

セキュリティアーキテクチャ技術の 研究開発成果と今後の課題



国立研究開発法人 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長事務取扱

平 和昌

実施した研究開発の概要

セキュアなネットワーク利用を実現する 新たなセキュリティ技術を開発

セキュリティに関する各種情報を集めた
知識ベースを構築・活用して
リスクの分析・提示

①
セキュリティ知識ベース
・分析エンジンの構築

③
暗号プロトコル
の安全性評価

セキュアな通信を支える
暗号プロトコルの安全性を
評価

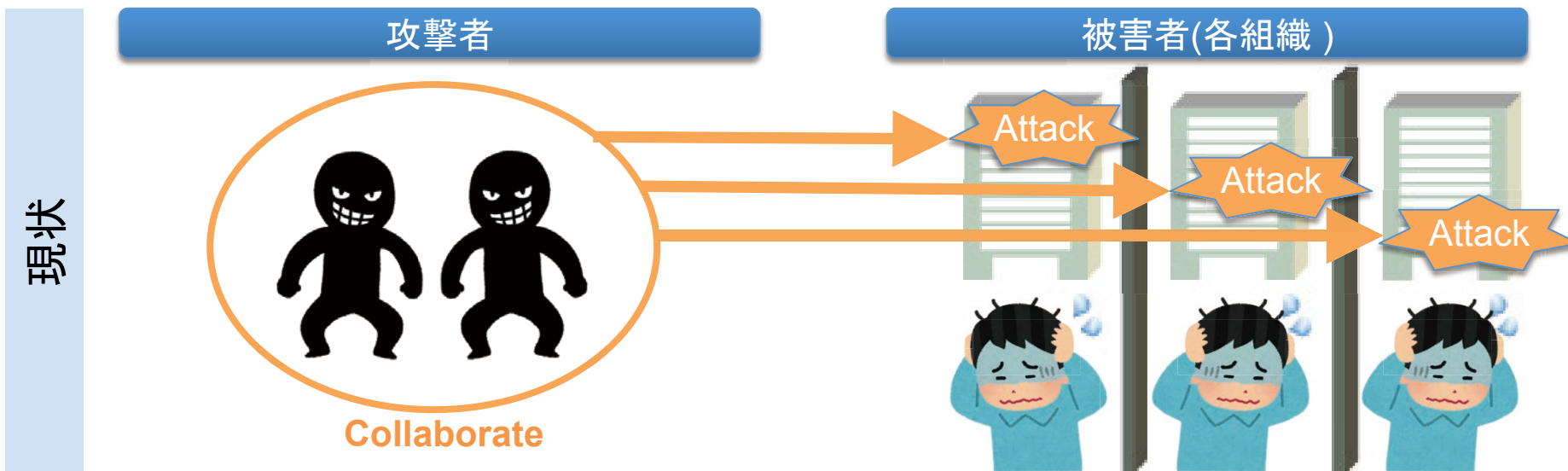
②
大規模ネットワーク向け
認証・プライバシー保護技術
の開発

省リソースデバイスの
セキュアな利用を実現する
認証・プライバシー保護技術を提案

①

セキュリティ知識ベース・ 分析エンジンの構築

組織を超えるセキュリティ情報の共有



セキュリティ脅威に対抗するために、**各組織が情報連携**することが必要。そのための技術について検討した。

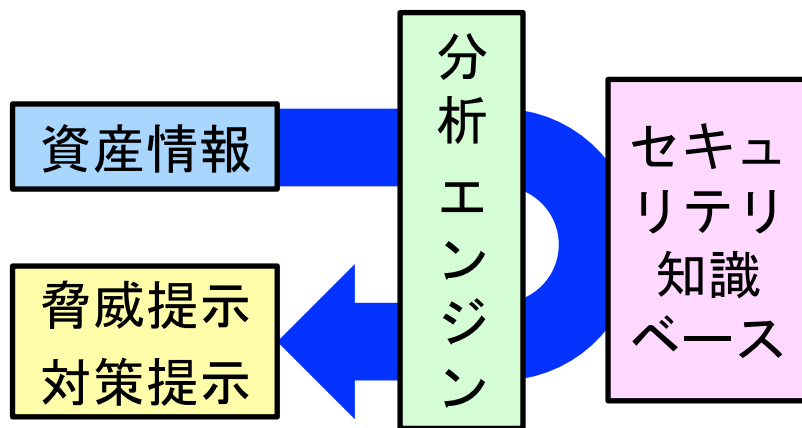
アプローチ

- IT資産情報、脆弱性情報などの**情報スキーマ**を構築
- 情報を多数蓄積する**知識ベース**を構築
- インターネット上で効果的に情報共有を実現する**情報交換プロトコル**を構築
- **国際標準化**活動(IETF MILE WG、ITU-T SG17など)にも貢献

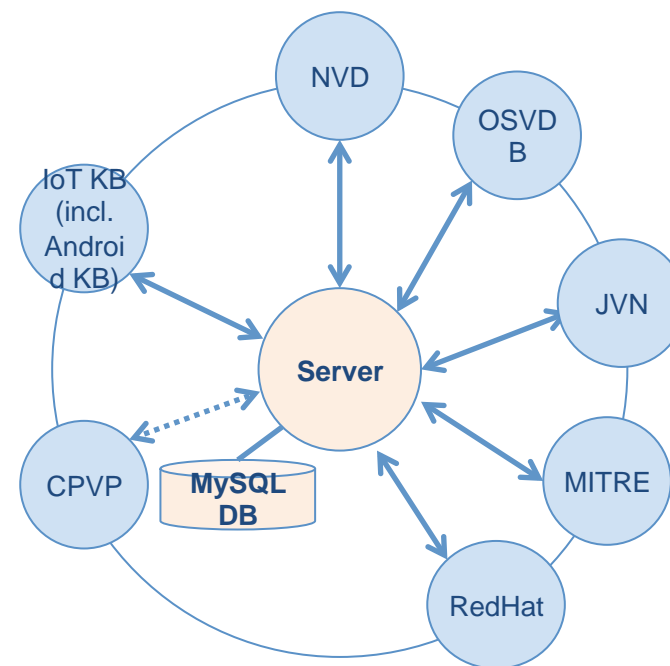
知識ベースを活用したリスク分析

セキュリティ対策の要となる「知識ベース」を構築しシステム化

- 「知識ベース」を情報連携の核とすることで、必要な情報が必要な時に入手できる環境を構築
- 独自の情報だけでなく、外部機関の知識ベースとも連携し、記述フォーマットの異なる各種セキュリティ情報の横断検索機能を実現

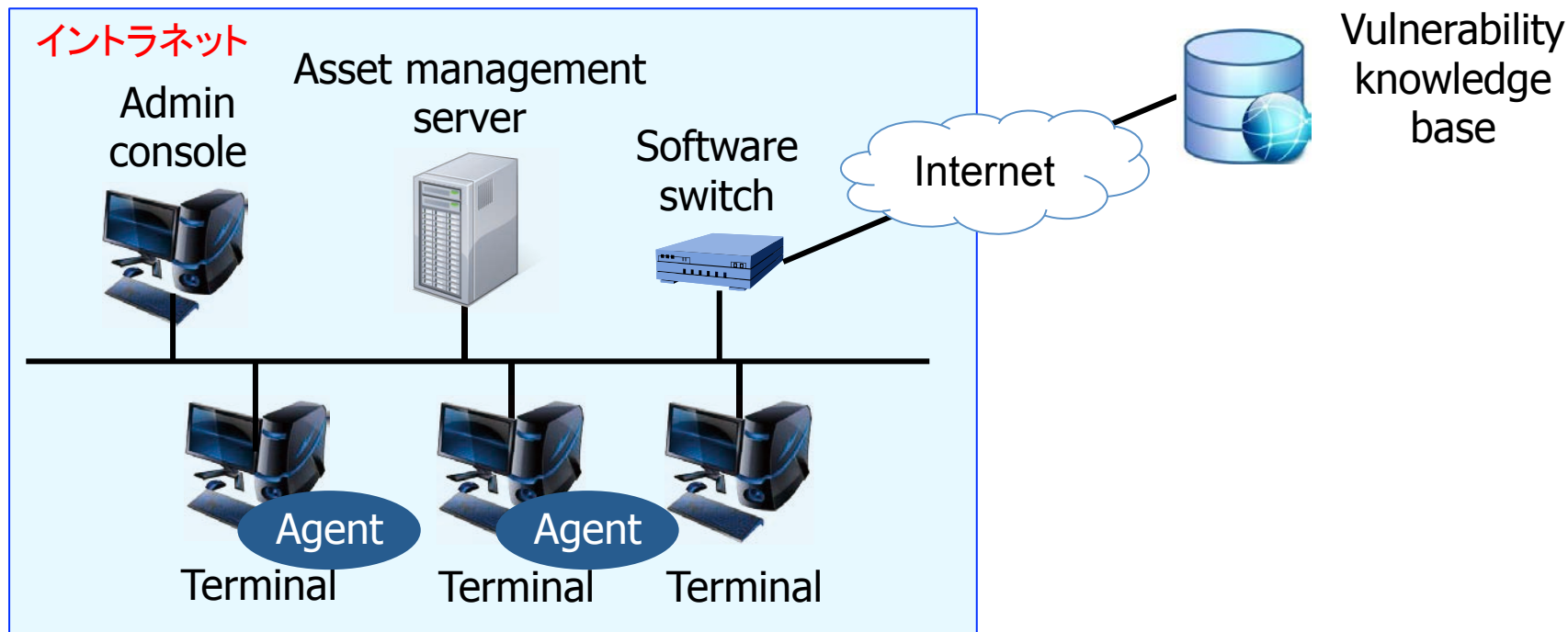


知識ベースを活用した
リスク分析のフレームワーク



複数の知識ベースの連携

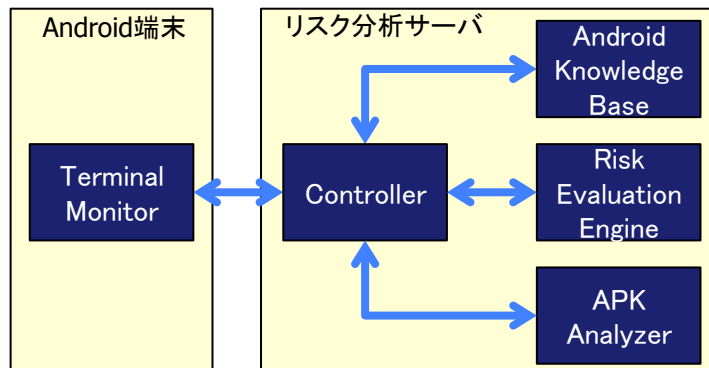
IT資産情報に基づく脆弱性自動提示システム



ソリューションの開発 ネットワーク上のIT資産に関する情報を自動的に収集し、それをID化する技術、また、そのIDを用いて知識ベース内の脆弱性情報を検索し、関連する脆弱性情報を管理者に通知する技術を構築。

成果の展開に向けた地方公共団体と連携 複数の地方公共団体に対して脆弱性管理の実態をヒアリングし、本技術のニーズを把握。いくつかの公共団体と協力して、当該団体の情報システム内に本技術を導入してその効果を確認する実験を実施中。

スマートフォンアプリのリスク分析・可視化



Androidアプリのリスク分析フレームワーク



マルウェア検知アルゴリズム

「脅威」の評価に対して、Webから取得したAndroidアプリのコンテキストにより判定する独自手法を提案・実装し、評価精度を大幅に向上

脆弱性検知アルゴリズム

共同研究先と連携し、既存脆弱性情報の引き当てに加え、コーディング上の弱点を検知し、判定に活用

情報の蓄積

共同研究先と連携し、**約10万件のAndroidアプリ**に対して本システムの有効性を検証し、分析結果及びメタ情報を**知識ベースに格納**

成果のシステム化

Androidアプリのリスク分析システムの**プロトタイプを構築**

②

大規模ネットワーク向け認証・
プライバシー保護技術の開発

省リソースデバイスにおける認証・プライバシー保護

IoT時代においては・・・

- センサなど多数の**省リソースデバイス**から多くのデータが発信
- 「モノ」のひとつひとつにも**タグ**がつけられて社会にばらまかれていく



省リソースデバイス向けの
セキュリティ／プライバシー対策が必要

本研究では**RFIDタグ**に対して、

- 証明可能安全性を有する**認証プロトコル**を構築
- プライバシー保護機能を載せた**認証プロトコル**を実装した**RFIDタグ**を作製して実験



RFIDタグのライフサイクルと所有権譲渡

理論

プロトコル構築
証明可能安全性
理論的構成要素

実装

実用的構成要素
計算時間
PUFのノイズ

RFID認証の実現可能性の検証

RFIDにおける認証・プライバシー保護技術

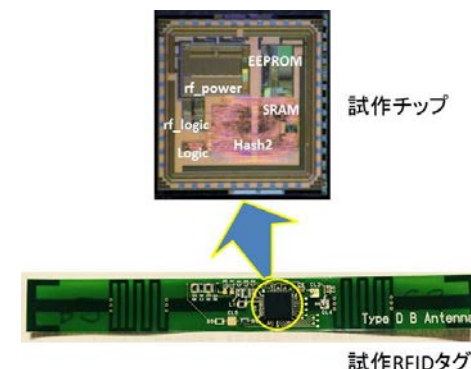
IoT時代における大規模ネットワーク上で多種多様な利用が想定される「RFIDタグ」に対して、セキュリティ・プライバシー要件の理論的な枠組みを構築

<理論： 所有権譲渡対策の Protokol>

安全性とプライバシーについて証明可能かつ効率的な所有権譲渡 Protokolを提案。

<実装： RFID認証の実現可能性の検証>

- 130nmプロセス製造のチップにより、市販のRFIDリーダーと**認証を行うチップを試作**。消費電力、回路規模、通信時間や通信可能距離の測定を実施(委託研究により実施)。
- **PUF**を用いることで偽造を防止できることから、PUFを活用したRFIDタグの認証 Protokolを構築。**FPGA 100台**を用いてSRAM PUFの挙動を分析し、回路規模や計算時間を測定。



試作RFIDタグ
プライバシー保護型RFID認証 Protokolを実装したRFIDタグの試作品



100台のFPGAを用いて、構築したRFID認証 Protokolの回路規模および演算時間を分析

③

暗号プロトコルの 安全性評価

暗号プロトコルの安全性評価への取組み

この2年間にもSSL/TLSにおける脆弱性がいくつも発見された...



暗号プロトコル評価に関するポータルサイトCPVPを開設

標準化プロトコルの評価とその結果の公開

2011年

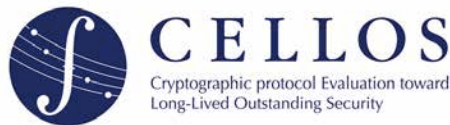
評価基準の標準化に寄与
ISO/IEC29128



2013年

CELLOSの設立を先導
国際連携体制を構築

発起人であり事務局を担う
重要な脆弱性情報を速報



暗号プロトコル評価技術
コンソーシアム「CELLOS」

2015年

58個の標準プロトコルの評価
結果をリスト化しCPVPで公開

- ・セキュリティの状態が一目でわかる、世界でも類がない試み
- ・暗号プロトコルの適切な利用への貢献



暗号プロトコル評価技術コンソーシアム「CELLOS」



CELLOS
Cryptographic protocol Evaluation toward
Long-Lived Outstanding Security

法人会員：10組織
個人会員：21名

【目的】

- 暗号プロトコルの安全性に関する国際的に信頼できる
情報の集約・共有・議論
- **安全性情報の公開**
- 安全な暗号プロトコルの普及促進

【設立】平成25年12月6日

【座長】手塚 悟 東京工科大学教授

【事務局】NICT

脆弱性の原因が実装と仕様のどちらか、実システムへの影響、回避策の有無などをまとめ、速報として公開

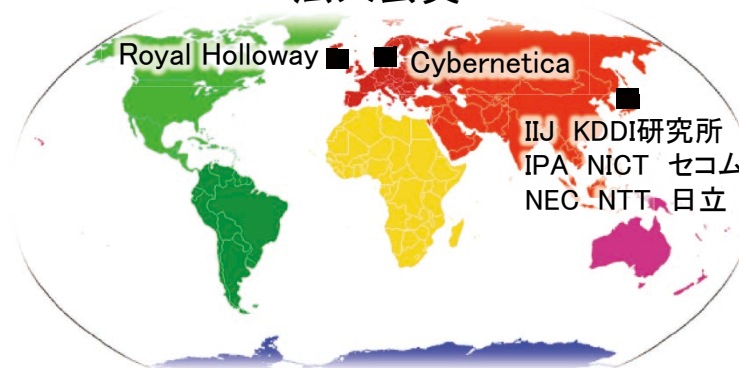
これまで発表した「速報」は、

- 2014年：7件
- 2015年：3件
- 2016年：2件

Heartbleed, POODLE, FREAK, Logjam, DROWN等



法人会員



www.cellos-consortium.org/

暗号プロトコルの安全性評価結果の公開

58個の標準プロトコルの評価結果をリスト化してWebサイトで公開

crypto-protocol.nict.go.jp

Cryptographic Protocol Verification Portal

AKE Protocol Zoo About us Update Contact

The AKE Protocol Zoo

The AKE Protocol Zoo は、安全な通信インフラに不可欠な認証および鍵交換 (AKE, Authentication and/or Key Exchange) の主要な暗号プロトコルの現時点の安全性が一目で分かる画期的なウェブサイトです。このサイトは、産官学全ての組織のみならず個人まで広く使っていただけます。

凡例

評価の厳密さを★の数の多さ (1~4) で表し、利用の可能性を色で区別しています。表の最後のページを最後までご覧ください。

- 現状安心して利用できる (現時点において攻撃が発見されていない)
- 現状安心して利用できる (攻撃が発見されているが現時点では非現実的な脅威)
- 対策を施せば安心して利用できる (攻撃が発見されているが回避策がある)
- もはや安心して利用できない (現実的な脅威のある攻撃が発見されている)

国際標準

プロトコル名	機能	評価結果
EAP-AKA	相互認証・鍵交換	★★★★ [詳細]
EAP-Archie	相互認証・鍵交換	★★★★ [詳細]
EAP-IKEv2	相互認証・鍵交換	★★★★ [詳細]
EAP-SIM	相互認証・鍵交換	★★★★ [詳細]
EAP-TLS	相互認証・鍵交換	★★★★ [詳細]
EAP-TTLS	相互認証・鍵交換	★★★★ [詳細]

色と星の数で、セキュリティの状態と評価の厳密さを表す

- ・青、黄：現状安心して利用可能
- ・橙：対策を施すことで現状安心して利用可能
- ・赤：もはや安心して利用できない
- ・星の数1~4で、ISO/IEC29128における評価レベル PAL1~4を示す (星の数が多いほど評価が厳密)

暗号プロトコルの安全性評価結果を公開

～認証やプライバシー保護のためのプロトコルの安全性評価を推進～

2013年7月2日

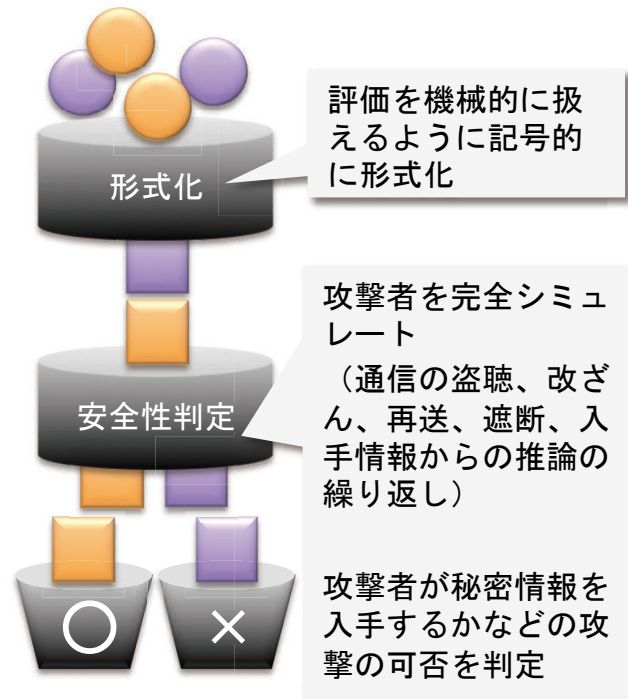
独立行政法人情報通信研究機構 (以下「NICT」、理事長：坂内 正夫) は、ネットワークにおける情報の暗号化、認証、情報の改ざん防止、プライバシー保護などを達成するために、暗号技術と通信のやり取りとを組み合わせた「暗号プロトコル」の技術開発を行っています。このたび、NICTは、認証やプライバシー保護に用いられる暗号プロトコルの安全性について、中立的な立場で評価し、その評価結果をICTシステムの安全な設計に役立てるための活動を開始します。その第一歩として、ISO/IEC 29128に沿った暗号プロトコル評価ツールによる評価結果をとりまとめたポータルサイトを7月1日に開設しました。今後は、ICTシステムの更なる安全性向上のために、ベンダ等への評価結果の提供、研究機関の国内連携及び国際標準候補の暗号プロトコルの安全性の確認などに貢献する基盤を構築していきます。

暗号プロトコルの安全性評価技術

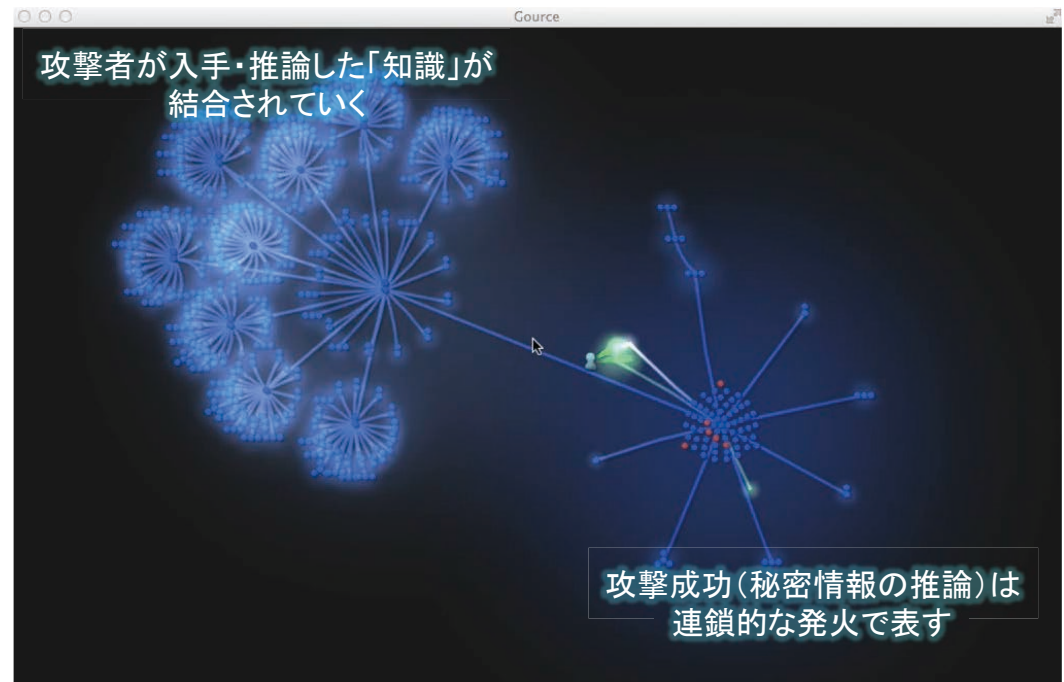
安全性評価において、攻撃状態を可視化することにより、人手による解析を支援

安全性評価の流れ

暗号プロトコルの仕様、攻撃者、安全性を記述



判定結果から
攻撃や脆弱性を解析



暗号プロトコルの安全性評価過程の可視化

今後に向けて…

今後の研究開発の展開方針

平成28年度以降

① セキュリティ知識ベース・分析エンジンの構築

知識ベースの開発

脆弱性の分析・自動対策技術

サイバーセキュリティ関連
情報の大規模集約・共有

成果の社会への展開

② 大規模ネットワーク向け認証・プライバシー保護議技術の開発

省リソースデバイスにおける
認証・プライバシー保護プロトコル

IoTシステムの
セキュリティ・プライバ
シー保護技術の開発

③ 暗号プロトコルの安全性評価

安全性評価ツールの開発

評価結果情報の集積・再評価・公開

CELLOS活動への参画

CRYPTRECにおける
暗号プロトコル安全性評価

本日はありがとうございました

