経済産業省
Ministry of Economy, Trade and Industry

産業分野における
サイバーセキュリティ政策

経済産業省　商務情報政策局
サイバーセキュリティ課
鴨　田　浩　明

１．サイバー攻撃の動向

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．WG1：「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．WG2：サイバーセキュリティ対策の基盤整備
～経営、人材育成、中小企業

５．WG3：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

(独)情報処理推進機構：情報セキュリティ10大脅威 2020

昨年順位		個　人	順　位	組　織	昨年順位	
↗	ランク外	スマホ決済の不正利用 NEW	1位	標的型攻撃による情報流出	1位	→
→	2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位	↗
↘	1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位	↘
↗	7位	インターネットバンキングの不正利用	4位	**サプライチェーンの弱点を悪用した攻撃**	4位	→
↘	4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位	↘
↘	3位	不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位	↗
↘	5位	ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）	10位	↗
→	8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取	7位	↘
↘	6位	偽警告によるインターネット詐欺	9位	IoT機器の不正利用	8位	↘
↘	12位	インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止	6位	↘

<出典：情報処理推進機構、2020.1.29.>

ASUS社端末におけるアップデート機能を悪用した攻撃
（サプライチェーンを通じた攻撃（水平的脅威））

- 台湾のIT機器大手ASUS社※1において、正規のアップデートサーバが攻撃を受け、当該サーバから**端末向けに配布されたアップデートファイルを介し、数十万の同社端末がマルウェアに感染**する事案が発生。
  （出典：MOTHERBOAR誌にてKim Zetter氏執筆。さらにKaspersky社が本件の簡易レポート発出。）
- 正規のダウンロード経路を悪用した同様の攻撃は、2017年に「CCleaner※2」においても発生しており、**マルウェア感染経路の一つ**として警戒を要する。

※1 ASUS社：台北市に本社を置く大手PC、スマートフォン、周辺機器製造メーカー。ソニー、アップル、HP、EPSON等への部品供給も行う。
※2 CCleaner：ハードディスク内部の不要なファイルやレジストリを削除するためのツール。イギリスの Piriform Ltd. が開発。

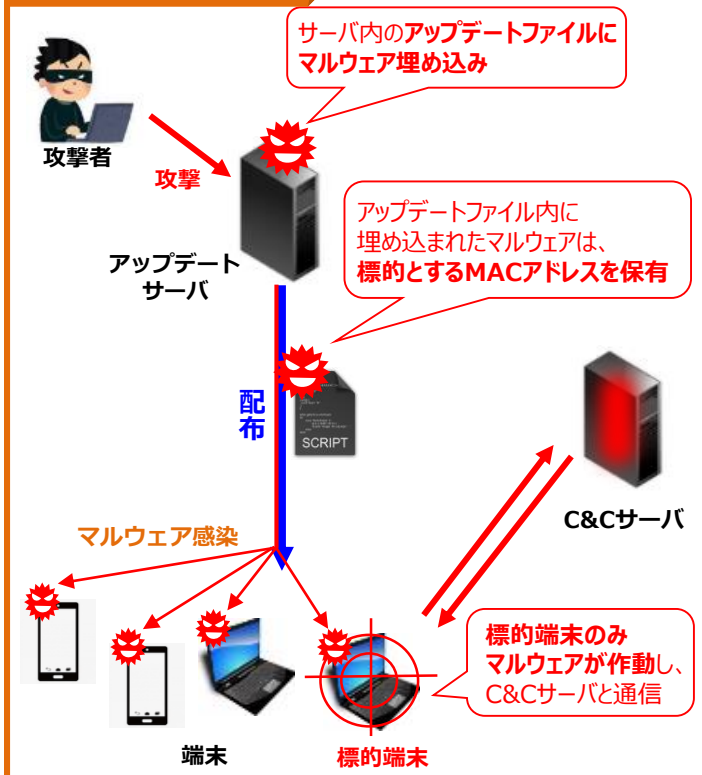
本事案の詳細（原因・影響）

- 本攻撃は**2018年6月から11月**にかけて発生。「Shadow Hammer」と呼ばれる。
- 「ASUS Live Update Utility（アップデートサーバ）」による**ソフトウェアアップデートを経由**し、**マルウェア（バックドアファイル）**が**数十万のASUS端末**に感染。　※Kaspersky社は数百万に上る可能性も指摘
- 本攻撃の大きな特徴として、**マルウェアは標的とする端末のMACアドレスをあらかじめ保有**しており、**感染端末のMACアドレスを参照し、それが標的端末であるかを識別**していた。
  ※Kaspersky社は、200の検体サンプルから600の標的MACアドレスを確認している由
- 識別の結果、**マルウェア感染端末が標的端末であった場合、C&Cサーバと通信を開始する攻撃手法**。実際に標的端末が感染。

✓ 標的端末以外ではマルウェアを作動させないことで、事案の発覚を遅らせる狙いがあるとみられる。

✓ 攻撃者はMACアドレスにより、生産ロット等から標的とする特定の出荷先を絞り込んだものと推測される。

事案のイメージ



OSSライブラリに悪意のあるコードが仕込まれる：Copay

- 仮想通貨（暗号資産）のウォレットアプリ「Copay」にユーザーの仮想通貨を盗み出すバックドアが仕掛けられて公開されていた。
- 攻撃者はCopay本体ではなく、Copayが利用する外部ライブラリの一つ（event-stream）を正規の権限で編集し、悪意のあるコードが仕込まれた外部ライブラリ（flatmap-stream）に関連させることでバックドアを仕掛けた。
- 悪意あるコードを追加する工程を複雑にし、かつ隠蔽を行うことで発覚を遅らせようとした。

2017.10 ・開発者によるevent-streamの最終更新

⋮

2018.8末 ・攻撃者がevent-streamの開発者に**「メンテナンスを引き継ぎたい」と持ちかけメンテナンス権限を取得**

2018.9.9 ・攻撃者がevent-streamを更新 → event-streamがflatmap-streamと関連

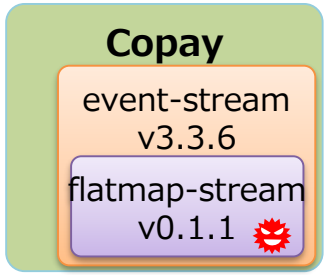
2018.10.5 ・攻撃者がflatmap-streamに**悪意のあるコードを追加**

2018.10.26 ・Copayが更新

→ Copayが悪意のあるコードが仕込まれたflatmap-stream に関連するようになり、攻撃者がバックドアを利用できるように

⋮

2018.11.26 ・ニュースになり、 flatmap-streamは削除された



サイバー攻撃の脅威レベルの増大（制御系にまで影響が波及）
（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））

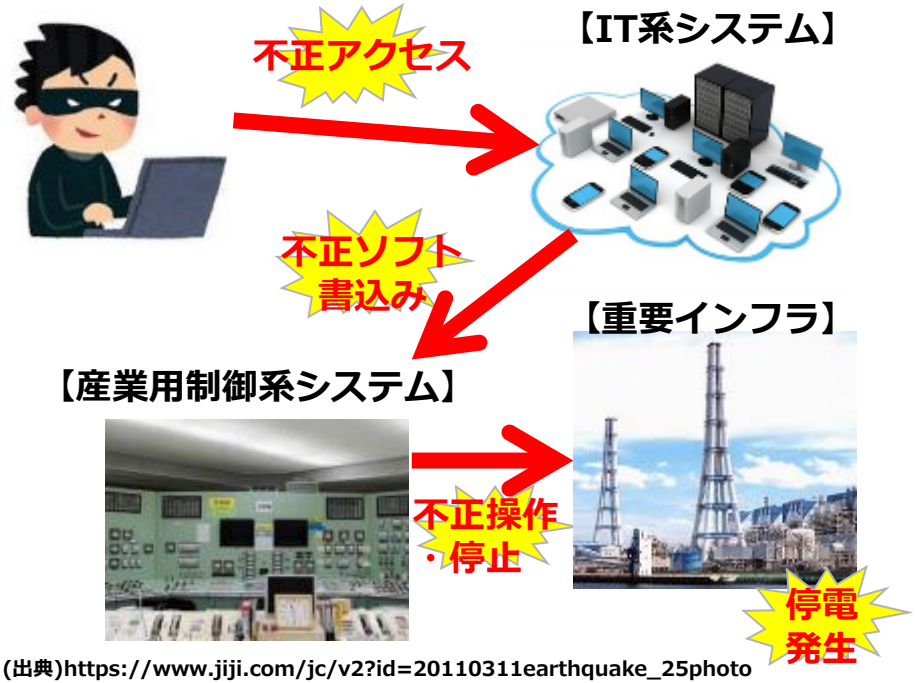
- 米国ICS-CERTの報告では、**重要インフラ事業者等において、制御系にも被害が生じている**。
- ウクライナでは、2015年と2016年にサイバー攻撃による停電が発生。**2016年の攻撃(CrashOverRide)**では、**サイバー攻撃のみで、停電が起こされた**。

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

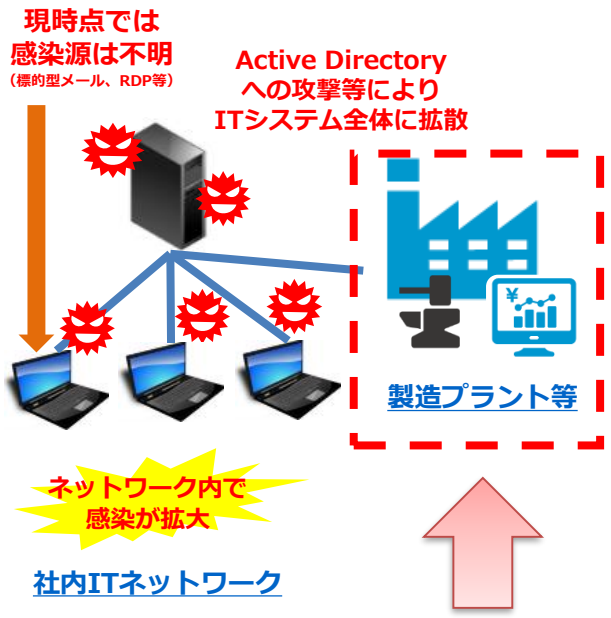
ランサムウェア(LockerGoga)によるノルウェーのアルミ精錬・加工企業への事業被害（情報システムを越えて制御システムに達する攻撃（垂直的脅威））

- 2019年3月、ノルスク・ハイドロ社（ノルウェーを拠点とする世界最大級のアルミニウム製錬・加工企業）が、 ランサムウェア「LockerGoga」による被害を受けた。
- アルミニウム製造・発電プラントのITシステムからの切り離し及び手動操作への切り替え、プレス加工等の一時的な生産停止など、**感染確認から1週間で4000万ドルに相当する事業被害。**

本事案の詳細（原因・影響

- 2019年3月19日、**ノルスク・ハイドロ社はランサムウェア「LockerGoga」への感染・大規模なシステム障害**を発表。
- 感染経路は不明（2019年３月時点）。
- ログオンシステム（ADサーバ）への攻撃を通じた感染拡大により、ほとんどの事業部門のITシステムが影響。
- **感染拡大・拡散防止のため、グローバルなITシステム全体を停止**。
- オフィス業務への影響の他、**プレス加工等の一時的な生産停止や、アルミニウム製造や発電プラントをITシステムから切り離して手動操作に切り替えるなどの影響**が生じた。
- 身代金の支払いには応じていないが、**感染の確認から1週間で4000万ドルに相当する事業への被害を確認**。

事案のイメージ



１．サイバー攻撃の動向

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．WG1：「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．WG2：サイバーセキュリティ対策の基盤整備
　～経営、人材育成、中小企業

５．WG3：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

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
アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
アクションプランを加速化する３つの指針を提示

構成員

※2019年4月開催時点

- **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
- **泉澤　清次**　三菱重工業株式会社取締役社長
- **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
- **篠原　弘道**　日本電信電話株式会社取締役会長
- **中西　宏明**　株式会社日立製作所会長
- **船橋　洋一**　アジア・パシフィック・イニシアティブ理事長
- **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

WG１（制度･技術･標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日

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　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日

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）

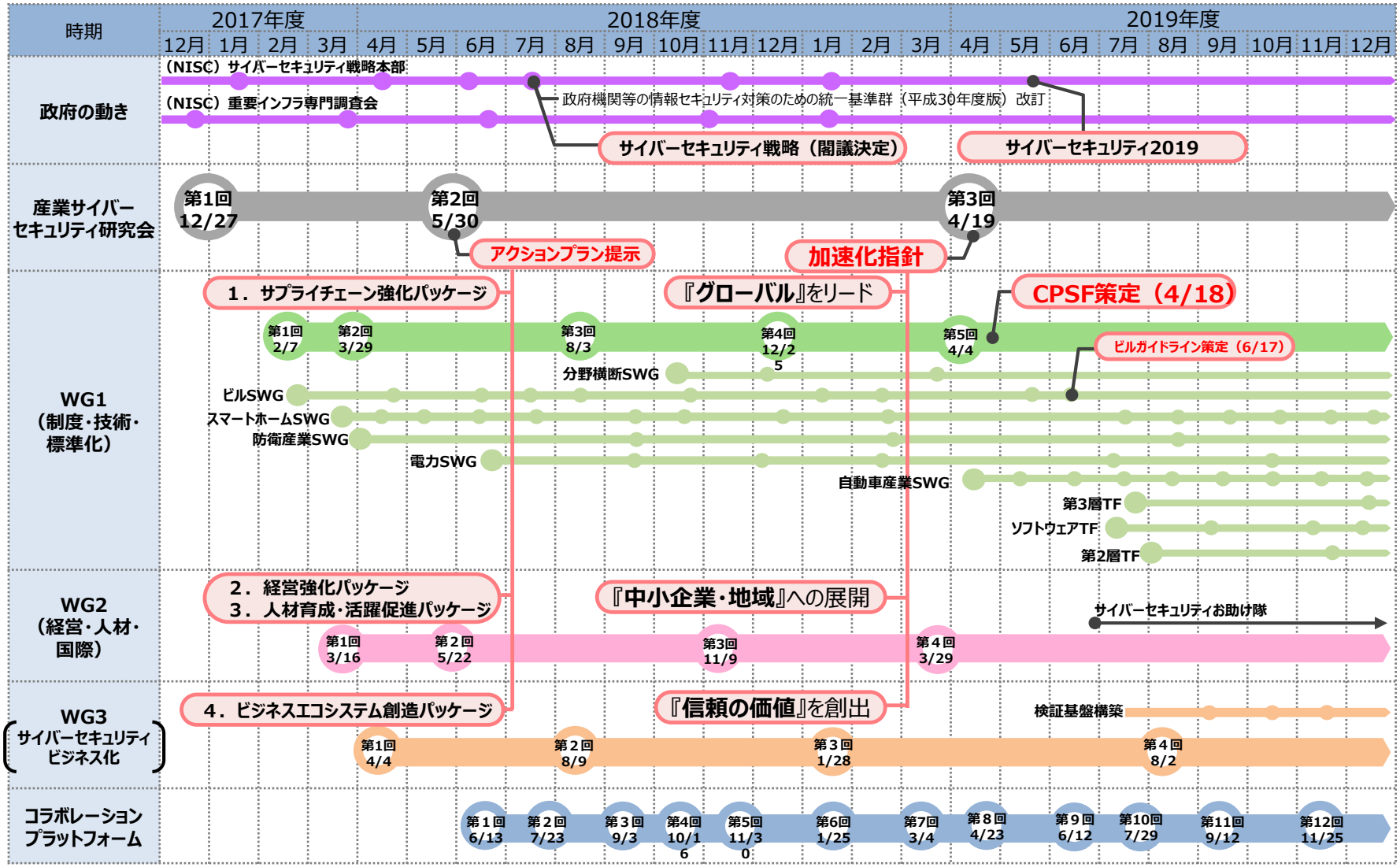
第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

産業サイバーセキュリティ研究会関連の動き



１．サイバー攻撃の動向

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．WG1：「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．WG2：サイバーセキュリティ対策の基盤整備
～経営、人材育成、中小企業

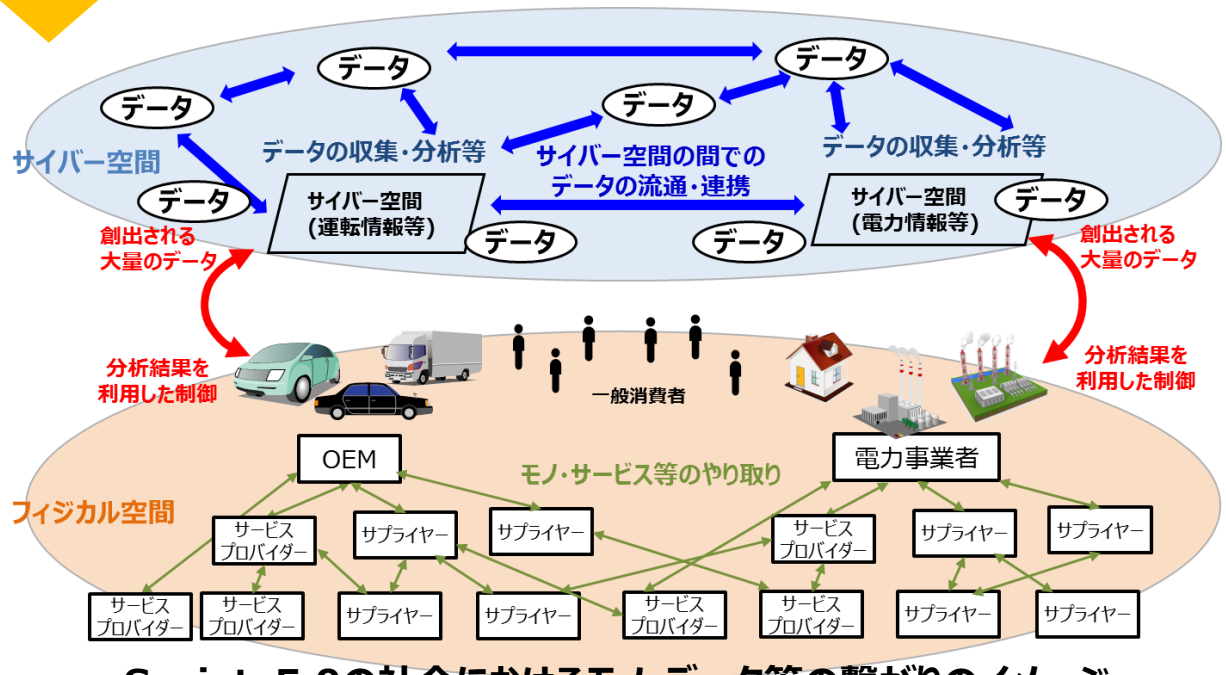
５．WG3：サイバーセキュリティビジネスの創出
～エコシステムの構築

サイバー・フィジカル・セキュリティ対策フレームワークの策定
＜サプライチェーン構造の変化＞

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**となる。

「Society5.0」以前

個々の企業主体の定型的なつながりで価値を生み出す



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

＜三層構造と６つの構成要素＞
サイバー・フィジカル一体型社会のセキュリティのためにCPSFで提示した新たなモデル

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造**と**６つの構成要素**）を提示。

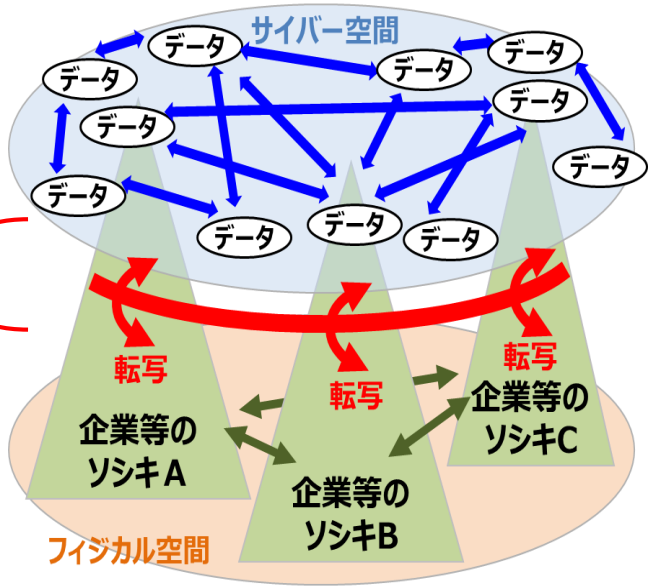
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

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**データの信頼性**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”する機能の信頼性**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
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保



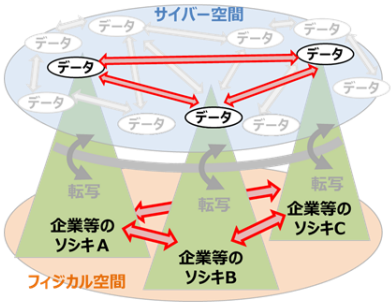
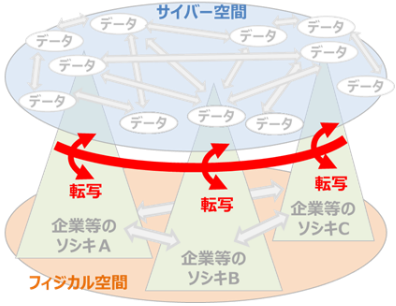
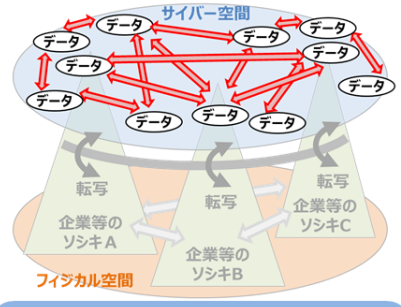
６つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を６つに整理**

構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	• ハードウェア、ソフトウェア及びそれらの部品 操作する機器を含む
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の一連の活動の手続き
システム	• 目的を実現するためにモノで構成される仕組み・インフラ

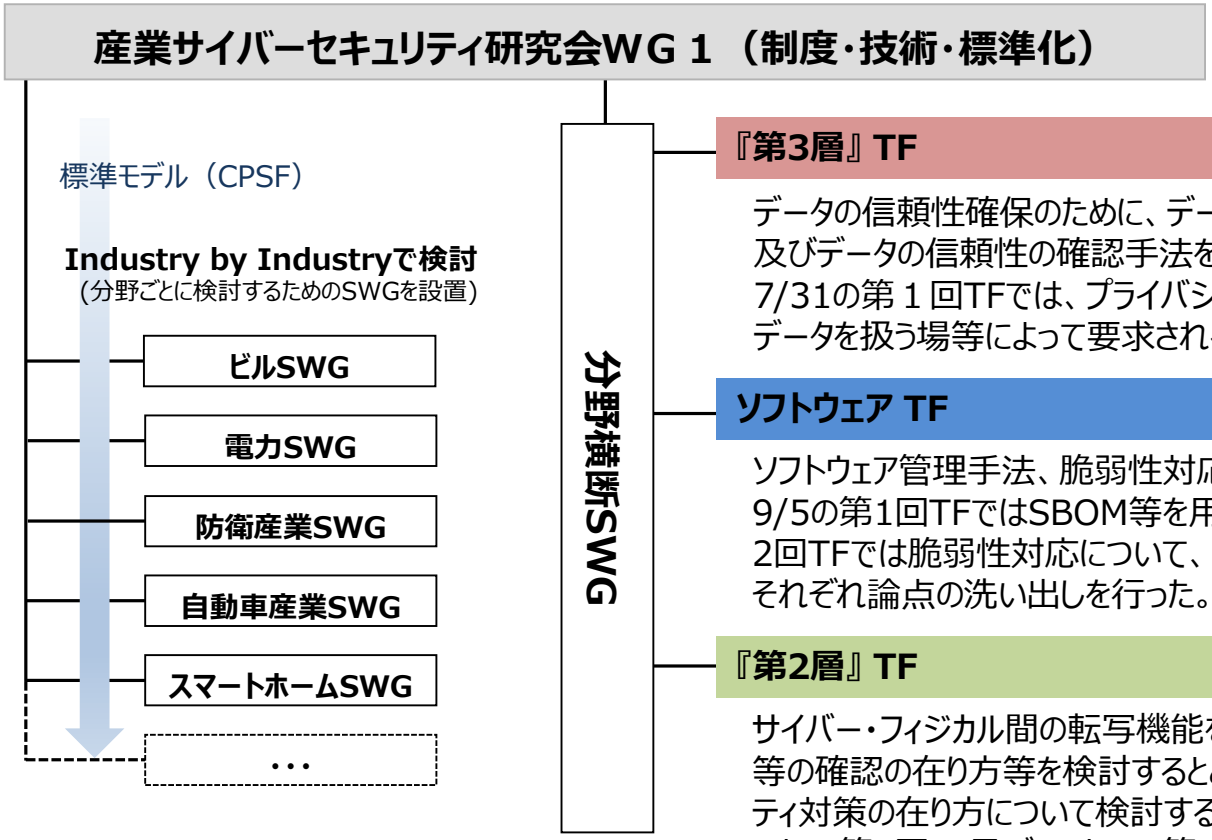
＜CPSFの全体概要＞
三層構造モデルに基づきリスク源、対応方針等を提示

- サプライチェーンの信頼性を確保する観点から、産業社会を３つの層から捉え、それぞれにおいて**守るべきもの、直面するリスク源、対応方針**等を整理。

	企業間のつながり【第１層】	フィジカル空間とサイバー空間のつながり【第２層】	サイバー空間におけるつながり【第３層】
新たなサプライチェーン構造の整理			
機能（守るべきもの）	• 平時及び緊急時のリスク管理・対応体制の構築と運用 • 企業内及び企業間のリスク管理・対応体制の構築と運用	• フィジカル空間とサイバー空間の境界における情報の正確な転写及び正確な転写の証明	• データの加工・分析 • データの保管 • データの送受信
セキュリティインシデント	• 保護すべき資産の棄損 • 他組織のセキュリティ事象発生に起因する事業停止	• 不正確なデータの送信 • 安全に支障をきたす動作	• 保護すべきデータの漏えい • なりすまし等による不正な組織からのデータ受信
リスク源（構成要素ごとに整理）	• セキュリティリスクに対するガバナンスの欠如 • 他組織との連携状況の未把握	• 不正なIoT機器との接続 • 許容範囲外の入力データ	• 通信経路が保護されていない • 通信相手を識別していない
対策要件	■ マネジメントルールの徹底 ■ 関係者との役割分担	■ 接続相手の認証 ■ 安全なIoT機器の導入	■ 暗号化によるデータ保護 ■ データの提供者の信頼性確認

分野別SWG と テーマ別TFの検討状況

- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）を新たに設置**。



『第3層』TF

データの信頼性確保のために、データの区分に応じた適切なセキュリティ対策要件及びデータの信頼性の確認手法を検討する。
7/31の第１回TFでは、プライバシーを含むデータの属性やデータに対する処理、データを扱う場等によって要求されるセキュリティが異なり得ること等を議論。

ソフトウェア TF

ソフトウェア管理手法、脆弱性対応、OSSの利活用等について検討する。
9/5の第1回TFではSBOM等を用いたソフトウェア管理手法について、11/6の第2回TFでは脆弱性対応について、 12/4の第3回TFではOSSの利活用についてそれぞれ論点の洗い出しを行った。

『第2層』TF

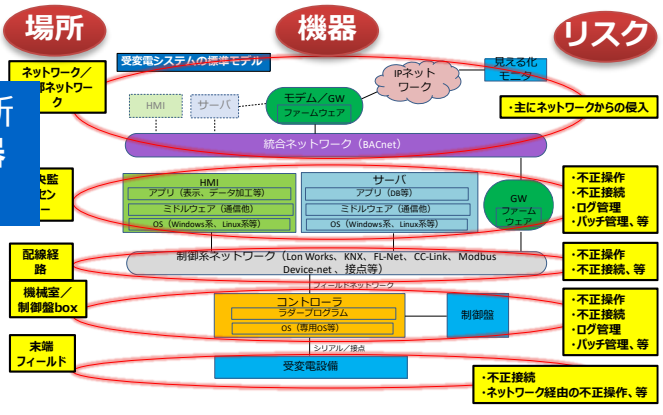
サイバー・フィジカル間の転写機能を持つ機器等について、自己適合宣言・認証等の確認の在り方等を検討するとともに、産業保安・製品安全も考慮したセキュリティ対策の在り方について検討する。
8/2の第1回TF及び11/27の第2回TFでは、安全とセキュリティを併せて考えることの重要性や求められるセキュリティに応じて機器をカテゴライズする必要性等について議論。

（参考）ビルSWG（座長：江崎 浩 東京大学 教授）

- 産業サイバーセキュリティ研究会WG1（制度・技術・標準化）の下の**ビルSWG（ビルオーナー～ベンダまで、ビル関連のステークホルダが参加）**において、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**ガイドラインを作成。2019年6月17日付で第1版を公開。**

- **場所→場所に置かれる機器→機器に想定されるリスク→対策要件→ライフサイクル別の対応策という流れで整理**

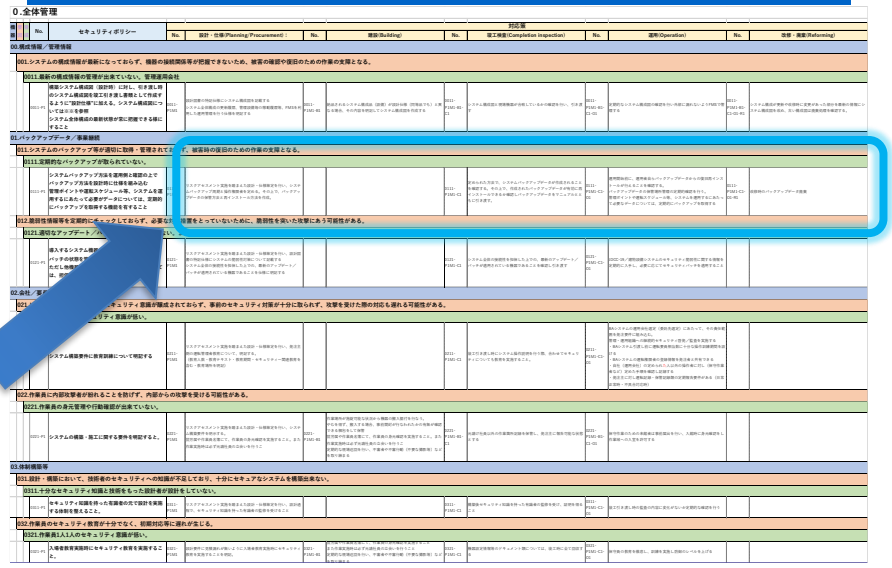
場所及びその場所に設置される**機器等**をリストアップ



4.1	全体管理	
2.	バックアップデータ／事業継続	
3.	会社／要員の管理	
4.	体制構築等	
4.2	組織	
1.	ネットワーク(クラウド、情報系NW、BACnet)	
	10	ネットワーク
	11	クラウドサーバ/Webサーバ
	12	情報系端末
	13	外部接続用ネットワーク機器（FW、ルータ）
	14	ビルシステム間相互接続
2.	防災センター（中央監視室）	
	20	防災センター（中央監視室）
	21	HMI/HIM
	22	保守用持ち込み端末
	23	統合NWにつながるネットワーク機器（FW、ルータ、SW）
	24	システム管理用サーバ（ビルシステム主装置）
3.	機械室／制御盤ボックス	
	30	機械室
	31	コントローラ（DDC、PLC等）
	32	ネットワーク機器（FW、ルータ、SW）
	33	ゲートウェイ機器
	34	各種制御盤・分電盤
4.	配線経路（MDF室、EPS、天井裏ラック）	
	40	MDF室／EPS／天井裏ラック
	41	内部に置かれたネットワーク機器（SW類）
5.	末端装置が置かれる場所	
	50	末端装置

	セキュリティインシデント	リスク源	セキュリティポリシー
1.	構成情報／管理情報		
(1)	ビルシステムへの被害発生時に、被害確認が遅れ、復旧作業の支障となる。	ビルの構成情報が最新状態に管理できておらず、機器の最新の接続関係が把握できない。	・構築システム構成図（設計時）に対し、引き渡し時のシステム構成図を竣工引き渡し書類として作成するように"設計仕様"に加える。 ・システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。
2.	バックアップデータ／事業継続		
(1)	適切なバックアップデータがなく、ビルシステムへの被害発生時に復旧作業の支障となる。	バックアップが取られていないまたはバックアップの範囲や対象が適切でない。	・システムバックアップ方法を運用側と確認の上でバックアップ方法を設計時に仕様を組み込む。 ・管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する機能を具備する。
(2)	システムの脆弱性をついた攻撃を受ける。	脆弱性についての認識が不十分で脆弱性が残ったままの状態になっている。	・既知の脆弱性に対して必要な対策（パ[illegible]現する。 ・ただし、他機器および他システムの正常稼動については、担保しなければならない。
3.	会社／要員の管理		
(1)	ビルシステムへの被害発生時に、迅速な対応ができず、被害が拡大する。	ビル管理会社においてセキュリティへの意識醸成、要員教育が十分ではなく、事前対策や対応準備が出来ていない。	・システム構築要件に教育訓練について明記する。
(2)	ビルシステムが内部作業員等から攻撃を受ける。	作業員等の身元確認や行動監視が不十分で、内部攻撃者が紛れることや攻撃を行うことを防ぐことが出来ていない。	・システムの構築・施工・保守にあたって、作業員等の身元確認や行動確認についての要件を明記する。
4.	体制構築等		
(1)	攻撃等への対応が効果的に出来ず、被害が拡大する。	十分なリスクアセスメントが出来ていないため、リスク対応の運用計画や体制が十分なレベルで構築できていない。	・リスクアセスメントを実施し、その結果を基に監理監査面からの「運用する管理体系」などを運用計画として 定義・整備する。

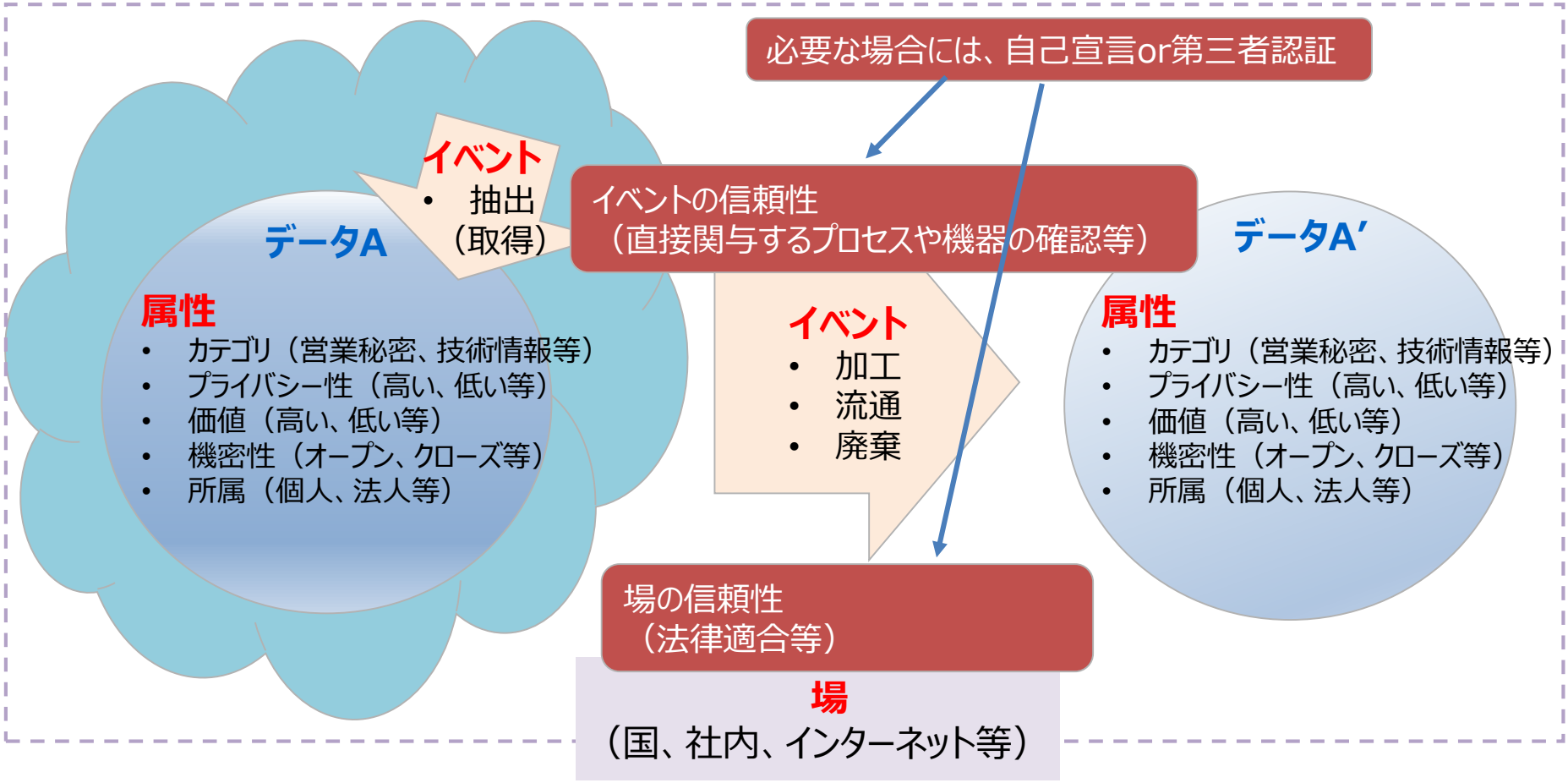
ビルシステムの**ライフサイクルの各フェーズ毎に対策**を展開



場所・機器別の想定される**インシデント**と**リスク源**を整理し、その**対策をポリシーレベル**で整理

第3層TF：データの信頼性の考え方

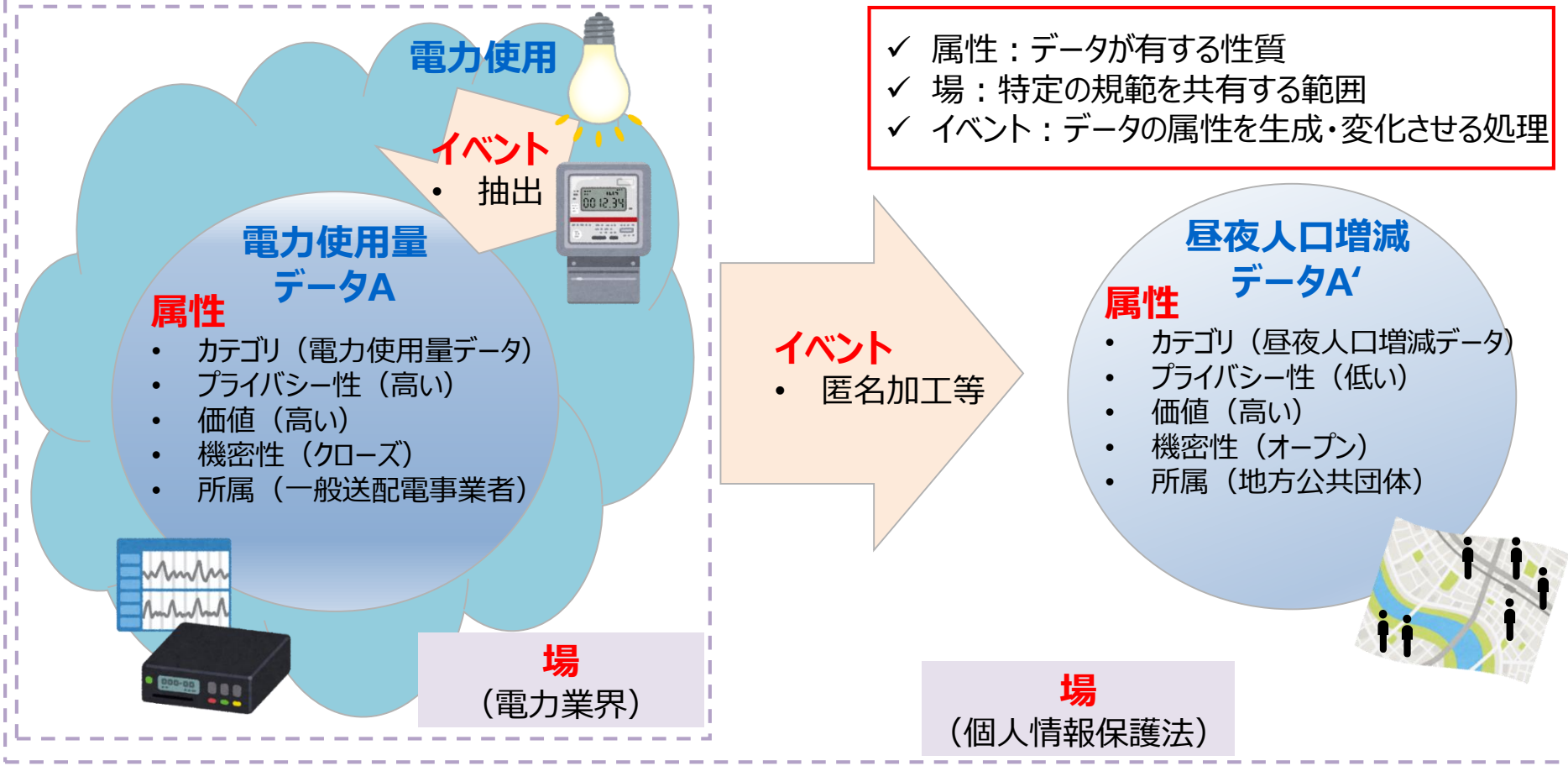
- データの信頼性とは、データの属性に応じて、イベントの信頼性及び場の信頼性を適切に確保すること、と考えてはどうか。



第3層TF：データの信頼性確保のためのセキュリティ要件の考え方

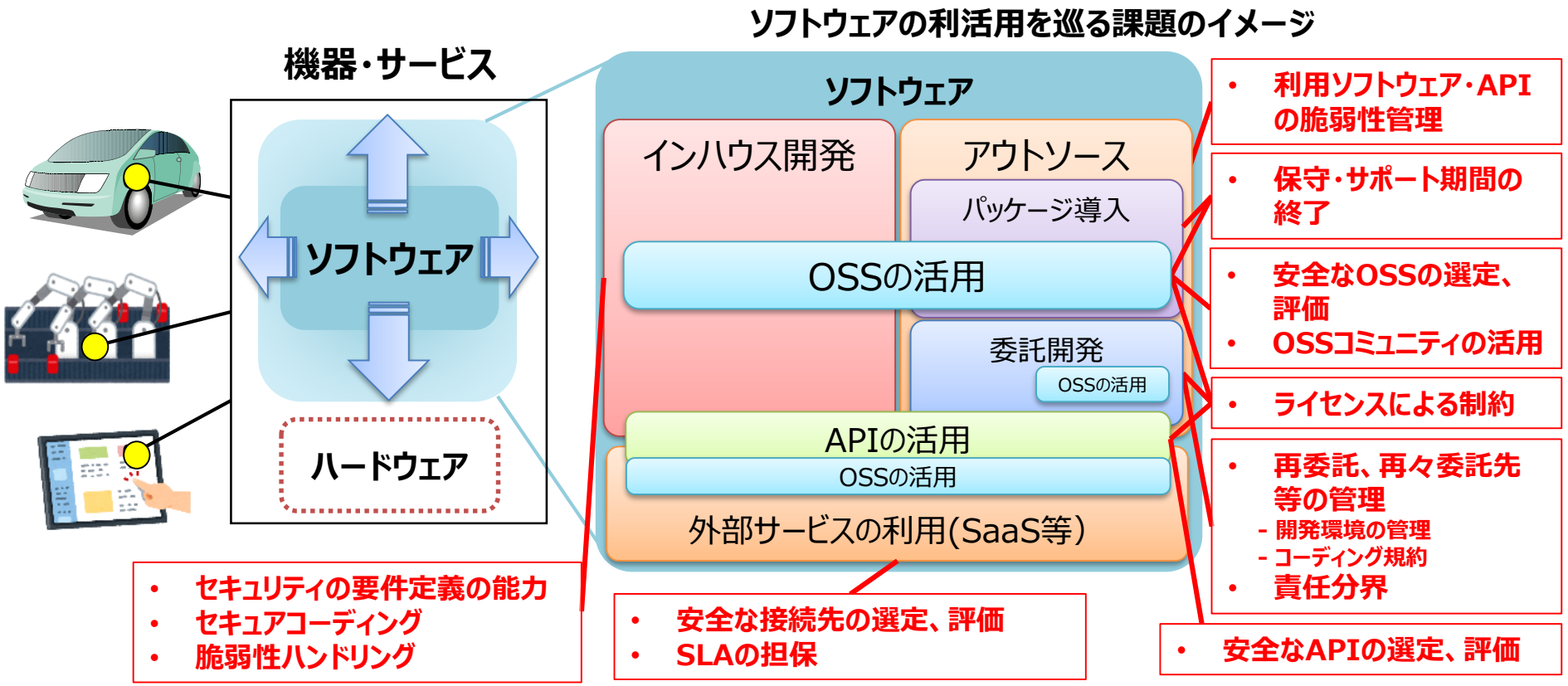
- セキュリティ要件は、データAの**属性**及び対応する**場**、並びに、データA‘へ処理するための**イベント**の影響を受けて決まるのではないか。

電力使用量データから防災等に活用するための昼夜人口増減データへの匿名加工化の想定（イメージ）



第2層TF：ソフトウェアの信頼性確保の検討の方向性

- 本タスクフォースにおいて、**米国NTIAのSoftware Component Transparencyの議論との連携を視野に**入れながら、**OSSを安全に活用するための手法、ソフトウェアの脆弱性管理手法等**を検討。



『ソフトウェアTF』における検討の方向性

- **ソフトウェア管理手法、脆弱性対応、OSSの利活用等**に関する検討を行う。

ソフトウェア管理手法の検討

- ソフトウェアの開発から、運用中の脆弱性発見まで
- 構成管理・脆弱性管理に求められるソフトウェア管理手法のあり方
- SBOM等ソフトウェア管理スキームの活用に求められる技術面・制度面の課題

第1回
検討事項

脆弱性対応手法の検討

- 脆弱性が発見された場合のソフトウェアへの対応
- 脆弱性発覚時に必要な脆弱性への対応手法・体制のあり方
- 運用中システムへの脆弱性対応に求められる技術面・制度面の課題

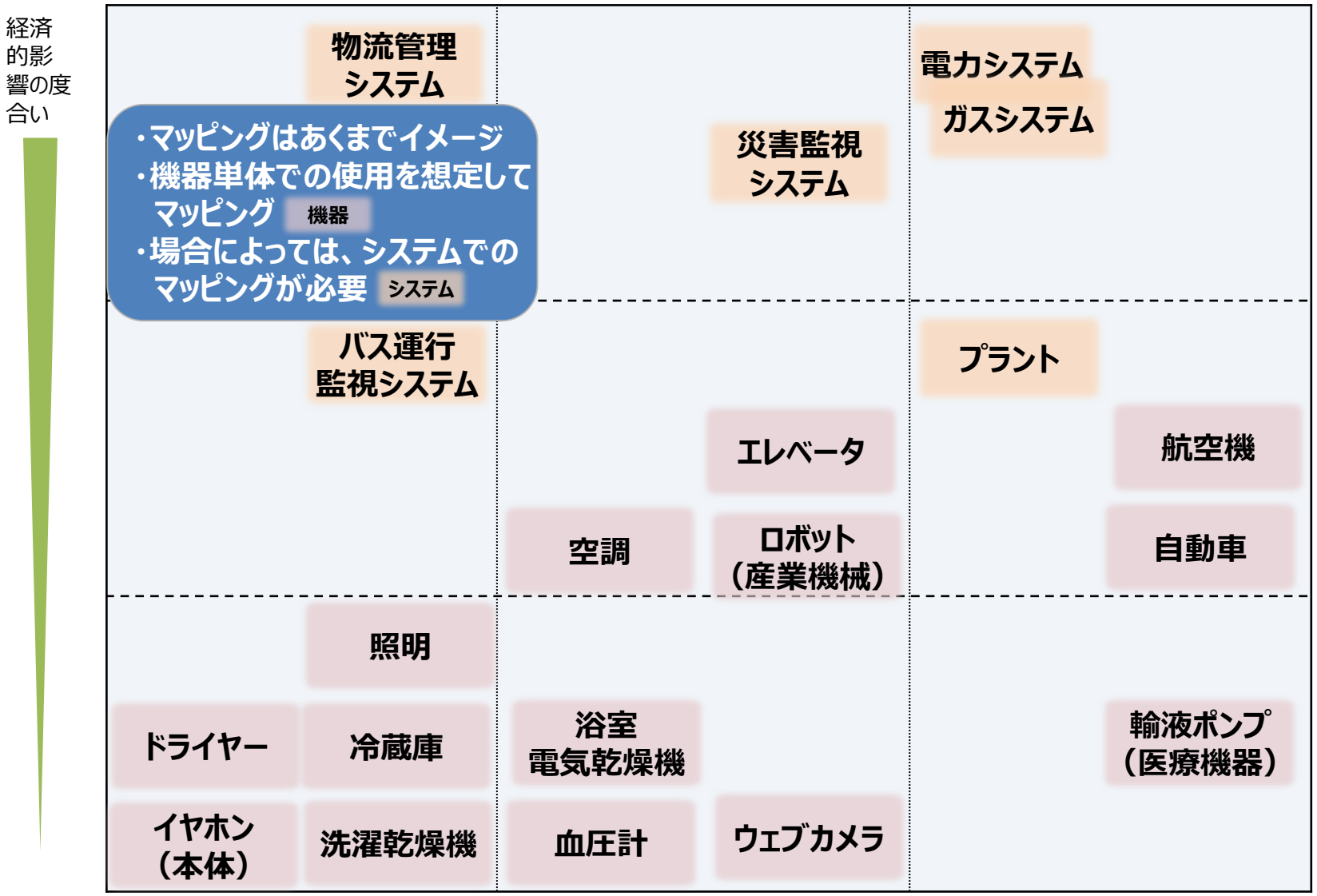
第2回
検討事項

OSSを利活用する際のビジネス的な側面の検討

・OSS利用に関連するライセンスや契約
・OSS活用のベストプラクティス／OSSコミュニティへの発信

第3回
検討事項

第3層TF：サイバー・フィジカル間をつなぐ機器・システムのリスクイメージ

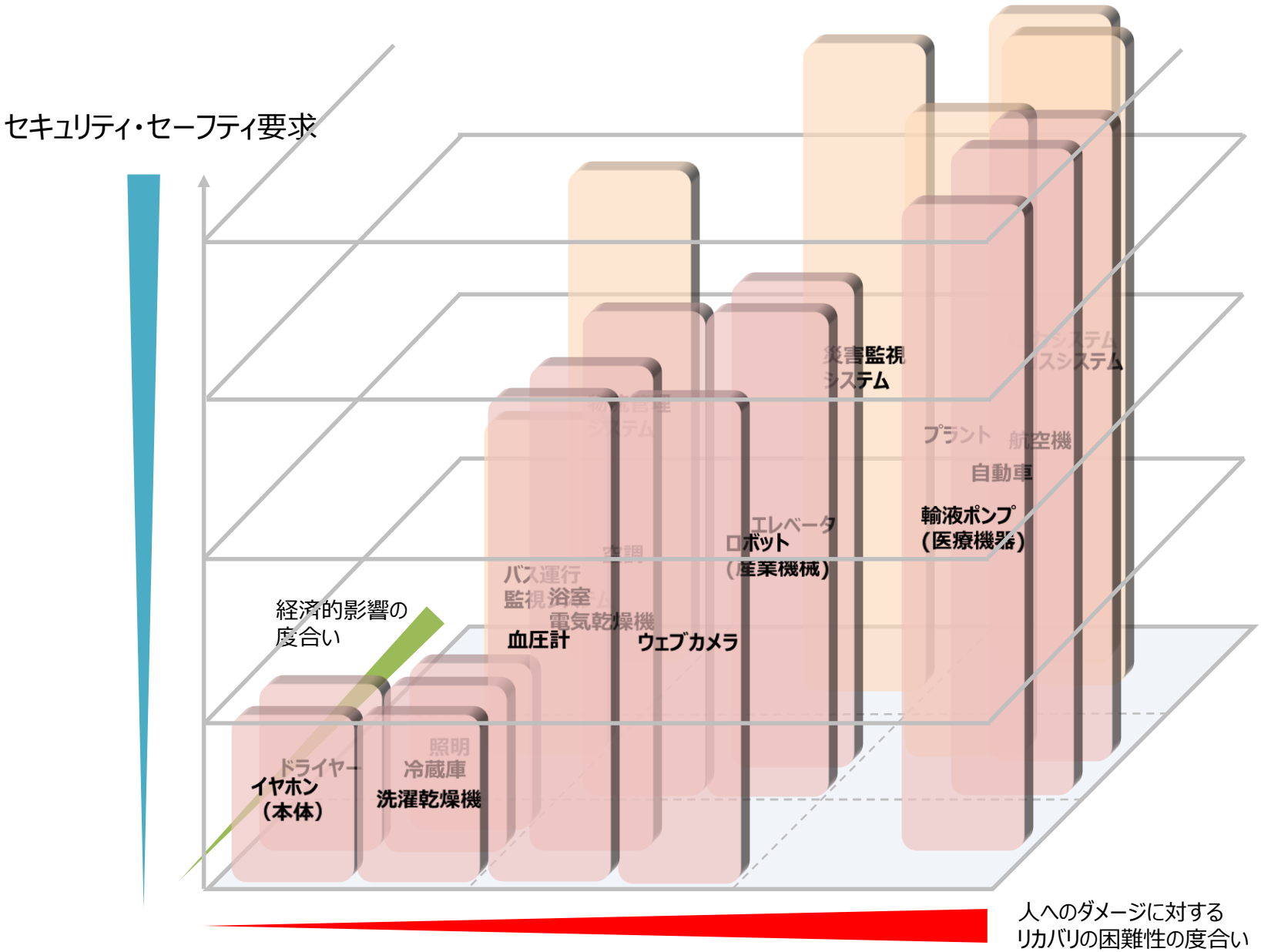


第3層TF：サイバー・フィジカル間をつなげる機器・システムのカテゴライズ基準の例

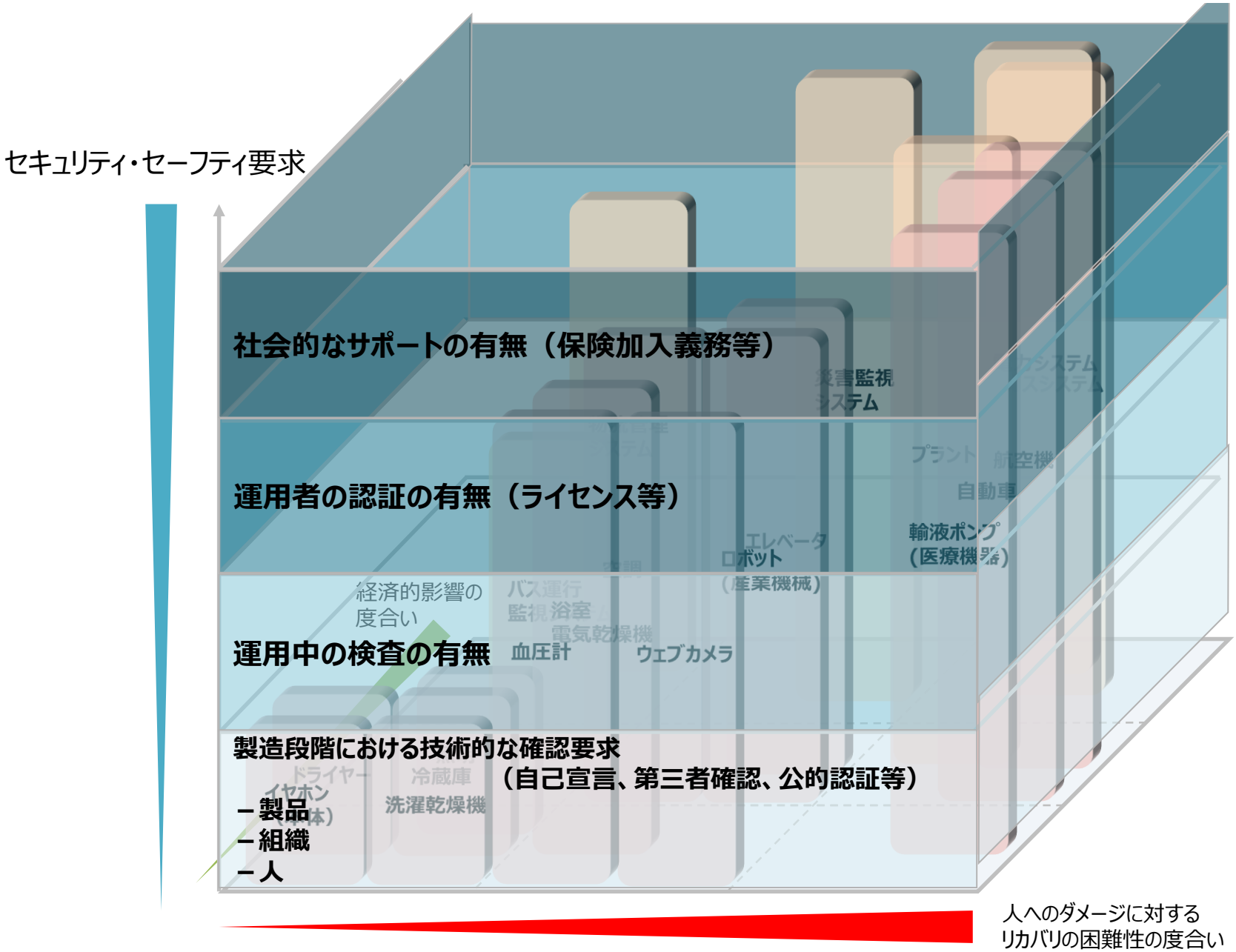
- 指摘のあった観点それぞれについて影響の度合いを整理。他に考慮すべき観点はないか、あるいは、各観点における影響の度合い（レベル）の表現は適切か、検討が必要
- CPSFを適用してリスクアセスメントを実施する際に、これらの観点が利用可能ではないか。

基準		それぞれの観点におけるカテゴライズ基準の例					
		ダメージに対するリカバリの困難性の度合い	経済的影響の度合い				
		人命/安全	プライバシー	資産	生活影響	社会影響	レピュテーション
Lv. 1	限定的な影響	軽傷	漏えい、悪用	損害	不便	悪影響	信用低下
Lv. 2	重大な影響	重傷	名誉毀損	大損害	支障	混乱	業績悪化
Lv. 3	致命的・壊滅的な影響	人命への影響	人命への影響	破産	困難	大混乱	倒産

第3層TF：カテゴリに応じて求められるセキュリティ・セーフティ要求の強度のイメージ



第3層TF：カテゴリに応じて求められるセキュリティ・セーフティ要求の強度のイメージ



１．サイバー攻撃の動向

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．WG1：「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

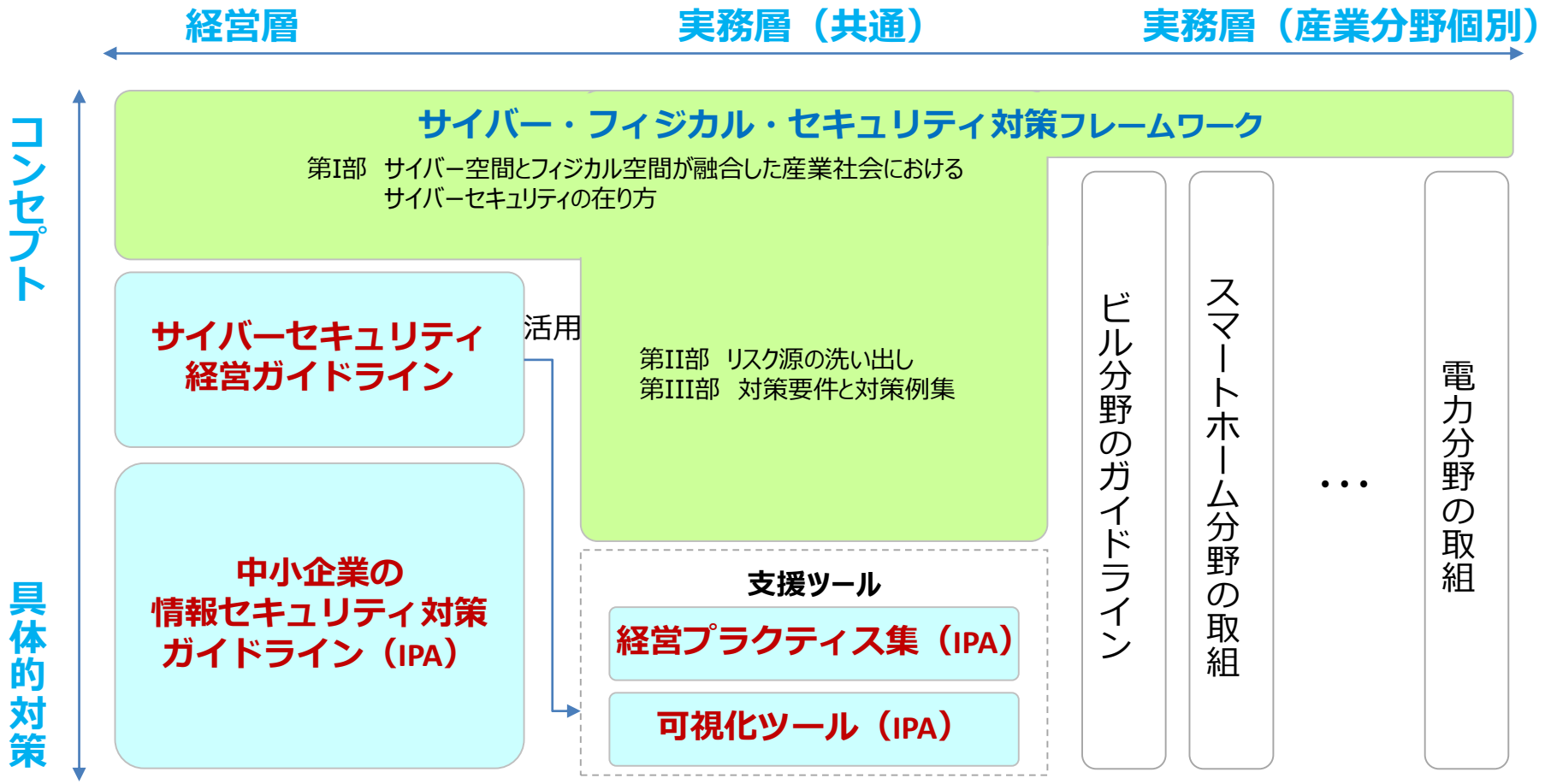
４．WG2：サイバーセキュリティ対策の基盤整備
～経営、中小企業、人材育成

５．WG3：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」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＞



経営者にサイバーセキュリティ経営を促す仕組み『 3 Steps 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

概要

経営者が適切なセキュリティ投資を行わないと…

- 社会からリスク対応の是非が問われる
- 経営責任や法的責任が問われる
- 国際的なビジネスに影響をもたらす

セキュリティ対策の実施を
「コスト」と捉えるのではなく「投資」と捉える

経営戦略としての**セキュリティ投資は必要不可欠**
かつ**経営者としての責務**

経営者が認識する必要がある 三原則

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

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

平時および
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

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）

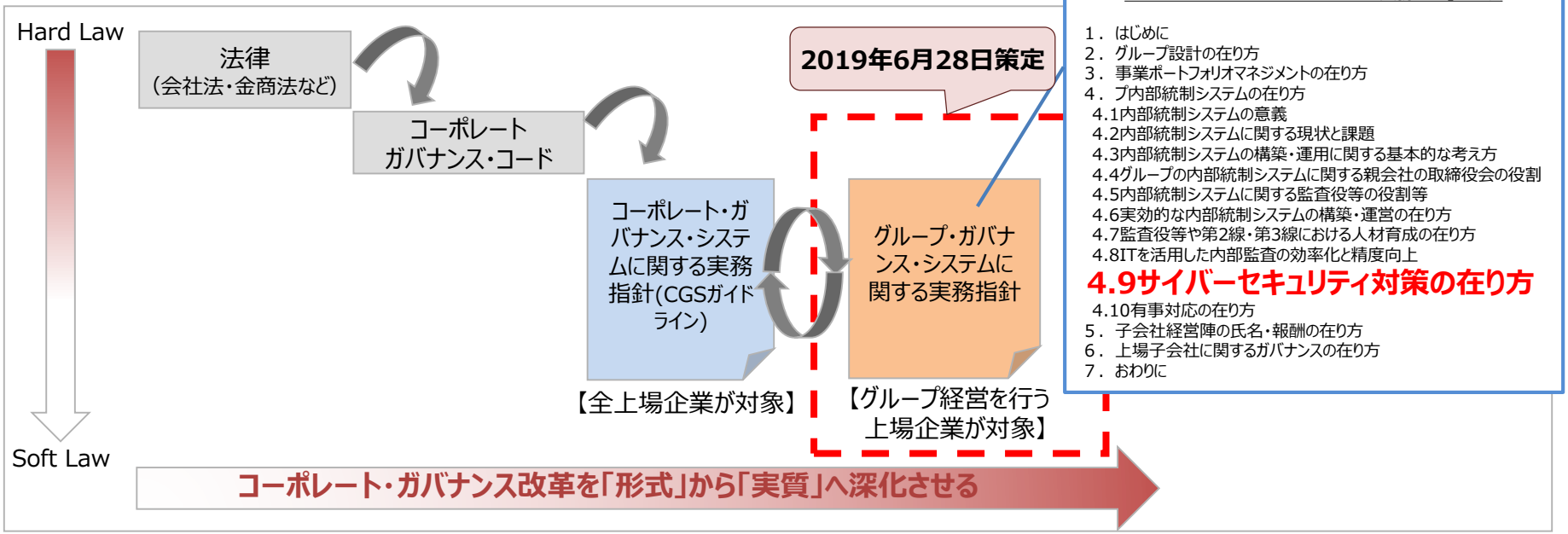
- 経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき**重要10項目**

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
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
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
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および状況
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および提供

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。
- 「グループ・ガバナンス・システムに関する実務指針(グループガイドライン)」において、**グループ内部統制システムの一つとして、サイバーセキュリティ対策の在り方を位置づけ**。(2019年6月公表)
- 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行うことを検討すべき**ことを明記。

<ご参考> グループ・ガバナンス・システムに関する実務指針の立ち位置



（出典）第13回CGS研究会資料より抜粋

『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

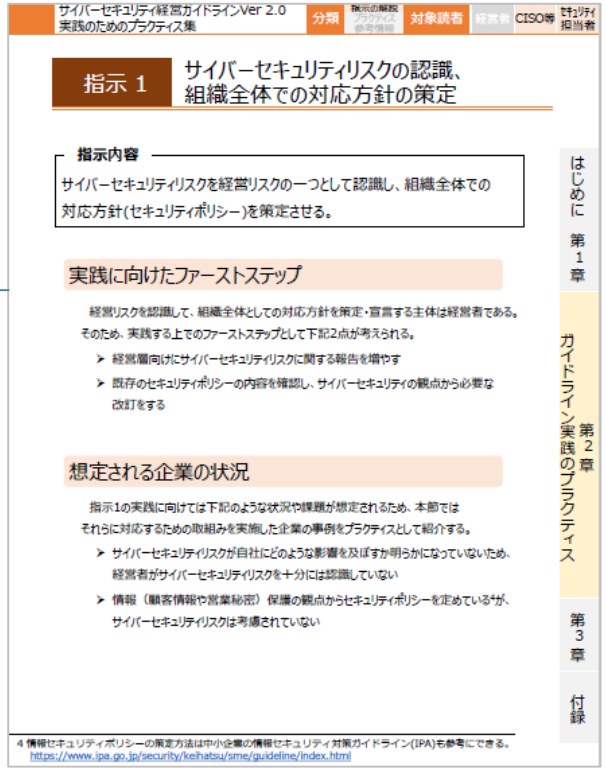
＜経営者、CISO等向け＞
なぜサイバーセキュリティが経営課題となるのか等を解説

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

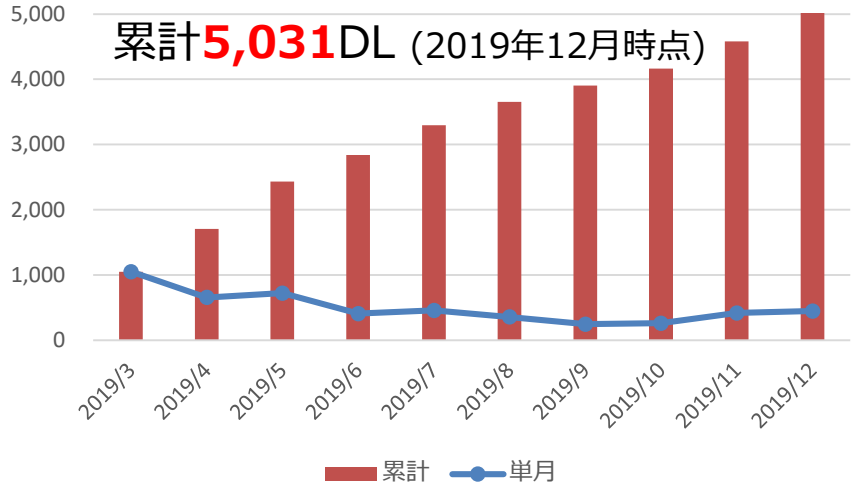
＜セキュリティ担当者向け＞
サイバーセキュリティ対策を実践する上での悩みに対する、企業の具体的な取組事例を紹介



（参考）『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』のアップデート状況

- 2019年3月25日にIPAより公開した「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」について、昨年度収集していない指示項目を中心にプラクティスを収集中であり、**今年度中にアップデート版を公開予定。**

<プラクティス集のダウンロード数推移>



【参考】上場企業数　第一部　2,157社
　　第二部　488社
（日本取引所グループ公表 2019年12月17日時点）

【参考】プラクティス集　目次

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

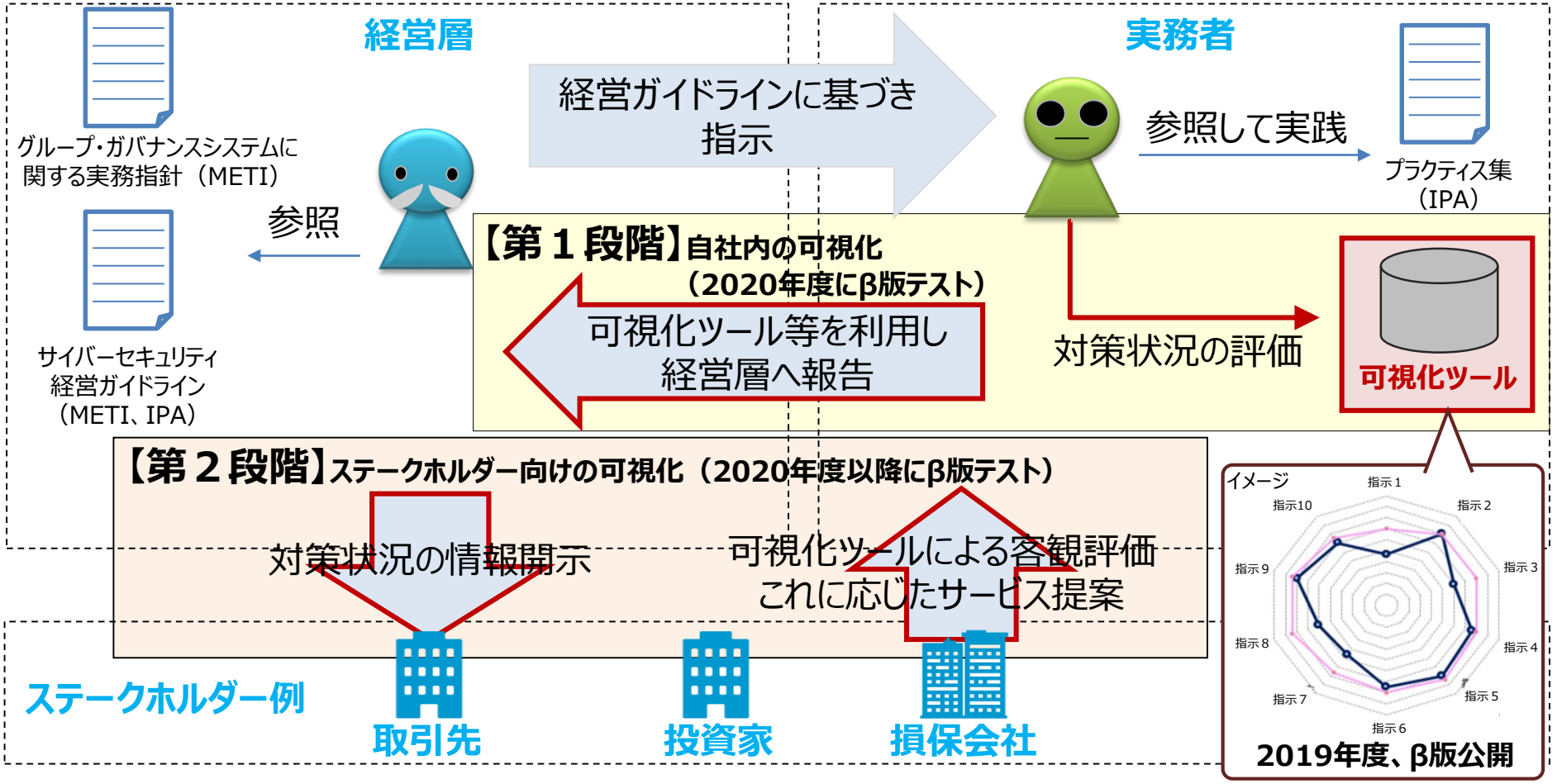
<セキュリティ担当者向け>
サイバーセキュリティ対策を実践する上での悩みに対する、企業の具体的な取組事例を紹介

<今年度アップデート予定の指示項目>

- 指示4　リスクの把握と対応計画策定（リスクアセスメント手法）
- 指示6　PDCAの実施（リスク管理に関するKPIの定め方、是正措置の実施方法、情報開示の手法）
- 指示10　情報共有活動への参加（情報の提供方法、入手した情報の活用方法）

可視化ツールの作成により目指すサイバーセキュリティ経営

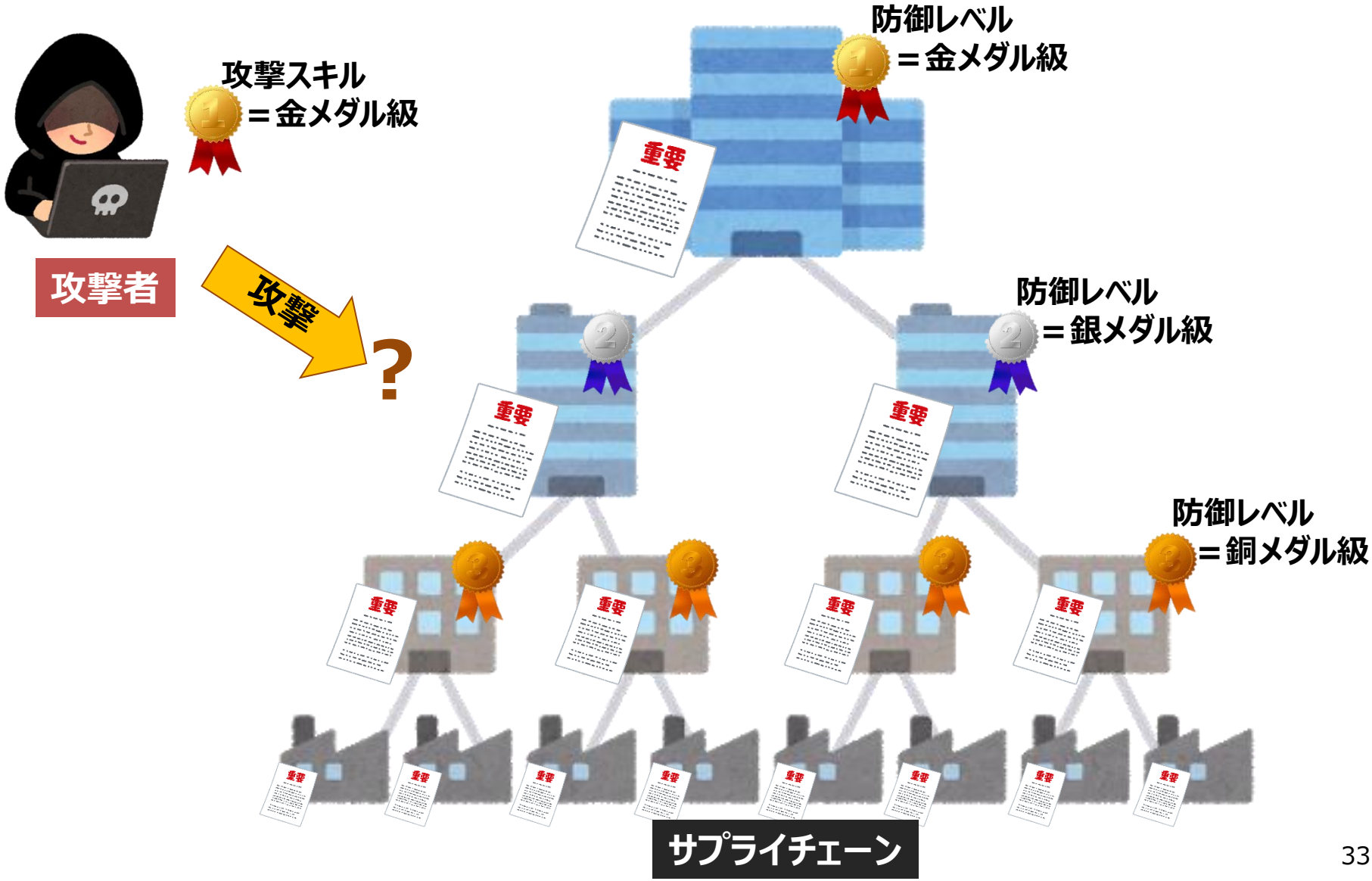
- サイバーセキュリティ経営ガイドラインをベースとした可視化ツールにより、自社内の可視化、投資家等ステークホルダー向けの可視化を段階的に実現、2nd～3rd stepをつなぐ。
- βテスト後、2020年度以降に可視化ツールV1.0をリリースし、広く展開する。



2020年度以降、可視化ツール**V1.0リリース、本格展開**

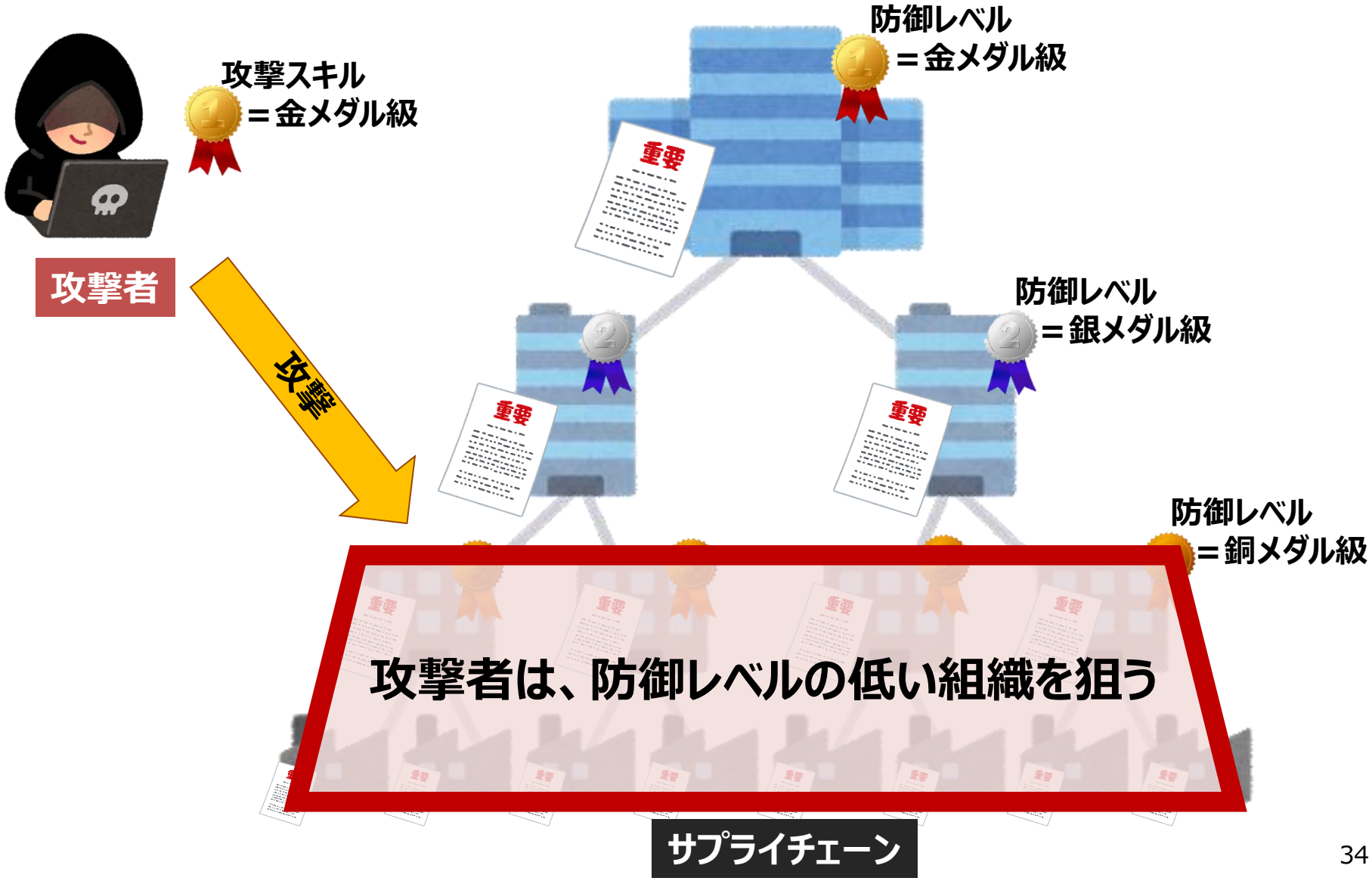
攻撃者はサプライチェーンのどこを狙うか

- 企業の対策レベルはバラバラだが、「金（カネ）」になる重要情報は至る所に存在する。



攻撃者はサプライチェーンのどこを狙うか

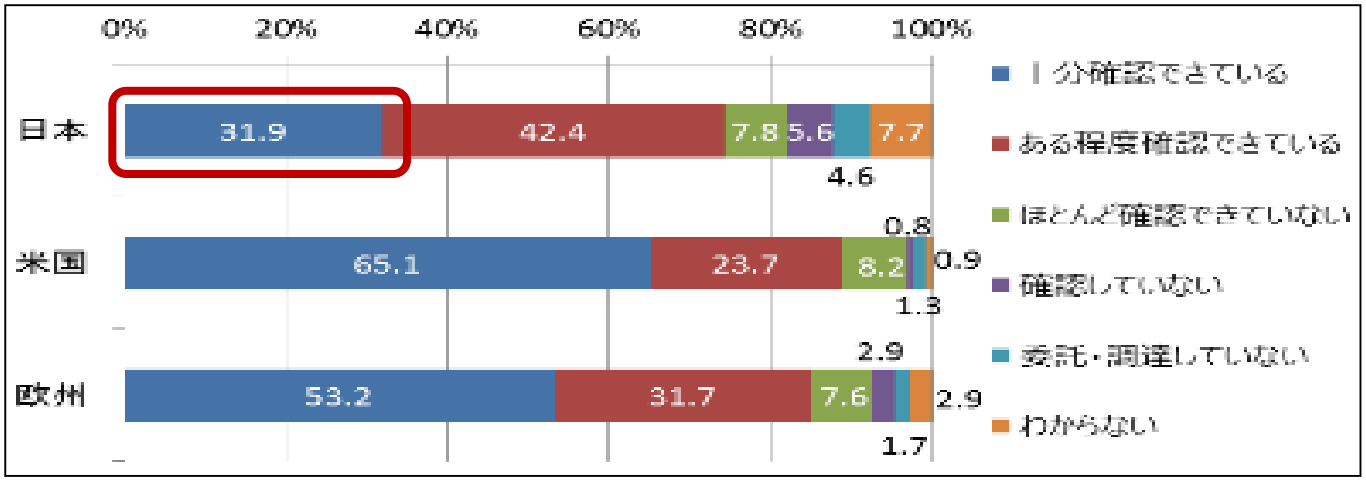
● 企業の対策レベルはバラバラだが、「金（カネ）」になる重要情報は至る所に存在する。



取引先へのサイバーセキュリティ対策の遅れ

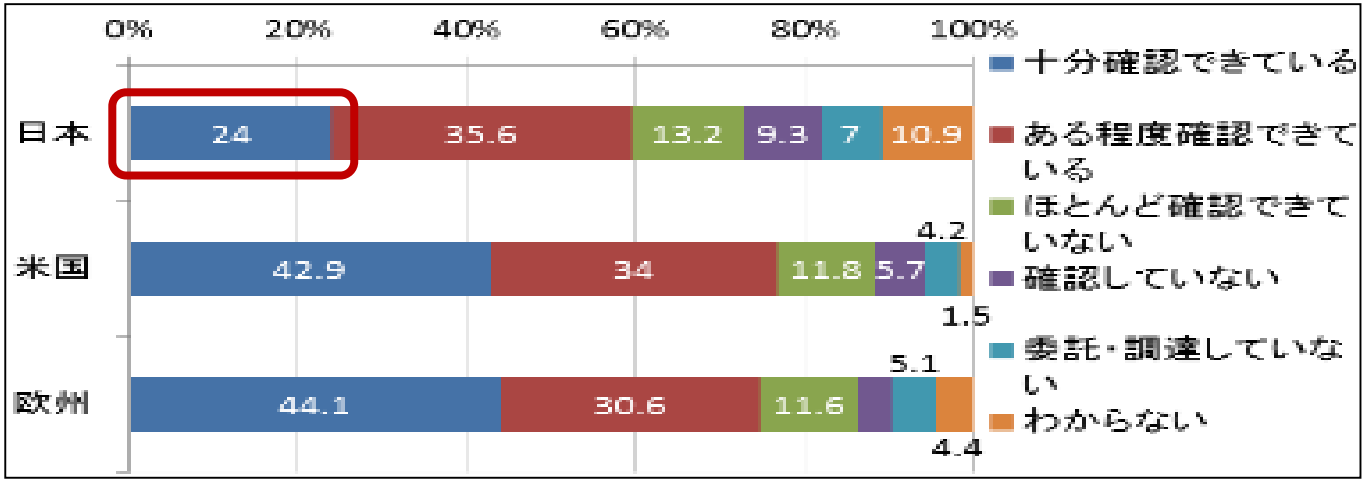
● 日本企業では、委託先等の取引先への対応が大幅に遅れている

■委託先のセキュリティ対策状況把握（業務委託先）



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（物品調達先）



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。

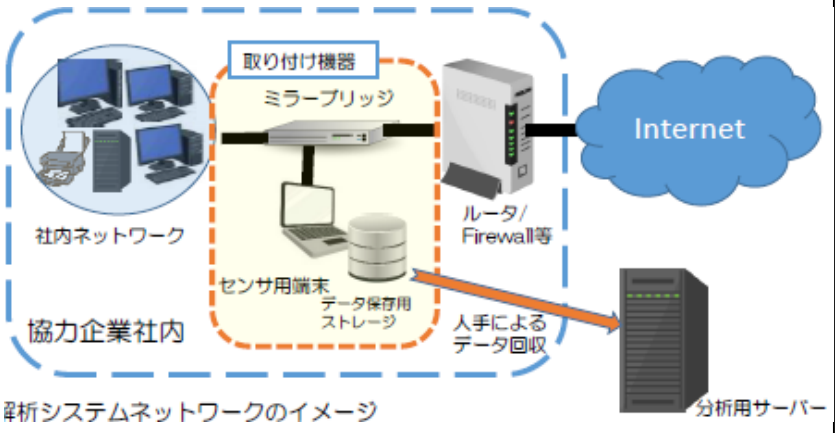
中小企業に対するサイバー攻撃の調査・分析結果（大阪商工会議所）

● 地域の中小企業も、例外なくサイバー攻撃の脅威にさらされている

中小企業被害実態に関する調査

■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収集。



解析システムネットワークのイメージ

■ 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。

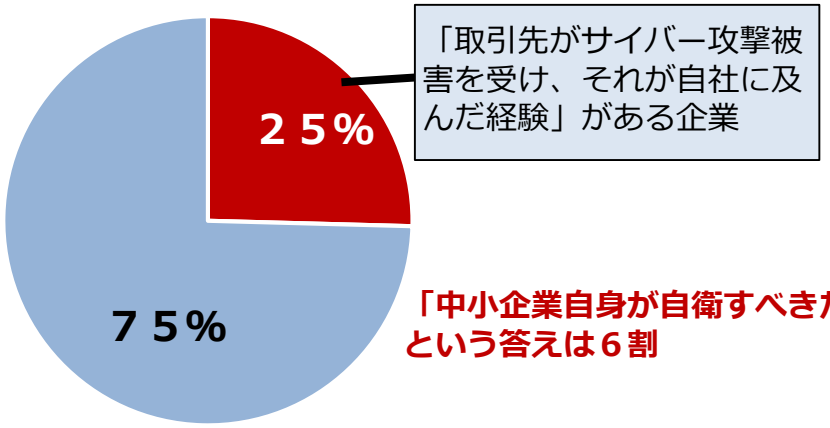
取引先経由の被害に関する調査

■調査内容

調査期間：平成31年2月～3月
調査内容：全国の従業員100人以上の企業を対象に、郵送、FAX、メール、Web、対面による依頼・回答

■調査結果（中間報告）

- 大企業・中堅企業118社に調査したところ、取引先がサイバー攻撃被害を受け、**影響が自社に及んだ経験**がある企業が30社あった（**25%**）



「中小企業自身が自衛すべきだ」という答えは６割

出典：大阪商工会議所「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」（2019年5月）

<出典：大阪商工会議所「平成30年度中小企業に対するサイバー攻撃実情調査（報告）」共同研究実施者：神戸大学、東京海上日動火災保険（株）（2019年7月）>

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

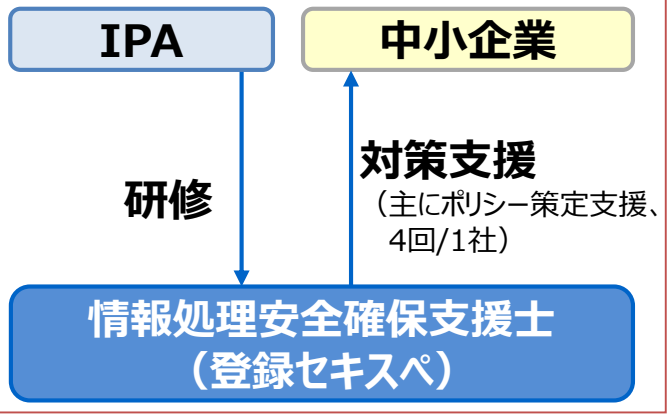
- セキュリティ対策を始めるに当たって何をやればいいのかわからない、そういった悩みをもつ中小企業に対し、**専門家を派遣し、セキュリティポリシーの策定を支援**。
- インシデントが発生してしまったが対処方法がわからない、そんな中小企業の事後対応を支援する簡易保険の実現を目指し、**サイバーセキュリティお助け隊による支援体制を構築**。

特定 → 防御 → 検知 → 対応 → 復旧

主に事前支援

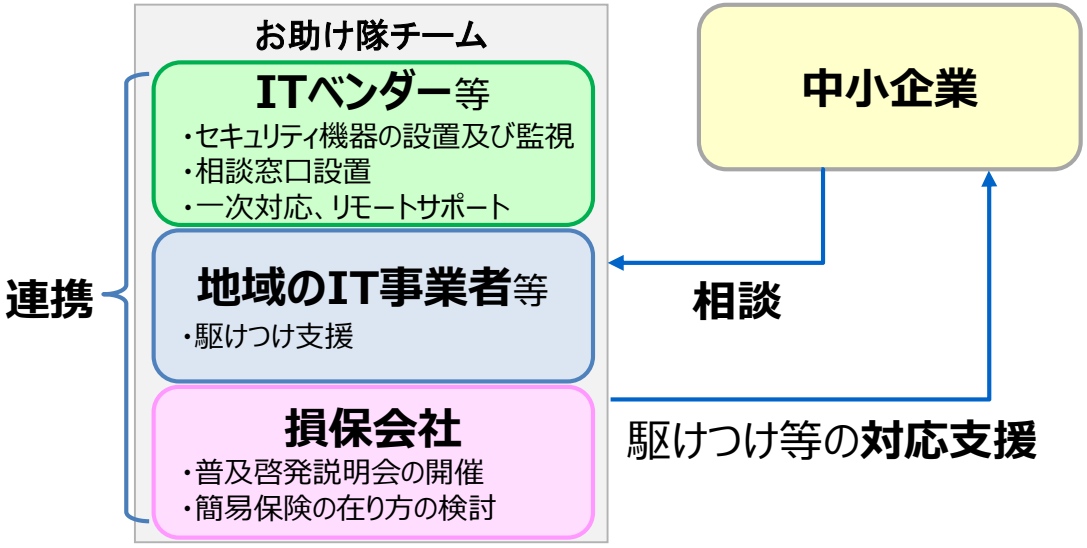
・**中小企業ガイドライン**
・**セキュリティアクション（９万社超が自己宣言）**

・**セキュリティマネジメント指導**：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**。



事前支援：中小企業の情報セキュリティ対策ガイドライン

- これからセキュリティ対策に取り組む企業向けの対策や、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に構成。

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

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

Step1 まず始める

最低限実施すべき
セキュリティ対策の5か条

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

こちらより無料ダウンロード可能です
https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

中小企業の情報セキュリティ対策ガイドライン・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（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。
- **９万者を超える中小企業が宣言**（2019年10月末時点）。

＜中小企業の情報セキュリティ対策ガイドライン＞

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

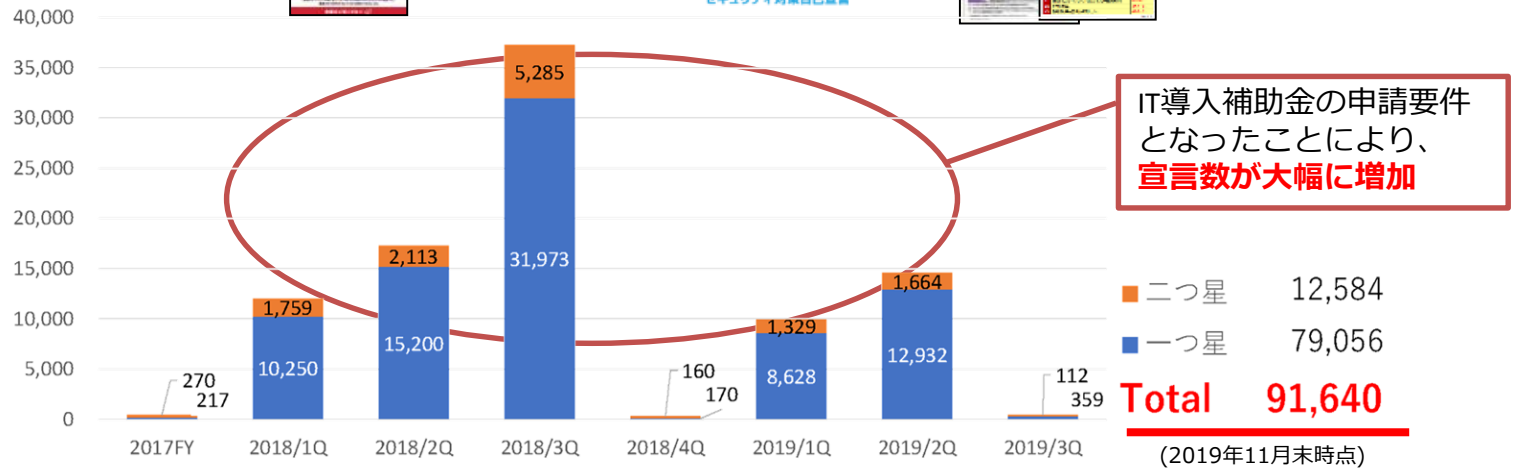
実践者が具体的にセキュリティ対策を実施していくための方法を、**企業のレベルに合わせて段階的にステップアップできる**ような構成で解説

★ 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



IT導入補助金の申請要件となったことにより、**宣言数が大幅に増加**

二つ星	12,584
一つ星	79,056
Total	**91,640**

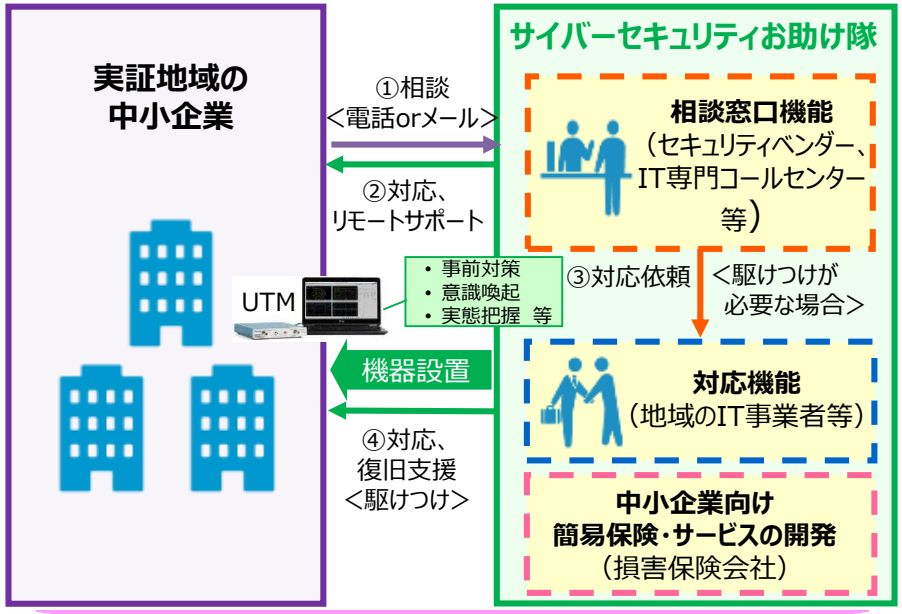
（2019年11月末時点）

主に事後支援：サイバーセキュリティお助け隊

- 全国**8地域**を対象に地域の団体、企業等と連携して、中小企業向けのサイバーセキュリティ対策支援の仕組みの構築を目的とした実証事業を実施
- 本事業を通じて、サイバー攻撃の実態や対策のニーズを把握するとともに、**中小企業の事前対策の促進、意識喚起**を図る

＜実証地域＞

＜実証のイメージ＞



実証結果

中小企業　側
- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

保険会社、セキュリティベンダー　側
- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

サイバーセキュリティお助け隊　今年度実証事業の状況

- 多くの中小企業に参加いただき、駆けつけ事例も発生している状況。

受託事業者	地域	参加中小企業数
株式会社デジタルハーツ	宮城県、岩手県、福島県	110
東日本電信電話株式会社	新潟県	148
富士ゼロックス株式会社	長野県、群馬県、栃木県、茨城県、埼玉県	109
SOMPOリスクマネジメント株式会社	神奈川県	151
株式会社PFU	石川県、富山県、福井県	120
MS&ADインターリスク総研株式会社	愛知県	201
大阪商工会議所	大阪府、京都府、兵庫県	112
株式会社日立製作所	広島県、山口県	111

計**1,064**社の中小企業が参加

(2020年1月10日時点)

お助け隊で観測されたサイバー攻撃の実例

お助け隊設置のUTMが不審な通信を観測。ボットネットへの通信が疑われた。
原因は、従業員がマルウェア感染が疑われる**私物のスマートフォン**を社内の無線アクセスポイントに接続したこと。
お助け隊が**駆けつけ対応を実施し、対処した**。

お助け隊による対処が行われず放置した場合・・・
スマートフォンに感染しているマルウェアがWi-Fiを経由して社内LANに侵入し、社員全員の業務用PC全25台に感染、業務停止や機密情報が漏洩する事態が考えられた。
この場合の保険会社算出の被害想定額※は、

約**4,925万円**

※初動対応、調査対応、復旧費用、事業停止による損失等。

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し、IT系・制御系に精通した専門人材の育成を開始。
- 世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ1年程度のトレーニングを実施。

1年を通じた集中トレーニング

中核人材育成プログラム– 年間スケジュール

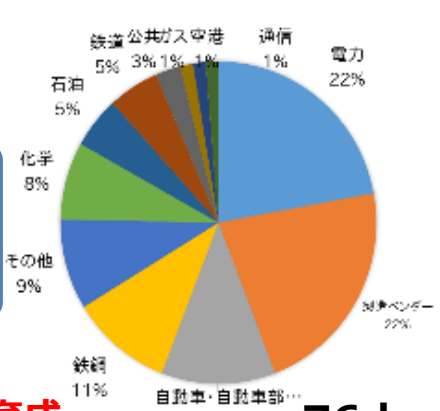
7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月
プライマリー（レベル合わせ）			ベーシック（基礎演習）				アドバンス（上級演習）			卒業プロジェクト	
開講式			ビジネス・マネジメント・倫理								修了式
			プロフェッショナルネットワーク（含む海外）								

◀模擬プラント全景

- 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

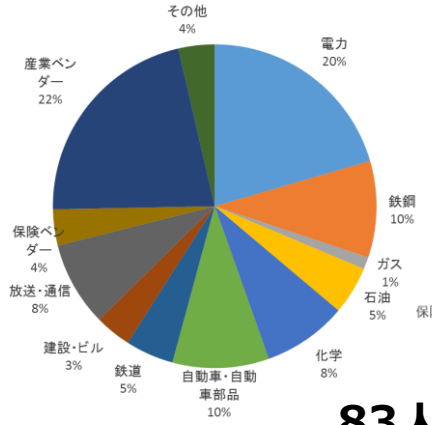
現場を指揮・指導するリーダーを育成

第１期受講生（平成29年7月～平成30年6月）業界別構成



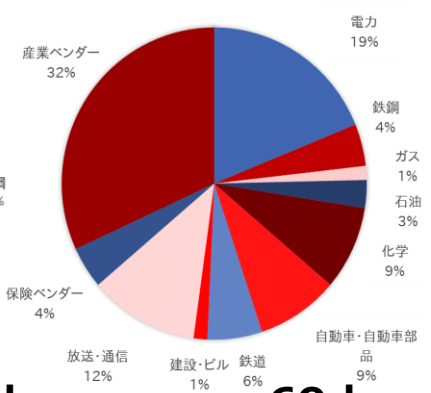
76人

第２期受講生（平成30年7月～令和元年6月）業界別構成



83人

第３期受講生（令和元年7月～令和2年6月）業界別構成



69人

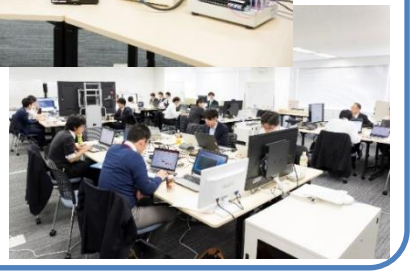
ＩＣＳＣｏＥの施設（千石、秋葉原）

- 座学や基礎演習を行う千石と、各業界を想定した実機を使った模擬プラントを実際に攻撃して脆弱性を洗い出すなどの実践的なプログラムを行う秋葉原で活動を展開。

千石ー研修･演習施設

＜座学＞

＜基礎演習＞



秋葉原ー模擬プラント

＜実践的プログラム＞

模擬プラントを攻撃

攻撃

①発電模擬プラント

②機械製造模擬プラント

脆弱性を発見

対策を検討

模擬プラント全景

③鉄鋼圧延模擬プラント
④鉄道運行管理模擬プラント
⑤スマートグリッド模擬プラント
⑥施設管理模擬プラント

受講生

模擬プラント

多様な短期プログラム（製造・生産分野の管理監督者層向けプログラム）

- 製造・生産現場のセキュリティに必要なIT・OT基礎からセキュリティ戦略立案まで、**現場が主体的に取り組むためのマネジメントスキル**を学ぶプログラム。
- 受講者は1つあるいは複数のコースを選択して受講可能。

	コース名	開催期間（2019年度）
1	製造・生産現場のセキュリティに必要なIT・OT基礎	11/11～11/14（4日間）
2	製造プラント・工場等が稼働している中でのリスク分析手法	2/3～2/7（5日間）
3	製造・生産現場へのセキュリティ製品導入及びベンダー選定方法	12/3 ～12/6 （4日間）
4	製造・生産現場向けセキュリティ教育の実施方法	12/16～12/19（4日間）
5	製造・生産現場でのセキュリティ・インシデント対応実践方法	1/20～1 /24（5日間）
6	製造・生産現場におけるセキュリティ業務の運用・保守手法	2/17～2 /20（4日間）
7	実践 製造・生産現場のためのセキュリティ戦略立案	3/3 ～3/6（4日間）

開催場所	独立行政法人情報処理推進機構（東京都文京区本駒込2-28-8）
定員	各コース 40名
受講料	各コース 15万円（税込）
申込	https://www.ipa.go.jp/icscoe/program/seizo-seisan/index.html

インド太平洋地域向け日米サイバー演習

- 経済産業省及びIPA産業サイバーセキュリティセンター（ICSCoE）が、日米の専門家による制御システムのサイバーセキュリティに関する演習をインド太平洋地域（14の国・地域）向けに実施。

■**日時・場所：**2019年9月9日（月）～12日（木）@東京（今年で２回目、以後毎年開催。）

■**参加者：**ASEAN９カ国、スリランカ、バングラデシュ、インド、NZ、台湾　35名

ICSCoE中核人材育成プログラム研修生　69名

■**来賓挨拶／講師：**

（米国）在日米国大使館首席公使代理、国務省東アジア・太平洋局首席次官補代理、エネルギー省、NIST、INL、ISA、米国企業

（日本）関芳弘経済産業副大臣、ICSCoE講師、日本企業

米国国務省挨拶


米国の専門家による講義


日本の専門家による講義


ハンヅオントレーニング


ワークショップ


サイバー攻撃のデモ

参加国・地域

国立高専機構と産・官との連携促進・具体化

- METI、IPA、JPCERT及び業界団体が国立高専機構と連携し、高専生の専攻（セキュリティ、IT、その他（機械、電気等））に応じた教育コンテンツの提供や講師の派遣等、産学官連携の具体化を推進中。

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

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（パワーポイント、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回程度開催（インシデント対応演習等）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回程度開催（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。  ゲーム形式教材のイメージ	・**JNSAが講師の派遣を検討中。** ・**METIがセキュリティ専門官を高度セキュリティ合宿に講師として派遣。**  開催の様子@石川高専
約20% 情報系学科の学生 → 主に**IT企業**に就職	・**JNSAのゲーム形式教材を石川高専と連携してアプリ化。** ※JNSA：NPO日本ネットワークセキュリティ協会 ・**四国地域企業のIPA ICSCoE終了生が講義を検討中。** ・**日立製作所が一関高専生向けに出前授業、インターンシップを実施し、出前授業は全国各校に配信。**	・**JNSAとSECCONビギナーズを石川高専と苫小牧高専で開催。** ・**JNSAがCTFビギナーズfor高専生@木更津高専に講師を派遣。** ・**IPAが高度セキュリティ合宿に講師を派遣し、App Goat（脆弱性体験学習ツール）の講習会を開催。** ・**METIがセキュリティ専門官を高知高専に派遣し、出前授業を実施。**
約80% 非情報系学科の学生 → 主に**ユーザー企業**に就職	・**CRICが佐世保高専と連携し、業界別（例．機械、電気、建築等）ビデオ教材（20分程度）を作成中。** ※CRIC：一般社団法人サイバーリスク情報センター	※セキュリティ合宿のような機会は特段なし。  AppGoat講習の様子
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。	・**IPAが教員向けにAppGoat講習会を開催。** ・**JPCERT/CCが情報担当教員向け研修に講師を派遣。** ・**教員がIPAのセキュリティキャンプ全国大会を見学。** ・**教師向け合宿で、METIがセキュリティ専門官の派遣を検討中。**

セキュリティスキルレベル

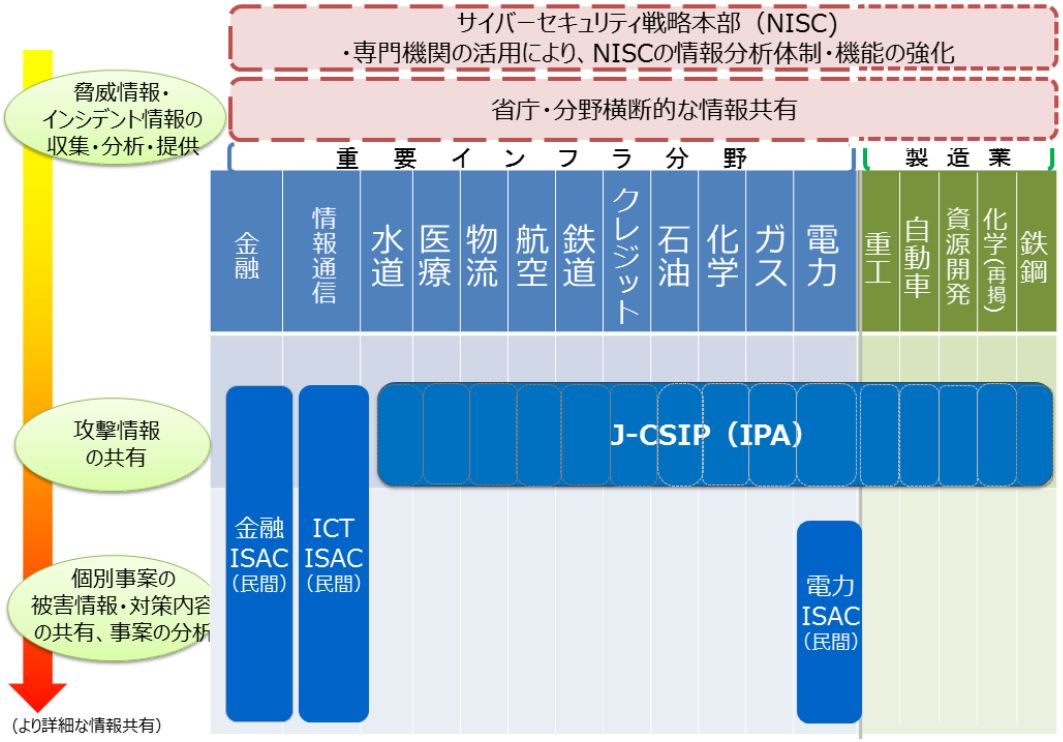
インシデント情報の収集・共有によるサイバーセキュリティ対策の強化

- 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　Cyber　Security　Information　sharing　Partnership of Japan、15業種、262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の仕組み】

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。

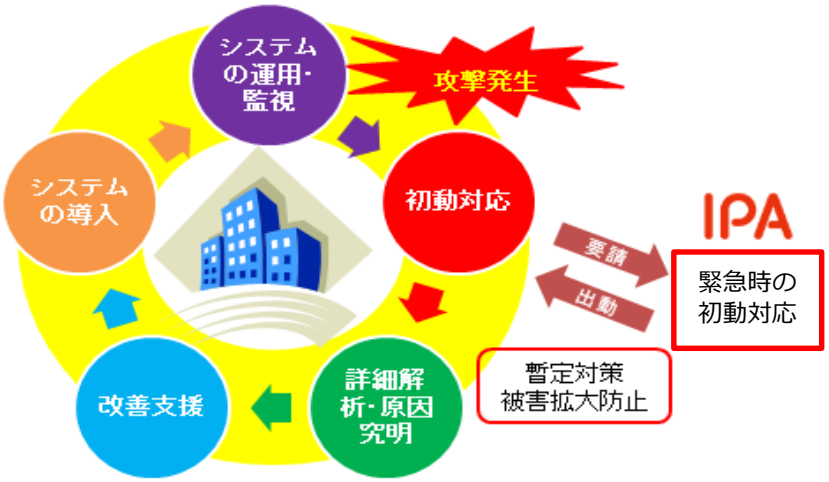
重要インフラ等企業
（重工、電気、ガス、化学、石油、資源開発、自動車、クレジット、物流、航空、鉄道、医療、空港、水道、鉄鋼
：15業種262組織）



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。
- 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、初動対応支援を実施。

【サイバーレスキュー隊の活動】



重要インフラ、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

IPA 独立行政法人 情報処理推進機構 Information-technology Promotion Agency, Japan

サイバーレスキュー隊

標的型サイバー攻撃特別相談窓口

https://www.ipa.go.jp/security/tokubetsu/index.html

E-mail: tokusou@ipa.go.jp

TEL: 03-5978-7599

１．サイバー攻撃の動向

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．WG1：「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．WG2：サイバーセキュリティ対策の基盤整備
～経営、人材育成、中小企業

５．WG3：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

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

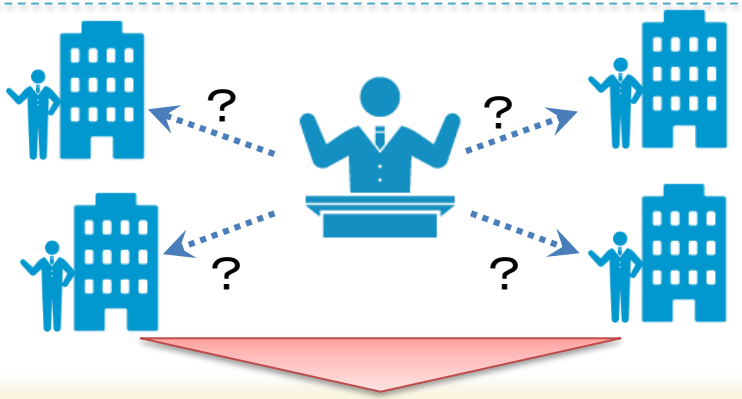
検証ビジネスの普及展開

『Proven in Japan』の促進

情報セキュリティサービス審査登録制度の概要

- **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7月）
- 基準に適合するサービスのリストを利用することで、ユーザーは**<u>一定の品質維持向上が図られているサービスを使うことが可能になる</u>**。

✓ 外部に委託したいがどの事業者のサービスを選べば良いか分からない

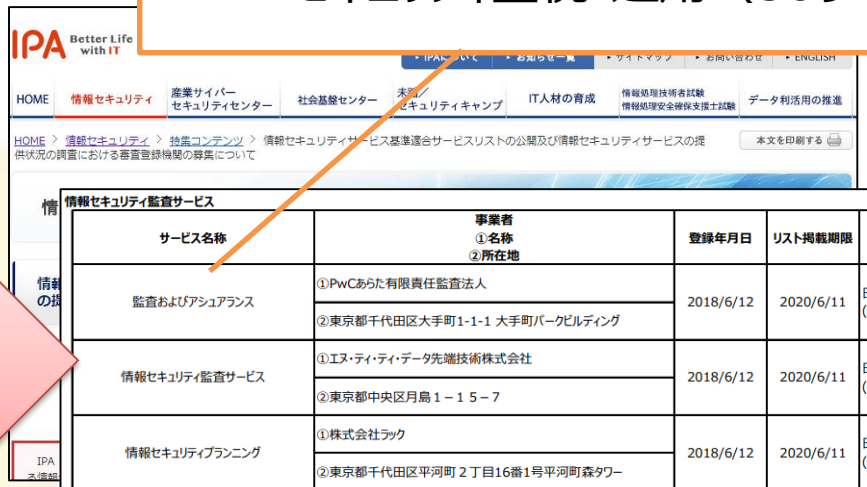


ユーザー
（企業やコンシューマ）

選定時に活用

最低限の品質を満たした
119サービスが掲載（2019年10月時点）

- 情報セキュリティ監査（25サービス）
- 脆弱性診断（47サービス）
- デジタルフォレンジック（17サービス）
- セキュリティ監視・運用（30サービス）



情報セキュリティ監査サービス　　掲載日：2018年7月5日

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


METI
Ministry of Economy, Trade and Industry