サイバーセキュリティ経営ガイドライン

Ver 3.0

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 Ver3.0 の策定にあたって

平成 27 年に Ver1.0 を公表して以来、サイバーセキュリティ経営ガイドラインは国内企業において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着実に普及しつつある。経済産業省が公表するコーポレートガバナンスに関する各種ガイドラインにおいてもサイバーセキュリティリスクについては本ガイドラインを参照することを求めるものが増えており、本ガイドラインは「中小企業の情報セキュリティ対策ガイドライン」[1]（独立行政法人情報処理推進機構発行）とともに、国内企業間でサイバーセキュリティ対策を行う際の共通言語としての役割を担っている。

平成 29 年の Ver2.0 の公開以降、企業のサイバーセキュリティ対策を取り巻く環境においては次のような変化が生じている。

- テレワーク等に代表される、デジタル環境の活用を前提とする働き方の多様化
- インターネットに代表されるサイバー空間と、現物の取引を行う場であるところのフィジカル空間とのつながりの緊密化とそれに伴うリスクの顕在化
- 情報資産とそれを扱う IT 系の環境のみを守ることから、制御系を含むデジタル基盤を守ることへのサイバーセキュリティの対象の変化・拡大
- ランサムウェアによる被害[2]の顕在化により、企業におけるサイバーセキュリティに関する被害は情報漏えいにとどまらず、企業の事業活動の停止へと影響が拡大
- 国内外のサプライチェーンを介したサイバーセキュリティ関連被害の拡大を踏まえた、サプライチェーン全体を通じた対策の推進の必要性の高まり
- ESG（Environment, Society, Governance）投資の拡大に伴う、コーポレートガバナンス及びエンタープライズリスクマネジメントの改善に向けた取組への関心の高まり

これらを踏まえ、Ver3.0 の策定にあたっては、Ver2.0 で定めた「経営者が認識すべき３原則」と「サイバーセキュリティ経営の重要１０項目」の基本的な構成を維持しつつ、最新の状況への認識と対策の実践が可能となるよう、記載内容の見直しを行った。また、本ガイドラインと連携して用いることが可能なツールや関連ガイドラインなどが整備されたことを踏まえ、これらとの関係性の整理図を追加するなど、本ガイドラインを利用する企業の利便性を高めるための改良を行っている。

なお、本ガイドラインの Ver1.0、及び Ver1.1 は、経済産業省と独立行政法人情報処理推進機構（IPA）の共催である「サイバーセキュリティリスクと企業経営に関する研究会」、Ver2.0 と Ver3.0 は「サイバーセキュリティ経営ガイドライン改訂に関する研究会」においてそれぞれ検討が行われ、とりまとめたものである。Ver3.0 の策定にあたっては、機関投資家やサイバーセキュリティの専門家等へのヒアリングを行い、これからの企業に対して求められるセキュリティ対策等を把握した上で改訂を行った。

---

[1] 「中小企業の情報セキュリティ対策ガイドライン」の詳細については、付録 B（サイバーセキュリティ対策に関する参考情報）参照。

[2] ランサムウェアによる被害については、付録 E（用語の定義）の当該項目参照。

サイバーセキュリティ経営ガイドライン・概要

Ⅰ．企業リスクマネジメントの一部としてのサイバーセキュリティ

○ 企業活動の多くをデジタル環境に依存する現在、会社法の求める内部統制システムの構築や必要な体制の整備、コーポレートガバナンス・コードに基づく開示と対話等において、サイバーセキュリティに関するリスクを考慮しなければ実態に即したものにはならず、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ている。

○ 多様化するサプライチェーン上のサイバー攻撃の起点は広く拡散しており、大企業等と直接の取引がない中小企業であっても、サプライチェーンを通じた間接的なつながりがある全ての企業において、地政学リスク[3]や自然災害等のリスクに加えて、サイバー攻撃等によるリスクを考慮したリスクマネジメントが求められている。

○ 経営者は、組織の意思決定機関が決定したサイバーセキュリティ体制が当該組織の規模業務内容に鑑みて適切でなかったため、組織が保有する情報の漏えいなどにより会社や第三者に損害が生じた場合、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。さらに、被害が深刻な場合の事業停止や新たな脅威に対処するための予算措置等の経営判断も要求され、担当者への丸投げは許されるものではない。

○ 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）[4]と位置付けることが重要**である。直接的な収益を算出することは困難ではあるが、企業の価値を維持・増大していく上で、**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**であるとともに、サイバーセキュリティリスクを組織の経営リスクの一環として織り込み、その観点から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[5]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**である。

○ 本ガイドラインは、大企業及び中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要１０項目」をまとめたものである。

---

[3] 本書では、特定地域における紛争、武力行使、政情不安又は大規模災害等により、企業の事業活動におけるサプライチェーンや市場に影響が生じるようなリスクの意味で扱う。

[4] 投資の概念については、会計、経営等様々な領域で定義が異なる。ここでは、直接の利益（リターン）を期待するものではないが、将来的なリスクを抑制し、リスクと利益の総和においてプラスの結果をもたらすための手段という意味で用いている。

[5] リスク評価及びリスクの低減に関する具体的な対策例については「サイバーセキュリティ経営の重要 10 項目」のうち指示 4 を参照。なお、許容可能水準に関しては所属業界のガイドラインや取引先からの要請などを考慮する必要がある。

II. 経営者が認識すべき３原則

経営者は、以下の3原則を認識し、対策を進めることが重要である。

(1) 経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要

（経営者はリーダーシップをとってサイバー攻撃のリスクと企業への影響を考慮したサイバーセキュリティ対策を推進するとともに、企業の事業継続のためのセキュリティ投資を実施すべきである。）

(2) 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、自社のみならず、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

（自社のサイバーセキュリティ対策にとどまらず、在来形の部品調達などの形態や規模にとどまらないクラウドサービスの利用等のデジタル環境を介した外部とのつながりの全てを含むサプライチェーン全体を意識し、総合的なサイバーセキュリティ対策を実施すべきである。）

(3) 平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

（平時から社外の利害関係者（株主、顧客等）はもとより、社内の関係者（CIO 等セキュリティ担当者、事業担当責任者等）に事業継続に加えてサイバーセキュリティ対策に関する情報開示を行うことなどで信頼関係を醸成し、インシデント発生時にもコミュニケーションが円滑に進むよう備えるべきである。）

（詳細は後述の「２．経営者が認識すべき３原則」を参照）

III. サイバーセキュリティ経営の重要１０項目

経営者は、以下の重要10項目について、サイバーセキュリティ対策を実施する上での責任者や担当部署（CISO、サイバーセキュリティ担当者等）への指示[6]を通じて組織に適した形で確実に実施させる必要がある。これらは、単なる指示ではなく、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リスク対策に関する実施方針の検討、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含まれる。

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

指示２　：サイバーセキュリティリスク管理体制の構築

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

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

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

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

指示７　：インシデント発生時の緊急対応体制の整備

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

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

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

（詳細は後述の「３．サイバーセキュリティ経営の重要１０項目」を参照）

[6] この場合の「指示」は JIS Q 38500:2015（情報技術－IT ガバナンス）における指示と同義であり、IT ガバナンスを実践する意味で用いている。担当者に丸投げしてしまうことではなく、実践の結果を確認する責任を負う。

1．はじめに

1．1．サイバーセキュリティ経営ガイドラインの背景と位置づけ

(1) サイバーセキュリティを包含するリスクマネジメントの必要性

かつて、サイバーセキュリティはサイバー攻撃から自社の IT システムやそこで扱われる情報資産の保護を主たる目的として議論されてきた。しかしながら、企業活動の多くをデジタル環境に依存する現在、会社法の求める内部統制システムの構築や必要な体制の整備、コーポレートガバナンス・コードに基づく開示と対話等において、サイバーセキュリティに関するリスクを考慮しなければ実態に即したものにはならず、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[7]が求められている。

多様化するサプライチェーン上のサイバー攻撃の起点は広く拡散しており、上場企業等と直接の取引がない中小企業であってもサプライチェーン[8]を通じた間接的なつながりがある全ての企業において、サイバーセキュリティリスクを考慮したリスクマネジメントが求められている。

表　インシデント損害額の試算例[9]

インシデント種類	損害額	損害額内訳
大規模なマルウェア感染	3億7,600万円	・事故原因・被害範囲調査費用：1億円 ・従業員端末・サーバー等の入れ替え費用：1.42億円 ・再発防止費用：5,000万円 ・利益損害：8,400万円（休止中に得られたはずの売上）
ECサイトからのクレジットカード情報等の漏えい	9,490万円	・事故対応費用：2,890万円（再発防止策導入含む） ・利益損害：3,000万円（休止中に得られたはずの売上） ・賠償損害：3,600万円（損害賠償請求額）
軽微なマルウェア感染	600万円	・事故原因・被害範囲調査費用：500万円 ・再発防止策：100万円

本ガイドラインはこうした状況変化を踏まえ、経営者のリーダーシップの下で、サイバーセキュリティに関わるリスクを把握・評価した上で、適切なリスク対応の実施を通じて

---

[7] 米国においても、国立標準技術研究所（NIST）が同様の目的の文書を公表している。
NISTIR 8286 "Integrating Cybersecurity and Enterprise Risk Management (ERM)"
https://csrc.nist.gov/publications/detail/nistir/8286/final
また、経済産業省では「コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」を「情報セキュリティガバナンス」と定義している。
https://www.meti.go.jp/policy/netsecurity/secgov-concept.html

[8] 本ガイドラインにおいて、サプライチェーンには製造業における部品調達のような関係のみならず、クラウドサービスなど外部のデジタルサービスの利用や、API（アプリケーションプログラムインタフェース）を介したシステム同士の連携など、デジタル環境を通じた多様かつ非定型の企業間のつながりも含む。

[9] 『インシデント損害額調査レポート 2021』（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）より引用
https://www.jnsa.org/result/incidentdamage/2021.html

残留リスク[10]を許容範囲以下に抑制する等、企業に求められる社会的要請に応えるための適切な投資と対策の実践を促すことを目的として提供されるものである。

(2) 本ガイドラインの対象者と責任

本ガイドラインは、経営者(企業の代表者として、統括責任を負う者(CEO))、さらに経営者から指示を受け、サイバーセキュリティ対策の実践に関する責任を負う者(CISO 等)を第一義的読者として想定している。このほか、サイバーセキュリティ対策の実践にあたって経営者や CISO 等を直接補佐する実務者による利用も考慮する。

経営者は、組織の意思決定機関が決定したサイバーセキュリティ体制が当該組織の規模業務内容に鑑みて不十分なことに起因して、組織が保有する情報の漏えいなどにより会社や第三者に損害が生じた場合、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。

このほか、企業経営の実務上では次のような判断を求められることから、CISO 等の担当者へのいわゆる「丸投げ」は許されない。サイバーセキュリティ対策を指示するだけではなく、定期的に実施状況等を確認するなど、日頃から判断に必要な情報を得ておく必要がある。

- **被害が深刻な場合の経営判断**: サイバー攻撃の深刻度によっては事業の全体又は一部を中断せざるを得ない場合があり、経営トップが状況に応じて適切な判断を下すことが求められる。
- **リスクの変化への対応に関する経営判断**: 財務、防災などのリスクと異なり、サイバーセキュリティリスクは変化のスピードが速く、突発的かつ避けられない対策の見直しとそのための予算措置が必要となる場合がある。

(3) 本ガイドラインで想定する企業

本ガイドラインは、大企業及び中小企業(小規模事業者を除く)[11]を想定した記述を行っている。なお、国家の安全保障を経済面から確保するという経済安全保障の重要性が増していること等を踏まえ、経済安全保障上の脅威については、サプライチェーンへの影響や社会的責任等の観点から、読者において別途考慮していく必要がある。

---

[10] 付録 E 参照。各種のリスク対策を実施した後でなお発生可能性のあるリスクのこと。

[11] デジタル技術を活用する企業、デジタル・トランスフォーメーション(DX)を進める企業やデジタル環境(基幹情報システム、工場内の制御システム、製品、サービス等)を介した外部とのつながりの全てを含むサプライチェーンに繋がる企業であれば、企業規模を問わず、サイバーセキュリティリスクを考慮することが求められるが、本ガイドラインにおいてあらゆる企業規模に対応した記述を行うことが困難であるため、大企業及び中小企業(小規模事業者を除く)を想定した記載としている。

(4) 本ガイドラインの位置付け

本ガイドラインは、コーポレートガバナンス及びエンタープライズリスクマネジメントを対象とする各種ガイドラインやフレームワークとの間に、次のような関係を有する。また、リスク対応に関する情報開示や体制構築など具体的な取組において、図中に示す各種のツール等を利用することが可能である。

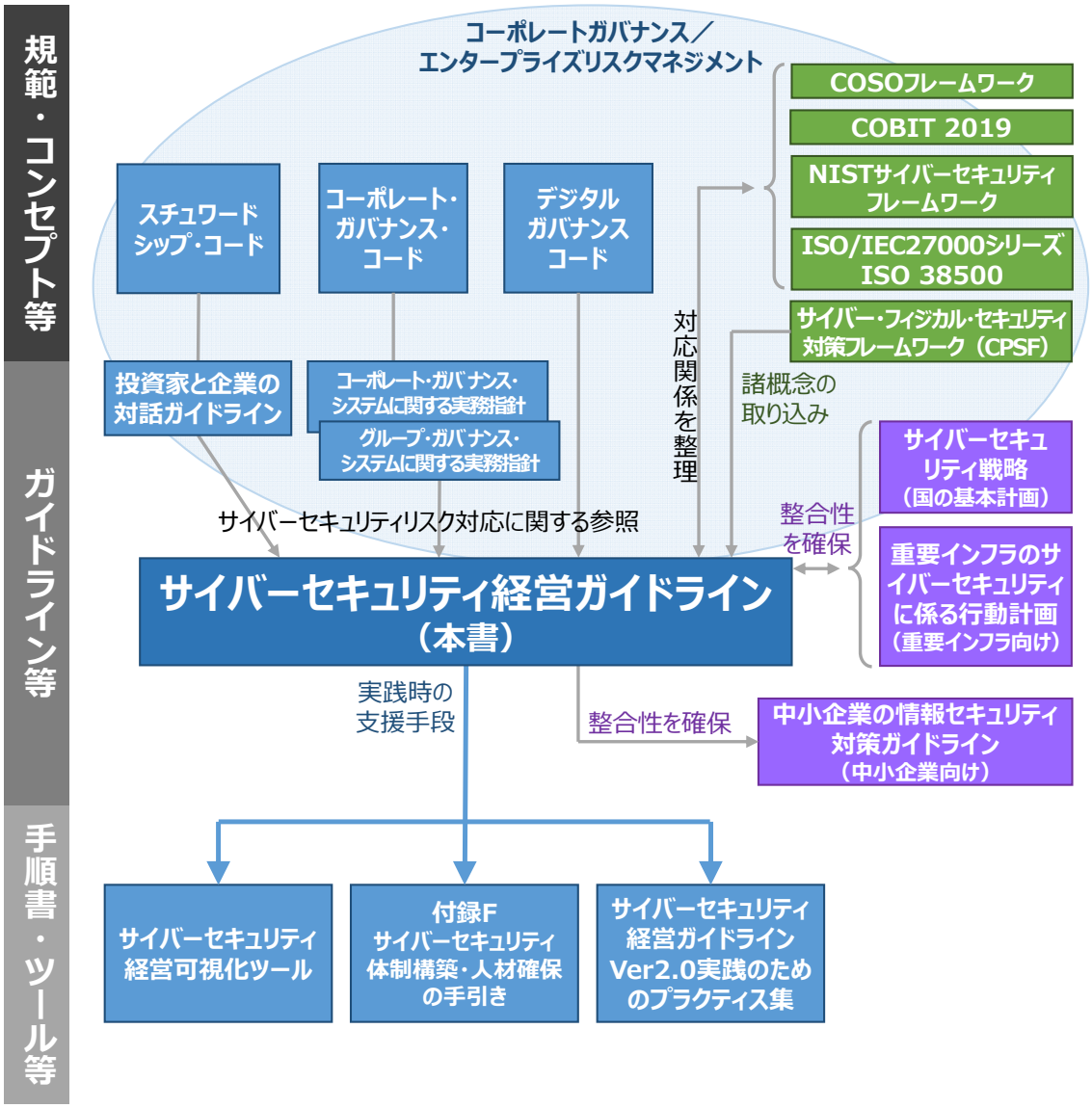

図 1　サイバーセキュリティ経営ガイドラインの体系

１．２．本ガイドラインの構成と活用方法

本ガイドラインは、以下の構成となっている。巻頭の概要は経営者向け、2章～3章はサイバーセキュリティ対策を実施する上での責任者である担当幹部（CISO 等）及びセキュリティ担当者向けである。

サイバーセキュリティ経営ガイドライン・概要
1．はじめに
2．経営者が認識すべき3原則
3．サイバーセキュリティ経営の重要10項目
付録
A) サイバーセキュリティ経営チェックシート
B) サイバーセキュリティ対策に関する参考情報
C) サイバーセキュリティインシデントに備えるための参考情報（別紙）
D) 関連する規格・フレームワーク等との関係（別紙）
E) 用語の定義
F) サイバーセキュリティ体制構築・人材確保の手引き（別冊）

経営者においては、最低限、巻頭の概要に目を通した上で、3原則を認識し、重要10項目について CISO 等に指示をしつつ、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必要である。

CISO 等は、経営者の指示に基づき、重要10項目の各解説ページの「対策例」も参考にしつつ、セキュリティ対策の取組みを、セキュリティ担当者に対してより具体的に指示をし、推進することが必要である。さらに、経営者に対して適宜状況報告を行うことを通じて、経営者が適切な判断を行うために必要な情報を提供しなければならない。

また、本ガイドラインでは、重要10項目の実施にあたって、参考となる情報を付録として提示している。各付録の内容は以下のとおりである。

付録 A　重要10項目が適切に実施されているかどうかを確認するためのチェックシート
付録 B　サイバーセキュリティ対策を実施する上で参考となる資料等
付録 C　インシデント発生に備えて、経営者及び組織内で整理しておくべき事項
付録 D　重要10項目と各種規格やフレームワーク等が規定する内容との関係性
付録 E　本ガイドラインで使用している用語の定義
付録 F　指示 2 と指示 3 に関する具体的な実践のための手引き書

なお、内部犯行による情報漏えい等のリスクへの対処については、必要に応じ、「組

織における内部不正防止ガイドライン」（IPA）[12]を参照することで、より効果的な対策が可能となる。

また、サイバーセキュリティ対策にこれから取り組む企業においては「中小企業の情報セキュリティ対策ガイドライン」（IPA）も参考となる。

[12] 組織における内部不正防止ガイドライン（IPA） https://www.ipa.go.jp/security/fy24/reports/insider/

２．経営者が認識すべき３原則

経営者は、以下の3原則を認識し、対策を進めることが重要である。

（1）経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要

（解説）

- ビジネス展開や企業内の生産性の向上のためのデジタル活用に限らず、制御系環境のリモート管理、IoT デバイスの活用、社外とのオンラインでのコミュニケーション、商取引、協業等、企業の事業活動におけるデジタル環境への依存度が増大している。このような中、サイバー攻撃による事業活動への影響の可能性も増大かつ深刻化しており、サイバーセキュリティ対策は企業活動におけるコストや損失を減らすための必要不可欠の投資であるとともに、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、経営者としての責務である。
- また、サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった場合には、人命への影響や法令違反が発生する可能性があるため、企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。
- このため、サイバーセキュリティリスクを多様な経営リスク（例：自然災害、地政学的事象、為替や原料価格の変動　等）の中での一つとして位置づけ、サイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）を任命するとともに、経営者自らがリーダーシップを発揮して自社の組織や事業におけるリスクを把握した上で、それに応じた対策の推進を主導することが必要である。

（2）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、自社のみならず、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

（解説）

- デジタル技術の業務利用が普及した環境において、サプライチェーンには在来形の部品調達などの形態や規模にとどまらない、クラウドサービスやモバイルデバイスの利用、情報を扱う機器の保守や情報を記録した媒体の廃棄のような、デジタル環境を介した外部とのつながりの全てが含まれ、かつこれらのつながりは時と共に刻々と変化するなど非定型である。
- サプライチェーンとしてつながる国内外の拠点、ビジネスパートナーやシステム管理等を含むあらゆる委託先等においてサイバー攻撃への対策が不十分

であった場合、それらのセキュリティが弱い組織を踏み台にしたサイバー攻撃による重要情報の流出等、サプライチェーン全体の機能が停止するのみならず、自社にも甚大な被害をもたらす等の問題[13]が生じうる。また、自社の対策不十分が原因である場合、自社がサプライチェーンの他企業にとっての加害者の立場になる。

・ このため、自社のみならず、サプライチェーンの国内外のビジネスパートナーやシステム管理等を含むあらゆる委託先等、サプライチェーンの一端を担う企業として全体を意識し、総合的なセキュリティ対策を徹底することが必要である。非定型のつながりの中で自社のリスクを低減し、顧客や社会からの信頼を得るためには、つながりをもつサプライチェーン全体のリスクを下げる必要があり、対策の推進はサプライチェーンに参加する企業規模を問わない全ての企業の経営者の責務である。

（3）平時及び緊急時のいずれにおいても、サイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

（解説）

・ 万一サイバー攻撃による被害が発生した場合、関係者と平時から適切なセキュリティリスクのコミュニケーションができていれば、関係者の不信感の高まりを抑えることができる。このときの関係者には、社内であれば CISO 等のセキュリティ担当者のみならずセキュリティ対策を実施すべき担当者等を含み、社外ではサイバーセキュリティ関連情報を扱う IPA、JPCERT/CC、商工会議所等などはもちろん、セキュリティ関連製品・サービスの事業者等を含む。

・ このため、関係者に対して、平時からサイバーセキュリティリスクや対策に関する気づきや課題の共有などのコミュニケーションを積極的に行うことが必要である。このようなコミュニケーションの仕組みがインシデント発生時には連絡体制として機能することで、迅速な報告や状況把握が可能となり、インシデントへの初動対応を早めるほか、外部関係者への円滑な説明の実現にもつながる。

[13] サイバーセキュリティに起因する被害例については付録 B（サイバーセキュリティ対策に関する参考情報）参照。

３．サイバーセキュリティ経営の重要１０項目

経営者は、以下の重要10項目について、CISO 等への指示を通じて組織に適した形で確実に実施させる必要がある。これらは、単に指示すればよいのではなく、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求められる。

自組織での対応が困難又は専門事業者による実施が適切と判断される取組については、その一部を外部委託によって実施することも検討する。

＜経営者がリーダーシップをとったセキュリティ対策の推進＞

（サイバーセキュリティリスクの管理体制構築）

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
指示２　サイバーセキュリティリスク管理体制の構築
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

（サイバーセキュリティ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
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
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

（インシデント発生に備えた体制構築）

指示７　インシデント発生時の緊急対応体制の整備
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

＜サプライチェーンセキュリティ対策の推進＞

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

＜ステークホルダーを含めた関係者とのコミュニケーションの推進＞

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

３．１．サイバーセキュリティリスクの管理体制構築

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

- サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針（セキュリティポリシー）を策定させる。
- 策定した対応方針を対外的な宣言として公表させる。

対策を怠った場合のシナリオ

・経営者がサイバーセキュリティリスクを経営リスクとして認識していないと、事業の中断など経営判断が求められる場合に必要な意思決定がなされず、結果的に被害の拡大を招くおそれがある。

・サイバーセキュリティリスクへの組織全体での対応方針が策定されないと、組織内での対応が一貫したものとならない。

・対応方針（セキュリティポリシー）を形式的に策定するのみでは、組織内での対応の責任が明確にならないため、リスク対応による効果が期待できない。

・企業として対応方針を宣言することにより、ステークホルダー（株主、顧客及び取引先など）の信頼性を高め、ブランド価値向上につながる。宣言がない場合には、企業におけるサイバーセキュリティ対策の重要度がステークホルダーに伝わらず、信頼性を高める効果が得られない。

対策例

・経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取ったセキュリティポリシーを策定する[14]。その際、製造、販売、サービス等、事業が立脚している全ての基盤（設備、システム、情報等の資産、流通プロセス等）に影響を及ぼすと考えられるサイバーセキュリティリスクに応じた対応方針を検討する。

・セキュリティポリシーは従業員が容易にアクセス可能な場所（社内ポータルサイト等）への掲載、従業員教育を実施するなどによって周知徹底を図る。

・セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示し、信頼性を高める。

・策定及び公開したセキュリティポリシーに基づき、サイバーセキュリティリスクの変化に対応した対策が持続的に実施されているかを指示６で扱う PDCA サイクルで定期的に把握し、組織として継続的な改善に取り組む。

[14] セキュリティポリシーの策定方法については、付録 B（サイバーセキュリティ対策に関する参考情報）参照。

指示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の管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構築させる。**
- **サイバーセキュリティリスクの管理体制の構築にあたっては、組織内のガバナンスや内部統制、その他のリスク管理のための体制との整合を取らせる。**

対策を怠った場合のシナリオ

・サイバーセキュリティリスクの管理体制を整備していない場合、責任の所在があいまいとなり、適切な対策が講じられず、かつ、インシデント発生時の被害が拡大する。

・組織内におけるその他のリスク管理体制との整合を取らないと、組織全体としてのリスク管理の方針と不整合が生じるおそれがある。

対策例

・サイバーセキュリティ対策のための人材確保・育成にあたっては、付録 F（別冊）として示す「サイバーセキュリティ体制構築・人材確保の手引き」の内容を参考にする。

・重要インフラに関わる企業に対しては、経営層、CISO、戦略マネジメント層、システム担当者の役割と責任に基づく、組織一丸となった対応が求められていることなどを踏まえ、自社の実態に応じた役割と責任割当に基づく体制を構築する。

・内部統制を機能させる観点から、サイバーセキュリティ対策の有効性や報告に関する信頼性確保等の目的達成を保証するための役割を体制内で明確化する。

・CISO 等は、組織内の全ての事業領域を包含したサイバーセキュリティリスク管理体制を構築し、それぞれの役割における責任範囲を明確にする。

・CISO 等が、組織内に設置された経営リスクに関する委員会に参加する。

・取締役、監査役はサイバーセキュリティリスク管理体制が適切に構築、運用されているかを監査する。

・役割遂行に求められる責任や専門性、人的資源の状況に応じて、組織内要員で対応すべきものと外部の専門サービスに委託すべきものとの切り分けを行う。

・グローバル展開する企業において、組織内のその他のリスク体制との整合を検討するにあたり、NIST IR 8286（8 ページの脚注参照）の内容を考慮する。

・セキュリティバイデザインの観点を踏まえて、企画・設計段階からサイバーセキュリティ対策を考慮した開発・運用体制を構築する。

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

- **サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討させ、その実施に必要となる資源（予算、人材等）を確保した上で、具体的な対策に取り組ませる。**
- **全ての役職員に自らの業務遂行にあたってセキュリティを意識させ、それぞれのサイバーセキュリティ対策に関するスキル向上のための人材育成施策を実施させる。**

対策を怠った場合のシナリオ

・適切な予算確保が出来ていない場合、組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、信頼できる外部のベンダへの委託が困難となるおそれがある。

・適切な処遇の維持、改善ができないと、サイバーセキュリティ対策に関する有用なスキルを備えた人材の確保が困難となり、自社にとどめておくことができない。

対策例

・サイバーセキュリティ対策のための人材確保・育成にあたっては、付録 F（別冊）として示す「サイバーセキュリティ体制構築・人材確保の手引き」の内容を参考にする。

・事業が立脚している全ての基盤の安全性の担保のために必要なサイバーセキュリティ対策を明確にし、それに要する費用を確保する。

・従業員向けやセキュリティ担当者向けなどの研修等のための予算を確保し、継続的に役割に応じたセキュリティ教育を実施する。

・セキュリティ対策業務に従事する人材のみならず、デジタル部門、事業部門、管理部門等のあらゆる業務に従事する人材に、「プラス・セキュリティ」知識・スキルの習得を促す。

・サイバーセキュリティに関する高度な専門性を有する人材を組織内で確保することが困難な場合は、専門ベンダの活用を検討する。

・組織内の IT 人材育成の戦略の中で、外部人材の採用も含めた社内のセキュリティ人材育成[15]、キャリアパスを設計検討する。

・自組織においてセキュリティ分野の教育・トレーニング等の実施が困難な場合は、外

[15] (参考)セキュリティ人材が有するスキルを測る指標の一つとして、民間企業が提供する専門資格や IPA が実施している情報処理安全確保支援士制度などを活用することも有効である。

部の組織が提供するセキュリティ研修[16]等の活用などを検討する。

[16] (参考)社会インフラ・産業基盤事業者の情報・制御システム関連業務に係わるセキュリティ人材を育成する事業（産業サイバーセキュリティセンター）も IPA にて提供している。

３．２．サイバーセキュリティ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、サービス及び情報を特定させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。
- サイバー保険の活用や守るべき情報やデジタル基盤の保護に関する専門ベンダへの委託を含めたリスク対応計画を策定させ、対応後の残留リスクを識別させる。

対策を怠った場合のシナリオ

・サイバーセキュリティリスクは企業の事業内容や組織形態によって異なる。自社のサイバーセキュリティリスクのアセスメントを行うことなく、他社の事例やベンダからの提案などを参考に実態にそぐわないリスク対応計画を策定した場合、未対策のリスクによる事業の中断や機密情報の漏えいなど、経営上許容できない損失が発生するおそれがある。

・同様に、「厳し目の対策を定めればリスクは抑えられる」として、リスク対応計画を自社の事業への影響を考慮せずに策定すると、通常の業務遂行に支障をきたすなどの不都合が生じるおそれがある。

対策例

・組織における情報のうち、経営戦略の観点から守るべき情報を特定し、それらがどこに保存され、どこで扱われているかを把握する。その際、自社の営業秘密を外部のクラウドサービスで管理したり、テレワーク等の新しい働き方を導入したりしていることの影響を適切に反映させる。

・守るべき情報やシステムに対して、発生しうるサイバーセキュリティリスクについて、自社のビジネスモデルや利用している技術に応じたリスクアセスメントにより把握する。リスクアセスメントの実施にあたっては、自社の事業内容や特徴に応じて、次に例示するようなアプローチから適切な方法を用いる。

－リスクの洗い出し
　例：守るべき情報やシステムの特定や把握。自社での過去の事故事例や、類似する他社事例の分析のほか、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なども活用

－リスクが顕在化する条件の検討
　例：情報の利用場面（テレワーク等）による相違、多層防御の有効性の評価

－リスクの特徴の分析
　例：発生頻度と影響の大きさのランク付け

－リスクの定量化（可能なものについて）
例：経営戦略上重要な営業秘密の流出による損害額試算

・把握したリスクに対して、実施するサイバーセキュリティ対策を以下の観点で検討する。
－リスク低減策の実施（リスクの発生確率を下げる対策）
例：重要な情報へのアクセス制御、ソフトウェア更新の徹底
－リスク回避策の実施（リスクが発生する可能性を除去する対策）
例：個人所有端末へのデータ保存の禁止（外部での情報漏えいのリスクを回避）
－リスク移転策の実施（リスクを他社等に移す対策）
例：クラウドサービスの利用、サイバー保険の加入[17]

・リスクの把握及び対策の検討にあたっては、付録 B に示す「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）」及び「サイバーセキュリティ経営可視化ツール」等を参照し、事業活動に影響を及ぼす可能性のあるリスク源（例：CPSF の添付 B に記載されている「システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染、正規ユーザによる内部不正」等）を適切に捉え、検討すべきセキュリティ対策を漏れなく把握する。

・サイバーセキュリティリスクの把握にあたっては、自組織のみならず、サプライチェーン全体を通じたリスクを対象とするとともに、サイバー攻撃以外のリスクとして偽情報、機械学習における誤判断、海外での法令違反等も考慮する[18]。

・リスクの発生確率や、発生したときの損害等を考慮して、サイバーセキュリティ対策の実施が不要又は困難と判断したリスクについては残留リスクとして識別する。

・法令上、安全管理措置が義務づけられている情報については、法令上の取り扱いも考慮したリスクの特定と緊急時に速やかに情報の保護が行えるような対策となっているかも検討する。

・製品・サービス等において、セキュリティバイデザインの観点を踏まえて企画・設計段階からサイバーセキュリティ対策を考慮する。

・リスクマネジメントは脅威の変化に応じて不断の見直しを要求するものであり、自組織におけるリスクとその対応方策が形骸化していないか、定期的な確認を行う。

[17] クラウドサービスの利用及びサイバー保険の加入のいずれも、自社が負うリスクをゼロにするものではなく、それぞれの効果と責任範囲を把握した上で実施を検討する必要がある。

[18] サイバーセキュリティに関する最新情報の収集方法については、付録 B（サイバーセキュリティ対策に関する参考情報）参照。

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

- サイバーセキュリティリスクに対応するための保護対策として、防御・検知・分析の各機能を実現する仕組みを構築させる。
- 構築した仕組みについて、事業環境やリスクの変化に対応するための見直しを実施させる。

対策を怠った場合のシナリオ

・指示4を通じて明らかにされたサイバーセキュリティリスクに応じた適切な対策が行われていない場合、サイバー攻撃を防げず、発生した場合の事業継続に影響する可能性があるのみならず、個人情報の漏えいや他社に対するサイバー攻撃への発展など社会全体に影響を与え被害が拡大する可能性がある。

・技術的な取組を行っていたとしても、攻撃の検知・分析とそれに基づく対応ができるよう、適切な運用が行われていなければ、サイバー攻撃の状況を正確かつ適時に把握することができず、攻撃者に組織内の重要情報を窃取されるなどの、致命的な被害に発展するおそれがある。

・働き方の多様化への対応等、自組織のデジタル環境の見直しの結果、クラウドサービスへの移行や、ゼロトラストモデルの採用などの変更を行っても、インシデントの予兆を検知する仕組みが従来どおりのままでは見逃しや対応の遅れが生じてしまう。

対策例

・重要業務を行う端末、ネットワーク、システム又はサービス（クラウドサービスを含む）には、多層防御を実施する。
　－必要に応じてスイッチやファイアウォールなどでネットワークセグメントを分離し、別のポリシーで運用する。
　－脆弱性診断等の検査を実施して、システム等の脆弱性の検出、及び対処を行う。
　－営業秘密や機微性の高い技術情報、個人情報などの重要な情報については暗号化や電子署名など、情報を保護する仕組みや、改ざん検知の仕組みを導入する[19]。
　－ゼロトラストモデルに基づく対策を講じる際には、境界防御の効果が期待できないことを踏まえた認証等の強化を図るとともに、インシデントの予兆の段階で即時の検知と対象ができるような仕組みや体制を整備する[20]。
　－クラウドサービスを利用する際には、クラウドサービスにおいて提供されるセキュリティ機能を考慮した選定を行い、それらの機能を活用するとともに、アクセス制限

[19] 対策としての暗号化の有効性を担保するためには、付録Ｅ（用語の定義）における関連用語参照のこと。
[20] 自組織のみで仕組みや体制の整備が難しい組織の場合、これらを支援する『サイバーセキュリティお助け隊』等の中小企業向け施策を活用することが考えられる。詳細については付録Ｂ（サイバーセキュリティ対策に関する参考情報）を参照のこと。

などの設定やアカウントの管理などが適切に維持・管理されるようにする[21]。

・自社内で対策実施に必要なスキルを有する人材を確保できない場合は、専門の情報セキュリティサービス等を提供する外部事業者を活用する。
  ー一定の品質を備えたサービスの選定には、IPA が公表している「情報セキュリティサービス基準適合サービスリスト」[22]を利用することができる。
  ーサービスを外部委託する場合でも、脆弱性診断や監視サービス等の提供事業者からの報告内容を適切に理解し、対策に反映するスキルを備えた人材が必要となることを認識し、必要な人材の確保・育成に取り組む必要がある。

・サイバーセキュリティリスクによりシステムが停止した場合に、業務を止めないための計画（BCP）を策定し、バックアップの取得や代替手段の整備等を行う。

・従業員に対する教育を定期的に行い、適切な対応が行えるよう日頃から備える。

[21] クラウドサービスの対策に関しては、付録 B（サイバーセキュリティ対策に関する参考情報）参照。
[22] 情報セキュリティサービス基準適合サービスリスト https://www.ipa.go.jp/security/it-service/service_list.html

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

- リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえた PDCA サイクルを運用させる。
- 経営者は対策の状況を定期的に報告させること等を通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる。
- 株主やステークホルダーからの信頼を高めるため、改善状況を適切に開示させる。

対策を怠った場合のシナリオ

・PDCA（Plan[計画]、Do[実行]、Check[実施状況の確認・評価]、Act[改善]）を適切に実施する体制が出来ていないと、最初に計画した内容のまま、新たな脅威への対応ができない等、リスクの変化に応じた改善が図られないおそれがある。

・定期的な報告等を受けておらず、経営者自身がリスクや問題を把握できていない場合、適切なセキュリティ対策が実施されず、サイバー攻撃を受けるおそれがある。

・サイバーセキュリティリスクを対象とする PDCA サイクルは、自然災害や機器故障等のリスクと比較してリスクが急激に変化することがある点に特徴があり、それ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運用しないと、有効な対策を講じることができない。

・継続的な改善を行わなければ、新たなリスクによるインシデント発生を通じて企業価値を損なう可能性が高まる。そのほか、改善に関する取組状況の適切な開示を行わない場合も、企業としての社会的責任の観点から、事業のサイバーセキュリティリスク対応についてステークホルダーの信頼を失うおそれがある。

対策例

・サイバーセキュリティリスクの変化に継続的に対応するための PDCA プロセスとその実施体制を整備する。
  －Plan の過程において、指示4における最新のリスク対応計画が反映されるようにする。
  －Check の実施にあたっては、「付録 A」及び「サイバーセキュリティ経営可視化ツール」を確認項目の参考として利用するとともに、実施している対策が現在のリスクに対して有効かどうかの評価も行う。

・PDCA プロセスの検討にあたっては、リスクの特徴に応じて自組織のみならず製品ベンダ等の関係者を含めた形で作成することに留意する。

・必要に応じて、ISO/IEC 27001 規格に基づく ISMS など、国際標準となっている

PDCA マネジメントシステムの認証を活用する。

・サイバーセキュリティリスク管理に関する KPI を定め、組織内の経営リスクに関する委員会においてその状況を経営者に報告する。KPI としては、リスク対応に関する組織内パフォーマンスの評価の観点から、次に例示するような指標が考えられる。
－対策をしなかった場合の被害額
－サイバーセキュリティに関わる原因によるサービス中断時間
－サイバーセキュリティ研修の受講率
－サイバーセキュリティ対策に従事する要員のスキルの自己評価平均値
－自組織におけるセキュリティ成熟度の自己評価平均値

・必要に応じて、目的に応じた脆弱性診断やペネトレーションテスト、情報セキュリティ監査等の外部サービス[23]を利用し、現状のシステムやサイバーセキュリティ対策の問題点を検出し、改善を行う。

・新たなサイバーセキュリティリスクの発見等により、追加的に対応が必要な場合には、速やかに対処方針を修正する。

・サイバーセキュリティ対策の状況について、サイバーセキュリティリスクの性質・度合いに応じて、情報セキュリティ報告書、CSR 報告書、サステナビリティレポートや有価証券報告書等への記載を通じた公表、又はサプライチェーン関係者への個別の開示等に取り組む。

[23] 外部サービスの選定にあたっては、独立行政法人情報処理推進機構が公表する「情報セキュリティサービス基準適合サービスリスト」を利用することで、一定の品質が確保されたサービスを選定することができる。
https://www.ipa.go.jp/security/it-service/service_list.html

３．３．インシデント発生に備えた体制構築

指示７　インシデント発生時の緊急対応体制の整備

- 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、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）を整備させる。
- 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。
- インシデント発生時の対応について、適宜実践的な演習を実施させる。

対策を怠った場合のシナリオ

・緊急時の対応体制を整備していないと、原因特定のための調査作業において、組織の内外の関係者間のコミュニケーションが取れず、速やかな対処ができない。

・速やかな情報開示が行われない場合、顧客や取引先等にも被害が及ぶおそれがあり、損害賠償請求など責任を問われる場合がある。

・法的な取り決めがあり、所管官庁等への報告が義務づけられている場合、速やかな通知がないことにより、罰則等を受ける場合がある。

・演習を実施していないと、不測の事態が起こった際に、担当者が緊急時に適切な行動をとれず、早期の収拾が困難になるばかりでなく、被害の拡大や影響の長期化を招くおそれがある。

対策例

・緊急時において、被害を最小限に抑えるための迅速対応の態勢を確立するため、以下を実施できるような対応体制（CSIRT）を構築する。

－インシデント対応体制の構築にあたっては社外からもしくは社外への波及等への対応についても意識する必要があり、高度にネットワーク化されるサプライチェーンにおいては、社外との多様なつながりの全てについて考慮する必要がある。

－インシデントの発生が懸念される場合に、経営者ほか関係者に速やかな報告を行えるようにする。

－サイバー攻撃による被害を受けた場合、被害原因の特定及び解析を速やかに実施するため、速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築するとともに、関係機関との連携による調査が行えるよう指示する。また、インシデントの原因調査にあたっては「付録Ｃ サイバーセキュリティインシデントに備えるための参考情報」も参考にすることができる。

－インシデント収束後の再発防止策の策定、所管省庁等への報告手順も含めて演

習を行う。

－緊急対応体制の検討にあたっては、必要に応じて外部の専門家の知見も活用することも検討する。

－緊急連絡網（システム運用、セキュリティベンダなどの連絡先）、社外を含む情報開示の通知先一覧を整備し、対応に従事するメンバーに共有しておく。

－初動対応時にはどのような業務影響が出るか検討し、緊急時に組織内各部署(総務、企画、営業等）が速やかに協力できるようあらかじめ取り決めをしておく。

－関係法令を確認し、法的義務が履行されるよう手続を確認しておく。

－インシデントに関する被害状況、他社への影響等について経営者に報告する。

・自社で設計・開発・製造・提供等を行う製品やサービスについて、それらを構成するソフトウェア等における脆弱性や障害により顧客に不利益をもたらす状況の発生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の発信等の対応を行う PSIRT[24]の構築及び運用を行う。

・インシデント発生時の体制整備、ルール整備に当たって、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」[25]を参照しながら、社内理解を深める。

・インシデントの発生を想定した緊急対応に関する演習を役員や職員に対して定期的に実施し、緊急時にどのような手順で初動対応を行うべきかについて、全ての関係者が体験を通じて理解する。

－演習の対象は情報系のインシデントに限らず、制御系に影響が及ぶようなインシデントも含める。

－インシデント以外で企業活動に影響をもたらす可能性のある事業（システム移行等）についても演習の実施も考慮する。

－自社内に限定せず、企業間をまたがった演習の実施も考慮する。

－演習でどのようなことを実施すればよいかの知見が社内で得られない場合は、演習を含む社外のトレーニングコース等を活用する。

[24] ここでは製品を対象とする組織として PSIRT（Product Security Incident Response Team）を示しているが、このほか対象別に FSIRT（工場（Factory）を対象とするもの）、DSSIRT や SSIRT（デジタルサービス（Digital Service）を対象とするもの）等があり、自組織の事業内容に応じたサイバーセキュリティインシデント対応組織の構築・運用を検討することが適切である。

[25] 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の詳細については、付録 B（サイバーセキュリティ対策に関する参考情報）参照。

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

- インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。
- 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させる。
- 業務停止等からの復旧対応について、対象を IT 系・社内・インシデントに限定せず、サプライチェーンも含めた実践的な演習を実施させる。

対策を怠った場合のシナリオ

・重要な業務が適切な時間内に復旧できないことで、顧客における重大な被害、さらには自社の経営に致命的な影響を与えるおそれがある。

・業務のデジタル環境へ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がある。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とれたデジタル環境の復旧計画及び体制を整える必要がある。

・演習を実施していないと、不測の事態が起こった際に、担当者が緊急時に適切に行動することが出来ない。

対策例

・業務停止等に至った場合に、以下を実施できるような復旧体制を構築する。

－サイバー攻撃により業務停止に至った場合、速やかに復旧可能とするため、復旧にあたって再発を防ぐための確認事項や、具体的な復旧手順を復旧計画としてあらかじめ定めておくとともに、関係機関との間で復旧時の協力体制について協議しておく。

－重要な業務をいつまでに復旧すべきかの目標について、組織全体として整合をとる（例えば BCP で定めている目標との整合等）。

・設備投資計画を立案する際に、事業継続に影響をもたらす要因として、自然災害やパンデミック等にサイバーセキュリティリスクを加え、その対策を要求仕様等に反映させる。

・定期的な復旧演習の実施により、復旧対応に関わる関係者がその手順について、体験を通じて理解する。

－演習の対象は情報系のインシデントに限らず、制御系に影響が及ぶようなインシデントも含める。

－インシデント以外で企業活動に影響をもたらす可能性のある事業（システム移行等）

についても演習の実施も考慮する。

－自社内に限定せず、企業間をまたがった演習の実施も考慮する。

－演習でどのようなことを実施すればよいかの知見が社内で得られない場合は、演習を含む社外のトレーニングコース等を活用する。

※なお、指示7及び指示8にて、演習の実施について言及しているが、それぞれ個別に実施するか、まとめて実施するかについては演習内容や組織の関係者の役割を踏まえて検討することが適切である。

３．４．サプライチェーンセキュリティ対策の推進

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

- サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた対策状況の把握を行わせる。
- ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。

対策を怠った場合のシナリオ

・自社の国内外拠点、系列企業やサプライチェーンの国内外ビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないと、これらの企業を踏み台にして自社が攻撃されることもある。その結果、他社の2次被害を誘発し、加害者となるおそれもある[26]。また、緊急時の原因特定などの際に、これらの企業からの協力を得られないことにより事業継続に支障が生ずる。

・システム管理などの委託業務において、自組織で対応する部分と委託する部分の境界が不明確となり、対策漏れが生じるおそれがある。

・クラウドなどの外部サービスを利用したり、自社システムとAPI連携で他社のシステムが接続されたりするなど、企業間の繋がり方は多様化している。このような状況において、従来の受発注関係におけるセキュリティ対策のように、相手に提供する情報の保護を要求するのみでは、サプライチェーン由来のサイバーセキュリティリスクへの対策として不十分である。

・委託先選定に際して地政学リスクや自然災害等のリスクを考慮しなかった結果、想定外の事業停止に追い込まれる。

対策例

・業界毎の事情やサプライチェーン内での役割分担、相手先の対応能力等の状況に応じて、以下に例示するような対策を実践する。

－サプライチェーンに参加する企業の合意のもと、それぞれの企業が実施すべき対策を定め、監査又は自己点検等の実施を通じてその実効性を担保する。

－契約書においてサイバーセキュリティ対策の責任主体を明確化するなどの工夫により、各社が自ら担うべき役割を理解し、対策漏れが生じないようにする。

[26] 加害者とならないための対策については、付録B（サイバーセキュリティ対策に関する参考情報）参照。

－相手先の定める約款で規定されているサイバーセキュリティ対策の変更ができない場合に、その約款を適用した場合の自社における残留リスクが許容範囲以下となることを確認した上で調達又は契約する。
－サプライチェーン内で扱う情報の機密性や重要性のランク別に実施すべき対策を定め、過剰な対策や対策の形骸化が生じないようにする。
－サプライチェーン内でのサイバーセキュリティリスクに関する情報共有等を行う。

・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委託先等がSECURITY ACTION[27]を実施していることを確認する。なお、ISMS 等のセキュリティマネジメント認証を取得していることがより効果的である[28]。
・委託先選定にあたっては、コストや体制、技術力のみでなく、環境リスク（自然災害やパンデミック等）、地政学リスク（テロや政治的な不安等）及び経済リスク（経済危機や原料の価格変動等）の影響を考慮する。
・サプライチェーン上での対策の底上げの手段として、サイバーセキュリティお助け隊[29]等の中小企業向け施策を活用する。
・緊急時に備え、委託先に起因する被害に対する補償手段の確保として、委託先に対してサイバー保険[30]への加入を推奨する。
・他社から業務委託等を請ける場合には、契約時に委託元と合意した情報の取扱いなどのセキュリティ関連の要求事項を遵守する。
・サプライチェーンにおけるサイバーセキュリティ対策を担保する手段として、第三者による評価検証結果を活用する（認証制度の活用、助言型外部監査の実施等）。

---

27 中小企業自らがセキュリティ対策に取り組むことを宣言する制度
https://www.ipa.go.jp/security/security-action/

28 ISMS 認証を取得していない場合でも、例えば、技術情報管理認証を取得していることを確認することなどが考えられる。https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html

29 中小企業を対象に、サイバーセキュリティに関する「見守り」「駆付け」「保険」をまとめて提供するサービス
https://www.ipa.go.jp/security/otasuketai-pr/

30 サイバー保険は情報漏えい等のサイバーセキュリティインシデント発生に伴い生じた損害に対する金銭的な補償の手段となり得るが、被害の全体が補償対象とならない場合があることや、国家レベルの攻撃の場合は戦争扱いとなり、補償の対象とならない可能性があることに留意する必要がある。

３．５．ステークホルダーを含めた関係者とのコミュニケーションの推進

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必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる。
- 入手した情報を有効活用するための環境整備をさせる。

対策を怠った場合のシナリオ

・情報共有活動への参加により、解析した攻撃手法などの情報を用いて、他社における同様の被害を未然に防止することができるが、情報共有ができていないと、新たな攻撃情報が入手できず、対策が遅れ、さらには標的となるリスクの増加につながる。

・インシデント発生時の備えがない場合、サイバーセキュリティインシデント発生時の情報漏えい等に関する所管省庁への報告義務や上場会社に求められる適時開示などを果たせず、国内外の法令等への違反となるおそれがあり、また、適切な情報開示を行わないことにより、株主や事業におけるステークホルダーに不信感を与えてしまう。

対策例

・情報の入手と提供という双方向の情報共有を通じて、社会全体でサイバー攻撃の防御につなげることが重要。情報共有を通じたサイバー攻撃の防御につなげていくため、情報を入手するのみならず、積極的に情報を提供する。

・株主やステークホルダーとの対話、広報による一般向け情報開示等の機会において、サイバーセキュリティインシデントに備えた日頃の取組等の情報開示に積極的に取り組む。

・「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参考に、インシデントに備え、サイバーセキュリティ専門組織との情報共有や被害に係る情報の公表を行うに当たっての観点について、あらかじめ理解しておく。

・IPA や一般社団法人 JPCERT コーディネーションセンター等による脆弱性情報などの注意喚起情報や、セキュリティ関連製品・サービスの事業者等とのコミュニケーションを、自社のサイバーセキュリティ対策に活かす。

・CSIRT 間における情報共有や、日本シーサート協議会、業種内でのセキュリティ情報共有組織（ISAC）等のコミュニティ活動への参加による情報収集等を通じて、自社のサイバーセキュリティ対策に活かす。

・IPA に対し、告示（コンピュータウイルス対策基準、コンピュータ不正アクセス対策基

準）に基づいてマルウェア情報や不正アクセス情報の届出をする。

・JPCERT コーディネーションセンターにインシデントに関する情報提供を行い、必要に応じて調整を依頼する。

・重要インフラ事業者の場合には、J-CSIP などの情報共有の仕組みを利用する。

・サーバ提供事業者や Web サイト制作事業者など、自社事業に関わる外部の事業者等と日常からサイバーセキュリティ関連情報の共有等に関して積極的な連携を行う。

・中小企業の場合は、商工会議所、商工会等を通じて地元で情報共有を行うことのできる相手を確保する。

付録Ａ　サイバーセキュリティ経営チェックシート

付録Ａ－１　「経営者が認識すべき３原則」に関するチェックシート

※本チェックシートは経営者によるセルフチェックを想定しているが、すべての内容を経営者が管掌することを求めるものではなく、企業規模やグループ構成等に応じて役割・権限を委譲している場合はその担当者とともに確認し、内容を理解しておくことが適切である。

※経営者による確認が難しい場合、経営者の指示を受けた CISO 等が自社での取組内容を確認し、経営者への説明に活用する等、コミュニケーションツールとしての利用も考えられる。

（1）経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要

- □ 自社の様々な経営判断において、考慮すべき重要リスクの一つとしてサイバーセキュリティリスクを位置付け、企業の事業継続のためのセキュリティ投資の必要性を認識している
- □ サイバーセキュリティ対策の実施を通じてリスクを許容可能とする水準まで低減することが、経営者としての責務であることを認識している
- □ サイバーセキュリティリスクへの対策として指示した内容が適切に実施されていることを定期的に確認するとともに、実施できていない場合には怠りなく対応を促している

（2）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、自社のみならず、国内外の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

- □ 委託関係にとどまらない多様なサプライチェーンによるつながりが、自社及び社会のサイバーセキュリティに重大な影響を及ぼし得ることを認識している
- □ 自社のリスクマネジメントを検討する際には、サイバーセキュリティリスクの要因を洗い出す対象範囲がグループ企業や外部委託先まで含まれていることを確認している
- □ サプライチェーン全体のサイバーセキュリティリスクを低減するには、全ての企業が加害者となり得る可能性があり、各社で総合的なセキュリティ対策を徹底する必要があることを理解し、その実践状況を確認している

（3）平時及び緊急時のいずれにおいても、サイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

- □ インシデント発生時の適切な対応に備え、平時から関係者との間でのサイバーセキュリティリスクに関するコミュニケーションの実践を心掛けている
- □ サイバーセキュリティインシデントが発生した場合に自社内での対応を担う関係者を把握し、緊急時に適切なコミュニケーションができるよう備えている
- □ 自社や委託先等でサイバーセキュリティに関するインシデントが発生した際、どのような情報発信をすれば社外関係者の信頼を維持できるかを理解している

付録Ａ－２　「サイバーセキュリティ重要10項目」に関するチェックシート

※本チェックシートの対象は経営者が指示した事項の実践状況であり、企業規模に応じて実務者にてチェックを行い、経営者が結果を確認することが適切である。

※本チェックシートの項目をもとに、サイバーセキュリティ経営ガイドラインの指示内容の実践状況に関する可視化を支援するツールを以下にて提供している。

「サイバーセキュリティ経営可視化ツール」（IPA）
https://www.ipa.go.jp/security/economics/checktool/index.html

※本チェックシートは、基本的な項目を示しており、企業の状況に応じて追加対策等を行うことも重要である。

※以降では、本チェック項目と NIST が提供するサイバーセキュリティフレームワーク[31]との対応関係も合わせて提示する（括弧書きはサイバーセキュリティフレームワークのサブカテゴリーの識別子に対応）。

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

□	経営者が、サイバーセキュリティリスクを経営者が負うべき経営リスクの１つとして認識している	（－）
□	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サイバーセキュリティの基本方針を策定し、宣言している	(ID.GV-1)
□	法令・契約やガイドライン等の要求事項を把握し、基本方針等に反映している	(ID-GV-3) (DE.DP-2)

指示２　サイバーセキュリティリスク管理体制の構築

□	組織の基本方針に基づき、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している	(ID-GV)
□	サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にしている	(ID.GV-2)
□	組織内のガバナンスや内部統制、事業継続に関する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している	(ID-GV-4)

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

□	経営会議等の議論により、サイバーセキュリティ対策とそれを実施できる資源（予算、人材等）を明確にしている	(ID-AM)
□	サイバーセキュリティ対策に関して、自組織で対応する部分と外部に委託する部分を適切に切り分けている	(ID.BE-3) (ID.BE-4) (ID.SC-2)

[31] NIST サイバーセキュリティフレームワークの詳細については、付録 B（サイバーセキュリティ対策に関する参考情報）参照。

☐	自組織に求められるセキュリティ人材の要件を明らかにし、計画的にサイバーセキュリティ人材を確保、育成するとともに、適正な処遇を与えている	(PR.AT-1) (PR.AT-2) (PR.AT-3) (PR.AT-4) (PR.AT-5)
□	プラス・セキュリティを担う人材を対象に、サイバーセキュリティの知識・スキルの習得を実施している	(PR.AT-1) (PR.AT-5)
☐	外部に委託する部分について、自社の課題、予算、場所等を考慮して適切な外部リソースを選定し、活用している	(ID.BE-3) (ID.BE-4) (ID.SC-3) (ID.SC-4)

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

☐	守るべきデジタル環境、サービス及び情報を特定し、当該資産の場所やビジネス上の価値等に基づいて対策の優先順位付けを行っている	(ID.AM-1) (ID.AM-2) (ID.AM-3) (ID.AM-4) (ID.AM-5)
☐	守るべきデジタル環境、サービス及び情報に対するサイバー攻撃（過失や内部不正を含む）の脅威、脆弱性を特定し、これらによるサイバーセキュリティリスクが自社の事業にいかなる影響があるかを把握している	(ID.RA-1) (ID.RA-3) (ID.RA-4) (ID.RA-5) (ID.RM-1) (ID.RM-2)
☐	リスクアセスメント結果に基づいてリスク対応計画を策定している	(ID.RA-3) (ID.RA-6)

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

☐	重要なシステムの資産管理・構成管理・パッチ管理を行っている	(PR.IP-1) (PR.IP-2) (PR.IP-3) (PR.PT-3)
☐	組織内でシャドーIT を利用させない対策を行っている	(PR.AC)
☐	システム設計時にリスクアセスメントを行い、必要なセキュリティ機能を具体化し、開発時に実装している	(ID.RA-6) (ID.RM-3)
☐	重要業務を行う端末・サーバー等には複数の技術的対策を実施してい	(PR.AC)

	る	(PR.DS) (PR.PT-1) (PR.PT-2) (PR.PT-3)
□	重要業務を行うネットワークには複数の技術的対策を実施している	(PR.AC) (PR.DS) (PR.PT-4)
□	システム等に対する定期的な脆弱性診断や、継続的なパッチ適用、その他の緩和策等の脆弱性対策の計画を立て、実行している	(PR.IP-12) (DE.CM-8) (RS.MI-3)
□	端末やネットワークからのログを収集・分析している	(PR.MA-1) (PR.MA-2)
□	サイバー攻撃を検知した際に通信を遮断する等のインシデント対応の仕組みを導入している	(DE.AE) (DE.DP)
□	インシデントの管理の仕組みを導入している	(PR.IP-9)
□	従業員に対して、サイバーセキュリティの教育・演習を実施している。	(PR.AT-1)

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

□	サイバーセキュリティ運用管理に関する KPI を定めている	(ID.RM-1) (ID.RM-2) (ID.RM-3)
□	経営者が定期的に、サイバーセキュリティ対策実施状況に関する報告を受け、議論・対策指示している	(ID.GV)
□	サイバーセキュリティに関する監査を実施し、その結果を踏まえ、サイバーセキュリティ対策を適時見直している	(PR.IP-7) (RP.PT-1)
□	サイバーセキュリティリスクへの対策状況についてステークホルダーとコミュニケーションしている	(ID.SC) (RS.CO-3) (RS.CO-4) (RS.CO-5)

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を考慮したインシデント対応計画を策定している	(PR.IP-9) (RS.RP-1) (RS.IM-1) (RS.IM-2) (RS.AN-4)

□	インシデントに対応可能な専門チーム（CSIRT 等）を設置している	(RS.CO-1)
□	組織外に共有・報告・公表すべき内容やタイミング等を定めている	(RS.CO-2) (RS.CO-1)
□	インシデント発生時の緊急対応の演習を定期的に行っている	(PR.IP-10)
□	インシデント発生時のログ分析・調査を速やかに行い、影響範囲を特定できるよう実施計画を策定している	(PR.MA-1) (PR.MA-2) (PR.PT-1) (RS.AN-4)

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

□	被害が発生した際の、サプライチェーン全体を考慮した業務の復旧計画を策定している	(ID.BE-5) (PR.IP-9) (RC.RP-1) (RC.IM-1) (RC.IM-2)
□	定期的に復旧対応演習を行っている	(PR.IP-10) (RC.CO)

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

□	グループ企業との取引や連携におけるサイバーセキュリティリスクへの対策状況を把握している	(ID.RA) (ID.BE-1)
□	委託先等の取引先との契約で合意したサイバーセキュリティリスクに関する役割と責任範囲に基づいて、適切な方策が講じられていることを確認している	(ID.AM-6) (ID.BE-1) (ID.SC)
□	自社事業に影響を及ぼすサプライチェーン全体にわたって、サイバーセキュリティリスクが許容可能な水準を超えていないことを確認している	(ID.RA-5) (ID.SC)

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

□	関係団体が提供する注意喚起情報の入手や、業界のセキュリティコミュニティ等への参加を通して情報共有を行い、自社の対策に活かしている	(ID.RA-2) (RS.AN-5)
□	マルウェア感染、不正アクセス等のインシデントがあった際に、関係団体やコミュニティへの共有・報告や、適切な公表等の情報提供を実施している	(RS.CO)

付録Ｂ　サイバーセキュリティ対策に関する参考情報

サイバーセキュリティ対策を担当する部署などにおいて、本ガイドラインで示している重要 10 項目等を実践する上で参考となる情報源や資料を以下に示す。これらは更新される可能性があるため、適宜最新版を参照するよう努めるべきである。

全般に関連する参考情報

○ サイバーセキュリティ・ポータルサイト（オフィス等でシステムを利用する人向け・経営層）（内閣サイバーセキュリティセンター（NISC））

（企業等の経営層を対象に、普及啓発や人材育成を目的として関係機関が発信している情報を紹介。）

https://security-portal.nisc.go.jp/curriculum/classified/6office_exe.html

○ 経営に役立つサイバーセキュリティコンテンツ（IPA）

（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）攻撃動向分析・対策ワーキンググループの活動の一環として、サイバーセキュリティ対策を実践している企業の経営者へのインタビュー、経営者が知っておくべきセキュリティに関するテーマを解説したコラム等を掲載。）

https://www.ipa.go.jp/security/sc3/activities/kougekiWG/content/

○ 中小企業の情報セキュリティ対策ガイドライン [第 3 版]（IPA）

（中小企業がセキュリティ対策に取り組む上でのポイントを解説したガイドライン。最低限対策が求められる「情報セキュリティ 5 か条」や、セキュリティポリシーのサンプル、企業のセキュリティ対策状況を診断する「5 分でできる！情報セキュリティ自社診断」、クラウドサービス安全利用の手引き等の付録も提供。）

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

○ サイバーセキュリティ関係法令 Q&A ハンドブック [Ver1.0]（NISC）

（企業における平時のサイバーセキュリティ対策及びインシデント発生時の対応に関する法令上の事項に加え、情報の取扱いに関する法令や情勢の変化等に伴い生じる法的課題等を可能な限り平易な表記で記述。）

https://security-portal.nisc.go.jp/law_handbook/

○ ISO/IEC 27002:2022（ISO/IEC）

（情報マネジメントシステムの仕様を定めた国際標準規格であり、情報セキュリティ管理のベストプラクティスを提供。）

○ Framework for Improving Critical Infrastructure Cybersecurity [Version 1.1]（NIST）

重要インフラに係わる企業向けに実施すべきセキュリティ対策を「特定」、「防御」、「検知」、「対応」、「復旧」の 5 つの機能に分類し、さらにそれらの機能を 22 のカテゴリーで提示した米国のガイドライン。重要インフラ以外の企業でも活用可能。）

https://www.nist.gov/cyberframework/framework （対訳）https://www.ipa.go.jp/files/000071204.pdf

○ SP800-53 [Rev.5]（NIST）

（連邦政府機関が実施すべきセキュリティ対策を提示した米国のガイドライン。米国連邦政府向けのクラウドサービスを提供する際に、本ガイドラインへの準拠が要求される場合がある。）

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

○ SP800-161 [Rev.1]（NIST）

（組織のあらゆる階層におけるサプライチェーン全体のサイバーセキュリティリスクを特定、評価、および軽減するためのガイダンスを提供。）

https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

○ SP800-171 [Rev.2]（NIST）

（連邦政府機関以外の組織及び情報システムに対する CUI[32]を保護する上で実施すべきセキュリティ対策を提示した米国のガイドライン。米国連邦政府関係の業務を受託する際に、本ガイドラインへの準拠が要求される場合がある。）

https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

○ CIS Controls [Version 8]（Center for Internet Security）

（組織が実施すべき優先度の高い管理策をカテゴリー別にまとめたもの。米国のセキュリティ関連の官民組織が参加する非営利団体によって定期的に更新されており、中小企業からセキュリティ専門家のいる組織まで3段階で対象とする組織を分類している。）

https://www.cisecurity.org/controls

経営者が認識すべき３原則に関連する参考情報

○ サイバーリスクハンドブック　取締役向けハンドブック　日本版

（一般社団法人日本経済団体連合会）

(米国と英国においてそれぞれ取締役向けに公表されていたサイバーリスクに関する文献において示されていたサイバーセキュリティに関する5つの原則を、日本企業向けに翻訳・整理して公表。)

https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.html

指示２及び指示３に関連する参考情報

○ サイバーセキュリティ体制構築・人材確保の手引き（経済産業省）

（本ガイドラインの別冊付録 F として、サイバーセキュリティ体制の構築及び人材の確保・育成にあたって考慮すべき事項と取組方法について解説。）

https://www.meti.go.jp/policy/netsecurity/mng_guide.html （本ガイドラインの公開ページ）

[32] Controlled Unclassified Information の略。管理すべき重要情報ではあるが、連邦政府が秘・極秘・機密等のように特別な取扱を定めてはいない情報を指す。

指示３に関連する参考情報

○ IT のスキル指標を活用した情報セキュリティ人材育成ガイド（IPA）

（サイバー攻撃等を防ぐためにどのような対策が必要で、その対策を実施するためにはどのような人材が必要なのかを例示し、人材育成を行うためのヒントをまとめたガイドライン。）

https://www.ipa.go.jp/files/000039528.pdf

○ 職場の情報セキュリティ管理者のためのスキルアップガイド [2015 年 9 月]（IPA）

（セキュリティ上の脅威を取り上げ、被害を防ぐためにはどのような対策を実施すべきかを例示し、セキュリティ管理者としての役割を具体的に提示したガイドライン。）

https://www.ipa.go.jp/files/000047872.pdf

指示４に関連する参考情報

○ サイバー・フィジカル・セキュリティ対策フレームワーク [Ver1.0]（経済産業省）

（サイバー空間とフィジカル空間が融合することで新たな価値を生み出していく「Society5.0」における産業社会を取り巻く環境では、サイバー攻撃の起点が拡大し、その被害がフィジカル空間に及ぼす影響も増大するなど、これまでとは異なる新たなリスクを伴うことを踏まえた、付加価値を創造する活動が直面する新たなリスクに対応していくための指針を提示。）

https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

○ 脆弱性等に関する最新情報の提供（IPA）

（放置すると不正アクセスやデータが盗まれるなどの危険性が高いセキュリティ上の問題と対策に関する情報提供を実施。）

https://www.ipa.go.jp/security/announce/alert.html

指示５に関連する参考情報

○ 情報セキュリティサービス審査登録制度（経済産業省）

（情報セキュリティサービス基準が定める技術要件と品質管理要件を満たすサービスをリストとして公表。）

https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html

○ 「高度標的型攻撃」対策に向けたシステム設計ガイド [2014 年 9 月]（IPA）

（標的型攻撃対策として、システム内部への侵入を前提とした上で、侵害拡大防止及び監視強化を目的とした内部対策について解説したガイドライン。）

https://www.ipa.go.jp/files/000046236.pdf

○ 高度サイバー攻撃への対処におけるログの活用と分析方法 [1.2 版]（JPCERT/CC）

（サイバー攻撃への備えと効果的な対策の観点から、一般的に利用される機器に攻撃者の活動の痕跡をログとして残すための考え方、それらのログから痕跡を見つけ出す方法等を記載したガイドライン。）

https://www.jpcert.or.jp/research/apt-loganalysis.html

○ 組織における内部不正防止ガイドライン [第 5 版]（IPA）

（組織における内部不正を防止するために実施すべき対策として、10 の観点（コンプライアンス、職場環境等）のもと 30 項目の対策を提示したガイドライン。）

https://www.ipa.go.jp/security/fy24/reports/insider/

○ 秘密情報の保護ハンドブック [令和 4 年 5 月]（経済産業省）

（秘密情報の漏えいを未然に防止するための対策例を集めて紹介したハンドブック。）

https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

○ クラウドサービス利用のための情報セキュリティマネジメントガイドライン（経済産業省）

（クラウドサービスの利用にかかわるリスク対応のために JIS Q 27002 から適切な管理策を選択し、導入するための助言とその最適な実施のための手引を提供。）

https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

○ クラウドセキュリティガイドライン活用ガイドブック（経済産業省）

（クラウドサービスで実際に発生した事故や、事業者が抱える様々なセキュリティ上の課題をベースに、IT サービスとしてのクラウドサービスに関するリスクと対策を、事業者と利用者のそれぞれについて解説。）

https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf

○ クラウドサービスを利用する際の情報セキュリティ対策（総務省）

（企業や組織がパブリッククラウドサービスを利用する際、クラウドサービスを提供する事業者やサービスを選定する際に確認すべき事項を紹介。）

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin_15.html

指示６に関連する参考情報

○ 情報セキュリティマネジメントシステム（ISMS）適合性評価制度（JIPDEC）

（情報セキュリティマネジメントシステムにおける国際標準規格 ISO/IEC27001 に基づいて第三者認証を行う制度。）

https://isms.jp/isms.html

○ サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度（JIPDEC）

（産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムにおける国際標準規格 IEC62443-2 に基づいて第三者認証を行う制度。）

https://isms.jp/csms.html

○ 情報セキュリティ管理基準（経済産業省）

（情報セキュリティマネジメントの構築から具体的な管理策に至るまで包括的な内容を含み、国際標準規格 ISO/IEC27001 とも整合を持った基準。）

https://www.meti.go.jp/policy/netsecurity/is-kansa/index.html

○ 情報セキュリティ対策ベンチマーク（IPA）

（Web 上で質問に答えることによって、自社のセキュリティ対策の実施状況を散布図、レーダーチャート、スコア等で表示するツール。自社の対策状況を他社の対策状況と比較することも可能。）

https://www.ipa.go.jp/security/benchmark/

○ 安全なウェブサイトの作り方 [第 7 版]（IPA）

（セキュリティを考慮した Web サイトを作成するための技術的な対策を提示したガイドライン。別冊として Web サイトに脆弱性が存在していないかを確認するためのテスト項目を提示したウェブ健康診断仕様等も提供。）

https://www.ipa.go.jp/security/vuln/websecurity.html

○ Japan Vulnerability Notes（JVN）（IPA、JPCERT/CC）

（日本で使用されているソフトウェア等の脆弱性関連情報とその対策情報を提供する、脆弱性対策情報ポータルサイト。）

https://jvn.jp/

○ サイバーセキュリティ対策情報開示の手引き（総務省）

（企業が情報開示の在り方を検討する際の参考資料として、開示書類におけるサイバーセキュリティ対策に関する開示項目の例や、既に公開されている開示書類の事例集を掲載。）

https://www.soumu.go.jp/main_content/000630516.pdf

指示 7 に関連する参考情報

○ CSIRT 構築マテリアル（JPCERT/CC）

（組織的なインシデント対応を行うための CSIRT を構築する上で、「構想フェーズ」、「構築フェーズ」、「運用フェーズ」のそれぞれの段階で考慮すべきポイントを解説したガイドライン。）

https://www.jpcert.or.jp/csirt_material/

○ CSIRT 構築に役立つ参考資料（日本シーサート協議会）

（CSIRT の構築に際し、構築初心者／経営者向け説明時／構築担当者の企画・構築・運用の各段階におけるドキュメント類をまとめた参考資料集。）

https://www.nca.gr.jp/ttc/wtda.html
https://www.nca.gr.jp/activity/build-wg-document.html

○ サイバー攻撃被害に係る情報の共有・公表ガイダンス（警察庁、総務省、経済産業省、サイバーセキュリティ協議会事務局（内閣官房内閣サイバーセキュリティセン

ター、JPCERT/CC）

（サイバー攻撃被害に関する情報共有の活性化を目的として、被害を受けた組織が保護されつつ、円滑かつ効果的に情報共有が行われるためのポイントを示すガイダンス資料。）

https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

指示８に関連する参考情報

○ 事業継続ガイドライン [令和３年４月改定]（内閣府）

（事業継続計画の策定・改善にあたって、事業継続の必要性を明示し、実施が必要な事項、望ましい事項等を提示したガイドライン。）

https://www.bousai.go.jp/kyoiku/kigyou/keizoku/pdf/guideline202104.pdf

指示９に関連する参考情報

○ サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて（経済産業省、公正取引委員会）

（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ための施策、並び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したもの。）

https://www.meti.go.jp/policy/netsecurity/index.html#partnership

○ 情報サービス・ソフトウェア産業における下請適正取引等の推進のためのガイドライン [平成 29 年３月]（経済産業省）

（下請適正取引等の推進を図ることを目的として策定したものであり、個人情報保護やセキュリティ対策に係る取り組み等の考慮すべき事項を解説したガイドライン。）

https://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf

○ 技術情報管理認証制度（経済産業省）

（紙媒体等を含む全ての情報を対象に、企業等による情報管理に関する取組を認証する制度。）

https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html

○ SECURITY ACTION セキュリティ対策自己宣言 （IPA）

（中小企業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。）

https://www.ipa.go.jp/security/security-action/

○ サイバーセキュリティお助け隊 （IPA）

（中小企業を対象に、サイバーセキュリティに関する「見守り」「駆付け」「保険」をまとめて提供するサービス。）

https://www.ipa.go.jp/security/otasuketai-pr/

指示１０に関連する参考情報

○ 届出・相談・情報提供（不正アクセスやマルウェア等に関する届出）（IPA）

（コンピュータウイルス等のマルウェア、不正アクセス、脆弱性関連情報等に関する届出を行う際の届出様式、届出先、届出状況等を提供する Web サイト。）

https://www.ipa.go.jp/security/outline/todoke-top-j.html

○ 標的型サイバー攻撃特別相談窓口（IPA）

（標的型サイバー攻撃を受けた際に、専門的知見を有する相談員が対応する窓口。）

https://www.ipa.go.jp/security/tokubetsu/

○ サイバー情報共有イニシアティブ（J-CSIP）（IPA）

（重要インフラで利用される機器の製造業者、電力業界、ガス業界、化学業界、石油業界、資源開発業界、自動車業界、クレジット業界において情報共有と早期対応を行うための活動。）

https://www.ipa.go.jp/security/J-CSIP/

○ インシデントの報告及び対応依頼（JPCERT/CC）

（国内に関連するインシデント対応活動として、インシデントに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための助言などを実施。）

https://www.jpcert.or.jp/menu_reporttojpcert.html

○ @police（警察庁）

（サイバー犯罪・サイバーテロの未然防止及び被害の拡大防止を図るために、ネットワークセキュリティに関する様々な情報を提供する Web サイト。）

https://www.npa.go.jp/cyberpolice/

付録Ｄ　関連する規格・フレームワーク等との関係

※本表は、「サイバーセキュリティ重要 10 項目」を実践する実務者向けの参考情報として、企業で用いられる国際規格（ISO/IEC 27000 シリーズ）及びサイバーセキュリティ関連のフレームワーク等との対応関係を示すものである。

重要10項目	ISO/IEC 27001:2022(●)、ISO/IEC 27002:2022(・)		NISTサイバーセキュリティフレームワークVer1.1		CIS Controls Ver8	
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	●5.1 ●5.2 ●7.3 ・5.1 ・5.4	リーダーシップ及びコミットメント 方針 認識 情報セキュリティのための方針群 経営陣の責任	ID.GV	ガバナンス	－	―
指示2　サイバーセキュリティリスク管理体制の構築	●5.3 ・5.2 ・5.3	組織の役割、責任及び権限 情報セキュリティの役割及び責任 職務の分離	ID.BE	ビジネス環境	－	―
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	●7.1 ●7.2	資源 力量	ID.AM PR.AT	資産管理 意識向上およびトレーニング	14	セキュリティの意識向上とスキルのトレーニング
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	●6.1 ●6.2 ●8.2 ●8.3 ・5.7 ・5.9 ・5.10 ・5.12 ・5.32	リスク及び機会に対処する活動 情報セキュリティ目的及びそれを達成するための計画策定 情報セキュリティリスクアセスメント 情報セキュリティリスク対応 脅威インテリジェンス 情報及びその他の関連資産の目録 情報及びその他の関連資産の利用の許容範囲 情報の分類 知的財産権	ID.RA ID.RM	リスクアセスメント リスクマネジメント戦略	01 02 04	組織の資産のインベントリと管理 ソフトウェア資産のインベントリと管理 組織の資産とソフトウェアの安全な構成
指示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	●7.5 ・5.13 ・5.14 ・5.15 ・5.16 ・5.17 ・5.18 ・5.33 ・5.34 ・5.37 ・6 ・7 ・8	文書化した情報 情報のラベル付け 情報転送 アクセス制御 識別情報の管理 認証情報 アクセス権 記録の保護 プライバシー及び PII の保護 操作手順書 人的管理策 物理的管理策 技術的管理策	PR.AC PR.DS PR.IP PR.PT	アイデンティティ管理、認証／アクセス制御 データセキュリティ 情報を保護するためのプロセスおよび手順 保護技術	03 05 06 09 10 12 16	データ保護 アカウント管理 アクセス制御管理 電子メールと Web ブラウザの保護 マルウェアの防御 ネットワークインフラストラクチャ管理 アプリケーションソフトウェアセキュリティ

重要10項目	ISO/IEC 27001:2022(●)、ISO/IEC 27002:2022(・)		NISTサイバーセキュリティフレームワークVer1.1		CIS Controls Ver8	
指示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	●7.4 ●8.1 ●9.1 ●9.2 ●9.3 ●10.1 ●10.2 ・5.8 ・5.11 ・5.31 ・5.35 ・5.36	コミュニケーション 運用の計画及び管理 監視、測定、分析及び評価 内部監査 マネジメントレビュー 継続的改善 不適合及び是正処置 プロジェクトマネジメントにおける情報セキュリティ 資産の返却 法令、規則及び契約上の要求事項 情報セキュリティの独立したレビュー 情報セキュリティのための方針群、規則及び標準の順守	PR.MA DE.PE DE.CM DE.DP	保守 異常とイベント セキュリティの継続的モニタリング 検知プロセス	07 08 13 18	継続的な脆弱性管理 監査ログ管理 ネットワークの監視と防御 ペネトレーションテスト
指示7 インシデント発生時の緊急対応体制の整備	・5.24 ・5.25 ・5.26 ・5.27 ・5.28	情報セキュリティインシデント管理の計画及び準備 情報セキュリティ事象の評価及び決定 情報セキュリティインシデントへの対応 情報セキュリティインシデントからの学習 証拠の収集	RS.RP RS.AN RS.MI RS.IM	対応計画 分析 低減 改善	17	インシデントレスポンスと管理
指示8 インシデントによる被害に備えた復旧体制の整備	・5.29 ・5.30	事業の中断・阻害時の情報セキュリティ 事業継続のための ICT の備え	RC.RP RC.IM	復旧計画 改善	11	データ復旧
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対策及び状況把握	●8.1 ・5.19 ・5.20 ・5.21 ・5.22 ・5.23	運用の計画及び管理 供給者関係における情報セキュリティ 供給者との合意におけるセキュリティの取扱い ICT サプライチェーンにおける情報セキュリティの管理 供給者のサービス提供の監視、レビュー及び変更管理 クラウドサービスの利用における情報セキュリティ	ID.SC	サプライチェーンリスクマネジメント	15	サービスプロバイダの管理
指示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	・5.5 ・5.6	関係当局との連絡 専門組織との連絡	RS.CO RC.CO	コミュニケーション コミュニケーション	－	―

付録Ｅ　用語の定義

本ガイドラインで用いている用語や略語の意味を以下に示す。

(1) 暗号化

暗号鍵を知る者以外がデータの内容を知ることができないよう、定められた計算処理によってデータを変換することをいう。暗号化されたデータが第三者に解読されないかどうかは、暗号鍵として用いる情報の長さ及び複雑さ、並びに計算処理の方法に関する数学的な強度に依存する。

(2) インシデント

サイバーセキュリティ分野において、サイバーセキュリティリスクが発現・現実化した事象のこと。

(3) 改ざん検知

暗号技術を用いて、あるデータが第三者に改ざんされているかどうかを技術的に判定すること。

(4) 監査

組織内においてサイバーセキュリティ対策が適切に実施されているかどうかを判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセスのこと。監査は、内部監査（第一者）又は外部監査（第二者・第三者）のいずれでも、又は複合監査（複数の分野の組合せ）でもあり得る。

(5) サイバー空間

コンピュータシステムやネットワークの中に広がる仮想空間のこと。

(6) サイバー攻撃

コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと。

(7) サイバーセキュリティ

サイバーセキュリティとは、電子データの漏えい・改ざん等や、期待されていた IT システムや制御システム等の機能が果たされないといった不具合が生じないようにすること。

(8) サイバーセキュリティリスク

サイバーセキュリティリスクとは、サイバーセキュリティに関連して不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと。

(9) 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)

サイバー空間とフィジカル空間が融合することで新たな価値を生み出していく「Society5.0」における産業社会を取り巻く環境では、サイバー攻撃の起点が拡大し、その被害がフィジカル空間に及ぼす影響も増大するなど、これまでとは異なる新たなリスクを伴うことを踏まえた、付加価値を創造する活動が直面する新たなリスクに対応していくための指針のこと。

(10)サプライチェーン

複数の事業者間での受発注等の契約を介した物や情報のやりとりを行うためのつながりのことを指すが、本ガイドラインにおいては、サイバー空間とフィジカル空間の両空間を跨いで、様々なモノやデータが動的につながって構成される付加価値の創造活動全て(付録 B で紹介している『サイバー・フィジカル・セキュリティ対策フレームワーク』における「バリュークリエイションプロセス」に相当)を含む。具体的には、部品製造を担う企業とそれらの部品を用いて組立を行う企業との関係にとどまらず、クラウドサービスなど外部のデジタルサービスの利用や、API(アプリケーションプログラムインタフェース)を介したシステム同士の連携などもサプライチェーンに含まれる。

(11)残留リスク

リスク対応(回避、低減、移転)後に残るリスク。残存リスク、保有リスクともいう。

(12)情報セキュリティ報告書

企業の情報管理・情報システム等のセキュリティの取組の中でも社会的関心の高いものについて情報開示することにより、当該企業の取組が顧客や投資家などのステークホルダーから適正に評価されることを目指すもの。

(参考: 経済産業省の「情報セキュリティ報告書モデル」:
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf)

(13)ステークホルダー

意思決定もしくは活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人または組織。具体的には、株主、債権者、顧客、取引先等である。

(14)セキュリティポリシー

企業・組織におけるセキュリティに関する理念である意図と方針を経営者が正式に表明したもの。セキュリティポリシーに沿って、組織内セキュリティ対策が規定される。

(15)多層防御

物理層、ネットワーク層からデータ層までの多層防御を導入することで、1つの機器やソフトウェアに依存する拠点防御対策や、単一の境界防御層(主としてネットワーク境界)に依存する対策の場合より、未知のマルウェアや新たな攻撃手法の登場により容易に突破されるリスクの軽減が期待される。

IPA では、多層防御の1例として、以下四つのポイントを紹介している。①ソフトウェア感染リスクの低減、②重要業務を行う端末やネットワークの分離、③重要情報が保存されているサーバーでの制限、④事後対応の準備。

(16)電子署名

暗号技術に基づき、あるデータが改変されていないことを保証するために用いる電子的な付加情報のこと。

(17)ビジネスパートナー

業務の委託先や受託元、物品・サービスの調達先等の取引関係のある企業のこと。

(18)フィジカル空間

サイバー空間以外の現実の世界のこと。

(19)プラス・セキュリティ

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。

(20)マルウェア

セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボットなどの悪意をもったプログラムを指す総称。これらのプログラムは、使用者や管理者の意図に反して(あるいは気づかぬうちに)コンピュータに入り込み悪意ある行為を行う。

(21)ランサムウェア

「Ransom(身代金)」と「Software(ソフトウェア)」を組み合わせた造語。感染したパソコンのデータを暗号化するなど使用不可能にし、その解除と引き換えに金銭を要求する。さらに新たな攻撃手法として、ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバー上のデータを窃取した上で一斉に暗号化してシステムを使用不可能にし、データの復旧に対する金銭要求に加えて、窃取したデータを公開しない見返りの金銭要求も行うなど、二重の脅迫を行う場合もある。

(22)リスク

国際規格(ISO/IEC 27000)では、「諸目的に対する不確かさの影響」と定義されている。

(23)リスク対応(回避、低減、移転、保有)

対処の方法には、大きく分けて「リスク回避」、「リスク低減」、「リスク移転」、「リスク保有」の4つがある。なお、さらに詳細化した分類として、JIS Q 0073 リスクマネジメント−用語では、リスク回避、機会を追及するためのリスクを取る又は増加させる、リスク源の除去、起こりやすさを変更すること、結果を変えること、リスク移転、リスク保有の7分類が定義されている。

① リスク回避

「リスク回避」とは、脅威発生の要因を停止あるいは全く別の方法に変更することにより、リスクが発生する可能性を取り去ることである。例えば、「インターネットからの不正侵入」という脅威に対し、外部との接続を断ち、Web 上での公開を停止してしまうような場合などが該当する。

② リスク低減

「リスク低減」とは、脆弱性に対してセキュリティ対策を講じることにより、脅威発生の可能性を下げることである。ノートパソコンの紛失、盗難、情報漏えいなどに備えて保存する情報を暗号化しておく、サーバー室に不正侵入できないようにバイオメトリック認証技術を利用した入退室管理を行う、従業員に対するセキュリティ教育を実施することなどが該当する。

③ リスク移転

「リスク移転」とは、リスクを他社などに移すことである。例えば、リスクが顕在化したときに備え、保険で損失をカバーすることや、組織内の IT システムの運用を他社に委託し、契約などにより不正侵入やマルウェア感染の被害に対して損害賠償などの形で移転すること等が該当する。

④ リスク保有

「リスク保有」とは、ある特定のリスクにより、起こり得る損失の負担を受容することである。

(24)リスク評価

リスクの大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準(リスクの重大性を評価するために目安とする条件であり、組織の目的並びに外部環境及び内部環境に基づいたもの)と比較するプロセスのこと。

(25)リスク分析

リスクの特質を理解し、リスクレベル(ある事象の結果とその起こりやすさとの組合せとして表現される、リスクの大きさ)を決定するプロセスのこと。

(26)ログ

コンピュータの利用状況やデータの通信記録。操作を行った者の ID や操作日付、操作内容などが記録される。セキュリティ上、インシデントの原因追究などに利用する。

(27)BCP(Business Continuity Plan)

企業が自然災害、テロ攻撃、サイバー攻撃などによる被害が発生した場合において、中核となる事業の継続、早期復旧を実現するために、平時及び緊急時における事業継続のため手段等を取り決めておく計画のこと。

(28)CISO(Chief Information Security Officer)

経営陣の一員、もしくは経営トップからその役を任命された、セキュリティ対策を実施する上での責任者のこと。

(29)CSIRT(Computer Security Incident Response Team)

インシデントの発生に対応するための体制のこと。

(30)PDCA

Plan - Do - Check - Act の略。品質改善や環境マネジメントでよく知られた手法であり、次のステップを繰り返しながら、継続的に業務を改善していく手法の1つのこと。

1.Plan:問題を整理し、目標を立て、その目標を達成するための計画を立てる。
2.Do:目標と計画をもとに、実際の業務を行う。
3.Check:実施した業務が計画どおり行われて、当初の目標を達成しているかを確認し、評価する。
4.Act:評価結果をもとに、業務の改善を行う。

(31)PSIRT(Product Security Incident Response Team)

自社の製品・サービスに関するインシデントの発生に対応するための体制のこと。

サイバーセキュリティリスクと企業経営に関する研究会　委員

（五十音順、〇は委員長）

岩井　博樹	デロイト トーマツ リスクサービス株式会社　シニアマネジャー
川口　洋	株式会社ラック　チーフエバンジェリスト
〇佐々木　良一	東京電機大学　教授　サイバーセキュリティ研究所　所長
徳田　敏文	日本アイ・ビー・エム株式会社　セキュリティ事業本部 セキュリティ・サービス担当部長
名和　利男	株式会社サイバーディフェンス研究所　理事
林　紘一郎	情報セキュリティ大学院大学　教授
松浦　幹太	東京大学　生産技術研究所　教授
三輪　信雄	S&J 株式会社　代表取締役社長
山口　利恵	東京大学　大学院情報理工学系研究科 ソーシャル IC 研究センター　次世代個人認証技術講座 特任准教授

（共同事務局）

（独）情報処理推進機構（IPA）技術本部セキュリティセンター

経済産業省商務情報政策局サイバーセキュリティ課

平成29年度サイバーセキュリティ経営ガイドライン改訂に関する研究会　委員

（五十音順、〇は委員長）

稲垣　隆一	稲垣隆一法律事務所　弁護士
小松　文子	長崎県立大学　情報システム学部　情報セキュリティ学科　教授
〇佐々木　良一	東京電機大学　教授　サイバーセキュリティ研究所　所長
林　紘一郎	情報セキュリティ大学院大学　教授
松下　正夫	特定非営利活動法人 IT コーディネータ協会　基幹業務部　部長
丸山　司郎	株式会社ベネッセインフォシェル　代表取締役社長
丸山　満彦	デロイト トーマツ リスクサービス株式会社　代表取締役社長
宮下　清	一般社団法人日本情報システム・ユーザー協会　常務理事
三輪　信雄	S&J 株式会社　代表取締役社長

（共同事務局）

（独）情報処理推進機構（IPA）技術本部セキュリティセンター

経済産業省商務情報政策局サイバーセキュリティ課

令和4年度サイバーセキュリティ経営ガイドライン改訂に関する研究会　委員

（五十音順、〇は委員長）

稲垣　隆一	稲垣隆一法律事務所　弁護士
小松　文子	長崎県立大学　情報システム学部　情報セキュリティ学科　教授
〇佐々木　良一	東京電機大学　名誉教授 兼 サイバーセキュリティ研究所　客員教授
佐藤　亘	一般社団法人日本情報システム・ユーザー協会　事務局長
比留間　貴士	特定非営利活動法人 IT コーディネータ協会　常務理事・事務局長
丸山　司郎	株式会社 FFRI セキュリティ　セキュリティサービス本部長
丸山　満彦	PwCコンサルティング合同会社 テクノロジーコンサルティング　パートナー
三輪　信雄	S&J 株式会社　代表取締役社長
山本　純也	株式会社 OT デザイン研究所　代表取締役
湯淺　墾道	明治大学 公共政策大学院 ガバナンス研究科 教授

（事務局）

経済産業省商務情報政策局サイバーセキュリティ課

みずほリサーチ＆テクノロジーズ株式会社デジタルコンサルティング部