リニューアル可能な暗号認証システムの検討

栃窪孝也[†] 岡田光司[†]
遠藤直樹[†] 岡本栄司[††,†††]

現在，システムで使用している暗号方式の安全性が低下した場合の対策が重要な問題になっている．従来の暗号認証システムは，使用する暗号方式が固定されているものが多く，また，使用する暗号方式を複数の中から選択して利用可能な暗号方式が固定されていないシステムでも，暗号方式の安全かつ効率の良い変更を考慮した設計がされていない．したがって，システムの暗号方式を変更しようとする場合，莫大な時間と金額が必要となる．また，システムで使用す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を行うことができないという問題も生じる．そこで，本論文では，システムで使用する暗号方式をネットワークを介して安全かつ効率良く更新可能であり，情報の価値を考慮して暗号方式を選択し使用可能な「リニューアル可能な暗号認証システム」を提案する．

Renewable Authentication and Encryption Systems

Kouya Tochikubo,[†] Koji Okada,[†] Naoki Endoh[†]
and Eiji Okamoto[††,†††]

In many authentication and encryption systems, the encryption algorithm of the system is fixed. These systems are not designed to renew the encryption algorithm of the system. Therefore in these systems, it takes much time and money to change the encryption algorithm of the system and all plaintexts have to be encrypted with the fixed encryption algorithm. In this paper, we propose a renewable authentication and encryption system and the renewal protocol. In the proposed system, an encryption algorithm can be used according to the value of a plaintext. The system can renew the encryption algorithm of the system securely and efficiently through computer networks in order to improve the security level of the system.

1. はじめに

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さかんに行われている．このような業務は便利である反面，通信データの第三者による盗聴や改ざん，データの不正コピーや偽造，他人になりすましてのアクセス等の様々な問題が生じる．そこで，それらの問題の対策技術として暗号認証技術が用いられている．

このような背景から，安全かつ効率の良い暗号方式の設計に関する研究がさかんに行われており，それと同時に，暗号方式の安全性の評価のため解読法の研究もさかんに行われている．また，近年のコンピュータの性能の飛躍的な向上に応じて，暗号方式の規格も変更されている．

システムで使用している暗号方式の安全性が低下すれば，それにともなった方式変更が必要になってくるが，従来のシステムは，システムで使用する暗号方式が固定されているものが多く，また，使用する暗号方式を複数の中から選択して利用可能な暗号方式が固定されていないシステムでも，暗号方式の安全かつ効率の良い変更を考慮した設計がされていない．したがって，従来のシステムでは，暗号方式の変更には莫大な時間と費用が必要になる．米国銀行協会における CD，ATM 等の端末の DES から Triple DES への移行が顕著な例である．

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欧米を中心に銀行間通信，CD，ATM 等の端末と銀行のホストコンピュータ間での PIN（暗証番号）の送信等に DES が利

† 株式会社東芝 SI 技術開発センター
SI Technology Center, TOSHIBA Corporation
†† ウィスコンシン大学暗号セキュリティセンター
Center for Cryptography, Computer and Network Security, University of Wisconsin, Milwaukee
††† 東邦大学理学部
Faculty of Science, Toho University

用されている．しかし，制定されてから 30 年以上も経つ今日では，DES Cracker と呼ばれる DES 解読の専用マシンが 25 万ドル程度で開発され，DES Cracker と 10 万台の計算機を用いて鍵の全探索により 22 時間 15 分で解読に成功している[7]．1998 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，現在 DES が使用されている部分を Triple DES に移行している．しかし，これらのシステムは，暗号方式のリニューアルを考慮した設計になっていなかったため，全体の 2/3 の機器に対し，ハードウェアの変更等の処置を行う必要があった[11]．さらに今後は，Triple DES から DES の後継暗号 AES（Advanced Encryption Standard）へのシステム変更等も予想される．

また，RSA の安全性に関しても，素因数分解のアルゴリズムの進歩と，計算機の性能の向上により，1980 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，1996 年には推奨サイズが 1024 ビットに変更された．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ている．また，RSA に代わる公開鍵暗号方式として，現在，楕円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等も予想される．

しかし，システムの暗号方式に変更が必要な場合，ネットワークを介しての変更では，暗号方式・秘密鍵等の秘密情報の外部への流出等の安全性を考慮する必要があり，ネットワークを介さない各端末個別の変更では，システムのすべての端末 1 台 1 台に変更を加えなければならないといった効率の面を考慮する必要がある．

以上のことから，本論文では，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良く更新することで，システムのセキュリティレベルの維持・向上が可能な「マルチメディア通信に適したリニューアル可能な暗号認証システム」を検討し，リニューアル可能な暗号認証システムおよび，ネットワークを介した暗号認証方式・鍵の更新プロトコルを提案する．

2. リニューアル可能な暗号認証システム

2.1 システムの要求仕様

米国の銀行の CD，ATM 等の端末での DES から Triple DES への変更の例のように，従来の暗号認証システムでは，システムの暗号認証方式の更新を考慮して設計されておらず，仮に暗号認証方式の更新を行う場合，端末 1 台 1 台に対し個別に大幅な変更を行う必要がある．

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，画像データ等多様化しており，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．

暗号方式をリニューアルすることが可能なシステムを実現しようとする場合，システムの端末全体に対し，新規暗号方式を効率良く更新する必要がある．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等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，

(1) システムで使用している暗号認証方式・鍵等の秘密情報をネットワークを介して効率良く更新可能
(2) センターが，各端末が使用している暗号方式の情報および暗号方式の使用権限情報を管理し，秘密情報を更新する際，当事者以外には更新不可能

という機能を実現する必要がある．また，PC 等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，

(3) 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
(4) 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等，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

という点も検討する必要がある．システムの使用環境等により，(3)，(4) は除外される場合がある．しかし，本論文では，PC 等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の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 (1)〜(4) と定める（**図 1**）．なお，検討するシステムには鍵配送および暗号認証方式の配布・管理を行うセンターを設置している．

上記の要求仕様を実現するリニューアル可能な暗号

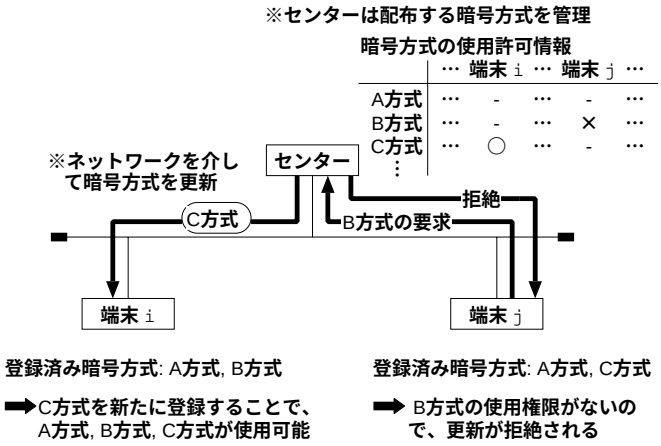

図 1 リニューアル可能な暗号認証システム
Fig. 1 Renewable authentication and encryption systems.

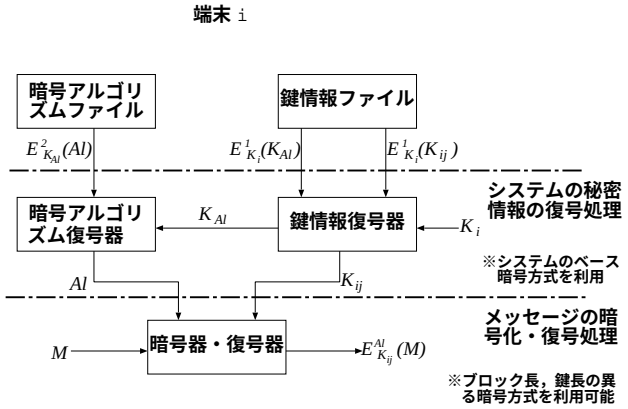

図 2 システムの構成
Fig. 2 Composition of the system.

認証システムを構築することで，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等が可能となり，システムの陳腐化を防ぐことができる．従来のシステムでは，暗号認証方式の更新を行う場合，端末 1 台 1 台に対し個別に大幅な変更を行う必要があるのに対し，本システムは，更新はネットワークを介して安全かつ効率良く行うことが可能になる．さらに，従来のシステムでは，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かったのに対し，本システムでは，暗号化するデータの種類，機密度によって使用する暗号方式を選択することができるため，情報の価値を考慮した効率的な暗号化が可能になる．

2.2 提案システムの構成

2.1 節で述べた要求仕様を満足する「リニューアル可能な暗号認証システム」を具体的に構成する（**図 2**）．ここで提案するシステムでは，鍵長の長いセキュアな暗号方式をシステムのベースの暗号方式とし，暗号方式のリニューアルの際にベースの暗号方式を利用するものである．なお，提案システムでは，システムのベースの暗号方式自体もリニューアルすることが可能である．ただし，ベースの暗号方式が破られてしまった場合は，4 章で説明する自己復号型秘密情報通信の手法を応用した方法や，リニューアルの処理をオフラインで行う等の処理が必要である．以下では $E^{x}_{K}(y)$ によって暗号方式 x，鍵 K を用いたメッセージ y の暗号文を表し，$a|b$ によって a と b の連接を表す．

各端末は，システムで使用する暗号方式のアルゴリズム（プログラム）を複数保存する暗号アルゴリズムファイルと暗号通信に用いる秘密鍵等を保存する鍵情報ファイルを備える．そして，暗号通信の際に使用する暗号方式と秘密鍵をそれぞれ暗号アルゴリズムファ

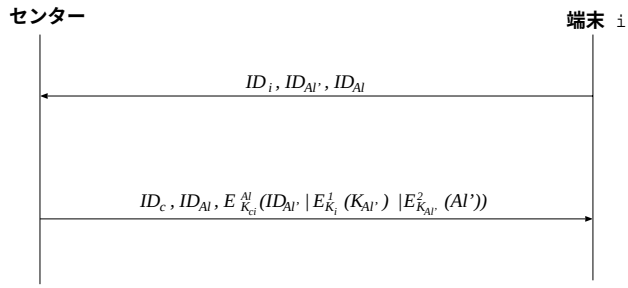

図 3 更新プロトコル 1
Fig. 3 Renewal protocol 1.

イルおよび鍵情報ファイルから読み込み，暗号器・復号器でメッセージの暗号化，暗号文の復号化を行う．暗号アルゴリズムファイルに保存されている暗号アルゴリズム Al は暗号方式 E^2，暗号方式固有の鍵 K_{Al} によって暗号化されている．また，鍵情報ファイルに保存されている暗号方式固有の鍵および，暗号通信に用いる秘密鍵は暗号方式 E^1，端末固有の鍵 K_i によって暗号化されている．

実際の通信は以下のように行われる．端末 i が端末 j へ暗号方式 Al でメッセージ M を送信する場合，鍵情報ファイルから暗号化された暗号方式固有の鍵 $E^1_{K_i}(K_{Al})$，i–j 間の暗号通信用の秘密鍵 $E^1_{K_i}(K_{ij})$ を呼び出し，鍵情報復号器で端末固有の鍵 K_i によって復号化し，K_{Al} を暗号アルゴリズム復号器，K_{ij} を暗号器・復号器へ送る．また，暗号アルゴリズムファイルから $E^2_{K_{Al}}(Al)$ を呼び出し，暗号アルゴリズム復号器において K_{Al} によって復号化し，Al を暗号器・復号器へ送る．最後に暗号器・復号器は，暗号方式 Al のブロック長，鍵長，各種パラメータ等の情報を基に K_{ij}，M を Al に入力する．そして，Al は K_{ij}，M から暗号文 $E^{Al}_{K_{ij}}(M)$ を作成し端末 j に送る．端末 j における受信した暗号文の復号化の処理も同様に行うことができる．

なお，本システムでは，各暗号方式のブロック長，鍵長，各種パラメータ等の記述方法，および，各暗号方式への入出力は，あらかじめ定義している入出力インタフェースに基づく．このような入出力インタフェースを定めることで，ブロック長，鍵長等が異なる様々な暗号方式を利用することが可能となる．

本システムでは，暗号アルゴリズムが非公開な暗号方式に対するリニューアルをも考慮に入れるため，暗号アルゴリズムファイルには暗号アルゴリズムが暗号化されて保存されているが，アルゴリズム公開の暗号方式に対しては暗号化せずに保存し，使用することも可能である．また，暗号アルゴリズムファイルに複数の暗号方式を保存しておくことで，情報の価値にふさわしい強度の暗号を使用可能である．さらに，暗号アルゴリズムや鍵情報等の秘密情報を暗号化して保存しているため，他人のみならず利用者本人からも秘密情報を保護することも可能となり，外部および内部の不正利用を防止することができる．

2.3 ネットワークを介した暗号認証方式の更新プロトコル

ここでは，2.2 節で提案したシステムでの暗号方式更新プロトコルを 2 つ示す．

なお，本システムでは，どの端末がどのような暗号方式を利用しているかの情報はセンターから得ることができる．

更新プロトコル 1：センターに新規暗号方式 Al' および暗号方式固有の鍵 $K_{Al'}$ を要求（**図 3**）

(1) 端末 i はセンターに，自分の ID 情報 ID_i，要求する暗号方式の ID 情報 $ID_{Al'}$ および更新の際に使用する暗号方式の ID 情報 ID_{Al} を送り更新要求を出す．

(2) センターは，端末 i が暗号方式 Al' の使用が認められているかをチェックし，使用が認められている場合は，端末 i にセンターの ID 情報 ID_c，ID_{Al}，$E^{Al}_{K_{ci}}(ID_{Al'}|E^1_{K_i}(K_{Al'})|E^2_{K_{Al'}}(Al'))$ を送信する．

更新プロトコル 2：他の端末に新規暗号方式 Al'，センターに暗号方式固有の鍵 $K_{Al'}$ を要求（**図 4**）

(1)-a 端末 i は端末 j に，自分の ID 情報 ID_i，要求する暗号方式の ID 情報 $ID_{Al'}$ および更新の際に使用する暗号方式の ID 情報 ID_{Al} を送り更新要求を出す．

(1)-b 端末 j は，端末 i に端末 j の ID 情報 ID_j，ID_{Al}，$E^{Al}_{K_{ij}}(ID_{Al'}|E^2_{K_{Al'}}(Al'))$ を送信する．

(2)-a 端末 i はセンターに，自分の ID 情報 ID_i，要求する暗号方式固有の鍵の ID 情報 $ID_{K_{Al'}}$ および更新の際に使用する暗号方式の ID 情報 ID_{Al}

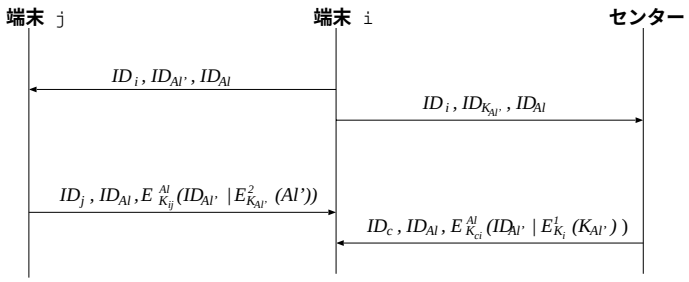

図 4 更新プロトコル 2
Fig. 4 Renewal protocol 2.

を送り更新要求を出す.

(2)-b センターは，端末 i が暗号方式 Al' の使用が認められているかをチェックし，使用が認められている場合は，暗号方式固有の鍵 $K_{Al'}$ を暗号方式 E^2，端末固有の鍵 K_i によって暗号化し，端末 i にセンターの ID 情報 ID_c，ID_{Al}，$E^{Al}_{K_{ci}}(ID_{K_{Al'}} | E^1_{K_i}(K_{Al'}))$ を送信する.

どちらのプロトコルでも，端末は送られてきた更新情報に手を加えることなく，送られてきた更新情報をそのまま暗号アルゴリズムファイルおよび鍵情報ファイルに保存するだけで更新が可能である．また，更新プロトコル 2 は，通信回数が増えるが，更新情報を分散して要求できるので，センターの負荷を減らすことができる．更新プロトコル 2 において，端末が他の端末から暗号方式の要求があった場合は，要求している暗号方式が他の端末へ送信することが可能な方式の場合にのみ送信を行う.

なお，暗号方式の更新の際に，センターは要求者が更新する暗号方式を使用可能かどうかチェックすることで，暗号方式の輸出規制等の暗号方式の管理にも対応可能である.

3. 考　　察

3.1 暗号認証方式更新時のセキュリティ

はじめに，2.2 節で述べたリニューアル可能な暗号認証システムの秘密情報更新時の主な脅威に対する安全性を考察する．ネットワークを介してデータをやりとりする場合でも，データの盗聴，改ざん等の問題が生じるが，リニューアル可能な暗号認証システムでは暗号認証方式のプログラム，暗号通信用の鍵等の秘密情報をネットワークを介してやりとりする必要がある．また，提案システムでは，送られてくる情報がプログラムなので，コンピュータウィルス等の問題も生じる．提案システムでは，更新情報を送信する際，センターが更新を要求している端末に暗号方式の使用権限があるかをチェックし，また，更新情報はセンターと要求者間の秘密鍵により暗号化して送信されるので，正規の端末以外への更新情報の流出を防ぐことが可能である．また，センターと端末による相互認証，送信情報の署名で，更新情報の改ざんの検出や，センターまたは端末へのなりすましの防止が可能となる．なお，署名方式や認証方式も破られる可能性があるため 2 つ以上の方式を保持する必要がある．提案システムでは，更新情報の改ざん，送信者の検証に用いる署名方式や認証方式（プログラム）も同様にシステムのベースの暗号方式を利用することで，ネットワークを介してリニューアル可能な仕組みになっている.

3.2 端末蓄積データのセキュリティ

2.2 節で提案したシステムでは，暗号方式のプログラムは，暗号方式固有の鍵で暗号化し，鍵情報は端末固有の鍵により暗号化して蓄積されている．これは，セキュリティ機能がない PC 等でもアルゴリズム非公開な暗号方式を利用可能にするためである．しかし，システムの構成によっては，端末固有の鍵の管理方法により，扱える暗号方式が異なる場合が生じる．端末固有の鍵の管理法としては，IC カードを利用した場合のような端末の利用者本人にも鍵が分からない管理法とパスワードのように端末の利用者本人には鍵（パスワード）が分かる管理法の 2 つがある．端末の利用者本人には鍵が分かる管理法では，鍵情報復号器に使用している暗号方式 E^1，暗号アルゴリズム復号器に使用している暗号方式 E^2 を解析できるシステムでは，暗号アルゴリズムファイルに保存されている（アルゴリズムが非公開な）暗号方式のプログラムが流出する恐れがある．なお，システムで使用する暗号方式がアルゴリズムが公開なものだけの場合は，システムの構成を簡潔にすることが可能である.

4. システム全体のリニューアル

2.2 節では，システムにベースとなる暗号方式を用

意し，端末の暗号ファイル内の暗号方式をネットワークを介して更新可能なシステムを提案した．ここでは，鍵情報復号器に使用している暗号方式 E^1，暗号アルゴリズム復号器に使用している暗号方式 E^2 のベースとなる暗号方式を含むシステム全体のリニューアルについて検討する．システム全体のリニューアルを行うためには，ネットワークを介して送られてきた更新情報（新規システムプログラム）がセンターから送られたものかを検証し，また，改ざんが行われていないことを検証する必要がある．送信される情報は新規システムのプログラムなので，送信相手を認証する手段および改ざんを検出する手段がなければ，悪意を持った第三者が更新情報と偽ってコンピュータウィルスを送り，端末のデータをすべて破壊するといったことも可能になる．

ここでは，鍵のみを共有している状態での，送信相手の認証，受信データの改ざんが検出可能な方法として，自己復号型秘密情報通信の手法を改良した更新プロトコルを提案する（**図 5**）．この手法を用いることで，センター–端末間の暗号通信用の秘密鍵の共有だけでシステムの更新が可能になる．はじめに，自己復号型秘密情報通信方式の概要を説明する．

従来の暗号通信では，当事者間の暗号化鍵の共有はもちろんのこと，暗号方式の共有も必要である．そこで，当事者が暗号方式を共有していない場合の暗号方式の共有の問題の解決策として，1996 年に南ら[15]によって自己復号型秘密情報通信方式が提案された．自己復号型秘密情報通信方式とは，情報の送信者が暗号文と復号アルゴリズムを同時に送り，受信者は受け取った暗号文をあらかじめ共有している鍵と，同時に送られてきた復号アルゴリズムを用いて復号化するといった方式である．

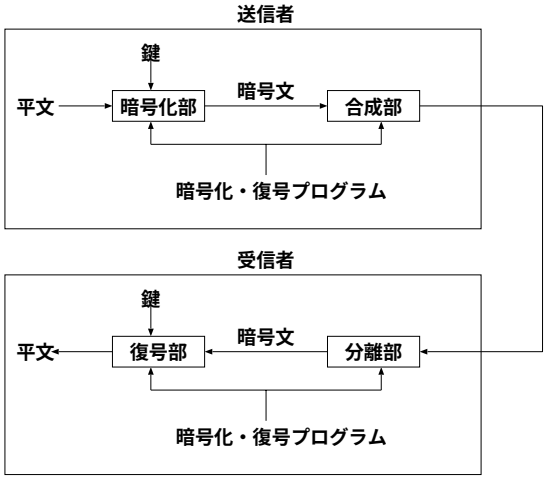

図 5 自己復号型秘密情報通信のモデル
Fig. 5 Self-deciphering secret communication.

この方式は，インターネットメールシステム等のような，システムのマシンや OS が多種多様で，受信者が送信者を特定できない状況での使用を想定している．

したがって，システムの端末に特定のマシンや OS に依存しない仮想マシンとしてインタープリタ言語 Scheme を持たせ，その仮想マシンにおいて送られた復号アルゴリズムにファイル入出力のコマンドやシステムコマンド等のシステムを破壊しうるコマンドがあるかをチェックしてから暗号文の復号化を行う仕組みになっている．

しかし，この方式では，インタープリタ言語を使用しているため処理速度に問題が残る．また，送信者の確認や受け取った暗号文や復号アルゴリズムの改ざんの検出等は不可能である．したがって，送られてきた暗号プログラムをそのまま使用して暗号文を他の端末に送ることはできず，また，復号化したデータが正しいものであるかを確かめることができない．

本システムでは，あらかじめ決められたシステム環境のみを考えればよいため処理の遅いインタープリタ言語を用いる必要はなく，新規暗号方式はコンパイル済みの実行形式を送信すればよい．そこで，自己復号型秘密情報通信方式をリニューアル可能な暗号認証システムでの更新プロトコルに適応するために次のような改良を行う．

- 暗号化・復号化プログラムはその署名とともに送信
- 送信する暗号化・復号化プログラムとその署名は，送信者と受信者が共有している暗号方式により暗号化

このような改良を行うことで，送られてきた暗号化・復号化プログラムが正しい送信者からの改ざんのない正しいデータであるかを検証できる．この方法は，送られてきた復号化プログラムが正しい送信者からの改ざんのない正しいデータであることを確かめてから復号化の処理を実行するので，送られてきたプログラムのコードを解析することなしにコンピュータウィルス等の問題に対処できる．

5. ま と め

本論文では，従来の暗号認証システムの

- 使用している暗号方式が破られた場合，システムを利用することができない，
- 暗号方式の更新を考慮して設計されていないため，暗号方式の新規格等に対応できない，
- 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，

といった問題点の解決策としてリニューアル可能な暗号認証システムを提案した．

本論文で提案したリニューアル可能な暗号認証システムは，暗号認証方式・鍵を新しいものに更新することで，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等が可能となり，システムの陳腐化を防ぐことができる．また，従来のシステムでは，暗号認証方式・鍵の更新を行う場合，端末 1 台 1 台個別に行う必要があるのに対し，提案システムは，更新はネットワークを介して効率良く行うことが可能である．さらに，従来のシステムでは，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かったのに対し，提案システムでは，情報の価値を考慮した効率的な暗号化が可能である．また，提案システムは，

- アルゴリズム非公開の暗号方式の使用
- セキュリティ機能のない機器の利用

等も想定したシステムである．

今後の課題としては，提案システムの様々な暗号認証システムへの応用やシステムの実装等があげられる．

謝辞 本研究の一部は，情報処理振興事業協会「独創的情報技術育成事業」の一環として行われたものである．

参 考 文 献

1) 岡本栄司：暗号理論入門，共立出版 (1993).
2) 岡本龍明，山本博資：現代暗号，産業図書 (1997).
3) Diffie, W. and Hellman, M.: Exhaustive cryptanalysis of the NBA data encryption standard, *Computer*, No.10, pp.74–84 (1977).
4) Biham, E. and Shamir, A.: Differential Cryptanalysis of the full 16-round DES, *CRYPTO'92*, LNCS, Vol.740, pp.487–496 (1992).
5) 松井 充：DES 暗号の線形解読法（I），*The 1993 Symposium on Cryptography and Information Security*, SCIS93-3C (1993).
6) 松井 充：DES 暗号の線形解読法（III），*The 1994 Symposium on Cryptography and Information Security*, SCIS94-4A (1994).
7) DESCHALL homepage, `http://www.frii.com/~rcv/deschall.htm`
8) Distributed Net homepage, `http://www.distributed.net/des`
9) Electronic Frontier Foundation homepage, `http://www.eff.org/descracker.html`
10) 下山武司：次期暗号標準 AES をどう考えるか?, 電子情報通信学会基礎・境界ソサイエティ大会予稿集，pp.252–253 (1998).
11) 岩下直行，谷田部充子：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).
12) 宇根正志，太田和夫：共通鍵暗号を取り巻く現状と課題—DES から AES へ，*IMES DISCUSSION PAPER SERIES*, No.98-J-27 (1998).
13) 栃窪孝也，遠藤直樹，岡本栄司：マルチメディア通信に適したリニューアル可能な暗号認証システムの検討，第 58 回情報処理学会全国大会論文集 (1999).
14) 新保 淳：変形 ElGamal 署名の設計，暗号アルゴリズムの設計と評価ワークショップ (1996).
15) 南 向鎮，岡本栄司，篠田陽一，満保雅浩：自己復号型秘密情報通信のためのプラットフォームの開発研究，*The 1996 Symposium on Cryptography and Information Security*, SCIS96-01C (1996).
16) 日本 CATV 技術協会：デジタル有線テレビジョン放送限定受信方式，日本 CATV 技術協会標準規格 JCTEA STD-001-1.0 (1997).
17) 川村信一：暗号機能付き IC カードの実用化動向とその課題，電子情報通信学会総合大会予稿集，TA-4-3 (1997).

(平成 11 年 11 月 30 日受付)
(平成 12 年 6 月 1 日採録)

栃窪 孝也（正会員）

平成 8 年東京理科大学理学部応用数学科卒業．平成 10 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．同年（株）東芝入社．現在，情報理論，暗号・情報セキュリティの研究開発に従事．電子情報通信学会会員．

岡田 光司

平成 6 年東京工業大学工学部電気・電子工学科卒業．平成 11 年同大学大学院理工学研究科電気・電子工学専攻博士課程修了．工学博士．同年（株）東芝入社．現在，暗号理論・情報セキュリティの研究開発に従事．

遠藤　直樹

昭和 54 年東京工業大学理学部応用物理学科卒業．昭和 56 年同大学大学院理工学研究科応用物理学専攻修士課程修了．同年（株）東芝入社．現在，同社 SI 技術開発センター主幹．情報セキュリティ技術および応用システムの研究開発に従事．電子情報通信学会，日本セキュリティ・マネジメント学会各会員．

岡本　栄司（正会員）

昭和 48 年東京工業大学工学部電子工学科卒業．昭和 53 年同大学大学院電子工学専攻博士課程修了．工学博士．同年日本電気（株）中央研究所入社．平成 3 年北陸先端科学技術大学院大学情報科学研究科教授．平成 11 年よりウィスコンシン大学暗号セキュリティセンター兼東邦大学理学部教授．グラフ理論，通信理論，数理計画，アルゴリズム，情報セキュリティをはじめとする情報数理システムの教育・研究に従事．平成 2 年電子通信学会論文賞，平成 5 年情報処理学会ベストオーサ賞受賞．著書「暗号理論入門」「電子マネー」等．IEEE シニア会員．ACM，IACR（International Association for cryptologic Research），電子情報通信学会，情報理論とその応用学会，応用数理学会，日本セキュリティ・マネージメント学会各会員．