資料８

関係省庁の取組状況について

【総　務　省】

資料８－１　総務省におけるサイバーセキュリティ施策の
取組状況について

【経済産業省】

資料８－２　経済産業省におけるサイバーセキュリティ施策の
取組状況について

資料８－１

総務省におけるサイバーセキュリティ施策の取組状況について

2021年5月

総務省サイバーセキュリティ統括官室

LINE株式会社おける情報管理の状況

- LINE株式会社が提供するLINEサービスに関するシステム**開発や運用の一部が中国企業や日本企業の中国拠点に委託**されていた。また、トークのテキストデータは国内のデータセンターに保管されている一方、**画像や動画等のデータは韓国のデータセンターに保管**されていた。
- LINEは国内で8,600万ユーザが利用するとともに、一部公共サービスにも利用されており、データの適正な取扱い、サイバーセキュリティ上のリスクに懸念がある。

データの保管場所

※LINE株式会社の公表資料及び同社から聴取した内容に基づき作成

サービス	データ	保管場所
LINEメッセンジャー（トーク）	テキスト	日本
	画像・動画・ファイル	日本・韓国
LINE公式アカウント（トーク）	テキスト	日本
	画像・動画・ファイル	韓国

国外での情報の取扱い

実施拠点	主な業務	主な取扱い情報
NAVER　China	・公開タイムラインと通報コンテンツのモニタリング（日本・台湾・タイ・インドネシア以外） ・LINEゲームサービスのモニタリング、テスト	通報されたテキスト・画像・動画・ファイル
日系企業A社の中国拠点	・公開タイムラインとオープンチャットのコンテンツモニタリング ・タイムラインとオープンチャットで通報されたコンテンツのモニタリング	通報されたテキスト・画像・動画・ファイル
LINE Digital Technology（通称LINE China）	・通報モニタリングツールの開発保守 ・画像処理、モニタリングフィルター開発	通報されたトーク・タイムライン・公式アカウントのテキスト/画像/動画

LINE株式会社に対する行政指導

■ LINE株式会社の報告に基づく限りにおいては、通信の秘密の侵害等があった旨は確認できなかった一方で、**社内システムの安全管理措置等や利用者に対する説明等に関して一部不十分な点が認められた**。

■ このため、令和３年４月26日、同社に対し文書による**行政指導を実施**。指導を踏まえて講じた措置の状況について、同年５月末までの報告を求めている。

１　社内システムに関する安全管理措置等に関する事項

（１）社内システムへのアクセス管理の徹底

社内システムへのアクセスを通じた利用者の個人情報や通信の秘密に該当する情報の漏えいが生じることのないよう、その万全を図るため、次のとおり、社内システムへのアクセス管理の強化徹底を図ること。

① 今回の報告において、LMP（社内システムの１つであるモニタリング支援システム：LINE Monitoring Platform）へのアクセス権限に関して、一部に適切なプロセスを経て付与されたものか否かが確認できないケースがあったと認められることを踏まえ、社内システムへのアクセス（外部向けサービスのためのシステムへの内部からのアクセスを含む。以下同じ。）の権限が、真に適切な者に対して、適切な範囲で付与されるプロセスになっているかについて、全般的に点検を行うとともに、その結果を踏まえて、必要に応じ、適切なプロセスを通じたアクセス権限の付与を確保するための措置を講じること。

② 今回の報告において、LMPへのアクセスのための通信について、不正の検知やログインしようとする者の認証の仕組みが、不正行為の防止や本人性の確認のための対策として必ずしも十分に厳格であるとはいえない部分があると認められることから、これらの対策について点検を行うとともに、その結果を踏まえて、必要に応じ、例えば、社内システムに対する不正・不審なアクセスの監視や監査、社内システムにアクセスする者の認証の強化等、内部からの不正・不審なアクセスやなりすましの防止に万全を図るための方策を検討し、具体的な措置を講じること。

（２）開発プロセス及び開発組織のガバナンスの強化

今回の報告において、内部向けシステムであるLMPの開発プロセスにおいて、権限管理やセキュリティチェックが適切に実施されていないケースがあったと認められることを踏まえ、LMPに限らずシステム開発全般について、適切な開発プロセスの下で実施されるよう確保することにより、利用者の個人情報及び通信の秘密に該当する情報の漏えいが生じることのないよう、その万全を図る観点から、次のとおり、開発プロセス及び開発組織のガバナンスの在り方を見直し、その強化を図ること。

① 内部向けシステムの開発プロセスについて、原則として電気通信役務の提供等の外部向けサービスのためのシステムに係る開発プロセスと同様の開発プロセスによることとするとともに、開発プロセス全般について再点検を行うこと。

② 適切な開発プロセスによる開発の実施や開発者に対するアクセス権限の適切な付与、また、不適切なケースがあった場合の迅速な対応を図るため、開発組織のガバナンスの在り方の見直しを含めた検討を行い、その着実な確保を図ること。

（３）社内システムに関するリスク評価等を通じた透明性・アカウンタビリティの向上

社内システムからの利用者の個人情報及び通信の秘密に該当する情報の漏えいの防止に万全を期す上でリスク評価が十分ではなかったと認められることを踏まえ、次のとおり、社内システムに関するリスク評価等を行い、これらの情報の適切な取扱いに係る透明性・アカウンタビリティの向上を図ることにより、利用者からの信頼の確保に努めること。

① 上記（１）及び（２）を含め、外国の法的環境による影響等にも留意しつつ、委託先を含めた社内システムの開発・運用に当たっての情報の取扱いに係るリスク評価を実施し、必要に応じ所要の措置を講じること。また、これらの措置を講じた場合には、当該措置を適切に反映した内容になるようポリシーを見直すこと。なお、例外的なプロセスを適用する場合には、適用の範囲及びその判断の手続についても当該ポリシーにおいて明確にすること。

② 貴社においては、データセキュリティのガバナンス強化と情報保護の強化の観点から「米国NISTが定めた世界トップレベルのセキュリティ基準への準拠」を図ることとしていると承知しているところ、今後貴社において必要な体制の構築等を図ることにより、同基準への準拠に向けた取組の強化を図るなど、透明性・アカウンタビリティの向上に努めること。

２　利用者への適切な説明に関する事項

トーク履歴等の通報機能使用に際して、利用者に示される文言が想定していたものと異なっていたケースがあったことを踏まえ、通信の秘密に関する情報の適切な取扱いを確保する観点から、トーク履歴の通報を行った際に、貴社に提供される情報の範囲、提供された情報の利用目的について利用者が分かりやすく理解できるようにするための措置を講じること。また、貴社に提供された情報が当該利用目的の範囲内で適切に取り扱われることを確保するための措置を講じること。

電気通信事業ガバナンス検討会

■ デジタル変革時代における安心・安全で信頼できる通信サービス・ネットワークの確保を図るため、電気通信事業者におけるサイバーセキュリティ対策及びデータの取扱いに係るガバナンス確保の今後の在り方について検討を行うことを目的として、令和３年５月より、「電気通信事業ガバナンス検討会」を開催。

検討事項

（１）電気通信事業者におけるサイバーセキュリティ対策及びデータの取扱いに係るガバナンス確保の今後の在り方
（２）上記（１）を踏まえた、政策的な対応の在り方
（３）その他

構成員

	相田　仁	東京大学大学院工学系研究科教授
	石井　夏生利	中央大学国際情報学部教授
	上沼　紫野	虎ノ門南法律事務所弁護士
（座長）	大橋　弘	東京大学公共政策大学院院長／大学院経済学研究科教授
（座長代理）	後藤　厚宏	情報セキュリティ大学院大学学長
	中尾　康二	一般社団法人ICT-ISAC顧問 国立研究開発法人情報通信研究機構サイバーセキュリティ研究所主管研究員
	中村　修	慶應義塾大学環境情報学部教授
	古谷　由紀子	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会監事
	森　亮二	英知法律事務所弁護士
	山本　龍彦	慶應義塾大学大学院法務研究科教授

オブザーバ　内閣官房内閣サイバーセキュリティセンター、内閣官房IT総合戦略室、個人情報保護委員会

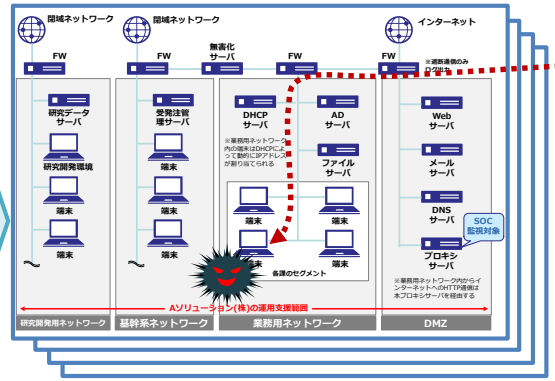
実践的サイバー防御演習（CYDER）

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習**(**CYDER**)を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施。 参加申込 → https://cyder.nict.go.jp
  ※2017年度：100回・3,009名／2018年度：107回・2,666名／2019年度：105回・3,090名／2020年度：106回・2,648名

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

北陸StarBED技術センターの大規模高性能サーバ群を活用



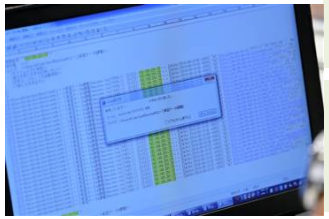
擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**

演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解



本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和３年度の実施計画

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	４７都道府県	６５回	７月～翌年２月
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国１１地域	２１回	10月～翌年２月
B-2				地方公共団体以外	東京・大阪・名古屋・福岡	１３回	翌年１月～２月
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京	２回	翌年１月～２月
オンラインA	ｵﾝﾗｲﾝ演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	（受講者職場等）	随時	秋以降開始 (6~8月に試験提供予定)

令和３年度から**新規**開設

資料８－２

経済産業省
Ministry of Economy, Trade and Industry

第６回
産業サイバーセキュリティ研究会
事務局説明資料（抜粋）

令和３年４月２日

経済産業省

商務情報政策局

アクションプランの持続的発展と、新たな課題へのチャレンジへ

2020年12月18日発出「注意喚起」のUpdate

- **サプライチェーン、クラウド、ファイル共有、制御系を狙った高度なサイバー攻撃事例**
- **最新の攻撃事例を踏まえた対策のアップデート**

Cyber New Normalにおける５つの処方箋　＜１～3年＞　（継続）

- **デジタル化が急加速する中でのサイバー脅威の常態化 “Cyber New Normal”**

① 「開発のための投資」から「検証のための投資」へのシフト
② サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定
③ セキュリティとセーフティの融合への対応
④ サプライチェーンセキュリティ確保のための産業界一丸となった対応
⑤ Like-mindedの関係強化

国としての対処能力の強化　＜ 1～5年 ＞　New !

- **国としての対処能力の構築**

For the future infrastructure　＜3～5年＞　（継続）

- **重要インフラ産業の“基盤インフラ”も仮想化時代へ突入**
  - インフラの機能を支える“高信頼な基盤インフラ”の構築・保守能力の確保

アクションプランの持続的発展と、新たな課題へのチャレンジへ

2020年12月18日発出「注意喚起」のUpdate

- サプライチェーン、クラウド、ファイル共有、制御系を狙った高度なサイバー攻撃事例
- 最新の攻撃事例を踏まえた対策のアップデート

Cyber New Normalにおける５つの処方箋　＜１～3年＞　（継続）

- デジタル化が急加速する中でのサイバー脅威の常態化 “Cyber New Normal”
  - ① 「開発のための投資」から「検証のための投資」へのシフト
  - ② サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定
  - ③ セキュリティとセーフティの融合への対応
  - ④ サプライチェーンセキュリティ確保のための産業界一丸となった対応
  - ⑤ Like-mindedの関係強化

国としての対処能力の強化　＜ 1～5年 ＞　New !

- 国としての対処能力の構築

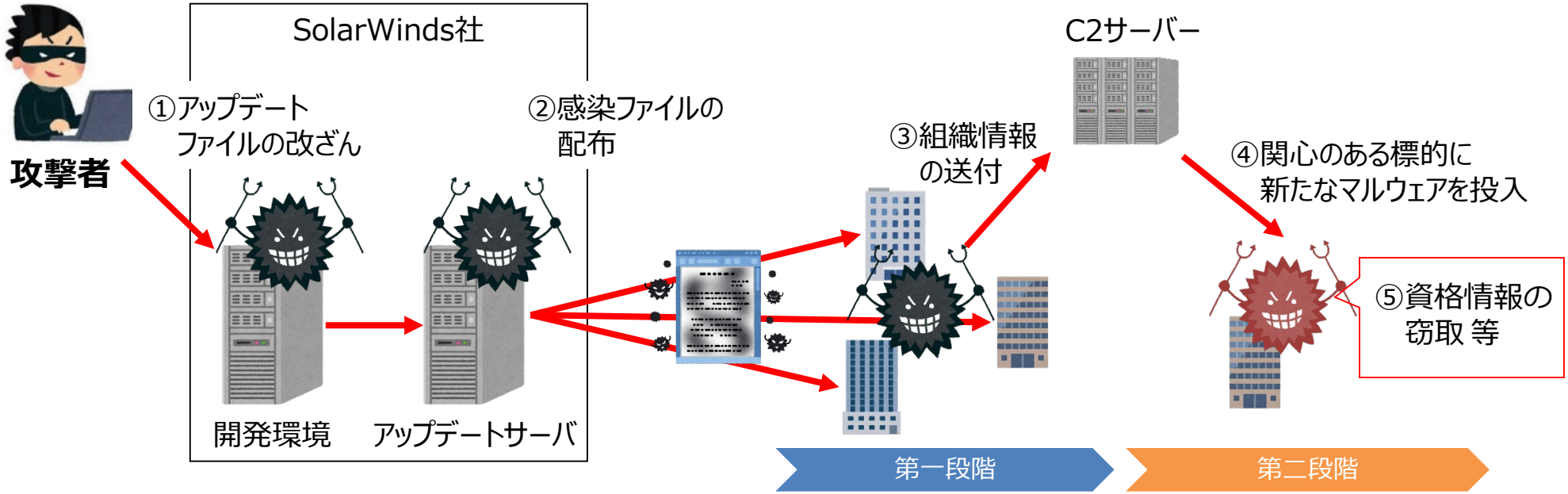
For the future infrastructure　＜3～5年＞　（継続）

- 重要インフラ産業の“基盤インフラ”も仮想化時代へ突入
  - ➢ インフラの機能を支える“高信頼な基盤インフラ”の構築・保守能力の確保

SolarWinds Orion Platformのアップデートを悪用した攻撃

- 2020年12月13日、SolarWinds社は同社のネットワーク監視ソフトウェア「Orion Platform」に、**正規のアップデートを通じてマルウェアが仕込まれた**ことを公表。
- 攻撃は2019年9月には始まっていたとみられ、2020年3月～6月のアップデートファイルが侵害されたことで、米政府機関等を含む**最大約18,000組織が影響**を受けたとされる。
- 初期段階のマルウェアは、セキュリティサービスの検知を回避しつつ被害組織の情報をC2サーバーへ送信。**攻撃者が関心のある標的に対しては第２段階のマルウェアが投入**され、資格情報を窃取した上で、**米国政府内、政府間のやり取りを傍受していた可能性が指摘されている。**

◆攻撃イメージ



（出典）各種公開情報に基づき経済産業省作成

クラウドサービスの設定不備を原因とする不正アクセス

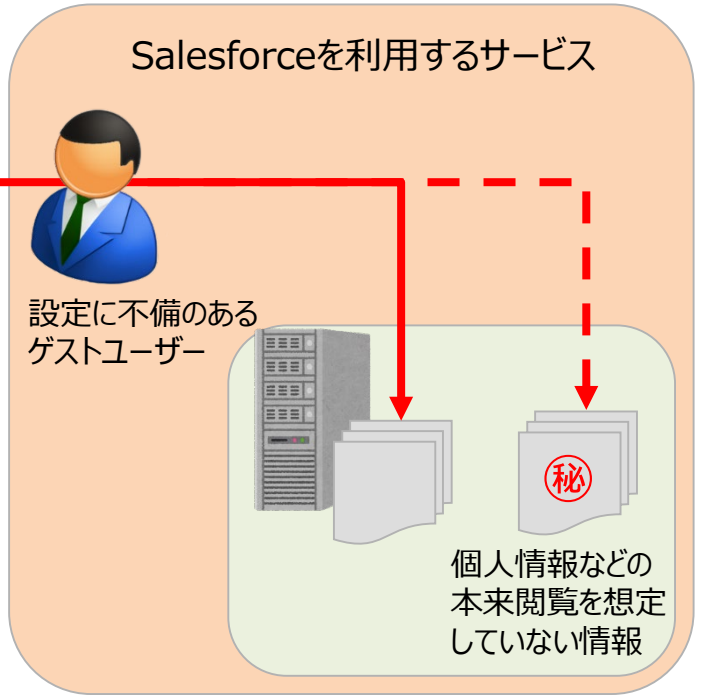
- 2020年12月25日、セールスフォース・ドットコムは、同社が提供するサービスにおける**ゲストユーザーに対する情報共有に関する設定が適切に行われていない場合、一部情報が第三者より閲覧できる**事象の発生を公表。また、**複数の国内事業者が本事象による不正アクセス及び個人情報漏えいの発生**を公表。
- 本サービスを組み込んだシステムがパッケージとして複数の顧客に提供され、同時に被害が発生したケースも。
- クラウドサービスを活用する際には、サービスの利用状況や各種設定の確認・見直しを行うなど、適切なセキュリティ対策を講ずることが重要。

◆不正アクセスがあったと公表した事業者等

- キャッシュレス決済サービス事業者
- サービス事業者
- クレジットカード事業者
- 小売事業者
- 玩具メーカー
- ガス事業者
- 地方自治体
- 独立行政法人　　他

◆攻撃イメージ

攻撃者

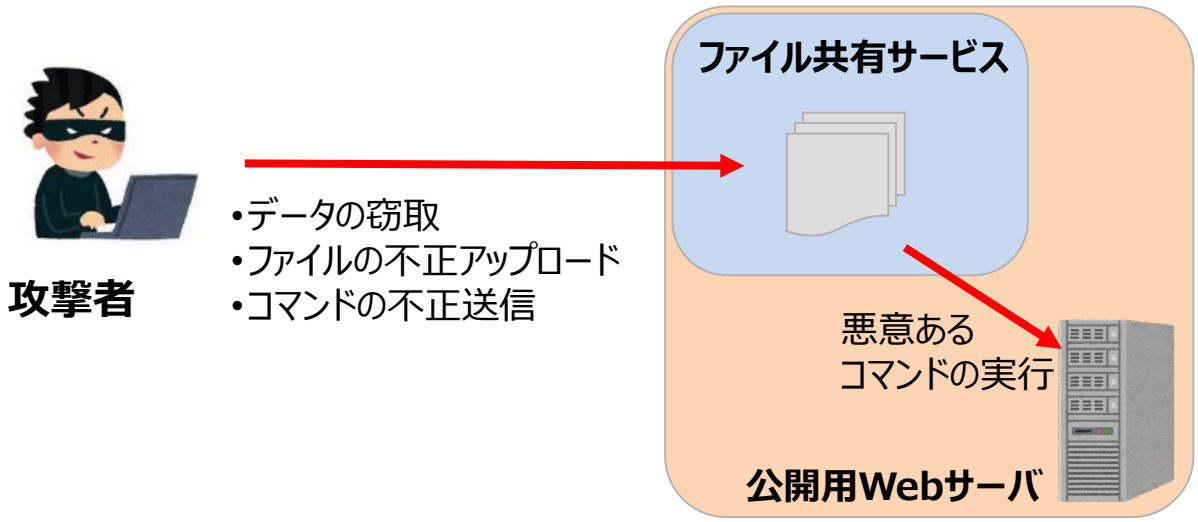


（出典）各種公開情報に基づき経済産業省作成

ファイル共有サービスを狙ったサイバー攻撃

- 2020年12月、ファイル共有サービスであるSoliton社のFileZenサービス及びAccellion社のFTA（File Transfer Appliance）における脆弱性の存在が公表された。
- 本脆弱性を悪用することで、ファイル共有サービス内の**データが窃取**されるほか、サービスへのログインを迂回した**ファイルの不正アップロード**や、**サービスを運用するサーバーで任意のコマンドが実行される**おそれがある。
- 複数の海外企業がFTAの**脆弱性を悪用した情報漏えいについて公表**したほか、データを窃取したサイバー攻撃集団による**被害企業に対する恐喝**が発生している。また、FileZenは日本企業が提供しており、**国内に多くのユーザーがいるため注意が必要**である。
- こうしたサービスは**機微情報の授受にも利用**されており、海外では住民の個人情報や社会保障番号、銀行の取引先の営業秘密、弁護士事務所の機密情報など、社会的影響の大きい情報も流出している。

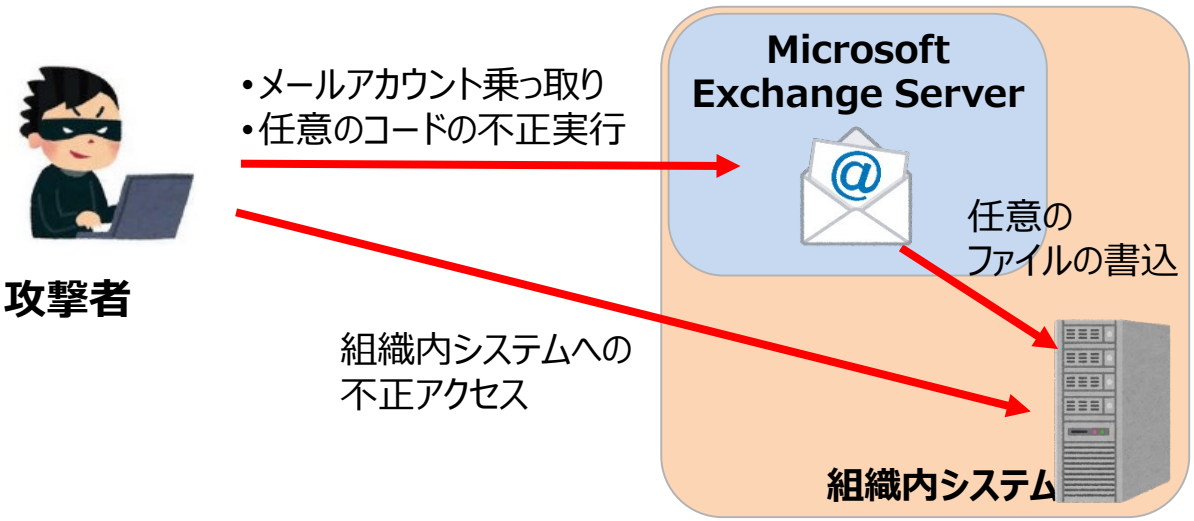
◆攻撃イメージ



Microsoft Exchange Serverを狙った国家支援型サイバー攻撃

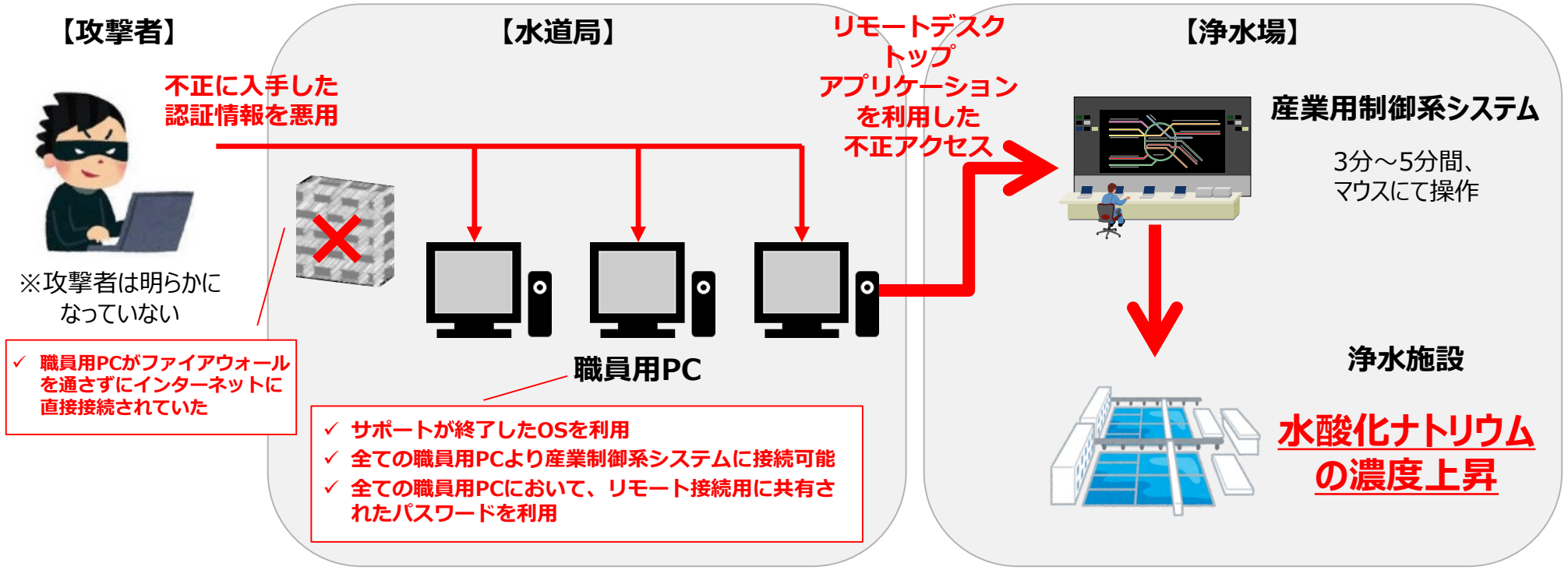
- 2021年3月2日、Microsoft社は**Microsoft Exchange Serverのゼロデイ脆弱性を悪用**した不正アクセス事案の発生及び当該脆弱性のセキュリティパッチを公表した。
- 本脆弱性を悪用することで、**Eメールアカウントの乗っ取りの他、攻撃者がさらなるシステム侵害を行うためのバックドアが設置**されるおそれがある。そのため、パッチの適用のみならず、侵害の有無の確認及び影響の排除を行う必要がある。
- 本事案が判明した時点で、**全世界で数十万にのぼる組織が攻撃を受けた**とされている。
- Microsoft社は、**中国の支援を受けた攻撃グループによる犯行**の可能性が高いとしている。

◆攻撃イメージ



水道システムへの不正アクセス事例

- 2021年2月、アメリカフロリダ州オールズマー市水道局は、**水道における産業用制御系システムを対象とした不正アクセス**によって、飲用水に含まれる水酸化ナトリウムの量が一時的に通常の約100倍に上昇したと発表した。なお、オペレーターが異常に気付き、即座に設定を戻したため、実際の被害はなかったとされる。
- 報道によると、**職員用PCよりリモートデスクトップアプリケーションを利用して、**産業用制御系システムへの不正アクセスが行われたとされている。



（出典）各種公開情報に基づき経済産業省作成

2020年12月18日発出「注意喚起」のUpdate　～最新事例から得られる教訓

- 2020年12月18日発出の「注意喚起」以降に発生したサイバー攻撃の動向等を踏まえ、ソフトウェア・システム開発ベンダ、ユーザー企業が留意すべき点をまとめる。

ソフトウェア・システム開発ベンダが留意するべき事項

- **ソフトウェア開発工程のセキュア化**
  - ➡ 開発環境への侵入を前提に、ゼロトラスト等の仕組みを導入し、ソフトウェア開発工程全体をセキュア化する。
- **ソフトウェア構成情報(SBOM）や、緊急的な攻撃回避策等の迅速・確実な提供**
  - ➡ 提供するソフトウェア・サービスに関して、顧客自らが正確にリスクを把握できるように、SBOM等を提供する。
  - ➡ 情報漏えいにつながりうる機能追加を実施したり、新たな脆弱性等が発見された場合には、被害を最小限に留めるための攻撃回避策や対応策について、迅速かつ確実に提供し、顧客を丁寧にサポートする。
  - ➡ 上記の問題が発生し、全ての顧客と相対で速やかに対応することが難しい場合、問題と対処法を速やかに公表する。

ユーザ企業が留意するべき事項

- **海外拠点（海外に業務委託している場合を含む）のセキュリティ対策の一層の強化**
  - ➡ 海外拠点経由のサイバー攻撃が急増していることや、海外の事業者に業務委託する中で情報流出が発生する懸念が明らかになってきていることを踏まえ、攻撃の起点となる脆弱なサーバ（野良サーバ等）が放置されていないか、サーバ上でWebshell等の危険度の高いツールが悪用される可能性がないか、業務委託している場合のアクセス範囲の設定などが適切になっているかなど、改めて総点検する。
- **利用中のシステム/クラウドサービスに関するリスクの永続的な見直しの実施**
  - ➡ システムを構築したまま放置したり、管理を委託先任せにしたりせずに、SBOM等を活用して関連する脆弱性情報を自ら積極的に把握し、迅速に対応できるようにする。
  - ➡ クラウドサービス利用時には、不都合な仕様変更がありうることを前提に、定期的な検証を実施する。

アクションプランの持続的発展と、新たな課題へのチャレンジへ

2020年12月18日発出「注意喚起」のUpdate

- サプライチェーン、クラウド、ファイル共有、制御系を狙った高度なサイバー攻撃事例
- 最新の攻撃事例を踏まえた対策のアップデート

Cyber New Normalにおける５つの処方箋　＜１～3年＞　（継続）

- **デジタル化が急加速する中でのサイバー脅威の常態化 “Cyber New Normal”**
  - ① 「開発のための投資」から「検証のための投資」へのシフト
  - ② サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定
  - ③ セキュリティとセーフティの融合への対応
  - ④ サプライチェーンセキュリティ確保のための産業界一丸となった対応
  - ⑤ Like-mindedの関係強化

国としての対処能力の強化　＜ 1～5年 ＞　New !

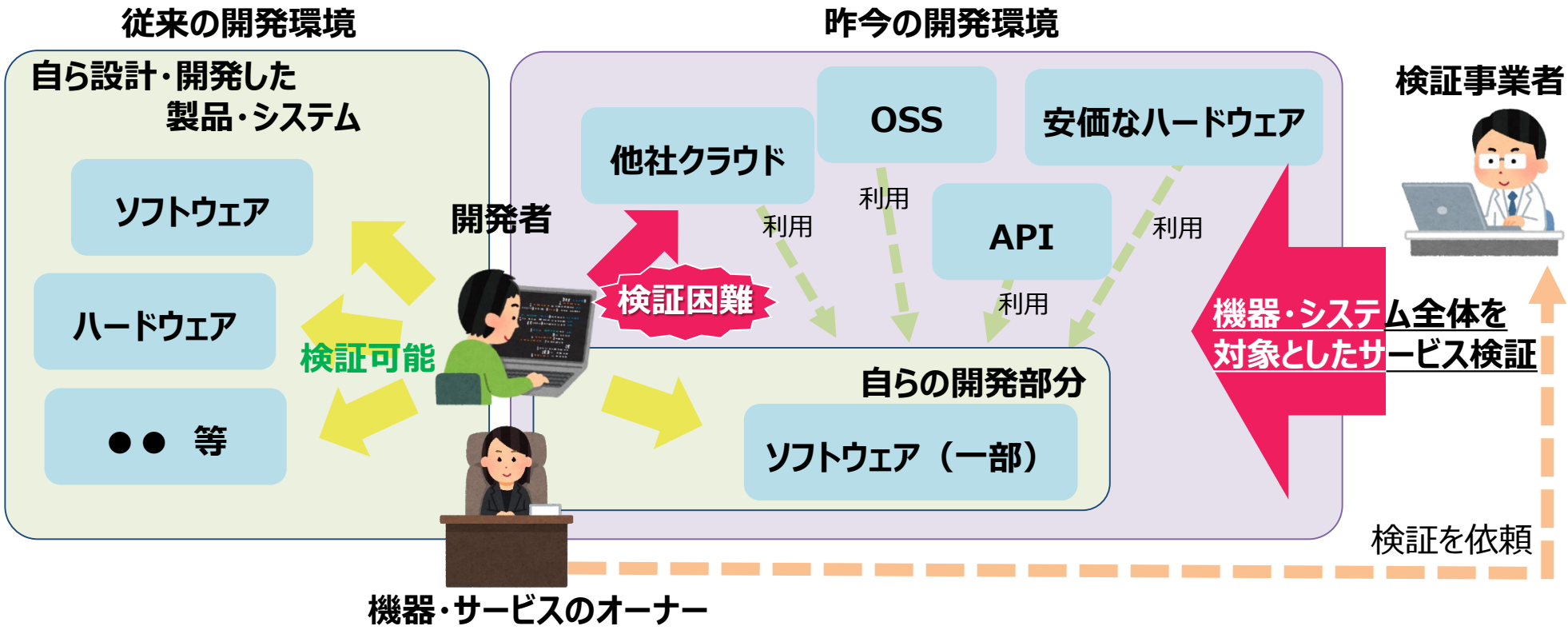
- 国としての対処能力の構築

For the future infrastructure　＜3～5年＞　（継続）

- **重要インフラ産業の“基盤インフラ”も仮想化時代へ突入**
  - ➢ インフラの機能を支える“高信頼な基盤インフラ”の構築・保守能力の確保

1 「開発のための投資」から「検証のための投資」へのシフト

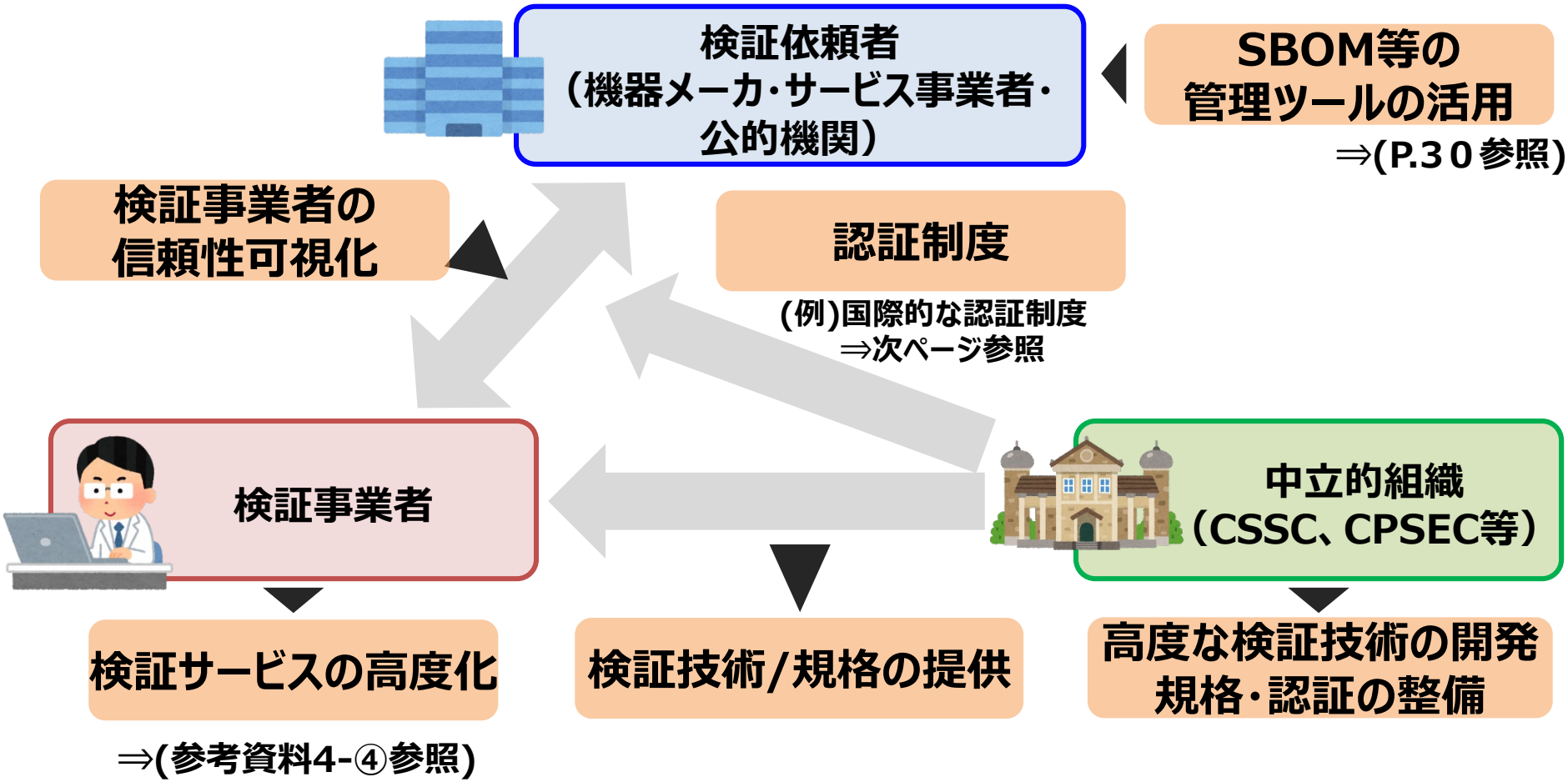
- 近年では**クラウドやIoTなどの新しい技術の活用が進み、またオープンAPIやOSSが充実したことで、必要な“機能”を容易に調達してシステム構築できる環境**になっており、**開発者自身がシステム全体を把握・検証することが困難**になりつつある。
- こうした環境の変化で、**官民において第三者によるセキュリティ検証の必要性が増大**し、**検証ビジネスの需要が拡大し、産業として重要になっていく**と考えられる。



1 「開発のための投資」から「検証のための投資」へのシフト

- サイバー・フィジカル一体社会が到来する今、**従来の「開発」中心の投資から、「検証」中心の投資行動へのシフトが求められる**のではないか。
- 「検証」中心の投資行動を促す政策はどうあるべきか。

「検証のための投資」活性化に向けた施策の体系（イメージ）

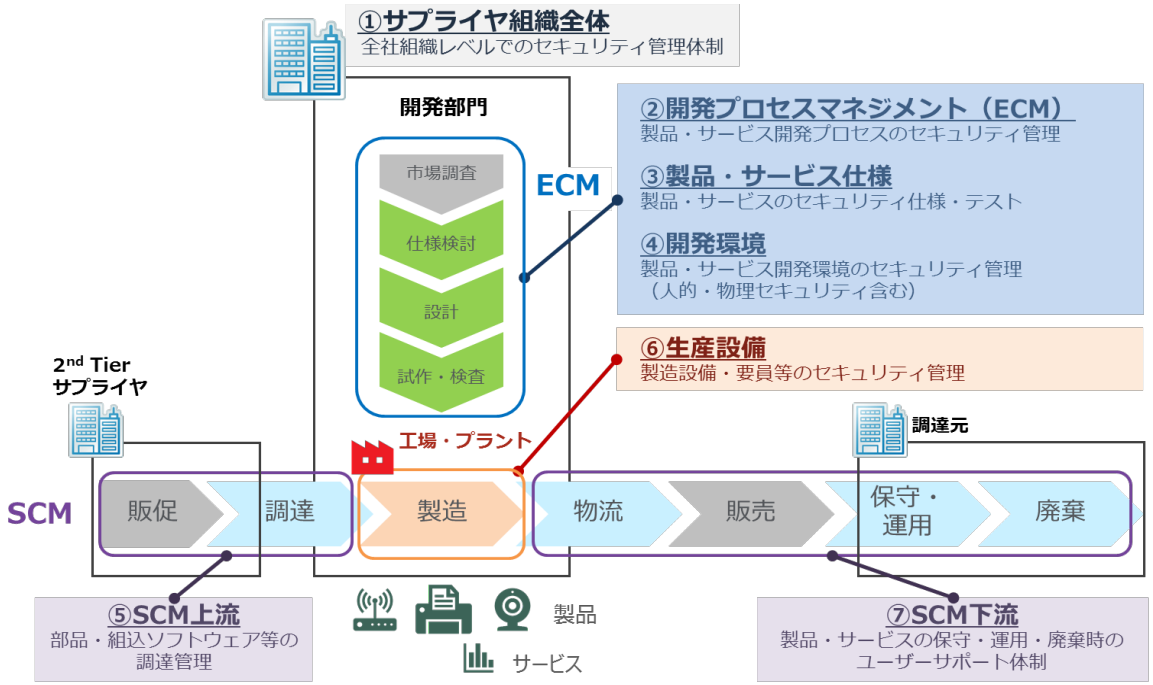


1 「開発のための投資」から「検証のための投資」へのシフト ～電力関連機器等のセキュリティ評価手法の確立（CPIC）

- 攻撃起点がサプライチェーンを通じて広がり、**重要機器のサプライチェーンリスクを管理するためのセキュリティ評価・可視化手法が必要**に。
- CPIC（Cyber Product International Certification：重要インフラに対するサイバー攻撃等の脅威に対処するための国際組織EIS Council が立ち上げた、米・英・イスラエルの官民を中心としたプロジェクト）においてその手法が議論されている。
- 国際的なステークホルダ間で、**サプライチェーンまで含めた機器の高いレベルの安全性を確保**できるように、日本主導で、国内電力事業者及びベンダーの協力による任意の認証制度の確立を目指す。

日本国内で検討中の素案

①ECM/SCM全体を考慮した評価カテゴリ分類



②スコアカード方式を活用した動的評価手法

図はクラウドサービスを事例としたイメージ

2 サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定

- データマネジメントに関する定義を明確化し、フレームを設定することで、主体間を転々流通するデータに関する**リスクポイントの洗い出しを可能に**する。
- また、本枠組みを**共通の定規として利用**することで、各国・地域などの**主体間のデータに関するルールのギャップ/データの流通プロトコルの問題を可視化、データの囲い込みを回避する**取組につなげる。

データマネジメントの新たな捉え方

▶データの "**属性**" が "**場**" における "**イベント**" により変化する過程をライフサイクル全体にわたって管理すること

属性
データが有する性質

✖

場
特定の規範を共有する範囲

✖

イベント
データの属性を生成・変化させる処理

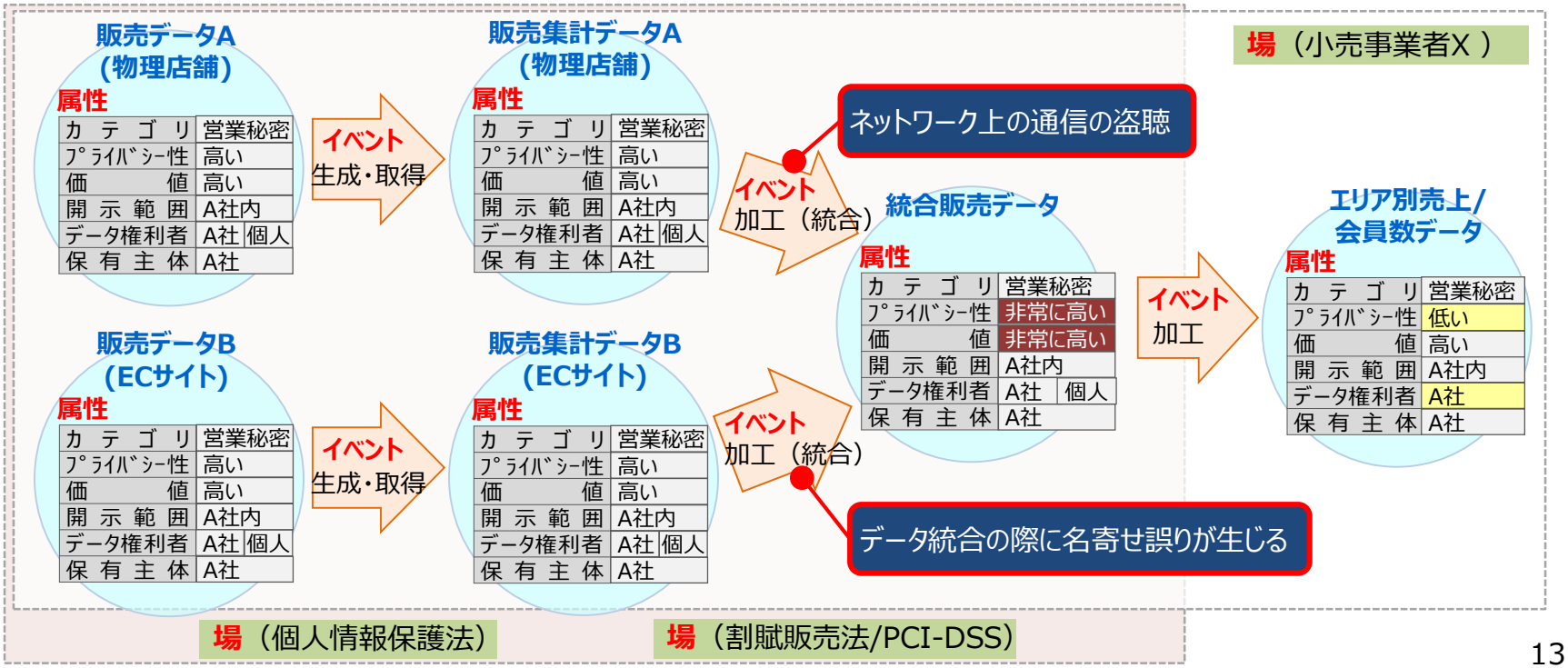
新たな捉え方への当てはめステップ（小売業におけるPOSデータの活用事例）

STEP 1
データ処理フロー(イベント)の可視化

STEP 2
必要な制度的な保護措置(場)の整理

STEP 3
「属性」の具体化

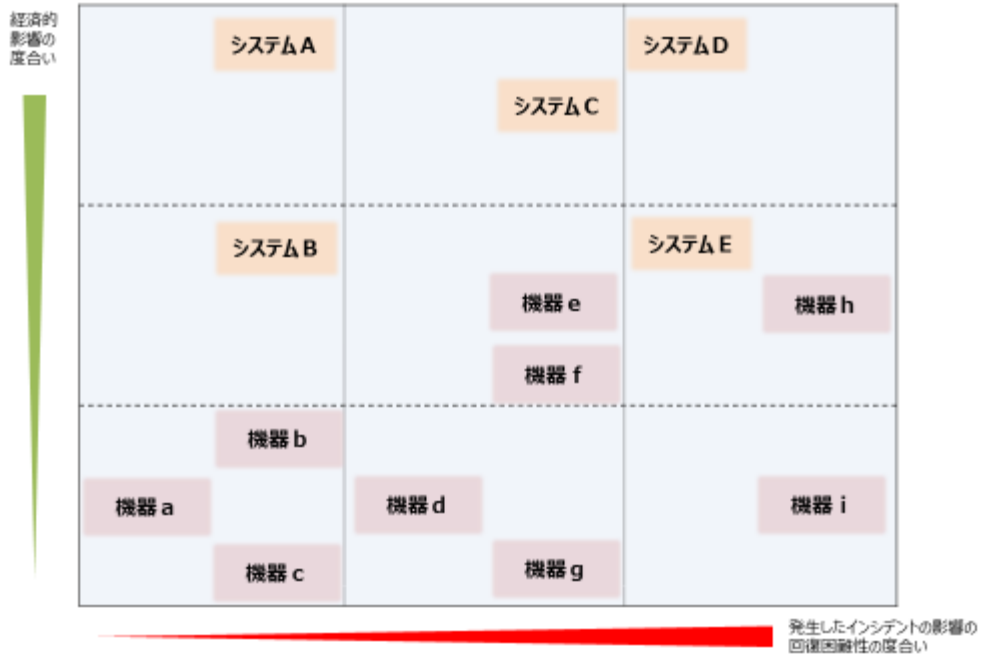
STEP 4
イベントごとのリスクの洗い出し



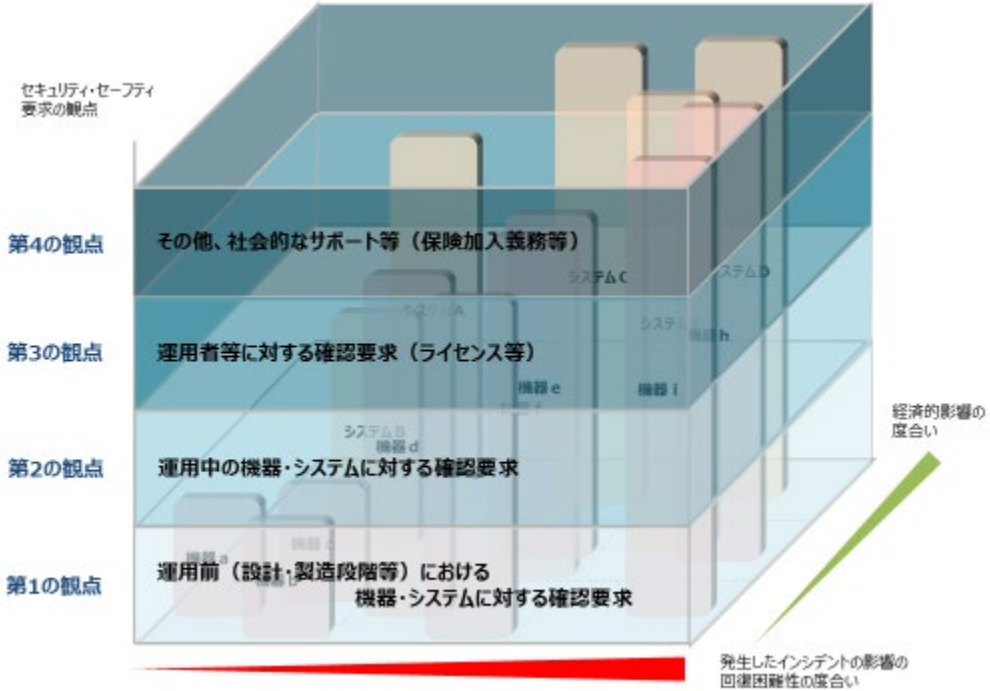
3 セキュリティとセーフティの融合への対応 ～IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

- **用途や使用環境によって課題が異なるIoT機器・システムに対するセキュリティ対策を、複数のステークホルダ間で合意する**際に活用できる**「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」を2020年11月5日に公開。**
- 本フレームワークで、IoT機器・システムをカテゴライズし、カテゴリごとに求められるセキュリティ・セーフティ要求の観点を把握・比較することにより、**それぞれに求める対策の観点・内容の整合性を確保できる**。

フィジカル・サイバー間をつなげる
機器・システムのカテゴライズのイメージ



カテゴリに応じて求められる
セキュリティ・セーフティ要求の観点のイメージ



※ 同じ機器・システムでも使用形態などによってマッピング先が異なり得る。
例えば、機器ｇと機器ｈが同じ機器で異なる使用形態である場合などがあり得る。）

3 セキュリティとセーフティの融合への対応 ～欧州NLF関連指令、IECのサイバーセキュリティ関連、製品安全分野における検討

- 欧州では、各NLF関連指令・規則に**サイバーセキュリティの要素を盛り込む**検討が進行。国際電気標準会議(IEC)においても、遠隔通信を行う**IoT機器にサイバーセキュリティの要素を要求する**動き。
- 日本では、平成30年度より**IoT化が進む製品を中心に製品安全確保の在り方**に関する検討会及び業界団体等によるワーキンググループを設置。令和２年度末以降、ガイドラインを取りまとめる予定。

欧州：各NLF関連指令の検討状況（例）

NLF関連指令	検討状況
無線指令(RED)	・**2021年Q2に改正予定** ・**EN 303 645**(消費者IoTに係る欧州標準)の参照を検討中。
機械指令（MD）	・**2021年Q1に改正予定**。 ・**IEC 62443**の参照を検討中。
一般製品安全指令(GPSD)	・**2021年Q2に改正予定** ・**サイバーセキュリティ要素の導入を検討中**

製品安全分野におけるサイバーセキュリティ関係の動き

規格	主な要求事項
IEC60335-1 (家庭用及びこれに類する電気機器の安全性 第1部：通則)	• 2020年9月発行 • 公衆ネットワークを介した遠隔通信に関する権限承認、暗号技術の適用等の製品安全に係るセキュリティ要求等を整理。

日本：製品安全分野における検討

IoT化を念頭にした製品安全対策を検討する有識者会議を設置。ガイドラインをとりまとめる予定。

●検討の背景
従来の製品安全対策では想定されていなかったインターネットを介した遠隔操作を念頭に、生命・身体に危害等が及ばぬよう追加すべき対策などを整理する。

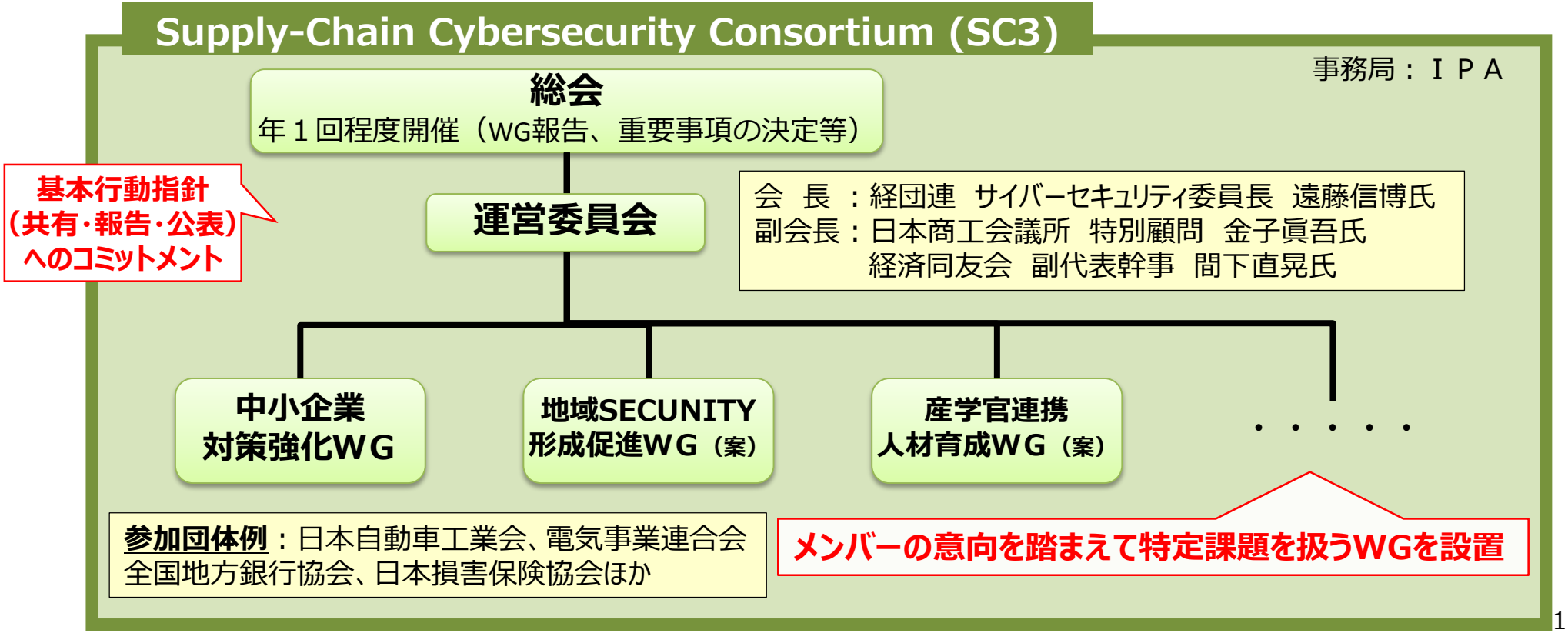
●委員構成
セーフティ及びセキュリティ分野の専門委員、業界団体 等

●検討内容
IoT化が進展している製品を中心に、インターネットを介し遠隔操作された場合のリスクシナリオ及びユースケースの検討を実施。

●令和2年度の取組
製品設計上の対応、安全機能のあり方などを整理。IoT化等製品の安全確保の在り方に関するガイドラインを策定検討。今後公表する予定。

4 サプライチェーンセキュリティ確保のための産業界一丸となった対応 ～サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）～

- **趣　旨:** 大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ、「基本行動指針※」の実践と中小企業・地域を含めたサプライチェーンのサイバーセキュリティ対策を産業界全体の活動として展開していく。
  ※サイバー攻撃事案発生時における、「共有、報告、公表」によるリスクマネジメントの徹底。
- **参加者:** 経済団体、業種別業界団体　等（2020年2月末時点で169会員）
- **設立日:** 2020年11月1日（設立総会：2020年11月19日）
- **活　動:** 特定の課題についてWGを設置し、具体的アクションを展開。



4 サプライチェーンセキュリティ確保のための産業界一丸となった対応 ～Supply-Chain Cybersecurity Consortium（SC3）の今後の活動方針

- 産業界全体で取り組むべきサプライチェーンセキュリティ対策の浸透のため、産学官連携や経営層の啓発、地域・業界別の取組等を加速するプラットフォームとしての機能に期待。

最新攻撃
動向・対策

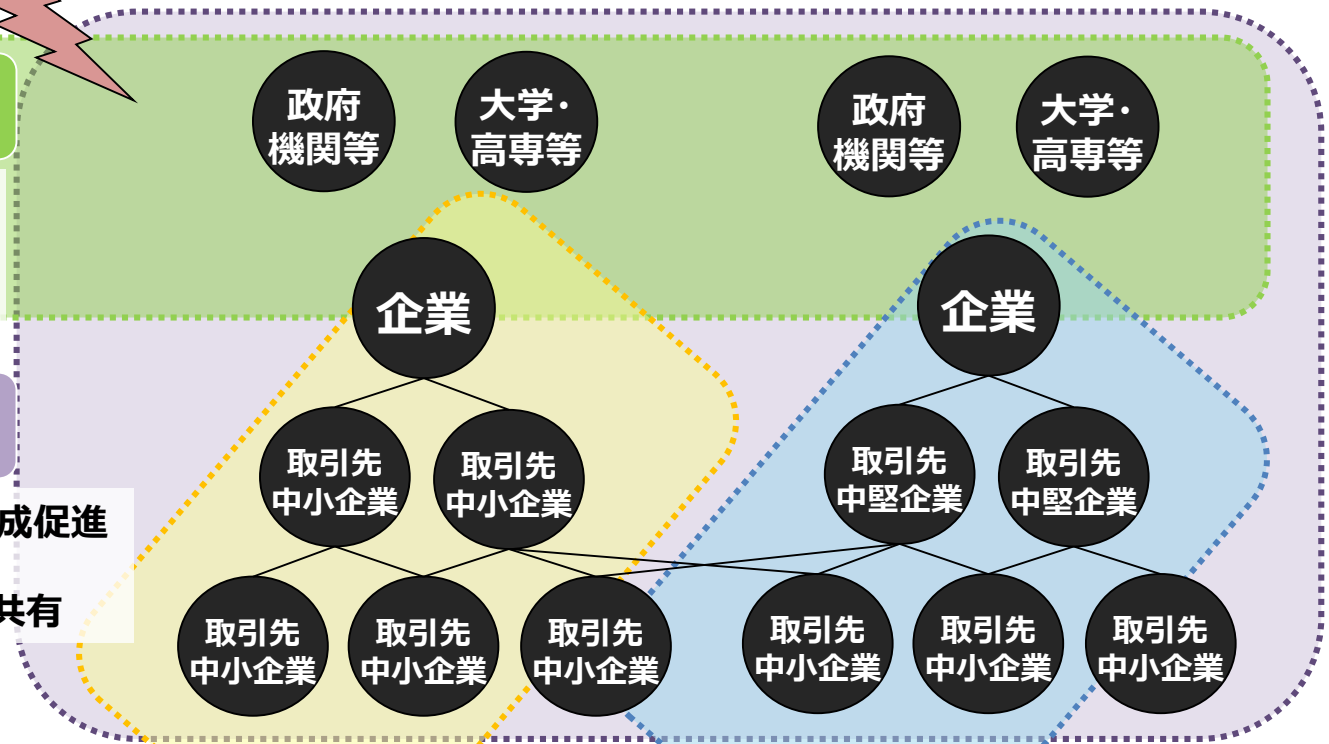
- 新たな脅威への対抗、サイバー攻撃動向の共有、対策検討
- 経営層向け注意喚起、WGやウェビナーでのプラクティス共有

産学官連携

- 産学官連携促進
- 人材育成
- 共同研究

地域SECUNITY
形成促進

- 地域SECUNITY形成促進
- 悩み・課題共有
- 解決策・プラクティス共有



中小企業
対策強化WG

- 中小企業対策促進
- サイバーセキュリティお助け隊の普及
- 悩み・課題・解決策・プラクティス共有

業界ごとのサプライチェーン対策

- ビル、自動車、電力、防衛、スマートホーム、宇宙などの業界別の取組の共有
- 他分野への横展開

5 Like-mindedの関係強化

- 日本の取組を国際的なものとするため、**CPSFや産業分野別/分野横断課題への検討成果を海外へ発信し国際的な議論に貢献**。

WG1 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）

産業分野別の検討
- ビルSWG：ビルシステムガイドライン
- 自動車SWG：自工会/部工会・サイバーセキュリティガイドライン
- スマートホームSWG：スマートホームガイドライン

分野横断的な課題の検討
- 第3層TF：データマネジメントの新たな捉え方（案）
- ソフトウェアTF：OSSの利活用に関する事例集
- 第2層TF：IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）

英語版公開／公開予定

国際標準化団体へ提案

成果を海外へも発信。
米国・欧州との対話を継続し、
共通認識のレベルを深め、
議論の仲介を図る。

5 Like-mindedの関係強化 ～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インプットとした国際規格の策定

- 国内エキスパートへ協力を仰ぎ、ISO/IECにおいて**CPSFのモデル等をインプットとした国際規格**の策定を推進。
- 他国の関連文書も考慮しながら、**CPSFのモデルをサイバー・フィジカル・システム（CPS）をとらえるモデルの一つとして位置づけ**、SC27/WG4 に**Technical Report（TR）を提案**している。
- 他SCの国内外エキスパートとも連携しながら、PWI（予備業務項目）としての議論を継続中。

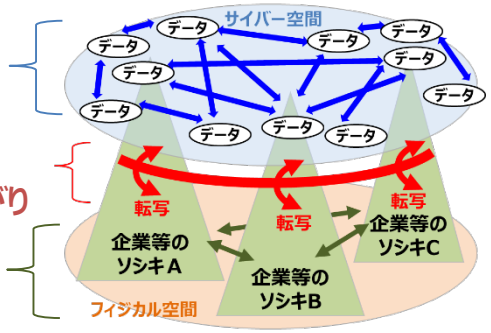
CPSFのモデル

<3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



<6つの構成要素>

ソシキ	ヒト	モノ
データ	プロシージャ	システム

国際標準化団体へ提案

・「3層構造」
・「6つの構成要素」
というCPSFのモデル等をインプットとしたTRを提案

ISO / IEC
↓
JTC1
↓
SC27
↓
WG4

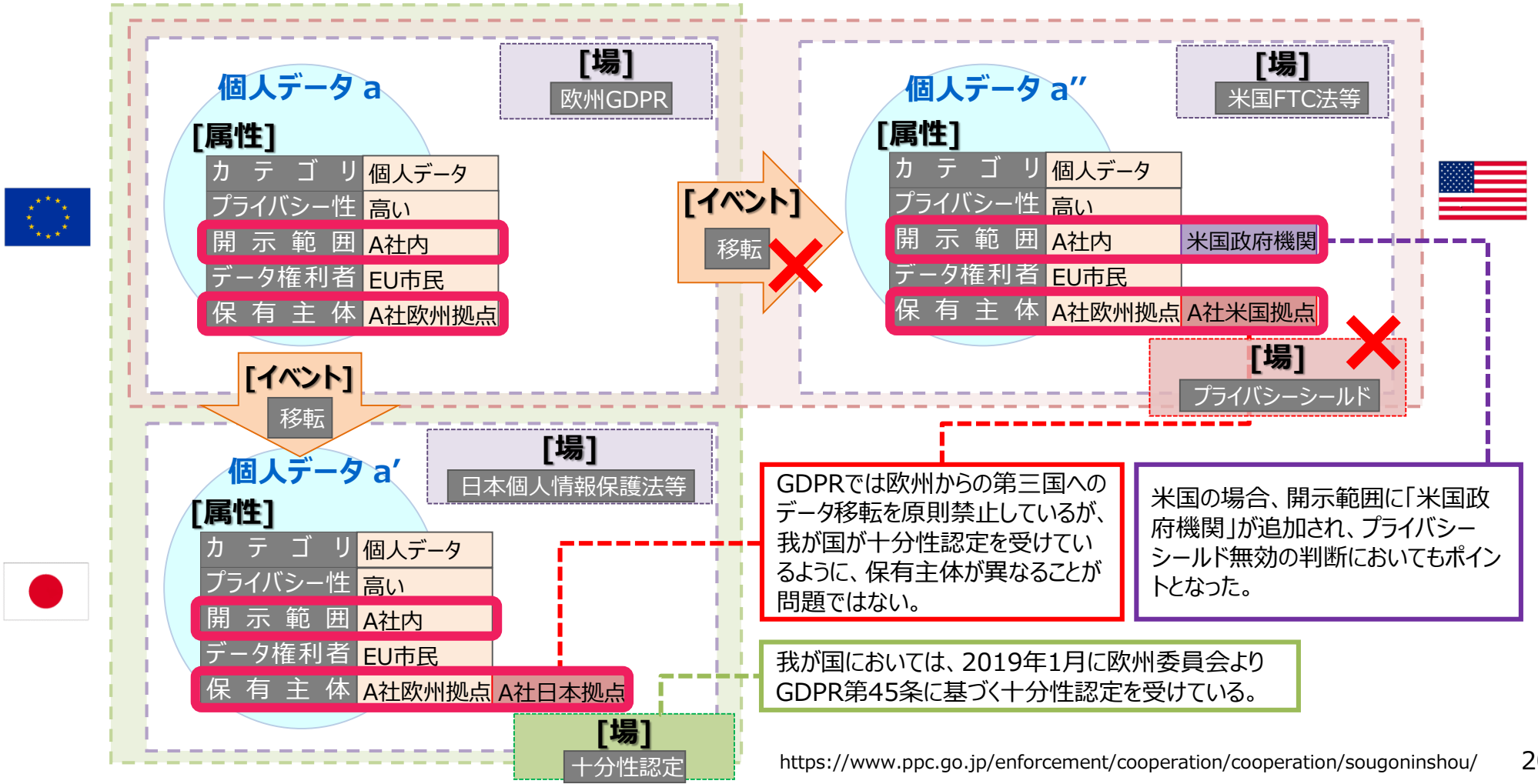
SC27/WG4において、これまでにPWIとして3度の意見募集を実施。
さらに議論を深め、国際規格（TR）の策定を目指す。

2020.4 1st PWI → 2020.9 2nd PWI → **2020.12 3rd PWI** → WD → TR発行

※今後のスケジュールは経済産業省および対応中のエキスパートによる想定

5 Like-mindedの関係強化 ～データマネジメント（第3層の取組）

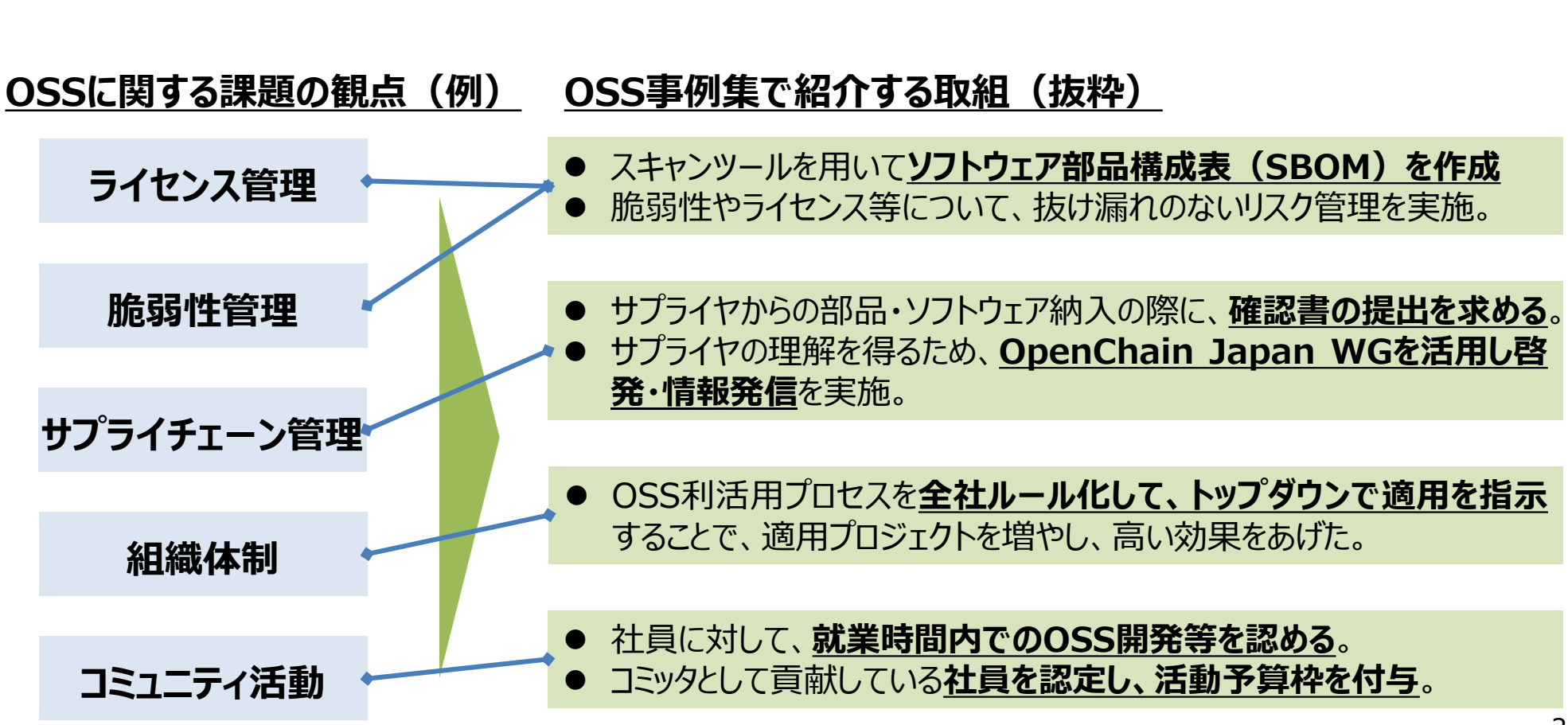
- データの取扱いに関する各国・地域のルールに対し、データマネジメントのフレームを当てはめることで、**<u>各国・地域のルール間のギャップ（凸凹）を把握しリスクポイントを可視化することが可能に</u>**。
- GDPRに関するSchrems Ⅱ判決の事例では、欧州からの個人データの移転に関し、プライバシーシールドが無効と判断された米国と、十分性認定を受けている我が国の制度の違いを可視化可能。



https://www.ppc.go.jp/enforcement/cooperation/cooperation/sougoninshou/

5 Like-mindedの関係強化 ～ソフトウェアTFの取組（OSS事例集）

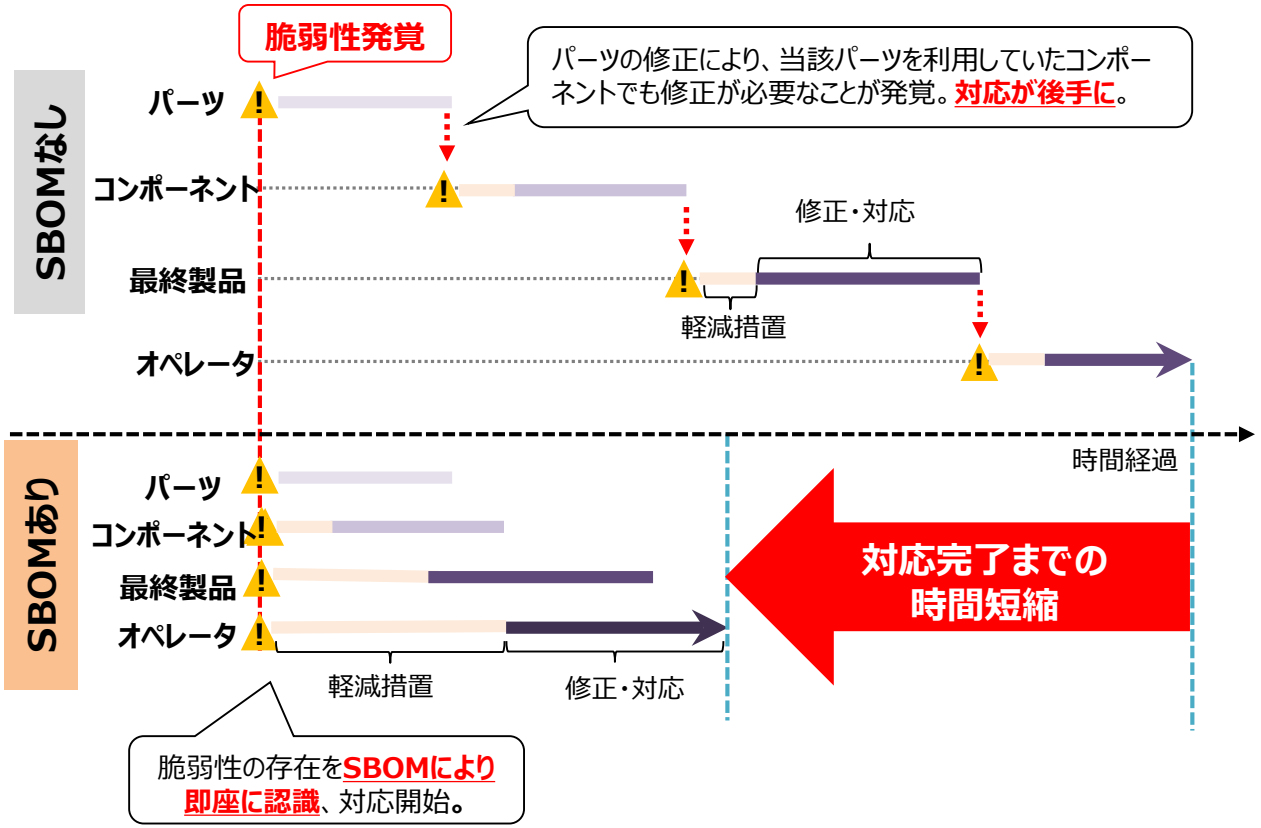
- OSSの利用が広がる一方、自社だけでOSSを検証するための体制等を整えることの負担は大きく、日本だけはなく米国でもベストプラクティスを共有することに対するニーズが存在。
- **「OSSの利活用及びセキュリティ確保に向けた管理手法」をまとめた事例集**を作成し、参考となる事例を共有して企業における適切なOSS利用を促進。日本から働きかけることで日米でOSSの活用・管理に関するベストプラクティスを共有する機会の確保を目指す。



5 Like-mindedの関係強化 ～ソフトウェアTFの取組（SBOM）

- ソフトウェアの成分構成を表す**SBOM（Software Bill of Materials）**を活用することにより、**ソフトウェアに何が含まれ、誰が作り、どのような構成となっているか**等の把握が容易になる。
- 米国NTIAが2018年から主導するSoftware Component Transparencyでは、ヘルスケア分野における実証事業（PoC）に続いて、自動車産業・電力分野にも取組が拡大。
- 日本においても業界構造や商習慣を考慮しつつ、SBOM活用に向けた実証事業の実施を検討。

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



米国NTIAにおけるSBOMのPoC

ヘルスケア分野（病院、医療機器）

病院、医療機器メーカー、ベンダーが参加。2回のPoCを経てSBOM活用の手法、課題等を公開。

自動車産業分野

Auto-ISACを中心としたサプライヤ中心のプロジェクト。12ヶ月ほどかけてサプライヤの推奨事項をとりまとめる予定。

電力分野

1/26キックオフ。米国エネルギー省からもプレゼンターとして参加。

アクションプランの持続的発展と、新たな課題へのチャレンジへ

2020年12月18日発出「注意喚起」のUpdate

- サプライチェーン、クラウド、ファイル共有、制御系を狙った高度なサイバー攻撃事例
- 最新の攻撃事例を踏まえた対策のアップデート

Cyber New Normalにおける５つの処方箋　＜１～3年＞　（継続）

- デジタル化が急加速する中でのサイバー脅威の常態化 “Cyber New Normal”

① 「開発のための投資」から「検証のための投資」へのシフト
② サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定
③ セキュリティとセーフティの融合への対応
④ サプライチェーンセキュリティ確保のための産業界一丸となった対応
⑤ Like-mindedの関係強化

国としての対処能力の強化　＜ 1～5年 ＞　New !

- **国としての対処能力の構築**

For the future infrastructure　＜3～5年＞　（継続）

- 重要インフラ産業の“基盤インフラ”も仮想化時代へ突入
  - インフラの機能を支える“高信頼な基盤インフラ”の構築・保守能力の確保

国としての対処能力の強化

- サイバー攻撃の高度化・激化が進んでいる中、**サイバー攻撃に対して対処する能力を強化すべき**という議論がある。産業界のサイバーセキュリティ対策を推進する経済産業省として、どのように貢献すべきか。

第26回サイバーセキュリティ戦略本部（令和３年２月９日）における議論

※太字・下線は事務局にて追記

「次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方」（令和３年２月９日サイバーセキュリティ戦略本部決定）より

第二　政府の役割を意識した政策立案の基礎となるものにすること（抄）

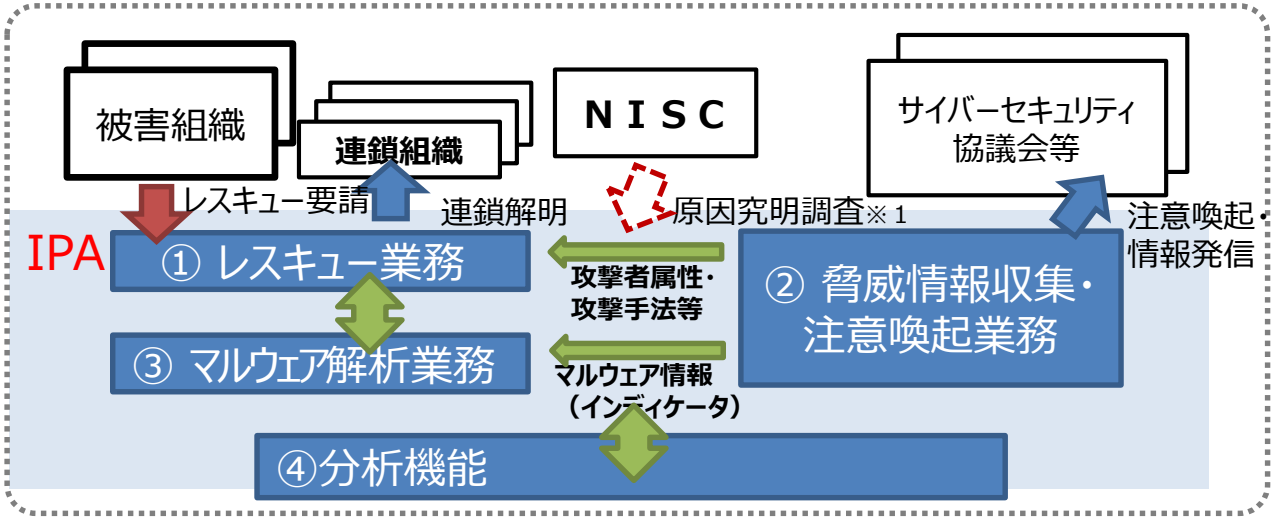
サイバー空間においては、関連技術の進展が早く、攻撃者優位ともされる中で、それぞれの主体が自らの役割を認識し対応するとともに、互いに連携・協働して取り組むことができる環境が重要。政府としては、社会全体を俯瞰した上で、攻撃者との非対称な状況の改善も含め、**自律的な取組や多様な主体の緊密連携、組織化・洗練化されたサイバー攻撃に対する公的機関の取組が効率的かつ戦略的に実現できるよう適切な対策を進める**など政府の役割を意識した政策立案の基礎となるものにすること。（以下略）

経産省としての取組例：J-CRAT

IPAのサイバーレスキュー隊（J-CRAT）は事案対処（レスキュー）で得られた知見をもとに、情報収集・分析機能を強化している。

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



※１　サイバーセキュリティ基本法（H28/4施行）第30条に定める原因究明のための調査

国としての対処能力の強化
～サイバーインシデントに係る事故調査の体制整備に向けた検討の開始

- サイバー攻撃がフィジカル領域に大きな影響を及ぼすようになり、経済活動の基盤を守るためには、**プラント等の事故が発生した場合に、サイバーインシデントの観点からの原因究明可能な機能**を有することが必要に（いわゆる「サイバー事故調」）。
- 産業サイバーセキュリティセンター（ICSCoE）は、**2025年を目途にサイバーインシデントに係る「事故調」機能を整備**するため、事故調査に必要な能力、体制、人材等に係る議論を開始。

サイバーインシデントに係る事故調査のイメージ

アクションプランの持続的発展と、新たな課題へのチャレンジへ

2020年12月18日発出「注意喚起」のUpdate

- サプライチェーン、クラウド、ファイル共有、制御系を狙った高度なサイバー攻撃事例
- 最新の攻撃事例を踏まえた対策のアップデート

Cyber New Normalにおける５つの処方箋　＜１～3年＞　（継続）

- デジタル化が急加速する中でのサイバー脅威の常態化 “Cyber New Normal”

① 「開発のための投資」から「検証のための投資」へのシフト
② サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定
③ セキュリティとセーフティの融合への対応
④ サプライチェーンセキュリティ確保のための産業界一丸となった対応
⑤ Like-mindedの関係強化

国としての対処能力の強化　＜ 1～5年 ＞　New !

- 国としての対処能力の構築

For the future infrastructure　＜3～5年＞　（継続）

- **重要インフラ産業の“基盤インフラ”も仮想化時代へ突入**
  - インフラの機能を支える“高信頼な基盤インフラ”の構築・保守能力の確保

社会インフラの将来像（基盤インフラ）

- 今後の社会インフラ（電力、工場、スーパーシティ等）は**ソフトウェア/仮想化基盤の上のアプリケーションとして実現**される流れ。
- 将来像を見据えながら、「要素技術の研究開発」、「次世代データセンター戦略」、「アーキテクチャ設計」「実証実験」の4つの軸で推進していく。

要素技術の研究開発

- ポスト5G情報通信システム基盤強化研究開発事業
- 2050年カーボンニュートラルに伴うグリーン成長戦略　　等

次世代データセンター戦略（経産省、総務省）

グリーン by デジタル
・データセンター国内立地推進
・再エネ導入支援
グリーン of デジタル
・データセンターの省エネ・高度化
（ソフトウェア処理効率化による省エネ化）

社会インフラ向け基盤の検討

社会システムや産業構造の全体最適な設計を通じ、総合的な信頼性等の確保と日本の産業競争力の強化を図る。

デジタルアーキテクチャ・デザインセンター IPA

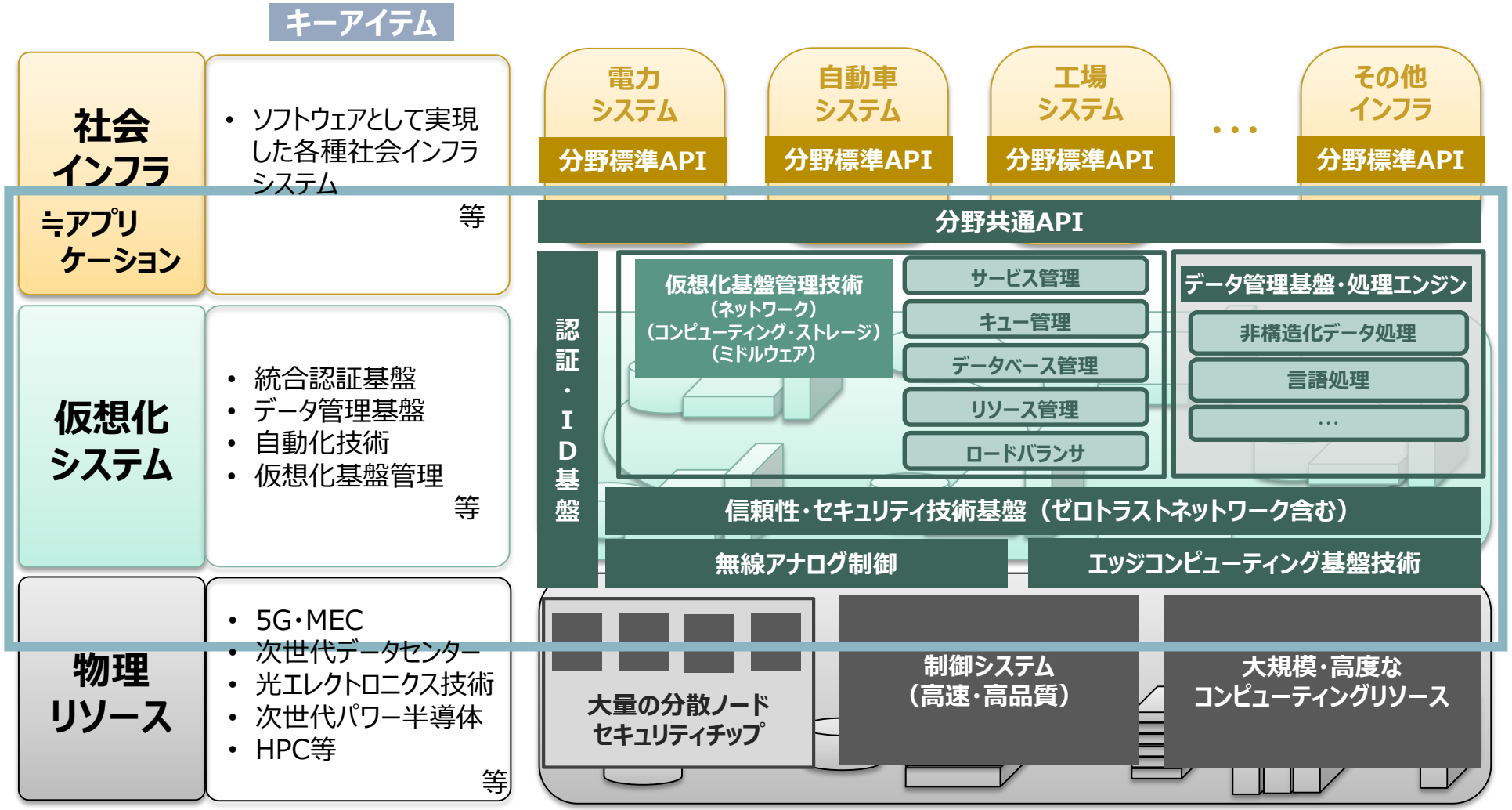
アーキテクチャ設計（IPAデジタルアーキテクチャ・デザインセンター）

・スマートシティ/スーパーシティ
・スマートファクトリー　等

実証実験（イメージ）

社会インフラの将来像（基盤インフラ）

- ソフトウェア/仮想化基盤の共通的な体系である基盤インフラのアーキテクチャを設計・整理。
- 様々な要素技術の中から、将来の社会インフラの基盤に資するものを選択し研究開発を進める。




METI
Ministry of Economy, Trade and Industry