NTT

NTT Information Sharing Platform Laboratories
NTT 情報流通プラットフォーム研究所

# SSLにおける暗号危殆化サンプル調査の報告

PKI day 2011 (2011.9.26)

NTT情報流通プラットフォーム研究所
セキュリティマネジメント推進プロジェクト
武藤　健一郎

# 本日の話題

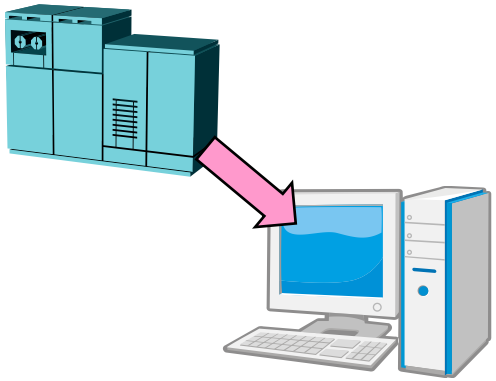
- 背景
  - 暗号危殆化
  - 暗号危殆化に関する動向
  - 暗号技術を利用した実サービスの例
  - SSLで利用する暗号
- SSLサンプル調査の概要
  - 調査概要
  - 調査内容
- 調査方法・調査結果・考察
  - 調査１：証明書における利用暗号
  - 調査２：サーバの暗号設定（接続可能暗号）
  - 調査３：ブラウザ接続時の利用暗号
- 暗号の世代交代に向けた対策の考察
- まとめ

# 暗号危殆化

**ある暗号アルゴリズムについて、当初想定したよりも低いコストで、そのセキュリティ上の性質を危うくすることが可能な状況を指す。**

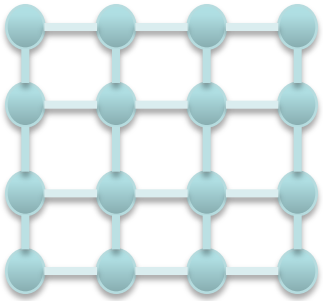
出典：IPA，暗号の危殆化に関する調査報告書，
http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/documents/crypt_compromize.pdf（2005年）

## 計算機能力の向上



ex）スーパコンピュータ

## 計算機モデルの変化



ex）量子計算機

## 攻撃手法の進歩

ex）弱鍵の発見

# 暗号危殆化に関する動向

**コンピュータの進歩などによる現在の主要暗号に対する安全性低下の深刻化に鑑み、官民双方で取り組み開始されている。**

## 米国

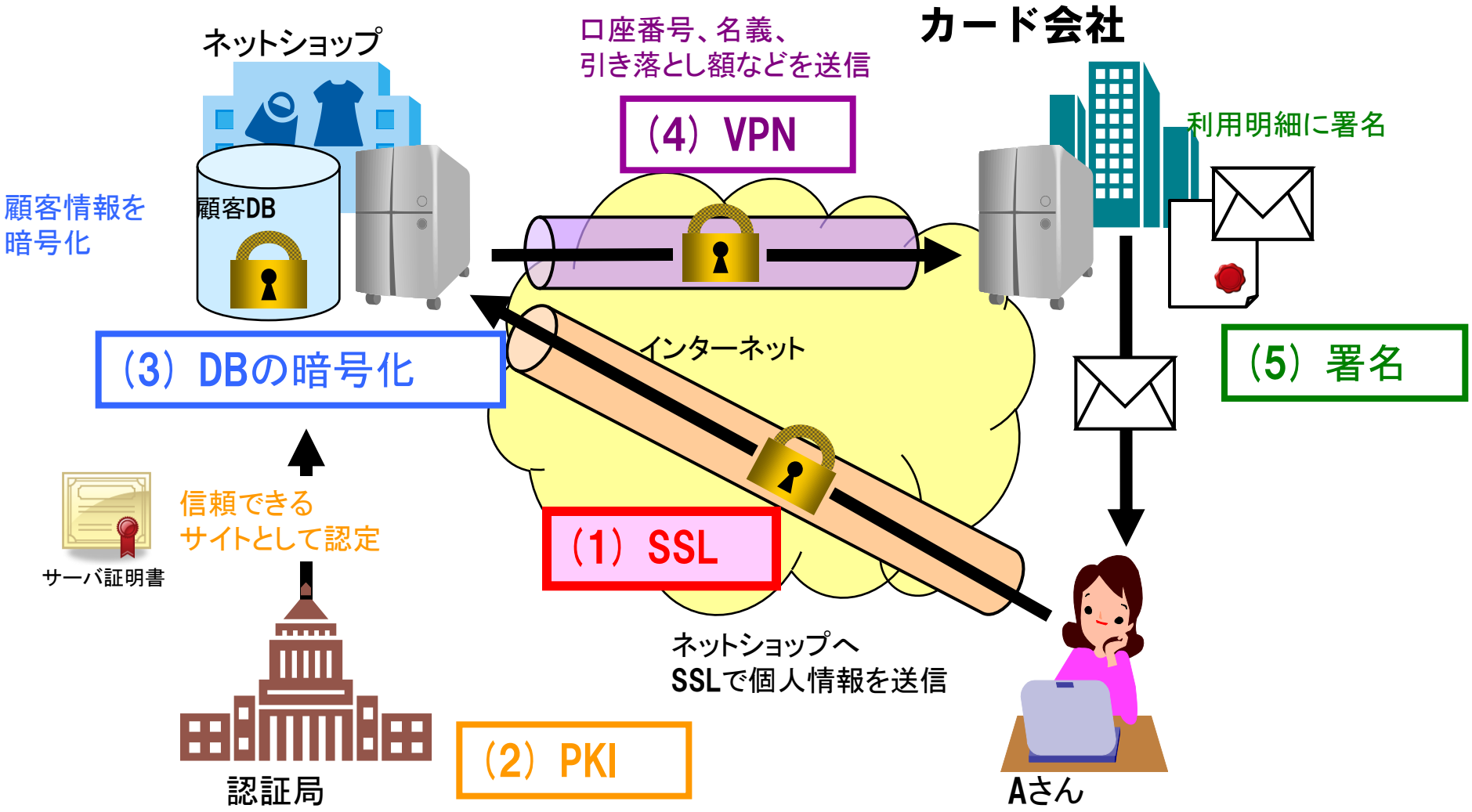
- **主要暗号を次世代暗号へ総入れ替え（2010年目処）**
  - 米国政府標準暗号の移行計画宣言（2005年公表）が大きく影響
  - 現在の主要暗号の多くは，米国政府標準暗号というお墨付きを失う

## 日本

- **2008.4.22　情報セキュリティ政策会議**
  - 2013年度までに各府省庁の情報システムの暗号切替対応を完了することを決定
  - 「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」を決定。
- **2009.1.6　日本ベリサイン**
  - MD5を利用したサーバ証明書の発行停止とSHA-1への移行を発表

# 暗号技術を利用した実サービスの例

**共通鍵暗号、公開鍵暗号、ハッシュ関数、デジタル署名などの技術を用いてデータの秘匿や改ざん防止を実現している**



# SSLで利用する暗号

## SSLでは、様々な暗号アルゴリズムが使われている

クライアント(ブラウザ)

1. 暗号セットA
2. 暗号セットB
3. 暗号セットC

暗号セットの
ネゴシエーション

サーバ

1. 暗号セットA ⇒ OK
2. 暗号セットB ⇒ OK
3. 暗号セットC ⇒ NG

サーバ証明書 = MD5 with RSA
秘密鍵交換 = RSA
データ暗号化 = RC4
HMAC = MD5

①サーバ証明書(公開鍵)の提示(RSA)

②秘密鍵の交換(RSA)

③通信の暗号化(RC4)
④データの改ざん検知(HMAC)

# SSLサンプル調査の概要

**調査の目的：**
**暗号利用状況の推移を把握し、暗号の世代交代に向けた対策方法を考察する**

**調査期間：**
SSLにおける利用暗号の定点観測を過去三回実施（2008年～2010年）

**調査対象：**
各トップページから辿ることができるSSLサーバ
- 金融系サイト
- 政府・公共系サイト

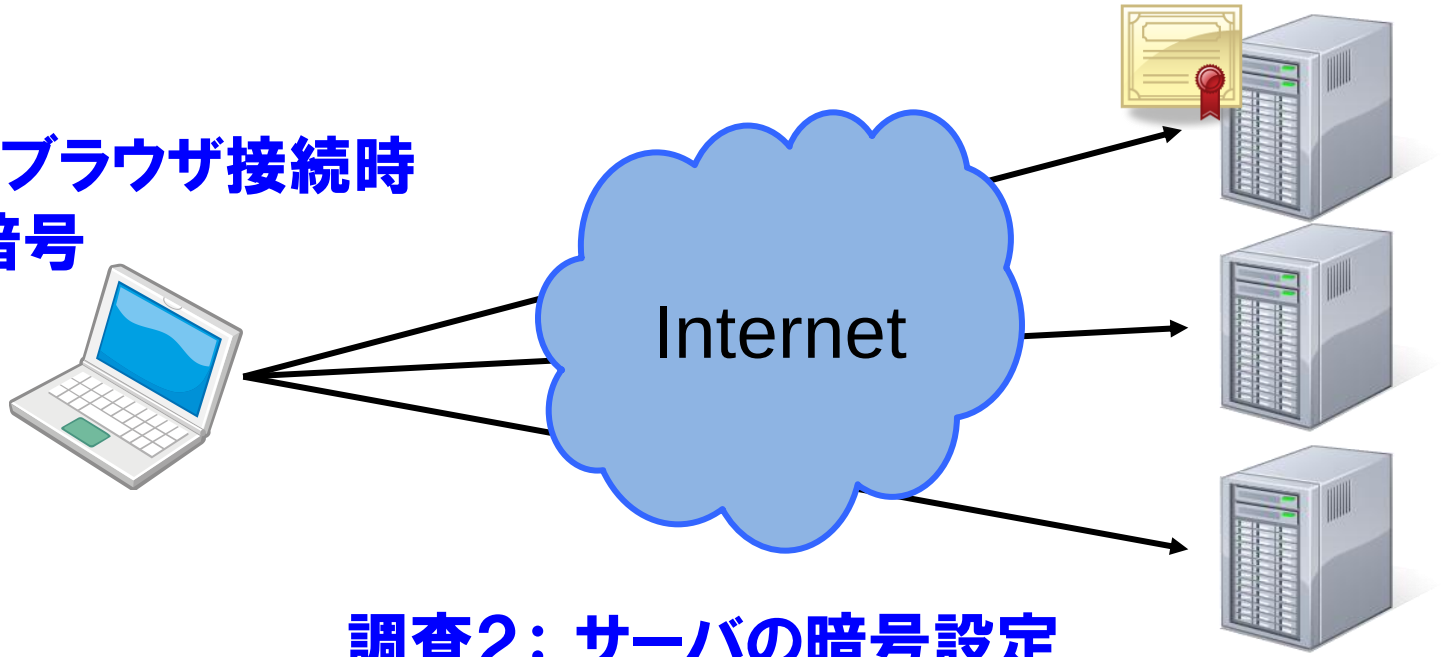
| | 調査期間 | 調査サーバ数 | |
|---|---|---|---|
| | | 金融系 | 政府・公共系 |
| 第一回調査 | 2008年10月～11月 | 138 | 147 |
| 第二回調査 | 2009年5月～6月 | 136 | 142 |
| 第三回調査 | 2010年8月 | 117 | 130 |

# 調査内容

**SSL通信時の暗号利用状況を調査する**

**調査1：証明書における利用暗号**

**調査3：ブラウザ接続時の利用暗号**



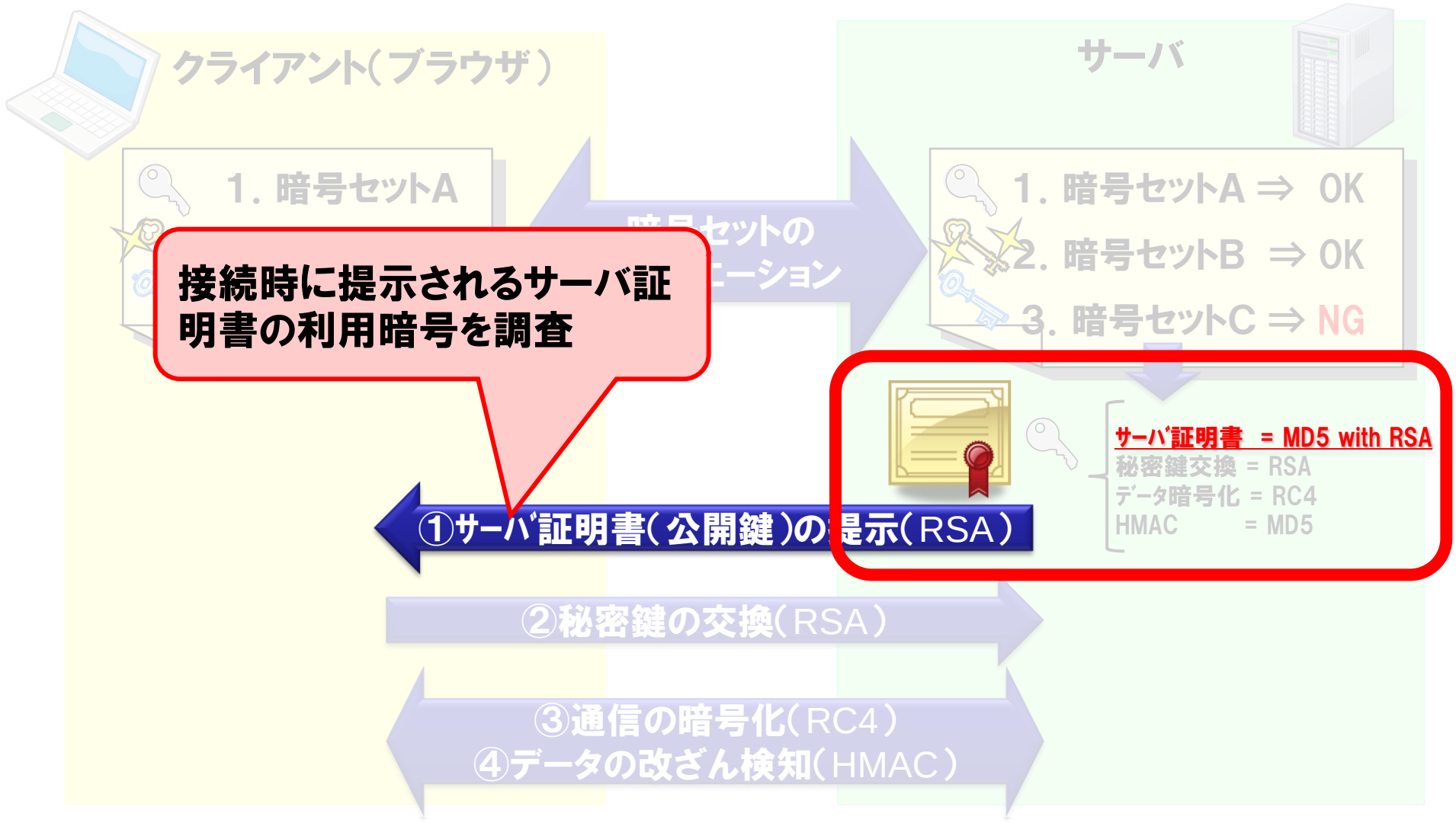

**調査2：サーバの暗号設定（接続可能暗号）**

**SSLサーバ群**

# 調査1： 証明書における利用暗号

## 調査方法

**SSLサーバ証明書の利用暗号を調査**

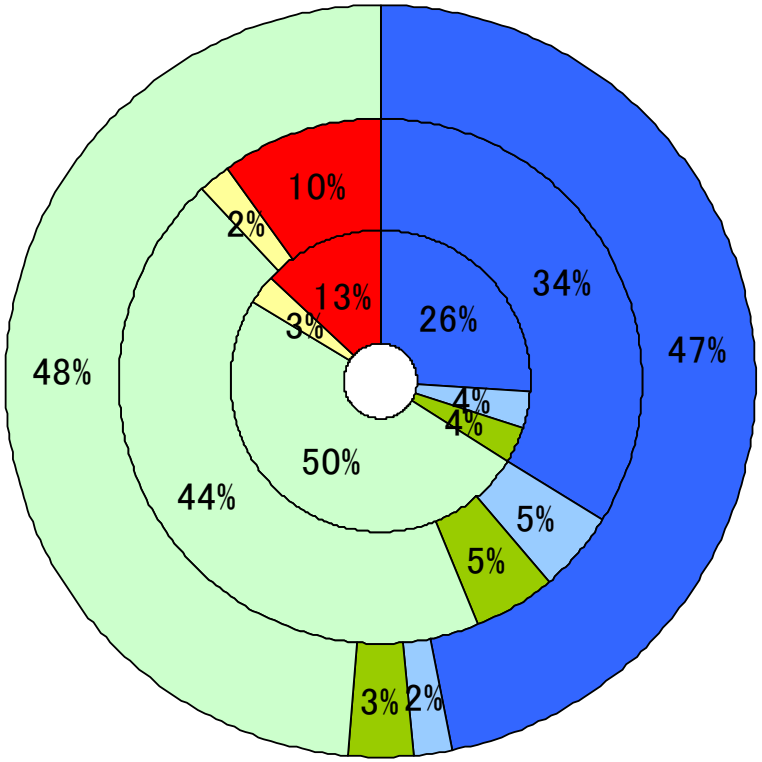


# 調査1： 証明書における利用暗号
# 調査結果

**年代で比較：**

- **危殆化が懸念されている”MD5 with RSA1024” が利用されなくなった**

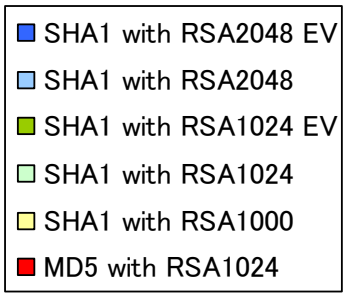
## 金融系サーバ



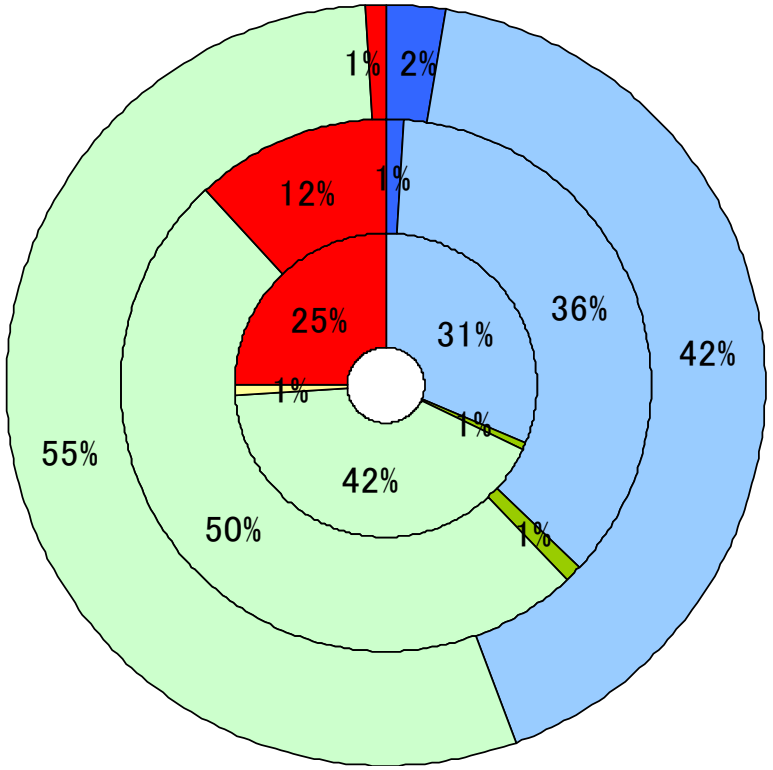

**内側：2008年**

**中央：2009年**

**外側：2010年**




## 政府・公共系サーバ



# 調査1：証明書における利用暗号
# 考察（1／2）

## MD5アルゴリズムへの衝突攻撃によるSSLサーバ証明書の偽造に関する報道について

2009年1月6日

2008年12月30日、ベルリンで開催された「第25回カオス コミュニケーション会議（CCC）」において、MD5アルゴリズムへの衝突攻撃を利用し、SSLサーバ証明書の「偽造」に成功した旨の発表が行われました。
この攻撃手法では、一般的なブラウザ上であたかも正しい認証局であるかのように振舞う認証局を不正に構築し、この認証局から不正なSSLサーバ証明書を発行することによりウェブサイトの「なりすまし」を試みます。
日本ベリサインではこの攻撃によるお客様のビジネスへのリスクを最小限にとどめるため、以下の対処を行います。

※ 尚、この攻撃は、既に発行されたサーバIDを利用した通信の「改ざん」「盗聴」などを可能にするものではありません。お客様のWebサイトにて現在ご利用いただいているグローバル・サーバIDおよびその他全てのサーバIDについて新たなリスクを生じさせるものではございません。

1. **MD5アルゴリズムを利用した全てのSSLサーバ証明書の発行を2009年1月6日（火）以降、停止いたします。**
   対象製品
   「グローバル・サーバID」（日本ベリサイン「ストアフロント」システムから発行分）

   ※ 上記以外のサーバID製品は影響がございません。

2. **上記対象製品の署名アルゴリズムを以下の通り、2009年1月15日（木）以降、MD5から、よりセキュアなSHA-1へ切り替えます。**
   詳細はこちら

   ※ 尚、1月6日から1月15日までの間、対象製品の発行を一時的に保留させていただきます。お客様にはご不便をおかけし大変恐縮ですが、どうぞご理解・ご了承ください。

   - 1月5日以前に申請いただき、1月6日時点で未発行のサーバIDは、1月15日以降に発行させていただきます。
   - また1月6日以降に申請されたサーバIDも同様に、1月15日以降に発行させていただきます。

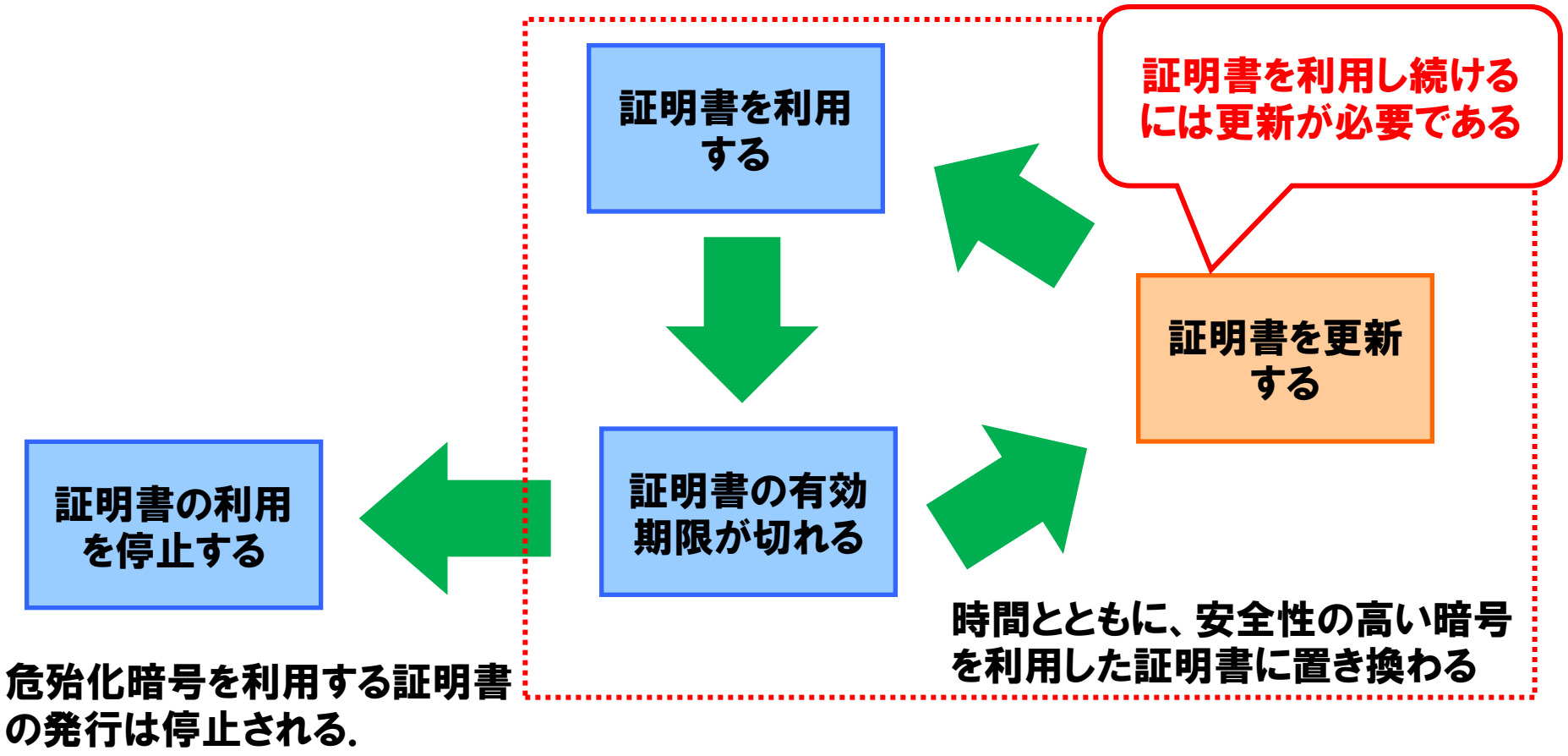
**MD5を利用した証明書の発行を停止**

**証明書ベンダの努力が調査結果に表れたのか・・・？**

**出典：日本ベリサイン，**”MD5**アルゴリズムへの衝突攻撃による**SSL**サーバ証明書の偽造に関する報道について”，**
https://www.verisign.co.jp/ssl/about/20090106.html（2009**年1月6日**）

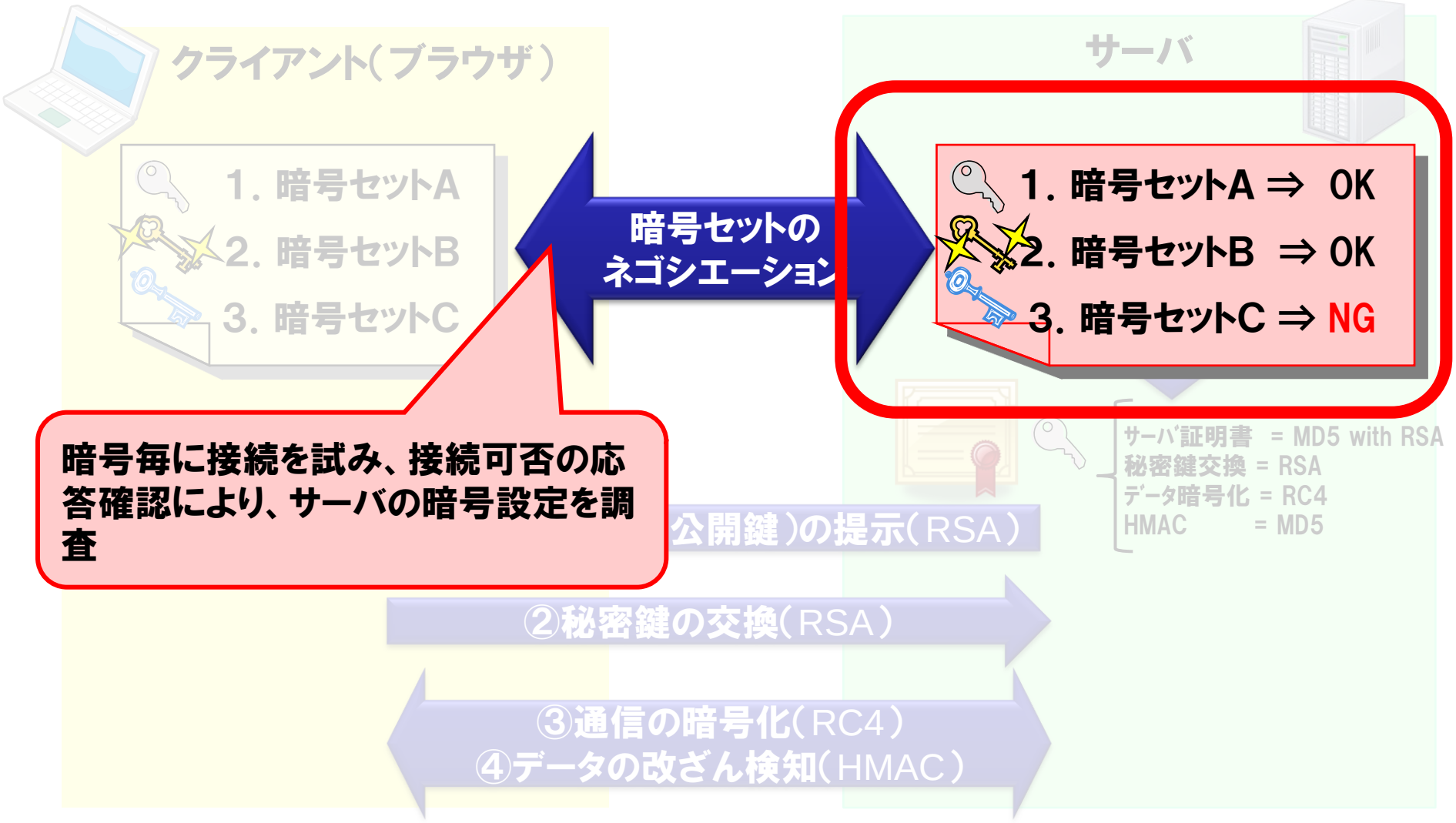
# 調査1：証明書における利用暗号
## 考察(2／2)

**証明書は暗号の世代交代を容易に行える環境にある**



# 調査2： サーバの暗号設定(接続可能暗号)
## 調査方法

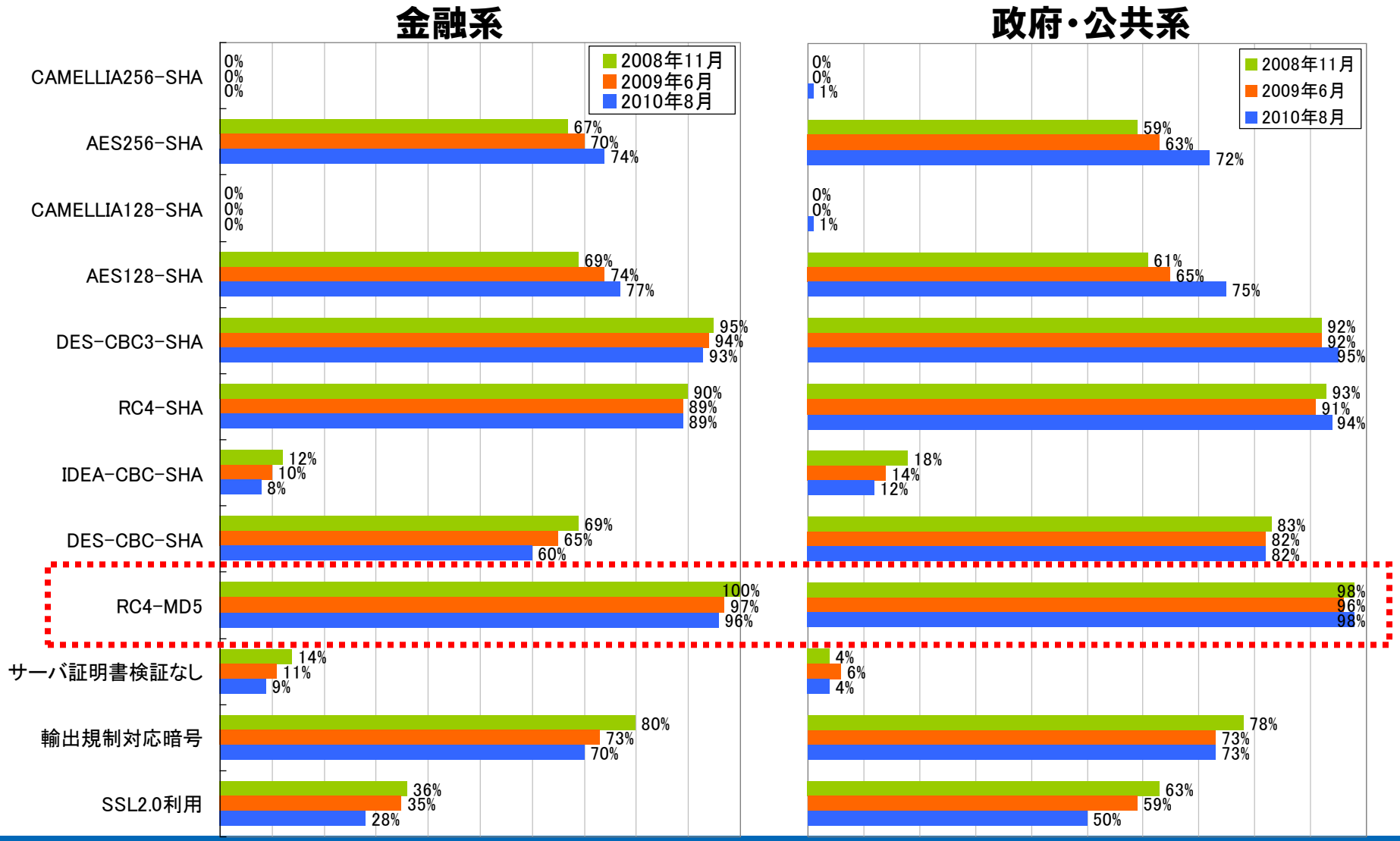
**SSLサーバの暗号設定を調査**



# 調査2： サーバの暗号設定（接続可能暗号）

## 調査結果

**年代で比較：**
- 暗号毎のサーバの暗号設定の大きな変化は無い
- ”RC4-MD5” を利用して接続できるサーバの割合が高いままである



# 調査2：サーバの暗号設定（接続可能暗号）
# 考察（1／2）

Apache 2.2.20 のデフォルト設定 (httpd-ssl.conf )：

SSLCiphersuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

利用可能な暗号一覧
(openssl-0.9.8r)

| | | | | | |
|---|---|---|---|---|---|
| DHE-RSA-AES256-SHA | SSLv3 | Kx=DH | Au=RSA | Enc=AES(256) | Mac=SHA1 | |
| DHE-DSS-AES256-SHA | SSLv3 | Kx=DH | Au=DSS | Enc=AES(256) | Mac=SHA1 | |
| AES256-SHA | SSLv3 | Kx=RSA | Au=RSA | Enc=AES(256) | Mac=SHA | |
| DHE-RSA-AES128-SHA | SSLv3 | Kx=DH | Au=RSA | Enc=AES(128) | Mac=SHA | |
| DHE-DSS-AES128-SHA | SSLv3 | Kx=DH | Au=DSS | Enc=AES(128) | Mac=SHA | |
| AES128-SHA | SSLv3 | Kx=RSA | Au=RSA | Enc=AES(128) | Mac=SHA | |
| EDH-RSA-DES-CBC3-SHA | SSLv3 | Kx=DH | Au=RSA | Enc=3DES(168) | Mac=SHA | |
| EDH-DSS-DES-CBC3-SHA | SSLv3 | Kx=DH | Au=DSS | Enc=3DES(168) | Mac=SHA | |
| DES-CBC3-SHA | SSLv3 | Kx=RSA | Au=RSA | Enc=3DES(168) | Mac=SHA1 | |
| IDEA-CBC-SHA | SSLv3 | Kx=RSA | Au=RSA | Enc=IDEA(128) | Mac=SHA1 | |
| RC4-SHA | SSLv3 | Kx=RSA | Au=RSA | Enc=RC4(128) | Mac=SHA1 | |
| RC4-MD5 | SSLv3 | Kx=RSA | Au=RSA | Enc=RC4(128) | Mac=MD5 | |
| EDH-RSA-DES-CBC-SHA | SSLv3 | Kx=DH | Au=RSA | Enc=DES(56) | Mac=SHA1 | |
| EDH-DSS-DES-CBC-SHA | SSLv3 | Kx=DH | Au=DSS | Enc=DES(56) | Mac=SHA1 | |
| DES-CBC-SHA | SSLv3 | Kx=RSA | Au=RSA | Enc=DES(56) | Mac=SHA1 | |
| DES-CBC3-MD5 | SSLv2 | Kx=RSA | Au=RSA | Enc=3DES(168) | Mac=MD5 | |
| IDEA-CBC-MD5 | SSLv2 | Kx=RSA | Au=RSA | Enc=IDEA(128) | Mac=MD5 | |
| RC2-CBC-MD5 | SSLv2 | Kx=RSA | Au=RSA | Enc=RC2(128) | Mac=MD5 | |
| RC4-MD5 | SSLv2 | Kx=RSA | Au=RSA | Enc=RC4(128) | Mac=MD5 | |
| DES-CBC-MD5 | SSLv2 | Kx=RSA | Au=RSA | Enc=DES(56) | Mac=MD5 | |
| EXP-EDH-RSA-DES-CBC-SHA | SSLv3 | Kx=DH(512) | Au=RSA | Enc=DES(40) | Mac=SHA1 | export |
| EXP-EDH-DSS-DES-CBC-SHA | SSLv3 | Kx=DH(512) | Au=DSS | Enc=DES(40) | Mac=SHA1 | export |
| EXP-DES-CBC-SHA | SSLv3 | Kx=RSA(512) | Au=RSA | Enc=DES(40) | Mac=SHA1 | export |
| EXP-RC2-CBC-MD5 | SSLv3 | Kx=RSA(512) | Au=RSA | Enc=RC2(40) | Mac=MD5 | export |
| EXP-RC4-MD5 | SSLv3 | Kx=RSA(512) | Au=RSA | Enc=RC4(40) | Mac=MD5 | export |
| EXP-RC2-CBC-MD5 | SSLv2 | Kx=RSA(512) | Au=RSA | Enc=RC2(40) | Mac=MD5 | export |
| EXP-RC4-MD5 | SSLv2 | Kx=RSA(512) | Au=RSA | Enc=RC4(40) | Mac=MD5 | export |

デフォルトでは
MD5が利用可能

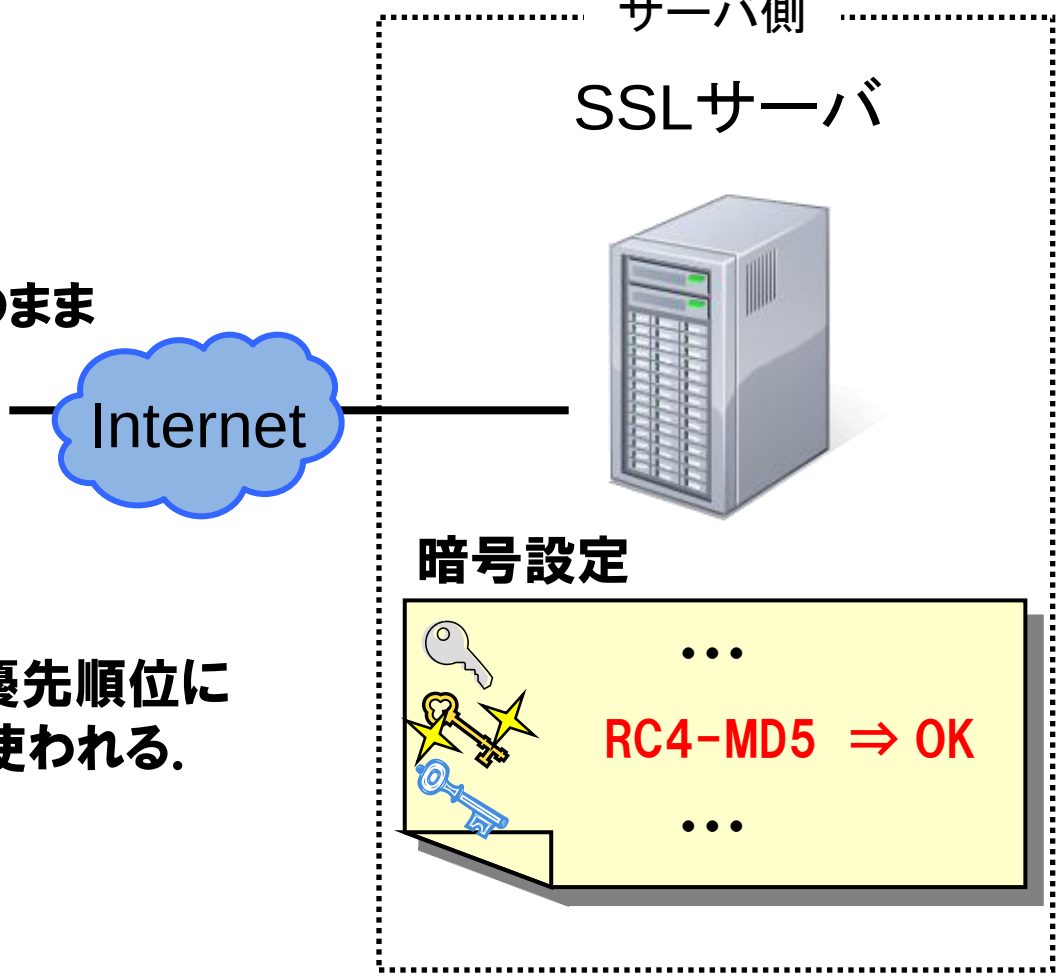
# 調査2:サーバの暗号設定(接続可能暗号)
# 考察(2／2)

**SSLサーバがデフォルト設定のまま運用されている可能性がある**

・RC4-MD5が使用できるサーバの割合が高い.

・SSLサーバがデフォルト設定のまま運用されている可能性がある.

・ブラウザが提示する暗号の優先順位によっては, 危殆化した暗号が使われる.



# 調査3:ブラウザ接続時の利用暗号

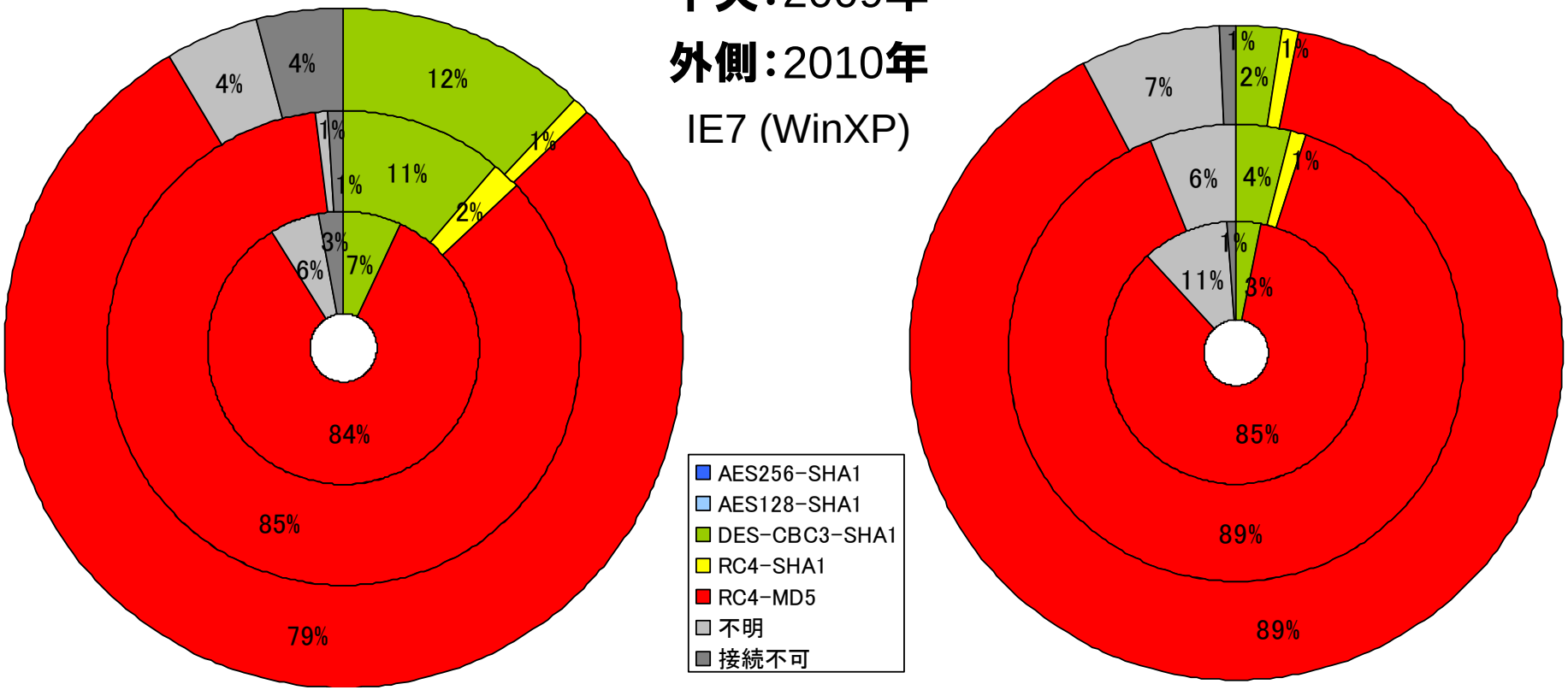
## 調査方法

**ブラウザ接続時に利用される暗号を調査**

# 調査結果3：ブラウザ接続時の利用暗号
# 調査結果（1／3）

IE7 (Win XP)で接続するとき利用される暗号

**年代で比較：**
- “RC4-MD5” の利用率が高いままである

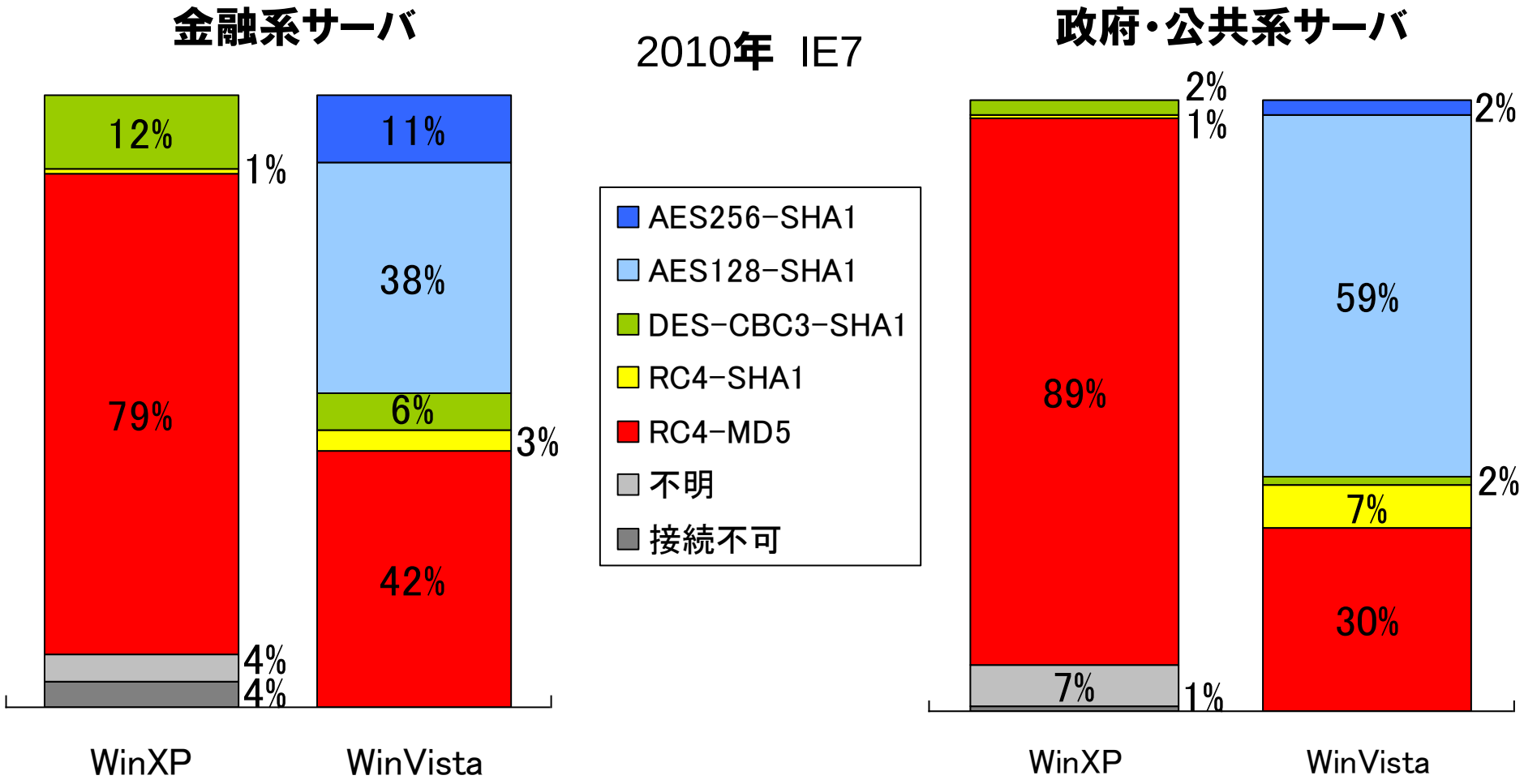


## 調査結果3:ブラウザ接続時の利用暗号

# 調査結果(2／3)

IE7 で接続するとき利用される暗号

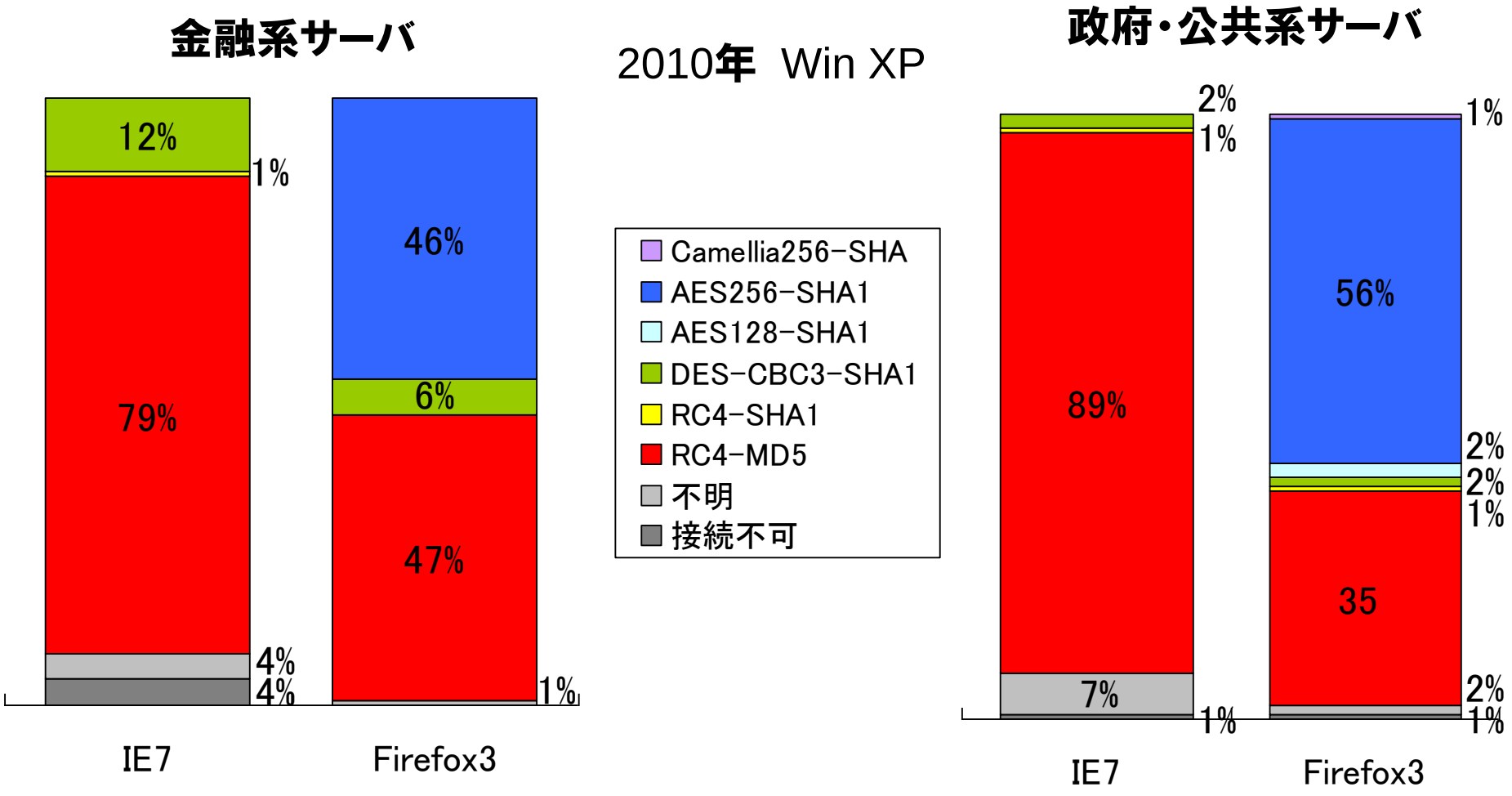
OS間の比較:
- Win XP より Win Vista の方が、安全性が高い暗号を利用する割合が高い



# 調査結果(3／3)

Win XPの環境下で接続するときに利用される暗号

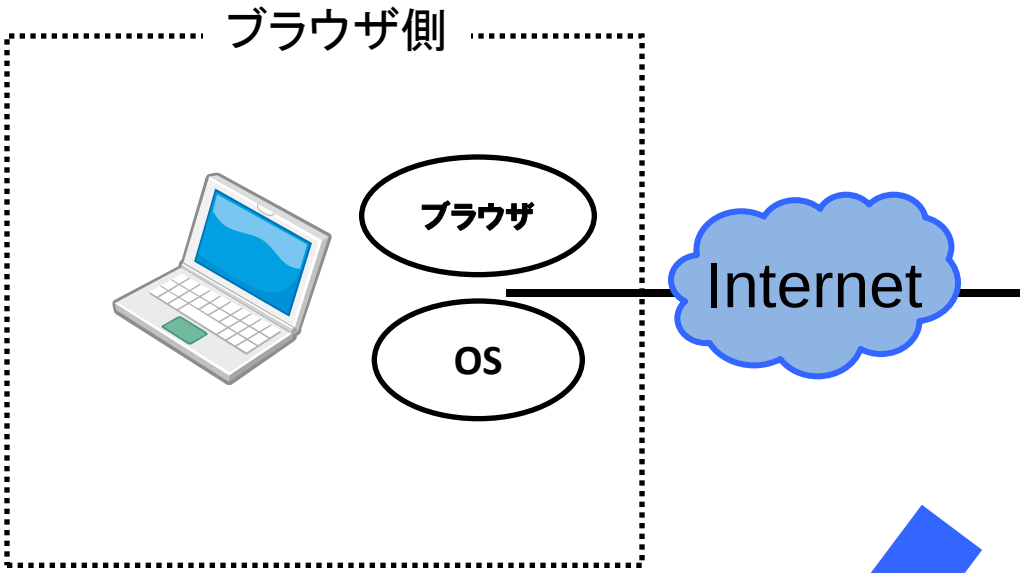
**ブラウザ間の比較:**
- IE7 より Firefox3 の方が、安全性が高い暗号を利用する割合が高い



# 調査結果3：ブラウザ接続時の利用暗号

## 考察

**利用暗号はブラウザ側の環境（ブラウザ、OS）に依存する**
**→ブラウザとOSの組み合わせを考慮した対策が必要**




・ブラウザ側の環境によっては危殆化した暗号が利用される

例：IE7 (Win XP)

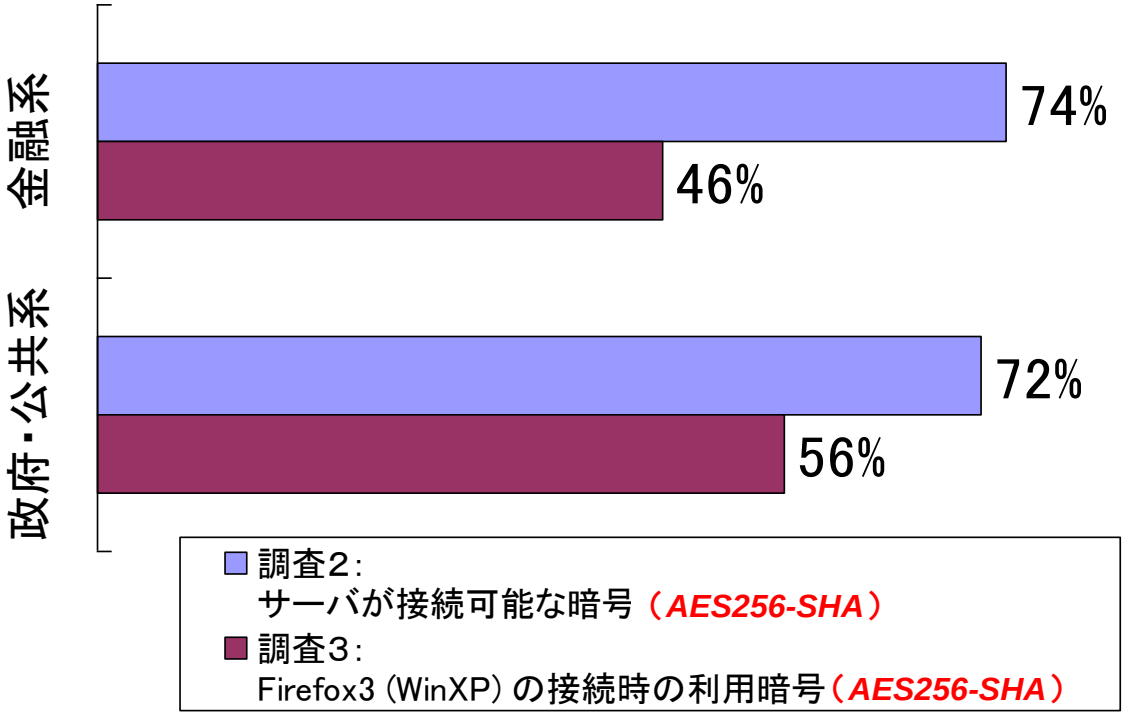
・ブラウザ側での対応により、危殆化した暗号の利用を回避できる場合がある

・OSを変更したくない場合は、IE以外のブラウザを利用すると改善可能

・IEを利用したい場合には、OSのバージョンアップを行えば改善可能

# 暗号の世代交代に向けた対策の考察(１／３)

**サーバの暗号設定と、ブラウザで接続する際に利用する暗号を比較**
**→ブラウザ側の優先順位を無視するサーバが存在**

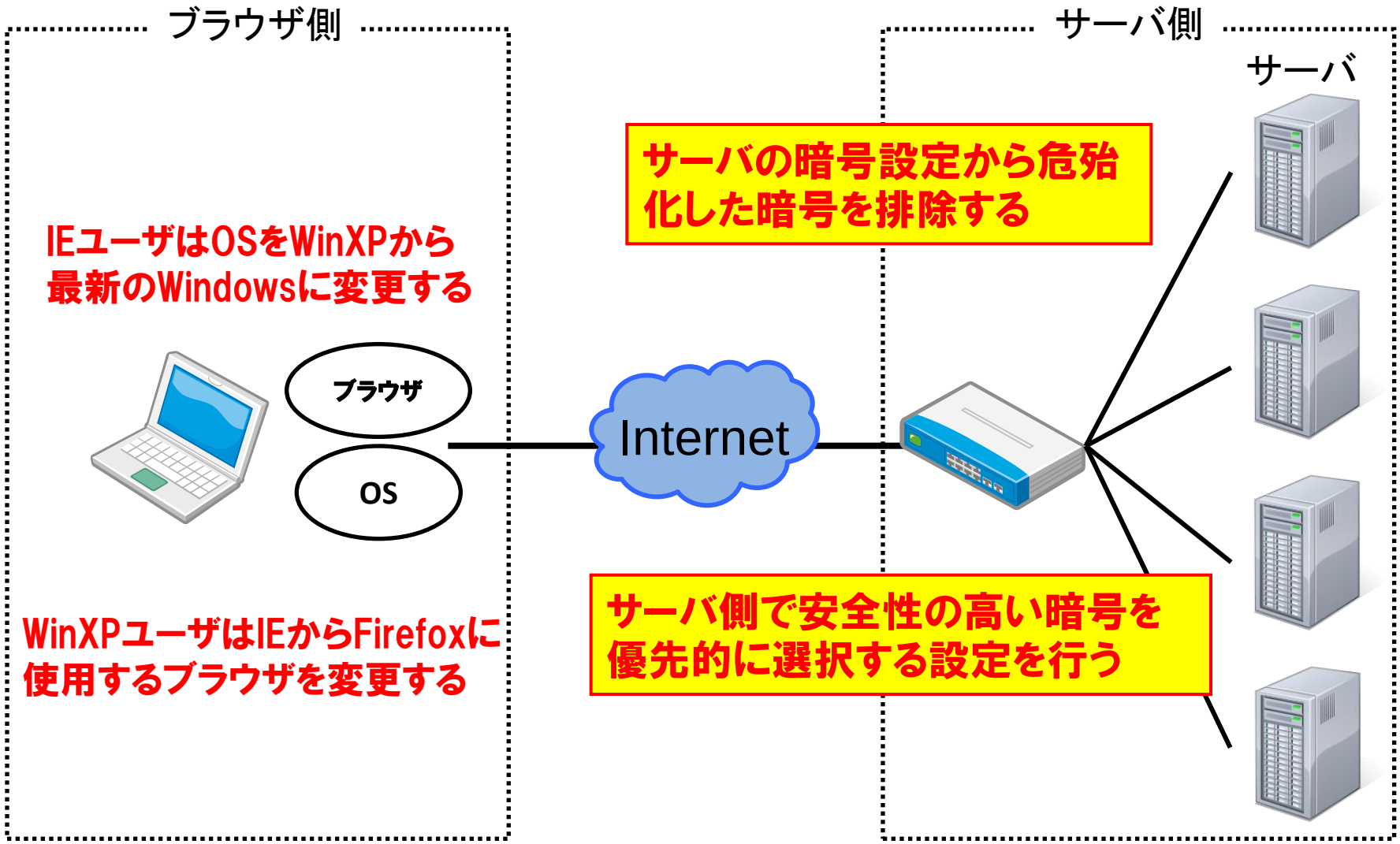



**ブラウザで指定した優先順位よりも下位の暗号セットで接続されるケースが存在**

| 暗号セット指定順序 (Firefox3.5, 3.6) | |
|---|---|
| 1 | TLS_EMPTY_RENEGOTIATION_INFO_SCSV |
| 2 | TLS_ECDHE_ECDSA_WITH_***AES_256_CBC_SHA*** |
| 3 | TLS_ECDHE_RSA_WITH_AES_***256_CBC_SHA*** |
| 4 | TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA |
| 5 | TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA |
| 6 | TLS_DHE_DSS_WITH_***AES_256_CBC_SHA*** |
| 7 | TLS_ECDH_RSA_WITH_***AES_256_CBC_SHA*** |
| 8 | TLS_ECDH_ECDSA_WITH_***AES_256_CBC_SHA*** |
| 9 | TLS_RSA_WITH_CAMELLIA_256_CBC_SHA |
| 10 | TLS_RSA_WITH_***AES_256_CBC_SHA*** |
| 11 | TLS_DHE_RSA_WITH_***AES_256_CBC_SHA*** |
| 12 | TLS_ECDHE_ECDSA_WITH_RC4_128_SHA |
| 13 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA |
| 14 | TLS_ECDHE_RSA_WITH_RC4_128_SHA |
| 15 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA |
| 16 | TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA |
| | … |

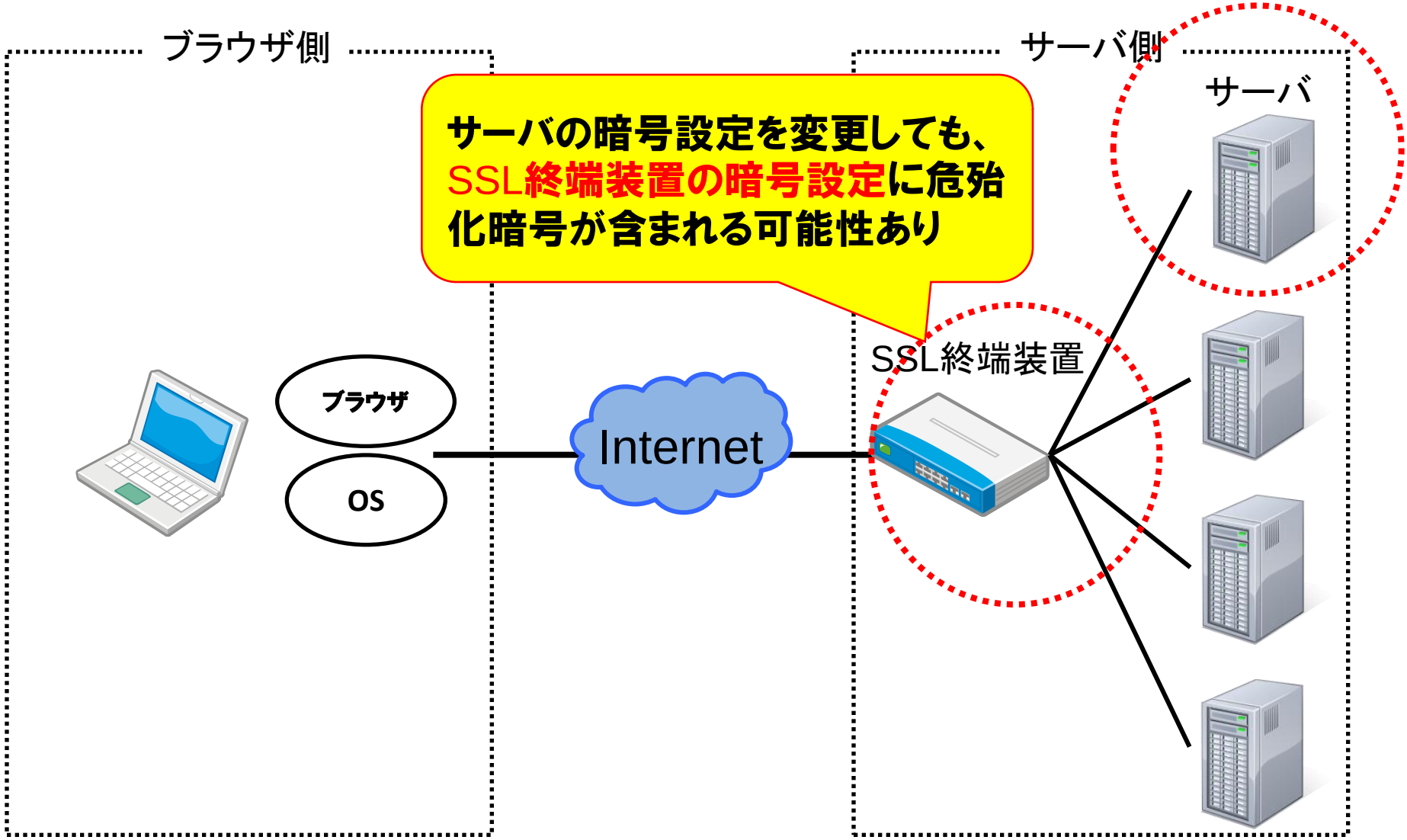
# 暗号の世代交代に向けた対策の考察(２／３)

**サーバ側，ブラウザ側の双方で暗号の危殆化の対策が必要**



# 暗号の世代交代に向けた対策の考察(３／３)

**ブラウザとサーバ以外の暗号設定も考慮する必要がある**



# まとめ

**金融系及び政府・公共系サイトの暗号利用状況の実態把握を行い、暗号の世代交代に向けた対処策を考察した**

**①証明書で使用されている暗号の世代交代は進んでいる**
→ “MD5 with RSA1024” が利用されなくなった

**②サーバの暗号設定における暗号の世代交代は進んでいない**
→ ”RC4-MD5” が利用できるサーバの割合が依然として高いままである

**③ブラウザ側の対応で危殆化した暗号の利用を回避できる場合がある**
→ OS のバージョンアップ（IE7ユーザ）
→ ブラウザの乗り換え（Win XPユーザ）

ブラウザ側の優先順位を無視するサーバが存在

**サーバ側，ブラウザ側の双方で危殆化の対策が必要であり，**
**特に、サーバ側での暗号設定の見直しによる対策が重要**