

Section	現在の内容	改定案																					
全般	<a href="#">RFC2459、すなわち、1999年1月</a> 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。	<a href="#">RFC3280、すなわち、2002年4月</a> 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。																					
全般(サービス終了)		「ペリサイン電子公証サービス」、「ペリサイン ローミング・サービス」に関して、「(過去に提供されていたが、現在では提供されておりません。)」を追記し、サービス提供の終了を記述																					
ペリサイン提供サービスの記述を廃止	1.1.2 上記サービスは、日本ペリサインの定める契約に従う。表3は、 <a href="#">日本ペリサインが提供するVTNサービスを要約したものである。</a>	1.1.2 上記サービスは、日本ペリサインの定める契約に従う。表3は、 <a href="#">日本ペリサインが提供するVTNサービスの一部である。</a>																					
個別の変更・追記とCPのセクション番号の変更に伴う変更	1.1 表1 <table border="1"> <thead> <tr> <th>文書</th> <th>公開状況</th> <th>公開場所</th> </tr> </thead> <tbody> <tr> <td>米国ペリサイン Trust Network Certificate Policies</td> <td>公開</td> <td>CP § 1.1.1.1 により日本ペリサインのリポジトリで公開。 <a href="http://www.verisign.com/repository/index.html">http://www.verisign.com/repository/index.html</a></td> </tr> <tr> <td colspan="3">VTN のセキュリティおよび運用に関する付属文書</td> </tr> </tbody> </table> <p>1.1(b) 異なるVTN参加者の役割についての簡単な説明は、CPの <a href="#">Section 1.1(b)</a> に規定されている。</p> <p>1.1.1 <a href="#">CP § 1.1.1 参照</a></p>	文書	公開状況	公開場所	米国ペリサイン Trust Network Certificate Policies	公開	CP § 1.1.1.1 により日本ペリサインのリポジトリで公開。 <a href="http://www.verisign.com/repository/index.html">http://www.verisign.com/repository/index.html</a>	VTN のセキュリティおよび運用に関する付属文書			1.1 表1 <table border="1"> <thead> <tr> <th>文書</th> <th>公開状況</th> <th>公開場所</th> </tr> </thead> <tbody> <tr> <td>米国ペリサイン Trust Network Certificate Policies</td> <td>公開</td> <td>日本ペリサインのリポジトリで公開。 <a href="https://www.verisign.com/repository/index.html">https://www.verisign.com/repository/index.html</a></td> </tr> <tr> <td colspan="3">VTN のセキュリティおよび運用に関する付属文書</td> </tr> <tr> <td>日本ペリサインセキュリティ</td> <td>秘蔵</td> <td>非公開</td> </tr> </tbody> </table> <p>1.1(b) 異なるVTN参加者の役割についての簡単な説明は、CPの <a href="#">Section 1.1</a> に規定されている。</p> <p>1.1.1 <a href="#">CP § 1.1 参照</a></p>	文書	公開状況	公開場所	米国ペリサイン Trust Network Certificate Policies	公開	日本ペリサインのリポジトリで公開。 <a href="https://www.verisign.com/repository/index.html">https://www.verisign.com/repository/index.html</a>	VTN のセキュリティおよび運用に関する付属文書			日本ペリサインセキュリティ	秘蔵	非公開
文書	公開状況	公開場所																					
米国ペリサイン Trust Network Certificate Policies	公開	CP § 1.1.1.1 により日本ペリサインのリポジトリで公開。 <a href="http://www.verisign.com/repository/index.html">http://www.verisign.com/repository/index.html</a>																					
VTN のセキュリティおよび運用に関する付属文書																							
文書	公開状況	公開場所																					
米国ペリサイン Trust Network Certificate Policies	公開	日本ペリサインのリポジトリで公開。 <a href="https://www.verisign.com/repository/index.html">https://www.verisign.com/repository/index.html</a>																					
VTN のセキュリティおよび運用に関する付属文書																							
日本ペリサインセキュリティ	秘蔵	非公開																					

VIN サービス	CP の参照箇所	提供サービス
証明書基本サービス		
ペリサイン マネージド PKI	CP § 1.1.2.1.1	マネージド PKI マネージド PKI ライト マネージド PKI for SSL マネージド PKI for SSL(プレミアム エディション)
オプション・サービス		
認証サービス	CP § 1.1.2.1.1	認証業務代行サービス
ペリサイン電子公証サービス	CP § 1.1.2.1.2	日本ペリサイン電子公証サービス
NetSign™ プロテクション・プラン	CP § 1.1.2.1.3	利用者、依頼当事者およびマネージド PKI カスタマ向け NetSign™ プロテクション・サービス
特例な用途の証明書		
ペリサイン マネージド PKI キーマネージメントサービス	CP § 1.1.2.1.3	マネージド PKI キーマネージメント・デュアル・キー・システム マネージド PKI キーマネージメント・シングル・キー・システム
ペリサイン ローミング・サービス	CP § 1.1.2.1.3	企業がエンタープライズ・ローミング・サーバを持つローミング・サービス 信頼される第 4 当事者がエンタープライズ・ローミング・サーバを持つローミング・サービス

表 3 日本ペリサインの提供する VIN サービス

### 1.1.2.1

日本ペリサインの提供するペリサイン マネージド PKI は、日本ペリサインの企業カスタマが証明書を従業員、パートナー、サプライヤーおよび顧客、さらにサーバ、ルーターおよ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完全に統合された PKI サービスである。[日本ペリサインの提供するマネージド PKI サービスの詳細は、CP § 1.1.2.1.1 に記述されている](#)。日本ペリサインのサブドメインにおけるマネージド PKI のセキュリティ要件は、エンタープライズ・セキュリティ・ガイド（利用可能な場合）に規定されている。マネージド PKI はアウトソース・サービスである。ペリサイン マネージド PKI を利用するカスタマは、3 種類に分けられる。

最後の種類は、セキュア・サーバ ID およびグローバル・サーバ ID として知られるサーバ証明書の証明書申請を承認するためにマネージド PKI を利用するカスタマである（[セキュア・サーバ ID およびグローバル・サーバ ID の違いについては、CP § 1.3.4.1.3.2 参照](#)）。

VIN サービス	提供サービス
ペリサイン マネージド PKI	マネージド PKI マネージド PKI ライト マネージド PKI for SSL マネージド PKI for SSL(プレミアム エディション) ペリサイン セキュアモデル ID
認証サービス	認証業務代行サービス
ペリサイン電子公証サービス	日本ペリサイン電子公証サービス
NetSign™ プロテクション・プラン	利用者、依頼当事者およびマネージド PKI カスタマ向け NetSign™ プロテクション・サービス
ペリサイン 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・デュアル・キー・システム マネージド PKI キーマネージメント・シングル・キー・システム
ペリサイン ローミング・サービス	企業がエンタープライズ・ローミング・サーバを持つローミング・サービス 信頼される第 4 当事者がエンタープライズ・ローミング・サーバを持つローミング・サービス

表 3 日本ペリサインの提供する VIN サービス

### 1.1.2.1

日本ペリサインの提供するペリサイン マネージド PKI は、日本ペリサインの企業カスタマが証明書を従業員、パートナー、サプライヤーおよび顧客、さらにサーバ、ルーターおよ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完全に統合された PKI サービスである。日本ペリサインのサブドメインにおけるマネージド PKI のセキュリティ要件は、エンタープライズ・セキュリティ・ガイド（利用可能な場合）に規定されている。マネージド PKI はアウトソース・サービスである。ペリサイン マネージド PKI を利用するカスタマは、3 種類に分けられる。

最後の種類は、セキュア・サーバ ID およびグローバル・サーバ ID として知られるサーバ証明書の証明書申請を承認するためにマネージド PKI を利用するカスタマである。

<p>1.1.2.1.2</p> <p>日本ペリサインは、<a href="#">CP § 1.1.2.1.2 に記載される</a> 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、日本ペリサインは、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、日本ペリサイン・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を発行する米国ペリサイン認証機関の登録機関となる。日本ペリサイン・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。</p> <p>日本ペリサインは、<a href="#">CP § 1.1.2.1.2 に記載する</a> 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。日本ペリサインは、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。日本ペリサインはまた、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。日本ペリサインは又、<a href="#">CP § 1.1.2.1.2 に記載するとおり</a>、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。米国ペリサインから日本ペ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。</p>	<p>1.1.2.1.2</p> <p>日本ペリサインは、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、日本ペリサインは、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、日本ペリサイン・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を発行する米国ペリサイン認証機関の登録機関となる。日本ペリサイン・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。</p> <p>日本ペリサインは、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。日本ペリサインは、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。日本ペリサインはまた、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。日本ペリサインは又、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。米国ペリサインから日本ペ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。</p>
--	---

<p>1.1.2.2.1</p> <p>日本ペリサインは、組織に対し、認証業務代行サービスを提供する。<u>これらの詳細は、CP § 1.1.2.2.1 に記述される。</u></p> <p>認証業務代行サービスにより、日本ペリサインは、カスタマの代わりに証明書申請者の実在性を確認する。</p> <p>1.1.2.2.2</p> <p>ペリサイン電子公証サービス</p> <p><u>日本ペリサインは、CP § 1.1.2.2.2 に規定する</u>ペリサイン電子公証サービスを提供する。このサービス提供の条件は、日本ペリサインとカスタマとの契約 <u>に従うものとする。</u></p> <p>1.1.2.3.2</p> <p>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、日本ペリサインの提供するペリサイン・キー・リカバリー・サービスと一体となって機</p>	<p>1.1.2.2.1</p> <p>日本ペリサインは、組織に対し、認証業務代行サービスを提供する。認証業務代行サービスにより、日本ペリサインは、カスタマの代わりに証明書申請者の実在性を確認する。</p> <p>1.1.2.2.2</p> <p>ペリサイン電子公証サービス(本サービスは、現在では提供されていません。)</p> <p>このサービス提供の条件は、日本ペリサインとカスタマとの契約 <u>がある場合にはそれに従うものとする。</u></p> <p>1.1.2.3.2</p> <p>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、日本ペリサインの提供するペリサイン・キー・リカバリー・サービスと一体となって機</p>
--	--

<p>能する。<a href="#">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。</a></p> <p>1.3.1 <a href="#">CP § 1.3.1 で検討するように、</a>米国ペリサインがRSA Security Inc.から買収したRSAセキュア・サーバ認証機関は、クラス3組織向け証明書とみなされるセキュア・サーバIDを発行する。米国ペリサインは、日本ペリサインのサブドメイン内で、RSAセキュア・サーバ認証機関をクラス3認証機関として承認しかつ指定する。RSAセキュア・サーバ認証機関が発行するセキュア・サーバIDは、他のクラス3組織向け証明書と同等の信頼性についての保証を提供するものとみなされる。</p> <p>1.3.4 本CPSは、日本ペリサイン、カスタマ、リセラー、利用者および依拠当事者を含む、日本ペリサインのサブドメイン参加者全てに適用される。本CPSは、VTN内の日本ペリサインのサブドメインおよびVTNを支える日本ペリサインの中心的なインフラストラクチャに適用される。本CPSは、CPに記載されるクラス1~3の証明書の日本ペリサイン・サブドメインにおける利用を規定する手続きを記載する。各クラスの証明書は、一般的に、<a href="#">CP § 1.3.4.1</a>および本CPS § 1.1.1 (表2)に定める用途に適している。しかしながら、契約によりもしくは特定の環境下(企業内での利用等)では、VTN参加者は本CPS § 1.1.1 および § 1.3.4.1 で記述するものより高いセキュリティを必要とする目的で証明書を使用することができる。ただし、かかる使用は、そのような使用をする組織内に限定され、本CPS § 2.2.1.2 および § 2.2.2 に従うことを条件とし、当該組織はかかる使用から発生する全ての損害について責任を負うものとする。</p>	<p>能する。</p> <p>1.3.1 米国ペリサインがRSA Security Inc.から買収したRSAセキュア・サーバ認証機関は、クラス3組織向け証明書とみなされるセキュア・サーバIDを発行する。米国ペリサインは、日本ペリサインのサブドメイン内で、RSAセキュア・サーバ認証機関をクラス3認証機関として承認しかつ指定する。RSAセキュア・サーバ認証機関が発行するセキュア・サーバIDは、他のクラス3組織向け証明書と同等の信頼性についての保証を提供するものとみなされる。</p> <p>1.3.4 本CPSは、日本ペリサイン、カスタマ、リセラー、利用者および依拠当事者を含む、日本ペリサインのサブドメイン参加者全てに適用される。本CPSは、VTN内の日本ペリサインのサブドメインおよびVTNを支える日本ペリサインの中心的なインフラストラクチャに適用される。本CPSは、CPに記載されるクラス1~3の証明書の日本ペリサイン・サブドメインにおける利用を規定する手続きを記載する。各クラスの証明書は、一般的に、<a href="#">CP § 1.4</a>および本CPS § 1.1.1 (表2)に定める用途に適している。しかしながら、契約によりもしくは特定の環境下(企業内での利用等)では、VTN参加者は本CPS § 1.1.1 および § 1.3.4.1 で記述するものより高いセキュリティを必要とする目的で証明書を使用することができる。ただし、かかる使用は、そのような使用をする組織内に限定され、本CPS § 2.2.1.2 および § 2.2.2 に従うことを条件とし、当該組織はかかる使用から発生する全ての損害について責任を負うものとする。</p>
---	--

	<p>1.3.4.1 適切な用途については、<a href="#">CP § 1.3.4.1</a>および本CPS § 1.1.1 (表 2) を参照。</p> <p>2.2.1.1 日本ベリサインのNetSure<sup>SM</sup>プロテクション・プランに関するより詳細な情報については、<a href="#">CPの § 1.1.2.2.3 および</a>本CPSの § 1.1.2.2.3 を参照されたい。</p> <p>2.8 日本ベリサインは、<a href="#">CP § 2.8</a>に従い、プライバシー・ポリシーを実施しており、当該ポリシーは、次のサイトにて閲覧可能である。</p>	<p>1.3.4.1 適切な用途については、<a href="#">CP § 1.4</a>および本CPS § 1.1.1(表 2) を参照。</p> <p>2.2.1.1 日本ベリサインのNetSure<sup>SM</sup>プロテクション・プランに関するより詳細な情報については、本CPSの § 1.1.2.2.3 を参照されたい。</p> <p>2.8 日本ベリサインは、<a href="#">CP § 9.4.1</a>に従い、プライバシー・ポリシーを実施しており、当該ポリシーは、次のサイトにて閲覧可能である。</p>																		
<p>1.1.1 表 2</p>	<table border="1"> <tr> <td>クラス 2: 個人</td> <td>リテール (現在提供されていないが、将来提供される可能性があります)。</td> <td>クラス 1 リテールの記録に加え、1 つ以上の第三者データベースまたは同等の情報源による申請情報の自動調査または管理者による調査。</td> <td>機密情報の暗号化による電子メールのセキュリティの向上、認証のためのデジタル署名およびウェブ上のアクセス・コントロール。個人と会社および</td> </tr> </table>	クラス 2: 個人	リテール (現在提供されていないが、将来提供される可能性があります)。	クラス 1 リテールの記録に加え、1 つ以上の第三者データベースまたは同等の情報源による申請情報の自動調査または管理者による調査。	機密情報の暗号化による電子メールのセキュリティの向上、認証のためのデジタル署名およびウェブ上のアクセス・コントロール。個人と会社および	<table border="1"> <tr> <td>クラス 2: 個人</td> <td>リテール</td> <td>クラス 1 リテールの記録に加え、1 つ以上の第三者データベースまたは同等の情報源による申請情報の自動調査または管理者による調査。</td> <td>機密情報の暗号化による電子メールのセキュリティの向上、認証のためのデジタル署名およびウェブ上のアクセス・コントロール。個人と会社および</td> </tr> </table>	クラス 2: 個人	リテール	クラス 1 リテールの記録に加え、1 つ以上の第三者データベースまたは同等の情報源による申請情報の自動調査または管理者による調査。	機密情報の暗号化による電子メールのセキュリティの向上、認証のためのデジタル署名およびウェブ上のアクセス・コントロール。個人と会社および										
クラス 2: 個人	リテール (現在提供されていないが、将来提供される可能性があります)。	クラス 1 リテールの記録に加え、1 つ以上の第三者データベースまたは同等の情報源による申請情報の自動調査または管理者による調査。	機密情報の暗号化による電子メールのセキュリティの向上、認証のためのデジタル署名およびウェブ上のアクセス・コントロール。個人と会社および																	
クラス 2: 個人	リテール	クラス 1 リテールの記録に加え、1 つ以上の第三者データベースまたは同等の情報源による申請情報の自動調査または管理者による調査。	機密情報の暗号化による電子メールのセキュリティの向上、認証のためのデジタル署名およびウェブ上のアクセス・コントロール。個人と会社および																	
<p>1.3.3 表 4</p>	<table border="1"> <tr> <td>クラス 2: 個人</td> <td>リテール (現在提供されていないが、将来提供される可能性があります)。</td> <td>全ての個人</td> </tr> <tr> <td></td> <td>マネージド IP</td> <td>マネージド IP にカスタマイズに関連する個人または関連する個人。</td> </tr> <tr> <td>クラス 3: 個人</td> <td>リテール (現在提供)</td> <td>全ての個人</td> </tr> </table>	クラス 2: 個人	リテール (現在提供されていないが、将来提供される可能性があります)。	全ての個人		マネージド IP	マネージド IP にカスタマイズに関連する個人または関連する個人。	クラス 3: 個人	リテール (現在提供)	全ての個人	<table border="1"> <tr> <td>クラス 2: 個人</td> <td>リテール</td> <td>全ての個人</td> </tr> <tr> <td></td> <td>マネージド IP</td> <td>マネージド IP にカスタマイズに関連する個人または関連する個人。</td> </tr> <tr> <td>クラス 3: 個人</td> <td>リテール (現在提供)</td> <td>全ての個人</td> </tr> </table>	クラス 2: 個人	リテール	全ての個人		マネージド IP	マネージド IP にカスタマイズに関連する個人または関連する個人。	クラス 3: 個人	リテール (現在提供)	全ての個人
クラス 2: 個人	リテール (現在提供されていないが、将来提供される可能性があります)。	全ての個人																		
	マネージド IP	マネージド IP にカスタマイズに関連する個人または関連する個人。																		
クラス 3: 個人	リテール (現在提供)	全ての個人																		
クラス 2: 個人	リテール	全ての個人																		
	マネージド IP	マネージド IP にカスタマイズに関連する個人または関連する個人。																		
クラス 3: 個人	リテール (現在提供)	全ての個人																		
<p>2.6.1 表 7 誤記修正</p>	<p><a href="https://www.verisign.co.jp/repository/index.html">https://www.verisign.co.jp/repository/index.html</a>の日本ベリサインのリポジトリにおけるクエリー機能を通じて依頼当事者に利用可能。</p> <p>また、<a href="https://directory.verisign.com">directory.verisign.com</a>の米国ベリサイン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</p>	<p><a href="https://directory.verisign.co.jp">directory.verisign.co.jp</a> のベリサイン LDAP ディレクトリ・サーバにおけるクエリーを通じて利用可能、</p> <p>また、<a href="https://directory.verisign.com">directory.verisign.com</a> の米国ベリサイン 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</p>																		

3.1.9 誤記修正	<p>証明書申請者が、証明書申請で特定された人物であること (クラス1証明書の<b>証明者</b>申請者を除く)</p>	<p>証明書申請者が、証明書申請で特定された人物であること (クラス1証明書の<b>証明書</b>申請者を除く)</p>																																												
3.1.9.2.2	<p><u>(現在提供されていないが、将来提供する可能性あり)</u></p> <p>日本ペリサインは、証明書申請中の確認すべき情報が日本ペリサインの承認した同一性を証明するためのデータベース(主要な信用機関またはその他の信用できる情報提供サービス)中の情報と合致すると決定した場合、クラス2リテール証明書の証明書申請を有効なものとする。証明書申請中の情報が、データベース中の情報と一致する場合、日本ペリサインは証明書申請を承認することができる。</p>	<p>日本ペリサインは、証明書申請中の確認すべき情報が日本ペリサインの承認した同一性を証明するためのデータベース(主要な信用機関またはその他の信用できる情報提供サービス)中の情報と合致すると決定した場合、クラス2リテール証明書の証明書申請を有効なものとする。証明書申請中の情報が、データベース中の情報と一致する場合、日本ペリサインは証明書申請を承認することができる。</p>																																												
4.6.2	<p>証明書に関する記録は、証明書の有効期間満了または取消しの日から少なくとも次の期間保管される。</p> <ul style="list-style-type: none"> <li>・ クラス1証明書については5年間</li> <li>・ クラス2証明書については<b>10年間</b></li> <li>・ クラス3証明書については<b>30年間</b></li> </ul>	<p>証明書に関する記録は、証明書の有効期間満了または取消しの日から少なくとも次の期間保管される。</p> <ul style="list-style-type: none"> <li>・ クラス1証明書については5年の期間</li> <li>・ クラス2証明書については<b>10年6ヶ月の期間</b></li> <li>・ クラス3証明書については<b>10年6ヶ月の期間</b></li> </ul>																																												
5.3.1	<p>信頼される人物になろうとする者は、将来の業務を十分に遂行するために必要な経歴、資格および経験を有することの証拠を提出しなければならない。さらに必要な場合、政府機関との契約に基づく証明サービスを履行するために必要な政府許可も提出しなければならない。経歴調査は、信頼される地位を有する人員について、<b>3年毎</b>に繰返されるものとする。</p>	<p>信頼される人物になろうとする者は、将来の業務を十分に遂行するために必要な経歴、資格および経験を有することの証拠を提出しなければならない。さらに必要な場合、政府機関との契約に基づく証明サービスを履行するために必要な政府許可も提出しなければならない。経歴調査は、信頼される地位を有する人員について、<b>5年毎</b>に繰返されるものとする。</p>																																												
6.3.2 表 18	<table border="1"> <thead> <tr> <th>証明書の発行者</th> <th>クラス1</th> <th>クラス2</th> <th>クラス3</th> </tr> </thead> <tbody> <tr> <td>自己署名された第一次認証機関(1024ビット)</td> <td>30年まで</td> <td>30年まで</td> <td>30年まで</td> </tr> <tr> <td>自己署名された第一次認証機関(2048ビット)</td> <td>50年まで</td> <td>50年まで</td> <td>50年まで</td> </tr> <tr> <td>自己署名された認証機関</td> <td>適用なし</td> <td>適用なし</td> <td>10年まで</td> </tr> <tr> <td>第一次認証機関から認証機関</td> <td>10年まで</td> <td>10年まで</td> <td>10年まで</td> </tr> <tr> <td>認証機関から下位認証機関</td> <td>5年まで</td> <td>5年まで</td> <td>5年まで</td> </tr> <tr> <td>認証機関から利用者</td> <td>2年まで</td> <td>通常は3年まで、ただし下記の場合には5年まで</td> <td>通常は3年まで、ただし下記の場合には5年まで</td> </tr> </tbody> </table> <p>表 18: 証明書の有効期間</p>	証明書の発行者	クラス1	クラス2	クラス3	自己署名された第一次認証機関(1024ビット)	30年まで	30年まで	30年まで	自己署名された第一次認証機関(2048ビット)	50年まで	50年まで	50年まで	自己署名された認証機関	適用なし	適用なし	10年まで	第一次認証機関から認証機関	10年まで	10年まで	10年まで	認証機関から下位認証機関	5年まで	5年まで	5年まで	認証機関から利用者	2年まで	通常は3年まで、ただし下記の場合には5年まで	通常は3年まで、ただし下記の場合には5年まで	<table border="1"> <thead> <tr> <th>証明書の発行者</th> <th>有効期間</th> </tr> </thead> <tbody> <tr> <td>自己署名された第一次認証機関(1024ビット)</td> <td>30年まで</td> </tr> <tr> <td>自己署名された第一次認証機関(2048ビット)</td> <td>50年まで</td> </tr> <tr> <td>第一次認証機関から申請認証機関(オフライン)</td> <td>10年まで(認証機関更新作業後は、15年まで)</td> </tr> <tr> <td>第一次認証機関から認証機関(オンライン)</td> <td>5年まで(認証機関更新作業後は、10年まで)(注)</td> </tr> <tr> <td>申請認証機関(オフライン)から認証機関(オンライン)</td> <td>5年まで(認証機関更新作業後は、10年まで)(注)</td> </tr> <tr> <td>認証機関(オンライン)から利用者(個人)</td> <td>通常は3年まで、ただし条件を満たす場合には5年まで(注)</td> </tr> <tr> <td>認証機関(オンライン)から利用者(組織)</td> <td>通常は3年まで(注)(注)</td> </tr> </tbody> </table>	証明書の発行者	有効期間	自己署名された第一次認証機関(1024ビット)	30年まで	自己署名された第一次認証機関(2048ビット)	50年まで	第一次認証機関から申請認証機関(オフライン)	10年まで(認証機関更新作業後は、15年まで)	第一次認証機関から認証機関(オンライン)	5年まで(認証機関更新作業後は、10年まで)(注)	申請認証機関(オフライン)から認証機関(オンライン)	5年まで(認証機関更新作業後は、10年まで)(注)	認証機関(オンライン)から利用者(個人)	通常は3年まで、ただし条件を満たす場合には5年まで(注)	認証機関(オンライン)から利用者(組織)	通常は3年まで(注)(注)
証明書の発行者	クラス1	クラス2	クラス3																																											
自己署名された第一次認証機関(1024ビット)	30年まで	30年まで	30年まで																																											
自己署名された第一次認証機関(2048ビット)	50年まで	50年まで	50年まで																																											
自己署名された認証機関	適用なし	適用なし	10年まで																																											
第一次認証機関から認証機関	10年まで	10年まで	10年まで																																											
認証機関から下位認証機関	5年まで	5年まで	5年まで																																											
認証機関から利用者	2年まで	通常は3年まで、ただし下記の場合には5年まで	通常は3年まで、ただし下記の場合には5年まで																																											
証明書の発行者	有効期間																																													
自己署名された第一次認証機関(1024ビット)	30年まで																																													
自己署名された第一次認証機関(2048ビット)	50年まで																																													
第一次認証機関から申請認証機関(オフライン)	10年まで(認証機関更新作業後は、15年まで)																																													
第一次認証機関から認証機関(オンライン)	5年まで(認証機関更新作業後は、10年まで)(注)																																													
申請認証機関(オフライン)から認証機関(オンライン)	5年まで(認証機関更新作業後は、10年まで)(注)																																													
認証機関(オンライン)から利用者(個人)	通常は3年まで、ただし条件を満たす場合には5年まで(注)																																													
認証機関(オンライン)から利用者(組織)	通常は3年まで(注)(注)																																													
6.3.2 表 18		<p>(注釈の追記)</p> <p>(#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場合がありますが、適切な時期に使用出来ない状態する。</p>																																												

		<p>(#2 5年の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、オンライン認証機関の有効期間は更新作業することなしに10年に設定され、5年経過後に認証機関鍵ペアの交換を行う。</p> <p>(#3 組織向け証明書に関しては、3年の有効期限の組織向け証明書を将来発行する可能性がある。このようなウェブ・サーバ証明書は、少なくとも2.5ヶ月毎に再認証が必要となる。</p> <p>(#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。</p>																																																																																																																																				
<p>3.1.8.1.1 表 10</p>	<table border="1"> <thead> <tr> <th>証明書の種類</th> <th>追加の手続き</th> </tr> </thead> <tbody> <tr> <td>全てのサーバ証明書</td> <td>日本ベリサインは、証明書申請者が証明書のサブジェクトであるサーバのドメイン・ネームの登録された所有者であること、またはその他の方法によりドメイン・ネームを利用する権限があることを検証する。</td> </tr> <tr> <td>グローバル・サーバ ID</td> <td>日本ベリサインは、米国輸出規制および米国 Department of Commerce Bureau of Export Administration (CEA)の発行する許可を充足するための調査を行う。</td> </tr> </tbody> </table> <p>表 10. 特約の認証手続き</p>	証明書の種類	追加の手続き	全てのサーバ証明書	日本ベリサインは、証明書申請者が証明書のサブジェクトであるサーバのドメイン・ネームの登録された所有者であること、またはその他の方法によりドメイン・ネームを利用する権限があることを検証する。	グローバル・サーバ ID	日本ベリサインは、米国輸出規制および米国 Department of Commerce Bureau of Export Administration (CEA)の発行する許可を充足するための調査を行う。	<table border="1"> <thead> <tr> <th>証明書の種類</th> <th>追加の手続き</th> </tr> </thead> <tbody> <tr> <td>全てのサーバ証明書</td> <td>日本ベリサインは、証明書申請者が証明書のサブジェクトであるサーバのドメイン・ネームの登録された所有者であること、またはその他の方法によりドメイン・ネームを利用する権限があることを検証する。</td> </tr> <tr> <td>グローバル・サーバ ID</td> <td>日本ベリサインは、米国輸出規制および米国 Department of Commerce Bureau of Export Administration (CEA)の発行する許可を充足するための調査を行う。</td> </tr> <tr> <td>Managed Entry for Intracorp-ETL Certificate (現在提供されていないが将来提供される可能性あり)</td> <td>日本ベリサインは、サブジェクトに割り当てられたホスト名(もしくは、IPアドレス)が、インターネットからアクセスしにくいこと、かつ、証明書所有者によって管理されていることを検証する。</td> </tr> </tbody> </table> <p>表 10. 特約の認証手続き</p>	証明書の種類	追加の手続き	全てのサーバ証明書	日本ベリサインは、証明書申請者が証明書のサブジェクトであるサーバのドメイン・ネームの登録された所有者であること、またはその他の方法によりドメイン・ネームを利用する権限があることを検証する。	グローバル・サーバ ID	日本ベリサインは、米国輸出規制および米国 Department of Commerce Bureau of Export Administration (CEA)の発行する許可を充足するための調査を行う。	Managed Entry for Intracorp-ETL Certificate (現在提供されていないが将来提供される可能性あり)	日本ベリサインは、サブジェクトに割り当てられたホスト名(もしくは、IPアドレス)が、インターネットからアクセスしにくいこと、かつ、証明書所有者によって管理されていることを検証する。																																																																																																																						
証明書の種類	追加の手続き																																																																																																																																					
全てのサーバ証明書	日本ベリサインは、証明書申請者が証明書のサブジェクトであるサーバのドメイン・ネームの登録された所有者であること、またはその他の方法によりドメイン・ネームを利用する権限があることを検証する。																																																																																																																																					
グローバル・サーバ ID	日本ベリサインは、米国輸出規制および米国 Department of Commerce Bureau of Export Administration (CEA)の発行する許可を充足するための調査を行う。																																																																																																																																					
証明書の種類	追加の手続き																																																																																																																																					
全てのサーバ証明書	日本ベリサインは、証明書申請者が証明書のサブジェクトであるサーバのドメイン・ネームの登録された所有者であること、またはその他の方法によりドメイン・ネームを利用する権限があることを検証する。																																																																																																																																					
グローバル・サーバ ID	日本ベリサインは、米国輸出規制および米国 Department of Commerce Bureau of Export Administration (CEA)の発行する許可を充足するための調査を行う。																																																																																																																																					
Managed Entry for Intracorp-ETL Certificate (現在提供されていないが将来提供される可能性あり)	日本ベリサインは、サブジェクトに割り当てられたホスト名(もしくは、IPアドレス)が、インターネットからアクセスしにくいこと、かつ、証明書所有者によって管理されていることを検証する。																																																																																																																																					
<p>4.4.11 誤記修正</p>	<p>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ウェブ・ベースのクエリー機能を通じて利用することができる。</p>	<p>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。</p>																																																																																																																																				
<p>4.4.11 誤記修正</p>	<p><a href="https://www.verisign.co.jp/repository/">https://www.verisign.co.jp/repository/</a> (個人の証明書について) および <a href="https://www.verisign.co.jp/repository/">https://www.verisign.co.jp/repository/</a> (サーバおよび開発者の証明書について)</p>	<p><a href="https://www.verisign.co.jp/directory/">directory.verisign.co.jp</a> の日本ベリサイン LDAP ディレクトリ・サーバ</p>																																																																																																																																				
<p>6.1.9 表 16</p>	<table border="1"> <thead> <tr> <th></th> <th>認証機関</th> <th>クラス1およびクラス2証明書</th> <th>クラス3およびクラス4証明書</th> <th>デュアル鍵ペア署名 (マネージド PKI キーマネージメント)</th> <th>デュアル鍵ペア暗号化 (マネージド PKI キーマネージメント)</th> </tr> </thead> <tbody> <tr> <td>criticality</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> </tr> <tr> <td>0</td> <td>クリア</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>1</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>2</td> <td>クリア</td> <td>セット</td> <td>クリア</td> <td>セット</td> <td>クリア</td> </tr> <tr> <td>3</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>4</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>5</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>6</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>7</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>8</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> </tbody> </table> <p>表 16. 鍵用途エクステンションの設定</p>		認証機関	クラス1およびクラス2証明書	クラス3およびクラス4証明書	デュアル鍵ペア署名 (マネージド PKI キーマネージメント)	デュアル鍵ペア暗号化 (マネージド PKI キーマネージメント)	criticality	FALSE	FALSE	FALSE	FALSE	FALSE	0	クリア	セット	クリア	クリア	クリア	1	クリア	クリア	クリア	クリア	クリア	2	クリア	セット	クリア	セット	クリア	3	クリア	クリア	クリア	クリア	クリア	4	クリア	クリア	クリア	クリア	クリア	5	セット	クリア	クリア	クリア	クリア	6	セット	クリア	クリア	クリア	クリア	7	クリア	クリア	クリア	クリア	クリア	8	クリア	クリア	クリア	クリア	クリア	<table border="1"> <thead> <tr> <th></th> <th>認証機関</th> <th>クラス1およびクラス2証明書</th> <th>クラス3およびクラス4証明書</th> <th>デュアル鍵ペア署名 (マネージド PKI キーマネージメント)</th> <th>デュアル鍵ペア暗号化 (マネージド PKI キーマネージメント)</th> </tr> </thead> <tbody> <tr> <td>criticality</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> </tr> <tr> <td>0</td> <td>クリア</td> <td>セット</td> <td>セット</td> <td>セット</td> <td>クリア</td> </tr> <tr> <td>1</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>2</td> <td>クリア</td> <td>セット</td> <td>セット</td> <td>クリア</td> <td>セット</td> </tr> <tr> <td>3</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>4</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>5</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>6</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>7</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>8</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> </tbody> </table> <p>表 16. 鍵用途エクステンションの設定</p>		認証機関	クラス1およびクラス2証明書	クラス3およびクラス4証明書	デュアル鍵ペア署名 (マネージド PKI キーマネージメント)	デュアル鍵ペア暗号化 (マネージド PKI キーマネージメント)	criticality	FALSE	FALSE	FALSE	FALSE	FALSE	0	クリア	セット	セット	セット	クリア	1	クリア	クリア	クリア	クリア	クリア	2	クリア	セット	セット	クリア	セット	3	クリア	クリア	クリア	クリア	クリア	4	クリア	クリア	クリア	クリア	クリア	5	セット	クリア	クリア	クリア	クリア	6	セット	クリア	クリア	クリア	クリア	7	クリア	クリア	クリア	クリア	クリア	8	クリア	クリア	クリア	クリア	クリア
	認証機関	クラス1およびクラス2証明書	クラス3およびクラス4証明書	デュアル鍵ペア署名 (マネージド PKI キーマネージメント)	デュアル鍵ペア暗号化 (マネージド PKI キーマネージメント)																																																																																																																																	
criticality	FALSE	FALSE	FALSE	FALSE	FALSE																																																																																																																																	
0	クリア	セット	クリア	クリア	クリア																																																																																																																																	
1	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
2	クリア	セット	クリア	セット	クリア																																																																																																																																	
3	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
4	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
5	セット	クリア	クリア	クリア	クリア																																																																																																																																	
6	セット	クリア	クリア	クリア	クリア																																																																																																																																	
7	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
8	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
	認証機関	クラス1およびクラス2証明書	クラス3およびクラス4証明書	デュアル鍵ペア署名 (マネージド PKI キーマネージメント)	デュアル鍵ペア暗号化 (マネージド PKI キーマネージメント)																																																																																																																																	
criticality	FALSE	FALSE	FALSE	FALSE	FALSE																																																																																																																																	
0	クリア	セット	セット	セット	クリア																																																																																																																																	
1	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
2	クリア	セット	セット	クリア	セット																																																																																																																																	
3	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
4	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
5	セット	クリア	クリア	クリア	クリア																																																																																																																																	
6	セット	クリア	クリア	クリア	クリア																																																																																																																																	
7	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
8	クリア	クリア	クリア	クリア	クリア																																																																																																																																	
<p>6.5 誤記修正</p>	<p>エンタープライズ・セキュリティ・ガイドに定める要件に合致する信頼できるシステムを用いることを要する。</p>	<p>エンタープライズ・セキュリティ・ガイド (利用可能な場合) に定める要件に合致する信頼できるシステムを用いることを要する。</p>																																																																																																																																				



<p>7.1.2.5 表 21</p>	<table border="1"> <thead> <tr> <th>証明書の種類</th> <th>証明書の種類</th> </tr> </thead> <tbody> <tr> <td>証明書 (CA)</td> <td>クラス3 インターナショナル・サーバ証明書</td> </tr> <tr> <td>OCSP レスポンダー</td> <td>クラス1~3 パブリック・プライマリ-OCSP レスポンダー セキュア・サーバ OCSP レスポンダー</td> </tr> <tr> <td>クラス3 ウェブ・サーバ証明書</td> <td>セキュア・サーバ ID グローバル・サーバ ID</td> </tr> </tbody> </table> <p>表 21: 拡張鍵用途を使用する証明書</p>	証明書の種類	証明書の種類	証明書 (CA)	クラス3 インターナショナル・サーバ証明書	OCSP レスポンダー	クラス1~3 パブリック・プライマリ-OCSP レスポンダー セキュア・サーバ OCSP レスポンダー	クラス3 ウェブ・サーバ証明書	セキュア・サーバ ID グローバル・サーバ ID	<table border="1"> <thead> <tr> <th>証明書の種類</th> <th>証明書の種類</th> </tr> </thead> <tbody> <tr> <td>証明書 (CA)</td> <td>クラス3 インターナショナル・サーバ証明書</td> </tr> <tr> <td>OCSP レスポンダー</td> <td>クラス1~3 パブリック・プライマリ-OCSP レスポンダー セキュア・サーバ OCSP レスポンダー</td> </tr> <tr> <td>クラス1 ウェブ・サーバ証明書</td> <td>セキュア・サーバ ID グローバル・サーバ ID</td> </tr> <tr> <td>コード/オブジェクト・サイニング利用証明書</td> <td>コード/オブジェクト・サイニング利用証明書</td> </tr> <tr> <td>利用証明書</td> <td>クラス1 利用証明書 クラス2 利用証明書</td> </tr> </tbody> </table> <p>表 21: 拡張鍵用途を使用する証明書</p>	証明書の種類	証明書の種類	証明書 (CA)	クラス3 インターナショナル・サーバ証明書	OCSP レスポンダー	クラス1~3 パブリック・プライマリ-OCSP レスポンダー セキュア・サーバ OCSP レスポンダー	クラス1 ウェブ・サーバ証明書	セキュア・サーバ ID グローバル・サーバ ID	コード/オブジェクト・サイニング利用証明書	コード/オブジェクト・サイニング利用証明書	利用証明書	クラス1 利用証明書 クラス2 利用証明書																																																																																																																																																				
証明書の種類	証明書の種類																																																																																																																																																																									
証明書 (CA)	クラス3 インターナショナル・サーバ証明書																																																																																																																																																																									
OCSP レスポンダー	クラス1~3 パブリック・プライマリ-OCSP レスポンダー セキュア・サーバ OCSP レスポンダー																																																																																																																																																																									
クラス3 ウェブ・サーバ証明書	セキュア・サーバ ID グローバル・サーバ ID																																																																																																																																																																									
証明書の種類	証明書の種類																																																																																																																																																																									
証明書 (CA)	クラス3 インターナショナル・サーバ証明書																																																																																																																																																																									
OCSP レスポンダー	クラス1~3 パブリック・プライマリ-OCSP レスポンダー セキュア・サーバ OCSP レスポンダー																																																																																																																																																																									
クラス1 ウェブ・サーバ証明書	セキュア・サーバ ID グローバル・サーバ ID																																																																																																																																																																									
コード/オブジェクト・サイニング利用証明書	コード/オブジェクト・サイニング利用証明書																																																																																																																																																																									
利用証明書	クラス1 利用証明書 クラス2 利用証明書																																																																																																																																																																									
<p>7.1.2.5</p>	<p>その他の種類の証明書については、日本ペリサインは拡張鍵用途エクステンションを使用しない。</p>	<p><u>通常</u>、その他の種類の証明書については、日本ペリサインは拡張鍵用途エクステンションを使用しない。</p>																																																																																																																																																																								
<p>7.1.2.5</p>	<table border="1"> <thead> <tr> <th></th> <th>クラス3 インターナショナル・サーバ ID</th> <th>OCSP レスポンダー</th> <th>セキュア・サーバ ID</th> <th>グローバル・サーバ ID</th> <th>コード/オブジェクト・サイニング利用証明書</th> </tr> </thead> <tbody> <tr> <td>Criticality</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> </tr> <tr> <td>0 ServerAuth</td> <td>クリア</td> <td>クリア</td> <td>セット</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>1 ClientAuth</td> <td>クリア</td> <td>セット</td> <td>セット</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>2 CodeSigning</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>セット</td> </tr> <tr> <td>3 EmailProtection</td> <td>クリア</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>4 ipsecEndSystem</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>5 ipsecTunnel</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>6 ipsecUser</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>7 TimeStamping</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>8 OCSP Signing</td> <td>クリア</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>Microsoft Server Gated Crypto (SBC) CID 1.3.6.1.4.1.311.10.3.3</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>セット</td> <td>クリア</td> </tr> <tr> <td>Metaspac SBC - CID 2.16.840.1.113730.4.1</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>セット</td> <td>クリア</td> </tr> <tr> <td>TBD - CID 2.16.840.1.113731.8.1</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> </tbody> </table> <p>表 22: 拡張鍵用途の設定</p>		クラス3 インターナショナル・サーバ ID	OCSP レスポンダー	セキュア・サーバ ID	グローバル・サーバ ID	コード/オブジェクト・サイニング利用証明書	Criticality	FALSE	FALSE	FALSE	FALSE	FALSE	0 ServerAuth	クリア	クリア	セット	クリア	クリア	1 ClientAuth	クリア	セット	セット	クリア	クリア	2 CodeSigning	クリア	クリア	クリア	クリア	セット	3 EmailProtection	クリア	セット	クリア	クリア	クリア	4 ipsecEndSystem	クリア	クリア	クリア	クリア	クリア	5 ipsecTunnel	クリア	クリア	クリア	クリア	クリア	6 ipsecUser	クリア	クリア	クリア	クリア	クリア	7 TimeStamping	クリア	クリア	クリア	クリア	クリア	8 OCSP Signing	クリア	セット	クリア	クリア	クリア	Microsoft Server Gated Crypto (SBC) CID 1.3.6.1.4.1.311.10.3.3	クリア	クリア	クリア	セット	クリア	Metaspac SBC - CID 2.16.840.1.113730.4.1	セット	クリア	クリア	セット	クリア	TBD - CID 2.16.840.1.113731.8.1	セット	クリア	クリア	クリア	クリア	<table border="1"> <thead> <tr> <th></th> <th>クラス3 インターナショナル・サーバ ID</th> <th>OCSP レスポンダー</th> <th>セキュア・サーバ ID</th> <th>グローバル・サーバ ID</th> <th>コード/オブジェクト・サイニング利用証明書</th> </tr> </thead> <tbody> <tr> <td>Criticality</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> <td>FALSE</td> </tr> <tr> <td>0 ServerAuth</td> <td>セット</td> <td>クリア</td> <td>セット</td> <td>セット</td> <td>クリア</td> </tr> <tr> <td>1 ClientAuth</td> <td>セット</td> <td>クリア</td> <td>セット</td> <td>セット</td> <td>クリア</td> </tr> <tr> <td>2 CodeSigning</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>セット</td> </tr> <tr> <td>3 EmailProtection</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>4 ipsecEndSystem</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>5 ipsecTunnel</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>6 ipsecUser</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>7 TimeStamping</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>8 OCSP Signing</td> <td>クリア</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> <tr> <td>Microsoft Server Gated Crypto (SBC) CID 1.3.6.1.4.1.311.10.3.3</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>セット</td> <td>クリア</td> </tr> <tr> <td>Metaspac SBC - CID 2.16.840.1.113730.4.1</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>セット</td> <td>クリア</td> </tr> <tr> <td>TBD - CID 2.16.840.1.113731.8.1</td> <td>セット</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> <td>クリア</td> </tr> </tbody> </table> <p>表 22: 拡張鍵用途の設定</p>		クラス3 インターナショナル・サーバ ID	OCSP レスポンダー	セキュア・サーバ ID	グローバル・サーバ ID	コード/オブジェクト・サイニング利用証明書	Criticality	FALSE	FALSE	FALSE	FALSE	FALSE	0 ServerAuth	セット	クリア	セット	セット	クリア	1 ClientAuth	セット	クリア	セット	セット	クリア	2 CodeSigning	クリア	クリア	クリア	クリア	セット	3 EmailProtection	クリア	クリア	クリア	クリア	クリア	4 ipsecEndSystem	クリア	クリア	クリア	クリア	クリア	5 ipsecTunnel	クリア	クリア	クリア	クリア	クリア	6 ipsecUser	クリア	クリア	クリア	クリア	クリア	7 TimeStamping	クリア	クリア	クリア	クリア	クリア	8 OCSP Signing	クリア	セット	クリア	クリア	クリア	Microsoft Server Gated Crypto (SBC) CID 1.3.6.1.4.1.311.10.3.3	クリア	クリア	クリア	セット	クリア	Metaspac SBC - CID 2.16.840.1.113730.4.1	セット	クリア	クリア	セット	クリア	TBD - CID 2.16.840.1.113731.8.1	セット	クリア	クリア	クリア	クリア
	クラス3 インターナショナル・サーバ ID	OCSP レスポンダー	セキュア・サーバ ID	グローバル・サーバ ID	コード/オブジェクト・サイニング利用証明書																																																																																																																																																																					
Criticality	FALSE	FALSE	FALSE	FALSE	FALSE																																																																																																																																																																					
0 ServerAuth	クリア	クリア	セット	クリア	クリア																																																																																																																																																																					
1 ClientAuth	クリア	セット	セット	クリア	クリア																																																																																																																																																																					
2 CodeSigning	クリア	クリア	クリア	クリア	セット																																																																																																																																																																					
3 EmailProtection	クリア	セット	クリア	クリア	クリア																																																																																																																																																																					
4 ipsecEndSystem	クリア	クリア	クリア	クリア	クリア																																																																																																																																																																					
5 ipsecTunnel	クリア	クリア	クリア	クリア	クリア																																																																																																																																																																					
6 ipsecUser	クリア	クリア	クリア	クリア	クリア																																																																																																																																																																					
7 TimeStamping	クリア	クリア	クリア	クリア	クリア																																																																																																																																																																					
8 OCSP Signing	クリア	セット	クリア	クリア	クリア																																																																																																																																																																					
Microsoft Server Gated Crypto (SBC) CID 1.3.6.1.4.1.311.10.3.3	クリア	クリア	クリア	セット	クリア																																																																																																																																																																					
Metaspac SBC - CID 2.16.840.1.113730.4.1	セット	クリア	クリア	セット	クリア																																																																																																																																																																					
TBD - CID 2.16.840.1.113731.8.1	セット	クリア	クリア	クリア	クリア																																																																																																																																																																					
	クラス3 インターナショナル・サーバ ID	OCSP レスポンダー	セキュア・サーバ ID	グローバル・サーバ ID	コード/オブジェクト・サイニング利用証明書																																																																																																																																																																					
Criticality	FALSE	FALSE	FALSE	FALSE	FALSE																																																																																																																																																																					
0 ServerAuth	セット	クリア	セット	セット	クリア																																																																																																																																																																					
1 ClientAuth	セット	クリア	セット	セット	クリア																																																																																																																																																																					
2 CodeSigning	クリア	クリア	クリア	クリア	セット																																																																																																																																																																					
3 EmailProtection	クリア	クリア	クリア	クリア	クリア																																																																																																																																																																					
4 ipsecEndSystem	クリア	クリア	クリア	クリア	クリア																																																																																																																																																																					
5 ipsecTunnel	クリア	クリア	クリア	クリア	クリア																																																																																																																																																																					
6 ipsecUser	クリア	クリア	クリア	クリア	クリア																																																																																																																																																																					
7 TimeStamping	クリア	クリア	クリア	クリア	クリア																																																																																																																																																																					
8 OCSP Signing	クリア	セット	クリア	クリア	クリア																																																																																																																																																																					
Microsoft Server Gated Crypto (SBC) CID 1.3.6.1.4.1.311.10.3.3	クリア	クリア	クリア	セット	クリア																																																																																																																																																																					
Metaspac SBC - CID 2.16.840.1.113730.4.1	セット	クリア	クリア	セット	クリア																																																																																																																																																																					
TBD - CID 2.16.840.1.113731.8.1	セット	クリア	クリア	クリア	クリア																																																																																																																																																																					