安全性の高いIIoTシステムを実現 amnimo senseを支えるセキュリティ機能とは

Industrial IoT（IIoT）システムを構築するにあたって最も大きな課題となるのは、IoTデバイスとの通信やセンサーから収集したデータを確実に保護するセキュリティ対策です。IIoTシステムを容易かつ迅速に構築できるアムニモの「amnimo sense」では、どのようなセキュリティ機能を擁し、高い安全性を担保しているのか。本稿でその全貌を紹介します。

IIoTシステムに必要なセキュリティ機能をあらかじめ組み込んで提供

製造業・産業領域におけるIoTシステム ── IIoTシステムを構築する際には、留意すべき部分がたくさんあります。中でもセキュリティ対策は、絶対に解決しておかなければならない課題です。

IIoTシステムは、ネットワークに接続されたデバイスが悪意のある第三者に乗っ取られてサイバー攻撃の踏み台にされたり、現場で稼働する制御・運用系（OT）システムを制御不能に陥れたりといったように、サイバー攻撃の対象となる多くのリスクが内在します。また、デバイスから取得したデータ真正性の担保、プライバシー情報の保護という観点からも、強力なセキュリティ対策を講じる必要があります。

IIoTシステムでも、なりすましによる不正アクセス、機密情報の盗聴／流出、データの改ざん、DoS（サービス不能）攻撃といった脅威から保護するために、一般的なITシステムと同様のセキュリティ対策が欠かせません。そのためにセンサーデバイスやIoTゲートウェイが設置されているエッジから、データを収集・蓄積・処理するクラウド基盤、データを実際に活用するエンドポイントまで、それぞれの脅威モデルを検討して詳細なリスク分析を行うことが求められます。しかしながら、これらすべてのセキュリティ対策を自社で設計・導入することは非常に困難です。

そこでアムニモの「amnimo sense」では、IIoTシステムに必要なセキュリティ機能をあらかじめ組み込んだ上でサービスを提供しています。amnimo senseはクラウド基盤としてMicrosoft Azure（以下、Azure）を採用していますが、Azureに用意されている有用なセキュリティ対策機能を最大限に活用しながら、独自のセキュリティ対策を追加するという方針に基づいてセキュリティを強化しています。

軽量センサー向けのセキュリティ機能を用意

amnimo senseは、データの収集・蓄積・処理を実行するクラウド基盤としてAzureを採用したシステム構成になっています。センサーデバイスから取得したデータはIoTゲートウェイを経由して「Azure IoT Hub」に接続するという仕組みになっていますが、この接続部分のセキュリティには、Azureの機能が使われています。

IoTデバイスを安全・確実に接続する仕組みとして利用されているのが「Azure Device Provisioning Service」です。これは正規のIoTデバイスを自動設定（ゼロタッチ・プロビジョニング）するサービスであり、amnimo senseではIoTデバイスの出荷前に機器固有のデバイスIDに基づいて発行されたデバイス証明書（X.509デジタル証明書）が組み込まれており、正規でないIoTデバイス（認証に失敗するデバイス）からクラウド基盤に接続することができないようになっています。当然、IoTゲートウェイとIoT Hubの間の通信は暗号化されているため、通信回線を流れるデータが盗聴・改ざんされるおそれもありません。

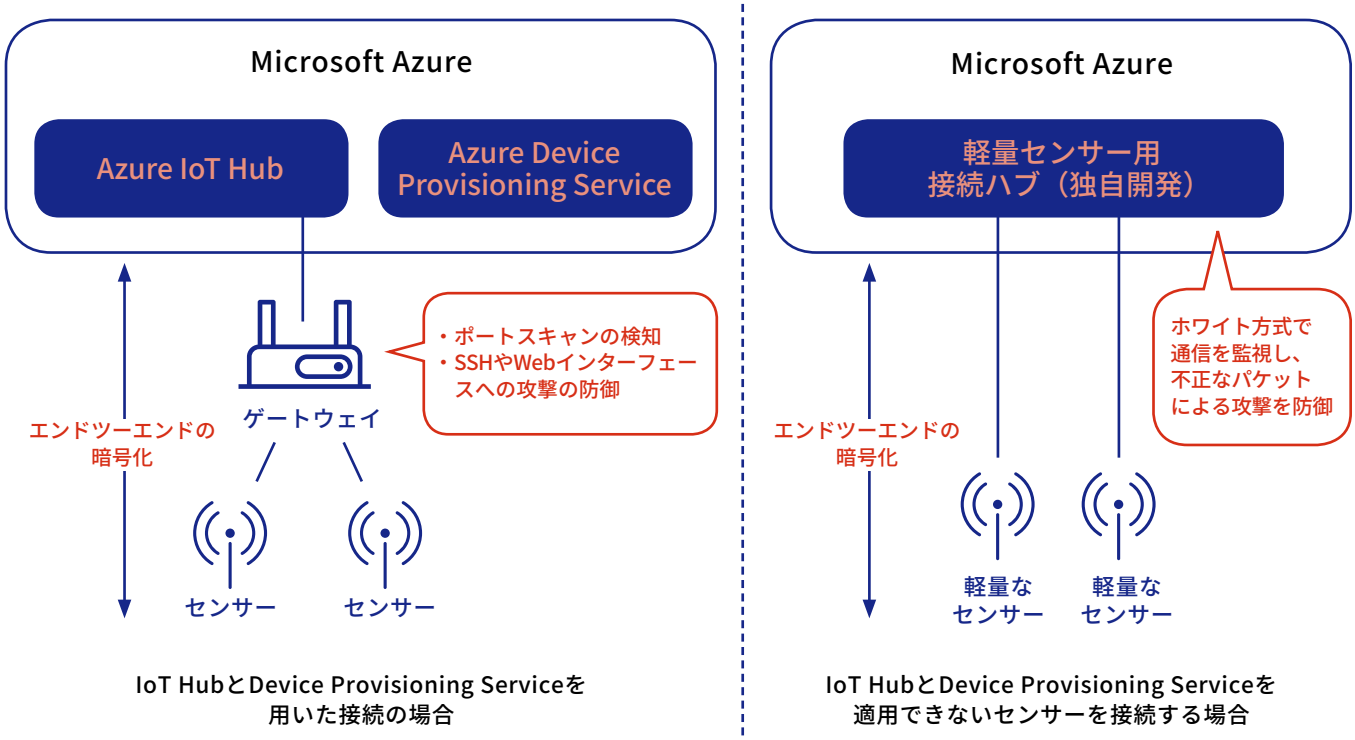

図1：IoTデバイスを安全に接続するamnimo senseの仕組み

IoTゲートウェイにはBayshore Networks社のセキュリティ技術が採用されており、外部から実行されるポートスキャンを検知したり、SSHまたはWebインターフェースへの攻撃を防御したりといった機能を持ち、サイバー攻撃からIoTゲートウェイを守る働きをしています。

また、ハードウェアリソースが限られている軽量なセンサーでは、IoT Hubに接続できないという場合がありますが、これに対してアムニモでは独自開発した軽量センサー接続用Hubをクラウド基盤に用意しています。軽量センサーには、出荷時に固有の公開鍵が組み込まれており、鍵認証やセキュリティトークンなどを使って暗号化通信する仕組みでセキュリティを確保しています。この軽量センサー接続用Hubには、米国Bayshore Networks社のセキュリティ技術が組み込まれており、ホワイトリスト方式で通信を監視するもので、システムの脆弱性をつくような不正なパケットによる攻撃から自動防御できるという特長があります。

クラウド基盤を守る Azureの各種セキュリティ機能

amnimo senseのクラウド基盤では、基本的にAzureが提供している各種セキュリティ機能が使われています。それぞれの役割を見ていきましょう。

■クライアントの認証を行う「APIM」「RBAC」

Azureが提供するリソースやサービスを呼び出す際にクライアントに認可を与える役割を持ち、クラウド基盤へのアクセス制御において重要な2つの機能が、「Azure API Management（APIM）」とアムニモが自社開発した「Role-Based Access Control (RBAC)」です。APIMでは外部からのすべてのAPI呼び出しが検知され、RBACでは対象のデータにアクセスする権限を持つユーザーのみがAPIの実行を許可されるように役割（ロール）が設定されています。ここでアクセスが認可されな

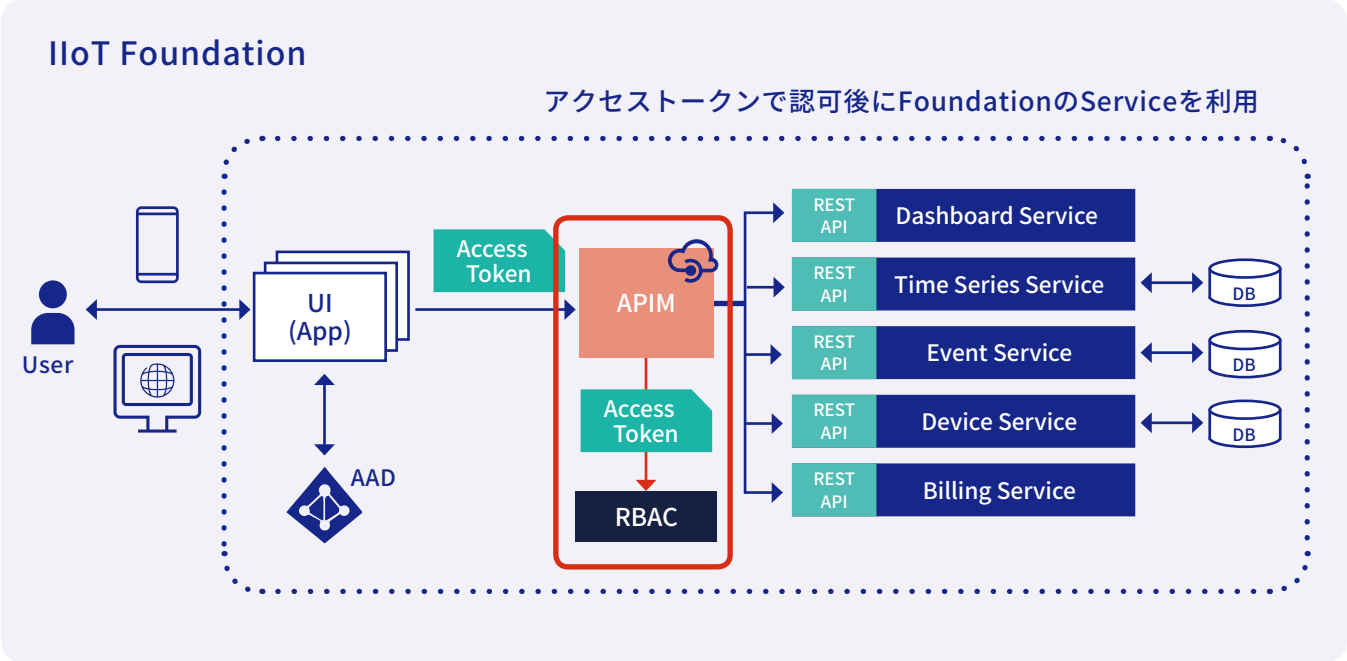

図2：AAD、APIM、RBACなどを利用したアクセス制御の仕組み

い限りAPIが実行されない仕組みになっています。

amnimoでは、カスタマーポータルで作成したアカウントの情報は「Azure Active Directory（AAD）」により管理が行われ、ユーザー認証されます。

クライアント側のアプリケーションからIoTシステムを利用する際は、その裏側ではシステムが提供する各種サービスがAPIによって呼び出されます。この呼び出しには、まずAADからIDトークンとアクセストークンを発行してもらい、それらのトークンを持った呼び出し側に対して認可を与えるのが、前述のAPIMとRBACというわけです。

■トークン、パスワード、証明書を安全に管理する
「Azure Key Vault」

トークンやパスワード、証明書などの機密情報は「Azure Key Vault」で保管・管理されています。これは機密情報を格納する保管庫（Vault）の役割、および保管した機密情報に安全にアクセスする仕組みを備えた機能です。

■WAFの機能を備えた
「Azure Application Gateway」

外部の攻撃などの脅威からクラウド基盤を守るために使われているのが「Azure Application Gateway」です。このサービスは、システムの脆弱性やそれを悪用した脅威からWebアプリケーションを保護するWebアプリケーション・ファイアウォール（WAF）の機能を提供するものです。SQLインジェクション、クロスサイトスクリプティング、コマンドインジェクション、HTTPプロトコル違反、ボット、クローラーなどからクラウド基盤で稼働するWebアプリケーションを守ってくれるものです。

■Webサービス側の設定

amnimo senseでは、Webサービスとして提供されるIIoTシステムをエンドポイント側のWebブラウザから操作することになります。そのため、そこに潜む脆弱性対策も必要です。そこではWebブラウザのセキュリティ機能を活用するとともに、Webサービス側でのWebサーバーの設定やプログラムの記述を適切に行うことで対応します。

アプリケーションの
セキュリティテストツールも提供

ここまでamnimo senseが備えるセキュリティ機能を紹介してきましたが、いくら基盤のセキュリティが十分でも、ユーザー側で実装するアプリケーションのセキュリティに不測があれば元も子もありません。そこでアムニモは、セキュリティテストの仕組みを提供することでユーザーアプリケーションのセキュリティもサポートしています。

アプリケーションのソースコード静的テストツールとして採用しているのが、英国Micro Focus社の「Fortify Static Code Analyzer（SCA）」です。このツールは各種プログラミング言語で書かれたソースコードをスキャンし、開発サイクルの早い段階でセキュリティの問題点を発見するものです。

また、侵入テスト（ペネトレーションテスト）にはユービーセキュアが提供する国産ツール「Vulnerability Explorer（VEX）」を採用。このツールは、特殊なプロキシを経由させることでWebサービスのやり取りを記録し、記録された通信内容からシナリオを作成して検査を実行。その結果レポートを解析して対策するというものです。またこのツールを用いて、ペネトレーションテストの自動化を行い、ソースコードベースでのセキュリティチェックを含めた対策で常にセキュリティの改善や強化を行っています。

amnimo senseではこれらのツールを使ったセキュリティテストの自動化も進めており、より安全なアプリケーションの迅速な開発の支援にも注力しています。さらにセキュリティ対策の確実性を求めるユーザーに対しては、外部専門家による高度なマニュアル検査のサービスも提供しています。

このようにamnimo senseは、Azureに用意されている有用な機能を活用しながら、不足する機能をサードパーティ製品で補うことで、堅牢なセキュリティ対策を実現しています。amnimo senseを利用すれば、難しいIIoTシステムのセキュリティ対策も任せることができるというわけです。セキュリティに不安でIoTの導入に二の足を踏まれている方も、ぜひamnimo senseで一歩を踏み出してみてはいかがでしょうか。

アムニモ株式会社

〒180-8750 東京都武蔵野市中町2-9-32

Tel **050-3160-0300**
Email **info@amnimo.com**
URL **https://amnimo.com/**

amnimo