2015 年 7 月 9 日
日本電信電話株式会社
三菱電機株式会社

暗号技術の安全性確認により、信頼性を向上

改ざん検知暗号 Minalpher® が米国暗号コンテスト一次選考通過

日本電信電話株式会社（本社：東京都千代田区、代表取締役社長：鵜浦博夫、以下「NTT」）と三菱電機株式会社（本社：東京都千代田区、執行役社長：柵山正樹、以下「三菱電機」）が、国立大学法人福井大学（文京キャンパス：福井県福井市、学長：眞弓光文、以下「福井大」）と開発した改ざん検知暗号 Minalpher®（ミナルファ）は、米国標準技術院（NIST）が支援する国際暗号評価コンテスト（CAESAR コンテスト）の一次選考を通過しました。

一次選考通過の概要

NTT と三菱電機は、福井大と連携して開発※ した、暗号化データの改ざんを検知できる高機能な暗号方式を Minalpher®（ミナルファ）と命名し、米国 CAESAR コンテストに応募しました。2014 年 8 月には米国で開催された国際ワークショップで Minalpher® の優位性を口頭発表するなど、その国際規模での認知に向けた活動を実施してきました。

CAESAR コンテストには世界から 57 方式が提案され、これまで主に安全性について、Minalpher® 設計陣を含む世界の暗号研究者により評価がされてきました。今回、CAESAR コンテストのコミッティが一次選考結果を発表し、Minalpher®を含めた 30 方式が通過しました。

※：2014 年 3 月 17 日報道発表

Minalpher® 開発の背景

ネットバンキングなどの高いセキュリティーが求められるサービスでは、第三者による情報の閲覧を防ぐ秘匿機能と、情報の変更の有無を検知する改ざん検知機能が不可欠です。システム全体の安全性を確保するためにはこれらの機能を適切に組み合わせてシステムに組み込む必要がありますが、現暗号方式では、この組み合わせ方法から生じる脆弱性が巧妙に利用されて攻撃を受けることがありました。このような課題解決のため、情報の秘匿と改ざん検知の両機能を同時かつ安全に実現する「改ざん検知暗号」が提案されていますが、従来の改ざん検知暗号は安全に利用するための制約条件が複雑で、システム設計者に負担がかかるものでした。

Minalpher®は、従来の改ざん検知暗号と比較して利用時の制約条件が大幅に少ないという高い利便性によってシステム設計時の安全性を確保しやすく、かつ世界最高レベルの安全性と処理性能を実現するものです。

CAESARコンテストについて

暗号技術では、安全性確認を行ない信頼性を得るために、暗号方式を公募し評価を行なう暗号評価コンテストが開催されます。改ざん検知暗号技術の必要性の高まりを受け、改ざん検知暗号に関する暗号評価コンテストとして、米国標準技術院（NIST）が支援する CAESAR コンテストが実施されています。

CAESAR コンテストは 2014 年 3 月までに応募があった暗号方式に対し、今回を含め 4 回の絞りこみをおこない、2017 年 12 月 15 日に最終結果を発表する予定です。本コンテストで採用された方式は、今後の安心安全社会を支える情報セキュリティー基盤技術のひとつとなることが期待されます。

今後の展開

NTT と三菱電機は今後 Minalpher® の CAESAR コンテストでの採用と、組み込み機器や様々な通信環境への適用を目指し、安全性の検証とともにさまざまなプラットフォームでの性能評価を行っていきます。

商標関連

Minalpher は登録商標です。

＜本件に関するお問い合わせ先＞
日本電信電話株式会社
サービスイノベーション総合研究所
企画部広報担当
TEL：046-859-2032
E-mail：randd@lab.ntt.co.jp

三菱電機株式会社
広報部　室井
TEL：03-3218-2346
E-mail：prd.prdesk@ny.MitsubishiElectric.co.jp