2007 年 12 月 17 日

株式会社日立製作所
学校法人東京理科大学
NTT コミュニケーションズ株式会社
独立行政法人情報通信研究機構

ユビキタスネットワーク社会における
多様かつ大量なデータの安全な流通・保存技術を開発

株式会社日立製作所(執行役社長：古川 一夫／以下、日立)、学校法人東京理科大学(理事長：塚本 桓世／以下、東京理科大)、NTT コミュニケーションズ株式会社(代表取締役社長：和才 博美／以下、NTT Com)の 3 社は、このたび、独立行政法人情報通信研究機構(理事長：宮原 秀夫／以下、NICT)からの委託を受け、ユビキタスネットワーク社会における多様かつ大量なデータの安全な流通・保存技術を共同で開発しました。これにより、さまざまな生活シーンにおいて、機密性の高いデータを扱う多種多様なサービスを、安全かつ快適に利用することが可能となります。

誰でもが、いつでも、どこでも、情報にアクセスすることができる「ユビキタスネットワーク」の普及と、それに伴う新たなサービスの出現により、ネットワークを介してやり取りされるコンテンツの多様化、大容量化が進み、また、モバイル環境で利用するための小型情報端末も次々と開発されています。今後、より一層サービスが多様化すると、例えば、著作権保護が必要な映画等の配信サービスや、官公庁への各種申請手続サービス、あるいは医療機関による健康管理サービスなど、ライセンス情報、個人情報を扱う機密性の高いサービスも出てくるものと予想されます。そのため、ユビキタスネットワーク社会において、それら機密性の高いサービスを安心して利用できるようにするための新しいセキュリティ技術が求められています。具体的には、従来パソコンで扱っていた動画コンテンツのような大容量データを、バッテリー容量が少ない小型情報端末で安全に利用するための「低消費電力暗号技術」や、不必要な情報開示をなくし情報漏えいリスクをできるだけ減らすために、各種申請手続きや健康管理に関する機密性の高い情報を，閲覧者の権限に応じて柔軟に閲覧制限するための「選択的開示暗号技術」が必要となります。また、サービスを提供する側にも、機密性の高いデータを長期間安全に保存し、かつ、障害等で一部の保存データが失われた場合でもサービスを容易に復旧できるようにするための「秘密分散技術」が必要です。

このたび、日立が低消費電力暗号化技術と選択的開示暗号化技術を、東京理科大が低消費電力暗号の安全性評価技術を、NTT Com が効率的な秘密分散技術を、それぞれ開発し、それら 3 つの技術を有機的に組み合わせることで、ユビキタスネットワーク社会における多様かつ大量なデータの安全な流通・保存技術を実現しました。

本技術は、NICT の委託研究「大容量データの安全な流通・保存技術に関する研究開発」(2005～2007 年度)の成果です。

今回開発した技術の特長は、以下のとおりです。

(1) 小型情報端末でも利用可能な低消費電力暗号技術

ユビキタスネットワーク社会において、いつでも、どこでも多種多様なサービスを享受するためには、より小型で持ち運びしやすい情報端末が必要となります。そのような小型情報端末はバッテリー容量が少ないため、大容量データを安全にやり取りするための暗号技術にも、安全性や高速処理に加えて、低消費電力で処理できることが求められていました。

そこで今回、既に電子政府推奨暗号であり ISO 標準でもある、高速性に優れた「日立ストリーム暗号 MUGI※1」をベースに、低消費電力で処理可能な新たなストリーム暗号「Enocoro」を開発しました。「Enocoro」では、内部状態を保持するレジスタの数を大幅に削減し、ハードウェアの規模を MUGI よりも小さく抑えることで、消費電力の低減を実現しました。また、SPN※2 2 層構成の攪拌関数を新たに採用することで、従来よりも強力にレジスタ上のデータを攪拌可能とするとともに、各層での処理を並列化して、安全性と高速性との両立を図っています。具体的には、暗号のデファクト・スタンダードである AES※3 と比べて、同程度の安全性・処理速度を実現しながら、ハードウェア化した場合の消費電力を 10 分の１以下※4 に抑えることが可能となりました。

一方、この新しいストリーム暗号のため、従来の手法よりも細かな単位で安全性評価が可能な新しい手法を東京理科大が開発しました。本評価手法は、昨今の並列 CPU 搭載コンピュータで、従来よりも高速な安全性評価が可能であるという特長を備えております。この評価手法により、「Enocoro」は、AES と同等の安全性を持つ事を確認いたしました。

(2) 利用者の役割や権限に応じて適切な個所だけが開示される選択的開示暗号技術

各種申請手続きや健康管理などのように機密性の高い情報を扱うようなサービスにおいて、情報漏えいリスクをできる限り減らすためには、不必要な情報を開示しないようにすることが重要となります。しかしながら、従来の暗号技術では、閲覧者の権限に応じて、あるコンテンツを閲覧できるかできないかというコンテンツ単位での制御は可能でしたが、そのコンテンツの中に含まれている各要素（例えば、氏名や年齢、職業等）を選択的に開示することはできませんでした。そのため、例えば、稟議書類のように複数部門に跨って処理されるようなケースでは、個々の部門では不必要な情報であるにもかかわらず、すべての情報が閲覧可能な状態となってしまうなど、情報漏えいの防止と情報共有の円滑化を両立することが困難でした。

そこで今回、閲覧者の権限に応じて、適切な箇所のみが復号され閲覧できる新たな暗号技術「選択的開示暗号技術」を開発しました。本技術では、コンテンツを複数の領域に分割し、それぞれの領域を、予め閲覧者の権限に対して割り当てられた暗号化鍵を用いてそれぞれ個別に暗号化することによって、同一の暗号化されたコンテンツであっても、閲覧者の権限に応じて閲覧できる箇所を制御可能としました。従来の単純な部分暗号化を利用した場合には、同じ領域を複数の閲覧者が閲覧する場合には、閲覧するユーザごとにその領域を部分暗号化したデータを用意する必要がありましたが、今回開発した選択的開示暗号技術では、複数の閲覧者がいる場合でも個々の領域の暗号化データは一つだけにし、閲覧者ごとに復号に必要なデータを整理して処理することによって、暗号化した結果得られる電子文書全体のデータサイズを削減す

ることができます。

なお、本技術は Web サービスなどで広く利用されている XML データに適用し、その有効性を確認しています。さらに、ビジネス文書として利用されている PDF ファイルに適用するための試作品の開発も行っており、今後、企業内の様々な電子文書に対して、利用者に応じた適切な情報開示を行うことが可能になります。

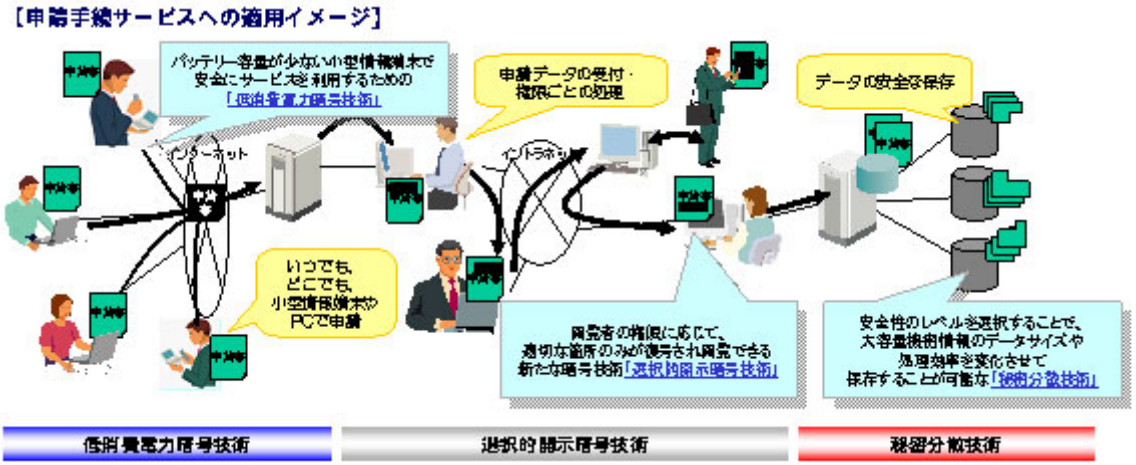
(3) 大容量データを安全に保存し、障害時には復旧もできる効率的な秘密分散技術

ネットワークストレージ環境の進展に伴い、地理的、ネットワーク構造的にロケーションの異なるデータが増加すること、および事故や災害によるデータ消失などのさまざまな障害を考慮し、これらを適切に保護可能にする方式を確立する必要があります。また、さまざまな価値を持つデータが混在することにより、長期間にわたる機密性および可用性を実現することに加え、安全性レベルの制御による、保存時の情報量抑制および符号化・復号の実行効率向上などを実現する方式を確立する必要があります。

そこで、本研究開発においては、NTT Com で開発した秘密分散法※5 を応用し、長期間に渡る機密性および可用性を実現するとともに、誤り訂正符号などを組み合わせることで、安全に機密情報を復元するための障害検知およびデータ復旧機能を実現しました。さらに、秘密分散法で利用する乱数の生成方式を新たに開発し、安全性のレベル、データサイズ、処理効率の変化を可能にしました。

これにより、セキュリティニーズに応じて安全性のレベルを選択することで、大容量機密情報を保存する際のデータサイズや処理効率を変化させることが可能となる秘密分散法のアルゴリズムを確立しました。

真性乱数と擬似乱数の中間の安全性を持つ乱数の生成法を考案し、それを秘密分散法に適用した場合の安全性の変化を理論的に証明したのは世界で初めての試みです。これにより、秘密分散法により電子データを保存する際の安全性のレベルとデータサイズを選択することが可能となりました。一般に企業は、機密性や保存年限が異なる様々な電子データを保存しているため、最適な安全性のレベルを選択することにより所要ストレージ量を削減できることのメリットは大きいと考えられます。



※1 ストリーム暗号 MUGI：鍵ストリームを使ってデータを 1 ビットずつ暗号化する方式です。MUGI (MUlti GIga cipher)は日立製作所が 2001 年に開発したストリーム暗号で、2003 年 3 月に電子政府推奨暗号リストに掲載され、2005 年 7 月に ISO 標準になっています。

※2 SPN (Substitution-Permutation Network)：AES でも採用されている攪拌方式です。なお、MUGI は Feistel 構造と呼ばれる攪拌方式を採用し、Feistel 構造 1 層で構成しています。Feistel 構造は、1977 年に米国が規格化した DES などの共通鍵暗号方式で広く採用されている、暗号の攪拌方式の一つです。

※3 AES (Advanced Encryption Standard)：2001 年に米国が規格化した共通鍵暗号の一方式であり、事実上の世界標準暗号です。米国の NIST (National Institute of Standards and Technology：国立標準技術研究所)の主催した 3 ヵ年に渡る公開評価を経て選定されています。

※4 10 分の 1 以下：実験的に、論理回路を書き込み可能なゲートアレイである FPGA (Field Programmable Gate Array)を使って 1 ビットのデータを暗号化する際に消費する電力を実測した結果、AES は 1.16nWs (ナノワット秒)、Enocoro は 0.103nWs でした。なお、数値は評価環境によって異なります。

※5 NTT Com で開発した秘密分散法：機密情報を 3 つのデータに分散し、分散された 3 つのデータのうち 2 つを組み合わせれば、元の情報が復元できます。さらに分散処理時に真性乱数を使用すれば、単独の分散情報からでは、元の情報を解読することは不可能となります。NTT Com が独自開発した、論理演算のみを使用した処理方式を採用することで、従来の秘密分散法では困難とされていた大容量のデータを高速に処理することができるため、スムーズな情報の分散、復元が可能です。NTT Com の秘密分散法は NTT Com から特許出願中で、今回の研究開発はこの秘密分散法を応用することにより新たな方式を確立しました。

■本件に関する照会先

株式会社日立製作所 システム開発研究所 企画室［担当：森］
電話：044-959-0325

学校法人東京理科大学 産学官連携課［担当：近藤］
電話：03-5228-8090

NTT コミュニケーションズ株式会社 第二法人営業本部第二営業部［担当：松岡］
電話：03-6700-7305

独立行政法人 情報通信研究機構 連携研究部門 委託研究グループ［担当：下谷、千葉]
電話：042-327-7286

以上

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL 等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。
