情報セキュリティ 10 大脅威 2020

情報セキュリティ 10 大脅威の活用法

独立行政法人情報処理推進機構
セキュリティセンター

2020 年 3 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 2020」
https://www.ipa.go.jp/security/vuln/10threats2020.html

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』（以下、『10 大脅威』と略す）の解説資料を、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」といったお話しを伺うこともあり、昨年公開した『情報セキュリティ 10 大脅威 2019』[1] の1章では、『10 大脅威』をお読みになる上での留意事項を掲載した（下記抜粋）。

■「情報セキュリティ 10 大脅威 2019」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た。『情報セキュリティ 10 大脅威 2020 各脅威の解説資料』（以下、『各脅威の解説資料』と略す）の冒頭においても、同様の留意事項を掲載している。

本資料では、『各脅威の解説資料』に示した『10 大脅威』の脅威と対策の解説を活用しながら、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、『各脅威の解説資料』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ので、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『各脅威の解説資料』や過去の『10 大脅威』の 2 章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『各脅威の解説資料』や過去の『10 大脅威』の 2 章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、2章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。その条件を満たして、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『情報セキュリティ 10 大脅威』を読んでいた A さんは、『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

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。

- その他
  - 顧客からの信用性
  - 取引先との信頼関係

（2）自組織に対する脅威の抽出

『各脅威の解説資料』や過去の『10 大脅威』の 2 章を読みながら、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 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
＜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
② DDoS 攻撃によるオンラインショッピングシステムへの妨害・脅迫
＜組織 10 位＞ サービス妨害攻撃によるサービスの停止
③ 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
＜組織 5 位＞ ランサムウェアによる被害
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
＜組織 7 位＞ 不注意による情報漏えい
⑤ 従業員による顧客情報や取引情報の不正持ち出し
＜組織 2 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
＜組織 4 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

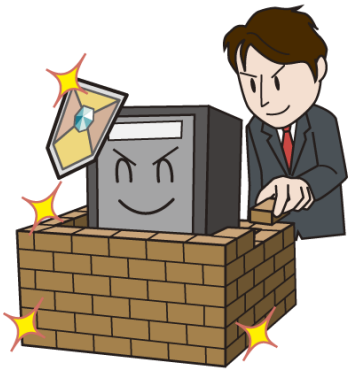
自組織の脅威に対する順位付けを一人で実施するのは難しい。上記の例では、被害額の算出結果に基づくとしているが、算出にはシステム所管部門や経理部門の協力が必要になるかも知れない。

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。

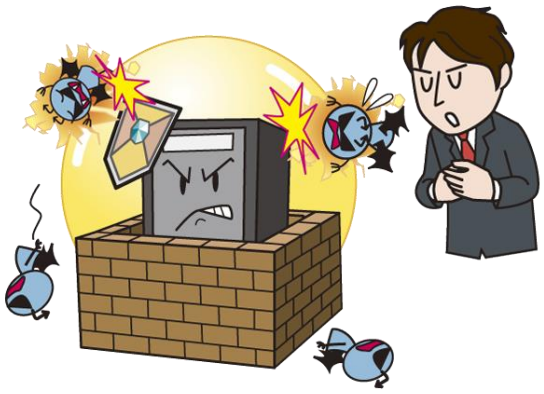
（３）対策候補（ベストプラクティス）の洗い出し

『各脅威の解説資料』や過去の『10 大脅威』の 2 章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。DDoS 攻撃対策や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。

緊急点検の結果、オンラインショッピングシステムに発見された脆弱性を解消した 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、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の表になるのであれば、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可能である。

先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	
被害予防	基本的な対策の実施	○		○			適宜選択	
	セキュリティ対策の予算・体制の確保	○		○				
	インターネット上のセキュアなサービス構築	○						
	セキュリティ診断の実施	○						
	WAF、IDS/IPS の導入	○	○					
	利用者に対するセキュリティ機能の提供	○						
	DDoS 攻撃緩和サービスの利用		○					
	システムの冗長化等の軽減策		○					
	ネットワークの冗長化		○					
	代替サーバーの用意と告知手段の整備		○					
	受信メールやウェブサイトの十分な確認			○				
	サポート切れ OS の利用停止、移行			○				
	フィルタリングツールの活用			○				
	共用サーバーへのアクセス権の最小化			○				
	バックアップの取得			○				
	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				○			
	重要資産の把握、管理体制の整備					○		
	重要情報の管理、保護				○	○		
	人的管理およびコンプライアンス教育の徹底					○		
早期検知	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					○		
事後対応	セキュリティ専門企業への調査依頼	○						
	影響調査および原因の追究	○	○	○		○	○	
	漏えいした内容や発生原因の公表	○			○			
	関係者、関係機関への連絡	○			○	○		
	通信制御		○					
	利用者への状況の告知		○					
	バックアップによる復旧			○				
	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実施					○		
	取引先への連絡						○	

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っ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『情報セキュリティ 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

『各脅威の解説資料』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～個人 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 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。
＜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

② 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。
＜個人 8 位＞ インターネット上のサービスへの不正ログイン

③ 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。
＜個人 1 位＞ スマホ決済の不正利用

④ 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。
＜個人 2 位＞ フィッシングによる個人情報等の窃取
＜個人 3 位＞ クレジットカード情報の不正利用

⑤ 脅迫メールが送られてくる。
＜個人 5 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

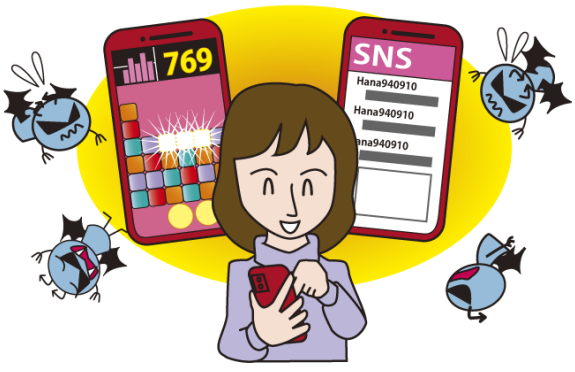
⑥ いつも利用しているオンラインショッピングサイトから「登録した個人情報が漏えいした」とお詫びの連絡がある。
＜個人 10 位＞ インターネット上のサービスからの個人情報の窃取

（3）対策候補（ベストプラクティス）の洗い出し

『各脅威の解説資料』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「備考欄」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、『情報セキュリティ 10 大脅威 2017』[2] 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。

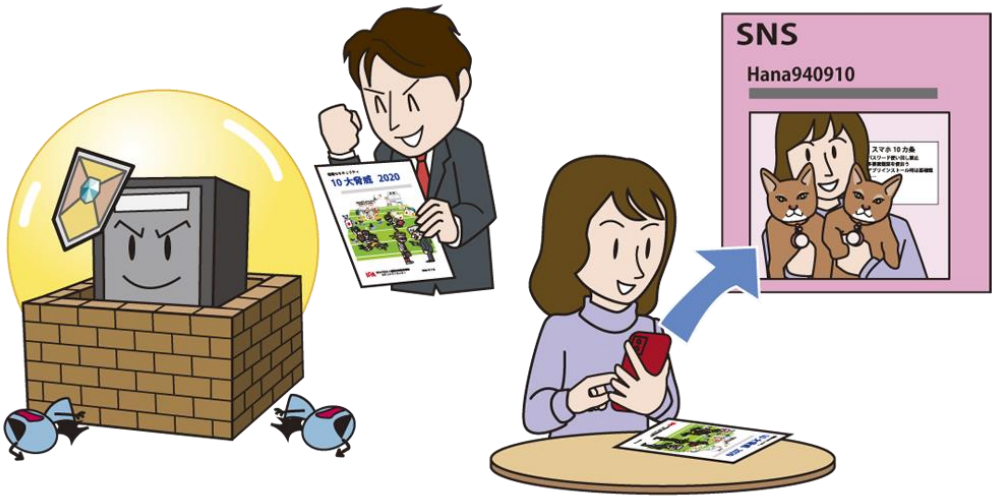


日常生活の中での様々なスマートフォンの利用面における脅威を正しく認識した B さんは、各種対策を忘れずに実行しつつ、今までと同様に、今まで以上に、スマートフォンを活用して充実した生活を送っている。インターネットバンキングにも興味があるので、『10 大脅威』**個人 4 位「インターネットバンキングの不正利用」**を読みつつ、先輩の C さんの話を聞き、情報を集め始めた。

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						備考
		①	②	③	④	⑤	⑥	
被害予防	基本的な対策の実施	○	○	○	○	○	○	
	公式マーケットからのアプリ入手	○						
	アプリインストール時のアクセス権確認	○						
	アプリインストールに関する設定注意	○						
	不要なアプリをインストールしない	○						
	添付ファイルやリンクの安易なクリック禁止		○		○			
	長く複雑なパスワードの使用		○	○			○	
	パスワードの使いまわしをしない		○	○	○		○	
	パスワード管理ソフトの使用		○	○			○	
	二要素認証や多要素認証の使用		○	○	○		○	
	不審なウェブサイトで認証情報を入力しない		○	○			○	
	利用していないサービスからの退会		○	○			○	
	過剰なチャージをしない			○				
	スマートフォンの盗難・紛失対策			○				
	受信したメールやウェブサイトの安全確認				○			
	受信した詐欺・脅迫メールの無視					○		
	不審メール送信者にこちらから連絡しない					○		
	必須項目以外はサービスに登録しない						○	
早期検知	利用しているサービスのログイン履歴確認		○	○	○			
	クレジットカードやポイントの利用履歴確認		○		○		○	
	スマホ決済サービスの利用履歴確認			○				
	利用状況の通知機能等の使用			○	○			
事後対応	不正アプリのアンインストール	○						
	パスワードの変更		○	○	○	○	○	
	クレジットカードや銀行口座の停止手続き		○	○	○		○	
	サービス運営者への連絡		○	○	○		○	
	信頼できる機関に相談／被害届の提出				○	○	○	

4. おわりに



本資料では、『10 大脅威 2020 各脅威の解説資料』や過去の『10 大脅威』の 2 章を活用して**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 3 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』[3] 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. IPA: 情報セキュリティ10大脅威 2019
https://www.ipa.go.jp/security/vuln/10threats2019.html
2. IPA: 情報セキュリティ10大脅威 2017
https://www.ipa.go.jp/security/vuln/10threats2017.html
3. IPA: IoT開発におけるセキュリティ設計の手引き
https://www.ipa.go.jp/security/iot/iotguide.html

10 大脅威選考会

氏名	所属	氏名	所属
石田 淳一	(株)アールジェイ	窪田 敏明	(株)神戸デジタル・ラボ
菅原 尚志	アクセンチュア(株)	宮﨑 清隆	国際マネジメントシステム認証機構(株)
中嶋 美貴	アクセンチュア(株)	萩原 健太	(社)コンピュータソフトウェア協会
石井 彰	旭化成(株)	福森 大喜	(株)サイバーディフェンス研究所
岡田 良太郎	(株)アスタリスク・リサーチ	荒川 大	(一社)サイバーリスク情報センター
徳丸 浩	EG セキュアソリューションズ(株)	宮内 伸崇	(株)サイント
安西 真人	(株)エーアイセキュリティラボ	奥石 隆	(社) JPCERT コーディネーションセンター
佐藤 直之	SCSK(株)	福本 郁哉	(社) JPCERT コーディネーションセンター
鈴木 寛明	SCSK(株)	唐沢 勇輔	Japan Digital Design(株)
大塚 淳平	NRI セキュアテクノロジーズ(株)	大久保 隆夫	情報セキュリティ大学院大学
小林 克巳	NRI セキュアテクノロジーズ(株)	東 恵寿	NPO セカンドワーク協会
芳賀 夢久	NRI セキュアテクノロジーズ(株)	金城 夏樹	(株)セキュアイノベーション
杉井 俊也	NEC フィールディング(株)	栗田 智明	(株)セキュアイノベーション
真鍋 太郎	NTT コミュニケーションズ(株)	鉢嶺 光	(株)セキュアイノベーション
北河 拓士	NTT コム ソリューションズ(株)	阿部 実洋	(株)セキュアベース
斯波 彰	NTT コム ソリューションズ(株)	薩摩 晴美	(一社)セキュリティ対策推進協議会
小林 義徳	(株)NTT データ	林 達也	(一社)セキュリティ対策推進協議会
宮本 久仁男	(株)NTT データ	持田 啓司	(一社)セキュリティ対策推進協議会
矢竹 清一郎	(株)NTT データ	澤永 敏郎	ソースネクスト(株)
池田 和生	NTTデータ先端技術(株)	勝海 直人	(株)ソニー・インタラクティブエンタテインメント
植草 祐則	NTTデータ先端技術(株)	坂本 高史	(株)ソニー・インタラクティブエンタテインメント
楯 研人	エムオーテックス(株)	相馬 基邦	(株)ソニー・インタラクティブエンタテインメント
徳毛 博幸	エムオーテックス(株)	中西 基裕	ソフトバンク(株)
間嶋 英之	エムオーテックス(株)	小島 博行	地方公共団体情報システム機構
池田 耕作	(株)オージス総研	金城 賀真	地方公共団体情報システム機構
岡村 耕二	九州大学	鈴木 一弘	地方公共団体情報システム機構
小関 直樹	京セラコミュニケーションシステム(株)	田中 卓朗	TIS(株)
佐藤 宏昭	京セラコミュニケーションシステム(株)	三木 基司	TIS(株)
西山 健太	京セラコミュニケーションシステム(株)	大谷 毅典	DXC テクノロジー・ジャパン(株)
高崎 庸一	グローバルセキュリティエキスパート(株)	前田 隆行	DXC テクノロジー・ジャパン(株)
三木 剛	グローバルセキュリティエキスパート(株)	黒岩 亮	(株)ディー・エヌ・エー
武藤 耕也	グローバルセキュリティエキスパート(株)	松本 隆	(株)ディー・エヌ・エー
遠藤 誠	(株)ケイテック	安永 貴之	(株)ディー・エヌ・エー
新井 哲	KDDI デジタルセキュリティ(株)	内山 巧	(株)電算
岩瀬 巧	KDDI デジタルセキュリティ(株)	坂 明	(公財)東京オリンピック・パラリンピック競技大会組織委員会
町田 則文	KDDI デジタルセキュリティ(株)	石川 朝久	東京海上ホールディングス(株)
小熊 慶一郎	(株)KBIZ / (ISC)2	小島 健司	(株)東芝
保村 啓太	KPMG コンサルティング(株)	田岡 聡	(株)東芝
飯島 憂	(株)神戸デジタル・ラボ	大浪 大介	東芝インフォメーションシステムズ(株)
梅津 直弥	(株)神戸デジタル・ラボ	原田 博久	(株)Doctor Web Pacific

氏名	所属	氏名	所属
大山 水帆	戸田市役所	荒井 大輔	(株)Bridge
今 佑輔	トレンドマイクロ(株)	柳川 俊一	(株)Bridge
加藤 雅彦	長崎県立大学	今野 俊一	Broadcom Inc.
須川 賢洋	新潟大学	林 聡	Broadcom Inc.
猪股 秀樹	日本アイ・ビー・エム(株)	山内 正	Broadcom Inc.
上村 理	日本アイ・ビー・エム(株)	島田 敏宏	(株)ベリサーブ
山下 慶子	日本アイ・ビー・エム(株)	樅山 清	(株)ベリサーブ
初見 卓也	(一財)日本情報経済社会推進協会	太田 良典	弁護士ドットコム(株)
磯田 弘司	日本電気(株)	垣内 由梨香	マイクロソフトコーポレーション
谷川 哲司	日本電気(株)	増田 博史	マイクロソフトコーポレーション
淵上 真一	日本電気(株)	山室 太平	マカフィー(株)
住本 順一	日本電信電話(株)	小屋 晋吾	(株)豆蔵ホールディングス
中島 周摩	NortonLifeLock Inc.	高江洲 勲	三井物産セキュアディレクション(株)
古谷 尋	NortonLifeLock Inc.	東内 裕二	三井物産セキュアディレクション(株)
常川 直樹	パナソニック(株)	山谷 晶英	三井物産セキュアディレクション(株)
渡辺 久晃	パナソニック(株)	村野 正泰	(株)三菱総合研究所
林 薫	パロアルトネットワークス(株)	古澤 一憲	(株)三菱総合研究所
浜田 譲治	PwC コンサルティング合同会社	平田 真由美	みゅーらぼ
岩佐 功	東日本電信電話(株)	石井 崇喜	(株)ユービーセキュア
齊藤 純一郎	東日本電信電話(株)	関根 鉄平	(株)ユービーセキュア
水越 一郎	東日本電信電話(株)	八幡 美希	(株)ユービーセキュア
折田 彰	(株)日立システムズ	島田 理枝	(株)ユビテック
寺田 真敏	(株)日立製作所	松田 和宏	(株)ユビテック
古賀 洋一郎	ビッグローブ(株)	福本 佳成	楽天(株)
山口 裕也	(株)ファイブドライブ	橘 喜胤	楽天ウォレット(株)
大高 利夫	藤沢市役所	山崎 圭吾	(株)ラック
原 和宏	富士通(株)	若居 和直	(株)ラック
原田 弘和	富士通(株)	有森 貞和	(株)両備システムズ
綿口 吉郎	富士通(株)	清水 秀一郎	
坂本 拓也	(株)富士通研究所	piyokango	

著作・制作	独立行政法人情報処理推進機構（IPA）		
編集責任	土屋 正		
イラスト製作	株式会社 創樹		
執筆協力者	10 大脅威選考会		
10 大脅威執筆者	土屋 正	辻 宏郷	黒谷 欣史
	亀山 友彦	渡邉 祥樹	大友 更紗
	吉本 賢樹	宇梶 宏美	田村 智和
	熊谷 悠平	佐々木 敬幸	佐藤 輝夫
	阿部 未歩		
IPA 執筆協力者	瓜生 和久	桑名 利幸	渡辺 貴仁
	松坂 志	加賀谷 伸一郎	

情報セキュリティ 10 大脅威 2020

情報セキュリティ 10 大脅威の活用法

2020 年 3 月 10 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/