**2\_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:**

* **了解整理各种安全协议。**
* **理解防火墙和 理解 WAF 的功能。**
* **了解DMZ 的作用。**

**情報セキュリティ管理**

セキュリティ管理和对策的关系

安全管理是“制定规则 + 建立体系”  
安全对策是“实际执行 + 措施内容

**ISMS**

**ISMS**是情報セキュリティ管理的核心体系

它不仅管理信息系统本身，还包括人、环境、流程等一整套安全策略的制度设计

**ISMS 中的信息安全对策的三大视角:**

|  |  |
| --- | --- |
| 物理的セキュリティ | 针对设施、设备、文书、记录媒介等的环境管理 |
| 人的セキュリティ | 对人的操作、管理方法、制度规则等的约束与规定 |
| 技術的セキュリティ | 利用硬件、软件、网络等技术手段来保护信息 |

**ISMS 的运行采用 PDCA 循环方式：**

**图形用户界面, 网站

AI 生成的内容可能不正确。**

|  |  |
| --- | --- |
| Plan | 建立 ISMS 策略与框架;**リスクアセスメント//风险评估** |
| Do | 实施 ISMS 系统并开始运作 |
| Check | 监督运行状况并做评估、审查 |
| Act | 改善系统、进行必要的更新与改进 |

。

**ISMS 中最核心的工作内容就是リスクマネジメント**/**//风险管理**

**リスクマネジメント**有3个步骤: **确立 - 评估 - 应对：**

|  |  |  |
| --- | --- | --- |
| **リスク基準の確立** | 情報資産を保護するための判断基準を決定する | 决定“哪些情况构成风险”的基准 |
|  | | |
| **リスクアセスメント①**  **リスク特定** | 情報資産に対する脅威・脆弱性などからリスクを特定する | 从“威胁（攻击）”与“脆弱性（弱点）”等中识别出可能发生的风险事件 |
| **リスクアセスメント②**  **リスク分析** | リスクの発生頻度や発生時の影響の大きさなどを分析する | 分析风险发生的“频率”与“发生时的影响程度”等重要要素 |
| **リスクアセスメント③**  **リスク評価** | リスク分析の結果などから、それぞれのリスクに対してリスク受容が可能かどうかを評価する | 根据分析结果，判断这个风险是否可以接受？要不要处理？ |
|  | | |
| **リスク対応** | 受容できないリスクに対し、リスク対応策を決定・実施する | 对于无法接受的风险，制定并实施应对策略（加密、防火墙等） |

**リスク対応**//风险应对策略

|  |  |  |
| --- | --- | --- |
| **リスク回避** | リスクを避けるために特定の活動やプロジェクトを中止する、または代替する。 | 中止或替代高风险活动，以完全避免该风险的发生。 |
| **リスク低減（予防）** | リスクの発生確率や影響を軽減するための対策を実施する。 | |  | | --- | |  |  |  | | --- | | 采取措施降低风险发生的概率或其影响，如使用防火墙、定期备份等。 | |
| **リスク移転** | 保険をかけたりリスクのある業務を委託したりすることでリスクに関する損失の負担を他者と分担する。 | 通过购买保险或外包，将可能带来的损失责任转嫁给他人。 |
| **リスク受容** | リスクを認識し、そのまま受け入れる。 | 明知存在风险但选择接受。 |

**情報セキュリティ対策**

1. **不正アクセス対策**

**不正アクセス対策 とは**、アクセス権のない利用者がシステムやデータを不正に使用するのを防ぐ対策である。

* 1. **パスワードクラック対策**// 防破解密码对策

|  |  |
| --- | --- |
| ブルートフォース  (総当たり攻撃) | 必要十分な長さにする。 |
| リバースブルートフォース攻撃  （逆総当たり攻撃） | 英数字、記号などを組み合わせた、意味のない文字列にする。 |
| 辞書攻撃・類推攻撃 | 味のない文字列にする。 |
| パスワードリスト攻撃 | 再利用しない。 |

**②　クラッキング対策**:// 防破解对策

**ポートスキャン**：//端口扫描（Port Scan）

コンピュータやルータのアクセス可能な通信ポートを外部から調査する行為。攻撃の前段階の調査として行われる場合と、攻撃を防ぐための対策として行われる場合がある。

//防破解的端口扫描是一种从外部侦测计算机或路由器“哪些通信端口是开放”的行为。  
它可能被用于攻击前的情报收集，也可能用于系统防御的安全检查

1. **マルウェア対策**

|  |  |  |
| --- | --- | --- |
| **パターンマッチング法**  **//**模式匹配法 | 既知のウイルスの特徴を記録した**ウイルス定義ファイル//病毒定义文件（パターンファイル//模式文件、シグネチャファイル//签名文件）**を参照し、これに該当するパターンが含まれていないか、実行ファイルなどをしらみつぶしに調べていく手法 | 参考记录了已知病毒特征的**病毒定义文件（模式文件、签名文件）**，逐个检查执行文件等中是否含有对应的病毒特征。 |
| **ルールベース法**  //规则基础法 | **ヒューリスティック法**：  ソースコードを静的に解析する手法  **ビヘイビア法（サンドボックス）**：不審なプログラムを実行する仮想環境などで検査対象を実行して、一般的なプログラムではありえないような挙動（重要なシステムファイルを書き換えようとする等）を検出する手法 | 启发式方法：静态分析源代码的方法 行为分析方法（沙盒）：在虚拟环境中运行可疑程序，检测是否存在“不符合正常程序”的行为（如尝试篡改系统文件）。 |

**Tips:耐タンパ性**