サイバーセキュリティ経営ガイドラインの改訂と活用のポイント

令和５年３月１７日

経済産業省
サイバーセキュリティ・情報化審議官
上村 昌博

- サイバー攻撃は、**社会や産業に「広く」、「深く」影響**を及ぼし得る。
- サイバー攻撃に際して、**経営者としてどう判断し、対処するか、が重要**になっている。

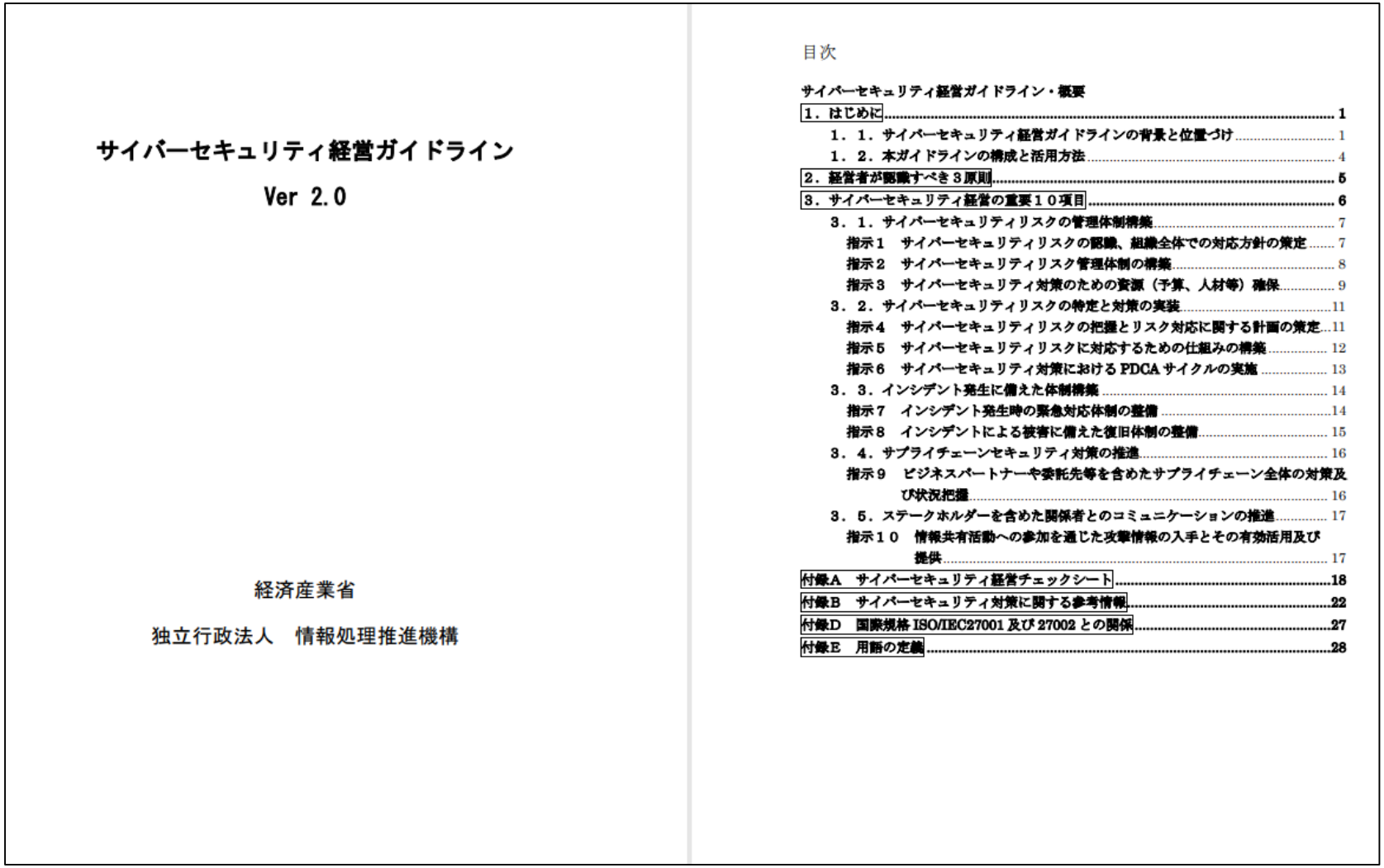
情報セキュリティ10大脅威 2023	
順　位	**組織向け脅威**
1位	**ランサムウェアによる被害**
2位	**サプライチェーンの弱点を悪用した攻撃**
3位	**標的型攻撃による機密情報の窃取**
4位	**内部不正による情報漏えい**
5位	**テレワーク等のニューノーマルな働き方を狙った攻撃**
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策情報の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）

<出典：(独)情報処理推進機構(IPA)、2023.1.25>

サイバーセキュリティ経営ガイドライン

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

- **経営者のリーダーシップが**、サイバーセキュリティ対策推進に**重要**。**経営者を対象**としたガイドラインを策定。
- **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**責任者（CISO等）に指示すべき１０の重要事項**をとりまとめ。



サイバーセキュリティ経営ガイドライン

Ver 2.0

経済産業省

独立行政法人　情報処理推進機構

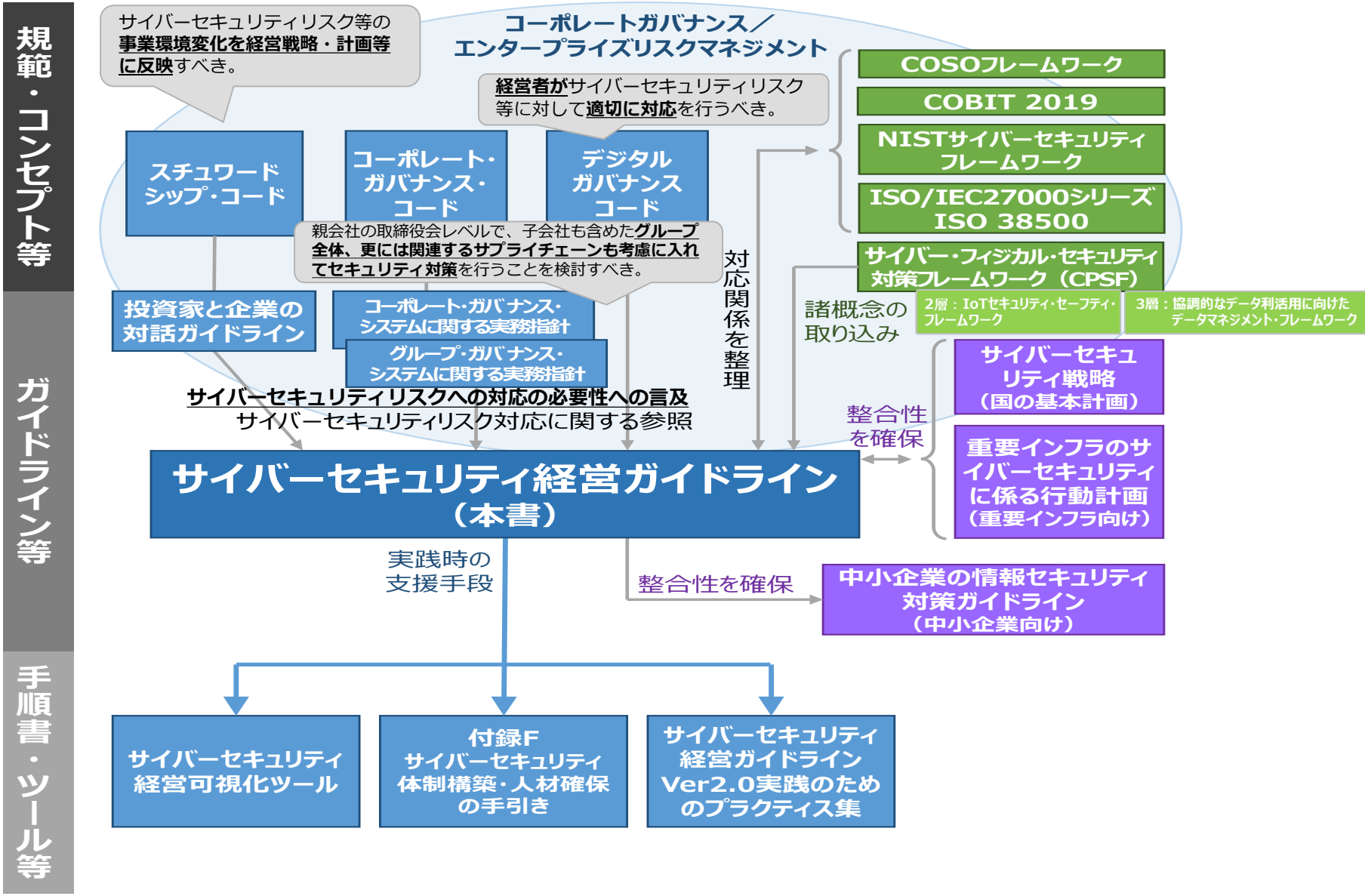
目次

サイバーセキュリティ経営ガイドラインV2.0のダウンロード数推移

サイバー

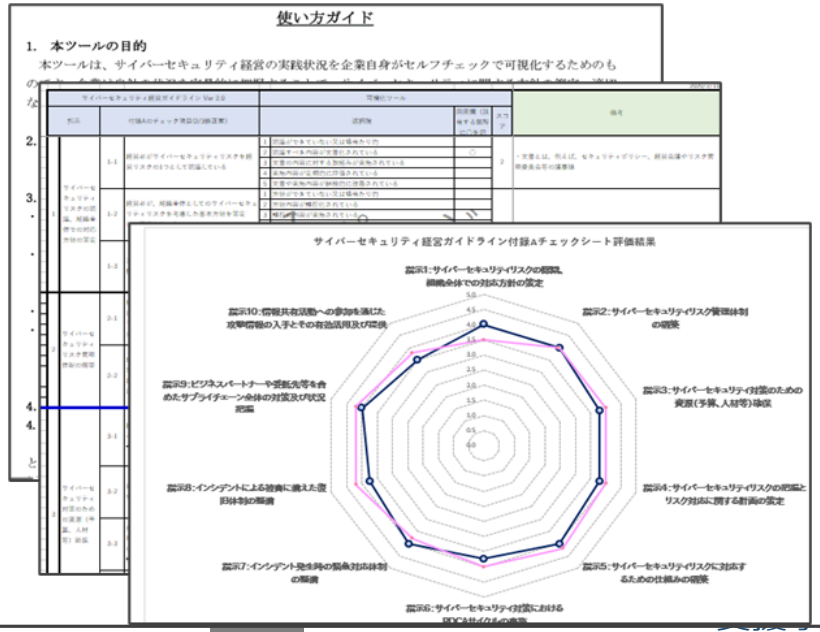
独立

● サイバーセキュリティ経営は、コーポレートガバナンスの一環。



●サイバーセキュリティ経営は、コーポレートガバナンスの一環。

- 39個の質問への回答結果を**<u>レーダーチャート表示で見える化</u>**。社内の経営層や外部ステークホルダーへの説明に利用できる。
- **<u>過去の診断結果との比較</u>**（経年変化）や、**<u>各業種の平均値とも比較できる</u>**。
- 「サイバーセキュリティ経営ガイドラインVer.2.0実践のためのプラクティス集」の**<u>実践事例のケースを表示</u>**できる。



対策ガイドライン
（中小企業向け）

手順書・ツール等

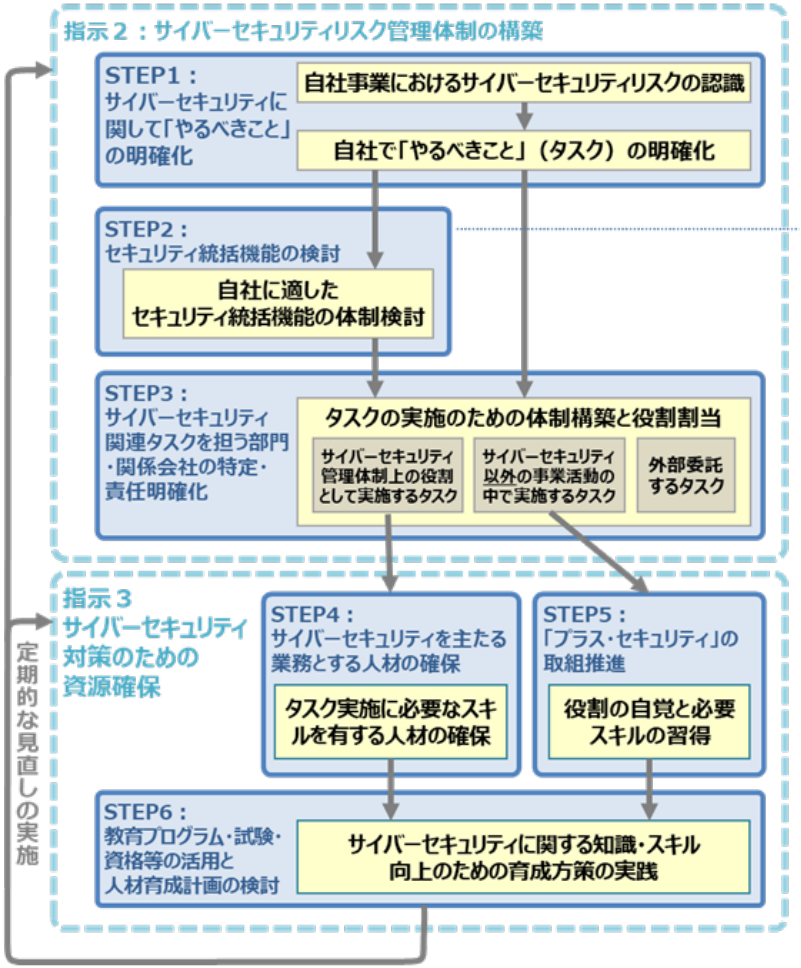
サイバーセキュリティ
経営可視化ツール

付録F
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
Ver2.0実践のため
のプラクティス集

●サイバーセキュリティ経営は、コーポレートガバナンスの一環。

- 経営ガイドラインに基づき、具体的にどのように、**セキュリティ体制づくり**を行うのか、**人材の確保、育成**はどのように行うのか、**非専門家における「プラス・セキュリティ」**といった知見の重要性などを**分かりやすく**提示。



- 経営GLの実践をステップバイステップで効率的に進めるための手順を提示

サイバーセキュリティ経営ガイドラインのVer3.0 への改訂

- サイバーセキュリティリスクも、**組織の経営リスクの一環として認識**していくことが必要。
- サイバーセキュリティ対策を**「投資」（将来の事業活動・成長に必須な費用）**と考えることが重要。**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。
- 組織の規模や業務内容から不適切な対応の場合、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。
- **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ジメントの実践**が求められ、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**残留リスクを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**。
- 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、事業停止等を含む**実施方針の検討**、新たな脅威への対応を含む**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。
- 大企業から中小企業まで**サプライチェーンの弱点や多様化・複雑化等の情勢変化を狙ったサイバー攻撃への対応、サイバー・フィジカル空間の融合に対応した制御系を含めた対策**が必要。

＜改訂の概要＞

＜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

●経営者の責務として、**エンタープライズリスクマネジメントの一環として、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、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、俯瞰的・総合的なセキュリティ対策の重要性**や社外のみならず、**社内関係者とも平時から積極的にコミュニケーションをとり迅速な報告・対応等に繋げる**。

●**プラス・セキュリティ**。セキュリティ以外のデジタル、事業、管理部門等の**あらゆる人材も、セキュリティを意識し、事業遂行に必要な対応が出来る**知識・スキル習得を促す。

●**DX進展、新技術・セキュリティ対策、地政学、心理学等の動向を基に自組織や製品等に係るリスク把握と見直し**を行い、**事業継続等を意識**した対策の実施。

●事業継続の観点から、**制御系も含めた業務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**。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**など。

●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。各種施策も活用しつつ、サプライチェーンリスクへの**対応状況把握・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対策実効性を確保。

●有益な情報を得るには**適切な情報提供も必要**。取組状況や被害の報告・公表への適切な備えや、ステイクホルダーとの**対話・連携**、セキュリティ**関連組織**(IPA、JPCERT、ISACなど）**の情報の活用**。

中小企業の情報セキュリティ対策ガイドライン第3.1版の構成と改訂予定

- **中小企業におけるITの利活用が進む**一方で、**新たな脅威も発現**し、**事業に悪影響を及ぼすリスクも高**まっている。
- DX推進やテレワーク普及といった動向や、情報セキュリティ関連技術の進展状況も踏まえつつ、**関連法令の記載内容の見直しや、中小・小規模事業者においても普及が進むテレワーク時のセキュリティ対策や、インシデント対応を追記**。

	構成	内容	改訂内容
本　編	第１部　**経営者編**	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明	関連法令や被害事例の内容を見直し
	第２部　**実践編**	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明	テレワークの情報セキュリティ、セキュリティインシデント対応に関する解説を追加
付　録	付録１　**情報セキュリティ５か条**	組織の規模を問わず必ず実行していただきたい重要な対策を5か条にまとめ説明	対策例を最新の内容に見直し
	付録２　情報セキュリティ**基本方針**（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプル	
	付録３　**５分でできる！情報セキュリティ自社診断**	あまり費用をかけることなく実行することで効果がある25項目のチェックシート	対策例を最新の内容に見直し
	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形	テレワークの情報セキュリティに関するひな形、サンプルを追加
	付録５　情報セキュリティ**関連規程**（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプル	テレワークの情報セキュリティに関するひな形、サンプルを追加等
	付録６　中小企業のための**クラウドサービス安全利用の手引き**	クラウドサービスを安全に利用するための手引き15項目のチェックシートが付いている	
	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができる	
	付録８　中小企業のためのセキュリティインシデント対応の手引き	情報漏えいやシステム停止などのインシデント対応のための手引き	新規追加

サイバーセキュリティお助け隊サービス

2021年度よりサービスブランドを立上げ。
R5.2時点で30事業者がサービスを提供。

- EDR・UTMによる異常監視
- 緊急時の対応支援・駆け付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

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

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）

お助け隊サービス利用の推奨等の中小企業の取組支援

サイバーセキュリティお助け隊

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。サプライチェーン全体の対処能力の底上げを目指す。

IT導入補助金による支援を拡充。

中小企業の意識啓発・サプライチェーンによる普及等の施策と一体となった展開。

IT導入補助金によるの導入支援

※「セキュリティ対策推進枠」を設置。サイバーセキュリティお助け隊サービス導入費用の１／２を補助。

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。 ※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（2022年10月時点、**９８団体含む175会員**）

設立日: 2020年11月1日（設立総会：2020年11月19日）

Supply-Chain Cybersecurity Consortium (SC3)

事務局：ＩＰＡ

総会
年１回程度開催（WG報告、重要事項の決定等）

会　長　：経団連　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
　　経済同友会　副代表幹事　間下直晃氏

参加団体例：日本自動車工業会、電気事業連合会、全国地方銀行協会、日本損害保険協会ほか

運営委員会

中小企業対策強化WG
サイバーセキュリティ対策強化に向けた課題や取の検討・推進

産学官連携WG
セキュリティ関連の人材育成・活躍推進等について検討・推進

・・・・・

攻撃動向分析・対策WG
経営層が認識すべきサイバー攻撃の動向や対策のポイントを産業横断で発信

地域SECUNITY形成促進WG
地域SECUNITYの取組を推進するための地域間の情報共有や共通課題の解決に向けた取組の検討・推進

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

● **「SECURITY ACTION」**

中小企業自らが、**セキュリティ対策に取り組むことを自己宣言**する制度。
24万社超の中小企業が宣言(令和５年２月)。

★一つ星

情報セキュリティ５か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

【内

■ **発**
し

強化を促
できたい。

■ **サ**
対
ジ

■ **セ**
組

ーン全体
ィ対策を

ため、その

■ **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

ようなケースを例示。

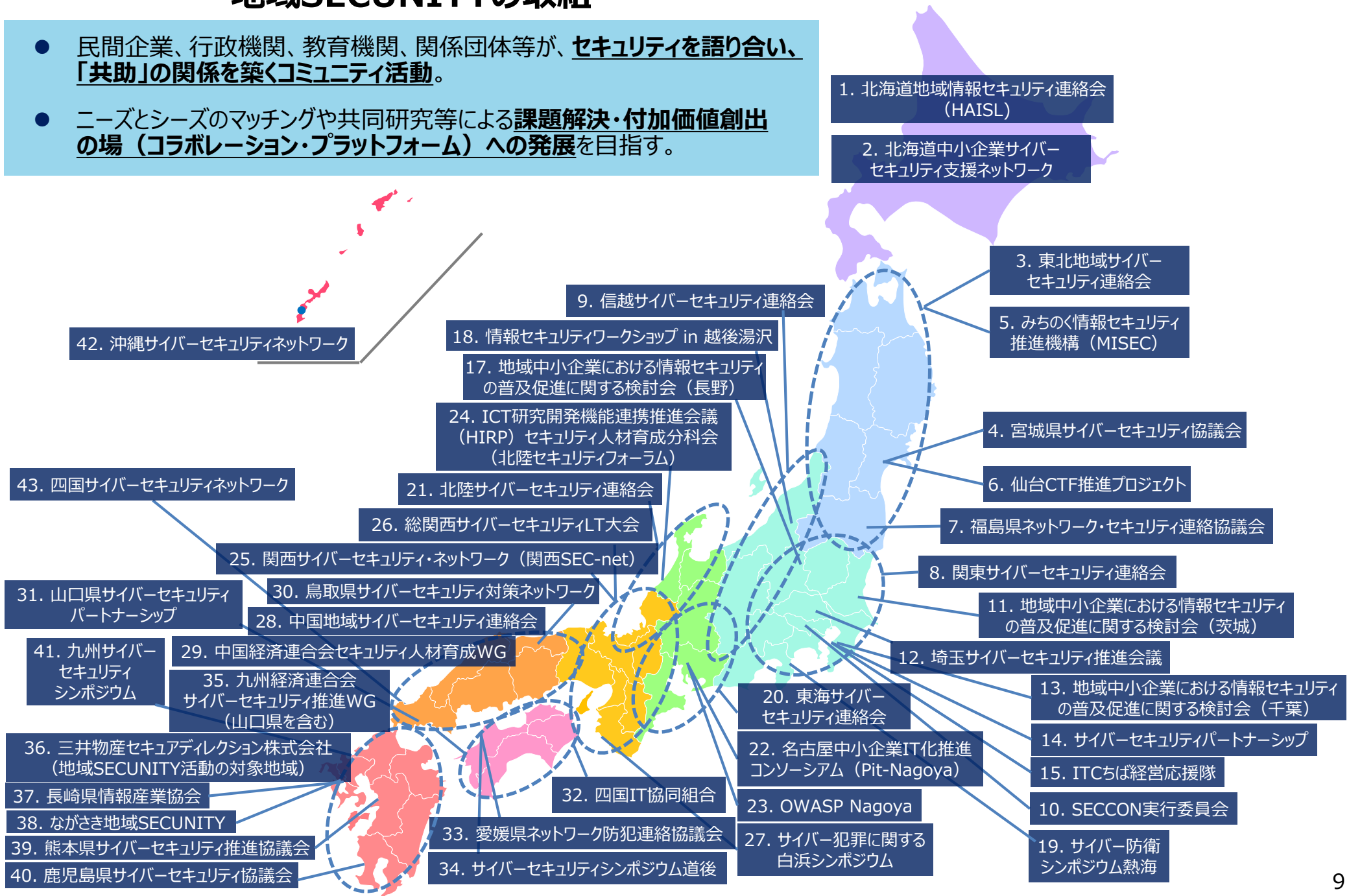
＜問題となるケースの例＞

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

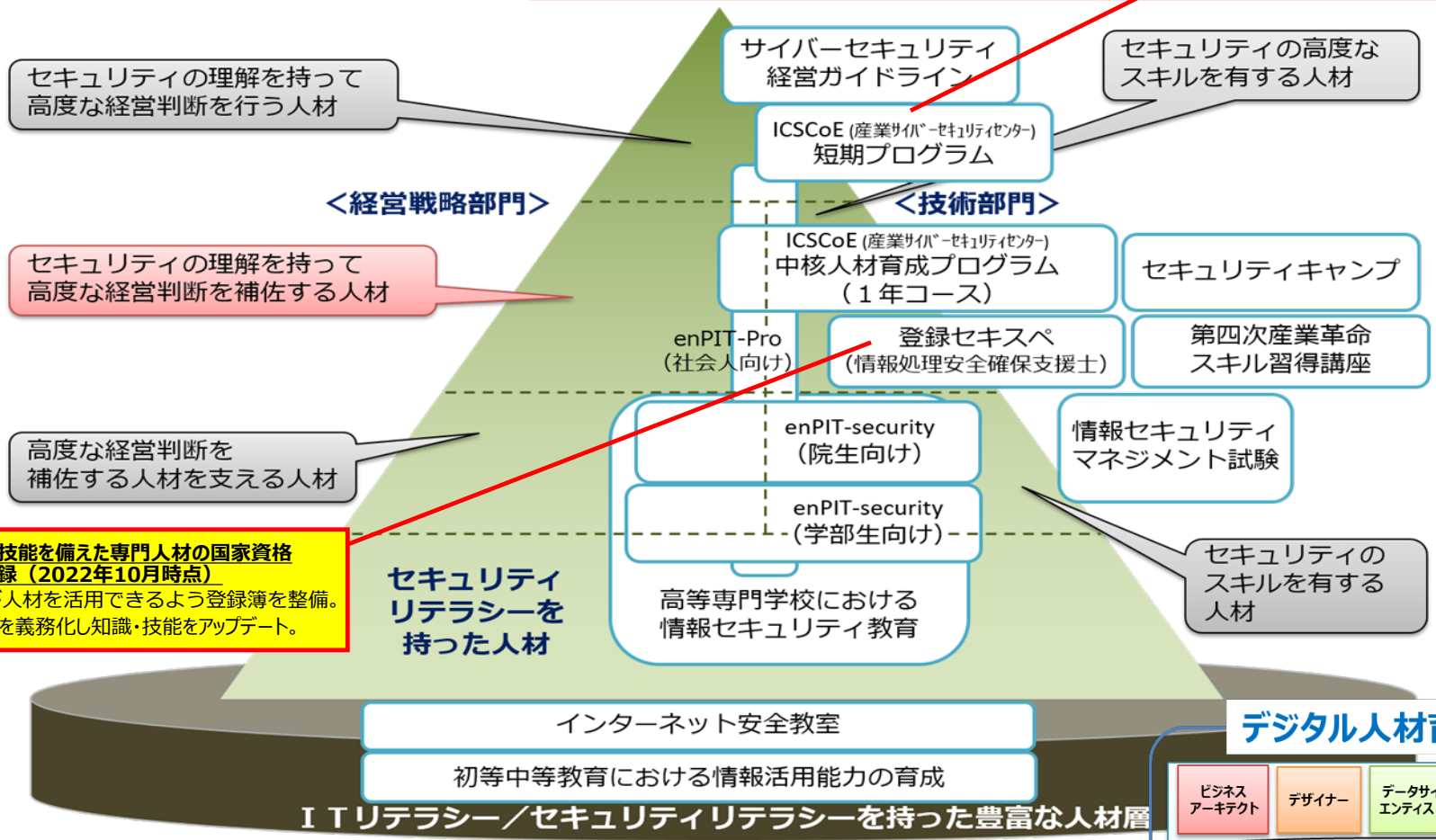
地域SECUNITYの取組

- 民間企業、行政機関、教育機関、関係団体等が、**セキュリティを語り合い、「共助」の関係を築くコミュニティ活動**。
- ニーズとシーズのマッチングや共同研究等による**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）への発展**を目指す。

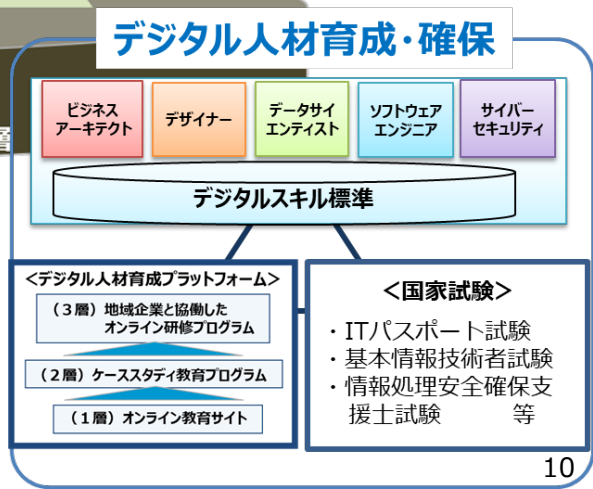


人材育成・活躍促進

- **IT系・制御系に精通**した専門人材の育成、**模擬プラントを用いた**攻撃・対策立案
- 実際の制御システムの脆弱性・信頼性検証等、 攻撃情報の調査・分析
- 1年間のコースで、**重要インフラ事業者等におけるセキュリティ人材を３百名以上育成**（2017年以降の累計）。



セキュリティ知識・技能を備えた専門人材の国家資格
- **20,745人登録（2022年10月時点）**
- 民間企業等が人材を活用できるよう登録簿を整備。
- 定期的な講習を義務化し知識・技能をアップデート。



- 産業全体の競争力強化や社会の課題解決のため、**「DX推進」と「デジタル人材の育成」を両輪で推進**していくことが重要。
- デジタル人材育成の具体的な取り組みとして、以下を実施。
  - **デジタルスキル標準の策定**によるデジタルスキルや能力の見える化
  - **デジタル人材育成プラットフォーム**における実践的な学びの場を提供
  - **国家試験である情報処理技術者試験**による、ITリテラシー・専門IT人材の知識・技能の客観的な評価
  - **DX認定、DX銘柄（上場企業）、DXセレクション（中堅・中小企業等）**等を通じて企業DXを推進

まとめ

- サイバー攻撃は、**社会や産業に「広く」、「深く」影響**を及ぼし得る。実務者による従来の取組継続だけでは対応困難。**経営者が、どう判断し、対処するか、が重要**に。

- サイバーセキュリティにどう取り組むべきか、経営者にとっての指針である**「サイバーセキュリティ経営ガイドライン」の最新版として、Ver3.0を公表**予定。

- **サイバーセキュリティ経営は、コーポレートガバナンスの一環。エンタープライズリスクマネジメントの一つとしてのサイバーセキュリティ。サプライチェーン対策の重要性も増大。**

- 必要となる、**人材の確保・育成**や、**情報共有・連携等**については、**各種施策や団体が存在。ぜひ有効活用を**。

- **社会・経済に提供する価値の継続**の観点から、この**ガイドラインを活用して、必要となる対策・体制の検討と、その実現に**取り組んで頂きたい。