第7章

M2Mのセキュリティ

Ioannis Broustis (*Alcatel-Lucent, New Jersey, USA*)
Ganesh Sundaram (*Alcatel-Lucent, New Jersey, USA*)
Simon Mizikovsky (*Alcatel-Lucent, New Jersey, USA*)
Harish Viswanathan (*Alcatel-Lucent, New Jersey, USA*)

セキュリティは、あらゆるデジタル通信環境において重要な機能となっている。セキュリティの役割は、M2Mソリューションにおいては更に重要となる。携帯電話システムのような既存のサービスインフラは一般に、サービス、ネットワーク、デバイスが密に結び付いており、通常、通信事業者一箇所で管理されている。一方、M2Mソリューションでは、アプリケーションプロバイダ、通信事業者、複数のデバイスメーカなど多くの事業者が関わっている。これらの事業者は、様々な面で相互関係があったり、あるいは関係がなかったりしている。言い換えると、特定のプレイヤー間では正規の信頼関係を築くことなくビジネスが成り立っているので、複雑な信頼関係がM2M環境の中に存在することになる。この問題を根本的に解決するためには、新しい概念で、スケーラビリティを持ち、かつ自動化されたセキュリティ機能が必要となる。このような機能は、M2Mデバイス数の将来における爆発的増加や、複数のアクセスネットワーク技術を利用する少数のM2Mオペレータにより提供される大量のアプリケーションに対応する必要がある。

本章では、様々なM2Mプレイヤー間における信頼関係の複雑性について説明する。この複雑性のために、セキュリティ戦略の設計、M2Mソリューション、及び設計上の脆弱性回避を想定したガイドラインを紹介する。さらに、予想される脅威から守るためにM2Mシステムに実装されるべき様々なセキュリティポリシーについても言及する。

7.1 はじめに

M2Mの市場は、多くの領域に様々なプレイヤーがいるため、極めて細分化されている。一方で、顧客企業の生産性や、ユーザの利便性・快適さの向上のために、M2Mサービスが貢献するポイントが極めて高いことを業界は把握している。既存設備の利益効率の観点から、大手通信事業者によるM2Mアプリケーションへの注目は増大傾向にあり、ネットワークとデバイスのオープン化の傾向と相まって、M2Mは前例のない流行の兆しを見せている。その中でセキュリティは、M2Mが大きな市場に受け入れられるための重要なエネーブラ（要件）となる。なぜならエンドユーザは、M2M通信には、従来の通信とほぼ同等のレベルのセキュリティを実現することを要求するからである。つまり、M2Mにおけるデジタルコンテキストのセキュリティにおいては、機密性や保護された完全性、あるいはプライバシーを管理する認証、認可の仕組みが、エンド・ツー・エンドで重要な要素となる。

いくつかのM2Mサービスシステムでは、すでに複数のシナリオを採用している。特に携帯電話網は現在、多くのM2Mソリューションで利用されている。本章では、セキュリティソリューションの適用例の１つとして、携帯電話網を利用したM2M通信のユースケースに焦点を当てて解説する。以下では、いくつかのセキュリティ対策が適用できない携帯電話網におけるM2Mシステム固有の課題について延べてみよう。

7.1.1 ●携帯電話網による M2M でのセキュリティの特徴

携帯電話網を利用したM2Mでは、実はモバイル機器のために現在使用されているセキュリティのいくつかのメカニズムは適用できない。従来の携帯電話網とは、事情が大きく異なっているのは次の３点である。

第一に、今日の携帯電話網によるサービスは、SIMカードが実装されたデバイスの供給からデバイスのプロビジョニング（初期設定）、ネットワークインフラの提供、音声通信とデータ通信のためのサービスの提供まで、単独のサービスプロバイダ（通信事業者）によって一手に提供されている。もちろん、この中からネットワークインフラの提供を行わない仮想移動体通信事業者（MVNO：Mobile Virtual Network Operator）という形態もある。一方、携帯電話網によるM2Mの場合は、複数のプレイヤーが何らかの限定的な関係を保持しながら成り立っている。

【1】ユースケースにみる各プレイヤーの関係

ここでは例として、ある電力会社が携帯電話網を利用したスマートメータの導入を計画しているという場合で、あらためて、M2M通信が従来の携帯電話網とはセキュリティ事情が大

きく異っている点を考えてみよう。典型的なM2Mサービスであるこのソリューションを実現するために、電力会社はメータの製造元にメータを発注し、複数の携帯電話事業者のネットワークアクセスと関連サービスを提供するMVNOとM2Mサービスの契約をする。そして電力会社は、自社のデータベースがMVNOのデータベース内でのプロビジョニングが済みしだい、このスマートメータからの検針結果を収集することが可能となる。このソリューションには、テレメタリングのアプリケーションを提供している電力会社の他に、ソリューション実現のために協力関係にあるM2Mオペレータ、携帯電話網を提供する通信事業者、メータの製造メーカ、そしてエンドユーザが関わっている。ここで注意して欲しいのは、メータを利用する電力会社と、携帯電話網の通信事業者とは利害関係はないということだ。言い換えると、この2つのプレイヤーは互いに信頼関係を有する必要がない。したがって、ここで採用されるセキュリティソリューションは、このようなオープンで無関係なビジネス環境下でも機能しなければならないことになる。この点が第一のポイントである。

従来の携帯電話網との2点目の違いは、多くのM2Mソリューションは膨大な数のデバイスで成り立っており、かつそれらのデバイスが扱うデータ量はわずかで、各デバイスからのデータ伝送量も極めて少ないということである。したがって、経済的な観点から見ても、M2Mにおけるセキュリティポリシーは、携帯電話端末で採用されているものと同等のものは望めない。そしてその多数性であるがため、デバイスメーカはデバイスを効率的に扱うことのできる、よりシンプルでかつ自動化されたプロセスを利用することが望ましくなる。例えば前述のスマートメータのユースケースでは、望まれる実装プロセスの1つとして、メータのメーカからエンドユーザには直接メータを出荷するという形態が考えられる。

一般にM2Mデバイスは、出荷されてから使用場所に設置されるまでの間、カスタマイズされることはない。それらのデバイスは、均一な仕様で実装された製品であり、各デバイスはMAC（Media Access Control）アドレスとシリアルナンバーのみで識別される。そしてデバイスは、当初の設置時のみでなく新たなユーザにより使用が再開される場合など、複数回インストールされることもあり、その都度ネットワークに対してシームレスに統合されるべきである。さらに、そのインストールは、経験に乏しいエンドユーザや契約者によって実施されることもある。

携帯電話やスマートフォン、あるいはワイヤレス接続が可能となっている環境下のノートPCとの比較における3点目の違いは、M2Mデバイスは人間が介在していないので、第三者からの破壊行為や不正使用に対して高いリスクに晒されていることである。特に、M2Mデバイスを不正に使い、第三者がWebブラウジングのような一般的なインターネットアクセスを行うといった行為は、正にリスクであり、そのような不正利用はデバイスへのアクセスが認められていないユーザによって引き起こされる。したがって、そこで適用されるセキュリティソリューションは、デバイスが不正アクセスから保護されるよう設計すべきであり、そしてまた、通信事業者もしくはM2Mアプリケーションプロバイダも保護されるように設計すべきである。

さらに、携帯電話網を利用したM2Mソリューションの場合、デバイス数の急激な増加（10億台規模になる可能性もあり得る）と、MVNO事業者により提供される多くのアプリケーションに対応しなければならない。したがって、デバイスメーカはエンドユーザに直接、あるいはアプリケーションプロバイダを介して安価なデバイスを販売するという比較的オープンなエコシステムを構築するのが望ましい。例えば、デバイスメーカとM2Mサービスプロバイダがビジネス面での利害関係を有していない（つまり、信頼関係もない）場合、エンドユーザにとってみればオープンマーケットからデバイスを購入することも可能である。また、電力計のように住居に直接設置されるケースでは、住宅のオーナーであるエンドユーザは、M2Mソリューションを提供しているMVNO事業者の存在を意識することはないだろう。しかし、アプリケーションのセキュア化は、M2Mに関わるすべてのプレイヤーにとって重要な課題である。

【2】不正攻撃の例

本項では、M2Mシステム固有の特徴に起因するM2Mデバイスを乗っ取る形態の攻撃の例を２種類紹介する。なおここでは、携帯電話網を利用した場合のソリューションを想定しているが、他のネットワークにおいても容易に起こり得る攻撃形態であることに注意して欲しい。

例１　SIMカードを抜き去ることによる認証情報の盗難

例えば、本来はユーザの心拍数や血圧を計測しネットワーク経由で健康状況を監視するために用いられるM2Mデバイスから、悪意の第三者が通信モジュールを引き抜き、自らのスマートフォンにSIMカードとして挿入し不正利用するのがこのケースの一例である。ここで用いられるSIMカードは正当なものであるので、携帯電話網はこのSIMカードを問題なく登録し、スマートフォンからのアクセスを許可するだろう。これは、端末をネットワークに登録するために必要なあらゆる情報がSIMカードに記録されているためである。言い替えると、ネットワーク側からは、不正にSIMカードを利用している端末を明示的に特定する手段がないということである。このようにSIMカードの不正利用の結果として、不正アクセス者は、M2Mデバイス用の極めて廉価な課金プラン[1]で、このスマートフォンからWebブラウジングができてしまうことになる。更に重要なことは、携帯電話網を提供する通信事業者は、デバイスの契約数やタイプに基づいてデータ通信量の計画的な予測を注意深く行っている点である。Webブラウジングのように認可されていないサービスへのアクセスが発生してしまった場合、通信事業者側は予測計画を見直し、そのアクセスにリソースを集中的に使用し、結果として他の正当なエンドデバイスの要求には応えられないサービスを提供してしまう事態に陥る

1　M2Mベンダと通信事業者との契約形態にもよるが、無料の場合もあり得る。

こともあるだろう。

同様に、不正アクセス者がSIMカードを抜き取り分析することによりM2Mデバイスの IPアドレスや認証情報（ネットワーク登録時に割り振られる一時的なID）を取得してしまい、そのデバイスが物理的にアクセスできない場合、不正アクセス者は正当なユーザになりすましてネットワークにアクセスすることができる。例えばCDMA 1xEV-DOネットワーク[1]や、UMTS / HSPAネットワーク用の単方向アクセス端末識別子（UATI：Unicast Access Terminal Identifier）の不正取得などが、このようなケースに相当する。このシナリオでは、不正アクセス者はデータパケットを、被害者となるM2Mデバイスが確立した正当なデータセッションに紛れ込ませることが可能となる。

例2　データの盗み取りによる乗っ取り

不正アクセス者は、SIMカードを抜き取ることなく、M2Mデバイスとアクセスネットワーク間で交わされている制御信号やデータトラフィックを盗み取ることで、携帯電話網への接続を乗っ取ることも可能だ。攻撃者の狙いは、ネットワークサービスに無料でアクセスするための正当なデバイスの認証情報を不正取得することにある。例えば、攻撃者がリモートホストとのUDP接続を確立し、EVDOベースのアクセスネットワークから不正にアップリンク方向でのビデオデータの配信をたくらんでいると仮定しよう（このような攻撃は、他のネットワークにも同様に適用可能である）。不正アクセス者は、以下の方法によりアップリンクチャネルを無料で利用可能となる。

- まず不正アクセス者は、M2M装置（M2ME：M2M Equipment）が登録（register）されている期間中に、M2MEと無線ネットワークコントローラ（RNC）との間のすべてのパケット交換の情報を盗み取る。これらのすべてのメッセージは、暗号化されていない。したがって、無線インタフェースのオペレーティングシステムによってアサインされているユーザ機器の無線チャネルに関するID（いわゆるUATI）、そしてIPアドレスは不正アクセス者に知られるところとなる。
- 不正アクセス者のクライアントデバイス上のアプリケーションレイヤ（Webカメラアプリケーション等）が、ビデオフレームを生成する。各フレームは、IPレイヤに転送されIPパケットにカプセル化される。IPパケット化は不正アクセス者によって以下のように改ざんされる。（1）盗み取ったIPアドレスを送信元とし、（2）不正アクセス者が送信したいリモートホストのIPアドレスを送信先とする。
- 分割化処理されたIPパケットは、MACレイヤに転送され、MACヘッダが付加される。このヘッダは、盗み取ったUATI24の値が付加される。次に、物理レイヤ（PHY）はすべてのMACフレームをアサインされたUATIに対応するロングコードを用いた基地局に伝送する。UATIは不正アクセス者に知られているので、後者の行為は盗み取られたUATIに対応するロングコードの再構成を可能にする。それぞれの分割化されたパケットの伝送では、RNCによってM2MEに割り当てられたアップリンクのトラフィックチャネルが使用される。