GRACE

CENTER FOR GLOBAL RESEARCH IN ADVANCED SOFTWARE SCIENCE AND ENGINEERING

セキュリティとコンピュータ ―攻撃に強いソフトウェアをいかにして作るか？―

国立情報学研究所 吉岡信和

2009年6月11日（木）

平成21年度市民講座「社会を変える情報学」

セキュリティとコンピュータ：攻撃に強いソフトウェアをいかにして作るか？

- セキュリティの重要性
  - 生活密着型情報インフラ vs. ネット被害の拡大
    - ▶ 安心して便利な機能が使えない！
- セキュリティとは？
  - 意図した攻撃への防御
- セキュリティの特徴
  - 被害にあわないと対策の効果が分からない！（パラドックス）
- 攻撃に強いソフトウェアを作るには？

ソフトだけど強い！？

まず相手を知り、身の程を知る
  - 知彼知己百戦不殆：彼を知り己を知れば百戦して殆（あや）うからず（孫子）
  - ➡ 価値のあるサービスに大きな被害が起きないように対策を講じる
- ソフトウェアの強さを保証する（特別講師：みずほ情報総研 金子浩之）
  - 強さの範囲を明らかにし、第三者が確認
- セキュリティの今後
  - さまざまな専門家が一致団結して、攻撃に立ち向かう必要がある！

ネット社会の光と影：生活への浸透

情報通信技術が生活基盤の一部に

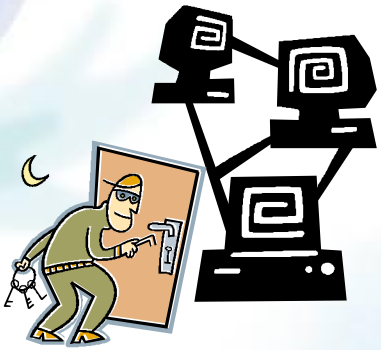
- ビジネスでの活用
  - オンライントレード
  - 受発注
- 生活に密着したサービスの普及
  - オンラインショップ
  - お財布携帯
  - ネットバンク
  - コンテンツ配信

➡ 生活はますます便利に

➡ デジタルの価値が向上

ネット社会の光と影：ネット被害の拡大

- コンピュータウイルスの蔓延
  - スパイウェアなどにより、個人情報の流出
- 迷惑メールの蔓延
  - 読みたいメールより迷惑メールの方が多い！
- Webサーバへのアタック
  - 個人情報を盗むホームページ（フィッシングサイト）に差し替えられる！
  - 迷惑メールの踏み台サーバにされてしまう！
- 全世界から攻撃される可能性：ネット社会に国境はない



➡ 被害が社会問題まで発展
  - 規模・額が年々増大
  - 社会活動が脅かされる

➡ セキュリティ対策は面倒・不便
  - ウイルス対策ソフトなしにはパソコンが使えない！
  - ウインドウアップデートがわずらわしい
  - 重要なメールが迷惑メールボックスに入っていた！

例）MasterCardのクレジットカード情報が流出

MasterCard Internationalは6月17日、各種ブランドの**4000万枚以上のクレジットカード情報が流出**し、不正利用される可能性があると明らかにした。この中にはMasterCardブランドのカード約1390万枚が含まれ、同社から加盟金融機関に連絡を取っているという。

同社の調べによれば、金融機関などからカード決済を請け負っているサードパーティーの決済処理会社米CardSystems Solutionsから情報が流出した。同社のシステムの脆弱性が原因で、**ネットワークに不正侵入され、カード情報にアクセス**された。

MasterCardでは司法当局にも通報して調査を進め、CardSystemsのシステムの脆弱性に対処、セキュリティ強化措置を講じたとしている。

記事：ITmedia 2005/06/18
http://www.itmedia.co.jp/enterprise/articles/0506/18/news008.html

例）ウイルス仕掛けネット預金９００万円詐欺

他人の銀行口座の**個人情報をもとにインターネットバンキングにアクセス**し、**預金を移し替えて約900万円をだまし取った**として、警視庁築地署は、容疑者（37）＝詐欺罪で公判中＝を不正アクセス禁止法違反と電子計算機使用詐欺の疑いで再逮捕したと26日発表した。・・・

同署によると、容疑者は昨年1月、東京都中央区の男性会社員（36）の**ネットバンク口座に不正にアクセス**し、実在する他人の身分証明書を使って開設した**架空口座に約900万円を移し替えた**疑いがある。複数の架空口座に移動させながら、金を引き出したという。
勝手に口座に名義を使われた人の自宅からはパスポートや健康保険証などの**身分証明書が盗まれ**ていたという。容疑者は「被害者らの自宅に侵入し、一部の人のパソコンに『バグベア』と呼ばれる**ウイルスを仕掛けた**」などと供述しているという。
バグベアはパスワードなどの個人情報を収集し、特定のアドレスにメール送信するウイルスで、同署は、容疑者がこれを使って**個人情報を入手**したとみている。

記事：朝日新聞 2009年1月26日

生活密着型情報インフラ vs. ネット被害の拡大

便利な機能を**便利に使える**ようにする必要がある

便利 ⟷ セキュリティ

悪用　安全　安心

被害　攻撃　使いづらい

面倒

怖い　リスク

コスト

便利と安全のバランスが取れたセキュリティが重要

セキュリティとは？

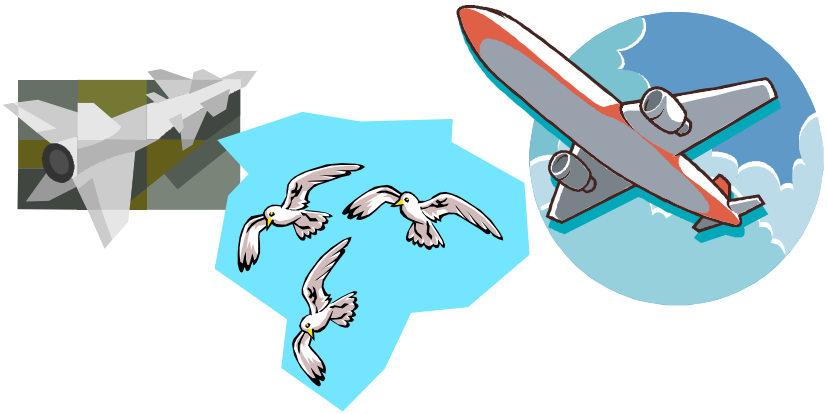
- 広辞苑の定義
  安全、保安、防犯
- コンピュータセキュリティ（ウィキペディア（Wikipedia））
  1. コンピュータを災害、誤用および不正な利用からコンピュータシステムを守ること
  2. ハードウェア、ソフトウェア、データのいずれについてもその機密性、完全性、可用性を維持すること
- セキュリティ工学分野におけるセキュリティの定義
  - 悪意のある攻撃、およびその被害からシステムを守ること

※災害、誤用は、セキュリティ技術の範囲外⇒セーフティとして扱う
※悪意があるないにかかわらず同じ被害をこうむる可能性がある
⇒ 同じ技術で対策できる可能性がある

参考：セキュリティとセーフティ

ハドソン川の奇跡

被害：バードストライクによる墜落



セキュリティ工学の範囲

ミサイルの到達区域を想定

セーフティ工学（安全工学）の範囲

鳥の群生区域を想定

想定範囲が異なる

セキュリティは目的ではない

【セキュリティの特徴】

- それ単独で**価値のある機能・サービスではない**
  - 使いたい機能・サービスを安全にするために存在
    例）ウイルス対策ソフトだけを使いたい人はいない
  - 価値のあるものを攻撃から守ってくれる
    例）個人情報が盗まれるのを守ってくれる
  - なくても困らないことがある
    例）ウイルスがいなければウイルス対策は不要
    例）個人情報を入力しなければ守る必要もない！
- 被害にあわないと**効果が分からない！（矛盾：パラドックス）**
  - セキュリティは、被害をなくす、もしくは最小限にとどめる（**リスク回避**）手段
    セキュリティを強化する ⇒ 被害がなくなる ⇒ セキュリティの効果が体感できない！
    ➡セキュリティは不要と**錯覚**

➡**起きないこと**に対して対価を支払う

参考：保険は、起きた被害を最小に食いとどめる

➡ **セキュリティの必要性が理解しにくい**

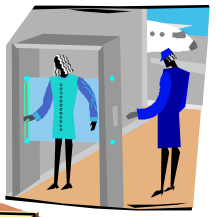
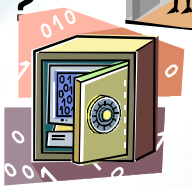
セキュリティの難しさ

- 考慮する範囲が広い
  - さまざまなことを考慮する必要がある
  - サービスの中だけではなく、それがおかれている状況も重要
- 完璧な安全はない
  - セキュリティと利便性はバランスが大事（トレードオフ）
- セキュリティはタダではない
  - セキュリティ強化にはコストがかかる
  - 起こりえる被害を優先して考慮する必要がある
- 漏れ・抜けにより被害が拡大
  - もっとも脆弱な部分（セキュリティホール）が狙われる
  - セキュリティ機能の使い方を間違えると標的になる

セキュリティは考慮する範囲が広い

- さまざまなことを考慮する必要がある
  - どのサービスが攻撃されるのか？何を守るべき（資産）なのか？
    例）ネット振込みサービスが攻撃、口座情報を守る
  - サービスに対してどんな攻撃がありうるのか？どんな被害があるのか？
    例）振込先情報の書き換えられ、預金を失う
  - どういう方針（ポリシー）で守るのか？
    例）利用者以外には口座番号は閲覧・変更できない運用にする
  - サービス・機能をどのように守る（対策する）のか？
    例）本人でないと振込みサービスが使えない、口座情報が見えない
  - 対策には、どういうセキュリティ機能をどこで使う必要があるのか？
    例）振込みサービスを使う前に本人を認証し、口座情報を暗号化する



- サービスの中だけではなく、それがおかれている状況も重要
  - 振り込みサービスが窓口で使えるのか、コンビニATMで使えるのか、パソコンで使えるのか、携帯で使えるのかで状況がまったく異なる


強盗

おれおれ詐欺

盗難

スパイウェア

完璧な安全はない

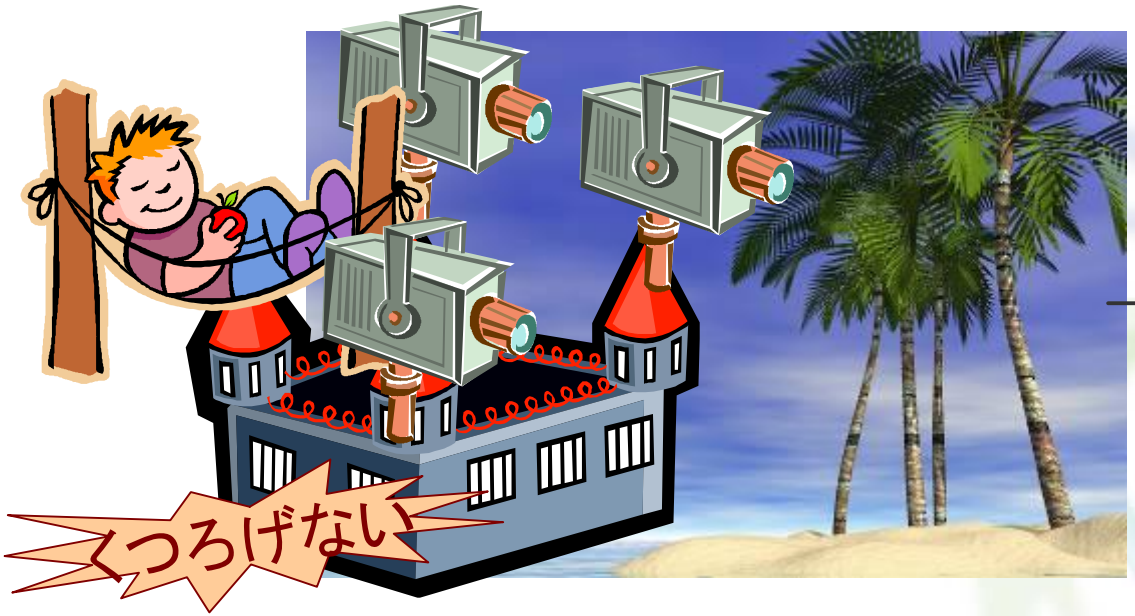
- あらゆる攻撃を守ることは**不可能**
  - 自分以外誰も信じないで、社会活動は成立しない
- ありとあらゆる不安を取り除くことが目的ではない
  - あくまで便利な**サービスを使うことが目的**
  - セキュリティの強化は利便性を下げる

例）携帯を守るために金庫に入れて持ち歩いていては不便！

例）個人情報流出させないためにノートパソコンの持ち歩きを禁止すると
せっかくの利便性が活用できない

➡ **セキュリティと利便性はバランスが大事（トレードオフ）**

セキュリティと利便性はトレードオフ



リゾート別荘の強固な塀と監視カメラ

観光に妨げ

重装備な観光旅行

ヘルメット＆マスク

防弾チョッキ

動きにくい！
警察にとめられる！

【適切なセキュリティ】
内ポケットに必要なお金だけで十分

セキュリティはタダではない

- セキュリティ強化にはコストがかかる
  - 分析コスト、対策コスト、保証コスト、運用コスト
    万里の長城：280年で8851キロ
  - サービス実現にプラスのコスト：可能な限り低くしたい

➡ 起こりえる大きな被害を優先して考慮する必要がある
  - めったに起こらず被害も少ないセキュリティにコストをかけたくない

例）洪水がこれまで起こったことがない川の治水工事、ダム建設は不要！
土砂崩れの危険レベルの高い斜面の補強工事を優先すべき！

漏れ・抜けにより被害が拡大

- もっとも脆弱な部分（**セキュリティホール**）が狙われる
  システムのセキュリティレベルはもっとも脆弱なレベルと同等

万里の長城：しばしば関守が買収されて開門

正面が重厚でも勝手口が狙われる
例）メンテナンス用機能が狙われる

- セキュリティ機能の**使い方を間違える**と標的になる

例）ログインパスワードをディスプレイに張る
IDとパスワードを同じにする

セキュリティを考える上でのポイント

- セキュリティの考慮・**保証範囲**を明確にする
  - どこまでの被害を防ぐか？
  - **最小限のコスト**で最大限のサービスを提供
  - 被害の分析、要求の優先付けが重要（**セキュリティ要求工学**）
- 想定した範囲で**もれ・抜けがない**ようにする
  - 対策は**十分**か？漏れがないか？
  - セキュリティの**要求**を満たしているか？
  - **想定したセキュリティレベル**は保たれているか？

➡ これらを保証するための技術（**セキュリティ工学**）が必要

攻撃に強いソフトウェアを作るには？

中国の春秋時代の武将、孫武

まず相手を知り、身の程を知る

知彼知己百戦不殆：

彼を知り己を知れば百戦して殆（あや）うからず（兵法書『孫子』）

相手を知り、身の程を知る

- 攻撃者・攻撃を知る
- リスクを知る

⇔

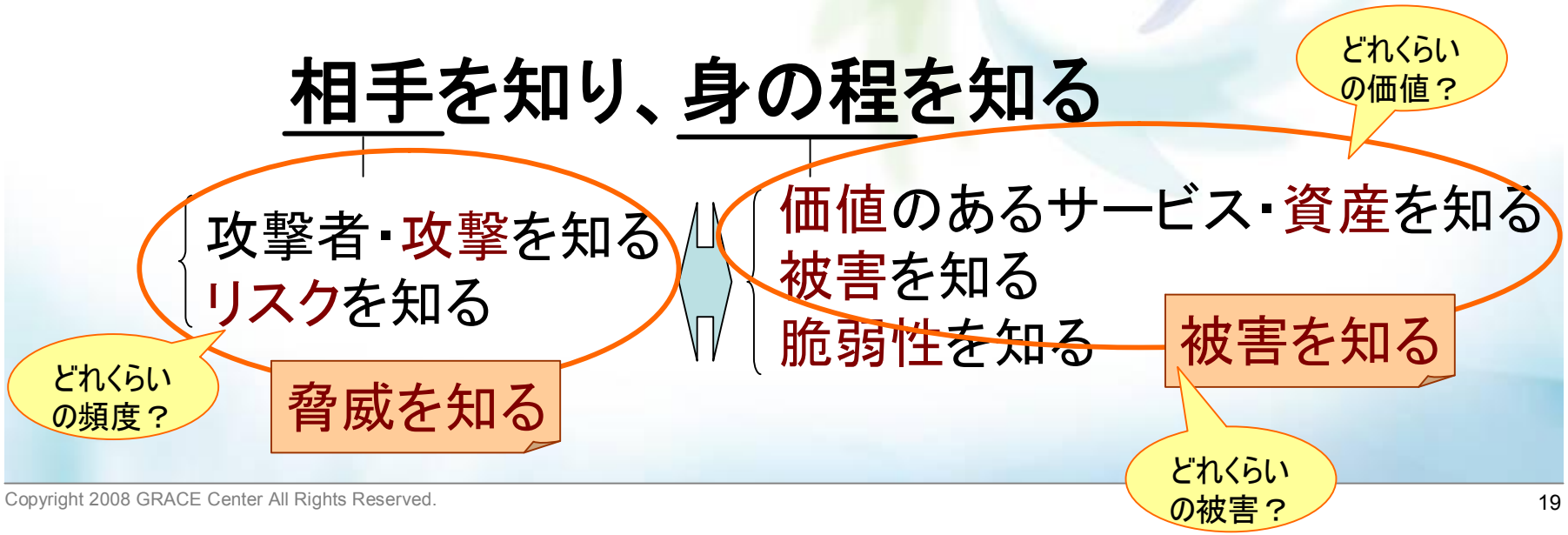
- 価値のあるサービス・資産を知る
- 被害を知る
- 脆弱性を知る

価値のあるサービスに大きな被害が起きないように対策を講じる

セキュリティの考慮・保証範囲を明確にする

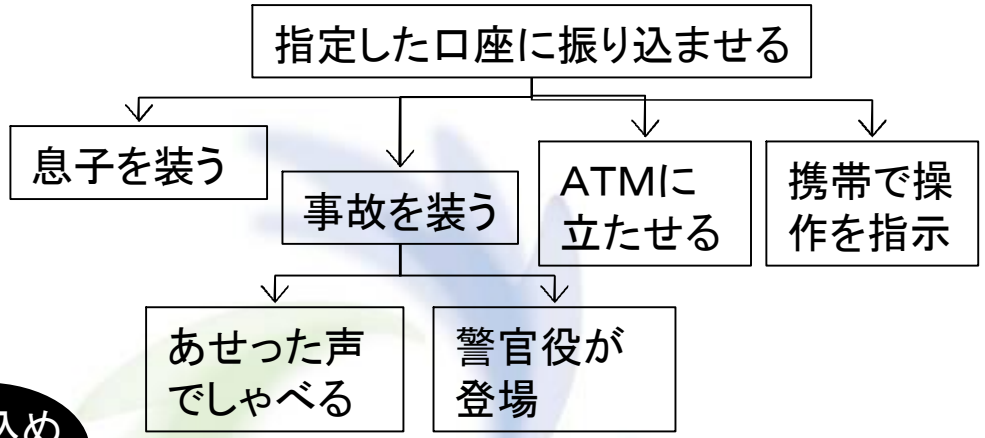
脅威に基づく分析が有効

- 脅威のない対策は不要
- 対象とする脅威が明確になれば、対策範囲も明確になる
- 対象とする脅威は？
  - 被害が大きく、起こりえる脅威を優先
  - 最小限のコストで最大限のサービスを提供

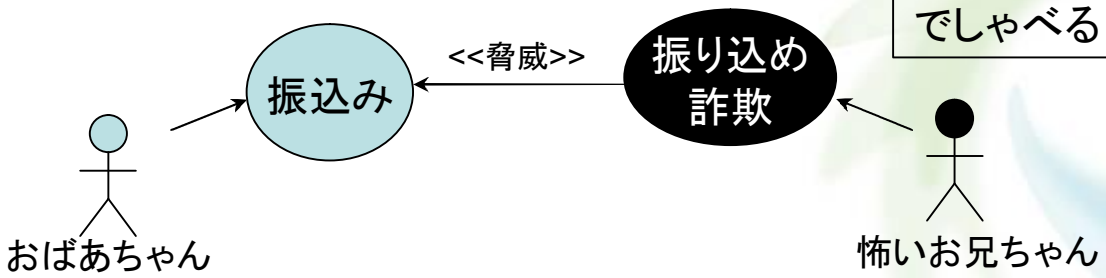


脅威と被害を分析する技術

- **攻撃ツリー**
  - 木構造で攻撃の詳細をブレイクダウン
  - 実際にありえる攻撃かを評価
  - 対策方針に利用



- **ミスユースケース**
  - 攻撃やその状況をモデル化（図示）



- **被害の分析手法:**
  - FMEA（Failure Mode and Effect Analysis）
    - 故障形態、その影響、程度、頻度、検出しやすさで数値で表現、重要度をランク付け

例）
振り込み詐欺、振込み機能の悪用、影響：大†、しばしば、あとで発見 ⇒ 重要度：大
携帯盗難、お財布機能の悪用、影響：大、しばしば、すぐ発見 ⇒ 重要度：大

†平成20年中の被害件数は3,718件、被害総額は約60億円

脅威分析の難しさ

- 起こっていない脅威を見つける難しさ
  - 攻撃される前に防御する必要がある！
- ネット社会では、攻撃者は不特定
  - 戦っている特定の相手がいるわけではない！
- 完璧な脅威分析はありえない
  - 常に新しい脆弱性と攻撃方法が考案される（セキュリティには寿命がある！）
  - 見つかった新たな攻撃はすぐに真似される

➡ 蓄積された最新のセキュリティ情報の有効利用

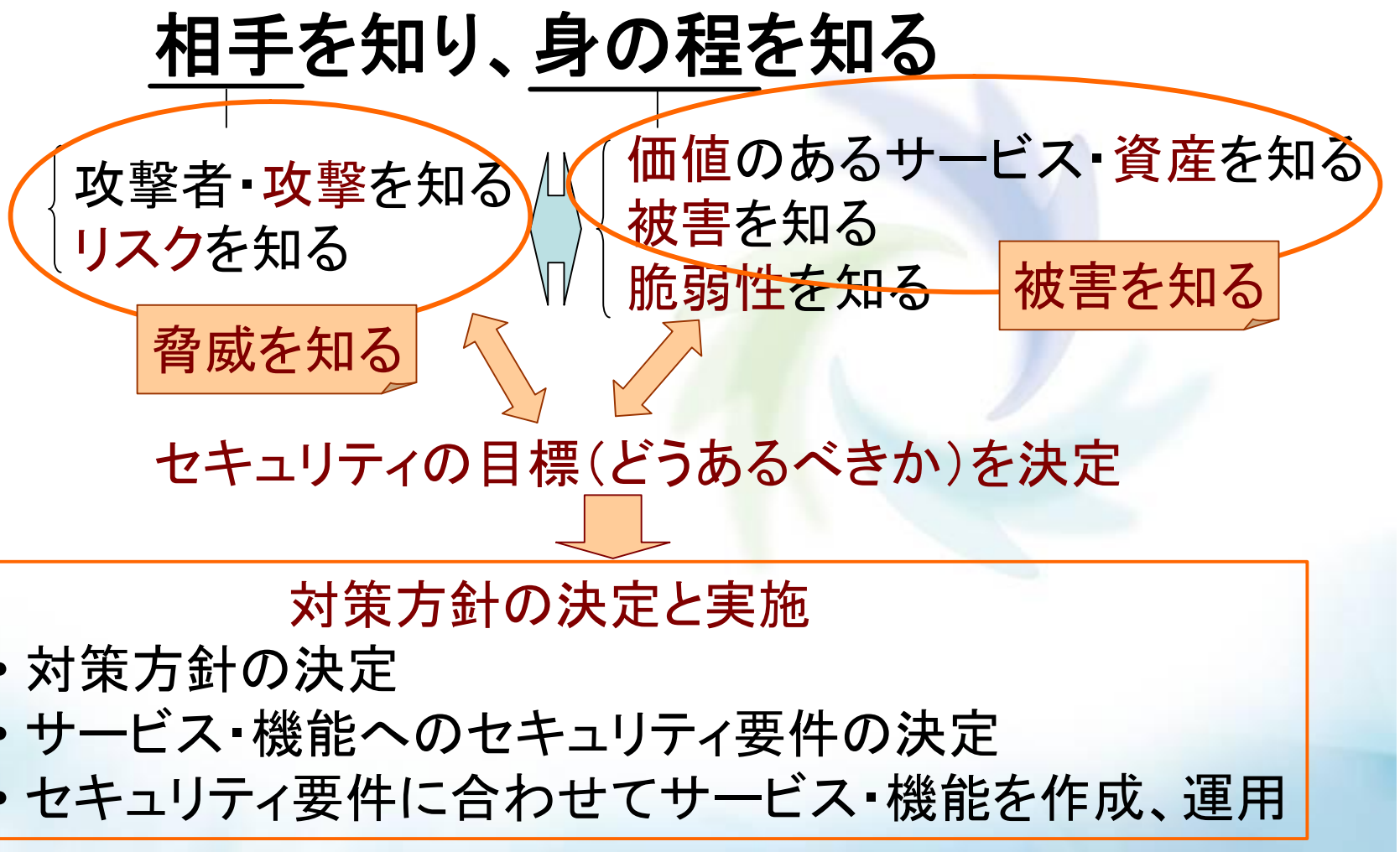
セキュリティ情報（インシデント情報）の蓄積・再利用が重要

➡ カタログ化・パターン化による再利用

典型的な攻撃は参考にしやすい形式でカタログ化

例）ネット情報の盗聴のパターン、ホームページ上の個人情報の取得パターン

大きな被害が起きないように対策を講じる



セキュリティ目標を定める

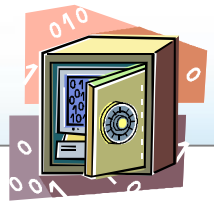
価値のあるサービスや資産が持つべき性質が成り立つことをセキュリティの目標とする

- 機密性
  - 限られた人・組織のみが閲覧、書き換えなどが出来ること
  - 例）口座の情報は本人のみが閲覧できる
- 整合性（完全性）
  - 情報が変化せずに完全に保たれている状態で、その情報をだれがいつ作成、変更したかを同時に証明できるようにすることが多い
  - 例）口座に振り込んだ額は、後日変化しない
- 可用性
  - 必要な時に必要な情報・サービスが利用可能になっていること
  - 例）24時間ネットで振込みが可能

※ この他にも、プライバシーやアカウンタビリティ（説明責任）をセキュリティの目標とすることもある

対策方針の決定と実施

- どのように対策を行うかの大まかな方針（対策方針）を決定
  例）本人でないと振込みサービスが使えない、口座情報が見えない
- サービス・機能が満たすべきセキュリティ上の必須条件（セキュリティ要件）の決定
  例）携帯バンクの振込みサービスを利用中は、携帯のIDとパスワードで認証する（システムでの対策）
  例）ATMの振込みサービスを利用中は、携帯の使用を禁止する（運用での対策）
- セキュリティ要件に合わせてサービス・機能を構築、運用
  - セキュリティの機能を使ってサービスを構築
    セキュリティ機能：暗号モジュール、署名モジュール、認証モジュールなど

パターンカタログを使った機能の構築

認証・アクセス制御のためのパターン例：

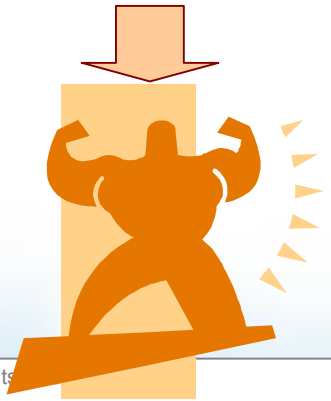
シングルアクセスポイントパターン

- サービス利用の入り口を一箇所に限定する
  - アクセスの制限を簡単に行える（門番を置く）
  - 攻撃されうる箇所を制限して対策を単純化する
- 利便性が損なわれる恐れがある

適用例）
振込み、残高照会、引き落としのどのサービスもログインページからしか辿れない

強いソフトウェア作成レシピ

1. 価値のあるサービス・資産を見つける
2. 攻撃とそのリスクを分析
3. 被害を分析し、対策すべき脅威を決定
4. セキュリティの目標を決定
5. 対策方針の決定
6. サービス・機能へのセキュリティ要件の決定
   システムへの対策、運用での対策、教育による対策などさまざま
7. セキュリティ要件に合わせてサービス・機能を作成、運用



→ 新しい攻撃・脅威・被害を発見

セキュリティの保証

- 対策が要件に合っているか、想定する脅威に対抗できているかを第三者が確認する必要がある
- 想定したソフトウェアの強さを保証する

  解説者：金子浩之（みずほ情報総研）

  - セキュリティを評価・認証する専門家

    これまでさまざまな製品・システムを認定
  - みずほ情報総研は、国に認定された民間評価機関

セキュリティの今後

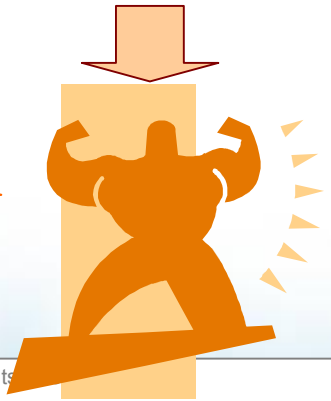
- 一貫した構築手順・ガイドラインの出現と普及
- セキュリティは異分野の協力が必須
  - 経営者、管理職、ソフトウェアエンジニア、ハードウェアエンジニア、暗号の専門家、研究者、教育者、アナリスト、法律家が一致団結して対策すべき
  - ➡ 知識領域も用語も違うなかで、どのように一致団結すべきか？
- 安心の実現
  - 安全性（セキュリティ・セーフティ）の実現と、その信頼性（トラスト）工学の確立
- 快適・エコとの融合

  地球に優しい暮らしやすいネット社会の実現
  - 快適：思ったとおりに振舞う
  - エコ：CO_2の排出が最小になる

セキュリティは異分野の協力が必須

1. **価値**のあるサービス・**資産**を見つける
2. **攻撃**とそのリスクを分析
3. 被害を分析し、**対策すべき脅威を決定**
4. セキュリティの**目標**を決定
5. **対策方針**の決定
6. サービス・機能への**セキュリティ要件**の決定
   システムへの対策、運用での対策、教育による対策などさまざま
7. セキュリティ要件に合わせてサービス・機能を**作成、運用**

経営者
暗号の専門家
エンジニア
法律家
教育者
管理職
認証者



→ 新しい攻撃・脅威・被害を発見

研究者
アナリスト

参考

吉岡信和、田口研治編集、セキュリティ要求工学の実効性、情報処理学会、情報処理、Vol.50、No.3、Mar.、2009