CRYPTREC
Cryptography Research and Evaluation Committees

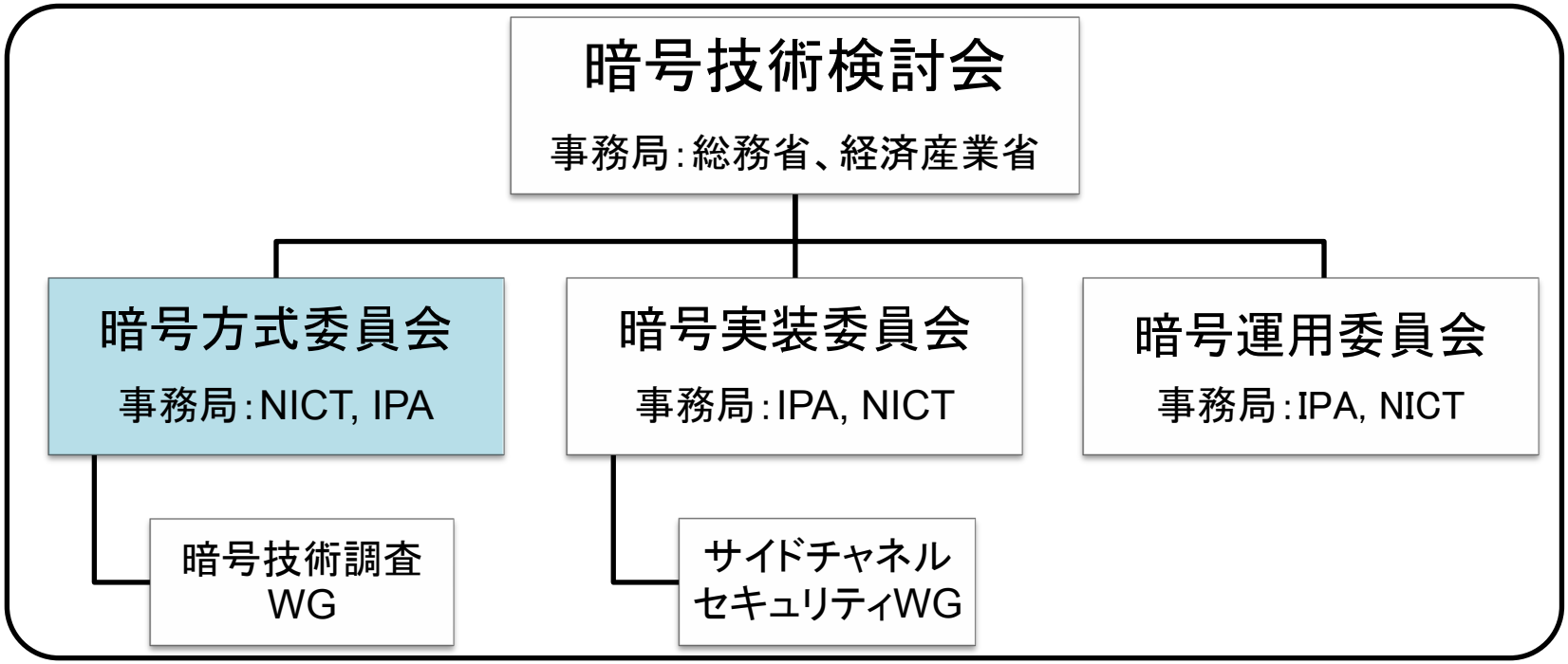
暗号方式委員会活動報告

委員長　今井 秀樹

中央大学

暗号方式委員会

- 電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討を行う。
- 暗号方式委員会は、2003～2008年度に設置された暗号技術監視委員会の後継委員会として、2009年度に設置された。



2012年度暗号方式委員会委員

委員長	今井　秀樹	中央大学 理工学部電気電子情報通信工学科
顧問	辻井　重男	中央大学 研究開発機構
委員	太田　和夫	国立大学法人電気通信大学 情報理工学研究科
委員	金子　敏信	東京理科大学 理工学部電気電子情報工学科
委員	佐々木　良一	東京電機大学 未来科学部情報メディア学科
委員	高木　剛	国立大学法人九州大学 マス・フォア・インダストリ研究所
委員	松本　勉	国立大学法人横浜国立大学 環境情報研究院
委員	盛合　志帆	独立行政法人情報通信研究機構 ネットワークセキュリティ研究所
委員	山村　明弘	国立大学法人秋田大学 工学資源学研究科
委員	渡辺　創	独立行政法人産業技術総合研究所 セキュアシステム研究部門

今回のリスト改定

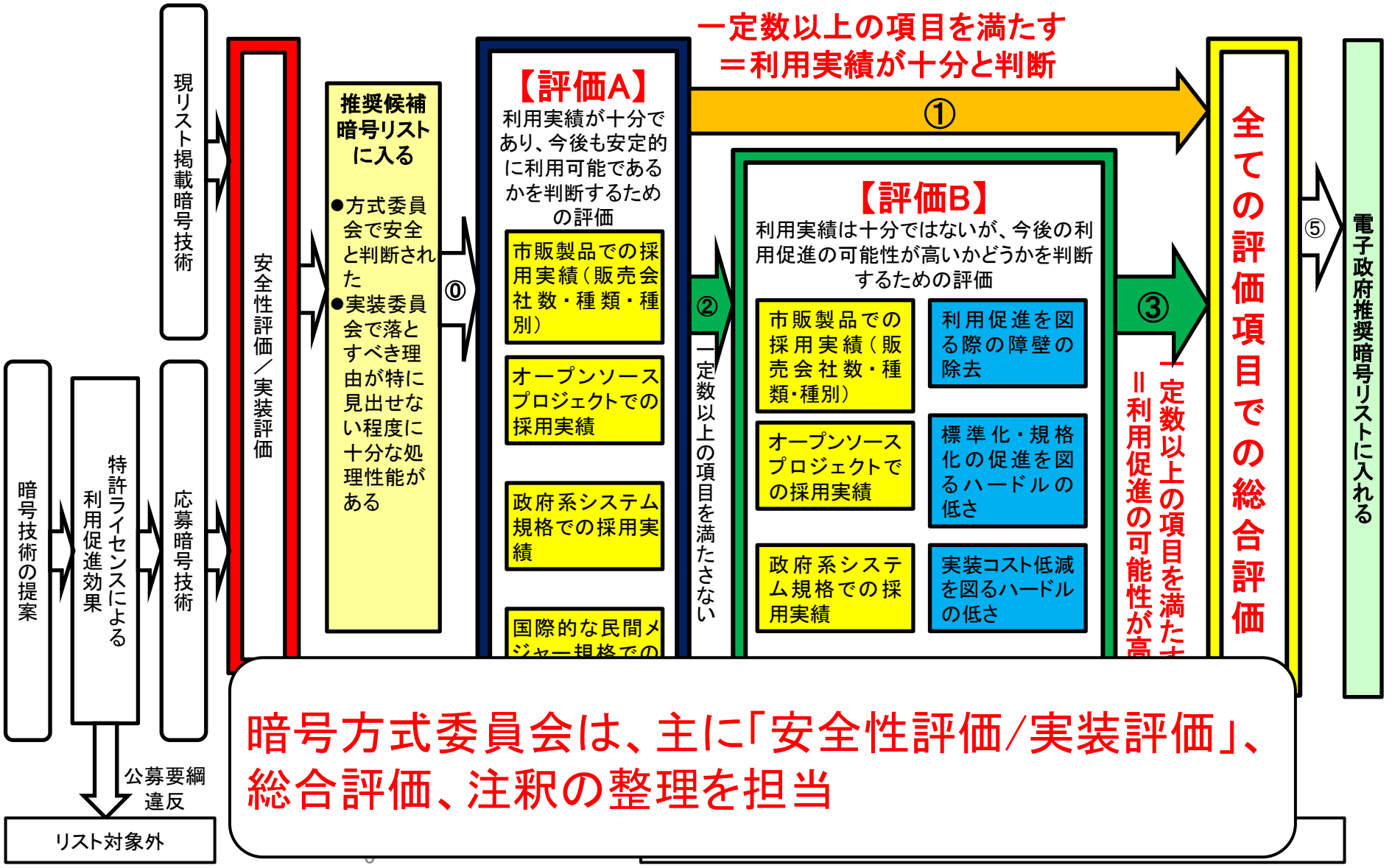
対象となった暗号技術

- 電子政府推奨暗号リスト(2003年)に掲載されている暗号技術
- 2009年度応募暗号技術
- 事務局選出暗号技術
  - 暗号利用モード、メッセージ認証コード、エンティティ認証

暗号利用モード	CBC,CFB,OFB,CTR,CCM,GCM
メッセージ認証コード	CBC-MAC,CMAC,HMAC
エンティティ認証	ISO/IEC 9798-2,ISO/IEC 9798-3, ISO/IEC 9798-4

リスト改定における暗号方式委員会の役割

CRYPTREC
Cryptography Research and Evaluation Committees



暗号方式委員会は、主に「安全性評価/実装評価」、総合評価、注釈の整理を担当

CRYPTREC暗号リスト
電子政府推奨暗号リスト

CRYPTREC
Cryptography Research and Evaluation Committees

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号	3-key Triple DES
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

CRYPTREC暗号リスト
推奨候補暗号リスト

CRYPTREC Cryptography Research and Evaluation Committees

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM
共通鍵暗号	64ビットブロック暗号	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01
ハッシュ関数		該当なし
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
エンティティ認証		ISO/IEC 9798-4

CRYPTREC暗号リスト
運用監視暗号リスト

CRYPTREC Cryptography Research and Evaluation Committees

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号	該当なし
	128ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4
ハッシュ関数		RIPEMD-160
		SHA-1
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		CBC-MAC
エンティティ認証		該当なし

安全性評価/実装評価における判定

対象となった暗号技術

- 電子政府推奨暗号リスト(2003年)に掲載されている暗号技術
- 2009年度応募暗号技術
- 事務局選出暗号技術

CRYPTREC暗号リスト

電子政府推奨暗号リスト（2013年）

推奨候補暗号リスト

運用監視暗号リスト
RSAES-PKCS1-v1_5,
SHA-1, RIPEMD-160,
128-bit RC4,
CBC-MAC

リスト対象外
第一次選考を通過しなかった
2009年度応募暗号技術

運用監視暗号リスト掲載の理由

RSAES-PKCS1-v1_5	Bleichenbacherの攻撃といった現実的な攻撃が存在するため
SHA-1 RIPEMD-160	本暗号技術のハッシュ長は160ビットであり、安全性の観点から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め
128-bit RC4	同じ平文を各々別々の鍵で暗号化しブロードキャストするような場合において、安全性に係る問題が報告されているため
CBC-MAC	メッセージ長が固定の場合、MACとして安全であるが、メッセージ長が可変の場合、容易にMACの偽造が出来るため

電子政府推奨暗号リスト 注釈の整理

CRYPTREC Cryptography Research and Evaluation Committees

RSA-PSS RSASSA-PKCS1-v1_5 RSA-OAEP	「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」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。 http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf （平成25年3月1日現在）
64ビットブロック暗号	より長いブロック長の暗号が利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(†)。
3-key Triple DES	3-key Triple DESは、以下の条件を考慮し、当面の利用を認める(†)。 1） NIST SP 800-67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。
GCM	初期化ベクトル長は96ビットを推奨する。

(†)改定前の注釈とほぼ同じ

推奨候補暗号リスト 注釈の整理

CRYPTREC
Cryptography Research and Evaluation Committees

PSEC-KEM	KEM (Key Encapsulating Mechanism) – DEM (Data Encapsulating Mechanism) 構成における利用を前提とする(†)。
64ビットブロック暗号	より長いブロック長の暗号が利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(†)。
MULTI-S01	平文サイズは64ビットの倍数に限る。

(†)改定前の注釈とほぼ同じ

運用監視暗号リスト注釈の整理（1）

CRYPTREC Cryptography Research and Evaluation Committees

RSAES-PKCS1-v1_5	「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」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。 http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf （平成25年3月1日現在） SSL 3.0 / TLS 1.0, 1.1, 1.2で利用実績があることから当面の利用を認める(†)。
128-bit RC4	128-bit RC4は、SSL（TLS 1.0以上）に限定して利用すること(†)。

(†)改定前の注釈とほぼ同じ

運用監視暗号リスト
注釈の整理（2）

CRYPTREC
Cryptography Research and Evaluation Committees

SHA-1	「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」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。 http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf （平成25年3月1日現在）
CBC-MAC	安全性の観点から、メッセージ長を固定して利用すべきである。

CRYPTREC新体制

暗号技術検討会

事務局：総務省、経済産業省

暗号技術評価委員会

事務局：NICT, IPA

- 「暗号技術の安全性評価を中心とした技術的な検討課題」を担当
- 暗号方式委員会の全部及び暗号実装委員会の一部からの課題を主に引き継ぐ

暗号技術活用委員会

事務局：IPA, NICT

- 「セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討課題」を担当
- 暗号運用委員会の全部及び暗号実装委員会の一部からの課題を主に引き継ぐ

暗号技術評価委員会の活動計画

①暗号技術の安全性に係る監視及び評価

②暗号技術の安全な利用方法に係る調査

③新世代暗号に係る調査

2013年度以降の活動計画
①暗号技術の安全性に係る監視及び評価

CRYPTREC
Cryptography Research and Evaluation Committees

- 検討が予定されているもの：
  - 推奨候補暗号リストへの新規暗号の追加
  - 既存の技術分類の修正を伴わない新技術分類の追加
  - 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格
  - 運用監視暗号リストからの危殆化が進んだ暗号の削除

2013年度以降の活動計画
②暗号技術の安全な利用方法に係る調査

CRYPTREC
Cryptography Research and Evaluation Committees

- 暗号技術の安全な利用方法に関するWGの設置を検討
  - 電子政府システムにおけるセキュリティを確保するために、CRYPTREC暗号リストに掲載されている暗号技術を利用する際の技術的ガイドラインを作成

2013年度以降の活動計画
③新世代暗号に係る調査

CRYPTREC
Cryptography Research and Evaluation Committees

- 新世代暗号の公募、安全性評価を検討（軽量暗号、耐量子計算機暗号、ペアリング暗号等）
- 暗号解読能力評価WGの設置を検討
  - 計算機能力評価WGの後継
  - 検討予定
    - 離散対数問題の困難性に関する調査
    - 格子問題等の困難性に関する調査
- 軽量暗号WGの設置を検討
  - 検討予定
    - 軽量暗号技術に求められる要求条件や評価方法
    - どのアプローチが望ましいか
      - 技術ガイドライン発行／共同開発／公募（海外連携も視野に入れるかどうか）等

おわりに

- これまでCRYPTRECに係る暗号技術に対して、
  - 延べ約300人の暗号研究者により200本以上もの技術報告書（その多くが安全性評価）
  - 暗号方式委員会による10年間以上の監視活動
  - WGによるRSA-1024、SHA-1などの危殆化予測

電子政府推奨暗号リストの信頼性は多くの暗号研究者によって支えられてきた

- 今後も引き続きCRYPTREC暗号リストの安全性の維持のため、皆様の協力が必要

付録:暗号技術名(フルスペル)一覧

電子政府推奨暗号リスト

技術分類		名称	フルスペル
公開鍵暗号	署名	DSA	**D**igital **S**ignature **A**lgorithm
		ECDSA	**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm
		RSA-PSS	**RSA**-**P**robabilistic **S**ignature **S**cheme
		RSASSA-PKCS1-v1_5	**RSA S**ignature **S**cheme with **A**ppendix, **P**ublic-**K**ey **C**ryptography **S**tandards#**1 v**ersion **1.5**
	守秘	RSA-OAEP	**RSA**-**O**ptimal **A**symmetric **E**ncryption **P**adding
	鍵共有	DH	**D**iffie–**H**ellman
		ECDH	**E**lliptic **C**urve **D**iffie-**H**ellman
共通鍵暗号	64ビットブロック暗号	3-key Triple DES	**D**ata **E**ncryption **S**tandard
	128ビットブロック暗号	AES	**A**dvanced **E**ncryption **S**tandard
		Camellia	
	ストリーム暗号	KCipher-2	
ハッシュ関数		SHA-256	**S**ecure **H**ash **A**lgorithm
		SHA-384	
		SHA-512	
暗号利用モード	秘匿モード	CBC	**C**ipher **B**lock **C**haining mode
		CFB	**C**ipher **F**eed**B**ack mode
		CTR	**C**oun**T**e**R** mode
		OFB	**O**utput **F**eed**B**ack mode
	認証付き秘匿モード	CCM	**C**ounter with **C**BC-**M**AC
		GCM	**G**alios/**C**ounter **M**ode
メッセージ認証コード		CMAC	**C**ipher-based **M**essage **A**uthentication **C**ode
		HMAC	**H**ash-**b**ased **M**essage **A**uthentication **C**ode
エンティティ認証		ISO/IEC 9798-2	
		ISO/IEC 9798-3	

付録:暗号技術名(フルスペル)一覧

推奨候補暗号リスト

技術分類		名称	フルスペル
公開鍵暗号	署名	該当なし	
	守秘	該当なし	
	鍵共有	PSEC-KEM	**P**rovably **S**ecure **E**lliptic **C**urve encryption-**K**ey **E**ncapsulation **M**echanism
共通鍵暗号	64ビットブロック暗号	CIPHERUNICORN-E	
		Hierocrypt-L1	
		MISTY1	
	128ビットブロック暗号	CIPHERUNICORN-A	
		CLEFIA	
		Hierocrypt-3	
		SC2000	
	ストリーム暗号	Enocoro-128v2	
		MUGI	
		MULTI-S01	
ハッシュ関数		該当なし	
暗号利用モード	秘匿モード	該当なし	
	認証付き秘匿モード	該当なし	
メッセージ認証コード		PC-MAC-AES	
エンティティ認証		ISO/IEC 9798-4	

付録:暗号技術名(フルスペル)一覧

運用監視暗号リスト

技術分類		名称	フルスペル
公開鍵暗号	署名	該当なし	
	守秘	RSAES-PKCS1-v1_5	**RSA** **E**ncryption **S**cheme, **P**ublic-**K**ey **C**ryptography **S**tandards**#1** **v**ersion **1.5**
	鍵共有	該当なし	
共通鍵暗号	64ビットブロック暗号	該当なし	
	128ビットブロック暗号	該当なし	
	ストリーム暗号	128-bit RC4	
ハッシュ関数		RIPEMD-160	**R**ACE **I**ntegrity **P**rimitives **E**valuation **M**essage **D**igest
		SHA-1	**S**ecure **H**ash **A**lgorithm
暗号利用モード	秘匿モード	該当なし	
	認証付き秘匿モード	該当なし	
メッセージ認証コード		CBC-MAC	**C**ipher **B**lock **C**haining **M**essage **A**uthentication **C**ode
エンティティ認証		該当なし	