経済産業省

資料３

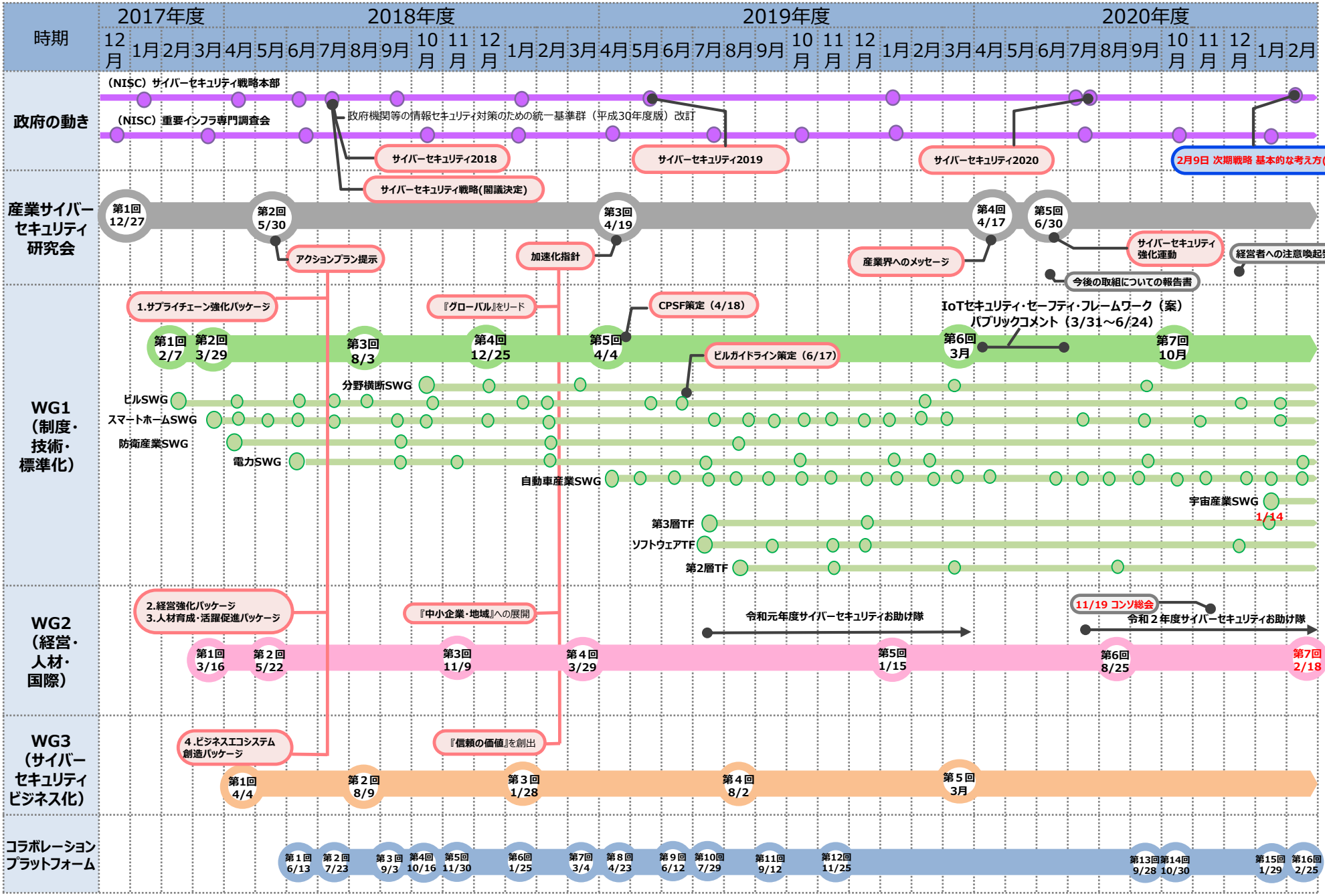
事務局説明資料

経済産業省

商務情報政策局

サイバーセキュリティ課

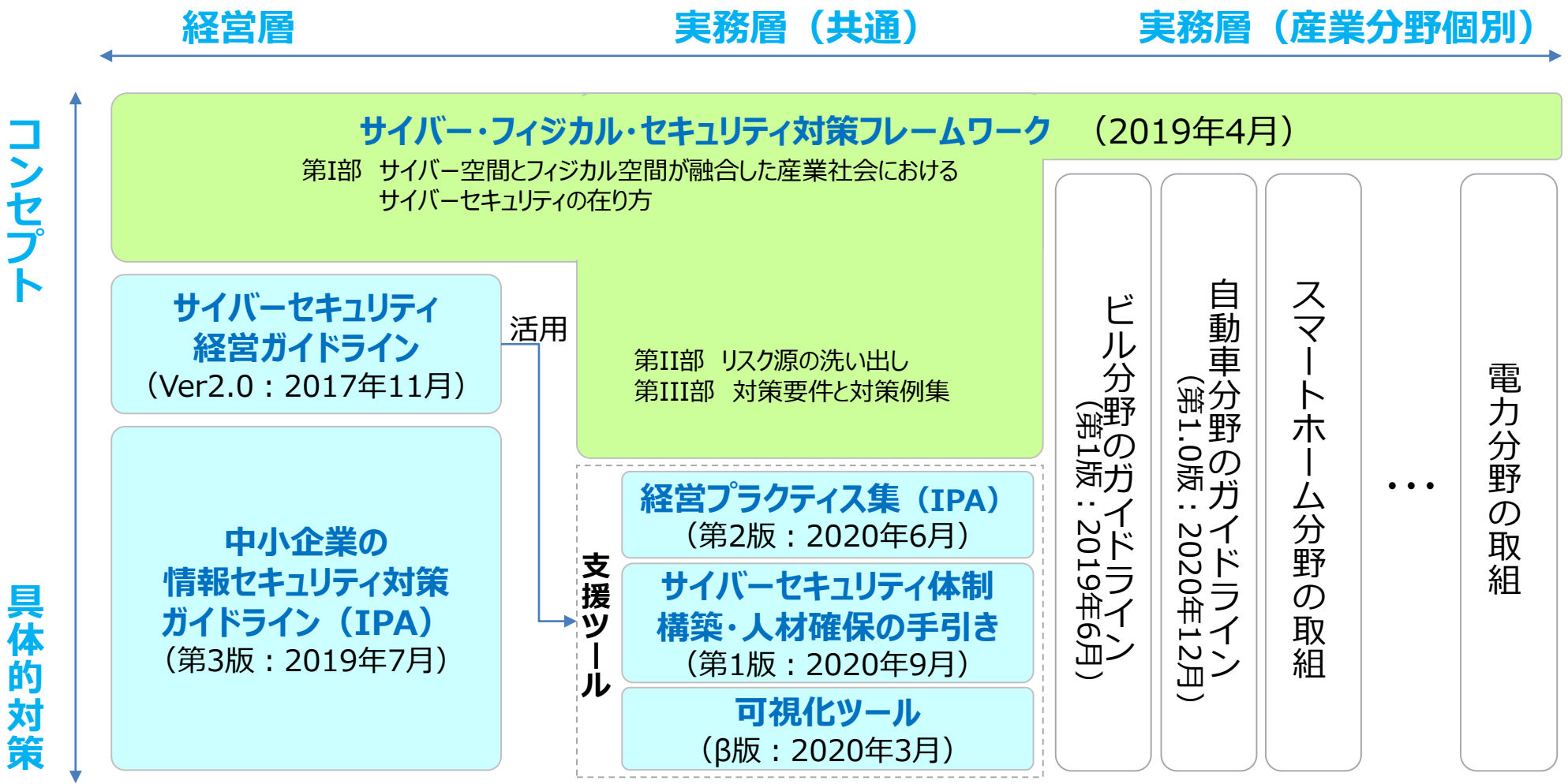
産業サイバーセキュリティ研究会関連会議の実績と予定



サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取組

- **「サイバー・フィジカル・セキュリティ対策フレームワーク」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示。**
- 全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞



１．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

２．経営

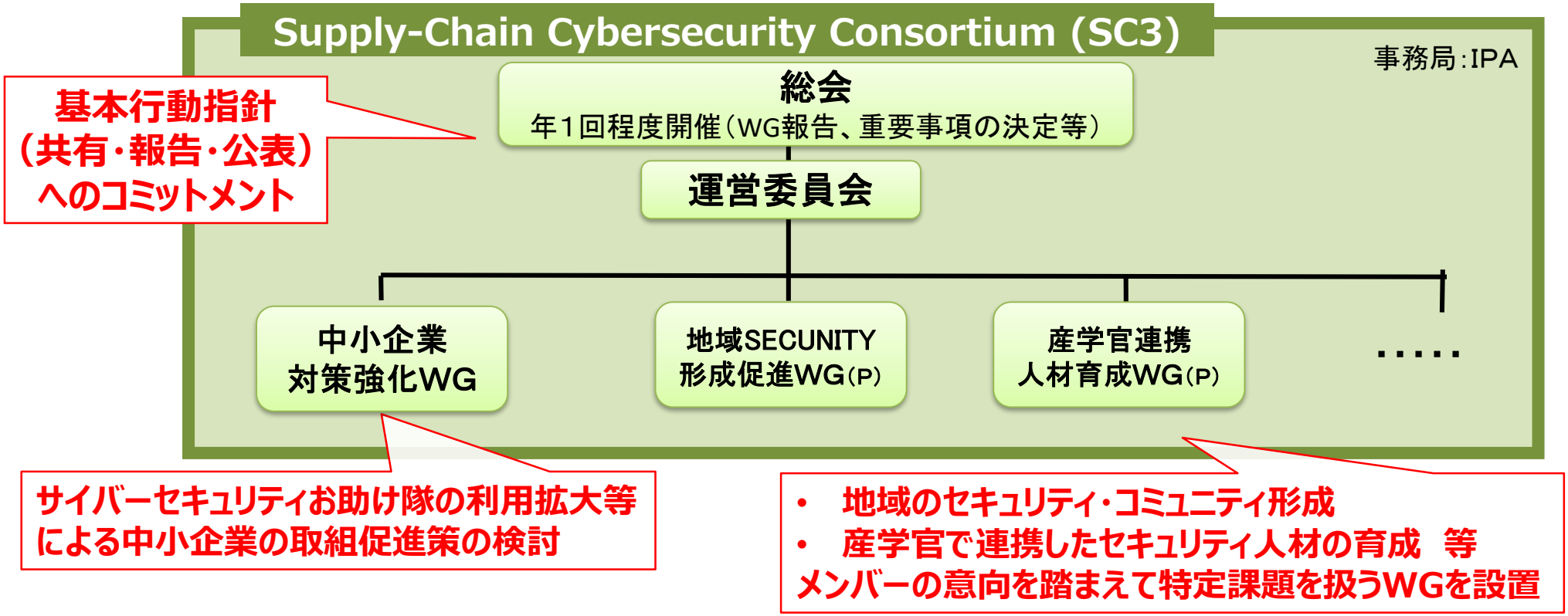
３．中小・地域

４．人材

５．国際

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

- **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（経団連、日本商工会議所、経済同友会）、業種別業界団体　等
- **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。



コンソーシアムの構成員

- 経済三団体（経団連、日本商工会議所、経済同友会）から役員が出ているほか、幅広い業界団体・個社が参加。（2021年1月末時点、90団体・76企業）

役員
- 会　長　：一般社団法人 日本経済団体連合会　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　、　公益社団法人経済同友会　副代表幹事　間下直晃氏

団体会員リスト

特定非営利活動法人 日本ネットワークセキュリティ協会
一般社団法人 コンピュータソフトウェア協会
一般社団法人 日本金型工業会
鋳型ロール会
一般社団法人 日本陸用内燃機関協会
一般社団法人 日本機械工業連合会
石油連盟
特定非営利活動法人 ITコーディネータ協会
一般社団法人 日本電子回路工業会
一般社団法人 全国地方銀行協会
一般社団法人 日本自動車工業会
日本商工会議所
一般社団法人 中小企業診断協会
一般財団法人 日本自動車査定協会
一般社団法人 日本鋳鍛鋼会
日本筆記具工業会
一般社団法人 日本ボディファッション協会
日本化学繊維協会
一般社団法人 日本金属熱処理工業会
静岡県ソフトウェア事業協同組合
一般社団法人 日本化学工業協会
一般社団法人 情報サービス産業協会
一般社団法人 全日本文具協会
一般社団法人 日本ガス協会
特定非営利活動法人 映像産業振興機構
全国商工会連合会
全国社会保険労務士会連合会
日本ドキュメントサービス協同組合連合会
一般社団法人 日本風力発電協会
日本小売業協会
電気事業連合会
一般社団法人 日本医療機器産業連合会
一般社団法人 日本航空宇宙工業会
特定非営利活動法人 みちのく情報セキュリティ推進機構
独立行政法人 中小企業基盤整備機構
一般社団法人 日本広告業協会
一般社団法人 情報処理安全確保支援士会
一般社団法人 日本電機工業会
一般社団法人 日本印刷産業連合会
一般社団法人 日本自動車部品工業会
一般社団法人 日本鉄鋼連盟
一般社団法人 ビジネス機会・情報システム産業協会
一般社団法人 太陽光発電協会
一般社団法人 日本中古自動車販売協会連合会
特定非営利活動法人 日本セキュリティ監査協会
一般社団法人 電子情報技術産業協会
一般社団法人 日本情報システム・ユーザー協会
一般社団法人 鹿児島県サイバーセキュリティ協議会
一般社団法人 日本工業炉協会
一般社団法人 日本経済団体連合会
一般社団法人 沖縄県情報産業協会
全日本フレキソ製版工業組合
一般社団法人 九州経済連合会
一般社団法人 日本金属プレス工業協会
産業横断サイバーセキュリティ検討会
一般財団法人 関西情報センター
一般社団法人 日本防衛装備工業会
四国ＩＴ協同組合
特定非営利活動法人 山梨ＩＣＴ＆コンタクト支援センター
一般社団法人 保健医療福祉情報システム工業会
せんい強化セメント板協会
一般社団法人 日本自動車機械器具工業会
一般社団法人 全国信用金庫協会
全国カレンダー出版協同組合連合会
一般社団法人 第二地方銀行協会
一般社団法人 日本損害保険協会
一般財団法人 デジタルコンテンツ協会
宮城県サイバーセキュリティ協議会
一般社団法人 中国経済連合会
一般社団法人 日本スポーツ用品工業協会
一般社団法人 日本オンラインゲーム協会
一般社団法人 長崎県情報産業協会
一般社団法人 日本レコード協会
一般社団法人 情報通信ネットワーク産業協会(CIAJ)
公益社団法人 経済同友会
一般社団法人 日本ボランタリーチェーン協会
公益社団法人 日本訪問販売協会
公益社団法人 日本マーケティング協会
一般財団法人 沖縄ITイノベーション戦略センター
公益社団法人 福岡貿易会
大阪商工会議所
公益財団法人 ハイパーネットワーク社会研究所
公益社団法人 関西経済連合会
一般社団法人 組込みシステム技術協会
一般社団法人 オープンガバメント・コンソーシアム
特定非営利活動法人 日本情報技術取引所
全国中小企業団体中央会
日本税理士会連合会
東部大阪経営者協会
一般社団法人 日本医療機器ネットワーク協会

サプライチェーン・サイバーセキュリティ・コンソーシアム設立・活動状況

- コンソーシアムが設立され、サプライチェーン全体でのセキュリティ確保に向け活動を開始。

＜2020年11月1日　コンソーシアム設立＞

- 規約に基づき、コンソーシアムが設立。

＜11月9日　第１回運営委員会開催＞

- コンソーシアムにおける情報の取扱いに関する原則、運営委員会会議規則、及び中小企業対策強化WGの設置について、審議・決定。

＜11月19日　経済三団体による共同宣言、設立総会開催＞

- 経団連、日本商工会議所、経済同友会より「サプライチェーン・サイバーセキュリティ確保に向けた共同宣言」を公表。
- YouTubeLiveによるオンライン開催で会員約290名(※)が参加し、コンソーシアム会長や梶山経産大臣からのビデオメッセージ、有識者による講演等を実施。※同時最大接続数

＜2021年2月1日　SC3会員向けウェビナー「最近のサイバー攻撃の実態と対策」開催＞

- 2020年12月18日の経済産業省の注意喚起に関連し、最新の攻撃動向に関する専門家からの解説とパネルディスカッションを実施。200名以上（最大250名以上）が視聴。

コンソーシアム　中小企業対策強化WGでの議論・検討の方向性

- 12月9日に開催した第一回WGでは、サイバーセキュリティお助け隊サービスのブランド化方針について了承いただいた。その他WGで取扱うべき議題や進め方について、委員より御意見をいただいた。

中小企業対策強化ＷＧ

- **趣旨**：中小企業のサイバーセキュリティ対策強化のために、現状の課題や官民が取り組むべき施策や方向性について幅広く検討。取組検討のためのセッションと、会員への情報共有のためのセッションの２種類のセッションを開催。

- **本WGにおいて取扱う議題案**：

①業界別のセキュリティ対策取組共有

各業種別業界団体より、サプライチェーンセキュリティ関連の取組を共有いただき、各業界で抱える課題や今後の方向性について業種間共有を図る。

②SECURITY ACTIONの次の展開

発注元企業のニーズも含むご意見をいただきながら、今後の展開について検討を行う。

③発注元企業として取り組むべき課題の整理

中小企業に対する取組の強化に加え、発注元となる企業として取り組むべき課題について整理。

ＳＣ３今後の活動方針

●今後、地域SECUNITYの形成促進や産学官で連携したセキュリティ人材の育成などの課題に焦点を当てたＷＧの設置を運営委員会で検討していくことを期待。

SC3で今後取り扱うことが期待される課題例

地域SECUNITYの形成促進

各地域におけるセキュリティ・コミュニティに関する取組のプラクティスや課題の共有により、日本各地のサプライチェーンサイバーセキュリティ対策の底上げ・強化を図る。（→詳細はP32）

産学官で連携したセキュリティ人材育成

産業界の求める人材像の共有、人材像を踏まえたカリキュラムの開発、各地域の高専等で生まれた産学官連携のプラクティスの共有を含む具体的な連携の促進などを通じ、サイバーセキュリティ分野における産学官連携での人材育成促進を図る。（→詳細はP48）

サイバー攻撃動向を踏まえた対策の検討

サプライチェーンのサイバーセキュリティを脅かすサイバー攻撃動向（例：Emotet、ランサムウェア、海外拠点経由での攻撃）を踏まえた対策を検討し、産業界全体での対策普及を図る。
（活動例：対策ガイドライン策定や注意喚起ウェビナーの開催等）

1．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

2．経営

3．中小・地域

4．人材

5．国際

「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」

●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

SC3会員向けウェビナー「最近のサイバー攻撃の実態と対策」

- 2021年2月1日、SC3会員及び団体会員の所属企業を対象としたウェビナーを開催。
- 2020年12月18日の経済産業省の注意喚起に関連し、Emotet、ランサムウェア、海外拠点経由での攻撃を題材とした著名な専門家からの解説と、視聴者からの質問にもとづくパネルディスカッションを実施。200名以上（最大250名以上）が視聴。

<プログラム>

開会挨拶：独立行政法人情報処理推進機構　参事 兼 セキュリティセンター長　瓜生 和久氏

講演１「Emotetの手口と対策」：
独立行政法人情報処理推進機構　セキュリティセンター
標的型攻撃対策グループリーダー　松坂 志氏

講演２「ランサムウェア(1)（サイバー犯罪者の傾向分析）」
株式会社エヌ・ティ・ティ・データ
エグゼクティブ・セキュリティ・アナリスト　新井 悠氏

講演３「ランサムウェア(2)（被害実態と対策）」
一般社団法人JPCERTコーディネーションセンター
早期警戒グループ　マネージャー・脅威アナリスト
佐々木 勇人氏

講演４「海外拠点を経由したサイバー侵害の実情と打開すべき課題」
株式会社サイバーディフェンス研究所
専務理事・上級分析官　名和 利男氏

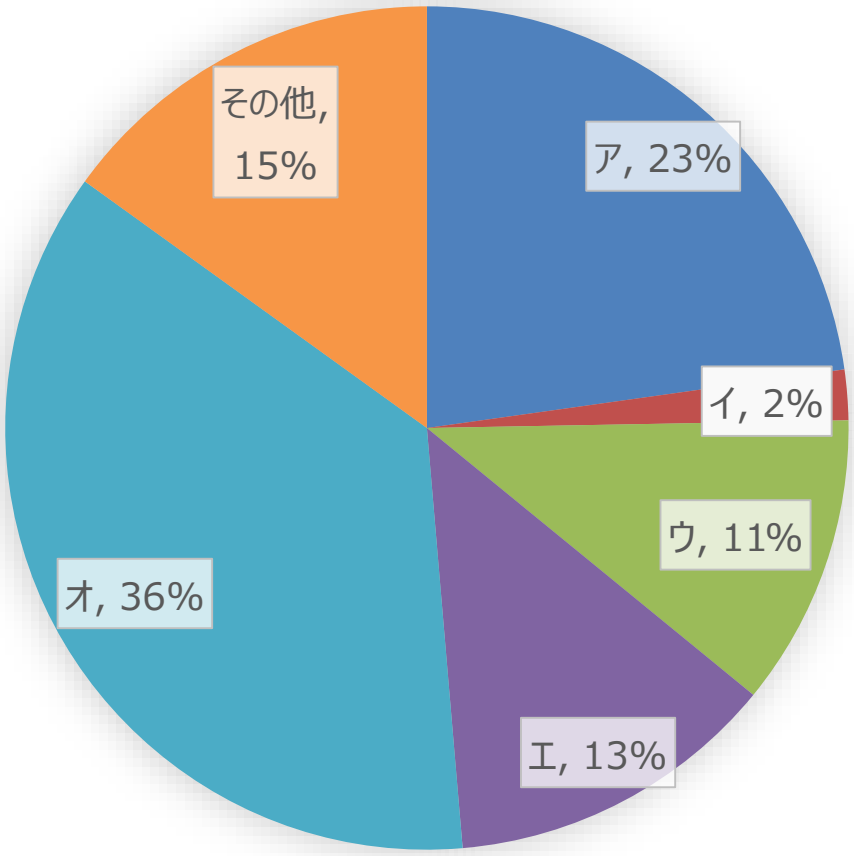
パネルディスカッション（モデレータ：経済産業省 商務情報政策局 サイバーセキュリティ課長　奥家 敏和）

パネルディスカッションの様子

ウェビナー参加者へのアンケート結果抜粋（注意喚起への対応状況）

- 注意喚起を受けた対応について、「経営者が注意喚起を読み、実務担当者に対応を指示した（しようとしている）」との回答は２割を超えたが、注意喚起を受けた対応は不明との回答が４割近くにのぼった。

注意喚起は誰が読み、どのような対応をしましたか



（回答選択肢）

ア：経営者が読み、実務担当者に対応を指示した（指示しようとしている）

イ：経営者は読んだが、実務担当者に対応を指示していない（指示するつもりはない）

ウ：経営者は読んでいないが、実務担当者が読み、経営者へ対応を提案した（提案の準備をしている）

エ：経営者は読んでいないが、実務担当者が読み、現場レベルで対応した（対応しようとしている）

オ：不明（誰がどのような対応をしたか（対応しようとしているか）不明）

カ：その他

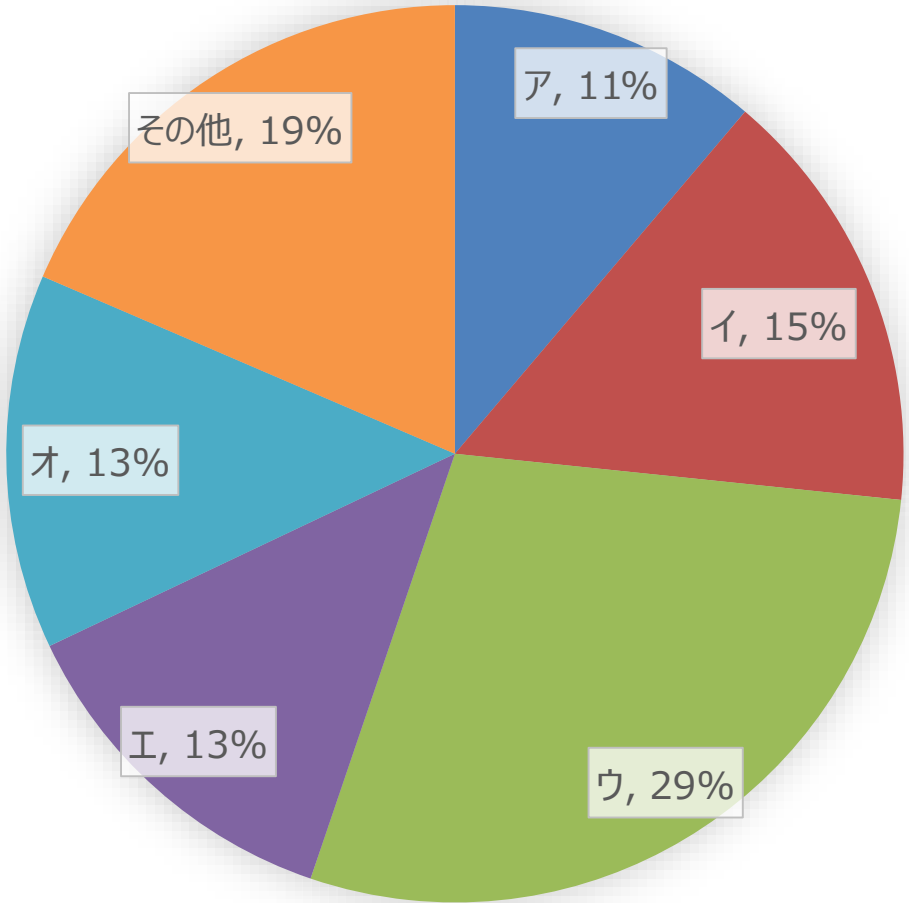
ここでの「経営者」は、CEOやCOOなど、組織全体の経営戦略・事業戦略に関わる者を指す。

有効回答数：259
※ウェビナー申込時のアンケートに基づき作成。

ウェビナー参加者へのアンケート結果抜粋（経営ガイドラインの浸透・活用状況）

- 経営ガイドラインの浸透度についても調査したところ、約3割が経営ガイドラインに沿った対策をしていると回答した一方、約３割が「一読したことはあるが、対策実施には移していない」と回答。また、ガイドライン自体の普及についても改善の余地があることが分かった。

経営ガイドラインを利用したことはありますか。



（回答選択肢）

ア：経営ガイドラインに沿った対策の実施だけでなく、「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」などの付属文書・ツールも活用している。

イ：経営ガイドラインに沿った対策を実施している。

ウ：経営ガイドラインは一読したことはあるが、対策実施には移していない。

エ：経営ガイドラインの存在は認識しているが、まだ読んだことはない。

オ：経営ガイドラインの存在も知らなかった。

カ：その他

有効回答数：259
※ウェビナー申込時のアンケートに基づき作成。

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10万件と注目度の高い状況が続いている。

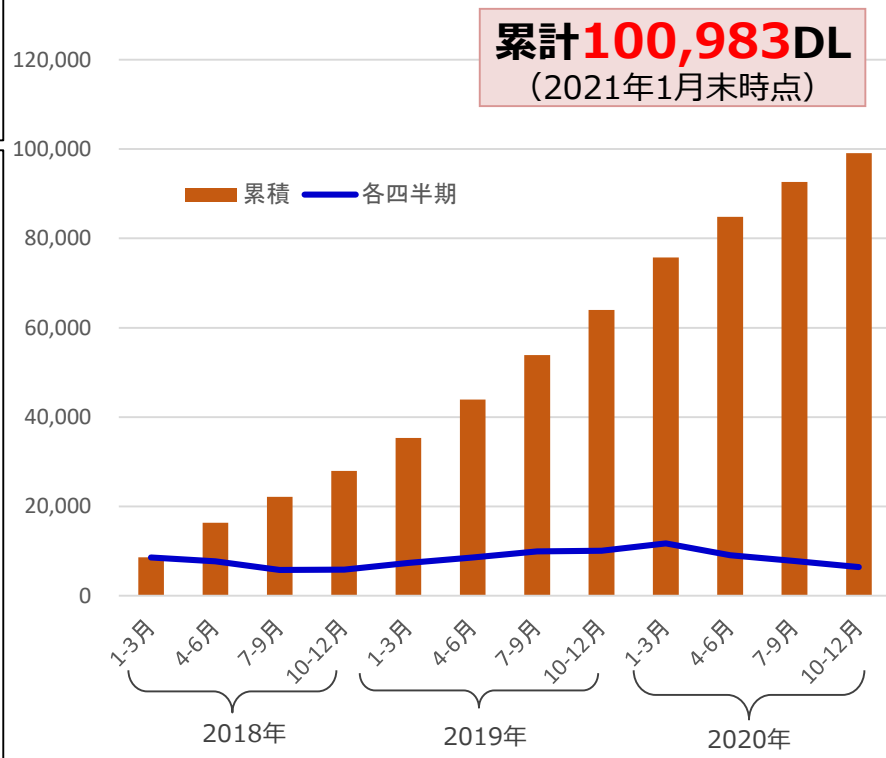
1．経営者が認識すべき３原則

（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　2,157社
第二部　488社

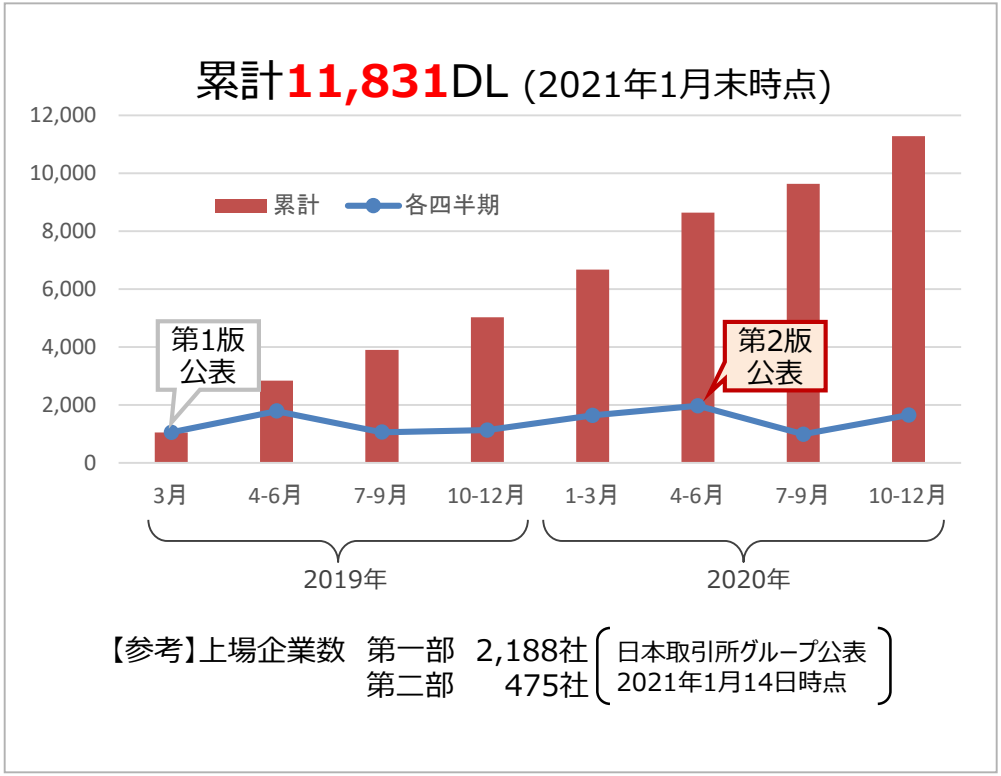
日本取引所グループ公表
2019年12月17日時点

『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**を実施中。2021年3月にIPAより調査結果を公表予定。

<プラクティス集のダウンロード数推移>



【参考】上場企業数　第一部　2,188社
第二部　475社
（日本取引所グループ公表 2021年1月14日時点）

<2020年度調査結果（速報）>

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。

サイバーセキュリティ経営ガイドラインベースの可視化ツール

2nd ～ 3rd step

- 自社の可視化、投資家等ステークホルダー向けの可視化を段階的に実現することにより、2nd step と 3rd step をつなぐ。

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

可視化ツール

- **自社内の可視化**
- **投資家等ステークホルダー向けの可視化**

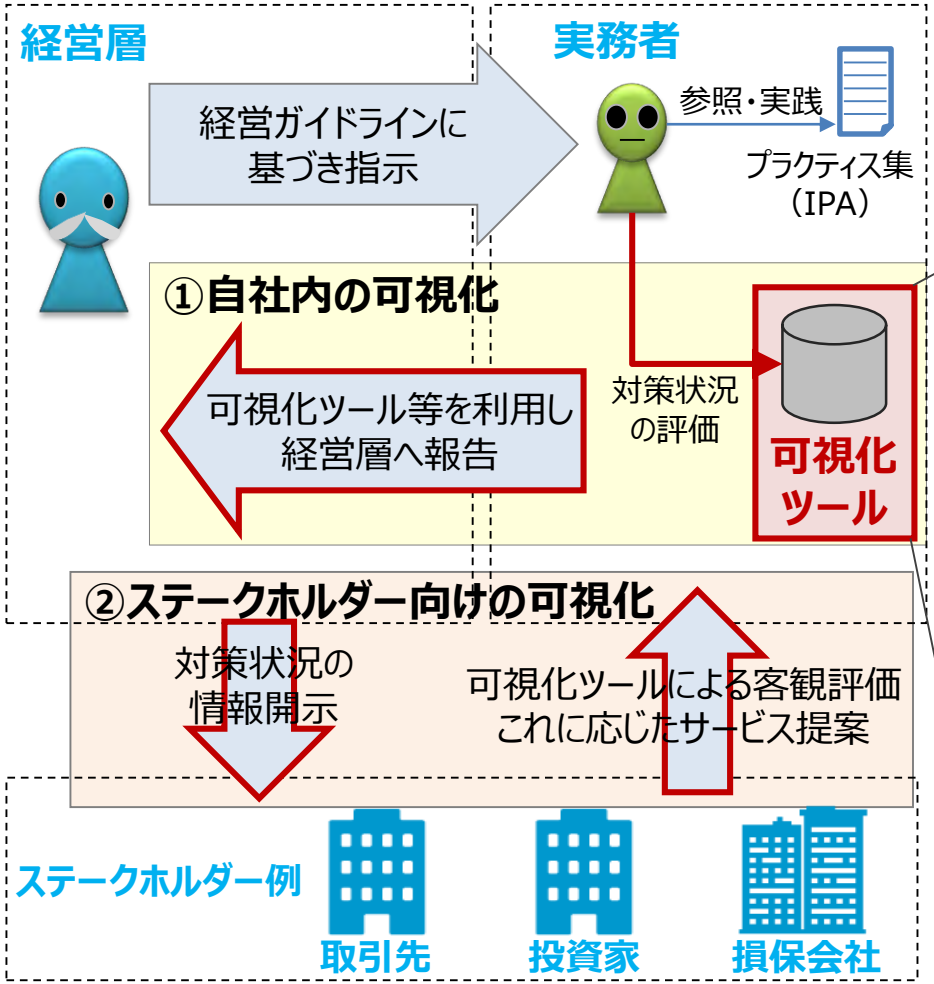
3rd Step

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

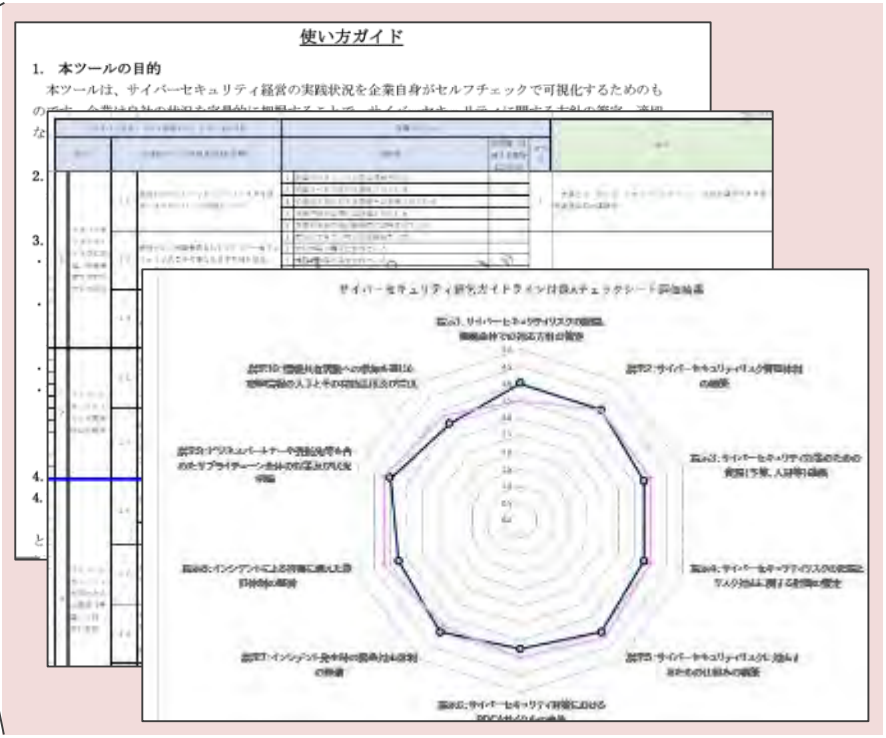
サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版を公開

- 2020年3月25日、可視化ツールβ版（Excel）をIPAから公開。
- Ver1.0（Web版）公開に向けて、今年度はユーザ企業、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。



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

今年度はβ版をベースにした調査とV1.0開発を推進

2nd ～ 3rd step

- ユーザ企業向け、ステークホルダー向けそれぞれヒアリング調査等を通じて用途と要件を明確化。Web化し、可視化ツールV1.0をリリースする。（2021年夏頃予定）

2020年3月25日	可視化ツールβ版（Excel）を公開
2020年度	**・ユーザ企業向け調査実施** - 前回WG2の後、JUASのご協力を得て**β版試行25社、インタビュー19社**実施 - 経営者⇔戦略マネジメント層⇔実務者・技術者層のコミュニケーションツールとしての利用を主たる用途と仮定し、使い方、個々の質問・選択肢等に関するご意見を収集
	・投資家等ステークホルダー向け調査実施 - JUASのご協力も得て、前回WG2から３社に追加ヒアリングを実施（**計９社**） （機関投資家２社、監査法人２社、損害保険会社２社、コンサルティングファーム３社） - 多様な立場のステークホルダーが、企業のサイバーセキュリティ対策に関してどのような情報を知りたいかを把握し、その用途に最適な可視化ツールを検討するためにご意見を収集
2021年夏頃※	可視化ツール**V1.0リリースと本格展開**

累計**4,954**ダウンロード
（2021年1月末時点）

※コロナ禍による関連業務遅延、リソース確保難等により、当初予定の2021年3月末からスケジュール変更

スケジュール

ユーザ企業及び投資家等ステークホルダー向け調査で得られた声と対応方針

- ユーザ企業、ステークホルダーともβ版に対して「抜本的な改修が必要」という意見はなし
- ユーザ企業からの声を基にβ版を改修し、V1.0としてリリース、ユーザ企業に展開する
- 同時並行で投資家等ステークホルダーにも共通言語としての活用を促していく

ユーザ企業	• 経営層とのコミュニケーション（定期報告等）に使える／使いたい • セキュリティに関する全体的な態勢・構えを見たい **⇒β版の質問構成で対応可能** • 業種・業界内比較（ベンチマーク）をしたい **⇒DB化することでベンチマーク機能を実現する** • 海外拠点等のチェックにも使いたい **⇒NIST Cybersecurity Framework (CSF) 等のグローバル標準と紐づける** • 推奨対策（で、どうすればいい？）を示してほしい **⇒プラクティス集と紐づける** • 投資家等ステークホルダーとのコミュニケーションに使いたい • その他（質問文・選択肢に関する指摘等） **⇒「備考」を「回答のヒント」に改称、ユーザがより客観的に回答できるよう記述を増強する**
投資家等 ステークホルダー	• 機関投資家からは、可視化ツールが共通言語として投資家と企業の間のリスクに関するコミュニケーション・議論に使えるとの可能性が示された • β版に対する細かな改修要望もユーザ企業と共通（ベンチマーク等） • ただし、多くの投資家はDXについて企業と話し始めた段階であり、サイバーセキュリティはその一歩先 **⇒ユーザ企業向けに可視化ツールV1.0を開発し、ユーザ企業での普及を進めながら、投資家にも同じものを将来的に利用することを促していく**

（参考）情報セキュリティ対策支援サイト（IPA）

情報セキュリティ対策支援サイト
https://security-shien.ipa.go.jp/

IPAが提供するセキュリティ関連コンテンツを集約したサイト
⇒このコンテンツの一つとして可視化ツールV1.0を追加する。

※現時点のイメージであり、今後変わる可能性があります。

（参考）Web版可視化ツールの画面イメージ

回答入力画面

結果表示画面

1．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

2．経営

3．中小・地域

4．人材

5．国際

（１）サイバーセキュリティお助け隊

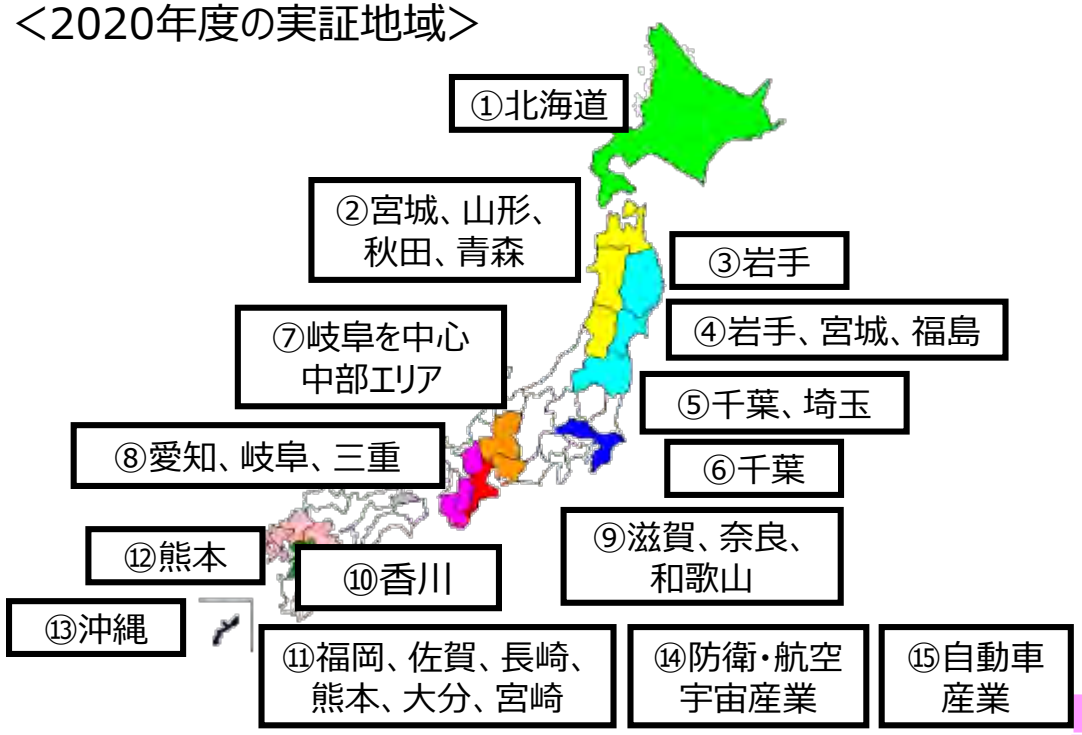
（２）地域SECUNITY

（旧称：地方版コラボレーション・プラットフォーム）

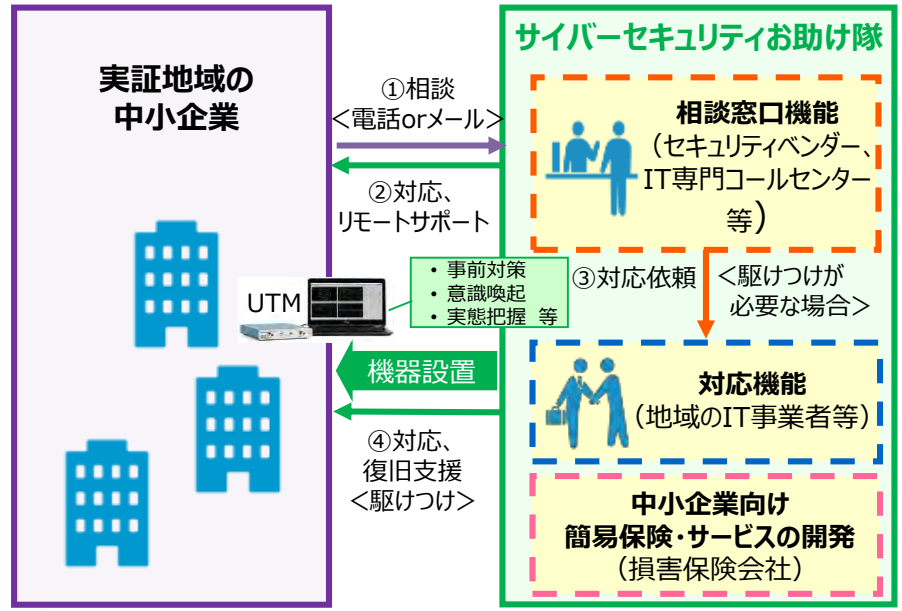
サイバーセキュリティお助け隊実証事業(2020年度)

- 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）。
- 本事業により、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティ簡易保険サービスの実現を目指す。**

＜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

（参考）サイバーセキュリティお助け隊チームリスト（2020年度）

	対象 （地域／産業分野）	実施体制 ●：実施主体）
①	北海道	●東日本電信電話株式会社 ・東京海上日動火災保険株式会社
②	宮城県、山形県、 秋田県、青森県	●東北インフォメーション・システムズ株式会社 ・ハイテックシステム株式会社 ・秋田システムマネージメント株式会社 ・あいおいニッセイ同和損害保険株式会社
③	岩手県	●富士ソフト株式会社 ・東京海上日動火災保険株式会社
④	岩手県、宮城県、 福島県	●株式会社デジタルハーツ ・損害保険ジャパン株式会社
⑤	千葉県、埼玉県	●富士ゼロックス株式会社 ・東京海上日動火災保険株式会社
⑥	千葉県	●SOMPOリスクマネジメント株式会社 ・ちばぎんコンピューターサービス株式会社 ・株式会社千葉銀行　・株式会社ラック ・損害保険ジャパン株式会社
⑦	岐阜県を中心とする 中部エリア	●MS&ADインターリスク総研株式会社 ・中部電力株式会社　・中部電力ミライズ株式会社 ・株式会社中電シーティーアイ ・三井住友海上火災保険株式会社 ・あいおいニッセイ同和損害保険株式会社
⑧	愛知県、岐阜県、 三重県	●名古屋商工会議所 ・株式会社日立システムズ ・西日本電信電話株式会社 ・東京海上日動火災保険株式会社 ・損害保険ジャパン株式会社
⑨	滋賀県、奈良県、 和歌山県	●大阪商工会議所 ・日本電気株式会社 ・東京海上日動火災保険株式会社 ・キューアンドエー株式会社

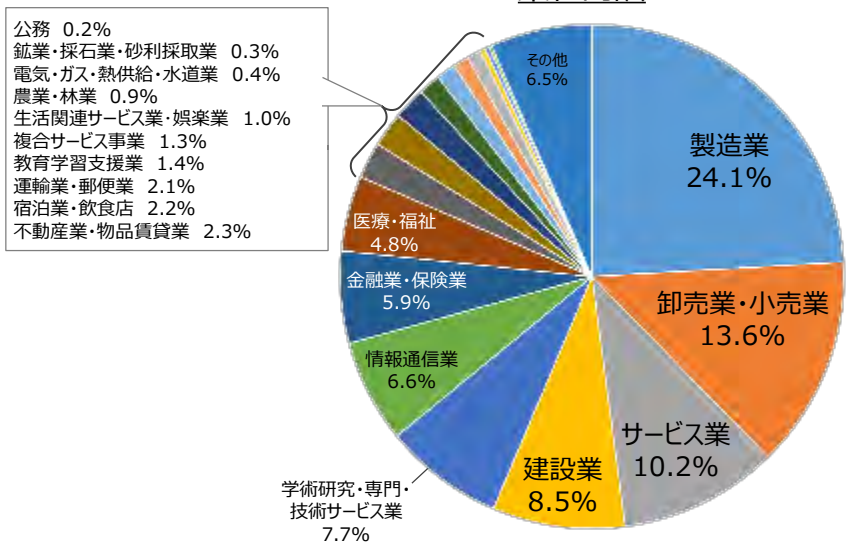
	対象 （地域／産業分野）	実施体制 ●：実施主体
⑩	香川県	●高松商工会議所 ・株式会社STNet ・西日本電信電話株式会社 ・キャノンマーケティングジャパン株式会社 ・損害保険ジャパン株式会社 ・東京海上日動火災保険株式会社
⑪	福岡県を中心とした 九州６県	●株式会社BCC ・日本電気株式会社 ・東京海上日動火災保険株式会社 ・NECフィールディング株式会社
⑫	熊本県	●西日本電信電話株式会社　熊本支店 ・株式会社くまなんピーシーネット ・東京海上日動火災保険株式会社 ・一般社団法人熊本県サイバーセキュリティ推進協議会
⑬	沖縄県	●沖電グローバルシステムズ株式会社 ・株式会社セキュアイノベーション ・ファーストライディングテクノロジー株式会社 ・那覇商工会議所 ・沖縄電力株式会社 ・損害保険ジャパン株式会社
⑭	防衛・航空宇宙 産業	●株式会社PFU ・株式会社エヴァアビエーション ・富士通株式会社 ・ウェブルート株式会社 ・損害保険ジャパン株式会社
⑮	自動車産業	●東京海上日動リスクコンサルティング株式会社 ・東京海上日動火災保険株式会社 ・エヌ・ティ・ティ・コミュニケーションズ株式会社 ・NTTコム ソリューションズ株式会社 ・NTTセキュリティ・ジャパン株式会社 ・ジェイズ・コミュニケーション株式会社

2020年度お助け隊実証事業の結果　①中小企業の実態

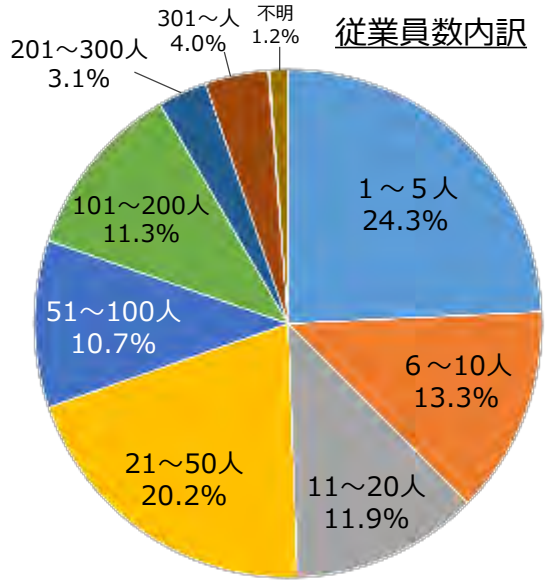
- 1,117社の中小企業が今年度の実証事業に参加。
- 昨年度の実証の結果と同様、内外に向けた不正通信等が数多く検知されるとともに、中小企業の実態や課題が浮き彫りに。

2020年度実証参加中小企業の内訳

業種内訳



従業員数内訳



- 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。

商用化においては、コストとの見合いでどこまできめ細かにサポート出来るかが課題。

2020年度お助け隊実証事業の結果　②リモート対処事例

- コロナ禍において、できる限り**リモートでの対処**を実施。

事例１	EDRサービスでブラウザハイジャッカーを確認。駆除方法を案内したが中小企業が自力で対応出来なかったため、お助け隊が**リモートで駆除実施**。
事例２	UTM設置後、**C&Cコールバックとみられる通信を検知**。コールセンターより対象の中小企業に連絡。該当端末は買替となり、その後アラートが出ていないことを確認済み。
事例３	UTMサービスを導入した企業において**「不正なIPアドレスへの通信」**が成立していることが確認されたため、緊急度「高」のアラートを発報し、支援を実施。
事例４	UTMがトロイの木馬を検知。中小企業から相談を受け、お助け隊事業者がリモート支援を実施。**フルスキャンの結果、内在していた別リスクを駆除**。
事例５	**「アドウェア感染」**や、**「フィッシングサイトへのアクセス」**を検知し、対象中小企業と連携の上、リモートでの対処を実施。

2020年度お助け隊実証事業の結果　③産業別実証での気づき

- 2020年度は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。

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

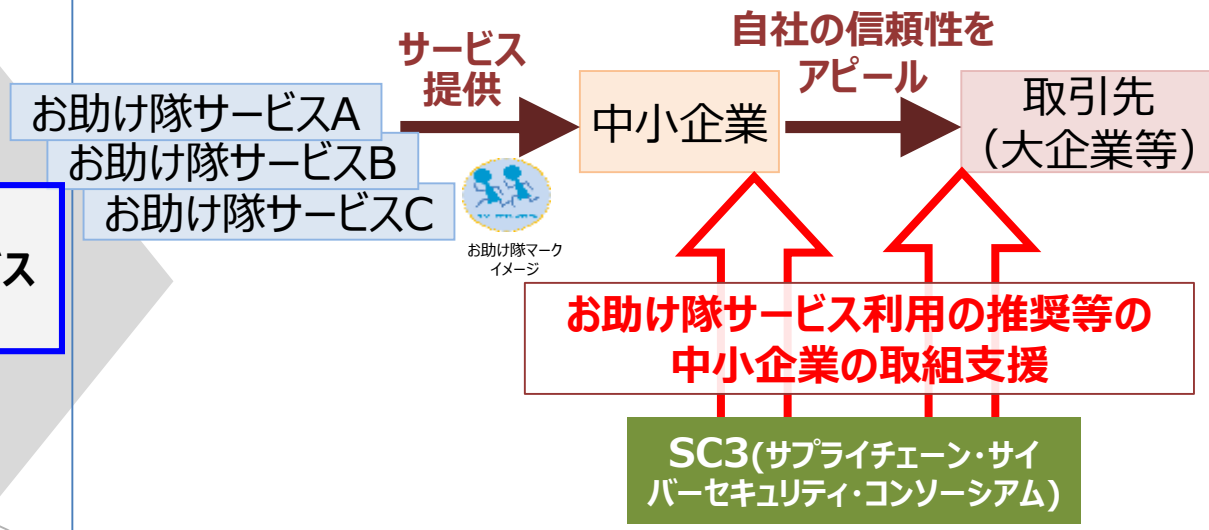
- 産業別実証事業は、「自動車産業の中小企業サプライヤーを対象とした実証」と、「防衛・航空宇宙産業に関わる中小企業及び今後防衛・航空宇宙産業に参入を検討する中小企業を対象とした実証」を実施。

実証事業から民間サービスへの移行・普及促進に向けたステップ

- 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より公開予定。
- 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。



→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）お助け隊サービス基準の概要

大項目	小項目	内容
要件	相談窓口	お助け隊サービスの導入・運用中に関するユーザからの各種相談を一元的に受け付ける窓口を設置すること
	監視の仕組み	・ユーザのネットワークを24時間監視し、攻撃を検知・通知する仕組み（UTM等のツールと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時間監視し、攻撃を検知・通知する仕組み（EDR等のツールと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	・営業エリア内であればユーザの指定する場所に技術者を派遣できること ・サービス規約等でユーザと合意した範囲であればリモート対応でも可
	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 例：・マニュアルに書かれている通りに数回クリックするだけでインストール完了
	中小企業でも導入・維持できる価格	・月額1万円以下（税抜き）（条件付きで可。PC〇台までなら等） ・最低契約年数は2年以内 ・初期費用、契約年数等の細かな条件も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保証するサイバー保険が付帯されていること。
	上記機能のワンパッケージ提供	ユーザがお助け隊サービスを購入したり、利用中の問合せ等を行う窓口が一本化されていること（営業窓口と技術支援窓口は別でも可）
	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の深いレベルの情報共有に合意し、そのための準備を行うこと
	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（地場のITベンダーは中小企業が多いことも考慮し、緩めの条件とする。）
	更新	2年毎に更新審査を受けること
附則 （推奨事項他）	独自のオプションサービス提供	例：・事前アセスメント等の簡易コンサルティングサービス ・端末監視の仕組み ・デジタルフォレンジック等より広い範囲をカバーするサイバー保険の提供 等
	日本発の技術・製品の活用	日本特有の攻撃に対応するため

（１）サイバーセキュリティお助け隊

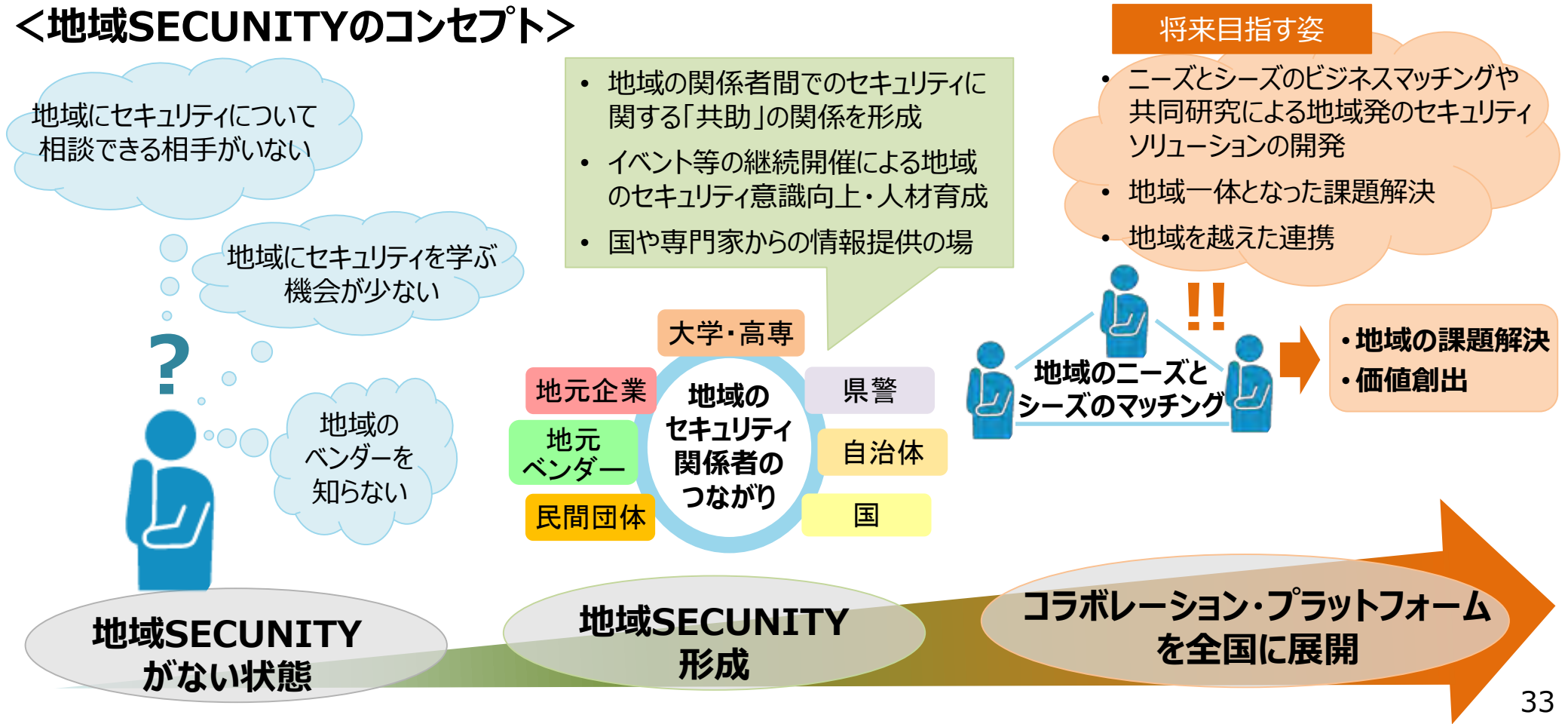
（２）地域SECUNITY

（旧称：地方版コラボレーション・プラットフォーム）

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①（北海道）

- 平成26年9月、**経済産業局、総合通信局、道警察の3者が連携し、全国に先駆けて「北海道地域情報セキュリティ連絡会（HAISL）」を発足。**道内の情報セキュリティ推進機関として、普及啓発や人材育成等を実施。
- 令和2年度は、サイバーリスクの理解促進に向けた取組を展開したほか、**大学・高専等と連携した人材育成プロジェクト「SC4Y」の始動**など、HAISLの取組を強化・拡充してサイバーセキュリティ普及を強力に推進。

道内中小企業のサイバー対策の現状

4割以上（41.6%）が
「経営者等の危機意識が低い」

3社に1社（90社）
サイバー攻撃の被害に

専門人材不足が浮き彫りに
41.6%（117社）
「対策できる人材がいない」

道内全域対象の
初の実態調査

普及啓発

☆情報セキュリティセミナー
中小企業等におけるサイバーリスクに対するリテラシー向上を目的に、DX with Cybersecurityに関する講演のほか、セミナーでは初となるサイバー攻撃演習を実施。(12/1)

☆Security College for Youth(SC4Y)
複数の道内教育機関等と連携し、学生向け教育カリキュラムを試行。
(勉強会：8/29、11/28、2/10、2/28)


定期的な勉強会の実施
（段階的に知識を身につける）


競技会やCTF等への参加
（研鑽した力を試す）

人材育成

令和２年度地域SECUNITY形成促進の取組①（東北）

- 地域におけるセキュリティコミュニティの形成に必要なキーパーソン、地域団体、登録セキスペへのアンケート、ヒアリングを含めた実態調査、セキュリティ対策強化に向けたモデル事業（企業に対する個別指導）やセキュリティに係る知識の向上、人材育成を図るスキルアップイベント等の実施、検証を行い、セキュリティコミュニティの形成を促進。

１．地域のキーパーソン等発掘調査

○東北地域におけるセキュリティノウハウ・スキルを持ったキーパーソンなど、継続的に活動できる地域セキュリティコミュニティの活動人材の発掘、管内セキュリティベンダーを把握するため、東北各県の大学、企業、自治体等に３０件程度のヒアリング調査を実施。

２．中小企業に対するセキュリティに関する意識調査

○東北地域の中小企業を対象に、セキュリティに関する課題や要望、予算額や各種外部認証取得を含めた取組状況、デジタル化の進捗、取組状況などの実態について約2,000社へアンケートを調査を実施。

３．登録セキスペ及び中小企業のセキュリティに関する活動調査

○東北地域に所在する登録セキスペに対し、中小企業支援の観点からの活動内容等をアンケート及びヒアリングにて実情や課題等を把握するとともに、地域中小企業のセキュリティ対策の向上に向けて連携出来る登録セキスペを発掘する。
○２．のアンケート回答に基づき、セキュリティ強化活動の取組状況の詳細について、中小企業５０社程度へヒアリングを実施。

４．地域関係機関との連携による相談対応

○東北地域の各種機関が開催する関連イベントと連携し、イベント参加者等に対するセキュリティに係る出張相談を６回実施。

５．セキュリティ関連スキルアップイベントの開催

○企業・組織のセキュリティ担当者や、セキュリティ技術に興味がある社会人・学生を対象に、「学びの場」としてセキュリティに関する講演、「腕試しの場」としてクイズ形式で行う、セキュリティに係る知識の向上、人材育成を図るイベントを３回実施。

６．中小企業セキュリティ対策支援モデル事業

○３．のヒアリング結果に基づきモデル企業３社を選定し、情報セキュリティ関連規程の策定支援等の個別指導を行いつつ、セキュリティ対策実施企業や支援者それぞれの課題を抽出し、今後の効果的な支援に結びつけるための対策を検討。

７．報告書取りまとめ

令和２年度地域SECUNITY形成促進の取組①（関東）

- 関東局管内における地域コミュニティ形成に向けた第一歩として、今年度は**千葉県をモデル地域**とし、地域中小企業の実態調査から、支援者検討会の開催、ユーザー企業向け説明会などの取組を実施（事務局：特定非営利活動法人ITコーディネータ協会／ちば経営応援隊）。

  ⇒ 来年度以降、本取組を管内他地域にも広げ、広域な地域コミュニティ形成を進める予定。

地域支援機関等による検討会

●メンバー

①明治大学　岡田教授
②千葉県よろず支援拠点
③公益社団法人千葉県産業振興センター
④千葉県商工会議所連合会
⑤千葉県商工会連合会
⑥千葉県中小企業団体中央会
⑦千葉銀行
⑧千葉信用金庫
⑨NPO法人ちば経営応援隊
⑩公益社団法人千葉県情報ｻｰﾋﾞｽ 産業協(CHISA)
⑪横展開先関係者（茨城県、長野県）

●オブザーバー

千葉県、IPA、関東総合通信局、
サイバーセキュリティお助け隊実施事業者

活動内容

- 地域企業への実態調査アンケートは検討会メンバーと連携し234社から回答。
- 普及啓発セミナーと横展開セミナーは、オンライン開催し、アンケート結果の内容や中小企業が対応すべきセキュリティ対策について紹介（全4回、各回50名程度）また、講演の様子はアーカイブでHPに掲載。（https://www.itc.or.jp/security-com/video.html）
- 検討会ではIPAや事務局等から支援施策や取組情報を共有しつつ、これらの情報を踏まえ地域企業に対しどのように普及させていくか金融機関や地域支援機関と検討を実施。
- 地域企業の個別相談の事例をとりまとめ、今年度の千葉県での取組の情報共有と併せて管内自治体担当者会議にて発表予定。
- 今後は、よりユーザー目線で取り組むべく、ユーザー企業も検討会に参加するよう働きかけるなど、コミュニティ活性化に向けて検討を進めるとともに、管内他地域への横展開を進める予定。

令和２年度地域SECUNITY形成促進の取組①（中部①）

- 最新のサイバー攻撃に関する知識の共有やサイバーセキュリティ対策の不備に対する問題意識の醸成、また、有効な対応力の習得等に資するよう

(1)地域サイバーセキュリティに関する課題の抽出
(2)課題解決策の検討、実施　例）セミナー開催などによる普及啓発活動、サイバーセキュリティ演習事業

などを行い、東海地域の中小企業のサイバーセキュリティ対策の質の向上を図ることを目的とした「東海サイバーセキュリティ連絡会」を総務省東海総合通信局と共同で設置。第１回を８月に、第２回を１月に開催した。

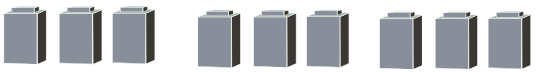
連絡会の活動イメージ

構成員間の
・セキュリティ対策
・インシデント情報
の共有

東海サイバーセキュリティ連絡会
（事務局：東海総合通信局・中部経済産業局）

セキュリティ対策
インシデント情報の
共有

セミナーの開催



中小規模の企業

構成員

- 地方公共団体：岐阜県、静岡県、愛知県、三重県
- 警察本部：岐阜県警、静岡県警、愛知県警、三重県警
- サイバー関係機関等：国立研究開発法人情報通信研究機構（NICT)、（株）ラック
- 通信事業者：西日本電信電話（株）、中部テレコミュニケーション（株）、（株）NTTドコモ、KDDI（株）、ソフトバンク（株）
- 放送事業者・団体：日本放送協会、（株）CBCテレビ、日本ケーブルテレビ連盟
- エネルギー事業者：中部電力（株）、東邦ガス（株）
- 自動車会社：トヨタ自動車（株）
- 経済団体等：名古屋商工会議所、（一社）中部経済連合会、（独）情報処理推進機構、デロイトトーマツサイバー（同）、MS＆ADインターリスク総研（株）
- 有識者：渡辺研司名古屋工業大学教授

令和２年度地域SECUNITY形成促進の取組①（中部②）

- 中部地域におけるセキュリティ実態調査

ヒアリング先一覧（２０２１年１月時点）
IoT、AI等の導入が進んでいると考えられる中小製造業を中心に１９社ヒアリングを実施。

調査企業業種

【愛知県】
・自動車向け金属部品製造業
・自動車、一般機械部品製造業
・一般機械部品製造業
・内装用シートカバー製造業
・自動車向け金型プレス

【岐阜県】
・金型設計、製造
・鋳物加工
・陶磁器製造業
・自動車向け金属プレス
・金型設計製作・プレス加工

【三重県】
・銑鉄鋳物業
・医薬品製造業
・一般機械製造、工具
・電子回路設計

【石川県】
・通信機器部品製造
・機械　輸送用機器

【富山県】
・建築用部材、車両用部材製造
・板金加工業
・産業用、一般機械部材製造

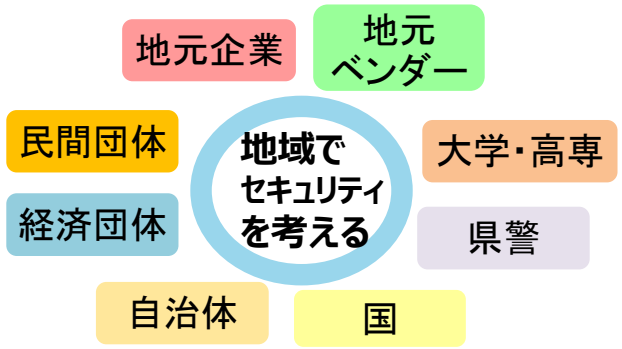
＜課題点＞

- 基本的に情報システム部＝セキュリティ専属の担当者はいない
- セキュリティに対する意識はあるが、ウイルスソフトやUTM以外の対策を取っているところはあまりない
- 社長もしくは経営に意見を言える副社長レベルの役員が、セキュリティに対する重要性を認識しているところほど独自の対策をしており、そうでないところは上記以外の対策はしていない
- 情報資産の特定ができておらず、情報流出を脅威に感じていない
- マルウェア感染などは経験があるが、実害がないという判断からその後の対策はあまり強化されていない
- 社内ルールやポリシーとして明記しているところはほとんどないが、今後BCPとしてセキュリティも設定しようという動きはある
- どこまでセキュリティ対策すればいいのか、他社と比べてどうなのか、国からしっかり指針だして欲しい

令和２年度地域SECUNITY形成促進の取組①（近畿）

- サイバーセキュリティ月間（2月1日～3月18日）に近畿２府５県（福井、滋賀、京都、大阪、兵庫、奈良、和歌山）でサイバーセキュリティの取組機運向上及び域内関係者間のつながりを深めることを目的としたセミナーや、企業のセキュリティ・マネジメントの重要性を紹介する資格取得促進セミナーを開催。
- 地域セキュリティコミュニティの活動支援、情報発信や、サイバーセキュリティ相談窓口の情報発信に加え、サイバーセキュリティ実態調査を実施。

地域の関係者の掘り起こし



地域のセキュリティ関係者が一堂に会する「サイバーセキュリティ地域別セミナー」
2/9(火)和歌山、2/26(金)奈良を皮切りに、3月は滋賀、京都、大阪、兵庫、福井で開催!

困り事、悩みの相談・共有

【相談窓口】
・よろず支援拠点
・大阪商工会議所
・情報処理推進機構
・府県警察本部　など

【セキュリティコミュニティ】
・総サイLT
・OWASP Kansai
・tktkセキュリティ勉強会

「サイバーセキュリティ相談窓口」
「地域セキュリティコミュニティ」

セキュリティコミュニティづくり

「地域セキュリティコミュニティ支援事業」
近畿圏に所在する企業・個人等が実施するサイバーセキュリティ関連の勉強会・研究会などのコミュニティ活動を支援！

【支援内容】
コミュニティ活動にかかる、会場費、講師謝金旅費、PR資料作成費用など

令和２年度地域SECUNITY形成促進の取組①（中国）

- 中国地域の企業や自治体、団体等との間で、サイバーセキュリティに関する情報を共有することにより、中国地域におけるセキュリティ対策の充実を図るため、「中国地域サイバーセキュリティ連絡会」を設立。（関係91機関）
- 構成員間の情報共有や、セミナー・演習等の共同開催のほか、今年度は中国経済連合会及び３大学と連携し、VOD教材による社会人セキュリティ人材育成研修を実施。

中国地域サイバーセキュリティ連絡会

【設　立】令和２年10月9日
【事務局】中国経済産業局、中国総合通信局
【構成員】※設立日時点
参加機関（中国地域５県、２政令市、通信・放送事業者、金融機関、業界団体、産業支援機関、大学等）76機関
連携機関（国の出先機関、NICT、IPA等）15機関

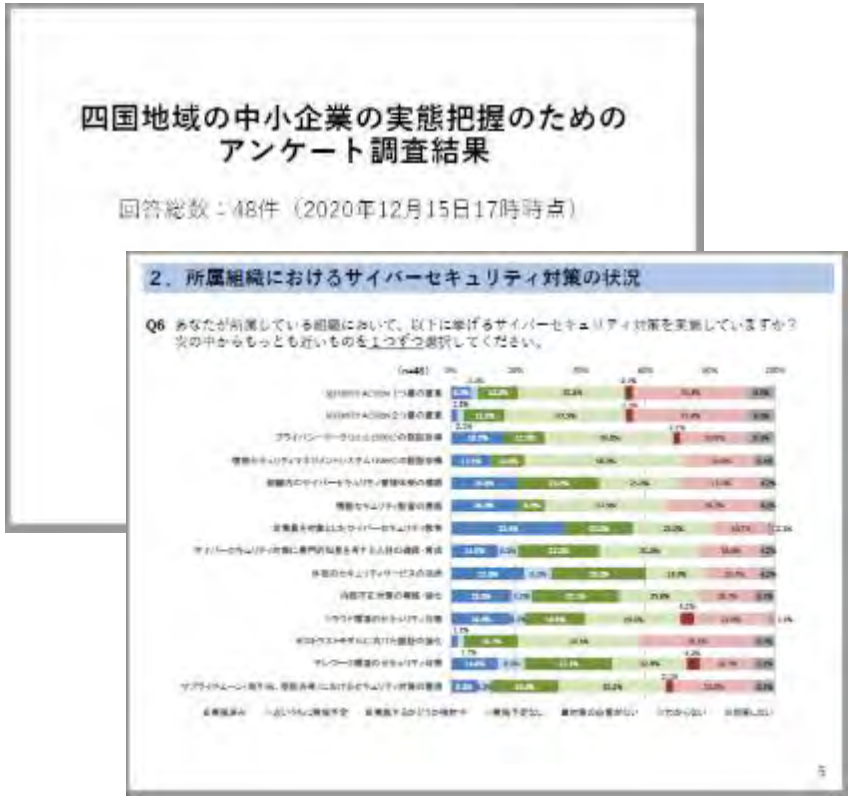
サイバーセキュリティ連絡会設立記念セミナー（会場・オンライン併用）

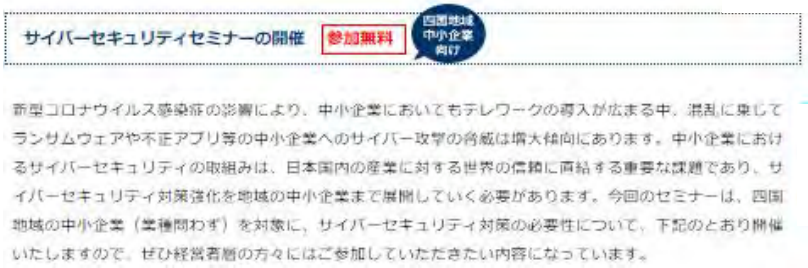
←人材の育成・確保が課題。
中国経済連合会と連携し、岡山大学、広島市立大学、大阪大学のVOD教材を活用した研修を実証的に実施。

サイバーインシデント対応勉強会
（R2年11月@広島市）
↓

令和２年度地域SECUNITY形成促進の取組①（四国）

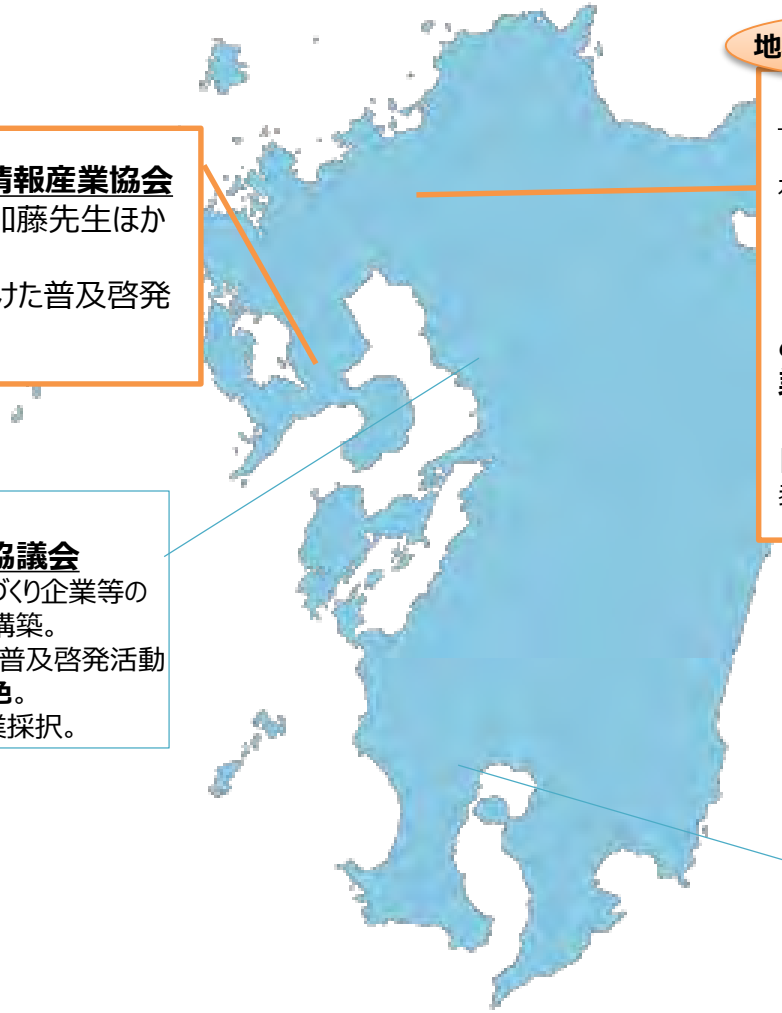
- 産学官によるセキュリティ関連関係者会議を設置。
- 四国地域の事業者に対し、実態把握のためのアンケート調査を実施。
- アンケート結果を踏まえ、県警を講師に中小企業向けサイバーセキュリティセミナーを開催。





令和２年度地域SECUNITY形成促進の取組①（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。

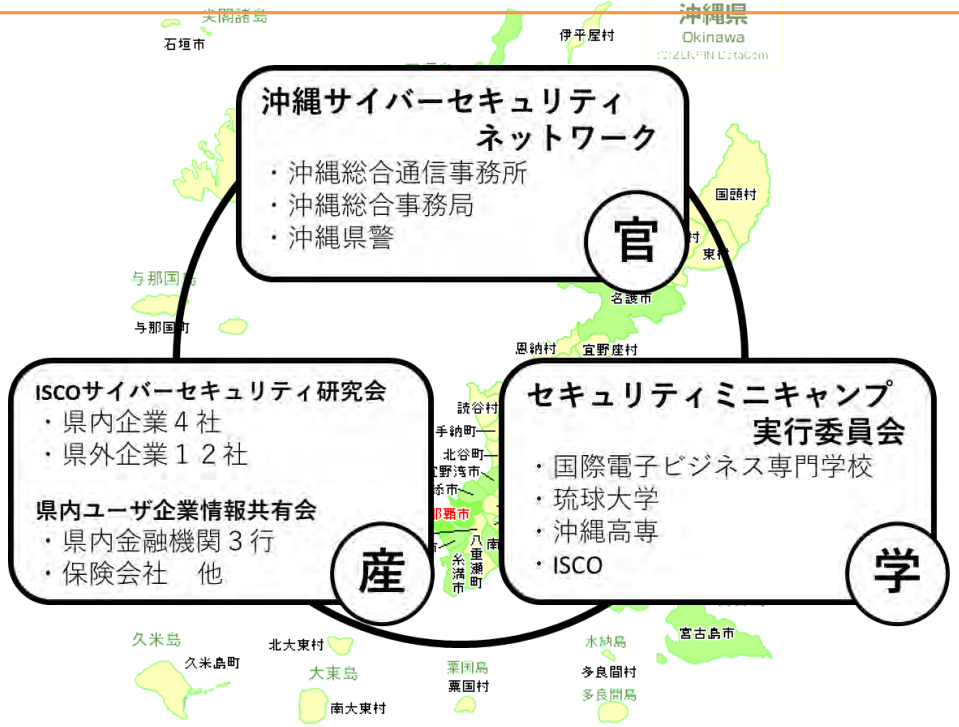
【参考】
鹿児島県サイバーセキュリティ協議会
会員企業向けに技術勉強会やセミナーを定期的に開催。
IT業界や自治体、県警、学校とのネットワークも構築し、サイバーセキュリティ対策の普及啓発に向けた働きかけも積極的実施。

令和２年度地域SECUNITY形成促進の取組①（沖縄）

- 沖縄サイバーセキュリティネットワーク（2015年3月発足）など既存の産学官のセキュリティ関連ネットワークを有機的に連携。
- 沖縄地域の自治体、事業者に対し、実態把握のためのアンケート調査を実施し、これを踏まえたセキュリティに関するセミナー開催、相談窓口設置などセキュリティ対策を検討。

【実施団体】沖縄ITイノベーション戦略センター（ISCO）
地域SECUNITY事業では、リテラシー向上のためのセミナー等を行い、様々な事業と連携した取組を展開。
・セキュリティビジネス創出のための研究会や、金融機関等との情報共有会、若手人材の発掘・育成のためのセキュリティミニキャンプを開催し、情報セキュリティマネジメント等の資格取得支援を実施。
・セキュリティ研究会の参加企業は、サイバーセキュリティお助け隊事業を活用して実証事業を検証中。

※自治体向けセキュリティセミナーは、ResorTech Okinawa（国際IT見本市）において、コロナ感染対策を考慮してWEBとの併用で開催。
中小企業向けセミナーは２月にWEB開催で予定。



2021年1月26日公開資料

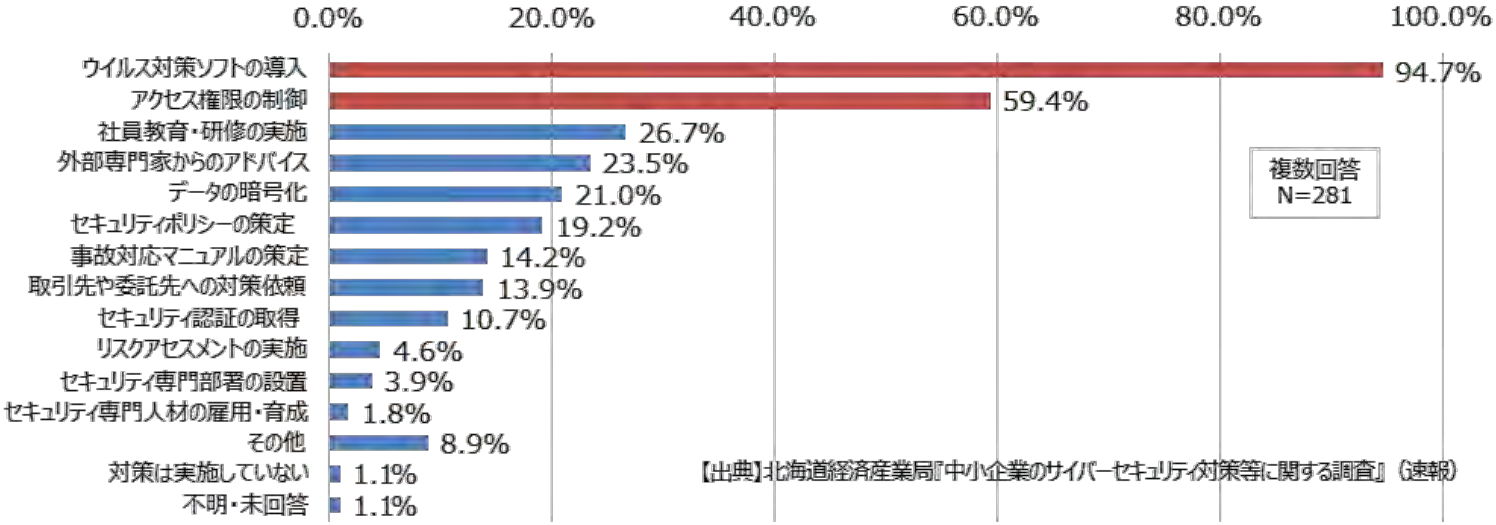
令和２年度地域SECUNITY形成促進の取組②

- 各経済産業局において、各地域の企業を対象としたサイバーセキュリティに関する実態調査を実施

サイバーリスクへの対策状況

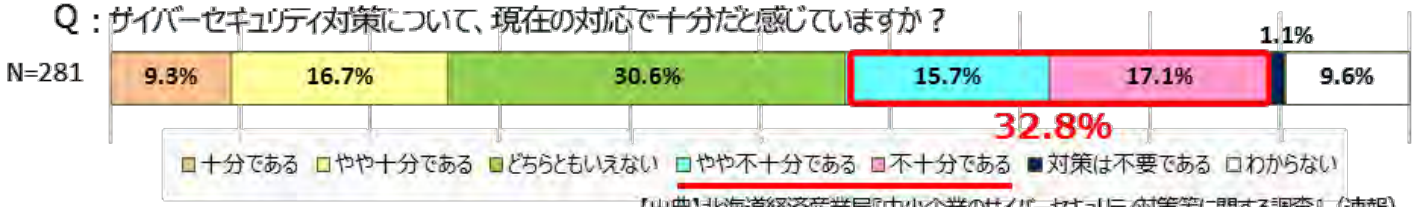
- サイバーセキュリティ対策として、「ウイルス対策ソフトの導入」（94.7%）が最も多く、次いで「アクセス権限の制御」（59.4%）など、**大半の企業でセキュリティ対策を実施済み。**（「対策は実施していない」と回答した企業は1.1%）
- 一方、**自社の対応を「不十分・やや不十分」と感じる企業が3割以上（32.8%）を占める。**

Q：実施済みのサイバーセキュリティ対策は何ですか？



【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』（速報）

Q：サイバーセキュリティ対策について、現在の対応で十分だと感じていますか？



【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』（速報）

2021年1月26日公開資料

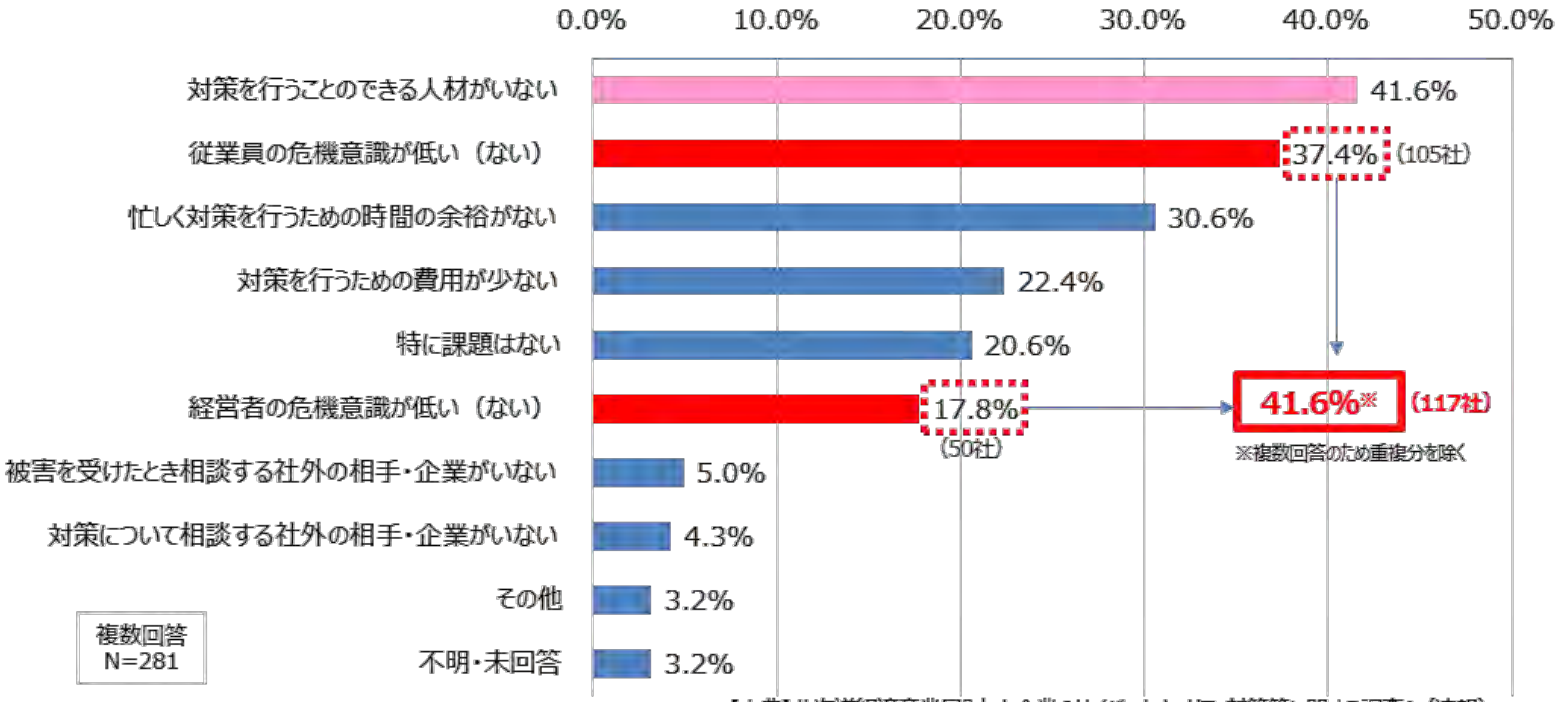
令和２年度地域SECUNITY形成促進の取組②

- 各経済産業局において、各地域の企業を対象としたサイバーセキュリティに関する実態調査を実施

サイバーセキュリティに関する課題

- サイバーセキュリティに関する課題について、4割以上の企業が「対策を行うことのできる人材がいない」と回答しており（41.6%）、**セキュリティ分野の人材不足が浮き彫り**となった。
- また、「経営者・従業員の危機意識が低い」と回答した企業も多く（41.6%）、**経営者・従業員の意識醸成の必要性も明らかになった。**

Q：サイバーセキュリティに関する課題は？



【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』（速報）

セキュリティコミュニティ形成のためのプラクティス集

- 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

今年度の取組を踏まえた来年度の取組方針（案）

- 今年度の地域SECUNITY活動を進めていく中で課題も出てきた。

今年度の地域SECUNITY活動を進めていく中で出てきた課題例

- セキュリティの相談については各地域で信頼できる関係者へというのがセキュリティの世界の特徴であるが、そもそも地元で相談できるようなセキュリティ人材が不足。今後、セキュリティの取組の中心になるようなセキュリティの人材を地域全体で育成していく必要がある
  ⇒ **地域における産学官連携人材育成の在り方を検討が必要**
- 特に新たにコミュニティを形成するにあたっては、どうしても対面でのコミュニケーションが必要になってくるが、**コロナ禍におけるコミュニティの在り方について議論が必要**

各コミュニティが手探りで進め方を検討する中で、全国規模で以下の取組を進めていく必要がある
① 広く関係者・関係機関が連携・協力し、理想的な地域セキュリティ・コミュニティの在り方の検討
② コミュニティ形成・活動にあたっての課題及びその解決策の議論
③ 各地の活動への業界団体・事業者や地域の団体の積極的な参加・役割の明確化等

来年度の取組方針（案）

- 地域の団体・業界団体が多く参加するSC３において、**地域SECUNITYの形成を促進するWG**を立ち上げ、各地域の取組に関する情報共有を中心に実施することも一案。
- 上記①～③を含む課題についても検討を行い、各地のコミュニティ活動の取組に反映することで、地域SECUNITYの形成及び活動を推進していく。

1．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

2．経営

3．中小・地域

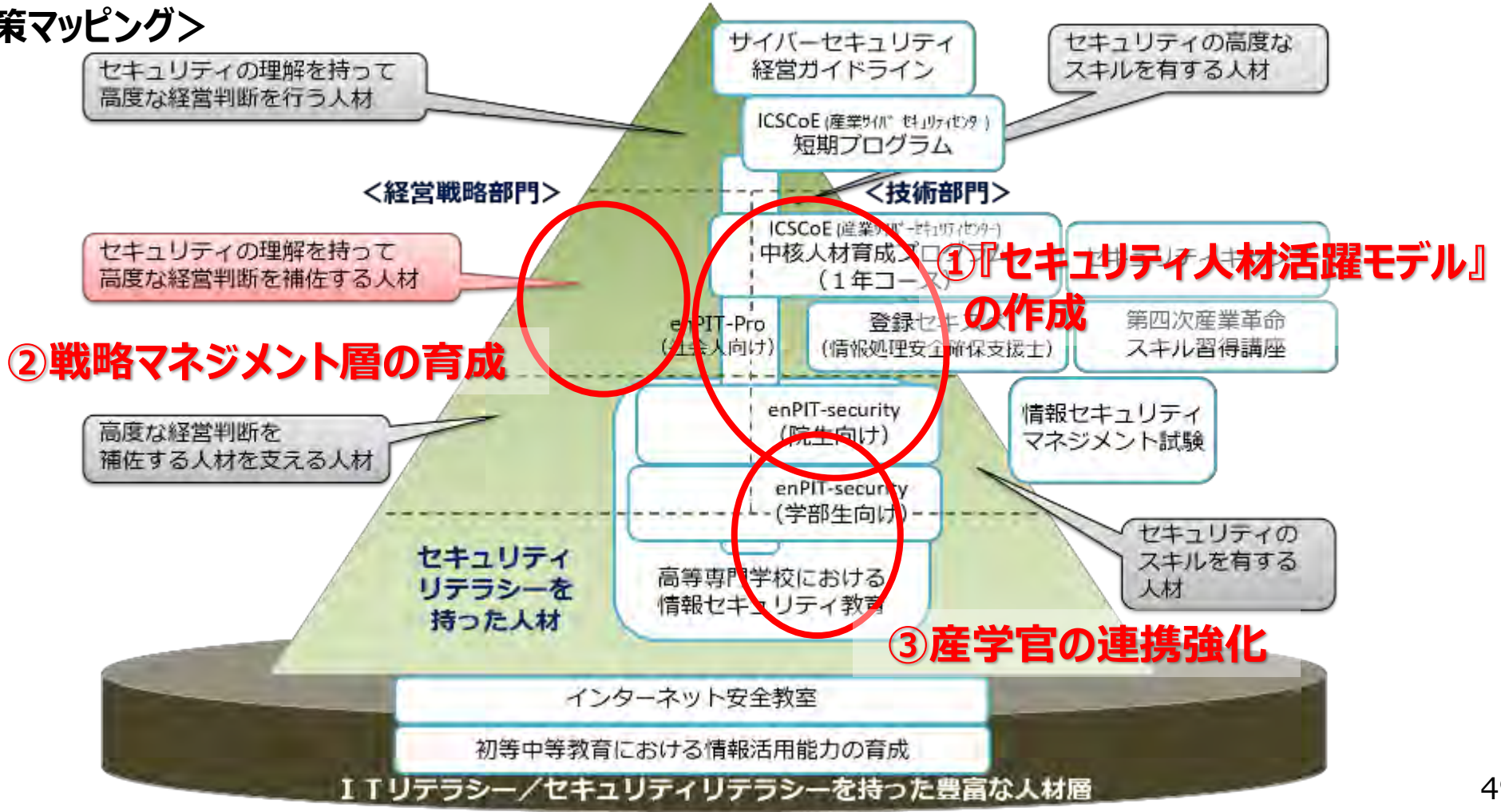
4．人材

5．国際

サイバーセキュリティ人材育成・活躍促進パッケージの全体像

- **セキュリティ人材の定義や育成・活躍の在り方のモデルが不明確。**
- **「セキュリティの理解を持って高度な経営判断を補佐する人材」の育成が不十分。**
- 教育プログラム策定への貢献など、**産業界の教育への取組の強化が期待される。**

＜政策マッピング＞



（１）『セキュリティ人材活躍モデル』の構築

（２）戦略マネジメント層の育成

（３）産学官の連携強化

（４）産業サイバーセキュリティセンター

『セキュリティ体制構築・人材確保の手引き』の開発

累計**3,940**ダウンロード
（2021年1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。年度内を目処に、今後の課題としていた箇所を更新し第1.1版として公表予定。

サイバーセキュリティ経営ガイドライン（10の指示）

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

手引き第１版目次

章	節見出し
1. はじめに	1.1　本書の目的
	1.2　本書の主な対象企業
	1.3　本書の対象読者と読者毎の活用方法
	1.4　本書の構成
2. セキュリティ体制の構築	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
3. セキュリティ関連タスクを担う人材の確保・育成	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
4. セキュリティ体制・人材に関する参考文献	

『セキュリティ体制構築・人材確保の手引き』第1.1版の更新ポイント（予定）

- 手引き第１版において、今後改定予定の版において追加予定としていた以下４項目について、可能な限りで追記を行った第1.1版を策定・公表予定。

①サイバーセキュリティ対策に従事する人材をどのように確保するか
→ ヒアリング等を通じプラクティスを収集。
手引き第1.1版にはできる限りで記載しつつ、今後の議論につなげていく。

②業務内容や役割に応じた人材の育成方法
→ 同上。

③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
→ 関係団体等と調整の上記載。

④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キャリアパス事例
→ 事例などをインタビュー調査の上、手引きとして読者の参考になる形で記載。

（１）『セキュリティ人材活躍モデル』の構築

（２）戦略マネジメント層の育成

（３）産学官の連携強化

（４）産業サイバーセキュリティセンター

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。
- このため、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。

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（予定）
  ※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。

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の広がり

- DXの加速により、「戦略マネジメント層」の育成の重要性は増しており、NISCにおける総務・経営企画・事業部門を対象とした取組をはじめ、各所において、取組を強化する動きが広がっている。

NISC「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」

戦略マネジメント層向けセミナー
「サイバー攻撃の被害事例から学ぶ
～総務・経営企画・事業部門が知っておきたいDX時代のサイバーセキュリティ～（仮）」

- サイバー攻撃の被害を受けた企業から被害経験を通じて得られた気付きなどを講演していただく機会を設け、戦略マネジメント層のサイバーセキュリティへの意識・理解の一層の醸成を図る。
- 主な対象は、総務部門、経営企画部門、事業部門の部長クラスを想定。
- 2021年3月18日（木）（サイバーの日）@オンラインで実施予定。経済産業省も講演予定。

NISCにおける「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

- 「戦略マネジメント層の確保・育成」ためのアプローチの１つとして、経営企画部門や事業部門のマネジメントに携わっている人材（部課長級など）に「プラス・セキュリティ」知識を補充する官民のプログラムの普及に向けた取組を検討中。
- まずは、今後デジタル化が進んでいく中で特に需要が高まると考えられる、「DXを推進する部門の責任者あるいは主要な役割を担う管理職」を対象層としてモデルカリキュラム開発を試行。

※NISCにおいては、「プラス・セキュリティ」知識を、「ITやセキュリティに関する専門知識や業務経験を必ずしも有していない人材が社内外のセキュリティ専門家と協働するにあたって必要な知識として、社会人になって以降も、時宜に応じてプラスして習得すべき知識」と定義し、基礎知識の整理作業等を実施。

- 関連して、情報セキュリティ大学院大学では、DX推進者を対象とした「DX with Cybersecurity 3日間教育コース」を実施（2020年11月18-20日）。

（１）『セキュリティ人材活躍モデル』の構築

（２）戦略マネジメント層の育成

（３）産学官の連携強化

（４）産業サイバーセキュリティセンター

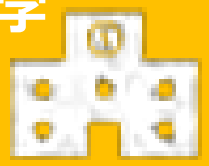
国立高専機構と産・官との連携促進・具体化に向けて

- 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の場の活用等を含め、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

- ・トップガン含むセキュリティ人材等の育成支援
- ・プラス・セキュリティ教育
- ・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

検討の進め方（案）

- 産学官関係者での連携推進のための検討を行うとともに、現場での連携事例も創出していく（SC3における議論・活動等にも期待。）

産学官連携による高専生の協働教育のステップ（案）

高専の教員と産業界の定期的な情報交換の場の創設
- 高専機構や業界団体・関係機関等が定期的に議論（SC3に期待）
- 各地域では地域SECUNITYの枠組を活用し各高専の教員、地元企業・関係機関等が連携

共通理解の醸成・目標の共有
- 高専生の教育の重要性や期待、議論の目的の共有。
- 高専卒業生の内訳（1%, 20%, 80%等）などの整理の共有

現状把握
- 現在の各社の高専生の採用状況・新入社員に求める能力、及び現在の高専のカリキュラム状況などを整理。

高専で育成すべき人材像の整理

高専人材の需要側についての議論

取組の具体化・継続化
- 人材像に基づくカリキュラムを設計するとともに、インターンや出前授業など個別の連携もカリキュラムに組み込むことで学習効果を上げていく。

現場での連携も並行して実施

授業見学
会社見学
→ 互いを知る機会の創出

出前授業
キャリア教育
インターンシップ
コンテスト・合宿
→ 取組具体化

カリキュラム・教材開発
人事交流・共同研究開発
→ 取組継続・深化

（参考）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 国立高専専門学校機構 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。**

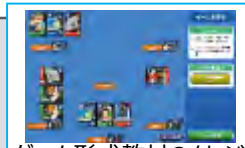
パターン①：90分程度
・高専教員がコンテンツを使って講義 又は 企業等の方が講義
(拠点校から全国各校に同時配信も可)

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

（１）『セキュリティ人材活躍モデル』の構築

（２）戦略マネジメント層の育成

（３）産学官の連携強化

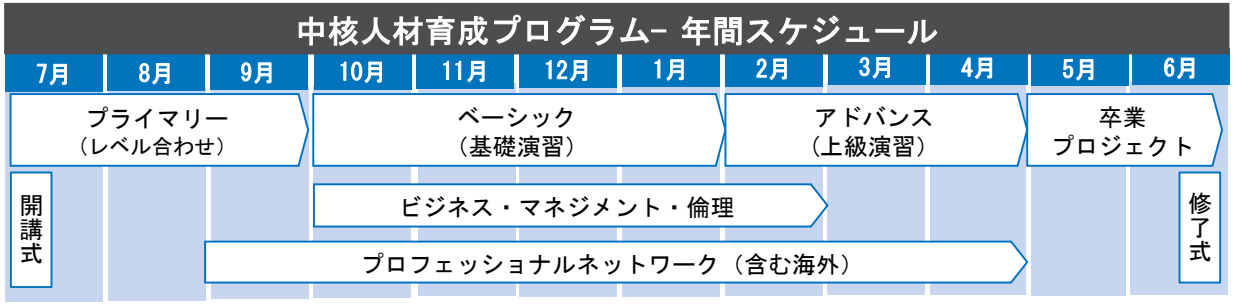
（４）産業サイバーセキュリティセンター

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。現在、第５期生募集中。

ロ　１年を通じた集中トレーニング

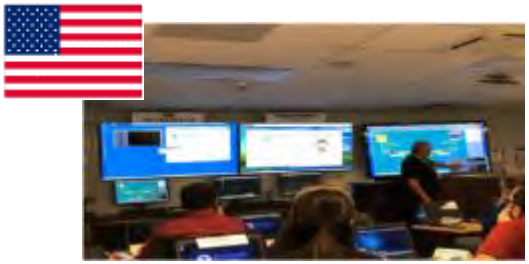
ロ　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：47人）



- 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

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

中核人材育成プログラムの成果と修了生の活動

中核人材育成プログラム受講生は、１年間のプログラムで学んだ技術や人脈を業界の課題に当てはめていくことを主眼に、**プログラムの最後にチーム別の卒業プロジェクトに取り組む**。業界のあるべき姿と現状のギャップを分析し、成果を公表。また、修了者の知見をアップデートし、また、その知見やノウハウを産業界や社会へ還元していくため、**業種横断の修了者コミュニティ「叶会」で情報共有システムを運用**、経済産業省や情報処理推進機構の取組に貢献。

最近の卒業プロジェクトの成果物

➢ **制御システムにおける資産管理ガイドライン（2020年6月）**
資産管理はセキュリティ対策の土台であると考え、制御システム向けの資産管理ガイドライン、自動化ツール、製品検証結果をまとめた成果物を作成。

➢ **「経営者のキモチ」冊子（2020年6月）**
経営者のサイバーセキュティに対する考え（キモチ）をできるだけ短く簡潔に、かつ網羅的に集約。また、経営者へのセキュティ提言時に注意すべきアドバイスも記載。

➢ **CSIRTカードゲーム制作（2020年6月）**
CSIRTの初期教育現場で共通の課題を解決すべく、CSIRT教育のはじめの一歩として「短時間（30分程度）」で「参加者同士が楽しく」、「CSIRT業務に特化」して学べる3種類のカードゲームを制作。

修了者コミュニティ　叶会

【目的】
- 卒業後も知見をアップデート
- 卒業年次・業種を超えた人脈形成
- 修了者の知見の社会還元

【主な活動】
- 年１回年次総会（今年度は１１月８日に開催）で最新動向と修了者の近況の活躍を発表
- サイバーセキュリティ情報提供活動
  →情報共有ツール「SIGNAL」を使い、ICSCoEが入手した脆弱性情報等を修了者に提供
- 東京以外の地域（関西・中京等）でも修了者がコミュニティを形成、各地でセミナー等を開催

●修了生の技術や知見の活用：「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」作成への貢献

中核人材育成プログラムでビルが直面するセキュリティの課題と解決手法を学んだ受講生が、有志で経済産業省のビルSWGに参加。カリキュラムのアウトプットとして、経済産業省が2019年6月にリリースした「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」をより分かりやすく理解できる “解説書”を作成するとともに、ビル関係者向けの脆弱性情報やその解説の配信にも協力。

1．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

2．経営

3．中小・地域

4．人材

5．国際

インド太平洋地域向け日米サイバー演習（第3回）の開催

- 経済産業省及びIPA産業サイバーセキュリティセンター（ICSCoE）が、日米の専門家による**インド太平洋地域向け産業制御システムに係るサイバーセキュリティ演習（第3回）を3月に実施予定。**
- **一部セッションには、日米に加えEUも参加。電力、ガス等のエネルギー分野にフォーカス。**

＜概要＞

◆2021年3月8－12日の5日間全編オンラインで実施。

◆月・火でハンズオントレーニング、水～金で各種ワークショップ（計9つ）を実施。

◆招聘国：ASEAN各国、インド、スリランカ、バングラデシュ、台湾、モンゴル

◆招聘者：
1）全編参加：政府機関、CERT、電力・石油会社から合計40名招聘。
2）一部のみ参加：政府機関、CERT、重要インフラオペレーター（通信会社等含む）から40-50名別途招聘。

JP-US ICS Cybersecurity Week for the Indo-Pacific Region in FY2020

(1) JP-US ICS Cybersecurity Training for the Indo-Pacific Region

- ICS-training session (remote hands-on training)
- Risk Assessment Workshop
- Supply Chain Risk Management Workshop
- Workforce Development & Incident Response Workshop

(2) JP-US Energy-sector Cybersecurity Workshop for the Indo-Pacific Region

- Electricity Sector Workshop 1: Generation, Transmission and Distribution
- Electricity Sector Workshop 2: ERAB, VPP, Renewable Energy and Demand-side
- Process Automation Sector Workshop: Oil & Gas, Chemical and Water
- Smart Home & Building Sector Workshop

(3) JP-US-EU Seminars on Cybersecurity in the post-COVID environment: Suggestions to the Indo-Pacific Region

- Policy and Standardization Workshop
- Healthcare Sector workshop

マルチ・バイを通じた国際協調への取り組み

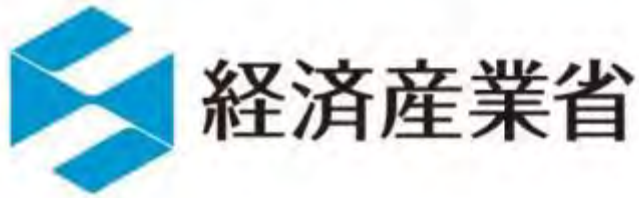
- **「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」**を軸に、各国のステークホルダーと議論、マルチの会議で紹介。サイバー・フィジカル・セキュリティに関する共通の認識を醸成。

- **日印ジョイント・ワーキング・グループ（2020年9月@オンライン）**
  - インド政府との協議において、CPSF、各TF、ビルガイドライン等の取組を広く紹介。
- **第11回インターネットエコノミーに関する日米政策協力対話（日米IED）（2020年9月@オンライン）**
  - 米国政府との協議において、CPSF、IoTセキュリティ・セーフティ・フレームワーク(IoT SSF)、日米サイバー演習の取組を紹介。
- **第2回５Ｇセキュリティ会議（プラハ会議）サイドイベント（2020年9月@オンライン）**
  - 米情報技術産業協会(ITI)/Open RAN Policy Coalition主催の国際会議において、5G・ドローン促進法の取組を紹介。
- **第10回日EU ICT戦略ワークショップ（2020年10月@オンライン）**
  - 欧州委員会との協議において、CPSF、IoT SSF、第3層TF、日米サイバー演習の取組を紹介。
- **第13 回 日・ASEAN サイバーセキュリティ政策会議（2020年10月@オンライン）**
  - ASEAN加盟諸国との協議において、CPSF、IoT SSF、第3層TF、日米サイバー演習の取組を紹介。
- **日EU・５Gワークショップ(2020年10月@オンライン）**
  - CEATECの枠内で、欧州委員会との公開フォーラムにおいて、CPSF、IoT SSF、第3層TFの取組を紹介。
- **グローバル・サイバー・キャビネット（2020年10月@オンライン）**
  - イスラエル国家サイバー総局主催の閣僚級協議において、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)を紹介。
- **欧州政策研究センター(CEPS)、欧州委員会との意見交換（2020年11月@オンライン）**
  - CEPSの調査ヒアリングにおいて、CPSF、各SWG、各TF、SC3、5G・ドローン促進法等の取組を広く紹介。

マルチ・バイを通じた国際協調への取り組み

- **「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）」**を軸に、各国のステークホルダーと議論、マルチの会議で紹介。サイバー・フィジカル・セキュリティに関する共通の認識を醸成。

- **英NCSCとの意見交換（NISC主催）（2020年11月@オンライン）**
  - 英NCSCとの協議において、CPSF、各SWG、各TF、SC3の取組を紹介。
- **デジタル「V4 + 日本」: サイバーセキュリティー・セミナー (2020年11月@オンライン）**
  - V4グループ（ポーランド、チェコ、スロバキア、ハンガリー）との公開セミナーにおいて、CPSF、IoT SSF、SC3、コラプラを紹介。
- **イスラエル国家サイバー総局（INCD）とのサプライチェーン・セキュリティに係る意見交換（2020年11月@オンライン）**
  - INCDに対し、日本のサプライチェーン・サイバーセキュリティの取組（SC3、お助け隊）を紹介。
- **APEC政策ラウンドテーブル（米商務省主催）（2020年12月@オンライン）**
  - 米商務省主催ラウンドテーブルにおいて、産業界へのメッセージ、CPSF、IoT SSF、SC3の取組を紹介。
- **Cybertech Tokyo Live 2020（2020年12月@オンライン）**
  - イスラエル発の国際的フォーラムにおいて、CPSF、各SWG、各TF、SC3等の取組を広く紹介。
- **イスラエル国家サイバー総局（INCD）とのサプライチェーン・セキュリティに係る意見交換（2021年1月@オンライン）**
  - INCDから、イスラエルのサプライチェーン・サイバーセキュリティの取組（可視化ツール）を紹介。


経済産業省