Cyber Security サイバーセキュリティ

日常生活におけるITセキュリティの基礎となる主要な概念とインターネットの安全な使用方法を学ぶことで、データと情報を適切に管理するためのスキルを学ぶことができるモジュールです。

1 セキュリティの概念

カテゴリ		概要	
1.1	データに対する脅威	1.1.1	データと情報の区別を理解する。
		1.1.2	サイバー犯罪、ハッキングなどの用語を理解する。
		1.1.3	個人・サービスプロバイダー・外部組織からの悪意的または偶発的なデータへの脅威を認識する。
		1.1.4	火災・洪水・戦争・地震など、異常事態によるデータへの脅威を認識する。
		1.1.5	クラウドコンピューティングを使用した場合のデータに対する脅威を認識する(データの統制、プライバシーの侵害など)。
1.2	情報の価値	1.2.1	情報セキュリティの基本的な特性である「機密性」「完全性」「可用性」について理解する(Confidentiality・Integrity・Availability)。
		1.2.2	個人情報を保護する理由を理解する(なりすましや詐欺の防止、プライバシーの確保など)。
		1.2.3	コンピュータやデバイス上の職場情報を保護する理由を理解する(盗難・不正使用・偶発的なデータ損失・破壊行為などへの対策)。
		1.2.4	データやプライバシーの保護・保全・管理の一般的な原則を確認する(透明性、合理的な目的、適正さなど)。
		1.2.5	用語「データ主体」および「データ管理者」を理解する。 データやプライバシー保護、保持および管理の原則をどのように適用するかを理解する。
		1.2.6	ICTの使用に関するガイドラインやポリシーを遵守することの重要性と、それらにアクセスする方法を理解する。
1.3	個人情報のセキュリティ	1.3.1	用語「ソーシャルエンジニアリング」を理解する。 コンピュータやデバイスへの不正アクセス・不正な情報収集・詐欺などに関連していることを理解する。
		1.3.2	ソーシャルエンジニアリングの手法を把握する(電話、フィッシング、ショルダーサーフィンなど)。
		1.3.3	用語「なりすまし(identity theft)」とその意味(個人・金融・ビジネス・法律)を理解する。
		1.3.4	なりすましの手口を確認する(インフォメーションダイビング・スキミング・プリテクスティング)。
1.4	ファイルのセキュリティ	1.4.1	マクロのセキュリティ設定を有効／無効にした場合の影響を理解する。
		1.4.2	暗号化の利点とその限界を理解する。暗号化パスワード、キー、証明書を開示したり、紛失したりしないことの重要性を認識する。
		1.4.3	ファイル・フォルダ・ドライブを暗号化する。
		1.4.4	文書・表計算ソフト・圧縮ファイルなどのファイルにパスワードを設定する。

2 マルウエア

カテゴリ		概要	
2.1	種類とその手口	2.1.1	用語「マルウェア」を理解する(トロイの木馬・ルートキット・バックドア)。 マルウェアがコンピュータやデバイスに侵入する際に、さまざまな方法で隠蔽されることを認識する。
		2.1.2	感染性のマルウェアの種類を認識し、ウイルスやワームなどの仕組みを理解する。
		2.1.3	データを盗み、不正に収益を上げようとしたり、正当な収益を流出させようとするマルウェアの種類を認識し、 それらの仕組みを理解する(アドウェア、ランサムウェア、スパイウェア、ボットネット、キーストローク・ロギング、ダイヤラー)。
2.2	保護	2.2.1	ウイルス対策ソフトの仕組みとその限界を理解する。
		2.2.2	パソコンやデバイスにウイルス対策ソフトを導入すべきであることを理解する。
		2.2.3	ウイルス対策ソフト・ウェブブラウザ・プラグイン・アプリケーション・オペレーティングシステムなどのソフトウェアを 定期的に更新することの重要性を理解する。
		2.2.4	ウイルス対策ソフトを使って、特定のドライブ・フォルダー・ファイルをスキャンする。 ウイルス対策ソフトを使って、スキャンをスケジュールする。
		2.2.5	古いソフトウェアやサポートされていないソフトウェアを使うことのリスクを理解する(マルウェアの脅威の増加、非互換性など)。
2.3	対応と削除	2.3.1	用語「検疫(隔離)」を理解する。感染したファイルや不審なファイルを検疫(隔離)することの効果を理解する。
		2.3.2	感染したファイルや不審なファイルを検疫(隔離)・削除する。
		2.3.3	マルウェアの攻撃は、オンラインリソースを使用して診断し、解決することができることを理解する。 (例：オペレーティングシステム・ウイルス対策ソフト・ウェブブラウザソフトのプロバイダーのウェブサイト・ 関係当局のウェブサイトなど。)

3 ネットワークのセキュリティ

カテゴリ		概要	
3.1	ネットワークと接続	3.1.1	用語「ネットワーク」理解する。 ローカルエリアネットワーク(LAN)・ワイヤレスローカルエリアネットワーク(WLAN)・ワイドエリアネットワーク(WAN)・ 仮想プライベートネットワーク(VPN)などの一般的なネットワークの種類を認識する。
		3.1.2	ネットワークへの接続が、セキュリティにどのような影響を与えるかを理解する。 (マルウェア・不正なデータアクセス・プライバシーの保護など)
		3.1.3	ネットワーク管理者の役割を理解する(アカウントの認証／権限の付与／管理・関連するセキュリティパッチや アップデートの監視とインストール・ネットワークトラフィックの監視・ネットワーク内で発見されたマルウェアへの対処など)。
		3.1.4	個人や職場環境におけるファイアウォールの機能とその限界を理解する。
		3.1.5	パーソナルファイアウォールを有効化する・無効化する。 パーソナルファイアウォールによるアプリケーション・サービス・機能のアクセスを許可、ブロックする。
3.2	無線ネットワークのセキュリティー	3.2.1	ワイヤレスセキュリティのさまざまなオプションとその限界を認識する。 WEP(Wired Equivalent Privacy)・WPA(Wi-Fi Protected Access)・WPA2(Wi-Fi Protected Access 2)・ MAC(Media Access Control)フィルタリング・SSID(Service Set Identifier)ステルス。
		3.2.2	保護されていないワイヤレスネットワークを使用していると、攻撃を受ける可能性があることを理解する。 (盗聴・ネットワークの乗っ取り・中間者攻撃)
		3.2.3	用語「パーソナルホットスポット」を理解する。
		3.2.4	安全なパーソナルホットスポットの有効化・無効化、デバイスの接続・切断を安全に行うことができます。

4 アクセスの制御

カテゴリ		概要	
4.1	手法	4.1.1	データへの不正アクセスを防止するための手段を把握する(ユーザー名・パスワード・PIN・暗号化・多要素認証など)。
		4.1.2	用語「ワンタイムパスワード」を理解する。その典型的な使用方法を理解する。
		4.1.3	ネットワークアカウントの目的を理解する。
		4.1.4	ネットワークアカウントは、ユーザー名とパスワードでアクセスし、利用しないときはロックまたはログオフすることを理解する。
		4.1.5	アクセスコントロールに使用する一般的な生体認証技術を識別する(指紋・網膜／光彩スキャン・顔認識・手形など)。
4.2	パスワードの管理	4.2.1	優れたパスワードの考え方を認識する。 (適切な長さのパスワード・適切な文字／数字／特殊文字の組み合わせること・パスワードを共有しないこと・ 定期的にパスワードを変更すること、サービスごとに異なるパスワードをつかうこと、など)
		4.2.2	パスワード管理ソフトの機能とその限界を理解する。

5 Webサービスの安全な使用

カテゴリ		概要	
5.1	ブラウザの設定	5.1.1	フォーム入力時のオートコンプリート・自動保存の有効化や無効化を設定する。
		5.1.2	ブラウザからプライベートなデータを削除する。 (閲覧履歴・ダウンロード履歴・キャッシュされたインターネットファイル・パスワード・クッキー・オートコンプリートデータなど)
5.2	安全なブラウジング	5.2.1	特定のオンラインでの活動(買い物、ネット銀行)は、安全なネットワーク接続を使用して、 安全なWebページでのみ行う必要があることを知る。
		5.2.2	ウェブサイトの信頼性を確認する方法を識別する。 (コンテンツの品質、通貨、有効なURL、企業や所有者の情報、連絡先、セキュリティ証明書、ドメイン所有者の確認など)
		5.2.3	用語「ファーミング」を理解する。
		5.2.4	コンテンツコントロールソフトウェアの機能・種類を理解する。 (インターネットフィルタリングソフト、ペアレンタルコントロール<保護者向け機能>ソフトなど)

6 コミュニケーション

カテゴリ		概要	
6.1	電子メール	6.1.1	電子メールの暗号化と復号化の目的を理解する。
		6.1.2	用語「デジタル署名」を理解する。
		6.1.3	詐欺メール・迷惑メールの可能性を識別する。
		6.1.4	フィッシングに共通する特徴を識別する。 (実在する組織や人物の名前を使用している・偽のウェブリンク、ロゴ、ブランドを使用している・個人情報の開示を促しているなど)
		6.1.5	フィッシングの疑いがある場合は、関連団体や関係当局に通報することができることを認識する。
		6.1.6	マクロや実行ファイルを含むメールの添付ファイルを開くと、コンピュータやデバイスがマルウェアに感染する 危険性があることを認識する。
6.2	ソーシャルネットワーク(SNS)	6.2.1	SNSで機密情報や個人を特定できる情報を公開しないことの重要性を理解する。
		6.2.2	アカウントのプライバシーや位置情報など、ソーシャルネットワークのアカウントを適切に設定し、定期的に見直す必要性を認識する。
		6.2.3	SNSのアカウント設定をする(アカウントのプライバシー・位置情報)。
		6.2.4	ソーシャルネットワーキングサイトを使用する際に起こりうる危険について理解する。 (いじめ・グルーミング・個人情報の悪意ある開示・身分や経歴の詐称・詐欺的または悪意あるリンク、コンテンツ、メッセージなど)
		6.2.5	ソーシャルネットワークの不適切な使用や行動を、サービスプロバイダーや関係当局に報告できることを認識する。
6.3	VoIPとIM	6.3.1	インスタントメッセージ【IM】やボイスオーバーIP【VoIP】のセキュリティ上の脆弱性について理解する。 (マルウェア・バックドア・ファイルへのアクセス・盗聴など)
		6.3.2	IMやVoIPを使う上で、機密性を確保する方法を認識する(暗号化・重要情報の非開示・ファイル共有の制限など)。
6.4	モバイル	6.4.1	非公式のアプリケーションストアのアプリケーションを使用する場合に起こりうる影響を理解する。 (モバイルマルウェア・不必要なリソースの使用・個人データへのアクセス・品質の低さ・隠れたコストなど)
		6.4.2	用語「アプリケーションパーミッション【アプリの権限】」理解する。
		6.4.3	モバイルアプリケーションは、モバイルデバイスから個人情報を抽出できることを認識する(連絡先・位置情報・画像など)。
		6.4.4	デバイスを紛失した場合の緊急措置や予防措置を認識する。 (遠隔操作による無効化・遠隔操作による消去・デバイスの所在確認など)

7 安全な削除と破棄／廃棄

カテゴリ		概要	
7.1	安全性の確保とバックアップデータ	7.1.1	コンピュータやデバイスの物理的なセキュリティを確保する方法を認識する。 (放置しない・機器の場所や詳細を記録する・ケーブルロックを使用する・アクセス制御を行うなど)
		7.1.2	コンピュータやデバイスのデータが失われた場合に備えて、バックアップの手順を確保することの重要性を認識する。
		7.1.3	バックアップ手順の特徴を識別することができる(規則性／頻度・スケジュール・保存場所・データ圧縮)。
		7.1.4	データをバックアップする(ローカルドライブ・外付けドライブ／メディア・クラウドサービスなど)。
		7.1.5	バックアップ先からデータを復元する(ローカルドライブ・外付けドライブ／メディア・クラウドサービスなど)。
7.2	安全性を確保した削除と廃棄	7.2.1	データを単に削除することと、永久に削除することを区別する。
		7.2.2	ドライブやデバイスからデータを永久に削除する理由を理解する。
		7.2.3	コンテンツの削除は、サービス上、永続的ではない場合があることを認識する。 (ソーシャルネットワーク・サイト・ブログ・インターネットフォーラム・クラウドサービス)
		7.2.4	データを永久に削除する一般的な方法を確認する。 (シュレッダー・ドライブまたはメディアの物理的破壊・デガウス<消磁>、データ破壊ユーティリティ)