業界セキュリティガイドライン等の共通項抽出業務　最終稿

2023/2/21

三菱UFJリサーチ&コンサルティング

MUFG

目次

1．共通項抽出方針

１．共通項抽出方針

- 情報セキュリティガイドラインが未整備の業界における情報セキュリティガイドライン策定促進や、業界横断的な共通水準の検討に活用いただくことを目的として、業界別のセキュリティガイドラインから、規定されている基準・要求事項等の情報や、複数の業界で共通の基準や要求事項（共通項）を抽出する。
- 共通項抽出の流れは以下のとおり。

【共通項抽出の流れ】

①業界ガイドラインの収集

- 業界団体の皆様から、業界ガイドラインの提供をいただく。

②共通項の抽出方針決定

- 業界団体様から提供いただいた業界別のセキュリティガイドラインの確認を行い、共通項の抽出方針を決定する。
- 抽出にあたっては、業界横断的に比較・検討が行うことができるような抽出軸を設定する。

③共通項抽出の実施

- 抽出軸にそって、業界別のセキュリティガイドライン内の記載の有無（共通項）の抽出を実施する。
- 抽出結果をとりまとめ、共通項の抽出資料初稿として整理する。

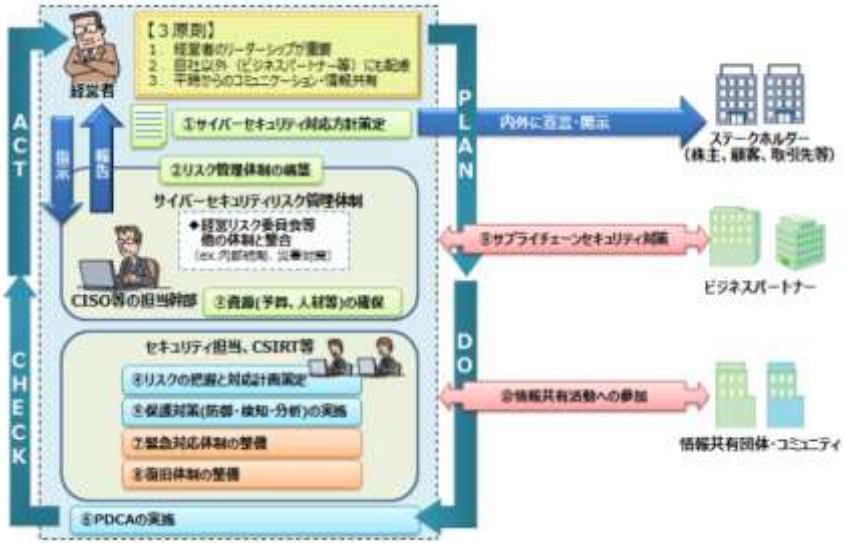
④とりまとめ

- 共通項抽出結果をご確認いただき、追加の調査や修正が必要な点を把握する。
- 修正の反映を行い、共通項の抽出資料最終稿としてとりまとめる。

1．共通項抽出方針

- 抽出にあたっては、業界ガイドラインを横断的に比較できるようにすることを念頭におき、汎用的な軸を設定し、共通項の抽出を行うこととする。
- 具体的には、経済産業省が発行する「サイバーセキュリティ経営ガイドラインVer 2.0」を参考とした軸を設定し、分析対象とするガイドラインを読み込み、軸に該当する記載の有無を確認することにより、共通項の抽出を行うことを基本とする。また、 NISTが発行する「重要インフラのサイバーセキュリティを改善するためのフレームワーク」に記載されているカテゴリを抽出軸とした場合の対応関係についても検討を行う（本調査においては、チェック項目ごとに対応する「NISTフレームワークのサブカテゴリ」を明らかとすることで対応関係を明確にした。詳細は、「ガイドライン共通項抽出結果（別紙） 」参照。）。

【サイバーセキュリティ経営ガイドライン Ver2.0の概要】



（出所）経済産業省『サイバーセキュリティ経営ガイドラインと支援ツール』
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

【NISTフレームワークコアの構造】

図 1:フレームワークコアの構造

（出所）Framework for Improving Critical Infrastructure Cybersecurity
重要インフラのサイバーセキュリティを 改善するためのフレームワーク Version 1.1
https://www.ipa.go.jp/files/000071204.pdf

1．共通項抽出方針

- 抽出する内容は、（サイバーセキュリティ経営ガイドライン Ver 2.0）を参考として事前に設定した項目の記載有無と、具体的な記載内容例とする。
- 取りまとめ時に想定される記載粒度としては、業界ガイドライン内の該当項目の記載有無を整理するとともに、特徴的な記載内容を抽出し、具体的な内容についても参考としていただけるように取りまとめる。

【抽出作業の流れ】

項目	作業内容とねらい
①設定項目の記載有無の確認	• 『サイバーセキュリティ経営ガイドライン Ver 2.0』を参考として設定した項目に沿って、ガイドライン内に記載があるかどうか、記載の有無を確認し、記録する。 • 記載内容の有無を確認することで、2 者以上のガイドラインを比較する際に、記載項目の抜け漏れを比較しやすくするようにする。
②設定項目の記載内容の確認	• 『サイバーセキュリティ経営ガイドライン Ver 2.0』を参考として設定した項目に関する記載の具体性や、記載内容の実現に向けたプロセスに関する記載有無を確認し、記載内容を記録する。 • 記載有無だけでなく、ガイドラインの読み手のセキュリティ対策の強化に資する内容であることが重要との観点から、読み手が実際の行動に移すための気づきや具体的な作業内容の記載があるかどうかを確認する。
③抽出結果のとりまとめ	• 『サイバーセキュリティ経営ガイドライン Ver 2.0』を参考として設定した項目ごとに記録した記載内容を整理し、ガイドライン内で特徴的な記載（ベストプラクティス等）を抽出する。
④特徴的な記載内容の整理	• 網羅性のある比較表として、ガイドラインの共通項を業界関係者間で共有いただけるような形の資料として整理する。 • 多くのガイドラインで記載されているものは重要との考えのもと、ガイドライン未策定の業界や、記載をブラッシュアップする際の参考としていただくことを狙いとする。

1．共通項抽出方針

■ 抽出にあたって用いる判断基準は、「サイバーセキュリティ経営ガイドラインVer 2.0」を参考として、以下のように10のカテゴリで設定した。

カテゴリ	チェック項目	チェックの内容（判断基準）
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)経営者のリスク認識	経営者がサイバーセキュリティリスクを経営リスクの 1 つとして認識するよう促している。
	(2)経営者によるセキュリティポリシーの策定・宣言	経営者が、組織全体としてのサイバーセキュリティリスクを考慮した対応方針（セキュリティポリシー）を策定し、宣言するよう促している。
	(3)法律・業界ガイドラインの把握	法律や業界のガイドライン等の要求事項を把握するよう促している。
②サイバーセキュリティリスク管理体制の構築	(1)サイバーセキュリティリスク管理体制の構築	組織の対応方針（セキュリティポリシー）に基づき、CISO 等からなるサイバーセキュリティリスク管理体制を構築するよう促している。
	(2)関係者の役割と責任の明確化	サイバーセキュリティリスク管理体制において、各関係者の役割と責任を 明確にするよう促している。
	(3)リスク管理体制とサイバーセキュリティリスク管理体制の明確な規定	組織内のリスク管理体制とサイバーセキュリティリスク管理体制の関係を明確に規定するよう促している。
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	(1)対策の明確化・費用評価・予算確保	必要なサイバーセキュリティ対策を明確にし、経営会議などで対策の内容 に見合った適切な費用かどうかを評価し、必要な予算を確保するよう促している。
	(2)人材の確保、役割の理解	サイバーセキュリティ対策を実施できる人材を確保し、各担当者が自身の 役割を理解するよう促している。（組織の内外問わず）
	(3)組織内の人材育成	組織内でサイバーセキュリティ人材を育成するよう促している。
	(4)セキュリティ人材のキャリアパス・待遇の設定	組織内のサイバーセキュリティ人材のキャリアパスの設計を検討、及び適正な処遇をするよう促している。
	(5)継続的なセキュリティ対策の実施	セキュリティ担当者以外も含めた従業員向けセキュリティ研修等を継続的に実施するよう促している。
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	(1)情報資産の優先順位付け	守るべき情報を特定し、当該情報の保管場所やビジネス上の価値等に基 づいて優先順位付けを行うよう促している。
	(2)経営戦略を踏まえたリスクの把握	特定した守るべき情報に対するサイバー攻撃の脅威、脆弱性を識別し、 経営戦略を踏まえたサイバーセキュリティリスクとして把握するよう促している。
	(3)リスクが事業にも足たらす影響の推計	サイバーセキュリティリスクが事業にいかなる影響があるかを推定するよう促している。
	(4)リスク対応計画の策定	サイバーセキュリティリスクの影響の度合いに従って、リスク低減、リスク回避、リスク移転のためのリスク対応計画を策定するよう促している。
	(5)残留リスクの識別	サイバーセキュリティリスクの影響の度合いに従って対策を取らないと判断したものを残留リスクとして識別するよう促している。
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の構築	(1)重要端末への多層防御の実施	重要業務を行う端末、ネットワーク、システム、またはサービスにおいて、ネ ットワークセグメントの分離、アクセス制御、暗号化等の多層防御を実施するよう促している。
	(2)脆弱性診断の実施・対応	システム等に対して脆弱性診断を実施し、検出された脆弱性に対処するよう促している。
	(3)検知すべきイベントの特定・迅速な検知のための体制構築	検知すべきイベント（意図していないアクセスや通信）を特定し、当該イベントを迅速に検知するためのシステム・手順・体制（ログ収集や分析のための手順書策定）を構築するよう促している。
	(4)意図しないイベントへの対応計画の策定	意図していないアクセスや通信を検知した場合の対応計画（検知したイベ ントによる影響、対応者などの責任分担等）を策定するよう促している。
	(5)サイバーセキュリティリスクへの対応内容の見直し	サイバー攻撃の動向等を踏まえて、サイバーセキュリティリスクへの対応内容（検知すべきイベント、技術的対策の強化等）を適宜見直するよう促している。
	(6)従業員に対する教育の実施	従業員に対して、サイバーセキュリティに関する教育（防御の基本となる対策実施（ソフトウェアの更新の徹底、マルウェア対策ソフトの導入等）の周知、標的型攻撃メール訓練など）を実施するよう促している。

（出所）経済産業省『サイバーセキュリティ経営ガイドライン Ver 2.0』より三菱UFJリサーチ＆コンサルティング作成

1．共通項抽出方針

■ 前頁続き。

カテゴリ	チェック項目	チェックの内容（判断基準）
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	(1)経営者への対策状況の報告	経営者が定期的に、サイバーセキュリティ対策状況の報告を受け、把握するよう促している。
	(2)外部監査の実施	サイバーセキュリティにかかる外部監査を実施するよう促している。
	(3)環境変化に応じたPDCAの整備	サイバーセキュリティリスクや脅威を適時見直し、環境変化に応じた取組体制（PDCA）を整備・維持するよう促している。
	(4)リスクと取組状況の外部への公開	サイバーセキュリティリスクや取組状況を外部に公開するよう促している。
⑦インシデント発生時の緊急対応体制の整備	(1)組織内外の連絡先の整備	組織の内外における緊急連絡先・伝達ルートを整備するよう促している。（緊急連絡先 には、システム運用、Web サイト保守・運用、契約しているセキュリティベンダの連絡先含む）
	(2)初動対応マニュアルの整備	サイバー攻撃の初動対応マニュアルを整備するよう促している。
	(3)インシデント対応専門チームの設置	インシデント対応の専門チーム（CSIRT等）を設置するよう促している。
	(4)経営者への報告ルート・公開内容等の設定	経営者が責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等を定めるよう促している。
	(5)初動対応マニュアルの見直し	インシデント対応の課題も踏まえて、初動対応マニュアルを見直すよう促している。
	(6)定期的な対応訓練の実施	インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行うよう促している。
⑧インシデントによる被害に備えた復旧体制の整備	(1)業務の復旧計画の策定	被害が発生した場合に備えた業務の復旧計画を策定するよう促している。
	(2)復旧計画の見直し	復旧作業の課題を踏まえて、復旧計画を見直すよう促している。
	(3)組織内外の連絡先の整備	組織の内外における緊急連絡先・伝達ルートを整備するよう促している。
	(4)定期的な対応訓練の実施	定期的に復旧対応訓練や演習を行うよう促している。
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	(1)システム管理の適切な委託の実施	システム管理などについて、自組織のスキルや各種機能の重要性等を考慮して、自組織で対応できる部分と外部に委託する部分を適切に切り分るよう促している。
	(2)委託先に実施を求めるセキュリティ対策の明確化	委託先が実施すべきサイバーセキュリティ対策について、契約書等により明確にするよう促している。
	(3)サプライチェーンのセキュリティ対策状況の把握	系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先などのサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握するよう促している。
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	(1)業界団体を通じた情報共有の実施	各種団体が提供するサイバーセキュリティに関する注意喚起情報やコミュニティへの参加等を通じて情報共有（情報提供と入手）を行い自社の対策に活かすよう促している。
	(2)関係団体への情報提供の実施	マルウェア情報、不正アクセス情報、インシデントがあった場合に、IPAへの届出や一般社団法人JPCERTコーディネーションセンターへの情報提供、その他民間企業等が推進している情報共有の仕組みへの情報提供を実施するよう促している。

（出所）経済産業省『サイバーセキュリティ経営ガイドライン Ver 2.0』より三菱UFJリサーチ＆コンサルティング作成

1．共通項抽出方針

- 共通項の抽出にあたっては、評価シートを作成したうえで抽出を行う。
- 共通項の記載粒度の評価にあたっては、ガイドラインの読み手がチェック項目を実現するための方法の具体例やプロセスに関する記載の有無により評価を行う。

【抽出に用いる評価シートイメージ】

	評価基準
①記載有無	• チェック項目に該当する記載が、ガイドライン内にあれば「〇」として評価 • チェック項目に該当する記載が、なければ「－」として評価。
②記載粒度	• 上記、①にて「〇（＋１）」となった項目のうち、チェック項目の実現に向けた具体例やプロセスを示している場合には「◎（＋２）」として評価。

カテゴリ	チェック項目	チェックの内容（判断基準）	記載箇所・内容	記載有無・粒度
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	経営者のリスク認識	経営者がサイバーセキュリティリスクを経営リスクの１つとして認識するよう促しているか。	ガイドライン内の該当箇所、記載内容を抽出（例：経営リスクとして認識することの重要性の説明に具体性がある場合には「◎」）	◎、〇、ーの三段階で評価
	経営者によるセキュリティポリシーの策定・宣言	経営者が、組織全体としてのサイバーセキュリティリスクを考慮した対応方針（セキュリティポリシー）を策定し、宣言するよう促しているか。	ガイドライン内の該当箇所、記載内容を抽出（例：セキュリティポリシーの策定者の指定・推奨を行っている場合には「◎」）	◎、〇、ーの三段階で評価
	法律・業界ガイドラインの把握	法律や業界のガイドライン等の要求事項を把握するよう促しているか。	ガイドライン内の該当箇所、記載内容を抽出（例：具体的に把握すべきガイドライン名・箇所等を指定している場合には「◎」）	◎、〇、ーの三段階で評価
②サイバーセキュリティリスク管理体制の構築	サイバーセキュリティリスク管理体制の構築	組織の対応方針（セキュリティポリシー）に基づき、CISO 等からなるサイバーセキュリティリスク管理体制を構築するよう促しているか。	ガイドライン内の該当箇所、記載内容を抽出（例：管理体制の在り方・構築方法について言及している場合には「◎」）	◎、〇、ーの三段階で評価
	関係者の役割と責任の明確化	サイバーセキュリティリスク管理体制において、各関係者の役割と責任を明確にするよう促しているか。	ガイドライン内の該当箇所、記載内容を抽出（例：役割・責任の分担について具体例の記載があれば「◎」）	◎、〇、ーの三段階で評価
	リスク管理体制とサイバーセキュリティリスク管理体制の明確な規定	組織内のリスク管理体制とサイバーセキュリティリスク管理体制の関係を明確に規定するよう促しているか。	ガイドライン内の該当箇所、記載内容を抽出（例：望ましい管理体制の関係性について具体例の記載があれば「◎」）	◎、〇、ーの三段階で評価

２．共通項抽出対象のガイドライン

2．共通項抽出対象のガイドライン

■ 抽出対象としたガイドライン等は以下のとおり。

【抽出対象としたガイドライン】

発行主体	ガイドライン名
日本自動車工業会/日本自動車部品工業会	自工会部工会・サイバーセキュリティガイドライン 2.0 版
ビジネス機械・情報システム産業協会(JBMIA)	ネットワーク機能付き事務機セキュリティガイドラインVer.1.00
情報通信ネットワーク産業協会(CIAJ)	通信ネットワーク機器セキュリティ ユーザーガイドライン Ver. 2.0
日本電気制御機器工業会(NECA)	制御システムセキュリティ運用ガイドライン（制御システムセキュリティ研究会 2017年改訂版）
経済産業省 産業サイバーセキュリティ研究会	スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0
国土交通省	鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第４版
防衛装備庁	装備品等及び役務の調達における情報セキュリティ基準
経済産業省 産業サイバーセキュリティ研究会	ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版
日本電気協会	電力制御システムセキュリティガイドライン JEAG 1111-2019
日本電気協会	スマートメーターシステムセキュリティガイドライン JEAG 1101-2019
一般社団法人 日本建設業連合会	元請け会社における情報セキュリティガイドライン 2020年11月 改訂
一般社団法人 日本建設業連合会	建設現場における情報セキュリティガイドライン 2020年11月 改訂
厚生労働省	医療情報システムの安全管理に関するガイドライン 第5.2版

【その他ベンチマークとなるセキュリティ基準等】

発行主体	ガイドライン名
経済産業省	サイバー・フィジカル・セキュリティ対策　フレームワーク Version 1.0
NIST	重要インフラのサイバーセキュリティを改善するためのフレームワーク（別添資料にて共通項との対応関係を整理）
米国政府機関	米国政府機関 制御システムセキュリティガイドライン（全般）　1.0版
総務省／経済産業省	IoTセキュリティガイドライン Ver 1.0
情報処理推進機構（IPA）	中小企業の情報セキュリティガイドライン　第３版

2．共通項抽出対象のガイドライン

	評価基準
①記載有無	• チェック項目に該当する記載が、ガイドライン内にあれば「○（＋１）」として評価 • チェック項目に該当する記載が、なければ「－（±０）」として評価。
②記載粒度	• 上記、①にて「○（＋１）」となった項目のうち、チェック項目の実現に向けた具体例やプロセスを示している場合には「◎（＋２）」として評価。

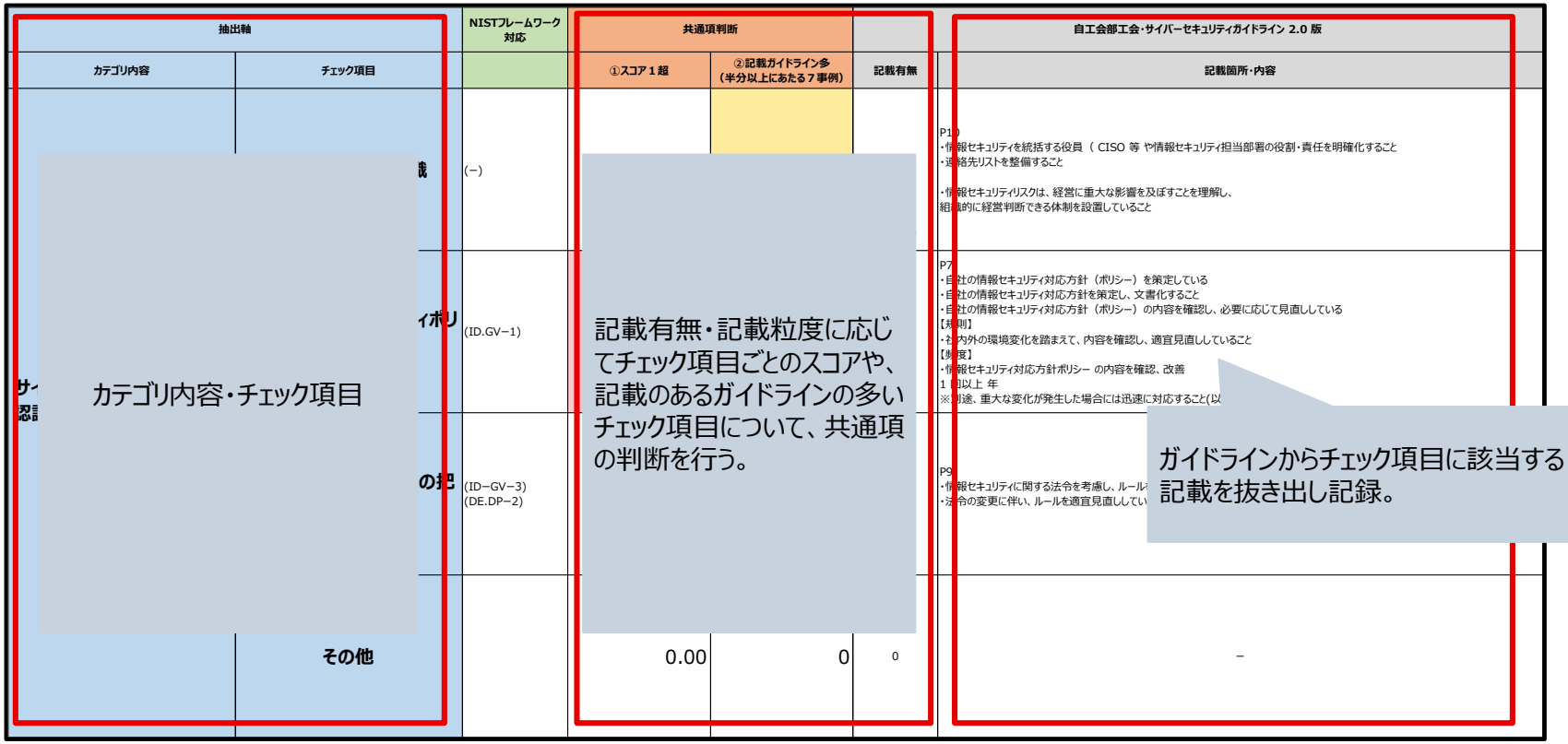
ガイドライン名	策定時期	最新版改訂時期	対象者（読み手）	ガイドラインの趣旨
自工会部工会・サイバーセキュリティガイドライン 2.0 版	令和２年３月31日	令和４年３月29日（第4版）	自動車産業に関係する全ての会社	自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した 、向こう3年の対策フレームワークや業界共通の自己評価基準を明示することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的とする。
ネットワーク機能付き事務機セキュリティガイドラインVer.1.00	令和３年６月	–	ネットワーク機能をもつ事務機メーカー等	ネットワーク機能をもつ一般オフィス/スモールオフィス/ホームオフィスユーザー向けのプリンター、スキャナー、ファクス、デジタルコピー機、デジタル複合機等のHard Copy Device(HCD)の購入者が必要とする基本的なセキュリティ要件を定義するもの。
通信ネットワーク機器セキュリティ ユーザーガイドライン Ver. 2.0	令和元年３月	令和２年５月	インターネット、IoTを構成する通信ネットワーク機器の利用者	当該機器ユーザーを対象に、通信ネットワーク機器のセキュリティ対策機能の取り扱いに関して、その必要性をご理解いただき、適切な設定/運用を実施頂くことを目的とするもの。
制御システムセキュリティ運用ガイドライン（制御システムセキュリティ研究会 2017年改訂版）	平成24年12月１日	平成29年11月24日	制御システムの運用・管理に携わる管理者、設計・構築に携わる設計者、保守に携わる保守担当者、オペレータ等	制御システムをよりセキュアに構築・運用し、操業を安全に継続するための指針を示すもの。
スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0	令和３年４月１日	–	スマートホームに関係する事業者、所有者住まい手	サイバーフィジカルシステムの一つであるスマートホームについて、主にサイバーセキュリティを強化するために、関係するステークホルダーが実施すべき基本的なセキュリティ指針を示すもの。
鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第４版	平成18年９月29日	平成31年３月29日（第4版）	鉄道分野に関係する事業者	鉄道分野において必要又は望ましい情報セキュリティ対策の水準を明示し、個々の重要インフラ事業者等が、重要インフラの担い手としての意識に基づいて自主的に取り組むPDCA サイクルに沿った対策の実施や検証に当たっての目標を定めるもの。
装備品等及び役務の調達における情報セキュリティ基準	–	–	防衛関連企業において保護すべき情報に接する全ての者	装備品等及び役務の調達に係る企業において当該調達に係る保護すべき情報の適切な管理を目指し、防衛省として求める対策を定めるもの。
ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版	令和元年６月17日	–	ビルシステムに関わるステークホルダ、ビルの利用者やビルにサービスを提供するサービスプロバイダ等	これまで取組が遅れていたビルシステムのサイバーセキュリティに関して、その確保のためのガイダンスを示すことを目的とするもの。
電力制御システムセキュリティガイドライン JEAG 1111-2019	平成28年５月30日	令和元年７月31日（第１回改訂）	電気事業者	電気制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策の要求事項について規定するもの。
スマートメーターシステムセキュリティガイドライン JEAG 1101-2019	平成28年３月10日	令和元年７月31日（第１回改訂）	一般送配電事業者が施設するスマートメーターシステムに携わる者	スマートメーターシステムのセキュリティ確保を目的として一般送配電事業者が実施すべきセキュリティ対策の要求事項について規定するもの。
元請け会社における情報セキュリティガイドライン 2020年11月 改訂	平成22年６月	令和２年11月	建設現場における元請会社	建設現場における情報セキュリティを一定水準以上のレベルに保つためには、各社個別の対応ではなく、建設業界全体としての取り組みが必要であることから、その指針となる具体的な対策を示すもの。
建設現場における情報セキュリティガイドライン 2020年11月 改訂	平成20年11月	令和２年11月	建設現場に関わる事業者	建設業界の目指すべき情報セキュリティ対策の指針として活用され、建設業各社の建設現場における情報セキュリティ事故発生防止に寄与することを目的とするもの。
医療情報システムの安全管理に関するガイドライン 第5.2版	平成17年３月	令和４年３月	医療機関等	医療機関等において、特にランサムウェアに代表されるっ攻撃への対策は喫緊の課題となっており、必要となる安全対策や、安全対策を行う江での背景となる考え方等を示すもの。
自工会部工会・サイバーセキュリティガイドライン 2.0 版	平成31年４月18日	–	事業者	サイバー空間とフィジカル空間が高度に融合した産業社会を3 つの切り口から捉え、サプライチェーンの信頼性（trustworthiness）を確保する観点から、それぞれの切り口において守るべきもの、直面するリスク源、対応の方針等を整理するもの。
ネットワーク機能付き事務機セキュリティガイドラインVer.1.00	平成30年４月16日	–	事業者	ビジネス上のニーズと組織のニーズに基づいた、費用対効果の高いサイバーセキュリティリスク対策・管理の「共通言語」を記すもの。
通信ネットワーク機器セキュリティ ユーザーガイドライン Ver. 2.0	平成25年４月	平成27年５月	事業者	産業用制御システムの概要及び一般的なシステムトポロジーについて示し、システムにとっての一般的な脅威と脆弱性を特定し、関連リスクを低減するための推奨セキュリティ対策を提示するもの。
制御システムセキュリティ運用ガイドライン（制御システムセキュリティ研究会 2017年改訂版）	平成28年７月	–	事業者	IoT 機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめたもの。
スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0	平成21年３月	令和元年３月	中小企業および小規模事業者	中小企業にとって重要な情報を漏えい、改ざん、焼失などの脅威から保護するための情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介することを目的とするもの。

3．抽出結果

3．抽出結果

- 抽出結果の詳細については、「F」にてとりまとめを実施した。「ガイドライン共通項抽出結果（別紙）」では、各ガイドラインの抽出結果を一覧化し、チェック項目に該当する記載の抜き出し、も行っている。
- 参考としたベンチマーク基準についても、「ベンチマーク抽出結果詳細（別紙）」にて、とりまとめを実施した。

【「ガイドライン共通項抽出結果（別紙）」のとりまとめイメージ】



3．抽出結果

- 抽出結果に基づき、チェック項目ごとの記載傾向を確認し、共通項の抽出を行うため、チェック項目別のスコアの平均点を算出した。
- 今回、**①チェック項目別のスコアの平均点が「１」を超えるチェック項目**、もしくは、**②記載が確認できたガイドラインが半数以上（７つのガイドライン以上）のチェック項目**を、共通項として抽出することとした。

【（例）チェック項目：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】

ガイドライン	抽出結果
自工会部工会・サイバーセキュリティガイドライン 2.0 版	○
ネットワーク機能付き事務機セキュリティガイドラインVer.1.00	－
通信ネットワーク機器セキュリティ ユーザーガイドライン Ver. 2.0	－
制御システムセキュリティ運用ガイドライン（制御システムセキュリティ研究会 2017年改訂版）	－
スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0	－
鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第４版	○
装備品等及び役務の調達における情報セキュリティ基準	○
ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版	○
電力制御システムセキュリティガイドライン JEAG 1111-2019	◎
スマートメーターシステムセキュリテ	◎
元請け会社における情報セキュリ	－
建設現場における情報セキュリテ	○
医療情報システムの安全管理に関するガイドライン 第5.2版	－
本チェック項目におけるスコアの平均点	**0.69**
記載を確認したガイドライン数	**7**

以下の場合に共通項として抽出する。
①：チェック項目別のスコアの平均点が「１」を超えた項目
②：①に該当しないものの記載が確認できたガイドラインが半数以上（７つのガイドライン以上）の項目

3．抽出結果

- **各ガイドラインのチェック項目別に、前述の評価基準をもとに評価を行い、抽出対象としたガイドラインにて記載が充実している項目、記載が多い項目について、共通項として抽出した。**
- **共通項として抽出されたチェック項目は以下のとおりである（赤字のチェック項目が共通項に該当）。**

カテゴリ	チェック項目	①チェック項目ごとの平均点が「１」を超えた項目	①に該当しないものの記載が確認できたガイドラインが半数以上の項目
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)経営者のリスク認識	―	○
	(2)経営者によるセキュリティポリシーの策定・宣言	○	―
	(3)法律・業界ガイドラインの把握	―	○
②サイバーセキュリティリスク管理体制の構築	(1)サイバーセキュリティリスク管理体制の構築	○	―
	(2)関係者の役割と責任の明確化	○	―
	(3)リスク管理体制とサイバーセキュリティリスク管理体制の明確な規定	―	―
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	(1)対策の明確化・費用評価・予算確保	―	―
	(2)人材の確保、役割の理解	―	○
	(3)組織内の人材育成	―	―
	(4)セキュリティ人材のキャリアパス・待遇の設定	―	―
	(5)継続的なセキュリティ対策の実施	―	―
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	(1)情報資産の優先順位付け	―	―
	(2)経営戦略を踏まえたリスクの把握	―	○
	(3)リスクが事業にも足たらす影響の推計	―	―
	(4)リスク対応計画の策定	―	○
	(5)残留リスクの識別	―	―
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の構築	(1)重要端末への多層防御の実施	○	―
	(2)脆弱性診断の実施・対応	○	―
	(3)検知すべきイベントの特定・迅速な検知のための体制構築	○	―
	(4)意図しないイベントへの対応計画の策定	―	―
	(5)サイバーセキュリティリスクへの対応内容の見直し	○	―
	(6)従業員に対する教育の実施	○	―

3．抽出結果

■ 前頁続き。

カテゴリ	チェック項目	①チェック項目ごとの平均点が「１」を超えた項目	①に該当しないものの記載が確認できたガイドラインが半数以上の項目
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	(1)経営者への対策状況の報告	ー	ー
	(2)外部監査の実施	ー	ー
	(3)環境変化に応じたPDCAの整備	ー	ー
	(4)リスクと取組状況の外部への公開	ー	ー
⑦インシデント発生時の緊急対応体制の整備	(1)組織内外の連絡先の整備	ー	ー
	(2)初動対応マニュアルの整備	ー	○
	(3)インシデント対応専門チームの設置	ー	ー
	(4)経営者への報告ルート・公開内容等の設定	ー	ー
	(5)初動対応マニュアルの見直し	ー	ー
	(6)定期的な対応訓練の実施	ー	ー
⑧インシデントによる被害に備えた復旧体制の整備	(1)業務の復旧計画の策定	ー	○
	(2)復旧計画の見直し	ー	ー
	(3)組織内外の連絡先の整備	ー	ー
	(4)定期的な対応訓練の実施	ー	ー
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	(1)システム管理の適切な委託の実施	ー	ー
	(2)委託先に実施を求めるセキュリティ対策の明確化	ー	○
	(3)サプライチェーンのセキュリティ対策状況の把握	ー	ー
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	(1)業界団体を通じた情報共有の実施	ー	ー
	(2)関係団体への情報提供の実施	ー	ー

3．抽出結果

- 共通項として抽出された項目について、各ガイドライン内で記載されていた内容例の一部を整理した。**記載内容が少ない水準の記載例を「第１段階」、記載が具体的であり望ましいと考えられる水準の記載例を「第２段階」、とレベル別に整理**している。
- また、**サイバーセキュリティお助け隊サービスを用いることで対応が可能な項目についても個別に記載**した。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
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	経営者のリスク認識	【第１段階】 （装備品等及び役務の調達における情報セキュリティ基準） ● 経営者等は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て、情報セキュリティ基本方針等の承認等を通して、自社における情報セキュリティの確保に努めるものとする。 【第２段階】 （電力制御システムセキュリティガイドライン） ● 経営層は、電力制御システム等におけるセキュリティの確保が事業遂行の重要な要素であることを認識し、電力制御システム等のセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。これを行わない場合、電気事業者が重要インフラとしての社会的責任を果たすためのセキュリティ対策が実行されない可能性がある。	本項目については、サイバーセキュリティお助け隊サービスを用いることにより、24時間365日、挙動や問題のある攻撃を検知することが可能となる。
	経営者によるセキュリティポリシーの策定・宣言	【第１段階】 （元請け会社における情報セキュリティガイドライン） ● 情報セキュリティ対策として各項目の具体的な手順やルールを定めます。従業員および協力会社を含めた現場構成員に周知します。定期的に手順・ルールの見直しを行い、変更した場合はその都度、現場構成員に周知することも必要です。 【第２段階】 （電力制御システムセキュリティガイドライン） ● 経営層は、電力制御システム等におけるセキュリティの確保が事業遂行の重要な要素であることを認識し、電力制御システム等のセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。これを行わない場合、電気事業者が重要インフラとしての社会的責任を果たすためのセキュリティ対策が実行されない可能性がある。	―
	法律・業界ガイドラインの把握	【第２段階】 （鉄道分野における情報セキュリティ確保に係るガイドライン） ● 「安全ガイドライン」の形態 各重要インフラ事業者等は、当該事業分野に関する法制度の下、関係する基準に従い、業を営んでいる。 このことを踏まえ、「指針」においては、各重要インフラ事業者等の判断や行為に関する基準又は参考となる文書類を「安全基準等」と呼び、次の①～④に分類している。 ①関係法令に基づき国が定める「強制基準」 ②関係法令に準じて国が定める「推奨基準」及び「ガイドライン」 ③関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」 ④関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等 本ガイドラインは②に対応し、国が定める「ガイドライン」として推奨事項を列挙しているものであり、事業分野の特性に鑑み、重要インフラ事業者等が自らの情報セキュリティ対策を実施する際に参考資料として活用することを想定している。	―

3．抽出結果

■ 前頁続き。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
サイバーセキュリティリスク管理体制の構築	サイバーセキュリティリスク管理体制の構築	【第１段階】 （元請け会社における情報セキュリティガイドライン） ● 情報セキュリティを推進する元請会社の管理体制を組織します。 【第２段階】 （自工会部工会・サイバーセキュリティガイドライン） ● 情報セキュリティを統括する役員（ CISO 等 や情報セキュリティ担当部署の役割・責任を明確化すること。 ● 連絡先リストを整備すること。 ● 情報セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、組織的に経営判断できる体制を設置していること。	―
	関係者の役割と責任の明確化	【第１段階】 （スマートメーターシステムセキュリティガイドライン） ● スマートメーターシステムに関連する者に対して、スマートメーターシステムに関するセキュリティ管理体制における役割を明確にし、それぞれが役割を理解したことを確認する。 【第２段階】 （装備品等及び役務の調達における情報セキュリティ基準） ● 経営者等は、取扱者の指定の範囲を業務の遂行上必要最小限度に制限するとともに、次に掲げる事項に合意した者の中からふさわしい者を取扱者に指定するものとする。 (ｱ) 在職中及び離職後において、業務上知り得た保護すべき情報を、第三者に漏えいしないこと（以下「守秘義務」という。）。 (ｲ) 守秘義務に違反した場合に法律上の責任を負うこと。 (ｳ) 守秘義務の内容を理解し、かつ、承諾すること。 ● 経営者等は、保護すべき情報に係る全ての情報セキュリティの責任を明確にするため、取扱者のうち、ふさわしいと認める者を次に掲げる者に指定するものとする。 (ｱ) 総括者 (ｲ) 保護すべき情報及びこれに関連する資産ごとに、それぞれ管理責任を負う者（以下「管理者」という。）」経営者等は、保護システムに係る全ての情報セキュリティの責任を明確にするため、保護システム利用者のうち、ふさわしいと認める者を次に掲げる者に指定するものとする。 (ｱ) 保護システムの運用管理に責任を負う者（以下「保護システム管理者」という。） (ｲ) 保護システム管理者の業務遂行を補佐する者（以下「保護システム担当者」という。）」	―

3．抽出結果

■ 前頁続き。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
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	人材の確保、役割の理解	【第１段階】 （ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版） ● ビルシステムに対して十分なセキュリティ知識を持った技術者の元で設計を実施する体制を整える。 【第２段階】 （鉄道分野における情報セキュリティ確保に係るガイドライン） ● 人材育成・配置・ノウハウの蓄積 システムにおける情報セキュリティ対策は複数の対策を組み合わせることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といった情報セキュリティ対策の水準を維持するための対応が必要である。このことから、情報セキュリティ対策に係る担当者が変更となっても情報セキュリティ対策の水準を維持できるよう、ノウハウを蓄積するとともに、実効性を考慮した継続的な人材育成と配置を行う。 また、情報セキュリティに係る教育は、システム業務に従事する人材のみならずシステムユーザーやＰＣ操作者も対象であることから、全社的に行う。 さらに、情報セキュリティ対策の推進役となるセキュリティ人材について、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人数等を確保・維持する観点から、これらのセキュリティ人材の事業者内のキャリアパス及び賃金政策をあらかじめ検討しておくことが重要となる。	ー

3．抽出結果

■ 前頁続き。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
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	経営戦略を踏まえたリスクの把握	【第１段階】 （自工会部工会・サイバーセキュリティガイドライン） ● 情報資産管理台帳の作成 重要度の判定は、情報資産ごとに３段階に分類し重要度に応じた取扱いを規定化し運用を行う。 【第２段階】 （鉄道分野における情報セキュリティ確保に係るガイドライン） ● 対策の指針 情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析結果及び演習・訓練を通じた課題抽出として、それぞれの取組の中で発見したリスク源となり得る脅威や脆弱性、影響を受ける維持すべきサービスレベル、脅威や脆弱性から生じ得る事象に鑑みてリスクを特定（リスク特定）する。	―
	リスク対応計画の策定	【第１段階】 （電力制御システムセキュリティガイドライン） ● セキュリティ対策は、事業計画に沿ってセキュリティ管理責任組織のもとで策定した方針にしたがって計画し、対象システムやネットワーク構成を把握したうえで、最適なリスクアセスメント手法を用いて選択する。セキュリティ対策の実施が困難な場合は、残存リスクとして識別し、次の改善時に対応が検討できるように文書に残す。セキュリティ事故発生時も、影響を最小限にとどめることを基本的な考え方として、サービス継続の観点にも留意し、対策を計画する。 【第２段階】 （装備品等及び役務の調達における情報セキュリティ基準） ● 高い機密区分の情報資産情報を一覧化している経営者等は、情報セキュリティ事故及び情報セキュリティ事象（以下「事故等」という。）の発生に備え、情報セキュリティ事故等対処計画を定めるものとし、総括者は、次に掲げる事故等対処の各段階に対処し得る体制、責任及び手順を定めるものとする。 ア 事故等への対処の準備 イ 事故等の発見及び検知時の報告・連絡要領 ウ 事故等の監視（システム監視を含む。）及び分析 エ 事故等による被害及び影響の抑制並びに局限 オ 事故等に係る証拠の保存及び原因の究明 カ 事故等からの復旧（復旧に要する時間の目標を含む。）」	―

3．抽出結果

■ 前頁続き。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
サイバーセキュリティリスクに対応するための仕組みの構築	重要端末への多層防御の実施	【第１段階】 該当の記載なし。 【第２段階】 （制御システムセキュリティ運用ガイドライン） ● 制御システムを接続するネットワークは業務用ネットワーク（情報システム）との間に、ファイヤーウォールでDMZ(De-Militarized Zone)を設置して、業務用ネットワークから制御システムネットワークへメールを送らないようにしたり、制御システムネットワークからインターネット接続をしないようにしたりする対策を推奨する。 （鉄道分野における情報セキュリティ確保に係るガイドライン） ● 取扱者は、情報システムに入力された情報若しくは情報システムから出力した情報を記載した書面について、情報の格付けに従って、適切に管理すること ● 取扱者は、情報をサーバ装置、端末又は外部記録媒体に保存する場合には、保存する情報の格付けに従って、暗号化を行う必要性の有無を検討し、必要があると認めたときは、客観的に評価された暗号技術により、情報を暗号化すること ● 取扱者は、情報をサーバ装置、端末又は外部記録媒体に保存する場合には、保存する情報の格付けに従って、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用する必要性の有無を検討し、必要があると認めたときは、インターネットや、インターネットに接点を有する情報システムに接続しない端末、サーバ装置等の機器等を使用するなどの対応を行うこと ● 取扱者は、情報を保存した機器等について、保存した情報の格付けに従って、盗難及び不正な持ち出し等の物理的な脅威から保護する必要性の有無を検討し、必要があると認めたときは、盗難及び不正な持ち出し等の物理的な脅威から保護するための対策を講ずること	―

3．抽出結果

■ 前頁続き。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
サイバーセキュリティリスクに対応するための仕組みの構築	脆弱性診断の実施・対応	【第１段階】 （電力制御システムセキュリティガイドライン） ● 通信路上のセキュリティ確保が必要な区間を予め定め、その内容に従って通信プロトコルを選択することが望ましい。採用した通信プロトコルについては、ぜい弱性情報を定期的に収集することが望ましい。また、通信プロトコルをカスタマイズする場合は、当初のセキュリティ機能を損なうことがないように実装することが望ましい。 【第２段階】 （自工会部工会・サイバーセキュリティガイドライン） ● 脆弱性の管理体制、管理プロセスを定めている ・脆弱性情報の収集から対応まで担当部署の役割・責任を明確化すること ・脆弱性情報 脅威情報を収集する情報源、ツール、頻度を定めること ・収集した情報の対応要否判断基準・対応手順を定めること ・対応履歴を記録し、月次でチェックすること ・社外へ公開している サーバー について、本番稼働前および稼働後に脆弱性診断を実施し、判明した脆弱性に対して対策 を行っている 【規則】 ・プラットフォームの脆弱性を診断すること ・脆弱性に対する対応の要否判断規則とリードタイムを決めること ・診断結果と対応結果を保管すること 【対象】 ・ 社外公開 サーバー の OS 、ミドルウェア 【診断頻度】 ・ 本番稼働前： 1 回以上 ・ 本番稼働後： 2 回 年およびシステムの大きな変更時 ・ 影響の大きな脆弱性が公開された時	ー

3．抽出結果

■ 前頁続き。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
サイバーセキュリティリスク管理体制の構築	検知すべきイベントの特定・迅速な検知のための体制構築	【第１段階】 （通信ネットワーク機器セキュリティガイドライン） ● 適切なログ管理を実施することで、悪意ある第三者等からの不正侵入、不正操作等の情報セキュリティインシデント及びその予兆を検知し、その原因究明を行うことができます。また、組織の利用者による不正行為を抑止する効果も期待できます。 【第２段階】 （鉄道分野における情報セキュリティ確保に係るガイドライン） ● 情報システムにおけるログとは、システムの動作履歴、取扱者のアクセス履歴、その他必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の重要インフラサービス障害（その予兆を含む。）を検知するための重要な材料となるものである。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、また、改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。	本項目については、サイバーセキュリティお助け隊サービスを用いることにより、24時間365日、挙動や問題のある攻撃を検知することが可能となる。
	サイバーセキュリティリスクへの対応内容の見直し	【第１段階】 （建設現場における情報セキュリティガイドライン） ● 情報セキュリティ対策の実効性を確保していくためには、定期的に運用状況の確認・改善を行っていくことが必要である。 【第２段階】 （スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン） ● IoT機器およびIoT機器を含むシステムの構成要素管理のセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施し、IoT機器およびIoT機器を含むシステムのライフサイクル全体に対し、受容できないセキュリティリスクおよび、セーフティに関するハザードに対応すること。 【サイバーセキュリティお助け隊サービスを用いた対応】 ● 本項目については、サイバーセキュリティお助け隊サービスを用いることにより、簡易的なサイバー保険に加入することができ、突発的な対応に係る費用負担が軽減されることから、リスク検討の際に考慮することが望ましい。	―
	従業員に対する教育の実施	【第１段階】 （元請け会社における情報セキュリティガイドライン） ● 各社の責任者、作業員および図面等の情報資産を取扱う担当者に対し 、情報セキュリティ 教育を実施します。 【第２段階】 （建設現場における情報セキュリティガイドライン） ● セキュリティ責任者は、関係者全員に情報セキュリティ教育を年１回以上の頻度で実施する。 主な教育内容 ・（各社の)情報セキュリティポリシー概要 ・建設現場でのセキュリティの必要性 ・現場事務所のルール、手順 ・情報セキュリティ事故の対応方法と再発防止策 ・利用者が行うこと、行ってはいけないこと	―

3．抽出結果

■ 前頁続き。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
インシデント発生時の緊急対応体制の整備	初動対応マニュアルの整備	【第１段階】 （自工会部工会・サイバーセキュリティガイドライン） ● 発生した情報セキュリティ事件・事故対応が実施され、事故の概要や影響および対応内容の記録がある 【規則】 ・情報セキュリティ事件・事故発生後の初動対応フローが整備されていること 【第２段階】 （電力制御システムセキュリティガイドライン） ● 責任と手順 また、経営層をはじめとする組織内の関係個所及び組織外の関係機関へのセキュリティ事故の報告を含むセキュリティ事故対応についての手順を策定し、定期的に見直しを実施する。手順にはセキュリティ事故対応および再発防止策の検討のための活動も含める。なお、役割や手順の策定にあたっては、セキュリティ事故対応のための体制や必要に応じた機器管理体制の迅速な立ち上げ、及び体制間での密接な情報共有等の連携にも留意する。なお、政府機関が大規模サイバー攻撃事態と判断した時には、政府機関の要請があれば、これに協力する。	本項目については、サイバーセキュリティお助け隊サービスを用いることにより、問題が発生した際に、地域のIT事業者等が駆付け、もしくはリモートで対応する駆付けサービスを利用できるため、初動対応マニュアルに組み込むことが望ましい。
インシデントによる被害に備えた復旧体制の整備	業務の復旧計画の策定	【第１段階】 （鉄道分野における情報セキュリティ確保に係るガイドライン） ● コンティンジェンシープラン及び事業継続計画等の整備 【対策の指針】 重要インフラサービス障害が発生した場合、安全を確保するとともに、許容可能な時間内に許容可能な水準まで復旧させることが要求されるため、重要インフラサービス障害の発生に備えた対処態勢をあらかじめ整備することが重要となる。そこで、初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープラン」及び事業継続を目的とした復旧対応の方針等を定めた「事業継続計画（BCP：Business Continuity Plan)」（以下「BCP」という。）を策定する（または、これらと同等の方針を定めた計画を策定する）とともに、当該計画の実行に必要な組織体制を整備する。 【第２段階】 （自工会部工会・サイバーセキュリティガイドライン） ● 事業継続上重要なシステムについては、要度に応じて決められた各システムの復旧ポイント、復旧時間を満足するデータと手順が整備されている 【規則】 ・求められる復旧ポイントへ復帰可能なバックアップ及びトランザクションデータログを保管すること。 ・求められる復旧時間でリストアできる手順書を整備すること 【対象】 ・事業継続上重要なシステム	ー

3．抽出結果

■ 前頁続き。

カテゴリ内容	チェック項目	内容例	サイバーセキュリティお助け隊サービスを用いた対応可否
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	委託先に実施を求めるセキュリティ対策の明確化	【第１段階】 （制御システムセキュリティ運用ガイドライン） ● 社外の作業者に保守作業等の作業をゆだねる際には、事前に審査登録済みの作業者または会社かどうかをチェックすること。また、入退室の管理やオペレータを認証する仕組みを導入することを推奨する。 【第２段階】 （建設現場における情報セキュリティガイドライン） ● 協力会社、委託先の管理 セキュリティ責任者は、協力会社・委託先が情報セキュリティ基本方針に基づき、情報セキュリティに関する具体的なルールや手順を遵守できるかのチェックを行う。基準を満たしていない場合は、改善要求し対応状況を確認する。現場所長またはセキュリティ責任者は、発注者と締結した契約書の秘密保持や情報セキュリティ関連事項を確認し、その内容を協力会社との下請負契約または委託先との業務委託契約の特記事項、条件書などに明記して契約を締結する。	ー

3．抽出結果（チェックシート）

- 前述の共通項として抽出された項目について、各ガイドライン内で記載されていた内容例を踏まえ、別紙にて業界ガイドラインから得られた共通項について、対処できているかどうかを確認するためのチェックシートを取りまとめた。
- 共通項として抽出された項目について、各ガイドライン内で記載されていた内容例の一部を整理した結果も踏まえ、中小企業にまず取り組んでもらうべき内容を「第１段階」、より踏み込んだ内容を「第２段階」として整理している。

【チェックシートイメージ】

カテゴリ	共通項として抽出されたチェック項目	チェックの視点	チェック
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	経営者のリスク認識	【第１段階】※達成していれば「○」 経営者がサイバーセキュリティリスクを認識している。 【第２段階】※達成していれば「◎」 認識したうえで、以下のような具体的な取り組みを行っている。 ① 経営者自身の責任の明確化。 ② 情報セキュリティの責任に関する方向性の検討。 ③ 自社のセキュリティ基本方針等の承認の実施	
	経営者によるセキュリティポリシーの策定・宣言	【第１段階】※達成していれば「○」 セキュリティポリシーを策定し、宣言している。 【第２段階】※達成していれば「◎」 セキュリティポリシーに以下のような視点が含まれているか。 ① 情報セキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかについて、自社に適した情報セキュリティに関する基本方針を定めている。 ② 自社の経営において最も重視される事項は何かを明確にしている。	
	法律・業界ガイドラインの把握	【第１段階】※達成していれば「○」 法律・業界ガイドラインについて把握している。 【第２段階】※達成していれば「◎」 法律・業界ガイドライン把握するにあたり、以下のような前提・認識を有している。 ① 情報技術の進化の早さから常に実施を検討するべき対策は目まぐるしく変化するため、自社だけで把握することは困難であることから、情報セキュリティに関する最新動向を発信している公的機関などを把握し、常時参照することで備えるように情報セキュリティ担当者に指示を行っている。 ② 知り合いやコミュニティへの参加を通じ情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有することとなっている。	
サイバーセキュリティリスク管理体制の構築	サイバーセキュリティリスク管理体制の構築	【第１段階】※達成していれば「○」 情報セキュリティ対策を推進する管理体制を定めている。 【第２段階】※達成していれば「◎」 以下のような管理体制が構築されている。	

4．考察

４．考察

■ 共通項が抽出されたカテゴリについて

- カテゴリ別にみると、**「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」、「 ②サイバーセキュリティリスク管理体制の構築」、「④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」「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の構築」、「⑦インシデント発生時の緊急対応体制の整備」、「⑧インシデントによる被害に備えた復旧体制の整備」、「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」について、共通項として抽出されたチェック項目が存在した。**
- 特に、**「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」、「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の構築」については抽出された共通項が多く、重要性の高いカテゴリとして認知されている傾向がある**と考えられる。

■ インシデント発生時の対応や復旧フェーズにおける記載が少ない。

- セキュリティに対する認識や体制構築に対する項目と比較すると、**インシデント発生時の対応や復旧体制にかかる記載が少ない傾向がみられた。**
- **今回、分析対象とした既存の業界ガイドラインにおいて、被害に遭うことを前提とした記載が少ないことは課題**といえる。たとえば、IPAが実施する既存調査で得られた事例集等も活用しつつ、業界ガイドライン内に、中小企業における被害事例を盛り込んでいただくよう働きかけ、業界団体や、業界ガイドラインの読み手に対して、情報セキュリティ被害が起こりえるものであるという認識を持っていただくことも有益ではないか。

４．考察

■ 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策定についての記載が少ない。

- 参考としたベンチマーク基準と比較すると、**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」カテゴリのチェック項目について業界ガイドラインにおける記載が少ない傾向がみられた**。
- 「情報資産の優先順位付け」は実施できているものの、**リスク評価やリスク対応計画の策定、対策を講じたうえでも残留するリスクについての認識を促す記載が少ないことが課題**といえる。
- リスクの特定、リスクの算定・評価を行ったうえで、リスク対策の選択・実施、残留リスクの評価・モニタリングの実施といった、**一連のリスクマネジメント対策の重要性に関する記載を業界ガイドラインに盛り込んでいく必要性があるのではないか**。

■ 委託先も含めたサプライチェーンセキュリティ対策のうち、自社がコスト・労力を要する必要のある記載が少ない。

- 委託先等を含めたサプライチェーンの状況把握については、**「委託先に実施を求めるセキュリティ対策の明確化」に関する記載が多く、取引先のセキュリティ対策に対する意識は高い傾向がみられた**。業界ガイドラインという文章の特殊性によるものと推察される。
- 一方で、「システム管理の適切な委託の実施」や、「サプライチェーンのセキュリティ対策状況の把握」、といった項目については項目別平均点が低くなっており、**自社がコスト・労力をかけて実施するサプライチェーンセキュリティ対策については、具体的な記載が少ないことが課題**といえる。

４．考察

■ 情報共有活動に対する重要性認識に課題がある。

- 参考としたベンチマーク基準において、情報共有活動の重要性は指摘されているものの、**業界団体や関係団体を通じた情報共有・情報提供の実施に関する記載がないガイドラインが多い**。
- 「2021年度中小企業における情報セキュリティ対策実態調査」をみても、中小企業が困ったことがあった際に相談する先として、業界団体を挙げた企業は、全体のうち2.7%にとどまっている。**業界団体として、業界ガイドライン内に情報共有活動に関連する記載を設けていくとともに、情報セキュリティに関する情報の入手・提供を行うことができる窓口の設置や、既に業界窓口を有する場合については、中小企業に対しても間口を広げていくことは有益ではないか**。

■ ガイドラインで言及している内容・レベル感にばらつきがある。

- 今回、共通項抽出対象としたガイドラインと、IPA中小企業の情報セキュリティガイドラインや、METIサイバーセキュリティガイドラインと比較すると、具体の記載のある項目については、IPAやMETIのガイドラインと同程度の内容の記載がみられる。
- 一方で、**業界によりガイドライン内で企業に求める水準には差がみられており、インフラ業界を中心に、中小企業にとっては実現が非常に困難と考えられる水準をガイドライン内で設定しているケースもみられる**。そのため、各業界においては、**今後盛り込むべきガイドラインの記載の追記や業界としての追加的な取組を行うことが望ましく、そのために本業務を通じて抽出された共通項を参考としてほしい**。

４．考察

■ 中小企業に求められる対応

- 共通項として抽出された項目については、今後、業界を問わず求められる水準のセキュリティ対策として認知される可能性が高く、取引先企業からの依頼される機会も増えることも見込まれる。
- そのため、**中小企業においては、共通項として抽出された項目のセキュリティ対策について積極的に対策を行うことで、取引先からの信頼獲得や取引の維持につながる効果も期待できる**。

■ 業界団体に求められる対応

- 業界によりガイドライン内で企業に求める水準には差がみられており、共通項として抽出された項目の一部については、すぐに対応することが難しい中小企業が多い業界もあることが想定される。しかし、**高度なセキュリティ対策を求められる業界と取引を行う企業においては、今後、自らの業界水準とは関係なく高い水準のセキュリティ対策の実施を要請される可能性が高い**。
- 現在、業界を超えた取引や多様な主体との連携により事業を行うことが求められるようになっていることを踏まえ、**自らの業界に求められる水準について意識を向けるだけでなく、より高い水準を設定して対策を行っている業界の動向を意識しつつ、自らの業界のセキュリティ水準を高める検討を行っていくことが必要**である。