

日本ペリサイン CPS3.4 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	6.2.5 秘密鍵の保管	<p>変更前記載:CPS 3.3.1</p> <p>日本ペリサイン認証機関のキー・ペアについてその有効期間が満了したときは、当該キー・ペアは少なくとも5年間保管される。保管されたキー・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て確実に保管される。保管されたキー・ペアは、再使用されないように必要な管理がされている。保管期間満了に伴い、保管された認証機関のキー・ペアは、本 CPS に従い、確実に破壊される。</p> <p>変更後記載:CPS3.4</p> <p>日本ペリサイン認証機関の満了時、その証明書に紐づくキー・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。</p>
2	6.2.10 秘密鍵の破壊の方法	<p>変更前記載:CPS 3.3.1</p> <p>日本ペリサイン認証機関の運用ライフタイムの終了に際し、1 つ以上の認証機関秘密鍵のコピーが本 CPS セクション6.2.5に従い保管される。残存する認証機関の秘密鍵のコピーは確実に破壊される。さらに、保管された認証機関秘密鍵は、保管期間の終了に際し、確実に破壊される。認証機関の鍵の破壊行為に関しては、複数の信頼できる個人の関与が要求される。</p> <p>変更後記載:CPS3.4</p> <p>このパラグラフは、削除されました。</p>
3	6.3.2 証明書の運用期間及びキー・ペアの使用期間	<p>変更前記載:CPS 3.3.1</p> <p>(#3) 日本ペリサインは、今後、3年の期間を持つリテール証明書を発行する可能性がある。</p> <p>変更後記載:CPS3.4</p> <p>(#3)組織向けリテール証明書は、3年を上限として発行される。</p>

4	6.3.2 証明書の運用期間及びキー・ペアの使用期間 Table8	Tbale8 への組織向けリテール証明書の期間を3年にすることを反映。
5	7.1.2.1 Key Usage	<p>変更前記載:CPS 3.3.1 KeyUsage エクステンションの Criticality は、通常「FALSE」に設定される。</p> <p>変更後記載:CPS3.4 KeyUsage エクステンションの Criticality は、認証機関証明書は通常「TRUE」に設定され、個人向け証明書は通常「TRUE」もしくは「FALSE」に設定される。</p>
6	7.1.2.1 Table10	7.1.2.1 における Criticality の見直しを反映。
7	7.1.4	<p>変更前記載:CPS 3.3.1 さらに、日本ベリサインは、利用者証明書中に、関連する依拠当事者に対し証明書の使用条件の URL を示す情報を含む追加の Organizational Unit フィールドを含める。これに対する例外は、証明書中の空白、書式設定または相互利用性の制限により、証明書の意図する用途に関連して Organizational Unit を利用することが不可能な場合にのみ許容される。</p> <p>変更後記載:CPS3.4 さらに、日本ベリサインは、利用者証明書中に、関連する依拠当事者に対し証明書の使用条件の URL を示す情報を含む追加の Organizational Unit フィールドを含めることができる。有効な依拠当事者規約へのポインターが、証明書の policy エクステンションに含まれない場合においては、本 Organizational Unit フィールドは、記述されなければならない。</p>
8	9.2.1 保険	<p>変更前記載:CPS 3.3.1 日本ベリサインはこのような賠償責任保険を付保している。</p> <p>変更後記載:CPS3.4 日本ベリサインはこのような”errors and omissions”賠償責任保険を付保する準備がある。</p>
9	9.2.3 拡張された保証	<p>変更前記載:CPS 3.3.1 NetSure プロテクション・プランは、VTN の日本ベリサイン・サブドメイン内で適用される拡張された保証である。これが適用される場合、日本ベリサイン NetSure プロテクション・プランは、リテール証明書を受領する利用者に、証</p>

		<p>明書中の公開鍵に対応する利用者の秘密鍵の盗難、偽造、紛失、意図せざる漏洩等の事故が発生した場合の他に、成りすまし及び利用者の証明書を利用できなかった場合の保護を提供する。NetSure プロテクション・プランは、このプランの対象となる証明書を信頼した、依拠当事者も保護する。NetSure プロテクション・プランは、保険会社の保険に基づき米国ベリサインが提供するプログラムである。NetSure プロテクション・プランに関する情報及びどの証明書がこの対象になるかは、<a href="http://www.verisign.co.jp/repository/netsure/summary.html">http://www.verisign.co.jp/repository/netsure/summary.html</a> を参照。</p> <p>NetSure プロテクション・プランによる保護は、日本ベリサインのマネージド PKI カスタマに対しても手数料を支払うことにより、提供される。マネージド PKI カスタマは、NetSure プロテクション・プランを、このプランの契約の条件に従い利用することができる。このサービスは、マネージド PKI カスタマにより証明書申請が承認された利用者だけでなく、マネージド PKI カスタマ自身にも適用される。例えば、マネージド PKI カスタマが、自己の従業員の証明書申請を承認し、当該従業員がマネージド PKI カスタマの営業目的で証明書を利用する場合に、利用者（上記の従業員）の行為により損失が発生し、最終損失負担者が利用者の雇用者であるためマネージド PKI カスタマとなる場合があげられる。NetSure プロテクション・プランの対象となる場合、マネージド PKI カスタマは利用者の行為により被った損失に関する補償請求をすることができる。</p> <p>変更後記載：CPS3.4</p> <p>NetSure プロテクション・プランは、日本ベリサインの不注意や契約上の責任による証明書発行時やその他の不正行為によって発生した欠陥による紛失/損害から保護するためのベリサインが提供する SSL/コード・サイニング証明書利用者への拡張された保障である。証明書利用者は、適用されるサービス規約に準じることで適用される。</p> <p>NetSure プロテクション・プランに関する一般的な情報及びどの証明書がこの対象になるかは、<a href="http://www.verisign.co.jp/repository/netsure">http://www.verisign.co.jp/repository/netsure</a> にて参照できる。</p>
10	9.3.3 機密情報保護責任	<p>変更前記載：CPS 3.3.1</p> <p>本 CPS セクション 9.4.4 参照。</p> <p>変更後記載：CPS3.4</p>

		ベリサインは、重要な秘密情報が損なわれ、第三者に漏洩しないよう安全な措置を講じる。
11	9.8 責任の制限	変更前記載:CPS 3.3.1 金 1,000 米ドル相当円から金 100 万米ドル相当円の範囲である。  変更後記載:CPS3.4 金 50,000 米ドル相当円から金 250,000 米ドル相当円の範囲である。
12	Appendix B1-B4	CA/Browser Forum に基づく EV SSL 証明書発行手順の反映。