

米国国家安全保障局 (NSA)
暗号アルゴリズムについて
-ハードウェア高速化の進む中で-

最近、IT セキュリティの世界で 2010 年問題、暗号鍵長について話題になっています。パソコンの CPU は Dual Core から Quad Core と大容量、高速処理が可能な時代において、“鍵は長くて複雑なほうが破れない”ほうが当然、情報の暗号化において安心です。鍵長が長いほど鍵の解読に時間が掛かるという単純なものです。話題は RSA 暗号鍵の 1024 ビット、2048 ビット、4096 ビット化となっていますが、RSA 暗号鍵が現在業界標準として使用されていることによります。鍵のビット数が多いということは自動的にハードウェアに掛かる負担が大きいということです。AES は比較的ビット数が低い割に、高い強度が確保できるということで、近年多く用いられるようになって来ています。

今後50年間破られることのない暗号鍵を求めて NSA は暗号アルゴリズムの策定を進めてきましたが、ハードウェアの高速化が進んでいる現在において、鍵が短命になってしまうのは自然の成り行きです。米国国家安全保障局 (NSA) は、高速化が進んでいるハードウェア環境に対処するため推奨暗号アルゴリズムを 2005 年 2 月の RSA Conference において発表しました。

Suite A

国家機密レベル暗号用として使用されるものの一部として以下がありますが、その他のアルゴリズムは一切公開もされておりませんし、詳細も不明です。

ACCORDION
MEDLEY
PEGASUS

Suite B

機密情報及び非機密情報の暗号化に供されインターオペラビリティに重きを置く暗号アルゴリズムのリストであり、構成するアルゴリズムは以下の通りであり用途別に使用され、商業的応用が可能です。RSA コンファレンスで発表された Suite B は AES に加え Hashing, デジタル署名、鍵交換の暗号アルゴリズムを包含した。高速で取扱いが容易な ECC (Elliptic Curve Cryptography) を採用したことが新しい変化です。

AES
ECDSA
ECDH
ECMQV
SHA-256
SHA-384

ECC の特許について

“Secret”レベルの暗号化に用いられる SHA-256 及び 128 ビット鍵とともに用いられる AES があります。“Top Secret”は SHA-384 と 192 ビット鍵とともに AES を使用し暗号化され、AES と SHA はパテントの制約はありませんが ECC はカナダの Certicom 社が楕円曲線技術に多くの特許を有していますが NSA は \$ 25 百万ドルにて 26 の特許を開放させました。NSA は Suite B を使用して IPsec の一部として 2006 年 12 月 IETF に RFC4869 を提出しました。

KK ICH 3-5-17-408 Nishigotanda, Shinagawa, Tokyo 141-0031 Japan
Phone +81-50-3735-0211
<https://www.ich-one.com>

NSA は業界に Suite B を開放し米国政府が使用する製品に使用するのを目的としています。Suite B は暗号アルゴリズムだけを規定するもので最適なシステムのアルゴリズムの組合せは各設計者に委ねられますが以下の要件を満たすものが求められます。

- ソフトウェア、ファームウェア、ハードウェアに供されるアルゴリズムの品質
- 米国政府の鍵交換の使用に準拠していること
- 米国のみ政府情報、核のコントロールとコマンドなどが保護されること
- 国内、国際的にインターオペラビリティがあること

これらはしかしながら、Suite B が規定するものではなく、情報システムの一要素として設計、設置されるものとしてされています。

Suite B の詳細情報は以下から入手してください。

Encryption:	Advanced Encryption Standard (AES) - FIPS 197 (with keys sizes of 128 and 256 bits) http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf *
Digital Signature:	Elliptic Curve Digital Signature Algorithm - FIPS 186-2 (using the curves with 256 and 384-bit prime moduli) http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf *
Key Exchange:	Elliptic Curve Diffie-Hellman or Elliptic Curve MQV Draft NIST Special Publication 800-56 (using the curves with 256 and 384-bit prime moduli) http://csrc.nist.gov/CryptoToolkit/kms/key_schemes-Jan03.pdf *
Hashing:	Secure Hash Algorithm - FIPS 180-2 (using SHA-256 and SHA-384) http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf *

Suite B に関する試験及び認証は以下のようになっています。

=====

The Cryptographic Module Verification Program (CMVP)は FIPS-140-2 に基づき NIST が規定している方法で行われる。Suite B に基づき採用され、組み込まれた暗号の試験に限り評価及び承認される。詳細は：
<http://csrc.nist.gov/cryptval/>

The Common Criteria Evaluation and Validation Scheme (CCEVS)は NSA 及び NIST で管理され Information Assurance 製品につき The Common Criteria for Information Technology Security Evaluation (CC), ISO/IEC 15408 で試験を行うことを規定している。(firewalls, smart cards, operating systems 等)が対象製品)
詳細は：<http://www.niap-ccevs.org/cc-scheme>

National Security Agency による評価は政府内の機密情報に関して各種規定に基づき行われる。Suite B に関する試験はこの試験からすると一部である。

1024 ビットの鍵長につき Suite B ではより長い鍵長を使用して、楕円曲線技術を使用しても良いことになっている。カナダの Certicom 社からのライセンスを解放させているので、各ベンダーは楕円曲線技術を自由に使用して製品を設計できる。

詳細は：<http://www.nsa.gov/ia/industry/cep.cfm>

鍵の管理

鍵の交換について、Suite B は Elliptic Curve Diffie-Hellman Key Exchange (ECDH) または ECMQV プロトコルを使用することを定めています。ECDH は現行のインターネットプロトコル、IKE, TLS, S/MIME にも適合しています。ECMQV は音声などの暗号化に最適と考えられています。NSA は商業的、及び政府のニーズに使用される幅広い PKI を基にした製品の開発を奨励しており米国で始めて **Suite B** を採用し製品化したのは**米国 Spyrus 社**です。

CNSSP-15 は TOPSECRET を扱うにも 192 ビット AES 鍵で十分であるとしおり、**Suite B** は 256 ビットを使用しインターオペラビリティの強化を図っています。NSA は EAL Level 4 以上の CCEVS ですべての評価を行います。これは Menezes, Qu, 及び Vanstone (MQV) 鍵交換の楕円曲線の変数です。

Suite B 用途と特許

基本的には政府が使用する製品に使用されるが結果商業的暗号システムの一部として IPsec などに用いることが出来る。使用する際に NSA とライセンス契約を結び使用する。許可なくとも個別に使用できますが、販売や配布は禁じられています。ベンダーは NSA とのライセンス契約が必要で、基本的には米国政府用途に開発された暗号、PKI 製品となります。

米国市場

2006 年よりいち早く Suite B を製品に採用したのは米国 Spyrus 社で、多くのベンダーが採用を予定している。Safenet 社、n-Cypher 社、AEP 社等のベンダーも Suite B 対応製品を計画中でのようです。高速化とサーバー負担を掛けない新しいアルゴリズム群 Suite B は今後多くのシステムに採用されると考えられます。

米国政府の製品採用基準は暗号鍵が 50 年間破られないことが挙げられています。ECC の暗号強度は正にこの要求に合わせて採用されたものとして注目されます。

以上簡単な調査結果ですが、ご質問ございましたら、ich-info@ich-one.com までお願いします。

株式会社アイシーエイチ