

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 2023 版



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 2023」

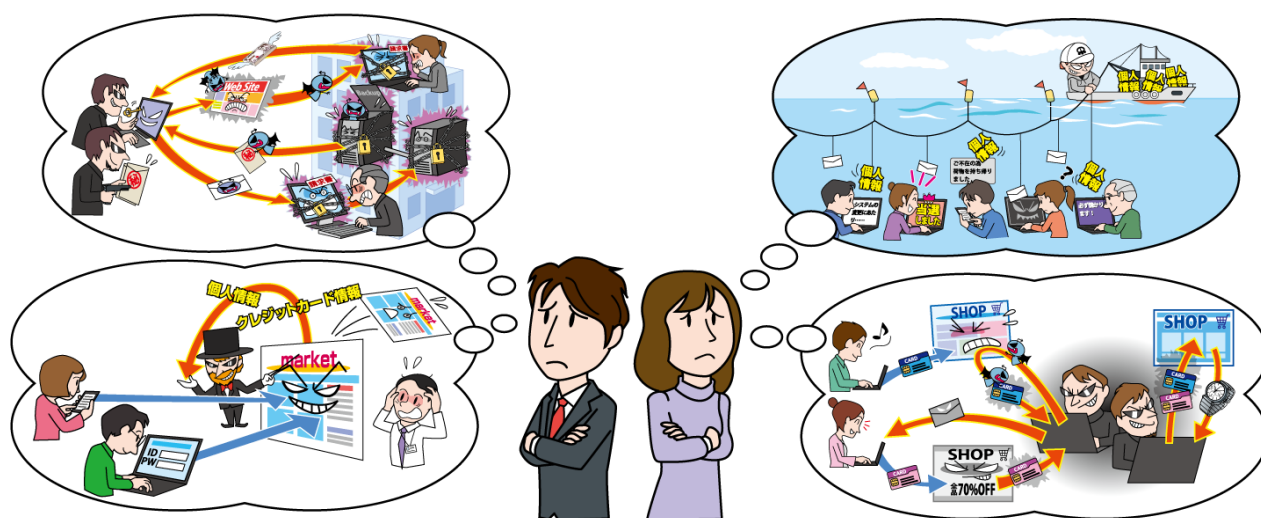
<https://www.ipa.go.jp/security/10threats/10threats2023.html>

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. 個人の検討例	13
4. おわりに.....	17

情報セキュリティ 10 大脅威の活用法

～自組織／自分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の方々は、熟読されていると考える。また、セキュリティ対策に十分な予算をお持ちの組織の方々は、『10 大脅威』にランクインした全ての脅威に対して、対策実施を検討されているだろう。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」といった声を伺うことも多い。

時には、「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」といったお話を伺うこともあり、『10 大脅威 2023』の冒頭において、『10 大脅威』をお読みになる上での留意事項を掲載している（下記抜粋）。

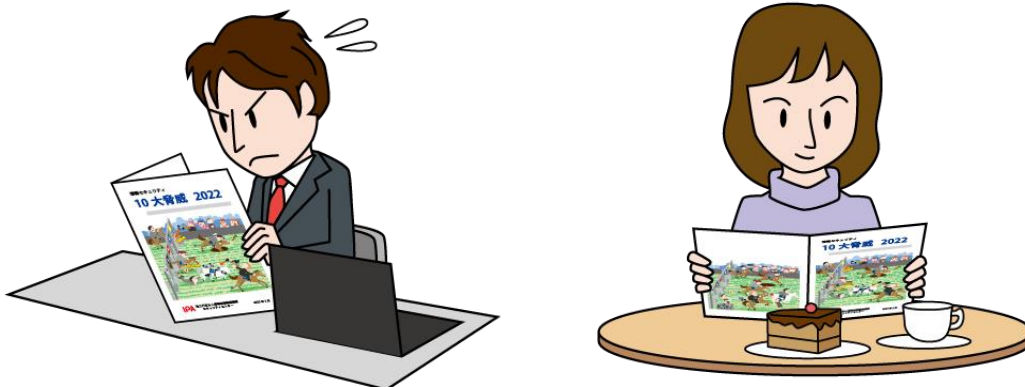
■「情報セキュリティ 10 大脅威 2023」をお読みになる上での留意事項

- ① 順位に捉われず、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』の順位は、「10 大脅威選考会」の投票結果により、社会全体として重要度が高いと考えられるものを選定、順位付けしたものである。上記の項番①②では、自組織や自分自身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や自分自身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 2023』に示した脅威と対策の解説書を活用しながら、組織や個人にとって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



自組織や自分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やランク外となった脅威の中から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（ベストプラクティス）を洗い出す。そして、予算等を考慮して、実施する対策を選択することになる。これは、以下の様なステップで脅威と対策を検討する。

（1）自組織／自分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（組織の場合）や自分（個人の場合）にとって、サイバー攻撃を受けて被害を受けたくない「守るべきもの」は何かを明らかにする。守るべきものには、以下が含まれる。

【組織の場合】

- 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」やシステム上で実現されている「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
- その他、守るべきもの
 - － 自組織の社会的地位、社会における信用性
 - － 取引先との信頼関係

【個人の場合】

- 自分が所有する「機器」
 - 情報処理機器や通信機器のハードウェア(PC、タブレット端末、スマートフォン、ルーター等)
 - それらの上で動作するソフトウェアやファームウェア
- 上記「機器」を用いて利用している「機能」や「サービス」
 - 自分が保有・構築・運用しているシステムによって実現されている機能やサービス
 - 他者が保有・構築・運用しているシステムによって提供されている機能やサービス
- 自分にとって重要な「情報」や「データ」
 - 上記「機器」内部に保存されている情報やデータ(アドレス帳やメール・写真等)
 - 利用中の機能やサービスに入力する情報やデータ(ログイン名、パスワードやクレジットカード番号等)
- その他、守るべきもの
 - 自分の社会的地位、社会における信用性
 - 友人との信頼関係

自組織の事業や活動、自分の生活行動様式を振り返って、これらの守るべきものを可能な限り洗い出す。

(2) 自組織／自分にとっての脅威を抽出する。

自組織／自分にとって「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 2023』を読み、掲載されている脅威が「守るべきもの」に対して発生した場合を想像する。自組織／自分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／自分の「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、ランク外となった脅威の中に自組織／自分にとって重要な脅威が含まれている可能性があるため、過去の『10 大脅威』も参照してみるとよい。

具体的な被害を書き出す際は、それが『10 大脅威 2023』や過去の『10 大脅威』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、組織であれば、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。



(3) 対策候補(ベストプラクティス)を洗い出す。

自組織／自分にとっての脅威を抽出したら、その元となった『10 大脅威 2023』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(ベストプラクティス)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 の様な表を作成して、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。選択に当たっては、以下の様な要素を考慮する。

- 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。それは実施可能か否か。
- 対策候補を実施しなかった場合の被害は何か。それは許容可能か否か。
- 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)で代替可能か否か。

追加実施する対策候補が決ったならば、優先順位付けを行い、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、実施予定計画に従って未実施あるいは部分的実施の対策の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常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出店を拡大してきたが、数年前から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、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ている。

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



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システムの二つに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もある。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

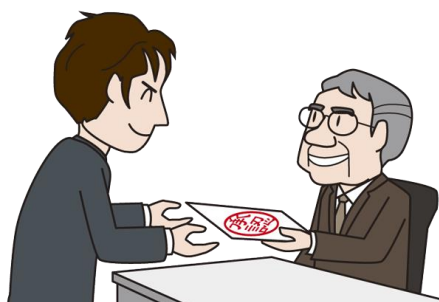
『10 大脅威 2023』や過去の『10 大脅威』を読みながら、Aさんは「守るべきもの」に対して発生し得る脅威を抽出した。オンラインショッピングシステムや社内 IT システムに対する直接的な脅威に加えて、従業員のミスや内部不正によって生じる脅威、攻撃の踏み台とされて取引先に迷惑をかける恐れについても、自組織に対する脅威として挙げた。関連部門の協力を得て、仮に脅威が生じた場合の被害額を算出し、会社の経営方針(事業の優先度)を考慮し、以下の通り順位付けを行った。



- 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 2023」組織 1 位＞ ランサムウェアによる被害
- 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 2020」組織 8 位＞ インターネット上のサービスからの個人情報の窃取
- ③ 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・不正操作
＜「10 大脅威 2021」組織 8 位＞ インターネット上のサービスへの不正ログイン
- ④ 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 2023」組織 9 位＞ 不注意による情報漏えい等の被害
- ⑤ 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 2023」組織 4 位＞ 内部不正による情報漏えい
- ⑥ 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 2023」組織 2 位＞ サプライチェーンの弱点を悪用した攻撃

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、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かも知れない。



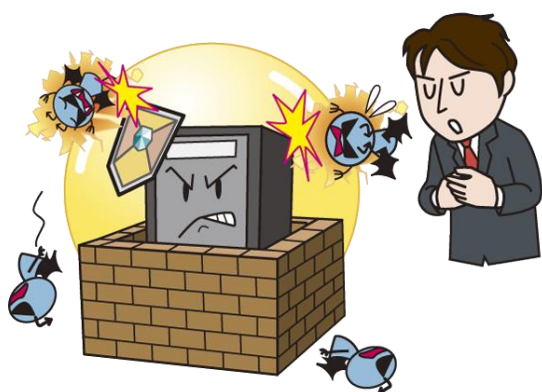
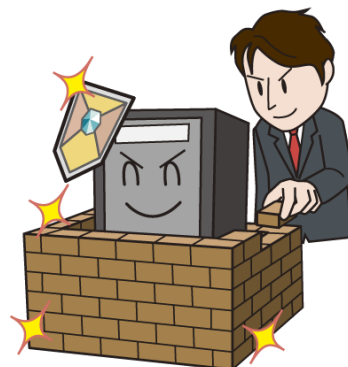
また、最終的な脅威の順位付けには、自組織が何を重視するのか、組織の経営方針に依存するため、経営方針の決定部門の判断が必要となる場合がある。最終的に実施する対策を選定する際も同様であるが、検討課程の重要なポイント各所において、その内容に経営方針の決定部門(可能であれば経営者・経営層)の了承を得て置くことが重要であり、その後の対策実施を速やかに進めることが出来るだろう。

(3) 対策候補(ベストプラクティス)の洗い出し

『10 大脅威 2023』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(ベストプラクティス)を洗い出した。①～⑥の 6 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かも知れない。

複数の担当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。このとき重要となるのが、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よう。

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	⑥	
情報モラルの向上や	従業員のセキュリティ意識教育				○			
	組織規程および確認プロセスの確立				○			
	組織規程および確認プロセスの見直し				○			
	人的管理及びコンプライアンス教育の徹底					○		
被害の予防	「情報セキュリティ対策の基本」を実施	○	○	○				
	セキュリティ対策の予算・体制の確保		○	○				
	利用者に対するセキュリティ機能の提供		○	○				
	迅速かつ継続的に対応できる体制（CSIRT等）の構築	○						
	多要素認証の設定を有効にする	○						
	添付ファイルやリンクを安易にクリックしない	○						
	提供元が不明なソフトウェアを実行しない	○						
	機器の脆弱性対策を迅速に行う	○						
	セキュリティ対策ツールの利用や設定見直し	○						
	ネットワーク分離	○						
	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	○						
	バックアップの取得	○						
	セキュアなインターネット上のサービス構築		○					
	セキュア開発ライフサイクルの実践		○					
	セキュリティバイデザインの実施		○					
	セキュリティ診断（ウェブアプリケーション診断、プラットフォーム診断等）の実施		○					
	WAF、IDS/IPSの導入		○					
	ミドルウェアやライブラリ利用状況の把握		○					
	アカウントの存在有無の確認に悪用されないサービス設計			○				
	確認プロセスに基づく運用				○			
	情報の保護（暗号化、認証）、機密情報の格納場所の掌握、可視化				○			
	DLP（情報漏洩対策）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				○				

対策／対応		脅威						実施状況
		①	②	③	④	⑤	⑥	
被害の予防	基本方針の策定					○		
	資産の把握、体制の整備					○		
	重要情報の管理、保護					○		
	物理的管理の実施					○		
	業務委託や情報管理における規則の徹底						○	
	報告体制等の問題発生時の運用規則整備						○	
	信頼できる委託先、取引先組織の選定						○	
	複数の取引先候補の検討						○	
	納品物の検証						○	
	契約内容の確認						○	
	委託先組織の管理						○	
	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						○	
	公的機関が公開している資料の活用						○	
早期被害の検知	適切なログの取得と継続的な監視		○	○				
	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					○		
被害を受けた後の対応	CSIRT への連絡							
	関係者、関係機関への連絡	○	○	○	○	○	○	
	組織の方針に従い各所へ報告、相談する							
	影響調査および原因の追究、対策の強化	○	○	○	○	○	○	
	漏えいした内容や発生原因等の公表		○	○	○			
	情報漏えいの被害者に対するすみやかな連絡と補償 被害への補償		○	○			○	
	セキュリティ専門企業への調査依頼		○	○				
	迅速な隔離を行うとともに、関連組織、取引先への連携を行い被害拡大の防止	○						
	バックアップからの復旧	○						
	復号ツールの活用	○						
被害拡大や二次被害要因の排除				○				
内部不正者に対する適切な処罰の実施					○			

3. 個人の検討例

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

【シナリオ】

Bさんは、社会人になって3年目、スマートフォンのヘビーユーザーである。

娯楽・友人との友好関係を目的とした SNS やゲームの利用に加えて、スマホ決済やオンラインショッピングでの利用等、自分専用の PC を持っていない Bさんの毎日の生活において、スマートフォンは不可欠な存在となっている。Bさんはまだ使用していないが、インターネットバンキングを利用している先輩の Cさんから、アカウント情報が漏えいして大変な目にあつたという話を聞いた。勤務先で使用している PC の設定でお世話になっている IT システム管理グループの Aさんに相談したところ、先日セキュリティ教育で使用した、IPA の『10 大脅威』の【個人編】が参考になる、と教えてくれた。Bさんは、『10 大脅威』の最新版をダウンロードして、自分にとっての脅威と対策は何かを考えてみようと思った。

(1) 「守るべきもの」の明確化

Bさんは、自分のスマートフォンの使い方を思い出しながら、自分にとって「守るべきもの」を洗い出した。自分の生活の様々な局面でスマートフォンに依存していること、重要なデータをスマートフォン内部に保存したり、会員になっているシステムに登録したりしていることを再認識した。

- 機器・機能・サービス
 - スマートフォン
 - SNS
 - スマホ決済
 - オンラインショッピング
- 情報・データ
 - スマートフォン内部に保存している個人情報（友人の情報を含む）
 - （スマホ決済やオンラインショッピングサイトに登録した）銀行口座やクレジットカード情報
- その他
 - スマートフォンを悪用した詐欺や脅迫に遭わないこと
 - 友人との信頼関係



(2) 自分に対する脅威の抽出

『10 大脅威 2023』の解説書を読みながら、Bさんは「守るべきもの」に対して発生し得る脅威を抽出した。個人 1 位～10 位には、スマートフォンに関連する脅威が数多くランクインしており、スマートフォンに対するサイバー攻撃の脅威を再認識した。



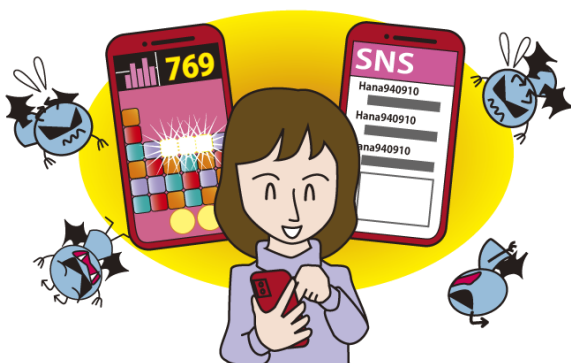
- ① どうしても欲しいチケットがあり、偽サイトでクレジットカード情報を入力してしまい、カードを不正利用されてしまう。
 <「10 大脅威 2023」個人 1 位> フィッシングによる個人情報等の詐取
 <「10 大脅威 2023」個人 4 位> クレジットカード情報の不正利用
- ② 不正アプリをインストールしてしまい、スマートフォン内部の友人の情報を窃取されてしまう。
 <「10 大脅威 2023」個人 6 位> 不正アプリによるスマートフォン利用者への被害
- ③ SNS のアカウントを乗っ取られてしまい、勝手に偽の投稿をされてしまう。
 <「10 大脅威 2023」個人 9 位> インターネット上のサービスへの不正ログイン
- ④ スマホ決済サービスを不正利用されて、自分のポイントを勝手に使われてしまう。
 <「10 大脅威 2023」個人 5 位> スマホ決済の不正利用
- ⑤ 脅迫メールが送られてくる。
 <「10 大脅威 2023」個人 3 位> メールや SMS 等を使った脅迫・詐欺の手口による金銭要求
- ⑥ いつも利用しているオンラインショッピングサイトから「登録した個人情報に漏えいした」とお詫びの連絡がある。
 <「10 大脅威 2023」個人 8 位> インターネット上のサービスからの個人情報の窃取

(3) 対策候補(ベストプラクティス)の洗い出し

『10 大脅威 2023』の該当脅威を読みながら、B さんは対策候補(ベストプラクティス)を洗い出した。①～⑥の6種類の脅威に対して、脅威と対策候補の関係を整理して、表 3 を作成した。

(4) 実施する対策の選定

洗い出した各対策候補について、B さんは現状を整理し、脅威と対策候補の関係表(表 3)の「実施状況」欄に、実施済みの対策には「○」を記入していった。表形式に整理すると、幾つかの基本的な対策は、複数の脅威に有効であることが分かった。既に実施している対策もあったが、新しいアプリをインストールした際に忘れてしまうかも知れないと考えた B さんは、『10 大脅威 2017』¹ の1章「情報セキュリティ対策の基本 スマートフォン編」も参考にしつつ、必ず実施すべきと考えた対策(「パスワードの使い回し禁止」等)を「スマホ 10 カ条」として書き出して、自室の壁に貼ることにした。



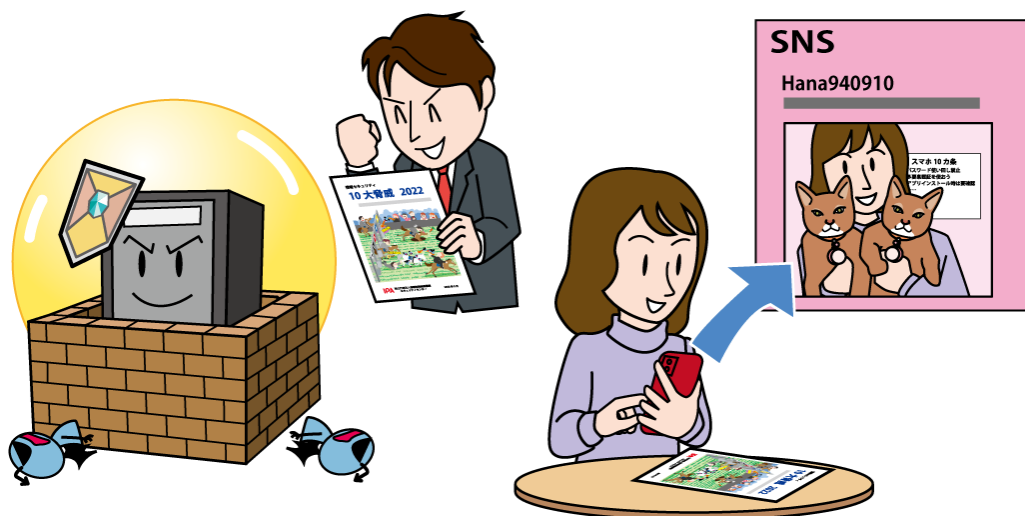
日常生活の中での様々なスマートフォンの利用面における脅威を正しく認識した B さんは、各種対策を忘れずに実行しつつ、今までと同様に、今まで以上に、スマートフォンを活用して充実した生活を送っている。インターネットバンキングにも興味があるので、『10 大脅威 2022』個人 9 位「インターネットバンキングの不正利用」を読みつつ、先輩の C さんの話を聞き、情報を集め始めた。

表3 個人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	⑥	
被害の予防	「情報セキュリティ対策の基本」を実施	○	○	○	○	○	○	
	SMS やメールで受信した URL や、SNS の投稿内の URL を安易にクリックしない	○						
	添付ファイルや URL を安易にクリックしない	○		○			○	
	不審なウェブサイトや安易に認証情報を入力しない (フィッシングに注意)			○	○		○	
	普段は表示されないような画面やポップアップが表示された場合、情報を入力しない	○						
	受信した脅迫、詐欺メールは無視する					○		
	メールに記載されている番号に電話をしない					○		
	メールで要求された支払いには応じない					○		
	アプリは公式マーケットから入手		○					
	アプリインストール時のアクセス権限の確認		○					
	アプリインストールに関する設定に注意		○					
	不要なアプリをインストールしない		○					
	利用しないアプリはアンインストールする		○					
	パスワードは長く、複雑にする			○	○		○	
	パスワードを使い回さない			○	○		○	
	パスワード管理ソフトの利用			○	○		○	
	サービスが推奨する認証方式の利用			○			○	
	多要素認証の設定を有効にする	○			○	○	○	
	3D セキュアを利用する				○			
	クレジットカード会社が提供している本人認証サービス (3D セキュア等) の利用	○						
	迷惑メールフィルターを利用	○						
	いつもと異なるログインがあった場合に通知する設定を有効にする	○						
	利用していないサービスからの退会			○	○		○	
	スマートフォンの紛失対策				○			
	プリペイドカードの利用を検討	○						
サービス利用の必要性を判断する						○		
不要な情報は安易に登録しない						○		

対策／対応		脅威						実施状況
		①	②	③	④	⑤	⑥	
被害の早期検知	利用しているサービスのログイン履歴の確認	○		○				
	クレジットカードやポイント等の利用履歴の定期的な確認			○				
	スマホ決済サービスの利用状況通知機能の利用および利用履歴の定期的な確認				○			
	連携する銀行口座の出金履歴の確認				○			
	クレジットカードやインターネットバンキングの利用明細を確認	○						
	クレジットカード利用明細の定期的な確認	○					○	
	サービス利用状況の通知機能の利用	○						
被害を受けた後の対応	不正アプリのアンインストール		○					
	パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）	○		○	○	○	○	
	ウイルス感染した端末の初期化	○						
	クレジットカードの停止	○		○			○	
	サービス運営者（コールセンター等）へ連絡	○		○	○		○	
	連携する金融機関へ連絡				○			
	警察への被害届の提出	○		○			○	
	警察に相談する				○	○		
	信頼できる機関に相談	○						

4. おわりに



本資料では、『10 大脅威 2023』や過去の『10 大脅威』を活用して自組織／自分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／自分の立場が変わることによって、新たな脅威が生じる恐れがある。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 7 位「ビジネスメール詐欺による金銭被害」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 2017 (IPA)
<https://www.ipa.go.jp/security/10threats/2017/2017.html>
2. IoTのセキュリティ(IPA)
<https://www.ipa.go.jp/security/iot/index.html>



著作・制作

独立行政法人情報処理推進機構 (IPA)

執筆者

内海 百葉 亀山 友彦 土屋 正

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 2023 版

2023 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/>