日本ベリサイン CPS3.8.7 における変更点は、以下となります。

番号	対象セクション	変更内容
1	全体	変更前記載：CPS3.8 ベリサイン・トラスト・ネットワーク（VTN） 変更後記載：CPS3.8.7 シマンテック・トラスト・ネットワーク(STN)
2	全体	変更前記載：CPS3.8 SSL 証明書 変更後記載：CPS3.8.7 SSL サーバ証明書
3	全体	変更前記載：CPS3.8 DN 変更後記載：CPS3.8.7 識別名
4	全体	認証機関名を英語表記に変更
5	全体	誤記、表記ゆれを修正
6	1.3.1 認証機関	変更前記載：CPS3.8 P12 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。 変更後記載：CPS3.8.7 P12 また、米国シマンテックは「 Symantec Universal Root Certification Authority 」及び「Symantec Class 3 Public Primary Certification Authority – G4」を管理する。「 Symantec Universal Root Certification Authority 」は、Class 3 および特定の Class 2 の下位認証機関証明書を発行する。

番号	対象セクション	変更内容
7	1.4.2 禁止される証明書の用途	変更前記載：CPS3.8 P15 米国シマンテックと日本ベリサインは定期的に中間認証機関をリキーする。中間認証機関をルート証明書として組み込んでいるサードパーティのアプリケーションまたはプラットフォームは、中間認証機関がリキーされた後は指定されたとおり動作しない可能性がある。従って、日本ベリサインは、中間認証機関をルート証明書として利用することを保証せず、これをアプリケーションまたはプラットフォームのルート証明書として組み込まないことを推奨する。 変更後記載：CPS3.8.7 P15 米国シマンテックと日本ベリサインは定期的に中間認証機関証明書のキー・ペアを変更する。中間認証機関証明書をルート証明書として組み込んでいるサードパーティのアプリケーションまたはプラットフォームは、中間認証機関証明書のキー・ペアが変更された後では指定されたとおり動作しない可能性がある。従って、日本ベリサインは、中間認証機関証明書をルート証明書として利用することを保証せず、これをアプリケーションまたはプラットフォームのルート証明書として組み込まないことを推奨する。
8	2.2 証明書情報の公表	記載追加：CPS3.8.7 P18、Table3 Class 3 SSL サーバ証明書およびコード・サイニング証明書; 日本ベリサインのリポジトリにある証明書ステータス確認のリンク先で検索が可能
9	2.2 証明書情報の公表	変更前記載：CPS3.8 P18、Table3 利用者証明書; 変更後記載：CPS3.8.7 P18、Table3 Class 3 SSL サーバ証明書およびコード・サイニング証明書を除く利用者証明書

番号	対象セクション	変更内容
10	3.1.1 識別名の種類	変更前記載：CPS3.8 P19 冒頭の「米国シマンテックによる買収に関する告知」の通り、VTN は米国シマンテックの所有となっているが、ブランド名移行が完了するまでの間、“VeriSign, Inc.”、“VeriSign Trust Network”と記載された各種証明書の発行を継続する。 変更後記載：CPS3.8.7 P19 現在、STN は米国シマンテックの所有となっているが、以前発行された証明書には買収前の社名およびブランド名が記載されている場合がある。該当する証明書にはOrganization（O）行に“VeriSign, Inc. ”、Organizational Unit（OU）に“VeriSign Trust Network”が記載されているが、これはそれぞれ「米国シマンテック」および「シマンテック・トラスト・ネットワーク」を意味する。
11	3.1.1 識別名の種類	変更前記載：CPS3.8 P20、Table5 Organizational Unit (OU) =; ・申請が日本ベリサインにより認証された証明書中に、“Authenticated by VeriSign Japan K.K.”及び“Member, VeriSign Trust Network 変更後記載：CPS3.8.7 P20、Table5 Organizational Unit (OU) =; ・日本ベリサインにより認証された証明書(SSL サーバ証明書とコード・サイニング証明書を除く)中に、“Authenticated by VeriSign Japan K.K.”及び“Member, Symantec Trust Network” ・日本ベリサインにより認証された証明書(SSL サーバ証明書とコード・サイニング証明書)中に、“Authenticated by Symantec”及び“Member, Symantec Trust Network”
12	3.1.1 識別名の種類	記載追加：CPS3.8.7 P20、Table5 Organizational Unit (OU) =; ・ “No organization affiliation”(個人向けコード・サイニング証明書)

番号	対象セクション	変更内容
13	3.1.1 識別名の種類	変更前記載：CPS3.8 P20、Table5 CommonName (CN) =; この属性は、次のものを含む。 ・OCSP レスポンダー証明書の場合、OCSP レスポンダー名 ・ウェブ・サーバ用証明書の場合、ドメイン・ネーム ・コード/オブジェクト・サイニング証明書の場合、組織名 ・個人向け証明書の場合、名前 変更後記載：CPS3.8.7 P20、Table5 CommonName (CN) =; この属性は、次のものを含む。 ・OCSP レスポンダー名(OCSP レスポンダー証明書) ・完全修飾ドメイン名(SSL サーバ証明書) ・組織名(コード/オブジェクト・サイニング証明書) ・個人の名前(個人向け証明書または個人向けコード・サイニング証明書)
14	3.1.1 識別名の種類	記載追加：CPS3.8.7 P20、Table5 E-Mail Address (E) =; Class 3 組織向けメール署名証明書の場合、電子メールアドレス
15	3.1.1 識別名の種類	記載追加：CPS3.8.7 P20、Table5 注釈 4 シマンテックまたは日本ベリサインの場合、Class 2 証明書の社内用途において O 行の値に社内用の接尾節を追加することがある。"Symentec Corporation -[xxxx] (例: Symantec Corporation - Build 5315)"のような形式の記載は法的にもシマンテックを表すものであると保証する。
16	3.1.1 識別名の種類	記載追加：CPS3.8.7 P20、Table5 注釈 5 認可された特定の条件において、日本ベリサインの内部用途のための Class 2 証明書が発行される。該当する証明書の識別名や OU として、内部用途以外での証明書の使用するうえでは信頼性に欠ける値を含む。

番号	対象セクション	変更内容
17	3.1.3　匿名またはペンネームの使用	変更前記載：CPS3.8 P20 Class1 証明書の利用者の本人確認は行われない。Class1 証明書の利用者は匿名を使用することができる。 変更後記載：CPS3.8.7 P21 Class 1 証明書の利用者の本人確認は行われない。Class 1 証明書の利用者は匿名またはペンネームを使用することができる。
18	3.2.2 組織の実在性確認	記載追加：CPS3.8.7 P22、Table6 Secure Mail ID; Class 3 組織向けメール署名用証明書の手続きはコード・サイニング証明書に順ずる。ただし、E-Mail Address (E)に含まれるメールアドレス内のドメインについては追加で所有確認を行う。
19	3.3.1　定期的なリキーに関する確認と認証	変更前記載：CPS3.8 P23 証明書のリニューアルの際、利用者の再登録情報とともに、チャレンジフレーズ（またはこれと同等なもの）が正しく提示され、申請責任者及び技術担当者情報を含む申請者情報が変更されていなければ、更新された証明書は自動的に発行される。 変更後記載：CPS3.8.7 P24 証明書のリキーの際、利用者の再登録情報とともに、チャレンジフレーズ（またはこれと同等なもの）が正しく提示され、申請責任者及び技術担当者情報を含む申請者情報が変更されていなければ、リキーされた証明書は自動的に発行される。

番号	対象セクション	変更内容
20	3.3.1　定期的なリキーに関する確認と認証	変更前記載：CPS3.8 P24 この方法によるリキーまたはリニューアル後、そしてそれ以降リキーまたはリニューアルが行われる機会に、日本ベリサインまたは登録機関は最初の証明書申請の認証要件に従い申請者の実在性の再確認を行う。 変更後記載：CPS3.8.7 P24 この方法によるリキー後、そしてそれ以降リキーが行われる際に、日本ベリサインまたは登録機関は証明書申請の認証要件に従い申請者の実在性の再確認を行う。
21	3.3.1　定期的なリキーに関する確認と認証	変更前記載：CPS3.8 P24 特に、Class 3 組織向け証明書のリキーの申請について、日本ベリサインは、証明書に含まれる組織名称、ドメイン名の再認証を行う。 変更後記載：CPS3.8.7 P24 特に、Class 3 組織向け SSL サーバ証明書の場合、日本ベリサインは、証明書に含まれる組織名称、ドメイン名の再認証を本 CPS セクション 6.3.2 に記載の間隔で行う。

番号	対象セクション	変更内容
22	3.3.1　定期的なリキーに関する確認と認証	変更前記載：CPS3.8 P24 以下の要件を満たす場合、日本ベリサインは、証明書の申請に際し、組織が申請を許可し、申請者に組織を代表して証明書の申請の権限があることについて、電話、郵便またはこれらに相当する方法による再確認は行わない。 ・チャレンジフレーズがリニューアルされる証明書に対して正しく使用されていること ・証明書の DN が変更されていないこと ・申請責任者及び技術担当者の情報が前回確認したものから変更されていないこと 証明書の有効期間満了から 30 日後のリキーについては再度認証を行い、証明書は自動的に発行されない。 変更後記載：CPS3.8.7 P24 要件 ・チャレンジフレーズがリキーされる証明書に対して正しく使用されているか、または、申請責任者から電子メールにより確認の返信を得られたこと ・証明書の識別名が変更されていないこと ・申請責任者及び技術担当者の情報が前回確認したものから変更されていないこと 日本ベリサインは、証明書のリキーの申請に際し、組織が申請を許可し、申請者に組織を代表して証明書の申請の権限があることについて、電話、郵便またはこれらに相当する方法による再確認は行わない。 証明書の有効期間満了から 30 日以降のリキーについては再度認証を行い、証明書は自動的に発行されない。

番号	対象セクション	変更内容
23	3.4 失効申請に関する確認と認証	変更前記載：CPS3.8 P24 利用者の失効申請を認証するための手続きには、以下のものを含む。 ・利用者に自己のチャレンジフレーズ（またはこれと同等なもの）を提出させ、記録されているチャレンジフレーズ（またはこれと同等なもの）と一致した場合には、自動的に証明書が失効すること。 変更後記載：CPS3.8.7 P25 利用者の失効申請を認証するための手続きには、以下のものを含む。 ・利用者に自己のチャレンジフレーズ（またはこれと同等なもの）を提出させ、記録されているチャレンジフレーズ（またはこれと同等なもの）と一致した場合には、自動的に証明書が失効すること。（注意:本オプションは全ての利用者で利用できるとは限らない）
24	3.4 失効申請に関する確認と認証	変更前記載：CPS3.8 P25 自動承認モジュールを利用するマネージド PKI カスタマは、日本ベリサインに失効申請を一括して提出することができる。当該申請は、マネージド PKI カスタマの自動承認用ハードウェア・トークン内の秘密鍵でデジタル署名された申請によって認証される。 変更後記載：CPS3.8.7 P25 自動承認モジュールを利用するマネージド PKI カスタマは、日本ベリサインに失効申請を一括して提出することができる。当該申請は、マネージド PKI カスタマの自動承認用の秘密鍵でデジタル署名された申請によって認証される。

番号	対象セクション	変更内容
25	4.6.3 証明書のリニューアル申請の手続	変更前記載：CPS3.8 P29 この方法によるリニューアル後、そしてそれ以降リニューアルが行われる機会に、日本ベリサインまたは登録機関は最初の証明書申請の認証要件に従い申請者の実在性の再確認を行う。 特に、Class 3 組織向け証明書のリニューアルの申請について、日本ベリサインは、証明書に含まれる組織名称、ドメイン名の再認証を行う。 変更後記載：CPS3.8.7 P29 この方法によるリニューアル後、そしてそれ以降リニューアルが行われる際に、日本ベリサインまたは登録機関は本 CPS に記載される証明書申請の認証要件に従い申請者の実在性の再確認を行う。 特に、Class 3 組織向け SSL サーバ証明書の場合、日本ベリサインは、証明書に含まれる組織名称、ドメイン名の再認証を本 CPS セクション 6.3.2 に記載の間隔で行う。
26	4.6.3 証明書のリニューアル申請の手続	変更前記載：CPS3.8 P29 以下の要件を満たす場合、日本ベリサインは、証明書の申請に際し、組織が申請を許可し、申請者に組織を代表して証明書の申請の権限があることについて、電話、郵便またはこれらに相当する方法による再確認は行わない。 ・チャレンジフレーズがリニューアルされる証明書に対して正しく使用されていること ・証明書の識別名が変更されていないこと ・申請責任者及び技術担当者の情報が前回確認したものから変更されていないこと 変更後記載：CPS3.8.7 P29 要件 ・チャレンジフレーズがリニューアルされる証明書に対して正しく使用されているか、または、申請責任者から電子メールにより確認の返信を得られたこと ・証明書の識別名が変更されていないこと ・申請責任者及び技術担当者の情報が前回確認したものから変更されていないこと 日本ベリサインは、証明書のリニューアルの申請に際し、組織が申請を許可し、申請者に組織を代表して証明書の申請の権限があることについて、電話、郵便またはこれらに相当する方法による再確認は行わない。

番号	対象セクション	変更内容
27	4.9.1　失効が行われる場合	記載追加：CPS3.8.7 P32 ・本 CPS セクション 6.3.2 に定める間隔で利用者の実在性がセクション 6.3.2 に従い再確認できなかった場合 ・利用者が期限までに利用料を支払わなかった場合
28	4.9.2　証明書の失効を申請することができる者	変更前記載：CPS3.8 P33 個人の利用者は、自己の証明書につき失効を申請することができる。 変更後記載：CPS3.8.7 P33 個人の利用者は、自己の証明書につき失効を日本ベリサインまたは登録機関を通じて申請することができる。
29	4.9.9 利用可能なオンラインによる失効/ステータス調査	変更前記載：CPS3.8 P34 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。 変更後記載：CPS3.8.7 P34 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、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。
30	4.9.9 利用可能なオンラインによる失効/ステータス調査	変更前記載：CPS3.8 P34 証明書ステータス情報は、次の日本ベリサインのリポジトリにアクセスすることにより LDAP ベースのクエリー機能を通じて利用することができる。 変更後記載：CPS3.8.7 P34 個人向け証明書ステータス情報は、次の日本ベリサインのリポジトリにアクセスすることにより LDAP ベースのクエリー機能を通じて利用することができる。 ・directory.verisign.co.jp SSL サーバ証明書およびコード・サイニング証明書のステータス情報は、日本ベリサインのリポジトリにある証明書ステータス確認のリンク先のクエリー機能を通じて利用することができる

番号	対象セクション	変更内容
31	4.12.1 鍵の預託と復旧及び実施	変更前記載：CPS3.8 P36 キーマネージメントサービスを利用するエンタープライズ・カスタマには以下の事項を実施することが推奨される。 ・利用者に対する当該利用者の秘密鍵が預託されたことの通知 ・利用者の預託された秘密鍵の不正な開示からの保護 ・利用者の預託された鍵の復旧に使用される管理者自身の鍵を含む全情報の保護 ・適切に認証され承認された要求に対してのみ預託された鍵を引き渡すこと ・暗号化された鍵を復旧する前に利用者キー・ペアを失効させること 変更後記載：CPS3.8.7 P36 キーマネージメントサービスを利用するエンタープライズ・カスタマには以下の事項を実施することが推奨される。 ・利用者に対する当該利用者の秘密鍵が預託されたことの通知 ・利用者の預託された秘密鍵の不正な開示からの保護 ・利用者の預託された秘密鍵の復旧に使用される管理者自身の鍵を含む全情報の保護 ・適切に認証され承認された要求に対してのみ預託された秘密鍵を引き渡すこと ・利用者自身が管理する秘密鍵の紛失により証明書の利用を終了する事象が発生した場合に、暗号化され預託された秘密鍵を復旧する前に利用者キー・ペアを失効させること
32	5.1.2 物理的アクセス	変更前記載：CPS3.8 P38 付加的な階層では、生体認証を含む二要素認証を必須とする。信頼される者とされていない従業員または訪問者等は、付き添いなしにこれらの保護された階層へ入室することができない。 変更後記載：CPS3.8.7 P38 付加的な階層では、生体認証を含む二要素認証を必須とする。従業員及び訪問者によるこれらの保護された階層へ入室においては、信頼された者の立会いを必須とする。

番号	対象セクション	変更内容
33	5.1.2 物理的アクセス	変更前記載：CPS3.8 P38 CSU 変更後記載：CPS3.8.7 P38 ハードウェア暗号モジュール
34	5.3.2 経歴調査手続き	変更前記載：CPS3.8 P41 経歴調査、及びこれにより収集された情報の取扱は、地域の法律に従う。 変更後記載：CPS3.8.7 P41 経歴調査、及びこれにより収集された情報の取扱は、日本の法律に従う。
35	5.4.2 記録を処理する頻度	変更前記載：CPS3.8 P43 重要なセキュリティ及び運用イベントが発生した場合、監査記録は、少なくとも1週間に一度の頻度で検査される。 変更後記載：CPS3.8.7 P43 重要なセキュリティ及び運用イベントが発生した場合にアラートを検知できるよう、認証機関システム及び監査記録は、常時監視される。
36	5.7.4.1 米国シマンテック	全面的に記載を変更
37	6.1.1 キー・ペア生成	変更前記載：CPS3.8 P49 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。日本ベリサインは、自動承認サーバによるキー・ペア生成が FIPS140-1 レベル 2 に認定された暗号モジュールを用いて実行されることを推奨している。 変更後記載：CPS3.8.7 P49 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。

番号	対象セクション	変更内容
38	6.1.5 鍵のサイズ	変更前記載：CPS3.8 P50 キー・ペアの予想される使用期間においては、キー・ペアは、暗号解読技術によってキー・ペアの秘密鍵が解かれないように十分な長さが使用されるべきである。 変更後記載：CPS3.8.7 P50 キー・ペアの予想される使用期間においては、暗号解読技術によってキー・ペアの秘密鍵が解かれないように十分な長さのキー・ペアが使用されるべきである。米国シマンテック標準における一次認証局と認証局の最小の鍵のサイズは 2048 ビットの RSA と同等の強度を持つキー・ペアを使用する。
39	6.1.5 鍵のサイズ	変更前記載：CPS3.8 P50 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。 変更後記載：CPS3.8.7 P50 米国シマンテックの第三及び第五世代(G3 及び G5)の第一次認証機関は、2048 ビット 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 2048 ビットの RSA キー・ペアを生成する。

番号	対象セクション	変更内容
40	6.1.5 鍵のサイズ	記載追加：CPS3.8.7 P50 注釈 6 旧式のプラットフォームを使用するカスタマをサポートするため、認証機関の信頼性は 1024 ビットの RSA キー･ペアからなる米国シマンテックの第一世代(G1)及び第二世代(G2)の第一次認証機関をアンカーとするものまで保証される。1024 ビットの RSA キー･ペアからなる利用者証明書の発行については、2011 年 12 月 31 日を以て有効期間満了となる条件において許可される。また、米国シマンテックの承認のもと、旧式アプリケーションを基盤とする事業継続維持のため、本 CPS セクション 6.3.2 に記載のプロセッシング・センタを運用するアフィリエートに対しても例外として許可される。
41	6.1.5 鍵のサイズ	記載追加：CPS3.8.7 P50 STN EV 証明書の鍵のサイズは、Appendix B2 に記載される。
42	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：CPS3.8 P55、Table6 認証機関(オンライン)から利用者(個人); 通常 2 年まで、ただし以下の(#2)の場合には 5 年まで 変更後記載：CPS3.8.7 P55、Table6 認証機関(オンライン)から利用者(個人); 通常 3 年まで、ただし以下の(#2)の場合には 5 年まで。この場合、リニューアルやリキーは選択できない。5 年後は新規申請が必要である。
43	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：CPS3.8 P55、Table6 認証機関(オンライン)から利用者(組織); 通常 5 年まで(#3) (#4) 変更後記載：CPS3.8.7 P55、Table6 認証機関(オンライン)から利用者(組織); 通常 5 年まで(#3)とし、 (#4)の場合を除き、リニューアルやリキーは選択できない。5 年後は新規申請が必要である。

番号	対象セクション	変更内容
44	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：CPS3.8 P55 (#1) VeriSign Onsite Administrator CA-Class 3 は、過去のシステムとの関係から 10 年を超える有効期間を持つが、適切な時期に失効される。 変更後記載：CPS3.8.7 P55 (#1) Symantec Onsite Administrator CA-Class 3、及び Class 3 OnSite Enterprise Administrator CA - G2 は、過去のシステムとの関係から 10 年を超える有効期間を持つが、適切な時期に失効される。
45	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：CPS3.8 P55 (#3)組織向けリテール証明書は、5 年を上限として発行される。 変更後記載：CPS3.8.7 P55 (#3)組織向けリテール証明書は、5 年を上限として発行される。3 年を超える有効期間をもつ利用者証明書が発行されている場合には、証明書の発行日から 3 年経過後に再度、その識別名についての本人確認がなされる。
46	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：CPS3.8 P55 (#4) 組織向け利用者証明書のうち VTN の一部機能をサポートするためだけの証明書に関しては、有効期間が5年とされ、更新作業後は最長10年とすることができる。 変更後記載：CPS3.8.7 P55 (#4)STN の機能の一部として利用される証明書に関しては、有効期間が 5 年までとされ、更新作業後は最長 10 年とすることができる。

番号	対象セクション	変更内容
47	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：CPS3.8 P55 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。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。 変更後記載：CPS3.8.7 P55 STN CP のセクション 6.3.2 について、日本ベリサインは、認証機関のキー・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機関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。当該例外措置はプロセッシング・センタを有するアフィリエートにおいて、SSL サーバ証明書の発行に関与しないインフラ用途、管理用途の認証機関にのみ適用される。また、当該例外措置は、14 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ず、その場合の有効期限は最大でも 2014 年 8 月 31 日までとし、、2011 年 12 月 31 日以降は使用できないものとする。

番号	対象セクション	変更内容
48	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：CPS3.8 P55-56 利用者に対して認証機関が発行した証明書は、次に定める要件を満たす場合に限り、2年を越えて最長5年までの有効期間を有することができる。 ・当該証明書が個人向けの証明書であること ・利用者のキー・ペアが、スマートカードのようなハードウェア・トークン上に存在すること, ・利用者はセクション 3.2.3 の規定に従い、最低 25 ヶ月ごとに再認証を受けること ・利用者はセクション 3.2.3 の規定に従い、秘密鍵と対応する公開鍵を保有していることの証明を最低 25 ヶ月ごとに行うこと ・万が一、利用者再認証手続きを完了することができず、または秘密鍵を保有していることの証明を行うことができない場合には、認証機関は当該利用者の証明書を取り消すものとされていること 変更後記載：CPS3.8.7 P56 利用者に対して認証機関が発行した証明書は、次に定める要件を満たす場合に限り、3 年を越えて最長 5 年までの有効期間を有することができる。 ・組織向け証明書の利用環境でのキー・ペアの保護については、データ・センタ内の高度な保護下で利用されること。個人向けの証明書については、利用者のキー・ペアがスマートカードのようなハードウェア・トークン上に存在すること, ・利用者は本 CPS セクション 3.2.3 の規定に従い、最低 3 年ごとに再認証を受けること ・万が一、利用者再認証手続きを完了することができず、または秘密鍵を保有していることの証明を行うことができない場合には、認証機関は当該利用者の証明書を取り消すものとされていること
49	6.5.2 コンピュータ・セキュリティの評価	変更後記載：CPS3.8.7 P58 適用せず。

番号	対象セクション	変更内容
50	7.1.2.1 Key Usage	変更前記載：CPS3.8 P59-60 X.509 バージョン 3 の証明書中の KeyUsage エクステンションは、通常、Table 10 に示すように、ビットのセット及びクリア、並びに Criticality が設定される。 変更後記載：CPS3.8.7 P59 記載削除
51	7.1.2.1 Key Usage	変更前記載：CPS3.8 P60、Table10 が存在 変更後記載：CPS3.8.7 P59 Table10 全体を削除
52	7.1.2.3 Subject Alternative Names	変更前記載：CPS3.8 P60 X.509 バージョン 3 証明書の subjectAltName エクステンションは、RFC 5280 に従い設定される。 変更後記載：CPS3.8.7 P60 X.509 バージョン 3 証明書の subjectAltName エクステンションは、RFC 5280 に従い設定される。ただし、一部の利用者証明書については、subjectAltName に電子メールアドレスが含まれないことがある。
53	7.1.2.4 Basic Constraints	変更前記載：CPS3.8 P61 エンドユーザ利用者証明書における BasicConstraints エクステンションは、Null に設定されなければならない。このエクステンションの Criticality は、認証機関証明書においては「TRUE」に、他の場合は「FALSE」に設定されなければならない。 変更後記載：CPS3.8.7 P60 エンドユーザ利用者証明書における BasicConstraints エクステンションは、CA フィールドが「FALSE」に設定されなければならない。このエクステンションの Criticality は、認証機関証明書においては「TRUE」に、利用者証明書の場合は「TRUE」または「FALSE」のいずれかに設定される。

番号	対象セクション	変更内容
54	7.1.2.5 Extended Key Usage	変更前記載：CPS3.8 P61 日本ベリサインは、Table 11 に示す特定の種類の X.509 バージョン 3 証明書について、Extended Key Usage エクステンションを使用することができる。通常、その他の種類の証明書については、日本ベリサインは Extended Key Usage エクステンションを使用しない。 変更後記載：CPS3.8.7 P60 通常、Extended Key Usage エクステンションが設定される場合、Criticality に関するフィールドは、「FALSE」に設定される。一部を除き、STN に属する認証機関証明書には Extended Key Usage は含まれない。
55	7.1.2.5 Extended Key Usage	変更前記載：CPS3.8 P61-62 Table11, Table12 が存在 変更後記載：CPS3.8.7 P60 Table11, Table12 を削除。 以降 Table 番号繰り上げ。
56	Appendix A. 略語・定義表	記載追加：CPS3.8.7 P76 TLS; Transport Layer Security
57	定義	変更前記載：CPS3.8 P79 マネージド PKI; 日本ベリサインのエンタープライズ・カスタマが VTN 内で証明書を従業員、パートナー、サプライヤー及び顧客、さらにサーバ、ルーター及びファイアウォール等のデバイスに発行することのできる日本ベリサインの完全に統合された PKI サービス。 変更後記載：CPS3.8.7 P78 日本ベリサインのエンタープライズ・カスタマが STN 内で証明書を従業員、パートナー、サプライヤー及び顧客、さらにサーバ、ルーター及びファイアウォール等のデバイスに発行することのできる日本ベリサインの完全に統合された PKI サービス。ベリサイン マネージド PKI または Symantec Managed PKI を意味する。

番号	対象セクション	変更内容
58	定義	記載追加：CPS3.8.7 P81 トランスポート・レイヤ・セキュリティ（TLS); SSLをもとに開発されたウェブ通信を保護するための業界標準方法。SSLと同じく、データの暗号化、サーバ認証、メッセージの完全性及びオプションとしてクライアント認証を提供する。
59	AppendixB 22. 特定の情報源の検証 (a) 検証済み弁護士意見書	変更前記載：CPS3.8 P98 (1) 検証の要件： 変更後記載：CPS3.8.7 P98 検証の要件：
60	AppendixB 22. 特定の情報源の検証 (a) 検証済み弁護士意見書	変更前記載：CPS3.8 P99 電子署名である意見書の場合には、書類の信憑性と署名確認の方法で日本ベリサインによりセクション 22(b)(2)(A)により確認され、信憑性に関するそれ以上の要求はされない。 変更後記載：CPS3.8.7 P99 電子署名である意見書の場合には、書類の信憑性と署名確認の方法で日本ベリサインによりセクション 22(a)(A)により確認され、信憑性に関するそれ以上の要求はされない。
61	AppendixB 22. 特定の情報源の検証 (b) 検証済み会計士意見書	変更前記載：CPS3.8 P99 (1) 検証の要件。 変更後記載：CPS3.8.7 P99 検証の要件：

番号	対象セクション	変更内容
62	AppendixB 22. 特定の情報源の検証 (b) 検証済み会計士意見書	変更前記載：CPS3.8 P99 電子署名である意見書の場合には、書類の信憑性と署名確認の方法で日本ベリサインによりセクション 22(b)(2)(A)により確認され、信憑性に関するそれ以上の要求はされない。 変更後記載：CPS3.8.7 P99 電子署名である意見書の場合には、書類の信憑性と署名確認の方法で日本ベリサインによりセクション 22(b) (A)により確認され、信憑性に関するそれ以上の要求はされない。
63	AppendixB 22. 特定の情報源の検証 (c)対面認証	変更前記載：CPS3.8 P99 この場合、宣誓書は、書類の信憑性を確認する方法と同じく、電子署名に限られ、日本ベリサインによって行われる署名の確認はセクション 22(c)(2)(A)の方法を用い、信憑性の確認に関するそれ以上の要求は行われない。 変更後記載：CPS3.8.7 P99 この場合、宣誓書は、書類の信憑性を確認する方法と同じく、電子署名に限られ、日本ベリサインによって行われる署名の確認はセクション 22(c) (A)の方法を用い、信憑性の確認に関するそれ以上の要求は行われない。
64	Appendix B2 EV 証明書の最小限の暗号アルゴリズムと鍵のサイズ	変更前記載：CPS3.8 P108 各表の「Certificate issued on or before 31 Dec 2010」の列が存在 変更後記載：CPS3.8.7 P108 記載削除
65	Appendix B2 EV 証明書の最小限の暗号アルゴリズムと鍵のサイズ	変更前記載：CPS3.8 P108 各表の「Certificate issued after 31 Dec 2 2010」 変更後記載：CPS3.8.7 P108 各表の「アルゴリズムの最低強度」