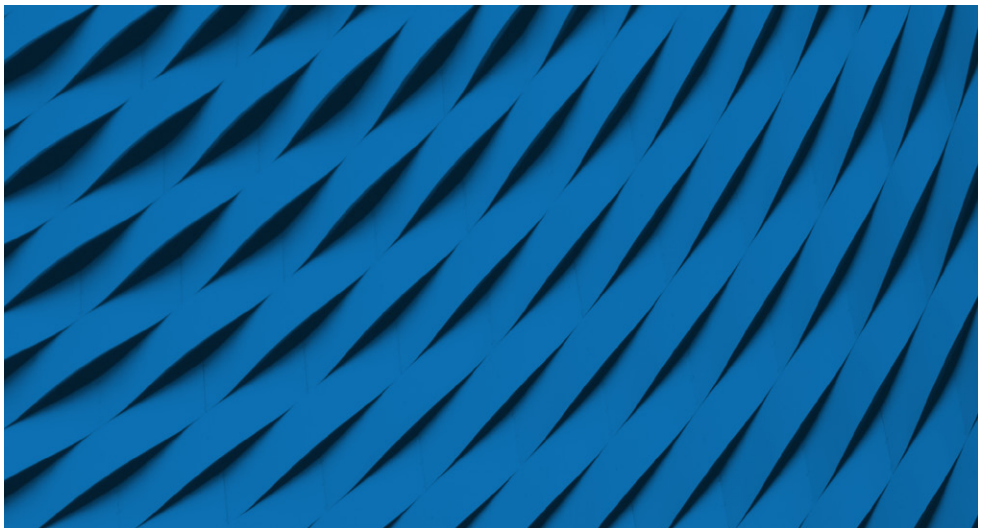
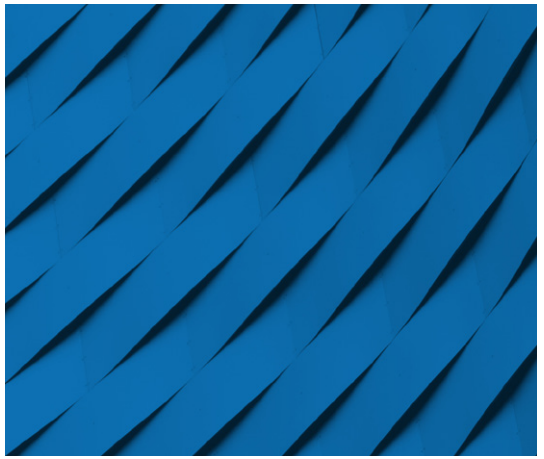
購入者ガイド

署名ソフトウェアの評価とコード署名ポリシーの採用

CI/CD パイプラインを遅延させることなく
ソフトウェアリリースプロセスのセキュリティを
強化するために検討すべきベストプラクティス





digicert®

はじめに

ソフトウェアサプライチェーン攻撃やその他のマルウェアへの感染は、顧客の信頼を損ない、信頼を取り戻すのに長い時間とコストがかかります。そのような攻撃が広く知られた結果、データの侵害、ランサムウェアによる要求、システム全体のシャットダウンが発生する場合もあります。

一方、ソフトウェアセキュリティの脆弱点も激増しています。アジャイル開発によりビルドサイクルの頻度が上がりました。クラウドへの実装とオーケストレーションがソフトウェアデリバリーに取って代わりました。さらに、コネクテッドデバイスの普及により、セキュアなファームウェア更新とコミュニケーションの必要性が高まっています。

企業がソフトウェア開発ライフサイクルのセキュリティ体制を向上する必要性は、今まで以上に高まっています。コード署名ソフトウェアは、コード署名アクティビティの管理を一元化し、ソフトウェアの脆弱性を減らすコード署名ポリシーおよび手法の標準化と施行を実現します。

コード署名ソフトウェアソリューションを評価し実装する際には、以下の基準が意思決定の参考になります。

1. 構成の柔軟性
2. 包括的な鍵保管と取り扱い手法
3. ワークフローの統合と自動化
4. 一元化された柔軟なレポーティング
5. リリースプロセスの制御
6. 柔軟でスケーラブルな導入

この購入者ガイドは、ソフトウェアリリースのセキュリティの向上を望むお客様向けに以下の情報をまとめたものです。

- コード署名ソフトウェアプラットフォームの評価基準
- コード署名ポリシーおよび手法を採用する方法について、うまくいったお客様の知恵

構成の柔軟性

アカウント構造とユーザーのロールおよび権限を細かく構成できることで、組織独自の要件にシステム機能を適合させることができます。

目的

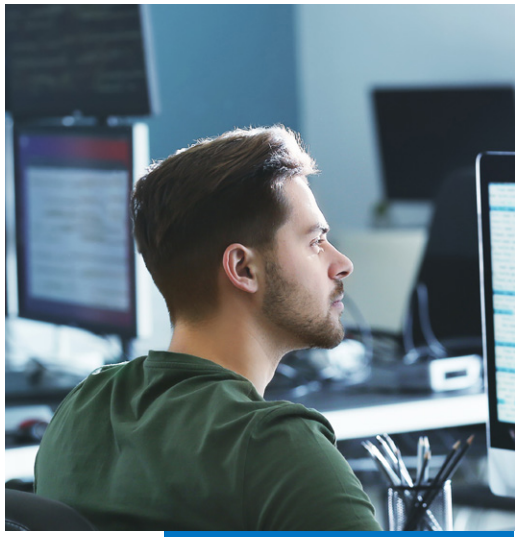
- 企業全体の署名鍵および利用証明書の一元管理
- セキュリティ上のニーズに合わせたアカウント構造と機能を適合させる
- システムのアクセスを指定したユーザーに限定
- 重要な機能について単一脆弱点をなくす
- アカウントアクセスにゼロトラストポリシーを適用
- システム権限の割り当てと取り消しの効率化

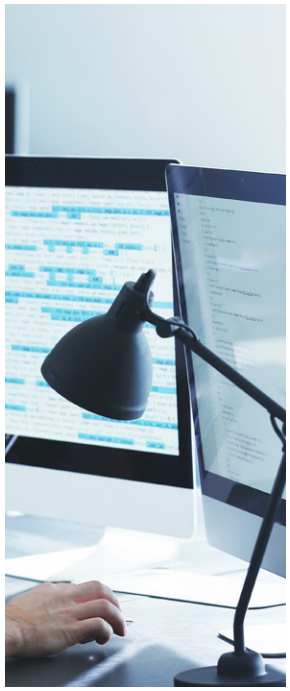
必要な機能

- 全ての鍵およびすべての利用証明書を統合するための鍵と証明書のインポート
- ユーザー構造の一元的アカウント構成（ICA および ICA 属性の設定を含む）
- アクセスポリシーの制御を含む細かなユーザーロールおよび権限
- 二者の承認機能を満たすための最少ユーザーのパーミッション
- 多要素認証のサポート
- グループのプロファイル

コード署名ポリシーと手法のヒント 1

お客様によれば、コード署名ポリシーをコード署名ソフトウェアの使用と結び付ける方法は多岐にわたります。正式なポリシー文書を作成する企業もあれば、コード署名手法に関する指針とトレーニングを行う企業、ソフトウェアを使用してポリシーを一元的に適用している企業もありました。





コード署名ポリシーと手法のヒント 2

お客様から挙げられた鍵の取り扱いに関する懸念事項のトップ 3 は、誰が鍵を管理するか、どこに鍵を保管するか、署名権限の定義と適用でした。

包括的な鍵保管と取り扱い手段

鍵保管と取り扱いの管理策を細かく定めることで、鍵の取り扱い手法の組織をまたいだ不整合がなくなり、権限のない不正なアクセスや使用を防止できます。

目的

- セキュリティニーズ（パブリックトラストまたはプライベートトラスト）に最もふさわしい鍵保管手段を選択
- 機密性の高いプロジェクトには厳しい制御を実装
- 潜在的な脅威を調査するときにアクセスを制限
- 本番環境とテスト環境で鍵使用方法を分離
- 対象のソフトウェアプラットフォームの要件に合った適切な鍵使用モデルを適用
- 期限切れ、脆弱、非準拠の暗号化要素を含む鍵の使用を削減
- 効率化とヒューマンエラーの削減

必要な機能

- ハードウェアセキュリティモジュール（HSM）または暗号化ストレージの鍵保管オプション
- 誰がどの鍵にいつアクセスできるかを制御する鍵アクセスプロファイル
- 素早い応答を可能にするオンラインおよびオフラインの署名鍵モード
- 本番用およびテスト用の署名鍵タイプ
- 静的、動的、およびローテーションの鍵使用モデル
- きめ細やかな鍵ペアプロファイルの制御
- 1 クリックの生成ワークフローによる証明書プロファイルテンプレート

ワークフローの統合と自動化

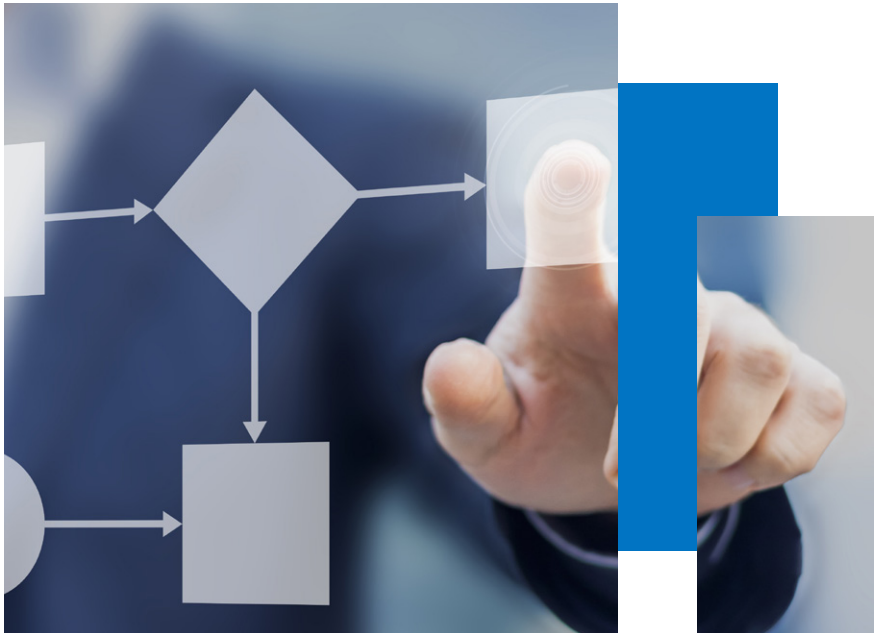
統合と自動化は、手作業によるミスを防ぎ、効率を高め、署名手法に一貫性をもたらし、アジャイル開発の市場への投入時間（Time-To-Market）目標の達成に役立ちます。

目的

- 開発プロセスを遅らせることなくセキュリティを保護する
- 手作業による署名プロセスと比べてユーザーの利便性を向上しながら企業のセキュリティとコンプライアンスのレベルを高める
- 署名プロセス中にソースコードが傍受されるリスクを最小限にする

必要な機能

- CI/CD パイプラインとの統合（コマンドライン、コンソール、または API オプションによる）
- 複数の CI/CD プラットフォームのサポート
- 開発者およびビルドサーバーに関する一元化された事前設定済みのアクセスおよび権限
- 事前設定済みの証明書テンプレートと証明書生成
- ハッシュ署名により、ソースコードの転送が不要



コード署名ポリシーと手法のヒント 3

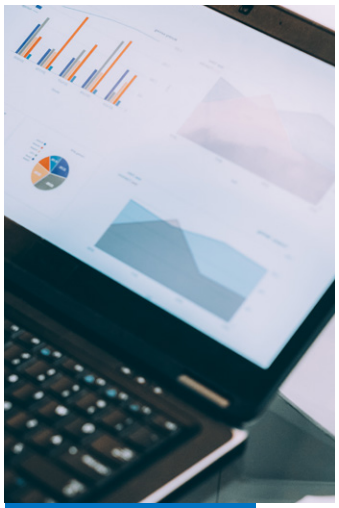
お客様によれば、コード署名ポリシーおよび手法の主な原動力となったのは、ビジネス/法律上のコンプライアンスと顧客要件でした。

コード署名ポリシーと手法のヒント 4

お客様によれば、専任のセキュリティまたは IT 組織によって管理され、コード署名ソフトウェアによって適用されたコード署名ポリシーは非常に効果的でした。

コード署名ポリシーと手法のヒント 5

お客様によれば、セキュリティチームと IT チームの両者がコード署名ポリシーの策定の鍵を握っていました。その他に、最高情報セキュリティ責任者（CISO）、コンプライアンスおよびリスク管理部門、DevOps、セキュリティ運用部門、製品管理部門、サイバーセキュリティおよび IT チームなどの名前が挙がりました。



リリースプロセスの制御

リリースプロセスの制御は、開発プロセス中にマルウェアが仕込まれるのを防ぐのに役立つ追加のチェックを提供します。

目的

- リリースプロセス中の悪意あるアクティビティの機会を減らします。

必要な機能

- アクセスを承認済みのユーザーに限定するためのユーザーアクセス権、スケジュール枠、その他の条件を定義するリリース枠属性および制御
- 再現可能なビルドの原則を使用して「ゴールドスタンダード」を定義し、それを以降のビルドの比較点として使用するリリース比較機能

一元化された柔軟なレポーティング

一元化されたレポーティングは、是正を素早く行い、監査要件に準拠し、潜在的な問題や脅威を特定するのに役立ちます。

目的

- 完全な可視化とコード署名アクティビティの制御
- いつ誰が何に署名したかを把握し、是正をスピードアップ
- 監査のコンプライアンスを提供

必要な機能

- 監査とトラッキングアクティビティをサポートする一元化されたログ記録とレポーティング
- レポートフィルター（raw およびフォーマットされたファイルタイプによるエクスポート機能付き）

コード署名ポリシーと手法のヒント 6

お客様によれば、メーカーから顧客に渡すソフトウェアパッケージのソースと完全性を保証することが重要であるのと同じように、コード署名プロセスを標準化し、文書化し、トレース可能にし、説明可能にし、セキュアにすることが重要です。

柔軟でスケーラブルな導入

組織内のさまざまな実装ニーズに対応するため、実装モデルに選択肢があることが必要です。また、予期される署名要件に対してソリューションのスケーラビリティを評価する必要があります。

目的

- 望ましい方法で実装できる能力
- 大容量および高スループットの署名アクティビティに対応できる能力
- オンデマンドのスケーラビリティを備えた効率的なセットアップ

必要な機能

- 組織全体の包括的なデリバリーのニーズに対応できるオンプレミス、クラウド、またはハイブリッドのオプション
- 具体的なセキュリティ構成要件をもつ部門のための ICA の高速かつ高効率なセットアップ
- 高速かつ高効率なスケーリングを行うためのオーケストレーション対応のコンテナベースのアーキテクチャ

まとめ

コード署名ソフトウェアはソフトウェアリリースプロセスの脆弱点を大幅に削減できます。柔軟な構成が可能で、包括的な機能セットを備えたエンタープライズグレードのソリューションは、企業のコード署名ポリシーおよび手法の目標を達成するのに最適です。このソリューションは以下を提供します。

保護

- 鍵の盗難や不正使用につながる可能性のある脆弱点をなくす
- リリースプロセスにマルウェアが仕込まれるのを防ぐ

管理

- 開発チーム全体のセキュリティ体制とコンプライアンスに一貫性をもたらす
- 署名アクティビティの可視化と制御を一元化する

生産性

- 効率を高め、ヒューマンエラーを削減する
- 暗号の変更と準拠の俊敏性を改善する

始めましょう

デジサートは、世界最大規模の組織に向けたエンタープライズクラスの TLS/SSL、PKI、IoT セキュリティのソリューションプロバイダであり、いついかなるときも安心感と安全なデータとを提供しています。当社の担当者にお客様のニーズをご相談ください。

詳細は、jpn-info-pki@digicert.com まで E メールでお問い合わせいただくか、www.digicert.com/jp/signing/secure-software-manager をご覧ください。