セコムIS研究所
Intelligent Systems Laboratory

# 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～

2008年11月27日

**セコム㈱IS研究所　松本　泰**

# 「暗号アルゴリズムの移行問題」に関連した松本の自己紹介

セコム IS 研究所 Intelligent Systems Laboratory

- セコム(株) IS研究所
- 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
- 次世代電子商取引推進協議会 (ECOM) 電子署名普及WG　副主査
- IPA情報セキュリティ分析ラボラトリー非常勤研究員
- 暗号技術検討会の構成員

セコムIS研究所
Intelligent Systems Laboratory

# 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～
# 概要

1. **鍵の危殆化**
2. **暗号アルゴリズムの脆弱化**
3. **ＮＩＳＣの移行指針**
4. **暗号アルゴリズムの移行問題**

# 暗号アルゴリズムの理解？

セコムIS研究所
Intelligent Systems Laboratory

- 古典暗号
  - 暗号アルゴリズム自体を秘匿
- 現代暗号
  - 暗号アルゴリズムは公開され、暗号化・復号に鍵を用いる
    - 守るべき対象は、暗号に利用する「鍵」
  - 「現代暗号」は、暗号アルゴリズムの客観的評価が必要
- 日本における暗号アルゴリズムの客観的評価の歴史
  - 2000年5月
    - CRYPTREC・暗号技術評価委員会の設置
  - 2003年3月
    - 電子政府推奨暗号リストの公表

# 鍵の危殆化の理解 - プエブロ号事件の例

セコム IS 研究所
Intelligent Systems Laboratory

- 1968 年に、USSプエブロ号（米海軍情報収集船）が北朝鮮に拿捕されました。 当 時、海軍の船舶はすべて、各種の暗号機のための対称鍵をさまざまなセキュリティレベルで扱っていました。
- それぞれの鍵は毎日変更されました。 これらの鍵がどのくらいプエブロ号の乗組員によって破られず、北朝鮮の手に落ちたのかを知る方法がなかったので、海軍はプエブロ号が所持していたすべての鍵が信用できなくなったと仮定しなければなりませんでした。
- 太平洋戦域のあらゆる船舶と沿岸基地（つまり、航海中の船舶を含む数千の施設）は、各施設にコードブックとパンチカードを物理的に運んで、すべての鍵を取り替えなければなりませんでした。

*出典：* セキュリティの概要　April 29, 2004

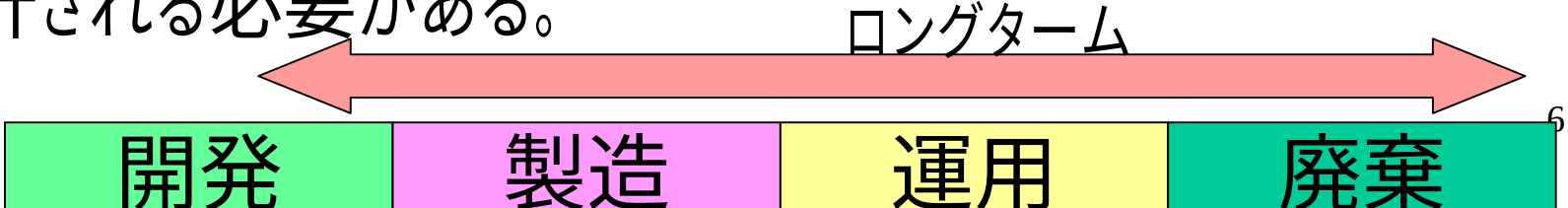
http://developer.apple.com/documentation/Security/Conceptual/Security_Overview/Concepts/chapter_3_section_4.html

# 暗号に関するセキュリティの3つの観点

セコムIS研究所 Intelligent Systems Laboratory

| 3つ観点 | ベースとなる技術等 | 状況 |
|---|---|---|
| 暗号アルゴリズム | 数学等 | 安全な暗号アルゴリズム<br>RSA暗号、ＡＥＳ暗号、etc.. |
| 暗号モジュールの実装 | ハードウェア<br>ソフトウェア | 暗号技術の実装上の評価。<br>「耐タンパー性」ハードウェア、ソフトウェアで「鍵」などの機密情報を守る仕組み |
| 暗号の鍵の運用 | 運用技術 | 現実的には、これが一番危ない？ |

- それぞれの観点にロングターム・セキュリティからの検討が必要
- 共通鍵暗号と、公開鍵暗号の特性も十分に理解した上で、設計される必要がある。



# 暗号アルゴリムの脆弱化
# SHA-1及びRSA1024の安全性評価

セコムIS研究所
Intelligent Systems Laboratory

- ハッシュアルゴリズムのSHA-1の安全性
  - **衝突発見困難性**のレベルは、現時点で**63ビット**以下。
  - スーパーコンピュータ・レベルのテクノロジとの比較では、2015 年前後には脅威となることが想定される。
  - **ターゲット型衝突発見困難性**のレベルは、まだ不確定である。
  - **第2原像計算困難性**のレベルは、現時点で**106ビット**以下。
- 公開鍵暗号のRSA　1024bitの安全性
  - 素因数分解問題の困難性のレベルは、現時点で70ビット以下。
  - スーパーコンピュータ・レベルのテクノロジとの比較では、概ね2015年以降に脅威となることが想定される。

**出展：**
**公的個人認証サービスにおける暗号方式等の移行に関する検討会 第1回会合資料**
http://www.soumu.go.jp/menu_03/shingi_kenkyu/kenkyu/kouteki_kojin/pdf/080916_1_si3.pdf

# 暗号アルゴリムの脆弱化

セコムIS研究所
Intelligent Systems Laboratory

- **暗号アルゴリズムの安全性**
  - **計算量的安全性**
- **暗号アルゴリムの脆弱化の二つの要因**
  - **計算機性能の向上**
  - **暗号アルゴリズムに対する攻撃の研究の進歩**

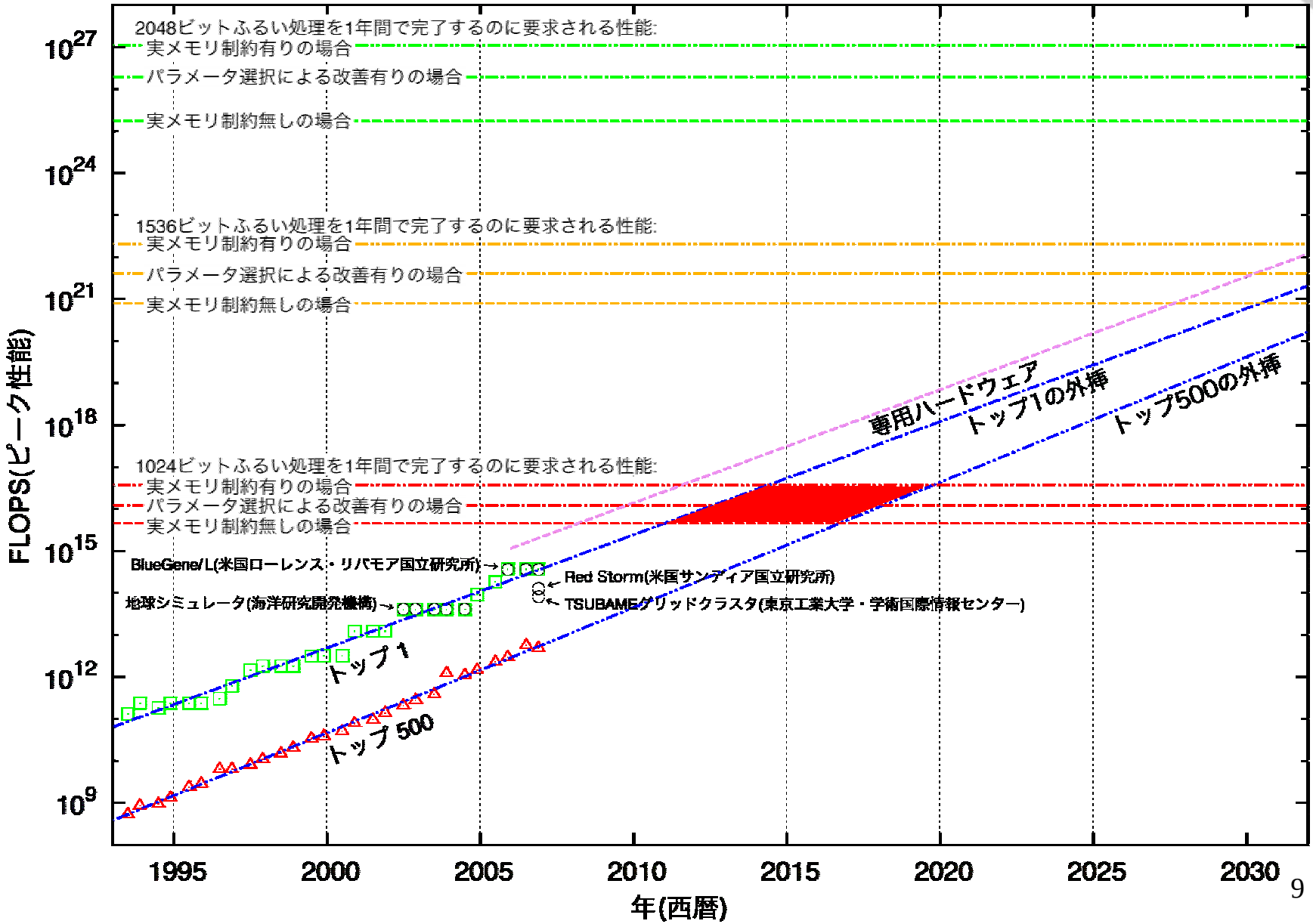
**暗号アルゴリズムの歴史**


「暗号の2010年問題」という言葉は、「暗号アルゴリムの脆弱化」に対して米国NISTが、米国政府の暗号アルゴリズムに関する調達基準を変更し、2010年までに移行すると宣言したことに由来している。

# CRYPTREC Report 2006 (17頁)

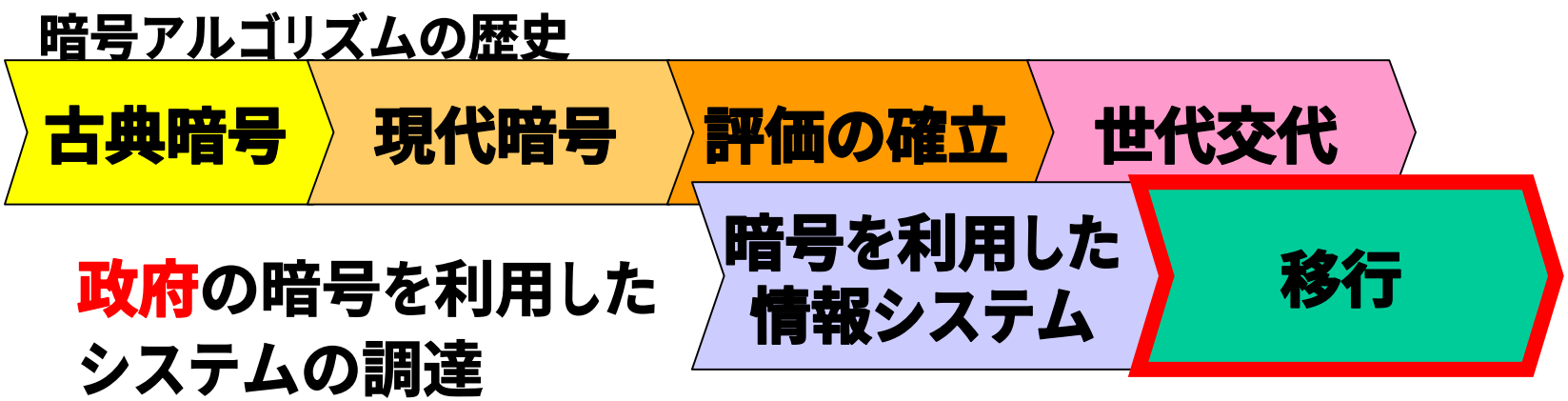
セコムIS研究所 Intelligent Systems Laboratory

## 1年間でふるい処理 (一般数体ふるい法の処理の一部) の要求される処理性能の予測



# NISC（内閣官房情報セキュリティセンター）の移行指針

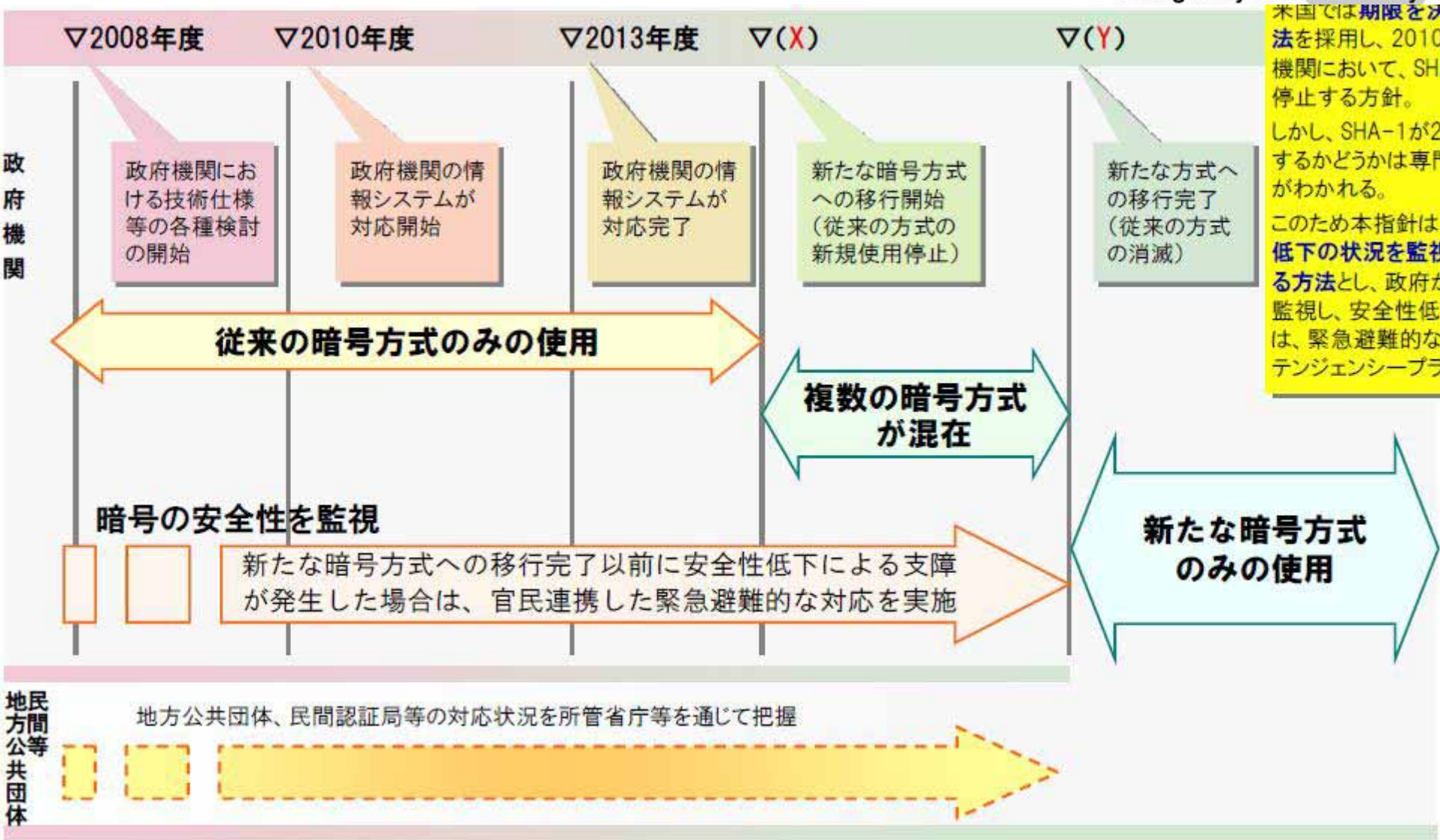
- 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」
- 2008年4月22日 情報セキュリティ政策会議決定




ここで、「暗号アルゴリズムの脆弱化」に対して「移行」が重要という認識が示された？？

# NISCの移行指針

セコムIS研究所
Intelligent Systems Laboratory




出展：公的個人認証サービスにおける暗号方式等の移行に関する検討会 第1回会合資料

# 「暗号アルゴリムの脆弱化」の対応

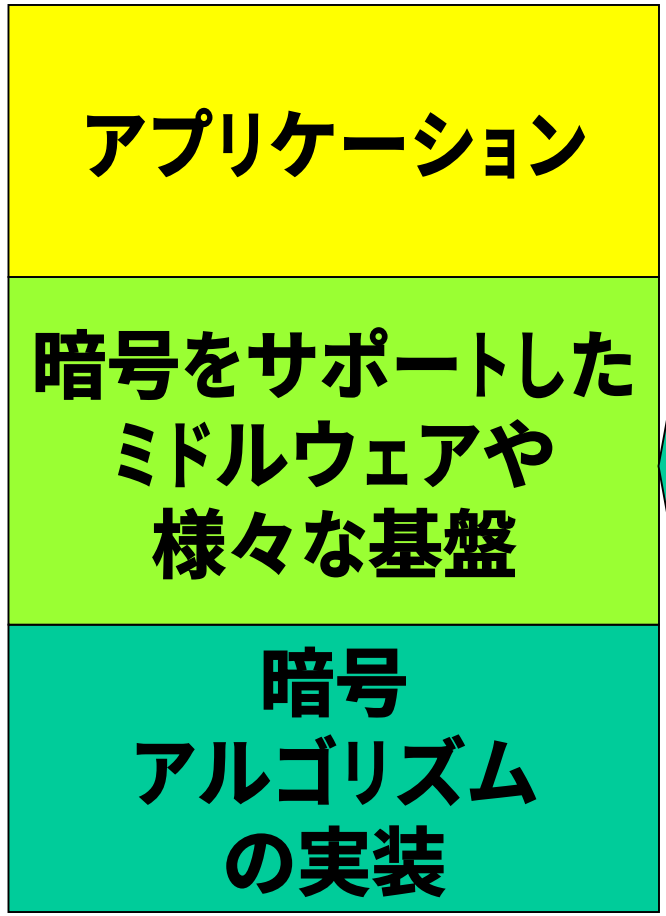
セコム IS 研究所
Intelligent Systems Laboratory

## 単純な利用

新しい
暗号アルゴリズム
に対応した
アプリケーション

新暗号
アルゴリズム
の実装

## 基盤化したITでの利用




- 非常に複雑。
- 暗号は、広く基盤化されたITに取り込まれている。
- 様々な標準化との密接な関係
- 広く展開されている実装

「暗号アルゴリムの脆弱化」の対応とは、様々な標準化の対応、また、広く展開されている実装を移行するための経済的な問題も含めた対応ということになる。

# 暗号アルゴリズムの移行の議論

セコムIS研究所
Intelligent Systems Laboratory

## 暗号アルゴリズムの歴史

古典暗号 → 現代暗号 → 評価の確立 → 世代交代

IETF, ISO, ITU
Etc…

暗号技術を利用した様々な標準化

標準化へのインパクト

電子署名法、Webサーバ
証明書の発行、etc….

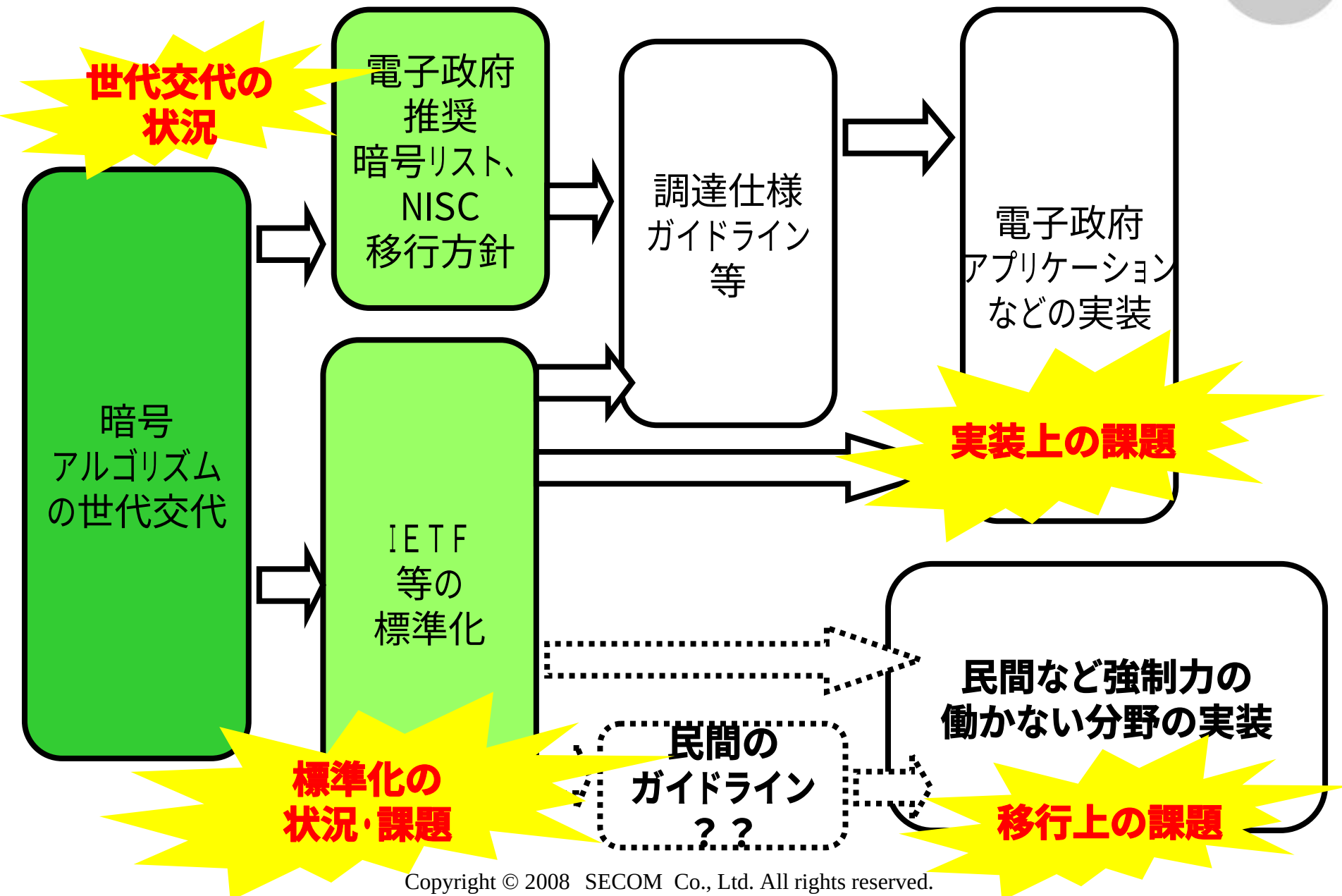
暗号技術を利用した様々な実装の展開基盤の確立

実装の展開基盤へのインパクト

**暗号は、ITソリューションの「米」じゃなくて「小麦」状態??**
**ありとあらゆるITソリューションに組み込まれている**

# 暗号アルゴリズムの移行問題

セコム IS 研究所
Intelligent Systems Laboratory



# 暗号アルゴリズムの移行問題（SHA-1）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
  - ???

「PKI**相互運用技術からみた**SHA-1**問題**　- PKI day 2006」**より。**
http://www.jnsa.org/seminar/2006/20060607/matsumoto_02.pdf

セコムIS研究所
Intelligent Systems Laboratory

# 暗号アルゴリズムの移行問題

2008年11月27日

セコム㈱IS研究所　松本　泰

# 移行の問題

- ＪＮＳＡから出した「移行指針案」へのパブリックコメント
- ＩＥＴＦにおける動向
- 暗号アルゴリズムの移行の議論

# ＪＮＳＡから出した「移行指針案」へのパブリックコメント

NICSの「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」（案）に対して、NPO JNSAのPKI相互運用技術WGが2008年３月に提出したパブリックコメントの抜粋

# ＪＮＳＡから出した「移行指針案」へのパブリックコメント
# (1) 電子証明書の SHA-1に関する脅威の根拠について

- 「(ア) 電子証明書の発行に使用する暗号アルゴリズムを複数の中から選択可能とする構成とし、使用する暗号アルゴリズムを特定の時期に切替可能とする」に関して、暗号技術検討会の報告書等では、RSA1024bitが解読可能になる時期については根拠が示されています。
- それに対してSHA-1に関しては、**現実的な脅威となる訳ではないコリジョン攻撃が可能になる推定**のみが示されています。
- 電子証明書に対する**現実的な脅威になる可能性がある Second-Pre-Image攻撃**が可能になる計算量や、可能になると想定される時期は示されていません。こうした根拠が示されるべきではないでしょうか。

# ＪＮＳＡから出した「移行指針案」へのパブリックコメント

## (2) 文書ファイルへの電子署名に関して

- 「(ア) 文書ファイルへの電子署名及びその検証に使用する暗号アルゴリズムを複数の中から選択可能とする構成とし、暗号アルゴリズムごとに電子署名及び検証を行う期間の開始及び終了時期を設定可能とする」に関して、文書ファイルへの電子署名に関して、署名者自身による攻撃は、Second-Pre-Image攻撃で想定される計算量よりも少ない計算量で成立する可能性があります。「期間の開始及び終了時期を設定可能」に関しては、RSA1024とSHA-1に関して、文書ファイルへの電子署名、電子証明書、それぞれの根拠を明確にして、その移行時期を検討するべきではないでしょうか。
- また既存の署名文書に対する方針も検討するべきではないでしょうか。

セコム IS 研究所 Intelligent Systems Laboratory

# (3) 移行時期について

- 「新たな暗号アルゴリズムへの切替時期並びにSHA-1及びRSA1024の使用停止時期について、2008年度中に検討する」とありますが、RSA1024からRSA2048への移行の考え方は概ね正しいと考えます。
- また、RSA2048について、GPKIの相互運用性仕様書では、RSA2048までの検証を要求しており、現時点でも検証は、可能なはずです。
- それに対してSHA-1からSHA-256への移行自体は正しいと考えられますが、**実際の脅威となるまでの時間の推定は、「電子文書への署名」と「証明書の署名」**では大きく異なるはずです。そのため一律にSHA-1の使用停止時期を決めるのは間違いだと考えます。
- もし、一律にSHA-1の使用停止時期を決めるのであれば、その根拠を明確にするようにお願いします。

# ＪＮＳＡから出した「移行指針案」へのパブリックコメント (4) まとめ

- 政府認証基盤（GPKI）の鍵更新は、最長5年のエンドエンティティの証明書発行することを想定した鍵管理のライフサイクルを想定していると推測されます。また、自己署名証明書は10年の有効期間で発行されています。利用するハードウェアに関しても**住民基本台帳ICカードのように10年の有効期限**を持ったものがあります。こうしたことから**移行に長い時間がかかることが想定されますが、今回の移行指針が提示は、あまりにも遅すぎるのではないでしょうか**。
- 移行指針が提示自体は、遅すぎると考えますが、移行のスケジュールに関しては、十分に検討をお願いします。現状、電子署名は、それほど普及している訳ではありません。無理な移行スケジュールは、適切に電子署名が利用されるべき場面においても、電子署名が利用されなくなる可能性も高いと考えます。電子署名が使われなくなるため問題も無くなるといった本末転倒な結果にならないよう十二分に検討をお願いします。

# IETFにおける動向

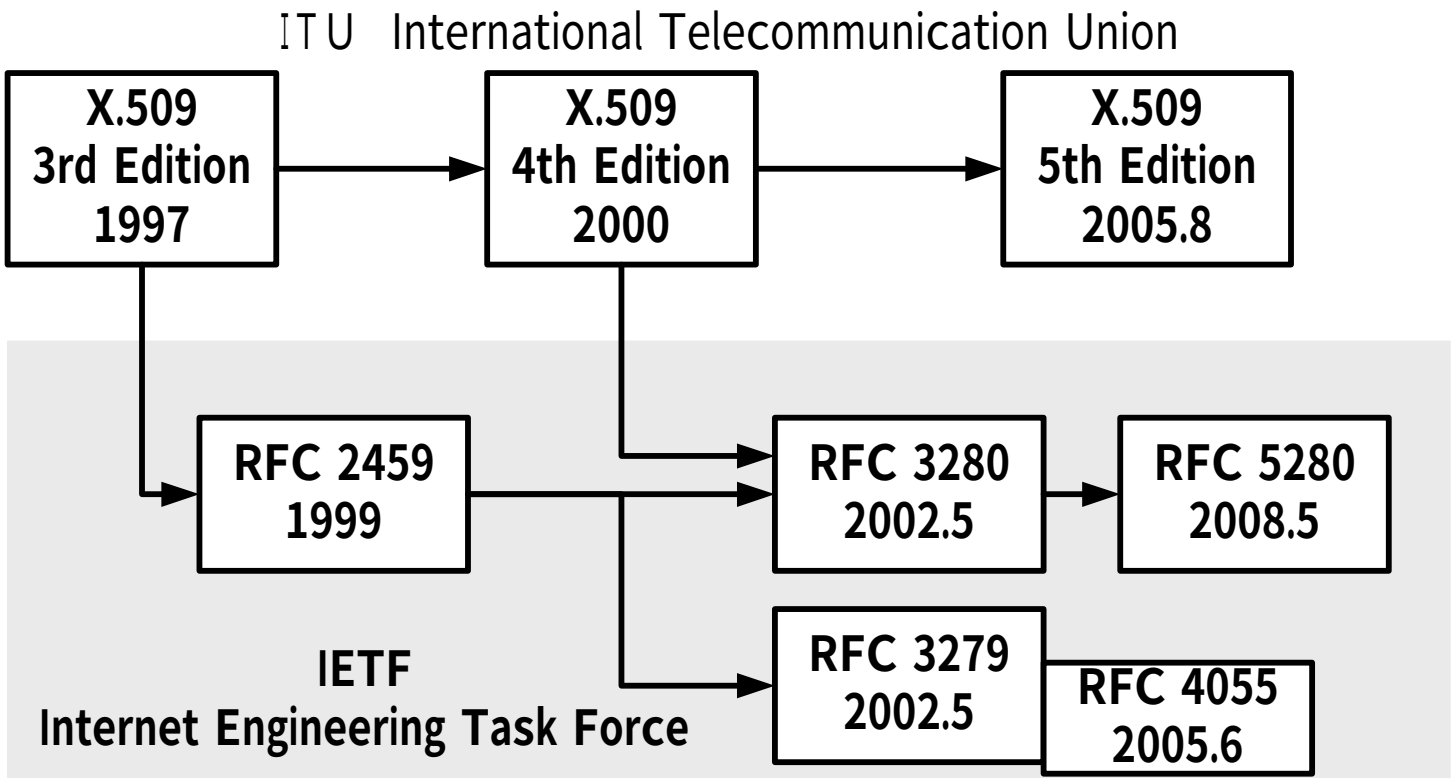
暗号アルゴリズム自体のレイヤーとの違いがある。

# IETFにおける動向
# 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　–2005年頃の見解
  - 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における動向
# 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における動向
# 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
- “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における動向
# RFC 5246 TSL 1.2 2008年8月 ＲＦＣ化

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 5246

•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における動向
# 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における動向
# 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。

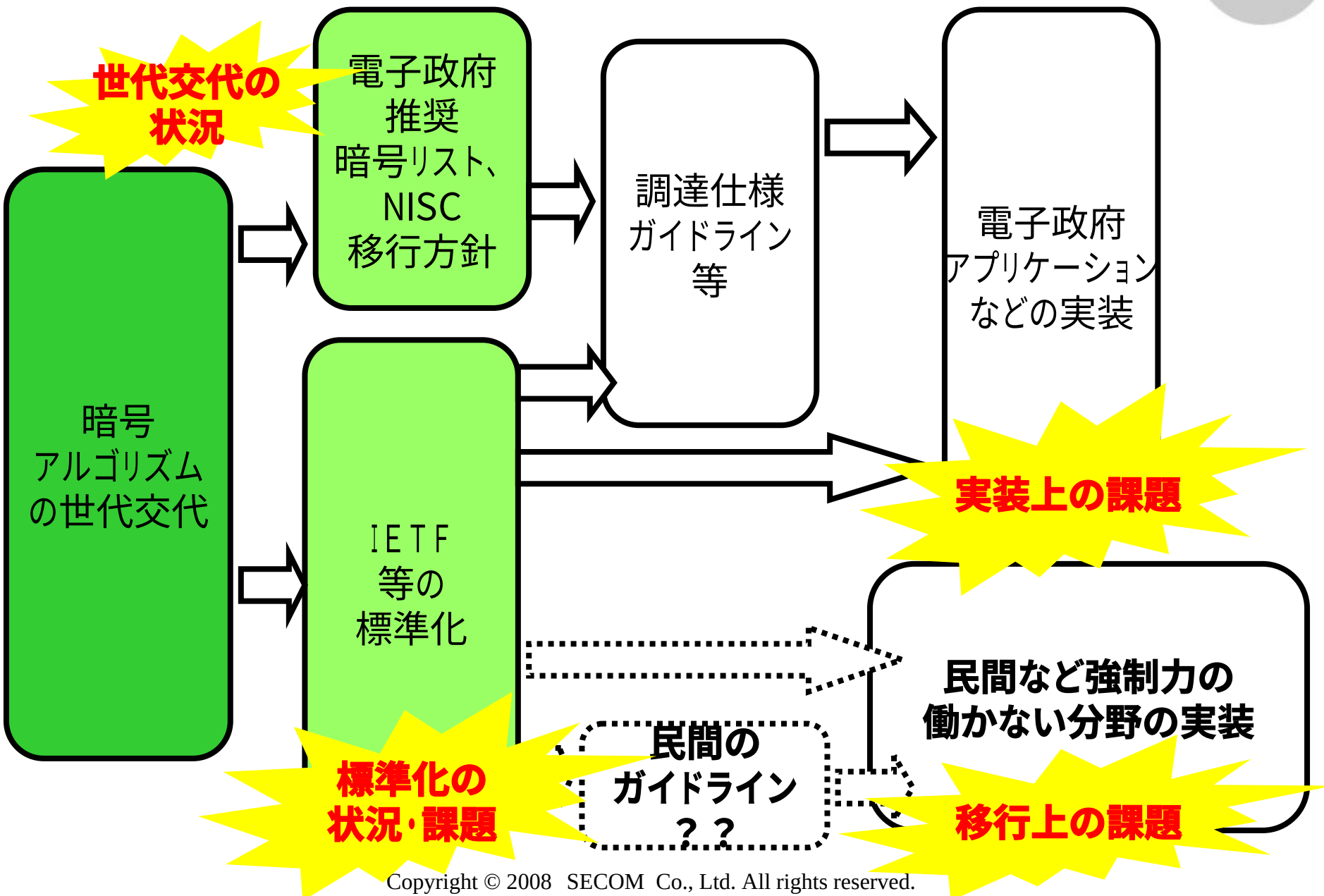
*これまでのインターネットプロトコルの開発の常識を超えている。これまでのインターネットプロトコルの開発は、Simple なプロトコルと実装を、下位互換性を確保しつつ、少しずつ進化してきた。送り手は保守的に受け側は革新的に。。。。で*

セコム IS 研究所
Intelligent Systems Laboratory

# 暗号アルゴリズムの移行の議論

# 暗号アルゴリズム、標準化、実装の関係

セコム IS 研究所
Intelligent Systems Laboratory



# (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
  - ???

「PKI相互運用技術からみたSHA-1問題 - PKI day 2006」より。
http://www.jnsa.org/seminar/2006/20060607/matsumoto_02.pdf

# 暗号アルゴリムの移行問題に関連した懸念されること

セコム IS 研究所
Intelligent Systems Laboratory

- 民間では、まったく無視されて。。。移行されない
- 誤った移行方針によりPKI等に関連したビジネスの障害になる可能性
  - 例えば。。電子署名が（更に）敬遠される可能性
    - ユーザID/パスワードへ流れる。。。
- 風評的なリスク
  - 危なくないものを危ないと思われるリスク
    - 「SHA-1はもうダメ」「RSA 1024bitはもうダメ」
- 移行のコスト
  - 現実的な問題

# 住基カードの対応スケジュール案？？


２０１１年末まで、RSA1024bitまでしか対応できない有効期間１０年の住基カードが、2011年末まで発行され続ける。

**出展：公的個人認証サービスにおける暗号方式等の移行に関する検討会 第1回会合資料**

# 松本の考え？

- 暗号アルゴリズム移行問題は、ロングターム・セキュリティ問題。IT技術が基盤化するなか、中長期的な展望を持って対応する必要がある。
- これには、多くの（普段は会話が成り立たない）関与者を取りまとめる努力が必要であり、こうした枠組み自体が課題
- 技術的な観点からは、鍵のライフサイクル管理の中で、暗号アルゴリズムの移行が行なわれる技術を確立する必要がある。

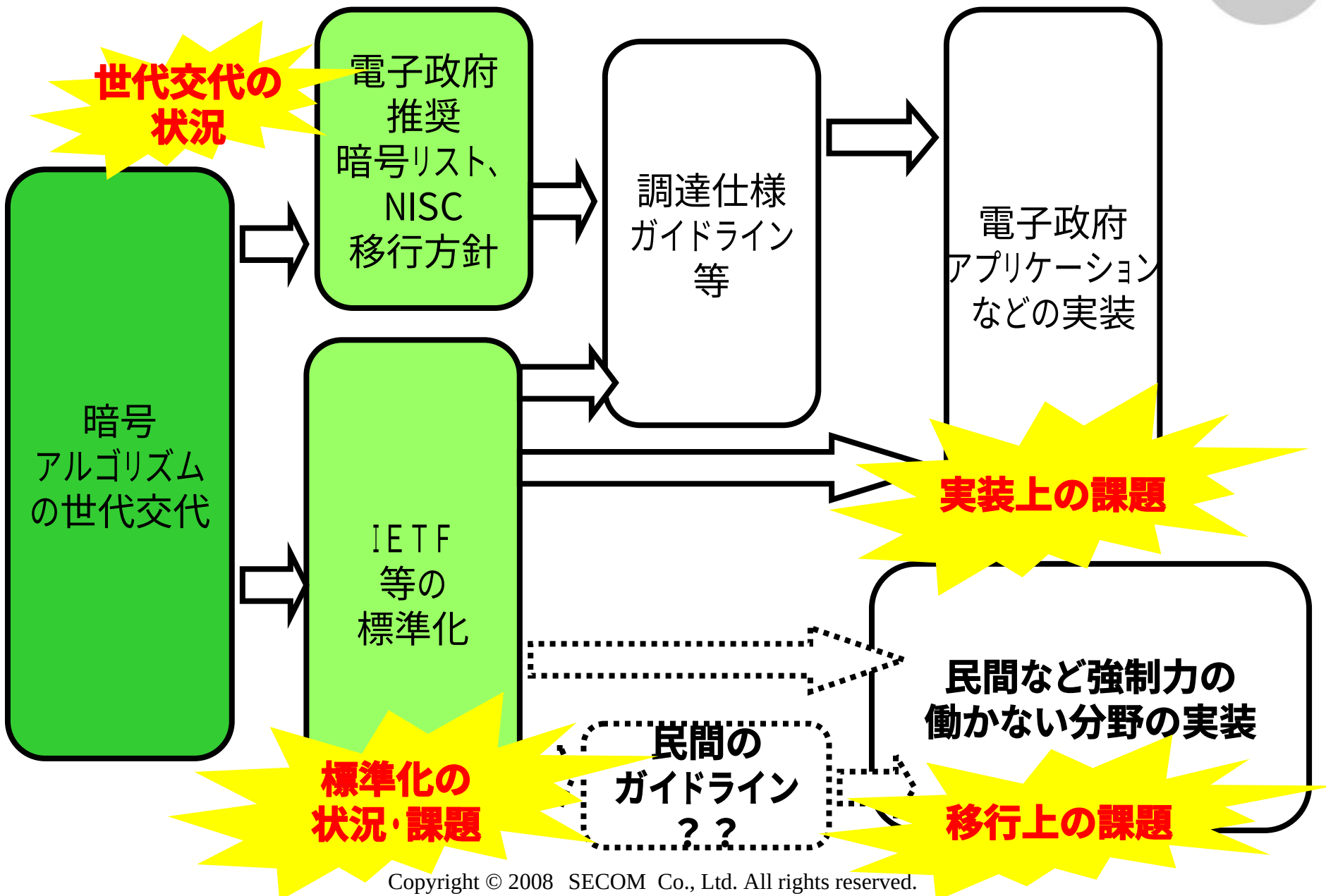
セコムIS研究所
Intelligent Systems Laboratory

# パネルディスカッション
# 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～

HTTPS Meeting　？？

# 暗号アルゴリズム、標準化、実装の関係

セコム IS 研究所
Intelligent Systems Laboratory



# 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～

- **各関与者の果すべき役割**
  - **政府**
  - **民間**
  - **暗号技術コミュニティ**
  - **インターネットコミュニティ**

# 付録

# 付録

- タイムスタンプの事例
- 認証局の鍵更新
- 現実の問題
- 2014年の出来事
- 電子署名法との関係
- 「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」報告書の記述

# タイムスタンプの事例

## 既にSHA-2ファミリを利用しているタイムスタンプ（時刻証明）の事例

# 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

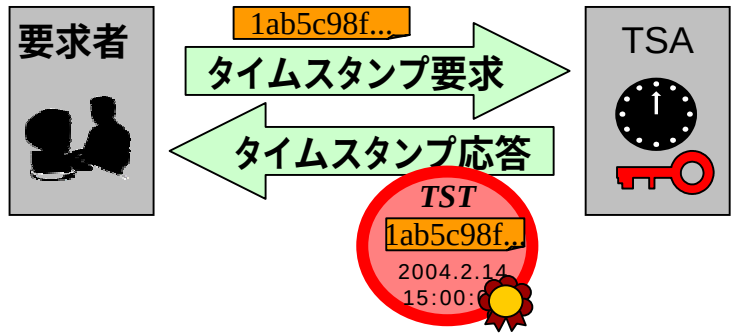
- 日本データ通信協会のタイムビジネス信頼・安心認定制度
  - http://www.dekyo.or.jp/tb/tbtop.html
- 日本データ通信協会のタイムビジネス信頼・安心認定制度の審査基準（2005年6月16日）
  - http://www.dekyo.or.jp/tb/shinsakizyun(DSHA-1henkou)2ndV0506.pdf
  - ハッシュ関数のビット長を2006年4月1日以降は256bit以上とすることを追記
    - messageImprintのhashAlgorithmが対象
    - TSAによる署名アルゴリズムは対象外
      - 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)



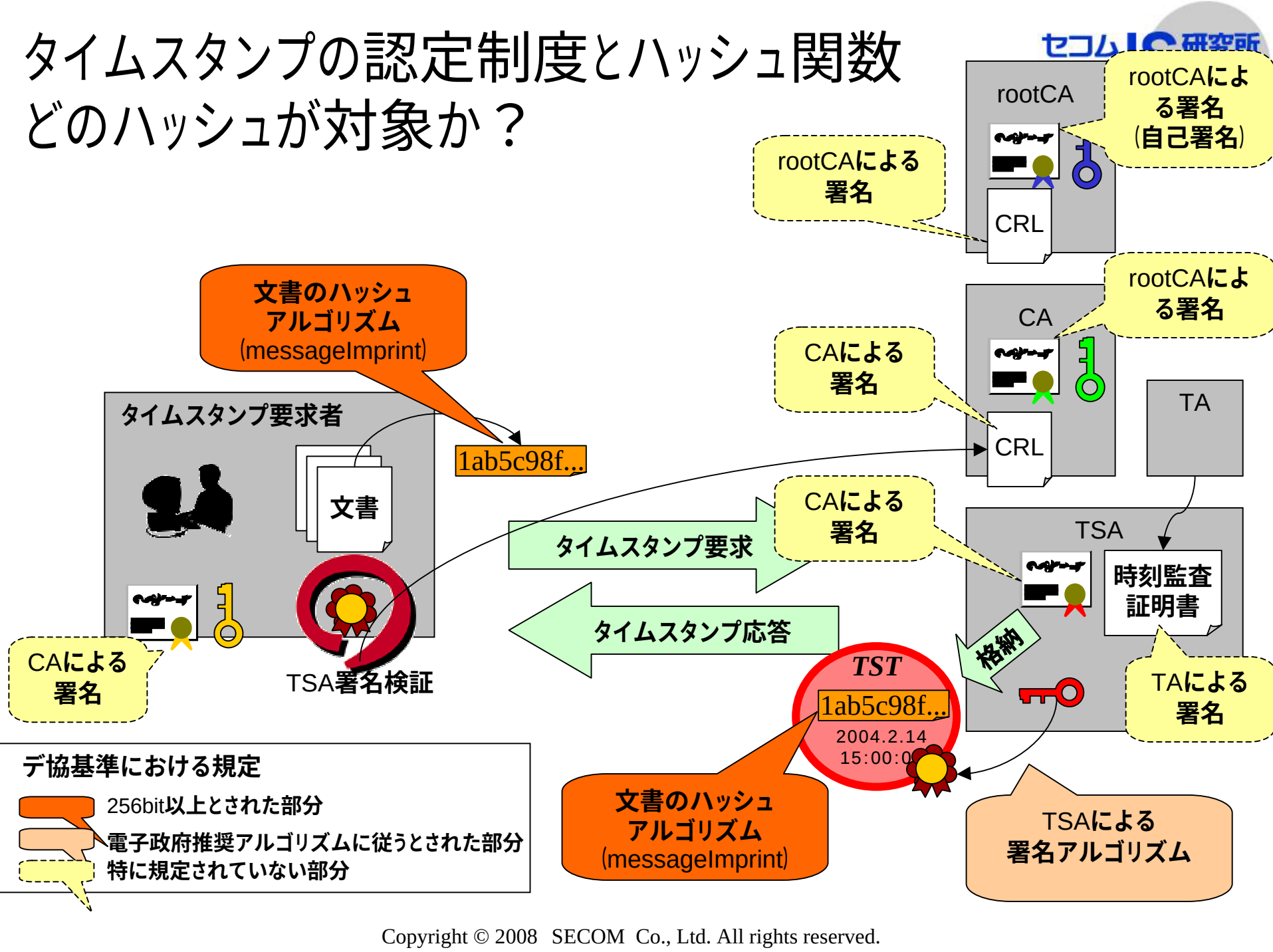

**TimeStampResp (タイムスタンプ応答)**

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

HTTPS Meeting??

# 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

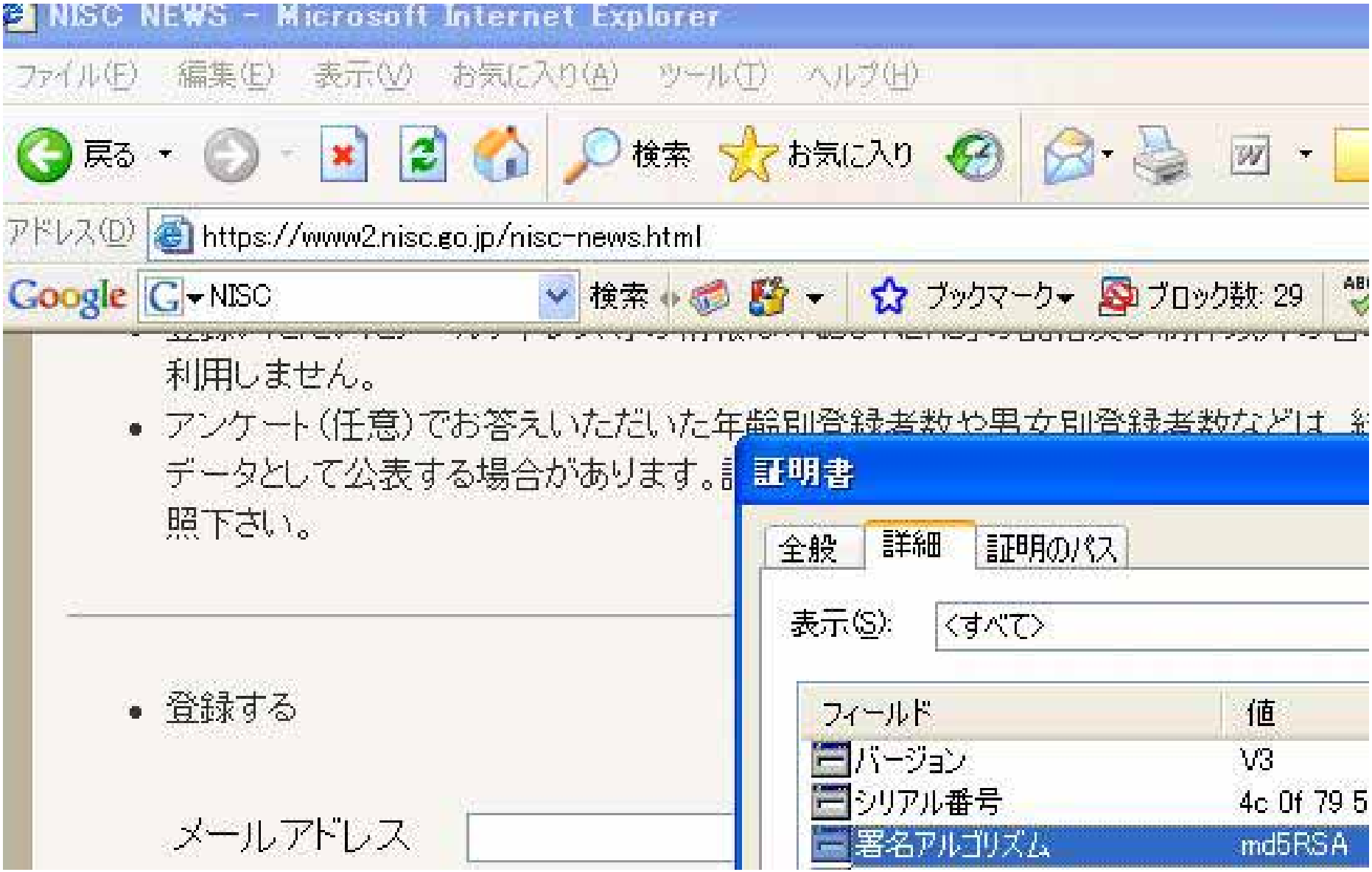
*・政府機関の情報セキュリティ対策のための統一基準（２００５年項目限定版）*

*・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。*

# どの位？危ないのか？
# 某サイトのSSL証明書

セコム IS 研究所
Intelligent Systems Laboratory



# 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？）

# 認証局の鍵更新

鍵には寿命があり、暗号技術を応用したシステムは鍵更新のメカニズムが重要。

この鍵更新のメカニズムの中に暗号アルゴリズムの移行も組み込まれるべきだが、こうした技術の重要性は、広く理解されるべき。

# 移行の問題
# 認証局の鍵更新

セコム IS 研究所
Intelligent Systems Laboratory

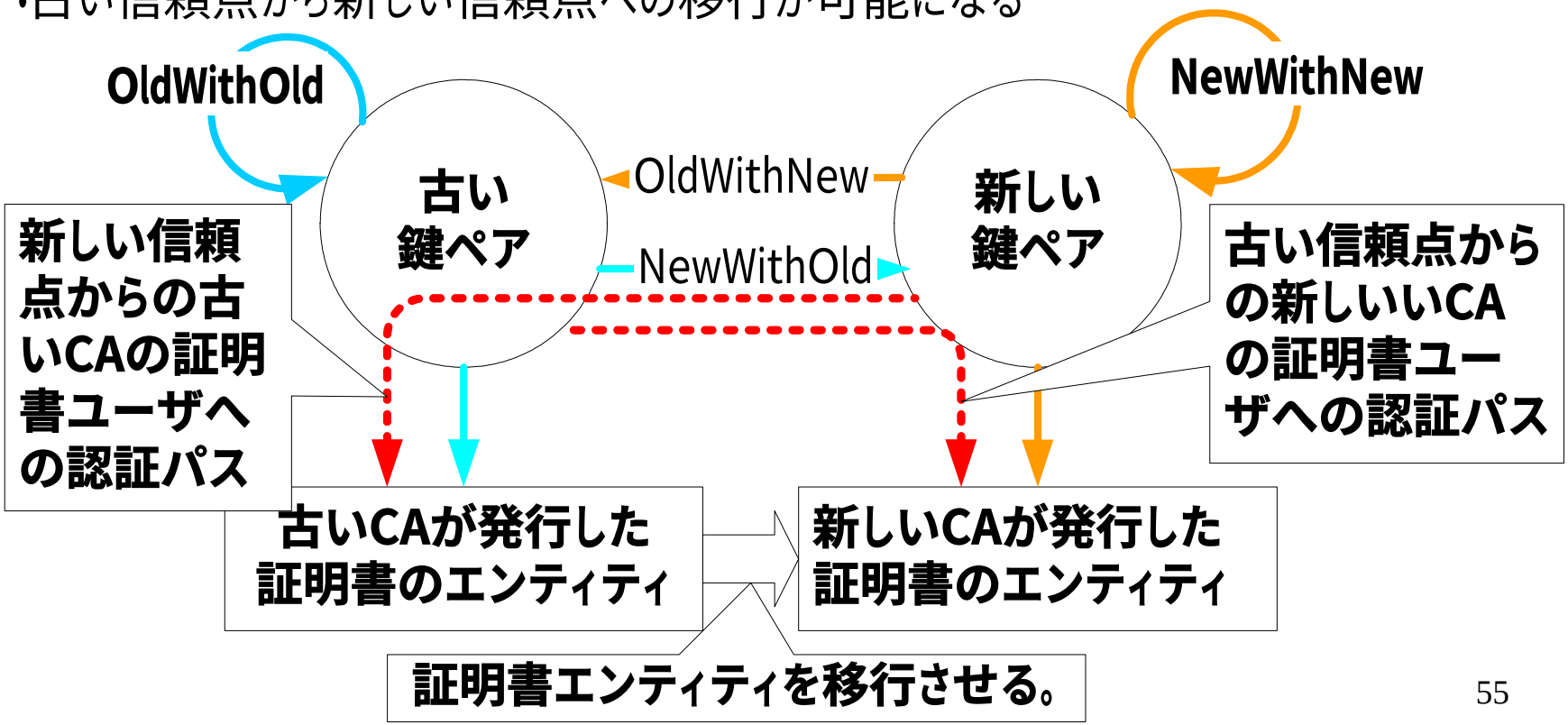
- 認証局の私有鍵(署名鍵)
  - 認証局にとって「鍵(署名鍵)は命」　-　認証局に限らずあるべきアーキテクチャ
- GPKI (政府認証基盤)の認証局の自己署名証明書と署名
  - 現在の暗号アルゴリズム　RSA (2048bit) With SHA-1
  - 自己署名証明書の有効期間　10年の有効期間
  - 署名鍵(私有鍵)の有効期間　5年 (5年で鍵更新)
- なぜ鍵更新が重要か
  - 鍵の耐用年数、暗号アルゴリズムの耐用年数などの対応だから。
    - つまり「鍵更新」は、Long-Term Security対応の技術
  - あまり長い自己署名証明書の有効期間は怪しい
- 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

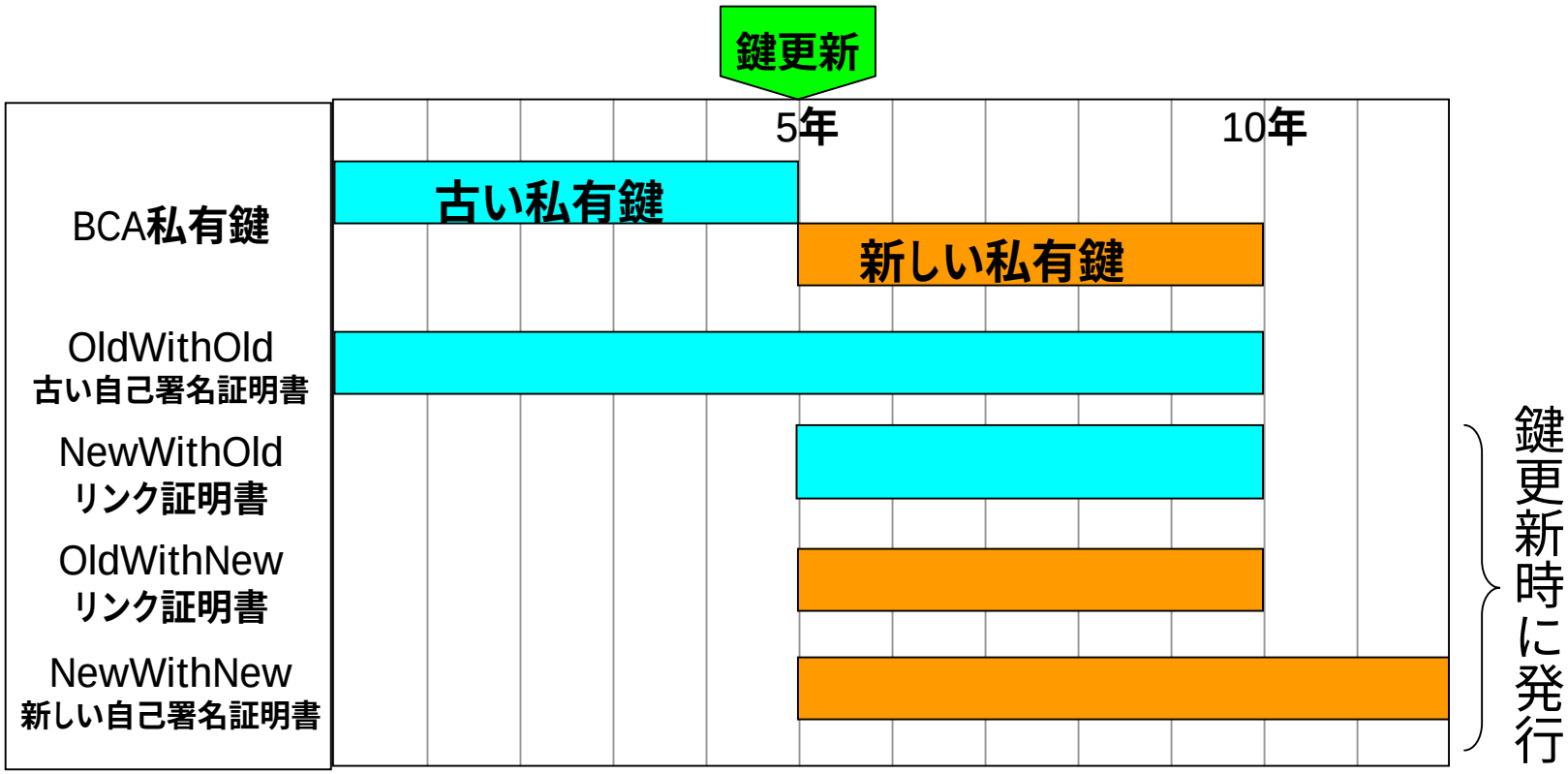
- 新しい鍵ペアと古い鍵ペアの関係を証明する自己発行証明書(Self Issue Certificate)が発行される。
  - 古い公開鍵を新しい私有鍵で署名した証明書(OldWithNew)
  - 新しい公開鍵を古い私有鍵で署名した証明書 (NewWithOld)
- 古い信頼点から新しい信頼点への移行が可能になる



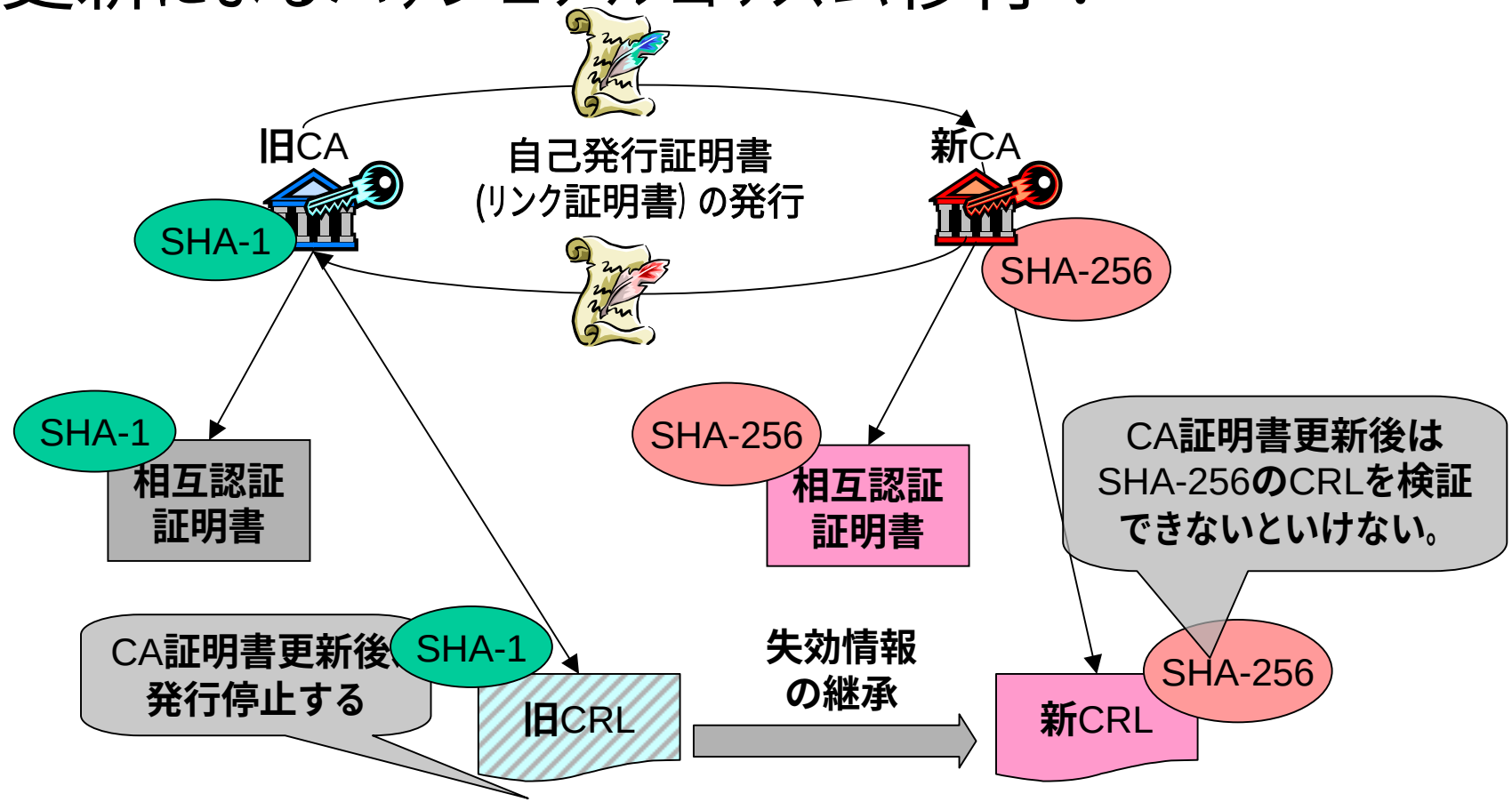
# 移行の問題
# ブリッジモデルにおける鍵更新の考え方

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<br>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。<br>sha1WithRSAEncryption (1.2.840.113549.1.1.5)<br>dsaWithSha1 (1.2.840.10040.4.3)<br>md5WithRSAEncryption (1.2.840.113549.1.1.4)<br>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。 |

# 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….

# 2015年の出来事

# 2015年の出来事。。。。
# 現実の電子署名のリスク

- 本申請では、これまで発行したRSA 1024bitの証明書は利用できなくなります。
- 本申請では、これを契機に、(評判の悪かった) 電子署名を省略することにしました。

セコムIS研究所
Intelligent Systems Laboratory

# 2015年の出来事。。。。
## リスクとセキュリティコストのトレードオフ

- 3万円以下の領収書の電子署名を付したスキャン文書の保管について
- RSA1024bit の証明書に対応した鍵が、世界最高速のコンピュータを１年借り切ることができると、破られることが分かりました。
- 以上の理由から「3万円以下」を「３千円以下」に変更します。

# 2014年の出来事。。。。
# 何がリスクか？

- 政府のセキュリティ基準へ適合させるため、PKIのクライアント証明書をSHA-2に変更する必要がありますが、そうするとVPNが動作しなくなります。
- そのため、ユーザID・パスワードに変更します。

# 電子署名法との関係

# 電子署名法に関連して懸念されること

セコム IS 研究所
Intelligent Systems Laboratory

- 誤った移行方針により電子署名に関連したビジネスの障害になる可能性
  - 電子署名が（更に）敬遠される可能性
    - ユーザID/パスワードへ流れる。。。
- 風評的なリスク
  - 危なくないものを危ないと思われるリスク
    - 「SHA-1はもうダメ」「RSA 1024bitはもうダメ」
- 移行のコスト
  - 現実的な問題
- 電子署名法の様々な問題点がかき消される
  - 電子署名法の制度的な問題点を改めるチャンスなのだが「暗号アルゴリズム」のみがフォーカスされてしまう

# 「懸念されること」が払拭されるには

- 「適切な移行方針」
  - 移行時の課題の理解
- 暗号アルゴリズムの脆弱化の正しい理解
- 電子署名法に対する正しい提言

# 暗号アルゴリズムの脆弱化の理解

- 現在、問題になっているのは、
  - RSA 1024 bit
  - SHA-1
- 「暗号アルゴリズムの脆弱化」の理解の問題
  - 「脆弱化」、「危殆化」、「世代交代」。。。。。。
  - そもそも、中短期的に「危ない」と呼べるものではない。。。が。。世の中の人が、そう思わない可能性がある。これを間違えると、移行のために「懸念されること」が顕在化する可能性がある。

# 電子署名法の疑問点

セコムIS研究所
Intelligent Systems Laboratory

- そもそも、現在の電子署名法自体、暗号アルゴリズムの扱いによく分からない点がある。
  - 電子署名法に記述されているのは、「EE」が署名で利用する「暗号アルゴリズムと鍵長」は、明示的に示されているが、「ハッシュアルゴリズム」に関しては分かりつらい。
  - 暗号アルゴリズムと鍵長は、EE証明書により決まるが、EEの署名のハッシュアルゴリズムに関しては、認証局への要求にはならない。したがって、誰に対する要求なの分からないところがある。
  - 認証局の証明書に利用するハッシュアルゴリズムは、規定されているのかどうかわからない。
  - 「電子証明書」は、EE証明書を指すと思われるが、CA証明書、自己署名証明書がある。リスクという観点からは、CA証明書、自己署名証明書の方が重要。しかし、これらのことは、電子署名法自体では示唆されていない。

# 電子署名法の記述

ハッシュアルゴリズムの扱いは、結構分かりにくい

# 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

セコムIS研究所 Intelligent Systems Laboratory

http://www.moj.go.jp/MINJI/minji32-3.html

- 第三条　規則第二条の基準を満たす電子署名の方式は、次の各号のいずれかとする。
  - 一　ＲＳＡ方式（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　五）又はＲＳＡ－ＰＳＳ方式（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　一〇）であって、モジュラスとなる合成数が千二十四ビット以上のもの
  - 二　ＥＣＤＳＡ方式（オブジェクト識別子　一　二　八四〇　一〇〇四五四　一）であって、楕円曲線の定義体及び位数が百六十ビット以上のもの
  - 三　ＤＳＡ方式（オブジェクト識別子　一　二　八四〇　一〇〇四〇　四三）であって、モジュラスとなる素数が千二十四ビットのもの

ここで、ハッシュ関数については、オブジェクト識別子を指定することにより指定されている。これは、わかりづらい。
「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」なので、EE環境におけるハッシュアルゴリズムに関しては、「特定認証業務の認定」とは、関係ないとも言える。

# 電子署名及び認証業務に関する法律施行規則 (平成十三年三月二十七日総務省・法務省・経済産業省令第二号)

セコム IS 研究所 Intelligent Systems Laboratory

- 第二条　法第二条第三項 の主務省令で定める基準は、電子署名の安全性が次のいずれかの有する困難性に基づくものであることとする。
- 一　ほぼ同じ大きさの二つの素数の積である千二十四ビット以上の整数の素因数分解
- 二　大きさ千二十四ビット以上の有限体の乗法群における離散対数の計算
- 三　楕円曲線上の点がなす大きさ百六十ビット以上の群における離散対数の計算
- 四　前三号に掲げるものに相当する困難性を有するものとして主務大臣が認めるもの

これは、EE環境の環境を規定していると言える。
ハッシュアルゴリズムに関しては、記述されていない。

# 電子署名及び認証業務に関する法律施行規則（平成十三年三月二十七日総務省・法務省・経済産業省令第二号）

セコム IS 研究所
Intelligent Systems Laboratory

- 四　認証業務用設備のうち電子証明書の発行者（認証業務の名称により識別されるものである場合においては、その業務を含む。以下同じ。）を確認するための措置であって第二条の基準に適合するものを行うために発行者が用いる符号（以下「発行者署名符号」という。）を作成し又は管理する電子計算機は、当該発行者署名符号の漏えいを防止するために必要な機能を有する専用の電子計算機であること。

「電子証明書」は、「第二条の基準に適合する」としている。
第二条は、鍵長について記述されているが、ハッシュアルゴリズムに関しては、記述されていない。

# 電子署名及び認証業務に関する法律施行規則（平成十三年三月二十七日総務省・法務省・経済産業省令第二号）

- 第六条第一項第三号 の主務省令で定める基準は、次のとおりとする。
- 四　電子証明書の有効期間は、五年を超えないものであること。
- 六　電子証明書には、その発行者を確認するための措置であって第二条の基準に適合するものが講じられていること。

# 「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」報告書の記述

この報告書は、ＮＩＳＣの方針案以前に公表されており、民間に対しての強制力の働く電子署名法としての方向性を示している。しかし、現状非常にニッチ？

# 報告書の記述
# ハッシュ関数の安全性に係る状況

セコム IS 研究所
Intelligent Systems Laboratory

- ハッシュ関数は、非可逆（一方向）な特徴や衝突発見困難性3を利用して、悪意を持った者による情報の改ざんや機器等の障害によるエラーを検出するために利用できる技 術であり、電子署名においても利用されている。
- 電子文書への電子署名においては、複数レベルの脅威が想定される。
- ・電子署名が無い複数の異なる文書に同一の電子署名が付される脅威（衝突計算攻撃）
- ・電子署名が付された電子文書と同一の電子署名が別の電子文書に付される脅威（第二原像計算攻撃4）
- 電子署名法は、電子文書に付す電子署名に紙文書における署名と同等の推定効を与える法律であるので、電子署名者による否認を防止できること及び電子署名の信頼性を技術的に確保する必要がある。このためには、第二原像計算攻撃による脅威のみならず、衝突計算攻撃による脅威も含めて想定する必要がある。
- 近年、従来より少ない計算量で衝突計算攻撃を行う手法が明らかになり（図２－１参照）、要する時間も短縮されつつある。

# 報告書の記述
# SHA-1における衝突計算攻撃に要する時間の推定

- 暗号技術検討会により示された情報によると、SHA-1 の衝突を総当りで見つけるには 2^80回程度SHA-1の実行を必要とし、国内最高速のスーパーコンピュータを用いて100万年程度の時間がかかると推定される。一方、同検討会において、新たな攻撃手法（Wangらの手法CRYPTO2005）を用いた場合、2^69回程度のSHA-1の実行で衝突が発見され、国内最高速のスーパーコンピュータを用いれば462年以下でそれが可能になると推定されて いる。ただし、処理時間については、計算アルゴリズムや計算機のアーキテクチャなどに依存して大きく変わり得る。
- SHA-1 等のハッシュ関数については新たな攻撃手法に関する研究の進展によって、衝 突発見までの時間が格段に短縮されるおそれがある。また、今後の技術の進歩によっては、スーパーコンピュータだけではなく、インターネットを利用して世界中の国々で分散処理を行う分散コンピューティングシステムによっても、本推定以上の衝突発見能力が実現される可能性もある。

セコムIS研究所
Intelligent Systems Laboratory

# 報告書の記述
# 鍵強度の低下に関する影響

- **RSA 暗号は、素因数分解問題の困難さをその安全性の根拠としている。長く用いられてきた既知の解法以外に画期的な解法が発見される可能性は低いと言われているもの**
- **の、コンピュータの計算速度の向上によって、本来秘密にしておかなければならない秘密鍵を公開鍵から導出することが可能となる。**
- **電子署名では、秘密鍵が解読されることにより、電子署名の偽造が可能な状態となる。**

# 報告書の記述

セコム IS 研究所
Intelligent Systems Laboratory

- ー SHA-1 は、電子署名のアルゴリズム中に利用されており、電子文書への電子署名においては、複数レベルの脅威が想定される。
- ・電子署名が無い複数の異なる文書に同一の電子署名が付される脅威（衝突計算攻 撃）
- ・電子署名が付された電子文書と同一の電子署名が別の電子文書に付される脅威（第二原像計算攻撃）
- 衝突計算攻撃に要する時間の推定に関しては、2006年6月時点において、国内最高速のスーパーコンピュータを用いれば462年以下で衝突発見されるおそれがあることが示されている。一方、第二原像計算攻撃に関しては、現時点において報告されてはいない。
- 電子署名法は、電子文書に付す電子署名に紙文書における署名と同等の推定効を与える法律であるので、電子署名者による否認を防止できること及び電子署名の信頼性を技術的に確保する必要がある。このためには、第二原像計算攻撃による脅威のみならず、衝突計算攻撃による脅威も含めて想定する必要がある。
- 衝突計算攻撃による脅威は、2015年前後には現実的になることが想定される（図２ー３）ので、念のため、より安全性（衝突発見困難性）の高いアルゴリズムに移行することが望ましいこと。

# 報告書の記述

- **二 RSA1024bitについては、概ね2015年以降に、危殆化のおそれが高まってくることが示されている（図2－4）こと。**

# 報告書案の記述

セコム IS 研究所
Intelligent Systems Laboratory

- 三 政府機関情報システム移行指針(案)において提示されている、政府機関の各情報システムを新暗号アルゴリズムへ適応させる時期は2013年度までであること。（注：政府機関情報システム移行指針（案）は、3月7日を締切日としてパブリックコメントの募集が行われており、その状況によってはこの提示どおりとはならない可能性がある）。
- したがって、これらの要素及び電子証明書の有効期間を勘案すれば、SHA-2 及びRSA2048bitによる電子署名についての特定認証業務の認定は遅くとも2014年度早期までに行うことが必要である。

# 報告書案の記述 – ここの解釈が難しい

セコム IS 研究所
Intelligent Systems Laboratory

| | |
|---|---|
| 2008年度早期 | **暗号アルゴリズムの移行に向けた具体的な検討の開始、特定認証業務に係る電子署名の基準にSHA-2を追加。** |
| (2010年度) | (政府機関システム暗号移行開始)　*政府機関システム移行指針(案)による |
| (2013年度) | (政府機関システム新旧暗号アルゴリズム(SHA-1及びSHA-2、RSA1024bit及び2048bit)対応環境構築が完了)　*政府機関システム移行指針(案)による |
| 2013年度末まで | 認定認証事業者に対して、暗号移行に係る変更認定のための調査が必要な場合は実施し、認定認証事業者は、RSA2048bitを用いた発行者鍵ペア[1]を新たに生成する必要がある場合は、生成。 |
| 2014年度早期まで | 認定認証事業者は、RSA2048bitによる発行者鍵ペアを活性化させSHA-2及びRSA2048bitによる電子署名についての認証業務を開始。 |
| 2014年度末前後を目途 | SHA-1、RSA1024bitによる利用者電子証明書の有効期間後に、特定認証業務に係る電子署名の基準から、SHA-1、RSA1024bitを削除。（SHA-1、RSA1024bitによる利用者電子証明書の有効期間について、各認定認証事業者は、SHA-2、RSA2048bitによる利用者電子証明書への切替を考慮し、あらかじめ調整を図ること等が求められる。） |

# 移行スケジュールに対する松本個人の考え

セコム IS 研究所 Intelligent Systems Laboratory

- 署名環境の問題
  - RSAwithSHA-1/RSA1024　2015年まで
  - RSAwithSHA-256/RSA2048　2014年より電子政府で利用可能
- EE証明書の問題
  - RSAwithSHA-1/RSA 1024　2015年まで
    - 5年が有効期限の証明書の発行は、2010年まで
  - RSAwithSHA-1/RSA 2048　2019年まで
    - 5年が有効期限の証明書の発行は、2014年まで
  - RSAWithSHA-256/RSA 2048
    - 2008年より発行可能。2014年より電子政府で利用可能なので、実質2014年から発行
- 自己署名証明書
  - RSAwithSHA-1/RSA 2048　2019年まで
  - RSAwithSHA-256/RSA 2048 ***

# 移行スケジュールに対する松本個人の考え

- 現状、EEの鍵長2048bitで、問題なく検証できるか？
  - GPKI相互運用性仕様書では、OKのはず。
- RSAwithSHA-1 (RSA 2048)の証明書が、2019年までの有効期限を持てるなら、RSAwithSHA-1 (RSA 1024)からRSAwithSHA-1 (RSA 2048)に切り替えて
- ＥＥ証明書5年を発行を継続できる。
- JPKIの場合、有効期限３年なので、2011年までに2048bit対応ができれば、有効期限３年が継続できる
  - #ただし、住基カードの多くは、現在、1024bitまでらしい。
- 2014年以降、SHA-1の証明書の新規発行は禁止する。ただし、発行済みのRSAwithSHA-1 (RSA 2048)は、まだ有効。
- 自己署名証明書は、2048bit SHA-1のまま。この「自己署名証明書は、2048bit SHA-1」のまま、SHA-256/RSA2048bit で署名した証明書とCRLを発行。
- 2014年以降、各認証局の鍵更新のタイミングで、各認証局は、新しい2048bit SHA-2 の自己署名証明書を発行する。

# 移行スケジュールに対する松本個人の考え

セコム IS 研究所 Intelligent Systems Laboratory

| 対象 | 署名 | 現状 | 今後の案 | 備考 |
|---|---|---|---|---|
| フィンガープリント | - | SHA-1 | SHA-256 | SHA-256にしても<br>影響は少ない |
| 自己署名証明書 | CA | 署名<br>RSA2048/SHA-1<br>鍵　RSA2048 | 署名<br>RSA2048/SHA-1<br>鍵　RSA2048 | MS証明書リストでは、<br>RSA1024/MD5も多数ある。<br>自己署名証明書がSHA-256である必然性はほとんどない。 |
| CA証明書<br>(相互認証証明書) | CA | 署名<br>RSA2048/SHA-1<br>鍵　RSA2048 | 署名<br>RSA2048/SHA-1<br>鍵　RSA2048 | RSA2048/SHA-256の必要は、当面ないのでは？<br>自己署名証明書よりは、早くSHA-256に移行する |
| EE証明書 | CA | 署名<br>RSA2048/SHA-1<br>鍵　RSA1024 | 署名<br>RSA2048/SHA-1<br>鍵　RSA2048　?? | EE鍵長が問題<br>自己署名証明書よりは、早くSHA-256に移行する |
| 署名 | EE | 署名<br>RSA1024/SHA-1 | 署名<br>RSA2048/SHA-256 | 署名プログラムの対応になる |

# 参考となる資料

# 参考となる資料　その１

- PKI相互運用技術からみたSHA-1問題
  - http://www.jnsa.org/seminar/2006/20060607/matsumoto_02.pdf
- 【パネルディスカッション】「暗号アルゴリズム移行問題」
  - http://www.jnsa.org/seminar/2008/0703/
- 「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」
  - http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf
- ご意見の概要及びご意見に対する考え方
  - http://www.nisc.go.jp/active/general/pdf/crypto_pl_resp.pdf

# 参考となる資料　その2

セコムIS研究所
Intelligent Systems Laboratory

- 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