

コードサイニング証明書の管理について

下記の内容をお読みいただき、ご了承いただいたうえでコードサイニング証明書をお申込みください。

1. 証明書および鍵ペアの使用、取り扱い

- (1) コードサイニング証明書（以下「本サービス」という）の利用にあたり、お客様が鍵ペアの生成を行う際は、信頼性の高い装置を使用するものとします。鍵生成の目的に適合する方法で生成し、電子署名の目的に適合した鍵長およびアルゴリズムを使用するものとします。
- (2) お客様は、第三者に不正利用されないよう、取得した証明書および秘密鍵は第三者がアクセス出来ない場所に厳重に保管し、管理をするものとします。
- (3) お客様は、秘密鍵を転送する必要がある場合、大文字、小文字、数字、記号を含む16文字以上でランダムに生成されたパスワードを使用し、暗号化して秘密鍵を転送するものとします。
- (4) お客様は、申込をした内容で証明書が発行されていることを確認したうえで、証明書を利用するものとします。

2. 使用制限、禁止事項

- (1) お客様は本サービスの利用にあたり、以下の目的で証明書を利用することはできません。
 - ・証明書記載した以外の組織名に関連する秘密鍵または公開鍵の操作に利用すること
 - ・証明書を使用して疑わしいコードに署名し、悪意のあるコンテンツや有害なコンテンツを配信すること（コンテンツの受領者に不都合を生じさせるコンテンツ）
 - ・第三者組織のために（または代理人として）利用すること
- (2) お客様は本サービスの利用にあたり、証明書の秘密鍵を本サービス以外の証明書に利用することはできません。また有効期限終了または失効後に、証明書の秘密鍵を再利用することはできません。

3. 審査

セコムトラストシステムズ株式会社（以下「当社という」）は日本国内に活動拠点を有する、会社その他の法人およびその他当社が認めた組織、個人事業者を対象として本サービスを提供するものとします。ただし、当社が以下の各号に抵触する行為、またはその恐れのある行為を行っているとは判断したときはこの限りではありません。

- (1) 公序良俗に反する行為
- (2) 犯罪行為
- (3) 他人の著作権を侵害する行為
- (4) 他人の財産、プライバシー等を侵害する行為
- (5) 他人の名誉を毀損しあるいは誹謗中傷する行為
- (6) その他法令に違反する行為
- (7) 当社の運営を妨げ、もしくは当社の信頼を毀損する行為

4. 第三者との情報共有

疑わしいコードの作成元情報、証明書発行を拒否した履歴、秘密鍵の侵害やマルウェアの発見などの理由により証明書が失効された場合、当社は状況を把握認識し、申請者、署名済みアプリケーション、証明書、および周囲の状況に関する情報はCA/Browser Forumを含む他のCAまたは業界グループと共有することがあります。

5. 本書面の変更

当社は、お客様に事前に通知することなくCA/Browser Forumで定めるBaseline Requirements for the Issuance and Management of Code Signing Certificates およびBaseline Requirements for the Issuance and Management of Publicly- Trusted Certificatesの変更 に準拠するため合理的な範囲で、本書面の内容を変更できるものとします。