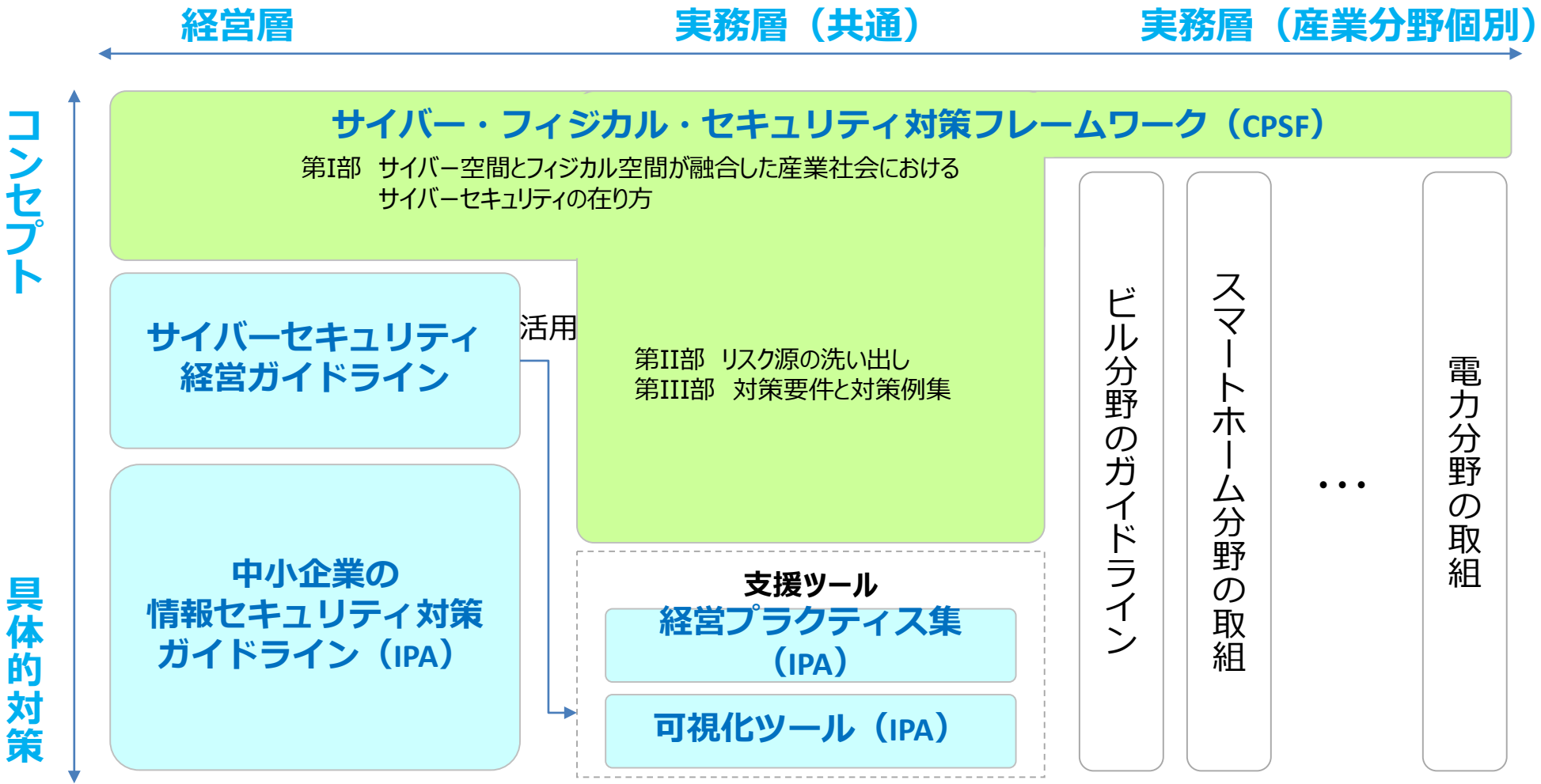
※1 KIIS･･･Kansai Institute of Information Systems、※2 JNSA･･･Japan Network Security Association、
※3 CRIC　CSF･･･Cyber Risk Information Center Cross Sectors Forum

（参考）
産業サイバーセキュリティ強化へ向けた
アクションプランの主な進捗

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を軸とした各種取組

- 「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示。
- 全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞



1. グローバルサプライチェーンに対応した **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**

アクションプラン(2018年５月)	取組の進捗
(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（CPSF）の策定	(A)フレームワークの提示と国際的議論 ①**フレームワークを策定・公表**。 ②策定に当たっては、 ・日本語版・英語版両方でのパブコメを２度実施 ・マルチ・バイの場での積極的な取り上げ を進めるなど**国際ハーモナイゼーションを推進** ③**産業分野ごとの落とし込み**に向けた議論を推進
(２)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の推進	
(３)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	(B)ＡＳＥＡＮ等への働きかけ強化 ①セキュアな**電力制御システムのインフラ輸出** ②ASEAN向け**日米共同演習**を初めて東京で開催
(４)サプライチェーンサイバーセキュリティに係る研究開発の推進	(C) ＳＩＰの推進と産総研拠点の設置 ①ＳＩＰを活用し、**フレームワークの社会実装に求められる研究開発**を推進 ②産総研に**「サイバーフィジカルセキュリティ研究センター」を設置**

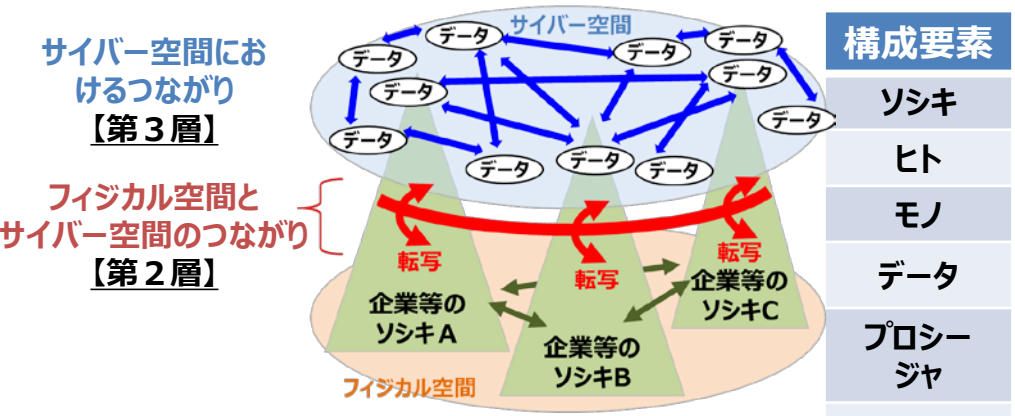
グローバルをリードするための指針となる

再掲

『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）』の策定・公表

- 2019年4月18日、**『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver1.0』を策定・公表。**
- 2度にわたる英文パブコメに対して**海外からも多数のコメントが寄せられ、国際的認知も進展。**
- **CPSFで示した『3層構造モデル』、『リスクベースアプローチ』、『マルチステークホルダーアプローチ』**に対する期待が大きい。

CPSFが示した『3層構造』、『6つの構成要素』



CPSFにおけるリスク管理の考え方

機能（守るべきもの） ⇒ セキュリティインシデント ⇒ リスク源（構成要素ごとに整理） ⇒ 対策要件

第2回パブリックコメント（英語表記含む）の結果

期間　：本年1月9日～2月28日
意見数：**国内27、海外13（米国7、欧州6）**から、**約500件**

＜主な意見＞

- CPSFの**3層構造モデル、リスクベースアプローチ、マルチステークホルダーアプローチ**等に対する**肯定的な意見。**
- データ保護、ソフトウェアセキュリティ等、**CPSFのより具体的な活用方法を求める**意見。

CPSFに対するパブリックコメントの結果

- ２度のパブリックコメントについて、いずれも**英語版のフレームワーク原案も同時公開**して実施し、積極的に意見を取り込んで**国際ハーモナイゼーションを推進。**

第１回 パブリックコメント

- **2018年4月27日～5月28日**
- **国内24, 海外9（米国7, 欧州2）の組織・個人より約300件の意見提出**

【代表的な意見】

- Society5.0 における信頼の確保へ向けた取組として趣旨に賛同。
- 三層構造の説明や、６つの構成要素で整理した理由を明確に説明して欲しい。
- セキュリティ対策の実施主体の明確化を希望。
- 中小企業にとって利用しやすいフレームワークとなることを期待。
- 国際標準や海外規格に留意して進めて欲しい。

第２回 パブリックコメント

- **2019年1月9日～2月28日**
- **国内27, 海外13（米国7, 欧州6）の組織・個人より約500件の意見提出**

【代表的な意見】

- 三層構造は、産業システムにおける関係者・関係性を理解するための有用な考え方を提供している。
- フレームワークで採用しているリスクベースのアプローチ、マルチステークホルダーを考慮したアプローチに賛同。
- 本フレームワークを企業の活動に実装するために、各産業分野への落とし込みが重要。
- 海外主要規格 との対応関係が明確になり有用性が向上した。

マルチ・バイを通じた国際協調への取組

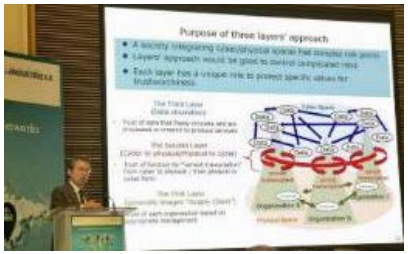
- 「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を軸に、**各国のステークホルダーと議論、マルチの会議で紹介**し、共通の認識を醸成。

【EU/OECD】

- OECD／CDEP（デジタル経済政策委員会）会合（2018年5月@パリ）
- 第8回日EU・ICT戦略WS（2018年12月@ウィーン）
- 第1回 繁栄のためのデジタルセキュリティに関するOECDグローバルフォーラム（2018年12月@パリ）

【Germany】

- Securing Global Industrial Value Networks（2018年5月@ベルリン）
- VDE Tec Summit 2018（2018年11月@ベルリン）



【US】

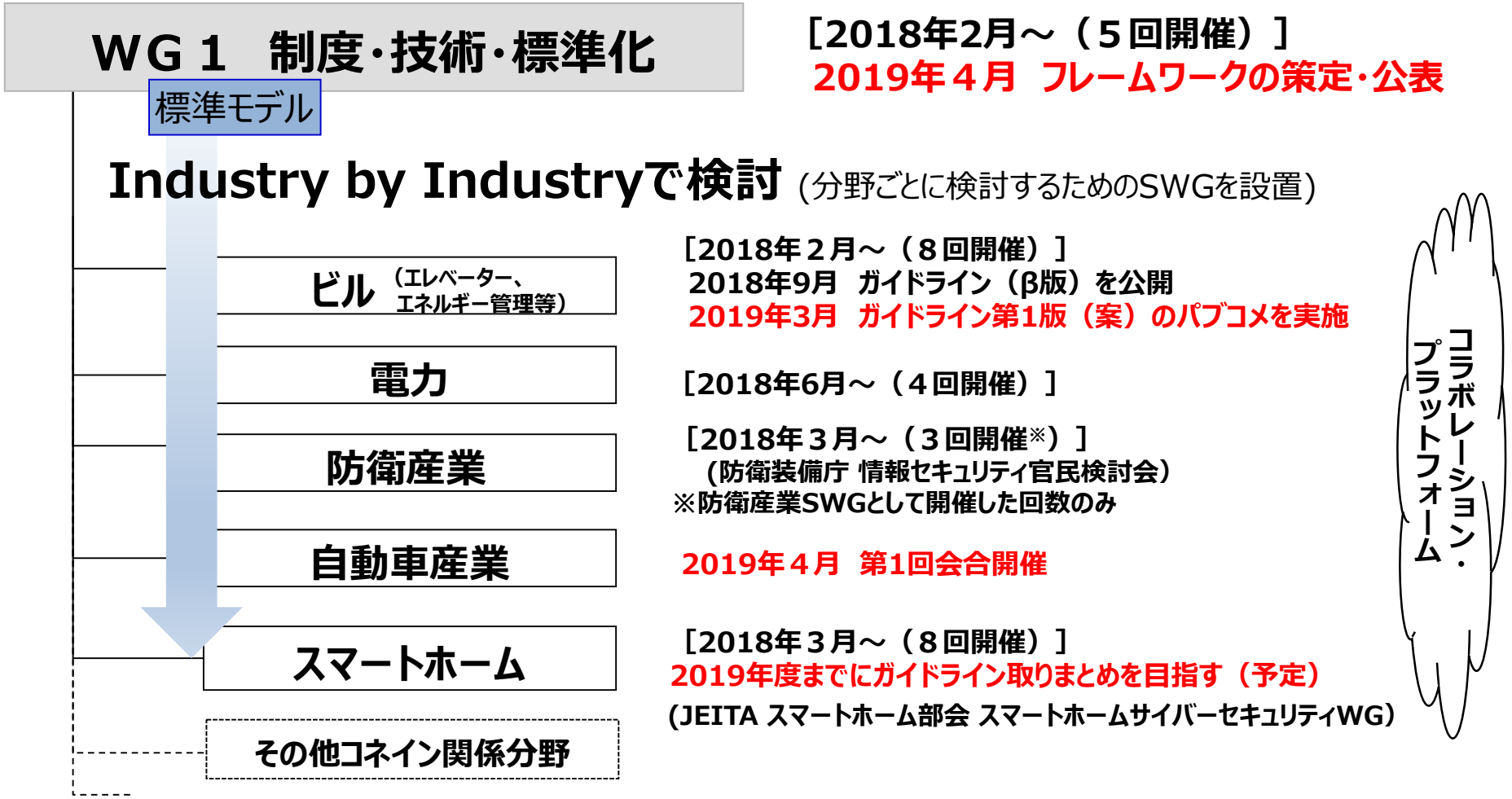
- TecGlobal （米国商工会議所主催）（2018年４月@ワシントンDC）
- Industrial Control Systems Joint Working Group (ICSJWG)（2018年４月@アルバカーキ）
- 2nd Global Cyber Dialogue（米国商工会議所主催）（2018年10月@ワシントンDC）
- CES 2019（2019年1月@ラスベガス）

【APEC/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）
- APEC TEL58（第58回電気通信・情報作業部会）（2018年10月@台湾・台北）


産業分野ごとの検討の促進：分野別のSWGの設置

- CPSF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。



ビルSWG（座長：江崎 浩 東京大学 教授）

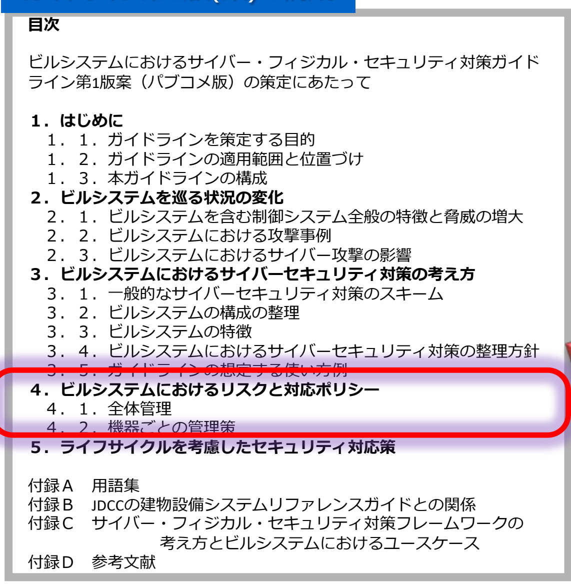
- オリパラ施設を含め、ビルの管理・制御を行うビルシステムに係る各種サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理し、ビルに関わるステークホルダーが活用できる**ガイドラインをとりまとめる。**

<構成員>

有識者	江崎浩東京大学大学院教授、松浦知史東京工業大学准教授、制御システムセキュリティセンター
ビルオーナー	日本生命、三井不動産、三菱地所、森ビル（イーヒルズ）、横浜市、日本ビルヂング協会連合会、不動産協会
ゼネコン、サブコン、設計事務所	鹿島建設、竹中工務店、きんでん、九電工、日建設計
個別システム事業者	アズビル、セコム、ダイキン工業、NTT、日立製作所、三菱電機、ビルディング・オートメーション協会

<ガイドライン・パブコメの実施：2019/3/11～4/9>

ガイドライン第1版(案)の構成

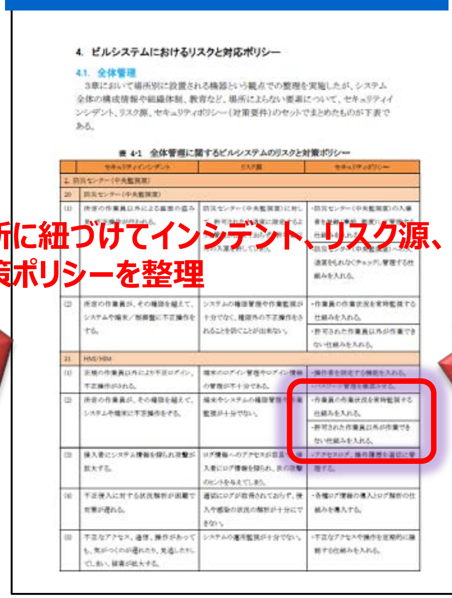

目次

ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版案（パブコメ版）の策定にあたって

1．はじめに
　1．1．ガイドラインを策定する目的
　1．2．ガイドラインの適用範囲と位置づけ
　1．3．本ガイドラインの構成
2．ビルシステムを巡る状況の変化
　2．1．ビルシステムを含む制御システム全般の特徴と脅威の増大
　2．2．ビルシステムにおける攻撃事例
　2．3．ビルシステムにおけるサイバー攻撃の影響
3．ビルシステムにおけるサイバーセキュリティ対策の考え方
　3．1．一般的なサイバーセキュリティ対策のスキーム
　3．2．ビルシステムの構成の整理
　3．3．ビルシステムの特徴
　3．4．ビルシステムにおけるサイバーセキュリティ対策の整理方針
　3．5．ガイドラインの想定する使い方例
4．ビルシステムにおけるリスクと対応ポリシー
　4．1．全体管理
　4．2．機器ごとの管理策
5．ライフサイクルを考慮したセキュリティ対応策

付録A　用語集
付録B　JDCCの建物設備システムリファレンスガイドとの関係
付録C　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考え方とビルシステムにおけるユースケース
付録D　参考文献

具体的な対策（ポリシーレベル）の記載



具体的な対策（ライフサイクル別）の記載

<今後の予定>

- 2019年5月：ガイドライン第1版（共通編）を公開予定
- さらに詳細な解説や事例の充実化、個別の設備に特化した個別編の作成、ビルシステムのセキュリティの管理体制の検討、など

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（CPSF）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）、電気事業者、業界団体

＜方向性＞

- 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

＜今年度以降検討していく課題＞

- **サプライチェーンリスクへの対応**について
  ・海外の事業者や国内他分野の動向を踏まえると、日本の電力分野においてはどのようなリスクが存在するか。
  ・日本の電力分野の関係者が継続的に取り組むべき事項は何か。
- **大手電気事業者**のサイバーセキュリティ対策について
  ・大手電気事業者のサイバーセキュリティ対策の取組の現状分析と、今後取り組むべき事項は何か。
- **新規プレーヤー**のサイバーセキュリティ対策について
  ・新規プレーヤー等のサイバーセキュリティ対策の取組の現状分析と、今後取り組むべき事項は何か。

防衛産業SWG（防衛装備庁 情報セキュリティ官民検討会）

● 我が国の防衛調達におけるセキュリティ強化の方策について検討

我が国の防衛調達における情報セキュリティ強化の方策について、防衛装備庁と主要な防衛関連企業（２３社４団体）との間で「**防衛調達における情報セキュリティ強化に関する官民検討会**」を開催

＜検討の背景＞

1. **我が国におけるサイバー攻撃の増大**：高度化するサイバー攻撃により、我が国のサプライチェーンが標的となる可能性。
2. **米国の情報セキュリティ強化の動き**：米国の新標準（NIST SP800-171）を満たすことが、今後の米国をはじめとする国際共同研究・開発への参加を継続する最低条件となる可能性。

＜対応方針＞

契約企業が保護すべき情報を取り扱う際に適用される情報セキュリティ基準を、**米国の新標準と同程度まで強化した新情報セキュリティ基準を策定**する。

＜開催の状況＞

	開催日	検討テーマ
第１回	平成２９年　２月２８日	米国の防衛調達における情報セキュリティ強化の動向
		我が国の防衛調達における情報セキュリティ強化の方向
第２回	平成２９年　４月　５日	情報セキュリティ強化のためのルールのあり方
第３回	平成２９年　５月１９日	
第４回	平成２９年　６月１５日	中間的論点整理
第５回	平成２９年１１月２８日	これまでの振り返り及び現在の検討状況
第６回	平成３０年　３月２９日	新基準適合に向けた取り組み
第７回	平成３０年　９月　５日	防衛調達におけるサイバーセキュリティの強化に向けて
第８回	平成３１年　２月２８日	サイバー攻撃に関する留意事項、米国企業のNIST SP800-171対応状況

（※）

※第６回検討会より、経済産業省産業サイバーセキュリティ研究会と連携を図るため「**産業サイバーセキュリティ研究会WG1防衛産業SWG** 」として実施。

＜作業部会の設置＞

第７回検討会以降10/15より、情報セキュリティ官民検討会における検討を促進していくための枠組みとして、作業部会を設置
→11/22までに計４回の作業部会を実施し、情報セキュリティ基準改正の考え方に関する、**技術的・専門的観点からの認識を共有**

自動車産業SWG（一般社団法人 日本自動車工業会 電子情報委員会）

- 日本の自動車業界として対象のセキュリティフレームワーク、ガイドライン、実現レベルを定め、活用を推進することで、適切なセキュリティ対策の実施を図る。

  ◆対象範囲（車載に関連する部分を除く）

  - 部品やサービス/ソフトウェアのサプライチェーン
  - 個社工場における設備や設備保守
  - “クルマやお客様”と”個社を含むサービス提供者”をつなぐシステムや提供するサービス及びデータ

個社の実施レベル測定と最適化

＜メンバー構成＞
日本国内の乗用車、二輪車、商用車生産の14社

＜開催状況＞
2019年4月16日(火) 第１回 電子情報委員会 サイバーセキュリティ部会 開催

＜進め方＞
国内外のフレームワークやガイドライン、国際標準規定をベースに、自動車業界のリファレンスとなるガイドラインの策定を行う

スマートホームSWG（JEITA スマートホーム部会スマートホームサイバーセキュリティWG）

- Society5.0の実現を目指し、IT・エレクトロニクス企業のみならず、人々の暮らしに関わる様々なメンバーが、それぞれの知見を結集して、スマートホームのセキュリティ対策の検討を実施。
- マネジメント不在といった**スマートホーム特有の脅威や、製品安全の観点も含めたスマートホーム分野のセキュリティガイドラインを整備する**とともに、運用の在り方についてまとめていく。

＜構成員＞　企業）家電・AV関連、IT・通信関連、車載関連、住宅設備・サービス関連

団体・機関）住宅（戸建て／マンション）・住宅設備分野、電機・通信分野、医療分野、研究機関

経済産業省

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

フレームワークと整合

①三層構造アプローチ
②リスクベース
③国際標準との調和

＋

スマートホーム特有の脅威を加味

①膨大な対象
②マネジメント不在
③利用者による想定外の事象

JEITA 一般社団法人 電子情報技術産業協会

スマートホーム実現に向けた サイバーフィジカルセキュリティ対策ガイドライン

- 定義と説明
  - スマートホームの定義
  - スマートホームを取り巻く環境や状況の変化
  - サイバー攻撃の事例
- スマートホームの住まい手である生活者に向けて
  - 機器やサービスの導入時のリスク
  - 機器やサービスの利用時のリスク
  - 機器やサービスの解約時・機器廃棄時のリスク
  - 利用シーンごとの対策と確認内容の例
- スマートホームを構成する機器やサービスの開発者、提供者に向けて
  - 製品とサービスのライフサイクル全体におけるセキュリティレベルの維持
    - 開発時に考慮を必要とする内容
    - 利用中の製品とサービスにおけるリスクと対策
    - サービス解約や機器廃棄時のリスクとその対策
  - 製品とサービスのサポート停止以降のセキュリティレベルの維持
- ユースケース
- リスク・対策・セキュリティ要件の例
- 国際規格等の各種規格との対応

2019年度内の策定を目指す

- **Society5.0社会の基盤となるスマートホーム**は、社会インフラや様々な産業、サービスが結節した、住まい手中心のバリュークリエイションプロセスにより構成
- 住まい手の**セキュリティをバリュークリエイションプロセス全体で確保**

ASEAN等向け日米サイバー共同演習の開催

- 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策に関するキャパシティ・ビルディング支援のため、**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2018年に初めて**開催。
- 参加国からの高い評価に加え、**2018年9月の日米首脳会談においても、「インド・太平洋構想」の重要な取組の一つとして位置づけられた。**

■**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
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

（当時）武藤副大臣ご挨拶（フジTVより）

ハガティ大使ご挨拶（大使のTwitterより）

９月の日米首脳会談において示された
インド太平洋地域の維持・促進に向けた日米協力の例


President Donald J. Trump and Prime Minister Shinzo Abe Are Working Together to Maintain a Free and Open Indo-Pacific

ECONOMY & JOBS

Let us work together for ... prosperous, and free In...

President Donald J. Trump

ENERGY: The United States and Japan are co... security and access in the Indo-Pacific, includ... States Strategic Energy Partnership.

INFRASTRUCTURE AND DEVELOPMENT FIN... Japan seek to ensure that infrastructure... together, generates local wealth, and l...

DIGITAL ECONOMY AND CYBERSECURITY: Cyb... engine of economic growth and innovation in...

MARITIME SECURITY AND DISASTER RISK RED... Japan are building capacity to advance the region's rules-based maritime order, and to boost resiliency to natural disasters that threaten lives and property and disrupt commercial activity.

DIGITAL ECONOMY AND CYBERSECURITY: Cyberspace increasingly will be an engine of economic growth and innovation in the Indo-Pacific.

- The United States and Japan are working together to foster a vibrant and resilient Indo-Pacific digital economy and ensure a secure cyber future.
- To bolster the cybersecurity defenses of critical infrastructure and promote focus on industrial control system security, the U.S. Department of Homeland Security and METI conducted joint training on industrial control systems for ASEAN member countries and other Indo-Pacific partners in September 2018.
- The United States is cooperating with Japan in providing capacity building and technical support to the Pacific Islands.

米国国土安全保障省（DHS）と経済産業省（METI）は、重要インフラのサイバーセキュリティの促進と制御システムセキュリティの推進のため、ASEANや他のインド太平洋諸国向けに、2018年9月に制御システムセキュリティに関する共同演習を実施。

出典：ホワイトハウスHP

サプライチェーンサイバーセキュリティに係る研究開発の推進

- 総合科学技術・イノベーション会議の**戦略的イノベーション創造プログラム（SIP）を活用した研究開発を着実に実施**すると共に、研究開発事業を拡充。
- **産業技術総合研究所にサイバー・フィジカル・セキュリティの中核的な研究開発拠点を開設。**研究成果の実装のための**認定・認証体制の強化**を推進。

SIP第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」
プログラムディレクター：後藤 厚宏 情報セキュリティ大学院大学 学長

SIP 戦略的イノベーション創造プログラム

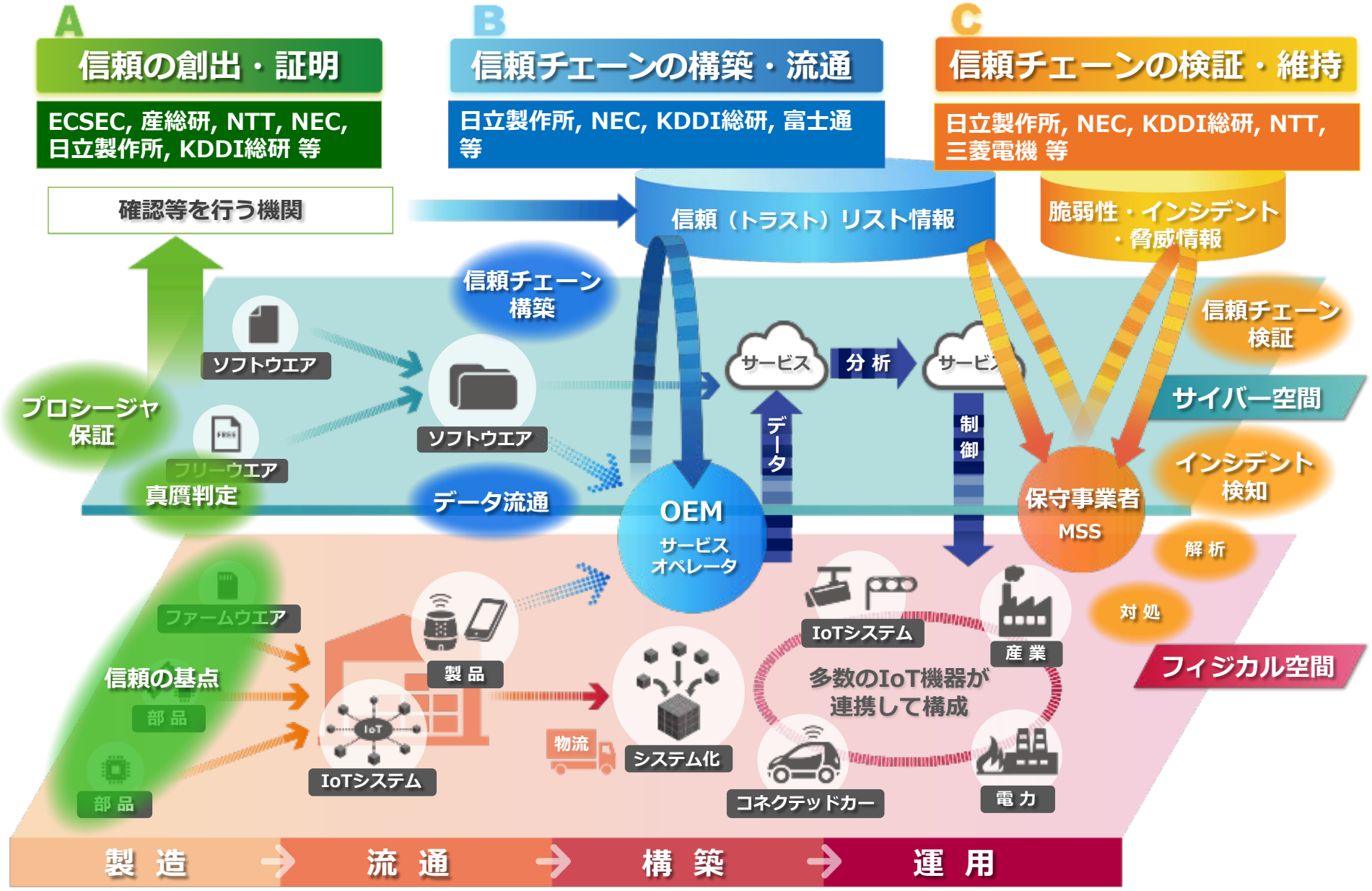
- セキュアな「Society5.0」実現に向けて、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の社会実装に求められる、IoTシステム・サービス及び大規模サプライチェーン全体を守る対策基盤の開発・実証。

産総研 サイバーフィジカルセキュリティ研究センター（2018年11月設立）
研究センター長：松本 勉 横浜国立大学 教授

CPSEC

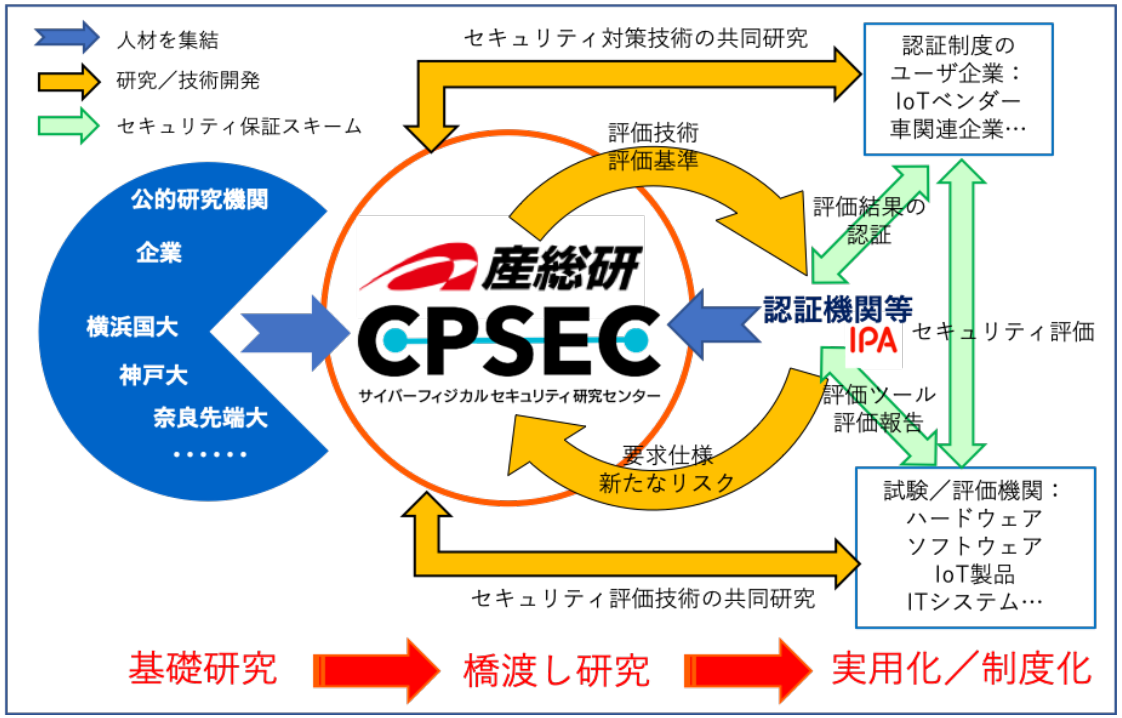
- バリューチェーンにおけるセキュリティで必要となる「研究開発」～「評価制度」まで技術面からサポート。
- セキュリティを測定可能とする研究、継続的な最新技術／知見の蓄積。

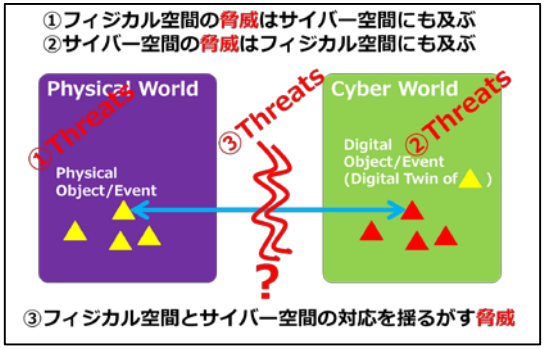
SIP第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」研究開発の取組内容・実施体制



中核的な研究開発拠点の設置
～ 産総研 サイバーフィジカルセキュリティ研究センター（CPSEC）

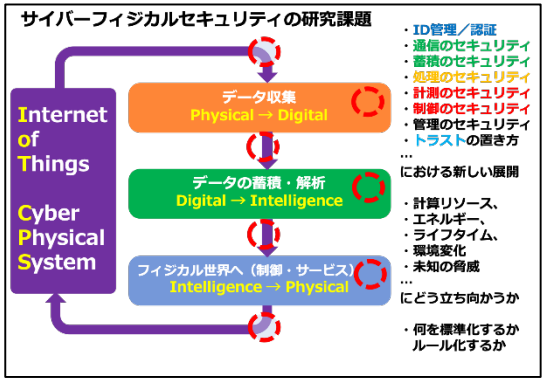
- サイバーフィジカルセキュリティの研究拠点として設置（2018年11月～2025年3月）
- 研究センター長　松本　勉（横浜国立大学とクロスアポイントメント）
- 産総研、企業、大学、試験／評価機関等から研究者や技術者をセンターに集結
  総員115名 ＝ 職員等(産総研の身分を有する者)88名+外来研究員等(含む学生)27名（12月17日時点）
- ７研究チーム（**セキュリティ保証スキーム／高機能暗号／暗号プラットフォーム／ハードウェアセキュリティ／インフラ防護セキュリティ／ソフトウェア品質保証／ソフトウェアアナリティクス**）及び企業との連携研究室で構成
- バリューチェーンにおけるセキュリティで必要となる「研究開発」～「評価制度」までを技術面からサポート
- セキュリティを測定可能とする研究、継続的な最新技術／知見の蓄積





サイバーフィジカル
セキュリティとは

セキュリティを
考慮すべき対象と
研究課題

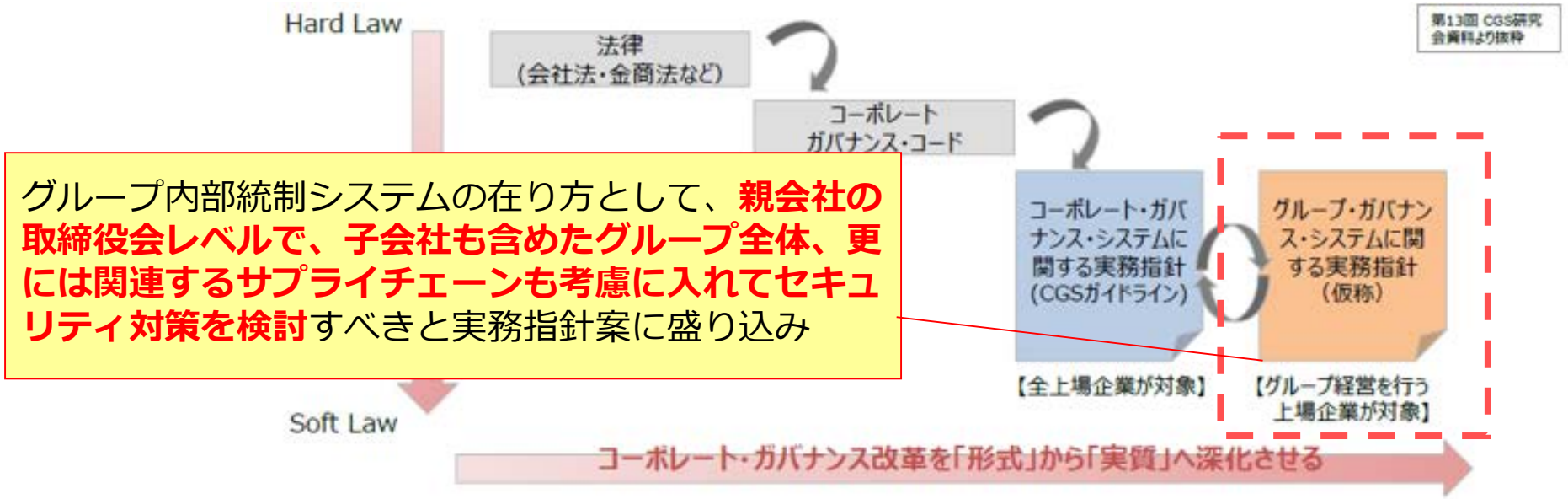


2. 経営・現場双方の課題に応える
サイバーセキュリティ経営強化パッケージ

アクションプラン(2018年５月)	取組の進捗
(１) サイバーセキュリティ経営実現に向けた体系的政策アプローチ ①経営層向け：サイバーセキュリティ経営を促す仕組みの構築	(A)**コーポレートガバナンスの一環で位置づけ**検討 ①グループ経営を行う上での内部統制システムへの位置づけ検討 ②サイバーセキュリティへの関与状況を含めた取締役会の実効性評価を推進
②現場の実務者向け：具体的な対策の導入を促す事例集と可視化ツールの整備	(B)実務者向けツールの提供 ①経営ガイドラインの実践のための具体的対応策を**プラクティス集**として取りまとめ ②取組状況を可視化するためのツールについて考え方を整理
③中小企業向け：サイバー保険等と連携した『サイバーセキュリティお助け隊』の創設	(C)中小企業への支援体制の強化 ①**中小企業向けガイドラインの改訂** ②**SECURITY ACTIONの普及促進** ③**サイバーセキュリティお助け隊**の地域実証
(２)情報共有の仕組みの強化	(D)サイバーセキュリティ協議会の立上げ(ＮＩＳＣ)

経営層向け：
コーポレートガバナンスの一環として、サイバーセキュリティ経営を位置づけ

- **海外では投資家がサイバーセキュリティをビジネス上の大きな脅威と認識**しており、経営層のサイバーセキュリティへの関わりを重要視。
- このため、**内部統制の一環としてサイバーセキュリティ対策の在り方を示す**とともに、経営層のサイバーセキュリティへの関与状況も含めた取締役会の実効性評価を促進。



グループ内部統制システムの在り方として、**親会社の取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れてセキュリティ対策を検討**すべきと実務指針案に盛り込み

CGS研究会（第2期）＜平成29年12月に第一回を開催し、平成31年4月までに16回開催＞

直近のスケジュール：
第14回（2/12）ガイドライン骨子
第15回（3/15）ガイドラインとりまとめ素案
第16回（4/18）ガイドラインとりまとめ

実務者指針公表に向け最終調整中

実務者向け：
『サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集』を策定

- **2019年3月、「サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集」を公開。**経営ガイドラインの重要10項目の実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示。
- 業界団体との連携も視野に入れつつ、**継続して収集し、2019年度も改訂を予定。**

第一章：経営とサイバーセキュリティ

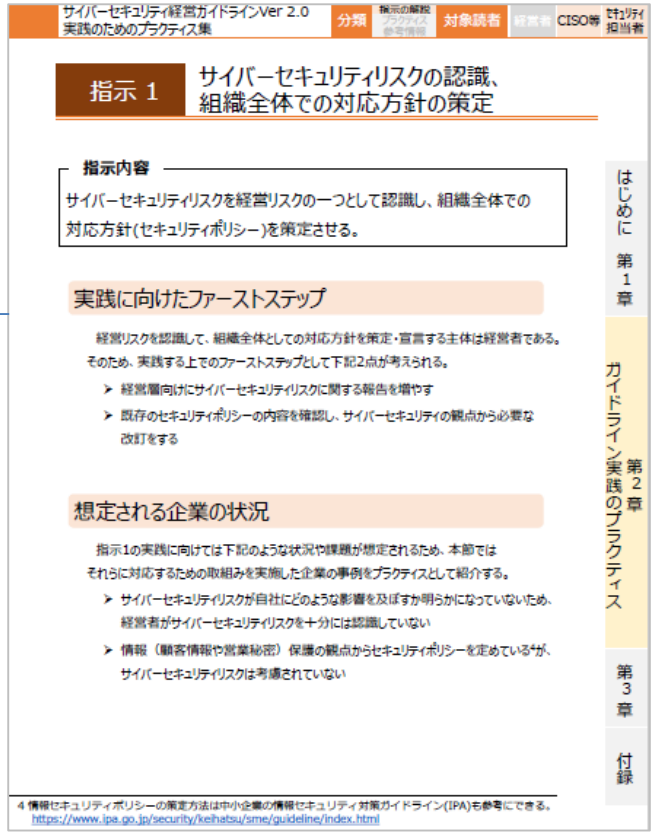
＜経営者、CISO等向け＞
なぜサイバーセキュリティが経営課題となるのか等を解説

第二章：サイバーセキュリティ経営ガイドライン実践のプラクティス

＜CISO等、セキュリティ担当者向け＞
企業の具体事例をベースとした重要10項目の実践手順、実践内容、取り組む際の考え方を解説

第三章：サイバーセキュリティ対策を推進する担当者の悩みと解決のプラクティス

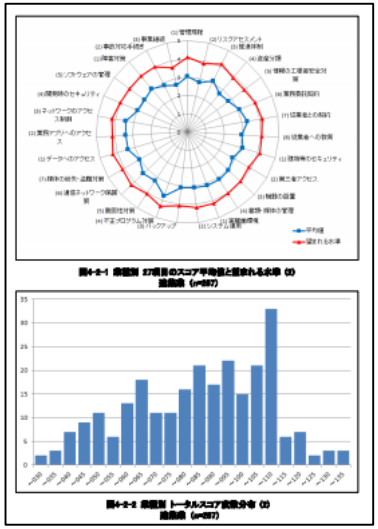
＜セキュリティ担当者向け＞
サイバーセキュリティ対策を実践する上での悩みに対する、企業の具体的な取組事例を紹介



実務者向け：
可視化ツールの整備：情報セキュリティベンチマークの抜本的な見直し

- Cybermaturity Platform（ISACA）、CAT(*)（FFIEC）等の海外の可視化ツールの調査を踏まえ、2019年度に**情報セキュリティベンチマーク（IPA）を拡張し、セキュリティ視点で抜本的な見直し**を行う。

＜可視化ツールの作成の方向性＞



情報セキュリティベンチマーク

セキュリティ視点で
項目追加・見直し

整合性を考慮すべきガイドラインの例

- サイバー・フィジカル・セキュリティ対策フレームワーク（METI）
- サイバーセキュリティフレームワーク（NIST）
- サイバーセキュリティ経営ガイドライン（METI、IPA）

ベンチマークの評価項目と経営ガイドラインを比較し、不足している項目の例
- 経営者がサイバーセキュリティ対策の報告を受けていること
- サイバーセキュリティに関する注意喚起情報等の情報共有、提供を行っていること

(*)FFIEC CAT（FFIEC（米国連邦金融機関検査協議会）が公開するCybersecurity Assessment Tool）

中小企業向け：
中小企業の情報セキュリティ対策ガイドラインの改訂

- 中小企業の経営者やIT担当者に向け、情報を安全に管理するための具体的な手順等を示した**中小企業ガイドラインを改訂（第3版）し、2019年3月に公開。**

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

実践者向けの解説

実践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

＜主な改訂ポイント＞

- サイバーセキュリティ経営ガイドラインVer2.0との整合性の改善
  （「検知」、「復旧」の観点について、中小企業の実態に即した対応策を提示）
- 中小企業向けに、わかりやすい表現や記述に見直し（第１部　経営者編）
- 組織的な対策の実施体制を、段階的に進めていけるよう構成の見直し（第２部　実践編）
- 「中小企業のためのクラウドサービス安全利用の手引き」を新規追加（付録）

中小企業向け：
セキュリティ対策自己宣言「SECURITY ACTION」の取得状況
～IT導入補助金要件化を機に増加

- 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（IPA）。
- IT導入補助金の申請において、「SECURITY ACTION」の宣言を必須要件化。
- **６万７千社を超える中小企業が宣言**（2019年2月末時点）。

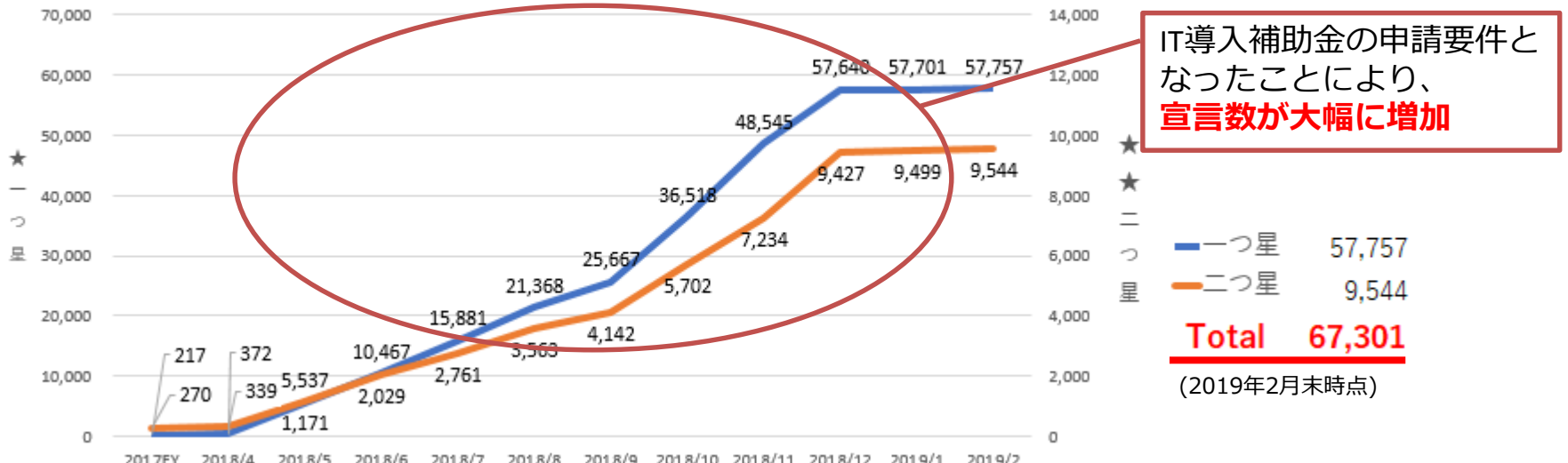
★ 一つ星

情報セキュリティ5か条に取り組む企業

★★ 二つ星

情報セキュリティ自社診断の実施及びセキュリティポリシーを策定する企業

※IPAにて、一般社団法人中小企業診断士協会、全国社会保険労務士会連合会、全国商工会連合会、全国中小企業団体中央会、特定非営利活動法人日本ネットワークセキュリティ協会、特定非営利活動法人ITコーディネータ協会、独立行政法人中小企業基盤整備機構、日本商工会議所、日本税理士会連合会と連携した普及促進活動を実施



中小企業における現場対応の徹底支援
～事前の備えから、インシデントが発生してしまった後の対応・復旧支援まで

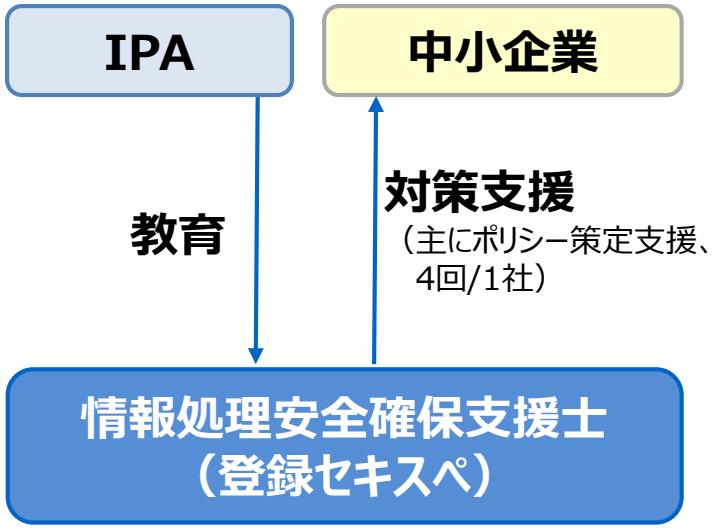
再掲

- セキュリティ対策を始めるに当たって何をやればいいのかわからない、そういった悩みをもつ中小企業に対し、**専門家を派遣し、セキュリティポリシーの策定を支援。**
- インシデントが発生してしまったが対処方法がわからない、そんな中小企業の事後対応を支援する簡易保険の実現を目指し、**サイバーセキュリティお助け隊による支援体制を構築。**

特定 → 防御 → 検知 → 対応 → 復旧

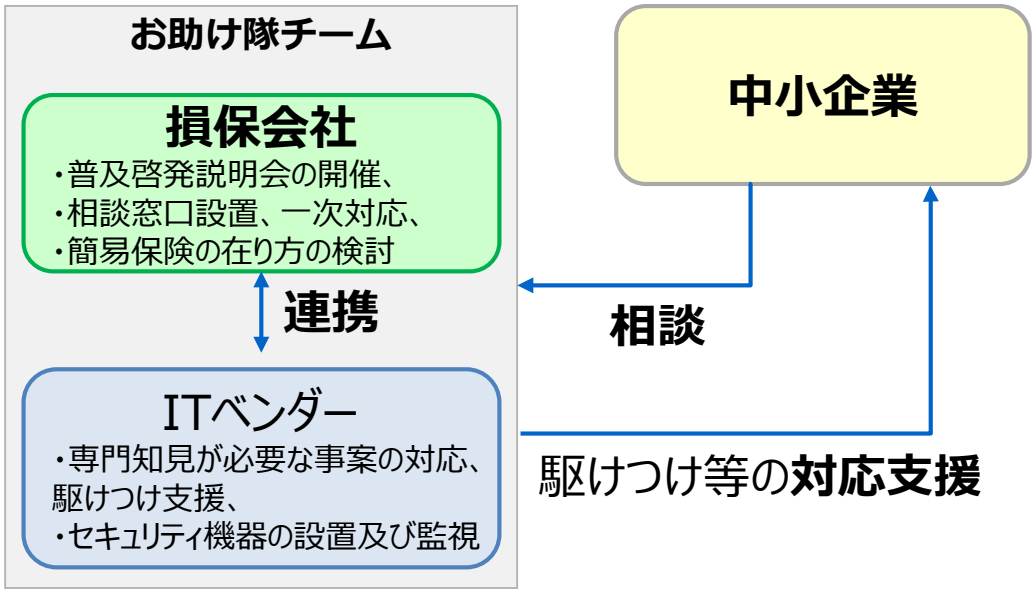
主に事前支援（セキュリティ専門家派遣）

・中小企業に専門家を派遣し、実践的なセキュリティ対策の定着につなげる。



主に事後支援（サイバーセキュリティお助け隊）

・中小企業がサイバー攻撃等で困った時の**相談窓口、駆けつけ支援体制**を構築。
・**将来的な民間サービスとしての自走を目指し、今年度は８地域で実証**。
・今年度の結果を踏まえ、来年度以降、**全国展開を目指すための方策を実施**。



サイバーセキュリティ協議会の概要

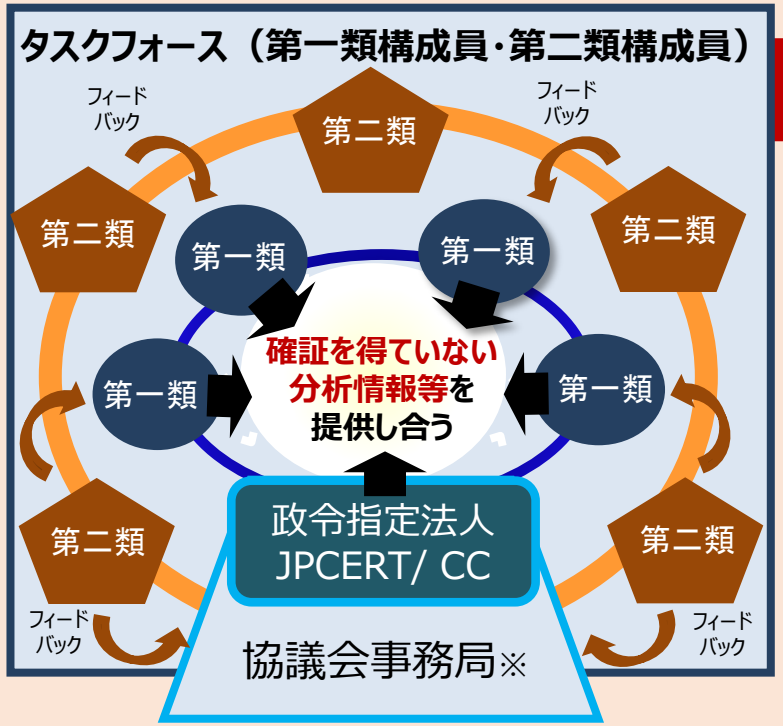
NISC HPから引用

目的

我が国のサイバーセキュリティに対する脅威に積極的に対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行う

➡ 主として、**脅威情報等の共有・分析、対策情報等の作出・共有等**を**迅速に**行う（原則システムを活用）

サイバーセキュリティ協議会（CS戦略本部長等により組織）



作出した対策情報等の共有

一般の構成員

総会

全構成員により構成（各構成員に１の議決権）
・総会は毎年開催（電子的手段の開催も可）
・規約の改正　等を実施

運営委員会

運営委員は、CS戦略本部長等
・構成員の入会の承認、除名
・**情報提供等協力の求め**
等に関することを担当

※事務局の庶務はNISC基本戦略２Gが担当

協議会の特徴

①官民、業界といった従来の枠を越えた**オールジャパンによる**情報共有体制

②システムを用いて情報共有等を行う「**バーチャル協議会**」

③直感的な違和感といった**早期の段階からの情報提供、相談等を促進**
構成員には、法律に基づく守秘義務※、情報提供義務が適用　※罰則付き

④**ギブアンドテイクルールを徹底し、積極的な情報提供者へのメリットを増加**　※積極的な情報提供に意欲と能力のある構成員を「**タスクフォース**」としてグループ化

我が国のサイバーセキュリティを確保する観点から、
構成員になるためには、右の要件を満たし、
運営委員会の承認を得なければならない
（加入は任意）

申込みを行うことのできる者

◆国の関係行政機関　◆地方公共団体　◆重要インフラ事業者
◆サイバー関連事業者（主にセキュリティ関連事業者を想定）
◆大学・教育研究機関　等であり、協議会の活動に賛同する者
（事業者等の団体や個人も含む）

3. サイバーセキュリティ対策を支える基盤となる **サイバーセキュリティ人材育成・活躍促進パッケージ**

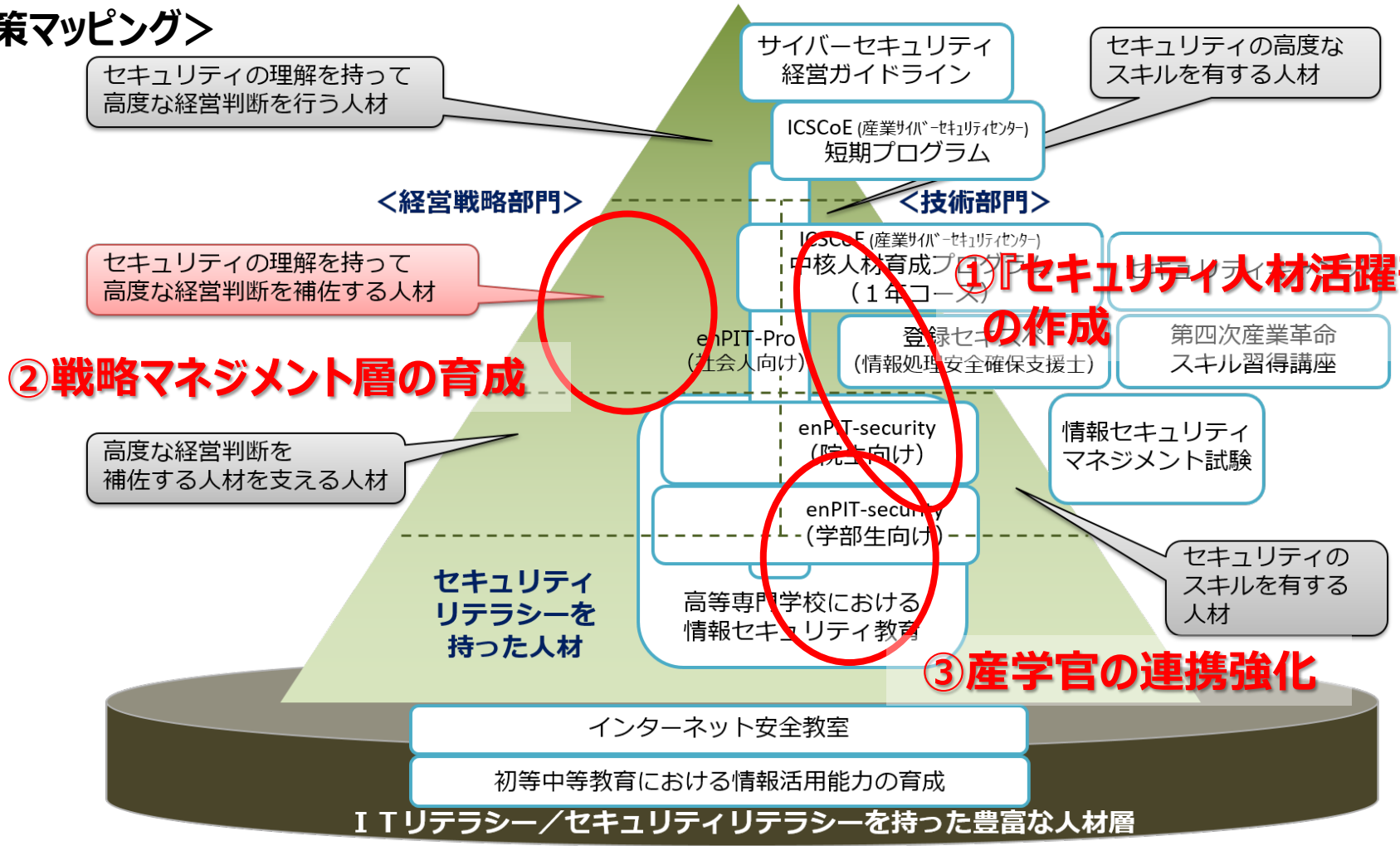
アクションプラン(2018年５月)	取組の進捗
(１)『セキュリティ人材活用モデル』の作成	(A)**セキュリティ人材活躍モデル**の整理 ①ユーザー企業のセキュリティ体制・人材の見える化 ②専門人材の役割・スキル定義の整理・明確化
(２)サイバーセキュリティ経営を進める 『戦略マネジメント層』の育成	(B)**戦略マネジメント層**向けセミナー IPA産業サイバーセキュリティセンター、一橋ビジネススクールICSで実践的プログラムを実施
(３)産学官連携の促進	(C)**高専との連携強化** METI、国立高専機構、IPA及び業界団体（CRIC CSF、JNSA等）において具体的連携を推進

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

第二回産業サイバーセキュリティ研究会資料を一部修正

- **セキュリティ人材の定義や育成・活躍の在り方のモデルが不明確。**
- **「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＞



(A) ニーズとシーズのマッチングのための『セキュリティ人材活躍モデル』の構築

- セキュリティ人材の役割定義の共通言語化等により、ニーズとシーズの見える化・マッチングを図る。

ユーザー企業	主にIT・セキュリティベンダー	人材

必要な機能（タスク）

企業において必要なセキュリティ機能は技術者のみでは確保できない

- セキュリティポリシー策定
- リスクマネジメント
- インシデント対応　等

機能を担う役割の整理

役割（ロール）

様々な団体から役割定義が公開されているが、目的や用途の違いもあり共通言語化されていない

自社ビジネスとセキュリティを理解し、事業の企画や調達等を行う役割		指示に基づき、専門的な業務を行う役割
・CISO ・戦略マネジメント層 ・運用担当　等	指示 ⇒ ⇐ 提供	・フォレンジックアナリスト ・脆弱性診断士 ・セキュリティ監査人　等
⇒ 主に内製で育成		⇒ 主に外注で確保

役割とスキルの紐づけ

知識・技能（スキル）

- ITSS+(IPA)
- SecBoK(JNSA)
- 統合セキュリティ人材モデル
- NICEフレームワーク（NIST）　等

スキルと資格等の紐づけ

資格・試験

- 登録セキスペ
- 民間資格　等

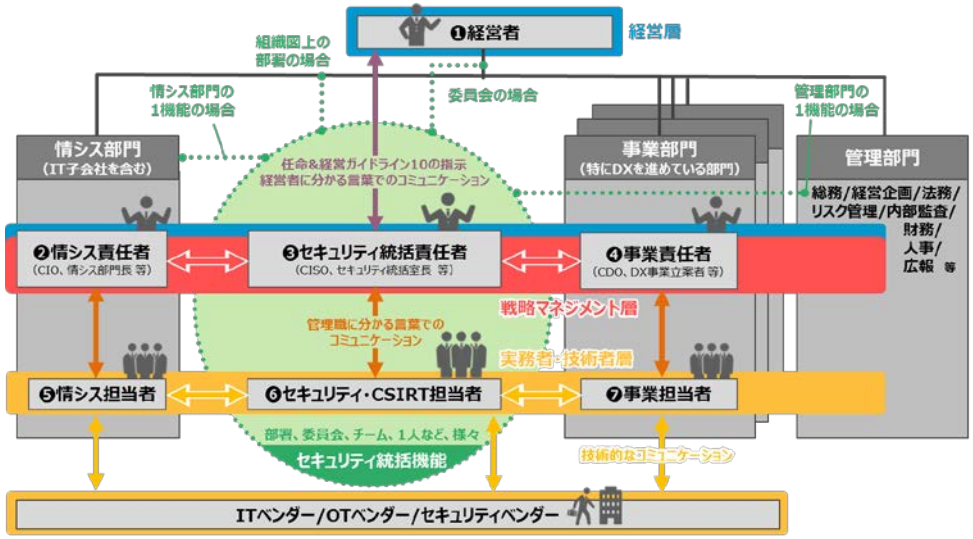
研修

- ICSCoE
- JNSA
- CRIC CSF　等

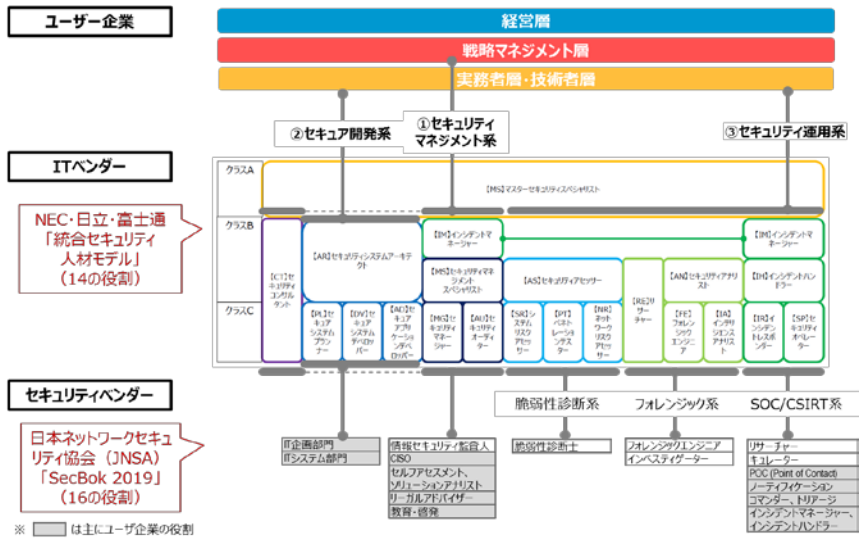
教育

- 大学シラバス
- 高専カリキュラム　等

ユーザー企業のセキュリティ体制・人材の見える化



専門人材の役割・スキル定義の整理・明確化



(B)戦略マネジメント層の育成

- IPA産業サイバーセキュリティセンターにおいて「戦略マネジメント系セミナー」を実施。
- 一橋ビジネススクールICSの協力でサイバーセキュリティを組み込んだDX時代における人材育成プログラムを実施。

産業サイバーセキュリティセンター「戦略マネジメント系セミナー」

- 2018年11月～12月（全７回）
- １７名（うち６名は部長以上）が参加
- 前半は専門家からの講義、後半はケース討議（グループディスカッション）の２部構成で実施
- アンケート調査の結果、参加者の約９割が有意義であったと回答

一橋ビジネススクールICS協力「デジタル・トランスフォーメーション時代における人材育成プログラム」

- 2018年9月～１１月（全12日間※修了式除く）
- 官民合わせて30社が参加
- DXに関するリテラシーが向上し、参加者間でのネットワークが構築

産業サイバーセキュリティセンターにおける「戦略マネジメント系セミナー」については、2018年度の実施結果を踏まえたカリキュラムや実施期間を見直しを行い、2019年度も実施する方向で検討中

(C) 高専機構等との産学官連携強化

- 全国51か所の国立高専のうち20か所においてセキュリティ人材の発掘・育成が重点的に実施されている。
- METI、国立高専機構、IPA及び業界団体（CRIC CSF、JNSA等）において具体的連携を推進していく。

使用できるインフラ
- 演習設備
- 同時中継
  (全国高専間で配信可)
- 仮想空間

セキュリティスキルレベル

国立高専卒業生 約1万人/年の内訳	コンテンツ開発・授業の提供 (PowerPoint、ビデオ等)	セキュリティ合宿に関する協力
	パターン①：90分程度 ・高専教員がコンテンツを使って講義 又は 企業等の方が講義 (拠点校から全国各校に同時配信も可) **パターン②：15分程度** 授業冒頭や隙間時間でビデオ放映	**高度セキュリティ合宿** (1泊2日) 年2回ペースで開催（NWトラブル演習等）参加者：35名程度 **KOSENセキュリティコンテスト** (１泊2日) 年1回ペースで開催（CTF）参加者：130名程度 ※開催期間中の一部の時間を利用して、一線で活躍するホワイトハッカーから講義を実施可能。
約１％ トップガンの学生 → 主に**セキュリティ企業**に就職	※トップガンの学生は、全国各校、各学科に散らばっているため、通常の授業時間で集合する機会がない。	• **JNSAが講師の派遣を検討中。** • **METIがセキュリティ専門官の派遣を検討中。**
約20% 情報系学科の学生 → 主に**IT企業**に就職	• **IPAが地元のICSCoE終了生による講義を検討中。** • **JNSAがコンテンツ開発を検討中。**	• **JNSAとSECCONビギナーズに係る協力を検討中。**
約80% 非情報系学科の学生 → 主に**ユーザー企業**に就職	• **CRIC CSFが業界別（例．機械、電気、建築等）のコンテンツ開発や授業提供について検討中。**	※セキュリティ合宿のような機会は特段なし。
KOSEN 国立高等専門学校機構 国立高専教員	※授業実施側のため。	• **JPCERT/CCが情報担当教員向け研修に講師を派遣。** • **IPAがセキュリティキャンプ全国大会の見学について検討中。** • **教師向け合宿において、METIによるセキュリティ専門官の派遣や、IPAによるAppGoatの使用方法等の派遣講義を検討中。**

４．ニーズとシーズをマッチングしてビジネスにつなげる
セキュリティビジネスエコシステム創造パッケージ

アクションプラン(2018年５月)	取組の進捗
(１)『コラボレーション・プラットフォーム』の設置	(A)コラボレーション・プラットフォーム設置・継続 ①**2018年６月、IPAに設置。以後、１～２か月に一度のペースで開催** ②地方展開に向けた検討
(２)『実戦的サイバーセキュリティ検証基盤』の構築	(B)2019年度本格実施に向けた事前調査等を実施 評価の方向性や対象等を明確化 2019年度、**「サイバーフィジカルセキュリティ対策促進事業（新規）」**により検証基盤を構築
(３)「質の高いインフラ輸出戦略」にサイバーセキュリティの位置付けを明確化	(C)**情報セキュリティサービス審査登録制度**の立上げ ４つのサービス分類について基準を定め、基準に適合するサービスを台帳で掲載

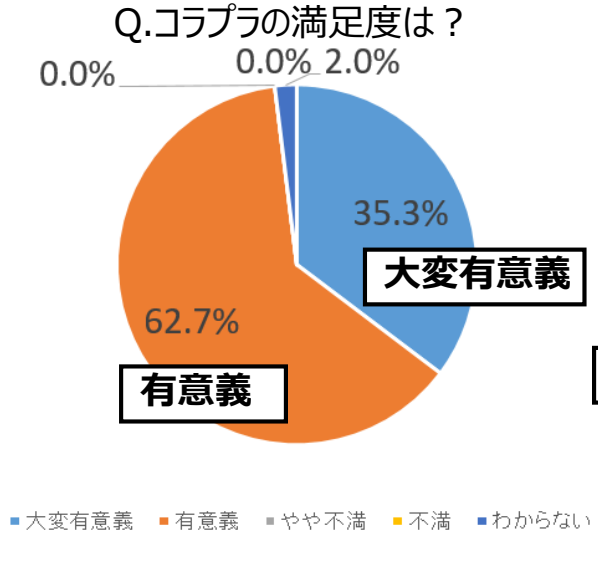
(A)官民の対話の場としてのコラボレーション・プラットフォームの開催

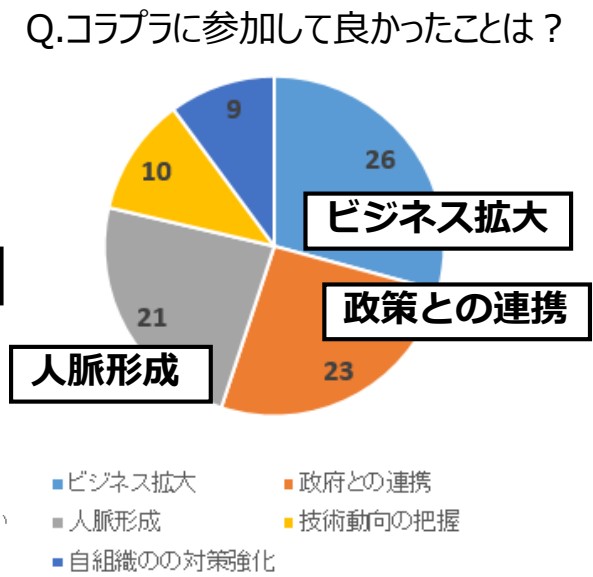
- 各WGの活動などを通じて顕在化したニーズとシーズをマッチングする“場”となる『**コラボレーション・プラットフォーム**』を**IPAに設置し、2018年6月から活動を開始。**

（参考）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。

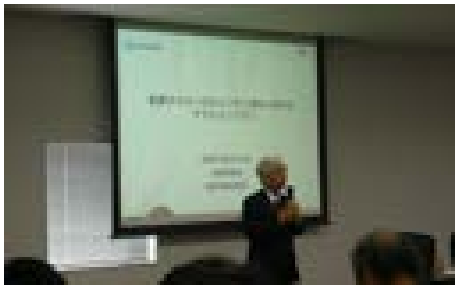
	日にち	参加人数(*)
第一回	6月13日	179名（99名）
第二回	7月23日	104名（74名）
第三回	9月3日	132名（69名）
第四回	10月16日	151名（56名）
第五回	11月30日	98名（40名）
第六回	1月25日	108名（48名）
第七回	3月4日	114名（42名）
第八回	4月23日	ー





※第五回コラボレーション・プラットフォームアンケートより

(*)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)

（詳細はIPAのサイトを参照）https://www.ipa.go.jp/security/announce/collapla_index.html

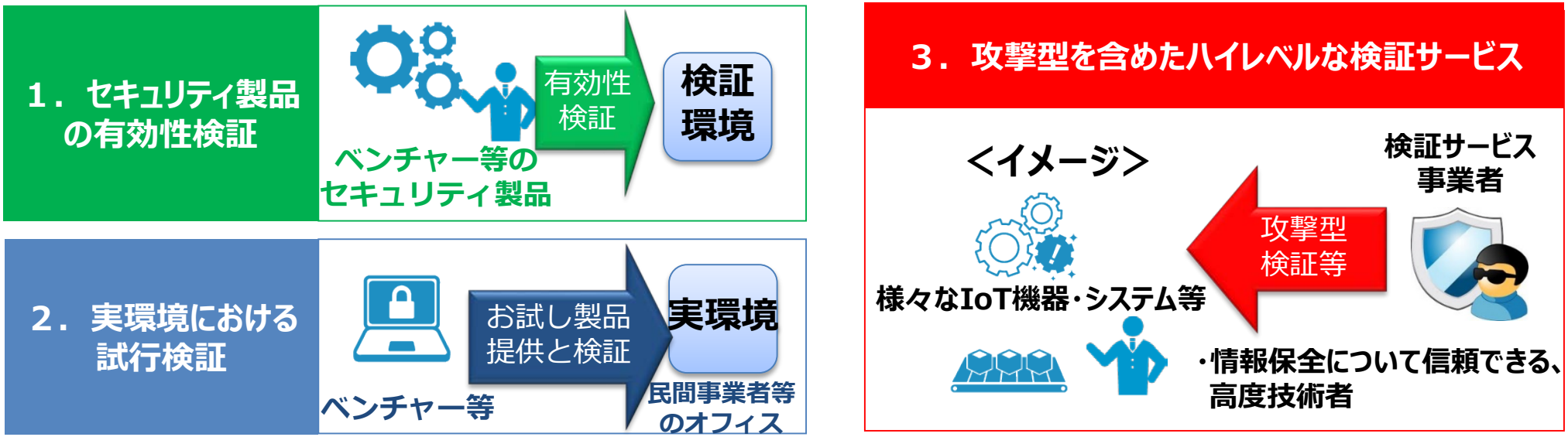
(B)包括的なサイバーセキュリティ検証基盤を構築し、『Checked by Japan（Proved by Japan）』を促進

再掲

- 「**Checked by Japan**」では、2つの方向を追求し、**セキュリティビジネスの成長を促進**。

① 有効性確認等を通じ、日本発のサイバーセキュリティ製品のマーケット・インを促進

② IoT機器等の信頼性を高度に検証するハイレベル検証サービスの拡大

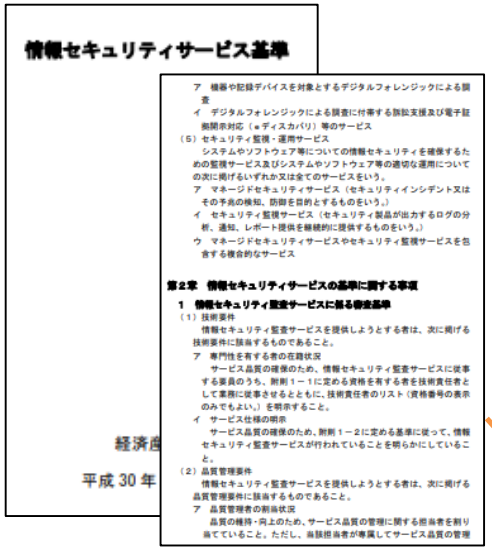


信頼できる
セキュリティ製品・サービス

世界に貢献する
高水準・高信頼の検証サービス

(C) 情報セキュリティサービス審査登録制度の構築・運用

- 一定の品質を維持・向上するための要件を定めた「情報セキュリティサービス基準」を策定し、基準に適合するサービスの台帳をIPAより公開（2018年6月）。
- 政府調達や税制・補助金において台帳の活用を推奨。



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

サービス名称	事業者 ①名称 ②所在地	登録年月日	リスト掲載期限	審査登録機関名
監査およびアシュアランス	①PwCあらた有限責任監査法人 ②東京都千代田区大手町1-1-1 大手町パークビルディング	2018/6/12	2020/6/11	日本セキュリティ監査協会(JASA)
情報セキュリティ監査サービス	①エヌ・ティ・ティ・データ先端技術株式会社 ②東京都中央区月島１－１５－７	2018/6/12	2020/6/11	日本セキュリティ監査協会(JASA)
情報セキュリティプランニング	①株式会社ラック ②東京都千代田区平河町２丁目16番1号平河町森タワー	2018/6/12	2020/6/11	日本セキュリティ監査協会(JASA)
	①株式会社ディアイティ			日本セキュリティ監査協会

100サービスが掲載（4月17日時点）
- 情報セキュリティ監査（22サービス）
- 脆弱性診断（37サービス）
- デジタルフォレンジック（16サービス）
- セキュリティ監視・運用（25サービス）