IoT (モノのインターネット) のための信頼のルート

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

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**
[illegible]
[illegible]

- 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でで X 嶋逗る