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・概要

Ⅰ．サイバーセキュリティは経営問題

- 企業の IT の利活用は、業務の効率化による企業の収益性向上だけでなく、グローバルな競争をする上で根幹をなす企業として必須の条件となっている。さらに、IoT といった新たな価値を生み出す技術が普及しつつある中で、AI やビッグデータなども活用した、新しい製品やサービスを創造し、企業価値や国際競争力を持ったビジネスを構築していくことが企業として求められている。

- サイバー攻撃は年々高度化、巧妙化してきており、サイバー攻撃によって純利益の半分以上を失う企業が出るなど、深刻な影響を引き起こす事件が発生している。さらには、攻撃の踏み台にされて外部へ攻撃をしてしまうだけでなく、国の安全保障上重要な技術情報の流出、重要インフラにおける供給停止など、国民の社会生活に重大な影響を及ぼす可能性のある攻撃も発生しており、その脅威は増大してきている。

- 経営者が適切なセキュリティ投資を行わずに社会に対して損害を与えてしまった場合、社会からリスク対応の是非、さらには経営責任や法的責任が問われる可能性がある。また、国内外に関わらずサプライチェーンのセキュリティ対策の必要性も高まっており、業務を請け負う企業にあっては、国際的なビジネスに影響をもたらす可能性が出てきている。

- また、セキュリティ投資は事業継続性の確保やサイバー攻撃に対する防衛力の向上にとどまるものではなく、IT を利活用して企業の収益を生み出す上でも重要な要素となる。**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・成長に必須なものと位置づけて「投資」と捉えることが重要**である。

- このように、サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としての**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。

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を認識し、リーダーシップによって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、企業の成長のためのセキュリティ投資を実施すべきである。）

(2) 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要

（自社のサイバーセキュリティ対策にとどまらず、サプライチェーンのビジネスパートナーや委託先も含めた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、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

（平時からステークホルダー（顧客や株主など）を含めた関係者に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、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）に対して以下の重要10項目を指示すべきである。

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対応するための仕組みの構築

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

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対策及び状況把握

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

（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）

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

近年、企業が有する個人情報や重要な技術情報等を窃取したり、企業のシステムを停止させたりするサイバー攻撃の件数は増加傾向にあり、約4割の企業がサイバー攻撃を受けた経験がある（図1）。しかし、サイバー攻撃の発覚経緯の約半数は外部からの指摘によるものとなっており、実際にはサイバー攻撃による被害を受けていても、そのことに気づいていないという企業がまだ多数存在することも予想される。昨今はランサムウェアのように被害にすぐに気づく攻撃も多発しているが、情報の窃取等を目的とした標的型攻撃においては、適切なセキュリティ対策を実施していなければ気づくことは困難である。このため、自社ではサイバー攻撃を受けていないとして、セキュリティ投資を行わないことはありえない。

さらに、業務用パソコンのみならず、インフラや工場等の制御システムをはじめ企業が管理する多くのシステムや機器が外部ネットワークにつながるようになっており、サイバー攻撃の影響が実際の環境にも及ぶようになっている。

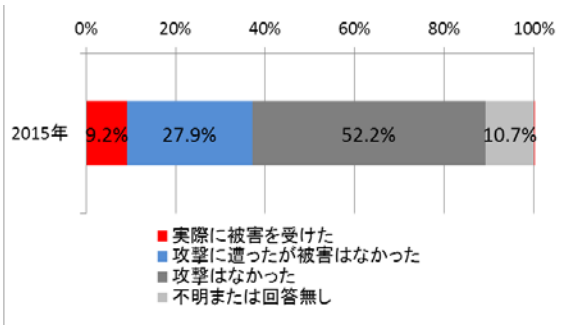

図１　サイバー攻撃（ウイルス以外）被害を受けた企業の割合）[1]

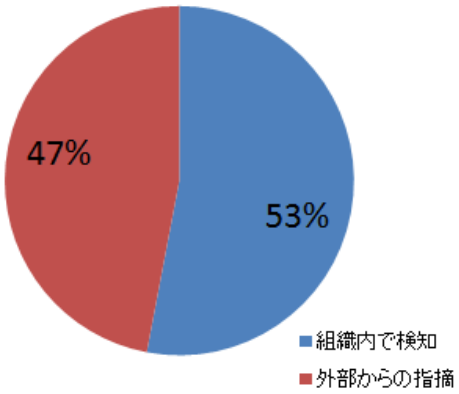

図２　セキュリティ侵害の発覚経緯 [2]

このように、企業を取り巻くサイバー攻撃への脅威が増す一方、多くの企業が十分な対策を取れているとは言いがたい。こうした原因の一つに、セキュリティ対策に対して経営者が十分なリーダーシップを発揮していないことが挙げられる。経営資源の配分としてセキュリティ投資を成長投資とみる企業は2割弱に留まり、セキュリティ投資はやむを得ない費用であると認識している企業が圧倒的に多数である。また、成長投資と考えている企業においては7割以上の企業が必要なセキュリティ予算を確保できているのに対し、やむを得ない費用と考えている企業においては4割程度に留まっている。

[1]独立行政法人情報処理推進機構（IPA）「企業の CISO や CSIRT に関する実態調査 2016 調査報告書」より経済産業省作成
[2]FireEye, Inc.「M-Trends2017：セキュリティ最前線からの視点」より経済産業省作成

このことからも、経営者がリーダーシップを取り、企業の成長のためにセキュリティ投資を行っていくことが、サイバー攻撃への耐性を高めることに繋がる。

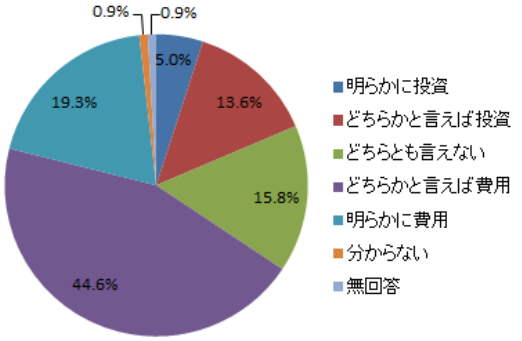

図 3　セキュリティ対策の支出の位置づけ（費用か投資か）[3]

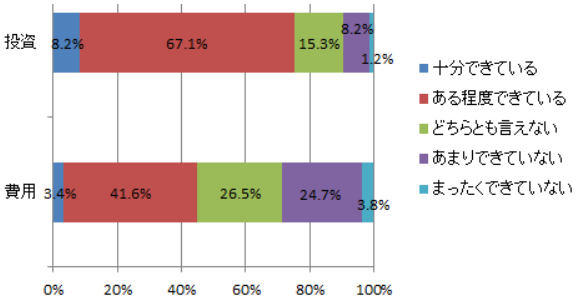

図 4　必要なセキュリティ予算の確保 [3]

経営者が行うべき重要な役割の一つとして、企業価値や競争力を向上させるために積極的な IT 投資を進めていく中で、事業の基盤として用いるシステムや営業秘密等の重要な情報に対する企業戦略上の価値・役割を認識し、サイバー攻撃によるリスク対処に係る方針を明確にすることがあげられる。IT 投資を行う際は、こうしたサイバーセキュリティリスクに備えたセキュリティ投資も同時に考える必要があり、企業価値を高めるために経営者がリーダーシップを取って企業戦略全体の中でサイバーセキュリティを考える必要がある。このような企業戦略の立案を怠ると、企業価値を高めるために IT を利活用したはずが、結果として、重大な損害を生じさせ、かえって企業の経営を揺るがす事態に発展することがありうる。

上記の背景に基づき、企業が IT の利活用を推進していく中で、経営者が認識すべきサイバーセキュリティに関する原則や、経営者のリーダーシップによって取り組むべき項目について取りまとめたサイバーセキュリティ経営ガイドラインを策定した。具体的には、経営者のリーダーシップの下での体制整備と対策の進め方、社会やステークホルダーに対する情報開示の在り方等を内容としている。なお、本ガイドラインは、企業の経営者を第一義的な読者として想定しており、本ガイドラインに基づき、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対する適切な投資が行われ、企業のサイバーセキュリティ対策強化が行われることを最大の目的としている。

本ガイドラインの適用対象は、大企業及び中小企業（小規模事業者を除く）を想定している。ただし、企業の規模やビジネスモデルによっては、本ガイドラインの適用が必ずしもサイバーセキュリティ対策として適切ではないケースもありうることから、自社の状況に応じて本ガイドラインを活用いただきたい。また、これからサイバーセキュリティ対

[3] KPMG コンサルティング「サイバーセキュリティサーベイ 2017」より経済産業省作成

策への取組を進めたいという事業者や小規模事業者においては「中小企業の情報セキュリティ対策ガイドライン[4]」もあわせて活用いただきたい。

なお、本ガイドラインの Ver1.0、及び 1.1 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 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。また、内閣サイバーセキュリティセンター（NISC）では、企業の経営層を対象としてグローバルな競争環境の変化の中でサイバーセキュリティをより積極的な経営への「投資」と位置づけ、企業の自発的な取組を促進するため、サイバーセキュリティの基本的な考え方と企業の視点別の取組方法について、考え方を示した文書（「企業経営のためのサイバーセキュリティの考え方」[5]）を策定している。本ガイドラインの取組の前提となる考え方を示した文書として、併せて活用することが期待される。

[4] 中小企業の情報セキュリティ対策ガイドライン(IPA)　https://www.ipa.go.jp/security/keihatsu/sme/guideline/
[5] 企業経営のためのサイバーセキュリティの考え方（NISC）　http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf

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) インシデント発生時に組織内で整理しておくべき事項（別紙）
D) 国際規格 ISO/IEC27001 及び 27002 との関係
E) 用語の定義

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 等に指示をすべきである。

CISO 等は、経営者の指示に基づき、重要10項目の各解説頁の「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。

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通りである。

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　インシデント発生時に原因調査等を行う際、組織内で整理しておくべき事項
付録 D　重要10項目と ISO/IEC27001、27002 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

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）[6]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。

[6] 組織における内部不正防止ガイドライン（IPA） https://www.ipa.go.jp/files/000044615.pdf

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を認識し、リーダーシップによって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に IT サービス等の提供や IT を利活用する機会は増加傾向にあり、サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としての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後、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適切な経営資源の配分を行うことが必要である。

（2）自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要

（解説）

- 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等の委託先がサイバー攻撃に対して無防備であった場合、自社から提供した重要な情報が流出してしまうなどの問題が生じうる。
- このため、自社のみならず、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等の委託先を含めたセキュリティ対策を徹底することが必要である。

（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リスクや対策に係る情報開示など、関係者との適切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。
- このため、平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにする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。

３．サイバーセキュリティ経営の重要１０項目

経営者は、CISO 等に対して、以下の10項目を指示し、着実に実施させるとともに、実施内容についてCISO 等から定期的に報告を受けることが必要である。自組織での対応が困難な項目については、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対応するための仕組みの構築
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

（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対策及び状況把握

＜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　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

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リスクの一つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定させる。

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への対応を策定し、宣言していないと、サイバーセキュリティ対策などの実行が組織の方針と一貫したものとならない。

・トップの宣言により、ステークホルダー（株主、顧客、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が、宣言がない場合は、企業におけるサイバーセキュリティへ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根拠がないこととなる。

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り、サイバーセキュリティリスクを考慮したセキュリティポリシーを策定する。その際、情報システムのみではなく、製造、販売、サービス等、事業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。

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対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。
その際、組織内のその他のリスク管理体制とも整合を取らせる。

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、組織としてサイバーセキュリティリスクの把握が出来ない。

・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恐れがある。

対策例

・CISO 等は、サイバーセキュリティリスク管理体制を構築し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構築、運用されているかを監査する。

・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リスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。

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恐れがある。

・適切な処遇の維持、改善ができないと、有能なサイバーセキュリティ人材を自社にとどめておくことができない。

対策例

・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。

・サイバーセキュリティ人材を組織内で雇用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[7]、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人材の育成が困難な場合は、外部の組織が提供するセキュリティ研修[8]等の活用などを検討する。

[7] (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。

[8] (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

経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる。
その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。

対策を怠った場合のシナリオ

・企業の経営戦略に基づき、各企業の状況に応じた適切なリスク対応を実施しなければ、過度な対策により通常の業務遂行に支障をきたすなどの不都合が生じる恐れがある。

・受容できないリスクが残る場合、想定外の損失を被る恐れがある。

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ているかを把握する。

・守るべき情報に対して、発生しうるサイバーセキュリティリスク（例えば、経営戦略上重要な営業秘密の流出による損害）を把握する。

・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：端末の持ち出し禁止（外部での盗難のリスクを回避）
　－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

・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。

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

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（防御・検知・分析に関する対策）を実施する体制を構築させる。

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、サイバー攻撃が発生した場合の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恐れがある。

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バックアップなど、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。

・アクセスログや通信ログ等からサイバー攻撃を監視・検知する仕組みを構築する。
　－検知すべきイベントを明確にし、アクセスログや通信ログから当該イベントが発生していないか、検知した場合には速やかに関係者にアラートを上げるなど適切な対処を行えるような体制を整える。
　－監視については専門的なスキルが必要となるため、自社に当該スキルを持った人材がいない場合は、外部の監視サービスを活用することも検討する。

・従業員に対する教育を行い、適切な対応が行えるよう日頃から備える。
　－従業員に対して、防御の基本となるソフトウェア更新の徹底、マルウェア対策ソフトの導入などによるマルウェア感染リスクの低減策等を実施させる。さらに定期的な対応状況の確認等を行う。
　－従業員が不審なメールを受信した場合、当該情報を報告させるとともに全従業員に対して類似のメールを開かないよう注意喚起を行う。

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

計画を確実に実施し、改善していくため、サイバーセキュリティ対策を PDCA サイクルとして実施させる。 その中で、定期的に経営者に対策状況を報告させた上で、問題が生じている場合は改善させる。 また、ステークホルダーからの信頼性を高めるため、対策状況を開示させる。

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]）を実施する体制が出来ていないと、立てた計画が確実に実行されない恐れがある。

・最新の脅威への対応ができているかといった視点も踏まえて組織のサイバーセキュリティ対策を定期的に見直さないと、サイバーセキュリティを巡る環境変化に対応できず、新たに発生した脅威に対応できない恐れがある。

・適切な開示を行わなかった場合、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とともに、インシデント発生時に企業価値が大きく低下する恐れがある。

対策例

・サイバーセキュリティリスクに継続して対応可能な体制（プロセス）を整備する（PDCA の実施体制の整備）。

・Check の実施にあたっては、「付録 A」も参考とする。

・必要に応じて、ISMS などの国際標準となっている認証を活用する。

・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、リスク分析での指摘事項数、組織内のセキュリティ教育の受講率、インシデントの発生数等が考えられる。

・必要に応じて、セキュリティ診断や監査を受け、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て開示を検討する。

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速やかに実施するための組織内の対応体制（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。 また、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恐れがあり、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に行動することが出来ない。

対策例

・緊急時において、以下を実施できるような対応体制を構築する。

－サイバー攻撃による被害を受けた場合、被害原因の特定およ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 インシデント発生時に組織内で整理しておくべき事項」も参考にすることが望ましい。

－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。再発防止策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予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きを確認しておく。

－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。

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

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。
BCP との連携等、組織全体として整合のとれた復旧目標計画を定めさせる。
また、業務停止等からの復旧対応について、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

・重要な業務が適切な時間内に復旧できず、企業経営に致命的な影響を与える恐れがある。

・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、速やかに復旧するため、関係機関との連携や復旧作業を実施できるよう指示する。また、対応担当者には復旧手順に従った演習を実施させる。

－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）。

※指示7、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望ましい。

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対策及び状況把握

監査の実施や対策状況の把握を含むサイバーセキュリティ対策の PDCA について、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等を含めた運用をさせる。 システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。

対策を怠った場合のシナリオ

・系列企業やサプライチェーンの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、加害者となる恐れもある。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、対策漏れが生じる恐れがある。

対策例

・系列企業や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のサイバーセキュリティ対策の内容を明確にした上で契約を交わす。

・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。

・個人情報や技術情報等の重要な情報を委託先に預ける場合は、委託先の経営状況等も踏まえて、情報の安全性の確保が可能であるかどうかを定期的に確認する。

・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[9]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望ましい。

・緊急時に備え、委託先に起因する被害に対するリスクマネーの確保として、委託先がサイバー保険に加入していることが望ましい。

[9] 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/

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　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

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加し、積極的な情報提供及び情報入手を行わせる。
また、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、社会全体において常に新たな攻撃として対応することとなり、企業における対応コストが低減しない。

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。

・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。

付録Ａ　サイバーセキュリティ経営チェックシート

※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[10]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対応方針（セキュリティポリシー）を策定し、宣言している　（ID.GV-1）
- □ 法律や業界のガイドライン等の要求事項を把握している　（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している　（－）
- □ 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している　（ID.GV-2）
- □ 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

- □ 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、必要な予算を確保している　（－）
- □ 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している（組織の内外問わず）　（PR.AT-2）（PR.AT-3）（PR.AT-4）（PR.AT-5）
- □ 組織内でサイバーセキュリティ人材を育成している　（PR.AT-1）
- □ 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、及び適正な処遇をしている　（－）
- □ 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している　（PR.AT-1）

[10] Framework for Improving Critical Infrastructure Cybersecurity(NIST)
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

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っている	(ID.AM-1) (ID.AM-2) (ID.AM-3) (ID.AM-4) (ID.AM-5)
□	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している	(ID.RA-3) (ID.RA-1) (ID.RM-1)
□	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している	(ID.RA-4) (ID.RA-5) (ID.RM-2)
□	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している	(ID.RA-6) (ID.RM-3)
□	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している	(ID.RA-6) (ID.RM-3)

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

□	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している。	(PR.AC) (PR.DS)
□	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している。	(PR.IP-12)
□	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）を構築している。	(DE.AE-1) (DE.AE-5) (DE.DP-3)
□	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）を策定している	(DE.AE-4) (DE.DP-1) (DE.DP-4)
□	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）を適宜見直している	(DE.DP-5)
□	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）を実施している。	(PR.AT-1)

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

□	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、把握している	(―)
□	サイバーセキュリティにかかる外部監査を実施している	(―)
□	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・維持している	(PR.IP-7)
□	サイバーセキュリティリスクや取組状況を外部に公開している	(―)

指示７　インシデント発生時の緊急対応体制の整備

□	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）	(RS.CO-3) (RS.CO-4) (RS.CO-5)
□	サイバー攻撃の初動対応マニュアルを整備している	(PR.IP-9) (RS.RP-1)
□	インシデント対応の専門チーム（CSIRT 等）を設置している	(RS.CO-1)
□	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ている	(RS.CO-2)
□	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している	(RS.IM-1) (RS.IM-2)
□	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っている	(PR.IP-10)

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

□	被害が発生した場合に備えた業務の復旧計画を策定している	(ID.BE-5) (PR.IP-9) (RC.RP-1)
□	復旧作業の課題を踏まえて、復旧計画を見直している	(RC.IM-1) (RC.IM-2)
□	組織の内外における緊急連絡先・伝達ルートを整備している	(RC.CO-1) (RC.CO-2) (RC.CO-3)
□	定期的に復旧対応訓練や演習を行っている	(PR.IP-10)

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

□	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けている	(ID.BE-3) (ID.BE-4)
□	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している	(ID.AM-6) (ID.BE-1) (PR.IP-8)
□	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、把握している	(―)

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

□	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、自社の対策に活かしている	(ID.RA-2)
□	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している	(ID.RA-2)

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情報システム部門などにおいて、本ガイドラインの重要10項目を実施する上で参考となる情報を以下に示す。各種ガイドラインの公開URLも示すが、ガイドラインは更新される可能性があるため、適宜最新版を参照することが望ましい。

重要１０項目全般に関連する参考情報

- サイバーセキュリティ経営ガイドライン解説書 [Ver.1.0]（IPA）
  （サイバーセキュリティ経営ガイドラインの3原則、重要10項目を具体的に実施するための考え方について解説。）
  https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html
- 中小企業の情報セキュリティ対策ガイドライン [第 2.1 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、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」等の付録も提供。)
  https://www.ipa.go.jp/security/keihatsu/sme/guideline/
- ISO/IEC 27002:2013（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 1.0]（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/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
- SP800-53 [Rev.4]（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。）
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- SP800-171 [Rev.1]（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[11]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。）
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

[11] 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 [2015 年 5 月]（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

○ 中小企業の情報セキュリティ対策ガイドライン [第 2.1 版]（IPA）

（本ガイドラインの 4 章にてリスク分析の手法を解説。また、リスク分析の実施を支援するリスク分析シートも付録して提示。）

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

指示５に関連する参考情報

○ 「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 [1.0 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 4 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/files/000057060.pdf

○ 秘密情報の保護ハンドブック [平成 28 年 2 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。）

http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.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。）

http://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。）

http://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

○ 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/

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。）

http://www.nca.gr.jp/activity/build-wg-document.html

指示８に関連する参考情報

○ 事業継続ガイドライン [平成 25 年 8 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。）

http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03.pdf

指示９に関連する参考情報

○ 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。）

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

○ 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/

指示１０に関連する参考情報

○ 届出・相談・情報提供（不正アクセスやウイルス等に関する届出） （IPA）

（コンピュータウイルス、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/

○ @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　国際規格 ISO/IEC27001 及び 27002 との関係

重要１０項目	ISO/IEC 27001（●）、ISO/IEC 27002（・）
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　リーダーシップ及びコミットメント ●5.2　方針
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　リスク及び機会、責任及び権限 ・6.1.1　情報セキュリティの役割及び責任
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　資源 ●7.2　力量
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　リスク及び機会に対処する活動 ●6.2　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 ・5.1.1　情報セキュリティのための方針群 ・5.1.2　情報セキュリティのための方針群のレビュー
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	・6.2　モバイル機器及びテレワーキング ・9　アクセス制御 ・10　暗号 ・11　物理的及び環境的セキュリティ ・12　運用のセキュリティ ・13　通信のセキュリティ
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　コミュニケーション ●8.1　運用の計画及び管理 ●8.2　情報セキュリティリスクアセスメント ●8.3　情報セキュリティリスク対応 ●9.1　監視、測定、分析及び評価 ●9.2　内部監査 ●9.3　マネジメントレビュー ●10.1　不適合及び是正処置 ●10.2　継続的改善 ・17.1.1　情報セキュリティ継続の計画 ・17.1.2　情報セキュリティ継続の実施 ・17.1.3　情報セキュリティ継続の検証、レビュー及び評価 ・18.1.1　適用法令及び契約上の要求事項の特定 ・18.2.1　情報セキュリティの独立したレビュー ・18.2.2　情報セキュリティのための方針群及び標準の順守 ・18.2.3　技術的順守のレビュー
指示７　インシデント発生時の緊急対応体制の整備	・16.1.1　責任及び手順 ・16.1.2　情報セキュリティ事象の報告 ・16.1.3　情報セキュリティ弱点の報告 ・16.1.4　情報セキュリティ事象の評価及び決定 ・16.1.5　情報セキュリティインシデントの対応
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	・17.1.1　情報セキュリティ継続の計画 ・17.1.2　情報セキュリティ継続の実施 ・17.1.3　情報セキュリティ継続の検証、レビュー及び評価
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　運用の計画及び管理 ・15.1.1　供給者関係のための情報セキュリティの方針 ・15.1.2　供給者との合意におけるセキュリティの取扱い ・15.1.3　ICT サプライチェーン ・15.2.1　供給者のサービス提供の管理及びレビュー ・15.2.2　供給者のサービス提供の変更に対する管理
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	・6.1.3　関係当局との連絡 ・6.1.4　専門組織との連絡

付録Ｅ　用語の定義

（1）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。

（2）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）または外部監査（第二者・第三者）のいずれでも、または複合監査（複数の分野の組合せ）でもあり得る。

（3）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。

（4）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。

（5）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。

（6）残留リスク

リスク対応（回避、低減、移転）後に残るリスク。保有リスクともいう。

（7）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）

(8) 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また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。

(9) 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。

(10)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での制限、④事後対応の準備。

(11)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。

(12)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。

(13)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。

(14)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または増加させる、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。

(15)リスク評価

リスクの大きさが、受容可能かまた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および内部環境に基づいたもの)と比較するプロセスのこと。

(16)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。

(17)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。

(18)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。

（19）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。

（20）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。

（20）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通り行われて、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。

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

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