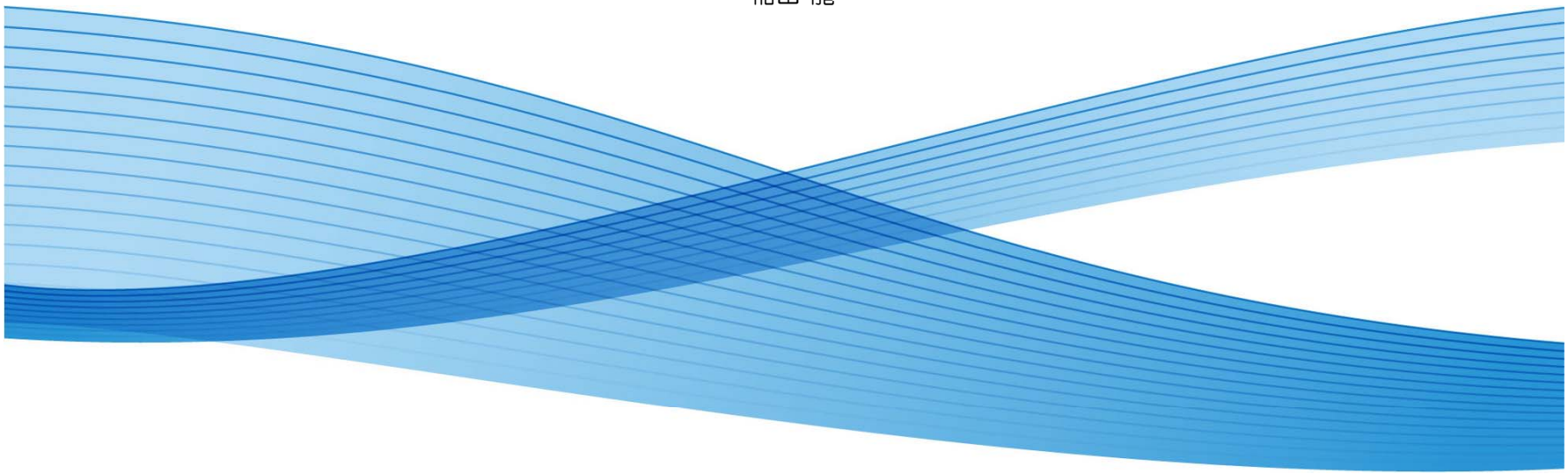
暗号アルゴリズム移行問題
もしくは
暗号の２０１０年問題への対応

富士ゼロックス株式会社
稲田 龍



FUJI Xerox

暗号の2010年問題

■ 暗号技術は、その**解析(解読)技術の進展およびコンピュータの計算能力の向上によって、時間と共に安全性が低下**する性質を持っている。
⇒ 攻撃に要する計算量に基づいた**「n ビット安全性」**として評価されている。

■ 近年の研究では、**RSA 1024やSHA-1(※)などの暗号技術は80ビット安全性以下で、2011年以降は十分な安全性の確保が難しいとの見方**が強まっている。
(※使用用途に拠り当面問題ない場合もある)

■ **今日直ちに実害ある攻撃が可能なわけではないが、2030年までの使用を想定した場合には112ビット安全性以上への移行が必要**と考えられている。

移行が必要

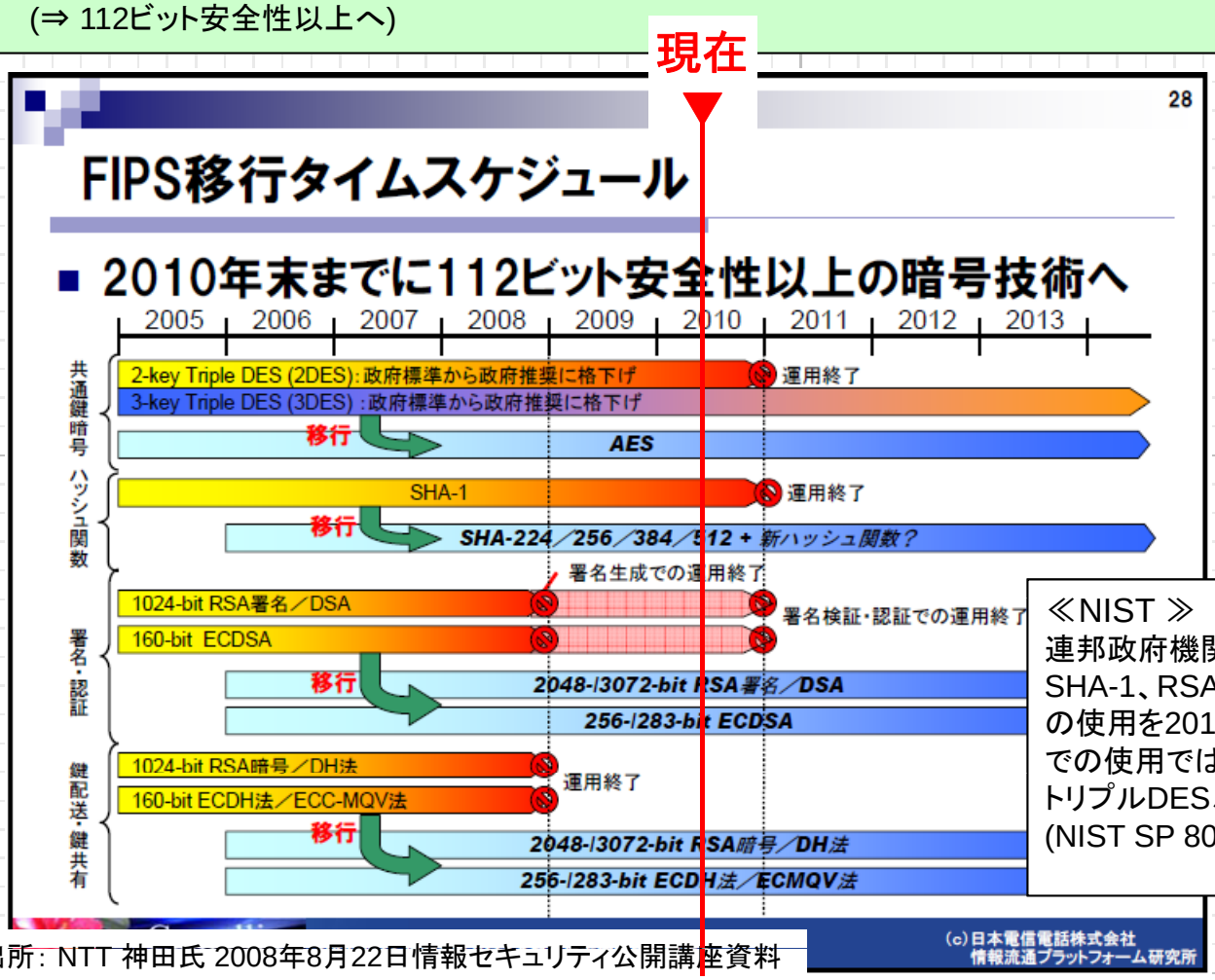
暗号技術 / n ビット安全性と使用推奨期間	共通鍵暗号（暗号化/MAC）	公開鍵暗号と鍵長			ハッシュ関数	
		素因数分解型（RSAなど）	離散対数型（DSAなど）	楕円曲線（ECDSAなど）	署名用途	HMAC/鍵生成/乱数生成用途
80ビット安全性 ～2010年	**2key-TDES**	**RSA 1024**	**DSA 1024**	**ECDSA 160-223**	**SHA-1（60ビット安全性に低下）**	
112ビット安全性 ～2030年	3key-TDES	RSA 2048	DSA 2048	ECDSA 224-255	SHA-224	SHA-1 (105-160)
128ビット安全性以上 2030年～	AES-128 AES-192 AES-256	RSA 3072	DSA 3072	ECDSA 256-384	SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512

※ ( )内はビット安全性。ハッシュ関数SHA-224以上を総称してSHA-2と呼んでいる。

FUJI Xerox

米国政府の対応状況

■ 米国は連邦政府機関情報システムにおいて、**より高い安全性を持つ暗号方式(SHA-2やRSA 2048以上など)への移行を既に開始、SHA-1やRSA 1024などの使用を2010年までに中止する。**
(⇒ 112ビット安全性以上へ)



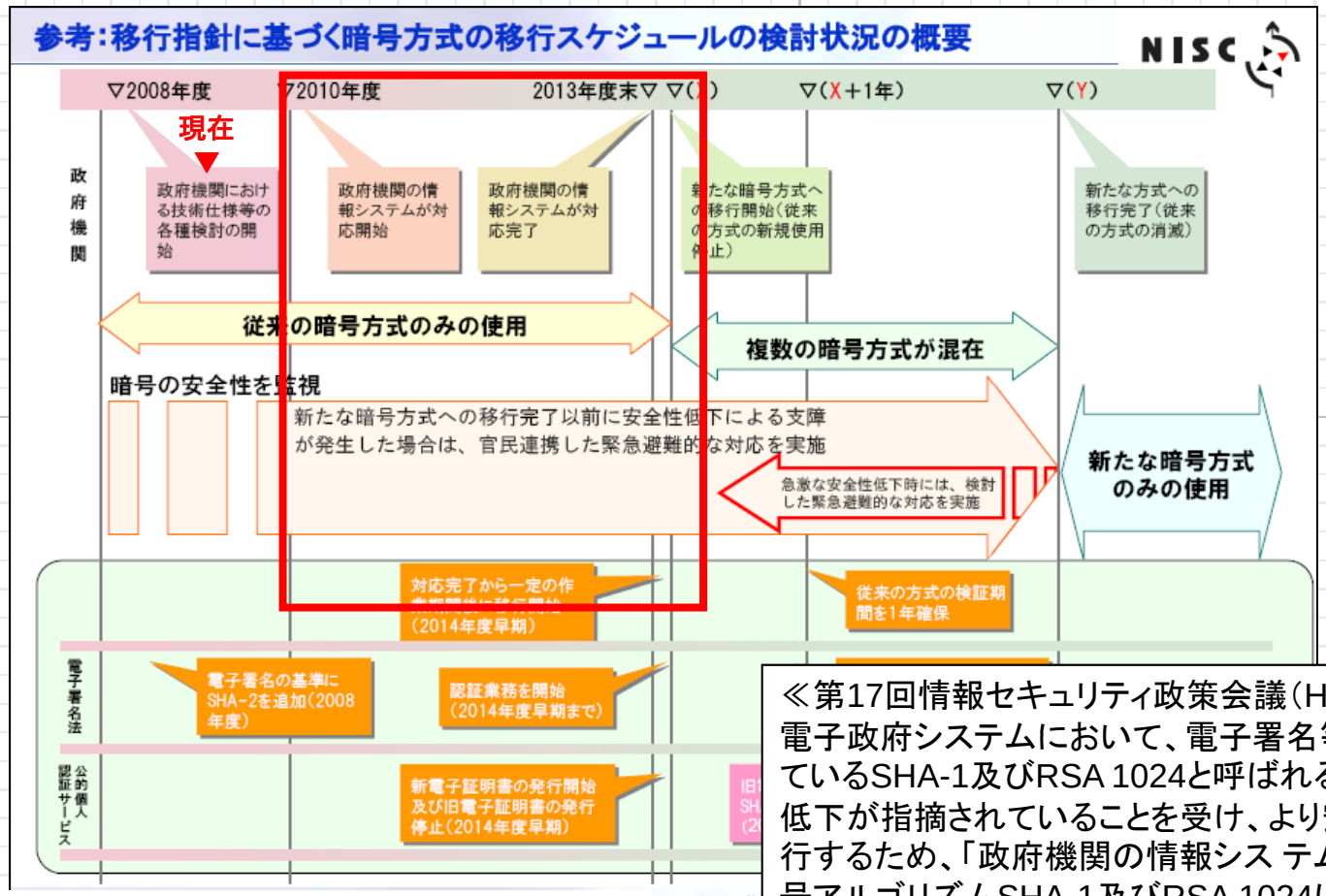
≪NIST ≫
連邦政府機関の情報セキュリティに係わり、SHA-1、RSA 1024および2-keyトリプルDESの使用を2010年までとすると共に、2030年までの使用ではSHA-2、RSA 2048以上、3-keyトリプルDES、AESなどを推奨する方針を発表(NIST SP 800-57(2005)、他)

出所：NTT 神田氏 2008年8月22日情報セキュリティ公開講座資料

FUJI Xerox

日本政府の対応状況（日本）

■ 日本は、政府機関情報システムで広く使用している暗号方式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**
(⇒ 112ビット安全性以上へ)



出所：内閣官房情報セキュリティセンター(NISC)作成資料

≪第17回情報セキュリティ政策会議（H20.4.22）≫
電子政府システムにおいて、電子署名等のために広く使用しているSHA-1及びRSA 1024と呼ばれる暗号方式 の安全性の低下が指摘されていることを受け、より安全な暗号方式への移行するため、「政府機関の情報シス テムに使用されている暗号アルゴリズムSHA-1及びRSA 1024に係る移行指針」を決定。

標準化などの対応状況

■ セキュリティ関連の標準化組織/関連機関では、暗号の脆弱性に対する認識が高まっており、標準の見直しを検討中。

■ **暗号アルゴリズムを応用する各種プロトコル標準化の方向性**

■ **1024bit以下のRSA暗号、2Key Triple DES、電子署名目的でのMD5/SHA-1の排除**

➢ 各種プロトコルを暗号アルゴリズムに依存しない形（必要に応じて別のアルゴリズムを選択することが可能）での標準化の議論が進んでいる他、ハッシュ関数SHA-1は利用方法に応じた延命策も議論されている。

➢ NSA
- ■ Suite-Bの制定

➢ NIST
- ■ FIPSの改訂
- ■ Hashコンテスト

➢ IETF
- ■ Security Area Directorが現IETF Chairに就任
- ■ Hashの使用に関しての全面的な見直し
  - ● RFC 4270 Attacks on Cryptographic Hashes in Internet Protocols. (P. Hoffman, B. Schneier. November 2005)
  - ● TLS/IPsecに関しての見直し作業

➢ CRYPTREC
- ■ 2006年より報告書内にてSHA-1の脆弱性に関しての記載あり

➢ JNSA
- ■ PKI相互運用技術WGでのサーベイ
- ■ PKI Day 2007/2008でのパネル討論
- ■ Security Day 2007/2008でのパネル討論

➢ JPNIC
- ■ Internet Week 2008にてパネルセッション：「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～」
- ■ 電子認証プラクティスフォーラムでの活動

➢ IPA
- ■ 情報セキュリティ分析ラボラトリー活動開始(2008年4月)

影響の範囲

主要なソフトウェアすべて(笑)

- ■Windows®オペレーティングシステムなどのOS
- ■アプリケーション
  - ●サーバー
  - ●クライアント
- ■組み込み機器
  - ●情報家電製品
  - ●自動車、コピー機
  - ●ATM/レジスター etc
- ■専用機器

主要なプロトコルの対応状況

証明書

■標準化

- IETF PKIX-WGなどで策定中

■実装

- 主要な実装では、対応済み

■運用

- 認証局の一部で証明書の発行を開始
- ICカードは利用可能なものも出始めてはいるが、大半はRSA 1024bit
- HSMも対応を開始

主要なプロトコルの対応状況

TLS(SSL)

- ■標準化
  - ●IETF TLS-WGで策定中
    - ■TLS 1.1で一部対応
    - ■TLS 1.2で完全に対応

      弱い暗号アルゴリズムの積極的な排除

      乱数発生機の更新
- ■実装
  - ●主要な実装サーバー・クライアントともに、対応済み
- ■運用
  - ● 対応可能
    - ■ 設定により「弱い」暗号で接続可能な設定になっている場合が多い

主要なプロトコルの対応状況

IPsec

- 標準化
  - IKEv2にて対応済み
    - RFC 4306

      TripleDES/AES-CBC/AES-CTR

      AES-128bit-XCBC
    - RFC 5282

      AES-GCM (Galois/Counter Mode)

      AES-CCM (AES in Counter with CBC-MAC Mode)
    - ただし、鍵交換に関してはD-H 768/1024
- 実装
  - 多くの実装では、固定の暗号アルゴリズムに決めうち。
  - 修正済みの実装も多いが、実勢としては状況不明
- 運用
  - 対応可能
    - ただし、弱い実装のままの運用している可能性も否定できない。
    - また設定により「弱い」暗号で接続可能な設定になっている場合が多い

組み込み機器の悩み

リソースが足りない

■コストの問題

- いや、厳しいんです(笑)

ネットワークにいつもつながっているわけではない

■更新が大変

- サポート要員がお客様のところに出向いて更新することもある

危殆化への対応

アルゴリズムの追加は難しい

■鍵長の変更は比較的楽

- 最終的にはリソースの問題なので、リソースさえ何とかすれば、単純なコスト計算で済む
  - ■RSA 1024bit以上にするのは比較的楽

    とはいえH/Wアクセレータとか搭載の場合は、泣く泣くアクセレータを使わない(!)とか選択を迫られる

とはいえ、新たな脆弱性への対応を考えると

■Secondary Cryptoが必要か?

課題

どの時期に対応すべきか?

■お客様は、「急に」対応を迫る

- いつ、お客様が「気にするようになるのか?」

どのくらいのコストなら許容されるか?

■コストがかかると対応が遅れる

- お客様にコストの負担がかかる
- 開発に時間がかかる

・タイムリーな提供には、ネットワーク経由での更新が有効だが……

■かならずしもネットワークにつながっているものだけではない


FUJI Xerox