サイバーセキュリティ経営ガイドライン

Ver 1.10

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

１．サイバーセキュリティは経営問題

○ 顧客の個人情報を収集・活用する、営業秘密としての技術情報を活用する、プラントを自動制御する、など様々なビジネスの現場において、IT の利活用は企業の収益性向上に不可欠なものとなっている。

○ 一方、こうしたビジネスを脅かすサイバー攻撃は避けられないリスクとなっている。純利益の半分以上を失うような攻撃を受けた企業も存在するなど、深刻な問題を引き起こすこともある。そして、その防衛策には、セキュリティへの投資が必要となる。つまり、企業戦略として、IT に対する投資をどの程度行うのか、その中で、どの程度、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という企業価値のためにセキュリティ投資をすべきか、経営判断が求められる。

○ また、サイバー攻撃により、個人情報や安全保障上の機微な技術の流出、インフラの供給停止など社会に対して損害を与えてしまった場合、社会から経営者のリスク対応の是非、さらには経営責任が問われることもある。

○ 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）のうち、IT に関する製品やシステム、~~や~~サービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業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、２．経営者が認識する必要がある「３原則」、及び３．経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO（最高情報セキュリティ責任者：企業内で情報セキュリティを統括する担当役員）等）に指示すべき「重要１０項目」をまとめたものである。

２．経営者が認識する必要がある「３原則」

(1) 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。~~セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。~~このため、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう。

(2) 子会社で発生した問題はもちろんのこと、自社から生産の委託先などの外部に提供した情報がサイバー攻撃により流出してしまうことも大きなリスク要因となる。このため、自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要である。

(3) ステークホルダー（顧客や株主等）の信頼感を高めるとともに、サイバー攻撃を

受けた場合の不信感を抑えるため、平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要である。

３.情報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」

指示１：サイバーセキュリティリスクへの対応について、組織の内外に示すための方針（セキュリティポリシー）を策定すること。

指示２：方針に基づく対応策を実装できるよう、経営者とセキュリティ担当者、両者をつなぐ仲介者としての CISO 等からなる適切な管理体制を構築すること。その中で、責任を明確化すること。

指示３：経営戦略を踏まえて守るべき資産を特定し、セキュリティリスクを洗い出すとともに、そのリスクへの対処に向けた計画を策定すること。

指示４：計画が確実に実施され、改善が図られるよう、PDCA を実施すること。また、対策状況については、CISO 等が定期的に経営者に対して報告をするとともに、ステークホルダーからの信頼性を高めるべく適切に開示すること。

指示５：系列企業やサプライチェーンのビジネスパートナーを含め、自社同様に PDCA の運用を含むサイバーセキュリティ対策を行わせること。

指示６：PDCA の運用を含むサイバーセキュリティ対策の着実な実施に備え、必要な予算の確保や人材育成など資源の確保について検討すること。

指示７：IT システムの運用について、自社の技術力や効率性などの観点から自組織で対応する部分と他組織に委託する部分の適切な切り分けをすること。また、他組織に委託する場合においても、委託先への攻撃を想定したサイバーセキュリティの確保を確認すること。

指示８：攻撃側のレベルは常に向上することから、情報共有活動に参加し、最新の状況を自社の対策に反映すること。また、可能な限り、自社への攻撃情報を公的な情報共有活動に提供するなどにより、同様の被害が社会全体に広がることの未然防止に貢献すること。

指示９：サイバー攻撃を受けた場合、迅速な初動対応により被害拡大を防ぐため、CSIRT（サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対処するための組織）の整備や、初動対応マニュアルの策定など緊急時の対応体制を整備すること。また、定期的かつ実践的な演習を実施すること。

指示１０：サイバー攻撃を受けた場合に備え、被害発覚後の通知先や開示が必要な情

報項目の整理をするとともに、組織の内外に対し、経営者がスムーズに必要な説明ができるよう準備しておくこと。

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~~を狙う~~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~~る~~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）。また、特定の組織を狙う標的型攻撃を中心としてその手口が巧妙化しており、~~インシデント~~サイバー攻撃の発覚経緯の約７割は外部からの指摘によるものといったように（図２）、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。~~攻撃を受けたこと自体に気づかないことが多い。~~

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空間にも及ぶようになっている。

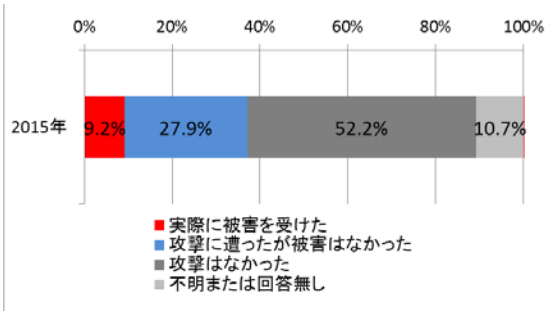
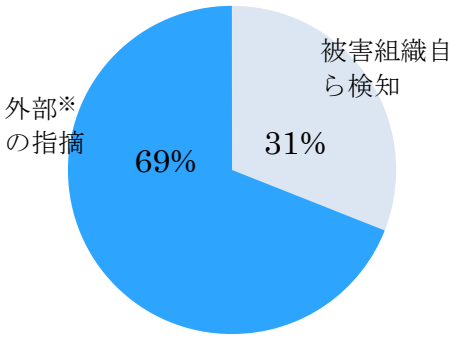


図１　サイバー攻撃（ウイルス以外）被害を受けた企業の割合）[1]



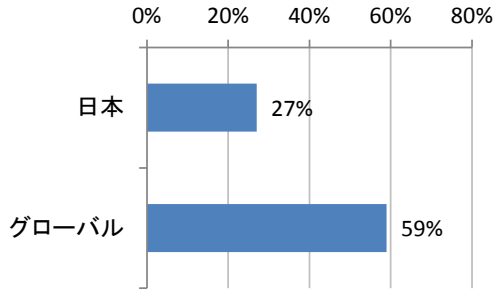
※取引先、顧客、捜査当局等

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。我が国においては、積極的にセキュリティ対策を推進する経営幹部が諸外国より大幅に少ない（図３）。また、諸外国では、大半の企業が、サイバー攻撃への対応について取締役レベルで議論すべきと考えているのに対し、我が国においては、意識の高まりは見られるものの諸外国と比較するとまだ低い傾向にある~~多くの企業がそのような考えを有していない~~（図４）。

[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」~~情報セキュリティ事象被害状況調査―報告書―~~より経済産業省作成

[2]ファイア・アイ(株)「M-trends2015：セキュリティ最前線からの視点」より経済産業省作成



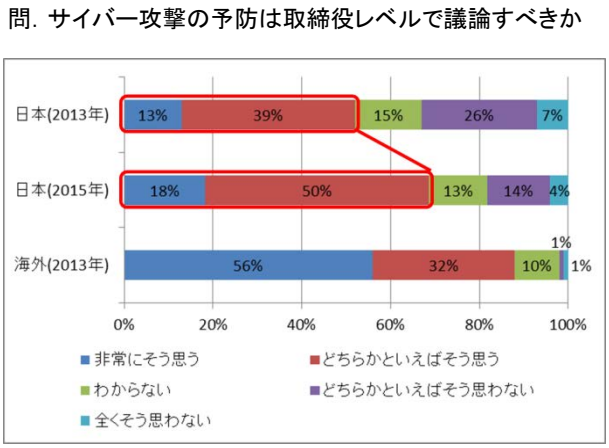


図 3　積極的にセキュリティ対策を推進する経営幹部がいる企業 [3]

図 4　サイバー攻撃への対処を議論するレベル [4]

企業の競争力を向上させる上で不可欠な積極的な 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重要な情報の事業戦略上の価値・役割を認識し、サイバー攻撃によるリスクへの対処に係る判断を行うことは、経営者が行うべき重要なの役割の一つである。そして、こうしたサイバーセキュリティリスクについて備えたセキュリティ投資は必要不可欠であるもののは、セキュリティ投資へのリターンが見えにくい性質のものであるため、経営者がリーダーシップを取らなければ、積極的に話が上がりな対策がされにくいものである。このため、結果として、企業として十分な備え対策ができず、また、万が一重大な事象が発生した場合、企業としての対応が後手にまわり、気づかないうちに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 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、このガイドラインに基づき、経営者のリーダーシップの下で企業自らがサイバーセキュリティの対応強化に取り組むことを最大の目的としている。

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）のうち、IT に関する製品やシステム、やサービス等を供給する企業及び経営戦略上 IT の利活用が不可

[3] プライスウォーターハウスクーパース(株)「2014 Global State of Information Security Survey 」より経済産業省作成

[4] KPMG ジャパン「サイバーセキュリティサーベイ 2013」、「サイバーセキュリティサーベイ 2016」KPMG Insight 日本におけるサイバー攻撃の状況と課題－セキュリティサーベイ 2013 から－」より経済産業省作成

欠である企業を想定している。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。

なお、本ガイドラインは、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」において検討が行われ、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のガイドを示した文書（「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。

[5] NISC ウェブサイトからダウンロードが可能（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章及び付録Aは情報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、それ以外の付録はセキュリティ担当者向けの参考資料である。

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．サイバーセキュリティ経営の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) 望ましい技術対策
C) 国際規格 ISO/IEC27001 及び 27002 との関係
D) 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、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、各重要10項目が、形式上のみならず、実態上、適切に実施されているかどうか確認し、その状況を経営者に対して報告をすることが求められる。こうした確認が可能となるよう付録 A のチェックシートをまとめている。

また、必ずしも経営者が全ての確認を行う必要はないものの、技術対策の観点から、CISO 等の指示によりセキュリティ担当者が実施することが望ましい項目を付録 B にまとめた。企業のセキュリティ担当者が、CISO 等と具体的な技術対策について説明や相談をする際の参考資料となることを期待している。

付録 C に参考として、国際規格 ISO/IEC27001 及び 27002 との関係を示した。実施すべき対策の確認や、経営者への各項目の検討・実施状況等の報告に活用することが可能である。

付録 D に、本ガイドラインに使われている用語の解説をしており、経営者向けに資料を作成する場合などに活用することが可能である。

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。

[6] IPA ウェブサイトからダウンロードが可能（https://www.ipa.go.jp/files/000044615.pdf）

２．サイバーセキュリティ経営の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、IT 活用を推進する中で、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。~~セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。~~
- 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のリスクとして、~~サイバーセキュリティリスクを経営リスクの中に~~適切に位置づけ、その~~対応について組織の内外に~~対応方針~~指針~~を組織の内外に明確に示しつつ、経営者自らがリーダーシップを発揮して経営資源を用いて対策を講じることが必要である。その際、変化するサイバーセキュリティリスクへの対応や、被害を受けた場合の経験を活かした再発防止も必要である。

（２）自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、IT システム管理の委託先を含めた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 IT システム管理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。
- 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 IT システム管理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、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

（解説）

- 事業のサイバーセキュリティリスクへの対応等に係る情報開示により、関係者や取引先の信頼性を高める。
- 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，関係者や取引先の不信感の高まりを抑え、説明を容易にすることができる。また、サイバー攻撃情報（インシデント情報）を共有することにより、同様の攻撃による他社への被害の拡大防止に役立つことを期待できる。
- 事業のサイバーセキュリティリスク対応として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、着実に実施させることが必要である。

1. リーダーシップの表明と体制の構築

（1） サイバーセキュリティリスクの認識、組織全体での対応の策定

（2） サイバーセキュリティリスク管理体制の構築

2. サイバーセキュリティリスク管理の枠組み決定

（3） サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定

（4） サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示

（5） 系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握

3. ~~リスクを踏まえた~~サイバー攻撃を防ぐための事前対策

（6） 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） IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保

（8） 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のための環境整備

4. サイバー攻撃を受けた場合に備えた準備

（9） 緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施

（10） 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

３．１．リーダーシップの表明と体制の構築

（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）を策定していますか？

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、宣言することにより、組織のすべての構成員にサイバーセキュリティリスクに対する考え方を周知することができる。宣言がないと、構成員による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、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マネジメントを考慮した~~の方針（~~セキュリティポリシー~~）~~を策定する。

（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、経営者とセキュリティ担当者をつなぐ仲介者としての CISO 等からなる適切なサイバーセキュリティリスクの管理体制の構築は出来ていますか？
各関係者の責任は明確になっていますか？
また、防犯対策など組織内のその他のリスク管理体制と整合をとらせていますか？

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が整備されていない場合、サイバーセキュリティリスクの把握が出来ない。

・CISO 等が任命され、権限を付与されていないと、技術的観点と事業戦略の観点からサイバーセキュリティリスクをとらえることができない。仮にサイバー攻撃を受け、事業の継続性に支障が生じるようなシステム停止等の判断が必要な局面において、経営者レベルでの権限が付与されていないと、適時適切な対応ができない。また、責任の所在が不明となる。

・組織内におけるリスク管理体制など他の体制との整合を取らないと、同様の活動を重複して実施することになり、また関連情報の共有ができず、非効率である。

・万が一、インシデントが発生した場合、組織としての対応ができず、被害の状況の把握、原因究明、被害を抑える手法、インシデント再発の防止などの対策を組織として取ることができない。

対策例

・組織内に経営リスクに関する委員会を設置し、サイバーセキュリティリスクに責任を持った者が参加する体制とする。

・組織の対応方針（セキュリティポリシー）に基づき、CISO 等の任命及び、組織内サイバーセキュリティリスク管理体制を構築する。

・CISO 等には、組織の事業戦略を把握するため取締役会への参加及び緊急時のシステム停止等の経営者レベルの権限を付与することを検討する。

・取締役、監査役はその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。

３．２．サイバーセキュリティリスク管理の枠組み決定

（３）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定

サイバー攻撃の脅威に対し、経営戦略の観点から、守るべき資産を特定させた上で、社内ネットワークの問題点などのサイバーセキュリティリスクを把握させていますか？
その上で、暗号化やネットワークの分離など複数のサイバーセキュリティ対策を組み合わせた多層防御など、~~やネットワークの分離などの~~リスクに応じた対策の目標と計画を策定させていますか？
また、サイバー保険の活用や守るべき資産について専門企業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ていますか？

対策を怠った場合のシナリオ

・IT を活用するすべての企業・組織は、何らかのサイバーセキュリティリスクを抱えている。ただし、リスクは、企業の守るべき資産（個人情報や重要技術等）の内容や現在の企業・組織内のネットワーク環境などによって企業ごとに異なる。

・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策をしなければ、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。

・受容できない残留リスクが残る場合、想定外の損失を被る恐れがある。

対策例

・経営戦略に基づくさまざまな事業リスクの一つとして、サイバー攻撃に伴うリスク（例えば、戦略上重要な営業秘密の流出による損害）を識別する。

・識別したリスクに対し、実現するセキュリティレベルを踏まえた対策の検討を指示する。その際、IT への依存度を把握した上で、セキュリティの三要件（機密性、完全性、可用性）の観点からリスクを分析する。その結果、リスク低減、回避、移転（サイバー保険の活用や守るべき資産について専門企業への委託等）が可能なものについてはリスク対応~~管理~~策を実施する。例えば、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を実施する。また、重要業務を行う端末、ネットワーク、~~情報~~ IT システム又は~~情報~~ IT サービス（クラウドサービスを含む）には、~~多層防御の導入や~~暗号化や情報資産別のネットワークの分離等の多層防御の実施を検討する。

（４）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示

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として実施するフレームワークを構築させていますか？
その中で、監査（または自己点検）の実施により、定期的に経営者に対策状況を報告させた上で、必要な場合には、改善のための指示をしていますか？
また、ステークホルダーからの信頼性を高めるため、対策状況について、適切な開示をさせていますか？

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]）を実施するフレームワークが出来ていないと、立てた計画が確実に実行されない恐れがある。また、組織のサイバーセキュリティ対策の状況を、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つつ正しく把握し、対策を定期的に見直すことが必要。これを怠ると、サイバーセキュリティを巡る環境変化に対応できず、対策が陳腐化するとともに、新たに発生した脅威に対応するための追加的に必要な対策の実施が困難となる。

・適切な開示が行われなかった場合、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不安感や不信感を惹起させるとともに、リスクの発生時に透明性をもった説明ができない。また、取引先や顧客の信頼性が低下することによって、企業価値が毀損するおそれがある。

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）。なお、その他の内部統制に係る PDCA のフレームワークが存在する場合には、当該フレームワークとの連動も含め、効率的に実施することも可能である。

・重点項目（2）で設置した経営リスクに関する委員会において、PDCA の実施状況について報告すべき時期や内容を定め、経営者への報告の機会を設けるとともに、新たな環境変化によるサイバーセキュリティリスクが生じていないかを確認する。

・必要に応じて監査を受け、現状の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、速やかに対処方針の修正を指示する。

・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への取組みを踏まえたリスクの性質・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。

（５）系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握

自社のサイバーセキュリティが確保されるためには、系列企業やサプライチェーンのビジネスパートナーを含めてサイバーセキュリティ対策が適切に行われていることが重要。このため、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、系列企業やサプライチェーンのビジネスパートナーを含めた運用をさせていますか？

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次被害の誘因となる恐れや、加害者になる恐れもある。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。

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のサイバーセキュリティ対策の内容を契約書等で合意する。

・系列企業やサプライチェーンのビジネスパートナー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。

３．３．~~リスクを踏まえた~~サイバー攻撃を防ぐための事前対策

（６）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は出来ていますか？
また、サイバーセキュリティ人材の育成や適切な処遇をさせていますか？

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の事前対策を明確にし、それに要する費用を明らかにするよう、指示を行う。

・セキュリティ担当者以外も含めた従業員向け研修等のための予算を確保し、継続的にセキュリティ教育を実施する。

・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た上で、予算として承認を得る。

・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。

・組織内人事部門に対して、組織内の IT 人材育成の戦略の中で、セキュリティ人材育成、キャリアパス構築を指示し、内容を確認する。

（７）IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保

サイバーセキュリティ対策を効率的かつ着実に実施するため、リスクの程度や自組織の技術力などの実態を踏まえ、IT システムの管理等について、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ていますか？また、IT システム管理を外部委託する場合、当該委託先へのサイバー攻撃等も想定し、当該委託先のサイバーセキュリティの確保をさせていますか？

対策を怠った場合のシナリオ

・IT システムなどの運用について、自組織に技術がない場合はシステム管理を十分に行えず、システムに脆弱性が残り、その脆弱性を突いた攻撃を受ける恐れが高まる。

・委託先のサイバーセキュリティリスク対応が事業にリスクを及ぼす状況であると、自社のみが対応をしてもリスクにさらされる恐れがある。

対策例

・自組織の技術力を踏まえ、各対策項目を自組織で対応できるかどうか整理する。

・委託先のサイバーセキュリティリスク対応を徹底するため、委託先のセキュリティレベルを契約書等で合意し、それに基づいて委託先の監査を実施する。

・個人情報や技術情報などの重要な資産を委託先に預ける場合は、委託先の経営状況などを踏まえて、資産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。

（８）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のための環境整備

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の参加と、入手した情報を有効活用するための環境整備をさせていますか？

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、全体最適化ができない。

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、積極的な情報提供が望ましい。

・IPA やー般社団法人 JPCERT コーディネーションセンター等による注意喚起情報を、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~~に基づく「ウイルス~~マルウェア情報や不正アクセス情報~~」~~の~~について~~届出をする。

・一般社団法人 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。

３．４．サイバー攻撃を受けた場合に備えた準備

（９）緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施

適切な初動対応により、被害拡大防止を図るため、迅速に影響範囲や損害を特定し、IT システムを正常化する手順を含む初動対応マニュアル策定や組織内の CSIRT 構築など対応体制の整備をさせていますか？また、定期的かつ実践的な演習を実施させていますか？

対策を怠った場合のシナリオ

・緊急時の対応体制が整備されていないと、原因特定のための調査作業において、組織の内外の関係部署間の情報の共有やコミュニケーションが取れず、速やかな原因特定、応急処置を取ることができない。

・緊急時は、定常業務時と異なる環境となり規定された通りの手順を実施することが容易でないことが多い。演習を実施していないと、担当者は、緊急時に適切に行動~~手順を実際に再確認~~することが出来ない。

対策例

・企業の組織に合わせた緊急時における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、関係機関との連携や、ログの調査を速やかにできるようにしておくよう指示する。また、対応担当者にはサイバー攻撃に対応する演習を実施する。なお、インシデント収束後の再発防止策の策定も含めて訓練を行うことが望ましい。

・緊急連絡網を整備する。その際には、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などの連絡先も含める。

・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。

・訓練においては技術的な対応のみならず、プレスリリースの発出や、所管官庁等への報告手順も含めて想定する。

（１０）被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

外部に対して迅速な対応を行うため、被害の発覚後の通知先や開示が必要な情報について把握させていますか？また、情報開示の際、経営者が組織の内外への説明が出来る体制の整備をさせていますか？

対策を怠った場合のシナリオ

・速やかに通知や注意喚起が行われない場合、顧客や取引先等へ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、所管官庁への報告等が義務付けられている場合、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。

・組織内情報管理の責任者である経営者が感染被害を発表しないと、ステークホルダーに対し、組織としての責任を明らかにすることができない。

対策例

・サイバー攻撃の被害が発覚後、速やかに通知や注意喚起が行えるよう、通知先の一覧や通知用のフォーマットを作成し、対応に従事するメンバーに共有しておく。また、情報開示の手段について確認をしておく。

・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。

・経営者が組織の内外への発表を求められた場合に備えて、~~サイバーセキュリティ~~インシデントに関する被害状況、他社への影響などについて経営者に報告を行う。

・インシデントに対するステークホルダーへの影響を考慮し、速やかにこれを公表する。

・社外への公表は、インシデントや被害の状況に応じて、初期発生時、被害状況把握時、インシデント収束時など、それぞれ適切なタイミングで行う。

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

(1) サイバーセキュリティリスクの認識、組織全体での対応の策定

□経営者がサイバーセキュリティ~~の~~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~~で~~のサイバーセキュリティリスク~~を~~考慮した~~に対する~~対応方針（セキュリティポリシー）を策定し、宣言している

(2) サイバーセキュリティリスク管理体制の構築

□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~~が構築している~~されている~~

□サイバーセキュリティリスク管理体制において、各関係者の責任~~を~~が明確にしている~~なっている~~

□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

(3) サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定

□守るべき資産を特定している

□特定した守るべき資産に対するサイバー攻撃の脅威を識別し、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

□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

□サイバーセキュリティリスクの影響の度合いに従って、低減、回避のための目標や計画を策定している

□低減策、回避策を取らないと判断したサイバーセキュリティリスクの移転策（サイバー保険の活用や守るべき資産について専門企業への委託等）を実施している

□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~~受容または~~残留リスクとして識別している

~~□残留リスクの移転策（サイバー保険の活用や守るべき資産について専門企業への委託等）を実施している~~

⑷ サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示

□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

□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

⑸ 系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握

□系列企業や、サプライチェーンのビジネスパートナー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

⑹ 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ている（組織の内外問わず）

□組織内でサイバーセキュリティ人材を育成している

□組織内のサイバーセキュリティ人材のキャリアパスを構築し、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

⑺ IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保

□IT システムの管理等について、自組織で対応できる部分と外部に委託する部分で適切な切り分けをしている

□委託先へのサイバー攻撃を想定し、委託先のサイバーセキュリティを確保している

⑻ 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のための環境整備

□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を行い、自社の対策に活かしている

□マルウェア~~ウイルス~~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

(9) 緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施

□組織の内外における緊急連絡先・伝達ルート~~が~~を整備している~~されている~~
（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）

□他の災害と同様に、サイバー攻撃の初動対応マニュアル~~が~~を整備している~~されている~~

□~~サイバー~~インシデント対応の専門チーム（CSIRT 等）~~が~~を設置している~~されている~~

□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

(10) 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

□組織外の報告先（ステークホルダーや所管官庁等を含む）をリスト化している

□開示・報告すべき情報を把握・整備している

□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について事前に検討している~~されている~~

付録Ｂ　望ましい技術対策と参考文献（注：これらは現時点における対策の例示であり、環境の変化や各企業の状況により、変更されるものである）

経営層と技術的対策を担当する情報システム部門などとの間において、以下のような対策項目や実施しないことのリスク、参考文献等があることを共通認識し、担当部門の検討・要請に基づき、実施に必要なリソースの手配を経営層が検討することが望まれる。

技術的対策の例については、別途「付録Ｂ－２」に記載するため、情報システム部門の担当者など、対策の実施担当者の参考としていただきたい。

経営ガイドラインの各項目	項目の実現に有効な技術的対策項目	対策をしないことのリスクや対策を実施する効果	参考ガイド、文献、ツール類
（３）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定	**防御対象の特定とリスクの把握** 事業を継続する上で、または法令及び業界内の安全基準等に遵守するために組織として守るべき資産（重要情報、個人情報など）の特定や組織内ネットワーク構成やその問題点などリスクの把握を行うこと。	● 守るべき資産（重要情報や個人情報など）を予め定めていなかった場合、緊急時の対応をすみやかに判断できず、優先的な対応ができない。 ● 組織内ネットワーク構成の把握を怠っていた場合、初動対応時に重要情報などを適切に守る対策が立てられないため、時間の浪費及び被害拡大を招き、また、被害範囲の特定と原因究明（どこから侵入されているのか）ができないため、事態の長期化を招く	
	多層防御措置の実施 マルウェア感染の予防のみならず、感染後の被害回避・低減のために複数の対策を多層に重ねる「多層防御措置」を行うこと。	● 感染防止対策（マルウェア対策ソフト）のみ実施している場合、未知のマルウェアに感染すると、被害をくい止めることができない。 ● マルウェア対策ソフトやネットワーク出口へのファイヤーウォール導入のような１つの機器やソフトウェアに依存するだけではなく、ネットワーク全体での対策を心がけ、侵入→感染→拡	【ガイド】 IPA『「高度標的型攻撃」対策に向けたシステム設計ガイド』 IPA『2015 年 6 月 2 日【注意喚起】ウイルス感染を想定したセキュリティ対策と運用管理を』 『情報セキュリティ 10 大脅威 2015（1 章対策の基本）』

		大という攻撃フェーズに応じた拡大防止及び緩和を図れる柔軟な対策実施が必要である。 ● ネットワーク出入り口に設置される機器の各種ログが記録・保存され、またこれを内部あるいは外部監視サービスにより定期的にチェックされていない場合、不正な通信の発生を検知することができない。	『組織における内部不正防止ガイドライン』 【ガイド】 JPCERT/CC『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』 IPA『iLogScanner』
（４）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示	**PDCA サイクルの実施と改善** ISMS の導入やセキュリティ監査の実施による PDCA サイクルの実施により、現状のセキュリティ対策の改善点を洗い出し、将来の改善計画を立案し実行していくこと。	● 環境や事業の変化に合わせて、対策の点検や改善を継続していない場合、新たな脅威に対抗できなくなる恐れがある。	【制度】 JIPDEC『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『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』 経済産業省『情報セキュリティ監査制度』 【ツール】 IPA『情報セキュリティ対策ベンチマーク』

	各種セキュリティ診断の実施 内部におけるセキュリティ対策レビューのほか、専門企業のサービスやツールによるウェブアプリケーションの脆弱性診断やプラットフォーム脆弱性診断を活用し、既存の脆弱性への対処状況の確認や対策実施を行う。	● 日々、多くの脆弱性が発見され、セキュリティパッチも数多く公開されることから、~~I T~~IT システムの規模が大きくなった場合、対策漏れが発生する恐れがある。 ● セキュリティ上の欠陥を定期的に検査しなかった場合、その欠陥の把握・対処が遅れることで、第三者に悪用されてマルウェア感染等の被害が発生してしまう。	【文献】 IPA『安全なウェブサイトの作り方』（ほか『別冊：ウェブ健康診断仕様』） IPA『ウェブサイトにおける脆弱性検査手法の紹介（ウェブアプリケーション検査）』 【ツール】 IPA MyJVN バージョンチェッカ 【参考】 JNSA『JNSA ソリューションガイド』
（５）系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握			【ガイド】 経済産業省『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』 JASA『サプライチェーン情報セキュリティ管理ガイド』
（６）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			【ガイド】 IPA『情報セキュリティ強化対応スキル指標』 IPA『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『職場の情報セキュリティ管理者の育成検討』

（7）IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保	**自組織で対応できる対策項目とできない項目の整理** 感染端末の調査など自組織では技術的に対応が困難なものについては外部専門機関、セキュリティベンダの力を借りることを予め想定し、①自組織で対応できること、②外部に依頼が必要なこと、を予め切り分けること。また、そのための予算も予め確保すること。	● 自組織で対応が困難である、高度な解析作業等が実施されない場合、原因究明と被害範囲の確定ができず、事態が長期化または第二波、第三波の攻撃を許してしまう恐れがある。	
（8）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のための環境整備	**情報共有活動や公的機関などからの提供情報の活用** サイバー攻撃への備えが十分か（世間並みかどうか）判断するために、サイバー攻撃に関する情報共有活動への参加や、公的機関や専門企業が発進する情報を活用すること。また、情報の入手のみならず、情報の提供活動も積極的に行うこと。	● サイバーセキュリティの分野は攻撃者、防御側ともに日進月歩であり、最新の攻撃手法などの情報を定期的に入手しないと自組織に必要な対策レベルが判断できない。 ● 情報共有や提供活動への参加が不足していた場合、業界全体での対処能力の低下を招いてしまう恐れがある。	＜制度等＞ IPA『コンピュータウィルス、不正アクセス、脆弱性関連情報に関する届出』 IPA『標的型サイバー攻撃特別相談窓口』 IPA『サイバー情報共有イニシアティブ（J-CSIP）』 JPCERT/CC『インシデントの報告』、『早期警戒情報の提供』、『日本シーサート協議会』 警察庁『@police』 https://www.npa.go.jp/cyberpolice/

（９）緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施	**緊急時のための「体制整備」と「被害特定のための準備」** ・日頃から攻撃を検知・記録する仕組みを構築し、検知時の対応手順を用意しておくこと。 ・確実に影響範囲・損害を特定し、ネットワーク正常化に着手できる準備や経営層へのエスカレーション手順、ルートを用意すること。 ・影響範囲の特定については、機器・ソフトウェアの機能だけに頼り切らず、セキュリティ専門家を含めた判断を行うこと。 ・外部機関からの攻撃情報提供・被害状況確認の問合せに対応する窓口、手順を日頃から用意すること。	● 対応体制、連絡／報告手順、対応手順が決められていない場合、攻撃に気付かない、感染被害範囲の判断、PC 端末の隔離・インターネット接続遮断等の判断の遅れを引き起こし、結果として初動対応に失敗し、通常業務やサービス提供への復帰が遅れ、また、組織の社会的責任の追及や訴訟、信用の失墜につながる。 ● 感染端末やマルウェアが残存していた場合、再度情報漏えい等が発生し、事象が長期化する。 ● 外部との通信が確認されていても適切な機器において、適切な期間におけるログが保存されていなければ、いつ、どのぐらいの端末が感染していたのか被害範囲を確認することができない。	＜体制整備＞ JPCERT/CC 『CSIRT 構築マテリアル』 日本シーサート協議会 『CSIRT スターターキット』 ＜攻撃検知・被害特定＞ IPA『潜伏しているかもしれないマルウェアの感染検査を今すぐ！』 JPCERT/CC『Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起』 JPCERT/CC『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』
	定期的な職員への訓練実施 インシデント対応訓練や標的型攻撃の訓練を実施すること。メールを開封したことを責めるのではなく、不審メールの受付窓口へ届出することが重要であることを徹底すること。	● 訓練をしない場合、攻撃者の組織内への侵入を簡単に許してしまう。 ● 標的型メールを誰かがひらいてしまうことはやむなしと認識する。訓練において不審メールを開封したことを責めると、本物の不審メールが届いた場合に届出がされず結果として被害拡大に繋がる。	

付録C　国際規格 ISO/IEC27001 及び 27002 との関係

	ISO/IEC 27001(●)、ISO/IEC 27002(・)
(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
(2) サイバーセキュリティリスク管理体制の構築	●5.3 組織の役割、責任及び権限 ・6.1.1 情報セキュリティの役割及び責任
(3) サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定	●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
(4) サイバーセキュリティ対策フレームワーク構築(PDCA)と対策の開示	●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
(5) 系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握	●8.1 運用の計画及び管理
(6) 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
(7) ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保	●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
(8) 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のための環境整備	・6.1.3 関係当局との連絡 ・6.1.4 専門組織との連絡
(9) 緊急時の対応体制(緊急連絡先や初動対応マニュアル、CSIRT)の整備、定期的かつ実践的な演習の実施	・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
(10) 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備	・6.1.3 関係当局との連絡 ・6.1.4 専門組織との連絡

付録Ｄ　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

~~監査基準が満たされている程度~~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リスク

サイバーセキュリティとは、サイバー攻撃により、情報の漏えいや、期待されていた IT システム等の機能が果たされないといった~~等の~~不具合が生じないようにすること。サイバーセキュリティリスクとは、そうした不具合が生じ、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。

（5）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。

（6）情報セキュリティ

情報の機密性、完全性、可用性を維持すること。

（7）情報セキュリティ報告書

企業の情報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。

~~（8）~~（9） セキュリティポリシー(情報セキュリティ基本方針)

企業・組織における情報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。

~~（9） 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。~~

（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

情報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。

~~（12）~~（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、リスク減の除去、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、脆弱性に対して情報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、従業員に対する情報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。

~~(13)~~(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。

~~(14)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。~~

~~(15)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、JISQ0073 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、リスク減の除去、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、脆弱性に対して情報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、従業員に対する情報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、組織内の情報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。~~

~~(16)マルウェア~~

~~情報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。~~

(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。情報セキュリティ上、インシデントの原因追究などに利用する。

（18）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、情報セキュリティ対策を実施する上での責任者のこと。

（19）CSIRT（Computer Security Incident Response Team）

本ガイドラインでは、~~サイバーセキュリティ~~インシデントの発生に対応するための体制のこと~~とする~~。

参考：CSIRT 構築マテリアル（一般社団法人 JPCERT コーディネーションセンター）

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

日本シーサート協議会　http://www.nca.gr.jp/

CSIRT スターターキット（日本シーサート協議会）

http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

CSIRT 構築に役立つ参考資料（日本シーサート協議会）

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

（20~~19~~）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

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
○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 ICT 研究センター　次世代個人認証技術講座　特任准教授

※○は委員長

（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~~情報セキュリティ政策室~~サイバーセキュリティ課