セコムIS研究所
Intelligent Systems Laboratory

PKI相互運用技術からみたSHA-1問題

セコム株式会社 IS研究所/
JNSA PKI**相互運用技術**WG**リーダー**
松本　泰

2006 **年** 6**月** 7**日**

セコムIS研究所
Intelligent Systems Laboratory

PKI相互運用技術からみたSHA-1問題

- SHA-1脆弱性問題
- ハッシュアルゴリズムのおさらい
- IETFでの動向
- タイムスタンプの認定制度とハッシュ関数
- 現実の問題　SSL証明書とMD5
- 米国政府の動向(NIST)
- 移行の問題 (最大の課題??)
- まとめ
- 参考

SHA-1脆弱性問題
電子政府推奨暗号リストでのハッシュアルゴリズム

セコムIS研究所
Intelligent Systems Laboratory

- 電子政府推奨暗号リスト　2003年3月20日
  - 新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。
  - http://www.soumu.go.jp/s-news/2003/030220_1.html
- SHA-1 の安全性に関する見解（案）　2006年XX月
  - このことは、SHA-1 を長期間にわたって利用する電子署名やタイムスタンプなどは、近い将来にSHA-1 の衝突発見が現実的な問題に発展する可能性を示唆している。このようなことから、**電子署名やタイムスタンプのように長期間にわたって利用するシステム**では、新規（更新を含む）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、256 ビット以上のハッシュ関数の使用を薦める。
  - http://www.ipa.go.jp/security/enc/CRYPTREC/fy17/documents/c05_wat_final.pdf
- セキュアジャパン2006(案)　2006年4月28日
  - 電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進めるとともに、電子政府推奨暗号のあり方の見直し等を含めた暗号利用に関する政府内の推進体制について、２００６年度に検討を開始する。
  - http://www.bits.go.jp/active/kihon/sj2006.html

SHA-1脆弱性問題
ハッシュ関数おさらい

セコムIS研究所
Intelligent Systems Laboratory

- ハッシュ関数
  - 任意長のデータを入力として固定長のデータ（ハッシュ値）を出力する機能
  - 一方向性と衝突困難性
- 代表的なハッシュ関数
  - MD5
    - 1991年にRivestが開発。
    - 128ビット
  - SHA-1
    - 1995年に、NSAが開発。
    - 160ビット
    - 後継としてSHA-2ファミリと呼ばれるSHA-224,SHA-256、SHA-384、SHA-512がある

SHA-1脆弱性問題
ハッシュ関数への攻撃

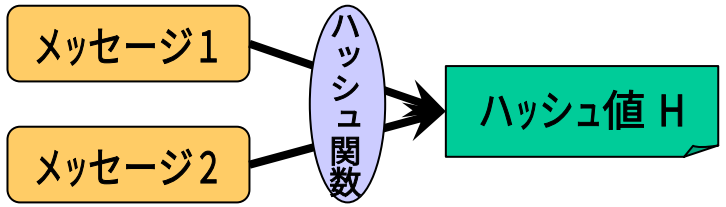
セコムIS研究所
Intelligent Systems Laboratory

衝突攻撃 (Collision Attack)

ハッシュ値が同じになる
任意のメッセージペアを見つける。

計算量

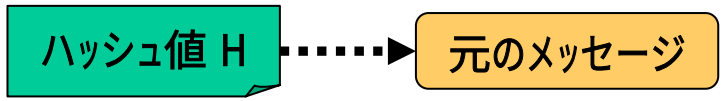
$2^{n/2}$



原像探索攻撃 (Pre-image Attack)

あるハッシュ値Hから
元のメッセージを見つける。

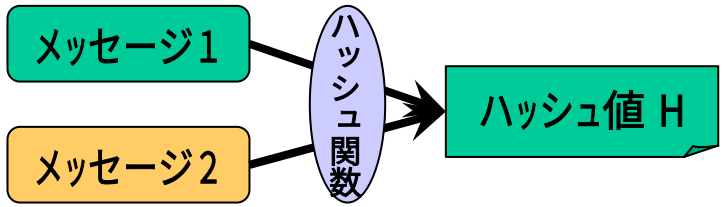
2^{n}



別原像探索攻撃(Second Pre-image Attack)

あるメッセージとハッシュ値が
同じになる別のメッセージ
を見つける

2^{n}



SHA-1脆弱性問題
ハッシュ関数に関する危殆化の報告

セコムIS研究所
Intelligent Systems Laboratory

- MD5
  - 2004年、X. Wangらにより、Collisionが2^{-37}で発見できることが発表される。
  - 2005年、A. Lensta、X. Wangらにより、ハッシュ値が衝突した2つの証明書ペアが作成される。
  - 2005年、V. Klimaがより高速にCollisionを発見する手法を提示。
- SHA-1
  - 2005年2月、X. WangによりCollisionが2^{-69}で発見できることが発表される。
  - 2005年10月、同じくCollisionが2^{-63}で発見できると発表される。

IETFでの動向
CRYPTREC等とのレイヤーとの違いがある

セコム IS 研究所
Intelligent Systems Laboratory

- SHA-256などSHA2ファミリーへの移行
  - 移行負荷が大きい。時間もかかる。
  - 運用だけでなく**関連アプリケーションとの相互運用性**についても配慮の必要あり
- SHA-1互換の安全な実装検討
  - 上記のような関連アプリケーションとの相互運用性問題を回避するため、現行SHA-1とできるだけ互換性の高い改善案の検討
    - IETF Hash BOFの3つの提案(63rd IETF ミーティング（パリ）)
- 新しいハッシュ関数を組み込んだTLS 1.2の検討
  - Eric Rescorla(TLS WG Chair)とSteve Bellovin（IETFセキュリティエリアの元ディレクタ）の見解
  - RFC化に2年、ベンダが設計・開発・テストするのにもう1,2年、展開に3～5年

IETFでの動向
RFC 4270（2005年11月）

セコムIS研究所
Intelligent Systems Laboratory

- インターネットプロトコルにおける暗号技術的ハッシュ関数についての攻撃
- “Attacks on Cryptographic Hashes in Internet Protocols”
  - P. Hoffman (VPNC)
  - B. Schneier (Counterpane Internet Security)
- 現状の説明と、現実的脅威の低さを強調
- その上で、両者の異なる意見を載せている
  - SHA-256への移行
    - すぐ移行を (B.Schneier)
    - (まだ) 賢明でない (P.Hoffman)
  - 新しいプロトコルでのハッシュ利用
    - 最初からSHA-256を使うこと (B.Schneier)
    - Collision攻撃の影響を受けない限りSHA-1を使う必要がある (P.Hoffman)

IETFでの動向
RFC 4346bis (TLS 1.2)

セコム IS 研究所
Intelligent Systems Laboratory

- Hash Agileなプロトコル設計
- MD5/SHA-1攻撃への対応が主題
- AESにも対応
- Downgrade protectionと脅威とのバランス
  - 今のところ脅威はない。
  - 動かなくなる実装があるのに積極的に取り組む必要ある?

•RFC 4346bis

•http://www.ietf.org/internet-drafts/draft-ietf-tls-rfc4346-bis-00.txt

•Deploying a New Hash Algorithm

–http://csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Bellovin_new-hash.pdf

•http://www.cs.columbia.edu/~smb/papers/new-hash.pdf

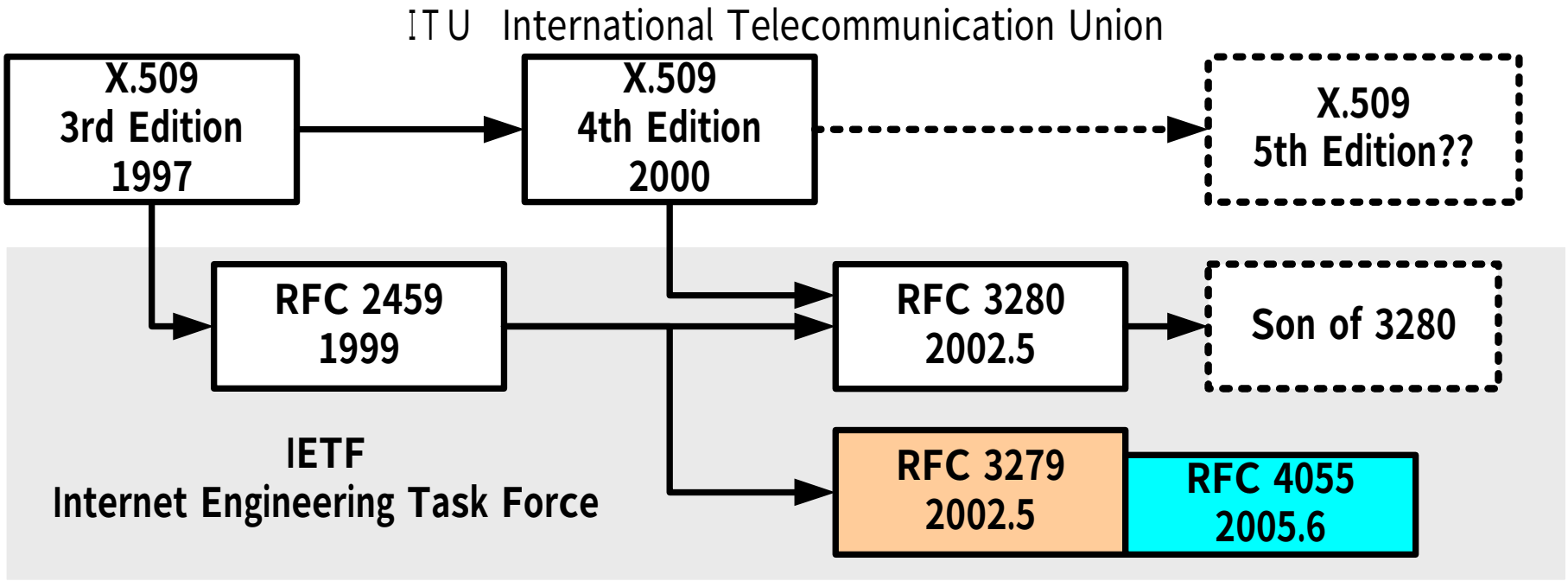
•Steven M. Bellovin and Eric K. Rescorla

IETFでの動向
Hash Agility、Algorithm Agility

セコム IS 研究所
Intelligent Systems Laboratory

- 古典的インターネットプロトコル
  - そもそも固定長のプロトコルフォーマットが多かった
- 暗号アルゴリズム依存
  - 仕様上(RFC)で暗号アルゴリズムを分離するようになったのは最近
  - 多くのプロトコルは、暗号アルゴリズムに依存している
- OCSP(RFC 2510)の例
  - SHA-1に依存している。
  - Hash Agilityなプロトコルにするためには仕様の改訂が必要
- Algorithm Agility in PKIX
  - http://www3.ietf.org/proceedings/06mar/slides/pkix-1/pkix-1.ppt
  - ハッシュだけでなく暗号アルゴリズムのAgility

IETFでの動向
ITU-T X.509とPKIX RFC3280



- RFC 3279
  - RFC 3280 (証明書プロファイル) で用いる暗号アルゴリズム
- RFC 4055 インターネットX.509 PKI 証明書と CRL 用 RSA 暗号技術についての追加的アルゴリズムおよび識別子　2.1.　One-way Hash Functions
  - http://www.ipa.go.jp/security/rfc/RFC4055EN.html#21
  - id-sha224, id-sha256, id-sha384, id-sha512

IETFでの動向
Hash Agility、Algorithm Agility

- IPA**の宮川さんの**Blog**の**
  - https://www.codeblog.org/blog/Miyakawa/20060515.html
  - IETF のセキュリティ・エリアの各 WG に共通する最近の話題は、「ハッシュ・アジリティ (ハッシュ関数の取り替え可能性の確保) 」です。ここで導入される考え方は、「**よりセキュアなアルゴリズムに移行できるようにすべきである**」ということですが、これをより進めた主張は、「**よりセキュアなアルゴリズムに移行しなければならない**」となります。ここで何が起きるかというと、「従前は是とされてきた**下位互換性の確保を断ち切らなければならない**」ことになります。下位互換性を確保することは、良くないこととされる可能性があるのです。したがって、相互運用可能性テストも変わります。

これまでのインターネットプロトコルの開発の常識を超えている。これまでのインターネットプロトコルの開発は、Simple なプロトコルと実装を、下位互換性を確保しつつ、少しずつ進化してきた。送り手は保守的に受け側は革新的に。。。。で

タイムスタンプの認定制度とハッシュ関数
タイムスタンプ認定制度の変更点

セコム IS 研究所
Intelligent Systems Laboratory

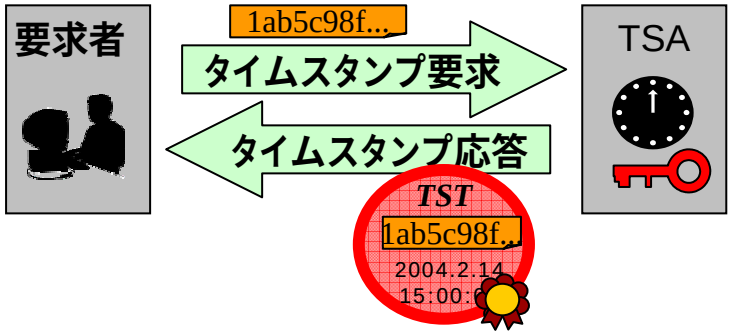
- 日本データ通信協会のタイムビジネス信頼・安心認定制度
  - http://www.dekyo.or.jp/tb/tbtop.html
- 日本データ通信協会のタイムビジネス信頼・安心認定制度の審査基準（2005年6月16日）
  - http://www.dekyo.or.jp/tb/shinsakizyun(DSHA-1henkou)2ndV0506.pdf
  - ハッシュ関数のビット長を2006年4月1日以降は256bit以上とすることを追記
    - messageImprintのhashAlgorithmが対象
    - TSAによる署名アルゴリズムは対象外
      - 電子政府推奨暗号リストに従うこと
- SHA-1 脆弱化対応に関する「移行猶予期間」の設定について（2006年2月21日）
  - 組み込みシステムに限り2006年12月31日までSHA-1の利用を認める（2006年2月21日決定）
  - 「組み込みシステム」の定義なし??

タイムスタンプの認定制度とハッシュ関数
タイムスタンププロトコル上の該当領域

セコムIS研究所
Intelligent Systems Laboratory

TimeStampReq (タイムスタンプ要求)

- version（バージョン番号：v1）
- messageImprint（ハッシュアルゴリズムのOIDとハッシュ値）
- reqPolicy（TSAのポリシID）
- nonce（オプション：リプレーアタック防止の大きな整数）
- certReq（オプション：TSAの証明書要求フラグ）
- extensions（オプション：要求の拡張領域）



TimeStampResp (タイムスタンプ応答)

status（要求に対する応答の状態：正常／拒否／その他）
TimeStampToken（ContentInfoと署名対象データ（TSTInfo）から成る）

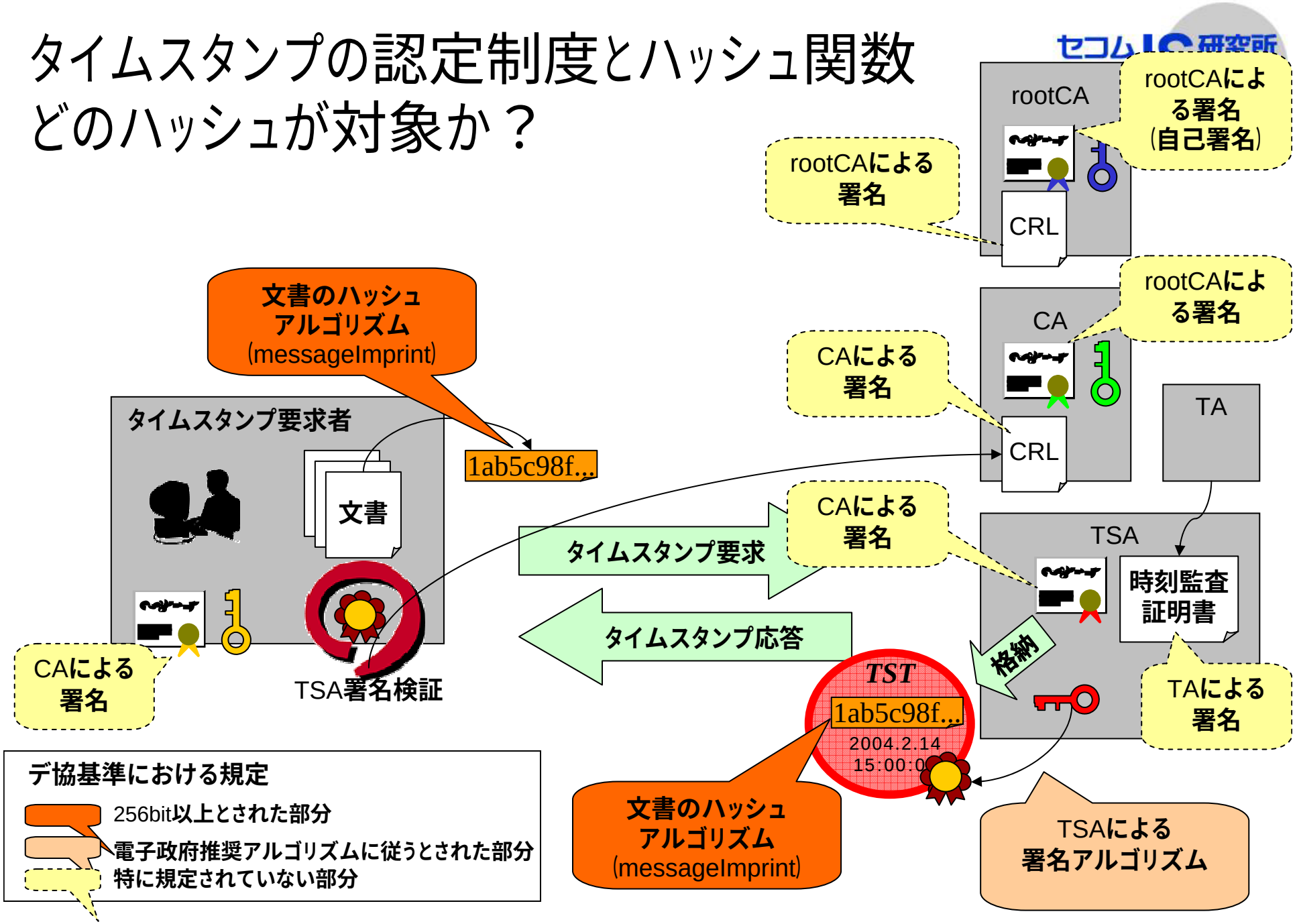
ContentInfo

- version（CMSバージョン番号：v1/v3）
- digestAlgorithms（ハッシュ関数のOID）
- encapContentInfo（署名対象データに関する情報）
  - eContentType(署名対象データの型)
  - eContent（署名対象データ：TSTInfo）
- certificates（TSA証明書、TAの時刻監査証明書）
- signerInfos（署名者に関する情報）
  - version（CMSバージョン番号：v1/v3）
  - sid（署名者（TSA）識別子）
  - digestAlgorithm（署名用ハッシュ関数のOID）
  - signedAttrs（署名の対象となるデータのハッシュ値）
  - signatureAlgorithm（署名アルゴリズムのOID）
  - signature（署名値）

TSTInfo

- version（トークンのバージョン：v1）
- policy（TSAのポリシOID）
- messageImprint（要求のmessageImprintと同じ）
- serialNumber（トークンのシリアル番号）
- genTime（UCT Time表記）
- accuracy（オプション：時間精度）
- ordering（オプション：順序付けのフラグ）
- nonce（要求のnonceと同じ）
- tsa（オプション：TSA証明書のsubject名）
- extensions（オプション：応答の拡張領域）

タイムスタンプの認定制度とハッシュ関数
どのハッシュが対象か？



現実の問題　SSL証明書とMD5
ルート証明書におけるハッシュ関数利用

セコム IS 研究所
Intelligent Systems Laboratory

	MD2	MD5	SHA-1
IE	11 (9.8%)	47 (42.0%)	54 (48.2%)
Opera	4 (5.5%)	20 (27.4%)	49 (67.1%)

現実の問題　SSL証明書とMD5

セコムIS研究所
Intelligent Systems Laboratory

某サイト

- NI*C
  - https://www2.bits.go.jp/opinion.html
  - SSL証明書　　md5withRSA
  - 自己署名証明書　md2withRSA

- *政府機関の情報セキュリティ対策のための統一基準（２００５年項目限定版）*
  - *http://www.bits.go.jp/active/general/pdf/2siryou04-3d.pdf*
  - *(e) 情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択すること。なお、複数のアルゴリズムを選択可能な構造となっている場合には、少なくとも一つを電子政府推奨暗号リストの中から選択すること。*

現実の問題　SSL証明書とMD5
代表的なSSL証明書のルート証明書

セコムIS研究所
Intelligent Systems Laboratory

認証プロバイダー	CA名	ハッシュ	鍵の種類	有効期限
A	a	SHA1	RSA1024	2018年8月23日
	b	MD5	RSA1024	2020年6月21日
B	c	MD2	RSA1024	2028年8月2日
	d	MD5	RSA1024	2021年1月1日
	e	MD5	RSA1024	2021年1月1日
C	f	MD2	RSA1024	2028年8月2日
	g	MD2	RSA1000	2010年8月8日
D	h	MD5	RSA1024	2018年8月14日
E	i	SHA1	RSA1024	2019年6月26日
F	j	SHA1	RSA1024	2019年5月26日

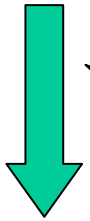
現実の問題
SSL証明書に対する脅威の考察（1）

セコム IS 研究所
Intelligent Systems Laboratory

現実的な脅威はない

現時的な脅威となっているのは、（Second）Preimage攻撃
ではなくCollision攻撃

- **あるメッセージに対して、同じハッシュ値をもつ別のメッセージを作ることに関して脆弱なわけではない**
- **現在の攻撃は少なくとも2つのメッセージの片方に一定の構造を持つことが要求される。**



もし（Second）Pre-image攻撃がうまくいったとしても

意味のあるSSL証明書のペアが出来るには
さらに高いハードルがある

現実の問題
SSL証明書に対する脅威の考察（2）

セコムIS研究所
Intelligent Systems Laboratory

もし（Second）Pre-image攻撃が自由にできるとしても

同一名称
特定のAという人になりすまして、証明書を利用
（発行先名称などは同一、公開鍵が異なる）

同一公開鍵
Aという名称として発行された証明書（のハッシュ値）を別のBとして利用
（公開鍵は同一、発行先名称などが異なる）

別公開鍵・別情報
Aという名称として発行された証明書（のハッシュ値）を別のBとして利用
（公開鍵、発行先名称ともに異なる）

いずれのケースも
プライベート鍵(CA,EE)が必要

ハードルは高い

SSL証明書発行後に
対応した鍵ペアを作成（同一名称）

SSL証明書発行後に
対応した証明書を作成（同一公開鍵）

移行の問題
暗号アルゴリズムの危殆化問題、移行問題

セコム IS 研究所
Intelligent Systems Laboratory

- 現実の世界
  - MSの証明書リストにある107個の自己署名証明書
    - MD5(46個)、MD2(11個)、SHA1(50個)
  - 自己署名証明書の有効期間は、10年から20年
  - これらは「信頼できる認証局の信頼点」になり得るのか？
    - MD5がダメといいつつMSの「信頼できる認証局の信頼点」を無条件に受け入れてはいないか？。こうしたギャップは埋められるものなのか？
- どうやって移行（マイグレーション）するのか??誰が全体を取りまとめるか??
  - 政策担当者(電子政府など)、暗号関係者、アプリケーション開発ベンダー、認証局、PKI標準化関係者等。これらの2者以上で会話することは極めて稀（3者は皆無、かつ。会話が成り立たない？）

移行の問題
SHA-1からの移行の問題 – デッドロック状態になるかも

セコム IS 研究所
Intelligent Systems Laboratory

- 暗号関係者 – CRYPTREC等
  - SHA2ファミリーに移行してね。。。
- (PKIなどの)標準仕様の策定者の悩み - IETFでの議論
  - 現実として展開されているプロトコルやフォーマットとの整合やマイグレーションの方法
- PKIミドルウェア(セキュリティ・ミドルウェア)開発者の悩み
  - 標準が曖昧でマイグレーションを考えると複雑な実装になってしまう。
  - #最新のバージョンのOS対応だけでいいよね？。。。。。
- アプリケーションベンダーの悩み
  - PKIミドルウェア頼み。悩みがないわけでもないが分からない。。。
  - #そもそも、そんな費用誰が負担するの??
- CA (認証局) 運営者の悩み
  - CAは、アプリケーションが対応しない限り、 SHA2ファミリに対応した証明書を発行できない。。。移行できない。
- (電子政府などの)??の悩み
  - ???

移行の問題
認証局の鍵更新

セコム IS 研究所
Intelligent Systems Laboratory

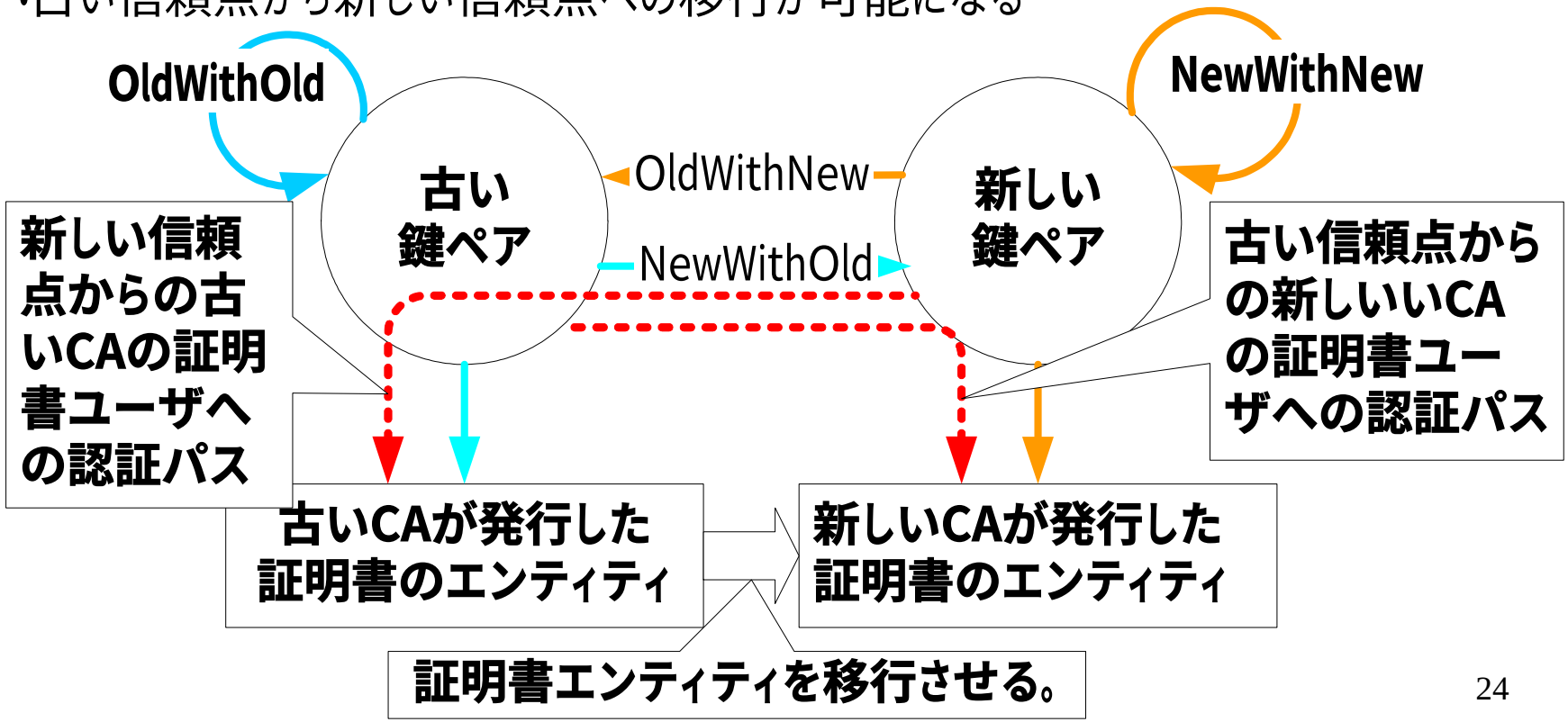
- 認証局の私有鍵(署名鍵)
  - 認証局にとって「鍵(署名鍵)は命」　-　認証局に限らずあるべきアーキテクチャ
- GPKI (政府認証基盤)の認証局の自己署名証明書と署名
  - 現在の暗号アルゴリズム　RSA (2048bit) With SHA-1
  - 自己署名証明書の有効期間　10年の有効期間
  - 署名鍵(私有鍵)の有効期間　5年 (5年で鍵更新)
- なぜ鍵更新が重要か
  - 鍵の耐用年数、暗号アルゴリズムの耐用年数などの対応だから。
    - つまり「鍵更新」は、Long-Term Security対応の技術
  - あまり長い自己署名証明書の有効期間は怪しい
- 鍵更新の課題は？(すなわちLong-Term Security対応の課題)
  - 標準化、相互運用性、クライアントの実装(セキュリティミドルウェア)の展開

鍵更新の重要性は、PKI(認証局) に限ったことではない。暗号を利用してLong-Term Securityを実現するためには、重要なはず。

移行の問題
鍵更新のメカニズム

セコム IS 研究所
Intelligent Systems Laboratory

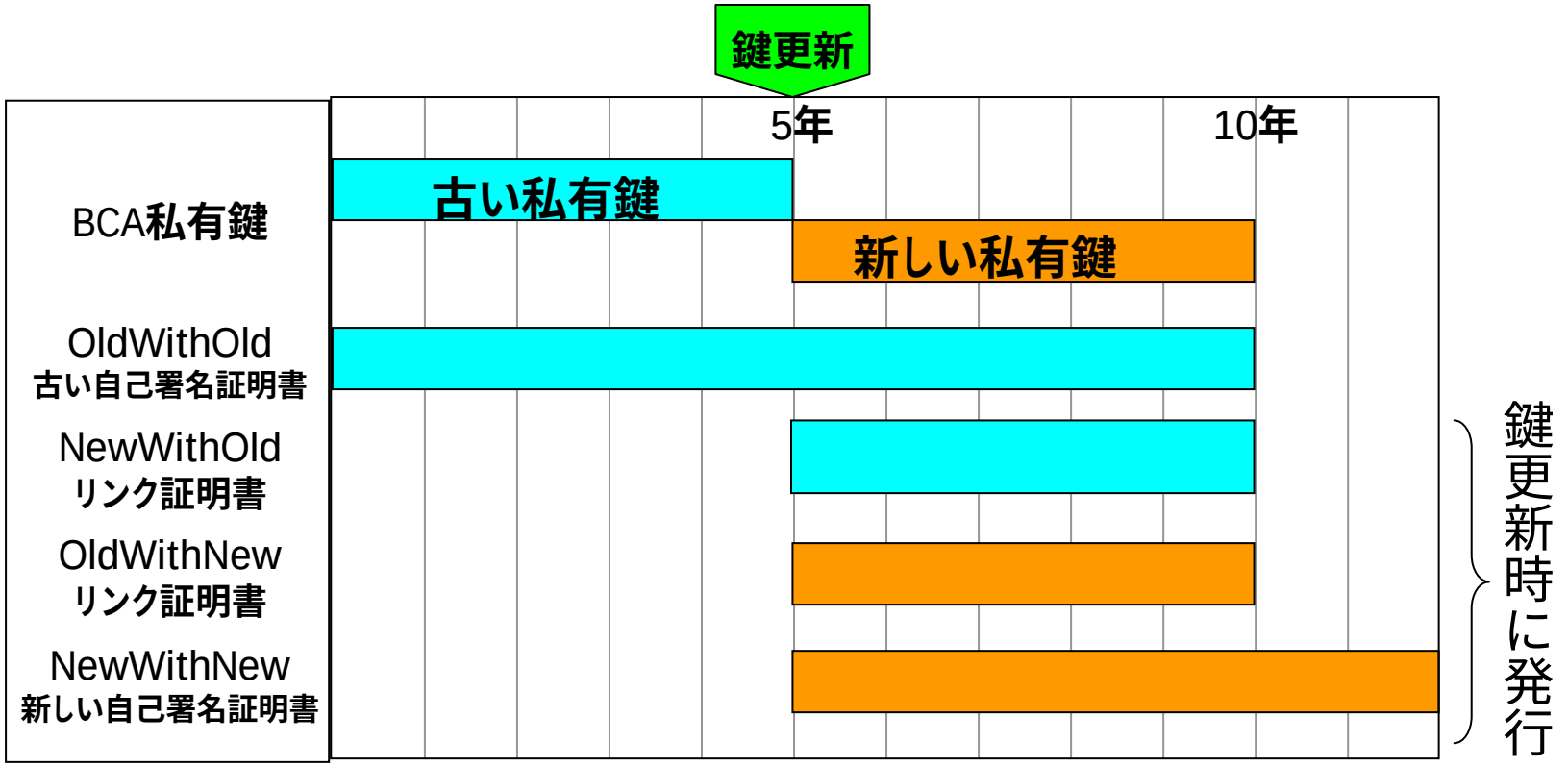
- 新しい鍵ペアと古い鍵ペアの関係を証明する自己発行証明書(Self Issue Certificate)が発行される。
  - 古い公開鍵を新しい私有鍵で署名した証明書(OldWithNew)
  - 新しい公開鍵を古い私有鍵で署名した証明書 (NewWithOld)
- 古い信頼点から新しい信頼点への移行が可能になる



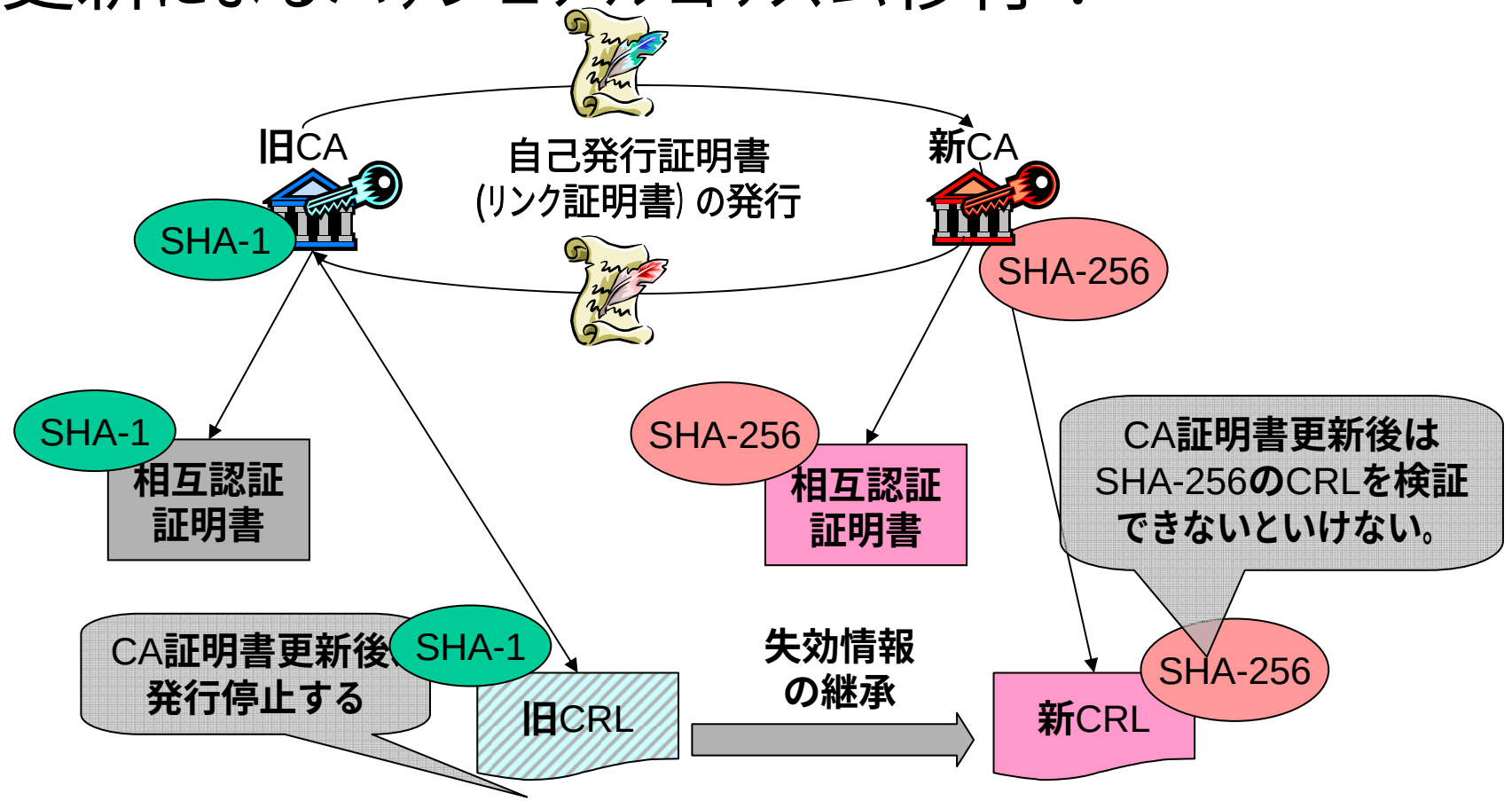
移行の問題
ブリッジモデルにおける鍵更新の考え方

セコム IS 研究所
Intelligent Systems Laboratory

GPKIブリッジ認証局の鍵更新における自己署名証明書とリンク証明書の関係



移行の問題
鍵更新によるハッシュアルゴリズム移行？



クライアント (署名検証者) が認証局の鍵更新のメカニズムに対応した証明書検証を実装し、ハッシュ関数としてSHA2に対応していない限り、認証局はSHA2等の証明書を発行できない。認証局ではなくクライアントの対応 (展開) が鍵。

移行の問題
電子政府現状のステータス？？

セコム IS 研究所
Intelligent Systems Laboratory

仕様、規定など	ハッシュアルゴリズムの扱い
電子政府推奨暗号リスト	新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。
電子署名法 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針	署名に対するハッシュアルゴリズムの規定はない？
電子政府(政府認証基盤相互運用性仕様書)	エンドエンティティは署名検証する際、署名者側が使用する署名アルゴリズムをサポートしていなければならない。署名アルゴリズムとして、以下が考えられる。 sha1WithRSAEncryption (1.2.840.113549.1.1.5) dsaWithSha1 (1.2.840.10040.4.3) md5WithRSAEncryption (1.2.840.113549.1.1.4) なお、md5WithRSAEncryption は過去の互換性のためにサポートするもので、新規に発行した証明書や署名データはmd5WithRSAEncryption を含まないものと想定する。

米国政府の動向(NIST)
Hash Algorithms (for digital signatures)

セコム IS 研究所
Intelligent Systems Laboratory

	Unclassified use		Suite B	
	Through 2010	***After 2010***	Secret	Top Secret
SHA-1	√			
SHA-224	√	√		
SHA-256	√	√	√	
SHA-384	√	√	√	√
SHA-512	√	√		

"NIST Cryptographic Standards Status Report", Bill Burr, NIST (April 2006)
http://middleware.internet2.edu/pki06/proceedings/burr-nist_crypto_standards.ppt

**** SHA-224があることに注意*

米国政府の動向(NIST)
Digital Signature

セコム IS 研究所
Intelligent Systems Laboratory

	Unclassified use		Suite B	
	Through 2010	After 2010	Secret	Top Secret
FFC or IFC (DSA or RSA)				
1024	√			
2048	√	√		
3072	√	√		
ECC				
160	√			
224	√	√		
256	√	√	√*	
384	√	√	√*	√*
512	√	√		

*** Prime Modulus curves only**

楕円暗号にシフトしていくかもしれない

まとめ

セコムIS研究所
Intelligent Systems Laboratory

- SHA-1脆弱性問題に限らず、暗号アルゴリスムの危殆化問題は、Long-termセキュリティの観点が必要
  - ハッシュアルゴリズムで一番多く利用されているのはたぶんMD5。これらがすべて問題がある訳ではない。
  - 移行には、ロードマップを示すことが重要。移行には長い時間がかかる。
- 暗号アルゴリズムの移行には、相互運用技術の観点からの検討が必須
  - 鍵更新、Hash Agility、Algorithm Agility、 Downgrade protection、etc….

参考

- 暗号アルゴリズムにおける2010年問題について　2005/11
  - http://www.imes.boj.or.jp/japanese/jdps/2005/05-J-22.pdf
  - 宇根 正志・神田 雅透
- RFC 4270　　2005年11月
  - インターネットプロトコルにおける暗号技術的ハッシュ関数についての攻撃
  - http://www.ipa.go.jp/security/rfc/RFC4270JA.html
  - P. Hoffman　VPN Consortium、B. Schneier　Counterpane Internet Security
- Deploying a New Hash Algorithm
  - http://csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Bellovin_new-hash.pdf
  - Steven M. Bellovin and Eric K. Rescorla. September 2005
- Algorithm Agility in PKIX
  - Tim Polk March 20, 2006
  - http://www3.ietf.org/proceedings/06mar/slides/pkix-1/pkix-1.ppt
- Attacks on MD5 and SHA-1: Is this the “Sword of Damocles” for Electronic Commerce?
  - http://www.isi.qut.edu.au/people/subramap/AusCert-6.pdf
- NIST Cryptographic Standards Status Report　　Tuesday, April 4, 2006
  - http://middleware.internet2.edu/pki06/proceedings/burr-nist_crypto_standards.ppt
  - Bill Burr, NIST
- 「CRYPTREC Report 2005 暗号技術監視委員会報告書」
  - http://www2.nict.go.jp/y/y213/cryptrec_publicity/c05_wat_final.pdf
  - 平成18 年3 月