日本ベリサイン CPS3.7 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	1.3.1 認証機関	変更前記載：CPS3.4 P.11 認証機関という用語は、VTN内で公開鍵証明書を発行する全ての組織に適用される包括的な用語である。認証機関は、第一次認証機関と呼ばれるカテゴリの発行者を包含する。第一次認証機関は、4つのドメインのルートとなり、 変更後記載：CPS3.7 P.12 に脚注 1 を追加 認証機関という用語は、VTN内で公開鍵証明書を発行する全ての組織に適用される包括的な用語である。認証機関は、第一次認証機関と呼ばれるカテゴリの発行者を包含する。第一次認証機関は、4つのドメインのルート 1 となり、 （脚注） 1　VTN では現在 Class 4 証明書の発行は行われていない。
2	1.3.1 認証機関	変更前記載：CPS3.4 P.12 日本ベリサインのエンタープライズ・カスタマは、米国ベリサインの第一次認証機関の下位に属する認証機関として、自らの認証機関を運営することができる。 変更後記載：CPS3.7 P.12 に下記フレーズ（下線部分）を追加 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。 日本ベリサインのエンタープライズ・カスタマは、米国ベリサインの第一次認証機関の下位に属する認証機関として、自らの認証機関を運営することができる。
3	4.1.2.1 エンドユー	変更前記載：CPS3.4 P.25 o 日本ベリサインに提示された公開鍵に対する秘密鍵を所有が証明できるこ

	ザ証明書の利用者	と 変更後記載：CPS3.7 P.26 に下記フレーズ（下線部分）を追加 o 日本ベリサインに提示された公開鍵に対する秘密鍵の所有および排他制御が証明できること
4	6.2.5 秘密鍵の保管	変更前記載：CPS3.4 P.50 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暗号化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 中の期間に関する定めが改定されない限り、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。 変更後記載：CPS3.7 このパラグラフは削除されました。
5	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：CPS3.4 P.53 本 CPS の発効日以降に発行された証明書に関する日本ベリサイン証明書の最長の有効期間は Table 8 に定めるとおりである。存在している利用者証明書から更新された利用者証明書は、より長い期間を持つ場合がある(上限は3ヶ月である。)。 変更後記載：CPS3.7 P.54 に下記脚注（下線部分）を追加 本 CPS の発効日以降に発行された証明書に関する日本ベリサイン証明書の最長の有効期間は Table 8# に定めるとおりである。存在している利用者証明書から更新された利用者証明書は、より長い期間を持つ場合がある(上限は3ヶ月である。)。 （脚注） # SHA 2 または ECC アルゴリズムや 2048 ビット以上の長さのキーが使用されるなど、より強力な暗号化アルゴリズムやキー長が使用されている証明書の場合、証明書の有効期間は、セクション 6.3.2 に定められている制限を超え

		て拡張できる。
6	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：CPS3.4 P.54 本セクションに別段の記載がある場合を除き、日本ベリサイン・サブドメインの参加者は、キー・ペアにつきその使用期間が終了した後は、いかなる使用をも止めなければならない。 変更後記載：CPS3.7 P.55 に下記フレーズ（下線部分）を追加 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。当該例外措置は、13 年間の有効期間を超えて認証機関の有効期間を延長するために適用してはならない。また、2011 年 4 月 30 日以降は使用できないものとする。本セクションに別段の記載がある場合を除き、日本ベリサイン・サブドメインの参加者は、キー・ペアにつきその使用期間が終了した後は、いかなる使用をも止めなければならない。
7	7.1 証明書のプロファイル	変更前記載：CPS3.4 P.58 (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 (“RFC 3280”) に準拠する。 変更後記載：CPS3.7 P.59 に下記フレーズ（下線部分）を修正 (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008 (“RFC 5280”) にほぼ準拠する。
8	7.1 証明書のプロファイル	変更前記載：CPS3.4 P.58/Table9 Valid From: Universal Coordinate Time を基準とする。RFC3280 に従いエンコードされる。 Valid To Universal Coordinate Time を基準とする。RFC3280 に従いエンコードされる。 変更後記載：CPS3.7 P.59 に下記フレーズ（下線部分）を修正

		Valid From: Universal Coordinate Time を基準とする。RFC 5280 に従いエンコードされる。 Valid To: Universal Coordinate Time を基準とする。RFC 5280 に従いエンコードされる。
9	7.1.2.1 Key Usage	変更前記載:CPS3.4 P.59 nonRepudiation ビットが KeyUsage エクステンションにセットされていない場合であっても、日本ベリサインは、これらの証明書について否認防止サービスをサポートする。PKI 一般において、nonRepudiation ビットの意味するところにおいてコンセンサスがとれておらず、nonRepudiation ビットがこれらの証明書中にセットされることは必須ではない。 そのようなコンセンサスが得られるまで、nonRepudiation ビットは潜在的な依拠当事者に対して意味のあるものにはならない。さらに、ほとんどの一般的アプリケーションは、nonRepudiation ビットを理解しない。それゆえ、 当該ビットをセットすることは、依拠当事者に対する信頼の決定の助けとならない。結果として、 本 CPS は、nonRepudiation ビットをクリアと設定されることを要求する。しかし、キーマネージメントを使用したデュアルキー・ペアの署名のための証明書の場合には、セットに設定されてもよい。 変更後記載:CPS3.7 P.60 に下記(下線部分)を修正 nonRepudiation ビットが KeyUsage エクステンションにセットされていない場合であっても、日本ベリサインは、これらの証明書について否認防止サービスをサポートする。PKI 一般において、nonRepudiation ビットの意味するところにおいてコンセンサスがとれておらず、nonRepudiation ビットがこれらの証明書中にセットされることは必須ではない。 そのようなコンセンサスが得られるまで、nonRepudiation ビットは潜在的な依拠当事者に対して意味のあるものにはならない。さらに、ほとんどの一般的アプリケーションは、nonRepudiation ビットを適切に扱っていない。それゆえ、 当該ビットをセットすることは、依拠当事者に対する信頼の決定の助けとならない可能性がある。そのため、nonRepudiation ビットの設定は、本 CPS では必ずしも要求されない。しかし、マネージド PKI キーマネージャーより発行されたデュアルキー・ペアの署名証明書の場合や、要求される場合には、当該ビットが設定されていてもよい。 デジタル証明書の使用に起因する非否認に関連する争議については、利用者と依拠当事者間のみの問題であり、日本ベリサインは当該争議に関する一切の責任を負わないものとする。

<table>
<tr><td></td><td></td><td>X.509標準仕様に従って、nonRepudiationビットはデジタル証明書では ContentCommitmentとして参照される場合がある。</td></tr>
<tr><td>10</td><td>7.1.3 アルゴリズムオブジェクト識別子</td><td>変更前記載：CPS3.4
P.61
日本ベリサインの証明書は、以下のアルゴリズムのうち一つを用いて署名される。
・ sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

変更後記載：CPS3.7
P.62 に下記アルゴリズム（下線部分）を追加
日本ベリサインの証明書は、以下のアルゴリズムのうち一つを用いて署名される。
・ sha256withRSAEncryption OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
・ ecdsa-with-Sha384 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}
・ sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}</td></tr>
<tr><td>11</td><td>Appendix A. 略語・定義表</td><td>変更前記載：CPS3.4
P.77
「国/主権国家/国際機関/親会社」についての定義はなし。
「子会社：EV の定義する子会社とは、QIIS の参照、CPA に登録されている財務上の声明(その他 UAS 以外の同等のもの)からほとんど支配されていると認識される企業。」

変更後記載：CPS3.7
P.79 に下記用語を追加＆修正
<table><tr><th>Term</th><th>Definition</th></tr><tr><td>Country
国</td><td>国とは本ガイドランでは、独立国であると定義する。</td></tr><tr><td>International Organization:
国際機関</td><td>国際組織とは制定文書により設立された組織。制定文書とは2つ以上の独立国政府またはその代行者によって署名されている憲章、条約、協定または同</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td></td><td><table>
<tr><td></td><td>等の文書である。</td></tr>
<tr><td>Parent Company
親会社</td><td>子会社の過半数を所有する会社であって、QIIS または登録されている Chartered Professional Accountant(CPA)か米国外では同様の組織によって提供された財務報告によって確認されたもの。</td></tr>
<tr><td>Sovereign State
独立国</td><td>独立国は州または国であり、独自の政府によって統治されていて、他の権力による従属、属国状態でないもの。</td></tr>
<tr><td>Subsidiary Company
子会社</td><td>子会社とは、申請者が全てを所有する会社であって、QIIS が登録されている Chartered Professional Accountant(CPA)か米国外では同様の組織によって提供された財務報告書によって確認されたもの。</td></tr>
</table></td></tr>
<tr><td>12</td><td>Appendix B1 Section 5 EV SSL 証明書の取得</td><td>変更前記載：CPS3.4
P.86
「(d) 非営利団体」に関する記載はなし。

変更後記載：CPS3.7
P87 に下記フレーズ（下線部分）を追加
(d) 非営利団体
ベリサインは、(a)、(b)および(c)を満たさない非営利団体に対して、以下の要求事項を満たせば EV SSL 証明書を発行することができる。
(1) 国際的な組織体
(A)申請者は国際的な組織体で、2 カ国以上またはその代行者によって署名されている国際憲章、国際協定または同等の協定書によって成立していること。
(B) 国際的な組織体は、その本部が日本ベリサインの管轄地の法律によって取引または証明書の発行を禁じられているいかなる国にもあってはならない。
(C) 国際的な組織体は日本ベリサインの管轄地の法律に基づく行政機関の拒否リストまたは禁止リスト(輸出禁止など)に記載されていてはならない。
適格な国際的な組織体の下部組織または部局は本ガイドラインに従って発行される EV 証明書に適格となる。</td></tr>
<tr><td>13</td><td>Appendix B1 Section 6(a)– (3)事業種別</td><td>変更前記載：CPS3.4
P.87<table>
<tr><th>Subject Type</th><th>Business Category string</th></tr>
<tr><td>Private Organization</td><td>V1.0, Clause 5.(b)</td></tr>
<tr><td>Government Entity</td><td>V1.0, Clause 5.(c)</td></tr>
</table></td></tr>
</table>

		<table><tr><td>Business Entity</td><td>V1.0, Clause 5.(d)</td></tr></table> 変更後記載：CPS3.7 P.88 に下記フレーズを追加＆修正 <table><tr><th>事業種別</th><th>事業種別として記載される値</th></tr><tr><td>民間組織</td><td>V1.0, Clause 5.(b)</td></tr><tr><td>行政機関</td><td>V1.0, Clause 5.(c)</td></tr><tr><td>事業体</td><td>V1.0, Clause 5.(d)</td></tr><tr><td>非営利団体</td><td>V1.0, Clause 5.(e)</td></tr></table> **Table 1. Business category field content**
14	Appendix B1 Section 14	変更前記載：CPS3.4 P.91 14. 申請者の法的存在及び本人であることの検証 EV SSL 証明書発行前に申請者の法的存在、同一性の確認のため、日本ベリサインは、発行されてから 3 ヶ月以内の登記簿謄本の原本(履歴事項全部証明書)により確認を行う。(活動中、有効、現在もしくは同等) 日本ベリサインは、申請団体の登記簿謄本に記録された申請者の正式な法的名称と EV SSL 証明書要求内の申請者の名前が一致していることを検証する。 日本ベリサインは、申請団体の登記簿謄本に記載されている会社法人等番号の確認を行う。日本ベリサインは、 登記簿謄本の発行者の住所を確認する。 日本ベリサインが実施する事業者組織の法的存在確認と識別は、申請書中で申請者が申請した組織が事業で用いている名称を確認する。日本ベリサインは、申請者の裁判管轄地の登録機関によって識別される申請者の正式な法的名称が EV SSL 証明書中の申請社名と一致することを確認する。日本ベリサインは、申請者の登録管轄で登録機関によって申請者が割り当てられた特別な一意の登録番号を記録され、登録申請日もまた、記録される。またその他に、事業者組織の代表者は、本 EV ガイドライン Section 14(b)(4)に従い認証される。 変更後記載：CPS3.7 P.92 に下記フレーズを修正 14. 申請者の法的存在及びアイデンティティ（本人であること）の検証 (1) 民間組織

		日本ベリサインは、申請者の法的存在及びアデンティティを審査するため、申請団体が法的に存在を認められた法人であり、申請団体の法人設立/登録管轄地の法人設立/登録機関によって形成（法人化など）されており、法人設立/登録機関の記録で「休眠(inactive)」、「無効(invalid)」、「不在(not current)」、またはこれからに相当する指定を受けていないことを審査する。 日本ベリサインは、申請団体の法人設立/登録管轄地の法人設立/登録機関に記録された申請団体の正式な法的名称と EV SSL 証明書要求内の申請団体の名前が一致していることを審査する。 日本ベリサインは、申請者の法人設立/登録管轄地の法人設立/登録機関が申請者に割り当てた登録番号を取得する。 日本ベリサインはさらに、申請者の法人設立/登録管轄地における申請者の Registered Agent または Registered Office(該当する場合)のアイデンティティ及び住所を取得する。 (2) 行政機関 日本ベリサインは、申請者が法的に行政機関であることを審査する。行政機関の運営の政治上の下部組織として存在。 a. 名称:申請者の法的正式名称が EV SSL 証明書申請の申請者名称と一致していることを審査する。 b. 登録番号: 日本ベリサインは申請者の設立、登録または立法上で行政機関が作られ確認された日を確認すべきである。これらの情報が得られない場合は、サブジェクトが行政機関であることを示す適切な言語を入力しなければならない。 (3) 事業体 a. 法的存在: 申請者が申請に含まれる名称で事業を行っているか審査する。 b. 組織名: 申請者の法的正式名称が EV SSL 証明書申請の申請者名と一致し、申請者の登録管轄地で登録機関によって認識されていることを審査する。 c. 登録番号: 申請者の登録管轄地の登録機関によって割り当てられた特定の固有の登録番 号を確認する。登録機関が登録番号を割り当てない場合は、申請者の登録日を確認する。 d. 代表者: 代表者の存在を審査する。 (4) 非営利団体(国際組織体) a. 法的存在: 申請者が法的に存在を認められた国際組織体か審査する。 b. 組織名: 申請者の法的正式名称が EV SSL 証明書申請の申請者名と一致

		していることを審査する。 c. 登録番号: 日本ベリサインは申請者の設立、登録または立法上で国際組織体が作られ確認された日を確認すべきである。これらの情報が得られない場合は、サブジェクトが国際組織体であることを示す適切な言語を入力しなければならない。
15	Appendix B1 Section 16 (a)	変更前記載：CPS3.4 P.92 日本ベリサインは、申請団体の物理的存在及び事業の存在を検証するために、申請団体が提示した住所が（郵便受けや郵便箱ではなく)申請団体が事業を行っている場所及び申請団体の事業所の住所であることを検証しなければならない。 行政機関の申請者においては、GGIS の記録にある申請者の管轄における住所が、識別される住所とされる。 その他の組織の場合、意見書が用意できない場合、日本ベリサインは、下記のような独自の方法で住所を確認する。 変更後記載：CPS3.7 P.93 に下記フレーズ（下線部分）を修正 日本ベリサインは、申請者の物理的存在及び事業の存在を検証するために、申請団体が提示した住所が(郵便受けや郵便箱ではなく)申請団体が事業を行っている場所及び申請団体の事業所<u>または親会社もしくは子会社</u>の住所であることを検証しなければならない。 行政機関の申請者においては、QGIS の記録にある申請者の管轄における住所が、識別される住所とされる。 <u>日本ベリサインは、下記のような独自の方法で住所を確認する。</u>
16	Appendix B1 Section 16 (b)	変更前記載：CPS3.4 P.92 日本ベリサインは、電話番号の記載された検証された弁護士意見書、検証された会計士の見解の証明書を要求する。 検証された弁護士意見書が用意できない場合、日本ベリサインは、申請団体の電話番号を以下の方法で検証する。

		変更後記載：CPS3.7 P.94 に下記フレーズを修正 日本ベリサインは、申請者の電話番号を以下の方法で検証する。
17	Appendix B1 Section 19	変更前記載：CPS3.4 P.94 弁護士意見書がない場合、日本ベリサインは、証明書承認者の権限と契約署名者雇用について以下の確認をする。 : : 弁護士意見書または、認証された会計士意見書がない場合には、日本ベリサインは、以下に示す方法の一つを用い契約署名者の権威を確認する。 変更後記載：CPS3.7 P.96 に下記フレーズを修正 日本ベリサインは、証明書承認者の権限と契約署名者雇用について以下の確認をする。 : : 日本ベリサインは、以下に示す方法の一つを用い契約署名者の権威を確認する。
18	Appendix B1 Section 16 (a) 申請者の事業所の住所	変更前記載：CPS3.4 P.95 「(5) 事前同等権限:」に関する記載はなし。 変更後記載：CPS3.7 P.97 に下記フレーズを追加 (5) 事前同等権限: 契約書署名者の署名権限及び証明書承認者の EV 権限(あるいは、契約書署名者の署名権限または証明書承認者の EV 権限)は、事前同等権限の証明に依拠して検証できる。 契約書署名者が、ベリサインまたはベリサインの親会社/子会社(あるいはその両方)と申請者の間で締結された法的に有効で強制力のある印鑑または手書きの署名がなされた拘束力を持つ契約を履行した場合で、なおかつ同契約が EV SSL 証明書の申請の 90 日前までに履行された場合に限り、契約書署名者の署名権限の確認または検証については、契約書署名者の事前同等権限に依拠できる。

		ベリサインは、事前の契約を正しく特定し、EV 申請に関連付けできるよう、事前の契約について詳細を記録しなければならない。 当該の詳細には、以下の項目が含まれる。 1.契約の表題と契約書署名者の署名の日付 2. 契約の参照番号 3. ファイルの保管場所 証明書承認者が以下のいずれかに該当する場合には、証明書承認者の EV 権限の確認または検証については、証明書承認者の事前同等権限に依拠できる。 (1) ベリサインまたは親会社/子会社と締結した契約において、申請者の企業登録機関の役割を果たした (または現在も果たしている)。 (2) 申請者が管理する公開サーバで現在使用されている、当該認証機関が発行した 1 つ以上の SSL 証明書の承認に参加した。 この場合、ベリサインまたは親会社もしくは子会社(またはその両方)は、あらかじめ承認された電話番号に電話で証明書承認者に事前に連絡するか、証明書要求を承認する旨の署名済みかつ認証済みの書簡を事前に受理していなければならない。
19	Appendix B4	変更前記載:CPS3.4 P.109 で下記事項を説明 「Assumed English Name」 「Roman Organization Name」 変更後記載:CPS3.7 P.111 で下記事項を説明 1. ラテン名ではない組織名称 2. ローマ字名称 3. 英語名称 国ごとの方法