1. はじめに

スターフィールド・テクノロジーズ LLC（以下、SF という言う）はインターネット基盤サービス分野におけるイノベーターであり、オンライン上での実在性の確立と電子商取引に欠かすことの出来ない先進的ソフトウェアとインターネットソリューションを提供する。

スターフィールド公開鍵基盤（以下、SF PKI と言う）は各種電子証明書を提供する為に設立された。

1.1 概略

この証明書手引及び認証業務規程（以下、CP/CPS と言う）は、SF PKI の実務につき説明し、SF PKI の階層構造に属する全ての認証機関（以下、CA と言う）に適用される。本 CP/CPS は SF PKI と関係を持つ全ての組織に適用され、そこには方針管理機関（以下、PA と言う）、CA、登録機関（以下、RA と言う）、証明書利用者（以下、利用者と言う）、そして依存当事者を含む。

1.2 本 CP/CPS の位置付けと翻訳

本 CP/CPS は公式には「スターフィールド・テクノロジーズ証明書手引及び認証業務運用規程」と参照される。　SF CA は本 CP/CPS の方針及び実務要求に従い証明書の発行を行う。

尚、本書は、本 CP/CPS の英文原本を和訳したものであるが、原本との間に実効性に欠く解釈が認められた場合、原則として原本が優先して適用される。　同原本最新版は以下 URL の SF のリポジトリにおいて本 CP/CPS 8 条に即し公開される。
https://certs.secureserver.net/repository/

1.3 関係者及び証明書の利用

1.3.1 認証機関（CA）

SF CA は以下記載の機能を有する

- 証明書の生成及び署名
- 利用者及び依存当事者への証明書の配布
- 証明書の失効
- 証明書失効リスト（以下、CRL と言う）或いはその他の方法による証明書のステータス情報の提供
- 証明書や証明書のステータス情報を保管し閲覧可能にするリポジトリの提供

SF PKI においては 2 種の CA、即ち Root CA と Issuing CA の 2 種であり、現在 SF PKI

の階層構造には以下英語版 CP/CPS Page2-3 に記載の CA が存在する。
https://certs.secureserver.net/repository

1.3.2 登録機関（RA）

RA は利用者による証明書管理取扱い（新規申請、更新や秘密鍵再発行、失効申請を含む）を評価し、その承認乃至は拒絶を行う。
SF は、SF PKI における唯一の RA となる。

SF Root CA においては、利用者及び中間認証機関（以下、中間 CA と言う）は SF の支配下にあり、従って、中間 CA に対する RA 機能は権限ある SF PKI の従業員により手動にて行われる。

SF Issuing CA においては、RA 機能は自動及び手動の混成された手続きにて SF によって行われる。

1.3.3 エンド・エンティティ

エンド・エンティティとは利用者及び依存当事者を含む。

SF Root CA においては、利用者とは中間 CA を含む。
SF Issuing CA においては、利用者とは通常は組織及び個人である。

依存当事者とは、ウェブサイトやデータ暗号化サービス、署名検証サービス、ユーザ認証サービスを提供している組織や個人の身元を判断する為に SF 証明書を信頼するあらゆる主体を言う。

1.3.4 証明書の利用

本 CP/CPS は SF PKI における SF CA により発行された全ての証明書に適用される。
本 CP/CPS は証明書が利用される関係者の特定の階層やタイプ、当該証明書の発行及び管理を行うための実務及び要求、当該証明書の意図された目的と利用方法を定義する。

1.4 連絡先

本 CP/CPS は SF PKI Policy Committee によって米国にて管理運用されており、その連絡先は以下の通り。

Starfield Technologies, LLC

14455 N. Hayden Road, Suite219
Scottsdale, AZ 85260, USA
Phone: +1-480-505-8800
Fax: +1-480-505-8865
E-mail: practices@starfieldtech.com

SF PKI Policy Committee は同社の経営陣、セキュリティ、PKI 事業部、法務部から構成されている。

2 一般条項

2.1 義務

2.1.1 SF PKI Governance & Policy Authority Committee（以下、GPAC と言う）の義務

GPAC の義務は以下の通り。

- 本 CP/CPS の承認及び運用
- 本 CP/CPS の運用解釈
- PKI 証明書の記載事項の特定
- 本 CP/CPS に関わる議論、紛争の解決
- セキュリティの脅威に関する最新知識の保持及び重大なるセキュリティ上の脅威への対抗策の実施

2.1.2 CA の義務

SF PKI における CA の義務は以下の通り。

- PKI 証明書の生成、発行、配布
- CA 証明証の配布
- 証明証ステータス情報の作成及び公開（CRL 等による）
- 証明書発行及び CRL 署名機能のセキュリティ、可用性、継続性の維持
- 利用者への証明書失効手段の提供
- 公開鍵の失効
- 本 CP/CPS への準拠状況の内部監査および外部監査の定期実施

2.1.3 リポジトリに関する義務

リポジトリサービス提供時の SF の義務は以下の通り。

- 公開鍵の保管及び配布（妥当な場合に限る）
- 証明書ステータス情報の保管及び配布（CRL 或いはその他オンライン情報）

・ 本 CP/CPS 及びその改訂版の保管及び配布
・ 依存当事者約款及び SSL 証明者サービス利用約款の保管及び配布

2.1.4 RA の義務

SF PKI における RA の義務は以下の通り。

・ 加入者からの公開鍵の取得
・ 本 CP/CPS に即した利用者の身元確認と認証
・ 利用者が確かに証明書生成に利用した公開鍵に相対する非対称秘密鍵を保持していることを検証すること
・ 認証された証明書失効要求の受領
・ RA 機能を担う人材への訓練の実施

2.1.5 利用者の義務

SF PKI における利用者の義務は以下の通り。

・ 一対或いは複数の対の非対称鍵の生成
・ 生成した公開鍵と登録情報を裏付ける証明書類等の提出
・ SF に対し利用者の証明書に記載されることになる情報や身元情報或いは認証情報の正確性と完全性に対する保証
・ 秘密鍵の危殆化を防ぐ手段を講ずること
・ 秘密鍵危殆化或いは証明書記載情報の誤りに関する迅速なる報告
・ 本 CP/CPS に即した鍵ペアの利用

2.1.6 依存当事者の義務

SF PKI における依存当事者の義務は以下の通り。

・ 利用者の PKI 証明書の有効期限を確認すること
・ 利用者が確かに証明書生成に利用した公開鍵に相対する非対称秘密鍵を保持していることを検証すること
・ 本 CP/CPS に即した利用者証明書の公開鍵の利用

2.2 責任

2.2.1 保証とその制限

SF PKI における、SF やその販売代理人或いはそれぞれの顧客との間の保証、保証の拒絶、責任の上限については、それぞれの間で締結される契約により規定され管理されるが、本条は SF CA が証明書を発行した最終利用者及びその依存当事者に対する SF CA による保証、保証の拒絶、責任の上限のみを対象とする。

SF 及び（必要があれば）その販売代理人は、本 CP/CPS に即し利用約款及び依存当事者約款を用意する。　当事者が販売代理人である場合、利用約款は SF により課される要求事項を満足するものでなければならない。　利用約款は保証、保証の拒絶、責任の上限を規定しなければならないとする要求事項については、販売代理人が利用する利用約款にも適用される。　SF は自らと利用者との利用約款において当該要求事項に合意する。　SF による保証、保証の拒絶、責任の上限に関する実務は SF と依存当事者との依存当事者約款にも適用される。

証明書発行申請者、利用者及び依存当事者は、SF 証明書及び CRL 等の SF 証明書アプリケーションサービスは、通信基盤（インターネット、電話、通信回線及びネットワーク、サーバ、ファイアーウォール、プロキシ、ルーター、スウィッチ、ブリッジ等通信機器を含むがそれらに限られない）上での情報交換に依存していること、そしてこうした通信機器は SF や SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）の管理下にはないことを、認識し合意している。　即ち、SF や SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）は、その原因が通信機器によるものである限り、SF 証明書や CRL 等の SF 証明書アプリケーションサービスに関するエラー、遅れ、中断、欠損或いは破壊につき一切責任を有さない。

2.2.1.1 SF CA による利用者及び依存当事者に対する保証

- SF はその合理的な技術と配慮をもって証明書サービスを提供することを保証する。
- SF はその知り得る限りにおいて、証明書発行申請を承認し或いは証明書を発行した主体が起源となっているか、或いは知り得た証明書記載事項に重大な虚偽表示がないことを保証する
- SF は、証明書記載情報に証明書発行申請の承認を行い或いは証明書を発行する過程において合理的配慮を欠いたことによる誤りがないことを保証する
- SF は SF 証明書が本 CP/CPS の重大な要求事項の全てを満足していることを保証する
- SF は証明書サービスや失効サービス或いはリポジトリサービスが本 CSP の重大なる要求事項を満足していることを保証する

2.2.1.2 損失の制限

SF やSF CA の管理下にてRA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）による、証明書発行申請者、利用者、及び依存当事者、或いはあらゆるその他の個人、主体、組織に対する、あらゆる SF 証明書サービス（その他あらゆる SF 証明書の利用及び同証明書への依存を含むがその限りではない）に起因する責任の総額は、スタンダードSSL では100,000US ドルを、デラックスSSL では250,000US ドルを、EV SSL では1,000,000US ドルを超えない。本上限は、SF 証明書サービスに起因する取引や要因の数に関わりなく、SF 証明書一枚当たり（証明書それぞれに固有のシリアル番号等証明書詳細情報により特定される一枚、とする）の上限として適用される。　本上限は一切の責任に適用され、根本的違反を含む契約不履行に基づくもの、不注意を含む不法行為によるもの、立法や責任法理によるもの（直接間接損害、特別損害、法的損害、懲罰的損害、警告、偶発的損害等を含むがそれらに限られない）等その根拠を問わない。

SF やSF CA の管理下にてRA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）による、証明書発行申請者、利用者、及び依存当事者、或いはあらゆる個人、主体、組織に対する、あらゆる SF 証明書サービス（その他あらゆる SF 証明書の利用及び同証明書への依存を含むがその限りではない）或いは SF 証明書や同記載情報が第三者の個人、主体或いは組織（その法的管轄区域を問わない）の特許、商標、著作権、商業機密或いはその他一切の知的財産権を侵害、不正流用、希釈化、不正競合或いは妨害しているとの申し立てに起因する、あらゆる損失、費用、債務、損害、補償、示談金等（を含むがそれに限られない）につき一切責任を有さない。

あらゆるSF 証明書サービス（その他あらゆるSF 証明書の利用及び同証明書への依存を含むがその限りではない）に起因する債務の累積合計額が本条に定める上限を上回った場合、司法による別途の裁定の無い限り、当該上限額のうち未消化（引当）分は妥結し確定した債務から順に割当てられる。　SF やSF CA の管理下にてRA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）は、補償請求者間での配分に関わらず、本条に定める責任の上限を越えて支払う義務は一切ない。

SF やSF CA の管理下にてRA 業務を行う第三者オペレータ、またはその販売代理人、

共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）は、偶発損害、特別損害、法的損害、懲罰的損害、警告、依存、間接損害等（その他、ビジネス上の損失や機会消失、暖簾の消失、利益損失、ビジネス中断、情報消失、貯蓄損失、その他金銭的損失を含むがそれに限られない）に関し、根本的違反を含む契約不履行に基づくもの、不注意を含む不法行為によるもの、立法や責任法理によるもの等その根拠を問わず、一切責任を有さない。　本上限は、本 CP/CPS に定める一切の救済策が失敗しようとも、また譬え SF や SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）がそうした損害の起こり得る可能性につき事前に知り得たとしても、本条に従い適用される。

ある司法当局が間接損害や偶発損害に関わる責任の免除や上限を認めないとの判断を行った場合の、本上限が特定の証明書発行申請者、利用者、依存当事者、或いはその他個人、主体や組織に対し適用されない可能性については、表明や保証、そして条件の拒絶、或いは本 CP/CPS に規定される責任の上限はいずれも、SF CPS や利用者契約、依存当事者約款の必須要件を構成するものであり、証明書発行申請者、利用者、依存当事者、或いはその他個人、主体や組織が、表明や保証、そして条件の拒絶、或いは本 CP/CPS に規定される責任の上限を契約上排除したまま、SF が利用者に SF 証明書を発行することは有り得ないこと、SF や SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）が SF 証明書に関わる何らかのサービスを提供することもないこと、そして本条は合理的なリスク配分を定めたものであることを、認めている。

加えて、SF は以下の如何なる損失に対しても責任を有さない。

- 戦争や自然災害、その他不可抗力による CA 或いは RA サービスに関わるもの
- 証明書を失効してからその直後に CRL が発行される時点との間で発生するもの
- SF PKI 証明書の権限外の利用、或いは本 CP/CPS に定めのない処方に起因するもの
- SF PKI 証明書或いは CRL の過失或いは不正利用に起因するもの
- SF PKI 証明書記載の個人情報の開示に起因するもの

2.2.1.3 有害な行為

SF 証明書及び SF により提供される SF 証明書に関わるサービスは、有害な行為に利用される為に設計、生成或いは意図されたものではなく、原子力施設や航空機、通

信システムや航空管制、医療機器やその他人命に直結する機械の安全装置として設計、生成或いは意図されたものでもない。 SF や SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）はそうした利用に関わる表明、保証や条件については、それが明確であろうがなかろうが、法定によるもの或いは商習慣に即したものであろうと、その一切の提供を拒絶する。

2.2.1.4 その他

SF や SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）は、以下の場合においては、SF 証明書或いは SF 証明書に関わるサービスの利用に起因するあらゆる損失、費用、債務、損害、補償、示談金等（を含むがそれに限られない）については、証明書発行申請者、利用者、依存当事者、或いはその他個人、主体や組織のいずれに対しても一切の責任を有さない。

(i) SF 証明書が利用者或いはその他の個人、主体或いは組織の過失、不当表明或いはその他不作為の結果として発行された場合

(ii) SF 証明書が期限切れ、或いは失効された場合

(iii) SF 証明書が修正或いは訂正された場合

(iv) 利用者が SF 証明書記載情報に変更があった後、或いは同情報が誤解を生む乃至は不正確であることが明らかになった後も証明書の利用を停止しなかった場合

(v) 利用者による本 CP/CPS 或いは利用約款の不履行があった場合、或いは依存当事者による本 CP/CPS 或いは依存当事者約款の不履行があった場合

(vi) SF 証明書に相対する秘密鍵が危殆化した場合

(vii) SF 証明書が本 CP/CPS に反する利用が成された場合、或いは法令に反して利用された場合

2.2.2 保証の拒絶

SF や SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）は、2.2.1.1 に定める責任の上限を除くその他一切の保証については、それが明確であろうとなかろうと（市場性や何らかの特定の目的への適合性、権利不侵害、所有権に関するものや、法定或いは商習慣に関するものを含むがそれらに限られない）、何ら表明をせず、それを明確に拒絶する。

SF は、SF 証明書サービスが何らかの期待に沿うものであること、同サービスが中断せず、適時に、安全に、過失無く提供されること、或いは欠陥があっても是正されることを、何ら保証しない。　SF は、SF が提供する全てのサービスの利用とその結果において、正確性、精度、信頼性等何らかのものを保証せず、表明しない。

2.2.3　利用者の義務

2.2.3.1 利用者の保証

利用者は利用約款により以下を保証しなければならない。

- 全てのデジタル署名は利用者が保有する証明書に記載された公開鍵に相対する秘密鍵を利用して生成されていること、そして証明書が承認され機能していること（デジタル署名が生成された時点で証明書が期限切れとなっておらず失効されていないこと）
- 権限無い如何なる人物も秘密鍵にアクセスしていないこと
- 証明書発行申請時に利用者により成された一切の表明が真実であること
- 利用者による証明書記載情報が真実であること
- 証明書は本 CP/CPS に即し権限ある合法的事由の為に利用されていること
- 利用者は CA ではなく証明書の利用者であり、証明書に記載の公開鍵に相対する秘密鍵を証明書（或いは認証された公開鍵のその他フォーマット）や CRL、CA その他にデジタル署名する目的で利用していないこと
- 利用者は第三者の権利を侵害する方法で証明書サービスを利用していないこと
- 利用者はエンドユーザーの同意なくダウンロードされるスパイウェアや悪意あるソフトウェアを含む、敵意あるコードにデジタル署名するのにコードサイン証明書を利用していないこと

2.2.3.2 秘密鍵の危殆化

利用約款は、もし利用者が PKI 要求事項に反する行いをし、そして秘密鍵が危殆化した場合、それに起因する一切の損失や障害の責任は利用者にあることを定めている。

2.3　財務的責任

利用者と依存当事者は、利用者や依存当事者が当事者たる取引や SF 証明書や SF 証明書に関わるサービスを利用する取引における、利用者、依存当事者、或いはその他個人、主体や組織が被る財務的結果に対し責任を有する。　SF は、SF 証明書や SF 証明書に関わるサービスを利用することで完結する如何なる取引の財務的実効性につき何ら表明せず、何ら保証或いは条件を提供しない。　SF や SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コン

トラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）は、SF 証明書や SF 証明書に関わるサービスを利用或いは信頼に資する目的に沿い本 CP/CPS に明確に定められた事項を除く一切に何ら責任を有さない。

2.3.1　利用者及び依存当事者による補償

2.3.1.1 利用者による補償

利用約款は、利用者に対し、法の範囲内において、SF 及び SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）に対し、依存当事者による SF 証明書や SF 証明書に関わるサービスの以下事例に類する利用或いは依存に起因する、一切の損失、費用、債務、損害、補償、示談金（合理的代理人費用、訴訟費用や専門家手数料を含む）等を補償するよう求める。

- 利用者による、証明書発行申請内容の誤記入、省略或いは不当表明
- 利用者による、SF 証明書記載情報の変更
- 利用者による、本 CP/CPS、利用約款、依存当事者約款或いは法令で認める範囲を逸脱した SF 証明書の利用
- 利用者による、秘密鍵の管理不備、或いは秘密鍵の危殆化や損失、漏洩や変更、権限外の利用を回避する為の予防措置の不首尾
- 利用者による、第三者の知的財産権を侵害する名義（Common Name や Domain Name 或いは e-mail address を含む）の利用

2.3.1.2 依存当事者による補償

利用約款及び依存当事者約款は、依存当事者に対し、法の範囲内において、SF 及び SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）に対し、依存当事者による SF 証明書や SF 証明書に関わるサービスの以下事例に類する利用或いは依存に起因する、一切の損失、費用、債務、損害、補償、示談金（合理的代理人費用、訴訟費用や専門家手数料を含む）等を補償するよう求める。

- 依存当事者による、依存当事者の履行義務違反
- 依存当事者により SF 証明書の適切な認証が成されない場合
- 依存当事者による、本 CP/CPS、利用約款、依存当事者約款或いは法令で認める範囲を逸脱した SF 証明書の利用
- 依存当事者により SF 証明書に依存する諸環境に対する合理的判断が成されない場合

・ 依存当事者により不適切な環境下で SF 証明書に依存した場合
・ 依存当事者により SF 証明書の有効期限或いは失効状況の確認が成されない場合

2.3.2 信頼関係

SF は、利用者或いは依存当事者の代理人ではなく、受託者、管財人或いはその他の代表者でもない。 利用約款や依存当事者約款は、法の範囲において、SF や SF CA の管理下にて RA 業務を行う第三者オペレータ、またはその販売代理人、共同販促パートナー、その他コントラクター、代理人、サプライヤー或いはそれらの役職員（を含むがそれに限られない）と、利用者或いは依存当事者との間の一切の信頼関係を拒絶する。

2.4 解釈及び実施

2.4.1 準拠法

本 CP/CPS の実効性、構成、解釈及び有効性は、その一切は米国アリゾナ州法に準拠し、同準拠法に認められる制限には従うが、その他契約や法の選択には一切影響を受けない。 同準拠法は、SF PKI 利用者の国籍に関わらず、利用者に統一された手続きと解釈を提供する。

同準拠法は本 CP/CPS にのみ適用されるが、何らかの契約に本 CP/CPS が参照された場合でも同契約が独自の準拠法を持ち得ることは認めるとしても、参照された CP/CPS 内容の実効性、構成、解釈或いは有効性については、同契約のその他の条文とは切り離して本 CP/CPS 2.4.1 条に準拠するものとし、同準拠法に認められる制限に従うものとする。

ソフトウェアやハードウェア或いは技術情報の輸出入に関わる一切の法規（国内外の法律、規制、政令その他一切の命令）は本 CP/CPS に適用される。

2.4.2 可分性、存続性、統合、通知

本 CP/CPS は本 CP/CPS に関わる全ての当事者の継承者を拘束する。

仮に本 CP/CPS の何らかの条項に実効性のないことが明らかになった場合、残りの条項は当事者の合理的意図を最大限実現するべく解釈される。 本 CP/CPS においては、全ての条項が、責任の上限や損害の排除、保証の拒絶や上限、約束やその他の義務を定めていることを、また全ての条項にその他一切の条項に対する可分性と独立性が確保されていることまたそのように実施されるべきであることを、明確に合意されている。

本 CP/CPS は、諸環境に鑑み誠実なる商業合理性が担保されているか、そしてその国際的広がり及び統一されたアプリケーションに即し解釈される。　本 CP/CPS の何らかの条項の実施に過失があった場合でも、それを持ってその他全ての条項の実施に過失があったとは見做されない。

本 CP/CPS に関わる通知、要求、要望については、本 CP/CPS に即し電子メールにて行うか、或いは筆記で行うものとする。　電磁的通信においては、意図された受領者がメッセージを受け取った時点で有効となるものとする。

2.4.3　争議解決手続き

本 CP/CPS に関わるサービスや条項に関する一切の論議或いは紛争については、法的侵害を受けた当事者が SF の経営層にその仔細につき連絡する。　SF 経営陣は適切なる SF 従業員を持ってその解決に当たらせる。

2.5　対価

2.5.1　証明書発行対価及び更新手数料

SF は、最終利用者に対し証明書発行、管理、更新の手数料を課する。

2.5.2　証明書閲覧手数料

SF は、SF 証明書をリポジトリ或いはその他妥当な手段にて閲覧可能な状態に置く為の手数料を課する権利を留保する。

2.5.3　証明書ステータス情報閲覧手数料、証明書失効手数料

SF は、本 CP/CPS 4.4.9 条に即しリポジトリ内で、或いは依存当事者に対して、CRL を閲覧可能とする為の手数料は課さない。　但し、SF は、顧客別 CRL や OCSP サービス、或いはその他の付加価値 CRL サービスの提供については、手数料を課す権利を留保する。　SF は、SF の事前の書面による承諾を得ずに SF 証明書ステータス情報を利用する製品やサービスを提供する第三者による、SF が提供する証明書ステータス情報や CRL、時刻認証の閲覧は認めない。

2.5.4　その他サービスに対する手数料

SF は、本 CP/CPS の閲覧に対しては手数料を課さない。　但し、本 CP/CPS の閲覧以外の目的、例えば複製、再配布、修正或いは派生ドキュメントの作成等（を含むがそれらに限られない）を意図した、その他一切の利用は著作権を有する SF との契約を必要とする。

2.5.5 返金制度

SF は、証明書の発行及びその管理に関する厳格な実務と方針を維持、運用している。如何なる理由であれ利用者が利用者に発行された証明書に満足出来ない場合、利用者は発行後 30 日以内に証明書の失効を SF に要求することが出来、証明書発行対価（但し、銀行諸掛等諸費用控除後の）の返金を受けることが出来る。　発行後 31 日以降において利用者が SF に証明書の失効を要求する場合、SF に利用者或いは利用者の証明書に関わる保証の違反、或いは本 CP/CPS に定める義務の重大なる不履行があった場合に限り、利用者は SF に対し証明書発行対価（但し、銀行諸掛等諸費用控除後の）の返金を要求出来る。　SF が利用者の証明書を失効した後、SF は証明書発行対価（但し、諸費用控除後の）の返金を行うに際し、利用者がクレジットカードにて支払いを行った場合には当該クレジットカード口座に、そうでなければ利用者が指定する銀行口座に返金するものとする。　本返金制度は唯一の法的救済ではなく、本 CP/CPS 上別途利用者に与えられるその他の救済を制限するものでもない。

2.6 情報公開とリポジトリ

2.6.1 CA 情報の公開

本 CP/CPS は 8 条に即し以下 URL の SF リポジトリにおいて公開される。
http://www.starfieldtech.com/repository/

2.6.2 公開の頻度

本 CP/CPS は 2.6.1 条に即し、CRL は 4.4.9 条に即し公開される。

2.6.3 閲覧制限

SF リポジトリの閲覧は誰に対しても一切制限されないが、加筆訂正は所定のアクセス制御を介し権限ある SF PKI 従業員のみに限られる。

2.6.4 リポジトリ

SF リポジトリには、本 CP/CPS 最新版、SF CA の Fingerprint、CRL 最新版、その他利用者や依存当事者に開示されるべき情報がストアされる。

SF は別途、発行済証明書データベースと権限ある SF PKI 従業員のみにそのアクセスが制限されている CRL を維持管理する。

SF リポジトリは以下 URL において公開される。
http://www.starfieldtech.com/repository

2.7 順守監査

2.7.1 順守監査の頻度

SF CA は、年に 1 度、WebTrust 監査 (WebTrust for CA)を受けなければならない。

2.7.2 監査人の身元及び資格要件

WebTrust CA 監査を実施出来るのは、公開鍵基盤技術や、情報セキュリティツールや技術、セキュリティ監査や第三者認証に関し習熟した監査人でなければならない。監査法人については、WebTrust CA 監査、WebTrust EV 監査のライセンスを保持し、且つ米国公認会計士協会（AIPCA）の会員であると共に、少なくとも 100 万米ドルの求償限度を有する業務責任過失不作為保険を付保していなければならない。

2.7.3 監査人と被監査人との関係

年次監査を実施する主体は、SF と独立した組織でなければならない。

2.7.4 監査対象事項

年次監査においては、本 CP/CPS の要求事項、CA の環境制御能力、CA の鍵管理、証明書ライフサイクル管理を監査する。

2.7.5 監査不首尾時の対応

順守監査において指摘される重大なる不首尾には何らかの対策を執らねばならない。SF PKI Policy Committee は監査人からの情報提供を踏まえその対策を決定する。SF 経営陣は、矯正案を直ちに策定すると共に、問題の重大性に鑑み適切な時間の中で矯正策を実施する責任を負う。

SF PKI の完全性を危殆化し得るほどの重大な不首尾が指摘されたならば、SF 経営陣は監査人からの情報提供を踏まえ、SF PKI の運用を中断するかどうかの判断を行う。SF PKI の階層構造に属するいずれかの CA の完全性を危殆化し得るほどの重大な不首尾が指摘されたならば、SF 経営陣は当該 CA の運用を中断するかどうかの評価を行う。

2.7.6 監査結果の報告

監査結果については SF 経営陣及びその他同経営層が適当と考える個人、組織に報告される。

2.8 守秘義務

2.8.1 守秘義務の対象となる情報

守秘性高い SF PKI 情報は SF の機密情報として保持されなければならない。　以下情報は SF の機密情報であり、公開されることはない。

- SF PKI に関する方針及び手続き、並びに本 CP/CPS を支持する技術書類
- 以下を含む利用者情報
  - ✧ 証明書発行申請書
  - ✧ 認証を証する書類
  - ✧ 利用者証明書への記載が求められる情報以外の申請関連情報
- 監査証跡記録
- SF PKI 階層構造に属する一切の秘密鍵
- SF 経営陣の判断により公開される WebTrust CA 監査報告書を除く監査結果

2.8.2　機密性有りと判断されない情報

本 CP/CPS、SF により発行される証明書及び CRL には機密性はない。

2.8.3　証明書失効情報の開示

利用者証明書ステータス情報は、CRL の利用により依存当事者に公開される。　証明書が失効されるに至った経緯やその他関連情報は機密情報として公開されない。

2.8.4　司法機関への情報開示

原則論として、SF PKI に属し管理されている書類や記録（登録情報を含む）は以下の場合を除き司法機関に対しても開示されない。

- 妥当性ある法規の要求である場合
- SF が準拠しなければならない裁判所や行政監督機関等による令状、指示命令がある場合
- SF に対する司法権を持って行政監督機関等から発せられた命令がある場合

2.8.5　民事公開手続き

原則論として、SF PKI に属し管理されている書類や記録（登録情報を含む）は以下の場合を除き民事公開手続きに対しても開示されない。

- 情報の開示を要求する妥当性ある民事手続きがなされた場合
- 裁判所により権限を付された、身元確認された情報公開を要求する個人からの要請があった場合

2.9　知的財産権

利用者及び依存当事者を除く SF PKI に関わるあらゆる当事者間の知的財産権の取り扱いについては、当事者間の適切な契約の定める所による。　以下に定める本条の付帯条文は利用者及び依存当事者に関わる知的財産権にも適用される。

2.9.1　証明書及び失効情報に関わる財産権

証明書及び失効情報に関わる知的財産権は、当該証明書を発行し失効した SF PKI 階層構造に属する CA に保持される。　一旦失効された証明書が依存当事者約款に即し再生成される場合、SF 及び利用者は同利用を非独占的に無償で許可する。　SF 及び利用者は、依存当事者約款或いはその他適切な契約に即し依存当事者独自の目的を達成する為に証明書の失効情報の利用を許可する。

2.9.2　契約に関わる財産権

SF PKI に関わるあらゆる当事者は、本 CP/CPS に関わる一切の知的財産権は SF が保持することを認める。

2.9.3　名義に関わる財産権

証明書発行申請時に記載、表記された商標や商品・サービス名、屋号や、証明書に記載された識別名において、それらに何らかの権利が留保されている場合、証明書発行申請者がそれら一切の権利を保持する。　SF は、SF が所有する商標や商品・サービス名、屋号やその他一切の商用シンボル等に関わる権利を保持する。

2.9.4　鍵及び鍵に関する資料に関わる財産権

SF の階層構造に属するあらゆる CA 及び利用者の証明書に相対する全ての鍵ペアは、それら鍵ペアがどこに物理的にストアされているか或いはそれら鍵ペアに関わる知的財産権を誰が所有しているかに関わらず、当該 CA 及び利用者の財産である。　前述に関わらず、SF Root CA の公開鍵や当該公開鍵を搭載している Root 証明書は SF の財産である。　SF は、ソフトウェアやハードウェアの製造者に対し、Root 証明書を複製し且つハッキングされる心配のないハードウェア機器やソフトウェア内に当該複製物をストアするライセンスを付与することが出来る。　前述一切の取決めを制限することなく、SF の階層構造に属する CA の秘密鍵の SECRET SHARING システム（CA 秘密鍵をセキュアに保全する為、秘密鍵を起動する為に必要なデータを Secret Share と呼ばれる分割された部分情報として Shareholder と呼ばれる本職務の為の訓練を受けた特定の信頼される SF 従業員により分散管理させるもの）は当該 CA の財産であり、それらに関わる知的財産権は当該 CA が保持する。

以下アイテムは SF の財産である。

- 本 CP/CPS
- SF により規定された証明書ポリシー
- SF PKI の運用を支持する方針と手続き
- SF により特定された Object Identifier (OID)

- SF CA により生成、発行された証明書及び CRL
- SF PKI において主体を表象する為に利用される識別名（Distinguished Names/DN）
- CA とその基盤の鍵ペア

3 身元確認と認証

3.1 初回の本人確認

3.1.1 名称の形態

全ての証明書保有者は、X.500 標準に即した識別名を必要とする。 SF PKI は証明書発行申請者に対し識別名の生成を行う為のルールを定める。 SF 証明書における発行者（Issuer）及び主体識別名（Subject Distinguished Name）については本 CP/CPS 7.1 条にて詳述する。

3.1.2 意味のある名称であることの必要性

SF PKI 証明書においては、識別名は一般に理解されている意味のある名称を含まなければならない。

3.1.3 識別名を解釈する為の方針

識別名の解釈は、本 CP/CPS の 3.1.1 条及び 3.1.2 条に即し行われる。

3.1.4 唯一の名称

Extended Validation 証明書（拡張認証証明書。以下、EV 証明書と言う）と High Assurance 証明書（高位信頼性証明書。以下、組織認証証明書或いは OV 証明書と言う）における、識別名は意味不明瞭であってはならず、また SF CA ドメインにおいては唯一の名称でなければならない。 但し、単一の利用者が単一の主体識別名で複数の証明書を同時に保持することは妨げない。 他方、Medium Assurance 証明書（中位信頼性証明書。以下、ドメイン認証証明書或いは DV 証明書と言う）或いはコードサイン証明書については、単一の主体識別名を複数の証明書間で共有することが認められている。

3.1.5 名称に関わる紛争解決手続き

証明書発行申請者は、如何なる場合も第三者の知的財産権を侵害する名称を証明書発行申請時に利用することは出来ない。 SF は、証明書発行申請者が証明書発行申請時の名称に関わる知的財産権を保持しているかどうかの確認は行わず、ドメイン

名や屋号、商標や商品･サービスのマーク等の所有権に関わる如何なる紛争の調停・仲裁や訴追、解決は行わない。　SF は、証明書発行申請者に何らの責任を負うことなく、そうした紛争を理由として、証明書の申請を拒否或いは保留することが出来る。

3.1.6　商標の認識、認証及び役割

本 CP/CPS の 3.1.5 条を参照。

3.1.7　秘密鍵を所有していることを確認する方法

利用者証明書発行要求には、認証済の公開鍵が搭載されており、且つ相対する秘密鍵により電子署名がなされていなければならない。

3.1.8　組織の実在性確認

OV 証明書を組織に発行する場合、SF は以下を確認する。

- 行政機関に現時点で登記されている組織を表象する組織名であるか
- 証明書の発行申請した個人が証明書発行申請時に特定されたドメイン名の管理権限を保有しているか
- 証明書の発行申請した個人が証明書に記載される組織から権限を付与された人物かどうか

3.1.9　個人の実在性確認

OV 証明書を個人に発行する場合、SF は以下を確認する。

- 証明書発行申請のあった個人の身元
- 証明書発行申請した個人が証明書発行申請時に特定したドメイン名の管理権限を保有しているか

行政機関に登記されない種類の個人事業等については、SF は、参考情報として未確認組織名称等を記載する OU フィールドに屋号（doing business as: DBA）の記載を行うことが出来る。

3.1.10　ユニファイド・コニュニケーション証明書認証

証明書の発行申請した個人がユニファイド・コニュニケーション証明書のコモンネーム或いはサブジェクトの別名欄（Subject Alternative Name Field）に含まれる全ての FQDN（完全修飾ドメイン名）の管理権限を有していることを確認する。一枚の OV ユニファイド・コミュニケーション証明書は、一つの組織或いは個人に対してのみ発行される。

3.1.11　ドメイン信頼性認証

DV 証明書を発行する場合、SF は以下を確認する。

・　証明書発行申請した個人が証明書発行申請時に特定したドメイン名の管理権限を保有しているか

3.1.12　EV 証明書における組織実在性確認

EV 証明書を発行する場合、SF は、EV 証明書の発行・管理手続きを世界標準規格として定めた CA/Browser Forum Guidelines（http://www.cabforum.org）に即し、以下を確認する。

・　利用者が法的登記済であって、その身元が法的に明確になっているか（法的実在性）
・　俗称、仮名（もしあれば）
・　事業所が確かに存在しているか（物理的実在性）
・　事業が実際に行われているか（事業実在性。事業暦が設立登記後 3 年未満の場合に限る）
・　ドメイン名を所有し独占的使用権を保持しているか
・　署名権者（Contract Signer）及び申請責任者（Certificate Approver）の名前、肩書、職務権限について

3.1.13　コードサイン証明書

組織認証コードサイン証明書を発行する場合、SF は以下を確認する。

・　行政機関に現時点で登記されている組織を表象する組織名であるか
・　証明書発行申請した個人が証明書に記載される組織から権限を付与された人物かどうか

3.2　定期的な鍵の再生

定期的な鍵の再生は、本 CP/CPS の 4.9 条に即し行われる。

OV 証明書や DV 証明書､そしてコードサイン証明書を利用の利用者で所定(3.1.8 条、3.1.9 条、3.1.10 条）の利用者身元確認及び認証手続きが SF によって過去 13 か月以内に行われている場合、SF は直近の認証情報をもって証明書の更新要求の認証に充てることが出来る。　EV 証明書を利用の利用者で所定（3.1.11 条）の利用者身元確認及び認証手続きが SF によって前年に行われている場合、SF は直近の確認情報をもって証明書の更新要求の認証に充てることが出来る。　上記に当てはまらない証明書の更新については､所定の利用者身元確認及び認証手続きを再度やり直さなければならない。

3.3　証明書失効後の鍵の再生

SF CA 証明書が失効されなければならない場合、CA は本 CP/CPS 4.9 条及び 4.10 条に即し再生される。

利用者証明書失効後の鍵の再生手続きについては、申請手続きを再度一からやり直さなければならず、新たな利用者鍵ペアの生成と本 CP/CPS 3.1.18 条及び 3.1.19 条に即した利用者身元確認及び認証手続きの再実行が必要となる。

3.4　証明書の更新

CA 証明書については、本 CP/CPS 4.9 条に即し実存する識別名に対する有効期限を延長した新たな証明書を発行することで、証明書の更新を行うことが出来る。

利用者証明書の更新については、本 CP/CPS 3.1.12 条に即し鍵の再生手続きを介して行われる。

3.5　失効申請

利用者は、証明書失効申請コーナーよりオンラインで証明書失効申請を行うことが出来る。　当該申請の認証は直近の認証情報を利用することで行われる。

当該申請が直近の認証情報により認証出来なかった場合、SF の証明書失効手続きに即し当該失効申請を十分に認証しなければならない。

3.6　利用中断申請

本 CP/CPS 4.4 条を参照。

3.7　利用中断の解除申請

本 CP/CPS 4.4 条を参照。

4　運用要件

4.1　証明書発行申請

証明書の発行申請に際しては、SF 証明書発行申請書に要求される全ての情報を記載する。

4.2　証明書発行

証明書は、本 CP/CPS 3.1.8 条、 3.1.9 条、 3.1.12 条から 3.4 条に即し行われる RA による認証が完了して初めて、生成、発行され、そして公開される。

4.3　証明書の承認

利用者による発行済証明書の受領とその後の鍵ペア及び証明書の利用を持って、利用者は証明書を受領した、ものと見做す。

証明書の受領により、利用者は以下事項に合意したものとする。

- 本 CP/CPS に定める利用者の責任及び義務に拘束されること
- 利用約款の定めに拘束されること
- 発行済証明書に相対する秘密鍵に対し、過去誰であろうと権限無き者がアクセスしていないことを表明し、保証すること
- 登録時に提供された証明書記載情報が真実であって、証明書上で正しく完全に公開されていることを表明し、保証すること

4.4　証明書の中断及び失効

SF は、全ての SF CA 証明書の失効についてはサポートするが、中断についてはサポートしない。

4.4.1　証明書が失効される為の要件

証明書は以下のいずれか或いは全ての状況において失効される。

- 利用者が、或いは利用者を代表する権限ある販売代理人が、本 CP/CPS 3.5 条に即し証明書の失効を要求した場合
- 証明書被発行人が本 CP/CPS の規定に違反した、或いは SF PKI のセキュリティ或いは完全性を危殆化したと認められる場合
- 利用者が利用約款の規定に違反したと認められる場合
- 利用者の秘密鍵が危殆化したと明らかになった、或いは疑われる場合
- 証明書有効期限が切れる前に、利用者証明書の Subject フィールドに記載された認証済組織名、或いは個人名に変更があった場合
- 利用者が、SF 発行の請求書を受領したと合理的に見做される日から 45 日以内に、請求代金の支払を完了しなかった場合

4.4.2　証明書失効の要求を行えるのは誰か

利用者証明書は、利用者或いは権限ある販売代理人、或いは SF により失効の要求が成される。

4.4.3　証明書失効の手続き

利用者証明書の失効要求は、直近の認証情報、或いは SF 失効手続きに即して認証される。　全ての失効要求は手動による承認手続きにより処理されなければならない。

4.4.4　証明書失効要求の猶予期間

SF は、自動失効要求については、直近の認証情報が正しく提供されている場合に限り要求の受領時をもって、他方手動による失効要求については受領後 1 営業日以内に、認証する。

SF は、失効要求認証後直ちに失効手続きに入る。　認証済失効要求の手続き開始後 7 営業日以内に証明書の失効ステータスを CRL に反映する。　失効された証明書情報は当該証明書の有効期限が失効するまで CRL に記載される。

4.4.5　証明書が利用中断される為の要件

適用せず。

4.4.6　証明書の利用中断の要求を行えるのは誰か

適用せず。

4.4.7　証明書利用中断の手続き

適用せず。

4.4.8　証明書利用中断期間の制限

適用せず。

4.4.9　CRL の発行頻度

SF CA の CRL の発行頻度は以下の通り。

- Root CA：　証明書失効時、その後は最長 365 日ごと
- Issuing CA：　最長 7 日ごと

4.4.10　依存当事者による CRL の確認要求

依存当事者は、証明書に依存する前に CRL を活用し証明書のステータスを確認しなければならない。

4.4.11　オンライン証明書失効/証明書ステータス確認機能

SF CF の OCSP は以下に従い発行される。

- Root CA：　証明書失効時、その後は最長 365 日ごと（但し、OCSP が機能する Root CA に限る）
- Issuing CA：　最長 4 日ごと

4.4.12　依存当事者によるオンライン証明書失効の確認要求

規定無し。

4.4.13　その他の証明書失効通知手段

規定無し。

4.4.14　依存当事者によるその他の証明書失効通知手段の確認要求

規定無し。

4.4.15　鍵の危殆化に関する特別要求

秘密鍵の危殆化により利用者証明書を失効する場合、求められる証明書失効手続きは前項に定めるところと差異はない。

前項に加え、SF の判断により、SF CA の秘密鍵が危殆化したと認識した場合、或いはそう信ずるに足る合理的理由がある場合、危殆化した旨を潜在的な依存当事者に通知するよう商業上合理的な範囲で努力をする。

4.5　証明書問題発生報告及びその対応

4.5.1　報告

SF は、本 CP/CPS 1.4 条にて公開された電子メール或いは電話において、利用者や依存当事者、アプリケーションベンダーやその他の第三者からの、不満や疑われる秘密鍵の危殆化、EV 証明書の悪用やその他の詐欺行為、EV 証明書に関連する危殆化、悪用或いはその他の不適切な行為につき、報告を受ける。

4.5.2　調査

SF は、前項報告から 24 時間以内に全ての証明書に関する問題につき調査し、以下の基準に即し、当該証明書の失効或いは適切なる処置の実施につき決定する。

(i)　争点となっている問題の本質

(ii)　特定の EV 証明書或いは同証明書の利用しているウェブサイトに関して受領した報告の数

(iii) 不満の実態（例えば、ウェブサイトに対する不満でも、非合法的な行為に与しているとの司法当局者からの不満の方が、ウェブサイトで発注済の物品が未だ届かない等の消費者からの不満より重視される。）

(iv) 実効性ある法制度

4.5.3 対策

SF は、緊急を要する証明書の問題の報告に対しては年中無休（24 時間×7 日間）で応ずる体制を維持し、必要であれば本 CP/CPS 4.4 条に即し当該証明書を失効し、或いはまた司法当局へエスカレーションする。

4.6 セキュリティ監査手続き

4.6.1 記録すべき事象の類型

SF PKI は以下の事象について漏れなくログ管理を行う。

- CA 鍵のライフサイクル管理（CA 鍵の生成バックアップ、保管、破壊を含む）及びその他暗号化機器のライフサイクル管理
- CA 及び利用者の証明書ライフサイクル管理上の事象
  -証明書発行申請、更新申請、鍵再生申請、証明書失効申請
  -申請の成功、不成功
  -証明書の生成及び発行
  -証明書の失効
  -CRL の発行と OCSP の生成
  -諸規定に即した認証手続き
  -電話音声認証の実施日時及び電話番号、認証相手氏名、その内容及び結果
- セキュリティ上重要な運用上の事象
  -PKI 認証の成功、不成功
  -PKI 及びその他セキュリティ活動
  -セキュリティ手続きの変更
  -システムクラッシュ、ハードウェア破壊及びその他の異常
  -ファイアーウォールやルーターの動静
  -CA 設備からの入退室管理
- CA 設備の入退場管理
- EV 証明書の為の複数の RA に分担された認証作業

4.6.2 必要なデータ類

全ての監査ログは少なくとも以下を含む。

- データエントリ日時

・ 仕訳作業を行った個人や組織の身元
・ データエントリ内容

4.6.3 ログ管理の頻度

監査ログの検証は必要に即し随時行われる。

4.6.4 監査ログの保持期間

監査ログは以下ログの類型に即し所定の期間保持される。

・ CA 鍵管理活動のログ： 30 年
・ 証明書管理に関する CA システムログ： 30 年
・ オペレーティングシステムログ： 5 年
・ 物理的アクセス管理システムログ：5 年
・ 物理アクセスに関する手動ログ： 5 年
・ CA 設備へのアクセス記録（ヴィデオ）： 90 日

4.6.5 監査ログの保護

論理的且つ物理的に生成、保管された監査ログは論理的且つ物理的アクセス制御により保護される。

4.6.6 監査ログバックアップ手続き

監査ログは定期的にバックアップされる。

4.6.7 監査事項収集システム（内部対外部）

自動化された監査データはアプリケーションやネットワーク、そしてオペレーティングシステムレベルで生成され、記録される。 手動で生成された監査データは SF 従業員により記録される。

4.6.8 監査事象の通知について

監査を要する事象が監査事項収集システムにて検地された場合でも、当該事象を発生せしめた本人やシステムに対する通知は必要ない。

4.6.9 脆弱性検査

SF は定期的に SF PKI 環境の脆弱性検査を実施する。 検査結果は当該環境のセキュリティレベル向上に利用される。

4.7　記録保管

SF PKI は SF PKI 階層構造に属する各 CA の記録を保管維持する。

4.7.1　記録される事象の類型

SF は、本 CP/CPS 4.6.1 条に特定された事象記録を含むログを保管維持する。

4.7.2　保管期間

SF は、本 CP/CPS 4.6.4 条に即し監査ログを保管する。

4.7.3　保管記録の保護

本 CP/CPS 4.6.5 条を参照。

4.7.4　保管記録のバックアップ手続き

SF は保管記録の複製を異なる場所に維持管理する。

4.7.5　保管記録のタイムスタンプに関する要件

SF PKI のシステム時計は、第三者の時計とシンクロしている。　自動データエントリはシステムにて生成された日時フィールドを含む。　手動データエントリには日時の手動入力フィールドを含む。

4.7.6　保管記録収集システム

規定せず。

4.7.7　保管記録情報の取得及び検証の手続き

規定せず

4.8　鍵の切替

SF CA は、本 CP/CPS 6.3.2 条に即し証明書署名の鍵の利用が許された最長期間に達する前に、証明書の発行を停止し、そして鍵を再生、或いは失効させる。　CA は、CA 証明書のライフタイムが終了するまで、継続して署名し CRL を発行する。　鍵の切替或いは CA の失効手続きは、利用者及び依存当事者に対する悪影響を最小限に留めるよう行われる。　影響ある主体には鍵の切替の前に連絡される。

4.9　危殆化及び災害からの復旧

災害時に SF PKI の運用を復旧させる為に、SF は以下を実施する。

- SF CA の秘密鍵の複製を格納したバックアップ暗号化ハードウェアモジュールのオフサイトでのセキュアな保管

- 欠くべからざる起動機器のオフサイトでのセキュアな保管
- システム、データ及び設定情報のバックアップのセキュアな保管
- SF の主要設備が被災した場合の運用を再開する災害時復旧サイトの確保
- 災害復旧プラン
- 定期的な災害復旧プランのテスト

SF は、物理的、論理的、手続きに関する制御をバランスよく実施することで、CA 鍵の危殆化を防ぐ。 CA 鍵の危殆化が認められた場合、或いは疑われる場合、SF 経営陣は、事態を評価し適切なる行動を決定する。

4.10 CA の失効

SF CA の運用の失効が必要と判断される場合、SF 経営陣は、失効の影響が最低限に抑えられるよう、失効プランを策定し、利用者と依存当事者と協調する。 SF は、現実的且つ合理的な範囲で利用者及び依存当事者に出来るだけ前広なる通知を行い、機能的且つ法的目的に照らし適合すると見做される期間、適宜記録を保管する。 SF CA の失効よりも先に必要とあらば、証明書の失効が行われる場合もある。

5 設備、手続き及び人的セキュリティの制御

5.1 物理的制御

5.1.1 立地場所及び構造

SF PKI システムは、多層的に物理アクセス制御を施している米国アリゾナ州スコッツデールのセキュアな設備を利用しホストされ運用されている。

5.1.2 物理的アクセス

SF PKI システムは、CA 環境のあらゆる機器に対するアクセスを二要素認証とデュアル制御で構成するセキュアな設備にハウジングされている。 CA 設備への物理的アクセスは自動的にログされ 24 時間×7 日で始終ヴィデオ記録されており、他方外部のセキュリティ会社によって 24 時間×7 日で始終監視されている。

5.1.3 電源及び空調

SF CA システムへの電源供給は、UPS システムと発電機の利用により保護されている。 天候制御システムが作動しており、CA 設備内の温度を合理的な運用限界温度の範囲内で維持している。

5.1.4　水害

CA をホストしている設備は、100 年間洪水とは無縁であった地域に設置されている。

5.1.5　火災予防及び保護対策

SF CA をホストしている設備は、煙検地システムとドライパイプ火災抑止システムを装備している。

5.1.6　メディアの保管

商用ソフトウェア、商用データ、システム監査情報を格納したメディアは、権限ある従業員のみがアクセス出来る物理的且つ論理的アクセス制御を施しセキュアに保管されている。

5.1.7　オフサイトバックアップ

オフサイトバックアップメディアは、第三者の保証付き保管庫にて物理的にセキュアに保管されている。

5.1.8　廃棄物処理

機密性高い文書及び資料は廃棄前にシュレッダー処理される。　機密情報を遣り取りするのに利用されたメディアは廃棄前に読取不能化される。　その他の廃棄物は SF の通常の廃棄要件に従い処理される。

暗号化された機器、スマートカード、その他秘密鍵或いは鍵処理された資料については、製造メーカーの廃棄処理ガイドに即し物理的に破裁或いは初期化される。

5.2　手続き制御

5.2.1　信頼される役割

SF PKI の運用に従事する全ての SF 従業員は、"信頼された役割"を担うものとされる。SF PKI においては、以下の信頼された役割が存在する。

- セキュリティ担当　セキュリティポリシー、手続き、基準の順守を確立し、監視する責任を有する。
- エンジニアリング/アーキテクチュア担当　SF PKI の設計及び開発に責任を有する。
- PKI 運用担当　SF PKI を支持するあらゆるシステムの管理、運用及び監視に責任を有する。
- 鍵管理担当　暗号化機器の管理に責任を有する。
- RA 運用担当　証明書発行申請及び失効要求の処理に責任を有する。

5.2.2　職務ごとに必要とされる従業員数

SF PKI における暗号処理に関わる機密性高い運用職、例えば CA 鍵の生成、CA 鍵の復旧、CA 鍵の起動、CA システム設定等の職務は、本 CP/CPS 6.2.2 条に即し複数の"信頼される"個人の関与が必要となる。　その他の運用職においては 1 名の信頼される個人が従事すれば十分である。

5.2.3　それぞれの職務に必要な身元の確認

SF PKI におけるそれぞれの信頼される役割を担う人材は、職務を遂行するに当たり経営層の承認を受けなければならず、また本 CP/CPS 5.3 条に即し職務要件を満足しなければならない。

5.3　人的制御

5.3.1　経歴、資格、経験及び許可要件

SF PKI に従事する個人の採用及び選択においては、経歴、資格、経験及び各職務の許可要件を考慮する。

5.3.2　経歴調査手続き

経歴調査は SF にての雇用を開始する前までに実施されなければならない。　調査には、身元調査、人物照会、過去の雇用実態確認、学歴調査、犯罪履歴が含まれるが、それらに限られない。　SF 従業員は薬物検査に合格することを要求される。

SF 従業員は守秘義務契約に署名すること、及び SF PKI 方針と手続きを順守することを求められる。

5.3.3　トレーニング要件

全ての SF PKI 従業員は以下のジョブトレーニングを受講する。

- PKI の基礎的理解
- 本 CP/CPS
- SF PKI セキュリティと運用の方針と手続き
- PKI システムソフトウェアの利用と運用
- 認証手続きにおける、フィッシング等のソーシャルエンジニアリング等の脅威

5.3.4　再トレーニングの頻度及び要件

SF PKI 従業員は、雇用後においては必要に応じ、PKI 製品の利用や SF PKI の方針と手続きについていのトレーニングを、公式、非公式を問わず受講する。　セキュリ

ティの認識を高めるキャンペーンは常に実施されている。

5.3.5 人事異動の頻度と順序

規定せず。

5.3.6 無権限行為に対する懲戒

あらゆる無権限行為とその他 SF PKI 方針と手続きに反する行いについては、会社方針に即し、懲戒措置が成される。

5.3.7 外部コントラクターの要件

SF PKI は必要に応じ外部コントラクターを雇用する場合、外部コントラクターに対し本 CP/CPS 5.3.1 条及び 5.3.2 条に規定される調査に相当する経歴調査を実施する。

5.3.8 従業員に提供される書類

SF PKI 従業員は本 CP/CPS を熟読しることを求められ、他方 SF PKI 方針や手続き及びそれぞれの職務遂行に必要な書類を付与される。

6 技術的セキュリティ制御

6.1 鍵ペアの生成

6.1.1 鍵ペアの生成

CA 鍵の生成には、本 CP/CPS 6.2.1 条に即し暗号化モジュールの使用が求められ、複数の信頼される SF 従業員の関与が必要となる。

利用者鍵ペアの生成は利用者にて行われる。

6.1.2 秘密鍵の受渡し

SF CA の鍵ペアは SF PKI が生成し管理する為、受渡しの必要はない。 利用者の鍵ペアについても、利用者自身が生成する為、秘密鍵の移送の必要が無い。

6.1.3 公開鍵の証明書発行体への受渡し

CA 証明書 CSR は、複数の信頼される SF 従業員の関与を要する制御された手続きにより同従業員により生成、手続きされる。 CA 証明書 CSR は、PKCS#10 にて成され、CA 公開鍵を格納の上、CA 秘密鍵により電子署名される。

利用者証明書 CSR については、利用者公開鍵は、利用者秘密鍵にて署名された CSR に格納され CA に提出される。　この仕組みは以下を担保する。

- 利用者公開鍵は受渡しの間に改ざんされる恐れがない
- 送り手である利用者が公開鍵に相対する秘密鍵を間違いなく保持している

6.1.4　CA 公開鍵の依存当事者への受渡し

SF Root CA は、共通のブラウザソフトウェアに格納搭載されており、依存当事者が利用出来る状態にある。

SF Root CA 証明書は、SF リポジトリからダウンロードすることが出来る。　160bit Sha-1 ハッシュの SF Root CA 証明書は SF リポジトリにポストされているので依存当事者は SF Root CA 証明書の信頼性を確認出来る。

6.1.5　鍵のサイズ

SF CA 鍵ペアは 1024bit 或いはそれ以上の暗号強度の RSA 鍵であり、利用者鍵ペアも同じく 1024bit 或いはそれ以上の暗号強度の RSA 鍵である。

6.1.6　公開鍵のパラメータ生成と品質確認

適用せず。

6.1.7　ハードウェア/ソフトウェア鍵生成

SF CA 鍵ペアは、米国連邦標準規格 FIPS140-1 level 3 の認定を受けたハードウェアセキュリティモジュール（以下、HSM と言う）の内部で生成され、保護されなければならない。

利用者鍵ペアは、ハードウェア或いはソフトウェアの内部で生成され、保護されなければならない。　利用者には、鍵の生成の為に同 FIPS140-1 の認定を受けた暗号化モジュールを利用することが望まれる。

6.1.8　鍵の利用目的

鍵ペアは以下の通り利用される。

- Root CA 鍵ペア：　中間 CA 証明書及び CRL への署名
- Issuing CA 鍵ペア：　利用者証明書及び CRL への署名
- 利用者鍵ペア：　サーバ認証、鍵の暗号化、データの暗号化

鍵の利用については、本 CP/CPS 7.1 条に即し証明書プロファイルの要件に従い設定される。

6.2 CA 秘密鍵の保護

6.2.1 暗号化モジュールの規格

SF PKI は、FIPS140-1 level 3 の認定を受け且つ無作為で主要な数字の生成の為の工業規格を満たす暗号化モジュールを利用する。

6.2.2 秘密鍵の複数人員による制御

Root CA は、オフラインにて運用される。

機密性高い CA 秘密鍵の運用（HSM の起動、中間 CA 証明書への署名、CRL への署名、CA 鍵のバックアップ、CA 鍵の復旧を含む）には複数の信頼される従業員の関与が必要となるが、その実施には以下が適用される。

- 本 CP/CPS 2.9.4 条に即し Secret Share を保有している 5 人の Shareholder の内の 3 人が、HSM を起動する為の起動情報を提示し、且つ
- 3 人の従業員が協働して HSM に物理的にアクセスし、且つ
- うち 1 人以上の従業員が CA システムに関する十分なる権限を保持している

Issuing CA はオンラインで運用される。

機密性高い CA 秘密鍵の運用（HSM の起動、CA 鍵のバックアップ、CA 鍵の復旧を含む）には複数の信頼される従業員の関与が必要となるが、その実施には以下が適用される。

- 本 CP/CPS 2.9.4 条に即し Secret Share を保有している 8 人の Shareholder の内の 2 人が、HSM を起動する為の起動情報を提示し、且つ
- 2 人の従業員が協働してオンライン HSM に物理的にアクセスし、且つ
- 3 人の従業員が HSM 起動に必要な情報に物理的にアクセスする

6.2.3 秘密鍵のエスクロー（預託）

CA 及び利用者の鍵ペアのエスクローは、法の執行或いはその他の理由があっても、SF PKI がサポートすることはない。

6.2.4 秘密鍵のバックアップと保管

CA 鍵の複製バックアップは、本 CP/CPS 6.2.1 条に定める要件を満足する暗号化モジュールを利用することで暗号化された状態で保管される。

CA が本 CP/CPS 6.3.2 条に即し失効される場合、CA 秘密鍵を格納した HSM は確実

に破壊されなければならない。

利用者の秘密鍵は SF PKI によりバックアップされることも保管されることもない。

6.2.5　秘密鍵の暗号化モジュールへの格納

CA 秘密鍵は、本 CP/CPS 6.2.1 条の要件を満足する HSM の内部で生成され利用される。　秘密鍵は暗号化された状態でのみ HSM の外部で存在出来る。

6.2.6　秘密鍵の起動方法

CA 秘密鍵の保護の為に利用される HSM は、本 CP/CPS 6.2.2 条に定める起動手続きに即し利用される。

利用者の秘密鍵はパスワード認証により保護される。

6.2.7　秘密鍵の無力化

CA 秘密鍵は HSM のセッションを終了させることで無力化される。

6.2.8　秘密鍵の破壊方法

CA 秘密鍵の破壊を行うには、複数の信頼された SF 従業員の関与と SF 経営陣の承認が必要。　CA 鍵を破壊する場合、CA 秘密鍵は、初期化するか或いは製造メーカーの指針に従い物理的に破壊することによって、完全に破壊されなければならない。

6.3　その他の鍵ペアの管理

6.3.1　公開鍵の保管

CA 及び利用者の証明書の複製は、本 CP/CPS 4.7 条に即し保管される。

6.3.2　公開鍵及び秘密鍵の使用期間

SF PKI CA 及び利用者の鍵及び証明書の使用期間は以下の要件を満足しなければならない。

主体	証明書署名鍵の 最長使用期間	CRL署名鍵の 最長使用期間	証明書の 最長有効期間
Root CA	15年	20年	30年
Issuing CA	20年	25年	20年
利用者	適用無	適用無	10年 （或いは適切な指針に従う）

6.4　起動情報

CA 秘密鍵保護に利用される HSM は、Secret Share を保有している 5 人の Shareholder の内の 3 人が､本 CP/CPS 6.2.2 条に定める HSM 起動情報を提示することを要求する。この起動情報は、必要な時のみ利用され、利用されていない時はセキュアな場所に保管されなければならない。

6.5　コンピュータ・セキュリティ制御

6.5.1　特定のコンピュータ・セキュリティの技術要件

CA ソフトウェアおよびデータファイルを維持管理している SF システムは、権限ないアクセスから保護されなければならない。　加えて、証明書発行の運用に供されているサーバへのアクセスは有効な業務上要求ある権限ある従業員にのみ限定される。

SF の証明書発行ネットワークは論理的に独立しており､特定のアプリケーションとの通信以外の当該ネットワークへのアクセスは許可されていない。　SF は、当該ネットワークを権限外の内部及び外部からのアクセスから保護し、証明書発行システムへのアクセスを行う活動を制限する為に、精度高いアクセス制御技術を導入している。

6.5.2　コンピュータ・セキュリティの評価

規定せず。

6.6　ライフサイクル技術制御

6.6.1　システム開発制御

全ての CA ソフトウェアは、書類化された SF ソフトウェア開発ライフサイクル手続きに即し開発される。　SF PKI Policy Committee により、その全ての開発段階で同 Committee の承認が求められる。　全ての開発コードは、証明書発行 CA の環境に配置される前に、電子署名やハッシュを利用することで検証される。

6.6.2　セキュリティ管理制御

SF は、CA システムの設定を制御し監視する為のツールと手続きを用意し導入している。　全てのソフトウェアの完全性は、証明書発行システムに供される前に SF により検証される。

6.6.3　ライフサイクルセキュリティの評価

規定せず。

6.7　ネットワークセキュリティ制御

SF の証明書発行ネットワークは、適切に設定されたルーターとファイアーウォールによる防御的制御と検知システムによる侵入検知により保護される。　SF は全ての CA 及び RA を、SF 運用指針に即し証明書発行ネットワークを活用することでセキュアに運用する。

6.8　暗号化モジュールエンジニアリング制御

SF PKI は本 CP/CPS 6.2.1 条の要件を満足する暗号化モジュールを利用する。

7　証明書及び CRL のプロファイル

詳細は、以下の米国スターフィールド・テクノロジーズ LLC レポジトリをご覧ください。 https://certs.starfieldtech.com/Repository.go

8　改訂

8.1　改訂手続き

本 CP/CPS の改訂については、SF PKI Policy Committee に承認を受けなければならず、SF リポジトリでの公開を持って同改訂内容が発効する。

8.2　公開及び通知方法

本 CP/CPS 及び関連する改訂箇所は、本 CP./CPS 2.6.1 条に即し SF リポジトリに公開される。　SF は本 CP/CPS を何等事前の通知なく何時でも改訂することが出来る。

8.3　CP/CPS 改訂承認手続き

本 CP/CPS 8.1 条に即す。

9　用語の定義

（省略）