# IoT (モノのインターネット) のための信頼のルート

digicert®

# はじめに

モノのインターネット (IoT) とは、さまざまな大きさのデバイスが直接あるいは間接的にインターネットに接続する、製品やサービスで構成されるエコシステムであり、現在急速に広がりつつあります。IoT に接続するデバイスは、 典型的なパソコンや携帯電話とは違います。新しい IoT デバイスには、 個人の消費者が使用するものもあれば、 組織が使用するものもあります。自動車、ホームセキュリティ、ホームオートメーション、生産設備、石油やガスの制御システム、変電設備、ジェットエンジン、医療用インプラント、X 線機器など、考えられる限りのあらゆる種類のデバイスに、IoT コンピューティングが組み込まれるでしょう。

言うまでもなく、これらの IoT デバイスでは、 実行するコードを検証できること、 他のデバイスに対して信頼性を立証できること、 他のデバイスと (インターネットへの接続の有無にかかわらず) 安全に接続できることが必要とされます。

## 信頼のルートとは

IoT が登場する前、ほぼすべてのパソコンの OS やブラウザに、SSL (現在の TLS や DTLS) などの公開鍵技術とコードサイニングが組み込まれました。コンピューティングの主役がデスクトップからモバイルに移り変わると、 SSL とコードサイニングはモバイルデバイスのセキュリティにとっても重要な技術であることが明らかになりました。コードサイニングと、SSL/TLS/DTLS による暗号化と認証の拠りどころとなるのが、 信頼のルート (Roots of Trust) です。

信頼のルートの重要性を理解するには、 まず SSL/TLS/DTLS の仕組みについて多少知っておく必要があります。Web サイト、あるいは Web サイトで提供されるサービス (インターネットバンキング、電子商取引、SNS、勤務先のサイトなど) に安全に接続しようとすると、 サイトからユーザーのブラウザに電子証明書が提示されます。電子証明書には、そのサーバー/サービス/サイトの識別情報が記載されています。これによってブラウザは、ユーザーがアクセスしようとしているサイトが本当に安全にアクセスできるのかどうかを検証できます。偽造を防ぐため、 電子証明書には、認証局 (CA) という組織によって暗号化された署名が施されています。このように、 数少ない CA に大きな信頼を置くことによって権限の集中化を図っています (CA はブランドを賭けて、そのエコシステムを保護します)。このことが、数兆ドルにのぼるオンライン商取引を支える土台となっています。数十億人のユーザーが数百万台のサーバーに安全にアクセスし、 安全に接続できるかどうかは、この点にかかっているのです。

このモデルは、 CA の信頼のルートがあらかじめユーザーのデバイスに埋め込まれていなければ機能しません。CA が信頼できる取引の仲介者を務めてくれなければ、 クライアントは通信相手であるサーバーの身元を確かめるすべがないのです。CA による検証を受けずに発行する自己署名証明書によって誰それであると名乗ることもできますが、その主張は確かめることも否定することもできません。ユーザーのデバイスに信頼のルートが埋め込まれていれば、デバイスはその中のルート証明書を使用し、 そのルート証明書によって署名されている (またはルート証明書につながっている) 数百万枚の証明書の真偽を確かめることができます。以前にそのサイトに一度もアクセスしたことがなかったとしてもです。この技術が非常に安全で、 しかも極めて拡張性に優れていることは証明済みです (現在インターネットユーザーは 24 億人、 SSL によって保護されている Web サイトは 300 万に達しています)。電子商取引の成功と安全を達成した CA は、 IoT でも同じ安全性と拡張性を実現したいと考えています。

digicert®

信頼のルートについてもう少し詳しくご説明しましょう。ルート証明書には、 暗号操作 (電子証明書への署名と、 署名の検証) で使用される鍵ペアのうちの公開鍵が含まれています。ルート証明書はソフトウェアではなくデータ (暗号鍵を含む 固定の ASCII テキスト) です。よって、知的財産ではありません。パソコンやブラウザの世界では、 このルート公開鍵は非常に大きな数 (現在は多くが 2048 ビット) であり、RSA という古い形式の暗号で使用されています。ルート証明書は通常、多くの CA から無償でライセンス提供されており、ハードウェア、OS、ブラウザ、その他のアプリケーションに埋め込まれます。これらの場所に信頼のルートが存在するからこそ、 未知の信頼されていないデバイス (たとえばブラウザ) から、 未知の信頼されていないサービス (たとえばオンラインの電子商取引サイト) に、 信頼のチェーンによって安全に接続することができるのです。クライアントとサーバーのデバイスが適切に設定されていれば、 ルート証明書を使用してサーバーがクライアントデバイスの身元確認を行うこともできます。この相互認証 (サーバーがデバイスを認証し、 デバイスがサーバーを認証する) が、 IoT セキュリティを支える重要な土台となります。相互認証は暗号化通信を開始する際の重要なステップであり、 完全性と機密性 (プライバシー) の両方が実現します。つまり、どちらのデバイスも、自分が期待している相手との間で安全に通信しているという確信を持つことができるのです。

## 信頼のルートの IoT への適応

パソコンやタブレット、携帯電話は、ギガヘルツ単位の高速処理が可能です。プロセッサは 32 ビット、あるいは 64 ビットで、ギガバイト単位の RAM に容易にアクセスできます。一方、 多くの IoT デバイスは 8 ビットデバイスであり、処理速度は 8 メガヘルツ以下、アクセスできる RAM はたったの 32 キロバイトという場合が多く、コンピューティング能力も暗号化能力も著しく低くなります。実際には IoT デバイスの中にも、デスクトップやサーバーと同じ 32 ビットまたは 64 ビットアーキテクチャで、 同じ処理能力、同じギガヘルツ単位の演算スピードを持つものもたくさんあります。しかし、IoT の世界は処理能力の高いものから低いものまで、さまざまなデバイスが混在しているうえ、処理能力の低いデバイスはこれからもずっと使われ続けることになります。

したがって、IoT の世界での暗号操作 (暗号化や認証など) は、処理能力の高いデバイスと低いデバイスの両方に対応しなければなりません。しかし、 パソコンやサーバーで行われている 2048 ビットの RSA 演算を、8 MHz で動作する一般的な 8 ビットマイクロコントローラで処理すると、 暗号操作に信じられないほど長い時間がかかってしまいます。幸い、ここ 10 年ほどの間に、 RSA に代わる暗号として楕円曲線暗号 (ECC) が有効であることがわかってきました。ECC では、 暗号化と認証の処理時間が RSA の約 10 分の 1 に短縮されます。しかも、RSA よりもずっと短い鍵長で、RSA と同等のセキュリティを実現します。実際、米国商務省標準化技術研究所 (NIST) は、224 ビット ECC を 2048 ビット RSA と同等と見なしています。つまり、スピードが遅く処理能力の低い IoT デバイスでも、ECC なら問題なく動作し、しかも処理は高速で、バッテリーの消耗も少ないのです。

このようなわけで、世界トップクラスの CA である DigiCert 社では、まもなく IoT 向けのパブリックな信頼のルートを作成する予定です。この IoT 向けの信頼のルートには、パソコンやモバイルデバイスなどのブラウザで使用されている従来のものとは大きく異なる点が 2 つあります。

- 1 つは、 IoT デバイスのコンピューティング能力を考慮し、ルート証明書に複数の暗号鍵 (ECC など) を持たせる予定であるという点です。暗号鍵を選択できるようにすることにより、 低処理能力デバイスにとっての悩みの種である、メモリ使用量と電力消費量をいずれも減らすことができます。

- もう 1 つは、SSL/TLS/DTLS とコードサイニングとで、ルート証明書を分ける予定であるという点です。パソコンやブラウザの世界では、 SSL/TLS/DTLS で使われているのと同じルート証明書がコードサイニングでも使われています。しかし、 これら 2 つの用途はまったく別のものであるため、 DigiCert 社は過去 15 年の経験に基づき、 ルート証明書を別にすべきと判断しました。特に、2 つの用途では要件がまるで異なります。

## IoT における信頼のルートの適用

まずコードサイニングに関してですが、IoT デバイスや IoT サービスでは早急にコードサイニングの採用が進むと予想されます。デバイスでは署名されていないコードを実行すべきではありません。確認されていないデバイスや確認されていないサービスからデータを受け取ることは、とても危険です。署名されていないコードをデバイスが実行できるとしたら、自分の名前でほかの誰かのコードを実行するといった、 悪質な改造が行われかねません。したがって、IoT 業界の主要企業の多くは (セキュリティに詳しくない企業も含めて)、 誰もが確実に自分のデバイスを制御し続けられるよう、 自社でコードサイニングの採用を進めると同時に、 他社も採用すべきだと主張しています。Apple® 社の iOS、 Microsoft® 社の Windows®、 Google™ 社の Android™ がコードサイニングを広く使用しているのと同じ理由で、 IoT でもコードサイニングをあらゆる場面で (ハードウェアが許せばセキュアブートにおいても) 活用する必要があります。すべての業務用アプリケーションのため、 また、 セキュリティ要件の厳しいコンシューマ向けアプリケーションのため、あらゆるソフトウェア、ファームウェア、 ブートイメージ、 アプリケーション、 実行可能なスケッチ、オペレーティングシステム、BIOS に署名がなされるべきです。こうしたあらゆる形式のコードへの署名と、 署名済みであることの検証は、信頼できる機関によって行われ、改ざんされていないことが検証されなければなりません。自動車や航空機、製造組立ラインなどでは、 セキュリティに取り組むべき理由が明白です。しかし、コンシューマ向けデバイスにも、意外に強いセキュリティニーズがあります。たとえば、悪意とは最も縁がなさそうに思われるベビーモニターでさえ、すでにハッカーの標的にされています。赤ちゃんを驚かせて起こしたり、家にいる夫婦の様子を覗き見したりする輩がいるのです。

次に SSL/TLS/DTLS に関してですが、 IoT デバイスや IoT サービスは、パブリックなインターネット上で運用するか、もしくはインターネットとの間でデータをやり取りする中継機器と接続することが必要になると予想されます (組立ライン業務のような比較的閉じた環境ではよくあることです)。IoT サービスに接続するエンドユーザーにとっては、デバイスが中央にあるサービスと通信する場合でも、デバイス間でピアツーピア通信を行う場合でも、強力な相互認証は必須です。IoT デバイスのメーカーは、個々のデバイスに検証可能な固有の識別情報を与えるため、デバイスの製造時に証明書を埋め込んでいますが、 シマンテックはすでにこうしたメーカーや業界団体と連携しています。

信頼のルートには、 コードサイニング用、 SSL/TLS/DTLS 用、そして相互認証用と、 3 つの階層が必要です。これらがすべて 1 つのデバイスに埋め込まれる場合もあります。IoT デバイスのメーカーでは、 安全にコードを更新したり独自にテレメトリを収集したりするため、 メーカー独自のプライベートな信頼のルートが必要になるでしょう。エコシステム (独立の業界標準化団体など) では、 メーカー間で相互運用や認証を行うための信頼のルートが必要になるでしょう。そして世界中で、 あらゆるマシン同士の通信と信頼のため、 パブリックな信頼のルートが必要になるでしょう。

DigiCert 社は単にこれらの信頼のルートを作成・管理するだけでなく、マネージド PKI サービスも提供しています。このサービスでは、 DigiCert 社が企業やエコシステムの代わりに、 権限、特権、 資格、 その正当性の根拠となる証明書などの発行、 登録、委譲、失効を管理することによって、強力なコントロールを可能にします。

この 3 階層モデルによって、企業は実行可能なソフトウェアのデバイスへのダウンロードを誰に許可するかを徹底して管理することができます。同様に、デバイスとサービスの間の通信の管理も徹底されます。

digicert®

## 総合的な IoT セキュリティアーキテクチャ

識別情報、認証、コードサイニングは、エコシステムにとって重要で価値があります。一方、DigiCert 社ではエンドツーエンドのセキュリティ戦略を推奨しています。たとえば、 OS を装備したデバイスのための軽量なホストベース保護、 IoT データを分析してさまざまな異常を発見するためのセキュリティ分析、 IoT 脅威情報の収集、 セキュリティの状況を総合的に把握するための IT および運用環境全体の相互相関分析、ソフトウェアやファームウェアの更新のための IoT 管理、 デバイス上のアプリケーションのリモート管理などがあります。

## 詳細情報

**製品についてのお問い合わせ:**

**デジサート・ジャパン合同会社**
〒104-0061
東京都中央区銀座6丁目10番地1号
GINZA SIX 8階
https://www.digicert.com
JPN-Info-MPKI@digicert.com
03-4560-3941