digicert®

エンドツーエンドの コード署名セキュリティの制御

近年、ソフトウェアサプライチェーンへの攻撃が増加していることから、企業はソフトウェア開発ライフサイクル（SDLC）全体のセキュリティを見直す必要に迫られています。手作業でコード署名を実施していたのでは、プロセスの不整合や脆弱なポイントが発生し、それが悪意のある攻撃者の標的になる恐れがあります。DigiCert® Secure Software Manager は、セキュリティ態勢を改善し、鍵と証明書の使い方をビジネスニーズに対応させたうえで、コード署名にシームレスで一貫した強力なセキュリティを提供します。

DigiCert® Secure Software Manager のセキュリティ機能

- アカウント管理の制御
- ユーザーアクセスおよび管理の制御
- 鍵と証明書のセキュリティの制御
- ソフトウェアリリースにおけるセキュリティの制御
- 追跡とレポート
- 自動化

アカウント管理の制御

アカウント管理の制御は、企業のセキュリティポリシーの適用、役割と義務の分掌、盗難や悪用を防ぐための重要なセキュリティ業務の標準化を実現します。

主な機能	利点
一元的アカウント構成	アカウント機能、制御、ユーザー構造を柔軟に設定して、組織のセキュリティニーズに対応します。
きめ細かいアクセス制御	権限のないユーザーが業務に関係のない鍵や証明書を作成するのを防止します。
アカウントレベルの制御	鍵ペア生成のアルゴリズム、鍵サイズ、暗号強度などをアカウントレベルで制御することで、ポリシーの遵守を徹底します。
他の鍵のインポート	すべての環境で作られた署名鍵と証明書の統合管理により、可視性と制御性を確保します。

ユーザーアクセスおよび管理の制御

ユーザーアクセスおよび管理の制御によって、指定されたシステム機能へのアクセスを許可されたユーザーのみに制限し、意図しないアクションや悪意あるアクションを最小限に抑えて、ポリシーの遵守をサポートします。

主な機能	利点
細かなユーザーロールおよび権限	ユーザーロールごとにシステムへのアクセスを定義することで、職務分掌をサポートし、迅速な実装、停止、削除、短期アクセスを有効化します。
最少ユーザーのパーミッション	重要な機能に対する単一承認による脆弱なプロセスを排除し、特定のアクティビティに対して二重のユーザー承認を義務づけます。
グループのプロファイル	アクセス権や生成権限を管理する鍵ペアと証明書のプロファイルを、ユーザーグループごとに割り当てたり取り消したりすることで、効率を向上させます。
多要素認証（MFA）	アカウントアクセスにゼロトラストポリシーを適用

鍵と証明書のセキュリティの制御

鍵および証明書の高度なセキュリティ制御によって、鍵の取り扱いの安全性を高め、盗難や不正使用を減らします。

主な機能	利点
鍵アクセスプロファイル	許可されたすべての署名者がアクセスできる「オープン」設定と、より厳重にセキュリティを制御する「厳密」設定によって、複数のセキュリティユースケースをサポートします。
鍵保管オプション	公開鍵と秘密鍵の両方について鍵の保管方法を選択でき、パブリック証明書の鍵の場合はハードウェアセキュリティモジュール（HSM）への保管も可能です。
本番用およびテスト用の署名鍵タイプ	本番用およびテスト用に鍵の種類を分けて定義します。本番用の鍵は常時有効で、公開および秘密のバイナリへの署名と、新しい証明書の生成に使用されます。テスト用の鍵は 30 日以内で失効し、内部リリースを検証する際にオンデマンドで使用されます。

静的、動的、および ローテーションの鍵使用モデル	鍵使用モデルを、主なソフトウェアプラットフォームのセキュリティ要件に対応させます。 • Android: アプリケーションのリリースごとに同じ鍵/証明書を使用する静的な鍵。 • Java および IoT: 鍵と署名が一対一の関係になる動的な鍵。 • Microsoft Smartscreen Filter: 証明書プール内で循環するローテーション鍵。
オンラインおよび オフラインの署名鍵モード	機密性の高いプロジェクトや、脅威を調査する場合などで、より厳重なセキュリティ管理を実現します。オンラインモードの場合、許可されたユーザーならいつでも鍵を使用できます。オフラインモードの場合、鍵がオンラインに戻るか、スケジュールに基づくリリース期間が作成されるまで鍵の使用を禁止します。
証明書プロファイルテンプレートと 証明書生成ワークフロー	コンプライアンスの向上、時間の削減、エラーの低減を図ります。事前定義された属性を証明書プロファイルテンプレートとして保存し、UI でワンクリックして、またはコマンドやスクリプトの一部として、証明書生成ワークフローで使用できます。
きめ細やかな鍵ペア プロファイルの制御	鍵ペアプロファイルの一元管理によって、暗号移行の俊敏性を向上させ、脆弱な暗号要素や準拠していない暗号要素をもつ鍵の使用を削減します。アルゴリズム、鍵サイズ、強度に対して鍵ペアプロファイルの制御を設定できます。

ソフトウェアリリースのセキュリティの制御

ソフトウェアリリースのセキュリティの制御は、リリースプロセス中のセキュリティを強化し、内部開発を狙ったソフトウェアサプライチェーン攻撃を阻止します。

主な機能	利点
リリースウィンドウ	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。許可されたユーザー、鍵の種類（オンライン、オフライン、テスト用など）、バイナリ数、開始/終了日時、事前に許可された署名期間、リリースメタデータなどのリリース属性を事前定義します。設定と承認によって、職務の分離を必要とするポリシーをサポートします。
リリース比較	リリースプロセス中にマルウェアが仕込まれていないことを確認できます。再現可能なビルドの原則を満たし、ソースコードから製品バイナリまでの検証可能なパスを提供することによって、本番用リリースで署名できる内容を制御できるベースラインビルドを定義します。

エンドツーエンドの追跡とレポート

集中管理されたエンドツーエンドの追跡とレポートによって、脅威の分析と検出が容易になり、悪意のあるアクションやエラーの迅速な修復をサポートして、業界標準の認証と監査をサポートします。

主な機能	利点
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	アカウント、鍵ペア、証明書操作、署名に関連するアクティビティの詳細なログを記録して、コード署名のアクティビティの完全な可視化と制御を実現します。成功したイベントと失敗したイベントのどちらも記録して、今後の是正措置に必要なインサイトを確保できます。レポートは、フィルタリングしたうえで、raw データまたはフォーマット済みデータとして、あるいは API 経由でエクスポートすることができます。

自動化

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ます。

主な機能	利点
継続的インテグレーション/継続的デリバリー（CI/CD）プロセスとの統合	アジャイル開発を遅らせることなく、署名プロセスを自動化し、セキュリティを提供します。CI/CD プラットフォームと統合します。デジサートのクライアント側ライブラリは、スクリプトによって自動的に呼び出すことができます。
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	直接介入することなく署名できる、事前設定済みの制御によって、セキュリティコンプライアンスとユーザーの利便性が向上します。制御は中央のパネルから設定でき、指定した間隔に限定することができます。ビルドサーバーを API ユーザーとして設定すれば、署名リクエストの自動処理も可能です。
ハッシュ署名	ソースバイナリを開発環境から出さずに済むため、ソースコード傍受のリスクを低減できます。ハッシュファイルをアップロードして署名し、ファイル転送のフットプリントとフルバイナリの転送に伴うレイテンシーを削減します。

詳細および無償トライアルのリクエストについては、jpn-info-pki@digicert.com まで E メールでお問い合わせいただくか、digicert.com/jp/signing/secure-software-manager をご覧ください。