



**ENTRUST
SSL Web Server Certification Practice Statement**

バージョン: 2.03

1 月 1 日, 2003 年

版權 c 2002 Entrust Limited 版權所有

改訂履歴

版	日付	変更事項
1.0	1999年5月26日	初版
2.0	2000年7月1日	Entrust.net SSL Web Server の公開鍵インフラにおける(第三者登録局などの)従属主体に関する規定を追加。その他、さまざまな条件の改正。
2.01	2001年5月30日	実質的な影響なしのマイナーな改正。
2.02	2002年1月1日	相互認証証明書変更に伴うマイナーな改正。
2.03	2003年1月1日	Entrust 法的社名変更。

目次

1 はじめに

1.1 概要

1.2 正式名称

1.3 共有および適用

1.3.1 認証局 (CA)

1.3.2 登録局 (RA)

1.3.3 エンドエンティティ

1.3.4 適用可能性

1.4 連絡先の詳細

1.4.1 仕様管理部門

1.4.2 連絡先

2 一般条項

2.1 義務

2.1.1 CA の義務

2.1.2 RA の義務

2.1.3 加入者の義務

2.1.3.1 加入者および申請者の明示および保証

2.1.3.2 加入者による通告に関する要件

2.1.4 信頼当事者の義務

2.1.4.1 信頼当事者の明示および保証

2.1.5 保管義務

2.2 責務

2.2.1 CA の責務

2.2.1.1 保証および保証限度

2.2.1.2 否認

2.2.1.3 損失制限

2.2.1.4 その他の除外

2.2.1.5 危険な活動

2.2.2 RA の責務

2.3 財務上の責任

2.3.1 信頼当事者による免責

2.3.1.1 加入者による免責

2.3.2 信頼関係

2.3.3 管理手順

2.4 解釈および執行

2.4.1 準拠法

2.4.1.1 不可抗力

2.4.1.2 解釈

2.4.2 分離、存続、合併、通知

2.4.2.1 分離

2.4.2.2 存続

2.4.2.3 合併

2.4.2.4 規定の相反

2.4.2.5 権利放棄

2.4.2.6 通知

2.4.2.7 権利の譲渡

2.4.3 紛争解決手順

2.4.3.1 仲裁および訴訟についての制限期間

2.5 サービスの料金

2.5.1 証明書発行料金、更新料金

2.5.2 証明書アクセス料

2.5.3 失効あるいはステータス情報アクセス料

- 2.5.4 ポリシ情報などその他のサービス料金
- 2.5.5 払い戻し方針
- 2.6 公表およびリポジトリ
 - 2.6.1 CA 情報の公表
 - 2.6.2 公表の頻度
 - 2.6.3 アクセスコントロール
 - 2.6.4 リポジトリ
- 2.7 準拠性監査
 - 2.7.1 準拠性監査の頻度
 - 2.7.2 監査人の身元保証・資格
 - 2.7.3 被監査部門と監査人の関係
 - 2.7.4 監査の対象となる主題
 - 2.7.5 監査指摘事項に対する措置
 - 2.7.6 監査結果の報告
- 2.8 機密性
 - 2.8.1 機密を保つべき情報の種類
 - 2.8.2 機密とみなされない情報の種類
 - 2.8.3 証明書の失効・停止情報の開示
 - 2.8.4 法執行官への公表
 - 2.8.5 民事手続上の開示に伴う公表
 - 2.8.6 所有者の要請に基づく開示
 - 2.8.7 その他の情報公開状況
- 2.9 知的財産権

- 3 識別および認証
 - 3.1 初期登録
 - 3.1.1 名称の種類
 - 3.1.2 名称が意味を持つ必要性
 - 3.1.3 様々な名称様式の解釈規則
 - 3.1.4 名称の独自性
 - 3.1.5 名称に関するクレームによる紛争の解決方法
 - 3.1.6 商標の認識、認証および役割
 - 3.1.7 秘密鍵の所有を証明する方法
 - 3.1.8 組織の身元の認証
 - 3.1.9 個人の身元の認証
 - 3.2 定期的な鍵更新
 - 3.3 失効時の鍵更新
 - 3.4 失効要求

- 4 運営要件
 - 4.1 証明書の申請
 - 4.2 証明書の発行
 - 4.3 証明書の受理
 - 4.4 証明書の一時的停止および失効
 - 4.4.1 失効処理を必要とする状況
 - 4.4.2 失効を要求できる当事者
 - 4.4.3 失効要求の手続
 - 4.4.4 失効要求の猶予期間
 - 4.4.5 一時的停止の状況
 - 4.4.6 一時的停止を要請できる人
 - 4.4.7 一時的停止要請の手続
 - 4.4.8 一時的停止期間の限度
 - 4.4.9 CRL の発行頻度
 - 4.4.10 CRL のチェックに関する要件

- 4.4.11 オンライン失効・状態確認の可用性
- 4.4.12 オンライン失効確認要件
- 4.4.13 利用可能な失効告知のその他の様式
- 4.4.14 失効告知のその他の様式の確認要件
- 4.4.15 鍵更新に伴う安全性喪失に関する特別要件
- 4.5 セキュリティ監査手続
- 4.6 記録の保管
- 4.7 鍵の切り替え
- 4.8 信頼性の喪失および災害復旧
- 4.9 CA の終了

5 物理的、手続的、および要員のセキュリティ管理

- 5.1 物理的管理
- 5.2 手続的管理
- 5.3 要員管理

6 技術的セキュリティ管理

- 6.1 鍵ペアの生成とインストール
 - 6.1.1 鍵ペアの生成
 - 6.1.2 ユーザへの秘密鍵の配布
 - 6.1.3 証明書発行者に対する公開鍵の配布
 - 6.1.4 ユーザに対する CA 用公開鍵の配布
 - 6.1.5 鍵のサイズ
 - 6.1.6 公開鍵パラメータの生成
 - 6.1.7 パラメータの品質チェック
 - 6.1.8 ハードウェア・ソフトウェアの鍵生成
 - 6.1.9 鍵の使用目的
- 6.2 秘密鍵の保護
- 6.3 鍵管理のその他の局面
- 6.4 活性化データ
- 6.5 コンピュータのセキュリティ管理
- 6.6 ライフサイクル技術管理
- 6.7 ネットワークセキュリティ管理
- 6.8 暗号モジュールの技術管理

7 証明書および CRL のプロファイル

- 7.1 証明書のプロファイル
- 7.2 CRL のプロファイル

8 仕様管理

- 8.1 連絡先情報
- 8.2 仕様変更手続
- 8.3 公表および告知方針
- 8.4 CPS 承認手続

9 略語

10 用語の定義

1 はじめに

Entrust SSL Web Server CA(認証局)は、SSL (Secure Sockets Layer) プロトコルを用い、Web サーバとブラウザ間の安全な通信を支援するため Entrust SSL Web Server 証明書を発行します。Entrust は、Entrust の賞を獲得した Entrust/PKI™ソフトウェアを利用しています。このソフトウェアはデジタル証明書の標準に準拠しており、セキュアなオンライン通信を可能にします。

1.1 概要

この Entrust SSL Web Server 認証局運用規定 (CPS)は、(1)Entrust SSL Web Server CA および(2)Entrust SSL Web Server CA のもとで運営される登録局 (RA)の業務および手続を記述しています。この CPS はまた、Entrust が Entrust SSL Web Server 証明書に関連して Entrust SSL Web Server CA および RA によるサービスを提供するための諸条件も定めます。この CPS の適用対象には、すべての申請者、加入者、信頼当事者、再販者、販売協業者のほか、(1)Entrust SSL Web Server 証明書やそれに付随して Entrust が提供するサービスに関連して Entrust と関係を有するか、あるいは(2)Entrust SSL Web Server CA が認定する RA もしくは Entrust SSL Web Server 証明書に関連してサービスを提供する再販者または販売協業者と関係を有する人、法人、または組織が含まれます(ただし、これらに限定するものではありません)。この CPS は、Entrust SSL Web Server CA が発行するすべての Entrust SSL Web Server 証明書に参照用に編入されます。この CPS は、申請者、加入者、信頼当事者、再販者、販売協業者やその他の人、法人、および組織に対して、Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA の業務とポリシーを表明するものです。この CPS はまた、Entrust SSL Web Server CA の配下で RA を運営する第三者のほか、申請者、加入者、信頼当事者、再販者、販売協業者、およびその他、Entrust SSL Web Server 証明書を利用または信頼する人、法人、または組織、あるいは Entrust SSL Web Server 証明書やそれに付随するサービスに関連して Entrust SSL Web Server CA もしくは Entrust SSL Web Server CA の配下で運営される RA と関係を有する人、法人、または組織に対して、Entrust の権利と義務を表明するものです。

1.2 正式名称

この CPS の正式名称は、Entrust SSL Web Server 認証局運用規定と呼びます。

1.3 共有および適用

Entrust SSL Web Server 証明書の使用は、SSL プロトコルを使用している Web サーバに限定されます。

1.3.1 認証局 (CA)

Entrust SSL Web Server の公開鍵インフラ(PKI)において、CA は、Entrust が直営する RA または Entrust SSL Web Server CA が認定する独立の第三者 RA がこの CPS の規定に従って身元を確認した申請者から証明書署名要求 (CSR) と公開鍵を受理します。Entrust SSL Web Server 認証申請書の有効性が立証されたら、当該 RA は、Entrust SSL Web Server 証明書の発行を求める要求書を Entrust SSL Web Server CA に送付します。Entrust SSL Web Server CA は、RA から送付された要求書に記載されている公開鍵と申請者の身元確認情報に基づいて Entrust SSL Web Server 証明書を作成します。かかる要求書に応じて作成された Entrust SSL Web Server 証明書には、Entrust SSL Web Server CA によるデジタル署名が付加されるものとします。

Entrust SSL Web Server 証明書を発行する権限は、Entrust が認可した CA だけに与えられます。Entrust SSL Web Server 証明書を発行する権限が複数の CA に与えられている場合には、Entrust はかかる権限を認定した CA のリストをリポジトリに掲載します。

1.3.2 登録局 (RA)

Entrust SSL Web Server PKI において、Entrust SSL Web Server CA のもとで運営される登録局(RA)は、申請者から Entrust SSL Web Server 証明書の申し込みを受理し、Entrust SSL Web Server 証明申込書などに含まれる識別情報の検証を行います。Entrust SSL Web Server CA のもとで運営される RA は、提供された情報を Entrust ポリシ認証局

によって規定された手続きに従って検証した後、Entrust SSL Web Server CA に対して、申請者に Entrust SSL Web Server 証明書を発行するように要求することができます。Entrust SSL Web Server 証明書の発行を求める要求書を Entrust SSL Web Server CA に送付する権限は、Entrust が認定した RA だけに与えられます。Entrust SSL Web Server 証明書に関するかかる職務を遂行する権限が複数の RA に与えられている場合には、Entrust はかかる権限を認定した RA のリストをリポジトリに掲載します。

1.3.3 エンドエンティティ

Entrust SSL Web Server PKI のエンドエンティティは下記より構成されています。

1. 申請者：申請者とは、Entrust SSL Web Server 証明書を申請したが、まだ発行を受けていない人、法人、あるいは組織をいいます。
2. 加入者：加入者とは、Entrust SSL Web Server 証明書を申請し、発行された人、法人、もしくは組織をいいます。
3. 信頼当事者：信頼当事者とは、加入者の身元と公開鍵の有効性を検証したり、かかる公開鍵を使って加入者との間で暗号化メッセージのやり取りをする目的で、Entrust SSL Web Server 証明書または Entrust リポジトリに登録されている他の情報を信頼もしくは利用する人、法人、または組織です。

1.3.4 適用可能性

この Entrust SSL Web Server CPS は、Entrust SSL Web Server CA によって発行された Entrust SSL Web Server 証明書に適用されます。Entrust SSL Web Server 証明書は、SSL をベースとしたサービスを提供する Web サーバが利用するために発行されます。Entrust.net SSL Web Server 証明書は、SSL の拡張子を持つ X.509 v3 に準拠しています。

1.4 連絡先の詳細

1.4.1 仕様管理部門

Entrust SSL Web Server CPS は、Entrust 運営責任者によって管理され、Entrust ポリシ認証局によって決められた方針に従っています。

1.4.2 連絡先

Entrust SSL Web Server 証明書に関する質問の連絡先は：

Entrust Inquiries
1000 Innovation Drive
Ottawa, Ontario
Canada K2K 3E7
Tel: 1-877-368-7483
Fax: 1-877-839-3538
E-mail: tsite.entrust@Entrust.net

2 一般条項

2.1 義務

2.1.1 CA の義務

Entrust SSL Web Server CA は下記を行うものとします。

- (1) Entrust SSL Web Server CPS の条件に基づいて CA サービスを提供すること。
- (2) かかる Entrust SSL Web Server CA により認定された RA から要求書を受理したうえで、Entrust SSL Web Server CPS の定める諸条件に従って Entrust SSL Web Server 証明書を発行すること。
- (3) Entrust SSL Web Server CPS の定める諸条件に従って Entrust SSL Web Server 証明書を発行し、さらに Entrust SSL Web Server 証明書 CRL を発行して Entrust リポジトリに公表し閲覧可能にすることによって、Entrust SSL Web Server 証明書の失効に関する情

報を開示すること。

(4) Entrust SSL Web Server CPS の条件に従って定期的に Entrust Web Server 証明書 CRL の発行および公表をすること。

(5) Entrust SSL Web Server CA のもとで運営される RA から要請を受け次第、Entrust SSL Web Server CPS の条件に従って Entrust SSL Web Server 証明書を失効処理すること。

Entrust SSL Web Server CA の運営に際して Entrust は、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に定められた義務を履行する 1 人または複数の代理人もしくは 1 つまたは複数の代行業者を利用することができますが、ただしその場合にも、かかる義務の履行責任は Entrust が負うものとします。

2.1.2 RA の義務

Entrust SSL Web Server CA のもとで運営される RA は下記を行うものとします。

(1) Entrust SSL Web Server CPS の条件に従い Entrust SSL Web Server 証明書の申し込みを受領すること。

(2) Entrust SSL Web Server CPS の定める諸条件に従って、Entrust SSL Web Server 証明書の発行を申請する申請者から提示された情報の検証を行い、かかる情報の有効性が立証されたら、Entrust SSL Web Server 証明書の発行を求める要求書を Entrust SSL Web Server CA に送付すること。

(3) Entrust SSL Web Server CPS の条件に従って、加入者からの Entrust SSL Web Server 証明書の失効要請を受領し、かかる要請の有効性が立証されたら、Entrust SSL Web Server 証明書の失効を求める要求書を Entrust SSL Web Server CA に送付すること。

(4) Entrust SSL Web Server CPS の条件に従って、Entrust SSL Web Server 証明書が加入者に発行済みであることを加入者に通知すること。

(5) Entrust SSL Web Server CPS の条件に従って、加入者に加入者の Entrust SSL Web Server 証明書が失効処理されたこと、あるいは間もなく期限切れとなる旨を通知すること。

Entrust は、Entrust 直営の RA に関して Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に定められている義務を履行する 1 人または複数人の代理人もしくは 1 つまたは複数の代行業者を使用することができますが、ただしその場合にも、かかる義務の履行責任は Entrust が負うものとします。Entrust は、Entrust SSL Web Server CA の RA として活動する独立の第三者を任命することができます。かかる独立の第三者 RA は、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に定められた自己の義務の履行責任を負うものとします。第三者 RA は、Entrust SSL Web Server CA が認定する RA として活動するに当たって自己の義務を履行するために 1 人または複数人の代理人または 1 つまたは複数の代行業者を使用することができます。ただしその場合にも、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に定められたかかる代理人または代行業者の義務の履行責任は、かかる第三者 RA が負うものとします。Entrust は、(1)Entrust SSL Web Server 証明書の取扱いと(2)Entrust SSL Web Server 証明書に関連するサービスの提供を請け負う再販者および販売協業者を任命することができます。その場合、かかる再販者および販売協業者は、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に定められた自己の義務の履行について責任を負うものとします。Entrust は、かかる再販者および販売協業者の義務について履行責任を負うものではありません。再販者および販売協業者は、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に定められた自己の義務を履行するために 1 人または複数人の代理人もしくは 1 つまたは複数の代行業者を使用することができます。ただしその場合にも、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に定められたかかる代理人または代行業者の義務の履行責任は、再販者および販売協業者が負うものとします。独立の第三者 RA、再販者、および販売協業者は、Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書に定められた(1)表明、保証、または条件付けの否認、(2)責務の制限、(3)申請者、加入者、および信頼当事者による表明および保証、ならびに(4)申請者、加入者、および信頼当事者による補償に伴う便益を享受する権利を有します。

2.1.3 加入者の義務

加入者と申請者は下記を行うものとします。

- (1)公開鍵暗号と Entrust SSL Web Server 証明書を含む証明書の使用について理解し、必要に応じて適切な教育を受けること。
- (2)Entrust または独立の第三者 RA との通信に際しては、誤謬、不実、遺漏のない正確な情報を提示すること。
- (3)加入者の Entrust SSL Web Server 証明書あるいは申請者の Entrust SSL Web Server 証明書申請に関連して使用する鍵ペアは、新しく、安全で、かつ暗号的に強固なものを生成すること。
- (4) Entrust SSL Web Server CPS および加入同意書のすべての条件を理解し合意すること。
- (5) Entrust SSL Web Server 証明書の内容の修正を行わないこと。
- (6) Entrust SSL Web Server CPS および該当法規の条件に従って、合法かつ承認された目的のみに Entrust SSL Web Server 証明書を使用すること。
- (7) Entrust SSL Web Server 証明書の対象としてリストされた人、法人、あるいは組織を代表するものとして Entrust SSL Web Server 証明書を使用すること。
- (8)ハードウェアトークンまたはディスクのいずれかに加入者または申請者の秘密鍵を保管し、さらに、使用しない場合は加入者または申請者のコンピュータから装置を切り離すことによって鍵を保護すること。
- (9)Entrust SSL Web Server 認証申請書の記載情報に変更のある時、もしくは状況の変化によりかかる申請書の記載情報の正確性が損なわれると見なし得る時には、かかる変更または変化を Entrust に対して、あるいは申請者がかかる申請書を独立の第三者 RA に提出している場合にはその第三者 RA に対して、常識的に可能な限り早急に通知すること。
- (10)加入者の Entrust SSL Web Server 証明書の記載情報に変更のある時、もしくは状況の変化によりかかる証明書の記載情報の正確性が損なわれると見なし得る時には、かかる変更または変化を Entrust に対して、あるいは加入者がかかる証明書を独立の第三者 RA を通じて受領している場合にはその第三者 RA に対して、常識的に可能な限り早急に通知すること。
- (11)加入者の Entrust SSL Web Server 証明書の記載情報に変更のある時、もしくは状況の変化によりかかる証明書の記載情報の正確性が損なわれると見なし得る時には、ただちにその証明書の使用を停止すること。
- (12)加入者または申請者の秘密鍵が安全性の喪失の事態に晒されている時、もしくはその可能性のある時には、ただちにその旨を Entrust に対して、あるいは加入者が自己の Entrust SSL Web Server 証明書を独立の第三者 RA から受領している場合にはその第三者 RA に対して通知し、かかる証明書の失効手続を要請すること。
- (13)(a)加入者の Entrust SSL Web Server 証明書が期限満了もしくは失効した時、あるいは (b)かかる Entrust SSL Web Server 証明書で認証されている公開鍵に対応する秘密鍵が安全性の喪失の事態に晒されている時、もしくはその可能性のある時には、ただちにかかる証明書の使用を停止し、Web サーバから削除すること。
- (14)加入者の Entrust SSL Web Server 証明書は常に 1 つの WWW サーバ上でのみ使用すること。
- (15)加入者の Entrust SSL Web Server 証明書に記載されている公開鍵に対応する秘密鍵を使って他の証明書に署名しないこと。
- (16)所与の状況の中で Entrust SSL Web Server 証明書を使用することが Entrust SSL Web Server 証明書のセキュリティ・レベルと信頼性に照らして適当であるか否かについては、加入者または申請者の独自の裁量によって判断すること。

Entrust SSL Web Server 証明書とその関連情報の輸出入や利用は規制の対象になります。加入者は、Entrust SSL Web Server 証明書またはその関連情報の輸出入や利用に携わる自己の権利に適用されるすべての法律および規則を遵守しなければなりません。加入者は、Entrust SSL Web Server 証明書またはその関連情報の輸出入や利用に携わるために必要なすべてのライセンスと許認可を取得する責任を有します。Entrust SSL Web Server 証明書の作成やそれに関連する作業に使用される暗号化手法、ソフトウェア、ハードウェア、およびファームウェア（総じて「技術」と呼ぶ）もまた、輸出入や利用の規制の対象になり

ます。かかる技術またはその関連情報の輸出入や利用に携わる自己の権利に適用されるすべての法律および規則を遵守しなければなりません。加入者は、かかる技術または関連情報の輸出入や利用に携わるために必要なすべてのライセンスおよび許認可を取得する責任を有します。

2.1.3.1 加入者および申請者の明示および保証

加入者または申請者は Entrust に下記のことを明示し、保証します。

- (1) 加入者または申請者が Entrust または独立の第三者 RA に提供するすべての情報は、正確で、誤り、脱落、または不実表示を含まないこと。
- (2) Entrust SSL Web Server 証明書の申請に関連して加入者や申請者が提出する公開鍵に対応する秘密鍵は、強固な暗号技術を用いて作られたものであり、破られていないこと。
- (3) Entrust SSL Web Server 証明書の申請に関連して加入者や申請者が Entrust または独立の第三者 RA に提供する情報(ドメイン名やディステイングィッシュネーム等を含む)は、いかなる人、法人あるいは組織の知的所有権やその他の権利を侵害、不正流用、希釈化、不正競合あるいはその他に違反していないこと。
- (4) 申請者の Entrust SSL Web Server 認証申請書の記載情報に変更のある時、もしくは状況の変化によりかかる申請書の記載情報の正確性が損なわれると見なし得る時には、申請者はかかる変更または変化を Entrust SSL Web Server に対して、あるいは申請者がかかる申請書を独立の第三者 RA に提出している場合にはその第三者 RA に対して、常識的に可能な限り早急に通知すること。
- (5) 加入者の Entrust SSL Web Server 証明書の記載情報に変更のある時、もしくは状況の変化によりかかる証明書の記載情報の正確性が損なわれると見なし得る時には、加入者はただちにその証明書の使用を停止すること。
- (6)(a) 加入者の Entrust SSL Web Server 証明書が期限満了もしくは失効した時、あるいは (b) かかる Entrust SSL Web Server 証明書で認証されている公開鍵に対応する秘密鍵が安全性の喪失の事態に晒されている時、もしくはその可能性のある時には、加入者はただちにかかる証明書の使用を停止し、Web サーバから削除すること。
- (7) 加入者や申請者は危険なあるいは非合法的な活動(不法活動を含む)のために Entrust SSL Web Server 証明書をを用いないこと。

2.1.3.2 加入者による通告に関する要件

信頼当事者に関する加入者の WWW サイト上の目立ちやすい場所(例えば、加入者の WWW サイトの「法的事項」または「否認」の欄)に下記の通告文を掲示しなければなりません。

「Entrust SSL Web Server 証明書に対する信頼は、Entrust SSL Web Server CPS(www.entrust.net/CPS) および信頼当事者の同意書(www.entrust.net/customer/relyingparty.htm)の定める諸条件に基づくものです。Entrust SSL Web Server 証明書を信頼することは、Entrust SSL Web Server CPS および信頼当事者の同意書の定める諸条件の承諾を構成するものとします。」

2.1.4 信頼当事者の義務

信頼当事者は下記を行うものとします。

- (1) 公開鍵暗号および Entrust SSL Web Server 証明書を含む証明書の使用について理解し、必要に応じて適切な教育を受けること。
- (2) Entrust SSL Web Server CPS および信頼当事者の同意書の条件を理解しかつ合意すること。
- (3) ITU-T Rec. X.509: 1997 | ISO/IEC 9594-8(1997)に規定された認証経路の確認手順に従って、重大な拡充事項や承認済みの技術正誤表を適宜考慮に入れながら、CRL の利用を含めて Entrust SSL Web Server 証明書の検証を行うこと。
- (4) Entrust SSL Web Server 証明書が期限切れや失効に至っていない場合、ならびに信頼できるルート上に適切な信頼の連鎖が確立可能である場合に限り、Entrust SSL Web Server 証明書を信頼して使用すること。
- (5) Entrust SSL Web Server 証明書によって検証されたデジタル署名を独自に判断し、信

頼すること。但し、かかる信頼が Entrust SSL Web Server 証明書および Entrust SSL Web Server 証明書を使用した取引の価値にかかわる場合は、その正当性の決定を含んだ状況下において信頼が合理的な場合のみとすること。

Entrust SSL Web Server 証明書とその関連情報の輸出入や利用は規制の対象になります。信頼当事者は、Entrust SSL Web Server 証明書またはその関連情報の輸出入や利用に携わる自己の権利に適用されるすべての法律および規則を遵守しなければなりません。信頼当事者は、Entrust SSL Web Server 証明書またはその関連情報の輸出入や利用に携わるために必要なすべてのライセンスと許認可を取得する責任を有します。Entrust SSL Web Server 証明書の作成やそれに関連する作業に使用される暗号化手法、ソフトウェア、ハードウェア、およびファームウェア（「技術」）もまた、輸出入や利用の規制の対象になります。信頼当事者はかかる技術またはその関連情報の輸出入や利用に携わる自己の権利に適用されるすべての法律および規則を遵守しなければなりません。信頼当事者は、かかる技術または関連情報の輸出入や利用に携わるために必要なすべてのライセンスおよび許認可を取得する責任を有します。

2.1.4.1 信頼当事者の明示および保証

信頼当事者は Entrust に次のことを明示および保証します。

- (1)信頼当事者は、証明書が信頼するに足るかを判断する前に、Entrust SSL Web Server 証明書が有効期限切れまたは失効していないこと、およびルートへの適切な信頼の連鎖が確立できることも含め、Entrust SSL Web Server 証明書が適切であることを確認すること。
- (2)信頼当事者は、失効または有効期限切れの Entrust SSL Web Server 証明書を信頼しないこと。
- (3)信頼当事者は、信頼できるルートを追跡確認できない Entrust SSL Web Server 証明書を信頼しないこと。
- (4)信頼当事者は、Entrust SSL Web Server 証明書および Entrust SSL Web Server 証明書を使用した取引の価値によってもたらされる信頼の性格を前提として、当該信頼が合理的かどうかを決定することを含め、当該状況下で Entrust SSL Web Server 証明書を信頼することが合理的であるかどうかの決定を、独自の判断で行うこと。
- (5)信頼当事者は危険なあるいは非合法的な活動（不法活動を含む）に対し Entrust SSL Web Server 証明書を使用しないこと。

2.1.5 保管義務

Entrust リポジトリは下記を行うものとしします。

- (1) Entrust SSL Web Server CPS の条件に従って、Entrust SSL Web Server CA が発行している Entrust SSL Web Server 証明書の発行・取消の情報を利用可能とすること。
- (2)Entrust SSL Web Server CPS の写し、ならびに Entrust SSL Web Server CA やその認定する RA によって提供される製品およびサービスに関連する他の情報を入手可能にすること。

2.2 責務

Entrust SSL Web Server 証明書または Entrust SSL Web Server 証明書に関連する Entrust のサービスを利用することが原因として、もしくはそれと関連して発生する損失、費用、経費、責務、損害賠償、クレーム、または和解金について、Entrust および Entrust SSL Web Server CA のもとで運営する独立の第三者 RA、再販者または販売協業者、もしくはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員が申請者、加入者、信頼当事者、またはその他の人、法人、組織に対して負うべき最大累積債務額は、Entrust SSL Web Server CPS により制限されます。この Entrust SSL Web Server CPS にはまた、制限付き保証、債務額の制限、ならびに表明、保証および条件付けの否認に関する規定も含まれています。

2.2.1 CA の責務

2.2.1.1 保証および保証限度

Entrust は、Entrust SSL Web Server CA の運営に関連して、加入者に対して以下の制限付き保証を行います。

- (1) Entrust SSL Web Server CA はこの Entrust SSL Web Server CPS に規定した手続に矛盾することなく公表およびリポジトリサービスを提供すること。
- (2) Entrust SSL Web Server CA はこの Entrust SSL Web Server CPS に規定した手続に矛盾することなく Entrust SSL Web Server 証明書の申し込みの確認を実施すること。
- (3) Entrust SSL Web Server CA はこの Entrust SSL Web Server CPS に規定した手続に矛盾することなく失効、期限切れ、および更新サービスを提供すること。

上記の定めにかかわらず、Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、または再販者または販売協業者、もしくはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員が申請者、加入者、信頼当事者、およびその他の人、法人、または組織に対して、以下の各事項に関連して表明、保証、条件付けを行うことはいかなる場合にも一切ありません。

- (1) 秘密鍵の安全性が喪失されているか否か、もしくは秘密鍵が確固とした暗号化手法を用いて作られたか否かを含め、Entrust SSL Web Server 証明書で認証されている公開鍵に対応する秘密鍵の生成および保管に用いる手法
 - (2) Entrust SSL Web Server 証明書と関連付けられるか、あるいはこれを活用する行為、業務、または処理を行う際に用いる暗号化手法または方法の信頼性
 - (3) ソフトウェアに関することすべて
 - (4) Entrust SSL Web Server 証明書発行の否認防止、あるいは Entrust SSL Web Server 証明書を使用することで推進される取引。
- これらのことに関する判断は、適用される法律による規制対象になります。

申請者、加入者、および信頼当事者は、Entrust SSL Web Server 証明書および Entrust SSL Web Server 認証申請書に関連する業務がインターネット、電話・通信回線およびネットワーク、サーバ、ファイアウォール、プロキシ、ルータ、スイッチ、およびブリッジなど（「電気通信設備」と呼ぶ）の通信インフラによる情報伝達に依存すること、そしてこの電気通信設備は Entrust もしくは Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者もしくはその下請業者、卸売業者、代理店、供給業者、従業員、または役員によって管理されるものではないことを認め、これに同意します。Entrust SSL Web Server 証明書、Entrust SSL Web Server 証明書の CRL、または Entrust SSL Web Server 認証申請書に関連する業務に過失、不履行、遅滞、中断、瑕疵、または違反があっても、それが電気通信設備に起因するものである限り、Entrust もしくは Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者、または販売協業者もしくはその下請業者、卸売業者、代理店、供給業者、従業員、および役員は一切責任を負うものではありません。

2.2.1.2 否認

2.2.1.1 項に特に定めのある場合は除き、Entrust または Entrust SSL Web Server CA の認定する独立の第三者 RA、あるいは再販者または販売協業者もしくはその下請業者、卸売業者、代理店、供給業者、従業員、または役員が何らかの表明を行ったり、保証や条件付けを提示することは、明示的、暗示的、あるいは合法的な方式によっても、また商標の利用やその他の手段によっても、一切ありません。また、Entrust、または Entrust SSL Web Server CA が認定する独立のすべての第三者 RA、あるいはすべての再販者または販売協業者もしくはそのすべての下請業者、卸売業者、代理店、供給業者、従業員、および役員は、市販可能性、権利侵害の防止、法的権利、満足な品質、あるいは用途に対する適合性についていかなる表明、保証、条件付けも行いません。

2.2.1.3 損失制限

Entrust SSL Web Server 証明書またはそれに関連するサービス(Entrust SSL Web Server 証明書の利用や Entrust SSL Web Server 証明書に対する信頼を含む)を原因として、あるいはこれに関連して Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、

再販者または販売協業者、あるいはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員が申請者、加入者、信頼当事者、もしくはその他の人、法人、または組織に対して負うべき累積債務総額は、1,000米ドル(\$1,000)を超えないものとします(「累積損害額の上限」)。この制限は、Entrust SSL Web Server 証明書またはそれに関連するサービスの結果として、あるいはこれに関連して発生する法律行為や申し立ての件数に関わらず、Entrust SSL Web Server 証明書の1件ごとに適用されるものとします。かかる制限は、契約に基づくにせよ(重大な違反を含む)、あるいは不法行為(過失を含む)または制定法に基づくにせよ、あるいは、直接的、間接的、例外的、法的、懲罰的、派生的、信頼に基づく、あるいは付随的な損害を含む他の債務理論に基づくにせよ、いかなる債務にも適用されるものです。

Entrust SSL Web Server 証明書または Entrust SSL Web Server 証明書に関して Entrust が提供するサービスから、あるいはそれらに関連して発生する債務が上記の本筋に規定の累積損害上限を超える場合、累積損害上限に基づいて利用できる金額は、正当な権限を持つ管轄裁判所によって命じられる場合を除き、最終的な紛争解決に一番早く達し賠償請求に、最初に割り当てられるものとします。いずれの場合も Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者、あるいはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は、請求者たちの割り当てに関わらず、Entrust SSL Web Server 証明書の累積損害上限を超えて支払う義務はないものとします。

いずれの場合も Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者、あるいはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は契約(基本的な違反を含む)、不法行為(過失を含む)、あるいはその他の責任理論から生じていようがなかろうが、付随する、特別な、懲罰的、間接的、信用あるいは派生的損害(ビジネスの損失、ビジネス機会の損失、営業権の損失、利益の損失、営業停止、データの損失、貯蓄の損失、あるいはその他類似の金銭的損失の損害を無制限を含む)に対して支払う義務はないものとします。

以上の定めは、本CPSに定める制限付き救済方法の本来の目的が機能していない場合でも、またEntrustまたはEntrust SSL Web Server CAが認定する独立の第三者RA、再販者または販売協業者、もしくはその下請業者、卸売業者、代理店、供給業者、従業員、または役員が前記損害の発生する可能性について予め忠告を受けていた場合でも、適用されます。

司法管轄によっては、派生的あるいは付随的損害に対する責任除外あるいは制限を許容していませんので、上に規定されたこれらの制限は、ある申請者、信頼当事者あるいはその他の人、法人、組織に適用されない場合があります。このCPSにおける責任の表示、保証、条件および制限の否認はEntrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書の基本的部分を構成します。すべての申請者、加入者、信頼当事者およびその他の人、法人、組織は、負債の表示、保証、および条件および制限のこれらの否認がない場合は、Entrust は加入者に Entrust SSL Web Server 証明書の発行しないであろうし、Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者、あるいはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は Entrust SSL Web Server 証明書に関してサービスを提供しないであろうし、またこれらの条項はリスクの正当な割り当てを規定していることを認めます。

2.2.1.4 その他の除外

下記のいずれかの場合は、制限無しに、Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者、あるいはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は Entrust SSL Web Server 証明書またはそれに関連するサービスの利用から、あるいは関連して発生する損失、コスト、費用、負債、損害、賠償請求あるいは和解金に対して申請者、加入者、信頼当事者、あるいはその他のいかなる者に対しても支払い義務がないものとします。

(1) Entrust SSL Web Server 証明書の発行が加入者のあるいはその他の人、法人、あ

- るいは組織の誤り、不実表示、あるいはその他の行為または脱落の結果なされた場合。
- (2) Entrust SSL Web Server 証明書が期限切れであるか失効された場合。
 - (3) Entrust SSL Web Server 証明書が修正か変更された場合。
 - (4) Entrust SSL Web Server 証明書の記載情報に変更が発生した後でも、あるいは状況の変化により Entrust SSL Web Server 証明書の記載情報が誤解の原因または不正確な情報になった後でも、加入者がかかる Entrust SSL Web Server 証明書の使用を停止しなかった場合。
 - (5) 加入者が Entrust SSL Web Server CPS または加入同意書に違反した場合、あるいは信頼当事者が Entrust SSL Web Server CPS または信頼当事者の同意書に違反した場合。
 - (6) Entrust SSL Web Server 証明書に関連する秘密鍵の安全性が損なわれた場合。
 - (7) Entrust SSL Web Server 証明書が Entrust SSL Web Server CPS によって許可された目的以外に用いられ、あるいは該当法規に違反して用いられる場合。

Entrust または Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者または販売協業者もしくはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は、自己が Entrust SSL Web Server 証明書の発行または発行要求を拒絶したことが原因で、あるいはそれに関連して発生する損失、費用、債務、経費、損害、クレーム、または和解金については、申請者、加入者、もしくはその他の人、法人、または組織に対して責務を負うものではありません。Entrust または Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者、販売協業者、もしくはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は、Entrust SSL Web Server 証明書の発行または発行要求における遅滞が原因で、あるいはそれに関連して発生するいかなる損失、費用、債務、経費、損害、クレーム、または和解金についても、申請者、加入者、もしくはその他の人、法人、または組織に対して責務を負うものではありません。

Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者、あるいはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は、いかなる場合も、Entrust SSL Web Server 証明書あるいは Entrust SSL Web Server 証明書の内容がいかなる管轄下にある人、法人あるいは組織の特許、商標、著作権、業務上の秘密、あるいはその他の知的財産権や他の権利を侵害、不正流用、希釈化、不正競合または違反する訴訟行為あるいは申し立てからあるいは関連して発生する損失、コスト、費用、負債、損害、賠償請求あるいは和解金に対して、加入者、信頼当事者、あるいはその他のいかなる人、法人あるいは組織へ支払う義務を負わないものとします。

2.2.1.5 危険な活動

Entrust SSL Web Server 証明書 と Entrust SSL Web Server 証明書に関して Entrust によって提供されるサービスは、危険な活動において、あるいは連携しての使用や核施設、航空機の航行、あるいは通信装置、航空交通管制、医療装置あるいは直接生命維持装置の運転を含む、フェールセーフの性能を要求する使用向けに設計、製造あるいは意図されていません。Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者、あるいはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は明示的であれ、黙示的であれ、法律上であれ、商標を利用し、あるいはその他の方法であれ、上記の使用の表示、保証あるいは条件を明確に否認します。

2.2.2 RA の責務

Entrust SSL Web Server CA に関してセクション 2.2.1 で適用されているのと同じ責務の条項が Entrust が直営する RA、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者、販売協業者、あるいはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員に関して適用されるものとします。

2.3 財務上の責任

加入者および信頼当事者は、加入者または信頼当事者が参加する取引または Entrust SSL

Web Server 証明書に関して Entrust によって提供されるサービスに対してかかる加入者、信頼当事者およびその他の人、法人、組織に対する財務上の結果に対して責任を有するものとし、Entrust は Entrust SSL Web Server 証明書あるいは Entrust SSL Web Server 証明書に関連して Entrust によって提供されるサービスを利用して完了した取引の財務上の有効性に関する表示は行わず、また保証や条件も与えません。また Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者、あるいはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は Entrust SSL Web Server 証明書または Entrust SSL Web Server 証明書に関連して Entrust により提供されるサービスの使用または信頼に関して明示的に規定されている場合を除き、責任を有しないものとし、

2.3.1 信頼当事者による免責

信頼当事者は、下記の場合を含め、Entrust SSL Web Server 証明書またはそれに関連するサービスを利用または信頼することが原因で、あるいはそれに関連して発生する債務、損失、費用、経費、損害、クレーム、および和解金（弁護士料、訴訟費用、および鑑定料を含む）のすべてを補償し、Entrust または Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者または販売協業者、もしくはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員（総称的に「免責当事者」と呼ぶ）になんらの損害も与えないものとし、

(1) 信頼当事者が Entrust SSL Web Server 証明書の有効性について適正な確認手を怠った場合。

(2) 信頼当事者が期限切れまたは失効した Entrust SSL Web Server 証明書を信頼した場合。

(3) Entrust SSL Web Server CPS、加入同意書、信頼当事者の同意書、および適用法規により許容されない仕方で Entrust SSL Web Server 証明書を利用した場合。

(4) 信頼当事者が Entrust SSL Web Server 証明書を信頼するに当たって妥当な状況判断を行わなかった場合。

(5) 信頼当事者による Entrust SSL Web Server 証明書または Entrust SSL Web Server 証明書の記載情報への信頼が、いずれの司法管轄区内であれ何者かの知的所有権またはその他の権利を侵害、不正流用、または希釈化したり、あるいはかかる権利との不正競争やその他の侵害行為に相当するとのクレームまたは申し立てが発生した場合。

以上の定めに関わらず、前記の免責当事者による故意の違法行為が原因で、あるいはそれに関連して発生する債務、損失、費用、経費、損害、クレーム、および和解金（弁護士料、訴訟費用、および鑑定料を含む）については、信頼当事者はかかる免責当事者に対して補償義務を負うものではありません。

2.3.1.1 加入者による免責

加入者は、下記の場合を含め、Entrust SSL Web Server 証明書またはそれに関連するサービスを利用または信頼することが原因で、あるいはそれに関連して発生する債務、損失、費用、経費、損害、クレーム、および和解金（弁護士料、訴訟費用、および鑑定料を含む）のすべてを補償し、Entrust または Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者または販売協業者、もしくはそれらの下請業者、卸売業者、従業員、または役員（総称的に「免責当事者」と呼ぶ）になんらの損害も与えないものとし、

(1) Entrust SSL Web Server 証明書の使用あるいは申請にあたって加入者が不実表示を行った場合。

(2) Entrust SSL Web Server 証明書の内容に加入者が修正を行った場合。

(3) Entrust SSL Web Server CPS、加入同意書、信頼当事者の同意書、および適用法規により許容されない仕方で Entrust SSL Web Server 証明書を利用した場合。

(4) 加入者の Entrust SSL Web Server 証明書公開鍵に対応する秘密鍵の損失、開示、危険にさらすこと、あるいは無許可使用を防止するのに必要な予防的注意を加入者が取ることができない場合。

(5) 加入者による Entrust SSL Web Server 証明書または Entrust SSL Web Server 証明書の記載情報への信頼が、いずれの司法管轄区内であれ何者かの知的所有権またはその他の権利を侵害、不正流用、または希釈化したり、あるいはかかる権利との不正競争やその他の侵害行為に相当するとの申し立てが発生した場合。

以上の定めに関わらず、前記の免責当事者による故意の違法行為が原因で、あるいはそれに関連して発生する債務、損失、費用、経費、損害、クレーム、および和解金（弁護士料、訴訟費用、および鑑定料を含む）については、加入者はかかる免責当事者に対して補償義務を負うものではありません。

2.3.2 信頼関係

Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書のいかなる規定も、Entrust SSL Web Server または Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者または販売協業者もしくはその下請業者、卸売業者、代理店、供給業者、従業員、または役員をして、申請者、信頼当事者、もしくはその他の人、法人、または組織の受託者、提携者、代理店、第三者債務者、または法律上の代表者に選任するものではなく、また、いかなる目的であれ、Entrust または Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者または販売協業者、もしくはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員と申請者、信頼当事者、もしくはその他の人、法人、または組織との間の信頼関係を創出するものではありません。Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書のいかなる規定も、加入者、申請者、信頼当事者、もしくはその他の第三者に対して、Entrust または Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者または販売協業者、もしくはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員に代わって行動し、あるいはその義務または責務の策定または代行し、もしくは表明を行う権限を付与するものではありません。

2.3.3 管理手順

規定なし。

2.4 解釈および執行

2.4.1 準拠法

法律や規則が矛盾する場合を除き、オンタリオ州の州法が Entrust SSL Web Server CPS、すべての同意書およびすべての信頼当事者同意書の解釈、有効性、執行性および履行を支配するものとし、Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書への商品の国際販売契約に関する国連条約を適用することは、明示的に除外されています。代替の紛争解決手続きにより解決されない Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書に関する紛争、あるいは Entrust SSL Web Server 証明書あるいは Entrust SSL Web Server 証明書に関して Entrust によって提供されるサービスに関する紛争は、オンタリオ州、オタワの地方、あるいは連邦裁判所に持ち込まれるものとし、各人、法人、あるいは組織はこの契約書により、かかる裁判所がかかる紛争に対して人的および排他的管轄権を持つものとするに合意します。いかなる問題であれ、州または連邦裁判所に持ち込まれた場合には、申請者、加入者、および信頼当事者は自己の陪審裁判権を放棄します。

2.4.1.1 不可抗力

Entrust ならびに Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者および販売協業者もしくはその下請業者、卸売業者、代理店、供給業者、従業員、および役員は、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に定める条件の履行遅滞、不履行、または違反の結果として、あるいはそれに関連して損失、費用、経費、債務、損害、クレーム、または和解金が発生しても、かかる遅滞、不履行、または違反が天災または公敵の所業、暴動および内乱、戦争、事故、火災、ストライキおよびその他の（Entrust が容認するとしなないとにかかわらず）労働争議、通商停止、裁判所命令の実施、上位認証機関の怠慢または懈怠、輸出許可や必要な労働力、資材、エネルギー、公益事業設備、部品、機械装置類の入手の不備または不能、行政当局または軍事当局の行為を含む不可抗力を原因とするものである場合には、この CPS に基づく懈怠の責めや債務を負うものではありません。

2.4.1.2 解釈

この Entrust SSL Web Server CPS において、「セクション」と参照されているものは、すべてこの Entrust SSL Web Server CPS のセクションを指します。この Entrust SSL Web Server CPS で用いられているように、中性の代名詞およびその変化は女性および男性を含むと見なされるものとし、また単数で用いられているすべての用語は、文脈が要求する場合、複数にあるいはその逆を含むと見なされるものとし、また「hereof」「herein」「hereunder」等の単語や、その他類似の意味の単語は全体として、この CPS をさしており、これらは適時修正または補足され、この Entrust SSL Web Server CPS に含まれている下位項目を指すことはありません。本 CPS で用いられている「including」の単語は排他的であることを意図せず、「制限なしで含んでいる」ことを意味しています。

2.4.2 分離、存続、合併、通知

2.4.2.1 分離

Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書の各々は、出来る限り、該当法律に基づき効果的かつ有効な方法にて解釈されるものとし、特定の事実や状況に対して Entrust SSL Web Server CPS、加入同意書、あるいは信頼当事者の同意書の条項あるいはその一部を適用することは、仲裁者や正当な権限を持つ管轄の裁判所によって無効または執行不能とされる場合、(1) その他の特別な事実や状況に適用されるような条項の正当性は、いかなる場合も影響を受けないし、損なわれないものとし、(2) かかる条項はその意向を効果的にするため最大可能な程度に執行されるものとし、またかかる条項を有効および執行可能とするのに必要な範囲まで、新たな行為なくして修正されるものとし、

確実性を高めるために、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書の中で、(1)債務または損害額の制限、(2)表明、保証、条件付け、または責務の否認、または(3)免責に関するすべての規定は Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書における他の規定から分離可能であることを明示的に意味するのであり、かつ、そのように解釈され、実施されなければならないことが明確に認識され、かつ同意されています。

2.4.2.2 存続

「定義」の条項ならびに 2.1.3.1、2.1.4.1、2.2、2.3、2.4、2.8、2.9、3.1.5、3.1.6、4.6、および 8.2 項の規定は、Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書の解除後または満了後も存続するものとし、Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書の解約後に存続する条項を参照する場合には、かかる条項の細目もすべて含んでいるものとし、Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書の解除後または満了後も、支払いに関する義務はすべて存続します。

2.4.2.3 合併

Entrust SSL Web Server CPS、加入同意書および信頼当事者の同意書は主題に関して Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者および販売協業者もしくはその下請業者、卸売業者、代理店、供給業者、従業員、役員、および申請者、加入者、信頼当事者またはその他の人、法人、組織の権利と義務のすべてを記述するものとし、かかる権利と義務は、口頭あるいは文書のいずれでなされたものであれ、いかなる性質の事前の合意、通信あるいは了解によって拡大されたり減じられたいしないものとし、Entrust または Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者および販売協業者もしくはその下請業者、卸売業者、代理店、供給業者、従業員、および役員の権利および義務は口頭で修正されたり、権利放棄されたりできないものとし、正当に権限が与えられた代表の Entrust によって署名されあるいは認証された書面でのみ修正可能とします。

2.4.2.4 規定の相反

Entrust SSL Web Server 証明書またはそれに関連するサービスに関して、Entrust SSL Web Server CPS の規定が、Entrust または Entrust SSL Web Server CA が認定する独立

の第三者 RA と加入者または信頼当事者との間の書面による明示的な合意と相反する場合には、かかる後者の書面による明示的な合意が優先されるものとします。この Entrust SSL Web Server CPS の規定と加入同意書または信頼当事者の同意書の規定との間に矛盾がある場合には、Entrust SSL Web Server CPS の諸条件が適用されるものとします。

2.4.2.5 権利放棄

Entrust がこの Entrust SSL Web Server CPS、加入者と Entrust との加入同意書、または信頼当事者と Entrust との同意書の規定を施行しないこと、あるいは、Entrust が申請者、加入者、信頼同意者、もしくはその他の人、法人、または組織に対してかかる規定の履行を要求しないことをもって、かかる規定に関する現在または将来の権利放棄と解釈されるものではなく、また、Entrust がその後かかる個々の規定を施行する能力に影響を及ぼすものでもありません。Entrust SSL Web Server CPS、加入者と Entrust との加入同意書、または信頼当事者と Entrust との同意書の規定、条件、または要件に関する Entrust の明示的権利放棄は、かかる規定、条件、または要件に対する将来の遵守義務の放棄を構成するものではありません。独立の第三者 RA または Entrust SSL Web Server CA が認定する再販者（「RA」）がこの Entrust SSL Web Server CPS、加入者とかかる RA との加入同意書、または信頼当事者とかかる RA との同意書の規定を施行しないこと、あるいは、Entrust が申請者、加入者、信頼同意者、もしくはその他の人、法人、または組織に対してかかる規定の履行を要求しないことをもって、かかる規定に関する現在または将来の権利放棄と解釈されるものではなく、また、その RA がその後かかる個々の規定を実施する権能に影響を及ぼすものでもありません。Entrust SSL Web Server CPS、加入者と RA との加入同意書、または信頼当事者と RA との同意書の規定、条件、または要件に関する Entrust の明示的権利放棄は、かかる規定、条件、または要件に対する将来の遵守義務の放棄を構成するものではありません。

2.4.2.6 通知

Entrust SSL Web Server CPS、加入同意書、あるいは信頼当事者の同意書に従って加入者、申請者あるいは信頼当事者によって与えられる通知は、前払い受取郵便、ファクシミリ、あるいは翌日配達急行便によって下記指定の住所宛に書面にて行うものとし、また以下の通り有効となるものとする。(1)ファクシミリまたは急行便の場合は、翌営業日、また(2)受取郵便の場合、郵便寄宅日の5日後。Entrust SSL Web Server CPS、加入同意書、あるいは信頼当事者の同意書に従って、Entrust によって与えられる通知は、電子メールが Entrust にファイルされている加入者の最後の住所宛に送られるものとします。電子メールによる通知の場合、その通知は翌営業日に有効となるものとします。前払い領収済みの郵便、ファクシミリ、または翌日配達急行便による通知の場合には、その通知の手段によって(1)または(2)に定める通りに有効となります。

Entrust 社の通知住所：

Entrust Limited

1000 Innovation Drive

Ottawa, Ontario

Canada, K2K 3E7

Attention: Director Operations,

Fax: 1-877-839-3538

2.4.2.7 権利の譲渡

Entrust SSL Web Server 証明書、ならびに Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に基づいて与えられる権利は、その加入同意書または信頼当事者の同意書を締結している当の申請者、加入者、または信頼当事者だけに適用されるものであり、これを譲渡、販売、移譲、またはその他の仕方でも処分することは、それが任意と不任意いずれによるものであれ、法律の運用に基づくものであれ、またその他いかなる手段によるものであれ、Entrust もしくはかかる申請者、加入者、または信頼当事者と契約を結んでいる Entrust SSL Web Server CA 認定の RA の書面による事前同意なしには一切できません。かかる事前同意なしに譲渡もしくは移譲が企図されても無効と見なされ、Entrust

SSL Web Server CPS、加入同意書、または信頼当事者の同意書に基づく、かかる申請者、加入者、または信頼当事者の権利は自動的に解除されるものとします。Entrust は、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書とそれらに基づく自己の権利および義務のすべてを譲渡、売却、移譲、もしくはその他の手段によって処分することは、(1)それが関連会社に対して行われる場合、あるいは(2)かかる CPS または加入同意書と関連する Entrust SSL Web Server の事業上の資産または株式のすべてもしくは実質的にすべての販売、合併、またはその他の移譲処置の一環として行われる場合には、容認されるものとします。以上の制限を条件として、本項は拘束力をもつものとし、場合によって Entrust SSL Web Server、Entrust SSL Web Server CA が認定する第三者 RA、申請者、加入者、および信頼当事者のうちのいずれかの公認の相続人および譲受人の利益に対して有効となります。

2.4.3 紛争解決手順

加入者または申請者と Entrust 間、あるいは信頼当事者と Entrust 間の紛争はオンタリオ州、オタワで行われる、米国仲裁協会の商業仲裁規則に従って仲裁に付託されるものとします。かかる紛争の解決が 30 日以内に仲裁により達成されない場合は、その紛争は拘束力を持つ仲裁へ付託されるものとします。仲裁人は仲裁についてすべての問題を決定する権利を有しているものとします。紛争は本条項によって修正されているとおり、米国仲裁協会の規則に従って仲裁により最終的に解決されるものとします。かかる仲裁は、Technology Panel から米国仲裁協会 (AAA) によって任命され、かつ電子商取引紛争に適切な知識を持つ AAA によって指名されたただ一人の仲裁人の面前で、オンタリオ州、オタワにて英語によって行われるものとします。仲裁人は抵触法の規定に関係なく、オンタリオ州の法律を適用するものとし、仲裁審理の終了日から 30 日以内に書面による判決を行うものとします。ただし、本件が仲裁に付託されてから 1 年以内になされるものとします。仲裁者の判定は拘束力を持ち、最終的なものとし、正当な管轄権を持つ裁判所に提訴することができます。各々の仲裁で、優勢な当事者が実際にかかった正当な弁護士料を含む、かかる仲裁におけるコストのすべてあるいは一部の裁定額を受け取る権利を有します。Entrust SSL Web Server CPS、加入同意書、あるいは信頼当事者の同意書の何ものも Entrust がセクション 2.4.3 に違反することなく、また (1) Entrust SSL Web Server 証明書の完全さに影響する危険性の申し立て、あるいは (2) Entrust SSL Web Server CPS、加入同意書、あるいは信頼当事者の同意書の条件違反の申し立てに関し、仲裁人の権力を縮小することなしに、正当な管轄権を持つ裁判所に一時的なあるいは不変の差し止め救済を申請することを妨げないものとします。仲裁あるいは訴訟の機関は、申請者、加入者あるいは信頼当事者より Entrust SSL Web Server CPS、加入同意書、あるいは信頼当事者の同意書に基づく義務を免除しないものとします。

2.4.3.1 仲裁および訴訟についての制限期間

Entrust SSL Web Server 証明書あるいは Entrust SSL Web Server 証明書に関し提供されるサービスに関連する紛争に関する、一切の仲裁あるいは法律訴訟は、(1) 紛争当事者の Entrust SSL Web Server 証明書の失効または取消後 1 年が過ぎるか、または (2) Entrust SSL Web Server 証明書に関する紛争となっているサービスあるいは諸サービスの規定日のうち、どちらか早い時期に始められるものとします。Entrust SSL Web Server 証明書あるいは Entrust SSL Web Server 証明書に関し提供されるサービスあるいは諸サービスに関連する紛争に関する、一切の仲裁あるいは訴訟が上記期間に始まらない場合は、かかる仲裁あるいは訴訟を起こすことを求めている当事者は、かかる仲裁あるいは訴訟の開始あるいは進行を禁じられるものとします。

2.5 サービスの料金

Entrust SSL Web Server 証明書に関連して Entrust が提供するサービスの料金は、Entrust リポジトリに定められています。これらの料金は変更されることがあり、その変更は、Entrust リポジトリに登録後ただちに発効するものとします。Entrust SSL Web Server 証明書に関連して独立の第三者 RA、再販者、および販売協業者が提供するサービスの料金は、かかる RA、再販者、および販売協業者が運営する Web サイト上に掲示されます。掲示された料金は変更されることがあり、その変更はかかる Web サイト上に掲示後ただちに発効

するものとしします。

2.5.1 証明書発行料金、更新料金

Entrust により請求される料金については Entrust リポジトリを参照してください。Entrust SSL Web Server CA が認定する RA、再販者、および販売協業者が請求する料金については、かかる RA、再販者、および販売協業者が運営する Web サイトを参照してください。

2.5.2 証明書アクセス料

Entrust により請求される料金については Entrust リポジトリを参照してください。Entrust SSL Web Server CA が認定する RA、再販者、および販売協業者が請求する料金については、かかる RA、再販者、および販売協業者が運営する Web サイトを参照してください。

2.5.3 失効あるいはステータス情報アクセス料

Entrust により請求される料金については Entrust リポジトリを参照してください。Entrust SSL Web Server CA が認定する RA、再販者、および販売協業者が請求する料金については、かかる RA、再販者、および販売協業者が運営する Web サイトを参照してください。

2.5.4 ポリシ情報などその他のサービス料金

Entrust により請求される料金については Entrust リポジトリを参照してください。Entrust SSL Web Server CA が認定する RA、再販者、および販売協業者が請求する料金については、かかる RA、再販者、および販売協業者が運営する Web サイトを参照してください。

2.5.5 払い戻し方針

Entrust、Entrust SSL Web Server CA が認定する RA、再販者、または販売協業者のいずれも、Entrust SSL Web Server 証明書またはそれに関連するサービスについて料金の払い戻しは致しません。

2.6 公表およびリポジトリ

Entrust は Entrust SSL Web Server 証明書および Entrust SSL Web Server CA、Entrust RA、Entrust SSL Web Server CA が認定する第三者 RA の運営に関連する、様々な情報を保存するのに用いられる Entrust リポジトリのメンテナンスを行います。Entrust SSL Web Server CPS および様々な他の関連情報は Entrust リポジトリに公表されます。Entrust SSL Web Server CPS はハードコピーで Entrust から入手可能です。

2.6.1 CA 情報の公表

以下の Entrust SSL Web Server 証明書の情報が Entrust リポジトリに公表されています。

- (1) Entrust SSL Web Server CPS
- (2) Entrust SSL Web Server 証明書の加入および信頼に関する情報および契約
- (3) Entrust SSL Web Server CA によって実施される Entrust SSL Web Server 証明書のすべての失効情報。

Entrust リポジトリで Entrust SSL Web Server 証明書と失効情報を公表するのに用いるデータのフォーマットは、その用途に推奨されている x.500 シリーズによって提供されるツールを用い定義された拡張と同様、推奨の x.500 (1997 年版) に規定されている関連固有データ構造の定義に従っています。

2.6.2 公表の頻度

Entrust SSL Web Server CPS はこの CPS のセクション 8 に規定された方針に従って再発行および公表される場合があります。

2.6.3 アクセスコントロール

Entrust SSL Web Server CPS は Entrust リポジトリで公表されます。Entrust SSL Web Server CPS の入手は、すべての申請者、加入者および信頼当事者に可能ですが、その修正は Entrust ポリシ認証局によってのみ可能とします。

2.6.4 リポジトリ

Entrust は Entrust SSL Web Server 証明書および CRL 情報にアクセスを許容するため、Entrust リポジトリを維持管理します。Entrust リポジトリ内の情報は Web インタフェースを通じてアクセス可能で、この Entrust SSL Web Server CPS に規定のとおり、Entrust によって定期的に更新されます。Entrust リポジトリは Entrust SSL Web Server 証明書に関する CRL およびその他の情報について唯一認可されたソースです。

2.7 準拠性監査

Entrust SSL Web Server CA、Entrust 直営の RA、および Entrust SSL Web Server CA が認定する独立の第三者 RA は、Entrust SSL Web Server CPS に定められている業務および手続に対する準拠状況について監査を受けるものとします。

2.7.1 準拠性監査の頻度

Entrust SSL Web Server CA、Entrust SSL Web Server 直営の RA、および Entrust SSL Web Server CA が認定する独立の第三者 RA は、Entrust SSL Web Server CPS に規定された、業務および手続に対して準拠しているかどうか年 1 回監査されるものとします。監査報告の結果、改善勧告が求められた場合、Entrust および該当する独立の第三者 RA はかかる監査報告を受領してから 30 日以内に是正措置を始めるものとします。

2.7.2 監査人の身元保証・資格

準拠性監査は認証および登録の評価において実証された能力を有する、公認会計士事務所によって行われるものとします。Entrust CA および RA の監査人としては Deloitte & Touche LLP が選任されています。

2.7.3 被監査部門と監査人の関係

Entrust SSL Web Server CA、Entrust 直営の RA、または Entrust SSL Web Server CA が認定する独立の第三者 RA に対する準拠性監査を実施するために選択された公認会計士事務所は、監査対象の法人から独立の立場になければなりません。

2.7.4 監査の対象となる主題

準拠性監査は Entrust SSL Web Server CPS に規定された方針および手続に対して、Entrust SSL Web Server CA、Entrust 直営の RA、または Entrust SSL Web Server CA が認定する独立の第三者 RA の準拠性を検査するものとします。

2.7.5 監査指摘事項に対する措置

改善勧告を指摘した監査報告を受領した時には、監査対象の Entrust SSL Web Server CA および Entrust 直営の RA、または Entrust SSL Web Server CA が認定する独立の第三者 RA は迅速な方法にてかかる指摘事項を是正する合理的な措置を取るものとします。

2.7.6 監査結果の報告

すべての準拠性監査の結果は、Entrust SSL Web Server CA が監査対象の場合には Entrust 運営責任者に、Entrust SSL Web Server CA の配下で Entrust が運営する RA が監査対象である場合には Entrust 運営責任者に、また Entrust SSL Web Server CA が認定する第三者 RA が監査対象である場合にはかかる RA の運営当局に報告するものとします。

2.8 機密性

Entrust または Entrust SSL Web Server CA が認定する独立の第三者 RA または再販者および販売協業者は、Entrust SSL Web Server 証明書の申請時に、申請者あるいは加入者により提出された申請者名または加入者名、あるいはその他の情報を開示したり販売した

りしないものとしします。ただし、この Entrust SSL Web Server CPS、加入同意書あるいは信頼当事者の同意書に規定されている範囲においてはこの限りではありません。Entrust または Entrust SSL Web Server CA が認定するすべての独立の第三者 RA、すべての再販者および販売協業者は、かかる情報が Entrust SSL Web Server CPS、加入同意書あるいは信頼当事者の同意書に規定された目的以外の目的で、利用されたり開示されたりするのを防ぐために相応の注意を払うものとしします。上記にもかかわらず、Entrust SSL Web Server 証明書の申請時に提供された情報のいくつかは Entrust SSL Web Server 証明書や CRL に組み込まれていることと、Entrust が Entrust リポジトリ内でかかる情報を一般に入手可能とする権利を有することを申請者と加入者は承認しています。

2.8.1 機密を保つべき情報の種類

Entrust SSL Web Server 証明書について加入、利用、あるいは信頼に必要とされる申請者、加入者あるいは信頼当事者によって提供される情報、および下記セクション 2.8.2 に記載の情報に含まれていない情報は、機密と見なされるものとしします。Entrust および Entrust SSL Web Server CA が認定する独立の第三者 RA は、Entrust SSL Web Server 証明書の申請において提供された情報の確認に際して、Entrust を援助している、あるいは Entrust SSL Web Server CA や Entrust RA の運営について Entrust を援助している、下請業者や代理人にかかる情報を開示する権利を有しているものとしします。機密と見なされる情報は、法的手続、司法手続、あるいは行政手続または法律により要求される他の方法に従って強制されないかぎり、開示されないものとしします。Entrust および Entrust SSL Web Server CA が認定する独立の第三者 RA は、かかる法的手続、司法手続、行政手続あるいは法律で要求されるその他の手続に関連して援助を与えてくれる、法律顧問および財務顧問に、また Entrust の合併、買収あるいは再編成に関連し弁護士、会計士、銀行および金融機関およびそれらの顧問にかかる情報を開示する権利を有するものとしします。

2.8.2 機密とみなされない情報の種類

Entrust SSL Web Server 証明書または CRL に記載されている情報は、機密情報とは見なされません。Entrust SSL Web Server CPS に含まれる情報も機密情報とは見なされません。以上の定めを制限することなく、(1)Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者、または販売協業者による漏洩がなくても知られている、あるいは知られ得る情報、(2)Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者が加入者以外の情報源から機密上または所有権上の制約なしに正確に知った、あるいは正確に知り得る情報、(3)Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者、または販売協業者が独自に創出した情報、または(4)加入者が開示を承諾した情報は、機密情報とは見なされません。

2.8.3 証明書の失効・停止情報の開示

Entrust SSL Web Server CA によって Entrust SSL Web Server 証明書の失効措置が取られた場合には、失効されたその Entrust SSL Web Server 証明書の連番が CRL の記入欄に記入されます。

2.8.4 法執行官への公表

Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者、または販売協業者は、機密と見なされる情報を適用される法律に従い法執行官に公表する権利を有しているものとしします。

2.8.5 民事手続上の開示に伴う公表

Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者、および販売協業者は、機密扱いにされている情報に関連する仲裁、訴訟、あるいはその他の法律上、訴訟上、または行政上の手続の過程において、かかる機密情報を開示することができます。かかる開示は、前記の機密情報の利用および開示範囲を、仲裁、訴訟、あるいはその他の法律上、訴訟上、または行政上の手続のために商道徳上合理的に要求される範囲内に規制するために裁判所が発する保護命令を取りつけるべく、Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者、または販売協業者が妥当な努力を払うことを条

件として容認されるものです。

2.8.6 所有者の要請に基づく開示

Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者、および販売協業者は、申請者、加入者、あるいは信頼当事者が Entrust、かかる RA、再販者、および販売協業者に提供した情報を、申請者、加入者、あるいは信頼当事者の要請を受け次第、開示することができます。

2.8.7 その他の情報公開状況

規定なし。

2.9 知的財産権

Entrust は、申請者あるいは加入者の財産のままとなっている、申請者あるいは加入者によって供給される情報、および Entrust SSL Web Server 証明書に含まれる情報を除き、すべての Entrust SSL Web Server 証明書における、証明書への、および証明書に基づく権利、権限、および利益（すべての知的財産権を含む）を保持します。すべての申請者および加入者は、Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書に従い、予期される諸目的のために、現在知られているか今後考案されるかを問わず、すべての手段およびすべての媒体を通じ、Entrust および Entrust SSL Web Server CA が認定するすべての RA に対し、かかる情報の使用、複製、修正、対外的な表示、および配布を行う非排他的な、世界中での、払い込み済み、使用料無料のライセンスの使用を許諾します。Entrust および Entrust SSL Web Server CA が認定するすべての RA はセクション 2.4.2.7 で意図されているとおり、Entrust による譲渡、移転あるいは付与に付随して、このライセンスを譲渡、移転あるいは付与する権利を有するものとします。Entrust は Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書に従い、かかる Entrust SSL Web Server 証明書が意図されているとおりに用いられるのを条件として、またさらに Entrust SSL Web Server 証明書が十分かつ正確に再現され、Entrust の明示の許可なしに、公に利用できるデータベース、リポジトリ、あるいはディレクトリに公表しないことを条件に、Entrust SSL Web Server 証明書を使用、複製および配布する非排他的、譲渡不能の権利を加入者と信頼当事者に許諾します。

本運用規定に明示的定めのある場合を除き、含意、禁反言、類推、その他によって別段の権利が付与されるとはみなされず、また、みなしてはならないものとします。状況に応じて Entrust はその単独裁量により、加入者向けに発行した Entrust SSL Web Server 証明書との併用のみの目的として、1 通または 2 通以上の相互認証証明書を同じその加入者のために用意することができます。Entrust は相互認証証明書に規定する、あるいはこれに関連もしくは準拠するすべての権利、権限、および権益（すべての知的財産権を含む）を保持します。

Entrust は、(1)Entrust SSL Web Server CPS の第 1 ページに記載されている著作権情報が Entrust SSL Web Server CPS のすべての写しに残存させ、かつ(2)Entrust SSL Web Server CPS の内容が完全かつ正確に複製することを条件として、Entrust SSL Web Server CPS の複製を許諾します。

Entrust SSL Web Server 証明書またはそれに関連するサービスが原因で、あるいはこれに関連して、いずれかの司法管轄区内の人、法人、または組織の特許権、商標権、著作権、企業秘密、またはその他の知的所有権、またはその他の権利の侵害、不法流用、希釈化、不正競争、もしくはその他の侵犯行為のクレームが発生した場合、それに起因もしくは関連して発生する損失、費用、債務、経費、損害、クレーム、または和解金については、Entrust または Entrust SSL Web Server CA が認定する独立の第三者 RA、あるいは再販者または販売協業者、もしくはそれらの下請業者、卸売業者、代理店、供給業者、従業員、または役員は、申請者、加入者、もしくは信頼当事者、またはその他の第三者に対して補償義務を負うものではありません。

3 識別および認証

3.1 初期登録

Entrust SSL Web Server 証明書を取得するためには、申請者は(1)機密保護および暗号上完全な鍵ペアを生成し、(2)Entrust SSL Web Server CPS および加入同意書の定める諸条件のすべてに同意し、(3)Entrust 直営の RA、または Entrust SSL Web Server CA が認定する独立の第三者 RA (「RA」) が要求する情報を正確に、しかも虚偽や疎漏なく提供するために、Entrust SSL Web Server 認証申請書に必要事項を記入して提出する必要があります。申請者が Entrust SSL Web Server 認証申請書に記入し、Entrust SSL Web Server CPS および加入同意書の定める諸条件を承諾したら、RA または RA の権限を与えられた第三者は、Entrust SSL Web Server 認証申請書に記載されている情報のいくつかについて制限付き検証を行います。RA によるこの制限付き検証で有効性が検証されたら、RA は、自己の単独の裁量により、Entrust SSL Web Server CA に対して Entrust SSL Web Server 証明書の発行を要求することができます。RA が Entrust SSL Web Server 証明書の発行要求を出すことを拒否する場合には、その RA は、(1)拒否の理由を電子メールで申請者に通知するための妥当な努力を払い、かつ(2)Entrust SSL Web Server 認証申請書に関連して支払われた金額を直ちに払い戻すものとします。Entrust SSL Web Server 認証申請書の有効性が検証されたら、RA は、Entrust SSL Web Server CA に対して Entrust SSL Web Server 証明書の発行要求書を提出し、Entrust SSL Web Server CA により Entrust SSL Web Server 証明書が発行されたら、その旨を電子メールで申請者に通知します。申請者には、当該 Entrust SSL Web Server 証明書を検索するための URL が紹介されます。Entrust SSL Web Server 証明書の発行後は、Entrust SSL Web Server、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者、もしくはその下請業者、卸売業者、代理店、供給業者、従業員、または役員のいずれも、Entrust SSL Web Server 認証申請書の記載情報について監視、調査、検証を続行する義務を負うものではありません。

3.1.1 名称の種類

Entrust SSL Web Server 証明書における利用者の名前は X.500 ディスティングィッシュネーム様式に合致します。Entrust SSL Web Server CA は下記の通り、単名規則を用いるものとします。

各 Entrust SSL Web Server 証明書は下記の情報を含むものとします。

(1) 「国名」(C) Entrust SSL Web Server 証明書のインストールを行う予定の Web サーバの構築化を計画している申請者が所在する国の 2 文字の ISO3166 コード。

(2) 「組織名」(O) とは、法人、会社、またはその他の法人からなる組織の名称です。自営者の場合には、この組織名は申請者の氏名としてもかまいません。

(3) 「組織単位名」(OU) は、任意選択の記入欄です。OU の欄は、組織内のさまざまな機構集団 (例えば、人事、マーケティング、開発の各部門) を区別するために使います。

(4) 「コモンネーム」(CN) は申請者が Entrust SSL Web Server 証明書をインストールする予定の Web サーバの DNS にて使用する完全に適格なホスト名。

3.1.2 名称が意味を持つ必要性

Entrust SSL Web Server 証明書中に用いられるコモンネームの有用性は、申請者が Entrust SSL Web Server 証明書をインストールする予定の Web サーバの DNS 内で使われる完全に適格なホスト名とします。

3.1.3 様々な名称様式の解釈規則

Entrust SSL Web Server 証明書の利用者はセクション 3.1.1 および 3.1.2 に規定されている通りに解釈されるものとします。

3.1.4 名称の独自性

名前は Entrust リポジトリ内の各利用者に対して曖昧でないように定義されているものとします。ディスティングィッシュネームの属性は、発行されている Web サーバに対して独自のものとし、二つの Entrust SSL Web Server 証明書が同じ被認証者名に割り当てられる

のを防ぐために用いられます。各 Entrust SSL Web Server 証明書はユニークな連番が付されます。これらの二つの要素を使用することは Entrust SSL Web Server 証明書の公開鍵が二つ以上の主体と関連づけられるのを防止するよう意図されています。

3.1.5 名称に関するクレームによる紛争の解決方法

Entrust SSL Web Server 証明書に記載される被認証者名は「先着順」に発行されます。Entrust SSL Web Server CA の配下にある RA は Entrust SSL Web Server 証明書に記載される被認証者名を承認するだけで、かかる情報の利用がいずれかの人、法人、または組織の知的財産権またはその他の権利を侵害、不正流用、または希釈化したり、もしくはこれと不正競争したり、あるいはその他の仕方でも侵害することになるかについては判断を下しません。Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA が、Entrust SSL Web Server 証明書の記載情報の利用に関連して加入者間、あるいは加入者と第三者の苦情申立て人との間の仲裁機関として行動したり、紛争解決に当たったりすることはありません。Entrust SSL Web Server CPS は、Entrust SSL Web Server 証明書の記載情報に関連して加入者または第三者苦情申立て人に手続上または法人上の権利を与えるものではありません。Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA のいずれも、Entrust SSL Web Server 証明書の記載情報を原因として発生する、加入者間または加入者と第三者苦情申立て人との間の紛争、あるいは加入者と Entrust SSL Web Server CA または Entrust SSL Web Server CA が認定する RA、もしくは第三者苦情申立て人と Entrust SSL Web Server CA または Entrust SSL Web Server CA が認定する RA との間の紛争に関連して、法律上または衡平法上の救済措置（差止命令による救済も含む）の対象から除外されるものではありません。Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA はそれぞれ、司法管轄区の仲裁機関または裁判所から正当に認証された Entrust SSL Web Server 証明書失効命令を受領した時点で、Entrust SSL Web Server 証明書を失効させる権利および失効を要求する権利を有するものとします。

3.1.6 商標の認識、認証および役割

Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA は、ある状況において、第三者原告の商標権を侵害する可能性のある利用者名を含んでいる Entrust SSL Web Server 証明書について措置を取ることがあります。第三者原告が Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA に(1)米国、カナダ、日本、オーストラリアあるいは EU 加盟国のうちの一国における主たる商標事務所での登録から 3 か月以内の商標登録で、更にかかる登録は依然として完全に効力を持っている認証の写し、(2)加入者の Entrust SSL Web Server 証明書の利用者名は原告の商標権を侵害していることを、原告が信じている旨の紛争中の Entrust SSL Web Server 証明書の加入者に事前の通知の写し、そして(3)通知方法とかかる通知が紛争中の Entrust SSL Web Server 証明書の加入者によって受領されたことを信じる根拠を表示した、原告による提出を行った場合は、Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA は次の措置を取ることがあります。Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA は、加入者の Entrust SSL Web Server 証明書の発行日が、原告が行った商標登録の登録日より前の日付となっているかどうかを判定します。加入者の Entrust SSL Web Server 証明書の発行日が商標登録日より前の日付となっている場合は、Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA は、仲裁人あるいは管轄権のある裁判所から真正の命令を提示されない限り、それ以上の措置は取りません。Entrust SSL Web Server 証明書の発行日が原告が行った商標登録日より後になっている場合は、Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA は、米国、カナダ、日本、オーストラリアあるいは EU 加盟国のうちの一国において、主たる商標事務所から加入者独自の対応する商標の所有証明書を、その加入者が提供することを求めるものとします。その加入者が上記に規定の通り、前の日付が原告の商標と同じ日に発行されている認証の写しを提供できる場合は、Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA は、仲裁人あるいは管轄権のある裁判所から真正の命令を提示されない限り、それ以上の措置は取りません。加入者が 10 営業日以内に応答しない場合、あるいは加入者により提示された登録商標の認証謄本の日付が前記申立て人により提示された登録商標の認証謄本の日付よりも遅れている場合には、Entrust SSL Web Server CA および

Entrust SSL Web Server CA が認定する RA はそれぞれ、係争中の Entrust SSL Web Server 証明書の失効または失効要求の手続を取ることができます。

加入者が申立て人を相手取って、あるいは申立て人が加入者を相手取って訴訟を起こし、かかる訴訟が発行済みの Entrust SSL Web Server 証明書の記載情報に関連しており、しかもかかる訴訟を起こした当事者が受理された訴状または最初の訴答書の写しを Entrust SSL Web Server CA または Entrust SSL Web Server CA が認定する RA に提出した場合、以降、Entrust SSL Web Server CA が Entrust SSL Web Server 証明書の現在の状態を維持するか、あるいは Entrust SSL Web Server 証明書の現在の状態を維持するよう、Entrust SSL Web Server CA が認定する RA が Entrust SSL Web Server CA に要求します。ただしその場合、Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に基づく Entrust SSL Web Server 証明書の状態の変更要求、もしくは規定または要求事項に従うものとします。訴訟期間中は、仲裁機関または司法管轄区の裁判所から命令されない限り、あるいは Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書による特段の規定または要求のない限り、Entrust SSL Web Server CA は係争中の Entrust SSL Web Server 証明書の失効手続を取らず、また Entrust SSL Web Server CA が認定する RA はかかる失効手続を要求しません。前記訴訟が発生した場合、Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA は、その訴訟の当事者として指名されていなくても、係争中の Entrust SSL Web Server 証明書に関しては当該司法管轄区の裁判所が発する命令に従います。Entrust または Entrust SSL Web Server CA の配下で RA を運営する第三者は、Entrust SSL Web Server 証明書に関連する訴訟の当事者として指名された場合、かかる訴訟に応じるために、あるいは抗弁するために適切と見なされる行為を取る権利が与えられるものとします。Entrust SSL Web Server 証明書に関連する訴訟に巻き込まれた加入者または信頼当事者は、Entrust SSL Web Server CPS、加入同意書、および信頼当事者の同意書の定める諸条件のすべてに従うものとします。

3.1.7 秘密鍵の所有を証明する方法

Entrust RA は Entrust SSL Web Server 証明書の申請で申請者が提出した CSR の署名を確認することにより、可逆性非対称アルゴリズム (RSA など) を用いて作成された CSR の所有権の立証を行います。

3.1.8 組織の身元の認証

Entrust SSL Web Server CA が認定する RA は、申請者あるいは加入者によって提出される組織の身元の制限的確認を行うものとします。Entrust SSL Web Server CA が認定する RA は、Entrust SSL Web Server 証明書の申請で提供された組織の身元、住所、およびドメイン名が第三者のデータベースや政府の情報源に含まれている情報と整合しているかどうかを認定するものとします。Entrust SSL Web Server 証明書の申請の制限的確認に用いられる情報や情報源は、申請者あるいは加入者の法的管轄によって異なる場合があります。政府の情報源に登録されていない組織の身元の場合、Entrust SSL Web Server CA が認定する RA はその組織の存在を確認する合理的な努力を払うものとします。かかる合理的な努力には、銀行やその他の信用機関への照会を含むこともできます。Entrust SSL Web Server CA が認定する RA は、Entrust SSL Web Server ポリシ認証局が指定するすべての検証手続を遵守するものとします。

Entrust SSL Web Server ポリシ認証局は、当該組織の身元確認方法を改善するために、独自の裁量により確認手続を更新することができます。確認手続の変更内容を公表する際には、Entrust SSL Web Server CPS の更新用の標準手順に準じるものとします。

3.1.9 個人の身元の認証

Entrust SSL Web Server CA が認定する RA は、申請者あるいは加入者によって提出される個人の身元の制限的確認を行うものとします。個人の身元の正確さを確定するために、個人は Entrust SSL Web Server CA が認定する RA 申請者の管轄内公証人の前に出頭することが要求されるものとします。個人は三種の身元確認を用意する必要があります。適切な身元確認の方法は、申請者の管轄によって異なるものとします。

Entrust SSL Web Server ポリシ認証局は、個人の身元確認方法を改善するために、独自の裁量により確認手続を更新することができます。確認手続の変更内容を公表する際には、Entrust SSL Web Server CPS の更新用の標準手順に準じるものとします。

3.2 定期的な鍵更新

各 Entrust SSL Web Server 証明書は証明書の有効期限を含んでいます。証明書の有効期限を持つ理由は、証明書に関連する鍵ペアの漏洩を最小限にとどめることです。この理由のため、新しい Entrust SSL Web Server 証明書の申請手続の際に、Entrust は、加入者に対し、新しい公開鍵を生成し、この鍵ペアの新しい公開鍵と加入者の Entrust SSL Web Server 証明書申請書を提出することを要求します。Entrust は Entrust SSL Web Server 証明書を更新しません。従って、加入者が現在の Entrust SSL Web Server 証明書の有効期限を超えて Entrust SSL Web Server 証明書の利用を継続することを望む場合、加入者は新しい Entrust SSL Web Server 証明書を入手し、期限切れになる Entrust SSL Web Server 証明書と置き換えなければなりません。新しい Entrust SSL Web Server 証明書の申請を行なう加入者は、新しい鍵ペアの生成、および Entrust SSL Web Server 証明書の初期申請手続に必要なすべての情報の提出を含めて、3.1 項に定める初期申請手続を完了させる必要があります。加入者の Entrust SSL Web Server 認証申請書の処理を完了した RA は、対応する Entrust SSL Web Server 認証申請書に記載されている技術関係の連絡窓口に電子メールを送り、その Entrust SSL Web Server 証明書の期限切れが迫っていることを加入者に通知します。Entrust SSL Web Server 証明書の期限が切れたら、加入者はただちにその証明書の使用を停止し、Web サーバから削除しなければなりません。

3.3 失効時の鍵更新

Entrust SSL Web Server CA および Entrust SSL Web Server CA が認定する RA は、失効した Entrust SSL Web Server 証明書の更新はしません。加入者が失効後 Entrust SSL Web Server 証明書を用いることを望む場合、加入者は新しい Entrust SSL Web Server 証明書を申請し、失効した Entrust SSL Web Server 証明書を取り替えなければなりません。別の Entrust SSL Web Server 証明書を入手するためには、加入者は鍵ペアの生成と Entrust SSL Web Server 証明書の最初の申請に必要なすべての情報の提出を含む、セクション 3.1 に記述の最初の申請過程を完了する必要があります。Entrust SSL Web Server 証明書の失効後、加入者は直ちにかかる Entrust SSL Web Server 証明書の使用を止めるものとし、かかる Entrust SSL Web Server 証明書を Web サーバから削除するものとします。

3.4 失効要求

加入者は、自分が当該 Entrust SSL Web Server 証明書の発行を受けた当の人、組織、または法人であることを Entrust SSL Web Server 認証申請書の処理に当たった RA に証明可能である限り、いつでもその Entrust SSL Web Server 証明書の失効を要求することができます。RA は、かかる加入者が提出したパスフレーズのほか、Entrust SSL Web Server 認証申請書および Entrust SSL Web Server 認証申請書の記載情報の一部を要求することにより、当該 Entrust SSL Web Server 証明書の失効要求を認証します。かかる情報を受理して確認したうえで、RA は、失効要求の有効性が確認されてから 48 時間以内にその加入者の Entrust SSL Web Server 証明書の失効を要求し、これを受けて Entrust SSL Web Server CA は、失効した Entrust SSL Web Server 証明書の連番を Entrust リポジトリの CRL に登録します。Entrust SSL Web Server CA が認定する RA は、当該加入者の Entrust SSL Web Server 認証申請書に記載されている技術およびセキュリティ関連の窓口に電子メールを送ることで、当該 Entrust SSL Web Server 証明書の失効の旨を加入者に通知するための適切な努力を払うものとします。

4 運営要件

4.1 証明書の申請

Entrust SSL Web Server 証明書を入手するためには、申請者は Entrust SSL Web Server CPS

のセクション 3.1 に記述した手続きに従わなければなりません。Entrust が直営する RA および Entrust SSL Web Server CA が認定する独立した第三者 RA は、申請者の身元の制限的確認を行うためにセクション 3.1.8 と 3.1.9 に記述した手続きに従うものとします。

4.2 証明書の発行

申請者が Entrust SSL Web Server 認証申請書に記入して提示した情報の制限付き検証を行ったら、Entrust SSL Web Server CA が認定する RA は、Entrust SSL Web Server CA に対して Entrust SSL Web Server 証明書の発行を要求することができます。Entrust SSL Web Server CA が認定する RA から発行要求を受けた Entrust SSL Web Server CA は、この Entrust SSL Web Server CPS のセクション 7 に定める証明書のプロファイルに従って Entrust SSL Web Server 証明書を作成し、デジタル署名を施すことができます。

4.3 証明書の受理

Entrust SSL Web Server 証明書が作成され、Entrust リポジトリに登録されたら、その Entrust SSL Web Server 証明書の発行を要求した RA は、申請者に対して、Entrust SSL Web Server 証明書が利用可能になったことを電子メールで通知するための妥当な努力を払うものとします。この電子メールでは、申請者が当該 Entrust SSL Web Server 証明書を検索するために使用する URL を紹介します。

4.4 証明書の一時停止および失効

Entrust SSL Web Server CA は、配下の RA から有効な失効要求を受領したら、当該 Entrust SSL Web Server 証明書の失効処理を行うものとします。Entrust SSL Web Server CA が認定する RA は、かかる Entrust SSL Web Server 証明書の加入者から有効な失効要求を受けたら、Entrust SSL Web Server CA に対して当該 Entrust SSL Web Server 証明書の失効を要求する権利を有するものとします。Entrust SSL Web Server CA が認定する RA は、Entrust SSL Web Server 証明書の使用停止を加入者に求める事態が発生していることに気づいたら、Entrust SSL Web Server CA に対してかかる Entrust SSL Web Server 証明書の失効処理を要求する権利を有するとともに、かかる要求を履行しなければなりません。

4.4.1 失効処理を必要とする状況

下記のいずれかの事態が発生していることを Entrust SSL Web Server CA または RA が認識するか、もしくはそれを信じるための合理的根拠を認識している場合には、Entrust SSL Web Server CA は、加入者の Entrust SSL Web Server 証明書の失効処理を行う権利を有し、かつ Entrust SSL Web Server CA が認定する RA は、かかる失効処理を要求する権利を有するとともに、その要求を履行しなければなりません。

- (1) Entrust SSL Web Server CA の秘密鍵、または上位の認証局の秘密鍵に安全性が損なわれている場合。
- (2) Entrust SSL Web Server CPS あるいは加入同意書のいずれかに、加入者が違反している場合。
- (3) 加入者に対して発行された Entrust SSL Web Server 証明書の記載情報に変更のある場合。
- (4) Entrust SSL Web Server 証明書発行料あるいはサービス料金が未払いの場合。
- (5) Entrust SSL Web Server 証明書が、Entrust SSL Web Server CPS および加入同意書の要件に従って発行されていないと判断される場合。
- (6) その他、Entrust SSL Web Server 証明書または Entrust SSL Web Server CA の整合性、セキュリティ、または信頼性に影響することを合理的に予測するだけの事由のある場合。

加入者が自己の秘密鍵の安全性が喪失されているとの疑念または認識を抱いている場合、あるいは加入者の Entrust SSL Web Server 証明書の記載情報に変更があるか、または状況の変化により加入者の Entrust SSL Web Server 証明書の記載情報が不正確、不完全、または誤解の原因となるとの疑念または認識を加入者自身が抱いている場合、かかる加入者は、その Entrust SSL Web Server 証明書の失効を要求しなければなりません。かかる失効要求は、加入者が加入者の Entrust SSL Web Server 認証申請書の処理に当たった RA に対して

提出するものとします。加入者の Entrust SSL Web Server 証明書がなんらかの理由により失効される場合、その加入者の Entrust SSL Web Server 証明書の処理に当たった RA は、対応する Entrust SSL Web Server 認証申請書に記載されている技術およびセキュリティ関係の窓口宛てに電子メールを送ることにより、その加入者に失効通知を行うための適切な努力を払うものとします。Entrust SSL Web Server 証明書が失効しても、それがこの Entrust SSL Web Server CPS、加入同意書、または信頼当事者の同意書に基づいて加入者が負うべき契約上の義務に影響するものではありません。

4.4.2 失効を要求できる当事者

加入者は、いついかなる理由によっても自己の Entrust SSL Web Server 証明書の執行を要求することができます。加入者が自己の Entrust SSL Web Server 証明書の失効を要求する場合には、その加入者は 3.4 項の定めに従い、当該 Entrust SSL Web Server 認証申請書の処理に当たった RA に対して、自分の身元証明を履行できなければなりません。加入者が 3.4 項および 4.4.3 項の定めに従って自分の身元証明を正当に履行できない限り、Entrust SSL Web Server CA は Entrust SSL Web Server 証明書の失効処理を行う義務を負わず、また Entrust SSL Web Server CA が認定する RA は失効要求を発行する義務を負うものではありません。4.4.1 に定めるいかなる理由によれ、またいつでも、Entrust SSL Web Server CA は加入者の Entrust SSL Web Server 証明書の失効処理を行い、かつ Entrust SSL Web Server CA が認定する RA はその失効処理を要求する権利を有するものとします。

4.4.3 失効要求の手続

Entrust SSL Web Server CA が認定する RA は、加入者の Entrust SSL Web Server 認証申請書の記載情報の一部、あるいは加入者の Entrust SSL Web Server 認証申請書で加入者が提示したパスワードの提示を求めるか、あるいは加入者と直接接触して確認することにより、加入者の当該 Entrust SSL Web Server 証明書の失効要求を認証します。かかる情報を受領して確認したら、その RA は、当該 Entrust SSL Web Server 証明書を発行した Entrust SSL Web Server CA に対して失効要求書を送付します。この失効要求書を受領した Entrust SSL Web Server CA は、受領後 48 時間以内に、失効対象の Entrust SSL Web Server 証明書の連番を Entrust SSL Web Server リポジトリの CRL に登録します。いかなる理由であれ加入者の Entrust SSL Web Server 証明書が失効した場合には、その Entrust SSL Web Server 証明書の失効を要求した RA は、対応する Entrust SSL Web Server 認証申請書に記載されている技術およびセキュリティ関係の連絡窓口宛てに電子メールを送り、失効の旨を加入者に通知するための適切な努力を払うものとします。

4.4.4 失効要求の猶予期間

秘密鍵が安全性喪失の事態が発生した場合、あるいはその疑念が持たれる場合には、加入者は、かかる安全性喪失または安全性喪失の疑念が発覚してからただちに当該 Entrust SSL Web Server 証明書の失効を要求しなければなりません。他の理由による失効要求は、常識的に可能な限り早急に行うものとします。

4.4.5 一時停止の状況

Entrust SSL Web Server CA は Entrust SSL Web Server 証明書の一時停止を行いません。

4.4.6 一時停止を要請できる人

Entrust SSL Web Server CA は Entrust SSL Web Server 証明書の一時停止を行いません。

4.4.7 一時停止要請の手続

Entrust SSL Web Server CA は Entrust SSL Web Server 証明書の一時停止を行いません。

4.4.8 一時停止期間の限度

Entrust SSL Web Server CA は Entrust SSL Web Server 証明書の一時停止を行いません。

4.4.9 CRL の発行頻度

Entrust SSL Web Server CA は、少なくとも 24 時間おきに CRL を発行するよう適切な努力

を払うものとします。CRLは通常、午前0時頃に発行されます。ただしこの発行間隔とは別に、例えば重大な安全性喪失が発覚している場合など、状況によって臨時に発行されることがあります。

4.4.10 CRLのチェックに関する要件

信頼当事者は、自分が信頼しようとする Entrust SSL Web Server 証明書が失効していないかをチェックしなければなりません。自分が信頼しようとする Entrust SSL Web Server 証明書が失効していないかを確認するために、信頼当事者は、適切なりポジトリに記録されている証明書失効リスト (CRL) をチェックします。Entrust、Entrust SSL Web Server CA が認定する独立の第三者 RA、再販者または販売協業者、もしくはその下請業者、卸売業者、代理店、供給業者、従業員、または役員は、(1)信頼当事者が Entrust SSL Web Server 証明書の失効または期限切れの確認を怠ったこと、あるいは(2)失効済みまたは期限切れの Entrust SSL Web Server 証明書を信頼当事者が信頼したことが原因で発生したいかなる損害についても、責任を負うものではありません。

4.4.11 オンライン失効・状態確認の可用性

Entrust リポジトリ内の CRL は連番によって検索できます。

4.4.12 オンライン失効確認要件

セクション 4.4.10 参照。

4.4.13 利用可能な失効告知のその他の様式

その他の仕組みは用意されていません。

4.4.14 失効告知のその他の様式の確認要件

規定無し。

4.4.15 鍵更新に伴う安全性喪失に関する特別要件

加入者の Entrust SSL Web Server 証明書に記載されている公開鍵に対応する秘密鍵の安全性が喪失されていることを加入者が認識している場合、あるいはその疑念を抱いている場合、ただちにその加入者は、4.4.3 項に定める手順により、自己の Entrust SSL Web Server 認証申請書の処理に当たった RA にその旨を通知しなければなりません。さらにその加入者は、ただちに当該 Entrust SSL Web Server 証明書の使用を停止し、Web サーバから削除しなければなりません。かかる安全性の喪失もしくはその疑念を生んでいる状況を調査すること、ならびにかかる安全性喪失もしくはその疑念による影響を受けるおそれのある信頼当事者に通知することは、加入者の責務とします。

4.5 セキュリティ監査手続

Entrust SSL Web Server CA における重大なセキュリティに関する事態は、自動的にファイル更新日時が記録され、監査証跡ファイル内の監査記録として記録されています。監査証跡ファイルは定期的に処理 (方針違反あるいはその他の重要事態がないかどうか見直す) します。監査記録の修正に対して保護するために監査証跡ファイルと共に確認コードが用いられています。監査証跡ファイルは定期的に記録されます。最新の監査証跡ファイルを含むすべてのファイルは磁気テープに移され、安全な記録施設で保管されます。

4.6 記録の保管

Entrust SSL Web Server CA の監査証跡ファイルおよびデータベースは、それぞれのアーカイブに保管されます。Entrust SSL Web Server CA のデータベース用アーカイブは、少なくとも 3 年間保持されます。監査証跡ファイル用のアーカイブは、少なくとも 1 年間保持されます。Entrust SSL Web Server CA のデータベースは、Entrust マスターキーによって暗号化され、保護されています。アーカイブの保存媒体は、Entrust が権限を与えた要員だけにアクセス可能なアクセス制限付きの施設に保管することによって保護されています。アーカイブ・ファイルが作成されるごとに、バックアップが取られます。オリジナルのファイルは、オンサイトにて保存され、Entrust SSL Web Server CA のシステムに収納されます。

バックアップ・ファイルは、安全でしかも地理的に離れた場所に保管されます。

4.7 鍵の切り替え

関連する鍵ペアの漏洩を最小限にとどめるため、有効期限のある Entrust SSL Web Server 証明書が加入者に発行されています。この理由により、Entrust は、期限切れとなるそれぞれの Entrust SSL Web Server 証明書の更新申請時に、新たに生成した鍵ペアと新しい公開鍵を提出するよう要求します。Entrust SSL Web Server 証明書の更新処理はセクション 3.2 に記載されています。

4.8 信頼性の喪失および災害復旧

Entrust SSL Web Server CA はシステム停止の場合、サービスの適時回復に備えるため災害復旧計画を用意しています。

Entrust は、Entrust SSL Web Server CA の統合性を維持するために厳重なセキュリティ管理体制を必要としています。Entrust の認識によれば、Entrust SSL Web Server CA が使用する秘密鍵の安全性が喪失する可能性はほとんど考えられませんが、それでも Entrust は、かかる安全性喪失の事態が発生した場合に取るべき方策と手順を用意しています。かかる安全性喪失の事態が発生した場合には、少なくともすべての加入者に対して可能な限り速やかに通達されます。

4.9 CA の終了

Entrust SSL Web Server CA が運営を終了する場合、Entrust SSL Web Server CA により発行されたすべての Entrust SSL Web Server 証明書はその有効期間の終わりに失効するものとして扱われます。

5 物理的、手続的、および要員のセキュリティ管理

5.1 物理的管理

Entrust Authority™ ソフトウェアは、Entrust SSL Web Server CA のソフトウェア構成を提供するのに用いられます。Entrust SSL Web Server CA のハードウェアとソフトウェアは業界の標準を満足する以上の物理的セキュリティとアクセスコントロールを持つセキュアな施設内に設置されます。Entrust/Authority ソフトウェアを収容する部屋は 2 人でのみ入室可能なように設計され、一人だけがこの部屋に入室することのないよう適切なコントロールを行います。Entrust SSL Web Server CA にアクセスする規則に対する違反を警備員に通知するため警報装置を配備します。

5.2 手続的管理

Entrust SSL Web Server CA は、Entrust SSL Web Server CA のソフトウェアで行われる機密性の高い操作を行うために信任されたいくつかの役割を設けております。Entrust SSL Web Server CA で使用されている Entrust/Authority ソフトウェアにアクセスする権限を取得しようとするオペレータは、経歴調査を受ける必要があります。アドミニストレータの追加や CA の方針の変更に関連する Entrust SSL Web Server CA の重要業務を執行するには、複数の要員が必要になります。

5.3 要員管理

Entrust SSL Web Server CA の業務要員には、Entrust SSL Web Server CA の業務責任と矛盾するようなその他の責任が割り当てられることはありません。Entrust SSL Web Server CA の業務要員に割り当てられる特権は、担当業務を行うのに最低限必要なものだけとします。

6 技術的セキュリティ管理

6.1 鍵ペアの生成とインストール

6.1.1 鍵ペアの生成

Entrust SSL Web Server CA が使用する署名用の鍵ペアは、Entrust/Master コントロール・アプリケーションの起動時に作成され、その Entrust SSL Web Server CA 専用のマスターキーにより保護されます。ハードウェア用の鍵は、少なくとも FIPS 140-1 レベル 3 に準拠するよう生成されます。

6.1.2 ユーザへの秘密鍵の配布

該当なし。

6.1.3 証明書発行者に対する公開鍵の配布

Entrust SSL Web Server 証明書に記載された公開鍵は、Entrust SSL Web Server 認証申請手続の一部として証明書署名要求書 (CSR) に記載されている Entrust SSL Web Server CA に配布されます。

6.1.4 ユーザに対する CA 用公開鍵の配布

Entrust SSL Web Server CA 用の公開鍵証明書は、GTE Corporation (“GTE”) 認証局による相互認証を受けております。GTE 認証局用の自己署名入り公開鍵証明書は、共通の WWW ブラウザと適切なソフトウェア業者による Web サーバ用ソフトウェアにプレインストールされています。

6.1.5 鍵のサイズ

SSL サーバの鍵サイズは加入者の Web サーバソフトウェアによって決められます。

6.1.6 公開鍵パラメータの生成

加入者の Web サーバソフトウェアは、どの公開鍵のパラメータが使われているかを管理しています。

6.1.7 パラメータの品質チェック

公開鍵のパラメータの品質はパラメータを生成する加入者の Web サーバソフトウェアによって制御されます。Entrust および Entrust SSL Web Server CA が認定する独立した第三者 RA、再販者、販売協業者、またはこれらのすべての下請業者、卸売業者、代理店、供給業者、従業員および役員は、Entrust SSL Web Server 証明書に含まれている公開鍵の品質について表示を行わず、保証や条件等を提供しません。

6.1.8 ハードウェア・ソフトウェアの鍵生成

Entrust SSL Web Server 証明書に関連する加入者の鍵ペアを生成する方法は、加入者のみが管理しており、Entrust および Entrust SSL Web Server CA が認定する独立した第三者 RA、再販者、販売協業者、またはこれらのすべての下請業者、卸売業者、代理店、供給業者、従業員および役員は加入者の鍵ペアの生成に対して何ら責任や義務などを負わないものとします。

6.1.9 鍵の使用目的

Entrust SSL Web Server CA が発行した Entrust SSL Web Server 証明書には、Entrust SSL Web Server 証明書の使用目的を制限する keyUsage および extendkeyUsage 証明書拡張子が記載されています。加入者および信頼当事者は、Entrust SSL Web Server CPS および適切な法律に違反しない範囲で Entrust SSL Web Server 証明書を使用しなければなりません。

6.2 秘密鍵の保護

Entrust SSL Web Server CA は、Entrust SSL Web Server CA の秘密鍵を保護するために、FIPS 140-1 レベル 3 への対応が認証されているハードウェア上で Entrust/Authority ソフトウェアを使用しています。加入者は、自分の Entrust SSL Web Server 証明書に記載されている公開鍵に対応する秘密鍵を保護する責任を負います。Entrust が Entrust SSL Web Server CA の秘密鍵を第三者に寄託することはありません。

6.3 鍵管理のその他の局面 規定無し

6.4 活性化データ 規定無し

6.5 コンピュータのセキュリティ管理

Entrust SSL Web Server CA が運用するワークステーションは、この Entrust SSL Web Server CPS の 5.1 項に述べるとおり、物理的に安全性が確保されています。Entrust SSL Web Server CA がワークステーション上で運用するオペレーティングシステムがユーザの身元確認と認証を実行します。Entrust SSL Web Server CA へのアクセス権を与えられているすべてのオペレータは、ハードウェア・トークンと PIN を共用して、その Entrust SSL Web Server CA 用の Entrust/Authority ソフトウェアを収容している物理空間へのアクセス権を取得しなければなりません。

6.6 ライフサイクル技術管理

この Entrust SSL Web Server CPS に記載のセキュリティ設定の有効性および妥当性は、毎年見直されます。鍵の長さを増やす必要があるか、あるいは業務手続を適時修正してシステムセキュリティの必要なレベルを維持する必要があるかどうかを決定するため、リスクおよび脅威についての評価が行われます。

6.7 ネットワークセキュリティ管理

Entrust/Admin インタフェース経由で Entrust/Authority への遠隔アクセスは、Secure Exchange Protocol および Entrust/Session のセキュリティ機能を用いて保護されています。

6.8 暗号モジュールの技術管理

Entrust/Authority ソフトウェアの暗号モジュールは、FIPS 140-1 レベル 1 の要求事項に適合するよう設計されています。オプションのハードウェア・トークンを使用して、もっと高いレベルの FIPS に準拠した鍵ペアを生成することもできますが、ただし、最低限レベル 1 はクリアすることが必須です。

7 証明書および CRL のプロファイル

7.1 証明書のプロファイル

Entrust SSL Web Server CA によって発行された Entrust SSL Web Server 証明書の概要は SSL プロトコルの使用に適合しています。

7.2 CRL のプロファイル

X.509 バージョン 2CRL フォーマットの以下のフィールドが Entrust SSL Web Server CA によって使用されます。

- ・バージョン：v2 に設定。
- ・署名：CRL を署名するアルゴリズムの識別子
- ・発行者：CRL を発行する CA のディステイングィッシュネーム
- ・今回の更新：CRL 発行時
- ・次回の更新：次回に予定されている CRL 更新
- ・失効した証明書：失効証明書のリスト

8 仕様管理

8.1. 連絡先情報

Director Operations, Entrust. Limited
Entrust. Limited
1000 Innovation Drive
Ottawa, Ontario

Canada K2K 3E7

Tel: (613)270-3157

Email: entrust.OA@entrust.net

8.2 仕様変更手続

Entrust は、自己の判断にて、Entrust SSL Web Server CPS、および CPS に含まれている条件を適宜修正することができます。Entrust SSL Web Server CPS の修正は、Entrust の判断により、申請者、加入者、および信頼当事者に、ほとんどあるいは全く影響がない場合は、CPS バージョン番号を変更せずに、また申請者、加入者および信頼当事者に通知することなく行うことができます。かかる変更は Entrust リポトリに公表次第、直ちに有効になるものとします。

Entrust SSL Web Server CPS の改訂のうち、申請者、加入者、および信頼当事者に重大な影響を与える可能性があるとして Entrust が判断する事項については Entrust リポトリで公表し、かかる公表から 15 日後に発効するものとします。ただし、かかる発効日より前に Entrust がその改訂版 Entrust SSL Web Server CPS を撤回した場合は本項の定める限りではありません。Entrust が Entrust SSL Web Server CPS に重大な改訂を実施したら、その Entrust SSL Web Server CPS の版数は適宜更新されます。Entrust SSL Web Server CPS の更新版が発効する日付よりも前に加入者が自己の Entrust SSL Web Server 証明書の使用を停止して削除し、その失効を要求しない限り、その加入者はかかる Entrust SSL Web Server CPS の更新版が定める諸条件に同意しているものと見なされ、かかる諸条件に拘束されるものとします。

8.3 公表および告知方針

この Entrust SSL Web Server CPS の大きな変更には先立ち、事前に変更の通知が Entrust リポトリに掲示されます。

8.4 CPS 承認手続

この Entrust SSL Web Server CPS および今後の変更は、Entrust ポリシ認証局によって承認されるものとします。

9 略語

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DNS	Domain Name Server
DSA	Digital Signature Algorithm
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
MAC	Message Authentication Code
OA	Operational Authority
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
RA	Registration Authority
RDN	Relative Distinguished Name

RFC	Request for Comment
SEP	Secure Exchange Protocol
SSL	Secure Sockets Layer
URL	Universal Resource Locator

10 用語の定義

関連会社 (Affiliate) : Entrust および Entrust が直接的あるいは間接的にコントロールする法人またはその他の法人。ここでいう「コントロールする」とは、ある当事者が当該法人または法人の取締役会その他の管理機構において 50 パーセント (50%) 以上の投票権を直接的あるいは間接的に所有または支配することを意味します。

申請者 (Applicant) : Entrust SSL Web Server 証明書を現在申請中であり、いまだ Entrust SSL Web Server 証明書の発行を受けていない人、法人、または組織、あるいは Entrust SSL Web Server 証明書を現在保有しており、かつ、その Entrust SSL Web Server 証明書の更新を申請中であるか、または追加の Entrust SSL Web Server 証明書を申請中である人、法人、または組織。

営業日 (Business Day) : カナダのオンタリオ州オタワ市の土曜・日曜日および法令や条例により定められた休日を除くすべての日。

証明書 (Certificate) : 少なくとも (a) 証明書の発行元たる認証局を特定し、(b) 被認証者の名前または身元を明らかにしており、しかも (c) 鍵ペアの公開鍵が記載され、(d) その運営期間が指定され、かつ (e) 連番と CA のデジタル署名が記載されているデジタル書類。

証明書失効リスト (CRL: Certificate Revocation List) : CA によるデジタル署名入りの失効済み証明書の連番とファイル更新時刻印が記入されたリスト。

認証局 (CA) : (1) とりわけ被認証者の公開鍵および被認証者の身元確認に資する他の情報を記載した証明書の作成とデジタル署名、(2) 証明書で確認されている被認証者との意思疎通の便宜を図るための証明書の閲覧サービス、ならびに (3) すでに失効しており、それ以上使用も信用もすべきでない証明書に関する情報を記載した証明書失効リストの作成およびデジタル署名を行う法人または組織。

認証局運用規定 (CPS: Certification Practice Statement) : 認証局が証明書の発行、管理、失効処理、更新、および証明書へのアクセスに際して適用する実施規則、ならびにこれらのサービスを提供する際の諸条件を定めた規定書。

販売協業者 (Co-marketers) : Entrust SSL Web Server または Entrust SSL Web Server 認証局のもとで運営される登録局によって Entrust SSL Web Server 証明書の販売促進を行う権限を付与された人、法人、または組織。

安全性の喪失 (Compromise) : 重要な機密情報またはデータの喪失、開示、または管理不能、もしくはその疑いがある状態。

CPS : 認証局運用規定を参照。

CRL : 証明書失効リストを参照。

相互認証証明書 : (1) Entrust 認証局により、あるいは Entrust 認証局のために生成された公開鍵と秘密鍵のペアの公開鍵を含み、(2) GTE Corporation またはその継承者が運営する認証局の電子署名が施されており、(3) GTE Corporation の公開鍵証明書を使用することにより加入者の公開鍵 SSL 証明書の検証を可能にし、かつ (4) 2006 年 2 月 23 日当日もしくはそれ以前を失効日とする証明書。

Entrust : Entrust 限られた。

Entrust.net : Entrust 限られた。

Entrust 運営責任者 (Entrust Operation Authority) : Entrust を支援または代行して活動し、Entrust SSL Web Server 認証局の運営について責任を負う人。

Entrust ポリシ認証局 (Entrust Policy Authority) : Entrust を支援または代行して活動し、Entrust SSL Web Server 認証局の運営を統括するためのポリシおよび手続の策定に責任を負う要員。

Entrust リポジトリ (Entrust Repository) : Entrust SSL Web Server 証明書および Entrust SSL Web Server 証明書に関連して Entrust が提供するサービスに関する情報を含んだデータベースおよび Web サイトを統合したもの。これらの情報には、Entrust SSL Web Server

認証局が発行する Entrust SSL Web Server 証明書の種別、Entrust SSL Web Server 証明書に関連して Entrust が提供するサービス、Entrust SSL Web Server 証明書のために Entrust が請求する料金、Entrust SSL Web Server 証明書、CRL、Entrust SSL Web Server 認証局運用規定、およびその他 Entrust SSL Web Server 証明書の使用を管理するための情報や契約に関連して Entrust が提供するサービスが含まれます。

Entrust SSL Web Server 認証局 (Entrust SSL Web Server Certification Authority) : Entrust SSL Web Server 証明書の発行、管理、失効、更新手続、およびアクセス・サービスを目的として Entrust によって運営されるか、あるいは Entrust を代行する認証機関。
Entrust SSL Web Server 認証局運用規定 (Entrust SSL Web Server Certification Practice Statement) : この文書のこと。

Entrust SSL Web Server CPS : Entrust SSL Web Server 認証局運用規定を参照。

Entrust SSL Web Server 証明書 (Entrust SSL Web Server Certificate) : WWW サーバ上での使用を目的として Entrust SSL Web Server 認証局が発行する証明書。

Entrust SSL Web Server 認証申請書 (Entrust SSL Web Server Certificate Application) : Entrust SSL Web Server 認証局のもとで運営される登録局が要求し、Entrust SSL Web Server 証明書の発行を申請する申請者が提出する申請書類。

FIPS : 連邦情報処理基準を意味します。特定の性能要件、業務、フォーマット、通信プロトコルおよびハードウェア、ソフトウェア、データおよび遠隔通信操作のその他の要求事項を規定する米国連邦基準です。連邦機関は、連邦の放棄手続に従って放棄が許諾されていない場合、規定の通りこれらの基準を適用することが期待されています。

IETF : インターネットエンジニアリングタスクフォースを意味します。IETF はインターネットアーキテクチャの発展とインターネットの効率的な運営に関する、ネットワークデザイン、オペレータ、ベンダおよび研究員の大規模で開かれた国際組織です。

鍵ペア (Key Pair) : 互いに数学的関連性のある 2 つの暗号鍵で、以下の特性をもちます。
(1) 一方の鍵を使って暗号化したメッセージはもう一方の鍵を使わなければ復号化できず、かつ (2) 一方の鍵を知っていても、もう一方の鍵を解明することは計算上不可能である。

オブジェクト識別子 (Object Identifier) : オブジェクト識別子の登録用として国際的に認知されている手続に従って特殊な書式で登録された数値。

OID : Object Identifier 参照。

運用期間 (Operational Period) : 証明書に関して、有効期間を意味します。運用期間は一般に証明書発行日 (または証明書に指定の後の日) に始まり、証明書に記された有効期限に終了するか、あるいは失効した場合はその期日より早く終わります。

PKIX : X.509 バージョン 3 証明書に基づき PKI 部品の技術仕様書の開発を行う IETF ワーキンググループを意味します。

秘密鍵 (Private Key) : 鍵ペアのうちのデジタル署名を作るのに用いられる鍵を意味します。この鍵は秘密にしなければなりません。

公開鍵 (Public Key) : 鍵ペアのうち、メッセージを暗号化するために使用する鍵。公開鍵は、当該鍵ペアの秘密鍵のホルダに暗号化メッセージを送ろうとするすべての人が自由に利用できるものとします。公開鍵はふつう、認証局が発行した証明書を通じて公開されるほか、リポジトリやデータベースにアクセスすることで入手されることがあります。公開鍵を使って暗号化したメッセージを復号化できるのは、対応する秘密鍵のホルダだけです。

RA : 登録局を参照。

登録局 (RA: Registration Authority) : (1) 証明書に名前が記載されている被認証者からの情報を受け取り、(2) 被認証者が提供する情報を特定の第三者データベースから入手した情報と照合して限定的な検証を行う、という 2 つの機能を果たす法人。被認証者が提供する情報がかかる第三者データベースの情報と対応している場合には、登録局は、登録局が検証した情報が記載された証明書の作成、デジタル署名、および発行を求める要請書を認証局に送ることができます。

信頼当事者 (Relying Party) : 公開鍵を入手、確認して加入者のデジタル署名を確認するために、Entrust SSL Web Server 証明書または Entrust SSL Web Server リポジトリに登録されている他の情報を信頼あるいは利用する人、法人、または組織。

信頼当事者の同意書 (Relying Party Agreement) : 信頼当事者と Entrust、あるいは信頼当事者と Entrust SSL Web Server 認証局が認定する独立の第三者登録機関または再販者と

の間で、Entrust SSL Web Server 証明書に関する一定の情報およびサービスの提供や利用について結ばれる契約。

リポジトリ (Repository) : 認証局が発行する証明書に関する情報、とりわけ認証局が提供する認証およびサービスの種別や料金、証明書失効リスト、認証局の業務や手続の内容、認証局が発行する証明書の使用を管理するためのその他の情報や契約書を記録したデータベースおよび Web サイトの集成。

再販者 (Reseller) : Entrust SSL Web Server 認証局が認定する Entrust SSL Web Server 登録局によって Entrust SSL Web Server 証明書の使用权を許諾する権限を付与された人、法人、または組織。

失効 (Revoke or Revocation) : 証明書に関し、先の規定の時期から証明書の運用期間を早期終了することを意味します。

Subject : 公開鍵が証明書中に証明されている人、法人、あるいは組織を意味します。

加入者 (Subscriber) : Entrust SSL Web Server 証明書を申請し、発行された人、法人、あるいは組織を意味します。

加入同意書 (Subscription Agreement) : 加入者と Entrust、あるいは加入者と Entrust SSL Web Server 認証局が認定する独立の第三者登録機関または再販者との間で、Entrust SSL Web Server 証明書の発行、管理、およびアクセス・サービス、ならびに Entrust SSL Web Server 証明書に関するその他のサービスの提供について結ばれる契約。