2014 年 3 月 17 日
日本電信電話株式会社
三菱電機株式会社

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開発
～従来の方式における様々な制約を解決～

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: 山西健一郎、以下「三菱電機」）は、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」）と連携し、暗号化データの改ざんを検知できる新たな暗号方式を開発しました。

今回開発した暗号方式は、従来、個別に提供されていた情報の秘匿化と改ざん検知の機能を安全に組み合わせ上で単一の機能として提供するものです。本暗号方式によって、システムの情報セキュリティの根幹をなす暗号機能の設計において、システム設計者が脆弱性を埋め込む可能性を低減することが可能になります。

NTT と三菱電機は福井大と連携し、本暗号方式を米国標準技術院（NIST）（注 1）が支援する暗号評価プロジェクト（CAESAR プロジェクト）へ応募するとともに、安心・安全な情報化社会の基盤の確立に向けて本方式の普及を進める予定です。

＜背景＞

ネットバンキングなどの高いセキュリティ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。しかしながら、2011 年の BEAST 攻撃（注 2）や 2013 年の Lucky Thirteen 攻撃（注 3）などでは、この組み合わせ方法における脆弱性が巧妙に利用されています。

このような問題を解決するために、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あるために、依然としてシステム設計者に負担がかかるものでした。

この度、NTT と三菱電機が福井大と連携して開発した新たな改ざん検知暗号は、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。

＜今回開発技術のポイント＞

（１）利用時の制約条件が大幅に少ない高い利便性

今回開発した方式は、秘匿機能と改ざん検知機能を同時に実現する改ざん検知暗号の一方式です。多くの従来方式では、復号処理の過程で生成される平文相当のデータが出力されると、攻撃者が改ざん検知をくぐり抜ける暗号文を偽造できるという問題がありました。そのため、従来方式を安全に利用するためには、復号処理が完了するまでは平文を出力することができませんでした。今回開発した方式では、復号処理の中間データを出力しても暗号文を偽造される恐れはありません。この性質により、復号したデータを溜め込まずに逐次的に出力できるので、記憶領域が少ないデバイスでも大きなデータを取り扱うことが可能となります。

また、既存の多くの改ざん検知暗号、例えば AES-GCM を安全に利用するためには、ナンスと呼ばれる毎回必ず異なる値を入力する必要がありますが、現実の利用においてはデータの再送やシステム構築の検証時に同一のナンスが使われ、安全でない利用となる場合がありました。本方式では、同じ値をナンスとして利用してもほとんどの利用場面では問題が起きない設計となっているため、万が一動作検証のために同じナンスの値が使われるよう状態のシステムをリリースしたとしてもシステム全体の安全性が脅かされる危険はきわめて低くなります。

さらに、AES-GCM では一度に暗号化できる平文の長さは 64GB が上限ですが、本方式では事

実上無制限に長い平文に対しても安全に利用可能です。

（２）高い安全性

暗号に求められる最も重要な要件は安全性です。本方式においても、プリミティブ（注 4）の安全性は既知の攻撃法に対して十分に安全であることを確認するとともに、モード（注 5）の安全性をプリミティブが安全であることから、数学的に安全であることを証明しており、高い安全性を担保しています。

（３）高速な処理性能の実現

本方式は多くの環境、例えばスマートフォン上において AES-GCM（注 6）の速度よりも高速に動作します。また IC カードや M2M で利用される組込みデバイスのようなメモリが限られた環境でも十分な性能を実現します。

＜CAESAR コンテストへの応募＞

暗号技術の安全性は、数多くの解読を試みる攻撃に長年耐えることにより評価が高まり、信頼を得ることが出来ます。短期間で評価を得るために暗号技術を公募し評価を行なう暗号評価コンテストが、暗号技術の安全性確認を行ない、信頼性を得るために重要な手順となっています。

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ます。CAESAR コンテストは 2014 年 3 月 15 日までに応募のあった暗号技術に対して、毎年 12 月 15 日（初年度である 2014 年については 2015 年 1 月 15 日）に応募技術の絞りこみ結果の発表を予定し、2017 年 12 月 15 日に最終結果発表を予定しています。

＜今後の展望＞

CAESAR コンテストの毎年の評価結果を受けてよりよい方式の改善に向けた研究を継続的に実施し、推薦技術となることを目指します。また、今後、普及が進むであろう M2M 通信などをより強固なものとし、攻撃の隙がない安心・安全な社会インフラの基盤技術の一つとなることを目指します。

＜用語解説＞

（注１）NIST

National Institute of Standards and Technology の略。アメリカで暗号技術の研究や標準を定めている組織。128 ビット共通鍵ブロック暗号 AES をはじめアメリカでの標準でありながら、ここで定められた標準は広く世界で使われている。

（注 2）BEAST 攻撃

Browser Exploit Against SSL/TLS 攻撃の略。Duong と Rizzo により指摘された。TLS1.0 の CBC 暗号化の脆弱性をつきアカウント認証に用いる情報を取り出す実証実験に成功している。

（注 3）Lucky Thirteen 攻撃

AlFardan と Paterson により指摘された攻撃。この攻撃によりウェブブラウザに格納された認証情報などを取り出すことができる。

（注 4）（暗号）プリミティブ

暗号を支える土台の技術。それそのものの安全性の証明には誰も成功しておらず、既知の攻撃が適

用できるかどうかの積み重ねにより安全性の信頼が増す。NIST が標準化した 128 ビットブロック暗号 AES や、NTT と三菱電機で開発した 128 ビットブロック暗号 Camellia などがプリミティブに相当する。

（注 5）（暗号利用）モード
プリミティブを簡単な演算で組み合わせ、秘匿や改ざん検知などを実現する方法。秘匿機能を実現する CTR モード、改ざん検知機能を実現する GCM などが知られている。

（注 6）AES-GCM
128 ビットブロック暗号 AES をプリミティブとし、秘匿機能を実現する CTR モードと改ざん検知機能を実現する多項式ハッシュを組み合わせた改ざん検知暗号。GCM は Galois Counter Mode の略。2004 年に McGrew と Viega により提案され、NIST により SP800-38D として標準化されている。暗号化通信プロトコル TLS1.2 で採用され、ウェブブラウザ Firefox27 から利用できる。大きく安全性を脅かす問題ではないが、安全性が低下する弱鍵の存在することが知られている。

【本件に関するお問い合わせ】
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
TEL: 03-3218-2865
E-mail:prd.prdesk@ny.MitsubishiElectric.co.jp