証明書管理ガイド:
基本ガイド

100枚以上の証明書を管理するSSL/TLS管理者のためのベストプラクティス

digicert®

目次

はじめに

証明書の管理を行う場合、管理する証明書を漏らしてはなりません。証明書の存在が忘れられたままになっていたり、証明書の期限が切れていたりすると、それによってコストや損害が生じてしまいます。大企業の場合、平均すると、証明書を1つ失効するごとに1,500万ドルの損失が生じると言われています[1]。さらには、顧客からの信頼が失墜したり、売上が低下したりするなど、セキュリティ面やブランドイメージにも影響が及びます。

公開鍵暗号基盤（PKI）の管理においては、証明書の管理、SSLのベストプラクティスに関する最新情報の把握、迅速な認証など、複数のポイントを考慮する必要があります。

このような役割において特に大きな課題になることの1つとして、スキャンをしても見つからない証明書がネットワークのどこかに存在しないか、常に気を配らねばならない点が挙げられます。こういった証明書があると、ある日突然サーバーがダウンして事態の収拾に追われることになります。

大がかりなチェックリストを複数使うような手法では、証明書を問題なく管理するのは容易ではないでしょう。そのような場合には、証明書のライフサイクルにおいて特に重要な部分だけに目を向けるしかありません。ネットワークのセキュリティを維持するうえで不可欠な項目です。

ネットワークがどの程度複雑であるのかはそれぞれに違いがあるので、どの組織でも使用できる単一のチェックリストというものは存在しません。一方で、証明書の管理を行う場合には、データ、企業、従業員を保護するために必ず注意を払わねばならない共通する事柄がいくつか存在します。

このガイドでは、証明書の管理を正しく行うために考慮すべき点をすべて説明しています。このガイドを活用すれば、APIの活用とグループの最適化を図りながら、証明書のライフサイクルに関するあらゆる注意点に精通することができるようになります。

以下のベストプラクティスによりPKI管理を知る

証明局（CA）や登録局（RA）、証明書のポリシー、証明書の管理システムをはじめとしたPKIの各要素を扱う作業には、大きなストレスが伴います。証明書のデプロイ自体は簡単ですが、セキュリティが確保されるよう、適切なデプロイと管理が必要です。

大企業の場合、SSLの管理者は、数百万とは言わないまでも数千は証明書を管理していることも少なくはありません。毎日あるいは毎週、証明書を適切にデプロイ、管理するとしたら、どのような手法があるでしょうか。

管理体制を維持していくのは容易ではありませんが、ベストプラクティスを用いればこの課題に対処できます。ベストプラクティスの利用により、管理体制の強化と作業時間の短縮が可能になり、証明書の利用に伴う不安が払拭されます。

ベストプラクティスに従えば、始終、証明書のことを気に掛ける必要がなくなり、セキュアなネットワークを安心して利用できるようになります。

ベストプラクティス：PKI管理プラットフォームを使用する

マネージドPKI（MPKI）ソリューションを導入すれば、社内認証局（CA）の管理にコストをかけることなく、証明書を発注および管理できます。公に信頼されているCAの多くがマネージドPKIソリューションを提供しており、コスト効率に優れているなどの理由から、大企業の大多数がこのソリューションを選択しています。

MPKIソリューションでは、PKIの大部分の管理をCAに任せられる一方で、証明書をセキュリティの確保に利用するメリットは変わらずに得られるほか、発行、実装、検知、修復、更新といった証明書のライフサイクル管理のあらゆる側面が簡素化されます。

概してMPKIでは作業時間の短縮が可能になり、その結果、証明書に関する以下のような重要性の高い詳細情報を容易に追跡できるようになります。

1 『2015 Cost of Failed Trust Report:When Trust Online Breaks, Businesses Lose Customers』（2017年6月26日、https://www.venafi.com/assets/pdf/wp/Ponemon-When-Trust-Online-Breaks-Businesses-Lose-Customers-white-paper.pdf）

- 証明書の有効期限
- SSLのエンドポイントエラー
- チームメンバーからの証明書のリクエスト
- 証明書の効力
- 証明書の発行元のCA

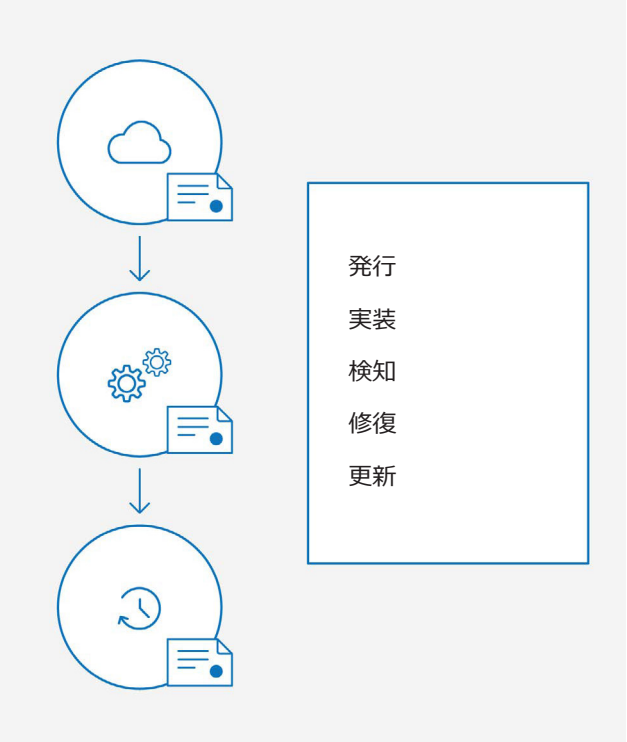
ほんの数年前までは多くの企業がスプレッドシートを使って手作業で証明書を管理していました。TechTargetが指摘しているように、また、自社の経験からもお分かりのように、このような管理方法では、証明書の紛失やミスマッチ、ラベルの誤りなどのミスを誘発することになります[2]。

しかし、MPKIプラットフォームを使用すれば、スプレッドシートで証明書の状態を管理する必要がなくなり、メールによる証明書のリクエストを処理する手間が省けます。これらの作業は自動化され、ヒューマンエラーの発生するリスクが抑えられます。認証の管理は容易になり、管理にかかる作業時間が短縮されます。

ベストプラクティス：APIを使用して自動化を始める

APIを活用すれば、さまざまテクノロジーを用いてアプリの開発ができ、企業間に存在する障壁を打破することが可能です。さらに具体的に言えば、APIは、証明書の管理機能を自動化およびカスタマイズする必要のあるITチームの負荷を軽減します。

MPKIプラットフォームによる証明書のライフサイクル管理の簡素化



小規模な企業の場合は、SSLの管理ツールにGUIが採用されていれば完全に満足するかもしれませんが、大企業が必要としているのはカスタマイズです。一部のPKI管理ツールではAPIを利用できるものがあり、APIを用いて機能やワークフローのカスタマイズが可能であるほか、APIを通じてプロセスを自動化し手間のかからない証明書の管理を実現できます。また、APIを利用すれば、SSLの管理を完全にカスタマイズすることも可能です。

2 『SSL certificate management:Avoiding costly mistakes』（2017年6月26日、Rob Shapland氏、http://searchsecurity.techtarget.com/tip/SSL-certificate-management-Common-mistakes-and-how-to-avoid-them）

業界によっては、数百万とは言わないまでも数千台はデバイスを管理していることでしょう。このような状況において、自動化を利用すれば、日々の作業が簡素化されます。また、ヒューマンエラーの数が抑えられ、証明書に起因したシステム障害の数を減らすことができるので、セキュアな環境を維持することが可能です。

APIの利用により、作業時間を短縮できるほか、SSL証明書のライフサイクルにおいて、以下のような多くのプロセスを自動化することが可能になります。

- 証明書のリクエスト
- リクエストの承認
- リクエストの却下
- 証明書のダウンロード
- 証明書の更新
- 証明書の取り消し
- 証明書の再発行

業界の標準が変化を続け、証明の有効期間が短くなっていることから、SSLの分野では将来、自動化は必須の機能となるでしょう。もはやこれを避けて通ることはできません。

APIを利用すると、発行元のCAが異なる証明書を管理する場合の作業が簡素化されます。また、リクエストの処理をプロセスから排除することで、証明書の更新作業をきめ細かく管理できます。90日、60日、あるいは30日以内に証明書の有効期限が切れる状態になった時点で更新が自動的に行われるようにすれば、証明書の期限が切れる前にチームのメンバーが所定のベンダーに証明書を発注しているかどうか気に掛ける必要がなくなります。処理は自動で完了しているのです。

APIは証明書の管理を自動化およびカスタマイズできるので、時間を節約する最適な方法と言えます。

ベストプラクティス：管理できていない証明書を見つける

証明書の管理者は皆、不正な証明書や未知の証明書の発見に頭を悩ませています。その背景には、証明書の利用環境の規模の変化や、複数の人間が個人で証明書を発注、実装している実態、大企業における一定水準の従業員の離職率があります。そして問題は、証明の存在を知っていなければ証明書を管理できない点にあります。

証明書の探索に検索ツールを使用すれば、すべての証明書の利用状況を包括的に把握できるほか、個々の証明書の状態をきめ細かく知る必要があるときに、詳細な調査を行うことも可能です。多くのCAが、証明書を探索したり、各スキャンから得られた情報をまとめたりするための検査ツールや検査エージェントを提供しています。このツールでは、ネットワーク上で使用されている証明書を発行元のCAに関係なくすべて見つけ出すことが可能で、デプロイされているすべての証明書の状態を把握できます。まさに理想どおりのツールです。探索ツールを使用すれば、手作業の追跡作業で発生するミスを回避できるほか、目録の管理に要する作業時間の短縮も可能になります。

定期的にスキャンを実行（少なくとも1週間に1回を推奨）すれば、現在使用されているすべて証明書の状態を完全に把握できます。また、脆弱性のリスクを詳細に調査することも可能になり、たとえば、ブランドを危険にさらすおそれのある不正な証明書を検出できます。忘れられていた証明書や放置されていた証明書を見つけて、それらの脆弱性を修正する措置が取れるのです。

ベストプラクティス：PKI管理に最適なチームを編成する

証明書の管理において基本となる要素の1つに、PKI関連の業務に携わる個人の管理があります。

主要メンバーに適切な人員を選び、部門やチームごとにこれらのメンバーを配置し、それぞれに相応しいレベルのアクセス権限を個々のメンバーに付与しなければなりません。また、各メンバーの職責を明確にすることや、導入した各プロセスの最新情報をメンバーに伝えることも必要です。

ユーザーを分類する

全国レベル、グローバルレベルで証明書のリクエストを管理する場合、個々のユーザーを部署や部門などの単位に分類（整理）すれば、管理がずっと容易になります。選択した単位に関わらずリクエストは、ロケーションやIPアドレス、内部のチームなどの分類に応じて整理できます。

このようなわずかな情報でも、内容が不完全なリクエストを受け付けたときなどに効力を発揮します。不足している内容を得るためにどのユーザーに確認すればよいかわかるからです。また、有効期限の切れた証明書が存在する場合に、その証明書を使用しているユーザーを追跡するうえでも役立ちます。

ユーザーロールを割り当てる

PKIを完全に管理できるようにするためには、チームの各メンバーにユーザーロールを割り当てる必要があります。管理プラットフォームへのアクセス権限が個々のメンバーに適切なレベルで割り当てられていれば、ストレスのない更新プロセスが実現し、追跡作業が効率化されます。

チームの個々のメンバー、メンバーが関係しているプロセス、メンバーの役割について評価を行いましょう。普通のユーザーであれ、リクエストを承認する管理者であれ、チームのメンバーには、証明書の管理プラットフォーム内における一定のロールを付与します。これにより、個々のメンバーには適切な権限が割り振られます。チームの別のメンバーでも処理できることはそのメンバーに対応をしてもらうように、リクエスの処理をユーザー自身に任せられれば、空いた時間を別の作業に回すことが可能になります。

ワンタイムユーザーがリクエストの処理を必要としているケースもあるでしょう。このような場合には、ゲストのアクセス権限をユーザーに付与してアクセスを管理します。この権限は、一時的に制限付きのアクセスだけをユーザーに許可するものです。この方法では必要最低限の情報しかユーザーに提供しないので、証明書の保護が強化されます。

チームにトレーニングを施す

各プロセスの最新情報をメンバーに伝え、新たなテクノロジーや実装機能についてメンバーにトレーニングを施します。これは継続して行う必要があります。

一方、システム管理者や開発者は、証明書を管理する方法やデプロイする方法についての技術的な情報を必要としています。必要に応じてシステム管理者や開発者と話し合う機会を持ち、彼らが必要とする情報をすべて提供するようにします。

さらに、システム管理者や開発者とは、要件やポリシーの変更について情報を共有する必要があります。CA/ブラウザフォーラムや特定のSSLプロバイダーのブログをフォローすれば、業界のトレンドや標準の変化について最新の情報を得ることができます。

ベストプラクティス：迅速な承認を行う

承認の処理をすばやく効率的に行うことが、大量の証明書を発行するうえでは欠かせませんが、このようなかたちでの承認の処理は、PKIの完全な管理を実現するという観点からも重要です。CAを用いて処理を行い、すばやく承認を行っているとしたら、証明書の発行プロセスにおいて一般的に時間のかかる処理は、証明書の管理者によるリクエストの承認だけです。

ユーザーと部署をすでに整理しているのであれば、承認を依頼するメールが適切な管理者に届くようにすることで、発行処理にかかる時間を短縮できます。そしてセグメントの処理を導入していれば、さらに認証のプロセスがスピードアップします。どの管理者も情報が正確であるかどうかのチェックと承認の処理だけをすればよいからです。承認を得るために管理者本人を追いかける必要がなくなって時間の節約ができ、デプロイ作業が長引くことも避けられます。

ベストプラクティス：通知機能を賢く使う

SSLの管理者のあいだでよく問題になっていることの1つとして、アラーム機能の欠如があります。この機能がないために、証明書の更新時期がきてもそれを見逃しセキュリティに影響が生じているケースが多く見られます。最低でも証明書の期限切れについてのアラーム通知が必要になるところですが、証明書のライフサイクルにおいて、通知機能が役立つ場面がほかにもあります。通知機能があれば、保留になっている証明書のリクエストや、最近取り消された証明書、再発行が必要な証明書がある場合にその存在を知ることができます。

スプレッドシートを使って証明書を管理する方法は規模の変化に対応できず、管理者に通知を行うプロセスがありません。証明書の更新の時期が近づいたらそれを知らせるようOutlookの予定表にリマインダーを設定している管理者もいますが、この方法にはいくつかの欠点があります。たとえば、イベントを作成してもリマインダーの設定を忘れていることがあります。また、その情報を引き継がずに退職してしまう管理者がいるなどといった問題もあります。スプレッドシートでは、100%信頼できる管理は実現しません。

更新の対象になっている証明書があり、そのオーナーが決められた期限内に更新を行っていない場合、そのオーナーが誰なのか、その証明書は実際に使用されているのか、その証明書はどのサーバーにインストールされているのかといったことをすぐに把握する必要があります。問題を早く認識できければそれだけ迅速なフォローアップが可能になります。

証明書に関する特定の問題の発生に備え、エスカレーションパスを設定しましょう。たとえば、証明書の有効期限があと7日で切れるような状況が発生した場合には、直接それがわかるようにします。適切なタイミングでエスカレーションができれば、手遅れになる前に問題を把握できます。このようなタイプのチェックを設定すれば、証明書の期限切れによって生じるシステムの停止を回避することが可能です。

ベストプラクティス：ネットワークの監視とレポートの生成を行う

ネットワークの状態を詳しく把握できないと、懸念材料が増えることになります。しかし、MPKIプラットフォームがあれば、ネットワークをスキャンして証明書の情報を収集し、これらの情報を単一のダッシュボードを通じて包括的に確認できます。ダッシュボードを利用して、徹底した検査を行いましょう。

ダッシュボードのビューを使用すれば、認証ネットワークの状態をすぐに詳しく把握でき、ネットワーク全体の健全性を一目で確認できます。また、有効期限が近づいている証明書や脆弱性のある証明書のエンドポイント、ほかのチームメンバーが発行してペンディングになっている証明書のリクエストなども確認できます。これらは、ダッシュボードを通じてネットワークを監視する場合に得られる情報例の一部に過ぎません。

このような方法でネットワークを監視し、継続的に探索を行い、調査結果のレポートを確認する作業は、可視性を高めるうえで最も重要な要素となります。そして、探索とレポーティングという2つの要素を組み合わせれば、証明書の利用環境について、詳細な情報の把握と効果的な管理が実現します。

これらのヒントをもとに、以下に示すような特殊な監視などを行います。

- エージェントを稼働させ、少なくとも30日に1回はネットワークをスキャンしてレポートを生成する
- スクリプトを使ってできるだけスキャンを自動化する
- 個々のスキャンが完了した都度、エンドポイントの脆弱性を修正する
- 証明書のリクエストをできるだけ早く承認する
- 証明書の更新処理を自動化して障害の発生を回避する

そして、証明書の利用状況の概要を十分に把握しながら、同時に個々の状況について詳細な確認を行うといった作業を、証明書のライフサイクルにおける検査ステップの一環として継続的に行う必要があります。

ベストプラクティス：脆弱性スキャニングツールを使用する

新たな脆弱性は時を選ばず表面化する可能性があり、その結果、脆弱性の修正作業は、証明書のライフサイクル管理において、迅速な対応が要求される作業となっています。

Bay Dynamicsの2017年のレポートによれば、非常に規模の大きな企業の場合、脆弱性のメンテナンスが手に余る作業になっていると、セキュリティチームの74%が感じていると言います。実際のところ、システム全体で常時、100万を超える脆弱性を管理することになるようなケースもあります。

「すべての脆弱性の管理とその影響の緩和を適切に行おうとするならば、その作業には大きなプレッシャーが伴います」[3]

3 『A Day in the Life of a Cyber Security Pro』（2017年6月26日、David Monahan氏、https://baydynamics.com/content/uploads/2017/05/4-19-17-FINAL-EMA-A-Day-in-the-Life-of-a-Security-Pro.pdf）

これらの脆弱性の一部は現時点でSSLのネットワーク内に潜んでいる可能性があります。旧式の暗号化方式や脆弱性のあるSSL/TLSのバージョンを使用していると、証明書を使ってもSSLサービスを十分に保護できません。SSLのエンドポイントについて脆弱性を管理する場合、ネットワークのスキャン、脆弱性の探索、脆弱性に関する情報の配布ができるツールを使用すればストレスが軽減します。

特定の脆弱性を検出してその情報をもとに影響を受けるエンドポイントを特定し、問題を生じさせずに素早く修復ができるという点において、このようなツールは大きな威力を発揮します。

ベストプラクティス：あらゆる作業が可能な単一のプラットフォームを選択する

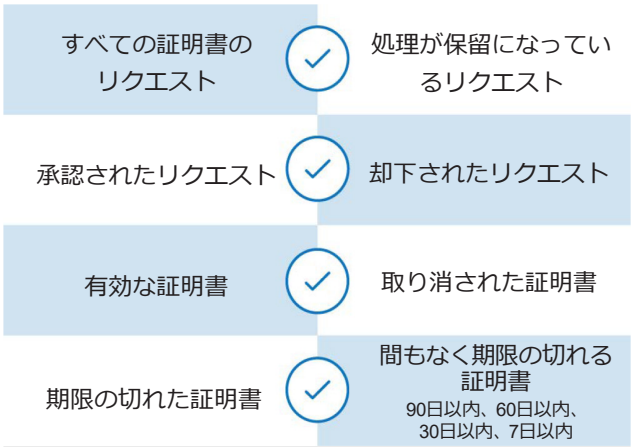
自社にとって作業が容易になる環境を整備しましょう。そのためには、以下のことが可能な証明書管理のプラットフォームを選択します。

- MPKIソリューションの利用
- 単一のダッシュボードによる包括的な情報の表示
- APIを通じた自動化
- 証明書の探索
- セグメント化およびユーザーロールの割り当て
- 通知機能とエスカレーションパスの設定
- 脆弱性のスキャン

PKIを完全に管理し、発行、実装、検知、修復、更新などの要素を含む証明書のライフサイクルを維持するうえで、このプラットフォームが基盤の役割を果たします。

DigiCertのCertCentral®プラットフォームはエンタープライズグレードの証明書管理ソフトウェアスイートです。このソフトウェアスイートは、管理の簡素化、ワークフローのカスタマイズ、発行処理の自動化を可能にすることを目的として設計されています。

ネットワークのあらゆる部分を監視することが求められる。証明書については、以下の事項に関するレポートを生成することが必要



SSLの管理者は、DigiCertのAPIを利用すれば、必要に応じてほぼすべてのプロセスを自動化できます。このAPIはサードパーティのアプリケーションと連携します。また、ブランディングを通じた、ほかのツールとの連携も可能です。

監視、管理、探索、脆弱性のスキャンができるオールインワンのプラットフォームを使用すれば、ネットワークの状態を把握できないことによって生じる不安が解消され、可視性も向上します。そして必要に応じて適切にチームを編成し、ロールを割り当て、分類を行えば、さらに管理性が向上します。

CertCentralは、あらゆる資産を漏れなく管理するうえで最も価値のある資産となるでしょう。

CertCentral®や弊社のAPIの詳細については、0120-707-637までお電話、またはmpki-ssl_jp@digicert.comからメールにて弊社営業部門までお問い合わせください。