■1 群（信号・システム）- 3 編（暗号理論）

15 章 標準化

（執筆者：近澤　武）[2008 年 11 月 受領]

■概要■

【本章の構成】

■1 群 - 3 編 - 15 章

15-1 各国／地域の標準化動向

（執筆者：近澤　武）［2008 年 11 月 受領］

15-1-1 米　国

(1) AES

AES（Advanced Encryption Standard）は, 米国の次世代標準暗号アルゴリズムである．従来, 米国連邦標準 FIPS（Federal Information Processing Standard）として DES（Data Encryption Standard）[1]を長年使用してきたが, 近年 DES の安全性や信頼性が低下してきたため, DES を 3 回繰り返す Triple DES（TDEA: Triple Data Encryption Algorithm が正式名称）[2]が FIPS46-3 として制定された．しかし，その Triple DES は，DES の三段重ねのために，安全性が向上した一方で，性能（処理速度）が低下した．そこで，新しい次世代の暗号アルゴリズムが必要とされるようになった．

1997 年, 米国商務省の技術標準化組織 NIST（National Institute of Standards and Technology）が AES の選定プロジェクトを開始した[3]．AES の技術的要求仕様は，共通鍵（ブロック）暗号であること，ブロックサイズが 128 ビットをサポートしていること，鍵長が 128 ビット，192 ビット，256 ビットの 3 種類をサポートしていることである．評価選定は二段階で行い，ラウンド 1（第一段階）で応募暗号アルゴリズムを振るいにかけて絞り，ラウンド 2（第二段階）で絞られた暗号アルゴリズムから AES を選定するプロセスである．

1998 年 8 月，NIST は応募された 15 の暗号アルゴリズムを公表し，1999 年 8 月，最終候補（Finalist Algorithms）として，MARS，RC6，Rijndeal，Serpent，Twofish の五つを発表した．そして，2000 年 10 月，NIST は Rijndeal を AES として選出した．FIPS のドラフト文書へのパブリックコメントを募集後，2001 年 11 月に AES が正式に FIPS197[4]として制定された．

(2) 新しいハッシュ関数

現在，米国政府は SHA-1 や SHA-2（SHA-224, SHA-256, SHA-384, SHA-512）をハッシュ関数の標準 FIPS-180-2[5]及び Change Notice 1[6]で制定している．一方，近年 SHA-1 や SHA-2 以外のハッシュ関数が攻撃されており，SHA-1 に関しても深刻な攻撃法も発表された．

このため，NIST は新しいハッシュ関数を AES と同様なプロセスで 2012 年までに制定することを決定し[7]，2008 年 10 月末に応募が締め切られた．

■1 群 - 3 編 - 15 章

15-2 欧　州

（執筆者：近澤　武）[2008 年 11 月 受領]

15-2-1 NESSIE

NESSIE（New European Schemes for Signatures, Integrity and Encryption）[8]は，欧州委員会（EC: European Commission）の情報社会技術プログラム（Information Societies Technology Programme）の一つとして，2000 年から 2002 年の 3 年間実施されたプロジェクトである．米国の AES 選定とは異なり，ブロック暗号だけでなく，ストリーム暗号，公開鍵暗号，署名認証方式，ハッシュ関数，擬似ランダム関数など，暗号部品に関する多くのカテゴリで，推奨リストを作成した．推奨リストを作成するための選定基準は，安全性，市場の要求，性能，柔軟性の四つである．選定は，AES と同様，二段階（フェーズ I とフェーズ II）で行い，途中，3 回のワークショップを開催．

2003 年 2 月に最終選考結果が発表された（表 15･1）．

表 15･1　NESSIE 最終選考アルゴリズム

- **ブロック暗号（応募 19 件）**
  - MISTY1（三菱電機）
  - Camellia（NTT、三菱電機）
  - SHACAL-2（フランス）

  AES（FIPS 197）
- **ストリーム暗号（応募 6 件）**
  - 選定なし
- **公開鍵暗号（応募 9 件）**
  - ACE Encrypt（スイス）
  - PSEC-KEM（NTT）
  - RSA-KEM（ISO/IEC 18033-2）
- **メッセージ認証アルゴリズム及びハッシュ関数（応募 3 件）**
  - Two-Track-MAC（ベルギー，ドイツ）
  - UMAC（米国，イスラエル）
  - CBC-MAC（ISO/IEC 9797-1）
  - HMAC（ISO/IEC 9797-1）
  - Whirpool（ブラジル，ベルギー）
  - SHA-256, SHA-384, SHA-512（FIPS 180-2）
- **電子署名（応募 7 件）**
  - ECDSA（米国，カナダ）
  - RSA-PSS（スウェーデン，米国）
  - SFLASH（フランス）
- **識別方式（応募 1 件）**

■1 群 - 3 編 - 15 章

15-3 日　本

（執筆者：近澤　武）[2008 年 11 月 受領]

15-3-1 CRYPTREC

CRYPTREC[9]は，日本の電子政府における適切な暗号利用を図るために，2000 年度から通商産業省（当時）が実施している（2001 年度からは，総務省と経済産業省の合同）プロジェクトである．正式な名称は，「暗号技術評価委員会」である．作成されたリストは，電子政府で使用する暗号アルゴリズム選定の際の参考情報となっている．

評価対象とする暗号技術は，公開鍵暗号，共通鍵暗号（ブロック暗号，ストリーム暗号），ハッシュ関数，擬似乱数生成であり，基本的には，応募された暗号技術を対象にスクリーニング評価と詳細評価の二段階で評価を行った．また，応募された暗号技術以外にも，「暗号技術評価委員会」独自に，電子政府システムを構築するために必須と判断した暗号技術や「電子署名法」関連で定めた暗号技術に対する評価も行った．

2003 年 3 月に電子政府推奨暗号リストが提示され，各省庁の合意及び調達への反映が行われている．

表 15･2　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
	鍵共有	DH
		ECDH
		PSEC-KEM
共通鍵暗号	64 ビットブロック暗号	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES
	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
その他	ハッシュ関数	RIPEMD-160
		SHA-1
		SHA-256
		SHA-384
		SHA-512
	議事乱数生成系	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 群 - 3 編 - 15 章

15-4 国　際

（執筆者：近澤　武）［2008 年 11 月 受領］

15-4-1 ISO/IEC

ISO/IEC JTC1/SC27（International Organization for Standardization（国際標準化機構）/International Electrotechnical Commission（国際電気標準化会議）Joint Technical Committee 1/Sub Committee 27 — 以下，ISO と略す）[10]では，情報セキュリティに関する標準化を行っている．現在，電子署名，認証手順，暗号化の際に必要な鍵の管理等の規格がある．一方，過去に ISO では，DES を国際規格化しようとした際に，米国から輸出規制や強度評価の困難性を理由に反対があったため，標準化を中止し，暗号アルゴリズムの登録制に切り替えた経緯があり，最近まで ISO では暗号アルゴリズムの標準化は行われていなかった．

だが，2000 年にようやく ISO でも 18033 という番号の新プロジェクトが発足し，暗号アルゴリズムの標準化に着手した．ISO/IEC 18033 のプロジェクトは四つのパートから構成され，パート 1 は総論，パート 2 は公開鍵暗号，パート 3 はブロック暗号，パート 4 はストリーム暗号をそれぞれ規格化した．現在，ストリーム暗号のいくつかのアルゴリズムを追加する追補文書（Amendment）作成の作業中である．また，2008 年 10 月にブロック暗号とストリーム暗号の改訂が決定し，新アルゴリズムの追加，掲載アルゴリズムの削除も今後予想される．

表 15･3　暗号アルゴリズムの種類

暗号アルゴリズムの種類		カテゴリ	アルゴリズム名（提案国）
公開鍵暗号（ISO/IEC 18033-2）		ElGamal 方式に基づく KEM（鍵カプセル化機構）	ECIES-KEM（米国）
			PSEC-KEM（日本）
			ACE-KEM（ドイツ）
		RSA 方式に基づく非対称暗号/KEM	RSAES（スウェーデン，米国）
			RSA-KEM（スウェーデン，米国）
		モジュラー平方演算に基づく暗号	HIME(R)（日本）
共通鍵暗号	ブロック暗号	64 ビットブロック暗号	TDEA（米国）
			MISTY1（日本）
			CAST-128（カナダ）
		128 ビットブロック暗号	AES（米国）
			Camellia（日本）
			SEED（韓国）
	ストリーム暗号（ISO/IEC 18033-4）	鍵ストリーム生成専用アルゴリズム	MUGI（日本）
			SNOW 2.0（スウェーデン）

また，最近，Signcryption の標準化が開始され，Lightweight cryptography の標準化作業も検討されている．

15-4-2 その他

インターネット関連技術の標準化を推進している IETF（Internet Engineering Task Force）

[11]は，メーリングリストや年 3 回の会合を中心に活動している．IETF には八つのエリアがあるが，その一つのセキュリティには，IPSec（IP Security Protocol），PKIX（Public-Key Infrastructure（X.509）），TLS（Transport Layer Security）などのワーキンググループがある．

第 3 世代移動通信（携帯電話）システム IMT-2000（International Mobile Telecommunications-2000）の標準化を行っている 3GPP（3rd Generation Partnership Project）[12]や 3GPP2（3rd Generation Partnership Project 2）[13]にもセキュリティを議論するワーキンググループがある．IMT-2000 は，世界に先駆けて，2001 年 10 月より日本で本サービスが開始された．IMT-2000 の特徴として，グローバルローミングの実現，動画などマルチメディアに対応できる端末の採用，地上回線並の高品質なサービスの提供などがあげられるが，更に，ユーザ保護を目的とした，高度なセキュリティ技術やプライバシー保護技術の採用が求められた．こうした要望に応えるため，IMT-2000 の一つである W-CDMA（Wideband-Code Division Multiple Access; 正式名称は DS（Direct Spread）-CDMA（直接拡散符号分割多元接続））方式の仕様策定に携わる 3GPP では，日本の暗号アルゴリズム MISTY1 をベースに携帯電話用にカスタマイズした暗号アルゴリズム KASUMI を採用した[14]．KASUMI は，W-CDMA 方式の無線区間の基本的な暗号化技術（秘匿及びメッセージ認証）として使用されている．

■参考文献

1) “National Institute of Standards and Technology,” Data Encryption Standard (DES), Federal Information Processing Standards Publication, vol.46, no.2, 1993.
2) “National Institute of Standards and Technology,” Data Encryption Standard (DES), Federal Information Processing Standards Publication, vol.46, no.3, 1999.
3) http://www.nist.gov/aes（2008.11.12 確認）
4) “National Institute of Standards and Technology,” Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication, vol.197, Nov. 2001.
5) “National Institute of Standards and Technology,” Secure Hash Standard, Federal Information Processing Standards Publication vol.180, no.2, 2002.
6) “National Institute of Standards and Technology,” Secure Hash Standard Change Notice 1, Federal Information Processing Standards Publication, vol.180, no.2 Change Notice 1, 2004.
7) http://www.nist.gov/hash-competition （2008.11.12 確認）
8) http://www.cryptonessie.org（2008.11.12 確認）
9) http://www.cryptrec.jp（2008.11.12 確認）
10) http://www.jtc1sc27.din.de/en（2008.11.12 確認）
11) http://www.ietf.org（2008.11.12 確認）
12) http://www.3gpp.org（2008.11.12 確認）
13) http://www.3gpp2.org（2008.11.12 確認）
14) 近澤武，松井充, “日本発の技術を 3GPP が採用 アルゴリズム「KASUMI」の全貌，”『モバイルインターネット最前線』，日経 BP 社，pp.194-199，Sep. 2000.