TLS ベスト プラクティスガイド 2022 年版

証明書ライフサイクル管理の 5 つの柱で
作業負荷とリスクを軽減

digicert®

先手必勝の証明書管理が重要

証明書ライフサイクル管理を成功させることはきわめて重要です。デジタル ID とセキュリティ を必要とするウェブページ、デバイス、システム、サーバー、ユーザーの数は爆発的に増加しており、PKI ユースケースの数と種類は増え続けています。 証明書管理プログラムの効率と効果を高めるベストプラクティスは、組織が必要とする保護と暗号化の俊敏性を実現します。本 e ブックは、現在から将来に至るまで、デジタルセキュリティの最先端に立って、完全なコンプライアンスを実現し続けるための詳細かつシンプルなフレームワークを提供します。

目次

検知

暗号化資産の全容を把握する

既知の攻撃手段に対する脆弱性を特定する

暗号スイートと TLS バージョンをスキャンして脆弱性を見つける

管理とレポート

秘密鍵を保護する

修正を優先的に行う

発行・配布済みのワイルドカード証明書を管理する

適切な TLS 証明書タイプを実装する

ベンダー提供の証明書をすべて管理する

すべてのシステムパッチが最新であることを確認する

証明書管理システムへのアクセスを保護する

ITSM システムと統合する

アラートによって必要なアクションを確認する

通知

通知とエスカレーション階層を設定する

通知のしきい値を設定する

CT（証明書の透明性）ログを監視する

CAA アラートを設定して不正な証明書要求を防ぐ

自動化

証明書ライフサイクルを自動化する

証明書の自動化によって暗号の俊敏性を実現する

自動化

ビジネスプロセスを自動化する

API を活用してカスタム統合を実現する

統合

ネットワーク全体でルート証明書を普及させる

CA に依存しない検知およびインポートサービスを使用する

暗号化資産の全容を把握する

検知は PKI ベストプラクティスの基本

証明書の証明書資産一覧を完全に把握できていない組織は、気付かぬうちにセキュリティリスクに晒されている可能性があります。検知サービスを用いて不正な証明書、期限切れ間近の証明書、脆弱な鍵やハッシュ、時代遅れのサーバーソフトウェアなどの脆弱性を検出、修正することは、停止や中断の可能性を未然に防ぐ最も効果的な手段の 1 つです。

手始めに CA から発行された証明書のリストを作成するのも良いでしょう。でも、どのようにすれば、すべての証明書をリストアップできたと分かるのでしょうか。内部 CA や証明書付きのネットワーク機器はどう扱えばよいのでしょうか。最初のステップとしてお勧めなのは、証明書のネットワークスキャンです。 サーバーに証明書、鍵、ユーザー証明書および暗号アルゴリズムがないか検査したり、プライベートルート証明書をインポートしてそのルート証明書から発行された証明書を特定したり、他の検知ツールからデータをインポートしたりすることによっても証明書資産一覧に追加できます。

ポイント :

検知サービスは PKI 管理のベストプラクティスの基本です。検知サービスを使用すると、組織の暗号化資産の全体像を詳細に把握できるようになります。スキャン、検査などの検知手法を求められるリスク軽減策に応じた頻度で用いることで、脆弱性の継続的な検出と修正が可能になります。

一元化された証明書資産一覧を作成

- ネットワークスキャン
- サーバーとファイルの検査
- プライベートルート証明書の検知
- サードパーティ製ツールからインポート

既知の攻撃手段に対する脆弱性を特定する

システムを標的とした攻撃から保護します。

証明書資産一覧情報には、Windows や Linux などの OS の情報、Apache などのアプリケーションの情報も含まれている必要があります。1 つ 1 つのシステムをチェックし、すべてのシステムが最新バージョンにアップデートされており、攻撃手段に対して脆弱でないことを確認する必要があります。

Heartbleed、POODLE（SSLv3）、FREAK、LogJam、DROWN などの攻撃手段に対して脆弱になっている可能性があるため、この作業は重要です。また、ウェブサーバの OS と証明書に関連するセキュリティ要因も評価する必要があります。

ポイント：

サーバー、ロードバランサー、アプリケーションフレームワーク、クラウドインフラ、データベース、その他の IT インフラのバージョンを把握することで、攻撃手段と脆弱性に対して先手を打つことができます。

暗号スイートと TLS バージョンをスキャンして脆弱性を見つける

暗号スイートと TLS/SSL バージョンを確認します。

通常、これらの項目はウェブサーバで設定されます。TLS/SSL にまつわる攻撃の多くは、古いバージョンの SSL（たとえば POODLE 攻撃は SSL 3.0 を攻撃）や安全でない暗号スイート（たとえば ROBOT は RSA 暗号化を攻撃）を対象としています。TLS 1.2、1.3 を含む最新バージョンの TLS を使用することをお勧めします。

暗号スイートとは

TLS/SSL ネットワーク接続のセキュリティを高めるためにウェブサーバに設定される一連の暗号アルゴリズムです。

秘密鍵を保護する

鍵の使い回しはパスワードの使い回しと同じです。時間の節約は増大するリスクに見合いません。

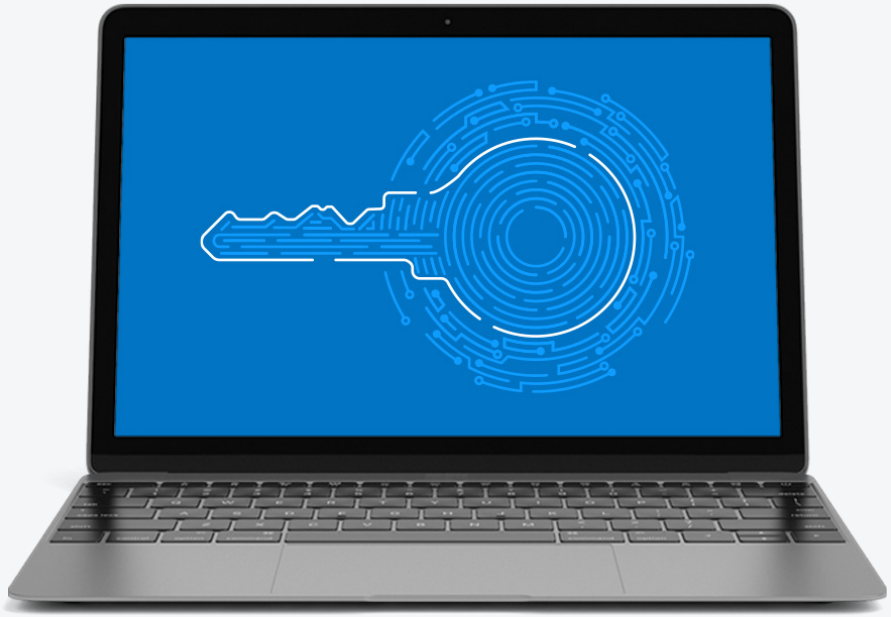
秘密鍵とは、サーバーとサーバーに接続するクライアントとの間でやり取りされるデータの暗号化/復号化に使用される個別のファイルです。これは、証明書署名リクエスト（CSR）において証明書の所有者によって作成されます。証明書を発行する認証局（CA）が秘密鍵を作成したり保持したりすることはありません。実際、組織の管理者以外の人がこのデータにアクセスできるようにしてはいけません。ベストプラクティスは、それぞれの証明書に新しい鍵ペアを作成することです。同様に、CSR の使い回しも厳禁です。CSR を再利用すると自動的に秘密鍵も再利用されるためです。

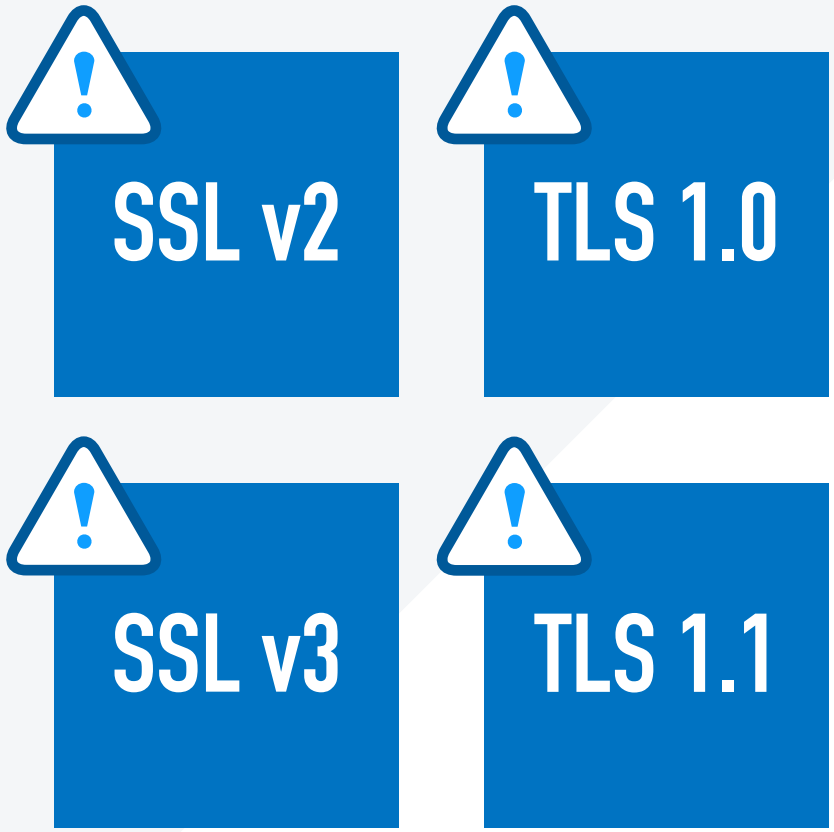
加えて、以下のことを行います。

- 脆弱な鍵がないかチェックする
- 既知の危殆化された鍵がないかチェックする
- 鍵を安全に保管する専用保管ツール、トークン、HSM を使用してセキュリティを高める

ポイント：

時間の節約のために CSR を使い回したくなるかもしれませんが、鍵を使い回せば、リスクは何倍にも膨らんでしまいます。証明書要求と更新を自動化することで、CSR の生成と証明書のプロビジョニングに必要な労力は大幅に削減できます。





修正を優先的に行う

証明書資産一覧内で見つかった脆弱な鍵、暗号、ハッシュ、古い資産を修正します。

証明書には、攻撃に対する脆弱性を持つ可能性のある公開鍵と署名が含まれています。公開ウェブサーバでは、鍵長が 2048 ビット未満の証明書、MD5 や SHA-1 などの古いハッシュアルゴリズムを使用している証明書を使用することはできなくなっています。ところが、内部のウェブサイトには見つかる可能性があります。もし見つかった場合、すぐにアップグレードすることが大切です。

脆弱な鍵やハッシュを持つ証明書を見つけること以上に大切なのは、お使いのウェブサーバでサポートされている TLS/SSL のバージョンと暗号スイートを確認することです。常に、TLS 1.2、TLS 1.3 を含む最新バージョンの TLS が有効化されている必要があります。暗号スイートについては、AES のような最新の暗号を使用するか、このリストを参照して廃止されたスイートを確認してください。

古い脆弱な TLS/SSL バージョン

- SSL v2
- SSL v3
- TLS 1.0
- TLS 1.1

発行・配布済みのワイルドカード証明書を管理する

ワイルドカード証明書を使用すると、証明書の発行は簡単になりますが、その他のセキュリティ上の懸念が生じます。

ワイルドカード証明書には管理者にとって分かりやすいメリットがありますが、同じ秘密鍵で複数のドメインを保護することはセキュリティリスクを伴います。たとえば、秘密鍵の紛失や盗難が起こった場合、その証明書を使用しているすべてのサーバーについて単一の侵害点が生じることになります。ネットワーク上で同じ秘密鍵を使い回したり、別の部署と共有したりすると、鍵の紛失や盗難につながり、関連するすべての証明書を交換しなければならなくなります。また、ワイルドカード証明書が何らかの理由で失効した場合、その証明書を使用しているすべてのサーバーで秘密鍵を更新しなければなりません。その更新は、ネットワークで転送中のデータの混乱を避けるために、すべて同時に行う必要があります。

更新後のワイルドカード証明書にもこれと同じプロセスが適用されます。元々は時間とコストを節約するためにワイルドカード証明書を使用したとしても、その更新の管理や、想定外の事情でワイルドカード証明書を交換する必要が生じた場合、かなりの手間がかかることになります。

ポイント：

ワイルドカード証明書を使用する場合、秘密鍵を保護することが重要です。ワイルドカード証明書の用途間で単一の秘密鍵を共有するリスクを最小限に抑えるには、ワイルドカード証明書の各コピーに別々の秘密鍵を使用し、秘密鍵を保護するためのセキュアなシステムを導入することが考えられます。さらに、ワイルドカード証明書がインストールされているすべてのサーバーで自動化を使用することをお勧めします。時間の節約になるだけでなく、人的ミスが減り、鍵の紛失も最小限に抑えられます。

適切な TLS 証明書タイプを実装する

業務に合った最適な保証レベルを選択します。

フォーム、ログインやパスワードなどでユーザー情報を収集する公開ウェブサイトを保護する場合、ブランドおよび企業の偽サイトを防止してブランドを保護するために OV または EV 証明書をお勧めします。

最高のブランド保証およびアイデンティティ保証が提供されるのは EV（拡張認証）TLS 証明書です。EV 証明書は、政府、グローバル企業、銀行、金融サービス業者などでよく使用されています。EV 証明書では、証明書申請者の連絡先と肩書きと雇用状況、連絡先のブロックリストチェック、ドメインの不正行為チェック、組織の登録番号、管轄、登録エージェントチェックなど、詳細な情報を 16 段階にわたって確認する最も厳しい検証プロセスが行われます。

次に保証レベルが高い証明書は、OV（企業認証）TLS 証明書です。OV は、組織の住所、証明書要求を認証するための電話連絡、不正行為チェックとブロックリストチェック、マルウェアチェックを含め、ドメインの所有者と組織のすべての連絡先を検証します。

最後に、最も認証水準が低いのが DV（ドメイン認証）TLS 認定書です。簡単になりすますことが可能なため、機密情報を扱うサイトにはお勧めできません。また、プライベート TLS 証明書は内部システムによく使用されていますが、セキュリティを維持するためにはプライベートルート証明書を適切なユーザーに配布する必要があります。

証明書のユースケース

EV（拡張認証）

- 銀行、金融サービス
- フォーチュン 500 企業
- グローバル 2000 企業
- 電子商取引サイト
- コンプライアンス（HIPPA、PCI など）

OV（企業認証）

- ログイン画面
- 企業サイト
- コンプライアンス（HIPPA、PCI など）

DV（ドメイン認証）

- ブログ
- 個人のウェブサイト
- 取引を行ったり個人情報を収集したりしないあらゆるウェブサイト

ベンダー提供の証明書をすべて管理する

ベンダー証明書は使いやすさ重視であり、必ずしもセキュリティを重視して設計されているわけではありません。

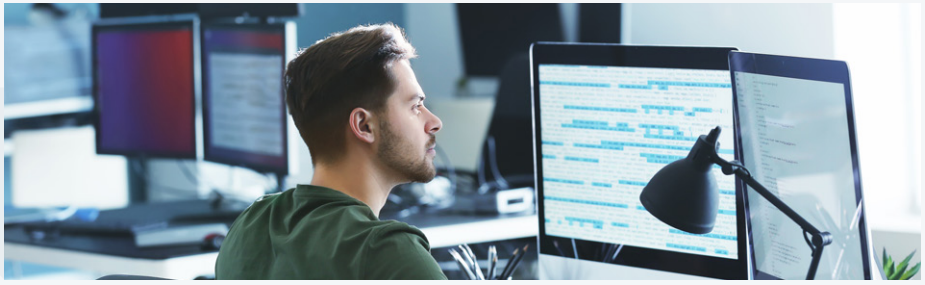
ベンダー証明書とは、デバイスにプリインストールされている、サードパーティのハードウェアベンダーが発行する証明書です。問題なのは、こういったサードパーティベンダーはこの種の証明書を実稼働ネットワーク上に配置することを前提としていないことです。デフォルトのベンダー証明書は自己署名だったり、有効期限が切れていたり、脆弱な鍵を使用していることがよくあり、ブラウザから信頼されません。多くの組織には、把握できていないベンダー証明書が何千も存在しています。これらの証明書はすべて削除し、信頼できる証明書（最低でもプライベート TLS/SSL 証明書）に交換する必要があります。この作業を効率化するには、API や ACME URL などの最新の自動化ツールを使用すると、交換やインストールが容易になります。

すべてのシステムパッチが最新であることを確認する

システムにパッチを適用することは、ウェブの最も壊滅的な攻撃の一部を回避するために重要です。

パッチとは、製品に含まれる脆弱性に対して保護するために OS、サーバー、アプリケーションフレームワーク、データベース、その他のソフトウェアおよびシステムに対して適用される更新プログラムです。たとえば、Windows/Linux OS、ウェブサーバ、ロードバランサーなどに適用できます。

これらの更新は、Heartbleed バグのような攻撃を防ぐのに役立ちます。このバグは OpenSSL の暗号ソフトウェアライブラリに見つかった脆弱性です。 脆弱なバージョンの OpenSSL ソフトウェアを使用した場合、そのソフトウェアで保護されたシステムのメモリを攻撃者が読み出せるバックドアができ、通信が盗聴されたり、サービスとユーザーからデータを盗み出すことが可能になっていました。



証明書管理システムへのアクセスを保護する

二要素認証やシングルサインオン（SSO）などの一般的なツールを活用します。

二要素認証（2FA）または多要素認証には、ログインを認証するのに複数のセキュリティ手法を使用することが求められます（一般的には何か「持っているもの」と「知っているもの」です）。より強固なセキュリティで証明書管理プラットフォームを保護し、多様な証明書資産一覧を管理する際の違反を防止します。

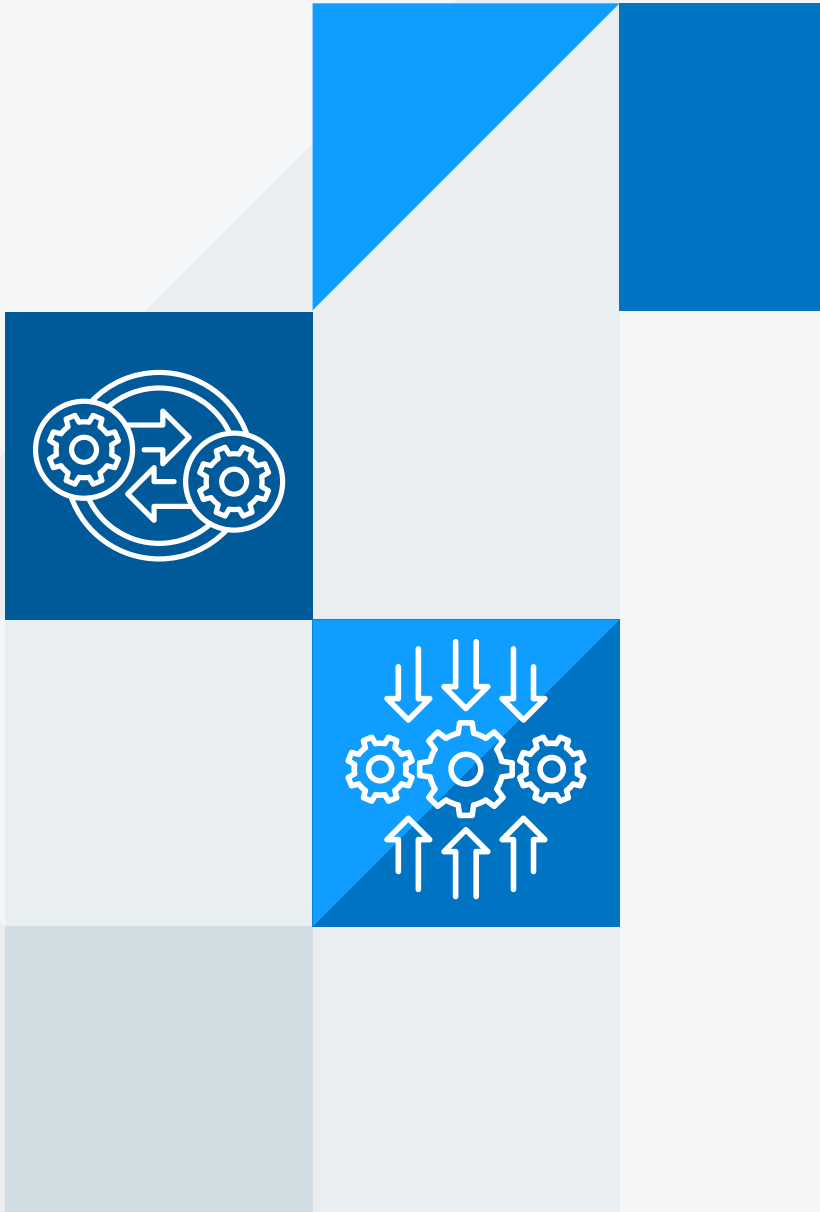
二段階認証の例としては、以下のものが挙げられます。

- モバイルデバイス 2FA 認証
- 認証アプリケーション 2FA
- トークンジェネレータ 2FA

ITSM システムと統合する

証明書管理プラットフォームは ServiceNow などの他のソフトウェアソリューションと統合して IT 運用とシームレスに連携できます。

より複雑な IT 環境では、証明書管理プラットフォームを ServiceNow などの ITSM（情報技術サービスマネジメント）と統合することで、組織のプロセスに適した証明書ライフサイクル管理承認フローを作成できます。これにより、従業員が証明書管理システムに直接アクセスせずに必要な TLS 認定書を申請できるようになります。ITSM システムを使ってエスカレーションプロセスを管理することで人的ミスが減り、稼働時間を長くすることができます。



アラートによって必要なアクションを確認する

対策や確認が必要な項目が一目で分かるダッシュボードを活用します。

一元化されたダッシュボードを活用して検知で特定された項目のステータスを追跡することは重要なファーストステップですが、表示データを次の行動につながるような分かりやすいものにブラッシュアップしていくことも重要です。

レポートシステムでは以下のことが必要です。

- 1 つのコンソールで証明書の全体像を把握する
- 詳細なレポートを作成、ダウンロード、スケジュール、統合する
- 不正な証明書、期限切れ間近の証明書、コンプライアンスの問題など、特定の問題やアクション項目を簡単に把握できる
- 伝わりやすく、明確な行動指針を示す直感的なデータビジュアライゼーションとグラフ

通知とエスカレーション階層を設定する

通知方法と通知先を定義し、自動化します。

通知とエスカレーション階層を設定することで、証明書の失効やセキュリティ侵害を防止します。これらの階層は証明書のグループについて以下のことを指定します。

- 通知がトリガーされるタイミング
- 通知の送信方法（E メール、アラート、Slack、ITSM）
- 配信先のロール（役割）
- エスカレーションのしきい値

必要な更新やインシデントに関する通知を受け取ることができるよう、発行 CA の E メール連絡先が最新になっていることも確認してください。

通知のしきい値を設定する

証明書の有効期限が切れる 90 日前、60 日前、または 30 日前に更新アラートを定義して自動化します。

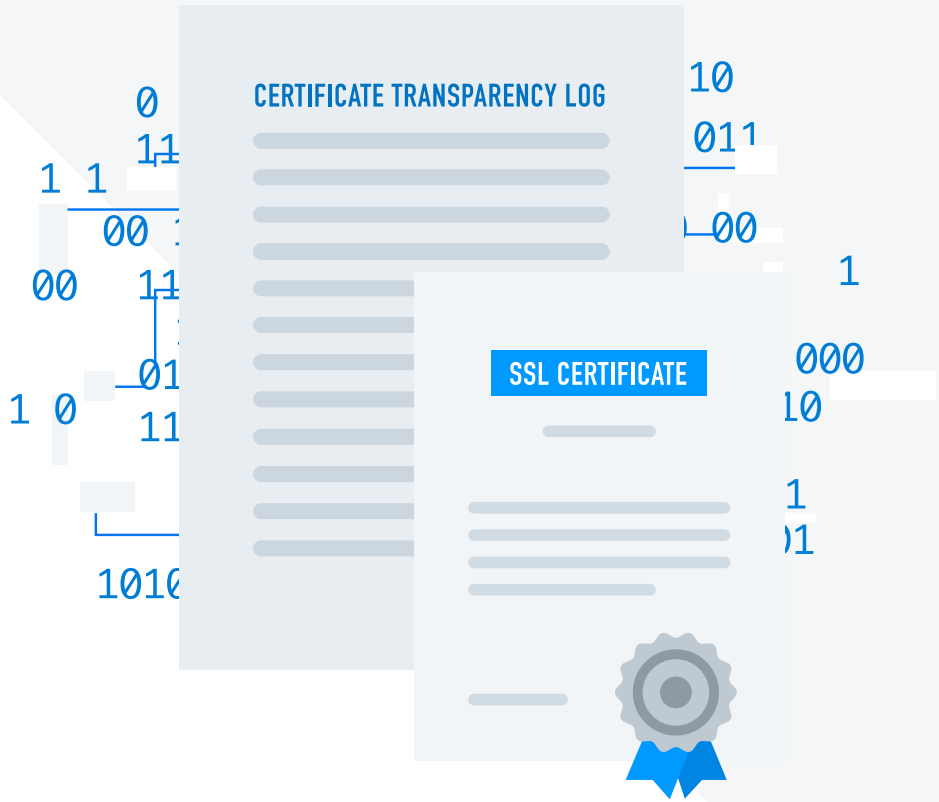
決められたしきい値（有効期限の 90 日前、60 日前、30 日前など）に通知を設定することにより、証明書有効期限を逃しません。テストや検証の時間を取るため、有効期限の少なくとも 15 日前に更新することをお勧めします。変更管理プロセスが長い場合、30 日間の方が基準として適切かもしれません。

同様に、期限切れの証明書についてもアラートのしきい値を定義する必要があります。

CT（証明書の透明性）ログを監視する

公開されている CT（証明書の透明性）ログに記載されていないパブリック証明書はブラウザから信頼されません。

CT ログ監視ツールを使用して、不正な証明書を迅速に検出し、誤って発行された証明書を見つけて修正します。CT ログにより、認証局は信頼できる TLS/SSL 証明書を発行する際の検証プロセスで説明責任を果たすことができます。そのドメイン名に対する証明書を発行したのが別の第三者の場合、それが悪意によるものでもポリシー違反によるものでも、CT ログ監視ツーがそのエラーを検出してただちに警告します。



CAA アラートを設定して不正な証明書要求を防ぐ

CAA（Certificate Authority Authorization: 認証局の承認）は自分のドメインに対して証明書の発行を許可する CA を指定するための DNS レコードです。

2017 年、CA/ブラウザフォーラムは、すべての CA に対して CAA DNS レコードをチェックして当該ドメインに対して見つかったエントリに従うことを義務づける Ballot 187 を発表しました。その目的は、ドメインの所有者が自らのドメインに対して証明書の発行を許可する CA を指定できるようにすることです。また、CAA では、何者かが承認されていない CA から証明書を申請した場合に通知を受け取る方法も提供されます。

証明書ライフサイクルを自動化する

証明書の更新、インストール、CSR 生成を効率化します。

証明書の自動化は、大量の証明書を効率的に管理する必要のある組織の運用にとって不可欠な仕組みです。証明書管理に付随するさまざまな手作業を自動化することで、人的ミスを最小限に抑えるとともに、証明書の有効期間の短縮による時間とリソースの負担を軽減できます。

証明書を自動化すると、以下のような効果があります。

- 証明書の発行、交換、更新に関係する作業負荷が削減される
- 人的ミスがなくなり、設定ミスが防止されることでダウンタイムや停止が回避される
- ユーザープロビジョニングを自動化することで、IT サポートデスクの負担が軽減される
- 危殆化した証明書を効率的に交換できるため、修正にかかる時間が短縮される

証明書の自動化によって暗号の俊敏性を実現する

耐量子コンピューター暗号の時代はすぐそこに

今のうちに自動化ツールを導入しておけば、業界や暗号の動向が今後どのように変化したとしても対応できる体制を整えることができます。証明書の発行と更新を自動化することで、証明書の管理と追跡、セキュリティイベント発生時に証明書を交換する時間を節約できます。自動化により、証明書の暗号化アルゴリズムを更新するのも容易になります。

ビジネスプロセスを自動化する

アクセスルール、ワークフロー、テンプレート、統合を定義します。

証明書管理の自動化の効果は、単に TLS 証明書のプロビジョニング、インストール、更新の手間が省けることだけではありません。ビジネスプロセスの自動化は、証明書および暗号証明書資産一覧全体の PKI 管理を効率化します。ビジネスプロセスの自動化がセキュリティ態勢を改善して運用を効率化する方法の例として、事前定義のアクセスルール、承認および通知ワークフローの自動化、登録申請の自動化、鍵の保護、企業システムとの統合などが挙げられます。

API を活用してカスタム統合を実現する

証明書管理プラットフォームと企業システムを直接統合します。

API 統合を活用して、既存のビジネスシステム、プロセス、または製品と合わせて証明書管理を効率化します。一般的な統合の例としては、ITSM システムと統合して証明書のステータス状況を変更履歴につなげる、ターゲット型検知ツールと統合して一元化された証明書資産の一覧表示を行うなどが挙げられます。

ネットワーク全体でルート証明書を普及させる

新しい CA（認証局）または小規模な CA の場合、そのルート証明書が一部のブラウザストアに含まれていないことがあります。これは古いブラウザで特に問題となります。

ベストプラクティスとしては、ルート証明書の普及率が高い CA が発行した証明書を使用することです。つまり、その証明書が新しいブラウザと古いブラウザのキーストアに存在し、99.9% のクライアントプラットフォームとブラウザに対応できるということです。

過去には、ブラウザの新バージョンが公開されたときに一部の認証局のルート証明書が含まれておらず、ウェブサイトの訪問者のブラウザにエラーメッセージが表示されたこともありました。このようなことが起きれば、ウェブサイトの所有者の売上（コンバージョン）や評判を大きく損なう可能性があります。

CA に依存しない検知およびインポートサービスを使用する

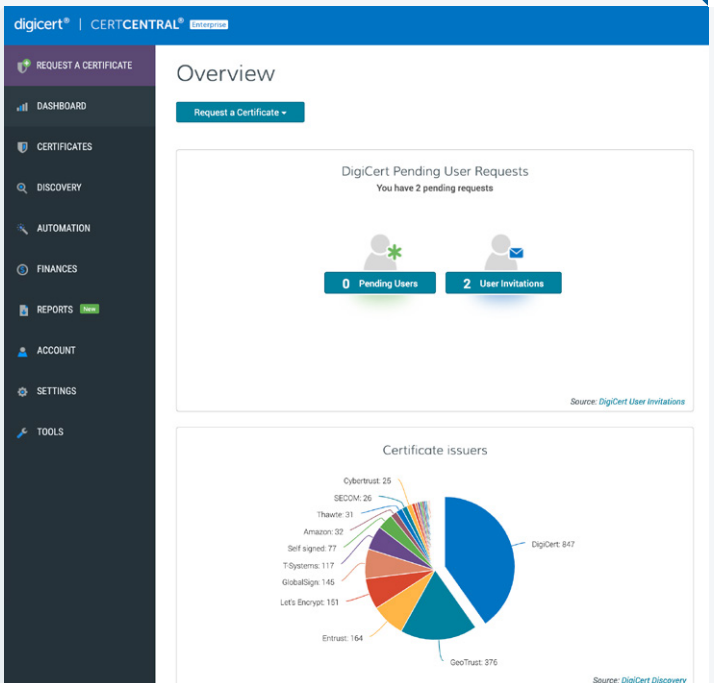
複数の CA が発行した複数の証明書をサポートする証明書管理プラットフォームを使用します。

CA に依存しないプラットフォームを使用すれば、証明書のタイプや発行 CA を問わず、どのような証明書でも 1 つのプラットフォームで追跡、管理できます。プライベートルート証明書をインポートしてそのルート証明書またはその他の暗号化資産から検知を行える検知ツールを探します。そうすることで、証明書の資産一覧全体を全て把握できる統合表示ができるようになります。

まとめ

面倒な証明書ライフサイクル管理業務の繰り返しから解放されましょう。

デジサートの証明書ライフサイクル管理ソリューションを使えば、TLS ベストプラクティスの 5 つの柱（証明書資産一覧の検知、管理とレポート、通知、統合、さらには自動化）を実践するために必要な機能がすべて揃います。直感的で、総合的で、証明書管理プログラムで先手を打つのに最高の方法です。



先手必勝の証明書管理を始めよう

証明書ライフサイクル管理を効率化し、本来の業務に専念できるようにしましょう。デジサートの製品を使うと、あらゆる証明書にベストプラクティスを実現できることをぜひご確認ください。お客様の証明書管理のお悩みについてご相談いただくには、server_info_jp@digicert.com までメールをお送りいただくか、www.digicert.com/jp/tls-ssl/certcentral-tls-ssl-manager からデモをご用命ください。