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

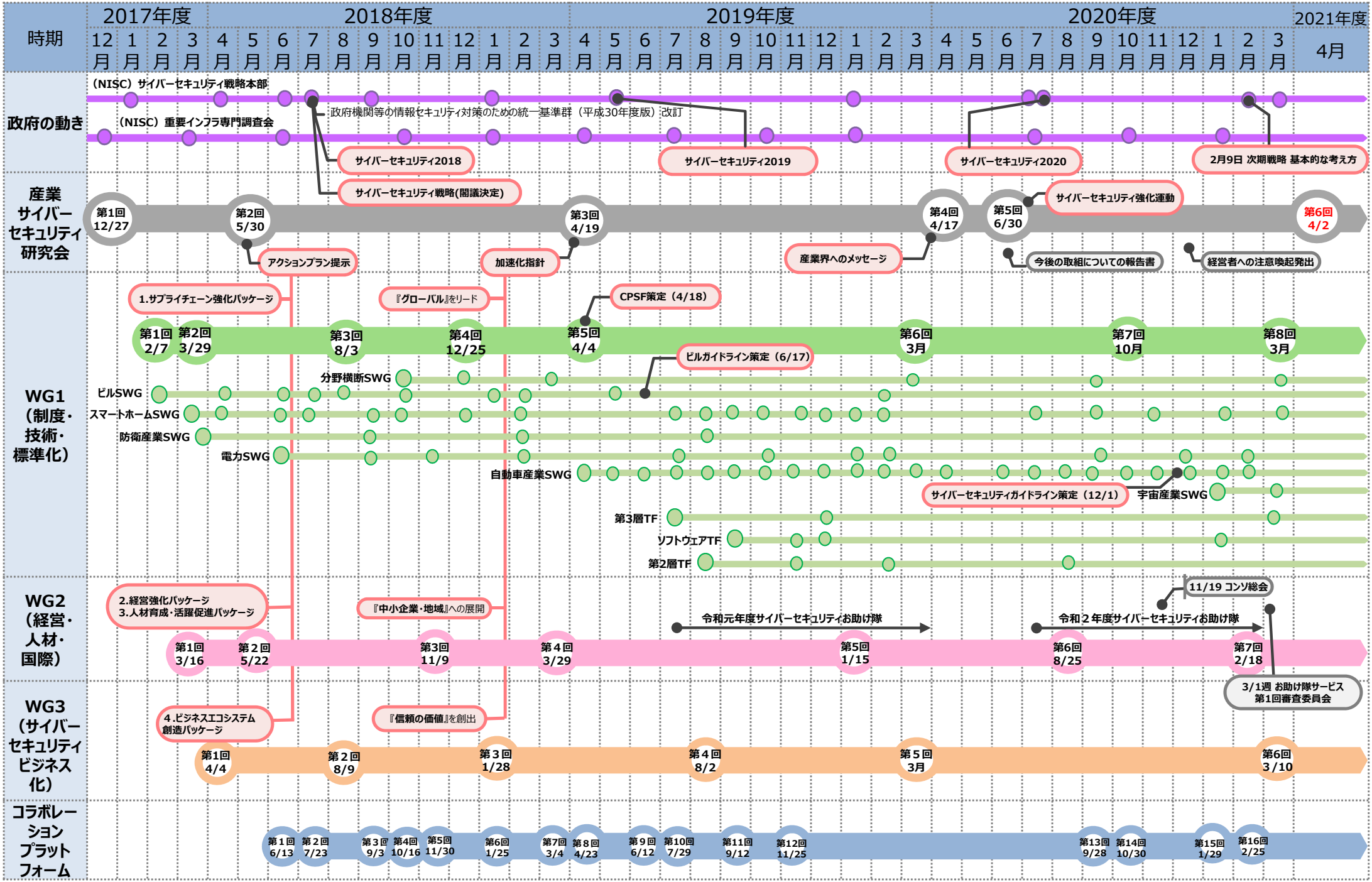
令和３年４月２日

経済産業省

商務情報政策局

復　習

産業サイバーセキュリティ研究会関連会議の実績



（復習）**アクションプランの4つの柱**

第2回研究会（2018年5月30日）において提示

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

- 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

2．サイバーセキュリティ経営強化パッケージ

- 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

3．サイバーセキュリティ人材育成・活躍促進パッケージ

- 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

4．セキュリティビジネスエコシステム創造パッケージ

- 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

（復習）

３つの「加速化指針」

第3回研究会（2019年4月19日）において提示

アクションプランを中心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　（Proven in 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

（復習）「産業界へのメッセージ」

第4回研究会（2020年4月17日）において提示

- 最近の**サイバー攻撃の高度化・攻撃起点の多様化**に加え、**新型コロナウィルスによる混乱等に乗じたサイバー攻撃**が欧米を中心に増加していることから、各企業に対し、**直近の状況及び今後のデジタル化の急加速に対応するためのサイバーセキュリティの取組を促すメッセージ**を発出。

＜「産業界へのメッセージ」のポイント＞

① 直近の状況に対応するために取り組んでいただきたいこと

- **新型コロナウィルスを騙る不正アプリやフィッシングメール/SMS等に注意**すること。
- 機器・システムに対して、**アップデート等の基本的な対策**をできるだけ実施すること。 等

② デジタル化を進めていく中で取組を進めていただきたいこと

1　事前対策の確認・強化

- **サプライチェーン全体を視野に入れたリスク管理**を行うこと。
- **パッチ当て等の基本的対策**に加え、振る舞い検知など、既存の対策を**すり抜けた攻撃を防御・検知する仕組み**を導入。等

2　事後対策の強化確認

- 適切な**初動対応を行う体制と計画を整備**すること。
- 平時の**“防災訓練”を徹底**して行うこと。

（産業界へのメッセージ）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf

（復習）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

第5回研究会（2020年6月30日）において提示

アクションプランの高度化　＜1～3年＞

- **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 (サイバー・ニュー・ノーマル)”
  - アクションプランの面的な拡大／質の高度化
  - 積極的サイバー防御を支える基盤の強化

For the future infrastructure　＜3～5年＞

- **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

「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」

2020年12月18日公開資料

●サイバー攻撃は規模や烈度の増大とともに多様化する傾向にあり、実務者がこれまでの取組を継続するだけでは対応困難になっている。

●アップデート等の基本的な対策の徹底とともに、**改めて経営者のリーダーシップが必要に**。

① 攻撃は格段に高度化し、被害の形態も様々な関係者を巻き込む複雑なものになり、技術的な対策だけではなく関係者との調整や事業継続等の判断が必要に。改めて経営者がリーダーシップを。

② ランサムウェア攻撃による被害への対応は企業の信頼に直結。経営者でなければ判断できない問題。

●「二重の脅迫※」によって、顧客等の情報を露出させることになるリスクに直面。日常的業務の見直しを含む事前対策から情報露出に対応する事後対応まで、経営者でなければ対応の判断が困難。

●金銭支払いは犯罪組織への資金提供とみなされ、制裁を受ける可能性のあるコンプライアンスの問題。

③ 海外拠点とのシステム統合を進める際、サイバーセキュリティを踏まえたグローバルガバナンスの確立を。

●国・地域によってインターネット環境やIT産業の状況、データ管理に係るルール等が異なっており、海外拠点とのシステム統合を通じてセキュリティ上の脆弱性を持ち込んでしまう可能性も。

●拠点のある国・地域の環境をしっかりと評価し、リスクに対応したセグメンテーション等を施したシステム・アーキテクチャの導入や拠点間の情報共有ルールの整備等、グローバルガバナンスの確立が必要。

④ 基本行動指針（高密度な情報共有、機微技術情報の流出懸念時の報告、適切な場合の公表）**の徹底を。**

※攻撃者が、被攻撃企業が保有するデータ等を暗号化して事業妨害をするだけではなく、暗号化する前にあらかじめデータを窃取しておいて支払いに応じない場合には当該データを公開することで、被攻撃企業を金銭の支払いに応じざるをえない状況に追い込む攻撃形態。

経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起（2020年12月18日）」https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

本　編

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**

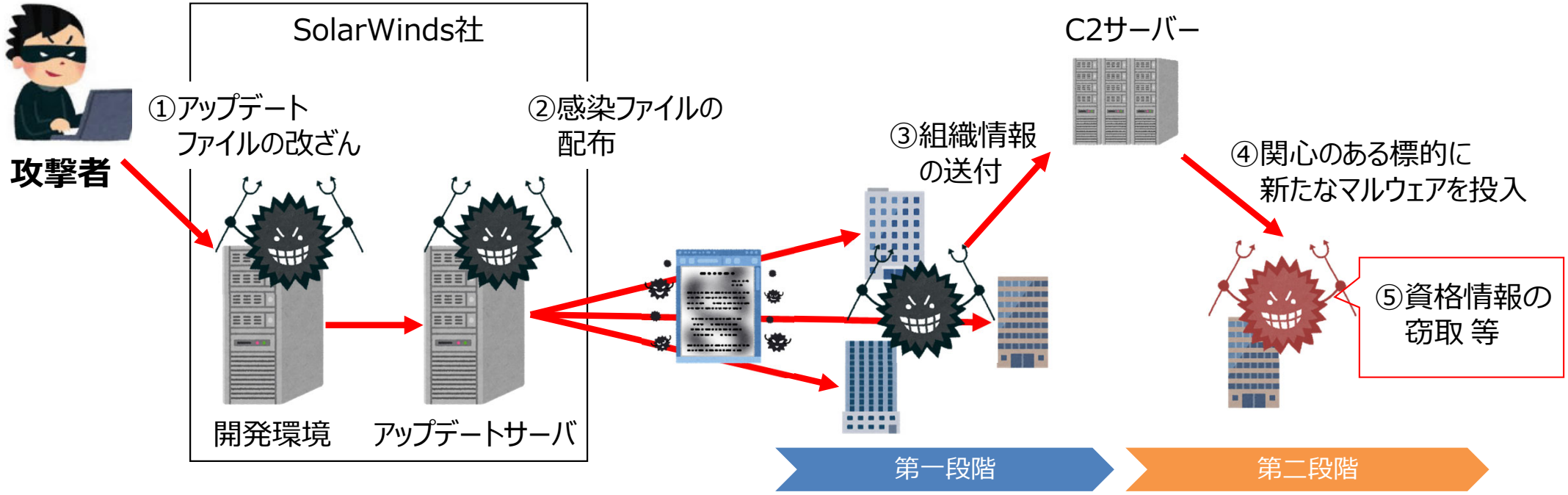
For the future infrastructure　＜3～5年＞　（継続）

- **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

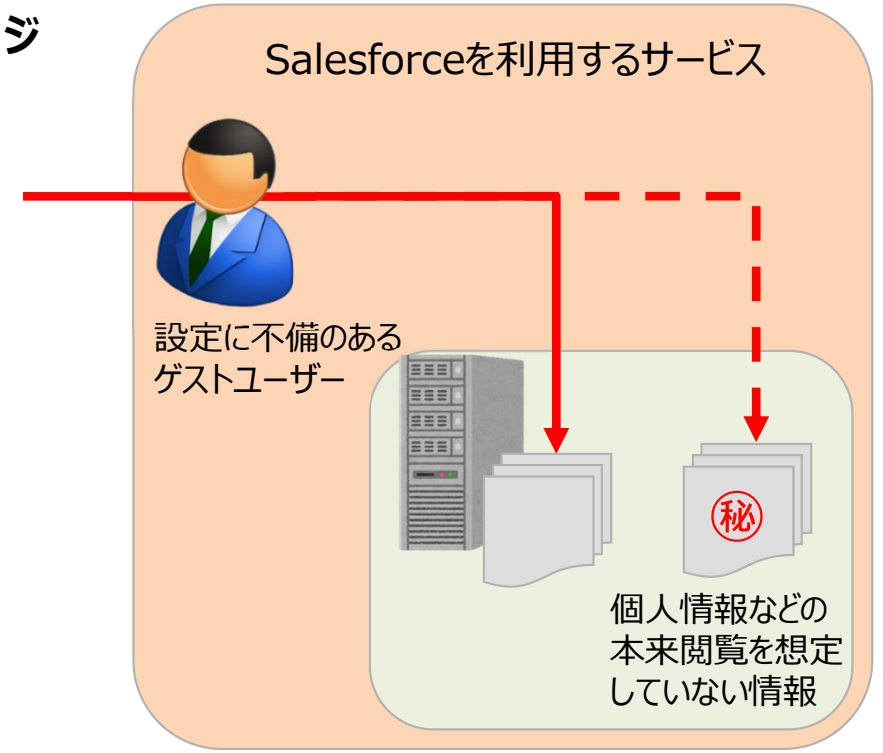
- 2020年12月25日、セールスフォース・ドットコムは、同社が提供するサービスにおける**ゲストユーザーに対する情報共有に関する設定が適切に行われていない場合、一部情報が第三者より閲覧できる**事象の発生を公表。また、**複数の国内事業者が本事象による不正アクセス及び個人情報漏えいの発生**を公表。
- 本サービスを組み込んだシステムがパッケージとして複数の顧客に提供され、同時に被害が発生したケースも。
- クラウドサービスを活用する際には、サービスの利用状況や各種設定の確認・見直しを行うなど、適切なセキュリティ対策を講ずることが重要。

◆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

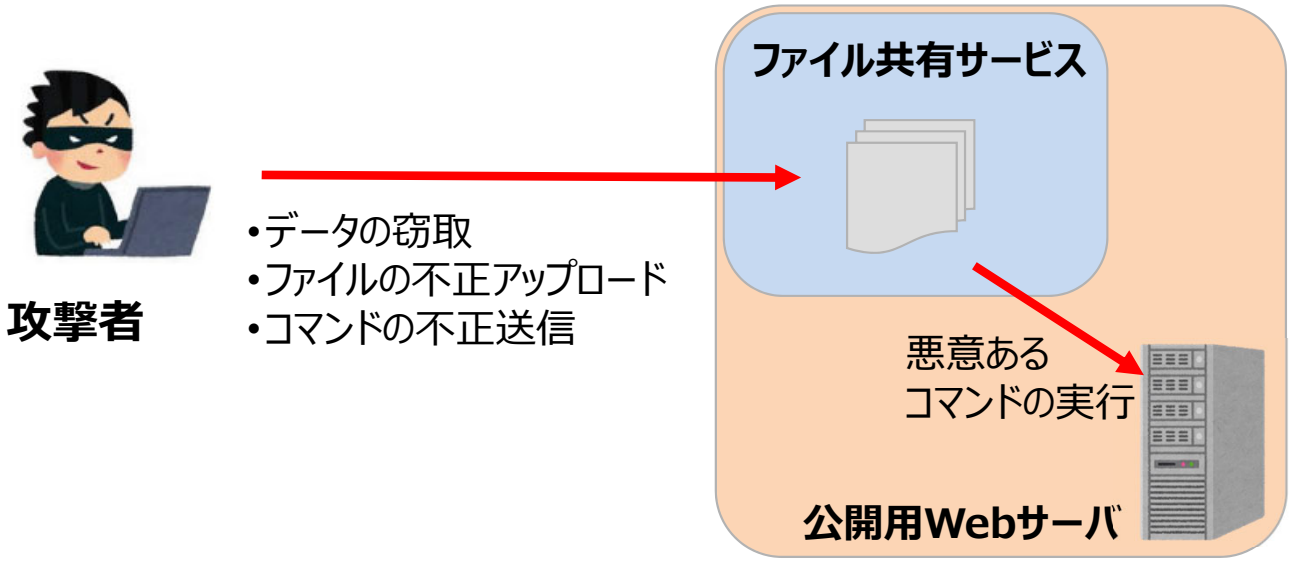


（出典）各種公開情報に基づき経済産業省作成

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。

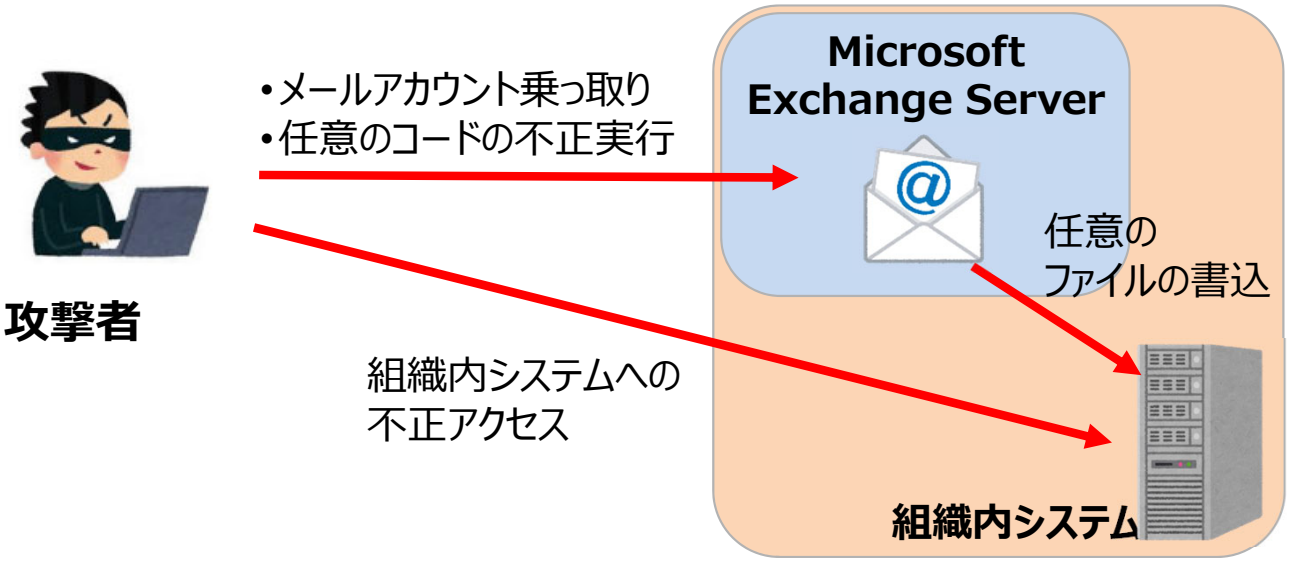
◆攻撃イメージ



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

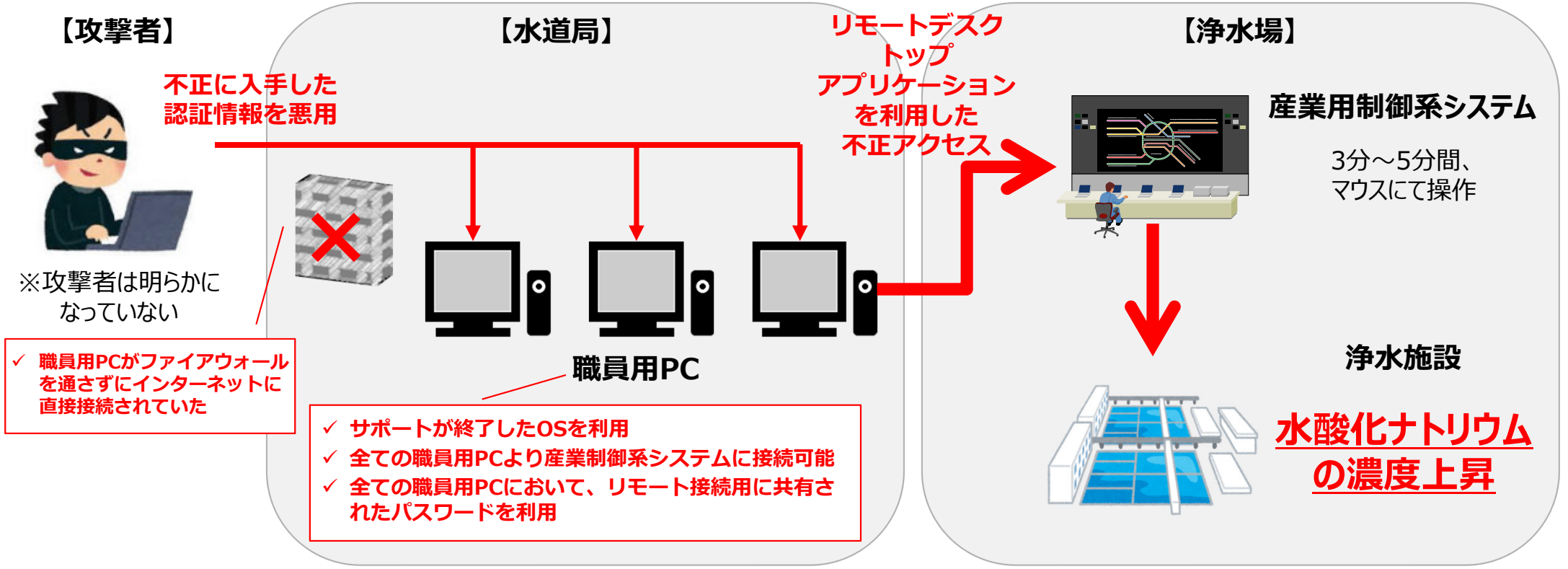
- 2021年3月2日、Microsoft社は**Microsoft Exchange Serverのゼロデイ脆弱性を悪用**した不正アクセス事案の発生及び当該脆弱性のセキュリティパッチを公表した。
- 本脆弱性を悪用することで、**Eメールアカウントの乗っ取りの他、攻撃者がさらなるシステム侵害を行うためのバックドアが設置**されるおそれがある。そのため、パッチの適用のみならず、侵害の有無の確認及び影響の排除を行う必要がある。
- 本事案が判明した時点で、**全世界で数十万にのぼる組織が攻撃を受けた**とされている。
- Microsoft社は、**中国の支援を受けた攻撃グループによる犯行**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

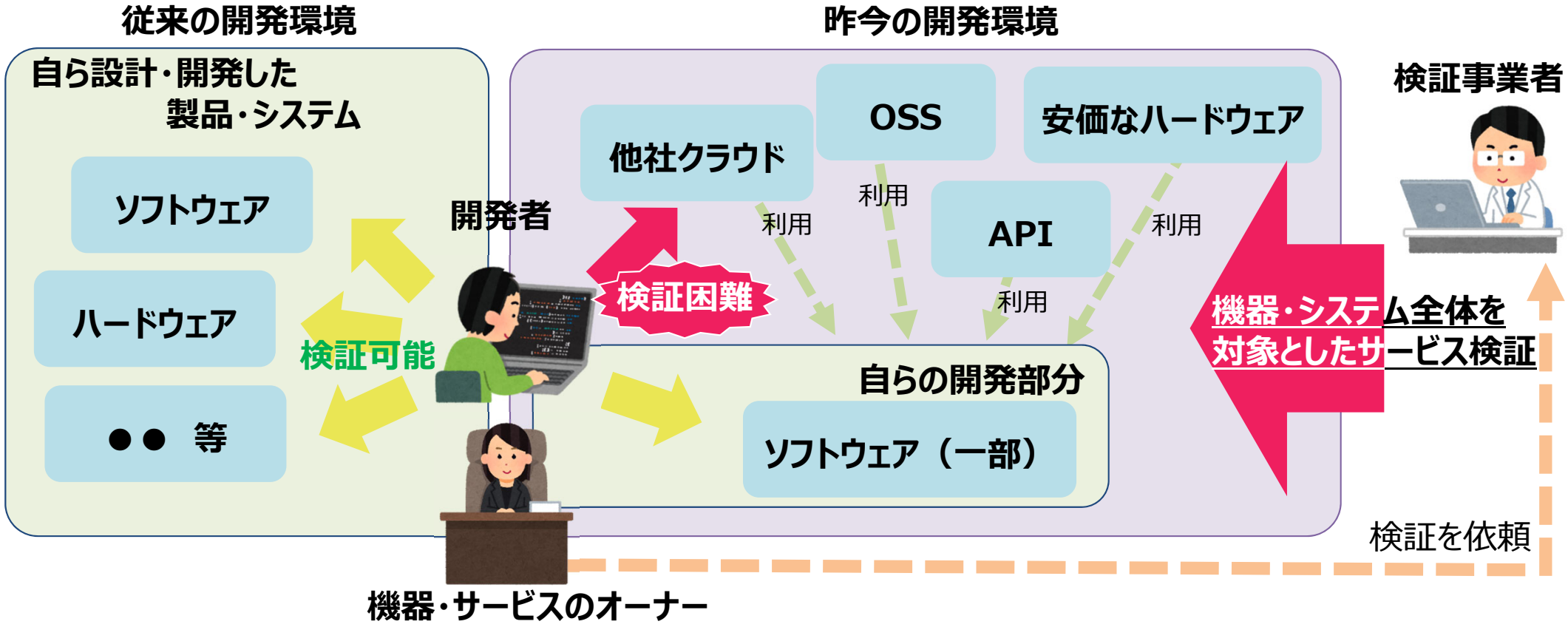
- 国としての対処能力の構築

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

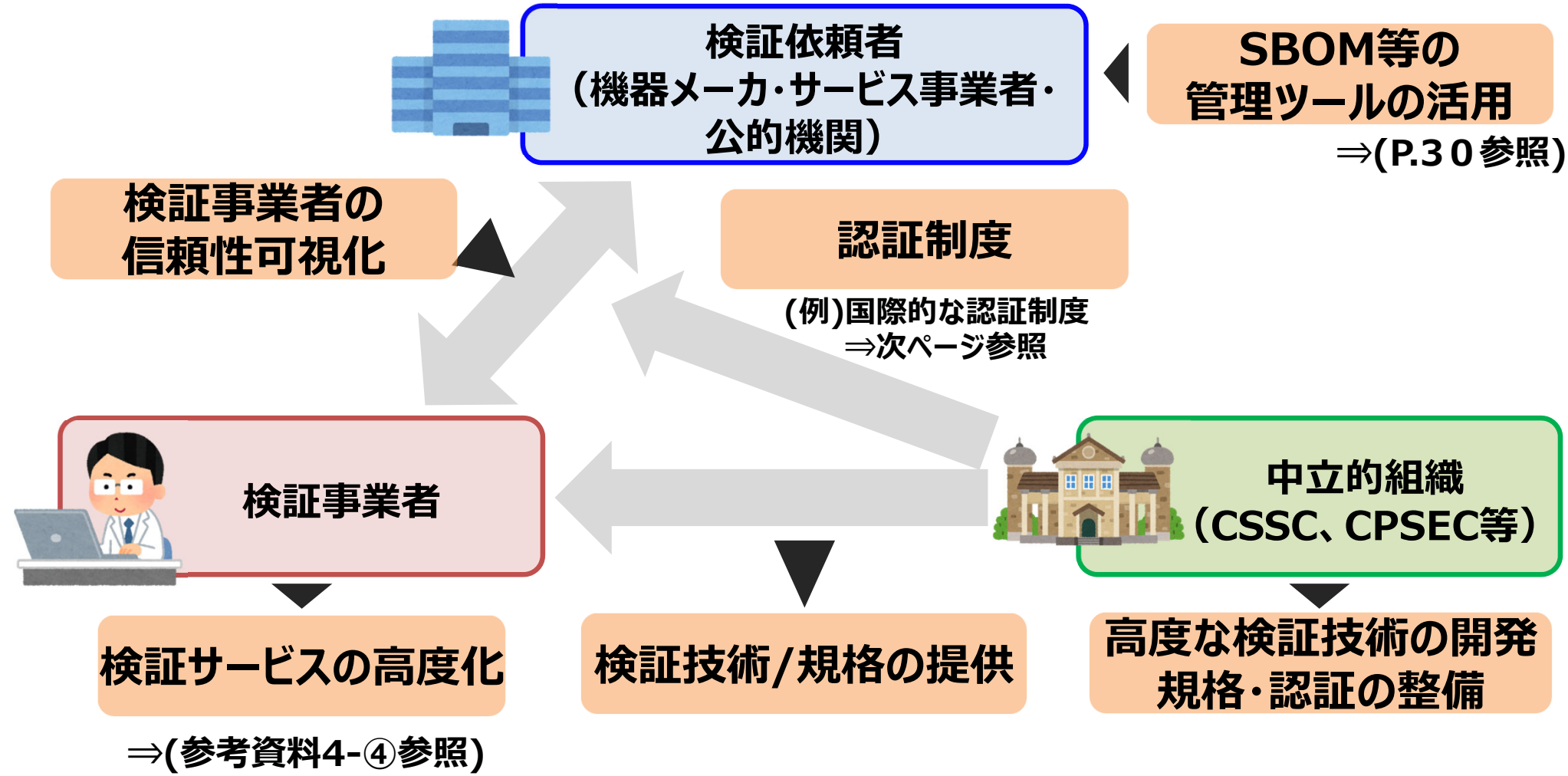
- 近年では**クラウドやIoTなどの新しい技術の活用が進み、またオープンAPIやOSSが充実したことで、必要な“機能”を容易に調達してシステム構築できる環境**になっており、**開発者自身がシステム全体を把握・検証することが困難**になりつつある。
- こうした環境の変化で、**官民において第三者によるセキュリティ検証の必要性が増大**し、**検証ビジネスの需要が拡大し、産業として重要になっていく**と考えられる。



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）

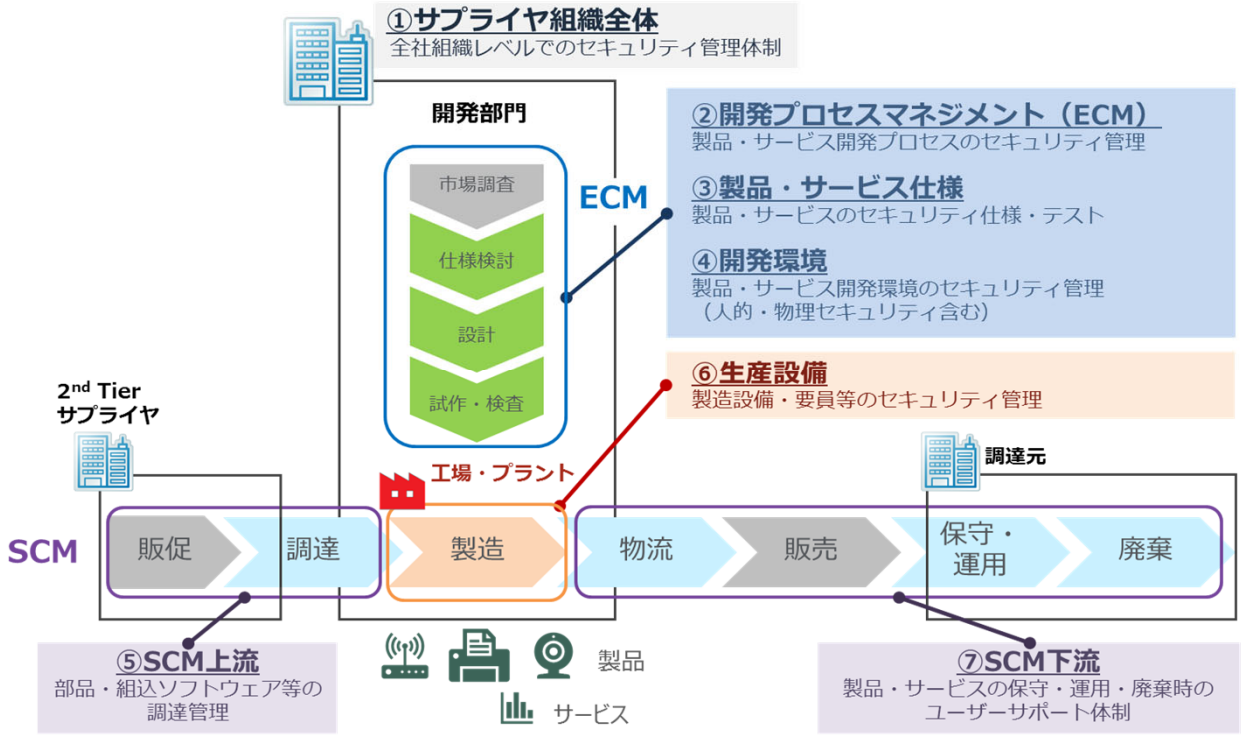


1 「開発のための投資」から「検証のための投資」へのシフト ～電力関連機器等のセキュリティ評価手法の確立（CPIC）

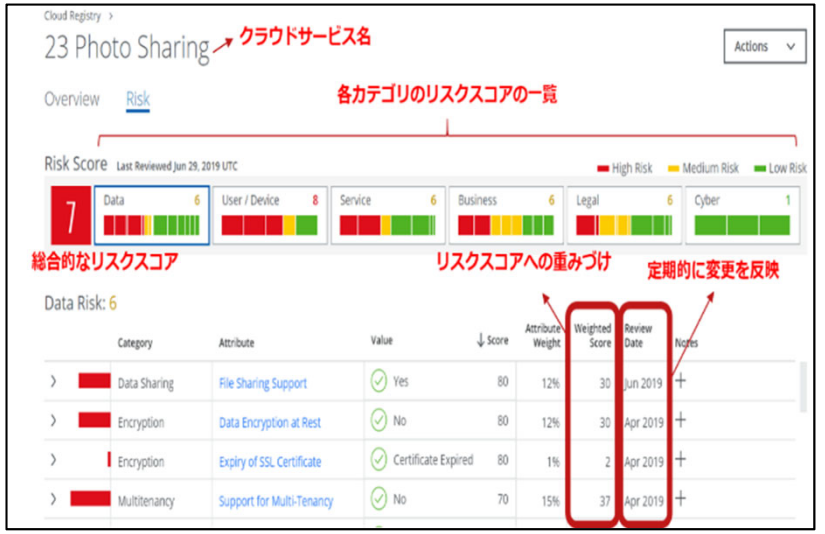
- 攻撃起点がサプライチェーンを通じて広がり、**重要機器のサプライチェーンリスクを管理するためのセキュリティ評価・可視化手法が必要**に。
- CPIC（Cyber Product International Certification：重要インフラに対するサイバー攻撃等の脅威に対処するための国際組織EIS Council が立ち上げた、米・英・イスラエルの官民を中心としたプロジェクト）においてその手法が議論されている。
- 国際的なステークホルダ間で、**サプライチェーンまで含めた機器の高いレベルの安全性を確保**できるように、日本主導で、国内電力事業者及びベンダーの協力による任意の認証制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

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

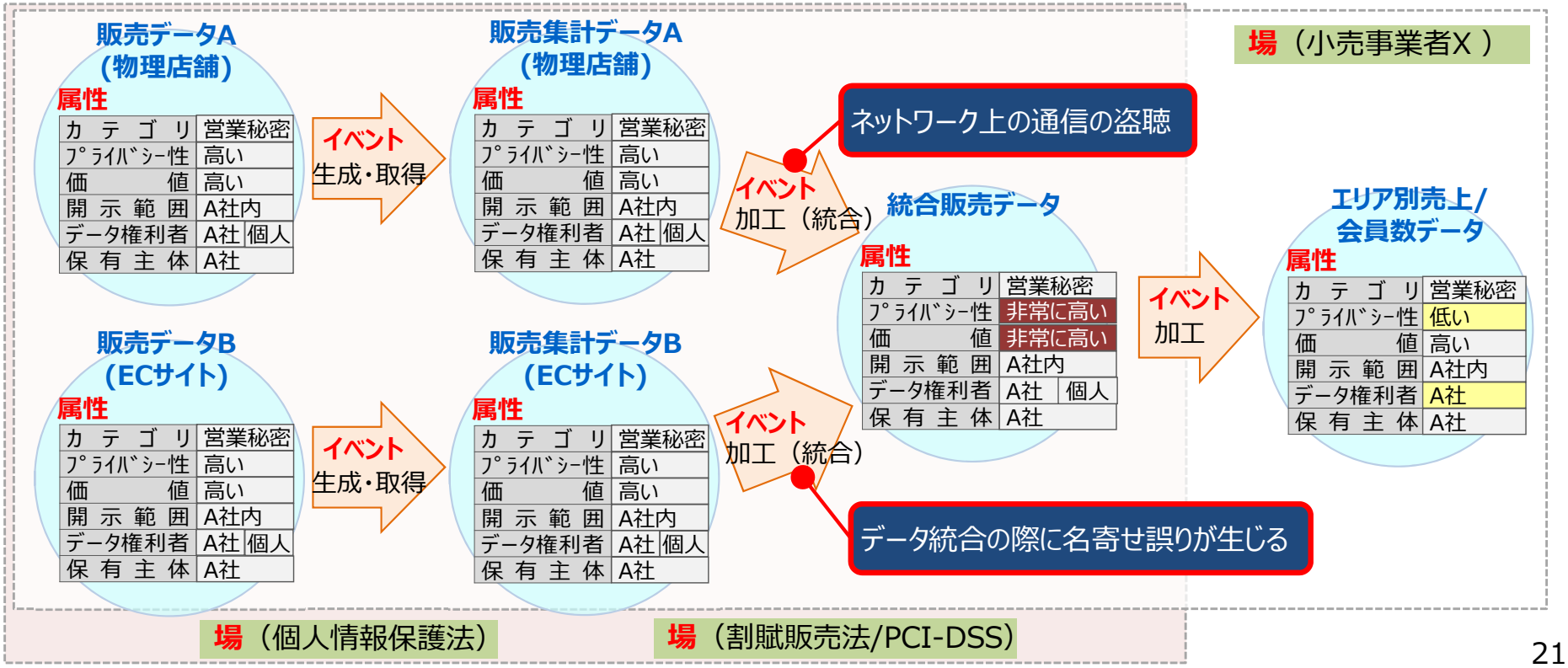
新たな捉え方への当てはめステップ（小売業におけるPOSデータの活用事例）

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

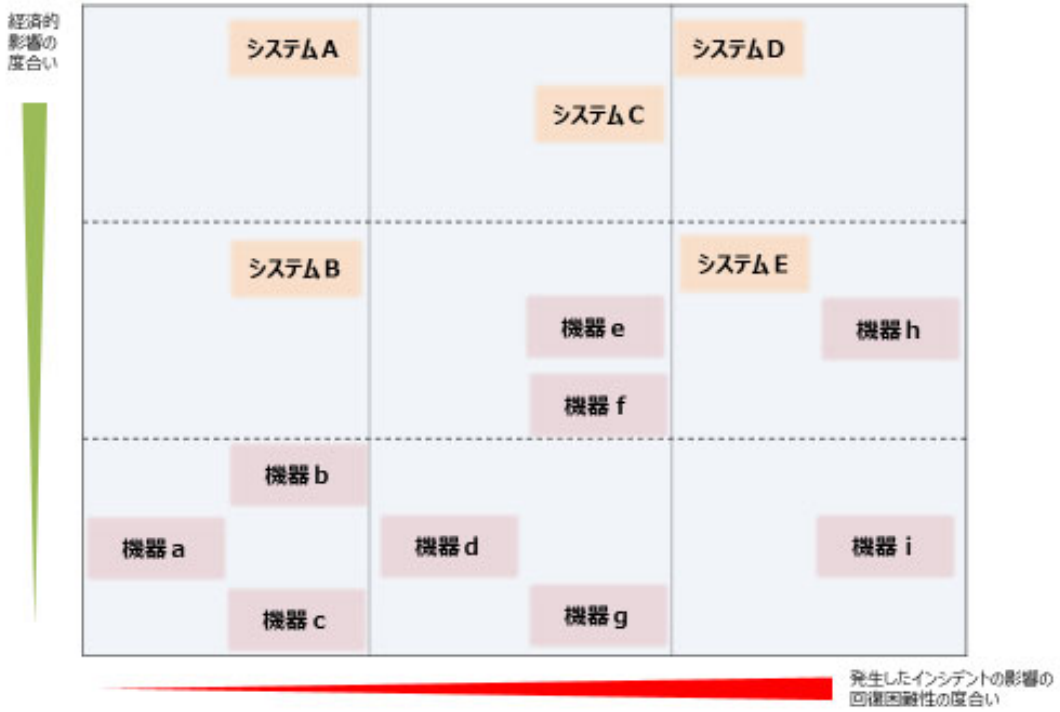
STEP 4
イベントごとのリスクの洗い出し



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

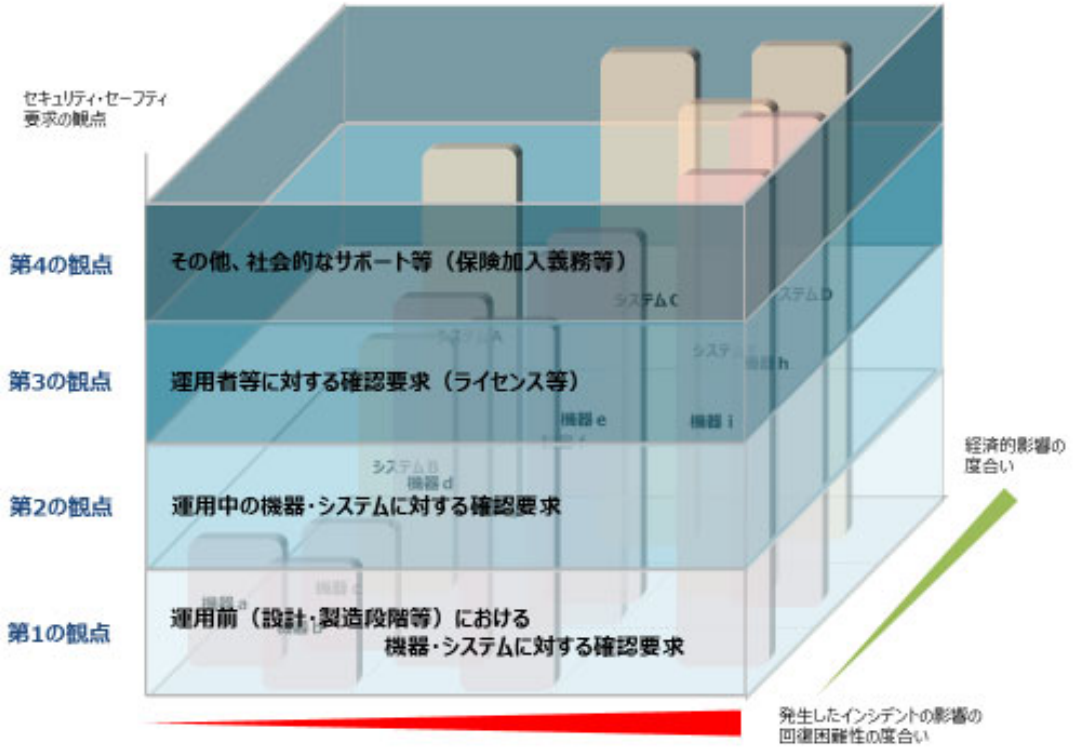
- **用途や使用環境によって課題が異なるIoT機器・システムに対するセキュリティ対策を、複数のステークホルダ間で合意する**際に活用できる**「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」を2020年11月5日に公開。**
- 本フレームワークで、IoT機器・システムをカテゴライズし、カテゴリごとに求められるセキュリティ・セーフティ要求の観点を把握・比較することにより、**それぞれに求める対策の観点・内容の整合性を確保できる**。

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



※ 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。）

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



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。

Supply-Chain Cybersecurity Consortium (SC3)

事務局：ＩＰＡ

総会
年１回程度開催（WG報告、重要事項の決定等）

基本行動指針（共有・報告・公表）へのコミットメント

運営委員会

会　長　：経団連　サイバーセキュリティ委員長　遠藤信博氏
副会長：日本商工会議所　特別顧問　金子眞吾氏
　　経済同友会　副代表幹事　間下直晃氏

- **中小企業対策強化WG**
- **地域SECUNITY形成促進WG（案）**
- **産学官連携人材育成WG（案）**
- ・・・・・

参加団体例：日本自動車工業会、電気事業連合会
全国地方銀行協会、日本損害保険協会ほか

メンバーの意向を踏まえて特定課題を扱うWGを設置

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

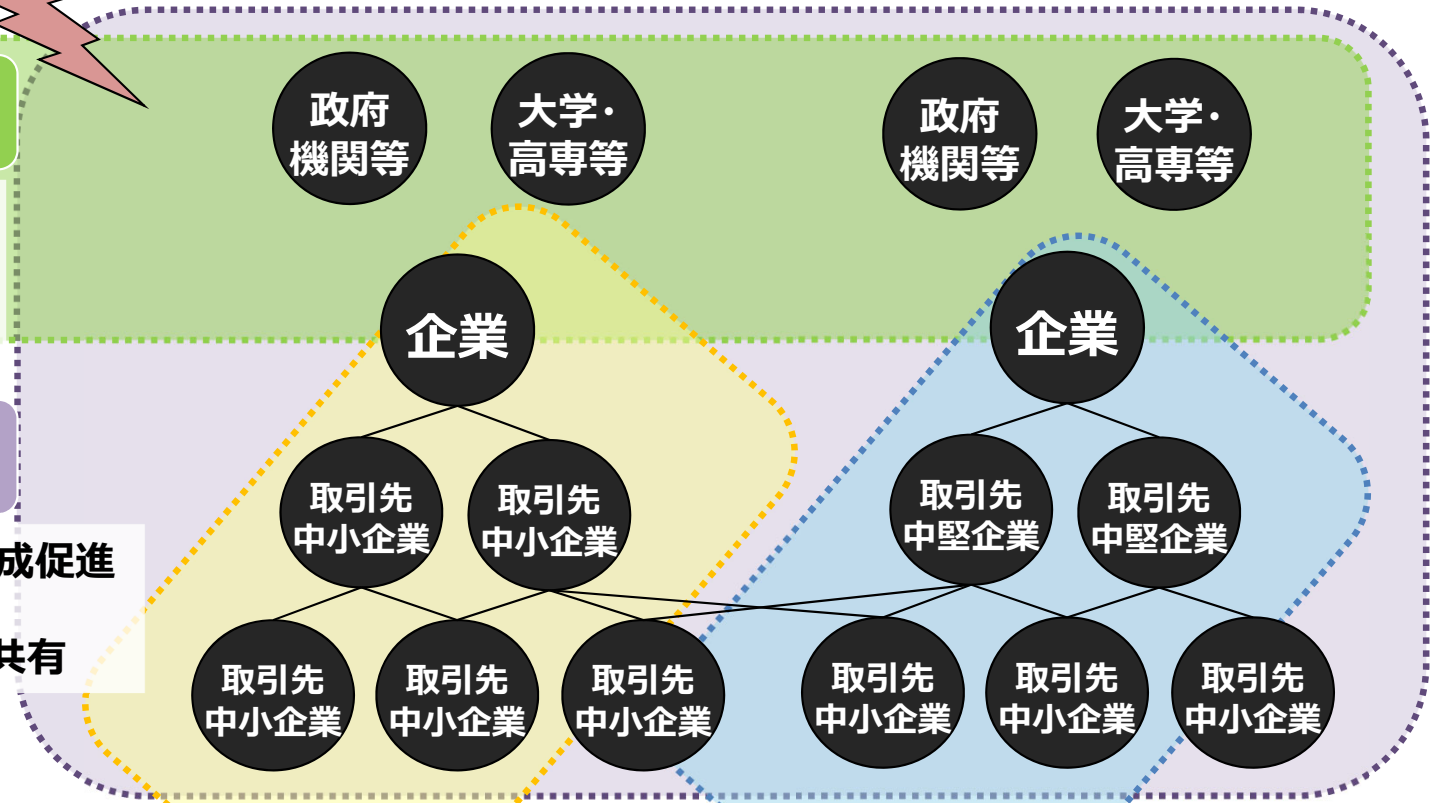
- 新たな脅威への対抗、サイバー攻撃動向の共有、対策検討
- 経営層向け注意喚起、WGやウェビナーでのプラクティス共有

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。

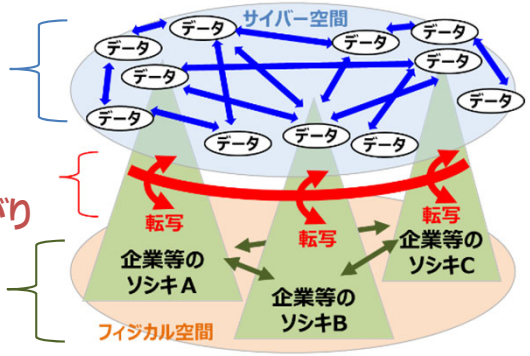
CPSFのモデル

<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

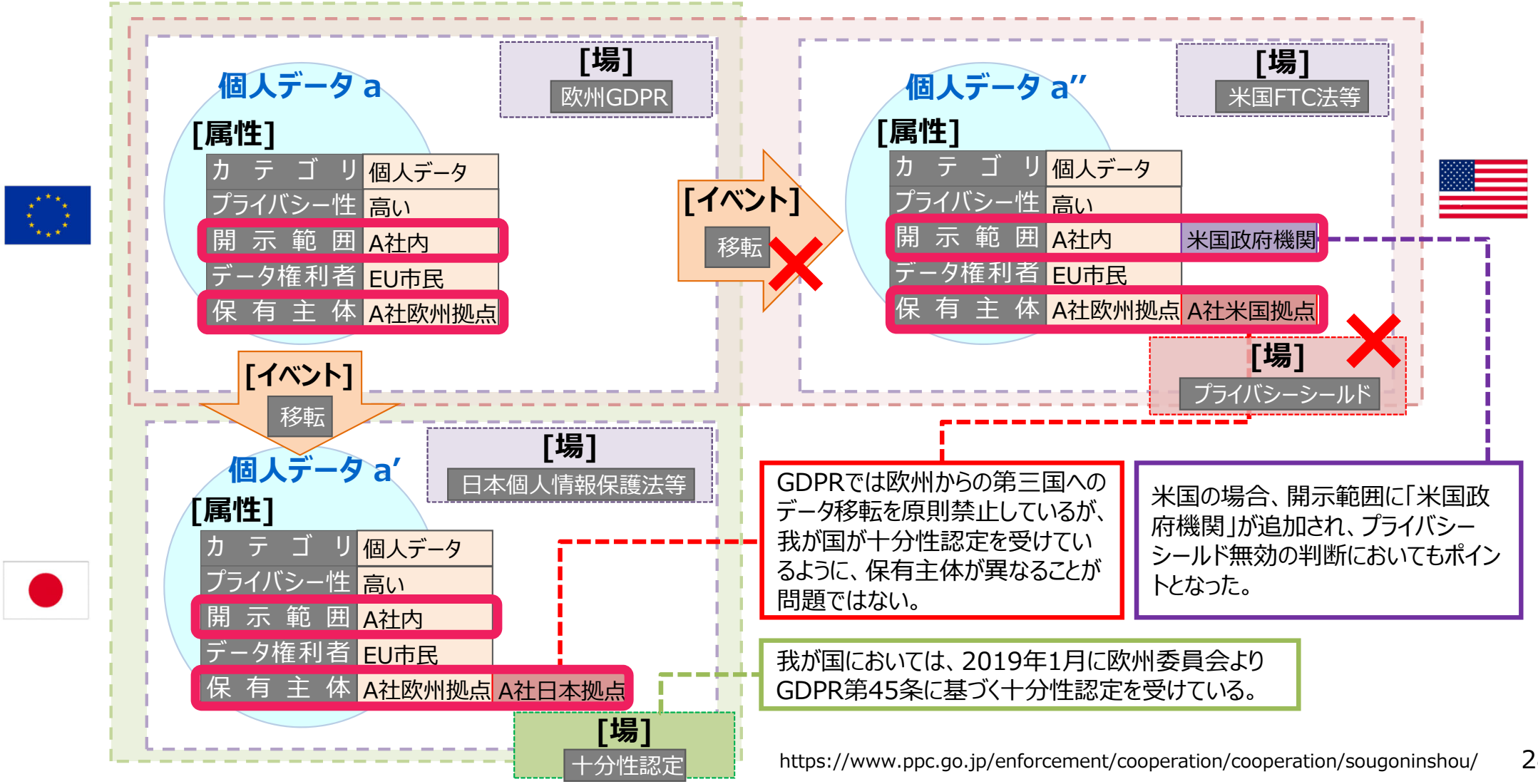
SC27/WG4において、これまでにPWIとして3度の意見募集を実施。
さらに議論を深め、国際規格（TR）の策定を目指す。

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）

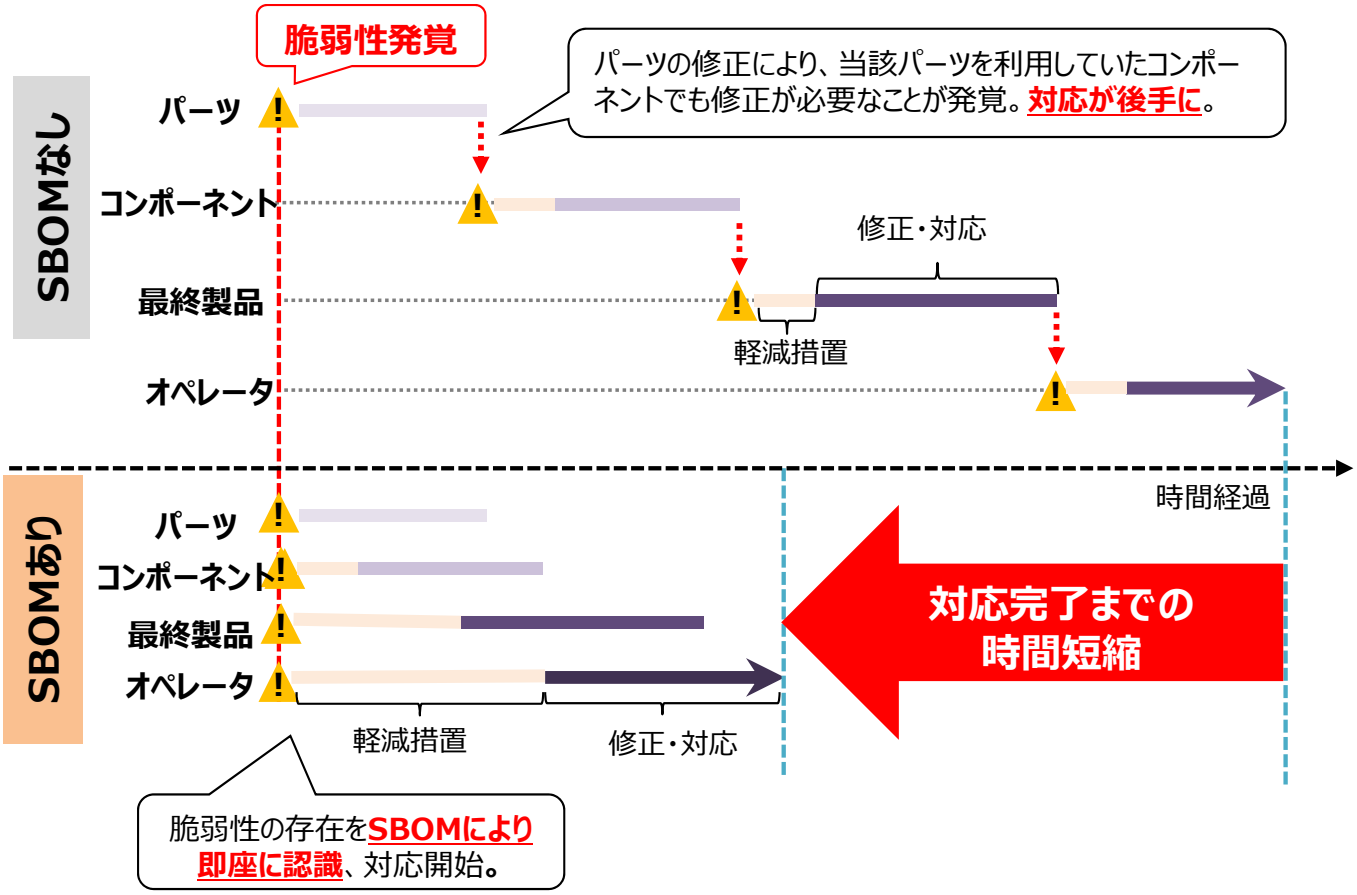
- OSSの利用が広がる一方、自社だけでOSSを検証するための体制等を整えることの負担は大きく、日本だけはなく米国でもベストプラクティスを共有することに対するニーズが存在。
- **「OSSの利活用及びセキュリティ確保に向けた管理手法」をまとめた事例集**を作成し、参考となる事例を共有して企業における適切なOSS利用を促進。日本から働きかけることで日米でOSSの活用・管理に関するベストプラクティスを共有する機会の確保を目指す。

OSSに関する課題の観点（例）	OSS事例集で紹介する取組（抜粋）
ライセンス管理 脆弱性管理	● スキャンツールを用いて**ソフトウェア部品構成表（SBOM）を作成** ● 脆弱性やライセンス等について、抜け漏れのないリスク管理を実施。
サプライチェーン管理	● サプライヤからの部品・ソフトウェア納入の際に、**確認書の提出を求める**。 ● サプライヤの理解を得るため、**OpenChain Japan WGを活用し啓発・情報発信**を実施。
組織体制	● OSS利活用プロセスを**全社ルール化して、トップダウンで適用を指示**することで、適用プロジェクトを増やし、高い効果をあげた。
コミュニティ活動	● 社員に対して、**就業時間内でのOSS開発等を認める**。 ● コミッタとして貢献している**社員を認定し、活動予算枠を付与**。

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）

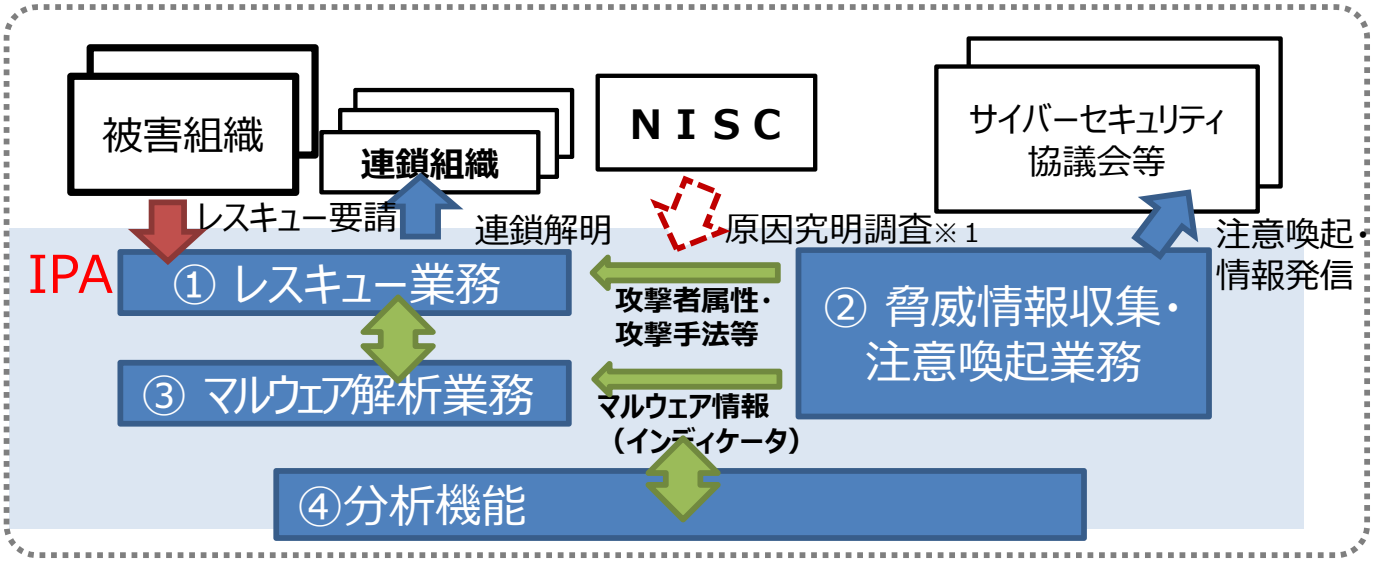
サイバー空間においては、関連技術の進展が早く、攻撃者優位ともされる中で、それぞれの主体が自らの役割を認識し対応するとともに、互いに連携・協働して取り組むことができる環境が重要。政府としては、社会全体を俯瞰した上で、攻撃者との非対称な状況の改善も含め、**自律的な取組や多様な主体の緊密連携、組織化・洗練化されたサイバー攻撃に対する公的機関の取組が効率的かつ戦略的に実現できるよう適切な対策を進める**など政府の役割を意識した政策立案の基礎となるものにすること。（以下略）

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

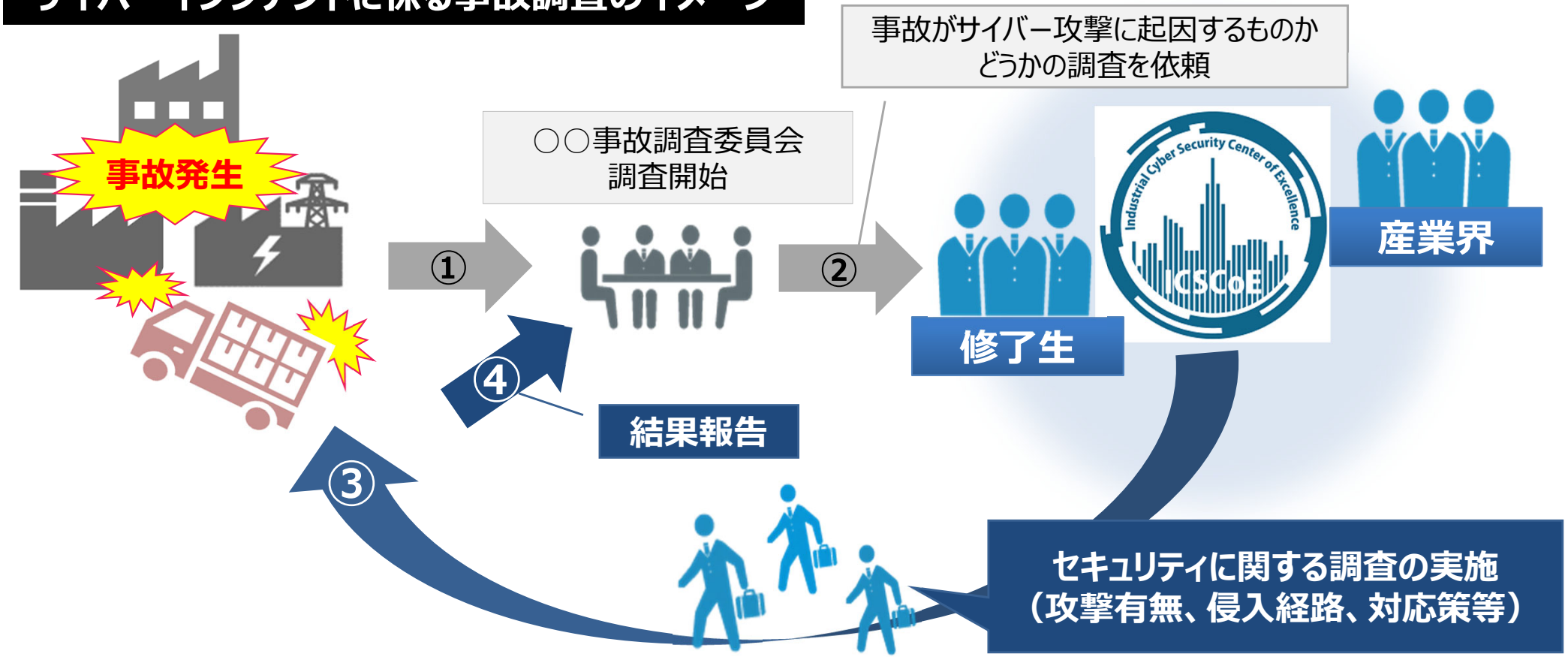


※１　サイバーセキュリティ基本法（H28/4施行）第30条に定める原因究明のための調査

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

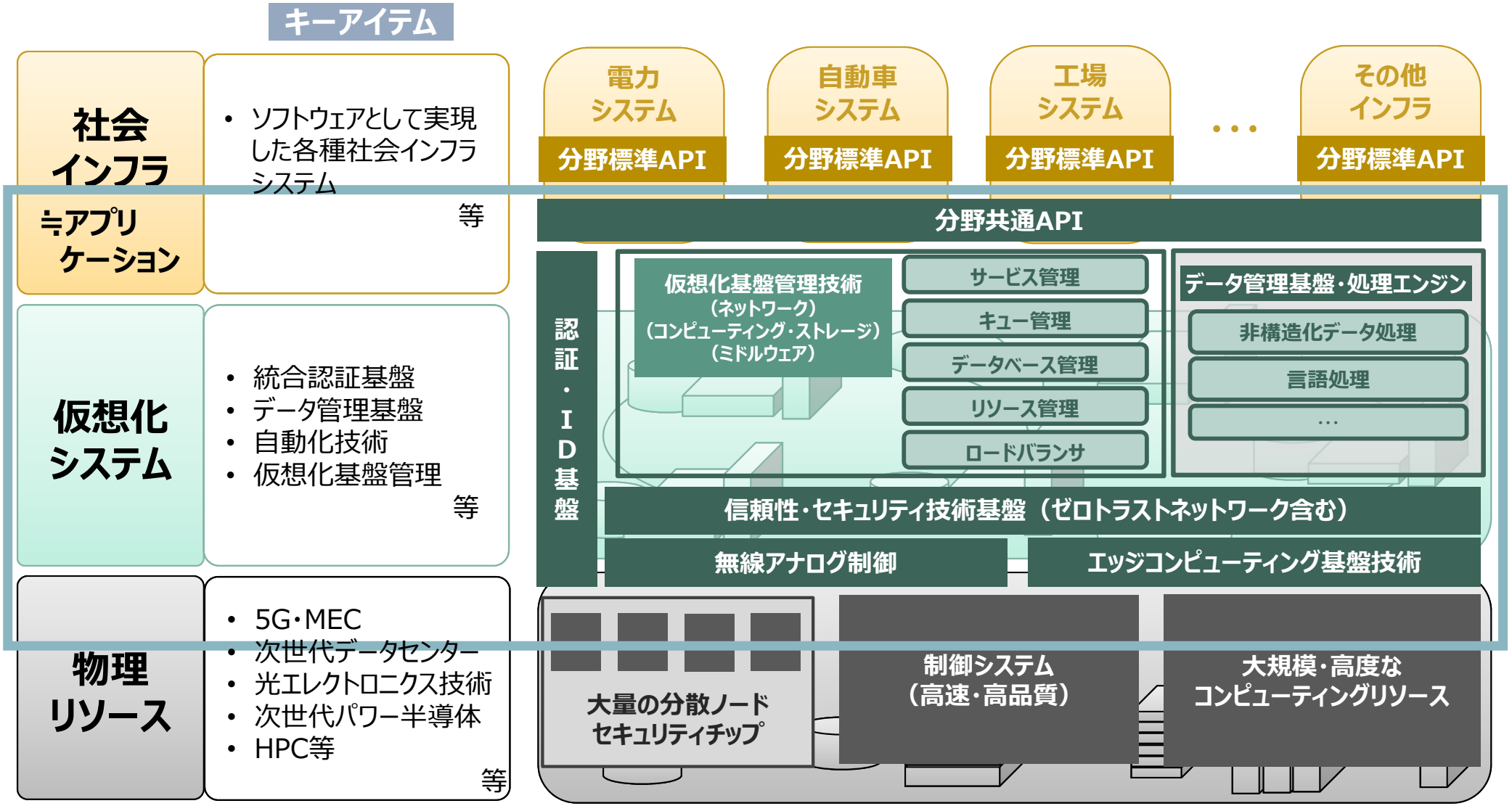
アーキテクチャ設計（IPAデジタルアーキテクチャ・デザインセンター）

・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。



（参考資料）

4つのアクションプランの進捗状況

● 4つのアクションプランは順調に進捗。

＜第５回研究会（2020年６月）以降に実現された取組及び今後の取組の方向＞

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

① 第3層TF、ソフトウェアTF、第2層TF開催（2019年8-2021年3月）
② IoTｾｷｭﾘﾃｨ・ｾｰﾌﾃｨ・ﾌﾚｰﾑﾜｰｸ（IoT-SSF）公開（2020年11月）
③ 自動車ガイドライン 1.0版公開（2020年12月）
④ スマートホームガイドライン公開（2021年4月）
⑤ 宇宙産業SWG設立（2021年1月）
⑥ ｻﾌﾟﾗｲﾁｪｰﾝ・ｻｲﾊﾞｰｾｷｭﾘﾃｨ・ｺﾝｿｰｼｱﾑSC3発足（2020年11月）
⑦ インド太平洋地域向け日米サイバー演習第3回（2021年３月）

2 サイバーセキュリティ経営強化パッケージ

① サイバーセキュリティお助け隊、13地域・２業種での実証事業完了
② サイバーセキュリティお助け隊ブランドの使用開始（2021年4月～）
③ 経営ガイドライン可視化ツールWeb版公開（2021年夏頃）

3 サイバーセキュリティ人材育成・活躍促進パッケージ

① 産業サイバーセキュリティセンター(ICSCoE)3期生修了(2020年6月)
② 「人材の手引き 第1版」(2020年9月)・第1.1版公開(2021年4月)
③ 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（2021年2月～6月）
④ 国立高専機構と産・官との連携促進
⑤ 各地域でのセキュリティコミュニティ（地域SECUNITY）形成促進
⑥ 地域SECUNITY形成のためのプラクティス集公開（2021年２月）

4 セキュリティビジネスエコシステム創造パッケージ

① 情報セキュリティサービス審査登録制度：223件登録（2020年12月）
② 基準適合サービスリストの改善（2021年2月）
③ セキュリティ製品の有効性検証・実環境における試行検証実施
④ ハイレベル検証：機器のサイバーセキュリティ確保のための検証の手引き策定（2021年3月）
⑤ 「情報システム・モデル取引・契約書」第二版公開（20210年12月）
⑥ コラボレーションプラットフォームの活動を継続

1-③：自動車ガイドライン 1.0版（2020年12月公開）

- 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。
- 2020年12月、エンタープライズ領域（会社全体のベースとなるOA環境）において業界全企業が実施すべき事項を規定した**「自工会／部工会・サイバーセキュリティガイドライン1.0版」を公開**。

＜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 第1回 電子情報委員会／サイバーセキュリティ部会を開催。
- 2020年12月4日 第1回 総合政策委員会／ICT部会／サイバーセキュリティ分科会を開催。
（自工会の組織体制変更に伴い名称変更）

＜2020年度進捗＞
- 2020年5月、**部工会と共同で、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とした「自工会／部工会・サイバーセキュリティガイドライン0.9版」を作成し公開**。
公開後、0.9版のチェックシートを用いたトライアルを業界内各社で実施。
- 2020年12月、**0.9版によるトライアルの結果を踏まえて内容を充実させ、「自工会／部工会・サイバーセキュリティガイドライン1.0版」を公開**。
- 2021年3月、**英語版公開**。
- 今後、ガイドライン対応状況の集約・分析、レベルアップに向けたガイドラインの項目拡充、工場セキュリティに関する課題対応、脆弱性/脅威情報に関する各社の情報共有等について検討を深める。

1-④：スマートホームSWG（JEITA スマートホーム サイバーセキュリティWG）

- スマートホームにおける安全で安心な生活の実現のため、スマートホームの提供事業者から住まい手まで、幅広いステークホルダに求められる最低限のセキュリティ対策をまとめたガイドラインを取りまとめた。

◆ガイドラインの対象

- スマートホーム向けIoT機器、スマートホーム向けサービス、スマートホーム（住宅）の開発・生産・販売・供給・サポート等を行う事業者
- スマートホーム化された区分所有型集合住宅および賃貸型集合住宅の管理者
- スマートホームの住まい手

＜メンバー構成＞

企業）家電・AV関連、IT・通信関連、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、医療関係、健康関連分野、研究機関

＜開催状況＞

2018年3月より、JEITA スマートホーム サイバーセキュリティWGとして開催。

＜2020年度進捗＞

- 2019年度に作成したガイドライン案について、2020年7月末から8月にパブコメを実施。
- パブコメで提出された意見も踏まえて修正を行い、「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」第一版として取りまとめた。

1-④：スマートホームガイドラインの策定

- 2018年3月からスマートホームSWGにおいて議論。2019年度にとりまとめたガイドライン原案について、2020年7月末から8月にかけてパブコメを実施。提出された意見等を踏まえて修正を行い、**「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」**として取りまとめ、**2021年4月に公開。**
- スマートホームにおけるステークホルダーは多様であり、セキュリティに関する知識・バックグラウンドも様々であるため、必要なセキュリティ対策を階層的に示している。

スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン

1-④：スマートホームガイドラインのポイント

- 知識やバックグラウンドが様々なステークホルダーに対応するため、**シンプルな対策ガイド（4章）から、具体的な対策要件や他の標準との対比（添付）まで、セキュリティ対策を階層的に整理**。

＜4章　スマートホームに求められる最低限のセキュリティ対策＞　※抜粋

4.1.(1)スマートホーム向けIoT機器の事業者
- IoT機器は**出荷時**や**初期状態**から**セキュリティを確保**する
- **セーフティ**を考慮する
- ソフトウェアを**アップデートするための仕組み**を提供する
- 利用者に**IoT機器の使い方**や**使用環境**を**ガイド**する、セキュアに利用するための情報を提供する

誰でも読みやすいように本編はシンプルな対策ガイドに抑え、より詳細な検討が必要な者が参照できるよう添付において詳述することで、**セキュリティ対策を階層的に整理。**

＜添付A　ステークホルダーにおける機能／想定されるインシデント／リスク源／対策要件＞　※抜粋

機能	想定される インシデント	リスク源			対策要件 ID	対策要件の例
		脅威	脆弱性 ID	脆弱性		
下記の機能 ・フィジカル空間の物理事象を読み取り、デジタル情報へ変換し、サイバー空間へ送る機能 ・サイバー空間での処理の結果により、IoT機器を制御する等のためにサイバー空間から受ける機能 ・外部からの管理機能	事前に想定されていない動作をする （IoT機器およびIoT機器を含むシステムにより提供されるサービスや機器の種類により、想定されていない動作は異なり、情報漏洩や不正な制御といった、人体・健康・住宅・防犯・環境・利便性・エネルギーメーターなどに影響するものがある）	・ソフトウェアの脆弱性やハードウェアの脆弱性を悪用してIoT機器内部に不正アクセスされる	MV.1	・利用されないネットワークポートやサービスなどが利用可能な状態のままとなっている	MO.1	・IoT機器およびIoT機器を含むシステムでの不要なネットワークポート、その他USBやシリアルポートなどを物理的または論理的に閉塞すること。 ・IoT機器およびIoT機器を含むシステムが提供する機能、サービス、アプリケーション、アカウントについては必要に応じて停止、変更、削除が可能なようにすること。

＜添付B＞：対策要件IDと国際規格との対応、　＜添付C＞：4章と添付Aの対応

1-⑤：宇宙産業SWG設立（2021年1月）

- 宇宙分野における民間事業者の役割拡大や、米国等における官民の取組を踏まえ、我が国でも、2021年１月に産学の有識者を委員に、宇宙産業SWGを設立。

＜背景＞

- 宇宙分野における民間事業者の役割拡大
- 国内外で宇宙分野のセキュリティインシデントが多発
  - 1986-2020年に国内外で90件以上
- 米国等において宇宙分野のセキュリティ対策を促進するための官民の取組が活発化
  - 国家安全保障システム委員会（CNSS）によるCNSSP12『安全保障任務に用いられる宇宙システムのための国家情報保証方針』 (07年3月発行。18年2月最終改訂）
  - 民主導による『商用宇宙システムセキュリティガイドライン』発行（20年5月）

＜委員一覧＞

鹿志村 修	宇宙システム開発利用推進機構(JSS) 研究開発本部長
片岡 晴彦	(株)IHI 顧問（元防衛省航空幕僚長）
木下 仁	IPAセキュリティセンター主任研究員
栗原 聡文	東北大学大学院工学研究科 航空宇宙工学専攻 宇宙ロボット研究室 准教授
小山 浩	三菱電機(株)　電子システム事業本部 主席技監
坂下 哲也(座長)	JIPDEC 常務理事
佐々木 弘志	マカフィー(株) シニア・セキュリティ・アドバイザー
名和 利男	(株)サイバーディフェンス研究所 専務理事・上級分析官
丸山 満彦	PwCコンサルティング　パートナー
満永 拓邦	東洋大学 情報連携学部 准教授
吉松 健三	CSSC

1-⑤：宇宙産業SWG設立（2021年1月）

- 民間事業者向けの宇宙システムに係るサイバーセキュリティ対策のガイドラインを令和3年度中を目標に開発予定。

＜メンバー構成＞

宇宙産業事業者、宇宙関係の業界団体・NPO、
有識者（大学、産業サイバーセキュリティ専門家等）

＜開催状況＞

2021年1月に第1回、3月に第2回を開催。

＜目標・検討内容＞

- 民間事業者向けの宇宙システムに係るサイバーセキュリティ対策のガイドラインを令和3年度中を目標に開発予定。開発するガイドラインは自主的な対策を促すためのものとする。（ただし、規制官庁が当該ガイドラインを参照することは妨げない。）
- 宇宙産業SWGの下に実務者からなる作業部会を設置。作業部会には30以上の組織が参加。第一回を2021年2月に開催。
- 本SWG及び作業部会には、宇宙分野の専門家、産業サイバーセキュリティの専門家の双方が参加し、お互いの専門領域について理解を深めることを通じ、「宇宙×サイバー」のコミュニティへと発展させることを目指す。

1-⑦：インド太平洋地域向け日米ICSサイバーセキュリティ演習（第3回）詳細

- 経済産業省及びIPA産業サイバーセキュリティセンターは、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省、エネルギー省、アイダホ国立研究所）と連携し、**インド太平洋地域向け産業制御システム・サイバーセキュリティ演習（第3回）**を実施。
- 演習の一部分として、日米にEUも加わる形で、**初めて日米欧サイバーセキュリティセミナーを開催。**

■ **日時・場所：**2021年3月8日（月）～12日（金）（オンライン開催）

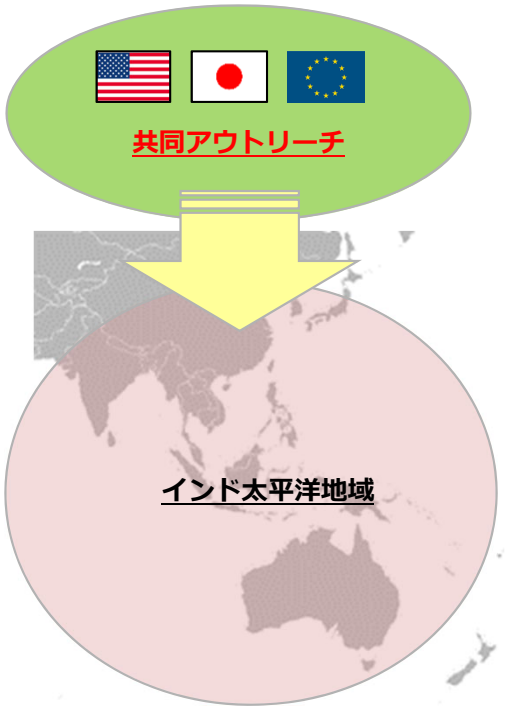
■ **参加者：**・ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の電力・石油会社、National CERT、エネルギー及びサイバーセキュリティ関係政府機関から40名を招聘。
・IPA産業サイバーセキュリティセンター（ICSCoE）の中核人材育成プログラム受講生も参加。

■ **開催概要：**リモートでのハンズオン演習や、日米欧の専門家によるエネルギー分野特有の問題も含む様々なサイバーセキュリティ関連のワークショップの受講、参加者間での知見の共有など、参加者に対してユニークかつ貴重な機会を提供。

長坂 経済産業副大臣挨拶

ウェールズ　米国DHS/CISA 長官代行挨拶


リモートハンズオン演習の様子




ロウハナ 欧州通信総局次長挨拶


ヤング 在日米国大使館　臨時代理大使挨拶


リモートハンズオン演習の様子

1-⑦：2020年度インド太平洋地域向け日米産業制御システム・サイバーセキュリティ演習

(0) オープニング・クロージングセレモニー

- 開会挨拶※・キーノートスピーチ（3/10）
  ※長坂副大臣、ウェールズ米DHS/CISA長官代行、ヤング米臨時代理大使、ロウハナ通信総局次長
- 閉会挨拶※（3/12）
  ※遠藤IPA産業サイバーセキュリティセンター長、ザックINL副所長、レパッサールENISA長官

(1) 日米産業制御システムサイバーセキュリテイ演習

- プレトレーニングセッション(リモート・ハンズオン)(3/8-9)（IPA産業サイバーセキュリティセンター）
- リスクアセスメント　ワークショップ
- サプライチェーン・リスクマネジメント ワークショップ
- 人材育成ワークショップ

(2) 日米エネルギーセクター サイバーセキュリティ ワークショップ

- 電力セクターワークショップ１：発電・送電・配電（従来型発電ビジネス）
- 電力セクターワークショップ２：エネルギー・ソース・アグリゲーション・ビジネス、再生可能エネルギー
- プロセスオートメーションセクター　ワークショップ：石油・ガス、化学、水
- スマートホーム・ビルセクター ワークショップ

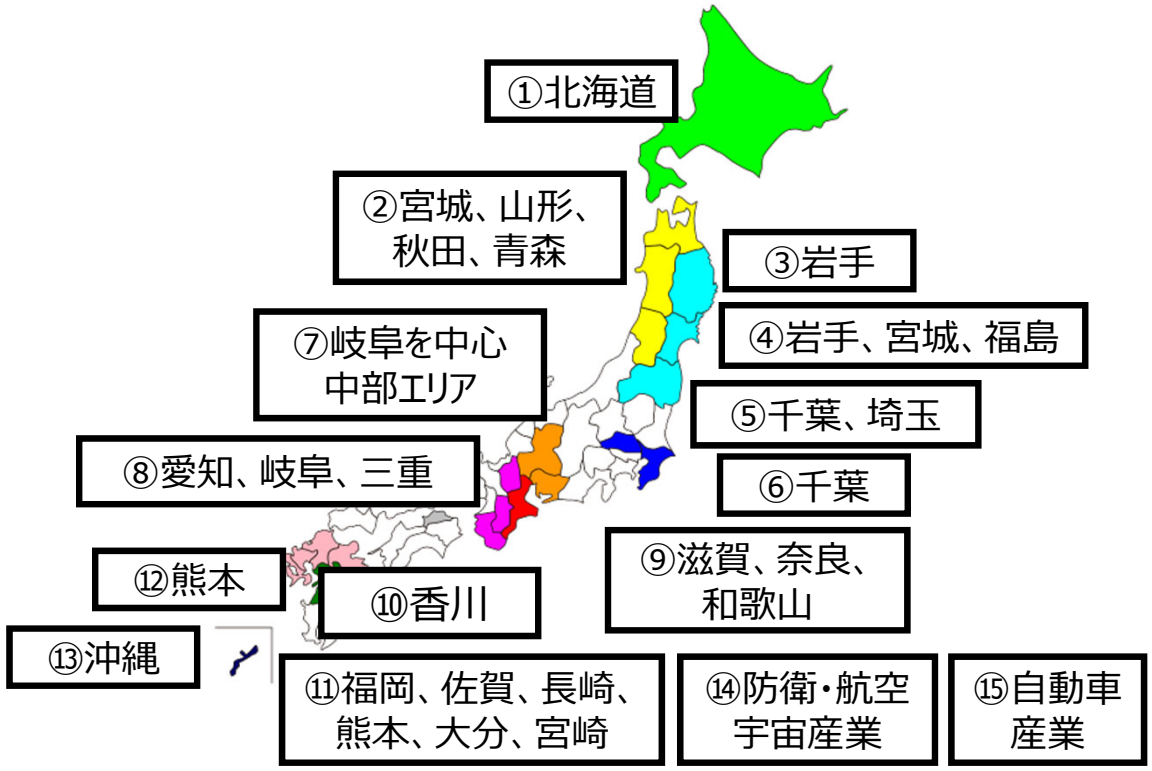
(3) 日米欧サイバーセキュリティセミナー～ポスト・コロナの時代に向けた提案

- 政策・標準化ワークショップ
- ヘルスケアセクター ワークショップ

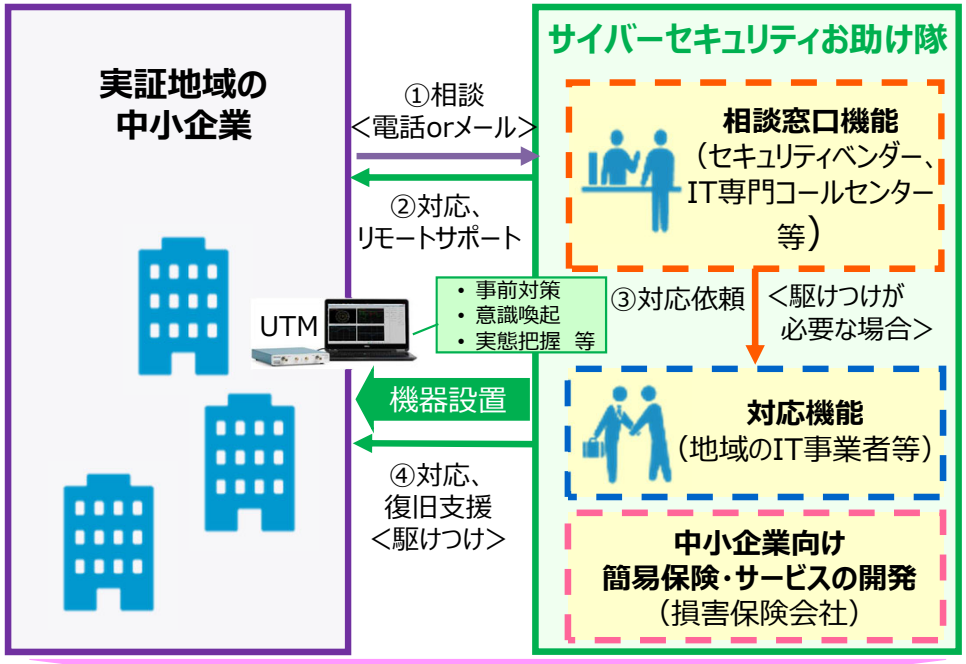
2-①：サイバーセキュリティお助け隊実証事業(2020年度)

- 地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けの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（全国で15件）。
- ２年間にわたる実証事業を通して、サイバーセキュリティに関する中小企業の実態を把握。2021年度より簡易サイバー保険を含むサイバーセキュリティお助け隊の民間自走化を促進すべく、お助け隊サービス基準を策定し、同基準を満たすサービスの審査登録制度の運営を開始。

＜2020年度の実証地域＞



＜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

※2019年度実証地域（全8地域、1064社の中小企業が参加）：
①宮城、岩手、福島②新潟③長野、群馬、栃木、茨城、埼玉④神奈川⑤石川、富山、福井⑥愛知⑦大阪、京都、兵庫⑧広島、山口

2-②：サイバーセキュリティお助け隊ブランドの使用開始

- 実証事業で得られた知見に基づき、中小企業向けのセキュリティサービス（お助け隊サービス）が満たすべき基準を整理、パブコメを経て２月末にIPAより公開。
- 2021年3月に第１回審査を行い、**４月以降、お助け隊マークが付与された民間サービスが市場に展開**される予定。

2019年度（実証１年目）	2020年度（実証２年目）	2021年度以降（民間で自走）
攻撃実態の把握 ニーズを踏まえたサービスのスリム化	地域特性・産業特性の考慮	
実証事業：中小企業が利用しやすい安価なセキュリティサービスの開発		
意識啓発	事前対策とのセットによるリスク低減	
	導入・運用負荷を下げる方法の検討	

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊の商標利用権を付与。

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC
→ サービス提供 → 中小企業 → 自社の信頼性をアピール → 取引先（大企業等）

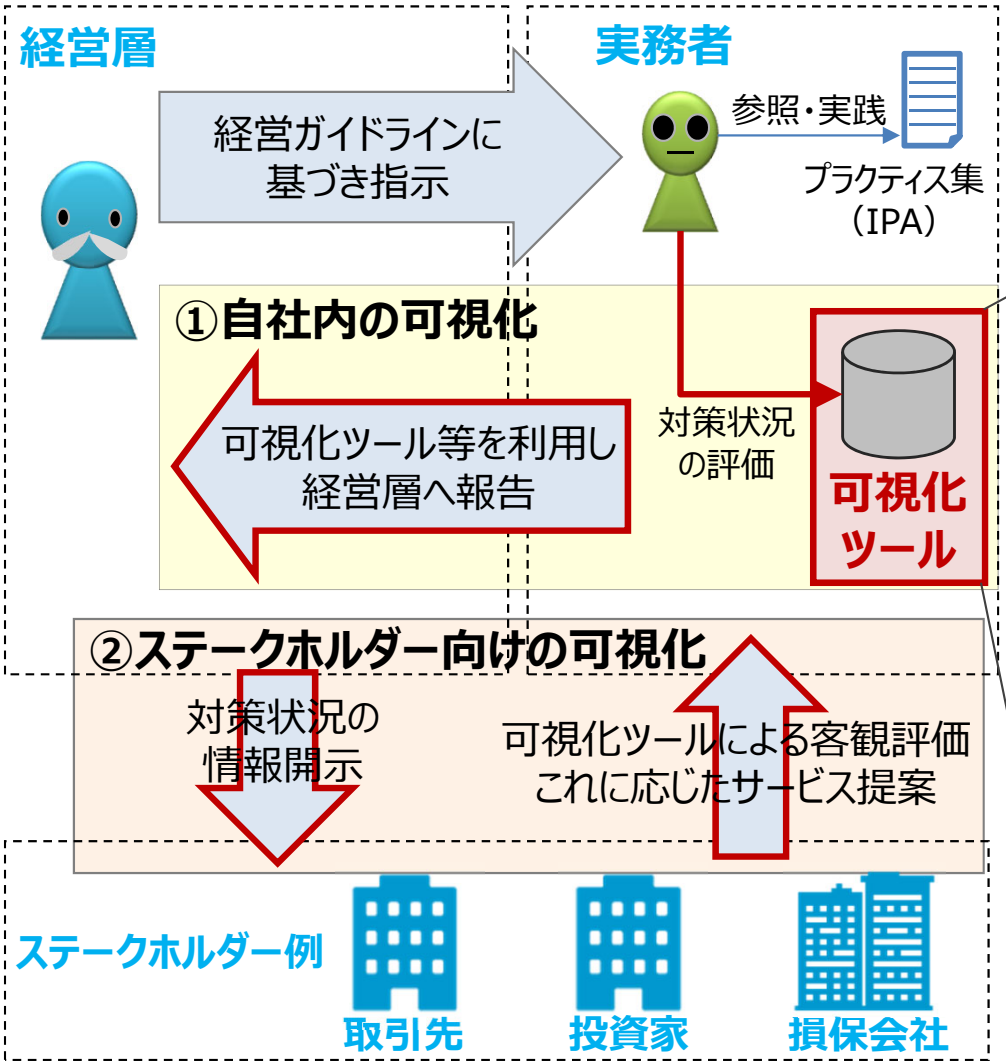
お助け隊サービス利用の推奨等の中小企業の取組支援

SC3(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（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。

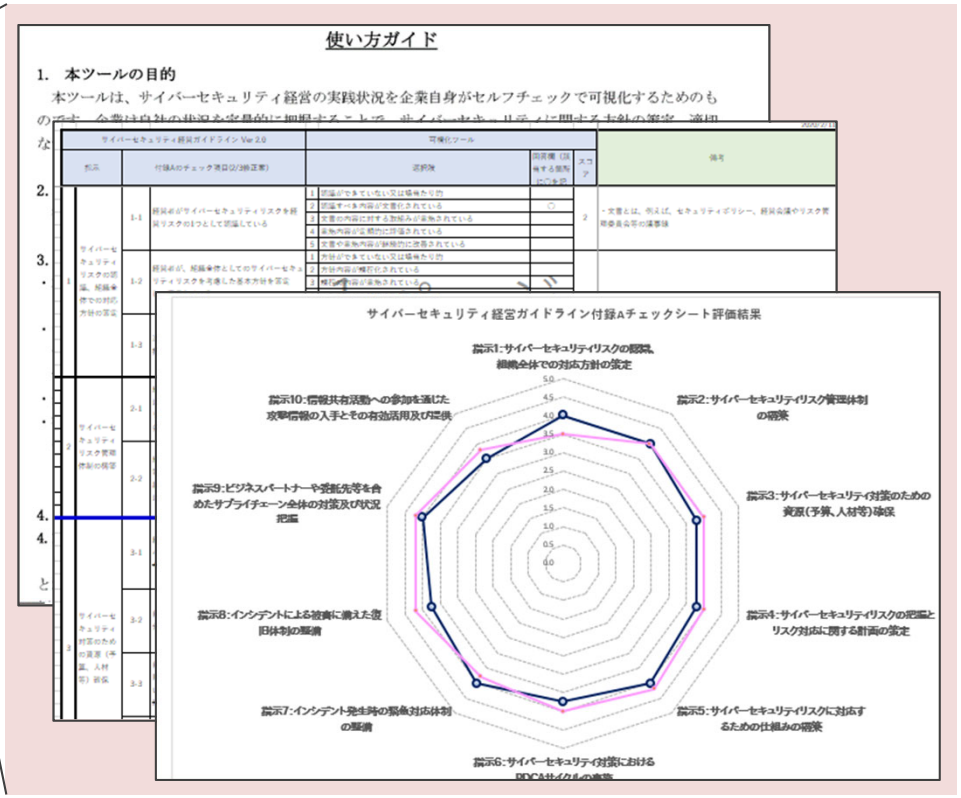
2-③：サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版を公開

- 2020年3月25日、可視化ツールβ版（Excel）をIPAから公開。
- 2020年度はユーザ企業、投資家等ステークホルダー向けにそれぞれβ版でテストを行い、ブラッシュアップを実施。**2021年夏頃のVer1.0（Web版）公開**に向けて開発推進中。



可視化ツールβ版の特徴：

- 「使い方ガイド」「チェックリスト」「可視化結果」の３種類のシート
- 39個の質問にセルフチェックで回答
- 回答方式は５段階の選択式（成熟度モデル）
- グループ会社間等での比較も可能



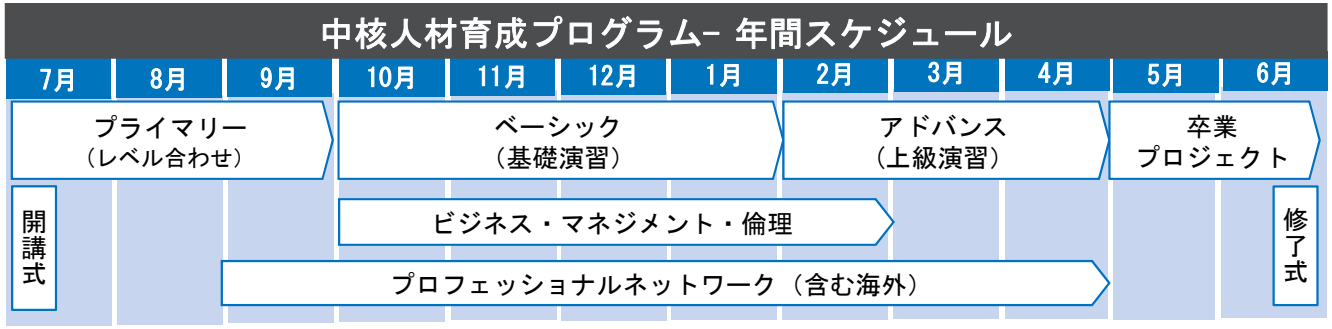
https://www.ipa.go.jp/security/economics/checktool/index.html

3-①：産業サイバーセキュリティセンター（ICSCoE）3期生修了、5期生募集中

- 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等を実施。
- 第４期中核人材育成プログラム（2020年7月開講）には、47名が参加。

□　１年を通じた集中トレーニング

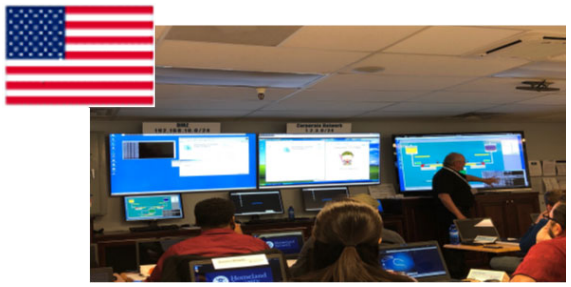
□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：47人）



- 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

□　米・英・仏等の海外とも協調したトレーニングを実施



➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加

➢ 政府機関、自動車業界、スタートアップ企業の代表者等からの講義や意見交換を実施

➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

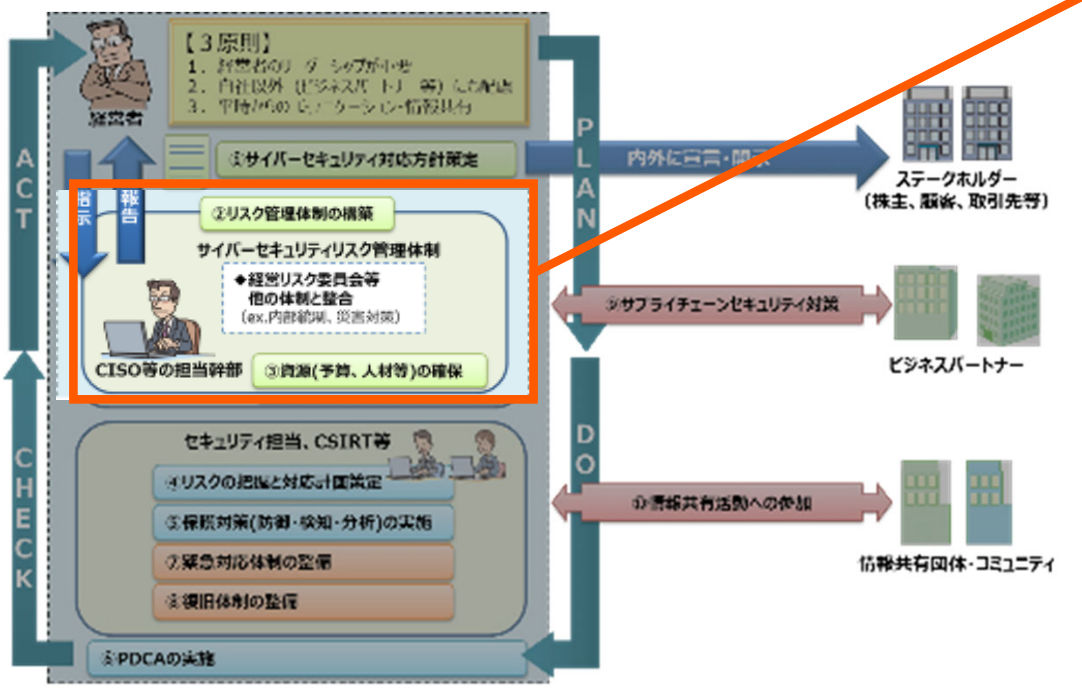
など

3-②：『セキュリティ体制構築・人材確保の手引き』の開発

累計**4,569**ダウンロード
（2021年2月末時点）

- サイバーセキュリティ経営ガイドラインの付録文Fとして**2020年9月30日に第１版を公表。**
  今後の課題としていた箇所を更新し、第1.1版として4月に公表予定。

サイバーセキュリティ経営ガイドライン（10の指示）



手引きの構成（指示2、3の深掘り）

指示２
サイバーセキュリティリスク管理体制の構築

- 2.1 経営者のリーダーシップの下でのセキュリティ体制の検討
- 2.2 セキュリティ統括機能の検討
- 2.3 セキュリティ関連タスクを担う部門・関係会社の特定・責任明確化

指示３
サイバーセキュリティ対策のための資源確保

- 3.1 セキュリティ人材の確保
- 3.2 プラス・セキュリティ人材の確保
- 3.3 教育プログラム・試験・資格等の活用と人材育成計画の検討

第1.1版での更新ポイント：

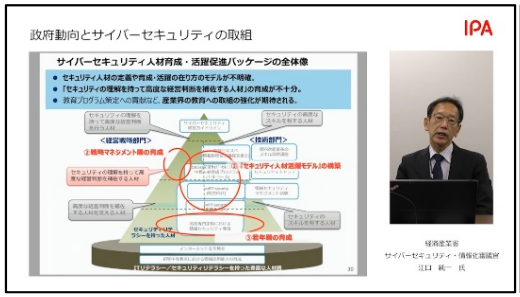
- サイバーセキュリティ対策に従事する人材の確保
- 業務内容や役割に応じた人材の育成方法
- ユーザー企業で必要となるスキルの習得に活用可能な資格制度
- ユーザー企業でサイバーセキュリティ対策に従事する人材の育成パスのイメージ

3-③：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

- 経営層が示す戦略の下、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場である「戦略マネジメント層」の育成が急務。以下の取組を推進中。
  - サイバーセキュリティ2020に基づき、IPA産業サイバーセキュリティセンターでは、2019年度に引き続き2020年度も戦略マネジメント層向けのセミナーを実施。
  - 東京工業大学CUMOTは「サイバーセキュリティ経営戦略コース」を開催。
  - NISCも「戦略マネジメント層向けサイバーセキュリティセミナー」の開催、「プラス・セキュリティ」知識を補充するモデルカリキュラムの策定といった取組を推進。

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」

- 2021年２月実施（2018年度から3回目）
- サイバーセキュリティは経営課題であること及び経営層をはじめ関係者が認知すべきセキュリティ機能の重要性の理解を目指す。
- 2020年度はオンライン（オンデマンド形式）で開講。講演・パネルディスカッション・講義（約10時間分収録）により、先進事例・課題や解決策・ノウハウなどを体系的に学ぶプログラムを提供。



東京工業大学ＣＵＭＯＴ「サイバーセキュリティ経営戦略コース」

- 2021年2月～6月
  ※新型コロナウィルス感染症対策で原則オンライン開催。
- サイバーセキュリティ経営及びその戦略立案に求められる知識・能力を備え、企業・組織を先導する人材の育成を目的とする。
- 座学だけでなく、受講生同士による議論やグループ課題によって理解を深める実践的なスタイルの講義を１回2時間、全20回実施。

3-④：国立高専機構と産・官との連携促進・具体化に向けて

- 国立高専におけるセキュリティ教育が産業界の求める人材像とも整合していくためには、産学官の継続的な協力関係が必要。
- これまで国立高専機構がIPAや業界団体（CRIC CSF、JNSA）等と進めてきた連携を効果的かつ継続的なものとするために、SC3の場の活用も含め、産学官連携を推進していく。

＜高専・産・官の対話の場（イメージ）＞

継続的な協力体制

学

高専機構　等
- ■高度セキュリティ人材、情報系人材、非情報系人材
- ■教員　　等

産

企業・業界団体
- ■CRIC CSF、JUAS、JNSA
- ■ユーザー企業、IT・セキュリティベンダー　等

ニーズ・シーズの整理・具体化 ▶ 協力の検討 ▶ 産業界に求められるセキュリティ人材の育成・輩出

- ・トップガンの育成支援
- ・キャリア教育
- ・機械・建築・生物等の分野別教材の開発・素材提供
- ・セキュリティ教員向けのFD（Faculty Development）
- ・講師派遣
- ・産業界に求められるセキュリティ人材像の共有
- ・適切なプレイヤーとのマッチング

官

関係省庁・独法等
- ■NISC、文科省
- ■IPA、JPCERT/CC　　等

3-④：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

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（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
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。	・**高専機構がJNSAに講師派遣を依頼できる体制を構築。** ・**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。**
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 ・**JNSAがオンライン授業環境を利用した現場第一線講師による最新事例授業の開催検討中** ※一度に数十校を対象に同時開催可能。JNSAで実施中の岡山理科大学遠隔授業内容を最新事例中心に発展・展開。 ・**高専機構が四国地域企業のIPA ICSCoE修了生に講師派遣を依頼できる体制を構築。** ・**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が高専機構と連携し、業界別（例．機械、電気、建築等）ビデオ教材（20分程度）を作成。** ※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。
KOSEN 国立高等専門学校機構 国立高専教員	・**JNSAが教員向けのセキュリティ基礎講座の実施を検討中。** ※神奈川県での高校教員向けセキュリティ基礎講座の実績を展開。	・**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。** ・**高専機構が、教師向け合宿の機会に、METIにセキュリティ専門官の講師派遣を依頼できる体制を構築。**

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。


ゲーム形式教材のイメージ

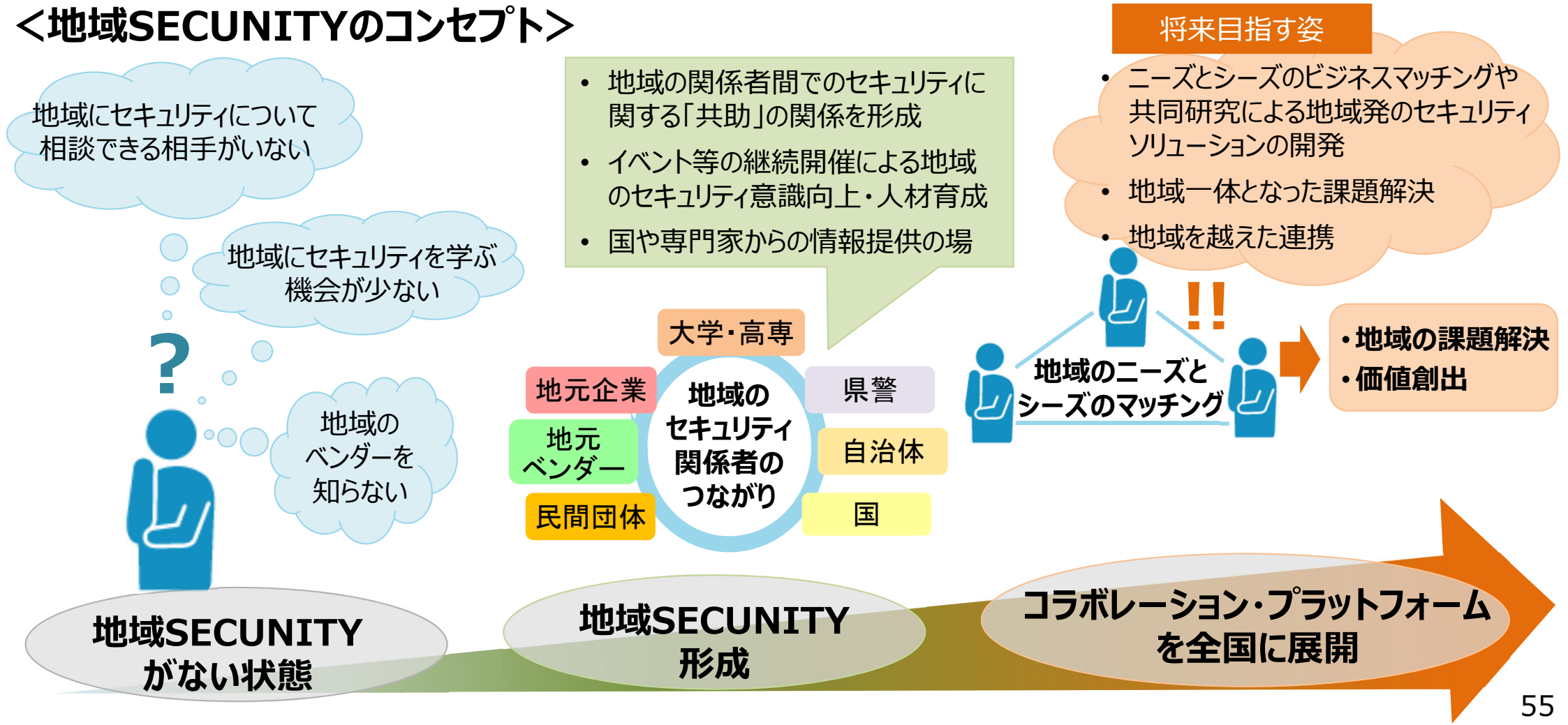

開催の様子@石川高専


AppGoat講習の様子

3-⑤：地域に根付いたセキュリティ・コミュニティ（地域SECUNITY）の形成促進

- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動を、「地域SECUNITY」と命名。
- まずは各地域で地域SECUNITYの形成を促進し、将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指す。

＜地域SECUNITYのコンセプト＞



3-⑥：地域SECUNITY形成のためのプラクティス集（2021年2月17日公開）

- 2020年度、全国各地域で経済産業局や地元の協力機関等とともにセキュリティコミュニティの形成を促進（北海道、東北、関東、東海、関西、中国、四国、九州、沖縄）
- 各地域におけるセキュリティコミュニティの形成を促進するため、モデルとなるようなコミュニティへのヒアリングを実施し、プラクティスとして公開
- 合わせてコミュニティ形成に関連するセキュリティセミナー等への対応が可能な講師派遣制度のリストも公開

＜プラクティス集概要＞

対象コミュニティ

- 北海道地域情報セキュリティ連絡会
- 北海道中小企業サイバーセキュリティ支援ネットワーク
- サイバーセキュリティセミナ in 岩手
- 宮城県サイバーセキュリティ協議会
- みちのく情報セキュリティ推進機構　みちのく情報セキュリティ推進センター
- 関西サイバーセキュリティ・ネットワーク
- 総関西サイバーセキュリティLT大会
- 九州経済連合会　サイバーセキュリティ推進WG
- 熊本県サイバーセキュリティ推進協議会
- 鹿児島県サイバーセキュリティ協議会

項目

1．コミュニティ設立の経緯・狙い
2．取組方針
3．協力機関・団体等との関係性
4．取組・イベント開催概要
5．実践からのプラクティス

北海道地域

北海道地域情報セキュリティ連絡会
(Hokkaido Aria Information Security Liaison：HAISL)
URL: https://www.facebook.com/haisl0929

1．コミュニティ設立の経緯・狙い

サイバー空間における脅威が増大し、情報セキュリティ対策の重要性が高まる中、産学官が保有する幅広い情報を共有するとともに、これらの情報を広く発信することにより、北海道地域における情報セキュリティ意識の向上等を図ることを目的に、北海道経済産業局・北海道総合通信局・北海道警察の3機関を事務局として平成26年9月に発足。

2．取組方針

産学官による地域コミュニティとして、企業経営者・セキュリティ担当者、支援機関等を対象とした情報セキュリティに関する意識の喚起や、情報セキュリティ技術・セキュリティマネジメント能力向上に向けた機会を提供することにより、人材育成や機運醸成を図る。

3．協力機関・団体等との関係性

下表のほか、北海道中小企業サイバーセキュリティ支援ネットワークとも連携。

教育機関	北海道大学ほか大学10機関、高専1機関、専門学校1機関
民間企業・団体	企業14社、業界団体12団体
官公庁	北海道、北海道教育庁、札幌市、札幌市教育委員会
事務局	北海道経済産業局、北海道総合通信局、北海道警察

4．取組・イベント開催概要

以下のイベントのほか、メルマガやfacebookによる情報発信、関係団体主催のイベント支援等。

■会員向けセミナー
会員向けの勉強会を年2回程度開催。事務局機関が持ち回りで幹事となり、事務局からの情報提供、外部講師による講演を実施。

■大規模セミナー
会員のほか、企業経営者やセキュリティ担当者等を対象としたセミナーを年１回程度開催。事務局からの情報提供のほか、複数名の外部講師による講演を実施。

■Hardening Project
Web Application Security Forum(WASForum) が実施するセキュリティ堅牢化に向けた競技会。令和元年7月、道内初開催の第14回にHAISLが共催で参画。これを契機に令和元年11月には学生向け競技会をHAISLと北海道警察の主催で開催。

5．実践からのプラクティス（１／２）

プラクティス1	ヒアリングや会合等の機会を活用し、参加機関拡大に向けて団体・企業・大学等へのPRを強化

プラクティスの実践を通じて得られる効果
企業の参加を促進する／地域の関係機関を巻き込む／継続的な活動を可能にする／活動の効果を高める／運営の負担を軽減する、他

目的	参加機関の拡大に向け、候補となる団体・企業・大学による活動を認知してもらい、関心を持ってもらえるようにする
実施主体	地域セキュリティコミュニティ事務局
実施内容	● ヒアリングや会合等の機会に、事務局機関の所管機関や関係団体などに**積極的な情報提供を行うことを通じて、通年にわたって参画機関を募集**。 ● 事務局機関のチャネルを活かしメディアにアプローチすることで、活動を**社会が認知する機会を創出**。
効果	● 積極的なPRを通じて、活動に関心をもつ団体・企業・大学等に参加が歓迎されていることを伝え、参加しやすい環境を作ることで、参画機関の拡大を実現。 ● メディアを通じたコミュニティ活動に関する社会の認知度向上は、サイバーセキュリティに関する啓発効果を高めることにつながり、結果的にコミュニティ活動そのものの効果も向上させる。

4-①：情報セキュリティサービス審査登録制度の概要

- **一定の技術・品質管理要件を定めた「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リストを2018年6月よりIPAが公開。

＜情報セキュリティサービスにおける課題＞

どの事業者のサービスを選べば良いか分からない

信頼できるサービス事業者にお願いしたい

ユーザ
（企業、政府機関等）

選定時に活用

我が社のサービスをもっと見つけて欲しい

我が社の技術力、サービス品質をアピールしたい

ベンダー
サービス提供事業者

審査を受けてリストに掲載

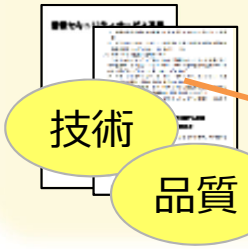
○情報セキュリティサービス基準適合サービスリスト（IPA）

審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開

基準を満たした223サービスが掲載

- 情報セキュリティ監査（62サービス）
- 脆弱性診断（91サービス）
- デジタルフォレンジック（29サービス）
- セキュリティ監視・運用（41サービス）

2020年12月現在



○情報セキュリティサービス基準（METI）

上記４サービスに関して技術要件・品質管理要件を定めた基準

本制度を通じて目指す社会

専門的知識を持たないユーザでも、自社に最適かつ品質を備えたサービスを選択できる

技術と品質を備えた情報セキュリティサービスの普及・発展

制度の普及・浸透

（参考）登録サービス事業者の所在地の内訳

- **情報セキュリティ監査**（62サービス）　東京47、神奈川6、埼玉3、兵庫2、千葉1、京都1、大阪1、広島1
- **脆弱性診断**（91サービス）　東京73、神奈川6、大阪3、新潟2、兵庫2、宮城1、茨城1、千葉1、大分1、沖縄1
- **デジタルフォレンジック**（29サービス）　東京24、神奈川3、兵庫1、熊本1
- **セキュリティ監視・運用**（41サービス）　東京32、神奈川6、大阪1、兵庫1、大分1

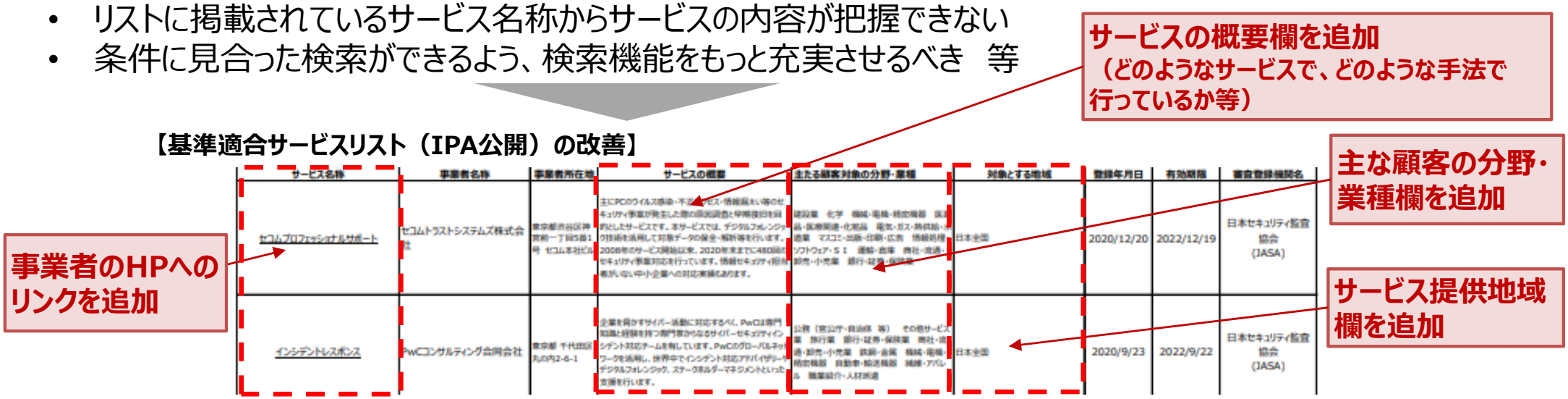
4-②：基準適合サービスリストの改善（2021年2月）

- 制度ユーザーからの要望を踏まえ、利用者にとってより分かりやすいものにすべく、基準適合サービスリストを改善。（2021年2月1日公開）
- 官側の利用促進が必要との意見もあるところ、政府統一基準群等への引用も検討中。

ユーザーからの要望

- リストから条件に合った事業者を検索するのが不便である
- リストに掲載されているサービス名称からサービスの内容が把握できない
- 条件に見合った検索ができるよう、検索機能をもっと充実させるべき　等

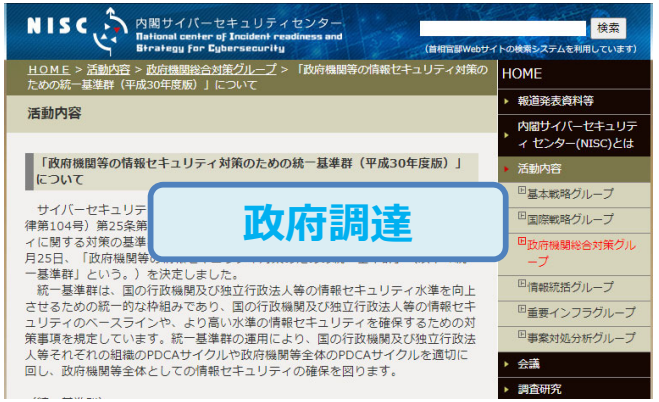
【基準適合サービスリスト（IPA公開）の改善】



有識者からの意見

- 政府調達で本制度が使われる等、官側の利用促進も図っていくべき　等

「政府機関等の情報セキュリティ対策のための統一基準群」等での引用も検討中。



4-③④包括的なサイバーセキュリティ検証基盤を構築し、『Proven in Japan』を促進

- 「Proven in 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

4-③：セキュリティ製品の有効性検証・実環境における試行検証実施

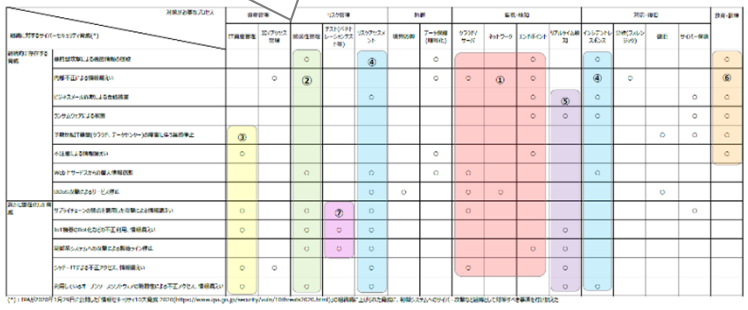
緑 青

- 有識者会議を開催し、重要分野の選定、該当分野の製品の公募、検証作業を実施。
- 有効性検証、実環境における試行検証それぞれのアウトプットを取りまとめ、コラボレーション・プラットフォームで発表。

累計1,967DL
（2020/4/10～2021/1/31）

有識者会議でセキュリティ領域の全体マップを作成し、**重要分野**を選定（市場性、日本発の製品が強味を発揮可能か等の観点から）

① 脅威の可視化
② 脆弱性の可視化
③ IT資産管理
④ 脅威インテリジェンスの整理・管理
⑤ マルウェア感染/は省の重篤度判定
⑥ 教育・トレーニング
⑦ ハイレベルセキュリティ検証



重要分野に該当する**製品を公募で選定**
有効性評価、実環境における試行**評価を実施**

結果をIPAから公表した他、第13回コラボレーション・プラットフォーム（2020年9月）で発表、**ビジネスマッチング**を実施

日本発製品・サービスのプロモーションに資するため、主に以下の内容を公表

有効性検証結果
製品のストロングポイント

実環境における試行検証結果
『試行導入・導入実績公表の手引き』
- 公表のメリット／デメリット
- 公表可否判断のポイント
- 公表内容
- ステークホルダーとの調整 等

4-③：セキュリティ製品の有効性検証・実環境における試行検証実施

緑 青

- コラボレーション・プラットフォームで成果発表とビジネスマッチングを実施、90名が参加
- ベンダー各社は有効性検証に参加したことを自社の宣伝活動に活用

コラボレーション・プラットフォームでビジネスマッチングを実施

（第13回、2020年9月28日）

- 「課題解決に役立つ対策技術のご紹介」と題し、検証に参加いただいたベンダーの製品紹介と、個別相談会を実施
- 90名参加

ベンダー各社が有効性検証の成果を自社製品の宣伝に活用

- **Visional社ブログ**
  - 「yamory」が IPA のセキュリティ製品の有効性検証の試行対象として選定
  - 「yamory」の終わりなき技術的挑戦。Visionalの仲間とともに、サイバーセキュリティの未来を創る。
- **アラクサラネットワークス社広報**
  - 「IPAがアラクサラのネットワーク可視化・異常検知ソリューション(AX-NV)の検証結果を公表」
  - 日刊工業新聞、日経新聞、日経産業新聞がアラクサラの広報を転載して紹介


yamory Blog

2020/4/13 お知らせ

「yamory」が IPA のセキュリティ製品の有効性検証の試行対象として選定

編集チーム

オープンソース脆弱性管理ツール「yamory」は、この度、独立行政法人情報処理推進機構（IPA）の「セキュリティ製品の有効性検証の試行」において対象製品に選ばれ、その結果が公表されました。

1. オープンソース脆弱性管理ツール「yamory（ヤモリー）」について
2. 「セキュリティ製品の有効性検証の試行」について
3. 有効性検証の試行結果

オープンソース脆弱性管理ツール「yamory（ヤモリー）」について

yamoryは、オープンソースの利用状況を自動で把握し、脆弱性を検出、管理・対策できるサービスです。

オープンソースに関する最新の脆弱性情報を用いて、yamory 独自の脆弱性データベースを構築しています。


AlaxalA

お問い合わせ

ホーム ＞ 会社情報 ＞ プレスリリース ＞
IPAがアラクサラのネットワーク可視化・異常検知ソリューション(AX-NV)の検証結果を公表

IPAがアラクサラのネットワーク可視化・異常検知ソリューション(AX-NV)の検証結果を公表

2020年5月25日
アラクサラネットワークス株式会社

アラクサラネットワークス株式会社（本社：神奈川県川崎市　代表取締役社長兼CEO 中川 勝博 ／ 以下、アラクサラ）のネットワーク可視化・異常検知ソリューションAX-Network-Visualization（AX-NV）は、独立行政法人情報処理推進機構（IPA）が行った「セキュリティ製品の有効性検証の試行」において「利用者の実環境における試行検証」の対象製品として選定され、その結果が公表されました。

https://www.ipa.go.jp/security/economics/shikoukekka2019.html

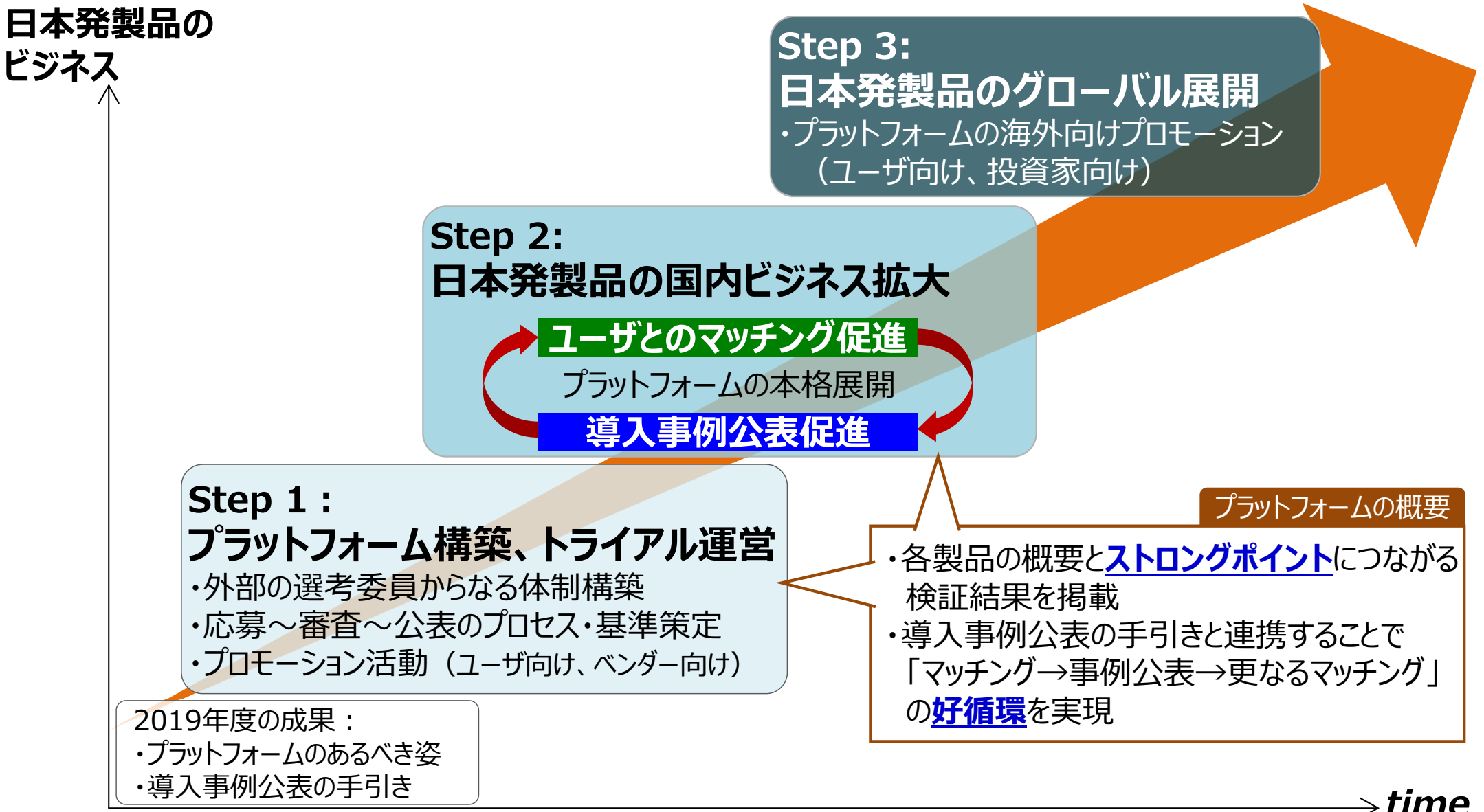
経済産業省の産業サイバーセキュリティ研究会の下に設置したWG3は、日本発の新たなセキュリティ製品の市場参入を促進するために、有効性検証および実環境における試行導入検証を実施し、その内容を発信することで、ユーザが日本発の製品を選定しやすい環境の構築を進めています。

これを受けて「サイバーセキュリティ検証基盤構築に向けた有識者会議(以下、有識者会議)」をIPA内に2019年9月に立ち上げました。そして有識者会議が、日本のユーザ企業の重要課題に対応可能な日本発のセキュリティ製品として、AX-NVを対象にユーザの実環境における試行検証を行いました。

4-③：セキュリティ製品の有効性検証・実環境における試行検証実施

緑 青

２年間に渡る本事業の成果を基に、マッチングプラットフォーム構築、日本発セキュリティ製品の国内ビジネス拡大、更に海外展開を目指す。



赤

4-④：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

- 検証サービスの信頼性向上及び検証ビジネスの活性化のために、2019年度に作成した手引きについて、2020年度は**本編を拡充するとともに、検証サービス事業者・検証依頼者それぞれを対象とし、より具体的な記載を行った別冊を作成**。

実証

検証事業者

検証

・IoT機器等
＜2019年度＞
ルータ、UTM、タブレット、スマートロック
＜2020年度＞
ドローン、スイッチ、ロボット掃除機、ノートPC

実証の成果と活用のイメージ

機器のサイバーセキュリティ確保のための セキュリティ検証手引き

検証サービス事業者、検証依頼者の双方が、検証における各フェーズにおいて留意すべき事項等を記載

別冊1：検証サービス事業者向け

本編の記載を検証サービス事業者向けに深掘り
・脅威分析の手法　・実施すべき検証項目　・検証の流れ　等

別冊2：検証依頼者（特に機器メーカ）向け

本編の記載を主な検証依頼者である機器メーカ向けに深掘り
・機器開発における検証の重要
・検証を依頼する際に必要な事項　等

別冊3：検証人材の育成について

検証人材の育成について深掘り
・検証人材に求められるスキル・知識、キャリアデザイン　等

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

赤

4-④：ハイレベル検証：機器のサイバーセキュリティ確保のための検証の手引き策定

- 検証サービスの信頼性向上及び検証ビジネスの活性化のために、2019年度に作成した手引きについて、2020年度は**本編を拡充するとともに、検証サービス事業者・検証依頼者それぞれを対象とし、より具体的な記載を行った別冊を作成**。

機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き （2019年度作成、2021年3月拡充）

- 検証スキルの向上や検証サービスの高度化を目的とし、検証サービス事業者が実施すべき事項や、検証依頼者が実施すべき事項や用意すべき情報、二者間のコミュニケーションにおいて留意すべき事項等を記載。
- 信頼できる検証サービス事業者を判断・選択するための基準を記載。

別冊1：脅威分析及びセキュリティ検証の詳細解説書（2021年3月作成）

- 検証ビジネス全体の底上げのために、検証サービス事業者が実施すべき脅威分析の手法や実施すべき検証項目、検証の流れを詳細に示す。
- 機器全般に汎用的に活用できる整理を目標とするが、対象の例としてIoT機器を例示し具体的な記載も行う。

別冊2：機器メーカに向けた脅威分析及びセキュリティ検証の解説書（2021年3月作成）

- 機器メーカが実施すべき事項や用意すべき情報等、意図した検証を依頼するために必要な事項を詳細に示す。
- 攻撃手法への対策例や、検証結果を踏まえたリスク評価等の対応方針を示す。
- 機器開発におけるセキュリティ検証の重要性を示す。

別冊3：検証人材の育成に向けた手引き（2021年3月作成）

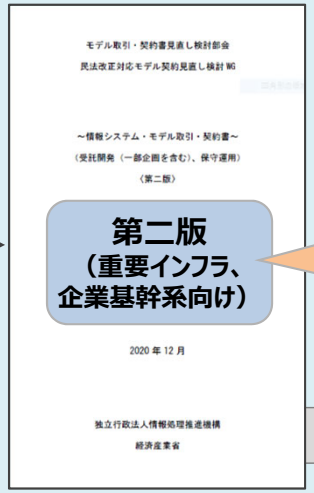
- 検証人材に求められるスキル・知識を示し、それらのスキル・知識を獲得するために望まれる取組を示す。
- 検証人材のキャリアを構想・設計する上で考慮すべき観点を示し、検証人材のキャリアの可能性を示す。

4-⑤：「情報システム・モデル取引・契約書」第二版を公開（2020年12月22日）

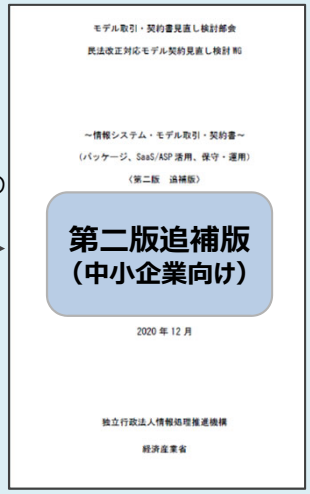
- モデル契約本体はセキュリティ条項（第50条）等の記述を強化
- セキュリティ仕様策定を支援するための参照文書を２点作成
  - 「セキュリティ仕様策定プロセス」
  - 「情報システム開発契約のセキュリティ仕様作成のためのガイドライン（Windows Active Directory編）」
- 各種イベントでの講演や各業界団体を通した展開等により普及・啓発を進める

モデル契約本体

第一版（2007年4月公表）→ 今回改訂 → 第二版（重要インフラ、企業基幹系向け）



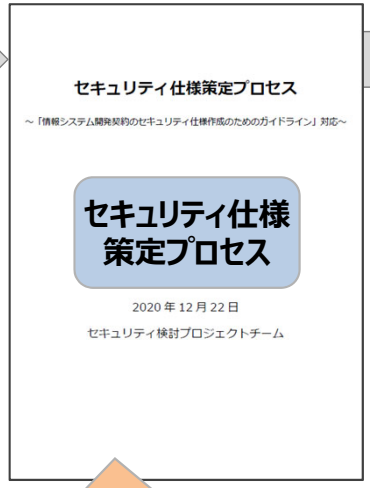
（第一版の）追補版（2008年4月公表）→ 今回最低限の改訂 → 第二版追補版（中小企業向け）



特に**第50条（セキュリティ条項）**の記述を大幅に増強

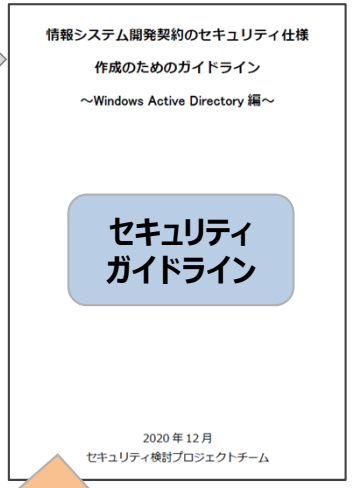
- ユーザとベンダとは、それぞれの立場に応じて**必要な情報を示しつつ**、リスクやコスト等について**相互に協議**することにより、システムに実装する「セキュリティ仕様」を決めることが必要という観点で記述
- ベンダーは当該仕様に基づいてセキュリティ対策を行う義務を負うにとどまることを明記する等、**責任分界点を明確化**

参照 →



ユーザ・ベンダー間のあるべき検討プロセスの解説

参照 →



脅威分析と、その対策としてのOS等のセキュリティ設定ガイド

コラボレーション・プラットフォームを含む各種イベントでの紹介や業界団体を通じた展開等で普及・啓発

↓

今後の開発案件におけるシステムのセキュリティ強化、ユーザ・ベンダー間のトラブル防止に貢献

4-⑥：コラボレーション・プラットフォームの2020年度開催状況

- サイバーセキュリティに関する情報交換、交流を行っていただける「場」を提供することを目的としたコラボレーション・プラットフォームを2018年6月からIPAを会場として開催してきたが、コロナ禍において**2020年度は計４回オンライン開催**。

	開催日	参加人数	テーマ
第13回	**2020年9月28日**	**90名**	**課題解決に役立つ対策技術のご紹介**
	➢ 検証基盤構築事業ならび に中小企業向け製品検証事業の取り組みの紹介 ➢ 事業に参加いただいた製品・ソリューションの個別相談会の実施		
第14回	**10月30日**	**91名**	**テレワークとセキュリティ**
	➢ 前半は講演、後半は⑴テレワークで注意すべきサイバー攻撃、⑵テレワークにおけるガバナンス、⑶テレワークにおけるインシデント対応のあり方をテーマに、解決策や対策のヒントなどをベンダー・ユーザー双方の立場から議論いただくパネルディスカッションを実施。		
第15回	**2021年1月29日**	**123名**	**中小企業との情報共有のあり方**
	➢ 今年度のお助け隊実証事業での事例の紹介 ➢ 中小企業とのサイバーセキュリティ関連での脅威情報やその対策情報の共有のあり方や、課題やその解決策についてあらゆる立場から議論いただくパネルディスカッションを実施。		
第16回	**2月25日**	**172名**	**クラウドシフトのセキュリティ**
	➢ テレワーク、DX等の新しい業務形態やゼロトラスト、データドリブン等のパラダイムの受容が求められる中、クラウド利用におけるセキュリティ課題と対応について講演とパネルディスカッションを実施。		

4-⑥：コラボレーション・プラットフォームの今後の方向性

- オンライン開催では気軽に参加いただける一方で、コラプラが目指してきた「あらゆるコラボレーションの創出」には、双方向でのコミュニケーションが取りづらい等のオンライン開催特有の障壁あり。
- コロナの状況を踏まえ、オンラインでの開催を工夫しながら継続しつつ、物理開催の復活を目指して企画の検討等を進めていく。

【参加者からのアンケート結果（第14回の一部抜粋）】

- 政策や他社動向について大変勉強になりました。
- 各パートにつながりがありコンテンツとして大変有意義でした。
- 最後に質疑応答の時間があれば良かったです。
- 取り上げて欲しいテーマ　①クラウド利用におけるセキュリティ　②DXにおけるセキュリティ　③脅威の最新動向
- オンラインより会場での開催が良いですね。

（前回WG3資料の再掲）コラボレーション・プラットフォームの目指す姿

【政策とのコラボレーション】

政策に関する意見交換の機会を設定し、**参加者からのご意見を着実に政策に反映**。

⇒政策紹介、グループディスカッション、情報交換会を通じて、意見交換を継続実施。

【シーズサイドのコラボレーション】

ベンダー企業間で連携を図り、**より大きなソリューションを市場に流通。**

⇒ベンダー、SIer等幅広い方々に参加いただき、参加者同士での連携検討を期待。

【ニーズサイドのコラボレーション】

ユーザ企業や大学等の間で課題を共有し、**セキュリティに関するニーズを具体化**。

⇒業界ごとのユーザニーズをプログラムに反映させるため、業界団体との連携等を検討。

【ニーズとシーズのコラボレーション】

ニーズサイドとシーズサイドの連携を図り、**ビジネスマッチング**につなげる。

⇒製品検証事業等の協力ベンダに登壇いただく等、ベンダ側とユーザ側とのパスとなるプログラムを検討。


METI
Ministry of Economy, Trade and Industry