令和5年度
中小企業サイバーセキュリティ対策
継続支援事業

セキュリティリスク評価及び
対策基準に記載されるべき管理策【対策基準レベル②】

サイバーセキュリティ
人材育成
社内体制整備支援

目次

第11章. リスクマネジメント

11-1. リスクマネジメント：概要

11-2. リスクマネジメント：リスクアセスメント

11-3. リスクマネジメント：リスク対応

章の目的
第11章では、リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方について学ぶことを目的とします。

主な達成目標
◘ リスクマネジメントの意義について理解すること ◘ リスクマネジメントプロセスの全体像を理解すること ◘ リスクアセスメント、リスク対応のプロセスを理解すること

11-1-1. リスクマネジメントプロセス（ISO31000）

企業や組織にはさまざまなリスクが存在しています。これらのリスクを効率的に管理し、発生する可能性がある損失を回避したり低減したりするプロセス全体のことを「**リスクマネジメント**」と言います。

リスクマネジメントの国際規格として**ISO 31000**があります。ISO 31000では、リスクマネジメントを「原則」「枠組み」「プロセス」の3つの要素から構成されるものとして捉えています。

リスクマネジメント

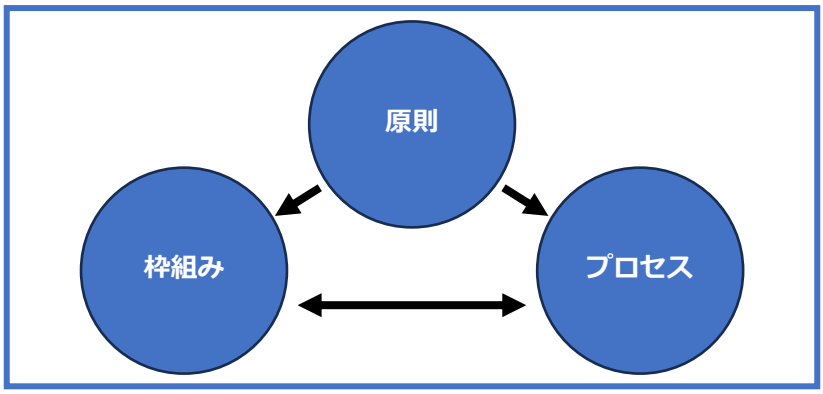


図46. リスクマネジメントの3要素

原則	リスクマネジメントを実施する際に、組織が取り組むべき事項です。 「統合」「体系化及び包括」「組織への適合」「包含」「動的」「利用可能な最善の情報」「人的及び文化的要員」「継続的改善」で構成されています。
枠組み	リスクマネジメントを組織全体に定着させるための仕組みです。 「統合」「設計」「実施」「評価」「改善」で構成されています。
プロセス	リスクマネジメントに取り組む上で実施すべき、一連の活動です。 「コミュニケーション及び協議」「適用範囲、組織の状況及び基準」「リスクアセスメント」「リスク対応」「モニタリング及びレビュー」「記録作成及び報告」で構成されています。

実際にリスクに対応していくにあたっては、リスクマネジメントプロセスにおける「**リスクアセスメント**」が必須事項となります。リスクアセスメントとは、組織や企業が抱える資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位づけをしていくプロセスのことを表します。リスクアセスメントの実施により、個々の資産が持つリスクと、リスクに対する管理策、および管理策に投じるべき費用の識別が期待できます。また、リスクを評価するということは情報資産の持つ固有の弱点や脅威を明確にする過程を含みます。そのため、事前にリスクを把握することで必要な投資額を含め、適切な対策を検討することが可能になります。

11-1-2. 情報セキュリティリスクマネジメント（ISO/IEC27005）

ISO/IEC 27005は、情報セキュリティにおけるリスクマネジメントに関する国際規格です。先に説明したISO31000と整合性がありますが、情報セキュリティに特化した内容になっています。この規格は、組織の情報資産を安全に保つことに焦点が当てられており、情報セキュリティリスクの特定、分析、評価、対応、管理、レビューなどを実施するための手引きになっています。中小企業を含むすべての組織における情報セキュリティリスクのマネジメントに有用です。

ISO/IEC 27005の情報セキュリティリスクマネジメントプロセスは、ISO 31000の一般的なリスクマネジメントプロセスに基づいており、リスクの特定、リスクの評価、リスクの対処、およびリスクの監視とコントロールに関するステップから構成されます。以下の図で示すように情報セキュリティリスクマネジメントプロセスは循環しており、反復的に実施されるものです。組織を取り巻く環境の変化や組織内の変化に応じて、新しいリスクが発生したり、既存のリスクが変化したりする上に、リスクへの対処法も進化するからです。特に、リスクマネジメントプロセスに含まれているリスクアセスメントは、リスク対応の方策や、対応の優先順位づけの前提になる重要な工程です。

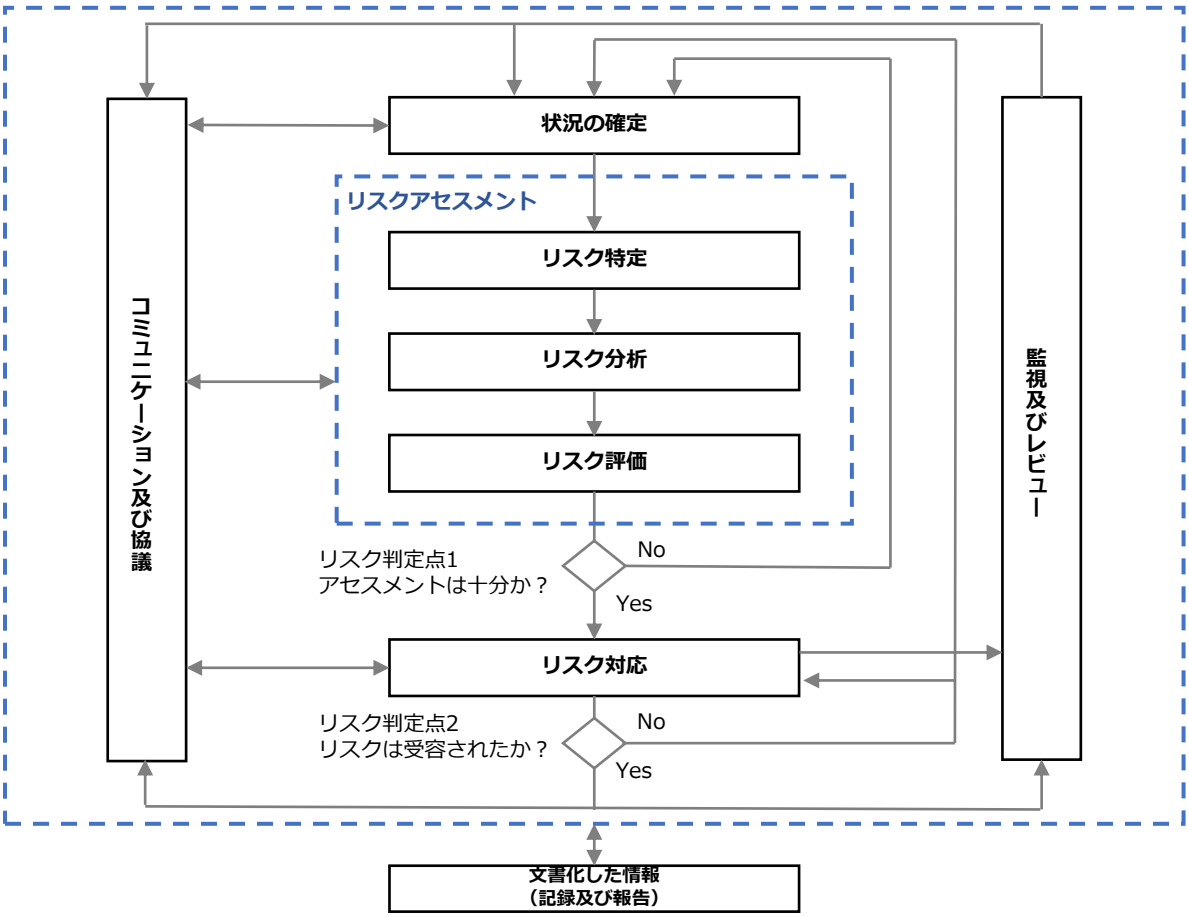


図47. 情報セキュリティマネジメントプロセスの概要
（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

11-1-2. 情報セキュリティリスクマネジメント（ISO/IEC27005）

リスクアセスメントからリスク対応までの流れを表す図を記載します。リスク対応を実施する過程では、「低減」「移転」「回避」「受容（保有）」の4つ選択があり、それらの選択は以下の図で示すプロセスで行われます。

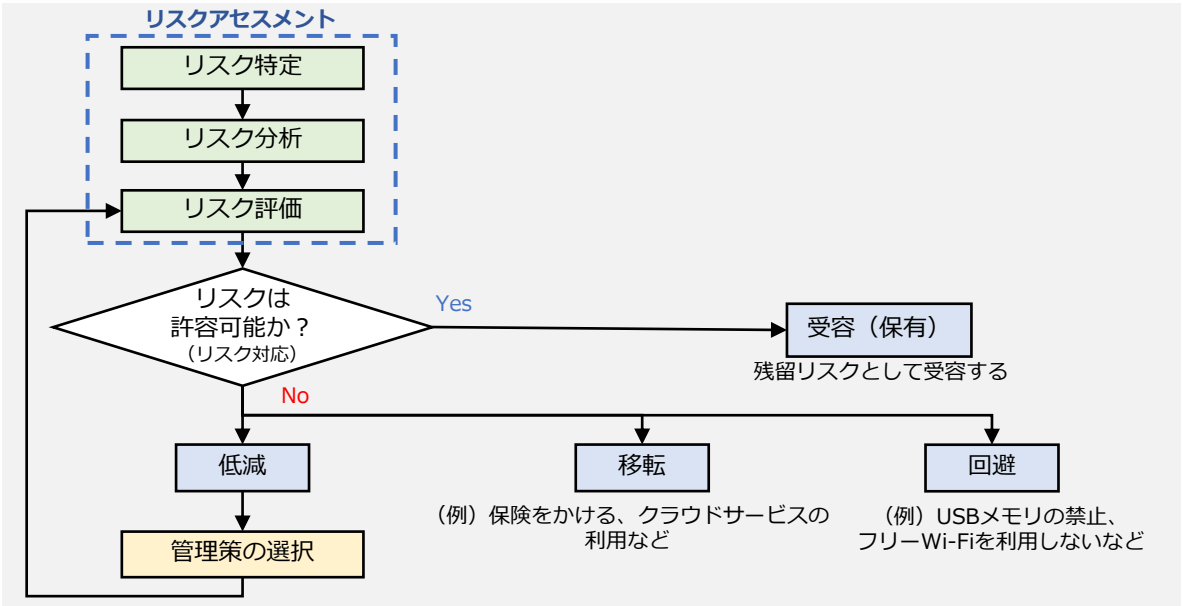


図48. リスクマネジメント全体の流れと、リスク対応の選択プロセス

リスクを低減する

自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げます。

リスクを受容（保有）する

事故が発生しても受容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持します。

リスクを回避する

仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。
（例）
・従来は商品の発送先である住所や氏名などの個人情報を発送完了後もパソコンに保存し続けていたが、保存中の漏えいを避けるために、利用後はすぐに消去する
・インターネットバンキングに使用するパソコンでメールやウェブ閲覧をしていたが、ウイルスに感染しないようにインターネットバンキング専用のパソコンを設置し、ウイルス感染の原因となるメールやウェブ閲覧に利用せず、USBメモリ、外付けHDDも接続を禁止する
また、リスクレベルが大きく自社の対策だけでは不十分であったり、多額の費用がかかり、実施できなかったりする場合は「リスクの移転」を検討します。

リスクを移転する

自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げます。
（例）
・商品を販売するウェブサイトではクレジットカード番号を非保持化し、代金の決済はセキュリティ対策を十分行っている外部の決済代行サービスに変更する
・社内のサーバで運用していた業務システムをセキュリティ対策の充実した外部クラウドサービスに移行する
・情報漏えい、システム障害などの事故発生に伴う損失に対して保険金が支払われる情報セキュリティに関連した保険商品に加入する

（出典）IPA 「中小企業の情報セキュリティ対策ガイドライン第3.1版」を基に作成

11-1-3. ISO/IEC 27001におけるリスクマネジメント手順

ISO/IEC 27005は、情報セキュリティ**リスクマネジメント**の手法を提供する規格であり、ISO/IEC 27001（ISMS）は情報セキュリティ**マネジメントシステム**の設計と実装に関する規格です。つまり、ISO/IEC 27001は情報セキュリティマネジメントシステムの枠組みを提供し、その中で必要となるリスクマネジメントの具体的な手法やプロセスの詳細を提供しているのが、ISO/IEC 27005になります。

ISO/IEC 27001（ISMS）の活動は、ISO/IEC 27005におけるリスクマネジメントプロセスと関連付けて整理することが可能です。

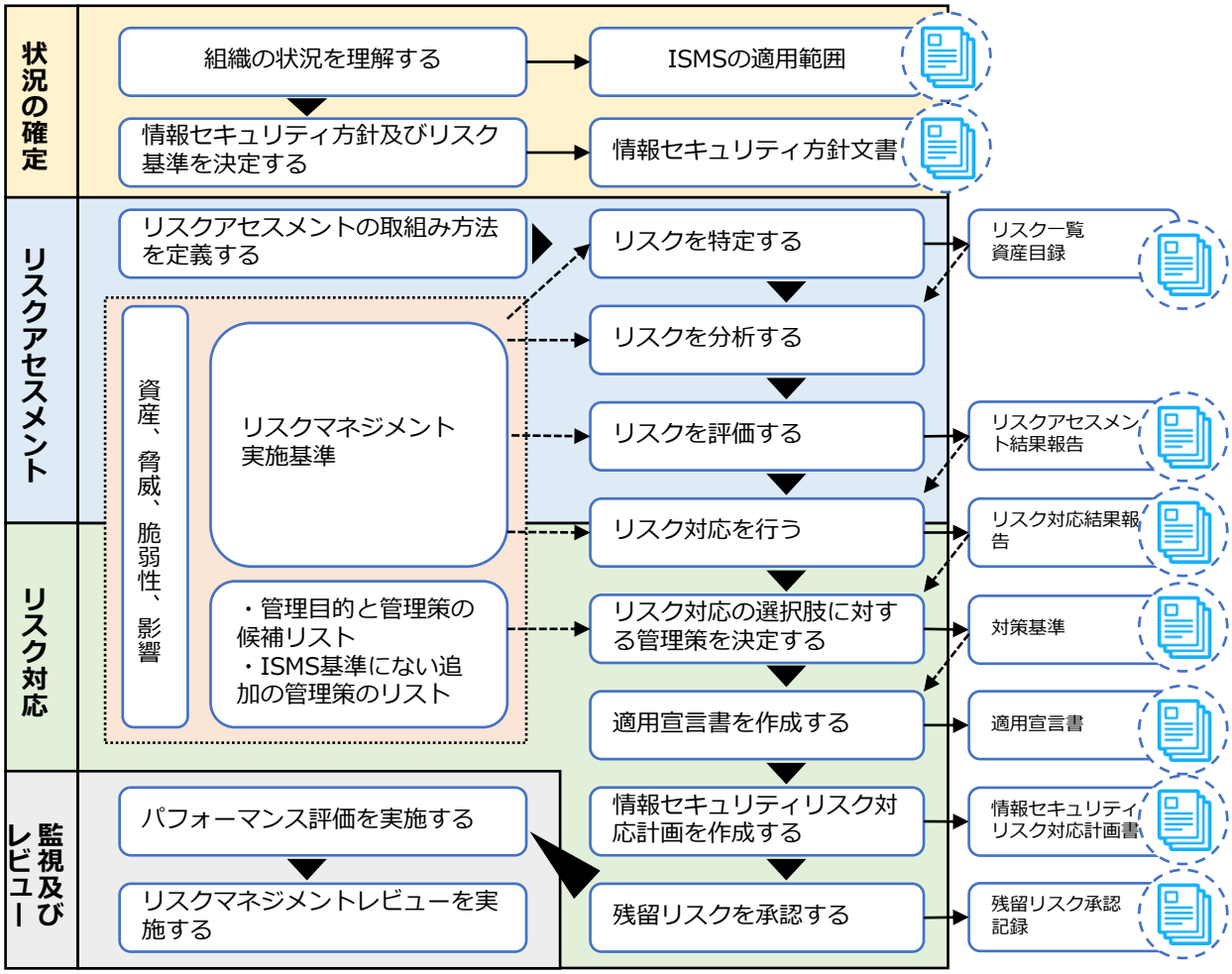


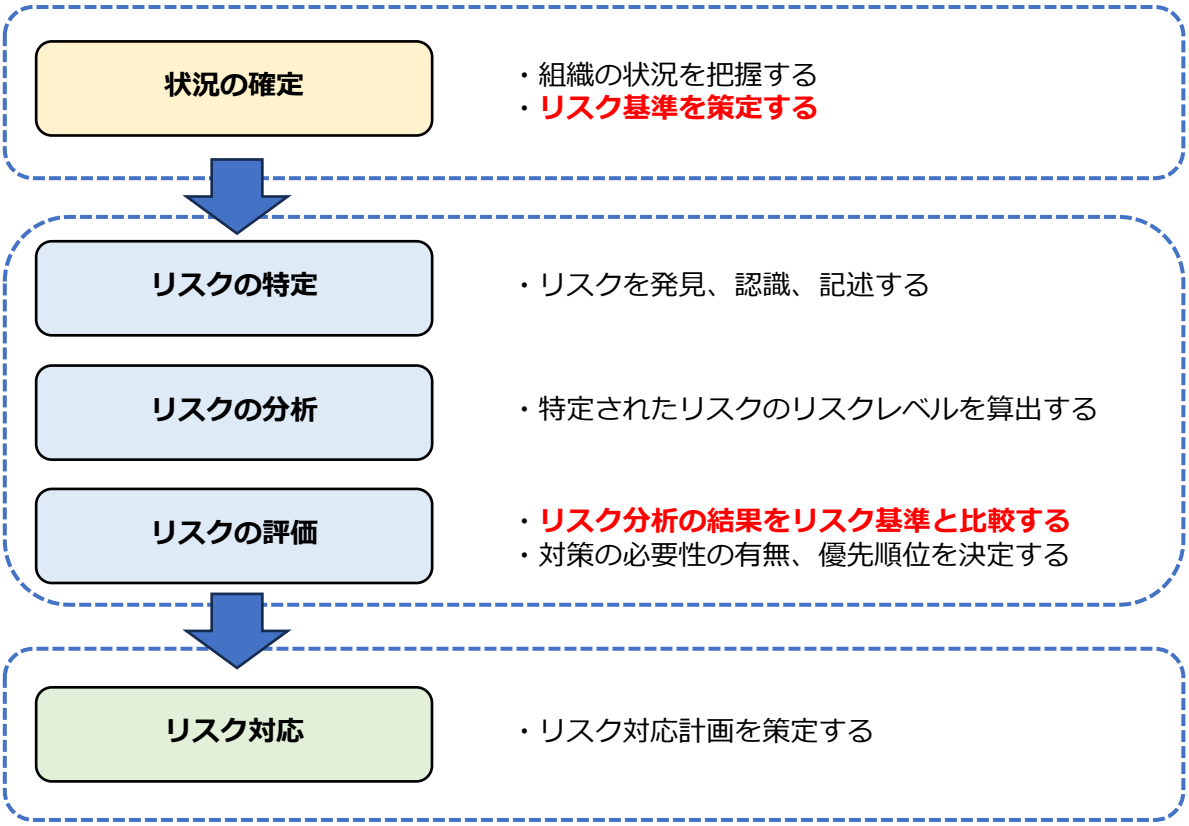
図49. ISMSにおけるリスクアセスメントおよびリスク対応に関する作業の概要

11-2-1. リスク基準の確立

必要なリスク基準

リスクアセスメントを実施するにあたって、リスクの重大性を評価するための目安となる条件を決める必要があります。その条件のことをリスク基準と言います。ISMSでは、リスク基準に「リスク受容基準」と「情報セキュリティリスクアセスメントを実施するための基準」を含むよう明示されています。

リスク受容基準
どの程度のリスクであれば受け入れることが可能かの判断基準です。 あるリスクに対して、どの程度のレベル感や優先順位でリスク対応を実施するのか、リスクが顕在化した際にどの程度の大きさまでなら許容するのかを明確にする必要があります。
情報セキュリティリスクアセスメントを実施するための基準
いつ、どのようなときにリスクアセスメントを実施するのかを決める要件です。 リスクアセスメントの実施条件や実施時期、タイミングや頻度などを明確にする必要があります。



11-2-2. リスクの特定

リスク特定

リスクアセスメントの1つ目のプロセスである「リスク特定」について説明します。リスク特定とは、「リスクを発見、認識及び記述するプロセス」[21]のことです。リスク特定を実施するために一般的に使用されるアプローチは「資産ベースのアプローチ」および「事象ベースのアプローチ」の2つがあります。

【情報セキュリティリスクの特定および記述】

アプローチ手法	概要	メリット	デメリット
資産ベースのアプローチ	• 資産、脅威及び脆弱性の検査を通じてリスクを特定しアセスメントを行う。 • 資産は、その種類及び優先度に従って主要資産及び支援資産として特定できる。 • 脅威は、資産の脆弱性につけ込み、対応する情報の機密性、完全性または可用性を侵害する。 • 資産のリストを作成することが望ましい。	• 資産、脅威及び脆弱性のすべての有効な組合せをISMSの適用範囲で列挙することができれば、理論上はすべてのリスクが特定される。	• 情報資産が増えたときに、資産のリストの行数が多くなる。 • 同様のリスクを繰り返し記載したりしなければならない場合がある。
事象ベースのアプローチ	• 事象及び結果の評価を通じてリスクを特定し、アセスメントを行う。 • 事象及び結果は、トップマネジメントから見た懸念、リスク所有者及び組織の状況を決定する際に特定された要求事項によって発見できる。	• 詳細なレベルで資産を特定することに多大な時間を費やすことなく、高いレベルまたは戦略的なシナリオを確立することができる。	• 網羅性において、資産ベースのアプローチに劣る。

（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

リスク所有者の特定	・特定されたリスクに対し、リスク所有者を関連付ける。 ・リスク所有者は、トップマネジメント、セキュリティ委員会、プロセス所有者、機能所有者、部門マネージャーおよび資産所有者など、リスクマネジメントに権限を持つ人とする。（通常、組織内で一定の権限を持つ人が選ばれる）

[21]: JISC 日本産業標準調査会.”JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”. https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000, （2023-09-21）.

11-2-2. リスクの特定

リスク特定（資産ベースのアプローチ）

資産ベースのアプローチでは、はじめに情報資産を洗い出し（資産目録の作成）、その過程でリスク所有者を特定します。リスク所有者とは、リスクが顕在化した際に責任を取る人のことを指します。その後、情報資産ごとに「機密性」「完全性」「可用性」が損なわれた場合、事業にどれほど影響があるか評価を行い、重要度を判断します。

情報資産の洗い出し

↓

機密性・完全性・可用性が損なわれた場合の影響度を評価

↓

影響度の評価をもとに重要度を算定

情報資産の洗い出し（例）

情報資産の洗い出しでは、業務で利用する電子データや書類などを特定し、資産目録を作成します。洗い出した情報資産は、「営業」「人事」「経理」など管理部門ごとに分類します。企業活動に大きな影響を与えかねない重要な情報を、できる限り漏れないように洗い出すことが重要です。影響がほとんどない情報であれば、漏れても大きな問題はありません。情報資産の洗い出しの粒度は、細かすぎると管理が大変ですが、逆に粗いと次のリスク分析が難しくなります。そのため、適度な粒度にすることが重要です。以下は、情報資産のリストアップ例です。

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	事務所PC
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部長	人事部	書類
経理	給与システムデータ	税務署提出用 源泉徴収票	給与計算担当	経理部長	人事部	事務所PC
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	経理部長	総務部	書類
経理	発行済請求書控え	当社発行の請求書の控え（過去3年分）	総務部	経理部長	総務部	書類
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部長	営業部	可搬電子媒体
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部長	営業部	社内サーバ
営業	受注契約書	受注契約書原本（過去10年分）	営業部	営業部長	営業部	書類

資産目録の例
（出典）IPA 「リスク分析シート」を基に作成

電子化された情報を洗い出す際は、「普段パソコンで見ているこのデータは、どこに保存されているのだろう」というように、社内のIT機器や利用しているクラウドサービスを思い浮かべて記入します。また、複数の組織を持つ企業の場合、管理部署ごとにシートを分けて作成すると、内容の見直しの際に便利です。

11-2-2. リスクの特定

リスク特定（資産ベースのアプローチ）

資産目録を作成する際、情報資産を情報、情報を支援する資産として「主要/事業資産」と「支援資産」2つのカテゴリに分類して整理する方法も有効です。

「主要/事業資産」

「主要/事業資産」とは、「組織にとって価値のある情報又はプロセス」[22]のことです。主要資産は、「事業プロセス及び事業活動」と「情報」の2つに分けられます。

「事業プロセス及び事業活動」の例
- その損失又は低下によって、組織の使命達成が不可能となるプロセス
- 機密プロセス又は専有技術を伴っているプロセス
- 修正された場合、組織の使命の達成に大きく影響するプロセス
- 組織が契約、法令又は規則の要求事項を遵守するために必要となるプロセス

「情報」の例
- 組織の使命又は事業の遂行に不可欠の情報
- プライバシーに関する国内法にいう意味で、特別に定義することができる個人情報
- 戦略的方向性によって決定される目的の達成に必要となる戦略情報
- 収集、保管、処理、送信に長時間を要する高コスト情報及び高い取得費用を伴う情報

「支援資産」

「支援資産」とは、「1つ以上の事業資産の基礎となる情報システムの構成要素」[23]のことです。

「支援資産」の例
- ハードウェア、ソフトウェア、ネットワーク、要員、サイト、組織

（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

One Point

情報資産のグループ化

ISMS適用範囲に存在する情報資産を洗い出す作業は、負荷が非常に大きくなりやすいです。そこで、資産価値や保管形態、保管期間や用途などが同じものを1つのグループとしてまとめて管理することで、作業負荷を軽減したり、作業を効率化したりすることができます。

（例）事務所内のパソコンで会計ソフトや表計算ソフトを使って帳簿を作成している場合

- 仕訳帳
- 総勘定元帳
- 現金出納帳
- 当座預金出納帳
- 小口現金出納帳
- 仕訳帳
- 売上帳

情報資産名称：「会計データ」
「会計データバックアップ」
（バックアップを取っている場合）など

媒体・保存先：「事務所PC」（会計ソフトの保存先）
「可搬電子媒体」
（USBメモリがバックアップ保存先）

[22][23]: ISO.” ISO/IEC 27005:2022”. https://www.iso.org/standard/80585.html, （2023-09-21）.

11-2-2. リスクの特定

リスク特定（資産ベースのアプローチ）

機密性・完全性・可用性が損なわれた場合の影響度を評価

情報資産ごとに「機密性」「完全性」「可用性」が損なわれた場合の事業への影響度を評価します。具体例として、以下の評価基準を参考に「機密性」「完全性」「可用性」それぞれの評価値（3～1）を決定します。

評価値		評価基準	該当する情報の例
機密性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データとして指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報
完全性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報 ●顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	●廃版製品カタログデータ
可用性	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供しているECサイト ●顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ　（インターネット向け事業の場合）
	1	利用できなくなっても事業にほとんど影響はない	●廃版製品カタログ

情報資産の機密性・完全性・可用性に基づく重要度の定義
（出典）IPA 「中小企業の情報セキュリティ対策ガイドライン第3.1版」を基に作成

11-2-2. リスクの特定

リスク特定（資産ベースのアプローチ）

影響度の評価をもとに重要度を算定

重要度の算出例を説明します。重要度は「機密性」「完全性」「可用性」いずれかの評価値の最大値で判断します。なお、事故が起きると法的責任を問われたり、取引先、顧客、個人に大きな影響があったり、事業に深刻な影響を及ぼすなど、企業の存続を左右しかねない場合や、個人情報を含む場合は、前項の算定結果に関わらず、重要度は3とします。

	情報資産の価値・事故の影響の大きさ	
重要度	3	事故が起きると、「 法的責任を問われる」「 取引先、顧客、個人に大きな影響がある」「 事業に深刻な影響を及ぼす」など、企業の存続を左右しかねない
	2	事故が企業の事業に重大な影響を及ぼす
	1	事故が発生しても事業にほとんど影響はない

重要度の判断例：自社のホームページ（電子データ）		評価値
「機密性」	公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない	⇒ 1
「完全性」	不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられたりすると顧客や閲覧者に被害が発生し、信用を失う	⇒ 3
「可用性」	サーバの障害などでアクセスできなくなると、来店客が減少し、売上も減少する	⇒ 3
➡ 完全性と可用性の評価値3が最大値なので、**重要度は評価値：3**		

重要度の判断例
（出典）IPA 「中小企業の情報セキュリティ対策ガイドライン第3.1版」を基に作成

One Point

重要度を判断する際のポイント

- 重要度の判断は、立場や見識によっても異なることがあるので、情報資産管理台帳に記入する前に「重要ではない」と判断するのではなく、記入した後に組織的に重要度を判断します。
- 情報資産の「重要度」は、時間経過とともに変化することがありますが、現時点の評価値を記入します。また時間経過に伴う重要度の変化を台帳上で更新することが難しい場合は、最大値で評価します。

11-2-2. リスクの特定

リスク特定（事象ベースのアプローチ）

事象ベースのアプローチでは、従業者の業務プロセスを起点にリスクを特定します。それにより、詳細なレベルで資産を特定することに多大な時間を費やすことなく、戦略的なシナリオを確立することができます。その結果、組織は自らのリスク対応の取組みを、重大なリスクに集中させることができます。

前述の資産ベースのアプローチに比べると網羅性に劣るというデメリットはありますが、その分、日々の業務をもとにして洗い出すため、現実的なリスクを洗い出すことができるというメリットがあります。また、資産ベースのアプローチの際、情報資産の洗い出しにより出てきた主要資産（事業プロセスおよび事業活動）に対しても、事象ベースのアプローチでリスク特定が可能です。

① リスクの特定	業務プロセスや取扱っている重要な資産に対して、業務上起きたら困ること（リスク）もしくは、過去に発生して業務に影響を及ぼしたことを記載します。 （例） 「ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ」

② リスク所有者の特定	①で特定されたリスクの所有者を記載します。

リスク	評価値			重要度	リスク所有者
ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ	機密性	情報が漏えいする類の事象ではない	1	3	○○○○
	完全性	ネットワーク障害の原因がサイバー攻撃やマルウェアの場合、情報が被害を受ける可能性がある事象である	3		
	可用性	ネットワークが利用できなくなり、自社や取引先、顧客に大きな影響をおよぼす事象である	3		

事象ベースのアプローチによるリスク特定の例
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

上記内容でリスク特定を実施した後、特定されたリスクおよび「重要度」に対して後述のリスク分析を実施します。

11-2-3. リスクの分析

リスク分析（例）

特定されたリスクに対して「リスク分析」を行います。リスク分析とは、「リスクの性質を理解し、リスクレベルを決定するプロセス」[24]のことです。リスクレベル（リスクの大きさ）は、優先的・重点的に対策が必要な情報資産を把握するために使用されます。リスクレベル（リスクの大きさ）を算定するにはさまざまな方法があります。算定方法の一例を以下に示します。

「リスクレベル」 ＝ 「重要度」 ※リスク特定で算出方法を説明 × 「被害発生可能性」

「被害発生可能性」とは、脅威が脆弱性を利用して、どの程度被害をもたらす可能性があるかを示す指標です。「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の2つの数値を「被害発生可能性の換算表」に当てはめて算出します。

起こりやすさ（脅威）	
3	通常の状況で脅威が発生する（いつ発生してもおかしくない）
2	特定の状況で脅威が発生する（年に数回程度）
1	通常の状況で脅威が発生することはない（通常発生しない）

つけ込みやすさ（脆弱性）	
3	対策を実施していない（ほぼ無防備）
2	部分的に対策を実施している（一部対策を実施）
1	必要な対策をすべて実施している（対策を実施）

換算表で算出

被害発生可能性の換算表		つけ込みやすさ（脆弱性）		
		3	2	1
起こりやすさ（脅威）	3	3	2	1
	2	2	1	1
	1	1	1	1

（例）
- 脅威の起こりやすさ：「2」、 脆弱性のつけ込みやすさ：「2」
  ➡ 被害発生可能性は**「1」：通常の状況で被害が発生することはない**
- 脅威の起こりやすさ：「3」、脆弱性のつけ込みやすさ：「2」
  ➡ 被害発生可能性は**「2」：特定の状況で被害が発生する（年に数回程度）**
- 脅威の起こりやすさ：「3」、脆弱性のつけ込みやすさ：「3」
  ➡ 被害発生可能性は**「3」通常の状況で被害が発生する（いつ発生してもおかしくない）**

[24]: JISC 日本産業標準調査会.”JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”. https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000, （2023-09-21）.

11-2-4. リスクの評価

リスク評価

リスク評価とは、「特定・評価したそれぞれのリスクが、受容可能かどうかを評価するプロセス」のことです。リスク分析で算出したリスクレベルを、リスク基準（リスク受容基準）と比較し、リスク対策が必要かどうか判断します。また、リスクレベルをもとに対策の優先順位をつけます。

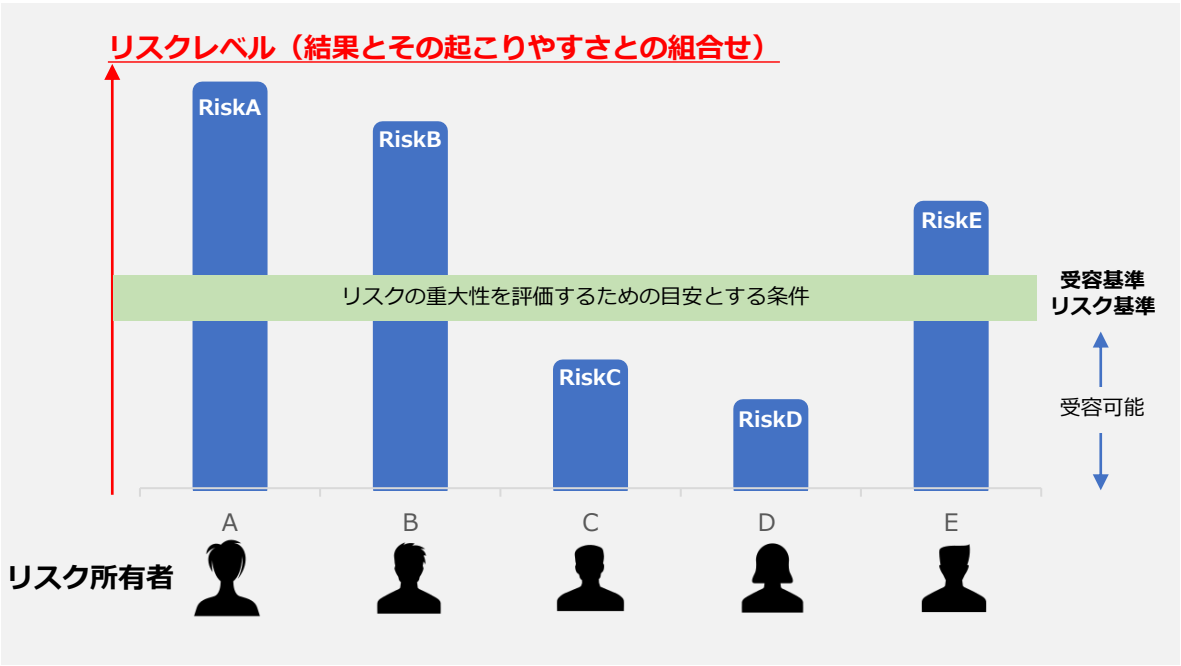


図50. リスク評価の概要図
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

11-2-4. リスクの評価

リスク評価（例）

「重要度」 × 「被害発生可能性」でリスクレベルを算出し、リスク評価を行います。例として、算出したリスクレベルを以下の表に当てはめて行います。

リスクレベル 評価値		被害発生可能性		
		3	2	1
重要度	3	9	6	3
	2	6	4	2
	1	3	2	1

※リスクレベル＝「重要度」 × 「被害発生可能性」　※赤色、黄色、青色の網掛けは以下の「リスク受容基準」を示す

リスク受容基準（例）

リスクレベル	リスク評価	記述
低（青）	そのままで受容可能	それ以上の活動なしにリスクを受容可能
中（黄）	管理下で受容可能	リスクマネジメントの観点からフォローアップを実施し、中長期にわたる継続的改善の枠組みにおいて活動を設定することが望ましい
高（赤）	受容できない	リスクを低減するための対策を短期間で行うことが絶対に望ましい。そうでない場合、活動の全部又は一部を拒否することが望ましい

（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

また、情報セキュリティリスクの場合、以下の図で示す考え方をすることが多いです。以下の図では、発生頻度が高く被害が非常に大きいものについては「回避」、発生頻度は低いが被害が大きいものについては「移転」、発生頻度は高いが被害が大きくないものについては「低減」を検討するという考え方を示しています。

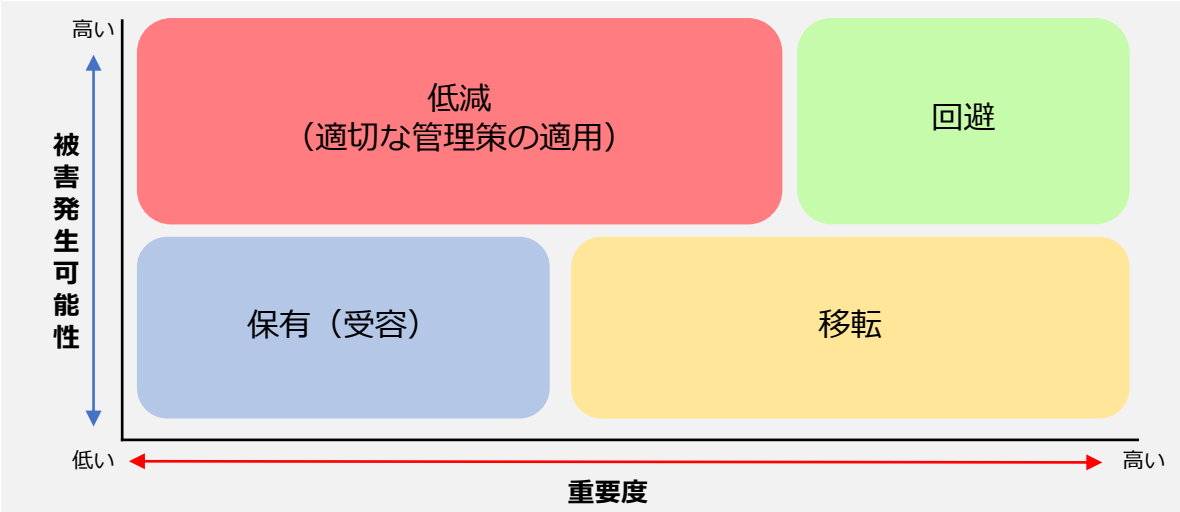


図51. 情報セキュリティリスクの考え方
（出典）JNSA.”2-4 リスクアセスメントとリスク対応”. https://www.jnsa.org/ikusei/01/02-04.html,（参照 2023-09-21）

11-3-1. 対策案の検討

リスク対応プロセス

リスク対応とは、「リスクを修正するプロセス」[25]のことです。リスクアセスメントプロセスの結果に基づいており、リスク基準に基づき対応すべき優先順位づけされたリスクに対応する内容となります。

1. 適切な情報セキュリティリスク対応の選択肢の選定	
リスク対応の選択肢は以下の通りです。	
リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすることです。たとえば、個人情報を受け取らないようにしたり、その業務自体をやめたりするといった方法です。
リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくすることです。「軽減」「修正」と呼ばれることもあります。
リスク移転	リスクを他者に移して、自分たちの責任範囲外にしたり、リスクが顕在化したときの損失を他者に引き受けさせることです。たとえばクラウドのサーバを利用することによって、サーバが破壊されたり盗難されたりするリスクを移転することができます。「共有」と呼ばれることもあります。
リスク受容（保有）	対策を行わずにリスクを受け入れるということです。被害は大きいが発生可能性がほとんどない場合や、発生しても被害がほぼない場合が該当します。
2. 情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策の決定	
ISO/IEC 27001:2022の附属書A、ISO/IEC 27017などの管理策集から、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要な全ての管理策を決定します。	
3. 決定した管理策とISO/IEC 27001:2022附属書A の管理策との比較	
必要な全ての管理策を、ISO/IEC 27001:2022附属書Aに挙げられている管理策と比較します。	
4. 適用宣言書の作成	
必要な全ての管理策と、その理由及び実施状況を文書化します。適用宣言書に含まれる全ての管理策の実施状況は、“実施された”、“一部実施された”または“実施されていない”として記述できます。	
5. 情報セキュリティリスク対応計画	
組織がリスクに対応する必要性を含んだリスク対応計画を作成します。リスク対応計画とは、組織のリスク受容基準を満たすようにリスクを修正するための計画のことです。 - 組織の必要な管理策を実施するためのプロジェクト計画 - リスクを修正するために管理策が環境と相互にどのように作用するかを記述した設計計画	
6. リスク所有者による承認	
リスク所有者は、リスク対応計画を承認します。	
7. 残留している情報セキュリティリスクの受容	
リスク所有者は、残留リスクが受容可能かどうかを判断し、決定します。	

（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

[25]: JISC 日本産業標準調査会.”JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”. https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000, （2023-09-21）.

11-3-1. 対策案の検討

リスク対応プロセス（例）

例：自社のホームページ（電子データ）

リスクの内容

不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失う

リスク対応

リスク評価の結果をもとにリスク対応を決定する（今回は例として「リスクを低減する」方法を選択）

対策例：不正アクセスが発生する可能性を低減させるために、アクセス権限を最小化したり、パスワードを複雑にしたり、多要素認証を実施したりするなど、認証の強化を行い、不正アクセスが発生する可能性を低減する

対応する管理策：5.15アクセス制御

対策基準の策定（対策基準の例）

技術的対策

- 公開サーバへの不正アクセス対策
- 公開サーバへのアクセス権の最小化と管理の強化
- 多要素認証の設定の有効化

残留リスク

残留リスクとは、「リスク対応後に残っているリスク」[26]のことです。残留リスクを受容するためには、リスク所有者の承認が必要になります。受容可能だと判断された残留リスクであっても、資産の価値や脅威、脆弱性など環境の変化に合わせて、リスクレベル（リスクの大きさ）を見直し、必要に応じて追加のリスク対応を行う必要があります。

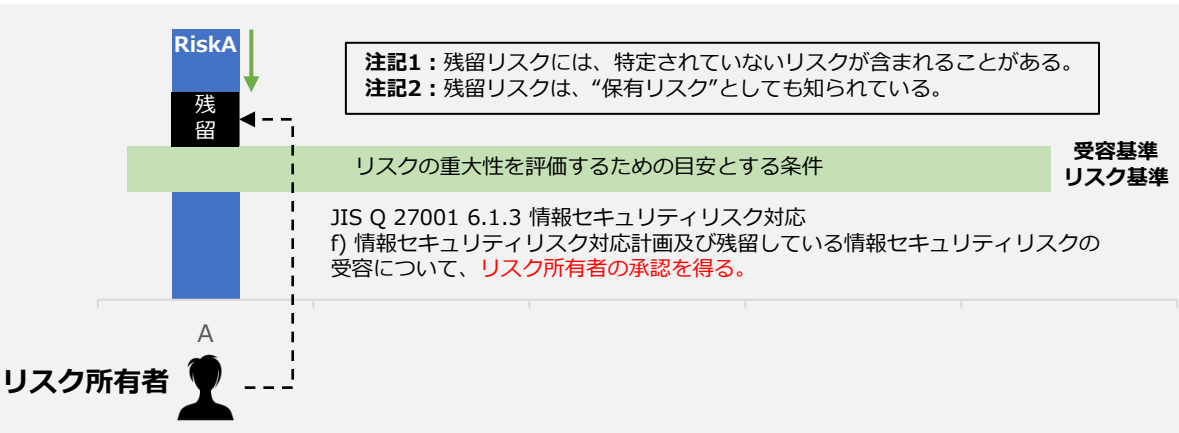


図52. 残留リスクの概要
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

[26]: JISC 日本産業標準調査会.”JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”. https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000, （2023-09-21）.

編集後記

セミナー6日目では、リスクマネジメントプロセスに沿って、リスク基準の確立、リスクアセスメント、リスク対応について手法なども交えながら解説しました。リスクマネジメントはセキュリティ対策にとって欠かせないものですが、顕在化していないリスクについて考えることが難しい場合もあるでしょう。リスクマネジメントプロセスにおける各段階での考え方や手法を用いることで、円滑なリスク特定、分析と対応策の検討を実施できることを、今回のセミナーを通じて理解いただければと思います。

本テキストでは、最初にリスクマネジメントの概要について説明を行い、その必要性やプロセスの全体像、ISO/IEC 27001との関連性について取り上げました。その後、プロセスの各段階の説明としてリスク基準の確立、リスクアセスメント、リスク対応を説明し、リスク対策を検討するまでの一連の流れとして説明を行いました。組織の状況やそれに応じたリスクは流動的に変化するため、リスクマネジメントプロセスを繰り返し回していくことが重要です。次回は、セキュリティ対策のアプローチ手法とその手順について解説します。

引用文献

ISO/IEC 27005:2022

https://www.iso.org/standard/80585.html

中小企業の情報セキュリティ対策ガイドライン第3.1版

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

JISC 日本産業標準調査会 JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語

https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000

中小企業の情報セキュリティ対策ガイドライン第3.1版 付録7 リスク分析シート（全7シート）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx

MSQA ISMS推進マニュアル活用ガイドブック 2022年 1.0版

https://msqa.actibookone.com/content/detail?param=eyJjb250ZW50TnVtIjo3ODgwMSwiY2F0ZWdvcnlOdW0iOjEwNzI0fQ==&pNo=1

JNSA 2-4 リスクアセスメントとリスク対応

https://www.jnsa.org/ikusei/01/02-04.html

用語集

■AI
Artificial Intelligenceの略。「AI（人工知能）」という言葉は、1956年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。1950年代後半から1960年代が第一次AIブーム、1980年代が第二次AIブーム、現在は2000年代からはじまる第三次AIブームである。
「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている
…… 1-1-1、4-1-1、4-2-5、5-2-1、5-2-2、5-2-3、6-1-1、6-1-3

■BCP
Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画
…… 2-3-2

■CSIRT（シーサート）
Computer Security Incident Response Teamの略。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総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う
…… 2-1-3、6-1-3、7-5-3

■DDoS攻撃（ディードスこうげき）
Distributed Denial of Service Attackの略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることで、過剰な負荷をかけてサービスを利用できなくする攻撃手法
…… 2-2-2、2-2-5、第一回コラム、7-4-4

■DFFT
Data Free Flow with Trustの略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している
…… 5-2-1

■EDR
Endpoint Detection and Responseの略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する
…… 2-2-4、2-2-5、3-1-1、3-4-1

■eKYC
electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと
…… 5-2-1

■GビズID
行政手続きなどにおいて手続を行う法人を認証するための仕組み。1つのID・パスワードで本人確認書類なしに様々な政府・自治体の法人向けオンライン申請が可能になる
…… 5-2-1

■ICSCoE中核人材育成プログラム
2017年4月にIPA内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている
…… 2-1-2

■ICT
Information and Communication Technologyの略。IT（情報技術）だけでなく、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる
…… 4-1-2、5-2-1、7-2-2、7-3-1

■IoT（アイ・オー・ティー）
Internet of Thingsの略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電など様々な「モノ」が接続され、データを収集したり、相互に情報をやり取りしたりする概念や仕組み、技術のこと
…… 1-1-1、2-1-2、2-2-2、4-1-1、4-2-5、5-2-2、5-2-3、6-1-2、7-4-3、7-4-4

用語集

■IPS
Intrusion Prevention Systemの略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。
IPSは、異常を検知した場合、管理者に通知するだけではなく、その通信を遮断する
…… 2-2-2、3-4-2

■IPアドレス
コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。 IPアドレスは、127.0.0.1のように0～255までの数字を4つ組み合わせたもので、単にアドレスと略されることがある。 現在主に使用されているこれら4つになる数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量にIPアドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6では、アドレス空間の増加だけでなく、情報セキュリティ機能の追加などの改良も加えられている
…… 2-3-1、6-2-2

■ISMS
Information Security Management Systemの略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的な対策を含む、経営者を頂点とした総合的で組織的な取組み。組織がISMSを構築するための要求事項をまとめた国際規格がISO/IEC 27001（国内規格はJIS Q 27001）であり、審査機関の審査に合格すると「ISMS認証」を取得できる
…… 3-3-1、7-1-1、7-1-2、7-2-2、7-2-3、7-3-1、7-3-4、7-4-1、8-1-2、9-1-1、11-1-3

■ITリテラシー
コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能
…… 3-1-1

■LockBit2.0
「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される
…… 2-3-2

■NISC
National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当
…… 5-2-1、6-1-3

■NIST サイバーセキュリティフレームワーク（CSF）
米国政府機関の重要インフラの運用者を対象として誕生し、防御にとどまらず、検知・対応・復旧といったステップも含み、インシデント対応を含めており、日本も今後普及が見込まれる
…… 3-3-1、7-1-1、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-3-4

■RPA
Robotic Process Automationの略。定型的な業務をソフトウェアのロボットにより自動化すること
…… 4-2-3

■SASE（サシー）
Secure Access Service Edgeの略。2019年に提唱されたゼロトラストセキュリティを実現する方法の1つで、IT環境のネットワークの機能とセキュリティの機能をクラウド上で統合して提供するサービス、また、その考え方・概念
…… 2-2-4

■SBOM（エスボム）
Software Bill of Materialsの略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOMは、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOMは、ソフトウェアのリスクを把握・管理するのに役立つ
…… 6-1-1

用語集

■SDP
Software-Defined Perimeterの略。ゼロトラストを実現するための仕組みで、すべての通信をチェックおよび認証する。VPNは、ネットワーク接続前に一度だけ認証を行うのに対し、SDPは、ユーザの情報（デバイス、場所、OSなど）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う
…… 2-2-5

■SECURITY ACTION
中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度
…… 2-1-2、3-3-1

■Society5.0
サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）
…… 1-1-1、4-1-1、5-2-2、6-1-1、7-1-1、7-4-1、7-4-2、7-4-3

■SWG
Secure Web Gatewayの略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することでセキュアな通信環境を実現
…… 2-2-4

■VPN
Virtual Private Networkの略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することで、盗聴やデータの改ざんを防ぐ。このようにVPNを使用することで、ユーザは物理的な専用線で通信しているかのような安全な通信を行うことができる
…… 2-1-3、2-2-2、2-2-5、2-3-1、2-3-2、2-3-3

■WAF（ワフ）
Web Application Firewallの略。 従来のファイアウォールが、IPアドレスとポート番号で通信を制御していたことに対して、Webアプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと
…… 2-2-2

■アクセス制御
特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザを制限する機能のこと
…… 2-2-5、第一回コラム、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、9-1-1

■アセスメント
システムや運用環境などを客観的に調査・評価すること。現在の利用状況を把握することで、システムの再構築や運用改善の参考情報となる
…… 2-2-4、7-3-1、7-4-5、11-1-2

■暗号化
データの内容を変換し、第三者には、内容を見ても解読できないようにすること
…… 2-1-3、2-2-1、2-2-5、2-3-2、3-3-3、3-4-1、第一回コラム

■アンダーグラウンドサービス
合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス
…… 2-1-3

■インターネットバンキング
インターネットを利用した銀行や金融機関との取引を行うサービスのこと。銀行の窓口やATMに出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振込や残高照会などの取引を行うことができる
…… 3-2-2、11-1-2

■ウイルス定義ファイル（パターンファイル）
セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの
…… 3-2-2、3-3-3

■エンティティ
個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと
…… 7-2-1

■エンドポイントデバイス
ネットワークに接続して、ネットワークを介して情報を交換するデバイス（デスクトップコンピュータ、仮想マシン、サーバなど）
…… 2-2-4

用語集

■改ざん
文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT分野では、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為
…… 2-1-2、5-2-2、6-1-3、7-4-4、8-1-2、11-2-2、11-3-1

■可用性
許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性
…… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2、11-2-2

■完全性
参照する情報が改ざんされていなく、正確である特性
…… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2、11-2-2

■機密性
許可された者だけが情報や情報資産にアクセスできる特性
…… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2、11-2-2

■クラッキング
悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為
…… 第一回コラム

■限定提供データ
不正競争防止法で次のように定義されている。「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）をいう。」
…… 11-2-2

■個人情報保護委員会
個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱を確保することを任務とする、独立した機関のこと。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱に関する監視・監督、認定個人情報保護団体に関する事務などの業務を行う行政機関（組織的には内閣府の外局）
…… 2-2-3、5-2-1、6-2-1、8-1-2

■サイバー攻撃
インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまで様々である。ネット社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある。
…… 2-1-2、2-1-3、2-2-2、2-2-5、2-3-2、3-3-1、4-3-1、4-3-2、5-2-2、5-2-3、6-1-1、6-1-2、6-1-3、7-1-2、7-3-4、7-4-1、7-5-2、7-5-3

■サイバーセキュリティお助け隊サービス制度
中小企業のサイバーセキュリティ対策に不可欠な各種サービスをワンパッケージで安価に提供するサービス
…… 2-1-2

■サイバーセキュリティ戦略
組織や企業がセキュリティに関する目標を達成するための計画やアプローチ
…… 3-3-1、5-1-1、6-1-1

■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）
単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク
…… 3-3-1、7-1-1、7-1-2、7-4-1、7-4-2、7-4-3、7-4-4、7-4-5

用語集

■サプライチェーン
製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される
…… 2-1-3、2-2-2、2-2-4、4-1-1、4-2-4、4-3-2、5-1-1、5-2-2、6-1-1、6-1-2、6-1-3、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-4-1、7-4-2、7-4-3、7-4-5、7-5-1、7-5-2

■情報資産
営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報
…… 3-3-1、7-2-1、7-2-2、7-3-4、7-4-4、7-5-1、8-1-2、11-1-1、 11-1-2、11-2-2、11-2-3

■情報セキュリティの3要素「CIA」
情報セキュリティの3つの要素、機密性（Confidentiality）、完全性（Integrity） 、可用性（Availability）の頭文字をとって「CIA」と呼ぶ
…… 第一回コラム、第五回コラム

■真正性
情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある
…… 2-1-3、第一回コラム、6-1-3、7-2-1、第五回コラム

■信頼性
システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性
…… 第一回コラム、6-1-1、6-1-3、7-2-1、7-4-2、7-4-3、7-4-4 、第五回コラム

■スクリーンロック
デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない
…… 2-2-2

■脆弱性
情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）におけるセキュリティ上の欠陥のこと
…… 2-1-1、2-1-3、2-2-1、2-2-2、2-2-4、2-2-5、2-3-1、2-3-2、2-3-3、3-3-1、第一回コラム、6-1-3、7-2-2、7-4-4、7-4-5、9-1-2、10-1-1、11-1-2、11-1-3、11-2-2、11-2-3、11-3-1

■脆弱性診断
システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること
…… 2-3-1

■責任追跡性
情報資産に対する参照や変更などの操作を、どのユーザが行ったものかを確認することができる特性
…… 第一回コラム、7-2-1 、第五回コラム

■セキュリティインシデント
セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象などがインシデントに該当
…… 2-1-1、2-1-2、2-1-3、2-2-1、4-1-1、7-2-2、7-3-1、7-4-4、9-1-1、9-1-2

■セキュリティ・キャンプ
情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した22歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している
…… 2-1-2

■セキュリティホール
情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある
…… 3-3-1

用語集

■セキュリティポリシー
企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的
…… 2-1-1、2-2-1、3-3-1、6-1-2、7-4-4、8-1-1

■ゼロデイ攻撃
OSやソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと
…… 2-1-3

■ゼロトラスト
従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、すべてのネットワーク通信を信用できない領域として扱い、すべての通信を検知し認証するという新しいセキュリティの考え方
…… 2-2-4

■ソリューション
問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」
…… 2-2-5

■ダークウェブ
特別な手法でないとアクセスできない、匿名性の高い非公開のWebサイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている
…… 2-1-3

■多要素認証
多要素認証は、サービス利用時において利用者の認証を行うために、3つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも2つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年ではFIDO2と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている
…… 2-2-5、2-3-3、8-1-2、 、第五回コラム、11-3-1

■データサイエンス
数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること
…… 1-1-1

■デジタル化
紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネス・プロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードをCD（コンパクトディスク）にするのがデジタイゼーション、音楽をダウンロード販売するのがデジタライゼーションである
…… 1-1-1、2-1-1、2-1-2、3-3-1、4-1-2、4-2-3、5-1-1、6-1-1、6-1-3、7-4-3

■デジタル情報
0、1、2のような離散的に（数値として）変化する量
…… 第一回コラム

■内部監査
内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格であるISO27001の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する
…… 3-3-1、7-2-1、7-3-1

■ビジネスメール詐欺
攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Email Compromiseとも略される
…… 2-1-3

用語集

■ビッグデータ
全体を把握することが困難な程、膨大な規模のデータ群
…… 1-1-1、5-2-2、5-2-3

■否認防止性
システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性
…… 第一回コラム 、第五回コラム

■標的型攻撃
機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルス付きメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている
…… 2-1-2、2-1-3

■標的型メール攻撃
特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある
…… 2-2-4

■ファイアウォール
本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンのOSに付随しているもの、セキュリティソフトに付いているもの、専用のハードウェアになっているものなど形態は様々である
…… 2-3-1、3-4-1、3-4-2

■不正アクセス
利用権限を持たない悪意のあるユーザが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、2000年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている
…… 2-1-1、2-1-2、2-1-3、2-2-1、2-2-2、2-2-3、2-2-5、2-3-1、4-3-2、5-2-1、7-4-4、8-1-2、11-2-2、11-3-1

■踏み台
不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することで、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ
…… 2-1-3、4-3-2

■フォレンジック
犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組みを指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる
…… 2-2-3、2-3-2

■ブラックマーケット
広義には、不法な取引が行われる市場を指す。不正に入手した個人情報などを売買するネット上の市場（闇市）
…… 2-1-3

■フレームワーク
フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃など様々なセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな形」としてまとめたもの
…… 2-2-4、3-4-1、7-1-1、7-1-2、7-2-1、7-3-1、7-3-2、7-4-1、8-1-1、8-1-2、9-1-2

■ブロックチェーン
複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する仕組み
…… 1-1-1

用語集

■ベストプラクティス
何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例やよい成果をもたらす方法論
…… 2-1-3、2-3-1、7-1-1

■マルウェア
パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる
…… 2-2-2、2-2-4、2-2-5、第一回コラム、7-2-2

■ミラサポコネクト
ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤
…… 5-2-1

■無線LAN
LAN は Local Area Network の略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線LANを通じて、コンピュータはインターネットにアクセスできる
…… 3-2-3

■ランサムウェア
悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する
…… 2-1-2、2-1-3、2-2-1、2-2-2、2-2-5、2-3-2、2-3-3、7-5-1、8-1-2

■リスクアセスメント
企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外は何らかの対策を講じる必要がある
…… 3-3-1、7-3-1、7-4-5、第四回コラム、11-1-1、11-1-2、11-1-3、11-2-1、11-2-2、11-3-1

■リスク評価
組織やプロジェクトにおける特定されたリスクに対して、重要度や影響度を評価するプロセス
…… 2-3-2、3-4-1、7-3-2、7-4-5、11-1-2、11-2-4、11-3-1

■リモートデスクトップ接続
パソコン、タブレット、スマートフォンなどのデバイスを使用して、遠隔地から特定のパソコンに接続する方法
…… 2-2-2

令和5年度
中小企業サイバーセキュリティ対策
継続支援事業