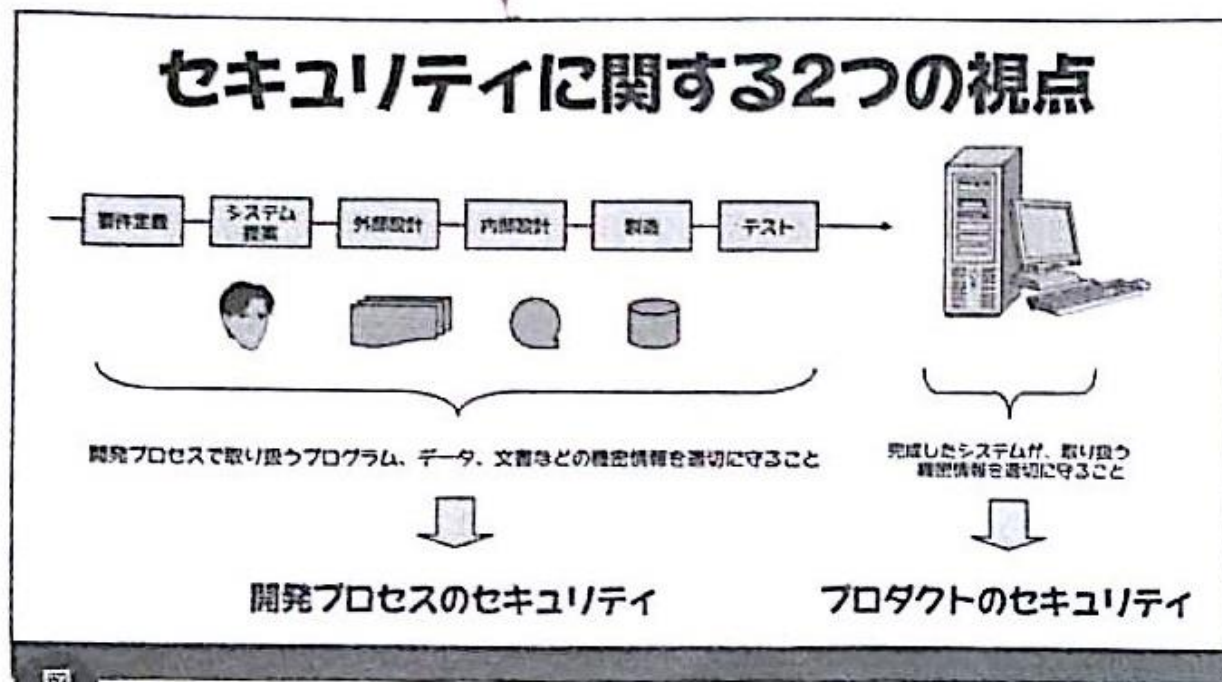


セキュリティ

60161017 金城 清史

システム開発のセキュリティ

- セキュリティの2つの視点
 - プロダクトのセキュリティ
 - 開発プロセスのセキュリティ



プロダクトのセキュリティ

- プロダクトセキュリティは開発工程の上流ですべき
 - 要件定義や外部設計の段階から考慮し始めるのがベスト
- どのようなセキュリティ手法を扱うかは、データに求められる機密性や顧客が必要とするセキュリティレベルに合わせる

セキュリティ項目

- | | |
|---|------------------------------------|
| 1 | 主体認証に関する項目 |
| 2 | アクセス制御に関する要件 |
| 3 | 権限管理に関する要件 |
| 4 | 監視・分析用アクセスログに関する要件 |
| 5 | 不正アクセスなどの監視要件（侵入検知システムの種類、監視場所） |
| 6 | ファイアウォール設置に関する要件（ファイアウォールの種類、設置場所） |
| 7 | ウィルス対策要件（クライアントPC、サーバーごとの要件） |
| 8 | 暗号要件（伝送メッセージ、データベース） |

セキュリティと利便性

- セキュリティと利便性はトレードオフの関係にあることが多い
 - 例：売上データ
 - データの開示すると、各担当者が様々な角度で分析できて便利⇔情報漏えいの危険性が高まる

実装攻撃と耐タンパ性

- 実装攻撃

- 稼働しているシステムを物理的に改変
- プログラムを動的または静的に分析
- 漏れ出している電磁波を読み取る

⇒ システム内部にしか存在しない機密データを読み出す行為

- この攻撃から機密性の高いデータを守ることを耐タンパ性と呼ぶ

耐タンパ性を与える技術

- 自己インテグリティ検証
 - プログラムが治部地震の改ざんを検出し、改ざんされている場合は実行しない仕組み
- 自己書き換え
 - 実行中にプログラムが、自分自身を書き換えることで、動作解析を困難にする
- テーブルネットワーク型実装
 - データの暗号化や復号化の際に、メモリや、ファイルに秘密鍵が現れないアルゴリズム

開発プロセスのセキュリティ

- 開発プロセスを向上させるポイント

保護区域と入退室	・機密情報を取り扱う区域を設定し、関係者だけがその区域に立ち居入れるようにする
資産と装置の管理	保護区域から持ち出すPCは許可を必要とする
設備と自然災害	停電などが少ない質の良い電源を確保する
日常の情報管理	PC画面は一定時間経過後にロックをかける
媒体の保管と持ち出し	指定された場所に指定された方法で管理する
媒体の複写	媒体の無断での複写を禁止する
媒体の移動や配送	移動する媒体を書き込むデータはパスワードを設定する・暗号化する
媒体の導入と廃棄	外部から勝手に媒体を持ち込まない

セキュリティのポイント

- 人間の行為がセキュリティに大きく関わる
 - ルールを守る
 - ルールの周知
 - 外部からUSBを持ち込まない
 - 勝手にコピーを作らない

まとめ

- プロダクトのセキュリティでは、ファイアウォールなどはもちろん実装攻撃に対するセキュリティも考える
- 開発プロセスのセキュリティでは、人間の行為に対する節制に注意する

セキュリティ項目 1

- 主体認証に関する要件
 - ユーザを識別するための認証方法をどうするか
 - 例
 1. IDとパスワードでログインする
 2. 電子証明書を使う など

セキュリティ項目 2

- アクセス制御に関する要件
 - システム上の情報に対して、誰がどのようにアクセスを行えるのか
- 例
 1. 重要なデータの読み書きはシステム管理者のみ許可など

セキュリティ項目 3

- 権限管理にかんする要件
 - ユーザに対して、どのような形で権限を与え、どのように管理するか
 - 例
 1. システム管理者グループに属するユーザは、システム管理者のみ許可 など

セキュリティ項目 4

- 監視・分析用アクセスログに関する要件
 - システムの利用状況監視や不正アクセスを分析するために必要なアクセス記録をどうするか
 - 例
 1. Webサーバのアクセスログ形式
 2. 管理者権限でデータ書き換えをおこなったユーザの記録 など

セキュリティ項目5

- 不正アクセスなどの監視要件（侵入検知システム（ネットワーク型IDS、ホスト型IDS）の種類、監視場所など）
 - ネットワークやサーバーへの不正アクセス監視をどうするか
 - 例
 1. 侵入検知システム設置の有無
 2. タイプ
 3. 設置場所

など

*IDS（Intrusion Detection System）＝侵入検知システム

セキュリティ項目 6

- ファイアウォール設置に関する要件（ファイアウォールの種類（ハード型・ソフト型）設置場所、冗長構成など）
 - 外部ネットワークから組織内ネットワーク、あるいはその逆の通信の可否を制御するしすてむであるファイアウォールについての検討
 - 例
 1. ファイアウォールの種類
 2. 設置場所
 3. 必要な機能

セキュリティ項目7

- ウィルス対策要件（クライアントPC、サーバごとの要件、ウィルス対策ゲートウェイなどの要件）
- 行うべきウィルス対策の全体像や具体的な方法をどうするか
 - 例
 1. ウィルス対策を行う位置
 2. ウィルス対策の内容

セキュリティ項目 8

- 暗号化の要件（伝送メッセージ、データベース、外部連携データなど）
- システム内外で暗号化を行う必要とする情報や部分の検討
 - 例
 1. 個人情報を扱う画面ではhttpsを使用する
 2. データベースに格納する項目のうち個人情報は暗号化して格納するなど