IMES DISCUSSION PAPER SERIES

# 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

松本 泰（まつもと やすし）・宇根正志（うね まさし）

Discussion Paper No. 2010-J-11

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

**IMES Discussion Paper Series 2010-J-11**
**2010 年 4 月**

# 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

**松本 泰（まつもと やすし）*・宇根正志（うね まさし）****

要　　旨

インターネット上で重要な情報をやり取りする際には、アクセス先のサーバーが正当なサーバーであることを確認する必要がある。仮にサーバーの確認が困難な場合、偽のサイトに誤ってパスワード等の重要な情報を入力してしまうおそれがある。インターネット・バンキング等では、こうした問題への対策として、SSL（Secure Socket Layer）と呼ばれる暗号通信プロトコルによってサーバー認証を行うケースが多い。

こうしたなか、近年、SSL で利用されている暗号アルゴリズムの安全性低下が顕著になってきている。特に、サーバー認証等に用いられる「SSL 証明書」や「ルート証明書」と呼ばれるデータを、より安全性の高い暗号アルゴリズムを利用したものに更新する必要がある。しかしながら、金融機関のサーバーの設定が適切に更新されたとしても、末端の利用者の PC や携帯電話等の設定が更新されなければサーバー認証が実行困難となり、偽サイトにおける情報漏洩等のリスクが残存してしまう。このような状況を回避するためには、サーバー運営者である金融機関をはじめ、末端の利用者、ブラウザー・ベンダー、認証局ベンダー等の関係者が歩調を合わせて対応を検討することが必要である。

本稿では、SSL 証明書等における暗号アルゴリズムの安全性低下とその移行問題について説明するとともに、SSL 証明書やルート証明書の更新を進めていくうえで今後どのような取組みが必要かを検討する。

キーワード：暗号アルゴリズム、インターネット・バンキング、サーバー認証、ルート証明書、SSL 証明書、認証局

JEL classification: L86、L96、Z00

*　セコム株式会社 IS 研究所（E-mail: yas-matsumoto@secom.co.jp）
**　日本銀行金融研究所企画役（E-mail: masashi.une@boj.or.jp）

本稿の作成に当たっては、京都大学の岡部寿男教授から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行およびセコム株式会社の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

# 目　次

## １．はじめに

インターネット・バンキングがわが国の銀行によって提供されはじめたのは、今から約 10 年前の 1990 年代後半である。その後、多くの金融機関がインターネット上での金融サービスを提供するようになり、現在ではインターネットは金融サービスの重要なチャネルの 1 つになっている[1]。その背景には、インターネット技術の確立、ネットワーク帯域の拡大や普及といったインターネットの発展に加えて、サービスの利用者が、金融機関のサーバーにアクセスすることによって24時間いつでも金融サービスを利用できるという利便性上のメリットや、パソコンに標準装備されているソフトウエア（ブラウザー[2]）によってサーバーの認証や暗号通信を実現可能であり、「一定レベルのセキュリティを確保できている」という安心感を享受できることも寄与していると考えられる。

インターネット・バンキングのサーバー認証や暗号通信には、通常、インターネット標準となっているプロトコル SSL（Secure Socket Layer）が使われる。サーバー認証では、各サーバー固有の「SSL 証明書」と呼ばれるデータに対する認証局のデジタル署名を検証することによって行われるが、その検証用の鍵は「ルート証明書」と呼ばれるデータに含まれて PC 等にあらかじめ組み込まれる。仮に、SSL 証明書のデジタル署名が十分な安全性を確保していない場合、SSL 証明書の偽造が検知困難であり、偽のサーバーにパスワードや銀行口座情報等を入力し不正に盗み取られるおそれがある。1 つのルート証明書は数多くの SSL 証明書の検証に利用されており、そうしたルート証明書が偽造されると、多くの金融機関のサービスの信頼性に影響が及ぶ可能性がある。

こうしたなか、ルート証明書におけるデジタル署名の暗号アルゴリズム（デジタル署名方式とハッシュ関数）の安全性低下が顕著になってきている（宇根・神田[2006]）。ルート証明書のデジタル署名方式に関しては、「鍵のサイズが 1024 ビットの RSA」（以下、1024 ビット RSA と呼ぶ）が利用されるケースが多いが、「2010 年代後半に解読が現実のものとなる可能性が高い」との見方が一般的である（例えば、Joppe *et al.*[2009]、Kleinjung *et al.*[2010]）。ルート証明書の有効期間は通常 20～30 年程度に設定され、2020～2030 年まで有効とされているものが多く、その有効期限前に 1024 ビット RSA が安全でなくなる可能性が高い。1024 ビット RSA の安全性低下の影響を回避するためには、同署名方式を利用しているルート証明書を廃し、より安全性の高い署名方式（例えば、鍵長が 2048 ビッ

---

[1] 平成 20 年度の FISC アンケート調査によれば、回答を寄せた金融機関（468 社）のうち、インターネットを利用した金融サービスを提供している先は 88.4%となっている（金融情報システムセンター[2009]）。

[2] ブラウザーは、インターネットのサイト等を閲覧するためのソフトウエアであり、マイクロソフト社のインターネット・エクスプローラーが代表例として挙げられる。

トの RSA）のルート証明書に更新するとともに、SSL 証明書も新しいルート証明書のもとで取得することが必要である。

ルート証明書の暗号アルゴリズムの問題について、ブラウザー・ベンダーや認証局ベンダーでは一部対応が開始されている。マイクロソフト社は、Windows-OS に組み込むルート証明書の取扱方法をマイクロソフト・ルート証明書プログラム（Microsoft[2009a]）に 2009 年 1 月に記述し、暗号アルゴリズムの安全性低下の際には当該証明書の削除を促す等の対応方針を示している。また、認証局／ブラウザー・フォーラム（CABF）[3]は、2007 年に「EV 証明書」と呼ばれる新しい証明書のカテゴリーを導入し、同カテゴリーの証明書（例えば EV SSL 証明書）において十分な安全性を有する暗号アルゴリズムを採用する旨を記載した「EV 証明書のためのガイドライン」（CABF[2009]）を公表している。

こうした対応に基づいて PC 等に組み込まれているルート証明書を更新するためには、末端の PC 等の利用者（以下、端末利用者と呼ぶ）や金融機関等のサーバー運営者の協力が必要になる。しかし、すべての端末利用者の協力を期待することは現実的でなく、サーバー運営者にしても、既存のルート証明書を使い続ける端末利用者に配慮した対応を優先したいとのインセンティブが存在するとみられる。認証局やブラウザーのベンダーは、こうした意向をビジネス上無視できず、古いルート証明書の削除に向けた積極的な対応が困難であるとみられる。また、携帯電話や地上波デジタル放送対応テレビ（以下、地デジと略す）では、古いルート証明書が選択され組み込まれるケースが少なくないようである。こうした事情を背景に、安全性の高いルート証明書に更新する動きが弱いのが実情であり、今後、更新に向けた動きに拍車がかかる可能性は低い。

暗号アルゴリズムの安全性低下が深刻化する前に、上記の暗号アルゴリズム移行の必要性に関する認識を関係者間で共有し、安全性低下がサーバー認証や SSL への信頼性に与える影響を見極めることがまず必要である。そのうえで、スムーズな移行に向けて各関係者がどのように行動すべきかを検討する必要がある。サーバー運営者としての金融機関は、自社の端末利用者における PC 等の環境を踏まえたうえで、必要に応じて、EV SSL 証明書への移行を検討するとともに、ルート証明書の安全性低下に伴うリスクとその対応に関する説明を端末利用者に対して実施することが望まれる。

本論文は、こうした SSL 証明書やルート証明書における暗号アルゴリズムの安全性低下の問題を説明するとともに、ルート証明書の更新が遅れている背景や今後の対応のあり方を検討する。

---

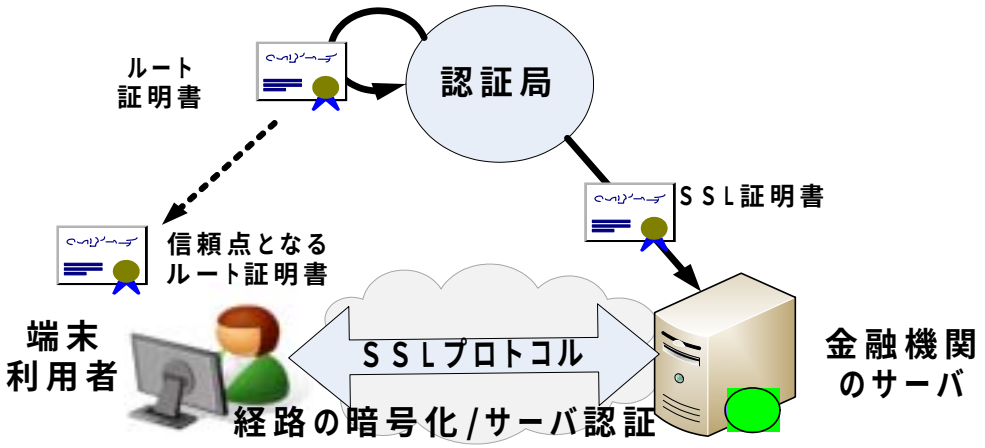
[3] 認証局／ブラウザー・フォーラム（CABF: Certificate Authority/Browser Forum）は、SSL 証明書発行時の審査基準を厳格化した EV 証明書の新設を主たる目的として、主要な認証局ベンダーおよびブラウザー・ベンダーによって 2006 年に設立された団体である。

## ２．SSL によるサーバー認証とルート証明書

本節では、SSL を利用したサーバー認証の仕組みと現状を説明し、SSL 証明書やルート証明書の暗号アルゴリズムの移行に深く関連するルート証明書の信頼について説明する。

### (1) SSL によるサーバー認証の仕組み

SSL によるサーバー認証は、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ーの名称や同サーバー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、①SSL 証明書に記載されたサーバーの名称等の確認[4]と、②当該サーバーが生成するデジタル署名[5]の検証によって実行される。上記①は、PKI（public key infrastructure、公開鍵暗号基盤）における認証局（CA: certificate authority）が、サーバーの名称や同サーバーの署名検証鍵等が記載された SSL 証明書を当該サーバーに対して発行し、端末利用者が SSL 証明書をサーバー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ジタル署名を検証することで実行される。端末利用者が認証局のデ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、この署名検証鍵は、当該認証局が発行する「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ーの署名検証鍵を用いて実行される。

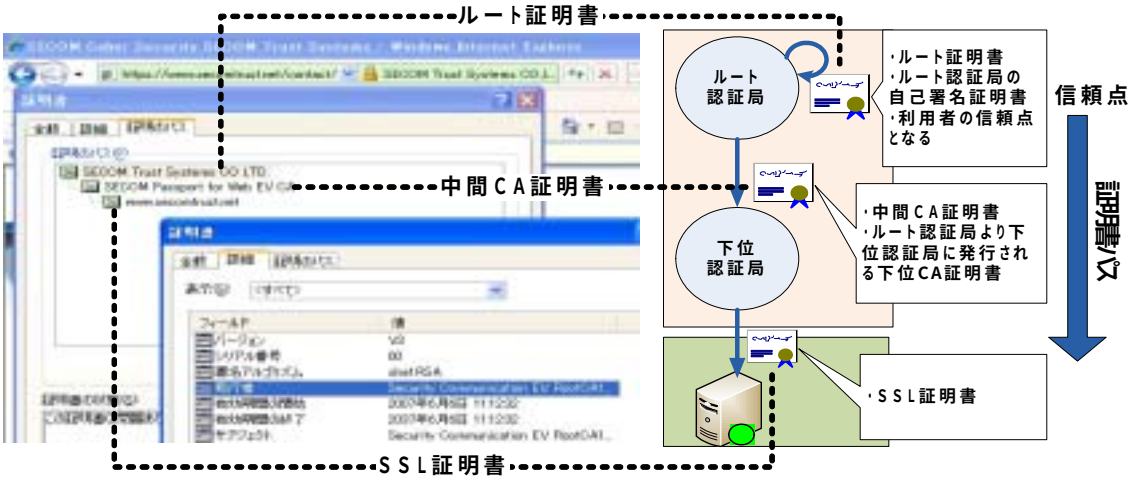



図表 1：ルート証明書・SSL 証明書を用いたサーバー認証（概念図）

[4] 具体的には、ブラウザーは、SSL 証明書に記載されたドメイン名（FQDN：Fully Qualified Domain Name）とサーバーの FQDN の比較を行う。

[5] ここでのデジタル署名は、公開鍵暗号をベースとするデジタル署名方式によって実現される。すなわち、デ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。

最も単純な「1 つの認証局が SSL 証明書を発行している」という場合（図表 1 参照）、認証局がサーバーに 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、その認証局のデジタル署名が施される[6]。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 証明書に対して生成された認証局のデ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ー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明書に対応する認証局は「ルート認証局」と呼ばれる。




図表 2：証明書パスを構成する証明書群と実際のブラウザー上での表示

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（図表 2 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ジタル署名が施される。また、SSL 証明書には下位認証局のデ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 証明書のデジタル署名を検証するという流れとなる。こ

[6] このように、認証局が自分自身に対して発行している証明書は、当該認証局によるデジタル署名が施されることから「自己署名証明書（self-signed certificate）」と呼ばれる。ルート証明書には、通常この自己署名証明書が使われる。

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。図表 2 では下位認証局が 1 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 によるサーバー認証の実行には、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。そのうえで、端末利用者は、①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ーの 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ーのデジタル署名の検証によってアクセス先のサーバーを確認する。

また、暗号アルゴリズムの観点からは、証明書パスのすべての証明書におけるデ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。

### (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[7]。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は、マイクロソフト社によって提供される Windows Update[8]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、どのルート証明書を OS やブラウザーに組み込むかを決定するのは、次に示す各ベンダーである[9]。

a) PC の OS ベンダー（PC の OS に組み込まれるルート証明書を決定）
b) ブラウザー・ベンダー（ブラウザーに組み込まれるルート証明書を決定）
c) 携帯キャリア（携帯電話等に組み込まれるルート証明書を決定）
d) 地デジやゲーム機等のベンダー（各機器に組み込まれるルート証明書を決

---

[7] 2009 年 9 月 22 日時点において Windows-OS の証明書ストアに存在するルート証明書の数は 291 となっている（Microsoft [2009b]）。

[8] Windows Update は、Windows-OS やそれを利用した各種ソフトウエアの更新を行うために、ネットワーク経由あるいは 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エアを 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 に組み込まれた同社のルート証明書を信頼点としている。

[9] なお、携帯情報端末のルート証明書の組込みでは、携帯キャリア、ブラウザー・ベンダー、当該端末機器のベンダー等のさまざまなケースがある。

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、上記の各ベンダー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。通常、端末利用者は、各ベンダーが組み込んだルート証明書を所与として利用することになる。一方、金融機関等のサーバー運営者は、当該サーバー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ーは、サーバー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。また、SSL 証明書における暗号アルゴリズム移行に関しても同様と考えられる。

### (3) ルート証明書に関連する基準

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、認証局／ブラウザー・フォーラムの「EV 証明書のためのガイドライン」が挙げられる。

#### イ．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。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[10] ”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。

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、

[10] WebTrust for CA は、ルート証明書プログラムに合わせて策定され、認証局の運用が証明書ポリシーと認証局運用規程を遵守しているかを確認することに主眼が置かれている。証明書ポリシー（CP: certificate policy）は、公開鍵証明書の用途・機能等を規定するものであり、各認証局が公開鍵証明書ごとに規定し公表する。認証局運用規程（CPS: certification practice statement）は、各証明書ポリシーに基づいて当該公開鍵証明書の発行・廃棄等に関する運用形態を具体的に規定するものであり、証明書ポリシーと同様に公開される。

2009 年 9 月 22 日現在で 291 のルート証明書が組み込まれている（Microsoft [2009b]）。これらは、例えば、マイクロソフト社の代表的なブラウザーのインターネット・エクスプローラー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ー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[11]。このように、本プログラムと WebTrust for CA 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持っているといえる。

**ロ．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背景として、証明書発行時の審査方法[12]が WebTrust for CA の監査等において認証局の裁量に委ねられており、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が挙げられる。このような SSL 証明書[13]はフィッシング詐欺等に悪用されるおそれがあり（Raza [2009]）、SSL のサーバー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ーに表示される「南京錠マーク[14]」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、サーバーを運営する組織の確認が認証局によって行われたこと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。そうしたなか、**３．**で説明する 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、認証局／ブラウザー・フォーラムは、証明書の新たなカテゴリーとして EV 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。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[15]。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

---

11 マイクロソフト社以外の代表的なブラウザーである 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 による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。

12 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。

13 こうした SSL 証明書は DV SSL 証明書（domain validated SSL certificate）と呼ばれている。

14 初期のブラウザーにおいて、「SSL で接続した状態」を「南京錠が閉った状態」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。

15 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。

準を追加した“ WebTrust EV Program ”が開始された[16]。

証明書の暗号アルゴリズムについては、EV 証明書のカテゴリーに含まれる SSL 証明書、中間 CA 証明書、ルート証明書が利用を推奨される暗号アルゴリズム（デジタル署名方式とハッシュ関数）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レベル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。

認証局／ブラウザー・フォーラムの設置以前は、複数のブラウザーのベンダー等と複数の認証局の間における合意の場はなかった。同フォーラムは、今後、証明書の暗号アルゴリズムの問題も含め、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考えられる。

### (4) PC 以外のルート証明書の配布

PC の OS やブラウザー以外でも、SSL 証明書の利用は増加している。わが国においては、携帯電話における SSL 証明書の利用が顕著であり、例えば、モバイル・バンキングをはじめとする携帯電話を利用した金融サービスを提供する金融機関がこれを利用している。その他、地デジの双方向通信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 における OS やブラウザー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ー（携帯電話であれば携帯キャリア）が「マイクロソフト・ルート証明書プログラム」のような基準を公開するケースはみられていない。第 2 に、1 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[17]。これは、携帯電話等の機器に搭載されるメモリー量に制約があり、組込み可能なルート証明書の数が制限されるためとみられる。こうした場合、組込みベンダーは、ルート証明書を選択するに当たって、接続先となるサーバーの 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

16 これらのほか、認証局／ブラウザー・フォーラム参加のブラウザー・ベンダーは、EV SSL 証明書のサーバーにアクセスしたことを認識しやすくするための工夫をブラウザーに施した。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ーでは、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ーのベンダーの協力と合意によって、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。

17 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。

が組み込まれる可能性が高いとみられる。また、メモリー量の制約は、新しいルート証明書の組込みのハードルとなり、ルート証明書の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ーの多くは認証局／ブラウザー・フォーラムに加入しておらず、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。

## ３．暗号アルゴリズムの安全性低下とサーバー認証への影響

本節では、サーバー認証に利用されるデジタル署名とハッシュ関数の安全性評価の現状を説明し、暗号アルゴリズムの安全性低下の影響を説明する。

### (1)サーバー認証に用いられる主な暗号アルゴリズム

ブラウザーには多くのルート証明書が組み込まれているが、ルート証明書に格納されている署名検証鍵としては 1024 ビット RSA のものが少なくない。Microsoft [2009b]によれば、2009 年 9 月 22 日時点において Windows-OS に組み込まれている 291 のルート証明書のうち、1024 ビット RSA のルート証明書は 58 となっているほか、鍵長が 2048 ビットの RSA（以下、2048 ビット RSA という）のルート証明書は 186、鍵長が 4096 ビットの RSA（以下、4096 ビット RSA という）のルート証明書は 38 となっている。このように、現在安全性低下が問題となっている 1024 ビット RSA のルート証明書は全体の約 2 割を占めている。また、1024 ビット RSA のルート証明書は、1990 年代後半に発行され、有効期限が 2010 年代後半から 2030 年にかけて設定されているものが多い。

ルート証明書の（認証局の）署名において 1024 ビット RSA とともに利用されているハッシュ関数については、SHA-1 のルート証明書が 22 となっているほか、MD5 のルート証明書が 28、MD2 のルート証明書が 8 となっている。SHA-1 と MD5 については、本節において後述するように、安全性低下が問題となっている。また、MD5 よりも古いハッシュ関数 MD2 については、全数探索よりも非常に効率のよい攻撃法が提案されており（Knudsen *et al.*[2010]）、証明書用のハッシュ関数としての利用は既に推奨されていない[18]。

金融機関のサーバーにおける SSL 証明書の暗号アルゴリズムについては、2009 年 5～6 月、金融機関の SSL サーバー（約 130）を対象とした調査結果が発表されている（神田[2009]）。本結果をみると、「1024 ビット RSA と SHA-1」の組合せの SSL 証明書が 49%、「1024 ビット RSA と MD5」の組合せのものが 10%となっているほか、安全性上相対的に望ましい「2048 ビット RSA と SHA-1」の組合せのものが 39%となっている。SSL 証明書の有効期間は 1 年以下に設定されているものが 71%を占めているとの結果となっている。ただし、これらの SSL 証明書の信頼点となるルート証明書の暗号アルゴリズムは不明である。

[18]ベリサイン社では、2009 年 5 月より、認証局の証明書（ルート証明書、中間 CA 証明書）に利用するハッシュ関数の移行（MD2 から SHA-1 へ）を開始している。

### (2)各暗号アルゴリズムの安全性評価の現状

#### イ．学界等での評価結果

**（イ）1024 ビット RSA**

1024 ビット RSA の安全性は、1024 ビットの署名検証鍵の素因数分解がどの程度の時間と資金によって実行可能であるかが安全性評価上のポイントとなる。署名検証鍵のサイズが 1024 ビットの場合、2010 年代後半に素因数分解が実現する公算が高いとの評価が大勢となっている。例えば、Brent[2000]は、ムーアの法則[19]をベースとして過去の素因数分解の実績値から未来の素因数分解の可能性について検討したところ、2018 年頃には 1024 ビットの合成数は現実的に素因数分解可能な領域に入ってくる可能性があるとしている。暗号技術検討会の報告書（情報通信研究機構・情報処理推進機構[2007]）では、スーパーコンピューター（構築費：数千万～数億円）によって 1 年間計算を実行した場合を前提に試算を行った結果、素因数分解が成功する時期が 2010 年～2020 年の間になる可能性が高いとしているほか、Kleinjung *et al.*[2010]も同様の見通しを示している。

**（ロ）SHA-1 と MD5**

デジタル署名用のハッシュ関数において、仮に同一の出力となるような異なる入力 A、B が見つかった場合、入力 A に対するデジタル署名が入力 B に対しても正当なデジタル署名として通用する可能性がある。こうした状況を排除するために、ハッシュ関数には、①同一の出力となる（未知の）異なる入力 A、B のペア（“ 衝突ペア ”と呼ばれる）を探索困難であること（衝突ペア探索困難性）、および、②既知の入力 A と同じ出力となる（未知の）入力 B を探索困難であること（第二原像探索困難性）が求められる。

SHA-1 については、衝突ペアの探索に必要と見積られている計算量をスーパーコンピューターによって 1 年間で処理可能となる時期が見積もられており、概ね 2013 年頃から衝突ペアの探索が成功する可能性が濃厚とみられている（情報通信研究機構・情報処理推進機構[2007]）。ただし、あくまで理論的な見積りであり、筆者らが知る限り、実際の衝突ペアは報告されていないようである[20]。

SHA-1 の第二原像探索に関しては、攻撃者が利用可能な入力のサイズと探索に必要な計算量との間のトレード・オフ関係があることが知られている。SHA-1

---

[19] ムーアの法則（Moore’s law）は、「半導体の集積密度は18～24ヵ月で倍増する」という法則であり、ゴードン・ムーア博士が提唱したものである。本法則は、半導体の性能やそれに伴う情報技術の発展の予測に用いられることが多い。

[20] また、サーバー認証におけるなりすましに利用可能なデジタル署名を偽造するには、探索すべき衝突ペアは一定のフォーマットに合致した“意味”のある値であることが必要となる。したがって、実際に偽造に成功するような衝突ペアの探索に必要な計算量は、通常安全性の評価に用いられる単なる衝突ペアの探索に必要な計算量よりも大きいとみられる。

は、入力を 512 ビット単位のデータ（ブロックと呼ばれる）に分けて変換するが、2 の *X* 乗個のブロックが与えられた場合の探索に必要な計算量は 2 の（160－*X*）乗回の SHA-1 演算と同程度になる（Kelsey and Schneier[2005]）[21]。例えば、1024 ビット RSA の SSL 証明書の場合、そのサイズは約 1 キロ・バイト（ $2^4$ ×512 ビット）となり、2 の 4 乗個のブロックが与えられるケースに対応する。したがって、第二原像探索の計算量は 2 の 156（=160－4）乗の計算量となる。

MD5 については、PC レベルの計算資源によって 1 時間程度で衝突ペアの探索が 2004 年に成功した後（Wang *et al.*[2004]）、2008 年には、一定条件下で得られた衝突ペアによって中間 CA 証明書の偽造が成功した（Molnar *et al.*[2008]）[22]。これによって任意の中間 CA 証明書が偽造可能になったというわけではないものの、今後、MD5 に関して一層強力な攻撃法が提案される可能性が高まったことから、MD5 の使用中止が望ましいとの見方が大勢となっている[23]。

**図表 3：ハッシュ関数 SHA-1 と MD5 の安全性に関する学界の評価**

| | 衝突ペア探索困難性 | 第二原像探索困難性<br>（証明書サイズ：1 キロ・バイト） |
|---|---|---|
| SHA-1 | ・2005 年：全数探索よりも**効率的に探索可能**（Wang, Yao, and Yao [2005]）。<br>― “2 の 63 乗回”程度の SHA-1 演算処理に相当する計算量との理論的な見積り。<br>・2007 年：スーパーコンピューターによる 1 年間の計算能力を前提にすると、2013 年頃から衝突ペアの探索が成功する可能性が濃厚との試算（情報通信研究機構・情報処理推進機構[2007]）。 | ・2005 年：“2 の 156 乗”回程度の SHA-1 演算相当の計算量によって可能（Kelsey and Schneier [2005]）。 |
| MD5 | ・2004 年：PC レベルの計算機資源によって**1 時間程度で探索成功**（Wang *et al.* [2004]）。<br>・2005 年：衝突ペアから SSL 証明書ペア生成に成功（Lenstra, Wang, and de Weger [2005]）。<br>・2008 年：一定条件での衝突ペアの探索によって中間 CA 証明書の偽造が成功（Molnar *et al.* [2008]）。 | ・2009 年：“2 の 123.4 乗”回程度の MD5 演算相当の計算量によって可能（Sasaki and Aoki [2009]）。 |

MD5 の第二原像探索については、2 の 123.4 乗の計算量で探索可能との研究成

[21] 「2 の（160－X）乗」の“160”はハッシュ関数の出力のサイズ（SHA-1 の場合は 160 ビット）を意味する。また、本計算量の下限は 2 の 80 乗となることが知られている。

[22] 2009 年 1 月 7 日、JVN（Japan Vulnerability Notes）では、MD5 の SSL 証明書偽造の脆弱性を説明したうえで、MD5 を使用しない等の対応策を脆弱性レポート「MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造」（JVNVU#836068）として発表した。JVN は、日本で使用されているソフトウエア等の脆弱性関連情報とその対策情報を提供すること等を目的とする脆弱性対策情報ポータルサイトであり、JPCERT コーディネーションセンターと情報処理推進機構によって共同で運営されている。

[23] ベリサイン社では、2009 年 1 月 6 日、MD5 の SSL 証明書の発行を同日より停止し、同月 15 日から SHA-1 を使った SSL 証明書の発行に切り替える旨を発表した。

果が発表されている（Sasaki and Aoki[2009]）。上記の SHA-1 と同様の攻撃法も MD5 に適用可能であり、MD5 の出力のサイズが 128 ビットであることから、その計算量は 2 の 124（=128－4）乗となる。以上は図表 3 のように整理できる。

**ロ．公的機関等における対応方針**

1024 ビット RSA、SHA-1、MD5 の安全性低下が懸念されているなかで、公的機関等が今後の対応方針を示している。基本的には、**1024 ビット RSA と SHA-1 について、2010 年代前半までに使用を停止し、より安全性の高い暗号アルゴリズム（RSA の場合は 2048 ビット RSA 等、ハッシュ関数の場合は SHA-256 等）に移行する**との対応が主流となっている。また、MD5 については、そもそも CRYPTREC による電子政府推奨暗号リストに含まれていないなど、今後中長期的に使用する暗号アルゴリズムとして位置付けられていないケースが多い。

米国立標準技術研究所[24]は、鍵管理に関するガイドライン SP800-57 Part 3（NIST[2009]）を 2009 年末に公開している。本ガイドラインでは、認証局が証明書発行・検証等の目的でデジタル署名を利用する際、①RSA を採用する場合には鍵のサイズを 2048 ビット以上とするほか、②ハッシュ関数として SHA-1 を採用する場合にはその使用は 2010 年末までに限るという対応が推奨されている。このように、1024 ビット RSA は推奨に含まれておらず、2048 ビット RSA が推奨されている。

わが国政府では、電子署名法関係における対応として、「2014 年度早期までに 2048 ビット RSA と SHA-256 による電子署名に係る特定認証業務を開始するとともに、2014 年度末前後を目途として 1024 ビット RSA と SHA-1 を特定認証業務に係る電子署名の基準から削除する」という方向で検討を進めている（総務省[2008]）[25]。また、「電子政府推奨暗号の利用方法に関するガイドブック」では、SSL 証明書の検証用の暗号アルゴリズムとして、RSA については鍵のサイズを 2048 ビットとすることが推奨されているほか、ハッシュ関数については条件付き[26]で SHA-1 が推奨されている（情報通信研究機構・情報処理推進機構[2008]）。

---

24 米国立標準技術研究所（NIST: National Institute of Standards and Technology）は、米商務省傘下の政府機関であり、連邦政府機関が採用する情報技術等の調達基準の策定を担当している。暗号アルゴリズムについても（軍事目的での使用を除き）標準暗号等の認定や同アルゴリズムを実装した暗号製品の試験・認定の枠組みを管理している（田村・宇根[2008]）。

25 SHA-1 や 1024 ビット RSA を利用した証明書のうち、2014 年度末以降も有効期間が残っているものの取扱いは、筆者の知る限り明確になっていないようである。

26 本ガイドブックでは、SSL をインターネット標準として規格化した国際標準 RFC 4346（Transport Layer Security, version 1.1）を前提に記述されており、SHA-1 について「利用は推奨されないが、RFC 4346 の規定上他のアルゴリズムは選択できない。RFC 4346 の規定が変更されるなどで、推奨されるアルゴリズムに変更できるようになった場合は、暗号の切り替え等を検討することが推奨される」と記述されている。

金融業務で利用される情報技術等の国際標準化を担当する ISO/TC68 においては、暗号アルゴリズムの推奨対応策（ISO[2007]）が 2007 年に策定されている（田村[2009]）。本推奨対応策では、「基本的には個々の情報システムにおけるシステム更改のタイミング等を勘案しつつ、運用も含めた対応を個々のアプリケーションに応じて検討することが重要」としたうえで、「1024 ビット RSA と SHA-1 については 2010 年末までの利用を推奨する」旨を記述している。また、2011 年以降に利用を推奨する暗号アルゴリズムとしては、2048 ビット RSA や SHA-256 等が記述されている。

### (3)ルート証明書における 1024 ビット RSA の安全性低下の影響

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し利用できなくなってしまう可能性が濃厚と評価されている。こうした評価をベースとすれば、2020 **年以降も有効期間が設定されているルート証明書の多くが、安全性の観点から有効期限到来前に信頼できないものになる可能性が高い**といえる。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いる。したがって、安全性の観点からルート証明書を信頼できなくなった場合、そうしたルート証明書が少数であったとしても、同証明書を信頼点として利用する数多くのサーバーの認証が無意味なものになってしまう（図表 4 参照）。


**図表 4：1024 ビット RSA 安全性低下による影響（概念図）**

また、MD5 や SHA-1 の安全性が低下し、衝突ペア探索困難性や第二原像探索困難性が失われた場合においても、上記の 1024 ビット RSA の場合と同様の影響が考えられる。ただし、1024 ビットの署名検証鍵の素因数分解が現実のものとなって 1024 ビット RSA の安全性が失われた場合には、任意の中間 CA 証明書や SSL 証明書の偽造が可能となるのに対し、ハッシュ関数の安全性が失われた場合、偽造可能となるのは特定の中間 CA 証明書や SSL 証明書に限定される可能性が高いと考えられる。したがって、安全性低下の深刻化による影響の大きさという点では、1024 ビット RSA の場合の影響が相対的に大きく、特に留意が必要であると考えられる。

こうしたデジタル署名やハッシュ関数の安全性低下が深刻化した場合におけるインターネット・バンキングへの影響を考えると、まず、偽造された SSL 証明書を有する偽の金融機関サーバーが立ち上げられ、フィッシング詐欺等に悪用されるおそれが考えられる。安全性が失われたルート証明書が PC 等に組み込まれたままとなっている端末利用者は、上記の偽金融機関サーバーを SSL の認証によって適切に排除することができず、本物の金融機関サイトと誤って判断してしまう可能性が高い。その結果、当該端末利用者は、同サイトにおいて、銀行口座情報、取引用パスワード、個人情報等の重要な情報を入力してしまうおそれがある。また、こうした状況が特定の端末利用者だけでなく多くの端末利用者において発生した場合、現在インターネット上で提供されているサーバー認証のための主要な手段が失われることとなり、インターネット上での金融取引全体の信頼性が損なわれる状態に至ることも考えられる。

## ４．ルート証明書の移行に向けた対応のあり方

本節では、ルート証明書に利用されている暗号アルゴリズムの移行に関する動向を説明するほか、ルート証明書を移行していくうえで関係者の間で共有すべき事項を説明し、今後の対応のあり方を検討する。

### (1)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 や SHA-256 のルート証明書は、2000 年以降に発行されはじめた。しかし、既存の SSL 証明書がこうした新しいルート証明書を信頼点として必ず利用するわけではない。サーバー運営者が、マイクロソフト社の Windows 2000 以前の古い OS のブラウザーにおいても SSL によるサーバー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（松本[2008]）。また、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。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（4 つ）すべてが 1024 ビット RSA のルート証明書であった。

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、携帯電話や組込み機器においては、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。仮に、そうした携帯電話や組込み機器がルート証明書を更新する機能を有していない場合、これらの機器では古いルート証明書が使用され続けることとなる。

ハッシュ関数の移行については、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[27]。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限定されているといえる。

### (2) 暗号アルゴリズムの移行を促す動き

#### イ．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 やブラウザーによる接続を許

27 ただし、エヌ・ティ・ティ・ドコモ社の携帯電話のうち、2009 年冬モデルにおいて 2 つの SHA-256 のルート証明書が組み込まれた。

容しない）という方針の採用が求められる。しかし、本節(1)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ー運営者のインセンティブに反するとともに、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、サーバー運営者、認証局ベンダー、ブラウザー・ベンダー等が足並みを揃えて対応するという状況を期待することは難しい。また、ブラウザー・ベンダー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 1 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 1 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。

**ロ．EV 証明書とそのガイドラインの導入**

**２．(3)**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はじめて、SSL 証明書やルート証明書が利用を推奨される暗号アルゴリズムとその最小鍵長が規定された。ハッシュ関数と、デジタル署名方式のなかから RSA に焦点を当てて整理すると、以下の図表 5 のとおりである[28]。

**図表 5：EV 証明書におけるデジタル署名方式（RSA）とハッシュ関数の推奨**

| 証明書の種類 | 推奨される暗号アルゴリズム | |
|---|---|---|
| | 2010 年 12 月 31 日以前に発行される証明書のケース | 2010 年 12 月 31 日より後に発行される証明書のケース |
| 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 ビット以上の RSA** | 鍵長が 2048 ビット以上の RSA |
| 中間 CA 証明書 | SHA-1 | SHA-1*、 SHA-256、SHA-384、SHA-512 |
| | 鍵長が 1024 ビット以上の RSA | 鍵長の 2048 ビット以上の RSA |
| SSL 証明書 | SHA-1 | SHA-1*、 SHA-256、SHA-384、SHA-512 |
| | 鍵長が 1024 ビット以上の RSA | 鍵長が 2048 ビット以上の RSA |

（備考）* SHA-1 の使用は、端末利用者のブラウザーが広く SHA-256 に対応するまでに限定。
** 初期のガイドライン（2007 年 **11** 月版）においては 1024 ビット RSA のルート証明書が許容されていたことから、既存のルート証明書には 2048 ビット未満のものも一部存在している。

図表 5 のとおり、EV 証明書のためのガイドラインの推奨は、NIST の鍵管理に関するガイドライン（SP800-57 Part 3）が示す暗号アルゴリズムの移行スケ

[28] デジタル署名方式としては、RSA のほかに、有限体上で定義された楕円曲線における離散対数問題に基づくデジタル署名方式も推奨されている。特に、NIST が規定したデジタル署名方式の調達基準 FIPS 186-2 の楕円曲線 NIST P-256（公開鍵長：256 ビット）が推奨されている。

ジュールと整合的である。ルート証明書については、現時点で既に 1024 ビット RSA が推奨される方式として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。サーバー運営者は、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。ただし、EV SSL 証明書自体の普及度合いはまだ低く[29]、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はない。

**ハ．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暗号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を契機に、2009 年 1 月に暗号アルゴリズムの安全性低下への対応に関する記述が追加された。具体的には、①1024 ビット RSA の安全性低下の深刻化、②SHA-1 の衝突ペア発見、③MD5 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（SP 800-57 Part 3）や「EV 証明書のためのガイドライン」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、**２．**(3)で説明したように、同社の 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において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ー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 に対応していない古い 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。

### (3) SSL 証明書の関係者と暗号アルゴリズム移行のスタンス

このように、現時点でも暗号アルゴリズム移行に向けた動きはみられるものの、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。

**イ．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

29 英国のネットクラフト社の調査によると、最初の EV SSL 証明書の発行から 2 年経過した 2009 年 2 月時点での EV SSL 証明書の利用は 1.1%とされている（Netcraft [2009]）。

が、実質的にはルート証明書の組込みベンダーに依存している。すなわち、Windows 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 や古い携帯電話では、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 証明書のサーバーにアクセスするためには、端末利用者は PC や携帯電話を更新する必要が出てくる。こうしたなかで、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がサーバー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ー認証における将来発生しうるリスクに関して理解を求めたとしても、現在サーバー認証が支障なく動作しているなかで、当該リスクの深刻さを認識してもらうことは容易でないと考えられる。

### ロ．サーバー運営者

サーバー運営者のなかでも、金融機関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 によるサーバー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、神田[2009]において示されたとおり、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難い。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ーから購入するサーバー運営者は、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、仮に上記の利便性重視というスタンスをサーバー運営者が選択し、今後も同様の姿勢を維持するとすれば、サーバー運営者が後方互換性を喪失するような要望をルート証明書の組込みベンダーに対して行うことは考えにくい。

### ハ．SSL 証明書を発行する認証局ベンダー

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さまざまな OS、ブラウザー、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、ルート証明書がさまざまな OS、ブラウザー、携帯電話等の機器に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、携帯電話や地デジ等の機器では、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、普及している古いルート証明書が選択される場合が多いとみられる。

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ー運営者のもとでは、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と考えられる。その結果、ビジネス的な観点から、古いルート証明書を信頼点とする SSL 証明書を発行するインセンティブを認証局ベンダーが有することになり、暗号アルゴリズム移行という面でマイナスに作用すると考えられる。

**二．信頼点（ルート証明書）を組み込むベンダー**

PC の OS やブラウザーのベンダーは、認証局／ブラウザー・フォーラム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みられる。その一方、古いルート証明書を更新しようという意欲は必ずしも高いとはいえないようである。

携帯電話のキャリアやベンダーについても、古い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みられる。

### (4)今後の対応のあり方

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 金融機関のサーバー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（デジタル署名方式としては 2048 ビット RSA 等、ハッシュ関数としては SHA-1 あるいは SHA-256[30]）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 のルート証明書への移行の必要性（移行しない場合のリスク）と移行に伴う利便性（接続性）の一時的な低下の可能性を十分に説明する。**

上記①については、**金融機関は現在のサーバー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

[30] EV 証明書のためのガイドラインに示されているように、ハッシュ関数としては、将来的には SHA-256 が推奨される。

するという対応が挙げられるほか、現時点で EV SSL 証明書を採用していない場合には、次回の SSL 証明書更新の際に EV SSL 証明書に移行するという対応も有用であろう[31]。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、そのルート証明書の普及状況によっては、当該金融機関サーバーにアクセスできなくなる端末利用者が出てくる可能性がある。**上記の対応を検討する際には、現時点で当該金融機関サーバーにアクセスしている端末利用者がどのような OS やブラウザーを利用しているかを把握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。

上記②に関しては、**サーバー運営者としての金融機関が 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、当該サーバーへのアクセスが困難なケースがあることを、2048 ビット RSA への移行の必要性と併せて分かりやすく説明することがまず必要である。**そのうえで、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が必要である。

以上の 2 点について対応を検討する場合、**対応完了までにどの程度の時間が必要になるかに留意する**ことが求められる。まず、端末利用者に信頼点としてのルート証明書の更新を依頼する場合、個々の端末利用者の事情によって対応の早さが異なることから、一定の猶予期間を準備することが重要である。金融機関では、その猶予期間が終了したタイミングで（安全性の高い暗号アルゴリズムを利用した）新しい SSL 証明書を導入することが望ましい。

また、Windows Update のような方法で暗号アルゴリズムの移行を実施する手段が存在しないケースでは、そうした手段を実現するようにルート証明書の組込みベンダーやブラウザー・ベンダーに働き掛けることも検討する必要があると考えられる。こうした関係者への要請を行うとすれば、対応完了までにはさらに時間が必要となろう。1024 ビット RSA の安全性低下が深刻化すると予想されている 2010 年代後半までに、ルート証明書の暗号アルゴリズム移行の問題について一定の対応が完了するように、各金融機関は必要に応じて今後のスケ

[31] EV SSL 証明書については、フィッシング詐欺等への対策の 1 つとして従来から指摘されており（例えば、中山[2007]）、既に一部の銀行では導入が始まっている。

ジュールを検討することが求められる。

単独の金融機関において上記のような検討を推進することは容易でないかもしれない。その際には、金融業界としての SSL 証明書のガイドラインの作成を検討することが考えられる。本ガイドラインは、ISO/TC68 における暗号アルゴリズム移行の推奨対応策（ISO[2007]）[32]や認証局／ブラウザー・フォーラムの EV 証明書における暗号アルゴリズム対応の内容を参考にしながら、端末利用者の対応状況等、日本国内での状況を考慮した内容にすることがまず考えられる。金融業界がこうしたガイドラインによって暗号アルゴリズムの移行に関して何らかの方針を示すことは、その他の分野のサーバー運営者や SSL 証明書の関係者に大きな影響を与えることになろう。SSL におけるサーバー認証というインフラの信頼性を維持・向上させていくという観点でも、金融機関の姿勢や取組みは重要であるといえる。

32 ISO/TC68 における推奨対応策では、推奨される暗号アルゴリズムや金融機関としての対応のあり方が記述されているものの、インターネット・バンキングにおける端末利用者への対応等に関しては記述されていない。

## ５．おわりに

インターネット・バンキングの利用者がアクセス先の金融機関サーバーを適切に認証するためには、同認証に用いられるデジタル署名が十分な安全性を確保している必要がある。しかし、現在主流となっているデジタル署名方式（1024 ビット RSA）やハッシュ関数（MD5、SHA-1）の安全性低下が近年顕著となってきており、2010 年代後半頃に十分な安全性を確保できなくなる可能性が学界等から指摘されている。これらの暗号アルゴリズムが十分な安全性を確保できなくなった場合、利用者は「金融機関サーバー」と偽る攻撃者のサーバーを検知不可能となり、なりすましによる情報漏洩等のリスクが高まる可能性がある。さらに、SSL のサーバー認証の仕組み自体が信頼を喪失し、インターネットが金融取引のチャネルの 1 つとして機能しなくなる状況に至る可能性もある。

こうした状況を回避するためには、金融機関サーバーとインターネット・バンキングの利用者の双方が、2048 ビット RSA 等、より安全性が高いデジタル署名方式を利用する環境に移行する必要がある。金融機関サーバー側では、2048 ビット RSA の SSL 証明書やルート証明書を採用することが求められる。利用者側では、PC 等に組み込まれている「ルート証明書」（ルート認証局の署名検証鍵）の更新が必要であり、1024 ビット RSA 等を利用する古いルート証明書の使用停止と新しいルート証明書の組込みを認証局ベンダーやブラウザー・ベンダー等と協力して進めていくことが求められる。ただし、こうした対応を進めた場合、ルート証明書の更新を実施しない利用者にとっては、サーバー認証が実施できずインターネット・バンキングを利用できなくなるおそれがある。

安全で安心して利用できるインターネット・バンキングのサービス提供を今後も継続していくうえで、金融機関は、上記のリスクと利用者の利便性等を勘案し、必要に応じてサーバー認証におけるデジタル署名の安全性低下への対応を検討する必要がある。具体的には、自社サーバーが利用している SSL 証明書やルート証明書のデジタル署名方式を調査したうえで、サーバー認証における今後のリスクや利便性に与える影響を検討し、必要に応じて、SSL 証明書等を更新することが考えられる。ただし、2048 ビット RSA のルート証明書を新たに採用した場合、同証明書を使用できない環境下の利用者はインターネット・バンキングを利用できなくなる可能性がある。こうした点を考慮し、SSL 証明書等の更新の必要性、利用者側において想定される利便性の一時的な低下の可能性等に関して十分な説明を行って理解を得たうえで、一定の移行期間を設定して利用者側の環境の変更を促すなどの対応が求められよう。

# 参考文献


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』第 25 巻別冊第 1 号、日本銀行金融研究所、2006 年、31-72 頁

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 説明資料』、日本ネットワークセキュリティ協会、2009 年 6 月

金融情報システムセンター（FISC）、『金融情報システム　金融機関業務のシステム化に関するアンケート調査結果』、金融情報システムセンター、2009 年 10 月

情報通信研究機構（NICT）・情報処理推進機構（IPA）、『CRYPTREC Report 2006』、NICT・IPA、2007 年

――――・――――、『電子政府推奨暗号の利用方法に関するガイドブック』、NICT・IPA、2008 年

――――・――――、『CRYPTREC Report 2008』、NICT・IPA、2009 年

田村裕子、「ISO/TC68 における金融分野向け推奨暗号アルゴリズムの検討状況」、『金融研究』第 28 巻第 1 号、日本銀行金融研究所、2009 年、173～205 頁

――――・宇根正志、「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において活用していくために」『金融研究』第 27 巻別冊第 1 号、2008 年、79～114 頁

総務省、『「電子署名及び認証業務に関する法律の施行状況に係る検討会」報告書（案）』、総務省、2008 年 3 月 13 日

中山靖司、「インターネット・バンキングの安全性を巡る現状と課題――2007 年」、『日銀レビュー』2007-J-14、日本銀行決済機構局、2007 年

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 プレゼンテーション資料』、Japan Network Information Center、2008 年 11 月

Bos, Joppe W., Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra, and Peter L. Montgomery, "On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography," *ePrint 2009/389*, IACR, 2009.

Brent, Richard, "Recent progress and prospects for integer factorization algorithms," *Proceedings of COCOON 2000*, LNCS 1858, Springer-Verlag, 2000, pp.3-20.

CA/Browser Forum, *Guidelines For The Issuance And Management Of Extended Validation Certificates*, version 1.2, CA/Browser Forum, October 1st, 2009.

Dierks, Tim, and Eric Rescorla, "Request for Comments 5246: The Transport Layer Security (TLS) Protocol Version 1.2," Internet Engineering Task Force, August 2008.

International Organization for Standardization (ISO), *Financial services – Recommendations on cryptorgraphic algorithms and their use – Standing Document*, ISO, 2007.

Kelsey, John, and Bruce Schneier, "Second Preimages on *n*-Bit Hash Functions for Much Less than $2^n$ Work," *Proceedings of EUROCRYPT 2005*, LNCS 3494, Springer-Verlag, 2005, pp.474-490.

Kleinjung, Thorsten, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomè, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann, "Factorization of a 768-bit RSA modulus," *Cryptology ePrint Archive 2010/006*, International Association for Cryptologic Research,　January 7, 2010.

Knudsen, Lars R., John Erik Mathiassen, Frédéric Muller, and Soren S. Thomsen, "Cryptanalysis of MD2," *Journal of Cryptology* 23 (1), IACR, 2010, pp.72-90.

Lenstra, Arjen K., Xiaoyun Wang, and Benne de Weger, "Colliding X.509 Certificates," *Cryptography ePrint Archive,* 2005/067, IACR, 2005.

Microsoft, *Microsoft Root Certificate Program*, Microsoft, January 15, 2009a.

———, *Windows Root Certificate Program Members*, Microsoft, September 22, 2009b.

Molnar, David, Marc Stevens, Arjen Lenstra, Venne de Weger, Alexander Sotirov, Jacob Appelbaum, and Dag Arne Osvik, "MD5 considered harmful today: Creating a rogue CA Certificate," *Presentation at 25th Chaos Communication Congress*, 25C3, December 2008.

National Institute of Standards and Technology (NIST), *NIST Special Publication 800-57 Recommendation for Key Management Part 3: Application-Specific Key Management Guidelines*, NIST, December 2009.

Netcraft, *Extended Validation SSL Certificates 2 Years Old*, Netcraft, February 2009.

Raza, Zahid, *Phishing Toolkit Attacks are Abusing SSL Certificates*, Symantec Security Blogs, July 8th, 2009. (http://www.symantec.com/connect/blogs/phishing-toolkit-attacks-are-abusing-ssl-certificates)

Sasaki, Yu, and Kazumaro Aoki, "Finding Preimages in Full MD5 Faster Than Exhaustive Search," Proceedings of EUROCRYT 2009, LNCS 5479, Springer-Verlag, 2009, pp.134-152.

VeriSign, *VeriSign Confirms All SSL and EV SSL Certificates Remain Safe From Potential Threats Newly Presented at Black Hat Conference,* VeriSign, July 31, 2009.

Wang, Xiaoyun, Dengguo Feng, Xuejia Lai and Hongbo Yu, "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD," *Cryptography ePrint Archive*, 2004/199, IACR, 2004.

————, Andrew Yao, and Frances Yao, "New Collision Search for SHA-1", *Presentation at CRYPTO 2005 Rump Session*, IACR, 2005.