Barracuda WAF モデル 360

SSL/TLS アプライアンス製品の暗号設定方法等の調査報告書

1. 調査結果詳細

※本書は「SSL/TLS アプライアンス製品の暗号設定方法等の調査報告書」の1 部分を取り出したものである。調査の背景、調査方法等は報告書を参考にされたい。

1.x.1 章記載の表 1.x.1-1 暗号設定内容（デフォルト） の見方を以下に示す。

- CipherSuite 選択優先権

プロトコル	設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	クライアント	7
tls1.1	OFF	-	0
tls1.0	ON	クライアント	5
sslv3	OFF	-	0
sslv2	設定不可	-	-

1

- XXXXXXX で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				----	ON	OFF	ON	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	----	ON	OFF	ON	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	----	ON	OFF	ON	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	----	ON	OFF	ON	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	----	ON	OFF	ON	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	----	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	----	ON	OFF	OFF	OFF	OFF

2

※XXXXXXXは機種名

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

3

図 1 暗号設定内容（デフォルト）の表記例

表 1 暗号設定内容（デフォルト）の表の見方

項番	項目	説明
1	CipherSuite 選択優先権	・「設定状況」欄：設定されていれば「ON」、設定されていなければ「OFF」、設定不可であれば「設定不可」。 ・「CipherSuite 選択優先権」欄：暗号スイートの優先権がサーバにあるかクライアントにあるか。 「サーバ」：サーバ優先。 「クライアント」：クライアント優先。

		「-」：当該プロトコルが使用できない場合。 ・「CipherSuite 数」欄：該当する暗号スイートの数（reserved または unassigned の暗号スイートで、有効な数を含む）。
2	使用可能な暗号スイート ※Appendix2 の表も同様	・IANA で規定されている全ての暗号スイートに対してプロトコル毎に「ON」(使用可能)「OFF」(使用不可)を示す。項番 1 の CipherSuite 選択優先権がサーバ優先で、且つ「ON」であった場合、「ON」の隣に暗号スイートの優先順位を示す（例：「ON：1」）。 ・「高」「推」「例」欄：それぞれ設定ガイドラインの「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」のいずれのグループに属するかを示す。いずれにも属さない場合は空欄。 「α」「β」「A」～「H」：設定ガイドラインの要求設定のグループを示す。 「α追加」「β追加」「A 追加」～「F追加」：設定ガイドラインの各グループへの追加または代替を示す。 ・「鍵交換パラメータ」欄：鍵交換の暗号が DH/DHE、ECDH/ECDHE 且つ「ON」であった場合は、複数の鍵長の設定値から通信時のネゴシエーションによって選択された DH/DHE の鍵長、または、ECDH/ECDHE の namedcurve の名前のうち、一つを例示している。該当しない場合は「---」。 ・二重線は鍵交換の種類(DH, DHE, ECDH, ECDHE, KRB5, NULL, PSK, RSA, SRP)の区切りを示す。
3	Extension	・サーバの Extension（拡張機能）の情報をプロトコル毎に「対応」、「非対応」または「-」で示す。 「-」の場合はプロトコルで拡張機能自体がない場合を示す。 「signature_algorithms」：クライアントの使用可能な署名アルゴリズムを受入可否。「対応」の場合で、クライアントが安全性の低い署名アルゴリズムしか受け入れられない場合は、TLS/SSL 通信で使用される暗号がダウングレードする可能性がある。 「heartbeat」：サーバ側での Heartbeat（死活監視）機能が有効か否か。Heartbeat 機能が有効な場合、HeartBleed 攻撃を受ける可能性がある。

※項番は図 1 中の番号。

1.1. バラクーダネットワークス Barracuda WAF シリーズ

本章では、Barracuda WAF について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書と ECDSA 証明書が設定可能である。RSA 証明書を設定した場合と ECDSA 証明書を設定した場合で有効となる暗号スイートが異なり、両方の証明書を設定した場合は、両方の暗号スイートが有効になる。1.1.3 **エラー! 参照元が見つかりません。**については、RSA 証明書と ECDSA 証明書の両方を設定した結果について記載する。ただし、デフォルト設定では RSA 証明書のみの設定になっているため、1.1.1 **デフォルトでの暗号設定内容の調査**については、RSA 証明書のみを設定した結果について記載する。

1.1.1. デフォルトでの暗号設定内容の調査

デフォルトでは ECDSA 証明書の設定は無効になっているため、RSA 証明書のみ設定した場合について記載する。

表 1.1.1-1　暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	サーバ	20
tls1.1	ON	サーバ	13
tls1.0	ON	サーバ	13
sslv3	ON	サーバ	4
sslv2	設定不可	ー	ー

- Barracuda WAF で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				secp256r1	ON:9	ON:10	ON:10	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON:12	ON:12	ON:12	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:13	ON:11	ON:11	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:11	ON:13	ON:13	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:4	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:3	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:2	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:1	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON:20	ON:1	ON:1	ON:1	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON:10	ON:9	ON:9	ON:4	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	ON:2	ON:2	ON:2	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:16	ON:6	ON:6	ON:3	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:17	ON:5	ON:5	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:14	ON:8	ON:8	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:8	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:7	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	ON:19	ON:3	ON:3	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	ON:15	ON:7	ON:7	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	ON:18	ON:4	ON:4	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON:6	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON:5	OFF	OFF	OFF	OFF

※tls1.2～sslv2 欄が全て OFF:デフォルトでは設定可能になっていない暗号スイート。

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	対応	対応	対応	ー	ー

1.1.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ブラウザで管理画面にログインし、(1) 基本設定ー (2) サービスをクリックしてサービス一覧を表示し、(3) 現在有効なサービスの「Edit」をクリックする。

図 1.1.2-1 サービス一覧画面

B) サービス編集画面の SSL 欄で、(4)「高度な設定を非表示」を選択する。(5) ECDSA Certificate で (6) 使用する証明書を選択する。(7) SSL プロトコル欄の SSL 3.0、TLS 1.0、TLS1.1、TLS1.2 を選択して、有効にするか無効にするかを (8) 有効化 (9) 無効化にチェックを入れ、(10) 保存ボタンで確定する。

※ECDSA 暗号の有効化でオンを選択し、ECDSA 証明書を選択しないと ECDSA を含む暗号スイートが有効にならない。

※ECDSA 証明書のみは設定できず、RSA 証明書を設定することが前提となる。

図 1.1.2-2　サービス編集画面（プロトコルバージョン）

II. 暗号スイートの設定

A) サービス編集画面の（1）PFS（Perfect Forward Secrecy）の有効化で（2）はいを選択する。（3）暗号欄で（4）カスタムにチェックを入れると（5）Selected Ciphers 欄と（6）Available Ciphers 欄が表示されるので、（7）追加ボタンと（8）削除ボタンで Selected Ciphers 欄に追加し、（9）保存ボタンで確定する。

※PFS（Perfect Forward Secrecy）を有効化しないと ECDHE を含む暗号スイートは選択しても有効にならない。

※デフォルトでは全て Selected Ciphers 欄に追加されている。

※優先度は Selected Ciphers 欄の上から順となるため、一度全て Available Ciphers 欄に移動する必要がある。

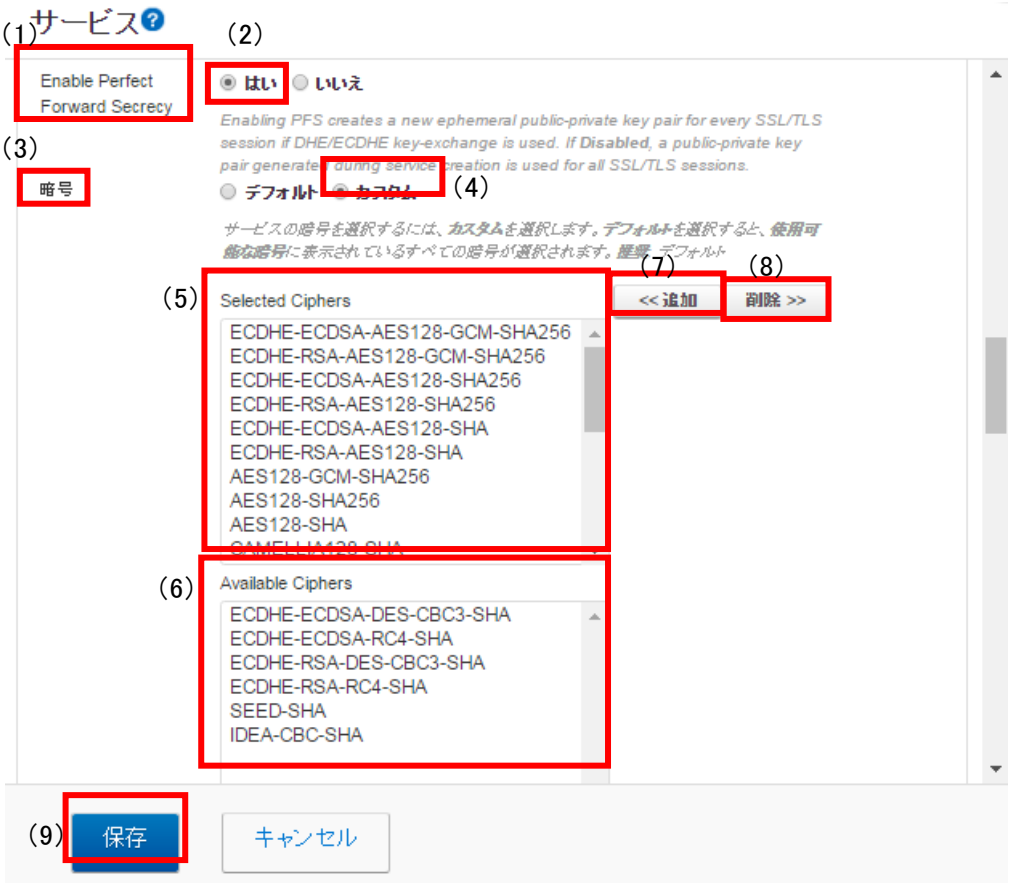

図 1.1.2-3 サービス編集画面（暗号スイート）

III. DH/DHE、ECDH/ECDHE の鍵長の設定

設定方法なし。

ECDHE の鍵長は、既定で 256bit(secp256r1)である。

※ECDSA512bit の証明書を設定した場合でも secp256r1 が使用される。

IV. サーバクライアントの優先順位の設定

既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定

II 暗号スイートの設定した結果による。

VI. Extension の設定

設定方法なし。

1.1.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

1.1.3.1. 高セキュリティ型

③「暗号スイートを具体的に設定する方法」により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

暗号スイートを具体的に指定する以外に設定方法がないため、デフォルトでの暗号設定内容の調査結果を以下に示す。

I. プロトコルバージョン
TLS1.1、TLS1.0、SSL3.0 が有効である。

II. 暗号スイート
1.1.1 表 1.1.1-1　暗号設定内容（デフォルト）の Barracuda WAF で使用可能な暗号スイートのとおり。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。
※1.1.1 表 1.1.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

V. 暗号スイートの優先順位の設定
1.1.1 表 1.1.1-1　暗号設定内容（デフォルト）の Barracuda WAF で使用可能な暗号スイートのとおり。

VI. Extension の設定
1.1.1 表 1.1.1-1　暗号設定内容（デフォルト）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
TLS1.1、TLS1.0、SSL3.0 が有効である。

II. 暗号スイート

差分あり。

高セキュリティ型に含まれる 12 個の暗号スイートのうち、表 1.1.3.1-1 設定ガイドラインとの差分（高セキュリティ型） の「設定ガイドラインの高セキュリティ型（一部）」にある 2 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 18 個の暗号スイートが使用可能である。優先順位についても表 1.1.3.1-1 設定ガイドラインとの差分（高セキュリティ型） のとおりである。

表 1.1.3.1-1 設定ガイドラインとの差分（高セキュリティ型）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)
β	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)
－	設定ガイドラインの高セキュリティ型に該当しない暗号スイート	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
		4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
		5	TLS_RSA_WITH_AES_256_GCM_SHA384
		6	TLS_RSA_WITH_AES_128_GCM_SHA256
		7	TLS_RSA_WITH_AES_256_CBC_SHA256
		8	TLS_RSA_WITH_AES_128_CBC_SHA256
		9	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		10	TLS_RSA_WITH_RC4_128_SHA
		11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
		12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
		14	TLS_RSA_WITH_AES_256_CBC_SHA
		15	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
		16	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		17	TLS_RSA_WITH_AES_128_CBC_SHA
		18	TLS_RSA_WITH_SEED_CBC_SHA
		19	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
		20	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン

SSL プロトコル：有効化：TLS1.2

無効化：SSL3.0、TLS1.0、TLS1.1

（図 1.1.2-2 参照）

II. 暗号スイート

1.1.2 II 図 1.1.2-3　サービス編集画面（暗号スイート）の「暗号」「Select Ciphers」欄に、表 1.1.3.1-2 暗号スイートの設定（高セキュリティ型、個別指定）の順番で「追加」する。

表 1.1.3.1-2　暗号スイートの設定（高セキュリティ型、個別指定）

優先順位	暗号スイート
1	ECDHE-ECDSA-AES256-GCM-SHA384
2	ECDHE-RSA-AES256-GCM-SHA384
3	ECDHE-ECDSA-AES128-GCM-SHA256
4	ECDHE-RSA-AES128-GCM-SHA256

※グループ内の順番は順不同。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定

既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定

II.暗号スイートで設定した結果による。

VI. Extension の設定

設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

II. 暗号スイート

差分なし。

高セキュリティ型に含まれる 12 個の暗号スイートのうち、表 1.1.3.1-3 設定ガイドラインとの差分（高セキュリティ型、個別指定）の「設定ガイドラインの高セキュリティ型（一部）」にある 4 個の暗号スイートの使用が可能である。優先順位についても表 1.1.3.1-3 設定ガイドラインとの差分（高

セキュリティ型、個別指定） のとおりである。

表 1.1.3.1-3 設定ガイドラインとの差分（高セキュリティ型、個別指定）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追加)	1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)	2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)
β	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

1.1.3.2. 推奨セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

暗号スイートを具体的に指定する以外に設定方法がないため、デフォルトでの暗号設定内容となる。

調査結果は、1.1.3.1 **高セキュリティ型**と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分あり。

SSL3.0 が有効である。

II. 暗号スイート

差分あり。

推奨セキュリティ型に含まれる 64 個の暗号スイートのうち、表 1.1.3.2-1 設定ガイドラインとの差分（推奨セキュリティ型） の「設定ガイドラインの推奨セキュリティ型（一部)」にある 14 個の暗号スイートの使用が可能である。その他、推奨セキュリティ型に含まれない 6 個の暗号スイートが使用可能である。

表 1.1.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	17	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	8	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）	19	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	6	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	14	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	7	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）	15	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	5	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	9	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		10	TLS_RSA_WITH_RC4_128_SHA
		12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		16	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		18	TLS_RSA_WITH_SEED_CBC_SHA
		20	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

③　プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I.　プロトコルバージョン

SSL プロトコル：有効化：TLS1.0、TLS1.1、TLS1.2

無効化：SSL3.0

（図 1.1.2-2 参照）

II.　暗号スイート

1.1.2 II 図 1.1.2-3　サービス編集画面（暗号スイート）の「暗号」「Select Ciphers」欄に、表 1.1.3.2-2 暗号スイートの設定（推奨セキュリティ型、個別指定）の順番で「追加」する。

表 1.1.3.2-2　暗号スイートの設定（推奨セキュリティ型、個別指定）

優先順位	暗号スイート
1	ECDHE-ECDSA-AES128-GCM-SHA256
2	ECDHE-RSA-AES128-GCM-SHA256
3	ECDHE-ECDSA-AES128-SHA256
4	ECDHE-RSA-AES128-SHA256
5	ECDHE-ECDSA-AES128-SHA
6	ECDHE-RSA-AES128-SHA
7	AES128-GCM-SHA256
8	AES128-SHA256
9	AES128-SHA
10	CAMELLIA128-SHA
11	ECDHE-ECDSA-AES256-GCM-SHA384
12	ECDHE-RSA-AES256-GCM-SHA384
13	ECDHE-ECDSA-AES256-SHA384
14	ECDHE-RSA-AES256-SHA384
15	ECDHE-ECDSA-AES256-SHA
16	ECDHE-RSA-AES256-SHA
17	AES256-GCM-SHA384
18	AES256-SHA256
19	AES256-SHA
20	CAMELLIA256-SHA

※グループ内の順番は順不同。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDHE の鍵長は 256bit(secp256r1)である。

※ECDSA（256bit）の証明書を設定した場合 256bit(secp256r1)が使用される。

IV. サーバクライアントの優先順位の設定

既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定

II.暗号スイートで設定した結果による。

VI. Extension の設定

設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

II. 暗号スイート

差分なし。

推奨セキュリティ型に含まれる 64 個の暗号スイートのうち、表 1.1.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型） の「設定ガイドラインの推奨セキュリティ型（一部)」にある 20 個の暗号スイートの使用が可能である。優先順位についても表 1.1.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型） のとおりである。

表 1.1.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
B	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	7	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	8	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA(B)	9	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)	10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)
D	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	11	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	12	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)	13	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	15	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_AES_256_CBC_SHA(D 追加)	16	TLS_ECDHE_RSA_AES_256_CBC_SHA(D 追加)
E	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	17	TLS_RSA_WITH_AES_256_GCM_SHA384(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	18	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
	TLS_RSA_WITH_AES_256_CBC_SHA(E)	19	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)	20	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

1.1.3.3. セキュリティ例外型

③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に設定方法がないため、デフォルトでの暗号設定内容となる。調査結果は、1.1.3.1 **高セキュリティ型**と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

II. 暗号スイート

差分あり。

セキュリティ例外型に含まれる 67 個の暗号スイートのうち、表 1.1.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）の「設定ガイドラインのセキュリティ例外型（一部）」にある 16 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 4 個の暗号スイートが使用可能である。

表 1.1.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	17	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	8	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）	19	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	6	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）

E	TLS_RSA_WITH_AES_256_CBC_SHA（E） TLS_RSA_WITH_AES_256_CBC_SHA256（E） TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E） TLS_RSA_WITH_AES_256_GCM_SHA384（E）	14	TLS_RSA_WITH_AES_256_CBC_SHA（E）
		7	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
		15	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
		5	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
G	TLS_RSA_WITH_RC4_128_SHA（G）	10	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	16	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）
-	設定ガイドラインのセキュリティ例外型に該当しない暗号スイート	9	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		18	TLS_RSA_WITH_SEED_CBC_SHA
		20	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン

SSL プロトコル：有効化：SSL3.0、TLS1.0、TLS1.1、TLS1.2　（図 1.1.2-2 参照）

II. 暗号スイート

1.1.2 II 図 1.1.2-3　サービス編集画面（暗号スイート）の「暗号」「Select Ciphers」欄に、表 1.1.3.3-2 暗号スイートの設定（セキュリティ例外型、個別指定）の順番で「追加」する。

表 1.1.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定）

優先順位	暗号スイート
1	ECDHE-ECDSA-AES128-GCM-SHA256
2	ECDHE-RSA-AES128-GCM-SHA256
3	ECDHE-ECDSA-AES128-SHA256
4	ECDHE-RSA-AES128-SHA256
5	ECDHE-ECDSA-AES128-SHA
6	ECDHE-RSA-AES128-SHA
7	AES128-GCM-SHA256
8	AES128-SHA256
9	AES128-SHA
10	CAMELLIA128-SHA
11	ECDHE-ECDSA-AES256-GCM-SHA384

優先順位	暗号スイート
12	ECDHE-RSA-AES256-GCM-SHA384
13	ECDHE-ECDSA-AES256-SHA384
14	ECDHE-RSA-AES256-SHA384
15	ECDHE-ECDSA-AES256-SHA
16	ECDHE-RSA-AES256-SHA
17	AES256-GCM-SHA384
18	AES256-SHA256
19	AES256-SHA
20	CAMELLIA256-SHA
21	RC4-SHA
22	DES-CBC3-SHA

※グループ内の順番は順不同。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDHE の鍵長は 256bit(secp256r1)である。

※ECDSA（256bit）の証明書を設定した場合 256bit(secp256r1)が使用される。

IV. サーバクライアントの優先順位の設定

既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定

II.暗号スイートで設定した結果による。

VI. Extension の設定

設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

II. 暗号スイート

差分なし。

セキュリティ例外型に含まれる 67 個の暗号スイートのうち、表 1.1.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、個別指定）の「設定ガイドラインのセキュリティ例外型（一部）」にある 22 個の暗号スイートの使用が可能である。優先順位についても表 1.1.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）のとおりである。

表 1.1.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、個別指定）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
B	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	7	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	8	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA(B)	9	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)	10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)
D	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	11	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	12	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)	13	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	15	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_AES_256_CBC_SHA(D 追加)	16	TLS_ECDHE_RSA_AES_256_CBC_SHA(D 追加)
E	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	17	TLS_RSA_WITH_AES_256_GCM_SHA384(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	18	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
	TLS_RSA_WITH_AES_256_CBC_SHA(E)	19	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)	20	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)
G	TLS_RSA_WITH_RC4_128_SHA(G)	21	TLS_RSA_WITH_RC4_128_SHA(G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)	22	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

付属情報

- 製品情報
  Barracuda Web Application Firewall 360 ファームウェアバージョン: 8.1.0.009 (2016-05-04 22:58:07)

- 参考情報
  Barracuda Web Application Firewall　日本語セットアップガイド