National Institute of Information and Communications Technology

ネットワーク利用における
リスクと対策を可視化する技術

独立行政法人　情報通信研究機構
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室

松尾　真一郎

講演の概要

1. ネットワーク利用におけるリスク
2. リスク評価と対策提示に向けたプラットフォーム
3. 今後の研究課題と方向性

1.ネットワーク利用における**リスク**

（情報でない）セキュリティの身近な例

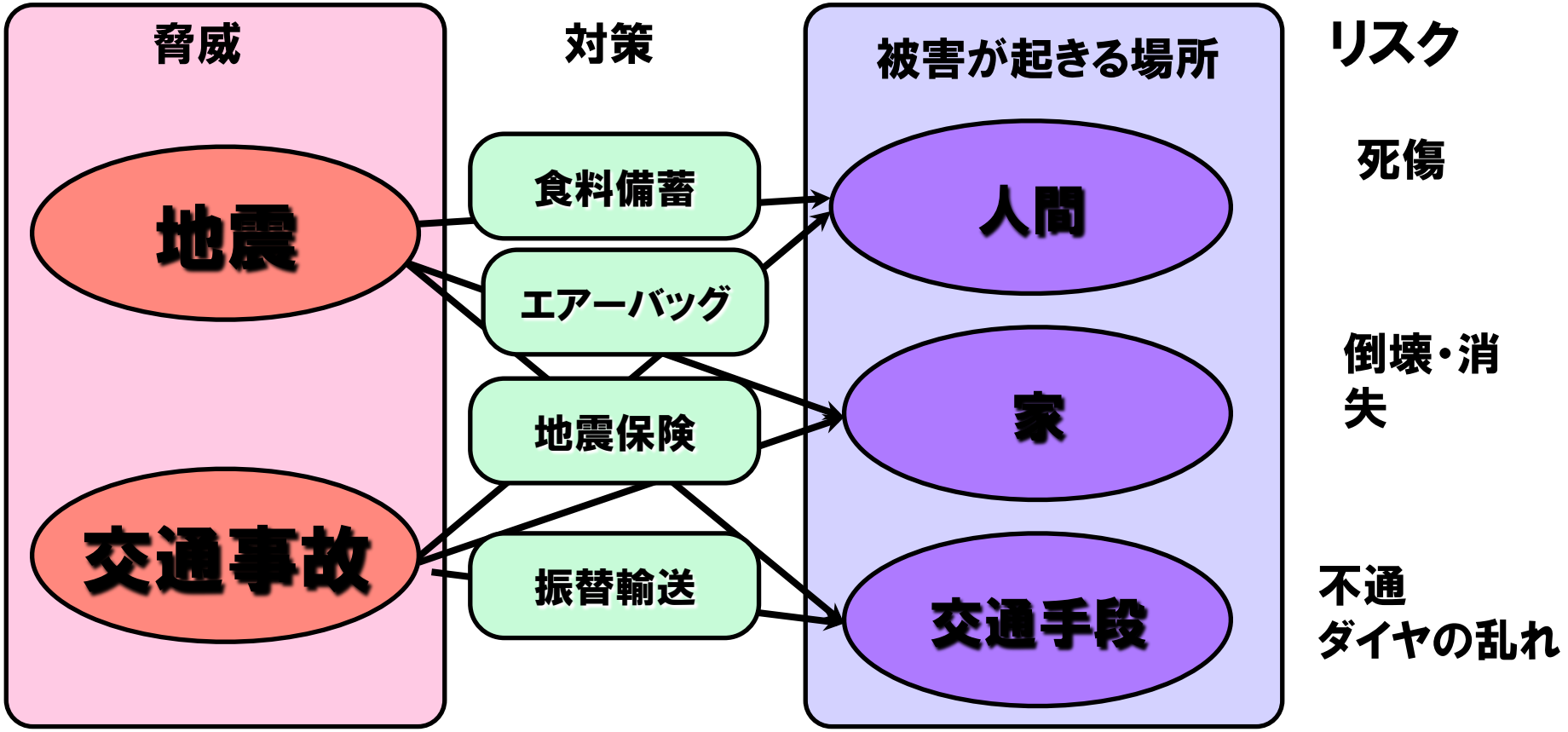
- 交通事故
- 空き巣
- 地震
- 火事
- 病気 …

（情報でない）セキュリティの身近な例 – 交通事故

原因	被害	対策
交差点での衝突	人的被害 自動車・自転車の破損 交通渋滞	信号機 エアーバッグ、ガードレール バンパー、衝撃を抑える設計 カーナビ、交通情報
電車の脱線	人的被害 電車の破損 ダイヤの乱れ	信号機、緊急停止装置、 手動コック 振替輸送
ハイジャック	人的被害 物的被害 金銭・政治的要求への同意	ゲートでのセキュリティチェック 預け荷物のチェック

セキュリティにおける脅威・リスク・対策の関係

- 脅威：セキュリティ上の問題を起こす原因
- リスク：脅威によってもたらされる被害（の定量的評価）
- 対策：リスクを0（あるいは少なくする）ために、脅威を抑える手段



情報に置き換えると…

- 被害が起きる場所
  - 情報
- 脅威（攻撃の手段）
  - ネットワークへの侵入
  - マルウエア
  - 盗聴
  - なりすまし
- リスク
  - 個人情報の流出
  - ID・パスワードが盗まれて、銀行取引をされてしまう
  - サイバー攻撃によるWebサイトの改ざん・サービス停止

情報漏洩リスクの事例

宇治市住民基本台帳データ流出事件（1999年）

- 1999年5月21日、京都府宇治市の住民基本台帳のデータ21万7617件分が、民間業者が持ち込んだMO ディスクによって外部に流出し、名簿業者によってインターネット上で販売された

- 市民による損害賠償請求訴訟の結果、2002年7月11日、最高裁は宇治市の上告を棄却し、宇治市に 1人あたり 1万円の慰謝料の支払いを命じる

- 金銭的リスクは、21億円＋裁判費用
- その他に信用リスク

なりすましリスクの事例

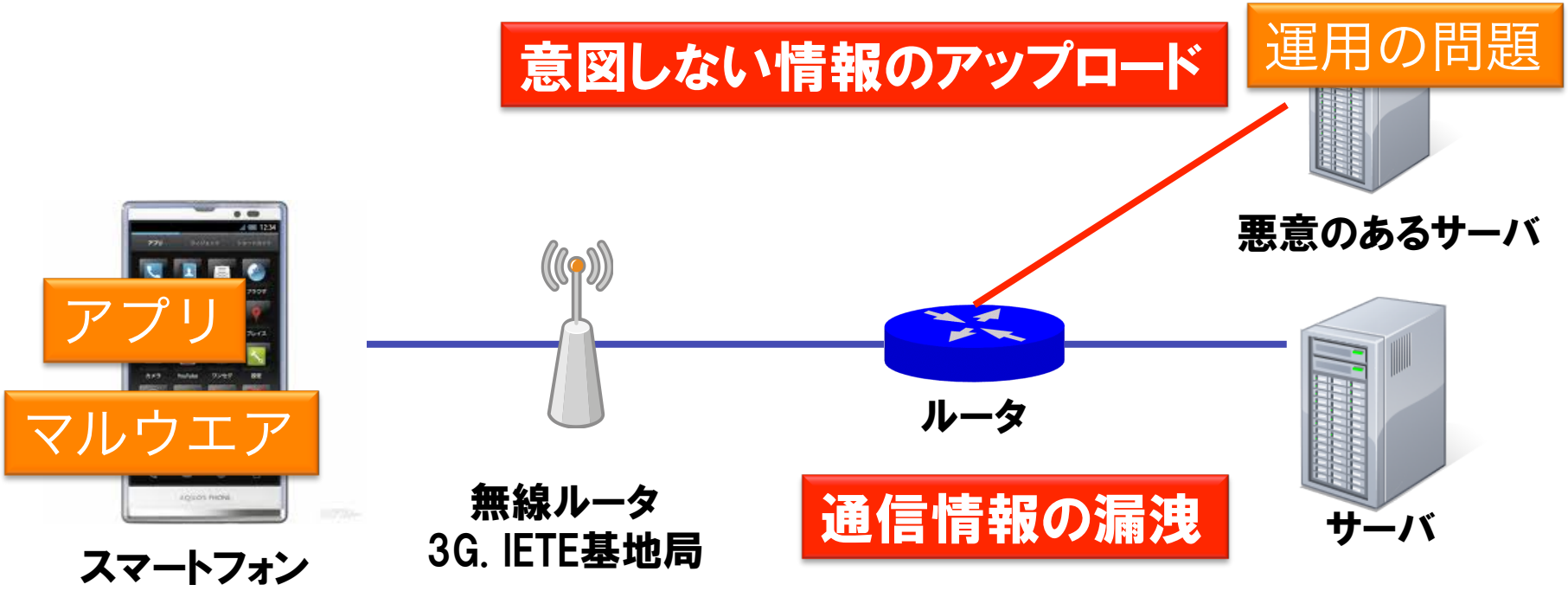
- 銀行サイトへのログインを模したサイトへ誘導(フィッシング)
- ログインに必要な情報を攻撃者が取得
- なりすましにより、口座内の金銭が奪われるリスク
- 共通のパスワードにより他のサイトのなりすましも

講演者に最近来ている、類似のなりすまし攻撃の事例

- パスワードリセットを装ったフィッシング
- パスワードを入力するサイトに誘導して、IDとパスワードを奪取
- なりすましにより買い物を勝手にされたり、もし共通のパスワードを使っていれば、他のサイトでもなりすましされるリスク

リスクの原因はあらゆるところにある

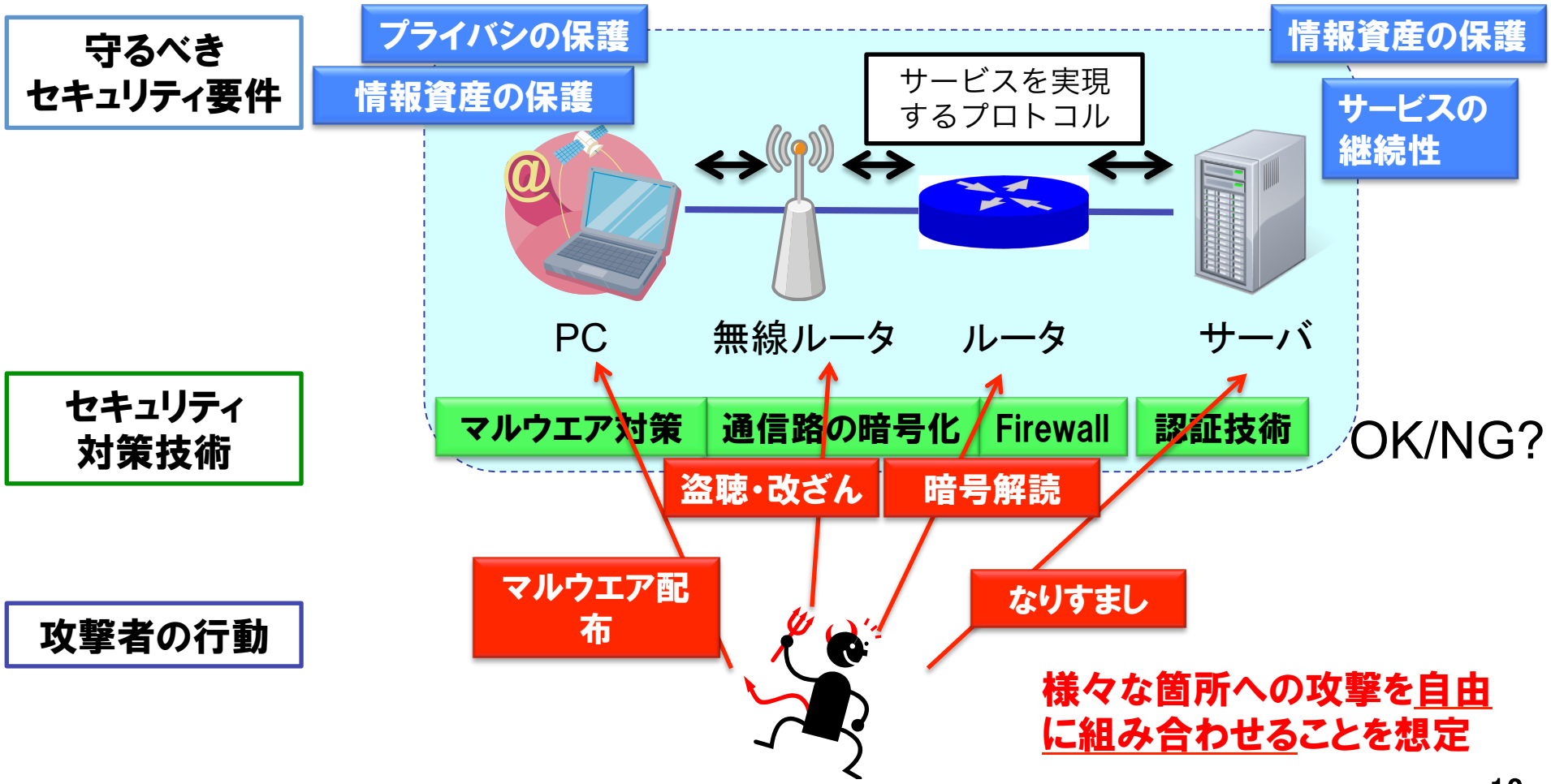
マルウエア（ウイルスなど）、サーバの運用だけではなく、ネットワーク、サーバなどとの組み合わせでリスクが拡大



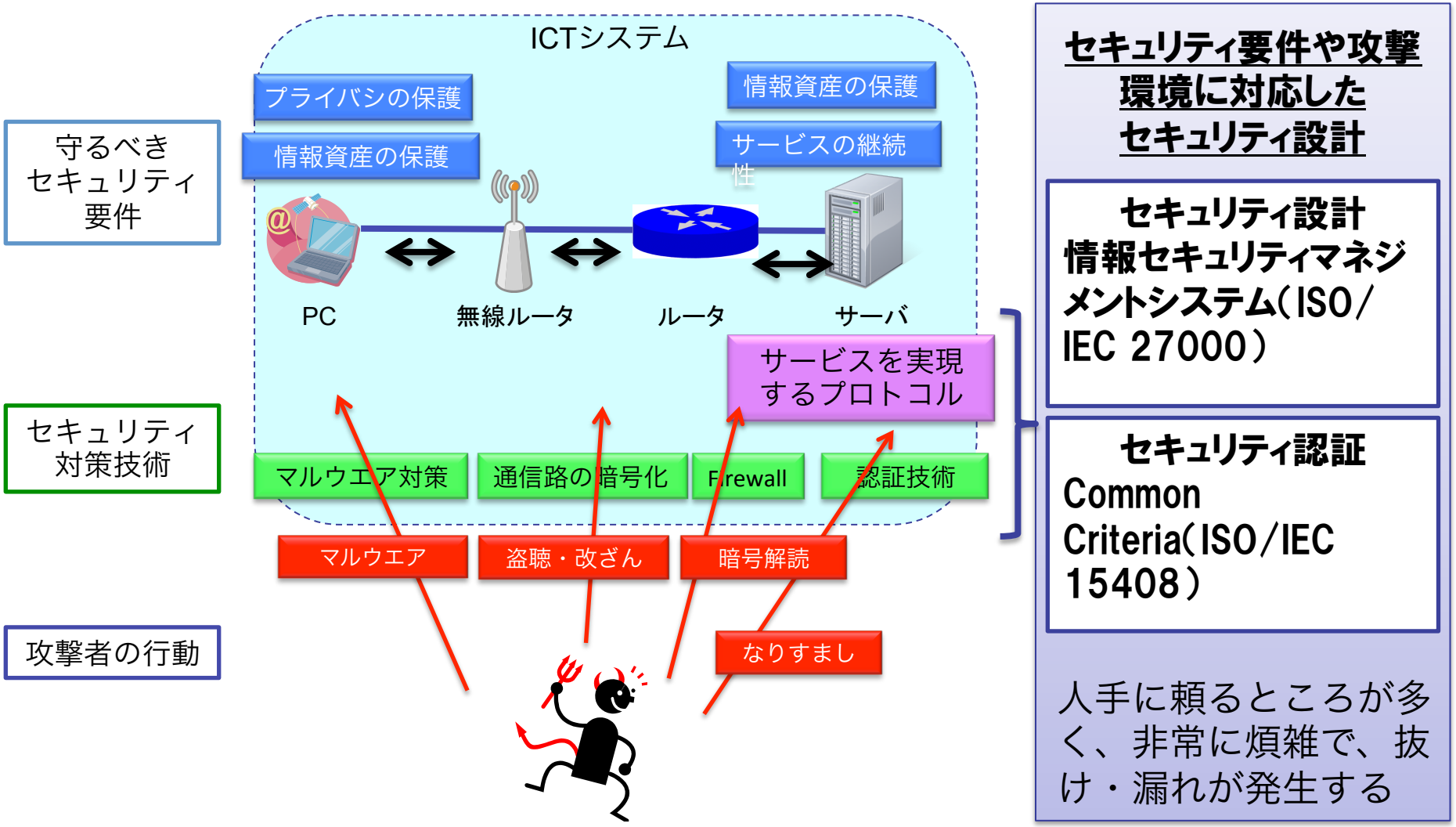
ネットワーク視点でのリスク評価・リスク管理が必要

ICTシステムにおけるリスクとは

守るべきセキュリティ要件に対して、対策技術が攻撃者の行動をどれだけブロックできているか



ICTシステムにおけるセキュリティ確保の現状



現状のシステムセキュリティ評価

- 情報セキュリティマネジメントシステム(ISMS、ISO/IEC 27000)によるリスク分析
- システム設計時に以下の表を作成することで、情報資産ごとのリスクの期待値を人間の手で評価

情報資産	脅威と発生確率				発生時の損失	リスクの期待値	対策手段	対策費用
	不正アクセス	改ざん	情報漏洩	DoS攻撃				
Webサイトのページ	-	10%	-	-	1000万円	100万円	ファイアウォール	20万円
スマートフォンの位置	-	-	10%	-	1万円	1,000円	OSによる警告	1万円
ID・パスワード	-	-	10%	-	5億円	5000万円	データベース暗号化	100万円

・
・
・

システムが複雑になると工数は爆発的に増大し、やりきれなくなる

リスクの認識における問題

- 多くのネットワークユーザは、利用しているネットワークにおけるセキュリティ・プライバシのリスクの在処を認識できない
  - 問題は(可視化されやすい)マルウエアだけではない
  - リスクの在処の例
    - 悪意のあるアプリ
    - 無線LANの暗号/認証の設定
    - サービスの認証方式
    - 問題のある古いバージョンのソフトウエアの継続利用
    - SSLの暗号設定

リスクの認識における問題（続き）

- リスクは、利用するサービスや利用環境によって異なる
  - 本当であれば、ISMSで行うような（一般ユーザにとって）複雑なリスク分析を行う必要があるが、その手間は掛けられない

- 手間を掛けられるとしても、リスク分析を行う材料が揃わない
  - ユーザは、手元の情報資産、ソフトウエア、設定を把握することは困難
  - そもそも、セキュリティ要件を認識できていないかもしれない

リスクの認識に必要なこと

1. セキュリティ要件と情報資産が洗い出せること
2. ネットワーク環境（攻撃環境）が洗い出せること
3. 現在使っている対策技術が洗い出せること
4. リスク分析ができること

2.リスク評価と対策提示に向けたプラットフォーム

リスクの可視化

ネットワークサービスを利用した時のリスクを可視化

- 守るべきセキュリティ要件と情報資産
  - 利用するサービスと想定される途中経路から判断

- 攻撃者の行動
  - アプリの脆弱性、無線LAN設定や認証方式の甘さ、途中経路の脆弱性などから判断

- 対策技術
  - 利用されている暗号化、認証などから判断

タブレット利用におけるリスク分析デモ

インターネットを経由した企業ネットワークへのアクセスにおけるリスクを可視化するシステム
（5号館4階でもデモをご覧いただけます）

企業ネットワーク
管理者への警告

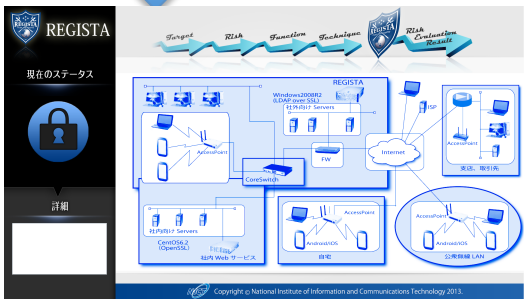
必要な
セキュリティ
を入力

タブレット

リモートアクセス

リスクと原因の
可視化

リスク分析



企業
ネットワーク

タブレット上のリスク表示

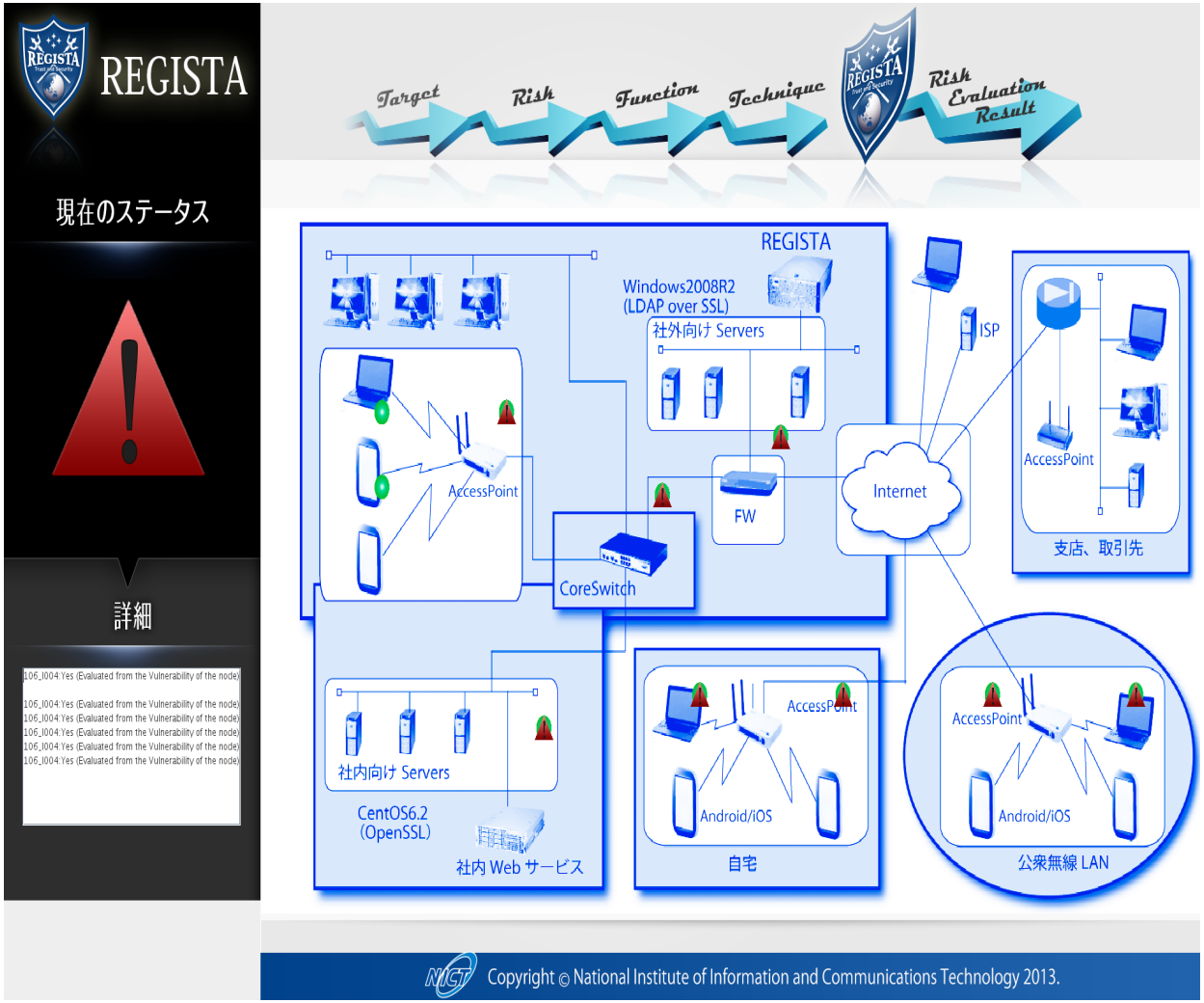
- 現在の利用方法に対するリスクの高さを表示
- 必要に応じて原因を確認可能

企業ネットワーク管理者向けの管理画面

- リスクを含むアクセスが合った場合に、企業ネットワークの管理者にその事実を通知
- リスクの原因に関する分析結果を表示可能
→対策に活用

全体表示

- ネットワークアクセス全体におけるリスクとその所在をリアルタイム表示



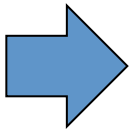
Demo

リスクの管理に向けて

リスクを常に許容範囲に保つためのサイクル

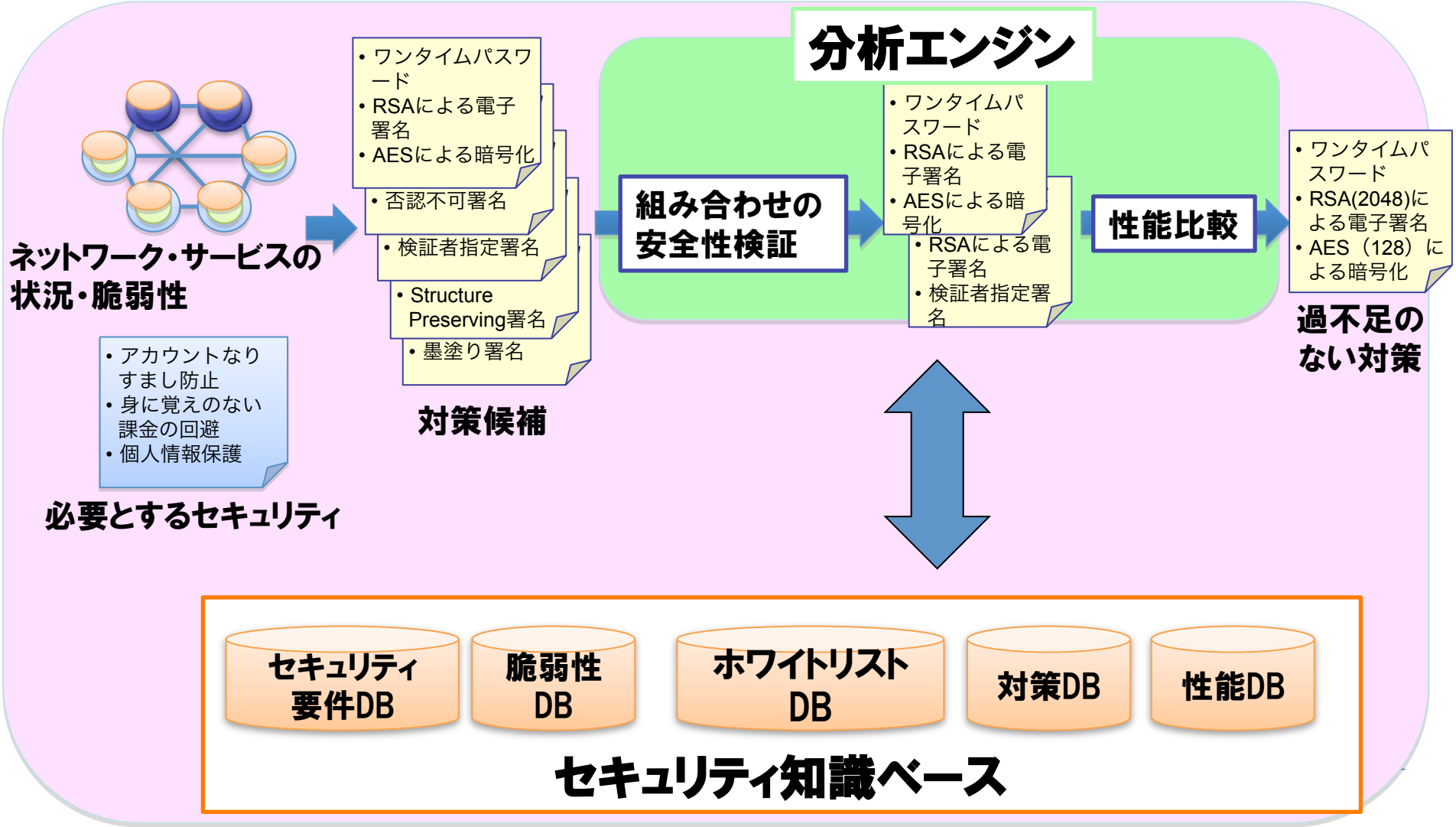
- 可視化されたリスクに対して適切な対策を取る
  →リスクの低減

- リスクに変動を及ぼす、新たな攻撃や脆弱性が発生した場合には、リスクの再評価を行い、管理策を適用



  - リスク分析の自動化によるコスト削減
  - 最新の脆弱性情報を有する知識ベースの構築
  - 対策の提示と、適用に向けたアシスト

セキュリティ知識ベース・分析エンジンREGISTA



REGISTAの特徴

リスク評価に必要なセキュリティ知識ベース

- サービスに必要なセキュリティ要件
- ソフトウエア、ネットワーク機器等の脆弱性
- 標準的なセキュリティ対策技術
- セキュリティ技術の組み合わせに対して、検証済みの対策を収めたホワイトリスト

より精密な分析を行うための分析エンジン

- 網羅性を持った対策技術のセキュリティ評価

現在、NICTで構築、実証中

3.今後の研究開発の方向性

利用形態の多様化に対応したリスク分析の高度化

スマートフォンやクラウドをはじめとする環境やアプリの多様化への対応

- PCとは異なる運用モデル、アーキテクチャ
  - アプリケーション主体となるため、アプリケーションの挙動のモデル化が必要
- スマートフォン特有の情報資産
  - 電話帳
  - 写真
  - GPS、ライフログ　etc.
- SNS、クラウド連携を考慮したセキュリティ・プライバシ保護要件
  - 情報の流通範囲の拡大
  - リンクによるプライバシ問題

リスク評価手法の高度化とよりわかりやすい可視化

- 多角的なセキュリティ・プライバシ評価
  - 各種アプリ解析結果との連携
  - アプリケーションの脆弱性や攻撃性と、ユーザ視点でのリスクの関連性
  - アプリケーション単体だけでなく、他サービスとの連携によるリスクの評価

- リスク評価結果の可視化方法
  - ユーザのリテラシーレベルに応じた可視化
  - 利用者に誤解を与えない可視化方法の検討