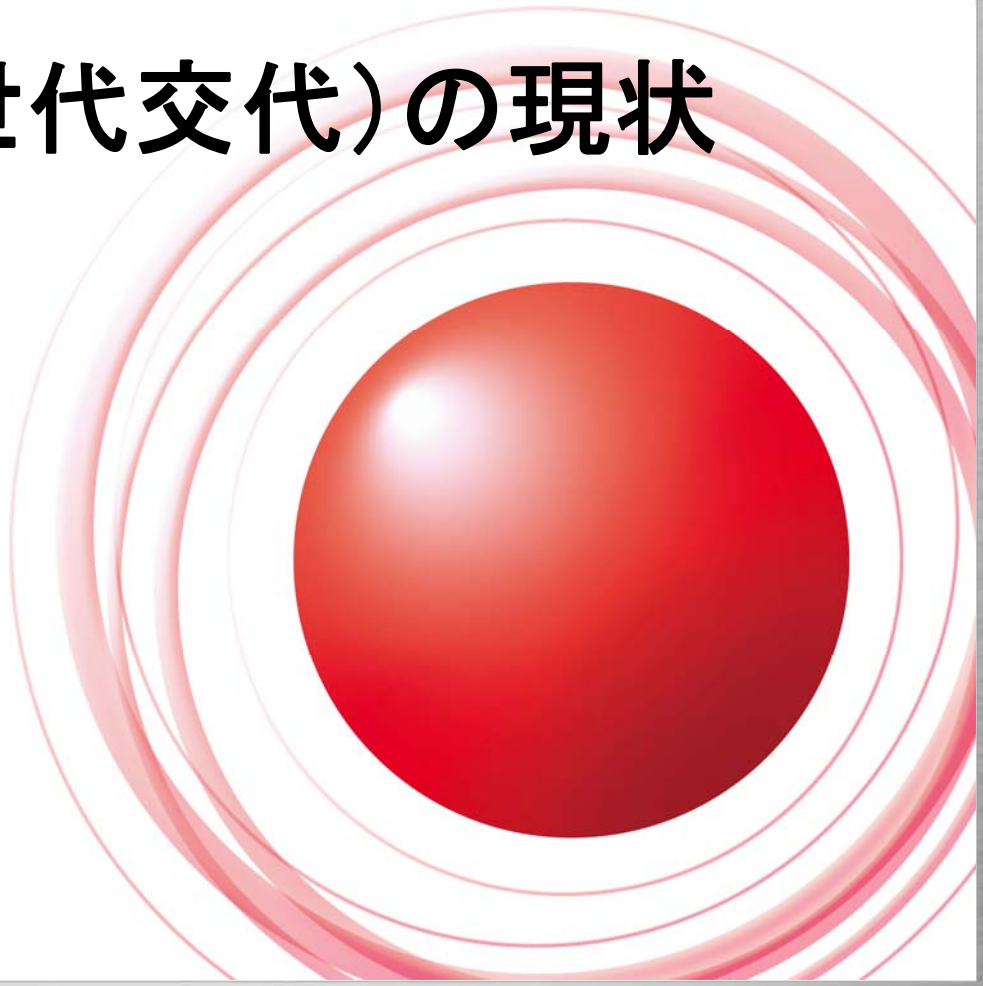
セキュリティ動向 2010 (1)
暗号2010年問題
（暗号世代交代）の現状

IIJ Internet Initiative Japan

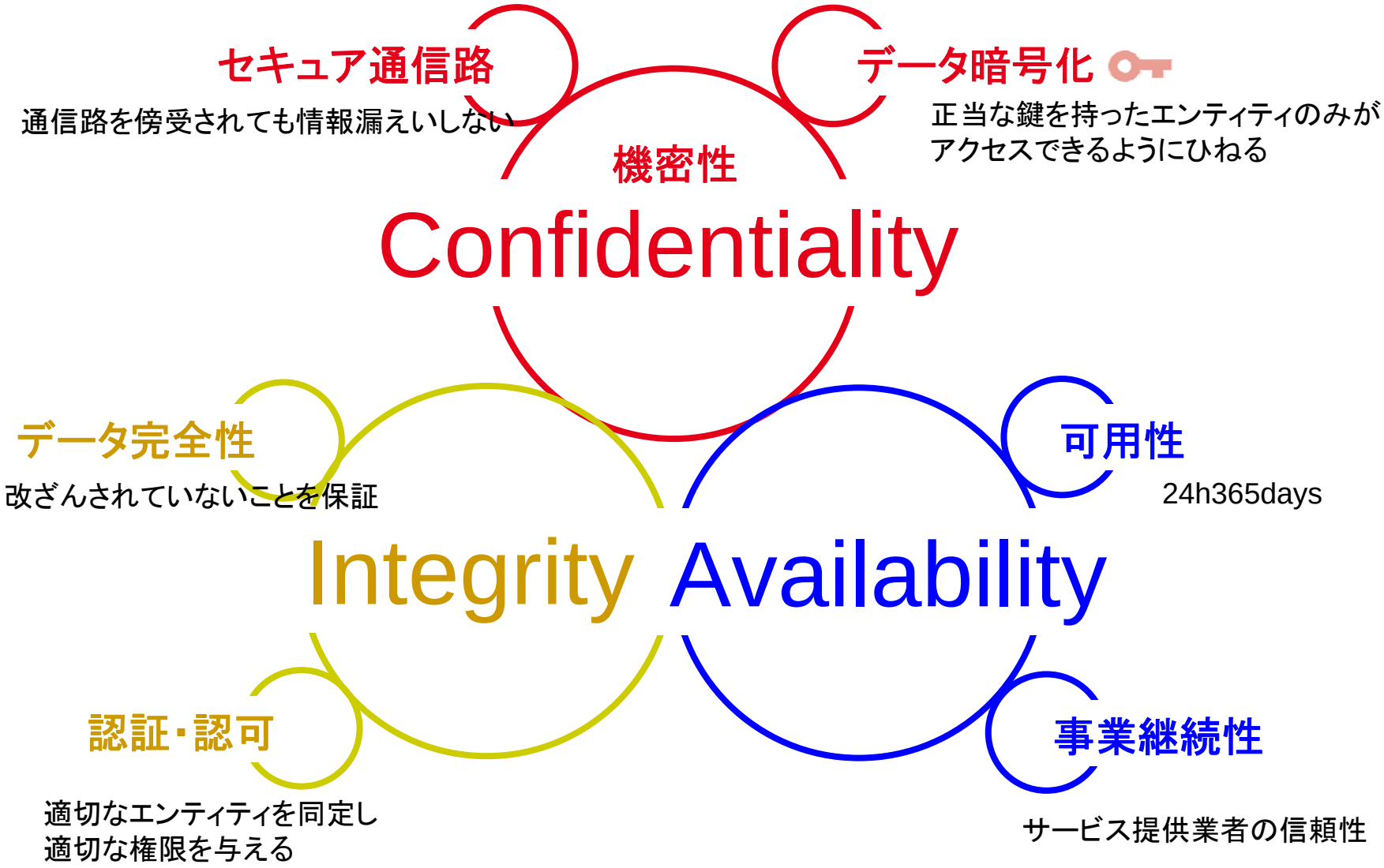


2010/11/19

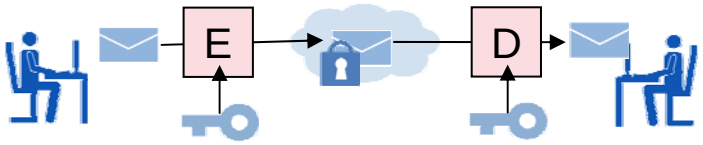
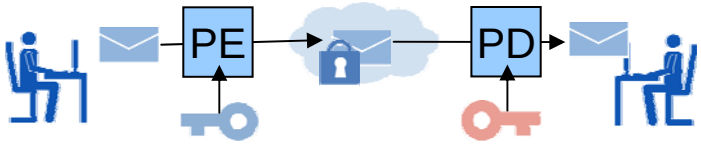
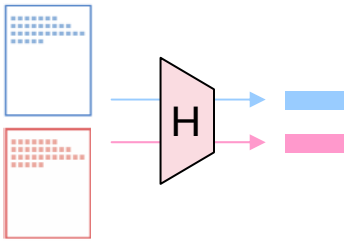
株式会社インターネットイニシアティブ
サービス本部 セキュリティ情報統括室
須賀 祐治

Ongoing Innovation

一般的なセキュリティ要件



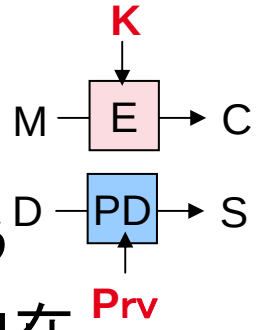
暗号アルゴリズムの分類

暗号プリミティブ	特徴・用途	アルゴリズム例
共通鍵暗号	暗号化と復号で同じ鍵を用いて秘匿 	ブロック暗号 AES, DES, Camellia ストリーム暗号 RC4, MUGI
公開鍵暗号 Confidentiality	対になる2つの鍵を用いて 守秘(暗号化)，署名，鍵共有 	素因数分解 RSA 離散対数 DSA，DH 楕円離散対数 ECDSA, ECDH
Integrity		
ハッシュ関数	衝突しない固定長データに圧縮  (デジタル署名 タイムスタンプ 等で利用)	専用(dedicated) 関数 MD5, SHA-1/SHA-256 ブロック暗号ベース ISO 10118-2

暗号アルゴリズムの危殆化

暗号アルゴリズムの危殆化

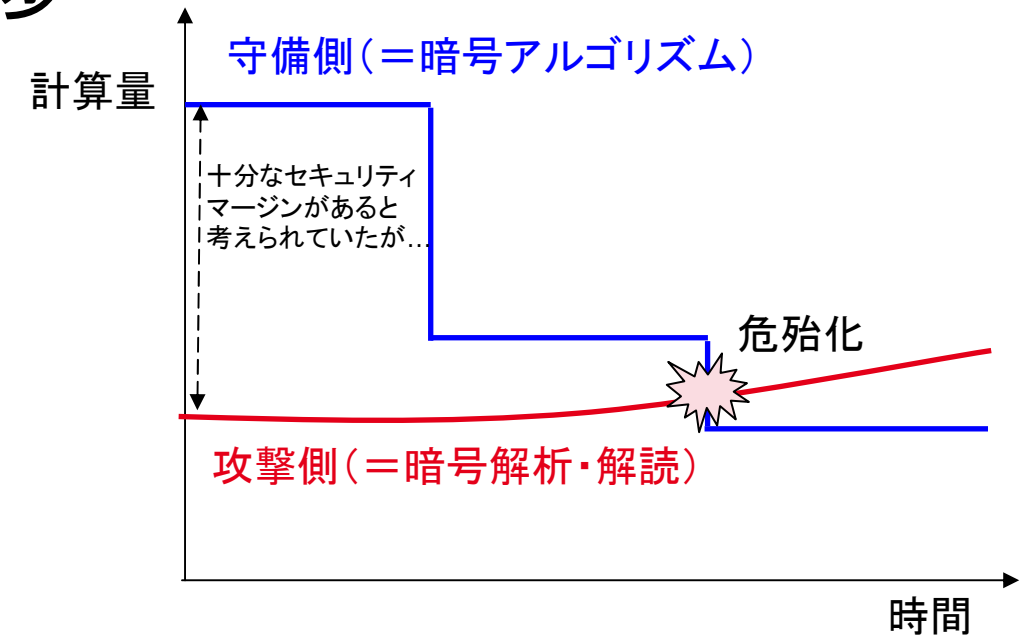
- 暗号アルゴリズム自体に欠陥が生じる問題
  - 当初想定したよりも低いコストで
    「セキュリティ上の性質」が確保できない状況
    - 機密性：暗号鍵が無くても 復号できてしまう
    - 完全性：秘密鍵が無くても デジタル署名が偽造できてしまう
  - 設計当時は安全と思われていたがアルゴリズムに内在していた欠陥が近年の暗号解析研究によって明らかに



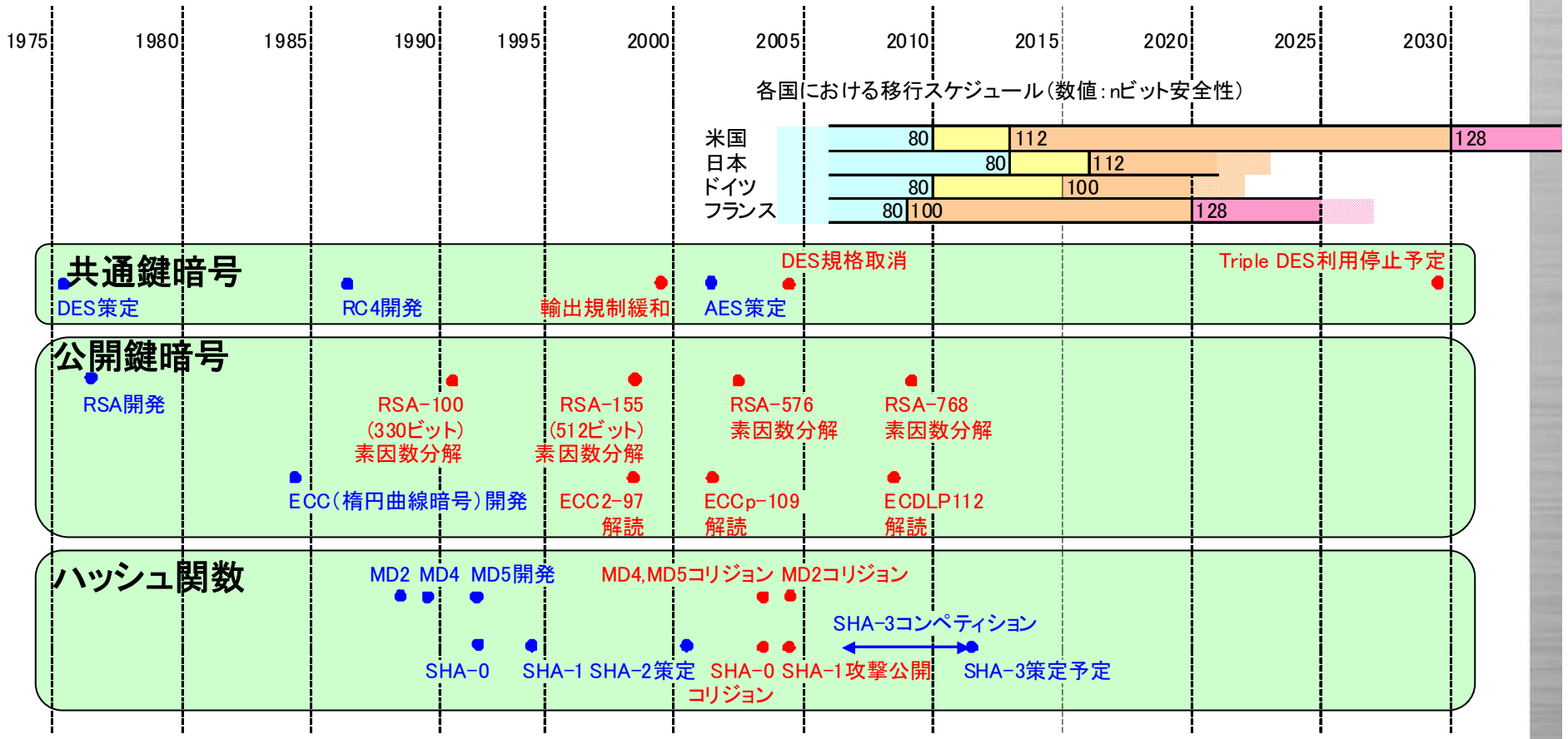
- 対処方法：暗号アルゴリズムを差し替える
  - 移行コスト，社会的インパクトが大きい
    - 1976年に策定されたDESはTriple DESとして
      現在も使われており米国では**2030年まで**利用を容認

暗号危殆化の要因

- 時間とともに緩やかに進行 ＝ 経年劣化
  - 計算機能力の向上：CPU性能の向上
  - 計算機モデルの変化：量子計算機の実現
- 急に進展することがあり得る
  - 暗号解析手法の進歩
    - nビット安全性の nが急激に低下



アルゴリズムの危殆化事例



青字：新しい暗号アルゴリズムの開発など安全性の向上要因　赤字：危殆化を促進する事件，暗号アルゴリズムの利用禁止

Internet Infrastructure Review vol.8 図9 - http://www.iij.ad.jp/development/iir/pdf/iir_vol08_infra.pdf

暗号2010年問題の発端

- NIST's Policy on Hash Functions March 15 2006
  - http://csrc.nist.gov/groups/ST/hash/policy.html

NIST'S POLICY ON HASH FUNCTIONS

March 15, 2006: ***The SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms.*** Federal agencies ***should*** stop using SHA-1 for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010. After 2010, Federal agencies may use SHA-1 only for the following applications: hash-based message authentication codes (HMACs); key derivation functions (KDFs); and random number generators (RNGs). Regardless of use, NIST encourages application and protocol designers to use the SHA-2 family of hash functions for all new applications and protocols.

- 2010年末をもってSHA-1の利用を停止し
  SHA-2へ全面移行する声明を発行
  - 背景：SHA-1を含む複数のアルゴリズムへの攻撃が公に
  - SHA-2 ファミリー：SHA-224/256/384/512

（アルゴリズム名の数値はそれぞれダイジェストの出力ビット長）

2030年末にもう一度起こる

- NIST Special Publication 800-57 Part 1
  Recommendation for Key Management
  - 2030年を越えればAESへ完全移行
    - 最低**128ビット安全性**を確保

アルゴリズム（と鍵長）から方式の安全性を数値で示す一方式

Table 4. Recommended algorithms and minimum key sizes

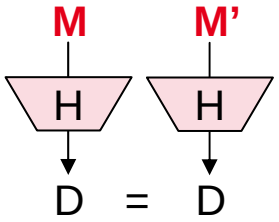
ライフタイム	n ビット 安全性	共通鍵暗号	公開鍵暗号 素因数分解	公開鍵暗号 楕円離散対数	
2010年まで	≧ 80	2TDES, 3TDES AES-128/192/256	1024	160	2010年問題
2030年まで	≧112	3TDES AES-128/192/256	2048	224	2030年問題
2031年以降	≧128	AES-128/192/256	3072	256	

http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

「困難さ」の表現方法

- 「セキュリティ上の性質」を危うくする（＝危殆化）ために実際に必要な計算量で表現
  - 共通鍵暗号：全数探索する際鍵空間の大きさ = 2^n
    - [n:共通鍵ビット長]
  - ハッシュ関数：一方向性 2^n，衝突困難性 $2^{n/2}$
    - [n:ハッシュ関数出力ビット長]

全ての鍵を総当りで試す



異なる入力に対し同じダイジェストを出力しない性質

- 上記の理論値を下回ると，本来持つはずの安全性を確保できないことを意味する

Triple DES は168ビット鍵暗号

  - 例：3-key TDESは本来 2^{168} の「困難さ」を持つべきだが暗号解析研究により 2^{112} まで落ちている
- 「nビット安全性」：攻撃に2^nの計算量が必要なとき
  - nを大きくすることは，安全性を向上させる大きな要因
    - 共通鍵暗号：鍵長を長くする / ハッシュ関数：出力ビット長を長くする
    - 一方で暗号処理に計算コストを要することになる

公開鍵暗号の等価安全性

- 公開鍵暗号を「nビット安全性」で表現する試み
  - 共通鍵暗号，ハッシュ関数と足並みを揃える必要があるため

nビット安全性	Lenstra (1999)	RSA Lab (2000)	Lenstra (2004)	NIST (2007)	ECRYPT2 (2010)	FUJITSU (2010)
56		430			640	
64	682		640		816	850
80	1513	760	1329	1024	1248	1219
112	4509		3154	2048	2432	2206
128	6669	1620	4440	3072	3248	2832
192				7680	7936	6281
256				15360	15424	11393

2010年問題

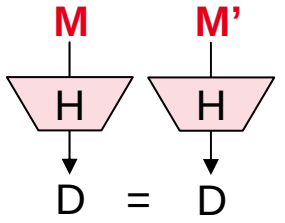
2030年問題

Internet Infrastructure Review vol.8 表1 - http://www.iij.ad.jp/development/iir/pdf/iir_vol08_infra.pdf

危殆化の影響

危殆化による直接的な影響

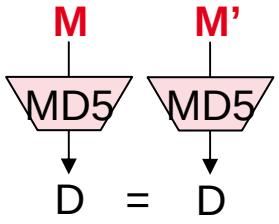
- 暗号化
  - 権限のないエンティティによる復号
- デジタル署名（MAC）
  - 権限のないエンティティによる署名（MAC）の偽造
- ハッシュ関数
  - 署名対象データのすり替えによる改ざん
  - タイムスタンプの証拠性が担保できない



アルゴリズムの移行で対処可能と認識されている

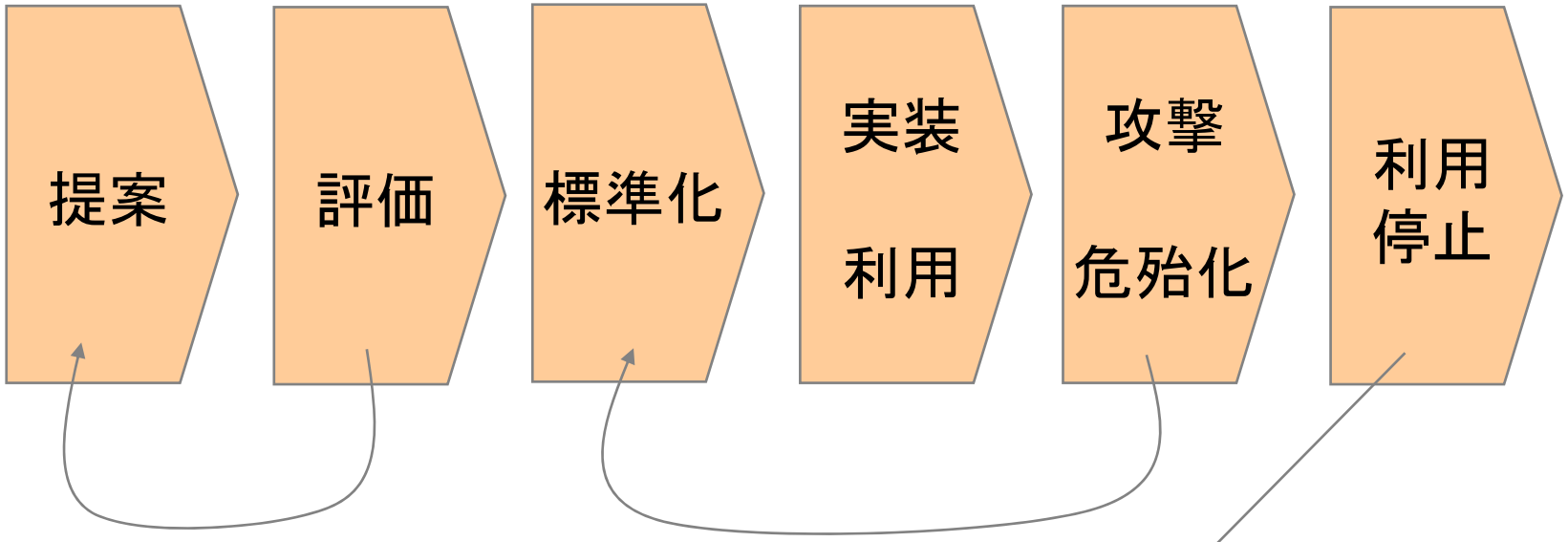
危殆化による間接的な影響

- APOP, SIP, HTTP Authentication における パスワードリカバリ攻撃
  - Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro, "Extended Password Recovery Attacks against APOP, SIP, and Digest Authentication," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E92-A, No. 1, pp. 96-104, 2009.
- X.509中間CA証明書偽造攻撃
  - MD5 considered harmful today
    - http://www.win.tue.nl/hashclash/rogue-ca/
- ともにMD5コリジョン攻撃を利用

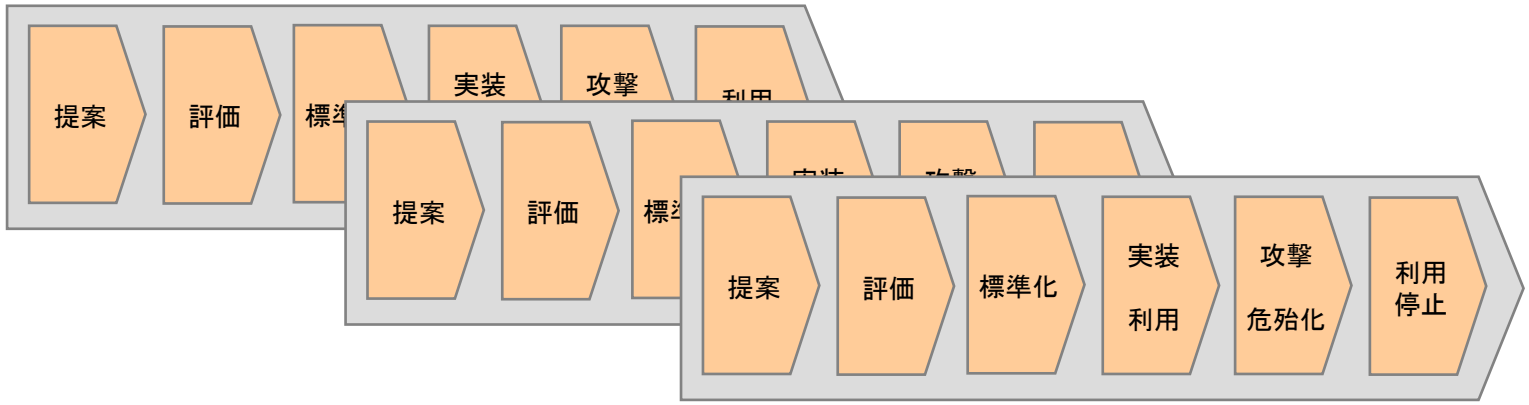


移行に対する考え方

暗号アルゴリズムのサイクル



暗号アルゴリズムは完全なものではなくどこかのタイミングで捨てて
今後も新しいものに移行し続けないといけない



日本政府系システム 移行状況

- 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/conference/seisaku/dai17/pdf/17siryou0102.pdf
  - 情報セキュリティ政策会議第17回会合（2008年4月22日）で承認
  - 同20回会合(2009年2月3日) 検討状況公表
    - 最短で2014年度早期にSHA-2利用開始予定
    - 最短で2017年度早期にSHA-1，RSA-1024利用停止予定
      - 複数の暗号方式が混在する期間も想定

NISC：内閣官房情報セキュリティセンター

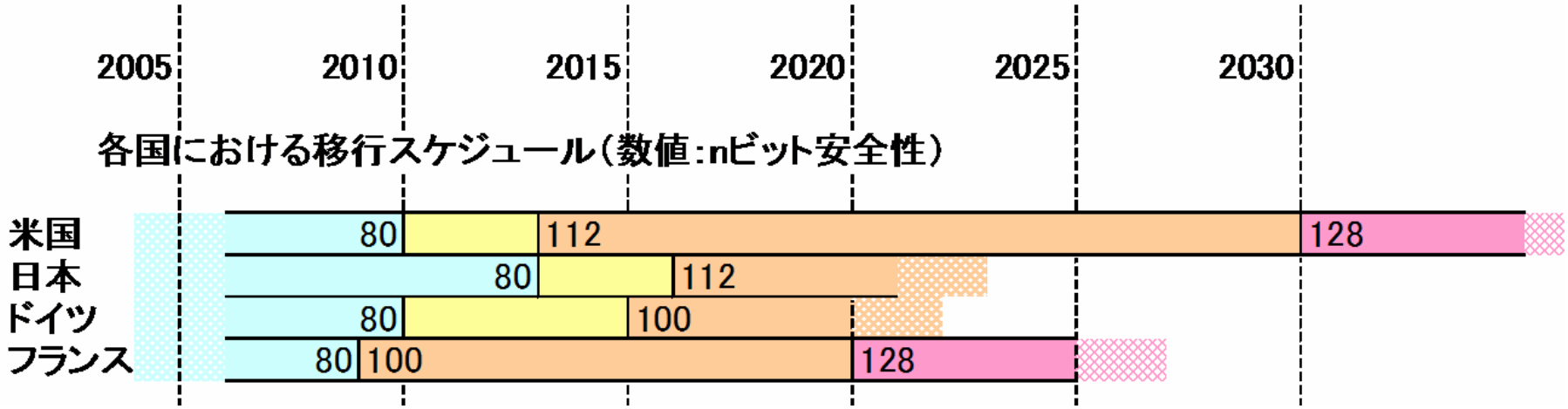
電子政府推奨暗号リスト 改訂状況

- CRYPTREC
  - Cryptography Research and Evaluation Committees
  - 電子政府推奨暗号の安全性を評価・監視し，暗号モジュール評価基準等の策定を検討するプロジェクト
    - 総務省及び経済産業省が共同で運営
- 電子政府推奨暗号リスト
  - 電子政府システムに適用可能な暗号技術を公募
  - 電子政府に利用可能な暗号技術を提示
- 2002年度版リスト を策定済
  - http://www.cryptrec.go.jp/list.html
- 現在2013年度版リストを改訂中
  - 2009年10月に改訂のための暗号技術公募開始(応募締切済)

米国での制限緩和状況

- NIST SP800-113（SP800-57 を改訂予定）
  - DRAFT Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes
    - http://csrc.nist.gov/publications/drafts/800-131/draft-sp800-131_spd-june2010.pdf
- **3年の猶予期間**を置く
  - 2013年末までは “Deprecated” という状態で継続利用可
    - 利用者はリスクを理解し，このリスクを許容すること
    - 理解できないのであれば利用しないこと
  - 猶予期間は 2-key Triple DESのみ5年
  - 署名検証のためのレガシー利用時も5年猶予あり

参考：各国の移行スケジュール



Internet Infrastructure Review vol.8 図9 - http://www.iij.ad.jp/development/iir/pdf/iir_vol08_infra.pdf

各業界での動き

- CA/Browser Forum：EV証明書
  - 有効期限が2011年以降となる公開鍵証明書は
    RSA-1024は利用できずRSA-2048に制限
  - ハッシュ関数：SHA-256以降のアルゴリズムが推奨
    - SHA-2ファミリーがブラウザに搭載されるまでの期間
      のみSHA-1の利用可能
- タイムビジネス認定センター
  - 2012年3月末までにSHA-2およびRSA-2048へ移行する方針
- PKIベンダー
  - A社：10月以降基本RSA-2048のみ発行という方針（2010年1月）
    - SP800-131ドラフト発行後に撤回
      有効期間が2013年12月31日を超えないケースではRSA-1024対応可能
- 携帯電話ベンダー
  - ソフトウエア更新を随時行う

まとめ

- 暗号の危殆化は経年変化だけでなく期せずして起こる
  - 暗号アルゴリズムの強度を(「nビット安全性」で)数値化して判断
- 暗号危殆化は通信プロトコル・フォーマットへも影響する
  - 影響範囲は大きく，移行に時間がかかる
- 新方式への移行と旧方式の廃棄の両方への考慮が必要
  - 暗号アルゴリズムは完全なものではない
  - どこかのタイミングで捨てて
    今後も新しいものに移行し続けねばならない
- 2010年末までに急な対策が必要な状況ではないが
  リスクを把握した上で速やかな計画を策定すべき

補足:さらに詳しく知りたい方々へ

- 情報処理学会 第73回全国大会 http://www.ipsj.or.jp/10jigyo/taikai/73kai/
  - 2011年3月3日 9:30～12:00（東京工業大学 大岡山キャンパス）
  - パネルディスカッション
    「RSA-1024はもう危険なのか？暗号2010年問題を正しく理解する」

「暗号世代交代の本質と課題」	神田雅透（IPA）
「RSA暗号危殆化曲線について」	猪俣敦夫（NAIST）
「ハッシュ関数の標準化動向」	渡辺大（日立製作所）
「政府機関の情報システムにおけるSHA-1及びRSA1024の移行状況」	山口理恵（NISC/AIST）
「認証局運用の観点でみる暗号アルゴリズムの移行」	木村泰司（JPNIC）
「社会基盤化しつつある暗号技術」	松本泰（セコム）
司会・進行	須賀祐治（IIJ）

- 電子情報通信学会 学会誌 H23年11月号
  - 暗号世代交代に関する特集号を企画中

IIJ Internet Initiative Japan

ご清聴ありがとうございました

お問い合わせ先　IIJインフォメーションセンター
TEL：03-5205-4466（9：30～17：30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/

Ongoing Innovation