経済産業省

サプライチェーンにおける
サイバーセキュリティ政策

令和５年９月２２日

商務情報政策局　サイバーセキュリティ課

サイバーセキュリティ戦略専門官　山田　剛人

１．最近のサイバー攻撃の現状と課題

２．サイバーセキュリティ経営ガイドライン

３．具体的な取組のご紹介

高度化･巧妙化するサイバー攻撃の現状

- **昨今のサイバー攻撃は、**企業等の情報を暗号化して金銭をゆすり取る「ランサムウェア攻撃」や、国家支援型の攻撃集団等が特定の企業を執拗に狙う「標的型攻撃」など、**多種多様**。
- 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。

情報セキュリティ10大脅威の変遷

- 2023年の組織向け脅威には、**「ランサムウェアによる被害」が３年連続で１位にランクイン。**
- **サプライチェーンの弱点を悪用する攻撃が2位にランクイン。**対策の重要性が増してきている。
- **「犯罪のビジネス化」が初のランクイン。**攻撃の多様化、被害組織の広がりにつながっている。
- 被害が潜伏する標的型攻撃については、引き続き、注意が必要。

脅威の種類		順位の変遷							
		2023	2022	2021	2020	2019	2018	2017	2016
1	ランサムウェアによる被害	1	1	1	5	3	2	2	7
2	サプライチェーンの弱点を悪用した攻撃	2	3	4	4	4	-	-	-
3	標的型攻撃による機密情報の窃取	3	2	2	1	1	1	1	1
4	内部不正による情報漏えい	4	5	6	2	5	8	5	2
5	テレワーク等のニューノーマルな働き方を狙った攻撃	5	4	3	-	-	-	-	-
6	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	6	7	-	-	-	-	-	-
7	ビジネスメール詐欺による金銭被害	7	8	5	3	2	3	-	-
8	脆弱性対策情報の公開に伴う悪用増加	8	6	１０	-	9	4	-	-
9	不注意による情報漏えい等の被害	9	10	9	7	10	-	-	-
10	犯罪のビジネス化（アンダーグラウンドサービス）	10	–	–	–	-	-	-	-

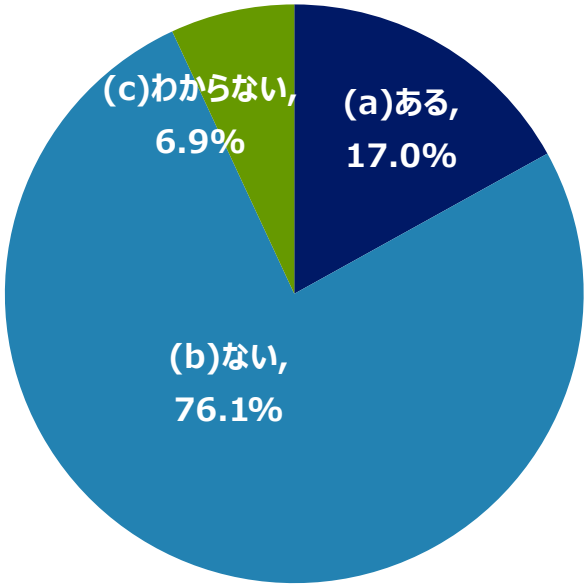
取引先等を経由した大企業・中堅企業のサイバー攻撃被害

- **取引先企業を含むサプライチェーンのサイバーセキュリティ対策は、自社組織のセキュリティ対策に並び重要な要素となっていること**を踏まえ、大企業・中堅企業を対象に、各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の課題や優良事例を経済産業省が調査（※）。
- **大企業・中堅企業の５社に１社に近い割合で取引先等を経由したサイバー攻撃被害の経験**がある。

取引先等を経由したサイバー攻撃被害の経験

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、それが貴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）



(N=1876)

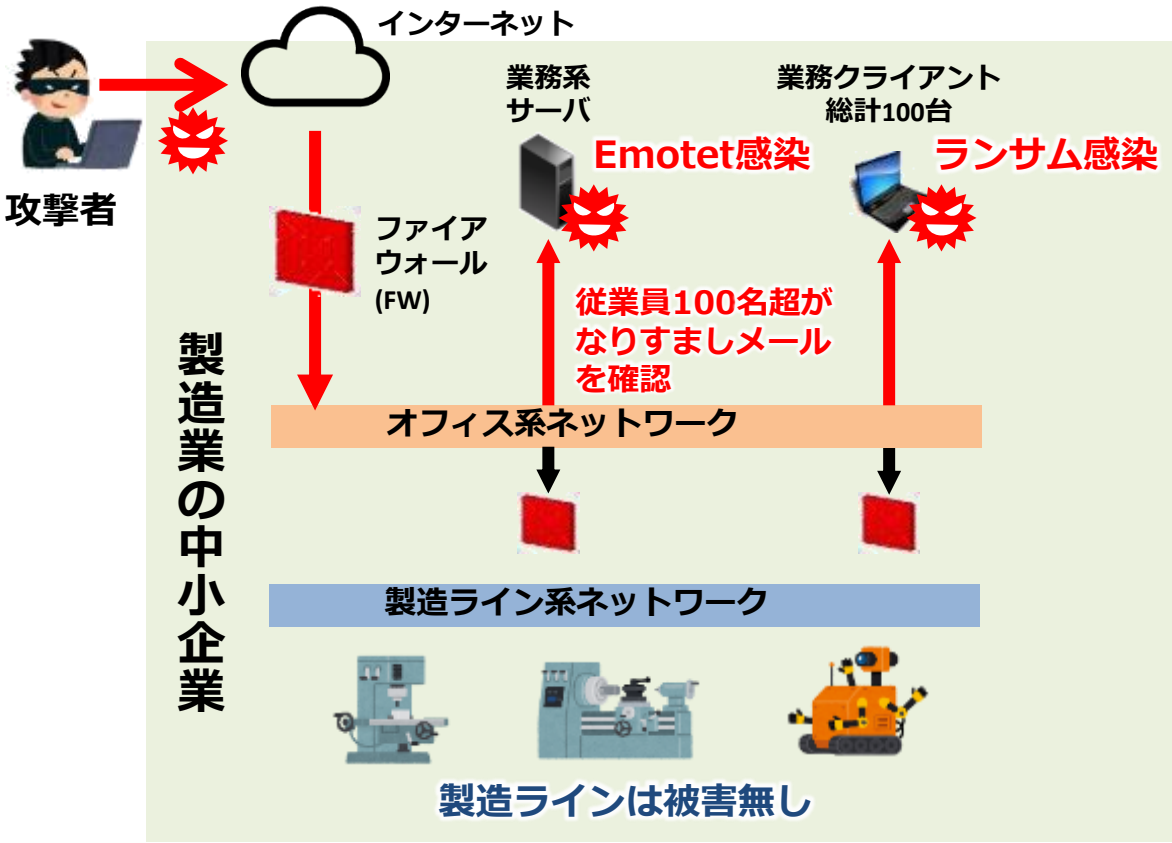
攻撃被害の主な内容

Emotet	● 取引先等がEmotetに感染し、不正なメールを受信
ランサムウェア	● 取引先等がランサムウェアに感染し、自社関連情報が暗号化／外部漏洩 ● 取引先等がランサムウェアに感染、業務停止し、自社業務に影響
不正アクセス	● 取引先等のシステムが不正アクセスをうけ、自社関連の情報が漏洩 ● グループ会社がVPNの脆弱性をついた不正アクセスによりネットワーク侵害をうけ情報が漏洩
ビジネスメール詐欺	● 取引先等がマルウェアに感染し、取引先を装い金銭を要求する詐欺メールを受信
DDoS攻撃	● 委託先のシステムや利用するクラウドサービスがDDoS攻撃を受け、自社業務に影響
その他	● 取引先等のホームページの改ざんによる、不正サイトへの誘導、自社業務への影響 ● 取引先が提供する電子決済サービスの悪用による顧客口座の不正送金 ● 設備業者がメンテナンスのために持ち込んだPCから社内環境にウイルスが侵入　等

（※）令和３年度サイバー・フィジカル・セキュリティ対策促進事業（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）

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**。

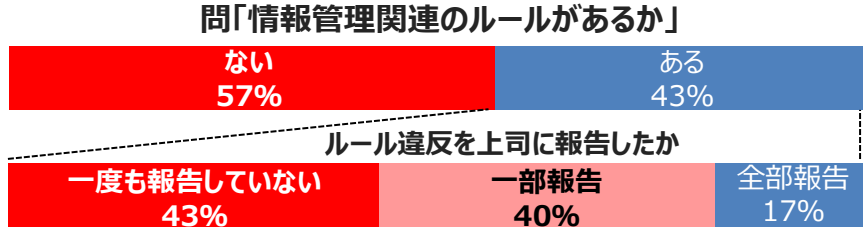
セキュリティ対策実施のきっかけ

	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

- **約60%**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

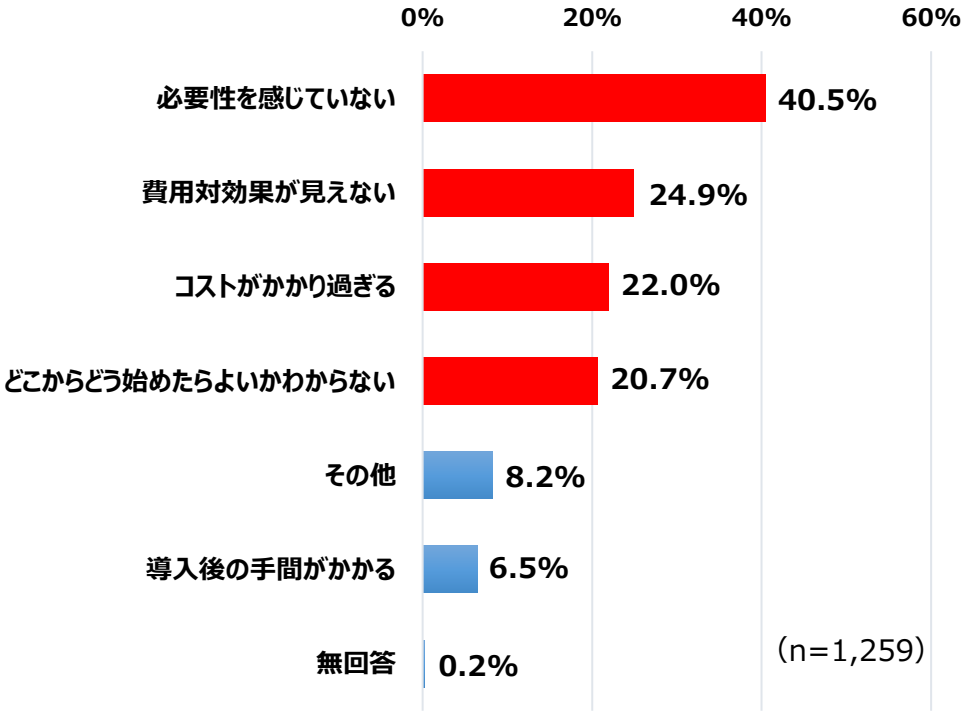
- 中小企業への調査によると、ガイドラインの認知度は14%で、**7割**の中小企業がIPAによる支援を**「知っているものはない」**と回答。
- 中小企業は**情報セキュリティ業務について、「委託していない（58.7%）」、「わからない（11.3%）」**と回答する企業で**７割**を占めており、自力で対策する必要がある。他方、情報セキュリティについて、**「組織的には行っていない（49.2%）」、「兼務だが担当者が任命されている（31.5%）」**となっており、専属者が居ない。

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）

中小企業のセキュリティ対策のリソース不足

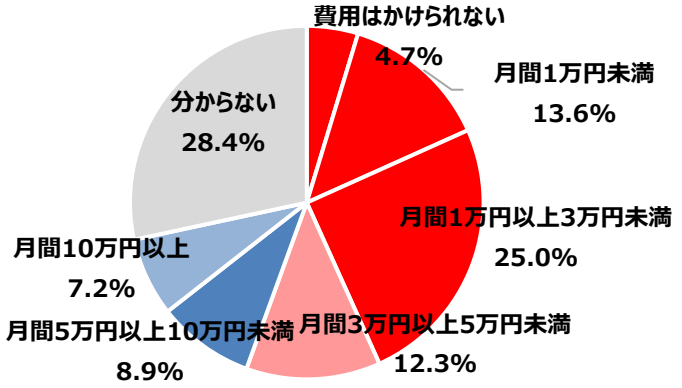
- 中小企業のうち、**過去３年間、全くセキュリティ投資をしていないと回答する企業が３割**に上る。このうち、**４割の企業が「必要性を感じない」**、**2割が「費用対効果が見えない」**と回答。また、合計で**４割が「どこからどう始めたらよいかわからない」「コストがかかり過ぎる」**と回答。
- 中小企業については、セキュリティに支出可能な金額は**月額３万円未満と回答する企業が４割超**。
- 大企業も含めたセキュリティ人材については、米・豪は９割が「充足している」と回答しているが、日本企業は**9割**がセキュリティ対策人材が**「不足している」**と回答。

情報セキュリティ対策投資を行わなかった理由



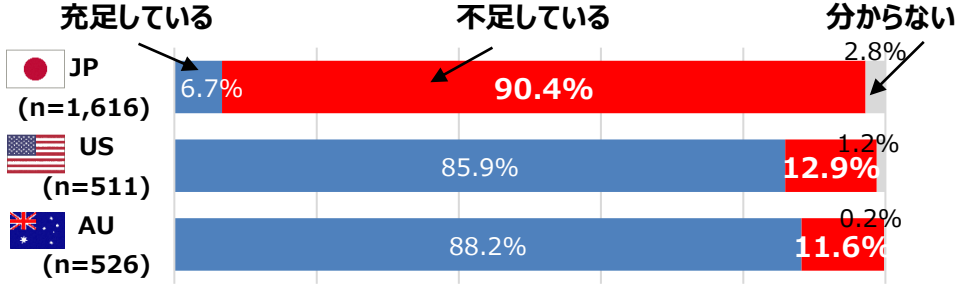
出典：2021年度中小企業における情報セキュリティ対策に関する実態調査

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）

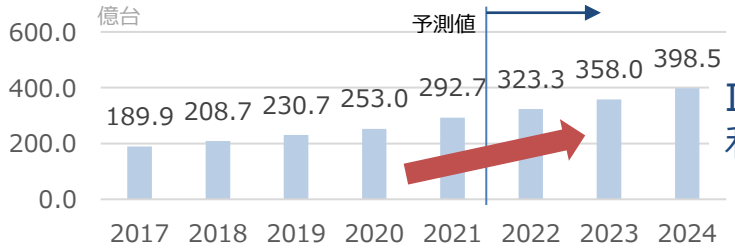
セキュリティ対策人材の不足



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）

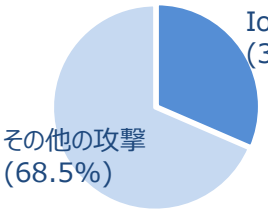
IoT機器の利用拡大に伴い増加するリスクと、その経営への影響

ネットワークに接続される機器(IoT機器)は増加傾向、IoT機器を狙った攻撃は多い



IoT機器の
利用数は増加

世界のIoT機器数の推移及び予測(※1)



ダークネットにおける年間観測パケット数の割合(※2)

不審な通信のうち
約1/3はIoT機器を狙った攻撃

[※1] 出所:総務省「情報通信白書令和4年版 データ集」(3章関連データ)
[※2] 出所:NICT「NICTER観測レポート2022」調査を除く攻撃パケットのうち、23/TCP、22/TCP、5555/TCP、81/TCPへのパケットを集計。

IoTにおけるセキュリティインシデントが経営に大きな影響を及ぼす可能性が高まっている

操業停止や逸失利益の発生を含む事業への直接的な影響

半導体製造工場の制御装置に対する攻撃によって、**3日間の操業停止、営業機会損失が発生(売上高(四半期)の3%損失)**[台湾:2018]

石油化学工場の安全計装システムを対象とした攻撃による**操業停止。プラント爆発のおそれ**[サウジアラビア:2017]

脆弱性対応や損害賠償を含む追加費用の発生

脆弱性発見による自動車140万台のリコールの発生。脆弱性等の対応で、**2億9900万ユーロ(約394億円)の赤字を計上**(四半期の最終損益) [米国:2015]

評判の低下等より生じる競合優位性の低下

高級ホテルで客室のカードキー発行システムがランサムウェアに感染し、一切のシステム操作が不可能となった。客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生。**サービスの品質が著しく低下** [オーストリア: 2017]

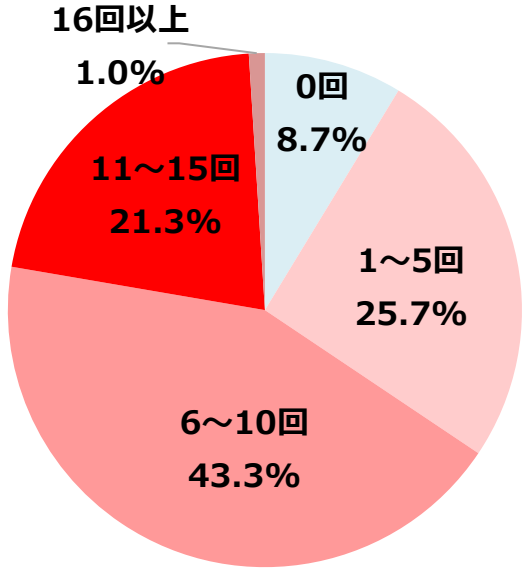
[参考] 各公開情報を基に作成

制御系システムへのサイバー攻撃の影響

- 制御系システムを有する国内の製造・電力・石油/ガス産業へのアンケート調査によると、直近１年で**サイバー攻撃によりシステムの1日以上のシステムの中断を９割の組織が経験。**
- そのうち**２日以上システムの中断が続いたと回答した組織は８割**であり、絶えず稼働することが前提のシステムの中断は、短期間の中断でも組織の収益に大きく影響。**金銭的損害は平均で2.7億円。**

システムの中断を経験した回数

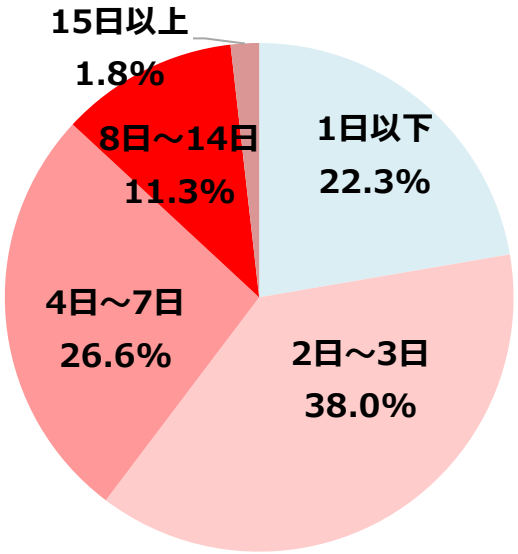
質問：「過去 12 か月間に、サイバー攻撃 （マルウェアの感染、脆弱性を悪用する攻撃、不正アクセスなど）により、あなたの組織の ICS/OT システムの運用は何回中断しましたか」



（n=300）

システムが中断した期間

質問：過去 12 か月間の間、サイバー攻撃の結果、組織の ICS/OT システムの運用は通常、どのくらいの期間中断しましたか」



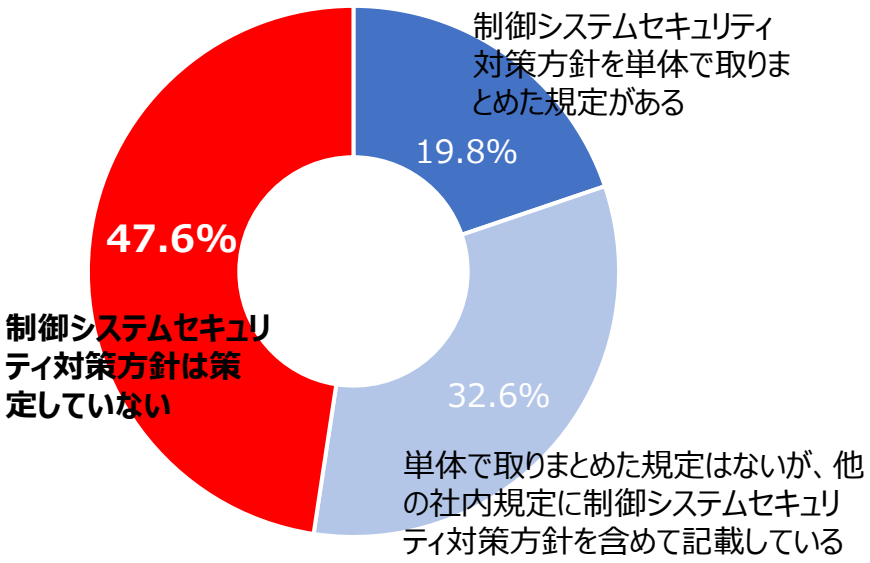
（n=274）

出典：2022年 トレンドマイクロ株式会社 産業制御システムのサイバーセキュリティ実態調査を基に経済産業省が作成
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220711-01.html

制御システムのセキュリティ対策の遅れ

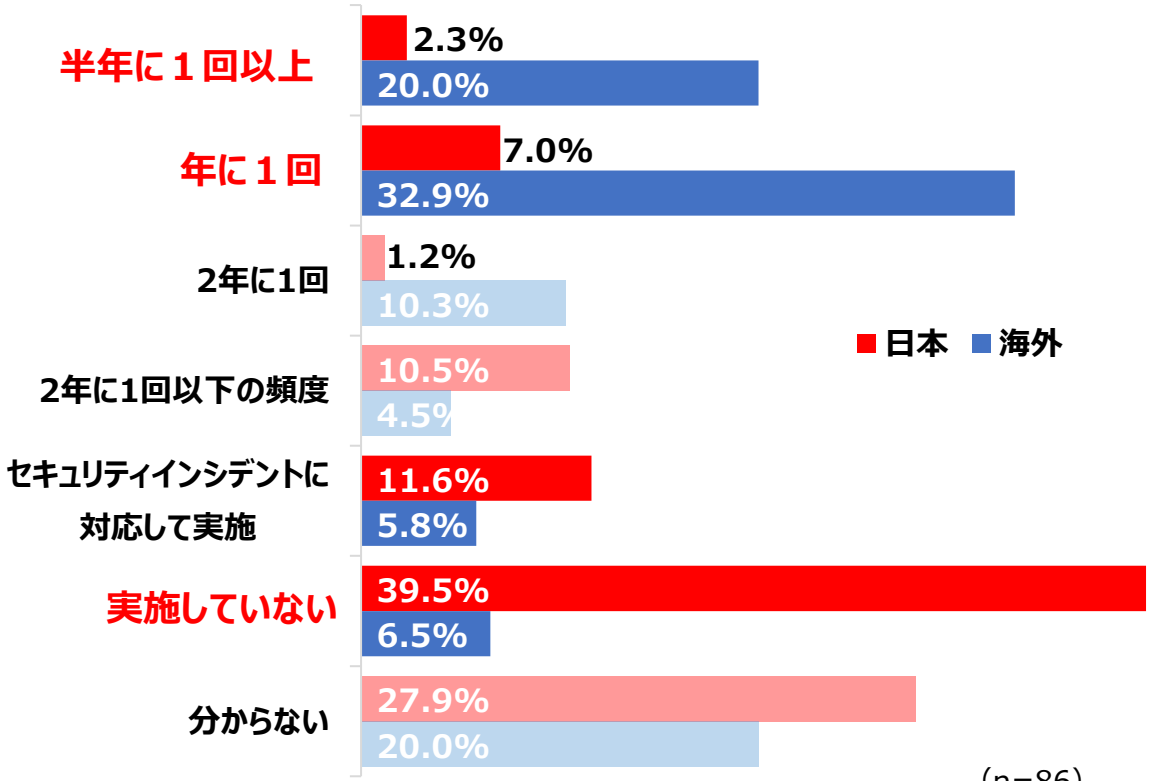
- アンケート調査によると、**制御系セキュリティシステムの対応方針を策定していない企業が５割**存在。
- セキュリティアセスメントについては、**実施していないと回答する企業が４割存在**し、５割以上が半年又は年に１回以上実施する海外と大きく乖離。
- 制御システムのセキュリティ対策方針を主体的に検討し、実際のアセスメントを実施できる、経営層と現場担当者を繋ぐ**中核人材の育成が不可欠**。

制御システムセキュリティ対策方針の整備状況



（n=86）

制御システムに対するセキュリティアセスメントの実施状況



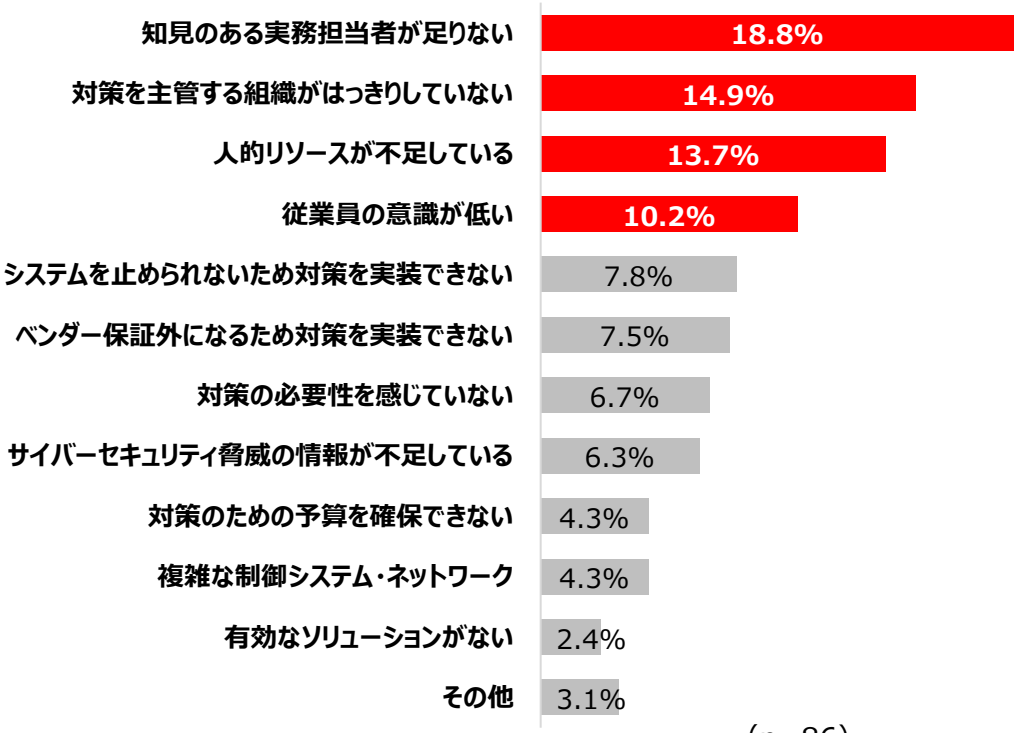
（n=86）

出典：KPMGサイバーセキュリティサーベイ2022
https://assets.kpmg/content/dam/kpmg/jp/pdf/2022/jp-cyber-security-survey2022.pdf

制御システムのセキュリティ人材の不足

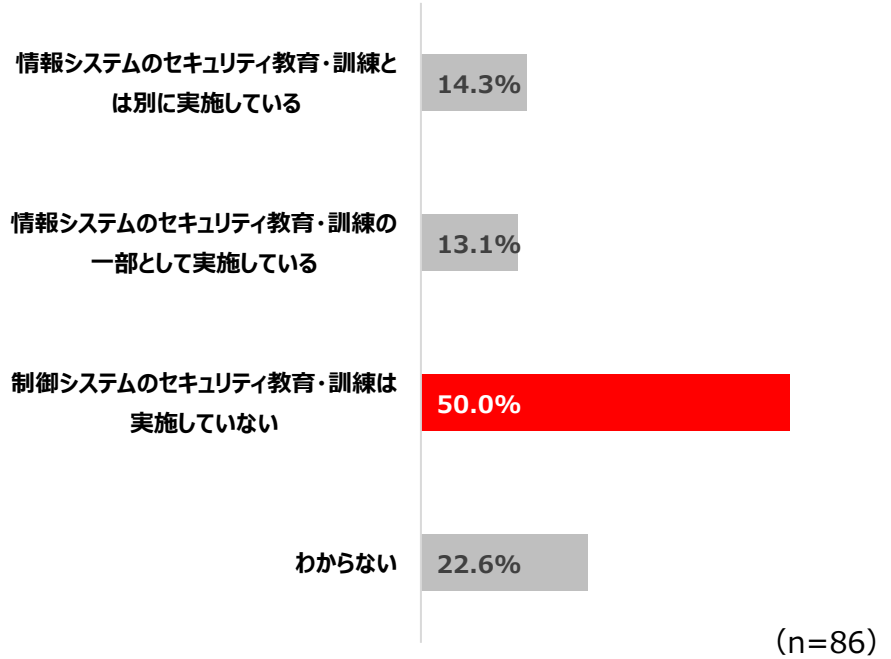
- 制御システムの対策が進んでいない原因として、知見・人的リソースの不足、主管組織が明確になっていないことが主な原因として挙げられており、**組織のセキュリティの中核を担う人材がいない**。
- 制御システムの**「セキュリティ教育・訓練を実施していない」と回答する企業が５割**に上っており、制御システムのセキュリティ人材の確保・育成は大きな課題。

制御システムセキュリティ対策が進んでいない原因



（n=86）

制御システムのセキュリティ教育・訓練の実施状況



（n=86）

出典：KPMG サイバーセキュリティサーベイ2022
https://assets.kpmg/content/dam/kpmg/jp/pdf/2022/jp-cyber-security-survey2022.pdf

１．最近のサイバー攻撃の現状と課題

２．サイバーセキュリティ経営ガイドライン

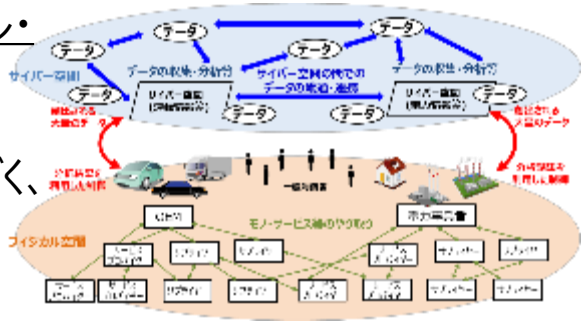
３．具体的な取組のご紹介

経済産業省におけるサイバーセキュリティ政策の全体像

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、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**新たなリスクへの対応が必要**となる。

①業種別／分野横断的なガイドライン等の作成

- 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）に基づく、セキュリティ対策の提示



- SBOM活用に向けた実証事業の実施

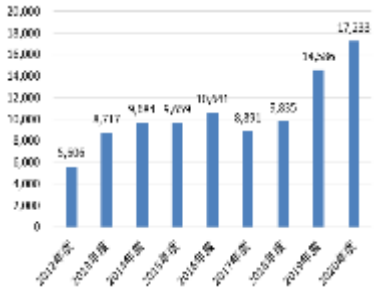
③中小企業/地方へのサイバーセキュリティ対策の普及促進

- サイバーセキュリティお助け隊サービスの普及促進
- 地域単位でセキュリティのためのコミュニティ（地域SECUNITY）の創出
- SC3の活動支援を通じた、サプライチェーン全体でのサイバーセキュリティ強化の取組強化

②事案対処に備える基盤の構築

- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 公的機関や重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- ICSCoEにおける事故調査体制の構築

サイバー攻撃事案の調整件数（年度集計）



④人材育成/国際貢献

- IPA/産業サイバーセキュリティセンターを中心とした人材・組織・システム・技術の開発
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

「Society5.0」の社会を見据えた対策の検討

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、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**新たなリスクへの対応が必要**となる。
- **サイバー・フィジカル・セキュリティ対策フレームワークを策定**し、必要な対策を検討。

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

CPSFのモデル

<3層構造>

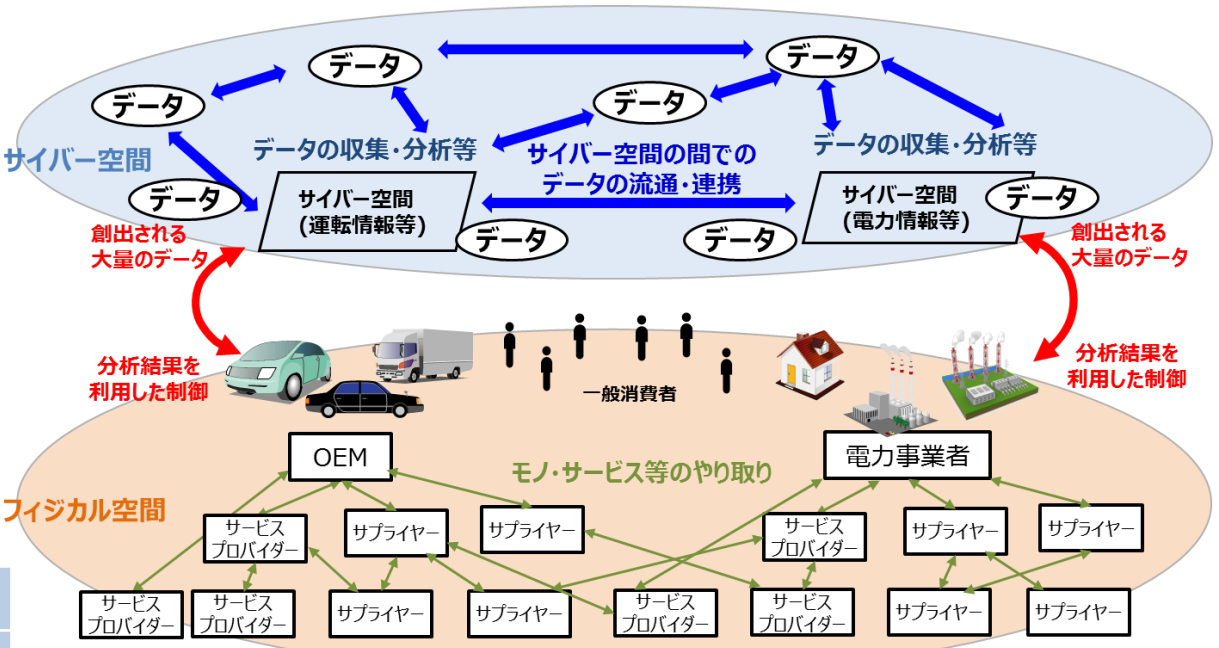
【第３層】
サイバー空間におけるつながり

【第２層】
フィジカル空間とサイバー空間のつながり

【第１層】
企業間のつながり

<6つの構成要素>

ソシキ	ヒト	モノ
データ	プロシージャ	システム



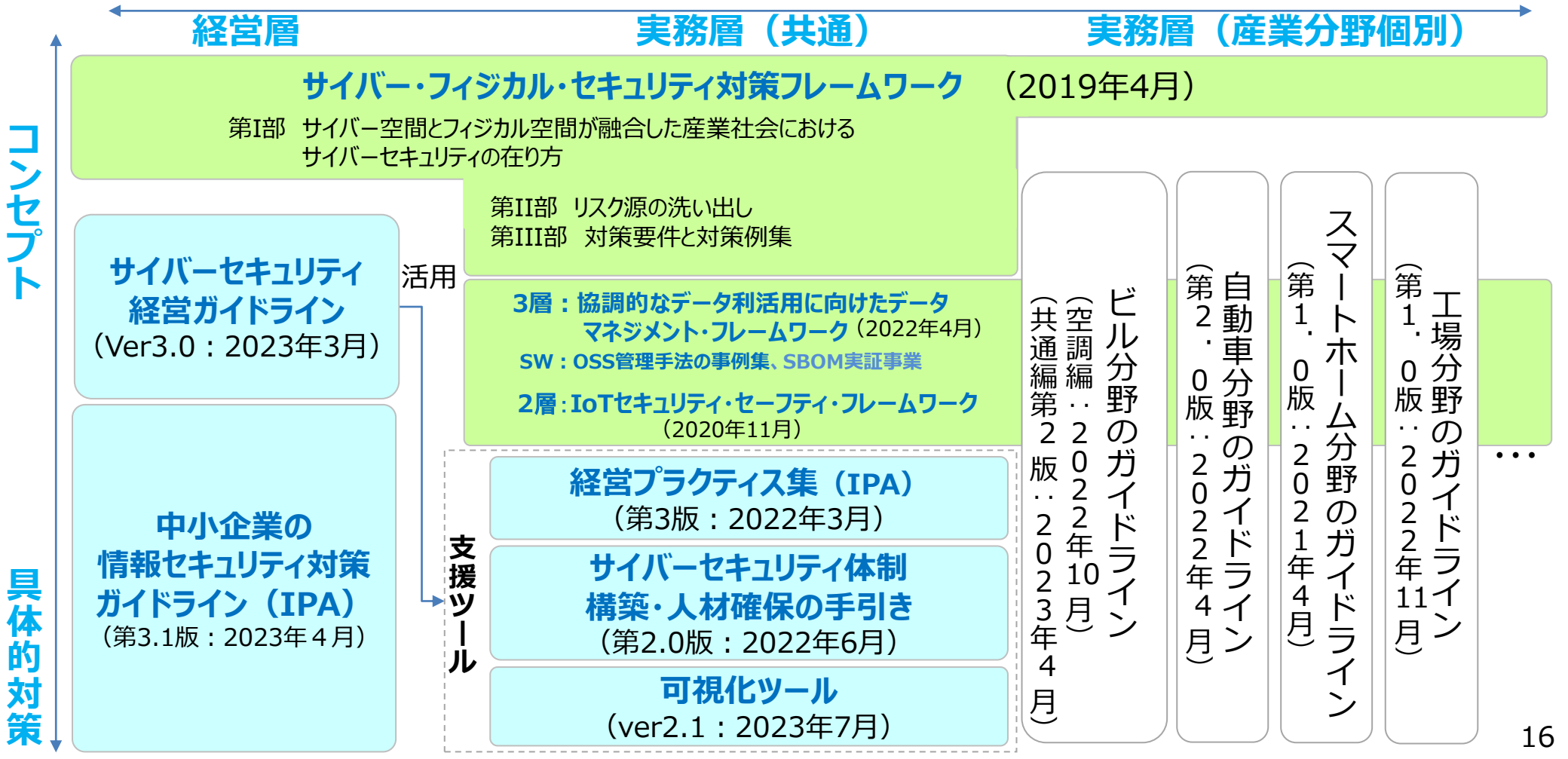
Society5.0の社会におけるモノ・データ等の繋がりのイメージ

https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html

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

- 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＞



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
令和5年3月24日第3版公表

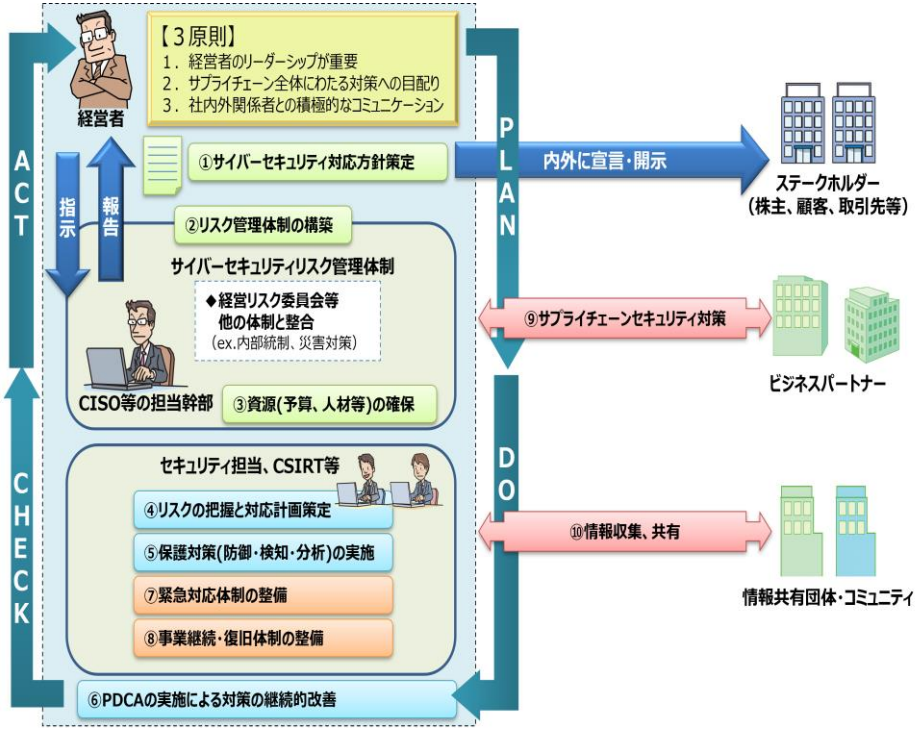
- サイバーセキュリティ対策に当たっては、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要。サイバーセキュリティ対策を推進するため、**経営者を対象としたサイバーセキュリティ経営ガイドラインを策定**。
- ガイドラインにおいては、**経営者が認識すべき３原則**及び**経営者が情報セキュリティ対策を実施する上での責任者（CISO等）に指示すべき１０の重要事項**をまとめている。

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、**サプライチェーン全体にわたる対策**への目配り
（３）平時及び緊急時のいずれにおいても、**社内外関係者との積極的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

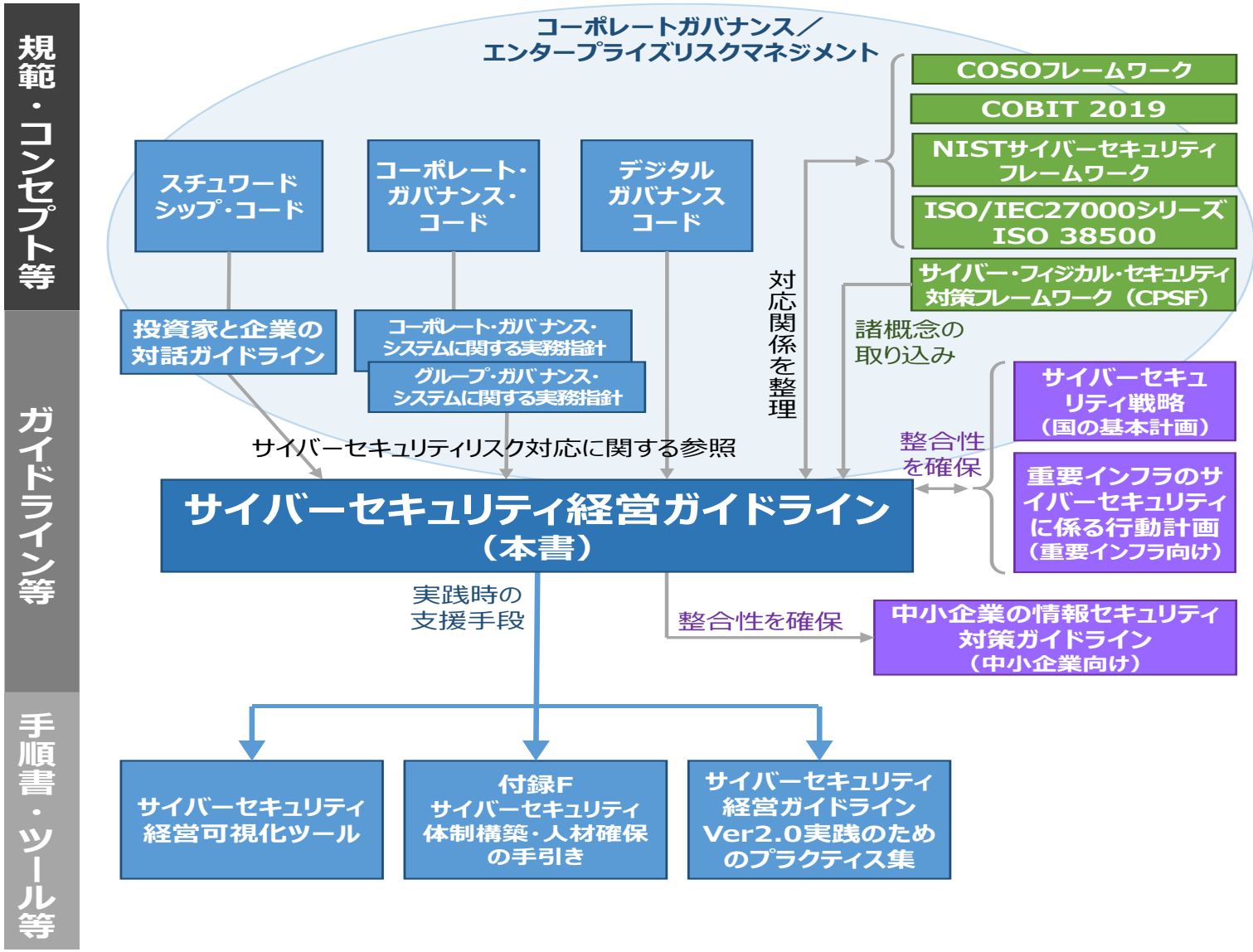
リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAの実施による対策の継続的改善
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 事業継続・復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の状況把握・対策
関係者とのコミュニケーション	**指示10** 情報収集、共有等の促進



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の位置づけ

- 経営者の主導のもとで組織的なサイバーセキュリティ対策を実践するための指針を示すもの。
  経営者、CISO等、また、その人たちを直接補佐する実務者による活用を想定。



サイバーセキュリティ経営ガイドライン Ver3.0の改訂概要（全体）

● 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。

＜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、**サプライチェーン全体にわたる対策**への目配り
（３）平時及び緊急時のいずれにおいても、**社内外関係者との積極的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サイクルの実施による継続的改善
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** 事業継続・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状況把握及び対策
関係者とのコミュニケーション	**指示10**情報収集、共有及び開示の促進

＜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

企業経営におけるサイバーセキュリティ対策の重要性が拡大

- 「投資家と企業の対話ガイドライン」や「グループ・ガバナンス・システムに関する実務指針(グループガイドライン)」、「デジタルガバナンスコード」などにおいて、サイバーセキュリティ対策の必要性について言及。
- 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認識し、**サイバーセキュリティを包含するエンタープライズリスクマネージメントの実践が求められており、対策の実施を通じてサイバーセキュリティに関する残留リスクを許容水準まで低減することは経営者の責務**。
- そのため、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**。

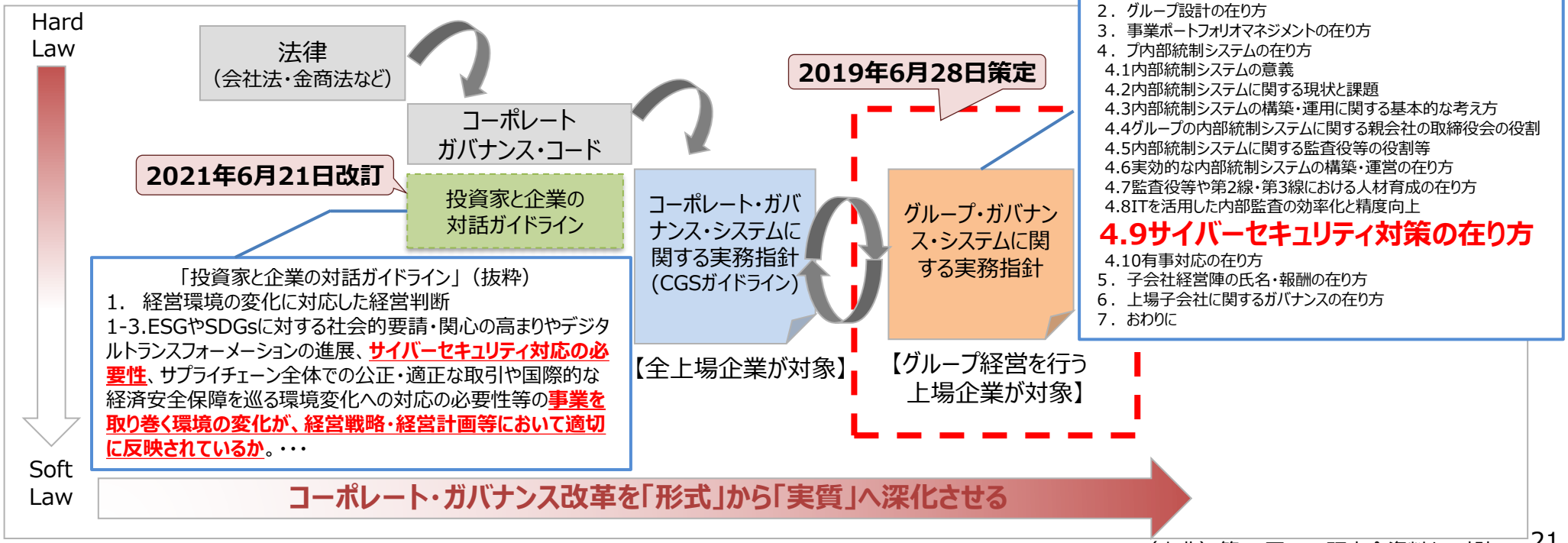
〔Ver.2.0〕
・セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必要なものと位置づけて「投資」と捉えることが重要
・セキュリティ投資は必要不可欠かつ経営者としての責務
・経営責任や法的責任が問われる可能性がある

〔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（けたい）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

コーポレートガバナンスの一環として、サイバーセキュリティ経営を位置づけ

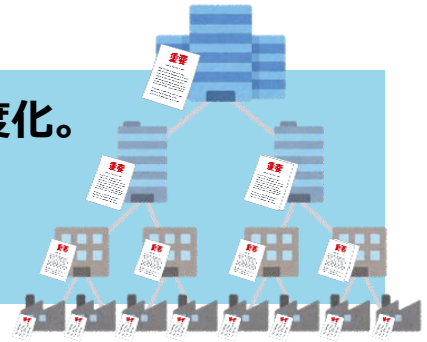
- **「グループ・ガバナンス・システムに関する実務指針(グループガイドライン)」**において、**グループ内部統制システムの一つとして、サイバーセキュリティ対策の在り方を位置づけ**(2019年6月公表)。親会社の**取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れてセキュリティ対策を行うことを検討すべき**ことを明記。
- また、**「スチュワードシップ・コード」及び「コーポレートガバナンス・コード」の付属文書である「投資家と企業の対話ガイドライン」**（金融庁、2021年6月改訂）においても、新たにサイバーセキュリティ対策の必要性等を含む事業環境変化の経営戦略・経営計画等への反映が盛り込まれた。
- このほか、DXを進める企業におけるステークホルダーとの対話の在り方を示す**「デジタルガバナンスコード」**(2020年11月公表)においても、経営者がサイバーセキュリティリスク等に対して適切に対応を行うべき旨を記載。

＜ご参考＞グループ・ガバナンス・システムに関する実務指針の立ち位置



（出典）第13回CGS研究会資料を一部加工

サプライチェーン全体のサイバーセキュリティ対策が急務に



- **大企業から中小企業まで、サプライチェーンの弱点を狙ったサイバー攻撃が顕在化・高度化。**
  - 取引先への攻撃を起点として、自社のシステムが被害を受けるケース
  - サイバー攻撃による取引先の事業停止により、自社の事業が影響を受けるケース
  - ネットワーク監視等のソフトウエアのアップデートを通じてマルウエアが仕込まれ、被害を受けるケース

〔Ver. 3 .0〕

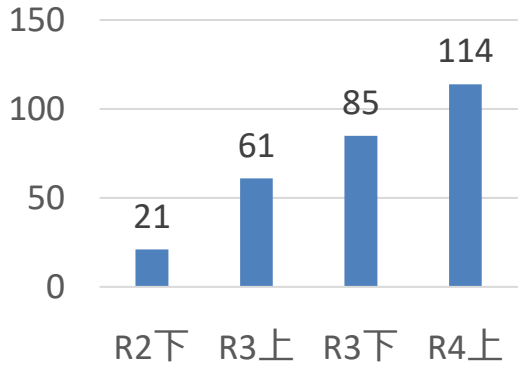
○経営者が認識すべき３原則（２）

・自社のサイバーセキュリティ確保に関する責務を全うするには、国内外の拠点、ビジネスパートナーや委託先等、**サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要**

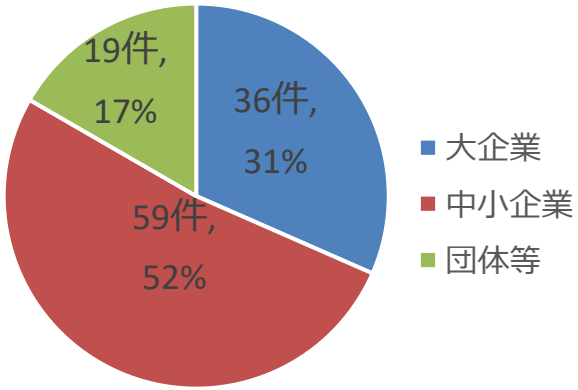
・サプライチェーン全体を俯瞰し、総合的なセキュリティ対策を徹底

○サイバーセキュリティ経営の重点10項目　指示９

・国内外の拠点、ビジネスパートナーや委託先等における状況等の把握をもとに、**サイバーセキュリティ対策の役割、責任の明確化や対策の導入支援等、サプライチェーン全体での方策の実効性を高める適切な方策を検討**



企業・団体等におけるランサムウェア被害の報告件数の推移



ランサムウェア被害の被害企業・団体等の規模別報告件数（令和４年上期）

警察庁「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和4年9月15日）」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

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

サイバーセキュリティ経営ガイドライン Ver3.0への主な改訂内容（1/2）

経営者がCISO等に指示すべき１０の重要事項　※経営者は単なる指示ではなく、リーダーシップの発揮が求められる

リスク管理体制の構築

（指示１）**サイバーセキュリティリスクの認識、組織全体での対応方針の策定**

※経営リスクとして認識、組織全体の対応方針の策定、それを対外的な宣言として公表

（指示２）**サイバーセキュリティリスク管理体制の構築**

※役割と責任の明確化、組織内のリスク管理体制とも整合

（指示３）**サイバーセキュリティ対策のための資源（予算、人材等）確保**

※外部ベンダーや自社のセキュリティ人材の確保・育成。セキュリティ従事者のみならず、事業、管理部門等の従業員も、その業務の中で意識し実施するタスクとしての「プラス・セキュリティ」知識・スキルの明確化、自覚、習得を促す。

リスクの特定と対策の実装

（指示４）**サイバーセキュリティリスクの把握とリスク対応に関する計画の策定**

※事業に用いるデジタル環境、サービス及び情報の特定、サイバー攻撃の脅威・影響度合を踏まえた対応計画。他社事例やベンダ提案のみから実態に合わない計画だと、未対策リスクによる事業中断や情報漏洩のおそれ。厳しければ良い、とするだけでも業務に支障のおそれ。自社のリスクアセスメントを踏まえた対応が必要。その際、脅威インテリジェンス、地政学、産業心理学、組織心理学等の知見等も活用しリスクを抽出。サプライチェーンも対象とし、偽情報、機械学習における誤判断等も、考慮。

（指示５）**サイバーセキュリティリスクに効果的に対応する仕組みの構築**

※保護対策として、防御、検知、分析とそれに基づく対応、といった仕組みの適確な運用。クラウドやゼロトラストモデルを使う場合、インシデント予兆検知の仕組みが従来のままでは見逃しや対応が遅れるおそれ。サイバーリスクに対応した事業継続計画。

（指示６）**PDCAサイクルによるサイバーセキュリティ対策の継続的改善**

※定期的な報告等を受けず、経営者自身でリスクや問題を把握できていない場合、対策が不適となるおそれ。自然災害や機器故障等と異なりリスクが急激に変化するサイバーセキュリティリスクの特徴に対応可能なサイクルの周期と変化に対応できる体制での運用。KPI設定と経営リスクに関する委員会等への報告。脆弱性診断、ペネトレーションテスト、監査等により問題点の抽出と改善。対策状況の情報セキュリティ報告書や有報等を通じた公表など。

サイバーセキュリティ経営ガイドライン Ver3.0への主な改訂内容（2/2）

インシデントに備えた体制構築

（指示７）**インシデント発生時の緊急対応体制の整備**

※サプライチェーン全体のインシデントに対応可能なCSIRT。経営者等への迅速な報告体制、製品・サービスの構成ソフトウェア等の脆弱性や障害対策、原因調査・対処等を行うPSIRT等の構築・運用。「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照し理解増進。役員を入れた定期的な演習（制御系、サプライチェーンも含む）により、緊急時の手順を理解。

（指示８）**インシデントによる被害に備えた事業継続・復旧体制の整備**

※業務のデジタル環境の依存度の増大に伴い、単純にIT環境を復旧させるだけでは事業を再開できない可能性。組織としての事業継続の観点から、業務の復旧プロセスと整合性の取れたデジタル環境の復旧計画及び体制を整備。制御系、サプライチェーン含めた実践的な演習。

サプライチェーンセキュリティ

（指示９）**ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策**

※クラウド利用やAPI連携など企業間の繋がり方は多様化。従来型の提供情報の保護要求のみでは不十分。契約書等において役割・責任の明確化の上、対策を定め、監査、自己点検等により、サプライチェーンリスクへの対応状況把握、対策の導入支援や共同実施、緊急時の協力などサプライチェーン全体での対策実効性を確保。

関係者とのコミュニケーション

（指示10）**サイバーセキュリティに関する情報の収集、共有及び開示の促進**

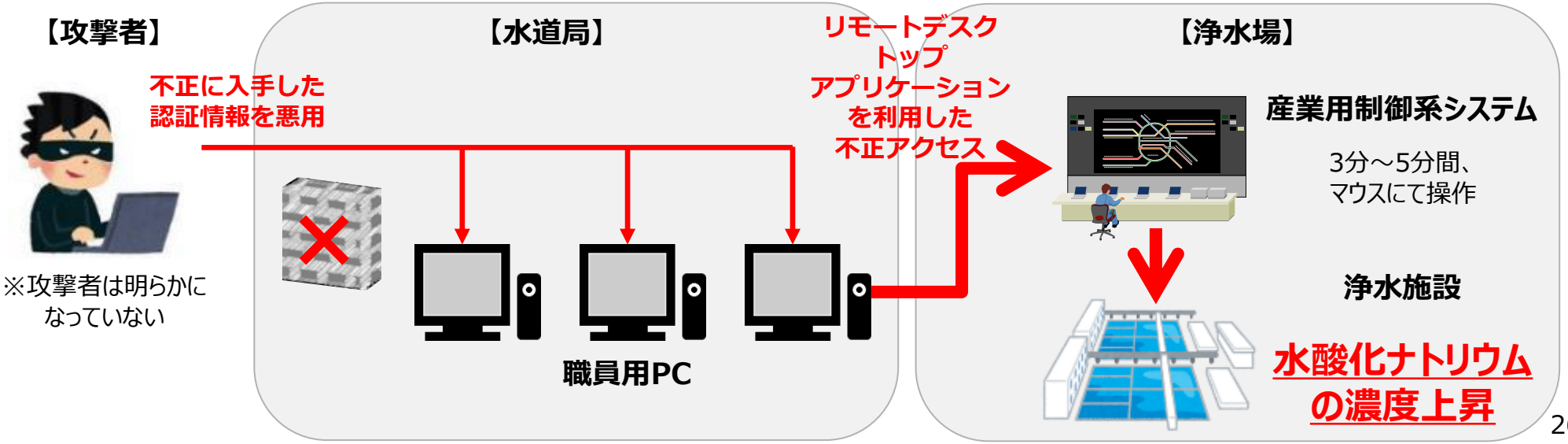
※有益な情報を得るには自ら適切な情報提供を行うことも必要。サイバー攻撃や対策に関する情報共有を行う関係性の構築、被害の報告・公表への適切な備え。「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照し、サイバーセキュリティ専門組織との情報共有や被害情報の公表を行う際の観点についてあらかじめ理解。

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

- データの流通・活用が進むことで、サイバー攻撃の対象も大きく拡大。
  - IoT機器の増加に伴う攻撃拠点の拡大
  - **サイバー攻撃が制御系システムにまで及ぶケース**

〔Ver. 3 .0〕
○サイバーセキュリティ経営の重点10項目　指示７
・制御系を含むサプライチェーン全体のインシデントに対応可能な体制（CSIRT等）を整備
・自社の製品やサービスについて、それらを構成するソフトウエア等における脆弱性や障害に備えた対策の実施や、インシデント発生時の原因調査や対処のための情報発信等の対応を行うPSIRTの構築・運用
○サイバーセキュリティ経営の重点10項目　指示８
・制御系も含めたBCPとの連携等、組織全体として有効かつ整合のとれた復旧目標計画を定める

水道システムへの不正アクセス事例（2021年2月米国）



サイバーセキュリティ体制構築・人材確保の手引き

- サイバーセキュリティ経営ガイドラインの付録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。**

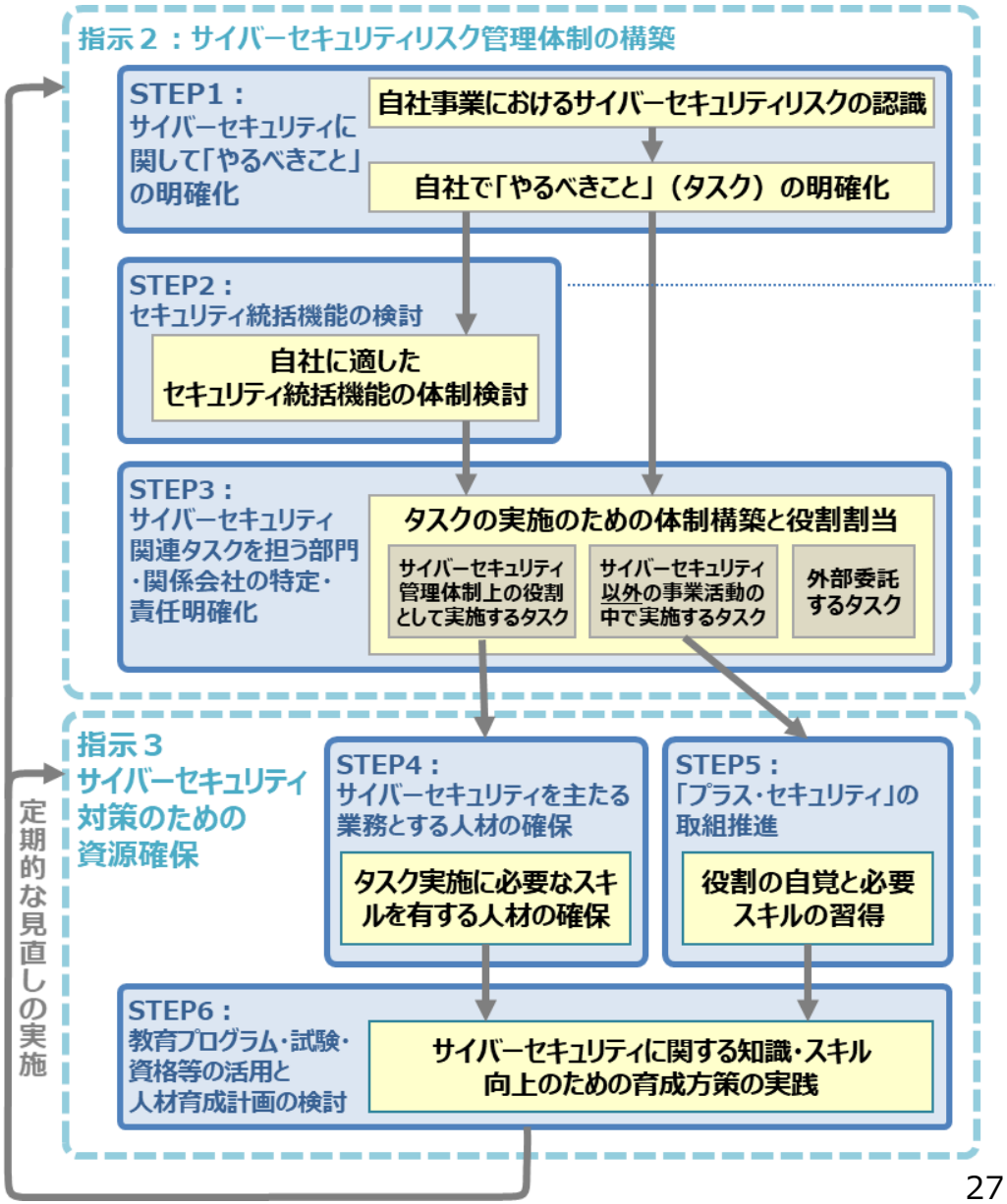
- 2020年9月30日策定、2021年4月15日改訂（Ver.1.1）
- 2022年6月15日改訂（Ver2.0）

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。

経営者のリーダーシップの下、
手引きのポイントを参照しながら、
適切な体制を検討

検討、実践を効率的に進めるための手順



【STEP5】「プラス・セキュリティ」の取組推進

ポイント：
- 関連部門の人材が、サイバーセキュリティを意識し、業務遂行に伴うサイバーセキュリティ対策の実施に必要な能力を備えることができるようにする「プラス・セキュリティ」の取組も重要
- 「プラス・セキュリティ」を担う人材に自らの役割と責任の自覚を促すための意識付け

「プラス・セキュリティ」とは？
自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと

例えば・・・以下のような担当者が「プラス・セキュリティ」を実装していないとこんなリスクが生じます。

クラウドを活用した新規事業を立ち上げるプロジェクトの企画担当者

目的にそぐわない不適切なクラウドを選定することや、シャドークラウド化による情報漏えいリスク

製品設計において組込ソフトウェアの機能仕様を設計する担当者

製品にサイバー攻撃に対する脆弱性を生じさせるリスク

自社の電話、インターネット設備、複合機等の保守契約を扱う総務担当者

不適切な設定のまま運用してしまうことによる、当該機器を介した情報漏えいリスク

手引き本体では、それぞれの人材確保方法について、メリットや留意点なども解説

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

- 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。その後第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**を実施し、2021年4月にIPAより調査結果を公表。本調査結果等も踏まえた上で、プラクティスの追加等を行った**第３版を2022年３月に公表（今年度に改訂を予定）**。

＜主な改訂内容＞

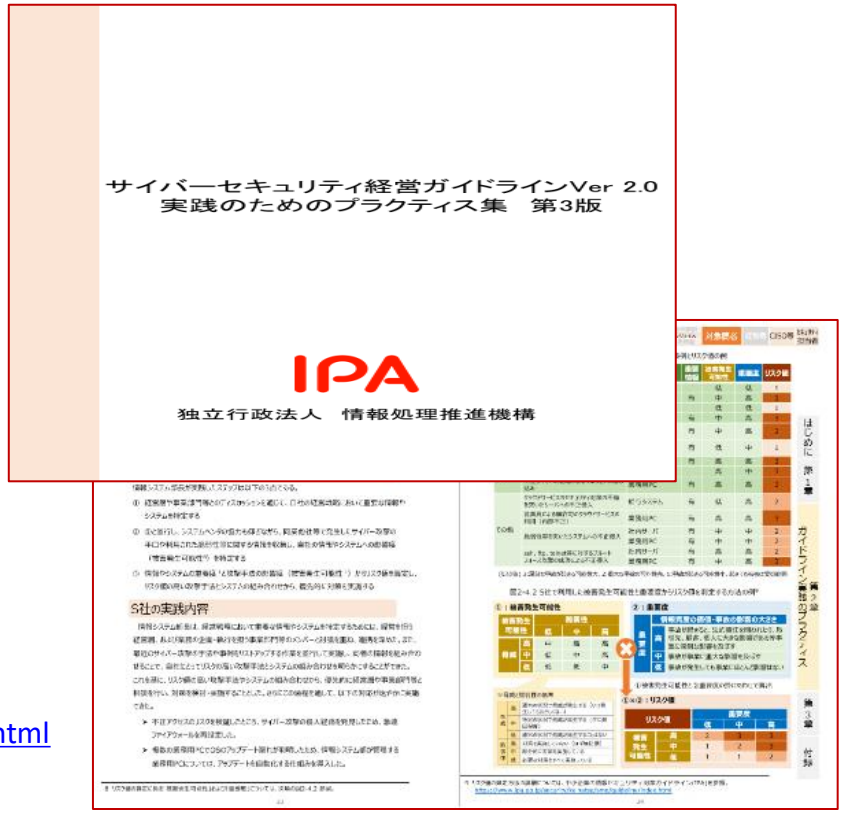
2020年度調査の結果を踏まえ、主に**第2章**と**第3章**の内容を充実させる形で改訂

◆第2章

経営ガイドラインの付録A「チェックシート」より、「指示１」、「指示５」、「指示6」、「指示7」のチェック項目に関するプラクティスを追加

◆第3章

情報セキュリティ10大脅威2022の「組織」向け脅威より、１位「ランサムウェアによる被害」、３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」、４位「サプライチェーンの弱点を悪用した攻撃」、５位「内部不正による情報漏えい」に関するセキュリティ担当者の悩みについてのプラクティスを追加



https://www.ipa.go.jp/security/fy30/reports/ciso/ab7z8i9y7j3o359864fg537y56n90jy8.html

第2章　サイバーセキュリティ経営ガイドライン実践のプラクティス

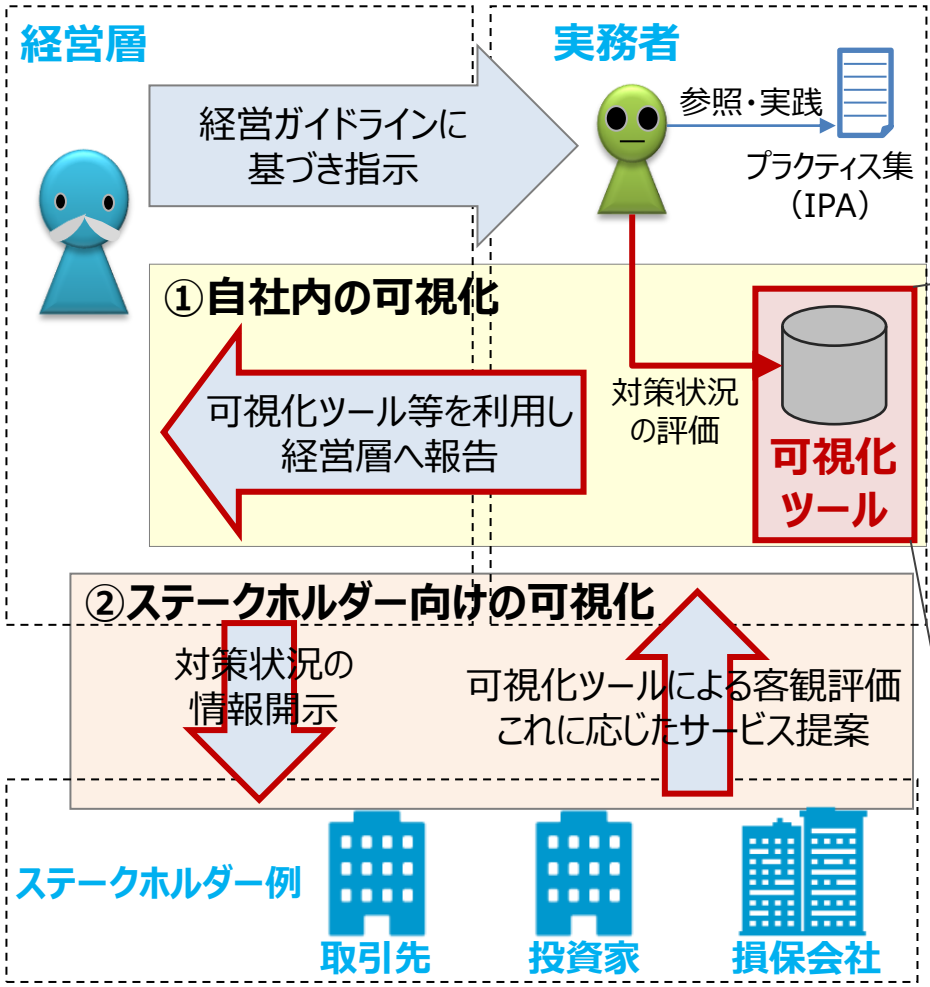
サイバーセキュリティ経営の重要１０項目		実践のプラクティス
1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定	1-1.経営者がサイバーセキュリティリスクを認識するための、他社被害事例の報告 1-2.最新の脅威によるリスクに対応するための、セキュリティポリシーの改訂・共同管理 1-3.海外拠点における情報保護に関するコンプライアンスを拠点別チェックリストで担保
2	サイバーセキュリティリスク管理体制の構築	2-1.サイバーセキュリティリスクに対応するための、兼任のサイバーセキュリティ管理体制の構築
3	サイバーセキュリティ対策のための資源（予算、人材等）確保	3-1.サイバーセキュリティ対策のための、予算の確保 3-2.サイバーセキュリティ対策のための、必要なサイバーセキュリティ人材の定義・育成
4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	4-1.経営への重要度や脅威の可能性を踏まえたサイバーセキュリティリスクの把握と対応
5	サイバーセキュリティリスクに対応するための仕組み構築	5-1.多層防御の実施 5-2.アクセスログの取得 5-3.セキュリティバイデザインを標準とする、クラウドベースの開発プロセスの励行
6	サイバーセキュリティ対策におけるPDCAサイクルの実施	6-1.PDCAサイクルの検証と、演習・訓練を通じた評価・改善プロセスの強化 6-2.一律のルール適用が困難なビジネスにおけるセキュリティKPIを用いたリスク管理 6-3.ステークホルダーの信頼を高めるための、サイバーセキュリティ関連情報発信の工夫
7	インシデント発生時の緊急対応体制の整備	7-1.司令塔としてのCSIRTの設置 7-2.従業員の初動対応の規定 7-3.インシデント発生時の優先度に応じた顧客への通知・連絡・公表手順 7-4.想定されるインシデントについてのセキュリティ分析計画の事前策定
8	インシデントによる被害に備えた復旧体制の整備	8-1.インシデント対応時の危機対策本部との連携 8-2.組織内外の連絡先の定期メンテナンス
9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	9-1.サイバーセキュリティリスクのある委託先の特定と対策状況の確認
10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	10-1.情報共有活動への参加による信頼獲得と、収集した知見の社内への還元 10-2.業界団体を活用した情報共有活動

第3章　セキュリティ担当者の悩みと取組みのプラクティス

	セキュリティ担当者の悩み	取組のプラクティス
セキュリティ意識の向上	(1)IT部門のみで経営層のセキュリティ意識を向上させることに限界を感じている	外部講師による経営層向けの研修会を実施する
	(2)インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある	社外専門家を活用しながら自社でサイバーセキュリティ人材を育成する
	(3)海外拠点のセキュリティ意識が低い	対面のコミュニケーションを通じ、セキュリティ意識を向上させる
	(4)従業員に対してセキュリティ教育を実施しているが効果が感じられない	特定の部署・役職等に向けたフォローアップの仕組みを企画し、試行する
	(5)IoT機器が「シャドーIT」化している	製造部門とIT部門が連携し、不正接続機器や不適切な設定を排除する
	(6)自前でのシステム運用の負担が大きく、セキュリティ対策に不安を感じる	自社のセキュリティルールに整合する、適切なクラウドサービスを利用する
	(7)内部不正で情報漏えいが生じた場合の自社事業への深刻な影響が心配	内部不正を検知するための複数対策を組合せて導入し、周知により発生を抑制
	(8)全国各地の拠点におけるセキュリティ管理状況に不安がある	拠点におけるセキュリティの取組を把握し、対面で対話する
	(9)インシデント対応の初動における情報共有に不安がある	標的型メール訓練で開封したかではなく報告したかを意識させる
	(10)スタートアップ企業のセキュリティ管理体制に不安を感じ、取引先として推奨できない	セキュリティ対策の取組、セキュリティ認証の取得状況を確認する
コミュニケーション	(11)経営層にセキュリティ対策の事業遂行上の重要性を理解してもらえない	事業部門と協同し、事業戦略の一環としてセキュリティ対策の必要性を訴求
	(12)外部サービスの選定でIT部門だけでは対応が困難である	社内の関連部門と連携して外部サービスの選定を行う
	(13)効果的な演習をする方法がわからない	演習実施部門と演習対象部門が協同して、演習内容を企画する
	(14)サプライチェーンの委託先企業がセキュリティ対策に協力的でない	相手先が自分事として対策を進めてもらえるよう、工夫や配慮を実践
リスク対策費用の確保	(15)インシデントが起きた際の財務面でのリスクヘッジが十分ではない	初動対応のリスクを減らすサイバー保険の活用を検討する
マルウェア対策	(16)ランサムウェア感染による事業停止を回避したい	ランサムウェア感染の可能性をゼロにできないことを社内で共有し、被害軽減策を準備
制御システムの対策	(17)工場のサイバーセキュリティ対策が急務となっている	工場システムのネットワークにおける役割分担を明確にする
新しい働き方の対策	(18)テレワーク導入等の急激な環境変化に対応したセキュリティ管理規程に見直したい	新しい働き方に相応しい情報管理ルールを整備し、安全性と利便性を両立させる

サイバーセキュリティ経営可視化ツール

- 「サイバーセキュリティ経営ガイドライン」で定める重要10項目の実施状況を5段階の成熟モデルで可視化（レーダーチャート表示）するツール（2023年7月Excel版、Ver2.1公開）。
- **自社のサイバーセキュリティ対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定、適切なセキュリティ投資の実行等が可能。**



特徴

- 40の設問に回答⇒実践状況をレーダーチャート表示
- 業界ごとの平均値を参考値として表示することも可能。

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

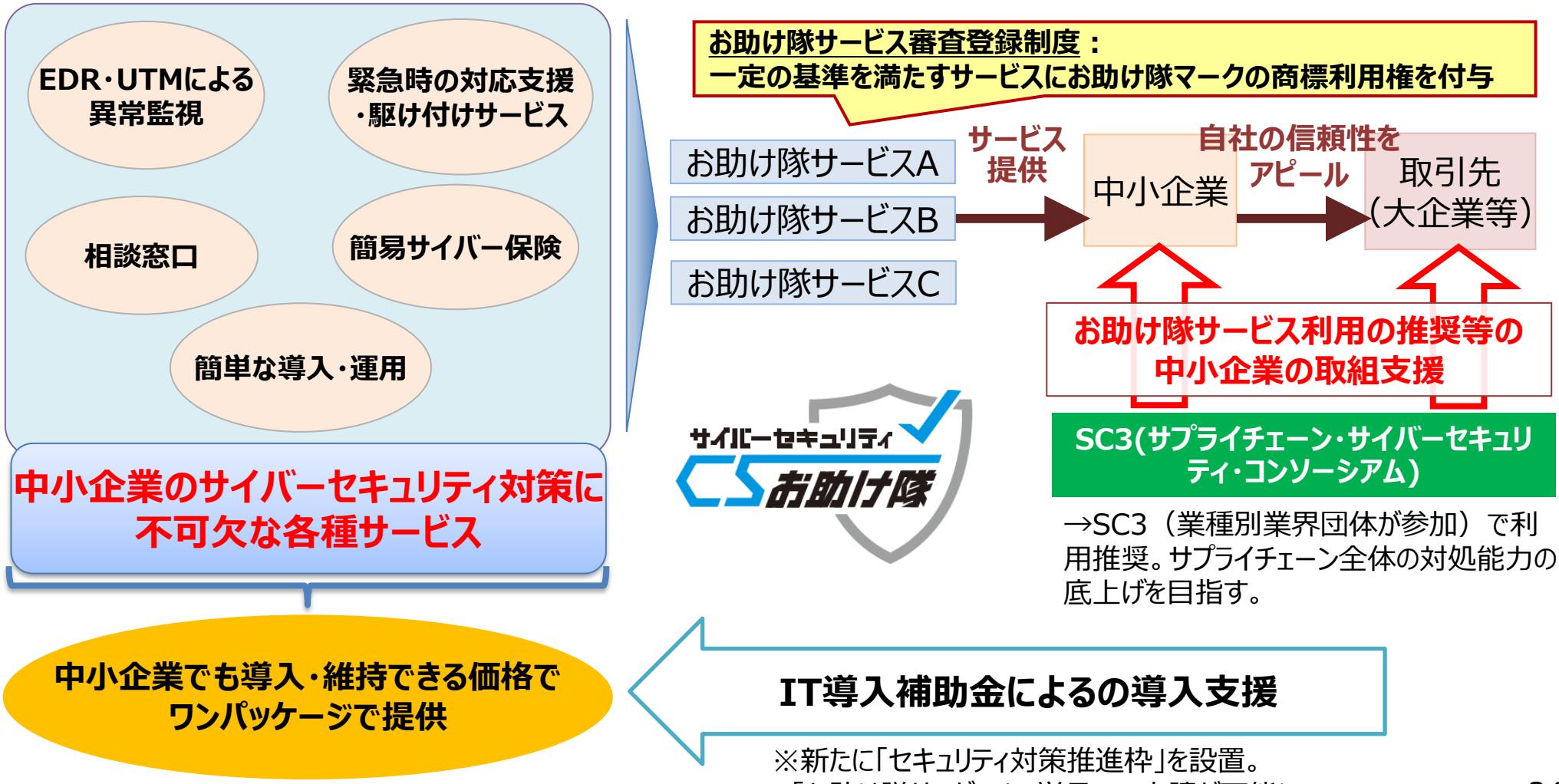
１．最近のサイバー攻撃の現状と課題

２．サイバーセキュリティ経営ガイドライン

３．具体的な取組のご紹介

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。現時点で35事業者がサービスを提供。
- 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。IT導入補助金による支援を拡充。



サイバーセキュリティお助け隊サービス　登録サービスリスト

- 全国各地域の中小企業にとって選択・利用可能な「サイバーセキュリティお助け隊サービス」のリスト。現時点で35事業者がサービスを登録・提供中。

【サイバーセキュリティお助け隊サービス　事業者・登録サービスリスト】

	事業者名 (サービス名称)
1	**大阪商工会議所** （商工会議所サイバーセキュリティお助け隊サービス）
2	**ＭＳ＆ＡＤインターリスク総研株式会社** （防検サイバー）
3	**株式会社ＰＦＵ** （PCセキュリティみまもりパック）
4	**株式会社AGEST** （EDR運用監視サービス「ミハルとマモル」）
5	**ＳＯＭＰＯリスクマネジメント株式会社** （SOMPO SHERIFF）
6	**株式会社アイティフォー** （ランサムガード）
7	**富士ソフト株式会社** （オフィスSOCおうちSOC）
8	**株式会社BCC** （セキュリティ見守りサービス「＆セキュリティ＋」）
9	**中部事務機株式会社** （CBM ネットワーク監視サービス）
10	**中部電力ミライズ株式会社** （中部電力ミライズ　サイバー対策支援サービス）
11	**セントラル警備保障株式会社** （ＣＳＰサイバーガード）
12	**沖電グローバルシステムズ株式会社** （PCお助けパック　PC定期侵害調査プラン）
13	**株式会社コハマ** （ネットワークセキュリティ見守り隊＆PCセキュリティ見守り隊サービス） （ネットワークセキュリティ見守り隊）
14	**NTTコミュニケーションズ株式会社** （マイセキュア　ビジネス）
15	**セキュアエッジ株式会社** （セキュアエッジＭＤＲ９９）
16	**株式会社大塚商会** （Cloud Edge運用支援EasySOC Plus　パック）
17	**株式会社アクロネット** （アクロネットサイバーセキュリティサービス）
18	**コスモテレコム株式会社** （ビジネスサポートサービス）
19	**京セラドキュメントソリューションズジャパン株式会社** （TASKGUARD EDR WS セキュリティーサービス） （TASKGUARD UTM CP セキュリティーサービス）
20	**三井物産セキュアディレクション株式会社** （MBSD Global Security Platform （略称：MGSP））
21	**ラディックス株式会社** （ラディックスお助け隊サービス）
22	**株式会社テクノル** （MRⅡ Plus）
23	**株式会社四日市事務機センター** （YONJINサイバーセキュリティ UTM） （YONJINサイバーセキュリティ UTM&EDR）
24	**株式会社ハイテックシステム** （TSOCエンドポイントパッケージ）
25	**株式会社アクシス** （AXIS総合セキュリティパック） －ネットワーク＆端末監視コース －小規模ネットワーク＆端末監視コース －端末監視コース
26	**富士フィルムビジネスイノベーションジャパン株式会社** （beat/solo 見守りサービス）
27	**株式会社アクト** （データお守り隊）
28	**株式会社ケーオウエイ** （サイバーセキュリティお助け隊パック）
29	**株式会社ソフトクリエイト** （SecurityFREEレスキュー隊 for PC監視）
30	**グローバルセキュリティエキスパート株式会社** （サイバードラレコ）
31	**株式会社ブロードバンドセキュリティ** （サイバープロテクション（CP））
32	**ステラグループ株式会社** （ステラお助け隊サービス）
33	**田中工業株式会社** （ネットワークセキュリティパッケージ　パソコンセキュリティパッケージ）
34	**バリオセキュア株式会社** （VCR116wPlus）
35	**タクテックス株式会社** （タクテックスセキュリティサービス）

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。

https://www.it-hojo.jp/

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	
補助額	５万円～150万円未満	150万円～450万円以下	会計・受発注・決済・ECソフト 50万円以下	会計・受発注・決済・ECソフト 50万円超～350万円	PC・タブレット等 ～10万円	レジ・券売機等 ～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。

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＞

地域にセキュリティについて相談できる相手がいない

地域にセキュリティを学ぶ機会が少ない

地域のベンダーを知らない

?

- 地域の関係者間でのセキュリティに関する「共助」の関係を形成
- イベント等の継続開催による地域のセキュリティ意識向上・人材育成
- 国や専門家からの情報提供の場

大学・高専
地元企業
県警
地元ベンダー
地域のセキュリティ関係者のつながり
自治体
民間団体
国

将来目指す姿

- ニーズとシーズのビジネスマッチングや共同研究による地域発のセキュリティソリューションの開発
- 地域一体となった課題解決
- 地域を越えた連携

!!

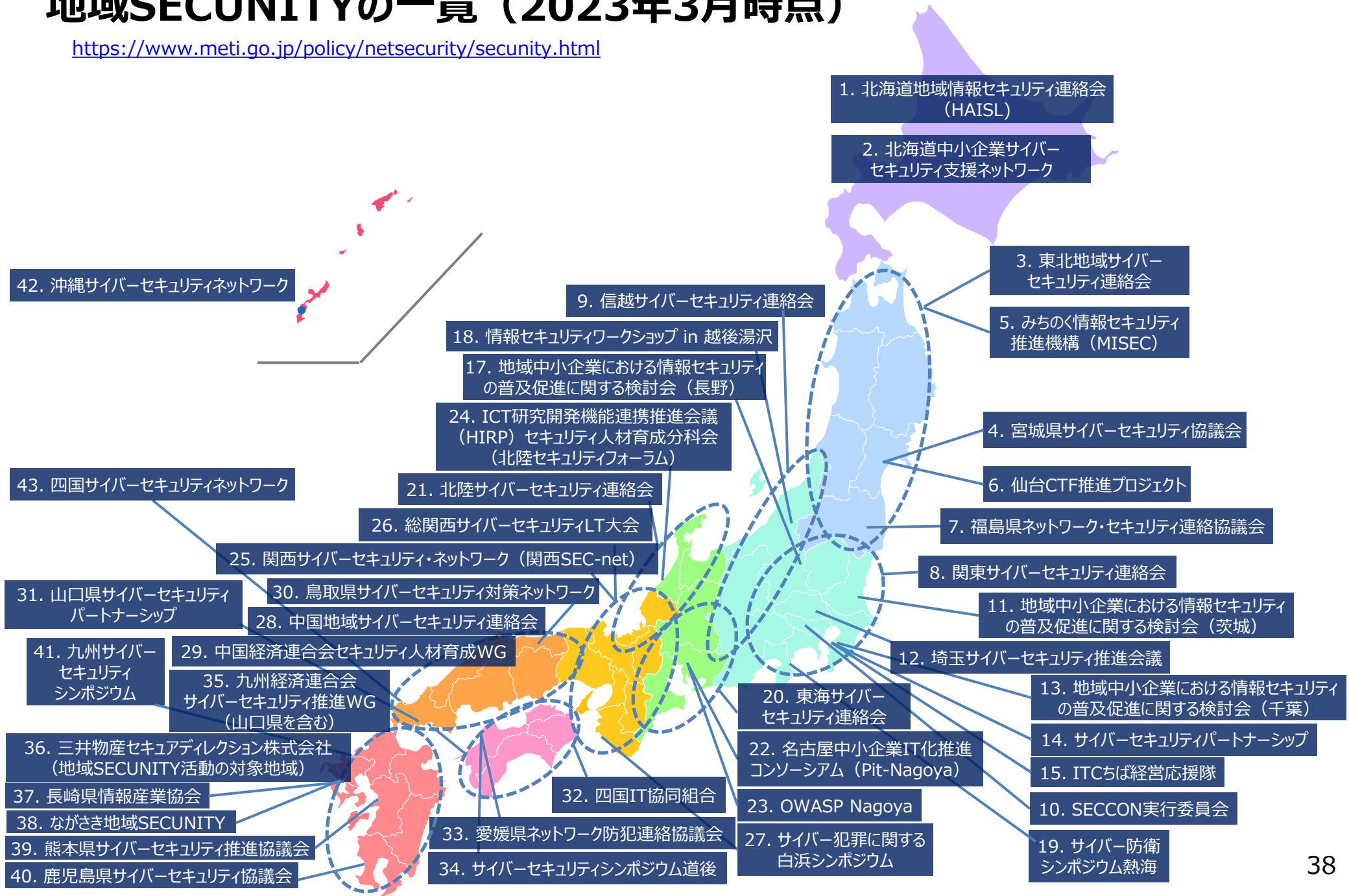
地域のニーズとシーズのマッチング

- **地域の課題解決**
- **価値創出**

地域SECUNITYがない状態 → **地域SECUNITY形成** → **コラボレーション・プラットフォームを全国に展開**

地域SECUNITYの一覧（2023年3月時点）

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



令和４年度　地域SECUNITY形成促進の取組（九州）

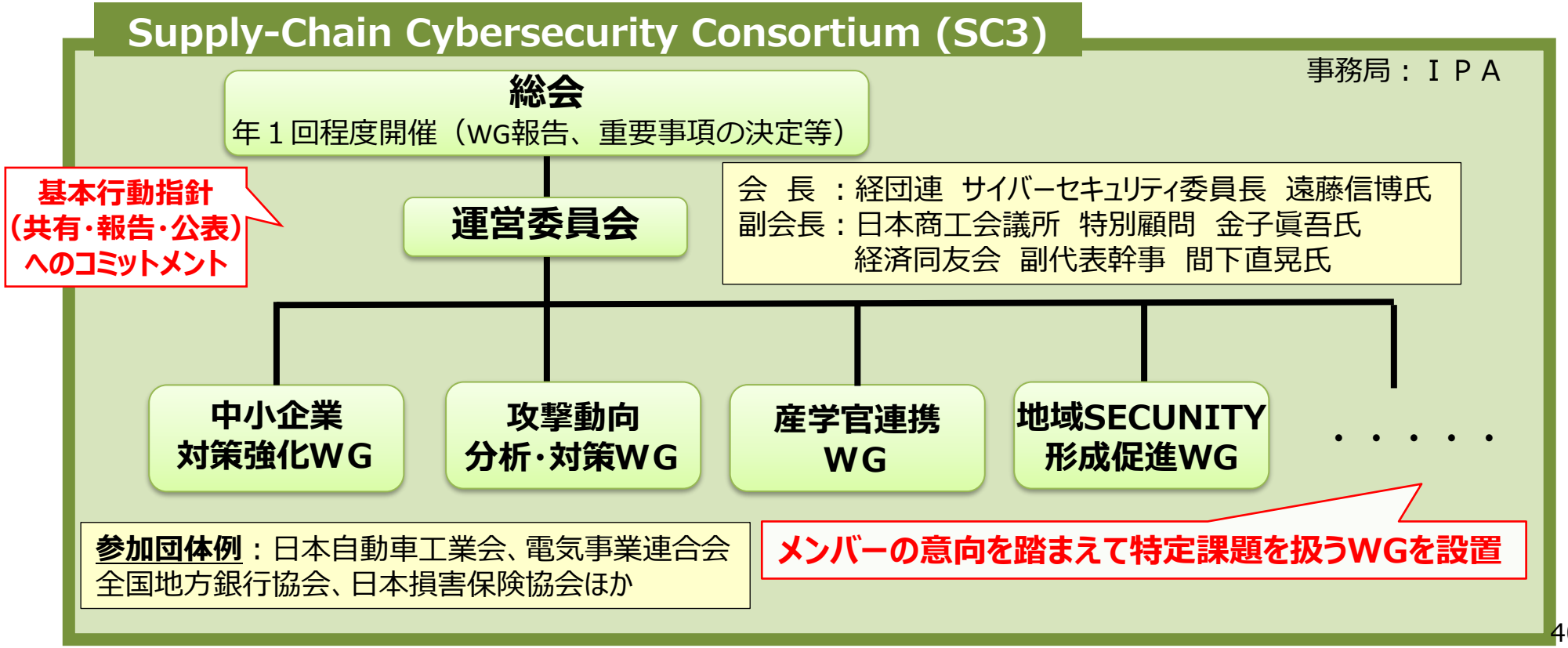
- 中小企業からの要望が多い「具体的な対策」を中心に、業種ごとの特徴を踏まえたテーマを設定し、**計９回**のセミナー・ワークショップを実施。**延べ912名が参加**。
- 企画、運営面においても地域企業や地域団体との連携が進み、地域SECUNITYとしての**主体的かつ自立的な取組が活発化**。

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

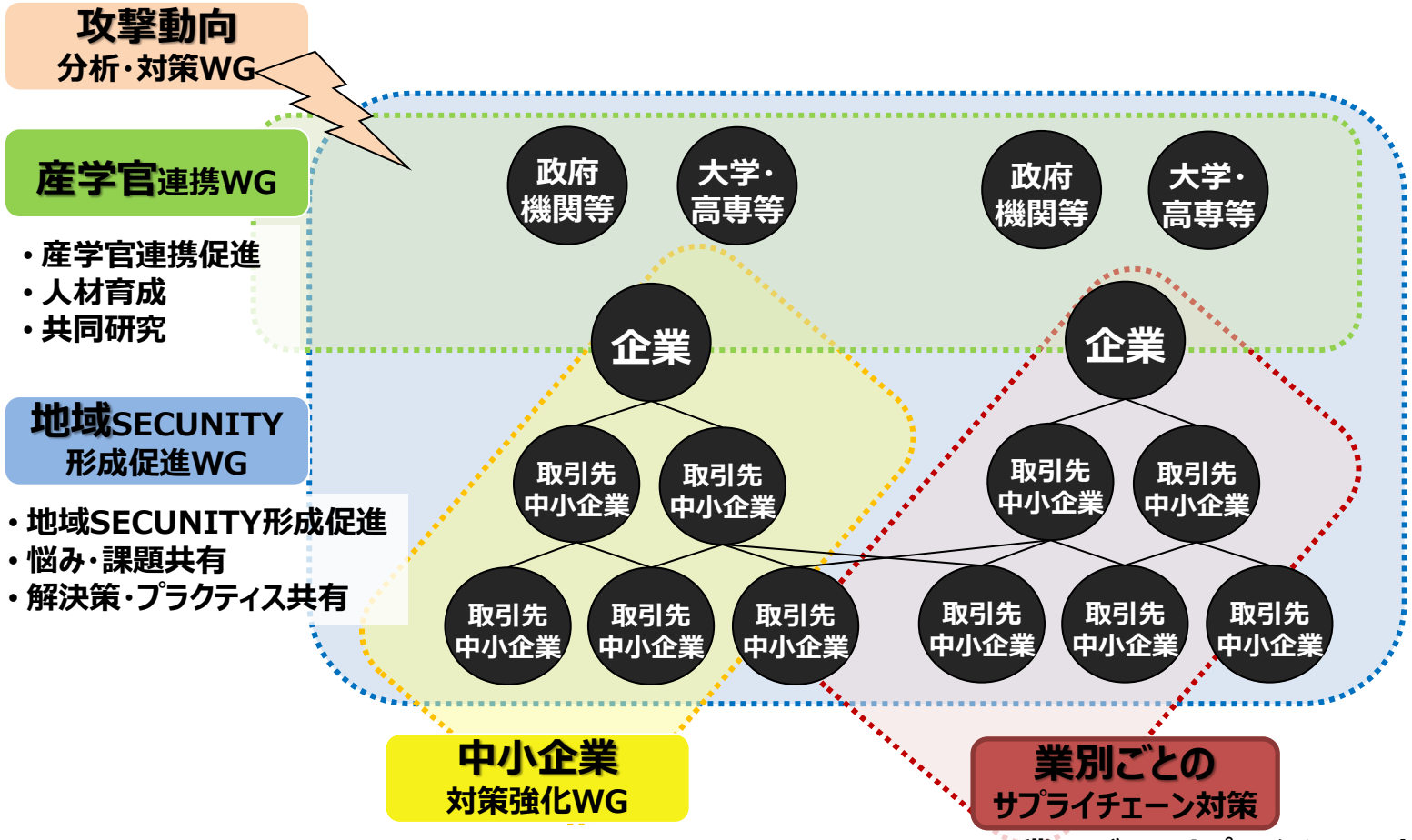
サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

- **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（2023年６月末時点で177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。



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。（2023年６月末日時点、101団体含む177会員）

役員
- 会　長　：一般社団法人 日本経済団体連合会　副会長/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 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 ビジネス機械・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
独立行政法人　国立高等専門学校機構
一般社団法人　日本スマートフォンセキュリティ協会
一般社団法人　日本建設機械工業会
ICSCoE叶会
モバイルコンピューティング推進コンソーシアム
一般財団法人草の根サイバーセキュリティ運動全国連絡会
一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG財団）
一般社団法人日本福祉用具供給協会
一般社団法人サイバーセキュリティ連盟
一般社団法人日本建設業連合会

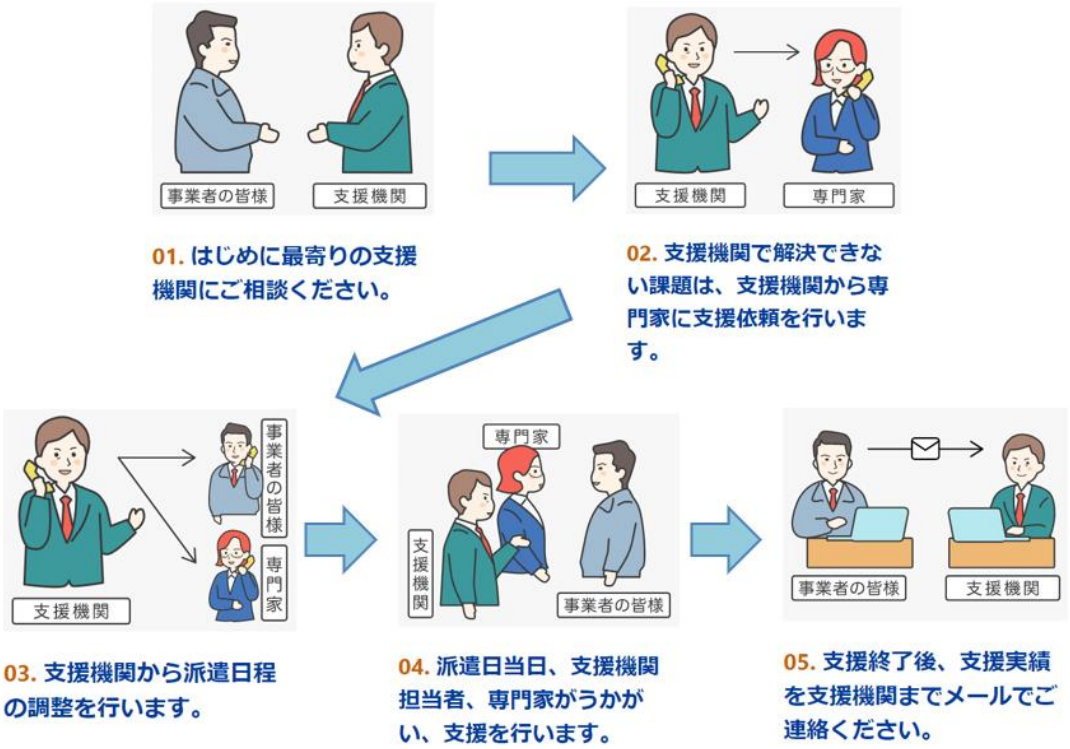
「中小企業119」（専門家派遣事業）について

- **<u>中小企業・小規模事業者等の自助努力だけでは解決困難な経営課題</u>**について、よろず支援拠点又は地域プラットフォーム※の構成機関からの派遣申請に基づき、**<u>専門家派遣を実施中</u>**。

  ※地域プラットフォーム：自主的な取組として地域の支援機関（商工会、商工会議所、都県等中小企業支援センター、金融機関など）による中小企業支援を目的とした連携体。

- 中小企業・小規模事業者等が、**<u>年5回まで専門家派遣に対して補助を受けることが可能</u>**。（**<u>初回無料</u>**、2回目以降は中小企業等が一部費用負担。）

【専門家派遣の流れ】



派遣可能な専門家に、セキュリティ専門家を増強中

例）情報処理安全確保支援士（登録セキスペ）

- サイバーセキュリティの確保を支援する、セキュリティに係る最新の知識・技能を備えた専門人材の国家資格。

支援可能な内容の例

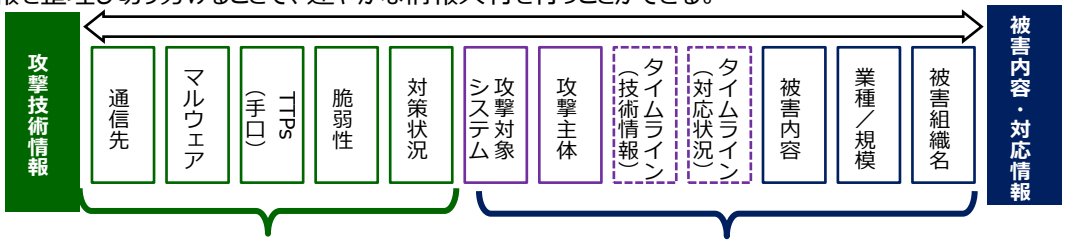
- セキュリティポリシーの策定や、既存のセキュリティポリシーの検証
- 課題に応じたセキュリティ対策ツールのアドバイス
- 情報資産の洗い出しの支援

サイバー被害に係る情報共有ガイダンスの策定

- **攻撃手法が高度化する中で、単独組織による攻撃の全容解明はより困難**に。被害組織はお互いに「他にどのような情報が存在するかを知ることができない」ため、情報共有がなかなか行われにくく、また、共有タイミングも遅いケースが多い。
- サプライチェーンが複雑化する中で、被害組織での対応が適切に行われているか否か外部から確認できず、また、被害組織も被害公表を通じた情報の開示に消極的なため、**被害組織によるインシデント対応（結果）に不安や警戒を募らせるような状況**。
- 本ガイダンスでは、被害組織の担当部門（例：セキュリティ担当部門、法務・リスク管理部門等）を主な想定読者とし、**被害組織を保護しながら、いかに速やかな情報共有や目的に沿ったスムーズな被害公表が行えるか**、実務上の参考となるポイントFAQ形式で整理。

どのような情報を？（様々な種類・性質の情報が存在）

情報を整理し切り分けることで、速やかな情報共有を行うことができる。



基本的に個別の被害組織には紐づかず、対応初期で見つかりやすく、早期に情報共有しなければ効果を得られない情報

ある程度調査期間を経なければ判明しない情報や、ステークホルダー等との調整が必要な機微な情報などが含まれるため、公表までに時間がかかる情報

どのタイミングで？（サイバー攻撃への対処の時系列を意識）

どのような主体と？（様々なサイバーセキュリティ関係組織が存在）

想定読者（被害組織等）

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