CRYPTRECシンポジウム2009　パネル2　　2009.2.18

ユーザーから見たCRYPTRECの意義

―― ユーザーと専門家のギャップをどう埋めるか？

日本銀行 金融研究所
情報技術研究センター長
岩下 直行

本資料の内容や意見は発表者個人に属します。日本銀行あるいは金融研究所の公式見解を示すものではありません。

論者の立ち位置と基本的な考え方

【現状認識】 暗号については専門家とユーザーの間の認識のギャップがまだ大きく、どうやってそれを埋めていくかが課題となっている。

- シングルDESの危殆化から2010年問題まで、ユーザーは、暗号アルゴリズムの危殆化問題に大きな影響を受けてきた。
- 電子政府のみならず、広く社会全体で安全な暗号が使われるためには、CRYPTRECなどの専門家が何をすべきか、ユーザーが何をすべきか、を考えたい。
- 必ずしも表に見えている部分だけが問題ではない。
  - 例えば、SHA-1の問題が活発に議論されている一方、未だにMD5が広く使われているのをどう考えるか。
  - ICカードに実装されている暗号の強度をどう考えるべきか。
- その一方で、ユーザーがコストとリスクを勘案して(勝手に)判断してしまっていることをどのように受けとめればよいのか。
  - 必ずしも教条的に「強い暗号に変えるべき」と言うことが正しいとは限らないが、ユーザーが本当にちゃんとリスクが認識できているのかが不安なケースも多い。
  - ユーザー：「システムのセキュリティを暗号だけで守っている訳ではない」
    →では、暗号が危殆化した場合に、本当にそれ以外の対策が有効に働くのか？
- ユーザーが問題を正しく理解し、適切な対応を進めていくために、専門家とユーザーの間の認識のギャップを埋めていくことが必要である。

電子政府推奨暗号リスト

技術分類		名称
公開鍵暗号	署名	DSA, ECDSA, RSASSA-PKCS1-v1_5, RSA-PSS
	守秘	RSA-OAEP, RSAES-PKCS1-v1_5 ※1
	鍵共有	DH, ECDH, PSEC-KEM ※2
共通鍵暗号	64ビットブロック暗号※3	CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, 3-key Triple DES ※4
	128ビットブロック暗号	AES, Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000
	ストリーム暗号	MUGI, MULTI-S01, 128-bit RC4 ※5
その他	ハッシュ関数	RIPEMD-160※6, SHA-1※6, SHA-256, SHA-384, SHA-512
	擬似乱数生成系※7	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1, PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1, PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

※1　SSL3.0/TLS1.0で使用実績があることから当面の使用を認める
※2　KEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism)構成における利用を前提とする
※3　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128ビットブロック暗号を選択することが望ましい
※4　3-key Triple DESは、以下の条件を考慮し、当面の使用を認める
①FIPS46-3として規定されていること　②デファクトスタンダードとしての位置を保っていること
※5　128-bit RC4は、SSL3.0/TLS1.0以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい
※6　新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない
※7　擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である

前回の電子政府推奨暗号リスト選定およびリストの現状に関する総括

- 電子政府推奨暗号リストを選定したことにどのような意義があったか。
  - 10年前、CRYPTREC以前のユーザーは悩んでいた。
    - 得体の知れない独自開発暗号の横行、売り込み。
    - 新旧暗号アルゴリズムの混在。移行の要否。
    - 安全性評価の「基準軸」が定まらない悩み。
- もしもCRYPTRECがなかったら今頃どうなっていたか？
  - 種々雑多な暗号が提案、採用され、混沌とした状態になっていたかも。
  - 電子政府や民間企業が利用した暗号アルゴリズムがアタックされ、そのトラブル対応が深刻な問題になっていたかも。
  - 被害が深刻化すれば、単独の国際標準暗号への統合化がより進んだ可能性も。
- CRYPTRECが電子政府推奨暗号リストを選定したことで、ユーザーが安心して候補暗号を採用できる環境が整った。

電子政府推奨暗号リストの現状についてどのような問題点があったか

- 前回の選定方法に関する反省点
  - 候補暗号の数が多すぎる。
  - 実際には利用できないアルゴリズムも含まれている。
  - 本当に選択肢として考慮すべき候補のリストになっているのか？
- 10年前は、外部評価を受けていない独自暗号を売り込む業者が多数存在していた。良いものとそうでないものをどう見分けるかが問題となり、一定のレベルを達成した暗号を広く候補とすることで、多くの関係者を味方につけることができた。さもなければ、多数の協力を得られず、問題のある暗号を排除することは難しかっただろう。
- しかし、所期の目的を達成した現在、よりユーザーフレンドリーかつ維持管理コストの安い、「限定された推奨暗号リスト」を指向しても良いのではないか。
- その観点からは、「互換性維持暗号」への選別の仕方とその受けとめられ方がポイントとなる。

今後のCRYPTRECの活動について

公募対象のカテゴリーの追加をどう見るか？

- 今回の見直しで新しいカテゴリーが追加された。あまりリストの構造を複雑にしない方が、ユーザーから理解されやすいと思われるので、今後リストに更にカテゴリーを追加することについては慎重な議論が必要では。

CRYPTRECと他の枠組みとの役割分担のあり方

- 例えば、個別用途を意識してリストに更にカテゴリーを追加するよりも、国際・国内標準（ISO/JIS）として規定したほうが自然なものもあると思われる。CRYPTRECだけで完結させるのではなく、外部の枠組みとどう役割分担していくかを検討するべきでは。
- CRYPTRECは、電子政府推奨暗号リストの記載項目を更に増やす方向に進むよりも、基本となる暗号アルゴリズムの評価に特化することで、そのリソースを有効に活用できるのではないか。

専門家とユーザーのギャップを埋めるには

- 食品安全や薬品の認定、交通・航空事故の安全対策等と比較して、暗号の安全性評価は、評価を行う専門家側とユーザー側のギャップが大きい。
  - 専門家側は、ユーザーがどこでどのような暗号を利用しているかを特に知らされない。
  - ユーザー側は専門家の評価結果を時に無視して独自の判断を下す傾向が強い。
  - その結果、評価する専門家側は、「評価基準を厳しいものにして徹底を図りたい」というバイアスがかかり勝ちである。
- この構造は中長期的にみて安定的ではないため、今後は、①専門家側が評価に当たって実務上の影響を分析し、考慮する枠組みを整備するとともに、②ユーザー側が評価結果を実務によりきちんと反映させる体制に、徐々に移行していくことが必要ではないか。