digicert

# DigiCertコードサイニング：ユーザーの信頼を得る

## 課題：「このコードは信頼できるか？」

作成したソフトウェアをインターネット経由でユーザーに配布する場合、ソフトウェアが改ざんや改変されることなくユーザーに届けられることをいかにして保証できるでしょうか？また、そのようなソフトウェアがダウンロードしても安全であることをいかにして保証できるでしょうか？残念ながら、悪意ある攻撃者は、ソフトウェアのコピーを簡単に傍受した後、バンドルされたマルウェアと共にソフトウェアを再配布している可能性があります。

最も一般的なマルウェアとして、「トロイの木馬」が挙げられます。この悪意あるソフトウェアは、その名が示す通り、ギリシャ人が巨大な木馬を使ってトロイに兵士を忍び込ませたのと同じように、一見正常なファイルであると見せかけたオブジェクトの中にマルウェアを仕込んでいます。

よくあるマルウェアとしては、次のものが挙げられます。

- スパイウェア：個人情報を収集するもの
- アドウェア：望ましくない広告マテリアルをダウンロードするもの
- ウイルス：プログラムファイルに感染するもの
- ワーム：ネットワーク全体で自己複製を行うもの
- トロイの木馬：正当なソフトウェアを装うもの

## ソリューション：コードサイニング証明書

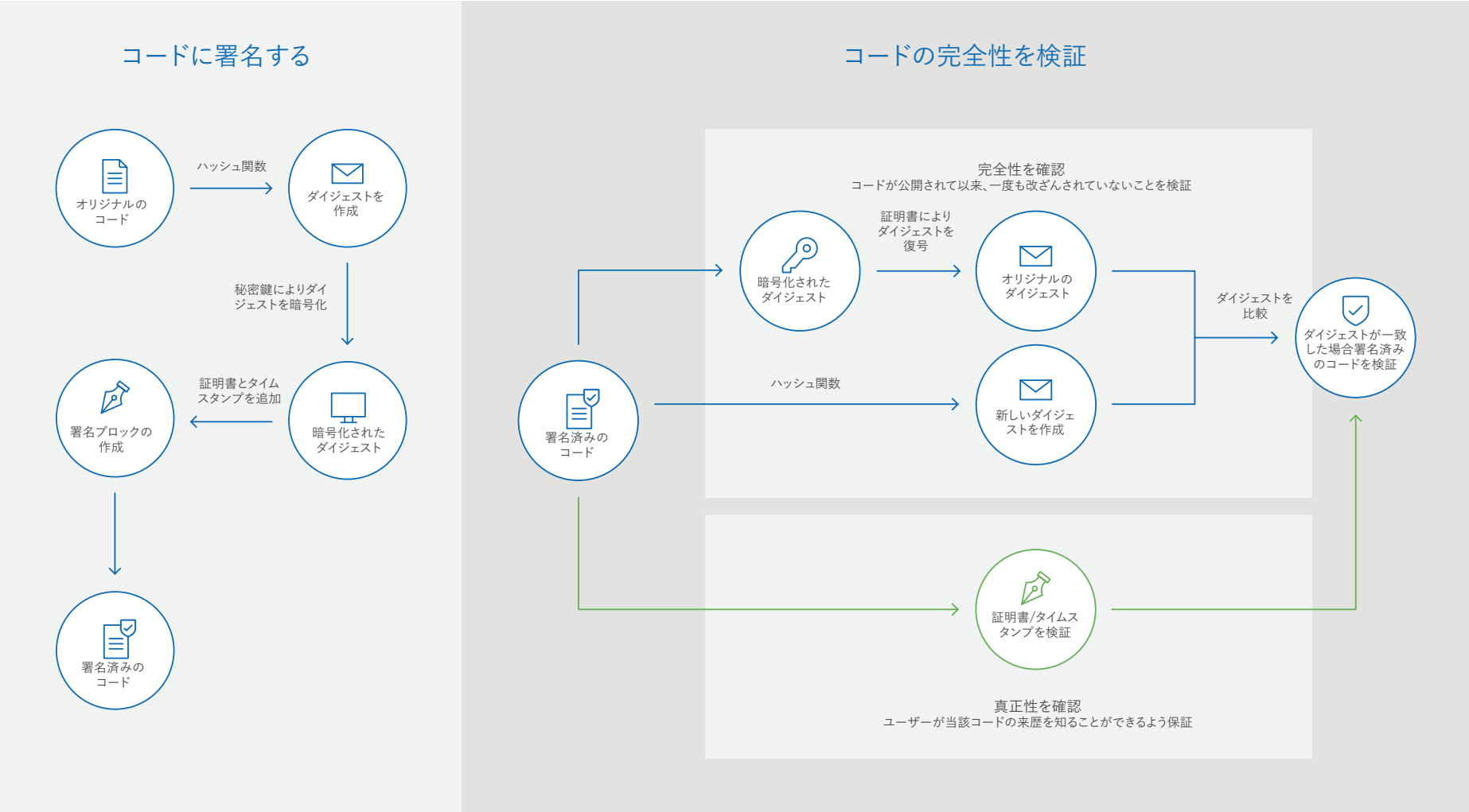
マルウェアを回避するために、ソフトウェア開発者は、コードサイニング証明書を使用して、アプリ、ドライバ、ソフトウェアプログラムに対するデジタル署名を行います。こうすることで、エンドユーザーは、当該コードが第三者によって改ざんされていないことを確認できるようになります。

コードサイニング証明書は、SSL/TLS 証明書がWebサイトのIDを認証する場合に使用するテクノロジーと同じものを使用します（注：コードサイニング証明書は、ファイルやデータの暗号化は行いません）。コードサイニング証明書は、秘密鍵と公開鍵のペアを使用してソフトウェアにデジタル署名を行うことで、当該コードが正当であり信頼できるものであることをエンドユーザーに対して証明します。

コードサイニング証明書には次のものが含まれます。

- 署名
- 会社名
- タイムスタンプ（必要な場合）

# コードサイニングの仕組み



## 機能と価格

| | コードサイニング | EVコードサイニング |
|---|---|---|
| 1年分の価格 | 90,000円 | 134,000円 |
| 2年分の価格 | 162,000円 | 234,000円 |
| 3年分の価格 | 252,000円 | 335,000円 |
| 暗号化されたデジタル署名 | ✓ | ✓ |
| 組織に関する厳格な拡張認証(EV)が必要 | | ✓ |
| Microsoft Smartscreen フィルタにより即時の安全評価 | | ✓ |
| ハードウェアトークンを使用した2要素認証が必要 | ✓ ※ | ✓ ※ |

※　USB ハードウェアトークン：20,000円
2023年6月1日 より業界標準としてすべてのコードサイニング証明書の秘密鍵を、FIPS 140 レベル2、Common Criteria EAL 4+、または同等の認定を受けたハードウェアに格納する必要があります。この変更にともない証明書以外にUSBハードウェアトークンが必要な方は証明書の申請時にUSBハードウェアトークン付の製品を選択ください。過去にデジサートより入手した上記の規格を満たしたトークンをお持ちの方は、再利用が可能です。

DigiCertのコードサイニング証明書は、標準のコードサイニングまたは拡張認証(EV)として提供されます。DigiCert EVコードサイニング証明書には、標準のコードサイニングが持つメリットに加えて、厳格な審査プロセスが追加されています。これにより、暗号化されたトークンとMicrosoftのSmartScreen® Application Reputationフィルタを使用した2要素認証が可能となるため、エンドユーザー向けの警告メッセージを減らすことができます。

## DigiCertコードサイニングのメリット

### ユーザーを保護

コードサイニングを行うことで、ユーザーはそのコードが本物であり、改ざんされていないことを確認できるようになります。また、コードサイニングを行うことで、ソフトウェアを窃盗やマルウェアから守ることも可能となります。

### パートナーの要件に応える

パートナーおよびソフトウェアを配布するチャネルは、企業が、顧客のデータを保護することを期待しています。ソフトウェアに署名することで、顧客データの安全性に対するコミットメントをアピールできます。

### ユーザーの信頼を高める

コードサイニングを行うことで、ユーザーのブラウザに警告メッセージが表示されないようになるため、ソフトウェア発行者としての信頼を築くことができます。その結果、より多くのユーザーを獲得できるようになります。

digicert

# DigiCertを選ぶ理由

## 市場をリードするプラットフォームとツール

セキュアなネットワークを維持するには、SSLサーバ証明書を購入してインストールするだけでなく、適切な設定、脆弱性アセスメント、継続的な監視、そしてタイムリーな更新が必要となります。DigiCertが提供するプラットフォームとツールは、証明書関連のタスクを自動化することで、管理を容易にします。

## 信頼のカスタマーサポート

顧客がサポートを必要とするときにはいつでも、DigiCertが長年にわたって提供してきた高い評価を受けているテクニカルサポートチームを利用できます。経験豊富な日本人による日本語でのサポートにより様々な種類の証明書の発行から利用、更新に至るまで支援します。

## 世界のトップブランドを保護

世界トップクラスのハイアシュアランスデジタル証明書のプロバイダーとして、当社は、IoT（Internet of Things）を実現する企業を含む、世界で最もイノベーティブな企業と提携する幸運に恵まれています。そのような提携を通じて、当社は、毎日289億件以上のWeb接続を保護しています。

facebook Nintendo IBM CISCO NASA hp invent Microsoft SONY Medtronic

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

© 2023 DigiCert, Inc. All rights reserved. DigiCertは、米国およびその他の国における登録商標です。
その他のすべての商標および登録商標は、それぞれの所有者に帰属します。