

ジオトラスト

認証業務運用規程

(Certification Practices Statement)

Version 1.1.4

Effective Date:2010年9月22日



GeoTrust, Inc
350 Ellis Street
Mountain View, CA 94043 USA
+1 650.527.8000
www.geotrust.com

ジオトラスト認証業務運用規程 (Certification Practices Statement)

© 2010 Symantec Corporation. All rights reserved.
Printed in the United States of America.

改訂日：2010年9月

Trademark Notices

GeoTrust、及び GeoTrust ロゴは、GeoTrust Inc.の登録商標である。True Credentials、QuickSSL、True Business ID、及び Power ServerID は、GeoTrust の商標ならびにサービスマークである。本文書中のその他の商標及びサービス・マークは、それぞれの権利者に帰属する。GeoTrust Inc. はシマンテック・コーポレーションの完全子会社である。

本文書に関するすべての著作権は、ジオトラストが留保しており、さらに下記で許諾された場合を除き、ジオトラストの書面による事前の同意なく、電子的、機械的、複製、録音その他手段を問わず、本文書のいかなる部分も複製、検索可能なシステム内での保管、送信を行うことはできないものとする。

上記の規定にかかわらず、本文書は以下に定める条件を満たす場合に、非独占的かつ無料で複製し配布することができる。(i)冒頭の著作権に関する表示及びこの前書きの部分を、複製されたそれぞれの文書に目立つように表示すること、(ii)本文書がすべて正確に複製され、本文書がジオトラストに帰属する旨の記述を含むこと。

その他ジオトラスト認証業務運用の複製を許可する要望（コピーの要望も含む）はすべて、以下のシマンテック・コーポレーションに問い合わせなければならない。

Symantec Corporation
350 Ellis Street, Mountain View, CA 94043 USA
担当部署：Practices Development
電話：+1 650.527.8000
Fax：+1.650.527.8050
メール：practices@verisign.com.

目次

1. はじめに.....	1	4.2 証明書申請手続.....	9
1.1 概要.....	1	4.2.1 本人性確認と認証機能の実施.....	9
1.2 文書名と識別.....	1	4.2.2 証明書申請の承認もしくは拒絶.....	9
1.3 PKI 参加者.....	1	4.2.3 証明書申請の処理時間.....	10
1.3.1 認証機関.....	1	4.3 証明書発行.....	10
1.3.2 登録機関.....	1	4.3.1 証明書の発行過程における認証機関の行為.....	10
1.3.3 エンド・エンティティ.....	1	4.3.2 認証機関の利用者に対する証明書発行通知.....	10
1.3.4 依拠当事者.....	2	4.4 証明書の受領.....	10
1.3.5 他の参加者.....	2	4.4.1 証明書の受領となる行為.....	10
1.4 証明書の利用.....	2	4.4.2 認証機関による証明書の公開.....	10
1.4.1 適切な証明書の利用.....	2	4.4.3 他のエンティティに対する認証機関の証明書発行通知.....	10
1.4.2 禁止される証明書の用途.....	3	4.5 キー・ペアと証明書の用途.....	11
1.5 ポリシー管理.....	3	4.5.1 利用者の秘密鍵及び使用.....	11
1.5.1 本文書の管理部署.....	3	4.5.2 依拠当事者の公開鍵及び証明書の使用.....	11
1.5.2 連絡先.....	3	4.6 証明書のリニューアル.....	11
1.5.3 CPS 承認手続き.....	3	4.6.1 証明書がリニューアルされる場合.....	11
1.6 定義.....	4	4.6.2 リニューアルを申請することができる者.....	12
2. 公表及びリポジトリに関する責任.....	4	4.6.3 証明書のリニューアル申請の手続.....	12
2.1 リポジトリ.....	4	4.6.4 利用者に対する新しい証明書発行通知.....	12
2.2 証明書情報の公表.....	4	4.6.5 リニューアルされた証明書の受領確認の行為.....	12
2.3 公表の頻度.....	4	4.6.6 認証機関によるリニューアルされた証明書の公開.....	12
2.4 リポジトリへのアクセス制限.....	4	4.6.7 他のエンティティに対する認証機関の証明書発行通知.....	12
3. 確認と認証.....	4	4.7 証明書のリキー.....	12
3.1 名称.....	4	4.7.1 リキーされる場合.....	12
3.1.1 識別名の種類.....	4	4.7.2 新しい公開鍵の証明書を申請することができる者.....	12
3.1.2 意味のある名称であることの必要性.....	5	4.7.3 証明書のリキー申請の手続.....	13
3.1.3 匿名またはペンネームの使用.....	5	4.7.4 利用者に対する新しい証明書発行通知.....	13
3.1.4 識別名を解釈するための指針.....	5	4.7.5 リキーされた証明書の受領確認の行為.....	13
3.1.5 唯一の名称.....	5	4.7.6 認証機関によるリキーされた証明書の公開.....	13
3.1.6 商標の認識、認証及び役割.....	5	4.7.7 他のエンティティに対する認証機関の証明書発行通知.....	13
3.2 初回の本人確認.....	6	4.8 証明書の変更.....	13
3.2.1 秘密鍵を所有していることの証明方法.....	6	4.8.1 証明書が変更される場合.....	13
3.2.2 組織の実在性確認.....	6	4.8.2 証明書の変更を申請することができる者.....	13
3.2.3 ドメイン・ネームの認証.....	6	4.8.3 証明書の変更申請の手続.....	13
3.2.4 個人の実在性確認.....	7	4.8.4 利用者に対する新しい証明書発行通知.....	13
3.2.5 確認を行わない申請情報.....	7	4.8.5 変更された証明書の受領確認の行為.....	13
3.2.6 権限の確認.....	7	4.8.6 認証機関による変更された証明書の公開.....	14
3.2.7 共同運営の条件.....	8	4.8.7 他のエンティティに対する認証機関の証明書発行通知.....	14
3.3 リキー申請の確認と認証.....	8	4.9 証明書の失効及び効力の停止.....	14
3.4 失効申請に関する確認と認証.....	8	4.9.1 失効が行われる場合.....	14
4. 証明書のライフサイクルの運用.....	9	4.9.2 証明書の失効を申請することができる者.....	14
4.1 証明書申請.....	9		
4.1.1 証明書申請を行うことができる者.....	9		
4.1.2 登録手続き及び責任.....	9		

4.9.3 失効申請要求の手続	15	5.4 監査記録の手続き	22
4.9.4 失効申請の猶予期間	15	5.4.1 記録されるイベントの種類	22
4.9.5 認証機関が失効申請を処理しなければならない期間	15	5.4.2 記録を処理する頻度	22
4.9.6 依頼当事者に要求される CRL の調査	15	5.4.3 監査記録を保持する期間	22
4.9.7 CRL の発行頻度	15	5.4.4 監査記録の保護	22
4.9.8 CRL の最大発行所要時間	15	5.4.5 監査記録のバックアップ手続	22
4.9.9 利用可能なオンラインによる失効/ステータス調査	15	5.4.6 監査ログ集計システム (内部対外部)	22
4.9.10 オンラインによる失効調査要件	15	5.4.7 イベントを生ぜしめた Subject に対する通知	22
4.9.11 利用可能な失効の公表についての他の形式	16	5.4.8 脆弱性の評価	22
4.9.12 鍵の危殆化に関する特別な要件	16	5.4.9 保管記録収集システム (内部又は外部)	22
4.9.13 効力を停止する場合	16	5.4.10 保管記録情報の取得及び検証の手続	23
4.9.14 効力停止申請をすることができる者	16	5.5 記録の保管	23
4.9.15 効力停止申請の手続	16	5.5.1 保管される記録の種類	23
4.9.16 効力停止の制限	16	5.5.2 記録保管の期間	23
4.10 証明書ステータス・サービス	16	5.5.3 保管記録の保護	23
4.10.1 運用上の特徴	16	5.5.4 保管記録のバックアップ手続	23
4.10.2 サービスの利用可能性	16	5.5.5 記録のタイム・スタンプに関する要件	23
4.10.3 オプション機能	16	5.5.6 保管記録収集システム (内部又は外部)	23
4.11 利用の終了	16	5.5.7 保管記録情報の取得及び検証の手続	23
4.12 鍵の預託と復旧	17	5.6 鍵の切り替え	24
4.12.1 鍵の預託と復旧及び実施	17	5.7 危殆化及び災害からの復旧	25
4.12.2 セッションキーのカプセル化及び復旧のポリシー及び実施	17	5.7.1 事故及び危殆化の取扱手続	25
5. 設備、管理及び運用統制	17	5.7.2 コンピューターの資源、ソフトウェア、またはデータが破損した場合	25
5.1 物理的管理	17	5.7.3 エンティティの秘密鍵が危殆化した場合の手続	25
5.1.1 立地場所及び構造	17	5.7.4 災害後の事業継続能力	25
5.1.2 物理的アクセス	18	5.8 認証機関または登録機関の終了	25
5.1.3 電源及び空調	18	6 技術的セキュリティ・コントロール	26
5.1.4 水による被害	18	6.1 キー・ペア生成及びインストール	26
5.1.5 火災予防及び保護対策	18	6.1.1 キー・ペア生成	26
5.1.6 メディアの保管	18	6.1.2 秘密鍵の受渡	26
5.1.7 廃棄物処理	18	6.1.3 公開鍵の証明書発行者への受渡	26
5.1.8 オフサイト・バックアップ	18	6.1.4 認証機関公開鍵のユーザへの受渡	26
5.2 手続的管理	19	6.1.5 鍵のサイズ	27
5.2.1 信頼される役割	19	6.1.6 公開鍵のパラメータの生成	27
5.2.2 職務ごとに必要とされる人数	19	6.1.7 鍵用途目的 (X.509 バージョン 3 の Key Usage フィールドのとおり)	27
5.2.3 それぞれの任務に必要な身元の確認	19	6.2 秘密鍵の保護	27
5.2.4 職務の分離を必要とする役割	20	6.2.1 暗号モジュールの基準	27
5.3 人事的管理	20	6.2.2 複数人による秘密鍵 (m of n) の管理	27
5.3.1 経歴、資格、経験及び許可要件	20	6.2.3 秘密鍵の預託	28
5.3.2 経歴調査手続	20	6.2.4 秘密鍵のバックアップ	28
5.3.3 トレーニング要件	21	6.2.5 秘密鍵の保管	28
5.3.4 再トレーニングの頻度及び要件	21	6.2.6 秘密鍵の暗号化モジュールへの入出力	28
5.3.5 人事異動の頻度及び順序	21	6.2.7 秘密鍵の暗号モジュールへの格納	28
5.3.6 無権限の行為に対する制裁	21	6.2.8 秘密鍵の起動の方法	28
5.3.7 請負事業者の要件	21	6.2.9 秘密鍵の非活性化の方法	28
5.3.8 要員に提供される資料	22	6.2.10 秘密鍵の破壊の方法	28
		6.2.11 暗号モジュールの評価	29

6.3 キー・ペアの管理に関する他の点	29	9.2 財務的責任	35
6.3.1 公開鍵の保管	29	9.2.1 保険	35
6.3.2 証明書の運用期間及びキー・ペアの使用期間	29	9.2.2 その他の資産	35
6.4 起動データ	29	9.2.3 拡張された保証	35
6.4.1 起動データの生成とインストレーション	29	9.3 業務情報の機密保持	36
6.4.2 起動データの保護	29	9.3.1 機密情報の範囲	36
6.4.3 起動データに関する他の点	30	9.3.2 機密とみなされない情報	36
6.5 コンピュータ・セキュリティ管理	30	9.3.3 機密情報保護責任	36
6.5.1 特定のコンピュータ・セキュリティの技術的要件	30	9.4 個人情報の保護	36
6.5.2 コンピュータ・セキュリティの評価	30	9.4.1 プライバシーポリシー	36
6.6 ライフサイクル技術管理	30	9.4.2 個人情報	36
6.6.1 システム開発管理	30	9.4.3 個人情報とみなされない情報	36
6.6.2 セキュリティ管理	30	9.4.4 個人情報の保護責任	36
6.6.3 ライフサイクル・セキュリティ	30	9.4.5 個人情報を利用するための通知及び同意	37
6.7 ネットワーク・セキュリティ管理	30	9.4.6 司法または行政手続きによる開示	37
6.8 タイム・スタンプ	31	9.4.7 他の情報開示に関する状況	37
7. 証明書、CRL 及び OCSP のプロファイル	31	9.5 知的財産権	37
7.1 証明書のプロファイル	31	9.5.1 証明書及び失効情報に関する財産権	37
7.1.1 バージョン番号	31	9.5.2 本 CPS に関する知的財産権	37
7.1.3 アルゴリズムオブジェクト識別子	32	9.5.3 名称に含まれる権利	37
7.1.6 証明書ポリシー・オブジェクト識別子	32	9.5.4 鍵及び鍵のデータに関する財産権	38
7.1.7 ポリシー制約エクステンションの使用	32	9.6 表明と保証	38
7.1.8 ポリシー修飾子の構文及び意味	32	9.6.1 認証機関の表明と保証	38
7.1.9 クリティカルな Certificate Policies エクステンションに対する解釈方法	32	9.6.2 登録機関の表明と保証	38
7.2 CRL のプロファイル	33	9.6.3 利用者の表明と保証	38
7.2.1 バージョン番号	33	9.6.4 依拠当事者の表明と保証	39
7.2.2 CRL 及び証明書失効リスト・エントリ・エクステンション	33	9.6.5 その他の参加者の表明と保証	39
7.3 OCSP プロファイル	33	9.7 保証の否認	39
7.3.1 バージョン番号	33	9.8 責任の制限	39
7.3.2 OCSP エクステンション	33	9.9 補償	39
準拠性監査とその他の評価	33	9.9.1 利用者による補償	39
8.1 評価の頻度・状況	33	9.9.2 依拠当事者による補償	40
8.2 評価人の身元と資格	33	9.10 有効期間と終了	40
8.3 評価人と被評価者との関係	34	9.10.1 有効期間	40
8.4 評価対象項目	34	9.10.2 終了	40
8.5 欠陥の結果としてとられる処置	34	9.10.3 終了の効果と効力の残存	40
8.6 結果の伝達	34	9.11 参加者の個別の通知と連絡	40
9. 業務及び法律に関するその他の事項	34	9.12 改訂	40
9.1 料金	34	9.12.1 改訂手続き	40
9.1.1 証明書発行または更新の手数料	34	9.12.2 通知方法と期間	40
9.1.2 証明書のアクセス手数料	34	9.12.3 OID の変更が必要な場合	41
9.1.3 失効またはステータス情報のアクセス手数料	34	9.13 紛争の解決	41
9.1.4 他のサービスの手数料	35	9.13.1 ジオトラスト、アフィリエイト、カスタマ間の紛争	41
9.1.5 返金制度	35	9.13.2 利用者または依拠当事者との紛争	41
		9.14 準拠法	41
		9.15 法の遵守	41
		9.16 雑則	42
		9.16.1 完全合意条項	42

9.16.2 譲渡.....	42
9.16.3 分離可能性.....	42
9.16.4 強制執行（弁護士費用と権利放棄）.....	42
9.16.5 不可抗力.....	42
9.17 その他の条項.....	42
Appendix A. 略語・定義表.....	43

1. はじめに

本書は、ジオトラストの認証業務運用規程（Certification Practice Statement）（以下「本 CPS」という）である。本 CPS は、ジオトラスト認証機関が証明書の発行、管理、失効及び更新を含む一連のサービスを提供する際に採用する手続きを記載したものである。

1.1 概要

このジオトラストの認証業務運用規程（CPS）は、ジオトラストのデジタル証明書の発行及びライフサイクル管理において採用する原則ならびに手続きを示したものである。本 CPS 及び改訂版はすべて、本 CPS に基づいてジオトラスト証明書を参照することにより組み込まれる。

インターネット・サービス・プロバイダ、ホスティング会社、その他の企業（パートナー）は、利用者の代わりに証明書の発行に関連する一部の機能を実行できる（利用者情報の収集、証明書署名要求の作成及び転送、発行後の証明書のインストール及び使用など）。そのような場合、本 CPS に記載されているプロセス及び手続きは、できる限り実際の利用者と同じように、パートナーに適用される。

1.2 文書名と識別

本書は、ジオトラストの認証業務運用規程（Certification Practice Statement）である。

1.3 PKI 参加者

1.3.1 認証機関

認証機関（CA）とは、本 CPS に基づき証明書を発行し、証明書発行に関連するすべての機能を実行する信頼される第三者エンティティである。

1.3.2 登録機関

登録機関は、ジオトラスト認証機関の代わりに、エンドユーザ証明書の申請者の本人確認と認証を行い、エンドユーザ証明書の失効要求を行い、証明書のリニューアルまたはリキーの申請を承認するエンティティである。ジオトラストは、自らが発行する証明書の登録機関になることができる。

ジオトラストと契約を締結する第三者は、自らの登録機関となり、ジオトラスト認証機関が発行する証明書の認証を行うことができる。第三者登録機関は、ジオトラスト CPS 及びジオトラストと締結する契約に定めるすべての要件を遵守しなければならない。しかしながら、登録機関は、内部要件に基づき、より限定的な運用を行うことができる。

1.3.3 エンド・エンティティ

エンド・エンティティは、ジオトラスト認証機関により発行される証明書のすべてのエンドユーザ（エンティティを含む）を含む。エンド・エンティティは、証明書のエンドユーザ利用者となるエンティティである。エンドユーザ利用者としては、個人、組織、またはファイアウォール、

ルーター、信頼されるサーバもしくは組織内で通信を安全に行うためのその他の機器でインフラストラクチャを構成するものがありうる。

認証機関は、自己署名した証明書を発行する認証機関として、または上位の認証機関による証明書を発行される認証機関として、技術的にはジオトラスト証明書の利用者でもある。本 CPS における「エンド・エンティティ」及び「利用者」という場合は、エンドユーザ利用者にも適用される。

1.3.4 依拠当事者

依拠当事者はジオトラスト認証機関によって発行される証明書またはデジタル署名に依拠して行為する個人またはエンティティである。依拠当事者はジオトラスト証明書の利用者である場合もあるし、利用者でない場合もある。

1.3.5 他の参加者

規定しない。

1.4 証明書の利用

1.4.1 適切な証明書の利用

ジオトラスト証明書は、必要に応じて SSL エクステンション、コード・サイニング、クライアント認証エクステンションを含む X.509 証明書であり、ジオトラストの信頼されるルートとチェーンを形成している。

ジオトラスト **SSL 証明書**は、利用者のサーバを限定する認証を提供し、依拠当事者のブラウザと利用者のサーバ間の SSL 暗号化によるトランザクションを許可することで、安全な電子取引を容易にする。ジオトラストはワイルドカード証明書を発行できる。これは SSL エクステンションを含む X.509 証明書であり、特定レベルのドメインに対して確認が行われ、さらにその特定レベルのドメインが属する上層レベルのすべてのドメインに関して使用できる。また、ジオトラストのクライアント証明書として証明書を使用できるようにすることもできる。

ジオトラスト**発行元証明書**の使用目的は、(i) コード・サイニング・ポータルにアクセスする当事者としての発行元の身元確認、及び (ii) 適切なコード確認証明書による後続の再署名のためのローカルでのコード・サイニングに限定できる。

ジオトラスト**コード確認証明書**は、発行元からのコード確認の要望に応じて、ジオトラストが、関連付けられた秘密鍵を使用して、発行元証明書の秘密鍵により電子署名されたアプリケーション・コードを電子的に再署名できるようにする。

ジオトラスト **My Credential™** クライアント証明書は、発行された S/MIME エクステンションを含む X.509 証明書であり、利用者のクライアントを限定する認証を提供し、依拠当事者と利用者のクライアント間の安全な VPN アクセス及び S/MIME 通信を許可することで、安全な電子取引を容易にする。

True Credentials® 及び **True Credential Express** クライアント証明書は、S/MIME エクステンションを含む X.509 証明書であり、利用者のクライアントを限定する認証を提供し、依拠当事者と利用者のクライアント間の SSL クライアント認証、安全な VPN アクセス、及び S/MIME 通信

を許可することで、安全な電子取引を容易にし、さらに場合によっては、コード・サイニングや文書署名にも使用できる。

1.4.2 禁止される証明書 の用途

証明書は、適用される法律、特に輸出入に係る法律の認める範囲でのみ利用されなければならない。

ジオトラスト証明書は、危険な環境下における制御装置での利用または再販のため、あるいは、機能停止が直接に死亡、身体障害、または深刻な環境被害をもたらすようなフェイル・セーフ機能を必要とする核施設、航空・通信システム、航空管制、兵器管理システム等での利用のために設計されているものでも、意図されているものでも、また認められているものでもない。クライアント証明書は、クライアント・アプリケーションでの用途を意図しており、サーバまたは組織向け証明書として使用することはできない。

1.5 ポリシー管理

1.5.1 本文書の管理部署

本 CPS の管理部署は、シマンテック・コーポレーションである。

問い合わせ先：

Symantec Corporation

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527-8000 (voice)

+1 (650) 527-8050 (fax)

practices@verisign.com

1.5.2 連絡先

本 CPS についての質問の送り先：

メール：practices@verisign.com

住所：

Symantec Corporation Practices

350 Ellis Street

Mountain View, CA 94043

USA

1.5.3 CPS 承認手続き

本 CPS（及び本 CPS のすべての改訂版）はジオトラストによる承認を受けなければならない。ジオトラストは予告なしに、本 CPS をいつでも変更できる。本 CPS 及び改訂版はすべて、<http://www.geotrust.com/resources/repository/legal>に掲載されている。本 CPS の改訂版であることは、改訂版が純粋に事務的なものである場合以外は、新しいバージョン番号と日付により証明される。

1.6 定義

Appendix A 参照。

2. 2. 公表及びリポジトリに関する責任

2.1 リポジトリ

ジオトラストは、ジオトラスト証明書の利用者と依頼当事者の両者に提供される CRL を運用する。各 CRL は、発行する認証機関により署名される。失効手続きは、本 CPS の他の場所に記載されているとおりである。

2.2 証明書情報の公表

ジオトラストは、認証機関が存在する間はすべての証明書のコピーを保持するが、期限切れの CRL または新しいものにとって代わられた CRL は保管もしくは保持しない。

2.3 公表の頻度

本 CPS の改訂は、本 CPS セクション9.12に従い、公表される。利用規約及び依頼当事者規約の改訂は必要に応じ公表される。証明書は、発行後に公表される。証明書ステータス情報は本 CPS のために従い公表される。

2.4 リポジトリへのアクセス制限

ジオトラストのウェブ・サイトのリポジトリ部分に公表される情報は、公的にアクセス可能なものである。当該情報に対する閲覧のみのアクセスは制限されないものとする。

3. 確認と認証

3.1 名称

3.1.1 識別名の種類

証明書は、SubjectName フィールドに X.501 識別名を含み、以下の表に定めるものから構成される。

属性	値
Country (C) =	2文字の ISO 国コード、もしくは使用せず。
Organization (O) =	この属性は、次のように使用される。 <ul style="list-style-type: none">ウェブ・サーバ向け証明書及び組織と関連を有する個人向け証明書の 場合、利用者の組織名(ドメイン制御検証のみを実施し、組織検証を実施しないウェブ・ サーバ向け証明書の場合) ドメイン名、または「GeoTrust Verified Site」もしくは組織フィールド内の類似用語

属性	値
Organizational Unit (OU) =	<ul style="list-style-type: none"> 適用できる場合、組織が認識されていないことを表す用語 ジオトラスト証明書は、以下に定める一つ以上の OU 属性を含むことができる。 <ul style="list-style-type: none"> 組織向け証明書及び組織と関連を有する個人向け証明書の場合、利用者組織単位 証明書の種類を説明する記載 検証を実行したエンティティを説明する記載 必要な場合は「検証されたドメイン制御」 カスタマの住所
State or Province (S) =	使用されている場合は、利用者の都道府県を示す
Locality (L) =	使用されている場合は、利用者の市町村を示す
Common Name (CN) =	本属性には以下を含めることができる。 <ul style="list-style-type: none"> ウェブ・サーバ用証明書の場合、ドメイン名 コード/オブジェクト・サイニング証明書の場合、組織名 個人に発行される証明書の場合、個人名 IP アドレス (TrueBusiness ID)
E-Mail Address (E) =	使用されている場合は、証明書に関連付けられた電子メールアドレス

EV SSL 証明書の項目とプロファイルの要求項目については、本 CPS Appendix A3 に記載される。

3.1.2 意味のある名称であることの必要性

ドメイン名は意味のあるものまたは一意のものである必要はないが、InterNIC に掲載されたときに第 2 レベル・ドメイン名と一致しなければならない。

3.1.3 匿名またはペンネームの使用

True Credential 及び **True Credential Express** を除き、利用者は匿名（利用者の本名または組織名以外の名前）の利用は許可されない。

3.1.4 識別名を解釈するための指針

規定しない。

3.1.5 唯一の名称

規定しない。

3.1.6 商標の認識、認証及び役割

証明書申請者は、証明書申請において、他者の知的財産権を侵害するような名称を使用してはならない。ジオトラストは、証明書申請者が証明書申請に記載の名称の知的財産権を有しているかどうかの検証を行わない。また、ドメイン・ネーム、商号、商標、サービス・マークに関する紛争を仲裁、調停、その他の方法で解決するものではない。ジオトラストは、証明書申請者に何等の責任を負うことなく、上記の紛争を理由として証明書申請を拒絶する権利を有する。

3.2 初回の本人確認

3.2.1 秘密鍵を所有していることの証明方法

証明書申請者は証明書に含まれる公開鍵と対になる秘密鍵を正当に所有していることを PKCS#10、暗号的にこれと同等の方法またはジオトラストが承認したその他の方法のいずれかにより証明しなければならない。キー・ペアが認証機関により利用者の代理として生成される場合（予め生成された鍵をスマートカードに格納する場合など）には、上記の要件は適用されない。

3.2.2 組織の実在性確認

証明書に組織名が含まれる場合、ジオトラストもしくは登録機関は、合理的な手段を講じて、組織に代わって行われた証明書申請が正当なものであり、適切に承認されていることを立証する。ジオトラストは以下のことを確認する。(a) 組織名が、国、及び可能であれば登録場所あるいは現在ビジネスを営んでいる場所を問題なく特定できる別の地域の都道府県に関連して記載されている、(b) 地域、都道府県、あるいは国の機関で登録されていると合理的に予想される組織の場合、特定の状況においてジオトラストは登録文書のコピーを取得、表示、検証する。たとえば、ジオトラストができるのは、(a) 発行元の機関を通じて登録の正当性を検証する、(b) 評判が高い第三者のデータベースまたはその他のリソースを通じて登録の正当性を検証する、(c) 信頼できる第三者を通じて組織の正当性を検証する、(d) 通常登録されるタイプでも、条項 (b) に従って検証されることが可能なタイプでもない組織の場合は組織が存在することを確認する、ということである。

3.2.3 ドメイン・ネームの認証

ドメイン・ネームが組織名と共に証明書に含まれている場合、ジオトラストもしくは登録機関は、利用者が申請を行ったときのドメイン・ネームをその利用者が使用する権限を有していたことを確認する。たとえばジオトラストは、利用者が、関連するドメイン・ネーム登録機関からのドメイン・ネーム登録を保有している人物と同一またはエンティティであること、もしくはそのようなドメイン・ネームの使用を利用者が承認されていることを確認することで、この検証を実行できる。上記で説明したようなドメイン・ネーム検証が実行されるのは、**TrueBusiness ID**、**Enterprise SSL** 及び **Enterprise SSL Premium** 証明書に対してである。

True Business ID 証明書は、CommonName フィールドに IP アドレスを含めることができる。このような場合、ジオトラストは組織における IP アドレスの所有権を検証する。

ドメイン・ネームが証明書に含まれているが、そのドメイン・ネームを所有するエンティティが認証されていない場合、ジオトラストもしくは登録機関は、申請フォームが送信されたときに、ドメイン・ネームとそのオーナーの第三者データベースにアクセスすることで、利用者がそのようなドメイン・ネームを制御できることを確認する。これを行うにあたり、ジオトラストは、証明書申請の確認、及びドメイン・ネームで証明書を発行する許可を要求する電子メール・メッセージを、以下の電子メールアドレスのいずれかに送信する。(a) ドメイン・ネームを含む公式の InterNIC ドメイン・ネーム・レジストリにおいて、ドメイン・ネームの管理担当者または技術担当者として記載されている電子メールアドレス、(b) ドメイン・ネームで権限を受けた者の、最もよく利用される一般的な電子メールアドレスの限定リスト（「`admin@domain.com`」、「`hostmaster@domain.com`」など。domain.com はドメイン・ネームを表す）、(c) ジオトラストによって実行される検証の手動プロセスを使用し、*whois* データベースによって、登録ドメイ

ン・オーナーとして特定された電子メールアドレス。任意で、確認用電話番号は、*whois* に記載されているドメイン・オーナーの電話番号に置き換えることができる。

ジオトラストは、証明書発行を許可する確認の電子メール・メッセージを受信すると、以下のよう
に証明書を発行する。加えて、申請者に対する確認電話は、ドメイン制御証明書申請に対して
実行できる。

ドメイン・ネーム制御は、以下の表に記載されている製品に対して実行される。

製品名
ジオトラストパワーサーバID証明書
ジオトラストクイックSSL証明書
ジオトラストクイックSSLプレミアム証明書

3.2.4 個人の实在性確認

ジオトラスト **My Credential** 証明書の申請者は、利用者の代わりとして、ジオトラストが定めた
フォームでジオトラスト My Credential 申請を完了するものとする。すべての申請は、ジオトラ
ストによって審査、承認、受領が行われる。申請者はすべて、My Credential 申請書内に連絡先
の電子メールアドレス（「Contact Address」）及び電話番号（「Telephone Number」）を含め、
「Contact Address」と「Telephone Number」を制御できることを証明するよう求められる。ジ
オトラストはその他の形で申請者の申請フォームに含まれる情報の正確性を検証せず、"errors
and omissions" もチェックしない。

True Credential 利用者は、自分の Common Name と電子メールアドレスのデータを CSR に含
めるか CSR と一緒に提供する必要がある。会社の管理者は、すべての証明書の発行申請を承認
する責任を単独で負う。

承認されると、ジオトラストは証明書についての情報を確認することなく、証明書申請を処理す
る。会社は必要に応じて、申請規約を通じて証明書発行の使用条件に同意することを求められ、
このサービスを介して証明書を受領する利用者は必要に応じて、管理者に承認されている証明書
を受領するために追加の使用条件に同意することを求められる場合がある。

3.2.5 確認を行わない申請情報

全製品の確認を行わない申請情報は以下の通り。

- Organization Unit (OU)
- 証明書において確認を行わないと明示されているその他の情報

パワーサーバID及びクイックSSL証明書の場合は、確認を行わない申請情報として国コード
も含む。

3.2.6 権限の確認

ジオトラストは、合理的な手段を講じて、組織に代わって行われた証明書申請が正当なものであ
り、適切に承認されていることを立証する。証明書が組織によって正当に承認されていることを
証明するために、ジオトラストは通常、組織の担当者（従業員または役員）の名前を要求する。
またジオトラストは通常、組織の承認形式も要求して組織が証明書を取得する意図を確認し、大

抵は組織の担当者を文書化する。ジオトラストは通常、記載の担当者に当該の承認内容を確認する。

3.2.7 共同運営の条件

規定しない。

3.3 リキー申請の確認と認証

証明書を継続して使用するためには、証明書の有効期限内に新しい証明書入手する必要がある。利用者は、自分の好みや、鍵生成ツールの機能及び制約に応じて、有効期限が満了するキー・ペアを取り替えるために新しいキー・ペアを生成するか（技術的に「リキー（reKey）」と定義される）、既存のキー・ペアで新しい CSR を作成する（技術的に「リニューアル（renewal）」と定義される）。本 CPS での説明上、前記の「リキー」と「リニューアル」のどちらもリニューアル証明書として扱われる。

リニューアル証明書は、本 CPS に記載されている、証明書の初回発行時に適用されるものと同じ認証手続きに従うものとする。

3.4 失効申請に関する確認と認証

ジオトラストによって発行された証明書の失効申請が許可される者は、利用者（指定された代理人を含む）、管理担当者、技術担当者、エンタープライズ管理者だけである。

失効申請を行うには、電子メール・メッセージ、国/地域の郵便、ファクシミリ、翌日配達便のいずれかで、利用者または権限を受けた申請者がジオトラストに連絡し、具体的に、利用者が特定した証明書の「revocation（失効）」（この用語を使用）申請を行う必要がある。

ジオトラストは、失効申請を受領すると、失効申請者に対して電子メール・メッセージで申請の確認を行う。メッセージ内容は、ジオトラストは失効申請を確認してから証明書を失効させること、及び失効情報が適切な CRL に掲載されることで利用者に証明書の失効について伝える通知が作成されることである。

ジオトラストは、確認の電子メール・メッセージの返信が失効を許可した管理担当者もしくは技術担当者から送信されるよう要求する（または、ジオトラストで許容できるその他の確認方法による）。ジオトラストは、確認の電子メール・メッセージを受信すると、証明書を失効し、その失効情報は適切な CRL に掲載される。証明書の Subject と Subject の指定連絡先に通知が送信される。失効前の猶予期間は利用者には与えられず、ジオトラストは翌日営業日以内に失効申請に対応し、失効情報を次回発行の CRL に掲載しなければならない。

エンタープライズ管理者は、ウェブ・ベースのアプリケーションで証明書を失効できる。

4. 証明書のライフサイクルの運用

4.1 証明書申請

4.1.1 証明書申請を行うことができる者

証明書申請を行うことができる者は、以下のとおりである。

- 証明書のSubjectに表示される個人
- 組織もしくはエンティティから権限を受けた代理人
- 認証機関から権限を受けた代理人
- 登録機関から権限を受けた代理人

4.1.2 登録手続き及び責任

4.1.2.1 エンドユーザ証明書の利用者

全エンドユーザ証明書の利用者は、関連する利用規約に同意することを明らかにし、次の各項目からなる申請手続きを履行するものとする。

- 証明書申請の必要事項を記載し、真正な情報を提供すること
- キー・ペアを生成もしくは生成させる手配をすること
- 自己の公開鍵を直接もしくは登録機関を通じてジオトラストに引き渡すこと
- ジオトラストに提示された公開鍵に対する秘密鍵の所有が証明できること

4.1.2.2 認証機関と登録機関の証明書

認証機関と登録機関証明書の利用者は、ジオトラストと契約を締結する。契約の過程において、認証機関と登録機関の申請者は、資格を証する書面と連絡先に関する情報を提供する。当該契約過程において、もしくは、遅くとも認証機関や登録機関のキー・ペアのキー・ジェネレーション・セレモニ前に、申請者は、ジオトラストに協力して、適切な Distinguished Name 及び申請者に対して発行されるべき証明書に記載される内容を決定する。

4.2 証明書申請手続

4.2.1 本人性確認と認証機能の実施

ジオトラスト、もしくは登録機関は、セクション3.2に規定される全利用者情報の確認と認証を行う。

ジオトラストが申請フォーム内の情報を確認できない場合の申請過程においては、カスタマ・サービス担当者が申請者に割り当てられ、申請過程の完了を促すことがある。それ以外にも申請者は、第三者による関連情報の修正、及び証明書の申請フォームの再提出を求められる場合がある。

4.2.2 証明書申請の承認もしくは拒絶

ジオトラストもしくは登録機関は、以下の基準が満たされている場合、証明書申請を承認する。

- セクション 3.2 において要求される利用者の全情報の確認及び認証が問題なく完了すること
- 支払いが完了していること

以下の場合、ジオトラストもしくは登録機関は、証明書申請を拒絶する。

- セクション 3.2 において要求される利用者の全情報の確認及び認証を完了することができないとき
- 利用者が、要求されたサポートのための資料提供をしないとき
- 利用者が、指定された時間内に返答をしないとき
- 支払いの完了を確認できないとき
- 利用者へ証明書を発行することがジオトラスト PKI の不信に繋がると信じられるとき

4.2.3 証明書申請の処理時間

ジオトラストは、受領から妥当な時間内に証明書申請の手続きを開始する。関連する利用規約、本 CPS もしくは他のジオトラスト PKI 参加者間の契約に別段の定めがない限り、申請処理を完了するまでの時間に関する規定は定めない。

その証明書申請は、拒絶または発行されるまで有効である。

4.3 証明書発行

4.3.1 証明書の発行過程における認証機関の行為

証明書は、ジオトラストによる証明書申請の承認後、または登録機関からの証明書発行申請を受領した後に、生成され発行される。ジオトラストは、証明書申請者に対し、証明書申請に含まれていた情報に基づき、当該証明書申請の承認後に、証明書を生成し発行する。

4.3.2 認証機関の利用者に対する証明書発行通知

ジオトラストは、直接もしくは登録機関を通じて、その証明書を生成したことを利用者に通知し、その証明書が利用可能になった旨を通知することにより、利用者に証明書へのアクセス手段を提供する。証明書は、エンドユーザ利用者がウェブ・サイトからダウンロードするか、API（アプリケーション・プログラミング・インターフェイス）を利用するか、もしくは当該利用者に対する証明書を含んで送信されたメッセージによるか、いずれかの方法により利用者が利用することができるようになる。

4.4 証明書の受領

4.4.1 証明書の受領となる行為

申請者は、当該証明書をダウンロードまたは使用することで、明示的に証明書の受領を示す。

4.4.2 認証機関による証明書の公開

ジオトラストは、一般にアクセス可能な公開されたりポジトリを用いて、発行した証明書を公開することがある。

4.4.3 他のエンティティに対する認証機関の証明書発行通知

登録機関は、自らの承認した証明書発行に関して通知を受け取ることがある。

4.5 キー・ペアと証明書の用途

4.5.1 利用者の秘密鍵及び使用

証明書における公開鍵に対応した秘密鍵の使用は、利用者が、利用規約に同意し、証明書を受領した場合にのみ許可される。その証明書は、ジオトラストの利用規約ならびに本 CPS の条件に従って合法的に使用されなければならない。証明書の使用は、証明書に含まれる keyUsage エクステンションに一致していなければならない（たとえば、もし Digital Signature が有効となっていない場合には、署名に使用されてはならない）。

利用者は、自らの秘密鍵を不正に使用されないよう保護し、証明書の有効期間が満了しましたは証明書が失効した場合は、秘密鍵の使用を中止しなくてはならない。

4.5.2 依拠当事者の公開鍵及び証明書の使用

依拠当事者は、証明書が関与するトランザクションを開始する前に、証明書失効リスト（CRL）を調べることで、その証明書が有効であることを確認しなければならない。ジオトラストは、不正に入手した証明書または CRL に掲載されている証明書への依拠について責任を負わない。証明書の依拠は、特定の状況下において、合理的でなければならない。具体的状況により追加の確認が必要であることを示している場合、依拠当事者は、そのような依拠が合理的であるとみなされるために、当該確認を行わなければならない。

依拠する行為を行う前に、依拠当事者は、独自に次のことを行う。

- 与えられた目的のために証明書を使用することが適当であるか否かを評価し、証明書が実際に、本 CPS で禁止されまたは制限されていない適切な目的に使用されるものであるか否かを決定する。ジオトラストは、証明書使用の適切さの評価について責任を負わない。
- 証明書は、証明書中に含まれる KeyUsage エクステンションに従って使用されるか否かを独自に評価する（たとえば、Digital Signature が有効でない場合には、証明書は、利用者の署名の有効性を検証するために依拠することはできない）。
- 証明書及び証明書を発行したチェーン内の全認証機関ステータスを評価する。証明書チェーン中の証明書が一つでも失効されている場合、依拠当事者は、エンドユーザ利用者の電子証明書によって、証明書チェーンの中の証明書が失効される前に署名された電子署名が信頼できるかどうかを調査する単独の責任がある。当該依拠は、依拠当事者の単独のリスクで行われるものとする。

証明書の使用が適切であることを前提として、依拠当事者は、実施したい電子署名の検証や他の暗号操作のために適切なソフトウェアやハードウェアを使用しなければならず、これがこれらの操作に関連する電子証明書に依拠する条件となる。当該操作は、証明書チェーンを識別すること、証明書チェーン内の全証明書の電子署名を検証することを含む。

4.6 証明書のリニューアル

4.6.1 証明書がリニューアルされる場合

証明書を継続して使用するためには、証明書の有効期限内に新しい証明書を手に入れる必要がある。利用者は、自分の好みや、鍵生成ツールの機能及び制約に応じて、有効期限が満了するキー・ペアを取り替えるために新しいキー・ペアを生成するか（技術的に「リキー（reKey）」と定義さ

れる)、既存のキー・ペアで新しい CSR を作成する (技術的に「リニューアル (renewal)」と定義される)。本 CPS での説明上、前記の「リキー」と「リニューアル」のどちらもリニューアル証明書として扱われる。

リニューアル証明書は、本 CPS に記載されている、証明書の初回発行時に適用されるものと同じ認証手続きに従うものとする。

4.6.2 リニューアルを申請することができる者

個人向け証明書についてはその利用者、組織向け証明書についてはその権限のある者のみが、証明書のリニューアルを依頼できる。

4.6.3 証明書のリニューアル申請の手続

本 CPS 4.2参照。

4.6.4 利用者に対する新しい証明書発行通知

利用者に対するリニューアルされた証明書の発行通知は、セクション4.3.2に従う。

4.6.5 リニューアルされた証明書の受領確認の行為

リニューアルされた証明書を受領したこととされる行為は、セクション4.4.1に従う。

4.6.6 認証機関によるリニューアルされた証明書の公開

規定しない。

4.6.7 他のエンティティに対する認証機関の証明書発行通知

登録機関は、自らの承認した証明書発行に関して通知を受け取ることがある。

4.7 証明書のリキー

本 CPS 3.3 参照。

4.7.1 リキーされる場合

本 CPS 3.3参照。

4.7.2 新しい公開鍵の証明書を申請することができる者

個人向け証明書についてはその利用者、組織向け証明書についてはその権限のある者のみが、証明書のリニューアルを依頼できる。

4.7.3 証明書のリキー申請の手続

セクション 4.6.3 の条項が適用される。

4.7.4 利用者に対する新しい証明書発行通知

利用者に対するリキーされた証明書の発行通知は、セクション4.3.2に従う。

4.7.5 リキーされた証明書の受領確認の行為

リキーされた証明書を受領したとされる行為は、セクション4.4.1に従う。

4.7.6 認証機関によるリキーされた証明書の公開

ジオトラストは、発行した証明書を公開しない。

4.7.7 他のエンティティに対する認証機関の証明書発行通知

登録機関は、自らの承認した証明書発行に関して通知を受け取ることがある。

4.8 証明書の変更

4.8.1 証明書が変更される場合

証明書の変更とは、既存の証明書の情報（利用者の公開鍵を除く）に変更があるために、新しい証明書の発行申請を行うことを指す。証明書の変更は、セクション4.1に規定される証明書申請として取り扱われる。

4.8.2 証明書の変更を申請することができる者

本 CPS 4.1.1参照。

4.8.3 証明書の変更申請の手続

ジオトラスト、もしくは登録機関は、セクション3.2に規定される全利用者情報の確認と認証を行う。

4.8.4 利用者に対する新しい証明書発行通知

本 CPS 4.3.2参照。

4.8.5 変更された証明書の受領確認の行為

本 CPS 4.4.1参照。

4.8.6 認証機関による変更された証明書の公開

適用せず。

4.8.7 他のエンティティに対する認証機関の証明書発行通知

本 CPS 4.4.3 参照。

4.9 証明書の失効及び効力の停止

4.9.1 失効が行われる場合

利用者は、以下のいずれかの理由で、いつでも証明書の失効を申請できる。利用者は、ジオトラスト（またはエンタープライズ管理者）に証明書の失効を申請するものとする。

- 証明書に記載されているいずれかの情報が変更されたか、古くなったとき
- 証明書に関連付けられている秘密鍵、または秘密鍵が保存されているメディアに危険が生じたとき
- 利用者のウェブ・サーバの所有権に変更が生じたとき

利用者は、失効申請を行う理由を申請時に提示しなければならない。

ジオトラストは、以下の場合に証明書を失効させる。

- 前述したように、利用者からの申請があったとき
- 証明書の署名に使用されるジオトラストの秘密鍵に危険が生じたとき
- 本 CPS または利用規約のいずれかに対する利用者の違反が発生したとき
- 証明書が適切に発行されなかったとジオトラストが判断したとき
- ジオトラストの許可なく、SSL 証明書が一度に複数のサーバにインストールされたとき
- カスタマもしくは利用者が、利用規約または申請規約に定める重要な義務を果たすことができなかったとき
- 発行元証明書が依拠当事者の信頼状態を危殆化する方法で使用されていると登録機関が合理的に判断したとき
- 発行元証明書に含まれる何らかの重要な事実が真実でなくなったとジオトラストが独自に判断したとき

ジオトラストは、証明書の失効を開始したら、利用者から指定された管理担当者及び技術担当者に対し、失効について電子メール・メッセージで通知するものとする。

ジオトラストが業務を停止する場合、ジオトラストのサービスを後継者に移行する計画も、別の方法で対処する計画もなければ、ジオトラストが発行した全証明書はジオトラストが業務を停止する日より前に失効されるものとし、またジオトラストは発行元から指定された技術担当に対し、失効及び失効理由について電子メール・メッセージで通知するものとする。

4.9.2 証明書の失効を申請することができる者

ジオトラストによって発行された証明書の失効申請が許可される者は、利用者（指定された代理人を含む）、管理担当者、技術担当者、エンタープライズ管理者、ジオトラスト、Microsoft（特定の状況下による）だけである。

4.9.3 失効申請要求の手続

4.9.3.1 エンドユーザ利用者の証明書失効申請手続

本 CPS 3.4参照。

4.9.3.2 認証機関もしくは登録機関証明書の失効申請手続

自らの認証機関または登録機関の証明書の失効申請を行う認証機関または登録機関は、ジオトラストに対しその旨知らせるものとする。ジオトラストは、それを受けて当該証明書の失効を行う。ジオトラストは、認証機関または登録機関の証明書の失効に自ら着手することもできる。

4.9.4 失効申請の猶予期間

証明書の失効申請は、商業上合理的な期間内に、可能な限り速やかに提出されるものとする。失効前の猶予期間は利用者に与えられない。

4.9.5 認証機関が失効申請を処理しなければならない期間

ジオトラストは、遅滞なく失効申請を処理するよう、商業上合理的な方策を講じる。

4.9.6 依拠当事者に要求される CRL の調査

依拠当事者は、自己が依拠しようとする証明書のステータスについて調査しなければならない。依拠当事者が証明書ステータスを調査するための一つの方法は、依拠当事者が依拠しようとする証明書を発行する認証機関が公表した最新の CRL を調査することである。CRL（証明書失効リスト）は、www.geotrust.com/resources/crls/index.aspで入手できる。

4.9.7 CRL の発行頻度

ジオトラストは、ジオトラストの事業継続プランで別段の定めのある場合を除いて、少なくとも週に一回（ただし、証明書失効後は 24 時間以内に）オンライン上に DER 形式で CRL を掲載するものとする。

4.9.8 CRL の最大発行所要時間

CRL は、作成後、商業的に合理的な時間内にリポジトリに掲載される。

4.9.9 利用可能なオンラインによる失効/ステータス調査

CRL の入手先：<http://www.geotrust.com/resources/crls/index.asp>

4.9.10 オンラインによる失効調査要件

依拠当事者は、依拠しようとする証明書のステータスをチェックしなくてはならない。

4.9.11 利用可能な失効の公表についての他の形式

適用せず。

4.9.12 鍵の危殆化に関する特別な要件

証明書の署名に使用されるジオトラストの秘密鍵に危殆が生じた場合、ジオトラストはできる限り速やかに全利用者に対して、秘密鍵なしで発行された証明書と一緒に電子メール・メッセージを送信する。メッセージ内容は、証明書が翌営業日までに失効されること、及び失効情報が適切な CRL に掲載されることで利用者に証明書の失効について伝える通知が作成されることである。

4.9.13 効力を停止する場合

ジオトラストは、証明書の効力停止はサポートしない。

4.9.14 効力停止申請をすることができる者

適用せず。

4.9.15 効力停止申請の手続

適用せず。

4.9.16 効力停止の制限

適用せず。

4.10 証明書のステータス・サービス

4.10.1 運用上の特徴

証明書のステータスは、ジオトラストのウェブ・サイトの CRL を通じて確認できる。

4.10.2 サービスの利用可能性

証明書ステータス・サービスは、1日24時間利用可能である。

4.10.3 オプション機能

適用せず。

4.11 利用の終了

利用者は、以下の事由によりジオトラスト証明書の利用を終了することができる。
・利用者の証明書を、リニューアルやリキーすることなく有効期限満了とした場合

- 利用者の証明書を、証明書を取り替えることなく有効期限前に失効させた場合

4.12 鍵の預託と復旧

作成された各認証機関証明書のルート鍵は、ハードウェアに保存され、バックアップされるが、預託はされない。ジオトラスト認証機関参加者は、エンドユーザ利用者の秘密鍵を預託できる。

4.12.1 鍵の預託と復旧及び実施

エンドユーザ利用者の秘密鍵は預託できる。

4.12.2 セッションキーのカプセル化及び復旧のポリシー及び実施

適用できる場合、秘密鍵はジオトラストの施設内で、暗号化された PKCS#12 構造体で保存される。一意の対称鍵が、各利用者の秘密鍵用に生成される。PKCS#12 構造体は、利用者の秘密鍵及び証明書で生成される。PKCS#12 構造体は、128 ビット AES を使用して、対称鍵で暗号化される。そして対称鍵は、128 ビット AES を使用して、エンタープライズのマスター・キー・リカバリー証明書の公開鍵で暗号化される。暗号化された PKCS#12 及び暗号化された対称鍵は、ジオトラストの施設で保存される。

秘密鍵及び電子証明書の復旧の場合、マスター・キー・リカバリー証明書のアクセス権を持つ管理者が、GeoCenter でエンタープライズ・アカウントに安全にアクセスし、記録される秘密鍵に対応している申請記録を選択することが求められる。それから管理者は、暗号化された PKCS#12 をダウンロードし、復旧プロセスを開始する。Java アプレットがローカルのワークステーションにダウンロードされ、管理者はマスター・キー・リカバリー証明書の場所と、マスター・キー・リカバリー証明書にアクセスするためのパスワードを特定するようプロンプトで指示される。Java アプレットは、マスター・キー・リカバリー証明書の秘密鍵にアクセスし、その秘密鍵を使用して、暗号化された対称鍵を復号する。そして対称鍵が表示され、管理者はその対称鍵を使用して、暗号化された PKCS#12 にアクセスできる。

5. 設備、管理及び運用統制

5.1 物理的管理

5.1.1 立地場所及び構造

ジオトラストの認証機関と登録機関業務は、公然または非公然の不正侵入及び機密情報とこれを扱うシステムの不正な使用、アクセスまたは開示を防止、予防、及び検知するよう物理的に保護された環境下で行われる。

ジオトラストの認証機関は、以下を含む高度にセキュアな施設に物理的に位置している。

- スラブで囲まれた防壁
- 電子制御アクセス・システム
- アラーム付きドア及びビデオ監視
- セキュリティ記録と監査
- 定義されたレベルの管理者により特別に承認された従業員が、カード・キーでアクセスする。

5.1.2 物理的アクセス

ジオトラストの権限のある従業員だけが、生体認証及び近接型カード・アクセスを使用して、ジオトラスト認証機関施設にアクセスできる。

5.1.3 電源及び空調

ジオトラストの認証機関施設は、一次及び予備として、以下の設備を備えている。

- 電力の継続的供給を確保する電源システム
- 温度及び相対湿度を管理するための暖房、換気、空調システム

5.1.4 水による被害

ジオトラストは、ジオトラストのシステムへの水による被害の影響を最小にするための合理的な漏水対策を講じている。

5.1.5 火災予防及び保護対策

ジオトラストは、火災の予防及び消火その他炎もしくは煙による影響を防ぐための合理的な予防策を講じている。ジオトラストの火災予防及び保護対策は、国内の火災安全規則に則って設計されている。

5.1.6 メディアの保管

商用ソフトウェア及びデータ、監査資料、保存記録またはバックアップ情報を格納するメディアはすべて、TL-15等級の安全性で、権限ある者だけがアクセスできる適切な物理的・論理的アクセス管理機能を有し、当該メディアの不測の損傷を防止するように設計されたジオトラストの複数の施設内に保管される。

5.1.7 廃棄物処理

機密文書及び資料は、廃棄前にシュレッダーにより処分されるものとする。機密情報を収集または伝達するために利用されたメディアは、廃棄前に読取不可能となるようにするものとする。暗号化デバイスは、廃棄前に、物理的に破壊されるか、または製造業者のガイドラインに従い初期化されるものとする。その他の廃棄物は、ジオトラストの通常の廃棄物処理要件に従い、廃棄される。

5.1.8 オフサイト・バックアップ

ジオトラストは、重要なシステム・データ、監査記録、その他の機密情報のバックアップを定期的に行う。重要な認証機関施設のバックアップ・メディアは、物理的にセキュアな方法でオフサイト施設で保管される。

5.2 手続的管理

5.2.1 信頼される役割

信頼される者には、以下の事項に重大な影響を及ぼしうる、認証または暗号作業にアクセスしもしくはこれを管理するすべての従業員、独立請負業者及びコンサルタントを含む。

- 証明書申請における情報の検証
- 証明書申請、失効要求、更新要求または申込情報の承認、拒絶その他の処理
- 証明書の発行または失効（リポジトリの制限された部分へアクセスする人を含む）
- 利用者の情報または要求の取扱

信頼される者には、以下の者を含むが、これに限定されない。

- カスタマ・サービス要員
- 暗号ビジネス運用要員
- セキュリティ要員
- システム管理者
- 技術要員のうち指定された者
- 認証基盤の信頼性を管理するために指名された経営陣

ジオトラストは、本セクションで明らかにされる要員の区分を、信頼される地位を有する信頼される者とする。信頼される地位を取得して信頼される者になろうとする者は、本 CPS に定める資格要件を完全に満たさなければならない。

5.2.2 職務ごとに必要とされる人数

ジオトラストは、業務内容に基づく職務の分離、及び機密を要する業務が信頼される者により実施されることを確実にするための厳格な管理手続きを定め、維持し、実施している。

職務上の責任に基づき、職務の分離を確実にするために、方針と管理手続きが制定される。認証機関用暗号ハードウェア（暗号署名ユニット、またはCSU）及び関連する鍵関係資料へのアクセス及び管理等の最も機密を要する業務は、信頼される者により行われる。これらの内部統制手続きは、物理的または論理的にデバイスにアクセスするために信頼される者が必要となるよう設計されている。認証機関用暗号ハードウェアへのアクセスは、その受入から最終の論理的または物理的破壊の検査までのライフサイクルを通じて、信頼される者により厳格に許可される。

5.2.3 それぞれの任務に必要な身元の確認

信頼される者になろうとするすべての者について、ジオトラストの人事部門またはセキュリティ部門への面前出頭及び広く認識されている身分証明書（パスポート、運転免許証等）の調査により、本人確認作業が行われる。身元については、さらに本 CPS セクション5.3.1に従い、身元調査が行われる。

ジオトラストは、ある人物に対して以下を実施する前に、当該人物が信頼される地位を獲得していること及び必要な部署の許可が取得されていることを保証する。

- アクセス用のデバイスが発行され、特定の必要とされた施設へのアクセスが許諾される
- ジオトラスト認証機関、登録機関、その他情報技術システムへアクセスし特定の業務を行うための電子的な資格証明書の発行を行う

5.2.4 職務の分離を必要とする役割

職務の分離を要求する役割は以下を含むが、これに限定されない。

- 証明書申請における情報の検証
- 証明書申請、失効要求、更新要求または申込情報の承認、拒絶その他の処理

5.3 人事的管理

信頼される者になろうとする者は、想定される業務を十分に遂行するために必要な経歴、資格及び経験を有することの証拠を提出しなければならない。さらに必要な場合、政府機関との契約に基づく証明サービスを履行するために必要な政府許可も提出しなければならない。経歴調査は、信頼される地位を有する人員について少なくとも5年毎に繰返されるものとする。

5.3.1 経歴、資格、経験及び許可要件

ジオトラストは、信頼される者になろうとする者が、想定される業務を十分に遂行するために必要な経歴、資格及び経験を有することの証拠を提出することを要求する。さらに必要な場合、政府機関との契約に基づく証明サービスを履行するために必要な政府許可も提出しなければならない。

5.3.2 経歴調査手続き

信頼される職務への雇用を行う前に、ジオトラストは以下の事項を含む経歴調査を行う。

- 過去の雇用の確認
- 職歴の照会
- 最高学歴もしくは適切な学歴の確認
- 犯罪歴の調査（地域、都道府県、国）
- クレジット/取引記録の照会
- 運転免許証の記録の調査
- 社会保障に関する記録の調査

地域の法律やその他の状況で禁止もしくは制限されているために、このセクションで定めたいずれかの要件を満たすことができない場合、ジオトラストは、実質的に同様の情報を得られ、法律上許される代替調査を利用する。これには、適切な政府機関が実行した経歴調査の入手を含むが、これに限定されない。

経歴調査により明らかになった事項で、信頼される地位の候補者として拒絶される理由となりうるもの、あるいは既存の信頼される者に対する何らかの措置を取る理由となりうるものは、一般的に以下のものを含む（ただし、これらに限定されない）。

- 候補者または信頼される人物の不実表示
- 極めて芳しくないまた信頼できない職業照会結果
- 刑事上の特定の有罪判決
- 財務に関する責任感が欠如している兆候

上記の情報を含む報告書は、人事及びセキュリティ要員が査定を行い、経歴調査で明らかになった事項の種類、影響度及び行動の頻度に照らし、適切な方針を決定する。そのような方針には、

最終的に、信頼される者への志願者の雇用取り消しや、既存の信頼される者の解雇などが含まれる場合がある。

経歴調査、及びこれにより収集された情報の取扱は、適切な連邦、州、及び地域の法律に従う。

5.3.3 トレーニング要件

ジオトラストは、検証業務を行うすべての者（認証スタッフ）に対し、基本的な公開鍵インフラストラクチャ（PKI）、認証及び検証のポリシーならびに手順、検証プロセスにおいてフィッシング及びその他のソーシャルエンジニアリング手法を含む一般的な脅威、そしてガイドラインに関するスキルトレーニングを実施する。

ジオトラストは、そのようなトレーニングの記録を維持して、認証スタッフ業務を任されている者が必ずその業務を満足に遂行できるだけの最小スキル要件を満たすようにする。EV SSL 証明書発行に関与する認証スタッフは、発行権限を有するために、ジオトラストのトレーニング及びパフォーマンスプログラムと一貫性のある適切なスキルレベルを保持しなければならない。

ジオトラストは、対応する検証業務を実行するための権限を検証スペシャリストに付与する前に、検証スペシャリストが必ずその検証業務で求められる各スキルレベルに達しているようにする。ジオトラストは、全認証スタッフが、ガイドラインに記載の EV SSL 証明書認証基準の概要に関する試験に合格することを要求する。

5.3.4 再トレーニングの頻度及び要件

ジオトラストは、従業員が業務を十分に遂行するための技能を維持することを確実にするために必要な範囲及び頻度で、再教育を行う。

5.3.5 人事異動の頻度及び順序

適用せず。

5.3.6 無権限の行為に対する制裁

無権限の行為またはジオトラストのポリシー及び手順に対するその他の違反に対しては、適切な懲戒処分が取られる。懲戒処分には解雇を含み、無権限の行為の頻度及び重大性に応じた措置が取られる。

5.3.7 請負事業者の要件

限定された環境下で、請負事業者またはコンサルタントが、信頼される地位を占めることがある。これらの請負業者またはコンサルタントに対しては、同種の地位にあるジオトラストの従業員に適用されるものと同じの業務上及びセキュリティ上の基準が適用される。

本 CPS セクション5.3.2に記載する経歴調査を完了または合格していない請負事業者ならびにコンサルタントは、信頼される者に付添われ、直接に監督される範囲でのみジオトラストの安全に管理された施設内にいつでもアクセスすることができる。

5.3.8 要員に提供される資料

ジオトラストは、業務を十分に遂行するために必要となるトレーニング及び資料の提供に従業員に対し行う。

5.4 監査記録の手続き

5.4.1 記録されるイベントの種類

ジオトラストは認証機関のイベント・データを記録する。

5.4.2 記録を処理する頻度

ジオトラスト認証機関のイベント・ジャーナル・データは、毎日及び月に一度の頻度で保管される。イベント・ジャーナルは審査対象である。

5.4.3 監査記録を保持する期間

監査記録は、少なくとも処理後2ヶ月間は記録を行った場所で保管され、その後はセクション5.5.2に従い保管されなければならない。

5.4.4 監査記録の保護

監査記録は、本 CPS セクション5.1.6に従って保護される。

5.4.5 監査記録のバックアップ手続

本 CPS 5.4.3参照。

5.4.6 監査ログ集計システム（内部対外部）

規定しない。

5.4.7 イベントを生ぜしめた Subject に対する通知

監査ログ集計システムによりイベントが記録される場合、当該イベントを生ぜしめた個人、機関、デバイスまたはアプリケーションに対しては、何らの通知をすることも要求されない。

5.4.8 脆弱性の評価

規定しない。

5.4.9 保管記録収集システム（内部又は外部）

規定しない。

5.4.10 保管記録情報の取得及び検証の手続

許可された信頼される者だけが保管記録へアクセスすることができる。保管された情報の復旧の際には、その整合性の検証を行う。

5.5 記録の保管

5.5.1 保管される記録の種類

ジオトラストは、以下の種類の記録を保管する。

- 証明書申請情報
- 証明書申請に関連する書類
- 失効、リキー、リニューアル申請情報などの証明書ライフサイクルに関連する情報

5.5.2 記録保管の期間

記録は、少なくとも3年間保管されなければならない。ただし、EV SSL 証明書の場合は、7年間の後の証明書の有効期間満了日または失効日までとする。

5.5.3 保管記録の保護

ジオトラストは、権限のある信頼される者のみがアクセスすることができるよう、保管された記録の保護を行う。保管された記録は、無権限者による閲覧、変更、削除その他改ざんができないよう、信頼されるシステムにより保護される。保管データを格納するメディア及び保管データを処理するために必要なアプリケーションは、本 CPS にて定められた期間、保管データにアクセスできることを確実にするために維持管理されなければならない。

5.5.4 保管記録のバックアップ手続き

規定しない。

5.5.5 記録のタイム・スタンプに関する要件

証明書、CRL 及びその他の失効に関するデータベースのエントリは、日時情報を含む。当該時間情報は、暗号化を要件とされない。

5.5.6 保管記録収集システム（内部又は外部）

規定しない。

5.5.7 保管記録情報の取得及び検証の手続

許可された信頼される者だけが保管記録へアクセスすることができる。保管された情報の復旧の際には、その整合性の検証を行う。

5.6 鍵の切り替え

ジオトラスト認証機関のキー・ペアは、本 CPS に定められたそれぞれのライフタイムの満了時にその役割を終了する。ジオトラスト認証機関証明書は、リニューアルできる。新規の認証機関キー・ペアは、たとえば、役割が終了する認証機関キー・ペアの交換を行う場合、実際に使用されているキー・ペアを補完する場合及び新しいサービスをサポートする場合など、必要に応じ生成される。

ジオトラスト認証機関のキー・ペアが有効期限の終了日時に達すると、その認証機関キー・ペアは少なくとも5年間は保管される。保管された認証機関キー・ペアは、ハードウェア暗号モジュールを使用して安全に保存される。手続的管理により、保管された認証機関キー・ペアは本番環境に戻らないようになる。保管期間が終了すると、保管されていた認証機関の秘密鍵は安全に破壊される。

ジオトラスト認証機関のキー・ペアはそれぞれの最大ライフタイムの満了時にその役割を終了するため、鍵の切り替えは発生しない。証明書は、その累計した証明書キー・ペアのライフタイムがその最大ライフタイムとして定められた期間を超えない限りにおいて、リニューアルすることができる。新規の認証機関キー・ペアは、本 CPS に従って、役割が終了する認証機関キー・ペアの交換を行う場合や、実際に使用されているキー・ペアを補完する場合、新しいサービスをサポートする場合など、必要に応じて生成される。

ジオトラスト認証機関キー・ペアのライフタイム

- ルート1 - Equifax Secure Certificate Authority : 有効期間満了日 2018年8月22日
- ルート2 - GeoTrust Global CA : 有効期間満了日 2022年5月21日
- ルート3 - GeoTrust Universal CA : 有効期間満了日 2029年3月4日
- ルート4 - Equifax Secure eBusiness CA-1 : 有効期間満了日 2020年6月21日
- ルート5 - Equifax Secure Global eBusiness CA-1 : 有効期間満了日 2020年6月21日
- ルート6 - GeoTrust Global CA2 : 有効期間満了日 2019年3月4日
- ルート7 - GeoTrust Universal CA2 : 有効期間満了日 2029年3月4日
- ルート8 - Equifax Secure eBusiness CA-2 : 有効期間満了日 2020年6月21日
- ルート9 - GeoTrust CA for Adobe : 有効期間満了日 2015年1月15日
- ルート10 - GeoTrust Mobile Device Root – Unprivileged : 有効期間満了日 2023年7月29日
- ルート11 - GeoTrust Mobile Device Root – Privileged : 有効期間満了日 2023年7月29日
- ルート12 - GeoTrust CA for UTI : 有効期間満了日 2024年1月23日
- ルート13 - GeoTrust True Credentials CA 2 : 有効期間満了日 2020年6月21日
- ルート14 - GeoTrust Primary Certification Authority : 有効期間満了日 2036年7月16日
- ルート15 – GeoTrust Primary Certification Authority - G2 : 有効期間満了日 2038年1月18日
- ルート16 – GeoTrust Primary Certification Authority – G3 : 有効期間満了日 2037年12月1日

本 CPS の発行後に作成された新しいルート及び認証機関の最大有効期間は、以下のようになる。

- 自己署名された認証機関の証明書 : 30年間
- 中間認証機関の証明書 : 15年間

5.7 危殆化及び災害からの復旧

5.7.1 事故及び危殆化の取扱手続

きわめて重要なビジネス情報及び認証機関情報のバックアップ用コピーは定期的に作成される。通常、バックアップはオンサイトで毎日、そしてオフサイトで週に一度の頻度で行われるが、本番環境のスケジュール要件に応じ、ジオトラストの判断で、実行頻度を減らすことができる。

5.7.2 コンピューターの資源、ソフトウェア、またはデータが破損した場合

コンピュータ・リソース、ソフトウェア、またはデータについて破損が生じた場合、当該事象の発生についてはジオトラストのセキュリティ担当部署に報告されるものとする。そして、適切な上位者に対する報告、事故調査、及び事故対応が行われる。

5.7.3 エンティティの秘密鍵が危殆化した場合の手続

ジオトラストの1つ以上のルート鍵（認証機関証明書を含む）で危殆化が発生した場合、ジオトラストは速やかに全利用者に電子メールで通知し、依拠当事者及びその他には www.geotrust.com に掲載される CRL と追加通知で知らせ、さらに当該ルート鍵で発行されたすべての証明書を失効させるものとする。

5.7.4 災害後の事業継続能力

ジオトラストは、重要な事業プロセスの妨害または失敗が発生した後で、合理的にタイミングのよい方法でジオトラスト認証機関の事業運用を保守または回復するための事業継続プラン（BCP）を有する。

きわめて重要なビジネス情報及び認証機関情報のバックアップ用コピーは定期的に作成される。通常、バックアップはオンサイトで毎日、オフサイトで週に一度、そしてジオトラストの災害復旧サイトで月に一度の頻度で行われるが、本番環境のスケジュール要件に応じ、ジオトラストの判断で、実行頻度を減らすことができる。

5.8 認証機関または登録機関の終了

ジオトラストまたはその認証機関が運用を終了させる必要がある場合、ジオトラストは認証機関が終了する前に、利用者、依拠当事者及び当該終了により影響を受ける他の当事者に対し、その旨を通知するよう商業上合理的な努力をする。認証機関の終了が必要な場合、ジオトラストは、利用者及び依拠当事者に対する混乱を最小限に抑えるために終了プランを作成する。当該終了プランは、適宜次の事項に言及する。

- 利用者及び依拠当事者など、終了により影響を受ける当事者に対し、当該認証機関の状況を知らせる通知の提供
- 当該通知費用の取扱
- ジオトラストにより当該認証機関に発行された証明書の失効
- 本 CPS で必要とされている期間中における当該認証機関の記録の保存
- 利用者及びカスタマ・サポート・サービスの継続
- CRL の発行などの失効サービスの継続

- 必要に応じ、利用者及び下位認証機関の証明書で、有効期間内かつ失効されていないものの失効
- 必要な場合、有効期間内かつ失効されていない証明書について、終了プランにより失効された利用者への補償の支払い。または、後継の認証機関による代替証明書の発行
- 当該認証機関の秘密鍵、及び当該秘密鍵を含むハードウェア・トークンの処分
- 当該認証機関のサービスを後継の認証機関に移行するために必要な規定
- ジオトラストの認証機関及び登録機関の記録を保管する保管機関の身元。利用者及び依頼当事者への通知で別の保管機関が示されなければ、ジオトラストの登録機関であるデータウェア・コーポレーションが管理機関になるものとする。

6 技術的セキュリティ・コントロール

6.1 キー・ペア生成及びインストール

6.1.1 キー・ペア生成

認証機関キー・ペアの生成は、複数の訓練を受けた信頼される個人により、セキュアなシステム、及びセキュリティならびに鍵生成に要求される暗号強度を提供する手順を用いてなされる。それぞれの鍵生成セレモニーにおいて行われた活動は記録され、日付が付され、携わったすべての個人により署名される。これらの記録は、ジオトラストの経営陣が適当であるとみなす期間、監査及び後日の調査の目的で保管される。

少なくとも、鍵生成に用いられる暗号モジュールは、FIPS140-1 レベル3 の要件を満たす。作成された各認証機関証明書のルート鍵は、ハードウェアに保存され、バックアップされるが、預託はされない。各認証機関証明書のルート鍵は、証明書の署名、CRL 署名、オフラインでの CRL 署名に使用できる。

ジオトラストの認証機関キー・ペアは、バックアップ及び鍵復旧手順が規定され、高度に保護された信頼される環境で維持される。

6.1.2 秘密鍵の受渡

適用せず。

6.1.3 公開鍵の証明書発行者への受渡

利用者及び登録機関は、その公開鍵をその認証のためジオトラストに対し、PKCS#10 の証明書署名要求 (CSR) を用いるか、または、セキュア・ソケット・レイヤ (SSL) によって保護されたセッションにおいて他のデジタル署名の付されたパッケージを用いて、送付するものとする。認証機関、登録機関、または利用者のキー・ペアは、ジオトラストにより生成される場合、本要件は適用されない。

6.1.4 認証機関公開鍵のユーザへの受渡

ジオトラストは、認証機関証明書をウェブ・ブラウザ・ソフトウェアに組み込むことにより、利用者及び依頼当事者が利用できるようにする。特定のアプリケーションにおいては、アプリケーションのルート・ストアを使用して、アプリケーション・ベンダーによりジオトラストの公開鍵が提供される。ジオトラストは通常、すべての証明書チェーン（発行認証機関証明書及びその子

エン内的認証機関証明書を含む)を、証明書の発行と同時に、利用者に対し提供する。ジオトラス認証機関証明書は、ジオトラスのリソース・ウェブ・サイト (<http://www.geotrust.com/resources>) からダウンロードすることもできる。

6.1.5 鍵のサイズ

キー・ペアの予想される使用期間においては、キー・ペアは、暗号解読技術によってキー・ペアの秘密鍵が解かれないように十分な長さが使用されるべきである。ジオトラスの現在の最小の鍵サイズは、1024ビット RSA の強度相当のキー・ペアで使用されるものであり、そのルート及び認証機関の場合はそれ以上である。1024ビットの RSA キー・ペアを有するジオトラス認証機関は、2013年12月31日までに2048ビットの RSA に移行するものとする。ジオトラスのユニバーサル・ルート認証機関は、4096ビットの RSA を有する。

ジオトラスは、登録機関及び利用者に対し2048ビットの RSA キー・ペアを生成するように推奨する。ジオトラスは、引き続き2048ビットの RSA よりも小さいサイズのキー・ペアで生成されたエンド・エンティティ証明書を承認していくが、1024ビットの RSA は2013年12月31日までに段階的に廃止する。

ジオトラス EV SSL 証明書の鍵サイズは、本 CPS の Appendix A2 に記載される。

6.1.6 公開鍵のパラメータの生成

適用せず。

6.1.7 鍵用途目的 (X.509 バージョン 3 の Key Usage フィールドのとおり)

セクション7.1.2.1.参照

6.2 秘密鍵の保護

ジオトラスは、ジオトラス認証機関の秘密鍵のセキュリティを確実にするため、物理的、論理的、及び手続的管理を実施している。利用者は契約により秘密鍵の紛失、漏洩、変更、または権限のない者による使用を防止するために必要な対策を取ることが要求されている。

6.2.1 暗号モジュールの基準

ルート認証機関のキー・ペアの生成及び認証機関の秘密鍵の保管に関し、ジオトラスは、少なくとも FIPS 140-1 レベル3 の認定を受けもしくは要件を満たすハードウェア暗号モジュールを使用している。

6.2.2 複数人による秘密鍵 (m of n) の管理

認証機関キー・ペアの生成は、複数の訓練を受けた信頼される個人により、セキュアなシステム、及びセキュリティならびに鍵生成に要求される暗号強度を提供する手続を用いてなされる。すべての認証機関キーペアは、予め計画された鍵生成セレモニーにおいて生成される。それぞれの鍵生成セレモニーにおいて行われた活動は記録され、日付が付され、携わったすべての個人により署名

される。これらの記録は、ジオトラストの経営陣が適当であるとみなす期間、監査及び後日の調査の目的で保管される。

6.2.3 秘密鍵の預託

各認証機関証明書のルート鍵は、バックアップされるが、預託はされない。

6.2.4 秘密鍵のバックアップ

ジオトラストの認証機関キー・ペアは、バックアップ手続が規定され、高度に保護された信頼される環境で維持される。

6.2.5 秘密鍵の保管

ジオトラスト認証機関のキー・ペアが有効期限の終了日時に達すると、その認証機関キー・ペアは少なくとも5年間は保管される。保管された認証機関キー・ペアは、オフライン・メディアを使用して安全に保存される。手続的管理により、保管された認証機関キー・ペアは本番環境に戻らないようにする。保管期間が終了すると、保管されていた認証機関の秘密鍵は安全に破壊される。

6.2.6 秘密鍵の暗号化モジュールへの入出力

秘密鍵の暗号化モジュールへの入出力は、製造元のモジュール・ガイドラインに従って安全な方法で実行される。

6.2.7 秘密鍵の暗号モジュールへの格納

秘密鍵の暗号モジュールへの格納は、製造元のモジュール・ガイドラインに従って安全な方法で実行される。

6.2.8 秘密鍵の起動の方法

ジオトラスト PKI 参加者はすべて、自己の秘密鍵の起動データにつき滅失、盗難、無権限者による漏洩または使用を防止しなければならない。

6.2.9 秘密鍵の非活性化の方法

ジオトラストの登録機関の秘密鍵（登録機関申請を認証するために用いられたもの）はシステムログオフで非活性化される。ジオトラストの登録機関は、その場を離れる場合に自らのワークステーションをログオフすることが要求される。

利用者は、自分の秘密鍵を適切に保護する義務がある。

6.2.10 秘密鍵の破壊の方法

保管された認証機関キー・ペアは、オフライン・メディアを使用して安全に保存される。手続的管理により、保管された認証機関キー・ペアは本番環境に戻らないようにする。

暗号化デバイスは、廃棄前に、物理的に破壊されるか、または製造業者のガイドラインに従い初期化されるものとする。

6.2.11 暗号モジュールの評価

本 CPS セクション6.2.1参照

6.3 キー・ペアの管理に関する他の点

6.3.1 公開鍵の保管

規定しない。

6.3.2 証明書の運用期間及びキー・ペアの使用期間

証明書の有効期間は通常、証明書の発行日（証明書に記載があればそれ以降）に始まり、有効期間内に失効されなければ、証明書に記載されている効力が終了する日時に終わる。キー・ペアの使用可能期間は、それに関連付けられた証明書の有効期間と同一であるが、秘密鍵に関しては復号化のため使用を継続することができ、公開鍵は署名の検証のために使用を継続することができる。

6.4 起動データ

6.4.1 起動データの生成とインストレーション

ジオトラスト登録機関は、自己の秘密鍵を保護するため、強度のパスワードを選択することを要求される。パスワード選択に関するガイドラインでは、システム・ログオン・パスワードに関し、次の要件を定めている。

- ユーザによって生成されること
- 少なくとも8文字以上であること
- 少なくとも1文字以上のアルファベットと1文字以上の数字を含むこと
- 少なくとも1以上の小文字を含むこと
- 同じ文字が多く含まれないこと
- オペレータの氏名等の属性と同一でないこと
- ユーザの属性から容易に推測される文字列を含むものでないこと

6.4.2 起動データの保護

ジオトラストのシークレット・シェア保有者は、そのシークレット・シェアを保護すること及び保有者としての責任を認識する合意書に署名することが要求される。

ジオトラスト登録機関は、その管理者/登録機関の秘密鍵を、パスワード保護を用い、暗号化した形式で保管することが要求される。

ジオトラストは、利用者に対し、その秘密鍵を暗号化した形式で保管すること及びその秘密鍵をハードウェア・トークンまたは強度なパスフレーズのいずれかまたは双方を用いて保護すること

を強く推奨する。2つの方法による認証メカニズム（たとえば、トークンとパスフレーズ、生体認証とトークン、または生体認証とパスフレーズ）が推奨される。

6.4.3 起動データに関する他の点

6.4.3.1 起動データの転送

秘密鍵の起動データを転送する場合、ジオトラスト認証機関の参加者は、当該秘密鍵の紛失、盗難、改ざん、不正な開示、無権限の使用が行われないようにしなければならない。Windows やネットワークのログインのためのユーザネームとパスワードの組み合わせがエンドユーザ利用者の起動データとして用いられる場合、ネットワークを経由したパスワードの転送は、無許可のユーザのアクセスから保護されなければならない。

6.4.3.2 起動データの破壊

適用できる場合、認証機関の秘密鍵の起動データは、当該起動データによって保護される秘密鍵の紛失、盗難、改ざん、不正な開示、無権限の使用を防止する方法を用いて、運用を中止する。

6.5 コンピュータ・セキュリティ管理

ジオトラストは、すべての認証機関及び登録機関の機能を、信頼されるシステムで履行する。

6.5.1 特定のコンピュータ・セキュリティの技術的要件

6.5.2 コンピュータ・セキュリティの評価

規定しない。

6.6 ライフサイクル技術管理

6.6.1 システム開発管理

規定しない。

6.6.2 セキュリティ管理

規定しない。

6.6.3 ライフサイクル・セキュリティ

規定しない。

6.7 ネットワーク・セキュリティ管理

規定しない。

6.8 タイム・スタンプ

証明書、CRL 及びその他の失効に関するデータベースのエントリは、日時情報を含む。当該時間情報は、暗号化を要件とされない。

7. 証明書、CRL 及び OCSP のプロファイル

7.1 証明書のプロファイル

ジオトラストの証明書は、(a) 国際電気通信連合・電気通信標準化部門勧告 X.509 バージョン 3 (1997):Information Technology - Open Systems Interconnection _ The Directory: Authentication Framework, June 1997 及び (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 (“RFC 5280”) にほぼ準拠する。証明書のエクステンションとその Criticality、ならびに暗号アルゴリズムオブジェクト識別子は、IETF RFC5280基準及び勧告に従い設定される。利用者の名前の形式は、ジオトラストの内部ポリシー、及び本 CPS の別の場所に記載されている認証手続きによって定められる。名前制約の適用は、名前制約エクステンションではなく、認証手続き及び各利用者との契約上の制限に従って行われる。ジオトラストは、特定の証明書ポリシー・オブジェクト識別子を適用することはないが、適用可能な CPS バージョンと URL アドレスを参照する。ポリシー制約エクステンション、ならびにポリシー修飾子の構文及び意味が使用される場合は、RFC 5280基準に準拠する。

EV SSL 証明書の項目とプロファイルの要求項目については、本 CPS Appendix A3 のセクション6に記載される。

7.1.1 バージョン番号

認証機関証明書は、X.509バージョン1またはバージョン3の認証機関証明書である。エンドユーザ利用者の証明書は、X.509バージョン3でなければならない。

7.1.2.1 Key Usage

X.509 バージョン3証明書は、一般に、RFC 5280 (Internet X.509 Public Key Infrastructure Certificate) に従い設定される。

7.1.2.2 Certificate Policies エクステンション

X.509バージョン3証明書のCertificatePolicies エクステンションは、通常使用されない。EV SSL 証明書の CertificatePolicies エクステンションは、本 CPS の Appendix A3 に従って設定される。

7.1.2.3 Subject Alternative Names

X.509バージョン3証明書の subjectAltName エクステンションが使用される場合は、RFC 5280 に従って設定される。

7.1.2.4 Basic Constraints

エンドユーザ利用者証明書における BasicConstraints エクステンションは、Null に設定されなければならない。

7.1.2.5 Extended Key Usage

規定しない。

7.1.2.6 CRL Distribution Points

ほとんどのジオトラストの X.509バージョン3の個人向け証明書及び認証機関証明書は、依頼当事者が CRL を入手し認証機関の証明書のステータス情報を確認できるように、cRLDistributionPoints エクステンション中に URL のロケーション情報を持つ。

7.1.2.7 Authority Key Identifier

通常、ジオトラストは、X.509バージョン3個人向け証明書と中間認証機関証明書の Authority Key Identifier エクステンションを設定する。

7.1.2.8 Subject Key Identifier

ジオトラストが、subjectKeyIdentifier エクステンションを有する X.509証明書を発行する場合、keyIdentifier は、当該証明書の Subject の公開鍵に基づき、RFC 5280に記述された方法の一つに従い生成される。

7.1.3 アルゴリズムオブジェクト識別子

暗号アルゴリズムオブジェクト識別子は、IETF RFC5280基準及び勧告に従い設定される。

7.1.4 名前の形式

ジオトラストは、本 CPS セクション3.1.1に従い、証明書を発行する。

7.1.5 名前制約

規定しない。

7.1.6 証明書ポリシー・オブジェクト識別子

本 CPS の Appendix A3 に従い、EV SSL 証明書のみ適用される。

7.1.7 ポリシー制約エクステンションの使用

規定しない。

7.1.8 ポリシー修飾子の構文及び意味

規定しない。

7.1.9 クリティカルな Certificate Policies エクステンションに対する解釈方法

規定しない。

7.2 CRL のプロフィール

規定しない。

7.2.1 バージョン番号

規定しない。

7.2.2 CRL 及び証明書失効リスト・エントリ・エクステンション

規定しない。

7.3 OCSP プロファイル

OCSP (Online Certificate Status Protocol) は、ある特定の証明書に対する失効情報を速やかに得るための一つの方法である。ジオトラストは、True Business ID with EV、True Credentials for Adobe、及び My Credential for Adobe の場合を除き、証明書ステータス要求をチェックするための OCSP を提供しない。

OCSP レスポンダーは、RFC 2560に準拠する。

7.3.1 バージョン番号

規定しない。

7.3.2 OCSP エクステンション

規定しない。

準拠性監査とその他の評価

8.1 評価の頻度・状況

拠性監査は、少なくとも年1回実施される。

8.2 評価人の身元と資格

ジオトラストの認証機関の準拠性監査は、次のような公的な監査法人により遂行される。

- 公開鍵インフラストラクチャ技術、情報セキュリティツール及び技術、セキュリティ監査ならびに第三者証明の職務に深い知識を有すること。及び、
- 米国公認会計士協会 (AICPA) から認定された者で、特定の技術の保有に加え、専門家同士の審査、能力テスト、業務に対する適正なスタッフの配置に関する基準といった品質を保障する手段、ならびに継続的な職業教育の要件を備えていること。

8.3 評価人と被評価者との関係

ジオトラストの運用についての準拠性監査は、ジオトラストとは独立の監査法人によって遂行される。

8.4 評価対象項目

ジオトラストが行う認証機関（またはこれと同等のもの）監査のための年次の WebTrust の範囲は、認証機関の環境統制、キーマネジメントの運用、インフラストラクチャ及び管理認証機関の統制、証明書ライフサイクル管理及び認証機関の業務に関する情報開示を含むものである。

8.5 欠陥の結果としてとられる処置

ジオトラストの運用に関する準拠性監査に関し、重大な例外または欠陥が当該準拠性監査において指摘された場合、とるべき措置が決定される。当該決定は、監査人からの指摘を受けて、ジオトラストの経営陣によりなされる。ジオトラストの経営陣は、是正措置の策定及び実施につき責任を負う。もし、ジオトラストが、当該例外または欠陥がジオトラスト認証機関のセキュリティもしくは完全性に対する直接的な脅威を示すものであると決定した場合には、是正措置が策定され、商業的に合理的な期間内に実施される。これよりも深刻度の低い例外または欠陥については、ジオトラストの経営陣は、当該事由の重要性について評価し、適切な措置を決定する。

8.6 結果の伝達

ジオトラストの WebTrust for CA 監査報告書のコピーは、ジオトラストのウェブ・サイトで WebTrust マークをクリックすると確認できる。

9. 業務及び法律に関するその他の事項

9.1 料金

9.1.1 証明書発行または更新の手数料

ジオトラストは、利用者に対し、証明書の発行、管理及び更新に関し、手数料を請求することができる。

9.1.2 証明書のアクセス手数料

ジオトラストは、証明書をリポジトリに置くかまたは他の方法により、依頼当事者がこれを利用することができるようにする対価としての手数を請求しない。

9.1.3 失効またはステータス情報のアクセス手数料

ジオトラストは、本 CPS の定めにより CRL をリポジトリで利用できるようにすること、または他の方法により、依頼当事者がこれを利用することができるようにする対価としての手数を請求しない。ただし、ジオトラストは、特別にカスタマイズされた CRL、OCSP サービス、その

他の付加価値のある失効及びステータス情報サービスに関しては手数料を請求することができる。ジオトラストの書面による事前の明示的な同意がない限り、証明書ステータス情報を活用する製品または役務を提供する第三者は、失効情報、証明書ステータス情報またはリポジトリ内のタイム・スタンプに対するアクセスをすることが許されない。

9.1.4 他のサービスの手数料

ジオトラストは、本 CPS に対するアクセスに関し手数料を請求しない。文書の単純な閲覧以外の目的、たとえば複製、再配布、変更または派生的文書の作成等を目的とする利用については、当該文書の著作権を有する者とのライセンスに関する合意を得ることを条件とする。

9.1.5 返金制度

ジオトラストの返金制度はジオトラストのウェブ・サイト (<http://www.geotrust.com/resources>) で確認できる。利用者がリセラなどジオトラスト以外の者に証明書の手数料を支払った場合は、その者からの返金を要求すべきである。

ほとんどの場合、利用者は、代替証明書の発行に返金を利用できる。代替証明書を取得するには、利用者が新たに証明書署名要求 (CSR) をジオトラストに提供するか、利用者からジオトラストに以前提供された CSR に基づいて証明書を再発行するよう要求する。

9.2 財務的責任

9.2.1 保険

ジオトラストは親会社を通じて、企業総合賠償責任保険に加入する。

9.2.2 その他の資産

エンタープライズ・カスタマは、自己の業務の遂行と義務の履行をするに足る十分な財政的基盤を有し、利用者及び依拠当事者に対する責任を合理的な範囲で負担することができなければならない。シマンテックの財務状況は、<http://investor.symantec.com/phoenix.zhtml?c=89422&p=irol-irhome> で公開されている。

9.2.3 拡張された保証

GeoSure プロテクション・プランは、ジオトラストの不注意や契約上の責任による証明書発行時やその他の不正行為によって発生した欠陥による紛失/損害から保護するための特定のジオトラスト証明書利用者への拡張された保証である。証明書利用者は、適用されるサービス規約に準じることで適用される。GeoSure プロテクション・プランに関する一般的な情報及びどの証明書がこの対象になるかは、http://www.geotrust.com/resources/cps/pdfs/GeoSure_Plan_v3.0.pdf で参照できる。

9.3 業務情報の機密保持

9.3.1 機密情報の範囲

証明書の申請フォームに入力して提供された、利用者についての特定の情報（個人の連絡先情報、クレジットカード情報など）は、ジオトラストによって機密扱いされ、ジオトラストは利用者の事前の同意がなければ当該情報を公開してはならない。前記の規定にかかわらず、ジオトラストは以下の場合に当該情報を開示できる。(a) 裁判所命令または召喚状が届いて、もしくはジオトラストの弁護士から助言を受けて、裁判所、捜査当局、その他第三者に開示する場合（民事訴訟における開示手続きへの対応による開示を含む）、(b) ジオトラストからの通報により、利用者による詐欺、不当表示、不正アクセス、違法活動の疑いを捜査するために、捜査当局者及びその他の者に開示する場合。

9.3.2 機密とみなされない情報

証明書に表示される情報、証明書の失効に関連する情報、またはジオトラストがすでに所有していたか単独で入手した利用者に関する情報は、機密とみなされない情報である。

ジオトラストは利用者の情報を集計ベースで開示できる。これにより利用者は、ジオトラストに対し、利用者の集計情報を修正する権限、及び第三者が代わりに当該機能を実行することを許可する権限を含む、情報開示の許可を与える。

9.3.3 機密情報保護責任

ジオトラストは、重要な秘密情報が損なわれ、第三者に漏洩しないよう安全な措置を講じる。

9.4 個人情報の保護

9.4.1 プライバシーポリシー

ジオトラストはプライバシー・ポリシーを作成し、
<http://www.geotrust.com/resources/legal/privacy.asp> で公開している。

9.4.2 個人情報

利用者に関する情報で、証明書、証明書ディレクトリ及びオンラインのCRLを通じて入手できない情報は、個人情報として取り扱う。

9.4.3 個人情報とみなされない情報

法律を従うことを条件に、証明書で公開される情報は、秘密情報とみなされない。

9.4.4 個人情報の保護責任

個人情報を受領したジオトラスト PKI 参加者は、当該情報が損なわれ、第三者に漏洩しないよう安全な措置を講じると共に、適用される個人情報保護に関する法律に従うものとする。

9.4.5 個人情報を利用するための通知及び同意

本CPS またはプライバシーポリシーに別途定めのない限り、もしくは別段の合意のない限り、個人情報は当該情報者の同意がない限り、利用することはできないものとする。本条は、適用される個人情報保護法規に従う。

9.4.6 司法または行政手続きによる開示

ジオトラストは、ジオトラストが以下に相当すると誠実に判断する場合、秘密情報及び非公開情報を開示することができる。

- 召喚状及び捜索令状により情報開示が必要な場合
- 召喚状、質問状、自白要請、文書作成要請などの民事訴訟または行政措置における情報開示プロセスで、司法、行政、その他の法的な手続きにより情報開示が必要な場合

本条は、適用される個人情報保護法規に従う。

9.4.7 他の情報開示に関する状況

規定しない。

9.5 知的財産権

利用者及び依拠当事者を除く、ジオトラスト PKI 参加者間での知的財産権の帰属は、ジオトラスト PKI 参加者間での契約により定められる。本 CPS セクション9.5以下の各項目は、利用者と依拠当事者に関する知的財産権について適用される。

9.5.1 証明書及び失効情報に関する財産権

認証機関は、自己が発行した証明書及び証明書失効情報に関するすべての知的財産権を留保する。ジオトラスト及びカスタマは、証明書を複製し、配布することを、非独占かつ無償で認めるが、当該複製はそれら全情報を完全な形で複製するものでなければならない。ジオトラスト及びカスタマは、適用される CRL 利用規約または他の適用される契約の定めるところに従い、依拠当事者機能を果たすため証明書失効情報を使用することを認める。

9.5.2 本 CPS に関する知的財産権

ジオトラスト PKI 参加者は、ジオトラストが本 CPS に関するすべての知的財産権を有することを確認する。

9.5.3 名称に含まれる権利

証明書申請者は、証明書申請に含まれる商標、サービス・マーク、商号ならびに証明書申請者に発行される証明書中の Distinguished Name に関するすべての権利を留保する。

9.5.4 鍵及び鍵のデータに関する財産権

認証機関及び利用者の証明書に対応するキー・ペアは、それらが保管及び保護されている物理的媒体の如何にかかわらず、当該証明書における Subject となっている認証機関及び利用者が保有するものであり、当該キー・ペアに係るすべての知的財産権は当該認証機関及び利用者に帰属する。前記の一般性を制限することなく、すべての自己署名証明書を含むジオトラストのルート公開鍵及びそれを含むルート証明書については、ジオトラストに帰属する。ジオトラストは、ソフトウェア及びハードウェア製造者に対し、信頼できるハードウェア・デバイス及びソフトウェア上に当該ルート証明書のコピーを置くために、当該ルート証明書を複製する権利を与えている。

9.6 表明と保証

9.6.1 認証機関の表明と保証

ジオトラストは、証明書発行の時点で、以下の限定保証を提供する。(i) ジオトラストは、実質的に本 CPS に準拠して証明書を発行した; (ii) 証明書内に含まれる情報は、すべての重要な点において、申請者によってジオトラストに提供された情報を正確に反映している; (iii) ジオトラストは、合理的な手段を講じて、証明書内の情報が正確であることを検証した (True Credential 及び True Credential Express クライアント証明書の場合を除く)。証明書に含まれる情報を検証するためにジオトラストが講じた手段の特性は、本 CPS に定めるとおりである。

9.6.2 登録機関の表明と保証

登録機関は、以下の事項を保証する。

- 証明書に記載される事実には、証明書申請を承認、または、証明書を発行するエンティティが知り、またはこれらに起因する重要な不実の記載は存在しないこと
- 証明書中の情報には、証明書申請を承認するエンティティが、証明書申請の取扱において合理的注意を怠ったことにより生じた誤りが存在しないこと
- 証明書が本 CPS に定めるすべての重要な要件に合致していること
- 失効サービス (該当する場合) 及びリポジトリの使用が、すべての重要な点において、適用される CPS に準拠していること

利用規約には、追加の表明と保証を定めることができる。

9.6.3 利用者の表明と保証

利用者は以下の事項を保証する。

- 証明書に記載される公開鍵に対応する秘密鍵を用いて生成するそれぞれのデジタル署名が、利用者のデジタル署名であり、デジタル署名を生成する時点において、証明書が受領され、有効なものであること (有効期間内で、失効されてもいないこと)
- 利用者の秘密鍵については、十分な保護がされており、かつ、権限を付与された者以外の何人もアクセスしたことがないこと
- 利用者が証明書申請時行った表明が真実であること
- 利用者によって提供され、証明書に記載されているすべての情報が真実であること
- 証明書が、正当で合法的な目的のためにのみ、かつ、本 CPS を遵守した態様によってのみ、使用されていること

- 利用者は、エンドユーザの利用者であって認証機関でなく、また、証明書に記載された公開鍵に対応する秘密鍵を、認証機関であるかどうかを問わず、証明書（あるいは公開鍵を証明するその他の形式）または CRL に、デジタル署名をする目的で使用していないこと

利用規約には、追加の表明と保証を定めることができる。

9.6.4 依拠当事者の表明と保証

依拠当事者は、証明書中の情報につき依拠すべき範囲を決定するために必要十分な情報を受領していること、及び当該証明書中の情報について依拠するか否かを決定することに関しては依拠当事者のみが責任を負うこと、ならびに本 CPS に定める依拠当事者の義務の履行を怠った結果についての法的責任を依拠当事者が負うことを認識し確認する。

9.6.5 その他の参加者の表明と保証

規定しない。

9.7 保証の否認

適用される法律上許される範囲内において、利用規約及び依拠当事者規約は、GeoSure プロテクション・プランの規定とは関係なく、商品性及び特定目的への適合性を含むジオトラストのその他一切の保証を否認する。

9.8 責任の制限

適用される法律上許される範囲内において、利用規約及び依拠当事者規約は、GeoSure プロテクション・プランの規定とは関係なく、ジオトラストの責任を否認する。

利用者の責任の上限は、適用される利用規約の中に記載される。

エンタープライズ登録機関、適用される認証機関の責任の上限は、彼らの中で結ばれる契約中に記載される。

依拠当事者の責任の上限は、適用される依拠当事者規約の中に記載される。

9.9 補償

9.9.1 利用者による補償

適用される法律上許される範囲内において、利用者は以下の事項から発生する損害を、ジオトラストに補償するものとする。

- 利用者の証明書申請について利用者が虚偽または不実の表明を行った場合
- 利用者が証明書申請に関する重要な事実を開示することを怠った場合で、不実の表明または事実を開示しないことが懈怠または関係者を欺く意図をもってなされたとき
- 利用者が利用者の秘密鍵の保護、信頼すべきシステムの使用、またはその他利用者の秘密鍵の危殆化、喪失、開示、変更もしくは権限のない使用を防ぐために必要な措置をとることを怠った場合

- 利用者が第三者の知的財産権を侵害するような名称（Common Name、ドメイン・ネーム、電子メールアドレスを含むがこれらに限られない）を使用した場合

利用規約には、追加の補償義務を定めることができる。

9.9.2 依拠当事者による補償

適用される法律上許される範囲内において、依拠当事者は以下の事項から発生する損害を、ジオトラストに補償するものとする。

- 依拠当事者が依拠当事者としての義務の履行を怠った場合
- 依拠当事者による証明書の依拠が特定の状況下において合理的でない場合
- 依拠当事者が、依拠しようとする証明書につき、有効期間が満了し、または失効されているか否かを決定するために証明書のステータスを確認するのを怠った場合

9.10 有効期間と終了

9.10.1 有効期間

本 CPS は、ジオトラストのリポジトリに掲載されたときに有効となる。本 CPS の変更も、ジオトラストのリポジトリに掲載されたときに有効となる。

9.10.2 終了

本 CPS は、新たな CPS が効力を発するまで、有効とする。

9.10.3 終了の効果と効力の残存

本 CPS が終了した場合においても、ジオトラスト PKI 参加者は、発行した証明書の残存有効期間中は、本 CPS の条項に拘束されるものとする。

9.11 参加者の個別の通知と連絡

関係者間で別途合意のない限り、ジオトラスト PKI 参加者は、連絡事項の重要性と内容を考慮し、相互に連絡を取り合うために商業上合理的な方法をとるものとする。

9.12 改訂

9.12.1 改訂手続き

ジオトラストは予告なしに、本 CPS をいつでも変更できる。本 CPS 及び改訂版はすべて、<http://www.geotrust.com/resources> に掲載されている。本 CPS の改訂版であることは、改訂版が単に事務的なものである場合以外は、新しいバージョン番号と日付により証明される。

9.12.2 通知方法と期間

規定しない。

9.12.2.1 コメント期間

適用せず。

9.12.2.2 コメントの取扱

適用せず。

9.12.3 OID の変更が必要な場合

適用せず。

9.13 紛争の解決

9.13.1 ジオトラスト、アフィリエイト、カスタマ間の紛争

ジオトラスト PKI 参加者間の紛争は、関係当事者間に適用される契約に従い解決するものとする。

9.13.2 利用者または依頼当事者との紛争

本 CPS またはジオトラストが発行した証明書に起因、関係、または関連する紛争、論争、または請求は、米国仲裁協会（AAA：American Arbitration Association）の仲裁規則に従って仲裁され、最終的に解決するものとする。すべての仲裁手続は、米国カリフォルニア州サンタクララ郡で実施される。AAA に指名された仲裁人が1名いるものとし、紛争、論争、または請求に関与もしくは存在する問題について適度に熟知しているものとする。仲裁人の裁定は、すべての当事者に拘束力がある最終的なものであり、裁定に基づく判決は、それに関する適切な管轄権を有する裁判所によって提出できる。本 CPS、及びそれに定められている当事者の権利義務ならびにジオトラストが発行した証明書における権利義務は、すべて有効なままであり、仲裁手続きにおける結果と裁定は審理中となる。この定めに従って発生するすべての仲裁において、仲裁人が勝訴当事者は実際に負担した合理的な弁護士報酬を含む費用の全部または一部を受けると決定しない限り、各当事者は、仲裁手続きに関連して発生する各自の費用の責任を負うものとする。

9.14 準拠法

本 CPS ならびにジオトラストにより発行されたすべての証明書の執行力、解釈及び有効性については、米国カリフォルニア州の実体法に準拠するものとする。ただし、(i) 抵触法の条項、及び (ii) 国際物品売買契約に関する国際連合条約は除く。

9.15 法の遵守

本 CPS は、ソフトウェア、ハードウェア、技術情報の輸出入に関する制限を含む国内外の法律、法令、規則、命令に従う。

9.16 雑則

9.16.1 完全合意条項

適用せず。

9.16.2 譲渡

適用せず。

9.16.3 分離可能性

本 CPS のいずれかの条項が無効、違法、または失効不能であると判断された場合においても、それ以外の条項の有効性、適法性、及び執行力は、そのことにより一切影響を受けずまたは損なわれない。

9.16.4 強制執行（弁護士費用と権利放棄）

適用せず。

9.16.5 不可抗力

ジオトラストは、この定めに基づく義務の不履行または履行遅滞のうち、火災、洪水、地震、天災、戦争行為、テロリズム、暴動、市民暴動、反乱、革命（米国における）、ストライキ、工場閉鎖、労働争議、その他合理的にジオトラストの力の及ばない類似の事由によるものについては、その責任を負わないものとする。

9.17 その他の条項

適用せず。

Appendix A. 略語・定義表

略語

Term	Definition
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce
CA	Certificate Authority
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
EV	Extended Validation
FIPS	United State Federal Information Processing Standards
ICC	International Chamber of Commerce
KRB	Key Recovery Block
LSVA	Logical security vulnerability assessment
OCSP	Online Certificate Status Protocol
PCA	Primary Certification Authority
PIN	Personal identification number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
RFC	Request for comment
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants)
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Sockets Layer

定義

Term	Definition
Administrator 管理者	検証その他認証機関または登録機関の役割を果たす、組織内で信頼される者。
Administrator Certificate 管理者証明書	管理者に発行される証明書で、認証機関または登録機関としての機能を果たすためにのみ利用される。
Affiliate アフィリエイト	技術、通信または金融サービス等の事業における、一流の信頼される第三者で、ある特定の地域においてサービスを提供するためにジオトラストと契約を締結している者。
Applicant 申請者	サブジェクトとして名称を付けて EV SSL 証明書を申請する（またはリニューアルを行う）民間組織または行政機関。
Applicant Representative 申請担当者	EV SSL 証明書の申請者によって雇用されている個人であり、(i) 申請者の代理で EV SSL 証明書申請の署名及び提出を行う者、または (ii) 申請者の代理で利用規約の署名及び提出を行う者。
Application Software Vendor アプリケーションソフトウェアベンダ	証明書を表示または使用し、ルート証明書を配布するインターネット・ブラウザ・ソフトウェアまたはその他のソフトウェアの開発業者。KDE、Microsoft Corporation、Mozilla Corporation、Opera Software ASA、Red Hat, Inc など。
Certificate 証明書	少なくとも、認証機関の名称を記載しまたは認証機関を識別し、利用者を識別し、利用者の公開鍵を含み、証明書の運用期間を識別し、証明書のシリアル・ナンバーを含み、これに認証機関がデジタル署名したメッセージ。
Certificate Applicant 証明書申請者	認証機関に対して証明書の発行を要求する個人または組織。
Certificate Application 証明書申請	証明書申請者（または証明書申請者から授権された代理人）から認証機関に対して証明書の発行を求める要求。
Certificate Approver 証明書承認者	証明書承認者は、(i)証明書要求者として行動するとともに他の従業員または第三者に証明書要求者として行動する権限を付与し、(ii)他の証明書要求者が提出した証明書要求を承認する、申請者に雇われた自然人または EV SSL 証明書の申請者の代理を務める明示的な権限を有する代理人である。
Certificate Chain 証明書チェーン	利用者及び認証機関の証明書を含む、一連の証明書リストのことで、ルート証明書で終了する。
Certificate Management Control Objectives 証明書管理の制御目標	準拠性監査に対応するために、エンティティが満たさなければならない基準。
Certificate Requester 証明書要求者	証明書要求者は、申請者に雇われ授権された自然人、申請者の代理を務める明示的な権限を有する代理人、または申請者の代理で EV SSL 証明書要求を作成、提出する第三者（ISP、ホスティング会社など）である。
Certificate Revocation List (CRL) 証明書失効リスト	CP セクション 3.4 に基づき有効期間満了前に効力を失効された証明書を特定する目的で、認証機関によってデジタル署名された定期的または緊急に発行されるリスト。このリストは、一般的に CRL 発行者の名前、発効日、次回 CRL 発行予定日、効力を失効された証明書のシリアル・ナンバー及びその具体的時期及び理由を示す。
Certificate Signing Request 証明書署名要求	証明書を発行させるための要求を伝達するメッセージ。
Certification Authority (CA) 認証機関	証明書の発行、管理、失効及び更新を授権されたエンティティ。
Certification Practice Statement (CPS) 認証業務運用規程	ジオトラストまたはアフィリエイトが証明書申請の承認または拒絶、ならびに証明書の発行、管理及び失効をする際に採用する運用手続を規定した文書。

Term	Definition
Challenge Phrase チャレンジフレーズ	証明書申請の際に、証明書申請者が選ぶ秘密のフレーズ。証明書申請者が証明書を発行すると、証明書申請者は利用者になり、認証機関または登録機関は利用者がその証明書を失効または更新を求めるとき、利用者を認証するためにチャレンジフレーズを利用する。
Class	各 class の保障は CP セクション 1.1.1 に記述されている。
Code Confirmation Certificate コード確認証明書	発行元からのコード確認の要望に応じて、ジオトラストが、関連付けられた秘密鍵を使用して、発行元証明書の秘密鍵により電子署名された申請フォームのコードを電子的に再署名できるようにするために、ジオトラストによって発行される証明書。
Compromise 危殆化	セキュリティ・ポリシーの違反またはその疑いのある行為で、機密情報の無権限の開示または管理の喪失が生じかねないこと。秘密鍵に関する危殆化は、紛失、盗難、開示、改変、無断使用または当該秘密鍵のセキュリティのその他の危殆化を意味する。
Confidential/Private Information 秘密情報	CP セクション 2.8.1 に従い秘密にすることを要求される情報。
Contract Signer 契約署名者	EV SSL 証明書の申請者の代理で利用規約に署名する、申請者に雇われた自然人、または申請者から授権された代理人。
Country 国	国とは本ガイドランでは、独立国であると定義する。
CRL Usage Agreement CRL 利用規約	CRL または情報を使用するための諸条件を規定する規約。
Demand Deposit Account 要求払預金口座	銀行またはその他の金融機関で、要求に応じて支払い可能な資金が預けられる預金口座。要求払預金口座の主な目的は、小切手、銀行為替手形、自動引き落とし、電子送金などによって現金不要の支払いを容易にすることである。使用方法は国によって異なるが、要求払預金口座は当座預金口座 (checking account)、シェアドラフト勘定 (share draft account)、当座預金 (current account) として一般に知られている。
EV Certificate EV SSL 証明書	EV ガイドラインに記載ある事項を含むデジタル証明書は、そのガイドラインに従い認証される。
EV OID	EV SSL 証明書の certificatePolicies フィールドに含まれる object identifier と呼ばれる識別番号は、(i) 証明書に関連する認証機関ポリシー・ステートメントを示し、(ii) 1 社以上のアプリケーションソフトウェアベンダとの事前合意により、EV SSL 証明書であることが証明書でわかるようにする。
Exigent Audit/Investigation 緊急監査または調査	ジオトラスト認証機関の基準に従うことに関するあるエンティティの怠慢、当該エンティティに関連する事故または危殆化、または当該エンティティが起こしたことによりもたらされるジオトラスト認証機関のセキュリティについての現実または可能性のある脅威を理由としてジオトラストが行う監査または調査。
Extended Validation	主要な認証機関及びブラウザ・ベンダで構成されるフォーラムによって発行された EV SSL 証明書のガイドラインで定められている検証手続き。
Intellectual Property Rights 知的財産権	著作権、特許権、企業秘密、商標及びその他の知的財産権に基づく権利。
Intermediate Certification Authority (Intermediate CA) 中間認証機関	エンドユーザ証明書の証明書チェーン内に証明書がある認証機関。
International Organization 国際機関	国際組織とは制定文書により設立された組織。制定文書とは 2 つ以上の独立国政府またはその代行者によって署名されている憲章、条約、協定または同等の文書である。
Key Generation Ceremony	認証機関または登録機関のキー・ペアが生成され、その秘密鍵が暗号モジュールへ移転され、その秘密鍵の予備がとられ、その公開鍵が認証される手続き。

Term	Definition
キー・ジェネレーション・セレモニ	
Nonverified Subscriber Information 確認を実施しない利用者情報	証明書申請者から認証機関または登録機関に対し送信された情報で、証明書に含まれるが、当該認証機関または登録機関により確認されていない情報。当該認証機関及び登録機関は当該情報が証明書申請者から送信されたものであるという事実以外には何らの保証も行わない。
Non-repudiation 否認防止	通信の発信者についての不当な否認、送信したことの否認、もしくは到達の否認に対する保護を与える通信の属性。発信者の否認には、過去に通信したことのある相手（その者を知らない場合でも）からのメッセージの否認を含む。注意：最終的には、裁判所による裁定、仲裁または他の裁決機関のみが、否認を否定するものである。たとえば、ジオトラスト証明書を引用するデジタル署名は、裁判所による否認を否定する判断のための証拠を提供するものであるが、デジタル署名自体が否認を否定するものではない。
Offline CA オフライン認証機関	ネットワークを利用する侵入者による攻撃から保護するために、セキュリティ上の理由からオフラインで維持されるジオトラスト第一次認証機関、ルート認証機関、その他指定の中間認証機関。これらの認証機関は、利用者証明書への署名は直接行わない。
Online CA オンライン認証機関	継続的な署名サービスを提供するために、オンラインで維持され、利用者証明書への署名を行う認証機関。
Online Certificate Status Protocol (OCSP)	依頼当事者に対しリアルタイムの証明書ステータス情報を提供するプロトコル。
Operational Period 運用期間	証明書が発行された日時（証明書にそれより後の日時の記載がある場合には当該記載された日時による）に始まり、当該証明書の効力が終了する日時（それ以前に失効された場合には当該失効の日時による）に終了する期間。
Parent Company 親会社	親会社とは、子会社の過半数を所有する会社であって、QIIS または登録されている Chartered Professional Accountant (CPA) か米国外では同様の組織によって提供された財務報告によって確認されたもの。
PKCS #10	RSA Security Inc. により開発された公開鍵暗号基準 (Public-Key Cryptography Standard) #10 で、証明書署名要求の構造について定義する。
PKCS #12	RSA Security Inc. により開発された公開鍵暗号基準 (Public-Key Cryptography Standard) #12 で、秘密鍵受渡のための安全な方法について定義する。
Primary Certification Authority (PCA) 第一次認証機関	ある特定の Class の証明書に対するルート認証機関として行動する認証機関で、下位の認証機関に対して証明書を発行する。
Principal Individual(s)	雇用者、従業員、関連会社、代理人から事業の実行者であると認識されている、民間組織、行政機関、個人事業主の個人のオーナー、パートナー、経営陣、重役、役員である個人の EV SSL 証明書の要求、発行、使用。
Public Key Infrastructure 公開鍵インフラストラクチャ	証明書を基盤とする公開鍵暗号システムの実施及び運用を総体的に成立させるアーキテクチャー、組織、技術、実務及び手続のこと。
Registration Agency	政府機関が登録したエンティティのビジネス形態、ライセンス、代理店、その他承認されたビジネスとして実する許可に関連した企業情報。以下のものに制限されない。(i)国営企業;(ii) 政府認可の企業(iii) 特定企業
Registration Authority(RA) 登録機関	認証機関から承認されたエンティティであって、証明書申請に際し証明書申請者を支援し、証明書申請に関し承認または拒絶し、証明書の失効または証明書の更新を行う。

Term	Definition
Regulated Financial Institution 規制された金融機関	金融機関の組織化及び認可について定めている、政府、国、都道府県、または地域の法律に基づいて、金融機関の行政権限を持つ政府、国、都道府県、または地域の機関によって規制、監督、調査されている金融機関。
Relying Party 依拠当事者	証明書またはデジタル署名に依拠して行為する個人または組織。
Relying Party Agreement 依拠当事者規約	認証機関により使用される規約で、個人または組織が依拠当事者として行動するための諸条件を規定する。
Reseller リセラー	特定の市場に対し、ジオトラストに代わり、サービスを販売するエンティティ。
RSA	Rivest、Shamir、Adelman によって発明された公開鍵暗号方式。
RSA Secure Server Certification Authority (RSA Secure Server CA) RSA セキュア・サーバ認証機関	セキュア・サーバ ID を発行する認証機関
RSA Secure Server Hierarchy RSA セキュア・サーバ階層	RSA セキュア・サーバ認証機関から構成される PKI 階層。
Secret Share シークレット・シェア	シークレット・シェアリング契約に基づく、認証機関の鍵の一部分または認証機関の秘密鍵を運用するために必要な起動データの一部。
Secret Sharing シークレット・シェアリング	認証機関の秘密鍵または認証機関の秘密鍵を運用するための起動データを分割する実務で、CP セクション 6.2.2 に定める認証機関の秘密鍵の運用を複数人の管理下におくためになされる。
Secure Server ID セキュア・サーバ ID	ウェブ・ブラウザとウェブ・サーバ間の SSL セッションをサポートするために用いられる Class 3 組織向け証明書。
Secure Sockets Layer (SSL) セキュア・ソケット・レイヤ	Netscape Communications Corporation によって開発されたウェブ通信を保護するための業界標準方法。SSL セキュリティ・プロトコルはデータの暗号化、サーバ認証、メッセージの完全性及びオプションとしてクライアント認証を提供する。
Sovereign State 独立国	独立国は州または国であり、独自の政府によって統治されていて、他の権力による従属、属国状態でないもの。
Subject	公開鍵に対応する秘密鍵の保有者。Subject という用語は、組織向け証明書の場合には、秘密鍵を保有する装置またはデバイスを指すこともある。Subject は、当該 Subject の証明書中に含まれる公開鍵と結合した明確な名称が割り当てられる。
Subscriber 利用者	利用者証明書の場合には、証明書が発行され、その Subject となっている人物をいう。組織向け証明書の場合には、証明書が発行され、その Subject となっている装置またはデバイスを所有する組織を言う。利用者は、証明書中に記載された公開鍵に対応する秘密鍵を利用することができ、また、利用する権限がある。
Subscriber Agreement 利用規約	認証機関または登録機関により利用される規約で、個人または組織が利用者として行動するための諸条件を規定する。
Subsidiary Company 子会社	子会社とは、申請者がすべてを所有する会社であって、QIIS が登録されている Chartered Professional Accountant(CPA)が米国外では同様の組織によって提供された財務報告書によって確認されたもの。
Symantec シマンテック	本 CPS の各関連部分について、記載されている特定の操作の責任を負うシマンテック・コーポレーションまたはシマンテックの完全子会社を意味する。
Trusted Person 信頼される者	ジオトラスト内のエンティティの従業員、独立請負業者またはコンサルタントで、当該エンティティ、その製品、サービス、施設または実務に関する基盤となる信頼性を管理する責を負う者。CP セクション 5.2.1 においてより詳細に規定される。

Term	Definition
Trusted Position 信頼される地位	ジオトラストにおける地位で、信頼される者がその任につくことを要する。
Trustworthy System 信頼すべきシステム	侵入、誤用から合理的に保護され、合理的レベルの可用性、信頼性及び操作の正確性を備え、意図する機能を合理的な程度に満たし、かつ、該当するセキュリティ・ポリシーを実施するコンピュータ・ハードウェア、ソフトウェア及び手続き。米国政府が定めた用語体系中の「信頼されるシステム (Trusted system)」とは必ずしも一致しない。