日本ベリサイン CPS3.3 差分表

VSJ CPS2.2			VSJ CPS3.3	
Section	Description		Section	Description
			その他	ベリサインインクの CPS バージョンとの整合をとるため、今回のバージョンを3．3とした。
全般	取消し		全般	用語見直し: 失効
全般	CPS の記述構成の変更: RFC 2527		全般	CPS の記述構成の変更: RFC 3647
6.3.2	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。		6.3.2	日本ベリサインは、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。
n/a			3.3.1 4.6.3	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
n/a			3.3.1 4.6.3	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、リニューアルされた証明書

			は自動的に発行される。
n/a		3.2.4	「確認を行わない申請情報」に関して追記
n/a		4.2.3	「証明書申請の処理時間」に関する項目を追加
n/a		4.5.2	証明書及び証明書を発行したチェーン内の全認証機関ステータスを評価する。証明書チェーン中の証明書が一つでも失効されている場合、依拠当事者は、エンドユーザ利用者の電子証明書によって、証明書チェーンの中の証明書が失効される前に署名された電子署名が信頼できるかどうかを調査する単独の責任がある。当該依拠は、依拠当事者の単独のリスクで行われるものとする。
n/a		4.12.1	鍵復旧における要求事項を追記
6.2.1	第一次認証機関、その他のルート認証機関並びに中間認証機関の鍵ペアの生成並びに認証機関の秘密鍵の保管に関し、米国ベリサインおよび日本ベリサインはFIPS140-1レベル3の認定を受けもしくは重要な点においてこの要求を満たすハードウェア暗号モジュールを使用している。他の認証機関に関しては、日本ベリサインは少なくともFIPS140-1レベル2の認定を受けたハードウェア暗号モジュールを使用している。	6.2.1	第一次認証機関、その他のルート認証機関及び中間認証機関のキー・ペアの生成並びに認証機関の秘密鍵の保管に関し、日本ベリサインはFIPS140-1レベル3の認定を受けもしくは重要な点においてこの要求を満たすハードウェア暗号モジュールを使用している。
n/a		7	証明書 エクステンションの

2.3.3	マネージドPKIカスタマは、利用者および依拠当事者に対する責任を合理的に負担することができるよう、自己の運用と義務の履行を維持するに足る十分な財源を有しなければならない。マネージドPKIカスタマは、更に、過失および怠慢に備えるため商業的に適切な水準の賠償責任保険を付保しなければならない。当該保険は、保険会社と締結するか、自家保険とするかを問わない。保険に関する上記の要求は、政府機関には適用されない。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。
2.2,1.3	また、日本ベリサインがある特定の証明書に関して負うことあるべき損害賠償額の上限は次のとおりである。

	basicConstraintのCriticality 見直し
9.2.1	エンタープライズ・カスタマは、過失及び怠慢によるリスクを担保するため、商業的に合理的な水準の賠償責任保険に加入することが推奨される。当該保険は、保険会社と締結するか、自家保険とするかを問わない。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。
9.8	また、利用者規約及び依拠当事者規約は、日本ベリサインがある特定の証明書に関して負うことあるべき損害賠償額の上限が次のとおりであることを含まなければならない。

	CPS2.2	
	(Eng)	(Jpn)
1	Introduction	はじめに
1.1	Overview	概要
1.2	Identification	文書の識別
1.3	Community and Applicability	コミュニティーおよび適用可能性
1.3.1	Certification Authorities	認証機関
1.3.2	Registration Authorities	登録機関
1.3.3	End Entities	エンド・エンティティ
1.3.4	Applicability	適用可能性
1.3.4.1	Suitable Applications	適切な用途
1.3.4.2	Restricted Applications	制限される用途
1.3.4.3	Prohibited Applications	禁止される用途
1.4	Contact Details	連絡先
1.4.1	Specification Administration Organization	管理部署
1.4.2	Contact Person	連絡窓口

	CPS3.3	
	(Eng)	(Jpn)
1	Introduction	はじめに
1.1	Overview	概要
1.2	Document name and Identification	文書名と識別
1.3	n/a	
1.3.1	Certification Authorities	認証機関
1.3.2	Registration Authorities	登録機関
1.3.3	End Entities	エンド・エンティティ
1.4	Certificate Usage	証明書の利用
1.4.1	Appropriate Certificate Usages	適切な証明書の利用
1.4.2	Prohibited Certificate Uses	禁止される証明書の用途
1.4.2	Prohibited Certificate Uses	禁止される証明書の用途
1.5	Policy Administration	ポリシー管理
1.5.1	Organization Administering the Document	本文書の管理部署
1.5.2	Contact Person	連絡先

1.4.3	Person Determining CPS Suitability for the Policy	本 CPS の適合性の決定	1.5.3	Person Determining CP Suitability for the Policy	CP への適合性の決定者
2	General Provisions	総則	n/a		
2.1	Obligations	義務	9.6	Representations and Warranties	表明と保証
2.1.1	CA Obligations	認証機関の義務	9.6.1	CA Representations and Warranties	認証機関の表明と保証
2.1.2	RA Obligations	登録機関の義務	9.6.2	RA Representations and Warranties	登録機関の表明と保証
2.1.3	Subscriber Obligations	利用者の義務	9.6.3	Subscriber Representations and Warranties	利用者の表明と保証
2.1.4	Relying Party Obligations	依拠当事者の義務	9.6.4	Relying Party Representations and Warranties	依拠当事者の表明と保証
2.1.5	Repository Obligations	リポジトリの義務	2.1	Repositories	リポジトリ
2.2	Liability	責任	9.6	Representations and Warranties	表明と保証
2.2.1	Certification Authority Liability	認証機関の責任	9.6.1	CA Representations and Warranties	認証機関の表明と保証
2.2.1.1	Certification Authority Warranties to Subscribers and Relying Parties	利用者および依拠当事者に対する認証機関の保証	9.6.1	CA Representations and Warranties	認証機関の表明と保証

2.2.1.2	Certification Authority Disclaimers of Warranties	認証機関の保証の制限	9.7	Disclaimers of Warranties	保証の否認
2.2.1.3	Certification Authority Limitations of Liability	認証機関の責任の制限	9.8	Limitations of Liability	責任の制限
2.2.1.4	Force Majeure	n/a	9.16.5	Force Majeure	不可抗力
2.2.2	Registration Authority Liability	登録機関の責任	9.6.2	RA Representations and Warranties	登録機関の表明と保証
2.2.3	Subscriber Liability	利用者の責任	9.6.3	Subscriber Representations and Warranties	利用者の表明と保証
2.2.3.1	Subscriber Warranties	利用者の保証	9.6.3	Subscriber Representations and Warranties	利用者の表明と保証
2.2.3.2	Private Key Compromise	秘密鍵の危殆化	5.7	Compromise and Disaster Recovery	危殆化及び災害からの復旧
2.2.4	Relying Party Liability	依拠当事者の責任	9.6.4	Relying Party Representations and Warranties	依拠当事者の表明と保証
2.3	Financial Responsibility	財政的責任	n/a		
2.3.1	Indemnification by Subscribers and Relying Parties	利用者および依拠当事者による補償	9.9	Indemnities	補償

2.3.1.1	Indemnification by Subscribers	利用者による補償	9.9.1	Indemnification by Subscribers	利用者による補償
2.3.1.2	Indemnification by Relying Parties	依拠当事者による補償	9.9.2	Indemnification by Relying Parties	依拠当事者による補償
2.3.2	Fiduciary Relationships	信認関係	9.7	Disclaimers of Warranties	保証の否認
2.3.3	Administrative Processes	管理手続	9.2.1	Insurance Coverage	保険
2.4	Interpretation and Enforcement	解釈と強制執行	n/a		
2.4.1	Governing Law	準拠法	9.14 9.15	Governing Law Compliance with Applicable Law	準拠法 法の遵守
2.4.2	Severability, Survival, Merger, Notice	分離可能性条項、残存規定条項、完全合意条項、通知条項	9.16.3	Severability	分離可能
2.4.3	Dispute Resolution Procedures	紛争解決手続	9.13	Dispute Resolution Provisions	紛争の解決
2.4.3.1	Disputes Among VSJ and Customers	日本ベリサインとカスタマとの間の紛争	9.13.1	Disputes among VeriSign, Affiliates, and Customers	サブドメインの参加者間の紛争
2.4.3.2	Disputes with End-User Subscribers or Relying Parties	日本ベリサインと利用者または依拠当事者との間の紛争	9.13.2	Disputes with End-User Subscribers or Relying Parties	利用者または依拠当事者との紛争
2.5	Fees	料金	9.1	Fees	料金

2.5.1	Certificate Issuance or Renewal Fees	証明書発行または更新の手数料	9.1.1	Certificate Issuance or Renewal Fees	証明書発行または更新の手数料
2.5.2	Certificate Access Fees	証明書のアクセス手数料	9.1.2	Certificate Access Fees	証明書のアクセス手数料
2.5.3	Revocation or Status Information Access Fees	取消しまたはステータス情報のアクセス手数料	9.1.3	Revocation or Status Information Access Fees	失効またはステータス情報のアクセス手数料
2.5.4	Fees for Other Services Such as Policy Information	ポリシー情報等の他のサービスの手数料	9.1.4	Fees for Other Services	他のサービスの手数料
2.5.5	Refund Policy	返金制度	9.1.5	Refund Policy	返金制度
2.6	Publication and Repository	公表およびリポジトリ	2	Publication and Repository Responsibilities	公表及びリポジトリに関する責任
2.6.1	Publication of CA Information	認証機関情報の公表	2.2	Publication of Certificate Information	証明書情報の公表
2.6.2	Frequency of Publication	公表の頻度	2.3	Time or Frequency of Publication	公表の頻度
2.6.3	Access Controls	アクセス・コントロール	2.4	Access Controls on Repositories	リポジトリへのアクセス制限
2.6.4	Repositories	リポジトリ	2.1	Repositories	リポジトリ
2.7	Compliance Audit	準拠性監査	8	Compliance Audit and Other Assessments	準拠性監査とその他の評価
2.7.1	Frequency of Entity Compliance Audit	準拠性監査の頻度	8.1	Frequency and Circumstances of	評価の頻度・状況

				Assessment	
2.7.2	Identity/ Qualifications of Auditor	監査人の資格	8.2	Identity/Qualifications of Assessor	評価人の身元と資格
2.7.3	Auditor's Relationship to Audited Party	監査人の監査対象の当事者との関係	8.3	Assessor's Relationship to Assessed Entity	評価人と被評価者との関係
2.7.4	Topics Covered by Audit	監査対象項目	8.4	Topics Covered by Assessment	評価対象項目
2.7.5	Actions Taken as a Result of Deficiency	欠陥の結果としてとられる措置	8.5	Actions Taken as a Result of Deficiency	欠陥の結果としてとられる処置
2.7.6	Communications of Results	結果の伝達	8.6	Communications of Results	結果の伝達
2.8	Confidentiality and Privacy	秘密性およびプライバシー	9.4.1	Privacy Plan	プライバシーポリシー
2.8.1	Types of Information to be Kept Confidential and Private	秘密に保持される情報の種類	9.3.1	Scope of Confidential Information	機密情報の範囲
2.8.2	Types of Information Not Considered Confidential or Private	秘密とみなされない情報の種類	9.3.2	Information Not Within the Scope of Confidential Information	機密とみなされない情報
2.8.3	Disclosure of Certificate Revocation/Suspension Information	証明書取消し・停止情報の開示	9.3.2	Information Not Within the Scope of Confidential Information	機密とみなされない情報

2.8.4	Release to Law Enforcement Officials	法執行機関への開示	9.4.6	Disclosure Pursuant to Judicial or Administrative Process	司法または行政手続きによる開示
2.8.5	Release as Part of Civil Discovery	民事事件の開示手続の一部としての開示	9.4.6	Disclosure Pursuant to Judicial or Administrative Process	司法または行政手続きによる開示
2.8.6	Disclosure Upon Owner's Request	保有者の要求による開示	9.4.6	Disclosure Pursuant to Judicial or Administrative Process	司法または行政手続きによる開示
2.8.7	Other Information Release Circumstances	他の情報開示に関する状況	9.4.7	Other Information Disclosure Circumstances	他の情報開示に関する状況
2.9	Intellectual Property Rights	知的財産権	9.5	Intellectual Property rights	知的財産権
2.9.1	Property Rights in Certificates and Revocation Information	証明書および取消し情報に関する財産権	9.5.1	Property Rights in Certificates and Revocation Information	証明書及び失効情報に関する財産権
2.9.2	Property Rights in the CP	本 CPS に関する財産権	9.5.2	Property Rights in the CPS	本 CPS に関する知的財産権
2.9.3	Property Rights in Names	名称に関する財産権	9.5.3	Property Rights in Names	名称に含まれる権利
2.9.4	Property Rights in Keys and Key Material	鍵および鍵のデータに関する財産権	9.5.4	Property Rights in Keys and Key Material	鍵及び鍵のデータに関する財産権

3	Identification and Authentication	確認と認証
3.1	Initial Registration	初期登録
3.1.1	Types of Names	識別名の種類
3.1.2	Need for Names to be Meaningful	意味のある名称であることの必要性
3.1.3	Rules for Interpreting Various Name Forms	識別名を解釈するための指針
3.1.4	Uniqueness of Names	唯一の名称
3.1.5	Name Claim Dispute Resolution Procedure	名称に関する紛争解決手続き
3.1.6	Recognition, Authentication, and Role of Trademarks	商標の認識、認証および役割
3.1.7	Method to Prove Possession of Private Key	秘密鍵を所有していることの証明方法
3.1.8	Authentication of Organization Identity	組織の同一性の確認
3.1.8.1	Authentication of the Identity of Organizational End-User Subscribers	組織向け証明書の利用者の同一性の確認

3	Identification and Authentication	確認と認証
n/a		
3.1.1	Type of Names	識別名の種類
3.1.2	Need for Names to be Meaningful	意味のある名称であることの必要性
3.1.4	Rules for Interpreting Various Name Forms	識別名を解釈するための指針
3.1.5	Uniqueness of Names	唯一の名称
3.1.6	Recognition, Authentication, and Role of Trademarks	商標の認識、認証及び役割
3.1.6	Recognition, Authentication, and Role of Trademarks	商標の認識、認証及び役割
3.2.1	Method to Prove Possession of Private Key	秘密鍵を所有していることの証明方法
3.2.2	Authentication of Organization identity	組織の実在性確認
3.2.2	Authentication of Organization identity	組織の実在性確認

3.1.8.1.1	Authentication for Retail Organizational Certificates	リテール組織向け証明書の確認	3.2.2	Authentication of Organization identity	組織の実在性確認
3.1.8.1.2	Authentication for Managed PKI for SSL or Managed PKI for SSL Premium Edition	マネージド PKI for SSL 又はマネージド PKI for SSL(プレミアム エディション)の認証	n/a		
3.1.8.1.3	Authentication for Class 3 Organizational ASB Certificates	クラス 3 組織向け ASB 証明書	n/a		
3.1.8.2	Authentication of the Identity of CAs and RAs	認証機関および登録機関の同一性の確認	3.2.2	Authentication of Organization identity	組織の実在性確認
3.1.9	Authentication of Individual Identity	個人の実在性の確認	3.2.3	Authentication of Individual Identity	個人の実在性確認
3.1.9.1	Class 1 Individual Certificates	クラス 1 個人向け証明書	3.2.3	Authentication of Individual Identity	個人の実在性確認
3.1.9.2	Class 2 Individual Certificates	クラス 2 個人向け証明書	3.2.3	Authentication of Individual Identity	個人の実在性確認
3.1.9.2.1	Class 2 Managed PKI Certificates	クラス 2 マネージド PKI 証明書	3.2.3	Authentication of Individual Identity	個人の実在性確認
3.1.9.2.2	Class 2 Retail Certificates	クラス 2 リテール証明書	3.2.3	Authentication of Individual Identity	個人の実在性確認
3.1.9.3	Class 3 Individual Certificates	クラス 3 個人向け証明書	3.2.3	Authentication of Individual Identity	個人の実在性確認

3.1.9.3.1	Class 3 Individual Certificates (Anticipated to offer)	クラス 3 個人向け証明書	3.2.3	Authentication of Individual Identity	個人の実在性確認
3.1.9.3.2	Class 3 Administrator Certificates	クラス 3 管理者用証明書	3.2.3	Authentication of Individual Identity	個人の実在性確認
3.2	Routine Rekey and Renewal	定期的なリキーおよびリニューアル	4.6.1	Circumstances for Certificate Renewal	証明書がリニューアルされる場合
3.2.1	Routine Rekey and Renewal for End-User Subscriber Certificates	利用者証明書用の定期的なリキーとリニューアル	3.3.1	Identification and Authentication for Routine Re-key	定期的なリキーに関する確認と認証
3.2.2	Routine Rekey and Renewal for CA Certificates	認証機関証明書の定期的なリキーとリニューアル	3.3.1	Identification and Authentication for Routine Re-key	定期的なリキーに関する確認と認証
3.3	Rekey After Revocation	取消し後のリキー	3.3.2	Identification and Authentication for Re-key After Revocation	証明書失効後のリキーに関する確認と認証
3.4	Revocation Request	取消し要求	3.4	Identification and Authentication for Revocation Request	失効申請に関する確認と認証
4	Operational Requirements	運用要件	4	Certificate Life-Cycle Operational Requirements	証明書のライフサイクルに対する運用要件
4.1	Certificate Application	証明書申請	4.1	Certificate Application	証明書申請

4.1.1	Certificate Applications for End-User Subscriber Certificates	利用者証明書の証明書申請	4.1.2.1	End-user Certificate Subscribers	エンドユーザ証明書の利用者
4.1.2	Certificate Applications for CA, RA, Infrastructure and Employee Certificates	認証機関、登録機関、インフラストラクチャおよび従業員証明書の証明書申請	4.1.2	Enrollment Process and Responsibilities	証明書申請手続
4.1.2.1	CA Certificates	認証機関証明書	4.1.2.2	CA and RA Certificates	認証機関と登録機関の証明書
4.1.2.2	RA Certificates	登録機関証明書	4.1.2.2	CA and RA Certificates	認証機関と登録機関の証明書
4.1.2.3	Infrastructure Certificates	インフラストラクチャ証明書	n/a		
4.1.2.4	VeriSign Employee Certificates	日本ベリサイン従業員証明書	n/a		
4.2	Certificate Issuance	証明書の発行	4.3	Certificate Issuance	証明書発行
4.2.1	Issuance of End-User Subscriber Certificates	利用者証明書の発行	4.3.1	CA Actions during Certificate Issuance	証明書の発行過程における認証機関の行為
4.2.2	Issuance of CA, RA and Infrastructure Certificates	認証機関、登録機関およびインフラストラクチャ証明書の発行	4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate	認証機関の利用者に対する証明書発行通知
4.3	Certificate Acceptance	証明書の受領	4.4	Certificate Acceptance	証明書の受領

4.4	Certificate Suspension and Revocation	証明書の効力の停止および取消し
4.4.1	Circumstances for Revocation	取消しの事由
4.4.1.1	Circumstances for Revoking End-User Subscriber Certificates	利用者証明書の取消し事由
4.4.1.2	Circumstances for Revoking CA, RA, or Infrastructure Certificates	認証機関、登録機関またはインフラストラクチャの証明書の取消し事由
4.4.2	Who Can Request Revocation	取消し要求をすることができる者
4.4.2.1	Who Can Request Revocation of an End-User Subscriber Certificate	利用者証明書の取消し要求をすることができる者
4.4.2.2	Who Can Request Revocation of a CA, RA, or Infrastructure Certificate	認証機関、登録機関またはインフラストラクチャ証明書の取消し要求をすることができる者
4.4.3	Procedure for Revocation Request	取消し要求の手続

4.9	Certificate Revocation and Suspension	証明書の失効及び効力の停止
4.9.1	Circumstances for Revocation	失効が行われる場合
4.9.1	Circumstances for Revocation	失効が行われる場合
4.9.3.2	Procedure for Requesting the Revocation of a CA or RA Certificate	認証機関もしくは登録機関証明書の失効申請手続
4.9.2	Who Can Request Revocation	証明書の失効を申請することができる者
4.9.2	Who Can Request Revocation	証明書の失効を申請することができる者
4.9.2	Who Can Request Revocation	証明書の失効を申請することができる者
4.9.3	Procedure for Revocation Request	失効申請要求の手続

4.4.3.1	Procedure for Requesting the Revocation of an End-User Subscriber Certificate	利用者証明書の取消し要求の手続	4.9.3.1	Procedure for Requesting the Revocation of an End-User Subscriber Certificate	エンドユーザ利用者の証明書の失効申請手続
4.4.3.2	Procedure for Requesting the Revocation of a CA or RA Certificate	認証機関または登録機関の証明書の取消し要求の手続	4.9.3.2	Procedure for Requesting the Revocation of a CA or RA Certificate	認証機関もしくは登録機関証明書の失効申請手続
4.4.4	Revocation Request Grace Period	取消し要求の猶予期間	4.9.4	Revocation Request Grace Period	失効申請の猶予期間
4.4.5	Circumstances for Suspension	効力の停止事由	4.9.13	Circumstances for Suspension	効力を停止する場合
4.4.6	Who Can Request Suspension	効力停止要求をすることができる者	4.9.14	Who Can Request Suspension	効力停止申請をすることができる者
4.4.7	Procedure for Suspension Request	効力停止要求の手続	4.9.15	Procedure for Suspension Request	効力停止申請の手続
4.4.8	Limits on Suspension Period	効力停止の制限	4.9.16	Limits on Suspension Period	効力停止の制限
4.4.9	CRL Issuance Frequency	証明書失効リスト(CRL)の発行頻度	4.9.7	CRL Issuance Frequency	CRL の発行頻度
4.4.10	Certificate Revocation List Checking Requirements	証明書失効リストのチェック要件	4.9.6	Revocation Checking Requirements for Relying Parties	依拠当事者に要求される CRL の調査

4.4.11	On-Line Revocation/Status Checking Availability	オンラインによる取消し／ステータス・チェックの利用可能性	4.9.9	On-Line Revocation/Status Checking Availability	利用可能なオンラインによる失効/ステータス調査
4.4.12	On-Line Revocation Checking Requirements	オンラインによる取消しチェック要件	4.9.10	On-Line Revocation Checking Requirements	オンラインによる失効調査要件
4.4.13	Other Forms of Revocation Advertisements Available	取消しの公示についての他の形式	4.9.11	Other Forms of Revocation Advertisements Available	利用可能な失効の公表についての他の形式
4.4.14	Checking Requirements for Other Forms of Revocation Advertisements	取消しの公示についての他の形式に関するチェック	n/a		
4.4.15	Special Requirements Regarding Key Compromise	鍵の危殆化に関する特別な要件	4.9.12	Special Requirements regarding Key Compromise	鍵の危殆化に関する特別な要件
4.5	Security Audit Procedures	セキュリティ監査手続	5.4	Audit Logging Procedures	監査記録の手続き
4.5.1	Types of Events Recorded	記録されるイベントの種類	5.4.1	Types of Events Recorded	記録されるイベントの種類
4.5.2	Frequency of Processing Log	記録を処理する頻度	5.4.2	Frequency of Processing Log	記録を処理する頻度
4.5.3	Retention Period for Audit Log	監査記録の保管	5.4.3	Retention Period for Audit Log	監査記録を保持する期間
4.5.4	Protection of Audit Log	監査記録の保護	5.4.4	Protection of Audit Log	監査記録の保護

4.5.5	Audit Log Backup Procedures	監査記録のバックアップ手続
4.5.6	Audit Collection System	監査集計システム
4.5.7	Notification to Event-Causing Subject	イベントを生ぜしめた主体に対する通知
4.5.8	Vulnerability Assessments	脆弱性の評価
4.6	Records Archival	記録の保管
4.6.1	Types of Events Recorded	記録されたイベントの種類
4.6.2	Retention Period for Archive	記録保管の期間
4.6.3	Protection of Archive	保管記録の保護
4.6.4	Archive Backup Procedures	保管記録のバックアップ手続
4.6.5	Requirements for Time-Stamping of Records	記録のタイム・スタンプに関する要件
4.6.6	Procedures to Obtain and Verify Archive Information	保管記録情報の取得および検証の手続
4.7	Key Changeover	鍵の切り替え

5.4.5	Audit Log Backup Procedures	監査記録のバックアップ手続
5.4.6	Audit Collection System (Internal vs. External)	監査ログ集計システム（内部 対 外部）
5.4.7	Notification to Event-Causing Subject	イベントを生ぜしめた Subject に対する通知
5.4.8	Vulnerability Assessments	脆弱性の評価
5.5	Records Archival	記録の保管
5.5.1	Types of Records Archived	保管される記録の種類
5.5.2	Retention Period for Archive	記録保管の期間
5.5.3	Protection of Archive	保管記録の保護
5.5.4	Archive Backup Procedures	保管記録のバックアップ手続き
5.5.5	Requirements for Time-Stamping of Records	記録のタイム・スタンプに関する要件
5.5.7	Procedures to Obtain and Verify Archive Information	保管記録情報の取得及び検証の手続
5.6	Key Changeover	鍵の切り替え

4.8	Disaster Recovery and Key Compromise	災害復旧および鍵の危殆化
4.8.1	Corruption of Computing Resources, Software, and/or Data	コンピュータのリソース、ソフトウェアおよびデータの変造
4.8.2	Disaster Recovery	災害復旧
4.8.3	Key Compromise	鍵の危殆化
4.9	CA Termination	認証機関の終了
5	Physical, Procedural, and Personnel Security Controls	物理的、手続的、人的セキュリティ管理
5.1	Physical Controls	物理的セキュリティ
5.1.1	Site Location and Construction	立地および建設
5.1.2	Physical Access	物理的アクセス
5.1.3	Power and Air Conditioning	電源および空調
5.1.4	Water Exposures	水による被害

5.7.1	Incident and Compromise Handling Procedures	事故及び危殆化の取扱手続
5.7.2	Computing Resources, Software, and/or Data Are Corrupted	コンピューターの資源、ソフトウェアまたはデータが破損した場合
5.7.4	Business Continuity Capabilities After a Disaster	災害後の事業継続能力
5.7.3	Entity Private Key Compromise Procedures	エンティティの秘密鍵が危殆化した場合の手続
5.8	CA or RA Termination	認証機関または登録機関の終了
5	Facility, Management, and Operational Controls	設備、管理及び運用統制
5.1	Physical Controls	物理的管理
5.1.1	Site Location and Construction	立地場所及び構造
5.1.2	Physical Access	物理的アクセス
5.1.3	Power and Air Conditioning	電源及び空調
5.1.4	Water Exposures	水による被害

5.1.5	Fire Prevention and Protection	火災予防
5.1.6	Media Storage	メディアの保管
5.1.7	Waste Disposal	廃棄物処理
5.1.8	Backup	バックアップ
5.2	Procedural Controls	手続上の管理
5.2.1	Trusted Roles	信頼される役割
5.2.2	Number of Persons Required Per Task	業務に必要な人員数
5.2.3	Identification and Authentication for Each Role	それぞれの任務に必要な身元の確認
5.3	Personnel Controls	要員管理
5.3.1	Background, Qualifications, Experience, and Clearance Requirements	経歴、資格、経験および許可要件
5.3.2	Background Check Procedures	経歴調査手続き
5.3.3	Training Requirements	トレーニング要件
5.3.4	Retraining Frequency and Requirements	再トレーニングの頻度および要件

5.1.5	Fire Prevention and Protection	火災予防及び保護対策
5.1.6	Media Storage	メディアの保管
5.1.7	Waste Disposal	廃棄物処理
5.1.8	Off-Site Backup	オフサイト・バックアップ
5.2	Procedural Controls	手続的管理
5.2.1	Trusted Roles	信頼される役割
5.2.2	Number of Persons Required per Task	職務ごとに必要とされる人数
5.2.3	Identification and Authentication for Each Role	それぞれの任務に必要な身元の確認
5.3	Personnel Controls	人事的管理
5.3.1	Qualifications, Experience, and Clearance Requirements	経歴、資格、経験及び許可要件
5.3.2	Background Check Procedures	経歴調査手続き
5.3.3	Training Requirements	トレーニング要件
5.3.4	Retraining Frequency and Requirements	再トレーニングの頻度及び要件

5.3.5	Job Rotation Frequency and Sequence	人事異動の頻度
5.3.6	Sanctions for Unauthorized Actions	無権限の行為に対する制裁
5.3.7	Contracting Personnel Requirements	請負事業者の要件
5.3.8	Documentation Supplied to Personnel	従業員に提供される資料
6	Technical Security Controls	技術的セキュリティ・コントロール
6.1	Key Pair Generation and Installation	鍵ペア生成およびインストレーション
6.1.1	Key Pair Generation	鍵ペア生成
6.1.2	Private Key Delivery to Entity	秘密鍵の受渡
6.1.3	Public Key Delivery to Certificate Issuer	公開鍵の証明書発行者への受渡
6.1.4	CA Public Key Delivery to Users	認証機関公開鍵のユーザへの受渡
6.1.5	Key Sizes	鍵のサイズ
6.1.6	Public Key Parameters Generation	公開鍵のパラメータの生成

5.3.5	Job Rotation Frequency and Sequence	人事異動の頻度及び順序
5.3.6	Sanctions for Unauthorized Actions	無権限の行為に対する制裁
5.3.7	Independent Contractor Requirements	請負事業者の要件
5.3.8	Documentation Supplied to Personnel	要員に提供される資料
6	Technical Security Controls	技術的セキュリティ・コントロール
6.1	Key Pair Generation and Installation	キー・ペア生成及びインストレーション
6.1.1	Key Pair Generation	キー・ペア生成
6.1.2	Private Key Delivery to Subscriber	秘密鍵の受渡
6.1.3	Public Key Delivery to Certificate Issuer	公開鍵の証明書発行者への受渡
6.1.4	CA Public Key Delivery to Relying Parties	認証機関公開鍵のユーザへの受渡
6.1.5	Key Sizes	鍵のサイズ
6.1.6	Public Key Parameters Generation and Quality Checking	公開鍵のパラメータの生成

6.1.7	Parameter Quality Checking	パラメータの品質のチェック
6.1.8	Hardware/Software Key Generation	ハードウェア・ソフトウェアの鍵生成
6.1.9	Key Usage Purposes	鍵用途目的
6.2	Private Key Protection	秘密鍵の保護
6.2.1	Standards for Cryptographic Modules	暗号モジュールの基準
6.2.2	Private Key (n out of m) Multi-Person Control	複数人による秘密鍵の管理
6.2.3	Private Key Escrow	秘密鍵の預託
6.2.4	Private Key Backup	秘密鍵のバックアップ
6.2.5	Private Key Archival	秘密鍵の保管
6.2.6	Private Key Entry into Cryptographic Module	秘密鍵の暗号モジュールへの収容

6.1.6	Public Key Parameters Generation and Quality Checking	公開鍵のパラメータの生成
6.1.1	Key Pair Generation	キー・ペア生成
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	鍵用途目的 (X.509 バージョン 3 鍵用途領域のとおり)
6.2	Private Key Protection and Cryptographic Module Engineering Controls	秘密鍵の保護
6.2.1	Cryptographic Module Standards and Controls	暗号モジュールの基準
6.2.2	Private Key (m out of n) Multi-Person Control	複数人による秘密鍵 (m out of n) の管理
6.2.3	Private Key Escrow	秘密鍵の預託
6.2.4	Private Key Backup	秘密鍵のバックアップ
6.2.5	Private Key Archival	秘密鍵の保管
6.2.6	Private Key Transfer Into or From a Cryptographic Module	秘密鍵の暗号化モジュールへの入出力

6.2.7	Method of Activating Private Key	秘密鍵の起動の方法
6.2.7.1	End-User Subscriber Private Keys	利用者の秘密鍵
6.2.7.1.1	Class 1 Certificates	クラス1証明書
6.2.7.1.2	Class 2 Certificates	クラス2証明書
6.2.7.1.3	Class 3 Certificates Other Than Administrator Certificates	管理者証明書を除くクラス3証明書
6.2.7.2	Administrators’ Private Keys	管理者の秘密鍵
6.2.7.2.1	Administrators	管理者
6.2.7.2.2	Managed PKI Administrators using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)	暗号モジュール(自動承認またはマネージド PKI キーマネージメントサービスとともに)を用いるマネージド PKI 管理者
6.2.7.3	Private Keys Held by VSJ	日本ベリサインが保有する秘密鍵

6.2.8	Method of Activating Private Key	秘密鍵の起動の方法
n/a		
6.2.8.1	Class 1 Certificates	Class 1 証明書
6.2.8.2	Class 2 Certificates	Class 2 証明書
6.2.8.3	Class 3 Certificates other than Administrator Certificates	Class 3 証明書(管理者を除く)
6.2.8.4	Administrators’ Private Keys (Class 3)	管理者の秘密鍵 (Class 3)
6.2.8.4	Administrators’ Private Keys (Class 3)	管理者の秘密鍵 (Class 3)
6.2.8.5	Enterprise RAs using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)	暗号モジュールを使用するエンタープライズ RA (自動承認またはキーマネージメントサービスを用いている場合)
6.2.8.6	Private Keys Held by Processing Centers (Class 1-3)	プロセッシング・センタに保管される秘密鍵 (Class 1-3)

6.2.8	Method of Deactivating Private Key	秘密鍵の非活性化の方法	6.2.9	Method of Deactivating Private Key	秘密鍵の非活性化の方法
6.2.9	Method of Destroying Private Key	秘密鍵の破壊の方法	6.2.10	Method of Destroying Private Key	秘密鍵の破壊の方法
6.3	Other Aspects of Key Pair Management	鍵ペアの管理に関する他の点	6.3	Other Aspects of Key Pair Management	キー・ペアの管理に関する他の点
6.3.1	Public Key Archival	公開鍵の保管	6.3.1	Public Key Archival	公開鍵の保管
6.3.2	Usage Periods for the Public and Private Keys	公開鍵および秘密鍵の使用期間	6.3.2	Certificate Operational Periods and Key Pair Usage Periods	証明書の運用期間及びキー・ペアの使用期間
6.4	Activation Data	起動データ	6.4	Activation Data	起動データ
6.4.1	Activation Data Generation and Installation	起動データの生成とインストレーション	6.4.1	Activation Data Generation and Installation	起動データの生成とインストレーション
6.4.2	Activation Data Protection	起動データの保護	6.4.2	Activation Data Protection	起動データの保護
6.4.3	Other Aspects of Activation Data	起動データに関する他の点	n/a		
6.5	Computer Security Controls	コンピュータ・セキュリティ管理	6.5	Computer Security Controls	コンピュータ・セキュリティ管理
6.5.1	Specific Computer Security Technical Requirements	特定のコンピュータ・セキュリティの技術的要件	6.5.1	Specific Computer Security Technical Requirements	特定のコンピュータ・セキュリティの技術的要件

6.5.2	Computer Security Rating	コンピュータ・セキュリティの評価
6.6	Life Cycle Technical Controls	ライフサイクル技術管理
6.6.1	System Development Controls	システム開発管理
6.6.2	Security Management Controls	セキュリティ管理
6.6.3	Life Cycle Security Ratings	ライフサイクル・セキュリティ評価
6.7	Network Security Controls	ネットワーク・セキュリティ管理
6.8	Cryptographic Module Engineering Controls	暗号モジュール・エンジニアリング管理
7	Certificate and CRL Profile	証明書および CRL の概略
7.1	Certificate Profile	証明書の概略
7.1.1	Version Number(s)	バージョン・ナンバー
7.1.2	Certificate Extensions	証明書エクステンション
7.1.2.1	Key Usage	鍵用途 (Key Usage)
7.1.2.2	Certificate Policies Extension	証明書ポリシー (Certificate Policies)

6.5.2	Computer Security Rating	コンピュータ・セキュリティの評価
6.6	Life Cycle Technical Controls	ライフサイクル技術管理
6.6.1	System Development Controls	システム開発管理
6.6.2	Security Management Controls	セキュリティ管理
6.6.3	Life Cycle Security Controls	ライフサイクル・セキュリティ
6.7	Network Security Controls	ネットワーク・セキュリティ管理
6.2.1	Cryptographic Module Standards and Controls	暗号モジュールの基準
7	Certificate, CRL, and OCSP Profiles	証明書、CRL 及び OCSP のプロファイル
7.1	Certificate Profile	証明書のプロファイル
7.1.1	Version Number(s)	バージョン番号
7.1.2	Certificate Extensions	証明書エクステンション
7.1.2.1	Key Usage	Key Usage
7.1.2.2	Certificate Policies Extension	Certificate Policies エクステンション

7.1.2.3	Subject Alternative Names	サブジェクト代替名（Subject Alternative Names）
7.1.2.4	Basic Constraints	基本制約（Basic Constraints）
7.1.2.5	Extended Key Usage	拡張鍵用途（Extended Key Usage）
7.1.2.6	CRL Distribution Points	CRL 配布点（CRL Distribution Points）
7.1.2.7	Authority Key Identifier	認証局鍵識別子（Authority Key Identifier）
7.1.2.8	Subject Key Identifier	サブジェクト鍵識別子
7.1.3	Algorithm Object Identifiers	アルゴリズム・オブジェクト識別子（Algorithm Object Identifiers）
7.1.4	Name Forms	名称形式（Name Forms）
7.1.5	Name Constraints	名称制約（Name Constraints）
7.1.6	Certificate Policy Object Identifier	証明書ポリシー・オブジェクト識別子（Certificate Policy Object Identifier）
7.1.7	Usage of Policy Constraints Extension	ポリシー制約利用エクステンション（Usage of

7.1.2.3	Subject Alternative Names	Subject Alternative Names
7.1.2.4	Basic Constraints	Basic Constraints
7.1.2.5	Extended Key Usage	Extended Key Usage
7.1.2.6	CRL Distribution Points	CRL Distribution Points
7.1.2.7	Authority Key Identifier	Authority Key Identifier
7.1.2.8	Subject Key Identifier	Subject Key Identifier
7.1.3	Algorithm Object Identifiers	アルゴリズムオブジェクト識別子
7.1.4	Name Forms	名前の形式
7.1.5	Name Constraints	名前制約
7.1.6	Certificate Policy Object Identifier	証明書ポリシー・オブジェクト識別子
7.1.7	Usage of Policy Constraints Extension	ポリシー制約エクステンションの使用

		Policy Constraints Extension)			
7.1.8	Policy Qualifiers Syntax and Semantics	ポリシー修飾子の記載と意味 (Policy Qualifiers Syntax and Semantics)	7.1.8	Policy Qualifiers Syntax and Semantics	ポリシー修飾子の構文及び意味
7.1.9	Processing Semantics for the Critical Certificate Policy Extension	クリティカルな証明書ポリシー・エクステンションの解釈	7.1.9	Processing Semantics for the Critical Certificate Policies Extension	クリティカルな Certificate Policies エクステンションに対する解釈方法
7.2	CRL Profile	CRL の概要	7.2	CRL Profile	CRL のプロファイル
7.2.1	Version Number(s)	バージョン・ナンバー (Version Number(s))	7.2.1	Version Number(s)	バージョン番号
7.2.2	CRL and CRL Entry Extensions	CRL および CRL エントリー・エクステンション (CRL and CRL Entry Extensions)	7.2.2	CRL and CRL Entry Extensions	CRL 及び証明書失効リストエントリ・エクステンション
8	Specification Administration	仕様管理	9.12	Amendments	改訂
8.1	Specification Change Procedures	仕様変更手続	9.12.1	Procedure for Amendment	改訂手続き
8.1.1	Items that Can Change Without Notification	通知なしに変更することができる事項	9.12.2	Notification Mechanism and Period	通知方法と期間

8.1.2	Items that Can Change with Notification	通知により変更することができる事項
8.1.2.1	List of Items	項目のリスト
8.1.2.2	Notification Mechanism	通知の方法
8.1.2.3	Comment Period	コメント期間
8.1.2.4	Mechanism to Handle Comments	コメントを取り扱う仕組み
8.1.3	Changes Requiring Changes in the Certificate Policy OID or CPS Pointer	CP のオブジェクト識別子または CPS ポインタの変更を要する変更
8.2	Publication and Notification Policies	公表および通知に関するポリシー
8.2.1	Items Not Published in the CPS	本 CPS に公表されない項目
8.2.2	Distribution of the CPS	本 CPS の配布
8.3	CPS Approval Procedures	本 CPS の承認手続
9	Definitions	定義

9.12.2	Notification Mechanism and Period	通知方法と期間
9.12.2	Notification Mechanism and Period	通知方法と期間
9.12.2	Notification Mechanism and Period	通知方法と期間
9.12.2.1	Comment Period	コメント期間
9.12.2.2	Mechanism to Handle Comments	コメントの取扱
9.12.3	Circumstances under Which OID Must be Changed	OID の変更が必要な場合
9.12	Amendments	改定
9.12	Amendments	改定
9.12	Amendments	改定
1.5.4	CPS Approval Procedure	承認手続き
Appendix A.	Table of Acronyms and definitions	略語・定義表