セコムIS研究所
Intelligent Systems Laboratory

パネルディスカッション
暗号アルゴリムの移行問題

セコム株式会社 IS研究所
松本　泰

2008 年 7月 3日

パネルディスカッション
暗号アルゴリムの移行問題

セコムIS研究所
Intelligent Systems Laboratory

- 「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」が2008年4月に決定しました。この「移行指針」の案に対して、NPO JNSAのPKI相互運用技術WGでは、パブリックコメントを提出しています。「移行指針」は、決定していますが、「PKI相互運用技術WG」のパブリックコメントの返答にあるとおり、移行には、課題があります。パネルディスカッション「暗号アルゴリズムの移行問題」では、政府に限らず、民間も含め、「暗号アルゴリズムの移行問題」についてディスカッションを行います。
- ＜参考＞
  「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)に対する提出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

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

暗号アルゴリズムの脆弱化の理解
RSAの話は、比較的分かりやすい

セコム IS 研究所
Intelligent Systems Laboratory

- **RSA 1024bitの扱い**
  - **ほとんどのCAの鍵はRSA 2048bit(RSA 1024bitも存在する)**
  - **現在、問題になっているのはEE証明書の鍵長**
- **「署名法施行状況検討会報告書」**
  - **「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こと」**
    - **根拠は、2015年頃、世界最高速なコンピュータを1年で公開鍵から秘密鍵(Private Key)を算出できる可能性がある。**
      - **EEの鍵の攻撃のコストとして、これが、本当にリスクなのか？といったことはさておき**
- **論点**
  - **RSA 1024bitの次は、RSA 2048bitなのか？**
    - **RSA 1536bit とか。。。。**
    - **ICカードの性能の問題**
      - **RSA 2048bitは、性能的、コスト的問題がある。**

暗号アルゴリズムの脆弱化の理解
SHA-1の話。。。。これの理解が難しい

セコム IS 研究所
Intelligent Systems Laboratory

- SHA-1の脆弱化で問題になるのは、その使われ方に大きく依存する。
- 暗号技術的な攻撃の分類には、衝突攻撃 (Collision Attack) 、原像探索攻撃 (Pre-image Attack) 、別原像探索攻撃(Second Pre-image Attack)の3つがあり、攻撃が成立する可能性があるのは、衝突攻撃 (Collision Attack) のみ。
- 衝突攻撃 (Collision Attack) が成立したとしても、現実的な攻撃が可能な訳ではない。
  - SHA-1で、「現実的な攻撃が可能」な計算量は、まだ、よく分かっていない。

「理解が難しい」だけではなく、「ハッシュアルゴリズムの脆弱化に対する実質的な脅威」についての研究も少なく、本当のところは分かっていない。そのため移行のための論理も飛躍しているところがある。

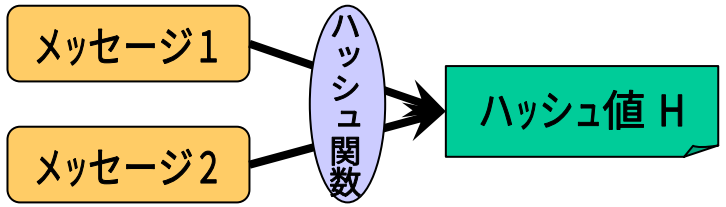
暗号アルゴリズムの脆弱化の理解
ハッシュ関数への攻撃

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。

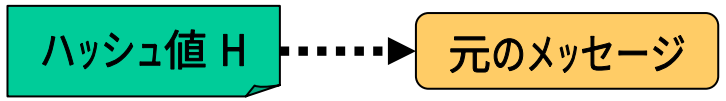
計算量 $2^{n/2}$



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。

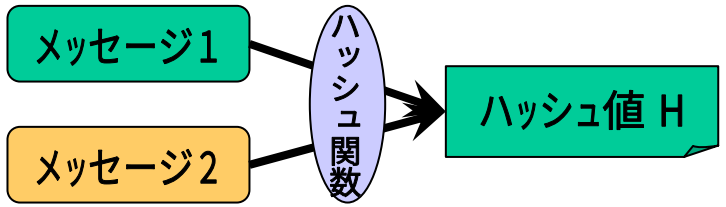
2^{n}



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

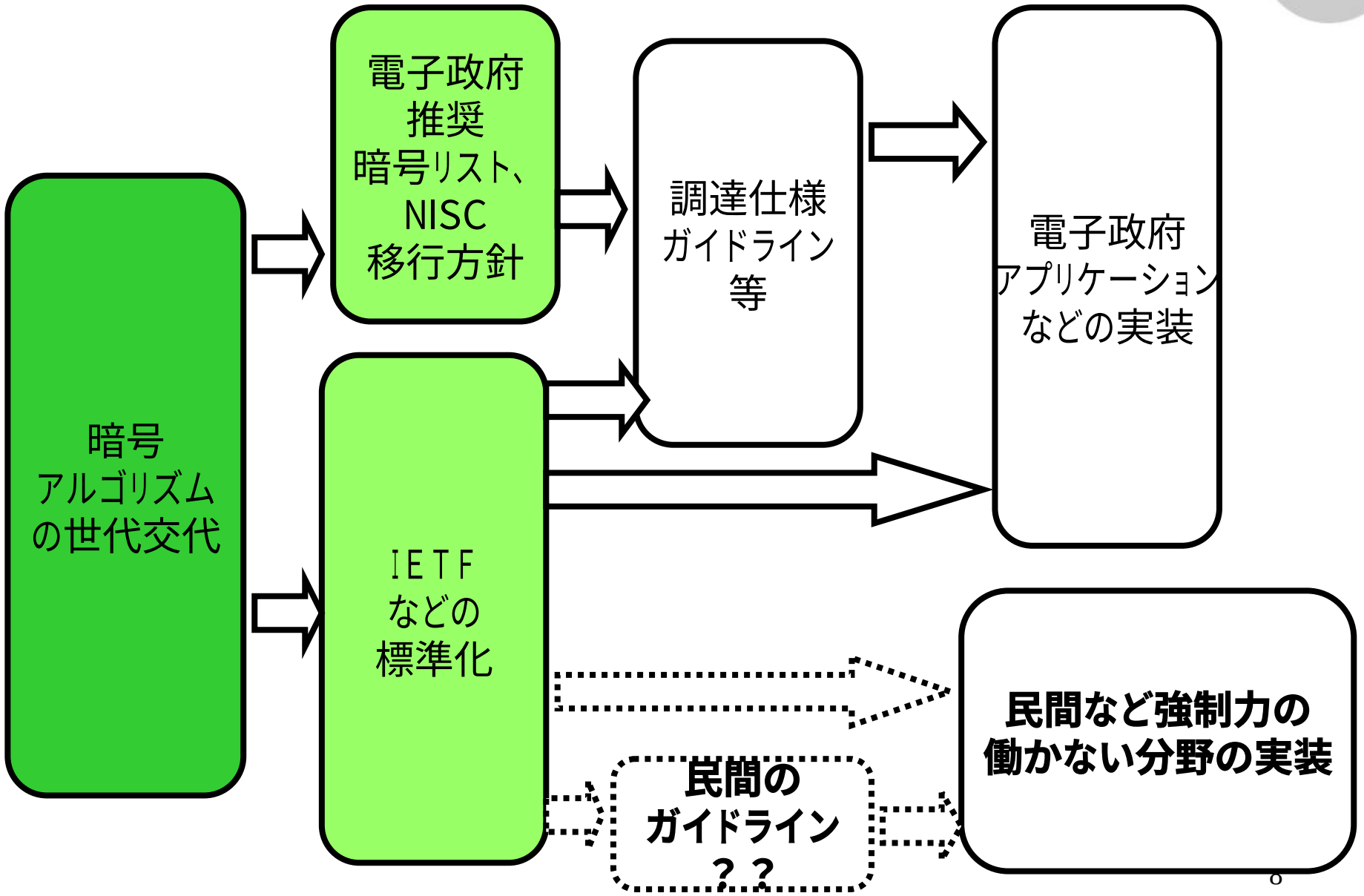
セコム IS 研究所
Intelligent Systems Laboratory

- 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

暗号アルゴリズム、標準化、実装の関係

セコムIS研究所
Intelligent Systems Laboratory



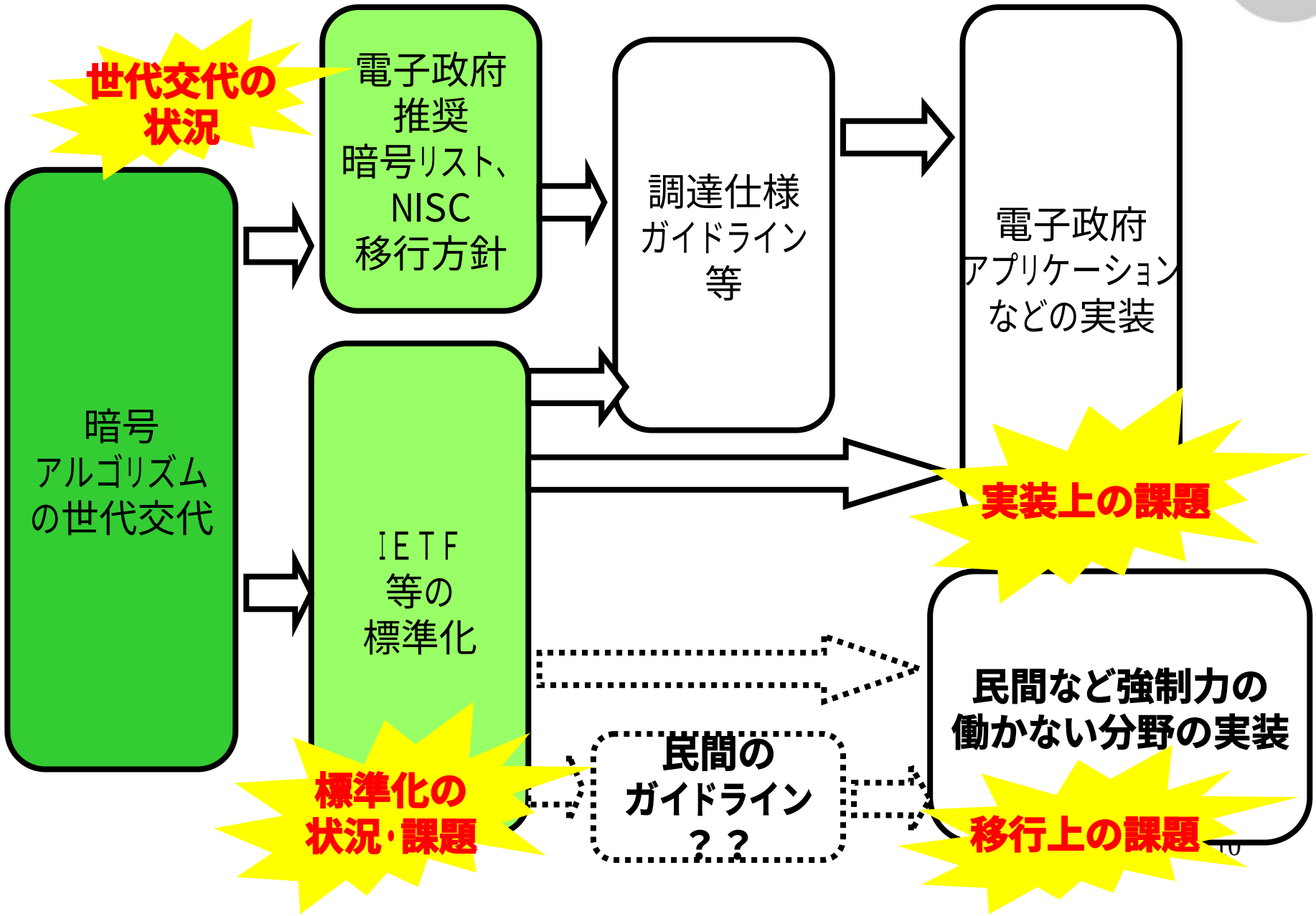
暗号アルゴリムの移行問題 パネラー

セコム IS 研究所
Intelligent Systems Laboratory

- 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 氏
  - CRYPTREC的立場??
- 富士ゼロックス株式会社　稲田 龍 氏
  - IETF標準化、実装、電子文書保存
- 松下電工株式会社　福田 尚弘 氏
  - 組み込み機器、セキュリティプロトコル
- 日本クロストラスト株式会社 代表取締役／日本電子認証協議会 代表理事　秋山卓司 氏
  - 身近な暗号＆PKIのSSL証明書

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



暗号アルゴリムの移行問題
お題目の予定。。。。（

セコム IS 研究所
Intelligent Systems Laboratory

- **どの位？危ないのか？**
- **移行は、どの位？大変なのか？**
- **デットロック問題は解決できるのか？**

参考

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
  - PKI day 2006
  - http://www.jnsa.org/seminar/2006/20060607/matsumoto_02.pdf
- 「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