リニューアル可能な暗号認証システム

Renewable Authentication and Encryption System

栃窪　孝也 TOCHIKUBO Kouya
岡田　光司 OKADA Koji
遠藤　直樹 ENDOH Naoki

現在利用されている暗号認証技術応用システムでは，使用する暗号認証方式が固定されているのが一般的であり，暗号認証方式の変更を考慮した設計がされていない。したがって，システムの暗号認証方式を変更しようとする場合，ばく大な時間と金額が必要となる。また，標準化やデファクト化への追随が困難であり，情報の価値を考慮した効率的な暗号化を行うことができない，などの問題も生ずる。そこで当社は，使用する暗号認証方式をネットワークを介して安全かつ効率よく更新／改善でき，上記のデメリットの解決策となる，リニューアル可能な暗号認証システムを開発した。

Currently available application systems with authentication and encryption functionality generally use "fixed" encryption and authentication primitives. Alteration or upgrading of these primitives is basically out of their scope. Therefore, considerable time and expense are required to improve the security of the system. Another demerit is that it is difficult to introduce standardized or de facto standard algorithms into the system. Hence, from the viewpoint of application, it is not possible to select or introduce the encryption algorithm that is most appropriate for the value of the information.

We have developed a renewable authentication and encryption system that solves the above problems by allowing primitives to be securely and efficiently altered via the network.

1 まえがき

インターネットに代表されるオープンなネットワークの急速な普及によって，ネットワークを利用した様々な業務が，現在盛んに行われている。このような業務は便利である反面，第三者による通信データの盗聴や改ざん，不正コピーや偽造，他人になりすましてのアクセスなど，様々な問題が生ずる。そこで，それらの問題の対策として暗号認証技術が利用されており，暗号認証技術が組み込まれたシステムが，電話やファクシミリ（FAX）の暗号通信，衛星放送やケーブルテレビの限定受信，電子商取引，デジタルコンテンツ配信業務などで用いられている。

このような背景から，安全性の高い暗号方式の設計に関する研究が活発に行われており，それと同時に，暗号方式の安全性評価のため解読法の研究も盛んに行われている。

一方，新しい解読法やコンピュータの性能の飛躍的な向上により，使用されている暗号方式の規格の変更や使用している暗号方式が解読されるといったことは現実に起こりうる。暗号方式が解読された場合，ネットワークを介した電子商取引やコンテンツ配信などの事業は，組み込まれている暗号技術の安全性の基に成り立っているため，暗号方式を変更しないかぎり，そのシステムをそのまま使用することができなくなる。すなわち，システムの暗号方式の変更などの処置が完了するまで業務を停止しなければならないこともありうる。

しかし，暗号化技術を組み込んだ従来のシステムの多くは，規格標準化などの理由によりシステムの仕様が一度決まると，それと同時に，使用する暗号方式が固定されるため，システムのセキュリティレベルもほぼ固定されてしまう。更に，新たな標準化やデファクト技術を導入するなど，暗号認証方式の更新を考慮して設計されておらず，変更箇所はシステム全体に及ぶこともある。また，更新処理をシステムの端末1台1台に対して行う必要があり，それにかかるコストはばく大なものになる。

また，現在，ネットワークを介して送信される情報は，テキストデータに限らず，音楽データ，画像データなど多様化しており，従来のシステムでは，システムで使用できる暗号方式が固定されているため，情報の価値を考慮した効率的な暗号化ができないのが現状である。

以上のことから，ここでは，システムで使用する暗号認証方式を，ネットワークを介して安全かつ効率よく更新することで，システムのセキュリティレベルの維持・向上，コスト削減，標準化への追従などが可能な，リニューアル可能な暗号認証システムの概要を説明し，今後の暗号認証システムのあるべき姿を述べる。

2 情報セキュリティにおけるリニューアルの必要性

2.1 暗号認証技術の安全性

はじめに，従来の暗号認証システムにおいてもっとも使わ

れている，秘密鍵（かぎ）暗号方式DES（Data Encryption Standard）と公開鍵暗号方式RSA（Rivest-Shamir-Adleman）の安全性について述べる。暗号の解読とは，当事者ではない第三者が暗号文を元の平文に戻すことであり，通常，平文とそれに対応する暗号文のペアや，公開されている暗号方式のパラメータなどから鍵を特定することを意味する。

DESは，1977年に米国商務省標準局によって制定されて以来，米国政府内はもちろん一般商用でも幅広く使われている。特に，金融分野においては，これまで欧米を中心に幅広い業務に利用されてきた。DESの解読法に関する研究は，制定当初から活発に行われており，94年には平文と暗号文のペア2^{47}組を使い，線形解読法により解読に成功している。近年では，コンピュータの性能の向上により，鍵の全数探索でも解読することが可能となっている。なお，現在では，DES Crackerと呼ばれるDES解読の専用マシンを25万ドルで開発し，DES Crackerと10万台のパソコン（PC）を用いて，22時間15分で解読に成功している（**表1**）。

表1．DESの解読レポート
Data Encryption Standard (DES) cracking report

	解読方法	解読時間
94年	線形解読法（平文と暗号文のペア2^{47}組＋PC 12台）	50日
97年	鍵の全探索（PC 1万台）	150日
98年	鍵の全探索（PC 800万台）	39日
98年	鍵の全探索（DES Cracker）	56時間
99年	鍵の全探索（DES Cracker＋PC 10万台）	22.25時間

公開鍵暗号方式は，秘密鍵暗号方式の鍵の配送やデジタル署名などに使われている。現在もっとも使われている公開鍵暗号方式は，78年に発表されたRSAである。RSAは，大きな数の素因数分解の困難さを安全性の根拠としている。現在よく知られているRSAの解読法（素因数分解法）には，$p-1$法，$p+1$法，*Fermat*法，二次ふるい法，数体ふるい法などがある（**表2**）。

これらの素因数分解のアルゴリズムの進歩と，計算機の性能向上により，80年代前半には，公開鍵のサイズは512ビットが推奨されていたが，96年には推奨サイズが1,024ビットに変更されている。そして，将来的にはより長い鍵のサイズの使用が予想される。

表2．素因数分解レポート
Prime factorization report

	アルゴリズム	ビット長
94年	二次ふるい法	425ビット
96年	数対ふるい法	430ビット
99年	数対ふるい法	463ビット
99年	数対ふるい法	512ビット

2.2 なぜリニューアルが必要か

2.1節で述べたように，暗号方式とは決して万能なものではなく，解読法の研究と近年のコンピュータ技術の発達及びコストパフォーマンスの改善により，暗号方式の強度は時間とともに相対的に低下するため，それに伴う変更が必要となる。

制定されてから20年以上も経つDESを例に挙げると，これまで欧米を中心に銀行間通信，CD（Cash Dispenser），ATM（Automatic Tellers Machine）などの端末と銀行のホストコンピュータ間でのPIN（暗証番号）の送信などに利用されてきた。しかし，98年7月の専用解読マシンによるDESの解読が報道されて以来，米国銀行協会ではDESの使用を中止し，DESが使用されている部分をDESより安全性の高いTriple DESに移行している。しかし，これらのシステムは，暗号方式の更新を考慮した設計になっていなかったため，ソフトウェアの変更など比較的容易な更新処理で済んだ機器は，全体の1/3程度であったのに対し，全体の2/3の機器では，ハードウェアの変更などの処置を行う必要があった。暗号方式の更新という点では，更に今後は，Triple DESからDESの後継暗号AES（Advanced Encryption Standard）へのシステム変更なども予想される。

また，公開鍵暗号方式に関しては，RSAに代わる公開鍵暗号方式として，現在，楕円（だえん）離散対数問題に基づく楕円曲線暗号が注目されている。楕円曲線暗号の公開鍵の鍵長は，RSAの公開鍵の鍵長に比べて1/8のサイズで，RSAと同程度の安全性が得られるという利点があり，今後，RSAから楕円曲線暗号へのシステム変更なども予想される。

以上のことから，今後の暗号認証システムには，使用している暗号方式の安全性が低下したときの対策技術や暗号認証方式を更新するリニューアルメカニズムが必要となってくる。

3 リニューアル可能な暗号認証システム

3.1 システムの要求仕様

暗号認証方式の更新を実現しようとする場合，更新処理は，システムの端末全体に対し，ネットワークなどを利用し効率よく行う必要がある。しかし，暗号方式の中には輸出規制の対象になっているものもあり，暗号方式の外部への流出問題などを考慮する必要がある。

したがって，リニューアル可能な暗号認証システムでは，使用する暗号認証方式を管理するセンターを設置し，次のような機能を実現する必要がある。

⑴ 使用している暗号認証方式を，ネットワークを介して効率よく更新可能であること。

⑵ センターが，各端末が使用している暗号方式の情報

及び暗号方式の使用権限情報を管理し，暗号認証方式を更新する際，当事者以外には更新不可能であること。

また，PCなどのセキュリティ機能のないオープンアーキテクチャ機器で，暗号認証技術を用いたアプリケーションが多数動作しているという点や，現在，利用されている暗号方式は，アルゴリズム公開の暗号方式だけではなく，アルゴリズム非公開の暗号方式も利用されているという点を考慮すると，次の点も検討する必要がある。

⑶ アルゴリズム非公開の暗号方式も，ネットワークを介して更新可能であること。

⑷ アルゴリズム非公開の暗号方式のプログラムや暗号通信用の鍵など，端末の記憶装置に蓄積されている秘密情報の保護が可能であること。

システムの使用環境などにより，⑶，⑷は除外される場合がある。しかし，ここでは，PCなどを含めたあらゆる使用環境を想定し，リニューアル可能な暗号認証システムの要求仕様を⑴～⑷と定める。

3.2 システム構成

提案システムは，鍵配送及び暗号認証方式の配布・管理を行うセンターと複数の端末から構成される（**図1**）。

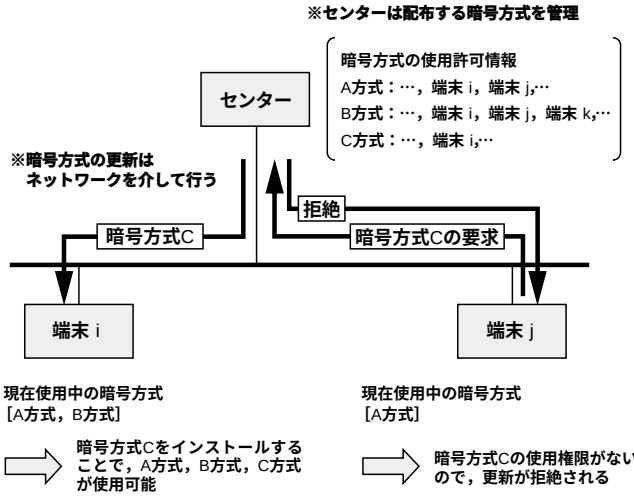

図1．リニューアル可能な暗号認証システム　暗号認証方式の配布，管理を行うセンターと複数の端末から構成される。
Renewable authentication and encryption system

端末は，コアモジュール，暗号認証モジュール，鍵管理モジュール，操作アプリケーションから成り，コアモジュールと暗号認証モジュール間には暗号認証方式API（Application Programming Interface），コアモジュールと鍵管理モジュールの間には鍵管理方式API，そして，コアモジュールと操作アプリケーションの間には操作APIが定義されている（**図2**）。

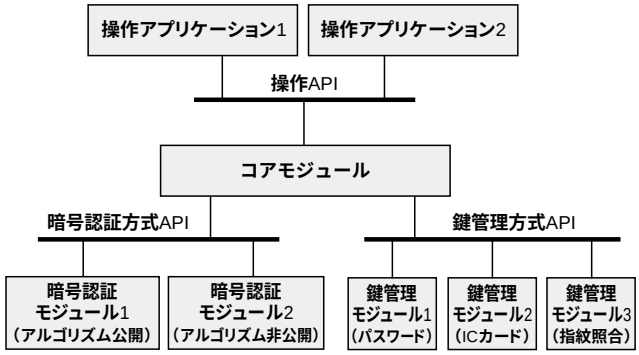

図2．端末の構成　端末は，三つのAPIにより，ブロック長，鍵長の異なる多様な暗号認証方式を組み込むことができる。
Structure of client

提案システムでは，一つの暗号認証方式が一つの暗号認証モジュールに対応する。また，提案システムの暗号認証モジュールは，秘密鍵暗号方式，公開鍵暗号方式，そしてハッシュ関数である。なお，暗号認証モジュールには，次のようなアルゴリズム情報が付随する。

⑴ アルゴリズム識別子
⑵ ブロック長
⑶ 鍵長
⑷ パラメータ情報

このアルゴリズム情報により，ブロック長，鍵長が多様な暗号認証方式を扱うことができる。更に，提案システムでは，アルゴリズム公開の暗号方式だけではなく，アルゴリズム非公開の暗号認証方式の利用も想定している。アルゴリズム非公開の暗号方式に対応する暗号認証モジュールは，通常，暗号化した状態で端末に保存され，実行時にだけ復号され処理を行う構成になっている。また，提案システムの暗号認証モジュールは，暗号認証方式APIに基づいて作成されている。したがって，暗号認証方式APIにより，様々な鍵長，ブロック長の新しい暗号方式をシステムに組み込むことが可能となる。

鍵管理モジュールは，端末の秘密鍵や，アルゴリズム非公開の暗号方式に対応する暗号認証モジュールを復号するための暗号認証方式復号鍵などの管理を行う。また，提案システムには，次のような様々な鍵管理モジュールを，使用環境やシステムのセキュリティレベルに応じて選択し使用することが可能である。

⑴ パスワードによる鍵管理モジュール
⑵ ICカードによる鍵管理モジュール
⑶ 指紋照合による鍵管理モジュール

なお，鍵管理モジュールは，鍵管理方式APIに基づいて作成される。

また，提案システムは，様々なアプリケーションでの利用を想定し，操作APIを定めている。したがって，操作API

を利用することで，提案システムを様々なアプリケーションに組み込むことが可能である。

このように，提案システムでは三つのAPIを定めることで柔軟なシステム構築を可能にしている。

3.3 暗号認証方式のリニューアル

提案システムでは，使用している暗号認証方式が破られた場合や，暗号認証方式の新しい規格が定まった場合に，新規暗号認証方式をネットワークを介し安全かつ効率よく更新することが可能である。暗号認証方式を更新していくことで，システムのセキュリティレベルの維持・向上が可能となり，また，陳腐化を防ぐことができる。暗号認証方式の更新は，端末からの要求，あるいはセンターからの指示により行われる。端末が暗号認証方式の更新を行う場合，はじめにセンターと端末間で相互認証を行う。相互認証が正しく行われない場合は，暗号認証方式の更新は行わない。

次に，センターは，要求している端末に新規暗号認証方式の使用権限があるかをチェックする。端末に使用権限がない場合は，更新は行わない。使用権限がある場合は，図3のような更新情報を作成する。

更新情報の送信は，端末が利用可能な暗号認証方式と，センターと端末の共有している鍵とにより行われる。端末は，センターから送られてきた更新情報に改ざんなどがあるかを検証し，なければ更新情報を復号し，更新情報の完全性検証データから，更新が正常に行われたかを検証する。更新が正常に行われたら，端末に新規暗号認証方式を登録する。

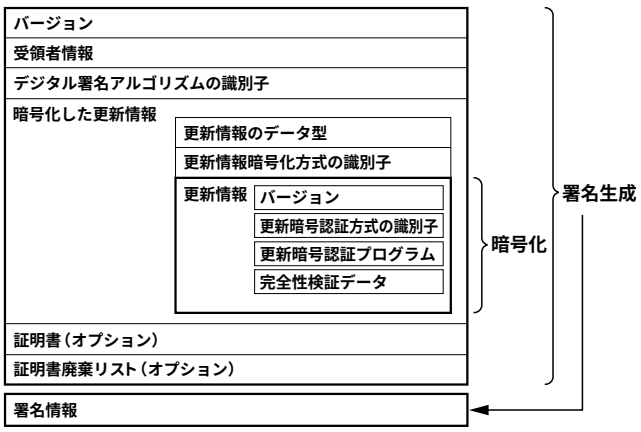

図3．更新情報の詳細　このような更新情報により，ネットワーク経由で新しい暗号認証方式を安全に送ることができる。
Details of renewal information

4 あとがき

ここでは，リニューアル可能な暗号認証システムの概要を述べた。暗号認証方式を新しいものに安全かつ効率よく更新する機構を設けることで，使用している暗号方式が破られた場合の暗号認証方式の変更や，暗号方式の新規格への対応などが可能となり，システムの陳腐化を防ぐことができる。

また，これからのネットワーク社会では，様々な種類のコンテンツがネットワークを通じてやり取りされる。そして，それに伴って，システムも多様な暗号認証方式に対応する必要があり，システムのセキュリティレベルを維持していく必要が生ずるため，暗号認証方式のリニューアル技術を，今後の暗号認証システムに取り入れていく所存である。

文　献

(1) 松井　充.“DES暗号の線形解読法（I）”. The 1993 Symposium on Cryptography and Information Security. SCIS93-3C, 1993.

(2) DESCHALL. homepage, http://www.frii.com/~rcv/deschall.htm

(3) 岩下直行, ほか.“金融分野における情報セキュリティ技術の国際標準化動向”. IMES DISCUSSION PAPER SERIES No.98-J-29, 1998, 25p.

(4) 栃窪孝也, ほか.“リニューアル可能な暗号認証システムの検討”. 情報処理学会論文誌. **41**, 8, 1999, p.2121－2128.

栃窪　孝也　TOCHIKUBO Kouya
e-ソリューション社 SI技術開発センター SI技術担当。
暗号・情報セキュリティ技術の研究・開発に従事。電子情報通信学会会員。
Systems Integration Technology Center

岡田　光司　OKADA Koji, D.Eng.
e-ソリューション社 SI技術開発センター SI技術担当，工博。
暗号・情報セキュリティ技術の研究・開発に従事。
Systems Integration Technology Center

遠藤　直樹　ENDOH Naoki
e-ソリューション社 戦略企画室参事。
情報セキュリティ技術及び同技術応用システムの開発に従事。
電子情報通信学会，日本セキュリティマネジメント学会会員。
e-Solution Co. Strategic Planning Div.