GlobalSign Certificate Policy
(証明書ポリシー)

本書は、GlobalSign Certificate Policy を日本語に翻訳したものであり、言語の違いにより、原文の意味合いを完全に訳することができない場合があります。英語の原本と本書の間で、解釈に不一致がある場合は、英語の原本が優先されます。

Date: September 25, 2019

Version: v.6.2

Legal-JP

電子署名者 : Legal-JP
日付 : 2020.04.20 17:25:05 +09'00'

目次

文書変更履歴

Version	Release Date	Author(s)	Status & Description
V4.0	22/03/12	Steve Roylance	Administrative update – Inclusion of additional WebTrust 2.0 and CA/BForum Baseline Requirements for issuance of SSL Certificates.
V4.1	29/03/12	Lila Kee	Addition of support for NAESB.
V4.2	07/06/12	Steve Roylance	Additional CA/BForum Baseline Requirements support
V4.3	01/07/12	Steve Roylance	Additional CA/BForum Baseline Requirements
V4.4	15/03/13	Giichi Ishii Lila Kee	Extended validity period of PersonalSign, Administrative updates. Modification to NAESB Certificates incorporating WEQ-012 v 3.0 updates
V4.5	31/03/13	Giichi Ishii	Statement of compliance to CA/Browser Forum Baseline Requirements, EPKI specification update
V4.6	07/03/14	Carolyn Oldenburg	Administrative updates/clarifications Modified provisions to ensure compliance with CA/Browser Forum Baseline Requirements
V4.7	25/06/14	Giichi Ishii	Modified availability requirement and maximum process time for revocation Administrative update/clarifications
V4.8	02/09/14	Steve Roylance	Modifications to enhance the description of domain validation processes, highlighted by public review.
V4.9	05/03/15	Carolyn Oldenburg Steve Roylance Giichi Ishii	Modified maximum validity period of Code Signing certificate GlobalSign's new R6 root and readability enhancements to cover new AATL offerings
V5.0	15/08/15	Steve Roylance	Policy OIDs and Publication of all of GlobalSign's Non Constrained Subordinate CAs
V5.1	02/05/16	Giichi Ishii Lila Kee	Annual Review Modified NAESB EIR requirements to reflect non WEQ energy participants requirements
V5.2	16/06/16	Steve Roylance	Adding Root R7 and R8 Certificates
V5.3	11/08/16	Giichi Ishii	Adding Test CA OID Reflected changes from CABF Ballot 173 Clarification on Certificate Transparency
V5.4	02/02/17	Giichi Ishii	Removal of Root R2 & R4; addition of code signing minimum requirements
V5.5	07/08/17	Giichi Ishii Carolyn Oldenburg Lila Kee Doug Beattie	Updates for AATL Digital Signing Service Added CAA record checking requirement Annual update/review to fix bugs
V5.6	14/12/17	Giichi Ishii Carolyn Oldenburg Lila Kee Doug Beattie Simon Labram	Updates related to Annual BR Self Assessment
V5.7	03/04/18	Doug Beattie	Max SSL validity set to 825 days Specified that GlobalSign no longer generates keys for SSL certificates

		Lila Kee	Updates for NAESB identify requirements
V5.8	06/15/18		Updates for Qualified Certificates
V5.9	09/28/2018	Giichi Ishii Arvid Vermote Doug Beattie Carolyn Oldenburg	Updates to revocation timelines in accordance with CABF Ballot SC6 Made a variety of definition/acronym updates to comply with 360 Browser root policy requirements
V6	03/12/2019	Arvid Vermote Paul Brown Jun Hosoi Doug Beattie Carolyn Oldenburg	Updated roles requiring separation of duties Added new ICAs for AATL and Timestamping Added new Email Domain Validation methods and definitions Added new Phone Domain Validation methods and definitions Added new IoT policy OIDs
V6.1	05/30/2019	Arvid Vermote Paul Brown Jun Hosoi Doug Beattie Carolyn Oldenburg	Added new GlobalSign R46/E46 Root Certificates Added new Private Client Certificate Policy OID Support for Qualified Time Stamping and Qualified Web Authentication Certificates Changed “re-key” definition to match WebTrust
V6.2	09/25/2019	Arvid Vermote Paul Brown Jun Hosoi Doug Beattie Carolyn Oldenburg	Removed reference to NAESB High Assurance certificates Removed “any other” method for IP Address approval

前提確認事項

本 GlobalSign CP は、以下に準拠する：

- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- North American Energy Standards Board (NAESB) Accreditation Requirements for Authorized Certificate Authorities

本 GlobalSign CP は、現時点における以下の外部要求事項に準拠する：

- AICPA/CICA, WebTrust 2.1 Program for Certification Authorities
- AICPA/CICA, WebTrust for Certification Authorities – Extended Validation Audit Criteria
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates
- CA/B Forum Network and Certificate System Security Requirements
- CA/B Forum EV Code Signing Certificate Guidelines
- Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.
- Browsers' Root programs

本文書及び上記外部要求の間に不一致があった場合、外部要求事項が本文書に優先して適用される。

1.0　はじめに

本証明書ポリシー(以下、「本 CP」という)は、GlobalSign nv/sa が提供する製品及びサービスに適用する。本 CP は、電子証明書の発行と、証明書の有効性チェックサービスを含むライフサイクル管理を主に取り扱う。また、GlobalSign nv/sa は、timestamping 等の追加サービスも提供する。本 CP は、1.5 項「ポリシー管理」に規定するとおり、適宜更新される。本 CP の最新版は GlobalSign グループ会社のリポジトリ(https://www.globalsign.com/repository)に公開される。(依拠当事者及び利用者に対し本 CP の理解を補助するために、本 CP の翻訳が提供されることがある。但し、言語によって内容の不一致がある場合、英語版が適用・引用される)

CP は、「共通のセキュリティ要件を持つ特定の集団及び/又はアプリケーションのクラスへの電子証明書の適用範囲を示す、一連の規則」である。本 CP は 2003 年 11 月に Internet Engineering Task Force(以下、「IETF」という)が発行した RFC 3647 に定められた構成に従って記述する(RFC 3647 の発行に伴い RFC 2527 は廃止されている)。この RFC は、電子署名と証明書の管理における標準的な業務手続きについて記述した公式の手引きである。本 CP において、章・節などは RFC 3647 の構成に準拠して設けているが、そこで扱うべき内容が GlobalSign nv/sa のサービスでは実装されていない事項に関するものである場合には、「規定なし」と記述している。付加的な情報を記載する必要がある場合には、標準的な構成に小項目を加えてそこに記述している。RFC 3647 の書式に合わせることで、他のサードパーティ認証局との比較照合を可能にし、相互運用性を高める。GlobalSign は、www.cabforum.org.に公開されている「Publicly-Trusted Certificates」の中にある発行と管理の規定に関して、CA ブラウザフォーラム（以下「CA/B Forum」という）の Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (以下「Baseline Requirements」という), the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (以下「EV ガイドライン」という), CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates (以下「EV Code Signing ガイドライン」という)の最新版及び、https://aka.ms/csbr に公開されている Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (以下「Code Signing Minimum Requirements」という)に準拠するものとする。本 CP と Baseline Requirements の最新版との間に不一致があった場合は、Baseline Requirements を優先するものとする。本 CP が準拠するその他の規格は前提確認事項の項に記載されている。

本 CP は、以下に限らないが、証明書のライフサイクル管理のための業界内のベストプラクティスを充足するために要求される、技術的要件、セキュリティ手順、要員及び訓練の必要性といった、ポリシー及び手続きの分野に対応する。ルート証明書は、ルート証明書自身を管理する同じエンティティによって直接的に制御されるよう想定されているか、制御されないかもしれない 1 つ以上の下位 CA の作成を通して証明書階層を管理するために使われる。

本 CP は最終版であり、GlobalSign nv/sa (所在地：Martelarenlaan 38, 3010 Leuven、VAT 登録番号：BE0459.134.256、商業登記番号：BE 0.459.134.256 RPR Leuven の会社法人。以下、「GlobalSign」という)と、本 CP に基づいて認証局が提供する認証サービスを利用する利用者及び又は、依拠する又は依拠しようとする依拠当事者を拘束する。

1.1　概要

本 CP は、GlobalSign が、自身のシステムから直接又は Trusted Root™ (自己署名のルート証明書及び鍵ペアを含む。以前の呼称は「Root Sign」)プログラムから間接的に発行する全証明書階層に適用される。
本 CP の目的は、ルート証明書及び発行 CA の管理に関し GlobalSign が採用する管理手続きを説明し、上述の業界標準の要件に準拠して電子証明書が発行されていることを証することである。さらに、eIDAS 規則(規則(EU)N910/2014)は、権限の認証又は否認防止の目的で使用される電子署名の認知を定めているが、この点に関し、GlobalSign はサービスの提供にあたり、本法の該当条項の射程の範囲内で運営を行っている。
本 CP は、本 CP に基づき発行される証明書のライフサイクルに関わる全ての主体の目的、役割、責任及び手続きを定める。いわば、「遵守すべきこと」を記述することで、商品サービスに対する運営上の規則の枠組みを設定している。

GlobalSign の Certificate Practice Statement(以下「本 CPS」という)は本 CP を補完し、「認証局がどのように CP に準拠するか」記述する。CPS は、エンドユーザに、発行 CA (すなわち、利用者に証明書を提供する事業体)がそのような証明書を作成し管理する際に使用するプロセス、手順、及び全般的な状況の概要を提供する。同様に、GlobalSign Trusted Root の利用者自身が発行 CA となる場合、その利用者は提供する製品及びサービスに適用する CPS を独自に維持・管理する。

GlobalSign は、本 CP 及び CPS に加え、以下のような問題に対処するポリシーを別途文書化して保持する。

- 事業継続計画・災害復旧計画
- セキュリティポリシー
- 人的ポリシー
- 鍵管理ポリシー
- 登録手続き

さらに、他の関連文書には、以下のものが含まれる：

- GlobalSign から提供される保障に関する事項を取り扱う GlobalSign ワランティーポリシー
- 個人情報保護に関する GlobalSign プライバシーポリシー
- GlobalSign のルート証明書の信頼対象を取り扱う GlobalSign CP

適用可能な GlobalSign の全てのポリシーは権限ある第三者から監査を受けており、これらのポリシーは WebTrust シールを付与した GlobalSign のウェブサイトで公開されている。追加情報は要求を受けて提供する。

本 CP に基づき管理される GlobalSign ルート CA 証明書の名称は以下の通り：

GlobalSign Public Root CA Certificates:

- GlobalSign Root CA – R1 with serial number 040000000001154b5ac394
- GlobalSign Root CA – R3 with serial number 04000000000121585308a2
- GlobalSign Root CA – R5 with serial number 605949e0262ebb55f90a778a71f94ad86c
- GlobalSign Root CA – R6 with serial number 45e6bb038333c3856548e6ff4551
- GlobalSign Root CA – R7 with serial number 481b6a06a6233b90a629e6d722d5
- GlobalSign Root CA – R8 with serial number 481b6a09f4f960713afe81cc86dd
- GlobalSign Root CA – R46 with serial number 11d2bbb9d723189e405f0a9d2dd0df2567d1
- GlobalSign Root CA – E46 with serial number 11d2bbba336ed4bce62468c50d841d98e843

Non-public Root Certificates:

- GlobalSign Non-Public Root CA – R1 with serial number 467437789376ad2301cdf9ba9e1d
- GlobalSign Non-Public Root CA – R3 with serial number 4674377c0fba34f6f1c3dcb75d3f

GlobalSign は、これらのルート証明書が、電子証明書に対応可能なハードウェア／ソフトウェアプラットフォームへ搭載されるよう、積極的に働きかけを行っている。GlobalSign は、可能な場合にはプラットフォームプロバイダと契約を締結し、ルート証明書の効果的なライフサイクル管理を行っている。同時に、GlobalSign はプラットフォームプロバイダが自己の裁量により、契約上の義務を負わずに当該ルート証明書を搭載することも積極的に奨励している。尚、GlobalSign Root CA - R2 及び GlobalSign Root CA - R4 は GlobalSign nv/sa の所有から外れた。

Trusted Root とは GlobalSign のサービスで、第三者が保有する CA を中間 CA を介して GlobalSign ルート証明書の 1 つにチェーンできるようにすることである。

- GlobalSign Trusted Platform Module Root CA with s/n 040000000001201909l9AE
- GlobalSign Trusted Platform Module ECC Root CA with s/n 45dc9c8c1515db59d0464b9d79e9[1]

Trusted Root TPM とは、第三者が運用する発行 CA を上記の GlobalSign Trusted Platform Module のルート CA 証明書の 1 つにチェーンさせるという GlobalSign のサービスである。

電子証明書により、エンティティは電子的取引の際、他の取引参加者に自己の身元を証明したり、データにデジタル署名をしたりすることができる。認証局は、電子証明書により利用者及びその秘密鍵の関連性を認証する。Trusted Root は、自身の発行 CA の証明書階層への信頼向上及び、ウェブブラウザといった第三者のアプリケーションが持つより高度な機能性を提供することを目的とし、GlobalSign の証明書階層に入れこまれる。Trusted Root 発行 CA の義務とは、常に GlobalSign のサービスの利点を活用していくことである。

---

[1] *Collectively Root R1, R3, R5, R6, R7, R8, R46, E46 and the TPM/TPM ECC Roots are referred to as the GlobalSign CA Root Certificates*

電子証明書を受領するプロセスには、ユーザの本人確認、名前確認、 認証、登録などと共に、電子証明書の発行、失効、有効期限満了といった証明書を管理するための手続きが含まれる。本ポリシーに従い、GlobalSign が、証明書の発行を通じて利用者が使用する公開鍵を限定することによって、証明書のユーザが本人であることを証明する。
このインスタンスのエンティティには、エンドユーザ又は他の認証局が含まれる可能性がある。GlobalSign が提供する電子証明書は、否認防止、暗号化、認証に使用 することができる。しかしながら、ワランティーポリシー又は証明書が使用されるアプリケーションの制約を受けて、証明書を特定のビジネス、契約、取引のレベルでのみ使用するよう限定されることがある。

GlobalSign は、本 CP に関するコメントを、*Policy Adminstration*1.5 項に記載されている住所宛に受理する。

1.1.1 Trusted Root 発行 CA への追加要求事項

本 CP では、当該サービスの利用を許諾された発行認証局向けの TrustedRoot サービスについても触れる。これは、GlobalSign が TrustedRoot のブランド名の下に提供する認証局の証明書チェーニングプログラムを通じ、発行認証局の中間証明書を GlobalSign 階層にチェーンするサービスである。TrustedRoot CA 証明書の取扱については以下のような特徴がある：

- 契約・監査・ポリシーなどによる要求事項を満たすサードパーティが運用する発行認証局に対し GlobalSign が発行する。
- 企業内に設立された認証局がそのブランドの下にその発行対象者に向け SSL 証明書・S/MIME 証明書を発行する目的においてのみ、発行する。
- キーエスクロー（鍵の第三者預託）証明書、OCSP により署名された証明書などに限らず、証明書のライフサイクル管理を提供するために必要なその他のタイプの証明書を発行することが許可される場合がある。
- Code Signing 証明書を発行する目的では使用することができない。
- サードパーティ、GlobalSign それぞれの階層を保護するため、SSL、S/MIME の目的において特定の領域内で使用するよう制限されている。

GlobalSign はチェーンサービスが MITM (Man in the Middle)による SSL/TLS に対するディープ・パケット・インスペクションに使用されることを明確に禁止する。

1.2 文書名称と本人確認

本文書は GlobalSign 証明書ポリシーである。 .

GlobalSign nv/sa のオブジェクト識別子（以下、「OID」という。）は、ISO (1)、識別された組織 (3)、DoD (6)、インターネット (1)、民間 (4)、企業 (1)、GlobalSign nv/sa (4146)、すなわち 1.3.6.1.4.1.4146 である。GlobalSign は本 CP が対象とするさまざまな証明書、文書に対し、次の OID を付与する：

Extended Validation	
1.3.6.1.4.1.4146.1.1	Extended Validation Certificates Policy – SSL
1.3.6.1.4.1.4146.1.1.1	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC)
1.3.6.1.4.1.4146.1.1.2	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC) – PSD2
1.3.6.1.4.1.4146.1.2	Extended Validation Certificates Policy – Code Signing
Domain Validation	
1.3.6.1.4.1.4146.1.10	Domain Validation Certificates Policy
1.3.6.1.4.1.4146.1.10.10	Domain Validation Certificates Policy – AlphaSSL
Organization Validation	
1.3.6.1.4.1.4146.1.20	Organization Validation Certificates Policy
Intranet Validation	
1.3.6.1.4.1.4146.1.25	IntranetSSL Validation Certificates Policy
Timestamping	
1.3.6.1.4.1.4146.1.30	Timestamping Certificates Policy
1.3.6.1.4.1.4146.1.31	Timestamping Certificates Policy – AATL
1.3.6.1.4.1.4146.1.32	Time Stamping Certificate Policy – Certificates for Qualified Time Stamping (QTS) under eIDAS regulation

Client Certificates

1.3.6.1.4.1.4146.1.40	Client Certificates Policy (Generic)
1.3.6.1.4.1.4146.1.40.10	Client Certificates Policy (EPKI – Enterprise PKI)
1.3.6.1.4.1.4146.1.40.20	Client Certificates Policy (JCAN – Japan CA Network)
1.3.6.1.4.1.4146.1.40.30	Client Certificates Policy (AATL)
1.3.6.1.4.1.4146.1.40.40	Client Certificates Policy (EPKI for private CAs)
1.3.6.1.4.1.4146.1.40.50	Client Certificates Policy (Private Hierarchy)

Qualified Certificates under eIDAS

1.3.6.1.4.1.4146.1.40.35	eIDAS Qualified Certificates (Generic)
1.3.6.1.4.1.4146.1.40.35.1	Qualified Certificates for Electronic Seals (Legal Persons)
1.3.6.1.4.1.4146.1.40.35.1.1	Qualified Certificates for Electronic Seals (Legal Persons) - PSD2
1.3.6.1.4.1.4146.1.40.35.2	Qualified Certificates for Electronic Signatures (Natural Persons)

これらの識別子に加えて、itu-t(0) identified-organization(4) etsi(0) other-certificate-policy(2042) policy-identifiers(1) ncpplus(2) に準拠する全ての証明書は、以下の追加識別子を含む：

0.4.0.194112.1.2	QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD (maps to 1.3.6.1.4.1.4146.1.40.35.2)
0.4.0.194112.1.3	QCP-l-qscd: certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD (maps to 1.3.6.1.4.1.4146.1.40.35.1)

Code Signing

2.23.140.1.4.1	Code Signing Minimum Requirements Policy
1.3.6.1.4.1.4146.1.50	Code Signing Certificates Policy

GlobalSign が発行した当該 OID を含む証明書は、Code Signing Minimum Requirements に従って発行・管理される。

CA Chaining and Cross Signing

1.3.6.1.4.1.4146.1.60	CA Chaining Policy – Trusted Root and Hosted Root
1.3.6.1.4.1.4146.1.60.1	CA Chaining Policy – Trusted Root (Baseline Requirements Compatible)

Others

1.3.6.1.4.1.4146.1.26	Test Certificate Policy (Should not be trusted)
1.3.6.1.4.1.4146.1.70	High Volume CA Policy
1.3.6.1.4.1.4146.1.80	Retail Industry Electronic Data Interchange Client Certificate Policy
1.3.6.1.4.1.4146.1.81	Retail Industry Electronic Data Interchange Server Certificate Policy
1.3.6.1.4.1.4146.1.90	Trusted Root TPM Policy
1.3.6.1.4.1.4146.1.95	Online Certificate Status Protocol Policy

Internet of Things (IoT)

1.3.6.1.4.1.4146.1.100	Internet of Things Device Certificates Policy

これらの識別子に加え、NAESB Business Practice Standards を遵守する全ての証明書は、以下の追加識別子の 1 つを含む。

2.16.840.1.114505.1.12.1.2	NAESB Rudimentary Assurance
2.16.840.1.114505.1.12.2.2	NAESB Basic Assurance
2.16.840.1.114505.1.12.3.2	NAESB Medium Assurance

これらの識別子に加え、Baseline Requirements を遵守する全ての証明書は、以下の追加識別子の 1 つを含む。

2.23.140.1.1	Extended Validation Certificate Policy
2.23.140.1.2.1	Domain Validation Certificates Policy
2.23.140.1.2.2	Organization Validation Certificates Policy

1.3 PKI における関係者

1.3.1 認証局 (「発行 CA」)

認証局の第一の責務は公開鍵基盤（以下、「PKI」という）に関する機能、すなわち証明書のライフサイクル管理、利用者登録、及び証明書の発行、更新、交付、失効などに関する業務を遂行することである。証明書のステータス情報は、証明書失効リスト（以下、「CRL」という。）の配布ポイント又はオンライン証明書ステータスプロトコル（以下、「OCSP」という）レスポンダの形式で、リポジトリを通じて、公開される。この認証局は、GlobalSign が直接又は間接的に管理する下位認証局（すなわち、TrustedRoot 発行 CA）の登録局（以下、「RA」という）からの依頼に基づき証明書を発行する役割を示す意味で「発行局」又は「発行 CA」の名で呼ばれることがある。

GlobalSign の Policy Authority は、GlobalSign の経営チーム、及び GlobalSign の取締役会で承認されたメンバーで構成されており、GlobalSign の証明書階層にチェーンされる全ての電子証明書の証明書ポリシーの維持管理に責任を負う。GlobalSign の Policy Authority は、全ての証明書のライフサイクル管理に関する最終権限を有する。この証明書には、ルート証明書、及び TrustedRoot の発行 CA を含む GlobalSign CA 証明書階層を構成する下位発行 CA の証明書などが含まれる。

以下、参照しやすくするため、本 CP に基づき証明書を発行する全ての認証局（GlobalSign を含む）を全て「発行 CA」と称する。

発行 CA は、発行される証明書の管理サービスを安定的に提供する。依拠当事者が失効された証明書についての情報を確実に知ることができるよう、適切な情報開示が必要である。発行 CA は、証明書のステータス情報を、電子証明書のプロパティ内に記載の通り、CRL の配布ポイント又は OCSP レスポンダの形式で、リポジトリを通じて提供する。

1.3.2 登録局(RA)

登録局（RA）は証明書の申請者を識別及び認証することに加えて、証明書の失効、再発行及び更新（Re-key と呼ぶこともある）の要求を受理し、それを転送したりする。GlobalSign はこの RA 業務を行うことができる組織であり、発行 CA は以下の各業務に責任をもって当たる。

- 証明書申請を受理し、評価し、当該証明書申請の登録を承認又は却下する。
- 利用者を証明書サービスへ登録する。
- (要求された証明書タイプに応じた)利用者の本人確認を行うシステムを提供する。
- 公証された、又は他の形で認められた文書を使用して申請者の申請をチェックし、本人確認を行う。
- 申請の承認後、多要素認証のプロセスに基づいて証明書の発行を要求する。
- GlobalSign の、関連する下位発行 CA、或いは下位のパートナー発行 CA からの要求を受け証明書失効手続きをとる。

GlobalSign と契約を締結したサードパーティの発行 CA が独自の RA を運営し、証明書の発行を行うことがある。この際、サードパーティは、本 CP が定める全ての要求事項並びに CA/B Forum が推奨する付加的な基準を参照により組み込む契約条項を遵守しなければならない。RA は、その内部ポリシーに基づき、より厳格な審査手続きを取ることがある。

特定のタイプの証明書を発行するにあたり、RA はサードパーティ認証局が発行した証明書、又はサードパーティの運営するデータベースや情報源などに依拠することがある。パスポートや eID といった国家が発行した個人の証明書、運転免許証等が該当する。RA がサードパーティ認証局発行の証明書に依拠している場合は、依拠当事者には、そうしたサードパーティの CPS を参照し、追加の情報を確認することを助言する。

発行 CA は、そのエンタープライズ RA が属する組織からの証明書申請を検証するために、エンタープライズ RA を指定することができる。エンタープライズ RA において、利用者の組織は認証及び事前定義され、システム構成によって制約されるものとする。

1.3.3 利用者

発行 CA の利用者は、発行 CA が管理する証明書階層からエンドエンティティ証明書の発行を直接的に受ける。又は、独自の PKI 階層から証明書を発行することができる発行 CA から証明書の発行を受けようとするサードパーティである。利用者は、取引、通信、デジタル署名の使用のため証明書を申請し受領した法人又は自然人をいう。個人はあるタイプの証明書の発行を受けることができない。

この文脈における利用者とは、証明書のサブジェクトであると同時に発行 CA と契約を締結し証明書の発行を受けるエンティティである。本人確認及び証明書の発行を受ける前の利用者を申請者という。

エンドエンティティ利用者は、以下のような者をいう：

- 利用者の証明書に記載された公開鍵と対になる秘密鍵について最終権限を有する。利用者は証明書のサブジェクトである場合も、そうでない場合（たとえば、組織が使用するファイアーウォール、ルーター、サーバ、その他のデバイスに対し機械名、役職名を掲載して発行される証明書など）もある。

Trusted Root の利用者は、以下のような者をいう：

- 証明書に記載されるサブジェクトの利益のため認証局証明書階層において認証サービスを提供する枠組みを構築する
- GlobalSign TrustedRoot サービスの運用手続き、及び技術的な実装の両面における契約上、監査上、及びポリシーで定められた要求事項を受諾し、履行する
- 企業内で閉じられた PKI の提供のみ許可される。公開 PKI サービスの提供は許可されない。
- GlobalSign は従属関係によりドメインの利用範囲を技術的に制限する権利を有する。（たとえば、RFC 5280 dNSName で規定される Name Constraints など）

自然人は以下の証明書のサブジェクトに記載される。

- **PersonalSign 2**
- **GlobalSign for AATL**

自然人、法人内の部署名、役職名は以下の証明書のサブジェクトに記載される：

- **PersonalSign 2 Pro**
- **PersonalSign 3 Pro**
- **Noble Energy**
- **NAESB v3.0**
- **GlobalSign for AATL**

あらゆる形で法人格を付与された法人、政府機関は以下の証明書のサブジェクトに記載される：

- **ExtendedSSL**
- **GlobalSign Timestamping**
- **Extended Validation Code Signing**

法人、自営業者は以下の証明書のサブジェクトに記載される：

- **OrganizationSSL**
- **ICPEdu**
- **Code Signing**

DNS 名は以下の証明書のサブジェクトに記載される：

- **DomainSSL**
- **AlphaSSL**

RFC822 に規定される電子メールアドレスは以下の証明書のサブジェクトに記載される：

- **PersonalSign 1**

1.3.4 依拠当事者

TrustedRoot の利用者の認証局から S/MIME 証明書の発行を受けるビジネスパートナーは、利用者であると同時に依拠当事者でもある。

電子証明書の有効性を検証するにあたり、依拠当事者は、通常エンドエンティティ証明書又はチェーンされた証明書に記載されている発行 CA の失効情報を参照しなければならない。

1.3.5 その他の関係者

その他の関係者には、ブリッジ認証局、PKI コミュニティ内において信頼される発行 CA を相互認証する認証局などを含む。

1.4 証明書の使用方法

証明書は、事業体が電子取引を行う際、その他の関係者に身元を証明することを可能にする。証明書は、本人確認用のカードの電子上の代替物として商業環境で使用される。

1.4.1 適切な証明書の使用方法

エンドエンティティ証明書は証明書エクステンションの Key Usage 及び Extended Key Usage を用いて、その使用方法を制限される。

TrustedRoot プログラムのもとで発行された下位認証局証明書は、下記を要求するトランザクションに対する証明書を発行するために使用される

- 認証
- 遠隔地にあるデバイスの出自・同一性の保証
- 暗号化

他の使用方法が提供可能になった場合には、エンドエンティティに具体的に告示する。GlobalSign 証明書を許可されていない方法で使用した場合には、GlobalSign は利用者及びその依拠当事者になんら保証を行わない可能性がある。

1.4.2 禁止されている証明書の用途

証明書は証明書エクステンションの Key Usage 及び Extended Key Usage を用いて、その使用方法を制限される。このエクステンションと合致しない目的で証明書を使用することは認められていない。通信において、限定ワランティーポリシーに示された信頼性の限度を超えた方法で証明書を使用することは認められていない。

証明書は、そのサブジェクトが信頼できること、信頼できる事業を行っていること、証明書がインストールされた機器に瑕疵、マルウェア、ウィルスがないことなどを保証するものではない。Code Signing 証明書は、署名されたコードにバグや脆弱性がないことを保証するものではない。

本 CP に準拠して発行された証明書は、以下の目的に使用してはならない：

- フェイルセーフ機能を必要とする用途
- 法により禁じられている場合
- NAESB WEQ-PKI に準拠して発行された証明書は以下の目的のために使用されてはならない
    - データが危殆化もしくは偽装された場合、懲役を受ける可能性があるデータの転送
    - 連邦法において違法とみなされるデータの転送

1.5 ポリシー管理

1.5.1 文書を管理する組織

発行 CA が認定スキームに準拠しているかどうかの情報を得たい場合、又はその他本 CP に関する問い合わせは、以下に送付すること。

GlobalSign NV
PACOM1 – CA Governance
GlobalSign NV
Martelarenlaan 38
3010 Leuven,
Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909

1.5.2 問合せ窓口

質問全般：

GlobalSign NV
attn. Legal Practices,
Martelarenlaan 38
3010 Leuven,
Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

電子証明書の問題報告
利用者、依拠当事者、アプリケーション・ソフトウェア・サプライヤ、及び他の第三者は、秘密鍵の危殆化の可能性、証明書の不正使用、又は他の種類の不正、セキュリティの侵害、証明書の誤発行、不適切な行為、又は証明書に関連する他の事項は、report-abuse@globalsign.com にメールで報告することとする。

GlobalSign は、この要求に応じて当該証明書を失効することが可能である。また、調査の結果、失効しない場合もある。この意思決定のために GlobalSign はセクション 4.9.5 に記載されている調査を実施する。

1.5.3 証明書ポリシーがポリシーに準拠しているかを判断する担当者

eIDAS における適格監査人から受領するアドバイスに基づき本 CP の適格性、適用可能性や CPS の本 CP への準拠性を判断するのは、PACOM1 – CA Governance である。

本 CP の信頼性を維持促進し、認定基準及び法的要件により的確に対応するため、PACOM1 – CA Governance は少なくとも年次で CP をレビューし、適宜又は状況に応じてポリシーを改訂し更新するべきである。更新されたポリシーは、すでに発行済の証明書、及び発行予定の証明書に対し、本 CP の公表に伴って拘束力を持つ。

1.5.4 証明書ポリシー承認手続き

CP の更新は PACOM1 – CA Governance により確認・承認される。CP の更新が PACOM1 – CA Governance に承認されると、CP の新バージョンが GlobalSign のリポジトリ（https://www.globalsign.com/repository）において公開される。

更新されたバージョンは、その告示が行われると共に、前のバージョンの CP に準拠して発行された証明書の利用者と依拠当事者を含む全ての当事者を拘束する。

1.6 定義と略語

本契約において使用されているが定義されていない文言は、Baseline Requirements、EV ガイドライン、EVCodeSigning ガイドライン、CodeSigning 証明書に関する最低要件、及び/又は eIDAS 規則において定義されるものとする。

関連企業：あるエンティティ、機関、部門、行政小区、政府機関の直接的支配下で運営されるエンティティなどが支配下におくか、これらの支配下におかれるか又は共通支配下にある企業、パートナー、ジョイントベンチャーその他のエンティティ

申請者：証明書の申請をする、又は更新しようとする自然人又は法人。証明書が発行されれば、自然人又は法人は利用者と呼ばれる。デバイス自体が証明書の申請データを送信している場合であっても、証明書に名称の記載されたデバイスを管理運用するエンティティがこの証明書の申請者である。

アプリケーションソフトウェアサプライヤ：ルート証明書を搭載し証明書を表示・使用するブラウザ、その他証明書に依拠するソフトウェアの提供者

認証状：サブジェクトの情報が正確であることを表明する文書

事業体：EV ガイドラインで定義されている民間組織、政府機関、非営利組織ではない組織。例としては、一般的なパートナー、非法人組織、個人企業などが挙げられるが、これらに限定されない

証明書：デジタル署名によってある公開鍵とある本人識別情報との間を紐づける電子文書

証明書権限(CAA)：CAA レコードは、どの証明書局がドメインに対して証明書を発行できるかを指定するために使用される。

証明書受益者：本証明書の利用契約又は利用条件の当事者である利用者、GlobalSign がアプリケーションソフトウェアサプライヤにより配布されるソフトウェアにルート証明書を含める契約を締結した全てのアプリケーションソフトウェアサプライヤ、及び有効な証明書に合理的に依拠する全ての依拠当事者。

証明書データ：認証局が保持、管理、又はアクセス権限を有する(申請者その他から入手する)証明書申請及び付随データ

証明書管理手続き：認証局が証明書データを検証し、証明書を発行し、リポジトリを管理し、証明書を失効する際に使用する、鍵、ソフトウェア、ハードウェアに関連するプロセス、実務、手続き

証明書ポリシー：共通のセキュリティ要件を持つ特定のコミュニティ内もしくは公開鍵基盤において、ある証明書が使用できるかどうかを示す一連のルール

電子証明書問題報告：証明書の危殆化の疑い、不正使用、その他の不正行為、危殆化、不正使用、証明書に関連する不適当行為に関する申し立て

証明書申請：証明書の発行を要求するために行われるBaseline Requirements 10項に規定される情報の伝達

証明書失効リスト：証明書を発行した認証局が作成し電子署名した、定期的に更新されるタイムスタンプ付きの失効した証明書の一覧

認証局：証明書の生成、発行、失効、管理に責任を負う組織。この用語は、ルート認証局、下位認証局のどちらを表す場合にも使用される。

認証業務運用規程：証明書を生成、発行、管理、使用する際の運用方法の枠組みを規定する複数の文書の一つ

Common CA Database (CCADB): パブリックなルートおよび中間 CA 証明書の全てが一覧になっている、Mozilla により運営されている証明書リポジトリ。

危殆化：機密情報が管理できなくなる事態を引き起こすセキュリティポリシー違反

適合性評価機関：規則(EC) No. 765/2008 第 2 条第 13 項に定義される機関であって、同規則に従って適格トラストサービスプロバイダの適合性、また、当該プロバイダが提供するトラストサービスの適合性評価を実施する権限を有すると認定されている機関。

国：国際連合の加盟国、又は少なくとも二つの国連加盟国が主権国家として認めた地理的地域

相互認証証明書：2 つのルート認証局がトラスト関係を構築するために使用する証明書

DCF77:ドイツの長波長信号と標準周波数無線局。

デジタル署名：メッセージを非対称暗号方式とハッシュ関数を用いてエンコードすること。オリジナルメッセージと署名者の公開鍵を所有する人物が、署名者の公開鍵と対になる秘密鍵を使用してエンコードが行われたこと、及びオリジナルメッセージがエンコード後に書き換えられたかどうかを正確に判断することができる。

DNS CAA Email Contact: CA/B Forum Baseline Requirements の Appendix B.1.1 に定義されている電子メールアドレス

DNS TXT Record Email Contact: CA/B Forum Baseline Requirements の Appendix B.2.1 に定義されている電子メールアドレス

DNS TXT Record Phone Contact: CA/B Forum Baseline Requirements の Appendix B.2.2 に定義されている電子メールアドレス

Domain Contact: Base Domain Name の WHOIS 又は DNS SOA のレコードに記載されている、或いは Domain Name Registrar へのダイレクトコンタクトを通して取得された、Domain Name Registrant、技術担当者、或いは管理契約(又は ccTLD における同等のもの)。

ドメイン名：ドメインネームシステムにおいて単一のノードに与えられた名称

ドメイン名システム(Domain Name System, DNS)：ドメイン名を IP アドレスに変換するインターネットサービス。

ドメイン名空間：ひとつのドメインネームシステム内においてある単一の下位ノードに与えられ得るあらゆるドメイン名全て

ドメイン名の登録者：「ドメイン名の所有者」とも呼ばれるが、より正確にはレジストラに登録された人物又はエンティティで、ドメイン名の使用について管理権限を有し、WHOISやレジストラに「登録者」として登録されている自然人又は法人を指す。

レジストラ：Internet Corporation for Assigned Names and Numbers（ICANN）又は各国のドメイン名管理当局・レジストリ、又はNetwork Information Center（その関連会社、契約業者、委託業者、承継人、譲受人を含む）の援助又は契約に基づきドメイン名の登録業務を行う人物又はエンティティ

eIDAS 規則：欧州議会及び理事会の規則(EU)第 910/2014 号。2014 年 7 月 23 日、欧州内市場における電子取引の電子本人確認及びトラストサービスに関する規則。指令 1999/93/EC を廃止する。

電子シール：電子形式のデータであって、電子形式で他のデータに添付されているか、又は論理的に関連付けられているものであって、他のデータの出所及び完全性を確保するためのもの

電子署名：電子形式のデータであって、電子形式で他のデータに添付され又は論理的に関連付けられ、かつ、署名者が署名するために使用するもの

エンタープライズ PKI (EPKI)：Microsoft Windows が信頼するデジタル ID、Adobe Approved Trust List、Adobe Certified Document Services のライフサイクル全体を管理するための、発行、再発行、更新、及び失効を含む、組織向けの製品サービス

エンタープライズ RA：認証局から証明書の発行権限を付与されているところの、認証局の関連会社ではない組織或いはその子会社の従業員又は代理人をいう。エンタープライズ RA は、パートナーや顧客、或いは関連会社、それら当該組織との交流を望むところの対象者に対するクライアント認証の権限を有する。

有効期限：証明書の有効期間の終わりを定義する証明書内の日付で、この日を境に証明書が無効となる。

完全修飾ドメイン名：ドメインネームシステム内の上位ノードに与えられる名前を含むドメイン名

GlobalSign Certificate Center(GCC):GCC は、顧客とパートナーが GlobalSign から証明書を購入、管理するクラウドベースの証明書管理システムである。

全地球測位システム（GPS）:現在位置、ナビゲーション、タイミング(PNT)サービスを利用者に提供する米国運用のシステム。

政府が承認した形式の ID:地方自治体が発行する身分証明書の物理的又は電子的形態、又は、地方自治体が自己の公的目的のために個人の身分証明書を検証するために受諾する身分証明書の形態。

政府機関：政府が運営する法的機関、省、支部、その他同様の国又は行政小区内の構成単位(たとえば州、県、市、郡など)

ハッシュ（SHA1、SHA256 など）：あるビット単位を別の（通常、より小さい）ビット単位に置き換えるアルゴリズムで、以下のような特徴を持つ。

- あるメッセージに対し、同じメッセージをインプットとして使用してアルゴリズムを実行した場合、毎回同じ結果が得られる
- アルゴリズムを用いて生成された結果から計算して元のメッセージを復元することは不可能である
- 二つの異なるメッセージから同じアルゴリズムを用いて同じハッシュ結果を生成することは不可能である

ハードウェアセキュリティモジュール（HSM）：デジタル署名及びサーバアプリケーションが重要な鍵へアクセスする際に強固な認証を行う機能など、デジタル鍵の管理と暗号化処理を行うセキュアな暗号プロセッサ

インターナル・サーバ・ネーム：公開DNSを使用して名前解決のできない（ドメイン名が登録されたもの、登録されていないものを含む）サーバ名

参照により組み込む：組み込むとの明示により、ある文書を別の文書の一部とみなすこと。その際、当該文書の全文を読者が入手できるようにし、また別の文書の一部とすることを明記する。組み込まれた文書は、組み込む文書と同様の効力を有する。

設立機関：民間機関にあっては、法人設立機関であって、法的存在を登録する政府機関。（例えば、設立証書を発行する政府機関）政府機関の場合、政府機関の法的存在を確立する法律、規則又は法令を制定する機関。

個人:自然人

IP アドレス: インターネットプロトコルを用いる機器に付与される、32 ビット又は 128 ビットの表示。

IP アドレス割当先: IP アドレス登録機関にて、(複数の)IP アドレス使用について管理権限を持つ主体として登録されている、(複数の)個人又は(複数の)エンティティ。

IP アドレス登録機関: The Internet Assigned Numbers Authority (IANA) 又は 地域インターネットレジストリ (RIPE, APNIC, ARIN, AfriNIC, LACNIC)。

発行 CA：証明書を発行する認証局。ルート認証局であることも、下位認証局であることもある

設立の管轄：民間機関の場合は、適当な政府機関又は組織(例えば、法人化された場所)への申請(又はその行為)により、当該機関の法的存在が設立された国及び(該当する場合は)州又は地域。政府機関の場合、当該機関の法的存在が法律により創設された国及び(該当する場合)州又は省。

鍵の危殆化：秘密鍵に対する権限を持たない人物に秘密鍵が漏えいした場合、権限を持たない人物による秘密鍵へのアクセスがあった場合、権限を持たない人物への秘密鍵の漏えいが技術に可能であった場合に、秘密鍵が危殆化したと称する。

鍵ペア：秘密鍵と、その対になる公開鍵

法人：団体、企業、パートナーシップ、自営業、信託、政府機関、その他ある国の法制度において法的地位を有するエンティティ

北米エネルギー規格委員会(NAESB)認証局認定要件：NAESB に認定認証局として認可を受けるために認証局が準拠すべき技術的・管理要件

公開鍵基盤(PKI)のための NAESB 事業手続き基準 WEQ-012(「NAESB 事業手続き基準」)：NAESB PKI 規格に準拠するために、認証局、それらの認証局によって発行された証明書、及びそれらの証明書を使用する最終エンティティによって満たされなければならない最低限の要件を定義する。

ネットワークタイムプロトコル (NTP): パケット交換可変遅延データネットワーク上のコンピュータシステム間のクロック同期のためのネットワーク化プロトコル。

オブジェクト識別子(OID)：ISO規格において特定のオブジェクト又はオブジェクトクラスに付与された英数字から成る一意の識別子

OCSPレスポンダ：証明書ステータス確認要求を処理するためリポジトリにアクセスする認証局の監督下で運営されるオンラインサーバ。オンライン証明書ステータスプロトコルの項も参照のこと。

オンライン証明書ステータスプロトコル：証明書に依拠するソフトウェアが証明書のステータスをオンラインで確認するためのプロトコル。OCSPレスポンダの項も参照のこと。

決済サービス指令(Payment Services Directive, PSD2): 全 EU 及び EAC 域内の支払サービス及び支払サービスプロバイダを規制する EU 指令 2015/2366

秘密鍵：鍵ペアの一方で、所有者が秘密裏に保管し、デジタル署名の生成や公開鍵を用いて暗号化された電子データやファイルを復号化するのに用いる。

民間団体:非政府の法人(所有権が非公開であるか公開であるかを問わない)であって、その存在が、設立機関への申請(又はその行為)又は設立管轄権における同等のものによって創出されたもの。

PSD2 証明書: PSD2 に特有の属性情報を含む適格証明書

PSD2 に特有の属性情報: PSD2 証明書 に特有の属性情報：

- 所轄官庁より発行されている場合は認証番号、あるいは国家またはヨーロッパ水準にて認識されている登録番号または金融機関の登録に含まれる法人番号
- 決済サービスプロバイダ(PSP)の役割
- 所轄官庁の名称(NCAName)および独自の識別子 (NCAId).

公開鍵：鍵ペアの一方で、対になる秘密鍵の所有者が公開する。対になる秘密鍵の所有者が生成したデジタル署名を依拠当事者が検証する際、或いは対になる秘密鍵を用いて復号化することができるようメッセージを暗号化する際に使用する。

公開鍵暗号基盤(PKI)：公開鍵暗号方式に基づき、証明書と鍵を信頼できる手法によって生成、発行、管理、使用するためのハードウェア、ソフトウェア、関係者、手続き、ルール、ポリシー、義務などを含む体制全般

一般に信頼される証明書：広く普及するソフトウェアに搭載されるトラストアンカーであるルート証明書にチェーンされている事実をもって信頼を享受する証明書

適格監査人:第 8.2 項(本人確認/評価者の能力)の要件を満たす自然人又は法人。

適格証明書:eIDAS 規則で定義された資格要件を満たす証明書。

e シールの適格証明書:適格なトラストサービスプロバイダによって発行され、eIDAS 規則の付属書 III に定める要件を満たす電子シールの証明書。

電子署名の適格証明書:適格トラストサービスプロバイダによって発行され、eIDAS 規則の付属書 I に定める要件を満たす電子署名の証明書。

適格 e シール：適格電子シール作成装置によって作成され、適格電子シール証明書に基づく高度な電子シール。

適格電子署名:適格電子署名作成装置によって作成され、かつ、適格電子署名証明書に基づく高度な電子署名。

適格政府情報源:政府機関によって維持されるデータベース。

適格国税情報源:民間組織、事業体又は個人に関する税務情報を具体的に記載した適格な政府情報源。

適格独立情報源:定期的に更新され、最新の、公的に利用可能なデータベースであって、それが参照される情報を正確に提供することを目的として設計され、一般的に信頼できる情報源として認識されているもの。

適格電子署名作成装置(QSCD):電子署名作成装置であって、eIDAS 規則の付属書 II に規定される要件を満たすもの。

適格タイムスタンピング(QTS): eIDAS 規則 42 条に準拠したタイムスタンプの提供。

適格トラストサービス・プロバイダ(QTSP):EU 加盟国の国内監督機関により、eIDAS 規則に定義されている資格を有するトラストサービスを提供する(サブセットの)ことを認められている自然人又は法人。

QWAC 証明書 (QWAC): eIDAS 規則 45 条に準拠する適格 SSL 証明

登録ドメイン名：レジストラに登録されたドメイン名

登録局（RA）：証明書のサブジェクトの本人確認と認証に責任を負う法人であり、認証局ではないため、証明書を発行したり、証明書に署名したりすることはない。登録局は証明書の申請手続き、失効手続きをサポートする。「登録局」が役割、機能を説明する場合、必ずしも独立した組織を指すとは限らず、認証局の一部であることもある。

依拠当事者：有効な証明書に依拠する自然人又は法人。アプリケーションソフトウェアサプライヤは、単に当該サプライヤが配布するソフトウェアがある証明書に関する情報を表示するというだけでは、依拠当事者とはみなされない。

レポジトリ：証明書ポリシーや認証業務運用規程など一般に公開される PKI 上の文書、及び CRL 又は OCSP レスポンスの形式によって配布される証明書ステータス情報などを含むオンラインデータベース

ルート認証局：アプリケーションソフトウェアサプライヤが配布するソフトウェアに搭載されるルート証明書を発行するトップ階層にある認証局で、下位認証局の証明書を発行する。

ルート証明書：ルート認証局が発行し自己署名した証明書。ルート認証局の下位認証局に発行した証明書を検証するために使用される。

サブジェクト：証明書にサブジェクトとして記載される自然人、デバイス、システム、部門、法人など。サブジェクトは利用者であるか、利用者が管理、運営するデバイスである。

サブジェクト本人識別情報：証明書のサブジェクトを識別するための情報。これには、subjectAltName エクステンションや commonName フィールドに記載されるドメイン名を含まない。

下位認証局：その証明書がルート認証局又は別の下位認証局に署名された認証局

利用者：証明書の発行を受ける自然人又は法人で、利用契約により法的に拘束される。

利用契約：認証局と申請者又は利用者との間で締結される契約で、当事者の権利義務を規定するもの

監督機関：加盟国の領域内に設立された適格なトラストサービス提供者を監督し、必要に応じて、加盟国の領域内に設立された非適格なトラストサービス提供者に関して行動をとる任務を負う機関。詳細は eIDAS 第 17 条に記載されている。

利用契約：申請者又は利用者が認証局の関連会社である場合に、本文書の要求事項に従い発行された証明書を保管・使用する際に準拠すべき条項

TPM（Trusted Platform Module）：Trusted Computing Groupが規定する暗号デバイス（https://www.trustedcomputinggroup.org/specs/TPM）

信頼できるシステム：侵入や不正使用から合理的に保護されており、適正なレベルの可用性と信頼性があり、正確に動作し、意図された機能の実行に適しており、セキュリティポリシーを厳格に適用するコンピュータ、ソフトウェア、手続きなど

有効期間：証明書が発行された日から有効期限までの期間。

有効な証明書：RFC 5280で規定される検証手続きの結果有効であると認められた証明書

検証スペシャリスト：本文書の要求事項に規定される情報の検証業務を行う担当者

認証局向けWebTrustプログラム：AICPA・CICAにより提供されるその時点で最新の認証局向けのWebTrustプログラム

WebTrust保証シール：認証局向けWebTrustプログラムにおいて準拠性を証明するもの

ワイルドカード証明書：サブジェクトとして、完全修飾ドメイン名の一番左の欄がアスタリスク（*）で示されたものを記載する証明書

WHOIS Lookup: RFC3912 で定義されたプロトコル、RFC7482 で定義されたレジストリデータアクセスプロトコル、又は HTTPS ウェブサイトを介してドメイン名登録官又はレジストリオペレーターから直接検索される情報。

X.400: 電子メールのための ITU-T(国際電気通信連合-T)の規格。

X.500: ディレクトリサービスのための ITU-T(International Telecommunications Union-T)の規格。

X.509：国際電気通信連合電気通信標準化部門(ITU-T)が規定する証明書の規格

AATL	Adobe Approved Trust List
AICPA	米国公認会計士協会
API	アプリケーション・プログラム・インタフェース
ARL	発行局失効リスト (エンドエンティティ失効リストではなく)
CA	認証局
CAA	Certificate Authority Authorization
ccTLD	国別コードトップレベルドメイン
CICA	カナダ公認会計士協会
CP	証明書ポリシー
CPS	認証業務運用規程
CRL	証明書失効リスト
DBA	事業名
DNS	ドメインネームシステム
EIR	Electric Industry Registry
EKU	拡張鍵
EPKI	エンタープライズ PKI
ETSI	欧州電気通信標準化機構
EV	Extended Validation
FIPS	(米国政府)連邦情報処理標準
FQDN	完全修飾ドメイン名
GCC	GlobalSign Certificate Center
GPS	Global Positioning System
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICPEdu	A Infraestrutura de Chaves Públicas para Ensino e Pesquisa
IETF	インターネット技術タスクフォース
ISO	国際標準化機構(International Organization for Standardization)
ITU	国際電気通信連合
LRA	ローカル登録局
NAESB	北米エネルギー規格委員会
NCA	所轄官庁
NIST	(米国政府)アメリカ国立標準技術研究所
NTP	ネットワーク・タイム・プロトコル
OCSP	オンライン証明書ステータスプロトコル
OID	オブジェクト識別子
PKI	公開鍵基盤
PSP	決済サービスプロバイダ
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	登録局
RFC	リクエスト・フォー・コメンツ
S/MIME	セキュア MIME(多目的インターネットメール拡張)
SSCD	安全な署名生成装置
SSL	セキュア・ソケット・レイヤー
TLD	トップレベルドメイン
TLS	トランスポートレイヤー・セキュリティ
VAT	付加価値税
WEQ	Wholesale Electric Quadrant

2.0 公開とリポジトリの責任

2.1 リポジトリ

GlobalSign はリポジトリにおいて、全ての CA 証明書、相互認証証明書、発行した証明書についての失効情報、証明書ポリシー、CPS、依拠当事者規約、利用契約を公開する。発行 CA は、発行した証明書についての失効情報及びルート証明書をリポジトリで常時供覧に付し、これらの情報の可用性について、最低 99%を保証する。また、計画的なダウンタイムに関しても 0.5%を超えないものとする。

GlobalSign は証明書のステータス情報を提供する際、一般にアクセス可能なディレクトリにおいて提出された情報を公開することを、発行 CA 証明書の発行、使用、管理に携わる全ての当事者に対し、ここに通知する。

GlobalSign はセキュリティ管理、業務の手続き、及び社内セキュリティポリシーといった、機密性の高い文書については公開しない。但しこれらの文書は、GlobalSign で WebTrust 又は ETSI の監査が実施される際、必要に応じて適格監査人に提供される。

GlobalSign は、本 CP の翻訳版及びそれを公開するウェブサイト、その他の文書を、販売活動の目的で提供する。しかしながら、GlobalSign の法的拘束力を有する公開リポジトリは https://www.globalsign.com/repository であり、言語によって何らかの不一致がある場合は、英語版を解釈・適用する。

2.2 証明書情報の公開

GlobalSign は CP、CPS、利用契約、依拠当事者規約を https://www.globalsign.com/repository に公開する。CP 及び CPS は RFC 3647 の全ての要求事項を含み、RFC 3647 に従って構成されている。

GlobalSign は以下に準拠する。

- 公的に信頼される証明書の発行及び経営に関する最新版の CA/B Forum の Baseline Requirements (以下、「Baseline Requirements」)
- CA/Browser Forum Guidelines for the Management of Extended Validation Certificate (以下、「EV ガイドライン」)
- www.cabforum.org に公開されている CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates (以下、「EV Code Signing Certificate ガイドライン」)
- https://aka.ms/csbr に公開されている Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (「Code Signing Certificates Minimum Requirement」)
- GlobalSign Root 証明書が組み込まれている他のルートストアのポリシー/プログラム。

本文書の解釈と Baseline Requirements との間に乖離が生じた場合、Baseline Requirements がこの文書に優先して適用・解釈される。Baseline Requirements と Mozilla Root Store ポリシーの解釈に乖離が生じた場合、Mozilla Root Store ポリシーが Baseline Requirements に優先して適用・解釈する。本 CP が準拠するその他の規格については、先述の「前提確認事項」を参照。

2.3 公開の時期及び頻度

CA 証明書は発行後すぐにサポートページからアクセス可能なリポジトリに公開する。エンドエンティティ証明書の CRL は 24 時間ごとに更新され、7 日間有効である。CA 証明書の CRL は少なくとも 3 か月ごとに更新し、また証明書が失効された際には 24 時間以内に更新される。それぞれの CRL には、更新ごとに 1 つずつ増加する連続した番号を付与する。

GlobalSign は、少なくとも年 1 回、CP 及び CPS を見直し、GlobalSign の動作が正確さ及び透明性を保ち、本 CP の「前提確認事項」の項に記載されている外部要件に準拠するように、適切な変更を行う。本 CP、CPS、利用契約、依拠当事者契約の新版及び改訂版は、PACOM1 – CA Governance により Adobe AATL PDF 署名証明書を用い、タイムスタンプ付きデジタル署名を受けた後、7 日以内に公開されるものとする。

2.4 リポジトリへのアクセス管理

発行 CA は、読み取りのみ可能な形でリポジトリを公開し、書き込み目的でのアクセスを防ぐ論理的・物理的な制御を施さなければならない。GlobalSign では、PDF 文書に付されるデジタル署名によって、その文書の完全性と真正性は保持される。

3.0 本人確認と認証

GlobalSignは申請者の本人確認情報とその他の属性情報が真正であるかを認証するための手続きを文書化して保管する。

GlobalSignは、承認された手続き及び基準を用いて、証明書階層にチェーンされることを希望する者（チェーンされることを希望する下位認証局、RA、エンタープライズ登録局、エンドエンティティ利用者など）からの申請を受け付ける。

GlobalSign は本 CP に従い、証明書の失効を申請する者について、係る権利を有する者であることを認証する。

3.1 名称

3.1.1 名称の種類

利用者の本人確認を行うにあたり、GlobalSignは、サブジェクトに割り当てられる名称の種類を含む名称・本人確認規則（X.500「識別名」、RFC 822「名称」、及び X.400「名称」など）に準拠する。識別名を使用する際、コモンネームは、名前空間において一意であることを担保し、誤解を招くものを含んではならない。RFC 2460（IPv6）又は RFC 791（IPv4）に規定される IP アドレスが記載されることがある。

3.1.2 意味のある名称である必要性

GlobalSignは、可能な場合、識別名を使用して証明書のサブジェクトと発行者の名称を区別する。ユーザ・プリンシパル名を使用する場合には、一意でなければならず、また組織体制を正確に反映していなければならない。

3.1.3 利用者の匿名又は Pseudonym の使用

GlobalSignは、証明書に適用されるポリシーにおいて禁じられていない場合、及び名称管理体系における一意性が担保される場合、エンドエンティティ証明書に匿名又はペンネーム(Pseudonym)の使用を許可することがある。

3.1.4 さまざまな形式の名称の解釈方法

証明書内の識別名の記載にあたっては、X.500 規格及び ASN.1 の構文を使用する。統一資源識別子（URI）及び HTTP 構文において X.500 に規定される証明書内の識別名を解釈する方法については、RFC 2253 及び RFC 2616 を参照のこと。

3.1.5 名前の一意性

GlobalSign は、識別名の一意性を、最低 20 ビットの非連続シリアルナンバーを証明書に含むことを必須とすることで担保することがある。

3.1.6 商標の認知、認証、役割

利用者は、他のエンティティの知的財産権を侵害する内容を含む証明書を申請してはならない。特に別段の定めのない限り、本 CP は申請者が商標を使用する権利を有するかどうかの検証を必須としない。しがしながら、GlobalSignは、紛争に関連性のある証明書ついては如何なるものであれ、その申請を拒否すること、或いはこの失効を要求することができる。

3.2 初回の本人識別情報の検証

GlobalSignは、証明書を申請する、或いは認証局のチェーンサービスなどの利用を申し込む、法人又は個人の申請者の本人確認のために必要な情報のやりとり、調査などにおいて、あらゆる法的手続きを用いる。

GlobalSignは、初回の審査において検証の結果真正と認められたサブジェクト識別名その他の本人識別情報を、事後、別の情報及び新規に審査した情報と組み合わせ、別の製品を提供する際にも使用することができ

る。申請が却下された申請者の以前に検証された情報を認証するためには、セクション 3.3.1 の再検証要件が遵守されていることを条件に、適切なチャレンジ・レスポンス方式のアカウント認証によって行われなければならない。

3.2.1 秘密鍵の所有を証明する方法

利用者は、GlobalSign に登録した公開鍵と対になる秘密鍵の所有を証明しなければならない。その関連性は、例えば、ネットワークを経由しない確認方法に加え、デジタル署名された証明書署名要求(以下「CSR」という。)等で検証することができる。

GlobalSign は、Trusted Root サービスのもとで発行 CA 証明書階層にチェーンされることを希望する他の発行 CA の申請を受領することができるが、一次評価を受け、発行 CA との個別契約を締結した後、下位認証局も秘密鍵の所有を証明しなければならない。認証局チェーンサービスの利用においては、（本人識別情報の検証を受けた）申請組織と発行 CA との間で契約が締結されていれば、下位認証局を代表する利用者が RA に直接赴いて審査を受けることは必須としない。

適格証明書及びその利用者の鍵は、Qualified Signature Creation Device (QSCD)内に生成され、保存されなければならない。QSCD 証明書のステータスは監視され、ステータスに変更があった場合は適切な措置を講じられなければならない。

3.2.2 組織の識別情報の認証

組織の識別情報を含む全ての証明書について、申請者は組織名、及び登記された（又は事業を営む）住所を提示しなければならない。組織の法的実在性、正式名称、(申請又は設立管轄における正式名称の一部に含まれている場合は)登記形態、及び組織が提示した住所は検証されねばならず、その検証に用いられた方法は CPS 内に記述されねばならない。

申請者が組織を代表して証明書を申請する権限を有するかについては、3.2.5 項に従って検証する。

3.2.2.1 LRA の認証

LRA の概念を持ったアカウントについては、認証済の組織情報をプロファイルとして発行 CA、RA に設定することがある。権限が付与されていることの認証を受けたアカウント管理者が、LRA の業務を担当し、証明書を申請する申請組織に属する個人ないし、組織が所有又は管理下におくサブドメインの認証を行う。（LRA は契約に基づき個々の認可を行う権限を有するが、対象全ドメインは全て、事前に、本 CP 及び Baseline Requirements に従い事前に許諾されたところの上位レベルドメインを有することが要件となる。）

3.2.2.2 機械、装置、組織および役割に基づく証明書の認証（DepartmentSign）

GlobalSign は、機械や装置や組織の部署、或いは役職に対する証明書を発行するにあたって、認証局に代わって業務を担当する RA、又は発行 CA・RA との契約に基づき義務を負う LRA に、それら機械や装置や組織の部署、或いは組織内の役職名及び組織の事業を正確かつ正しい方法で認証させなければならない。

3.2.2.3 適格証明書

GlobalSign は以下の通り、組織情報を含む適格証明書を 2 種類発行する：

- e シールの適格証明書(組織情報を証明)
- 電子署名の適格証明書(個人の組織に所属することを証明)
- QWAC 証明書

組織情報を含む全ての適格証明書について、申請者は、組織の正式名称(法的形式を含む)及びサブジェクトの事業所の物理的な所在地の住所を示ことが求められる。

GlobalSign は以下を参照し、法的存在及び住所を検証する：

- Qualified Government Information Sources に掲載されている公式の政府記録、又は
- 組織の法的設立、法的存在又は法的認知を有する管轄区域の政府機関により確認、もしくは提供される文書
- Qualified Independent Information Source により提供される記録

さらに、GlobalSign は以下を参照し、住所を検証する可能性がある：

- 検証された法的見解又は会計士の書簡
- 当該組織の有効な適格 e シールを用いて署名された物理的所在地の証明

各種証明事項の情報は、適格証明書の内容と一致していなければならない。

適格証明書には、組織の正式名称、ビジネス上の名義(商号又は取引における名義)も含めることができる。GlobalSign は、組織が、事業所管轄区域において、当該申請のために仮称の使用を適切な政府機関に登録したこと、及び当該登録が引き続き有効であることを検証する。

本人が組織に所属していることを主張する証明書に関して、GlobalSign は、下記の事項に基づいて、本人の所属を確認する：

- 機関が提供する確認であって、検証された伝達方法を用いて取得したもの
- 組織からの独立した確認
- 検証された法的意見又は検証された会計士の書簡
- 組織の有効な適格 e シールによって署名された証明
- LRA の業務対応において、適切な認証を受けたアカウント管理者によって取得された証明

組織および QWAC 証明書の同一性を主張する適格証明書については、GlobalSign は、組織の権限を付与された代理人の同一性及び権限を検証する。

GlobalSign は、下記事項を参考に、権限を与えられた代表者の権限を確認する：

- Qualified Government Information Source が提供する公式の政府記録
- 組織の法的設立、法的存在又は法的認知を有する管轄区域の政府機関により確認、もしくは提供される文書
- Qualified Government Information Source により提供される記録
- 検証された法的意見又は検証された会計士の書簡
- 組織の有効な適格 e シールを用いて署名された証明(その証明の記載事項は、適格証明書の内容と一致していなければならない)

GlobalSign は、セクション 3.2.3 に従って、授権された代表者の身元を確認する。
GlobalSign は PSD2 特有の属性について、国立の登録局、ヨーロッパ銀行の登録局、及び所轄官庁からの正式な伝達等、所轄官庁により提供されている情報をもとに検証する。

GlobalSign は所轄官庁を通知できる電子メールアドレスについて、新規発行の証明書内にて通知された場合、その証明書情報(証明書の 16 桁のシリアル番号、サブジェクトの識別名、発行者の識別名、証明書の有効期間、連絡先情報、失効申請についての案内、証明書ファイルのコピー等)をその電子メールアドレスへ平文にて送信する。

3.2.3 個人の本人識別情報の認証

GlobalSign 又は RA は個人に発行する証明書のクラスに応じて、以下の通り認証する。

3.2.3.1 Class 1

申請者は証明書に記載する電子メールアドレスに対する管理権限を証明する。発行 CA 又は RA には、その他の提示情報を検証することは求められない。

3.2.3.2 Class 2

申請者は、申請に含まれるアイデンティティ属性(証明書が関係する電子メールアドレスやドメイン名など)の管理を実証する必要がある。

申請者は政府機関発行の有効な身分証（運転免許証、軍人身分証明書、その他同様のもの）又は写真付き ID カードの判読可能なコピーを提出する。付加的に、政府機関発行以外の身分証、写真付き ID カードの提出を求められることもある。GlobalSign は証明書申請に含まれる名前と身分証に記載される名前、及び国、州、その他の住所の情報が一致することなど、適切なレベルで本人確認が行われることを担保する。

発行 CA 又は RA は、申請者の本人識別情報を以下のいずれか一つの方法によって認証する。

1. 信頼できる情報源からの電話番号を使用し、出願人に電話によるチャレンジ・レスポンスを行う。
2. 信頼できる情報源からの FAX 番号を使用し、申請者に対して FAX によるチャレンジ・レスポンスを行う。
3. 信頼できる送信元からの電子メールアドレスを使用し、申請者に対して電子メールによるチャレンジ・レスポンスを行う。

4. 信頼できる情報源から得た住所を使用し、申込者に対して郵送によるチャレンジ・レスポンスを行う。
5. 正当な公証人、委託を受けた第三者から、本人又は政府が認める身分証明書に基づくアイデンティティを証明する旨の証明を受けること。
6. 組織に所属する個人の場合、GlobalSign は承認されたローカル RA の証明に依拠することができる。ePKI 又は MSSL プロファイルを介して要求されるクラス 2 の証明書については、3.2.3.5 を参照のこと。
7. 政府が承認した証書に基づき、依頼者から自己のエンドカスタマーのアイデンティティを検証する旨の証明を受け、その一方で、依頼者は、これらの検証に関する安全な監査可能な証跡を保持する。
8. (文書に法的に署名することを許可する法的管轄において) 出願人の印鑑は、書面で受領した出願に含まれる。

出願人に対しては、更なる情報が要求されることがある。同等のレベルの信頼性を実証するために、他の情報及び/又は方法を利用してもよい。

電子メールアドレスが証明書に記載される場合、GlobalSign 又は LRA はその電子メールアドレスの所有の正当性について検証しなければならない。

3.2.3.3 Class 3

EV コードサイン証明書について、申請者は、証明書に記載される全ての電子メールアドレスに対する管理権限を証明することが求められる。

EV SSL 証明書について、申請者は、証明書に記載される全てのドメイン名に対する管理権限を証明することが求められる。

申請者は政府機関発行の有効な身分証（運転免許証、軍人身分証明書、その他同様のもの）又は写真付き ID カードの判読可能なコピーを提出する。付加的に、政府機関発行以外の身分証、写真付き ID カードの提出を求められることもある。GlobalSign は、証明書申請に含まれる名前と身分証に記載される名前、及び国、州、その他の住所の情報が一致することなど、適切なレベルで本人確認が行われることを担保する。

PersonalSign 3 Pro において、公証人又は信頼できる第三者は、その機会に及び国が発行する写真付き身分証を検証したこと、申請情報が正確であることを証言するため、申請者と面会する。

発行 CA 及び RA には、EV ガイドライン及び EV Code Signing ガイドラインに従い、申請者との信頼できるコミュニケーション手段として GlobalSign が検証した信頼できる伝達方法を用い、申請者の保有する、証明書のサブジェクトとして記載されることを希望している組織を代表する権限を認証することが求められる。

申請者又は申請者の属する組織は、さらに情報を提出することが求められることがある。また同じレベルの信頼性を担保する上記以外の方法を採用することもある。

3.2.3.4 適格証明書

GlobalSign は、以下の方法に従って、個々の利用者の識別を認証する：
1. 本人確認
2. 電子上の本人確認の使用
3. 適格電子署名の使用
4. ビデオ検証

3.2.3.4.1 本人確認

本人確認においては、利用者が物理的に存在している必要があり、以下の文書の提出が必要である：
1. 政府発行写真付き ID
2. 署名されたパーソナル・ステートメント
3. 二つの二次証拠書類

個人の肖像を写真付き ID と比較し、写真付き ID のセキュリティ機能を検査する。パーソナル・ステートメントの署名は、写真付き ID の署名と比較される。

この検証を実行できるエンティティ：
1. 認証局(CA)

2. 登録当局(RA)
3. 役人又は第三者検証者
4. ローカル登録当局 - 組織(個人の組織への所属性を示す適格証明書の場合。その従業員、請負業者、代理人の本人確認)

3.2.3.4.2 遠隔本人確認

GlobalSign は本人確認に遠隔地から電子的な方法で本人確認を行うこともある。全ての電子本人確認手段は、eIDAS 規則第 8 条に定める「実質的」又は「高水準」の保証水準を有する。また、発行に先立ち、本人の身体的存在が保証される。

1. 通知された電子本人確認スキームについては、保証水準は、加盟国から欧州委員会への通知によって決定される。
2. 通知されていない電子本人確認手段については、保証水準は欧州委員会によって記述された要件に従って決定される。適合性評価機関による審査の後、GlobalSign は、本項に定めている電子本人確認手段を受け入れる前に、審査結果を監督機関に提出し、許可を受ける。

自然人の物理的存在は、電子本人確認手段に利用される認証要素のカテゴリーを確認することによって確保することができる。GlobalSign は、以下の権限の認証要因を物理的存在の証明として受け入れている：

1. 少なくとも 1 つの固有の要素
2. 以下の各カテゴリーのうち 1 つ以上の、複数の要素
    - 保有に基づくもの(「保有に基づく認証要素」とは、サブジェクトが保有していることを証明するために必要な認証要素をいう)
    - 知識に基づくもの(「知識に基づく認証要素」とは、サブジェクトが知識を有していることを証明するために必要とされる認証要素を意味する。).

この検証を実行できるエンティティ：

1. 認証局(CA)
2. 登録局(RA)

3.2.3.4.3 適格証明書

GlobalSign は、利用者の有効な適格電子署名を個人のパーソナル・ステートメントに使用して、適格電子署名を作成するために使用される証明書に含まれる申請者の身元及び追加属性を確認する。

以下のいずれかの条件が満たされた場合、GlobalSign は上記のようにする：

1. 発行 CA にかかわらず、適格電子署名の作成に用いられる適格証明書が、高度な保証レベルを有すると通知された電子本人確認スキームの一部としてとして発行された場合
2. 適格証明書が新規証明書の発行前 825 日以内に直接本人確認をした後に GlobalSign により発行された場合

この検証を実行できるエンティティ：

1. 認証局(CA)
2. 登録局(RA)

3.2.3.4.4 ビデオ検証

GlobalSign は、ビデオ検証を使用することができる。利用者は、対面証明と同様に、以下の文書を提供することが求められる：

1. 政府発行写真付き ID
2. (電子的に)署名されたパーソナル・ステートメント
3. 二つの二次証拠書類

個人の肖像を写真付き ID と比較し写真付き ID のセキュリティ機能を検査する。この方式では、利用者がインターネット対応機器、ウェブカメラ又は他のビデオ機器、マイク及びサウンドシステムを利用できることを前提とする。

この検証を実行できるエンティティ：

1. 認証局(CA)
2. 登録局(RA)

3.2.3.5 ローカル登録局認証

マネージド PKI 及び SSL マネージドサービスアカウントを含む事前審査済み組織アカウントはローカル登録局（以下「LRA」）と考えることができるが、GlobalSign CA は、このアカウントに対し、認証済の組織情報をプロファイルとして設定する。こうしたアカウント内の証明書はプロファイルの情報を利用する。権限が付与されていることの認証を受けたアカウント管理者が、LRA の業務を担当し、証明書を申請する申請組織に属する個々の認証を行う。

3.2.3.6 北米エネルギー企画委員会（NAESB）向け証明書

北米エネルギー規格委員会（以下「NAESB」）向け証明書申請については、関連会社による利用者証明書の組織情報の真正性を確認するために、組織名、住所、及び組織が存在することの証明文書を含まなければならない。GlobalSign もしくは RA は、申請者の真正性及び申請者の当該組織における申請権限の有無も含めて、情報の審査をしなければならない。WEQ-012 の申請のために証明書を利用している利用者は、法的所在地を登録し、NAESB の EIR に登録され、利用者申請時や発行時に使用するための「利用者コード」を確保しなければならない。

WEQ-012 の申請以外の目的で、エネルギー産業内で使用される証明書を発行する場合、ACA は、NAESB EIR 内で利用者登録を必要とする WEQ-012-1.9.1、WEQ-012-1.3.3 及び WEQ-012-1.4.3 の規定を除き、NAESB WEQ-012 Public Key Infrastructure Business Practice Standards and Models の規定に準拠しなければならない。

GlobalSign は RA 運用を自社で実施するか、RA 運用/機能の一部もしくは全てを ePKI 経由で別の法人に外部委託することを選ぶことが可能である。どちらの場合においても RA 運用/機能を行う組織は身元証明、監査、ログ保存、利用者情報の保護、データ保存やその他 CP 及び NAESB 認定認証局要件及び NAESB Business Practices Standards に RA が実施すると定められている手続きを実施しなければならない。社内で RA 運用/機能を実施する場合、認証局に課せられた責務として、全ての RA 運用/機能に係る RA インフラ及び手続きは上記要件に準拠しなければならない。NAESB 認定認証局及び/又は委任されたエンティティは、RA 運用/機能を行う全ての当事者が NAESB 認定認証局要件を理解し、同意していることを保証しなければならない。

GlobalSign、及び/又は関連する RA は申請者の身元情報が GlobalSign の CP/CPS に記載されたプロセスにより審査されることを保証しなければならない。審査プロセスは証明書レベルにより異なり、NAESB Accredition Specification に記載されなければならない。尚、文書及び審査要件は保証レベルにより異なる。

本人確認の要件は以下の通り行う：

NIST Assurance Level	NAESB Assurance Level
Level 1	Rudimentary (最小限)
Level 2	Basic (低度)
Level 3	Medium (中程度)

GlobalSign 又は委託された RA(マネージド PKI の場合)は、申請者により提供された本人確認情報を全て、section 2.2.2: Authentication of Subscribers of the “NAESB Accreditation Requirements for Authorized Certification Authorities にて説明されている、Identity Proofing Process (IPP) Method に従って審査しなければならない。

3.2.4 検証されない利用者情報

GlobalSign は、証明書のサブジェクト識別名に記載される情報、或いはその CPS か発行する証明書そのものに記載する規定において除外される製品又はサービス固有の項目以外の全ての情報を検証する。GlobalSign は、サブジェクトの所属名（organizationalUnitName）フィールドを使用して、依拠当事者に検証されていない利用者情報又は免責事項、告知などの情報を提供する。個人の場合、携帯電話番号などの固有の識別子を個人の法律上の氏名と合わせて使用する場合がある。

- GlobalSign が自然人や法人の名称、事業名、商号、住所、所在地、その他を明確に識別することができる全てのタイプの証明書では、GlobalSign はこれらの情報を検証しなければならず、そのため免責事項の告知を記載しなくてもよい。
- 「マーケティング」などの文言が情報として証明書に記載されている等、明確に身元証明ができない場合、GlobalSign はこうした利用者情報が検証されていないことを告知する免責事項を証明書に記載しなくてもよい。Intranet SSL 証明書に限っては、GlobalSign は、申請者の希望により、イン

ターナルネットワーク内で使用されるドメイン名、非公開ドメイン名、ホスト名、RFC 1918 に規定される IP アドレスなどを、証明書の subjectAlternativeName フィールドに記載してもよく、これらの情報は申請者の申告にのみ依拠する。

SSL/TLS用の証明書、及びCode Signing証明書については、認証局は、申請者が自己申告の情報をサブジェクトの所属名（organizationalUnitName）フィールドに記載できない申請手続きを採用しなければならない。

GlobalSignは、クライアント認証用、文書署名用、S/MIME用、及び役職名を含む証明書の提供に際し、証明書の以下のフィールドのいずれかにポリシーOIDを記載することを条件に、情報をLRAに契約に基づき検証させてよい。

- サブジェクトの所属名（organizationalUnitName）
- commonName

3.2.5 権限の認証

PersonalSign1 Certificates	チャレンジ・レスポンス方式を用いて申請者が証明書に記載される電子メールアドレスを管理していることを検証する。
PersonalSign Demo Certificates	申請者が証明書に記載される電子メールアドレスを管理していることを検証する。
PersonalSign2 Certificates	信頼できる方法による申請者個人との連絡を通じた検証に加え、証明書に記載された電子メールアドレスを管理していることを検証する。
Noble Energy Certificates	申請組織又は申請者個人との信頼できる手段による意思確認を通し検証すると同時に、証明書に記載される電子メールアドレスをその申請者が管理していることを検証する。
NAESB Certificates	信頼できる方法による申請組織又は申請者個人との連絡を通じた検証に加え、申請者が証明書に記載される電子メールアドレスを管理していることを検証する。(3.2.3.5 項を参照)
PersonalSign2 Pro	申請者個人との信頼できる連絡手段を通し検証すると同時に、必要に応じ、証明書に記載される電子メールアドレスをその申請者が管理していることを検証する。マネージド PKI アカウントにより発行された証明書は、プロファイル設定時に、LRA の権限者を検証する。
PersonalSign2 Department Certificates	申請者個人との信頼できる連絡手段を通し検証すると同時に、必要に応じ、証明書に記載される電子メールアドレスをその申請者が管理していることを検証する。マネージド PKI アカウントにより発行された証明書は、プロファイル設定時に、LRA の権限者をが検証する。
PersonalSign3 Certificates	申請組織との信頼できる連絡手段を通し、申請者が組織を代表して証明書を申請する権限を有することを検証する。申請者の身元証明のため、申請者が RA 担当者と面会して身分証を提示することが必須であるほか、証明書に記載される電子メールアドレスをその申請者が管理していることを検証する。
Code Signing Certificates	Code Signing Minimum Requirements の規定に従い、申請組織及び申請者個人を検証する。
EV Code Signing Certificates	EV ガイドライン及び EV Code Signing ガイドラインの規定に従い、契約署名者及び証明書承認者の権限を検証する。
DV/AlphaSSL Certificates	3.2.7 項に規定されている認証方法の一つを使用し、申請者がドメイン名を保有又は管理していることを検証する。
OV SSL & ICPEdu Certificates	3.2.7 項に規定されている方法により、申請組織又は申請者個人との信頼できる手段による意思確認を通し検証すると同時に、必要に応じ、証明書に記載されるドメイン名を申請者が保有又は管理していることを検証する。マネージド SSL アカウントによって発行された証明書は、プロファイル設定時に、その権限を有する LRA が検証する。
EV SSL Certificates	EV ガイドラインの規定に従い、契約署名者及び証明書承認者の権限を検証する。同時に、3.2.7 項に規定されている方法を通し、申請者がドメイン名を保有又は管理していることを検証する。マネージド SSL アカウントによって発行された証明書は、プロファイル設定時に、その権限を有する LRA が検証する。

Timestamping Certificates	組織の申請者との信頼できる連絡手段を通し検証する
AATL and CDS	申請組織又は個人との信頼できる連絡手段を通し検証すると同時に、電子メールアドレスを証明書に記載する要求があった場合、申請者が電子メールアドレスを管理していることを検証する。マネージド PKI アカウントにより発行された証明書は、プロファイル設定時に、その権限を有する LRA が検証する。
Trusted Root	組織の申請者との信頼できる連絡手段を通し検証する。トップレベルドメイン/サブドメイン、又は 3.2.7 項で説明されているドメイン名といった、NameConstraints（名前の制限）に含まれる可能性がある全ての要素を検証する。
Qualified Website Authentication Certificates	3.2.2.3 項に規定されている方法に従い、契約署名者、証明書の承認者、および権限者の権限を検証する。同時に、3.2.7 項に規定されている方法に従い、申請者がドメイン名を保有または管理することを検証する。
Qualified Certificate for Electronic Seal	3.2.2.3 項に規定されている方法に従い、契約署名者が証明書の承認者かつ権限者であることを検証する。
Qualified Certificate for Electronic Signature	3.2.2.4 項に規定されている方法に従い、個人の申請者からの申請について権限を検証する。

3.2.6 Re-key 要求における本人確認と権限の認証

2.1 項に準ずる

3.2.7 ドメイン名の認証

Baseline Requirements 3.2.2.4 項の記載事項に従った方法により、全ての SSL/TLS 証明書について、申請されたドメイン名及び IP アドレスを申請者が保有又は管理していることを検証する。その方法の詳細は CPS に記載されなければならない。

申請者又は申請者の属する組織は、さらに情報を提出することが求められることがある。また同じレベルの信頼性を担保する上記以外の方法を採用することもある。

3.2.8 電子メールアドレスの認証

GlobalSign は、申請者が電子メールアドレスを管理又は使用する権利を有することを確認するために、以下いずれかの方法を使用する。

1. 要求された電子メールアドレス宛に任意の値を送信し、その値を用いて確認の返信を得ることで、申請者が要求された電子メールアドレスを管理していることを確認する。又は、
2. GlobalSign Certificate Practice Statement の 3.2.7 項に記載されたいずれかのドメイン認証の方法を用い、申請者が FQDN を管理又は使用する権利を保有することを確認する。検証されると、エンタープライズ RA は、その FQDN の下でアドレス指定された正確な電子メールアドレスを含む証明書を発行することができる。

3.3 鍵更新申請時における識別及び認証

発行 CA は、利用者の証明書について、有効期限が満了する前の鍵の更新(以下、「Re-key」という)申請に対応する。発行 CA は、証明書のライフサイクル期間における再発行要求にも対応する。再発行は、Re-key の一種の形態であり、Re-key との違いは、再発行を受けた証明書の有効期限が元の証明書と同じとなる点である。

3.3.1 定期的な Re-key とその際の本人確認及び権限の認証

- **PersonalSign1 Certificates** ユーザ名・パスワードによる 9 年ごとの再検証が必要
- **PersonalSign2 Certificates** ユーザ名・パスワードによる 9 年ごとの再検証が必要。又は、有効期間内かつ有効な証明書によるクライアント認証が必要。
- **Noble Energy Certificates** ユーザ名・パスワードによる 9 年ごとの再検証が必要。又は、有効期間内かつ有効な証明書によるクライアント認証が必要。
- **PersonalSign3 Certificates** ユーザ名・パスワードによる 6 年ごとの再検証が必要
- **Code Signing Certificates** ユーザ名・パスワードによる 825 日年ごとの再検証が必要
- **EV Code Signing Certificates** EV ガイドラインの指示に倣った、ユーザ名・パスワードによる

6 年ごとの再検証が必要

- **DV SSL Certificates** ユーザ名・パスワードによる 825 日ごとの再検証が必要
- **OV SSL & ICPEdu Certificates** ユーザ名・パスワードによる 825 日ごとの再検証が必要 825
- **EV SSL Certificates** EV ガイドラインの指示に倣った、ユーザ名・パスワードによる 6 年ごとの再検証が必要
- **Timestamping Certificates** 取り扱わない
- **CA for AATL Certificates** ユーザ名・パスワードによる 6 年ごとの再検証が必要
- **Trusted Root** 取り扱わない
- **AlphaSSL** 取り扱わない
- **NAESB Certificates** 認証された CA の利用者においては、再発行のために、以下のテーブルに基づいて本人確認が必要。(GlobalSign は NAESB High Assurance の証明書を発行していない。) :

保証レベル	本人確認要件
Rudimentary	有効期限が満了する前の秘密鍵を保持すること。
Basic	有効期限が満了する前の秘密鍵を保持すること。但し、最低でも初回の登録時より 5 年に 1 度は、初期登録時と同様のプロセスを実施し、本人確認情報を再検証しなければならない。
Medium	有効期限が満了する前の秘密鍵を保持すること。但し、最低でも初回の登録時より 3 年に 1 度は、初期登録時と同様のプロセスを実施し、本人確認情報を再検証しなければならない。

- **Qualified Certificate for Electronic Seals** ユーザ名・パスワードによる 13 か月ごとの検証が必要
- **Qualified Certificate for Electronic Signature** ユーザ名・パスワードによる 13 か月ごとの検証が必要
- **Qualified Web Authentication Certificates** EV ガイドラインの指示に倣った、ユーザ名・パスワードによる 13 か月ごとの検証が必要

3.3.2 失効後の再発行とその際の本人確認及び権限の認証

証明書の失効後、新しい証明書を発行する場合、利用者は本 CP の説明する初期登録時と同様のプロセスを実施する必要がある。

3.3.3 証明書情報変更の際の本人確認の再検証と再認証

証明書内のサブジェクト情報が変更となった場合は、CP/CPS に定められている識別情報の確認手続きを再度実施し、認証された情報を含む新しい証明書を発行すること。

GlobalSign は上記の有効期限を越えた利用を許可しないため、追加の認証を行うことなく証明書の再発行に対応することはない。

3.3.4 失効後の Re-key とその際の本人確認と権限の認証

証明書の失効後に定期的に設定されている再発行には対応しない。証明書失効後の再発行のために、利用者は初回の証明書発行時と同じ審査を受けなければならない。

3.4 失効申請における本人確認と権限の認証

GlobalSign は全ての失効申請について、要求者の権限を認証しなければならない。GlobalSign CA は、ユーザ名及びパスワードによるアカウントへのログイン、又は証明書に組み込まれた固有の要素を所有していることの証明といった、適切なチャレンジ・レスポンス方式に従い、失効申請を行う利用者に対してその権限を検証する。

GlobalSign はまた、該当する利用契約の規定に従い、利用者を代理して失効手続きを取ることがある。失効理由としては、利用契約への違反や、該当する料金の未払いなどがある。

4.0 証明書のライフサイクルに対する運用上の要求事項

4.1 証明書申請

4.1.1 証明書の申請者

GlobalSignは、証明書の申請を受諾しない個人又はエンティティのリストを独自に作成する。このブラックリストは、過去の取引履歴、或いはその他の情報源に基づいて作成される。加えて、GlobalSignがサービスを提供する国・地域の管轄政府当局が発行する、又は国際的に認知された取引禁止対象者リストなどの外部情報源に依拠して、証明書を発行しない申請者を選別する。

4.1.2 登録手続きとそこで負うべき責任

認証局は、依拠当事者に申請者の本人識別情報を提示する全てのタイプの証明書について、その情報の真正性を十分に検証するシステム、手続きを採用するものとする。申請者は、必要な検証を行えるよう、GlobalSign及びRAに対し情報を提出しなければならない。GlobalSign及びRAは、申請者が申請手続きにおいて情報を提出する際の通信の秘密を保護し、当該情報を安全に保管する。

4.2 証明書申請手続き

4.2.1 本人確認及び権限の認証の実施

GlobalSign は、CPS に準拠し、本人識別情報の真正性を十分に検証するシステム、手続きを採用するものとする。初回の本人確認は、GlobalSignの検証チーム又は契約しているRAが本CP3.2項の規定内容に沿って実施する。手続きに伴い行われる連絡の結果得られた情報は、提出された申請者の情報と共に、安全に保管される。初回以降の証明書申請については、単一要素による認証(利用者名かつパスワード)又は多要素認証(ユーザ名/パスワードとひもづけられた証明書)を用いて権限を検証する。

GlobalSignは、ドメインのCAAレコードと照合したパブリックなSSL証明書における各サーバのFQDNを検証しなければならない。GlobalSign の発行ドメインは"globalsign.com"である。CAA レコードがglobalsign.com を公証されたCAとして記載していない場合、GlobalSign は証明書を発行することができない。

CAAのチェックは、Name Constrained CAを利用する証明書を発行するGlobalSign Trusted Rootの利用者に対するオプションである。

4.2.2 証明書申請の認可又は却下

GlobalSignは、いずれかの項目について検証を完了することができない場合、証明書申請を却下する。
適切なベストプラクティスの手続きを経て全ての検証手続きが完了した場合には、GlobalSignは通常、証明書要求を承認する。 GlobalSign は以下に挙げるような理由があれば、申請を拒絶することが可能である：

- GlobalSign が申請を受領する際に GlobalSign のブランドが損傷される可能性がある。
- 以前に申請を却下されたか、又は以前に利用契約の条項に違反した申込者からの証明書。

GlobalSignは、申請を却下した理由を申請者に説明する義務を負わない。

GlobalSignは、パブリックなSSL証明書を社内サーバ名又は予約IPアドレスに対して発行してはならない。

4.2.3 証明書の申請処理に要する期間

GlobalSign は、証明書の申請を処理し評価するために、全ての合理的な方法が使用されることを保証するものとする。

4.3 証明書の発行

4.3.1 証明書発行時における認証局の業務

GlobalSign Root CAが証明書を発行するには、GlobalSignの信頼された役割にある正式なメンバーが、Root CAが証明書署名の業務を行うために、意図的に直接命令を発行することが必要である。

GlobalSign は、RA から証明書の発行を承認する旨の連絡を受け取る機能を有するシステムのアカウントに対し、多要素の認証を行う。検証を行う発行 CA が直接運営する RA、及び契約に基づいて運営される RA は、認証局に送信される情報が全て、確実に審査され真正性を担保されていることを保証する。

4.3.2 認証局から利用者への証明書の発行に関する通知

GlobalSign は、登録手続きの際に提示された合理的で適切な連絡先を通じて、証明書の発行を利用者に通知する。

4.3.3 利用者への NAESB 用証明書の発行に関する通知

申込者の本人確認及び権限の認証が問題なく完了した場合、GlobalSign は要求された証明書を発行し、申込者に通知し、証明書を申込者に提供しなければならない。

4.4 証明書の受領

4.4.1 証明書の受領とみなされる行為

GlobalSign は、利用者に対し、電子証明書に記載された情報が正しいことを確認するまでは、当該証明書を使用しないよう通知する。これが実のない規定とならないよう、GlobalSign は、電子証明書が受領されたものとみなされるまでの期間を設定することができる。

4.4.2 認証局による証明書の公開

GlobalSign は、利用者に証明書を交付することにより、又は Certificate Transparency Log といったしかるべきリポジトリにおいて、証明書を公開することができる。

4.4.3 認証局からその他のエンティティへの証明書の発行に関する通知

RA、LRA、パートナー/再販業者、又は GlobalSign は、最初の証明書情報の登録に関与していれば、発行について通知を受けることができる。

4.5 鍵ペアと証明書の利用

4.5.1 利用者による鍵ペアと証明書の利用

利用者は、秘密鍵が第三者に開示されることのないよう保護しなければならない。GlobalSign は、利用者の秘密鍵の保護義務を規定する利用契約を利用者との間で締結しなければならない。秘密鍵は、対になる公開鍵を含む証明書の Key Usage 及び Extended Key Usage フィールドに指定される用途以外に使用してはならない。秘密鍵のバックアップを保持する場合には、オリジナルの秘密鍵と同様に保護しなければならない。秘密鍵の有効期限が満了した後は、利用者はバックアップファイルも含め、全ての秘密鍵を安全に消去しなければならない。

GlobalSign は、GlobalSign のデジタル署名サービスにおいて、利用者の同意を得て、短期間のみ利用された証明書とそれに対応する秘密鍵をホスト、保護、管理する。

4.5.2 依拠当事者による公開鍵と証明書の利用

GlobalSignは、CRLやOCSPなど証明書の有効性を検証する適切な方法を通じた確認を必要とするなど、依拠当事者が電子証明書の情報に依拠する際の条件を、そのCPSに規定しなければならない。GlobalSignは、利用者の証明書に依拠するにあたり利用者が依拠当事者に提示すべき条件を規定した依拠当事者規約を、利用者に対し提供しなければならない。依拠当事者は、この規約に記載された情報をリスク評価のために確認しなければならず、証明書に記載の情報又はそこで提示されるあらゆる保証を信頼し依拠する前にリスク評価を行うことに全責任を負う。
依拠当事者が使用するソフトウェアは、ポリシーと Key Usage の解釈の際のベストプラクティスなどを含め、X.509 規格に準拠したものでなければならない。

4.6 証明書の更新

4.6.1 証明書更新の条件

証明書の更新とは、従前に発行を受けた証明書と同一の情報を記載し、同じ公開鍵を含む、有効期限の異なる証明書を新たに発行することである。(ただし、NAESB 証明書は常に再発行を行い、更新という概念は存在しない。) GlobalSign は、証明書の更新を取り扱う製品、サービスを明示しなければならない。GlobalSign は、以下の条件下で再発行を行ってよい:

- オリジナルの証明書が失効されていないこと、
- オリジナルの証明書に記載される公開鍵がなんらかの理由でブラックリストに登録されていないこと、及び、
- 証明書に記載されている全ての情報が正しく、改めて検証が必要でないこと

GlobalSign は、（上記の条件に基づき）すでに更新済又は Re-key 済の証明書を再更新又は再 Re-key することができる。オリジナルの証明書は更新後に失効してよいが、同じオリジナルの証明書を再度更新、Re-key してはならず、また記載情報を変更してはならない。

4.6.2 更新の申請者

GlobalSignは、オリジナルの証明書のライフサイクルを管理するアカウントにおける適切なチャレンジ・レスポンスによる認証を経て、オリジナルの証明書の利用者が承諾した更新申請を受理する。CSR は必須ではないが、証明書署名要求の提出を受ける場合には、オリジナルの証明書と同じ公開鍵を含んだものでなければならない。

4.6.3 証明書更新申請の処理

GlobalSign は証明書更新申請に対し、追加的に情報の提出を求めることができる。

4.6.4 利用者への新しい証明書の発行に関する通知

4.3.2 項に準じる。

4.6.5 更新された証明書の受領とみなされる行為

4.4.1 項に準じる。

4.6.6 認証局による更新された証明書の公開

4.4.2 項に準じる。

4.6.7 認証局からその他のエンティティへの証明書の発行に関する通知

規定しない

4.7 証明書の RE-KEY

4.7.1 証明書の Re-key の条件

証明書のRe-keyとは、利用者が新しい証明書を取得し、古い証明書と交換するためのプロセスである。この新しい証明書は、

- 古い証明書と同一の情報(アイデンティティ、ドメイン等)を記載している
- 有効期限が古い証明書とは異なる
- 古い証明書とは異なる公開鍵を含む

古い証明書の有効期限前に、新しい証明書が古い証明書と同一の有効期限を付与されてRe-keyされた場合、このプロセスは「再発行」と呼ばれる。

GlobalSign は、証明書の Re-key を取り扱う製品、サービスを明示しなければならない。GlobalSign は、以下の条件下で Re-key を行ってよい。

- オリジナルの証明書が失効されていないこと、
- 新しい証明書に記載される公開鍵がなんらかの理由でブラックリストに登録されていないこと、及び、
- 証明書に記載されている全ての情報が正しく、新規に、或いは改めて検証が必要でないこと

GlobalSign は、（上記の条件に基づき）すでに更新済又は Re-key 済の証明書を再 Re-key することができる。オリジナルの証明書は Re-key 後に失効してよいが、同じオリジナル証明書を再度更新、Re-key してはならず、また記載情報を変更してはならない。

4.7.2 新しい公開鍵を含む証明書の申請者

GlobalSignは、オリジナルの証明書のライフサイクルを管理するアカウントにおける適切なチャレンジ・レスポンスによる認証を経て、オリジナルの証明書の利用者又は利用者を代理して秘密鍵管理の責任を負う組

織担当者が承諾した Re-key 申請を受理することができる。Re-key 申請において CSR は必須であり、これには新しい公開鍵情報を含めなければならない。

4.7.3 証明書 Re-key 申請の処理

GlobalSign は証明書 Re-key 又は再発行申請を処理するにあたり、追加的に情報の提出を求めることがある。過去に情報を検証してから年数が経過している場合、再審査の対象たる利用者の本人識別情報を再検証する。再発行の申請では、チャレンジ・レスポンス方式による権限の検証を行うことができる。

4.7.4 利用者への新しい証明書の発行に関する通知

4.3.2 項に準じる。

4.7.5 Re-key された証明書の受領とみなされる行為

4.4.1 項に準じる。

4.7.6 認証局による Re-key された証明書の公開

4.4.2 項に準じる。

4.7.7 認証局からその他のエンティティへの証明書の発行に関する通知

規定しない

4.8 証明書記載情報の修正

4.8.1 証明書記載情報の修正の条件

証明書記載情報の修正とは、従前に発行を受けた証明書と異なる情報を含む証明書を新たに発行することである。新しい情報を記載した証明書は、従前の証明書と同じ公開鍵を含む場合もあれば、異なる公開鍵を含むこともある。また、有効期限も同じである場合もあれば、異なる場合もある。

- GlobalSign は、情報修正を、新規の証明書発行として取り扱う。
- GlobalSign は、過去に更新又は Re-key された証明書の情報を修正して発行することができる。オリジナルの証明書は情報修正後に失効してよいが、同じオリジナル証明書を再度更新、Re-key してはならず、また記載情報を変更してはならない。

4.8.2 証明書記載情報の修正の申請者

4.1 項に準じる。

4.8.3 証明書記載情報の修正申請の処理

4.2 項に準じる。

4.8.4 利用者への新しい証明書の発行に関する通知

4.3.2 項に準じる。

4.8.5 記載情報の修正された証明書の受領とみなされる行為

4.4.1 項に準じる。

4.8.6 認証局による記載情報の修正された証明書の公開

4.4.2 項に準じる。

4.8.7 認証局からその他のエンティティへの証明書の発行に関する通知

規定しない

4.9 証明書の失効、効力の一時停止

4.9.1 失効の条件

証明書の失効とは、CRL（証明書失効リスト）にシリアル番号と失効日時を記載し、それにより当該証明書をブラックリスト化する手続きをいう。CRL は失効される証明書に署名したものと同じ秘密鍵を使用してデジタル署名される。CRL にシリアル番号を記載することにより、依拠当事者はこの電子証明書のライフ

サイクルが終了していることを確認することができる。(有効期限を満了して 10 年経過した)CodeSigning 証明書を除き、発行 CA は CRL のファイルサイズを適切に管理するため、有効期限の到来した失効された証明書については、リストから消去することができる。発行 CA は、失効の手続きを取る前に、失効要求者の権限を検証する。

利用者証明書の失効は以下の条件下で、24 時間以内に行われなければならない：

1. 利用者が証明書の失効を希望する旨を書面で(証明書を発行した GlobalSign に)申請した場合。
2. 利用者が、元の証明書申請が承認されておらず、遡及的に承認を付与していないことを GlobalSign に通知した場合。
3. GlobalSign が(証明書の公開鍵と対になる)利用者の秘密鍵が危殆化したという合理的な証拠を取得した場合。
4. GlobalSign が通知の受領或いはその他の手段によって、利用者に利用規約又は約款上の重大な義務違反があったこと、かつ/又は利用者、利用規約、或いは事業機能の予期せぬ終了を認識した場合。
5. ドメイン認証或いは証明書内の FQDN 又は IP アドレスへの管理について検証する際、依拠すべきではない証拠を取得した場合。
6. PSD2 証明書について、その PSP より認証または登録されている所轄官庁から正式な失効申請を受領した場合(又はそうした所轄官庁からの失効申請を認証する場合)。失効の正当理由としては、PSP の権限が失効された際や、証明書に含まれる PSP の役割が失効された際が挙げられる。

利用者の証明書の失効は、24 時間以内に実施されるべきであり、以下のうち 1 つ以上の状況が発生した場合、5 日以内に実施される。

1. 証明書が、6.1.5 項及び 6.1.6 項に規定されているように、Baseline Requirements のアルゴリズムの種類及び鍵長についての要件をもはや準拠していない。
2. GlobalSign が、証明書が不正使用されたことを示す証拠を取得する。
3. GlobalSign が、証明書の公開鍵と対になる利用者の秘密鍵が危殆化に瀕しているという合理的証拠を取得する。
4. GlobalSign が、本証明書における FQDN 又は IP アドレスの使用がもはや法的に許可されていないことを示す状況(例えば、裁判所又は仲裁人がドメイン名を使用するドメイン名登録者の権利を取り消した場合、ドメイン名登録者と申請者との間におけるライセンス契約もしくはサービス契約が終了した場合、又はドメイン名登録者がドメイン名を更新しなかった場合)を認識する。
5. GlobalSign が、ワイルドカード証明書が、不正に誤解を招く下位 FQDN を認証するために使用されたことを認識する。
6. GlobalSign が、証明書に含まれる情報に重大な変更があった際、その旨通知を受けた、またその他の方法で知った。
7. GlobalSign が、証明書が Baseline Requirements 又は GlobalSign の CP 又は CPS に従って発行されたものではないことを認識した。
8. GlobalSign が、証明書に記載される情報のいずれかが正確でないか、誤解を招く恐れがあると判断する。
9. GlobalSign が、何らかの理由で業務を停止し、他の認証局(CA)に証明書の失効を委託しない。
10. GlobalSign が CRL/OCSP リポジトリの保守を継続する限りにおいて、Baseline Requirements の下に証明書を発行する権利が消失した、或いは取り消された又は終了した。
11. GlobalSign の CP 及び・又は CPS により失効が要求された。
12. 証明書の形式の技術的様式が、アプリケーションソフトウェアサプライヤ又は依拠当事者に容認できないリスクをもたらす(例えば、CA/B Forum は、利用されていない暗号/署名アルゴリズム又は鍵のサイズが容認できない危険性を示し、そのような証明書は、所与の期間内に CA によって失効、置き換えがなされるべきであると判断する可能性がある)。
13. GlobalSign が、公開鍵に基づいて簡単に計算できる方法(Debian weakey や http://wiki.debian.org/SSLkeys など)である、利用者の秘密鍵を危殆化する実証済又は証明済の方法を認識した場合。又は、秘密鍵を生成するために使用された方法に欠陥があることを示す明確な証拠がある場合。

利用者の証明書の失効は、次に掲げる事情があるときは、商業上合理的な期間内に行うこととする。

1. 利用者又は組織の管理者が、証明書のライフサイクルを管理する GCC アカウントを通じて証明書の失効を申請する。
2. 利用者は、GlobalSign のサポートチーム又は GlobalSign の登録当局へ、認証済み申請を通じて失効を申請する。

3. GlobalSign が、利用者が禁止対象者としてブラックリストに追加されたこと、又は、GlobalSign の法域の法律に基づき、禁止された地域から営業していることの通知を受領するか、又は、発見する。
4. 証明書のキャンセル申請を受けたとき。
5. 証明書が再発行された場合に、GlobalSign が以前に発行された証明書を失効可能なとき。
6. 一定のライセンス契約に基づき、GlobalSign は、ライセンス契約の満了又は終了後、証明書を取り消すことができる。
7. GlobalSign が、本証明書の継続使用が GlobalSign 又は第三者の事業に悪影響を及ぼすと判断する。証明書の利用が GlobalSign 又は第三者の事業又は評判に悪影響を及ぼすかどうかを検討する際、GlobalSign はとりわけ、受領した苦情の性質及び件数、苦情申立人の身元、有効な関連法規、及び利用者による有害とされる使用への対応を検討する。
8. Microsoft が、専らその裁量で、コードサイン又は EV コードサイン証明書を、偽名を含むか、又はマルウェア又は不要なソフトウェアの促進に使用されていると認定した場合、Microsoft から GlobalSign に連絡が行き、証明書の失効が要求される。GlobalSign は、商業的に合理的な期間内に本証明書を失効するか、又は Microsoft の要請を受領後 2 営業日以内に Microsoft に例外を申請する。Microsoft は、独自の裁量で、例外を許可又は拒否することができる。Microsoft が例外を認めない場合、GlobalSign は、2 営業日を超えない商業上合理的な期間内に本証明書を失効させる。
9. Microsoft が、或いは専らその裁量により、マルウェア又は望ましくないソフトウェアの販売促進に SSL 証明書が使用されていることを特定した場合、Microsoft から GlobalSign に連絡が行き、証明書の失効が要求される。GlobalSign は、商業的に合理的な期間内に本証明書を失効するか、又は Microsoft の要請を受領後 2 営業日以内に Microsoft に例外を申請する。Microsoft は、独自の裁量で、例外を許可又は拒否することができる。Microsoft が例外を認めない場合、GlobalSign は、2 営業日を超えない商業上合理的な期間内に本証明書を失効させる。
10. 利用者の死

下位認証局(CA)証明書の失効は、次の場合、7 日以内に行う。

1. 下位 CA が、下位 CA 証明書又は本認証実施規定(CPS)の第 1.5.2 条に詳細が記載されている権限を提供する GlobalSign 事業体に対し、GlobalSign が本証明書の失効を申請していることを書面で要求する。
2. 利用者が、元の証明書リクエストが承認されておらず、遡及的に承認を付与していないことを GlobalSign に通知する。
3. GlobalSign が、証明書内の公開鍵に対応する下位 CA の秘密鍵が危殆化した、又は、6.1.5 項及び 6.1.6 項に規定されているように、Baseline Requirements のアルゴリズムの種類及び鍵のサイズの要件をもはや満たさないという合理的な証拠を取得する。
4. GlobalSign が、証明書が不正使用されたことを示す証拠を取得する。
5. GlobalSign が、証明書が Baseline Requirements 又は CP もしくは CPS に従って発行されていないこと、又は下位認証局が Baseline Requirements もしくは CP もしくは CPS を遵守していないことを発見した。
6. GlobalSign が、証明書に表示される情報のいずれかが不正確であるか、誤解を招く恐れがあると判断する。
7. 発行 CA 又は下位 CA が、何らかの理由で業務を停止し、他の CA 証明書の失効を委託していない。
8. 発行 CA が、CRL/OCSP レポジトリを維持し続けるための調整をしていない限り、BaselineRequirements に基づき証明書を発行する CA 又は下位 CA の証明書発行権利は、満了するか、取り消されるか、又は終了する。
9. 発行 CA の CP 及び・又は CPS により失効が要求される。
10. 証明書の技術的な内容又は書式が、アプリケーションソフトウェアサプライヤ又は依拠当事者に、許容できないリスクをもたらす(例えば CA/B Forum が、推奨されない暗号/署名アルゴリズム又は鍵のサイズが容認できないリスクをもたらし、そのような証明書が一定の期間内に CA によって取り消され、置き換えられるべきであると判断するかもしれない場合)。

他の発行CAを相互認証する発行CAは、相互認証した発行CAが両当事者間で締結された契約条項に適合しない場合、相手の発行CAを失効することが可能である。

4.9.2 失効の申請者

GlobalSign 及び RA は、失効要求者が権限を有すると検証できた場合に要求を承認する。失効要求は、利用者本人又は証明書に記載された組織から提出された場合、権限のある要求として受理される。発行 CA は発行した証明書を自己の裁量で失効する権利を有し、これには相互認証する認証局に発行された証明書を含む。利用者、依拠当事者、アプリケーションソフトウェアサプライヤ、及び他の第三者は、証明書を取り消す合

理的な理由が疑われる場合、電子証明書の問題報告を提出し、その旨を GlobalSign に通知することができる。加えて PSD2 証明書においては、失効申請が PSP を認証又は登録した所轄官庁から行われうる。

GlobalSign はまた、自らの判断で、他のクロス署名の発行 CA に対して発行される証明書を含む証明書を取り消すことができる。

4.9.3 失効申請の処理手続き

失効要求の持つ性質と効率化の観点から、GlobalSign及びRAはシステムを通じて失効要求者の本人確認を行うことができる。たとえば、アカウントを通じて発行した証明書の失効要求を行う方法がある。RAはシステムを通じた失効手続きが取れない場合に、代替手段を取ることが可能である。

GlobalSign及びRAは、失効要求の記録を残し、要求者の本人確認を行い、要求者の権限が確認された場合には適切な失効手続きを取る。

失効された場合、証明書のシリアルナンバー、失効日、失効時刻が CRL に記載される。理由コードを含むこともある。CRL は直ちに発行されるか、或いは GlobalSign の CPS に準拠して発行される。

CA 及び RA の発行は、利用者、依拠当事者、アプリケーションソフトウェアサプライヤ、及び他の第三者が証明書失効要求を提出するための方法を作成するものとする。GlobalSign 及び RA は、この要求に応じて取り消すことができる、又はしないことがある。この決定を行うための CA 及び RA の発行に必要なアクションの詳細については、セクション 4.9.5 を参照すること。

4.9.4 失効申請までの猶予期間

SSL サーバ証明書およびコードサイニング証明書について、GlobalSign は失効要求までの猶予期間を設けない。

その他の証明書について、失効要求までの猶予期間とは、危殆化の疑いがある場合、脆弱な鍵を使用した場合、発行を受けた証明書に記載された情報に不正確な内容が含まれていた場合などに、利用者が失効を要求する前に必要な対策を取るための時間を指す。GlobalSign は、利用者に最大 48 時間の猶予を与えることができるが、これを過ぎると発行 CA は利用者の証明書を失効する、或いはその他利用者を代理した適切な手続きを取ることができる。

4.9.5 認証局が失効申請を処理すべき期間

GlobalSignは、報告を受けた後24時間以内にCertificate Problem Reportの調査を開始する。

エンドエンティティ証明書の失効要求については、アカウントを通じて送信された失効要求、及び GlobalSignが失効手続きを開始したもののいずれであっても、受理から最大でも30分以内に処理されなければならない。

他の GlobalSign の証明書を相互認証する GlobalSign は、失効要求を危殆化の事実の確認後 24 時間以内に処理し、認証局失効リスト（以下、「ARL」という）をキーセレモニー後 12 時間以内に発行する。

発行 CA 及び RA は、Report Abuse を通した報告を通じて、優先度の高い証明書問題報告に内部的に対応する能力を 24 時間 365 日維持し、必要に応じて、当該苦情を法執行権限に転送し、及び/又は当該苦情の対象である証明書を取り消すものとする。GlobalSign 及び RA は、報告の受領後 24 時間以内に、疑わしい鍵の危殆化又は証明書の誤用に対する調査手続きを開始するものとする。

GlobalSign は、少なくとも以下の基準に基づいて、失効又はその他の措置が正当化されるかどうかを決定する:

1. 申し立ての問題の性質
2. 特定の証明書又は利用者に関して受け取った報告の件数
3. 苦情を申し立てている主体、及び
4. 関連規則

適格証明書の場合、実際の失効ステータスは、失効決定後 60 分以内に全ての失効過程を通じて公開/利用可能となり、決して復元しない。

4.9.6 失効情報確認に関する依拠当事者への要求事項

証明書に記載された情報を信頼し依拠する前に、依拠当事者は、証明書が適正な目的のために使用されていることを検証し、各証明書が有効であることを保証せなければならない。依拠当事者は依拠しようとする証明書がチェーンされる全ての階層の証明書について、CRL 又は OCSP の情報を参照すべきであり、またこのチェーンが完全であり、IETF の X.509 規格に準拠していることを検証すべきである。これには、認証局鍵識別子（以下、「AKI」という）及びサブジェクト鍵識別子（以下、「SKI」という）の検証を含む。GlobalSign は、依拠当事者が失効情報の検証を容易に行えるよう、該当する URL を証明書に記載することがある。

4.9.7 CRL の発行頻度

GlobalSign は、CRL の発行頻度については、”CABForum Base Requirements for Publically Trusted Certificates”及び “CABForum Base Requirements for Extended SSL Certificates”に準拠しなければならない。オフライン認証局を運用する GlobalSign は、CRL を 3 か月ごとに発行する。オンライン認証局を運用する GlobalSign は、少なくとも 7 日ごとに CRL を発行しなければならず、また、nextUpdate のフィールドの値は thisUpdate のフィールドの値に加えて 10 日を超えてはならない。

下位 CA の証明書、CRL は、下位 CA 証明書を取り消した後、少なくとも 12 ヶ月に 1 回、24 時間以内に更新され、nextUpdate のフィールドの値は、thisUpdate のフィールドの値に加えて 12 ヶ月を超えてはならない。

4.9.8 CRL の最大通信待機時間

CRL は生成後、商業的に合理的な期間内にリポジトリに投稿される。

4.9.9 オンラインでの失効情報の確認

GlobalSign は、CRL の他に OCSP レスポンダにより失効情報を提供する場合、通常のネットワーク環境において、OCSP による応答までの待機時間が 10 秒を超えないよう管理する。

GlobalSign の OCSP 応答は、RFC6960 及び又は RFC5019 に準拠している。OCSP 応答は、OCSP 応答者によって署名されるものとし、その証明書は、その失効ステータスがチェックされている証明書を発行した CA によって署名される。OCSP 署名証明書は、RFC6960 で定義されるタイプ id-pkix-ocsp-nocheck の拡張を含まなければならない。

4.9.10 オンラインでの失効情報の確認の要件

利用者証明書のステータスについては:

- IGlobalSign CA は、OCSP を通じて提供される情報を少なくとも 4 日ごとに更新する。このサービスからの OCSP 応答は、有効期限 7 日を超えないものとする。

下位 CA 証明書のステータスについては:

- 発行 CA は、OCSP を通じて提供される情報を、少なくとも(i) 12 ヶ月ごと、及び(ii) 下位 CA 証明書を失効した後 24 時間以内に更新する。

発行されていない証明書のステータスのリクエストを受け取った OCSP レスポンダは、そのような証明書に対して「有効」と応答しない。

技術的に制約されていない CA の OCSP レスポンダは、7.1.5 項に沿って、このような証明書に対して「有効」と応答しない。

GlobalSign は、OCSP リクエストに次のデータを含めるよう要求する：

- プロトコルバージョン
- サービス要求
- 対象証明書識別子

4.9.11 その他の方法による失効情報の提供

利用者証明書が高トラフィック FQDN の場合、GlobalSign は[RFC4366]に従って、その OCSP 応答を分配するためにステープルに依存することを選択することができる。この場合、GlobalSign は、利用者が TLS ハンドシェイクで証明書の OCSP レスポンスを「ステープル」することを保証するものとする。GlobalSign は、利用契約を通じて、又は CA が実施する技術的検討手段によって、この要求事項を利用者に対して契約上執行するものとする。

4.9.12 認証局の鍵の危殆化に伴う特別な要件

発行 CA 及び RA は、その秘密鍵が危殆化した恐れがあるときには、合理的な方法をもって利用者にその旨の通知をする。これには、脆弱性が発見された場合、及び GlobalSign が自己の裁量により鍵の危殆化の疑いがあると判断した場合などが含まれる。鍵の危殆化に疑いの余地がない場合、発行 CA 証明書、エンドエンティティ証明書などを 24 時間以内に失効し、更新した CRL をオンラインで 30 分以内に発行する。

4.9.13 証明書の効力の一時停止を行う条件

証明書の効力の一時停止はクライアント証明書にのみ認められる。証明書の効力の一時停止は、他のタイプのエンドエンティティ証明書には許可されない。証明書の効力の一時停止は、SSL 証明書及び適格証明書には厳しく禁じられている。

4.9.14 証明書の効力の一時停止の要求者

発行 CA 及び RA は、認証済みの一時停止要求を受領するものとする。利用者又は証明書指定の関連機関から停止要求を受けた場合は、停止を許可する。GlobalSign はまた、他のクロス署名発行 CA に発行される証明書を含む証明書を自らの判断で停止することができる。

4.9.15 証明書の効力の一時停止手続き

一時停止要求の性質と効率上の必要性により、発行 CA 及び RA は、例えば一時停止要求された証明書を発行したアカウントを介す等して、一時停止要求を要求し認証するための自動機能を提供することがある。また、自動一時停止機能が不可能な場合、RA は手動のバックアッププロセスを提供することがある。発行 CA 及び RA は、一時停止要求を記録し、送信元を認証し、要求が真正でありかつ承認されている場合、証明書を一時停止するために適切な措置を講じる。一旦中断したら、CRL の理由を示すコードである「on hold」を含め、証明書のシリアル番号と日時が適切な CRL に追加される。CRL は、直ちに公表される場合もあれば、認証業務運用規程(CPS)に定義されている通りに公表される場合もある。

4.9.16 証明書の効力の一時停止期限

証明書の効力の一時停止期限には制限がない

4.10 証明書ステータス情報サービス

4.10.1 運用上の特徴

GlobalSign は証明書のステータス情報を、CRL 配布ポイント及び OCSP レスポンダを通じて公開する。コードサイン証明書および cRLDistributionPoints 拡張子を含む適格証明書においては、GlobalSign は、失効した証明書の有効期限から 10 年が経過するまで、CRL 又は OCSP の失効履歴を削除しない。他の種類の証明書の場合、GlobalSign は、失効された証明書の有効期限が過ぎるまで、CRL 又は OCSP 上の失効履歴を削除しない。

4.10.2 サービスを利用できる時間

GlobalSign は証明書ステータス情報を 24 時間 365 日提供する。この際、付加的にキャッシュされた情報を含むコンテンツ配信ネットワークを通じたクラウドサービスを使用することがある。最優先にある Certificate Problem Report に対し社内にて応答できる能力を 24 時間 365 日維持することとし、適切である場合は、法令の執行機関への準拠し、かつ/又はそうした訴えを受けている証明書を失効する。

4.10.3 運用上の特性

規定しない

4.10.4 利用の終了

利用者は、証明書サービスの利用を、証明書を失効すること、又は有効期限を満了することで終了することができる。GlobalSign がエンドエンティティに証明書を発行する下位認証局との契約を締結している場合、両当事者間の契約は証明書の有効期限中は継続されなければならず、契約を終了させる場合には証明書を失効させなければならない。

4.11 キーエスクロー及びリカバリー

4.11.1 キーエスクロー及びリカバリーの、ポリシー及び手続き

認証局の秘密鍵は預託されてはならない。利用者に対してキーエスクローサービスを提供する発行 CA は、利用者の秘密鍵を預託してよい。預託された秘密鍵は、オリジナルの秘密鍵と少なくとも同じセキュリティレベルで保管しなければならない。

4.11.2 鍵カプセル化及びリカバリーの、ポリシー及び手続き

規定しない

5.0 施設、経営、及び運用上の管理

5.1 物理的管理

GlobalSignは、証明書発行に使用及び管理されるシステムにおいて、物理的なアクセス管理、自然災害からの保護、火災安全要因、ライフラインの停止（例：電源、電話など）、施設の故障、水漏れ、盗難に対する安全対策、破壊及び不法侵入や、災害対策に対応する物理的かつ環境的セキュリティポリシーを持つものとする。
損失、損害、又は資産に対する損害、及び営業妨害、情報（データ）・データ処理施設の盗難を防ぐための管理対策を導入するものとする。

5.1.1 所在地及び建物

GlobalSignは、重要機密情報を処理する設備が適切なセキュリティ障壁及び入管管理体制を持つ安全な場所に設置されていることを保証するものとする。
これらは不正アクセス、損害、妨害から物理的に保護さるべきであり、またその保護とはリスク分析計画に明記のリスクに対応するものとする。

5.1.2 物理的アクセス

GlobalSign、証明書ライフサイクル管理に使用される設備が、不正アクセスがシステム又はデータに対してもたらす損害から物理的に保護された環境で運用されていることを保証するものとする。
物理的保護域に不承認者が立入る際は、常に承認された従業員が同行するものとする。
物理的な保護とは、認証局オペレーションを搭載するシステムの周囲に明確に定義されたセキュリティ境界（例；物理的な障壁など）を設置することで達成されるものとする。
この境界区域内においては、認証局資産の如何なる部分もその他組織の構成と共用されるものではない。

5.1.3 電源及び空調

GlobalSignは、電力供給及び空調設備が認証局システムの運用を補助するのに十分なものであることを保証するものとする。

5.1.4 水漏れ

GlobalSign は、認証局システムが水漏れから保護されていることを保証するものとする。

5.1.5 火災安全及び保護

GlobalSign は、消防システムにより認証局システムが保護されていることを保証するものとする。

5.1.6 メディア ストレージ(記憶媒体)

GlobalSignは、使用されるいずれのメディア（記憶媒体）も損害、盗難及び不正アクセスから保護され、安全に使用されていることを保証するものとする。
メディアの管理処理は一定期間、メディア本体の老朽化・劣化に対して保護されるべきであり、また記録の保持が必要とする。全てのメディアは情報資産分類スキームの条件に沿って安全に使用され、また機密情報を格納するメディアが必要とされなくなった際は、安全に破棄されなければならないものとする。

5.1.7 廃棄物

GlobalSignは情報の格納に使用された、全てのメディアが放出もしくは廃棄される前に、一般的に許容される方法において機密解除もしくは破壊されていることを保証するものとする。

5.1.8 オフサイト バックアップ

GlobalSignは、証明書発行システムの完全バックアップは、システム停止時にシステムを復旧するために適切なものであり、定期的に作成されていることを保証するものとする。（この期間はCPSにて定義されなければならない）重要な業務情報及びソフトウェアのバックアップ用コピーは定期的に作成されなければならない。災害又はメディア停止に伴い、全ての重要な営業情報及びソフトウェアが復旧できるように適切なバックアップ設備が提供されなければならない。
事業継続計画の条件を満たしていることを保証するため、個々のシステムのバックアップ調整は定期的にテストされるものとする。
少なくとも、1 つはシステムの完全なるバックアップコピーがオフサイト（証明書発行設備とは離れた場所）に格納されていなければならない。バックアップについても、通常の施設と同様に物理的・手続き上の管理が為された場所に格納されるものとする。

5.2 手続き的管理

5.2.1 信頼された役割

GlobalSignは、点検要員を含む全てのオペレーター及び管理者が信頼された役割の範囲内で稼動していることを保証するものとする。
信頼された役割とは利害の対立が発生不可能なものであり、如何なる人物も単独でCAシステムのセキュリティを破ることができないように権限分散される。
信頼された役割は以下を含む。（但しこれに限定するものではない）：

GlobalSign は、関連会社又はこれらの関連会社と(下請として)関係があることが特定されている個人のために、証明書を購入することがある。GlobalSignの関連会社としては、親会社および子会社、及びGlobalSignと同一の親会社を持つその他の企業がある。

- 開発：認証局システムの開発に対する責任がある
- セキュリティオフィサー又は情報セキュリティ長：認証局のセキュリティ実践導入の運営に対する全体的な責任(鍵のコンポーネント監視等)
- 管理者：証明書の生成/失効/停止を承認する
- インフラシステムエンジニア：認証局システムのインストール、設定及び保守に加え、認証局システムアーカイブ及び監査ログの閲覧及び保守に責任がある
- インフラオペレーター：日常的な認証局システムの操作及びバックアップ・復旧に責任がある
- キーマネージャー：暗号化に用いられる鍵のライフサイクル管理機能(鍵のコンポーネント監視等)に責任がある

5.2.2 タスク毎に必要な人員数

GlobalSign は、CPS 内でタスク毎に必要となる人員数を明確に強調して記載するものとする。この目的は、如何なる悪意ある行為も結託する必要が生じるため、全認証局サービス（鍵ペア生成、証明書生成、及び失効）への信頼を保証することとなる。他者間管理が必要な場合、少なくとも関係者の内一人は管理者となる。全ての関係者は先に 5.2.1 項に定義された信頼された役割である事が求められる。

5.2.3 役割ごとの本人確認と権限の認証

信頼された役割に指名する前に、GlobalSign は該当者の身元調査を行うものとする。
先に述べた各役割は、認証局をサポートするために適切な人物が適切な役割を所有していることを保証するために本人確認及び認証が行われている。

5.2.4 責任の分離を要する役割

GlobalSign は、認証局設備、手続き的、又はその両方の意味で、役割の分離を強制するものとする。
個別の認証局担当者は上記の 5.2.1 項に定義される役割に指定される。

職務分掌が要求される業務には以下のものがある：

- 証明書の生成、失効、及び停止の承認者
- CA システムのインストール、構成、及び維持管理を行う者
- CA のセキュリティ関連の活動について全面的な管理責任を負う者
- 暗号鍵ライフサイクル管理に関する職務を担う者（鍵コンポーネントの監督者など）
- CA システムの開発者

5.3 人員コントロール

5.3.1 資格、経験、及び許可条件

GlobalSignは、人員が証明書管理プロセスに従事する前に、従業員、代理人、又は契約社員としてのアイデンティティを検証することとする。

GlobalSignは、職務権限に適切であり、また提示されたサービスに対して必要な専門知識、経験及び資格を所有する人員を必要人数雇用するものとする。 GlobalSignの者は、正式な研修、教育、実地経験又はそのいずれか2つの組み合わせを通して、専門知識、経験及び資格の要件を、満たすものとする。 GlobalSignのCPSの中で指定される、信頼された役割及び責任は、職務記述書中で文書化されるものとする。GlobalSignの人員(一時的・永続的の両者)は、業務及び最小特権の分離の視点、職務及びアクセスレベル、バックグラウンドチェック、従業員教育に基づいた(職務やセキュリティに対する)理解度に基づく役職の機密性を考慮の上定義された職務記述書を有するものとする。GlobalSignの人員は、セキュリティ責任者である上級管理職によって信頼された役割に正式に指名されるものとする。職務記述書は技術及び経験の必要条件を含んでいる。管理者の人員は、電子署名テクノロジーでの実務又は研修経験を有し、またセキュリティ業務責任を担う人員のセキュリティ処置、及び情報セキュリティでの経験、リスク評価における経験など十分に管理機能を遂行出来る者が採用されるものとする。

5.3.2 バックグラウンドチェック手続き

GlobalSignの全信頼された役割に従事する者は、認証局運営の公平を不利にするような矛盾する利益を持たない者とする。 GlobalSignは、役職に対して適正に影響すると思われる重罪或いはその他犯罪に前科を持つ人物を、信頼された役割に指名しないものとする。
人員が雇用される法域で許可されている場合には、全ての必要な確認がなされ、その結果の分析が終わるまでは、人員は信頼済みの機能にアクセスしない。 信頼された役割に従事する人員は全員、忠実、信頼性及び健全性に基づいて選ばれるものとし、バックグラウンドチェックに従うものとする。

GlobalSignが行ったバックグラウンドチェックによって明らかになった情報の利用は如何なる場合も、その人員が雇用される法域の該当の法令に準拠するものとする。

5.3.3 研修要件

GlobalSign は、情報の認証業務を行う全ての人員に、公開鍵基盤の基本的な知識、認証、また審査のポリシーや手順（認証局の証明書ポリシー及び認証業運用規程を含む）、情報の認証プロセスにおける一般的な脅威（フィッシングや他のソーシャルエンジニアリングの方策を含む）、及び Baseline Requirements に関する技能研修を実施している。

GlobalSign は上記研修の受講記録を保持しており、審査要員に任命された人員が該当業務を十分に遂行できるような技能レベルを維持していることを保証する。

GlobalSign は審査要員にある業務の遂行を許可する前に、その人員が業務遂行に必要なスキルを有していることを文書化するものとする。

GlobalSign は審査要員全員に対し、認証局が提供している Baseline Requirements に記載の情報認証要件に関する試験の合格を必須としている。

5.3.4 再研修の頻度と要件

信頼された役割に任命されている全ての人員は、GlobalSign の研修及び業務遂行プログラムと同じレベルの技能を保持しているものとする。

信頼された役割の責任を負う者は、GlobalSign 又は RA における変更について可能な限り認識するものとする。オペレーションにおける如何なる顕著な変更がなされても、少なくとも年次の情報セキュリティ研修を含む研修（認知/周知徹底のための）計画を持ち、またこの計画の実行は文書化されるものとする。

5.3.5 職務のローテーション頻度及び順序

GlobalSignは、従業員に関わる如何なる変更も、システムのサービス効率又は安全性に影響するものではないことを保証するものとする。

5.3.6 不正行為に対する処罰

運用処理に関して GlobalSign CP、CPS、又は認証局関連の運用手順が定める規定及びポリシーに違反した人物に対しては、適切な懲罰的処罰が課せられる。

5.3.7 個別契約者の要件

GlobalSignに雇用される個人契約者は認証局の正規従業員と同様の処理、手続き、審査、セキュリティコントロール及び研修に従わなければならないものとする。

5.3.8 個人に付与された書類について

GlobalSignは本CP、該当するCPS、関連する法規、ポリシー又は契約書をその従業員に対して入手可能な状態にするものとする。その他の技術的、運用的及び管理書類（例：管理マニュアル、ユーザマニュアル等）については、信頼された役割に従事する者に対し、職務遂行の目的で提供されるものとする。

全人員について、トレーニング受講の有無及び、受講済みトレーニングのレベルを識別したうえで、文書化の作業が維持継続される。

5.4 監査ログの手続き

5.4.1 記録されるイベントの種類

監査ログファイルは、GlobalSignのセキュリティ及びサービスに関する全てのイベントに関して作成される。セキュリティ監査ログファイルは可能な限り、自動的に収集される。これが困難な場合は、記録帳、紙媒体又はその他の物理的メカニズムが使用される。コンプライアンス監査の期間中は、電子及び非電子に関わらず全監査記録が再取得及び入手可能な状態になるものとする。

GlobalSignは、証明書要求を処理し、証明書を発行するために取られた措置の内容を記録するものとし、これには、証明書要求に関連して生成された全ての情報及び受領した文書、日時、及び関係する職員が含まれる。GlobalSign はこれらの記録を、CA が「はじめに」において定める、関連する CA 監査スキームに準拠していることの証明として、適格監査人に提供するものとする。

GlobalSignは少なくとも以下のイベントを記録するものとする。認証局の主要なライフサイクル管理は以下を含む：

- 鍵の生成、バックアップ、保管、リカバリー、アーカイブ、及び破棄
- 暗号装置ライフサイクル管理
- CA システム機器構成

以下を含む、認証局及び利用者証明書のライフサイクル管理：

- 成功した場合と失敗した場合の両方に対する、証明書要求、更新、Re-Key 要求、及び失効。
- 発行された全ての証明書(失効及び失効した証明書を含む)
- 本 CPS に定める全ての検証活動
- 審査電話の日時、電話番号、電話の受け手、及び審査電話終了後の結果
- 証明書請求の受理及び却下
- 証明書の発行
- 証明書のディレクトリ及び CRL のディレクトリ上の読み取り/書き込み操作の失敗、並びに実際の CRL を含む、CRL 及び OCSP エントリの生成。

以下のようなセキュリティイベント：

- 成功及び不成功の PKI システムへのアクセス試行
- 実行された PKI 及びセキュリティ・システム・アクション
- セキュリティプロファイルの変更
- システムクラッシュ、ハードウェア故障、及びその他の異常
- ファイアウォールとルータのアクティビティ
- 認証局施設への出入

ログエントリには、以下の要素が含まれる。

1. 記入日時

2. 仕訳記入者の本人情報
3. エントリへの説明

5.4.2 ログ処理の頻度

監査ログは定期的に、如何なる悪意ある行為の証拠を確認するため、また重要なオペレーションを追跡するために適切にレビューされるものとする。

5.4.3 監査ログの保有期間

GlobalSign は生成された監査ログを少なくとも 10 年分は保有するものとする。GlobalSign はこれらの監査ログを必要に応じて適格監査人に提供する。

5.4.4 監査ログの保護

全ての保有期間中において、発生イベントは削除又は破壊（長期にわたり使用する媒体への移行を除く）されない方法で記録されなければならない。

イベントは、データの完全性、信頼性及び機密性に変更を加えることなく、許可・信頼の下でアクセスを許可された個人によってのみ、そのプロファイルに関する操作が可能であることが保証される状態で記録されなければならない。

イベントは、改変防止できかつ改ざんを検知できる状態で保護されなければならない。

イベントの記録には、記録の生成日から保存期間の終了日までの間、イベント及びその実行の間において信頼関係があることを証明するため、必ず日付の明記が必要となる。

5.4.5 監査ログバックアップ手続き

監査ログ及び監査概要は安全な場所(例：耐火性の金庫)に、信頼された役割に任命された人員の下、情報発生源となる機器とは分離された状態でバックアップされなければならない。バックアップされた監査ログはその原本と同様に保護されるものとする。

5.4.6 監査ログ収集システム(内部 vs.外部)

監査ログの処理はシステムの起動時に開始され、またシステムの終了時にのみ終了する。監査ログ収集システムは収集されたデータの信頼性及び可用性を保証するものである。監査ログ収集システムは必要に応じてデータの機密性を保護する。万が一監査での収集物を処理中に問題が発生した場合、GlobalSign は問題が解決するまでの間、当該認証局の運用を停止するかどうか判断し、GlobalSign の影響を受ける情報資産所有者に通知する義務がある。

5.4.7 イベント発生要因の対象への通知

規定しない

5.4.8 脆弱性の査定

GlobalSign は下記内容の年次リスク評価を実施する：

1. 証明書のデータ又は証明書の管理プロセスの不正アクセス、開示、悪用、改ざん、又は破壊につながる可能性のある予測可能な社内外の脅威を特定する。
2. 証明書データ及び証明書管理プロセスの機密性を考慮し、上記の脅威の可能性と潜在的な損害を評価する。
3. GlobalSIgn がそのような脅威に対抗するために制定している規程、手順書、情報システム、技術、及び他の取り決めの十分性を評価する。

また、GlobalSign は証明書の発行、製品及びサービスに関する GlobalSign の全資産に対して、脆弱性評価及び侵入テストを定期的に実施するものとする。当査定は、証明書発行処理に対する不正アクセス、改ざん、変更又は破壊を導き出す要因となる内部及び外部の脅威に重点をおくものとする。

5.5 アーカイブ対象記録

5.5.1 アーカイブ対象記録の種類

発行CA及びRAは、署名の正当性及び認証システムを正しい操作を構成しうるに十分な詳細が含まれる記録をアーカイブするものとする。

5.5.2 アーカイブの保有期間

GlobalSign は証明書の申請及び審査に関する全書類及び、全ての証明書かつ失効を、その書類を基にしている証明書の有効期限が切れてから少なくとも 10 年間保持するものとする。

5.5.3 アーカイブの保有

保存が必要とされる期間中、アーカイブは削除もしくは破棄（長期にわたり使用する媒体への移行を除く）されない方法で作成されるとものとする。アーカイブの保護は、データの完全性、正当性、及び機密性を変更することなく、許可された信頼できるアクセスのみが操作を行なえることを証明するものとする。一定期間、原本メディアがデータを保存できない場合は、定期的に新規メディアへアーカイブデータを移行するメカニズムがアーカイブ側により定義されるものとする。

5.5.4 アーカイブ バックアップ 手続き

GlobalSign のオンライン又はオフラインのシステムはバックアップがとられる。

5.5.5 データのタイムスタンプについての条件

データのタイムスタンプに、タイムスタンプサービスが使用されている場合、6.8 項に定義される条件に準拠しなければならない。タイムスタンプの方法に関わらず、全てのログにはイベントの発生時刻データが明示されている必要がある。

5.5.6 アーカイブ収集システム(社内又は社外)

アーカイブ収集システムは、5.3 項に定義されるセキュリティ条件に準拠しなければならない。

5.5.7 取得手続き及びアーカイブ情報の検証

GlobalSign のアーカイブ情報を保存するメディアは、作成にあたり確認される。定期的に、アーカイブ情報の統計サンプルにてデータの継続的な完全性、及び可読性が検証される。

許可された GlobalSign の設備、信頼された役割及びその他許可された人員のみがアーカイブへのアクセスを認められる。

5.6 鍵交換

GlobalSign は定期的に 6.3.2 項に伴い、鍵データを交換する場合がある。証明書のサブジェクト情報についても変更され、また証明書プロファイルも新たなベストプラクティスを守るべく、変更される可能性がある。以前、利用者の証明書を署名していた鍵は全利用者の証明書が期限切れとなるまで維持されるものとする。

5.7 危殆化及び災害からの復旧

5.7.1 インシデント及び危殆化に対応する手続き

GlobalSignは、コンピューティング資産、ソフトウェア又はデータの損壊・損失など、サービスの運営を妨げる、又は損なう事象の発生時に取るべき手段を解説した事業継続計画を構築するものとする。GlobalSignは、ビジネスリスクを評価するためのするリスクアセスメントの実施、災害復旧計画から導き出される必須のセキュリティ要件及びオペレーション手続きの決定を行う。このリスク分析は常時見直し、また必要あれば修正（脅威の進化、脆弱性の発展など）される。この事業継続は8項で述べるように、災害発生及び復旧計画後に、何が最初に保全されるオペレーションであるかを検証するため、監査処理の対象範囲となる。GlobalSignで信頼された役割及びオペレーションに従事する人員は、事業の核心部にあるオペレーションについて、災害復旧計画に規定された手続きに則してオペレーションするために特別に訓練される。

万一、GlobalSignがハッキング又はその他攻撃の可能性と思われる行為を発見した場合、その実態及び被害の程度を知るための調査を行なうものとする。 もしくはGlobalSignにより、認証局又はRAのシステムをリビルド（再構築）する必要性、いくつかの証明書が失効するのみの場合、そして（又は）被害によるCA階層の宣言が必要な場合の判断を行なうために、それぞれの被害の範囲を査定するものとする。 認証局の災

害復旧計画はどのサービスが維持されるべきかを明確化するものとする。（例えば、失効及び証明書のステータス情報）

5.7.2 コンピューティング資産、ソフトウェア、又はデータが損壊した場合

万一いずれかの設備が損壊又は操作不能な状態で、しかしながら秘密鍵が損壊していない場合、GlobalSign の事業継続計画に基づき証明書の状態情報の生成を優先し、可能な限り早急に再構築されるものとする。

5.7.3 秘密鍵が危殆化した際の手続き

GlobalSign の署名鍵が損壊、紛失した、又は破壊された、又は破損されたと考えられる場合：

- GlobalSign は問題の調査の後、GlobalSign 証明書を失効すべきかを判断する。その場合、
  - 証明書を発行された全利用者へ可能な限り最短のタイミングで、通達する。
  - 新規認証局の鍵ペアを生成又は既存の他の CA 階層を代替として使用して新規利用者の証明書を作成する。

5.7.4 災害後の事業継続能力

5.7.1 項に明記されるように、災害事業復旧計画は事業継続について取り決めている。証明書ステータス情報システムは 24 時間 365 日利用可能な状態に展開されるものとする。

5.8 認証局又は RA の稼動終了

発行 CA 又は RA の稼働を終了する必要がある場合には、その終了による影響は、一般的な状況に基づいて判断し、可能な限り最小限にとどめるものとし、また該当の発行 CA 又は RA との契約内容に従う。GlobalSign は、その電子証明書の発行及び管理業務の全部又は一部を終了する場合には、その終了の手順を明示する。その手順は少なくとも次の内容を含む：

- 認証局の終了のために生じる混乱を可能な限り最小限にとどめることを保証すること
- 認証局のアーカイブされたデータが保存されることを保証すること
- 認証局の終了に関する通知が利用者、承認された依拠当事者、アプリケーションソフトウェアプロバイダ、その他 GlobalSign の証明書ライフサイクルに利害関係を有する者に対して速やかに行われることを保証すること
- 認証局の終了後も一定の期間内は証明書の失効情報に関するサービスが引き続き提供及び維持される旨を保証すること。(例えば、証明書ステータス情報を他の GMO インターネットのグループ会社に伝達する場合等がある。)
- GlobalSign で発行された全ての電子証明書を認証局の終了の時点で失効させるための手続が維持されることを保証すること
- eIDAS 適合性評価機関をはじめすべての監査人に通知すること
- 関連法令に従いベルギーの eIDAS 監督機関（経済・中小企業・自営業者・エネルギー省）及びその他の政府証明書関係機関に通知すること

5.8.1 業務を引き継ぐ認証局

実利的かつ合理的な範囲において、後任の認証局は、終了する認証局と同じ権利義務を負うべきである。

6.0 技術的セキュリティ管理

6.1 鍵ペア生成及びインストール

6.1.1 鍵ペア生成

GlobalSign はルート CA の鍵ペアに対し下記の管理を行う：

1. 鍵生成のスクリプトを作成し、それに従う
2. 正規の監査人がルート CA 鍵ペア生成プロセスに立ち会うか、ルート CA 鍵ペア生成プロセス全体のビデオを記録する。
3. 正規の監査人が、鍵生成及び証明書生成プロセス中に GlobalSign がキーセレモニーに従い、鍵ペアの完全性及び機密性を確保するために使用されるコントロールを遵守した旨の報告書を発行する。

その他 CA の鍵ペアに対しては、下記の管理を行う：

1. CP 及び/又は CPS の 5.1 項及び 5.2.2 項に記載されている通り物理的に安全な環境で鍵を生成する
2. 複数の人員による管理及び知識分割という原則の下、信頼された役割に従事する人員が CA の鍵を生成する
3. CA の CP 及び・又は CPS に開示されているように、該当の技術的及び事業要件を満たす暗号モジュール内で CA 鍵を生成する
4. CA 鍵生成に係る作業をログに記録する
5. CP 及び・又は CPS、また（該当する場合）鍵生成スクリプトに記載された手順に準拠して秘密鍵が生成及び保護されているという合理的保証を実現するための有効的なコントロールを維持する

GlobalSign によって生成された利用者鍵については、6.1.5 項及び 6.1.6 項に規定されている鍵生成アルゴリズム及び鍵のサイズを使用して、FIPS 140-2 に準拠した安全な暗号装置において鍵生成が行われねばならない。

GlobalSign は、既知の脆弱な秘密鍵を用いて証明書が申請された場合、その申請を却下するものとする。

GlobalSignは物理的に安全な環境において、信頼された役割に従事している、少なくとも二名の管理下で、全ての発行鍵ペアを生成するものとする。 外部の立会人（理想としては通常日常的に監査を行なう独立監査人）が立会うか、或いはセレモニー全工程がビデオ録画されなければならない。GlobalSignの鍵生成は、少なくともFIPS140－2 レベル3又はそれ以上を満たすデバイスで行なわれるものとする。

6.1.2 利用者への秘密鍵配布

利用者の代理として秘密鍵を生成する GlobalSign は、鍵生成の工程から利用者への証明書発行過程において、十分なセキュリティが保たれている時にのみ、それを担うことができる。公開鍵/プライベート鍵生成に関する暗号アルゴリズム(暗号化、符号、暗号ハッシュ、RNG、PRNG など)は FIPS によって承認され、公開鍵/プライベート鍵生成アルゴリズムも FIPS 186-4 で規定されている。

生成された公開鍵/秘密鍵は、利用者によって提供された暗号コードで暗号化される。暗号化された公開鍵/秘密鍵は、利用者の管理者によって事前に登録されたパスワードによって認証された TLS セッションで配送される。

2018 年 3 月 1 日現在、GlobalSign はパブリックな SSL 証明書のための秘密鍵を生成しない。

6.1.3 証明書発行者への公開鍵配布

発行CAは、RAからの送付中は保護され、またRAがその起点の確実性及び完全性を適切に検証した場合にのみ、公開鍵を受け付けるものとする。RAは利用者からの公開鍵は本CPの3.2.1項に従う場合のみ、受け付けるものとする。

6.1.4 認証局から依拠当事者への公開鍵配布

GlobalSign は鍵のすり替えを防ぐ方法で依拠当事者へ公開鍵の配布することを保証しなければならない。これには、商業ブラウザ及びプラットフォームオペレーターと協力し、ルートストア及び OS にルート証明書公開鍵を組み込む作業を行う場合がある。また、認証局公開鍵の発行は、チェーニング証明書の形式により、又は GlobalSign が操作するレポジトリを介して利用者へ配布、もしくは発行済み証明書のプロファイル内で参照として行なわれる可能性がある。

6.1.5 鍵のサイズ

GlobalSignは米国国立標準技術研究所の推奨するタイムラインに従い、認証局ルート、発行CA、及び利用者に配布されるエンドエンティティ証明書の鍵データの選択に対して最善を尽くす。また発行CAの直接管理下にない、Trusted Rootプログラム下の下位認証局の場合も同様のベストプラクティスが合意の下義務付けられている。

ルート 証明書、発行 CA 証明書、及びエンドエンティティ証明書、並びに CRL/OCSP 証明書ステータスレスポンダにおける、下記の鍵サイズ又はハッシュ アルゴリズムから選択する。これらの選択は、Baseline Requirements 及び EV ガイドラインと整合している。

SSL 証明書はアルゴリズムの種類及び鍵長について、Baseline Requirements Section 6.1.5 の要件を満たさねばならない。

6.1.6 公開鍵パラメーター生成及び品質検査

GlobalSign は FIPS186 の定めに従い鍵ペアを生成し、また利用者から提示される公開鍵が適切であるか、適切な技術を用いて検証するものとする。既知の脆弱な鍵は検証され、また提出時に拒否される。GlobalSign はこれらの質を確認する際、Baseline Requirements Section 6.1.6 を参照する。

6.1.7 鍵の使用目的(X.509 v3 鍵使用フィールドにおいて)

GlobalSign は、申請で提案されるフィールドにしたがい、証明書における鍵の用途を、X.509 v3 鍵使用フィールドにより設定するものとする。（7.1 項を参照）

ルート証明書に紐づく秘密鍵は、以下の場合を除き、証明書に署名する用途では用いられない。

1. ルート CA 自身を表すための、自己署名証明書
2. 下位認証局及び相互認証の証明書
3. インフラストラクチャの目的(管理職の証明書、Internal CA を運営する機器の証明書)を想定した証明書
4. OCSP からのレスポンスを検証する証明書

6.2 秘密鍵保護及び暗号化モジュール技術管理

GlobalSign は、証明書の不正発行を防止するために、物理的及び論理的な対策を実装している。上記に明記された検証済みシステム又は装置以外の CA 秘密鍵の保護は、物理セキュリティ、暗号化、又は両方の組み合わせで構成され、CA 秘密鍵の公開を防ぐ方法で実装されなければならない。GlobalSign は、暗号化された鍵又は鍵部分の残存寿命中、暗号解読攻撃に耐えることができる最先端のアルゴリズム及び鍵長を用いて、その秘密鍵を暗号化する。

6.2.1 暗号化モジュール規定及び管理

GlobalSignは証明書、CRLの署名又はOCSPのレスポンスを生成する全システムにおいて、少なくともFIPS140－2 レベル3の暗号保護を使用していることを保証するものとする。 GlobalSignは利用者に対して、FIPS140－2 レベル2もしくはそれ以上のシステムを秘密鍵の保護に使用することを要求、また利用者が保護を保証するために当該システムもしくは適切なメカニズムを使用することに合意の上で責任を持つことを定める。これは例えば適切なCSP（暗号化サービスプロバイダ）が、登録処理の一環として既知のFIPSに準拠したハードウェアプラットフォームへ繋げるなどの限定的処置で達成可能となり得る。

6.2.2 秘密鍵(m 中の n) 複数の人員による管理

GlobalSignは、信頼された役割において職務を担う複数の人員による管理の下、秘密鍵を暗号化操作のためにアクティブに（認証局アクティブ化データを使用）するものとする。この秘密鍵の複数人員による管理に携わる信頼された役割は、強力に認証される。（例: PINコード及びトークン）

6.2.3 秘密鍵の第三者委託

GlobalSign は、如何なる者に対しても秘密鍵を第三者委託するものではない。

6.2.4 秘密鍵のバックアップ

GlobalSignは災害時事業継続計画の目的のため、原本の秘密鍵と同様に複数人員の管理下の元バックアップを行なうものとする。

6.2.5 秘密鍵のアーカイブ化

GlobalSign のデジタルサイニングサービス(DSS)を除き、GlobalSign は利用者の秘密鍵のアーカイブを行なわず、秘密鍵の生成過程で鍵が存在していた可能性のある一時的な記憶場所からも削除されることを保証する。

6.2.6 暗号モジュール間の秘密鍵移行

GlobalSign の秘密鍵は、ハードウェアセキュリティモジュールにおいて生成、アクティブ化、及び保存されている。秘密鍵がハードウェアセキュリティモジュールの外(保存又は移行のため)にある場合は、暗号化されていることが必須となる。秘密鍵は、暗号モジュール外の環境にて、一般テキスト状態で存在しては絶対にならない。
万が一、下位 CA の秘密鍵が許可されていない人物又は利用者と関連のない組織に付与されたことを GlobalSign が認識した場合、GlobalSign は付与された秘密鍵に対応する公開鍵を含む全ての証明書を失効させる。

6.2.7 暗号モジュールにおける秘密鍵の保存

GlobalSign は少なくとも FIPS140－2 レベル 3 もしくはそれ以上の規格において保存するものとする。

6.2.8 秘密鍵のアクティブ化方法

GlobalSign はハードウェアセキュリティモジュールの製造元が提供する仕様説明書に従い、秘密鍵をアクティブ化する責任を有する。利用者は、利用契約及び利用に関する合意書に示される責務に従って、秘密鍵を保護する責任を有する。

6.2.9 秘密鍵の非アクティブ化方法

GlobalSign はアクティブ化されたハードウェアセキュリティモジュールを放置せず、また不正アクセスが可能な状況にしないことを保証するものとする。GlobalSign のハードウェアセキュリティモジュールがオンラインかつ操作可能な間、証明書及び認証済み RA からの CRL/OCSP の署名にのみ使用される。認証局が運営停止となる際、その秘密鍵はハードウェアセキュリティモジュールから削除される。

6.2.10 秘密鍵の破棄方法

GlobalSign の秘密鍵は、不必要となった時点もしくは対応する証明書が期限切れ又は失効した際に破棄される。秘密鍵を破棄するにあたり GlobalSign は秘密鍵の如何なる部分も推定されないよう、HSM 内の関連する認証局の秘密アクティブ化データ全てを破棄する必要がある。

GlobalSign が生成した秘密鍵は、鍵ペアが利用者に取得されるまでの間 PKCS 12 形式で GCC に保管される。利用者の鍵ペアは、利用者が鍵ペアを受け取った時点、又は鍵生成から 30 日経過した時点で自動的に消去される。利用者の秘密鍵はその他の GlobalSign のシステムでは保管しないものとする。

6.2.11 暗号モジュール 評価

6.2.1 項を参照

6.3 その他鍵ペア管理の要素

6.3.1 公開鍵のアーカイブ化

GlobalSign は証明書の公開鍵をアーカイブ化しなければならない。

6.3.2 証明書の操作可能期間及び鍵ペアの使用期間

GlobalSign が認証及び更新する証明書は最長で下記に述べる有効期間を持つものとする。

種類	秘密鍵　用途	最長の有効期間
Root Certificates[2]	25 年	30 年
TPM Root Certificates	30 年	40 年
Publicly Trusted Sub-CAs/Issuer CAs	規定無し	17 年
Trusted Root	規定無し	10 年
PersonalSign Certificates	規定無し	39 ヶ月
Noble Energy Certificates	規定無し	5 年
Code Signing Certificates	規定無し	39 ヶ月
EV Code Signing Certificates	規定無し	39 ヶ月
AATL End Entity Certificates	規定無し	39 ヶ月
Qualified Certificate for Electronic Seals and Qualified Certificate for Electronic Signatures	規定無し	39 ヶ月
DV SSL Certificates	規定無し	825 日
AlphaSSL Certificates	規定無し	825 日
OV SSL & ICPEdu Certificates	規定無し	825 日
Intranet SSL	規定無し	5 年
EV SSL Certificates	規定無し	27 ヶ月
Timestamping Certificates	11 年	11 年
PDF Signing for Adobe CDS Certificates	規定無し	39 ヶ月

[2] *RSA によって 2003 年以前に生成された 2048 の鍵については、ハードウェア、ルートストア、及び OS における鍵長の制限のため用途が制限されており、利用可能年数を 25 年としている。*

NAESB Certificates	2 年	2 年
Qualified Website Authentication Certificates	規定無し	27 ヶ月

鍵ペアの使用期間は、最大で証明書と同じ有効期間に設定することができる。

特定の CA によって署名された証明書は、その鍵ペアの運用期間終了までに失効しなければならない。

GlobalSign 証明書は、最長有効期間に関し Baseline Requirements に準拠しなければならないため、それに従って証明書の有効期間を短縮する場合がある。利用者の証明書がそれよりも短い有効期間の場合は、期限が切れた後に元々の有効期間まで再発行が可能となる。
現行又は将来の Baseline Requirements が、証明書が最初に発行された時点では実施されていなかった証明書発行に対して認証権限に要件を課す場合、特に再発行の申請がなされた場合においては、利用者が最大の有効期間を享受できないことがある。
例：ある証明書の種類について本人確認及び権限の認証に対する追加要件が含まれる場合、又は最大の有効期間が短縮される場合。

6.4 アクティブ化データ

6.4.1 アクティブ化データ生成及びインストール

GlobalSign の秘密鍵をアクティブ化するために使用される、GlobalSign のアクティブ化データの生成及び使用はキーセレモニー（6.1.1 項を参照）中に行なわれるものとする。アクティブ化データは適切な HSM（ハードウェアセキュリティモジュール）により自動的に生成され、また信頼された役割を担う持分所有者に配布されなければならないものとする。配布方法においては、アクティブ化データの機密性及び完全性が保持されなければならない。

6.4.2 アクティブ化データの保護

発行 CA のアクティブ化データは、暗号及び物理的なアクセス管理の仕組みを介した漏洩から保護されなければならない。GlobalSign のアクティブ化データはスマート カードに格納されなければならない。

6.4.3 その他のアクティブ化データの要素

発行 CA のアクティブ化データの保持は、信頼された役割に従事する GlobalSign の人員に限定しなければならない。

6.5 コンピュータ セキュリティ コントロール

6.5.1 特定のコンピュータ セキュリティ技術条件

下記のコンピュータ セキュリティ機能はOS、又はOS、ソフトウェア及び物理的防御の組み合わせのいずれかにより提供されなければならない。GlobalSignのPKI構成は下記の機能を必ず含むものとする。

- 信頼された役割に対する認証済みログインを要求
- 最小限の権限と共に、任意のアクセスコントロールを提供する
- セキュリティ監査能力を提供（完全性が保護されていること）
- 対象物の再利用を禁止する
- 強固なパスワードを使用する方針を要求する
- セッション中のコミュニケーションに対して暗号使用を要求する
- 本人識別及び認証には、信頼済みパスを要求する
- 悪意あるコードを防止する手段を提供する
- ソフトウェア及びファームウェアの統合性を維持する手段を提供する
- 処理に対してドメインを分離し、システム及びプロセスを区分する
- OSに対して自己防御を提供する

証明書発行を直接的に引き起こすことのできるアカウントについては、GlobalSign は、多要素認証を実施するものとする。

6.5.2 コンピュータ セキュリティの評価

GlobalSign の PKI を構成するソフトウェアは全て、適切な対象者によるプロファイル保護の条件に準拠しなければならない。

6.6 ライフサイクル技術管理

6.6.1 システム開発管理

GlobalSign におけるシステム開発管理は以下の通り。

- 正式かつ書面化された開発方法にて設計並びに開発されたソフトウェアを使用しなければならない。
- 入手したハードウェア及びソフトウェアは、どんな特殊なコンポーネントが意図的に混入される可能性を低減する方法において購入されたものであること。（例: 購入時に機器が無作為に選択されたものであることを確認するなど）
- ハードウェア及びソフトウェアが管理された環境において開発され、その開発プロセスが定義・文書化されていること。この条件は商業的に流通するハードウェア及びソフトウェアには適用されない。
- 全てのハードウェアは、購入場所から運用場所まで一連の継続した責任体制を保証できる、管理された方法を介して配送又は配布されなければならない。
- これらのハードウェア及びソフトウェアで行なう業務は認証局の業務に限定される。認証局の運営に属さないアプリケーション、ハードウェア デバイス、ネットワーク接続又はインストールされたソフトウェアは存在しない。
- 正しい管理方法により不正なソフトウェアの機器への搭載を防いでいる。認証局の業務を行なうのに必要なアプリケーションのみが機器にインストールされ、ローカルポリシーにより認可されたソースから入手可能となる。GlobalSign のハードウェア及びソフトウェアは、最初の使用時及びその後は定期的に不正コード探知のためにスキャンされる。
- ハードウェア及びソフトウェア 更新版は、元の機器と同様の条件で購入又は開発され；また信頼され教育を受けた人員によって、定められる条件に基づきインストールされる。

6.6.2 セキュリティ マネージメント コントロール

GlobalSignシステムの設定は、いずれの変更及び更新と同様に書面化され、GlobalSignの管理・経営陣により管理されるものとする。GlobalSignのソフトウェア又は設定に対する不正な変更を検知するための仕組みを持つ。 正式な設定管理技法がGlobalSignシステムの導入及び稼働中の保守において使用されている。最初にGlobalSignのソフトウェアが起動される際、業者から納入された通りであり、変更がなされていないか、更に使用目的のバージョンであるかの確認がなされる。

6.6.3 ライフサイクル セキュリティ コントロール

GlobalSign は、評価また認証されたソフトウェア及びハードウェアの信頼度を維持するため、保守スキームを継続的に監視する。

6.7 ネットワーク セキュリティ コントロール

GlobalSign の PKI 構成は、これらがサービスへの妨害（停止）や侵入攻撃から守られていることを保証するため、適切なセキュリティ対応が導入されるものとする。このようなセキュリティ対応策には、ガードの使用、ファイヤウォール及びルーターのフィルタリングを含む。使用されていないネットワークポート及びサービスは遮断する。PKI 機器がホストされているネットワークを保護する目的で使用されるいずれの境界コントロールデバイスも、同じネットワーク上のその他機器においてその他サービスが有効化されていたとしても、PKI 機器に必要なサービス以外は全て拒否する。

6.8 タイムスタンプ

GlobalSignの全コンポーネントは常時原子時計又はネットワーク タイム プロトコル（NTP）のような時刻サービスと同期するものとする。信頼できる時刻の提供に専門の権威（タイム スタンピング オーソリティ等）が使用される可能性も有る。タイムサービス由来の時刻は以下の時刻を構成するのに使われるものとする。

- CA証明書の初期検証時刻
- CA証明書の失効
- CRLの掲示
- 利用者のエンドエンティティ証明書の発行

システム時刻の保守には電子的又は手動的手続きが適用される。時刻の調整は監査対象イベントとなる。

7.0 証明書、証明書失効リスト、及びオンライン証明書ステータスプロトコルのプロファイル

7.1 証明書プロファイル

7.1.1 バージョン番号

GlobalSign は、X.509 バージョン 3 に従ってデジタル証明書を発行するものとする。

7.1.2 証明書拡張子

GlobalSign は、RFC5280 及び受け入れ可能なベストプラクティスに従い、デジタル証明書を発行するものとする。名前の制限（NameConstraints）が設定された場合、依拠当事者を不要なリスクから守るために、重要度（クリティカリティ）についてはベストプラクティスに従って設定される。

7.1.3 アルゴリズム対象識別

GlobalSign は、下記の OID（管理情報識別子）に示されるアルゴリズムでデジタル証明書を発行するものとする。

SHA1WithRSAEncryption	{iso(1) member - body(2) us(840) rsadsi (113549) pkcs(1) pkcs - 1(1) 5}
SHA256WithRSAEncryption	{iso(1) member - body(2) us(840) rsadsi (113549) pkcs(1) pkcs - 1(1) 11}
SHA384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
ECDSAWithSHA1	{iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) 1 }
ECDSAWithSHA224	{iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 1 }
ECDSAWithSHA256	{iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 2 }
ECDSAWithSHA384	{iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 3 }
ECDSAWithSHA512	{iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 4 }
RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsassa-pss(10)}

7.1.4 名称形式

GlobalSign は、RFC 5280 に準拠した名称形式と SSL 証明書及びパブリックなルートにチェーンする EV CodeSigning 証明書に関する CA/B Forum の Baseline Requirements の 7.1.4 項に準拠した証明書を発行しなければならない。
証明書発行者の識別名は、RFC5280 の 4.1.2.4 節に規定される Name フィールドのチェーンをサポートするために、GlobalSign のサブジェクト DN と一致しなければならない。

7.1.5 名前の制限

GlobalSign は必要に応じて名前の制限(NameConstraints)を適用して下位認証局証明書を発行し、また TrustedRoot プログラムの一部として必要な場合にはそれを重要度として設定する。下位認証局に名前の制限(NameConstraints)が設定されていない場合、その CA は CP の 8.0 項に記載されている全面監査の対象に含まれなければならない。

7.1.6 証明書ポリシー識別子

GlobalSign は CA/B Forum Baseline Requirements の Section 7.1.6 に従う。

7.1.7 ポリシー制約拡張の使用

規定しない

7.1.8 ポリシー修飾子の構成と意味

GlobalSign は、依拠当事者がそれを受け入れ可能かどうかを判断できるように、ポリシー修飾子と適切なテキストを含めた形でデジタル証明書を発行する。

7.1.9 クリティカルな証明書ポリシー拡張についての解釈方法

規定しない

7.1.10 シリアル番号

各発行 CA は、CSPRNG からの最低 64 ビットのアウトプットを含む、0 以上の連番でない独自の（発行者サブジェクト識別名及び CA 証明書シリアル番号内のコンテクスト）証明書シリアル番号を含む証明書を発行しなければならない。

7.1.11 適格署名に関する特則

7.1.11.1. 適格署名

適格署名は以下の適格ステートメントを含む：

- esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
- esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD }
- id-etsi-qcs-QcSSCD OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
  esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED BY id-etsi-qcs-QcType }
  Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 } QcType::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-esign)

7.1.11.2. 適格シール

適格シールは以下の適格ステートメントを含む：

- esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
- esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD }
- id-etsi-qcs-QcSSCD OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
- esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED BY id-etsi-qcs-QcType }
  Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 } QcType::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-eseal)

7.1.11.3. 適格ウェブ認証証明書

適格ウェブ認証証明書は以下の適格ステートメントを含む：

- esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
- id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }
- esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED BY id-etsi-qcs-QcType } Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 } QcType::= SEQUENCE { qcType OBJECT IDENTIFIER {{id-etsi-qct-web}}}

7.2 証明書失効リストのプロファイル

7.2.1 バージョン番号

GlobalSign は RFC5280 に従い、バージョン 2 の CRL を発行するものとする。

7.2.2 証明書失効リスト及び証明書失効リストエントリ拡張子

CRL には以下の拡張が備わっている：CRL Number、Authority Key Identifier

7.3 OCSP プロファイル

GlobalSign は、RFC2560 又は 5019 に従い、OCSP のレスポンダを提供する。

7.3.1 バージョン番号

発行 CA はバージョン 1 の OCSP レスポンスを発行する。

7.3.2 オンライン証明書ステータスプロトコル 拡張子

規定しない

8.0 準拠性監査及びその他の評価

本 CP を含む、GlobalSign 運用が関与する複数の垂直的 PKI 業界に対する PKI 標準のうち、現状で適用可能な部分について網羅している。dNSNameConstraints による制約を受けない GlobalSign は、下記の規定について準拠性監査を受ける：

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities
- AICPA/CICA WebTrust for Certification Authorities – Extended Validation Audit Criteria
- AICPA/CICA WebTrust Principles and Criteria for Certification Authorities – Code Signing
- AICPA/CICA WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing
- AICPA/CICA WebTrust for Certification Authorities – SSL Baseline with Network Security
- Regulation (EU) No. 910/2014 (eIDAS)

8.1 評価の頻度及び状況

GlobalSign は、適格監査人を介して、AICPA は 1 年に 1 度、eIDAS は 1 年に 2 度、上述の AICPA/eIDAS の標準への準拠性について継続的に評価するものとする。

8.2 評価者の身元及び能力

GlobalSignに適用される監査は公認監査人により行なわれるものとする。適切な監査人とは、以下の条件及び技能を有する人物、法人、又は複数の人員及び複数の法人を意味する。

- 監査対象からの独立性
- 的確な監査スキームに明記される条件において、監査を遂行できる能力
- PKI技術、情報セキュリティ・ツール及び技術、IT及びセキュリティ監査、更に第三者を認証する機能について審査するにあたり、熟練した人員を雇用している
- 資格、認定、認可を有するもの、又は監査スキームに基づいた監査人の能力条件を満たすと評価される者。
- 法律、公的規定又は職種倫理規定により認定されている者
- 政府内監査機関の場合を除き、業務上の責任/過失・不備に対する、少なくとも 100 万米ドル($1,000,000)を填補限度額とする保険を保持する。

eIDAS は、ETSI EN 319 403 に定められた EN ISO/IEC 17065、特に、eIDAS 規則(EU)No 910/2014 に定義された要件に基づいて、欧州連合加盟国の認定機関により認定された適合性評価機関により監査が実施される。

8.3 評価者と被評価者との関係

GlobalSign は、GlobalSign とは完全に無関係の独立性を有する監査人もしくは評価者を選択しなければならない。

8.4 評価対象項目

監査は、評価が作成された監査スキームの定める条件を満たさなければならない。これらの要件は、監査スキームの変更に伴って、更新される可能性がある。更新された監査スキームは、それが採用された次年度から、GlobalSign に対して適用可能となる。

8.5 結果が不備である場合の対応

準拠性に不備があると提示された場合、相互認証発行 CA を含む、技術制約を受けない発行 CA はいずれも同様に、外部の監査人によって作成される適切な修正計画により不備を除去するために対応しなければならない。

8.6 結果についての連絡

監査結果は、分析及び是正措置による不備の解消のために、GlobalSign Policy Authority に報告されなければならない。当該結果は、法律、規則又は契約により、結果の写しを入手する権利を有するその他の適当な

事業体にも提供することができる。GlobalSign の WebTrust 監査報告書は以下を参照：https://www.globalsign.com/en/repository/

8.7 自己監査

GlobalSign は、発行された証明書のうち、少なくとも 3%(EV SSL 証明書及び EV Code Signing 証明書については 6%)の無作為に選択された証明書に対して、少なくとも四半期ごとに自己監査を実施することにより、CP、CPS、及び「確認事項」の項に明記されたその他外部要件の準拠性を監視し、サービス品質を厳格に管理する。

9.0 その他ビジネス及び法的事項

9.1 費用

9.1.1 証明書発行や更新費用

GlobalSign は証明書の発行及び更新に対して費用を請求できるものとする。また GlobalSign は、再発行及び Re-key についても同様に請求できるものとする。費用及び関連する情報、条件は申請者に対して明確に提示されるものとする。

9.1.2 証明書アクセス費用

GlobalSign は発行済み証明書を格納するデータベースへのアクセスに対して、費用請求できるものとする。

9.1.3 失効情報アクセスに関する費用

非常に多数の依拠当事者を有する利用者で、かつ、GlobalSign の証明書ステータス管理設備の負荷軽減のための技術である“OCSP ステープリング”や、それに類する対策を採用しようとしない利用者に対しては、発行 CA は負荷処理のための追加費用を請求できるものとする。

9.1.4 その他サービスの費用

GlobalSign はタイムスタンピングなどのその他追加サービスに対しては、これを請求できるものとする。

9.1.5 返金ポリシー

GlobalSign は利用者に対し、返金ポリシーを提案できる。返金ポリシーの行使を選択する利用者は、その選択時点で全ての発行済み証明書を失効していなければならない。

9.2 財務上の責任

9.2.1 保険の適用範囲

名称制約が課されていない場合の発行CAに関しては、少なくとも200万米ドル上限ポリシーの一般賠償責任保険を、また業務過誤や専門職業人賠償責任保険については、少なくとも500万米ドル上限ポリシーの保険を保有するものとする。発行CAの保有する保険のカバー範囲は：1)EV証明書の発行及び維持における行動、過失、不備、意図的ではない契約違反や不履行に対する損害請求、 2)如何なる第三者の所有権の侵害（コピーライト、特許、及び商標の侵害を除く）、プライバシーの侵害、及び広告侵害により生じた損害に対する請求、である。
保険会社は、現行版の最良の保険ガイド（又は格付け対象企業を会員とする企業団体）において評価が A-よりも上の評価を受けた会社であり、ここを通じて保険が提供されるものとする。

9.2.2 その他資産

規定しない

9.2.3 エンドエンティティに対する保険又は保証

GlobalSign は利用者に対して保証ポリシーを提供することができる。

9.3 業務情報の機密性

9.3.1 機密情報の範囲

GlobalSign は、CPS において機密情報の範囲を定義づけるものとする。

9.3.2 機密情報の範囲外に属する情報

CPS において機密情報であると定義されない情報は、公開情報とみなされる。証明書のステータス情報及び証明書そのものは公開情報とみなされる。

9.3.3 機密情報保護の責任

GlobalSign は機密情報を保護するものとする。GlobalSign は従業員、代理人、及び契約社員に対する研修と契約によって、機密情報を保護するものとする。

9.4 個人情報保護

9.4.1 保護計画

GlobalSign は本 CP に適切なレポジトリにおいて発行される個人情報保護規定に従い、個人情報を保護するものとする。

9.4.2 個人情報として取り扱われる情報

GlobalSign は申請者から受領する全ての情報を個人情報として取り扱い、通常証明書に記載しないものとする。この条件は、申し込みが受領され、デジタル証明書が発行された申請者及び、申し込みが却下された申請者に適用される。GlobalSign は情報へアクセス時に必須となる扱い注意及び注意喚起の研修を、情報に携わる全要員と同様に、全ての RA 及び点検要員に対しても、定期的行なうものとする。

9.4.3 個人情報とみなされない情報

証明書のステータス情報及び全ての証明書の内容は個人情報ではないとみなされる。

9.4.4 文書変更管理

GlobalSign は個人情報保護規定に従って、紙媒体又はデジタル形式に関わらず、受領した個人情報を安全に保管する責任を負う。如何なる個人情報のバックアップも、適切なるバックアップメディアに対し、その情報が移行される際には暗号化されていなければならない。

9.4.5 個人情報使用についての通知及び合意

申し込み及び登録処理中に、申請者から受領した個人情報は、非公開情報であるとみなされ、このような情報の使用に関しては、申請者から許可を得る必要がある。GlobalSign は、GlobalSign が提供する製品又はサービスの検証処理に利用する第三者から提供された追加情報に対しては、利用約款にその取扱い関連条項を盛り込むこととする。

9.4.6 法的又は管理処理に従う開示

GlobalSign は、法令により開示要求があった場合には、申請者又は利用者に対して通知することなく、個人情報を開示することが可能である。

9.4.7 その他情報開示の場合

規定しない

9.5 知的財産権

GlobalSign は第三者の知的財産権を、故意に損わないものとする。公開鍵及び秘密鍵はそれを正当に保持するところの利用者の財産権に属する。GlobalSign は証明書の所有権を保持するが、完全な形で複製・配布される場合に限り、非独占的かつ無償という条件にて証明書の複製・配布を許可する。

9.6 表明保証

9.6.1 認証局の表明保証

GlobalSign は、本 CP 及び該当する利用契約をもって、利用者及び依拠当事者に対し、発行済み証明書の使用に関する法的条件を告知する。表明保証を行う関係者には、GlobalSign 、RA、利用者、依拠当事者及びその他必要となる関係者が含まれる。発行 CA、RA、利用者を含む全ての関係者は、自己の秘密鍵の完全性について保証する。いずれの関係者も、万一秘密鍵の危殆化が発生したと疑われる場合は、直ちに該当する RA へ通知するものとする。

GlobalSign は証明書受益者に対して、証明書が有効である間、GlobalSign が証明書の発行と管理において、以下の内容を含む、CP 及び CPS に準拠していることを表明及び保証する：

- ドメイン名或いは **IP** アドレスの使用権**:** 証明書発行時点において、GlobalSign が
  (i) 証明書のサブジェクトフィールド或いはサブジェクト別名フィールドに格納されるドメイン名及び IP アドレスの使用権或いは管理権限を申請者が有している(或いはドメイン名のみの場合、使用権或いは管理権限を有する者からそれらの権利や管理を委譲されている)ことを検証する手続きを実施していること
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や CPS に明確に記述されていること(3.2 項を参照のこと)
- 証明書の承認 **:** 証明書発行の時点において、GlobalSign が
  (i) サブジェクトが証明書の発行を承認しており、申請代行者がサブジェクトに代わって証明書の発行を要求することを承認されていることを検証する手続きを実施していること
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や CPS に明確に記述されていること(3.2.5 項を参照のこと)
- 情報の正確性**:** 証明書発行の時点において、GlobalSign が
  (i) 証明書に格納される全ての情報(但し organizationalUnitName 属性を除く)の正確性を検証する手続きを実施していること
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や CPS に明確に記述されていること(3.2.3 及び 3.2.4 項を参照のこと)
- 誤解を招く情報がない**:** 証明書発行の時点において、GlobalSign が
  (i) 証明書のサブジェクトの organizationalUnitName に誤解を招くような情報が含まれる可能性を低減するための手続きを実施していること
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や CPS に明確に記述されていること(3.2.3 及び 3.2.4 項を参照のこと);
- 申請者の身元**:** 証明書がサブジェクトの身元情報を含む場合、GlobalSign が
  (i) 申請者の身元情報を検証するための手続きを実施していること
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や CPS に明確に記述されていること(3.2.3 及び 3.2.4 項を参照のこと);
- 利用契約**:** GlobalSign と利用者が関連会社でない場合、申請者と CA とは、Baseline Requirements を満たす適法かつ強制力のある利用契約にて位置づけられていること。或いは、両者が関連会社の関係ならば、申請代行者は当使用条件(4.5.1 項を参照)を認め、受諾すること
- ステータス**:** GlobalSign は全ての有期間中の証明書のステータス(有効か失効されたか)に関する現在の情報を 24 時間 365 日公的にアクセス可能な状態に維持すること
- 失効**:** GlobalSign は、Baseline Requirements、EV ガイドライン、また EV Code Signing ガイドラインにて定義されたいずれの失効要件に該当する証明書についても失効すること(該当する場合)(4.9.1 項を参照のこと)

さらに、GlobalSign は、NAESB 証明書の証明書受益者に対し、証明書が有効な間、GlobalSign が証明書の発行及び管理において CP 及び CPS に準拠していることを表明し、保証する。

- **NAESB** WEQ-PKI Standards に基づき、証明書を発行、また管理すること
- 利用者を識別及び証明書を発行する際、NAESB WEQ-PKI Standards の全要件に従っていること
- RA が証明書において検証した事項において、RA が知り得ているところの、或いは当然知り得るはずの虚偽表示がないこと
- 申請者から提供された情報が、正しく証明書に記載されていること
- 証明書が NAESB WEQ-PKI Standards の不可欠な要件を満たしていること

上記の保証に代えて、GlobalSign は、本証明書が有効である間、証明書の発行及び管理、並びに EV 証明書及び EV Code Signing 証明書に含まれる情報の正確性の検証において、GlobalSign が本 CP 及び CPS に従っていることを、EV 証明書及び EV Code Signing 証明書の受益者に対して表明し、保証する。

- 法的存在**:** GlobalSign は、証明書が発行された日現在、当該証明書に記名されているサブジェクトが設立又は登録管轄区域内で有効な団体又は事業体として法的に存在することを、そのサブジェクトの設立又は登録管轄区域内の設立又は登録機関と確認する。

- 識別**:** GlobalSign は、証明書が発行された日現在、証明書に記名されているサブジェクトの正式名称が、サブジェクトの設立又は登記管轄区域における設立又は登記機関の公式記録に記されている名称と一致していること、及び仮名が含まれている場合、その仮名がその事業所の管轄区域において、サブジェクトにより適切に登録されていることを確認する。
- ドメイン名を使用する権利**:** EV 証明書についてのみ、GlobalSign は、証明書が発行された日現在、証明書に記名されているサブジェクトが、証明書に記載された全てのドメイン名を使用する権利を有することを確認するために、合理的に必要な全ての措置を講じる。
- EV 証明書の発行許可：GlobalSign は、証明書に記名されているサブジェクトが証明書の発行を許可したことを確認するために、合理的に必要な全ての措置を講じる。
- 情報の正確性: GlobalSign は、証明書が発行された日現在、証明書内の全ての情報が正確であることを検証するために合理的に必要な全ての措置を講じる
- 利用契約**:** 証明書に記名されているサブジェクトは、法的に有効かつ強制力のある利用契約を、該当ガイドラインの要件を満たす CA と締結する、又は、関連会社の場合、申請者の代表者は、利用条件を確認、同意する。
- ステータス**:** GlobalSign は、EV 及び EV Code Signing ガイドライン(該当する場合)の要件に従い、年中オンラインアクセス可能なレポジトリにおいては、証明書の有効又は失効のステータスに関する最新の情報を維持する。
- 失効**:** GlobalSign は、EV 及び EV Code Signing ガイドラインの要件に従い、EV 及び EV Code Signing ガイドラインに明記された失効理由のいずれかに基づき、証明書を失効する。

9.6.1.1 NAESBE（北米エネルギー規格委員会）証明書に対する認証局の表明保証

NAESB WEQ-PKI（NAESB 認証局ルール）は、NAESB 発行 CA が以下の項目を保証することを要求している：

- NAESB Business Practice Standardsに基づき、証明書を発行、また管理すること
- 利用者の識別、及び証明書発行の際、NAESB Business Practice Standardsの全要件に従っている
- 証明書において検証した事項において、RAが知得した、或いは当然知られるであろう誤記や誤りがないこと
- 申請者から提供された情報が、正しく証明書に記載されていること
- 証明書がNAESB Business Practice Standardsの不可欠要件を満たしていること

9.6.2 RA の表明保証

GlobalSign は全 RA に対し、当該 RA が本 CP 及び関連する CPS に準拠していること、及びその CPS もしくは RA 契約書内にさらに付加的な表明事項を含めうることを自ら保証するよう要求する。

9.6.3 利用者の表明保証

本 CP に特別記述が無い限り、利用者は下記の項目に責任を有する。

- **情報の正確性:** 利用者は、証明書リクエスト及び証明書の発行に関連して発行側認証局(CA)から別段の要求があった場合、常に、正確かつ完全な情報を発行側認証局(CA)に提供する。
- **秘密鍵の保護:** 申込者は、要求された証明書及び関連するアクティブ化データ又は装置(例えば、パスワード又はトークン)に含まれる秘密鍵を常に独占的に管理し、秘密を保持し、適切に保護するためのあらゆる合理的な措置を講じるものとする。
- **証明書の受領:** 利用者は、証明書内容の正確性を確認し、検証する。
- **証明書の利用:** 利用者は、証明書に記載されている subjectAltName でアクセス可能なサーバにのみ SSL 証明書をインストールし、適用される全ての法律を遵守し、利用契約を単独で遵守して証明書を使用するものとする。
- **報告及び失効:** 利用者は、(a)証明書に含まれる公開鍵に関連する利用者の秘密鍵の実際の又は疑わしい誤用又は危殆化がある場合、直ちに証明書の取消を要求し、その秘密鍵及びその関連秘密鍵の使用を中止する;及び(b)証明書内の情報が不正確又は不正確であるか又は不正確となった場合、直ちに証明書の取消を要求し、その使用を中止する
- **証明書の有効期限:** 利用者は、当該証明書が取り消された時点で、証明書における公開鍵に関連する秘密鍵の使用を直ちに中止するものとする。
- **責任:** 利用者は、48 時間以内に、「危殆化」又は「証明書」の誤用に関する GlobalSign の発行指示に応答するものとする。
- **通知及び受領:** 申込者は、申込者が利用契約に違反した場合、又は証明書がフィッシング攻撃、詐欺、マルウェア配信などの犯罪行為を可能にするために使用されていることを発見した場合、申込者が直ちに証明書を取り消す権利を有することを認識し、承諾する。

9.6.3.1 NAESB（北米エネルギー規定委員会）の利用者

NAESB WEQ PKI Standard に加入する利用者は NAESB EIR に登録し、電気再販業務に従事することが許可されていることを提示しなければならない。また、NAESB WEQ PKI Standard に定められた認証方法を利用したアプリケーションにアクセスする必要があるが、電気再販業者の資格を持たないエンティティや組織(規制当局、大学、コンサルティング会社等)も NAESB EIR に登録する必要がある。

登録されたエンドエンティティ及びそのユーザコミュニティは、NAESB WEQ PKI Standard に定められたエンドエンティティの責任を全て果たす必要がある。

各利用者組織は NAESB WEQ PKI Standard に定められている以下の責任について理解していることを、GlobalSign を通じて示さなければならない。

各利用者組織は以下の WEQ-012 の項目を確認し、同意していることを認証局に対して証明しなければならない。

- 利用者は、電気業界が以下の目的で安全なプライベート電気通信を必要としていることに同意していること。
- 機密性：意図した受信者以外にデータが読み取られることがないという保証
- 認証：エンティティが主張する存在(組織、個人)が正確であるという保証
- 完全性：通信前後、もしくは過去から現在までの間に(意図的に、又は意図せずに)データが改ざんされていないという保証
- 否認防止：取引先が、取引を行ったこと、或は電子メールの送信を行ったことについて、あとからそれを否認することをできなくすること。
- 利用者は電気再販業界が公開鍵暗号方式(公開鍵証明書を利用し、個人やコンピュータシステムをエンティティに紐づけること)を利用することについて同意していること。
- 利用者が利用する認証局のCPSを認証局の認める業界基準に照らして評価していること。

利用者は法的所在地を登録し、NAESB の EIR に登録され、利用者申請時や発行時に使用するための「エンティティコード」を確保しなければならない。

利用者は以下の要件にも準拠しなければならない：

- 自分の秘密鍵を他者からのアクセスから保護すること
- 該当する場合、NAESB EIR を介して、利用者自らが GlobalSign を正式な認証局として選択したことに相違ないことを明らかにすること。
- GlobalSign がエンドエンティティに安全な電子通信を提供するために必要な CPS に規定されている通り、全ての同意書及び契約書に準拠すること。
- CPS に規定されている全てエンドエンティティの責任に準拠すること(証明書申請手続き、申請者識別証明/審査、及び証明書管理手続き等)
- PKI 証明書管理プログラムがあり、プログラムに参加する全ての従業員がトレーニングを受けること、また、当該プログラムへ準拠していることを確認すること。PKI 証明書管理プログラムは以下を含むが、それに限定されない。
    - 証明書秘密鍵セキュリティ及び運用手続き
    - 証明書失効ポリシー
- 利用者の本人確認情報を識別し(個人、役職、デバイス、もしくはアプリケーション等)、完全かつ正確な情報を証明書申請の際に提供すること

9.6.4 関係者の表明保証

GlobalSign の証明書を参照（依拠）する依拠当事者は下記の項目を保証する。

- 証明書を使用する技術的能力を有している
- GlobalSign 及び依拠当事者に関連する諸条件についての通知を受領する
- 正しい証明書パス検証手続きに従って GlobalSign から発行された、証明書ステータス情報（例：CRL 又は OCSP）を使用して発行 CA の証明書を検証する
- 正確かつ最新版の検証方法により、証明書の全情報が検証される場合にのみ、発行 CA の証明書を信頼する
- 妥当であると判断される状況においてのみ、GlobalSign の証明書に依拠する
- 依拠当事者が、秘密鍵が危殆化した可能性を察知した場合、適切な RA に通知する

依拠当事者が証明書に依拠することが妥当である判断した場合の義務は:

- 依拠当事者に提示される現状の失効ステータス情報を使用して、認証局の証明書の有効又は失効を検証する
- 証明書もしくは本 CP にて依拠当事者に示された、証明書の使用に関する全ての制限事項について注意を払う
- アプリケーションコンテキストによって提示されるその他のポリシー或いは規約と同様、GlobalSign の証明書中の規定に関しても十分な注意を払う

依拠当事者は、証明書が使用されているアプリケーションのコンテキスト等を勘案して、その状況において証明書に依拠することが妥当であるかどうかを常に立証しなければならない。

9.6.4.1 北米エネルギー規定委員会（NAESB）の依拠当事者

依拠当事者の責任については、以下の定め以外にも、これらの NAESB WEQ PKI Standard を用いた各 NAESB 要件の中に定めなければならない：

- 証明書が認定認証局である GlobalSign により発行されていること
- 認定認証局である NAESB 用 GlobalSign 発行 CA の証明書の有効性及び信頼チェーンの全てが損なわれておらず、有効であるということ
- 証明書が有効かつ失効されていないこと
- 証明書が NAESB 保証レベルの Object 識別子の一つに基づいて発行されていること

9.6.5 その他の関係者の表明保証

規定しない

9.7 保証の免責事項

GlobalSign は以下については保証しないことを明言しなくてはならない。

- 証明書に含まれる、検証不能な情報箇所の正確性。但し、以降本 CP 及びワランティーポリシーに記載された、関連製品の説明に規定されている場合を除く。
- 無料の、テスト配布の、又はデモ用の証明書に含まれる如何なる情報の正確性、完全性、妥当性又は一致性。

9.8 有限責任

GlobalSign の全責任の範囲は、関連する制限付きワランティーポリシー、及びその CPS に定められる制限範囲に準拠するものである。

9.8.1 損害に関する特定の項目の除外

GlobalSign は、如何なる場合も（詐欺行為又は故意の違法行為を除く）下記に上げる項目に対してその責任を負うものではないことを CPS において明記するものする。

- 利益の損失
- データの損失
- 証明書又はデジタル署名の使用、配布、免許、及び実行又は非実行に関連して発生する如何なる間接的、間接的損害、又は懲罰的損害賠償
- 本 CP の構成において提案された取引又はサービス
- 検証された証明書の情報（無料、テスト用、又はデモ用の証明書に表記される情報を除く）への信頼性を除くその他の損害
- 申請者の詐欺行為又は故意の違法行為の結果、検証された情報における誤差により発生する責任。

9.9 補償

9.9.1 発行者 CA による補償

発行者 CA（GlobalSign）の補償責任は、CPS、関連利用契約、又は第三者受益者に対する責任を含むところの依拠当事者規約において定められなければならない。

9.9.2 利用者による補償

GlobalSign は、利用者による補償責任について、 CPS の中にその関連規定を含めるものとする。

9.9.3 依拠当事者による補償

GlobalSign は、依拠当事者による補償責任について、CPS の中にその関連規定を含めるものとする。

9.10 有限責任

9.10.1 期間

本 CP は、GlobalSign によりそのウェブサイト又はレポジトリにおいて、無効である旨の通知が為されるまでの期間、有効である。

9.10.2 終了

通知された変更は、指定されたバージョンに適切に反映される。当変更はその通知から 30 日後に適用されるものとする。

9.10.3 終了の効果及び存続

GlobalSign は、本 CP の終了に関する条件及びその影響については、適切なレポジトリを介して伝達するものとする。

9.11 関係者への個別通知及び伝達

GlobalSign は、本 CP に関してデジタル署名されたメッセージ又は紙媒体を用いた通知を受け入れる。GlobalSign からの有効かつデジタル署名された受領通知があった時点で、通知の送信者はその伝達が有効であったとみなされることとする。送信者はこの受領通知を 20 営業日以内に必ず受領できるものとする。また書面による場合は、配達証明付きの配送サービスにより発送されるか、もしくは書留郵便、郵便料金前払い、配達証明付郵便を必須として、差出人宛てに書面通知するものとする。GlobalSign への個別の連絡は、legal@globalsign.com 宛、又は本 CP の 1.5.2 項に指定される GlobalSign のあて先に送付されるものとする。

9.12 改正条項

9.12.1 改正手続き

本 CP に対する変更があった場合は、適宜そのバージョン番号にて明確化する。

9.12.2 通知方法及び期間

GlobalSign は、本 CP に関する主要な又は重要な変更が為された際には、改定版の CP が承認されるまでの、一定の期間、その変更の件をウェブサイトに掲載するものとする。

9.12.3 OID(オブジェクト識別子)を変更しなければならない場合

規定しない

9.13 紛争解決に関する規定

審決を含む何らかの紛争解決手段、或いはこれの代替システム（小規模裁判、調停、拘束力のある専門家の助言、共同監視及び通常の専門家による勧告等の方法は全て該当する）に進む前に、当事者はその紛争解決策を模索するために努め、当該紛争点について GlobalSign へ通知することに同意するものとする。

紛争の通知を受けた GlobalSign は、GlobalSign 経営陣にその紛争をどのように取り扱うべきかを助言するための紛争協議会を召集する。紛争協議会は、紛争の通知を受領してから 20 営業日以内に召集されるものとする。紛争協議会は、法律顧問、データ保護責任者、GlobalSign 運営経営陣の者及びセキュリティオフィサー（セキュリティ最高責任者）により構成される。法律顧問又はデータ保護責任者のいずれかが会議の議長を務める。その解決策に関して、紛争協議会は GlobalSign 経営陣に対し解決方法を提案する。次いで GlobalSign 経営陣は、提案された当該解決方法について他の当事者に伝達・提案するものとする。

万一、本CPに従い最初の通知がなされた後、紛争が20営業日以内に解決しない場合、ベルギー国裁判所法典の1676から1723項に従い、関係当事者は紛争を仲裁へと進める。

仲裁人は、各当事者が夫々1 名の委員を提案、また双方が 1 名を第三者から選出することで、全 3 名の仲裁人から構成される。仲裁の場所は、ベルギー国 Leuven となり、必要となる費用は調停委員が決定するものとする。

9.14 準拠法

本 CP は、ベルギー国法に基づき、この支配を受け、また解釈される。この法律の選択は、居住地や、GlobalSign 証明書や他の製品及びサービスの使用地に関係なく、本 CP の解釈の一律性を確実にするためのものである。また、GlobalSign が、プロバイダ、供給業者、受益者又はその他の役割を担う GlobalSign の製品及びサービスに関し、本 CP が適用され、又は黙示的・明示的に引用されるところの GlobalSign の業務又は契約関係の全てに対して、ベルギー国法は、適用される。

GlobalSign のパートナー、利用者及び依拠当事者を含む各当事者は、ベルギー国、Leuven の地方裁判所の管轄権に変更不能の条件にて従うものとする。

9.15 適用法の遵守

GlobalSign は、適用法としてベルギー国法を遵守する。特定の GlobalSign パブリック証明書の管理をする製品及びサービスに使用される特定のタイプのソフトウェアの輸出には、何らかの公的認可又は民間機関の認可を必要とすることがある。各当事者は（GlobalSign CA、利用者及び依拠当事者を含む）、ベルギーにおいて該当する輸出法及び輸出規制に従うことに同意する。

9.16 一般事項

9.16.1 包括的合意

GlobalSign は、全ての証明書発行に携わる RA に対し、本 CP 及び全ての適用可能な業界ガイドラインに従うことを、契約上の義務として要求する。如何なる第三者も、同様の合意を強制するような依頼もしくは訴訟を起こすことはできない。

9.16.2 譲渡

本 CP に基づき業務を行なう事業者は、自身が持つ権利又は義務を GlobalSign からの事前の書面承認を得ずして譲渡することはできない。

9.16.3 分離条項

本ＣＰの、責任の制限に関する条項も含むところの、何れかの条項が、無効、或いは違法と判断された場合であっても、それ以外の条項は尚有効であり、当事者間の原義に沿った解釈の下に継続して施行されるものとする。

有限責任を規定する本 CP の各条項は、分離可能であり、それぞれが他の条項から独立していることを意図されているものであり、そのように施行されるものとする。

9.16.4 執行(弁護士の費用及び権利放棄)

GlobalSign は、ある当事者の行為に起因する損害、損失、費用に対する補償及び弁護士費用をその当事者に求めることができる。GlobalSign が本 CP の何れかの規定の執行を行わなかった場合でも、それはその後の同規定の執行、又はその他の規定の執行を放棄するということを意味するものではない。如何なる権利放棄も、書面に明記され、また GlobalSign の署名がある場合に有効となる。

9.16.5 不可抗力

GlobalSign は、政府機関の行為、戦争、暴動、妨害破壊行為、通商禁止、火災、洪水、ストライキ又はその他の行為、輸送の中断又は遅延、通信又は第三者サービスの中断又は遅延などを含む GlobalSign の合理的な管理の及ばない状況に起因又は関連する如何なる損失、費用、経費、責任、損害又は請求に対しても、責任を負わないものとする。

9.17 その他の規定

GlobalSign の TrustedRoot 認証局チェーニングサービスに加入したいと望む第三者発行 CA は、本 CP 及びその全条件を厳守しなければならない。これは、多くの法的、及び手続的管理によって実施され、また検証

される。また年度毎の監査により検証されるものとする。この管理には以下を含むが、これだけに限定されるものではない：

- TrustedRoot 利用者及び GlobalSign 間における認証局チェーニング契約書を締結すること
- TrustedRoot利用者の提出及び発行、また GlobalSign 及び・又は GlobalSign の監査人による審査、及びこれを受入れること
- TrustedRoot 利用者による PKI インフラ確認書の提出、及び GlobalSign 及び・又は GlobalSign 監査人を受入れること

9.17.1 CA チェーニング契約書

CA チェーニング契約書は、下記の規定及び条件を含む

- 利用者法人及びその子会社（50%以上の株式保有支配権）からのTrustedRootに限定して使用すること
- 非商業的利用に限定：発行された証明書は自身の利用、従業員及び既存のビジネス用途及び処理において利用者と提携する第三者の利用に限定すること
- エンドエンティティ証明書種類（S/MIME、SSL クライアント証明書及び SSLサーバ証明書）への制限を行うこと
- GlobalSign により審査及び受諾された CPS を提出すること
- 本CPに準拠すること
- 業界規定に遵守する、物理的、人員、ネットワーク、倫理的及び運用管理についてのPKI評価書類を提出すること
- CA及びサブCAの秘密鍵管理において、FIPS140-3又は同等の暗号化モジュールを使用すること
- 相互認証署名を禁止すること
- 米国輸出規定に基づき、発行済み証明書への輸出管理を実施すること
- GlobalSign及び・又はその監査人による年一度の監査を受諾すること
- CA環境への変更により、PKI評価及びCPSの報告内容と異なる場合は継続的にGlobalSignへ通知すること
- GlobalSign が GlobalSign レポジトリにおいて、（チェーニング系列 CA として）当利用者 CA のことを公開する場合があることを了解すること

GlobalSign 及び・又はその監査人により、TrustedRoot 利用者が CA チェーニング契約に違反したと判断した場合、GlobalSign は下位 CA 証明書を取り消すことができる。

9.17.2 PKI 審査

TrustedRoot 利用契約の施行は、GlobalSign 及び・又はその監査人による、利用者側 PKI に対する審査の受入れ、及びその審査に基づくものである。この審査は、利用者 CA の階層及びセキュリティ対応策を記録するものである。この審査には下記の項目を含むが、それだけに限定するものではない。

- 論理的セキュリティ対応が導入されている－人事事項かつ職務分掌及び二重制御も網羅されていること
- 物理的セキュリティ対応策が導入されていること
- ネットワークセキュリティ対応策が導入されていること
- CA階層が導入されていること
- HSM（ハードウェアセキュリティモジュール）の種類及びシリアル番号

9.17.3 利用者 CA の導入

GlobalSign は、利用者 CA のテスト署名を GlobalSign のテスト CA と連動して行うことを必須事項としてこれを実施する。 GlobalSign のテスト CA は GlobalSign のルート証明書を複製するが、これはテスト目的であると識別され(テスト CA 対 CA)、また第三者アプリケーション(ブラウザなど)に装填されるものではない。テスト署名が成功した場合のみ、利用者 CA は GlobalSign ルート CA から署名される。

9.17.4 継続条件及び監査

利用者 CA は常に、その義務に忠実でなければならない。利用者 CA は、前 9.17.2 項に記載された各項目の如何なる変更についても GlobalSign 及び・又はその監査人に報告する継続的な義務を有する。
GlobalSign は、WebTrust の CA 監査の一部として、その監査人に対し、上記の要求条件について年に一度の監査を行うよう指示し、また加えてコンプライアンス向上のため、ウェブサイトのスキャンサービスを提供する独立した外部の団体から、公開され利用可能なドメインの一覧を取得する。

（以下空白）