**14\_セキュリティ（安全）**

**目录:**

1. **情報セキュリティの概念**
2. **攻撃手法**
3. **情報セキュリティ技術**
4. 情報セキュリティ管理
5. 情報セキュリティ対策

**目标:**

* 能够区分各种攻击手段。
* 理解对称加密方式//共通鍵暗号方式与非对称加密方式//公開鍵暗号方式的区别。
* 理解数字签名的方法以及被认证的内容。

**情報セキュリティの概念**

**什么是信息安全?**

近年来，作为企业的经营资源，“信息”的重要性正不断提升。  
企业必须切实实施充分的信息安全对策//セキュリティ対策

以便正确管理信息，防止信息泄露或丢失等问题的发生。

**官方定义:**

根据 JIS Q 27000:2019:

“ 情報セキュリティ ” 指的是维护信息的：

● 機密性（Confidentiality）

● 完全性（Integrity）

● 可用性（Availability）

|  |  |
| --- | --- |
| **分類** | **定義** |
| **機密性** | 認可されていない個人、エンティティ//实体また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 |
| **完全性** | 正確さおよび完全さの特性 |
| **可用性** | 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 |

**不正トライアングル：**

组织发生安全事件，其原因常常可以归结为以下三大要素同时存在：

|  |  |
| --- | --- |
| 機会 | 有权限漏洞、审查不严、制度不完善 |
| 動機 | 金钱压力、报复心理、挑战欲 |
| 正当化 | “反正公司欠我钱” / “只是帮朋友查一下” 等心理说服 |

**各种安全问题具体例:**

DDoS攻撃によって、Webサイトがダウン//宕机した。

无法访问系统或服务是**可用性**的问题

キーボードの打ち間違いによって、不正確なデータが入力された。

数据不正确是**完整性**被破坏

PCがマルウェア//恶意软件に感染したことによって、個人情報が漏えいした。

信息被第三方看到就是**机密性**受损

**攻撃手法**

1. **ソーシャルエンジニアリング//社会工程**

コンピュータシステムにアクセスするために必要な情報などを、  
人間の行動や心理に生じる隙を利用して盗み出す行為  
// 一种攻击方式，利用人类的心理、行为疏忽、信任等弱点来非法获取信息。

|  |  |  |
| --- | --- | --- |
| **日文分類名** | **中文分類名** | **特征说明** |
| ショルダーハッキング | 肩窥攻击 | 偷看别人打密码（从肩膀后偷看） |
| なりすまし | 身份伪装 | 假装是管理员/上司/同事骗你提供密码 |
| トラッシング | 垃圾搜集 | 从垃圾中找重要信息（如账号纸条） |
| フィッシング電話 | 诱骗电话 | 假装是银行/公司打电话来套取资料 |
| フィッシングメール | 诱骗邮件 | 钓鱼邮件，骗你点击链接输入账号密码 |

1. **マルウェア//恶意软件**

悪意をもって作成された不正プログラムの総称である。

|  |  |  |
| --- | --- | --- |
| **日文分類名** | **中文分類名** | **特征说明** |
| トロイの木馬 | 特洛伊木马 | **潜伏系统中，窃取信息**。常见有远程控制（RAT）、键盘记录（キーロガー）、后门程序（バックドア）等。 |
| ウイルス | 病毒（狭义） | **依附文件运行，需宿主存在**。常见类型包括启动区感染型、宏感染型等。 |
| 暗号化・脅迫・破壊系 | 加密/勒索/破坏类 | 近年来威胁增加，代表有**勒索**软件（ランサムウェア）、**摧毁**数据的 Wiper、点击即感染软件等。 |
| ワーム | 蠕虫 | 能**自行复制并传播，不需宿主**。可通过网络或可移动设备感染传播。 |
| アドウェア | 广告软件 | 显示大量广告，骚扰用户。 |
| スパイウェア | 间谍软件 | **偷偷收集用户信息**、浏览记录、账号密码等。 |
| ハッキングツール | 黑客工具 | 用于渗透测试或攻击准备的**工具**（部分合法工具被恶意使用）。 |
| ボード | 僵尸程序 | 感染后，变成可**被远程控制的僵尸主机**, 攻击者通过 C&C 服务器操控 |

1. **パスワードクラック//密码破解**

パスワードを不正に解読・入手する攻撃手法

-

|  |  |  |
| --- | --- | --- |
| **日文分類名** | **中文分類名** | **特征说明** |
| ブルートフォース攻撃  （総当たり攻撃） | 暴力破解 | 针对某个 ID，尝试所有可能的密码组合，一一验证。 brute force 的原意是“靠蛮力”。 |
| リバースブルートフォース攻撃  （逆総当たり攻撃） | 反向暴力破解 | 固定一个常见密码，然后尝试各种 ID，找出哪些用户使用了该密码。 |
| 辞書攻撃 | 字典攻击 | 利用词典或人名等常用词作为候选密码进行尝试。 |
| パスワードリスト攻撃 | 密码列表攻击 | 利用从其他服务中泄露的账号 + 密码组合尝试登录系统。 |

1. **WEB①：クロスサイトスクリプティング（XSS）//跨站脚本攻击**

ウェブページに悪意のある命令（スクリプト//脚本）を埋め込んで、利用者から情報を盗み出す攻撃。

|  |  |  |
| --- | --- | --- |
| 步骤 | 日文说明 | 中文翻译 |
| ① | 脆弱性のある掲示板などに攻撃者がJavaスクリプトなどで書かれた不正プログラムを投稿する。 | 攻击者在存在漏洞的留言板等位置，嵌入恶意 JavaScript 脚本。 |
| ② | サイトを閲覧したユーザのブラウザ上で不正プログラムを実行する。 | 普通用户访问该页面后，脚本在浏览器中自动执行。 |
| ③ | 偽のサイトに誘導されたり、個人情報を搾取されたりの被害が報告されている。 | 用户可能被引导到假网站或个人信息被窃取，造成损失。 |

1. **WEB②：ドライブバイダウンロード//恶意自动下载**

Webサイトなどに不正なソフトウェアを隠しておき、  
閲覧者がアクセスすると気づかないうちに自動でダウンロードして実行する攻撃手法。攻撃に利用されるサイトは、攻撃者が用意したサイトとは限りません。  
一般企業などが運営してるホームページが第三者に改ざんされてしまい、  
結果としてコンピュータウイルスをばら撒いてしまうケースも報告されています。

|  |  |  |
| --- | --- | --- |
| 步骤 | 日文说明 | 中文翻译 |
| ① | Webサイトにマルウェアやウイルスを仕込む。 | 在网站中植入恶意软件或病毒。 |
| ② | サイト利用者が知らぬうちに、自動ダウンロードまたは実行させる。 | 用户在毫无察觉的情况下，恶意程序被自动下载或执行。 |

1. **WEB③：SQLインジェクション// SQL 注入攻击**

入力フォーム//输入框から入力した「SQL文を含む文字列」で、アプリケーション//应用程序が想定しないSQL文を実行させることにより、データベース//数据库を不正操作するサイバー攻撃//网络攻击の一種。

1. **ほかの攻撃手法①**：**DoS攻撃; DDoS攻撃//拒绝服务攻击; 分布式拒绝服务攻击**

Dos攻撃:

標的サーバに大量のデータを送信し続け、サーバのCPUやメモリなどに過剰な負荷をかけてサービスを妨害する攻撃。

DDos攻撃：

IoT機器を標的としてbot//僵尸程序を感染させ、攻撃者が操るC&Cサーバからの命令に従って一斉に攻撃を行うサイバー攻撃

1. **ほかの攻撃手法②：DNSキャッシュポイズニング**//DNS缓存投毒

DNS情報の探索を行うキャッシュサーバ//缓存服务器に不正な手段で嘘の情報を覚えさせ、利用者からの問い合わせに答えさせる手法。

 **用户请求**：  
　用户发送 DNS 查询：  
　>「https://www.〇〇〇.jp/ 的 Web 服务器的 IP 地址是多少？」

 **缓存服务器响应（已被篡改）**：  
　DNS 缓存服务器被攻击者事先写入虚假的 IP 地址，返回：  
　>「https://www.neec.ac.jp/ 的 IP 地址是『xx.xx.xxx.xxx』。」

 **用户被误导**：  
　用户信任该 IP 地址并访问，但实际上被诱导到**伪造的服务器**，而非真正的官方服务器。