IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

「暗号の世代交代」

独立行政法人　情報処理推進機構
セキュリティセンター　暗号グループ
山岸　篤弘＆松本　泰＆NTT　神田　雅透

a-yamagi@ipa.go.jp
http://www.ipa.go.jp/security/

Contents

1. 暗号の現状
   ～ NISTの見解と2010年問題 ～
2. NISCの動向（移行方針）
3. CRYPTRECの今後

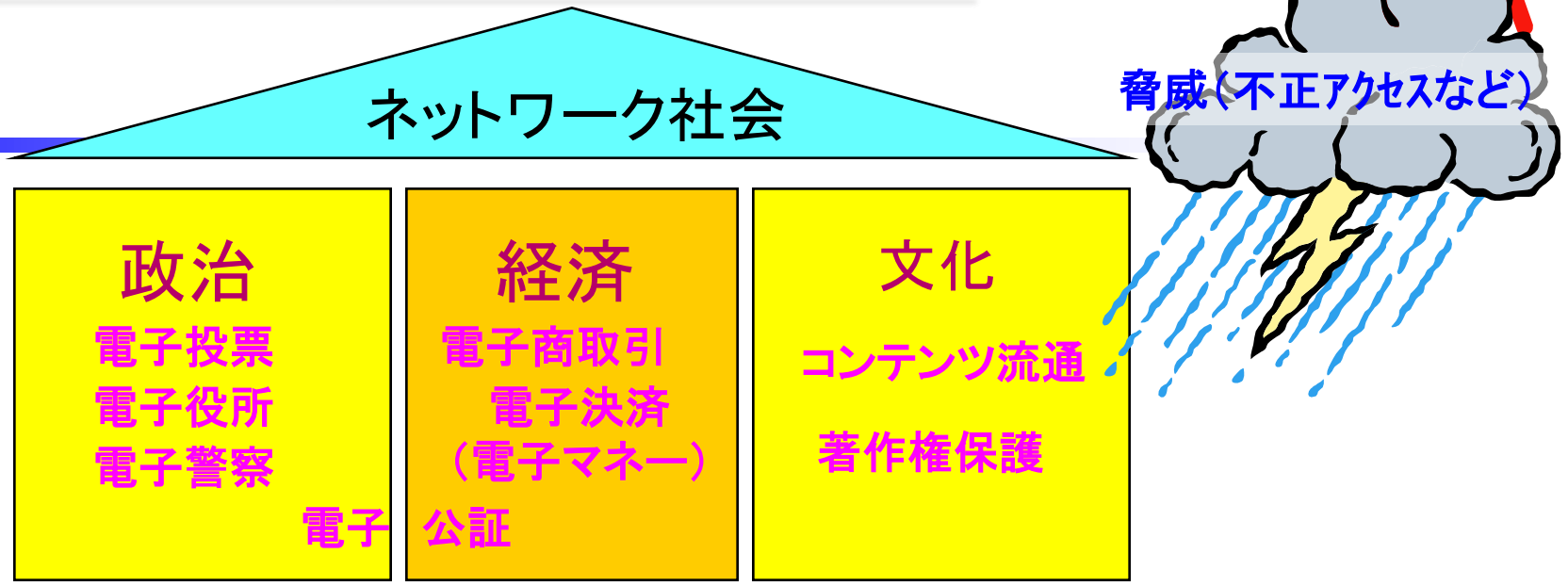
暗号って何？

- 現代暗号（1977年以降～）
  - 特に、公開鍵暗号を利用することが前提
  - 機密性
    - 「守秘」、現代暗号以前の特性
  - 完全性
    - データが改ざんされていないことを保証
    - ハッシュ関数、データ認証子（MAC)、ディジタル署名
  - 相手認証
    - データの出所を確認できる
    - 鍵管理、PKI（公開鍵暗号基盤）、ディジタル署名
  - 否認拒否
    - データの送信を特定できる
    - PKI（公開鍵暗号基盤）、ディジタル署名
  - アクセス制御
    - データに対する権限管理
    - 鍵管理

PKI: (Public Key Infrastructure)

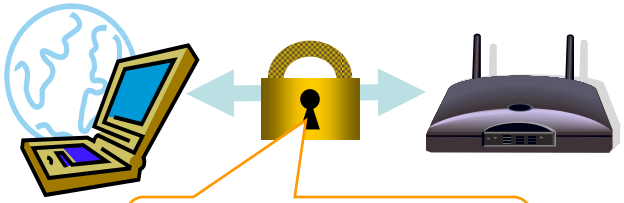
電子情報通信学会誌900号より

情報セキュリティ技術が支えるネットワーク社会



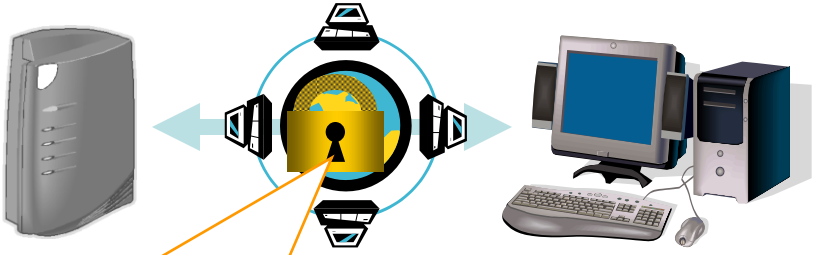
暗号技術の用途

多くのシステムで利用されている
暗号の安全性低下が無視できなくなってきた



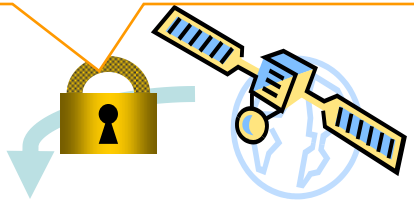
【無線LAN】
無線通信の暗号化

【暗号化USB】
持出データの暗号化



【HTTPS (SSL/TLS)】
インタネット上の通信の暗号化
サーバの認証

【CAS】
デジタル放送データの暗号化



【携帯電話】
携帯電話の認証
データの暗号化

【HDD暗号化】
持出しPCの暗号化

【ICカードのチップ】
カードの認証
電子マネー等の不正防止

MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造 JVNの公開日：2009/01/07

- 概要
  - MD5 アルゴリズムの衝突耐性の不備を利用した攻撃法により、X.509 証明書の偽造に成功した
- 詳細情報
  - 一方向性ハッシュ関数である MD5 は入力値から固定長のメッセージダイジェストと呼ばれる値を出力します。安全なハッシュ関数は特定のメッセージダイジェストに対応する入力値を見つけることが極めて困難である必要があります。異なる入力から同一のメッセージダイジェストが出力される事を〝衝突〟と呼びます。
  - 1996 年から MD5 アルゴリズムの衝突耐性の不備を利用した攻撃法が報告されています。その後、この攻撃手法が X.509証明書の偽造に使えることが示され、2008年に CA によって署名された証明書をもとに中間 CA 証明書の偽造に成功したことが報告されました。
- 対策方法
  - 以下の対策方法が考えられます。
  - MD5 アルゴリズムを使用しない
  - MD5 で署名されている証明書については偽造されている可能性があることに注意する

実態は？

- 調査対象：

  政府・公共系サイト及び金融系サイトの各トップページからたどることができるSSLサーバ
- 調査期間：2008年10月～11月
- 調査内容：
  - サーバ証明書の状況（有効期限、アルゴリズム、鍵長等）

中間調査結果を少々・・・（重複あり）
政府・公共系：147サーバ、金融系：138サーバ

Firefox3）

暗号選択状況の検査方法

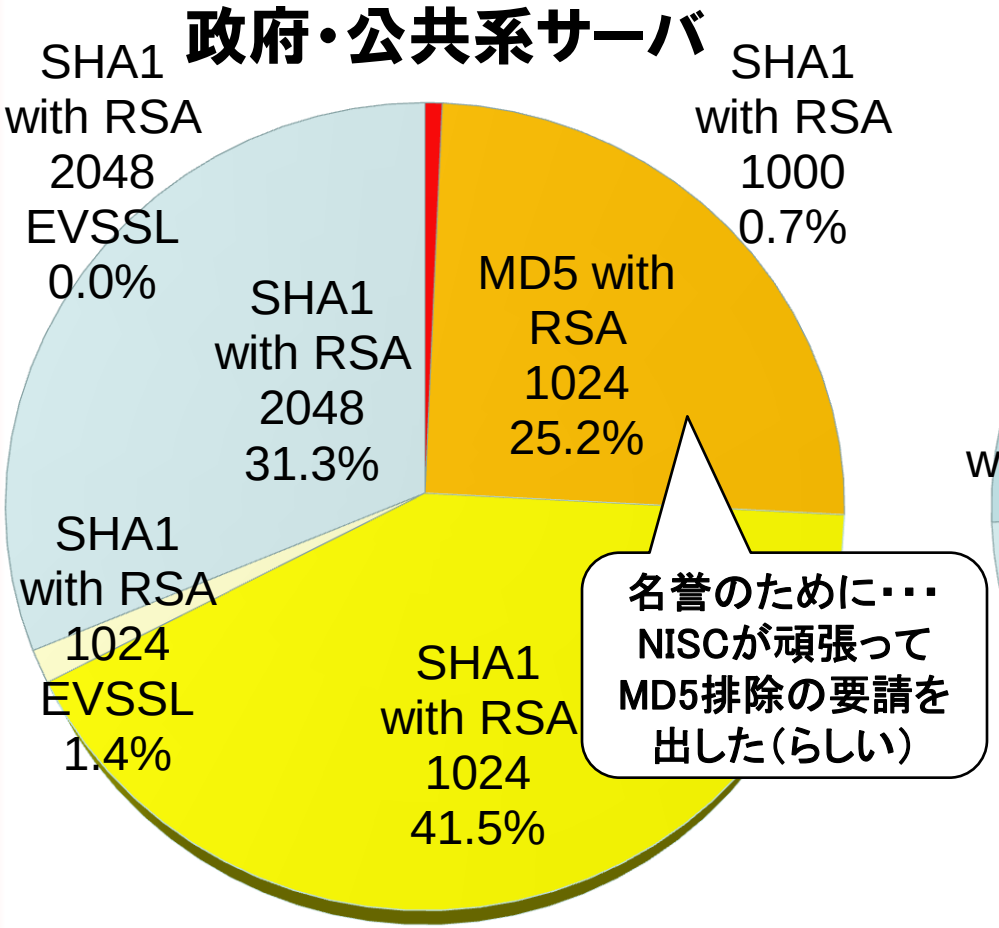
- 暗号スイート単位で選択

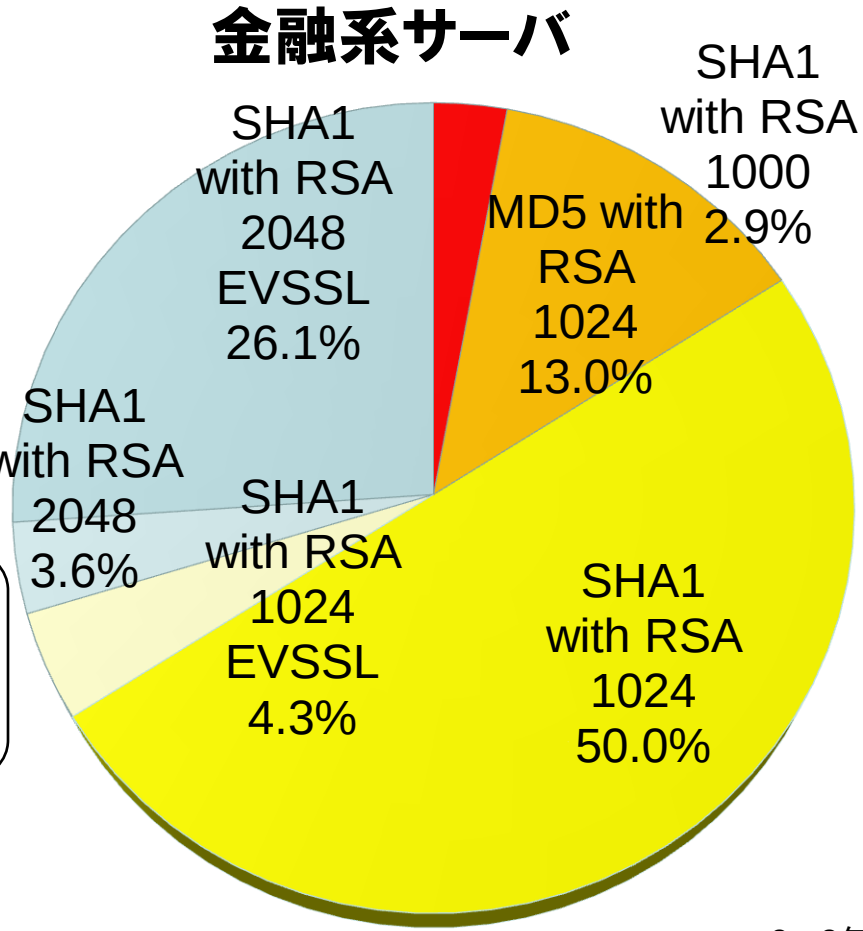
  「(鍵交換)ー(署名)ー(共通鍵暗号)ー(ハッシュ関数)」

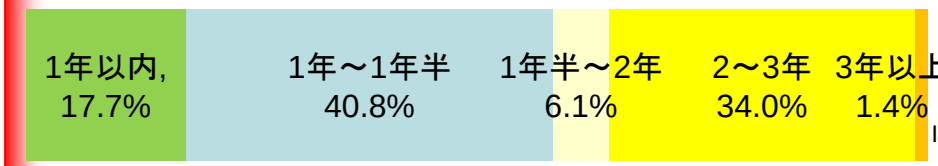
  - DHE – RSA – AES256 – SHA
  - (RSA – RSA –) RC4 – SHA
  - EXP – (RSA – RSA –) DES – CBC – MD5
  - ・・・・・

- 43種類の暗号スイートについて
  - 1回の接続要求に対して1つの暗号スイートだけを提示
  - 接続に成功すれば受入可能な暗号スイート

サーバ証明書の状況 （アルゴリズムと有効期限）

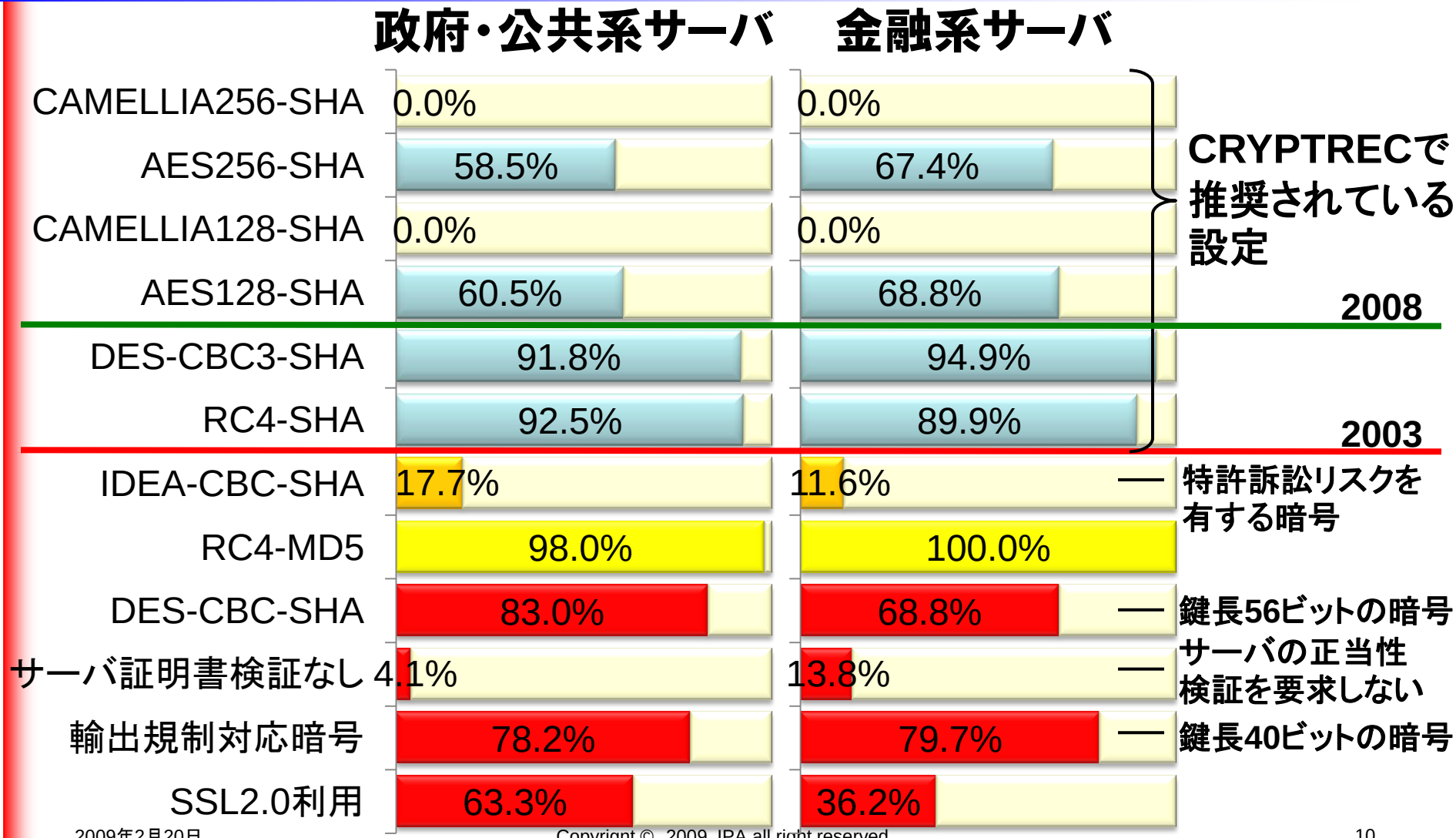




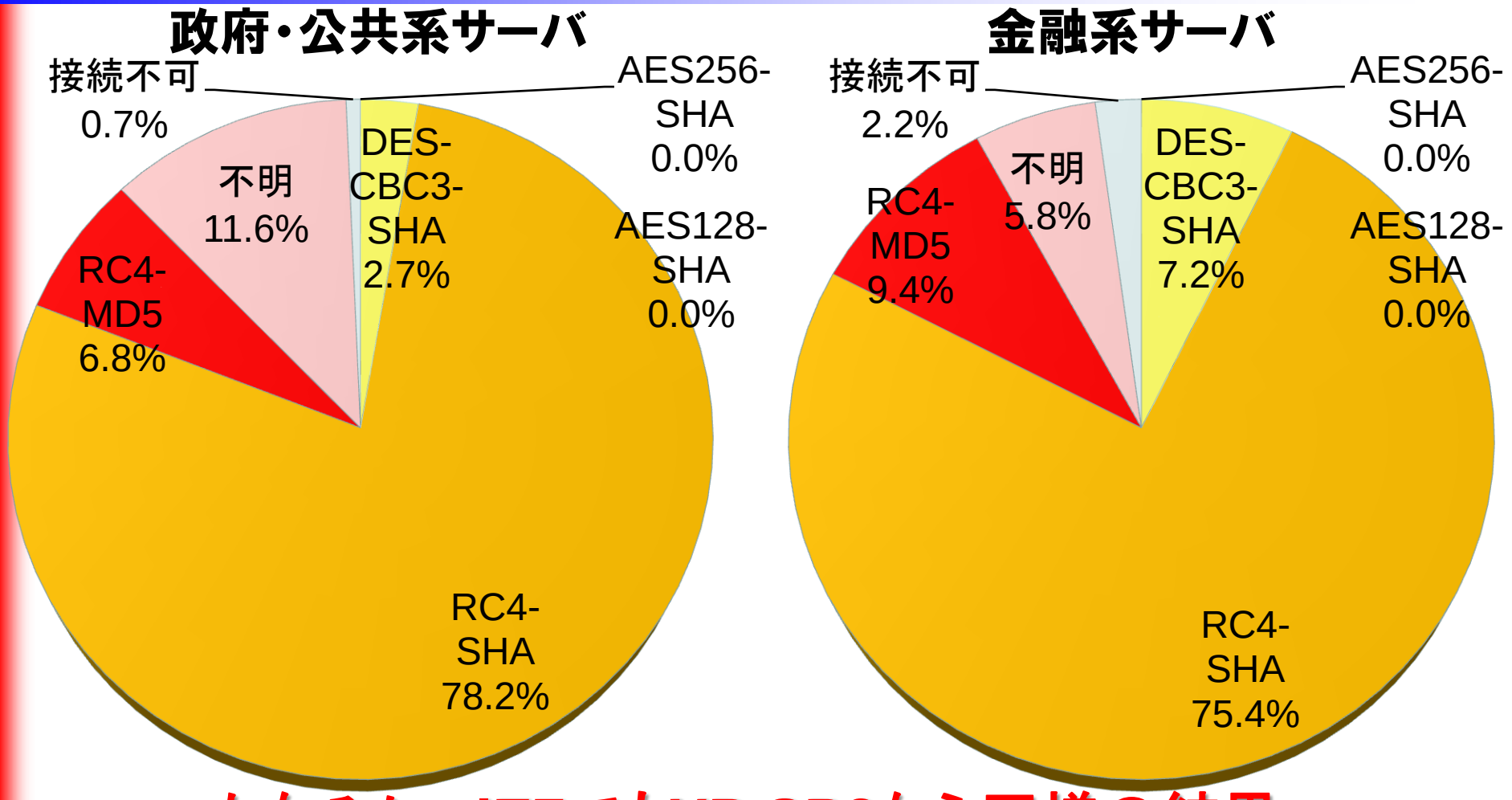


IPA

サーバでの暗号設定　～受入可能な主な暗号～

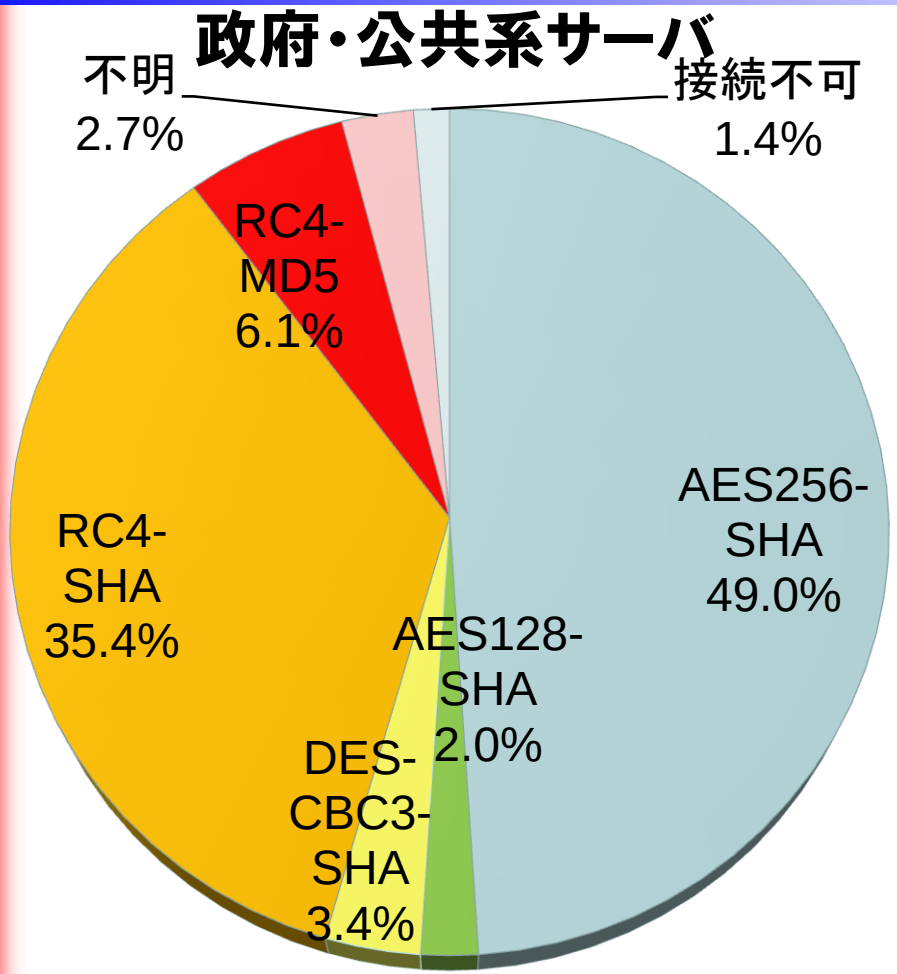


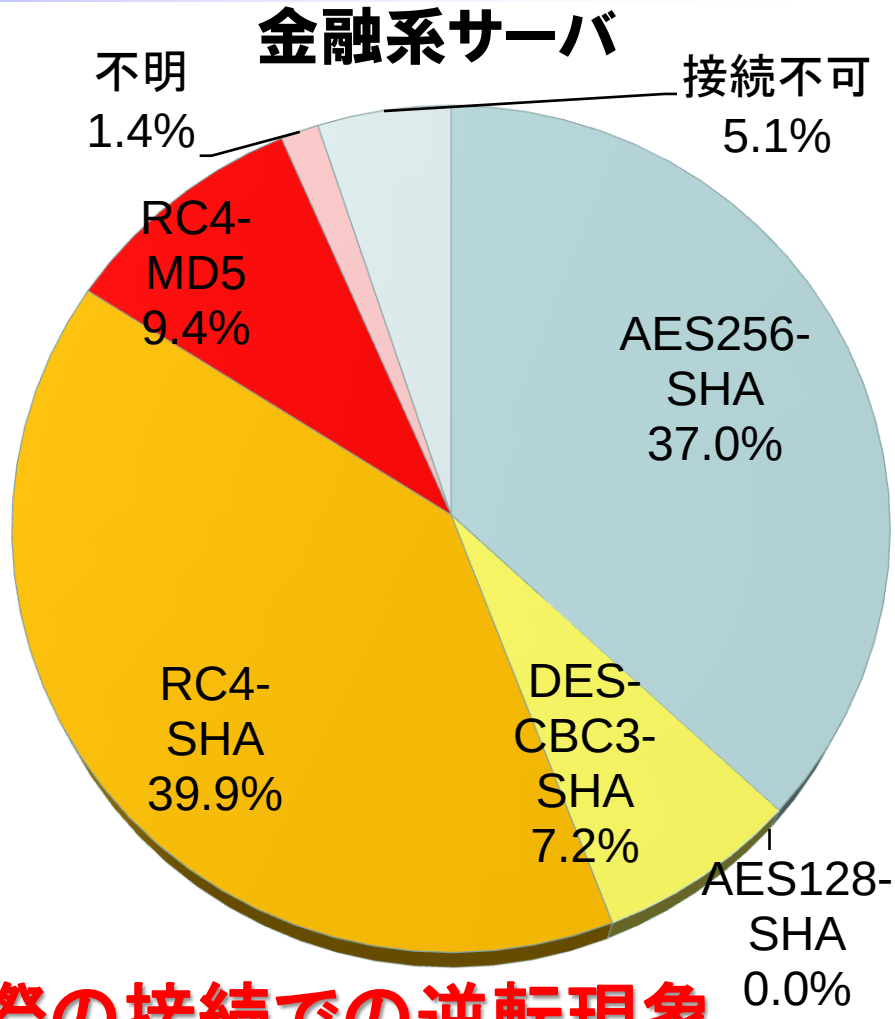
Internet Explorer 6 (XP SP2)での接続



ちなみに、IE7でもXP SP2なら同様の結果

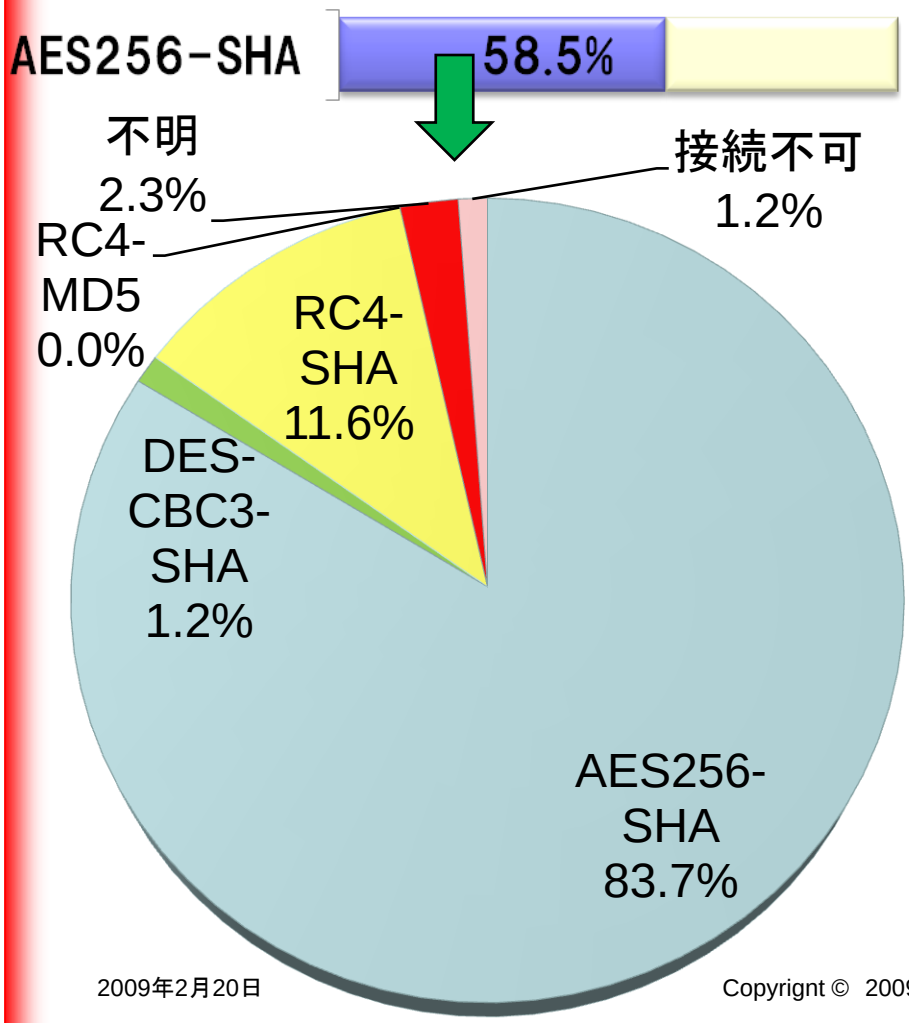
Firefox 3 (XP SP2)での接続アルゴリズム

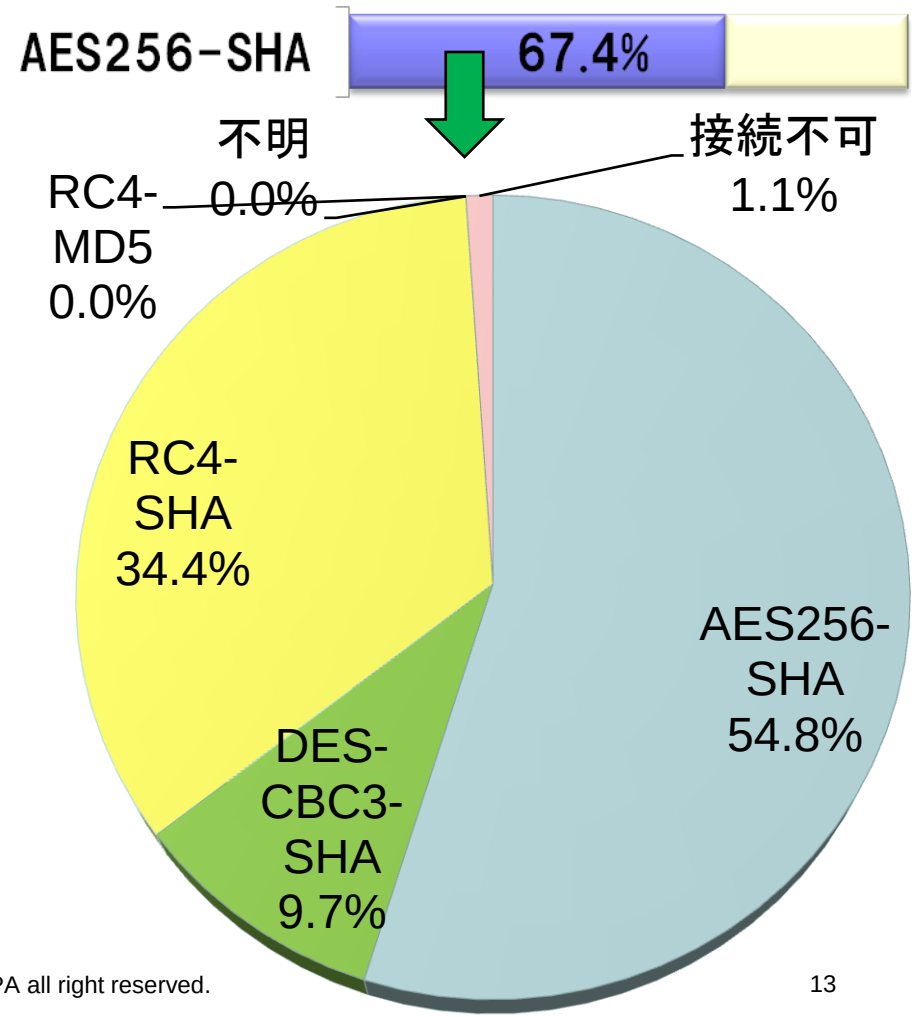




AESの暗号設定状況と実際の接続での逆転現象

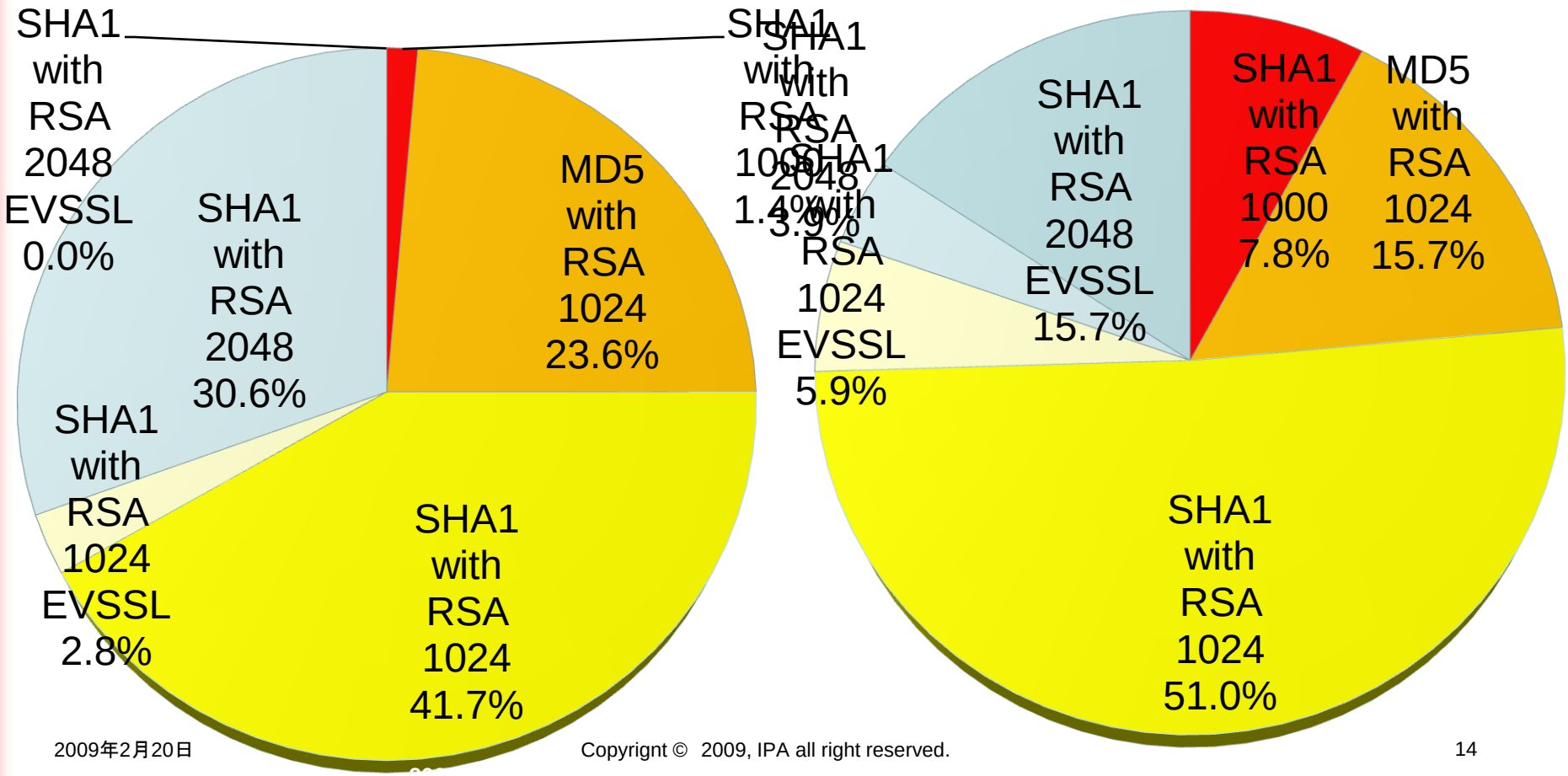
AESが利用される設定になっているか





SSLサーバ証明書と暗号のバランス

AES256-SHAで接続しているサーバに限定



IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

1.暗号の現状
～ NISTの見解と2010年問題 ～

世代交代が始まる
～ 2010年問題？ ～

- 現代暗号の利用
  - 1990年代以降
  - 公開鍵暗号、公開鍵暗号基盤の構築
  - 電子商取引，オークション，電子政府etc
- 暗号アルゴリズム
  - 解読技術の進歩
  - 計算機性能の向上
    - ムーアの法則（3年で2倍）

⇒ 世代交代が必要

“2010年問題”←理想的には、一定期間で新しい“暗号系”へ移行してゆくことが必要

⇒ ＝「予防保全」

暗号アルゴリズムの2010年問題

- 暗号アルゴリズムの2010年問題
  - 現在主流となっている暗号アルゴリズム（トリプルDES，鍵長1,024ビットのRSA，SHA-1）をどのようにしてより安全なものに移行していくか．
- 本問題の背景
  - 米国立標準技術研究所（NIST）は，これらの暗号アルゴリズムの利用によって情報システムの十分な安全性を中・長期的に確保することが困難と判断し，米国連邦政府内の情報システムにおいて2011年以降当該暗号アルゴリズムを使用しない方針を発表．

暗号アルゴリズムの等価安全性

- 暗号アルゴリズムの等価安全性（equivalent security）
  - 異なる種類の暗号の安全性を比較するための評価方法*.

- 暗号アルゴリズムへの攻撃に必要な計算量が2^nであるとき，当該アルゴリズムの強度を「nビット安全性（n-bits of security）」という.
  - 共通鍵暗号：秘密鍵を探索する計算量
  - ハッシュ関数：衝突ペアを探索する計算量
  - 公開鍵暗号：安全性が依拠する問題（素因数分解問題等）を解く計算量

* NIST，“SP 800-57: Recommendation on Key Management”において提唱されている.

暗号アルゴリズムの安全性と使用推奨期間

暗号アルゴリズムの安全性	使用推奨期間
80ビット安全性	～2010年
96ビット安全性	～2020年
112ビット安全性	～2030年
128ビット安全性	～2030年超

- 「使用推奨期間」は，少なくとも暗号アルゴリズムの安全性が確保されると見込まれる期間を示す．

ブロック暗号の推奨期間

暗号アルゴリズム*		鍵長	安全性	使用推奨期間
TDES	2-key TDES	128ビット	80ビット 〜 112ビット**	～2010年 〜 ～2030年
	3-key TDES	192ビット	112ビット	～2030年
MISTY, CAST-128, AES, Camellia, SEED		128ビット	128ビット	～2030年超
AES, Camellia		192ビット	192ビット	
AES, Camellia		256ビット	256ビット	

- 鍵の全数探索より効率のよい攻撃手法が知られていない場合，鍵長をnビットとするブロック暗号はnビット安全性をもつ．

* 「ISO/IEC 18033-3：ブロック暗号」で規定される暗号アルゴリズム
** NISTは2-key TDESの安全性を80ビットと評価．

2-key TDESの使用推奨期間

- 2-key TDESの安全性は$2^{\min(112,\ 120-t)}$と評価されている.
  - 全数探索攻撃の計算量：2^{112*}
  - Oorschot=Wienerの攻撃（既知平文攻撃）の計算量： 2^{120-t}
    - 2^tは攻撃者が入手した平文・暗号文ペアの数

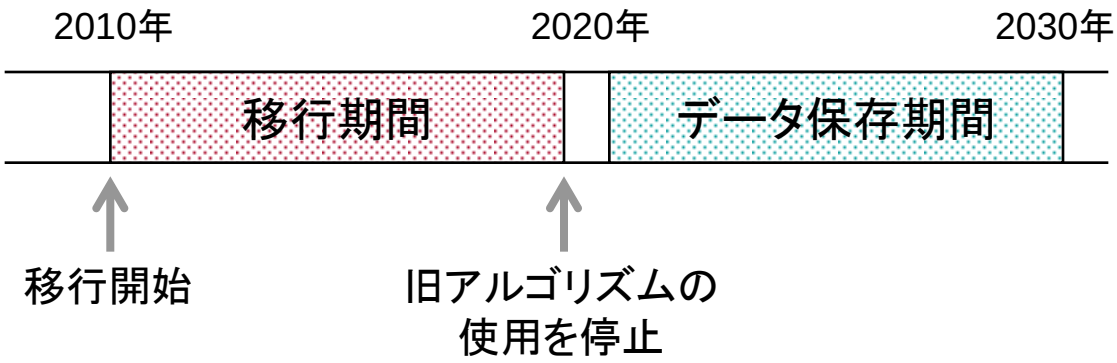
攻撃者が入手できる平文・暗号文のペア数	安全性	使用推奨期間
多い：2^{40}（約1兆）程度	80ビット	～2010年
中：2^{24}（約1600万）程度	96ビット	～2020年
わずか：2^8（256）程度	112ビット	～2030年

- Oorschot=Wienerの攻撃者が利用する平文・暗号文は同一の鍵のもとで生成されたペアであることから，鍵の使用方法が適切（頻繁に鍵を更新）であれば2-key TDESの利用可能期間を伸ばすことができると判断.

* 鍵128ビットのうち16ビットはパリティ・ビットであるため，実質的な鍵長は112ビットとなる.

暗号アルゴリズムの移行における留意点

- データの保護が必要な期間を考慮することが重要.
  - 例えば，10年間の保管を必要とするデータの暗号化に3-key TDESを利用するケースでは，新しいデータの暗号化は2020年に中止すべき（3-key TDESの使用推奨期間は2030年まで）と記述.



ハッシュ関数Hに求められる性質

① 原像計算困難性：与えられたハッシュ値yに対して，y=H(x)を満たす入力値xを求めることが困難であること.

② 第2原像計算困難性：与えられた入力値xに対して，H(x)=H(x')を満たす別の入力値x'を求めることが困難であること.

③ 衝突計算困難性：H(x)=H(x')となる入力値の組(x, x')を求めることが困難であること. この(x, x')は衝突ペアと呼ばれる.

- 安全なハッシュ関数（ハッシュ値：nビット）
  - 原像を求めるのに必要な計算量：2^n
  - 第2原像を求めるのに必要な計算量：2^n
  - 衝突ペアを求めるのに必要な計算量：$2^{n/2}$

ハッシュ関数の安全性評価

アルゴリズム*	ハッシュ値のサイズ	nビット安全性**	使用推奨期間	
			衝突計算困難性が求められる場合	第2原像計算困難性が求められる場合
RIPEMD-128	128ビット	<60ビット	推奨しない	～2020年
RIPEMD-160	160ビット	80ビット	～2020年	～2030年
SHA-1	160ビット	63ビット	～2010年	～2030年
SHA-224	224ビット	112ビット	～2030年	～2030年超
SHA-256	256ビット	128ビット		
SHA-384	384ビット	192ビット	～2030年超	
SHA-512	512ビット	256ビット		
WHIRLPOOL	512ビット	256ビット	～2030年超	～2030年超

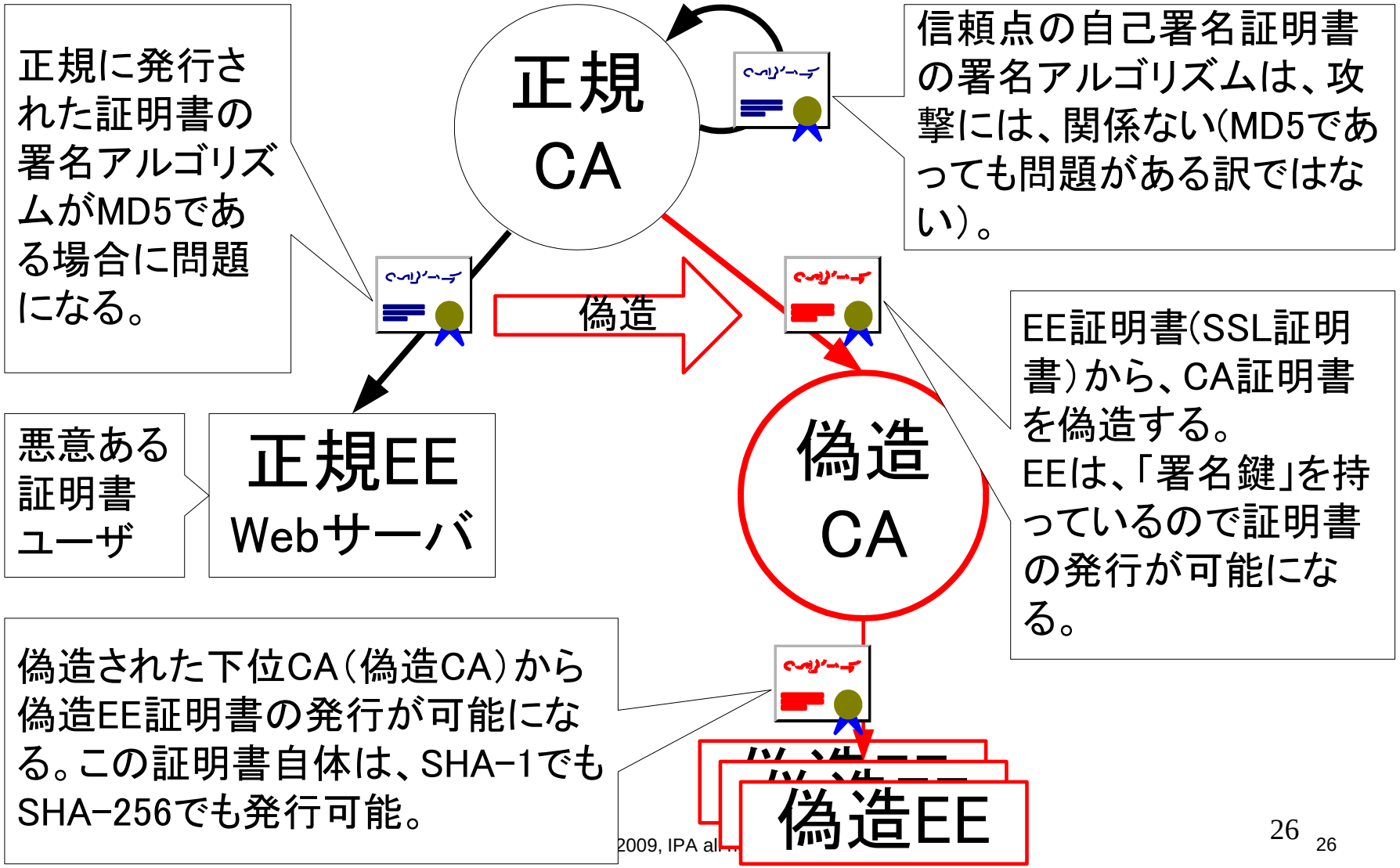
* 「ISO/IEC 10118-3：専用ハッシュ関数」で規定される暗号アルゴリズム
** 衝突ペアの探索に必要な計算量

MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造 JVNの公開日：2009/01/07

- 概要
  - MD5 アルゴリズムの衝突耐性の不備を利用した攻撃法により、X.509 証明書の偽造に成功した
- 詳細情報
  - 一方向性ハッシュ関数である MD5 は入力値から固定長のメッセージダイジェストと呼ばれる値を出力します。安全なハッシュ関数は特定のメッセージダイジェストに対応する入力値を見つけることが極めて困難である必要があります。異なる入力から同一のメッセージダイジェストが出力される事を〝衝突〟と呼びます。
  - 1996 年から MD5 アルゴリズムの衝突耐性の不備を利用した攻撃法が報告されています。その後、この攻撃手法が X.509証明書の偽造に使えることが示され、2008年に CA によって署名された証明書をもとに中間 CA 証明書の偽造に成功したことが報告されました。
- 対策方法
  - 以下の対策方法が考えられます。
  - MD5 アルゴリズムを使用しない
  - MD5 で署名されている証明書については偽造されている可能性があることに注意する

25

攻撃の概要

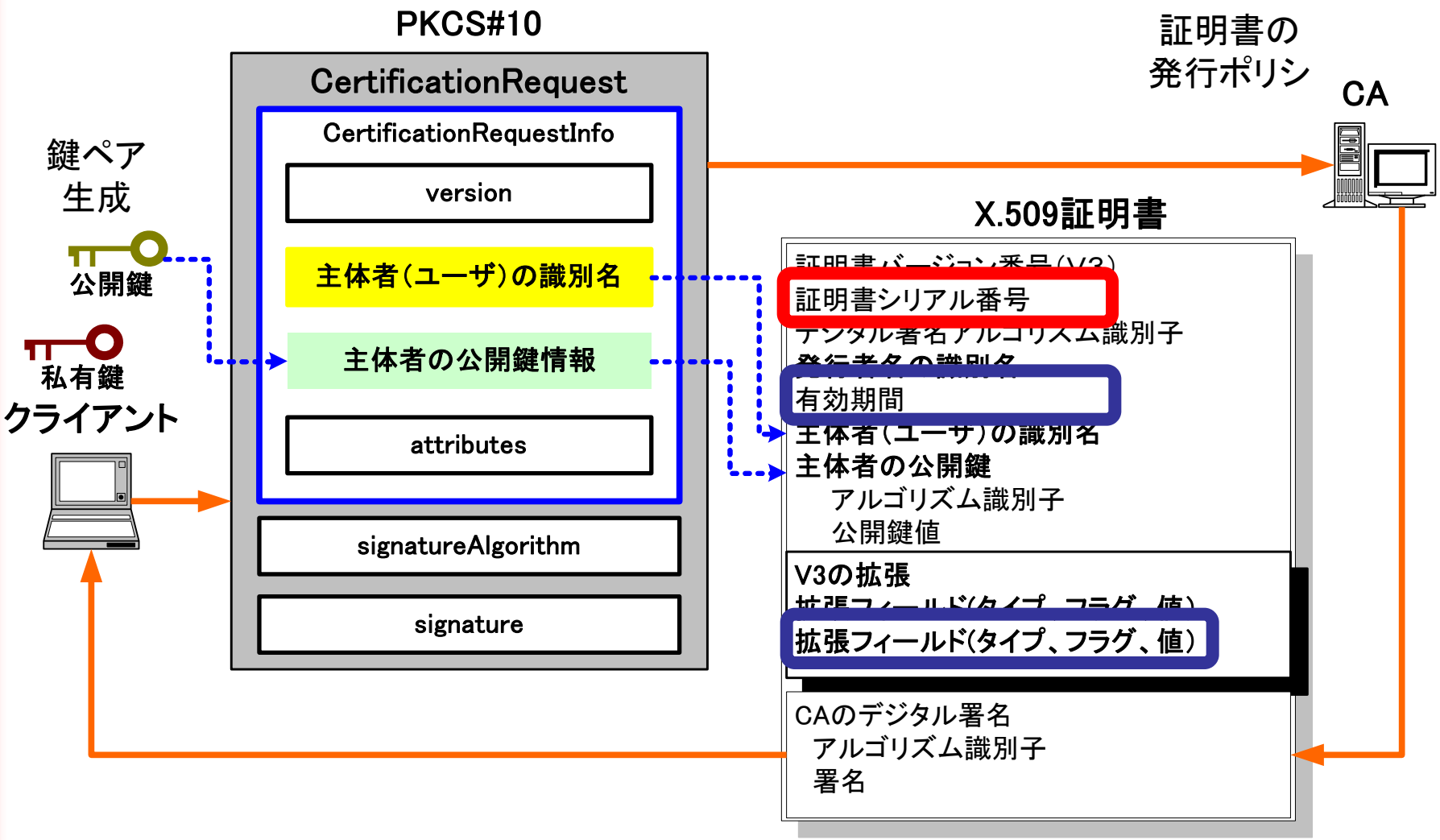


MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造 「偽造の条件」と「対策」について

- 「偽造の条件」は、証明書の内容が予測できること
  - 既存の「証明書」の偽造が可能になった訳ではない（2009年1月時点では）
  - 今回の実証では、証明書に記載される「シリアル番号」が予測できたことにより偽造が可能になった（ 「有効期限」も含めて ）
- JVNの対策方法
  - 「MD5アルゴリズムを使用しない」
    - 今後は、過去に「MD5 アルゴリズム」で署名された証明書の問題が浮上するかもしれない。
  - 「MD5で署名されている証明書については偽造されている可能性があることに注意する」
    - 中間CA証明書が(MD5で）偽造され、EE証明書はSHA-1の証明書というパターンもある（というか、そうなる）。
    - また、信頼点となる自己署名証明書（ルート証明書）のMD5に問題がある訳ではない(むしろRSA 1024bitであることの方が問題）。

27

MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造 証明書発行要求と証明書発行について

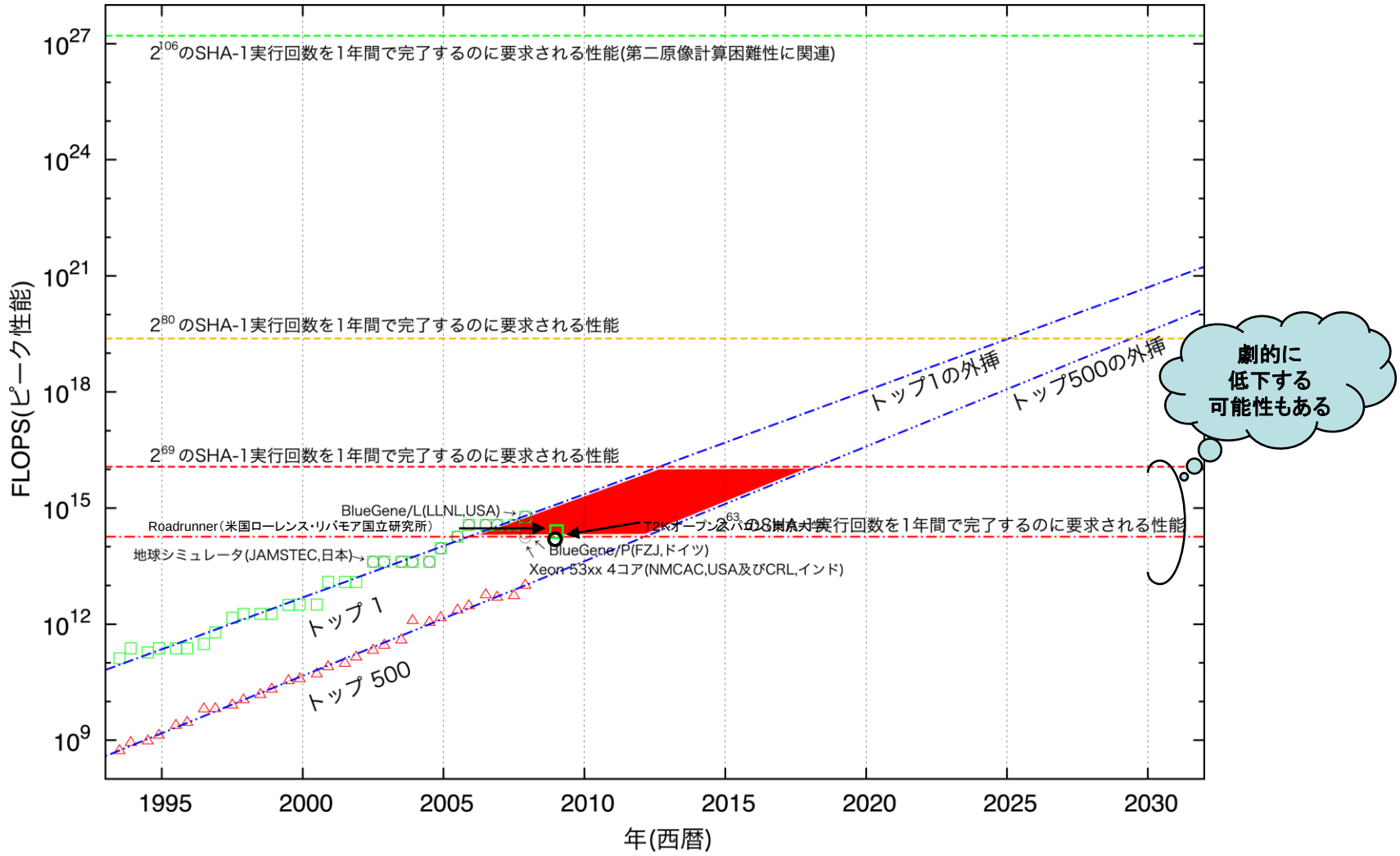


MD5 アルゴリズムへの攻撃を用いた X.509 証明書の偽造 今後、予想されること？？と今後の対応の示唆

- 過去に発行した「EE証明書」から「下位CA証明書（=中間CA証明書）を偽造すると（出来るとすると）、かなりのインパクトがある。
  - MD5のSecond-Pre-Image攻撃成立による脅威
- 可能になると、信頼点の証明書（ルートCAの証明書）まで、階層全体の信頼性が損なわれる。
- これは、末端のEE証明書に利用されているMDが停止されるだけでは解決せず、過去にMD5の証明書を発行した「階層全体」の移行が必要な可能性もあることを意味する（中間CAの切り離しも容易ではない）。
- これには非常に時間がかかる（故に早く取り掛かる必要がある）
  - 現時点で6つの有効な認証局が、過去にMD5のEE証明書を発行している。

29

SHA-1の安全性
- 衝突発見に必要な計算量 -



SHA-1に対する見解

- 衝突計算困難性が求められるアプリーションにおいては，SHA-1から別のハッシュ関数への移行について早急に検討すべき．仮に2010年までに移行が完了しなかった場合には，別の機構を組み込むことによって危殆化の影響を軽減する措置が求められる．
  - 移行にかかる時間の考慮も必要．2012年に発表予定のSHA-3*に移行する場合，移行に6年かかるとすれば2019年までSHA-1を使い続けることになる．
- 第2原像計算困難性に安全性を依拠するアプリケーションであれば，SHA-1を2010年以降も引続き利用することが可能．

* SHA-3は，NISTがSHA-224, 256, 384, 512に替わるハッシュ関数として開発を行っているものであり，公募・選考により2012年に政府調達標準となる見通し．

ハッシュ関数への攻撃のまとめ

ハッシュ	攻撃の推定計算量		攻撃状況	現実的な攻撃の脅威
MD5	衝突攻撃	2^{32}	2004年に最初の衝突が発見された。現在では、PC1台で数十秒から数分	（衝突が発見されているが）現実的な脅威はないと思われる。
	ターゲット型衝突攻撃	2^{50}	2007年のchosen-prefix collisions PlayStation 3の200台のクラスターで1,2日	一般論としては、署名者側の攻撃が可能となる。 2008年末、ある条件下で、偽造CAが可能なことが実証された。
	第2原像探索攻撃	2^{74}	攻撃は成立してない。 そろそろ可能かもしれない	これは、要注意。過去の証明書から偽造CAが出来る可能性。
SHA-1	衝突攻撃	2^{63}	攻撃は成立してない。 国内最高速のスパコンで約7年以下（2006年）	（衝突が発見されても）現実的な脅威はないと思われる
	ターゲット型衝突攻撃	2^{80}	攻撃は成立してない。	一般論としては、署名者側の攻撃が可能なる。
	第2原像探索攻撃	2^{108}	攻撃は成立してない。	当面、考える必要はない？

公開鍵暗号
～ 安全性の根拠 ～

- 公開鍵暗号の安全性の根拠
  - 素因数分解問題（FP：factoring problem）
    - RSA暗号等
    - nからn=p･qとなる素数p, qを求める問題
  - 離散対数問題（DLP：discrete logarithm problem）
    - DSA等
    - 有限群Gについて，g, y∈Gからy=g^xとなるxを求める問題
  - 楕円離散対数問題（ECDLP：elliptic curve DLP）
    - ECDSA等
    - 有限体F上の楕円曲線Eについて，E上の点G,YからY=xGとなるxを求める問題
- 各問題を解くアルゴリズム
  - アルゴリズムの計算量は入力データ（公開鍵）のサイズに依存．
    - FPとDLP：（ECDLPに比べて）相対的に効率のよいアルゴリズムが知られている．
    - ECDLP：効率のよいアルゴリズムが知られていない．

公開鍵暗号の使用推奨期間

FPベース[RSA]（n=p･q）	DLPベース[DSA]（$y=g^x$）	ECDLPベース[ECDSA]（Y=xG）	使用推奨期間
nのビット数	yのビット数L，xのビット数N	Yのビット数	
1,024	L=1,024 N=160	160～191	～2010年
1,536	L=1,536 N=192	192～223	～2020年
2,048	L=2,048 N=224	224～255	～2030年
3,072	L=3,072 N=256	256	～2030年超

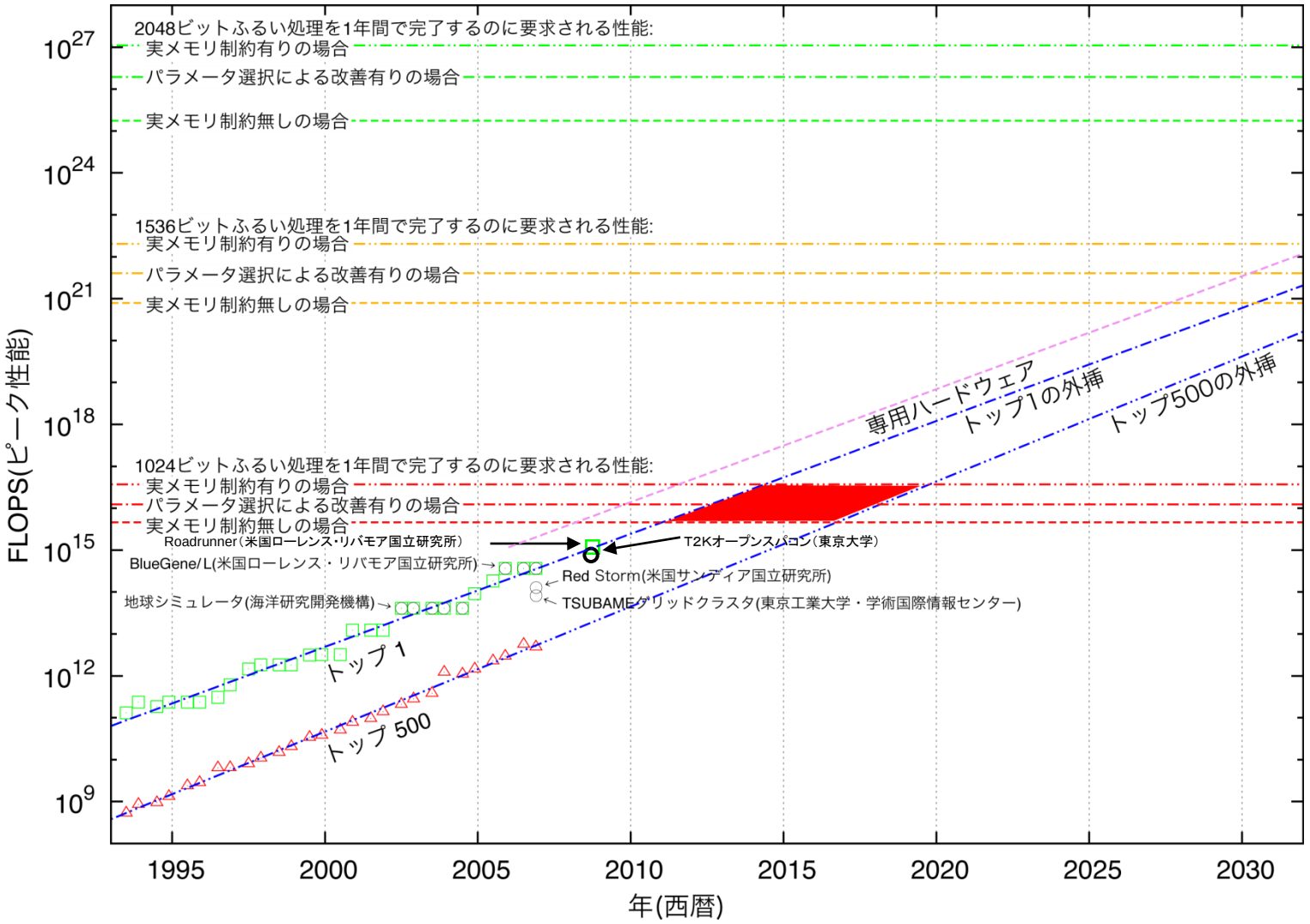
* ただし，ECRYPTでは，80ビット安全性をもつRSAの鍵長 （合成数nのサイズ）を1,248ビットとしている.

公開鍵暗号の安全性評価研究の動向

- 近年，専用HWを利用した安全性評価が盛んになっている.

	FPベース［RSA］（n=p･q）	ECDLPベース［ECDSA］（Y=xG）
	nのビット数	Yのビット数
汎用コンピュータによる実績	663	109
専用HWによる実績	423	――
専用HWによる計算の見積もり	約270年で768ビットのFPを解くことが可能. （HWデザインの提案：3,000万ドルかければ1年でFPを解くことが可能）	100万ドルかければ1年で$2.58*10^7$年で160ビットのECDLPを解くことが可能.

RSA暗号の安全性


2048ビットふるい処理を1年間で完了するのに要求される性能:
実メモリ制約有りの場合
パラメータ選択による改善有りの場合
実メモリ制約無しの場合
1536ビットふるい処理を1年間で完了するのに要求される性能:
実メモリ制約有りの場合
パラメータ選択による改善有りの場合
実メモリ制約無しの場合
1024ビットふるい処理を1年間で完了するのに要求される性能:
実メモリ制約有りの場合
パラメータ選択による改善有りの場合
実メモリ制約無しの場合
専用ハードウェア
トップ1の外挿
トップ500の外挿
Roadrunner(米国ローレンス・リバモア国立研究所)
T2Kオープンスパコン(東京大学)
BlueGene/L(米国ローレンス・リバモア国立研究所)
Red Storm(米国サンディア国立研究所)
地球シミュレータ(海洋研究開発機構)
TSUBAMEグリッドクラスタ(東京工業大学・学術国際情報センター)
トップ 1
トップ 500
FLOPS(ピーク性能)
10^{27}
10^{24}
10^{21}
10^{18}
10^{15}
10^{12}
10^{9}
1995
2000
2005
2010
2015
2020
2025
2030
年(西暦)

まとめ：推奨暗号アルゴリズムとその使用推奨期間

nビット安全性	ブロック暗号	ハッシュ関数	公開鍵暗号とその公開鍵長			使用推奨期間
			FPベース［RSA］	DLPベース［DSA］	ECDLPベース［ECDSA］	
80ビット	2-key TDES（攻撃者が2^{40}程度のペアを入手可能）	SHA-1*	1,024	L=1,024 N=160	160～191	～2010年
96ビット	2-key TDES（攻撃者が2^{24}程度のペアを入手可能）		1,536	L=1,536 N=192	192～223	～2020年
112ビット	2-key TDES（攻撃者が2^{8}程度のペアを入手可能） 3-key TDES	SHA-224	2,048	L=2,048 N=224	224～255	～2030年
128ビット	AES-128	SHA-256	3,072	L=3,072 N=256	256	～2030年超

* 現時点のSHA-1の安全性評価は63ビットであるが，使用推奨期間は2010年末までとされている．

国際標準での動き
～ ISO/IEC JTC1/SC27/WG2の対応 ～

- 06年9月（TC68/SC2総会）：JTC1/SC27に対して，ISO/IEC 18033-3（ブロック暗号）の脚注に記載されている「NISTは2009年までしか2-key TDESを推奨していない」との記述について，同じISO標準の中で矛盾が生じているとの見解から，「脚注を削除する，あるいは，2-key TDESに関するより詳細な文書を付加する」のいずれかの対応について検討を依頼.

- 07年5月（SC27総会）：脚注を削除するとともに，暗号アルゴリズムの安全性に関する事例をスタンディング・ドキュメントとして記述することを決議.
- 08年4月（SC27/WG2会合）：“ISO/IEC JTC1/SC27 Standing Document No.12 (SD12) on the Assessment of Cryptographic Algorithms and Key-Lengths”のドラフトについて審議し，修正版をSC27のサイトで公開することを決議.

SD12 1stドラフト（07年11月）の概要

- 2-key TDESは，2^tの平文・暗号文ペアを入手した攻撃者であれば，2^{120-t}の計算量で鍵を求めることができる．
- そもそもブロック長をnビットとするブロック暗号については，$2^{n/2}$個の平文・暗号文ペアを集めれば高い確率で解読が可能（暗号文一致攻撃*）であり，2-key TDESでは同じ鍵を2^{32}回以上利用すべきではない．
- 2-key TDESの安全性が「2^{40}個の平文・暗号文のペアを入手することの難しさ」のみで評価されるわけではないが，同じ鍵で大量のデータを暗号化しないようにするといったシステム設計が望ましい．

* 暗号文一致攻撃は，暗号文から平文を推測する攻撃であり，鍵の推測を目的とした攻撃ではない．

暗号の安全性低下の影響とは
～ ハッシュ関数を利用したアプリケーションの安全性評価研究 ～

- 衝突ペアの発見によって，MD5を利用したアプリケーションの安全性が低下．

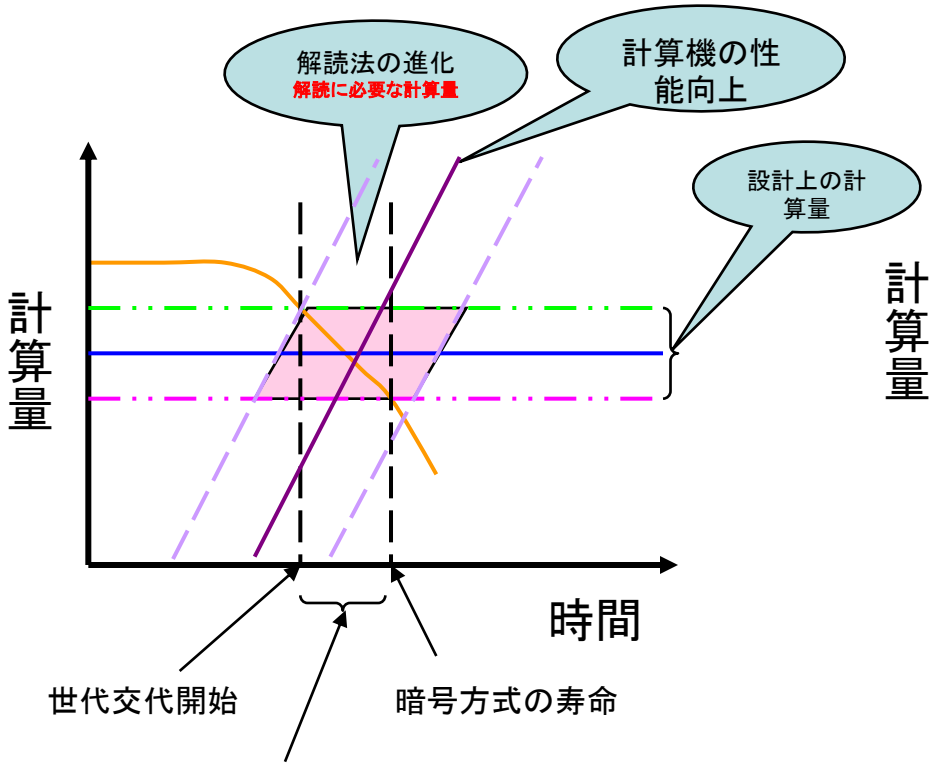
MD5を利用したアプリケーション	安全性評価の結果
APOP	• 2^{23}の計算量で13文字までのパスワードを解読．さらに，理論的には61文字までのパスワードを解読可能[08]．
X.509で規定される公開鍵証明書	• 2^{52}の計算量で異なる公開鍵と名前に対する公開鍵証明書の偽造が可能[07]．

暗号の世代交代

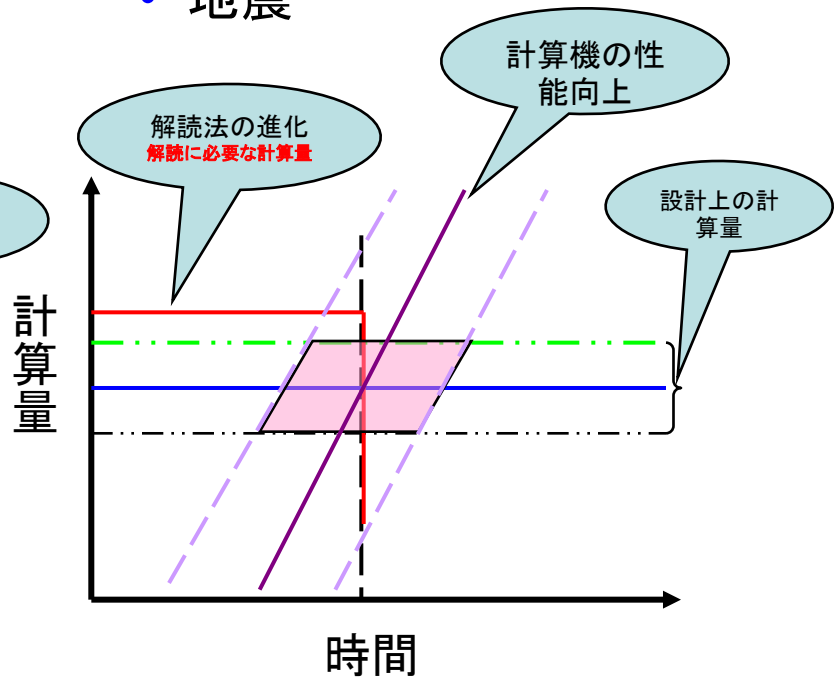
- 共通鍵暗号
  - 過去にも経験（軍用暗号）
  - DES暗号→AES暗号
    - 1995年から世代交代が始まる
      - DES→Triple-DES
    - 2001年から
      - Triple-DES→AES
- 公開鍵暗号と公開鍵暗号基盤（Public Key Infrastructure）
  - 初めての経験
  - RSA暗号とハッシュ関数SHA-1
    - RSA暗号は、鍵長（Modulo）の更新
      - 1024bit→2048bit
    - ハッシュ関数
      - メッセージダイジェスト長
        - » 160bit→256bit以上
        - » アルゴリズムの更新も必要
  - PKIの信頼性の維持
    - ディジタル証明書の偽造防止

世代交代と危殆化

- 世代交代
  - (ある程度)予測可能
    - 火山噴火



- 危殆化
  - 予測不可能
    - 地震



IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2. 我が国の動向（移行方針）

「移行指針」に至る経緯

2004年8月

- 山東大学　王小云教授
- SHA-1に対する攻撃法を発表

- 2005年度
  - CRYPTREC監視委員会
    - 電子署名WGを組織
  - 影響を評価→移行の必要性を指摘
    - 「SHA-1 の安全性に関する見解」
  - NISCと協議開始

移行指針

- 2007年9月
  - 「SHA-1等の安全性低下等への対応に関する各府省庁連絡会」
  - 実態調査
  - 移行指針の検討
- 2008年4月
  - 「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」を公表
- 我が国電子政府システムでの問題点
  - システムの更新/調達時期との整合性が必要
    - 予算確保（財務当局への説明）の困難性
    - セキュリティの確保は主たる予算要求理由にはならない
  - 米国
    - 2010年を目処に移行を計画
    - セキュリティの重要性を政府全体で認識

暗号屋の立場からは
定期的・計画的に移行することが**理想**

移行指針の概要

- 情報システムの設計要件
  - 政府認証基盤(GPKI)、商業登記認証局
    - RSA1024→RSA2048
    - SHA-1→SHA-1/SHA-256
  - GPKIに依存する情報システム
    - SHA-1→SHA-1/SHA-256
    - RSA1024→RSA1024/RSA2048
  - 当面の間、SHA-1/RSA1024も併用可能
    - 関連システムが移行完了時点
    - SHA-1/RSA1024の使用中止
    - 想定外の事象への対処案も必要

定期的な更新なら不要（？）

民間（特定認証業務）等

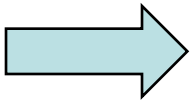
- 電子署名法の改正（政省令の見直し）
  - 電子政府システムに準拠
- その他民間のシステムへの波及を期待
  - 強制力はない
  - Verisign、Entrustなどは、米国の移行方針に準拠
    - 主要民間認証局では、MD5での認証書の新規発行を停止。

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

3. CRYPTRECの今後

CRYPTRECの今後

- 電子政府推奨暗号リストの改訂
  - 現在のリスト→2003年3月公開
    - 陳腐化
      - 3-Key Triple DES：今後何年間利用可能？
      - ハッシュ関数SHA-1は、いつまで安全か？
        - 「衝突の発見」は「認証書/文書の偽造」とは等価でない。
      - RSA暗号→鍵長1024bitは、時間の問題
        - 素因数分解できれば、RSA暗号ベースのPKIは崩壊
        - 鍵長2048bitであれば、当面OK
    - 2003年以降に開発された技術への対応も模索

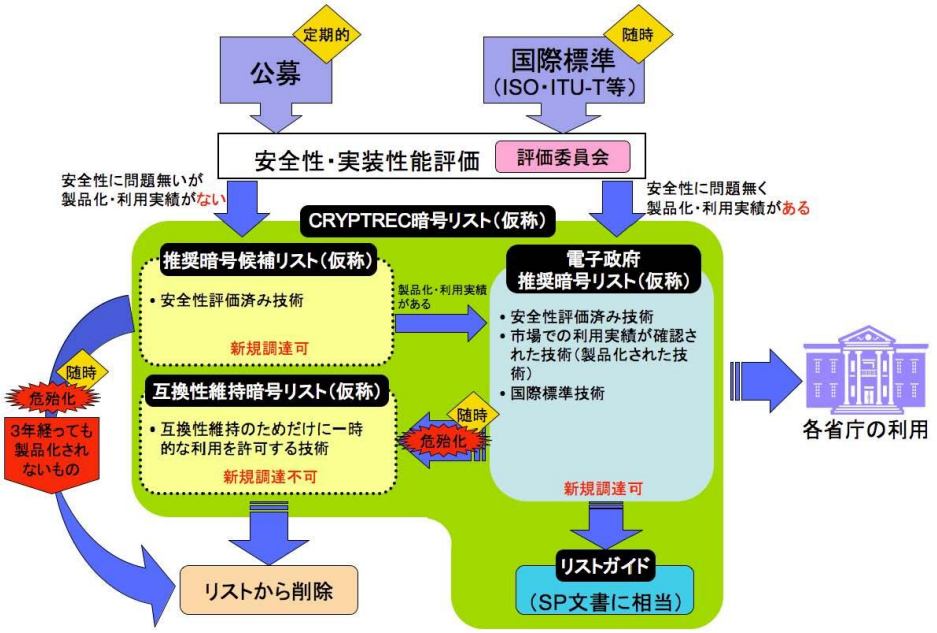


新しい提案を公募。
2013年には、新しい“リスト”へ移行したい。

次期電子政府推奨暗号リスト

公開鍵暗号	署名	DSA	共通鍵暗号	64ビットブロック暗号（注3）	CIPHERUNICORN-E
		ECDSA			Hierocrypt-L1
		RSASSA-PKCS-v1_5			MISTY1
		RSA-PSS			3-key Triple DES (注4)
	守秘	RSA-OAEP		128ビットブロック暗号	AES
		RSAES-PKCS-v1_5（注1）			Camellia
	鍵共有	DH			CIPHERUNICORN-A
		ECDH			Hierocrypt-3
		PSEC-KME（注2）			SC2000
その他	ハッシュ関数	RIPEMD-160（注6）		ストリーム暗号	MULTI-S01
		SHA-1（注6）			MUGI
		SHA-256/-384/-512			128-bit RC4 (注5)

シングルリスト



- 世代交代も意識したライフサイクルの管理
- 新「電子政府推奨暗号リスト」の絞り込み
- 実効性のあるリストへ