「情報セキュリティ 10 大脅威」解説書の
活用法（組織編）

独立行政法人情報処理推進機構
セキュリティセンター

2025 年 2 月

本資料は、以下の URL からダウンロードできます。

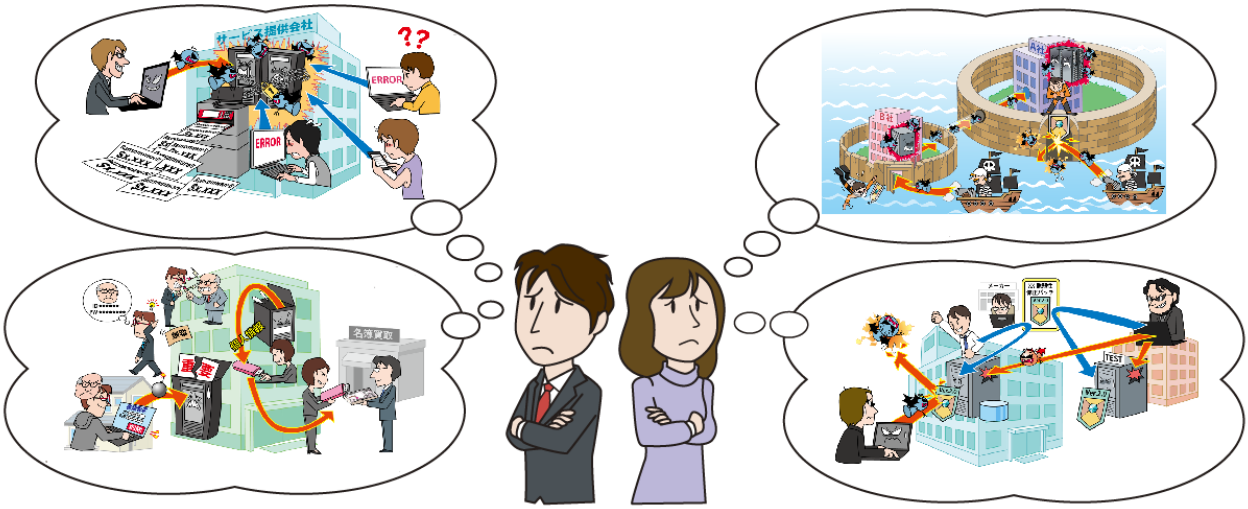
「情報セキュリティ 10 大脅威の活用法　組織編　2025」
https://www.ipa.go.jp/security/10threats/10threats2025.html

目次

情報セキュリティ 10 大脅威の活用法 4
1. 脅威と対策の検討方法 5
2. 組織の検討例 8
3. おわりに 12

情報セキュリティ 10 大脅威の活用法

～自組織にとっての脅威と対策を考える～



IPA が毎年公開している『情報セキュリティ 10 大脅威』（以降、『10 大脅威』と略す）の解説書を、セキュリティの専門家は熟読しているかと思われる。また、セキュリティ対策に十分な予算を持つ組織の人々は、『10 大脅威』にランクインした全ての脅威に対して、対策実施を検討しているだろう。その一方で、「多くの脅威が紹介されているが、全てを理解するのは難しい」、「セキュリティ対策に十分な予算が無いので、『10 大脅威』にランクインした全ての脅威に対して対策を実施するのは困難である」といった声を聞くことも多い。

ときには、「セキュリティ対策予算に制約があるため、『10 大脅威』の上位にランクインした脅威から優先的に対策を実施している」といった話を聞くこともあり、『10 大脅威 2025 組織編』の冒頭において、『10 大脅威』を読む上での留意事項を掲載している（下記抜粋）。

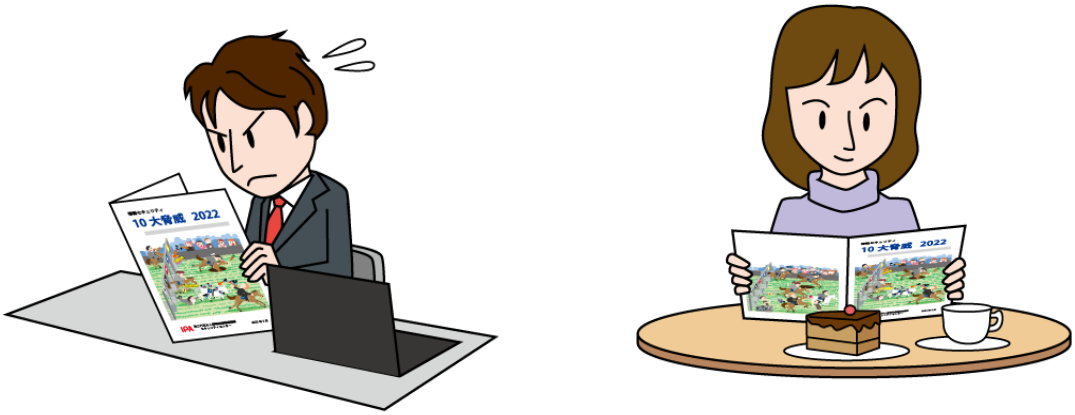
■「情報セキュリティ 10 大脅威 2025 組織編」を読む上での留意事項

① 順位に囚われず、立場や環境を考慮する
② ランクインした脅威が全てではない
③ 「情報セキュリティ対策の基本」が重要

『10 大脅威』は、情報セキュリティの有識者から成る「10 大脅威選考会」が、社会的影響が高いと考えられる脅威を投票により選ばれたものである。上記の①②は、自組織の立場や環境によって重要度が高い脅威は異なり、場合によっては、かつてランクインしていた脅威が自組織にとって重要なことがあり得る、ということを説明している。

本資料では、『10 大脅威 2025 組織編』に示した脅威と対策の解説書を活用しながら、組織にとっての脅威と対策を検討するための具体的な方法を紹介する。

1. 脅威と対策の検討方法



自組織にとっての脅威と対策を検討するためには、『10 大脅威』にランクインした脅威に限らず、自身にとって重要な脅威を抽出し、それらの脅威に対する対策候補を洗い出し、予算等を考慮して、実施する対策を選択する必要がある。そのために、以下のようなステップで脅威と対策を検討する必要がある。

（1）自組織にとって守るべきものを明らかにする

脅威と対策の検討に先立って、自組織にとって、サイバー攻撃による被害を受けさせたくない「守るべきもの」は何かを明らかにする。「守るべきもの」には、以下がある。

【守るべきもの】

- 自組織の**「業務プロセス」**
- 自組織が保有する重要な**「情報」**や**「データ」**
  - 法律で規定された守るべき情報（個人情報等）
  - 自組織として守るべき情報（営業機密や財務情報等）
- 上記「業務プロセス」を実現し、また重要な「情報」や「データ」を保護するための**「システム」**やシステムを用いて提供される**「サービス」**
  - 自組織が保有・構築・運用しているシステムやサービス
  - 他組織が保有・構築・運用していて、自組織が利用中のシステムやサービス
- 上記「システム」や「サービス」を構成している**「機器」**
  - 情報処理機器や通信機器のハードウェア（サーバー、PC、タブレット端末、スマートフォン等）
  - それらの上で動作するソフトウェアやファームウェア
  - クラウド環境上の仮想機器
- その他、守るべきもの
  - 自組織の社会的地位、社会的信用
  - 取引先との信頼関係

自組織の事業や活動を振り返って、これら「守るべきもの」を一通り洗い出す。

（２）自組織にとっての脅威を抽出する

自組織にとって「守るべきもの」が明らかになったら、それらに対する脅威を抽出する。

例えば、『10 大脅威 2025 組織編』を読み、そこに掲載されている脅威にさらされる「守るべきもの」がある場合を考えてみる。自組織にとって大きな損害・損失になると思った場合は、具体的な被害として脅威を書き出す。

自組織の「守るべきもの」に対して、該当する脅威があまり抽出できなかった場合は、過去にランクインした脅威の中に自組織にとって重要な脅威が含まれている可能性があるので、過去の『10 大脅威』も参照する。

具体的な被害を書き出す際は、それが『10 大脅威 2025 組織編』や過去の『10 大脅威 [1]』のどの脅威に対応するかをメモしておく。

脅威の抽出が終了したら、発生して欲しくない順番に脅威を並べ替える。例えば、自組織の想定被害額が大きい順番で脅威を並べ替えて、①②③…と番号を振る。

参考資料

1.情報セキュリティ10大脅威（IPA）
https://www.ipa.go.jp/security/10threats/index.html

（3）対策候補を洗い出す

自組織にとっての脅威を抽出したら、その元となった『10 大脅威　2025　組織編』や過去の『10 大脅威』の脅威とその対策を読み、各々の脅威に対して有効と考えられる対策候補を列挙する。

一つの脅威には複数の対策候補が存在し、対策候補の中には複数の脅威に対して有効なものが存在する。また、『10 大脅威』で紹介している対策は、その目的が「被害予防」「早期検知」「事後対応」に分類されるので、それらの分類を含めて、例えば、**表 1** のような表を作成して、脅威と対策候補の関係を整理すると良い。

表 1　脅威と対策候補の関係を整理する表形式の例

対策／対応		脅威				
		脅威①	脅威②	脅威③	脅威④	脅威⑤
被害予防	対策候補1	○	○	○	○	○
	対策候補2	○	○	○		
	対策候補3				○	○
早期検知	対策候補4	○		○		
事後対応	対策候補5				○	

（4）実施する対策を選択する

洗い出した対策候補の一つ一つに対して、実施状況（「実施済み」、「一部実施」、「未実施」のいずれであるか）を評価する。

「一部実施」、「未実施」の中から、今後実施する対策候補を選択する。全てを実施することが望ましいが、予算・時間・使用している機器の性能等の制約によって全てを実施することが困難な場合は、今後実施する（または一部実施から完全実施へ移行する）対策を選択する。選択にあたっては、以下のような要素を考慮する。

- 対策候補を実施するために必要な予算・時間・機器の性能等は十分か。それは実施可能か。
- 対策候補を実施しなかった場合の被害は何か。それは許容可能か。
- 対策候補を実施する代わりに、別の方法（例えば、特定の機能をオフにする）で代替可能か。
- 実務部門の担当者による運用が可能か。

追加で実施する対策候補が決まったならば、優先順位を付け、実施予定日を明らかにする。例えば、「今すぐに実施」、「一ヶ月以内に実施予定」、「半年以内に実施予定」、「一年以内に実施予定」等と分類する。今後は、実施計画に従い、未実施あるいは部分的に実施した対策に対する完全な実施をフォローしていく。

2. 組織の検討例

2.では、**1.**で紹介した検討方法に従って、**組織**にとっての脅威と対策を検討した例を示す。

【シナリオ】

〇〇商事は、自社開発の製品を含む日用生活雑貨を販売する中小企業である。創業以来、店頭販売を中心として店舗数を拡大してきたが、通信販売の売り上げを拡大して事業のもう一つの柱としたいと考え、数年前に自社が運営するオンラインショッピングサイトを立ち上げた。

A さんは、〇〇商事の IT システム管理グループに所属している。〇〇商事では、近年のサイバー攻撃の巧妙化が自社にとって大きな脅威になると考えており、A さんは、サイバー攻撃対策の見直しを上司から命じられた。毎年 IPA が公開する『10 大脅威』を読んでいた A さんは、それを活用して、自組織にとっての脅威と対策を検討することにした。

（1）「守るべきもの」の明確化

A さんは上司と相談しながら、自社にとって「守るべきもの」を洗い出した。売り上げを拡大したいと考えているオンラインショッピングシステムに加えて、製品開発・取引先との受発注業務に使用している社内 IT システム、それらが保有している情報やデータが大切であると考えた。

- 業務プロセス
  - オンラインショッピング事業
  - 取引先との受発注業務
- 情報・データ
  - 顧客情報（住所・氏名・クレジットカード情報等）
  - 取引先情報や受発注情報
- システム・サービス・機器
  - オンラインショッピングシステムとその構成機器
  - 社内 IT システムとその構成機器
- その他
  - 顧客からの信用
  - 取引先との信頼関係
  - 自社開発製品に関する機密情報

同僚と協力して検討する

上記の例では、A さんの会社のシステムは、オンラインショッピングシステムと社内 IT システムの二つだけと簡略化して説明しているが、実際には、イントラネットのポータル、勤怠管理システム、給与計算システム、メールシステム等、数多くのシステムを保有している場合がある。全てのシステムを一人の担当者が把握しているとは限らないので、複数の担当者で分担・協力しながら脅威と対策を検討することになるだろう。システムによっては、IT システム管理部門が詳細を把握していない場合もあり、所管部門と連携して進めなければならない。

（2）自組織に対する脅威の抽出

『10 大脅威　2025　組織編』や過去の『10 大脅威』を読みながら、A さんは「守るべきもの」がさらされるおそれのある脅威を抽出した。オンラインショッピングシステムや社内 IT システムに対する直接的な脅威に加えて、従業員のミスや内部不正によって生じる脅威、攻撃の踏み台とされて取引先に迷惑をかけるおそれについても、自組織に対する脅威として挙げた。関連部門の協力を得て、仮に脅威が生じた場合の被害額を算出し、会社の経営方針（事業の優先度）を考慮し、以下の通りに順位付けを行った。

① ランサムウェア感染による社内 IT システムの使用不能・脅迫
＜『10 大脅威　2025　組織編』1 位＞　ランサム攻撃による被害

② オンラインショッピングシステムからの顧客情報の漏えい
＜『10 大脅威　2025　組織編』3 位＞　システムの脆弱性を突いた攻撃

③ 登録会員向けメールマガジンの誤送信による顧客情報の漏えい
＜『10 大脅威　2025　組織編』10 位＞　不注意による情報漏えい等

④ 従業員による顧客情報や取引情報の不正持ち出し
＜『10 大脅威　2025　組織編』4 位＞　内部不正による情報漏えい等

⑤ 取引先である大企業へのサイバー攻撃の踏み台として悪用
＜『10 大脅威　2025　組織編』2 位＞　サプライチェーンや委託先を狙った攻撃

検討内容にお墨付き（了承）を得る

自組織の脅威に対する順位付けを一人で実施するのは難しい。上記の例では、脅威の順位は被害額の算出結果に基づくとしているが、算出にはシステム所管部門や経理部門の協力が必要になる可能性がある。

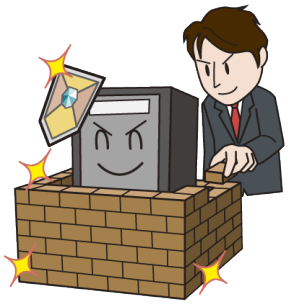
また、最終的な脅威の順位付けには、自組織が何を重視するのか等、組織の経営方針に依存するため、経営方針の決定部門の判断が必要になる場合もある。最終的に実施する対策を選定する際も同様であるが、検討過程の重要なポイント各所において、その内容に経営方針の決定部門（可能であれば経営者・経営層）の了承を得ておくことが重要になる。それができれば、その後の対策実施を速やかに進めることが出来るだろう。

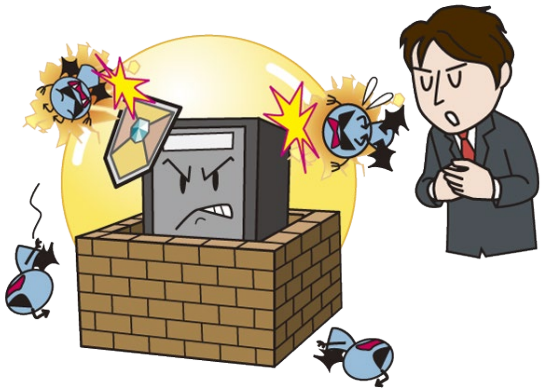
（3）対策候補の洗い出し

『10 大脅威　2025　組織編』や過去の『10 大脅威』の該当脅威を読みながら、A さんは対策候補を洗い出した。①～⑤の 5 種類の脅威を挙げたので、脅威と対策候補の関係を**表 2** に整理した。

（4）実施する対策の選定

洗い出した各対策候補について、A さんは現状を整理した。脅威と対策候補の関係表（**表 2**）の一番右に「実施状況」欄を設けたので、そこに「実施済み」、「一部実施」と記入していった。対策がどこまで出来ているか不明瞭なものについては「要調査」と記入し、IT システム管理部門の同僚と協力して調査することとした。





現状の対策状況を再確認した結果、導入済みファイアウォールの設定を急ぎ見直すこととした。オンラインショッピングシステム構築時以来、実施していなかったセキュリティ診断サービスは、予備費を活用して年度内に実施すべく上司を説得した。OS やソフトウェアの更新を計画的に実施すべく、社内のソフトウェア台帳をメンテナンスし、保守費を含む更新費用を漏れなく予算計上することとした。早期検知のための対策強化は、今後の課題として次年度以降に実施すべく、対応セキュリティ製品の調査に着手した。

実施したセキュリティ診断でオンラインショッピングシステムに脆弱性が発見されたが、これを速やかに対処してシステムの脆弱性を解消した A さんは、ほっと胸をなでおろした。

脅威と対策候補を効率的に検討する

表 2 の例では、社内の二つのシステムの脅威と対策候補を一つの表に整理してまとめた。社内に数多くのシステムが存在する場合、あるいは全てのシステムで共通に生じる脅威が少ない場合は、システム毎に別々の表を作成した方が効率的となる可能性がある。

複数の担当者で脅威と対策を検討するならば、分担して表を作成することも考えられる。この時に重要となるのが、可能な限り同一の判断基準で脅威と対策を検討することである。担当者毎の差異を最小化する方法の一つとして、検討課程や検討結果で用いる技術用語を統一するため、予め『10 大脅威』から抽出した用語集を作成しておき、それに従って作業を進める方法がある。

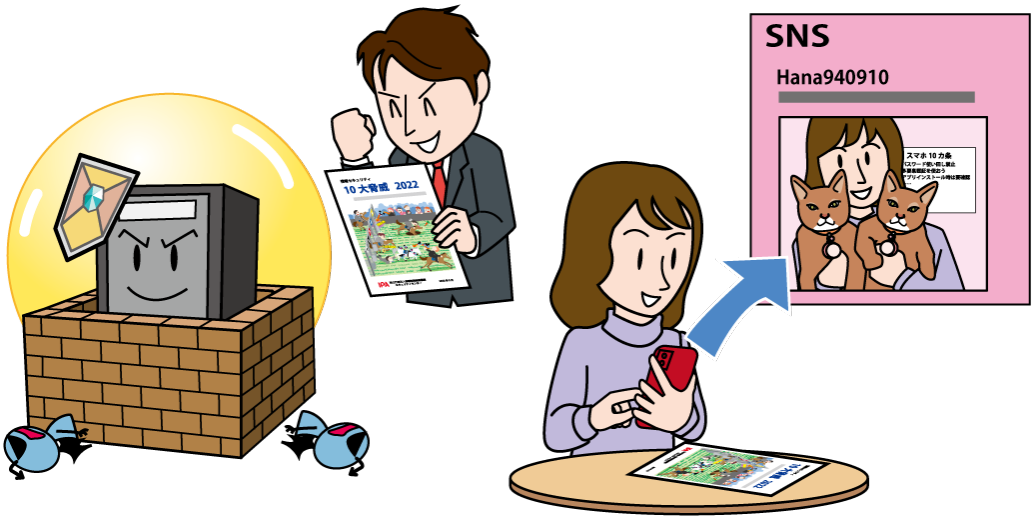
また、システム毎に表を作成すると膨大な数になるのであれば、例えば、システム構成や運用が類似しており、脅威の傾向が似通ったシステムをグループ化して、一つの表で整理した方が作業量を削減できる。

まずは一つのシステムに対して脅威と対策の検討を実施して、ノウハウを確立してから他のシステムの検討に着手する等、検討作業を効率的に進める工夫を考えるべきである。

表 2 組織における脅威と対策候補の洗い出し例

対策／対応		脅威					実施状況
		①	②	③	④	⑤	
組織としての体制の確立	**インシデント対応体制を整備し対応する**	○	○				
	セキュリティ対策の予算・体制の確保		○				
被害の予防及び被害に備えた対策	**インシデント対応体制を整備し対応する**	○	○			○	
	表1.3「情報セキュリティ対策の基本」を実施	○	○				
	メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない	○					
	多要素認証の設定を有効にする	○					
	提供元が不明なソフトウェアを実行しない	○					
	脆弱性情報の収集、対策状況の管理、パッチマネジメントの実施		○				
	サーバーやPC、ネットワークに適切なセキュリティ対策を行う	○	○			○	
	共有サーバー等へのアクセス権の最小化と管理の強化	○					
	公開サーバーへの不正アクセス対策	○					
	適切なバックアップ運用を行う	○					
	情報リテラシー、モラルを向上させる			○	○		
	確認プロセスに基づく運用			○			
	特定の担当者に業務が集中しない体制の構築			○			
	取り扱う情報の重要度を規定し、それに合わせた運用を行う			○			
	情報の保護（暗号化、認証）、機密情報の格納場所の把握、可視化			○			
	DLP（情報漏えい対策）製品の導入			○			
	外部に持ち出す情報や端末の制限			○			
	メールの誤送信対策等の導入			○			
	業務用携帯端末の紛失対策機能の有効化			○			
	HDDの廃棄の際、復旧できない方法での消去を周知し、徹底する			○			
	基本方針の策定				○		
	資産の把握、対応体制の整備		○		○		
	重要情報の管理、保護				○		
	物理的管理の実施				○		
	人的管理およびコンプライアンス教育の徹底				○		
	必要に応じ、秘密保持義務を課す誓約書に署名させる				○		
	定期的な職務の変更、職場の異動				○		
	情報管理規則の徹底					○	
	セキュリティ評価サービス（SRS）を用いた自組織のセキュリティ対策状況の把握					○	
	セキュリティのサポートが充実しているソフトウェアやバージョンを使う		○				
	信頼できる委託先、取引先、サービスの選定					○	
	契約内容の確認					○	
	委託先組織の管理					○	
	納品物の検証					○	
	取引先や委託先との連絡プロセスの確立					○	
	取引先や委託先の情報セキュリティ対応の確認、監査					○	
	情報セキュリティの認証取得					○	
	公的機関等が公開している資料の活用					○	
被害の早期検知	問題発生時の内部報告体制の整備			○			
	外部からの連絡窓口の設置			○			
	システム操作履歴の監視				○		
	適切なログの取得と継続的な監視						
	特定時期の監視の強化				○		
被害を受けた後の対応	**適切な報告／連絡／相談を行う**	○	○	○	○	○	
	適切なバックアップ運用を行う	○					
	インシデント対応体制を整備し対応する	○	○	○	○	○	
	被害への補償					○	
	内部不正者に対する適切な処罰の実施				○		

3. おわりに



本資料では、『10 大脅威 2025[1]』や過去の『10 大脅威』を活用して**自組織にとっての脅威と対策を検討する方法**を紹介した。

サイバー攻撃の脅威は、常に進化し続けており、また自組織の立場が変わることによって、新たな脅威にさらされるおそれがある。ここで紹介した脅威と対策の検討は、一度だけ実施して終了するものではない。例えば、A さんの会社のオンラインショッピングシステムが大成功を収めて、事業規模が大幅に拡大した場合、金銭目的のサイバー攻撃者の恰好の標的となり、ビジネスメール詐欺の攻撃を仕掛けられるかも知れない。この場合、今回の検討では対象外とした、**組織 9 位「ビジネスメール詐欺」**にも注目しなければならない。定期的に脅威と対策の検討を見直す動機付けとして、毎年 IPA から『10 大脅威』が公開されるタイミングを利用するのも一手段である。

今回は、主に構築済みのシステムやサービスを利用する立場の組織や個人の方を対象として、脅威と対策を簡易に検討する方法を紹介した。新しく構築するシステムやサービスの設計・開発に関わる立場の方に対しては、サイバー攻撃者の立場から具体的な攻撃方法を想定し、より詳細に脅威と対策を分析・検討する方法を『IoT 開発におけるセキュリティ設計の手引き』[2] にて紹介しているので、参考としていただきたい。

参考資料

1.情報セキュリティ10大脅威 2025（IPA）
https://www.ipa.go.jp/security/10threats/10threats2025.html
2.「IoT開発におけるセキュリティ設計の手引き」を公開（IPA）
https://www.ipa.go.jp/security/iot/iotguide.html

著作・制作　　独立行政法人情報処理推進機構（IPA）

執筆者　　土屋　正　　篠塚　耕一

イラスト製作　　株式会社　創樹

情報セキュリティ 10 大脅威の活用法

情報セキュリティ 10 大脅威　2025　版

2025 年　2 月 28 日　初　版

［事務局・発行］　独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス

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