Advanced Certificate Manager

Transport Layer Security（TLS）でアプリケーションを保護しながら、証明書ライフサイクル管理のオーバーヘッドを削減します。

TLSでWebアプリケーションを保護しながらチームの業務負荷を軽減

Advanced Certificate Managerは証明書を自動管理し、複雑なTLS要件に柔軟に対応可能

TLSはインターネット上のプライバシーとデータセキュリティの根幹であり、エンドユーザーがクレジットカード情報その他の機密データを露出することなく、インターネットでプライベートブラウジングできるようにします。**Advanced Certificate Manager**は、TLSでWebアプリのセキュリティを確保しやすくします。具体的には：

- TLS証明書の発行、管理、更新はCloudflareが受任します。証明書は自動管理されるため、チームの生産性が向上します。
- 作成される新ドメインすべてに、組織や規制上のニーズに合わせてカスタマイズ可能な自動暗号化が適用され、セキュリティポスチャが強化されます。

お客様に最適のソリューションは？	
以下に該当する場合は、Universal SSL証明書が最適：	**以下に該当する場合は、アドバンスドまたはカスタムの証明書が最適：**
• 証明書ライフサイクル管理のオーバーヘッドを削減するために、無料のSSL/TLSソリューションが必要 • サブドメインは1階層のみ • 汎用的ソリューションが必要	• すべてのホスト名をTLSで完全にカバーしたい • SSL/TLS証明書に記載するホスト名に関して、特定の要件がある • 有効期間をデフォルトの90日より短くしたい • 使いたい認証局がある • カスタム暗号スイートを設定したい

証明書管理の合理化

お客様に代わってCloudflareが自動的にTLS証明書を発行し、更新するため、オーバーヘッドが削減できます。

TLS展開のカスタマイズ

証明書のホスト名のカスタマイズ、有効期間の調整、認証局（CA）と暗号スイートの選択、独自の証明書の持ち込みなどが可能です。

コンプライアンスの確保

最新の暗号技術で、業界、規制当局、組織のコンプライアンス要件の遵守を維持できます。

Advanced Certificate Managerの主な機能

お客様が作成するすべての新ドメインについて、Cloudflareが証明書を自動発行

組織が成長するにつれて、新製品ラインやWebサイトのローカライズ版など、新しいホスト名やWebプロパティが必要になる可能性があります。新しいホスト名ができるたびに証明書が自動発行されるため、新たに作成されたドメインにセキュリティやプライバシーのギャップができません。新しいWebサイトの立ち上げは大変な作業です。TLS対応はCloudflareにお任せください。

複数階層のサブドメインを暗号化

Webサイトにサブドメインが追加されるたびに、Cloudflareがお客様に代わって証明書を発行し、有効期間が切れる時に更新します。

希望の認証局（CA）を選択

組織によっては、特定CAの使用を希望する場合があります。Advanced Certificate Managerでは、証明書を発行するCAを選択できます。当社と連携するCAの最新リストをご覧ください。

お客様は、証明書署名要求（CSR）を生成してご希望のCAからカスタム証明書を取得できます。プライベートキーの管理はCloudflareが行います。CSRに関連するプライベートキーはCloudflareが生成し、Cloudflareネットワークの外部へ出すことは決してありません。

証明書の有効期間をカスタマイズ

証明書の標準有効期間は通常90日ですが、Advanced Certificate Managerでは短期間の設定が可能で、セキュリティを強化し、侵害時の影響範囲を縮小することができます。

希望のTLSバージョンからの要求のみを受け入れ

TLS 1.1や1.2といった古いバージョンのTLSは、TLS 1.3よりも接続が遅く、セキュリティが劣る場合があります。要求が受け入れられるTLSの最小バージョンを設定することができます。例えば、最小バージョンをTLS 1.2に設定すると、 WebサイトはTLS 1.2と1.3を使用するクライアントからの接続を受け入れます。

TLSで使用する暗号スイートを制御

Advanced Certificate Managerを使用すると、Cloudflareとクライアント（Web訪問者のブラウザなど）の接続を制限して、特定の暗号スイートからの接続のみを許可できます。

特定の業界推奨事項に従う、脆弱または時代遅れの暗号スイートを無効にする、規制や組織の要件に準拠するといった目的で制限を希望する場合もあるでしょう。

「Advanced Certificate Managerは、厳格なセキュリティ要件を満たすことを可能にしながら、多くのドメインにわたる証明書の管理方法を簡素化しました。暗号スイートを管理する機能、およびパラメーター内の自動更新により、利用可能で安全な環境が実現します。」

Colin Henderson氏
OneTrust エンジニアリング担当ディレクター

OneTrust

