White Paper

IoT デバイスのセキュリティリスクによって、製造業で生産中に証明書のプロビジョニングを行う PKI セキュリティの採用が促進される

Sponsored by: DigiCert

Robyn Westervelt
July 2020

エグゼクティブサマリー

IoT（Internet of Things）は大きな価値をもたらしているが、ユーザーに豊富なデータやサービスを提供する IoT デバイスの急激な普及によって新たなリスクも生まれている。攻撃者は、デバイスのセキュリティ脆弱性や、導入、設定、管理の不適切さに付け込む。RFID、Bluetooth、および NFC の通信をひそかに傍受する簡単な方法が広範囲に渡って利用できる。また、製造上の欠陥を伝える報道も多い。たとえば、誤ってマルウェアを埋め込んだまま出荷されたデジタルフォトフレーム、データの暗号化をサポートする電子部品の設定が不適切な状態で出荷されたスマートロックなど。IDC の調査では、セキュリティの問題が IoT デバイスの購入者の最大の懸念事項であることが明らかになっている。セキュリティに敏感な購入者は、データの機密性、完全性、可用性、およびデバイスへのコンポーネントの適切な実装に関して妥協せざるを得ないことが、そうしたデバイスの使用シナリオにも影響する可能性を認識している。

本調査レポートでは、製造過程で証明書を発行するために PKI（Public Key Infrastructure：公開鍵基盤）管理プラットフォームを利用することを検討しているデバイス製造業者に向けたガイダンスを提供する。本調査レポートの要点は以下の通りである。

- デバイス製造業者は、ネットワークに接続される各 IoT デバイスに関するベースライン情報の監視、保護、および維持を支援するメカニズムの実装について、顧客や規制当局からいっそうの責任を果たすように求められている。
- IoT デバイスの購入者が求めるデータの完全性のレベルを実現するに当たって、製造業者は、暗号化と認証をサポートし、デバイスのファームウェア、オペレーティングシステム、およびアプリケーションの信頼性を保証するために、PKI の採用が必要である。
- デジタル証明書は、IoT デバイスから送信されるデータを効率的に保護してハードウェア、ファームウェア、およびソフトウェアの IP（Intellectual Property：知的財産）を守り、デバイスを不正に複製することを防ぎ、現場でファームウェアをアップデートする安全な方法を提供できる。
- セキュリティを強化しつつコストを予算内で収めるには、IoT 製品を設計する段階など、できるだけ早くセキュリティに関して計画を立て採用すべきであることが、多くの研究によって指摘されている。

製造業者はセキュリティに関する購入者の懸念を払拭しなければならない。その一環として、強力なソフトウェア開発とエンジニアリングの実践、PKI をサポートするための製品の調整、および出荷前の徹底的なコードレビュー、などを通じた「セキュリティの作り込み」が必要であることを意味している。製造時に適用されるデジタル証明書は、デバイス ID を確立する上での最初のトラストアンカー（信頼の起点）になる。

概況

IDC の調査では、デジタルトランスフォーメーション（DX）への投資によって、企業は 40%もの生産性の向上を実現できることが分かっている。製造業者は IoT デバイスの生産者であるだけでなく購入者でもあることが多い。多くの場合、製造業者は機器やプロセスに関する多くの知見を得るために、生産に最新のスマートセンサーコンポーネントを導入している。調達の観点から、製造業者はスマートセンサーの機密性、セキュリティ、および完全性の詳細な調査を行う。これらの IoT デバイスから収集されるデータは、製造業者が予防的なメンテナンスを行い、コストのかかるダウンタイムを削減するのに役立つ。さらに、ビジネス上の意思決定を下し、新たな製品やサービスを生み出すために分析される。

同様の詳細な調査は、無線接続のコンポーネントとデータ収集用のセンサーを搭載した最新デバイスの購入者によっても行われる。これらの IoT デバイスが安全な接続とデータ保護を適切なレベルでサポートしている場合、購入者は仮想イベントや物理イベントを効果的に作成および使用し対応することが可能な、相互接続された物理的／操作環境および仮想環境との結合レベルを達成できる。これはロボティクスなどのインテリジェントな運用システムをサポートすることによって運用上の回復力（耐障害性）をもたらすが、IoT デバイスの高レベルのデータの完全性が条件となる。このレベルのデータ完全性を実現するため、これらの IoT デバイスの製造業者は、暗号化、認証、およびデバイスのファームウェア、オペレーティングシステム、アプリケーションの完全性のために PKI をサポートするよう、多くの製品を調整する必要もある。

データの急増によって、より強力なデバイスセキュリティメカニズムへの関心が非常に高まっている。データの収集と送信を行う IoT デバイスの数は飛躍的に増加すると予測されており、その要因の一つは高度にスケーラブルな 5G 無線接続の将来性である。デバイスが導入されると、重要な要件としてセキュリティの問題が急浮上する。IDC の 2019 年のユーザー調査「*Global IoT Decision-Maker Survey*」では、IoT デバイスの製造業者やサービスプロバイダーに求める専門知識の分野として、セキュリティは第 1 位であり回答者の 40%以上を占める。セキュリティの次に多いのはデータプライバシーおよびソリューションパフォーマンスが続いており、これらの要求はいっそう高まる傾向にある。IDC は、インターネットまたはネットワーク対応デバイスが 2025 年までに少なくとも 559 億台に達し、2023 年にはコネクテッド IoT デバイスがその約 72%（352 億台）を占め、2025 年には 75%（416 億台）まで増加すると推定している。IDC の調査レポート『*Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023*（IDC #US45066919、2019 年 5 月発行）』では、それらの新たなコネクテッド IoT デバイスによって 80ZB 近くのデータが生み出されると予測している。そのデータの大部分はビデオ監視（監視カメラ）アプリケーションから生じるものであるが、産業ソースや医療ソースなどの他のカテゴリーから生じるデータも時間と共に増加するであろう。

企業は IoT デバイスに組み込まれたセキュリティを求めている

IoT デバイスの製造業者は、厳格化する購入者のセキュリティ要件を満たす製品を生産するための運用継続性とデジタル的に安全な環境を実現するセキュリティ戦略を維持しなければならない。たとえば、ネットワーク接続型の冷却ユニットの製造業者は、外的攻撃からコンポーネントを守る必要性の高まりに対応している。ネットワーク接続型の冷却ユニットで医薬品やワクチンを一定の温度に保たなければならない病院では、人命を守るために暗号化、認証、およびデバイス完全性のための PKI の必要性が最優先される。

サイバー攻撃を防ぐために常にプレッシャーにさらされている最高セキュリティ責任者は、セキュリティに関する強力なベストプラクティスを実証する IoT デバイスの製造業者を求めるようになっている。IDC の 2019 年のユーザー調査「Global IoT Decision-Maker Survey」では、IoT サプライヤーの選択基準についての質問に対する回答は「実績のあるセキュリティ能力」が圧倒的な 1 位となり、その次に「ソリューションコスト」と「統合」が続いた。このセキュリティの重視を促した要因の一つは、デジタルビデオレコーダーや Web カメラをターゲットにして大規模な DoS（denial-of-service）攻撃を行うことで有名な Mirai ボットネットであった。攻撃者は、横行する認

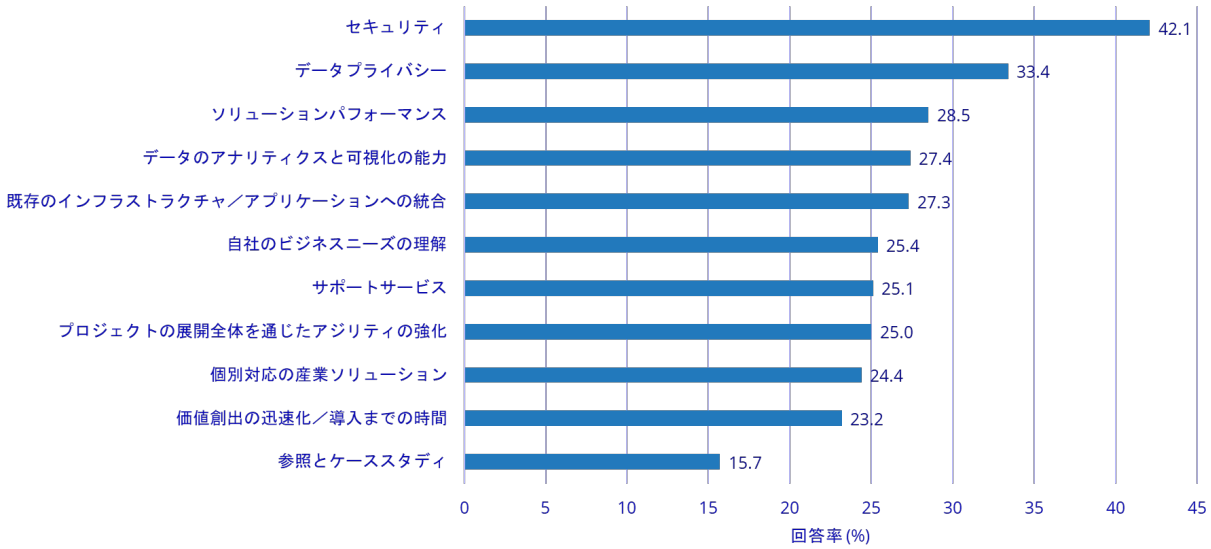
証情報の再利用や増え続ける未パッチ（セキュリティパッチへの未対応）の脆弱性に付け込んでいる。2019 年には、複数のレポートによって、ICS（Industrial Control System：産業用制御システム）やオペレーショナルテクノロジー（OT）インフラストラクチャに対する攻撃が著しく増加したことが立証された。セキュリティ研究者たちは 2020 年の初めに、攻撃者が極秘データを入手したりデバイスをクラッシュさせたりするためにリモートで操作する可能性があるとして、汎用ルーター、スイッチ、IP 電話、および IP カメラの幅広い脆弱性について警告した。

IDC の 2019 年のユーザー調査「Global IoT Decision-Maker Survey」では、既存の IoT ベンダーとサービスプロバイダーに改善してほしい専門知識の種類についての質問したところ、セキュリティ（42.1%）とデータプライバシー（33.4%）が回答の上位を占めた（Figure 1 を参照）。

FIGURE 1

望まれる IoT ソリューションプロバイダーの改善

Q.　既存の IoT ベンダー／サービスプロバイダーに改善してほしい専門知識の種類はどれですか？



Note: 集計対象は、従業員が 100 人を超えるグローバル組織を代表する 4,480 人の企業の意思決定者

Source: IDC's Global IoT Decision-Maker Survey, 2019

製造業者は費用効果の高いセキュリティ投資を行う必要がある

製造業者には、シリコンベースのセキュリティコンポーネントなど、費用効果の高い多様なセキュリティコントロールを見つけて使用するよう圧力がかけられている。これらのコンポーネントは物理攻撃やサイバー攻撃のリスクを大きく削減でき、製造業者がレガシーのソリューションや安全性に欠けるソリューションに対する競争優位を手に入れるのに役立つ。コストを抑え、かつ、セキュリティを強化するには、IoT 製品の設計フェーズなど、できるだけ早い段階でセキュリティに関する計画を立て採用を進める必要があることが、多くの研究によって指摘されている。

これらの問題にデバイスレベルで対処するため、製造業者は製品の設計および開発サービスに投資している。これらの投資は、セキュリティ設計者や最高情報セキュリティ責任者からの、新しいハードウェアおよびソフトウェアベースのセキュリティコンポーネントの要求に応えるものである。

IoTデバイスのコネクテッド化が進む中で、製造業者はデバイスのリスクに対応する際に以下のような主要課題に直面している。

- **デバイスの認証**：多くのデバイスは、他のシステムやユーザーに接続する前に安全な方法でデバイスIDを識別して検証するコンポーネントを搭載していない。そのため可視性に欠け、接続したリソースの監視が不十分となり、データの損失や窃盗につながる恐れがある。証明書は、IDの確認や特定のリソースへの接続の許可に使用できる。
- **データとシステムの完全性**：製品エンジニアリングチームは、認証および認可要件をサポートするため、生産時に強力なデバイスIDを組み込むことによって偽造デバイスを根絶するまたは大幅に減らすよう努めている。証明書は、ブート時のデバイスファームウェアの完全性の確認や、適用前のソフトウェアアップデートの信頼性の検証においても重要な役割を果たす。
- **データの暗号化**：デバイスが認証された場合、そのデバイスには安全な接続をサポートするメカニズムが搭載されているはずである。証明書には送信時にデータが保護されていることを保証する役割がある。攻撃者による誤った情報でのシステムのなりすましや通信の傍受を防ぐために、暗号化の適切な実装と設定を行う必要がある。

証明書のプロビジョニング：PKIプラットフォームは柔軟性を持ち、複雑性に対応する必要がある

NIST（National Institute of Standards and Technology：アメリカ国立標準技術研究所）のサイバーセキュリティフレームワークは、企業のセキュリティチームが組織内にある物理的なデバイスやシステムの一覧表を入手し、デバイスを認可するためのIDと認証情報の発行、管理、確認、取り消し、および監査を行うメカニズムを整備することを推奨している。この推奨に注意を払う組織は、デジタル証明書を使用してIoTエッジデバイスの完全な状況認識を維持している。

製造業者は、企業がこの重要な推奨事項を実行できるようにする立場にある。IoTに特化したPKIプラットフォームは、デバイス製造業者がPKIを使用してそのライフサイクル全体を通じてIoTデバイスのセキュリティを高められるよう設計されている。さらにこれらのプラットフォームは、その寿命全体を通じたデバイスIDとしての単純なラベルの使用や、パスワードや暗号化キーをハードコーディングして、誤ったセキュリティ感覚を提供するなどの長く続けられてきた疑わしいセキュリティ慣習を排除することもできる。

これらのIoT PKIプラットフォームは、複雑性を低減し、製造業者が認証、暗号化、および完全性に使用される証明書を提供するためにPKIを使用してデバイスの信頼の基点（Root of Trust）を確立できるよう設計されている。これらは、権限を与えられたユーザー、メッセージ、またはサーバーのみがデバイスにアクセスできるようにするためのIDの認証と確認においてデジタルの認証情報が重要な役割を果たすPKIの必須要素である。PKIはまた、無線によるソフトウェアアップデートが正当なものであり改竄がないことを、IoTデバイスに適用する前に確認するメカニズムとして有効である。PKIプラットフォーム製品は少なくとも、多くのデバイスに対して大規模に証明書の動的な作成とプロビジョニングを行う能力と、漏洩のない秘密鍵の作成および配布をサポートしている必要がある。

PKIプラットフォームはまた、サプライチェーンを強化し、組立工程における証明書のプロビジョニングを簡素化する必要もある。製造業者は、インターネットの接続性が悪いために生産時に接続が切れるリスクを排除するために、PKIプラットフォームプロバイダーのクラウドを利用するか、プロバイダーのローカルのCA（Certificate Authority：認証局）サービスを統合するかを選択できる。データレジデンシー要件や各国の規制、およびエアギャップ環境によって、PKIプラットフォームをオンプレミスで導入することが求められる場合もある。

デジサートの PKI ソリューションとサービス

デジサートは、ID と暗号化に関するスケーラブルな TLS/SSL、IoT、および PKI ソリューションのプロバイダーである。PKI 管理をモダナイズするデジサートのアプローチである DigiCert ONE は、迅速かつ柔軟な PKI の導入をサポートする。最新のソフトウェア設計とエンジニアリングに基づき、DigiCert ONE は多様な導入モデルや PKI ユースケースにおいてエンドツーエンドの一元化されたユーザーおよびデバイスの証明書管理を実現する。

デバイス ID、認証、暗号化、および完全性の管理に特化したデジサートの IoT Device Manager は、DigiCert ONE のコンテナベースのアーキテクチャに基づいて構築されている。

デジサートの IoT Device Manager は、クラウドまたはオンプレミスの PKI サービスを介して、大規模なコネクテッドデバイスへの証明書のプロビジョニングと管理を簡素化する。デジサートは、柔軟な証明書プロファイルの設定および登録方法の自動作成をサポートしている。さらにデジサートの IoT Device Manager は、IT 管理者に場所や時間を問わずに IoT デバイスを管理するための安全なアクセスを可能にする一元化された管理フレームワークを提供する。このソリューションは、他のデバイス、サービス、およびクラウドアプリケーションに対してデバイスを認証するために幅広く使用されており、組織に対し、スピードとスケールの両方において PKI の使用に関する柔軟性をもたらす。またこのソリューションは、コネクテッドデバイスをアプリケーションや関連データと共に保護するためにも使用され、管理者が登録や証明書の発行を自動化し、最終的にはサービスへのアクセスの制御、プライバシーコントロールの監視、およびアプリケーション制限の管理を可能にする。

機会、課題、および PKI ソリューションを使用する製造業者への IDC の提言

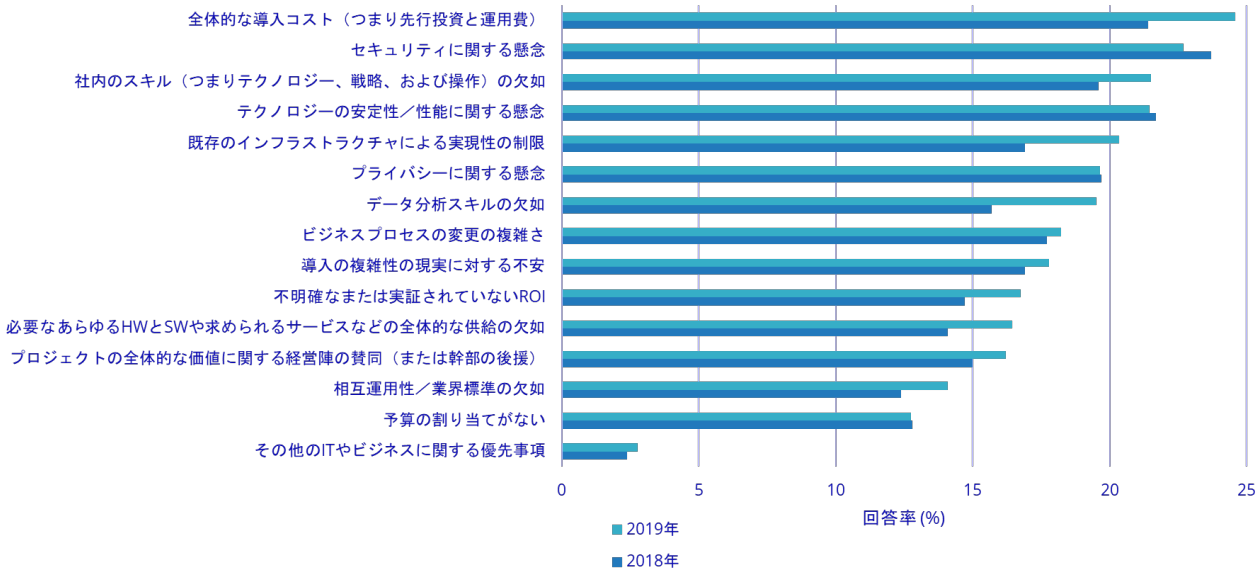
すべての製造業者に、その業務や環境に特化した独自のセキュリティ要件や安全要件がある。デジサートやその他の認証局は、特定の製造業者のニーズに沿った証明書管理サービスに関する専門知識を保有していることを明確に示す必要がある。製造業者は、PKI プロバイダーを評価するに当たって、業務の遂行に必要なシステム性能とサポート力はもちろん、業界の求める要件をそのプロバイダーがどこまで熟知しているかを含めて検討しなければならない。

セキュリティは IoT において最も大きく成長している分野である。Figure 2 に示すように、IDC の 2019 年のユーザー調査「Global IoT Decision-Maker Survey」では、組織内の IoT プロジェクトの進捗を阻害または鈍化させる上位課題において、セキュリティに関する懸念が第 2 位となった。

FIGURE 2

IoT プロジェクトの上位課題

Q.　貴社内の IoT プロジェクトの進捗を阻害または鈍化させる課題の上位 3 つは何であると考えますか？（最大で 3 つまで選択してください）



Note: 集計対象は、従業員が 100 人を超えるグローバル組織を代表する 3,828 人（2018 年）、4,480 人（2019 年）の企業の意思決定者

Source: IDC's Global IoT Decision-Maker Survey, 2018 and 2019

デバイスの購入者は、その製造業者に、セキュリティのベストプラクティスを確立させ、プロセスにセキュリティを組み込むことを余儀なくさせている。これらの懸念に対応するために、最新アプローチの設計プロセスでは、製造業者が維持しようとしている複雑かつ細分化の傾向にある PKI エコシステムを整理し自動化するため、オンプレミスで稼働するインフラストラクチャが必要になる場合がある。これは多方面からの複数年に渡る取り組みになる。製造業者は、デジサートやその競合他社の、できる限り負担の少ない形で PKI 戦略の設計を支援する能力を査定する必要がある。どの戦略も、結果的にはオンプレミスのインフラストラクチャとクラウドベースまたはリモートのインフラストラクチャからなるハイブリッドの PKI エコシステムの管理の必要性が浮上する。この作業には、先行投資と既存のビジネスプロセスや IT インフラストラクチャを熟知している PKI 専門家、重要なリソースの保管場所、および経営陣による既存リスク許容度と成長戦略が必要となる。

改善プロジェクトが、十分に練り上げられ計画的に実行されていない場合、急成長、合併や買収、新たなテクノロジーの導入、ビジネス戦略の変更、およびその他の外部要因によってそのプロジェクトが大きな影響を受け、頓挫することもあり得る。

IDC の提言

IoT デバイスへのセキュリティの組み込みは製造業者に競争優位をもたらすが、信頼される IoT デバイスには、製造時やデバイスのプロビジョニング時のデバイス ID の発行をサポートするセキュリティコンポーネントが必要である。安全な Network of Things エコシステムを構築するための認証および認可要件のサポートはタイミングが重要である。製造業者は、顧客やビジネスパートナーとの信頼関係を築くことによって、セキュリティへのコミットメントを実証しなければならない。この取り組みは、強力なソフトウェア開発工程と出荷前の詳細なコードレビューを通じた

「セキュリティの作り込み」と、デバイス ID をサポートする PKI やデジタル証明書を製造現場やデバイスの組立の過程で組み込むことから始まる。

製造業者はセキュリティを強化するために以下のアクションアイテムを検討すべきである。

- **将来のための投資**：セキュリティ要件への対応には、攻撃者にとっての障壁のレベルを引き上げる費用対効果の高い対策の実装も必要である。
- **設計によるセキュリティの確立**：いくつかの IoT デバイス製造業者は、IT ソフトウェアメーカーが数年前に学んだ「製品が市場に出た後にセキュリティコントロールを強化することはコストがかかる」という厳しい教訓を得ることになる。IoT デバイス製造業者は PKI をデバイスの設計に組み込むべきである。それによって購入者が求めるセキュリティとプライバシーに対するコミットメントが実証される。
- **ソフトウェアの脆弱性の保護**：製造業者は、生産しているデバイスに脆弱性がなく、狙い通りに機能するという一定の信頼度を提供しなければならない。新たな脆弱性や脅威が発見された場合、PKI は、デバイスのファームウェアやソフトウェアのアップデートの完全性の検証が求められる。

結論

IDC がインタビューを行った組み込みシステムの専門家は、今こそ製造業者がデバイス ID、認証、データの暗号化、および安全な接続に関するプロセスと設計の課題に対処するときであると考えている。IDC はこの見解を支持する。データのセキュリティとプライバシーは、顧客、ビジネスパートナー、および従業員と長期に渡る信頼関係を築くことを目指している企業にとって最も重要である。

最大の競争優位性を手にしている IoT デバイスの製造業者は、セキュリティへのコミットメントを実証することによって顧客との信頼関係を築いた面がある。進行中の IoT の取り組みについて 4,480 人の IoT 意思決定者を調査した IDC の 2019 年のユーザー調査「Global IoT Decision-Maker Survey」では、セキュリティを強化した製品はデバイスの選定基準の上位要素の一つである。IoT デバイスを組み込むプロジェクトに従事している回答者は、ベンダーが業界に関する深い専門知識を持つことを実証し、強力なセキュリティをサポートするベストオブブリードのデータ管理機能をもたらすことを期待している。

製造業者は、長期間使われ続けてきた PKI を始めとする実証済みのセキュリティのベストプラクティスをサポートするコンポーネントを利用して、安全な接続の基盤を築かなければならない。製造業者は、安全な接続基盤の構築を支援できる経験豊富な専門家とサポートリソースを有するスペシャリストを見つけるため、PKI ツールのプロバイダーを査定する必要がある。

製造時に適用されるデジタル証明書は、デバイス ID を立証する最初のトラストアンカー（信頼の起点）になる。デバイス製造業者は、ネットワークに接続される各 IoT デバイスに関するベースライン情報の監視、保護、および維持を支援するメカニズムの実装について、顧客や規制当局からますます責任を問われている。PKI は、IoT デバイスのベースラインレベルのセキュリティを可能にする主要な要素を備えている。PKI は暗号化と認証をサポートし、デバイスの所有者によるデバイスのファームウェア、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と信頼性の検証を可能にする。

スポンサーからのメッセージ

デジサートは、ID と暗号化に関するスケーラブルな TLS/SSL、IoT、および PKI ソリューションの大手プロバイダーです。Fortune 500 の 89%、グローバル銀行の上位 100 行のうちの 97 行を含む最も革新的な企業が、Web サーバー、エンタープライズ、および IoT デバイスの ID と暗号化に関する専門家としてデジサートを選択しています。当社はそのエンタープライズレベルの証明書管理プラットフォーム、迅速で見識のある顧客サポート、および市場をリードするセキュリティソリューションが広く認められています。デジサートの最新のニュースやアップデートについては、digicert.com をご覧になるか、@digicert をフォローしてください。

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