導入事例

Apache ソフトウェア財団

シマンテックのソリューションにより、4,000 人の開発者のコード署名を簡素化

ウェブに不可欠な 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う Apache ソフトウェア財団は、製品に暗号で署名し、作成元と安全性を確認するための簡単な方法と、SSL サーバ証明書管理の簡素化を必要としていたため、シマンテックのクラウドベースのコード署名および SSL サーバ証明書管理ソリューションを採用。全世界 4,000 名の開発者が安全にコード署名にアクセスできるようになり、リスクが最小化。また、オンデマンド SSL サーバ証明書により、処理が数日から数分に短縮された。

組織概要

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： 4,000 名

主な課題

Apache ソフトウェア財団は、350 の製品と全世界の 4,000 名の開発者のコード署名を合理化する必要があった。また、サーバの SSL サーバ証明書も管理する必要があった。

ソリューション

Apache ソフトウェア財団は Symantec™セキュア APP サービスを採用した。その理由は、この製品が、安全なクラウドベースサービスであるコード署名キーと、クラウドベース SSL サーバ証明書管理のための Symantec™マネージド PKI for SSL を提供できるからである。

メリット

- 全世界 4,000 名の開発者がクラウドベースのアクセスを使えるようになり、署名キーをダウンロードしないため安全性が向上
- 認証に基づいたアクセスにより、ユーザ名/パスワードの管理が不要
- 他から分離されたロールベースのアクセスによりリスクを最小化
- オンデマンド SSL サーバ証明書により、数日かかっていた発行処理を数分に短縮

大きな効果

インターネットは私たちの暮らし方と働き方を変えつつある。Apache ソフトウェア財団 (以下、ASF) はこの変化を実現する上で、主要な役割を果たしている。ASF は、1999 年に設立されたオープンソース開発者のコミュニティである。最もよく知られた製品である Apache Web サーバーは、Apple、PayPal、Wikipedia、Alibaba 等の人気サイトを含め全体の 50 パーセントを超える Web サイトに採用されている。[1]

インターネットの全世界の GDP (国内総生産) は、総計 8 兆米ドルと推定されている。[2] Apache Web サーバーは、ドイツやフランスの GDP を上回る、約 4 兆米ドルの価値創出に貢献していることになる。[3]

ASF は他にも、ビッグデータ向けの Apache Hadoop、Apache Tomcat アプリケーションサーバー、生産性を向上させる Apache OpenOffice をはじめ数百の製品を開発、管理している。Apache ソフトウェア財団インフラストラクチャ部門バイスプレジデントの David Nalley 氏は、以下のように述べている。「私たちはこのソフトウェアを無償で配布し、ユーザはそのソフトウェア上で、またはそのソフトウェアを使ってビジネスを構築する。財団が設立された当時、オープンソースコードは多くの企業から、やや疑いの目で見られていた。しかし 15 年たった今、オープンソースコードはますます多くの人に受け入れられるようになり、OpenOffice は 1 億ダウンロードを突破した」

「ASF には全世界で 4,000 名を超える開発者が存在する。彼らがコード署名に必要とするすべての鍵を保護しようとすることは非現実的である。Symantec セキュア APP サービスでは、クラウド上に保管された鍵を使って署名することでアクセスが可能になる。自分で実際の鍵を入手することはない。これは私たちにとって大きな成功となった」

David Nalley 氏
Apache ソフトウェア財団インフラストラクチャ部門
バイスプレジデント

オープンでありながら安全な方法

ASF の主要な課題は、組織が培った信用を維持することである。Nalley 氏は以下のように述べている。「かつては、オープンソースという私たちの特徴が悪用されたこともあった。OpenOffice などのコードをダウンロードし、コードにマルウェアまたはアドウェアをバンドルされたのである」

ASF は長年にわたり、コード作成者であることを確認し、コードが署名された時点から変更または改ざんされていないことを保証するために、コードに暗号で署名している。「問題は、コードに署名する方法が難解であり、コードが目的通りであることをユーザが検証するには非常に高度な PGP 暗号化ツールを使う必要があることだった」と Nalley 氏は述べている。「ほとんどのユーザは暗号化ツールに精通していないため、ツールが利用されなかったのだ」

Nalley 氏とチームは、プロセスの改善方法を調査し、独自のコード署名ソフトウェアの開発に向け評価を実施した。「私たちは市販のソリューションも評価した」と Nalley 氏は述べている。「長時間を必要としたが、それを明確にすることは重要だった」

クラウドベースのキーの保護

ASF は Symantec™ セキュア APP サービスを採用した。理由の 1 つは、セキュア APP サービスがコード署名に使う暗号鍵に提供する保護のレベルの高さである。鍵を紛失したり盗まれたりしたことがある場合、サイバー犯罪者がその鍵を悪用してマルウェアを含むコードに署名する恐れがある。

「Symantec セキュア APP サービスの特徴的な機能の 1 つは、各開発者自身は決して鍵にアクセスしないことだ」と Nalley 氏は述べている。「ASF には全世界 4,000 名以上のコミッタが存在する。コミッタは ASF の用語で、コードを作成する権限を与えられた開発者を指す。コミッタが必要とするすべての鍵を保護することは非現実的であるが、Symantec セキュア APP サービスでは、クラウド上に保管された鍵を使って署名することでアクセスが可能になる。自分で実際の鍵を入手することはない。これは私たちにとって大きな成功となった」

重要な制御

ASF は、コードに署名する権限を与えられた各開発者を識別し、必要な鍵にアクセスするユーザ資格を与える。「その後は、ユーザ名やパスワードは使わない」と Nalley 氏は述べている。「パスワードを紛失した、パスワードが脆弱である、パスワードを忘れたといった心配は不要である。安全性は認証に基づいている」

このソリューションは権限に依存したアクセスを提供し、鍵管理を隔離できる。「ASF の管理者はいかなるコードにも署名することはできない」と Nalley 氏は述べている。「また、プロジェクトの鍵は他のプロジェクトの署名には使えない。これによって、誤用と悪用を防ぐことができる」

Symantec セキュア APP サービスは、ASF の各プロジェクトに Pool of Rotating Keys（ローテーション鍵）の保管を提供する。これにより、鍵が無効になった場合のビジネスへの影響が最小限に抑えられる。「以前、まさに鍵を無効にする必要が生じたことがあった。しかし、複数のローテーション鍵が存在するため、そのプロジェクトによって署名された他のリリースには影響しなかった」と Nalley 氏は述べている。

コンプライアンスと費用を可視化

Symantec セキュア APP サービスではレポートと監査ログが生成されるため、Nalley 氏とその他の管理者は動作を簡単に追跡し、監視することができる。「監査ログは非常に役に立つ。私たちは毎月点検している」と Nalley 氏は述べている。「最近、誰かが不審なファイルに署名しているケースが見つかったが、結局そのファイルは私たちの標準的なルールに従って命名されていないだけであるということが分かった。調査の結果、セキュリティの問題ではないことが確認できた」

監査ログにより、Nalley 氏はソリューションの利用回数も把握できる。「Symantec セキュア APP サービスは、署名されたソフトウェアごとに課金する方式ではなく、署名イベントごと、つまり同時に署名したすべてのものに課金する方式を採用している」と Nalley 氏は述べている。「ASF では多数のソフトウェアを 1 回でリリースすることがあるため、この課金方式によってサービスの提供コストを劇的に削減できる」

最も大きな利益を得るのは ASF のソフトウェアを利用するエンドユーザである。「大部分のプラットフォームは、ユーザが入手したコードは署名済みであることを前提としているため、未署名コードをインストールしようとすると警告する。ASF が作成したソフトウェアであることが保証されているので、ユーザは安心して、簡単にインストールできるようになった」

ソリューション

- Symantec™ セキュアAPPサービス
- Symantec™ マネージドPKI for SSL

Symantec

「SSL サーバ証明書をその都度管理する方法を採用していた当時は、SSL サーバ証明書の入手が 2 週間遅延することもあった。マネージド PKI for SSL を導入した今では、数分で SSL サーバ証明書を入手できる。まさに、証明書の管理、要求、更新、取り消しをオンデマンドで行うワンストップショップである」

David Nalley 氏
Apache ソフトウェア財団インフラストラクチャ部門
バイスプレジデント

サーバ認証処理を数日から数分に短縮

ソフトウェアでは信頼されている作成者の認証が必要となるが、サーバも認証を必要とする。SSL (Secure Socket Layer) サーバ証明書はこの機能を実行する。認証局 (CA) はドメインの所有者を確認し、SSL サーバ証明書を発行してサーバ上にインストールする。すると、ブラウザの URL バー内にあるドメイン名の左に小さな緑の南京錠マークが表示される。この南京錠マークは、ユーザの接続が暗号化されておりドメイン名の所有者が認証済みであることを示している。

ASF は従来、SSL サーバ証明書をさまざまな認証局 (CA) から随時入手していた。問題のある証明書の発行や更新の前には、毎回 CA が ASF に連絡し、ASF の確認を行うというプロセスが必要であった。このプロセスには数日またはそれ以上かかることもあり、ASF では、それぞれの更新日付を監視し証明書が失効していないことを確認する必要があった。

ASF の Web サイト数の増加に従い、Nalley 氏とチームは SSL の管理を簡素化したいと考えるようになり、Symantec™マネージド PKI for SSL の導入を選択した。マネージド PKI for SSL は、証明書を全社的に管理するためのクラウドベースのコンソールである。組織は、組織の詳細、ドメイン名、連絡先情報を提出し、確認の電話を受け取ることで、認証プロセスを一度で済ませることができる。確認済みデータは認証および保存され、その時点から、シマンテック認証サービスの注文が有効な間は、顧客からの連絡があれば即座にシマンテックの SSL サーバ証明書を発行できる。

「SSL サーバ証明書をその都度管理する方法を採用していた当時は、SSL サーバ証明書の入手が 2 週間遅延することもあった」と Nalley 氏は述べている。「マネージド PKI for SSL を導入した今では、数分で SSL サーバ証明書を入手できる。まさに、証明書の管理、要求、更新、取り消しをオンデマンドで行うワンストップショップである」

シマンテックを採用したことで得られた最大の利点は、単に技術的なソリューションだけではないと Nalley 氏は述べている。「技術的な視点からは、多くの人々が問題を解決できるだろう。重要なことは、プロセスに関する問題の解決方法、つまり大規模な組織内でコードに署名したり、SSL サーバ証明書を発行したりするための方法を Symantec が理解していることである。これによりユーザは、ガイドラインに従いながら問題を解決することができる。このことが組織全体に価値をもたらしているのだ」

詳しくは、以下をご参照ください。
https://www.symantec.com/ja/jp/code-signing/secure-app-service/または
https://www.symantec.com/ja/jp/ssl-certificates/managed-pki-ssl/

合同会社シマンテック・ウェブサイトセキュリティ
〒107-0052　東京都港区赤坂 1-11-44 赤坂インターシティ
Tel : 03-5114-4137
E-mail : mpki-ssl_jp@symantec.com
https://www.jp.websecurity.symantec.com/

[1] W3Techs、「Usage statistics and market share of Apache for websites」、2015 年 4 月参照
[2] Derek Thompson、「The $8 Trillion Internet:McKinsey's Bold Attempt to Measure the E-conomy」、『The Atlantic』、2011 年 11 月
[3] Wikipedia.com、「List of countries by GDP (nominal)」、2015 年 4 月参照