GlobalSign CA
Certification Practice Statement
(認証業務運用規程)

本書は、GlobalSign CA Certification Practice Statement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: March 15th 2013

Version: v.7.4

目次

文書変更管理

バージョン	リリース日	著者	ステータスと説明
V.5.0	10/07/05	Andreas Mitrakas	Draft
	30/08/05	Jean-Paul Declerck	Final version
	02/02/06	Johan Sys	Administrative clean-up
v.5.1	13/03/06	Johan Sys	Added GlobalSign Educational ServerSign
v.5.2	29/11/06	Philippe Deltombe	Added GlobalSign OrganizationSSL
	6/12/06	Johan Sys	Removed SureServer products
v.5.3	23/01/07	Johan Sys	Added GlobalSign DomainSSL Added GlobalSign Root CA R2 Adjusted liability gaps
v.5.4	30/3/07	Johan Sys	Administrative update / clarifications
v.5.5	19/6/07	Johan Sys	Renamed product names
v.5.6	25/06/07	Steve Roylance	Final modification for EV Issue 1.0
v.6.0	17/12/07	Steve Roylance	Major Release supporting new certificate lifecycle solutions
v.6.1	20/05/08	Steve Roylance	Administrative update/ clarifications
v.6.2	13/10/08	Steve Roylance	Administrative update/ clarifications
v.6.3	16/12/08	Steve Roylance	Administrative update/ clarifications
v.6.4	11/02/09	Steve Roylance	Administrative update/clarifications
v.6.5	12/05/09	Steve Roylance	Administrative update/clarifications
v 6.6	03/02/10	Lila Kee	Administrative update
v 6.7	12/05/10	Johan Sys	Administrative update/clarifications
v 7.0	22/03/12	Steve Roylance	Administrative update – Inclusion of additional WebTrust 2.0 and CABForum Minimum Guidelines for issuance of SSL certificates
v 7.1	29/03/12	Lila Kee and Steve Roylance	Addition of support for NAESB and Incorporation of the AlphaSSL product range
v 7.2	07/06/12	Steve Roylance	Additional CABForum requirements
v 7.3	01/07/12	Steve Roylance	Final CABForum requirements
v7.4	03/15/13	Giichi Ishii Lila Kee	Extended validity period of Personal Sign, Administrative updates, Modification to NAESB certificates incorporating WEQ-012 v3.0 updates

履歴

Changes in v7.4 (publication date : 15th March 2013) with respect to v7.3

- Extended validity period of Personal Sign
- Modification to NAESB certificates incorporating WEQ-012 v3.0 updates.
- Administrative changes and clarification

Changes in v.7.3 (publication date : 1st July 2012) with respect to v.7.2

- Endorsement of additional CABForum Minimum Guidelines provisions – C name checking

Changes in v.7.2 (publication date : 7th June 2012) with respect to v.7.1

- Endorsement of additional CABForum Minimum Guidelines provisions

Changes in v.7.1 (publication date : 29th March 2012) with respect to v.7.0

- Support for NAESB certificates
- Support for AlphaSSL certificates

Changes in v.7.0 (publication date : 22nd March 2012) with respect to v.6.7

- Administrative changes and clarifications – Structural rewrite for RFC compliance and better understanding
- Removal of DocumentSign and introduction of Adobe CDS

Changes in v.6.7 (publication date : 18th May 2010) with respect to v.6.5

- Administrative changes and clarifications
- Removed Educational ServerSignSSL

Changes in v.6.6 (publication date : 27th January 2010) with respect to v.6.5

- Administrative changes supporting delivery of ObjectSign to Individuals. Rename ObjectSign to CodeSigning

Changes in v.6.5 (publication date : 12th May 2009) with respect to v.6.4

- Administrative changes

Changes in v.6.4 (publication date : 11th February 2009) with respect to v.6.3

- Administrative changes
- Support of timestamping certificate services.
- Support of TrustedRoot TPM and DocumentSign

Changes in v.6.3 (publication date : 16th December 2008) with respect to v.6.2
- Administrative changes
- Support of enhanced validation and application processes – higher degree of automation.

Changes in v.6.2 (publication date : 13th October 2008) with respect to v.6.1
- Administrative changes
- Clarification of Certificate Profiles and removal of Certificate Suspension.

Changes in v.6.1 (publication date : 20th May 2008) with respect to v.6.0
- Administrative changes
- SubjectAlternativeName and non-public domain support

Changes in v.6.0 (publication date : December 17th 2007) with respect to v.5.6
- Removal of the HyperSign product range
- The addition of role and department based PersonalSign Pro 2 certificates.
- The option for GlobalSign to generate Private Key pairs and CSRs on behalf of the applicant
- The use of API functions for all products.
- Minor administrative changes to aid readability.

Changes in v.5.6 (publication date : June 25 20**0**7) with respect to v.5.6
- Administrative changes
- Incorporation of modifications to support EV Guidelines at Issue 1.0

Changes in v.5.5 (publication date : June 19 2007) with respect to **v**.5.5
- Administrative changes
- Renamed some products

Changes in v.5.4 (publication date : March 30 2007) with respect to v.5.3
- Administrative changes

Changes in v.5.3 (publication date : Jan 26 2007) with respect to v.5.2
- Added GlobalSign DomainSSL product
- Added GlobalSign Root CA R2
- Adjusted Liability gap for OrganizationSSL and ExtendedSSL

Changes in v.5.2 (publication date: December 2006) with respect to v.5.1
- Added GlobalSign ExtendedSSL product
- Removed Sureserver products, Renamed GlobalSign Educational ServerSign to GlobalSign Education GlobalSign OrganizationSSL.
- Administrative changes

Changes in v.5.1 (Publication Date: 13 March 2006) with respect to v.5.0
- Added GlobalSign Educational ServerSign product

Changes in v.5.0 (Publication Date: 10 July 2005) with respect to v.4.3.2
- Adaptation to the RFC 3647 format
- Separation of Data protection policy, warranty policy and consumer policy.
- Updated references to GlobalSign Certificate Policy

Changes in v.4.3.2 (Publication Date: 8 April 2005) with respect to v.4.3.1
- Separated references to GlobalSign Qualified Certificates product

Changes in 4.3.1 (Publication Date: 10 October 2003) with respect to v.4.3
- Added SureServer product

Changes in 4.3 (Publication Date: 10 October 2003) with respect to v.4.2
- Section 1.4: Updated wording
- Section 4.3.6: Updated wording
- Section 5.13: Updated reference to logs retention period.
- Section 21.10: Updated wording
- Section 21.22: Updated wording
- Section 21.23: Updated wording

Changes in v.4.2 (Publication Date: 1 August 2003) with respect to v.4.1
- New Chapter 21 GlobalSign PersonalSign 3 Qualified certificates issued under Belgian Law of 9 July 2001 implementing the European Directive 1999/93/EC of the Council and the Parliament on a Community Framework on Electronic Signatures.
- Updated Chapter 10 GlobalSign Limited Warranty Policy to include warranty requirements for product named GlobalSign PersonalSign 3 Qualified certificate.
- Updated Section 5.12 on records retention period for PersonalSign 3 Qualified certificate.
- Appropriate additions to the definitions list with regard to qualified certificates.
- Minor editorial updates to accommodate PersonalSign 3 Qualified in the Introduction.

前提確認事項

このGlobalSign CA CPSは、以下の業界標準をすべてまたは部分的に支持する：

- RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
- RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
- RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
- RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.ETSI TS 101 042: Policy requirements for certification authorities issuing public key certificates (Normalised level only).
- The ISO 1-7799 standard on security and infrastructure
- FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
- X509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
- North American Energy Standards Board (NAESB) Public Key Infrastructure (PKI) Standards – WEQ-012

本 CPS は、以下のスキームの要件に従って評価される:

- AICPA/CICA, WebTrust 2.0 Program for Certification Authorities.
- AICPA/CICA, WebTrust for Certification Authorities – Extended Validation Audit Criteria.
- CABForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

1.0 はじめに

この認証業務運用規程(以下、「本 CPS」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 CPS 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。本 CPS 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 CPS 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の理解を助けるために、本 CPS の翻訳が提供されることがある。ただし、英語版がオリジナルである。)

認証業務運用規程は、「共通のセキュリティに関する要求事項を持つ特定の団体もしくはアプリケーション類にデジタル証明書を発行するための手続き」を定めるものである。本 CPS 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 CPS 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。また、証明書に記載された情報を信頼し依拠する者(以下、「依拠当事者」という)は、本 CPS を参照することで、認証業務手続きをあらかじめ知ることができる。本 CPS 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 CPS は、GlobalSign CA が発行する証明書のライフサイクル期間中において GlobalSign CA が採用する技術、手続き、及び要員に関するポリシーを規定している。

GlobalSign CA は GlobalSign nv/sa の事業活動の範囲で運用されている。本 CPS は、さまざまな種類の証明書を発行する GlobalSign CA への要求事項を記述しており、どのルート認証局にチェーニングされるかは中間証明書の選択、もしくはプラットフォームやクライアント側で使用される、または提供されている相互認証証明書によって異なる。

本 CPS は最終であり、GlobalSign nv/sa(所在地：Martelarenlaan 38, 3010 Leuven、VAT 登録番号：BE 0459.134.256、商業登記番号：BE 0.459.134.256 RPR Leuven の会社法人。以下、「GlobalSign CA」という)と、本 CPS 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、及び依拠し、または依拠しようとする依拠当事者を拘束する。

利用者については、利用契約(以下、利用約款による場合を含む)に同意することにより本CPSが発効し、利用者を拘束する。依拠当事者については、本CPSに基づき発行された証明書に依拠することにより、本CPSが依拠当事者を拘束する。加えて、利用者は利用契約により、本CPSが依拠当事者を拘束することを依拠当事者に告知する義務を負う。

1.1 概要

本 CPS は GlobalSign CA が発行する証明書階層すべてに適用されるものであり、その目的は GlobalSign CA が採用する証明書管理の実務手続きを説明し、GlobalSign CA が規定する要件ならびに上述の業界標準の要件の双方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。2001 年 7 月 9 日、ベルギー法は欧州理事会、欧州議会による電子署名におけるコミュニティフレームワークに関する EU 指令 1999/93/EC を施行し、認証及び否認防止の目的で使用される電子署名を承認した。これに基づき、GlobalSign CA はそのサービスの提供にあたり同法の適用される項の規定の範囲で業務を行っている。本 CPS は上述の範囲においてのみ適用されるものであり、残余をすべて除外する。本 CPS の狙いは GlobalSign CA による認証サービスとクライアント証明書、サーバ証明書、その他の目的のためのエンドエンティティ証明書の証明書ライフサイクル管理を容易にすることである。本 CPS が取り扱う証明書タイプは以下のとおり。

PersonalSign 1/PersonalSign Demo	保証のレベルが低い個人向け証明書
PersonalSign 2	保証のレベルが中程度の個人向け証明書
PersonalSign 2 Pro	保証のレベルが中程度で所属する職業・組織の情報を含む個人向け証明書
PersonalSign 2 Pro DepartmentSign	保証のレベルが中程度で所属する職業・組織の情報・役職の情報を含む個人向けの証明書
PersonalSign 3 Pro	保証のレベルが高く所属する職業・組織の情報を含む個人向け証明書

PersonalSign Partners	PersonalSign 2 Pro を発行するトラストアンカーとして顧客の注文に応じて構築される認証局
DomainSSL(以下、「DV SSL」または「DV」ともいう)	ウェブサーバを認証する証明書
AlphaSSL	ウェブサーバを認証する証明書
OrganizationSSL(以下、「OV SSL」または「OV」ともいう。)	ウェブサーバを認証する証明書
ExtendedSSL(以下、「EV SSL」または「EV」ともいう)	ウェブサーバを認証する証明書 ※
GlobalSign Time Stamping	時刻情報の発行元を認証する証明書
GlobalSign CA for AATL	ハードウェアにインストールされ、Adobe AATL に中程度の保証を提供する個人向け証明書
Code Signing	データオブジェクトを認証する証明書
Extended Validation Code Signing	データオブジェクトを認証する証明書 ※
Digital IDs for North American Energy Standard Board (NAESB) Authorized CA certificates	北米エネルギー規格委員会の指定を受け権限を与えられた認証局が発行する、保証レベルが rudimentary, basic, medium, high のいずれかの個人、役職、サーバ、もしくはデバイス証明書
PDF Signing for Adobe CDS ※※	Adobe Root CA にチェーンされ、保証レベルが中程度のハードウェアに搭載された証明書であり、所属する企業組織の情報を含む場合がある
PersonalSign for Adobe CDS	Adobe PDF で作成された文書に署名することを目的に、組織内の自然人(個人)に所属する企業組織の情報を含まず発行される証明書
PersonalSign Pro for Adobe CDS	Adobe PDF で作成された文書に署名することを目的に、所属する企業組織の情報を含み発行される個人向け証明書
DepartmentSign for Adobe CDS	Adobe PDF で作成された文書に署名することを目的に、所属する企業組織の情報・役職の情報を含む証明書
TrustedRoot for Adobe CDS	GlobalSign CA for Adobe 証明書階層の第二階層を担う中間認証局
Time Stamping for Adobe CDS	時刻情報の発行元を認証する証明書
Test Digital ID for Adobe CDS	ハードウェアの保証を要しないテストもしくはデモを目的とした証明書

※この証明書は CA/Browser Forum が発行する"Guidelines for Extended Validation Certificates"に従って発行・管理される。当該ガイドラインは、本 CPS に参照により組み込まれる。
その他の証明書については、1.2 項で詳述するとおり、CA/Browser Forum ポリシーOID を証明書に記載し、CA/Browser Forum が発行する"Baseline Requirements for the Issuance and Management of Policy-Trusted Certificates"に従って発行・管理される。
※※この証明書は、Adobe Systems 社証明書ポリシー(http://www.adobe.com/misc/pdfs/Adobe_CDS_CP.pdf)に従って発行・管理される。

GlobalSign CA 証明書は、以下の目的に使用することができる。

- 取引の際、手書きの署名の代わりに電子署名を使用する
- サーバその他のデバイスを含むウェブリソースを認証する
- コード、文書その他のデータオブジェクトに電子署名する
- データを暗号化する

本 CPS では、GlobalSign CA の証明書のライフサイクル、使用、当該証明書への依拠、及び管理などに関与するすべてのエンティティの役割、責任、実務を明らかにする。実務、サービスレベル、義務と責任を記述する本 CPS の条項は GlobalSign CA、GlobalSign 登録局(以下、「GlobalSign RA」という)、利用者、依拠当事者など関与するすべてのエンティティを拘束する。また条項によっては認証サービスプロバイダ、アプリケーションプロバイダなど、上述以外のエンティティにも適用される。

GlobalSign 証明書ポリシー(以下、「GlobalSign CP」という)は本 CPS を補完する。GlobalSign CP の目的は「順守すべきこと」を明らかにすることであり、そのためにさまざまな GlobalSign CA の製品・サービスに関する業務ルールの枠組みを定めている。

本 CPS は「認証局が証明書ポリシーに準拠する方法」を定めており、GlobalSign CA がその証明書を生成し管理するにあたって採用するプロセス、手続き、条件などについて詳述し、エンドユーザにこの情報を提供する。証明書ポリシー、認証業務運用規程の他に、GlobalSign CA は以下を含むがこれに限らず、さまざまなポリシー文書を規定している。

- 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

その他の付属文書には以下のものがある。

- 保障に関する事項を取り扱う GlobalSign ワランティポリシー
- 個人情報保護に関する GlobalSign プライバシーポリシー
- GlobalSign のトップルートの信頼対象を取り扱う GlobalSign 証明書ポリシー

GlobalSign CA の発行する証明書の利用者、依拠当事者は、GlobalSign CA が発行する証明書を信頼するため、また当該証明書の発行に際して採用された実務を知るために、本 CPS を参照すべきである。階層全体の証明書チェーンの信頼性を確認することも重要であり、これにはルート認証局、その他のあらゆるオペレーショナル・ルートの証明書が含まれる。本 CPS における GlobalSign CA の表明にもとづき信頼性を確認すること。

適用可能な GlobalSign CA のすべてのポリシーは権限ある第三者により継続的な監査、審査を受けており、これらのポリシーは WebTrust サイトシールを付与した GlobalSign CA 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。

1.1.1 証明書名称

本 CPS に基づき発行される GlobalSign CA 証明書の名称は以下のとおり。

- GlobalSign Root CA – R1(シリアルナンバー：040000000001154b5ac394)
- GlobalSign Root CA – R2(シリアルナンバー：0400000000010f8626e60d)
- GlobalSign Root CA – R3(シリアルナンバー：04000000000121585308a2)
- GlobalSign Root CA – R4(シリアルナンバー：2a38a41c960a04de42b228a50be8349802)
- GlobalSign Root CA – R5(シリアルナンバー：605949e0262ebb55f90a778a71f94ad86c)
- GlobalSign Primary SHA256 CA for Adobe(シリアルナンバー：35fbe4fadfe4b092276c319b99f8ceb3)
- GlobalSign CA for Adobe(シリアルナンバー：0100000000012872543bd4)
- North American Energy Standards Board Inc. Issuing CA – SHA 256 – G2
- AlphaSSL G2(シリアルナンバー：04 00 00 00 00 01 2F 4E E1 37 02)

GlobalSign CA は、これら 5 つのルート証明書(R1～R5)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及び関連暗号サービスへ搭載されるよう、積極的に働きかけを行っている。GlobalSign CA 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 CA 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。

TrustedRoot とは、第三者が運用する発行局を GlobalSign CA のルート証明書の一つにチェーニングさせるという、GlobalSign CA のサービスである。当該サービスにおけるエンドエンティティ証明書は、第三者が規定する CPS の対象範囲であり、本 CPS の対象外である。

- GlobalSign Trusted Platform Module Root CA(シリアルナンバー：040000000001201909 19AE [2])

TrustedRoot TPM とは、第三者が運用する発行認証局を GlobalSign Trusted Platform Module のルート CA 証明書にチェーンさせるという、GlobalSign のサービスであり、当該サービスにおけるエンドエンティティ証明書も、本 CPS の対象外である。

[2] R1～R5 ルート及び Trusted Platform Module ルートをまとめて GlobalSign CA ルート証明書という。

電子証明書により、エンド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、データに電子的に署名したりすることができる。GlobalSign CA は、電子証明書を使用するエンティティ(サブジェクト)の名前、及び当該エンティティがその公開鍵を持つことを審査し確認する。電子証明書の提供を受けるプロセスには、ユーザの本人確認、名前確認、認証、登録などとともに、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。電子証明書を発行するさまざまな手続きを通じて、GlobalSign CA は証明書のユーザが本人であること、及び当該エンティティが使用する公開鍵をもとに電子証明書が生成されたことを証明する。GlobalSign CA 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また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 CAはチェーンサービスがMITM(中間者)によるSSL/TLSパケットの盗聴に悪用されることを防ぐため主体的な取り組みを行う。その目的においてGlobalSign CAは、サードパーティのアプリケーションにGlobalSign CAのルート証明書を搭載するにあたり、主導的な役割を保持する。

1.2 文書名称と識別子

本書は GlobalSign CA 認証業務運用規程である。

GlobalSign nv/sa(GlobalSign CA)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 (2)、DoD (3)、インターネット (4)、民間 (5)、企業 (1)、GlobalSign nv-sa (4146)、すなわち 1.3.6.1.4.1.4146 である。GlobalSign は本 CPS(適宜更新する)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。

1.3.6.1.4.1.4146.1.1	Extended Validation 証明書ポリシー(SSL)
1.3.6.1.4.1.4146.1.2	Extended Validation 証明書ポリシー(Code Signing)
1.3.6.1.4.1.4146.1.10	Domain Validation 証明書ポリシー
1.3.6.1.4.1.4146.1.10.10	Domain Validation 証明書ポリシー(AlphaSSL)
1.3.6.1.4.1.4146.1.10.20	~~Domain Validation 証明書ポリシー(SignTrust)(廃止)~~
1.3.6.1.4.1.4146.1.20	Organization Validation 証明書ポリシー
1.3.6.1.4.1.4146.1.30	Time Stamping 証明書ポリシー
1.3.6.1.4.1.4146.1.40	Client 証明書ポリシー
1.3.6.1.4.1.4146.1.40.10	Client 証明書ポリシー(ePKI – Enterprise PKI)
1.3.6.1.4.1.4146.1.40.20	Client 証明書ポリシー(JCAN – Japan CA Network)
1.3.6.1.4.1.4146.1.50	Code Signing 証明書ポリシー
1.3.6.1.4.1.4146.1.60	CA Chaining ポリシー(TrustedRoot™)
1.3.6.1.4.1.4146.1.80	流通 EDI クライアント証明書ポリシー
1.3.6.1.4.1.4146.1.81	流通 EDI サーバ証明書ポリシー
1.3.6.1.4.1.4146.1.90	TrustedRoot TPM ポリシー
1.3.6.1.4.1.4146.1.95	Online Certificate Status Protocol ポリシー

上記の識別子に加え、North American Standard's Board Certification Authority Accreditation Specification に準拠するすべての証明書には、以下の識別子を付与する。

2.16.840.1.114505.1.12.1.2	NASESB 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
2.16.840.1.114505.1.12.4.2	NAESB High Assurance

上記の識別子に加え、CA/Browser Forum が発行する「Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates」に準拠するすべての証明書には、以下の識別子を付与する。

2.23.140.1.2.1	Domain Validation 証明書ポリシー
2.23.140.1.2.2	Organization Validation 証明書ポリシー

上記の識別子に加え、Adobe Systems 社の証明書ポリシーに準拠するすべての証明書には、以下の識別子を付与する。

1.2.840.113583.1.1.5	Adobe ドキュメント認証サービス OID

1.3 PKI における関係者

1.3.1 認証局

GlobalSign CA は本 CPS に基づき高品質、高信頼性の証明書を発行する認証局である。GlobalSign CA は、認証局として、公開鍵基盤に基づく証明書のライフサイクル管理にまつわる業務を行う。この業務には、利用者の登録、及び証明書の発行、更新、交付、失効などが含まれる。GlobalSign CA は、証明書のステータス情報を、証明書失効リスト(以下、「CRL」という)配布ポイントの形式で示されるオンラインレポジトリ及び/また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。)レスポンダを使用して提供する。この認証局は、下位発行認証局の登録局(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」または「GlobalSign CA」の名で呼ばれることがある。

GlobalSign CA の Policy Authority は、GlobalSign CA の経営チーム、及び GlobalSign CA の取締役会で承認されたメンバーで構成されており、GlobalSign CA の証明書階層に含まれるすべての電子証明書の認証業務運用規程の維持管理に責任を負う。GlobalSign CA の Policy Authority は、すべ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 の発行認証局を含む GlobalSign CA 証明書階層を構成する下位発行認証局の証明書などが含まれる。

GlobalSign CA は外部に委託して認証局運営を行うにあたり、安全な設備管理を行っている。GlobalSign CA の外部委託業者は、サービス契約に基づき GlobalSign CA にサービスを提供しており、その範囲は証明書の発行及び失効サービスである。この外部委託業者は、GlobalSign CA から要求される指定サービス及びサービスレベルの要件への適合を保証し、GlobalSign CA に代わってサービス及び証明書の管理に関する業務を行う。これらの業者はベルギー及びフランスに拠点を置く。

GlobalSign CA はタイムスタンプ局(以下、「TSA」という)でもあり、特定の日時にデータが存在したことを証明する。GlobalSign CA は TSA サービスを適宜外部に委託し、日時・時刻に関係する認証業務を独自に行うことを許可する。

GlobalSign CA は、そのルート証明書の下で発行される証明書の管理サービスを安定的に提供する。このサービスは、特定のアプリケーションで利用可能である、ないし必要となる、証明書の発行、失効、ステータス検証などを含むがこれに限定しない。GlobalSign CA は、当該認証局の下位認証局、発行認証局の下で発行されるすべてのタイプの証明書に向け、オンライン登録システム、及び種々の API を提供管理する。

証明書のライフサイクル管理に関する業務のいくつかは、GlobalSign RA に委任され、この業務は GlobalSign CA とのサービス契約に基づき遂行される。

1.3.2 RA

RA は、証明書の申請者の本人確認を行うエンティティである。RA は、証明書の失効、再発行、更新(Re-key と呼ぶこともある)を要求したり、または他のエンティティからの要求を受理しそれを転送したりする。GlobalSign CA は以下のような業務を通じ、発行した証明書の RA としての役割を果たすこともある。

- 証明書要求を受理し、チェックし、承認または却下する
- 利用者を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、または他の形で認められた文書を使用して利用者の申請をチェックし、本人確認を行う
- 多要素認証をした権限ある要求者からの証明書の発行要求を承認する
- GlobalSign CA の下位発行局からの要求を受け証明書失効手続きを取る

GlobalSign CA と契約を締結したサードパーティ発行局が独自の 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、証明書ポリシーが定めるすべての要求事項ならびに CA/Browser 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順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、また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。身分証明書、運転免許証などは、利用者の本人確認のための信頼できる情報源となる。依拠当事者には、本 CPS を参照し具体的な情報を確認することが求められる。

RA の果たすいくつかの機能は、ローカル登録局(以下、「LRA」という)が実行する。LRA は GlobalSign RA の監督支配下にあり、またマネージド PKI Lite(以下、「ePKI」という)や SSL マネージドサービス(以下、

「MSSL」という)においては GlobalSign Certificate Centre(以下、「GCC」という)にプリセットされた、認証済の情報を使用した証明書のみ発行できる。このエンティティをエンタープライズ RA という。

1.3.2.1 EV 証明書・EV Code Signing 証明書固有の RA への要求事項

EV 証明書・EV Code Signing 証明書の発行にあたっては、GlobalSign CA は各 RA または委託先に対し、参照により本 CPS に組み込まれる EV ガイドラインのすべての適用要件に準拠し、必要な手続きを取ることを義務付ける。

EV ガイドラインの条項に基づき、GlobalSign CA は、特定の有効な EV 証明書のサブジェクトに対し、契約に基いて RA としての機能を果たし、また GlobalSign CA が当該のオリジナルの EV 証明書に記載されたドメインの第三レベルあるいはそれ以上のレベルのドメインに対して追加の証明書(これをエンタープライズ EV 証明書という。)を発行することを許可することがある。この場合、サブジェクトはエンタープライズ RA とみなされ、第三階層以上の EV 証明書をエンタープライズ RA またはエンタープライズ RA が所有するまたは直接支配する企業以外のサブジェクトに対し発行することを認証局に許可してはならないものとする。GlobalSign CA はこの要件をシステムを通じ機械的に強制する。

GlobalSign CA は EV ガイドライン 24 項の最終相互相関関係ならびにデューディリジェンス要件の履行をエンタープライズ RA に委任しない。

1.3.3 利用者

GlobalSign CA の利用者とは、取引、通信、電子署名の使用のため証明書を申請し受領した法人または自然人をいう。
証明書のサブジェクトとは、証明書に名前を記載される当事者をいう。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 GlobalSign 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。

法人は付属定款、役員の任命、官報、QIIS や QGIS などのサードパーティデータベースなどに基づき組織情報の検証が行われる。自営業を営むサブジェクトは居住国の管轄当局が発行する商業登録証明に基づき組織情報の検証が行われる。

すべての利用者は、証明書のオンライン申請を行う際に説明される要求事項に従い、さらなる信用証明情報の提出が必要となる。

GlobalSign CA が発行するエンドエンティティ証明書の利用者には、GlobalSign CA のネットワーク資源にアクセスする必要がある日常業務に携わる従業員、委託業者が含まれる。利用者は鍵ペアの生成を行い証明書を保管する署名生成デバイスの運用上または法的な所有者である場合もある。

利用者である組織は GlobalSign CA が当該利用者に GlobalSign CA 証明書サービスを使用するアプリケーションの範囲内において特定の機能を果たす権限を与える雇用契約またはサービス契約を締結することが求められる。GlobalSign CA と利用申請を行うエンドエンティティの間で締結された契約に基づいてのみ、利用者である組織に証明書を付与する。

1.3.4 依拠当事者

依拠当事者は利用者の証明書に記載された公開鍵を参照することで検証可能な証明書または電子署名に依拠する自然人または法人である。

電子証明書の有効性を検証するにあたり、依拠当事者は配布ポイント及び OCSP レスポンダを通じて CRL の形式で提供される GlobalSign CA の失効情報を参照しなければならない。

Adobe は Acrobat® 9.12 以上の製品で AATL プラットフォームを提供している。これにより、文書の受領者は、認証された PDF 文書が本物であることをより確実に保証される。ここでの文書の受領者は、Adobe 製品でこの機能をサポートするプラットフォームを使用し、認証された文書になされた利用者の署名を検証する依拠当事者である。ベストプラクティスは、文書を認証しようとする作成者が、署名する PDF に証明書ステータス情報と適切なタイムスタンプを含めることである。依拠当事者は適切な Adobe PDF リーダーのバージョンを使用してこうした情報を検証することができる。

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局を相互認証する認証局などを含む。たとえば GlobalSign CA のルート証明書 R1 は Microsoft に相互認証されており、GlobalSign

CA をサブジェクトに記載し、64 ビットのカーネルモードドライバを提供している。この相互認証証明書は以下の URL よりダウンロードできる。

http://download.microsoft.com/download/2/4/E/24E730E6-C012-448F-92B6-78744D3B77E1/GlobalSign%20Root%20CA.zip

Base64 形式の証明書は以下に記載する。

-----BEGIN CERTIFICATE-----
MIIFJjCCAw6gAwIBAgIKYSkVJwAAAAAAKjANBgkqhkiG9w0BAQUFADB/MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHUmVkbW9uZDEe
MBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSkwJwYDVQQDEyBNaWNyb3Nv
ZnQgQ29kZSBWZXJpZmljYXRpb24gUm9vdDAeFw0xMTA0MTUxOTU1MDhaFw0yMTA0
MTUyMDA1MDhaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52
LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxTaWduIFJvb3Qg
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZjc6j40+Kfvvx
i4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavpxy0Sy6scTHAH
oT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp1Wrjsok6Vjk4
bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdGsnUOhugZitVt
bNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJU26Qzns3dLlw
R5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N89iFo7+ryUp9/
k5DPAgMBAAGjgcswgcgwEQYDVR0gBAowCDAGBgRVHSAAMAsGA1UdDwQEAwIBhjAP
BgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzAf
BgNVHSMEGDAWgBRi+wohW39DbhHaCVRQa/XSlnHxnjBVBgNVHR8ETjBMMEqgSKBG
hkRodHRwOi8vY3JsLm1pY3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNy
b3NvZnRDb2RlVmVyaWZSb290LmNybDANBgkqhkiG9w0BAQUFAAOCAgEAX/jQZXRq
gcamylsDtpFK6Eu97yuhQvDvtKWtzTOJ7AuVhaxiUBEIqljSWqCDEOWmM3ryWvLF
/nh88JyD3xkK2XOWAC3WLM3pFNQdneg/PBp295BO+wE1CmyTE6DDVutnoOTRepbe
wmfxkPgKe/UyG5TsX3UfjRs02mxYp8stJ54iJrfJqjDMB3e4NuOCAbU5PMyN2adf
fyOzh3/bV5iRi9fOJSDjnWRP3Yf3K2hJAxjgpd98X2hkTTaDjUeB8ungqGmr+nsW
PAWkSeqIMBkKbHMFUXjf1B3dOtR/LeROVL6DQx56dDO0pOvXcHO8KgKYiWbu9ryP
dJN44ykCWlpD4lj0fM+aytI2iTviX9omBU7I1OcskQ4Xl8W+7osTESMjKU/6g9BQ
9rr61T2zFz30/wNKoyXc5nVh0fo1CGvWJ0TQaLeNReDrhSzIoV1hRHQWDllYrtK1
7qW81tcHarYpeP2XZ2fdjU8XlE/S7QyvlyQ3w6Kcgdpr4UO2V3tM7L95Exnnn+hE
6UeBt15wHpH4PdF7J/ULcFZDSAXdqS+rhhAdCxLjGtBMbnXe1kWzC3SIh5NcVkpB
Apr3rreZ2LZ/iPoR8kV89NcbkcAc8aD71AgKQRoUKs706zRIbmaHntVLejI/uw49
OGHPc1cG5BIGa9lrUwjNcBjCLU+XRpG8qfA=
-----END CERTIFICATE-----

1.4 証明書の使用方法

電子証明書とは、特別な形式のデータオブジェクトで、本人確認された利用者と公開鍵(RSA 方式または ECC 方式)を暗号によって結びつけるものである。

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。GlobalSign CA が発行する証明書は以下のような機能を必要とするパブリックドメインでの通信で使用することができる。

- 否認防止：当事者は、取引を行ったこと、電子メッセージを送信したことを否認することができない。
- 認証：あるエンティティに対し、別のエンティティが主張する人物(組織・物)であることを証明する
- 機密性(秘匿性)：あるエンティティに対し、明確に受信者として意図された相手以外には誰もデータを読み取ることができないことを保証する
- 完全性：あるエンティティに対し、送信者から受信者に送られる間、及び送信された時刻から受信された時刻までの間に、データが意図的にまたは意図せず変更が加えられていないことを保証する

電子署名：デジタル(電子)署名は電子フォーム、電子文書、電子メールなど電子署名に対応する特定の取引にのみ使用することができる。署名用の証明書は、電子証明書をサポートするアプリケーションにおいてのみ電子署名の生成を保証する。電子署名に使用できる証明書は以下のとおり。

- **PersonalSign 2：** 取引の否認防止(中程度の保証レベル)
- **PersonalSign 2/3 Pro：** 組織内の担当者として取引を行う当事者による取引の否認防止(中程度の保証レベル)
- **CA for AATL：** 組織内の担当者として取引を行う当事者による取引の否認防止(中程度のハードウェアレベルの保証)
- **PDF Signing：** 組織内の担当者として取引を行う当事者による取引の否認防止(中程度のハードウェアレベルの保証)。(Adobe 証明書ポリシーで規定されるとおり、キーエスクロー(鍵の預託)サービスの提供ができないこと及びデ

ジタル ID の唯一性をかんがみ、デジタル ID を暗号化に使用することは推奨されない。)

- **PersonalSign 3 Pro：** 組織内の担当者として取引を行う当事者による取引の否認防止(高い保証レベル)

認証(ユーザ)：ユーザ認証証明書は、ウェブサイトその他のオンラインデータへのアクセス、電子メールなど、電子的な認証を必要とする通信に使用することができる。電子証明書の認証機能は電子証明書のエンドユーザ利用者を認証する目的での通信に使用できる。この認証機能を説明する言葉として、しばしば「電子署名」が用いられる。

- **PersonalSign 1：** 電子メールアドレスの実在性を認証する
- **PersonalSign 2：** 自然人を認証する(中程度の保証レベル)
- **PersonalSign 2 Pro：** 組織内の自然人または組織内の役職名を認証する(中程度の保証レベル)
- **CA for AATL：** 自然人または組織内の自然人、組織内の役職名を認証する(中程度の保証レベル)
- **PersonalSign 3 Pro：** 組織内の自然人を認証する(高い保証レベル)
- **NAESB Rudimentary：** NIST SP800-63 Version 1.0.2 Section 7.2.1 に記載されている内容を認証する
- **NAESB Basic：** NIST SP800-63 Version 1.0.2 Section 7.2.1 に記載されている内容を認証する
- **NAESB Medium：** NIST SP800-63 Version 1.0.2 Section 7.2.1 に記載されている内容を認証する
- **NAESB High：** NIST SP800-63 Version 1.0.2 Section 7.2.1 に記載されている内容を認証する

認証(デバイスおよびオブジェクト)：デバイス認証証明書は、ウェブサイトその他ソフトウェアオブジェクトをはじめとするオンラインリソースなど、電子的な認証を必要とする通信に使用することができる。電子証明書の認証機能は利用者が電子証明書を用いてデバイスを認証する目的での通信に使用できる。この認証機能を説明する言葉として、しばしば「電子署名」が用いられる。

- **DomainSSL：** ドメイン名とウェブサービスの認証、通信の暗号化
- **AlphaSSL：** ドメイン名とウェブサービスの認証、通信の暗号化
- **OrganizationSSL：** ドメイン名、ドメイン名と関連づけられる組織名とウェブサービスの認証、通信の暗号化
- **ExtendedSSL：** ドメイン名、ドメイン名と関連づけられる組織名とウェブサービスの認証、通信の暗号化
- **Code Signing：** 法人、法的エンティティとそのデータオブジェクトの認証
- **EV Code Signing：** 法人、法的エンティティとそのデータオブジェクトの認証
- **Time Stamping：** 組織内での日付・時刻に関連するサービスの認証
- **PersonalSign(全種)：** 組織に関連づけられるデバイスやマシンの認証
- **NAESB Rudimentary：** NIST SP800-63 Version 10.2 section 7.2.1 に記載されている内容を認証する
- **NAESB Basic：** NIST SP800-63 Version 10.2 section 7.2.1 に記載されている内容を認証する
- **NAESB Medium：** NIST SP800-63 Version 10.2 section 7.2.1 に記載されている内容を認証する
- **NAESB High：** NIST SP800-63 Version 10.2 section 7.2.1 に記載されている内容を認証する

保証レベル：利用者は依拠当事者が信頼して通信を行う適切な保証レベルを選択する必要がある。たとえば、あまり知られていないブランド名を使用する利用者は高いレベルの保証を持つ(ExtendedSSL)証明書を使用して積極的に自らの身元を依拠当事者に保証すべきであり、閉じられたコミュニティ内でよく知られた URL を用いる場合には低い保証レベルのソリューションが選択できる。

- **低い保証レベル:** Class 1 証明書は、認証された本人識別情報が証明書内に記載されないため、本人確認には適していない。否認防止サービスを提供しない。
- **中程度の保証レベル:** Class 2 証明書は、サブジェクトの本人識別情報が証明書内に記載された、個人または組織に発行される証明書である。中程度の保証を必要と

する通信を安全にする目的での使用に適しており、この通信には組織間及び組織内の通信、商取引、個人的な電子メールなどが含まれる。

- **高い保証レベル:** Class 3 証明書は、Class 1・Class 2 証明書に比較してサブジェクトの本人識別情報について高いレベルの保証を提供する、個人または組織に発行される証明書である。
- **高い保証レベル(EV):** EV 証明書は EV ガイドラインに準拠して GlobalSign CA が発行する Class 3 証明書である。
- **NAESB Rudimentary:** エンドエンティティに対し、最も低い保証レベルを提供する。このレベルの主な目的は署名された情報の完全性を保証するために使用される。このレベルは悪意のある行動をとることが少ないと考えられる環境にて使用されることを想定している。このレベルは認証を必要とする取引には適していない。また、一般的に機密性を必要とする取引には適していないが、より高い認証レベルの証明書が使用できない場合は、このレベルの証明書を使用してもよい。
- **NAESB Basic:** データ漏えいにつながるリスクがあるがその影響が大きくないと考えられる環境において、基礎レベルの保証を提供する。この環境はプライベート情報にアクセスするが、悪意のあるアクセスが行われる可能性は高くない環境を含む。なお、この保証レベルでは悪意を持ったユーザはいないと想定している。
- **NAESB Medium:** このレベルはデータ漏えいにつながるリスクが中程度にある環境に関係している。この環境は大きな金銭的価値がある取引や不正のリスク、または不正アクセスの可能性が大きい環境においてプライベート情報にアクセスすることを含む。
- **NAESB High:** このレベルはデータに対する脅威が大きい環境、またはセキュリティサービスの不備があった場合の影響が高い環境のために残されている。

機密性：タイムスタンプ及び Code Signing 用の証明書を除くすべてのタイプの証明書は、電子証明書により通信の機密を保全する目的で使用することができる。機密情報にはビジネス上の通信、個人的な通信、個人情報、プライバシーなどがある。

北米エネルギー規格委員会(以下、「NAESB」という) の PKI において発行された証明書はビジネスプラクティススタンダード WEQ-001、WEQ-002、WEQ-003、WEQ-004、WEQ-005 における取引に使用することができる。また、双方の合意がある場合はそのほかの取引にも使用することができる。ビジネスプラクティススタンダード WEQ-012 に基づいて発行された証明書は以下のすべての使用方法を禁ずる。

- 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

上記以外の目的での電子証明書の使用は本CPSの対象外である。電子証明書を使用する際、同じ証明書を使って電子署名（否認防止）と認証（デジタル署名）をすることができる。上記の用語はIETF、及びEU指令1999/93/EC（電子署名におけるコミュニティフレームワーク）の法的枠組みにおいて区別して使用される。

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。

本 CPS に準拠して発行された証明書は、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 CPS 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。

- 以下に挙げるような、フェイルセーフ機能を必要とする用途。
  - 原子力設備の運用
  - 航空管制システム
  - 航空機ナビゲーションシステム
  - 兵器誘導システム

  - その他、誤動作・機能不全が人の怪我や死、または環境被害をもたらす可能性があるシステム
- 法により禁じられている場合。
- NAESB WEQ-PKIにおいて発行された証明書は以下の目的で使用してはならない。
  - 危殆化や改ざんが起きた場合投獄され得るような通信やデータ伝送
  - 連邦法において違法とみなされる通信やデータ伝送

1.4.2.1 証明書エクステンション

証明書エクステンションは X.509 v.3 規格に準拠している。EKU は Enhanced(Extended)Key usage(拡張鍵用途)の略である。

- PersonalSign 1、Demo -(EKU)クライアント認証、S/MIME
- PersonalSign 2 / 2 Pro -(EKU)クライアント認証、S/MIME
- PersonalSign 3 Pro -(EKU)クライアント認証、S/MIME
- NAESB -(EKU)クライアント認証、S/MIME、サーバ認証を含む異なる機密情報の保護に使用できる。
- GlobalSign CA for AATL -(EKU)クライアント認証、S/MIME
- OrganizationSSL* -(EKU)クライアント・サーバ認証
- DomainSSL* -(EKU)クライアント・サーバ認証
- AlphaSSL* -(EKU)クライアント・サーバ認証
- ExtendedSSL* -(EKU)クライアント・サーバ認証
- Time stamping -(EKU)タイムスタンプ
- Code Signing、EV Code Signing -(EKU)コードサイン
- PDF Signing -(EKU)Adobe CDS ドキュメントサイン
- TrustedRoot -すべてのポリシー

*下位互換性を保つため Server Gated Cryptography(SGC)が設定されることがある。

1.4.2.2 クリティカル・エクステンション

GlobalSign CA は発行する証明書において、以下に挙げるようなクリティカル・エクステンションを使用する。

- Key Usage の基本制限で証明書が CA 証明書であるか否かを示すもの
- 鍵の使用方法を示すもの
- CA 証明書のどの階層レベルにいるかを示すもの
- TrustedRoot CA 証明書を顧客の特定領域における使用に限定するもの

1.5 ポリシー管理

1.5.1 文書を管理する組織

発行局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、またはその他本CPSに関する問い合わせは、以下に送付すること。

Principle 1 Policy Authority
GlobalSign NV
Martelarenlaan 38,
3010 Leuven,
Belgium.
Tel:+ 32 (0)16 891900
Fax: + 32 (0) 16 891909

1.5.2 問い合わせ窓口

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

1.5.3 認証業務運用規程がポリシーに適合しているかを判断する担当者

WebTrust における独立監査人から受領するアドバイスに基づき証明書ポリシーの適格性、適用可能性や本 CPS の準拠性を判断するのは、Principle 1 Policy Authority である。

本 CPS に信頼性をもたせ、認定基準及び法的要件により的確に対応するため、Policy Authority は適宜、または状況に応じて、ポリシーを改訂し更新する。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 CPS の公表から 30 日後に拘束力を持つ。

新バージョン、公表される更新内容は、それぞれのポリシーについて 3 つのうちの適切な Policy Authority の 1 つの承認を受ける。具体的には、パブリック手続き(WebTrust Principle 1 Policy Authority)、審査手続き(WebTrust Principle 2 Policy Authority)、セキュリティ手続き(WebTrust Principle 3 Policy Authority)に分かれる。現在の組織体制において、各 Policy Authority は、以下のメンバーで構成される。

- GlobalSign CA またはグループ会社の経営チームメンバーから少なくとも 1 名
- GlobalSign CA の手続きやポリシーの起草、策定に直接関与した、権限のある代理人少なくとも 2 名

経営チームのメンバーがそれぞれの Policy Authority の議長を務め、Policy Authority は GlobalSign nv/sa の取締役会に報告を行う。

それぞれの Policy Authority のメンバーは、ポリシーの適格性を判断するにあたり議決票を 1 つ持つ。その他のいかなる人物に対しても議決権は付与されない。票が同数の場合には、Policy Authority の議長票を 2 票と数える。

各 Policy Authority 議長は独立第三者監査人から受領するフィードバックをそのポリシーに反映させる責任を負う。

1.5.4 認証業務運用規程承認手続き

ポリシーの更新が Policy Authority に承認されると、認証業務運用規程の新バージョンが GlobalSign CA のオンラインリポジトリ(https://www.globalsign.com/repository)において公開される。

新バージョンは、その告示が行われてから 30 日以内に不承諾の通達を利用者から受けない限り、既存のすべて利用者、及びこれから証明書を利用しようとする者を拘束する。当該期間の経過後は、認証業務運用規程の新バージョンは前のバージョンの認証業務運用規程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すべての当事者を拘束する。

変更により影響を受ける利用者は、Policy Authority に対し、告示から 15 日以内であれば、意見を述べることができる。ポリシーの変更に対し異議を唱えることができるのは、利用者と監督機関(Webtrust 監査人)のみである。利用者ではない依拠当事者は異議を唱える権利を有しない。

GlobalSign CA は本 CPS の最新 2 バージョンをそのウェブサイトで公開する。

1.5.4.1 変更についての通知

たとえば特定の権能を持つ監査人など、改訂の通知を受け取るべき法的義務を負う当事者に対しては、本 CPS の改訂が通知される。

1.5.4.2 版管理、変更履歴

認証業務運用規程に対する変更は、新しいバージョン番号の付与により示される。大きな改訂の場合は小数点第一位に 0 を付けた整数で示される。小さな改訂は 0 以上の小数点第 1 位で示される。小さな改訂には以下を含む。

- 小さな編集上の訂正など
- 問いあわせ窓口の変更など

1.6 定義と略語

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また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、または更新しようとする自然人または法人。証明書が発行されれば、自然人また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。

申請代表者：申請者自身、または申請者に雇用される者、申請者を代理する明示的な権限を持つ代理人などの自然人または保証人。申請代表者は、(i)申請者に代わって証明書申請に署名、提出、承認し、(ii)申請者に代わって利用契約に署名、提出し、(iii)申請者が認証局の関連企業である場合には、証明書利用契約を承認し同意する。

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

監査基準：8 項に基づく監査スキームを充足するためにエンティティが従うべき本文書に規定されるまたはその他のあらゆる要求事項

監査報告書：認証局または登録局が要求事項を順守することを表明する有資格監査人が発行する声明、報告書、文書

紐づけ:証明書に名前の記載されたエンティティとその公開鍵に関係性があるとする RA の表明

ドキュメント認証サービス(CDS)：Adobe PDF バージョン 6.0 以上に実装された Adobe Root CA Policy Authority が作成した文書署名アーキテクチャ

証明書：電子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

証明書データ：認証局が保持、管理、また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

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

証明書要求：証明書の発行を要求するために行われる 4.1 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

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

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

電子署名：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。

ドメイン名使用許諾書：申請者が特定のドメイン名空間において証明書要求を行う権限を有することをドメイン名の登録者が認定する委任状その他の文書

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すべて

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またはエンティティで、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または法人を指す。

レジストラ：Internet Corporation for Assigned Names and Numbers(ICANN)または各国のドメイン名管理当局・レジストリ、または 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)の援助または契約に基づきドメイン名の登録業務を行う人物またはエンティティ

発効日：適格監査スキームにおいて決定される要求事項がその効力を発する日

エンタープライズ証明書：エンタープライズ RA から発行の承認を受けた証明書

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、認証局の関連会社ではない組織の雇用者または代理人

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

政府機関：政府が運営する法的機関、省、支部、その他同様の国また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)：電子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

発行局：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。

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。

独立監査：本文書に規定される要求事項や 8 項に基づく 1 つ以上の監査スキームへのエンティティの準拠性を判断するために有資格監査人により実施される監査

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)公開鍵基盤(PKI)基準 WEQ-012：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

オブジェクト識別子：ISO 規格において特定のオブジェクトまた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。

秘密鍵：鍵ペアの一方で、所有者が秘密裏に保管し、電子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。

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電子署名を依拠当事者が検証する際、ある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。

公開鍵基盤：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

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または法人。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。

リポジトリ：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 または 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

予約された IP アドレス：IPv4 または IPv6 の IP アドレスで、IANA が「予約アドレス」と指定したもの

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

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。

ルート鍵生成スクリプト：ルート認証局の鍵ペアを生成するための計画及び手続きを記した文書

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また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または法人で、利用契約により法的に拘束される。

利用契約：認証局と申請者また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

約款：申請者また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

登録されていないドメイン名：登録ドメイン名ではないドメイン名

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

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

AICPA	米国公認会計士協会
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
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
ETSI	欧州電気通信標準化機構
FIPS	(米国政府)連邦情報処理標準
FQDN	完全修飾ドメイン名
GSCA	GlobalSign 認証局
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	インターネット技術タスクフォース
IM	インスタントメッセージ
ISO	国際標準化機構(International Organization for Standardization)
ISO	国際標準化機構(International Standards organization)
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
NIST	(米国政府)アメリカ国立標準技術研究所
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
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
VOIP	ボイス・オーバー・インターネット・プロトコル

2.0 公開とリポジトリの責任

2.1 リポジトリ

GlobalSign CA はオンラインリポジトリにおいて、すべての 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。GlobalSign 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、ダウンタイムが年間 0.5%を超えない最低 99%を保証する。

GlobalSign CA 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。

GlobalSign CA はセキュリティ管理、手続き、社内セキュリティポリシーなど、一部の文書については公開しない。ただし、GlobalSign CA が準拠する、認証局向け WebTrust プログラムや EV 向け WebTrust プログラムなど、公式認定スキームに関連して行われる監査においては、これらの情報を開示する。

GlobalSign CA 及びそのグループ会社は、本 CPS 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 CA の法的拘束力を有するリポジトリは https://www.globalsign.com/repository であり、解釈を論じるにあたっては英語版を原本とみなす。

2.2 証明書情報の公開

GlobalSign CA は証明書ポリシー、CPS、利用契約、依拠当事者規約を https://www.globalsign.com/repository に公開する。CRL はオンラインリポジトリで公開する。CRL には、有効期限が満了しておらず、有効であり、かつ失効されたすべての証明書が、種類に応じて掲載されている。

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。エンドユーザ証明書の CRL は少なくとも 3 時間ごとに更新される。CA 証明書の CRL は少なくとも 6 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 つずつインクリメントする連続した番号を付与する。

証明書ポリシー、本 CPS、利用契約、依拠当事者規約の新版及び改訂版は、Principle 1 Policy Authority により、タイムスタンプ付きの Adobe CDS PDF 署名証明書を用いて電子署名された後、7 日以内に公表されるものとする。

2.4 リポジトリへのアクセス管理

GlobalSign CA は、公開リポジトリ及びポリシー(証明書ポリシー、CPS など)を無償で供覧に付すが、サードパーティデータベース、民間ディレクトリなどにおいてステータス情報を公開する際には料金を課すことがある。
GlobalSign CA は PDF 文書に付される電子署名によって、その文書の完全性と真正性を保証する。

3.0 本人確認と認証

GlobalSign CA は RA を運営しており、RA は証明書の申請者の本人識別情報及びその他の属性情報を認証し、真正であることを確認する。

証明書申請者は、他者の知的財産権を侵害する名称を証明書内で使用してはならない。GlobalSign CA は、申請者が申請に含まれる名称の知的財産権を有する者であるかを検証せず、またドメイン名、商標、サービスマークの所有に関連する紛争について、調停、仲裁、その他の方法で解決に関与しない。GlobalSign CA は、証明書申請者に対しなんらの義務を負うことなく、かかる紛争を理由として申請を却下することができるものとする。

GlobalSign RA は、証明書の失効を申請する者について、かか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

GlobalSign CA が発行する証明書に含まれるサブジェクト識別名は、X.500「名称」、RFC 822「名称」、及び X.400「名称」に規定される要求事項に準拠している。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まない。しかしながら、Unified Communications SSL 証明書など、特定の証明書製品については、「.local」というトップレベルドメイン名を使用したドメイン名、あるいは RFC 1918 に規定されるプライベート IP アドレスなど、外部ネットワークにおいて名前解決のできないものをサブジェクトの別名として記載することがある。GlobalSign CA は発行する証明書に RFC 2460(IPv6)または RFC 791(IPv4)に規定される IP アドレスを記載することがある。

ワイルドカード SSL 証明書及び Unified Communications SSL 証明書には、完全修飾ドメイン名または IP アドレスを記載しない。

ワイルドカード SSL 証明書では、ワイルドカードを示すアスタリスク(*)をドメイン名に含んで発行する。この証明書を発行するに先立って、GlobalSign CA はレジストリ管理下のドメイン名または「パブリック・サフィックス」の直前にワイルドカード文字(アスタリスク)が挿入されていないか(たとえば、「*.com」や、「*.co.uk」など。詳しくは RFC 6454 の 8.2 章を参照のこと)を判定するためのベストプラクティスを遂行する。証明書を申請するドメイン名空間は利用者の管理下になければならず(たとえば、「*.globalsign.com」など)、従って、GlobalSign CA は前述のようなワイルドカード SSL 証明書の申請を却下する。

SSL 証明書については、Subject フィールドの commonName の欄に完全修飾ドメイン名または正式なドメイン名が記載される一方、ホスト名欄に「www」の文字列を付加したドメイン名をサブジェクトの別名エクステンションに記載することがある。サブジェクトの別名は RFC 5280 の規定に従い、ノンクリティカルとマークされる。

3.1.2 意味のある名称である必要性

GlobalSign CA は、可能な場合、識別名を使用して証明書のサブジェクトや発行者を特定する。GlobalSign CA の製品によっては、役職名や部署名を記載するものもあり、この場合、OU フィールドの識別名に付加的な一意の要素を記載して、依拠当事者による特定を可能にすることがある。

3.1.3 利用者の匿名または Pseudonym の使用

GlobalSign CA は、ポリシーにおいて禁じられていない場合、及び名前空間における一意性が担保される場合、匿名または Pseudonym のエンドエンティティ証明書を発行することがある。GlobalSign CA は法の求めるところにより、利用者の本人識別情報を開示する権利を有する。

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 CA は証明書内のサブジェクト名の一意性を以下のとおり担保する。

- **PersonalSign1 証明書：** 一意のメールアドレスのみ

- **PersonalSign/Pro 証明書：** 一意のメールアドレス、組織名、住所、及び組織に属する個人の名前または部署名。または、一意のメールアドレス、個人の名前、及び国名
- **Code Signing 証明書：** 一意の組織名と住所、一意の個人名と住所、メールアドレスを付加することもある
- **SSL 証明書：** ICANN により一意と認められたドメイン名を commonName に記載
- **Time Stamping 証明書：** 一意の組織名と住所、メールアドレスを付加することもある
- **CA for AATL 証明書：** 一意のメールアドレス、組織名、住所、及び組織に属する個人の名前または部署名。または、一意のメールアドレス、個人の名前、及び国名
- **NAESB Rudimentary：** 一意のメールアドレスのみ
- **NAESB Basic、Medium、High：** 一意のメールアドレス、組織名、住所、及び組織に属する個人の名前または部署名
- **PDF Signing 証明書：** 一意のメールアドレス、組織名、住所、及び組織に属する個人の名前または部署名。または、一意のメールアドレス、個人の名前、及び国名
- **TrustedRoot：** CA/Browser Forum の「一般に信頼される証明書の発行及び管理に関する基本要件」に準拠する

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、GlobalSign CA は利用者が商標の所有権を有するかどうかを検証しない。しかしながら、GlobalSign CA は係争中の商標権を含む証明書を失効する権利を有する。

3.2 初回の本人識別情報の検証

GlobalSign CA は、証明書を申請する、あるいは認証局のチェーニングサービスなどの利用を申し込む、法人・個人の利用者の本人確認のために必要な連絡、調査などにおいて、あらゆる法的手続きを用いる。

GlobalSign CA は、初回の審査において検証の結果真正と認められた本人識別情報を、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。GCC アカウントにログインが可能であることをもって、検証済の情報に依拠して証明書の発行ないしサービスの提供を受ける権利を有することを確認する。再申請をする申請者については、GCC アカウントが保持する検証済の本人識別情報を、3.3.1 章の規定に従い、年月の経過に応じて再検証することとし、申請者にはその旨が通知される。

3.2.1 秘密鍵の所有を証明する方法

利用者は、PKCS#10 形式の CSR(証明書署名要求)または SPKAC(Signed Public Key and Challenge)形式のデータフォーマットで、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。

GlobalSign CA は、TrustedRoot サービスの下で GlobalSign 証明書階層にチェーンされることを希望する発行局の申請を受領するが、一次評価を受け、GlobalSign CA との個別契約を締結した後、発行局も秘密鍵の所有を証明しなければならない。認証局チェーニング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 GlobalSign CA との間で契約が締結されていれば、発行局を代表する者が RA に赴いて審査を受けることは必須としない。

3.2.2 組織の識別情報の認証

組織の識別情報を含むすべての証明書について、申請者は組織名、及び登記された(または事業を営む)住所を提示しなければならない。また、EV 証明書を除くすべての証明書については、以下のいずれか一つの方法によって、組織の法的実在性、正式名称、登記形態、及び組織が提示した住所を検証する。

- 申請者を管轄する政府機関への確認
- GlobalSign CA が正確であり信頼に足ると判断したサードパーティデータベースの情報を用いた確認
- 会計士、弁護士、政府機関担当者、その他サブジェクトの情報の検証者として通例信頼できるとみなされる第三者が、この情報が正確であることを証した認証状

上記の方法のほか、GlobalSign CA は申請者の(本人識別情報ではなく)住所を公共料金の請求書、銀行取引明細、クレジットカード明細、政府発行の税務書類、その他 GlobalSign CA が正確であり信頼に足ると判断した証明書類に基づいて検証することがある。

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 章に従って検証する。

SSL/TLS 証明書については、以下のいずれか一つの方法によって、申請する証明書に含まれるドメイン名を申請者が所有するか管理下に置いていることを検証する。

- GlobalSign の OneClickSSL の機能を用いて、GlobalSign CA が指定するテスト証明書をインストールすることで、申請者がドメインに対する管理権限を有することを証明する
- ドメイン配下の指定されたページに特定のメタデータを含むファイルをアップロードする
- レジストラまたは WHOIS に登録された連絡先に直接確認する
- 以下のいずれかの一つ以上のメールアドレスに送付されたチャレンジ・レスポンスを求めるメールに返信できることを確認する
  - webmaster@domain.com, postmaster@domain, admin@domain.com, administrator@domain.com, hostmaster@domain
  - WHOIS に連絡先として登録されているメールアドレスのいずれか
  - 3.3.1 項の規定に基づく年月の経過に応じた再検証の対象となるドメイン名の管理権限を過去に検証し、事実管理権限を有すると認められた際に使用されたメールアドレス
- レジストラから、登録者が申請者にドメインの使用を許諾していることを証する信頼に足る連絡を受ける

申請者には、さらに情報を提出することが求められることがあり、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。

3.2.2.1 LRA の認証

ePKI 及び MSSL サービスで使用するアカウントについては、GlobalSign CA は、認証済の組織情報をプロファイルとして固定する。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人、ないし組織が所有また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、すべてのサブドメインは事前に GlobalSign CA によって事前に認証済みである。)

3.2.2.2 役職情報を含む証明書の認証(DepartmentSign)

GlobalSign CA は、役職名を記載した証明書の記載内容が真正であることを正しく認証する。LRA は、組織のプロファイルに登録される役職名を、契約に基づき正確に検証する義務を負う。

役職名を含む証明書は、個人に対し発行してはならない。

3.2.2.3 EV 証明書(SSL、Code Signing)

EV 証明書については、CA/Browser Forum の「Extended Validation 証明書ガイドライン」に準拠する。

3.2.3 個人の本人識別情報の認証

GlobalSign CA は個人に発行する証明書のクラスに応じて、以下のとおり認証する。

3.2.3.1 Class 1(Personal Sign 1、PersonalSign 1 Demo 証明書)

申請者は証明書に記載するメールアドレスに対する管理権限を証明する。GlobalSign CA は、GCC への新規登録を含む、申請者が GlobalSign CA のサービスに登録する際に提示したその他の情報を認証しない。

3.2.3.2 Class 2(PersonalSign2、SSL、Code Signing、個人向け AATL)

申請者は証明書に記載するメールアドレスに対する管理権限を証明する。

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)または写真付き 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 CA 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。

GlobalSign CA 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。

- 申請者の電話番号を信頼できる情報源から入手し、電話によるチャレンジ・レスポンスを求める
- 申請者の住所を信頼できる情報源から入手し、郵便によるチャレンジ・レスポンスを求める
- 公証人または信頼できる第三者から、申請者個人と面会したこと、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の証言を得る
- 申請者の印影(管轄地方行政機関がその法的文書への押印を認めたもの)が、書面による申請に付与されている

GlobalSign CA は、申請者にさらに情報を提出することが求めることがある。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。

3.2.3.3 Class 3(PersonalSign3 Pro 証明書)

申請者は証明書に記載するメールアドレスに対する管理権限を証明する。

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)または写真付き 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 CA または信頼される第三者は、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。

公証人また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。この手続きは、PersonalSign 3 Pro の発行においては必須である。

GlobalSign CA は、以下のいずれか一つの方法によって、組織に属する申請者が証明書を申請する権限を有するかを検証する。

- 申請者の属する組織の電話番号を信頼できる情報源から入手し、電話によるチャレンジ・レスポンスを求める
- 申請者の属する組織の住所を信頼できる情報源から入手し、郵便によるチャレンジ・レスポンスを求める

申請者また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 LRA の認証

ePKI 及び MSSL サービスで使用するアカウントは 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固定する。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。

3.2.3.5 NAESB 向け証明書

NAESB向け証明書の申請については、関連会社による利用者証明書の組織認証申請の真正性を確認するために、組織名、住所、およ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。グローバルサインもしくはRAは、申請者の真正性およ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。エンドエンティティ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。

グローバルサインは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およびNAESB認定認証局要件に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、すべてのRA運用/機能に係るRAインフラおよび手続きは上記要件に準拠しなければならない。NAESB認定認証局および/または委任されたエンティティは、RA運用/機能を行うすべての当事者が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。

グローバルサイン、および/または関連するRAは申請者の身元情報がグローバルサインの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の保証レベルにより異なり、NAESB認定認証局要件に記載されなければならない。なお、文書およ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 保証レベル	NAESB 保証レベル
Level 1	Rudimentary
Level 2	Basic
Level 3	Medium
Level 4	High

GlobalSign CA または委託された RA(ePKI の場合)は、申請者により提供された本人識別情報をすべて NIST SP800-63(http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf)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 CA は、証明書のサブジェクト識別名に記載される情報のうち、CPS の本章における規定において除外される項目以外のすべてを検証する。GlobalSign CA は、サブジェクトの別名(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または免責事項、告知などの情報を提供する。

- GlobalSign CA 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すべてのタイプの証明書では、GlobalSign CA はこれらの情報を検証し、免責事項の告知を記載しない。

- GlobalSign CA が明確に識別できない「マーケティング」などの文言を情報として証明書に記載する場合には、GlobalSign CA は免責事項の告知を証明書に記載しないが、本 CPS において、こうした情報が検証されていないことを告知する。OV SSL/TLS 用の証明書に限っては、GlobalSign CA 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、これらの情報は申請者の申告にのみ依拠する。CA/Browser Forum の基本要件では、こうした情報の証明書への記載がいつまで許容されるかを規定しており、これらの項目は検証されない利用者情報に分類される。

SSL/TLS 用の証明書、及び Code Signing 証明書については、GlobalSign CA 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する。

GlobalSign CA は、ePKI サービス向けに、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を提供する。LRA は、契約に基づき役職や名称を検証する義務を負う。サブジェクトの所属名(organizationalUnitName)または commonName フィールドに記載の情報が LRA によって検証済であることを示すために、ポリシーOID(1.3.6.1.4.1.4146.1.40.10)を記載する。

3.2.5 権限の認証

- **PersonalSign1 証明書：** 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メールアドレスを管理していることを検証する
- **PersonalSign2 証明書：** 信頼できる方法による申請組織または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メールアドレスを管理していることを検証する
- **NAESB 証明書：** 3.2.3.5 項の規定に従い、信頼できる方法による申請組織または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メールアドレスを管理していることを検証する
- **PersonalSign3 証明書：** 信頼できる方法により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り、また申請者が証明書に記載されるメールアドレスを管理していることを検証する

- **Code Signing 証明書：** 信頼できる方法による申請組織または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メールアドレスを管理していることを検証する
- **EV Code Signing 証明書：** EV ガイドラインの規定に従い、契約書署名者、証明書承認者の権限を検証する
- **DV/AlphaSSL 証明書：** 以下のいずれかのチャレンジ・レスポンス方式を用いて、ドメインの所有または管理権限を検証する
  - GlobalSign の OneClickSSL の機能を用いて、GlobalSign CA が指定するテスト証明書をインストールすることで、申請者がドメインに対する管理権限を有することを証明する
  - ドメイン配下の指定されたページに特定のメタデータを含むファイルをアップロードする
  - レジストラに登録された連絡先に直接確認する
  - 以下のいずれかの一つ以上のメールアドレスに送付されたチャレンジ・レスポンスを求めるメールに返信できることを確認する
    - webmaster@domain.com, postmaster@domain, admin@domain.com, administrator@domain.com, hostmaster@domain
    - WHOIS に連絡先として登録されているメールアドレスのいずれか
  - もし証明書情報(DN:Distinguished Name)に国コードが含まれている場合、GlobalSign は DNS クエリーで獲得した IP アドレスの位置情報(geolocation)に基づき、国情報を検証する
- **OV SSL 証明書：** 信頼できる方法による申請組織または個人との連絡を通じた検証に加え、レジストラまたは WHOIS に登録されている連絡先に対しチャレンジ・レスポンス方式を用いて、もしくは直接連絡して、ドメインの所有または管理権限を検証する
- **EV SSL 証明書：** EV ガイドラインの規定に従い、契約書署名者、証明書承認者の権限を検証する
- **Time Stamping 証明書：** 信頼できる方法により、申請組織との連絡を通じて検証する
- **CA for AATL 証明書：** 信頼できる方法による申請組織または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メールアドレスを管理していることを検証する
- **PDFSigning 証明書：** 信頼できる方法により、申請組織または個人との連絡を通じて検証する
- **TrustedRoot：** 信頼できる方法により、申請組織との連絡を通じて検証する

3.2.6 相互運用のための基準

該当なし

3.3 Re-key 要求における本人確認と権限の認証

GlobalSign 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)要求に対応する。GlobalSign 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。GCC においては、Re-key は「更新」と呼ばれている。

3.3.1 定期的な Re-key とその際の本人確認と権限の認証

- **PersonalSign1 証明書：** ユーザ名・パスワードによる 9 年ごとの再検証が必要
- **PersonalSign2 証明書：** 9 年ごとに本人識別情報の再検証が必要であり、ユーザ名・パスワードによる認証またはその時点で有効期限が満了していない、かつ失効していない証明書を用いたクライアント認証が求められる
- **PersonalSign3 証明書：** 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 証明書：** ユーザ名・パスワードによる 6 年ごとの再検証が必要
- **EV Code Signing 証明書：** EV ガイドラインに従った本人識別情報の再検証が必要であり、ユーザ名・パスワードによる認証が求められる
- **DV SSL 証明書：** ユーザ名・パスワードによる 6 年ごとの再検証が必要
- **OV SSL 証明書：** ユーザ名・パスワードによる 6 年ごとの再検証が必要
- **EV SSL 証明書：** EV ガイドラインに従った本人識別情報の再検証が必要であり、ユーザ名・パスワードによる認証が求められる
- **Time Stamping 証明書：** 取り扱わない
- **CA for AATL 証明書：** ユーザ名・パスワードによる 6 年ごとの再検証が必要
- **PDFSigning 証明書：** 取り扱わない
- **TrustedRoot：** 取り扱わない
- **Alpha SSL：** 取り扱わない
- **NAESB 証明書：** 以下のテーブルに基づいて本人確認が必要

保証レベル	本人確認要件
Rudimentary	有効期限が満了する前の鍵を保持すること。
Basic	有効期限が満了する前の鍵を保持すること。ただし、最低5年に1度は初期登録時と同様のプロセスを実施し、本人識別情報を再検証が必要となる。
Medium	有効期限が満了する前の鍵を保持すること。ただし、最低3年に1度は初期登録時と同様のプロセスを実施し、本人識別情報を再検証が必要となる。
High	有効期限が満了する前の鍵を保持すること。ただし、最低年次で初期登録時と同様のプロセスを実施し、本人識別情報を再検証が必要となる。

証明書失効後の再発行における本人確認および認証方法
証明書が失効していた場合、利用者は初期登録時と同様のプロセスを実施し、新しい証明書を発行する必要がある。

証明書情報が変更になった際の再審査および本人識別情報
CA により発行された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 CA は、利用者が上記の上限を超えて証明書を使用することを許可せず、利用者が上記の上限を超えての証明書の利用を希望する場合には、Re-key の際に再審査を行う。

3.3.2 失効後の Re-key とその際の本人確認と権限の認証

GlobalSign CA は失効されていない証明書の Re-key に対応する。証明書を失効後、再度証明書の発行を希望する場合、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 失効要求における本人確認と権限の認証

GlobalSign CA は、失効要求について、要求者の権限を検証する。GlobalSign CA は、失効要求を行う要求者に対して、ユーザ名・パスワードによる認証、証明書に記載されたドメイン名やメールアドレスなどが要求者の所有するものであることの確認、ネットワークを経由しない方法で検証済の特定の情報を用いて本人確認を行うなどのチャレンジ・レスポンス方式を用いて、その権限を検証する。

- **PersonalSign1 証明書：** ユーザ名・パスワードによる認証またはオフラインでの検証
- **PersonalSign2/Pro 証明書：** ユーザ名・パスワードによる認証またはオフラインでの検証
- **NAESB 証明書：** ユーザ名・パスワードによる認証またはオフラインでの検証
- **PersonalSign3 Pro 証明書：** ユーザ名・パスワードによる認証またはオフラインでの検証
- **Code Signing 証明書：** ユーザ名・パスワードによる認証またはオフラインでの検証
- **EV Code Signing 証明書：** EV ガイドラインに準拠する

- **DV SSL 証明書：** ユーザ名・パスワードによる認証、オフラインでの検証または OneClickSSL 機能によるドメインの管理権限の検証
- **AlphaSSL 証明書：** オフラインでの検証または OneClickSSL 機能によるドメインの管理権限の検証
- **OV SSL 証明書：** ユーザ名・パスワードによる認証またはオフラインでの検証
- **EV SSL 証明書：** EV ガイドラインに準拠する
- **Time Stamping 証明書：** オフラインでの検証
- **CA for AATL 証明書：** ユーザ名・パスワードによる認証またはオフラインでの検証
- **PDFSigning 証明書：** ユーザ名・パスワードによる認証またはオフラインでの検証
- **TrustedRoot：** オフラインでの検証

GlobalSign CA は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。該当するケースには、たとえば、利用者の利用契約違反、料金の不払いなどに伴う失効手続きがある。

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 CA は、証明書の申請を承認しない個人またはエンティティのリストを独自に作成する。加えて、GlobalSign CA 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、また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。
GlobalSign CA は、その事業所の所在国の法律が取引を禁じる対象者に証明書を発行しない。
EV ガイドラインは、EV SSL または EV Code Signing 証明書発行のための規則を規定する。申請者は、GlobalSign CA の提供するサービスの内容に応じて、適切な形式の証明書要求を提出し、ならびに電子的に、またはその他の事前に承認された形式の利用契約に同意しなければならない。

証明書申請は以下のいずれかの方法で提出できる。

- **オンライン申請：** Web インターフェース(https セッション)による申請。証明書申請者は、GlobalSign CA が規定する手続きに従い安全な方法で申請を送信する。GlobalSign CA と直接契約をする顧客の多くはこの方法を使用する。このために使用するアカウントを GCC、すなわち GlobalSign Certificate Centre と呼び、このアカウントへのログインには適切な強度のユーザ名とパスワードを使用する。GCC アカウントでは、証明書のライフサイクルを管理することができる。このアカウントは、MSSL サービス顧客用、ePKI サービス顧客用、直接取引顧客用、パートナー用、代理店用に別けられる。

- **API 経由の申請：** 代理店、パートナー、大企業は、GlobalSign CA に適切な形式の証明書要求を送信するにあたり、API (Application Programming Interface)を使用することができる。API を通じてデータを送信する際には、適切な強度のユーザ名とパスワードが求められる。GlobalSign CA は、ほかに利用制限をかけない場合には、申請者の送信元 IP アドレスをデータに含めることを求めることができる。提供するアカウントは、API 用または SAPI(Simple API)用に別けられる。

- **OneClickSSL による申請：** アカウントを持たないユーザは、OneClickSSL 機能を使用して申請することができる。この申請手続きにおいてドメインの管理権限が確認できた場合には、この認証済のドメイン名を用いて初回及びその後の証明書ライフサイクル管理を行う。

- **マニュアル申請：** TrustedRoot サービスの利用、タイムスタンプ証明書の発行、または GCC アカウントで申込みが可能な上限数を超え

た SubjectAlternativeName を証明書に記載することを希望する申請者は、直接電子メールによって、またはネットワークを経由しない方法で申請情報の検証を受けるよう申し込むことができる。

4.1.2 登録手続きとそこで負うべき責任

GlobalSign CA は、依拠当事者に申請者の本人識別情報を提示するすべ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、手続きを採用している。申請者は、必要な検証を行えるよう、GlobalSign CA 及び GlobalSign RA に対し情報を提出しなければならない。GlobalSign CA 及び GlobalSign 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。

申請にあたっては以下の手続きを踏むことになるが、鍵の生成は検証が終わってから行われる場合もあり、必ずしもこの順番では行われない。

- 適切に安全なプラットフォームにおいて、鍵ペアを生成する
- 適切に安全なツールを用いて証明書署名要求(CSR)を生成する
- 証明書タイプに応じた申請と必要な情報を提出する
- 利用契約、約款に同意する
- 料金を支払う

4.2 証明書申請手続き

4.2.1 本人確認と認証の実施

GlobalSign CA は、本 CPS の規定に従い、本人識別情報の真正性を十分に検証するシステム、手続きを採用している。初回の本人確認は、GlobalSign CA の検証チームまたは契約している RA が 3.2 項の規定に準拠して実施する。ファックス、電子メールで GlobalSign CA に提出された申請者の情報は、GCC アカウント、またはパートナーから GlobalSign CA 提供の API 経由で提出された情報とともに、安全に保管される。初回以降の証明書申請については、ユーザ名・パスワードの単一要素による認証か、または電子証明書とユーザ名・パスワードの多要素による認証のいずれかを用いて権限を検証する。

4.2.2 証明書申請の承認または却下

GlobalSign CA 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。GlobalSign CA は、証明書申請を承認することが GlobalSign CA のブランドを傷つける可能性があると判断した場合も、それを却下することができる。GlobalSign CA は、過去に証明書申請を却下した、あるいは利用契約に違反した申請者からの証明書申請を却下することができる。

SSL 及び Code Signing 用 EV 証明書については、検証チームの 2 名が証明書申請を承認しなければならない。GlobalSign CA は各国で事業を行っているが、GlobalSign CA が社内で処理できない言語の申請については、当該言語で申請を処理し、文書を翻訳することのできる、適切に研修と経験を積んだ外部の RA に事前審査手続きを委託することができる。

本 CPS の規定に従いすべての検証手続きが完了した場合には、GlobalSign CA は証明書要求を承認する。

GlobalSign CA は、証明書申請が却下された理由を申請者に説明する義務を負わない。

4.2.3 証明書の申請処理に要する期間

GlobalSign CA は、証明書申請を検証し処理するために必要とされるすべての適切な手続きを行う。GlobalSign CA の支配の及ばない理由によって問題が生じた場合には、GlobalSign CA は申請者に適切に情報を伝達する。

EV 証明書については、GlobalSign CA は、契約書署名者に利用契約への同意を求める前に、すべての提出された情報が正しいかどうか、検証を行う。

以下は、証明書申請の処理、及び証明書の発行までに必要な時間の概算である。

- **PersonalSign1 証明書：** およそ 1 分
- **PersonalSign2 証明書：** およそ 24～48 営業時間
- **PersonalSign2 Pro 証明書：** およそ 36～72 営業時間
- **NAESB 証明書：** およそ 24～48 営業時間
- **PersonalSign3 Pro 証明書：** およそ 48～72 営業時間

- **Code Signing 証明書：** およそ 24～48 営業時間
- **EV Code Signing 証明書：** およそ 48～96 営業時間
- **DV SSL 証明書：** およそ 1～5 分(*)
- **AlphaSSL 証明書：** およそ 1～5 分(*)
- **OV SSL 証明書：** およそ 24～48 営業時間
- **EV SSL 証明書：** およそ 48～96 営業時間
- **Time Stamping 証明書：** およそ 5～10 営業日
- **CA for AATL 証明書：** およそ 24～48 営業時間
- **PDF Signing 証明書：** およそ 24～48 営業時間
- **TrustedRoot：** 6～12 週間(テスト、及びオフラインのキーセレモニーのスケジューリングを含む)

*DV・Alpha SSL 証明書の申請におけるドメイン名の所有または管理権限の検証にあたって、潜在リスクが高いとみなされた場合には、OV SSL 証明書の申請に近い検証手続きを取ることがある。

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 CA 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。これは、GlobalSign CA が直接運営する RA に限らず、契約に基づいて運営される RA も同じである。エンタープライズ RA、LRA については、GlobalSign CA と直接的な通信を行なわないため、多要素の認証は必須ではない。RA は、GlobalSign CA に提出されたすべての情報を検証し、改ざん、不正使用されないようこれらの情報を保護する。

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 CA は、登録手続きの際に連絡先として提示されたメールアドレス、または同様の連絡先を通じて、証明書の発行を利用者に通知する。この通知を行うメールには、発行する証明書タイプ用のワークフローにより、証明書そのものを添付している場合、もしくはダウンロードするための URL を記載している場合がある。

4.3.3 利用者への NAESB 用証明書の発行に関する通知

申請者の本人確認及び権限の検証の結果、証明書が発行できると判断され次第、GlobalSign CAは証明書を発行し、申請者に通知し、申請者に証明書を提供する。

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 CA 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。利用者が、このような通知を含む GlobalSign CA からの電子メールを受信後 7 日以内に GlobalSign CA に連絡をしない場合、この電子証明書は受領されたものとみなす。

4.4.2 認証局による証明書の公開

GlobalSign CA による証明書の公開は、利用者に証明書を交付することにより行われる。加えて、企業である顧客に対しては、GlobalSign CA は LDAP のようなディレクトリを通じて証明書を公開することがある。

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、パートナーまたは代理店は、利用者の登録手続きに関与した場合、当該利用者への証明書の発行が通知される。

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 CA 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する。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。鍵ペア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、すべての鍵を安全に消去しなければならない。

4.5.2 依拠当事者による公開鍵と証明書の利用

GlobalSign CA は、CRL や OCSP など証明書の有効性を検証するサービスによる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本 CPS に規定する。GlobalSign CA 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、利用者に対し提供する。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また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。

GlobalSign CA は、以下の製品・サービスについて、証明書の更新を取り扱う。

- **PersonalSign1 証明書：** GCC アカウントで Re-key として取り扱う
- **PersonalSign2 証明書：** GCC アカウントで Re-key として取り扱う
- **PersonalSign2 Pro 証明書：** GCC アカウントで Re-key として取り扱う
- **PersonalSign3 Pro 証明書：** GCC アカウントで Re-key として取り扱う
- **Code Signing 証明書：** GCC アカウントで Re-key として取り扱う
- **EV Code Signing 証明書：** GCC アカウントで Re-key として取り扱う
- **DV SSL 証明書：** GCC アカウントで Re-key として取り扱う
- **AlphaSSL 証明書：** GCC アカウントで Re-key として取り扱う
- **OV SSL 証明書：** GCC アカウントで Re-key として取り扱う
- **EV SSL 証明書：** GCC アカウントで Re-key として取り扱う
- **Time Stamping 証明書：** マニュアル手続きで対応
- **NAESB 証明書：** GCC アカウントで Re-key として取り扱う
- **CA for AATL 証明書：** GCC アカウントで Re-key として取り扱う
- **(すべての)PDF Signing 証明書：** GCC アカウントで Re-key として取り扱う
- **Managed SSL(MSSL)：** サービスに付帯して提供するシステムに再発行機能が搭載されている
- **Enterprise PKI(ePKI)：** サービスに付帯して提供するシステムに再発行機能が搭載されている
- **TrustedRoot：** マニュアル手続きで対応

GlobalSign CA は、以下の条件下で再発行を行う。

- 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
- 証明書に記載されているすべての情報が正しく、改めて検証が必要でないこと

GlobalSign CA は、(上記の条件に基づき)すでに更新済または Re-key 済の証明書を再更新または再 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 CA は、GCC アカウントのログイン認証など、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。ITEF の RFC の規定では、更新申請において証明書署名要求(CSR)は必須ではないが、GlobalSign CA では、「更新」という用語を、同一の公開鍵を使用するものの技術的観点からは Re-key となる手続きを指して使用している。

4.6.3 証明書更新申請の処理

GlobalSign CA 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ある。

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

(規定なし)

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、従前に発行を受けた証明書と同一の情報を記載しているが、新しい公開鍵を含み、有効期限の異なる証明書を新たに発行することである。

証明書の有効期限に到達する前に、同一の有効期限で証明書を Re-key した場合、これを「再発行」と呼ぶ。

GlobalSign CA は、以下の製品・サービスについて、証明書の Re-key または再発行を取り扱う。

- **PersonalSign1 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **PersonalSign2 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **PersonalSign2 Pro 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **PersonalSign3 Pro 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **Code Signing 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **EV Code Signing 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **DV SSL 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **AlphaSSL 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **OV SSL 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **EV SSL 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **Time Stamping 証明書：** マニュアル手続きで Re-key・再発行に対応
- **NAESB Certificates** GCC アカウントで Re-key・再発行を取り扱う
- **CA for AATL 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **PDF Signing 証明書：** GCC アカウントで Re-key・再発行を取り扱う
- **Managed SSL(MSSL)：** サービスに付帯して提供するシステムに再発行機能が搭載されている
- **Enterprise PKI(ePKI)：** サービスに付帯して提供するシステムに再発行機能が搭載されている
- **TrustedRoot：** マニュアル手続きで Re-key・再発行に対応

GlobalSign CA は、以下の条件下で Re-key を行う。

- 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
- 証明書に記載されているすべての情報が正しく、新規に、あるいは改めて検証が必要でないこと

GlobalSign CA は、(上記の条件に基づき)すでに更新済または 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 CA 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または利用者を代理して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。Re-key 申請において証明書署名要求(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 CA は証明書 Re-key また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、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

(規定なし)

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 CA は、情報修正を、新規の証明書発行として取り扱う
- GlobalSign CA は、過去に更新または 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

(規定なし)

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)にシリアルナンバー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鍵を使用して電子署名される。シリアルナンバー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。GlobalSign CA は CRL のファイルサイズを適切な管理するため、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。GlobalSign 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。失効は以下の条件下で行われる。

- 利用者または組織の担当者が、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失効を要求した場合
- 利用者が OneClickSSL の機能を用いて電子証明書の失効を要求した場合
- 利用者が GlobalSign CA のサポートチーム、または GlobalSign CA の RA を通じて失効を要求し、利用者の本人確認ができた場合
- GlobalSign CA が、利用者の秘密鍵(証明書に記載される公開鍵と対になるもの)が危殆化したこと、脆弱なアルゴリズムを用いて生成されたこと、あるいは電子証明書が不正に使用されたことを示す相当な証拠を入手した場合
- GlobalSign CA が、利用者に利用契約に基づく重大な義務違反があったとの報告を受けるか、あるいは何らかの方法で知った場合
- GlobalSign CA が、利用者が証明書をフィッシングなどの犯罪行為に使用したとの報告を受けるか、あるいは何らかの方法で知った場合
- GlobalSign CA が、証明書の Subject または subjectAlternativeName フィールドに記載された利用者の情報について利用者が使用する権利を失効させる裁判所判決または調停裁決があったこと、あるいは使用する権利を喪失したことの報告を受けるか、あるいは何らかの方法で知った場合
- GlobalSign CA が証明書に記載された情報に重大な変更があったとの報告を受けるか、あるいは何らかの方法で知った場合
- GlobalSign CA が、自己の裁量により、GlobalSign CA のベストプラクティスまたはそのポリシーに基づいて証明書が発行されなかったと判断した場合
- GlobalSign CA が証明書に記載された情報が正確ではないと判断した場合
- GlobalSign CA が事業を停止し、他の認証局より証明書の失効サービスを提供する手配をしなかった場合
- GlobalSign CA が証明書を発行する権利を喪失するか、その証明書が失効または有効期限を満了し更新されなかった場合
- GlobalSign CA の発行局証明書の秘密鍵が危殆化した場合
- GlobalSign CA が、利用者が取引禁止対象者リストなどに登録されたこと、あるいは GlobalSign CA の事業所のある国・地域の法律で取引を禁止された国、地域に居住するか事業を行っているとの報告を受けるか、あるいは何らかの方法で知った場合
- 証明書の使用を継続することが、GlobalSign CA の事業または依拠当事者に対し害をなす場合
- 利用者がハードウェアトークンのパスフレーズを逸失するなど、トークンに搭載された秘密鍵に対する管理権限を喪失する可能性がある場合

証明書の使用が GlobalSign のブランドを傷つけると考えられる場合、GlobalSign CA は以下を含む項目について検討する。

- 寄せられる申し立ての内容及び数
- 申立人が誰であるか
- 効力を有する適用法
- 利用者が証明書を使用することが有害とされることについての対応

TrustedRoot 認証局については、GlobalSign CA は発行局の証明書を以下の場合に失効する。

- TrustedRoot 認証局が GlobalSign CA との契約条項に適合しない場合

4.9.2 失効要求者

GlobalSign CA 及びその 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、利用者本人または証明書に記載された組織から提出された場合、受理される。GlobalSign 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。

4.9.3 失効要求の処理手続き

失効要求の持つ性質と効率化の観点から、GlobalSign CA はシステムを通じて失効要求者の本人確認を行う。第一に、GCC 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。次に代替方法として、ファックス、郵便、電話などを通じて、ネットワークを経由せずに失効を要求することができる。この場合、GCC アカウントを通じて共有される非公開情報に基づいて、失効要求者の本人確認を行う。また、GCC アカウントが提供されない利用者については、証明書のサブジェクト識別名に関連する一つ以上の要素に対する管理権限を証することで、失効要求権限を検証することもできる。SSL/TLS 証明書については、OneClickSSL 機能によるドメインの管理権限の検証をもって代替とすることが可能である。S/MIME 証明書については、メールアドレスの管理権限の検証をもって代替とすることが可能である。

GlobalSign CA 及び GlobalSign 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 は本 CPS に準拠して発行される。

4.9.4 失効要求までの猶予期間

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。利用者は 24～48 時間の猶予を与えられるが、これを過ぎると GlobalSign CA は利用者の証明書を失効することができる。利用者、GlobalSign CA のいずれかが、何らかの理由により失効を処理できない場合、リスク分析を行い、記録する。

4.9.5 認証局が失効要求を処理すべき期間

GlobalSign CA は、鍵の危殆化の疑いや証明書の不正使用の報告を受けた後、24 時間以内に調査を開始する。

エンドエンティティ証明書の失効要求については、GCC アカウントを通じて送信された失効要求、及び GlobalSign CA 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 30 分以内に処理されなければならない。

TrustedRoot サービスについては、GlobalSign CA 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)を生成後 12 時間以内に発行する。

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、証明書が有効であることを確認しなければならない。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すべての階層の証明書について、CRL または 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 CA は、依拠当事者が失効情報の検証を容易に行えるよう、以下の URL を証明書に記載する。

- http://crl.globalsign.net
- http://crl.globalsign.com/gs/
- http://ocsp.globalsign.com
- http://ocsp2.globalsign.com
- http://crl2.alphassl.com/gs/
- http://crl.alphassl.com/

PDF 署名証明書については、依拠当事者は Adobe ルート CRL も検証することが必要である。この CRL は本 CPS の規定の範囲ではないが、次の URL で参照することができる。http://crl.adobe.com/cds.crl

4.9.7 CRL の発行頻度

GlobalSign CA は、CRL の発行頻度については、CA/Browser Forum が発行する「一般に信頼される証明書の発行及び管理に関する基本要件」及び「Extended Validation 証明書ガイドライン」に準拠する。GlobalSign のルート認証局及びオフライン認証局は、CRL を 6 か月ごとに発行する。GlobalSign CA のオンライン認証局 G2(第 2 世代)及び G2-SHA256(SHA256 対応第 2 世代)については、3 時間ごとに有効期間が 1 週間の CRL を発行する。GlobalSign CA が過去に運用し、今後証明書を発行しない認証局は、有効期間が 1 週間～1 か月の間の CRL を発行する。

4.9.8 CRL の最大通信待機時間

GlobalSign CA は、オンライン認証局の CRL を 3 時間ごとに発行する。GlobalSign が運用する RA システムから受領する失効要求は、CRL の発行 30 分前までに受領すれば、3 時間ごとに発行される CRL の次回分に記載される。
GlobalSign CA が相互認証する TrustedRoot サービスにおいて運用される認証局については、GlobalSign CA は危殆化の事実の確認後 24 時間以内に失効し、ARL を生成後 12 時間以内に発行する。

4.9.9 オンラインでの失効情報の確認

GlobalSign CA は、CRL のほか、OCSP レスポンダにより失効情報を提供する。通常のネットワーク環境においては、OCSP による応答までの待機時間は 10 秒を超えない。

4.9.10 オンラインでの失効情報の確認の要件

依拠当事者は失効情報を確認しなければならず、これを怠った場合には、すべての保証は適用されない。

4.9.11 その他の方法による失効情報の提供

(規定なし)

4.9.12 認証局の鍵の危殆化に伴う特別な要件

GlobalSign CA 及びその 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 CA 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、GlobalSign CA は発行局の証明書、エンドエンティティ証明書などを 24 時間以内に失効し、CRL をオンラインで 30 分以内に、及び ARL を 12 時間以内に発行する。

4.9.13 証明書の効力の一時停止を行う条件

GlobalSign CA は証明書の効力の一時停止を行わない。

4.9.14 証明書の効力の一時停止の要求者

該当なし。

4.9.15 証明書の効力の一時停止手続き

該当なし。

4.9.16 証明書の効力の一時停止期限

該当なし。

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 CA 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。このサービスは以下の URL において電子証明書の依拠当事者に提供される。

- http://crl.globalsign.net
- http://crl.globalsign.com/gs/
- http://ocsp.globalsign.com
- http://ocsp2.globalsign.com
- http://crl2.alphassl.com/gs/
- http://crl.alphassl.com/

4.10.2 サービスを利用できる時間

GlobalSign CA 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。

4.10.3 運用上の特性

(規定なし)

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、または有効期限を満了することで終了することができる。TrustedRoot サービスについては、GlobalSign CA と利用者との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 キーエスクローとリカバリー

4.11.1 キーエスクローとリカバリーのポリシーと手続き

認証局の秘密鍵は預託されてはならない。GlobalSign CA は利用者に対してもキーエスクローサービスを提供しない。

4.11.2 鍵カプセル化とリカバリーのポリシーと手続き

(規定なし)

5.0 施設、経営及び運用上の管理

5.1 物理的管理

GlobalSign CA 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、災害対策など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、また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為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 CA 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 CA は、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またはデータに対して齎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線(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 CA 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 CA 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 CA 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 CA 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。すべ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 CA は情報の格納に使用された、すべ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 CA 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為に適切なものであり、週に一度作成される。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も、週に一度作成される。災害またはメディア停止に伴い、すべ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為、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 CA は、点検要員を含むすべ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、いかなる人物も単独で 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)

- セキュリティ　オフィサーまたは情報セキュリティ長：セキュリティ実践導入の管理に対する全体的な責任
- 管理者：証明書の作成、廃止、停止を承認
- システム　エンジニア：　証明書のライフサイクル管理に使用される認証局システムのインストール、設定及び保守を許可されている
- オペレーター：日常的に認証局システムの操作に責任を持つ。システムバックアップ及び復旧操作を許可されている
- 監査人：認証局本体のアーカイブ及び監査ログの閲覧を許可されている。
- 認証局起動データ保有者：認証局ハードウェアセキュリティモジュール操作に必要である、認証局起動データの保有を許可されている
- 点検要員：適切な登録システムを経由したデジタル証明書内に含まれる為に、データの信頼性及び整合性確認の責任を持つ

5.2.2 タスク毎に必要な人員数

GlobalSign CA は、タスクごとに少なくとも 2 名の要員を要求する。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為、全認証局サービス(鍵生成、証明書生成、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。すべての関係者は先に 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 各役割の本人確認及び認証

信頼された役割に指名する前に、GlobalSign CA は該当者のバックグラウンドチェックを行うものとする。
先に述べた各役割は、認証局をサポートする為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為のものである。

5.2.4 責任の分離を要する役割

GlobalSign CA は、認証局設備、手続き的、また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の 5.2.1 項に定義される役割に指定される。以下の役割を同時に所有することは禁止されている。

- セキュリティ　オフィサー及びシステム・エンジニアか、オペレーター
- 監査人及びセキュリティ　オフィサーか、オペレーター、管理者あるいはシステム・エンジニア
- システム・エンジニア及びオペレーターか、管理者

如何なる個人も、1 つ以上の役割に割り当てられないものとする。

5.3 人員コントロール

5.3.1 資格、経験及び許可条件

GlobalSign CA 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 CA の人員は、正式なトレーニング、教育、実地経験またはそのいずれか 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。
5.2.1 項にて規定される、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 CA の人員(一時的勤務・永続的勤務の両者を含む)は、責任分散及び権限の最小化という視点に立ち、職務、アクセスレベル、バックグラウンドチェック、従業員教育、意識度などに基づく役職の詳細を明確にする職務表を有するものとする。
GlobalSign CA 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またはトレーニング経験を有し、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 CA の信頼された役割に従事する者は全員、認証局運営の公平さを損なうような相反する利益を持たない者とする。
GlobalSign CA は、役職に対して適正に影響すると思われる重罪あるいはその他犯罪に前科を持つ人物を、信頼された役割あるいは管理者に指名しないものとする。
すべての必要な確認が終わるまでは、人員は信頼済みの機能にアクセスしないものとします。
GlobalSign CA は、当該人物に対し過去の前科内容の提供を要求し、またそれを拒否する場合には適用を却下するものとする。
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。

5.3.3 研修要件

GlobalSign CA は、認証局のオペレーションに関して業務を行なう人員が全員、次にあげる中で包括的な研修を受けることを保証する。

- 認証局・RA セキュリティ規則及び仕組み
- 認証局システム上で使用のソフトウェア・バージョンにて
- 各担当者が履行すると考えられる業務
- 災害復旧と事業継続の手続き

GlobalSign CA または RA システムで変更が生じる場合、GlobalSign CA または RA 人員は再教育されるものとする。
更新研修は必要に応じて行い、また GlobalSign CA は少なくとも一年間に一度は更新と研修の必要性を見直すものとする。

5.3.4 再研修の頻度及び条件

信頼された役割の責任を負う者は、GlobalSign CA または 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も研修(認識度)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条件

GlobalSign CA 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また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、本 CPS、認証局の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 CA 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トレーニング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 CA は本 CPS、該当する証明書ポリシー、関連する法規、ポリシーまた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、ユーザーマニュアル等)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。
書類は全人員のトレーニング受講有無及び、受講済みトレーニングのレベルを認識の上、保守される。

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、認証局のセキュリティ及びサービスに関するすべ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

また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 CA は、認証局のサービスにおいて信頼された役割を担う者が行なう如何なる行為の透明性を証明する為、認証書ライフサイクルに関するすべての事項は記録されるものとする。少なくとも、各監査記録は下記の要素を含むものとする。(自動的または手動的の記録如何に関わらず)

- イベント(出来事)の種類
- イベントの発生した日時
- 可能であれば、そのイベントの成功または不成功
- イベントを生じた物またはオペレーターの識別
- イベントが目標とされた物の識別
- イベントの原因

5.4.2 ログ処理の頻度

監査ログは定期的及び如何なる悪意ある行為の証拠の確認、また重要なオペレーションの追跡ために適切に見直されるものとする。

5.4.3 監査ログの保有期間

監査ログ記録は、該当する法規の定めに従い、必要な法的証拠を提供可能な期間中は保有されなければならない。稼働中の証明書についての取引に関する質問が発生する限りは、記録が必要とされる可能性がある。

5.4.4 監査ログの保護

すべての保有期間中において、発生イベントは削除または破壊(長期的メディアへの移行を除く)されない方法で記録されなければならない。
イベントは、データの整合性、信頼性及び機密性に変更を加えることなく許可・信頼されるアクセスによってのみ、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。
保存期間中、イベントは解読可能な状態で保護されなければならない。イベントには、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為、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(例としては、防災対策など)に、正当かつ信頼性のある当該担当者の下、関連する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)

監査処理はシステムの起動時に呼び出され、またシステムが終了時に終了する。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。監査収集処理中に問題が発生した場合、GlobalSign CA は問題が解決するまでの間、当該認証局のオペレーションを停止するかを必ず判断し、そ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

(規定なし)

5.4.8 脆弱性の査定

GlobalSign CA は、証明書発行製品及びサービスに関する GlobalSign CA の資産に対して、日常的に脆弱性に関する査定を行なうものとする。当査定は、証明書発行処理に対する不正アクセス、不正行為、改ざん、入れ違いまた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

GlobalSign 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。少なくとも、下記のデータはアーカイブするものとする。

下記を含む、GlobalSign CA の鍵ライフサイクル管理イベント

- 鍵生成、バックアップ、格納、復旧、アーカイブ、そして破棄
- 暗号化デバイスのライフサイクル管理イベント　及び
- 認証局システムの設備設定

下記を含む、認証局の鍵発行システム管理イベント

- システムの起動及び終了
- 生成、削除、またはパスワードの設定もしくはシステム変更を企てる行為
- 発行局の鍵に対する変更

下記を含む、認証局及び利用者の認証ライフサイクル管理イベント

- 認証要求、更新及び Re-key 要求、ならびに失効における成功・不成功両方のケースの結果
- 本 CPS に規定されるすべての検証行為
- 検証電話の日時、使用された電話番号、会話をした人物名及び最終結果
- 認証要求の受諾及び拒否
- 証明書の発行
- 証明書及び証明書失効リストのディレクトリに対する閲覧及び記入操作の失敗を含む、証明書失効リストの作成及びオンライン証明書状態プロトコルの入力操作

下記を含むセキュリティ　イベント

- PKI テムのアクセス実行の結果(成功・不成功を含む)
- PKI 及びセキュリティシステムでの操作
- セキュリティプロファイルの変更
- システムのクラッシュ、ハードウェアの故障、またその他異常事態
- ファイヤーウォール及びルーターの稼動内容
- 認証局施設への進入及び退出

書類及び監査

- GlobalSign　CA 及びコンプライアンス監査人の間で交わされるコミュニケーションに関わる全作業を含む全書類の監査
- GlobalSign CP 及び以前のバージョン
- GlobalSign CPS 及び以前のバージョン
- 利用者及び GlobalSign CA 間で交わされる合意契約書

タイムスタンプ

- 時刻同期

その他

- アーカイブ内容を確認可能なその他データ、もしくアプリケーション
- 設備故障
- UPS 故障または停電
- GlobalSign CP または本 CPS に対する違反行為

5.5.2　アーカイブの保有期間

アーカイブされたデータの最短保存期間は 10 年間となる。

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(長期的メディアへの移行を除く)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、データの整合性、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

(規定なし)

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を考慮しなければならない。スタンピング方法に関わらず、すべてのログはイベントの発生時刻データの明記が必要となる。

5.5.6 アーカイブ収集システム(内部または外部)

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従うものとする。

5.5.7 取得手続き及びアーカイブ情報の検証

GlobalSign CA 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整合性の継続、及び可読性が検証される。許可された GlobalSign CA 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 CA は、6.3.2 項に従って定期的に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強調すべく、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 事故及び危殆化に対する対応手続き

GlobalSign CA は、コンピューティング資産、ソフトウェアまたはデータの損壊・損失など、サービスの運営を妨げる、また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 CA 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為、監査処理の対象範囲となる。
GlobalSign CA で信頼された役割及びオペレーションを担う人員は、特に重要な業務について、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 CA がハッキングまた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為の調査を行なうものとする。
もしくは GlobalSign CA により、認証局または 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(または)被害による認証局階層の宣言が必要な場合の判断を行なう為に、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、失効及び証明書の状態情報)

5.7.2 コンピューティング資産、ソフトウェア、またはデータが損壊

万一いずれの設備が損壊または操作不能な状態で、しかしながら署名鍵が損壊していない場合、GlobalSign CA 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、可能限り早急に再構築されるものとする。

5.7.3 エンティティの秘密鍵が危殆化した際の手続き

GlobalSign CA の署名鍵が危殆化、紛失した、または破壊された、または破損されたと考えられる場合、

- GlobalSign CA は問題の調査の後、CA 証明書を失効すべきかを判断する。もし GlobalSign CA が失効すべきと判断した場合、以下を実施するものとする。
  - 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または既存の他の認証局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、災害復旧計画は事業継続について取り決めている。証明書状態情報システムは 1 日 24 時間、年間 365 日を通して利用可能な状態に展開されるものとする。(予定された保守操作を除き、99.95%の利用可能状態)

5.8 認証局または RA の稼動終了

GlobalSign CA または RA が稼動終了する場合、GlobalSign CA は終了前に全利用者に通知をするものとし、且つ、以下を実施する：

- 本 CPS に従って、証明書の配布を停止する
- 全監査ログ及びその他情報を、終了前にアーカイブする
- 全秘密鍵を終了にあたり、破棄する
- アーカイブデータが同様のサービスを提供する他の GlobalSign CA などの適切な権限保持者に移行されていることを保証する
- 顧客及びソフトウェアプラットフォーム提供者に対して、トラストアンカーを削除するよう安全な手法を用い通知する

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 CA 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 2 名の管理で、すべ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)が立会い、またセレモニー全工程はビデオ録画されなければならない。GlobalSign CA の鍵生成は、少なくとも FIPS140－2 レベル 3 また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(AutoCSR)GlobalSign CA は、鍵生成の工程から利用者への全発行過程において、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。これには、鍵の整合性、適切な乱数生成機または暗号論的擬似乱数生成器を介して鍵データのランダム性、また鍵を利用者に届ける為の適切な暗号メカニズムを選択できる能力を含む。GlobalSign CA は秘密鍵をアーカイブしないこと、また鍵生成工程中に鍵が存在した、いずれの一時的な場所においても消去されたことを保証しなければならない。

6.1.3 証明書発行元へ公開鍵の配布

GlobalSign 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整合性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 CPS 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 CA は依拠当事者への公開鍵の配布は、鍵のすり替えを防ぐ為、相応の方法で請け負うことを保証するものとする。これには、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商業ブラウザー及びプラットフォームオペレーターと作業することを含む可能性がある。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、または GlobalSign CA 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 CA 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、認証局ルート鍵データの選択に対して最善を尽くし、認証局及びエンドエンティティ証明書を発行、利用者に配布するものとする。また GlobalSign CA の直接管理下にない、いずれのサブ的認証局の発行の場合も同様に実行することが合意の下義務付けられているものとする。

下記の鍵サイズ及びハッシュ　アルゴリズムは、認証局/ブラウザフォーラムの定める基本条件及び検証拡張処理に従い、ルート証明書及びエンドエンティティ証明書、及び証明書失効リスト/オンライン証明書状態プロトコルの状態レスポンダーに使用可能です。

- 2048 ビット RSA 鍵　セキュア　ハッシュ　アルゴリズム 1 にて (SHA-1)
- 2048 ビット RSA 鍵　セキュア　ハッシュ　アルゴリズム 2 にて(SHA-256)
- 256 ビット ECDSA 鍵　セキュア　ハッシュ　アルゴリズム 2 にて(SHA-256)
- 384 ビット ECDSA 鍵 セキュア　ハッシュ　アルゴリズム 2 にて(SHA-384)

可能であれば、証明書のチェーン全体及びいずれの証明書状態のレスポンスも同じレベルのセキュリティ及び暗号技術を使用するものとする。相互認証証明書による例外は認められる。

暗号の強度が適切でない証明書は、信頼する対象、利用者及び発行局を守るために、適切な期間中に交換されるものとする。

6.1.6 公開鍵パラメーター生成及び品質検査

GlobalSign CA は FIPS186 の定めに従い鍵を生成、また利用者から提示される鍵の適切性を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。

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 CA 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)

6.2 秘密鍵保護及び暗号化モジュール技術管理

6.2.1 暗号化モジュール規定及び管理

GlobalSign CA は証明書、証明書失効リストの署名またはオンライン証明書状態プロトコル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 CA 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ー)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 CA は、信頼された役割において職務を担う複数の人員の管理の下、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 CA 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 CA は災害時事業継続計画の目的の為、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 CA は秘密鍵のアーカイブを行なわない。

6.2.6 暗号モジュール間の秘密鍵移行

GlobalSign CA 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、及び保存されなければならない。秘密鍵がハードウェアセキュリティモジュールの外(保存もしくは移行のため)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。

6.2.7 暗号モジュールにおける秘密鍵の保存

GlobalSign CA 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 CA 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、利用者規定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 CA 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が立会いのない状態に置かれておらず、また不正アクセスに対して利用可能な状態に置かれていないことを保証するものとする。

GlobalSign CA の暗号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 からの証明書失効リスト/オンライン証明書状態プロトコル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 CA 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または失効した際に破棄されなければならない。秘密鍵の破棄は、秘密鍵の如何なる部分も推定されないよう、認証局による関連する全認証局の秘密アクティブ化データの破棄が必要となる。

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 CA 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 CA 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	証明期間
ルート証明書 [3]	20 年	30 年
TPM ルート証明書	30 年	40 年
発行局証明書	11 年	15 年
PersonalSign 証明書	規定無し	5 年
Code Signing 証明書	規定無し	3 年
EV Code Signing 証明書	規定無し	39 ヶ月
DV SSL 証明書	規定無し	5 年
AlphaSSL 証明書	規定無し	5 年
OV SSL 証明書	規定無し	5 年
EV SSL 証明書	規定無し	27 ヶ月
Time Stamping 証明書	11 年	11 年
AATL CA 証明書	規定無し	5 年
PDF Signing 証明書	規定無し	5 年
TrustedRoot	規定無し	10 年
NAESB 証明書	2 年	2 年

GlobalSign CA 証明書は、最長有効期間に関し"CABForum Minimum Guidelines for Publically Trusted SSL Certificates"に準拠しなければならず、従って証明書の有効可能な期間が縮小されることとなる。

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 CA の秘密鍵をアクティブ化する為に使用される、GlobalSign CA 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整合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

発行局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 CA 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。

[3] 2003 年以前に RSA を使用して生成された 2048 ビット鍵は、ハードウェア、ルート格納及び OS 内の鍵サイズ規制により、25 年間使用可能となる。

6.4.3 その他のアクティブ化データの要素

GlobalSign 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 CA 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、または 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 CA 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
- 任意のアクセスコントロールを提供
- セキュリティ監査能力を提供(整合性が保護されていること)
- 対象物の再利用を禁止する
- 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
- 本人確認及び認証には、信頼済みパスを要求する
- 処理に対してドメインの分離を提供する
- OS に対して自己防御を提供する

GlobalSign CA の PKI の設備がコンピュータ セキュリティ保証要求の準拠性について評価済みのプラットフォームにホストされている場合、そのシステム(ハードウェア、ソフトウェア、OS)は可能な限り、高度に設定された中で運用されるものとする。少なくとも、そのようなプラットフォームは査定評価を受けたコンピュータ OS と同じバージョンをを使用するものとする。コンピュータ システムは必要最小限のアカウント、ネットワークサービス及びリモート ログインのない状態に設定される。

6.5.2 コンピュータ セキュリティの評価

GlobalSign CA のすべての PKI を構成するソフトウェアは、適切な対象者による保護プロファイル条件を遵守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 CA 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なら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う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)
- 開発された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たものであること。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
- すべてのハードウェアは、購入場所から運用場所まで一連の責任が継続した追跡性を提供できる、管理された方法を介して配送また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、ネットワーク接続また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 CA 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為にスキャンされる。
- 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または開発され、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 CA 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 CA の管理・経営陣により管理されるものとする。GlobalSign CA のソフトウェアまたは設定に対する不正な変更を検知する為の仕組みを持つ。

正式な設定管理技法が GlobalSign CA 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 CA 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 CA 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保持するため、保守スキームを継続的に維持管理する。

6.7 ネットワーク セキュリティ コントロール

GlobalSign CA 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為、適切なセキュリティ対応が導入されるものとする。このような対応策には、ガードの使用、ファイヤー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すべて拒否する。

6.8 タイムスタンプ

GlobalSign CA の全コンポーネント定期的に信頼できるタイムサービスとの同期を行う。GlobalSign CA は 1 つの GPS ソース、1 つの DCF77 ソース及び 3 つの非認証の NTP ソースのクロックを、正確な時刻を確立するために使用する。

- CA 証明書の初期検証時刻
- CA 証明書の失効
- 証明書失効リストの掲示
- 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または手動的手続きが適用される。時計の調整は監査対象イベントとなる。

6.8.1 PDF 署名タイムスタンピングサービス

CDS 利用者のデジタル ID によって作成されるすべてのデジタル署名には、RFC3161 に準拠し、Adobe ルート証明書にチェーンされたタイムスタンプ局(TSA)によって発行されたタイムスタンプを含むことができる。当該 TSA の証明書は FIPS140-2 レベル 2 かそれ以上の HSM に格納されるべきである。タイムスタンピングサービスは GlobalSign CA または GlobalSign CA が業務委託した代行業者によって提供される。タイムスタンピングサービスが代行業者によって管理されている場合、GlobalSign CA は当該 CPS に従ってタイムスタンピング証明書を発行する。

6.8.2 CodeSigning 及び EV CodeSigning タイムスタンピングサービス

CodeSigning またはに EV CodeSigning よって作成されるすべてのデジタル署名には、RFC3161 に準拠し、GlobalSign ルート CA にチェーンされたタイムスタンプ局(TSA)によって発行されたタイムスタンプを含むことができる。当該 TSA の証明書は FIPS140-2 レベル 2 かそれ以上の HSM に格納されるべきである。タイムスタンピングサービスは GlobalSign CA または GlobalSign CA が業務委託した代行業者によって提供される。タイムスタンピングサービスが代行業者によって管理されている場合、GlobalSign CA は当該 CPS に従ってタイムスタンピング証明書を発行する。

7.0 証明書、証明書失効リスト、及びオンライン証明書状態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 CA 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 CA 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 CA 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}
- 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 }
- ECDSAWithSH256 {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)

7.1.4 名称形式

GlobalSign CA は、RFC5280 に従う名称形式にてデジタル証明書を発行するものとする。各発行認証局のドメイン内において、GlobalSign CA は 20 桁のエントロピーを示すユニークでの連続性のない証明書シリアル番号を含まなければならない。

7.1.5 名前の制限

GlobalSign CA は必要なに応じて名前の制限(NameConstraints)を適用してデジタル証明書を発行し、また TrustedRoot プログラムの一部として必要な場合にはそれをクリティカルとして設定する。

7.1.6 証明書ポリシー識別子

(規定なし)

7.1.7 ポリシー制約拡張の使用

(規定なし)

7.1.8 ポリシー修飾子の構成と意味

GlobalSign CA 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

(規定なし)

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 CA は RFC5280 に従い、バージョン 2 の証明書失効リストを発行するものとする。失効リストは以下のフィールドを含む。

- 発行者 GlobalSign XXX 等 (製品による)
- 有効開始日 日付及び時間
- 次回更新日 日付及び時間
- 署名アルゴリズム sha1RSA, sha256RSA 等 (製品による)
- 署名ハッシュアルゴリズム sha1, sha256 等 (製品による)
- シリアル番号 失効された証明書のシリアル番号
- 失効日 失効日

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ー拡張子

証明書失効リストは、以下の拡張(エクステンション)を含む。

- CRL 番号 連続する番号
- 発行者鍵識別子 (AuthorityKeyIdentifier) リクエストの検証や証明書のチェーニングのための発行 CA 鍵の識別子

7.3 OCSP プロファイル

GlobalSign CA は、RFC2560 または 5019 に従い、AIA 拡張中の OCSP レスポンダ URI を通してオンライン証明書状態プロトコル(OCSP)レスポンダを提供する。

7.3.1 バージョン番号

GlobalSign CA は以下のフィールドを含むバージョン 1 の OCSP レスポンスを発行する。

- レスポンダ ID　　レスポンダの公開鍵の SHA-1 ハッシュ
- 生成時間　　OCSP レスポンスが署名された時間
- 証明書ステータス　　問い合わせを受けた証明書のステータス(有効/失効済み/不明)
- ThisUpdate/NextUpdate　　推奨されているレスポンス検証の間隔(CRL と同じ)
- 署名アルゴリズム　　SHA-1 RSA、SHA256 RSA 等(商材により異なる)
- 署名　　レスポンダにより生成された署名
- 証明書　　OCSP レスポンダの証明書

7.3.2 オンライン証明書状態プロトコル 拡張子

OCSP リクエストにナンスフィールドが含まれている場合、対応するレスポンスも同じナンスを返送する。

8.0 準拠性監査及びその他の評価

本 CPS に記載される手続きは、GlobalSign CA 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、現状で適応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 TrustedRoot CA は、下記の規定について準拠性監査を受ける。

- AICPA/CICA WebTrust for Certification Authorities Version 1.0
- AICPA/CICA WebTrust for Extended Validation

8.1 評価の頻度及び状況

GlobalSign CA は、独立監査人を介して、1 年に 1 度、上述の AICPA の標準に準拠性について評価するものとする。

8.2 評価者の身元及び能力

GlobalSign CA の監査は、下記の要件と能力を有する「適合監査人」である Ernst & Young によって行われる。

- 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
- 公開鍵基盤技術、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、更に第三者認証の機能の審査において、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、また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、公的規定または職種倫理規定により認定されている者
- 業務上の責任及び過失、不備に対する、少なくとも 100 万米ドルを填補限度額とする保険を保持する

8.3 評価者と被評価者の関係

GlobalSign CA は、GlobalSign CA 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する。

8.4 評価対象項目

監査は、8.0 項に記載される、評価のための監査スキームの要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が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 CA 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

GlobalSign CA 及び技術的制約を受けない相互認証された発行認証局は共に、監査法人によって準拠性についての問題を提示された場合には、不備を排除するための適切な是正計画を作成しなければならない。CP 及び CPS によって定められたポリシーや手続きに対して直接影響を与える是正計画については、ポリシー委員会に上程するものとする。

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、ポリシー委員会に報告される。

9.0 その他ビジネス及び法的事項

9.1 費用

9.1.1 証明書発行及び更新費用

GlobalSign CA 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 CA は、再発行(当該証明書の有効期間内における Re-key)に対しては費用を請求しない。費用及びそれに関連する約款は、申し込みの過程の WEB インターフェース及び GlobalSign の複数の言語の WEB サイト上にある営業・マーケティングマテリアルを通じて、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 CA 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 失効またはステータス情報へのアクセス費用

GlobalSign CA は、多数の依拠当事者を持ちながら、OCSP ステープリングやその他の GlobalSign の証明書ステータス基盤の負荷を軽減するための技術を採用しない利用者に対して、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 CA 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、請求できるものとする。

9.1.5 返金ポリシー

GlobalSign CA は利用者に対し、GlobalSign CA の Web サイト https://www.globalsign.com/repository に掲載されている返金ポリシーを提示する。返金ポリシーの行使を選択する利用者は、すべての発行済み証明書を失効しなければならない。

9.2 財務上の責任

9.2.1 保険の適用範囲

GlobalSign nv-sa は、少なくとも 200 万米ドルを填補限度額とするの企業総合賠償責任保険、および少なくとも 500 万米を填補限度額とする業務過誤/専門職業人賠償責任保険に加入する。GlobalSign の保険ポリシーは、以下の補償範囲を含む。
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
現行版の最良の保険ガイド(または格付け対象企業を会員とする企業団体)において被保険者の評価が A-よりも上の評価を受けた会社を通じて提供されるものとする。

9.2.2 その他資産

(規定なし)

9.2.3 エンドエンティティに対する保険もしくは保証

GlobalSign CA は利用者に対して GlobalSign の Web サイト https://www.globalsign.com/repository 上のワランティーポリシーを提示する。

9.3 業務情報の機密性

9.3.1 機密情報の範囲

以下の項目は機密情報として定義され、審査担当オペレータと管理者を含む GlobalSign CA スタッフによる相当な配慮と注意の対象となる。

- 9.4 項に記載される個人情報
- CA 及び RA システムの監査ログ
- 6.4 項で記載される、CA の秘密鍵を活性化するための活性化データ
- 災害復旧計画と事業継続計画を含む GlobalSign CA の内部的なビジネスプロセス文書
- 8.0 項で記載される独立した監査人からの監査報告

9.3.2 機密情報の範囲外に属する情報

本 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 CA は、従業員、代理人、及び契約社員に対する研修と強制によって、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 CA は、GlobalSign CA の Web サイト https://www.globalsign.com/repository 上で公開されるプライバシーポリシーに従い、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 CA は申請者から受領する、通常証明書に記載されないすべての情報を個人情報として取り扱う。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 CA は、すべての RA 及び審査スタッフと、個人情報に対してアクセスが必要なすべての従業員に対して、履行するべき注意義務に関して定期的にトレーニングを行う。

9.4.3 個人情報とみなされない情報

証明書の状況情報及びすべ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 個人情報保護の責任

GlobalSign CA は個人情報保護規定に従って、紙媒体また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存する責任を有する。如何なる個人情報のバックアップも、適切なバックアップメディアに移行される際は、暗号化されなければならない。プライバシーポリシーは、GlobalSign の Web サイト https://www.globalsign.com/repository 上で公開される

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 CA は、GlobalSign CA が提供する製品また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を含め、適切な利用者約款に関連条項として盛り込む。

9.4.6 法的または管理処理に従う開示

GlobalSign CA は、法令により要求があった場合には、申請者また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

(規定なし)

9.5 知的財産権

GlobalSign CA 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正当に保持するところの利用者の所有権に属する。GlobalSign CA 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。

GlobalSign 及び GlobalSign のロゴは、GMO グローバルサイン(株)の登録商標である。

9.6 表明保証

9.6.1 認証局の表明保証

GlobalSign CA は、本 CPS 及び該当する利用契約を使用して、利用者及び依拠当事者に発行済み証明書の使用に関する法的条件を告知する。GlobalSign CA、RA、利用者を含むすべての関係者は、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、万一秘密鍵が危殆化されたと疑われる場合は、直ちに適切な RA へ通知するものとする。

GlobalSign CA は以下の証明書受益者に対し：

- 利用契約の当事者としての利用者
- 契約上、提供するアプリケーションに Root CA を含めることになっているすべてのアプリケーションソフトウェア提供者
- 有効な証明書に合理的に依拠する依拠当事者

証明書が有効である間、GlobalSign CA が証明書の発行と管理において、以下の内容を含む、証明書ポリシーと CPS に準拠していることを表明及び保証する。

- **ドメイン名あるいは IP アドレスの使用権：** 証明書発行時点において、GlobalSign CA が
  (i) 証明書のサブジェクトフィールドある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 アドレスの使用権あるいは管理権限を申請者が有している(あるいはドメイン名のみの場合、使用権ある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 CA の証明書ポリシー(GlobalSign CP)や認証業務規程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 CA 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 や認証業務規程に明確に記述されていること(3.2 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 CA が
  (i) 証明書に格納されるすべての情報(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 や認証業務規程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 CA 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 や認証業務規程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 CA 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 や認証業務規程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 CA と利用者が関連会社でない場合、申請者と CA とは、これらの条件を満たす適法かつ強制力のある使用契約にて位置づけられていること。あるいは、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 CA はすべ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 CA は、CABForum Baseline Requirements 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(4.9.1 項を参照のこと)

GlobalSign CA は NAESBE 証明書に関し、以下を表明保証する。

- 北米エネルギー規格委員会 WEQ-PKI 規定に基づき、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、北米エネルギー規格委員会 WEQ-PKI 規定の全要件に従っている
- 既存の証明書または RA により合理的に知られる、または RA が証明書において検証した事項において、誤記や誤りがないこと
- 記載目的で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
- 証明書が北米エネルギー規格委員会 WEQ-PKI 規定の定める要件を満たしていること

9.6.2 登録局(RA)の表明保証

RA は以下を保証する。

- 発行手続きが本 CPS 及び関連証明書ポリシーに準拠していること

- GlobalSign CA に対して提供する情報が、誤解を招く、あるいは虚偽のものを含まない
- RA によって提供されるすべての翻訳された資料が正確であること

9.6.3 利用者の表明保証

本 CPS に特別な記述が無い限り、利用者は下記の項目に責任を有する。

- デジタル証明書の利用に対し、知識を有し、また必要があれば研修の機会を希望すること
- 自身の秘密鍵・公開鍵のペアを信頼するシステムを使用して安全に生成すること
- GlobalSign CA との通信中の情報が正確で誤りがないこと
- GlobalSign CA に提示された公開鍵が、使用されている秘密鍵に正確に対応すること。
- GlobalSign CA のレポジトリにて提供される利用契約、GlobalSign CP 及び関連するポリシーに定められるすべての規定及び条件を受諾すること
- 発行済み証明書を使用した不正行為に携わらない
- 本 CPS に従い、証明書を合法的で承認された目的に限定して使用すること
- 提出された情報における如何なる変更についても、GlobalSign CA または RA へ通知すること
- 記載される情報のいずれかが無効となった場合は、証明書の使用を中止すること
- 証明書が無効となった際は、使用を中止すること
- 証明書が無効となった場合には、インストールされたアプリケーション及び・またはデバイスから削除すること
- 状況に応じて、妥当な場合に証明書を使用すること
- 秘密鍵の危殆化、損失、漏洩、改ざん、または不正使用を防ぐこと
- 利用者のパートナーや代理人による作為または不作為の秘密鍵の生成、保持、預託または破壊
- 法律またはいかなる団体の権限を侵害する内容を含む資料の提出を行なわないこと
- 証明書の完全性に影響を及ぼす事象が発生した場合には、証明書の失効を請求すること
- 利用者が秘密鍵が危殆化した可能性を察知した場合は、直ちに適切な RA へ通知すること
- 本 CPS、特に登録に関する項目に従い正確かつ完全な情報を GlobalSign CA に提出すること
- 鍵ペアを電子署名あるいは本 CPS、または TrustedRoot 認証局チェーニング合意書によって利用者に通達されたその他すべての制約事項に則した用途にのみ使用すること
- 秘密鍵への不正使用を防ぐ為に、完全な注意取り扱いを実行すること
- 本 CPS に示される鍵の長さ及びアルゴリズムを使用すること
- 以下に示す有効性が失われる事項が発生した際は、いかなる理由であっても遅滞なく GlobalSign CA に通知を行なうものとする
  - 利用者の秘密鍵が遺失、盗難、もしくは危殆化した可能性
  - 活性化データ(例：PIN 番号またはパスフレーズ)の危殆化により、利用者の秘密鍵に対する管理能力が失われた場合
  - 不正確な内容、または証明書の内容に対する変更が利用者に通知された場合

利用者は証明書を申請する際に当事者が下す判断に最終的な責任を持つ。申請者及び GlobalSign CA は、信頼できるデバイスの使用または組織関連の選択を指定しなければならない。

9.6.3.1 北米エネルギー規定委員会(NAESB)利用者

ビジネスプラクティススタンダード WEQ-012 v3.0 に加入するエンドエンティティは NAESB EIR に登録し、卸電気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 ビジネスプラクティススタンダード WEQ-012 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、卸電気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およびそのユーザコミュニティは、ビジネスプラクティススタンダードに定められたエンドエンティティの義務をすべて果たす必要がある。
各利用者組織は WEQ-012 に定められている以下の義務について理解していることを、GlobalSign CA を通じて示さなければならない。

各エンドエンティティの組織は以下の WEQ-012 の項目を精査し、同意していることを証明しなければならない。

- エンドエンティティは、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、または意図せずに)データが改ざんされていないという保証
  - 否認防止：取引や電子メールの送信を送信者が否認できなくなること。

- エンドエンティティは卸電気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。
- エンドエンティティが利用する認証局の認証業務運用規程を業界基準と比較し、評価していること。

エンドエンティティ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。

また、エンドエンティティ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
- NAESB EIRからGlobalSignのグローバルサインが認定認証局として選んだエンティティを識別すること
- グローバルサイン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、当認証業務運用規程に規定されている通り、すべての同意書および契約書に準拠すること
- 当認証業務運用規程に規定されているすべてエンドエンティティの義務に準拠すること(証明書申請手続き、申請者識別証明/審査、およ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すべ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。
    - o 証明書秘密鍵セキュリティおよび運用手続き
    - o 証明書失効ポリシー
- 利用者の本人識別情報を識別し(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 依拠当事者の表明保証

発行局の証明書に関連する対象は下記の項目を約束する。

- デジタル証明書を使用する技術的能力を有している
- 発行局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発行局から発行された、証明書ステータス情報(例:証明書失効リストまたはオンライン証明書状態プロトコル)を使用して発行局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、発行局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、発行局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または失効を検証する
- 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すべ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あるいは規約と同様、発行局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

依拠当事者の責任は、以下の他に、これらのビジネスプラクティススタンダードを利用する各 NAESB の要件に定められている。

- 証明書が認定認証局であるグローバルサインにより発行されていること
- 認定認証局である NAESB 用グローバルサイン発行局の証明書の有効性および信頼チェーンのすべ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

9.6.4.2 その他関係者の告知保証

(規定なし)

9.7 保証の免責事項

GlobalSign CA は以下については保証しない。

- 証明書に含まれる、検証不能な情報の正確性。但し、本 CPS 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、テスト配布、またはデモ用の証明書に含まれる如何なる情報の正確性、正当性、完全性または一致性。

9.8 有限責任

いかなる場合においても、詐欺または故意の違法行為を除き、GlobalSign CA は、いかなる間接的、偶発的または結果的損害、利益の損失、データの損失またはその他の本 CPS によって提示または準拠する証明書あるいは電子署名またはその他のあらゆるトランザクションまたはサービスの利用、配布、許諾、履行または不履行の結果として、あるいはそれに派生して生じる間接的、偶発的または結果的損害に対して、一切責任を負わない。 ただし、証明書の発行時点において検証済みの情報に依拠した場合で、GlobalSign CA の Web サイトの正当なリーガルレポジトリ上の保証に関する通達文書に定められた金額を上限とするものを除く。
GlobalSign CA はこの検証済み情報の誤りが、申請者詐欺または故意の違法行為によるものである場合には責任を負わない。
ユーザーが本 CPS に記載されている義務を尊重していない場合、GlobalSign CA は責任を負わない。

9.9 補償

9.9.1 GlobalSign CA による補償

GlobalSign CA は、アプリケーションソフトベンダーに対し、当 CA 発行の Extended-SSL 証明書、あるいは Code Signing に関連して被ったところのいかなるクレーム、損害、あるいは損失に対し、その訴因、法的根拠に拘わらず、これを補償せねばならない。
但し、これらが(1)有効かつ信頼性のあるＥＶ証明書を、(誤って)無効あるいは信頼性欠如と表示してあった場合、また逆に(2)(ｉ)期限終了の証明書、(ⅱ)失効された証明書、などについて失効情報がオンラインで確認可能な状況でありながら(誤って)これを信頼性ありと表示したような場合を除く。

9.9.2 利用者による補償

利用者は、法律の許す範囲で、GlobalSign CA、GlobalSign CA のパートナー、及びトラステッドルートの企業、またそれらの役員、幹部、従業員、代理店、そして請負業者らに対して、以下の事由に起因するあらゆる損失、損害、あるいは出費、またこれらに関連する弁護士費用を補償するものとする。

(i) 利用者による虚偽、不作為、それらが意図的であれそうでないものであれ。
(ii) 利用者の利用契約への違反、また本 CPS あるいは適用法への違反。
(iii) 利用者の責に帰するべき、証明書あるいは秘密鍵のセキュリティ侵害、あるいは許諾された範囲外の使用。
(iv) 利用者の、証明書あるいは秘密鍵の誤使用。

9.9.3 依拠当事者(1.3.4 参照)による補償

依拠当事者は、法律の許す範囲で、GlobalSign CA、GlobalSign CA のパートナー、及び相互認証の企業、またそれらの役員、幹部、従業員、代理店、そして請負業者らに対して、以下の事由に起因するあらゆる損失、損害、あるいは出費、またこれらに関連する弁護士費用を補償するものとする。

(i) 依拠当時者による依拠当事者用契約書への違反、エンドユーザ向けライセンス契約、また本 CPS あるいは適用法への違反。
(ii) 依拠当時者による、証明書への不合理な依拠。
(iii) 依拠当時者による、使用前の証明書ステータスの確認ミス。

9.10 期間及び終了

9.10.1 期間

本 CPS は、GlobalSign CA によりそのウェブサイトまた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

通知された変更はバージョン番号の表示により、明確化される。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 終了及び残存物

GlobalSign CA は適切なレポジトリを介して、本 CPS の終了による条件及び影響につい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 CA は、本 CPS に関してデジタル署名されたメッセージまたは紙媒体を用いた通知を受け入れる。GlobalSign CA 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すこととする。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、書留郵便受領通知を必須として、差出人宛てに書面通知するものとする。GlobalSign CA への個別の連絡は、legal@globalsign.com 宛、または本 CPS の 1.5.2 項に指定される GlobalSign CA 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 CPS 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こと。

9.12.2 通知方法及び期間

GlobalSign CA は、本 CPS に関する主要なまたは重要な変更が為された際には、改定版の CPS 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

(規定なし)

9.13 紛争解決に関する規定

裁決またはその他の紛争解決策(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助言などによる方法を例外なく含む)に進む前に、当事者はその紛争解決策を模索する為、紛争について GlobalSign CA 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 CA は、GlobalSign CA 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 CA 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。法律顧問また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 CA 上層経営陣に対し解決方法を提案する。次いで GlobalSign CA 上層経営陣は、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、GlobalSign 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、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、ベルギー国ルーヴェンとなり、必要となる費用は調停委員が決定するものとする。

すべて技術に関連する紛争、及び GlobalSign CP に関連する紛争に関しては、両当事者は下記の住所に所在する、「スティッチング ゲスチルノプロッシング アートマティスセリング」(Stichting Geschillenoplossing Automatisering)のベルギー支店を仲裁機関(補足：機関仲裁の場合をいう)とすることに承諾する。

J. Scheepmansstraat 5,
3050 Oud-Heverlee, Belgium.
Tel.: +32-47-733 82 96, Fax: + 32-16-32 54 38

9.14 準拠法

本 CPS 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 CPS の解釈の一律性を確実にするためのものである。また、GlobalSign CA が、プロバイダー、供給業者、受益者またはその他の役割を担う

GlobalSign CA 製品及びサービスに関し、本 CPS が適用され、または暗示的・明示的に引用されるところの GlobalSign CA の業務または契約関係のすべてに対して、ベルギー国法は、適用される。

GlobalSign CA 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全面的に服するものとする。

9.15 適用法の遵守

GlobalSign CA は、適用法としてベルギー国法を遵守する。特定の GlobalSign CA 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、何らかの公的認可または民間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 強要行為への対応

GlobalSign CA はベルギー管轄権に従い、またベルギーの規制の枠組に従う。GlobalSign の CA 基盤はベルギー及びフランスに拠点を置き、また RA 基盤はベルギー及び日本に拠点を置いている。GlobalSign CA の営業部署及び・または戦略的パートナーは、GlobalSign CA 基盤の如何なる部分にも、アクセスすることはできない。
また、GlobalSign CA は、GlobalSign CP 及び CPS に違反する証明書の発行を強要するような第三者からの行為に対しては、あらゆる合理的な法的防御措置を取るものとする。

9.16.2 存続事項

本 CPS の法的条件の項目に関する義務事項、あるいは制限事項は本 CPS の終了後も存続する。

9.16.3 包括的合意

GlobalSign CA は、すべての証明書発行に携わる RA に対し、本 CPS 及びすべ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。

9.16.4 譲渡

本 CPS に基づき業務を行なう事業者は、自身が持つ権利または義務を、GlobalSign CA 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。

9.16.5 分離条項

本 CPS は、その責任の制限の項目を含む何れかの規定が無効であるか、あるいは法的強制力が失効となった場合にも、本 CPS の他の条項は当事者の本来の意図に沿った方法で解釈されるものとする。

9.16.6 施行(弁護士の費用及び権利の放棄)

GlobalSign CA 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 CA が本 CPS の何れかの規定の行使を怠った場合でも、それはその後の同規程の行使、またはその他の規定の行使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 CA の署名がある場合に有効となる。

9.17 その他の規定

(規定なし)