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

- **セキュアな IoT（Internet of Things）デバイス：**機密情報のやりとりが多い IoT デバイスに関して、デバイス ID を提供し、信頼の基点（Root of Trust）を確立し、ソフトウェアとファームウェアの完全性を保持する機能

企業は多くの分野でセキュリティ対策のために PKI を利用し続けるものの、機密データに対する攻撃が巧妙となり、攻撃頻度も高まるため、セキュリティチームはより包括的で整合性のあるアプローチを取り、進化を続けるビジネス戦略をサポートする必要がある。企業の 60%が、今後 24 か月以内に DX 戦略を採用すると IDC は予測している。IT トランスフォーメーション（ITX）は DX 戦略のキーとなるコンポーネントであり、データのセキュリティと可用性は ITX の礎である。PKI は、企業の IT インフラストラクチャの完全性、可用性およびレジリエンシーを維持する上で重要な役割を果たしているが、脅威が多様化し巧妙化するにつれて、急速に進むハイブリッド環境をカバーするデータ保護の管理は、ますます複雑になりつつある。最近の一連のデータ侵害が関心を集めているが、これは現在の高度に分散され複雑化した企業環境によって生じる問題を示している。攻撃者は、データベースサーバーをインターネット上に公開し放置するなどの手痛いミスにつけ込んでいる。攻撃者は絶えず、脆弱なパスワード、デフォルトのままのパスワード、盗まれたパスワードを悪用し続け、分散環境でのデータ管理によって生じる脆弱性を探し続けている。調査対象企業の 30%以上が既存の IT インフラストラクチャを利用したハイブリッド環境とマルチクラウド環境を統合することの難しさを挙げている。また、37%の企業が「セキュリティソリューションの複雑さ」という項目について、今後 2 年間に直面するであろう 3 大脅威のうち、「攻撃の巧妙化」と「クラウド導入のリスク」に次ぐ 3 番目の脅威であるとしている。問題は、PKI オペレーションの破綻が、しばしば、ユーザーの生産性の低下、顧客とパートナーの信頼関係の毀損、甚大な損害を与えるセキュリティインシデントとデータ侵害などを、さらに悪化させてしまうことである。

クリティカルなビジネスアプリケーションの PKI によるサポートは「非常に効果的」である

この調査で行われたインタビューで、PKI が業界に特有のさまざまなビジネスアプリケーションといかにシームレスに統合できているかについて、非常に肯定的な印象が得られた。PKI は、暗号化をサポートする先進的なアナリティクスレポジトリーを含むさまざまなバックエンドシステムとの統合、カスタムコンテンツ管理システムを使用した契約の完全性を維持するためのデジタル文書の署名の有効化、リモートアセス向けの複雑な支払いアプリケーションや販売時点情報（POS：Point of Sale）端末に対応するようなスケーリングが評価されていた。

PKI が適切に実装され能動的に運用されている場合、CISO およびセキュリティアーキテクトは非常に良い印象を持っており、「極めて効果的」としている。インタビューを受けた企業のほとんどは、複数の PKI 環境を配備し、それらと業界固有のビジネスアプリケーションおよび Active Directory とを組み合わせて利用している。これらの企業は、自社の組織での成長と変革が十分に実感できるほどの期間において PKI を管理しつつある。また、強固なセキュリティ体制を維持するために、既存の PKI 環境を何度もアップデートしている。PKI の有効性を強化するために、IT 組織は以下のアクションを取るべきであると、IDC は提言する。

- セキュリティアーキテクトが、既存の PKI 環境を管理することに関心を持ち、トレーニングを受け、業務を続けようとするか否かを、適切に把握すべきである。また、デジタル認証のためのスケーラブルなアプリケーションを必要とする新しいビジネス目標をサポートできる専門知識をチームが有しているかを判断すべきである。
- 管理を合理化し複雑さを減らすために、マネージド PKI サービスの活用を考えるべきである。いったん PKI の仕様が決まり運用が始まると、仕様やプロセスの変更はやっかいなものになる。前もって投資しておくことが重要である。

調査方法

IDC の調査では、大企業数社の最高情報セキュリティ責任者およびセキュリティアーキテクトに、既存の PKI インフラストラクチャに関して、企業のクラウドの導入と DX 戦略をサポートするために、インフラストラクチャをどのように適応させたかについてインタビューを行った。このインタビューから得られたインサイトは、セキュリティハイブリッドとマルチクラウド環境に関する新しい調査結果を組み合わせている。この調査によって、さまざまなユースケースに関連する効率の改善と管理コスト削減が明らかになった。ユースケースには、IoT デバイスのソフトウェアのアップデートの真正性を検証するためのコードサイニング管理が行われたオンプレミス PKI の実装環境、文書ファイルのデジタル署名による紙と手作業のプロセスの排除、セキュアな電子メール、セキュアなリモートアクセス、機密性の高い企業リソースに対するユーザー認証とコンピューター認証などが含まれる。

概況

攻撃成功を阻止し、重要なリソースの防護に必要不可欠な PKI

多くの企業は、インフラストラクチャの断片化と冗長化を排し、コスト削減のための DX イニシアティブの一環として、デジタル証明書の管理を合理化し、集中化し、自動化を進めるための PKI スペシャリストのサポートを求めている。このサポートには、さまざまなビジネスユニットを支援する 1 つ以上の PKI 環境の管理をマネージド PKI サービスとして自動化することで、適切なメンテナンスと信頼性を確保することが含まれる。

多くの PKI への投資の背景として、コスト削減と効率向上がしばしば挙げられていることが本調査によって明らかになった。しかし、PKI 導入の主たる促進要因（ドライバー）は、セキュリティ製品の実装と管理の複雑さから生じる弱点と脆弱性であった。IDC のユーザー調査「Data Services for Hybrid Cloud Survey」では、IT セキュリティ、LOB（Line of Business）およびデータ管理の各分野の専門家のほぼ 40%が、攻撃の高度化とセキュリティ製品の管理とサポートの複雑化が大きな課題であると述べている。本調査では、セキュリティとプライバシーに関わる懸念の増加に、セキュリティチームが直面していることが明らかになった。チームは、強化される傾向にあるコンプライアンス義務を果たすというプレッシャーを受け続けており、企業の重要なリソースを標的とした多方面からのサイバー攻撃の増加に、チームは常に防御を強いられている。

評判の失墜、直接的なコストの増加および規制に対する制裁措置に加えて、サイバー攻撃は、計画外のダウンタイムや競合上の機密情報の漏洩、データの永続的な喪失を引き起こす可能性がある。IDC の調査では、ダウンタイムに伴う平均コストは、業界全体で 1 時間当たり 25 万ドルであった。攻撃に対する防御策のコストとリカバリーソフトウェアのコストを 1 時間のダウンタイムと比較しても、このコストはしばしば正当化される。データ侵害があった場合、侵害を受けたことの公表が必要であり、必然的に評判の失墜につながる。しかもそれが長期間に及ぶことが多い。顧客やデータを永久に失うことになり、それを取り戻す方法は皆無である。データ侵害のほぼ半数でその企業の評判が失墜し、リカバリーコストと修復のためのコストがさらに増えることが、IDC の調査で明らかになった。

日々公表されるセキュリティ侵害は、企業も消費者も ID 認証がセキュリティの要であることを常に再認識させられている。複雑さの増大に伴い生じることが多い脆弱性や環境設定の問題が、セキュリティインシデントの一因であることが多数の調査で示されている。断片化され、散り散りとなっている PKI の実装環境を整備することで、攻撃者に付け込まれるようなユーザーおよびシステムによって引き起こされるエラーが削減され、プロセスのデータ漏洩を防ぐことができる。適切に導入、管理されている PKI は、厄介で費用もかかるデータ漏洩を避けるために企業が利用できる最も強力なツールの一つである。危険性への状況把握能力を高め、セキュリティ体制を強化するために、暗号化と鍵管理の戦略を見直す企業が増えている。

この調査でインタビューに答えたセキュリティの専門家は、PKI はデータ暗号化をサポートし、データとトランザクションの完全性を検証する上で必須であり、十分実績のあるコンポーネントであるとしている。また、PKI は、企業でのユーザーと端末の ID を確認する上で非常に重要であるとも述べている。PKI は、攻撃者が重要なリソースに侵入するに当たって破らなければならない障壁を高めることができる。PKI は、高速の、または多方面での重要なビジネスプロセスで要求される拡張性のあるセキュリティにも対応している。また、PKI では、エンドユーザーのアクティビティの透明性が維持されるため、ユーザーの生産性と顧客維持率を向上させることも証明されている。

インタビューで浮かび上がった 1 つのテーマは、セキュリティ対策にしばしばフラストレーションを感じるユーザーとセキュリティアプリケーションの間で繰り返されるせめぎ合いである。これに応じて、セキュリティ担当者は、ビジネス活動中にリスクが特定され次第、既存の IT とセキュリティインフラストラクチャで確実に実行できるソリューションを設計するために、PKI プロバイダーに求めることが増えている。PKI ソリューションの設計とそのプロアクティブな管理を選択した企業にとっては、セキュリティは機能性または生産性を後押しするものとなる。適切に実装された最新の PKI は、エンドユーザーが認証を完了させるために必要なステップ数を削減できる。セキュリティプロシージャが、ビジネスユーザー間に軋轢を生じさせるような面倒なプロシージャであれば、それを大幅に自動化できる。セキュリティへの考慮すべき事項として、監査結果やデータ侵害、セキュリティインシデントを受け、ある種のコンプライアンス規制や企業のポリシー要件を満たすことは、大抵、最優先事項である。今日、企業は多要素認証や暗号化、モバイル対応など、PKI でサポートされている機能を追加している。

本調査でインタビュー対象の中には、PKI インフラストラクチャの状態を評価する予算の枠内で、CIO から、コスト削減やクラウドファーストの推進を促される CISO も存在していた。CISO は、急速に進むテクノロジーの実装とビジネスの成長が生み出す軋轢で破綻し始めている PKI 環境を特定し、文書化した。これらの企業は、状況によっては、IT セキュリティを熟知した専門家を惹き付けられず、その雇用を維持できないために、既存のインフラストラクチャの管理が不十分な状況に陥っていた。企業の合併や買収の結果として、PKI の環境が断片化される、あるいはセキュリティやプロセスの制約条件が異なるために、ビジネスユニットごとに別の環境が要求されることから、PKI が断片化したままという企業もある。成長を続けると同時に分散化が進むという企業環境のリソースの性質のために、ほとんど常に、複雑さという課題が付きまとう。企業はこれらの課題との苦闘を継続していることが、IDC のユーザー調査「Data Services for Hybrid Cloud Survey」に示されている。企業は PKI を、重要な課題であると述べており、暗号化の実装と管理または情報漏洩対策プラットフォームの導入と調整と同等に困難な課題であるとみている。

PKI ユースケース

次のセクションのケーススタディでは、企業が自社に特有な要求を満たすために、PKI をいかに強化しているかに焦点を合わせる。

電子メールのセキュリティのための PKI、製造業のセキュリティ体制を強化する認証

このグローバルな消費者製品メーカーでは、サイバーセキュリティに大きな優先度が与えられたことはかつてなかった。企業の機密リソースにアクセスしようとしている従業員を認証したり、または従業員のリモートからのアクセスリクエストの完全性を確認したりするための効果的で信頼できる方法がないことから、企業が深刻な脆弱性をほとんど無視してしまう事態が生じていた。標的型マルウェア「SamSam」の形態の破壊的なランサムウェアの急激な増加は、ついに製造業者の親会社の経営陣の目に触れ、電子メールのセキュリティをサポートする PKI への投資がなされた。製造業者でのユーザー認証は、経営陣が行ったアクションの第一歩であった。

「SamSam」の背後に忍ぶ攻撃者は、その会社の FTP（File Transfer Protocol）サーバーに関わる脆弱性を容易に特定して標的とし、最初の足掛かりを得るために脆弱なパスワードに対してブルートフォース攻撃を仕掛けた。この手痛い侵害によって、会社はほぼ全面的な生産停止に追い込まれ、1 日当たり数百万ドルの損失を被った。役に立つバックアップがないため、従業員は、自分が紙の形で所有していた資料からの貴重な知的財産（IP）のリカバリーに一役を買った。IP の一部はテープストレージにバックアップされていたため、そこからリストアを実行した。セキュリティインフラストラクチャを改善するために、この会社は、PKI を利用して電子メールのセキュリティレベルを上げることなど大きな投資を行うことになった。

この攻撃の直後に、セキュリティプログラムを構築し、その製造業者の親会社の標準レベルまで上げるために役員になった CISO は、「私は、セキュリティプログラムを一から構築するために採用されました。会社にポリシーはありましたが、それ以上のものは皆無でした。会社のアプリケーションは最新のものではありませんでした。会社を支えるセキュリティインフラストラクチャの構成も貧弱であるか、インフラストラクチャすら存在していませんでした。機密データがどこにあるのかを十分に把握した上で、適切なツールを整備する必要があると感じました。これが、最新の PKI を利用して会社のセキュリティインフラストラクチャを再設計した理由です。ユーザーがどこにいるのか、どのデバイスを使用しているのかに依存しない、当社の全ユーザーを対象にしたユーザー認証と電子メールのセキュリティを実現するために、インフラストラクチャを再設計しました」と述べている。

セキュリティチームには、今後、転送される電子メールやデータファイルがセキュアなものであることを保証する必要があり、チームは、時代遅れの Lotus Notes から Microsoft Office 365 の実装へのマイグレーションの一部として親会社と共同で PKI を導入した。まず会社は、必ず二要素認証を行うことから始めて、クライアント証明書を使用して脆弱なパスワードを排除し、Office 365 のアカウントのすべて（1,300 アカウント）の ID を検証し、PKI をマイクロソフトのアクティブディレクトリフェデレーションサービス（AD-FS）に統合した。

会社は、従業員のデジタル署名を提供することで暗号化と完全性に対応するためにデフォルトで使用可能な S/MIME 証明書を有効にした。これには、社内の他の従業員、パートナーまたは社外の協力者と共に作業する際に、メッセージの受領確認をリクエストする機能も含まれる。電子メールアプライアンスは、送信および受信されるメッセージを詳細に検査し、電子メールと Web を防護するために、Web プロキシを使用する。このアプローチによって、S/MIME を有効にすることで、中間者（MITM：man-in-the-middle）攻撃を防ぎ、必要に応じて重要な知的財産を暗号化することでさらに大きなベネフィットが得られるため、製造業者のセキュリティ体制は大幅に強化された。

セキュリティツール以外に、会社はトレーニングと意識向上のイニシアティブにも投資を行った。CISO によれば、「従業員は、自分が扱っているコンテンツが制限付きあるいは厳重な制限付

きのコンテンツである場合、たとえ社内の人に電子メールを送る場合ですら、暗号化すべきであると理解しています」ということである。

この製造業者の親会社は、PKI の専門家と共同で、電子メールの混乱を避ける暗号化の実装を設計し、調整した。電子メールの配信を混乱させた暗号化トラフィックを拒否したり、隔離したりする既存のセキュリティポリシーとの間の登録の問題がいくつか存在したが、CISO は、結果論になるがトレーニングプログラムの管理にさらにプランニングが組み込めたのではないかとし、「従業員は、マルウェアのインシデントに遭遇して、新しいポリシーと自分たちのプロセスの変更を受け入れました」と述べている。この会社は、現在もセキュリティプログラムの完成度を高める歩みを継続している。同社は、データディスカバリとデータクラシフィケーションへの取り組みを始めており、そのオンプレミス資産を中心とした境界ベースのセキュリティの改善に取り組み続けている。

最新の融資プロセスをセキュアにし、先進的な分析と統合するための PKI

融資プロセスを最新化して顧客エクスペリエンスを高めようとしている大手銀行は、銀行のデジタル化された融資文書を保護し、コンプライアンスの責任を果たすために、文書を暗号化された状態で確実に保つように PKI ソリューションを維持管理する。セキュリティは投資の重要な一要素であり、新規顧客とダイナミックで無駄のないエクスペリエンスを形成するという重要な目標を妨げるものであってはならない。

銀行は、融資プロセスの開始から終わりまでを加速するビジネス戦略を強化できるセキュリティソリューションを評価した。評価チームは、現場に導入できるほど柔軟であり、既存のバックエンドインフラストラクチャと統合可能な PKI ソリューションを探した。行員は、使用しやすいが堅牢であり、複数の認証局と統合されているにもかかわらずフットプリントが小さく、パフォーマンスに優れたソリューションを必要としていた。

銀行は、ビッグデータレイク内の非構造化コンテンツの構文解析を行い、バーチャルアシスタントを実行している AI エンジンをサポートする構造化コンテンツにするソリューションを設計する必要があった。銀行には、この設計を引き受けるデータサイエンティストと開発チームに投資するために必要なリソースがあった。このデータのセキュリティをサポートするためは、当然ながら、PKI ソリューションが選択された。

PKI サービスには、新規顧客の新人研修をモニターする社内のコンプライアンスソフトウェアとの統合が要求されていた。セキュリティ要件は、高可用性、強力な災害復旧能力および銀行の仮想プライベートクラウド内で機能する PKI サービス専用のインスタンスを必要としていた。さらに、PKI ソリューションは、銀行のコンテンツリポジトリーと最新の分析環境を統合して融資文書の暗号化をサポートする必要があった。顧客保持をサポートし、銀行の提供するサービスを強化するために、このリポジトリーとアナリティクス環境が多用される。

「ダウンタイムなどは論外であり、銀行側が鍵を握り完全にコントロールできる保証が必要でした。極めて重要なアセットに関する我々のセキュリティ要求を満足する最善の方法は、PKI であることを知っていました。これまで、ビジネス面での非常に大きな改善を得られました。重要な取り引きをセキュアに進め、自行のコンプライアンス遵守義務を果たす能力には自信が持てるようになっています」と、この CISO は IDC に述べている。

文書作成と提出時の暗号化とデジタル署名の各々の要求を満たすために、この KPI の実装には、サーバーサイドコードベースが必要であり、エンドポイントのエージェントを利用する。HTTPS プロトコルを使い、Web に対応しており、ワークフロー全体が監視され、記録される。エンドポイントでは、行員が文書の作成を行うが、リポジトリーはサーバー上にある。

銀行のコンテンツリポジトリーと最新の分析環境は、新しいバーチャルアシスタントに統合されつつある。このバーチャルアシスタントは、借り手の署名の取得プロセスを自動化し、融資プロセスからストレスを除くように設計されている。融資申請書のスキャン、印刷、FAX 送信は、もはや不要になった。いったん PKI ソリューションが借り手の ID を確認したら、借り手は、手続きのために銀行の支店を訪問して、プライベートバンカーまたはリレーションマネージャーと会う必要はない。こうして、申請者は、自宅のくつろげる環境からオンラインで各ステップをセキュアに進めることができる。現在、このソリューションは、法務担当者、リスクとコンプライアンス担当役員、融資担当役員、顧客および融資プロセスに関わる他の人々を含め、2 万人までをサポートできるほど規模を拡大している。

「PKI ソリューションの実装には慎重なプランニングが必要です。セキュリティインフラストラクチャを合理的に集中化することは理にかなっていますが、データ漏洩など政策的なリスクが必ず付きまといます。全部の卵を一つのバスケットに入れる、つまりすべてを一つに託する場合、ハッキングされる恐れが生じます。集中化のためにすべきことは、すべてのサイロを横断してユーザーの行動分析を行うことです」と、CISO は述べている。

拡張されたベリフィケーションとモビリティをサポートするための、地方銀行のマネージド PKI へのアップグレード

規模の大きい地方銀行は、社内の認証局（CA）をサポートするインフラストラクチャを運用しながら、長い年月をかけて PKI プログラムを構築した。しかし、熟練したセキュリティ専門家を採用し、セキュリティインフラストラクチャ管理のトレーニングを行い、雇用し続けようと、日々悪戦苦闘している。IDC のインタビューを受けた銀行の主任セキュリティエンジニアによれば、セキュリティチームのメンバーの中には、断片化された PKI プログラムを管理する複雑さに圧倒されて、「逃げ出す」メンバーもいるとのことである。

社内の IT チームは、ユーザー認証を無効にする恐れのある複数の PKI 環境の管理に苦闘していた。VPN やモバイルデバイスに使うアクセスのソリューションであるスマートカードおよび電子メールの暗号化と署名に対応している並列システムをサポートするために、ほぼ 10 年かけて個別のソリューションが設計された。陳腐化した証明書発行メカニズムが原因で、個別のソリューションの複雑さがエンドユーザーに混乱を引き起こすことがしばしばある。社内の CA が新しいアクセスコントロールリストを発行し損なうことがあれば、エンドユーザーがネットワーク認証を行えなくなる。複数の理由で障害が起こり得る。ハードウェアであるセキュリティモジュールの障害、あるいは Windows サーバーの障害であることがある。「さまざまなことが起こり得ます」とセキュリティエンジニアは述べている。

「ネットワークをダウンさせてしまう可能性があるポイントまで進んでしまうのではないかと恐れています。もし PKI が利用できなくなったら、すべてのユーザーが、いくつかのアプリケーションを使えなくなったり、または認証できなくなったりして、IT チームは窮地に陥ります」と、セキュリティエンジニアは IDC に語っています。

現在、銀行は、PKI を最新のモバイルデバイス管理プラットフォームに統合している。この統合によって、マネージド PKI サービスを使いモニターされた単一のモバイルデバイススマートカードのアプリケーションに信用情報をストリーミングで提供している。これによって、モバイルデバイスユーザーと VPN ユーザーに対する複雑さが解消されている。「デバイス証明書発行プロセスの最新化とアクティブディレクトリとの整合性をさらに高めたスマートカードの使用から始めて、IT チームは冗長システムの数を徐々に減らしています」とセキュリティエンジニアは述べている。

マネージド PKI サービスへ舵を切ることで、IT チームの負担も軽減されるようになった。「すべてがオンプレミスのインフラストラクチャと我々が到達しようとしているセキュリティレベルによって、当行のスタッフではサポートできないほどの複雑さとオーバーヘッドが生じていました。巨大なチームを持つ大企業でない限り、PKI プログラムをあえて社内で管理することはないでしょう」とセキュリティエンジニアは述べている。

さらに、証明書発行をスマートカードに統合するために、社内の IT チームは PKI 専門家と共同作業している。電子メールのセキュリティを保つために、ばらばらのシステムも整理して、マネージドサービスに置き換える必要がある。銀行は、その Active Directory を管理して、認証局の管理と証明書発行のためのプロセスの統一を継続している。銀行のスマートカード管理プラットフォームが証明書管理と統合されたため、VPN アクセスにデジタル証明書が使用できる。マネージド PKI を採用することで、40 支店での証明書のライフサイクル管理が大幅に合理化され、IT チームをもう一つのタスクから解放して、別のプロジェクトに注力させる機会が生まれた。

デバイス ID と VPN アクセスをサポートし、重要資産を保護するためのゼロトラスト環境の実現に向けて PKI を選択するハイテク産業

電源管理ソリューションのプロバイダーは、マイクロソフトの Active Directory 証明書サービスに搭載されている機能をフル活用し、デバイス証明書とその PKI インフラストラクチャを使用し、管理されたデバイスの検証を義務付けることによって、その環境をロックダウンした。重要なリソースへの VPN アクセスをリクエストしてきたユーザーの真正性を確認する方法を確立し、管理対象デバイスのヘルスチェックを実施してからプライベートネットワークのリソースへのアクセスを認めること、つまり重要なリソースへのアクセスを厳重にロックダウンすることが目標であった。ハイテク企業は、セキュアなコネクティビティを確保し、またユーザーがそのロケーションとは無関係に企業のリソースへアクセスを得るプロセスを高速化したいと望んでいた。デジタル証明書を使用して、重要なリソースにアクセスするエンドポイントの完全な管理を要求することで、従業員をしっかりと管理する。また、デジタル証明書を使用して、必要に応じてアクセスを制限したりファイアウォール規則を適用したりできるユーザー認証証明書を発行して、契約者およびビジネスパートナーのアクセスを制限できる。

「当社の防御体制は、マイクロソフトのデバイスからの暗号鍵の抜き出しが極めて困難になるように構築されている」とハイテク企業の CISO が述べている。この CISO は、同社が「ゼロトラスト」環境に向けて段階的な投資を行っているとも語っていた。これを管理する課題は、エンジニア、マーケティングおよびその他の特別なユースケース向けにネットワークに Mac を展開することで、いっそう難しくなっている。この展開は現在進行中である。ハイテク企業は、PKI 専門家と共同して、Mac に認証証明書を導入し、プライベートキーを確実、安全に保管でき、エクスポートできないようにする方法を設計している。

企業への展開が続くにつれて、新しく発行した証明書にメタデータを追加しデバイスのフィンガープリンティングを可能にする。証明書は認証プロセスの一部として利用され、オンプレミス Web アクセス管理プラットフォームへの VPN 接続として利用される。ハイテク企業は、従業員が自分のモバイルデバイスから Office 365 を含むポータルや会社のその他のリソースにアクセスできるプラットフォームの柔軟性を好む。

ハイテク企業の主任セキュリティアーキテクトは、モバイルデバイス上での証明書ベースの認証に関して、「ハイテク企業があるデバイスの証明書を入手できたというのみで、そのデバイス上のすべてがその証明書とやり取りできるとは言えません。アプリケーションの開発者が、そのデバイスに関して一般的に使える証明書が利用できるように申請書を書かなかった場合、そのアプリケーションは決して使用されないでしょう」と注意を促している。アプリケーションは、証明書を持つデバイスから証明書を受領できない可能性がある。結果として、企業は、従業員が使用する社内およびサードパーティの双方が開発したアプリケーションをサポートするクラウド ID 向けに新しい戦略を策定している。

企業のモビリティ戦略と従業員のリモートアクセス要求に不可欠なデジタル証明書

グローバルな電子製品試験会社は、ユーザー証明書とデバイス証明書を合わせて使用して、会社支給および従業員所有のラップトップやモバイルデバイス上の機密リソースへのアクセスを認めている。CISO によれば、この結果、従業員の定着率が高まり、従業員が気持ちよく働ける自由度

が得られ、デジタル証明書を使い強力なセキュリティ体制を維持することにプライドを持った革新的なエンジニアリングチームが形成された。

「当社のビジネスパートナーのすべてが、モバイルデバイスを使い BYOD を管理するユーザーと同様に VPN 向けの証明書を持っているため、当社のさまざまなユースケースには、証明書が最善のコンポーネントであると判断しました」と CISO は語っている。

PKI に関して最も困難な作業は、信頼チェーンをインストールさせて、すべてのクライアントに行き渡らせることである。会社の開発チームとエンジニアリングチームも、会社のマーケティングとセールス部門も、相互運用の開発に興味を持っていなかったために、会社の PKI 環境の間にも相互運用性がない。会社の経営は PKI 環境ごとに別々のトラストチェーンに頼っているが、一元化されたアプローチを採用すれば、展開すべき信頼チェーンは一つになり、効率的で費用対効果も改善する。

強度の高いセキュリティを維持するための会社の取り組みの一環として、モバイルと VPN アクセス向けの PKI 環境は、マイクロソフト側の証明書プロファイル向けに、ほとんど全面的にカスタマイズされている。重要なリソースへのアクセスを得るように作られた証明書の盗難やブルートフォース攻撃のリスクを減らすために、同社はカスタム化した証明書を開発した。ログインしたユーザーには、証明書を求めるプロンプトではなく、パスワードを求めるプロンプトのみが示されるが、これによって証明書は個人ユーザーにのみ有効とされる。これは、証明書とパスワードが決して一緒に使われないことを保証する一対一の関係である。「私からすれば、これは証明書の展開に不可欠なセキュリティコンポーネントです」と CISO が述べている。

PKI を使い数千の POS 端末を保護するペイメントプロセッサー

暗号化、認証および承認をサポートするために、またデバイスファームウェア、オペレーティングシステムおよびアプリケーションの完全性を検証するために、IoT デバイスにハードウェアベースおよびソフトウェアベースのセキュリティメカニズムを追加するという、大きなプレッシャーにメーカーはさらされている。デジタル証明書は、組み込みシステムのセキュリティの基本的なレベルを達成するために使われるトラストアンカー（認証の起点）である。

欧州のペイメントプロセッサーは、マネージド PKI サービスを利用して数万の POS システム端末を保護している。この PKI サービスによって、ネットワークへデバイスの認証が可能となる。この認証は、信頼の置けるサードパーティの相互認証である。ペイメントプロセッサーが開発した新しいアプローチでは、デバイス ID 向けのデジタル証明書のインストールおよびペイメントプロセッサーのクラウドベースプラットフォームと通信できるデバイスエージェントが必要である。POS システムのプロビジョニング、モニタリングおよびメンテナンスに、また証明書のローテーションを行うセキュアなメカニズムの確立に、このプラットフォームが使用される。

デジタル証明書の使用によって製造者レベルでの不正行為が減少し、会社はデバイス使用の監視がさらに容易になったと KPI 実装を監視するセキュリティアーキテクトが述べている。「ライフサイクル全体を通して、証明書を管理できるので PKI を選択しました」とセキュリティアーキテクトは語っている。セキュリティアーキテクトは、「不正なデジタル証明書を使用した攻撃者が、ハイジャックできないソリューションを確立することが、主な要求でした」と言う。開発されたメカニズムによって、転送中のデータでも、転送中ではないデータでも、セキュアであることが保証される。また、情報を送受信するエンティティが本人であることが確認される。

このソリューションは、POS システムのデバイスのプロビジョニングおよび信用情報管理の監視を続けること以外にも、プロバイダーのポリシー駆動型の暗号化サービスの販売を可能にし、販売者がコンプライアンスの責任を果たしていることを保証する。

プロバイダーが使用しているその他の高リスクデバイスは、エージェントアプローチに対応していない。ペイメントプロセッサーなどを使い作業する組み込みシステム製造業者は、エージェントまたはクライアントのソフトウェアをサポートするスペースもパワーもない製品を出荷する。

PKI がコンピューター同士のセキュアな通信とコードサイニングに対応するように製造されている場合は、エンジニアリングチームはその PKI を使用したと、製造業者が IDC に述べていた。エンジニアリングチームと共同作業を行ったセキュリティチームのリーダーは、「当社の顧客は、我々が顧客に出荷するすべてのコードの完全性を保証する方法の確立を要望されていました」と述べている。PKI ソリューションを製造業者に既存の PKI 環境に組み込むのではなく、マネージド PKI ソリューションを選択することが目標であった。

「社内のプロセスに注力しているチームに負担を掛けずに、プロセスを自動化する方法を探していました」とリーダーが述べている。

DigiCert の導入検討

DigiCert は、ハイアシュアランス（企業認証および EV 認証）デジタル証明書のプロバイダーである。この証明書は SSL/TLS および PKI の単純化、さらには、Web と IoT で使用される ID とその認証および暗号化の各ソリューションの単純化を目指している。DigiCert は、フレキシブルな証明書プロファイル構成の自動作成、登録方法、および電子メールセキュリティをサポートするセキュアキーエスクローを使ったリカバリーに対応している。証明書は、電子メールのコンテンツの完全性の検証、メッセージのプライバシー確保、および極めて重要なメッセージの作成者証明に使用される。証明書はしばしば、ビジネスの成長と継続に不可欠な法的文書、契約書および請求書の完全性を維持するデジタル署名を裏付けるためにも使われる。

DigiCert のプラットフォームは、IT 管理者に集中管理フレームワークを提供している。このフレームワークは、いつ、どこからのアクセスであれ、作業に対するセキュアなアクセスをサポートしている。プラットフォームは、従業員のアプリケーションや Web サイトへの認証に広範に使用されており、カスタム証明書プロファイルと登録メカニズムを構築する柔軟性を企業に提供している。これは、高速かつ大規模に VPN とネットワーク接続とモビリティのセキュリティをサポートするためのメカニズムである。さらに、モバイル電子メール、アプリケーション、関連データを含めて、モバイルデバイス環境の全体を保護するために使用される。これによって、IT 管理者は、エンタープライズサービスへのアクセスを最終的にコントロールし、プライバシーコントロールをモニターし、アプリケーションの制限を管理するために、登録と証明書発行を自動化できる。DigiCert の PKI プラットフォームは、IoT をサポートして、企業が接続されているデバイスを大規模にプロビジョニングし、クラウド PKI サービスを経由した証明書管理を可能にする。これによって、秘密鍵（certificate key）にセキュアな保存と管理が提供される。

課題／機会

企業は、社内の既存の PKI インフラストラクチャへの投資を長期に渡り続けてきた。IDC がインタビューを行ったセキュリティの専門家は、自分たちが維持しようとしている PKI エコシステムは複雑で断片化していることが多く、その合理化と自動化のプロセスは、多面的であり、複数年を要する骨の折れる取り組みであると語っていた。この取り組みには、初期投資と PKI 専門家が必要であり、この専門家は、既存のビジネスプロセスと IT インフラストラクチャ、重要なリソースのロケーション、リスクに対する経営陣の許容度および経営陣の成長戦略を熟知している必要がある。急速な成長、合併と買収、新しいテクノロジーの採用、ビジネス戦略の変更およびその他の外的要因は、改善プロジェクトの計画が不十分であるか、体系的に実行されない場合は、プロジェクトに大きな影響が及び、失敗につながることもあり得る。

結論

クラウドの採用が継続的に拡大し、ハイブリッドおよびマルチクラウド環境全体で企業データや他のリソースへのアクセスを管理する企業が増えることを考慮すると、PKI テクノロジーには、取引の完全性を立証し、人とシステムの間にセキュアで信頼できるコネクションを確立する上で、より大きな役割を果たすようになるであろう。IDC のユーザー調査「Data Services for Hybrid Cloud Survey」のデータはこれを裏付けている。2010 年当時は、従業員が 1 万人を超える企業の 32%が、自社のセキュリティプログラムの一部に PKI を使用していると述べるにとどまった。2018 年には、大企業の 65%が、適用可能なすべてのデータストアとリソース全体に渡り、広範囲

に、あるいは全面的に、堅牢な PKI を実装していると回答した。なぜ PKI が重要性を高めたかを示唆する主な所見を次に示す。

- **スケーラビリティ：**この調査で、インタビューを受けた企業は PKI を大規模に活用しており、ユーザー基盤のサイズ、ドメイン数および認証リクエスト量に関するデータを提供してくれた。これらの IT 企業は、スケーリングに関する非常に多数の要求に対処している。調査に回答した企業の規模は、従業員数 1,000 人から 12 万人に渡り、調査対象となった全企業が業績と会社の成長力に満足しており、モバイル、リモートアクセス、セキュアな無線接続、ドキュメントサイニング、暗号化、セキュアな電子メールなどに関連した今後のニーズに対して、PKI テクノロジーを利用して成長し続けられるであろうと自信を持っていた。
- **マネージド PKI サービス：**既存の問題や懸念は、PKI テクノロジーを複数実装することで複雑さが増えることと、この複雑さを管理する熟練したネットワークエンジニアやセキュリティエンジニアが不足することに関連していた。この問題や懸念は、既存の人員を補強するために、また新入社員の登録や証明書の発行や取り消しのような一般的な PKI 作業の自動化がもたらす混乱を最小限に抑えるために、マネージド PKI サービスの採用を促している。
- **攻撃の巧妙化：**インタビューを受けた企業は、稼働している PKI について「壊れていないのであれば、PKI には触れたくない」と IT チームからはしばしば要請されると報告している。しかし、複雑さが増し、プロアクティブな監視が不十分であると、脆弱性および構成に関わる問題が生じて攻撃者に付け込まれる。構成の弱点に乗じた攻撃者は、特定の従業員を監視に置くために中間者（MITM）攻撃を仕掛け、さらに金銭を目的に機密データを盗む可能性が高い。

この IDC の調査から、さまざまなビジネスとユースケースに関して DX イニシアティブを確実に進める上で、PKI が必須であることが明らかになった。今日のビジネスプロセスは、PKI に支えられて自動化を促進でき、摩擦を減らし、デジタル情報と電子商取引のプロセスを合理化できる。PKI は、データプライバシーとデータセキュリティに関する新しい規制に直面しているセキュリティチームも利用すべき必須の要素である。PKI 環境を整理すると複雑さが緩和され、マネージド PKI サービスを採用すると管理のオーバーヘッドとコストも削減でき、セキュリティチームはその他の逼迫した事案に取り組めると、CISO は述べている。さらに、デジタル証明書は、標的型攻撃を阻止でき、機密性の高いトランザクションの完全性を確保できることがこの調査で検証された。また、ビジネス取引の当事者が、間違いなくその本人であることも、デジタル証明書で検証される。さらに重要なことは、PKI は、顧客が自宅で快適、安全に機密データを扱えるために、顧客満足度の改善に向けた新たなビジネスプロジェクトのイネーブラーともなり得ることが、この調査で明らかになった。

IDC 社 概要

International Data Corporation（IDC）は、IT および通信分野に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です。50 年にわたり、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。

現在、110 か国以上を対象として、1,100 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査・分析および市場予測を行っています。

IDC は世界をリードするテクノロジーメディア（出版）、調査会社、イベントを擁する IDG（インターナショナル・データ・グループ）の系列会社です。

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2019 IDC. Reproduction without written permission is completely forbidden.