CPS改定案

<table>
<tr><th>セクション</th><th>現在の内容</th><th>改定案</th></tr>
<tr><td>1.1.2.1.2</td><td>1.1.2.1.2　VTNにおける日本ベリサインの役割
日本ベリサインは、CP§1.1.2.1.2 に記載されるサービスセンターの機能をもつ。これにより、日本ベリサインは、リテール証明書の場合、証明書申請を承認または拒絶することができ、マネージドPKI証明書の場合、プロセッシングセンターを利用しマネージドPKIカスタマに対しバックエンドの証明書ライフサイクル・サービスを提供することができる。サーバ証明書を提供するときは、日本ベリサイン・サービスセンターはVTN内でセキュア・サーバIDまたはグローバル・サーバIDを発行する米国ベリサイン認証機関の登録機関となる。日本ベリサイン・サービスセンターは、セキュア・サーバIDまたはグローバル・サーバIDの証明書申請を確認または拒絶する検証機能を果たす。
日本ベリサインは、CP§1.1.2.1.2に記載するプロセッシングセンターであり、証明書発行に利用される秘密鍵を有する暗号モジュールを含む認証機関システムを収容する安全な施設を保有する。日本ベリサインは、VTNにおいて認証機関として活動し、証明書の発行、管理、取消しおよび更新を行うライフサイクル・サービスを提供する。日本ベリサインはまた、自らの下位に位置するマネージドPKIカスタマまたはサービスセンターのマネージドPKIカスタマの代理として認証機関のキーマネージメントおよび証明書ライフサイクル・サービスを提供する。日本ベリサインは又、CP§1.1.2.1.2に記載するとおり、個人向け（クラス1および2のクライアント・リテール証明書）、ウェブ・サイト向け（セキュア・サーバIDおよびグローバル・サーバID）および企業向け（マネージドPKIサービスを提供する）の3種類の事業分野において証明書を提供する。米国ベリサインから日本ベリサイン提供されるサービスに関する実務については、本CPSの対象外である。</td><td>1.1.2.1.2　VTNにおける日本ベリサインの役割
日本ベリサインは、CP§1.1.2.1.2 に記載されるサービスセンターとプロセッシングセンターを運用する。これにより、日本ベリサインは、リテール証明書の場合、証明書申請を承認または拒絶することができ、マネージドPKI証明書の場合、プロセッシングセンターを利用しマネージドPKIカスタマに対しバックエンドの証明書ライフサイクル・サービスを提供することができる。サーバ証明書を提供するときは、日本ベリサイン・サービスセンターはVTN内でセキュア・サーバIDまたはグローバル・サーバIDを発行する米国ベリサイン認証機関の登録機関となる。日本ベリサイン・サービスセンターは、セキュア・サーバIDまたはグローバル・サーバIDの証明書申請を確認または拒絶する検証機能を果たす。
日本ベリサインは、CP§1.1.2.1.2に記載するプロセッシングセンターであり、証明書発行に利用される秘密鍵を有する暗号モジュールを含む認証機関システムを収容する安全な施設を保有する。日本ベリサインは、VTNにおいて認証機関として活動し、証明書の発行、管理、取消しおよび更新を行うライフサイクル・サービスを提供する。日本ベリサインはまた、自らの下位に位置するマネージドPKIカスタマまたはサービスセンターのマネージドPKIカスタマの代理として認証機関のキーマネージメントおよび証明書ライフサイクル・サービスを提供する。日本ベリサインは又、CP§1.1.2.1.2に記載するとおり、個人向け（クラス1および2のクライアント・リテール証明書）、ウェブ・サイト向け（セキュア・サーバIDおよびグローバル・サーバID）および企業向け（マネージドPKIサービスを提供する）の3種類の事業分野において証明書を提供する。米国ベリサインから日本ベリサイン提供されるサービスに関する実務については、本CPSの対象外である。</td></tr>
<tr><td>1.1.2.3.2</td><td>1.1.2.3.2　ベリサイン マネージドPKI キーマネージメントサービス
マネージドPKI キーマネージメントサービスは、マネージドPKIカスタマが承認する証明書申請を行う利用者の代理で、マネージドPKIカスタマが鍵ペアを生成することを可能にする。マネージドPKI キーマネージメントサービスは、当該利用者の秘密鍵を安全な方法で送信すること、当該秘密鍵の予備を安全な方法で保持すること、および必要な場合当該秘密鍵を回復することも可能にする。マネージドPKIキーマネージメントサービスは、シングル・キー・ペア・システムとデュアル・キー・システムの双方に対応している。シングル・キー・ペア・システムは、利用者が、デジタル署名と機密保持機能の両方に使用する鍵を生成する。デュアル・キー・システムは、対照的に、利用者が機密保持のために使用する鍵を生成する。一方、利用者は、自己のデジタル署名用の鍵ペアを生成する。デュアル・キー・システムにおいては、利用者はそれぞれの公開鍵用に1つの証明書、合計2つの証明書を受領する。マネージドPKIキーマネージメントは、日本ベリサインの提供するベリサイン・キー・リカバリー・サービスと一体となって機能する。マネージドPKIキーマネージメントの詳細は、CP§1.1.2.3.2に記載される。

マネージドPKI キーマネージメント・ソフトウェアは、秘密鍵の予備をマネージドPKIカスタマのサイトで暗号化された状態で保管する。各利用者の秘密鍵は、独自の秘密鍵で個別に暗号化される。キー・リカバリー・ブロック（以下「KRB」という）は、キー・リカバリー技術を用い当該秘密鍵から生成され、当該秘密鍵は消去される。利用者の暗号化された秘密鍵とKRB は、マネージドPKI カスタマシステム上のキーマネージメント・データベースで保管される。
マネージドPKI キーマネージメント・ソフトウェアは、日本ベリサインの提供するベリサイン・キー・リカバリー・サービスと一体となって機能する。秘密鍵の回復には、マネージドPKIカスタマの管理者の指示に基づき、データベースからKRBを取出し、日本ベリサインの安全なデータ・センター外で運用されるキーリカバリーサービスにオンラインで送信する、マネージドPKIキーマネージメントを必要とする。日本ベリサインのみが、KRBを取出すことおよび埋め込まれた暗号鍵を回復することのできる秘密鍵を保持する。日本ベリサインに対する秘密鍵回復の要請には、KRBの取出しを許可するために必要とされるエンタープライズ・エマージェンシー・リカバリー・コードを含めるものとする。有効なKRBが届けられ、正確なエマージェンシー・リカバリー・コードが提供された場合、キーリカバリーサービスは、マネージドPKIキーマネージメントに暗号鍵を返し、対応する利用者の秘密鍵を回復することを可能にする。</td><td>1.1.2.3.2　ベリサイン マネージドPKI キーマネージメントサービス
マネージドPKI キーマネージメントサービスは、マネージドPKIカスタマが承認する証明書申請を行う利用者の代理で、マネージドPKIカスタマが鍵ペアを生成することを可能にする。マネージドPKI キーマネージメントサービスは、当該利用者の秘密鍵を安全な方法で送信すること、当該秘密鍵の予備を安全な方法で保持すること、および必要な場合当該秘密鍵を回復することも可能にする。マネージドPKIキーマネージメントサービスは、シングル・キー・ペア・システムとデュアル・キー・システムの双方に対応している。シングル・キー・ペア・システムは、利用者が、デジタル署名と機密保持機能の両方に使用する鍵を生成する。デュアル・キー・システムは、対照的に、利用者が機密保持のために使用する鍵を生成する。一方、利用者は、自己のデジタル署名用の鍵ペアを生成する。デュアル・キー・システムにおいては、利用者はそれぞれの公開鍵用に1つの証明書、合計2つの証明書を受領する。マネージドPKIキーマネージメントは、日本ベリサインの提供するベリサイン・キー・リカバリー・サービスと一体となって機能する。マネージドPKIキーマネージメントの詳細は、CP§1.1.2.3.2に記載される。

マネージドPKI キーマネージメント・ソフトウェアは、秘密鍵の予備をマネージドPKIカスタマのサイトで暗号化された状態で保管する。各利用者の秘密鍵は、独自の暗号鍵で個別に暗号化される。キー・リカバリー・ブロック（以下「KRB」という）は、キー・リカバリー技術を用い当該暗号鍵から生成され、その後当該暗号鍵は消去される。利用者の暗号化された秘密鍵とKRB は、マネージドPKI カスタマのシステム上のキーマネージメント・データベースで保管される。
マネージドPKI キーマネージメント・ソフトウェアは、日本ベリサインの提供するベリサイン・キー・リカバリー・サービスと一体となって機能する。秘密鍵の回復には、マネージドPKIカスタマの管理者の指示に基づき、データベースからKRBを取出し、日本ベリサインの安全なデータ・センター外で運用されるキーリカバリーサービスにオンラインで送信する、マネージドPKIキーマネージメントを必要とする。日本ベリサインのみが、KRBを取出すことおよび埋め込まれた暗号鍵を回復することのできる秘密鍵を保持する。日本ベリサインに対する秘密鍵回復の要請には、KRBの取出しを許可するために必要とされるエンタープライズ・エマージェンシー・リカバリー・コードを含めるものとする。有効なKRBが届けられ、正確なエマージェンシー・リカバリー・コードが提供された場合、キーリカバリーサービスは、マネージドPKIキーマネージメントに暗号鍵を返し、対応する利用者の秘密鍵を回復することを可能にする。</td></tr>
<tr><td>3.1.1
表9</td><td>
<table>
<tr><th>属性</th><th>値</th></tr>
<tr><td>Country (C) =</td><td>JP もしくは使用せず。</td></tr>
<tr><td>Organization (O) =</td><td>この属性は、次のように使用される。
・“VeriSign Japan K.K.”（日本ベリサイン OCSP レスポンダーおよび個人向け証明書）
・利用者の組織名（ウェブ・サーバ証明書）
・コード／オブジェクト・サイニング用証明書には使用せず</td></tr>
<tr><td>Organization Unit (OU) =</td><td>日本ベリサイン利用者証明書は以下に定める一つ以上の OU 属性を含むことができる。
・利用者組織単位（組織向け証明書）
・VeriSign Trust Network
・証明書の使用条件を規定する依拠当事者規約を参照する旨の記載
・著作権に関する通知
・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.” および “Member, VeriSign Trust Network”
・“Persona Not Validated”（クラス 1 個人向け証明書）
・証明書の種類を説明する記載</td></tr>
<tr><td>State or Province (S) =</td><td>都道府県</td></tr>
<tr><td>Locality (L) =</td><td>市区町村</td></tr>
<tr><td>Common Name (CN) =</td><td>この属性は、次のものを含む。
・OCSP レスポンダー名（OCSP レスポンダー用証明書）
・ドメイン・ネーム（ウェブ・サーバ用証明書）
・組織名（コード／オブジェクト署名用証明書）
・名前（個人用証明書）</td></tr>
<tr><td>E-Mail Address (E) =</td><td>電子メールアドレス（クラス 1 個人向け証明書）</td></tr>
</table>
</td><td>
<table>
<tr><th>属性</th><th>値</th></tr>
<tr><td>Country (C) =</td><td>JP もしくは使用せず。</td></tr>
<tr><td>Organization (O) =</td><td>この属性は、次のように使用される。
・“VeriSign Japan K.K.”（日本ベリサイン OCSP レスポンダーおよび個人向け証明書）
・利用者の組織名（ウェブ・サーバ証明書）
・コード／オブジェクト・サイニング用証明書には使用せず</td></tr>
<tr><td>Organization Unit (OU) =</td><td>日本ベリサイン利用者証明書は以下に定める一つ以上の OU 属性を含むことができる。
・利用者組織単位（組織向け証明書）
・VeriSign Trust Network
・証明書の使用条件を規定する依拠当事者規約を参照する旨の記載
・著作権に関する通知
・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.” および “Member, VeriSign Trust Network”
・“Persona Not Validated”（クラス 1 個人向け証明書）
・証明書の種類を説明する記載</td></tr>
<tr><td>State or Province (S) =</td><td>都道府県もしくは使用せず。</td></tr>
<tr><td>Locality (L) =</td><td>市区町村もしくは使用せず。</td></tr>
<tr><td>Common Name (CN) =</td><td>この属性は、次のものを含む。
・OCSP レスポンダー名（OCSP レスポンダー用証明書）
・ドメイン・ネーム（ウェブ・サーバ用証明書）
・組織名（コード／オブジェクト署名用証明書）
・名前（個人用証明書）</td></tr>
<tr><td>E-Mail Address (E) =</td><td>電子メールアドレス（クラス 1 個人向け証明書）</td></tr>
</table>
</td></tr>
<tr><td>3.2.2</td><td>3.2.2　認証機関証明書の定期的なリキーとリニューアル
日本ベリサイン認証機関のリキーは、本CPS§4.7に従い定期的に行われる。

日本ベリサイン認証機関証明書は、本CPS§6.3.2に定める範囲内でリニューアルが行われる。例えば、存続期間10年の第一次認証機関証明書が最初に発行された場合、認証機関の鍵ペアの有効期間を更に20年間延長するために、リニューアルされた証明書が発行され、許容された最大限の有効期間である30年に達することになる。認証機関証明書のリニューアルは、証明書の有効期間満了後は行うことができない。

米国ベリサインの自己署名した第一次認証機関証明書、日本ベリサインのルート証明書および日本ベリサインの認証機関証明書については、リニューアルの要求は、複数の信頼された個人の参加を要求する管理された手続きを通じ、権限ある米国ベリサインの要員によって作成され、承認される。
米国ベリサイン第一次認証機関につながる非日本ベリサイン認証機関証明書については、日本ベリサインは、マネージドPKIカスタマが現実に認証機関証明書の利用者であることを検証するための適切な手続きをとるものとする。認証手続きは、本CPS§3.1.8.3に従った本来の手続きと同一とする。</td><td>3.2.2　認証機関証明書の定期的なリキーとリニューアル
日本ベリサイン認証機関のリキーは、本CPS§4.7に従い定期的に行われる。

日本ベリサイン認証機関証明書は、本CPS§6.3.2に定める範囲内でリニューアルが行われる。例えば、存続期間10年の第一次認証機関証明書が最初に発行された場合、認証機関の鍵ペアの有効期間を更に20年間延長するために、リニューアルされた証明書が発行され、許容された最大限の有効期間である30年に達することになる。認証機関証明書のリニューアルは、証明書の有効期間満了後は行うことができない。

米国ベリサインの自己署名した第一次認証機関証明書、日本ベリサインのルート証明書および日本ベリサインの認証機関証明書については、リニューアルの要求は、複数の信頼された個人の参加を要求する管理された手続きを通じ、権限ある米国ベリサインの要員によって作成され、承認される。
米国ベリサイン第一次認証機関につながる非日本ベリサイン認証機関証明書については、日本ベリサインは、マネージドPKIカスタマが現実に認証機関証明書の利用者であることを検証するための適切な手続きをとるものとする。認証手続きは、本CPS§3.1.8.2に従った本来の手続きと同一とする。</td></tr>
</table>

<table>
<tr><th>セクション</th><th>現在の内容</th><th>改定案</th></tr>
<tr><td>4.1.1
表14</td><td>
<table>
<tr><th>証明書のクラス／種類</th><th>証明書申請を処理する機関</th><th>証明書を発行する機関</th></tr>
<tr><td>クラス１　個人向けリテール証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
<tr><td>クラス１　個人向けマネージド PKI 証明書</td><td>クラス１　マネージド PKI カスタマ</td><td>日本ベリサイン</td></tr>
<tr><td>クラス２　個人向けリテール証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
<tr><td>クラス２　個人向けマネージド PKI 証明書</td><td>クラス２　マネージド PKI カスタマまたはマネージド PKI ライト・カスタマ</td><td>日本ベリサイン</td></tr>
<tr><td>クラス３　個人向けリテール証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
<tr><td>クラス３　管理者証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
<tr><td>クラス３　組織向けリテール証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
<tr><td>クラス３　組織向けマネージド PKI 証明書（マネージド PKI for SSL またはマネージド PKI for SSL(プレミアム エディション)）</td><td>マネージド PKI for SSL カスタマまたはマネージド PKI for SSL(プレミアム エディション)カスタマ</td><td>米国ベリサイン</td></tr>
<tr><td>認証機関、インフラストラクチャおよび日本ベリサイン従業員証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
</table>
</td><td>
<table>
<tr><th>証明書のクラス／種類</th><th>証明書申請を処理する機関</th><th>証明書を発行する機関</th></tr>
<tr><td>クラス１　個人向けリテール証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
<tr><td>クラス１　個人向けマネージド PKI 証明書</td><td>クラス１　マネージド PKI カスタマ</td><td>日本ベリサイン</td></tr>
<tr><td>クラス２　個人向けリテール証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
<tr><td>クラス２　個人向けマネージド PKI 証明書</td><td>クラス２　マネージド PKI カスタマまたはマネージド PKI ライト・カスタマ</td><td>日本ベリサイン</td></tr>
<tr><td>クラス３　個人向けリテール証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
<tr><td>クラス３　管理者証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
<tr><td>クラス３　組織向けリテール証明書</td><td>日本ベリサイン</td><td>米国ベリサイン</td></tr>
<tr><td>クラス３　組織向けマネージド PKI 証明書（マネージド PKI for SSL またはマネージド PKI for SSL(プレミアム エディション)）</td><td>マネージド PKI for SSL カスタマまたはマネージド PKI for SSL(プレミアム エディション)カスタマ</td><td>米国ベリサイン</td></tr>
<tr><td>認証機関、インフラストラクチャおよび日本ベリサイン従業員証明書</td><td>日本ベリサイン</td><td>日本ベリサイン</td></tr>
</table>
</td></tr>
<tr><td>4.4.9</td><td>4.4.9　証明書失効リスト（CRL）の発行頻度
日本ベリサインは、日本ベリサインの証明書の取消しを示すCRLを公表し、証明書ステータスを調査することができるサービスを提供する。利用者証明書を発行する認証機関についての証明書失効リストは、毎日公表される。認証機関証明書のみを発行する認証機関に関する証明書失効リストは、四半期毎および認証機関証明書が取消される都度公表される。有効期間が経過した証明書は、証明書失効リストから削除される。</td><td>4.4.9　証明書失効リスト（CRL）の発行頻度
日本ベリサインは、日本ベリサインの証明書の取消しを示すCRLを公表し、証明書ステータスを調査することができるサービスを提供する。利用者証明書を発行する認証機関についての証明書失効リストは、毎日公表される。認証機関証明書のみを発行する認証機関に関する証明書失効リストは、四半期毎および認証機関証明書が取消される都度公表される。有効期間が経過した証明書は、証明書失効リストから削除されることがある。</td></tr>
<tr><td>6.1.9</td><td>6.1.9　鍵用途目的
X.509バージョン3の証明書に関し、日本ベリサインは一般的に証明書の鍵用途(KeyUsage)エクステンションを、RFC2459、すなわち、1999年1月のインターネットX.509公開鍵インフラストラクチャ証明書およびCRLプロファイルに従い定めている。米国ベリサインのX.509バージョン3証明書の鍵用途エクステンションは、次の例外を除き、表16に従って定められている。
・鍵用途エクステンションはグローバル・サーバID、クラス１個人証明書およびクラス２個人向け証明書には用いられない。
・マネージドPKIキーマネージメントを通じたデュアル・キー・システムにおける署名用証明書には否認防止ビット(nonrepudiation bit)を設定することは許される。
・鍵用途エクステンションのクリティカリティーは、将来的には他の証明書に関しても真（TRUE）に設定される可能性がある。</td><td>6.1.9　鍵用途目的
X.509バージョン3の証明書に関し、日本ベリサインは一般的に証明書の鍵用途(KeyUsage)エクステンションを、RFC2459、すなわち、1999年1月のインターネットX.509公開鍵インフラストラクチャ証明書およびCRLプロファイルに従い定めている。米国ベリサインのX.509バージョン3証明書の鍵用途エクステンションは、次の例外を除き、表16に従って定められている。
・マネージドPKIキーマネージメントを通じたデュアル・キー・システムにおける署名用証明書には否認防止ビット(nonrepudiation bit)を設定することは許される。
・鍵用途エクステンションのクリティカリティーは、将来的には他の証明書に関しても真（TRUE）に設定される可能性がある。</td></tr>
<tr><td>7.1.3</td><td>7.1.3　アルゴリズム・オブジェクト識別子（Algorithm Object Identifiers）
日本ベリサインX.509 証明書は、RFC 2459 に従い、sha1RSA (OID: 1.2.840.113549.1.1.5)またはmd5RSA (OID: 1.2.840.113549.1.1.4)アルゴリズムを用い署名される。米国ベリサインは、一部の古い認証機関および利用者証明書をmd2RSA (OID: 1.2.840.113549.1.1.2)アルゴリズムを用い署名した。</td><td>7.1.3　アルゴリズム・オブジェクト識別子（Algorithm Object Identifiers）
日本ベリサインX.509 証明書は、RFC 3280 に従い、sha1RSA (OID: 1.2.840.113549.1.1.5)またはmd5RSA (OID: 1.2.840.113549.1.1.4)アルゴリズムを用い署名される。米国ベリサインは、一部の古い認証機関および利用者証明書をmd2RSA (OID: 1.2.840.113549.1.1.2)アルゴリズムを用い署名した。</td></tr>
<tr><td>7.2
表23</td><td>
<table>
<tr><th>フィールド</th><th>値</th></tr>
<tr><td>バージョン (Version)</td><td>本 CPS §7.2.1 参照。</td></tr>
<tr><td>署名アルゴリズム (Signature Algorithm)</td><td>CRL に署名するために使用されるアルゴリズム。米国ベリサイン CRL は、RFC 3280 に従い、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。</td></tr>
<tr><td>発行者 (Issuer)</td><td>CRL を署名し発行した主体。CRL 発行者名 (CRL Issuer Name)は、本 CPS §7.1.4 に規定する発行者識別名(Issuer Distinguished Name)の要件に従う。</td></tr>
<tr><td>発効日 (Effective Date)</td><td>CRL の発行日。日本ベリサイン CRL は、発行と同時に有効となる。</td></tr>
<tr><td>次回更新 (Next Update)</td><td>その日までに、次の CRL が発行される。日本ベリサイン CRL の次回更新(Next Update)の日は、次のとおり記載される。米国ベリサイン第一次認証機関については発効日(Effective Date)から 3 ヶ月、日本ベリサインの認証機関については、発効日から 10 日。CRL の発行頻度は、本 CPS §4.4.9 に従う。</td></tr>
<tr><td>失効した証明書 (Revoked Certificates)</td><td>失効した証明書のシリアル・ナンバー(Serial Number)および失効日(Revocation Date)を含む、失効した証明書の一覧。</td></tr>
</table>
</td><td>
<table>
<tr><th>フィールド</th><th>値</th></tr>
<tr><td>バージョン (Version)</td><td>本 CPS §7.2.1 参照。</td></tr>
<tr><td>署名アルゴリズム (Signature Algorithm)</td><td>CRL に署名するために使用されるアルゴリズム。米国ベリサイン CRL は、RFC 3279 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。</td></tr>
<tr><td>発行者 (Issuer)</td><td>CRL を署名し発行した主体。CRL 発行者名 (CRL Issuer Name)は、本 CPS §7.1.4 に規定する発行者識別名(Issuer Distinguished Name)の要件に従う。</td></tr>
<tr><td>発効日 (Effective Date)</td><td>CRL の発行日。日本ベリサイン CRL は、発行と同時に有効となる。</td></tr>
<tr><td>次回更新 (Next Update)</td><td>その日までに、次の CRL が発行される。日本ベリサイン CRL の次回更新(Next Update)の日は、次のとおり記載される。米国ベリサイン第一次認証機関については発効日(Effective Date)から 3 ヶ月、日本ベリサインの認証機関については、発効日から 10 日以内。CRL の発行頻度は、本 CPS §4.4.9 に従う。</td></tr>
<tr><td>失効した証明書 (Revoked Certificates)</td><td>失効した証明書のシリアル・ナンバー(Serial Number)および失効日(Revocation Date)を含む、失効した証明書の一覧。</td></tr>
</table>
</td></tr>
<tr><td>7.2.1</td><td>7.2.1　バージョン・ナンバー（Version Number(s)）
日本ベリサインは、現在X.509バージョン1CRLを発行している。</td><td>7.2.1　バージョン・ナンバー（Version Number(s)）
日本ベリサインは、X.509のCRLバージョン1およびバージョン2を発行する。</td></tr>
</table>