サイバー攻撃

○IoT[1]機器へのサイバー攻撃

インターネットに接続された情報家電などに対するサイバー攻撃である. 今後, 増加すると予測されている一方で, その情報セキュリティ対策が, パソコンなどに比べて, おろそかになっている.

(例)

- パスワードが, 工場出荷時の初期設定のままで変更されていないため, IoT 機器に不正アクセスされる.
- アップデートが行われていないため, 脆弱性[2](セキュリティホール)を突かれて, IoT 機器に不正アクセスされる.
- 廃棄・譲渡する前に初期化しないため, IoT 機器内の設定や重要情報を悪用される.

◆ボット[3]

感染した情報機器[4]を, インターネット経由で外部から操ることを目的とした不正プログラムである. ボットに感染した場合, 攻撃者であるボットハーダーが, C&C サーバ経由で, ボットネット内のボットに対して指令を出し, 遠隔操作されたボットが, 様々な攻撃を行う.

関連する用語は, 次のとおりである.

ゾンビ	ボットに感染し, 遠隔操作されるコンピュータ. ホラー映画のゾンビ(死体のままよみがえった人間)にたとえている.
ボットハーダー	ボットネット内の数多くのボットに攻撃を指令する攻撃者. 語源は, bot(ボット)＋herder(牛飼い・羊飼い)から. ボットを家畜に例えている.
C&C サーバ	ボットハーダーが, ボットに命令を送り, 遠隔操作するためのサーバ. Command and control server の略.
ボットネット	ボットに感染した, 複数のコンピュータで構成されたネットワーク.

◆DDoS 攻撃[5]

複数台の情報機器から何度も連続してサーバに通信を行い, サーバをパンク状態にしてサービスを停止させる攻撃である.

- DoS 攻撃は, 攻撃側が 1 台が, 相手側 1 台に対して攻撃する. つまり, 攻撃側と相手側は, 1 対 1 の関係.
- DDoS 攻撃は, 攻撃側複数台が, 相手側 1 台に対して攻撃する. つまり, 攻撃側と相手側は, 多対 1 の関係.
- ボットに感染した IoT 機器は, 踏み台[6]として利用され, 大規模な DDoS 攻撃を行うことがある.

---

1 Internet of Things (モノのインターネット)の略. インターネット経由で様々なモノをつなげること.
2 脅威(攻撃)がつけ込める弱点
3 語源は, 動作がロボットに似ていることから.
4 ここでは, IoT 機器だけでなく, パソコン・スマートフォン・タブレットなどを含む.
5 語源は, Distributed Denial Of Service (分散型サービス妨害) から.
6 サイバー攻撃の攻撃者は, 自身が犯人であることを隠すために, 証拠を残さないようにする第三者を経由した攻撃を仕掛ける. 踏み台とは, 中継点となる第三者のこと.

○IoT 機器へのサイバー攻撃の対策

被害に合わないための対策は, 次の通りである.

●ネットワークの接続前に
- 初期設定のパスワードから安全なパスワードンに変更する
- 使わない機能を無効化する
- 自動アップデート機能などのセキュリティ機能を有効化する

●ネットワーク接続後に
- ソフトウェアのアップデートを行う
- 定期的にアップデートを行う
- 使用しないときは電源をオフにする

●IoT 機器を廃棄するとき
- 設定を初期化する
- 初期化機能がない場合は, 物理的に破壊する

IoT 機器へのサーバー攻撃の対策は, 次のとおりである.

◆耐タンパ性[7]

IC カードなどの, 中身の細工・改ざん・偽造に対する耐性である. 例えば, 耐タンパ性のある IC カードでは, IC カード内にある IC チップに触ると, 記憶内容が破壊されて, 外部から盗み見されることを防ぐ技術が使われている.

◆セキュアエレメント[8]

外部からの解析攻撃に耐えるセキュリティ能力を持つ半導体製品の総称である. 非接触型のクレジットカード・一部のスマートフォンなどに搭載されている.

◆TPM[9]

セキュリティチップともいい, パソコンに内蔵された, 耐タンパ性がある半導体である. TPM が内蔵されたパソコン内の, 暗号化されたハードディスクが万一, 盗難にあっても, 他のパソコンでは, データの読出しが困難なため, 不正な持ち出しの対策となる. また, 暗号や認証のために用いる, 次の機能が搭載されている.

- RSA[10]による暗号化と復号, 公開鍵・秘密鍵の生成
- ハッシュ関数による計算
- ディジタル署名の生成・検証

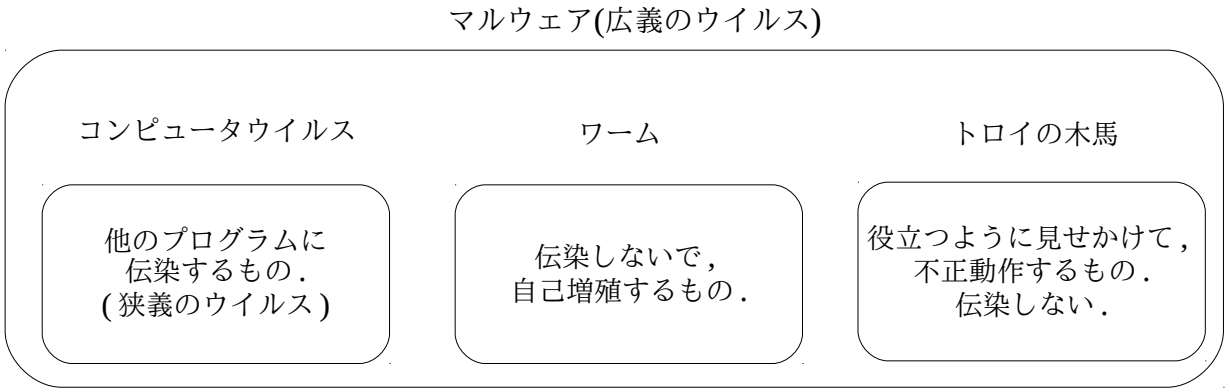
◆ファジング[11]

組み込み機器[12]やソフトウェアから, バグ(欠陥)・未知の脆弱性を検出するためのセキュリティテストである. 問題を引き起こしそうな細工を施したデータを検査対象に送り, 異常な動作の有無により検査する.

---

7 語源は, tamper(改ざんする)＋resistant(耐える・抵抗力のある)から.
8 語源は, Secure(安全な)＋Element(素子)から.
9 Trusted Platform Module の略
10 公開鍵暗号方式の代表格の暗号技術
11 語源は, fuzz(問題を引き起こしそうなデータ)を大量に送りつけることから.
12 用途が限定された情報機器. パソコンのような様々な用途に使う情報機器とは異なり, 家電・自動車・機械などのように, ある用途に特化した情報機器.

○マルウェア[13]
利用者の意図しない動作をするソフトウェアの総称である. IPA では, ウイルスを広義と狭義で 2 つに分類している.
このうち, 広義のウイルスをマルウェアと呼んでいる.
マルウェアに含まれる主なものには, 他のプログラムに伝染するコンピュータウイルス・伝染せずに自己増殖するワーム・役立つように見せかけて不正動作するトロイの木馬などがある. マルウェアの主な分類は, 次のとおりである.



◆コンピュータウイルス[14]
伝染するマルウェアのことである. 他のプログ r 舞うの一部を書き換えて, 自分自身をコピーし, そのプログラム実行時にさらに自分自身を別のプログラムにコピーして増殖していく.

◆ワーム[15]
自己増殖するマルウェアのことである. コンピュータウイルスとは違い, ワーム自身が独立して実行可能なプログラムのため, 別のプログラムを使わず自身を増殖させられる. インターネットを通じて, コンピュータの脆弱性(セキュリティホール)を悪用して侵入するケースが多い.

13 語源は, mal(悪質な)＋ware(software：ソフトウェア)から.
14 語源は, 動植物に感染するウイルスが増殖するプロセスとよく似ていることから. つまり, 自己増殖できる細菌・カビとは異なり, ウイルスは自分だけでは増殖できず, 正常な細胞(プログラム)に規制したへんしつさせて, 増殖していく.
15 語源は, worm はイモムシやミミズのように「這い回る虫」の意味で, ネットワークに接続された他の情報機器に出現するため, ネットワーク内を自分自身で動き回り感染拡大する姿にたとえている.

◆トロイの木馬[16]
役立つように見せかけて, 不正動作するプログラムである. ただし, ウイルスとは異なり, 他へ伝染しない. トロイの木馬には, 潜入したすぐに破壊活動を開始するもの, 潜伏し時間が経ってから発症するもの, 他のコンピュータが乗っ取るための窓口として機能するものなどがある.

トロイの木馬の主な種類は, 次のとおりである.

●ダウンローダ[17]
攻撃するためのプログラムを外部からダウンロードするマルウェアである. 感染後に, 院 t なーネットから不正プログラムをダウンロードして, それを実行することで攻撃する. ダウンローダ自体は, ウイルス対策ソフトのパターンマッチング法では発見されにくい.

●ドロッパ[18]
攻撃するためのプログラムを内部に隠し持つマルウェアである. 感染後に, 内部になる不正プログラムを取り出して, それを実行することで攻撃する.

●バックドア[19]
一度, 不正アクセスできたコンピュータに対し, 再び侵入するために, 仕掛ける裏口のことである. 攻撃者が特殊な裏口を作るため, 発見が難しい.

16 ギリシア神話で, トロイ戦争の際, 兵隊らが身を潜めた木馬(木製の大きな馬の張り子)を, 敵が勘違いしてトロイ城内に連れ込んだ結果, 兵隊らは, 敵を陣地内で攻撃したため勝ったという伝説がある. 転じて「相手をだます」罠の意味になった.
17 語源は, downloader(ダウンロードするもの)から.
18 語源は, dropper(感染後に不正プログラムを投下するもの)から.
19 語源は, back door(裏口)から.

○マルウェアへの対策

◆ウイルス対策ソフト

マルウェアを検出・削除し, コンピュータにマルウェアが感染することを防ぐための製品である. ワクチンソフトと同義語である. 代表的なウイルス検出方法として, パターンマッチング法とビヘイビア法がある.

●パターンマッチング法

あらかじめウイルスの特徴(シグネチャコード[20]) を定義したウイルス定義ファイルを用意し, それに合致するかどうかでウイルスの有無を調べる方法である. ただし, ウイルス定義ファイルに定義されていない未知のウイルスは, 検出できない.

●ビヘイビア法[21]

パターンマッチング法を補うための方法で, プログラムが行う危険な行動(振る舞い)を検出した時点で, ウイルス対策ソフトは, ウイルスに感染したと判断できる. 動的解析の一種である. 例えば, ファイルの書き込み・コピー・削除, 通信量の異常増加を危険な行動とみなす. 検査対象はメモリ上の仮想環境で実行し, 挙動を監視する.

◆サンドボックス[22]

マルウェアかどうかを識別するために, 影響が他へ及ばないように隔離した領域内で, 対象のプログラムを動作させることである. サンドボックス内では, 実行可能な機能・ファイル操作・インターネと接続などが制限される.

例えば, 受信メールの添付ファイル・Web サイトからダウンロードしたファイルを, サンドボックス上で事前に検査し, マルウェアと判断すれば, 受信不可能にする.

◆URL フィルタリング

閲覧できる Web サイトを制限するために, 指定した URL を許可・拒否する機能である. ブラックリストとホワイトリストという 2 つの方式があり, 組み合わせて設定する.

- ブラックリストは, 通過を禁止する対象をまとめた一覧. 多数ある Web サイトの中から, 禁止すべき Web サイトをすべて特定するのは, 困難なため, 漏れ・抜けがありうる.
- ホワイトリストは, 通過を許可する対象をまとめた一覧. それ以外の Web サイトを閲覧できないため, 業務に支障をきたす可能性がある.

URL フィルタリングにより, 有害・不適切な Web サイトへの閲覧・不正なファイルのダウンロードを防ぐ.

◆コンテンツフィルタリング

Web サイトの内容を監視し, あらかじめ設定された条件に合致した Web サイトを排除・遮断する機能である. Web サイト内に含まれる, 業務とは無関係の語句を, 遮断する条件に設定する.

コンテンツフィルタリングにより, 有害な Web サイトの閲覧・不正なファイルのダウンロードを防ぐ.

---

20 マルウェアであると識別できる, プログラムコード中の特徴のある一部分. 英語で, signature code.
21 語源は, behavior(振る舞い)から.
22 語源は, 保護された領域を, 公園の砂場(サンドボックス)に例えたことから.

◆プロキシサーバ[23]
社内ネットワークとインターネットからの接続を代理する機器である. 特徴は次のとおりである.

- プロキシサーバに搭載された URL フィルタリングにより, 閲覧できる Web サイトを制限する
- プロキシサーバ上でキャッシュに保存されたファイルのマルウェアを検出する
- プロキシサーバに搭載された端末認証機能により, シャドー IT[24]によるマルウェア感染を防ぐ

◆VDI[25]
通常は, 情報機器が行う処理を, サーバ上の仮想環境上で行い, 情報機器にはその画面だけを転送する方式である. アプリケーション・データなどはすべてサーバ上にあり, 利用者の情報機器にはないことによるメリットは, 次のとおりである.

- 情報機器の管理を, 個人任せにせず, サーバ側で統括して行える. そのため, 最新のウイルス定義ファイル・セキュリティパッチ[26]を速やかに適用でき, 抜け・漏れを防げる

- 情報機器にはデータが入っていないため, 紛失・盗難が合っても情報漏えいを防げる

VDI は, 仮想環境上で処理を行い, 画面を転送する. 一方で, シンクライアント[27]は, 実機上で処理を行う点が異なる.

23 語源は, proxy(代理)＋server(サーバ)から.
24 個人所有(私物)の情報機器を, 許可なく業務に利用すること. 語源は, shadow(影の)＋IT から.
25 Virtual Desktop Infrastructure(仮想デスクトップ基盤) .
26 OS・ソフトウェアの脆弱性を修正するためのファイル. 語源は, つぎはぎ用のあて布(patch)から. 修正プログラムともいう.
27 Thin Client. 最小限の機能のみ実装したクライアントで, データとアプリケーションを持たないので, インストール作業の軽減につながる. 対となるのはリッチクライアント.

○標的型攻撃

特定の組織[28]に狙いを定めて行うサイバー攻撃の総称である. 不特定を対象としたマルウェアとは対象的に, 攻撃対象の脆弱性[29]を事前に調べたうえで, その脆弱性を突く攻撃を仕掛けて, 秘密情報を奪い取る. 特徴は次のとおりである.

- 攻撃対象のために作られた, 新種や亜種[30]のマルウェアを使うため, ウイルス対策ソフトでは検知されにくい.
- 攻撃対象が少数のため, 発見が遅く, ウイルス対策ソフトのウイルス定義ファイルの対応が遅くなる.

◆標的型攻撃メール

標的となる組織に存在するメールアドレスに送りつけるメールである. 内容を変えて, 長期間にわたって繰り返し送り続ける. メール受信者に不信感を抱かれないように, 次のような様々なだましのテクニックを駆使している.

- 業務に関係が深い話題
  例えば, 取材依頼・製品の問い合わせ・クレーム
- 組織全体への案内
  例えば, 人事情報・新年度の事業方針
- 実在する組織名や個人名を含む
  例えば, 情報セキュリティに関する注意喚起・インフルエンザの流行情報.

◆やり取り型攻撃

辻褄の合う内容のメールをやり取りし, 受信者を信頼させた上で, マルウェアを添付したメールを送りつける攻撃である. 返信せざるを得ない, 外部向け問い合わせ窓口のメールアドレスに対して, 事前に「ここが問い合わせ先で間違いないか？」などの偵察メールがあったり, 適切な内容を複数回返信したりして安心させたうえで, マルウェアを送りつける.

◆APT[31]

標的となる組織の脆弱性を突くために, 事前に調査した上で, 複数の攻撃手法を組み合わせて作られたマルウェアで行う攻撃である. 既存の攻撃手法の中から, システムへの侵入を目的とする共通攻撃部と, システムの侵入後に特定のシステムを標的とする個別攻撃部を組み合わせて, マルウェアを作る.

◆水飲み場攻撃[32]

標的は組織がよく利用する Web サイト(水飲み場)にマルウェアを埋め込み, その組織から接続したときだけマルウェアを感染させる攻撃である. 特徴は, 次のとおりである.

- IP アドレスなどから接続元を解析し, 標的となる組織から接続されたときだけ, 攻撃する
- 攻撃対象を, 標的となる組織だけに限定することで, 攻撃の発覚を遅らせ, 攻撃の成功率を高める

---

28 企業・役所・法人・団体などを含む.
29 例えば, 情報セキュリティ製品(ファイアウォール・プロキシサーバなど)の有無・セキュリティパッチが未適用の情報機器の有無.
30 元となるマルウェアを改造したマルウェア.
31 語源は, Advanced Persistent Threats(高度かつ継続的な脅威)から. 情報処理推進機構(IPA)では, APT を「新しいタイプの攻撃」と呼んでいる
32 Watering Hole Attack. 語源は, 砂漠にあるオアシス(水飲み場)に寄ってくる動物を, 猛獣が待ち伏せて仕留める攻撃と似ていることから.

○標的型攻撃への対策

◆ファイアウォール[33]
インターネット(外部)と社内ネットワーク[34](内部)の境界に配置し, 外部から内部への不正な通信の侵入や, 内部から外部への不正な通信の送出を遮断する製品である. 例えば, ファイアウォールにより, プロキシサーバ[35]を経由しない, 内部から外部への通信を遮断する.

◆出口対策[36]
万一, 不正侵入されたとしても, 情報を外部に送出させないための対策である. ウイルス対策ソフトやファイアウォールなどを使って, マルウェアを, 外部(インターネットなど)から内部(社内ネットワーク)に入れないための入口対策だけでは, 対応しきれない攻撃が増えているため, 出口対策も重要視されている.

サイバー攻撃による被害を防ぐには, 次の 3 つの対策をバランスよく実施する必要がある.

- 入口対策：攻撃をネットワークシステムやシステムに不正侵入させない
- 内部対策：ネットワークやシステムの内部に不正侵入された後に被害を拡大させない
- 出口対策：情報を外部に送出させない

◆多層防御
入口対策・内部対策・出口対策のように, 複数の対策を, 多くの階層・段階で行うことである.

◆VLAN[37]
通常利用する社内ネットワークと, 機密情報にアクセスできる社内ネットワークとを, 分離して設置するために使う. VLAN を使うと, わざわざ各ネットワーク用にスイッチングハブを別々に設置しなくても, 共通のスイッチングハブを設置するだけで済む. なぜなら VLAN を使えば, 2 種類のネットワークを別物として扱えるためである. 費用が削減でき, また, セキュリティ向上を目的としたネットワークの分離がしやすくなる.

◆パーソナルファイアウォール[38]
不正な通信の通過を禁止したり, 正規の通信の通過を許可したりするソフトウェア製品である.
ファイアウォールとの違いは, 次のとおりである.

	ファイアウォール	パーソナルファイアウォール
製品の種類	ハードウェア機器・ソフトウェア	各情報機器にインストールするソフトウェア
目的	インターネットと社内ネットワークの境界に配置し, 外部から内部への不正侵入を防ぐ	社内ネットワーク内の各情報機器に導入し, 内部での被害拡大や情報の外部への送出を防ぐ

パーソナルファイアウォールは, サイバー攻撃により不正侵入されたとしても, そこから同じネットワーク上にある別の情報機器に被害を広めないため(内部対策)や, 情報を外部に送出させない(出口対策)ために, 使用する.

---

33 語源は, firewall(防火壁)から. 防火壁とは, 火災の炎症を防ぐ目的で設置される耐火構造の壁である.
34 企業などの組織内のみで構築されたネットワーク環境. LAN.
35 社内ネットワークとインターネットの境界に配置し, インターネットからの接続を代理する機器.
36 語源は, 攻撃者が内部に侵入し, 機密情報を持って出る際の出口になるから.
37 Virtual LAN(仮想 LAN)の略.
38 語源は, 各情報機器に個別(personal)に導入するファイアウォールであることから.

○その他のサイバー攻撃

◆ゼロデイ攻撃[39]
ソフトウェアにセキュリティホール(脆弱性)が発見された際, 修正プログラムが提供されるより前に, そのセキュリティホールを悪用して行われる攻撃である.

◆ランサムウェア[40]
コンピュータのファイルやシステムを使用不能にし, その復旧と引き換えに金銭を要求するソフトウェアである.

◆ドライブバイダウンロード[41]
Web サイトを閲覧しただけで, マルウェアを Web 閲覧者のコンピュータにダウンロードさせる攻撃である. 主に, Web ブラウザや OS の脆弱性(セキュリティホール)が悪用される.

○パスワードクラック

パスワードを見破る攻撃である. パスワードが見破られると, 不正侵入やなりすましされ, 個人情報や秘密情報が盗まれたり, システムやデータが破壊されたりする.

◆類推攻撃
利用者の情報をもとに, 攻撃者がパスワードを類推する方法である. パスワードが, 利用者 ID[42]・名前・生年月日・地名・出身校などの場合, 攻撃者がパスワードを見破ることがある.

◆辞書攻撃[43]
パスワードに単語を使う人が多いことを悪用し, 辞書の単語を利用してパスワードを推察する方法である. ブルートフォース攻撃に比べて, 見破るまでの効率が良いため, ブルートフォース攻撃の前に, まず辞書攻撃でパスワードの見破りを試す.

辞書の例は, 次のとおりである.
- 12345678
- password
- qwerty(キーの並び)
- admin(管理者権限の ID)
- login

◆ブルートフォース攻撃[44]
パスワードの可能な組み合わせをしらみつぶしにすべて試す方法である. 総当り攻撃ともいう. 効率が悪い方法のため, 人間ならば面倒で諦める作業であるが, コンピュータにやらせてパスワードを見破ろうとする. 例えば, 銀行 ATM(現金自動預払機)の場合, 暗証番号は 4 桁なので 0000～9999 まで最大 1 万回すべて試せば, 必ず暗証番号を見破れる.

---

39 語源は, 修せプログラムが提供された日を 1 日目とし, それより前である 0 日(Zero Day)に攻撃が行われることから.
40 語源は, ransom(身代金)＋ware(software：ソフトウェア)から.
41 語源は, Drive-by Download(ダウンロードにより, マルウェアが実行)から.
42 ユーザを識別するための名前や番号のこと. ユーザアカウントともいう.
43 「辞書」とは, 一般的な辞書ではなく, パスワードとなりそうな単語をまとめたパスワード候補集のこと.
44 語源は, brute force(力づくの)から.

◆リバースブルートフォース攻撃[45]
1 つの利用者 ID について, 様々なパスワードを試すブルートフォース攻撃とは対照的に, 1 つのパスワードについて, 様々な利用者 ID を試す方法である. 1 つの利用者 ID について, 何度もログインを試すわけではないため, アカウントロックアウトは, 対策とならない.

◆パスワードリスト攻撃[46]
利用者 ID・パスワードを使いまわす利用者が多いことから, ある Web サイトやシステムから流出した利用者 ID とパスワードのリストを使って, 別の Web サイトやシステムへの不正ログインを試みる攻撃である. 不正ログインされる Web サイトやシステムに脆弱性がなくても, 攻撃が成功する.

◆レインボー攻撃
予想したパスワードをもとに求められたハッシュ値[47]と, 利用者のパスワードのハッシュ値を照合し, パスワードを見破る方法である. パスワードは, 通常, そのまま保存されず, パスワードをもとに, ハッシュ関数により計算されたハッシュ値が保存されている. 予想したパスワードのハッシュ値の一覧表(レインボーテーブル)と, 利用者のパスワードのハッシュ値を比較することで, パスワードを特定する.

○パスワードクラックへの対策
◆コアパスワード
使い回しがなく, 長く, 複雑なパスワードを作るための, パスワード共通部分である. パスワードを定期的に変更することは, ブルートフォース攻撃が多かった従来は効果的であった. しかし, 細菌はフィッシング[48]やパスワードリスト攻撃によるパスワード流出が主流であるため, IPA では, パスワードの定期変更を推奨するのではなく, 複雑なパスワードを作り, サービスごとに使いまわさないための, コアパスワードなどを使ったパスワードの作り方を推奨している.

●コアパスワードを作る手順
① 好きな日本語を決める.
② ローマ字に変更する.
③ 一部分を大文字にしたり, 記号・数字を追加したりする.

●サービスごとに異なるパスワードを作る手順
① サービス名の略称・頭文字・URL の一部などから, サービスごとの文字列を決める.
② サービスごとの文字列を, コアパスワードの前または後に追加する.

●パスワードの管理方法
コアパスワードのみを暗記し, サービスごとの文字列は, 電子ファイルや紙で記録する. コアパスワードとサービスごとの文字列は別々に管理されるため, 万一盗まれても片方の情報だけでは悪用できない.

---

45 語源は, ブルートフォース攻撃の reverse(逆)であり, パスワードではなく, 利用者 ID を試すことから.
46 語源は, 攻撃者が何らかの方法で事前に入手した利用者 ID とパスワードの「リスト」を使うことから.
47 ハッシュ関数により計算された値. ハッシュ関数は, パスワードからハッシュ値は作れるが, 逆はできないという一方向性・不可逆性をもつ.
48 有名企業や金融機関等を装った偽のメールを送りつけ, 偽の Web サイトに誘導して, 個人情報を入力させてだまし取る行為.

◆ワンタイムパスワード[49]
1 回限り有効な使い捨てパスワードである. 認証のたびにパスワードを作り, 時間が経過するとパスワードは無効になる. 仮にパスワードが盗聴されても, 次回は異なるパスワードに変わるため, 不正利用を防止できる.

例えば, ネットバンキングで高額の取引を行う場合, なりすましを防ぐために, ハードウェアトークン[50]により生成したワンタイムパスワードの入力が必要になることがある.

◆生体認証
バイオメトリクス認証[51]ともいい, 人間の身体的特徴(生体器官)や行動的特徴(癖)などの生体情報を使って, 利用者を認証することである. 事前に登録・採取した生体情報と, 認証時にセンサで読み取った生体情報とを比較して本人確認を行う. 代表的な生体認証技術は, 次のとおりである.

●身体的特徴(生体器官)
- 静脈パターン認証：手のひらの血管の分岐点の分岐角度や分岐点間の長さの特徴
- 顔認証：顔の形や目・鼻などの位置関係
- 指紋認証：指のしわの分岐や切れ目の位置などの特徴

●行動的特徴(癖)
- 声門認証：声を, 時間と周波数の分布で解析した特徴

生態的認証には, 次の長所と短所がある.

- 長所：盗難・貸し切り・複製・紛失の心配がない
- 短所：認証のための機器の費用がかかる. 利用者情報の事前登録に手間がかかる. 本人拒否率[52]・他人受入率[53]をゼロにはできない.

◆ロックアウト[54]
ある回数以上パスワードを誤入力した場合, その利用者 ID を使用禁止にすることである. ブルートフォース攻撃の対策になる.

◆ソルト[55]
パスワードを見破りにくくするために, パスワードとハッシュ関数をもとにハッシュ値を決める際に, パスワードに付け加える文字列のことである. ソルトは, 長く, かつ利用者 ID ごとに異なるランダムな文字列にする. パスワードにソルトを付け加えた文字列をもとに, ハッシュ値を求めることにより, 元のパスワードが同じであっても, ハッシュ値は利用者ごとに別々になる. そのため, 元のパスワードを見破ることが難しくなり, レインボー攻撃の対策となる.

49 OTP(One Time Password)ともいう.
50 カード型やキーホルダー型の専用機器. この機器を持っていなければ, ワンタイムパスワードは生成できないため, 所有物認証になる.
51 語源は, biology(生物学)＋metrics(測定)から.
52 誤って本人を拒否する確率. FRR(False Rejectionn Rate)ともいう.
53 誤って他人を受け入れる確率. FAR(False Acceptance Rate)ともいう.
54 語源は, lock out(締め出す, 排除する)から.
55 語源は, 見破りにくくするために文字列を付け加えることを, salt(塩)による味付けに例えたことから.

◆ストレッチング[56]
パスワードを見破るまでの時間を増やすために, パスワードを元にハッシュ関数で計算して求めたハッシュ値に対し, 更にそのハッシュ値をもとにハッシュ関数で計算してハッシュ値を求めるという作業を繰り返すことである.

◆リスクベース認証
不正アクセスを防ぐ目的で, 普段とは異なる利用環境から認証を行った場合に, 追加の認証を行うための仕組みである. 例えば, 認証時の, IP アドレス・OS・Web ブラウザなどが, 普段と異なる場合に, 攻撃者からのなりすましでないことを確認するため, 合言葉による追加の認証を行うことである.

◆ログ
システムやネットワークで起きた異常を時系列に記録・蓄積した通信履歴である. ログインの失敗をログに記録しておけば, あとで攻撃者の特定に役立つ.

◆ログの管理
情報機器の稼動状態・障害や以上の発生状況を記録するログを管理する. ログ管理目的は, 情報システムが組織のルールに従って使われているかの確認・障害や異常の検知・不正アクセスや情報漏えいの調査や原因究明である.

●取得するログ
取得すべきログは, 次のとおりである.

- 利用者・管理者による情報システムの操作記録(利用者 ID・ログオンとログオフの日時・データやファイルへのアクセスの成功と失敗の記録・特権操作[57]の記録・無許可のアクセス)
- ファイアウォール・IDS・IPS などの通信記録・プログラムの動作記録・システム警告や障害

●ログの保存と管理
ログの保存と管理方法について, 次を検討すべきである.

- 保存場所
  それぞれの機器内にログが保存するか, ログを 1 か所にに集約し一元管理するか
- 保存期間
  ログのサイズは膨らみやすいため, どのくらいの期間, ログを保存するか
- ログのローテーション
  ログがいっぱいになる前に, 外部の記憶媒体[58]へ退避するか
- ログの保護
  侵入者による不正操作の証拠隠滅を目的とした, ログの消去を防ぐため, 複数ヶ所にログを保存したり, ログへのアクセス制御を行ったりする.

●時刻合わせ
情報セキュリティ事故発生後の原因究明で, 前後関係を特定するために, 複数の機器の, 複数のログの時刻を事前に同期(時刻合わせ)させておく必要がある. そのために, 時刻の動機を自動で行うためのプロトコルである NTP[59]を使うことがある.

---

56 語源は, stretching(引き伸ばすこと)から.
57 利用者 ID の登録・削除・アクセス制御など, システム管理者が行う操作.
58 情報を保存するための装置やメディア. 例えば, DVD・USB メモリ.
59 正確な現在時刻を取得するためのプロトコル. Network Time Protocol の略.

◆WORM[60]
書き込みは１回限りで, 読み取りは何回も可能な記憶媒体である. 例えば, CD-R・DVD-R・BD-R がある. 一度書き込んだ情報は, 消去も書き換えもできないため, ログなど, 故意に消される危険性があるデータを保存する場合に用いる.

◆ディジタルフォレンジックス[61]
情報セキュリティの犯罪の証拠となるデータを収集・保全することである. 例えば, ログや記憶媒体の消去・改ざんを防止するために, 書き込み禁止にしたり, コピーしたりして, その後の捜査や訴訟に備える.

60 Write Once Read Many の略.
61 語源は, digital(ディジタル)＋forensics(科学捜査・鑑識)から. コンピュータ・フォレンジクスともいう.