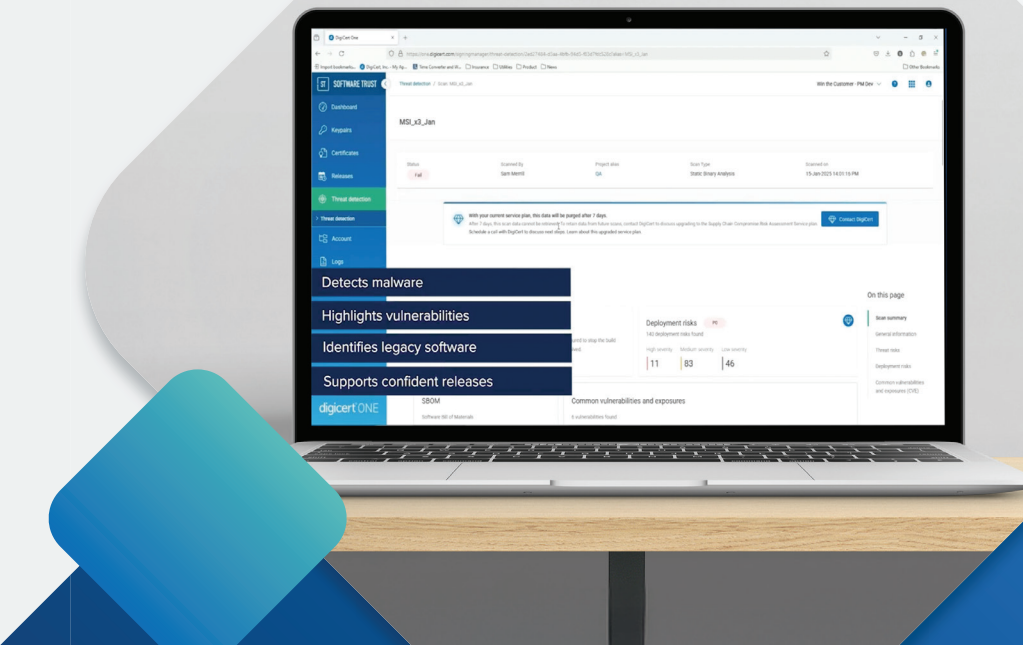
digicert®

キヤノン、コード署名へのセキュリティ強化と厳格な統制を導入



ケーススタディ

キヤノン、コード署名へのセキュリティ強化と厳格な統制を導入

概要

企業名: キヤノン株式会社
事業部門:デジタルプリンティング事業本部
https://global.canon/

業種: 電気機器
本社: 東京都大田区

「共生」の企業理念のもと、プリンティング、イメージング、メディカル、インダストリアルの4グループが新規事業を中心に、新たなイノベーションを創出しています。

主なビジネス要件:

- アプリケーション、プリンタードライバーなどに対しコード署名
- CA/Bフォーラムが求める秘密鍵の保護を管理するコード署名システム
- コンプライアンス統制

ソリューション:

- DigiCert Software Trust Manager

主な特長:

- すべてのコード署名業務の完全な可視化と制御により、潜在的な脅威に対する迅速な検出と対応が可能に
- 役割ベースのアクセス管理により、署名業務と管理業務を分離、作業負荷を軽減し、ヒューマンエラーやセキュリティ侵害のリスクを最小限に
- 自動化されたワークフローと直感的なツールにより、コード署名にかかる時間が半減、プロセスの合理化と技術的な専門知識に関係なくユーザーに権限を委任
- 一元化された厳格な管理により、企業のセキュリティ・ポリシーと法規制の遵守を徹底するとともに、企業のセキュリティ体制を明確に把握

要件

内製コード署名システムからベンダー製システムへのリプレースにより、秘密鍵保護に関する基本要件にいち早く対応

デジタル・イメージング・ソリューションの世界的リーダーであるキヤノン株式会社は、コード署名プロセスのセキュリティを強化する必要に迫られていた。同社の売上の約5割を占めるプリンティング部門は、さまざまな業界向けのプリンターや複合機（MFP）を製造している。社内で開発されるプリンター機器用アプリケーション、プリンタードライバーは、接続されたデバイスの安全性と最新のオペレーティングシステムとの互換性を確保するために安全でなければならない。最近までキヤノンは自社向けに開発したコード署名システムを利用してきたが、進化するセキュリティ要件により改変を検討する必要があった。一つは2023年6月以降、CA/B フォーラムにより安全な秘密鍵の保護が求められることになったことである。

その一方、グローバルなソフトウェア・サプライチェーンへの攻撃が憂慮すべきほど増加しており、コード署名プロセスを一元的に管理し、組織全体で機能するソリューションが必要だった。キヤノンは、自社システムの大幅な改善なしに使い続けることはできず比較検討の結果、デジサートが提供するクラウド型のDigiCert Software Trust Managerの利用を決めた。 これにより厳格な鍵管理と同時に事業本部内の署名プロセスの可視化、社内コンプライアンスの統制を実現した。

「署名メンバーが一回の署名で行う作業フローの半分程度を削減できました。」

複数拠点で行われるコード開発

キヤノンの主力ビジネスの一つであるプリンティング部門は、個人向けから企業向け、さらには印刷業界や製造業、食品向けといったありとあらゆる印刷に関わる製品を開発している。そのためにアプリケーションやファームウェアが果たす役割は非常に大きい。そのアプリケーションに求められるセキュリティ要件は高く、従来よりコードサイニング証明書とコード署名システムを利用してきた。これにより接続するコンピューターなどの安全を守り、最新の多様なOSでも動作することが保証される。

なお、このアプリケーションやファームウェアなどを開発し署名を行うメンバーはキヤノンの各拠点に分散しているのが現状だった。

CA/B フォーラムのBASELINE REQUIREMENT更新対応と社内フローの変更

2022年11月、全世界的にコードサイニング証明書とその秘密鍵の漏えい事件の頻発を背景にしてCA/B フォーラムが 秘密鍵の生成と保護要件に関してコードサイニング証明書のBaseline Requirement（基本要件）の変更を決定した。OVコードサイニング証明書の秘密鍵もEVコードサイニング証明書同様FIPS140-2 Level 2 もしくは Common Criteria EAL 4+以上の安全なHSMに保存すべきことが決定したのだ。キヤノンでは、よりセキュリティ要件が厳格なEVコードサイニング証明書への移行を検討しているところではあったが、秘密鍵の保護要件は事業本部内の業務に大きな変更を強いることになる。

そこで、従来より利用してきた署名もシステムを新しい標準に合わせて改修し利用し続けるのかというのが新たな課題として挙がってきた。

ソリューション

コード署名の業務の可視化と役割ベースのアクセス管理

キヤノンがこれらの状況を背景に、内製署名システムの改修および運用費用とベンダー製システムの費用、鍵管理、署名プロセスの可視化による社内コンプライアンス統制によるメリットを総合的に比較し導入を決めたのがDigiCert Software Trust Managerである。

Software Trust Manager はキヤノンに、組織全体におけるすべてのコード署名業務を追跡・監視するための可視性と制御を提供する。この全社的な監視により、同社のセキュリティ・チームはそれを把握できるようになった：

- コード署名がいつ、どのシステムで行われたか。
- 誰が署名業務を行ったか。
- 使用された証明書、秘密鍵はどれか

このきめ細かな可視化により、セキュリティチームは異常や潜在的な脅威を従来よりも迅速に検知し、対応できるようになった。

さらに、Software Trust Managerは役割ベースのアクセスコントロールを提供し、キヤノンは開発者の責任を大幅に軽減することができた。これで開発者は、証明書や鍵の管理まで心配する必要がなくなり、コードに署名するという行為だけを心配すればよくなった。この業務分離は、開発者の作業負担を軽減するだけでなく、ヒューマンエラーや潜在的なセキュリティ侵害のリスクも最小限に抑えた。

SoftwareTrust Manager管理担当者は「SoftwareTrust Managerが面倒な鍵の管理などを署名メンバーから開放したことで、署名メンバーが一回の署名で行う作業フローの半分程度を削減できた。また、コード署名業務の全てが管理・統制できたことで、事業本部内でのコード署名業務の管理にかける時間が大幅に削減できた。」と語る。

多様なソフトウェア開発環境と開発者の嗜好に対応する署名

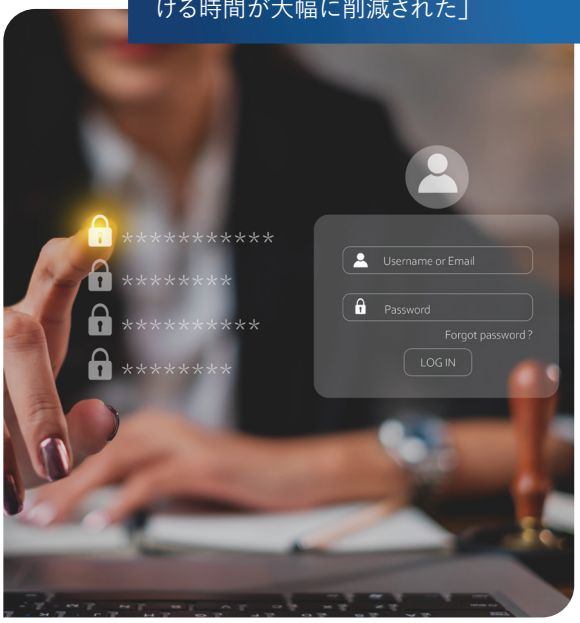
キヤノンがSoftware Trust Managerを選択したもう一つの大きな理由に署名業務フローの効率化がある。Software Trust Managerで署名を行う方法には、署名ツールやプラットフォーム毎に複数のやり方が用意されている。特にMicrosoftのSignToolによる署名方法には、コマンドラインで呼び出して署名する手法や「DigiCert Click-to-Sign」と呼ばれる右クリックで署名できる手法が用意されており、特に後者は設定を事前に行えば簡単に署名ができることから業務負荷を大幅に削減できる。それは通常のPCの操作と同じように行えることから幅広い利用者から支持を得られそうだと判断した。実際に利用者からは「コマンドラインから署名する手法よりも右クリックで容易に署名が実施できるようになり、ITリテラシーのレベルに関係なく幅広い方々が署名を実施できるようになった」と好評である。

さらにClick-to-Signでは、署名システムへアプリケーションをアップロードし、署名実行の後、署名システムからダウンロードする従来の方法より署名に利用する時間を半減できたという。また署名メンバーは署名行為を行うだけで自動でログを残すので、管理システムへ履歴入力が不要なため署名管理の観点でも効率化とデータの完全性が実現した。

この大幅な時間短縮を実現しているClick-to-Signだが、キヤノンの開発をサポートする複数の要望が提案された。DigiCert はアジャイル開発により顧客メリットや要望により短い期間で更新を行っているため、その実現は更なる効率改善を実現するだろう。

DigiCert Click-to-sign

「事業本部内でのコード署名業務の管理にかける時間が大幅に削減された」



キヤノンのコードへのデジタルトラストへの取組の見通し

署名鍵の管理と既存の管理システムの置き換えをトリガーに導入した SoftwareTrust Managerの導入であったが、セキュアソフトウェア開発フレームワークがカバーする範囲は幅広い。ソフトウェアに署名をするから安全なのではなく、安全に作成されたソフトウェアに署名を行うわけである。また、近年のソフトウェアは多くのライブラリやコンポーネントを組み合わせて構成されている。それらのコンポーネントの一つで脆弱性が発見されると、そのコンポーネントを使えなくする手段を取ることが求められるし、利用するコンポーネントの脆弱性を常に管理することが求められる。

また、開発の手法も常に新しい手段が出てきており、それらの変化に対してもソフトウェア開発フレームワークの手法を利用して常にユーザーに安全を届けることが必要になる。

SoftwareTrust Managerは、これらのソフトウェア開発フレームワークへの対応にさまざまな統合、連携機能を実装している。コードをバイナリスキャンし、脆弱性や秘密情報を見つけ出す脅威検知機能、そのスキャン結果をもとにSBOMを生成する機能、作成したSBOMに対して改竄を防ぐドキュメントサイニングを行う機能などを備えている。

そこで、さまざまある機能のうち近い将来利用を期待している機能について訊ねてみた。

「すでにユーザーはコード署名に利用する秘密鍵にアクセスすることはないので、安全なソフトウェアへの署名と鍵管理は実現できている。しかし、もし利用したライブラリやコンポーネントに脆弱性が発見された場合、署名ごとに秘密鍵をローテーションすることで特定の署名を行ったソフトウェアのみ失効させることが可能だ。この機能には興味がある。」とSoftwareTrust Manager管理担当者は語る。

未来へ向けた準備

今後、日本だけでなく海外、また各業界団体でソフトウェア・コードのセキュリティ標準がそれぞれ定められつつある。それらに対応するのは、多くの労力を要する。また生成AIの発展により量子コンピューターの実現が早まることが多く報じられるようになってきた。これは量子コンピューターによりさまざまな発明や予測などの精度が上がることが期待される反面、現在利用されている暗号は容易に解読されることが想定される。それはコード署名も同じで、解読され改竄されるリスクが課題になるのである。

それらの対応をするには証明書、署名、そしてそれらがどの暗号強度のアルゴリズムなのかというインベントリーを整備し、各標準・規格への対応状況をきちんと把握し、優先順位をつけて対策計画を遂行することが重要である。

その際にSoftwareTrust Managerにより、インベントリーの一元管理を行い、厳格な統制を効かせた体制は未来へ向けた強力な備えとなるだろう。

「署名ごとに秘密鍵をローテーションすることで特定の署名を行ったアプリケーションのみ失効させることが可能だ。」