digicert®

世界中の開発者の認証と署名済みリリースの管理

組織

ウェブサイト : www.apache.org
業種 : テクノロジー
本部 : 米国デラウェア州ドーバー
開発者数 : 6,000 人

主な課題

Apache ソフトウェア財団は、6 大陸で 6,000 人の開発者と 350 の製品を擁し、コードサイニングの効率化を迫られる一方、SSL/TLS サーバ証明書の管理も必要としていました。

ソリューション

- DigiCert® Secure Software Manager
- DigiCert CertCentral® Enterprise

利点

- ダウンロードしないで利用するクラウドベースの署名鍵によって、6 大陸 6,000 人の開発者のセキュリティが向上
- 証明書ベースのアクセス制御が行われるため、ユーザー名/パスワードの管理が不要
- 切り離されたロールベースのアクセスによって、認証のリスクが最小化
- オンデマンドの SSL/TLS サーバ証明書の発行処理が数日から数分に短縮

Apache ソフトウェア財団は、ウェブのサービスやサポートに欠かせない 350 のオープンソースソフトウェア製品の開発と配布を行っています。同財団は、SSL/TLS サーバ証明書の管理方法を改善するとともに、暗号技術による製品の安全性確保、署名、作成者の検証を簡素化する必要に迫られ、デジサートのクラウドベースコードサイニングと SSL/TLS ソリューションを採用しました。DigiCert® Secure Software Manager と DigiCert CertCentral® Enterprise を導入したことで、6 大陸 6,000 人の開発者は効率的かつ安全にコードサイニングを利用できるようになりました。また、リスクが最小限に抑えられ、オンデマンドの SSL/TLS サーバ証明書の発行処理が数日から数分に短縮される結果につながりました。

大きな影響力

インターネットは私たちの暮らしぶりや働き方に変化をもたらしていますが、その効果を享受にする上で大きな役割を果たしているのが Apache ソフトウェア財団です。同財団は 1999 年に設立されたオープンソースの開発者コミュニティです。その代表的な製品である Apache Web サーバーは、全ウェブサイトの 50% 以上で利用されていると推定され、その中には Apple、PayPal、Wikipedia、Alibaba などの人気サイトも含まれています[1]。

この他にも、ビッグデータの処理に利用される Apache Hadoop、アプリケーションサーバーの Apache Tomcat、生産性ツール Apache OpenOffice など、数百もの製品の開

[1] W3Techs、“Usage statistics and market share of Apache for websites”、2015 年 4 月

発と管理を行っています。同財団のインフラストラクチャ担当バイスプレジデント、デイヴィッド・ナリー氏は次のように述べています。「私たちはソフトウェアを無料で提供し、人々はこれを使って、あるいはこれを土台としてビジネスを構築しています。財団の設立当初、企業の中にはオープンソースコードというものをちょっと疑いの目で見る人も少なくありませんでした。しかし、15 年が経った今、オープンソースコードは多くの人々に受け入れられるようになりました。OpenOffice はダウンロード数が 1 億件に達しています」

オープン性と安全性の両立

Apache ソフトウェア財団の主な課題は、組織が培ってきた信頼を維持することです。ナリー氏は次のように述べています。「中にはオープン性を悪用する人もいます。OpenOffice などのコードをダウンロードし、マルウェアやアドウェアをバンドルする例が後を絶ちません」

作成者を検証し、コードに改ざんや変更が加えられていないことを保証するため、同財団では長年、ある種の暗号による署名を利用してきました。「問題は、私たちが利用してきた署名方法が難解で、コードが意図された通りのものであることを検証するにはユーザーが複雑な PGP 暗号化ツールを使用しなければならなかったことです。大半のユーザーはそうした暗号化ツールに慣れていませんから、わざわざ使おうとはしません」

ナリー氏率いるチームは、このプロセスを改善するため、さまざまな方法を調査しました。独自のコードサイニングソフトウェアを作ることも検討しました。「ソリューションを求めて徹底的に市場を探し回りました。ずいぶん時間がかかりました。納得のいくまで調べることを重視したからです」

クラウドベースの鍵保護

さまざまなソリューションを検討した末、Apache ソフトウェア財団は DigiCert Secure Software Manager を選びました。決め手の一つは、コードへの署名に用いるデジタル鍵の保護レベルの高さでした。鍵を失くしたり盗まれたりすれば、サイバー犯罪者によって、マルウェアを含むコードへの署名に悪用されるおそれがあります。

「当財団には 6 大陸 6,000 人以上の開発者がいます。彼らが (コードサイニングのために) 必要とする鍵をすべて安全に管理するのは、並大抵のことではありません。SSM では、鍵はクラウドに置かれていて、それを使って署名をすることはできるけれど、鍵そのものを実際に取り出すことはできない仕組みになっています。これは私たちにとって大きな利点です」

Apache ソフトウェア財団
インフラストラクチャ担当バイスプレジデント、デイヴィッド・ナリー氏

ナリー氏は次のように述べています。「DigiCert Secure Software Manager の特筆すべき点の一つは、鍵そのものにアクセスできないようになっていることです。当財団には、6 大陸 6,000 人以上のコミッターがいます。コミッターとは、財団の用語で、コードを書く権限を持つ開発者のことです。彼らが必要とする鍵をすべて安全に管理するのは、並大抵のことではありません。DigiCert Secure Software Manager の場合、鍵はクラウドに置かれていて、それを使って署名をすることはできるけれど、鍵そのものを実際に取り出すことはできない仕組みになっています。これは私たちにとって大きな利点です」

重要な管理機能

Apache ソフトウェア財団では、コードへの署名ができる権限を持つ開発者の本人確認を行い、彼らが必要な鍵にアクセスするためのユーザー資格情報を取得できるようにしています。ナリー氏は次のように述べています。「それ以来、ユーザー名とパスワードは要らなくなりました。パスワードを失くしただの、弱すぎるだの、忘れただのと心配する必要がなくなりました。証明書ベースのセキュリティだからです」

このソリューションでは、鍵と切り離されたロールベースのアクセスを提供しています。「財団の管理者はコードに署名することができません。また、あるプロジェクトで使った鍵を別のプロジェクトに使うこともできません。そのため、誤用や悪用を防ぐことができます」

DigiCert Secure Software Manager では、交代で使用できるいくつかの鍵のセットがプロジェクトごとに提供されます。そのため、一つの鍵が失効してもビジネスへの影響は最小限で済みます。「実際、鍵を失効させなければならなくなったことがあったのですが、交代で使える鍵がいくつもあったので、そのプロジェクトで署名した他のリリースには影響がありませんでした」

コンプライアンスや利用状況の可視化

DigiCert Secure Software Manager には、レポートや監査ログの生成機能があるため、ナリー氏をはじめとする管理者陣は署名アクティビティを簡単に追跡・監視することができます。ナリー氏は次のように述べています。「監査ログは非常に役立っています。月に 1 回ログの検査を行っています。最近も、誰かが変なファイルに署名を行っているのが見つかりました。単にファイル名が慣例通りにつけられていなかっただけなのですが、調査を行って、セキュリティの問題ではないことを明らかにすることができました」

最大の利点は、財団のエンドユーザーの利便性です。「多くのプラットフォームでは、ユーザーは署名済みのコードを利用することになっていて、署名されていないコードをインストールしようとすると警告が表示されます。けれども今ではソフトウェアが実際に Apache ソフトウェア財団から配布されたものであることが保証されるようになったため、インストール時のユーザー体験が向上しました」

「場当たり的に管理していた頃は、SSL/TLS サーバ証明書を取得するまでに 2 週間もかかっていました。それが、DigiCert CertCentral Enterprise を導入してから、数分で取得できるようになりました。必要に応じて、証明書の管理、要求、更新、失効をワンストップで行うことができます」

Apache ソフトウェア財団
インフラストラクチャ担当バイスプレジデント、デイヴィッド・ナリー氏

証明書発行時間の短縮

ソフトウェアと同様、サーバーも、信頼できる機関からの認証が必要です。SSL/TLS サーバ証明書がこの機能を担っています。認証局 (CA) がドメインの所有者の検証を行い、そのサーバーにインストールする SSL/TLS サーバ証明書を発行します。

Apache ソフトウェア財団では、SSL/TLS サーバ証明書をいろいろな認証局から場当たり的に取得していました。そのため、証明書の発行や更新に先立ち、CA が財団に連絡をとり本人確認を行うという認証プロセスが毎回必要でした。それには数日、あるいはそれ以上かかるときもありました。

また、財団では証明書が期限切れとならないよう、人手をかけてそれぞれの更新日を監視しなければなりませんでした。

財団のウェブサイトの数が増えるにつれ、ナリー氏のチームは証明書の管理を簡素化したいと考えるようになりました。そこで、エンタープライズクラスのクラウドベース証明書管理コンソール、DigiCert CertCentral Enterpriseが選ばれたのです。CertCentral Enterprise を利用すれば、認証プロセスはたったの 1 回で済ませることができます。組織の詳細情報とドメイン名、連絡先情報を送信し、確認の電話に応答するだけです。すると検証されたデータが認証を受けて保存され、その時点以降、指定された顧客担当者がデジサートの SSL/TLS サーバ証明書をデジサート認証オーダーの全期間にわたって即時発行することができます。

ナリー氏は次のように述べています。「場当たり的に管理していた頃は、SSL/TLS サーバ証明書を取得するまでに 2 週間もかかっていました。それが、DigiCert CertCentral Enterprise を導入してから、数分で取得できるようになりました。必要に応じて、証明書の管理、要求、更新、失効をワンストップで行うことができます」デジサートとの連携の最大の利点は、単に技術面の問題を解決できることではないとナリー氏は言います。「技術的な側面から問題を解決できる人はたくさんいます。最大の利点は、デジサートにはプロセス面の問題、つまり大きな組織内でコードへの署名や SSL/TLS サーバ証明書の発行ができるようにするにはどうしたらいいかという問題を解決するためのノウハウがあり、ガイドラインを順守しながら物事を進めるためのサポートができることです。それが組織全体に価値をもたらしています」

デジサートについて

デジサートは創立当初より、インターネットの安全を守るためのより良い方法を探すことを企業理念として掲げています。だからこそデジサートの証明書は、あらゆる場所で、1 日に何百万回も、世界中の企業によって利用されているのです。また、デジサートのサービスとサポートはお客様から常に 5 つ星の高い評価をいただいています。デジサートは、より革新的で安全な未来を目指し、今後も業界をリードし続けます。SSL、IoT、PKI — デジサートはどの分野でも比類のない存在です。

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