講座

情報セキュリティ

2024年4月29日予定

担当：新田

情報セキュリティとは？

情報の**機密性**、**完全性**及び**可用性**を維持すること

ISO/IEC27000 JIS Q27000で定義　出典：https://kikakurui.com/q/Q27000-2019-01.html

特性	意味	例
機密性 confidentiality	• 認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また開示しない特性。 • データが漏洩せず守られていること。	• アクセス権限 • パスワード管理 • データの暗号化
完全性 integrity	• 正確さ及び完全さの特性。 • データの改ざんや削除が発生せず、正確な状態を保つようにすること。	• ハッシュ関数 • バージョン管理 • データのバックアップ
可用性 availability	• 認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。 • 使いたいデータを必要に応じてすぐに使えるようにしておくこと。	• 機器の冗長化 • 負荷分散 • メンテナンス

さらに**真正性**、**責任追跡性**、**否認防止**、**信頼性**などの特性を維持することを含めることもある。

ISO/IEC27000 JIS Q27000で定義

特性	意味	例
真正性 Authenticity	• エンティティは、それが主張するとおりのものであるという特性。 • 通信相手が本人かどうかを確実にすること。	• デジタル署名 • 二段階認証
責任追跡性 Accountability	• あるエンティティの動作がその動作から動作主のエンティティまで一意に追跡できることを確実にする特性。 • インターネット上の一連の動作を追跡し、後になってインシデントが発覚した際に責任を追求できる状態を維持すること。	• 操作ログ • アクセスログ • アクセス制御
否認防止 non-repudiation	• 主張された事象又は処置の発生、及びそれらを引き起こしたエンティティを証明する能力。 • 情報システムの利用や操作、データの送信などに関連して、確かにある特定の人物が行なったことを後から証明できるようにする仕組みや技術。	• デジタル署名 • タイムスタンプ • アクセスログ
信頼性 Reliability	• 意図する行動と結果とが一貫しているという特性。 • 意図した動作が確実に行われることを担保すること。	• システム構築時の設計（例外処理やバリデーション）

情報セキュリティの観点では、**機密性**、**完全性**、**可用性**を**バランスよく**維持する必要がある

- 機密性に偏った対策を行うと、情報アクセスが制限されすぎて可用性が低下することがある。
- 完全性に重点を置きすぎると、過剰な情報管理が求められ、業務効率が低下する可能性がある。
- 可用性を重視して、システム障害による損失を最小限にしようとすると、コストが高くなる可能性がある。

リスクマネジメント

どのような危険（リスク）があるかを把握し、その影響を回避、または最小におさえるための一連のプロセス。

- **リスク特定** → どんなリスクがあるか洗い出す
- **リスク分析** → リスクが発生した場合の影響度や発生確率を明らかにする
- **リスク評価** → リスク分析の結果を可視化し、リスクの優先順位付けを行う
- **リスク対応** → リスク評価で決定した方法に従って対策を講じる

リスクアセスメント

リスク対応

- **リスク回避**
  - リスクを取り除く。（問題を発生させない）
  - リスクの大きいサービスから撤退する。
- **リスク移転（転嫁）**
  - リスクを他社に移す。（保険に加入するなど）
- **リスク低減（軽減）**
  - リスクの発生確率を下げる。
  - リスクの影響を最小化する。
- **リスク受容（保有）**
  - リスクを受け入れる。

情報セキュリティの脅威

情報セキュリティを脅かすもの（リスクを引き起こす要因）

人的脅威

- なりすまし
- 不正アクセス
- クラッキング
- 誤操作
- 紛失
- 情報漏洩

技術的脅威

- マルウェア
- フィッシング詐欺
- ブルートフォース攻撃
- 標的型攻撃
- ランサムウェア
- XSS
- Dos攻撃

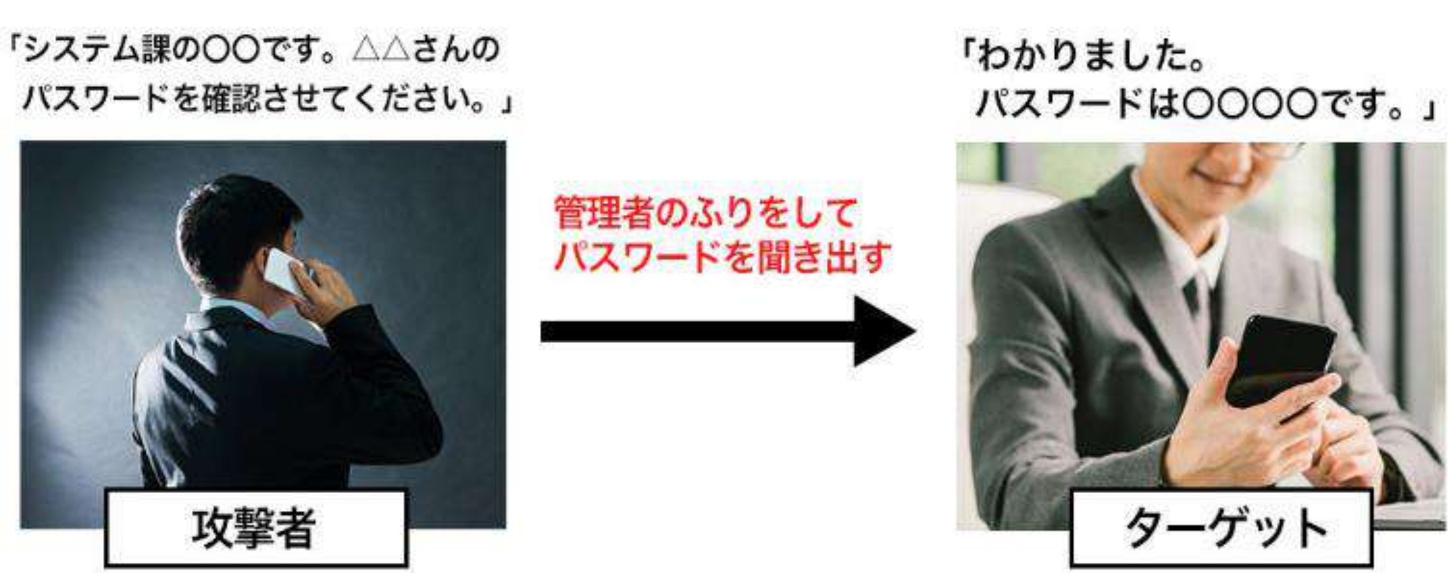
物理的脅威

- 地震
- 洪水
- 火災
- 経年劣化による故障

ソーシャルエンジニアリング

人の心理的な隙や不注意に付け込み、情報を不正に入手する方法

- なりすまして、電話やメールでパスワードを聞き出す
- のぞき見（ショルダーハッキング）
- ゴミ箱をあさる（トラッシング）
- ターゲットから攻撃者に連絡させる（リバースソーシャルエンジニアリング）



引用元
https://www.amiya.co.jp/column/3936/

サイバー攻撃

インターネットやデジタル機器を絡めた手口で、個人や組織を対象に、**金銭の窃取**や
個人情報の詐取、あるいは**システムの機能停止**などを目的として行われる攻撃

◆特定のターゲットを狙った攻撃
・ランサムウェア
・標的型攻撃
・サプライチェーン攻撃
・キーボードロギング
・ドライブバイダウンロード攻撃
・水飲み場攻撃
・スプーフィング攻撃
・ビジネスメール詐欺

◆不特定多数を狙った攻撃
・フィッシング詐欺
・ゼロクリック攻撃
・ジュースジャッキング攻撃
・ドメイン名ハイジャック攻撃
・MITM攻撃

◆脆弱性を狙った攻撃
・SQLインジェクション
・OSコマンド・インジェクション
・クロスサイトスクリプティング
・クロスサイトリクエストフォージェリ
・ゼロデイ攻撃
・ルートキット攻撃
・セッションID固定化攻撃
・フォームジャッキング攻撃
・バッファオーバーフロー攻撃
・ディレクトリ・トラバーサル攻撃
・DNSキャッシュポイズニング

◆サーバーに負荷をかける攻撃
・DoS攻撃
・DDoS攻撃
　・フラッド型攻撃
　・F5アタック
　・ランダムサブドメイン
　・スマーフ攻撃
　・PoD(ping of death)
　・メールボム攻撃

情報セキュリティの脆弱性

コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生したサイバーセキュリティ上の欠陥。

セキュリティホールとも呼ばれる。

脆弱性が残された状態でコンピュータを利用していると、**不正アクセス**に利用されたり、**ウイルスに感染**したりする危険性がある。

出典：総務省　国民のためのサイバーセキュリティサイト
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/intro/intro.html

情報セキュリティ10大脅威　2024

- IPAが2006年から毎年発行している資料
- 前年に発生したセキュリティ事故や攻撃の状況等からIPAが脅威候補を選出
- セキュリティ専門家や企業のシステム担当等から構成される「10大脅威選考会」が投票
- TOP10入りした脅威を「10大脅威」として脅威の概要、被害事例、対策方法等を解説

情報セキュリティ10大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/10threats/10threats2024.html

情報セキュリティ 10 大脅威 2024 ～脅威に呑まれる前に十分なセキュリティ対策を
https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf

情報セキュリティ10大脅威　2024 【個人編】

- インターネット上のサービスからの個人情報の窃取
- インターネット上のサービスへの不正ログイン
- クレジットカード情報の不正利用
- スマホ決済の不正利用
- 偽警告によるインターネット詐欺
- ネット上の誹謗・中傷・デマ
- フィッシングによる個人情報等の詐取
- 不正アプリによるスマートフォン利用者への被害
- メールやSMS等を使った脅迫・詐欺の手口による金銭要求
- ワンクリック請求等の不当請求による金銭被害

情報セキュリティ10大脅威 2024 簡易説明資料[個人編]
https://www.ipa.go.jp/security/10threats/m42obm00000047oa-att/setsumei_2024_kojin.pdf

情報セキュリティ10大脅威　2024 【組織編】

- ランサムウェアによる被害
- サプライチェーンの弱点を悪用した攻撃
- 内部不正による情報漏えい等の被害
- 標的型攻撃による機密情報の窃取
- 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
- 不注意による情報漏えい等の被害
- 脆弱性対策情報の公開に伴う悪用増加
- ビジネスメール詐欺による金銭被害
- テレワーク等のニューノーマルな働き方を狙った攻撃
- 犯罪のビジネス化（アンダーグラウンドサービス）

情報セキュリティ10大脅威 2024 簡易説明資料[組織編]
https://www.ipa.go.jp/security/10threats/m42obm00000044ba-att/setsumei_2024_soshiki.pdf

情報セキュリティ対策の基本

攻撃の糸口	セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し、攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視すべき対策を理解する

日常における情報セキュリティ対策

企業・組織の従業員向け8つの対策を説明した動画シリーズ

出典：華麗なる情報セキュリティ対策 | 情報セキュリティ |IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/videos/kareinaru.html

- パソコンやスマホの**OS**や各種**ソフトウェア**に修正プログラムを適用し、**最新バージョン**に更新する。
- **セキュリティソフト**を導入し、セキュリティソフトの定義ファイルが常に最新の状態か確認する。
- **パスワード**の適切な管理と運用をする。
  - 可能な限り長く複雑に（大小英字・数字・記号を混在させる）
  - 同じパスワードを使いまわさない。
- 不審に思った**メールの添付ファイル**や**URL**を不用意にクリックしない。（送り主の確認、報告）
- 所有者が不明、もしくは自身が管理していない**USBメモリ**などの外部記憶媒体をPCに接続しない（ウイルス感染予防）
- 第三者に見られたり操作されたりしないよう、PCやスマホの画面に**ロック**を設定する。

セキュリティソフトウェアの役割

- ウイルス・マルウェアの検知・駆除
- 悪質なWebサイトをブロック
- 個人情報の漏洩を防止
- パーソナルファイアウォール
- Webアクセスフィルタリング　　　　　　　などなど

Windows標準搭載のWindows Defender、MacOSのGatekeeperやXprotectでも、一定のセキュリティレベルを保つことができる。

有償のセキュリティソフトと比較すると、機能やサポート面が不足しているとの指摘もある。

パスワードの設定

- 初期設定のままにしない。
- 数字、アルファベット、記号など複数の文字種を組み合わせる。推奨は**大文字と小文字のアルファベット、数字、記号を含んだ 10 桁以上。**
  - IDとパスワードを同じ文字列にしない。
  - 生年月日や名前を使わない。
  - 連続した数字やアルファベットにしない。
- パスワードを極力使いまわさない。
- パスワードを他人に教えない。
- パスワードを書いたメモや付箋を近くに置かない。
- 複数人使うPCでは、ブラウザにパスワードを記憶させない。

パスワードの使用率ランキング

出典：Top 200 Most Common Passwords List | NordPass
https://nordpass.com/most-common-passwords-list/

順位	文字列
1	123456
2	admin
3	12345678
4	123456789
5	1234
6	12345
7	password
8	123
9	Aa123456
10	1234567890

順位	文字列
11	1234567
12	123123
13	111111
14	Password
15	12345678910
16	00000
17	admin123
18	1111
19	P@ssw0rd
20	root

- 連続した数字
- 繰り返しの数字
- 文字列の「password」「admin」「root」

などがランクイン

自分の使っている
パスワードの強度
を調べておこう！

多要素認証

複数の要素を組み合わせて、
本人確認を行う。

知的情報

- パスワード
- 暗証番号
- 秘密の質問

所持情報

- 携帯電話（SMS ワンタイムパスワード）
- ICカード

生体情報

- 指紋認証
- 顔認証
- 静脈認証

アカウントの乗っ取りや不正アクセスのリスクを下げる

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

- 安易にリンクやQRコードを開かない。
- 記載された電話番号に電話をかけない。
- 添付ファイルを開かない。
- WordやExcelのマクロにも注意する。
- 有名サービスのメールを騙っていることもあるため、怪しい場合はメール内リンクは使わず、対象のサービスをブラウザで検索して正規のWeb サイトを開いて確認する。

SMSによる誘導（スミッシング）

出典：フィッシング対策協議会
https://www.antiphishing.jp/

◆ **リンクをクリックしてしまうと・・・**

偽サイトに飛ばされ、正規の入力フォームを装った画面で個人情報の入力が求められたり、不審なアプリのインストールが促され、インストールするとマルウェアに感染したりする。

例）AMAZONを騙るフィッシングメール

お支払方法に問題があり、プライム特典をご利用いただけない状況です。

支払方法を更新する

の部分のリンク
http://www.amazon-●●●●.biz/など

Amazon利用いただきありがとうございます。

ご指定いただいたお客様のお支払い方法が承認されないため、。Amazonは無料ですが、ご登録の際には適用可能なお支払い方法を確認させていただきます。これは、ご登録時にご同意いただいたように。

1日以内に、アマゾンからの請求へのお支払いが確認できない限り、お客様のAmazon登録はキャンセルされ
他の有効な支払方法を更新・追加し、Amazonをご利用されたい場合は、以下の手順に従って更新してください。
Webページが乗っ取られないようにするためにご本人認証下記携帯電話でQRコードをスキャンする確認ください

>>>> <<<<

の部分のリンク
https://zjg●●●●/jpなど

1. お客様のお支払い方法にアクセス
2. Amazon登録したAmazon.co.jpのアカウントを使用してサインイン
   登録済みのお支払手段の有効期限を更新、または新しく支払い手段を追加し、「続行」ボタンをクリック現在ご指定のお支払い方法が承認されない原因は、提携会社(クレジットカード会社等)の事情により異なりますが、利用可能限度額の超過、有効期限切れ、カード利用不可などが考えられます。大変お手数ですが詳細についてはサービスの提供元会社に直接お問い合わせください。

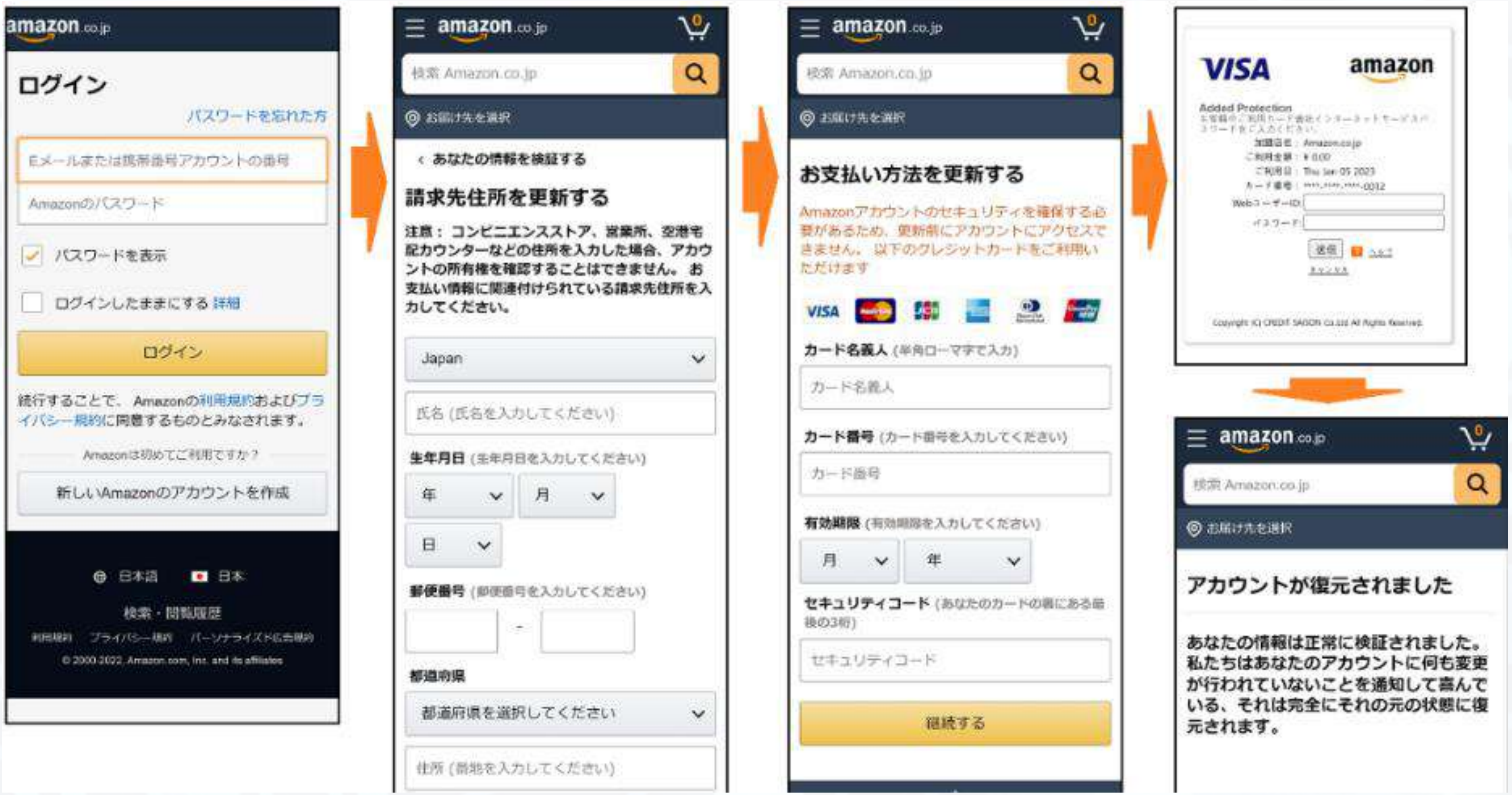
Amazon.co.jpをご利用いただき、ありがとうございます。
今後ともAmazon.co.jpをよろしくお願いいたします。

Amazon.co.jpカスタマーサービス

メール文面の例

出典：フィッシング対策協議会
https://www.antiphishing.jp/

本物のサイトをコピーして作られているため、見た目での判別は困難

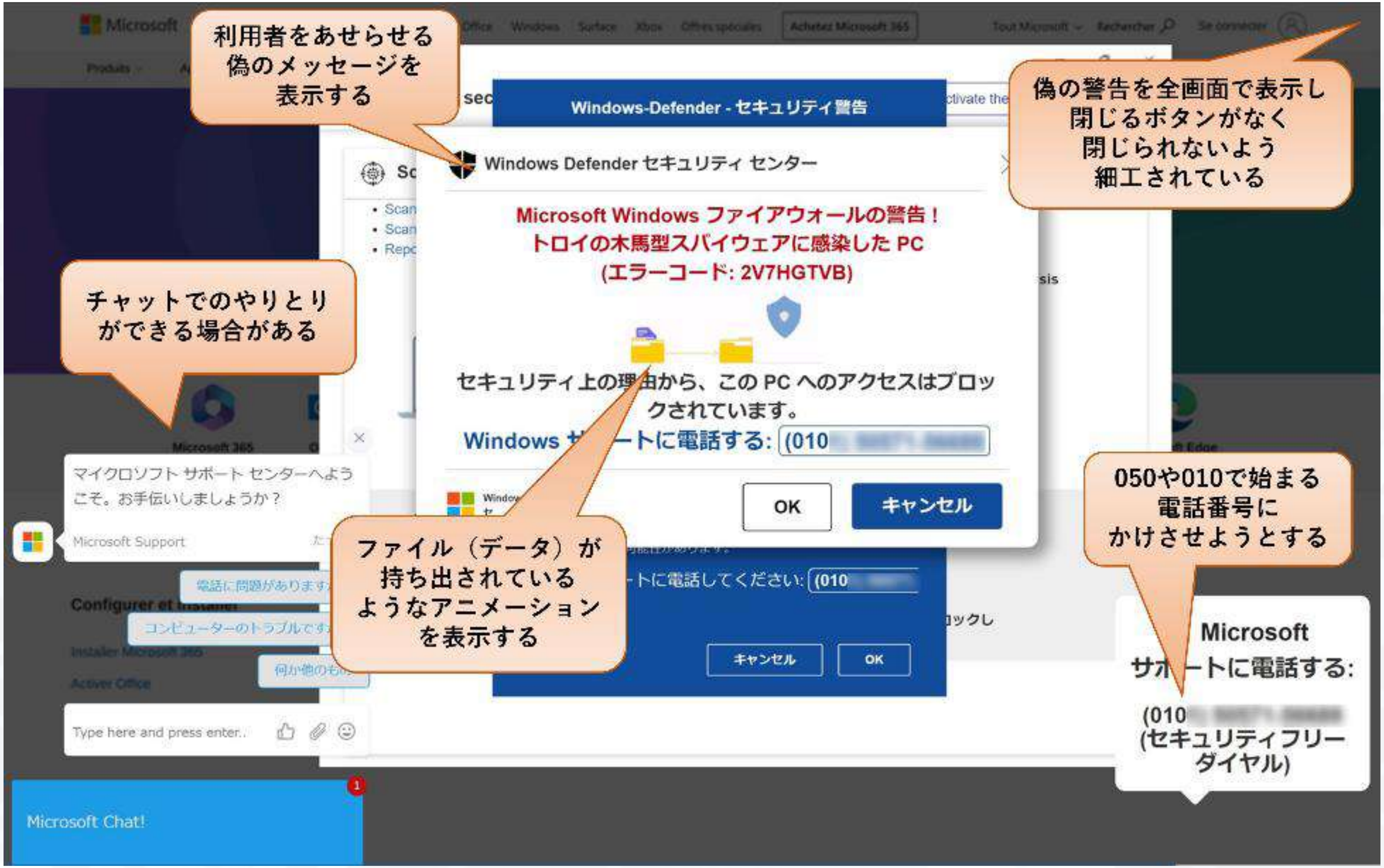


出典：フィッシング対策協議会
https://www.antiphishing.jp/

- 発信元の電話番号を確認する。
- 正規のドメインかどうかチェック（本物のURLと比べる）
- Yahoo!メールやＧmailの場合、正規のメールならブランドアイコンがある

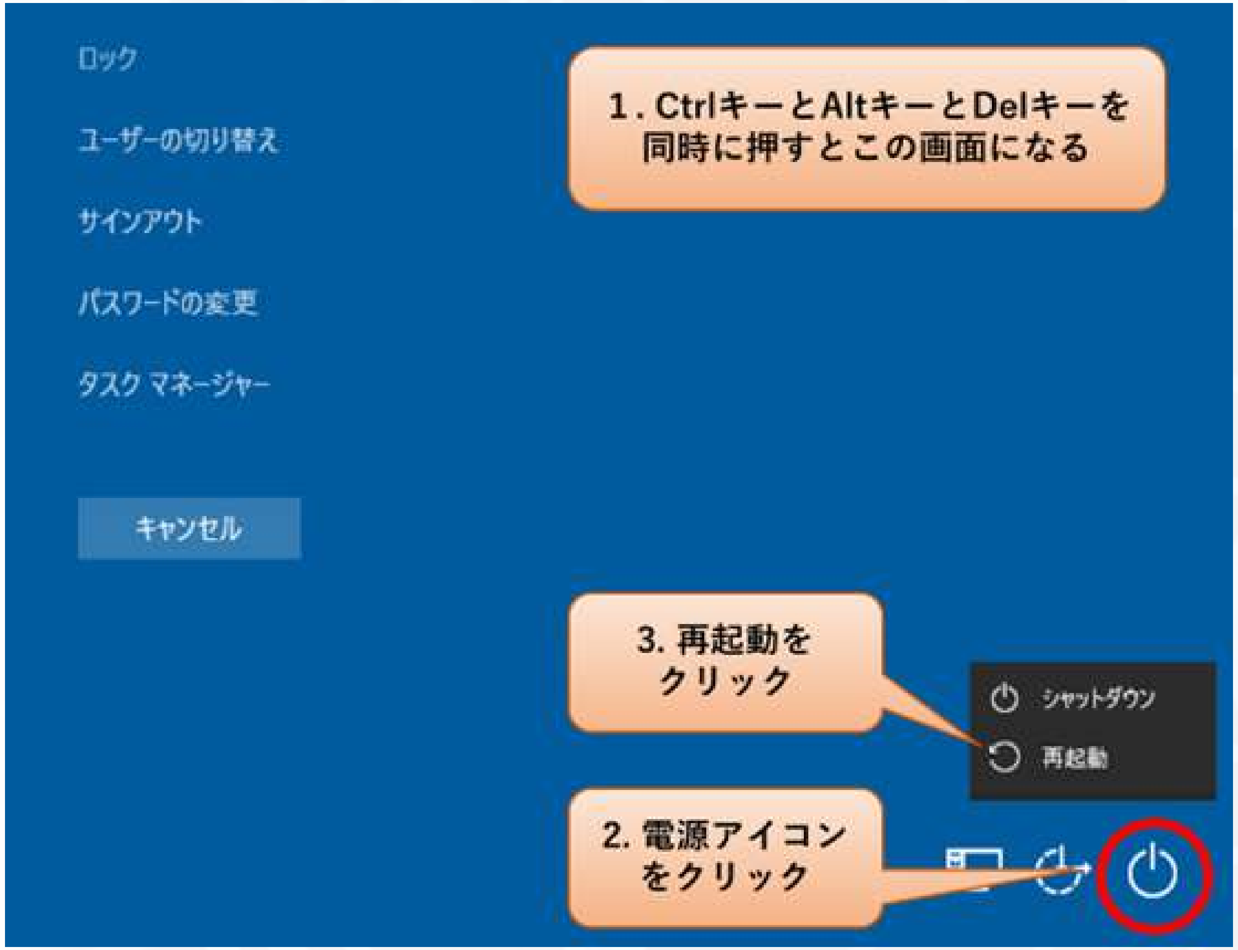
例）サポート詐欺（マイクロソフトセキュリティアラーム）

出典： 一般財団法人日本サイバー犯罪対策センター
https://www.jc3.or.jp/threats/topics/article-396.html



出典：独立行政法人情報処理推進機構セキュリティセンター
https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20231219.html

サポート詐欺画面の対処法

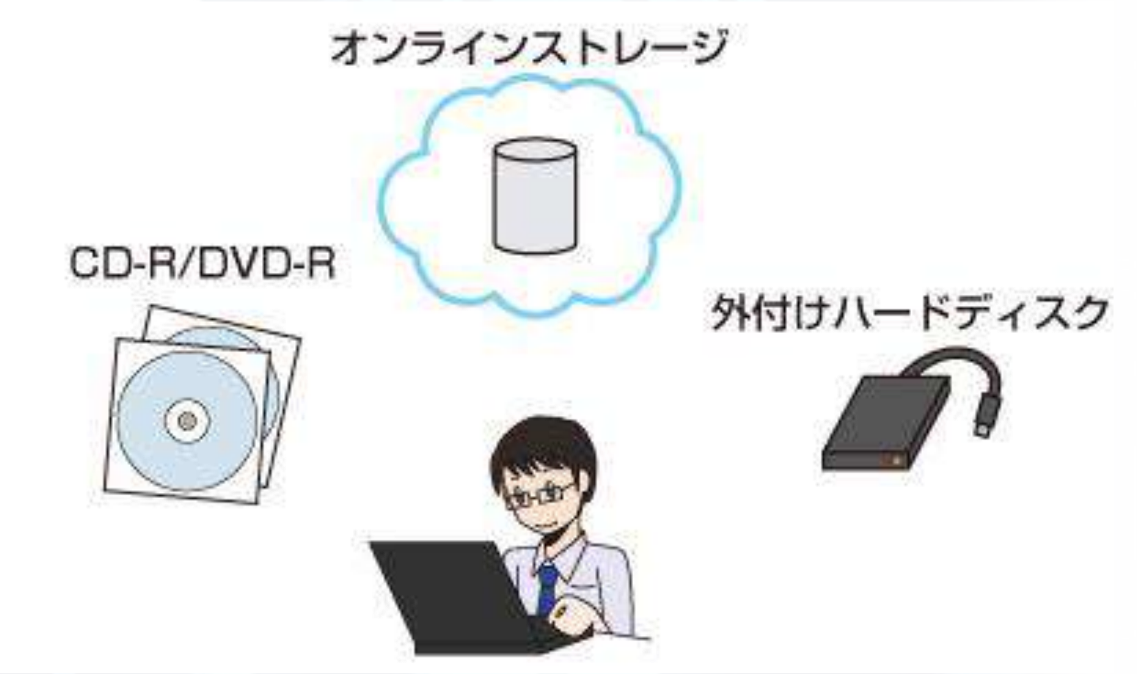


出典：独立行政法人情報処理推進機構セキュリティセンター
https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20231219.html

- 右上の×（閉じる）ボタンで警告画面を消す。
- ESCキーを長押しすると、全画面表示が解除されて、×ボタンが表示される場合もある。
- ×ボタンが表示されない場合は **Ctrl + Alt + Del** を押して、左の画面の電源アイコンから、再起動をクリック。
- 左の画面からタスクマネージャーを開いて、該当のタスクを終了させるのも有効。

バックアップについて

- 安全にパソコンを利用するためには、**定期的なバックアップ**が不可欠。
- ワープロソフトや表計算ソフトなどで作成したドキュメントファイルだけでなく、送信した電子メールや受信した電子メール、よく利用するホームページのURLなどの情報も、バックアップしておく。
- バックアップは「やりっ放し」ではなく、定期的に復元方法を確認する。



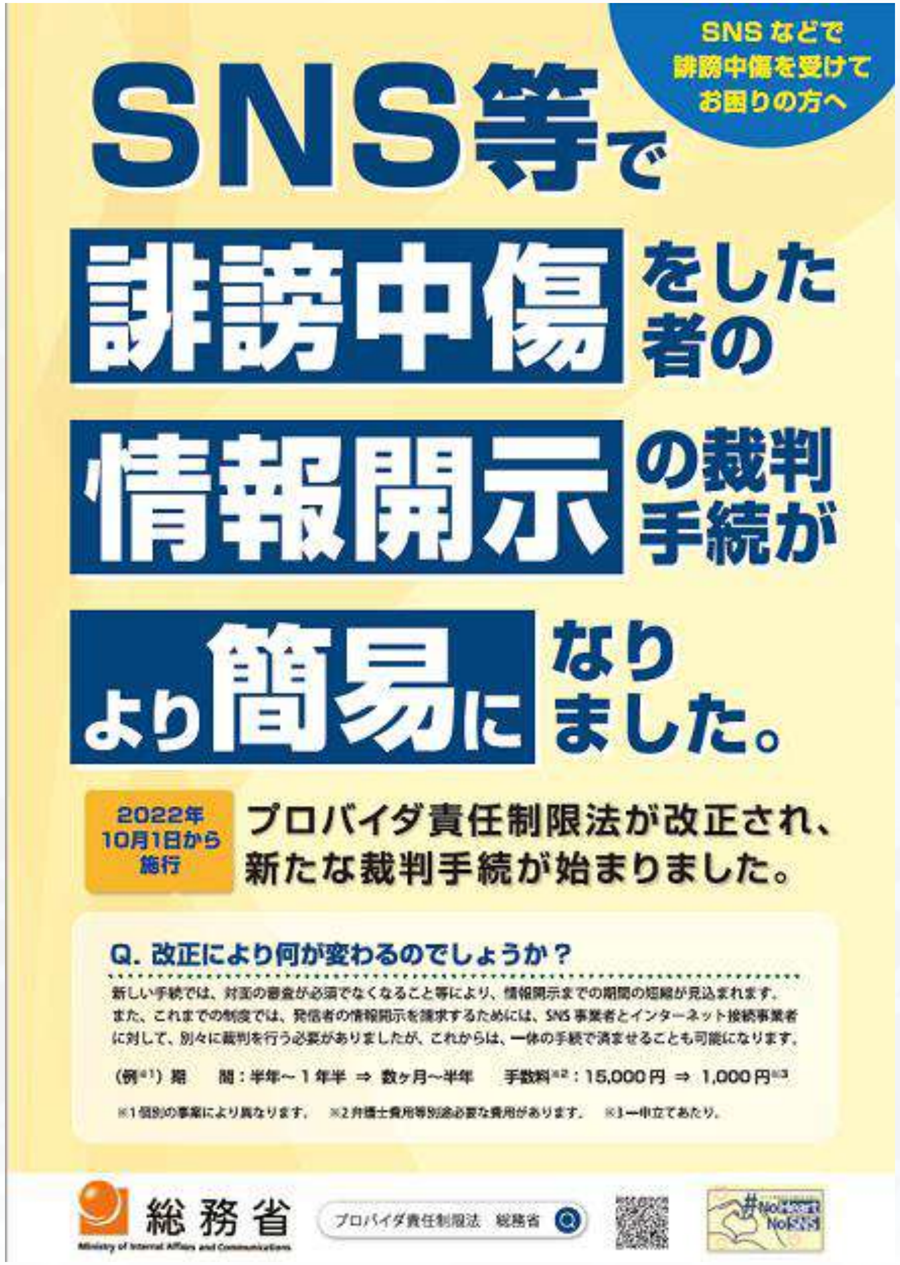
主なバックアップ媒体

出典：国民のためのサイバーセキュリティサイト（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_staff_07.html

情報リテラシー・モラルの向上

◆ SNSの利用

- 悪意の有無に関わらず、誤った情報が広まる恐れがあるため、情報を鵜呑みにしない。
- 情報を安易に拡散しない。（**誹謗・中傷やデマの発信**は**犯罪**になり、**拡散した人**も、その行為を特定され、社会的責任を問われる場合がある。）
- 情報発信は慎重に行う。（真偽を判断できない情報や他人を攻撃するような発言は控える。）



参照：SNSの誹謗中傷～あなたが奪うもの・失うもの～ #NoHeartNoSNS｜政府広報オンライン

https://www.gov-online.go.jp/prg/prg21546.html

◆ 自身が誹謗中傷を受けた場合

- ミュートやブロックなどで、相手を「見えなくする」
- SNS事業者に誹謗中傷の投稿削除を依頼する
- 信頼する人や公的な相談窓口に相談する

・違法・有害情報センター（総務省）	https://ihaho.jp/
・人権相談（法務省）	https://www.jinken.go.jp/
・誹謗中傷ホットライン	https://www.saferinternet.or.jp/bullying/
・まもろうよ こころ（厚労省）	https://www.mhlw.go.jp/mamorouyokokoro/

被害にあった際は、適切な人や機関へ相談

- 迷惑メール相談センター（日本データ通信協会）
  https://www.dekyo.or.jp/soudan/index.html
- フィッシング対策（警視庁）
  https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html
- 都道府県警察本部サイバー犯罪相談窓口
  https://www.npa.go.jp/bureau/cyber/soudan.html
- IPA（安心相談窓口）
  https://www.ipa.go.jp/security/anshin/about.html
- ネットの誹謗中傷（セーファーインターネット協会）
  https://www.saferinternet.or.jp/bullying/

リンク

- 情報セキュリティ　（IPA 独立行政法人情報処理機構）
  https://www.ipa.go.jp/security/index.html

- 国民のためのサイバーセキュリティサイト（総務省）
  https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/enduser/enduser_security01.html

- みんなで使おう サイバーセキュリティ・ポータルサイト
  https://security-portal.nisc.go.jp/

- NICT サイバーセキュリティ研究所
  https://csri.nict.go.jp/