# 政府機関及び金融機関のSSLサーバ暗号設定に関する調査結果について

NTT情報流通プラットフォーム研究所
情報セキュリティプロジェクト
神田　雅透


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 本日の目次

## PKI Dayということで、PKIに関連しそうな暗号の話から

- **【政策】GPKI・公的個人認証での暗号移行**
  - 「暗号2010年問題」「暗号世代交代」のおさらい
- **【技術】MD5中間CA偽造攻撃**
  - SHA-1以前にMD5をどうしましょうか
- **【運用】政府・金融機関のSSLサーバ暗号設定調査結果**
  - 教訓：運用にも注意しましょうね

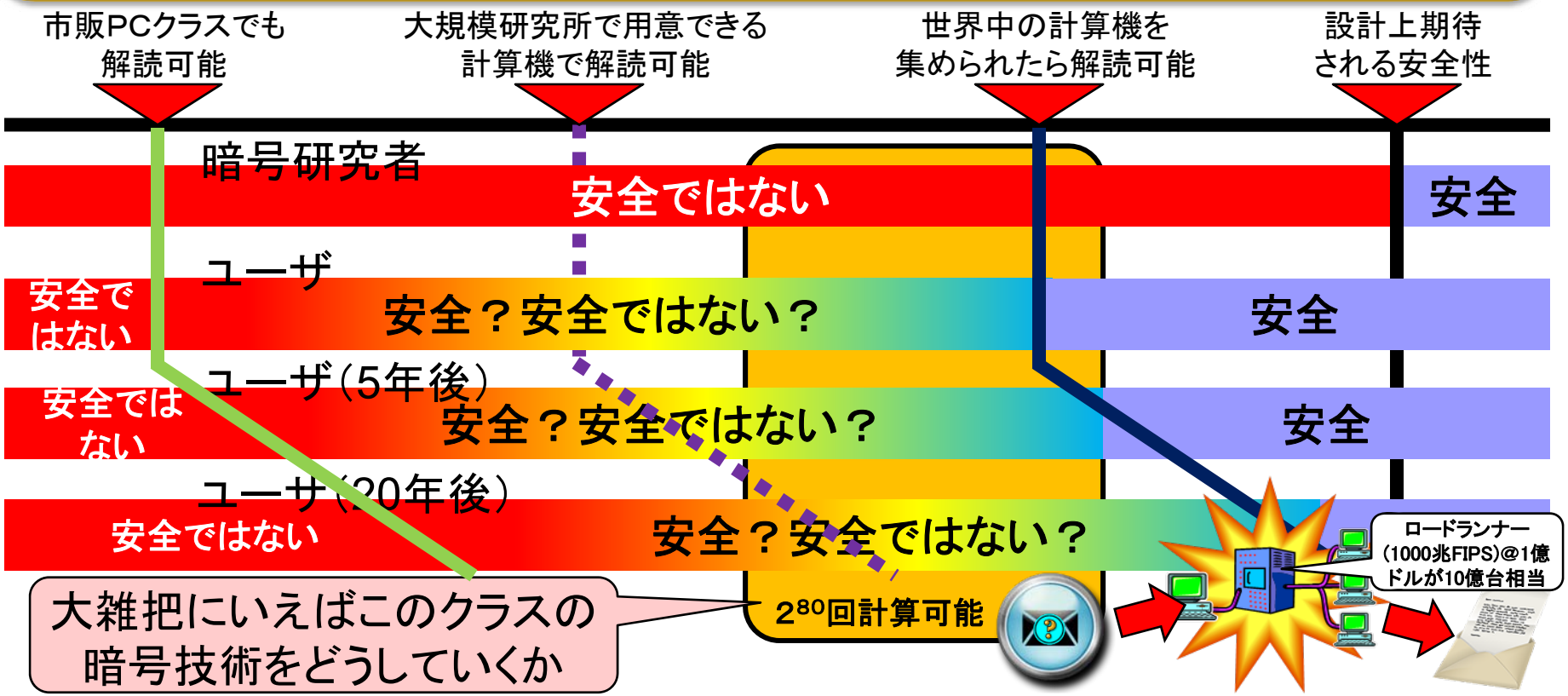

(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 政策的に・・・
# GPKI・公的個人認証での暗号移行など


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 「2010年問題」「世代交代」、一言でいえば・・・・

**多くのシステムで利用されている**
**様々な暗号の安全性低下が無視できなくなってきた**
**～解読技術の改良を考慮しておおむね1年で2倍の攻撃能力に～**



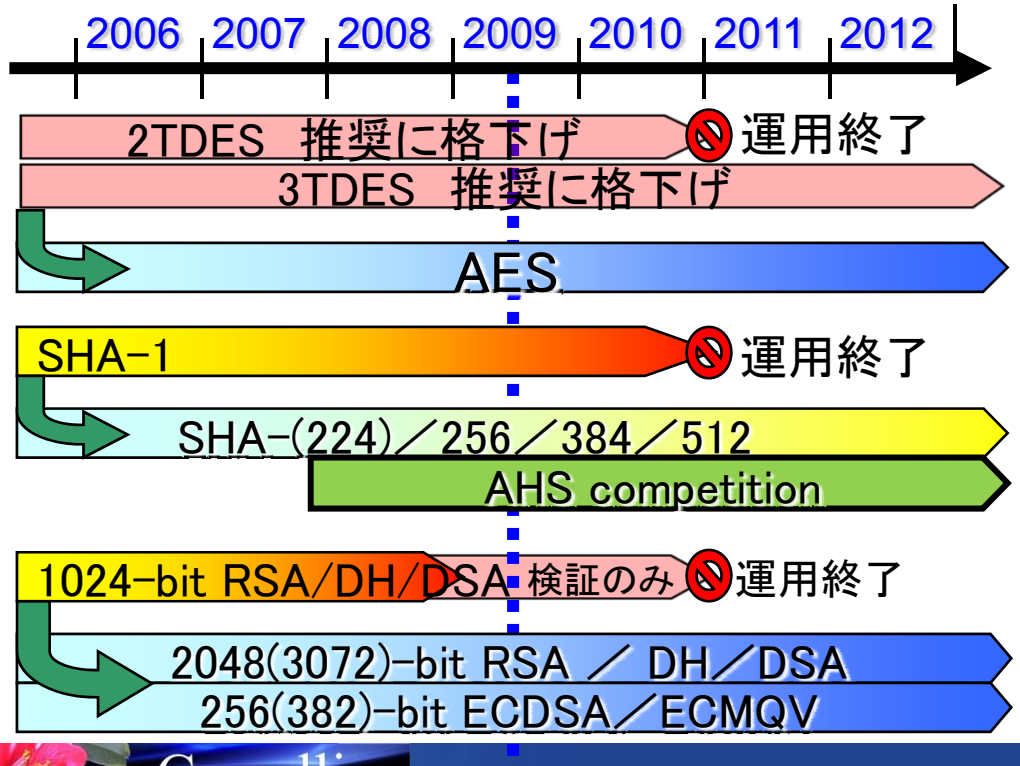


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 米国政府の暗号世代交代指針

- **政府機関の情報セキュリティ施策遂行権限をNISTに法的付与**
  - FISMA (Federal Information Security Management Act of 2002)
  - Executive Order #13011

**～デファクトとしての米国政府標準暗号の交代～**




- **NSAが国家安全保障システムで利用する暗号を規定**

**NSA Suite B Cryptography**

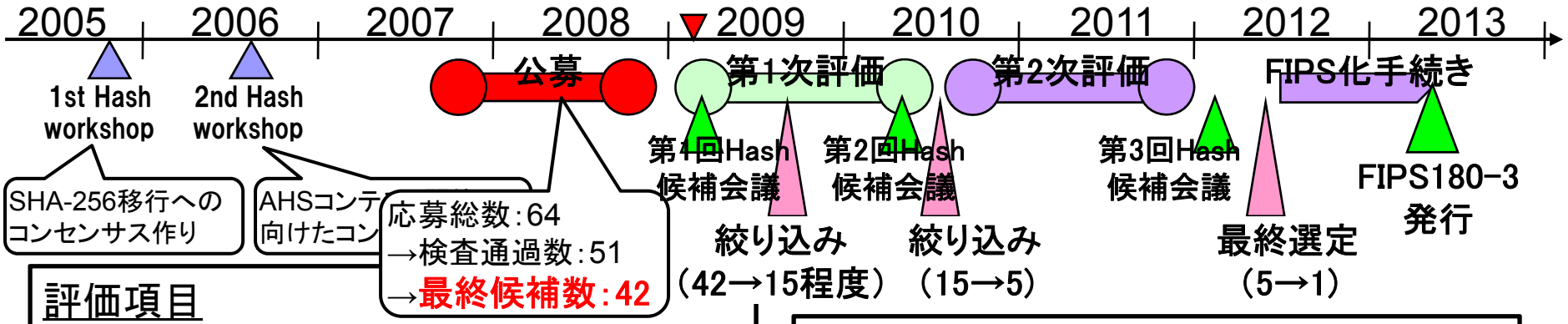
- 暗号化：AES（鍵長128ビット及び256ビット）
- 署名:ECDSA（256ビット素体及び384ビット素体）
- 鍵交換：ECDHまたはECMQV（256ビット素体及び384ビット素体）
- ハッシュ関数：SHA-256及びSHA-384

ECDSAとECMQVを指定したため、NSAはCerticomから26個の特許を購入し、米国政府向けシステム用に無償ツールキットを提供


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# Advanced Hash Standard (AHS) - SHA-3

- SHA-2に替わる(追加する)高度標準ハッシュ関数
  - ハッシュ長はSHA-2と同じ(224, 256, 384, 512ビット)
  - ロイヤリティフリー、知財権の制約なしで利用可能
  - 安全性・性能がSHA-2よりも本質的に優れている
    - SHA-2と同等以上の安全性で性能がすごく優れている
    - SHA-2に有効な攻撃手法が適用困難




評価項目
1. Security (Security important factors)
2. Cost (Efficiency, Memory requirement)
3. Characteristics (Flexibility, Simplicity)

代表的な設計方針の傾向
1. ブロック暗号の設計方針を踏襲
2. スポンジ関数の設計方針を採用


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 推奨公開鍵長の比較

| 利用期間の目安 | | 短期保護 | 中期間保護 | | 長期間保護 | | |
|---|---|---|---|---|---|---|---|
| | | - 2010 | - 2020 | - 2030 | 2030 + | 2030 ++ | 2030 +++ |
| 等価安全性（＝共通鍵暗号の安全性） | | 80 | 100 | 112 | 128 | 192 | 256 |
| RSA | NIST | 1024 | | 2048 | 3072 | 7680 | 15360 |
| | DCSSI | 1536 | 2048 | | 4096 | | |
| | ECRYPT | 1248 | 1776 | 2432 | 3248 | | 15424 |
| | BSI | 1728 | 2048 | | | | |
| | EMVCo | 1024 | 1984 | | | | |
| DSA | NIST | 1024/160 | | 2048/224 | 3072/256 | 7680/384 | 15360/512 |
| | DCSSI | 1536/160 | 2048/256 | | 4096/256 | | 15424/512 |
| | ECRYPT | 1248/160 | 1776/192 | 2432/224 | 3248/256 | | |
| | BSI | 2048/224 | 2048/224 | | | | |
| ECC | NIST | 160 | | 224 | 256 | 384 | 512 |
| | NSA Suite B | | | | 256 | 384 | |
| | DCSSI | 160 | 256 | | 256 | | |
| | ECRYPT | 160 | 192 | 224 | 256 | | 512 |
| | BSI | 224 | 224 | | | | |

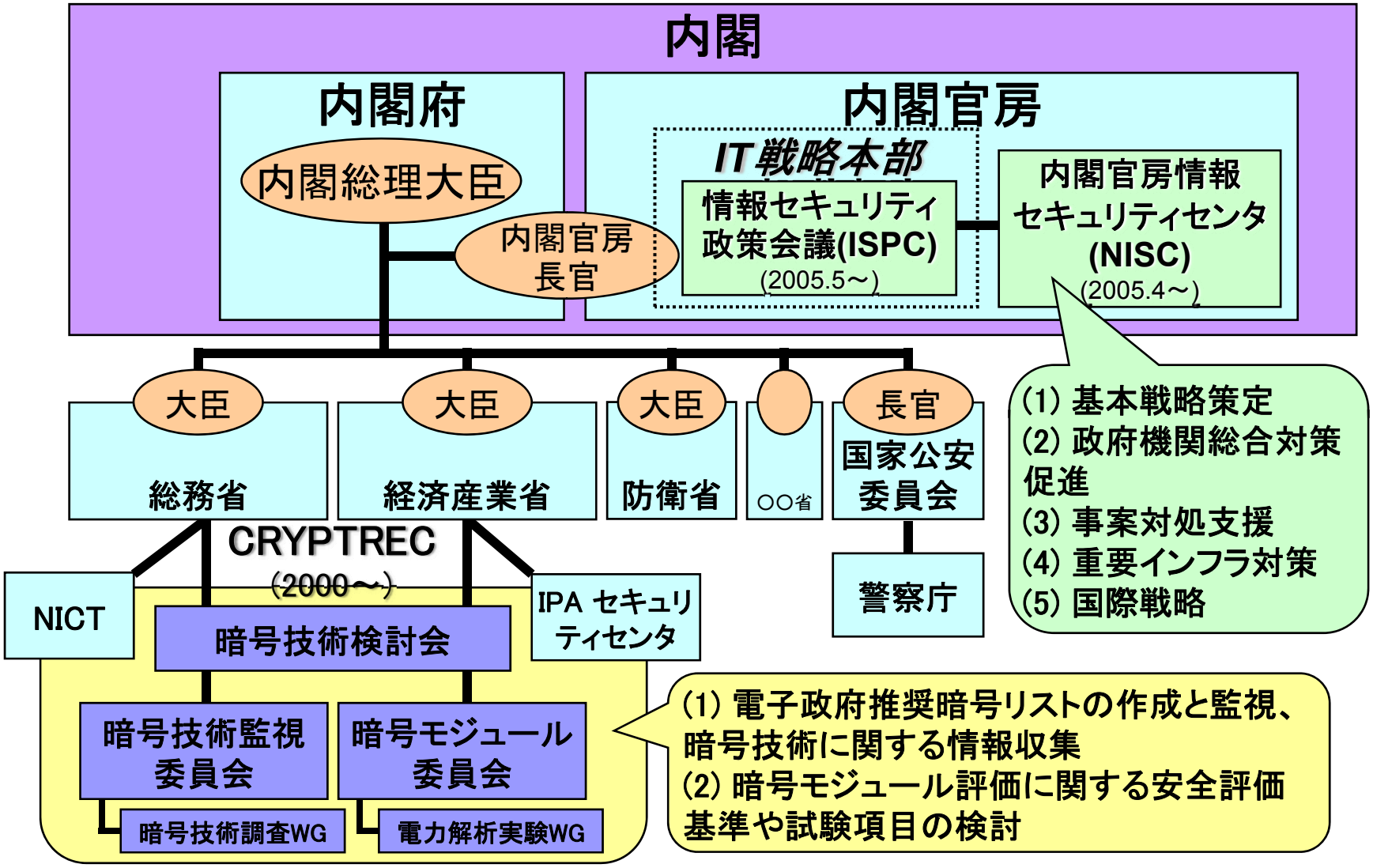

(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 技術面からの暗号世代交代について

- **共通鍵暗号は「より安全で、より処理性能が高い新しいアルゴリズムへ」**
  - 64ビットブロック暗号（Triple DES, MISTY1など）から128ビットブロック暗号（AES, Camelliaなど）への移行で問題なし
- **公開鍵暗号は「より安全にするために鍵長をより長く」**
  - PKIインフラが必要な場所ではRSAの優位性は揺るがず
  - 楕円暗号は個別システムから導入が進むと予想
- **ハッシュ関数は「緊急避難的にとりあえずSHA-2へ」**
  - SHA-1取扱いについて公式アナウンス（@'06/3/15）
    - デジタル署名／タイムスタンプサービス等で利用：速やかに移行
    - 2010年以降もSHA-1が利用可能：鍵導出・HMAC・擬似乱数生成
  - SHA-3(AHS)が市場に出てくるのは早くても2015年以降の話


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

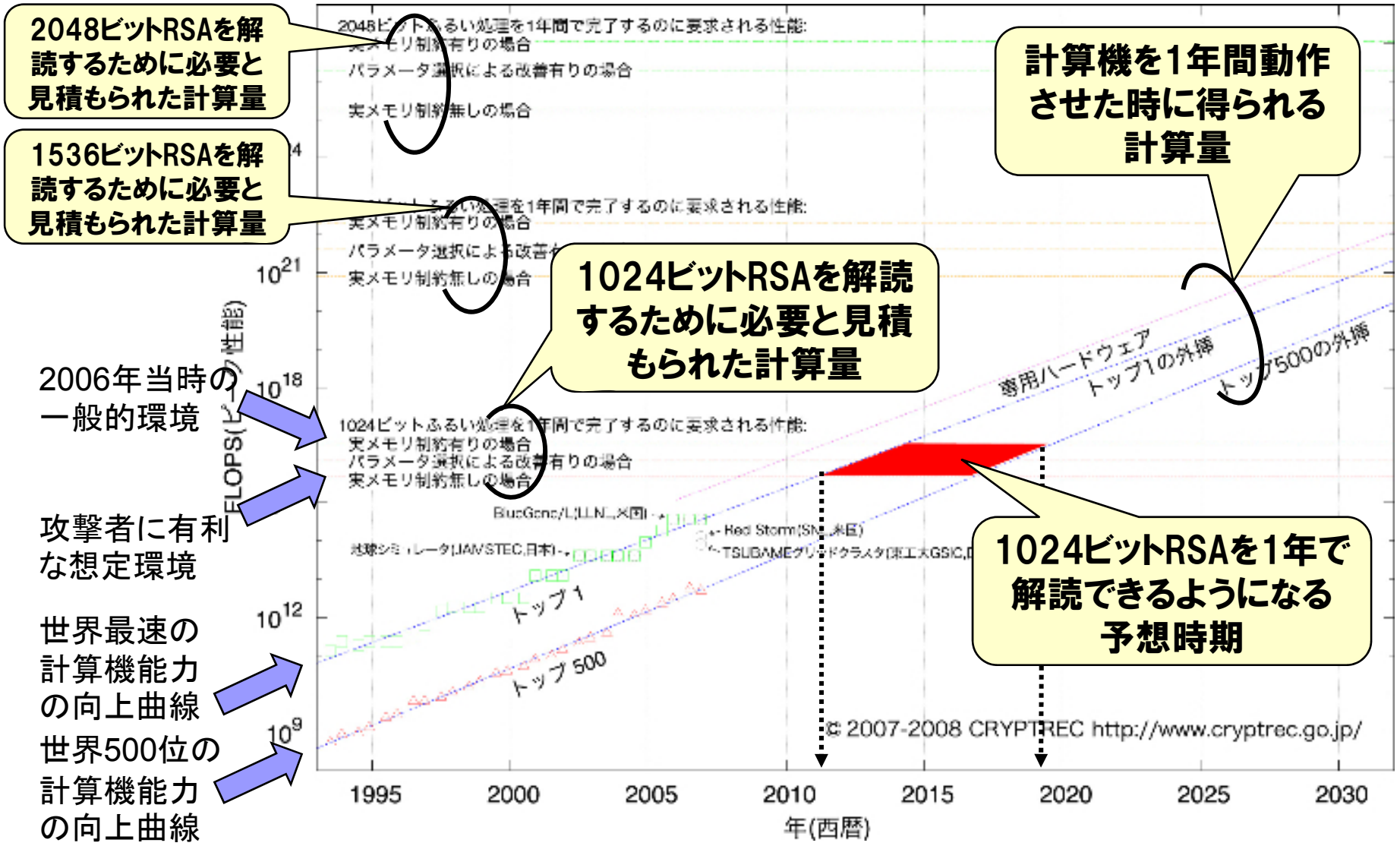
# 日本政府の暗号政策への取り組み体制



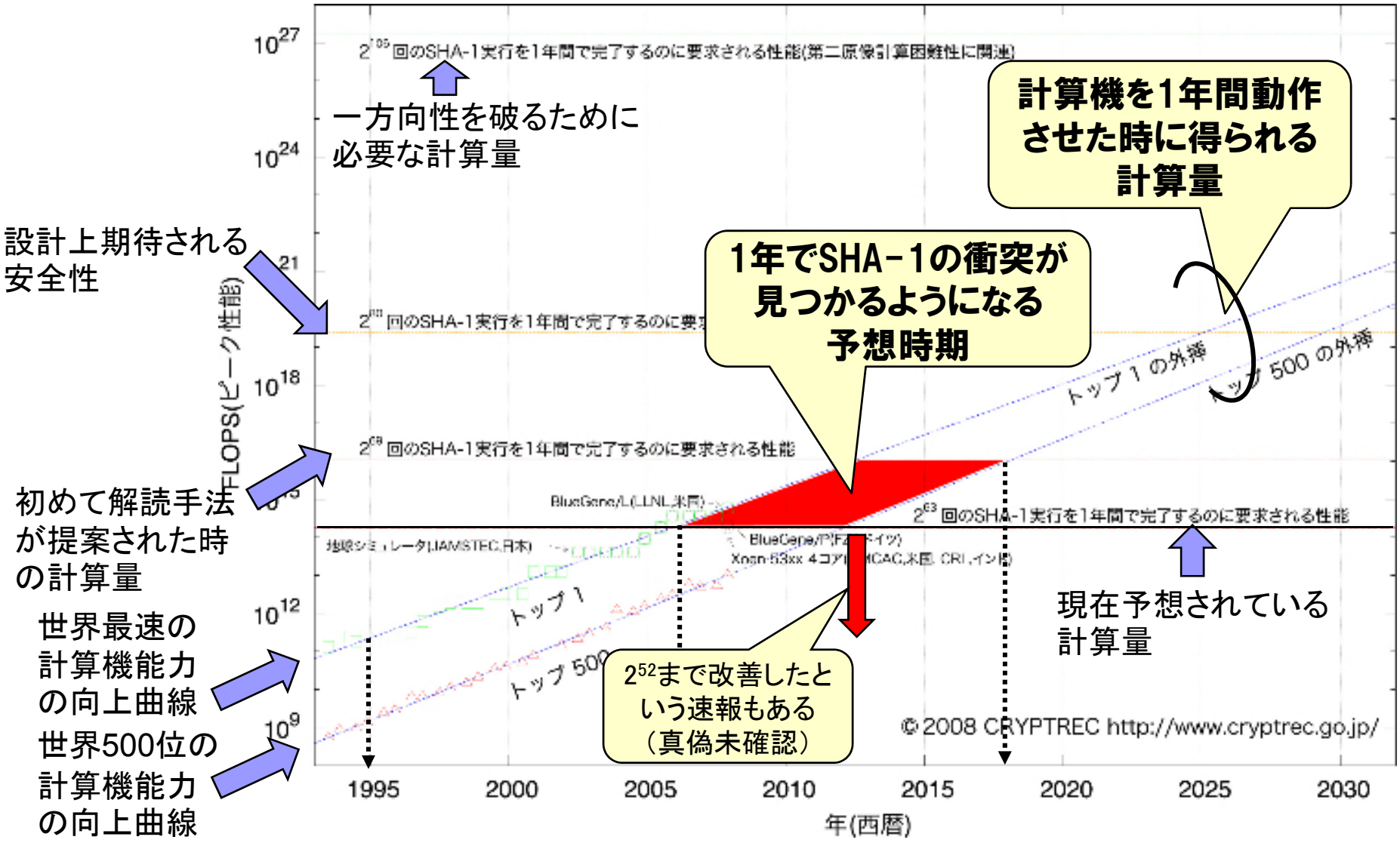


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# CRYPTRECによるRSA暗号安全性の見積もり

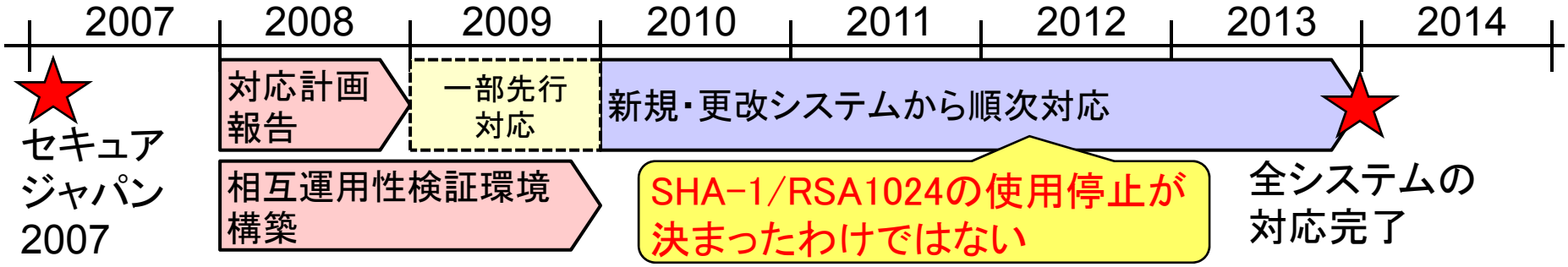


# CRYPTRECによるSHA-1安全性の見積もり



# 移行指針@情報セキュリティ政策会議(08.4.22)

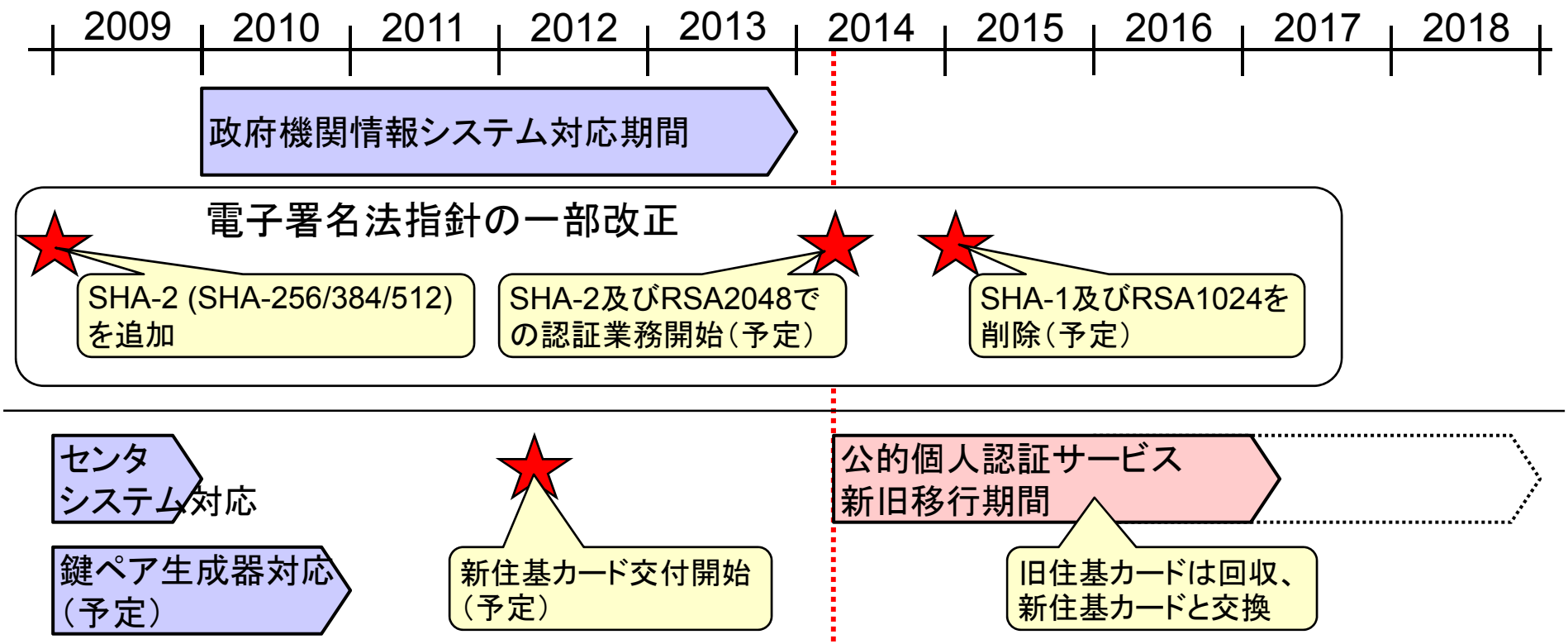
## 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」




| システム | 政府認証基盤(GPKI)及び商業登記認証局 | 政府認証基盤に依存する情報システム | その他の情報システム |
|---|---|---|---|
| 構成要件 | 電子証明書の発行・検証に使用する暗号を複数の中から選択可能とする構成 | 文書ファイルへの電子署名・検証に使用する暗号を複数の中から選択可能とする構成 | 別の暗号への変更が速やかに対応できる措置を事前に用意 |
| 用意するアルゴリズム | ■ RSA2048withSHA-1およびRSA2048withSHA-256を含める<br>■ エンドユーザ向けはRSA1024とRSA2048を含める | SHA-1およびSHA-256、RSA1024およびRSA2048を含める | 複数の暗号を導入する際は、SHA-256相当以上、RSA1152相当以上のものを含める |
| その他の要件 | ■ 電子証明書の発行では特定時期に切替可能とする<br>■ 検証では開始・終了時期を設定可能 | 開始・終了時期を設定可能にする | RSA1024withSHA-1以外があるときは原則そちらを利用し、必要なときのみRSA1024withSHA-1を利用可能とする構造 |
| | 緊急避難的に、電子証明書の失効・再発行等を行うことで、業務継続性が確保される構造 | | |


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 公的個人認証サービスにおける移行スケジュール




| | |
|---|---|
| 2014年度早期 | RSA2048withSHA-256による電子証明書の発行を開始<br>RSA1024withSHA-1による電子証明書の発行停止 |
| 2017年度早期（電子証明書の有効期間が延長された場合は2019年度早期） | RSA1024withSHA-1による電子証明書の有効期限終了後に、SHA-1及びRSA1024による認証業務を停止 |

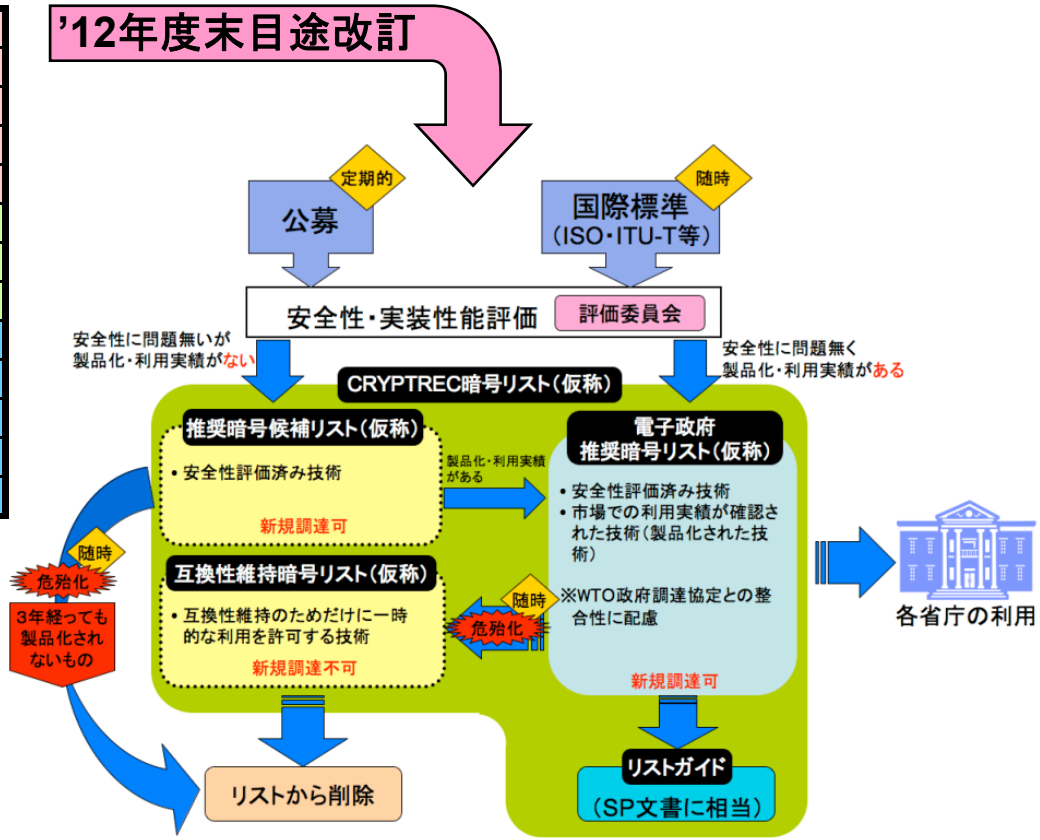

(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# その他の暗号に関する日本政府の動き

- 電子政府推奨暗号リスト(「各府省の情報システム調達における暗号の利用方針」了承)の改訂に向けた活動

現行電子政府推奨暗号リスト(2003.2.20)

| | | | |
|---|---|---|---|
| 署名 | DSA | 128ビットブロック暗号 | AES |
| | ECDSA | | Camellia |
| | PSASSA PKCS#1 v1.5 | | CIPHERUNICORN-A |
| | RSA-PSS | | Hierocrypt-3 |
| 守秘 | RSA-OAEP | | SC2000 |
| | RSAES PKCS#1 v1.5 | ストリーム暗号 | MUGI |
| 鍵共有 | DH | | MULTI-S01 |
| | ECDH | | 128-bit RC4 |
| | PSEC-KEM | ハッシュ関数 | RIPEMD-160 |
| 64ビットブロック暗号 | CIPHERUNICORN-E | | SHA-1 |
| | Hierocrypt-L1 | | SHA-256 |
| | MISTY1 | | SHA-384 |
| | 3-key Triple DES | | SHA-512 |





(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 他機関での暗号世代交代に向けて

- IETF
  - 2005/11 IETF会合でSHA-2への対処を求めるディレクタ指示発令。各WGにて、SHA-2について利用可能とするような仕様変更を2006年頃から審議
  - おおむね今年度中には仕様化終了。相互接続試験を経て、2011年以降の本格的普及には間に合う見込み
- PKI
  - 主要CA（日本ベリサイン、日本サイバートラスト等）が電子証明書で利用するハッシュ関数として、
    - SHA-256への対応を開始
    - MD5を使う電子証明書の発行を停止
  - サイバートラストは楕円暗号を利用した証明書発行も準備


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 問題は対応したくても直ぐには対応できない

**暗号アルゴリズムを移行する仕組みを持っていない装置・製品が世の中には大量に出回っている**
**～ 相当長期にわたる移行期間・並行運用期間が必要 ～**

- **似た事例：2011年完全地デジ化は約10年前から広報していても、対応率はやっと50%に到達した程度**
- **暗号世代交代の障害になりそうな主要製品例**
  - Windows XP SP2以前のOS
    - SHA-256やAESが使えない
  - 任天堂DS、過去に無償配布された無線LAN装置
    - WPA/WPA2が使えない
  - 過去に販売された携帯電話
    - RSA2048, SHA-2未対応機種が存在

**W3Counterによれば Windows XP利用率は約70%**


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 技術的に・・・
# MD5中間CA偽造攻撃


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 新年早々のホットな話題 = MD5証明書偽造 =

## “MD5 Considered Harmful Today–Creating a rogue CA certificate”

@CCC 2008 (Chaos Communication Congress, 2008.12.30)

**「SSL証明書の偽造」に研究者らが成功、計算には200台のPS3を使用**

**MD5アルゴリズムの弱点を突く、詳細については未公表**

米国やスイス、オランダなどのセキュリティ研究者7名は2008年12月30日、ドイツで開催されたセキュリティ関連の国際会議において、SSL通信に使用するデジタル証明書（SSL証明書）の偽造に成功したことを明らかにした。偽造に必要な計算には、ソニー・コンピュータエンタテインメントのゲーム機「プレイステーション3（PS3）」を200台組み合わせて利用したという。

計算に使用されたPS3（研究者の一人であるBenne de Weger氏のWebサイトから引用）
[画像のクリックで拡大表示]

出典：日経パソコンより

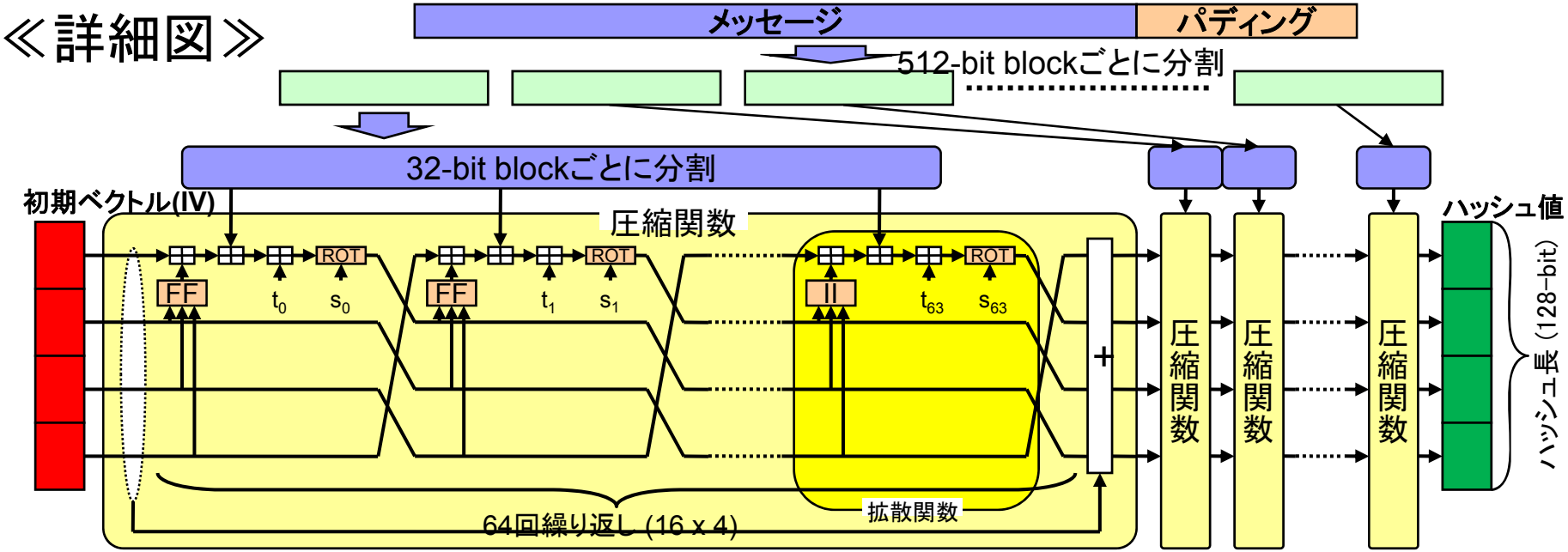




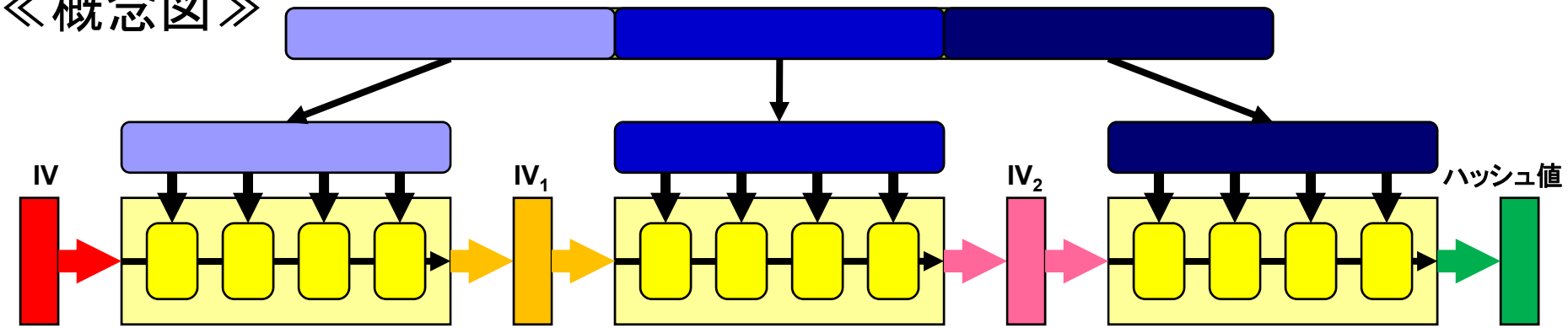
(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# MD5 (Merkle-Damgard構造)

≪詳細図≫




≪概念図≫



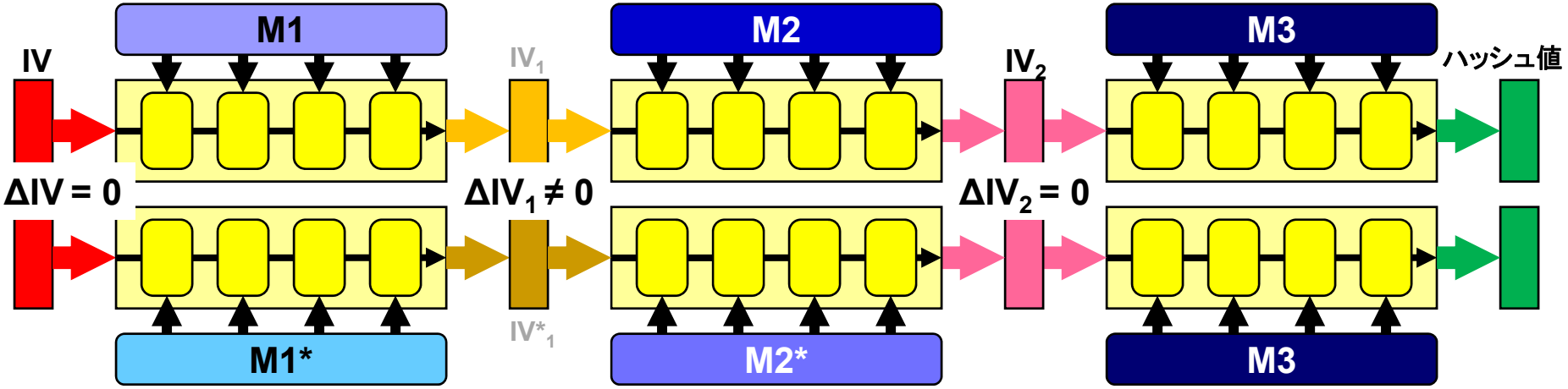


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# MD5（Merkle-Damgard構造）の衝突

- **衝突攻撃：2004年Wangらにより発見**

  **MD5（M）=MD5（M*）となる（M,M*）を見つける**

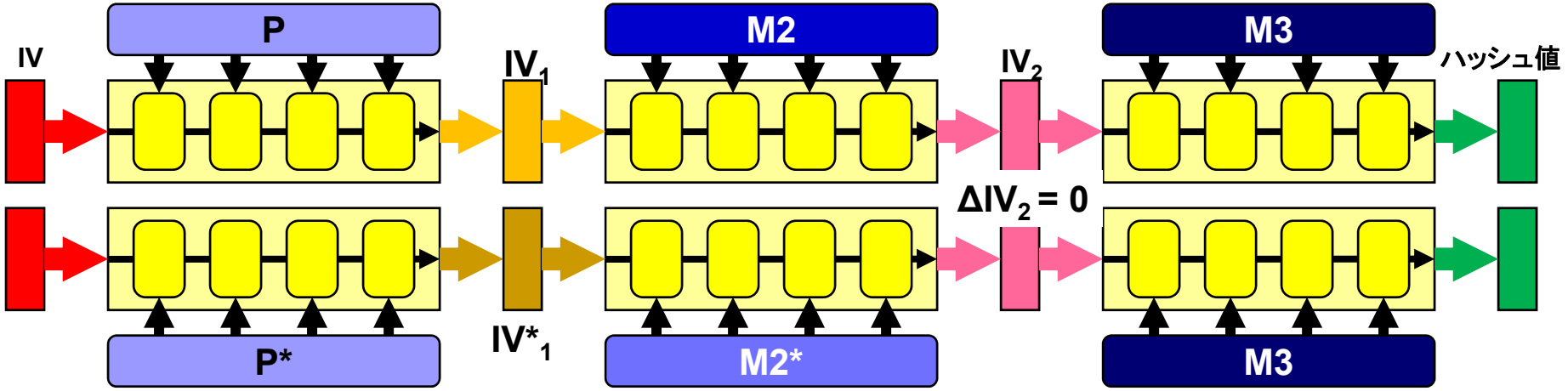



  - 計算量：約$2^{39}$回→約$2^{30}$回で可能
  - Length-extension攻撃に脆弱＝M3以降に何をつけても衝突
  - **2006年：公開鍵情報を衝突させたX.509証明書の偽造例が発見（X.509フォーマットに合わせた形のハッシュ値が一致するだけで上位CAの署名をもらったわけではない）**

# MD5 (Merkle-Damgard構造) の衝突

- **選択プレフィックス衝突探索：2007年Stevensらが発見**

**任意の (P,P*) に対しMD5 (P|M) =MD5 (P*|M*) となる (M,M*) を求める**

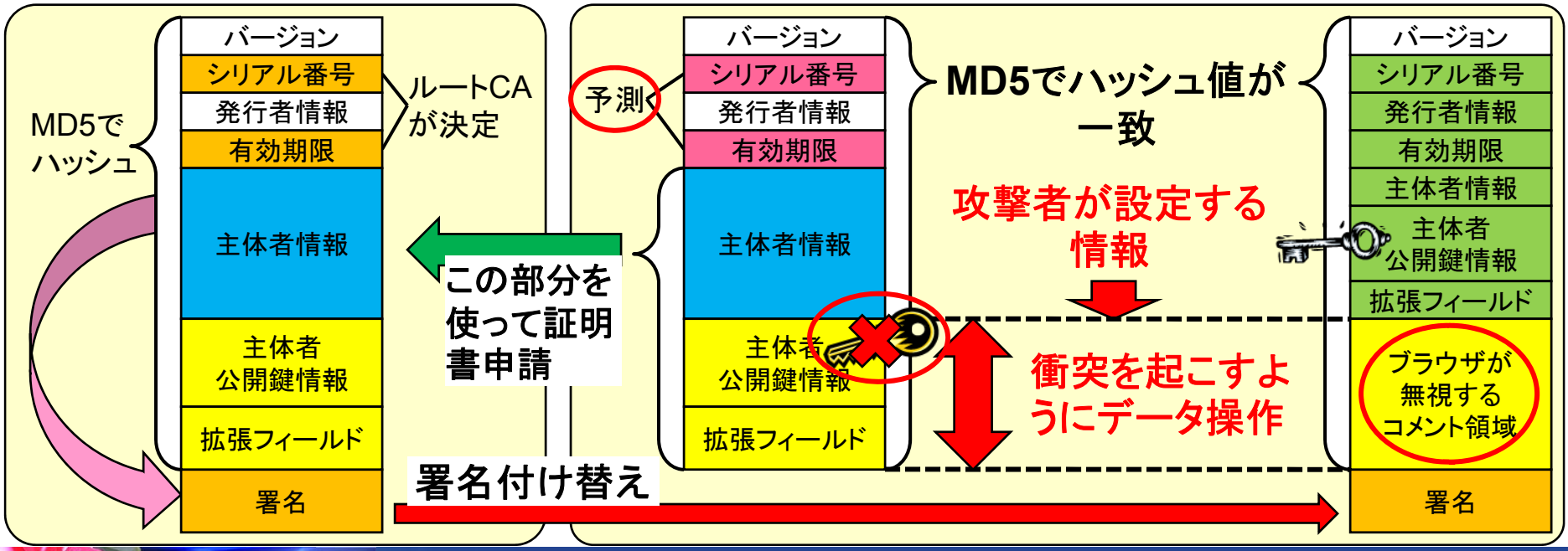



- 計算量：約$2^{52}$回・約6ヶ月@1200台PC
- 制御不可のビットが存在＝衝突攻撃より制約条件が多い
- **2008年：PにRoot CAをだますためのダミー情報、P*に公開鍵を含む偽造情報を入れて選択プレフィックス衝突探索手法を実行し中間CA EE証明書を偽造。PS3 200台で約1日**


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# MD5を使った偽造SSL証明書

- 何が問題だったのか？
  - MD5の耐衝突性が脆弱
  - POP（Proof-Of-Possession）未対応のルートCAが存在
  - ルートCAが決める「シリアルナンバー」「有効期限」が予測可
  - ブラウザが無視するコメント領域が存在

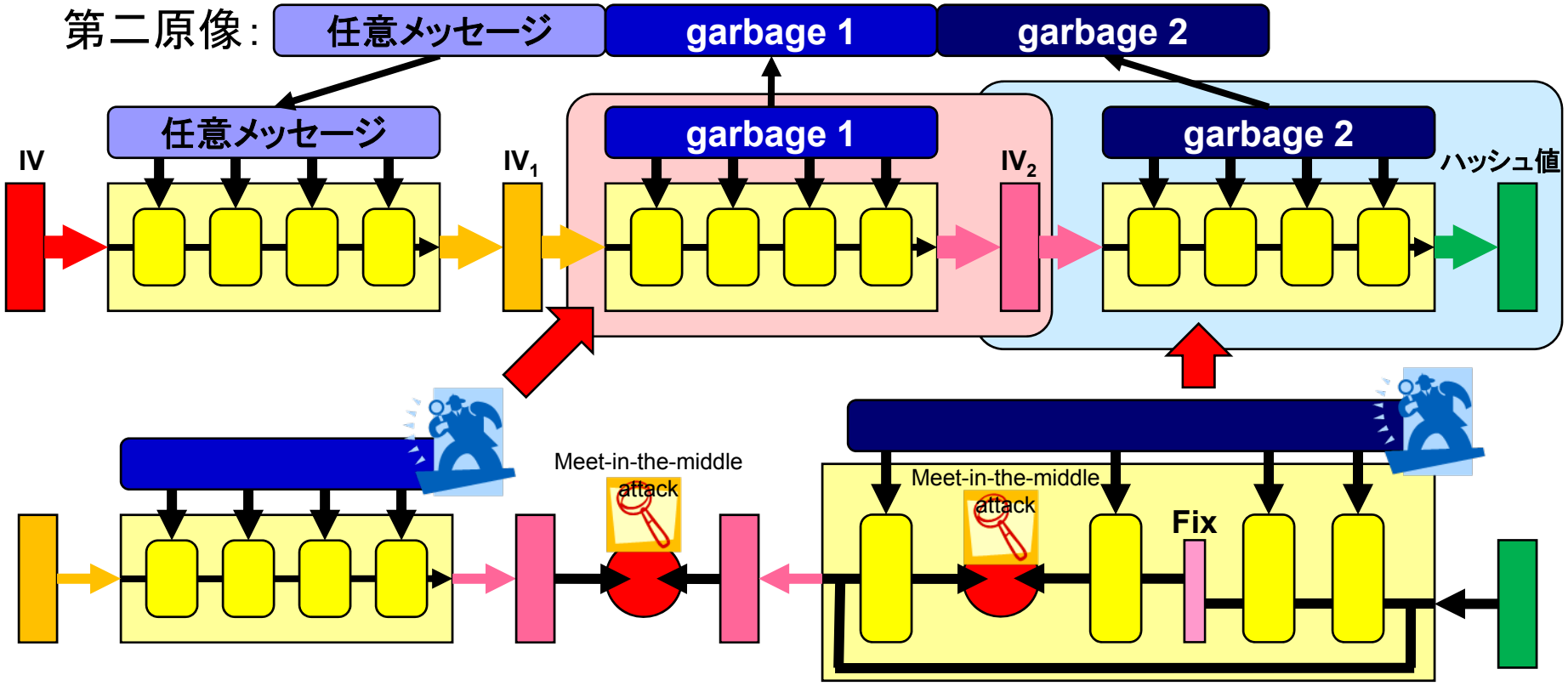




(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# ちなみに第二原像攻撃は

- **MD5第二原像攻撃成功：2008年青木らが発見**
  - 計算量：$2^{127}$ ⇒ ほんのちょっとだけ全数探索より効率的！
  - “garbage”につじつま合わせの情報を付け加える

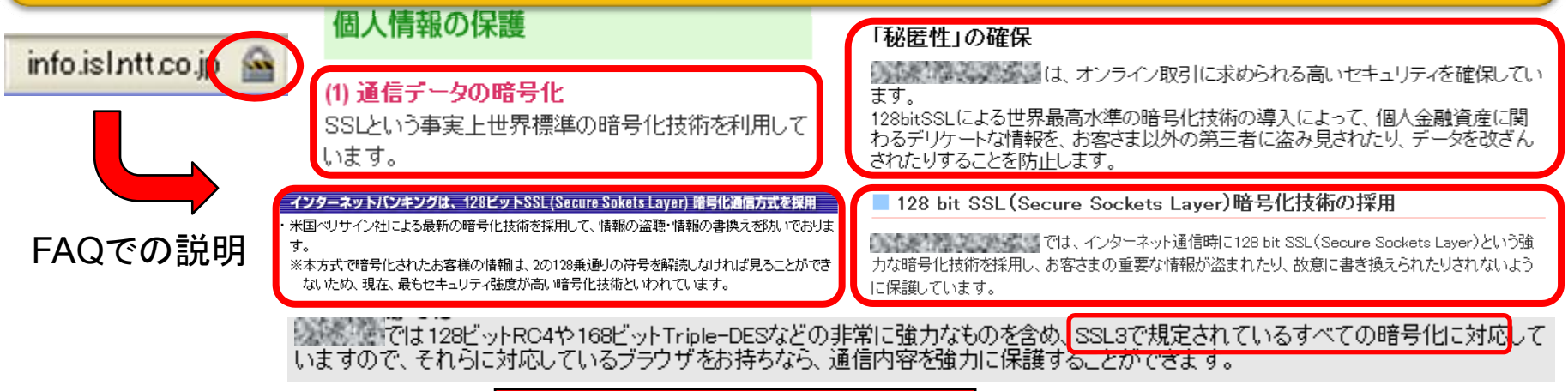


# 運用的に・・・
# 政府・金融機関のSSLサーバ暗号設定調査結果


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 【実例7】SSL/TLSは暗号化技術？

**「暗号化はSSLで」の一言で片づけられていないか**
**～ どんな暗号を使っているか認識されていないのに「適切な設定」がなされているか ～**




FAQでの説明

**しかし、実際には**

**SSL/TLSで利用可能な暗号**

| | | |
|---|---|---|
| 共通鍵暗号 | ブロック暗号 | RC2(40), DES (40,56), Triple DES, IDEA, AES, Camellia, SEED |
| | ストリーム暗号 | RC4(40, 128) |
| 公開鍵暗号 | | RSA, ECDH, DH |
| デジタル署名 | | RSA, DSS(DSA), ECDSA |
| ハッシュ関数 | | MD5, SHA-1, SHA-256, SHA-384, SHA-512 |

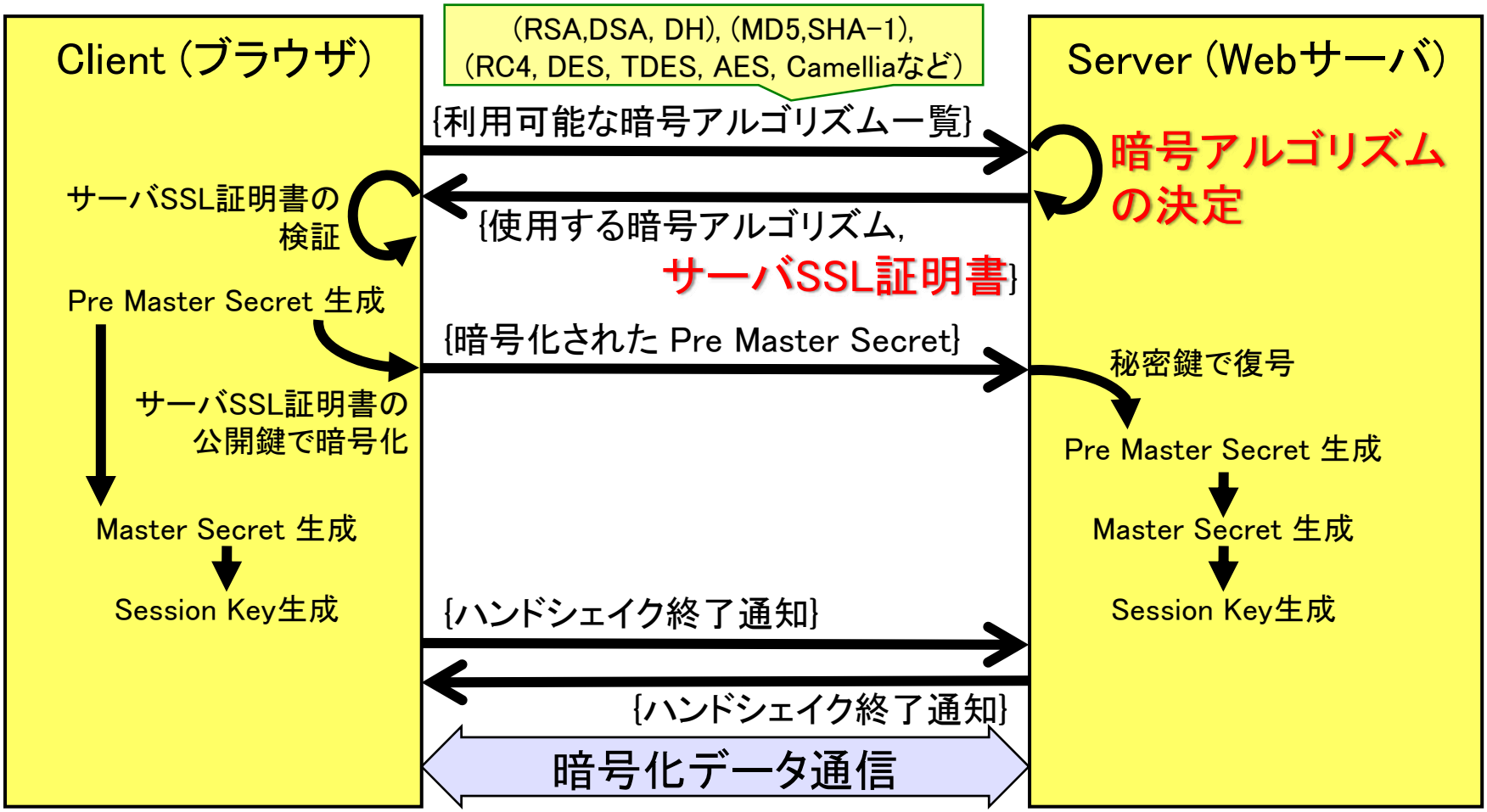
これらのうちどれを使うかは
サーバとブラウザが事前に
ネゴシエーションして決定

設定によって実際の暗号化に使われる暗号が異なる


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 【実例7】SSL/TLSの概要

- ハンドシェイクで使用する暗号アルゴリズムを決定





(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 【実例7】SSL/TLSは暗号化技術？

## セキュリティに関することで「下位互換」を重視すべきか？

例えば、SSL2.0でもつなげられることはユーザの利益か

「SSL 2.0には既知の脆弱性があるため、HTTPSプロトコルなどの SSLで保護された通信が解読され、重要な情報が漏洩する可能性があります。（IPAセキュリティセンタ）」

## SSLサーバ証明書はどこまで信用していいものか？

実在証明無しの証明書はドメインさえ所有していれば誰にでも発行

**EV SSL証明書の登場**

**運営組織の実在性確認**

**プロセスの厳格化**


**色表示ルールが IE と Firefox とで違う！**


出典：ITPro>セキュリティ
http://itpro.nikkeibp.co.jp/article/NEWS/20060214/229197/

# 【実例7】CRYPTREC推奨は？

## SSL/TLSに対する(たぶん国内唯一の)公式ガイドライン

2003年2月決定の電子政府推奨暗号リストに基づく推奨

| | | |
|---|---|---|
| 公開鍵暗号（署名） | RSA 1024 bit以上<br>DSA 1024 bit以上<br>ECDSA 160 bit 以上 | SHA-1 |
| 公開鍵暗号（鍵共有） | RSA 1024 bit以上<br>DH 1024 bit以上<br>ECDH 160 bit以上 | SHA-1 |
| 共通鍵暗号 | AES 128 bit以上<br>Camellia 128 bit以上<br>3-key Triple DES<br>128-bit RC4 | |

⇨ MD5はこの時点ですでに推奨ではなかった

2008年3月発行の電子政府推奨暗号の利用方法に関するガイドブックに記載の推奨

| | | |
|---|---|---|
| 公開鍵暗号（署名） | RSA 2048 bit以上<br>DSA 2048 bit以上<br>ECDSA 224 bit 以上 | SHA-1* |
| 公開鍵暗号（鍵共有） | RSA 2048 bit以上<br>DH 2048 bit以上<br>ECDH 192 bit以上 | SHA-1* |
| 共通鍵暗号 | AES 128 bit以上<br>Camellia 128 bit以上 | |

* 利用は推奨されないが、変更できるようになった場合には暗号切替等を検討することを推奨

⇨ RC4とTriple DESも推奨から外されている


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# OpenSSLで利用可能な暗号アルゴリズム

| | | サーバ認証なし | 輸出規制対応 | SSL2.0対応 |
|---|---|---|---|---|
| CAMELLIA256-SHA | RC4-SHA | ADH-CAMELLIA256-SHA | EXP-DES-CBC-SHA | DES-CBC3-MD5 |
| DHE-RSA-CAMELLIA256-SHA | IDEA-CBC-SHA | ADH-CAMELLIA128-SHA | EXP-EDH-RSA-DES-CBC-SHA | IDEA-CBC-MD5 |
| DHE-DSS-CAMELLIA256-SHA | RC4-MD5 | ADH-AES256-SHA | EXP-EDH-DSS-DES-CBC-SHA | RC4-MD5 |
| AES256-SHA | DES-CBC-SHA | ADH-AES128-SHA | EXP-RC4-MD5 | RC2-CBC-MD5 |
| DHE-RSA-AES256-SHA | EDH-RSA-DES-CBC-SHA | ADH-DES-CBC3-SHA | EXP-RC2-CBC-SHA | DES-CBC-MD5 |
| DHE-DSS-AES256-SHA | EDH-DSS-DES-CBC-SHA | ADH-RC4-MD5 | EXP-ADH-DES-CBC-SHA | EXP-RC4-MD5 |
| CAMELLIA128-SHA | | ADH-DES-CBC-SHA | EXP-ADH-RC4-MD5 | EXP-RC2-CBC-MD5 |
| DHE-RSA-CAMELLIA128-SHA | | | | |
| DHE-DSS-CAMELLIA128SHA | | | | |
| AES128-SHA | | | | |
| DHE-RSA-AES128-SHA | | | | |
| DHE-DSS-AES128-SHA | | | | |
| DES-CBC3-SHA | | | | |
| EDH-RSA-DES-CBC3-SHA | | | | |
| EDH-DSS-DES-CBC3-SHA | | | | |

**SSLで利用する暗号アルゴリズムとして**
**これらの中のどれかが一つを**
**サーバが選択する**


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# ブラウザが利用する暗号のデフォルト優先順位

| | IE8 | | IE7 | | | IE6 | | FX3 | FX2 | Safari3.2 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Vista1 | XP3 | Vista2 | Vista1 | XP3 | XP3 | XP2 | XP2 | XP2 | Vista2 | XP3 |
| ECDHE_RSA_WITH_RC4_128_SHA | | | | | | | | 13 | 10 | | |
| ECDHE_RSA_WITH_AES_256_CBC_SHA | 8 | | 8 | 8 | | | | 2 | 2 | 8 | |
| ECDHE_RSA_WITH_AES_128_CBC_SHA | 7 | | 7 | 7 | | | | 14 | 11 | 7 | |
| ECDHE_ECDSA_WITH_RC4_128_SHA | | | | | | | | 11 | 8 | | |
| ECDHE_ECDSA_WITH_AES_256_CBC_SHA | 6 | | 6 | 6 | | | | 1 | 1 | 6 | |
| ECDHE_ECDSA_WITH_AES_128_CBC_SHA | 5 | | 5 | 5 | | | | 12 | 9 | 5 | |
| ECDH_RSA_WITH_AES_256_CBC_SHA | | | | | | | | 7 | 5 | | |
| ECDH_ECDSA_WITH_AES_256_CBC_SHA | | | | | | | | 8 | 6 | | |
| **RSA_WITH_RC4_128_SHA** | **3** | **2** | **3** | **3** | **2** | **2** | **2** | **25** | **19** | **3** | **2** |
| **RSA_WITH_RC4_128_MD5** | **12** | **1** | **12** | **12** | **1** | **1** | **1** | **24** | **18** | **12** | **1** |
| RSA_WITH_CAMELLIA_256_CBC_SHA | | | | | | | | 9 | | | |
| **RSA_WITH_AES_256_CBC_SHA** | **2** | | **2** | **2** | | | | **10** | **7** | **2** | |
| **RSA_WITH_AES_128_CBC_SHA** | **1** | | **1** | **1** | | | | **26** | **20** | **1** | |
| **RSA_WITH_3DES_EDE_CBC_SHA** | **4** | **3** | **4** | **4** | **3** | **3** | **3** | **33** | **27** | **4** | **3** |
| **DHE_RSA_WITH_CAMELLIA_256_CBC_SHA** | | | | | | | | **3** | | | |
| DHE_RSA_WITH_CAMELLIA_128_CBC_SHA | | | | | | | | 15 | | | |
| **DHE_RSA_WITH_AES_256_CBC_SHA** | | | | | | | | **5** | **3** | | |
| DHE_DSS_WITH_CAMELLIA_256_CBC_SHA | | | | | | | | 4 | | | |
| DHE_DSS_WITH_CAMELLIA_128_CBC_SHA | | | | | | | | 16 | | | |
| DHE_DSS_WITH_AES_256_CBC_SHA | 10 | | 10 | 10 | | | | 6 | 4 | 10 | |
| DHE_DSS_WITH_AES_128_CBC_SHA | 9 | | 9 | 9 | | | | 18 | 13 | 9 | |
| DHE_DSS_WITH_3DES_EDE_CBC_SHA | 11 | 4 | 11 | 11 | 4 | 7 | 7 | 30 | 24 | 11 | 7 |
| **SSL2_RC4_128_WITH_MD5** | | | | | | **4** | **4** | | | | **4** |
| **SSL2_DES_192_EDE3_CBC_WITH_MD5** | | | | | | **5** | **5** | | | | **5** |
| **SSL2_RC2_CBC_128_CBC_WITH_MD5** | | | | | | **6** | **6** | | | | **6** |

# 【実例7】実際にどうなっているのか検証

- **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**

**政府・公共系：約145サーバ、金融系：約135サーバ**

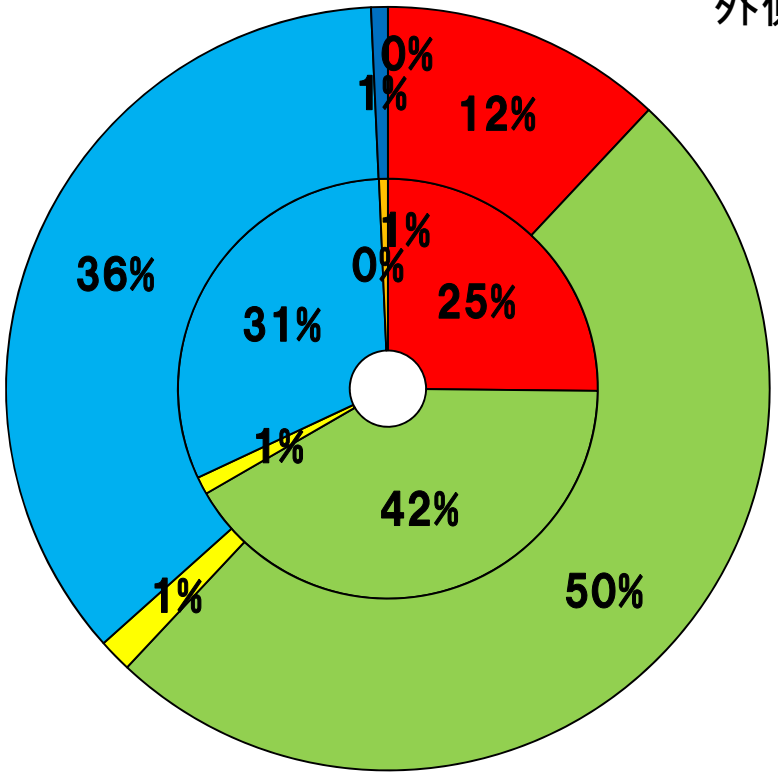
- **調査期間：2008年10～11月／2009年5～6月**
- **調査内容：**
  - サーバ証明書の状況（有効期限、アルゴリズム、鍵長等）
  - 暗号選択設定の状況（接続可能なアルゴリズム）
  - ブラウザでの実際の接続状況（IE6, IE7, Firefox3）


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# サーバ証明書の状況（アルゴリズムと有効期限）

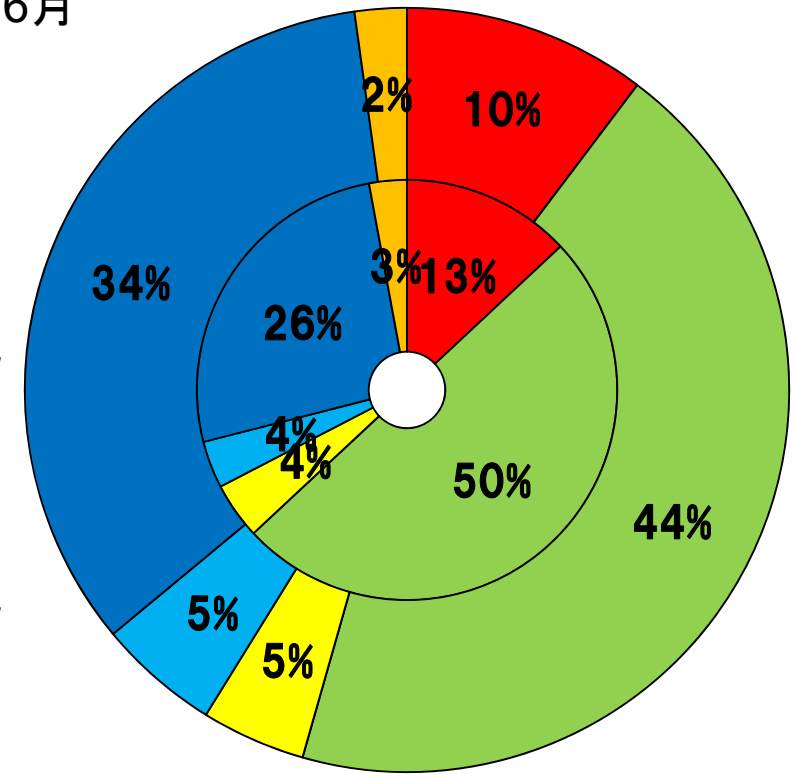
## 政府・公共系サーバ

内側：2008年11月
外側：2009年　6月

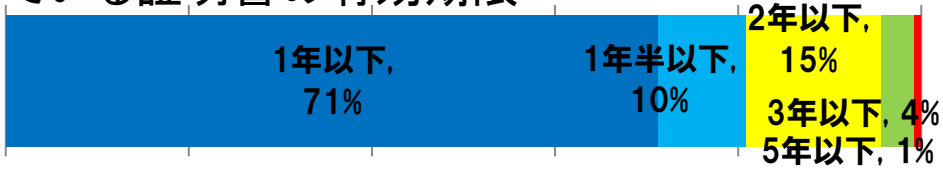



- MD5 with RSA1024
- SHA1 with RSA1024
- SHA1 with RSA1024 EV
- SHA1 with RSA2048
- SHA1 with RSA2048 EV
- SHA1 with RSA1000

## 金融系サーバ



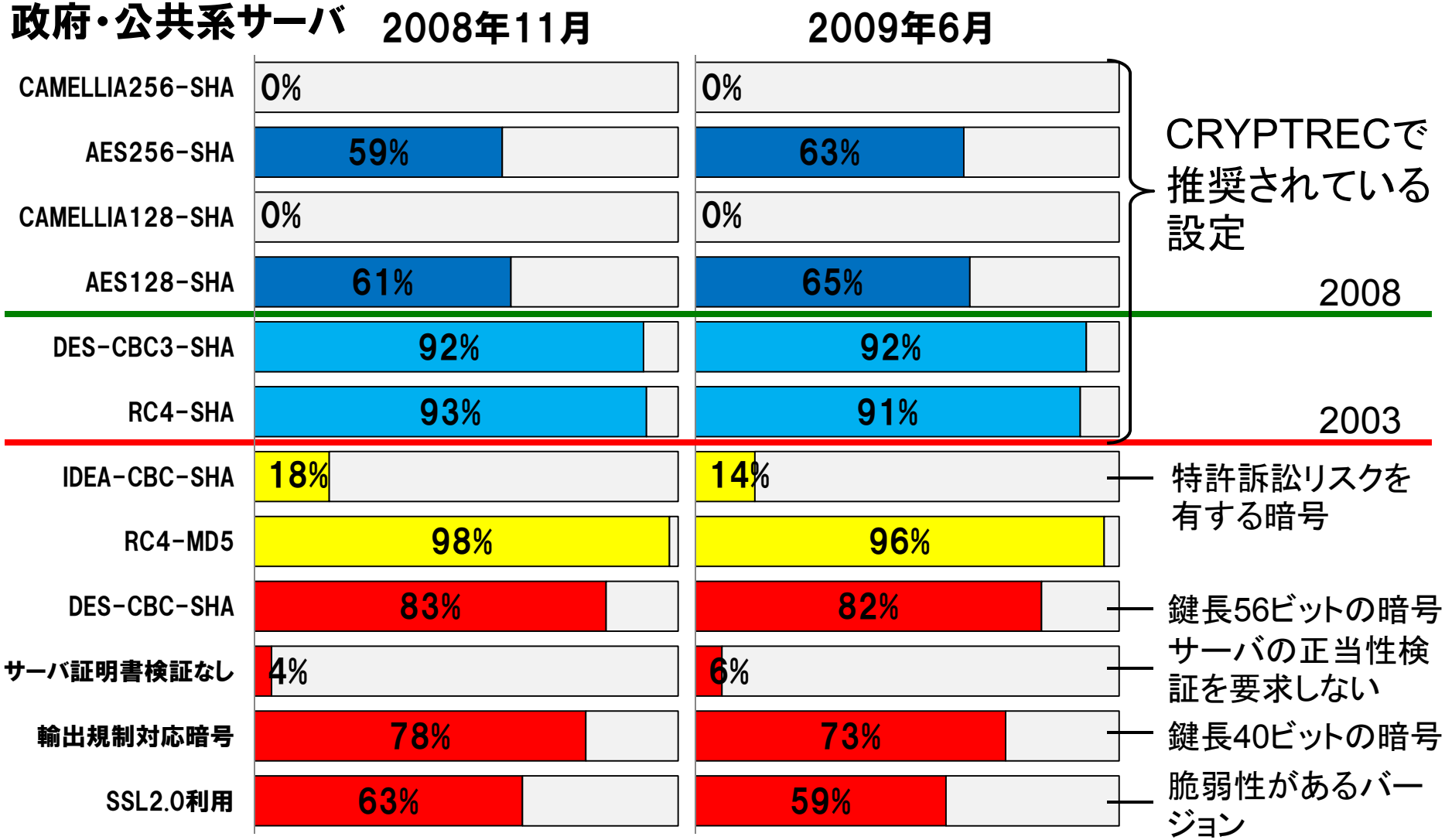

2009年6月時点で利用されている証明書の有効期限



(c)日本電信電話株式会社
情報流通プラットフォーム研究所

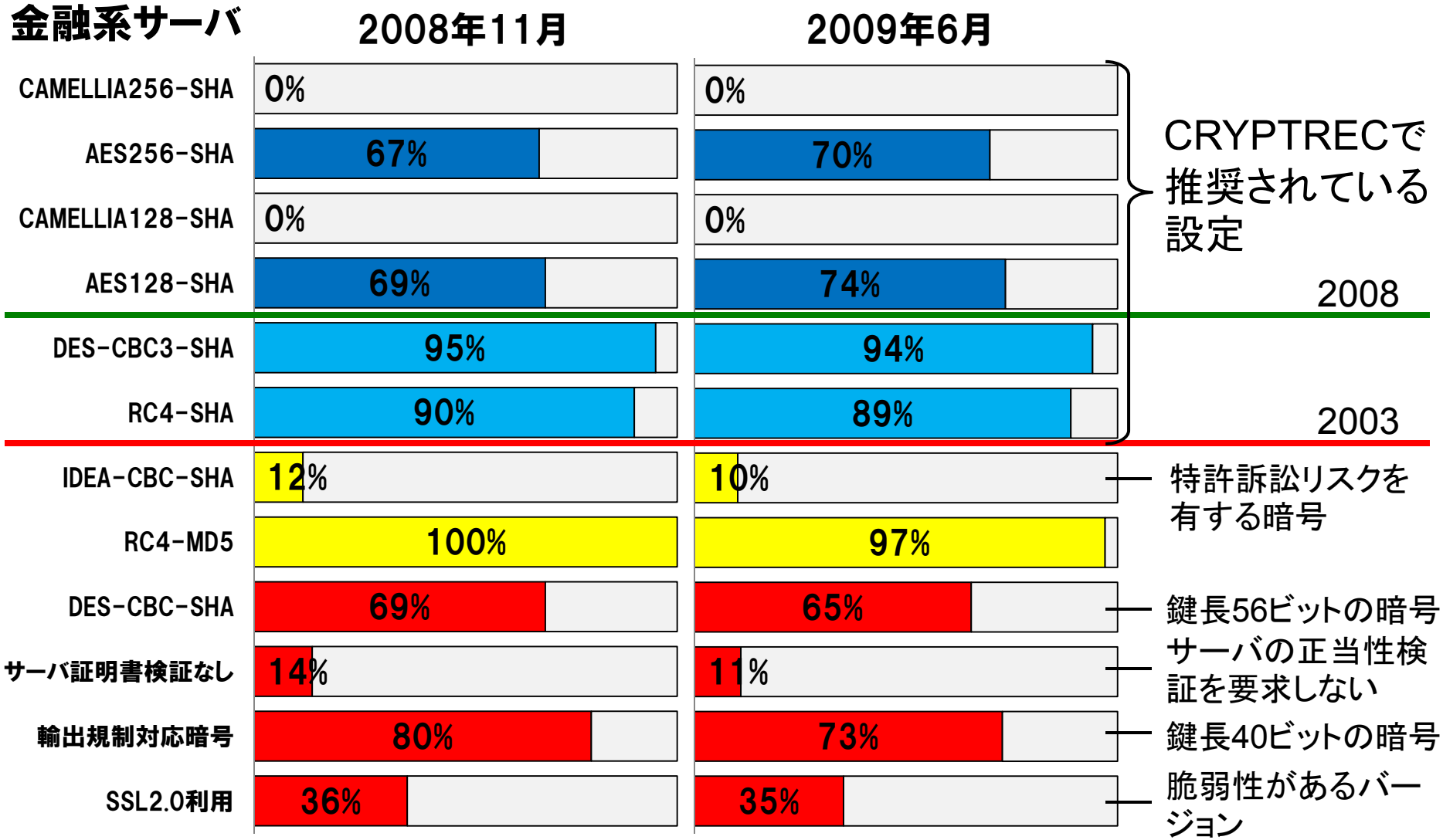
# サーバでの暗号設定　～受入可能な主な暗号～





(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# サーバでの暗号設定　～受入可能な主な暗号～



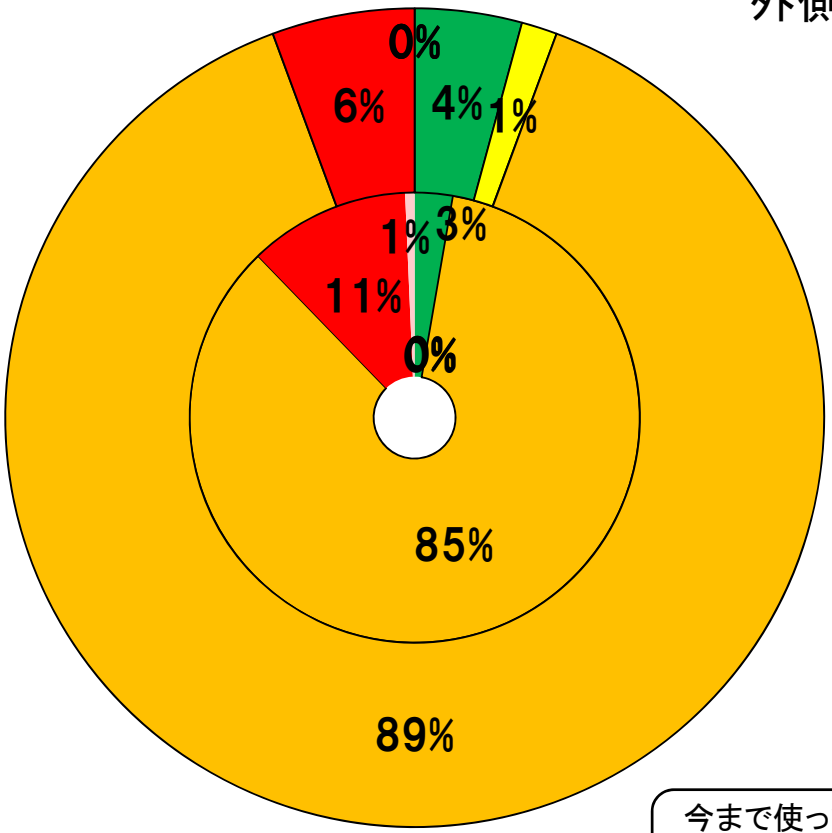


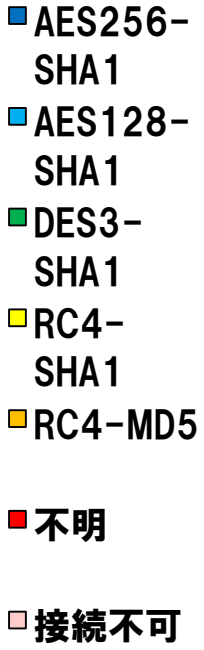
(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# Internet Explorer 7 (Win XP)での接続

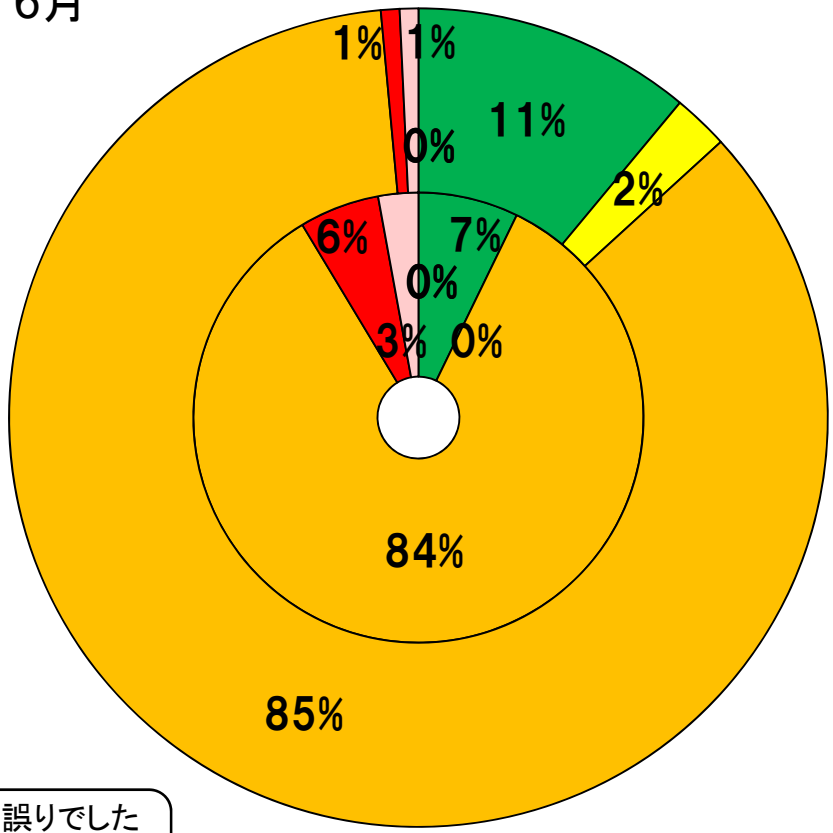
## 政府・公共系サーバ

内側：2008年11月
外側：2009年　6月




## 金融系サーバ

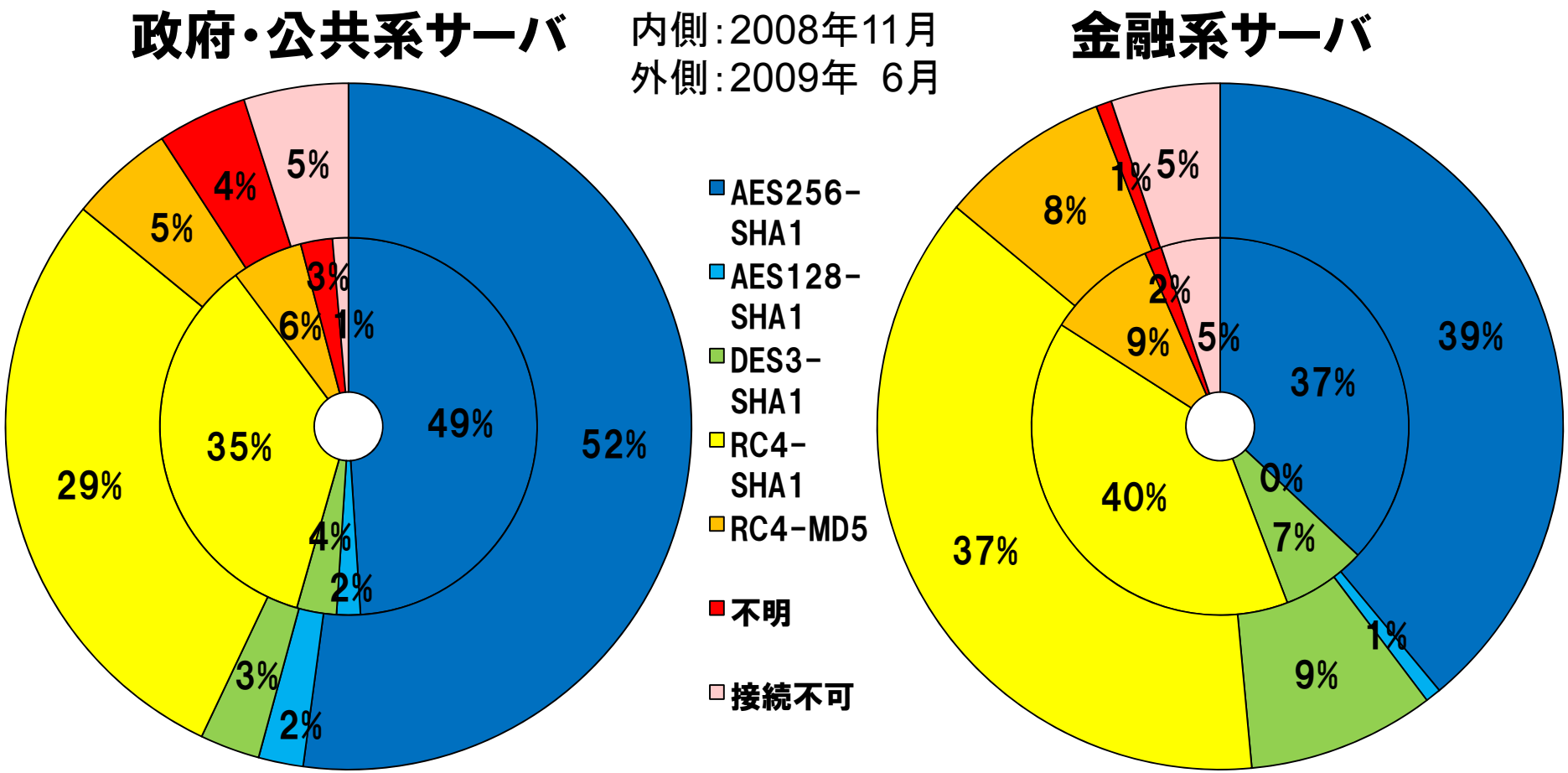



今まで使っていたデータは誤りでした
m(._.)m

RC4はSHA1ではなくMD5でした。XP SP3でも同様


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

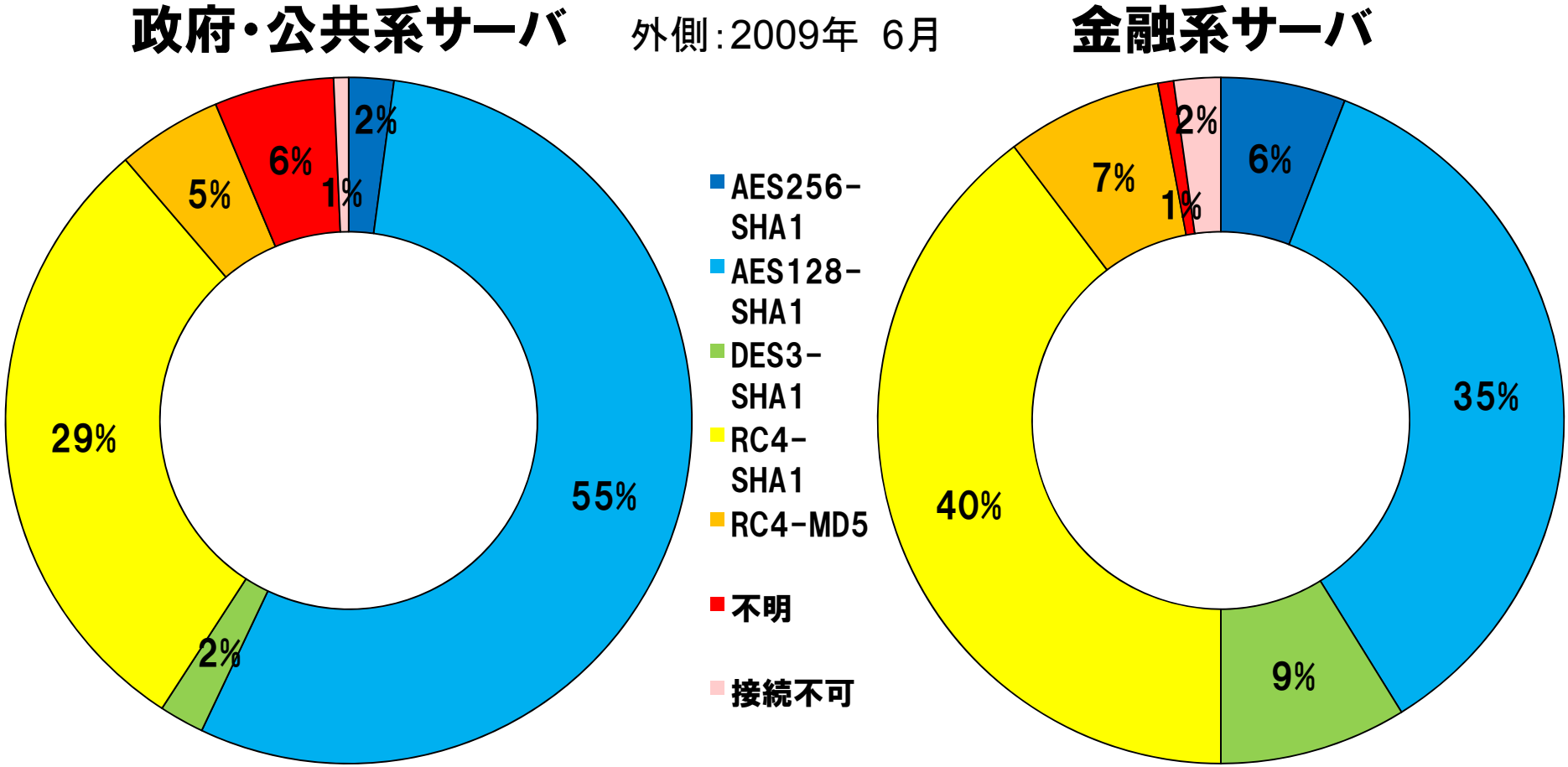
# Firefox 3 (Win XP)での接続




## AESの暗号設定状況と実際の接続での逆転現象


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# Internet Explorer 7 (Win Vista)での接続

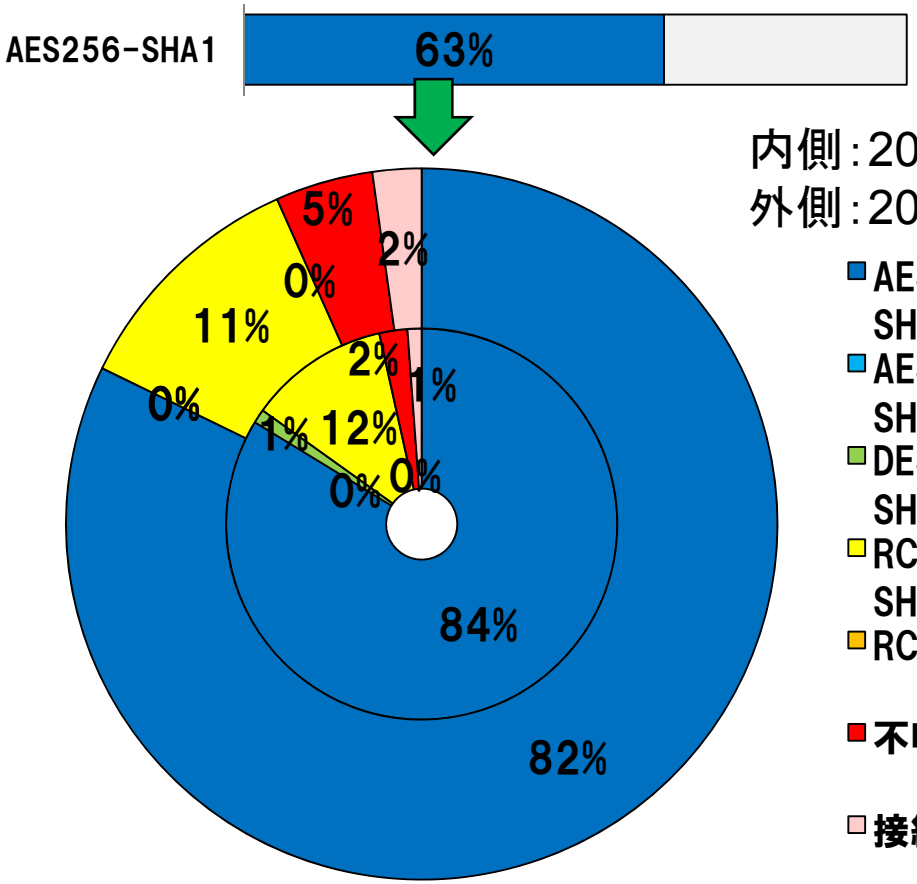



AESは使われるけども、AES128のほうが優先

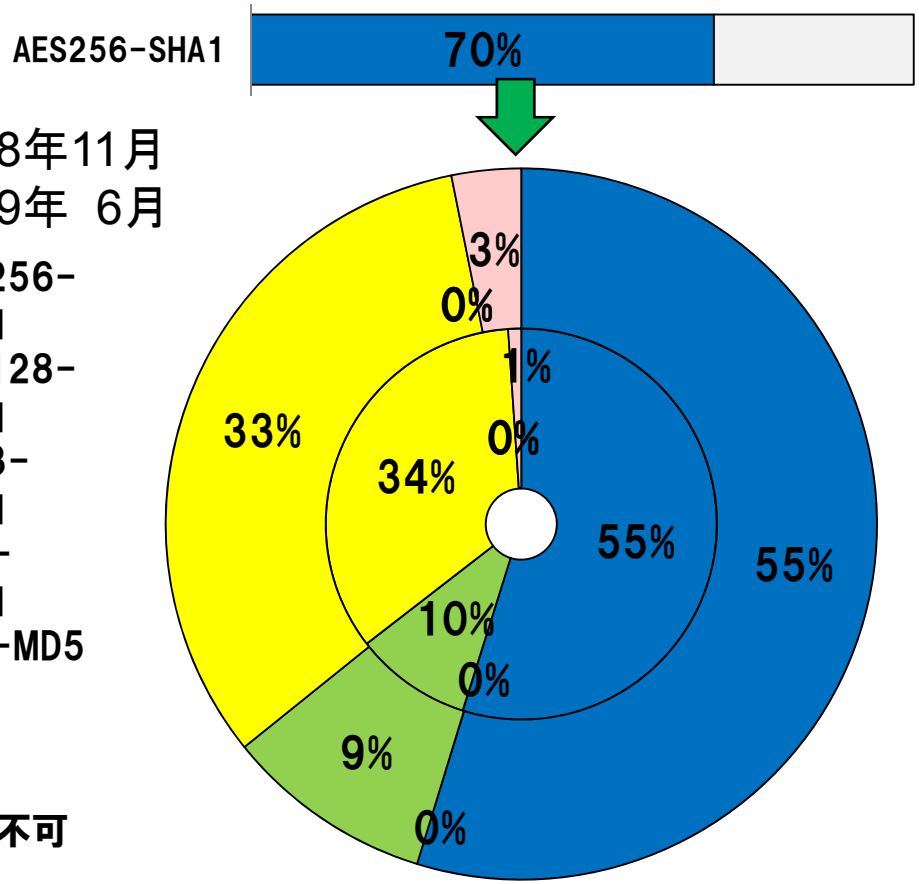

(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# AESが利用される設定になっているか

## 政府・公共系サーバ




## 金融系サーバ




内側：2008年11月
外側：2009年　6月

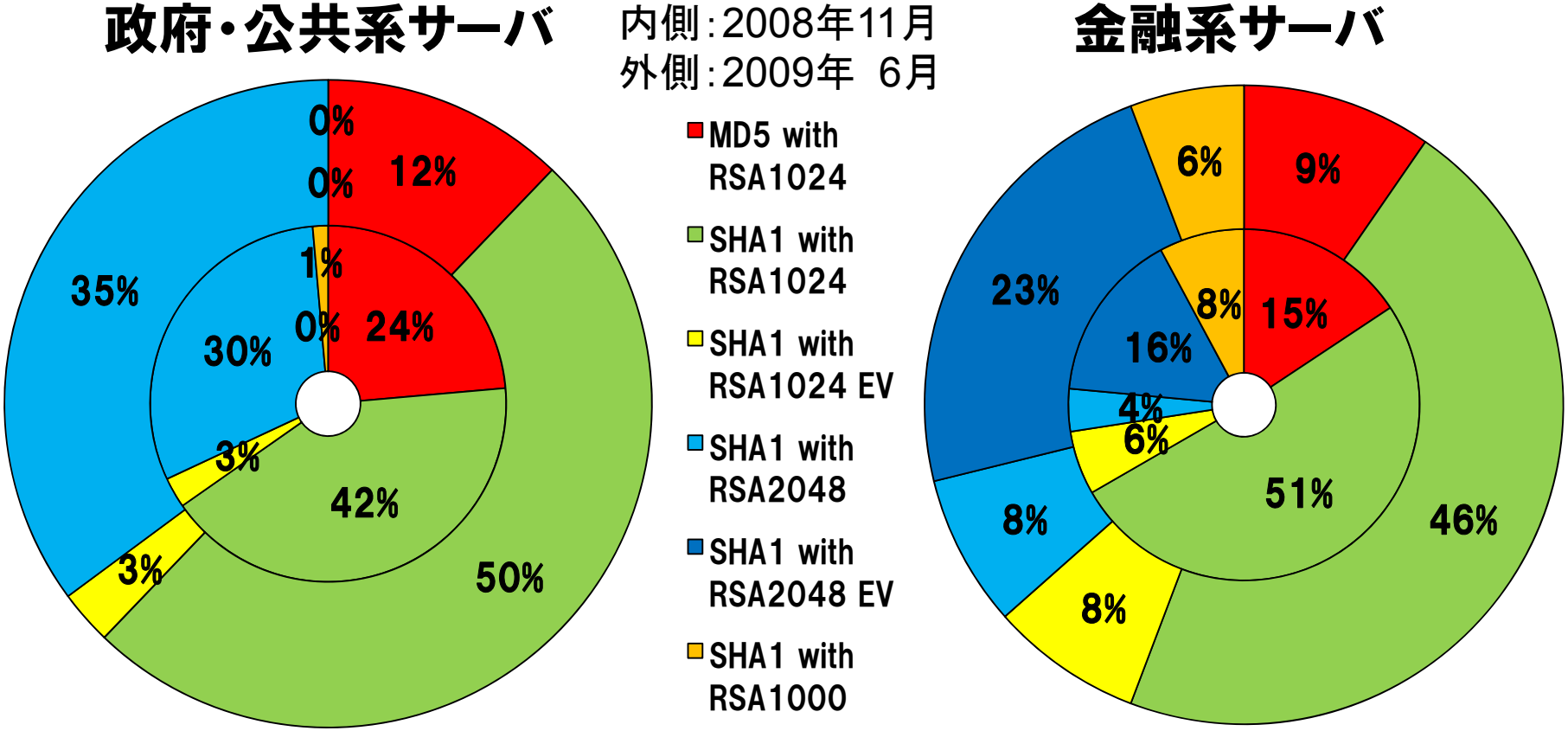
- AES256-SHA1
- AES128-SHA1
- DES3-SHA1
- RC4-SHA1
- RC4-MD5
- 不明
- 接続不可

**設定変更してもAESの利用率はほとんど変わっていない**


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# 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




AESを使っているサーバだから証明書も、とはなっていない


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# SSLの調査結果から

**整合的に暗号設定が行われている形跡が見いだせない**
**～ 暗号アルゴリズム設定がベンダ任せになっていませんか ～**

- 「暗号化はAES256ビット」なのに「鍵交換は512ビットRSA」
- RC4で接続といってもSHA1を使っているとは限らない
- AESを使えるようにしたのにMD5のサーバ証明書のまま
- 同じ企業内のサーバであっても設定内容に一貫性がない
- どの暗号アルゴリズムが選択されたかブラウザ(クライアント)からは確認できない

**せっかく設定を変えたのに・・・設定失敗**

- AESを使えるようにしたらSSL2.0やEXPも利用可能になった
- 「AES256-SHA1」が使えるはずなのに「RC4-MD5」を選択


(c)日本電信電話株式会社
情報流通プラットフォーム研究所

# SSLの調査結果から

## SSL証明書の中身を確認しているか？

- 更改できるタイミングが何回もあったはずなのにMD5のSSL証明書が未だに健在
- MD5や署名長は変わっても、鍵交換用RSAの鍵長は変わらない

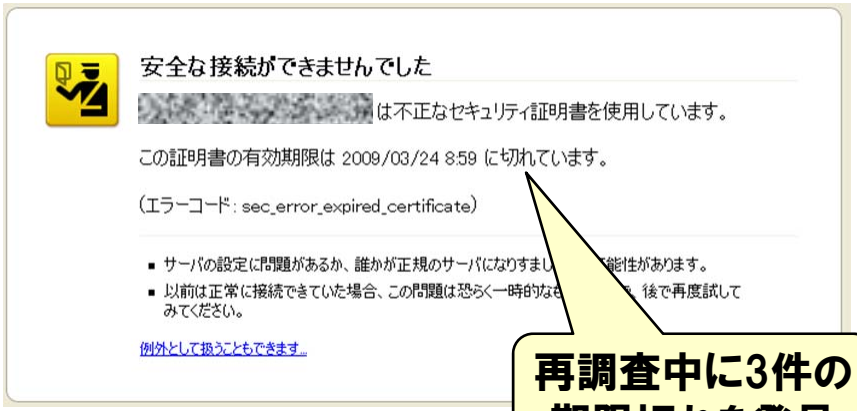
## SSL証明書の期限切れを起こすことが意外と多い

**全日空のCIO、搭乗システム障害について会見、「担当者の会話が不十分だったためのごく初歩的なミス」と反省の弁**

全日空幹部は2008年9月18日会見を開き、14日に発生したシステム不具合の原因を公表し反省を語った。払い戻しなど直接的な損失額は、全日空グループ全体で2億円。

原因は、既報されているように、チェックイン端末を管理するサーバー内の暗号化機能の有効期限の設定ミスによるもの。今回のトラブルについて、同社のCIO(最高情報責任者)である上席執行役員の佐藤透IT推進室長は、2点を挙げた。

記者会見の冒頭謝罪する全日空の経営陣
[画像のクリックで拡大表示]




再調査中に3件の期限切れを発見

出典：日経情報ストラテジー
http://itpro.nikkeibp.co.jp/article/NEWS/20080918/315052/

# まとめに代えて

「暗号学会がいう安全性」＝“将来”への予防措置
「ビジネスサイドがいう安全性」＝“現時点”での実害対処
～ 分かっている知見は開発段階から反映するのが効果的 ～

運用中の基幹システム・大規模システムでは
一朝一夕に暗号の世代交代をさせることは不可能
～ 並行運用期間が今後10年単位でかかることも想定内 ～

すぐにできることと、すぐにはできないこととを区別
～ すぐにできることをきちんとするだけでも効果がある ～

調和がとれた移行を促すための業界団体しての
「ガイドライン・移行指針」の作成
～ 暗号学会とビジネスサイドの認識ギャップを埋める ～


(c)日本電信電話株式会社
情報流通プラットフォーム研究所