



National Institute of Information and Communications Technology

スマートフォン時代のプライバシー保護と リスク管理プラットフォーム

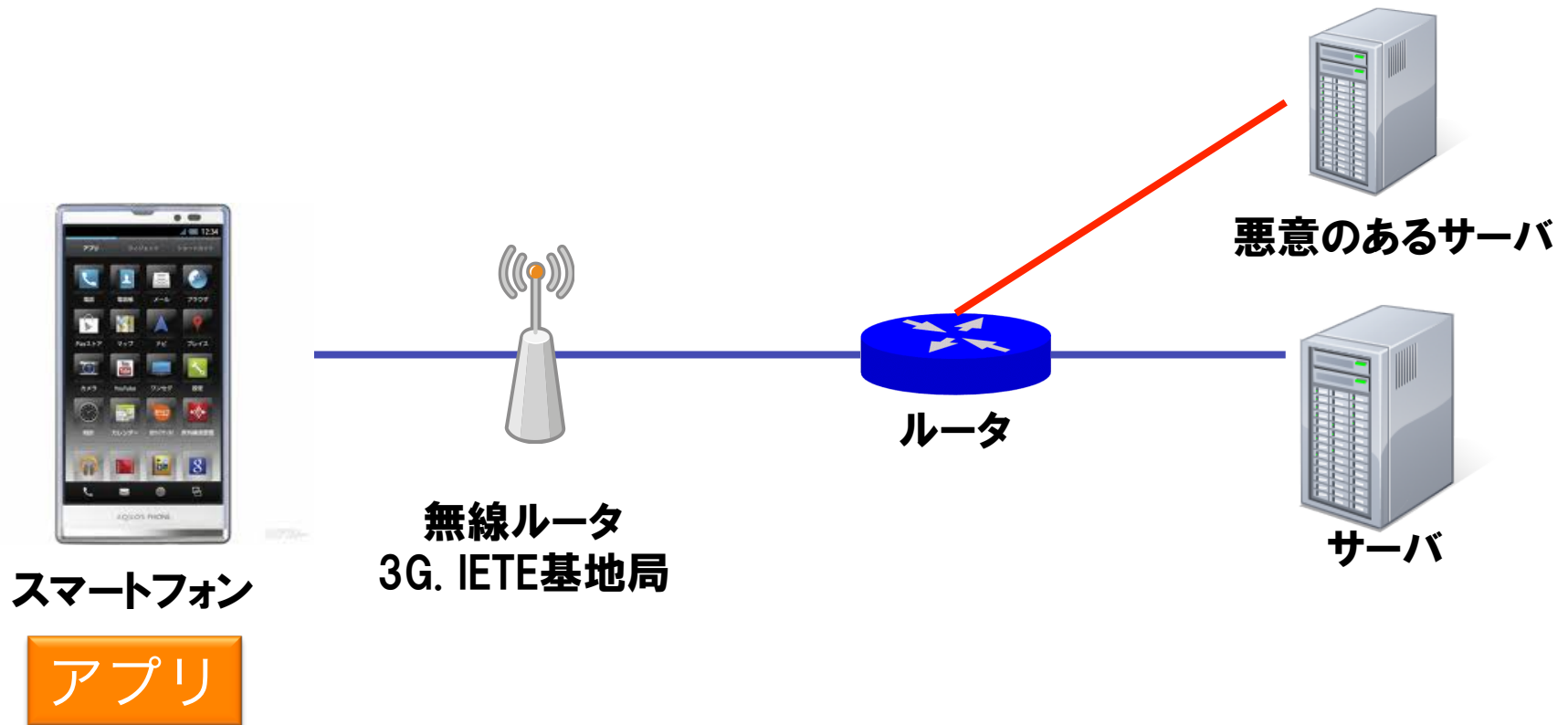
独立行政法人 情報通信研究機構
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室

松尾 真一郎

- 1. スマートフォンにおけるセキュリティ・プライバシーに関するリスク**
- 2. ネットワーク利用におけるリスク管理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.スマートフォンにおける セキュリティ・プライバシーに関するリスク

スマートフォン利用時のネットワークの概要



ネットワーク利用における新たな脆弱性



Lucky Thirteen: Breaking the TLS and DTLS Record Protocols

4th February 2013

Introduction	Who are we?	What is affected?	How severe are the attacks?
How does this work relate to known attacks?	Why are the attacks called "Lucky Thirteen"?	What are the countermeasures?	Patches, advisories and press
Is it still safe to use TLS?	Source code	Responsible disclosure	For more information

Introduction:

The Transport Layer Security (TLS) protocol aims to provide confidentiality and integrity of data in transit across untrusted networks like the Internet. It is widely used to secure web traffic and e-commerce transactions on the Internet. Datagram TLS (DTLS) is a variant of TLS that is growing in importance. We have found new attacks against TLS and DTLS that allow a Man-in-the-Middle attacker to recover plaintext from a TLS/DTLS connection when CBC-mode encryption is used. The attacks arise from a flaw in the TLS specification rather than as a bug in specific implementations. We have carried out experiments to demonstrate the feasibility of the attacks against the OpenSSL and GnuTLS implementations of TLS, and we have studied the source code of

[Lucky 13](#)

[Research paper \(pdf\)](#)

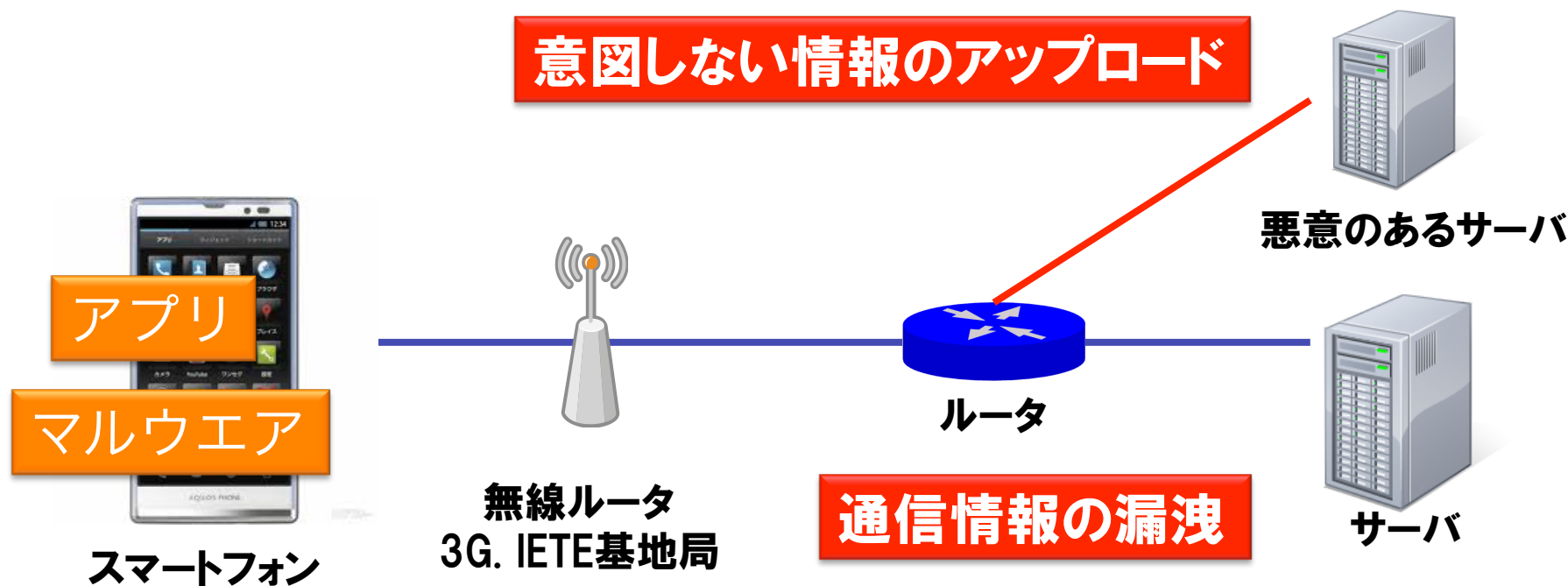
[Contact](#)

[Supported by](#)

- 2013年2月4日に論文で公開
- 中間者攻撃を利用して、TLSにおける暗号データの解読
- TLSプロトコルにおける暗号化部分のCBCモードの使い方(仕様)に起因
- すでに製品では修正を実施

スマートフォン利用時のリスク

アプリ単体だけではなく、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



ID/Passwordの漏洩

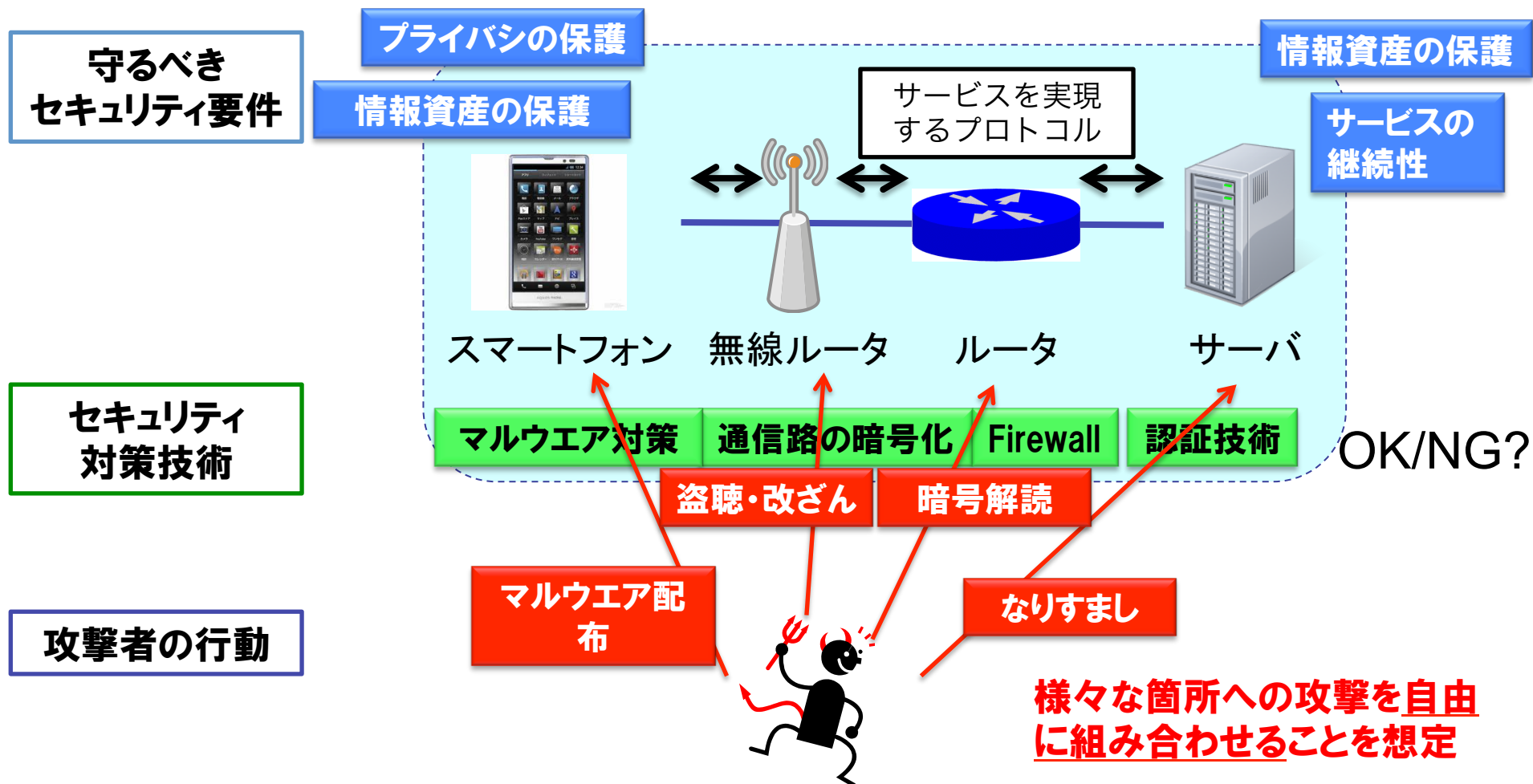
異なる情報の連携によるプライバシー漏洩

➡ ネットワーク視点でのリスク評価・リスク管理が必要

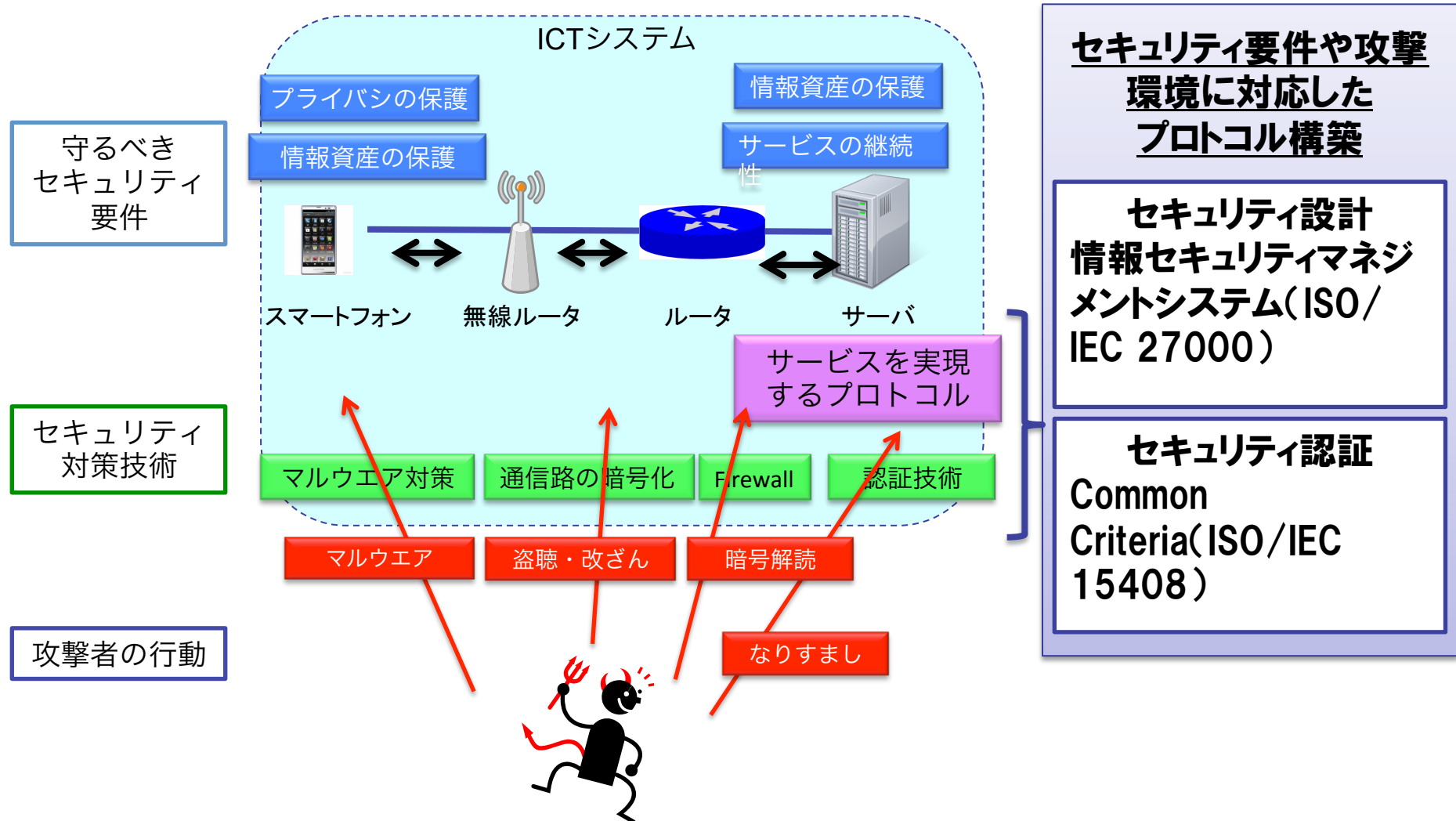
2.ネットワーク利用における リスク管理に向けたプラットフォーム

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システムのセキュリティ確保と現状



複合的な脅威に対して、リスクとコストに見合った対策の構築が必要

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

⋮

- **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・プライバシー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)マルウェアだけではない**
 - **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ェアの継続利用**
 - **SSLの暗号設定**

- **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、ソフトウェア、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**

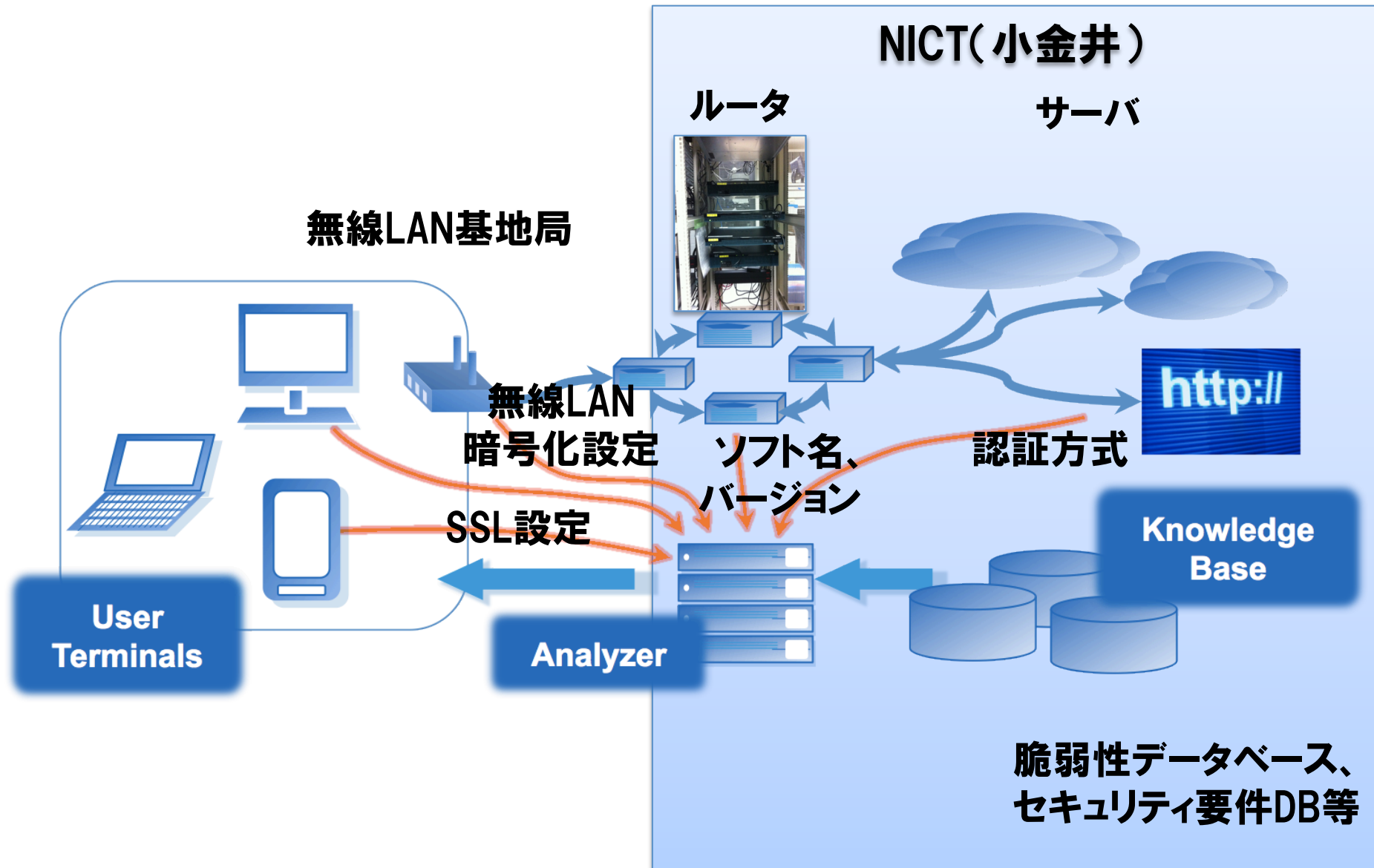
1. セキュリティ要件と情報資産が洗い出せること
2. ネットワーク環境(攻撃環境)が洗い出せること
3. 現在使っている対策技術が洗い出せること
4. リスク分析ができること

スマートフォン利用におけるリスク可視化の試み

スマートフォンのアプリから、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**

リスク可視化システムの構成



リスク可視化システムのユーザインターフェース



Simple Mode

Topology Mode

Detailed Mode

Demo

脆弱性情報とのマッチング



脆弱性情報とユース
ケース対応した
セキュリティ評価と
のマッチング

National Vulnerability Database (NVD) National Vulnerability Database (CVE-2012-5187)
web.nvd.nist.gov/view/vuln/detail?vulnid=CVE-2012-5187

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities Checklists 800-53/800-53A Product Dictionary Impact Metrics Data Feeds Statistics

Home SCAP SCAP Validated Tools SCAP Events About Contact Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:
55074 CVE Vulnerabilities
202 Checklists
231 WebCEP Alerts
2690 85-CERT Vuln Notes
8140 CVE Publications
68974 CVE CVEs
1737 CVE Names

Email List

NVD provides four mailing lists to the public. For information

National Cyber-Alert System

Vulnerability Summary for CVE-2012-5187

Original release date: 02/06/2013
Last revised: 02/07/2013
Source: US-CERT/NIST

Overview

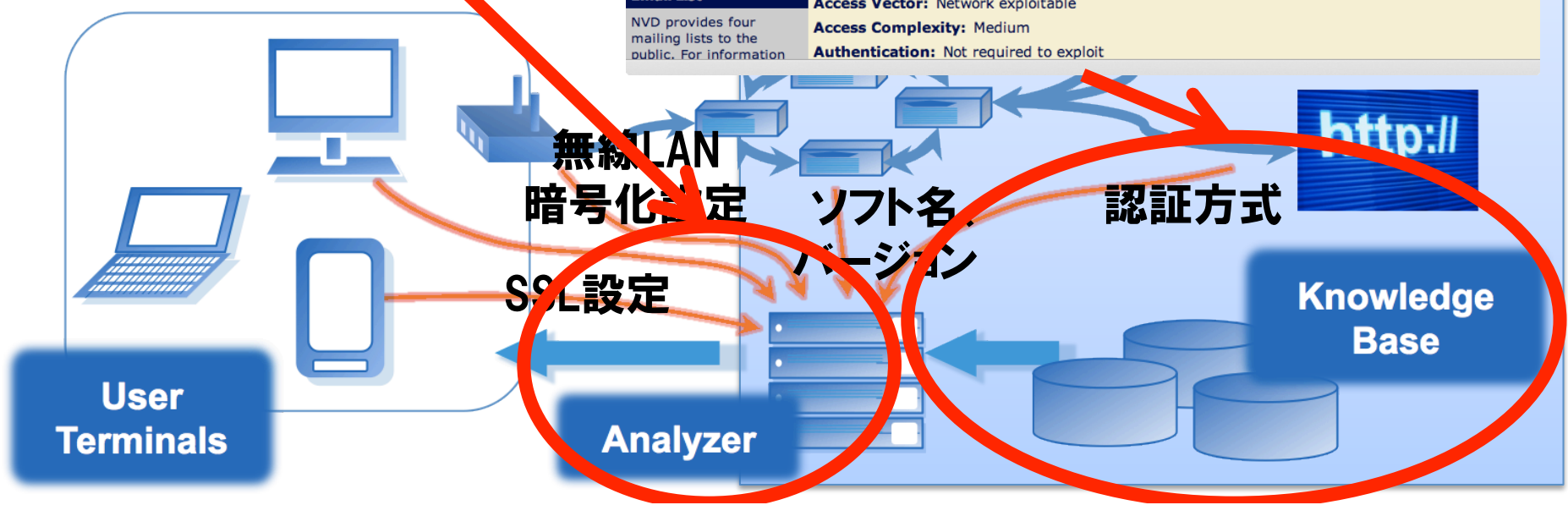
The Weathernews Touch application 2.3.2 and earlier for Android allows attackers to obtain sensitive information about logged locations via a crafted application that leverages read permission for system log files.

Impact

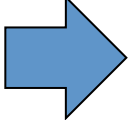
CVSS Severity (version 2.0):
CVSS v2 Base Score: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:N/A:N) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:
Access Vector: Network exploitable
Access Complexity: Medium
Authentication: Not required to exploit

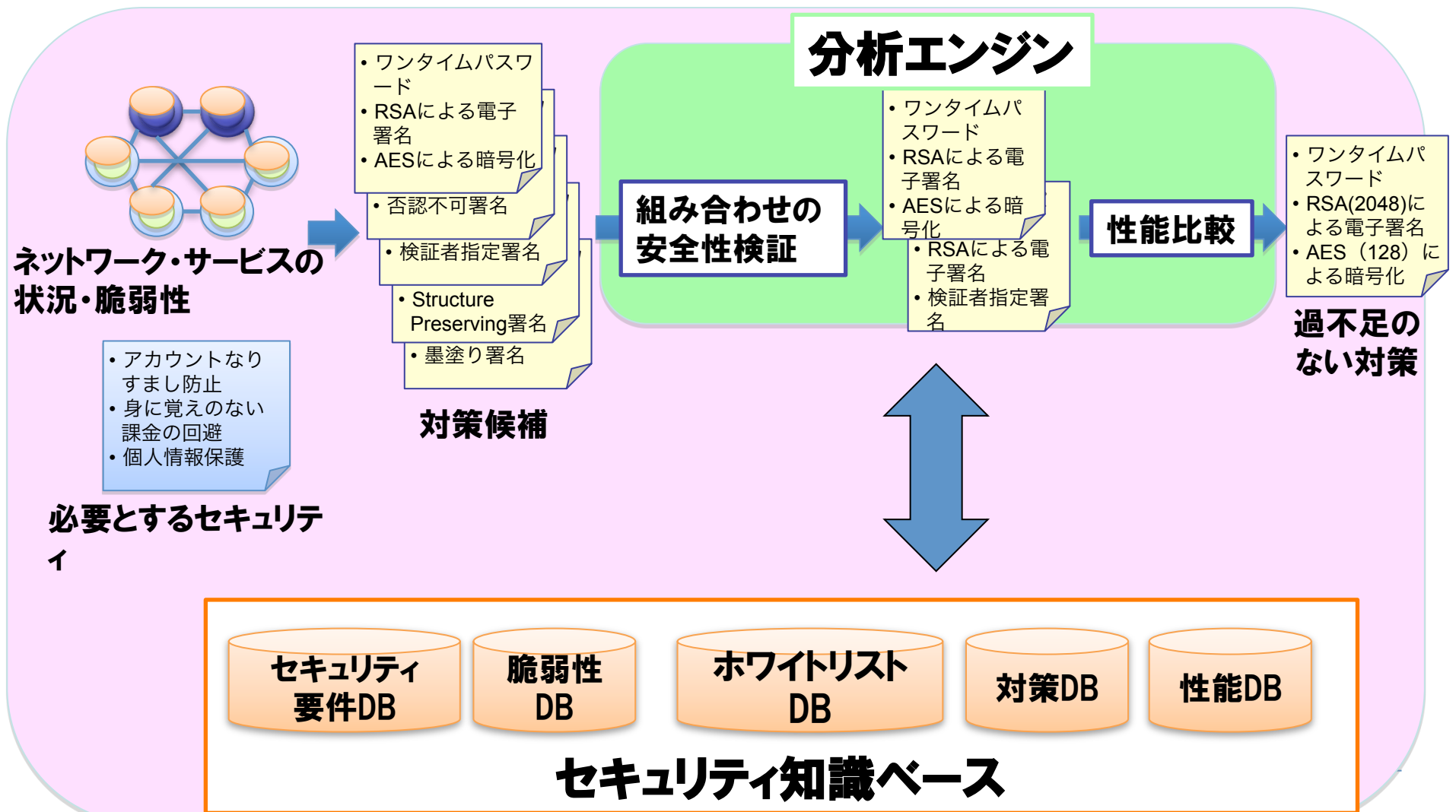
無線LAN基地局



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
 - 管理策の提示と、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



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
- ソフトウェア、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

- 形式化手法を用いることで、漏れのない対策技術のセキュリティ評価

現在、NICTで構築、実証中

3. 今後の研究課題と方向性

スマートフォンにおけるリスク分析手法の検討が必要

- **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・プライバシー保護要件**
 - 情報の流通範囲の拡大
 - リンクによるプライバシー問題

- **アプリケーション自体セキュリティ・プライバシー評価**
 - **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**