

第12章 セキュリティ 第13章 プロジェクト完了報告

資料：ずっと受けたかったソフトウェアエンジニアリングの新人研修 p.234～249

発表者：野口耕二郎

目次

- セキュリティの重要性
- 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
- プロジェクト完了報告
- まとめ

セキュリティの重要性

プロダクトに及ぶ危険

- ID, パスワードの詐取
- Webページの改ざん
- 不正アクセス
- 等々 ...

開発プロセスに及ぶ危険

- 開発工程の中で作成された文書やソースコードの盗難，漏洩
- 企業秘密の漏洩による会社運営の危機
- 内部構造が分かることになり，プロダクトへの危険につながる

セキュリティの重要性

- これら2つの危険に対しての対策がなければ会社運営は不可能
- これら2つの危険は性格が異なり，対策方法も異なる

プロダクトのセキュリティ

セキュリティ項目

- 上流工程で考慮し始めるのが理想的
- 各項目でどのような手法を採用するかを顧客と検討する

項目
主体認証に関する要件
アクセス制御に関する要件
権限管理に関する要件
監視・分析アクセスログに関する要件
不正アクセスなどの監視要件
ファイアウォール設置に関する要件
ウイルス対策要件
暗号化の要件

設計段階で考慮すべきセキュリティ項目

プロダクトの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
- 十分なセキュリティを確保したいが、利便性が顧客の要望に合わないという事態が少なくない
- それを避けるためにセキュリティに関しては顧客と十分に認識を合わせる必要がある

実装攻撃と耐タンパ性

- 実装攻撃：システムの内部にしかない機密性の高いデータを盗む攻撃
- 耐タンパ性：実装攻撃から機密性の高いデータを守る性能

名称	説明
自己インテグリティ検証	プログラムが自身の改ざんを検出し、停止する機能
自己書き換え	プログラムが自身を書き換え、動作解析を困難にする機能
テーブルネットワーク型実装	データの暗号化や複合化の際にメモリやファイルに秘密鍵が現れない機能

プログラムに耐タンパ性を与える技術

開発プロセスのセキュリティ

開発関係者の行動に注意が必要

- 開発関係者が何らかの理由で機密情報を盗む可能性がある
- 開発関係者の不注意で情報が漏えいすることがある
- 開発関係者がセキュリティについての知識を蓄えておく必要がある

セキュリティ項目

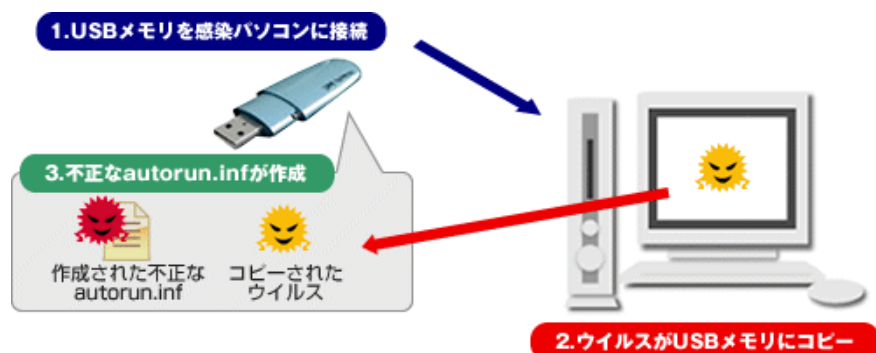
- 開発関係者の行動だけでなく自然災害に気をつける必要がある
- 項目の半分が媒体に関することに注意

項目
保護区域と入退室
資産と装置の管理
設備と自然災害
日常の情報管理
媒体の保管と持ち出し
媒体の複写
媒体の移動や配送
媒体の導入と廃棄

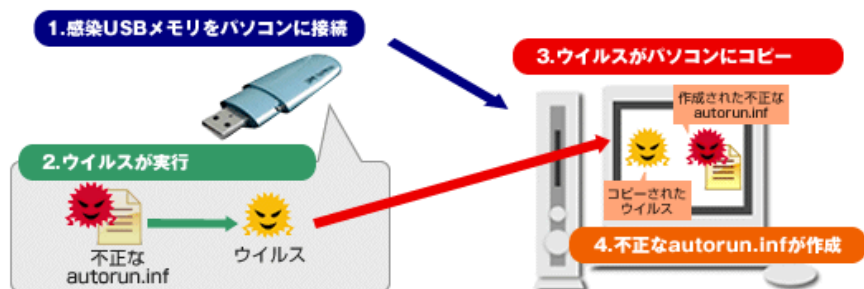
開発プロセスのセキュリティ項目

USB接続によるウイルス感染

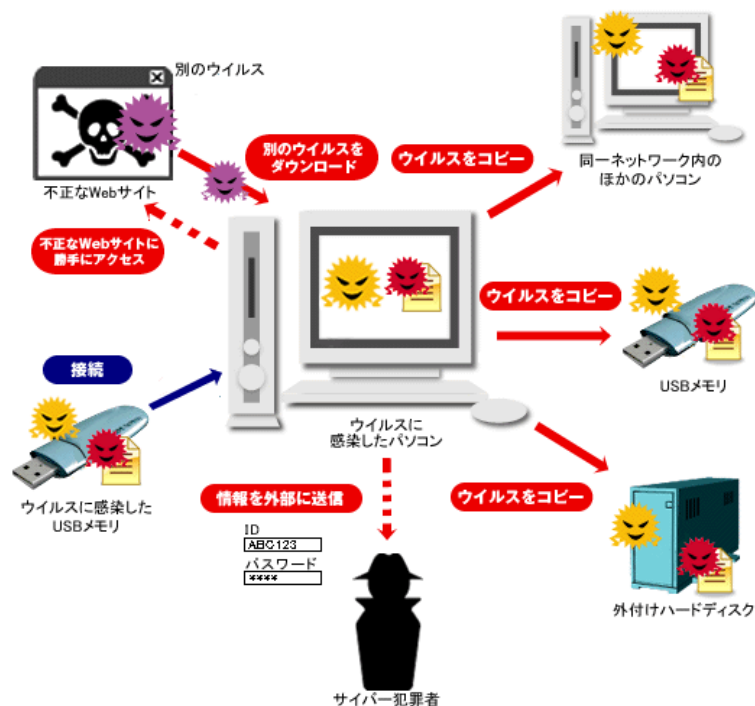
1. PC→USBにウイルス感染



2. USB→社内PCにウイルス感染



3. ウィルス感染による被害の発生



プロジェクト完了報告

完了報告書の必要性

- 自社の経営陣に開発結果を報告するための文書
- 開発計画書に対する結果として経営陣が具体的に知るために必要
- 計画書に書かれていることのうち、どれだけ達成できたかを明確にする

記述項目例

- それぞれの面を定性的、定量的に評価し、明確な報告をするようにする
- 人材育成状況など、経営陣が知っておきたいことも記述する

分類		記述項目
経営面	定性的	- 目標達成度 - 顧客満足度 - プロジェクト推移総括 - プロジェクトで得られた教訓 - 業務の継続性 - 業務の発展性
	定量的	- 売上高 - 稼働量 - 開発期間 - 利益 - 利益率
技術面	定性的	- 技術的課題と対策結果 - 工夫点 - 蓄積できた技術 - 人材育成状況
	定量的	- 開発規模 - 品質 - 生産性
所感		- 反省点 - 提案

まとめ

- ソフトウェア開発ではプロダクトとプロセスに対するセキュリティ対策がそれぞれ必要
- プロダクトのセキュリティでは利便性とのトレードオフ関係を考慮すべき
- プロセスでのセキュリティでは開発関係者の行動に注意が必要
- 完了報告書は経営陣が納得するように開発計画書に対する結果として作成する必要がある