DigiCertのSSL製品

お客様に適した証明書の選択

SSL/TLS証明書を購入する場合、様々な選択肢があります。選択が正しいか知るにはどうすればよいのでしょうか？ご安心ください。本文書で現在のニーズに合った証明書を選択できるようになります。

標準的なSSLサーバ証明書

単一ドメイン（例：www.example.com）の認証と暗号化を確保します。この証明書は、所有しているドメイン数が少ない企業にとって最適です。この証明書をでは、たとえばwww.example.comとexample.comを保護できます。

EV（Extended Validation）SSL証明書

最高レベルの認証により、顧客の信頼性とコンバージョンを向上させます。EVは、標準SSLが持つすべてのメリットに加えて、最も強力な身元保証を提供するため、顧客は安心して取引を行えるようになります。この証明書は、最高レベルの顧客の信頼を必要とする場合に最適です。

マルチドメイン（SAN）

マルチドメイン（SAN）証明書は、その名の通り、複数のドメインの保護を可能にするものです。この証明書が提供する柔軟性は、Microsoft ExchangeやOSC環境のように、異なるドメイン間で複数の名前を保護する必要がある場合に最適です。

EVマルチドメイン

マルチドメイン証明書の持つ柔軟性とEV証明書の提供するセキュリティを組み合わせたものです。企業は、単一つの証明書で最大250件のサブドメインにおけるブランドとアイデンティティの保護が行えるようになるため、自社サイトの信頼性と顧客の信頼性を高めることができます。

ワイルドカード

マルチドメイン（SAN）証明書とは異なり、DigiCertのワイルドカード証明書を使うと単一ドメインのみを保護できますが、第1レベルのサブドメイン数に制限はありません。この証明書は、多数のサブドメインにまたがってホスティングされている複数のサイトを管理する場合に最適です（たとえば、*.example.comは、www.example.comやmail.example.com などを保護します）。

クライアント（S/MIME）

Eメール通信の暗号化、ドキュメントやEメールへのデジタル署名、サーバーに対するユーザー認証を行います。クライアント証明書は、ユーザー名やパスワードを紛失した場合や盗まれた場合に、単純なユーザー認証を超えて強化されたセキュリティ対策としても利用できます。

コードサイニング

アプリケーションのソースと整合性を検証することにより、お使いのソフトウェアが安全ではないことをユーザーに伝える警告メッセージが表示されないようにし、信頼性を高めます。この証明書は、Microsoft Authenticode、Office VBA、Adobe AIR、AppleのMac OS、Mozillaオブジェクト、およびその他の主要なプラットフォームをサポートします。

EVコードサイニング

標準的なコードサイニング証明書の持つメリットを厳格なEVプロセスと組み合わせたものです。MicrosoftのSmartScreen® Application Reputationフィルタを使って警告メッセージを減らすことで、ブランドの評判とエンドユーザーの信頼を高めることができます。

ドキュメントサイニング

受信したドキュメントの送信元を明らかにし、変更されていないことを受信者に保証します。編集ソフトで署名機能をクリックするだけで、署名が完了します。この証明書は、Adobe PDF、Microsoft Office、OpenOffice、LibreOfficeの各ドキュメントをサポートしています。

digicert®

DigiCertの特長

使いやすい

- クラウドベースのプラットフォームを活用
- APIにアクセスすることでSSL管理の自動化やカスタマイズを実現
- 迅速な発行
- 業界トップクラスのOCSP応答時間

顧客重視

- 5つ星の評価を受けている業界唯一のCA
- グローバルなカスタマーサポート
- スケーラブルで柔軟なソリューション
- カスタマーアドバイザリーパートナーシップ

業界トップクラス

- EV SSL開発に貢献
- CA/Bフォーラムのメンバー
- CA Security Council（CASC）の創設メンバー
- OTA Allianceの理事

著名な企業からの信頼

詳細については、https://www.digicert.com/jp/のお問い合わせフォームよりお問い合わせください。