MC-04

暗号アルゴリズム移行における
オペレータ認証基盤の運用ガイドライン

平成 23 年 12 月 26 日　　1.0 版

一般社団法人電波産業会
高度無線通信研究委員会
モバイルコマース部会

暗号アルゴリズム移行における
オペレータ認証基盤の運用ガイドライン

目次

1. はじめに

1.1. 検討の背景と目的

高度無線通信研究委員会　モバイルコマース部会・技術専門委員会　認証 WG（以下、認証 WG）が本報告書「暗号アルゴリズム移行におけるオペレータ認証基盤の運用ガイドライン」を取りまとめた背景には、暗号アルゴリズムの 2010 年問題がある。

2008 年度に情報システムの暗号・ハッシュアルゴリズムの更改に関する動向調査が実施され、標準化、官民での取り組み状況とともに、移行の課題も明らかになっている。

1.1.1. 2010 年問題の調査結果

NIST（The National Institute of Standards and Technology）では、推奨鍵長の利用保護期間の目安として、図表 1－1 のように推奨するアルゴリズムと最小鍵長を示している。

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA[23] 3TDEA AES-128 AES-192 AES-256	Min.: $L = 1024$; $N = 160$	Min.: k=1024	Min.: f=160
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: $L = 2048$ $N = 224$	Min.: k=2048	Min.: f=224
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: $L = 3072$ $N = 256$	Min.: k=3072	Min.: f=256

図表 1－1　NIST の推奨するアルゴリズムと最小鍵長

（出典：“RECOMMENDATION FOR KEY MANAGEMENT Part1:General(Revised)”, NIST Special Publication 800-57, NIST, 2006-5 [Table.4]
http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf
※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”, JNSA PKI day, No.7, 2009　[P.7]にも同様の資料あり
http://www.jnsa.org/seminar/2009/0624/）

NIST における検討では、公開鍵暗号の鍵長について、用途ごとに推奨鍵長を定めている（図表 1－2)。その上で、認証での RSA-1024 ビットについては 2013 年※まで利用可能とし、またデジタル署名での RSA-1024 ビットについては 2008 年※まで利用可能としている。5 年の差は、デジタル署名の保存期間を考慮したものである。

※　米連邦政府認証基盤（Federal PKI）において認証と署名用の鍵として 2010 年まで RSA1024 ビットが認められたとあるが、既存製品を考慮したものであり、安全性の観点からは、認証は 2013 年、署名は 2008 年に段階的に移行されるべきである。

鍵用途	使用可能期間	アルゴリズムと鍵長
認証	～2013/12/31	RSA　：　1024 or 2048bits ECDSA　：　Curve P-256
	2013/12/31～	RSA　：　2048bits ECDSA　：　Curve P-256
デジタル署名	～2008/12/31	RSA signature or 鍵配送　：　1024 or 2048bits ディフィー・ヘルマン鍵　：　1024 or 2048bit ECDSA　：　Curve P-256 or P-384
	2008/12/31～	RSA signature or 鍵配送　：　2048bits ディフィー・ヘルマン鍵　：　2048bits ECDSA　：　Curve P-256 or P-384
CA及びOCSPのレスポンダ署名	該当なし	RSA　：　2048 or 3072 or 4096bits ECDSA　：　Curve P-256 or P-384

図表 1－2　NIST における推奨鍵長

（出典：“RECOMMENDATION FOR KEY MANAGEMENT Part3:Application-specific key Management Guidance”, NIST Special Publication 800-57, NIST, 2008 [Table-2.1] http://csrc.nist.gov/publications/）

また、ハッシュ関数のハッシュ長については、推奨署名アルゴリズムとして図表 1－3 のように定めており、署名アルゴリズムでのハッシュ関数としての SHA-1 については 2010 年 12 月 31 日まで利用可能としている（ただし、RSA-2048 ビットに限る）。

署名作成日	公開鍵アルゴリズム・鍵長	ハッシュ関数	パディングスキーム
～2009/12/31	RSA ： 2048, 3072, 4096bits	SHA-1	PKCS #1 v1.5
		SHA-256	PKCS #1 v1.5
	ECDSA ： Curve P-256	SHA-256	該当なし
	ECDSA ： Curve P-384	SHA-384	該当なし
2009/12/31～～2010/12/31	RSA ： 2048, 3072, 4096bits	SHA-1	PKCS #1 v1.5
		SHA-256	PKCS #1 v1.5, PSS
	ECDSA ： Curve P-256	SHA-256	該当なし
	ECDSA ： Curve P-384	SHA-384	該当なし
2010/12/31～	RSA ： 2048, 3072, 4096bits	SHA-256	PKCS #1 v1.5, PSS
	ECDSA ： Curve P-256	SHA-256	該当なし
	ECDSA ： Curve P-384	SHA-384	該当なし

図表 1－3　NIST における推奨署名アルゴリズム

（出典：“RECOMMENDATION FOR KEY MANAGEMENT Part3:Application-specific key Management Guidance”, NIST Special Publication 800-57, NIST, 2008 [Table-2.2] http://csrc.nist.gov/publications/）

これらの諸課題を解決し、オペレータ認証基盤に関するアルゴリズム更改スケジュール策定に資するガイドラインとすることが、本報告書の目的である。

1.2. 検討のスコープ

認証 WG では 2002 年度に、モバイル事業者共通の認証基盤（以下、「オペレータ PKI」とする）の提供を目的とし、携帯加入者向け証明書プロファイル（以下、「加入者証明書プロファイル」とする）を策定した。そこでは最低の安全性保証を目的とし、RSA 鍵長 1024 ビット以上とのみ規定した。

本要件については、技術進歩に伴う見直しが必要である。また、本プロファイルに沿って作られたサービスの証明書にも、有効期間まで安全性が保証しにくいものが出てきている。当然、これらも 2010 年問題への対応は必須であり、スムーズな移行が求められる。

そこで本検討のスコープとして、mITF(モバイル IT フォーラム)においてガイドライン化し、現在も普及活動を行っている「オペレータ PKI における署名アルゴリズム（ハッシュを含む)」を対象とした。

モバイル環境においては、特にモバイル特有の環境（携帯電話と UIM）に焦点を当て、検討を行った。また、サーバ認証と暗号アルゴリズムに関しては、すでに各通信事業者において対応が済んでいるため、本検討のスコープには含まなかった。

なお、加入者証明書プロファイルとは、以下のような目的で提供されるものである。今後、さまざまな業務に携帯電話を利用したサービスが構築されていくことが想定されるが、これらのサービスの共通課題のひとつとして、通信先の認証の必要性が挙げられる。その認証方法のひとつに電子証明書を利用した方法が考えられるが、携帯電話利用者の認証としてモバイル事業者ごとに別々のポリシーで電子証明書が発行された場合、サービス提供者はそれぞれ異なる対応が必要となることが懸念される。

そこで認証 WG では、モバイル事業者が発行する加入者証明書について共通化が求められる内容をまとめ、システム構築のための参考プロファイルとして公開することとした。

本プロファイルは、携帯電話契約の「契約」に対して発行されるものである。また、証明書に記載する発行対象は、契約ごとに一意で、かつ証明対象の特定が困難な「モバイル ID」で表現する。

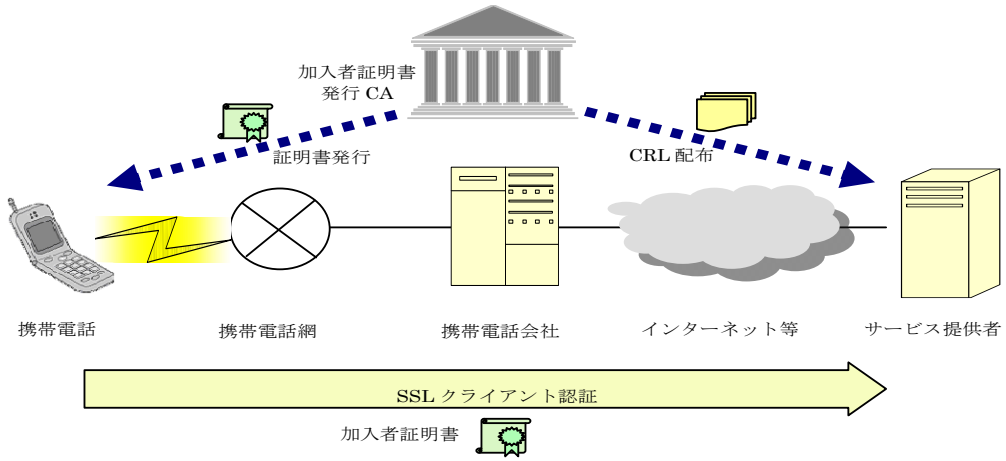
なお、加入者証明書プロファイルは、当面多くの利用が見込まれる「SSL クライアント認証用証明書」を対象としており、デジタル署名は対象としていない。

1.3. オペレータ PKI サービスの概要

この加入者証明書プロファイルを用いたオペレータ PKI サービスとしては、モバイル事業者による電子認証サービスがある。

同サービスでは、ユーザーは、加入者証明書を格納した UIM を挿入した携帯電話から対応するサイトに証明書を送信することにより、インターネットアクセスにおいてより安全性の高い SSL クライアント認証の利用が可能となる（図表 1－4）。これにより、企業の社内ネットワークへのアクセスや会員制サイト等へのログインに際し、従来の ID/パスワード方式等の認証方法よりもシンプルな操作で、かつ、より安全性の高いネットワーク環境が構築できることが特長である。

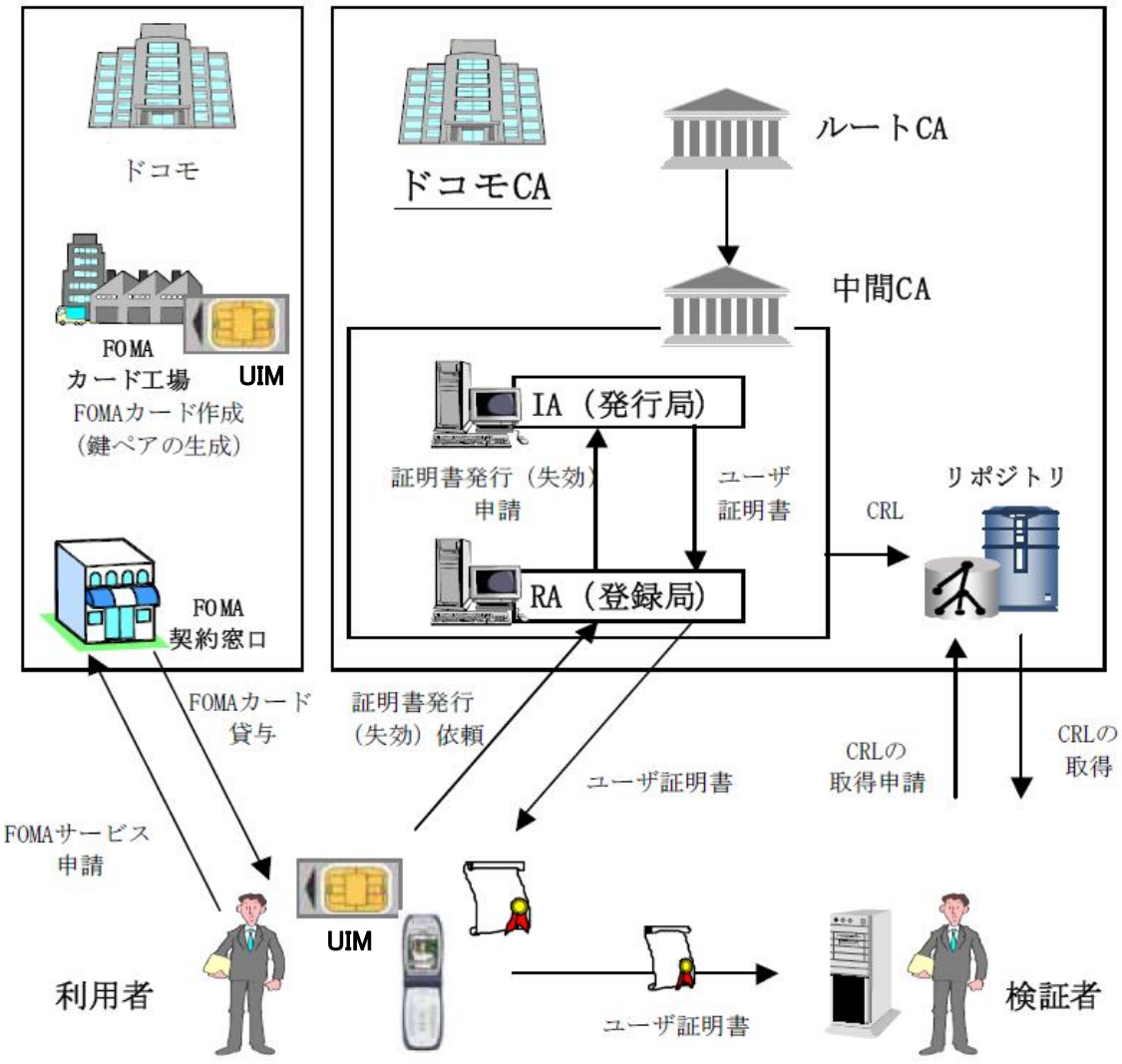
具体的な商用サービス事例としては、NTT ドコモ社の「FirstPass」（2003 年開始、2012 年サービス終了予定）、KDDI 社の「Security Pass」（2005 年開始）がある。



図表 1－4　オペレータ PKI の利用モデル例（SSL クライアント認証）

本検討の対象となる加入者証明書プロファイルは、これら一連のサービスフローにおいて、モバイル事業者の CA から発行され、ユーザーの UIM に格納、SSL クライアント認証等に利用される「加入者証明書」に対して適用されるものである（図表 1－5）。

1 章で解説した暗号アルゴリズムの 2010 年問題を受け、この加入者証明書プロファイルについてもアルゴリズムの更改が求められることから、以降の章ではその移行モデルと移行シナリオ、そして移行時期についての考察を行う。



図表 1－5　オペレータ PKI サービスの全体像

（出典：NTT ドコモ　「FirstPass 運用規定」 第 1.23 版　2009 年 7 月 1 日）

2. アルゴリズム更改における前提条件

アルゴリズム更改における前提条件は下記の通りである（図表 2－1)。

まず、移行するアルゴリズムおよびそのセキュリティパラメタについては、RSA の鍵長を RSA-1024 ビットから RSA-2048 ビットへ移行するものとし､ハッシュ関数は SHA-1 から SHA-2 へと移行する。また、ルート証明書の構成は、「ルート証明書」、「中間証明書」、「クライアント証明書」からなるものとする。

共存要件については、①新旧 CA 及びそれらが発行した有効な証明書の共存機関があること、②新携帯電話と旧携帯電話との共存期間があること、③新 UIM と旧 UIM の共存期間があること、④旧証明書を利用する SP と新証明書を利用する SP の共存機関があること、の 4 つを定めている。

また互換性要件として、新旧携帯電話と新旧 UIM のすべての組み合わせで PKI サービスが継続できること、および、SP は移行期間において旧証明書の利用が可能であること、としている。

「モバイル ID」の条件については、モバイル ID が引き継がれる場合と引き継がれない場合の両方を考えること、とした。

■移行するアルゴリズムおよびそのセキュリティパラメタ ● RSA の鍵長： RSA-1024 から RSA-2048 へ移行 ● ハッシュ関数： SHA-1 から SHA-2 へ移行
■ルート証明書の構成 ● ルート証明書、中間証明書、クライアント証明書
■共存要件 ● 新旧 CA 及びそれらが発行した有効な証明書の共存機関があること ● 新携帯電話と旧携帯電話との共存期間があること ● 新 UIM と旧 UIM の共存期間があること ● 旧証明書を利用する SP と新証明書を利用する SP の共存機関があること
■互換性要件 ● 新旧携帯電話と新旧 UIM のすべての組み合わせで PKI サービスが継続できること ● SP は移行期間において旧証明書の利用が可能であること
■モバイル ID 条件 ● モバイル ID は引き継がれる場合と、引き継がれない場合の両方を考えること

図表 2－1　モバイル認証基盤における暗号･ハッシュアルゴリズム更改における前提条件

3. アルゴリズム更改

3.1. アルゴリズム更改における移行モデル

オペレータ PKI におけるアルゴリズムを実装する 3 つのエンティティ、つまり、UIM、携帯電話、サービス提供者（SP）を規定し、それぞれにおける移行の状態を定義した（図表 3－1)。その上で、現行運用→並行運用→移行終了の移行シナリオを定義し、各シナリオにおける課題を抽出している（3.2 節および 3.3 節に詳述)。

■｛旧｝　・・・　旧方式のみ ● 旧 UIM だけが世の中にある ● 旧携帯電話だけが世の中にある
■｛新旧｝・・・　旧方式と新方式が世の中に混在 ● 新 CA 局があり、旧 UIM と新 UIM（新旧暗号方式の両対応）が世の中にある ● 旧携帯電話と新携帯電話（新旧暗号方式の両対応）が世の中にある ● 新 CA 局があり、旧ルート証明書と新ルート証明書が世の中にある
■｛新｝　・・・　新方式のみ ● 新 UIM（新旧の両対応）だけが世の中にある ● 新携帯電話（新旧暗号方式の両対応）だけが世の中にある

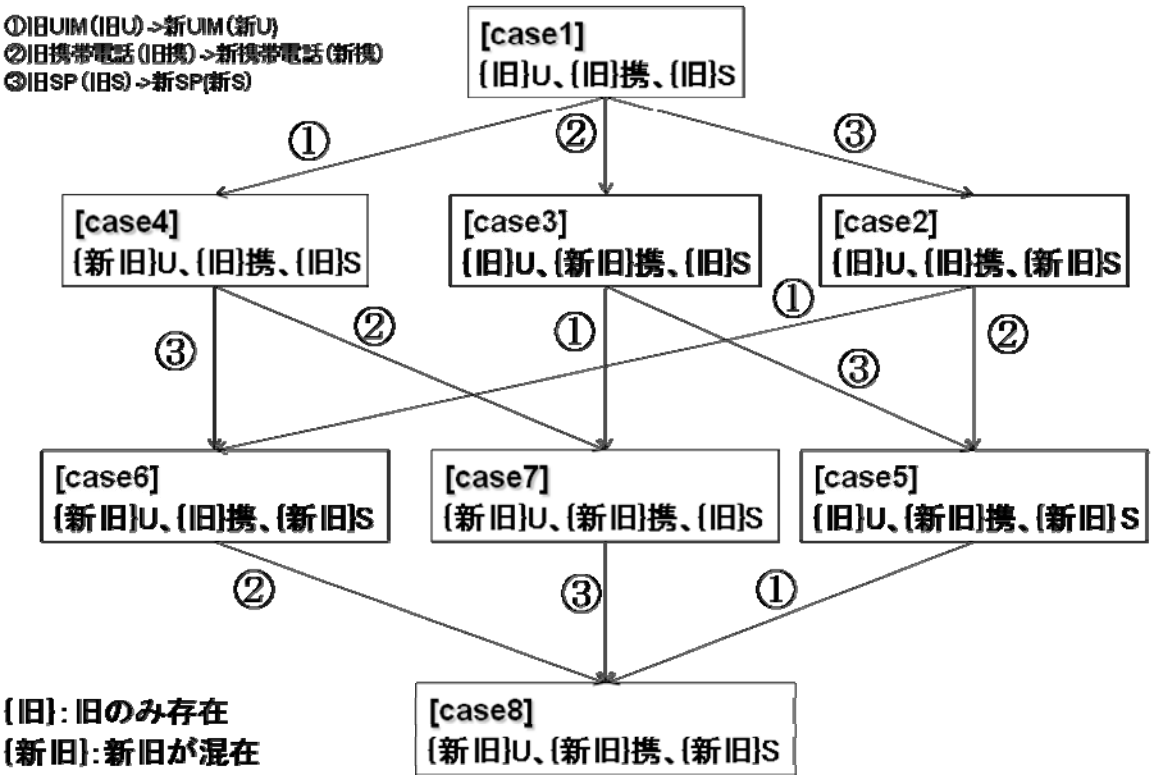
図表 3－1　移行モデルの定義（前提条件）

3.2. 現行運用から並行運用の移行シナリオ

現行運用から並行運用までの状態遷移を図表 3－2 に示す。また、図表中の各 CASE におけるサービス提供者、および、モバイル事業者の課題を図表 3－3 に示す。

CASE.2, CASE.5, CASE.6 のリスクについては、UIM もしくは携帯電話が商用リリースしていない状態で CA 局のみをリリースしたとしても、SP としてメリットがないことから、この状態遷移する可能性は低いと判断する。

また CASE.3 のリスクは、携帯電話販売時に UIM がリリースされていないため、SP 側、モバイル事業者側の双方で UIM リリース後に事後対応が必要となることである。



図表 3－2　現行運用から並行運用への状態遷移

: SP先行対応に伴うリスクあり　: 携帯電話先行対応に伴うリスクあり

CASE	UIM	携帯電話	SP	サービス提供者の課題	モバイル事業者の課題
1	{旧}	{旧}	{旧}	危殆化への懸念	
2	{旧}	{旧}	{新旧}	危殆化への懸念 {新旧}証明書に対応するための設定	携帯電話・UIM未提供の状態で CA局を先行リリースをするメリットがない
3	{旧}	{新旧}	{旧}	危殆化への懸念	UIM交換の対応
4	{新旧}	{旧}	{旧}	危殆化への懸念	
5	{旧}	{新旧}	{新旧}	危殆化への懸念 {新旧}証明書に対応するための設定	携帯電話・UIM未提供の状態で CA局を先行リリースをするメリットがない
6	{新旧}	{旧}	{新旧}	危殆化への懸念 {新旧}証明書に対応するための設定	携帯電話・UIM未提供の状態で CA局を先行リリースをするメリットがない
7	{新旧}	{新旧}	{旧}	危殆化への懸念	
8	{新旧}	{新旧}	{新旧}	{新旧}証明書に対応するための設定	

※モバイルID(CN)管理について
・モバイル事業者　：　CA内で新旧証明書のCN設定について要整理
・サービス提供者　：　CA側のCN設定でユーザ管理に影響あり

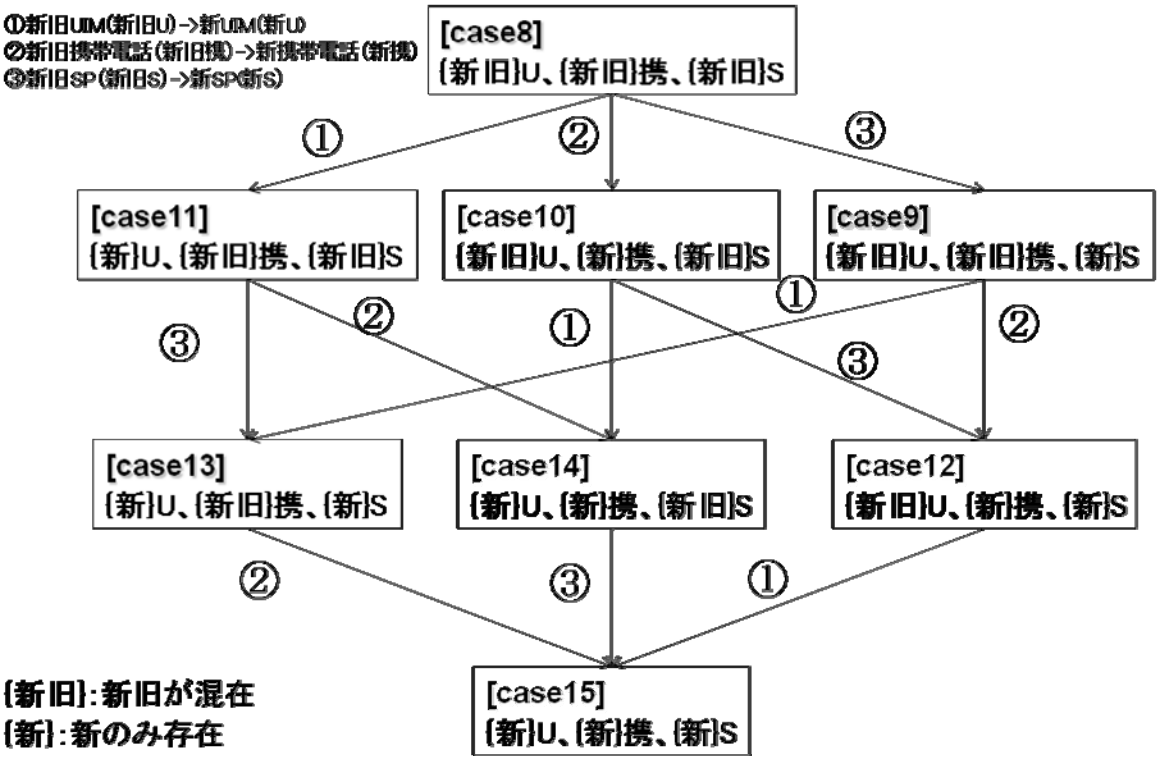
図表 3－3　現行運用から並行運用への移行における課題マトリクス

3.3.　並行運用から移行終了の移行シナリオ

並行運用から移行終了までの状態遷移を図表 3－4 に示す。また、図表中の各 CASE におけるサービス提供者、および、モバイル事業者の課題を図表 3－5 に示す。

CASE.10，12，14，15 については、携帯電話は UIM の差替えによって利用機種を容易に変更できることから、全ての以降を完了させることは困難である。

SP・モバイル事業者での対応，UIM のリリース間隔を考慮すると（CASE.8）⇒UIM（CASE.11）⇒SP（CASE.13）の順番で遷移していくのが望ましいと考えられる。



図表 3－4　並行運用から移行終了への状態遷移

：携帯電話の移行に関するリスク

CASE	UIM	携帯電話	SP	サービス提供者の課題	モバイル事業者の課題
8	{新旧}	{新旧}	{新旧}	{旧}方式をいつまで利用するかの判断が必要	{新旧}CA局の並行運用をいつまで続けるか？
9	{新旧}	{新旧}	{新}	{旧}方式の利用ユーザに{新}方式へどう案内するか？	{新旧}CA局の並行運用をいつまで続けるか？
10	{新旧}	{新}	{新旧}	売り切りの携帯電話を全て移行することは サービス提供者にもモバイル事業者にも制御不可	
11	{新}	{新旧}	{新旧}		UIMは貸与品であることから、 モバイル事業者にて移行を把握することが可能
12	{新旧}	{新}	{新}	売り切りの携帯電話を全て移行することは サービス提供者にもモバイル事業者にも制御不可	
13	{新}	{新旧}	{新}		UIMは貸与品であることから、 モバイル事業者にて移行を把握することが可能
14	{新}	{新}	{新旧}	売り切りの携帯電話を全て移行することは サービス提供者にもモバイル事業者にも制御不可	
15	{新}	{新}	{新}	売り切りの携帯電話を全て移行することは サービス提供者にもモバイル事業者にも制御不可	

※モバイルID(CN)管理について
・モバイル事業者 ： CA内で新旧証明書のCN設定について要整理
・サービス提供者 ： CA側のCN設定でユーザ管理に影響あり

図表 3－5　並行運用から移行終了における課題マトリクス

4. 移行時期についての考察

国内においては、内閣官房情報セキュリティセンター（NISC）が政府機関情報システム暗号方式の移行について指針を示している[資料[1][2]]。上記の指針によれば、SHA-1 および RSA-1024 について、SHA-2（SHA-256)およびRSA-2048 への移行対応を 2010 年度から開始、2013 年度末までに終了する予定である。さらに、2013 年以降は、複数方式が運用され、最終的には、移行後のアルゴリズムのみとなる予定である。

モバイル環境においても、これらの指針を踏まえ、各モバイル事業者のサービス、携帯電話、UIM のリリース時期を勘案しつつ、3 章の移行手順を考慮し、各モバイル事業者の判断にもとづいた対応を実施していくことが望ましい。

5. おわりに

暗号アルゴリズムの危殆化にともなう暗号アルゴリズムの移行について、モバイル事業者の PKI 認証基盤における署名アルゴリズム（ハッシュを含む）を対象とし、特にモバイル特有の環境（携帯電話と UIM）に焦点を当て検討を行った。本検討の結果、携帯電話利用者の利便性を損ねることなく、UIM、携帯電話、SP それぞれの運用要件を考慮したスムーズな移行が実現できることを机上にて実証した。

---

[1] 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（平成 20 年 4 月 22 日情報セキュリティ政策会議決定)」に基づく検討状況について」”, 資料 5-2, 平成 21 年 2 月 3 日
http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0502.pdf

[2] 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」の決定について”, 資料 1-1, 平成 20 年 4 月 22 日
http://www.nisc.go.jp/conference/seisaku/dai17/pdf/17siryou0101.pdf

暗号アルゴリズム移行における
オペレータ認証基盤の運用ガイドライン

MC-04　1.0 版

平成 23 年 12 月　1.0 版第 1 刷発行

発　行　所

一般社団法人　電　波　産　業　会
高度無線通信研究委員会モバイルコマース部会
〒100-0013　東京都千代田区霞が関１－４－１
日土地ビル１１階
電　話　03-5510-8594
ＦＡＸ　03-3592-1103