平成 25 年 12 月 19 日

独立行政法人 情報通信研究機構
株式会社日立製作所
株式会社 KDDI 研究所
日本電信電話株式会社

「暗号プロトコル評価技術コンソーシアム」の設立について

独立行政法人 情報通信研究機構(理事長: 坂内 正夫)、株式会社日立製作所(執行役社長:中西 宏明)、株式会社 KDDI 研究所(代表取締役所長:中島 康之)、日本電信電話株式会社(代表取締役社長:鵜浦 博夫)は、国内外の学識経験者及び他の企業等と、安心・安全なネットワーク利用の促進に向けて、認証やプライバシ保護などを実現する暗号プロトコルの安全性向上のため、平成 25 年 12 月に「暗号プロトコル評価技術コンソーシアム」(以下「本コンソーシアム」、座長:東京工科大学 手塚 悟 教授)を設立しました。

本コンソーシアムでは、暗号プロトコルに対する新たな攻撃やその対策も含めた安全性情報を集約し、国内外の専門家が検討した結果を Web サイトで迅速に公開します。これにより、これまで個人や単独の組織では把握が困難であった暗号プロトコルの利用に関して専門家が検討した情報を、システムベンダやプロトコル利用者が容易に入手できるようになり、利用を想定している暗号プロトコルに対して利用可否の判断に活用できることから、新たな ICT システムの設計に還元できるため、安全な暗号プロトコルの利用促進につながります。

1. 本コンソーシアム設立の趣旨

近年のネットワークの発展は、単なるコミュニケーション促進だけでなく、モバイルネットワークやクラウドコンピューティングなど、我々の生活の向上に向けて、新たな情報通信の可能性を開こうとしています。これに加え、プライバシ保護など、高度な安全性も要求されるようになっており、単に通信内容の暗号化や認証を行うだけでは不十分となっています。

それに対して、多種多様な暗号技術を組み合わせた「暗号プロトコル」が精力的に研究開発され、現在 400 を超える暗号プロトコルが国際標準化されています。しかし、無線 LAN 用暗号プロトコル WEP に次々と脆弱性が発見されるなど、これらの暗号プロトコルが現実の ICT システムに即した安全性評価は、これまで十分に行われていませんでした。とりわけ、世界レベルかつ最新の安全性に関する情報を集約し、専門家による議論を経た、幅広く技術的に詳細な情報を社会に公開する活動は、これまで国際的に見てもありませんでした。一方で、日本は、ISO/IEC において主導的に安全性評価指標の標準化を行うなど、安全な暗号プロトコルに関する世界の研究開発をリードしてきました。

そこで、これまでの日本の研究開発成果を基盤として、暗号プロトコルの技術的な安全性に関する情報の集約と共有、現実の ICT システムに即した技術的な議論、それらから得られた安全性情報の公開、安全な暗号プロトコルの普及促進を目的として、「暗号プロトコル評価技術コンソーシアム」(以下「本コンソーシアム」という)を設立しました。

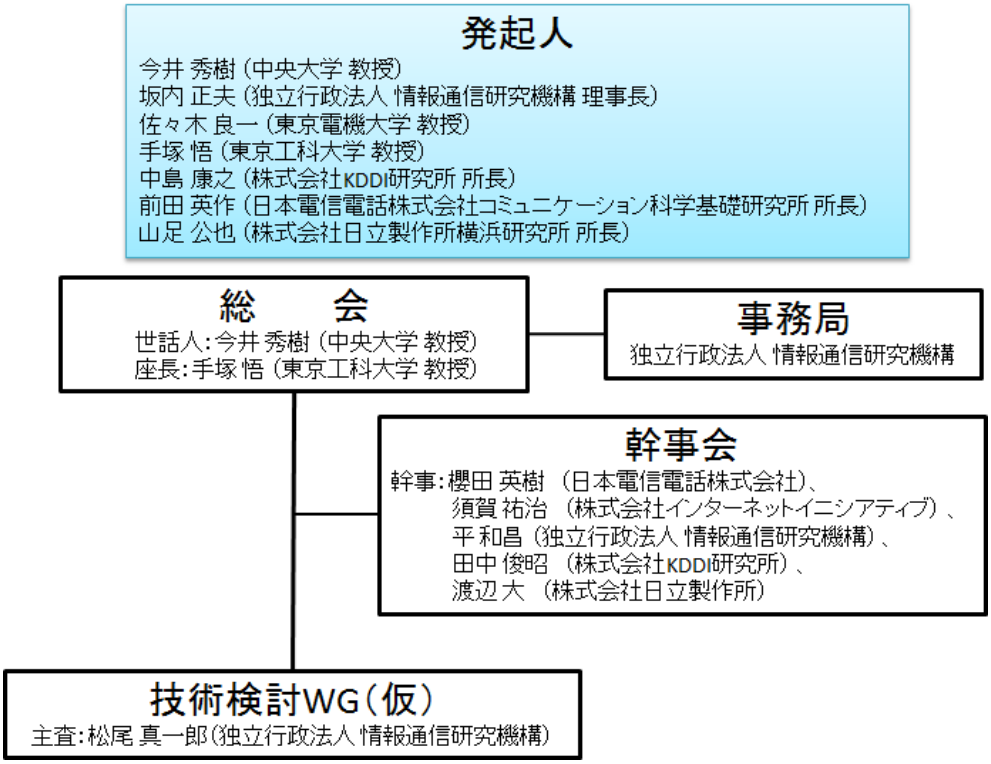
本コンソーシアムにおいては、暗号プロトコル研究に関連する国内外の大学や研究機関、そして関係企業から活動に参加いただき、日本のみならず国際的な協力体制で、暗号プロトコルの高度な安全性を確保するための情報の集約・共有・発信の国際拠点となる活動に取り組みます。

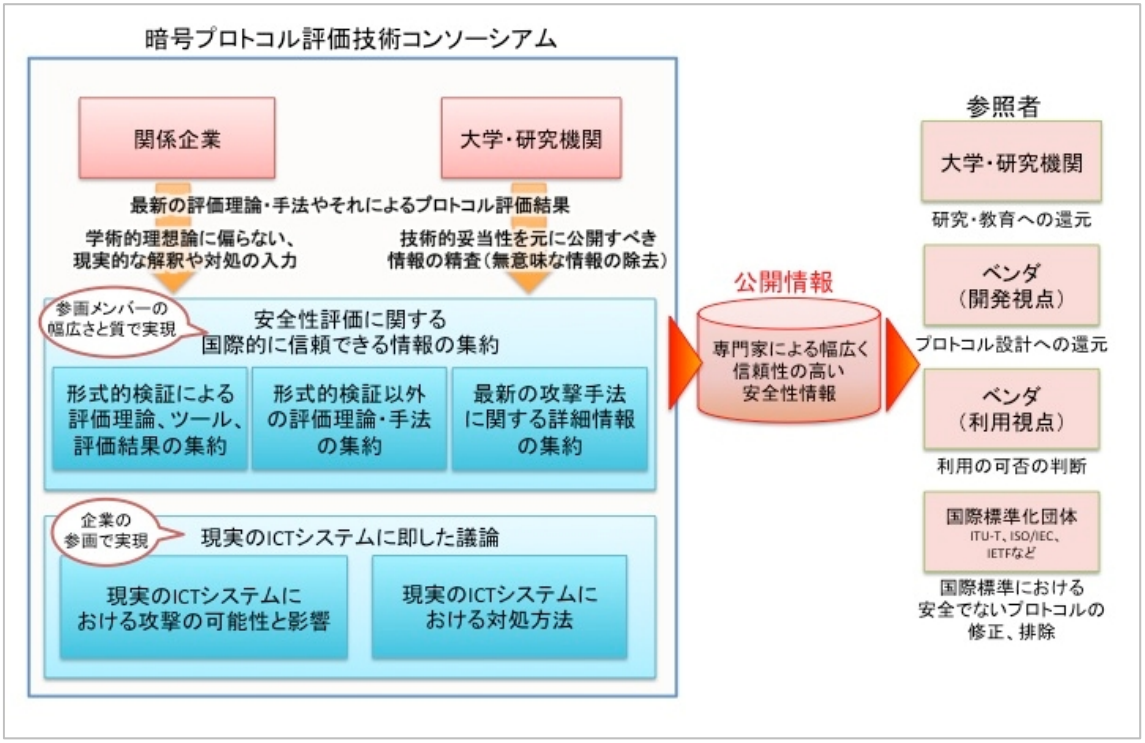
本コンソーシアムは、このような活動を通じ、ネットワークセキュリティの向上に大きく貢献し、今後のネットワーク利用の安心・安全に繋がるよう先導的かつ主導的役割を果たしていきます。

2. 本コンソーシアムの概要

本コンソーシアムでは、暗号プロトコルの技術的な安全性評価を行うための理論や手法及び評価結果、新たな攻撃手法に関する情報を集約し、技術的事実の確認と現実の ICT システムへの影響や対処方法に関して議論します。その際、情報通信研究機構が開発している暗号プロトコルの安全性評価システムを本コンソーシアムの活動に活用します。暗号プロトコルの安全性に関する専門家の議論を経た情報を迅速に発信することで、暗号プロトコルの利用の可否の判断や安全な暗号プロトコルの設計が可能となり、安心・安全なネットワークの利用が促進されます。

【本コンソーシアムの体制図】





3. 各社の役割分担等

(1)独立行政法人 情報通信研究機構

情報通信研究機構は、ネットワークセキュリティに関する研究の一環として、暗号プロトコルの安全性評価技術に関する研究開発を行っております。これまでに暗号プロトコルの安全性評価に関する国際標準規格である ISO/IEC 29128 "Verification of Cryptographic Protocols"の標準化をプロジェクトエディタとして推進し、また、ISO/IEC 29128 に沿った暗号プロトコル評価結果を公開する「暗号プロトコル評価ポータルサイト」を公開しております。当コンソーシアムでは、暗号プロトコル評価に関する研究成果を展開していくとともに、事務局を担当し、国際的にも信頼される成果を出していけるように貢献して参ります。

(2) 株式会社日立製作所

日立製作所は、暗号プロトコルの安全性評価に関する国際標準規格である ISO/IEC 29128 "Verification of Cryptographic Protocols"の標準化をプロジェクトエディタとして推進するなど、セキュリティ技術に関するさまざまな研究開発、標準化活動を行ってきました。当コンソーシアムにおいては、これらの知見を活かし、ネットワーク利用のより一層の安全・安心の実現に貢献して参ります。

(3) 株式会社 KDDI 研究所

KDDI 研究所は、誰もが安心してネットワーク上のサービスを使えるようにするためのセキュリティ技術に関する研究開発を行っています。サービスに対する安全性を確保するために必須となる暗号プロトコルに対しては、計算量理論に基づく安全性評価技術の研究を行い、独自の安全性検証ツールを開発しています。当コンソーシアムにおいては、これまで培った理論的検証技術及び上記の独自ツールを用いて、暗号プロトコルの安全性評価を実施していきます。

(4) 日本電信電話株式会社(NTT)

NTT 研究所は、安心・安全な社会実現に貢献するための暗号・セキュリティ技術に関する研究開発を行っています。特に暗号プロトコルの安全性評価については、数理論理学を応用したフォーマルメソッド(形式手法、数理的技法)と呼ばれる手法を駆使して厳密に評価を行う技術の研究を行なっており、当コンソーシアムにおいては、これまで培った研究技術及び専門的知見に基づいて暗号プロトコルの安全性に厳密かつ客観的な評価を与えられるよう注力していきます。

4. 今後の進め方

本コンソーシアムでは、新たな攻撃手法に対する現実のシステムへの影響、対処方法に関して、迅速な情報公開を本コンソーシアムの Web ページにて行います。

なお、本コンソーシアムの会員や活動など詳細については、本コンソーシアムの Web ページでお知らせしていきます。(https://www.cellos-consortium.org)