2016 年 7 月 22 日(初版)
2017 年 1 月 27 日(改版)
富士通株式会社

Interstage Application Server における SHA-2 証明書対応について(広報)

SHA-1 の安全性低下の指摘(注)を受け、暗号化通信で使用される電子証明書について、各認証局から SHA-1 証明書発行中止、SHA-2 証明書への移行が広報されています。
また、2017 年 1 月以降、SHA-1 証明書をご使用中の Interstage Application Server のシステムと Web ブラウザの暗号化通信ができなくなる場合があります。
本資料では、Interstage Application Server における SHA-2 証明書対応についてお知らせします。
Interstage Application Server にて、SHA-1 証明書をご使用中のシステムでは、SHA-2 証明書への移行をお願いいたします。
注) Cryptrec「SHA-1 の安全性について」など。
http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html

1．SHA-2 証明書が使用可能なバージョンについて

表 1 SHA-2 証明書が使用可能なバージョン

製品・バージョン	対応情報
Interstage Application Server V10 以降 Interstage Web Server Express V11 以降 Interstage Web Server V10 Interstage Business Application Server V10 以降 Interstage Job Workload Server V9.3.1 以降 Interstage Service Integrator V9.4.1 以降 Interstage Service Integrator V9.4.0(Solaris(32bit)のみ)	SHA-2 証明書に対応しています。 (注 1) (注 2)
Interstage Application Server V9 以前 Interstage Web Server V9 Interstage Business Application	SHA-2 証明書に対応していません。(注 3) ただし、V9 の一部サービスは SHA-2 証明書に対応しています。(注 4)

Server V9 以前 Interstage Job Workload Server V9.3.0 以前 Interstage Service Integrator V9.3.1 以前 Interstage Service Integrator V9.4.0(Solaris(32bit)以外)	

※V9 ご使用のお客様で SHA-2 証明書対応のご要望がある方は、当社担当営業にお問い合わせください。

注 1) 「Interstage Application Server/Interstage Web Server Express Java EE 運用ガイド(Java EE 6 編)」＞「Java EE 6 機能のセキュリティ」＞「Java EE 6 アプリケーションのセキュリティ機能」＞「SSL」において、認証局証明書の署名アルゴリズムは「SHA1withRSA」と記載していますが、製品出荷後に SHA-2 に対応できることを確認済みです。

注 2)本製品で生成する証明書は、SHA-1 証明書です。該当する証明書は以下です。SHA-2 証明書で運用される場合は、認証局が発行する証明書に切り替えてください。

・本製品で生成する Interstage 管理コンソール/ Interstage Java EE 管理コンソール用の証明書

・Interstage 証明書環境のテスト用サイト証明書作成機能で生成する証明書

注 3) SHA-2 証明書対応のパッチはありません。

注 4) 本製品では、証明書/鍵管理環境として、「Interstage 証明書環境」、「SMEE コマンドで構築した証明書/鍵管理環境」、「キーストア」を提供しています。
以下の場合のみ、SHA-2 証明書に対応しています。

・V9 を使用、かつ、キーストアを使用、かつ、JDK5 または JDK6 を使用するサービス。該当するサービスは以下です。

- Interstage Web サービスクライアント
- Portable-ORB
- ebXML Message Service
- SOAP クライアント
- J2EE の Web アプリケーション(SSL クライアントとして動作時)
- Java EE 5 の Web アプリケーション(SSL クライアントとして動作時)

２．SHA-2 証明書運用に関する注意事項

本製品の証明書の変更が必要な例１）

SHA-1 証明書を使用して運用している Web サイトで、Web ブラウザが SHA-1 証明書の受け入れを拒否する仕様に変更された場合、Web ブラウザから Web サイトへ通信が行えなくなる可能性があります。Web ブラウザが SHA-1 証明書の受け入れを拒否する仕様に変更される場合、事前に、Web サイトを SHA-2 証明書に変更する必要があります。

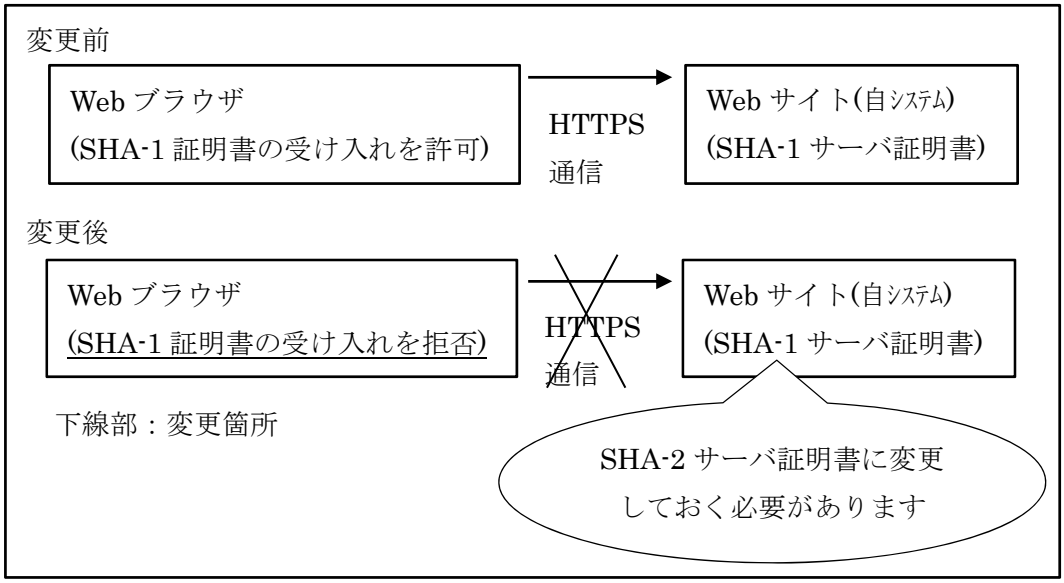

図１　本製品の証明書の変更が必要な例１

本製品の証明書の変更が必要な例２）

自システムのアプリケーションが通信相手システムと SSL 通信している場合、相手システムの証明書期限切れなどで SHA-2 証明書変更が発生したとき、突然通信できなくなるトラブルが発生する可能性があります。この場合相手システムの SHA-2 証明書を受信するため、自システムも SHA-2 証明書に対応している必要があります。

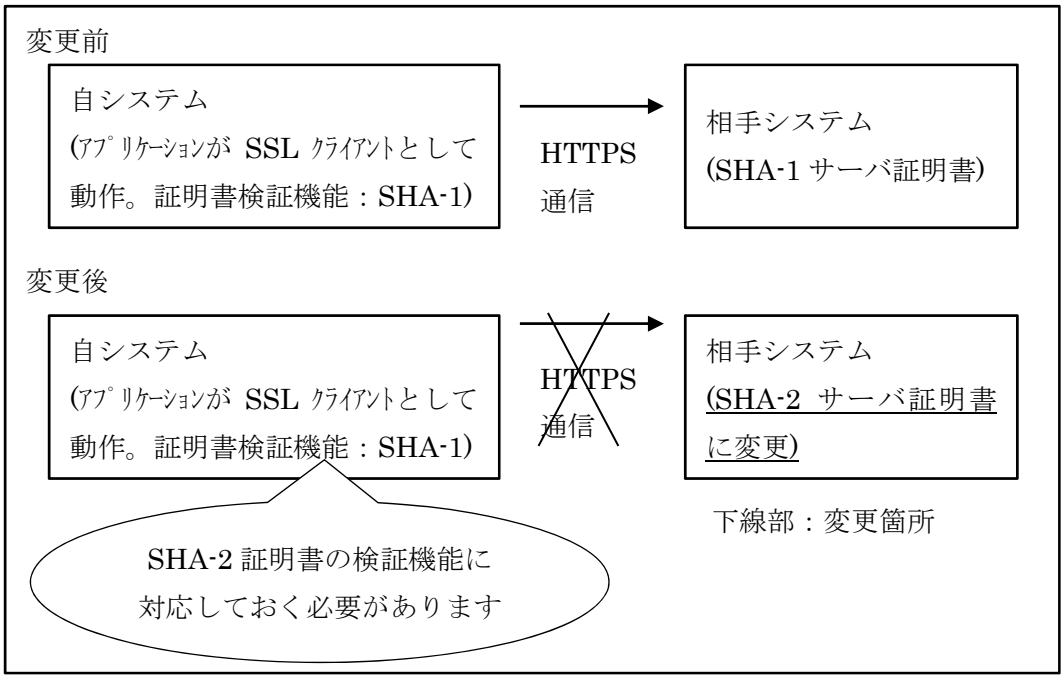

図２　本製品の証明書の変更が必要な例２

本製品の証明書の変更が必要な例３）

自システムでクライアント認証をしている環境で、クライアント側が証明書期限切れなどでクライアント証明書を SHA-2 証明書に変更したとき、当該クライアントが突然通信できなくなるトラブルが発生する可能性があります。この場合、クライアントの SHA-2 証明書を受信するため、自システムも SHA-2 証明書に対応している必要があります。

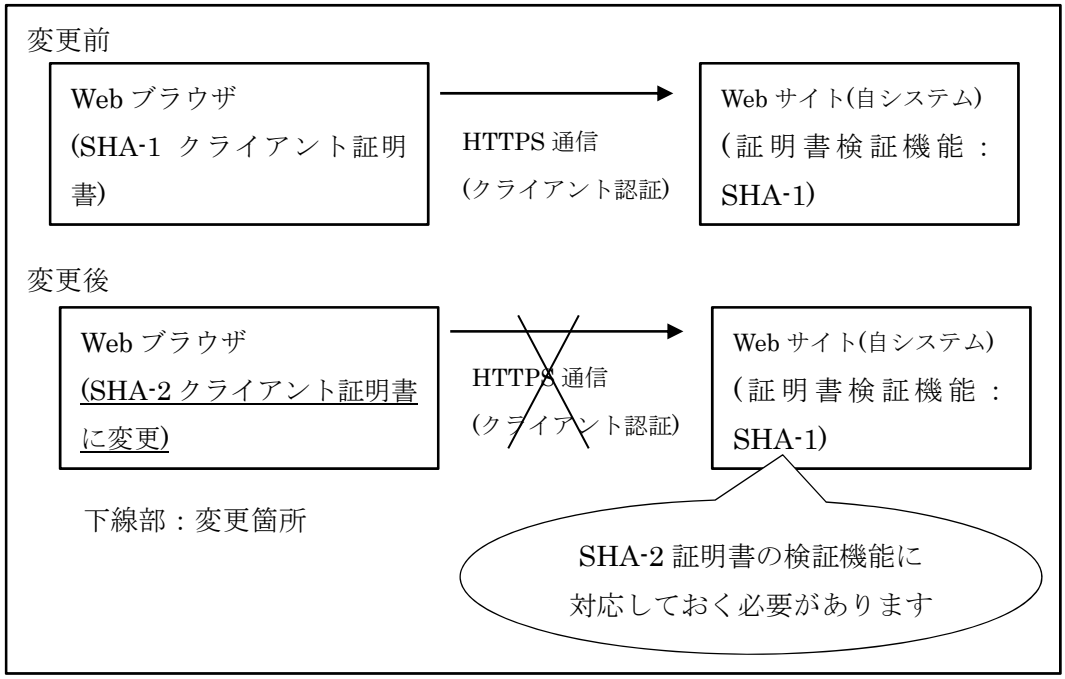

図 3　本製品の証明書の変更が必要な例３

本製品の証明書の変更が不要な例)

SSL アクセラレータで SHA-1 証明書を使用して Web ブラウザと HTTPS 通信し、SSL アクセラレータと Web サイト間は HTTP 通信している環境で、Web ブラウザが SHA-1 証明書の受け入れを拒否する仕様に変更される場合、SSL アクセラレータで使用する証明書を SHA-2 証明書にすれば、Web サイト側での対処は必要ありません。

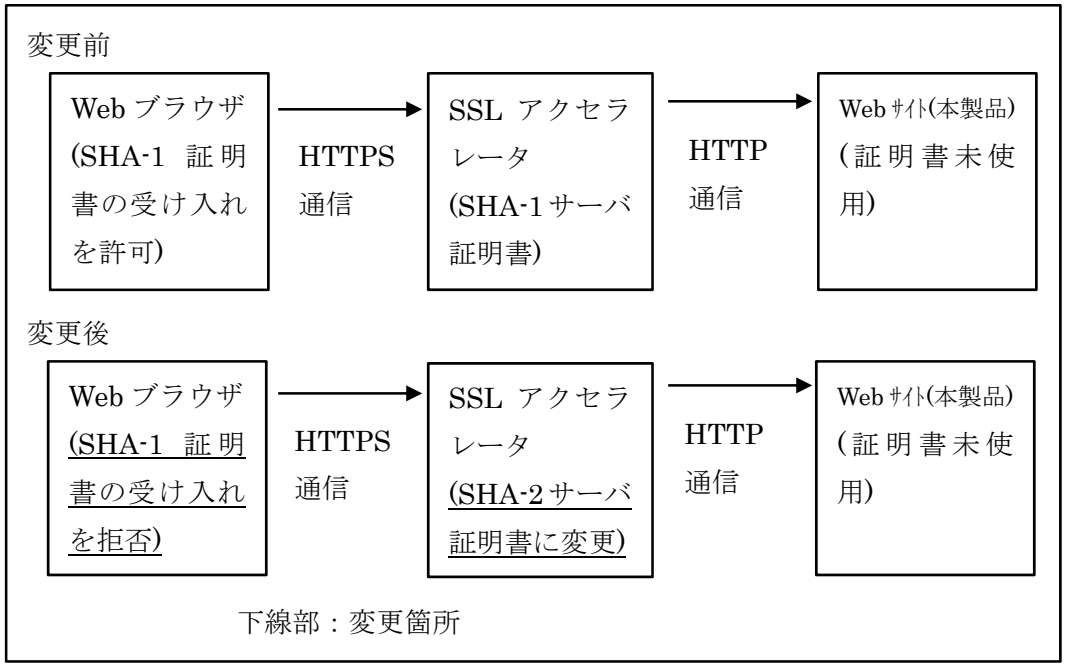

図 4　本製品の証明書の変更が不要な例

３．Web ブラウザの暗号化通信への影響

2017 年 1 月以降、SHA-1 証明書をご使用中の Interstage Application Server のシステムと Web ブラウザの暗号化通信ができなくなる場合があります。

[現象]

現象 A)

2017 年 1 月 31 日以降、SHA-1 証明書をご使用中の Interstage Application Server のシステムと Google Chrome との暗号化通信ができなくなる場合があります。

現象 B)

2017 年 1 月 24 日以降、SHA-1 証明書をご使用中の Interstage Application Server のシステムと Mozilla(R) Firefox(R)との暗号化通信ができなくなる場合があります。

現象 C)

2017 年 2 月 14 日以降、SHA-1 証明書をご使用中の Interstage Application Server のシステムと Windows(R) Internet Explorer(R) 11 との暗号化通信で、Web ブラウザ上に証明書に問題がある旨の警告が出る場合があります。

現象 D)

2017 年 2 月 14 日以降、SHA-1 証明書をご使用中の Interstage Application Server のシステムと Microsoft(R) Edge との暗号化通信で、Web ブラウザ上に証明書に問題がある旨の警告が出る場合があります。

[環境]

現象 A の環境)

1) Interstage Application Server と Google Chrome の間で暗号化通信を行っている。かつ、
2) 公的認証局から発行された SHA-1 証明書をご使用中の場合。

現象 B の環境)

1) Interstage Application Server と Mozilla(R) Firefox(R)の間で暗号化通信を行っている。かつ、
2) 公的認証局から発行された SHA-1 証明書をご使用中の場合。

現象 C の環境)

1) Interstage Application Server と、Windows(R) Internet Explorer(R) 11 の間で暗号化通信を行っている。かつ、
2) 公的認証局から発行された SHA-1 証明書をご使用中の場合。

現象 D の環境)

1) Interstage Application Server と Microsoft(R) Edge の間で暗号化通信を行っている。かつ、
2) 公的認証局から発行された SHA-1 証明書をご使用中の場合。

[発生条件]

Web ブラウザから、Interstage Application Server で SHA-1 証明書をご使用中のシステムに、暗号化通信でアクセスする場合。

[原因]

現象 A の原因)

Google Chrome は、2017 年 1 月 31 日にリリース予定の Chrome 56 で、SHA-1 証明書の受け入れを中止するためです。

現象 B の原因)

Mozilla(R) Firefox(R)は、2017 年 1 月 24 日にリリース予定の Firefox 51 で、SHA-1 証明書の受け入れを中止するためです。

現象 C の原因)

Windows(R) Internet Explorer(R) 11 は、2017 年 2 月 14 日以降、SHA-1 証明書を受け取ると、証明書に問題がある旨の警告を出すためです。

現象 D の原因)

Microsoft(R) Edge は、2017 年 2 月 14 日以降、SHA-1 証明書を受け取ると、証明書に問題がある旨の警告を出すためです。

なお、上記は、2017 年 1 月 17 日現在の情報です。
最新の情報は、それぞれの Web ブラウザに関する公開情報をご参照ください。
(各 URL は、2017 年 1 月 17 日時点で有効なものを記載しています。
URL は、今後変更になる場合があります)

Google Chrome
https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html

Mozilla(R) Firefox(R)
https://blog.mozilla.org/security/2016/10/18/phasing-out-sha-1-on-the-public-web/

Windows(R) Internet Explorer(R)、Microsoft(R) Edge
https://blogs.technet.microsoft.com/jpsecurity/2015/11/02/faq-sha-1-sha-2/
https://aka.ms/sha1

４．対処方法

1) SHA-2 証明書に対応している製品をご使用中の場合は、SHA-1 証明書から SHA-2 証明書への切り替えをお願いいたします。

2) SHA-2 証明書に対応していない製品をご使用中の場合は、SHA-2 証明書に対応して

いる製品へのバージョンアップ、および SHA-2 証明書への切り替えをお願いいたします。

５．ご使用の証明書が SHA-2 か SHA-1 かの確認方法

1) 証明書/鍵管理環境として Interstage 証明書環境をご使用の場合

Interstage 証明書環境では、証明書のアルゴリズムを確認する機能は提供しておりません。登録した当時の証明書をご確認ください。

2) 証明書/鍵管理環境として SMEE コマンドで構築した証明書/鍵管理環境をご使用の場合

(1) 確認したい証明書を表示します。

SMEE コマンドの cmdspcert(※3)に、-ed、-nn オプション(※4)を指定し証明書を表示します。

■表示例

```
CERTIFICATE:
  VERSION:                    V3
  SERIALNUMBER:               0C
  SIGNATURE ALGORITHM:        SHA1WithRSAEncryption
以降省略
```

(2) SHA-2 か SHA-1 かの確認

(1)で表示された証明書の「SIGNATURE ALGORITHM」に出力されている文字列で確認します。

出力された文字列により SHA-2 か SHA-1 を判断できます。

SHA1WithRSAEncryption → SHA-1 の証明書です。

SHA256WithRSAEncryption → SHA-2 の証明書です。
(ハッシュアルゴリズムが SHA-256)

SHA384WithRSAEncryption → SHA-2 の証明書です。
(ハッシュアルゴリズムが SHA-384)

SHA512WithRSAEncryption → SHA-2 の証明書です。
(ハッシュアルゴリズムが SHA-512)

(※3)コマンドの詳細は以下マニュアルを参照。

Interstage Application Server リファレンスマニュアル
(コマンド編)
SSL 環境設定編
＞ SSL 環境設定コマンド
＞ cmdspcert

(※4)SMEE コマンドの cmentcert で証明書登録時に指定した-ed、-nn オプションを指定する。

3) 証明書/鍵管理環境としてキーストアをご使用の場合

JDK keytool の 「データの表示」コマンド(-list)に、-v オプションを指定することで、署名アルゴリズム名を確認できます。
JDK ドキュメントの keytool の説明を参照してください。
JDK7 の場合：
http://docs.oracle.com/javase/jp/7/technotes/tools/windows/keytool.html

(1) keytool の 「データの表示」コマンド(-list)を実行します。

■表示例

```
keytool -list -v -keystore sample

別名: sample
作成日: 2016/08/29
エントリ・タイプ: trustedCertEntry
所有者: CN＝xx, OU＝xx, O＝xx, C＝xx
発行者: CN＝xx, OU＝xx, O＝xx, C＝xx
シリアル番号: 1e97fe60
有効期間の開始日: Mon Aug 29 09:16:40 JST 2016 終了日: Tue
 Aug 29 09:16:40 JST 2017
 証明書のフィンガプリント:
        MD5:  F0:1B:2B:9F:17:45:49:49:1E:05:E4:EE:4F:D6:21:
              73
        SHA1: 4C:EC:AC:73:FE:D0:FC:66:DB:7D:E9:D5:97:3E:3C:
              03:48:6F:D4:17
        SHA256: 94:6D:48:55:E5:62:C7:1A:99:C4:21:F4:89:4D:
                76:78:03:89:AB:1E:95:04:32:E5:E9:74:B2:35:
```

19:15:80:19
署名アルゴリズム名: SHA256withRSA
バージョン: 3
拡張:
・・・(略)・・・

(2) SHA-2 か SHA-1 か確認します。

(1)の表示の「署名アルゴリズム名」に出力されている文字列で確認します。
出力された文字列により SHA-2 か SHA-1 を判断できます。
- SHA1withDSA、SHA1withRSA の場合、SHA-1 をベースにしたアルゴリズムで署名されています。
- SHA256withRSA、SHA384withRSA、SHA512withRSA の場合、SHA-2 をベースにしたアルゴリズムで署名されています。

６．SHA-2 証明書への変更方法

SHA-2 証明書は、各認証局から取得してください。
SHA-2 証明書への変更方法は、マニュアルに記載の証明書の更新と同様の手順で実施します。
認証局によっては移行前に使用していた「認証局の証明書(発行局証明書)」や「中間 CA 証明書(中間認証局証明書)」と異なる場合があります。
そのためサイト証明書の登録前に、SHA-2 証明書に必要な「認証局の証明書」や「中間 CA 証明書」の確認を行い、不足している証明書を登録する必要があります。
なお、証明書の更新の手順については、ご使用の証明書/鍵管理環境のマニュアルを参照してください。また、SHA-2 証明書に必要な「認証局の証明書」や「中間 CA 証明書」については、ご使用の認証局に問合せてください。

1) 証明書/鍵管理環境として Interstage 証明書環境をご使用の場合

以下のマニュアルを参照してください。
Interstage Application Server セキュリティシステム運用ガイド
SSL による暗号化通信
＞ Interstage 証明書環境の構築と利用
＞ 証明書の管理

2) 証明書/鍵管理環境として SMEE コマンドで構築した証明書/鍵管理環境をご使用の場合

以下のマニュアルを参照してください。

Interstage Application Server セキュリティシステム運用ガイド

SSL による暗号化通信

＞ SMEE コマンドによる証明書/鍵管理環境の構築と利用

＞ 証明書/鍵管理環境の管理

3) 証明書/鍵管理環境としてキーストアをご使用の場合

JDK keytool で、鍵と証明書を管理する場合は、-sigalg オプションで署名アルゴリズムを指定します。

JDK ドキュメントの keytool の説明を参照してください。

JDK7 の場合：

http://docs.oracle.com/javase/jp/7/technotes/tools/windows/keytool.html

７．SHA-1 証明書の有効期限が切れる場合の注意事項

公的認証局は、既に 2016 年 1 月から SHA-1 証明書の発行を停止しています。

したがって、これから SHA-1 証明書の有効期限を迎える場合は、SHA-2 証明書に切り替える必要があります。

８．JDK のバージョンよる SHA-2 証明書対応可否

証明書/鍵管理環境として、キーストアを使用している場合は、JDK のバージョンにより、SHA-2 証明書対応可否がことなります。本製品の各バージョンに搭載されている JDK のバージョンと SHA-2 証明書対応可否について以下に示します。

表 2 Interstage Application Server/Interstage Business Application Server/Interstage Web Server 各バージョンに搭載されている JDK のバージョンと SHA-2 証明書の関係

JDK のバージョン / 製品のバージョン	1.1	1.2	1.3	1.4	5	6	7
V5	×	×	×	×	－	－	－

V6	－	×	×	×	－	－	－
V7	－	－	×	×	－	－	－
V8	－	－	×	×	－	－	－
V9.0/V9.1	－	－	－	×	○	－	－
V9.2/V9.3	－	－	－	×	○	○	－
V10	－	－	－	－	○	○	－
V11	－	－	－	－	－	○	○

○：SHA-2 証明書対応　×：SHA-2 証明書非対応　－：対象の JDK 非搭載

表 3 Interstage Job Workload Server 各バージョンに搭載されている JDK のバージョンと SHA-2 証明書の関係

JDK のバージョン (注) / 製品のバージョン	1.1	1.2	1.3	1.4	5	6	7
V8	－	－	×	×	－	－	－
V9.0.0～V9.1.0	－	－	－	×	○	－	－
V9.2.0～V9.3.0	－	－	－	×	○	○	－
V9.3.1	－	－	－	－	○	○	－
V9.3.2～V9.4.1	－	－	－	－	－	○	○

○：SHA-2 証明書対応　×：SHA-2 証明書非対応　－：対象の JDK 非搭載

注)JDK は、本製品内の Interstage Application Server 部分に搭載されており、そのバージョンを記載しています。

表 4 Interstage Service Integrator 各バージョンに搭載されている JDK のバージョンと SHA-2 証明書の関係

JDK のバージョン (注) / 製品のバージョン	1.1	1.2	1.3	1.4	5	6	7
V9.0.0～V9.1.0	－	－	－	×	○	－	－
V9.2.0～V9.3.1 V9.4.0(Solaris(32bit)以外)	－	－	－	×	○	○	－
V9.4.0(Solaris(32bit)のみ)	－	－	－	－	○	○	－
V9.4.1～V9.6.1	－	－	－	－	－	○	○

○：SHA-2 証明書対応　×：SHA-2 証明書非対応　－：対象の JDK 非搭載

注)JDK は、本製品内の Interstage Application Server 部分に搭載されており、そのバージョンを記載しています。

９．本情報の対象となる環境

表 5　本情報の対象となる環境

本情報の対象製品	[Windows(x86)] Interstage Application Server Enterprise Edition V5～V11 Interstage Application Server Standard-J Edition V8～V11 Interstage Application Server Standard Edition V5～V7 Interstage Application Server Plus V5～V7 Interstage Application Server Web-J Edition V5～V8 Interstage Web Server Express V11 Interstage Web Server V9～V10 Interstage Business Application Server Standard Edition V8～V11 Interstage Job Workload Server V9 Interstage Service Integrator Enterprise Edition V9 Interstage Service Integrator Standard Edition V9 [Windows(x64)] Interstage Application Server Enterprise Edition V9～

	V11 Interstage Application Server Standard-J Edition V9～V11 Interstage Business Application Server Enterprise Edition V11 Interstage Business Application Server Standard Edition V11 Interstage Job Workload Server V9 Interstage Service Integrator Enterprise Edition V9 Interstage Service Integrator Standard Edition V9 [Windows(Itanium)] Interstage Application Server Enterprise Edition V8～V9 Interstage Application Server Standard-J Edition V9 [Solaris(32bit)] Interstage Application Server Enterprise Edition V5～V11 Interstage Application Server Standard-J Edition V5～V11 Interstage Application Server Standard Edition V5～V7 Interstage Application Server Plus V5～V7 Interstage Application Server Web-J Edition V5～V8 Interstage Web Server Express V11 Interstage Web Server V9～V10 Interstage Business Application Server Enterprise Edition V7～V11 Interstage Business Application Server Standard Edition V8～V11 Interstage Job Workload Server V8～V9 Interstage Service Integrator Enterprise Edition V9 Interstage Service Integrator Standard Edition V9 [Solaris(64bit)] Interstage Application Server Enterprise Edition V11 Interstage Application Server Standard-J Edition V11

	Interstage Business Application Server Enterprise Edition V11 Interstage Business Application Server Standard Edition V11 Interstage Job Workload Server V9 Interstage Service Integrator Enterprise Edition V9 Interstage Service Integrator Standard Edition V9 [Linux(x86)] Interstage Application Server Enterprise Edition V5～V11 Interstage Application Server Standard-J Edition V8～V11 Interstage Application Server Standard Edition V5～V7 Interstage Application Server Plus V5～V7 Interstage Application Server Web-J Edition V5～V8 Interstage Web Server Express V11 Interstage Web Server V9～V10 Interstage Business Application Server Standard Edition V8～V11 Interstage Service Integrator Enterprise Edition V9 Interstage Service Integrator Standard Edition V9 [Linux(Intel64)] Interstage Application Server Enterprise Edition V9～V11 Interstage Application Server Standard-J Edition V9～V11 Interstage Business Application Server Enterprise Edition V9～V11 Interstage Business Application Server Standard Edition V9～V11 Interstage Job Workload Server V9 Interstage Service Integrator Enterprise Edition V9 Interstage Service Integrator Standard Edition V9

	[Linux(Itanium)] Interstage Application Server Enterprise Edition V7～V9 Interstage Application Server Standard-J Edition V9 Interstage Business Application Server Enterprise Edition V8～V9 Interstage Business Application Server Standard Edition V8～V9 Interstage Job Workload Server V8～V9 Interstage Service Integrator Enterprise Edition V9 Interstage Service Integrator Standard Edition V9
対象製品の動作 OS	[Windows(x86)製品のサーバパッケージ] Microsoft(R) Windows Server(R) 2016 Standard Microsoft(R) Windows Server(R) 2016 Datacenter Microsoft(R) Windows Server(R) 2012 Foundation Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Datacenter Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Datacenter Microsoft(R) Windows Server(R) 2008 Foundation Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter Microsoft(R) Windows Server(R) 2008 R2 Foundation [Windows(x64)製品のサーバパッケージ] Microsoft(R) Windows Server(R) 2016 Standard

	Microsoft(R) Windows Server(R) 2016 Datacenter Microsoft(R) Windows Server(R) 2012 Foundation Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Datacenter Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Datacenter Microsoft(R) Windows Server(R) 2008 Foundation Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter Microsoft(R) Windows Server(R) 2008 R2 Foundation [Windows(Itanium)製品のサーバパッケージ] Microsoft(R) Windows Server(R) 2008 for Itanium-Based Systems [Solaris(32bit)製品のサーバパッケージ] Oracle Solaris 11 Oracle Solaris 10 Oracle Solaris 9 Oracle Solaris 8 [Solaris(64bit)製品のサーバパッケージ] Oracle Solaris 11 Oracle Solaris 10

	[Linux(x86)製品のサーバパッケージ] Red Hat Enterprise Linux 6 (for x86) Red Hat Enterprise Linux 6 (for Intel64) Red Hat Enterprise Linux 5 (for x86) Red Hat Enterprise Linux 5 (for Intel64) Red Hat Enterprise Linux AS (v.4 for x86) Red Hat Enterprise Linux AS (v.4 for EM64T) [Linux(Intel64)製品のサーバパッケージ] Red Hat Enterprise Linux 6 (for Intel64) Red Hat Enterprise Linux 5 (for Intel64) [Linux(Itanium)製品のサーバパッケージ] Red Hat Enterprise Linux AS (v.4 for Itanium) Red Hat Enterprise Linux 5 (for Intel Itanium) [本製品のクライアントパッケージ] Windows(R) 10 Home Windows(R) 10 Pro Windows(R) 10 Enterprise Windows(R) 8.1 Windows(R) 8.1 Pro Windows(R) 8.1 Enterprise Windows(R) 8 Windows(R) 8 Pro Windows(R) 8 Enterprise Windows(R) 7 Ultimate Windows(R) 7 Enterprise Windows(R) 7 Professional Windows(R) 7 Home Premium Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Home Basic Windows Vista(R) Home Premium Windows Vista(R) Ultimate

－以上－

改版履歴

版数	改版日	変更内容
初版	2016年7月22日	新規作成
第二版	2016年8月26日	対象の製品に、Interstage Job Workload Server、Interstage Service Integratorを追加。 問い合わせ方法や誤字の修正。
第三版	2016年10月28日	Webブラウザの暗号化通信への影響、対処方法、ご使用の証明書がSHA-2かSHA-1かの確認方法、SHA-2証明書への変更方法、2017年より前にSHA-1証明書の有効期限が切れる場合の注意事項を追加。 本情報の対象となる環境に、Solaris(32bit)版Interstage Business Application Server Enterprise Edition V7を追加。
第四版	2017年1月27日	Webブラウザでの SHA-1証明書の扱いを最新化。 「2017年より前にSHA-1証明書の有効期限が切れる場合の注意事項」を「SHA-1証明書の有効期限が切れる場合の注意事項」に変更。