－EZweb 仕様書－

【EZweb 全般】SHA-2 対応ケータイアップデートについて

Version-1.3

2017-05-31
KDDI Corporation

ーはじめにー

『【EZweb 全般】SHA-2 対応ケータイアップデートについて』（以下、本書）は、2012 年 5 月 24 日より開始されたケータイアップデートについて、コンテンツを提供する際の注意事項を記載するものです。

ー関連仕様書ー

・EZweb 仕様書ー【EZweb 全般】EZweb コンテンツ制作ガイド
・SSL 証明書一覧

ー目次ー

1. 2012 年 5 月 24 日より開始されたケータイアップデートについて

1.1. 概要

2012 年 5 月 24 日より開始されたケータイアップデートにおいて、SHA-2 を利用した認証仕様に対応いたします。

※「ケータイアップデートのお知らせ」(http://www.au.kddi.com/seihin/up_date/kishubetsu/au_info_20120524.html)を参照ください。

上記のケータイアップデートは、移動機が搭載するルート証明書の一部変更、TLS ハンドシェイク手順の変更なども含まれております。

ケータイアップデートでの変更点	Web サーバへの影響	影響概要	影響詳細	参照
SHA-2 を利用した認証仕様への対応	無し	-	-	-
搭載するルート証明書の一部変更	一部有り	SSL 通信が行えない場合がある	Web サーバに古い中間 CA 証明書がインストールされていると、移動機でエラーとなり、SSL 通信が行えない。	2.1. ルート証明書の一部変更
TLS ハンドシェイク手順の変更	一部有り	SSL 通信が行えない場合がある	Web サーバが TLS 拡張を含む Client Hello に Alert を返すと、移動機でエラーとなり、SSL 通信が行えない。	2.2. TLS ハンドシェイクの変更
Empty Data Record の送信	一部有り	SSL 通信が行えない場合がある	Web サーバが TLSPlaintext の fragment が空である SSL レコードをに対応していないと、移動機でエラーとなり、SSL 通信が行えない。	2.3. Empty Data Record の送信

上記のケータイアップデートにより、Web サーバ側で対処が必要となることは基本的にはありませんが、Web サーバの設定によってはケータイアップデートによって移動機の動作に差分が発生し、Web サーバでの対処が必要になる場合があります。

本書をご確認いただき、必要な場合は対処を実施するようお願いいたします。

2. 詳細

2.1. ルート証明書の一部変更

(1) 変更点

「SSL 証明書一覧」にも記載しておりますが、5 月 24 日より開始されたケータイアップデートにより、移動機が搭載しているルート証明書が変更されます。

2009 年 5 月 18 日以降、ベリサイン社から署名アルゴリズムが SHA-1 に変更されたルート証明書「VeriSign Class 3 Primary CA」が発行されており、一部機種についてはそちらに変更して搭載しております。署名アルゴリズムは変更となりますが、公開鍵そのものは変更ありませんので、Web サーバの設定変更は不要です。

VeriSign Class 3 Primary CA
・変更前
　署名アルゴリズム　MD2

・変更後
　署名アルゴリズム　SHA-1

但し、中間 CA 証明書、クロスルート設定用証明書はベリサイン社によりルート証明書の署名アルゴリズム変更とあわせて変更になっていますので、最新の中間 CA 証明書、クロスルート設定用証明書をサーバに設定していない場合、アップデート後の端末との SSL 通信ができなくなる可能性がございます。

※対象機種は、「SSL 証明書一覧」を参照ください。

なお、ベリサイン社からも下記の通知が出ております。ご参照ください。
SSL サーバ証明書、コードサイニング証明書における認証局証明書(ルート認証局証明書、中間認証局証明書)の変更、およびメンテナンスのお知らせ
https://www.verisign.co.jp/support/maintenance/announce20090408.html

(2) 対処

「VeriSign Class 3 Primary CA」にひもづくサーバ証明書を使用されている Web サーバでは、最新の中間 CA 証明書、クロスルート設定用証明書を使用いただくようお願いします。

2.2. TLS ハンドシェイクの変更

(1) 変更点

5 月 24 日より開始されたケータイアップデートにより、EZ ブラウザで TLS の拡張をサポートいたします。
（F001 および 12 夏以降の機種では、発売時点で TLS の拡張をサポートしております。
なお拡張を含まない TLS1.0 については、EZ ブラウザ搭載のすべての機種が対応しております。
EZweb の対応プロトコルは、「EZweb 仕様書ー【EZweb 全般】EZweb コンテンツ制作ガイド」を参照ください。）

これにより、TLS ハンドシェイクにて EZ ブラウザが送信する Client Hello メッセージに、TLS SessionTicket 拡張(RFC5077)が含まれるようになります。

一部の Web サーバでは、TLS SessionTicket 拡張を含む Client Hello メッセージを受信した際に、Alert メッセージ（unexpected Message）を応答するため、EZ ブラウザでエラーと判断し、SSL 通信(※1)を行えません。

※1 End-to-End SSL のみ。Link-by-Link SSL では EZ サーバ～Web サーバ間で SSL 通信が行われるため、エラーは発生しません。

TLS では、サーバが TLS 拡張をサポートしない場合でも、互換性を確保するために TLS 拡張を含む ClientHello メッセージを受容することを要求しています。(サーバは ClientHello に追加された解釈できないデータは無視する必要があります。) (RFC2246、4366)

(2) 対処

ご都合に合わせて以下のいずれかの対処をお願いします。なお設定変更方法などの詳細は、使用している Web サーバのマニュアルなどをご参照ください。

■ TLS 拡張のサポート

Web サーバを TLS SessionTicket 拡張に対応させ、SessionTicket 拡張に対応した Server Hello を応答するようにする。

■ TLS 拡張の無視

TLS SessionTicket 拡張を Web サーバでサポートしない場合、Alert メッセージではなく、拡張を無視した Server Hello メッセージを応答するようにする。

2.3. Empty Data Record の送信

(1) 変更点

このケータイアップデートにより、SSL の動作が変更され、ハンドシェイク成功直後に Empty Data Record（TLSPlaintext の fragment が空である SSL レコード）を送信するようになっています。
これは、OpenSSL 0.9.6d から変更された動作です。詳細は、http://www.openssl.org/~bodo/tls-cbc.txt をご覧ください。

一部の Web サーバでは Empty Data Record を受信すると、Alert メッセージを送信します。その場合、移動機では「接続できません。しばらくたってからリトライしてください」などのエラーが表示されます。

(2) 対処

Empty Data Record に対し、Alert メッセージを送信しないよう対処してください。
なお設定変更方法などの詳細は、使用している Web サーバのマニュアルなどをご参照ください。

2.4. Cipher Suites 対応の状況

(1) 変更点

このケータイアップデートにより、EZ ブラウザの Cipher Suites 対応状況が変更となります。

▽SHA-2 未対応(ケータイアップデート前)

優先順位	ショートネーム	ロングネーム
0	0a	DES-CBC3-SHA
1	05	RC4-SHA
2	04	RC4-MD5
3	64	EXP1024-RC4-SHA
4	62	EXP1024-DES-CBC-SHA
5	60	EXP1024-RC4-MD5
6	09	DES-CBC-SHA
7	08	EXP-DES-CBC-SHA
8	03	EXP-RC4-MD5

▽SHA-2 対応(ケータイアップデート後)

優先順位	ショートネーム	ロングネーム
0	35	AES256-SHA
1	0a	DES-CBC3-SHA
2	2f	AES128-SHA
3	05	RC4-SHA
4	04	RC4-MD5
5	62	EXP1024-DES-CBC-SHA
6	09	DES-CBC-SHA
7	64	EXP1024-RC4-SHA
8	08	EXP-DES-CBC-SHA
9	03	EXP-RC4-MD5

3. SHA-2 対応機種一覧

SHA-2 対応機種には、ケータイアップデートにより SHA-2 対応となる機種のほかに、発売時点から SHA-2 対応している機種があります。以下にそれぞれの一覧を示します。

3.1. ケータイアップデートにより SHA-2 対応となる機種一覧

CASIO	EXILIM ケータイ W63CA
	CA001
	G'zOne CA002
	EXILIM ケータイ CA003
	EXILIM ケータイ CA004
	EXILIM ケータイ CA005
	EXILIM ケータイ CA006
	G'zOne TYPE-X
	CA007
FUJITSU	E09F
	E09F(カメラなし)
HITACHI	Wooo ケータイ H001
	Mobile Hi-Vision CAM Wooo
	beskey
KYOCERA	安心ジュニアケータイ K001
	K002
	簡単ケータイ K003
	簡単ケータイ K004
	簡単ケータイ K005
	簡単ケータイ K010
	K006
	K006 (カメラなし)
	K007
	簡単ケータイ K008
	E07K
	mamorino
	mamorino2
	K009
	E10K
	Mi-Look
NEW STANDARD	ベルトのついたケータイ NS01
	ケースのようなケータイ NS02
Panasonic	P001
PANTECH	簡単ケータイ W62PT
	PT002
SANYO	SA001
	SA002
SHARP	SH001
	SOLAR PHONE SH002
	URBANO
	Sportio water beat
SHARP	AQUOS SHOT SH003

	SH004
	SH005
	AQUOS SHOT SH006
	SOLAR PHONE SH007
	AQUOS SHOT SH008
	SH009
	AQUOS SHOT SH010
	SH011
	E05SH
	E06SH
Sony Ericsson	W64S
	Cyber-shot™ケータイ S001
	Walkman® Phone,Premier3
	BRAVIA® Phone U1
	S002
	URBANO BARONE
	Cyber-shot™ケータイ S003
	BRAVIA® Phone S004
	BRAVIA® Phone S005
	URBANO MOND
	Cyber-shot™ケータイ S006
	S007
	URBANO AFFARE
TOSHIBA	フルチェンケータイ T001
	T008
	REGZA Phone T004
	T005
	T006
	T007
	T002
	Biblio
	T003
	E08T
	E08T(カメラなし)
iida	LIGHT POOL
	lotta
	misora
	PRISMOID
	X-RAY
	G9

iida	G11
	PLY
	ドッツ・オブセッション 水玉で幸福いっぱい
	宇宙へ行くときのハンドバッグ
	私の犬のリンリン

3.2. 発売時点から SHA-2 対応している機種一覧

FUJITSU	F001
KYOCERA	K011
	簡単ケータイ K012
	mamorino3
	GRATINA
	MARVERA
	MARVERA 2
	GRATINA2
PANTECH	PT003

－更新履歴－

Version	日付	更新内容
1.3	2017/05/31	「2.4. Cipher Suites 対応の状況」を追記
1.2	2015/02/02	今まで別紙になっていたケータイアップデート対象機種の一覧などを、「3. SHA-2 対応機種一覧」として統合
1.1.1	2014/10/29	「2.2. TLS ハンドシェイクの変更」から、SSL を使用することによる対処を削除。 また拡張を含まない TLS1.0 については、EZ ブラウザ搭載のすべての機種が対応していることを明記。
1.1	2013/11/25	「2.3. Empty Data Record の送信」を追記
1.0	2012/06/22	初版