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

ソフトウェアの脅威分析
－開発ライフサイクルの観点から－

情報セキュリティ大学院大学
大久保 隆夫

自己紹介

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

- 大久保 隆夫
- ～2013年 (株)富士通研究所 セキュアコンピューティング研究部に勤務
- ソフトウェア工学、Webアプリケーションセキュリティ、セキュリティ要求分析の研究に従事
- 2006～2009年 本学博士後期課程
  博士（情報学）学位取得

自己紹介（続き）

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

- 2013年 本学に准教授として赴任
- 専門研究テーマ
  - セキュリティ＋ソフトウェア工学
    いかに安全なソフトウェアを作るか
  - セキュリティ＋プライバシー分析
  - 要求＋運用＋マネジメント分析
  - 攻撃技術に関する研究
  - アプリケーションセキュリティ、Webセキュリティ
  - モバイルセキュリティ、HTML5セキュリティ

24-twenty four-

- Counter-Terrorism Unitとテロの戦い
- 暗号解読(blowfish)
- インフラ(通信、交通、電力網)への攻撃
  - 防護ファイアウォール無効化
  - 航空管制センターの通信システムに侵入
    3000機の飛行機のコントロールを奪う
  - 化学工場へのサイバー攻撃→バイオテロ
- 監視映像の改ざん
- 一度しかダウンロードできないファイル形式？

Stuxnet

- 2010年(24 シーズンVIIは2009年！）
- イランの核施設を標的とした攻撃
- ソフトウェアの脆弱性をついて
  トロイの木馬型ウィルスに感染
- 遠心分離機が稼働不能に

Stuxnet

- 2010年(24 シーズンVIIは2009年！）
- イランの核施設を標的とした攻撃
- ソフトウェアの脆弱性をついて
  トロイの木馬型ウィルスに感染
- 遠心分離機が稼働不能に

自動車のセキュリティ

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

- 近年注目されている
- マルウェアのインストール
- 制御系に対する攻撃
- 位置情報の窃取→プライバシー問題

Software everywhere!

ソフトウェアのセキュリティ確保

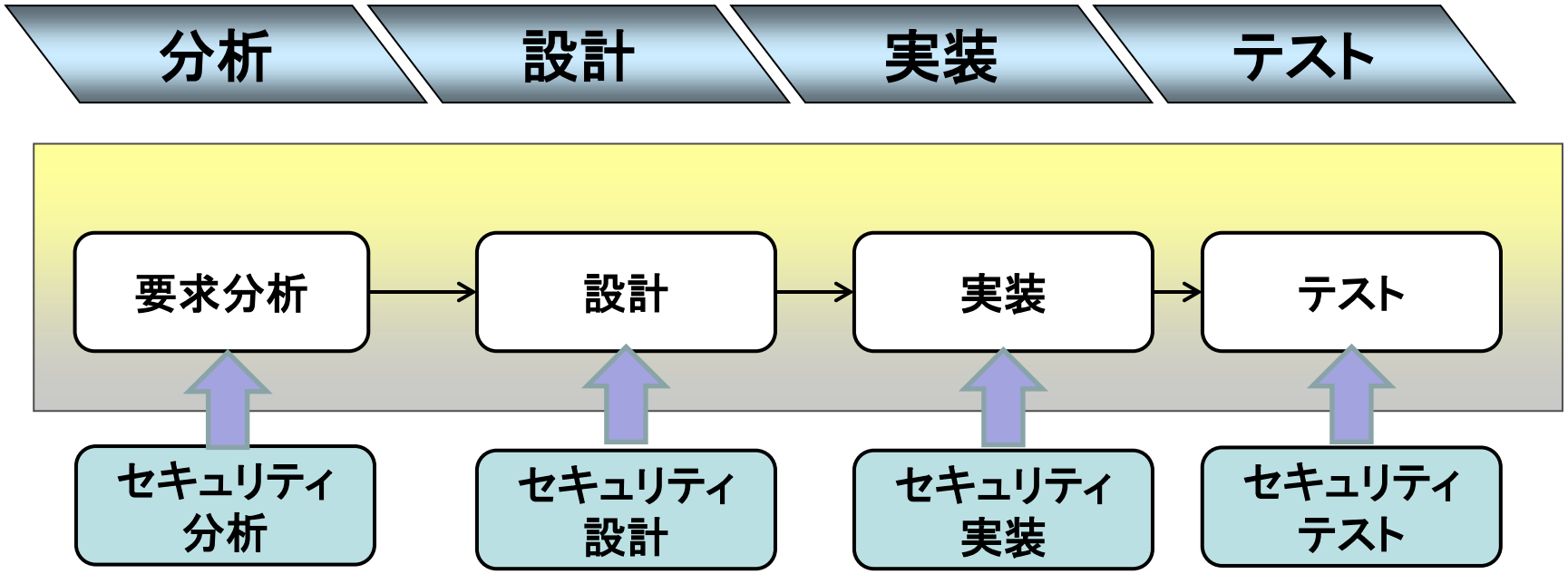
- 脆弱性をなくす
  - 脆弱性：障害のうち、攻撃によって意図しない挙動をしてしまう弱さ
- 脆弱性をなくすには、開発の早期段階からの分析、排除が必要

脅威分析：従来分析との相違

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

- ステークホルダ観点のみでは実現できない
  ＝攻撃者観点の要求を想定し
  →攻撃者の要求を実現できないように
  開発
- 上記について、知識、ノウハウがないと観点漏れで脆弱性のあるソフトウェアになる
- 「できるだけ」網羅的な脅威抽出が必要

開発ライフサイクルとセキュリティ



セキュリティ要求分析

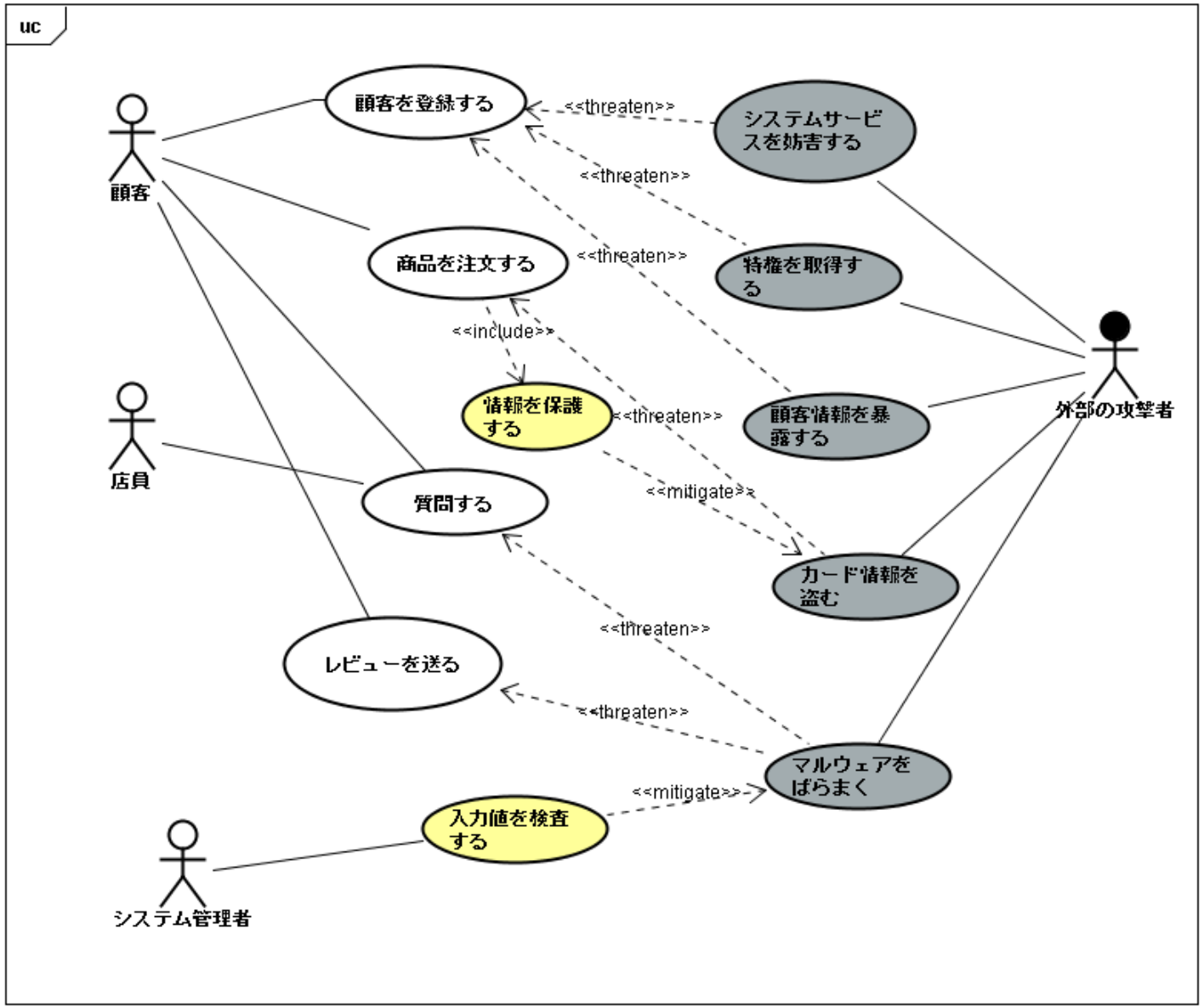
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- ソフトウェア工学的手法
  - ゴール指向分析(GOA)
  - エージェント指向：i*、Secure Tropos
  - 問題フレーム
  - UMLの拡張
- セキュリティに特化した手法
  - CC(ISO/IEC 15408)
  - SQUARE

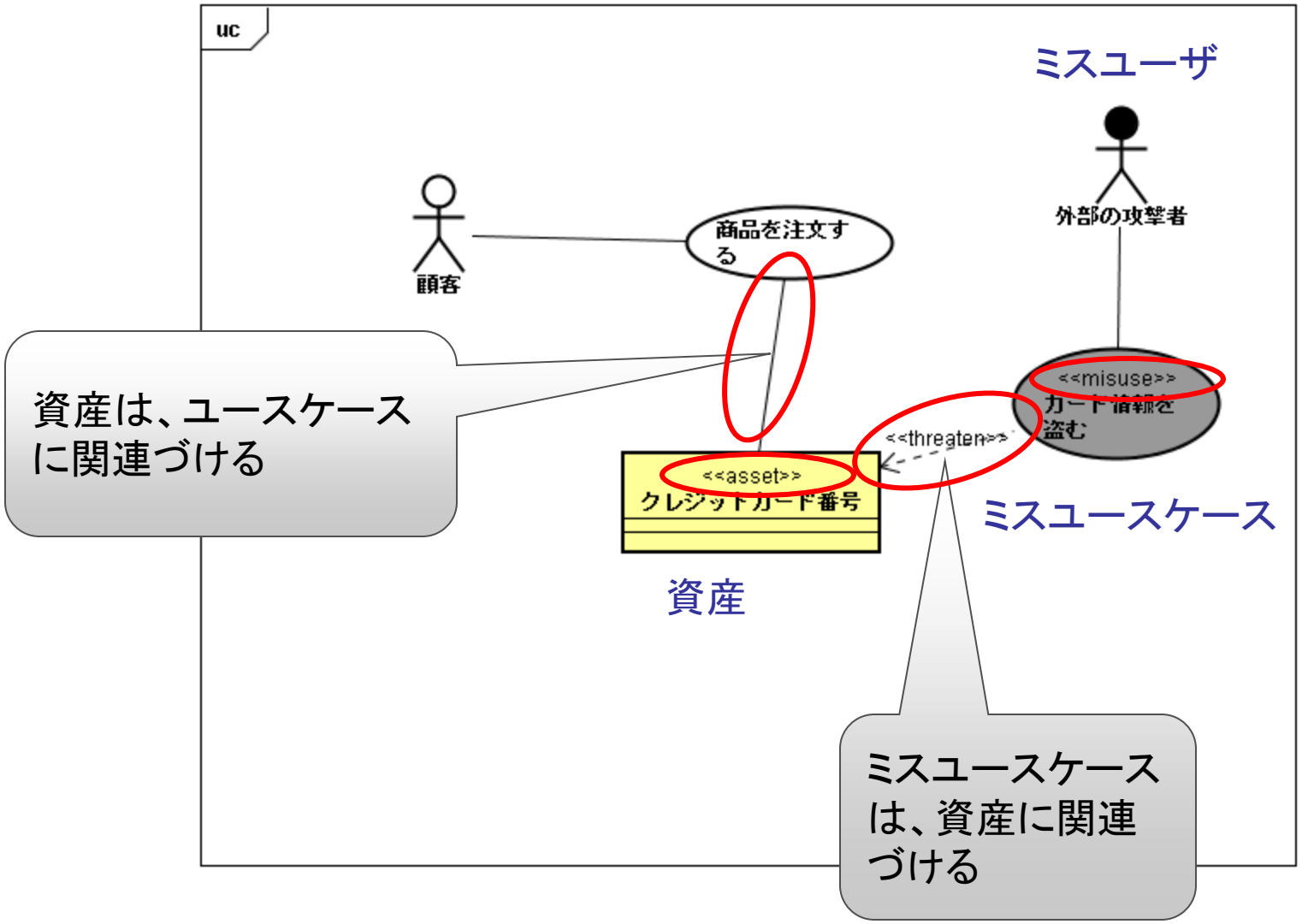
要求分析手法

- ミスユースケース: UMLの拡張
- →資産、セキュリティゴールを意識した拡張：MASG(大久保、田口、吉岡モデル）

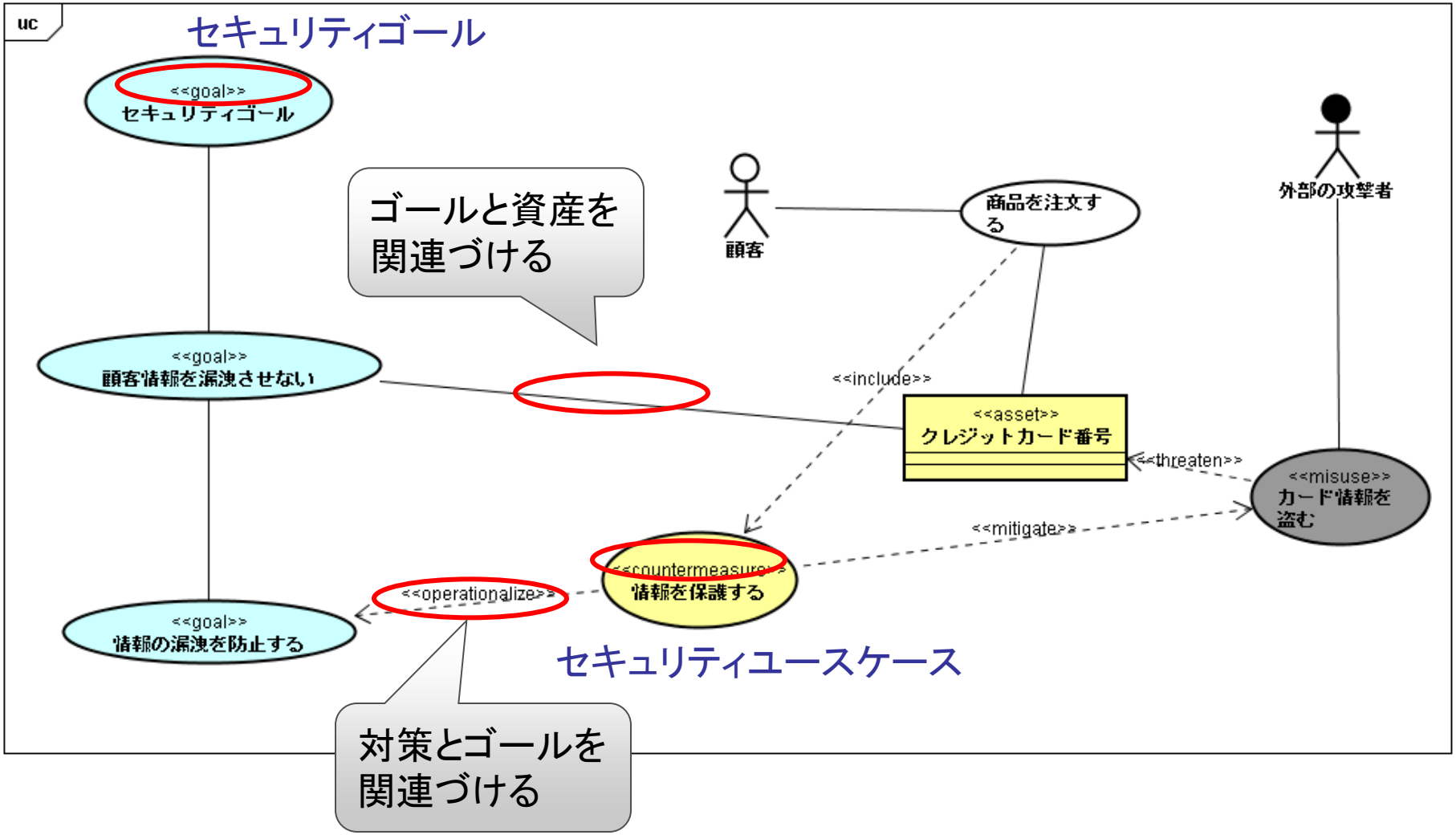
セキュリティユースケースの



MASG (1)


uc
ミスユーザ
外部の攻撃者
顧客
商品を注文する
<<misuse>>
カード情報を盗む
<<threaten>>
<<asset>>
クレジットカード番号
ミスユースケース
資産
資産は、ユースケースに関連づける
ミスユースケースは、資産に関連づける

MASG (2)


uc
セキュリティゴール
<<goal>>
セキュリティゴール
ゴールと資産を
関連づける
顧客
商品を注文する
外部の攻撃者
<<goal>>
顧客情報を漏洩させない
<<include>>
<<asset>>
クレジットカード番号
<<threaten>>
<<misuse>>
カード情報を
盗む
<<mitigate>>
<<countermeasure>>
情報を保護する
<<operationalize>>
<<goal>>
情報の漏洩を防止する
セキュリティユースケース
対策とゴールを
関連づける

セキュリティ設計

- 脅威分析
- セキュリティ設計
  - セキュリティパターン
- 検証
  - 形式検証・モデル検査

脅威分析

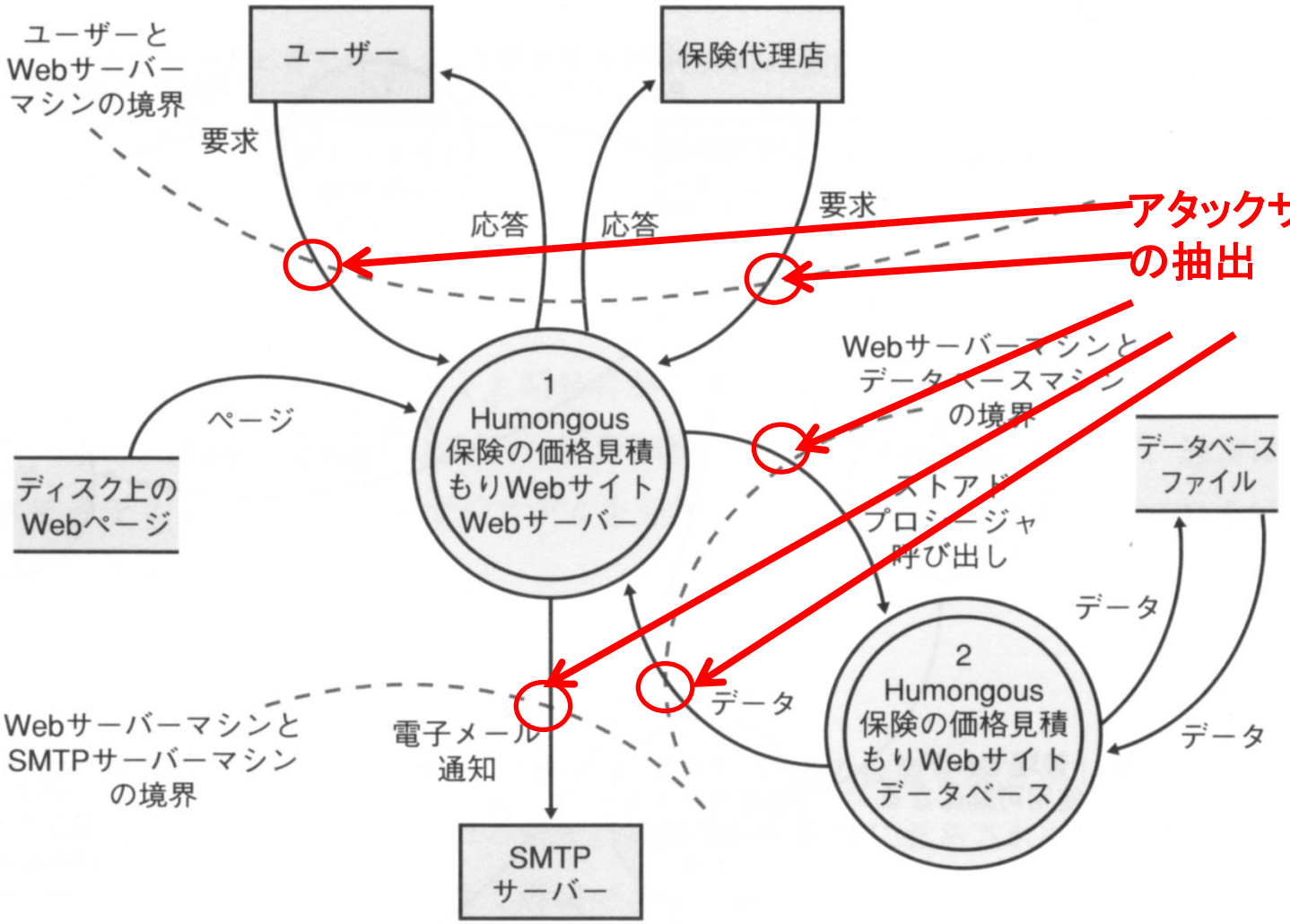
1. 資産の識別
2. セキュリティ目標の決定
3. 脅威の識別
4. 脅威のリスク評価
5. 対策決定

脅威モデリング

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

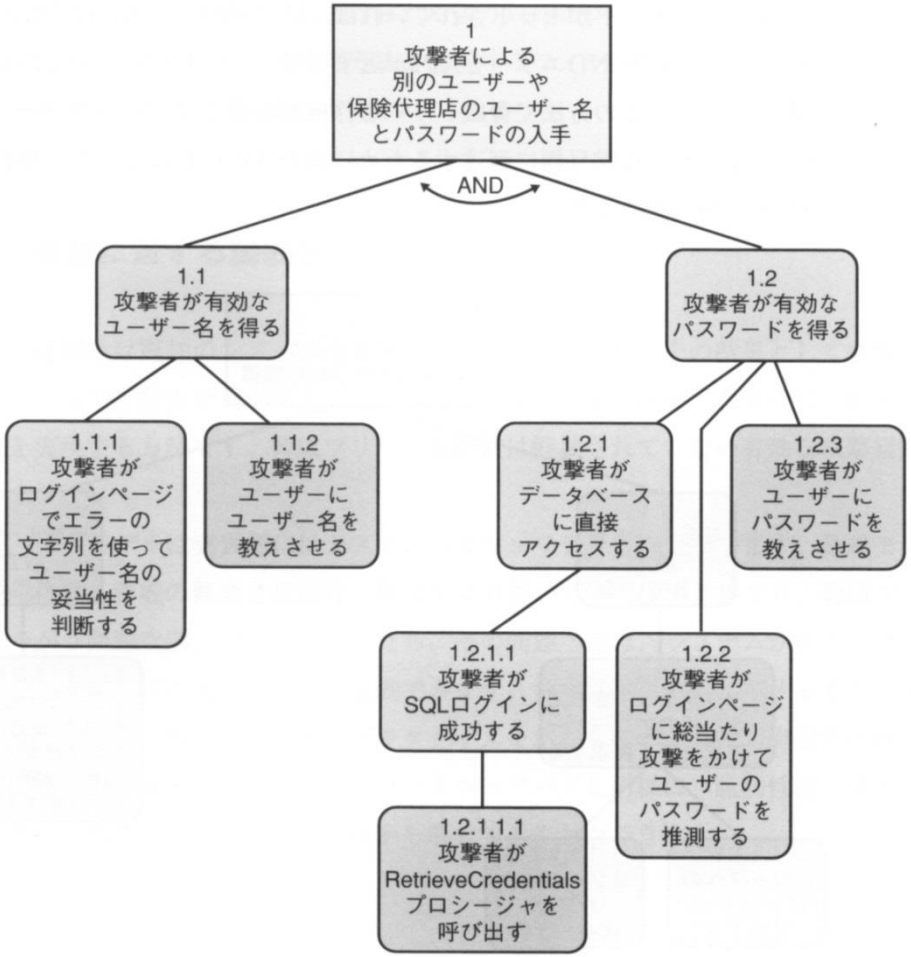
- 設計したシステムにおける脅威分析(脅威の抽出、評価)を行う手法
  - Data Flow Diagram(DFD)を用いた脅威抽出
  - STRIDEによる脅威分類
  - 脅威ツリー、DREADによる脅威評価
- アーキテクチャが明確なとき、脅威抽出の手法としては有効
- 対策抽出は行わない

DFD



出典：Swiderski et.al. writing secure code(上)

脅威ツリー



出典：Swiderski et.al. writing secure code(上)

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)

まとめ

- セキュリティ脅威分析手法をご紹介
- 一般の開発観点とは異なる
  悪意を想定した分析、設計が必要
- ソフトウェアのセキュリティ
  - 大まかな概念としては共通
  - 今後は、広範囲の分野を考慮していく必要
    インフラ、制御系など

明日の信頼を創る情報セキュリティ人材を育成します

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

学長　田中英彦

- 本学は2004年に開学し、新しい学問の体系化と専門家の育成を旗印に、情報セキュリティ専門の独立大学院として教育と研究に携わってきました。
- 2012年度までに、修士226名、博士21名の修了生が巣立ち、それぞれの所属組織において情報セキュリティに関する中核的業務を担っています。
- 本学はこれからも、様々な分野の意欲的な学生を受け入れ、「明日の信頼を創る」高度な情報セキュリティ専門人材の育成に努める所存です

本学の特色

- 情報セキュリティ専門の大学院大学：　修士（情報学）　博士（情報学）
- 技術・管理・法制、セキュリティ総合教育のカリキュラム
- 将来のCIO/CISOを育成する実務指向教育と深い専門研究成果の蓄積
- 横浜市神奈川区鶴屋町2-14-1（横浜駅きた西口徒歩1分）

育成する人材像と修士課程コース

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

［技術系］
エンジニア、システムコンサルタント
を目指す方

暗号テクノロジコース（CT）

法とガバナンスコース（LG）

システムデザインコース（SD）

セキュリティ／リスクマネジメントコース（MS）

［マネジメント系］
セキュリティマネージャー、ビジネスコンサルタントを目指す方

＜修了後の進路 ・ 企業派遣の社会人＞
情報通信／情報サービス／SIer／メーカー／セキュリティベンダー／シンクタンク／コンサルティングファーム／金融／流通／新聞・出版・印刷／教育・研究機関／調査機関／官公庁、博士後期課程進学 など
（2012年度までに修士226名、博士21名の修了生）