

Entrust Datacard 証明書サービス加入契約

注意 –本 **Entrust Datacard 証明書サービス加入契約**（以下「**本契約**」という）は、**お客様**（以下で定義）と **Entrust Datacard**（以下で定義）の間の法的な契約です。契約を締結する前に、**本契約**および**本契約**に組み込まれている **CPS：認証局運用規定**（適宜改訂されます）を細部まで注意してお読みください。これらは併せて、お客様がこの**証明書サービス**について限定された使用権を取得するための諸条件を定めたものです。

下部の[accept（同意する）]アイコンをクリックするか、**証明書サービス**の申請書を送信した個人は、（i）自身が**お客様**を**本契約**（**CPS**を含む）の諸条件に拘束させる法的な権限を有すること、および（ii）**お客様**が**本契約**の諸条件に法的に拘束されることを表明し、保証したものとみなされます。ご自身または**お客様**が**本契約**の諸条件に同意しない場合、下部の[decline（拒否する）]アイコンをクリックし、申請のプロセスを続行しないでください。なお、**Entrust Datacard** は、**本契約**を修正または補充するために、ウェブサイトで通知する場合があります。その場合、**本契約**は、たとえ、その通知が英語のみであったとしても、通知されたとおりに通知日において修正または補充されたものとみなされます。

本契約の諸条件は、**Entrust Datacard** が**証明書サービス**に関する個別のサブスクリプション契約、基本契約、または付随する契約を**お客様**との間で締結した場合には適用されないことにご留意ください。

1. 定義

本契約または **CPS** の他の箇所で定義された太字の用語に加え、次の太字で記載された語句は、下記の意味を有します。

「**発効日**」とは、次のうちいずれか早い日付を意味します。（i）**お客様**が **Entrust Datacard** から**管理サービス**を購入した場合において、**Entrust Datacard** が**証明書サービス**を**お客様**の使用に供した日、または（ii）**お客様**が **Entrust Datacard** から**管理サービス**を購入していない場合において、**お客様**に対して1つもしくは複数の**証明書**が発行された日。

「**関連会社**」とは、**Entrust Datacard** に関しては、直接もしくは一つ以上の仲介者を介して間接的に **Entrust Datacard** を統制するか、統制されるかもしくは共通の統制下にある者または法人をいい、**お客様**に関しては、**お客様**が直接または間接に統制する会社その他の法人/個人をいいます。なお、「統制」とは、議決権株式の50%以上を保有するか、株式会社でない場合はこれに相当する権利を有することを意味します。

「**代理人**」とは、(1) **EV SSL 証明書**および**EV コード署名証明書**の場合は、**CPS**に定義された(i) **証明書申請者**、(ii) **証明書承認者**、(iii) 登録された**代理人**および(iv) **契約署名者**をいい、(2) **SSL 証明書**および**プライベート SSL 証明書**の場合は、**CPS**に規定されている加入者の技術連絡担当者を意味します。いずれの場合も、**代理人**には(a) **お客様**もしくは**お客様**の関連会社にホスティングサービスを提供する第三者(以下「**Web ホスティング業者**」という)、または(b) 加入者に代わってコードにデジタル署名する組織(以下「**署名機関**」という)が含まれます。**お客様**または**お客様**の関連会社によって最初に任命される**代理人**は附属書類Aの一覧に示すか、または登録時に**Entrust Datacard**に対して別途通知するものとします。**お客様**はこのような**代理人**の任命について**Entrust Datacard**が随時定める手段を使用して変更することができます。

「**アプリケーションソフトウェアベンダー**」または「**ASV**」とは、**証明書**を表示または使用するインターネットブラウザソフトウェア、電子メールソフトウェアまたは他のソフトウェアの開発者を意味します。これには、Adobe、Apple、Google、Intel、Microsoft、Mozilla および Oracle が含まれますが、これに限定されません。

「**基本要件事項**」とは、(i) 最新版の『CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates』(一般的に信用された**証明書**の発行と管理に関するCA/ブラウザフォーラム**基本要件事項**) (以下「**パブリックトラスト基本要件事項**」とする)を意味し、また、(ii) コード署名**証明書**に関しては、最新版の『CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates』(一般的に信用されたコード署名**証明書**の発行と管理に関するCA/ブラウザフォーラム**基本要件事項**) (以下「**コード署名基本要件事項**」とする)を意味します。これらの**基本要件事項**は、インターネット上の<https://cabforum.org/baseline-requirements-documents/> (英文)に掲載されています。

「**証明書**」とは、少なくとも以下の情報が記されたデジタル文書を意味します；(a) 発行認証局の特定、(b) 名前その他の方法による加入者の特定、(c) 鍵ペアの公開鍵の記載、(d) 公開鍵の運用期間の特定、および(e) シリアル番号の記載と認証局によるデジタル署名。**Entrust Datacard**が加入者に発行できる**証明書**には、加入者が購入した**証明書**サービスに応じて、さまざまな**証明書**タイプがあります。例えば、**SSL 証明書**、拡張認証(以下「**EV**」という)**SSL 証明書**、**コード署名証明書**、**EV コード署名証明書**、**ドキュメント署名証明書**、**認証マーク証明書**(以下「**VMC**」という)、**モバイルデバイス証明書**、**プライベート SSL 証明書**、**セキュア電子メール個人向け証明書**、**セキュア電子メール企業向け証明書**、**eIDAS 資格ウェブサイト認証証明書**(以下「**eIDAS QWACs**」という)、**PSD2 資格ウェブサイト認証証明書**(以下「**PSD2 QWACs**」という)がありますが、これらに限られるものではありません。

「**証明書受益者**」とは、**アプリケーションソフトウェアベンダー**であって、**Entrust Datacard**がその**アプリケーションソフトウェアベンダー**が配布するソフトウェアに自己のルート**証明書**を組み込む旨の契約を締結したすべての者および**依頼当事者**であって、**証明書**の**有効期間**中に、その**証明書**に実際に**依頼**するすべての者をまとめて意味します。

「**証明書サービス**」とは、**Entrust Datacard**が随時使用できるいずれかのブランドでの1つまたは複数の**証明書**の発行または失効に関し、**お客様**が（**お客様**自身のためにまたは該当する場合は**お客様**の関連会社の代理で）購入する特定のサービスを意味します。また、**証明書サービス**には、**管理サービス**、**外部証明書管理権**および**マルウェアスキャンサービス**が含まれることもあります。さらに、**証明書サービス**には、**本契約**に基づいて使用するために**Entrust Datacard**グループの構成企業によって**お客様**（または該当する場合、**お客様**の関連会社）に発行され、ライセンスされたあらゆる**証明書**も含まれます。**Entrust Datacard**は、**契約期間**中に自己の裁量で**証明書サービス**を変更する権利を留保します。

「**契約署名者**」とは、加入者に代わり、また、加入者の権限に基づいて**本契約**に同意して署名する個人を意味します。

「**CPS**」とは、最新版の認証局運用規程であり、**本契約**と加入者に発行される**証明書**に組み込まれます。**CPS**は、その諸条件に従って、随時変更されます。具体的な**証明書**に適用される**CPS**は、**証明書**の種類に応じて異なります。**CPS**を入手するには、インターネットで<http://www.entrust.net/cps> (英文) にアクセスするか、**Entrust Datacard**までご連絡ください。たとえば、**eIDAS QWACs** および **PSD2 QWACs** の**証明書**の使用には、『Certification Practice Statement For Qualified Certificates』（認証**証明書**に関する認証局運用規程）という文書の最新バージョンが適用され、プライベート SSL **証明書**の使用には、『Certification Practice Statement For Private Trust Certificates』（プライベート信頼**証明書**に関する認証局運用規程）という文書の最新バージョンが適用され、他の一切の**証明書**の使用には、『Certification Practice Statement』（認証局運用規程）という文書の最新バージョンが適用されます。

「**お客様**」とは、**証明書サービス**を受けるために**本契約**を締結した法人/個人を意味します。

「**DPA**」とは、**Entrust Datacard**の顧客のためのデータ処理に関する合意の最新版を意味し、<https://www.entrustdatacard.com/resource-center/licensing-and-agreements> (英文) から入手できます。

「**エンタープライズ**」とは、**お客様**および**お客様**の関連会社を意味します。

「**Entrust Datacard**」とは、**お客様**が米国在住の場合は Entrust, Inc.を意味し、それ以外の場合、**Entrust Datacard Limited** を意味します。「**Entrust Datacard グループ**」とは、**Entrust Datacard**、その子会社、ライセンサー、リセラー、サプライヤー、ならびにこれらの取締役、役員、下請人、**代理人**および従業員を総称するものです。

「**EV ガイドライン**」とは、(i) **EV SSL 証明書**に関しては、最新版の『CA/Browser Forum Guidelines For The Issuance And Management of Extended Validation Certificates』（拡張認証**証明書**の発行と管理に関する CA/ブラウザーフォーラムガイドライン、以下「**EV SSL ガイドライン**」という）を意味し、(ii) **EV コード署名証明書**に関しては、最新版の『CA/Browser Forum Guidelines For The Issuance And Management of Extended Validation Code Signing Certificates』（拡張認証コード署名**証明書**の発行と管理に関する CA/ブラウザーフォーラムガイドライン、以下「**EV コード署名ガイドライン**」という）を意味します。これらのガイドラインは、インターネット上の次のアドレスに掲載されています。

<https://cabforum.org/about-ev-ssl/> (英文)

「**外部証明書**」とは、**本契約**に基づいて**お客様の管理サービス**アカウントから発行されたものではない、あらゆる**証明書**を意味します。なお、**外部証明書**には、他の**管理サービス**アカウントから発行された**証明書**、**Entrust Datacard**のリテール Web サイトから購入した**証明書**、他の**Entrust Datacard**の提供サービスから発行された**証明書**、第三者によって発行された**証明書**が含まれますが、これに限定されません。

「**外部証明書管理権**」とは、購入した**外部証明書管理権**ごとに提供される**外部証明書**をドキュメントの指定に従って管理するために**管理サービス**アカウントを使用できるようにするために**お客様**に提供されるオプションのライセンスを意味します。**お客様**が使用できる**外部証明書管理権**の数は、**お客様の管理サービス**アカウントによって追跡されます。また利用可能な**外部証明書管理権**の数は、**お客様の管理サービス**アカウントに追加された、または、そこから取り出された**外部証明書**の数に応じて増減します。

「**業界標準**」とは、次のそれぞれの最新版をまとめて意味します。**EV ガイドライン**、**基本要
求事項**、『European Standards produced by the ETSI Technical Committee Electronic Signatures and Infrastructures』（ETSI Technical Committee Electronic Signatures and Infrastructures が作成した欧州における基準）、**認証マークガイドライン**ならびに **Entrust Datacard** によって発行された一般的に信用されるさまざまな**証明書**に適用される可能性があり、**Entrust Datacard** がそのような**証明書**の発行者として従い、また拘束される法律および規則。

「マルウェアスキャンサービス」とは、毎日実施されるオプションのマルウェアスキャンサービスです。このサービスは、**証明書**を保有することで利用でき、第三者サプライヤーが **Entrust Datacard** に代わってホスティングします。各 **SSL 証明書** には、1つのドメインに対し、最大 250 ページの限定的マルウェアスキャンと、ブラックリストモニタリングを毎日実行するオプションが含まれています。**EV SSL 証明書** の場合は、サービスの一部として、ドキュメントに記載された1つのドメインに対し、最大 500 ページの限定的マルウェアスキャン、ブラックリストモニタリング、および同様な他の補助的なスキャンを毎日実行するオプションが含まれています。上記にかかわらず、プライベート **SSL 証明書** には、**マルウェアスキャンサービス** は含まれていません。そのような **マルウェアスキャンサービス** は、このサービスを実行するために必要な情報を **お客様** が提供することを条件として第三者サプライヤーによって以下のいずれか早い時点まで提供されます。(i) **契約期間** の終了時点、(ii) スキャン対象のドメインに対応する適用可能な **証明書** の失効の時点、および (iii) **Entrust Datacard** による **マルウェアスキャンサービス** の打ち切りの時点。**Entrust Datacard** は、**契約期間** を通じて、**マルウェアスキャンサービス** の機能を変更し、または終了する権利を留保します。またこのようなサービスは、すべてのマルウェア、セキュリティ脅威もしくは脆弱性の検出または検出可能性を保証するものではありません。

「**管理サービス**」とは、**Entrust Datacard** がホスティングするセルフサービスの管理ツールです。このツールは、**Entrust Datacard** によって **お客様** に提供される **証明書** を管理できるように設計されており、**お客様** はこれを使用することで、**証明書サービス** の一部として **お客様** に発行される1つまたは複数の **証明書** の発行、失効、および満了を管理できます。**管理サービス** は、ドキュメントに記載されているように、**証明書プーリングモデル**（以下「**プーリング**」という）と **ノンプーリングモデル**（以下「**ノンプーリング**」という）の2種類のモデルで利用できます。

「**許可されたグループ**」とは、(i) **SSL 証明書**、**EV SSL 証明書**、**プライベート SSL 証明書**、**EV コード署名証明書**、**ドキュメント署名証明書**、**コード署名証明書** および **VM 証明書** の場合は、**お客様** および **お客様** の関連会社を意味し、(ii) **モバイルデバイス証明書**、**セキュア電子メール個人向け証明書** および **セキュア電子メール企業向け証明書**（「**クライアント証明書**」）の場合は、**お客様** の従業員、または **エンタープライズ** 関連の業務を行い、かつ、そのような業務上の目的のために **エンタープライズ** が電子メールアドレスまたはモバイル機器を割り当てた第三者を意味します。ただし、そのような第三者への割り当てが、インターネット上の <http://www.entrust.net/cps> (英文) を通じて得られる「**Client Certificate Agreement**」の最新版に従ってなされたこと、また、(i) **お客様** が各 **Client Certificate** に含まれる情報が正確であると確認し、(ii) **Client Certificate** が発行される個人がその **Client Certificate** に組み入れられる一切のデータの包含に同意し、(iii) **お客様** が **Client Certificate** に適用されるライセンス料

を支払い、また(iv)そのような Client Certificate が**エンタープライズ**関連の業務のために使用されることを条件とします。

「**法人/個人**」とは、個人、法人または会社（株式会社、企業合同、合名会社、有限責任会社、組合、合併事業、政府機関、公共団体）およびその他の外国又は国内法人または商業組織を意味します。

「**リセラー**」とは、**Entrust Datacard** から承認を受けて、**お客様**に**証明書サービス**を再販する法人を意味します。

「**依拠当事者**」とは、**有効**な証明書に依拠する個人または団体を意味します。疑義を避けるために明記すると、ASVによって配布されるソフトウェアが証明書に関する情報を単に表示するのみである場合、そのような ASV は「依拠当事者」ではありません。

「**対象者**」とは、証明書において与えられる公開鍵に関連する秘密鍵の所有者として証明書で特定される法人/個人を意味します。

「**加入者**」とは、**許可されたグループ**内の法人/個人であって、**本契約**に基づいて証明書を申請し、または発行される**法人/個人**を意味します。

「**契約料金**」とは、**証明書サービス**、**管理サービス**、および ECS サポートサービスの使用料として、**Entrust Datacard** が定め、**お客様**が支払う料金を意味します。**契約料金**は、**Entrust Datacard** のインターネット Web サイトおよび/または**管理サービス**の付属文書に随時掲載される金額、または **Entrust Datacard** から**お客様**への見積書に記載された金額、または**お客様**が **Entrust Datacard**（もしくはリセラー）に発行した発注書に記載され **Entrust Datacard** が同意した金額となります。前記にかかわらず、**お客様**がリセラーを通じて**証明書サービス**を購入した場合、**契約料金**は、**お客様**とかかるリセラーの間で合意した料金となります。ただし、これはリセラーが **Entrust Datacard** に対して、その**契約料金**の中から、**Entrust Datacard** とリセラーの間で書面によって合意した金額を支払うことを条件とします。

「**契約期間**」とは、**発効日**から起算される、**お客様**が**証明書サービス**の利用に同意した期間を意味します。**お客様**が**証明書サービス**を購入した場合の**契約期間**は次のとおりです。(i) 一つの証明書向けである場合、**契約期間**は当該証明書の**有効期間**です。(ii) 「**プーリング**」**管理サービス**が含まれている場合、**契約期間**は、当該**管理サービス**の使用権を契約した期間であり、**証明書サービス**の一部として**お客様**に発行される証明書が当該期間を超えているかどうかは関係ありません。(iii) 「**ノンプーリング**」**管理サービス**が含まれている場合、**管理サービス**に基づいて発行される適用可能な証明書の**有効期間**が**契約期間**となります。ただし、発行日から 1 年以内にすべての証明書が発行されることが条件となり、その後は、発行を要求できな

くなるものとします。**お客様**が、**契約期間**の満了時に、**証明書サービス**契約を更新して、期間を更新すること（以下「**更新期間**」という）を選択する場合、**契約期間**は、**更新期間**の**契約料金**の支払をもって、**更新期間**を含めたものとして延長されるものとします。いずれの場合も、**契約期間**は、**本契約**の第 10 条（期間および終了）に従って短縮される場合があります。

「**サスペクトコード**」とは、悪意のある機能もしくは重大な脆弱性を持つコードまたは一連の命令を意味します。これにはスパイウェアやマルウェアなど、ユーザーの同意なしにインストールされるコードやそれ自体の削除が困難であるコード、および設計者が意図しない方法で悪用されて、それが動作するコンピューティング環境の信頼性を侵害する可能性のあるコードが含まれます。

「**有効**」とは、満了しておらず、かつ失効していない証明書を意味します。

「**認証マークガイドライン**」とは **VMC** のために Authindicators Working Group によって承認されたガイドラインの最新版を意味します。

2. 公開鍵のインフラストラクチャの働き

CPS は、公開鍵のインフラストラクチャを管理し、証明書を発行する **Entrust Datacard** の運用について定めたもので次のものを含みます。

- (a) 適用される**業界標準**およびポリシーの仕様
- (b) 依拠当事者に関する情報
- (c) イベントログの保持期間
- (d) 苦情および紛争解決のプロセス
- (e) 適用されるコンプライアンスに関する監査その他の調査についての仕様
- (f) 証明書に関する問い合わせの連絡先情報
- (g) 取消状況に関する情報の提供方法およびこれが入手可能な期間

3. サービスおよびライセンス

3.1 証明書の発行および失効:**証明書サービス**の申請を受け取ると、**Entrust Datacard** は、**エンタープライズ**によって提出された情報について、限定的確認（**CPS** の記載に従った確認）を行います。この確認完了後、**Entrust Datacard** は、**お客様**または**お客様の関連会社**（該当する場合）に対し、1つまたは複数（**お客様**が支払った**契約料金**によります）の証明書を **CPS** の規定に従って発行することができます。**Entrust Datacard** が**お客様**または**お客様の関連会社**（該当する場合）に**証明書サービス**を発行する場合、**Entrust Datacard** はその証明書を取得できるように提供します。**Entrust Datacard** は、**お客様**が失効を求めた場合、**本契約**が満了

もしくは終了した場合、または、**本契約**、**CPS** もしくは**業界標準**に照らし失効に値する理由がある一切の場合に、**証明書**を失効させることができます。

3.2 権利の付与: **本契約**の諸条件に従うことを条件として、**Entrust Datacard** は、**エンタープライズ**に対し、**証明書サービス**（疑義を避けるために明記すると、すべての**証明書**を含む）を使用する非独占的で譲渡不能な権利を付与します。ただし、当該**エンタープライズ**は、**証明書**については、**CPS**に定める目的でのみ、他の**証明サービス**については、**証明サービス**に付随して提供される文書に定める目的でのみ使用できます。**エンタープライズ**は、**Entrust Datacard**またはリセラーから購入した**証明書**の数のみを管理できるとし、次のことを行わないものとします。(a) **本契約**に定める以外には、**証明書サービス**のいかなる構成部分についても、ホスト、タイムシェア、貸与、リース、販売、ライセンス、サブライセンス、譲渡、配布、移転または第三者への利用許可すること、(b) **証明書サービス**について複製、変更、翻訳、リバースエンジニアリング、逆コンパイルもしくは逆アSEMBルまたは派生物を作成すること（契約上の別段の制限にもかかわらず、法がこの制限を明確に禁止する場合を除く）、(c) **証明書サービス**の一部として提供された構成要素に表示または付加された制限または付与のメカニズムをすり抜けたり、無効化しようとする、(d) **証明書サービス**の一部として**Entrust Datacard**が提供したパスワードその他のログインに関する情報を第三者に提供すること、(e) **証明書サービス**の非一般公開の機能やコンテンツを第三者と共有すること、(f) 競合する商品やサービスを作出したりベンチマークする目的で、または、**証明書サービス**の類似のアイデア、特徴もしくは機能を使用した商品やサービスを作出する目的で、**証明書サービス**にアクセスすること、(g) 侵害性あるもしくは違法な文書、ウィルス、ワームス、タイムボム、トロイの木馬およびその他の有害又は悪意あるコード、ファイル、スクリプト、エージェントまたはプログラムを送信または保存する目的で**証明書サービス**を使用すること、(h) **本契約**ならびに適用される**業界標準**、法および規制に従わずに**証明書サービス**を利用すること。**エンタープライズ**は、**本契約**に定める以外には、**証明書サービス**を複製、変更、適用またはコピーの統合をしないものとします。**エンタープライズ**は、契約上の制限にもかかわらず法がこの制限を明確に禁止する場合を除き、**証明書サービス**について翻訳、リバースエンジニアリング、分解もしくは解体はしないものとします。

3.3 ECS サポートサービス: **管理サービス**を購入した**お客様**は、以下に定める ECS サポートサービスを受けることができます。「**ECS サポートサービス**」とは、以下の機能に関するメンテナンス、サポートおよび検証のサービスを意味します。(i) **お客様**または**お客様の関連会社**への1つまたは複数の**証明書**の発行および失効、(ii) **証明書サービス**、および(iii) **お客様**が選択および支払（該当する場合）を行ったサービスプランに従って、**Entrust Datacard**が提供する**管理サービス**。ECS サポートサービスは、以下のサービスプランで利用できます。(i) **シルバーサポート**プラン（以下「**シルバーサポート**」という）、(ii) **プラチナサポート**プラン（以下「**プラチナサポート**」という）。ECS サポートサービスは、**Entrust Datacard**

によって、インターネット上の www.entrust.net/cps (英文) を通じ入手可能な ECS サポートサービス契約の諸条件に従って、**契約期間中**、提供されます。**Entrust Datacard** は、**契約期間中**、自己の裁量で ECS サポートサービスを変更する権利を留保します。**お客様が管理サービス**に加入している場合、**シルバーサポートサービス**は、加入した**管理サービス**の一部として追加料金なしで**お客様**に提供されます。**管理サービス**に加入している**お客様**は、ご希望に応じて、適用される**契約料金**を支払うことで、ECS サポートサービスを**プラチナサポートプラン**にアップグレードすることができます。**プラチナサポートプランの契約料金**は、**契約期間中の管理サービス**アカウントの全証明書に対して支払い、それ以降は追加分を支払う必要がありません。

3.4 オプションソフトウェア：**証明書サービス**または ECS サポートサービス（関連するサポートまたは専門的なサービスを含む）の一部として、**エンタープライズ**がダウンロードして利用できるソフトウェア（以下「**オプションソフトウェア**」という）は、そのようなソフトウェアに付帯または関連する諸条件のもとで、**エンタープライズ**に対しライセンスが付与されます。**オプションソフトウェア**は、**本契約**の諸条件に従うものではありません。

4. 料金

お客様は、**お客様**に対して発行されたすべての証明書について適用されるすべての**契約料金**を支払うものとします。すべての料金は取消および返金不可です。**本契約**のもと、**Entrust Datacard** に支払われるべき一切の料金は、請求書を発行した **Entrust Datacard 関連会社**に対し支払われるものとします。**契約料金**は、**契約期間**の初めに**請求**されるものとし、**お客様**はこれを相殺、反対請求、減額または控除することなく、請求書発行日から 30 日以内に支払うものとします。**お客様**は、一切の税（**Entrust Datacard** の正味収入に課される税は除きます）、料金、義務または他の同種の負担について責任を負うものとします。支払期限の到来した税は、**お客様**が支払うものとします。**Entrust Datacard** は、料金の支払遅滞について、月利 1.5%または法で許容される上限の料率の利息のいずれかを選択し、**お客様**に請求することとします。上記にかかわらず、**お客様**がリセラーを通じて購入した場合、料金や税に関する諸条件は**お客様**とリセラーの間で決定されるものとします。書面による滞納の通知を受領してから 5 営業日以内に支払がなされない場合、**Entrust Datacard** は証明サービスの一部または全部の提供を停止し、その後の追加の**証明書サービス**の申請の手続きを拒否し、証明書を失効させることができるものとします。

5. 表明、保証、および追加的義務

5.1 **お客様**は、**Entrust Datacard** およびすべての**証明書受益者**に対し、**お客様**が**お客様の関連会社**を**本契約**に拘束する権限を有することを表明し、保証します（該当する状況において、お

お客様の**関連会社**に対して**証明書**が発行されるか、**本契約**に基づいて購入された**管理サービス**に関して**証明書サービス**を受ける場合)。

5.2 お客様は、加入者または対象者として行動する場合は、**お客様**に適用される附属文書 B に規定する要求事項に従うものとします。

5.3 お客様は、**お客様の関連会社**、**代理人**およびその他**本契約**の下または**お客様の管理サービス**を通じて加入者または対象者として行動する一切の法人/個人に対し、**証明書サービス**および**証明書**に関しこれらの行為および役割に適用される附属文書 B を含む**本契約**に規定する要件に従う必要があることを通知し、これらによる順守に責任を負うものとします。

6. 機密保持

本条において、「開示者」とは、以下で定義する機密情報を開示した当事者を意味し、「受領者」とは、これを受領した当事者を意味します。機密情報が当事者の**関連会社**によって開示されたり、受領されたりした場合、その当事者自身によって開示または受領されたものみなされるものとします。受領者は、受領したすべての機密情報の機密性を保持するものとし、**本契約**に基づく権利を行使し、また義務を果たす目的でのみ機密情報を利用するものとします。受領者は、自己の同種の情報に関する権限の無い利用や開示に対するものと同等の注意義務を尽くし、受領した機密情報を取り扱うものとします。ただし、この義務の程度は合理的な注意義務の程度を下回らないものとします。受領者は、一切の書類およびその他の資料に付された専有または機密との説明や注意書きを取り外したり、削除したりしないものとします。受領者は、開示者の機密情報を自己または自己の**関連会社**の機密情報を知る必要がある従業員および**代理人**（以下「**受領者代理人**」という）にのみ開示するものとします。受領者は、**受領者代理人**に本機密保持の規定を順守させるものとし、本機密保持の規定に反する**受領者代理人**の作為または不作為は、受領者の作為または不作為とみなすものとします。機密情報とは、受領者に対し伝達もしくは提示された事業上、技術上、財務上または他の情報で、開示者によって機密と指定された情報または合理的に受領者が機密と考えるべき情報から受領者が得た情報を含みません。機密情報には次のものは含まれません。(i) 個人情報、認証情報または**証明書情報**（これらは、本条に代わり、個人情報、認証情報または**証明書情報**に関する第 12 条の規定に従います）、(ii) 開示の前に合法的に受領者が保有していた情報、(iii) 開示の前に適法に公知となっていたか、**本契約**に反することなく一般に入手可能となった情報、(iv) 第三者が開示者に対する秘密保持の義務を負うことなく受領者に対し開示した情報、または(v) 受領者が開示者の機密情報を参照することなく独自で開発した情報。受領者が、法律、裁判もしくは行政手続または他の法律による要請により開示者の機密情報を開示せざるを得ない場合、受領者は、そのような機密情報が機密に取り扱われるよう合理的な努力を尽くすものとし、法的に許容される場合には、開示者が防御的な他の裁判所命令を取得することができるよう、開示者に

対し事前の通知をするものとします。受領者は、機密情報に関する本条の違反が開示者に回復不能な損害を発生させることがあり、これに対する金銭的な損害賠償が適切な補償とはならないことを認め、他の一切の救済に加え、開示者が本条の違反または違反のおそれに対し、差し止めによる救済を求める権利を有することに同意します。

7. 保証免責

本契約（CPSを含む）に明示された場合を除き、証明書サービスは現状有姿で提供されるものとし、Entrust Datacard は、明示的又は黙示的であるかを問わず一切の表明、条件または保証を否認します。これには、法定、取引慣行、履行慣行または使用上もしくは商業上のものかを問わず、非侵害、権原、商品性もしくは特定の目的への適合性、品質の充足または一切の使用や取引の保証の否認を含みます。Entrust Datacard グループは、第三者の製品またはサービスに関する表明、条件または保証を否認します。これには、一切のベンダー製品または証明書サービスと一緒に使用されるかもしれない他の一切の第三者の製品を含みます。本契約および CPS で明示的に表明、保証および条件づけられたものを除き、証明書サービス、証明書およびデジタル署名認証の使用に関するリスクは、すべてお客様の負担とします。

8. 知的財産に関する補償

8.1 知的財産に関する補償：Entrust Datacard は、本契約の範囲内で提供され、使用された証明書サービスが、カナダ、米国、またはヨーロッパ連合において、特許（発効日時点で公開済みのもの）、商標権、著作権、営業秘密、またはその他の財産権を侵害している旨の第三者からの請求（以下「請求」という）からお客様を保護し、かかる請求に関する手続において、お客様に最終的に下された裁判所判決また仲裁裁定に基づき、すべての損害賠償金、和解金、および費用（裁判費用および妥当な弁護士費用を含むがこれに限定されない）を支払うものとします。ただし、これは、お客様が、(i) 予測されるまたは受け取った各請求について、速やかに書面によって Entrust Datacard に通知し、(ii) Entrust Datacard に、かかる請求の調査、防御、および解決について管理および指揮する包括的な権利を付与し、かつ (iii) 請求について和解または解決していない場合に限られます。

8.2 Entrust Datacard による対応：(a) Entrust Datacard が、実際のもしくは潜在的な請求に気づいた場合、または (b) お客様が Entrust Datacard に対し、実際のもしくは潜在的な請求を通知した場合、Entrust Datacard は、Entrust Datacard 単独で選択し費用を負担することで、以下のいずれかの対応を取ることがあります（お客様に対する差止命令の場合は、必ず対応を取るものとします）。(i) 証明書サービスのうち影響を受ける部分について、お客様が継続して使用できるように権利を調達すること (ii) お客様による使用が権利侵害に当たらないように、証明書サービスの影響を受ける部分を、同等以上の機能の証明書サービスと置き換

えること。(iii) (i) と (ii) がいずれも商業的に合理的でない場合、影響を受ける証明書を失効させ、失効した証明書の費用を案分した金額からかかる証明書に関する未払い金を差し引いて**お客様**に支払うこと。

8.3 補償の例外：以下のいずれかに該当する場合、**Entrust Datacard** は、補償の責任を負わないものとし、かつ**お客様**によって補償され、損害を負わないように防御されるものとします。

(a) **お客様**による**証明書サービス**の使用が、**本契約**もしくは**本契約**で付与されるライセンスの範囲を超えている場合、または **Entrust Datacard** の文書で想定されている**証明書サービス**の使用法または使用目的を逸脱している場合、(b) **証明書サービス**が、事前の書面による**Entrust Datacard** の同意なしに改変された場合、(c) **請求**が、以下のいずれかに起因する権利侵害に基づく場合：(i) 証明書署名要求 (CSR) を発行した Web サーバソフトウェア、(ii) 証明書署名要求 (CSR) もしくはそれに記載されている情報、または (iii) **お客様**が **Entrust Datacard** に提供した情報、データもしくは仕様。

8.4 責任の制限：本第 8 条 (知的財産に関する補償) は、第 9 条 (責任) の定めに従うものとし、**Entrust Datacard** の唯一かつ排他的な責任を定めるものであり、本条に規定されているような請求に関する加入者の唯一かつ排他的な救済とします。

9. 責任

9.1 免責：**Entrust Datacard** グループは、いかなる場合も、結果的、間接的、特別、偶発的、懲罰的もしくはみせしめの損害、または事業、機会、収入、利益、預金、営業権、名声、利用もしくはデータの損失、または再調達もしくは事業中断の費用について責任を負わず、また、**本契約**および **CPS** に基づき提供された証明書または証明書サービスの使用または依拠から直接生じたものでない一切の損失または損害（これには、証明書または証明書サービスを **Entrust Datacard** が提供したものでないソフトウェアもしくはハードウェアと併用または統合することにより生じた損失または損害で、証明書または証明書サービス単体では生じなかったであろう一切の損失または損害を含みます。）についても責任を負わないものとし、**お客様**は、これらに関する一切の権利を放棄します。

9.2 上限：**本契約**、**CPS** ならびに**本契約**に規定する製品およびサービスに付随関連して発生する **Entrust Datacard** グループの責任の総額は、関連する製品またはサービスに関し責任を発生させた時からさかのぼって 12 か月間に **Entrust Datacard** に支払われた額（返金、サービスクレジットまたは控除分については減額する）を超えないものとします。

9.3 適用：免責および責任の上限について規定する本条は、(A) 訴訟（重大な違反を含む契約上のもの、過失を含む不法行為、保証、法律上の義務違反、不実表示、厳格責任、厳格製造物責任その他に関するものを問いません）の形式を問わず、(B) 請求、取引またはデジタル署名もしくは証明書の数等を問わずに総計ベースで、(c) 問題となっている損害が知られていたか、事前に伝えられていたか、または予見可能であった場合であっても、また、(d) 救済が本質的目的を果たさなかったとしても適用されます。お客様は、Entrust Datacard が本契約の本質的な基礎を構成する責任の制限と上限を定める本条項に依拠して、価格を設定し、本契約を締結することに同意します。

9.4 特別の除外：Entrust Datacard またはその関連会社は、以下のいずれかの場合、本契約もしくは CPS に基づいて発行された証明書の使用、誤用またはそれへの依拠から、またこれらに関連して生じた損害について、加入者、依拠当事者、またはその他一切の法人/個人に対して責任を負いません。(i) 期限切れまたは失効の場合、(ii) 本契約または CPS で定める目的以外に使用された場合、(iii) 改ざんされた場合、(iv) 証明書のもとにある鍵ペアまたはそのような鍵ペアの生成に使用される暗号化アルゴリズムが、Entrust Datacard またはその関連会社以外の者（加入者または依拠当事者を含むが、これに限らない）の行為によって侵害された場合、(v) 他の当事者（加入者および依拠当事者を含むがこれに限定されない）の不実もしくは誤解を生じる作為または不作為による場合。本契約で明示的に定める場合を除き、Entrust Datacard およびその関連会社は、いかなる場合も、証明書の内容（VMC の認証マークを含む）が第三者の特許権、商標権、著作権、営業秘密、またはその他の知的財産権の侵害であるとの請求から生じる損害に関し、加入者、依拠当事者、またはその他の当事者への賠償責任を負わないものとします。

9.5 責任に関する本条および本契約の他の条項の定めにかかわらず、適用される法の要求する限りにおいて、Entrust Datacard は、(i) 自己の過失に起因する死亡または身体の傷害、(ii) 自己の詐欺または詐欺的な不実表示、または (iii) 適用される法で除外または制限できない一切の責任について、責任を除外または制限するものではありません。

10. 期間および終了

本契約は、契約期間中有効としますが、お客様またはお客様の関連会社が本契約（誤解を避けるために付言しますが CPS を含みます）の重要な諸条件を順守しない場合、または、Entrust Datacard が本契約に基づくすべての証明書を取消した場合でその取消が契約期間満了前であるときには、早期に終了します。明確性のために付言すると、代理人の違反はお客様による違反とみなされます。また、Entrust Datacard は、Entrust Datacard が従うべき第三者のライセンス供与またはその他の契約上もしくは法律上の義務（業界標準を含みます）を順守するため、お客様に通知することにより、自らの裁量で本契約を終了することができます。お客様

は、**契約期間**の満了または契約の終了時、直ちに**証明書サービス**のすべての使用を中止し、インストールしている機器およびソフトウェアから**本契約**に基づき発行したすべての証明書を除去しなければなりません。**本契約**の終了後の履行を意図または要求する条項、または、期間および終了を規定する本条の諸条件、機密保持、責任の制限および除外ならびに支払義務を含むその本質的な目的の履行のために存続すべき**本契約**の条項は、終了後も存続し、完全に履行されるまで、またはその本質的な目的の履行のために必要な期間、完全な効力を保持するものとします。

11. セキュリティ、不正アクセス

お客様は、パスワードその他のログイン情報を保護することを含め、**証明書サービス**への不正アクセスを防止するためのあらゆる合理的な措置を講じるものとします。**お客様**は、**証明書サービス**の不正使用もしくは**証明書サービス**に関連するセキュリティの違反が判明した場合またはその疑いがある場合、直ちに**Entrust Datacard**に通知し、当該違反を止めるために商業的に合理的な努力を尽くすものとします。**Entrust Datacard**が、実際のまたは潜在的なセキュリティ上の懸念（**証明書サービス**により処理される他の顧客もしくはそれらの使用者の情報、他の情報もしくはデータのセキュリティに関するものを含む）に対応するために合理的に必要であると判断する場合、**Entrust Datacard**は、その範囲内で、**お客様**に書面で通知して、そのようなセキュリティ上の懸念が適切に対処されるまで、該当する**証明書サービス**の全部または一部の提供を停止することができます。**Entrust Datacard**は、セキュリティ上の懸念に関する最新の状況をお客様に伝えるものとします。

12. 個人情報、認証情報および証明書情報

12.1 個人情報：**Entrust Datacard**が、**お客様**のために**本契約**の履行に際して個人情報（DPAに定義される）を処理するかぎり、ここに言及されることで本書に組み込まれるDPAの諸条件が適用され、両当事者は当該諸条件を順守することに同意するものとします。**お客様**による**本契約**の受諾は、DPA（DPAに添付される標準契約条項を含みます）の受諾および署名として取り扱われるものとします。**Entrust Datacard**は、法律および規則の要求に応えるため、DPAを随時更新し、製品およびサービスについて改良および強化により最新の状態に保つ権利を留保します。**Entrust Datacard**のウェブサイトに掲載される最新版が常に適用されるものとします。**お客様**は、申請プロセスまたは**証明書サービス**の利用を通じて、個人情報が不必要に**Entrust Datacard**に開示されないことを確保するものとします。

12.2 第三者データベース：限定的な認証を行う際、**Entrust Datacard**は、**お客様**の**証明書サービス**申請とともに提供された組織の識別情報、住所、およびドメイン名が、第三者データベース（以下「データベース」という）と一致していることを確認します。**Entrust Datacard**

は、特定の個人情報やその他の情報を確認する調査を行うことがあります。これにはたとえば、**お客様**の商号、住所、電子メールアドレス、電話番号、業種、設立年、従業員数、CEO、電話番号、および**お客様**の会社の存立（総称して「認証情報」）などの情報が含まれます。**お客様**は、認証情報の一部がデータベースに追加される場合があることを承諾するものとします。

12.3 **証明書情報**：Entrust Datacard は、認証情報や個人情報を含め、**お客様**が**証明書サービス**の申請で Entrust Datacard に提供した任意の情報を証明書に挿入することができます（以下「**証明書情報**」という）。また、Entrust Datacard は、以下のことができるものとします。（a）**お客様**が Entrust Datacard に提供した情報を加入者の認証に使用すること、（b）一般ユーザーが参照できる1つまたは複数の CT（Certificate Transparency: 証明書の透明性）ログに**お客様**の証明書を公開すること、（c）**本契約**および Entrust Datacard 個人情報保護方針に定める目的でかかる情報を使用すること。**お客様**は、Entrust Datacard が米国および/またはカナダならびに Entrust Datacard グループが所在するその他の法域で**証明書情報**を処理および/または転送することを認識し、これに同意するものとします。

12.4 その他のプライバシー規定：個人情報、認証情報および**証明書情報**に関する本条または DPA に別段の定めがない限り、Entrust Datacard は、**本契約**に基づいて**証明書サービス**を履行する中で取得した個人情報、認証情報、または**証明書情報**を第三者に開示しないものとします。ただし、Entrust Datacard は次の場合、該当情報を提供することができます。（i）受け取った裁判所命令もしくは召喚状に対応するため、または Entrust Datacard の法律顧問に従って、裁判所、法執行機関またはその他の第三者に提供する場合（民事開示手続きに応じた開示を含む）、（ii）Entrust Datacard から見て、**お客様**の詐欺、虚偽表示、不正アクセスが疑われるか、その他違法行為の可能性があるときに、これらを調査する目的で法執行機関の職員に提供する場合、（iii）Entrust Datacard が**本契約**に基づく責任を果たすために必要な範囲で第三者に提供する場合。

13. Entrust セキュアサイトシールの使用

本契約の諸条件に従うことを条件に、**お客様**は**証明書サービス**を Entrust セキュアサイトシールとともに使用することができます。ただし、利用には、（i）Entrust Datacard が**お客様**に対し**証明書サービス**とともにまたはそれに関連して Entrust セキュアサイトシールを提供する必要があり、（ii）下記[Accept（同意する）]アイコンをクリックし、Entrust セキュアサイトシールを使用することにより、**お客様**は、Entrust セキュアサイトシールに関するライセンス契約（<http://www.entrust.net/cps>（[英文](#)）に掲載）の諸条件への拘束に同意したものとみなされます。

14. 第三者製品

お客様は、特定の第三者**ベンダー**（以下「**ベンダー**」という）の製品およびサービス（以下「**ベンダー製品**」という）が**証明書サービス**を通じてまたはこれに関連して提供される場合があることを認識し、同意します。**本契約**に明示的に記載されている場合を除き、**Entrust Datacard**は、**ベンダー製品**に関する義務を負わず、すべての責任から免責されます。**ベンダー製品**の使用は、**ベンダー製品**に組み込まれる、またはその他の方法で提供される**ベンダー**の諸条件およびポリシー（以下「**ベンダー条件**」という）のみに従うものとします。

特に、

14.1 **お客様**が**Entrust Datacard**を通じてまたは**証明書サービス**に関連して、Sixscape **ベンダー製品**を購入する場合、Sixscape **ベンダー製品**の使用は、製品に組み込まれるかまたは一緒に提供される Sixscape **ベンダー**の諸条件に従うものとし、これは、

www.sixscape.com/product-and-warranty/（[英文](#)）から入手できます。**Entrust Datacard**は、インターネット上の www.entrust.net/cps（[英文](#)）から入手可能な ECS サポートサービス契約書の諸条件に基づき、Sixscape **ベンダー製品**に関するサポートを提供するものとします。ただし、次の場合を除きます。(a) インシデントの解決に**ベンダー製品**の変更または修正が必要な場合、**Entrust Datacard**の唯一の義務は、そのインシデントを**ベンダー**に伝達することとし、(b) ECS サポートサービス契約書に定める期間は、**Entrust Datacard**が**ベンダー**からの回答または解決を待つ必要があるすべての時間を除外するものとします。

14.2 **お客様**が、WebID face-to-face 認証に関する**ベンダー製品**を使用する場合、その使用は、使用に先立ち承諾しなければならない当該 WebID **ベンダー**の諸条件に従うものとします。**お客様**は、管理ポータルを通じて、個人情報を含む認証情報を WebID に提出する権限があること、および WebID が認証結果を報告するために記録データのパッケージを **Entrust Datacard** に引き渡すことを認め、同意します。明確にするために付言すると、認証情報および個人情報の **Entrust Datacard** による処理は、すべて、**本契約**の第 12 条（個人情報、認証情報および**証明書情報**）の規定に従って行われ、WebID による処理は、WebID **ベンダー**の諸条件に従って行われます。

15. 分離

適用される法で許容されるかぎりにおいて、両当事者は、**本契約**（**CPS**を含みます）の一部を無効またはその他何らかの点で執行不能とする法律の適用を放棄します。**本契約**のある条項が、特定の事実または状況に適用されるにあたり、無効またはその他執行不能を判示された場合、(a) 当該条項は、適用法により許容される最大限の範囲において、その意図された目的を遂行するために必要な範囲で解釈および修正され、他の事実または状況に適用されるその**有**

効性および執行可能性は、影響を受けず、また損なわれないものとします。(b) 他の**本契約**の条項は、引き続き完全に**有効**に存続します。念のため付言すると、責任の制限および免責、表明、保証および諸条件の否認、または補償に関する各条項は、他の一切の条項から分離可能であることが明示的に理解され意図されています。

16. 関係性

本契約のいかなる規定も、いずれかの当事者またはその従業員について、相手方当事者のパートナー、**代理人**、フランチャイジーまたは法定**代理人**となるとはみなされず、また、目的のいかんを問わず、信託関係を作成するとはみなされません。**本契約**に別段の明示の規定がある場合を除き、**本契約**のいかなる規定も、いずれかの当事者またはその従業員に対し、相手方当事者のために行動し、拘束し、または義務もしくは責任を作成または引き受ける権限を付与するものではありません。両当事者は、**Entrust Datacard** のいかなる従業員も**お客様**の従業員ではなく、将来もそのようにみなされるものではないことに合意します。

17. Entrust Datacard の関連会社

Entrust Datacard は、**本契約**に基づく自己の義務を履行するために、1つまたは複数の**関連会社**を使用することができます。ただし、これが**Entrust Datacard** の**本契約**上の義務に影響を及ぼさないことを条件とします。

18. 第三受益者

本契約で明示的に規定されている**証明書受益者**または両当事者が書面で別段の合意をした場合を除き、**本契約**は、その両当事者ならびにそれぞれの継承者および承諾された譲受人の利益のためにのみ締結され、他のいかなる個人または法人は、1999年英国契約法（第三者の権利）に基づくものを含め、**本契約**に基づくいかなる権利または利益も有するものではなく、取得しません。

19. ハイリスクアプリケーション

お客様は、**証明書サービス**の不具合が人の死亡、傷害、または深刻な身体もしくは財産の損害につながる可能性のあるアプリケーション（以下「**ハイリスクアプリケーション**」という）において、**証明書サービス**の一切を使用せず、また第三者に使用させないものとします。これには、原子力施設、大量輸送システム、航空機ナビゲーションもしくは航空機通信システム、航空交通管制、兵器システム、および直接生命維持機器を監視、操作または制御するものを含みます。**Entrust Datacard** は、**ハイリスクアプリケーション**への適合性に関する一切の明示または黙示の保証を明確に否認します。

20. 非排他性

本契約のいかなる規定も、**Entrust Datacard** またはその**関連会社**が、**本契約**に基づき**お客様**に提供される製品、サービスまたは成果物と同一もしくは類似の製品、サービスまたは成果物を第三者に提供することを妨げるものではありません。

21. 通知

CPS に基づいて何らかの通知またはその他の通信が必要となった場合、または、発信が許可される場合、そのような通知または通信は、**CPS** の指定に従い提供されるものとします。その他の通知もしくは通信が必要もしくは許可される場合、または **CPS** に指定がない場合、通知もしくは通信は、書面によるものとし、(a) 受領と同時に送達されたとみなされる手交、または、(b) 配達を確認された時点で送達があったとみなされる下記住所への配達確認付きの国際航空宅配便によるものとする。

お客様への通知:注文書に記載されている住所

Entrust Datacard への通知: 1000 Innovation Drive, Ottawa, Ontario, Canada K2K 3E7

22. パブリシティ

契約期間中およびその後 30 日間、**お客様**は、**Entrust Datacard** に対し、ウェブサイトまたはその他マーケティングもしくは広告資料において、**お客様**を **Entrust Datacard** の顧客として特定するために、**お客様**の名称および/またはロゴを世界中において無償で使用する権利を許諾するものとします。

23. 法の選択

本契約に基づいて提供される製品およびサービスに関連する紛争、ならびに**本契約**の解釈、有効性、翻訳、執行可能性および履行については、(i) **お客様**がアメリカ合衆国に所在する場合、アメリカ合衆国ミネソタ州の法律に準拠し、ミネソタ州ヘネピン郡に所在する連邦裁判所および州裁判所に提起されるものとし、(ii) **お客様**が他の世界中のいずれかの場所に所在する場合、カナダ・オンタリオ州の法律に準拠し、オンタリオ州オタワに所在する州または連邦裁判所に提起されるものとします。各当事者は、法の選択に関する本条項において特定される該当する裁判所が、当該紛争に対して人的な排他的管轄権を有することに同意します。郡、州または連邦裁判所に何らかの案件が提起された場合、各当事者は陪審による裁判を受ける権利を放棄します。適用法で許容される最大限において、両当事者は、改正された国際物品売買契

約に関する国連条約の規定が**本契約**に適用されないことに合意します。法の選択に関する本条は、不法行為を含む**本契約**に起因または関連するすべての請求に適用されます。

24. 不可抗力

不可抗力による遅滞または履行不能に起因する場合、**本契約**に基づく **Entrust Datacard** の義務の履行遅延または履行不能は**本契約**の違反とならず、その結果につき一切責任を負わないものとします。ただし、(i) **Entrust Datacard** が、**お客様**への損害を限定し、義務の履行を再開するために合理的な努力を尽くすこと、および(ii) 遅延または履行不能が、**Entrust Datacard** が当該不可抗力と同種の事象または状況を回避するための合理的な措置を講じなかったことに起因するものでないことを条件とします。不可抗力とは、天災または公共の害悪、内乱、騒乱、暴動、反乱、戦争、テロ、悪意による損害、事故、火災、洪水、ハリケーン、地震、暴風雨、ストライキおよびその他の労働争議（**Entrust Datacard** が要求を認める立場にあるか否かを問いません）、禁輸措置、民間または軍事当局の行為、司法措置、公共施設、輸送または通信インフラの障害（インターネット、電話ならびに通信およびネットワーク回線、サーバー、ファイアーウォール、プロキシサーバー、ルーター、スイッチおよびブリッジを含みます）、上位 CA の不全または不履行、輸出許可もしくは承認、必要な労働力、材料、エネルギー、光熱源、部品もしくは機械の欠如または取得不能、および第三者供給業者もしくはサービスプロバイダーの行為または不履行を含み、予見可能性の有無を問わず、**Entrust Datacard** によって引き起こされたものではない一切の事象または状況を意味します。

25. 権利放棄の否定

権限を有する代表者の明確な書面による放棄の場合を除き、一切の権利、救済もしくは権限に関する不行使、行使の遅れならびに言及または表明をしないことは、これらの放棄となるものではなく、**本契約**に基づくいかなる権利、救済または権限の単独または部分的行使も、その他の権利または更なる行使を不可能にするものではなく、**本契約**、法律もしくは衡平法に定めるその他の権利、救済または権限の行使を妨げないものとします。**本契約**に基づく行為または条件の履行期限の放棄は、行為または条件自体の放棄となるものではありません。

26. 承継人と譲渡

各当事者は、相手方当事者の事前の書面による同意なく、**本契約**または**本契約**に基づく権利もしくは義務を、自発的、非自発的、法律の運用その他であることを問わず、譲渡、売却、移転またはその他の処分を行わない（いずれの当事者もこれを行う権利を有するものではありません）ことに同意します。承継人と譲渡に関する本条に反する譲渡、売却、移転、委任その他の処分は効力を生じず、無効です。上記にかかわらず、**Entrust Datacard** は、**お客様**の同意を得ることなく、**本契約**を**本契約**上の権利および義務と共に、(i) **関連会社**に譲渡することがで

き、または (ii) **本契約**に関連する事業のすべてまたは実質的にすべての資産の売却、合併もしくはその他の移転の一部として譲渡することができます。上記の譲渡および委任の制限に従ったうえで、**本契約**は、両当事者ならびにそれぞれの継承者および承認された譲受人を拘束し、それらの利益のために効力を生じるものとします。

27. 適用される法の順守

証明書サービスおよび関連情報、ならびに**証明書サービス**の処理または**証明書サービス**と併用して使用される特定の暗号技術、ソフトウェア、ハードウェアおよびファームウェア（総称して「技術」）は、輸出、輸入、および/または使用の制限を受けることがあります。**お客様**は、あらゆる点で、適用されるすべての法律、規則および規制を順守し、**お客様**ならびに**お客様**の加入者および対象者による技術の受領および**本契約**の一部に基づく自己の権利の行使に関連して、要求される可能性のあるすべての許可、ライセンス、認可または証明書を取得するものとします。**お客様**は、自身ならびにその**関連会社**、加入者および対象者に関し、(a) **本契約**に基づきライセンス許諾されたソフトウェアもしくは技術または関連情報の輸出が、米国、カナダまたはその他の適用法域の適用法令、規則または規制により禁止される国に所在せず、当該国の管理下になく、また当該国の国民もしくは居住者ではないこと、(b) **本契約**に基づきライセンス許諾されたソフトウェアもしくは技術または関連情報の輸出物受領者が米国、カナダまたはその他の適用法域の法律により禁止されるような個人ではないこと、および(c)

Entrust Datacardによりもしくは**Entrust Datacard**を通じて提供される製品またはサービスの輸出を管理する米国、カナダおよびその他の適用法域、州、地方または適用法域の適用法令、規則ならび規制を順守し、将来においても順守することを表明し、保証します。**お客様**は、適用される輸出に関する法律、規則または規制によって禁止されている目的のために、**証明書サービス**を一切使用せず、また、その使用を許可しないものとします。これには、核兵器、化学兵器または生物兵器の拡散に関連するものを含みますがこれらに限定されません。

28. 他の権利の非付与

本契約に基づいて付与される権利は、**本契約**に明示的に規定されるもののみです。**本契約**の結果としてまたは**本契約**に基づくいずれかの当事者の行為によって、黙示、禁反言、推論またはその他によるかを問わず、他の権利または便益が付与されたり、付与されたりしたとみなされることはありません。**Entrust Datacard**およびそのライセンサーは、**Entrust Datacard**が提供する製品およびサービスに関するすべての所有権、権原ならびに利益を明示的に保持します。**お客様**に提供されたもの全部または一部の許可された複製には、**Entrust Datacard**が**お客様**に納品したものに表示されているように、すべての著作権表示、制限付きの権利表示、専有マークなどが含まれていなければなりません。

29. 言語

CPSを含む**本契約**の最終版は、英語で記載されます。**本契約**が他の言語に翻訳され、英語版と翻訳版の間に矛盾がある場合、英語版を正文とします。

30. 完全合意

CPSを含む**本契約**は、**本契約**の主題に関する当事者間の完全な合意を構成するものとし、従前のすべての通信、合意、提案およびその他の通信は、**本契約**の諸条件に完全に取って代わるものとし、注文書またはこれに関連する文書の諸条件は、加入する**証明書サービス**の特定および数量以外には効力を有しません。注文書に含まれるソフトウェアは、そのソフトウェアに付属する契約条項に基づいて提供されます。

31. 解釈

両当事者は、**本契約**がいずれかの当事者に有利または不利に厳格な解釈をされることなく、その条件に従って公正に解釈されること、および曖昧さは関連する文言を起草した当事者に不利に解釈されないことに合意します。**本契約**において、「含まれる」、「含む」、および「含みます」という用語は、それぞれ、「これに限定されない」という語が後に続くものとみなされます。**本契約**中の条項または他の見出しは、便宜のためおよび参照の容易性のためにのみ挿入されるものであり、**本契約**のいずれかの条項の解釈または理解において考慮されるものではありません。**本契約**において言及される附属文書、文書または別表とは、**本契約**およびその適用される条項において許容される範囲内で、随時、修正、補足および変更される附属文書、文書または別表を意味します。法令または規則への言及は、その時点で改正された法令または規則を意味し、後にこれらを承継したものを含みます。別段の定めがない限り、前文、条、小節、項、別表および附属文書への言及は、**本契約**の前文、条、小節、項、別表および附属文書を言及したものとなります。**本契約**におけるすべてのドル金額は、別段の表示がない限り、米国通貨をいいます。

附属文書 A

証明書申請者:

証明書承認者:

契約署名者:

WEB ホスティング 業者:

技術的連絡先:

附属文書 B

加入者および対象者の表明、保証および義務

第 1 部：加入者

加入者に対してまたは加入者のために発行される証明書を有する条件として、各加入者は、本人として、また該当する場合には下請業者もしくはホスティングサービス関係に基づくその支配者または**代理人**として、**証明書受益者**、**Entrust Datacard**、および加入者に対してまたは加入者のために証明書を発行する **Entrust Datacard** の**関連会社**の利益のため、以下を表明し、約束し、確約し、また保証します。

1. 加入者が他の法人/個人に対して、または他の法人/個人のために証明書の発行を申請している場合、当該他の法人/個人は、自身に代わって加入者が証明書を**請求**することを含め、加入者と同様に、加入者が当該他の法人/個人に代わって本附属文書の表明、約束、確約および保証を行うことを許諾していること。
2. 加入者は、証明書に関連して使用される新しい、安全で暗号として健全な鍵ペアを（**CPS** において要求される場合、暗号モジュールにおいて）生成すること。
3. 証明書要求および証明書発行に関連するその他の方法を含め、**証明書サービス**に関連して加入者が常時提供するすべての情報および表明は、完全で、正しくかつ正確であり（当該情報および表明は、そのような完全性、正確性および的確性を維持するために必要に応じて随時速やかに更新される）、いかなる法域においても、いかなる個人、事業体または組織の知的財産またはその他の権利も侵害せず、誤用せず、希釈せず、不当に競合せず、また、その他違反をしないこと。明確にするため付言すると、事前の資格情報を使用して証明書の要求を提出するにあたり、加入者は、本附属文書Bに定める表明、約束、確約および保証を新たに行ったものとみなされ、当該情報がその後何らかの形で変更されたか、または不的確、不正確、誤解を招く可能性があることが判明した場合、**Entrust Datacard** は、事前の資格情報を含む証明書を発行する義務を負いません。
4. 証明書要求と共に**Entrust Datacard**に提出された公開鍵に対応する秘密鍵は、健全な暗号技術を用いて作成されたこと、また、秘密鍵（および関連するアクセスまたはアクティベーションデータまたはデバイス、たとえばパスワードやトークン）の管理(**EV**コード署名証明書の場合は単独の管理)、秘密の保持、適切な保護、権限のない使用の禁止をするためのあらゆる合理的な措置を講じること。これには、コード署名証明書および**EV**コード署名証明書に署名する場合の**コード署名基本要項**にある『Data Security and Private Key Protection』（データセキュリティおよび秘密鍵の保護）に関する規定を含みます。
5. 秘密鍵を保管する機器が安全な方法で操作され、維持されること。

6. 加入者（またはコード署名証明書の場合は加入者の**代理人**）が、証明書の内容が的確かつ正確であることを確認するまで証明書をインストールまたは使用しないこと。
7. **Entrust Datacard** のSSL証明書、**EV SSL**証明書、およびプライベートSSL証明書の場合
はすべて、証明書に掲げられているドメイン名（subjectAltName（s））でアクセス可能なサーバーにのみ証明書がインストールされること。
8. 証明書および当該証明書に記載された公開鍵に対応する秘密鍵は、すべての適用法を順守し、**本契約**に基づき権限を有する企業/団体の事業のためのみに使用され、当該証明書に
対象者として記載された組織に代わってのみ使用されること。
9. 証明書の内容を不当に変更しないこと。
10. 加入者は、次の場合、**Entrust Datacard**に通知し、すべての証明書および証明書の公開鍵
に対応する秘密鍵のすべての使用を停止し、証明書の失効を要求すること。
 - 10.1. 証明書または証明書の申請書に含まれる情報が変更された場合、不正確もしくは
不的確である、またはそのようになった場合、または何らかの事情の変更により
証明書の情報が誤解を招く可能性が出てきた場合（速やかに）
 - 10.2. 証明書の公開鍵に対応する秘密鍵（またはキーアクティベーションデータ）につ
いて、紛失もしくは紛失の疑い、盗難、誤用または侵害があった場合（直ち
に）。これには、秘密鍵の値が未承認者に開示された場合または未承認者がアク
セスした場合（以下「**鍵の侵害**」という）を含み、また、その他の理由で秘密鍵
の支配が失われた場合を含みます。
 - 10.3. コード署名証明書または**EV**コード署名証明書の場合、証明書が**サスペクトコード**
に署名するために使用された証拠がある場合（直ちに）
11. 証明書の期間の満了または失効と同時に、加入者は、当該証明書および当該証明書の公開
鍵に対応する秘密鍵のすべての使用を速やかに中止し、当該証明書をインストールした機
器またはソフトウェアから削除すること。
12. 加入者は、**鍵の侵害**または証明書の誤用もしくは誤用の疑いに関する**Entrust Datacard**の
指示に直ちに応じること。
13. 次の場合、**Entrust Datacard**が直ちに証明書を取り消す権利を有することについて、加入
者が認識し、同意すること
 - 13.1. **お客様**が**本契約**に違反した場合
 - 13.2. **Entrust Datacard**が証明書の**秘密鍵の侵害**を発見した場合
 - 13.3. **Entrust Datacard**が、フィッシング攻撃、詐欺または**サスペクトコード**の配布を
含む犯罪行為を可能にするために証明書が使用されていることを発見した場合
 - 13.4. **Entrust Datacard**が、証明書または証明書で使用された公開鍵に関連する秘密鍵
が**サスペクトコード**に電子署名するために使用されたことを発見した場合
14. 証明書に記名された対象者が加入者とは別の法人/個人である場合、対象者が対象者の情
報を証明書に含めることを承認したこと。

15. 加入者は、証明書に記載されたドメイン名またはメールアドレスを所有、管理、または使用する独占的な権利を有すること。
16. 加入者が、**業界標準**の変更に従うために必要な場合、**Entrust Datacard**が**本契約**を修正する権利を有することを認識し、これに同意すること。
17. 加入者は、証明書によって提供されるセキュリティおよび信頼の水準を考慮して、所定の状況において証明書を使用することが適切かどうかについて適切な判断をすること
18. 加えて、コード署名証明書および**EV**コード署名証明書に関しては、
 - 18.1. 加入者は、<https://www.entrustdatacard.com/pages/guides-and-whitepapers>にアクセスするか、または**Entrust Datacard**に連絡することにより入手可能なコード署名ベストプラクティス文書（以下「**コード署名ベストプラクティス**」という）に記載されているコード署名に関する最良の事例を採用するために商取引上合理的な努力を払うこと
 - 18.2. 加入者は、コード署名ベストプラクティスに記載されているように、秘密鍵を保管する機器を安全な方法で生成および操作し、秘密鍵を輸送するために大文字、小文字、数字および記号を含む少なくとも16文字でランダムに生成されるパスワードを使用すること
 - 18.3. 加入者は、他の種類の**証明書**と共に使用されるまたは使用される可能性のある公開鍵を含むコード署名**証明書**または**EV**コード署名**証明書**を要求しないこと
 - 18.4. **証明書**および当該**証明書**の公開鍵に対応する秘密鍵は、認可された合法的な目的にのみ使用され、**サスペクトコード**にデジタル署名するために使用されないこと
 - 18.5. **証明書**の公開鍵に対応する秘密鍵の悪用から保護するために、適切なネットワークおよびその他のセキュリティ管理を提供すること
 - 18.6. 加入者は、以下の場合、CA/ブラウザーフォーラムを含む他の認証局または業界団体と、加入者、署名済みのアプリケーション、**証明書**、および周辺環境に関する情報を共有する権限を**Entrust Datacard**に与えることを認識し、同意すること
 - 18.6.1. **証明書**が**サスペクトコード**のソースとして特定された場合
 - 18.6.2. **証明書**を要求する権限が検証できない場合
 - 18.6.3. **証明書**が**お客様**の要求以外の理由で取り消された場合（秘密鍵の侵害、マルウェアの発見その他の理由など）
 - 18.7. 加入者は、ASVが独自に**証明書**について悪意または危険であると判断する可能性があること、およびASVおよびASV製品が、**お客様**または**Entrust Datacard**に通知することなく、かつコード署名**証明書**または**EV**コード署名**証明書**の失効の状況にかかわらず、**お客様**の行為を修正する、またはコード署名**証明書**もしくは**EV**コード署名**証明書**を「ブラックリスト」に登録する能力を有する可能性があることを認識すること

- 18.8. **EV**コード署名**証明書**に関して、**お客様**は、**証明書**を**EV**コード署名ガイドラインに記載される要件に適合する署名コードについてのみ使用すること
19. 加えて、**eIDAS QWACs**および**PSD2 QWACs**の場合、
 - 19.1. 加入者は、安全な暗号装置を使用するための**CPS**の諸条件を順守し、必要に応じて、
 - 19.1.1. 対象者の秘密鍵を安全な暗号装置とともに暗号機能にのみ使用し、
 - 19.1.2. 対象者の鍵が加入者または対象者の管理下で生成される場合、対象者の鍵を安全な暗号生成装置で生成する。
 - 19.2. 加入者は、**Entrust Datacard**が登録、対象機器の条件（これが加入者に対するものであるかどうかに限らず、異なる場合には対象者に対するものであるものを含みます）、その後の一切の取消、**証明書**に記載された身元および一切の具体的な属性に使用された情報の記録を保管すること、ならびに**Entrust Datacard**がサービスを終了する場合に**業界標準**に必要な条件と同一の条件でこれらの情報を第三者に移転させることに同意すること
 - 19.3. 加入者は、**CPS**に定める方法および諸条件に従い、**証明書**の公開を要求し、該当する場合には、その公開に対する対象者の同意を得ること
 - 19.4. 秘密鍵および**証明書**に関連付けられた対応する公開鍵は、**CPS**を含む、加入者に通知された制限に従ってのみ使用すること
 - 19.5. 加入者または対象者が対象者の鍵を生成する場合、
 - 19.5.1. 対象者の鍵は、**CPS**に明記されている認証鍵の使用に関する**業界標準**に規定されているアルゴリズムを使用して生成されること
 - 19.5.2. 鍵の長さおよびアルゴリズムは、**証明書**の有効期間中、**CPS**に明記される認証鍵の使用に関する**業界標準**に規定されたとおりとすること
 - 19.5.3. 対象者が個人である場合、対象者の秘密鍵は、対象者単独の管理下に置かれること
 - 19.5.4. 対象者が個人ではなく法人の場合、対象者の秘密鍵は対象者の管理下に置かれること
 - 19.6. 対象者の**証明書**が取り消されたこと、または発行CAが危険にさらされたことが通知された場合、加入者は、**証明書**の公開鍵に対応する秘密鍵が対象者によって使用されないことを保証すること
20. 加えて、**VMC**の場合：
 - 20.1. 加入者は、**VMC**ガイドラインに従い、**VMC**を申請し、使用すること
 - 20.2. **VMC**アプリケーションで提出される商標は、加入者が所有するか、または**VMC**ガイドラインに添付されている利用規約において限定的なライセンスを許諾できる十分なライセンスを取得している登録商標を表示し、該当する商標を所有してい

ない、または十分なライセンスを有していない場合は、ただちに**VMC**を取り消すこと

第2部：個別の対象者で、加入者と異なる場合

対象者と加入者が別個の法人であり、対象者が法人/個人（すなわち機器ではないこと）である場合、対象者に発行された eIDAS QWAC または PSD2 QWAC を有する条件として、対象者は以下の義務を受諾するものとします。

1. 対象者は、安全な暗号装置を使用するための**CPS**の諸条件を順守するものとし、必要に応じて、対象者の秘密鍵を、安全な暗号装置とともに暗号機能にのみ使用すること
2. 対象者は、登録、対象機器の条件（これが加入者に対するものであるかに限らず、異なる場合には対象者に対するものを含みます）およびその後の一切の取り消し、**証明書**に記載された身元および一切の具体的な属性に使用された情報の記録を**Entrust Datacard**が保持することに同意し、**Entrust Datacard**がサービスを終了する場合にETSI EN 319 411-1が要求する条件と同一の条件で第三者に当該情報を移転することに同意すること
3. **証明書**に関連する秘密鍵および対応する公開鍵は、**CPS**を含め、対象者に通知された制限に従ってのみ使用すること
4. 対象者の秘密鍵の権限のない使用を禁止すること
5. 対象者の鍵を生成する場合において、
 - 5.1. 対象者が個人である場合には、対象者の秘密鍵は、対象者単独の管理下に置かれること
 - 5.2. 対象者が個人ではなく法人である場合には、対象者の秘密鍵は対象者の管理下に置かれること
6. 対象者は、次の場合、直ちに**Entrust Datacard**に通知すること：
 - 6.1. **証明書**に含まれる情報が変更された場合、不正確もしくは不的確である、またはそのようになった場合、または状況の変化により**証明書**の情報が誤解を招く可能性が出てきた場合
 - 6.2. **証明書**内の公開鍵に対応する秘密鍵（またはキーアクティベーションデータ）の紛失もしくは紛失のおそれ、盗難、誤用または侵害の疑いがある場合。この場合、該当する鍵の使用を直ちにかつ永久的に中止すること。これには、秘密鍵の値が権限のない者に開示されているか、または権限のない者がアクセスしていた場合、またはその他の理由で秘密鍵に対するコントロールが失われた場合を含む。
7. 対象者の**証明書**が失効したこと、または発行されたCAが危険にさらされたことを知らされた場合、対象者は秘密鍵を使用しないこと

