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
2023年３月

１．昨年WG以降のサイバーセキュリティを巡る状況変化

２．昨年WGで御指摘いただいた事項の対応状況

３．本日御議論いただきたい論点

サイバー攻撃の現状

- 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」が引き続き多く見られる。
- 特に、セキュリティ対策に弱点のある取引先等が攻撃経路として狙われ、被害が拡大する「サプライチェーンの弱点を悪用した攻撃」により、甚大な影響が生じている。

情報セキュリティ10大脅威 2023

順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5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
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策情報の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）

<出典：(独)情報処理推進機構(IPA)、2023.1.25>

事例

- 2022年10月末、**国内の公立病院がランサムウェア攻撃を受け、電子カルテシステムに障害が発生**し、**緊急以外の手術や外来診療が一時停止する等**通常診療ができない状況に。
- **病院の給食を委託していた業者のサーバーからウイルスが侵入**した可能性が高いとみられている。
- ２ヶ月超にわたり通常診療を見合わせ。

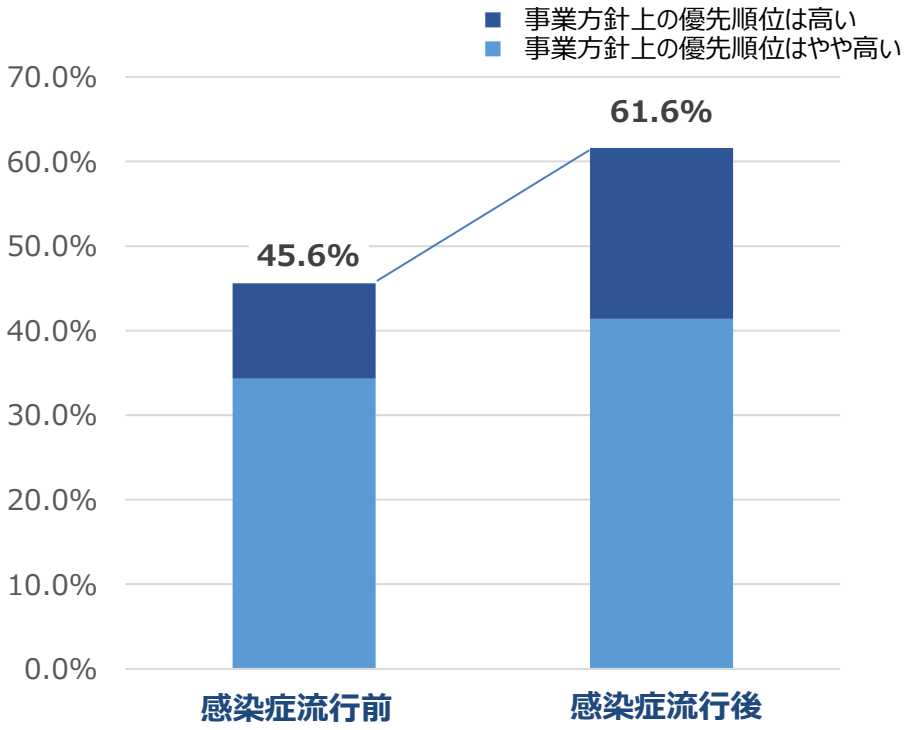
- 2022年11月、警察庁とNISCが日本国内の学術関係者、シンクタンク研究員等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラム(マルウェア)を実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されていると注意喚起。

- ランサムウエアグループ「Hive（ハイブ）」は、機器の脆弱性やメールを通じて被害者のネットワークに侵入。2021年6月以来、ハイブは、世界中で1,500以上の組織を標的とし、1億ドルを超える身代金を獲得していた。
- 2023年1月、米連邦捜査局（FBI）等の米当局が、1年半をかけてランサムウエアグループに対する破壊作戦を実施したと発表。

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

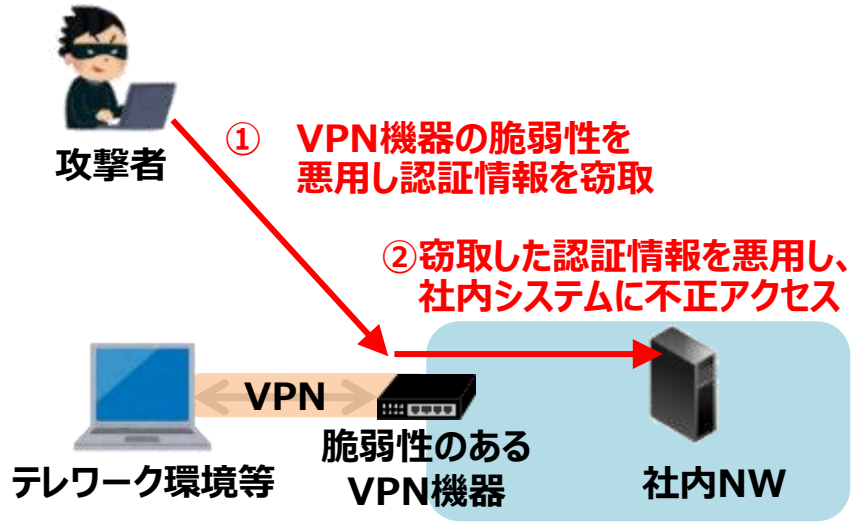
- デジタル化に対する意識は、**<u>コロナ禍の前後で変化</u>**。
- テレワークの利用等が増える中、VPNの脆弱性を突いたサイバー攻撃が増加するなど、**<u>サイバー攻撃の脅威はあらゆる産業において無縁ではなくなっている</u>**。

全産業※で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」
※全産業（製造業、建設業、情報通信業、運輸業,郵便業、卸売業、小売業、学術研究,専門・技術サービス業、宿泊業,飲食サービス業、生活関連サービス業,娯楽業、その他業種）

VPN機器に対する不正アクセス

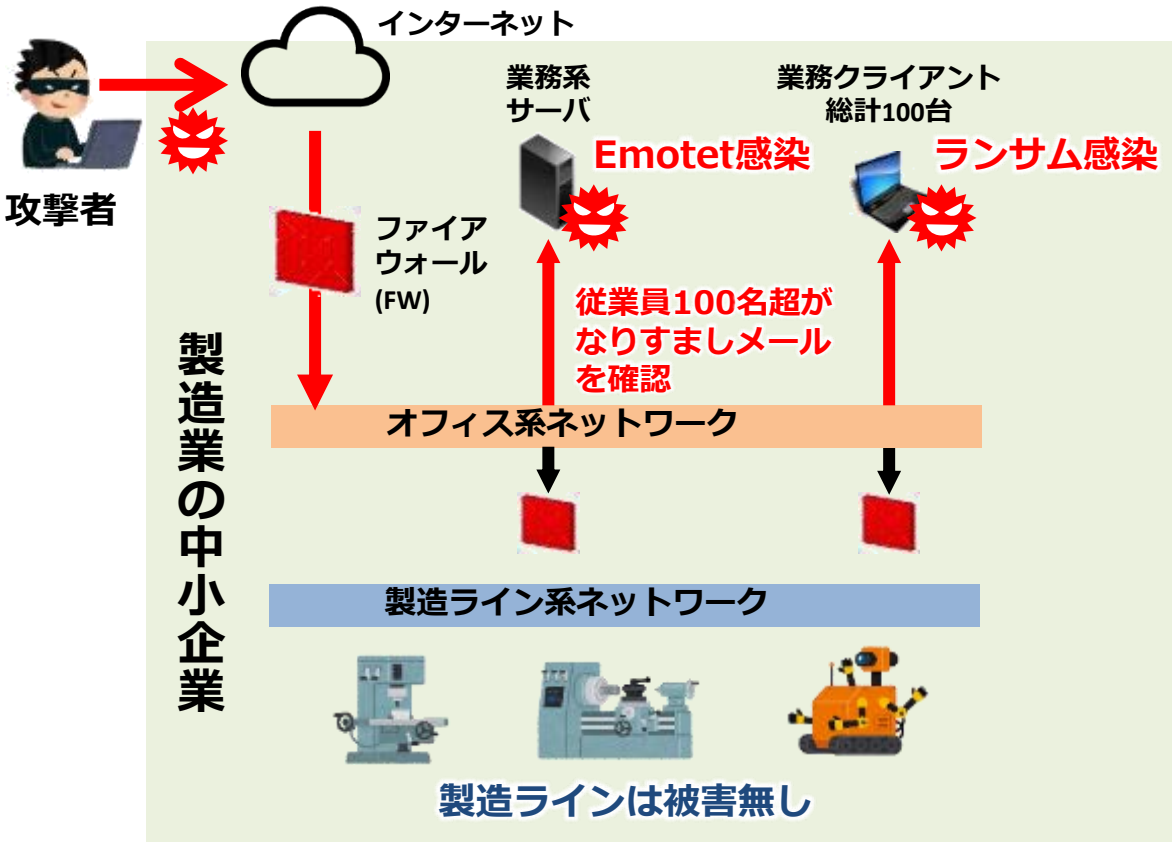


事例：Fortinet製FortiOSの脆弱性

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。

中小企業におけるサイバー攻撃の事例

- 重要インフラに関連する製造業の中小企業（従業員200名規模）で、Emotetとランサムウェアに感染。Emotetに感染したメールアカウントは100名程度。原因は、受信メールの添付ファイルを自動実行する環境で開封したことであった。
- サイバーインシデントの初動対応体制や手順、セキュリティポリシーが整備されておらず、業務停止の判断等が困難な状況に陥った。
- 結果として、製造ラインの業務停止はなかったが、取引先へは、製造ラインに被害が無いことを証明する必要があり、影響範囲の特定を行うためフォレンジック調査費だけで500万円程度かかった。



対処時の問題点

- 業務停止の判断基準が整備されておらず、数日間判断が出来ないまま時間が経過。
- インシデント時の初動対応体制の役割分担が不明確であり、適切な人員確保もできず。
- 重要インフラを取り扱う業種で、影響範囲の把握が急務だったが自社内では調べきれず。

業務影響/被害額

- 製造ラインに影響はなかったものの、結果を取引先に報告する必要あり。
- フォレンジック調査費だけで500万円程度を支出。高額な緊急支出に。
- 原因の判明だけでも10営業日程度を要した。
- 設計データなど最重要データが一部消失した。
- 取引先から問合せと苦情が殺到し、数週間にわたって業務がひっ迫した。

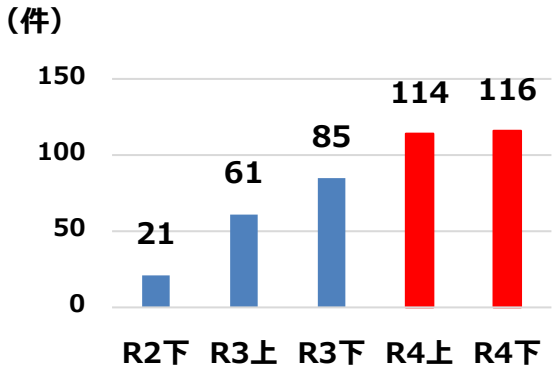
中小企業に対するサイバー攻撃の現状

- 近年、大企業を標的としたサイバー攻撃のみならず、サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、**中小企業自身**及びその**取引先である大企業等への被害が顕在化**している。
- 大企業等を直接標的とせず、弱いところを狙って**サプライチェーン経由で攻撃を行うなどサイバー攻撃が巧妙化**。**取引先等を経由したサイバー攻撃被害**を２割が経験。**取引先に対するサイバー攻撃により、大企業の操業が停止するケース**も発生。
- **対策不足の中小企業がサプライチェーンに存在することは大きなリスク**。産業界の取組と連携し、人材育成や、サイバーセキュリティお助け隊サービス等のセキュリティ対策の普及を行うとともに、どのように対策を進めていけば良いか分からない経営層も含めた中小企業の人材の「プラス・セキュリティ」を推進し、中小企業を含めたサプライチェーン全体での対策を推進する必要。

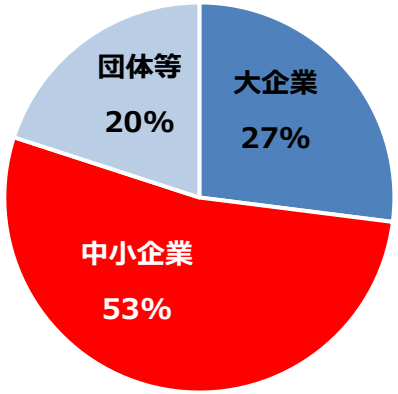
中小企業に対するランサムウェア攻撃が増加

- サイバー被害（ランサムウェア被害）は右肩上がりに増加。
- 被害件数(230件)の内訳は、大企業が63件（27%）に対して、中小企業は121件（53%）と５割を占める。

企業・団体等における ランサムウェア被害の報告件数



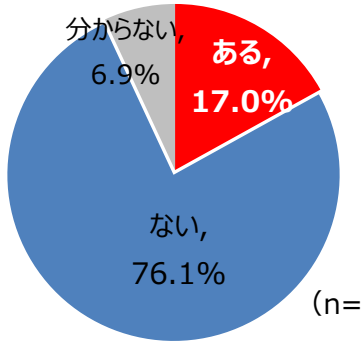
ランサムウェア被害企業等の 規模別件数



出典：警察庁「令和４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5年3月16日）」

取引先等を経由したサイバー攻撃被害の経験

過去に取引先等がサイバー攻撃の被害を受け、それが自社に及んだ経験がありますか（仕入・外注・委託先等の取引先）



出典：令和３年度企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査

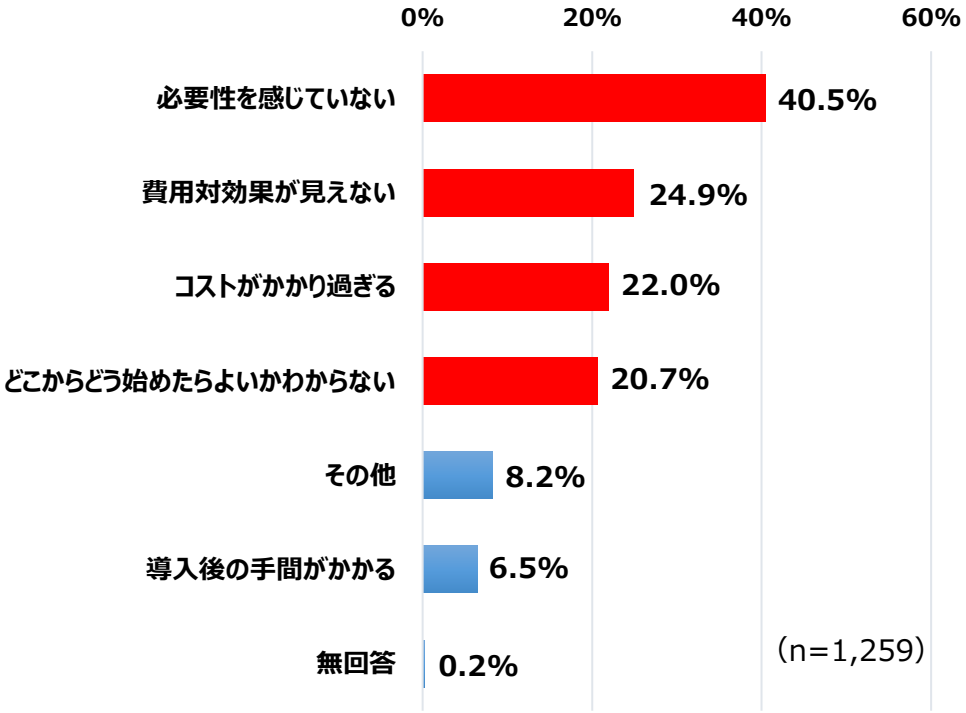
自動車関連企業へのサイバー攻撃事例（2022年3月）

- **大手自動車会社の取引先企業**のサーバー等がランサムウェアに感染。更なる感染拡大を防ぐため、**全サーバをネットワークから切断し、全てのシステムを停止し、受注困難**になった。
- 大手自動車会社は、部品供給の停止により、**全国の工場で生産が困難**になったため、１日間の稼働停止を余儀なくされた。

中小企業のセキュリティ対策のリソース不足

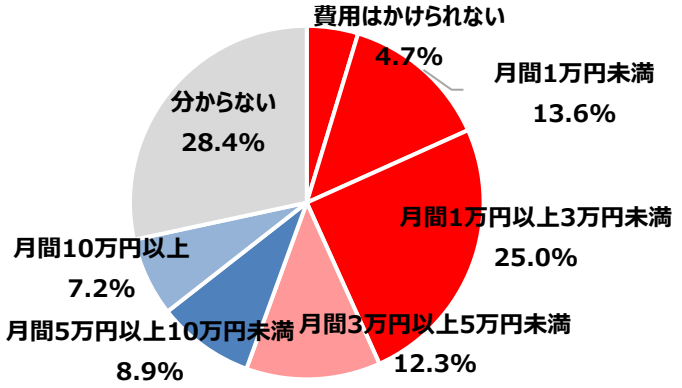
- 中小企業のうち、**過去３年間、全くセキュリティ投資をしていないと回答する企業が３割**に上る。このうち、**４割の企業が「必要性を感じない」**、**2割が「費用対効果が見えない」**と回答。また、合計で**４割が「どこからどう始めたらよいかわからない」「コストがかかり過ぎる」**と回答。
- 中小企業については、セキュリティに支出可能な金額は**月額３万円未満と回答する企業が４割超**。
- 大企業も含めたセキュリティ人材については、米・豪は９割が「充足している」と回答しているが、日本企業は**9割**がセキュリティ対策人材が**「不足している」**と回答。

情報セキュリティ対策投資を行わなかった理由



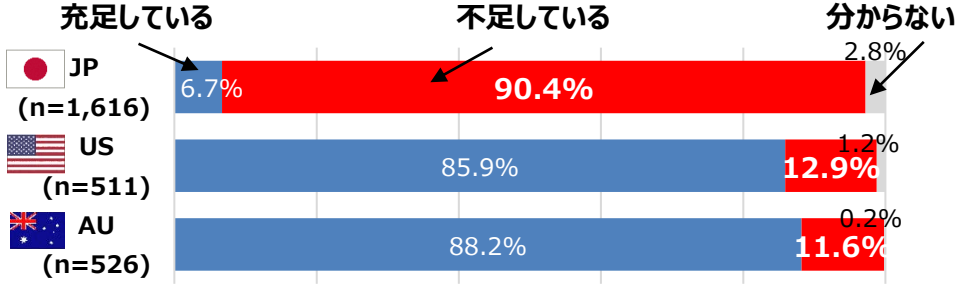
出典：2021年度中小企業における情報セキュリティ対策に関する実態調査

サイバーセキュリティに支出可能な金額



出典：令和３年度中小企業サイバーセキュリティ対策促進事業
（北海道におけるサイバーセキュリティコミュニティ強化に向けた調査）

セキュリティ対策人材の不足



出典：NRI Secure Insight 2021 [企業における情報セキュリティ実態調査」
（日本は株式上場企業または従業員数350人以上の企業が対象）

中小企業のセキュリティ対策の状況

- セキュリティ対策実施のきっかけを問うと、**米・豪では５割を超える企業が「経営層のトップダウン指示」**で実施しているにもかかわらず、**日本は「他社でのセキュリティインシデント」と回答する者が最も多く、次に「自社でのセキュリティインシデント」と回答**。
- **セキュリティ関連の規程の整備状況やセキュリティ業務実施についても、十分な状況ではない**。
- IT導入補助金の申請要件に、セキュリティ対策の実施を自己宣言する「セキュリティアクション」の宣言を必須化するなど、DXとセットでの取組を進めているが、これとあわせて、**取組の強化が必要**。

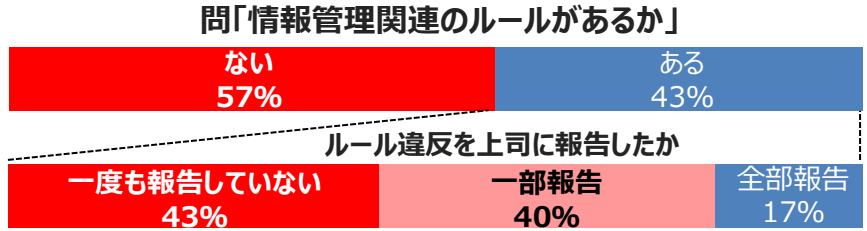
セキュリティ対策実施のきっかけ

	日本	米国	豪州
1位	**27.6% 他社でのセキュリティインシデント**	**54.8% 経営層のトップダウン指示**	**52.7% 経営層のトップダウン指示**
2位	**25.6% 自社でのセキュリティインシデント**	25.0% 他社でのセキュリティインシデント	25.3% 他社でのセキュリティインシデント
3位	21.6% 経営層のトップダウン指示	24.5% 株主や取引先からの要請	22.1% 株主や取引先からの要請

出典：NRI Secure Insight 2021～企業における情報セキュリティ実態調査～（日米豪2,653社を対象）

中小企業のセキュリティ関連規程の整備状況

- **６割**の中小企業が**「情報管理ルールがない」**と回答。
- ルールがある企業でも、**40%以上の従業員がルール違反を報告していない**実態。



出典：全国の中小企業に勤務する従業員1,000名に対するサイバーセキュリティに関するアンケート（2021年度）

中小企業の情報セキュリティ業務の状況

- 中小企業への調査によると、ガイドラインの認知度は14%で、**7割**の中小企業がIPAによる支援を**「知っているものはない」**と回答。
- 中小企業は**情報セキュリティ業務について、「委託していない（58.7%）」、「わからない（11.3%）」**と回答する企業で**７割**を占めており、自力で対策する必要がある。他方、情報セキュリティについて、**「組織的には行っていない（49.2%）」、「兼務だが担当者が任命されている（31.5%）」**となっており、専属者が居ない。

出典：2021年度中小企業における 情報セキュリティ対策に関する実態調査（n=4,074）

インド太平洋地域向け日米EU産業制御システム（ICS）サイバーセキュリティ演習

- 経済産業省及びIPA産業サイバーセキュリティセンターは、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省、エネルギー省、アイダホ国立研究所）、EU政府（通信総局）と連携し、**インド太平洋地域向け産業制御システム・サイバーセキュリティ演習（第５回）**を2022年10月に実施。

■ **日時・場所：**2022年10月24日（月）～28日（金）（ハイブリッド開催）

■ **参加者：**ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の電力・石油会社、National CERT、エネルギー及びサイバーセキュリティ関係政府機関から37名が参加。一部セミナー部分にはオブザーバーも含め約130名が参加。

■ **開催概要：**リモートでのハンズオン演習や、日米欧の専門家によるサイバーセキュリティ政策、サプライチェーンマネジメント及びエネルギー分野特有の課題も含むセミナーを提供するとともに、アイダホ国立研究所が提供するワークショップを提供。実機を用いたハンズオン演習など参加者に有益な能力構築機会を与えるとともに、参加者間の知見共有を行った。

演習の様子

経済産業省　上村審議官挨拶

ゴールドスタイン　米国DHS/CISA 長官代行挨拶

アロンソ 欧州通信総局デジタル社会・トラスト・サイバーセキュリティ局長挨拶

リモートハンズオン演習の様子

インド太平洋地域からの受講生

EUサイバーレジリエンス法（草案）

- 2022年9月に草案提出。2023年後半の発効、**2025年後半の適用**を目指す。
- 例外を除き、**デジタル要素を備えた全ての製品が対象。SBOM作成や更新プログラム提供等セキュリティ要件への適合（自己適合宣言/第三者認証）が求められる。**
- **重要なデジタル製品について、低リスク製品でEUCCやEN規格対象外の製品は第三者認証を、高リスク製品には第三者認証を求める。**（中小企業の認証手続き減額）
- 適合性評価証明書にはEU適合宣言書（CEマーク）/EUCC証明書を用いる。
- **脆弱性の悪用やインシデント発見後24時間以内にENISAへの報告を義務化。**
- **罰則あり。**（最高1,500万ユーロ又は当該企業の全世界売上高の2.5%以内）

注：EUCCとは、IoT製品を対象とする欧州サイバーセキュリティ認証。
EN規格とは、欧州整合化規格

【対象】デジタル要素を備えた全ての製品

・デバイスやネットワークに直接的/間接的に接続されるものも含む。
・医療機器規則、体外診断用医療機器規則、民間航空機規則、自動車の型式承認規則の対象製品は適用除外。
・国家安全保障に関するデジタル製品や軍事目的・機密情報処理目的のものは除外。
・SaaSなどのソフトウェアサービスは対象外。研究開発目的のOSSなども対象外。

【適合性評価】使用環境等のリスクレベル毎に以下を求める。

- **「デジタル製品」　・・・　自己適合宣言か第三者認証を選択**
- **「重要なデジタル製品」のうちクラスI（低リスク）・・・EUCCやEN規格の対象外は第三者認証**
- **「重要なデジタル製品」のうちクラスII（高リスク）・・・第三者認証**

【適合性評価証明書】

・EU適合宣言書（CEマーク）に基づく証明書
・EUCCに基づく証明書（必要に応じてEUCCを必要とする製品を指定）
※この他、市場サーベイランスも行われる。
※第三国（日本も含む）との相互承認も可能。※条文上は見当たらず。

CEマーク

米国サイバー戦略　（令和5年3月3日）

- ２０２３年３月２日（現地時間）、米ホワイトハウスは、４年４ヶ月ぶりに「国家サイバー戦略」を公表。社会全体のデジタル技術への依存度の高まりや、中国、ロシア、イラン、北朝鮮及び非国家主体の悪意あるサイバー活動による、米国の安全保障や経済的への影響を踏まえ、以下の５つを柱として構成。
- これらの柱を実現するため、**①消費者や中小企業等の特定のプレイヤーに過度に依拠せず、重要システムの開発主体に取組を要請**、**②目先の脅威への対応にとらわれるのではなく、デジタルインフラの強靭化に向けた取組にインセンティブを付与する等により、長期的な防御能力を高めること**の２点を挙げている。

第一の柱　重要インフラの防護

１．１ 国家の安全保障や公共の安全を支えるサイバーセキュリティ要件の確立
１．２ 官民協力の拡大
１．３ 連邦政府のサイバーセキュリティーセンターの統合
１．４ 連邦政府のインシデント対応計画及びプロセスの改訂
１．５ 連邦政府防衛の現代化

第二の柱　脅威主体の阻止と解体（Disrupt and Dismantle）

２．１ 連邦政府による阻止活動の統合
２．２ 敵対者を阻止するための官民の運用協力の強化
２．３ インテリジェンス・シェアリング及び被害通知の加速と規模拡大
２．４ 米国内に存在するインフラの悪用阻止
２．５ サイバー犯罪への対抗、ランサムウェアの打倒

第三の柱　セキュリティ及び強靭性強化のための市場原理の形成

３．１ データ管理者の説明責任を果たさせる
３．２ 安全なIoTデバイス開発の推進
３．３ 安全性に問題のあるソフトウェア及びサービスに対する法的責任の転嫁
３．４ 安全を確保した設計に対する連邦政府の補助金及びその他のインセンティブの活用
３．５ 説明責任を向上させるための連邦政府調達の活用
３．６ 連邦政府によるサイバー保険安全措置の検討

第四の柱　強靭な未来（Resilient Future）への投資

４．１ インターネットの技術的基礎の安全確保
４．２ サイバーセキュリティーのための連邦政府の研究開発の再活性化
４．３ ポスト量子に対する備え
４．４ クリーンエネルギーの将来性の確保
４．５ デジタル・アイデンティティー・エコシステムの発展の支援
４．６ サイバー人材強化のための国家戦略の策定

第五の柱　共通の目標を追求する国際パートナーシップの形成

５．１ デジタル・エコシステムに対する脅威に対処するコアリションの形成
５．２ 国際的なパートナーの能力の強化
５．３ 同盟国及び同志国を支援する米国の能力の拡大
５．４ 国家の責任ある行動についてのグローバルな規範の強化のためのコアリションの形成
５．５ 情報、通信並びにオペレーショナルテクノロジー製品及びサービスのグローバルサプライチェーンの安全確保

１．昨年WG以降のサイバーセキュリティを巡る状況変化

２．昨年WGで御指摘いただいた事項の対応状況

３．本日御議論いただきたい論点

昨年度のWGで御指摘いただいた主な事項の対応状況

（１）経営

【主な御指摘事項】

- 自社や取引相手のセキュリティ対策状況を可視化し、セキュリティリスクを事前に把握することが必要である。

①企業におけるセキュリティ対策状況の可視化

- 経営ガイドラインの改訂に伴い、**可視化ツールも更新済**。今後、**業界平均値等**を提示し、産業界での活用を促す。
- 取組強化のため、本日、特に議論いただきたい。【詳細、後記】

②経営ガイドラインの改訂

- **3月２４日に改訂**。次項以降を参照。

【参考】昨年度WG2での経営ガイドライン改訂に際していただいた御意見

- グローバルなサプライチェーンのなかで中小企業を扱うべきである。また、企業がグローバルで実施しなければならないことを整理してはどうか。サイバーインテリジェンスへの対応が必要である。
- サイバーリスクを企業のビジネスリスクの一部として扱い、リスクに対してビジネス部門がまずは責任を持つべきだと明記してはどうか。
- 指示事項9は、『製品やサービス提供の連鎖への攻撃』と『情報のやり取りの連鎖への攻撃』のどちらを指すのか。
- 経営層の善管注意義務という法的要請に紐付いた解釈を入れ込んだ方が良い。
- 投資家やその他のステークホルダーに対して、有価報告書やESG報告書等でセキュリティリスクを積極的に開示することが重要である。
- 経済安全保障推進法案の内容も反映させてはどうか。
- DX with Securityのコンセプトや重要性を全面に打ち出してはどうか。

（参考）サイバーセキュリティ経営ガイドラインの改訂の概要①

- 本ガイドラインについて、**経営者の責務としてサイバーセキュリティに関する残留リスクを低減すること**等を明記するとともに、**サプライチェーンの多様化・複雑化等の情勢の変化やサイバー・フィジカル空間の融合に対応した対策の必要性**を踏まえた改訂を実施予定。

＜現行のガイドライン構成＞

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

＜改訂の概要＞

●取引関係にとどまらず、国内外のサプライチェーンでつながる関係者へのセキュリティ対策への目配り、総合的なセキュリティ対策の重要性や社外のみならず、社内関係者とも積極的にコミュニケーションをとることの必要性を記載

●セキュリティ業務従事者のみならず、全ての従業員において、必要かつ十分なセキュリティ対策を実現できるスキル向上の取組の必要性を記載

●サイバーセキュリティリスクの識別やリスクの変化に対応した見直しやクラウド等最新技術とその留意点などを記載

●事業継続の観点から、制御系も含めた業務の復旧プロセスと整合性のとれた復旧計画・体制の整備やサプライチェーンも含めた実践的な演習の実施等について記載

●サプライチェーンリスクへの対応に関しての役割・責任の明確化、対策導入支援などサプライチェーン全体での方策の実行性を高めることについて記載

（参考）サイバーセキュリティ経営ガイドラインの改訂の概要②

- 特に、サイバーセキュリティ対策は事業活動・成長に必須なものであり、サイバーセキュリティリスクを組織の経営リスクの一環として織り込み、対策の実施を通じてリスクを低減することは経営者の責務であることを詳細に明記するとともに、経営者の責務として、損害発生時の善管注意義務違反や任務懈怠による賠償責任を問われ得るなど、法的責任などを明記。
- 組織のリスクマネジメントの責任を担う経営者が自らの役割として実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが重要であることを明記。

〔Ver.2.0〕

・セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必要なものと位置づけて「投資」と捉えることが重要

・セキュリティ投資は必要不可欠かつ経営者としての責務

・経営責任や法的責任が問われる可能性がある

〔Ver.３.0〕

・サイバーセキュリティ対策は「投資」（将来の事業活動・成長に必須な費用）と位置付けることが重要。企業活動におけるコストや損失を減らすために必要不可欠な投資。

・サイバーセキュリティリスクを把握・評価した上で、対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務。

・善管注意義務違反や任務懈怠に基づく損害賠償責任を問われ得るなどの会社法・民法等の規定する法的責任やステークホルダーへの説明責任を負う。

（※）この他、「国家の安全保障を経済面から確保するという経済安全保障の重要性が増していること等を踏まえ、経済安全保障上の脅威については、サプライチェーンへの影響や社会的責任等の観点から、読者において別途考慮していく必要がある」こと等を明記。

（２）中小

【主な御指摘事項】

- 中小企業がサイバーセキュリティお助け隊サービスを導入するにあたり、コスト負担を補助金等で支援できないか。
- お助け隊サービスの加入促進策の検討では、発注元企業からの紹介事例や利用者の加入経緯等を分析してはどうか。
- 地域の金融機関に中小企業のセキュリティ対策支援を実施してもらうのは良いアイディアだが、金融機関側の課題意識が無いのではないか。地域中小企業のセキュリティ対策のインセンティブとして、金融機関で金利減免や貸付枠の拡大などの工夫が必要。
- 中小企業に対しては情報漏洩よりも事業継続リスクに焦点を当て、意識の醸成を図ってはどうか。
- セキュリティに関心のない企業に対し、セキュリティに目を向けてもらうためには何ができるか。

①サイバーセキュリティお助け隊サービスの導入促進の取組

- **IT導入補助金**において、サイバーセキュリティお助け隊サービスを導入する中小企業に対し、最大100万円まで、補助率1／2以内で支援を実施（2022年８月～）。あわせて、同補助金において、ITツールと一体的にお助け隊サービスを導入する場合に、申請者に加点措置を実施（2022年３月～）。
- IT導入補助金以外にも、**「ものづくり・商業・サービス生産性向上促進補助金」**の「デジタル枠」（2023年１月～）、**「事業承継・引継ぎ補助金」**の「経営革新事業」「専門家活用事業」（2023年3月～）において、**「サイバーセキュリティお助け隊サービス」を利用している中小企業等への加点措置**を実施。
- SC3に参加している業界団体（31団体）との意見交換を実施し、**業界団体に加盟する発注元企業から取引先となる中小企業へのお助け隊サービスを紹介**するよう依頼。
- お助け隊サービス提供事業者とIPAで構成する「事業者連絡会」において、**中小企業の導入事例を共有し、横展開**につなげている。

②地域金融機関との連携強化と事業継続リスクへの対応

- 地銀協等との意見交換を実施し、顧客の中小企業に対し、お助け隊サービス等の支援策の情報提供に協力いただいている。
- 中小企業等経営強化法に基づく**「中小企業の事業継続力強化計画策定の手引き」にサイバーセキュティ対策を追記**することで、サイバーセキュリティ対策も同計画の対象であることを明確化し、日本公庫による低利融資の活用を促進。

【主な御指摘事項】

- パートナーシップ構築宣言の中で、サイバーセキュリティ対策を進められるように中小企業庁に依頼できないか。
- 発注元企業やサプライチェーンの頂点にある企業がセキュリティ対策を義務付ければ、セキュリティに関心がない企業も対策せざるを得ないのではないか。事例を収集し、横展開できないか。

③サプライチェーンにおける取組の強化

- 中小企業等におけるサイバーセキュリティ対策や、発注側企業の取引先に対するサイバーセキュリティ対策の支援・要請に関する考え方について整理した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を経済産業省・公正取引委員会で発表（2022年10月）。**特に発注者側となる事業者に対し、サプライチェーンの保護に向けて、取引先のサイバーセキュリティ対策の強化を促しつつ、サプライチェーン全体での付加価値の向上に取り組み、取引先とのパートナーシップの構築を目指していただく**よう、支援策及び考え方を整理。業界団体等に対し、説明会を順次、実施中。
- 「パートナーシップ構築宣言」のひな形に新たな項目を追加（2022年4月）。

（参考）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。2023年２月時点で30事業者がサービスを登録・提供中。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を開始。

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等による異常監視
- 緊急時の対応支援・駆付けサービス
- 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
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）IT導入補助金による「サイバーセキュリティお助け隊サービス」の導入支援

- 「通常枠」及び「デジタル化基盤導入枠」において、オプションとして「サイバーセキュリティお助け隊サービス」をメインツールと組み合わせて申請することが可能。この際、「サイバーセキュリティお助け隊サービス」を申請する事業者については、**申請採択における審査時に加点対象**になっている。
- 2022年８月から、新たに「セキュリティ対策推進枠」を創設。**「サイバーセキュリティお助け隊サービス」のみでの補助金申請が可能**になっている。

メインツールと組み合わせて、**オプションとして「サイバーセキュリティお助け隊サービス」**を申請可能。

「サイバーセキュリティお助け隊サービス」のみで申請可能。

	通常枠		デジタル化基盤導入枠				セキュリティ対策推進枠
	A類型	B類型	デジタル化基盤導入類型			複数社連携IT導入類型	
			会計・受発注・決済・ECソフト		PC・タブレット等	レジ・券売機等	
補助額	５万円～150万円未満	150万円～450万円以下	50万円以下	50万円超～350万円	～10万円	～20万円	(1)デジタル化基盤導入類型の対象経費（左記同様） (2)消費動向等分析経費（上記(1)以外の経費）※1 50万円×参画事業者数 補助上限：(1)+(2)で3,000万円 (3)事務費・専門家費 補助上限：200万円	5万円～100万円
補助率	1/2以内		3/4以内	2/3以内（※2）	1/2以内		(1)デジタル化基盤導入類型と同様 (2)・(3) 2/3以内	1／2以内
補助対象経費	ソフトウェア購入費、クラウド利用料（最大２年分）、導入関連費		ソフトウェア購入費、クラウド利用料**（最大2年分）**、導入関連費、**ハードウェア購入費**					**「サイバーセキュリティお助け隊」利用料（最大2年分）**
	オプションとして**「サイバーセキュリティお助け隊」を申請した場合、利用料1年分（「サイバーセキュリティお助け隊」導入は加点要素）**							

(※1)消費動向等分析経費のクラウド利用料は、１年分が補助対象。
(※2)交付の額が50万円超の場合の補助率は、当該交付の額のうち50万円以下の金額については3/4、50万円超の金額については2/3。

（参考）お助け隊サービス導入事例

- お助け隊サービスの広報やお助け隊サービス提供事業者による説明会をきっかけとした導入や地域SECUNITYの取組を通じたお助け隊サービスの地域企業への導入が進みつつある。

導入事例①

●製造業、医療機器メーカー
●従業員約30名

【導入経緯】
セキュリティシステム導入検討開始→ITベンダーから見積もりを取得したが高額なため消極的に→お助け隊サービス事業者の説明会に出席→お助け隊サービスの内容を認識→導入打合せ→導入開始

【お助け隊サービスに決めた理由】
・安価で必要十分な機能と判断した。
・レポートによるアンチウイルスの見える化
・ほぼ自社によるメンテナンスフリー

導入事例②

●薬局、ドラックスア
●従業員約600名

【導入経緯】
令和２年度から地域SECUNITY事業を通じて事業者と関係を構築。事業者が中小企業が望まれるセキュリティソリューションを開発しお助け隊サービスに登録した後、地域でのサイバーセキュリティ強化に向けた協力体制を構築すべく、サービスの導入を決定。

【お助け隊サービスに決めた理由】
自らの気づきと事業者が提供するお助け隊サービスを自社のみならず地域への貢献、中小企業経営者の方々への気づいてもらう活動に繋げる。

（参考）意見交換実施結果

- 2022年7月～11月に業界団体等との意見交換を実施。

１．団体におけるサプライチェーン・セキュリティに関する取組内容

（１）各団体における取組

【取組例】

- セキュリティ対策についてのセミナー（ランサムウェア、標準型メール攻撃対策）を実施（事業団体）
- 団体内でサイバーセキュリティ対策に関する部会を立ち上げ、啓発・周知活動を実施（製造業団体）
- 会員の金融機関において、顧客向けのセキュリティ対策関連のセミナーを実施（金融団体）
- 一般向けにサイバーリスクに関する注意喚起等の啓発コンテンツを作成（金融団体）
- 会員事業者がセキュリティ対策のために対応すべき項目の検討し手引書を作成する取組と、企業経営者層への意識改革を行う取組をそれぞれ実施（製造業団体）

【課題例】

- サイバーセキュリティ対策は会員企業にお任せしており、団体としての取組はない（製造業団体）
- SC3立ち上げ時にはアナウンスを行ったが、それ以降は継続した情報発信は行ってこなかった（製造業団体）

（２）サプライチェーンへのサイバーセキュリティ対策の展開の重要性

- メーカー団体とも連携し全体のレベルを上げていきたい（製造業団体）
- 団体としてサイバーセキュリティ対策について直接周知が届くのは会員の大企業までで、一次サプライヤーまでは伝わるかもしれないが、二次サプライヤー以降となると難しい（製造業団体）
- 当団体には関連分野の事業者も加盟しているが、このような事業者まで横断的な取組を行うことは困難（事業団体）

2． IT導入補助金の活用を含むお助け隊サービスの活用・推奨依頼

（１）お助け隊サービスの情報発信の重要性

- 価格的にも現実的で周知を期待（情報通信業団体）
- お助け隊サービスはこれまで知らなかったが、今後周知していきたい（技術団体）
- 費用対効果はいいため、会員企業にどう関心を持ってもらうかが重要（製造業団体）

（２）お助け隊サービスの効果的な推進策

- 単に補助金を紹介するだけでなく、補助金活用後の便益も明示した方がいい（製造業団体）
- セキュリティ対策自体の必要性から説明できるような一般的な窓口があるといい（士業団体）
- 問題意識を有している中小企業は少ないのが実情であるため、実際の活用・施行事例があると訴求しやすい（金融団体）

（３）中小企業より規模の大きい企業における活用の検討

- 中小企業にとっては適切なサービス内容だが、中堅規模以上になると活用が難しくなるため、より高度なサービスを組み合わせるなど考えてもいい（製造業団体）

3．今後のSC3の活動に対する期待

- SC3からの情報は委員会や会員企業全体に展開し参考にしており、サイバーセキュリティの動向についての情報を提供してもらえると助かる（情報通信業団体）
- SC3には他業界との業界横断的な意見交換の場になることを期待（経済団体）
- SC3にて、他業界団体が行っている取組で、参考となるものを紹介してほしい（製造業団体）
- SC3が各業界団体を支援できるような形になればいい（製造業団体）
- SC3とともに活動し、サプライチェーンの奥深いところまで手が届くように取り組みたい（製造業団体）

サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて（概要）

令和４年10月28日
経 済 産 業 省
公 正 取 引 委 員 会

【 背　景 】

■ 昨今、サイバーセキュリティ対策が不十分な**中小企業がサイバー攻撃に狙われ、サプライチェーン全体に問題が波及**する事態が発生。

■ 令和４年４月、「原油価格・物価高騰等に関する関係閣僚会議」（内閣総理大臣、内閣官房長官、関係大臣、公正取引委員会委員長が出席）において、**コロナ禍における「原油価格・物価高騰等総合緊急対策」**を決定。

「サイバーインシデントによってサプライチェーンが分断され、物資やサービスの安定供給に支障が生じることのないよう、**中小企業等におけるサイバーセキュリティ対策を支援**するとともに、**取引先への対策の支援・要請に係る関係法令の適用関係について整理**を行う。」

【 内　容 】

■ 発注者側となる事業者は、以下を参考に、**サプライチェーンの保護に向けて、取引先のサイバーセキュリティ対策の強化を促しつつ、サプライチェーン全体での付加価値の向上に取り組み、取引先とのパートナーシップの構築**を目指していただきたい。

①サイバーセキュリティ対策に関する支援策

■ **サイバーセキュリティお助け隊サービス**（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ワンパッケージで提供）の利用促進

■ **セキュリティアクション**（中小企業がセキュリティ対策に取り組むことを宣言）の推進

■ **中小企業の情報セキュリティ対策ガイドライン**（中小企業を対象に、情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき方針、対策を実践する際の手順や手法をまとめたもの）の活用

■ **パートナーシップ構築宣言**（発注側企業が取引先との間でパートナーシップを構築することを宣言）の中で、取引先にサイバーセキュリティ対策の助言・支援を行うことを取組例として記載

②サイバーセキュリティ対策の要請に係る独占禁止法・下請法の考え方

■ サイバーセキュリティ対策の必要性が高まる中、**サプライチェーン全体のセキュリティ対策強化は重要**な取組。**サイバーセキュリティ対策を要請すること自体が直ちに問題となるものではない**。

■ ただし、要請の方法や内容によっては、問題となることもあるため、そのようなケースを例示。

＜問題となるケースの例＞

① 取引上の地位が優越している事業者が、サイバーセキュリティ対策の実施によって取引の相手方に生じるコスト上昇分を考慮することなく、一方的に著しく低い対価を定める場合

② 取引上の地位が優越している事業者が、新たなセキュリティサービスを利用する必要がないにもかかわらず、自己の指定する事業者が提供するより高価なセキュリティサービスの利用を要請し、当該事業者から利用させる場合

（参考）「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」の説明会

- 2022年10月に経済産業省・公正取引委員会で発表した、中小企業等におけるサイバーセキュリティ対策や発注側企業の取引先に対するサイバーセキュリティ対策の支援・要請に関する考え方について整理した文書について、経団連サイバーセキュリティ委員会サイバーセキュリティ強化WG及びJUASアカデミーで説明会を実施。主に発注側となる企業から約180名が参加した。

【主な御意見】

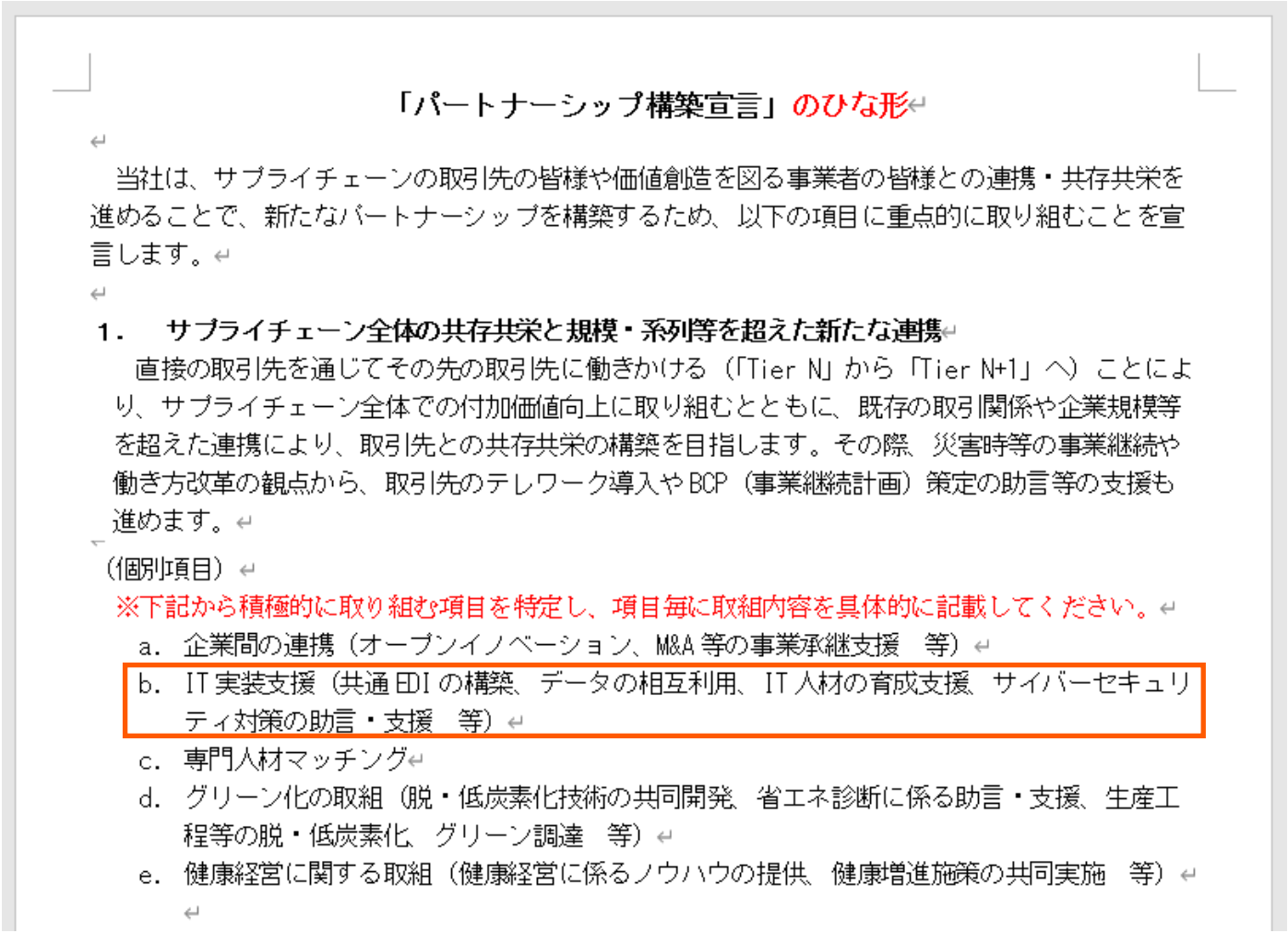
- サイバーセキュリティ実施レベルのチェックシートを提出するよう、発注側企業から求められることが増えている一方、**チェック内容は企業ごとに異なるため、現場には負担感もある。国の統一基準を設置できないか。**
- サプライチェーンでのサイバーセキュリティ対策は重要であることは理解できるが、**具体的にどのような対策まで要請すべきかのさじ加減が難しい。**
- 取引先が下請法の対象となる場合、セキュリティ対策の進め方に十分注意する必要を感じているため、**スピード感をもった取組は難しい。**

【質疑応答における主な回答】

- **サイバーセキュリティ対策において留意すべきポイントは、業界や業務内容（契約関係、取り扱う情報等）によって様々であるため、個別のケースに応じてチェックする必要がある**と考えている。国の統一基準については、課題として状況を注視することとしたい。
- 取引先の対策が自社の要求するレベルに達しておらず、取引を停止する場合に優越的地位の濫用に当たるかについて、事業者間の取引は基本的には自由であるが、個別の状況に照らして判断することとなる。一概には言えないが、**両者で協議を重ね、合理的な範囲の要請がされているか否かや、取引を打ち切ることを示唆して問題となるような行為を実行に移そうとしているかなどが重要なポイント。**

（参考）「パートナーシップ構築宣言」のひな形改訂

- 2022年４月、サプライチェーンの取引先や価値創造を図る事業者との連携・共存共栄関係の構築を目指す「パートナーシップ構築宣言」のひな形を改訂し、個別の項目にサイバーセキュリティ対策に係る助言・支援等を追加。



「パートナーシップ構築宣言」のひな形

当社は、サプライチェーンの取引先の皆様や価値創造を図る事業者の皆様との連携・共存共栄を進めることで、新たなパートナーシップを構築するため、以下の項目に重点的に取り組むことを宣言します。

1．　サプライチェーン全体の共存共栄と規模・系列等を超えた新たな連携

直接の取引先を通じてその先の取引先に働きかける（「Tier N」から「Tier N+1」へ）ことにより、サプライチェーン全体での付加価値向上に取り組むとともに、既存の取引関係や企業規模等を超えた連携により、取引先との共存共栄の構築を目指します。その際、災害時等の事業継続や働き方改革の観点から、取引先のテレワーク導入やBCP（事業継続計画）策定の助言等の支援も進めます。

（個別項目）

※下記から積極的に取り組む項目を特定し、項目毎に取組内容を具体的に記載してください。

a．企業間の連携（オープンイノベーション、M&A等の事業承継支援　等）

b．IT実装支援（共通EDIの構築、データの相互利用、IT人材の育成支援、サイバーセキュリティ対策の助言・支援　等）

c．専門人材マッチング

d．グリーン化の取組（脱・低炭素化技術の共同開発、省エネ診断に係る助言・支援、生産工程等の脱・低炭素化、グリーン調達　等）

e．健康経営に関する取組（健康経営に係るノウハウの提供、健康増進施策の共同実施　等）

（参考）令和4年度 中小企業等に対するサイバー攻撃の実態調査

- 取引先企業への攻撃の足掛かりとして、サイバー攻撃を受ける恐れが大きいと考えられる中小企業等を対象に、ネットワーク環境・セキュリティ対策の状況把握とネットワーク及び端末における異常を監視する等により、攻撃の実態について調査・分析した。

※調査にご協力いただいた企業の6割は、従業員数が100名超、あるいは売上高10億円超である。

ネットワーク環境・セキュリティ対策の状況把握

- ルール・ポリシーの有無、ネットワークのセキュリティ対策状況、セキュリティ製品の運用状況をヒアリングで確認。
- UTMを既に設置している企業が多かったものの、アラートの確認はベンダ任せになっている。
- ヒアリングで「できていない」と認識している事項として、ポリシー策定、USB対策、工場LAN対策が挙げられた。

産業分野	対象者数	UTM既設	アラート確認		
			自社	ベンダ	無し
半導体	5	3	0	2	1
自動車部品	24	17	1	16	0
航空部品	11	4	1	2	1
防衛装備	3	2	1	1	0

ネットワーク及び端末における異常監視

- 既設UTMレポートの活用と、新規にUTMを17者、EDRを30者に導入いただき、インターネット側から社内ネットワークへ届く攻撃や社内ネットワーク内で発生する不正な通信を監視した。
- ランサムウェアやC&Cサーバとの通信といったセキュリティ侵害に当たる攻撃は検知されなかった。
- 民間のUTM監視サービスや、過去のサイバーセキュリティお助け隊サービスの実証事業結果と比較しても、特定産業分野のサプライチェーンに属する企業ではインターネット側から攻撃が多く、内部侵入のきっかけになるような動作も多いことから、リスクがより高いと考えられる。

✓ メールやWebを契機としたウイルス感染に対しては、UTMとEDRの双方で防ぎ、被害拡大を防止する事が有効。
✓ 定期的に検知レポートを確認し、不審なアプリケーションやサイバー攻撃の兆候を把握し、対策を継続的に行うことが有効。
✓ セキュリティの有識者等適切な知識経験を有した人員によるネットワーク構成の確認や検証が有効。

（３）地域

【主な御指摘事項】

- 大学、自治体と地元企業の三者でコンソーシアムを作り、地域におけるセキュリティの活動を議論してはどうか。
- 地域を管轄する警察や自治体を管轄する総務省と連携し、支援すべき中小企業の対象領域を拡大できないか。
- 事故からアラートが上がるような仕組みはあるが、日頃のコミュニケーションの中で相談できるような窓口のようなものがあったら良い。

①全国で地域SECUNITYを組成

- 総務省総合通信局等とも連携し、経済産業局が事務局となって、大学や自治体、地元企業等で構成する「地域SECUNITY」を組成しているところ（2022年12月に四国サイバーセキュリティネットワークを設置）。民間主体で活動している団体についても、経済産業省／地方経産局のホームページで募集を開始する予定。
- 各地域SECUNITYで、63回ワークショップ等を開催し、2800名以上が参加（2022年4月～2023年3月）。
- SC３地域SECUNITY形成促進WGで、地方会議を全国９地域で開催し、地元企業や支援機関等との意見交換を実施。

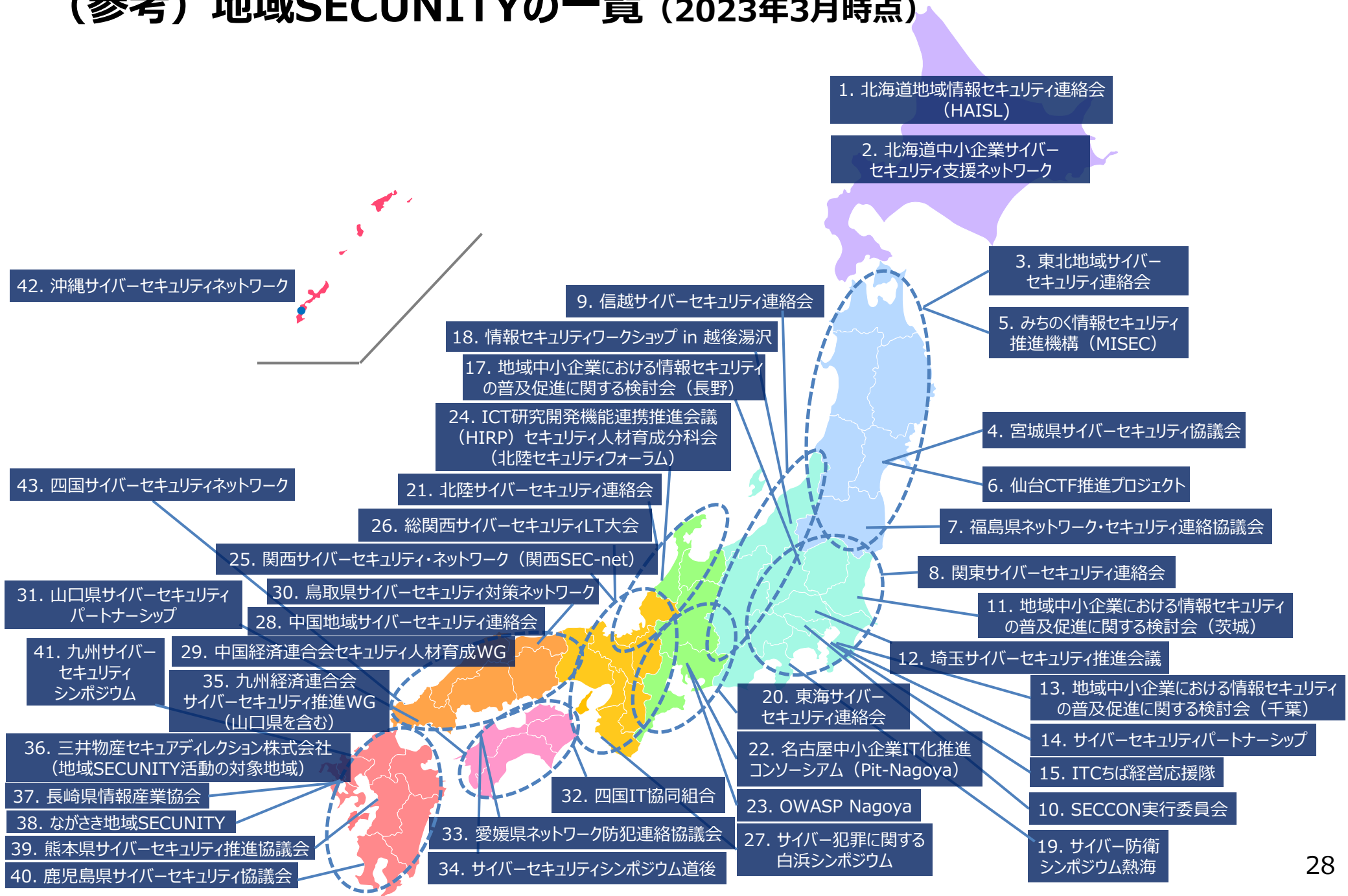
②県警や総務省との連携強化

- 中小企業のサイバーセキュリティ対策の推進に向けて、サイバーセキュリティお助け隊サービスの紹介を県警からも実施いただくなどの連携強化を進めているところ。
- 経済産業省／総務省の地域SECUNITYの紹介ホームページにおいて、それぞれの取組を紹介している。

③相談体制の強化

- 本日議論。

（参考）地域SECUNITYの一覧（2023年3月時点）



令和４年度　地域SECUNITY形成促進の取組（九州）

- 中小企業からの要望が多い「具体的な対策」を中心に、業種ごとの特徴を踏まえたテーマを設定し、**計９回**のセミナー・ワークショップを実施。**延べ912名が参加**。
- 企画、運営面においても地域企業や地域団体との連携が進み、地域SECUNITYとしての**主体的かつ自立的な取組が活発化**。

R4.10.21　地域SECUNITY×第18回フューチャーセッションの様子

タイトル・概要		日時	参加者数	主催（・共催）
地域SECUNITY セミナー 「サイバーセキュリティ対策の“基本”」		R4.8.23	105名（オンライン）	九州経済産業局、IPA、（一社）九州経済連合会
ECサイトワークショップ	「EC サイトの被害事例の実態から利用者側の視点での対策を考える」	R4.10.19	28名（会場9名・オンライン19名）	（公社）福岡貿易会、（一財）九州オープンイノベーションセンター
	「避けては通れないオンラインショッピングの危ないお話」	R5.1.25	44名（オンライン）	
地域SECUNITY × 第18回フューチャーセッション「衛星データを安全に利用するために知っておきたいセキュリティの知識」		R4.10.21	89名（会場33名、オンライン56名）	九州経済産業局、IPA、（一社）おおいたスペースフューチャーセンター
サイバーセキュリティセミナー	「事業継続のためのサイバーセキュリティ対策」	R4.8.30	180名（オンライン）	（一社）九州経済連合会、九州経済産業局（共催：福岡商工会議所）
	「激化するランサムウェア、企業が取るべき対策とは？」	R5.2.10	210名（会場16名、オンライン194名）	
サイバーセキュリティカレッジ	「データから読み解くサイバー攻撃動向と組織に求められる課題と解決策」／「地域 SECUNITY 事業の取り組みとセキュリティ対策推進のポイント」	R4.10.27	54名（会場）	（一社）熊本県サイバーセキュリティ推進協議会、熊本県警
	「ランサムウェア対策に防災訓練の実施を」／「ストレージに求められるランサムウェア対策術」等	R5.2.8	126名（会場49名、オンライン77名）	
地域SECUNITY 「サイバーセキュリティセミナー」		R5.2.16	76名（会場26名・オンライン50名）	（公社）福岡貿易会、（一財）九州オープンイノベーションセンター

令和４年度　事業継続に向けた実践的教育機会の提供（九州）

- **<u>九州大学</u>**が取り組む**<u>社会人リカレント教育プログラム（SECKUN）との連携</u>**で、特別参加プログラムを提供。
  中小企業の経営者や現場責任者等の人材育成として、実践的教育の機会を提供。
- サイバー攻撃によって設備停止等の支障が出た場合に、**<u>“事業継続”できる体制を備える</u>**ことを目的に、対策本部活動を模擬体験し、課題対応を共に考え、組織のあり方への気付きを提供。**<u>中小製造業向け演習は全国初の新規事業。</u>**
- 参加者からは**<u>「社内だけでなく社外の対応等、想像以上のことが起こることに気付いた。対岸の火事ではない」、「サイバー攻撃を受けた際に気付けるかどうか、生産を進めるかの判断が必要なとき、何を判断にすればよいかなどを考えることができた」、「BCPマニュアルに組み込む必要性を感じました」</u>**とコメント。

R5.2.4（土）サイバーセキュリティインシデント対応机上演習
（医療・調剤薬局向け）@佐賀県

県内２病院１調剤薬局から１０名が参加
（佐賀県警２名も参加）

R5.3.8（水）中小製造業向け体験型演習in北九州
@福岡県北九州市

中小製造業７社１０名が参加（福岡県警３名も参加）
【オンライン聴講者４１名を含めると合計６６名が参加】

R5.2.1
事前説明会には
112名が参加

警察との連携

- 県警察等のウェブサイトにてサイバーセキュリティお助け隊サービスを紹介する等、警察との連携も進めている。

・県警察ウェブサイト上での紹介例

サイバーセキュリティお助け隊サービス制度（外部サイトへリンク）

「サイバーセキュリティお助け隊サービス」は、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をワンパッケージで安価に提供するサービスです。

https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

県警の中小事業者向けのサイバーセキュリティ対策関連リンク集にて、お助け隊サービスが紹介されている。

（愛知県警察ウェブサイトより引用 https://www.pref.aichi.jp/police/anzen/cyber/tokusetsu/link.html）

・県ウェブサイト上での紹介例

（兵庫県ウェブサイトより引用 https://web.pref.hyogo.lg.jp/cybertaisaku/）

サイバー攻撃のデータや県内でのサイバー攻撃事例、事案発生時の対策などを紹介する県のホームページにおいて、お助け隊サービスが紹介されている。

（４）人材

【主な御指摘事項】

- 情報システム担当者が経営層へインシデントの説明ができるように、担当者と経営者の双方の知識やスキルを上げる必要がある。
- プラスセキュリティ人材の育成について、具体策を検討し企業へ提示していくべきである。プラスセキュリティとは、どの人材層に何を実施しようとしているのかを明確にすべきである。
- セキュリティ人材やプラスセキュリティ人材の評価方法と人事・給与制度の連携を検討すべき。
- サイバーセキュリティ戦略で、「対策推進に向けた専門人材との協働等に資するよう、法令への理解を深めるツール等の活用促進を図る。」とあるが、このツールがどこかにあると期待している。
- ベンダやサプライヤをコントロールするためにも、セキュリティ言語は統一すべき。

①サイバーセキュリティ体制構築・人材確保の手引き（経営ガイドライン 付録F）の改訂

- 経営層、戦略マネジメント層、実務者・技術者層といった人材の**各層に応じたプラスセキュリティの実装のため、それぞれの役割等を明記**し、経営者による人材育成を進めやすくするよう**「サイバーセキュリティ体制構築・人材確保の手引き（経営ガイドライン付録F）」を改訂**（2022年６月）。

②「デジタルスキル標準　第１版」の策定（プラスセキュリティ人材の定義と浸透）

- DXを推進する人材の役割や習得すべきスキルを定義した**「デジタルスキル標準　第１版」を公開**（2022年12月）。５つの人材類型で求められるサイバーセキュリティに関するスキルについても定義し、DXを推進する人材の役割や習得すべき知識・スキルを示し、それらを育成の仕組みに結び付けることで、リスキリングの促進、実践的な学びの場の創出、能力・スキルの見える化の実現につなげる。

③セキュリティ人材の活躍の場の拡大

- 本日議論。

④法令理解を深めるツールの整備

- 関連主要法令の概要と、平時・インシデント対応に関する法令上の事項、情報の取扱いに関わる法的課題等を分かりやすく記載した「関係法令Q＆Aハンドブック 第１版」をNISCが整備（2020年3月）。現在、**NISCのワーキンググループにおいて改訂を検討中**。
- 【再掲】発注者側の事業者に、サプライチェーンの保護に向けて、取引先のサイバーセキュリティ対策の強化を促しつつ、サプライチェーン全体での付加価値の向上に取り組み、取引先とのパートナーシップの構築を目指していただくため、中小企業等におけるサイバーセキュリティ対策や、発注側企業の取引先に対するサイバーセキュリティ対策の支援・要請に関する考え方について整理した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を策定（2022年10月）。

⑤産官学が参照できるセキュリティ用語のマッピングの整理

- 産業界が主に参照しているNICEフレームワーク（NIST SP800-181)と、学界が主に参照しているCAE-CD/KU*の関係を整理し、それらで用いられる用語の英和対照表とともに、共通語彙集の試案を策定（2023年3月）。

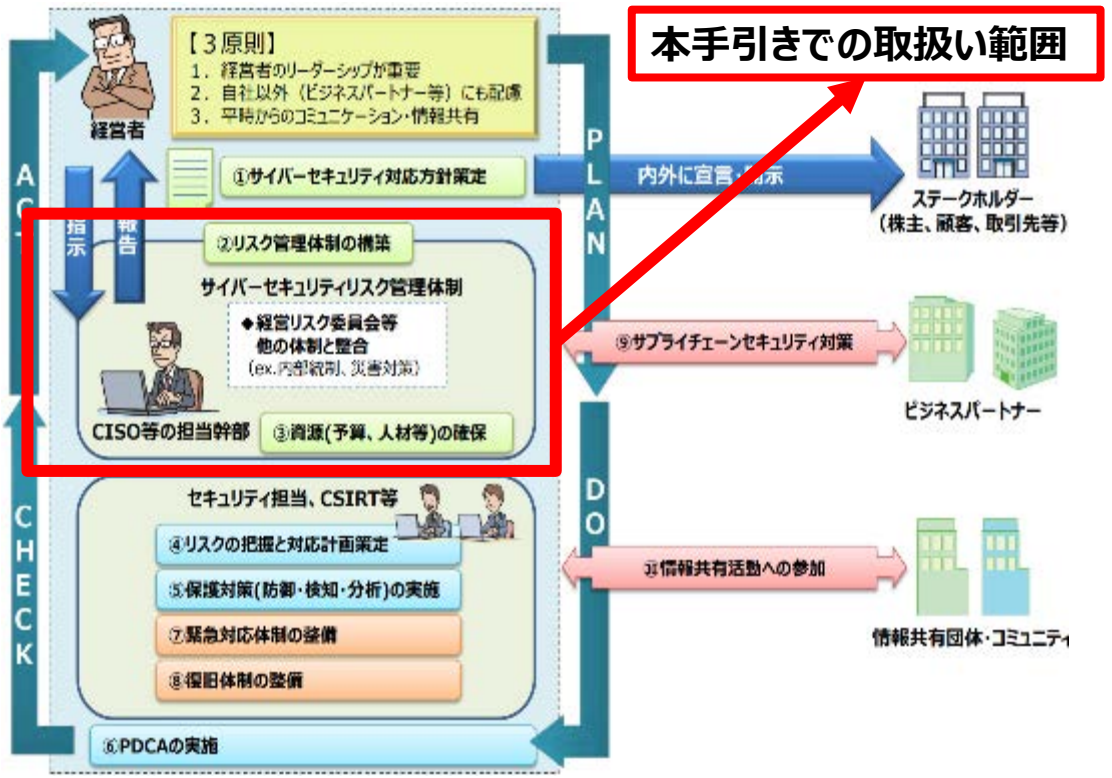
*CAE-CD/KU: National Centers of Academic Excellence Cyber Defense / Knowledge Unit

『セキュリティ体制構築・人材確保の手引き』の開発

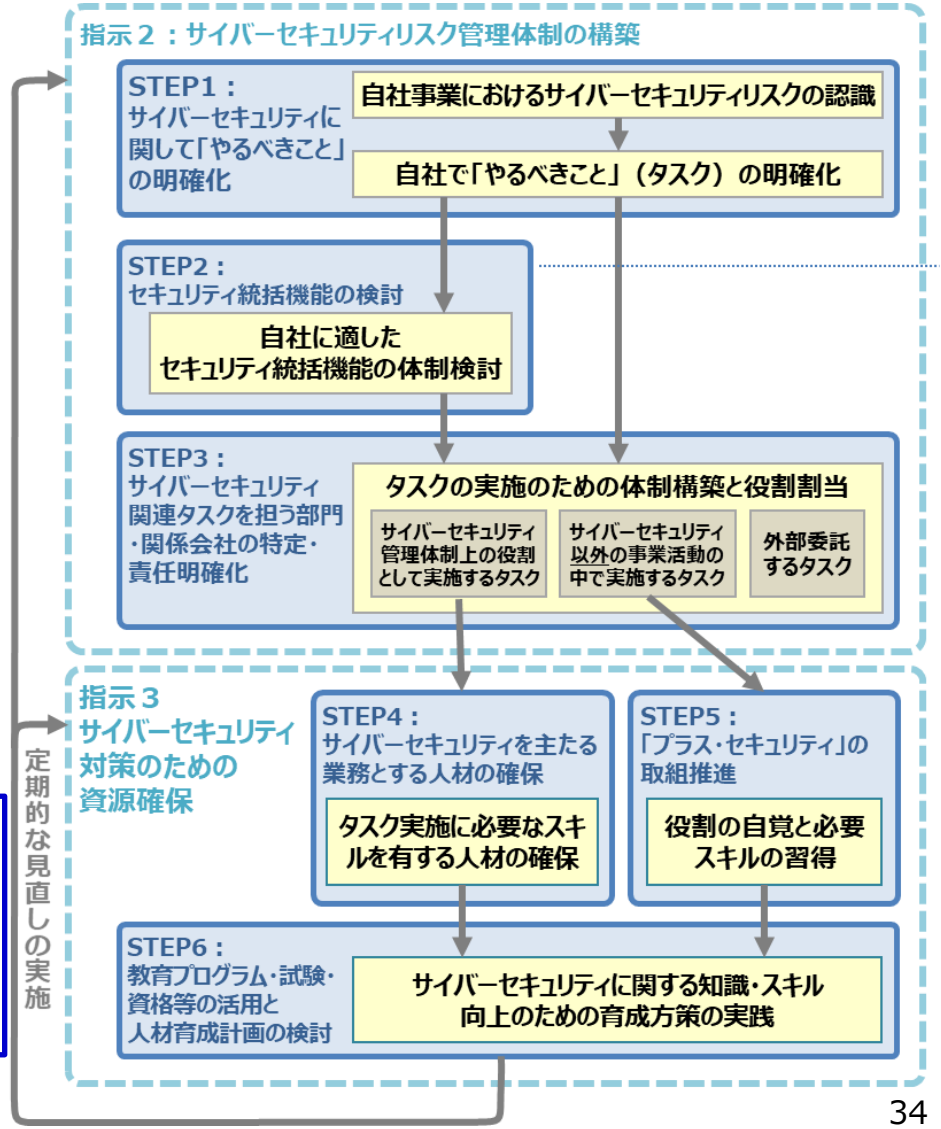
- 2020年9月30日策定
- 2021年4月15日改訂（Ver.1.1）
- 2022年6月15日改訂（Ver2.0）

● 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**。各組織における検討の流れをステップ・バイ・ステップで整理した**第2.0版を2022年6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）



検討を実践を効率的に進めるための手順



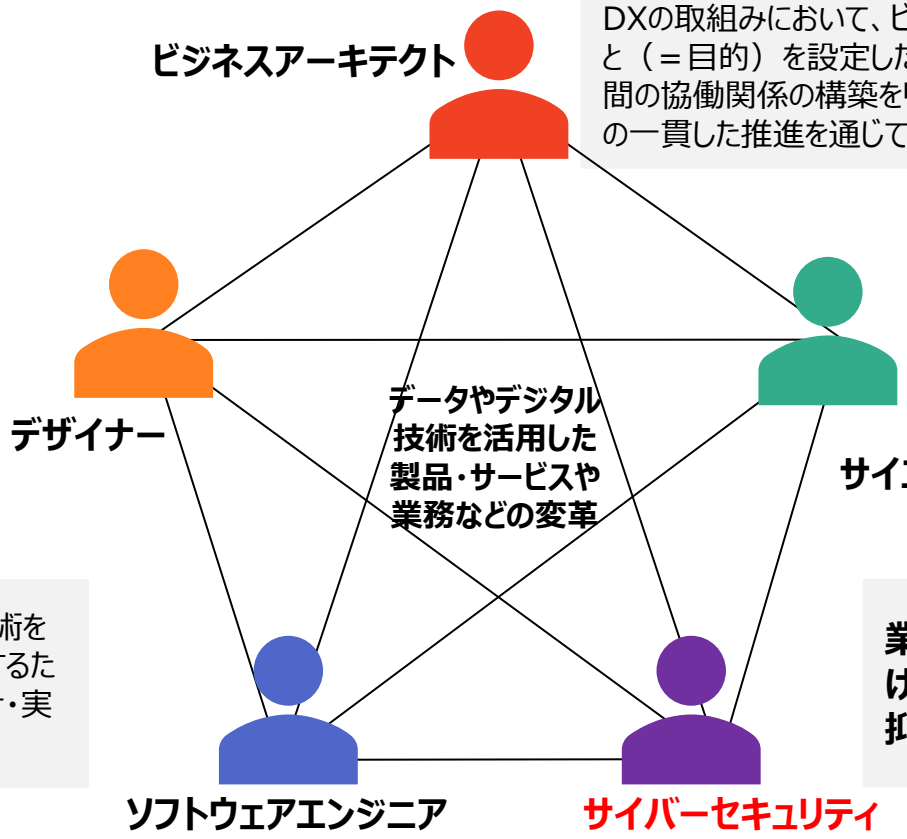
第2.0版での更新の主なポイント

- 読みやすさを重視し、step by stepでポイントを記載。
- ITSS+（セキュリティ領域）について、プラス・セキュリティの重要性の増加等を踏まえ、「セキュリティ」「デジタル」「その他」の3分類からセキュリティタスクが占める割合のグラデーションでの表現に変更。
- 人材育成計画について、OT分野とプラス・セキュリティにフォーカスして詳細に解説。

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

（参考）デジタルスキル標準（対象人材５類型とセキュリティ担当のロール）

- DXを推進する人材は、他の類型とのつながりを積極的に構築した上で、他類型の巻き込みや他類型への手助けを行う



DXの取組みにおいて、ビジネスや業務の変革を通じて実現したいこと（＝目的）を設定したうえで、関係者をコーディネートし関係者間の協働関係の構築をリードしながら、目的実現に向けたプロセスの一貫した推進を通じて、目的を実現する人材

ビジネスの視点、顧客・ユーザーの視点等を総合的にとらえ、製品・サービスの方針や開発のプロセスを策定し、それらに沿った製品・サービスのありかたのデザインを担う人材

DXの推進において、データを活用した業務変革や新規ビジネスの実現に向けて、データを収集・解析する仕組みの設計・実装・運用を担う人材

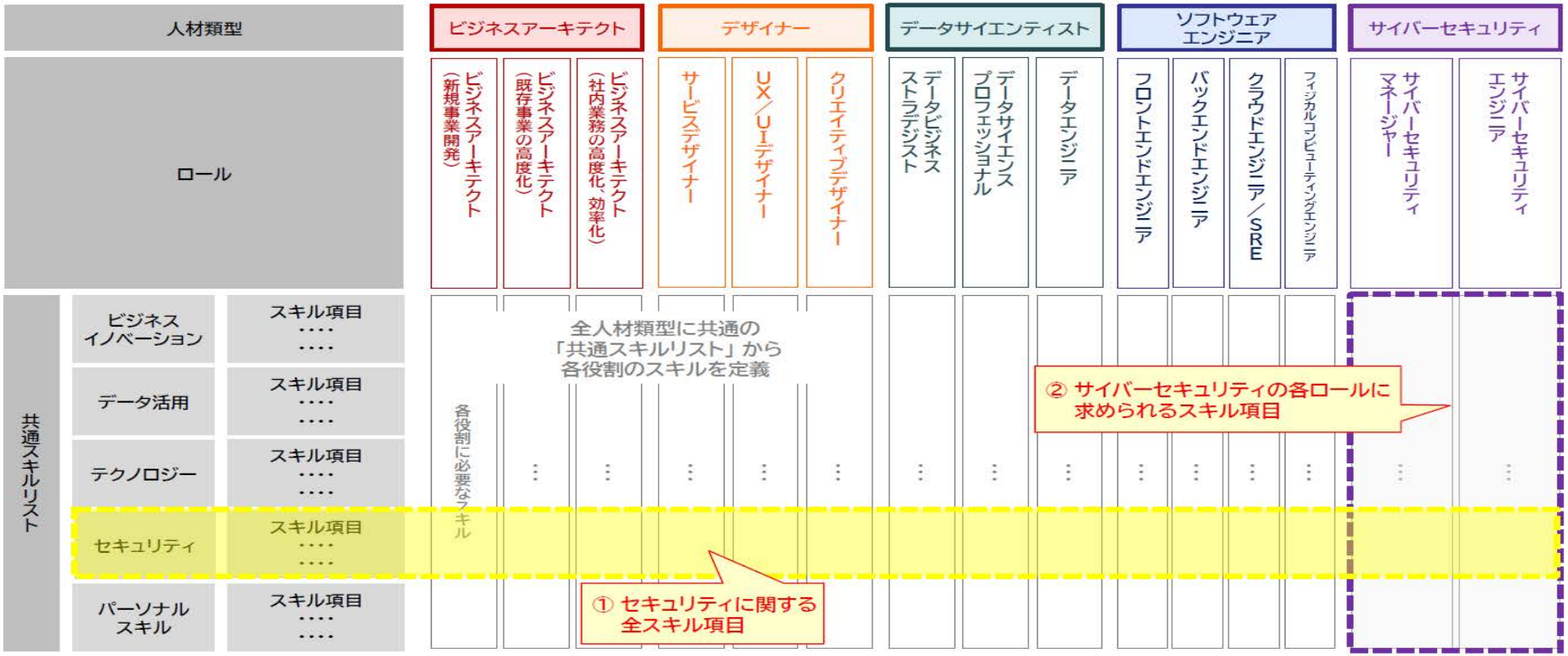
DXの推進において、デジタル技術を活用した製品・サービスを提供するためのシステムやソフトウェアの設計・実装・運用を担う人材

業務プロセスを支えるデジタル環境におけるサイバーセキュリティリスクの影響を抑制する対策を担う人材

人材類型	ロール	DX推進において担う責任
サイバーセキュリティ	サイバーセキュリティマネージャー	顧客価値を拡大するビジネスの企画立案に際して、デジタル活用に伴うサイバーセキュリティリスクを検討・評価するとともに、その影響を抑制するための対策の管理・統制の主導を通じて、顧客価値の高いビジネスへの信頼感向上に貢献する
	サイバーセキュリティエンジニア	事業実施に伴うデジタル活用関連のサイバーセキュリティリスクを抑制するための対策の導入・保守・運用を通じて、顧客価値の高いビジネスの安定的な提供に貢献する

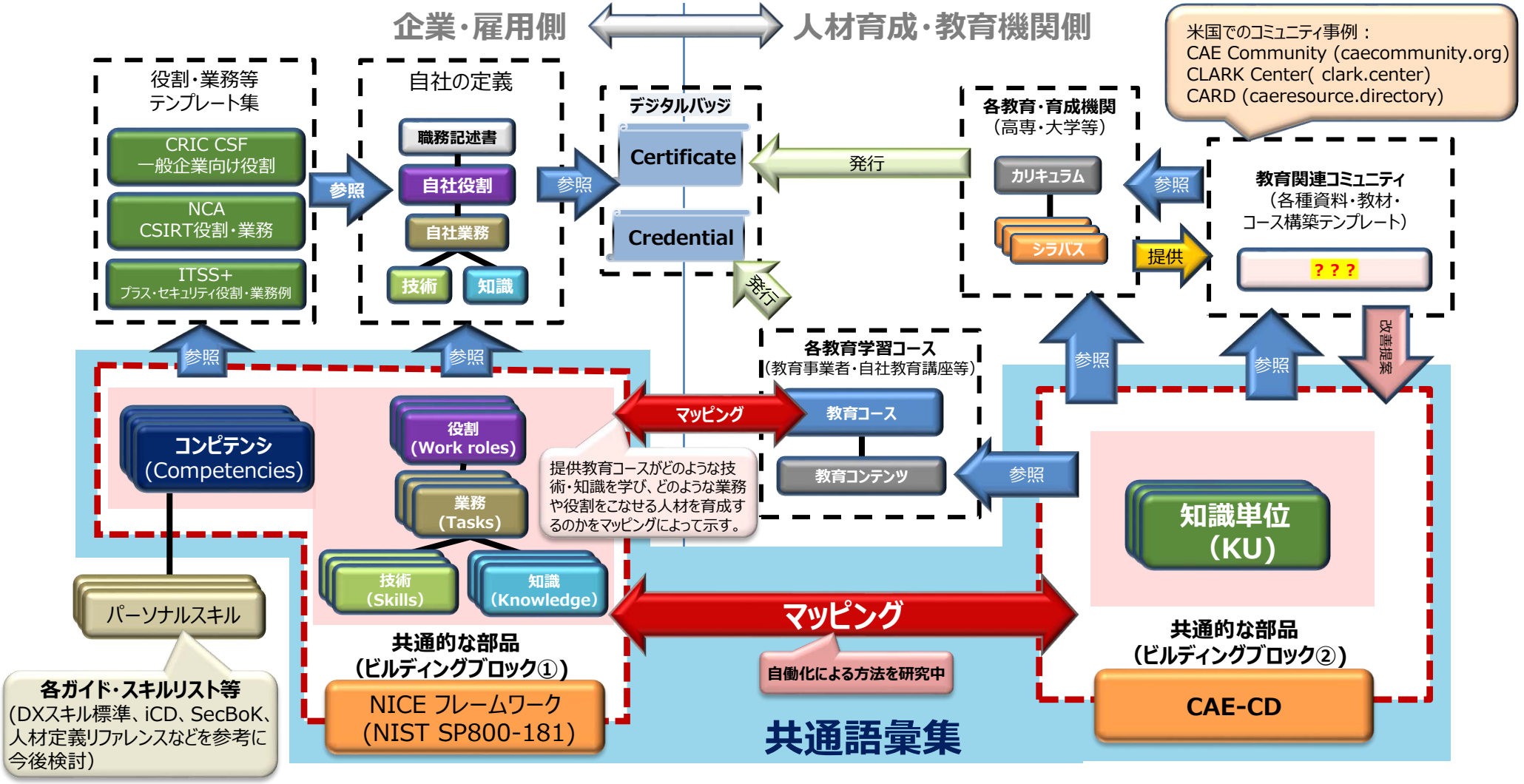
（参考）デジタルスキル標準（セキュリティの位置づけとプラス・セキュリティの対象

- 『サイバーセキュリティ』人材類型の定義：
  業務プロセスを支えるデジタル環境におけるサイバーセキュリティリスクの影響を抑制する対策を担う人材
  - セキュリティを専門としない人材が、自らの担当業務の遂行において必要となるセキュリティスキルの習得に向けた取り組みである**「プラス・セキュリティ」とも連動する**ものである



（参考）共通語彙集の位置づけと概要

- セキュリティ人材に求められる知識・スキル項目について、産・学が共通の認識を持つためのフレームワーク。
- 企業が参照しているNIST SP800-181r1と、学が参照しているCAE-CD/KUの各項目の相互関係を整理。



CAE-CD: National Centers of Academic Excellence Cyber Defense

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）

第７回産業サイバーセキュリティ研究会資料
（2022年４月11日開催）

- 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

サイバーセキュリティに関する米国国土安全保障省（DHS）との大臣級MOC

- **2023年1月6日、マヨルカス国土安全保障長官と西村経産大臣が会談**し、人権タスクフォースへの協力を確認するとともに、**サイバーセキュリティに関するMOCに署名**。
- 今回のMOCでは、①「国家安全保障戦略」の改定を踏まえた経済産業省と国土安全保障省との協力関係の深化、②「開かれたインド太平洋（FOIP）」の実現に向けたインド太平洋における能力構築、③サイバーセキュリティ制度調和の促進、の実現を目指す。

【MOC概要】

経済産業省と米国国土安全保障省は、高度化し増加し続けるサイバー攻撃への対応のため、関係機関からの協力も得ながら、以下のサイバーセキュリティ分野について協力を行う。

＜協力分野＞

- 運用面での協力
- 制御システムセキュリティの向上
- インド太平洋地域等の能力向上に関する協力
- サイバーセキュリティ関連規制及びスキームの調和のための対話促進

＜MOC改定のねらい＞

①「国家安全保障戦略」改定を踏まえた経済産業省とDHSとの協力深化
②「FOIP」実現に向けたインド太平洋地域での能力構築
③制度調和の促進

＜今回のMOCにおいて追加された協力分野＞

・インド太平洋地域等の能力向上
・日米間のサイバーセキュリティ関連規制・制度の調和に向けた対話
（SBOMやIoT機器ラベリング制度等の調和を想定）

ご指摘事項一覧

	主な御指摘事項	取組状況
経営	自社や取引相手のセキュリティ対策状況を可視化し、セキュリティリスクを事前に把握することが必要である。	経営ガイドラインの改訂に伴い、可視化ツールを更新済。
	経営ガイドライン改訂に関する御意見。	経営ガイドラインの改訂に反映。
中小	中小企業がサイバーセキュリティお助け隊サービスを導入するにあたり、コスト負担を補助金等で支援できないか。	IT導入補助金において、サイバーセキュリティお助け隊サービスの導入支援を実施。
	お助け隊サービスの加入促進策の検討では、発注元企業からの紹介事例や利用者の加入経緯等を分析してはどうか。	「事業者連絡会」において、業界団体に加盟する発注元企業からの紹介があったことなど、中小企業の導入事例を共有。
	地域の金融機関に中小企業のセキュリティ対策支援を実施してもらうのは良いアイディアだが、金融機関側の課題意識が無いのではないか。地域中小企業のセキュリティ対策のインセンティブとして、金融機関で金利減免や貸付枠の拡大などの工夫が必要。	地銀協等との意見交換を実施し、顧客の中小企業に対し、お助け隊サービス等の支援策の情報提供に協力いただいている。
	中小企業に対しては情報漏洩よりも事業継続リスクに焦点を当て、意識の醸成を図ってはどうか。	「中小企業の事業継続力強化計画策定の手引き」にサイバーセキュティ対策を追記。
	セキュリティに関心のない企業に対し、セキュリティに目を向けてもらうためには何ができるか。	より効果的な訴求方法について議論予定。
	パートナーシップ構築宣言の中で、サイバーセキュリティ対策を進められるように中小企業庁に依頼できないか。	「パートナーシップ構築宣言」のひな形にセキュリティの項目を追加。
	発注元企業やサプライチェーンの頂点にある企業がセキュリティ対策を義務付ければ、セキュリティに関心がない企業も対策せざるを得ないのではないか。事例を収集し、横展開できないか。	取引先に対するサイバーセキュリティ対策の支援・要請に関する考え方について整理した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を経済産業省・公正取引委員会が発表。

	主な御指摘事項	取組状況
地域	大学、自治体と地元企業の三者でコンソーシアムを作り、地域におけるセキュリティの活動を議論してはどうか。	大学や自治体、地元企業も参加する各地域SECUNITYで、63回ワークショップ等を開催し、2,800名以上が参加。
	地域を管轄する警察や自治体を管轄する総務省と連携し、支援すべき中小企業の対象領域を拡大できないか。	サイバーセキュリティお助け隊サービスの紹介を各県警からも実施いただくなどの連携強化を進めている。
	事故からアラートが上がるような仕組みはあるが、日頃のコミュニケーションの中で相談できるような窓口のようなものがあったら良い。	中小企業の相談体制の強化も含めて、本日議論予定。
人材	情報システム担当者が経営層へインシデントの説明ができるように、担当者と経営者の双方の知識やスキルを上げる必要がある。	「サイバーセキュリティ体制構築・人材確保の手引き（経営ガイドライン付録F）」を改訂。
	プラスセキュリティ人材の育成について、具体策を検討し企業へ提示していくべきである。プラスセキュリティとは、どの人材層に何を実施しようとしているのかを明確にすべきである。	「デジタルスキル標準　第１版」で、DXを進める事業部門におけるサイバーセキュリティに関するスキルについて定義。
	セキュリティ人材やプラスセキュリティ人材の評価方法と人事・給与制度の連携を検討すべき。	セキュリティ人材の活躍の場の確保について、本日議論予定。
	サイバーセキュリティ戦略で、「対策推進に向けた専門人材との協働等に資するよう、法令への理解を深めるツール等の活用促進を図る。」とあるが、このツールがどこかにあると期待している。	「関係法令Q＆Aハンドブック 第１版」の改訂をNISCのワーキンググループにおいて検討中。
	ベンダやサプライヤをコントロールするためにも、セキュリティ言語は統一すべき。	NICEフレームワーク（NIST SP800-181)と、CAE-CD/KU*の関係を整理し、共通語彙集の試案を策定。

１．昨年WG以降のサイバーセキュリティを巡る状況変化

２．昨年WGで御指摘いただいた事項の対応状況

３．本日御議論いただきたい論点

特に御議論いただきたい事項

１．サプライチェーン対策（中小企業・地域、経営）

（１）中小企業・地域

- 中小企業は我が国企業数の大部分を占め、重要なサプライチェーンを構成している。取引先を踏み台にした攻撃も確認されていることから対策は急務。 IPAの調査（2021）では、業務用パソコンを使用する企業は９割を超えて、Webサイトの開設、独自ドメインの電子メールの使用、会計システム・アプリの活用は６割を超える一方、３年間セキュリティ投資を行っていないと回答する企業が３割存在。
  - 中小企業の規模は様々であり、規模に応じて、実行可能なセキュリティ対策は異なる。守るべき情報の量・性質も企業にとって様々であるが、リスク分析・情報資産管理やセキュリティ機器・サービス導入といった基本的な対策について、**様々な企業規模の中小企業に対し、経営のIT依存度の観点も考慮しつつ、どのように促していくべきか**。
  - 取引先からのセキュリティに関する取引上の要請はないと回答する企業が６割。発注元企業の独禁法／下請法への抵触を懸念する声に対応し、経産省・公取委は考え方を公表したが、**発注元企業と発注先企業のパートナーシップによるセキュリティ対策の向上に、どのように取り組むべきか**。
  - **セキュリティ対策の必要性を感じていない企業**に対し、どのように働きかけていくべきか。
  - **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**は創設から３年目を迎え、業種別ガイドラインの共通項の抽出や人材育成のためのセキュリティ用語の整理など、個々の業界では対応できない業界横断的な課題に取り組んでいる。サプライチェーンが複雑化し、動的に構成されていく中、横断的に取り組むべき課題としては、どのようなものがあるか。
  - **中小企業は情報システム担当を専任で設置することができない現状**がある中で、**セキュリティ対策も含めて、情報システム部門のシェアサービスの活用が有効**との指摘がある。中小企業がセキュリティ対策に取り組むことができるような環境整備として、どのようなことが考えられるか。
  - 中小企業のセキュリティに関する**相談体制や、被害状況の把握の充実・被害の拡大防止**を図るために、どのような環境整備を進めることが必要か。

- 地域に広がるサプライチェーン対策の強化のため、総務省や県警等の協力を得て、地域SECUNITYを形成してきた。**ラストワンマイルを担うプレイヤーはそれぞれの地域で多様**である中、地域の活動を継続的かつ効果的なものとしていくため、**どのような組織の参画を得て、どのように連携をしていくべきか**。地域SECUNITYでは、**イベントの開催等を通じて、コミュニティの形成支援を進めてきたが、さらに地域企業の参画を促すべく、どのような機能**が求められるか。

（２）サイバーセキュリティ経営の評価と実効性向上

- **企業のセキュリティレベル（成熟度）を評価するツール**は、IPAによる「可視化ツール」をはじめ、様々なものが存在している。サプライチェーンを構成する企業のサイバーセキュリティ経営を促す観点から、企業のセキュリティレベルが可視化されることで、経営者の善管注意義務への働きかけや市場での評価につながることが期待されるが、それぞれのツールの特徴に応じた活用をどのように進めていくべきか。
- 企業間の取引においても、取引先にセキュリティの実施状況を確認する取組が進んできていると認識しているが、様々な業界又は企業と取引が行われる中で要請される確認事項が多種多様であり、発注元／発注先双方とも負担感が高まっているといった声もある。**サプライチェーンにおけるセキュリティ実施状況の確認について、発注元／発注先双方の負担軽減策**を検討してはどうか。あわせて、対策実施を自己宣言する**セキュリティ・アクション**について、普及賛同企業の協力も得つつ、**企業間の取引において宣言企業が評価されるようにする**など、その活用を促すため、どのようなことが取組が考えられるか。
- 可視化ツールやシステム監査基準等については、ガバナンスやセキュリティ運用・管理に関わる対策状況等を評価するものとして機能している。一方、実施や認証取得が主となっているなど、継続的なセキュリティ改善につながっていない可能性もあるため、ガバナンス等に係る評価がメインであり、**より実態的・技術的なセキュリティ対策状況の把握や評価**が必要ではないか。ガバナンスの実効性向上の観点から、技術面・実態面の可視化・評価として、例えば、脆弱性診断や外部アセスメント、ASM（Attack Surface Management）等の活用を促進してはどうか。

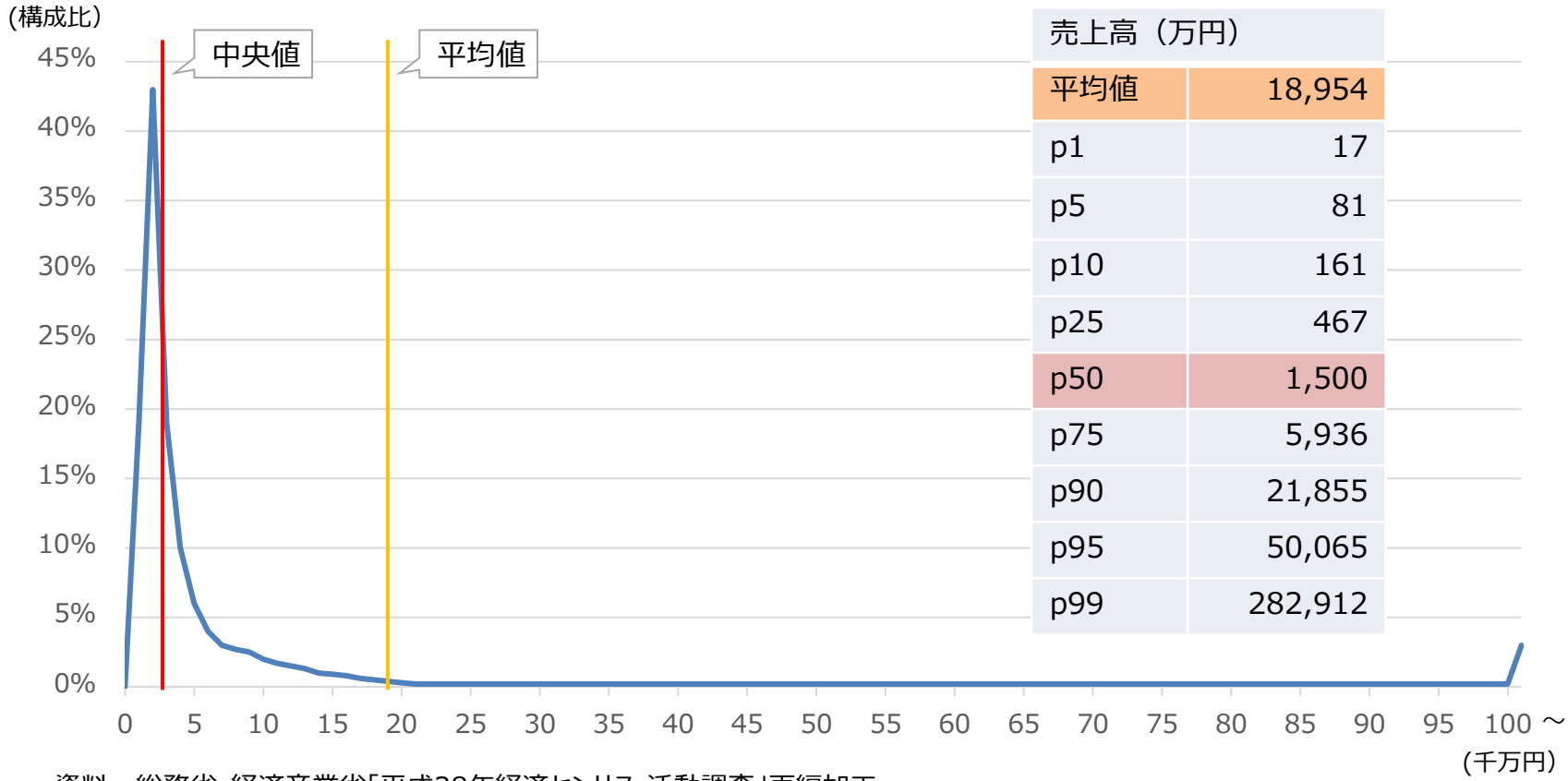
２．人材

- 民間企業の調査によれば、日本企業の９割はセキュリティ人材が不足していると感じ、過去10年以上改善が見られないとの結果がある。同調査によれば、CISOの設置状況は４割にとどまり、９割以上設置している米・豪に比べて大幅に低い状況であり、セキュリティ人材の育成と活躍の場の確保が急務。セキュリティ人材がユーザー企業ではなく、その他分野の企業に偏在しているとの指摘もある。
- セキュリティを専任とする人材の中には、繁忙期における業務量から疲弊してしまう者やセキュリティ業界におけるキャリアパスを描けず他業種へ転身してしまう者、事業を支える立場であるセキュリティ人材は事業部門の人材よりも評価されづらい、といった課題も伺っている。若手から中核クラスまで、政府全体でセキュリティ人材の育成を進めているが、**企業内部における人事制度やセキュリティ人材のキャリアパスの予見性確保の観点から、どのような取組を官民連携で進めていくべきか**。
- 中小企業への専門家派遣事業において、専門家として登録セキスペも対象であることを明確化し、中小企業が相談しやすい環境を構築するとともに、こうした取組を通じた登録セキスペの活躍を支援している。**登録セキスペの活躍を拡充していくため、どのような取組を進めていくべきか**。

（参考）中小企業の売上高分布

- 中小企業の**売上高平均値は２億円弱、中央値は1,500万円**で、**売上高1,000万円以下に４割の中小企業が存在**している。他方で、**売上高10億円超の中小企業は３%**存在している。

第1-2-8図　中小企業の売上高の分布（企業）



売上高（万円）	
平均値	18,954
p1	17
p5	81
p10	161
p25	467
p50	1,500
p75	5,936
p90	21,855
p95	50,065
p99	282,912

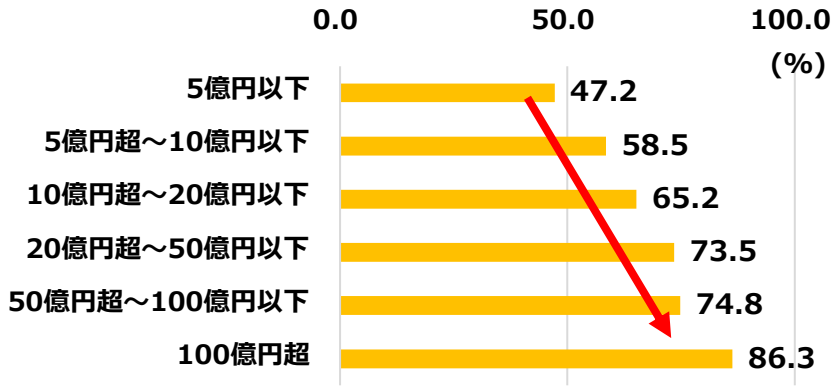
資料：総務省・経済産業省「平成28年経済センサス-活動調査」再編加工

（出典）2021年度中小企業白書　**第1部　令和2年度(2020年度)の中小企業の動向**　第2章：　中小企業・小規模事業者の実態
https://www.chusho.meti.go.jp/pamflet/hakusyo/2021/PDF/chusho/03Hakusyo_part1_chap2_web.pdf

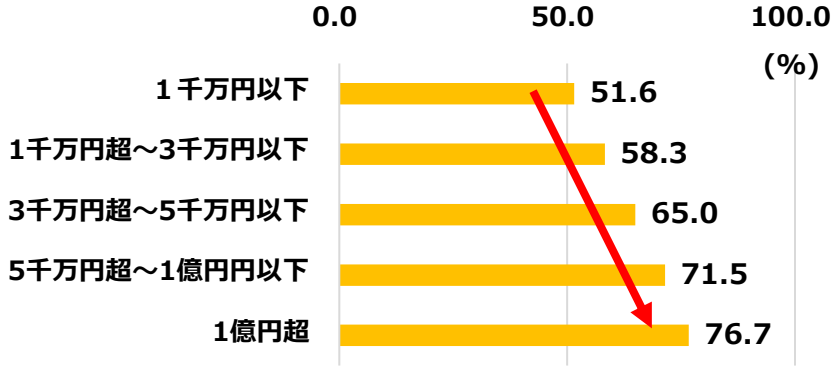
（参考）中小企業のIT導入状況と売上高

- IT依存度について、**ITツール・システムの導入状況は、**従業員、売上、資本金別では**企業規模が大きいほど、導入状況が進んでいる**傾向にある。

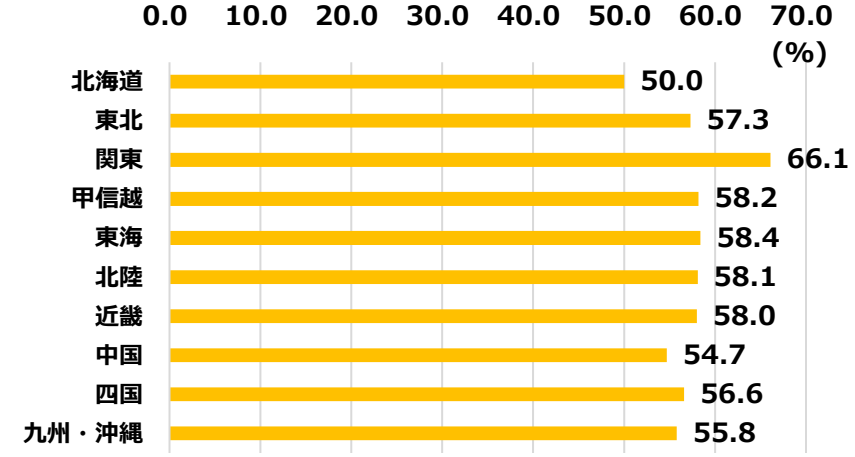
IT導入の実施割合（売上規模別）



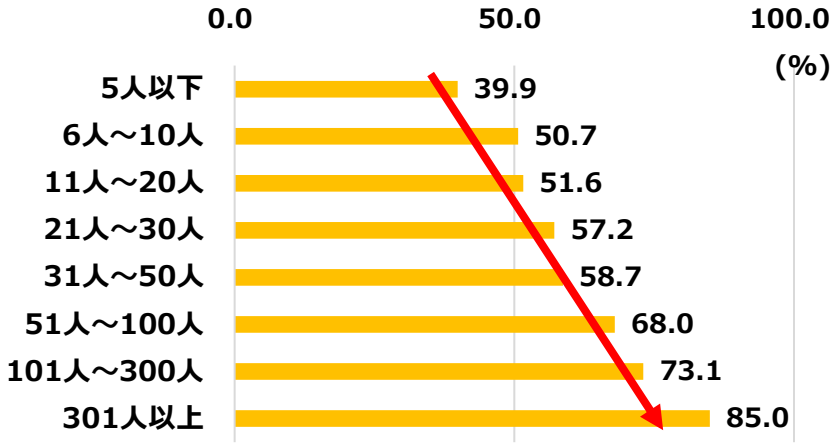
IT導入の実施割合（資本金規模別）



IT導入の実施割合（地域別）



IT導入の実施割合（従業員規模別）



（出典）中小企業のIT導入・活用状況に関する調査（2021年　商工中金）n=4,890, https://www.shokochukin.co.jp/report/research/pdf/other202101.pdf