■■■全てのパートナー様に該当する可能性のある■■■
■■■　　重要なお知らせです　　■■■

2018 年 3 月 16 日

パートナー各位

デジサート・ジャパン合同会社

ベストプラクティスのご紹介 – 秘密鍵の取り扱いについて

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。

DigiCert 認定パートナー様には、弊社製品・サービスの提供だけではなく、セキュリティのベストプラクティスに関する情報の提供を通じ、安心して SSL サーバ証明書の販売拡大に取り組んでいただく支援を継続させていただきたいと考えております。

昨今、SSL サーバ証明書に対応する秘密鍵の取り扱の強化が業界全体に求められております。秘密鍵の取り扱いについてのベストプラクティスをご紹介いたしますので、お客様の秘密鍵を預かることがございましたら、この機会にぜひプロセスの見直しをご検討いただけますようお願い申し上げます。なお、ホスティングパートナ様は秘密鍵にアクセスする必要がございますので、これまでどおり引き続き厳重に管理していただくようお願い申し上げます。

記

1. 秘密鍵を預からないで(または保護して)ください
申請者の秘密鍵は、申請者を一意的に認証するために使用されるものです。CSR を生成する際に秘密鍵も一緒に生成されますが、CSR とは別に保存されます。申請者の秘密鍵にサーバ運営担当者以外の誰かがアクセスできる場合、セキュリティ上の重大なリスクになります。
特定の状況(ホスティング環境など)では、ホスティングプロバイダが申請者の秘密鍵にアクセスする必要がありますが、それ以外の場合は、絶対に必要な場合を除き、パートナー様は秘密鍵にアクセスすることを避けるべきです。
CAB フォーラムで規定されているベースラインリクアイアメントのセクション 6.1.2 では、加入者以外の当事者が、加入者による明示的な承認なしに加入者秘密鍵を保管してはならないことを明記しています。この要件を満たす最善の方法は、申請者が秘密鍵をご自身で生成し、パートナー様がアクセスできないようにすることです。

2. 申請者情報を保護してください
パートナー様は、証明書を取得する過程の一環として顧客から提出された情報が安全に保護されていることを確認する必要があります。申請者情報が秘密であることを保証する最善の方法は、必要以上にそれを保持しないことです。
申請者情報を保管する必要がある場合は、暗号化された形式で保存する必要があり、情報へのアクセスはデータにアクセスする必要がある、権限が管理された人に限定する必要があります。

また、申請者情報は個人識別情報(PII)に該当する場合があります。
そのような場合は、個人情報の保護に関する法律を始め、適用されるすべての規則および法律に従って処理および保管する必要があります。

3. 支払い情報を保護してください
クレジットカード番号のような慎重な支払い情報は、該当する各国の法律およびコンプライアンス要件に沿って保護する必要があります。支払い情報は、支払い情報を扱うように設計されたサービスによってのみ処理され、支払い情報は安全でない場所に保管されるべきではありません。

4. CSR の生成手順
弊社では、加入者が CSR の作成を支援するための情報ページを公開しています。CSR の生成が必要なお客様へのご案内の際にぜひご活用ください。
https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=SO24325

5. 詳細情報
上記の対応方法についての詳細や、お客様に安全なユーザ体験を提供する方法についてその他の質問がある場合は、ssl-partner@digicert.com までお気軽にお問い合わせください。

以上

デジサート・ジャパン合同会社 パートナー営業部
パートナープログラム事務局
電話番号 : 03-6893-2743 FAX 番号 : 03-6368-9578
メールアドレス : ssl-partner@digicert.com
