経済産業省
Ministry of Economy, Trade and Industry

資料３

第７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４年４月11日

経済産業省

商務情報政策局

サイバー脅威の増加を踏まえた、攻めのサイバーセキュリティ強化へ

昨今の情勢を踏まえたサイバーセキュリティ対策の強化

- **昨今の情勢を踏まえたサイバー攻撃事案の潜在的なリスクの高まり**
- **産業界へのメッセージ（ランサムウェアやEmotetへの対応を含めて）**

Cyber New Normalにおける６つの処方箋 （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 サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化
② ソフトウェアの脆弱性対応強化（脆弱性情報の共有、SBOM）
③ 医療分野での対応（SBOM、お助け隊）
④ 「開発のための投資」から「検証のための投資」へのシフト
⑤ 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
⑥ Like-mindedの関係強化（国際情勢）

国としての対処能力の強化 （継続）

- **国としての対処能力の構築**

➢ サイバーインシデントに係る事故調査機能の構築
➢ サイバー攻撃被害に係る情報の共有・公表のあり方検討

高度化・巧妙化するサイバー攻撃の現状

- **昨今のサイバー攻撃は、**企業等の情報を暗号化して金銭をゆすり取る「ランサムウェア攻撃」や、国家支援型の攻撃集団等が特定の企業を執拗に狙う「標的型攻撃」など、**多種多様**。
- 加えて、**サイバー攻撃が高度化・巧妙化**するとともに、あらゆるものがネットワークにつながり、**攻撃の起点が増加**したことで、**サイバー攻撃が社会や産業に「広く」、「深く」影響を及ぼすように**なっている。

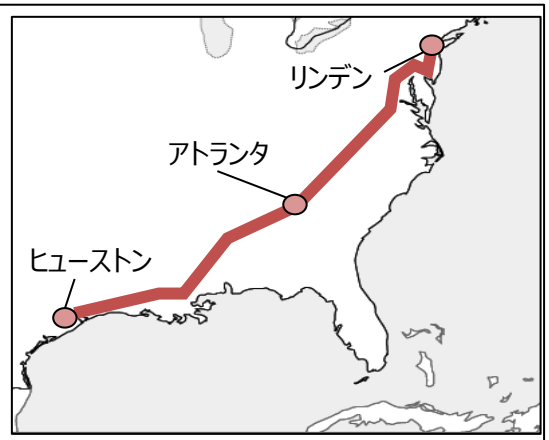
情報セキュリティ10大脅威 2022

順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報窃取
3位	サプライチェーンの弱点を悪用した攻撃
4位	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8位	詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10位	不注意による情報漏えい等の被害

<出典：(独)情報処理推進機構(IPA)、2022.1.27>

事例（海外）

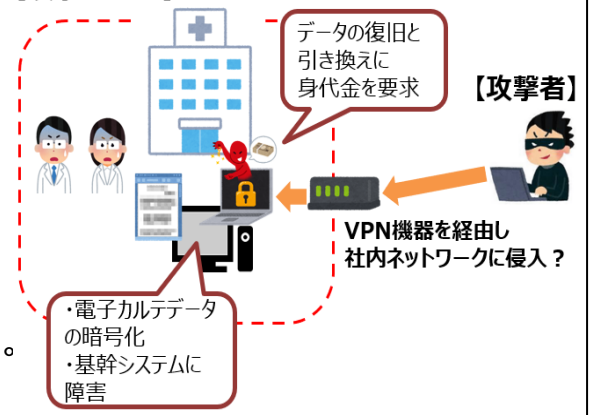
- 米国の専門機関によれば、米国における重要インフラ事業者等への攻撃のうち、**約1割は制御系システムまで影響を及ぼした**。
- 一例として、2021年5月には、米石油パイプライン大手がランサムウェア攻撃を受け、**全てのパイプラインを一時停止**。米運輸省が燃料輸送に関する緊急措置の導入を宣言する事態に陥った。



事例（国内）

- 2021年10月末、**国内の公立病院がランサムウェア攻撃を受け、電子カルテが暗号化され閲覧不可**になったほか、**診療報酬計算や電子カルテ閲覧に使用する基幹システムが使用不能**になったため、**新規患者の受け入れを停止**。
- 病院は、**身代金要求には応じず**、同年12月29日にサーバーを復旧させ、2022年1月４日から通常診療を再開。

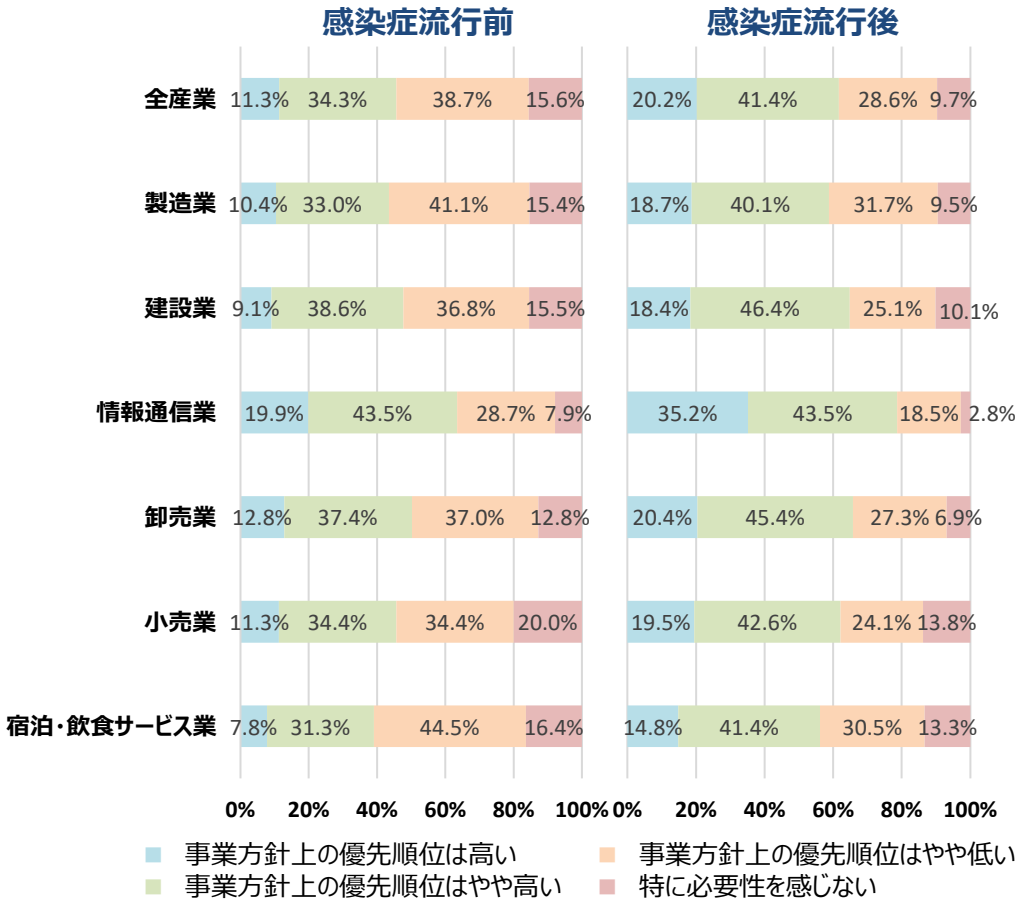
【攻撃イメージ】



デジタル化の進展とサイバーセキュリティ対策の必要性

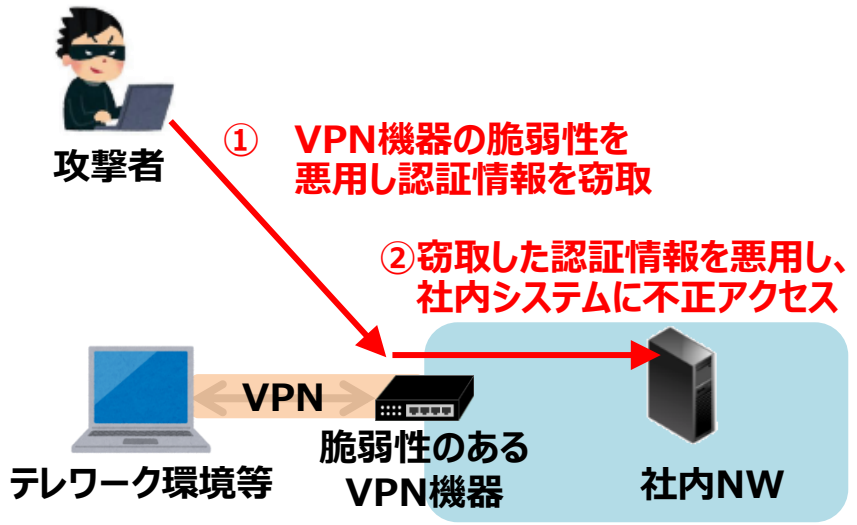
- デジタル化に対する意識は、コロナ禍の前後で、**産業領域を問わず大きく変化**。
- 一方、テレワークの利用等が増える中、VPNの脆弱性を突いたサイバー攻撃が増加するなど、**サイバー攻撃の脅威はあらゆる産業において無縁ではなくなっている**。

デジタル化に対する優先度の変化



（出典）中小企業庁「中小企業白書2021」

VPN機器に対する不正アクセス



事例：Fortinet製FortiOSの脆弱性

2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等その後追加公開があり、対象が計8.7万台に拡大。

米国上下水道分野における継続的なセキュリティ脅威

- 2021年10月、米国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（CISA）、連邦捜査局（FBI）、環境保護庁（EPA）等は、共同でサイバーセキュリティ勧告を発表し、上下水道への継続的なサイバー脅威について詳述。
- 米国ではこの数年、上下水道施設を対象にしたサイバー攻撃が多数報告されており、地域社会に清潔な飲料水を提供し、効果的に廃水を管理する能力が脅かされているとされる。

上下水道への攻撃事例

2019年から2021年にかけて上下水道システム(WWS)への攻撃が多数発生している。

2021年3月

ネバダ州にてWWS施設のSCADA及びバックアップに対して未知のランサムウェアによる攻撃

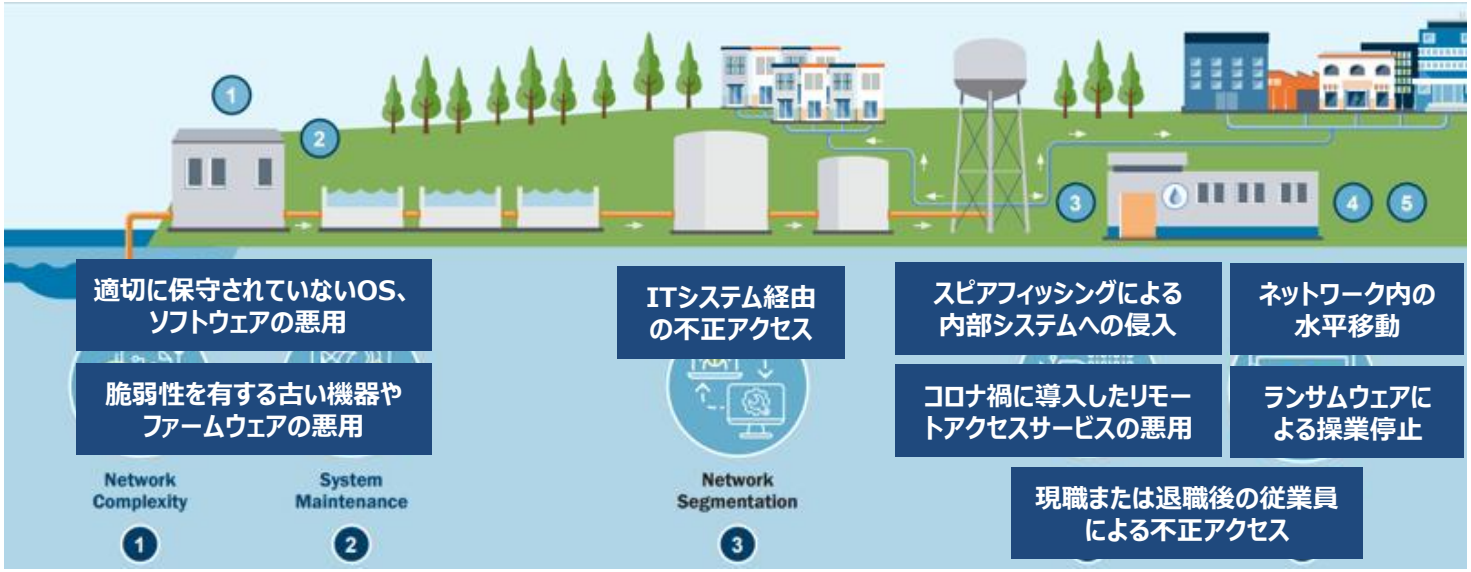
2021年7月

メイン州にてWWS施設のSCADAがランサムウェア ”ZuCaNo”に感染。復旧まで、手動のオペレーションを強制

2021年8月

カルフォルニア州のWWS施設にて3台のSCADAサーバがランサムウェア”Ghost”亜種に感染

共同勧告にて注意喚起がなされている脅威と推奨される対策



推奨される対策

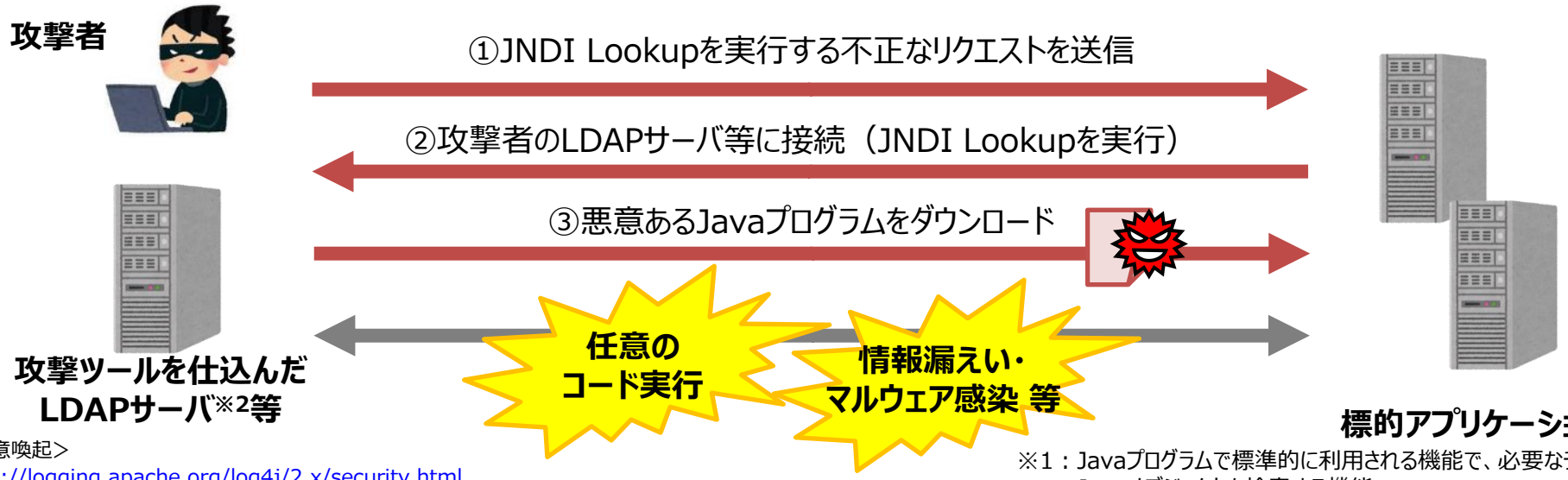
システム監視による不審な活動の検知	リモートアクセスの保護	IT/OTネットワークのセグメント化	対応計画の策定及び訓練等の実施	独立した安全制御システムの設置

[出典] CISA “CYBER RISKS RESOURCES FOR THE WATER AND WASTEWATER SYSTEMS SECTOR”等 を参考に作成

Apache Log4jの脆弱性：Log4Shell（CVE-2021-44228等）

- 2021年12月、Javaベースのオープンソースログ出力ライブラリ**Apache Log4jにおける任意コード実行の脆弱性が発表**された。当該脆弱性はLog4jのJNDI Lookup※1機能に起因するもので、Log4Shellとも呼ばれる。
- この脆弱性を利用することで、**Log4jが動作するアプリケーションに対して外部からの任意コード実行が可能**となり、情報漏えいやマルウェア感染等の被害に繋がる恐れがある。
- 脆弱性の公表をうけて、**NISCから重要インフラ事業者等へ注意喚起を発出。**多くのユーザーへの影響が考えられることから、**一般向けにも注意喚起**を公開。前後して、**専門機関（IPA、JPCERT/CC）からも、Log4jのバージョンアップや回避策を講じることで脆弱性に対処するよう注意喚起**がなされた。
- その後、この脆弱性の悪用を試みる通信が観測されているほか、Microsoft社より本脆弱性を利用したランサムウェアの存在が報告されるなどしている。

◆ **Log4Shell（CVE-2021-44228等）を利用した攻撃のイメージ**



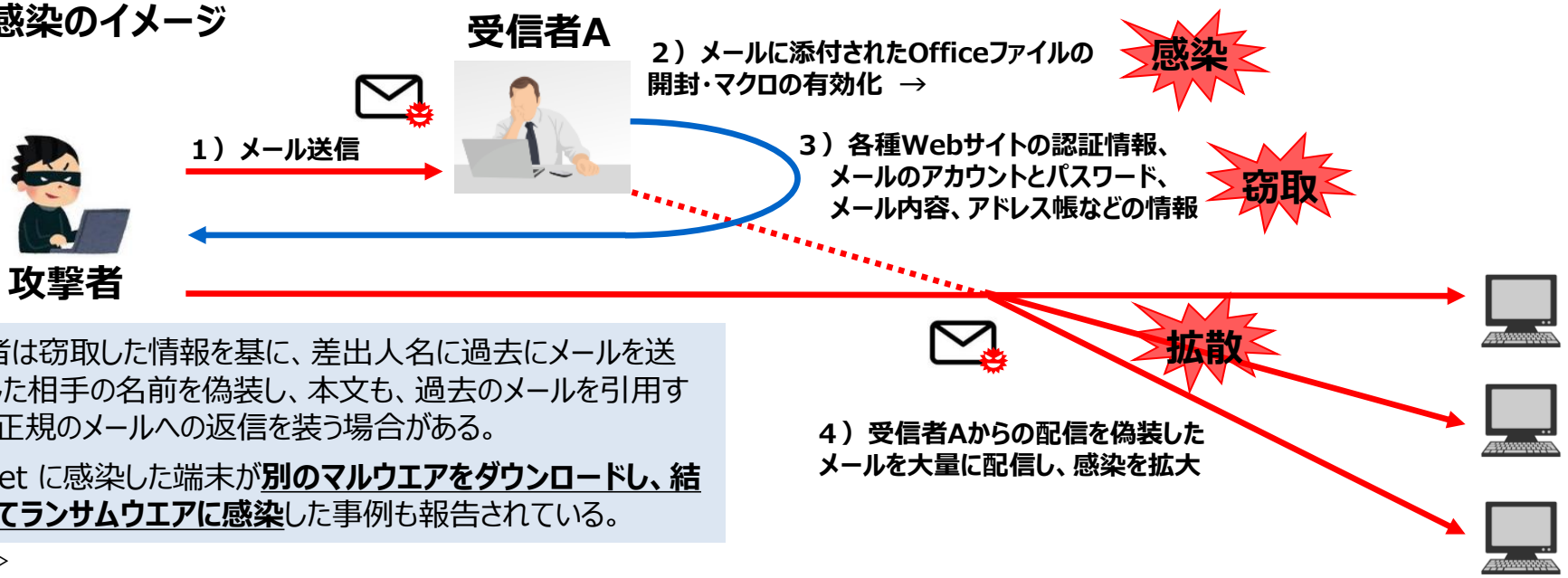
※1：Javaプログラムで標準的に利用される機能で、必要なデータを含むJavaオブジェクトを検索する機能
※2：特定のキーに対応する情報を返すディレクトリサーバ

<注意喚起>
https://logging.apache.org/log4j/2.x/security.html
https://www.nisc.go.jp/press/pdf/20211213NISC_press.pdf
https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html
https://www.jpcert.or.jp/at/2021/at210050.html

ウイルスへの感染を狙う攻撃メール：“Emotet”

- **Emotetは、メールを介して感染する、情報の窃取や他のマルウェアへの感染のため利用されるマルウェア**であり、国内でも2019年10月頃に複数企業で被害事例が相次いだ。2021年1月にテイクダウン（ サーバー等攻撃インフラの接収）が行われ、一時感染は落ち着いた。
- 2021年11月に攻撃活動再開の兆候が確認され、**2022年2月の第一週より急速に拡大**。**改めて、IPAやJPCERT/CCが注意喚起**を行っている。
- 初期と異なる攻撃手法として、**Emotetが正規のメールから添付ファイルを窃取して Emotetへの感染を引き起こすOfficeファイルとともに送付する事例**や、メール配信経路のセキュリティ製品による検知からのすり抜けを狙って**パスワード付きZIPファイルが添付される事例**が確認されている。

攻撃・感染のイメージ



- ✓ 攻撃者は窃取した情報を基に、差出人名に過去にメールを送受信した相手の名前を偽装し、本文も、過去のメールを引用する等、正規のメールへの返信を装う場合がある。
- ✓ Emotet に感染した端末が**別のマルウエアをダウンロードし、結果としてランサムウエアに感染**した事例も報告されている。

<注意喚起>
https://www.ipa.go.jp/security/announce/20191202.html
https://www.jpcert.or.jp/at/2022/at220006.html

サイバーセキュリティ対策についての産業界へのメッセージ（概要）　（案）

- 昨今、ランサムウェアやEmotet（エモテット）をはじめ、サイバー攻撃による被害が増加傾向。政府からも注意喚起を発出。
- 各企業・団体等においては、**組織幹部のリーダーシップ**の下、以下に掲げる対策を講じることにより、**対策の強化に努めるとともに、被害を受けた場合の適切な対応**が必要。

１．サイバーセキュリティ対策を徹底し、持続可能な体制を確立する

- 保有する情報資産を漏れなく把握する。
- 不審なメールへの警戒や、機器等に対して最新のセキュリティパッチを当てる等、脆弱性対策を徹底する。
- 多要素認証等により認証を強化する。
- データ滅失に備えデータのバックアップを取得し、ネットワークから切り離された場所に保管する。
- サイバー攻撃を受けた際の対応について、普段から役員および職員に対して教育・訓練を行う。
- システムが停止した場合に、業務を止めないための計画（BCP）を策定し、代替手段を整備する。

２．感染が確認された場合には、適時、報告・相談・対応を行う

- 感染拡大防止に留意するとともに、専門機関やセキュリティベンダー等へ支援を依頼しつつ、早期の業務復旧を図る。
- サイバー攻撃者への金銭の支払いは厳に慎む。
- Emotetの場合、取引関係者間などで感染が拡大することから、取引先を含めた関係者に状況を共有する。
- 警察、所管省庁等への相談・報告・届出を実施する。報告義務のある事案については、正確かつ迅速に行う。

３．中小企業においては「サイバーセキュリティお助け隊サービス」などの支援パッケージを活用する

- 自社がサイバー攻撃による被害を受けた場合、その影響は、サプライチェーン全体の事業活動や経済全体に及ぶ可能性があることを踏まえ、「サイバーセキュリティお助け隊サービス」※の活用など積極的なサイバーセキュリティ対策に取り組む。

４．ITサービス等提供事業者は、製品・サービスのセキュリティ対策に責任を持つ

メッセージの全文は下記のURLを参照
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20220411.pdf

※異常監視や、サイバー攻撃を受けた初動対応支援、被害を受けた場合の簡易保険など、中小企業に必要な対策をワンパッケージにまとめたサービス
参考　中小企業の情報セキュリティ：https://www.chusho.meti.go.jp/keiei/gijut/security.htm

サイバー脅威の増加を踏まえた、攻めのサイバーセキュリティ強化へ

昨今の情勢を踏まえたサイバーセキュリティ対策の強化

- **昨今の情勢を踏まえたサイバー攻撃事案の潜在的なリスクの高まり**
- **産業界へのメッセージ（ランサムウェアやEmotetへの対応を含めて）**

Cyber New Normalにおける６つの処方箋 （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 サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化
② ソフトウェアの脆弱性対応強化（脆弱性情報の共有、SBOM）
③ 医療分野での対応（SBOM、お助け隊）
④ 「開発のための投資」から「検証のための投資」へのシフト
⑤ 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
⑥ Like-mindedの関係強化（国際情勢）

国としての対処能力の強化 （継続）

- **国としての対処能力の構築**
  - サイバーインシデントに係る事故調査機能の構築
  - サイバー攻撃被害に係る情報の共有・公表のあり方検討

分野別SWGにおけるサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化

- **産業分野別サブワーキンググループ**を設置。CPSFに基づくセキュリティ対策の具体化を推進。
- 今後は、政府と産業界の協業を進めつつ、国際的なルール形成の推進に向けた取組や、**サプライチェーン全体のセキュリティ向上に向けた取組の実装**を進める。

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）
Industry by Industryで検討
（分野ごとに検討するためのSWGを設置）

ビルSWG

- ビルの管理・制御を行うビルシステムに係るサイバーセキュリティ対策を整理し、**ガイドライン第1版を公開（2019年6月）**。
- **2021年度は個別編(空調編)をドラフト**するとともに、**インシデントレスポンスに対する要求の方針案を整理**。

防衛産業SWG

- 米国の新標準と同程度まで強化した**新情報セキュリティ基準を策定（2022年４月１日）**。

スマートホームSWG

- シンプルな対策ガイドから、具体的な対策要件や他の標準との対比まで、セキュリティ対策を階層的に整理し、**ガイドライン1.0版を公開（2021年4月）**。

工場SWG

- **2022年夏を目途にガイドラインを作成予定**。

電力SWG

- 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、官民が取り組むべき課題と方向性について広く検討。CPSFも踏まえ、さらに取組が加速している諸外国の動きも視野に、様々な課題への対応を強化していく。
- **小売電気事業者ガイドラインを策定(2021年2月)**。

自動車産業SWG

- エンタープライズ領域（会社全体のベースとなるOA環境）対象とした**「自工会／部工会サイバーセキュリティガイドライン1.0版」を策定（2020年12月）し、サプライチェーンへの展開を実施。ガイドライン2.0版の作成（2022年4月予定）**。
- 工場セキュリティの課題対応についても検討中。

宇宙産業SWG

- 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、2021年１月に立ち上げ。
- **ガイドラインβ版を開発し、2022年2月からパブコメを実施。**

・・・

ソフトウェアの脆弱性対応強化

- ソフトウエア等の脆弱性への対応は、サイバーセキュリティ対策の基本。脆弱性情報への対応を促進するため、**脆弱性情報の共有制度の改善**や**機器・サービス提供事業者との連携強化**、**SBOMの活用**などの検討を進める。

【SBOMの活用に向けた今後の検討内容】

今年度の実証事業で、ソフトウェアの成分構成を表すSBOM（Software Bill of Materials）を活用することの有効性は確認された一方で、実際にビジネスで活用するためには課題も残されていることから、**産業分野ごとの状況を踏まえ、「規制や推奨化が見込まれる分野」や「効果が大きいと思われる分野」等を候補に実証**を継続予定。

1. SBOM活用モデルの最適化

- 産業分野によっては規制等の動きもあるため、**産業分野の状況に応じたSBOMの効果的な活用モデルを整理**。

2. SBOM共有のための環境整備

- 各分野等における標準的な**SBOMの項目、粒度、フォーマット、部品命名規則等の整理**。
- **契約、責任、費用負担**の整理。

3. SBOM自動生成ツールの活用促進による効率化

- SBOMツールの導入や利用方法に係る**情報発信、ノウハウの共有による導入工数の低減**。

4. 国際的な基準との整合性確保

- グローバルサプライチェーンにおいて国内と海外の整合性を確保しつつ効率的に部品管理を行うためには、**国内外の基準の整合化**が必要。

医療分野のサイバーセキュリティに関する検討の状況

- **医療機器のセキュリティ対策として、2020年3月、国際医療機器規制当局フォーラム（IMDRF）より**、医療機器のサイバーセキュリティ対策に関する**ガイダンスが発行**。**日本においても**、**2023年を目途に各種の基準等の改正**を予定。
- 医療機関における外部ネットワーク接続の拡大等を踏まえ、厚生労働省において、サイバーセキュリティ対策の在り方を検討中。

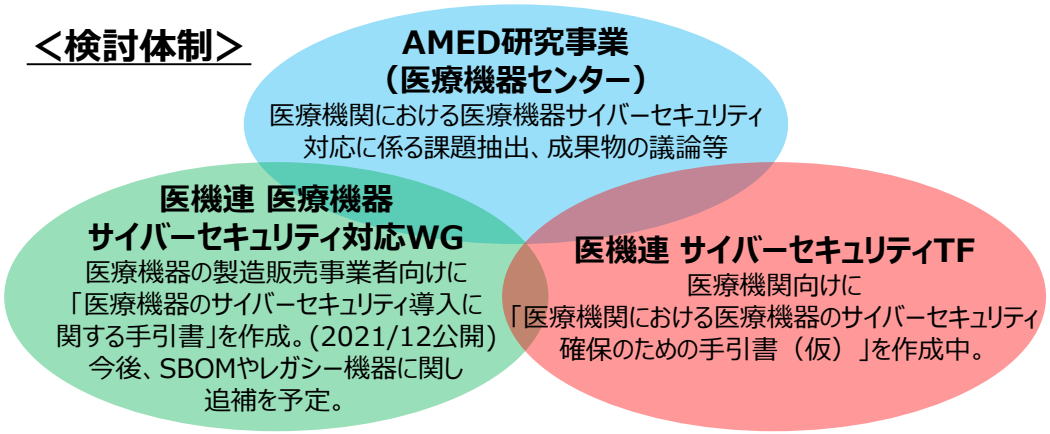
IMDRFガイダンス※1と国内対応

IMDRFガイダンスでは、医療機器のサイバーセキュリティに関する国際整合を図るため、「一般原則」と「ベストプラクティス」を提供。

○SBOMに関する記載

- 【市販前】ソフトウェアの透明性確保や脆弱性対応等のため、**顧客へのSBOM提供を医療機器製造業者に対して推奨**。
- 【市販後】**医療機関によるSBOMの要求**と、**インシデント対応や機器のライフサイクル管理での活用**について記載。
- 日本においても、**国際整合の観点からIMDRFガイダンスを導入すべく**、関係機関において、**医療機器のサイバーセキュリティに係る開発目標や技術要件を検討中**。

＜検討体制＞



医療機関等のサイバーセキュリティ対策

厚生労働省において、医療機関における外部ネットワーク接続の拡大や、国内の医療機関を標的にしたサイバー攻撃の増加を踏まえ、医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究を実施。

本調査研究事業では、

- ✓ 国内外における医療情報セキュリティ動向調査
- ✓ 医療情報システムのクラウド化における現状調査
- ✓ よりわかりやすいチェックリストの提案
- ✓ 有効なモデルセキュリティポリシー案の策定
- ✓ **医療機関における「サイバーセキュリティお助け隊」の活用可能性・追加すべきオプション等の検討**

を実施予定。

医療機関の規模やネットワーク構成等により、お助け隊をそのまま活用できるもの、特殊事情に合わせたオプションを必要とするものなどが存在する可能性。これらを**厚生労働省と連携し精査・検討していく**。

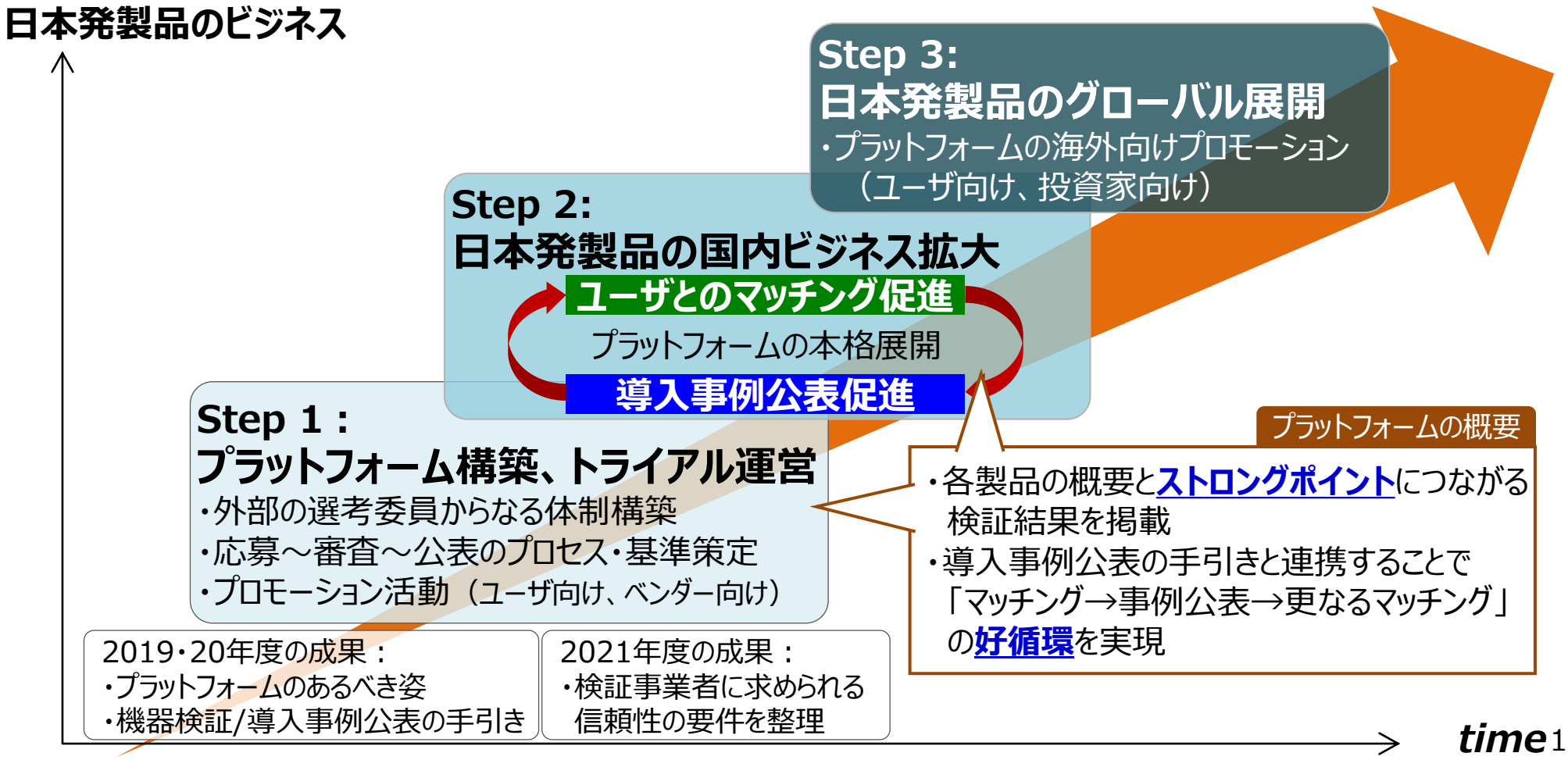
『Proven in Japan』の促進

- 「**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

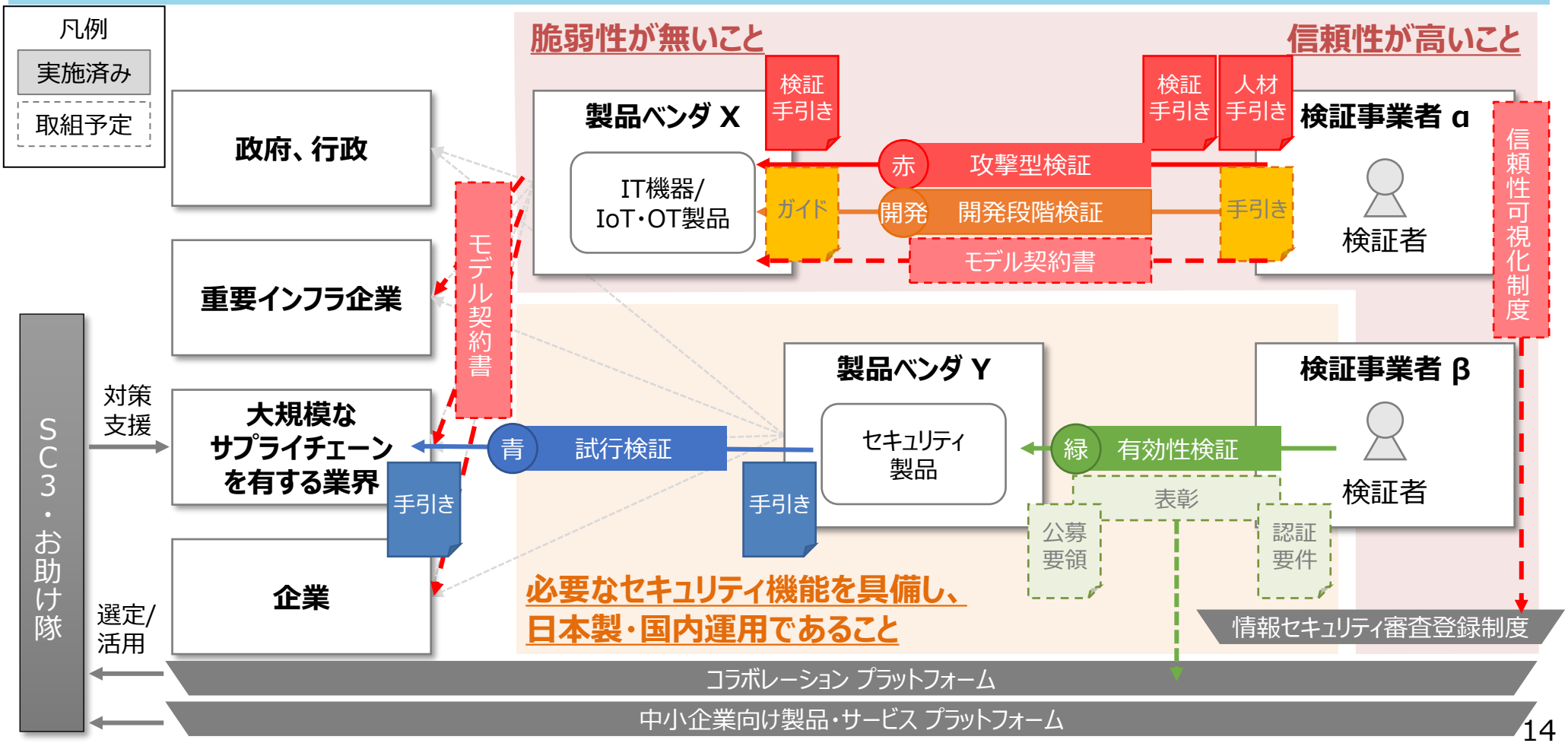
② IoT機器等の信頼性を高度に検証するハイレベル検証サービスの拡大

⇒今年度は新たに開発段階の製品・設計書等の検証も実施。



検証基盤の今後の方向性

- セキュリティ製品については、**市場が求める検証レベルを考慮した有効性検証**を実施し、その結果に基づき**表彰を行うためのスキームを構築**していく予定。
- 検証ビジネスについては、**検証事業者の信頼性を可視化する仕組みとして情報セキュリティ審査登録制度へ反映**等、検証事業者の信頼性向上に向けた取組を引き続き実施していく。
- **IPA、JNSA、中小機構の３者の連携**により、関連機関のアセットや既存プログラムを活用し、**セキュリティベンチャー企業がステージに応じて必要とする支援を、経営/技術/事業の３面から実施**する。



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

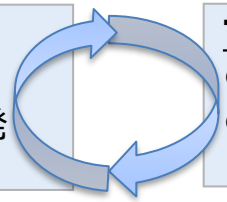
- 中小企業にとって身近な相談相手でもある**地域金融機関（地方銀行、第二地方銀行、信用金庫等）**や、**地域でのコミュニティ活動（地域SECUNITY）**を通じて、中小企業を含むサプライチェーン全体のサイバーセキュリティ対策の底上げを図る。
- 中小企業におけるセキュリティ対策を推進するために、**中小企業のターゲットごとに既存制度を活用したアプローチ、SC3参加団体や業界の取組に沿った制度普及**を図る。

ツール
- サイバーセキュリティ経営ガイドライン/中小企業向けガイドライン
- SECURITY ACTION
- サイバーセキュリティお助け隊

- 2021年度、サイバーセキュリティ体制構築・人材確保の手引きを改訂。
- 経営ガイドラインは、2022年度中にサイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)のコンセプトの反映やサプライチェーンの再整理など、所要の改訂を行う予定。

実態把握　（2021年度調査（経産省、IPA））
- 「対策の必要性を感じていない」企業が約２割で2016年度の前回調査から変化がないなど、中小企業のセキュリティ対策意識は依然として低い。
- 「SECURITY ACTION」や「サイバーセキュリティお助け隊」の認知度は1割以下。
- 取引先等へ要請を行う上で課題※や足かせがあると回答した企業は約３割。
  ※対策費用の負担、取引先等の意識・リテラシーの低さ、求めるべき事項・基準等が不明、下請法等の法令への抵触等
- 一方で、「費用・備品の一部負担」、「教育の実施」など支援が行われている事例もあり。
- 業界でガイドラインを策定し、サプライチェーンを構成する取引先のセキュリティ対策状況のセルフチェックに活用している事例もあり。

地域における普及啓発
- 地域金融機関を通じた普及啓発
- 地域SECUNITYによる人材育成・普及啓発
- 大学・高専と連携した地域人材育成



サプライチェーンを通じた取組促進
- SC3中小企業対策強化WG
- 業界団体や各企業における取組の横展開

【参考】自動車業界における取組

【米国】国家のサイバーセキュリティの改善に係る米国大統領令の署名

- 2021年5月12日、バイデン大統領は、連邦政府機関におけるサイバーセキュリティ改善に係る大統領令に署名。
- **官民での脅威情報の共有**、**ソフトウェアサプライチェーンセキュリティ対策**の強化、**ゼロトラストアーキテクチャ**への移行等を通じて、連邦政府機関のサイバーセキュリティ対応能力の向上を図っている。

本大統領令における主な指示事項

1 **官民の脅威情報共有における障害の除去** (Section 2)	● ITサービスプロバイダーが連邦政府と確実に脅威情報を共有できるようにしたうえで、特定のインシデント情報の共有を義務づける。
2 **連邦政府におけるより強力な標準の近代化と導入** (Section 3)	● FedRAMP改定等を通じて、連邦政府が安全なクラウド及びゼロトラストアーキテクチャに移行することを支援し、多要素認証と暗号化の導入を義務づける。
3 **ソフトウェア・サプライチェーンのセキュリティ向上** (Section 4)	● NISTを通じて**政府が調達するソフトウェアの開発に関するセキュリティ基準(安全な開発環境の確保や構成要素に関する詳細（SBOM）の開示等を含む)を確立**し、特に**重要なソフトウェアに対して一定の対策を義務づけ**る。 ● 商務省は、**既存のラベル表示などを参考にして、消費者向けの情報提供に関するパイロット制度を開始**する。
4 **サイバー安全審査委員会の創設** (Section 5)	● 国土安全保障省は、重大なインシデントが生じた際に政府と民間事業者が共同議長を務める「サイバー安全審査委員会」を設置し、サイバーセキュリティ向上に向けた具体的な提言を行う権限を与える。
5 **インシデント対応のための標準プレイブックの策定** (Section 6, 7)	● 国土安全保障省は、連邦政府機関によるインシデント対応のためのプレイブックを策定する。 ● 連邦政府機関は、エンドポイント検知・対応(EDR)イニシアチブを展開し、インシデントの検知、積極的なサイバーハンティング、有事対応をサポートする。
6 **調査及び修復能力の向上** (Section 8)	● 連邦政府機関に対してセキュリティイベントログの要件を設け、侵入を検知し、対処する組織能力の向上を支援する。

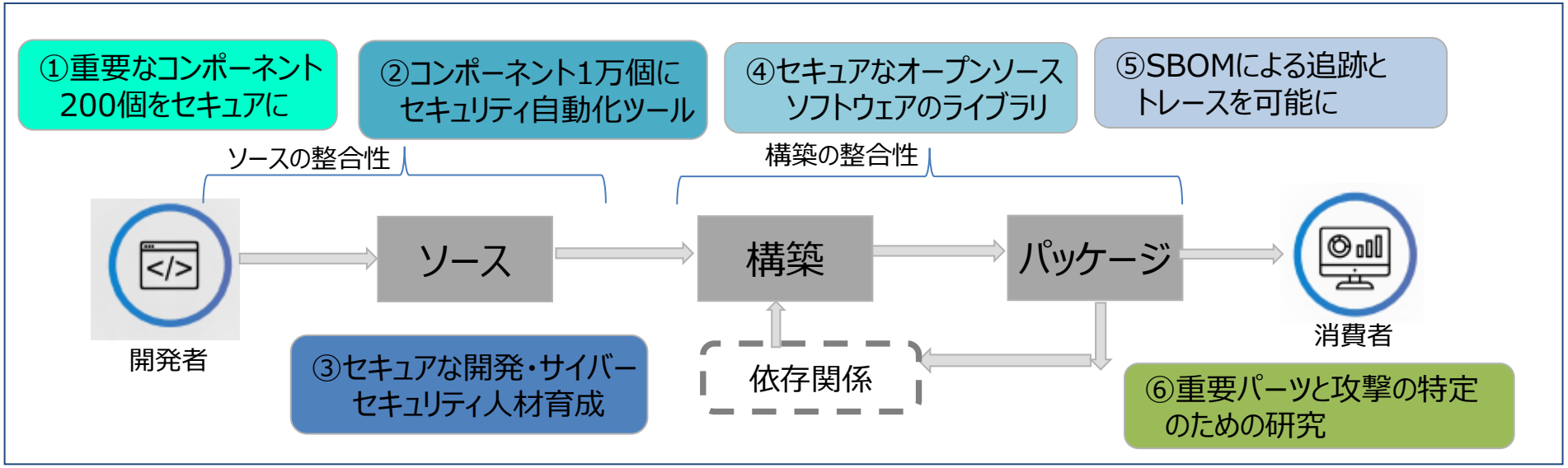
（出典）各種公開情報より作成

Linux FoundationによるOpenSSFの取組

- Linux Foundation（LF）は、SBOM開示等を含む米大統領令の署名以降、OpenSSFを立ち上げ、セキュリティ自動化ツールの開発・サイバーセキュリティ人材教育等を行っている。
- 2021年末のLog4j脆弱性発覚以降、米ホワイトハウスがセキュリティサミットを開催し、LFも参加。
- ソフトウェア脆弱性にグローバルに対応するため、日本企業の経営層（CTO/CIO等）の認識を得て、日本企業からOpenSSFへの積極的な参画を希望。春頃、東京でのセミナー開催を検討。

Linux Foundation
41カ国の2300以上の組織が加盟する非営利の技術コンソーシアム

Open SSF（Open Source Security Foundation）
SBOMフォーマットの標準（SPDX）をサプライチェーンにて適用すべく、日本を含め国際的な協調を目指し、以下のような仕組みを構想中。



IoT機器・システムのセキュリティに係る日米欧の制度化動向

- 民間部門を対象としたものとしては、米国では、「国家サイバーセキュリティの向上に関する大統領令」に基づく**消費者向けIoT製品のラベリングプログラムの開発**、欧州では、サイバーセキュリティ法に基づく**認証制度の策定及びNLF関連指令/規則による対策の規制化**が進められている。

	 **米国における検討状況** **(連邦政府で議論されているもの)**	 **EUにおける検討状況** **(EU単位で議論されているもの)**	 **日本政府の検討状況** **(主にIoT機器・システムの認定に係るもの)**
主な法令等	**国家サイバーセキュリティの向上に関する大統領令** (Executive Order 14028)	**サイバーセキュリティ法(CSA)** **NLF関連指令/規則** (例：機械規則案)	**電気通信事業法** 上記のほか、IT関連製品を対象にした認証制度として、ITセキュリティ評価及び認証制度(JISEC)等が存在する。
適用対象	**消費者向けのIoT製品** IoT製品には、IoT機器に加え、機器の利用に必要な製品コンポーネント(ネットワーク機器、モバイルアプリ等)を含み得る。	**製品分野等により異なる** 機械規則や無線指令等の各NLF関連指令/規則に規定が設けられており、現状は垂直的な規制が議論されている。	**インターネット等に接続する端末機器** ルータ、ウェブカメラ等が該当し、IPを使用しない機器やインターネット等に直接接続しない機器は含まれない。
セキュリティ基準	**消費者向けIoT製品のサイバーセキュリティ・ラベリングのための推奨基準** 現行案はNISTIR 8259シリーズをベースに策定されている。	**製品分野等により異なる** 機械規則や無線指令等の各NLF関連指令/規則に規定が設けられており、現状は垂直的な規制が議論されている。	**端末設備等規則** 必ずしも機器・システム等の認定に関わらないものとしては、IoTセキュリティガイドライン、CPSF/IoT-SSF等が存在する。
事業者の義務等	**現状では必ずしも議論されていない** NISTは、政府主導の認証・ラベリング制度ではなく、今後制度を開発する主体が参照するものを志向している。	**NLF関連指令/規則を通じて義務化される見込み**	**技術基準適合認定が求められる場合等を除けば、必ずしも対策は義務とされていない。**
今後の予定	• 2022年5月12日までに、NISTは、上記検討に関する総括報告書を発行する予定。 • 上記報告書の公開後、基準に基づく認証制度の検討が推進される見込み。	• EUCC等、CSAに基づく認証制度の具体化が進む見込み。 • 草案が公開されているNLF関連指令/規則は、順次欧州議会等で議論が進められる。 • 2022年下期に、水平的なセキュリティ基準の確立を志向する「サイバーレジリエンス法」公表を予定。	• IoTを対象にした具体的な認証・ラベリング等の議論はなされていない。

サイバー脅威の増加を踏まえた、攻めのサイバーセキュリティ強化へ

昨今の情勢を踏まえたサイバーセキュリティ対策の強化

- **昨今の情勢を踏まえたサイバー攻撃事案の潜在的なリスクの高まり**
- **産業界へのメッセージ（ランサムウェアやEmotetへの対応を含めて）**

Cyber New Normalにおける６つの処方箋 （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 サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化
② ソフトウェアの脆弱性対応強化（脆弱性情報の共有、SBOM）
③ 医療分野での対応（SBOM、お助け隊）
④ 「開発のための投資」から「検証のための投資」へのシフト
⑤ 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
⑥ Like-mindedの関係強化（国際情勢）

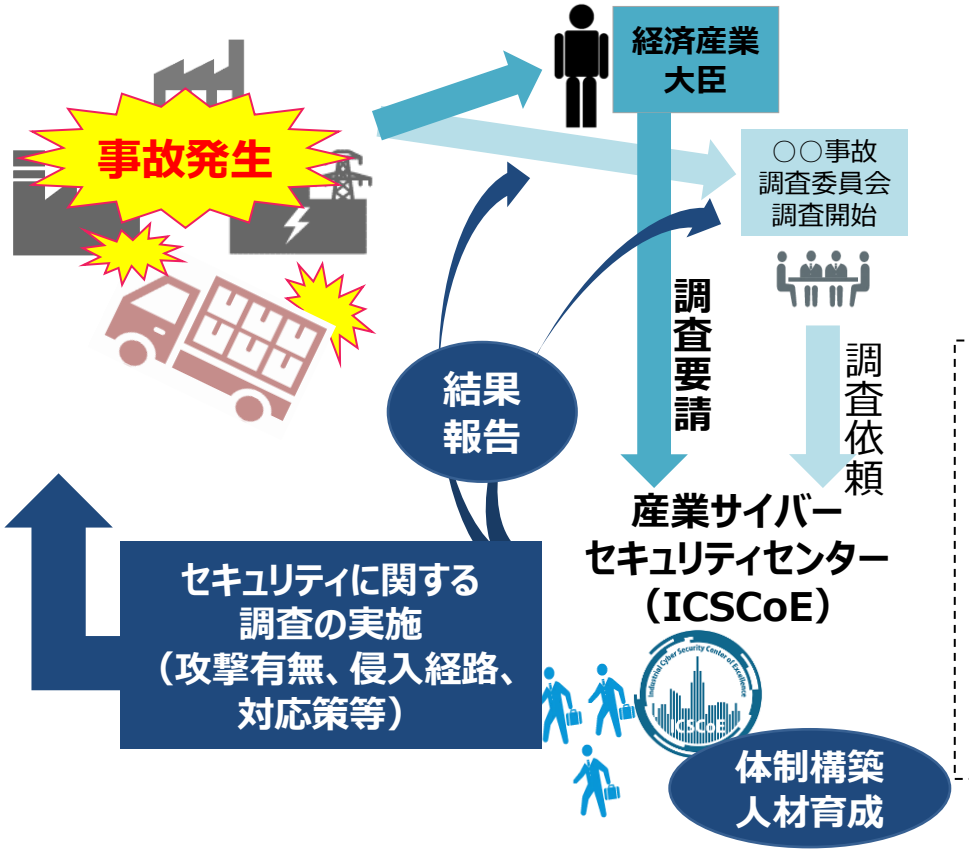
国としての対処能力の強化 （継続）

- **国としての対処能力の構築**
  - サイバーインシデントに係る事故調査機能の構築
  - サイバー攻撃被害に係る情報の共有・公表のあり方検討

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

- サイバー攻撃の起点が拡散し、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ることから、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」）**。
- IPA産業サイバーセキュリティセンター（ICSCoE）は、「サイバー事故調」機能を整備するため、**2022年度に、重要インフラ２分野においてパイロット・実証事業を実施。経済産業大臣からの調査要請**が規定される**高圧ガス保安法等の一部を改正する法律案の施行（2023年12月頃を想定）にあわせて、機能整備**の準備を推進。

サイバーインシデントに係る事故調査のイメージ



取組の概要

＜令和４年度＞パイロット・実証

- **サイバー事故調機能のあり方は産業分野により様々**であるとの仮説を基に、令和4年度は、令和３年度の成果を活用しつつ、**２分野でパイロット・実証事業を実施**。
- 具体的には、重要インフラである**電力等産業保安分野**から事業者の協力を得て、現在行われている**通常の事故調査と将来的なサイバーインシデントに係る事故調査の円滑な連携に向けた課題の洗い出しや連携方策**に係る検討を実施する。

＜参考＞高圧ガス保安法改正案　（※3月4日閣議決定）

（調査の要請）

第60条の2　経済産業大臣は、認定高度保安実施者その他の保安の確保上特に重要な者として経済産業省令で定める者において保安に係るサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）に関する重大な事態が生じ、又は生じた疑いがある場合において、必要があると認めるときは、独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる。

（ガス事業法、電気事業法の改正案にも同趣旨の記載。）

サイバー攻撃被害に係る情報の共有・公表の在り方について

- サイバー攻撃被害を受けた組織が、サイバーセキュリティ関係組織等と攻撃被害に係る情報を共有することは、被害組織自身にとっても、社会全体にとっても非常に有益。
- サイバー攻撃被害を受けた組織の立場にも配慮しつつ、攻撃被害に係る情報を取り扱う際の実務上の参考となるガイダンス示し、これを普及していくことで、円滑かつ効果的な情報共有を促進する。

● どんな情報を？

コンテクスト情報

様々な種類・性質の情報が存在

- 被害組織名
- 業種／規模
- 被害内容
- タイムライン（対応状況）
- タイムライン（技術情報）
- 攻撃主体に関する情報
- 攻撃対象システム
- 対策状況
- 脆弱性
- その他TTP
- マルウェア
- 通信先

技術情報

被害組織

CSIRT
システム運用部門

法務・リスク管理・
企画・渉外・広報部門

● どのタイミングで？

サイバー攻撃への対処の時系列

● どんな主体と？

専門組織

情報共有活動

所管省庁等

警察

各種ステークホルダ

本 編 参 考

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

第４回：令和2年　　4月17日　開催
（電話開催）

産業界へのメッセージを発信

第５回：令和2年　　6月30日　開催

サイバーセキュリティ強化運動の展開

第６回：令和３年　　４月２日　開催

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

WG１
（制度・技術・標準化）

１．サプライチェーン強化パッケージ

WG２
（経営・人材・国際）

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

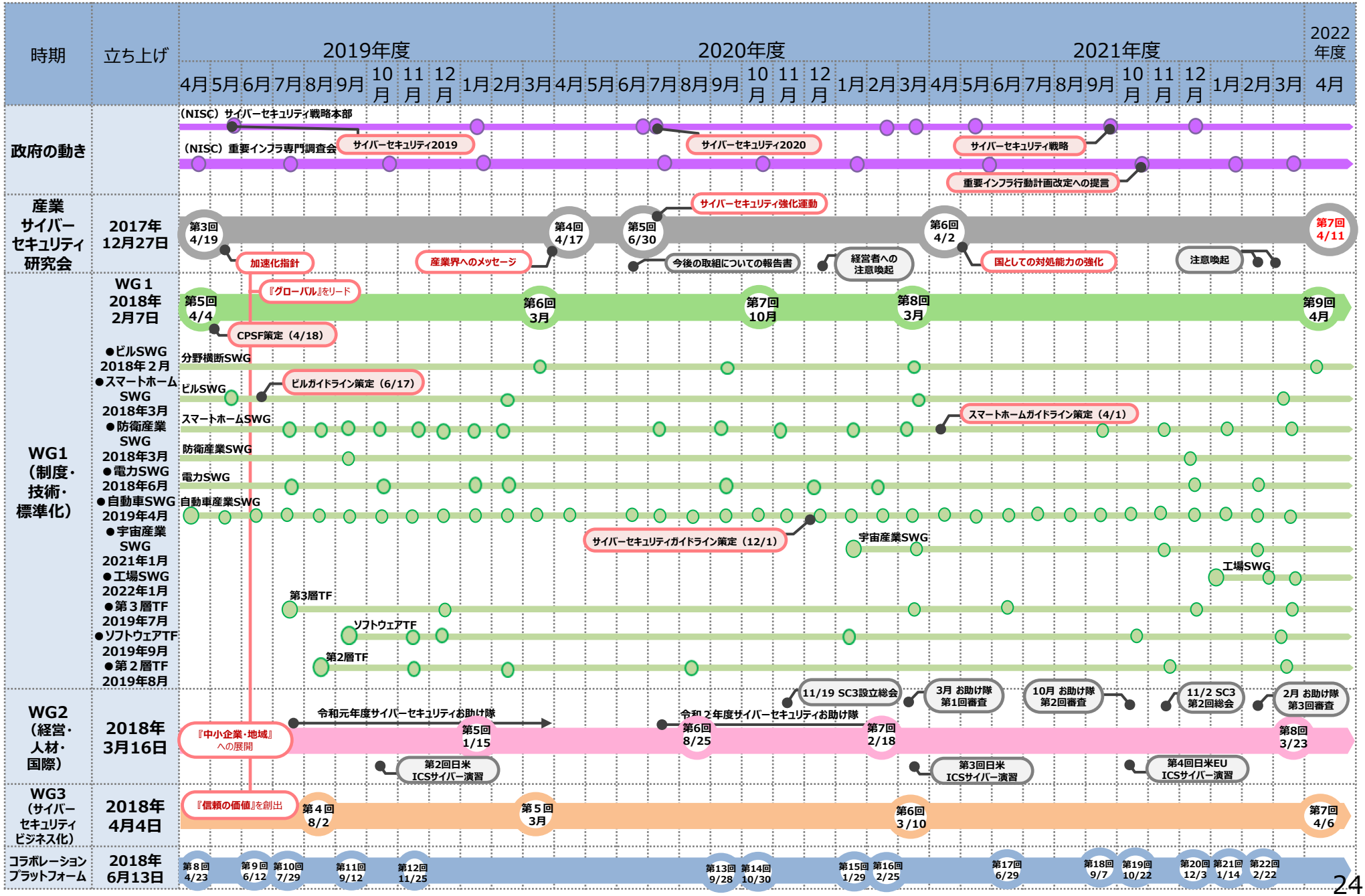
WG３
(サイバーセキュリティビジネス化)

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会議の実績

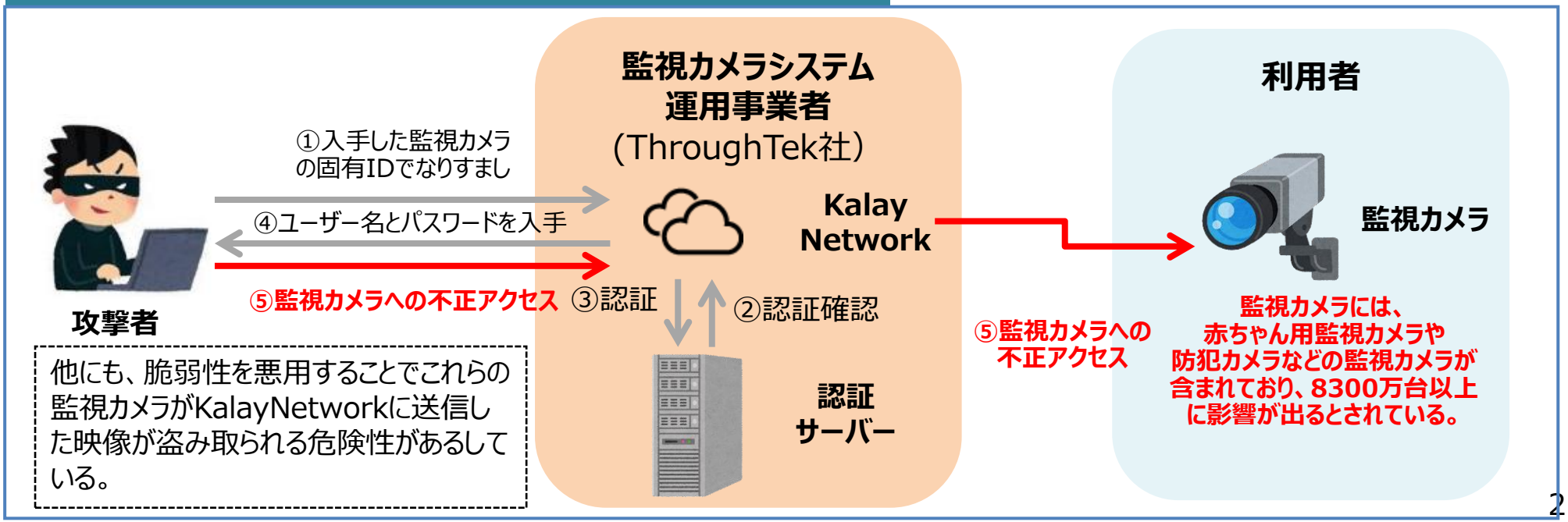


IoT機器への攻撃

- 2021年8月、Mandiantは監視カメラを含む8300万台以上のIoT機器が影響を受ける脆弱性「CVE-2021-28372」を発表。KalayNetworkで不適切なアクセス制御がなされる可能性があり、本脆弱性によって、ネットワークカメラの映像を盗み取られたり、家庭内の機器に不正アクセスされる可能性があるとされている。
- 監視カメラに限らず、無停電電源装置（ＵＰＳ）などの制御装置のIoT化により、インターネットに接続可能な機器の増加が攻撃機会の拡大につながっていることから、インターネットから直接の接続を避ける、多要素認証を導入する、デフォルトのID/PWを使用せず複雑なPWを適用することなどの対応が必要。

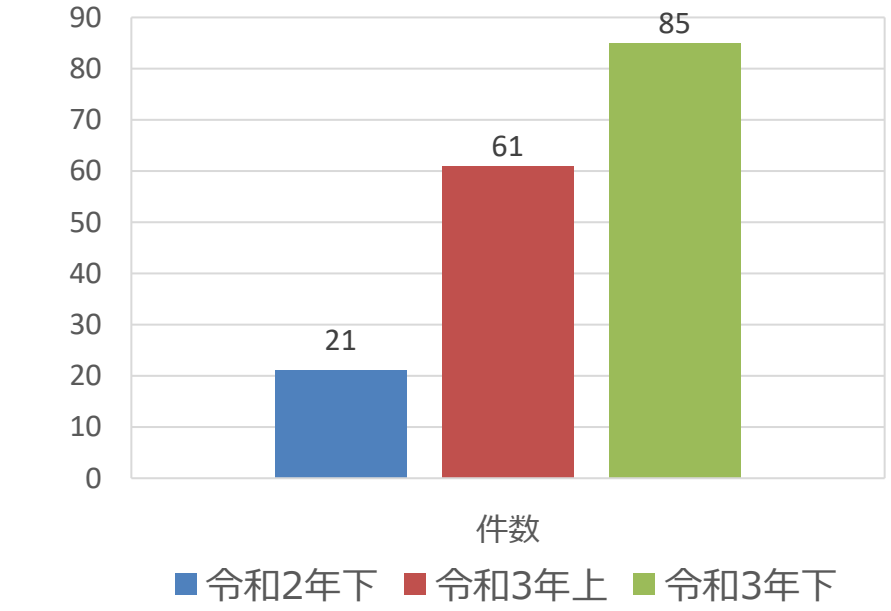
※2022年3月、CISAが無停電電源装置（UPS)への攻撃の回避手法を公開。
URL: https://www.cisa.gov/uscert/ncas/current-activity/2022/03/29/mitigating-attacks-against-uninterruptable-power-supply-devices

攻撃者が監視カメラに不正アクセスするイメージ

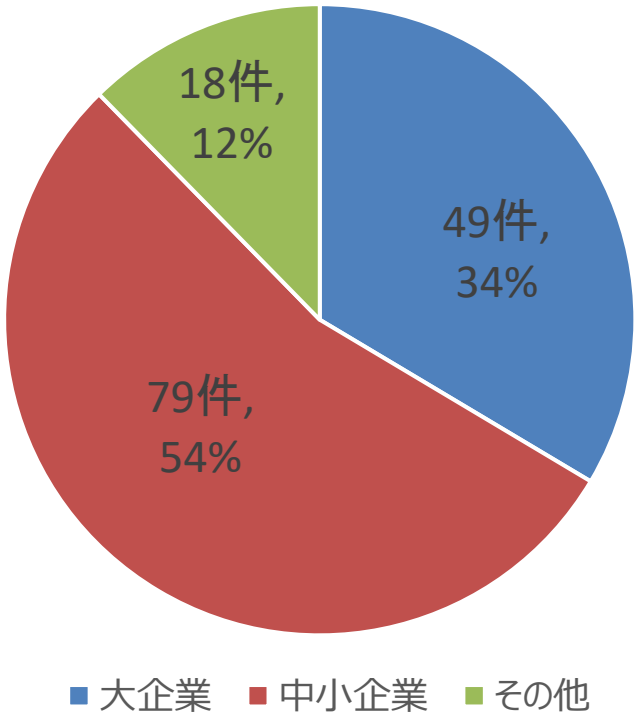


中小企業のランサムウェア被害の増加

- 企業・団体等におけるランサムウェア被害として、令和3年に全国の都道府県警察から警察庁に報告があった件数は146件であり、前年と比較可能な**７～12月だけで４倍と大幅に増加**。
- 被害件数(146件)の内訳は、大企業が49件（34%）に対して、**中小企業は79件（54%）と過半数超**。



企業・団体等におけるランサムウェア被害の報告件数の推移



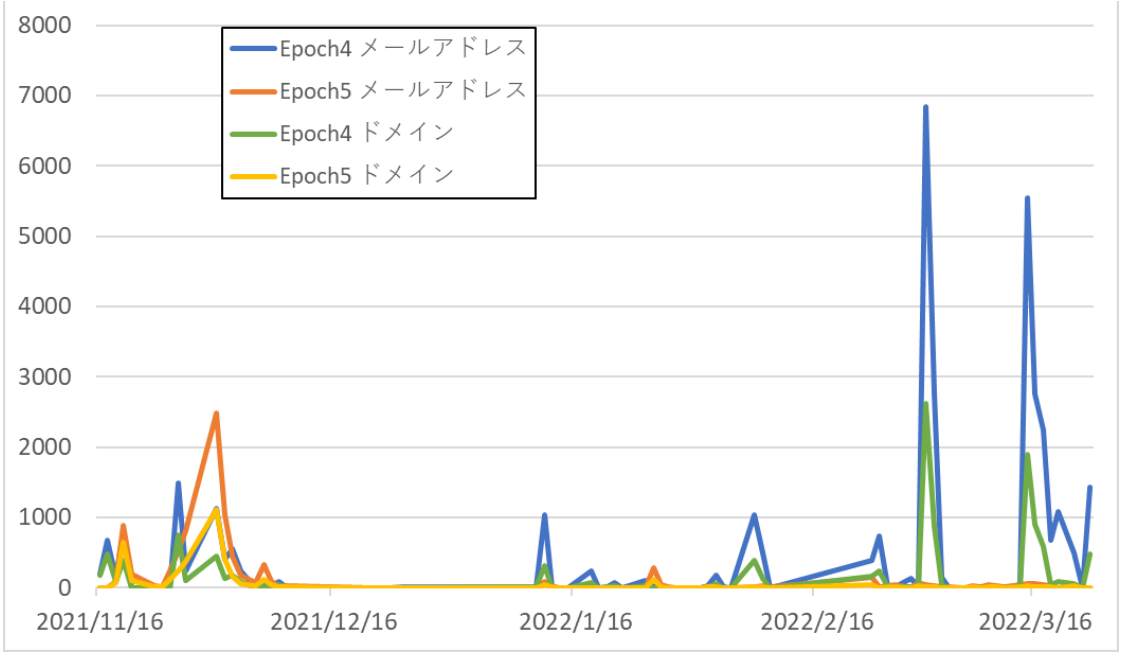
ランサムウェア被害の被害企業・団体等の規模別報告件数
（令和３年）

警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について（令和4年2月10日）」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

マルウェアEmotetの感染再拡大

- 2021年11月後半より活動の再開が確認されているマルウェアEmotetの感染が2022年2月の第一週より急速に拡大。
- IPA（2021年11月～）及びJCERT/CC（2022年2月～）から注意喚起等を実施。
  - 正規メールへの返信を装うなどの手口を解説し、身に覚えのないメールの添付ファイルは開かないよう注意喚起
  - 感染が疑われる場合のチェックツール「EmoCheck」を公開

Emotet感染メールアドレス/ドメイン数（.jp、ボットネット別）



出典：JPCERT/CC

「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」

●昨今の情勢を踏まえると**サイバー攻撃事案の潜在的なリスクは高まっている。**
●**組織幹部のリーダーシップ**の下、サイバー攻撃の脅威に対する認識を深め、対策の強化を。
●**不審な動きを把握した場合**は、早期対処のために速やかに経済産業省やセキュリティ関係機関（IPA、JPCERTなど）に情報提供、警察にも相談を。

１．リスク低減のための措置

〇本人認証の強化
（パスワードが単純でないか、アクセス権限の確認、多要素認証の利用、不要なアカウントの削除等）
〇IoT 機器を含む情報資産の保有状況の把握
特にVPN 装置等へのセキュリティパッチ（最新のファームウェアや更新プログラム等）の迅速な適用
〇組織内での基本の徹底
（添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等）

２．インシデントの早期検知

〇サーバ等における各種ログの確認
〇通信の監視・分析やアクセスコントロールの再点検

３．インシデント発生時の適切な対処・回復

〇データ消失等に備えて、データのバックアップの実施及び復旧手順の確認
〇インシデント発生時の対応確認
（インシデントを認知した際の対処手順、対外応答や社内連絡体制等）
➢ 侵入型ランサムウェア攻撃を受けたら読むFAQ　https://www.jpcert.or.jp/magazine/security/ransom-faq.html

経済産業省「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について　（2022年2月23日）」 https://www.meti.go.jp/press/2021/02/20220221003/20220221003.html
経済産業省等７省庁「サイバーセキュリティ対策の強化について（2022年3月1日）」 https://www.meti.go.jp/press/2021/03/20220301007/20220301007.html
経済産業省等４省庁「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（2022年3月24日）」https://www.meti.go.jp/press/2021/03/20220324008/20220324008.html

分野横断SWGにおける
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化

- **分野横断の共通課題**を検討するために、**3つのタスクフォース（TF）**を設置。

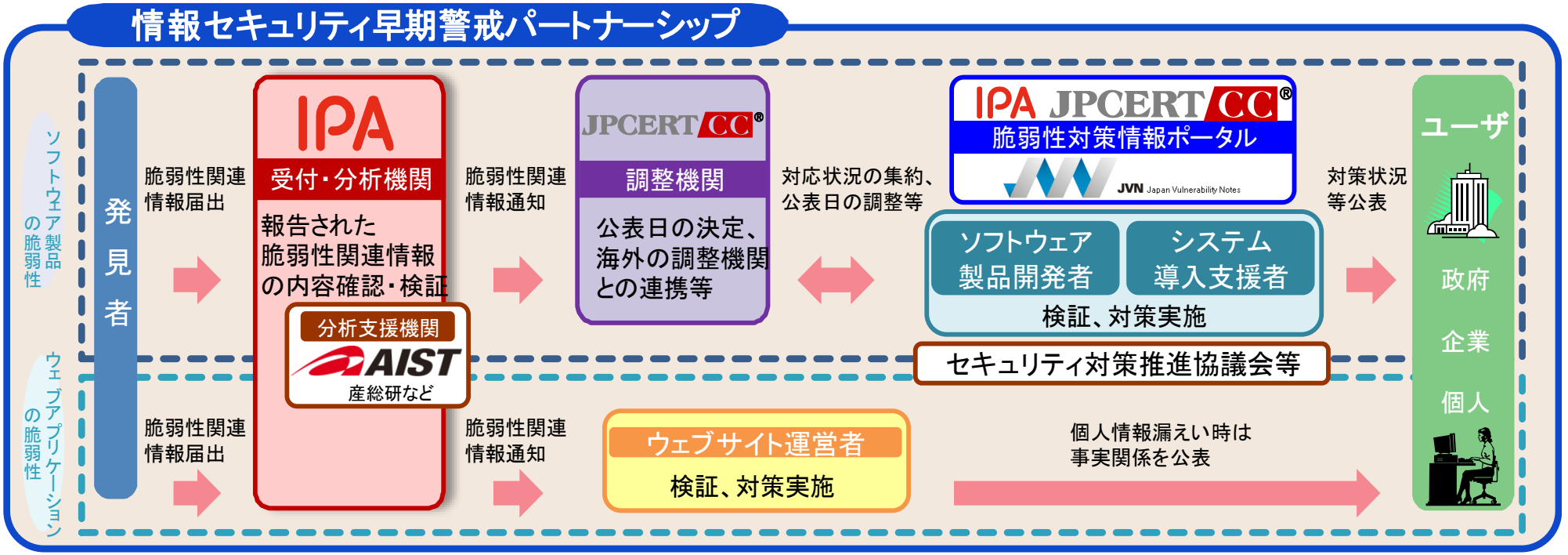
産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

分野横断SWG

『第3層』TF： 『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース	• 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。 • **「協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ」を公開**（2022年4月）。 • 包括的な視点でアーキテクチャを整理している**行政分野（DFFT等）での取組における適用・応用を目指す**。
ソフトウェアTF： サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース	• 「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公開（2021年4月）。**追補版の公開を予定（2022年4月）** • **SBOM活用促進に向けた実証事業（PoC）を実施**。令和3年度の実証結果を踏まえて、令和4年度以降、実証の対象を拡大し、活用／取引モデルの検討等を進める。
『第2層』TF： 『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース	• フィジカル空間とサイバー空間のつながりの信頼性の確保するための**「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開（2020年11月）**。 • **新たに６つのユースケースを公開予定（2022年4月）。** • 今後、ユースケースを活用した、**IoT-SSFの普及啓発と自立的な活用の促進**に向けた取組を進めていく。

ソフトウェアの脆弱性対応強化

- 脆弱性情報への対応を促進するため、脆弱性情報の共有制度の改善を進める。
  - Ø 2022年度は、脆弱性対策情報データベース JVN iPediaの改定を予定。脅威インテリジェンス情報の共有規格（STIX/TAXII）での情報提供を可能とするなど、使い勝手の改善を図る。
  - Ø JVNにおける脆弱性の悪用(いわゆる「in the wild」）に関する情報の取り扱いについても検討。



※IPA：独立行政法人情報処理推進機構、JPCERT/CC：一般社団法人 JPCERTコーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

SBOM実証のシナリオと結果

- 実証では、従来の部品管理を含む4つのシナリオに関し、SBOM等の作成、活用に係る工数・費用を計測。
- 今回の比較条件では、SBOMは初期工数（ツール導入等の環境整備、学習等）が大きいが、運用工数（SBOM作成、活用）は従来の手作業部品管理に比べ小さい結果となり、**管理対象のソフトウェア部品が多いほど、SBOM導入効果が大きくなると想定**。
- ツールによる脆弱性特定の自動化により、**脆弱性発表から特定までのリードタイム短縮と工数削減**に繋がる。

実証のシナリオ

①従来の部品管理(独自形式)

Excelの独自形式で手作業管理。
脆弱性やライセンスの情報は手作業で検索。

②SBOM(手動作成)

ツールのフォーマットに合わせて手作業でSBOMを作成。
脆弱性やライセンスの特定はそれぞれOSSの無償ツールで実施。

③SBOM(無償ツール)

OSSの無償ツールによりSBOMを作成。
脆弱性やライセンスの特定はそれぞれOSSの無償ツールで実施。

④SBOM(有償ツール)

有償ツールにより、SBOM作成、脆弱性管理、ライセンス管理をシームレスに実施。

実証のまとめ

SBOMのメリット等

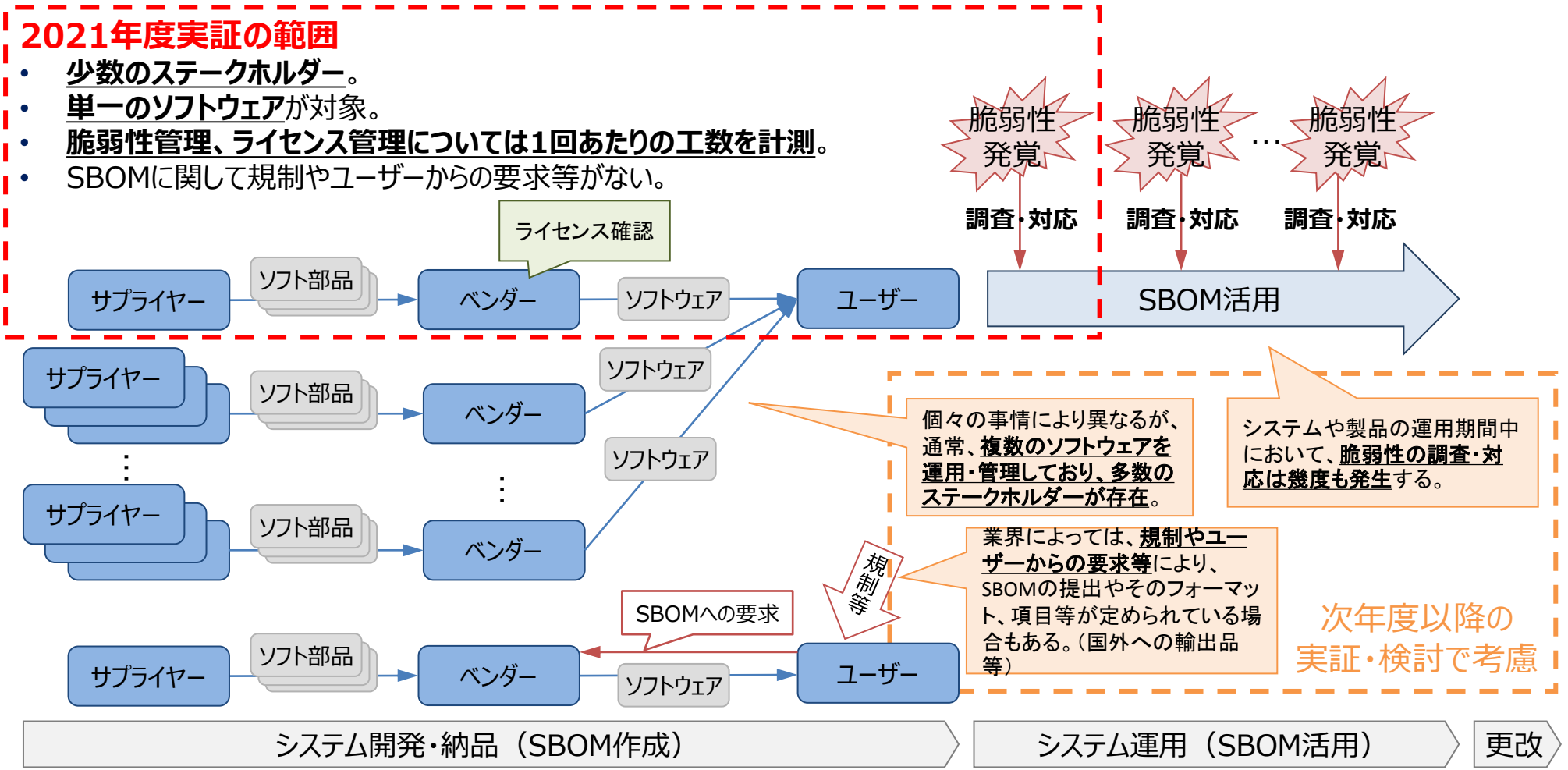
- **SBOMは導入するための初期工数（ツール導入等の環境整備や使用方法習得のための学習等）が大きいが、ツールを活用することで運用（SBOM作成、活用）工数は小さく**なった。
- **SBOMツールにより脆弱性発表から特定までのリードタイムを短縮可能**（手作業の場合は脆弱性特定業務の頻度に依存）。
- 有償ツールでは、**OSSの依存関係を解析し、構成ファイルから特定できなかった、OSSによる他のOSSの再利用も検出**（**但し検知結果の精査工数が大**）。

確認した課題

- 無償ツールはドキュメントやノウハウが不足。機能・精度面も十分とはいえない。
  - **ツールの使用方法、留意事項等のノウハウを整理した日本語ドキュメント整備のような対応**が考えられる他、**ツール自体の精度、機能の向上に期待**。
- 開発者以外がSBOMを作成する場合、ツールにより検出されるOSSの再利用やソースコード改変部品などの精査に係る工数が大きくなる、もしくは精査が困難。開発者自身が認識していない部品が検出された場合の管理責任が曖昧になり得る。
  - **開発者（ベンダーやサプライヤー）自身がソフトウェア部品を特定し、標準的なSBOMフォーマットで共有することが、サプライチェーン全体における部品管理の効率化や責任の明確化につながる**と考えられる。

（参考）2021年度の実証の範囲

- **SBOMの作成・活用に関しては様々なパターン**が考えられる。
- **初年度である2021年度実証は、少数のステークホルダーが関係するソフトウェアを対象**にSBOMを作成して脆弱性およびライセンス管理へ活用するケースについて、効果とコストを比較。



【米国】大統領令におけるソフトウェア・サプライチェーンに関するタイムライン

- 大統領令では、**ソフトウェア・サプライチェーンの確保に向け、NISTが中心となりガイドラインを策定する**旨を指示しており、この**ガイドラインには製品購入者に対するSBOM提供に関する項目も含まれる**。
- また、NISTに対して、NTIAと連携して**SBOMの最小要素を公表すること**を指示している。
- 将来的には、公開されたソフトウェア・サプライチェーンに関するガイダンスの要求事項に基づき、**連邦政府のソフトウェア調達に関するFAR（連邦調達規則）が改正される予定**である。

2021.5.12	大統領令の署名
2021.6.25	「重要なソフトウェア」の定義の公表 NIST DoD DHS OMB
2021.7.9	「重要なソフトウェア」のセキュリティ対策に係るガイダンスの公開 NIST DHS OMB
	ソフトウェア検証の最低基準に関するガイドラインの公表 NIST DHS
2021.7.12	SBOMの最小要素の公表 NIST NTIA
2021.7.25まで	「重要なソフトウェア」の定義を満たすソフトウェア製品のカテゴリを特定し、政府機関に通知 DHS NIST
2021.8.10	NISTが公開した重要なソフトウェアのセキュリティ対策に関するガイダンスを、各省庁が遵守することを求めるための措置を講じる OMB
2021.10.28	ソフトウェアサプライチェーンのセキュリティを強化するための予備的なガイドラインの公表 NIST
2022.2.4	ソフトウェアサプライチェーンのセキュリティを強化するための指針を示すガイダンスの公表 NIST
2022.3.8まで	大統領令以降に調達されたソフトウェアに関して、各省庁がNISTによる指針を遵守するための適切な措置を講じる OMB
2022.5.8まで	「予備的なガイダンス」の定期的な見直し・更新のための手順を含む追加のガイドラインの公表 NIST
2022.5.12まで	FAR審議会に対し、各省庁が購入可能なソフトウェアサプライヤーに対する上記ガイダンスに基づく要求事項の遵守と、遵守の証明を義務付ける契約文言を勧告 DHS
(現状、期限の指定なし)	⇨ DHSによる勧告の検討、FARの改正 FAR審議会
	FAR改正に伴い、FARの要件を満たさないソフトウェア製品を調達契約から削除 各省庁

出所）White House, “Executive Order on Improving the Nation’s Cybersecurity” https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ , NIST, “Executive Order” https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/executive-order

【日本】OpenChain Japan WGの取組

- OpenChain Japan WGは、OpenChainプロジェクトに参加する国内企業が日本語で議論する場を作ることを目的に、2017年に設立。（第3回TF資料4参照）
- 現在、**OpenChainに関する文書やSPDX仕様の翻訳、OSSの管理や透明性向上に向けたOSSマネジメントに関するスキル標準作成等の活動を実施中**。

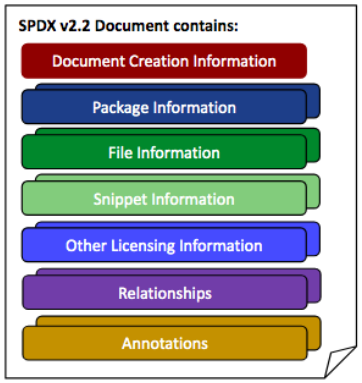
OpenChain文書やSPDX仕様の翻訳

- **関連する英語文書の日本語翻訳の取組を有志にて実施中**。
- 現在対応している文書は下記のとおり。
  - OpenChain ISO/IEC 5230 Security Assurance Reference Guide（OpenChain（ISO/IEC 5230:2020）の使用方法のガイダンス。）
  - SPDX2.2（ISO/IEC 5962:2021）仕様　※翻訳作業中（仕様策定において、OpenChain Japan WGはSPDX Lightを作成。）
- **翻訳後は順次公開**予定。


OPENCHAIN　OpenChain セキュリティアシュアランスリファレンスガイド 1.0

目次

OpenChain ISO/IEC 5230 – Security Assurance Reference Guide（日本語版）：
https://qiita.com/kida_oss/items/bf6a9d005dd1b50b5875



SPDX仕様（英語版）：https://spdx.dev/specifications/

OSSマネジメントに関するスキル標準作成

- システム開発におけるOSS利用が増え、OSS管理業務が複雑化、**使用OSSやライセンス・脆弱性の把握が困難**に。
- OSS に関わる人材育成や役割分担のため、**OSSライセンスコンプライアンス・脆弱性対応業務等に関するスキル標準の作成**を検討。
- 第1歩として「スキル標準フレームワーク（全体マップ）及び職種別業務」を作成。
- **既存のITSS+等との整合性も図りつつ作成を継続**予定。

		業務		職種別業務									
				エンジニア		調達・営業		情報セキュリティ		法務・知財		マネジメント	
業務フェーズ	企画	1)コミュニティ投資	13) ガバナンス 14) 教育 15) コントリビューション	1)	13) 14) 15)	4)	13) 14) 15)	2)	13) 14) 15)	1)	13) 14) 15)	1)	13) 14) 15)
		2)OSS活用検討		2)						2)		2)	
		3)特許調査		3)						3)			
		4)調達契約策定		4)						4)			
	開発	5)OSS活用		5)		7)		8)		7)		8)	
		6)SBOM作成		6)						8)		9)	
		7)サプライヤ管理		7)						9)		10)	
		8)活用可否判断		8)						10)			
		9)ライセンス対応		9)									
		10)OSS化検討		10)									
	保守	11)脆弱性対応		11)		12)		11)		12)			
		12)ユーザ対応		12)									

スキル標準フレームワーク（全体マップ）及び職種別業務
（企画～保守における業務と各職種が行うべき業務をマッピング）

OpenChain Japan WG : https://openchain-project.github.io/OpenChain-JWG/index.html

サイバーセキュリティ人材施策の全体像

- 昨年度は、「セキュリティ体制構築・人材確保の手引き」の改訂を行うとともに、セキュリティ人材育成の既存施策を進めつつ、特に、セキュリティを本務としない者が自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につける「プラス・セキュリティ」の取組を推進するため、SC3での検討や地域での具体的な取組を推進。

取組の全体像

セキュリティ対策を進めるための体制・人材の考え方

セキュリティ体制構築・人材確保の手引き（「サイバーセキュリティ経営ガイドライン」付録F）

セキュリティ人材の育成

- ICSCoE中核人材育成プログラム
- 情報処理安全確保支援士
- セキュリティキャンプ

プラス・セキュリティの普及

- SC3産学官連携WGでのプラス・セキュリティ具体化
- NISCにおけるモデルカリキュラム策定
- 地域SECUNITYにおける人材育成

デジタル人材育成プラットフォームにおけるスキル標準の整理・教育コンテンツ・実践型教育

大学・高専等と産業界の連携

今後の方向性

- 手引きの普及による各企業での体制構築の促進と各種セキュリティ人材育成施策を引き続き実施するとともに、プラス・セキュリティの取組を普及させるため、SC3産学官連携WG、デジタル人材育成プラットフォーム、各地域における産学官連携の取組（地域SECUNITY）との連携による取組の具体化・拡大を進めていく。

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:**「基本行動指針（インシデント発生時の共有・報告・公表）」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。
- **参加者:** 経済団体、業種別業界団体　等（2022年3末時点で96団体含む175会員）
- **設立日:** 2020年11月1日（設立総会：2020年11月19日）

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）

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

2021年11月
第2回総会

運営委員会

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

中小企業対策強化WG
中小企業のサイバーセキュリティ対策強化に向けた課題や取組の検討・推進

産学官連携WG
産学官連携によるセキュリティ関連の人材育成・活躍推進等について検討・推進

・・・・・

攻撃動向分析・対策WG
経営層が認識すべきサイバー攻撃関連動向や対策のポイントを産業横断で発信

地域SECUNITY形成促進WG
地域SECUNITYの取組を推進するための地域間の情報共有や共通課題の解決に向けた取組の検討・推進

地域SECUNITY形成促進の全体像

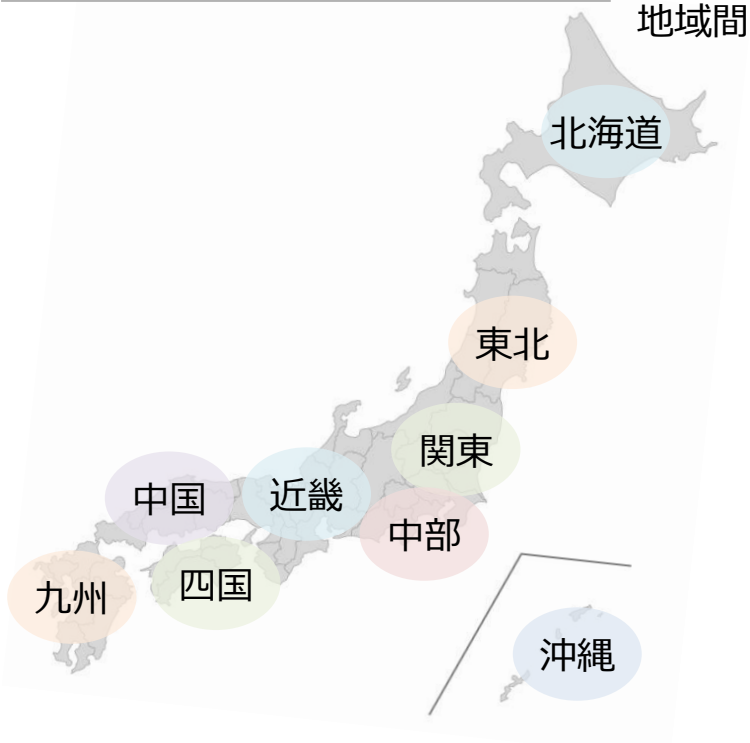
- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ（「地域SECUNITY」）の形成を全国において推進。
- 各地の取組をさらに促進するため、地域間の情報共有や、共通課題の解決に向けた取組の検討／推進を行うため、**SC3において地域SECUNITY形成促進WGが設立。**

①各地域での活動

各地域においてSECUNITYの活動を推進

他地域への事例共有

WSで得た知見の活用
地域間の連携創出



②活動の横展開

- **SC3地域SECUNITY形成促進WGワークショップ（WS）の開催**
- **地域SECUNITY形成・運営のためのプラクティス集の拡充**
- **地域SECUINITYリストの作成**

【活動の中で出てきた課題の例】

SECUNITYとしての地域の人材不足にどう対応するか。

活動の継続性をどう確保するか。
活動の裾野をどのように広げるか。

他のSECUNITYと連携しつつ、地域の特性にあったコミュニティの形成を目指すには

?

サイバーセキュリティお助け隊サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。2022年３月時点で12サービスが登録。サービス審査登録制度の運営とともに、中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

- EDR・UTMによる異常監視
- 緊急時の対応支援・駆け付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

中小企業でも導入・維持できる価格でワンパッケージで提供

サイバーセキュリティお助け隊サービスウェブページ（11/10公開）
＜https://www.ipa.go.jp/security/otasuketai-pr/＞

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マーク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）

サイバーセキュリティお助け隊

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。

（参考）サイバーセキュリティお助け隊サービス　登録サービスリスト

- 全国各地域の中小企業にとって選択・利用可能な「サイバーセキュリティお助け隊サービス」登録サービスリスト
（第１回審査：5件、第２回審査：４件、第３回審査：３件）

【登録サービスリスト】

	サービス名	事業者名	対象地域
1	**商工会議所サイバーセキュリティお助け隊サービス**	大阪商工会議所	近畿（2府5県）全域、近畿に本社を置く中京圏都市部・福岡県北部の支社・工場、首都圏、長野県　等
2	**防検サイバー**	ＭＳ＆ＡＤインターリスク総研株式会社	全国
3	**PCセキュリティみまもりパック**	株式会社ＰＦＵ	全国
4	**EDR運用監視サービス「ミハルとマモル」**	株式会社デジタルハーツ	全国
5	**SOMPO SHERIFF（標準プラン）**	ＳＯＭＰＯリスクマネジメント株式会社	全国
6	**ランサムガード**	株式会社アイティフォー	関東地方、中部地方、関西地方、九州地方、沖縄県
7	**オフィスSOCおうちSOC**	富士ソフト株式会社	東北地方（岩手）を中心　※全国展開を計画中
8	**セキュリティ見守りサービス「＆セキュリティ＋」**	株式会社BCC	全国
9	**CBM ネットワーク監視サービス**	中部事務機株式会社	岐阜県（飛騨地方除く）・愛知県（三河地方除く）
10	**中部電力ミライズ サイバー対策支援サービス**	中部電力ミライズ株式会社	愛知県・岐阜県・三重県・長野県・静岡県（富士川以西）
11	**ＣＳＰサイバーガード**	セントラル警備保障株式会社	東京・神奈川・千葉・埼玉　※順次全国に拡大予定
12	**PCお助けパック　PC定期侵害調査プラン**	沖電グローバルシステムズ株式会社	沖縄県を中心　※全国展開を計画中

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

⇒今年度は新たに開発段階の製品・設計書等の検証も実施。

1.セキュリティ製品の有効性検証

ベンチャー等のセキュリティ製品

有効性検証

検証環境

2.実環境における試行検証

ベンチャー等

お試し製品提供と検証

実環境

民間事業者等のオフィス

3.攻撃型を含めたハイレベルな検証サービス

検証サービス事業者

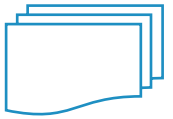
攻撃型検証等

IoT機器・システム等

4.セキュリティ・バイ・デザインを実現する開発段階検証

検証サービス事業者

開発段階検証



設計書・ソースコード等

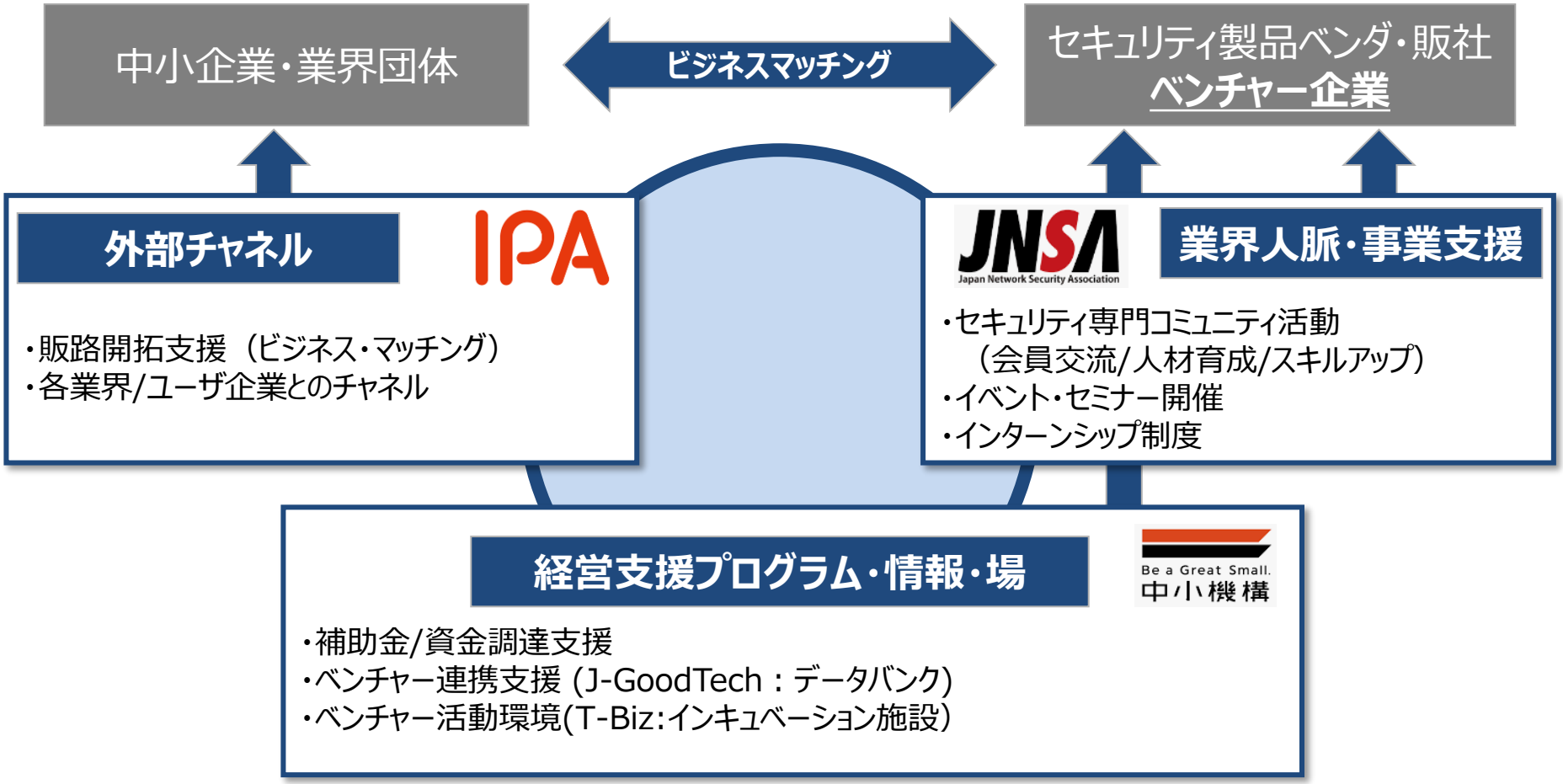
New

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

実現すべきエコシステム（イメージ）

- 今後、関連機関のアセットや既存プログラムを活用し、セキュリティベンチャー企業がステージに応じて必要とする支援を、経営/技術/事業の３面から実施する。
- また、IPAによる顧客接点・業界チャネルを活用し、販路開拓・事業化支援を実施する。



国際連携の全体像

- サイバーセキュリティ政策については、国際的な動向も踏まえつつ、関係国と連携して検討・推進することが重要。引き続き、関係国の官民と連携した情報収集・政策検討や、日本企業の多くが事業を展開するインド太平洋地域におけるキャパビルなどの国際貢献を実施していく。

取組の全体像

①インド太平洋向け演習

- 日米EU産業制御システムサイバーセキュリティウィーク
- JICA課題別研修（産業制御システムサイバーセキュリティ演習）
- [参考]「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」

情報収集　施策連携　施策周知　国際連携

②海外施策や国際標準等の動向

- 海外政府の施策動向調査
- 国際標準の動向

情報収集

③国際会議

- サイバー協議（米・独・英・ASEAN・エストニア等）
- 日米豪印サイバー上級グループ

情報収集　施策連携　施策周知

④関係国の官民との連携

- 米(DHS/CISA・DOS・DOE)、EU(DG CONNECT)、英(DCMS・NCSC)、イスラエル（INCD）
- Linux Foundation、EIS Council

情報収集　施策連携

サイバー・フィジカル・セキュリティ対策フレームワークが盛り込まれた国際規格の策定

- ISO/IECの国内エキスパートの協力のもと、**CPSFのモデル等を盛り込んだ国際規格策定**を推進。
- **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**、SC 27/WG 4 に**Technical Specification（TS）として提案**。
- 当初、CPSF単独の内容でTRとして提案していたが、これまでの議論を通じて、CPSに関連する他の議論（IoT、Digital Twin等）との整合性を確保しながら進めることとなりTS策定を目指す方向に。

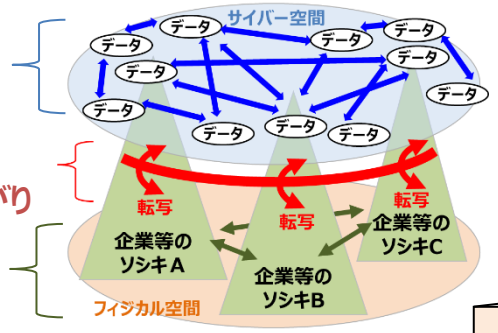
CPSFのモデル

<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のモデル等を盛り込んだドラフトを提案

ISO / IEC
↓
JTC 1
↓
SC 27
↓
WG 4

2020.4～2021.10
1st ～ 5th PWI
(Preliminary work Item)

2021.11
NWIP
(New work item Proposal)

TS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


METI
Ministry of Economy, Trade and Industry