情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

脅威分析法
組み込みの安全性とセキュリティを保証するために

2015/6/11

情報セキュリティ大学院大学
大久保隆夫

概要

- 講義
  以下について理解することを目標
  - ◆セキュリティ要求分析
  - ◆脅威分析
  - ◆安全性とセキュリティ

機能要求と非機能要求（要件）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 機能要求：ある機能を実現するもの
  - 情報を登録、参照する
  - データを計算する
  - メッセージを送受信する
- 非機能要求：機能以外のもの
  - 性能(スピード、処理能力)
  - 品質
  - セキュリティ

セキュリティ要求（要件）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 他の要求との違い(難しさ)
  - 要求策定者、利害関係者(ステークホルダー)ではない他者(悪意を持つ者)の要求に基づく
  - 特定の攻撃に対する対策を考慮した要求が必要(になる場合あり)
- 脅威(攻撃)に対する対策仕様≒セキュリティ要求仕様

セキュリティ要求分析

セキュリティ要求分析=セキュリティ要求仕様の策定

整理する要素

- 資産
  - 何を守るべきか
  - 個人情報データ、パスワード、重要な機能etc
- セキュリティゴール
  - 資産をどう守るかの目標
  - 機密性，完全性，可用性などのセキュリティ特性の観点で規定
- セキュリティ上のリスク
  - 対策しない場合のリスクを明確化
- セキュリティ要求
  - リスクとその脅威にどのような対策を行い，セキュリティゴールを達成すべきかをセキュリティ要求として明確に
- セキュリティ機能要求
  - 認証や，暗号化などのセキュリティの機能を明確に

脅威分析

- 対策を明らかにするために必要な作業
  - 守るべきもの(資産)は何か
  - 資産に対してどのような脅威があるか
  - 脅威によりどのようなリスクが発生するか
  - リスクに対してどのような対策をすれば目標を達成できるか

セキュリティ要求分析技術

- フォールトツリー分析
- ゴール指向(KAOS)の応用
- エージェント指向の応用
- UMLの応用
  - ミスユースケース
- SQUARE
  (Security Quality Requirements Engineering)

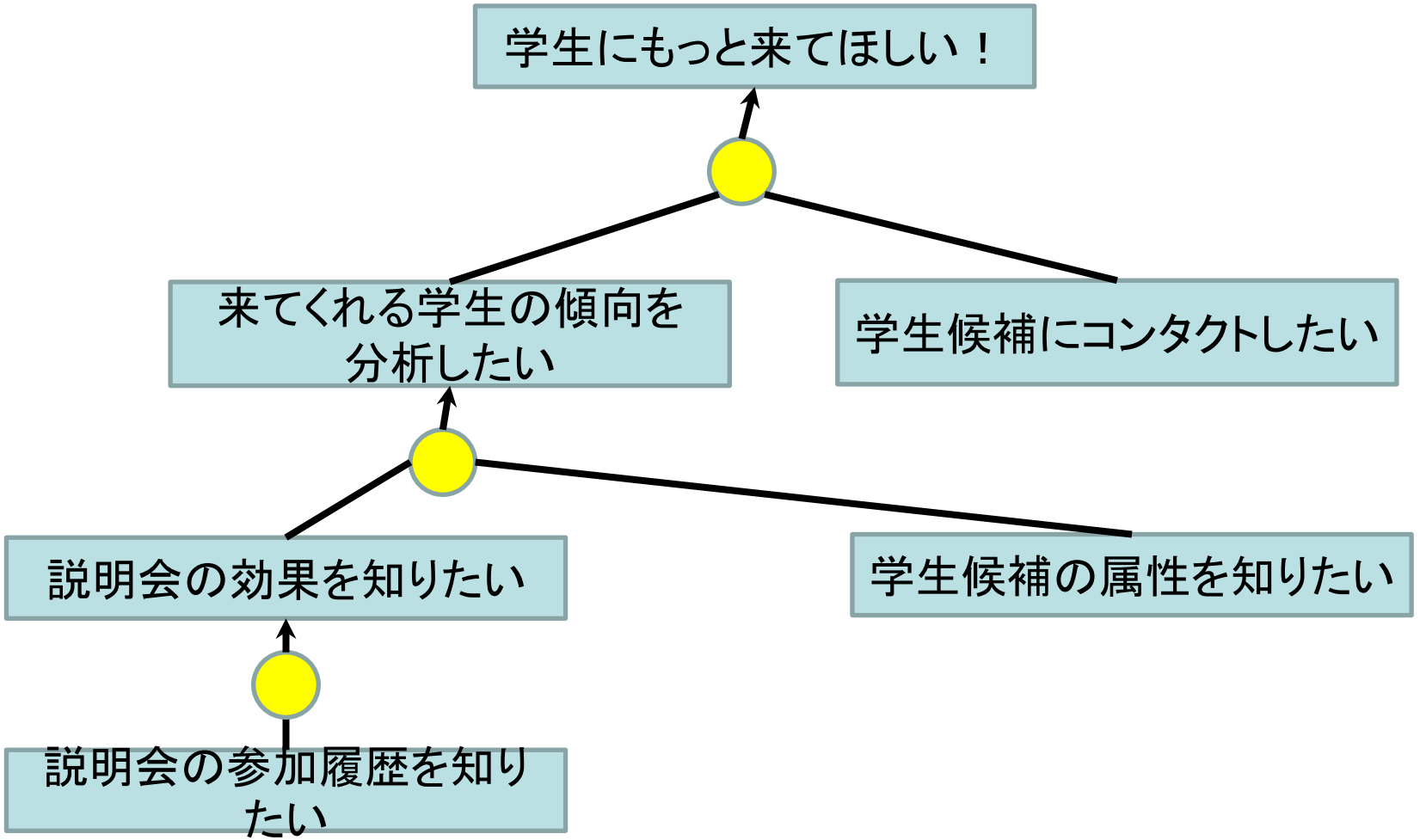
ゴール指向分析

- ゴール(目標)を詳細化することで要求を的確に獲得
- KAOS
  - ◆まずトップレベルのゴールを決め、順に詳細化する（サブゴール）
  - ◆サブゴールどうしと上位ゴールはAND/OR関係で連結

KAOS

- 要求工学的手法の中では、わりと使われている方
- 後述のエージェント指向的手法にも関連
- 応用としては、形式検証など

KAOS


学生にもっと来てほしい！
来てくれる学生の傾向を分析したい
学生候補にコンタクトしたい
説明会の効果を知りたい
学生候補の属性を知りたい
説明会の参加履歴を知りたい

ミスユースケース

- 2000年、Sindre,Opdahlが提案
- UMLユースケース図の拡張
  - ミスユーザ：意図しないことをするアクタ
  - ミスユースケース：意図しない挙動(脅威)
    ※必ずしも、悪意があるとは限らない
    ⇒セキュリティを含む「安全」も対象にできる
  - 対策：ユースケースで表記
- 脅威とその関係者、対策の関係が明確

脅威分析

脅威モデリング

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 設計したシステムにおける脅威分析(脅威の抽出、評価)を行う手法
  - Data Flow Diagram(DFD)を用いた脅威抽出
  - STRIDEによる脅威分類
  - 脅威ツリー、DREADによる脅威評価
- アーキテクチャが明確なとき、脅威抽出の手法としては有効
- 対策抽出は行わない

STRIDE

- Spoofing(なりすまし)
- Tampering(改竄)
- Repudiation(否認)
- Information disclosure(情報の漏洩)
- Denial of service (DoS攻撃)
- Elevation of privilege(権限昇格)

DREAD

- Damage potential(潜在的な損害)
- Reproductivity(再現可能性)
- Exploitability(攻撃利用可能性)
- Affected users(影響ユーザ)
- Discoverability(発見可能性)

脅威分析の手順

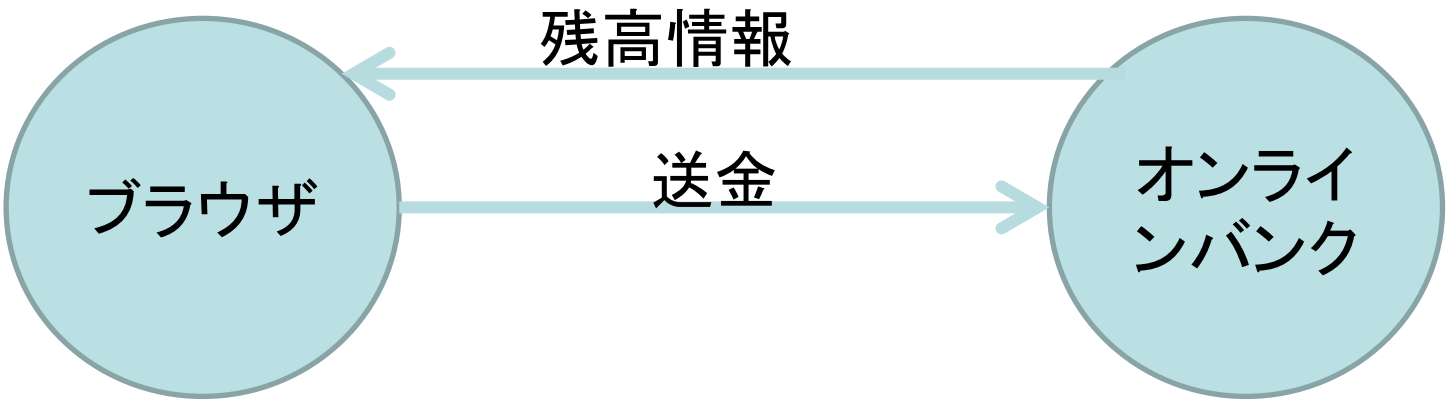
1. 資産の識別
2. セキュリティ目標の設定
3. 脅威の識別
4. 脅威の評価
5. 対策設計

例:オンラインバンク

- インターネット経由で口座所有者が自身の口座にアクセス
- 何が脅威？

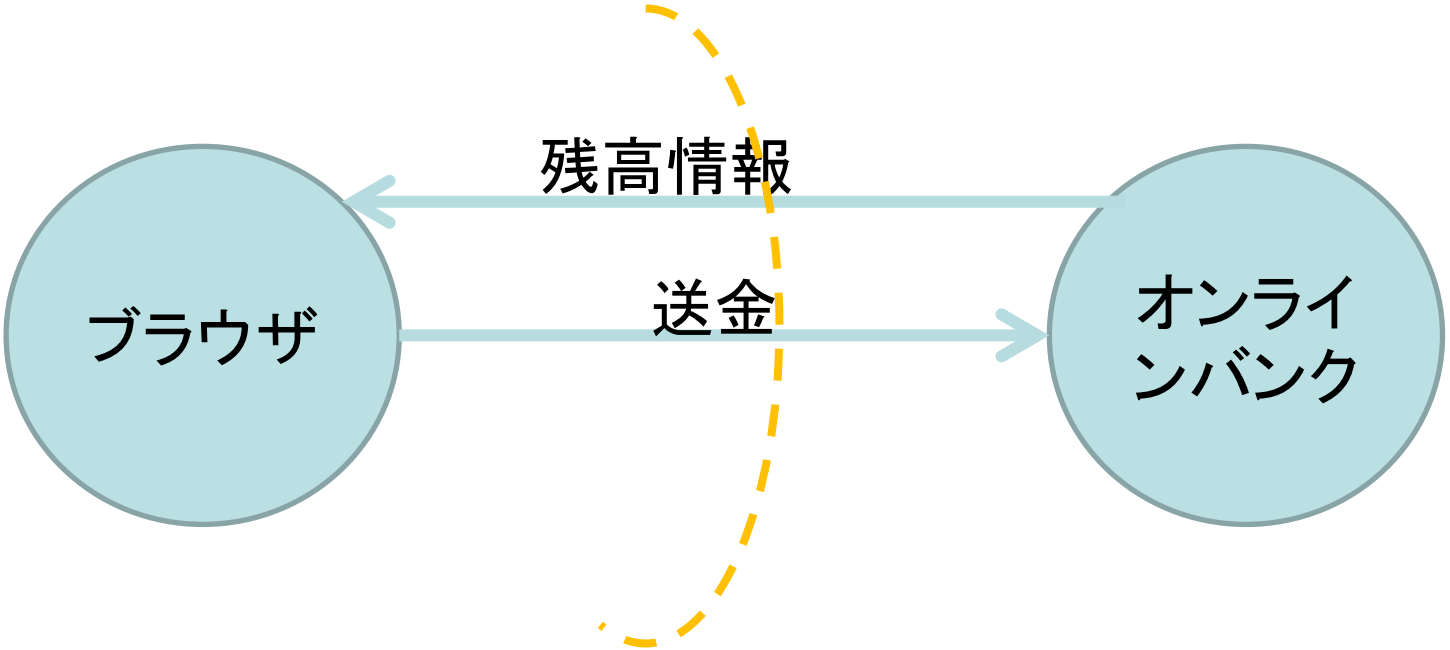
脅威の識別（1）

■データフロー(データの流れ)を書いてみる



脅威の識別（2）

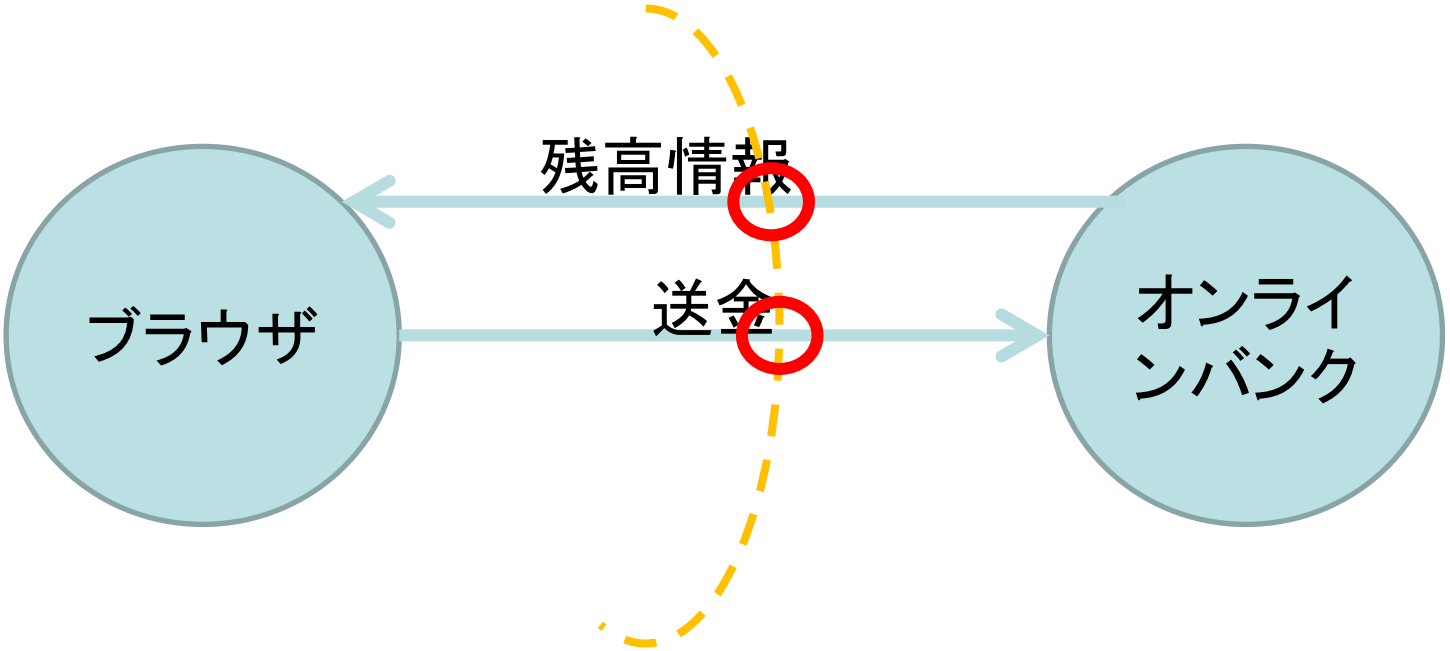
■信頼境界を設定する



脅威の識別（3）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

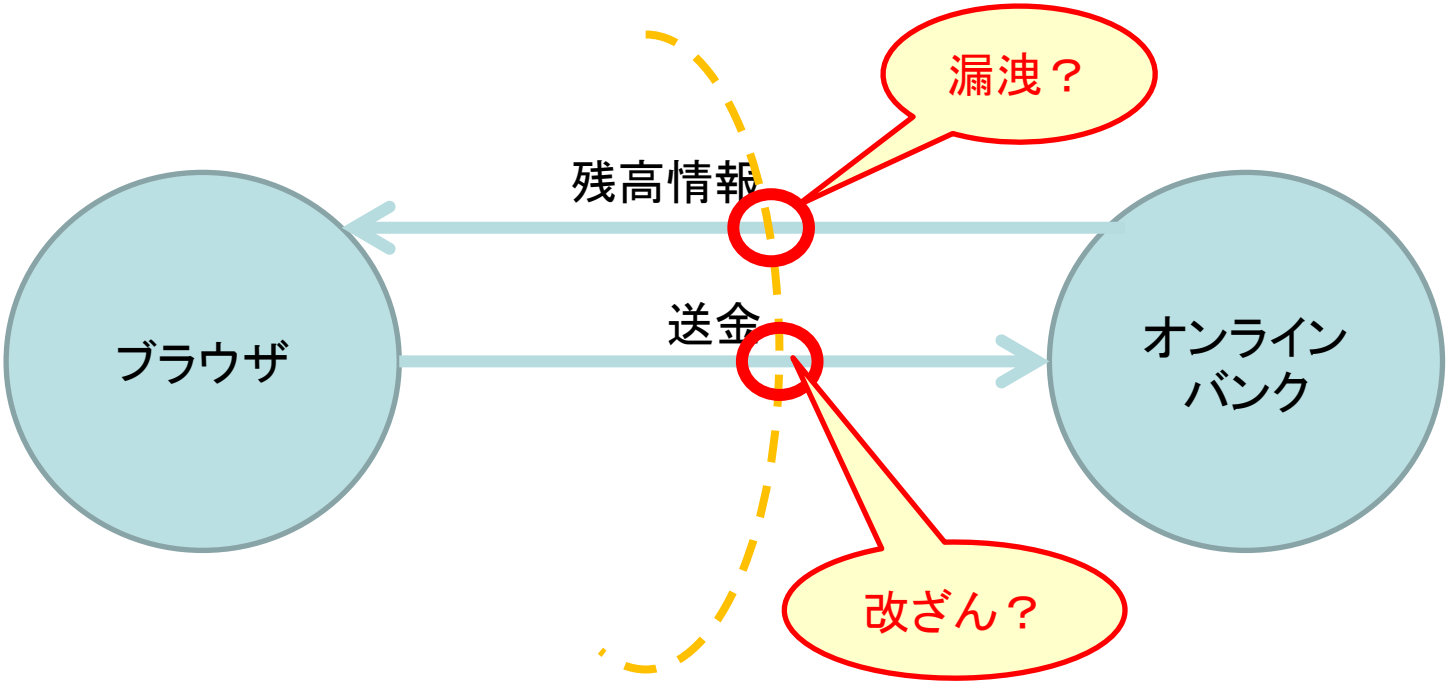
■攻撃ポイント(アタックサーフェス)を識別する



脅威の識別（4）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■アタックサーフェスで起きる脅威を考える



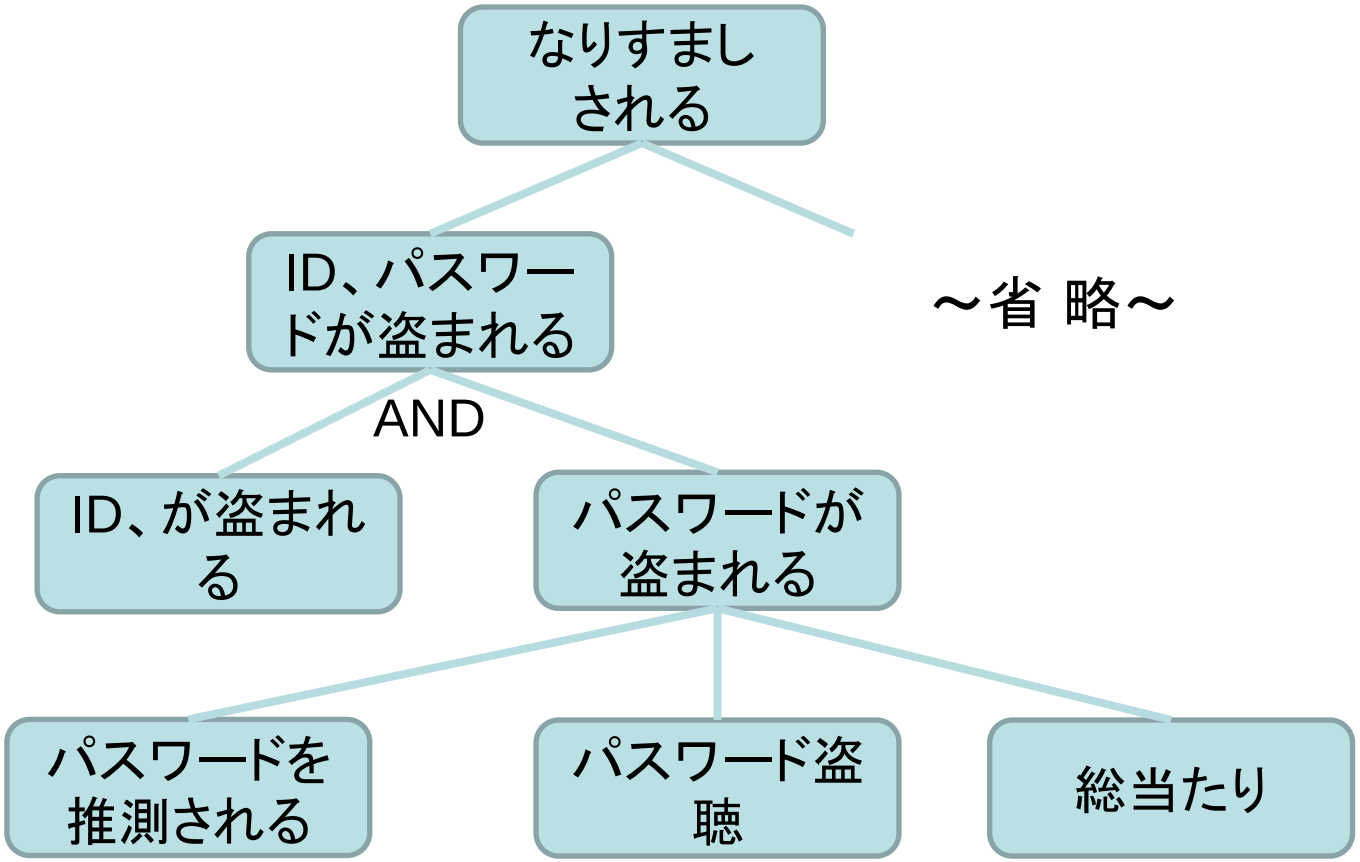
脅威分類

- 脅威を識別するための参考
- STRIDE(Microfost SDL)
  - Spoofing(なりすまし)
  - Tampering(改竄)
  - Repudiation(否認)
  - Information disclosure(情報の漏洩)
  - Denial of service (DoS攻撃)
  - Elevation of privilege(権限昇格)

脅威評価（1）

- 脅威の細分化:具体的条件、攻撃手段の検証
- 脅威木/アタックツリー/故障木

脅威木


なりすまし
される
ID、パスワードが盗まれる
～省 略～
AND
ID、が盗まれる
パスワードが盗まれる
パスワードを推測される
パスワード盗聴
総当たり

脅威評価（3）

- 脅威の影響を評価
- DREAD(Microsoft SDL)
  - Damage potential(潜在的な損害)
  - Reproductivity(再現可能性)
  - Exploitability(攻撃利用可能性)
  - Affected users(影響ユーザ)
  - Discoverability(発見可能性)

安全性とセキュリティ（2）

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- セキュリティで安全性をカバーできるか
- セキュリティ分析の能力
  - データフロー→CANの解析には不向き
  - 安全性重視の解析ではない
- IT系との相違
  - セキュアブート？
    車載には「off」の瞬間がない
  - スペック上の制約(帯域、メモリ、コスト…)

インターネット
（将来接続）

カーナビ

エンジン

ECU

ECU

CAN

CAN: Control er Area Network
ECU: Electric Control Unit

ECU

ECU

ECU

ECU

パワーウィンドウ

トランスミッション

ブレーキ

イグニッション

クルマが「安全」とは？

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

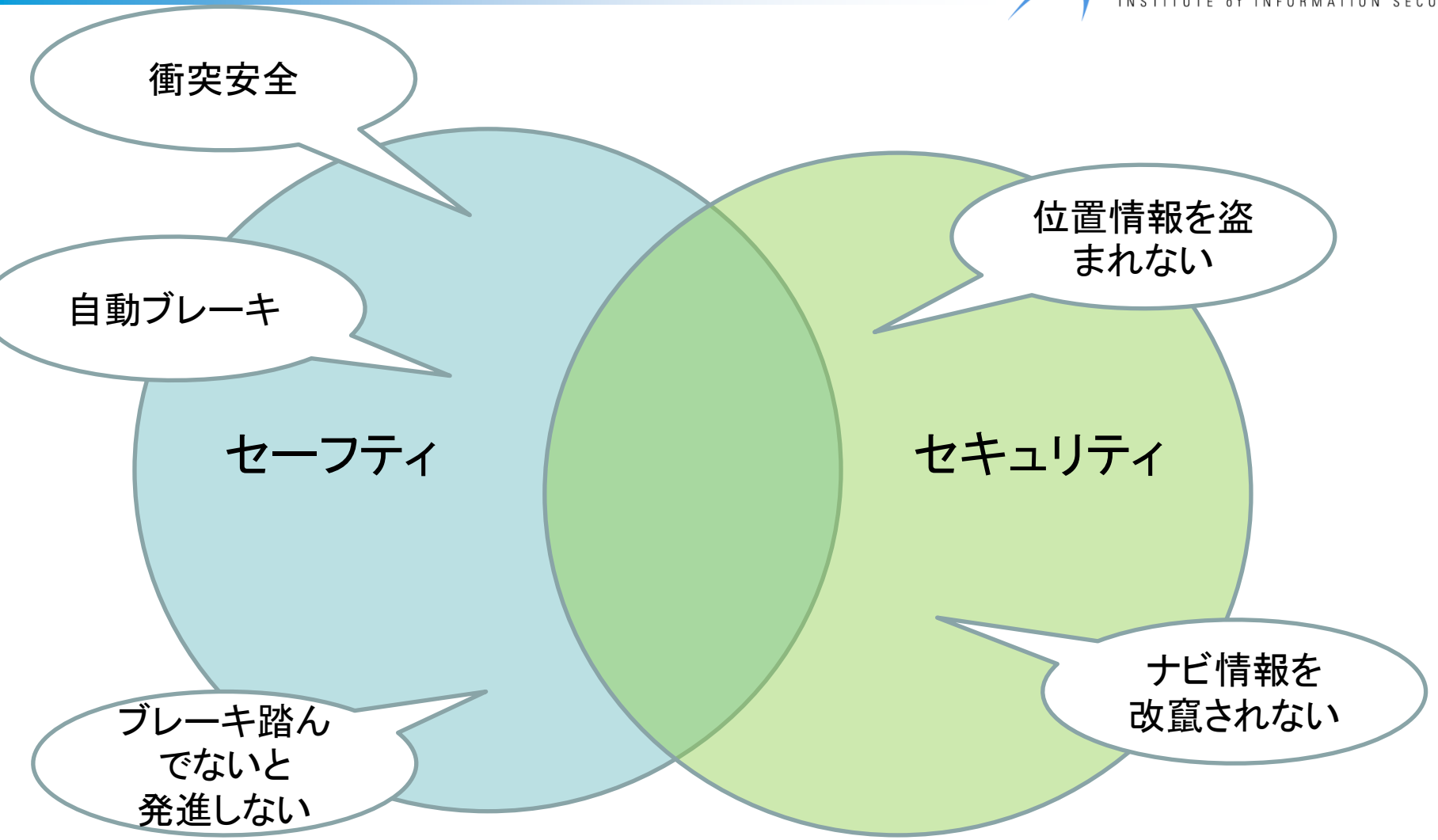
衝突安全

位置情報を盗まれない

自動ブレーキ

ナビ情報を改竄されない

ブレーキ踏んでないと発進しない


衝突安全
自動ブレーキ
セーフティ
ブレーキ踏んでないと発進しない
位置情報を盗まれない
セキュリティ
ナビ情報を改竄されない

「情報セキュリティ」に足りないもの

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 物理的安全（特に人命）を資産として考える
- 人命に対する脅威を最優先
- コンプライアンス：製造物責任法(PL法）

「セーフティ」に足りないもの

- 「悪意」「故意」という観点
  ⇒多重故障、フェールセーフでは守れない？
- 情報資産に対する脅威がもたらすもの
- 安全性優先の結果、それ以外の脅威が軽視される可能性
  最終的にエンジン停止すれば安全確保できる
  ⇒でも、攻撃により頻繁に停止してしまったら？
- 安全性の基盤であるソフトウェアの置きかえ
  ⇒前提が崩れないか？
  来るべき信号が来ないことへの対応⇒〇
  偽の信号が来たら⇒？
- 安全性の最後の責任を人に帰着する
  異常があったら警告灯表示
  ⇒では、改ざんにより警告灯が出ないようにされたら？

安全性

- 本質安全(Inherent Safety)
  根源からリスクをなくして達成される安全
- 機能安全(Functional Safety)
  - 機能による安全
    機能を導入し、許容できるレベルの安全を確保する
  - 機能の安全
    機能が故障しない、あるいは壊れても安全を確保できる

情報セキュリティ

- 「情報資産」が中心
  - 個人情報、機密情報
- 情報セキュリティのCIA
  - 機密性、完全性、可用性
- CIAに対する脅威
  - 盗聴、改竄、DoS攻撃…

まとめ

- 脅威の詳細化や手段は共通化可能なものも
- 情報セキュリティと制御系では重要視する資産が異なる
- 安全性とセキュリティは共通する部分もあるが、それぞれのゴールが一致しない場合もあるため、双方の観点での分析が必要
- 従来のDFD分析だけでは、情報不足の場合がある。またソフトウェアの書換えによりフローが変わる可能性も

明日の信頼を創ろう。

情報セキュリティ大学院大学

INSTITUTE of INFORMATION SECURITY

http://www.iisec.ac.jp