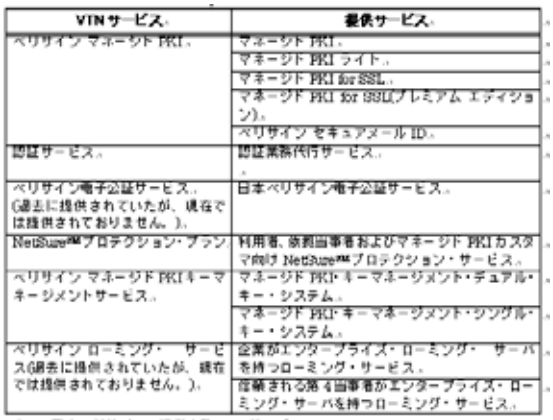
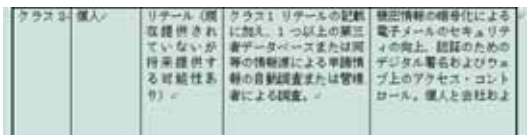
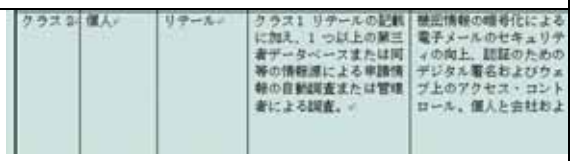
Section	現在の内容	改定案
全般	RFC2459、すなわち、1999 年 1 月のインターネットX.509公開鍵インフラストラクチャ証明書およびCRLプロファイルに従い定めている。	RFC3280、すなわち、2002 年 4 月のインターネットX.509公開鍵インフラストラクチャ証明書およびCRLプロファイルに従い定めている。
全般(サービス終了)		「ベリサイン電子公証サービス」、「ベリサイン ローミング・ サービス」に関して、「(過去に提供されていたが、現在では提供されておりません。)」を追記し、サービス提供の終了を記述
ベリサイン提供サービス一覧の記述を廃止	1.1.2 上記サービスは、日本ベリサインの定める契約に従う。表3は、日本ベリサインが提供するVTNサービスを要約したものである。	1.1.2 上記サービスは、日本ベリサインの定める契約に従う。表3は、日本ベリサインが提供するVTNサービスの一部である。
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  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Section 1.1(b)に規定されている。 1.1.1 CP§1.1.1 参照	1.1 表1  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Section 1.1に規定されている。 1.1.1 CP§1.1 参照

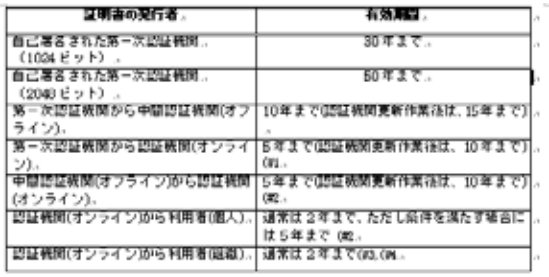
	 表 3 日本ベリサインの提供する VIN サービス	 表 3 日本ベリサインの提供する VIN サービス
	1.1.2.1 日本ベリサインの提供するベリサイン マネージドPKIは、日本ベリサインの企業カスタマが証明書を従業員、パートナー、サプライヤーおよび顧客、さらにサーバ、ルーターおよびファイアウォール等のデバイスに発行することのできる完全に統合されたPKIサービスである。日本ベリサインの提供するマネージドPKIサービスの詳細は、CP§1.1.2.1.1 に記述されている。日本ベリサインのサブドメインにおけるマネージドPKIのセキュリティ要件は、エンタープライズ・セキュリティ・ガイド（利用可能な場合）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。ベリサイン 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）。	1.1.2.1 日本ベリサインの提供するベリサイン マネージド PKI は、日本ベ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。日本ベ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。ベリサイン 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。

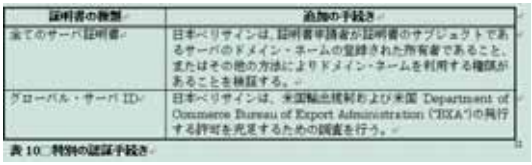
	1.1.2.1.2 日本ベリサインは、CP§1.1.2.1.2 に記載されるサービスセンターとプロセッシングセンターを運用する。これにより、日本ベリサインは、リテール証明書の場合、証明書申請を承認または拒絶することができ、マネージドPKI証明書の場合、プロセッシングセンターを利用しマネージドPKIカスタマに対しバックエンドの証明書ライフサイクル・サービスを提供することができる。サーバ証明書を提供するときは、日本ベリサイン・サービスセンターはVTN内でセキュア・サーバIDまたはグローバル・サーバIDを発行する米国ベリサイン認証機関の登録機関となる。日本ベリサイン・サービスセンターは、セキュア・サーバ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。	1.1.2.1.2 日本ベリサインは、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、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、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。

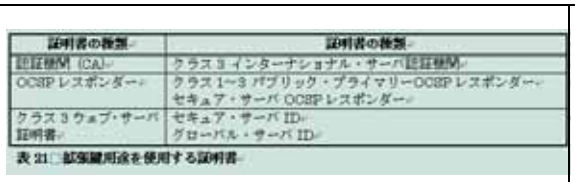
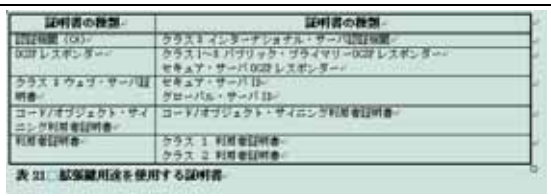
	1.1.2.2.1 日本ベリサインは、組織に対し、認証業務代行サービスを提供する。これらの詳細は、CP§1.1.2.2.1 に記述される。認証業務代行サービスにより、日本ベリサインは、カスタマの代わりに証明書申請者の実在性を確認する。	1.1.2.2.1 日本ベリサインは、組織に対し、認証業務代行サービスを提供する。認証業務代行サービスにより、日本ベリサインは、カスタマの代わりに証明書申請者の実在性を確認する。
	1.1.2.2.2 ベリサイン電子公証サービス 日本ベリサインは、CP§1.1.2.2.2 に規定するベリサイン電子公証サービスを提供する。このサービス提供の条件は、日本ベリサインとカスタマとの契約に従うものとする。	1.1. 2.2.2 ベ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おりません。) このサービス提供の条件は、日本ベリサインとカスタマとの契約がある場合にはそれに従うものとする。
	1.1.2.3.2 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	1.1.2.3.2 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。 1.3.1 CP§1.3.1で検討するように、米国ベリサインが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。米国ベリサインは、日本ベ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。 1.3.4 本CPSは、日本ベリサイン、カスタマ、リセラー、利用者および依拠当事者を含む、日本ベ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内の日本ベリサインのサブドメインおよびVTNを支える日本ベ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に記述されるクラス1～3の証明書の日本ベリサイン・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、CP§1.3.4.1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。	能する。 1.3.1 米国ベリサインが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。米国ベリサインは、日本ベ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。 1.3.4 本CPSは、日本ベリサイン、カスタマ、リセラー、利用者および依拠当事者を含む、日本ベ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内の日本ベリサインのサブドメインおよびVTNを支える日本ベ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に記述されるクラス1～3の証明書の日本ベリサイン・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、CP§1.4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。

	1.3.4.1 適切な用途については、CP§1.3.4.1および本CPS§1.1.1（表2）を参照。 2.2.1.1 日本ベリサインのNetSure℠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、CPの§1.1.2.2.3 および本CPSの§1.1.2.2.3 を参照されたい。 2.8 日本ベリサインは、CP§2.8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。	1.3.4.1 適切な用途については、CP§1.4および本CPS§1.1.1(表2)を参照。 2.2.1.1 日本ベリサインのNetSure℠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。 2.8 日本ベリサインは、CP§9.4.1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。
1.1.1 表2		
1.3.3 表4		
2.6.1 表7 誤記修正	https://www.verisign.co.jp/repository/index.html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拠当事者に利用可能。 また、directory.verisign.com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	directory.verisign.co.jp 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、 また、directory.verisign.com 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

3.1.9 誤記修正	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 証明書の証明者申請者を除く）	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 証明書の証明書申請者を除く）
3.1.9.2.2	（現在提供されていないが、将来提供する可能性あり） 日本ベリサインは、証明書申請中の確認すべき情報が日本ベ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、日本ベリサインは証明書申請を承認することができる。	日本ベリサインは、証明書申請中の確認すべき情報が日本ベ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、日本ベリサインは証明書申請を承認することができる。
4.6.2	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。 ・ クラス 1 証明書については 5 年間 ・ クラス 2 証明書については10 年間 ・ クラス 3 証明書については30 年間	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。 ・ クラス 1 証明書については 5 年の期間 ・ クラス 2 証明書については10 年 6 ヶ月の期間 ・ クラス 3 証明書については10 年 6 ヶ月の期間
5.3.1	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、3 年毎に繰返されるものとする。	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、5 年毎に繰返されるものとする。
6.3.2 表 18	 表 18: 証明書の有効期間	
6.3.2 表 18		(注釈の追記) (#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。

		(#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。 (#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２５ヶ月毎に再認証が必要となる。 (#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。
3.1.8.1.1 表 10		
4.4.11 誤記修正	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。	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。
4.4.11 誤記修正	https://www.verisign.co.jp/repository/ （個人の証明書について） および https://www.verisign.co.jp/repository/ （サーバおよび開発者の証明書について）	directory.verisign.co.jp の日本ベリサイン LDAP ディレクトリ・サーバ
6.1.9 表 16		
6.5 誤記修正	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。	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。

7.1.2.5 表 21		
7.1.2.5	その他の種類の証明書については、日本ベリサインは拡張鍵用途エクステンションを使用しない。	通常、その他の種類の証明書については、日本ベリサインは拡張鍵用途エクステンションを使用しない。
7.1.2.5