White Paper

PKI への投資が企業のセキュリティの向上とビジネスプロセスの最適化を支援する

Sponsored by: DigiCert Inc.

Robert Westervelt
August 2019

エグゼクティブサマリー

IT セキュリティ専門家と運用チームは、急速な進化を続けるエンタープライズデジタルトランスフォーメーション（DX）イニシアティブに対応するために、ミッションクリティカルなシステムのセキュリティとレジリエンシーを管理するという大きなプレッシャーにさらされている。成長を続けるハイブリッドおよびマルチクラウド環境の中で、このプレッシャーを緩和し、さらに効果的にリソースを配分できるように、最高情報責任者（CIO：Chief Information Officer）、最高情報セキュリティ責任者（CISO：Chief Information Security Officer）およびセキュリティアーキテクトは、公開鍵基盤（PKI：Public Key Infrastructure）の実装に取り組んでいる。しかしながら、その実態は、しばしば一貫性を欠き、管理も不十分であることが多い。

サイバーセキュリティのレジリエンシーを重視する多くの企業が、PKI をそのバックボーンと位置付ける理由は、企業がデジタル証明書と公開鍵暗号を利用し、データセキュリティポリシーとプロシージャを強化するプロセスを自動化できるためである。PKI は、そもそもシステム間で認証された信頼できるコネクションを確立し、重要な情報源へのユーザーのアクセスを妨げることがないように設計された。やがて、暗号化されたコードサイニング証明書を使ったドキュメント、電子メールおよびコードの完全性を保護すると共に、デバイス証明書を用いたデジタル ID によるデータ資産と個人を保護する目的でも使用されるようになった。

現在、セキュリティチームはこれまで以上に大きなプレッシャーにさらされているため、PKI は徹底的にテストを受け、信頼されるにいたっている。ビジネスがクラウドサービスの利用を拡大するにつれ、チームは PKI を使いリスクを軽減しようと試みるが、これに対し攻撃者はセキュリティインフラストラクチャがセグメント化されることで生じる複雑さと環境設定の問題に付け込もうとする。IDC のユーザー調査「Data Services for Hybrid Cloud Survey」によると、CISO はこの課題への取り組みを優先事項としている。この調査では、欧州と北米の IT セキュリティおよびデータ管理の専門家、400 人以上を調査の対象とした。この中で、企業の約 65%が、以下に挙げるさまざまな機能をサポートするためにデジタル証明書と PKI を使っていると報告している。

- **セキュア BYOD：**モバイルユーザのエクスペリエンスを損なうことなく、管理対象外の BYOD（Bring Your Own Device）デバイスにも対応することで、企業のリソースへのセキュアなアクセスを維持する機能
- **セキュア認証：**機密情報を含むアプリケーションに対する個人認証を強化する機能
- **セキュアリモートアクセス：**ワイヤレスネットワークや VPN（Virtual Private Network）へのアクセスをセキュアにするための従業員とパートナーの認証を強化する機能
- **セキュア電子メール：**ユーザーが、企業のすべてのデバイスに対して、暗号化されデジタル署名された電子メールを送信することを可能にする機能
- **ドキュメントサイニングの完全性：**重要なドキュメント上のデジタル署名の完全性と真正性を認証する機能