経済産業省

サイバーセキュリティ経営ガイドライン Ver3.0のポイント

経済産業省商務情報政策局　サイバーセキュリティ課

課長補佐　三田 真史

１．最近の攻撃動向など

２．サイバーセキュリティ経営ガイドライン

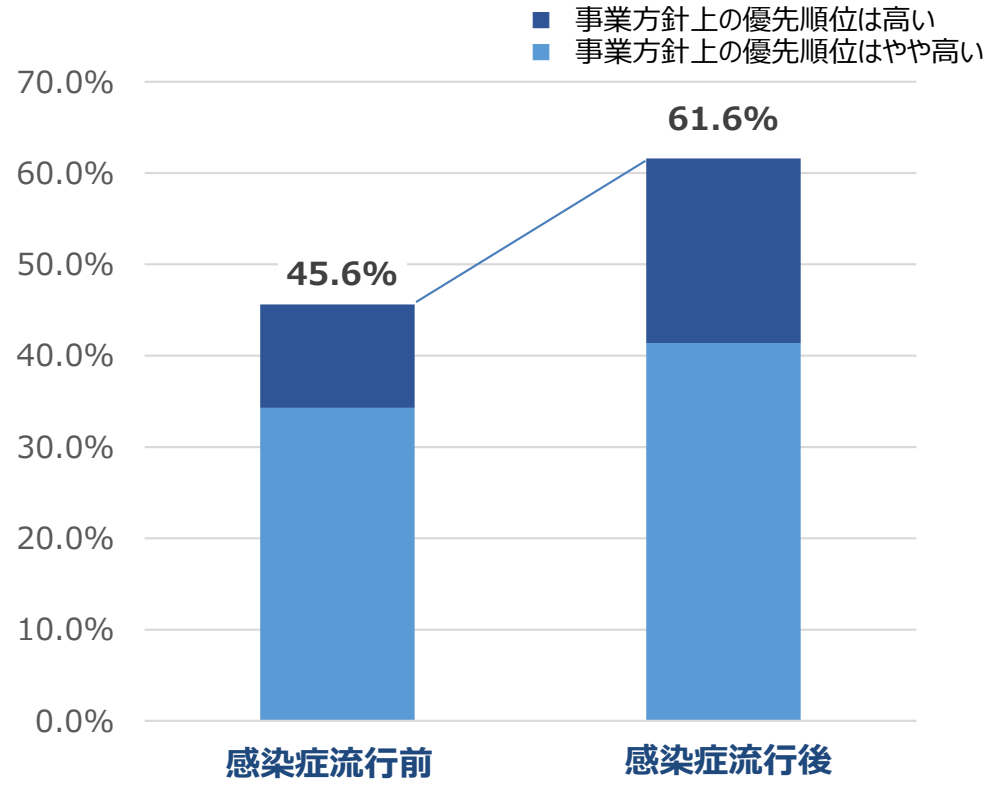
３．ガイドライン改訂のポイント
～経営者の責務
～サプライチェーン全体での対策
～サイバー・フィジカル空間の融合に対応した対策の必要性

４．ガイドラインの活用にむけて

企業におけるデジタル化

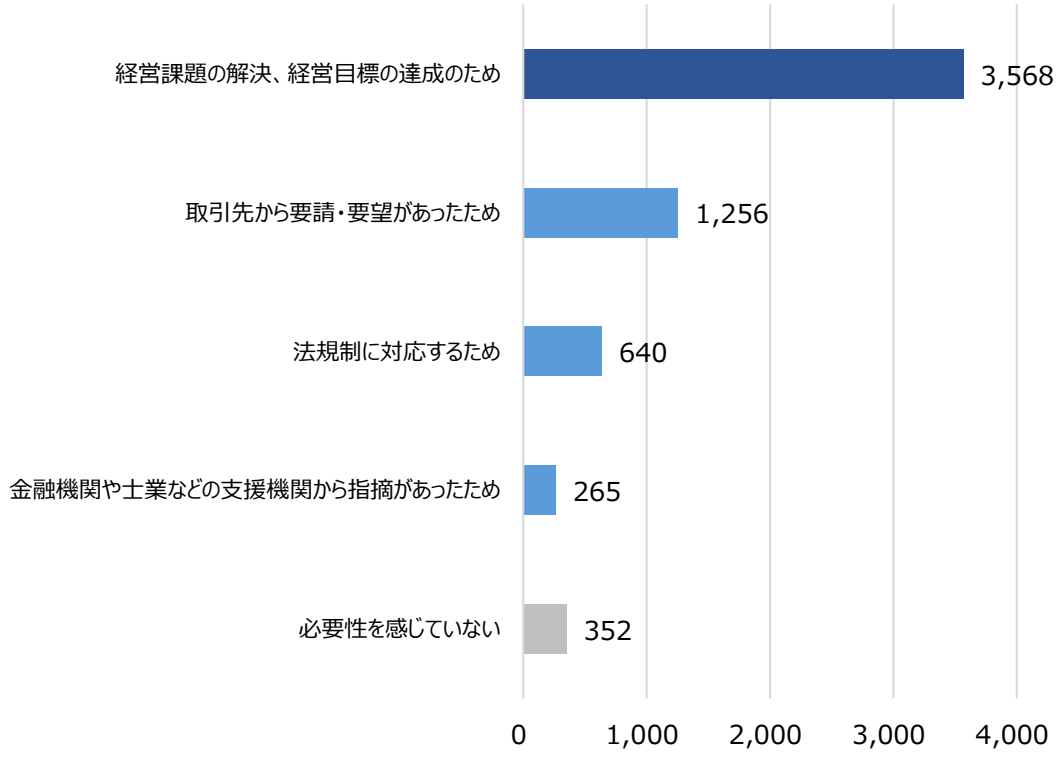
- デジタル化に対する意識は、**コロナ禍の前後で変化**。
- 多くの中小企業が経営課題の解決、経営目標の達成を図るため、デジタル化を推進。

全産業※でデジタル化に対する優先度の変化



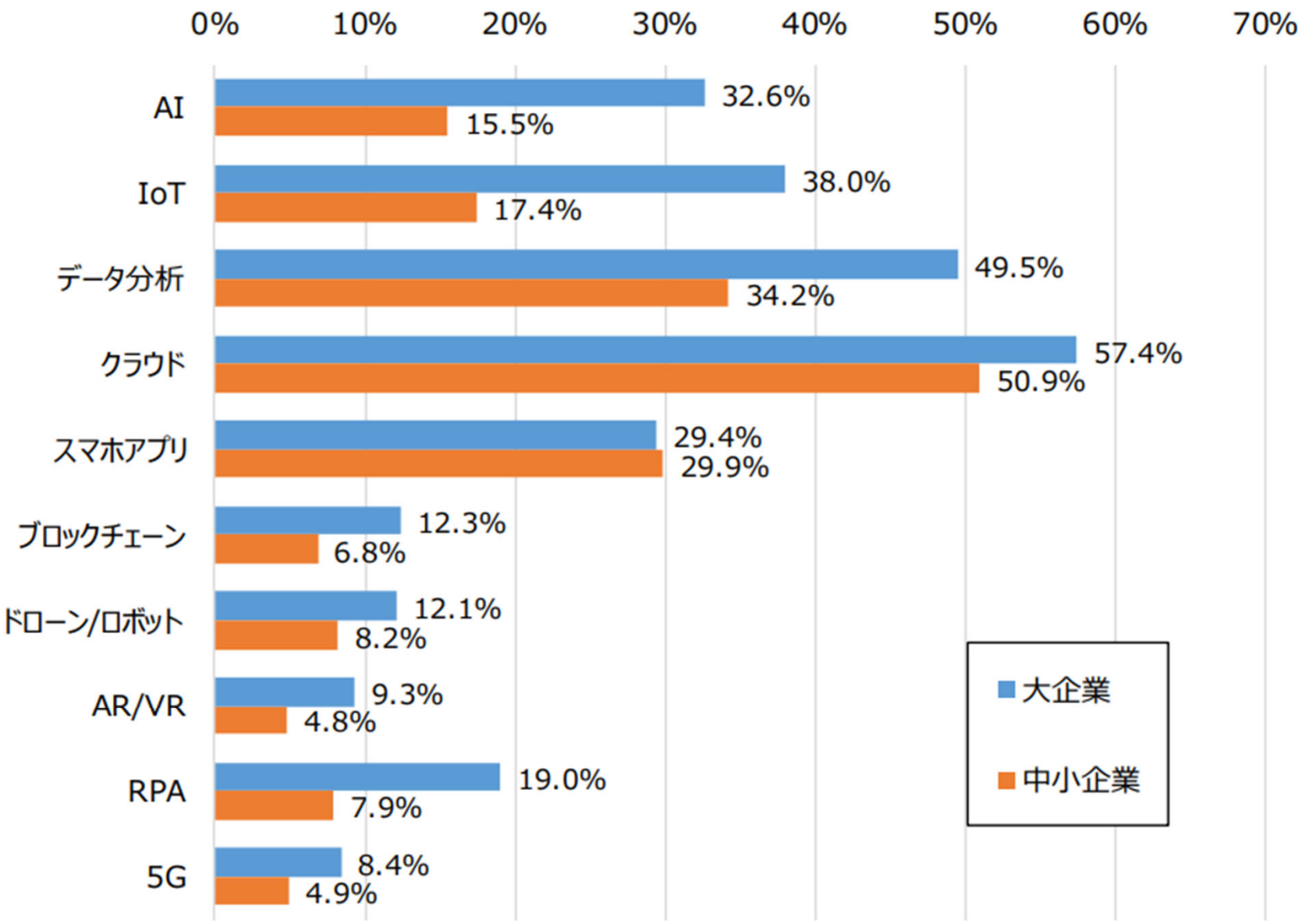
（出典）中小企業庁「中小企業白書2021」
※全産業（製造業、建設業、情報通信業、運輸業、郵便業、卸売業、小売業、学術研究、専門・技術サービス業、宿泊業、飲食サービス業、生活関連サービス業、娯楽業、その他業種）

デジタル化の必要性を感じたきっかけ



（出典）令和２年度中小企業のデジタル化に関する調査に係る委託事業報告書
※中小企業4,827社に対するアンケート調査

（参考）ICT関連技術・サービス等の活用状況

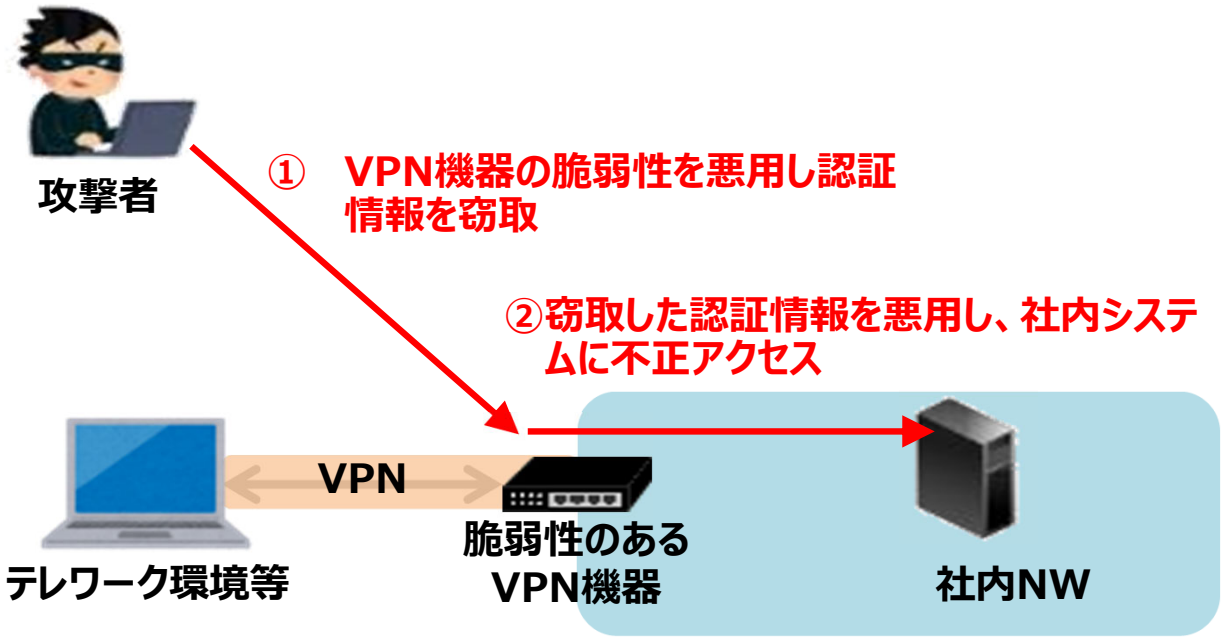


（出典）総務省「デジタル・トランスフォーメーションによる経済へのインパクトに関する調査研究」（2021）　※大企業・中小企業2,093社へのアンケート調査結果

デジタル化の進展に伴うリスク

- 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>**。

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。

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。

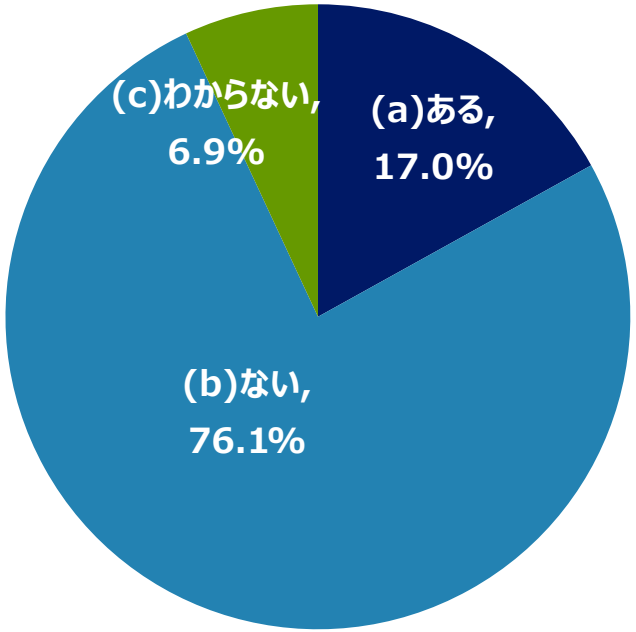
【事例】取引先等を経由した大企業・中堅企業のサイバー攻撃被害

- **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

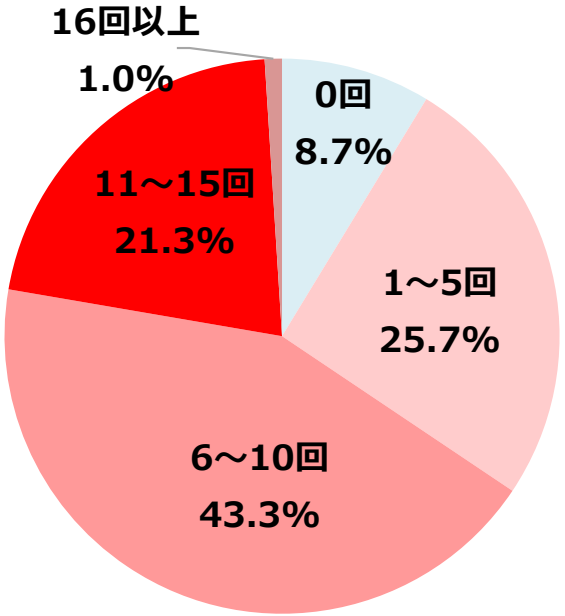
（※）令和３年度サイバー・フィジカル・セキュリティ対策促進事業（企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査）

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

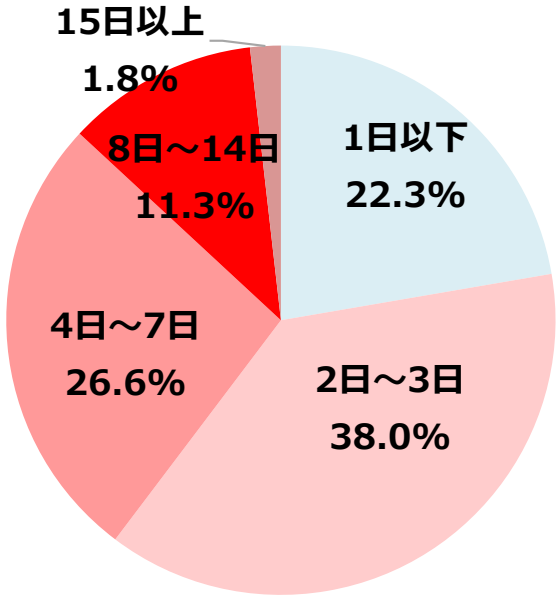
質問：「過去 12 か月間に、サイバー攻撃 （マルウェアの感染、脆弱性を悪用する攻撃、不正アクセスなど）により、あなたの組織の ICS/OT システムの運用は何回中断しましたか」



（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」

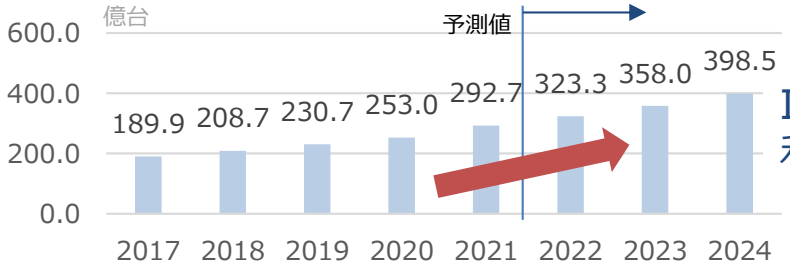


（n=274）

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

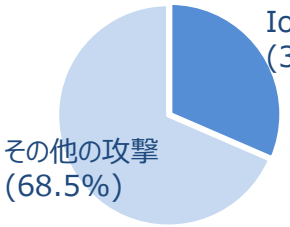
IoT機器の利用拡大に伴い増加するリスクと、その経営への影響

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



世界のIoT機器数の推移及び予測(※1)

IoT機器の
利用数は増加



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

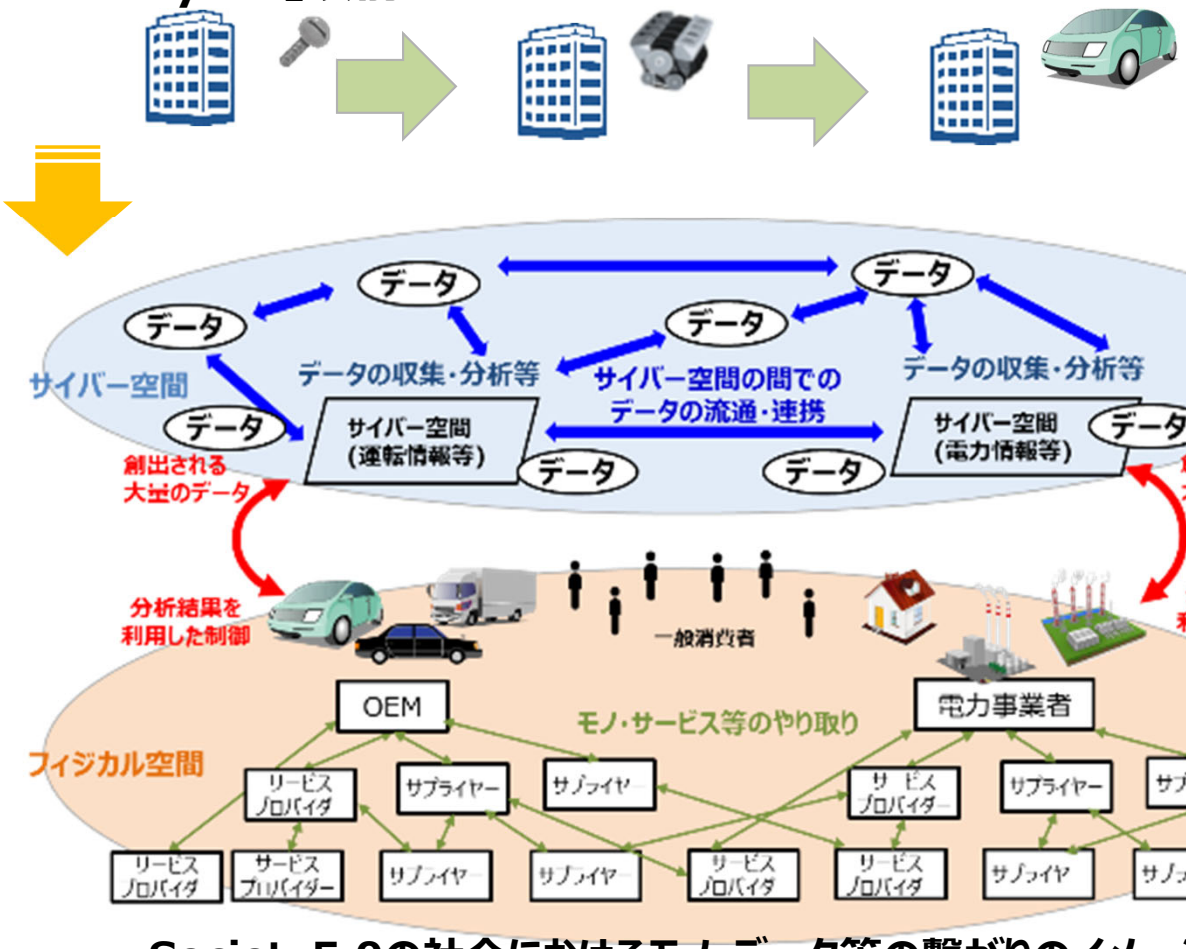
高級ホテルで客室のカードキー発行システムがランサムウェアに感染し、一切のシステム操作が不可能となった。客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生。**サービスの品質が著しく低下** [オーストリア: 2017]

[参考] 各公開情報を基に作成

<サプライチェーン構造の変化>

- 「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。

「Society5.0」以前



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

個々の企業主体の定型的なつながりで価値を生み出す

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

１．最近の攻撃動向など

２．サイバーセキュリティ経営ガイドライン

３．ガイドライン改訂のポイント
～経営者の責務
～サプライチェーン全体での対策
～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

４．ガイドライン活用にむけて

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

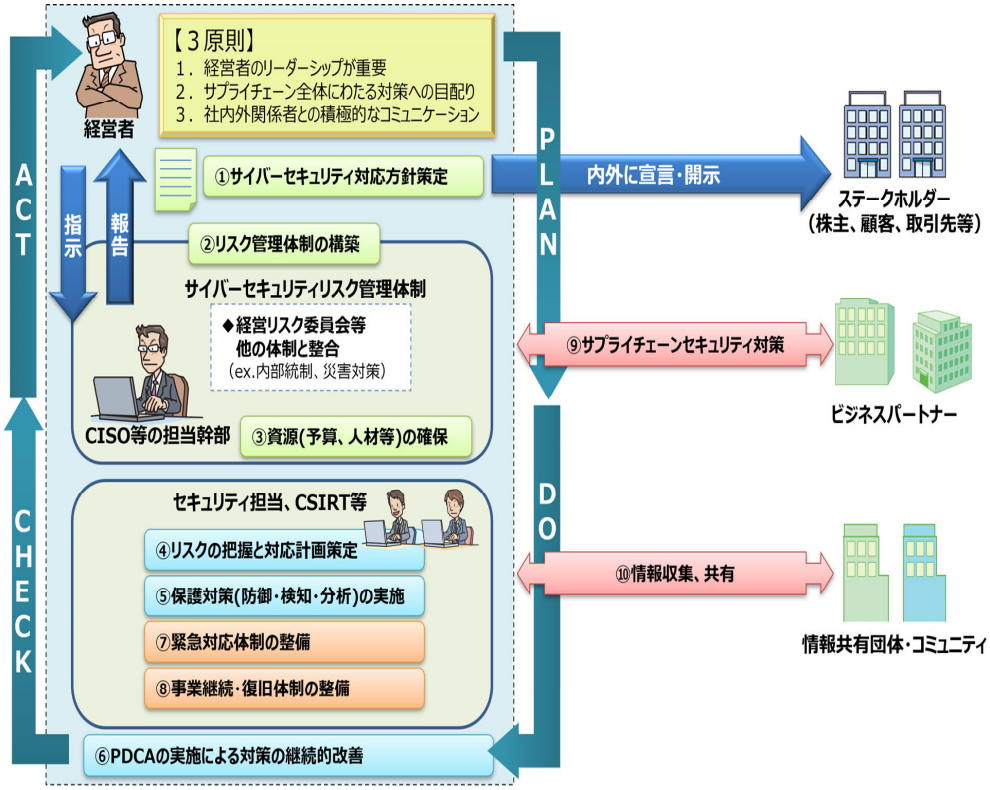
- サイバーセキュリティ対策に当たっては、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要。サイバーセキュリティ対策を推進するため、**経営者を対象としたサイバーセキュリティ経営ガイドラインを策定**。
- ガイドラインにおいては、**経営者が認識すべき３原則**及び**経営者が情報セキュリティ対策を実施する上での責任者（CISO等）に指示すべき１０の重要事項**をまとめている。

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

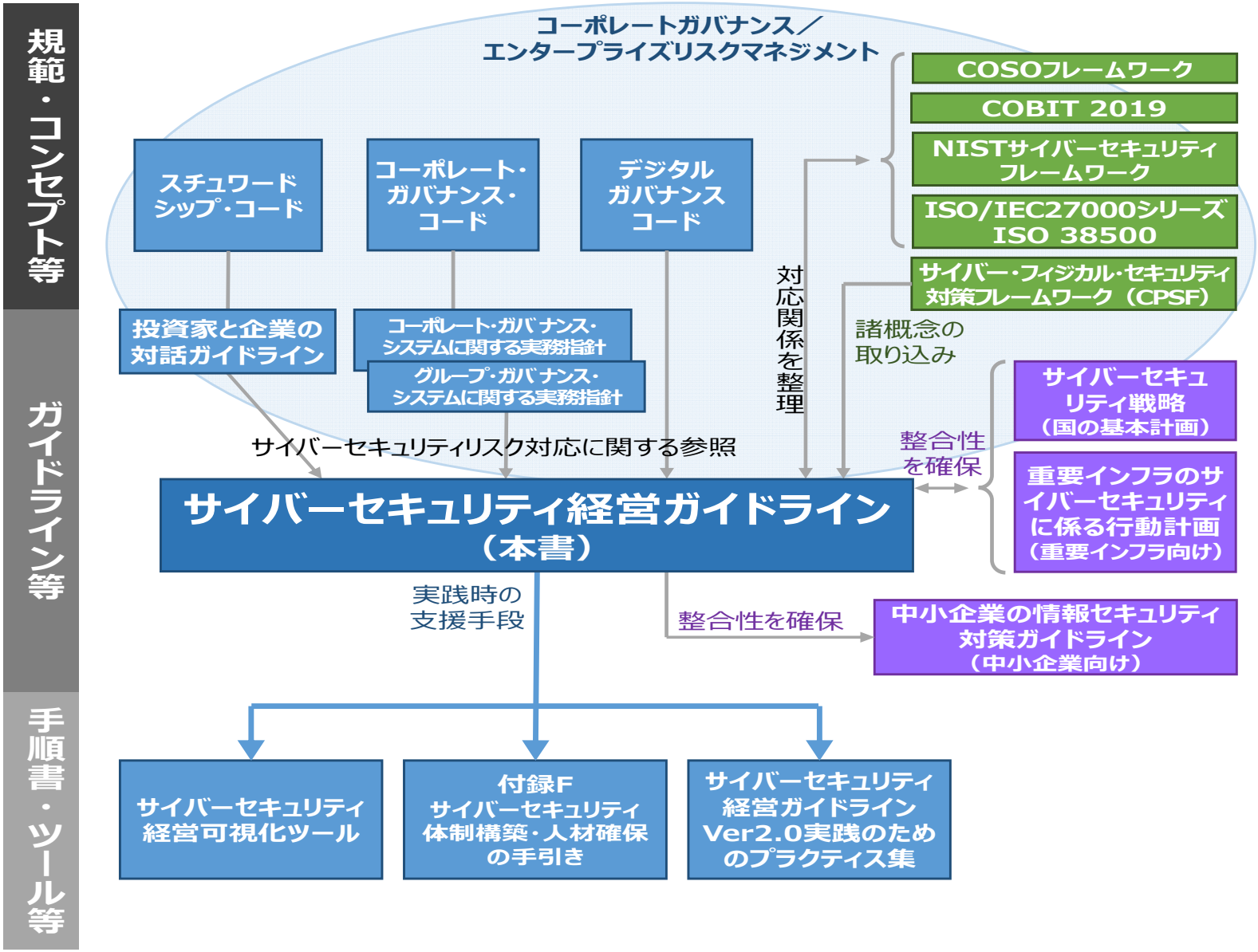
リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAの実施による対策の継続的改善
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 事業継続・復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の状況把握・対策
関係者とのコミュニケーション	**指示10** 情報収集、共有等の促進



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として、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



１．最近の攻撃動向など

２．サイバーセキュリティ経営ガイドライン

３．ガイドライン改訂のポイント
　～経営者の責務
　～サプライチェーン全体での対策
　～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

４．ガイドライン活用にむけて

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**。

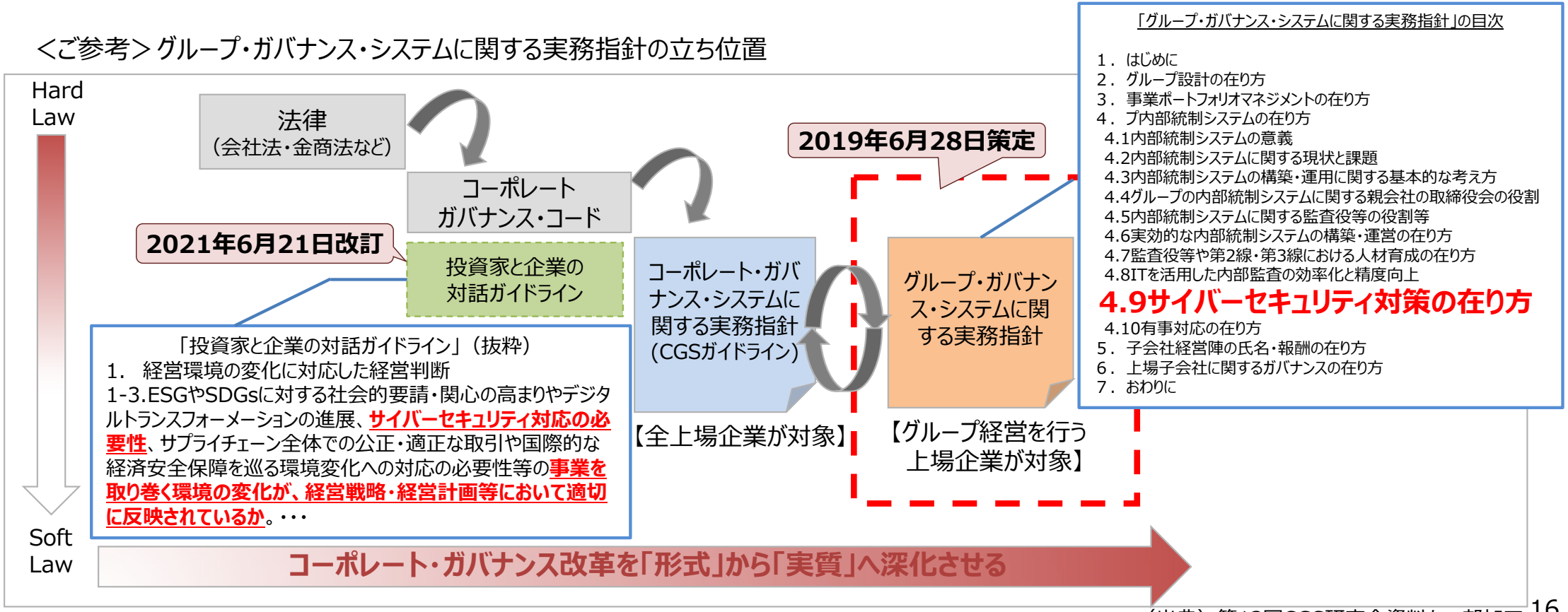
〔Ver.2.0〕
・セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必要なものと位置づけて「投資」と捉えることが重要
・セキュリティ投資は必要不可欠かつ経営者としての責務
・経営責任や法的責任が問われる可能性がある

〔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

（参考）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

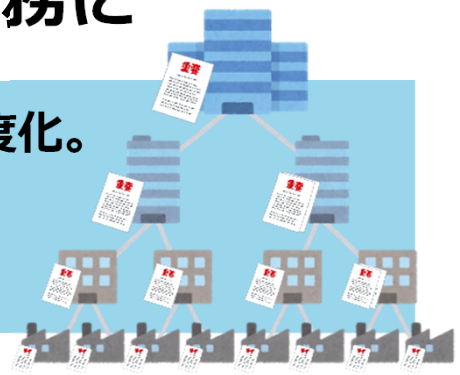
- **「グループ・ガバナンス・システムに関する実務指針(グループガイドライン)」**において、**グループ内部統制システムの一つとして、サイバーセキュリティ対策の在り方を位置づけ**(2019年6月公表)。親会社の**取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れてセキュリティ対策を行うことを検討すべき**ことを明記。
- また、**「スチュワードシップ・コード」及び「コーポレートガバナンス・コード」の付属文書である「投資家と企業の対話ガイドライン」**（金融庁、2021年6月改訂）においても、新たにサイバーセキュリティ対策の必要性等を含む事業環境変化の経営戦略・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）

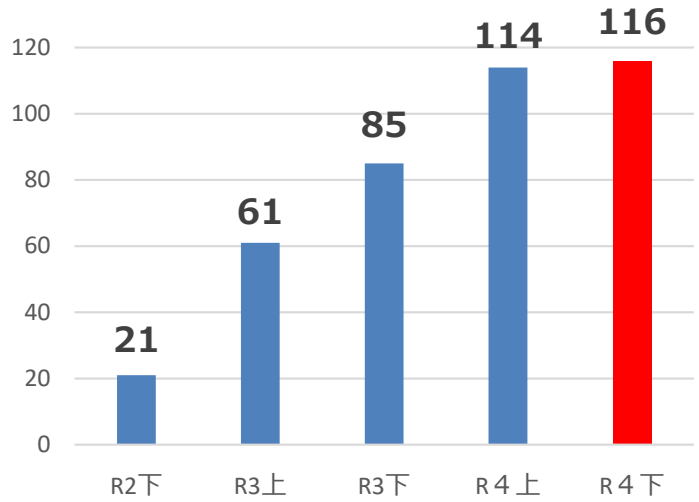
・自社のサイバーセキュリティ確保に関する責務を全うするには、国内外の拠点、ビジネスパートナーや委託先等、**サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要**

・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

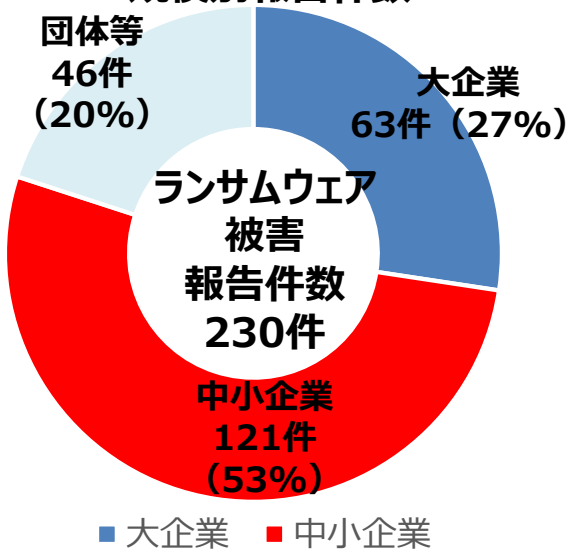
○サイバーセキュリティ経営の重点10項目　指示９

・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企業・団体等の規模別報告件数



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）」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_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。

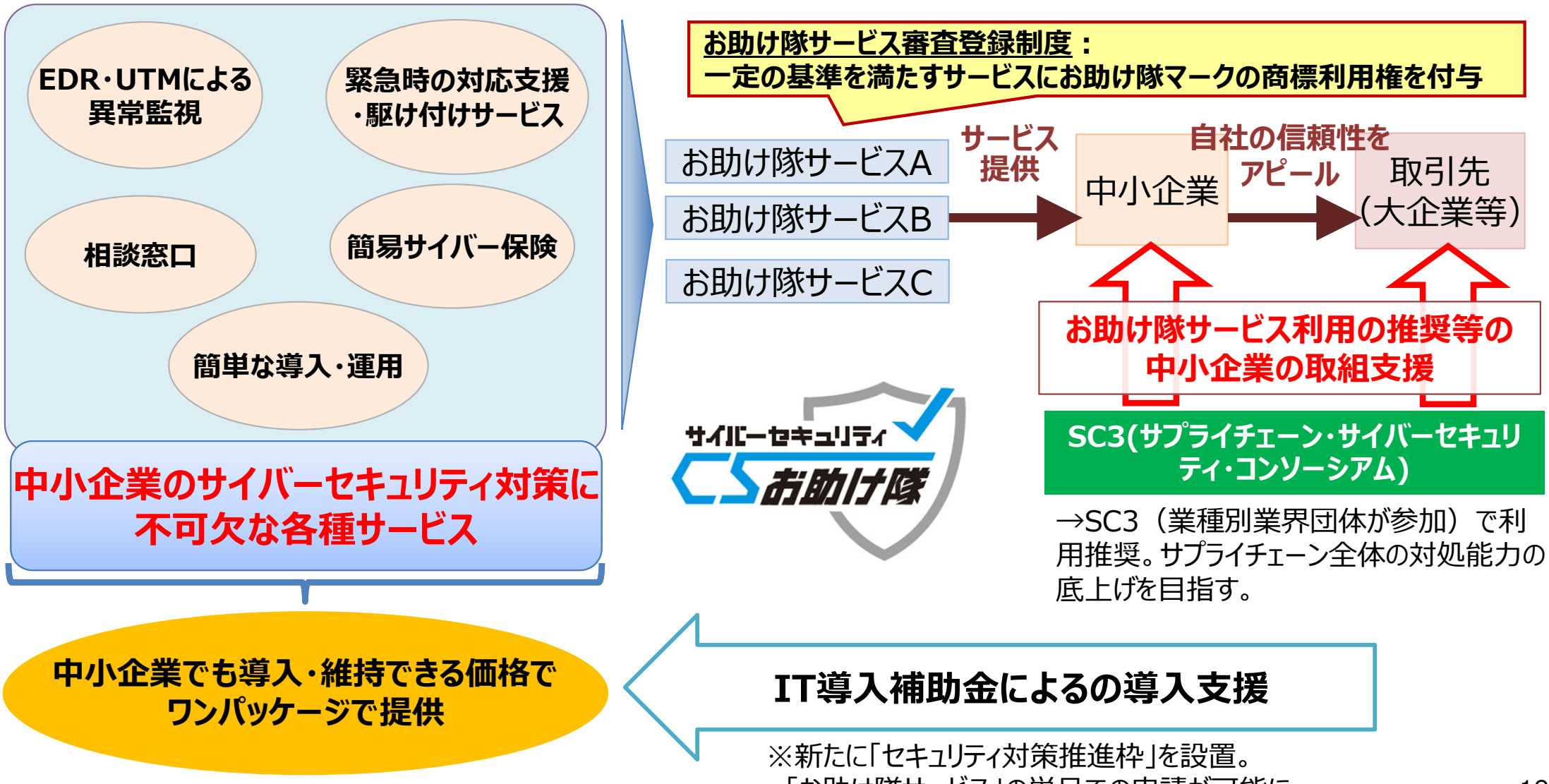
＜問題となるケースの例＞

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

（補足）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40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。



（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）**							

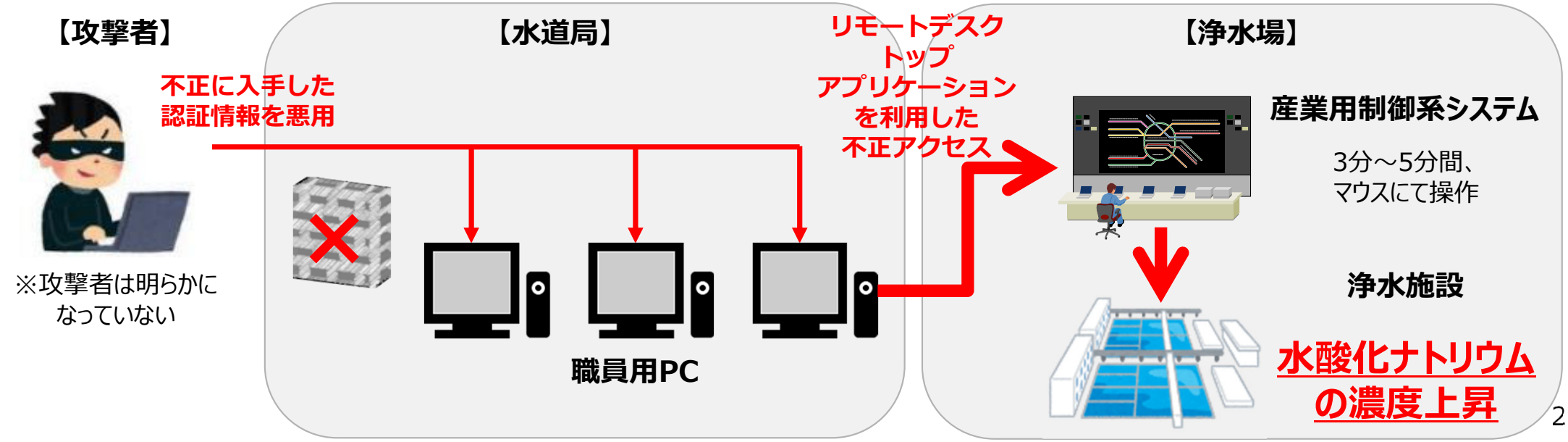
(※1)消費動向等分析経費のクラウド利用料は、１年分が補助対象。
(※2)交付の額が50万円超の場合の補助率は、当該交付の額のうち50万円以下の金額については3/4、50万円超の金額については2/3。

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経営ガイドライン Ver3.0への主な改訂内容

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）**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。

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。

１．最近の攻撃動向など

２．サイバーセキュリティ経営ガイドライン

３．ガイドライン改訂のポイント
～経営者の責務
～サプライチェーン全体での対策
～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

４．ガイドライン活用にむけて

『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。**

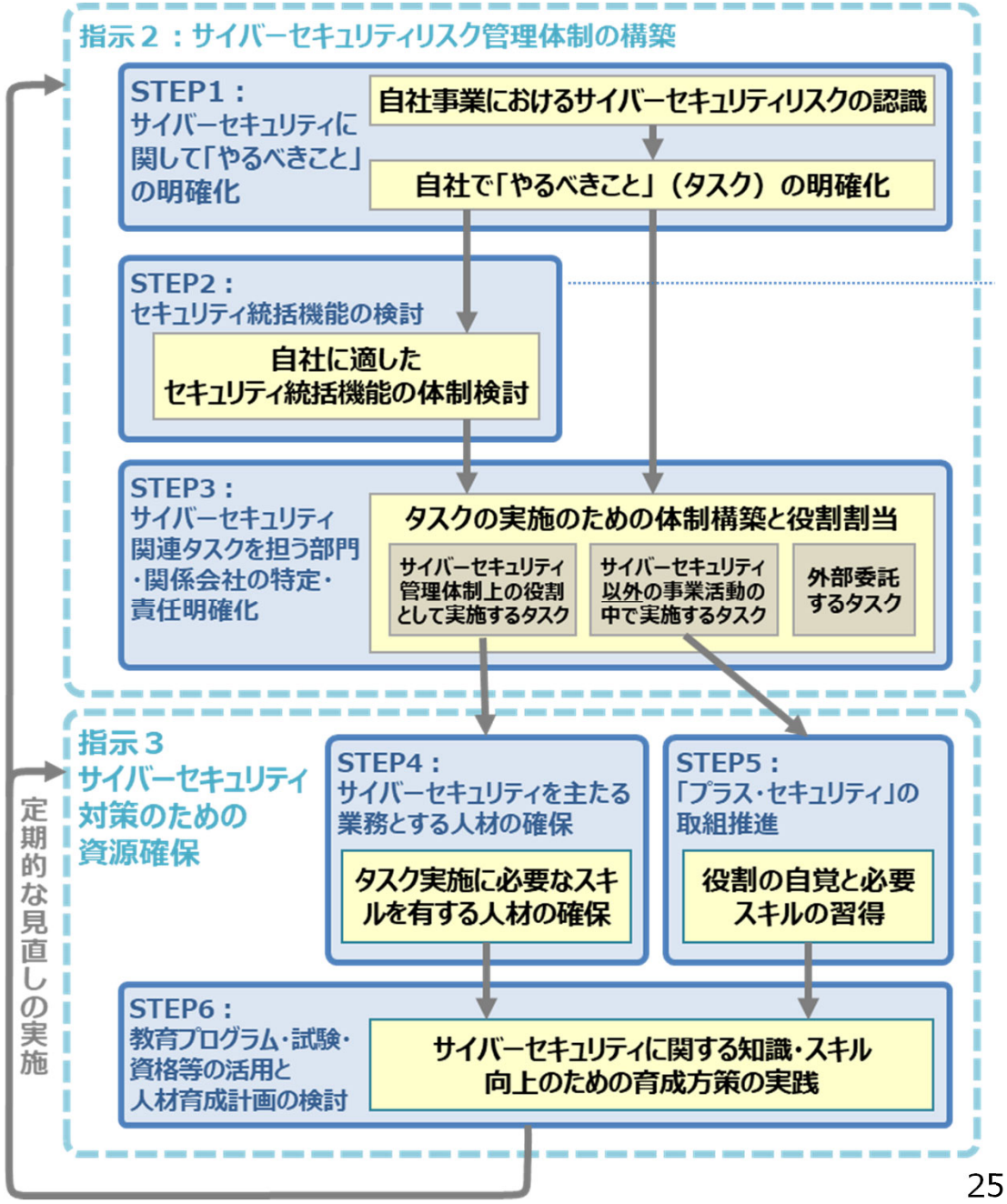
- 2020年9月30日策定、2021年4月15日改訂（Ver.1.1）
- 2022年6月15日改訂（Ver2.0）

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

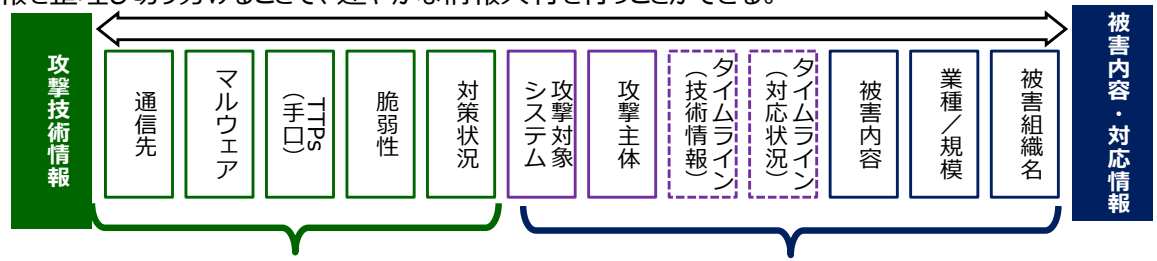
手引き本体では、それぞれの人材確保方法について、メリットや留意点なども解説

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）

- 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。
- **組織幹部のリーダーシップの下**、**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

- 「サイバーセキュリティ経営ガイドライン」を活用して、適切な体制の検討を

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