招待論文

SSL 証明書の事例に見る暗号アルゴリズムの移行問題
——収束しない 2010 年問題——

島岡　政基[†a)]　　松本　泰[†]

Issues on Transition of Cryptographic Algorithm Learned from a Case Study of SSL Certificates

Masaki SHIMAOKA[†a)] and Yasushi MATSUMOTO[†]

あらまし　社会基盤化しつつある現代の情報通信は，暗号技術なくしては成り立たない．しかし，この暗号技術が情報通信に広く取り込まれたのは，それほど古い話ではなく，今後解決すべき課題も数多く残されている．その課題の一つに暗号アルゴリズムの移行問題がある．情報通信に広く取り込まれた暗号技術であるが，ここで利用されている暗号アルゴリズムは，徐々に脆弱化していき，世代交代が必要になっている．情報通信技術や情報通信基盤は，こうした暗号アルゴリズムの世代交代に伴う移行に対応できる必要がある．しかし暗号技術を利用した情報通信技術が基盤化するほどに，この暗号アルゴリズムの移行は困難なものになると予想される．本論文では，既に広く利用されている SSL 及び SSL 証明書の事例を示すことにより移行問題の複雑さと重要さを説明するとともに，今後の取り組むべき課題について考察を行う．

キーワード　暗号アルゴリズム，暗号移行可能性，ルート証明書，SSL 証明書，認証局

1. まえがき

1.1 暗号技術の社会基盤化

社会基盤化しつつある現代の情報通信は，暗号技術なくしては成り立たない．しかし，この暗号技術が情報通信に広く取り込まれたのは，それほど古い話ではない．暗号技術で利用される暗号アルゴリズムの標準化が確立し，暗号技術が通信プロトコル等に広く取り入れられたのは，1990 年代後半からになる．その後のインターネットの爆発的な普及とともに，暗号技術も様々な情報通信に広く組み込まれ，その安全性に基づき，情報通信を利用する組織や人の信頼関係の構築にも用いられるようになった．そして現在では情報通信技術の社会基盤化が進み，その中での暗号技術は，「社会的信頼関係」の構築に不可欠なものとなってきた．

こうした社会基盤化した暗号技術の一つに，パスワードやクレジットカード情報など機密情報の送受信を実現する Secure Sockets Layer (SSL) (注1)が挙げられる．

1.2 暗号アルゴリズムの脆弱化

一方，暗号技術において広く利用されてきた既存の暗号アルゴリズムは，その多くが暗号アルゴリズムの強度を計算量的安全性に基づいているが，計算機処理性能が年々向上するに伴い計算量的安全性も相対的に低下するため，暗号アルゴリズムは徐々に脆弱化してくる．脆弱化が進むと，想定された暗号強度が保てなくなり解読できる可能性が高まるため，より計算量的安全性の高い他の暗号アルゴリズムに移行したり，同じアルゴリズムでもより計算量的安全性の高い鍵長の鍵へ移行するといった世代交代が必要となる．しかし，現在の基盤化されつつある情報通信技術と暗号技術は，**2.** で後述するように必ずしも暗号アルゴリズムの世代交代を前提に設計されているわけではない．

直近では，公開鍵暗号に広く用いられている鍵長

† セコム株式会社 IS 研究所，三鷹市
Intelligent Systems Laboratory, SECOM Co., Ltd., SECOM SC Center, 8–10–16 Shimorenjaku, Mitaka-shi, 181–8528 Japan
a) E-mail: m-shimaoka@secom.co.jp

(注1)：SSL 3.0 [30] の後継プロトコルとして Transport Layer Security 1.2 [15] があり，合わせて SSL/TLS と表記する場合もあるが，本論文ではこれらを総称して SSL と表記する．

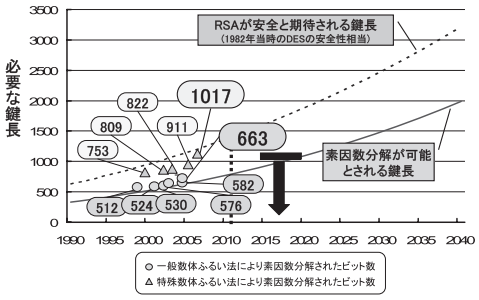

図 1　RSA の計量的安全性低下 [1]
Fig. 1　Decreasing computational security of RSA.

1024 ビットの RSA 鍵（以下，1024 ビット RSA）が，図 1 に示すとおりもはや十分な計算量的安全性が確保できなくなりつつあるとして，より暗号強度の高い 2048 ビット RSA などへの世代交代が各方面で推進されている [2], [3]．また，公開鍵暗号と組み合わせることでディジタル署名に用いられる主なハッシュアルゴリズムの一つである SHA-1 についても，2005 年に安全性低下が報告され [4]，より暗号強度の高い SHA-256 などへの世代交代が推奨されるとともに，更に暗号強度の高い次世代ハッシュアルゴリズムの開発が検討されている状況 [5] にある．この直近の暗号アルゴリズム脆弱化問題は，米国 National Institute of Standards and Technology (NIST) が 1024 ビット RSA と SHA-1 からの移行期限を 2010 年末までとした [2] ことから「暗号アルゴリズムの 2010 年問題」[6] として知られている(注2)．

1.3　本論文の構成

本論文では，暗号アルゴリズムの世代交代と世代交代に伴う移行問題を考えるために，暗号技術が情報通信基盤にどのように取り込まれているか整理する．このためまず **2.** では，暗号アルゴリズムの世代交代と移行を検討する上で考慮すべき暗号技術のレイヤの考え方と，特に重要な論点として「暗号移行可能性(注3)の確保」「多数の関係者間の調整」の二つを示している．続く **3.** ～ **5.** では，具体的な移行の事例として，社会基盤化されているといってもよい公開鍵暗号技術の応用である SSL に焦点を当てる．**3.** で SSL の基本的な仕組みとルート証明書の配布について解説した上で，**4.** 及び **5.** では，**2.5** で挙げる二つの課題のうち，社会基盤における課題として「多数の関係者間の調整」について，SSL におけるルート証明書の移行の事例を示す．最後に **6.** で，公開鍵暗号技術や SSL に限らず，暗号アルゴリズムの世代交代に関して，今後取り組むべき課題を示している．

2.　暗号技術のレイヤ

社会基盤として利用される暗号技術という視点から見た場合，現代の暗号技術は，おおむね「アルゴリズム」,「標準」,「実装」,「社会基盤」という四つ程度のレイヤがあると考えられる．本章では，これら四つのレイヤについて解説するとともに，暗号アルゴリズムの移行問題において特に重要な課題について述べる．

2.1　アルゴリズム

暗号が脆弱化していく背景には，暗号解読に利用する計算機スピードの向上がある．そのため時代の要請に応じたバランスの良い暗号アルゴリズムや鍵長が求められる．特に，新しい暗号アルゴリズムの場合は，その安全性が独立した評価機関（日本であれば CRYPTREC など）による客観的な評価が求められる．しかし，客観的な評価には非常に長い年月と専門的知識が必要とされるという課題もある．例えば NIST が標準化した共通鍵暗号の Advanced Encryption Standard (AES) は 1997 年 9 月の公募開始から 2001 年 3 月の標準仕様公開までに約 3 年半を要し，その大半が評価機関による評価に割かれた．

2.2　標　　準

ここでの標準は，暗号アルゴリズム自体ではなく暗号を利用したプロトコル等の標準を意味する．Internet Engineering Task Force (IETF) 等の標準化団体で開発された暗号技術が組み込まれた初期のプロトコルの多くは，特定の暗号アルゴリズムに依存した形で設計されてきた．暗号アルゴリズムの世代交代に迅速に対応するためには，複数の暗号アルゴリズムを利用できる必要がある．既に様々なプロトコルを策定してきた標準化団体としては，まず既存のプロトコルについて暗号移行可能性を分析する必要があり，これは手間の掛かる作業となる．そして，暗号移行可能性が不十分なプロトコル等は適宜改訂していくことになるが，その際には脆弱化した暗号アルゴリズムによる後方互換

(注2)：過去に有名な 2000 年問題 [31] は，時刻処理に起因した問題であり，2000 年が絶対的なマイルストーンであったのに対して，暗号アルゴリズムの 2010 年問題においては，2010 年はあくまで NIST が目標とした移行期限であり，2011 年以降平穏化するたぐいのものではないことに注意する必要がある．
(注3)：IETF における (Cryptographic) algorithm agility や Hash agility，マイクロソフト社における Cryptographic agility などの考え方を総称して，ここでは暗号移行可能性と呼ぶことにする．

性攻撃 (Downgrade Attack) に対しても配慮する必要がある [16]．これは安全性を確保する一方で，後方互換性を絶ち切ることでもあるため，実装への普及の遅れが課題となってくる．

2.3 実　　装

暗号技術が組み込まれた製品には，特定の暗号アルゴリズムに依存した形で実装されているものも多い．オンラインでソフトウェア更新可能な OS などであっても，モジュール化されていないカーネルコードなどがそうした実装であると，一般的なソフトウェア更新の仕組みでは対応できず，システム停止を伴う更新作業などが必要となる場合がある．つまり，実装においても暗号移行可能性を確保したアーキテクチャ設計，モジュール構成が求められる [7]．

また，近年，暗号技術が取り込まれた組込み機器が急速に普及しているが，これらの暗号アルゴリズムの移行問題も不可避である．しかし，ソフトウェア更新による対応が難しい，あるいはソフトウェア更新を前提とすることが難しい組込み機器などでは実質的に暗号移行可能性を確保することができないケースもあり得る．典型的な例として IC カードや携帯機器などが知られているが，ネットワークアプライアンスなどにもこういった問題が生じる可能性があることを認識しておく必要がある．こうしたケースでは，暗号アルゴリズムの移行を想定して機器のライフサイクルを考慮する必要がある．一方，暗号移行可能性を確保するのであれば，組込み機器特有の課題の一つである高モジュール性の確保の難しさや，場合によっては暗号処理モジュールのチップ化による性能確保，オフライン運用によるソフトウェア更新の難しさといった事情も含めて対応を検討する必要がある．

2.4 社 会 基 盤

情報通信に取り込まれた暗号技術は，いまや情報通信を利用する組織や人同士の信頼関係の構築に不可欠な存在となっている．具体的には，暗号技術で利用する「鍵」が安全であることを前提として，通信の安全性やエンティティの本人性が担保されている．そして，こうした暗号技術を取り込んだ情報通信が社会基盤化したことにより，暗号技術は社会的信頼関係の形成にも不可欠な存在となってきた．ここでいう「社会基盤化」とは，様々な人，組織，デバイス，サービスが利用する基盤となることであり，そこにおける社会的信頼関係とは，そうした様々なエンティティの多様な信頼関係を意味する．

暗号アルゴリズムを移行するということは,「鍵」を新しい暗号アルゴリズムで生成されたものに更新するという作業にほかならない．多数の関係者が新しい「鍵」を安全に利用するにあたっては，関係者の利用する環境における標準や実装の対応がまず必要であり，レイヤ縦断的に検討を進める必要がある．また鍵の更新後は，セキュリティ確保の観点から，どのタイミングで古い「鍵」を無効化するか [8] についても考慮する必要があるが，これは後方互換性を断ち切ることを意味しており，社会基盤化した技術の移行にあたっては解決が難しい問題となってくる [9]〜[11]．こうした問題の解決には，社会基盤を利用する「多数の関係者間の調整」が不可欠と考えられる．

2.5 移行問題における論点

表 1 に示すように，暗号アルゴリズムの世代交代に伴う移行には，レイヤごとにそれぞれ課題が存在する．このうち現状における対応が特に不十分な課題として,「標準」及び「実装」における「暗号移行可能性の確保」,「社会基盤」における「多数の関係者間の調整」が挙げられる．本節ではこれら二つの課題について解説し，**3.** 以降では,「暗号移行性の確保」及び「多数の関係者間の調整」の事例として SSL におけるルート証明書の移行問題を説明する．

[暗号移行可能性の確保]

暗号移行可能性の確保は，標準と実装における今後の課題である．標準における暗号移行可能性とは，IETF において (Cryptographic) Algorithm Agility や Hash Agility などと呼ばれ，ハッシュアルゴリズムも含めた暗号アルゴリズムの移行可能性として 2005 年ごろからセキュリティエリアを中心に [12], [13]，PKIX WG [14] や TLS WG [15] など様々な WG で議論されてきている．

しかし，前述のように暗号技術を取り入れたすべてのプロトコルについて暗号移行可能性を分析し，適切な改訂を行い，これを反映した実装が普及するまでには非常に時間がかかるものと見られている [16]．

実装における暗号移行可能性に対する取組みは，例えばマイクロソフト社の Cryptographic Agility [7] などが知られているが，基本的にはベンダ内部に閉じた取組みであるため，オープンになっている情報があまり多くない．また，日本においては携帯電話の 2048 ビット RSA 対応が現在も続いている．2005 年以前に発売された機種には対応していないものが多く，未対応機種の利用者がいる限り，携帯電話向けコンテンツ

表 1　暗号アルゴリズム移行のレイヤと課題
Table 1　Layers and issues in cryptographic algorithm transition.

レイヤ	関係者	一般的な課題	SSL の事例
アルゴリズム	CRYTPTREC や NIST などの暗号アルゴリズム評価機関	暗号アルゴリズムの評価期間	N/A
標準	IETF などの標準化団体	暗号移行可能性の確保	プロトコルの暗号アルゴリズム移行可能性
実装	マイクロソフト社などの製品ベンダ	暗号移行可能性の確保	携帯電話の 2048 ビット RSA 対応や SHA-256 対応など
社会基盤	暗号技術を利用する関係者	多数の関係者間の調整	CA/Browser Forum などの合意の場

プロバイダなどは 2048 ビット RSA に移行しづらいといった状況にある．

［多数の関係者間の調整］

これまでのレイヤでは，例えばアルゴリズムの設計者，標準化団体，実装ベンダというように主体者が明確であったが，暗号技術を社会基盤化するのは特定の関係者ではなく，暗号技術を社会基盤として利用する多数の関係者である．このため，特定の関係者による判断，決定によって問題を解決できるわけではなく，多数の関係者間で調整を行う場や機会が必要であり，また調整を円滑に進めるには，一部の関係者のみに限定しない開かれた場や機会が提供されることが理想と考えられる．

3. SSL の仕組みとルート証明書の配布

本章では，情報通信に暗号技術が取り入れられ社会基盤化した事例として SSL の仕組みと，社会基盤化した SSL において重要な役割を果たすルート証明書の配布について説明する．

3.1 SSL によるサーバ認証の仕組み

SSL によるサーバ認証は，端末利用者がインターネット経由でアクセスしているサーバの名称や同サーバ運営者の組織等を確認するために実行される．基本的には，① SSL 証明書に記載されたサーバの名称等の確認と，②当該サーバが生成するディジタル署名(注4)の検証によって実行される．上記①については，PKI（Public Key Infrastructure，公開鍵暗号基盤）における認証局（CA：Certification Authority）が，サーバの名称や同サーバの署名検証鍵等が記載された SSL 証明書を当該サーバに対して発行し，端末利用者が SSL 証明書をサーバから入手して記載内容を確認することで実行される．その際，SSL 証明書の一貫性の確認が必要となるが，SSL 証明書に対して生成された認証局のディジタル署名を検証することで実行可能となる．端末利用者が認証局のディジタル署名を検証するためには認証局の署名検証鍵が必要となるが，こうした署名検証鍵は，当該認証局によって発行される「ルート証明書」等の形態であらかじめ PC 等に組み込まれる．上記②は，SSL 証明書に含まれるサーバの署名検証鍵を用いることで実行可能となる．

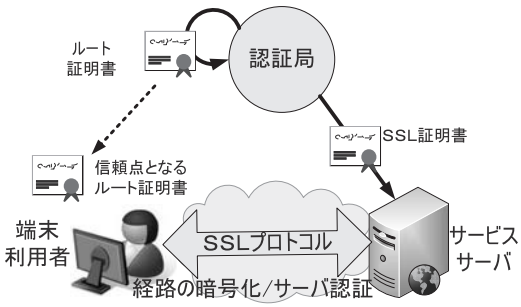

図 2　ルート証明書・SSL 証明書を用いたサーバ認証（概念図）
Fig. 2　Server authentication using root certificate and SSL certificate.

最も単純な「一つの認証局が SSL 証明書を発行している」という場合（図 2 参照），認証局がサーバに SSL 証明書を発行するほか，認証局が自分自身に対して「ルート証明書」を生成・発行する．ルート証明書には，当該認証局の署名検証鍵が含まれるほか，その認証局のディジタル署名が施される．このようにしてルート証明書に含まれる署名検証鍵が，SSL 証明書に施された認証局のディジタル署名を検証する鍵として用いられる．ルート証明書の署名検証鍵がサーバ認証を実行する際の要となることから，同署名検証鍵（あるいはその鍵を含んだルート証明書）は「信頼点」と呼ばれている．また，こうした信頼点であるルート証

(注4)：ここでのディジタル署名は，公開鍵暗号をベースとするディジタル署名方式によって実現される．すなわち，ディジタル署名の生成は公開鍵暗号の秘密鍵（署名生成鍵）によって行われ，ディジタル署名の検証は公開鍵暗号の公開鍵（署名検証鍵）によって行われる．

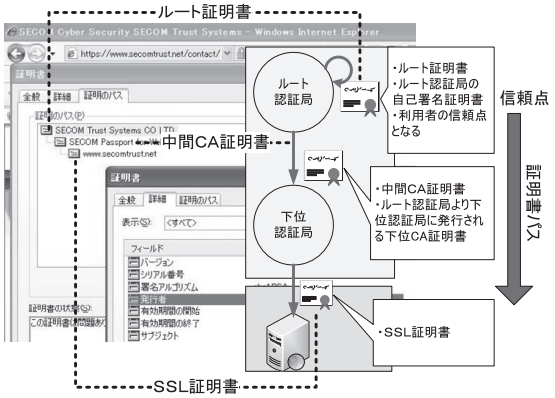

図 3　証明書パスを構成する証明書群と実際のブラウザ上での表示

Fig. 3　Certification path and certificates in web browser.

明書に対応する認証局は「ルート認証局」と呼ばれる．

現在，多くの SSL 証明書は，ルート認証局から直接発行されるのではなく，ルート認証局以外の認証局（下位認証局）から発行されている（図 3 参照）．この場合，ルート認証局は下位認証局の署名検証鍵を含む証明書（中間 CA 証明書と呼ばれる）を同認証局に対して発行するが，この中間 CA 証明書にはルート認証局のディジタル署名が施される(注5)．また，SSL 証明書には下位認証局のディジタル署名が施されることとなる．この結果，SSL 証明書のディジタル署名を検証する際には，①ルート証明書の署名検証鍵を信頼点として中間 CA 証明書のディジタル署名をまず検証し，②次に，中間 CA 証明書に含まれる（下位認証局の）署名検証鍵を用いて SSL 証明書のディジタル署名を検証するという流れとなる．この信頼点としてのルート証明書から SSL 証明書までは「証明書パス」と呼ばれ，信頼点から SSL 証明書を検証することは「証明書パスの検証」と呼ばれる．図 3 では下位認証局が一つの場合を示しているが，下位認証局が複数存在して階層を構成し，他の下位認証局に対して中間 CA 証明書を発行するケースも実際には存在する．この場合，証明書パスには，信頼点としてのルート証明書，最下層となる SSL 証明書，双方の証明書の間に位置するすべての中間 CA 証明書が含まれる．

このように，SSL によるサーバ認証の実行には，端末利用者が PC 等に組み込まれるルート証明書を「正しいルート証明書」として何らかの理由で信頼することが必要となる．その上で，端末利用者は，①信頼点となったルート証明書の署名検証鍵から「証明書パスの検証」を行うことでサーバの SSL 証明書を検証し，②上記検証が成功した場合には，SSL 証明書の記載内容とサーバのディジタル署名の検証によってアクセス先のサーバを確認することができる．暗号アルゴリズムの観点からは，証明書パス中のすべての証明書に施されているディジタル署名が十分な安全性を確保していることが必要となる．このディジタル署名には，脆弱化が進んでいる 1024 ビット RSA の公開鍵暗号と SHA-1 のハッシュアルゴリズムが多く利用されており，これらの移行が必要になっている．

3.2　SSL のルート証明書の組込み

ルート証明書は製品の出荷時に組み込まれるケースが多い．例えば，マイクロソフト社の Windows OS の場合，出荷時に「証明書ストア」と呼ばれる部分に数多くのルート証明書が同社によって格納される．その後，ルート証明書を追加したり削除したりする必要がある場合においては，マイクロソフト社によって提供される Window Update(注6)を実施すること等によって対応することができる仕組みとなっている．また，その他の OS，携帯電話等においても，どのルート証明書を OS やブラウザに組み込むかを決定するのは，次に示す各ベンダである．

（1）　PC の OS ベンダ（PC の OS に組み込まれるルート証明書を決定）

（2）　ブラウザベンダ（ブラウザに組み込まれるルート証明書を決定）

（3）　携帯キャリヤ（携帯電話等に組み込まれるルート証明書を決定）

（4）　地デジの双方向サービスに対応した受信者機器やゲーム機等のベンダ（各機器に組み込まれるルート証明書を決定）

PC 等に組み込まれるルート証明書が信頼点として機能するためには，端末利用者が「信頼できるルート証明書が組み込まれている」ことを認識できる必要があり，上記の各ベンダがルート証明書の組込みをどのような基準で決定したかが重要な要素となる．端末利

(注5)：また，下位認証局から更に下位の認証局に中間 CA 証明書が発行されている場合もある．

(注6)：Windows Update は，Windows OS やそれを利用した各種ソフトウェアの更新を行うために，ネットワークや CD-ROM によってマイクロソフト社から提供されたソフトウェアを PC 等にインストールする仕組みである．Windows Update を実行する際も PKI が利用されており，Windows OS に組み込まれたマイクロソフト社のルート証明書を信頼点としている．

用者は，基本的には，各ベンダが決定して組み込んだルート証明書を所与の信頼点として利用することになる．一方，サーバ運営者は，当該サーバにアクセスする端末利用者がどのようなルート証明書を利用できる環境を有しているかを考慮して SSL 証明書を購入すると考えられる．

このように，ルート証明書の組込みベンダは，サーバ認証がどのような証明書によって実行されるかにおいて大きな役割を果たしている．

3.3 ルート証明書の組込み基準

組み込まれるルート証明書に関連する基準として，①マイクロソフト・ルート証明書プログラムが挙げられるほか，②ルート証明書の暗号アルゴリズムに関するものとして，「EV 証明書のためのガイドライン [24]」が挙げられる．

3.3.1 マイクロソフト・ルート証明書プログラムと WebTrust for CA

SSL 証明書は 1990 年代中頃から利用が始まったが，当初はルート証明書の組込みに関するルール等は存在しなかった．こうした状況に対して，マイクロソフト社は，2002 年の Windows XP のリリース時に OS（MS-Windows）に組み込むルート証明書に関する基準をマイクロソフト・ルート証明書プログラムとして公表した [17]．本プログラムでは，組み込むルート証明書の認証局に対して，米国とカナダの公認会計士協会が策定した認証局の監査基準 “WebTrust for CA” [18] に基づく第三者監査を受けていることが条件として求められた(注7)．

このように，マイクロソフト・ルート証明書プログラムと WebTrust for CA は，同社の OS に組み込まれるルート証明書について，認証局の運用体制の確認という点で一定の品質を保証するものと理解することができる．本プログラム開始後，マイクロソフト社の OS には多数のルート証明書が組み込まれるようになり，2009 年 9 月 22 日時点で 291 のルート証明書が組み込まれている [19]．これらは，例えば，マイクロソフト社の代表的なブラウザのインターネットエクスプローラにおいて信頼点として参照されているほか，グーグル社のブラウザ Chrome も Windows OS に組み込まれているルート証明書を信頼点として参照している(注8)．このように，本プログラムと WebTrust for CA 等の第三者監査の枠組みは数多くのルート証明書の利用に関して大きな影響力をもっているといえる．

3.3.2 EV 証明書のためのガイドライン

本ガイドライン策定の主な要因は，証明書発行時の審査方法(注9)が WebTrust for CA の監査等において認証局の裁量にゆだねられており，証明書発行申請元の組織の実在性確認を行わずに SSL 証明書を発行する認証局が出現したことである．このような SSL 証明書，いわゆる DV SSL 証明書（Domain Validated certificate）はフィッシング詐欺等に悪用されるおそれがあり [20]，SSL のサーバ認証に対する信頼の低下につながった．SSL の暗号通信時にブラウザに表示される「南京錠マーク(注10)」は，通信経路が暗号化されていることを示すものではあるが，サーバの運営組織の確認を必ずしも示すわけではないといえる．

また，ルート証明書や SSL 証明書の暗号アルゴリズムの観点からは，WebTrust for CA 等に特段の基準がなく認証局の裁量となっていたために，後方互換性を優先したい利用者ニーズとコストを優先して，減価償却の進んだ 1024 ビットルート認証局を用いて安価な SSL 証明書を発行するベンダが増えた．そうした中，1024 ビット RSA 等の安全性低下が顕著となり，証明書の暗号アルゴリズムの安全性確保に何らかの基準の策定が必要との認識が高まった．

これらを背景として，SSL 証明書発行時の審査基準の厳格化を主たる目的とした CA/Browser Forum (CABF) が，主要な認証局ベンダ及びブラウザベンダによって 2006 年に設立された(注11)．CABF では証明書の新たなカテゴリーとして SSL 証明書発行時に WebTrust for CA よりも厳格な審査を必要とする EV

(注7)：現在では，WebTrust for CA 以外に欧州の ETSI において標準化が行われている ETSI TS 101 456 [32]，ETSI TS 102 042 [33] による第三者監査も認められており，欧州ではこうした事例が増えている．

(注8)：マイクロソフト社以外の代表的なブラウザである Firefox や Opera においては，組み込むルート証明書の基準を独自に設定しており，マイクロソフト・ルート証明書プログラムの直接的な影響を受けない．ただし，双方とも，当該ルート証明書の認証局が WebTrust for CA 等の第三者監査を受けていることを組込みの条件としている．

(注9)：一般に，SSL 証明書の発行審査としては，発行申請者（ドメイン）の本人性確認や発行申請者が属する組織の実在性確認が行われる．

(注10)：初期のブラウザにおいて，「SSL で接続した状態」を「南京錠が閉まった状態」のアイコンで表したことから SSL において「南京錠マーク」が一般的になった．

(注11)：CABF 参加のブラウザベンダは，EV 証明書のサーバにアクセスしたことを認識しやすくするためのブラウザの実装を行った．従来の南京錠マークが通信の暗号化の判別しかできなくなったことに対し，EV 証明書対応のブラウザでは，EV 証明書であることをアドレス・バーの色変化（緑色に変化）によって認識できるほか，発行対象の組織名と認証局を南京錠マークのクリックによって確認できるという仕組みが採用された．複数の認証局とブラウザのベンダの協力と合意により，信頼性がより高い証明書の枠組みが提供されたといえる．

証明書（Extended Validation Certificate）を導入し，その指針として EV 証明書のためのガイドラインを 2007 年に公開した [24]．証明書発行審査に関して，本ガイドラインは，EV 証明書発行時に発行申請元の組織の実在性確認をより厳格に行うことを規定した(注12)．また，本ガイドライン公開と同時に，認証局の監査として，従来の Web Trust for CA に実在性確認の運用等に関する基準を追加した “WebTrust EV Program” が開始された．

証明書の暗号アルゴリズムについては，EV 証明書の証明書パスを構成する SSL 証明書，中間 CA 証明書，ルート証明書のディジタル署名で使用されている RSA 公開鍵暗号の鍵長とハッシュアルゴリズムの扱いがガイドラインに明記された．このように暗号アルゴリズムの安全性を一定以上に設定することで，信頼点としてのルート証明書への端末利用者による信頼が向上するという効果があると考えられる．

CABF の設置以前は，複数のブラウザのベンダ等と複数の認証局の間において，こうした暗号アルゴリズムなどの利用方針に関する合意の場はなかった．今後は，CABF が，証明書の暗号アルゴリズムの問題なども含め，SSL 証明書，ルート証明書の信頼に関して一定の役割を果たしていくと期待される．

3.4 PC 以外に組み込まれるルート証明書

PC で利用する OS やブラウザ以外でも，SSL 証明書の利用は増加している．特に我が国においては，携帯電話における SSL 証明書の利用が顕著である．その他，地デジの双方向サービスに対応した受信者機器やゲーム機においても SSL が利用されている．

これらの機器におけるルート証明書の組込みの状況は PC において利用される OS やブラウザの状況とは大きく異なる．第 1 に，ルート証明書を組み込むベンダ（携帯電話であれば携帯キャリヤ）が「マイクロソフト・ルート証明書プログラム」のようなルート証明書組込みのための基準を公開するケースは見られていない．第 2 に，一つの機器に組み込まれているルート証明書の数が少ない(注13)．これは，携帯電話等の機器に搭載されるメモリ量に制約があり，組込み可能なルート証明書の数の制約が強いためと見られる．こうした場合，組込みベンダは，接続先となるサーバの SSL 証明書の信頼点としてどの程度広く採用されているかを重視する傾向がある．一般に，古くから存在するルート証明書の方が高いシェアを有していると考えられることから，そうしたルート証明書が組み込まれる可能性が高いと見られる．また，メモリ上の制約は，新しいルート証明書の組込みのハードルとなり得るため，ルート証明書移行を困難にする要因であると考えられる．第 3 に，PC 以外のルート証明書の組込みベンダの多くは CABF に加入しておらず，複数の認証局との合意の場がない．

これらの点を踏まえると，携帯電話等の分野におけるルート証明書の信頼性確保や暗号アルゴリズム移行問題の検討は，PC の分野の場合に比べてより困難であると考えられる．

4. SSL 証明書やルート証明書の更新に向けた動向

本章では，社会基盤化した情報通信技術の暗号アルゴリズムの移行問題として SSL の 1024 ビット RSA のルート証明書に関する移行の動向について説明する．

4.1 ルート証明書における 1024 ビット RSA の安全性低下の影響

現在，多くのルート証明書に利用されている 1024 ビット RSA は，現時点の技術環境を前提にすると 2010 年代後半に安全性低下が深刻化する可能性が濃厚と評価されている．暗号アルゴリズムの脆弱化に伴う問題は，ルート証明書だけではないが，社会基盤，及び「社会的信頼関係」という視点からルート証明書の安全性低下の影響は，やはり大きなものがある．ルート証明書は，通常，中間 CA 証明書を介して数多くの SSL 証明書の検証に用いられており，ルート証明書の安全性低下は多くのサーバの認証を無意味なものにしてしまう．ルート証明書の脆弱化は，SSL 証明書により築かれた社会的信頼関係の崩壊につながる．このルート証明書の入換えには「多数の関係者の調整」が必要になり時間がかかる．時間がかかるゆえに，その対応は喫緊の問題になる．

4.2 利用が推奨される暗号アルゴリズムのルート証明書

現時点で推奨される 2048 ビット RSA，SHA-1 のルート証明書は，2000 年以降に発行され始めた．しかし，既存の SSL 証明書がこうした新しいルート証明書

(注12)：具体的には，発行対象を法人のみに限定するとともに，法人の確認のために登記事項証明書等の提出を求め，証明書には登記情報に基づく記載を求める内容となっている．

(注13)：例えば，2000 年に発売されたエヌ・ティ・ティ・ドコモ社の最初の第 3 世代携帯電話では，4 枚のルート証明書が組み込まれていた．その後，2009 年 12 月の最新機種においては 22 枚のルート証明書が組み込まれているものの，PC の場合と比較すると非常に少ない．

を信頼点として必ず利用するわけではない．サーバ運営者が，マイクロソフト社の Windows 2000 以前の古い OS のブラウザにおいても SSL によるサーバ認証を実行可能にしようとした場合，1990 年代発行の古いルート証明書を信頼点とする SSL 証明書を利用せざるを得ない [21]．実際，古い携帯電話の場合には，携帯電話の仕様自体が 2048 ビット RSA に対応していないケースがある．例えば，2000 年に発売されたある携帯電話では，組み込まれたルート証明書（四つ）すべてが 1024 ビット RSA のルート証明書である．

このように，古いルート証明書ほど既存の SSL 証明書の信頼点として広く利用されているのが現状である．今後も古い OS の端末利用者からのアクセスを可能にするという姿勢を維持する限り，PC に古いルート証明書が残るほか，ルート証明書の更新ができない携帯電話や組込機器においては新製品であっても 1024 ビット RSA のルート証明書が組み込まれて出荷され続ける可能性が高い．

なお，ハッシュアルゴリズムの移行については，PC の場合，Windows XP SP2 よりも古い OS において SHA-256 に対応していないほか，携帯電話の場合には大半の機種が SHA-256 に対応していない．こうしたことから，SHA-256 のルート証明書を利用できる余地は現時点では極めて限定されているといえる．

4.3 暗号アルゴリズムの移行を促す動き

4.3.1 方向性と現状

ルート証明書の暗号アルゴリズム移行を進めるためには，古い暗号アルゴリズムのルート証明書の使用を停止する必要がある．その場合，通信プロトコルとしての後方互換性を維持しない（一部の古い OS やブラウザによる接続を許容しない）という方針の採用が求められる．しかし，**4.2** のとおり，可能な限り幅広い端末利用者からのアクセスを可能にしたいというサーバ運営者のインセンティブに反するものであるとともに，通信プロトコルの後方互換性を確保しながら発展してきたインターネットの常識と異なる考え方であることから，サーバ運営者，認証局ベンダ，ブラウザベンダ等の関係者が足並みをそろえて対応するという状況を安易に期待することはできない．また，ブラウザベンダ等が古いルート証明書を削除するためのプログラム（例えば，Windows Update）を準備したとしても，どの程度の端末利用者がそれを実行するかは不明である．

ただし，暗号アルゴリズムの移行を促す動きが皆無というわけではない．そうした動きの一つは，暗号アルゴリズムを明記した EV 証明書とそのガイドラインの導入であり，もう一つは，マイクロソフト・ルート証明書プログラムにおける暗号アルゴリズム移行に関する記述の追加である．こうした動きは「多数の関係者間の調整」において，少なからぬ影響力をもつものと期待される．

4.3.2 EV 証明書とそのガイドラインの導入

3.3.2 で説明したように，EV 証明書のためのガイドラインにおいて初めて SSL 証明書やルート証明書の暗号アルゴリズムとその最小鍵長が規定された．暗号アルゴリズムの中から RSA に焦点を当てて整理すると，表 2 のとおりである．

表 2 のとおり，EV 証明書のガイドラインは，NIST の鍵管理に関するガイドライン [2] が示す暗号アルゴリズムの移行スケジュールと整合的である．ルート証明書に利用可能な暗号アルゴリズムについては，現時点で既に 1024 ビット RSA が明記されていないほか，SHA-1 の使用は SHA-256 の普及が進むまでに限定されている．サーバ運営者は，EV SSL 証明書を今後新たに利用することで，ルート証明書も含めた暗号アルゴリズムの移行に対応できるようになっているといえる．

EV 証明書自体の普及度合はまだ低く [22]，SSL 証明書の暗号アルゴリズム全体に対する影響度は必ずしも高くないが，こうしたガイドラインが主要な認証局ベンダ及びブラウザベンダの合意によって規定されたことの意義は大きいといえる．

4.3.3 マイクロソフト・ルート証明書プログラムにおける記述の追加

マイクロソフト・ルート証明書プログラムでは，当初，SSL 証明書やルート証明書のアルゴリズムに関する記述はなかったが，MD5 の脆弱性による中間 CA 証明書の偽造が 2008 年 12 月に発表されたこと [23] を契機に，2009 年 1 月に暗号アルゴリズムの安全性低下の対応に関する記述が追加された．具体的には，① 1024 ビット RSA の脆弱化，② SHA-1 の衝突発見，③ MD5 の原像探索についての対応が記述されている．この記述は，Windows Update の利用を前提としたルート証明書更新のための緊急時対応のためのものであり，NIST のガイドライン [2] や「EV 証明書のためのガイドライン [24]」のように移行のスケジュールを示したものではない．

マイクロソフト・ルート証明書プログラムは，**3.3.1**

表 2　EV 証明書における暗号アルゴリズムと鍵のサイズ
Table 2　Cryptographic algorithm and key sizes for EV certificates.

証明書の種類	2010 年 12 月 31 日以前に発行される証明書	2010 年 12 月 31 日より後に発行される証明書
ルート証明書	MD5（推奨しない），SHA-1	SHA-1*，SHA-256，SHA-384，SHA-512
	鍵長が 2048 bit 以上の RSA**	鍵長が 2048 bit 以上の RSA
中間 CA 証明書	SHA-1	SHA-1*，SHA-256，SHA-384，SHA-512
	鍵長が 1024 bit 以上の RSA	鍵長が 2048 bit 以上の RSA
SSL 証明書	SHA-1	SHA-1*，SHA-256，SHA-384，SHA-512
	鍵長が 1024 bit 以上の RSA	鍵長が 2048 bit 以上の RSA

* SHA-1 の使用は，端末利用者のブラウザが広く SHA-256 に対応するまでに限定．
** 信頼点となるルート証明書は 2048 ビット未満の鍵長の RSA を使用可能．

で説明したように，マイクロソフト社の Windows OS 製品以外への影響が大きいと考えられる．仮に，同社のルート証明書プログラムが今後暗号アルゴリズムの移行に向けて記述を修正する等の対応が開始されるとすれば，他のルート証明書の組込みベンダも歩調を合わせて対応を開始する可能性がある．ただし，マイクロソフト社の製品であっても，Windows Update がサポートされない古い OS の PC 等においてはルート証明書の更新が実行されない．

4.3.4　その他の動向

暗号アルゴリズムの移行に関する動きは，日本国内においても存在する．電子政府暗号推奨リストを作成している CRYPTREC は，SHA-1 及び RSA1024 に関する安全性に関する見解を公表しているが [25]，内閣官房情報セキュリティセンター（NISC）は，この見解に基づき，「政府機関の情報システムにおいて使用される暗号アルゴリズム SHA-1 及び RSA1024 にかかわる移行指針」を公表している [3]．NISC のこの移行指針は，政府機関内の情報システムに対する行動指針ではあるが，民間に対する影響も大きく，SSL 証明書に関する暗号アルゴリズムの移行に向けた動きを後押ししている側面はある．

このように，社会基盤となった SSL においては，もはや実装レイヤまでの範囲で解決することは難しくなっており，多数の関係者間の調整によってのみ解決の可能性があるといってよい．そして，そこには影響力のある者が一定の主導権を発揮していくこともまた不可欠であると考えられる．

5.　SSL に見る関係者間の調整

暗号技術を利用した情報通信技術が社会基盤化した場合，暗号アルゴリズムの移行問題の解決には，「多数の関係者間の調整」が不可欠となる．本章では，SSL の事例をもとに，こうした調整の難しさを説明する．

5.1　SSL 証明書の関係者と暗号アルゴリズム移行のスタンス

4. で述べたように，現時点でも暗号アルゴリズム移行に向けた動きは見られるものの，その推進力は十分とはいえず，ルート証明書の関係者による主体的な取組みが必要である．ここでは，ルート証明書の関係者のスタンスを整理する．

5.1.1　端末利用者

端末利用者には，PC の利用者，携帯電話利用者，地デジ等の機器の利用者等が含まれる．PKI における信頼点は，端末利用者が決定して管理するものであるといえるが，実質的にはルート証明書の組込みベンダに依存している．すなわち，Windows OS を利用する PC では，マイクロソフト・ルート証明書プログラムに沿ってルート証明書が組み込まれ，Windows Update によってルート証明書の更新が実行される．Windows Update に対応していない古い OS の PC や古い携帯端末では，2048 ビット RSA の新しいルート証明書を組み込むことができない．

いずれにしても，新しいルート証明書を信頼点とする SSL 証明書のサーバにアクセスするためには，端末利用者は PC や携帯端末を更新する必要が出てくる．こうした中で，端末利用者から，ルート証明書を更新し暗号アルゴリズムの移行を促進してほしいとの要望の声がサーバ運営者に寄せられるとは考えにくい．仮に，端末利用者に対して，サーバ認証における将来発生し得るリスクに関して理解を求めたとしても，サーバ認証が現在支障なく動作している中で当該リスクの深刻さを認識することは容易でないと考えられる．

5.1.2　サーバ運営者

サーバ運営者の中でも，公共機関や金融機関等のように社会的に大きな信頼を寄せられ，従来からセキュリティ対策に積極的に取り組んできた組織においては，SSL によるサーバ認証を今後も確実に実行できる環境を整備していこうという前向きな姿勢が期待できよう．しかし，現時点では，暗号アルゴリズム安全性低下への取組みが十分に広がっているとは言いがたい [26]．

その背景として，インターネットによるサービスをできるだけ幅広い端末利用者に提供したいという意味での利便性，接続性を重視するという姿勢に軸足が置かれているためとも考えられる．

SSL 証明書を認証局ベンダから購入するサーバ運営者は，ルート証明書等の移行に関して一定の発言力を有する．しかし，仮に上記の利便性，接続性重視というスタンスをサーバ運用者が選択しており，今後も同様の姿勢を維持するとすれば，サーバ運営者はルート証明書の組込みベンダに対して後方互換性を喪失するような要望を自ら寄せることはないと考えられる．

5.1.3 SSL 証明書を発行する認証局ベンダ

古くから運営されている認証局の場合，そのルート証明書は様々な OS，ブラウザ，携帯電話等の機器に組み込まれているケースが多い．これに対して，比較的最近運営を開始した認証局の場合には，ルート証明書が様々な OS，ブラウザ，携帯電話等の機器に広く組み込まれるようになるまでには相応の時間が必要となり，普及しているケースは非常に少ない．特に，携帯電話や地デジの双方向サービスに対応した受信者機器等では，組込みが可能なルート証明書の数に強い制約が存在すること等から，相対的に普及が遅れているルート証明書は選択されない可能性が高いと見られる．

こうした点を踏まえると，上記のように後方互換性を重視する端末利用者やサーバ運営者のもとでは，古くから運営されている認証局のルート証明書を信頼点とする SSL 証明書へのニーズが相対的に大きい．つまり，マーケットであるサーバ運営者等からの要求として，1024 ビット RSA 等の暗号アルゴリズムのルート証明書から SSL 証明書を発行してほしいという要求が強ければ，認証局ベンダとしてはビジネス的観点から無視できないことになり，暗号アルゴリズム移行という面にはマイナスに作用すると考えられる．

5.1.4 信頼点（ルート証明書）を組み込むベンダ

PC の OS やブラウザのベンダは，CABF 等において複数の認証局と一定の合意を形成しつつ，ルート証明書の組込み基準の明確化や，新しい OS への新しいルート証明書の組込みを進める動きが見られる．その一方，古い OS のサポートについても積極的に行う意欲は高くなくルート証明書更新の意欲も低いと見られる．

携帯電話のキャリヤやベンダについても，古い認証局のルート証明書が携帯電話等に組み込まれるケースが主流となっており，ルート証明書更新への意欲は低いと見られる．

5.2 今後の対応のあり方

認証局ベンダとルート証明書組込みベンダに関して，移行を促す動きが形成されつつあることを **4.3** で述べた．本節では，暗号アルゴリズム移行に関する状況の適切な理解と対応が求められるサーバ運営者の観点から，今後の対応のあり方を説明する．ルート証明書の暗号アルゴリズム移行の主なポイントは以下の 2 点である．

（1） サーバにおける証明書パス上の公開鍵証明書（ルート証明書，中間 CA 証明書，SSL 証明書）として，いずれも十分な安全性を有する暗号アルゴリズム（2048 ビット RSA 等，ハッシュアルゴリズムとしては，SHA-1 ないし SHA-256 (注14)）を採用している SSL 証明書を利用する．

（2） 端末利用者に対しては，1024 ビット RSA のルート証明書から 2048 ビット RSA ルート証明書の移行に伴う接続性の低下を十分に説明する．

上記（1）については，サーバ運営者は現在の同サーバにおける証明書パスの状況をまず確認することが求められる．仮に，証明書パス上のルート証明書が 1024 ビット RSA を利用しており，有効期限が 2011 年以降という設定になっていた場合，そうしたルート証明書の利用の見直しについて検討する必要がある．例えば，2048 ビット RSA を利用するルート証明書を証明書パスとする SSL 証明書に更新するという対応が挙げられる．通常，SSL 証明書は有効期間が 1 年程度に設定されているケースが多く，SSL 証明書の有効期限切れのタイミングで移行することが考えられる．こうした対応は，暗号アルゴリズムの安全性低下に伴う証明書パス上の中間 CA 証明書等の偽造のリスクを低減させる効果を有すると考えられる．

ただし，新しいルート証明書の利用を開始した際に，当該ルート証明書の普及状況によっては，当該サービスサーバにアクセスできなくなる端末利用者が発生する可能性がある．上記の対応を検討する際には，現時点で当該サービスサーバにアクセスしている端末利用者がどのような OS やブラウザを利用しているかを調査することが必要である．そうした調査に基づいて端末利用者からのアクセスへの影響を勘案し，望ましい対応を決定していくこととなる．

(注14)：ハッシュアルゴリズムとしては，将来的には SHA-256 が推奨される．

上記（2）に関しては，サーバ運営者としてのサービス提供者が 2048 ビット RSA のルート証明書に完全に移行した場合に，端末利用者自身の対応がなければ，接続性が一時的に下がることに対して分かりやすく説明することがまず必要である．その上で，ルート証明書更新を実施する場合には，その際に端末利用者がどのような対応を実施する必要があるかを説明することとなる．例えば，Windows OS の PC の場合，ルート証明書の更新を行うためには Windows Update の実施を行うことになると考えられるが，そうした対応の実施を端末利用者に呼び掛けることになると考えられる．

こうしたサーバ運営者が，端末利用者に対して移行を促しやすくするためには，端末利用者も含めた啓発も必要になる．セキュリティに関連した組織や CRYPTREC 等が，移行対策等を含めた，適切な暗号技術の選択を支援するとともに，暗号アルゴリズムの移行問題を広く認知してもらうための活動も期待される．

6. むすび

インターネットが社会基盤となったといわれるようになって久しいが，社会基盤化したインターネットは，IPv6 移行問題等をはじめとして様々な移行問題を抱えている．こうした社会基盤の移行は，複雑に絡み合った様々な関係者の調整が必要になる．

インターネットのセキュリティも，また多くの移行問題が存在している．多くのインターネットプロトコルは，“Rough consensus and running code” といったコンセプトで開発され，これらのプロトコルが，後方互換性を保ち発展してきた．そして，このことがインターネットの爆発的な普及の要因の一つになっている．しかし，現在のインターネット上の様々な問題，特にセキュリティに関連した問題の多くは，よりセキュアなプロトコルに移行できないことにある．ここで，セキュアなプロトコルに移行できない理由の多くは，セキュアなプロトコルや実装等の技術が存在しないからではない．多くの場合，移行しないことによるリスクがきちんと認識されていなかったり，移行のインセンティブが弱いまたは正しく理解されていないといった理由によって移行問題が生じている．普及した DNS に対する DNSSEC への移行 [27] は典型な例になる．

2. の「暗号技術のレイヤ」では，四つのレイヤごとに移行の課題が必要なことを説明しているが，暗号アルゴリズムの脆弱化等が明らかになった 2005 年ごろ，こうした脆弱化の対応は，新たな暗号アルゴリズムの開発と単純に考えられていた面がある．その後，「標準」「実装」における暗号移行可能性ということに関して大きな技術的なチャレンジがあることが認識されてきた．実際，SSL 関係に関しても，SHA-256 への移行ということに関して言えば，暗号技術を利用した標準化，暗号技術を組み込んだ実装と展開における課題も多い．

暗号技術を利用した情報通信技術が基盤化するほどに「社会基盤」としての暗号アルゴリズムの移行の問題が顕著化する．これは，インターネットプロトコルにおける後方互換性の要求からくる移行問題と同様，非技術的側面の課題が大きい．本論文では，具体的な移行の事例として公開鍵暗号技術の応用である SSL を題材に，非技術的側面でもある「多数の関係者間の調整」を説明している．この非技術的側面の課題解決にしても技術の理解が欠かせないところに課題解決の難しさがある．本論文ではあまり取り上げられなかったが技術面においても，鍵管理技術，鍵更新技術等は，暗号移行可能性以前に技術としても未成熟な段階にある．

公開鍵暗号技術だけにこうした課題が存在するわけではない．共通鍵暗号技術においても同様の暗号アルゴリズムの移行問題は存在する．例えば [28] では，共通鍵暗号である 2-key Triple DES の移行スケジュールも示されているが，やはり移行に関する懸念の声がパブリックコメントとして多く寄せられた [29]．これらのコメントは，2-key Triple DES を主に利用している IC カード発行管理等の等の調整の難しさを示したもの(注15)であり，日本国内においても同様の状況があると考えられる．

暗号技術を利用した情報通信基盤の暗号アルゴリズムの移行には，本論文で示したとおり様々な課題があると考えられる．こうした移行に関する課題の理解がないと，移行にかなりの時間がかかるということが認識されず，結果として，スケジュール的に移行が間に合わない状況に至る可能性もある．本論文で事例として取り上げた SSL 証明書に関しても注意しなければならない状況にある．

情報通信技術，暗号技術は，社会の基盤として使わ

(注15)：具体的にはペイメントのカードや，IC カードの発行管理の規格である Global Platform などにおける移行の難しさが懸念されている．

れていく．社会基盤である限り，その技術は長期的な視野に立った設計が必要になる．その中で暗号アルゴリズム世代交代と世代交代に伴う移行問題への対応は避けて通れない．また，これからの情報通信基盤は，暗号アルゴリズムの世代交代に対応するための暗号移行可能性を考慮した設計，構築が望まれる．こうした分野における幅広い議論が期待される．

謝辞　本論文掲載の機会を頂いた本論文誌編集委員会，本研究のきっかけを作って頂いた日本銀行システム情報局の宇根正志企画役，校閲に御協力頂いた東京大学情報基盤センターの佐藤周行准教授及び奈良先端科学技術大学院大学情報科学研究科の猪俣敦夫特任准教授に謝意を表する．

文　献

[1] 神田雅透，“暗号アルゴリズムの安全性のお話，” Internet Week 2008, Japan Network Information Center, Nov. 2008.

[2] National Institute of Standards and Technology (NIST), “Recommendation for key management part 3: Application-specific key management guidance,” NIST Special Publication 800-57, NIST, Dec. 2009.

[3] 内閣官房情報セキュリティセンター (NISC)，“政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針，” 情報セキュリティ政策会議決定，内閣官房，April 2008.

[4] X.Y. Wang, F.D. Guo, X.J. Lai, and H.B. Yu, “Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD,” Rump Session of Crypto2004, Cryptography ePrint Archive, 2004/199, IACR, Aug. 2004.

[5] NIST, “Cryptographic hash algorithm competition,” in Federal Register Notice, Nov. 2, 2007.

[6] 宇根正志，神田雅透，“暗号アルゴリズムの 2010 年問題について，” 金融研究，vol.25, no.1（別冊），pp.31–72, 日本銀行金融研究所，2006.

[7] B. Sullivan, “Cryptographic agility,” MSDN Magazine, http://msdn.microsoft.com/en-us/magazine/ee321570.aspx, Aug 2009.

[8] NIST, “Recommendation for key management part 1: General (revised),” NIST Special Publication 800-57, NIST, March 2007.

[9] 松本　泰，宇根正志，“SSL 証明書における暗号アルゴリズム移行の現状と今後の対応，” ディスカッション・ペーパー・シリーズ　2010-J-11, 日本銀行金融研究所，April 2010.

[10] 宮川寧夫，“セキュリティ機能の移行技術，” 情報セキュリティ技術動向調査タスクグループ報告書，情報処理推進機構，March 2008.

[11] NIST, “Cryptographic key management workshop summary — June 8-9, 2009,” NIST Interagency Report 7609, NIST, Jan. 2010.

[12] IETF, “Hash BoF,” 63rd IETF Meeting, IETF, Aug. 2005.

[13] P. Hoffmann and B. Schneier, “Attacks on cryptographic hashes in Internet protocols,” RFC 4270, IETF, Nov. 2005.

[14] T. Polk, “Algorithm agility in PKIX,” 65th IETF Meeting, IETF, March 2006.

[15] T. Dierks and E. Rescorla, “The transport layer security (TLS) protocol version 1.2,” RFC 5246, Internet Engineering Task Force (IETF), Aug. 2008.

[16] S.M. Bellovin and E.K. Rescorla, “Deploying a new hash algorithm,” Cryptographic Hash Workshop, NIST, Oct. 2005.

[17] Microsoft, “Microsoft root certificate program,” Microsoft, http://technet.microsoft.com/en-us/library/cc751157.aspx, Jan. 15, 2009.

[18] American Institute of Certified Public Accountants, Inc. (AICPA) and Canadian Institute of Chartered Accountants (CICA), “WebTrust program for certification authorities,” Version 1.0, AICPA/CICA, Aug. 2000.

[19] マイクロソフト，“Windows ルート証明書プログラムのメンバー，” マイクロソフト，http://support.microsoft.com/kb/931125, May 2010.

[20] Z. Raza, “Phishing toolkit attacks are abusing SSL certificates,” Symantec Security Blogs, http://www.symantec.com/connect/blogs/phishing-toolkit-attacks-are-abusing-ssl-certificates, July 2009.

[21] 松本　泰，“次世代暗号アルゴリズムへの移行—暗号の 2010 年問題にどう対応すべきか，” Internet Week 2008, Japan Network Information Center, Nov. 2008.

[22] Netcraft, “Extended validation SSL certificates 2 years old,” Netcraft, http://news.netcraft.com/archives/2009/02/27/extended_validation_ssl_certificates_2_years_old.html, Feb. 2009.

[23] D. Molnar, M. Stevens, A. Lenstra, V. Weger, A. Sotirov, J. Appelbaum, and D.A. Osvik, “MD5 considered harmful today: Creating a rogue CA certificate,” 25th Chaos Communication Congress, Dec. 2008.

[24] CA/Browser Forum, “Guidelines for the issuance and management of extended validation certificates,” version 1.2, CA/Browser Forum, Oct. 2009.

[25] 情報通信研究機構（NICT），情報処理推進機構（IPA），“CRYPTREC report 2006,” NICT, IPA, March 2007.

[26] 神田雅透，“政府機関及び金融機関の SSL サーバ暗号設定に関する調査結果について，” PKI Day 2009, 日本ネットワークセキュリティ協会，June 2009.

[27] グレン　マンスフィールド，太田耕平，“DNSSEC 技術動向，” 情報セキュリティ技術動向調査タスクグループ報告書，情報処理推進機構，March 2008.

[28] NIST, “Recommendation for the transitioning of cryptographic algorithms and key lengths,” Draft, NIST Special Publication 800-131, NIST, June 2010.

[29] NIST, “Comments received on the second review of

SP 800-131 (recommendation for the transitioning of cryptographic algorithms and key lengths),” NIST, July 2010.
[30] A. Frier, P. Karlton, and P. Kocher, “The SSL 3.0 protocol,” Netscape Communications Corp., Nov. 1996.
[31] 内閣コンピュータ西暦二千年問題対策室, “コンピュータ西暦 2000 年問題に関する報告書,” 首相官邸, March 2000.
[32] ETSI, “Policy requirements for certification authorities issuing qualified certificates,” Version 1.2.1, ETSI TS 101 456, ETSI, April 2002.
[33] ETSI, “Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates,” Version 1.2.2, ETSI TS 102 042, ETSI, June 2005.

（平成 22 年 7 月 26 日受付，9 月 17 日再受付）

島岡　政基

1998 慶應義塾大学大学院理工学研究科修士課程了．同年セコム（株）入社，2004 より同 IS 研究所，現在に至る．2005 より国立情報学研究所特任助教授（非常勤）を経て 2009 まで同客員准教授．ネットワークサービス，ネットワークセキュリティ，電子認証の研究開発，また IETF にて PKI 相互運用に関する標準化に従事．2010 現在 ICSS 専門委員．

松本　　泰

1984 UNIX 上のビデオテックスの開発に従事．1990 UNIX 上の大規模パソコン通信システムの開発に従事．1994 各種インターネットサービスの開発に従事．1998 サイバーセキュリティ事業の立ち上げに従事．2007 経済産業省商務情報政策局長表彰「情報セキュリティ促進部門」受賞．2010 現在 NPO 日本ネットワークセキュリティ協会，PKI 相互運用技術 WG リーダ，IPA 情報セキュリティ分析ラボラトリー非常勤研究員，日本データセンター協会セキュリティWG リーダ，CRYPTREC 構成員．