ホワイトペーパー

IoTをスケールアップしつつ セキュリティを確保するには

セキュリティを取り巻く環境は日々変化しています。個人のサイバー犯罪者だけでなく、国家が支援する犯罪組織によって、より大規模な企業が重点的に攻撃されるケースが増えています。企業は今すぐセキュリティの強化に取り組むべきです。

本ホワイトペーパーでは、サイバー犯罪の変化と、IoT製品のセキュリティを確保する手段について紹介します。Telenor IoTが最新のテクノロジーや堅牢なセキュリティ対策、社外の協力関係、厳格なISO認証によって、お客様のIoTデバイスのセキュリティと将来に向けた取り組みをどのように支援しているかをご説明します。

telenor IoT

IoTを標的にした次世代型サイバー攻撃への備え

大規模なIoT環境が整ったことに伴い、サイバー犯罪者からの攻撃対象が拡大しています。センサーやモジュール、接続、プロセッサなどが潜在的な侵入ポイントとなるからです。ラスベガスのカジノへの攻撃に水槽のポンプが使われたという話や、タイヤ空気圧監視システムが車載システムへの侵入ポイントになっていたという話もあります。つまり、IoTのセキュリティを確保するには多方面からの検討が必要になるのです。

はっきりしているのは、攻撃の件数が増えていることと多様化していることです。セキュリティに精通した企業であるカスペルスキーによる調査では、2021年の上半期にIoTデバイスを標的にした攻撃が15億件以上発生したことが明らかになっています。同社のテレメトリデータ（攻撃の情報を集めるためのハニーポットから収集したデータ）によると、IoTデバイスへのサイバー攻撃は半年前と比較して100%以上増加しています[1]。

IoTが直面する潜在的な脅威についての理解を深め、セキュリティの脆弱性を塞ぐために強力な対策を講じる必要があります。ただし、セキュリティはリスクに応じた適正なレベルでなければならず、IoTのセキュリティに対する過剰な投資は、将来の拡張を妨げ、現在の市場参入時期を遅らせてしまう恐れがあります。

とはいえ、別の面から見れば、攻撃は急増しており、ダメージはさまざまな形で発生しています。そのすべてが明確な金銭的被害を伴うわけではありません。たとえば、顧客のデータ情報を盗み取る攻撃によって即座に収益を失うことはないかもしれません。しかし、それをきっかけに風評被害が生じたり、最終的に規制当局から多額の罰金を課されたりすることがよくあります。また、サイバー犯罪は急速にその手口が高度化しています。

[1] https://www.techdigest.tv/2021/09/iot-cyber-attacks-double-in-first-half-of-2021.html

進化するサイバー犯罪

以前は、無計画なハッカーがほぼ無作為にランサムウェアやフィッシングメール、DDoS（分散型サービス拒否）攻撃を使って企業を攻撃していました。しかし、今日のサイバー犯罪はより高度化し、企業や他国に対する攻撃を認め支援している一部の国によって管理されている場合もあります。被害者にランサムウェアの身代金を払わせるためのコールセンターを保有し、特定の国の特定の企業を標的にするような組織化されたサイバー犯罪者が存在するのです。

DDoS攻撃はサイバー犯罪者が使用する手法の1つで、大規模な攻撃でもわずか数ドルのコストしかかかりません。そのため、攻撃対象となるIoTが急速に増加しても、極めて低いコストで大量の攻撃を実行できます。したがって、IoTを運用する企業は最大のリスクに対応することを優先し、自社とユーザーを守るためにすぐに導入できて費用対効果の高い方法を見つける必要があります。また、セキュリティ対策は継続的なプロセスであり、1回きりで済むものではありません。企業ではIT担当者が不足傾向にあるため、限られたコストやスケジュールでセキュリティを確保するための手段はIoTエコシステムから調達することになります。

同時に、IoTデバイスのコネクティビティの安全性は向上しており、デバイスのIDは従来のプラスチック製のSIMカードを使用する場合よりも確実に保護されるようになっています。統合型SIM（iSIM）などの新しいSIM技術はセキュリティの向上を実現する可能性を持っていますが、導入はまだ初期段階であり、事業者間のセキュアキーの共有について対処すべき課題も残っています。また、埋め込み型ユニバーサル集積回路カード（eUICC）によってデバイス内の物理ソケットが不要になります。このソケットは、かつては犯罪者にとって格好の侵入ポイントでした。埋め込み型、統合型のSIMをリモートのSIM管理システムで管理できれば、ユーザーは十分に実証済みの方法で接続のセキュリティを確保し、デバイスのIDを保護できることになります。

> **デバイスの堅牢化とは、ハッカーからの攻撃に対する安全性と耐久性の向上を意味します。**

主な脅威

IoTデバイスの物理的な堅牢化不足

脆弱なデバイスが市場に出回る原因の1つはコストです。デバイスのコストを安価にしようとするニーズは最終的に脆弱なデバイスにつながります。従来のプラスチックカード型のSIMではない統合型SIMのようにハッキングされる方法が少ない堅牢化されたデバイスの導入は、リスクを大幅に軽減します。

セキュリティが不十分なデータのストレージと転送

IoTデバイスのデータをストレージに保存する際の通信のセキュリティは、IoTシステムにおける大きな問題です。ここで機密データが詐取される可能性があるためです。データを暗号化すれば、産業スパイによる「盗聴」攻撃を有効に防ぐことができます。暗号化は、ハッカーが2つのデバイスの間のメッセージを傍受して新しいメッセージにすり替える中間者攻撃に対する防御策にもなります。

脆弱なパスワード

ハードコーディングされているパスワードや簡単に推測できるパスワードはハッカーの絶好の餌食です。「password」や「ABC123」のようなデフォルト設定のパスワードを使用しているケースは現在でも非常に多く見られます。マルウェアは一般的なパスワードを使用し、そのようなデバイスに比較的簡単に侵入します。IoTのIDやアクセス管理システムは幅広いデバイス認証機能があり、攻撃にさらされるケースを減らすことができます。

セキュリティが不十分なエコシステムのインターフェース

IoT製品は一般に、データの処理と通信を行う複数のアプリやデバイス、ソフトウェア、システムで構成されます。それらのデータの受け渡し点が犯罪者に悪用される場合があります。リスクを軽減するには、堅牢なデバイス認証と強力な暗号化が必要です。

脆弱なデバイス管理

IoTデバイスの数が増えるにつれ、デバイス管理の問題も大きくなります。量産型の低価格デバイスを導入し、更新や保守を怠る場合も増えるからです。これらのデバイスは、特に機密性の高いデータを扱っている業界でランサムウェアの標的になります。デバイス管理が脆弱な企業は手遅れになるまで攻撃に気づかない場合があるからです。デバイスの管理、保守、更新、廃止を行うIoTプラットフォームは、リスクの軽減に役立ちます。また、プロビジョニング、ファームウェア更新、セキュリティパッチを効率化することで導入のスピードアップに貢献します。

特に、IoTを標的とするタイプの犯罪として、ボットネット、高度な持続的攻撃、人工知能（AI）対応の脅威、DDoS（分散型サービス拒否）攻撃、IDの詐取、データの詐取、中間者攻撃、ソーシャルエンジニアリング攻撃が多く見られます。

また、攻撃の自動化が増えており、近い将来には攻撃型AIによる攻撃が発生することも予想されています。現在、侵入初期（自然言語ジェネレータがソーシャルエンジニアリングメッセージを生成し、被害者をフィッシングサイトに誘導）から、データの流出（ニューラルネットワークが重要な情報を選択し、データを転送）まで、攻撃キルチェーンの各段階にオープンソースツールが利用されています。

スマートメーター企業がリスクを軽減するには

Telenor IoTのお客様の中に、スマートメーターの登場当初からお付き合いさせていただいているスマートメーター企業があります。スマートメーターは、重要インフラとの相互作用が重大な結果をもたらしかねないため、セキュリティ関連の厳しいコンプライアンスの遵守が求められる複雑な市場です。

同社は、当初からセキュリティ対応に取り組むことにより、暗号化されたデータがメーターからデータセンターに直接セキュアに転送できるようにしました。これを実現したのが、IPSEC VNP、それにIoTプラットフォームとお客様のデータセンターを結ぶオプションの専用回線です。

もう1つの重要な取り組みは、サブスクリプションのロックを可能にしたことです。その結果、SIMの状態の変更やSIMの解約など、デバイスに対する変更はブロックされます。変更できるのは、最も上位のアクセス権限を持ち、セキュリティ標準に則して審査を受けた人員のみです。それ以外の人はデバイスに一切の変更を加えることができません。

Telenor IoTがお手伝いできること

Telenor IoTは業界トップクラスのセキュリティ対策を導入することにより、お客様のビジネスの保護と将来を見据えた対応に全力で取り組んでいます。私たちはTelenorグループの一員として数十年に及ぶセキュリティ対策の経験を有し、それをお客様のセキュリティの実現とサポートに生かしています。

当社は2019年にISO 27001 ISMS（情報セキュリティマネジメントシステム）のコンプライアンスの認証を取得しました。ISO 27001とは、情報資産のセキュリティを管理するための体系的な枠組みの構築と管理に関する規格です。これにより企業は、自社のデータ資産の機密性、完全性、可用性、プライバシーを強力な管理機能で保護すると同時に、顧客データも保護し、規制の要件を確実に満たすことができます。

ISO 27001の要件を満たしていることに加えて、定期的に社外のセキュリティ専門家による侵入テストやセキュリティチェックを受けたTelenorの従業員のみが、顧客に対して機密性の高い処理作業を行えるようにするセキュリティ審査や、スタッフ向けのセキュリティ教育を受けたすべての新入社員の身辺調査を実施しています。また、オフィスへの入室を制限する物理的なセキュリティの採用や、パートナーやサプライヤーに対する厳しい審査やデューデリジェンスの手続きもあります。

Telenor IoTは業界トップクラスのセキュリティ対策を導入することにより、お客様のビジネスの保護と将来を見据えた対応に取り組みます。

Telenor IoT CEO
マッツ・ルンドクヴィスト

Telenor IoTはISO 27001: 2013に基づいて、リスク管理、事業継続、インシデント管理、物理セキュリティなどで構成される情報セキュリティマネジメントシステムを運営しています。セキュリティリスク管理は当社の業務の1つです。当社のリスク管理ポリシーはISO 27005を参考にしており、リスクを管理するための明確なプロセスを定義しています。このプロセスには、事業の関係者や、ビジネスセキュリティオフィサーなどのサービス運用と専任のサイバーセキュリティの専門家を含むリスクステアリングコミッティの設置があります。

サイバーセキュリティに対する対応において長い歴史を持つ企業として、Telenor IoTは、サイバー犯罪者が攻撃の規模を拡大し、サイバー犯罪の脅威が新しい時代を迎えていることを認識しています。国家支援型の犯罪組織（あるいは持続的標的型攻撃（APT）グループ）であるか、既知のマルウェアの再利用や再プログラミングによって新しいタイプの脅威を生み出している個人であるかを問わず、新たなマルウェアや未知の手法が日々作り出されています。ウイルス対策ソフトウェアやファイアウォール、メールゲートウェイのような従来型のセキュリティ対策ツールは防御の第一選択肢としては効果がありますが、これらのツールは既出の攻撃に基づいてルールやシグネチャをコードに書き込んでおり、未知の脅威を防ぐことはできません。

当社は、クラウドファーストアプローチによって既知、未知のすべての脅威からAWSインフラを保護することが、お客様に質の高いサービスを提供する上で不可欠と考えます。私たちは常に自社のクラウド環境を改善し、お客様の効率と社内のサービス（IoT監視やコンピュータ分析など）の効率を高めています。

脅威情勢の変化に対応するため、Telenorは、サイバーセキュリティAI（人工知能）のグローバルリーダーであるDarktraceをはじめ、多く

の企業と協力しています。Darktraceの自己学習型AIテクノロジーを活用し、AWS環境全体におけるすべてのデバイスやユーザーのアクティビティを深く理解して「活動パターン」を構築しています。当社のこのような事業運営をダイナミックに理解することで、Darktraceは新手の攻撃のちょっとした兆候でも検出できます。また、AWSのインフラ環境を可視化し、詳細な情報を取得するとともに、わかりやすいセキュリティレポートを短時間で生成します。

数年にわたり、パートナーとしてTelenorとの素晴らしい取り組みに関わっています。当社はネットワークやサービスの限界を超えていこうとするTelenorの姿勢に常に尊敬の念を抱いています。Telenorの自己学習テクノロジーに対する取り組みは、ダイナミックな運用、インフラ、顧客データのセキュリティ確保という課題に立ち向かう上で重要な要素です。

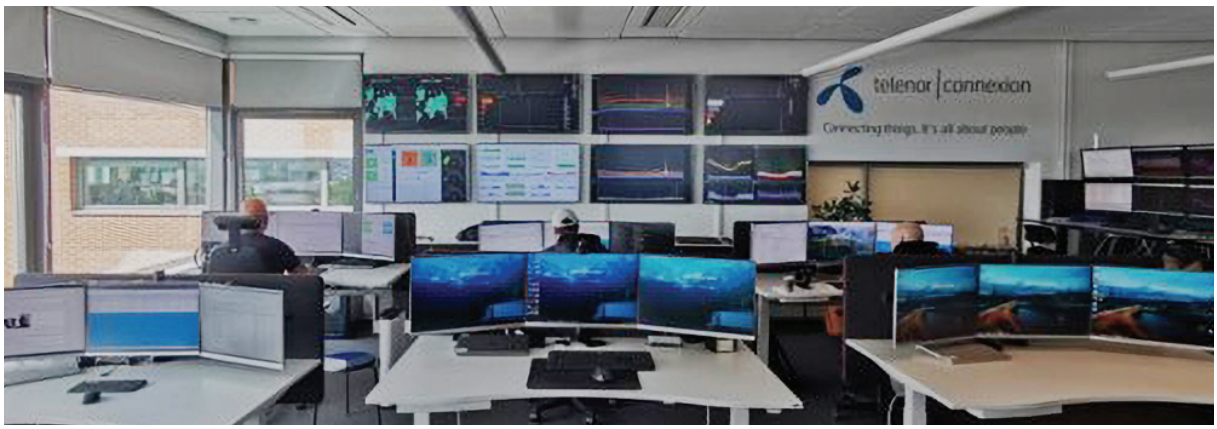
Darktrace Industrial副社長　クリス・トーマス

私たちは、自社のクラウド環境を保護するだけでなく、保存データや転送データの暗号化からエンドツーエンドのチャンネル保護まで、必要に応じてお客様にもセキュリティを提供します。また、セキュリティレベルを強化した独自のアクセスポイント名（APN）や、インターネット上の情報転送を保護する独自の仮想プライベートネットワーク（VPN）を提供します。

さらに、顧客サービスポータルでセキュリティ設定を提供し、多要素認証、CAPTCHA、パスワード試行回数制限によるアクセスの一時的なロックなどの機能を使用できます。当社のクラウドプラットフォームでは、接続されるすべてのデバイスは厳格な暗号によるセキュア認証を使用して認証され、すべての通信が暗号化（TLS暗号化）されている必要があります。

当社のサービスオペレーションセンター（SOC）は24時間体制でトラフィックを予防的に監視し、警告や疑わしいトラフィックパターンをチェックしています。つまり、セキュリティ上の問題を示す異常があれば、すぐに当社のチームが検出し、対応するということです。

SOCのすべての人員はセキュリティ検査を受けた専任のIoT専門家です。脅威を取り巻く環境の定期的な評価、セキュリティスキル向上のための投資、警戒を怠らない文化の育成によって、多層防御の考え方を備えた信頼性の高いシステムを構築できます。また、お客様に特有の要件に対応するために追加的なセキュリティ対策の付加サービスを提供しています。具体的には、プロセスのカスタマイズや個々のお客様のセキュリティ要件に合わせたレポートなどが可能です。これらのすべてのサービスは、複数の国際的および国内のセキュリティ規制要件に対応しています。



セキュリティは絶えず変化する

さまざまな脅威がIoT展開の各フェーズで明らかになっています。そのため、企業は今すぐセキュリティの強化に取り組む必要があります。脅威の数は増加しており、新しい脅威がさらに発生する可能性があります。セキュリティ対策は1回で終わるものではありません。定期的な更新やアップグレードで常にサイバー犯罪者の先を行かなければならない継続的なプロセスです。IoTとセキュリティについて熟知している専門家のパートナーがいれば、新しい脅威に対しても常に最先端の対応ができます。

お客様のIoTのセキュリティを今すぐ最適化する方法、IoTの今後の変化に備える方法につきましては、当社までお問い合わせください。

telenor IoT

TELENOR CONNEXION

Telenor IoTは、世界の主要な携帯電話事業者の１つであるTelenorグループのIoTソリューションです。20年以上にわたり、さまざまな規模の企業にグローバルなIoT接続、クラウドサービス、専門家によるサポートを提供してきました。現在、ボルボ、スカニア、日立建機、Verisure Securitas Direct、Husqvarnaなどの企業向けに1,700万台を超える接続デバイスを運用しています。IoTソリューションは、北欧地域においては各国のTelenorの事業部門を通じて、そのほかの地域ではTelenor Connexionを通じて提供されています。Telenor Connexionは、高度なサポートとカスタマイズを必要とする国際企業向けにIoTソリューションを提供するTelenorの子会社です。

iot.telenor.com

sales@telenorconnexion.com