経済産業省

産業分野におけるサイバーセキュリティ政策

経済産業省　商務情報政策局

サイバーセキュリティ課　企画官

佐藤　秀紀

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html

１．はじめに　最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サプライチェーン全体のセキュリティのためのCollective Activities
～CPSFを中心としたリスクマネジメント・ツールの整備
～中小企業のためのセキュリティ・サービス
～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）

４．サイバーセキュリティ経営

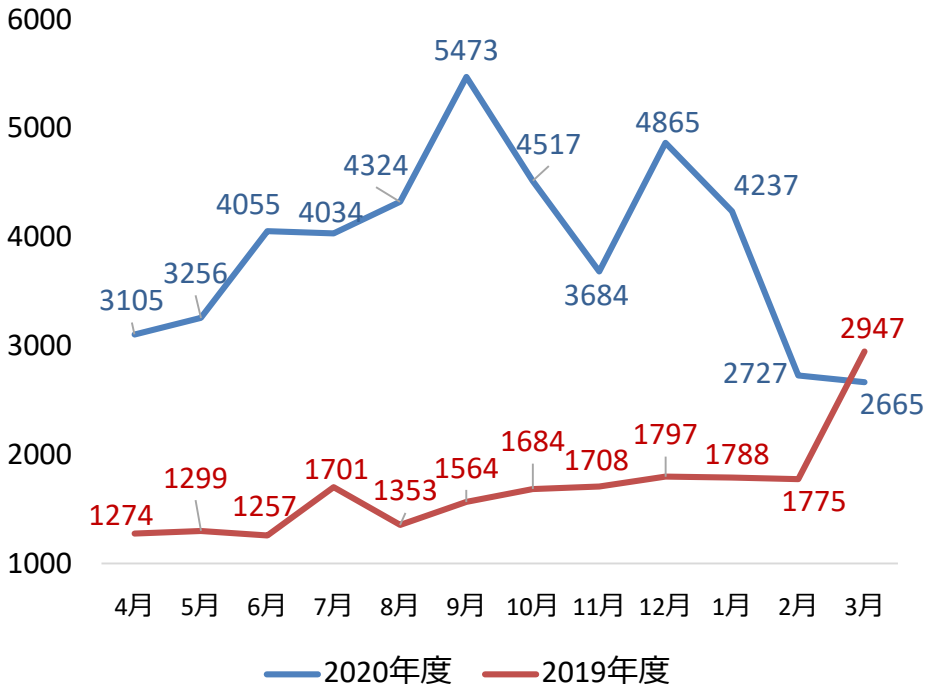
５．検証文化の定着

６．人材育成

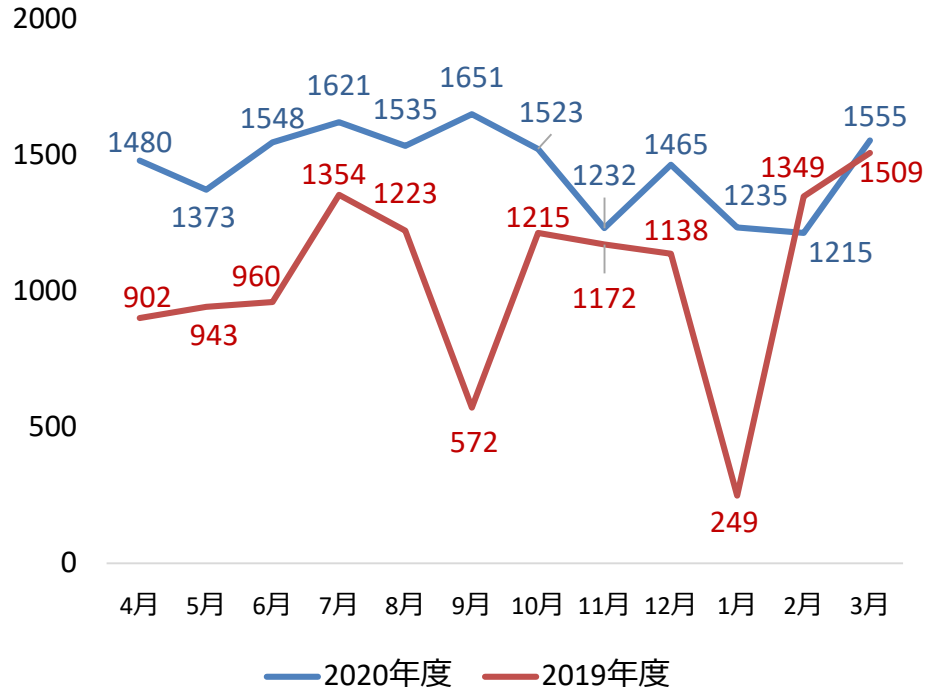
サイバー攻撃に関する相談窓口の最近の状況

- 新型コロナウイルスの感染が拡大した2020年3月以降、インシデントの相談調整件数ともに増加。
- 以降、2020年度を通して高止まりの傾向にある。

JPCERT/CCへのインシデント相談報告件数（月別）

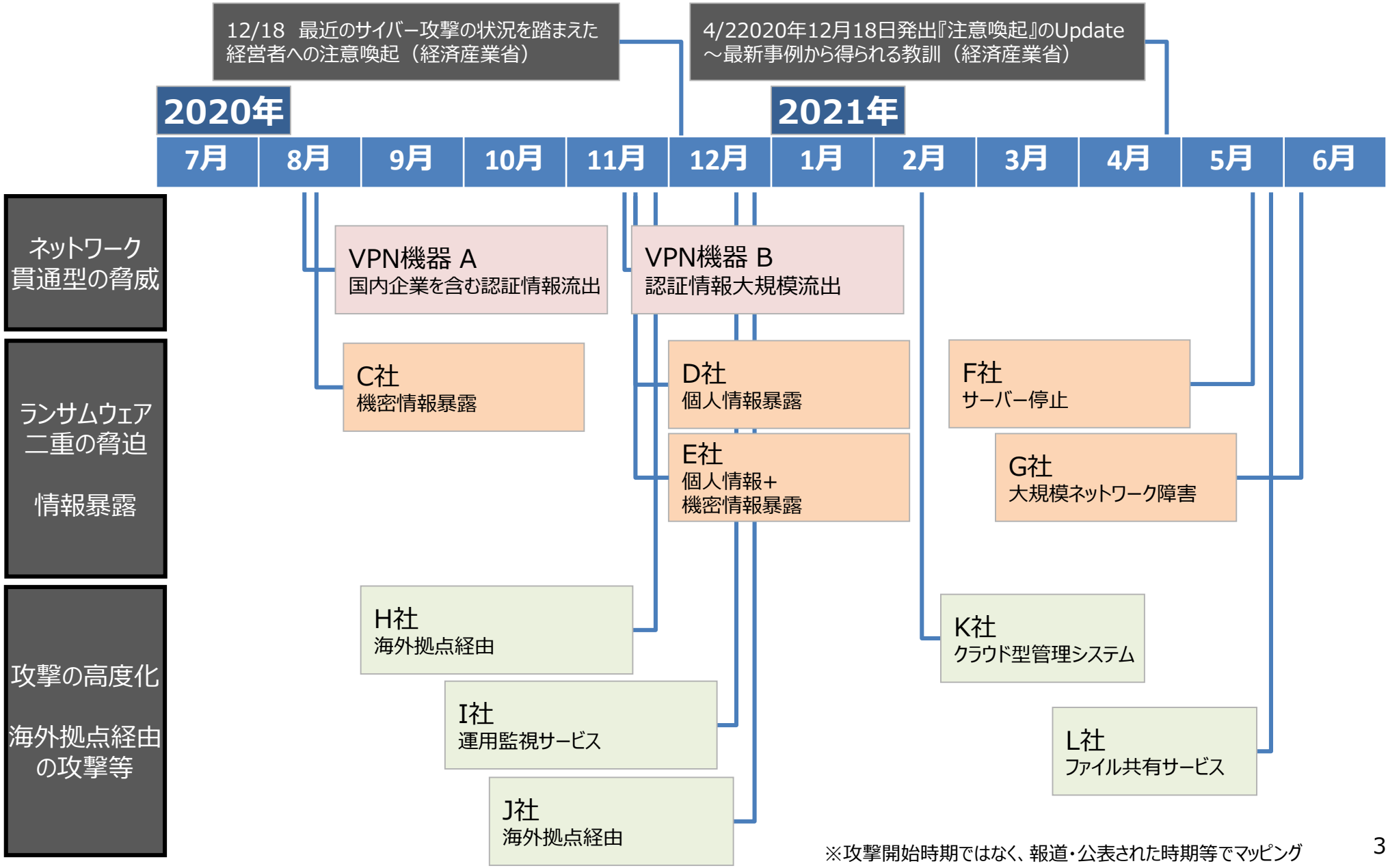


JPCERT/CCでのインシデント調整件数（月別）



<出典>（一社）JPCERT/CC>

2020～2021年の主なサイバー攻撃事案

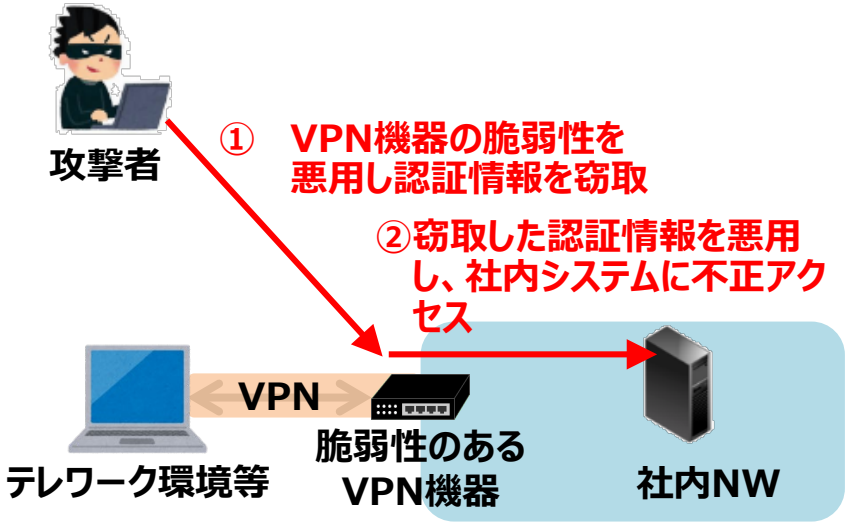


※攻撃開始時期ではなく、報道・公表された時期等でマッピング

VPN機器の認証情報流出

- **VPN機器の脆弱性**が相次いで報告され、そうした脆弱性を**悪用するコードが公開**されるなど深刻な状況が発生。**攻撃者はこうした脆弱性を通じて直接的に社内ネットワークへ侵入**し、攻撃を展開。
- 2020年8月、Pulse Secure製VPN機器の脆弱性が悪用され、**国内外900以上の事業者からVPNの認証情報が流出**。2020年11月、Fortinet製品の**VPN機能の脆弱性の影響を受ける約5万台の機器に関する情報が公開**。**認証情報等が悪用されることで容易に侵入されるおそれ**。
- **どちらのケースも既に悪用されている可能性**があるため、**機器のアップデートや多要素認証の導入といった事前対策**に加え、事後的措置として**侵害有無の確認や、パスワード変更等の対応**が必要。

VPN機器に対する不正アクセス



Pulse Secure製VPN機器の脆弱性

2019年4月	脆弱性情報公開
2019年8月	脆弱性の悪用を狙ったとみられるスキャンを確認
2019年9月	脆弱性を悪用したとみられる攻撃を確認
2020年8月	国内外900社（国内は38社）の認証情報が公開

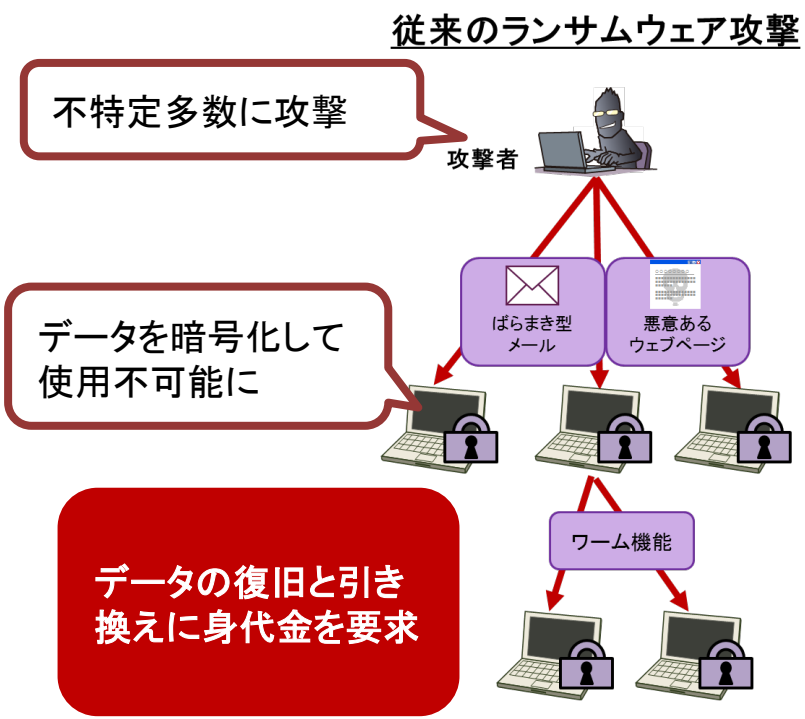
Fortinet製FortiOSの脆弱性

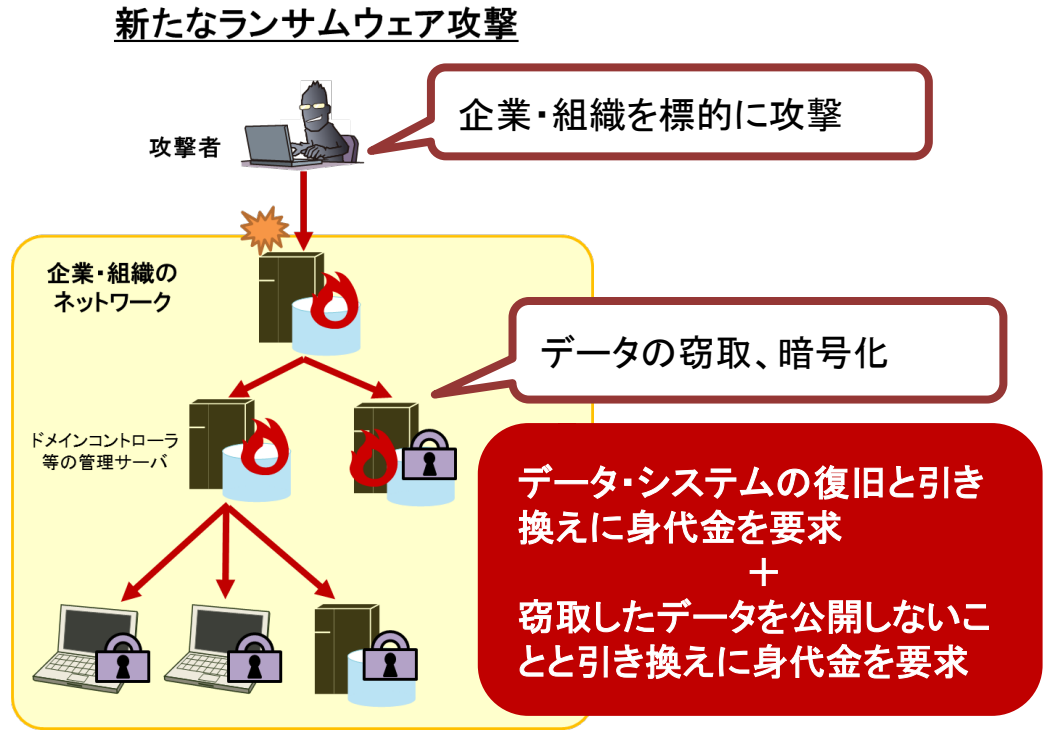
2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等

https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.html

ランサムウェアとその手口の変化（二重の脅迫）

- ランサムウェアは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。感染したパソコンのデータを暗号化するなど使用不可能にし、その**解除と引き換えに金銭を要求**する。
- **新たな（標的型）ランサムウェア攻撃（二重の脅迫）とは**
  - ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを窃取した後に一斉に暗号化してシステムを使用不可能にし、脅迫をするサイバー攻撃。
  - システムの**復旧に対する金銭要求**に加えて、窃取した**データを公開しない見返りの金銭要求**も行うので、**二重の脅迫**と恐れられる。窃取された情報に顧客の情報や機微情報を含む可能性がある場合には、被害組織はより困難な判断を迫られることになる。

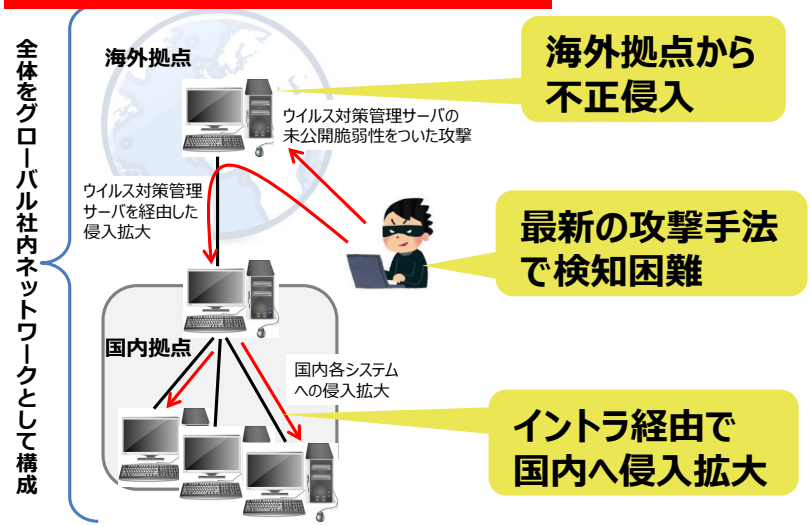




海外拠点経由の攻撃

- ビジネスのグローバル化に伴って、**海外拠点とのネットワークを国際VPN等によりWAN（広域社内ネットワーク）に取り込んで構築**しているケースが増加。海外とのビジネス効率化に寄与する一方で、**海外拠点への不正侵入によって、即国内ネットワークまで侵入される危険も**伴っている。
- 海外拠点（海外支社の他、関連会社、提携先、取引先等を含む）においては様々な原因により、日本国内と同等なレベルのセキュリティ対策が十分に取れないケースが多い。
  - 安価だが品質管理が不十分なソフトウェアが利用されている（コピー版等の利用により最新の脆弱性管理が適用されない）
  - 本社のガバナンスが行き届かず、システムの脆弱性が放置され、インシデントの監視・対応体制も十分に確保できていない
  - 従業員教育が十分でなく、私用機器やソフトウェアなどが許可なくシステムに接続されている
  - 信頼性の低いプロバイダを利用せざるを得ない　等
- このような国内環境よりも脆弱な**海外拠点において不正侵入を許してしまい、そこを足掛かりに、国内システムの奥深くまで到達されるケースが増加。**

A社事案における攻撃ルート



B社、他数社の事案の概要

- 指定秘密等の重要情報の漏えいは免れたとされている。
- ただし、攻撃者は社内の複数のシステムを渡り歩き、B社事案ではサーバ上の27,445件のファイルが不正アクセスを受けるなど、システム内部にかなりの侵入を許してしまっていた。
- 検知が遅れていれば、さらなる広範なシステムへの侵入を許していた可能性もある。

重要情報に係わるシステム分離、脆弱性対策の迅速なアップデート適用、振る舞い検知など最新の対策導入が重要

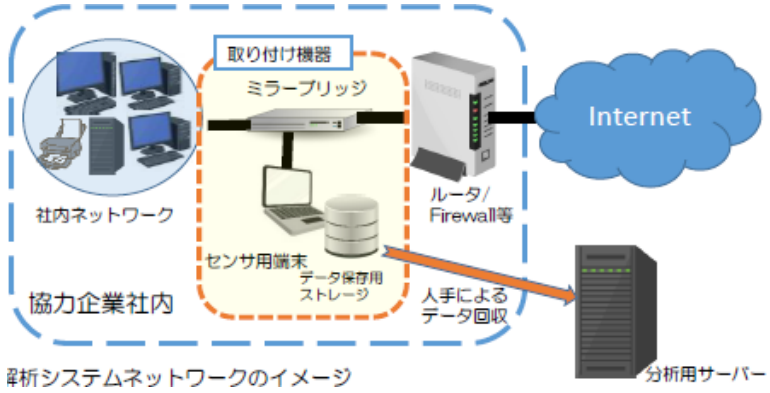
中小企業に対するサイバー攻撃の調査・分析結果（大阪商工会議所）

● 地域の中小企業も、例外なくサイバー攻撃の脅威にさらされている。

中小企業被害実態に関する調査

■調査内容

実証期間：平成30年9月～平成31年1月
実証内容：中小企業30社を対象に、ネットワーク上の通信データ等を一定期間収集。



解析システムネットワークのイメージ

■ 調査結果

- 調査した**30社全てでサイバー攻撃**を受けていたことを示す不審な通信が記録されていた。
- 少なくとも5社ではコンピューターウイルスに感染するなどして、**情報が外部に流出したおそれ**があることが分かった。

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

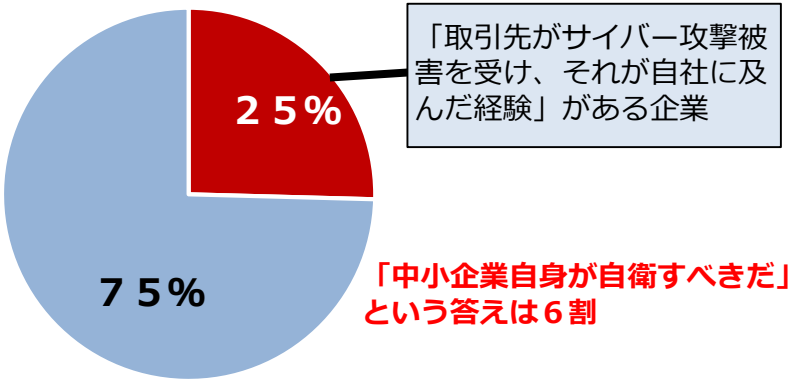
取引先経由の被害に関する調査

■調査内容

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

■調査結果

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



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

「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。

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

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。

１．はじめに　最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サプライチェーン全体のセキュリティのためのCollective Activities
～CPSFを中心としたリスクマネジメント・ツールの整備
～中小企業のためのセキュリティ・サービス
～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）

４．サイバーセキュリティ経営

５．検証検証文化の定着

６．人材育成

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

※2021年4月開催時点

構成員

- **泉澤　清次**　三菱重工業株式会社取締役社長
- **遠藤　信博**　日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等
- **大林　剛郎**　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
- **櫻田　謙悟**　経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役社長
- **篠原　弘道**　日本電信電話株式会社取締役会長
- **中西　宏明**　株式会社日立製作所取締役会長
- **船橋　洋一**　アジア・パシフィック・イニシアティブ理事長
- **村井　純(座長)**慶應義塾大学教授
- **渡辺　佳英**　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

オブザーバー　NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

WG１（制度・技術・標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日
第６回　令和2年3月（書面開催）
第７回　令和2年10月（書面開催）
第８回　令和3年３月15日

１．サプライチェーン強化パッケージ

WG２（経営・人材・国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日
第５回　令和2年1月15日
第６回　令和2年8月25日
第７回　令和3年2月18日

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３（サイバーセキュリティビジネス化）

第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日
第５回　令和2年3月(書面開催)
第６回　令和3年3月10日

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

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

１．はじめに　最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サプライチェーン全体のセキュリティのためのCollective Activities
～CPSFを中心としたリスクマネジメント・ツールの整備
～中小企業のためのセキュリティ・サービス
～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）

４．サイバーセキュリティ経営

５．検証文化の定着

６．人材育成

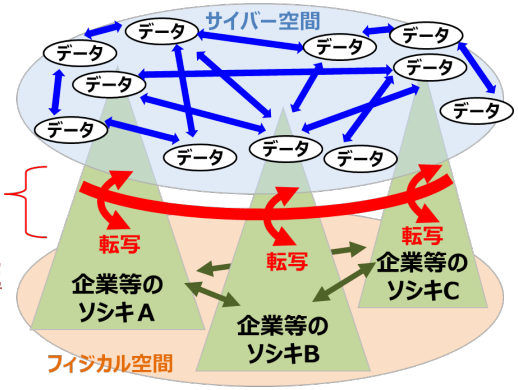
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
～ Society5.0 における新たなサプライチェーン（バリュークリエイションプロセス）の信頼性の確保に向けて ～

- サイバーとフィジカルが高度に融合する**「Society5.0」**では、**より柔軟で動的なサプライチェーンの構成が可能**になる一方、**サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスク**に直面。
- そのため、Society5.0における**新たなリスクに対応するセキュリティ対策の全体像を整理した『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver1.0』を2019年4月18日に公表**。
- 2度にわたるパブコメ（日本語、英語）に対して**国内外から多数のコメント**（合計：約800件、国内51・海外22の個人・組織）が寄せられ、**国際的認知も進展**。

CPSFが示した『3層構造』

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保



企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保

CPSFが示した『6つの構成要素』

- **リスクベースの対策**につなげるため、動的に構成されるサプライチェーンの**構成要素を6つに整理**

ソシキ	ヒト	モノ	データ	プロシージャ	システム

CPSFにおけるリスクマネジメントの考え方

（各層の）機能 → セキュリティインシデント → リスク源（構成要素ごとに整理） → 対策要件 → 対策例（3つにレベル分け）
- High-Advanced
- Advanced
- Basic

CPSFと国際規格等との整合性確保

- **国際規格等との対応関係を記載**（第Ⅲ部、添付C及び添付Ｄ）
- **以下3つの主要な国際規格等から見た対応表も整理**（添付D）
  - NIST Cybersecurity Framework
  - NIST SP800-171
  - ISO/IEC 27001付属書A

https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

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 とテーマ別TFにおける検討

- **6つの産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 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）

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**
  - ガイドライン第1版の策定(2019.6)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - 2021年1月に第1回を開催
- ・・・

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

検討事項：
データマネジメントを俯瞰するモデルを提案し、データの信頼性確保に求められる要件を検討

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

検討事項：
OSSの管理手法に関するプラクティス集の策定、SBOM活用促進に向けた実証事業（PoC）を検討

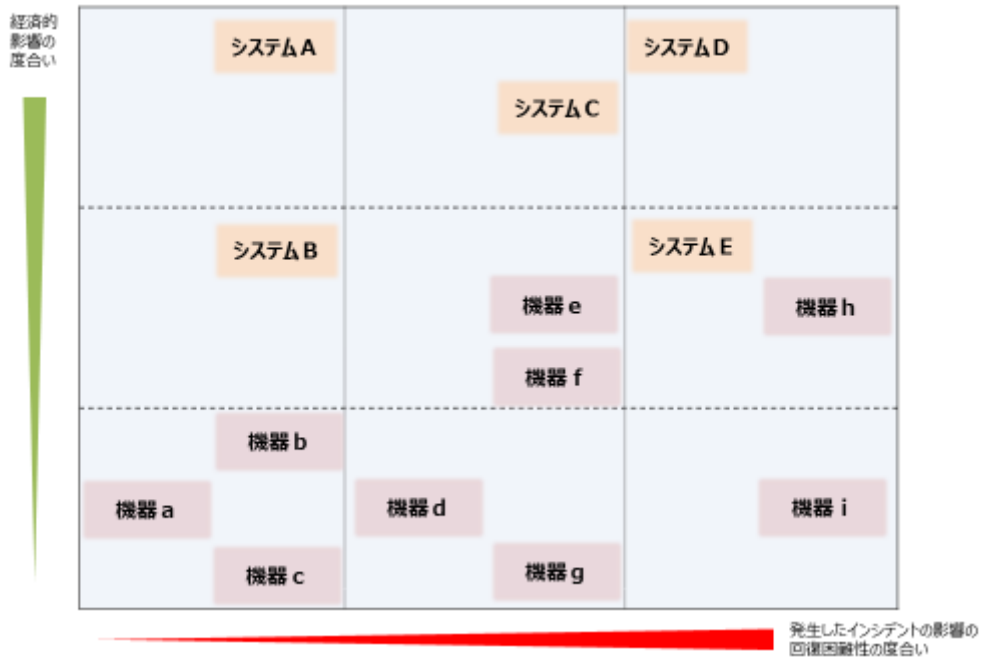
『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
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。

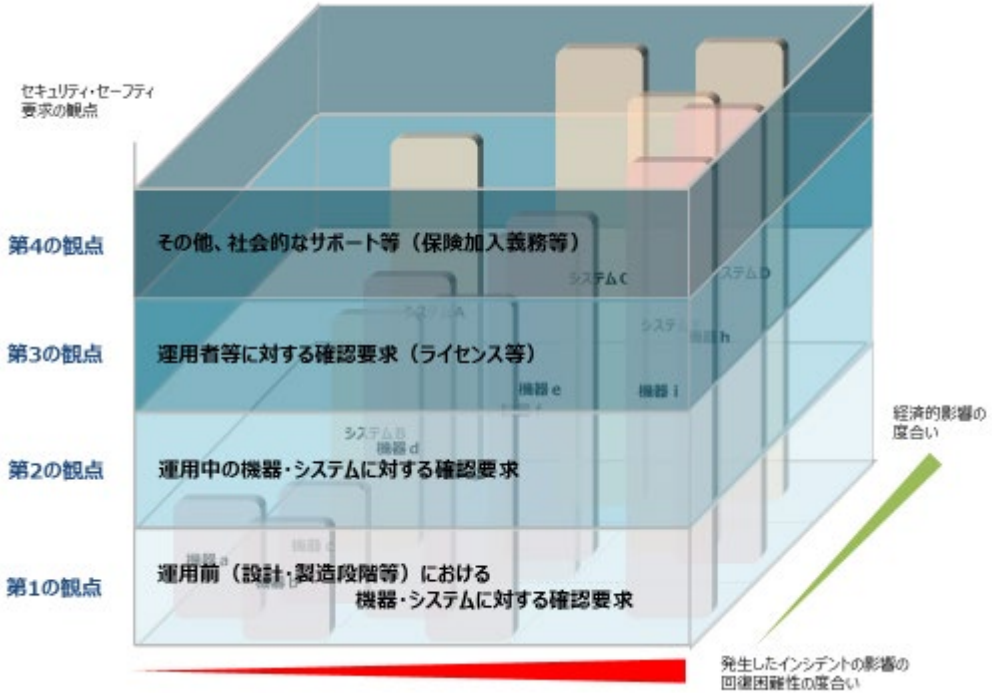
セキュリティとセーフティの融合への対応
～IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

- **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。）

https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html

ソフトウェアタスクフォースの検討の方向性（OSS事例集の作成）

- 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負担は大きく、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していることを踏まえ、**「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、2021年4月21日に公開**。

掲載事例

ヒアリング調査

- トヨタ自動車　：サプライチェーンにおけるソフトウェア使用状況把握
- ソニー　：各事業部による主体性のある取組
- オリンパス　：ヒヤリ・ハット事象を契機とした全社的取組
- 日立製作所　：製品化の過程における徹底したOSS管理
- オムロン　：PSIRTの連携を通じたOSS対応
- 東芝　：グループにおける一貫したOSS対応体制
- デンソー　：サプライチェーン全体における最適なOSS管理
- 富士通　：部門横断のOSS対応体制と全社統一的なソフトウェア管理
- NEC　：事業部毎の取組から全社的取組へ
- NTT　：OSSサポートに係る適切な役割分担
- 匿名企業A社　：OSS選定基準の明確化とコミュニティ活動
- 匿名企業B社　：グループ内SIerを中心としたセキュリティ強化
- 損害保険ジャパン　：ソフトウェア部品構成表を活用した脆弱性管理
- Visionalグループ　：自社状況に対して最適なツールの利用
- サイボウズ　：OSSエコシステムに貢献するOSSポリシー

文献調査

- マイクロソフト　：OSSに係るセキュリティリスク緩和策
- ザランド　：OSSプロジェクトの全社的な推進
- Linux FoundationとハーバードによるCensus Ⅱプロジェクトの予備的レポート
  ：アプリケーションに最も利用されているFOSSコンポーネントに関する調査

https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html

ソフトウェアTF：OSS事例集（2021年4月21日公開）

- 企業が**OSSを利活用するに当たって留意すべきポイントを整理し、そのポイントごとに参考となる事例をとりまとめて公開**することで、OSSの留意点を考慮した適切なOSS利用を促進。
- 日本だけで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。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）

- ライセンス管理
- 脆弱性管理
- サプライチェーン管理
- 組織体制
- コミュニティ活動

OSS事例集で紹介する取組（抜粋）

- 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。

- 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。

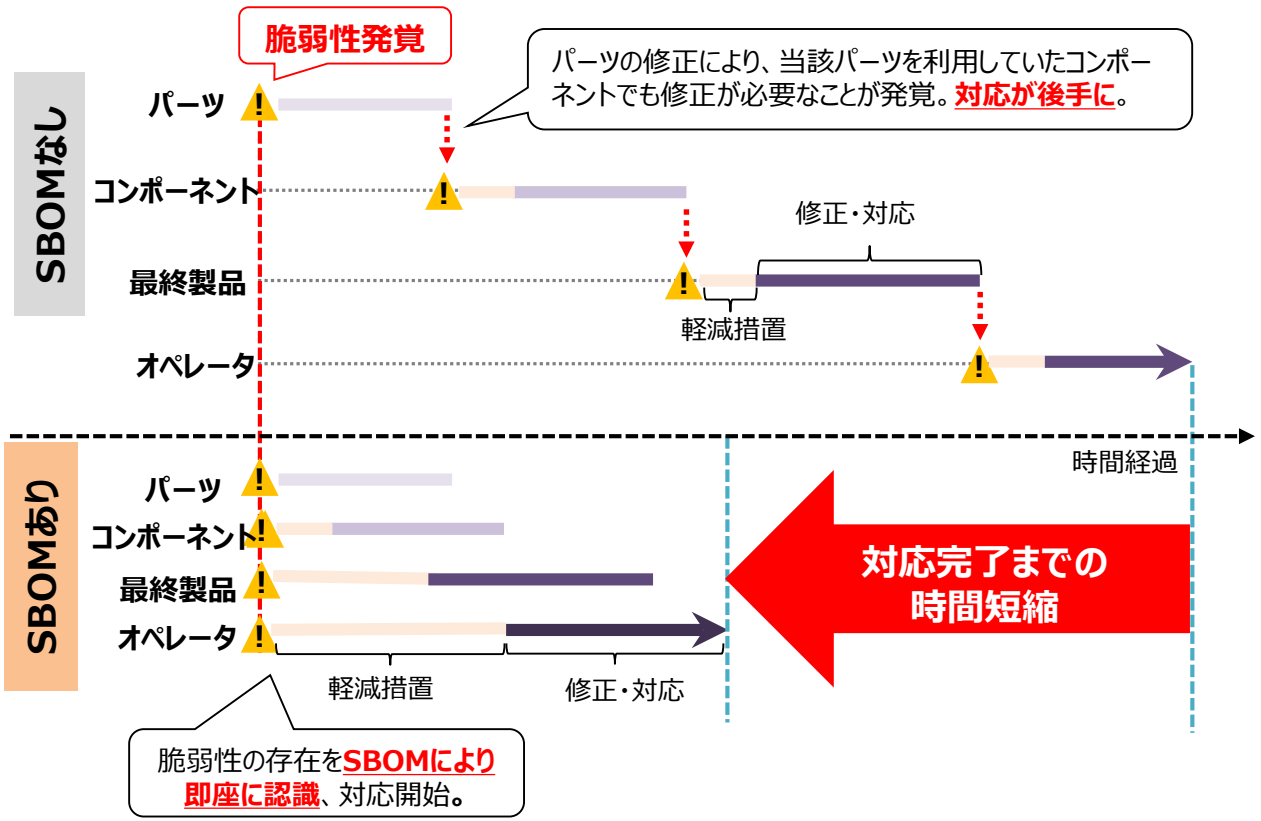
- 社員に対して、**就業時間内でのOSS開発等を認める**。
- **自社開発したソフトウェアをOSS化**し、コミュニティ型開発による性能向上を図る

https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html

ソフトウェアTF：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

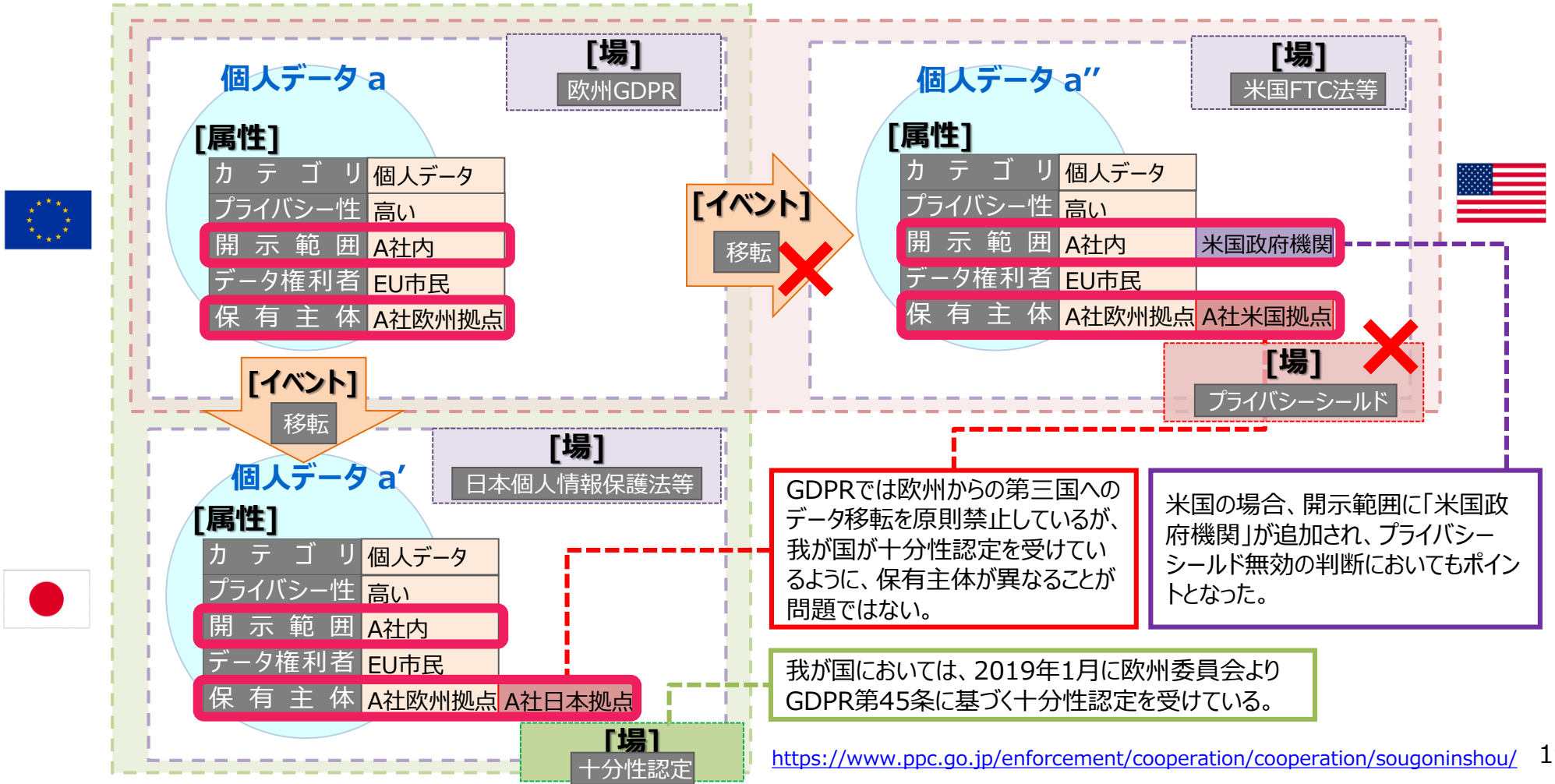
1/26キックオフ。米国エネルギー省からもプレゼンターとして参加。

第3層TF：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。データの取扱いに関する各国・地域のルールに対し、本フレームを当てはめることで、**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**。

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



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

１．はじめに　最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サプライチェーン全体のセキュリティのためのCollective Activities
～CPSFを中心としたリスクマネジメント・ツールの整備
～中小企業のためのセキュリティ・サービス
～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）

４．サイバーセキュリティ経営

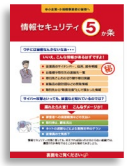
５．検証検証文化の定着

６．人材育成

中小企業のセキュリティ対策自己宣言「SECURITY ACTION」

- 中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度（IPA）。
- IT導入補助金の申請において、「SECURITY ACTION」の宣言を必須要件化。
- **１５万社を超える中小企業が宣言**（2021年2月末時点）。

★一つ星



情報セキュリティ５か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

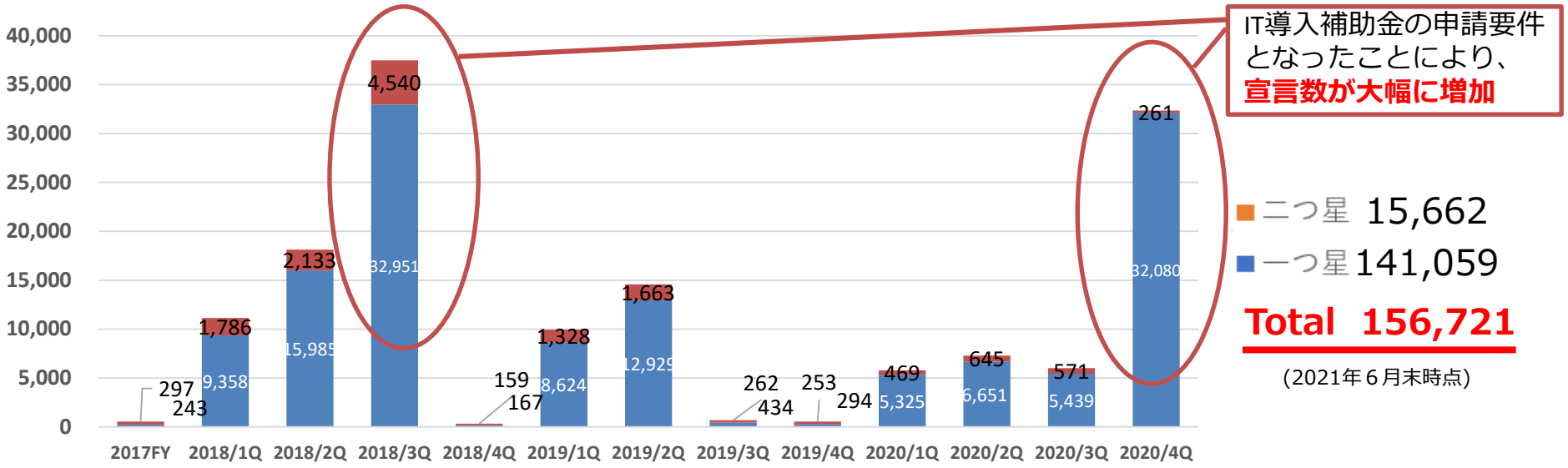
<ご参考> 中小企業の情報セキュリティ対策ガイドライン

経営者向けの解説

経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説

企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

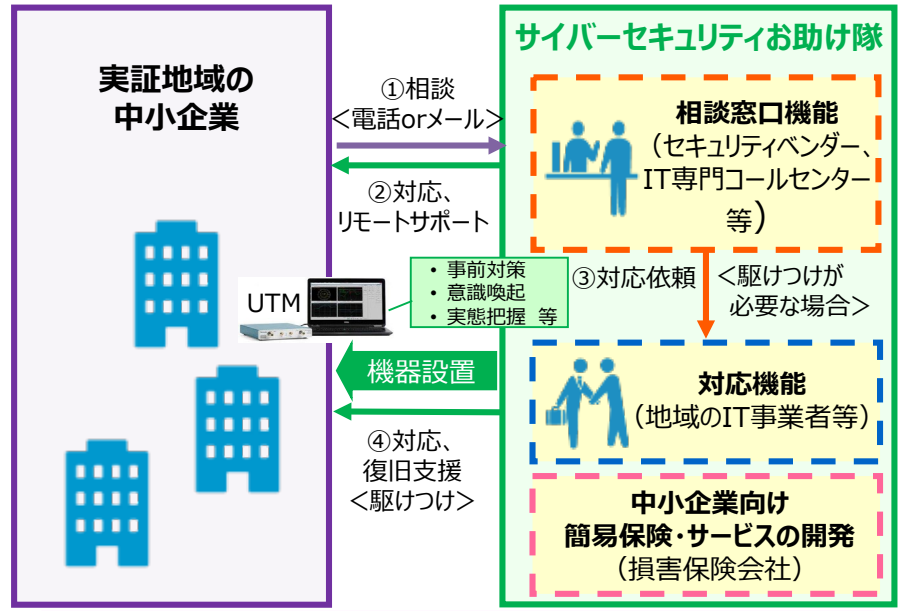


サイバーセキュリティお助け隊実証事業(2019･2020年度)

- 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（2019年度：全国で8件、2020年度：全国で15件）。のべ2,181社の中小企業が参加。
- 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、1,064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

サイバーセキュリティお助け隊実証事業の結果（2019年度）

- 1,064社が参加した実証期間中に、重大なインシデントの可能性ありと判断し、**対処を行った件数**は**128件**。対処を怠った場合の**被害想定額**が**5000万円**近くなる事案も。
- 実証参加前後の中小企業の意識変化や、お助け隊サービスに求められる機能等が明らかになった。

＜駆け付け支援の対象となった特徴的な対応事例＞

古いOSの使用

・Windows XPでしか動作しないソフトウェア利用のために、**マルウェア対策ソフト未導入のWindows XP端末を使用**。

・社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。

・検知・駆除できていなかった場合の**想定被害額は5,500万円**。

私物端末の利用

・社員の**私物iPhoneが会社のWi-Fiに無断で接続**されていたことが判明。

・私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバーと通信していた。

・検知・駆除できていなかった場合の**想定被害額は4,925万円**。

ホテルWi-Fiの利用

・社員が**出張先ホテルのWi-Fi環境**でなりすましメールを受信し、添付されたマルウェアを実行したことで**Emotetに感染**。

・感染により悪性PowerShellコマンドが実行され、アドレス情報が抜き取られた後、**当該企業になりすまして、取引先等のアドレス宛に悪性メールが送信**された。

サプライチェーン攻撃

・実証参加企業でマルウェア添付メールを集中検知。

・**取引先のメールサーバーがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。

・メールは賞与支払い、請求書支払い等を装うなりすましメールであり、**サプライチェーンを通じた標的型攻撃**であった。

https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

サイバーセキュリティお助け隊実証事業の結果（2020年度）

- 1,117社が参加した実証期間中に、セキュリティ機器による検知、および脆弱性診断等の結果に基づき、計293件のインシデント対応ほか技術的支援を実施。
- コロナ禍において、できる限り**リモートでの対処**を実施。
- また、2020年度に新たな取組として実施した産業別実証では、業界内での仕組み作りを求める声等があった。

＜リモート対応事例＞

お助け隊EDRサービスを導入した企業において、**不正プログラム「ブラウザハイジャッカー」をEDRで検知**、駆除方法を案内したが自力で対応出来なかったため、お助け隊が**リモート支援により駆除を実施**した。

UTMサービスを導入した企業において、**マルウェアへの感染の疑いがある通信をUTMで検知**。フルスキャンの結果、**Hacktool及びトロイの木馬、計6件のマルウェアを発見したため、お助け隊でリモート駆除を実施**。

＜産業別実証での気づき＞

自動車産業

- 外部診断の結果、実証参加企業全体のセキュリティ管理レベルの平均は、**製造業の平均と比べ比較的高かった**。
- 取引先からの要請は高まっているが、セキュリティ対策を行う上でのリソースが全般的に不足。**業界内での人材プールを共有できる仕組み**等の整備が課題。
- **同業他社の状況**を知ることができると、投資判断における経営者への動機付けになる。

防衛・航空宇宙産業

- セルフアセスメント（情報セキュリティ整備状況診断）を実施したところ、今後業界として求められるであろう**レベルに到達していた企業は10%** ※
- **防衛・航空宇宙産業という名目で特別な対策を要求**された企業は**38%**。要求された対策の中にはアクセス権に関するものもある一方で、セルフアセスメントでは、**秘密情報へのアクセス管理について約半数の企業が実施できていない**と回答。

※CMMC Level 1の17項目全てを達成しているか否かで判定

- 産業別実証事業は、「自動車産業の中小企業サプライヤーを対象とした実証」と、「防衛・航空宇宙産業に関わる中小企業及び今後防衛・航空宇宙産業に参入を検討する中小企業を対象とした実証」を実施。

サイバーセキュリティお助け隊実証事業の声・課題（2019・2020年度）

実証参加事業者の声（2019年度　参加中小企業のアンケート結果より）

- アラート通知が実際にあり、**他人事ではないとの意識につながった。**（大阪府・建設業）
- UTM導入時、当社に**専門知識が無いため、業者と話がかみ合わず、導入に手間取った。**（神奈川県・サービス業）
- 参加することで、情報セキュリティ対策を実施していることを、**外向けにアピールできる**のが良い。（新潟県・電気通信工事業）
- 総務担当がセキュリティを兼務していることもあり、**ワンパッケージでやってくれると非常に助かる。**（石川県・製造業）

実証におけるサービス提供事業者の声（2020年度抜粋）

- Webセキュリティ診断において緊急性の高い脆弱性が発見されるなど、中小企業のウェブサイトの多くは、過去に
  構築後、**脆弱性に対する対応が行われないまま放置されている**例が数多く見られた。
- リスク診断等の簡易ツールを用意しても**自主的に取り組める中小企業は少なく**、個別サポートが必要。
- EDRの検知レポートを送付しても読んでもらえないことが多く、電話で説明すると喜んでもらえる。

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15日にお助け隊マークが付与された民間サービスが「サイバーセキュリティお助け隊サービス※」として登録され、市場に展開。**

※中小企業のサイバーセキュリティ対策支援サービスに不可欠な各種サービス内容（相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など）の基準を満たした民間による支援サービス事業

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）

サイバーセキュリティ お助け隊

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

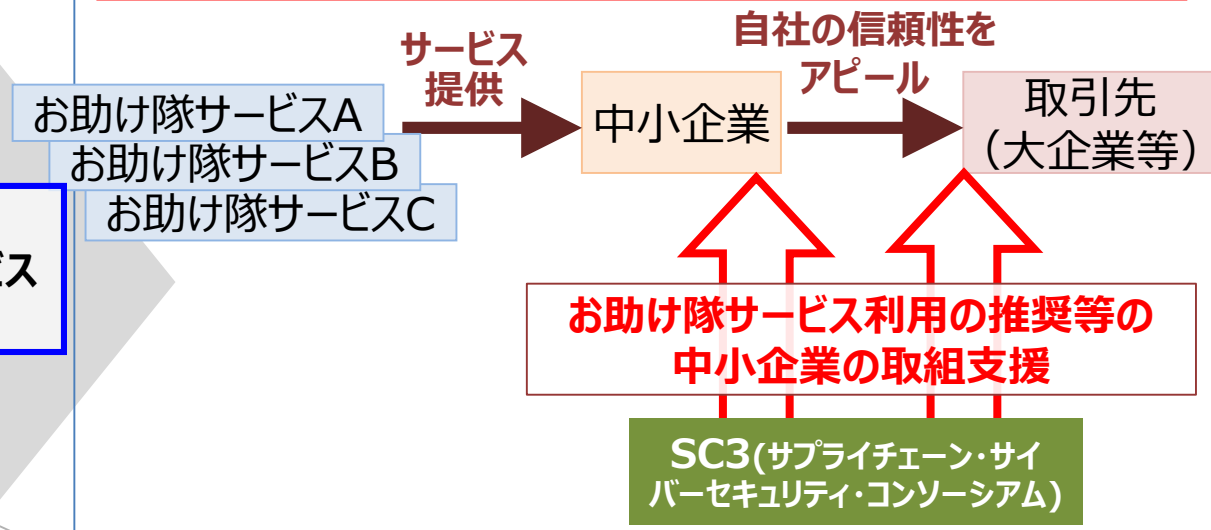
実証事業：
中小企業が利用しやすい安価なセキュリティサービスの開発

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。



→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。

サイバーセキュリティお助け隊サービス　登録リスト

- 全国各地域の中小企業の皆様にとって選択・利用可能な「サイバーセキュリティお助け隊サービス」第1回登録サービスリスト（5件）

【第1回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	近畿エリア、名古屋・東京・神奈川の都心部 ※近畿地方に本社を置く企業
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

（参考） 「サイバーセキュリティお助け隊サービス基準」の概要

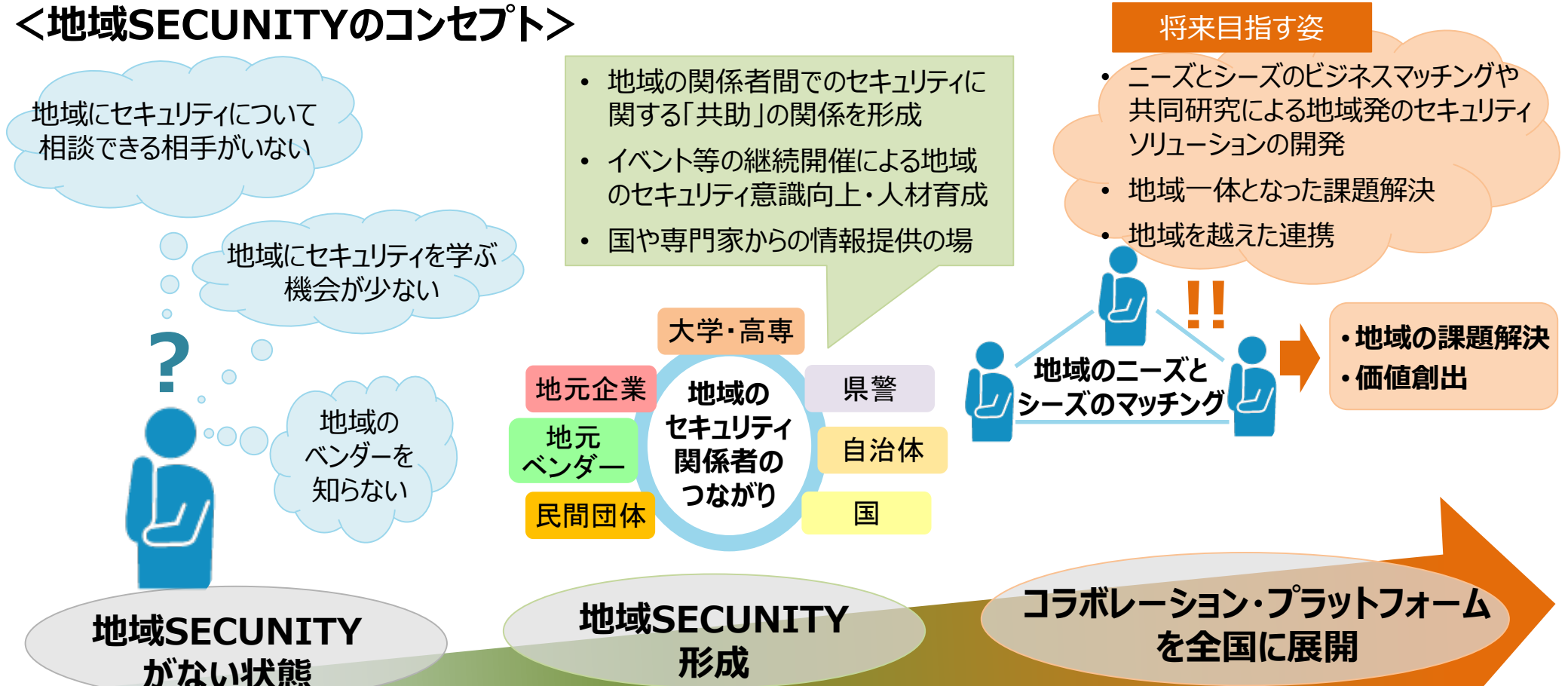
- 【コンセプト】中小企業に対するサイバー攻撃への対処として**不可欠なサービス**を**効果的**かつ**安価**に、**確実**に提供する。「v1.0版」として公開した同基準の概要は以下のとおり。
- 第1回審査(3月)において新たに出た論点を踏まえ、第2回中小企業対策強化WGにおいて、基準改定や基準解釈の目安となるガイドの作成等の方針を議論。今後、詳細を詰めていく予定。

主な要件	概要
相談窓口	お助け隊サービスの導入・運用に関するユーザからの各種**相談を受け付ける窓口を一元的に設置／案内**
異常の監視の仕組み	・ユーザのネットワークを24時間見守り、攻撃を検知・通知する仕組み（UTM等のツールと異常監視サービスから構成）を提供すること（**ネットワーク一括監視型**の場合） ・ユーザの端末（PCやサーバ）を24時間見守り、攻撃を検知・通知する仕組み（EDR等のツールと異常監視サービスから構成）を提供すること（**端末監視型**の場合）
緊急時の対応支援	ユーザと合意したサービス規約等に基づき、ユーザから要請された場合、ユーザの指定する場所に**技術者を派遣する等により緊急時の対応支援を行う**こと
中小企業でも導入・運用できる簡単さ	IT・セキュリティの**専門知識のないユーザでも導入・運用できるような工夫**が凝らされていること
中小企業でも導入・維持できる価格	・**ネットワーク一括監視型**の場合：**月額１万円以下**（税抜き） ・**端末監視型**の場合：**端末１台あたり月額2,000円以下**（税抜き）（端末1台から契約可能であること） ・最低契約年数は２年以内 ・**初期費用、契約年数等の契約にかかる条件をサービス規約等に記載するとともに、口頭又は書面によりユーザに分かりやすく説明**すること
簡易サイバー保険	インシデント対応時に突発的に発生する各種コストを補償する**サイバー保険が付帯**されていること なお、当該保険は初動対応（駆付け支援等）の費用を最低限補償するものであること
上記機能のワンパッケージ提供	・原則として、これら機能をユーザが個別に契約することなく**一元的に購入可能**であること （例外的に個別契約とする場合にも、ユーザにおいて手続上の煩雑さを伴わないよう工夫が凝らされていること）
中小企業向けセキュリティ事業の実績	お助け隊実証事業に参加していたこと又は上記構成のサービスを**中小企業向けに提供・運用した実績**があること
情報共有	お助け隊サービス事業者どうし等の深いレベルの**情報共有（少なくともアラートの統計情報の提供）**に応じること
事業継続性	要員の確保、品質管理等の社内プロセス整備、企業としての安定した財政基盤、経理処理能力等
更新	**２年毎に更新審査**を受けること

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

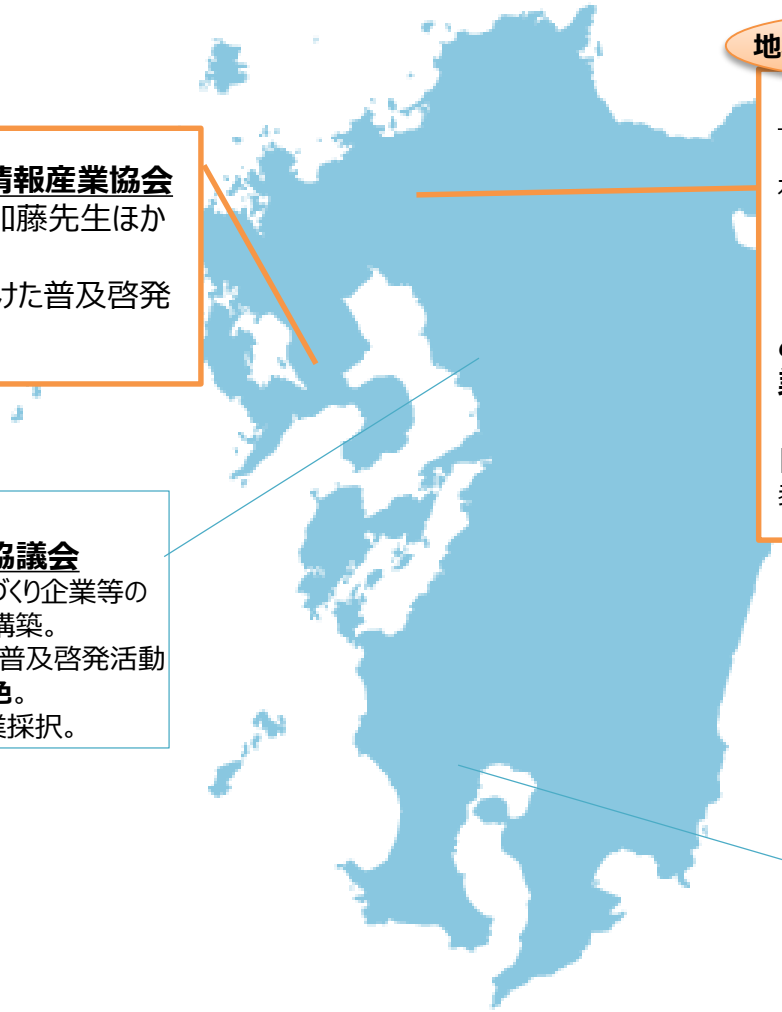
- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動を、「地域SECUNITY」と命名。
- まずは各地域で地域SECUNITYの形成を促進し、将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指す。

＜地域SECUNITYのコンセプト＞



令和２年度地域SECUNITY形成促進の取組（九州）

- 令和２年度事業採択を契機に、企業や大学等のキーパーソンを中心とした産学官連携のコミュニティ形成が進行中。
- 既存の取り組み、ネットワークも活用しながら、九州全域での展開を目指す。



地域SECUNITY事業採択

・事業主体：（一社）長崎県情報産業協会
・キーパーソン：長崎県立大学　加藤先生ほか
・事業内容：**長崎県**において、
サイバーセキュリティ対策強化に向けた普及啓発セミナー（R3.1.27）を実施。

【参考】
熊本県サイバーセキュリティ推進協議会
自治体・県警を中心に、IT業界・ものづくり企業等の産業界、大学と産学官の推進体制を構築。
学生のボランティア活動の支援を通じた普及啓発活動など**参加大学の学生による活動が特色**。
R2FYサイバーセキュリティお助け隊事業採択。

地域SECUNITY事業採択

・事業主体：三井物産セキュアディレクション(株)
・協力：（公財）福岡貿易会、（一社）九州経済連合会
福岡貿易会ほか
・キーパーソン：九州大学　小出先生ほか

・事業内容：**福岡県・佐賀県**において、**業界普及への推進役となりうる地域企業（製造業や医療法人）の協力**のもと、**業界コミュニティ**として、各業界ごとに普及啓発セミナー（R3.2.3、R3年夏頃にも開催予定）等を実施。
自治体、県警のほかセキュリティ事業者、保険事業者、教育関連事業者とも連携体制を構築。

【参考】
鹿児島県サイバーセキュリティ協議会
会員企業向けに技術勉強会やセミナーを定期的に開催。
IT業界や自治体、県警、学校とのネットワークも構築し、サイバーセキュリティ対策の普及啓発に向けた働きかけも積極的実施。

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

１．はじめに　最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
　～産業サイバーセキュリティ研究会

３．サプライチェーン全体のセキュリティのためのCollective Activities
　～CPSFを中心としたリスクマネジメント・ツールの整備
　～中小企業のためのセキュリティ・サービス
　～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）

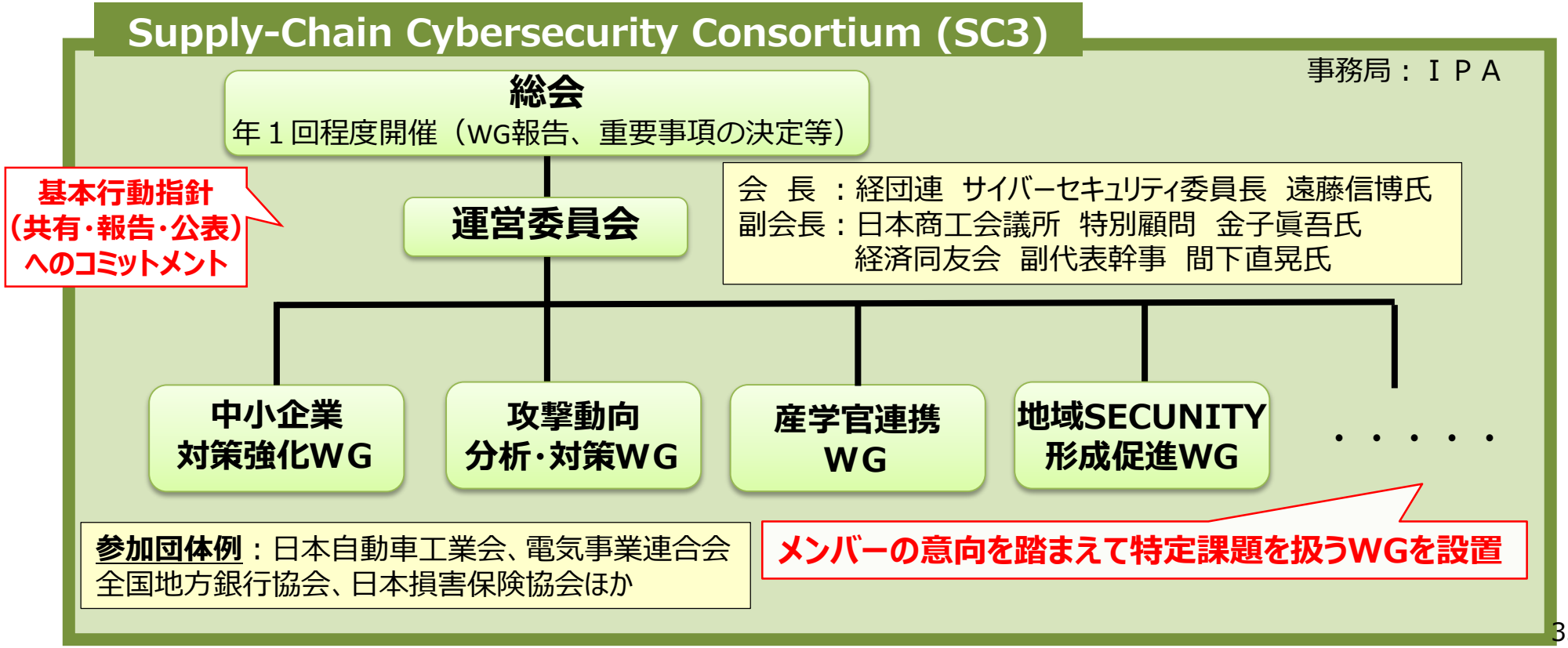
４．サイバーセキュリティ経営

５．検証文化の定着

６．人材育成

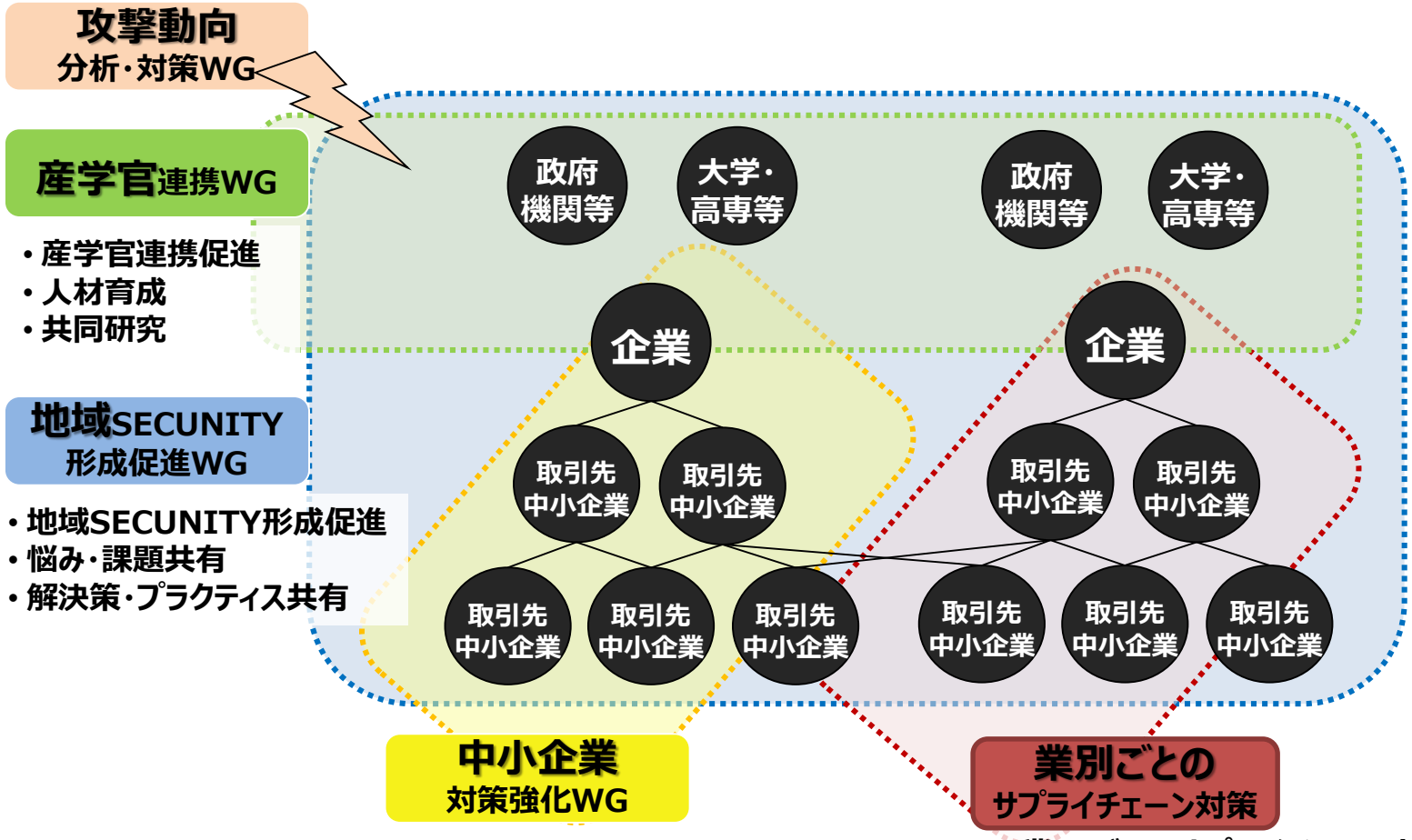
サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

- **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（2021年６月末時点で171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。



SC3の全体像

- 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議論・浸透のため、SC3に対し、産学官連携や経営層向けの注意喚起、地域・業界別の取組・課題共有等のプラットフォームとしての機能への期待の声が挙がったことを踏まえ、中小企業対策強化WGに加えて、新たに３つのWGを設置。



１．はじめに　最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サプライチェーン全体のセキュリティのためのCollective Activities
～CPSFを中心としたリスクマネジメント・ツールの整備
～中小企業のためのセキュリティ・サービス
～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）

４．サイバーセキュリティ経営

５．検証文化の定着

６．人材育成

段階的なサイバーセキュリティ経営の実現

- 以下の3Stepにより、サイバーセキュリティ経営の定着を目指す。

1st Step

サイバーセキュリティ経営の明確化

- サイバーセキュリティ経営ガイドラインの普及・定着

2nd Step

サイバーセキュリティ経営の実践

- GGS(グループ・ガバナンス・システム)ガイドラインにサイバーセキュリティを反映
- プラクティス集、人材の手引きの整備により、サイバーセキュリティ経営を現場レベルで推進
- DXの進展を踏まえ、サイバーセキュリティリスク対応の重要性に対する意識啓発を推進
- 投資家に対してもサイバーセキュリティの重要性を啓発

3rd Step

セキュリティの高い企業であることの可視化

- 可視化ツールの普及によるサイバーセキュリティ経営の可視化の推進
- セキュリティの高い企業であることを投資家が評価できるようにするための、サイバーセキュリティ経営に関する情報の開示の在り方の検討

サイバーセキュリティ経営ガイドライン

平成27年12月28日策定
平成28年12月8日改訂（Ver.1.1）
平成29年11月16日改訂（Ver2.0）

1st step

- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドライン。
- 2017年11月公開のVer2.0は、ダウンロード数累計約11万件と注目度の高い状況が続いている。

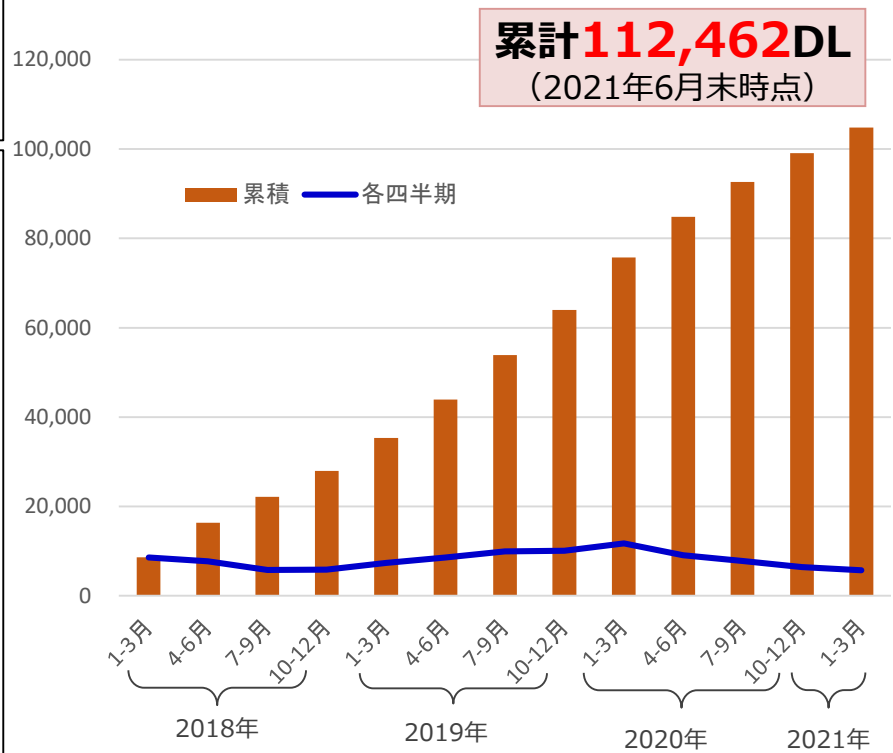
1．経営者が認識すべき３原則

（1）経営者が、**リーダーシップを取って対策**を進めることが必要
（2）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（3）平時及び緊急時のいずれにおいても、**関係者との適切なコミュニケーション**が必要

2．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の対策及び状況把握
関係者とのコミュニケーション	**指示10** 情報共有活動への参加

サイバーセキュリティ経営ガイドラインV2.0のダウンロード数推移



【参考】上場企業数　第一部　2,192社
　　第二部　474社
（日本取引所グループ公表 2021年５月31日時点）

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

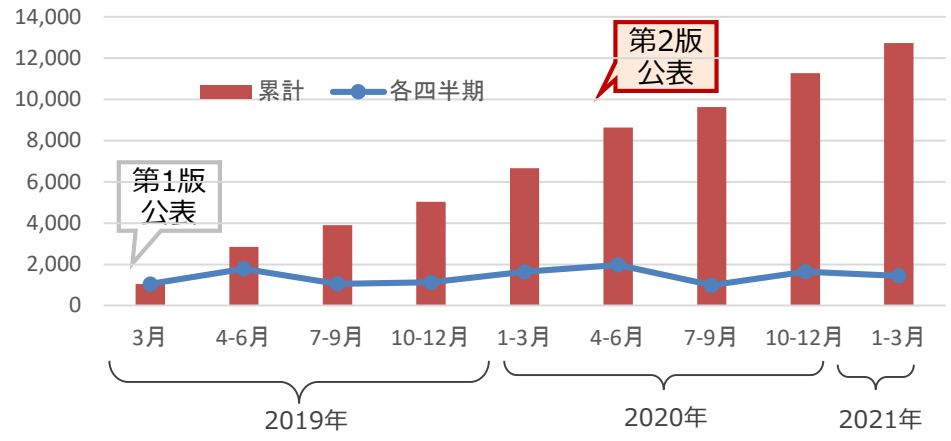
『サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集』

2nd step

- 2019年3月、**「サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集」を公開**。経営ガイドラインの重要10項目の実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示。プラクティスを追加した**第2版を2020年6月3日に公表**。
- １万件超のダウンロードがあるなど一定の評価を得ているが、更なる改善のために、2020年度は**プラクティス利用の実態把握や企業が使いやすいプラクティスの在り方を明確にするための調査**を実施。2021年4月にIPAより調査結果を公表。

<プラクティス集のダウンロード数推移>

累計**14,278**DL (2021年６月末時点)



【参考】上場企業数　第一部　2,192社
第二部　474
（日本取引所グループ公表 2021年５月31日時点）

<2020年度調査結果>

文献調査（6件）／アンケート調査（930社）／有識者インタビュー（3名）／企業インタビュー（5社）

◆文献調査
- 国内外のセキュリティ関連のプラクティスの多くは、**民間企業などがボランティアで作成・共有**している。

◆アンケート調査
- 企業ユーザのプラクティス集の**認知度は4割強**で、**インシデント発生時に備えた**セキュリティ強化を目的として活用されている。
- 半数以上の企業ユーザが**プラクティス集**のようなセキュリティ対策事例の**必要性**を感じており、**プラクティス集の作成に協力的**である。

◆有識者・企業インタビュー
- **「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」と連携**し、企業が本ツールを用いて自己診断を行った結果、対策レベルの低い項目について、プラクティスの事例を表示させることができると良い。
- 現在、企業が直面しているセキュリティの脅威に対して打てる**具体的な対策が示されている**と良い。

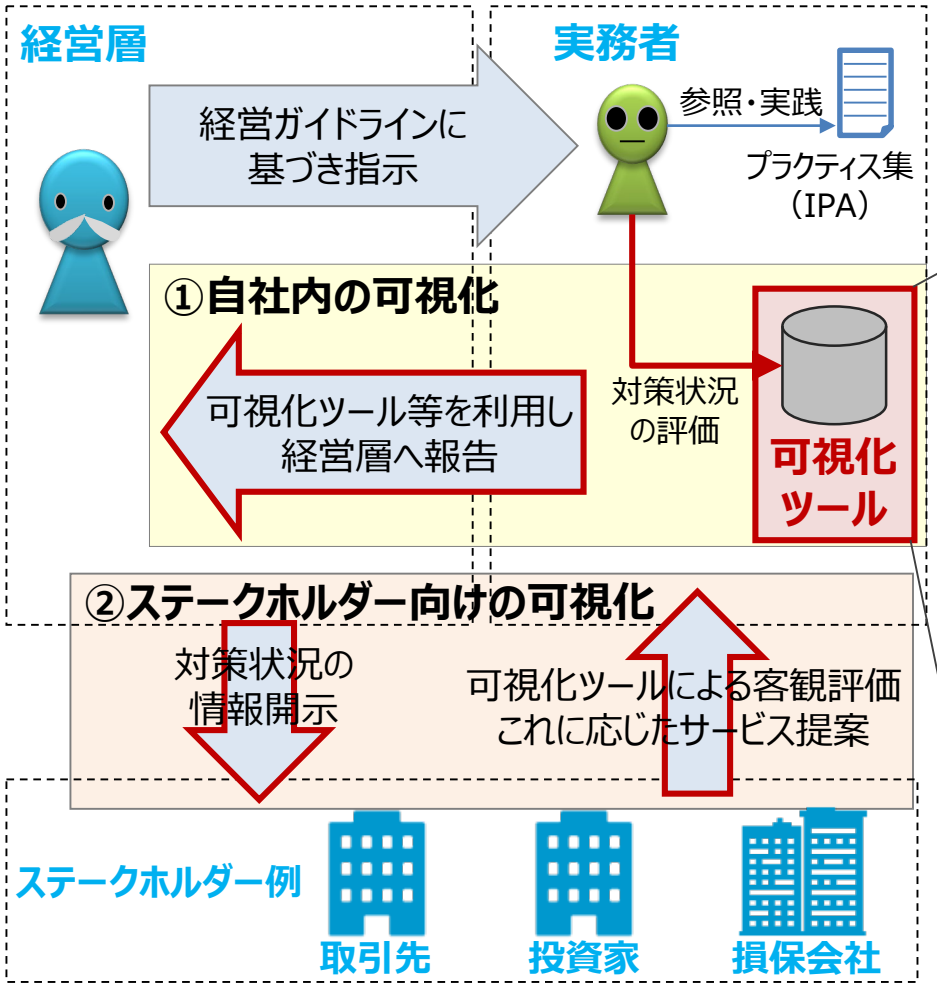
https://www.ipa.go.jp/security/fy30/reports/ciso/index.html

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

2nd ～ 3rd step

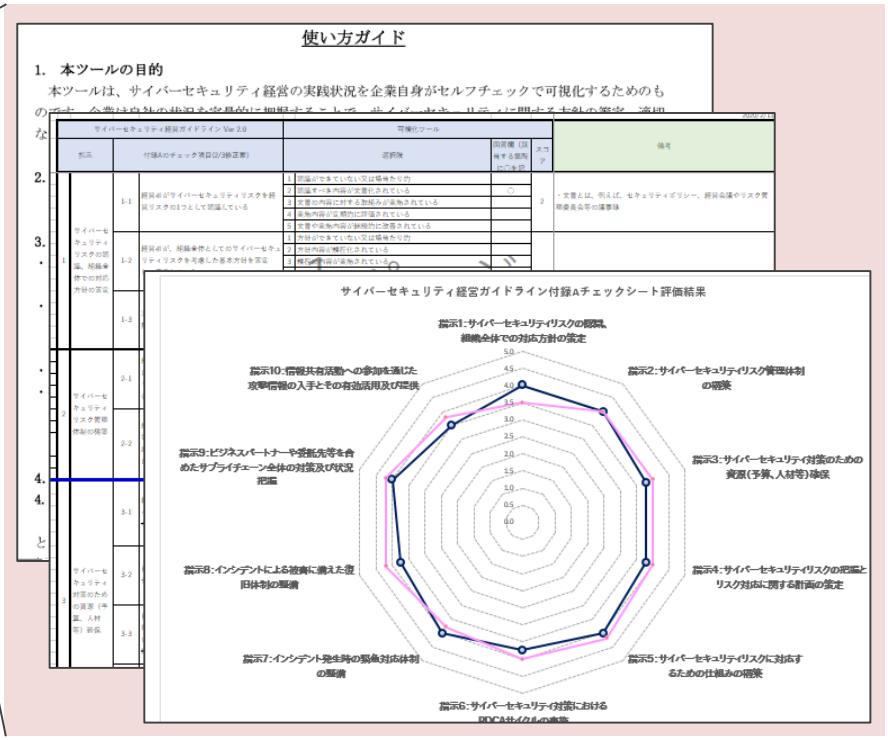
累計6,154ダウンロード
（2021年６月末時点）

- 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

１．はじめに　最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サプライチェーン全体のセキュリティのためのCollective Activities
～CPSFを中心としたリスクマネジメント・ツールの整備
～中小企業のためのセキュリティ・サービス
～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）

４．サイバーセキュリティ経営

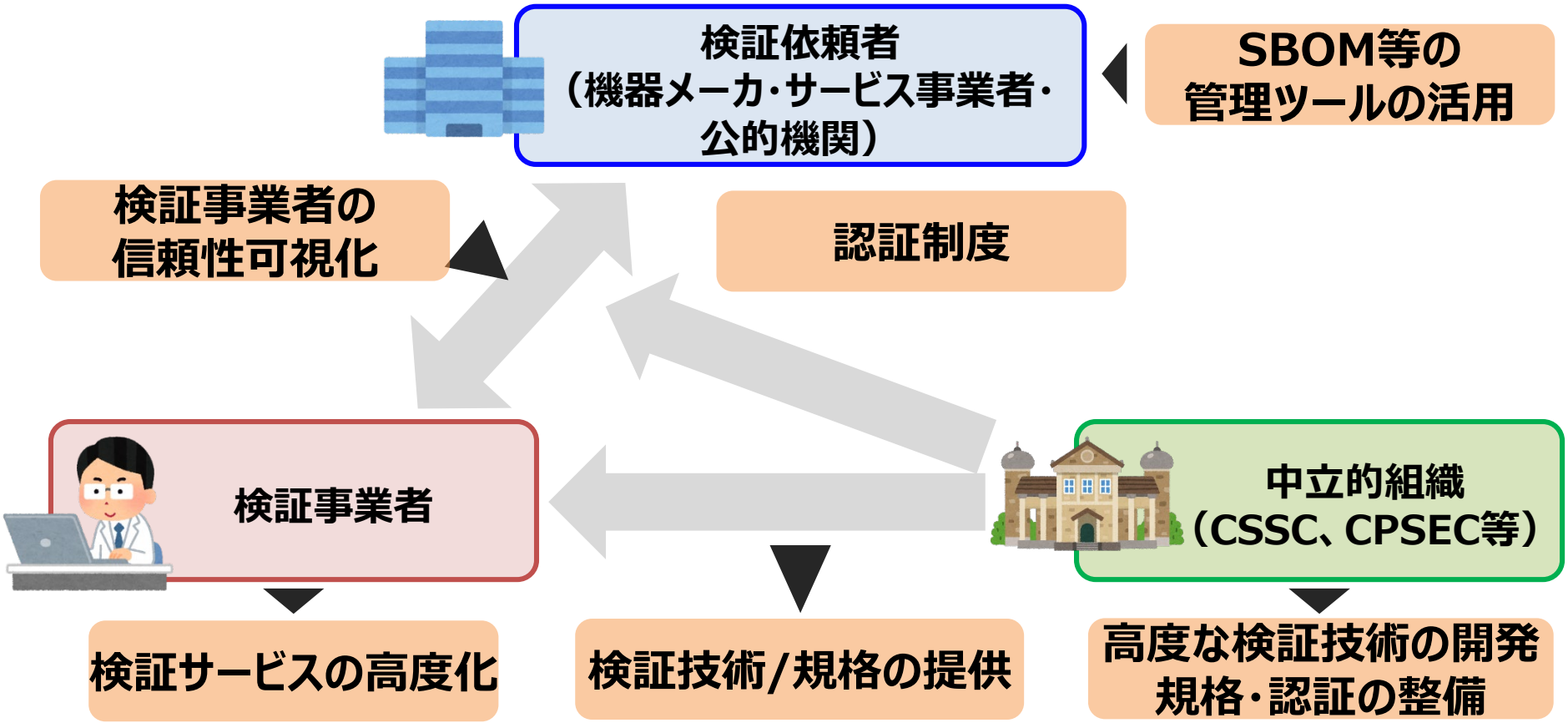
５．検証文化の定着

６．人材育成

「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）



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、2021年4月に公開。**

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、2020年度拡充）

- 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（2020年度作成）

- 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3：検証人材の育成に向けた手引き（2020年度作成）

- 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。

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（2020年度作成）

- 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。

https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

１．はじめに　最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サプライチェーン全体のセキュリティのためのCollective Activities
～CPSFを中心としたリスクマネジメント・ツールの整備
～中小企業のためのセキュリティ・サービス
～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）

４．サイバーセキュリティ経営

５．検証文化の定着

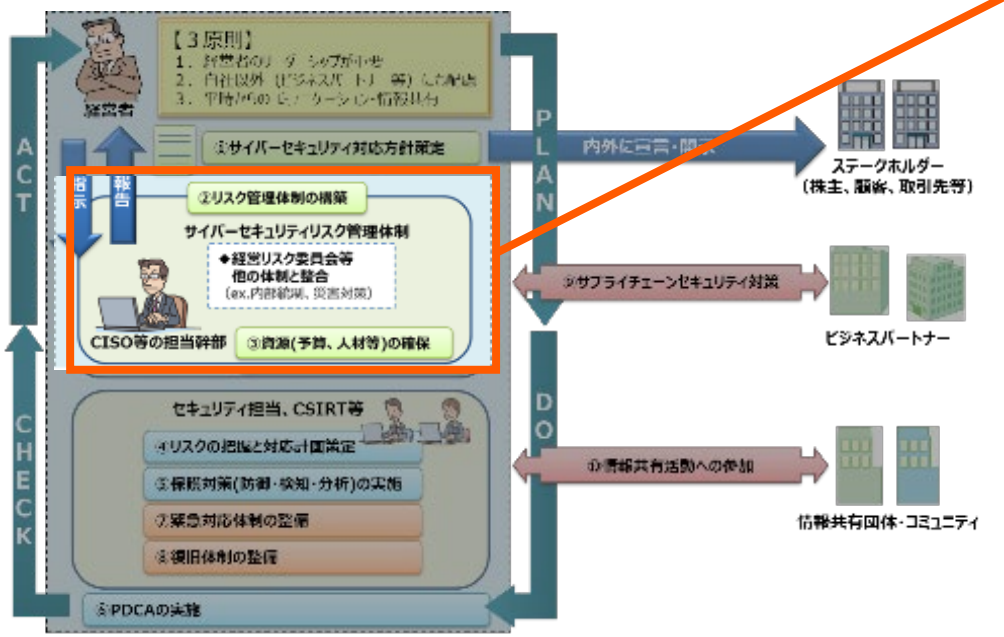
６．人材育成

『セキュリティ体制構築・人材確保の手引き』の開発

累計**6,925**ダウンロード
（2021年6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た**第1.1版を2021年4月15日に公表。**

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（例）：

- サイバーセキュリティ対策に従事する人材の確保
- 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

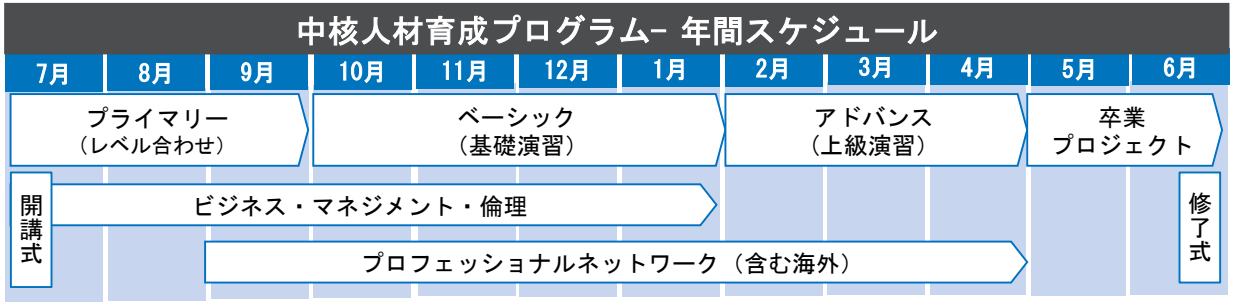
https://www.meti.go.jp/press/2021/04/20210426002/20210426002.html

産業サイバーセキュリティセンター（ICSCoE）（2017年4月設置）

- 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5期中核人材育成プログラム（2021年7月開講）には、48名が参加。

ロ　１年を通じた集中トレーニング

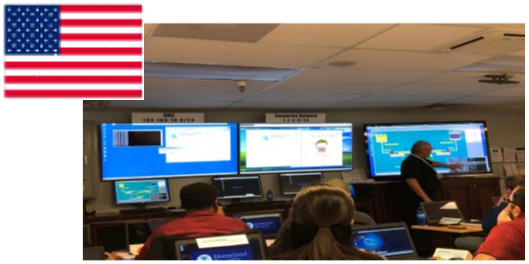
ロ　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人）



- 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

ロ　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

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

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html