単元
07

情報セキュリティ全般

物理的脅威／その他の脅威

・一般的な物理的脅威の種類と特徴について理解する
・クラッキングについて理解する
・その他の脅威の種類と特徴について理解する

一般的な物理的脅威

1）**災害**

自然災害（地震，洪水など）や人的災害（火災など）によって，機器や建物が使えなくなったり，機器自体がなくなってしまったりすること

2）**事故／故障**

偶発的な事故や故障などによって，機器や建物が使えなくなること

3）**破壊**

悪意のある第三者による妨害行為，破壊行為などによって，機器や建物が壊れて使えなくなること

4）**盗難**

情報が保存されているPCやUSBメモリなどが盗まれること（人的脅威にも該当するが，機器が物理的に無くなることから物理的脅威に分類されることもある）

5）**不正侵入**

機器が設置された建物や室に，権限のない者が侵入すること（破壊や盗難などが起きる危険性がある）

クラッキング

悪意をもって他人のPCやシステムなどに侵入（不正アクセス）して，データを盗み見たり，破壊したりする行為

・バックドア

クラッキングを行ったクラッカーが，次回以降の侵入に利用するために設置する経路（裏口）のこと（攻撃者が秘密裏に作成した利用者アカウントなども含む）

・エシカルハッカー（ホワイトハッカー）

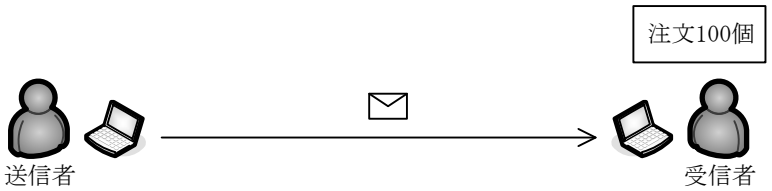
クラッキング（悪意のハッキング）を行うクラッカーに対して，セキュリティ上の問題点がないかを検証する目的などで善意のハッキングを行う人の総称

その他の脅威

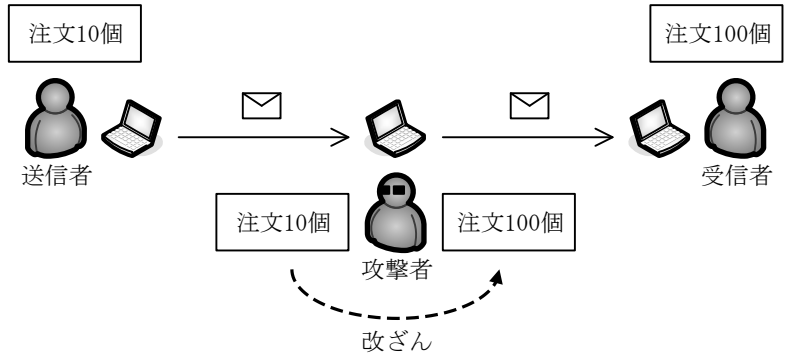
1）**中間者攻撃**（Man-in-the-middle）

通信している２者間に攻撃者が入り込み，送信者及び受信者の両方になりすましながら，通信内容の盗聴・改ざんなどを行う攻撃

① 送信者から「注文 100 個」というメールが届いたように見えるが･･･



② 実際には，攻撃者が「注文 10 個」というメールを改ざんしている



・**MITB 攻撃**（Man-in-the-browser）

マルウェアなどによって利用者の Web ブラウザに侵入し，Web ブラウザと Web サーバ間の通信内容の盗聴・改ざんなどを行う攻撃（中間者攻撃の一種であり，正規の Web サイトを利用しているように見せかけたまま，入力内容の盗聴や送信内容の改ざんが行われるため，利用者が被害に気付きにくいという特徴がある）

2）**ゼロデイ攻撃**

ベンダー企業からソフトウェアの脆弱(ぜいじゃく)性の修正プログラムが提供される前に，その脆弱性を悪用して行われる攻撃

3）**サイドチャネル攻撃**

動作中の IC チップの消費電力，放射電磁波などの副次的情報（サイドチャネル情報）を測定・解析して，機密情報を入手する攻撃

4）**危殆化**

コンピュータ技術が向上することで安全性が低下すること

AI に対する脅威

AI は業務の効率化や高度な判断を可能にする一方で，その特性を悪用した新たな脅威も生じている（標的型攻撃・フィッシング・なりすましの巧妙化，マルウェアの生成，攻撃者によるシステムの脆弱性発見の効率化 など）

1）**ディープフェイク**

AI 技術を利用して作成される，非常に精巧な偽の画像，映像，音声のこと

人物の顔や声などを置き換えることで，実在しない出来事や発言をまるで本物であるかのように見せることができるため，誤情報の拡散や詐欺，プライバシー侵害など，様々な悪用のリスクが問題視されている

2）**敵対的サンプル**（Adversarial Examples）

AI に誤った判断（誤分類）を引き起こさせるように，人間にはほとんど違いが分からない微小なノイズや加工を意図的に加えた画像や音声などの入力データのこと（AI を利用したシステムが誤作動を起こすことで，不正アクセスや物理的な被害につながるおそれがあるほか，システムの信頼性が損なわれるといった影響を及ぼす）

3）**プロンプトインジェクション**

AI モデルやチャットボットに対して，誤った動作や情報提供が起きるようなプロンプト（動作指示）を与えることで，システムの制御を奪ったり，本来出力が禁止されている情報（機密情報や犯罪行為に利用される情報など）を引き出したりする攻撃（AI が外部からの入力に基づいてコンテンツを生成する“生成 AI”の普及に伴って急増している技術的脅威の一つ）

関連知識

情報セキュリティインシデント

事業運営を危うくする確率及び情報セキュリティを脅かす確率が高い，望まない又は予期しない単独もしくは一連の情報セキュリティ事象

ラテラルムーブメント

攻撃者が侵入に成功したシステムを足掛かりとして，同一ネットワーク内の他の端末やサーバへと（水平方向に）次々に侵入範囲を拡大する行為

攻撃者は，権限昇格や認証情報の窃取などを行いながら，重要な情報資産や目的のシステムへの到達を狙う（内部ネットワークで長期間にわたって，正規の利用者として振る舞いながら侵入を進めていくため検知が困難という特徴がある）

単元07 科目A問題演習

問1 攻撃者がコンピュータに不正侵入したとき，再侵入を容易にするためにプログラムや設定の変更を行うことがある。この手口を表す用語として，最も適切なものはどれか。

ア　盗聴　　イ　バックドア
ウ　フィッシング　　エ　ポートスキャン

問2 ゼロデイ攻撃の説明として，適切なものはどれか。

ア　TCP/IP のプロトコルのポート番号を順番に変えながらサーバにアクセスし，侵入口と成り得る脆弱(ぜい)なポートがないかどうかを調べる攻撃
イ　システムの管理者や利用者などから，巧妙な話術や盗み見などによって，パスワードなどのセキュリティ上重要な情報を入手して，利用者になりすましてシステムに侵入する攻撃
ウ　ソフトウェアに脆弱性が存在することが判明したとき，そのソフトウェアの修正プログラムがベンダーから提供される前に，判明した脆弱性を利用して行われる攻撃
エ　パスワードの割り出しや暗号の解読を行うために，辞書にある単語を大文字と小文字を混在させたり数字を加えたりすることで，生成した文字列を手当たり次第に試みる攻撃

問3 ディープフェイクを悪用した攻撃に該当するものはどれか。

ア　AI 技術によって加工した CEO の音声を使用して従業員に電話をかけ，指定した銀行口座に送金するよう指示した。
イ　企業の PC をランサムウェアに感染させ，暗号化したデータを復号するための鍵と引き換えに，指定した方法で暗号資産を送付するよう指示した。
ウ　企業の秘密情報を含むデータを不正に取得したと誤認させる電子メールを従業員に送付し，不正に取得したデータを公開しないことと引き換えに，指定した方法で暗号資産を送付するよう指示した。
エ　ディープウェブにて入手した認証情報で CEO の電子メールアカウントに不正にログインして偽りの電子メールを従業員に送付し，指定した銀行口座に送金するよう指示した。

解説・解答　8ページ