日本ベリサイン CPS3.8 における変更点は、以下となります。

	対象セクション	変更内容
1	全体	変更前記載：CPS3.7 米国ベリサイン（ベリサイン） 変更後記載：CPS3.8 米国シマンテック（日本ベリサイン及び米国シマンテック）
2	全体	変更前記載：CPS3.7 EV SSL 証明書 変更後記載：CPS3.8 EV 証明書

3	全体	変更前記載：CPS3.7
		http;//www.verisign.co.jp
		
		変更後記載：CPS3.8
		https;//www.verisign.co.jp

4	全体	誤記修正
5	Trademark Notice	変更前記載：CPS3.7 P.2 VeriSign は、VeriSign Inc.の登録商標である。VeriSign のロゴ、VeriSign Trust Network、Netsure は、VeriSign Inc.の商標並びにサービス・マークである。本文書中のその他の商標及びサービス・マークには、それぞれの権利者に帰属する。 変更後記載：CPS3.8 シマンテック（Symantec）、 ノートン（Norton）、およびチェックマークロゴ（the Checkmark Logo）は米国シマンテック・コーポレーション（Symantec Corporation） またはその関連会社の米国またはその他の国における登録商標、または、商標である。

		ベリサイン（VeriSign）、ベリサイン・トラスト（VeriSign Trust）、およびその他の関連するマークは米国 VeriSign, Inc.またはその関連会社の米国またはその他の国における登録商標、または、商標である。その他の名称もそれぞれの所有者による商標である可能性がある。
6	1.3.1 認証機関	変更前記載：CPS3.7 P.12 また、米国ベリサインは「ベリサイン・ユニバーサル・ルート認証機関」を管理する。ベリサイン・ユニバーサル・ルート認証機関は、特定の認証 Class で定義されるものではなく、下位認証機関の任意の Class を発行する場合がある。 変更後記載：CPS3.8 P.12 また、米国シマンテックは「ベリサイン・ユニバーサル・ルート認証機関」及び「ベリサイン・ECC ユニバーサル・ルート認証機関」を管理する。ベリサイン・ユニバーサル・ルート認証機関は、特定の認証 Class で定義されるものではなく、下位認証機関の任意の Class を発行する場合がある。
7	1.4.1.2 組織に発行される証明書	変更後記載：CPS3.8 P.14 Table 2 Class 3 EV 証明書の行を追加。
8	2.2 証明書情報の公表	変更前記載：CPS3.7 P.17～18 Table 3 米国ベリサイン第一次認証機関及び米国ベリサイン中間認証機関ルート証明書 最新のブラウザに含まれ、下記のクエリーを通じて利用者証明書と共に取得できる証明書チェーンの一部として、依拠当事者に利用可能 変更後記載：CPS3.8 P.17～18 Table 3 VTN 第一次認証機関及び VTN ルート認証機関証明書 最新のブラウザに含まれ、依拠当事者に利用可能
9	2.2 証明書情報の公表	変更前記載：CPS3.7 P.17～18 Table 3 利用者証明書

		また、directory.verisign.com にある米国ベリサイン LDAP ディレクトリ・サーバにおけるクエリーを通じても利用可能 変更後記載：CPS3.8 P.17～18 Table 3 記載削除
	3.2.2 組織の実在性確認	変更後記載：CPS3.8 P.22 Table 6 ACS 証明書の行を追加
	3.2.3 個人の実在性確認	変更前記載：CPS3.7 P.22 Table 7 Class 3 の管理者証明書の認証は、組織の確認、雇用の確認及び管理者の権限の確認に基づき行う。 変更後記載：CPS3.8 P.22 Table 7 Class 3 の管理者証明書の認証は、組織の確認、実在性の確認及び管理者の権限の確認に基づき行う。
10	4.9.6 依拠当事者に要求される CRL の調査	変更前記載：CPS3.7 P.33 認証機関は、失効のステータスを調査するために、依拠当事者に、適切な CRL、ウェブ・ベースのリポジトリまたは OCSP(利用可能である場合)の所在場所についての情報を提供する。 変更後記載：CPS3.8 P.33 認証機関は、失効のステータスを調査するために、依拠当事者に、適切な CRL、LDAP　ベースのリポジトリまたは OCSP(利用可能である場合)の所在場所についての情報を提供する。
11	4.9.9 利用可能なオンラインによる失効/ステ	変更前記載：CPS3.7 P.34 オンラインによる失効及び他の証明書のステータス情報は、ウェブ・ベースの

	ータス調査	リポジトリ及び（提供されている場合は）OCSP を通じて提供される。 変更後記載：CPS3.8 P.34 オンラインによる失効及び他の証明書のステータス情報は、LDAP ベースのリポジトリ及び（提供されている場合は）OCSP を通じて提供される。
12	4.10.2 サービスの可用性 （旧：サービスの利用可能性）	変更前記載：CPS3.7 P.35 証明書ステータス・サービスは、1 日 24 時間利用可能である。 変更後記載：CPS3.8 P.35 証明書ステータス・サービスは、計画停止を除き 24 時間 365 日利用可能である。
13	4.12 鍵の預託と復旧	変更前記載：CPS3.7 P.36 キーマネージメントサービスを用いるエンタープライズ・カスタマは、自己が承認した証明書申請を行った利用者の秘密鍵のコピーを預託することできる。日本ベリサインは、利用者の秘密鍵の保管は行わないものの、当該利用者の鍵の復旧手順に関し、重要な役割を果たす。 変更後記載：CPS3.8 P.35～36 キーマネージメントサービス(または日本ベリサインが承認した同等のサービス)を用いるエンタープライズ・カスタマは、自己が承認した証明書申請を行った利用者の秘密鍵のコピーを預託することできる。キーマネージメントサービス(または日本ベリサインが承認した同等のサービス)は日本ベリサインの安全なデータ・センタ施設内もしくは施設外で運用される。日本ベリサインは、利用者の秘密鍵の保管は行わないものの、当該利用者の鍵の復旧手順に関し、重要な役割を果たす。
14	4.12.2 セッションキーのカプセル化及び復旧	変更前記載：CPS3.7 P.36～37 秘密鍵は、エンタープライズ・カスタマの施設内で暗号化され保管される。それ

	のポリシー及び実施	ぞれの利用者秘密鍵は、個々に triple-DES で暗号化される。Key Escrow Record (KER) が生成され、次に、triple-DES の鍵が、ハードウェアの中で生成されたランダムセッションキーマスクと結合され、破棄される。結果として生じたマスクドセッションキー(MSK)のみが、日本ベリサインに安全に送られ、保管される。KER(エンドユーザの秘密鍵を含む) とランダムセッションキーマスクは、エンタープライズ・カスタマの施設内のキーマネージャー・データベースに保管される。 秘密鍵及び電子証明書の復旧の場合、(中略)キーマネージャーは、MSKをランダムセッションキーと結合させ、最初に秘密鍵を暗号化するのに使われた triple-DES の鍵を再生成し、エンドユーザの秘密鍵を復旧させる。 変更後記載:CPS3.8 P.36～37 秘密鍵は、キーマネージャー・データベース内で暗号化され保管される。それぞれの利用者秘密鍵は、個々に triple-DES で暗号化される。Key Escrow Record (KER) が生成され、次に、triple-DES の鍵が、ハードウェアの中で生成されたランダムセッションキーマスクと結合される。結果として生じたマスクドセッションキー(MSK)のみが、日本ベリサインのマネージド PKI データベースに安全に送られ、保管される。KER(エンドユーザの秘密鍵を含む) と個々のセッションキーは、キーマネージャー・データベースに保管され、その他の鍵関連データは破棄される。 マネージド PKI データベースは日本ベリサインのデータ・センタ施設外から安全に操作することができる。エンタープライズ・カスタマはキーマネージャー・データベースを日本ベリサインの安全なデータ・センタ施設内もしくは施設外で運用することができる。 秘密鍵及び電子証明書の復旧の場合、(中略)キーマネージャーは、キーマネージャー・データベースからセッションキーを取り出し MSK と結合させ、最初に秘密鍵を暗号化するのに使われた triple-DES の鍵を再生成し、エンドユーザの秘密鍵を復旧させる。
15	5.1.8 オフサイト・バックアップ	変更前記載:CPS3.7 P.39 日本ベリサインは、セキュアなオフサイト施設において、重要なシステム・デー

		タ、監査記録その他の機密情報のバックアップを定期的に行う。 変更後記載：CPS3.8 P.39 日本ベリサインは、重要なシステム・データ、監査記録その他の機密情報のバックアップを定期的に行う。オフサイト・バックアップ・メディアは、保障付きの第三者の保管施設及び日本ベリサインの災害復旧施設を使用する物理的に安全な方法で保管される。
16	5.2.4 職務の分離を必要とする役割	変更前記載：CPS3.7 P.40 ・証明書申請、失効要求、更新要求または申込情報の承認、拒絶その他の処理 変更後記載：CPS3.8 P.40 ・証明書申請、失効要求、復旧要求、更新要求または申込情報の承認、拒絶その他の処理
17	5.7.3 エンティティの秘密鍵が危殆化した場合の手続	変更前記載：CPS3.7 P.46 日本ベリサイン認証機関、日本ベリサインのインフラストラクチャまたはカスタマ認証機関の秘密鍵についての危殆化が認知されるか、その疑いが生じた場合、日本ベリサインの鍵危殆化対応手続が、危殆化事故対応チームにより制定される。このチームは、セキュリティ、暗号ビジネス運用、プロダクション・サービスの要員及び他の日本ベリサイン管理者の代表者を含むものであるが、（以下省略） 変更後記載：CPS3.8 P.46 日本ベリサイン認証機関、日本ベリサインのインフラストラクチャまたはカスタマ認証機関の秘密鍵についての危殆化が認知されるか、その疑いが生じた場合、日本ベリサインの鍵危殆化対応手続が、インシデントレスポンスチームにより制定される。このチームは、セキュリティ、キーマネージャー、システム運用部門の要員及び他の日本ベリサイン管理者の代表者を含むものであるが、（以下省略）

18	6.1.1 キー･ペア生成	変更前記載：CPS3.7 P.49 マネージド PKI カスタマは、自動承認サーバを用いて、自らのキー・ペアを生成する。 変更後記載：CPS3.8 P.49 マネージド PKI カスタマは、自動承認サーバで使用されるキー・ペアを生成する。
19	6.1.2 秘密鍵の受渡	変更前記載：CPS3.7 P.49 エンドユーザ利用者のキー・ペアは、当該利用者自身により通常生成されるため、この場合には利用者への秘密鍵の受渡は生じない。 変更後記載：CPS3.8 P.49 エンドユーザ利用者のキー・ペアは、当該利用者自身により通常生成されるため、この場合には利用者への秘密鍵の受渡は生じない。ACS アプリケーション ID の場合も、秘密鍵の受渡は生じない。
20	6.1.5 鍵のサイズ	変更前記載：CPS3.7 P.50 米国ベリサインの第三世代（G3）の一次認証機関は2048 ビットのRSA キー・ペアを有する。 日本ベリサインは、登録機関及び利用者に対し 1024 ビットの RSA キー・ペアを生成するように推奨する。日本ベリサインは、利用者のキー・ペアが 512 ビット以下の場合には、承認しない場合がある。 変更後記載：CPS3.8 P.50 米国シマンテックの第一世代(G1)及び第二世代(G2)の第一次認証機関とこれらにより発行された下位認証機関は 1024 ビットの RSA キー・ペアを有する。第三世代（G3）及び第五世代(G5)の第一次認証機関は 2048 ビットの RSA キー・ペアを有する。RSA キー･ペアを用いた各 Class の証明書への署名は 2013 年 12 月 31 日までに 2048 ビット以上の（またはそれと同等の強度の）鍵

		サイズを有する第一次認証機関よりなされるよう、変更されなければならない。 日本ベリサインは、登録機関及び利用者に対し 2048 ビットの RSA キー・ペアを生成するように推奨する。2013 年 12 月 31 日を以て 1024 ビットの RSA キー･ペアを使用して発行された全ての証明書の使用を終了する。 米国シマンテックの Class 3 第一次認証機関の第四世代(G4)「ECC ユニバーサル・ルート認証機関」は 384 ビット ECC キー･ペアにより生成されている。 全 Class における VTN 第一次認証機関とその下位認証機関、登録局及び利用者証明書に含まれるデジタル署名では、SHA-1 及び SHA-2 署名アルゴリズムが使用される。また、特定のバージョンのプロセッシング・センタでは、利用者証明書の発行において、SHA-256 と SHA-384 を使用することができる。
21	6.2.5 秘密鍵の保管	変更前記載：CPS3.7 なし 変更後記載：CPS3.8 P.52 日本ベリサイン認証機関の満了時、その証明書に紐付くキー・ペアは、本 CPS に定める要件に合致するハードウェア暗号モジュールを用い最低 5 年間確実に保存される。認証局証明書は、本 CPS に定める期間内にリニューアルされない限り、これらの認証局キー・ペアは、それらの期間満了後、署名に使用されることはない。 日本ベリサインは、登録機関及び利用者のキー・ペアのコピーについては保管しない。
22	6.2.10 秘密鍵の破壊の方法（旧章番号：6.2.9）	変更前記載：CPS3.7 P.54 鍵の破壊が完了した際には、認証機関の鍵破壊活動は記録される。 変更後記載：CPS3.8 P.54

		鍵の破壊に関する認証機関の活動は記録される。ACS アプリケーション ID の秘密鍵については、証明書の利用と同時に鍵がシステムから破棄される。
23	6.3.2 証明書の運用期間及びキー・ペアの使用期間	変更前記載：CPS3.7 P.54 Table 8 認証機関(オンライン)から利用者(組織) 通常 3 年まで 変更後記載：CPS3.8 P.55 Table 8 ・認証機関(オンライン)から利用者(組織) 通常 5 年まで ・また、自己署名された第一次認証機関の行を 2 行追加
24	6.3.2 証明書の運用期間及びキー・ペアの使用期間	変更前記載：CPS3.7 P.55 VTN CP のセクション6.3.2 について、日本ベリサインPMA は、米国ベリサインの承認を得た上で、CA キー・ペアの移行中にPKI サービスが中断しないように、指定の制限数を拡張し、CA 数を増加する例外措置を認めるものとする。 変更後記載：CPS3.8 P.55 VTN CP のセクション 6.3.2 について、日本ベリサインは、認証局キー・ペアの移行中に PKI サービスが中断しないように、例外措置として認証局が上記の指定を超える有効期間を持つことを認めるものとする。
25	6.3.2 証明書の運用期間及びキー・ペアの使用期間	変更前記載：CPS3.7 P.55 また、米国ベリサインは「VeriSign Class 3 International Server CA」ならびに「Class 3 Open Financial Exchange CA – G2」も管理する。これらはPCA によって署名されているオンライン認証局である。 変更後記載：CPS3.8 P.56 また、米国シマンテックは「VeriSign Class 3 International Server CA」、

		「Thawte SGC CA」ならびに「Class 3 Open Financial Exchange CA」も管理する。これらは第一次認証機関によって署名されているオンライン認証局である。
26	7.1.3 アルゴリズムオブジェクト識別子	変更前記載：CPS3.7 P.62 記載なし 変更後記載：CPS3.8 P.62 ecdsa-with-Sha256 OBJECT IDENTIFIER の記載を追加
27	7.1.3 アルゴリズムオブジェクト識別子	変更前記載：CPS3.7 P.63 これらのアルゴリズムを用いて生成された証明書の署名は、RFC3279 に従わなければならない。sha-1WithRSAEncryption の使用は、md5WithRSAEncryption よりも強く推奨される。 md2WithRSAEncryption は、利用者証明書にはもはや使用されない。ただし、一部のとても古い認証機関及び利用者証明書のためのCRL への署名においては使用される。 変更後記載：CPS3.8 P.63 これらのアルゴリズムを用いて生成された証明書の署名は、RFC3279 に従わなければならない。sha-1WithRSAEncryption は今後、md5WithRSAEncryption に代わって使用される。 md5WithRSAEncryption による署名は、レガシー・アプリケーションをサポートし事業継続性を保全する目的であると事前の承認を得た場合においてのみ使用される。
28	7.2 CRL のプロファイル	変更前記載：CPS3.7 P.64 Table 13 Signature Algorithm ベリサインのCRL は、RFC3279 に従い、sha1RSA(OID: 1.2.840.113549.1.1.5)、md5RSA(OID:1.2.840.113549.1.1.4)またはmd2RSA(OID: 1.2.840.113549.1.1.2)アルゴリズムを用い署名される。

		変更後記載：CPS3.8 P.64 Table 13 Signature Algorithm RFC3279 (CP セクション 7.1.3)に従う。
29	7.3 OCSP プロファイル	変更前記載：CPS3.7 P.64 日本ベリサインは、OCSP を以下に対して使用する。 o Class 2 におけるエンタープライズ向け証明書 OCSP レスポンダーは、RFC2560 に準拠する。 変更後記載：CPS3.8 P.64 日本ベリサインは、OCSP を以下の証明書に対して使用する。 ・RFC2560 に準拠する、Class 2 におけるエンタープライズ向け証明書 ・RFC5019 に準拠する、TGV (VeriSign's Trusted Global Validation protocol) において使用される Class 3 組織向け証明書
30	7.3.1 バージョン番号	変更前記載：CPS3.7 P.64 RFC2560 に規定される OCSP のバージョン 1 の仕様がサポートされる。 変更後記載：CPS3.8 P.64 RFC2560 もしくは RFC5019 に規定される OCSP のバージョン 1 の仕様がサポートされる。
31	7.3.2 OCSP エクステンション	変更前記載：CPS3.7 P.64 規定しない。 変更後記載：CPS3.8 P.64 TGV サービスでは、OCSP レスポンスの最新性を確立するためにタイムスタンプと有効期限を参照する。日本ベリサインでは OCSP レスポンスの最新性の

		確立のために Nonce エクステンションを使用しない。また、クライアントは OCSP レスポンスに含まれる Nonce エクステンションの値がこれに該当する OCSP リクエストの値と一致することを要求できない。OCSP レスポンスの最新性の確認のためにはローカル時刻を参照することとする。
32	Appendix A 略語	変更後記載：CPS3.8 P.77 QGIS 、QIIS の行を追加
33	Appendix A 定義	変更後記載：CPS3.8 P.82 VSJ Repository 日本ベリサイン・リポジトリ の行を追加 （VeriSign Repository の行を削除）
34	Appendix B1 Section 2	変更前記載：CPS3.7 P.83 EV証明書は、TLS/SSLプロトコルを使ったウェブベースのデータ通信を確立するために使われることを意図している。 変更後記載：CPS3.8 P.83 EV証明書は、TLS/SSLプロトコルを使ったウェブベースのデータ通信の確立、及び、実行コードの信頼性の検証のために使われることを意図している。
35	Appendix B1 Section 2 (a)	変更後記載：CPS3.8 P.83 以下の記載を追加 実行コードの発行元の確認: アプリケーションソフトウェアに依拠するユーザに対し、そのコードがEV証明書に記載の名前、事業所所在地の住所、法人設立/登録管轄地、登録番号で特定される法人によって提供されていることを合理的に保証する。
36	Appendix B1 Section 2 (b)	変更前記載：CPS3.7 P.83 EV SSL証明書の第2の目的は、ウェブ・サイトを運営する組織の正当性の立

		証を支援すること、及び、フィッシングその他のオンラインアイデンティティ詐欺に関連する問題に対処する手段を提供することである。EV SSL証明書は、ウェブ・サイト所有者に関する第三者が審査した信頼性の高いアイデンティティ情報及び住所情報を提供することによって、以下に貢献する。 変更後記載：CPS3.8 P.83 EV 証明書の第2の目的は、ウェブ・サイトを運営、もしくは実行コードを流通させている組織の正当性の立証を支援すること、及び、フィッシング、破壊工作ソフトその他のオンラインアイデンティティ詐欺に関連する問題に対処する手段を提供することである。EV 証明書は、組織に関して第三者が審査した信頼性の高いアイデンティティ情報及び住所情報を提供することによって、以下に貢献する。
37	Appendix B1 Section 3 (a)	変更前記載：CPS3.7 P.84 ドメイン名使用権：日本ベリサインは、EV SSL証明書を発行した時点において、EV SSL証明書に記載されているサブジェクトが、EV SSL証明書に記載のドメイン名の排他的使用権を有することを審査するために必要と合理的に認められる手段をすべて講じたこと 変更後記載：CPS3.8 P.84 ドメイン名使用権：日本ベリサインは、EV 証明書を発行した時点において、EV 証明書に記載されているサブジェクトが、EV 証明書に記載のあらゆるドメイン名の排他的使用権を有することを審査するために必要と合理的に認められる手段をすべて講じたこと
38	Appendix B1 Section 4（c）	変更前記載：CPS3.7 P.85 日本ベリサインは、現行バージョンの Best's Insurance Guide に記載されているPolicy Holder's Ratingにおいて格付けがA以上の会社と以下の保険契約を締結する。 o 補償限度額 200 万ドル以上の企業総合賠償責任保険及び o (i)EV 証明書発行または保守時の履行、過失、怠慢、悪意のない契約違反、不履行に起因する損害賠償の請求、及び、(ii)任意の第三者の所有権侵害(著作権及び商標の侵害を除く)、プライバシー侵害ならびに広告上の損害

		に起因する損害賠償請求に対する補償を含む、補償限度額 500 万ドル以上の専門職責任保険/エラーズ&オミッションズ保険 変更後記載：CPS3.8 P.85 日本ベリサインは、ガイドラインに基づくかかる当事者の履行および義務に起因して生じる賠償責任を自家保険とする。
39	Appendix B1 Section 6	変更前記載：CPS3.7 P.87 EV SSL証明書のサブジェクトのアイデンティティに関連するEV SSL証明書内容の最小限の要件を規定する。 変更後記載：CPS3.8 P.87 EV 証明書のサブジェクトのアイデンティティに関連するEV 証明書内容の最小限の要件を規定する。サブジェクトフィールドの中のオプションのサブフィールドには認証局によって確認された情報をが含めているか、空白にする必要がある。入力フィールドに適用できないコンマ、ハイフン、スペース、及びその他の記号などは使用してはならない。
40	Appendix B1 Section 6 (a)	変更前記載：CPS3.7 P.87 日本ベリサインは、組織名の先頭または末尾の法人格を略称にすることができる。例： Official Record で、"*会社名* Incorporated"となっている場合、"*会社名*, inc."とすることができる。 変更後記載：CPS3.8 P.87 ベリサインは、組織名の先頭または末尾の法人格を略称にすることができる。例：QGISで、"*会社名* Incorporated"となっている場合、"*会社名*, inc."とすることができる。
41	Appendix B1 Section 8 (b)	変更前記載：CPS3.7 P.89 1年

		変更後記載：CPS3.8 P.89 13ヶ月
42	Appendix B2 Section 1～3	変更前記載：CPS3.7 P.108 ECC 224, 233, 256 or 283 bits 変更後記載：CPS3.8 P.108 ECC 256 or 384 bits
43	Appendix B3 Section 3	変更後記載：CPS3.8 P.110 (f) extKeyUsage 、 (g) SubjectAltName の記載を追加