2022 年 10 月 4 日

パートナー各位

デジサート・ジャパン合同会社

適用日変更のお知らせ：
[重要]コードサイニング証明書における要件変更について(2023 年 6 月)

平素は弊社製品の販売支援をいただき、誠にありがとうございます。

さる 2022 年 6 月 10 日にご案内いたしました「[重要]コードサイニング証明書における要件変更(※１)について(2022 年 11 月）」に関しまして、このたび CA/ブラウザフォーラムは、適用日を 2022 年 11 月 15 日から 2023 年 6 月 1 日(UTC)に延期(※2)することを決議いたしました。これをうけて、弊社 CertCentral における企業認証コードサイニング証明書のご申請、および発行手順の仕様変更についても延期することといたしましたのでご案内申し上げます。お客様におきましては余裕をもってご準備いただけます。なお、今後の予定につきましては確定次第ご案内申し上げます。

弊社では引き続きサービスの向上に努めてまいりますので、今後ともご愛顧を賜りますようお願い申し上げます。

※1 Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
https://cabforum.org/wp-content/uploads/Baseline-Requirements-for-the-Issuance-and-Management-of-Code-Signing.v2.8.pdf

※２ Voting results Ballot CSCWG-17: Subscriber Private Key Extension
https://lists.cabforum.org/pipermail/cscwg-public/2022-September/000891.html

記

1.（更新）適用予定日
変更前： 2022 年 11 月頃
変更後： 2023 年 6 月

※ CertCentral における変更の適用日日程は、決まり次第別途ご案内いたします。

2. (更新)変更内容
2-1. CA/ブラウザフォーラムにおけるコードサイニング証明書基本要件について

変更前：当該要件では、2022 年 11 月 15 日（UTC)以降に発行されるコードサイニング
証明書の秘密鍵は、FIPS140 Level2、 Common Criteria EAL 4+、または同等の
セキュリティ要件を満たすハードウェアに格納されなければならないと定められております。

変更後：当該要件では、2023 年 6 月 1 日（UTC)以降に発行されるコードサイニング
証明書の秘密鍵は、FIPS140 Level2、 Common Criteria EAL 4+、または同等の
セキュリティ要件を満たすハードウェアに格納されなければならないと定められております。

当変更により EV コードサイニング証明書と同等に企業認証のコードサイニング証明書の
秘密鍵を安全に保護することができます。
なお、当要件は、2023 年 6 月 1 日以降に発行されるコードサイニング証明書に影響します。
2023 年 6 月 1 日以前に発行された証明書は影響を受けません。お客様のお客様は、証明書を
適用日以降に再発行しない限り、これらの証明書とその秘密鍵の要件を満たす
ハードウェアトークンやハードウェアセキュリティモジュール（以下、HSM）に
保存しなくても、業界要件に準拠し、継続してその有効期限までご利用いただけます。

2-2. (再掲)CertCentral におけるコードサイニング証明書の新規/更新申請について

CertCentral において、申請の際の入力項目、および証明書の取得手順が変更となります。

変更前：
申請時に CSR を提出し、弊社による認証完了後に CertCentral から証明書を取得し
クライアント端末/サーバにインストールする。 または、CSR は提出せずに申請し、
弊社による認証完了後に、弊社鍵生成ツールを利用してクライアント端末の
ブラウザ上で鍵ペアを生成、証明書を取得しクライアント端末/サーバにインストールする。

変更後：
申請の際に、証明書を格納するためのオプション（プロビジョニング方式）を選択する。

オプションには、 a）デジサートが提供するトークンを利用する、b）ご自身で
準備した要件を満たすトークンを利用する、 c）ハードウェアセキュリティモジュール
(HSM)
を利用する、があり、この中からひとつ選択して申請を完了する。
弊社による認証完了後に、選択したプロビジョニング方式に応じて、鍵ペアを作成し
証明書をハードウェアにインストールする。

2-3. (更新)CertCentral における再発行申請について
適用日前に発行済みの証明書を適用日以降に再発行する場合も当要件が適用されます。
手元に要件を満たすハードウェアがない場合は、その時点で DigiCert からトークンを
購入できるようにご案内いたします（予定)。再発行のお手続きの詳細は、確定次第
ご案内いたします。

デジサートでは、要件の適用日である 2023 年 6 月 1 日よりも前に、お客様にトークンを
ご購入できるよう準備いたします。 トークンの注文に関する詳細は、確定次第、
おって電子メールでお知らせします。

2-4. (再掲）署名の手順について
適用日以降に発行され、トークンや HSM に格納されたコードサイニング証明書を
使用するには、トークンまたは HSM にアクセスし、そこに保存されている証明書を
使用するための認証情報が必要となります。例えば、トークンを利用してコード署名を
行うには、トークンをコンピュータに接続し、その後、トークン上の
コードサイニング証明書を使用してコードに署名するためにパスワードが必要です。

3.(再掲）ご参考）DigiCert® Secure Software Manager のご紹介
当該要件に伴い、証明書は個別のトークン/HSM 単位で管理が必要となります。
リモートワークの浸透や、複数の作業者がコードの署名に携わる場合は、
これまで以上に鍵の保管、管理方法の見直しが求められます。

DigiCert® Secure Software Manager では、クラウド型の HSM と統合し鍵と証明書を
一元管理します。複数の開発担当者やユーザが、随時必要に応じて素早く簡単にツール、
アプリケーションやライブラリ等「コード」型のあらゆるソフトウェアに署名することが
できます。

主な機能
- HSM キーストレージ

- 秘密鍵・証明書、および署名作業を集中管理
- 社内/部門のセキュリティポリシーを適用
- CI/CD パイプラインとの統合

詳しくはこちらをご覧ください。
DigiCert Secure Software Manager
https://www.digicert.com/jp/signing/secure-software-manager

4. 本件に関するお問合せ

購入に関するお問合せ
電話：0120-707-637
お問合せフォーム： https://updates.digicert.com/salescodesign

テクニカルサポート
Email：authcode_info_jp@digicert.com
電話：03-4578-1368（自動音声ガイダンス 3）
受付時間：土日祝日および年末年始を除く平日 9:30 - 17:30

以上