2011年度版リストガイド(IPsec)

平成24年3月

独立行政法人情報通信研究機構
独立行政法人情報処理推進機構

目 次

1　本書の位置づけ

1.1　本書の目的

リストガイドは、電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、電子政府推奨暗号を利用する際に必要となる情報並びに推奨を示すものである。

本書では、電子政府をはじめとして、よく利用されている IPsec について、その利用方法並びに選択すべき暗号アルゴリズムについて情報提供を行うものである。

1.2　本書の構成

第 2 章において、本書で利用する用語の定義及び表記を示し、第 3 章において IPsec に係る情報提供並びに利用を推奨する暗号アルゴリズムを示す。

1.3　本書の利用範囲

本書の内容は 2012 年 3 月 31 日時点の情報に基づき構成されている。従って、今後、電子政府推奨暗号の改訂や電子政府推奨暗号に係る攻撃方法の研究動向、Internet Engineering Task Force (以下、「IETF」という。) における各種 Request For Comments(以下、「RFC」という。) やその他標準規格の策定状況及び米国 National Institute of Standards and Technology の Special Publicaion(以下、「SP」という。) をはじめとする推奨文書等の改定状況等によって、本書に掲載される内容がそぐわないくなるケースが発生する可能性がある。

本書を利用する際には、関連する標準規格並びに各種推奨文書等も同時に参照し、適切に判断を行うことを勧める。

2　定義と表記

2.1　定義

表 1: 用語の定義

用語	定義
AH	Authentication Header プロトコル。IPsec のプロトコルの一つ。
ESP	Encapsulating Security Payload プロトコル。IPsec のプロトコルの一つ。
IKE	Internet Key Exchange プロトコル。IPsec のプロトコルの一つ。IKEv1、IKEv2 の 2 つのバージョンが存在する。
暗号化	ある暗号アルゴリズムおよび鍵を用いて、平文を暗号文に変える処理。
暗号スイート	当該プロトコルにおいて選択可能な暗号アルゴリズムの組合せ。プロトコルの仕様により異なる。
完全性	不当に情報が改変または消去されていないことを示す特性。データが生成、移送、蓄積されて以後、許可されていない方法で当該データが変更されていないことを示す。本文書では、ある暗号アルゴリズムにより「完全性が与えられる」という表現は、当該アルゴリズムが、不当な改変または消去を発見するために用いられることを意味する。

2.2　表記

表 2: 略語の定義

略語	定義
IETF	Internet Engingeering Task Force
NIST	National Institute of Standards and Technology
RFC	Request For Comments
SP	Special Publications

3　IPsec に関する推奨

RFC では相互運用性の確保を目的に IPsec で使用する各暗号アルゴリズムの組み合わせを暗号スイートとしてまとめ、2 つの RFC で合計 6 種類の暗号スイートを公開している。

これとは別に ESP および AH の暗号アルゴリズム実装要求 (RFC4835)、IKEv1 のアルゴリズム実装要求 (RFC4109)、IKEv2 のアルゴリズム実装要求 (RFC4307) を公開している。

IPsec の主たる用途である VPN では、機器設置者が統一的にセキュリティポリシを設定するため、既存の暗号スイートに基づく選択は必ずしも必要ではなく、組織で統一的に使用する暗号アルゴリズムの組み合わせを定めてもよい。

IPsec の接続ノード間で暗号化および認証の鍵を手動で変更するのは非現実的であるので、IKE による自動的な鍵管理が行われることを前提とする。

3.1　各種標準の暗号スイート

3.1.1　RFC で規定される暗号スイート

相互運用性の確保を目的に IPsec で推奨する暗号アルゴリズムの組み合わせを暗号スイートとして定義した 2 つの RFC がある。

- IPsec 用暗号スイート（RFC4308）：2 つの暗号スイートを定義
- IPsec 用 Suite B 暗号スイート（RFC6379, 4869）：4 つの暗号スイートを定義

3.1.1.1　IPsec 用暗号スイート (RFC4308)

2005 年に作成された RFC4308 では相互運用性の確保を目的に、2 つの IPsec 推奨暗号スイートを定めている。VPN-A は運用中機器の相互運用性を重視した構成で、VPN-B は安全性を重視したより新しい機器向けの構成である。推奨暗号リストに含まれる暗号アルゴリズムのみで構成されるのは VPN-A であり、VPN-B には推奨暗号リスト外の AES-XCBC-MAC が含まれる。

表 3: RFC4308 で規定される暗号スイート

暗号スイート		VPN-A	VPN-B
IP パケット	プロトコル	ESP	ESP
	暗号化	3DES-CBC	AES-CBC (128 ビット鍵)
	完全性	HMAC-SHA1-96	AES-XCBC-MAC-96
IKEv1/IKEv2	暗号化	3DES-CBC	AES-CBC (128 ビット鍵)
	乱数	HMAC-SHA-1	AES-XCBC-PRF-128
	完全性	HMAC-SHA-1-96	AES-XCBC-MAC-96
	鍵共有	1024 ビット DH	2048 ビット DH
	鍵更新（IKEv1）・CREATE_CHILD_SA(IKEv2) をサポートする		

3.1.1.2 IPsec 用 Suite B 暗号スイート (RFC6379, 4869)

Suite B は NSA が定めた暗号化アルゴリズム群であり、共通鍵暗号は AES、ハッシュは SHA-2、公開鍵暗号は楕円曲線暗号（ECDSA による署名および ECDH による鍵共有）から構成され、RSA は含まれない。

2007 年に作成された RFC4869 ではこの Suite B 暗号アルゴリズム群から選択した暗号アルゴリズムの中で GCM と GMAC のそれぞれで 2 種類の鍵長で、合計 4 種類の暗号スイートを定めている。GMAC を使用する暗号スイートは完全性のみを提供し IP パケットの暗号化を行わないため、利用すべきでない。

表 4: Suite B 暗号スイート (RFC 4869)

暗号スイート		Suite-B-GCM-128	Suite-B-GCM-256
IP パケット	プロトコル	ESP	
	暗号化	AES-GCM (128 ビット鍵、16 バイト ICV)	
	完全性	GCM に含まれる	
IKEv1	暗号化	AES-CBC （128 ビット鍵）	AES-CBC （256 ビット鍵）
	乱数	HMAC-SHA-256	HMAC-SHA-384
	ハッシュ	SHA-256	SHA-384
	鍵交換	256 ビット ECDH	384 ビット ECDH
	鍵更新をサポートすること		
IKEv2	暗号化	AES-CBC （128 ビット鍵）	AES-CBC （256 ビット鍵）
	乱数	HMAC-SHA-256	HMAC-SHA-384
	完全性	HMAC-SHA-256-128	HMAC-SHA-384-192
	鍵交換	256 ビット ECDH	384 ビット ECDH
	認証	256 ビット ECDSA	384 ビット ECDSA
	CREATE_CHILD_SA をサポートすること		

表 5: Suite B 暗号スイート (RFC 6379)

暗号スイート		Suite-B-GCM-128	Suite-B-GCM-256
IP パケット	プロトコル	ESP	
	暗号化	AES-GCM (128 ビット鍵、16 バイト ICV)	
	完全性	GCM に含まれる	
IKEv2	暗号化	AES-CBC（128 ビット鍵）	AES-CBC （256 ビット鍵）
	乱数	HMAC-SHA-256	HMAC-SHA-384
	完全性	HMAC-SHA-256-128	HMAC-SHA-384-192
	鍵交換	256 ビット ECDH	384 ビット ECDH
	認証	256 ビット ECDSA	384 ビット ECDSA

3.1.2 IANA 暗号アルゴリズム ID

IPsec の暗号アルゴリズム選択では、IANA のプロトコルレジストリに登録された番号で暗号アルゴリズムを識別する[1]（http://www.iana.org/protocols/ ）。特に自動鍵更新（IKEv1/IKEv2）を使用する場合、SA のアルゴリズム折衝で暗号アルゴリズムを識別する ID が必要不可欠である。

表 6: IANA 暗号アルゴリズム ID への参照

仕様	URL
暗号スイート	http://www.iana.org/assignments/crypto-suites/crypto-suites.xml
ISAKMP	http://www.iana.org/assignments/isakmp-registry
IKEv1	http://www.iana.org/assignments/ipsec-registry
IKEv2	http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xml

3.1.3 SP 800-57,Part3[SP 800-57,part3]

[SP 800-57,part3] では、新規導入機器では IPsec-v3 への対応を求めている。また、ESP の使用を推奨し、AH の使用は非推奨としている。一方で運用中の機器を考慮して IPsec-v2 で使用すべき暗号アルゴリズムも合わせて記述している。

表 7: IPsec のバージョン、機能及び関連仕様

バージョン	仕様	秘匿	認証	(自動) 鍵管理
IPsec-v2	RFC2401	RFC2406	RFC2402,2406	IKEv1 RFC2407,2408,2409
IPsec-v3	RFC4301	RFC4303	RFC4302,4303	IKEV2 RFC4306,4718

[SP 800-57,part3] では、暗号スイート VPN-A と VPN-B を参照しているが、VPN-A は利用期限付き（当時で 2010 年まで）で推奨している。セキュリティの高い VPN-B は AES-XCBC を含むため推奨していない。

VPN で IPsec を使用する場合、統一的なセキュリティポリシの運用が正しくなされるならば相互接続性は担保できるので、個々の暗号アルゴリズムを列挙し実装の必要度をコメントしている。暗号化は 128 ビットの AES-CBC。認証あるいは完全性には HMAC-SHA-1 および HMAC-SHA-1-96 を必須（Mandatory）とし、他をオプショナル（Optional）としている。ESP は暗号化と完全性検証を組み合わせて使用するよう求めている。

[1] プライベート番号による運用も可能であるが、相互運用性に欠ける。

3.2 電子政府における推奨

以下、電子政府においてIPsecを利用することを推奨する暗号スイートを以下に示す。

3.2.1 留意点

本文書で推奨する暗号スイートは、電子政府推奨暗号リストに記載されている暗号アルゴリズムの利用を前提として構成している。このため、現在の電子政府推奨暗号として規定されない技術カテゴリが組み合わされた暗号スイートについては、以下の方針に基づき推奨暗号スイートとしている。

方針 1 現在の電子政府推奨暗号リストに掲載された暗号アルゴリズムを用いているが、プロトコルの仕様上、鍵長の選択等で十分な安全性があると認められる場合。

方針 2 2013年に決定予定の次期電子政府推奨暗号の評価プロセスにおいて評価が行われており、特段の問題がない場合には電子政府推奨暗号リストに掲載される可能性が高いアルゴリズムを用いている場合。

方針 3 現在の電子政府推奨暗号リストに掲載されておらず、かつ、2013年決定予定の次期電子政府推奨暗号の評価プロセスで評価が行われていない暗号アルゴリズムを用いる場合で、安全性に問題がない場合。

なお、HMAC-SHA1-96は96bit相当の安全性を有していることを確認しており、方針1に基づくと推奨暗号スイートとはしないことが妥当である。しかしながら、現状のIPsecにおける実装状況を踏まえ、HMAC-SHA1-96を推奨暗号スイートとしないことは不適切であると判断し、推奨暗号スイートとしている。このため、利用の際には留意されたい。

3.2.2 AH及びESPの認証アルゴリズム 推奨暗号スイート

ESPはペイロードの暗号化と完全性機能を提供する。ESPの完全性機能とAHの認証機能では保護範囲が異なるが、使用するアルゴリズムは同じである。

推奨暗号リストへの提案中のアルゴリズムを推奨アルゴリズムに含める。

表 8: AH 及び ESP の認証アルゴリズムの推奨暗号スイート

推奨暗号スイート	RFC	備考
HMAC-SHA-1-96	2404	
HMAC-SHA2-256-128	4868	
HMAC-SHA2-384-192	4868	
HMAC-SHA2-512-256	4868	
HMAC-RIPEMD-160-96	2857	
AES-CCM_12	4309	
AES-CCM_16	4309	
AES-GCM_12	4106	
AES-GCM_16	4106	
RSASSA-PKCS1-v1_5	4359	
RSASSA-PSS	4369	
AES-CMAC-96	4615	IKEv1 では未定義
Camellia-CCM_12	5529	IKEv1 では未定義
Camellia-CCM_16	5529	IKEv1 では未定義

3.2.3 ESP 暗号化 推奨暗号スイート

推奨暗号リストへの提案中のアルゴリズムを推奨アルゴリズムに含める。

表 9: ESP 暗号化の推奨暗号スイート

登録番号	推奨暗号スイート	RFC	備考
3	ENCR_3DES-CBC	2451	
12	ENCR_AES-CBC	3602	
13	ENCR_AES-CTR	3686	
15	ENCR_AES-CCM_12	4309	
16	ENCR_AES-CCM_16	4309	
19	AES-GCM with a 12 octet ICV	4106	
20	AES-GCM with a 16 octet ICV	4106	
22	IEEE P1619 XTS-AES		Reserved
23	ENCR_Camellia-CBC	5529	
24	ENCR_Camellia-CTR	5529	
26	ENCR_CAMELLIA_CCM with a 12-octet ICV	5529	
27	ENCR_CAMELLIA_CCM with a 16-octet ICV	5529	

3.2.4 IKEv1 推奨暗号スイート

IKE のフェーズ 1 では ISAKMP SA、フェーズ 2 では IPsec のセキュリティプロトコルの SA を決定する。

3.2.4.1 暗号化アルゴリズムスイートの推奨

表 10: IKEv1 暗号化アルゴリズムスイートの推奨

登録番号	暗号化アルゴリズムスイート	RFC
5	3DES-CBC	2409
7	AES-CBC	3602
8	CAMELLIA-CBC	4312

3.2.5 ハッシュアルゴリズムの推奨

表 11: IKEv1 ハッシュアルゴリズムの推奨

登録番号	ハッシュアルゴリズム	RFC
2	SHA	[FIPS 180-1]
4	SHA2-256	4868
5	SHA2-384	4868
6	SHA2-512	4868

3.2.6 認証方式の推奨

表 12: IKEv1 認証アルゴリズムの推奨

登録番号	認証アルゴリズム	RFC
1	pre-shared key	2409
2	DSS signatures	2409
3	RSA signatures	2409
4	Encryption with RSA	2409
5	Revised encryption with RSA	2409
9	ECDSA with SHA-256 on the P-256 curve	4754
10	ECDSA with SHA-384 on the P-384 curve	4754
11	ECDSA with SHA-512 on the P-521 curve	4754

3.2.6.1 Diffie-Hellman 鍵共有の推奨

MODP グループは 1024 ビット以上の利用を推奨とする。

表 13: IKEv1 Diffie-Hellman 鍵共有の推奨

登録番号	Diffie-Hellman 鍵共有	RFC
2	alternate 1024-bit MODP group	2409
3	EC2N group on GP[2ˆ155]	2409
4	EC2N group on GP[2ˆ185]	2409
5	1536-bit MODP group	3526
6	EC2N group over GF[2ˆ163]	reserved
7	EC2N group over GF[2ˆ163]	reserved
8	EC2N group over GF[2ˆ283]	reserved
9	EC2N group over GF[2ˆ283]	reserved
10	EC2N group over GF[2ˆ409]	reserved
11	EC2N group over GF[2ˆ409]	reserved
12	EC2N group over GF[2ˆ571]	reserved
13	EC2N group over GF[2ˆ571]	reserved
14	2048-bit MODP group	3526
15	3072-bit MODP group	3526
16	4096-bit MODP group	3526
17	6144-bit MODP group	3526
18	8192-bit MODP group	3526
19	256-bit random ECP group	5903
20	384-bit random ECP group	5903
21	521-bit random ECP group	5903
22	1024-bit MODP Group with 160-bit Prime Order Subgroup	5114
23	2048-bit MODP Group with 224-bit Prime Order Subgroup	5114
24	2048-bit MODP Group with 256-bit Prime Order Subgroup	5114
25	192-bit Random ECP Group	5114
26	224-bit Random ECP Group	5114

3.2.7 IKEv2 推奨暗号スイート

用途別 4 種類のトランスフォームタイプの暗号スイートと、認証ペイロードで使用する認証方式を以下に示す。

表 14: IKEv2 における Transform Type Value

Type	記述	用途	RFC
1	暗号化アルゴリズム (ENCR)	IKE, ESP	5996
2	擬似乱数 (PRF)	IKE	5996
3	完全性アルゴリズム	IKE, AH,(ESP)	5996
4	Diffie-Hellman 鍵共有	IKE, (AH, ESP)	5996

() はオプションでの利用を示す。

3.2.7.1 Transform Type1: 暗号化アルゴリズム (ENCR)

ESP の暗号アルゴリズムと同じである (表 9 参照)。

3.2.7.2 Transform Type2: 擬似乱数 (PRF)

表 15: PRF アルゴリズム (Transform Type2) の推奨暗号スイート

登録番号	推奨暗号スイート	RFC
2	PRF_HMAC_SHA1	2104
5	PRF_HMAC_SHA2_256	4868
6	PRF_HMAC_SHA2_384	4868
7	PRF_HMAC_SHA2_512	4868
8	PRF_AES_CMAC	4615

3.2.7.3 Transform Type3: 完全性アルゴリズム

表 16: IKEv2 認証アルゴリズムの推奨暗号スイート

登録番号	推奨暗号スイート	RFC
2	AUTH_HMAC_SHA1_96	5996
7	AUTH_HMAC_SHA1_160	4595
8	AUTH_AES_CMAC_96	4494
12	AUTH_HMAC_SHA2_256_128	4868
13	AUTH_HMAC_SHA2_384_192	4868
14	AUTH_HMAC_SHA2_512_256	4868

3.2.7.4 Transform Type4: Diffie-Hellman 鍵共有

表 17: IKEv2 Diffie-Hellman 鍵共有 (Transoform Type 4) の推奨

登録番号	Diffie-Hellman 鍵共有	RFC
2	Group 2 - 1024-bit MODP Group	5996
5	1536-bit MODP Group	5996
14	2048-bit MODP Group	5996
15	3072-bit MODP Group	3526
16	4096-bit MODP Group	3526
17	6144-bit MODP Group	3526
18	8192-bit MODP Group	3526
19	256-bit random ECP group	5903
20	384-bit random ECP group	5903
21	521-bit random ECP group	5903
22	1024-bit MODP Group with 160-bit Prime Order Subgroup	5114
23	2048-bit MODP Group with 224-bit Prime Order Subgroup	5114
24	2048-bit MODP Group with 256-bit Prime Order Subgroup	5114
25	192-bit Random ECP Group	5114
26	224-bit Random ECP Group	5114

3.2.7.5 IKEv2 認証ペイロード

IKEv2 には様々なペイロードタイプがあり (表 18)、SA/KE/AUTH などの認証に係るペイロードタイプが含まれる。

表 18: IKEv2 認証ペイロードのタイプ

Value	Next Payload Type	Notation	RFC
33	Security Association	SA	5996
34	Key Exchange	KE	5996
35	Identification - Initiator	IDi	5996
36	Identification - Responder	IDr	5996
37	Certificate	CERT	5996
38	Certificate Request	CERTREQ	5996
39	Authentication	AUTH	5996
40	Nonce	Ni, Nr	5996
41	Notify	N	5996
42	Delete	D	5996
43	Vender ID	V	5996
44	Traffic Selector - Initiator	TSi	5996

表 18: IKEv2 認証ペイロードのタイプ

Value	Next Payload Type	Notation	RFC
45	Traffic Selector - Responder	TSr	5996
46	Encrypted and Authenticated	SK	5996
47	Configuration	CP	5996
48	Extensible Authentication	EAP	5996
49	Generic Secure Password Method	GSPM	5996

IKEv2 認証ペイロードに係る暗号アルゴリズムの推奨を表 19 に示す。

表 19: IKEv2 認証ペイロードに係る推奨

推奨暗号スイート	RFC	備考
RSASSA-PKCS1-v1_5	5996	
PSK	5996	機器設定した鍵（パスワード）と MAC アルゴリズムを組み合わせた方法
DSA	5996	
ECDSA with SHA-256 on P-256	4754	
ECDSA with SHA-384 on P-384	4754	
ECDSA with SHA-512 on P-512	4754	

参考文献

[SP 800-57,part1] National Institute of Standards and Technology, “Recommendation for Key Management - Part1: General(Revised),” March, 2007.

[SP 800-57,part3] National Institute of Standards and Technology, “Recommendation for Key Management - Part3: Application-Specific Key Management Guidance,” December 2009.

発行日　2012 年 9 月 30 日第 1 版 第 1 刷
発行者
・〒184-8795
東京都小金井市貫井北四丁目 2 番 1 号
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 セキュリティアーキテクチャ研究室、
セキュリティ基盤研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN
・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
独立行政法人 情報処理推進機構
（技術本部 セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN