

KS Solutions 証明書発行サービス 利用法人規約

第1条（目的）

1. 「KS Solutions 証明書発行サービス 利用法人規約」（以下、「本規約」という）は、株式会社オプテージ（以下、「オプテージ」という）が運営する「KS Solutions ルート認証局」および「KS Solutions ユーザ証明書認証局」（以下、「KS Solutions ルート認証局」と「KS Solutions ユーザ証明書認証局」をまとめて「本認証局」という）にて提供する「KS Solutions ユーザ証明書発行サービス」（以下、「本サービス」という）の利用に関して、本認証局と本サービスの利用契約（以下、「利用契約」という）を締結した法人等（以下、「利用企業」という）との関係を定めるものである。
2. 利用企業の社員、役員、外部委託者等（以下、「証明書利用者」という）が本サービスを利用するには、利用企業が本規約の内容に同意したうえで、本認証局に対してユーザ証明書の発行を申請しなければならない。
3. 利用企業は、日本国内で商業登記を行っている法人、あるいは日本国内法に従って設置された公の団体でなければならない。
4. 証明書利用者が自然人でない場合、当該利用企業を証明書利用者を含むものとする。
5. 本規約に記載されていない本サービスに関する事項に関しては、別途「KS Solutions 証明書発行サービス 認証局運用規則」（「Certification Practice Statement」以下、「CPS」という）に定める。

第2条（サービス）

1. 本サービスにより本認証局が証明書利用者に対して発行する電子証明書（以下、「ユーザ証明書」という）の利用目的は、以下の事由のみとする。
 - ① 情報システム等へ認証によるアクセスコントロール
 - ② 電子メールの署名・暗号化
2. 利用企業は、証明書利用者对本規約および CPS に定める適用範囲内において利用させる義務を負う。

第3条（ユーザ証明書の発行申請）

1. 証明書発行申請に際し、利用企業は事前に当社指定システムより申請もしくは、印鑑証明書によって照合可能な印（以下、「公印」という）で捺印した「申請担当者登録依頼書」によって、利用企業内の特定の担当者（以下、「利用企業担当者」という）とその連絡先電話番号を本認証局に登録しなければならない。
2. 利用企業は、公印を捺印した「セキュリティデバイス発注依頼および代行入力依頼書」

に必要事項を記載し、利用企業担当者を通じて、本認証局にユーザ証明書の発行申請を行う。ただし、利用企業が別の申請書類に公印を捺印している場合、「セキュリティデバイス発注依頼および代行入力依頼書」への捺印は省略できる。

3. 本認証局と利用企業との間で協議を行った結果、本認証局が承認した場合に限り、公印を代替印に変更することができる。
4. ユーザ証明書発行に関する申請手段としては「セキュリティデバイス発注依頼および代行入力依頼書」による申請方法以外に、本認証局と利用企業との間で協議を行った結果、本認証局が承認した場合に限り、代替方法を使用することができる。

第4条（ユーザ証明書の発行、送付手順）

1. 本認証局は、第3条による手続きで登録された利用企業担当者からのユーザ証明書の発行申請を受理し、所定の方法で審査を行う。その結果、本認証局にて発行承認を得た申請内容に関して、ユーザ証明書の発行を行う。
2. 本認証局は審査の結果、ユーザ証明書を発行できないと判断した場合、発行不承認の旨とその理由を所定の方法により通知する。
3. 本認証局は、発行したユーザ証明書と証明書利用者の秘密鍵（以下「ユーザ証明書一式」という）をセキュリティデバイスに格納し、利用企業担当者に送付する。但し、証明書インストール時にセキュリティデバイスが接続できない端末を利用する場合は、PKCS#12形式のデータを用い、ユーザ証明書一式を利用企業担当者へ送付する。
4. 本認証局は、ユーザ証明書一式を利用可能な状態にするためのPIN（以下、「利用者PIN」という）を、所定の方法により通知する。
5. 利用企業担当者は、本認証局より送付したセキュリティデバイスもしくはユーザ証明書一式および利用者PINを安全かつ確実に証明書利用者のもとに届けなければならない。
6. 利用企業担当者および証明書利用者は、セキュリティデバイスもしくはユーザ証明書一式を受領後、速やかにセキュリティデバイスもしくはユーザ証明書一式の記載誤りや疑義、初期不良が無いことを確認する。
7. 本認証局は、セキュリティデバイス送付後、所定の手順により受領登録されていることを確認、もしくはお客さまより受領書が返送されていることを確認し、ユーザーがセキュリティデバイスもしくはユーザ証明書一式を受領したとみなす。

第5条（ユーザ証明書の有効期間）

1. ユーザ証明書の有効期間は、本認証局と利用企業との間で協議を行った結果、両者で合意した期間とする。

第6条（認証局による利用者証明書の失効）

1. 本認証局は、以下に定める事由が発生した場合、ユーザ証明書を失効する権限を有す

る。

- ① 本認証局より送付したセキュリティデバイスもしくはユーザ証明書一式を、何らかの事由によりユーザーが受領できなかった場合
 - ② ユーザ証明書の記載事項が事実と異なることを発見した場合
 - ③ 本サービス利用契約が解除された場合
 - ④ 利用企業が解散した場合
 - ⑤ 利用企業へセキュリティデバイスを送付する前に、初期不良が判明した場合
 - ⑥ 本認証局の秘密鍵が危殆化した場合、またはその恐れがある場合
 - ⑦ 本認証局が認証業務を廃止する場合
 - ⑧ 証明書がインストールされた端末を盗難、紛失もしくは破損にて利用できなくなった場合
 - ⑨ 上記以外の事由により、本認証局がユーザ証明書を失効する必要があると判断した場合
2. 失効処理完了後、本認証局は「セキュリティデバイス失効報告書」を、利用企業担当者に送付する。なお、前項 5 号の場合については、「セキュリティデバイス失効報告書」の送付は実施しない。
 3. 本認証局は、ユーザ証明書の失効処理が完了した後、証明書失効リスト（CRL）に失効情報を登録し、リポジトリにおいて公開する。

第7条（利用企業によるユーザ証明書の失効申請）

1. 利用企業は、以下の事由が発生した、もしくは証明書利用者から申告を受けた場合、公印または代替印を捺印した「セキュリティデバイス失効依頼および代行入力依頼書」に必要事項を記載し、利用企業担当者を通じて、速やかに本認証局に対してユーザ証明書の失効申請を行わなければならない。
 - ① 証明書利用者の秘密鍵が危殆化した場合、またはその恐れがある場合
 - ② 証明書利用者がセキュリティデバイスを紛失した場合、または盗難された場合
 - ③ 破損等によって証明書利用者のセキュリティデバイスが使用できなくなった場合
 - ④ セキュリティデバイスおよびユーザ証明書の記載事項が事実と異なることを発見した場合
 - ⑤ セキュリティデバイスおよびユーザ証明書の記載事項に変更が生じた場合
 - ⑥ ユーザ証明書の利用を中止する場合
 - ⑦ 証明書利用者である社員の退職、役員の退任、あるいは外部委託者の契約が解除となった場合
 - ⑧ 証明書利用者が、「KS Solutions 証明書発行サービス 証明書利用者規約」（以下、「証明書利用者規約」という）に違反した場合

- ⑨ 証明書がインストールされた端末を盗難、紛失もしくは破損にて利用できなくなった場合
 - ⑩ 上記以外の事由により、利用企業がユーザ証明書を失効する必要があると判断した場合
2. 本認証局は、利用企業からの「セキュリティデバイス失効依頼および代行入力依頼書」を受領し、失効申請の内容を確認できた時点から原則として 24 時間以内に証明書失効リスト（CRL）に失効情報を登録し、リポジトリにおいて公開する。
3. 失効処理完了後、本認証局は「セキュリティデバイス失効報告書」を利用企業担当者に送付する。

第8条（ユーザ証明書の再発行）

1. 利用企業は、以下の場合に限り、ユーザ証明書の再発行を申請することができる。ユーザ証明書の再発行申請については、「セキュリティデバイス再発行依頼および代行入力依頼書」に必要事項を記載し、公印または代替印を捺印した上で、利用企業担当者を通じて利用企業に送付するものとする。
- ① 証明書利用者の秘密鍵が危殆化した場合、またはその恐れがある場合
 - ② 証明書利用者がセキュリティデバイスを紛失した場合、もしくは盗難された場合
 - ③ 破損等によって証明書利用者のセキュリティデバイスが使用できなくなった場合
 - ④ セキュリティデバイスおよびユーザ証明書の記載事項に変更が生じた場合
 - ⑤ 証明書がインストールされた端末を盗難、紛失もしくは破損にて利用できなくなった場合
 - ⑥ 上記以外の事由により、利用企業がユーザ証明書を再発行する必要があると判断した場合

第9条（ユーザ証明書の費用）

1. 利用企業は、ユーザ証明書に関する費用として、別途定める金額を所定の方法で本認証局に支払わなければならない。

第10条（認証局の業務終了または停止）

1. 本認証局がその業務を終了または停止する場合は、原則として利用企業に対して事前に通知を行う。ただし、本認証局の秘密鍵が危殆化する等、緊急を要する場合には、この限りではない。

第11条（利用企業による証明書利用者の管理）

1. 利用企業は証明書利用者に対して、以下の義務を遵守させなければならない。

- ① セキュリティデバイスもしくはユーザ証明書一式および、利用者 PIN を第三者に不正に利用されないよう、安全に管理しなければならない。
- ② 自身の秘密鍵が危殆化したか、あるいはその恐れがある場合に、利用企業担当者に対し、速やかに通知しなければならない。
- ③ 本規約および、CPS に定める適用範囲内に限定して本サービスを利用しなければならない。
- ④ 証明書利用者規約および CPS に定められた義務を遵守しなければならない。

第 1 2 条 (契約の解除)

1. 本認証局は、以下の事由が発生した場合、利用企業との本サービス利用契約を解除する権限を有する。
 - ① 各種費用が不払いの場合
 - ② 利用企業が廃業、解散した場合
 - ③ 利用企業が利用契約、本規約、CPS に違反した場合

第 1 3 条 (損害賠償責任と範囲)

1. 利用企業は、利用契約、本規約、CPS 等に違反した、または過失等により本認証局に損害を与えた場合、その損害に対する賠償責任を負う。
2. 利用企業は、当該利用企業の証明書利用者が利用契約、証明書利用者規約、CPS 等に違反した、もしくは過失等により本認証局に損害を与えた場合、連帯してその損害に対する賠償責任を負う。
3. 本認証局は、CPS 上で規定する責任事項を全うせず、利用企業に対して損害を与えた場合は、別途定められた金額の範囲内で賠償責任を負う。

第 1 4 条 (本認証局の免責)

1. 本認証局に責を帰すべき事由のない行為によって発生した損害について、本認証局は一切その責任を負わない。
2. 利用企業が、本サービスの利用に起因してコンピュータシステム等のハードウェア・ソフトウェアに何らかの影響、障害が発生しても、本認証局は一切その責任を負わない。
3. その他天災、災害等に起因した本サービスの停止により利用企業が損害を受けても、本認証局は一切その責任を負わない。

第 1 5 条 (通知および公表)

1. 本認証局から利用企業への各種情報に関する通知方法については、リポジトリでの公開を原則とする。
2. 本認証局が別途必要と判断した場合においては、書面の郵送、電子メール等により、

通知を行う。

第16条（民事手続上の情報開示）

1. 本認証局は、民事手続（調停（仲裁）、起訴、法的手続き、裁判上手続き、行政手続き等）上の要請に基づき情報の開示請求を受けた場合には、情報の開示を実施する。

第17条（個人情報の取扱）

1. 本認証局は、ユーザ証明書の発行申請および失効申請時において利用企業が提出する個人情報について、本サービスを提供するために利用する以外は使用しない。
2. 本認証局は、利用企業が提供する個人情報について、本認証局から不正に流出しないよう、適切に管理を行う。
3. 本認証局は、証明書利用者から利用企業を通じて本人による個人情報の請求を受けた場合、利用企業を通じて、該当する情報の開示を実施する。

第18条（権利譲渡等の禁止）

1. 利用企業は、本規約に基づく契約上の地位または、これに基づく権利、もしくは義務を他人に譲渡、または担保を設定する等の行為を行ってはならない。

第19条（本規約の変更権限）

1. 本認証局は、必要に応じて本規約を変更することができることとし、利用企業はあらかじめこれを承諾するものとする。
2. 本認証局は、本規約の変更を行った場合は、変更後の規約をリポジトリに公開する。

第20条（準拠法）

1. 本規約の執行、解釈および有効性は、当事者間の契約や他の準拠法を選択する旨の規定の有無に係らず、また、日本国に営業上の関連性を有するか否かを問わず、日本国内法および規則に準拠し、同法の適用を受けるものとする。

第21条（管轄裁判所）

1. 本規約に関して生じた紛争についての専属的合意管轄裁判所は、大阪地方裁判所とする。

第22条（協議）

1. 本規約に定められていない事項やこれらの文書の解釈に関して疑義が生じた場合、各当事者は、その課題を解決するために訴訟に先立ち誠意をもって協議するものとする。

(附則)

本規約は 2019 年 4 月 1 日より実施します。

(改訂履歴)

2005 年 2 月 1 日	新規作成
2016 年 4 月 1 日	修正
2019 年 4 月 1 日	修正