

# DigiCert® IoT Device Manager

## 3つの共通課題

私たちは、業種や企業の規模に関係なくIoTのエコシステムを安全に開発する際に、3つの共通課題に直面します。

### 1. IDのないIoT

安全のレベルは、接続されている最も脆弱なデバイスに依存します。また、その状態でより多くのデバイスをさらに接続すると脆弱性が潜在化し修復が困難になります。

安全なIoT環境を構築するためにまず必要となるのは、各製造工程ですべてのデバイスを識別、監視、管理するシンプルなID管理ツールです。

### 2. 手に負えない複雑さ

多くのIT基盤は新たな要求や課題が発生したときににその場しのぎで異なるアプリケーション、ベンダー、サービスを採用してきた結果、非常に複雑になっています。

複雑さが増すにつれてIT管理者は、IT基盤全体の安全性管理よりも複雑になったテクノロジーの監視に多くの時間を割くことになります。

本当必要なのは、工程の最初から最後まで一貫した統合ソリューションです。

### 3. スケーラビリティに欠けるセキュリティ

世界中でIoTデバイスは数十億を数え、モノを接続するための新しいアイデアが毎日飛躍的に増加しています。しかし、まったく同じIoTの実装は2つとないため、事態は複雑になるだけで、規制やセキュリティ要件が絶えず変化しています。

そこで必要になるのは、ニーズを満たすPKIサービスを迅速に導入するためのフレキシブルなソリューションとデバイスの数と種類の増加に対応できるプラットフォームです。

## 唯一の卓越した方法

DigiCert IoT Device Managerは、個別のニーズに合わせて設計された最新のPKI PlatformであるDigiCert One上に構築され、最新のIoT環境の厳しい要求に応えます。

## メリット

### 完全なID管理

製造工程の任意の工程で（半導体製造から製品へ実装まで）量を問わず、デバイスにIDを割り当てて管理します。デバイスに発行された証明書全体を可視化して運用することができます。

### セキュリティと管理の簡素化

検出、レポート、動的証明書作成、失効、ユーザーアクセス、その他を管理します。あらゆるニーズ（ペースメーカーのような小さなデバイスから民間航空機のような大きなモノまで）に合わせて証明書プロファイルのカスタマイズすることやプロビジョニングすることができます。

さらに、バックアップ、更新、負荷分散を自動化することで、スピードやシンプルさを犠牲にすることなく、最適化されたパフォーマンスを得られます。これらすべてを最新で使いやすいインターフェイスで実現します。

### スピードと柔軟性

IoT向けに構築されたプラットフォームを使用して、短時間でセットアップと実装を行えます。自動化された中間証明書の生成、柔軟な証明書プロファイルやテンプレートなど充実したアカウントオプション、そして実装が容易な様々なプロトコルオプションが、IoT Device Managerの立ち上げを迅速にしカスタマイズを容易にします。それぞれのニーズに最適な実装オプションを選択することができます。DigiCertによるクラウドサービス、お客様環境によるオンプレミス、お客様がご契約のクラウド環境のどこでも選択が可能です。

## 主な機能

- デバイス証明書について、作成、登録からプロビジョニング、更新、失効までライフサイクル全体を管理
- あらゆるIoT環境のニーズを満たすための証明書プロファイルのカスタマイズ機能
- 認証局証明書生成機能
- あらゆる工程での証明書プロビジョニング（半導体製造から製品への実装まで）
- デバイスIDのプロビジョンと追跡
- 安全なデバイス証明書更新
- コンテナ化アーキテクチャによる固有のプロセスとコンプライアンスのニーズに合わせた構成
- 証明書ステータス、デバイスアイデンティティ、その他のメタデータに関するレポートの生成
- ポリシーコンプライアンスを確認するための監査ログの生成

## 技術仕様

- 証明書管理プロトコル（REST API、SCEP、CMPv2、ESTなど）
- HSMサポート
  - SafeNet Luna Network HSM
  - SafeNet Luna G5
- サポートされる標準
  - OCSPおよびCRL証明書ステータス
  - PKCS#10証明書申請（CSR）
  - PKCS#12、PEM、PKCS#7証明書フォーマット
- 3GPP、LTE/4G/5G対応のサービス
- HTTP転送プロトコルによる通信

## DigiCertについて

より良い方法も、誰かが見つけなければ、一般的な方法にはなりません。

DigiCertは設立以来、インターネットを守るより良い方法をひたすら追求してきました。その結果、DigiCertのSSLサーバ証明書は、Fortune 500の89%、グローバルバンクトップ100のうち97、グローバルeコマースの81%の企業で毎日数百万の信頼を得ています。これが、業界のサービスとサポートのレビューでDigiCertが一貫して最も多くお客様から5つ星をいただいている理由です。企業と政府のアイデンティティ、アクセス、サーバ、ネットワーク、Eメール、コード、署名、ドキュメント、およびIoTデバイスの保護を支援するためにDigiCert ONEプラットフォームと管理ツールを構築し、PKIを最新化した理由はここにあります。SSL、IoT、PKI、その他でもDigiCertは共通項におさまりません。

詳細については、<https://www.digicert.com/jp/>をご覧ください。

© 2020 DigiCert, Inc. All rights reserved. DigiCert、DigiCertのロゴ、およびCertCentralはDigiCert, Inc.の登録商標です。Nortonおよびそのチェックマークのロゴはライセンスに基づいて使用されるNortonLifeLock Inc.の商標です。その他の名前は、それぞれの所有者の商標である可能性があります。

digicert®