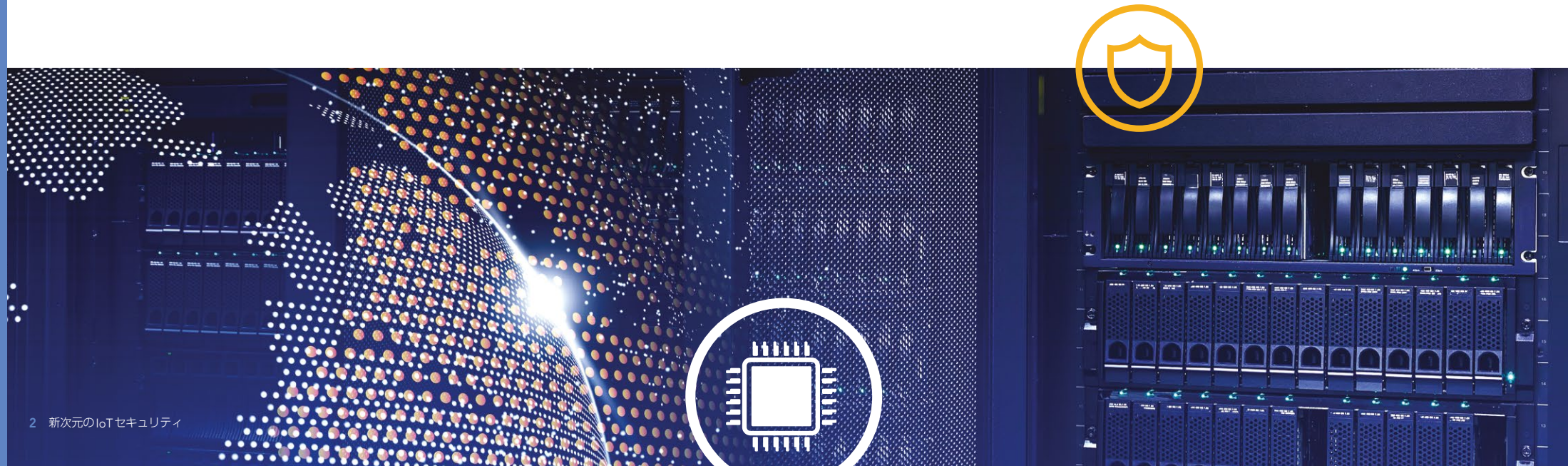
新次元の IoTセキュリティ

高い信頼性と操作性を

目次

新次元の IoTセキュリティ



01 今日のIoT

機会とリスクとの微妙なバランス

モノのインターネット（IoT）は、今ではごくありふれたものになりました。公共インフラ、産業用制御アプリケーション、医療機器から、スマートホーム家電、フィットネス・ブレスレット、自転車シェアリング・サービス、そしてもちろんスマートフォンやコネクテッド・カーに至るまで、IoTは私たちの身の回りに数多く存在しています。

急速に広がるIoT

IoTの経済効果は1兆ドル規模、IoTデバイスの数は数十億に及んでいます。2017年の市場分析報告書（Gartner, 2017）では、コネクテッド・デバイスの数はすでに50億を上回り、2020年までには120億を超えると予測されています。

この急速な成長に対応するため、Alibaba、Amazon Web Services、Google、IBM、Microsoftといった大手インターネット・プレーヤーが独自のクラウド・サービスの構築を進める中、業界のサプライヤーはプライベート・クラウド・サービスの拡張に向けて迅速に動いています。

コネクティビティが作り出す重大な脆弱性

残念なことに、コネクテッド・デバイスは、ネットワークへの不正アクセス、悪意のあるデバイス操作、あるいはIoT 収集データの盗用を図る人たちの恰好のターゲットになっているのが現実です。IoTのエコシステムの複雑化が、こうした危険を招いているのです。デバイスはさまざまなベンダーから供給されていて、セキュリティ・レベルもそれぞれ異なるため、想定外の脆弱性、予期せぬ結果、危険な動作につながる可能性があるからです。

たとえばエアコンであれ、洗濯機であれ、自動車であれ、IoTにつながった機器はその種類を問わずリモートで操作されたり、危険な動作を引き起こされたりする可能性があります。さらに、エネルギーや水の流通を管理するスマートグリッドが許可なく変更されたり不正にアクセスされたりした場合、人の健康や社会の安全に重大な危険が及ぶことがあります。

危害を加えたり情報を盗み取ったりしようとする人々は、すばやく行動して弱点を悪用し、不正アクセス、システムのハッキング、データの不正入手のための新しい方法を常に開発しています。それらは壊滅的な結果を引き起こします。

IoTの機会	IoTのリスク
• 資産活用度の向上 • リアルタイム最適化 • エンドユーザーに関する知見の拡大 • より良い意思決定 • 物理的資産のより自律的な動作 • より簡単に情報やサービスにアクセス	• サイバー犯罪、サイバー戦争、サイバーテロ • データの漏洩やプライバシーの侵害 • ボットネット、ランサムウェアなどのマルウェア • DDoS攻撃などのサービス妨害 • リモート操作による製品の誤動作 • 知的財産（IP）の盗難

復旧コストは甚大に

過去2年間だけでも、サイバー犯罪による経済的被害は1兆ドルを超えます。機密データを取り出すことのない、単に運用を妨害する限定的なマルウェア攻撃でさえ、企業にとっては、ビジネス·チャンスの喪失、信用の失墜、一時的な対策、製品のリコール、広報対応、および長期的な解決策のために数億ドルの費用がかかる可能性があります。怪我など賠償責任を問われる場合には法的費用も発生します。その他に、ランサムウェアが関連した場合のように、エンドユーザーにも被害が及ぶことがあります。

実害はなかったが、支払った対価は大きい

2015年 Fiat Chryslerは、一人のセキュリティ研究者が同社のコネクテッド·カー·ソフトウェアの脆弱性を見つけ、それがWired誌に掲載された後に、140万台の自動車をリコールしました。研究者たちは、実際に走行デモンストレーションでJeep Cherokeeの車載コンピューターの制御を乗っ取ることに成功し、リモートで車のスピードを上げたり、ブレーキを操作したり、場合によってはハンドルも操作しました。見つかった脆弱性に直接結びつく事故は起こっておらず、影響を受ける恐れのある自動車のリコールが予防的な措置であったにもかかわらず、Fiat Chryslerは、リコールおよび改修費用、ジープ·ブランドのイメージ·ダウン、賠償責任の可能性という高い対価を支払いました。

適切な保護の選択

あらゆるIoTデバイスには基本的な保護が必要だとわかってはいますが、そのセキュリティを実現する最適な方法は何でしょうか?

なにしろ、すべてのデバイスが同様のリスクに直面しているわけではなく、家庭のWi-Fiネットワークにつないだスマート·アクション·フィギュアと原子力発電所の制御機構は違うのです。そのため、保護のあり方と、それに伴う実装コストや維持コストとのバランスを取り続ける必要があります。

IoTデバイスのセキュリティを検討する場合、手始めに動作環境から考えるのが1つの方法です。デバイスは周囲のシステムとどのようなやり取りをして、それにどのようなリスクが関連するのか?

たとえば、どのIoTデバイスがクラウドにデータをアップロードするのか、どのクラウド·サービスにアップロードするのか?誰がそれぞれのデバイスをコントロールするのか?どのようなハードウェアがデバイスの動作に使用され、どのようなソフトウェアが実行を許可され、いつ実行されるのか?　そのIoTデバイスを使用すると料金は発生するのか? IoTデバイスは機密関連の機器やアプリケーションと共存するのか?といったことを検討するのです。

それぞれのデバイスを大きなエコシステムの一部として位置付け、そのエコシステム内の脅威を予測することで、どのような保護が最適で、それをどのように実装するのかが把握しやすくなります。

02 IoTデバイスを見守る

製造から廃棄まで

IoTセキュリティとは、ネットワークに接続している間だけデバイスを保護すればいいというものではありません。細工や悪用の機会は、IoTのエコシステム内のほぼすべてのポイントで、しかもIoTデバイスのライフサイクル全体を通して常に存在します。つまり、設計、製造から、サプライチェーン内の輸送、サブコンポーネントの組み込み、デバイスの流通、実装、そして廃棄の方法に至るまでが関わってくるのです。

製造と流通

工場やサプライチェーン内では、ICやデバイスにマルウェアの注入、偽造、キー・キャプチャ、バックドアの作成の可能性があります。

実装と運用

現場に実装した後は、細工やリバース・エンジニアリングといった物理的攻撃だけでなく、マルウェアの注入、不正接続、暗号化されていないデータの盗難、悪意のあるソフトウェアのアップデートなどの多様な論理的攻撃の可能性があります。

廃棄

ICやデバイスが役目を終えて使用済みとなる場合には、基板に保存された使用記録、個人情報、ログイン資格情報が、データ・アクセスの目的で、物理的細工、論理的改ざんの標的になる可能性があります。

危険は至るところに

最近のニュースでは、デバイス・セキュリティの脆弱性（暗号化されていない接続や信頼性に乏しいアクセス制御など）や、分散型サービス妨害（DDoS）などによる被害が取り上げられていますが、それ以外にも数え切れないほどの妨害行為があります。たとえばリモートのスケーラブルな攻撃では、物理的ハードウェア・レベルで情報を抜き出したり、メモリ内容を物理的に書き換えたりすることが可能になっています。これは最近までローカルな攻撃でしかできなかったことです。

攻撃のタイプ	攻撃の概要
ソーシャル・エンジニアリング	嘘、なりすまし、策略、賄賂、恐喝、脅迫など、個人が使う手口で、他者が情報システムを攻撃するように仕向ける。
脆弱なセキュリティ	適切に保護されていないシステムの攻撃。これには不十分なセキュリティ慣行が関係している。たとえば、暗号化、データ完全性、または認証のないまま接続する、デフォルトのパスワードや簡単に誰でもアクセスできるような無防備な資格情報を使って信頼性の低いアクセス制御を行う、総当たり攻撃や辞書攻撃で簡単にハッキングできるシステムを使う、ポートが開いたままになっているなど設定が不適切な通信スタックを使う、などが挙げられる。
脆弱性攻撃	ソフトウェアやハードウェアのバグなどのシステムの脆弱性を悪用し、データへのアクセス、任意コードの実行、サービス停止といった意図しない動作を引き起こす。
サイドチャネル攻撃	タイミング・シーケンス、電力消費、漏洩電磁波、さらには音といったシステム動作の物理的特性をローカルまたはリモートで検出および測定することで、鍵などの機密情報を推測し、システムへの不正アクセスやシステム破壊を図る。
故障注入	ローカルまたはリモート操作でシステムのハードウェアやソフトウェアを改変し、システム動作を狂わせる。メモリ・ロケーションの移動、ヒューズの細工、データバス上の値の変更など。
製造攻撃	生産時に被害を与える。知的財産（IP）や認証情報の盗難、セキュリティ・レベルの引き下げ、隠し機能の追加、機能性の改変（ソフトウェアを不正に改変する、偽コンポーネントを組み込む、など）。
ソフトウェア／ハードウェアのリバース・エンジニアリング	ソフトウェアの場合には、コードの仕組みをわからないようにするプログラム設定を解除することを狙い、ハードウェアの場合には、製造時に設けられた、回路構成を隠す物理的障壁を突破する。

ハートブリードの教訓

2014年の調査で、**ハートブリード**と呼ばれる極めて危険なバグが、OpenSSL（オープンソース暗号ライブラリ）に見つかりました。このバグにより、侵入検出システムを迂回し何の痕跡も残さないまま、秘密鍵、ログイン、パスワード、クレジットカード番号、eメール、インスタント・メッセージといった機密情報にリモート操作でアクセスすることが可能でした。

OpenSSLのコア開発者が見落としていて、2年近く誰にも気づかれることがなかったため、ハートブリードはインターネット・サーバ全体の3分の2に存在するとみられています。OpenSSLコミュニティは修正プログラムで迅速に対応したものの、すでに現場に埋め込まれたシステムすべてに修正プログラムを実装するのは非常に困難です。

修正プログラムによるアップグレードが必要なIoTの実装は今だに残っている可能性があります。だからこそ、IoTセキュリティが大部分は実装の問題であり、IoTデバイスが使う秘密データを適切に保護することが重要なのです。

守りを固めて、安心を得る

大切なインフラを守る

エネルギーや化学物質の生成や流通に関わる通信ネットワークも、破壊行為の潜在的なターゲットです。
SA/IEC 62443規格は、産業用オートメーションおよび制御システム（IACS）の電子的なセキュリティを実現する手順を規定したもので、こういった通信ネットワークを守るために作られました。
この規格の順守により、サイバー・セキュリティがスマートグリッドの展開と運用の一環として制度化されていることが保証されます。

社会と企業を支える

IoTアプリケーションの大半は、特にスマート・シティやインダストリー 4.0などでは、24時間の連続稼働が必須です。強固な認証、効果的なデータ保護、精確なコマンド制御のための業界標準の方法にサポートされ、十分に設計されたシステム構成は、スマート・ユーティリティ・グリッドであれ、工場の精密機械であれ、サプライチェーンの自動化であれ、スマート都市交通であれ、デバイス・セキュリティに関連して生じうるダウンタイムを最小限に抑えるのに必要な保護を提供します。

IoTの実装は、適切なセキュリティが確保されていると、ライフサイクル全体を通して保護されるので、効果的にデータを保護し、生産性を高め、運用を保証し、人々を危険から守ります。

個人情報を守る

好みや行動、購買習慣といった個人に関連する情報を扱うIoTの実装には情報の保護が求められます。2018年5月時点でEC内で企業活動を行っている組織には、EU居住者に関するデータの管理、保護、処理について定めた「一般データ保護規則（GDPR）」の順守が義務付けられています。

GDPRは、プライバシー保持のために欠かせない要件について詳述しているため、EU内に限らず、収集データの保全に関する指針として役立ちます。GDPRは支持を広げており、欧州ネットワーク情報セキュリティ庁（ENISA）は、検査および認定のための勧告と合わせて、セキュリティ規制の基本要件として採用することを提案しました。

健康と機密性を守る

医療デバイスやITネットワークを標的にした悪意あるプログラミング・コードやサイバー攻撃は、医療システムの破壊や人命にかかわる可能性があります。デバイスが集めた患者の医療記録や健康状態に関する情報の機密性は守らなければなりません。最近公表されたUL 2900-1基準では、ネットワーク接続可能な製品のソフトウェアのサイバー・セキュリティに触れ、医療用デバイスの評価と検査を呼び掛けています。米国では、食品医薬品局（FDA）のガイダンス・モデルとなっています。

03 真の防御は、
シリコン・レベルの
セキュリティから

IoTにダメージを与えようと思えば、様々な方法が可能です。そのため、接続デバイスには広範囲な防御が必要です。シリコン・レベルから保護すること、それがデバイスを脅威から守るうえで非常に有効です。理由は次の通りです。

01

シリコンは、デバイスの核です

ハードウェア、ファームウェア、ソフトウェアが異なる抽象化レイヤで動作する複雑なシステム構成の接続デバイスが増えています。各レイヤは、その下のレイヤのコンポーネントと動作に依存しています。

たとえばユーザー・インターフェースならオペレーティング・システムを、オペレーティング・システムはファームウェアを、そしてファームウェアはシリコン・レイヤで作動するハードウェア回路を信頼する必要があります。このようにセキュリティが階層化されるため、しっかりとした基盤が必要なのです。

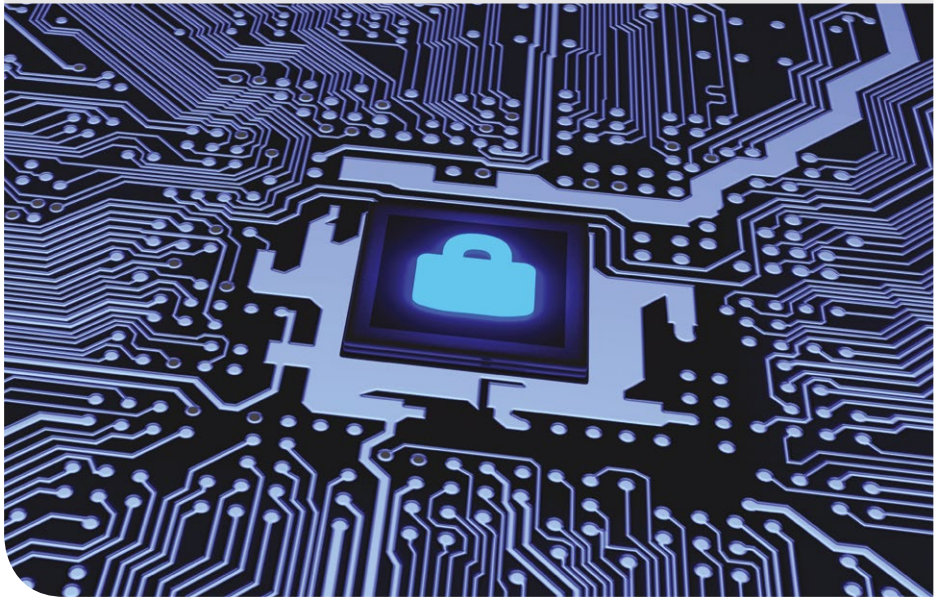
セキュリティは信頼の基点から始まります。シリコンは、信頼の基点を証明し管理するための強固な土台です。

02

信頼性の高いシリコン

このセキュリティ階層の起点、つまり抽象化レイヤを支えるベースは「信頼の基点」として知られています。信頼の基点とは、本質的に信頼できるもの、確実にリスクフリーだと信頼できるものを指します。信頼の基点がしっかりとしていると、セキュリティ基盤も堅牢になります。砂上に建ったブロック塀が不安定なのと同様、しっかりとした信頼の基点なくして電子システムのセキュア化はありえません。

シリコンは信頼の基点として理想的なソースです。命令行、メモリ内のデータ、オペレーティング・システム、ユーザー・インターフェースなどは改変やダメージを受けやすいのに対し、シリコンで物理的に隔離されたもの、すなわち外部からの影響を受けないシリコン内で保護されたプログラムやデータは信頼性が高く、改変に対する耐性を持っています。



03

導入時の留意点

セキュリティに必要なのは、完璧さです。導入時のごく小さな手違いであっても、脆弱性を作り出し、設計全体を危険にさらしてしまうことがあります。

効果的なセキュリティ・ソリューションは、厳密な開発プロセスの産物といえます。それには、設計ルールを明確に定義し、慎重な見直しを何度も繰り返し、設計に組み込まれるたくさんのサブコンポーネントを完全に制御することが求められます。

セキュリティ開発は、リスク特性を広い視野から捉えられるようシステム・レベルで考えることが大切です。そしてマルチレイヤのリスク緩和戦略と検証手順を整え、防御態勢を強化します。

消費者やサービス・プロバイダーからも、IoT製品のセキュリティ保全を求める声が高まっており、セキュリティ要件を順守していることを保証する第三者機関の評価も重要になってきています。

04 プラグ&トラスト

IoTセキュリティのための「プラグ&トラスト」手法

NXPでは、強固なセキュリティを実現することが必ずしも難しいことではないと考えています。

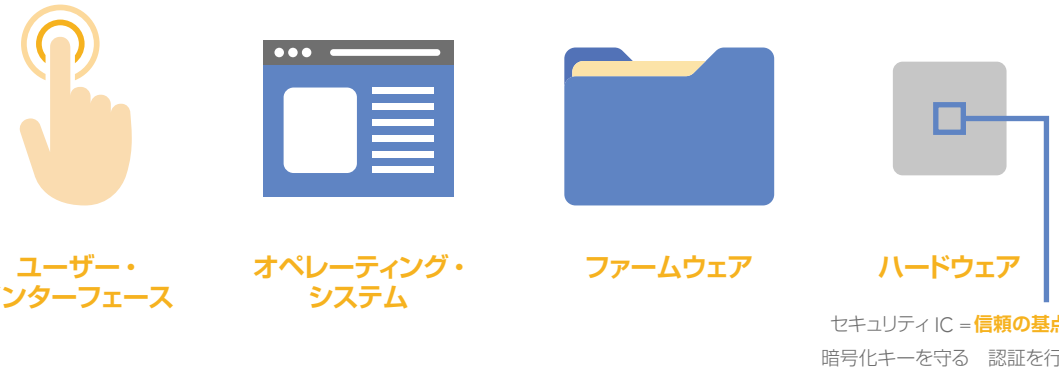
また、最も効果的なセキュリティ・ソリューションは安心感だけでなく簡潔さも実現するものと認識しています。NXPはIoTセキュリティを新しい視点から捉え、開発者が設計プロセスを効率化しながら保護機能を追加するための新たな手法を作り出しています。

NXPのシリコンをベースとしたセキュリティ・ソリューションは、IoTが生まれた当初から取り入れられてきました。その先駆的なソリューションを土台にして、アルゴリズムを改善し、アーキテクチャを進化させています。「プラグ&プレイ」手法がコンピューター設定を楽にしたのと同様、NXPの「プラグ&トラスト」手法は、今日のIoTデバイスのセキュリティ強化の手間を軽減します。

並外れた強靭さをもつ
「Root of Trust：信頼の基点」

NXPのスタンドアロン・セキュリティICには、IoT内での安全な動作に不可欠なステージング処理および認証を実行するための自己完結型の安全な環境が用意されています。セキュリティICは、IoTアプリケーション・ソフトとそれに付随する複雑性から重要なセキュリティ処理を切り離す障壁を設けるため、処理を安全なサンドボックス環境で実行することができます。

この隔離環境は、さまざまな攻撃シナリオを想定したハードウェアおよびソフトウェアによる100以上の対抗手段を講じて、セキュリティ・キーのために銀行級の保護機能でセキュア化されています。セキュアな不揮発性メモリがICに統合されているため、キーは安全に輸送、管理されます。また、セキュアな製造環境下でシリコン注入を施された専用のキー管理プロセスも提供されます。



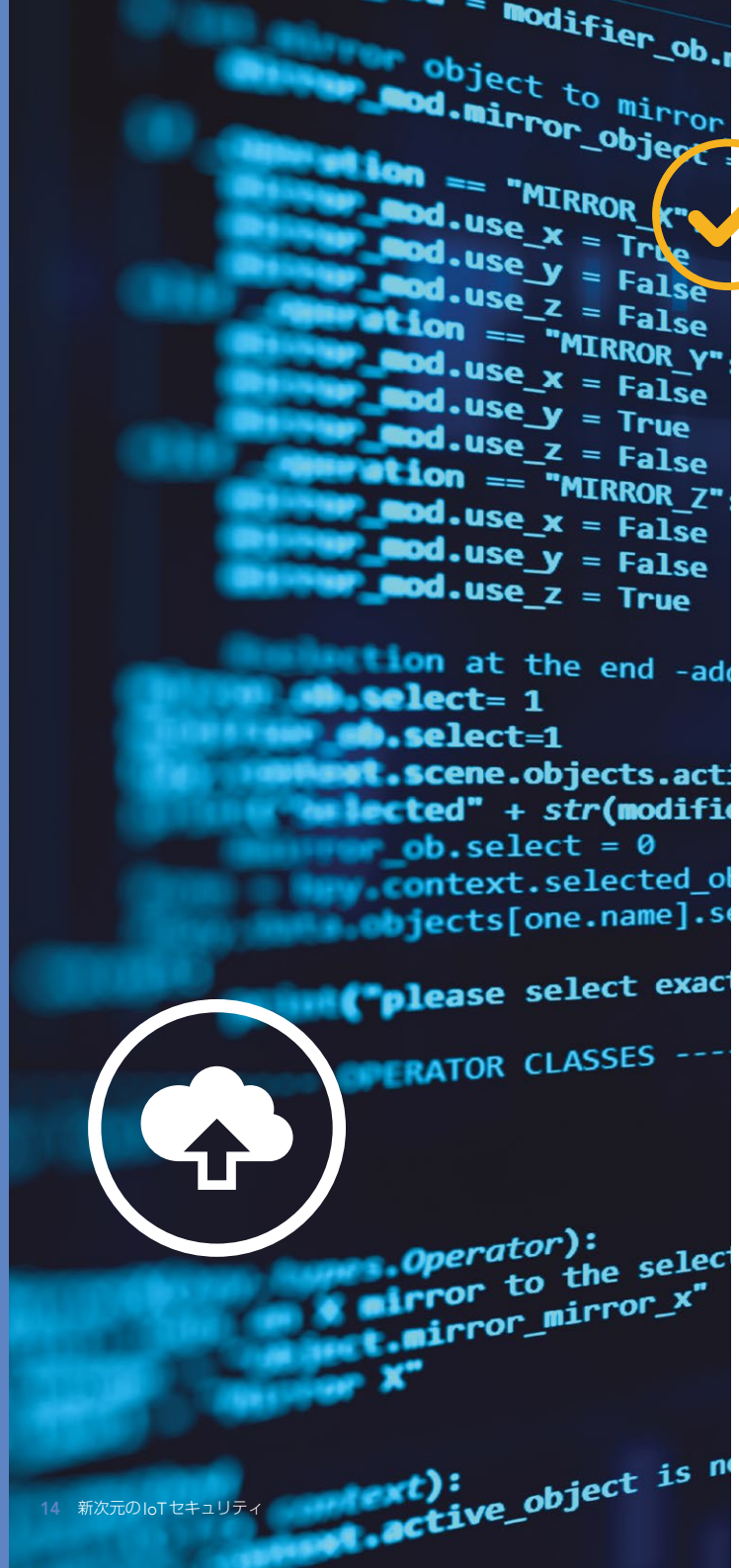
このようにして、セキュリティ認証情報はデバイスの製造から廃棄に至るどの段階でも保護されます。搭載データは信用でき、リアルタイム自動化システム用のコマンド・ソースも信頼できるとみなせるため、デバイスとの秘密情報のやりとりは交信中もセキュアに保たれます。通信は信頼性、機密性が保たれ、データは改変もなく一切損なわれることはありません。

接続を守る

接続は、IoT 操作の基本処理のひとつです。 IoT デバイスをネットワークやインフラ、クラウド内のサービスに安全につなげるにはまず、接続の完全性を確保し、データの機密性を保つために認証情報を守ること。

認証情報の保護を隔離し、接続のセキュア化の処理を、システムの残りの部分から切り離された状態で行います。接続の安全性は強化されてより堅牢なものとなります。

NXP の内蔵型ソリューションで、IoT プラットフォームとの接続も安全に行えます。ジャストインタイムでサービス登録ができ、難しい設定なしですぐに使えます。



高い信頼性

セキュリティ開発で必要なのは規律ときめ細かさであるという理念のもと、デバイスのライフサイクル全体を考慮し、関連する脅威を予測し、複数レベルで有効な防御態勢を構築して、安全、安心な環境を提供します。NXPのソリューションは、セキュリティ界の革命をもたらしたと言われ、コモン・クライテリアが認証した製品ラインナップは業界最高レベルの幅広さを誇ります。

デバイス・オリジンの安全性

製造元が疑わしい製品には、あとから攻撃が仕掛けられるようバックドアが作り込まれたものがあります。システム障害や物理的なダメージ、さらには人的被害にも及ぶようなかたちで信頼性が損なわれます。NXPのデバイス・オリジン・ソリューションなら、ライフサイクルのどの時点においてもIoTデバイスの安全性が確認できます。オリジン・データはデバイスのライフサイクルの期間中だけでなく廃棄処分後も機密性が保たれるので、ハッカーが情報を盗み出す恐れはありません。

無線アップデートでより安全に

ファームウェアをワイヤレス接続で配信するいわゆるOTA配信は、セキュリティ機能を最新の状態に保つ方法の1つですが、危険にさらされることがないよう、そのアップデート処理には注意が必要です。NXPのシリコベースのセキュリティは、OTA配信を保護する便利な方法を用意しており、ファームウェア・アクセスとバリデーションに関連するデータが入った信頼性のあるリポジトリを現場で安全に実装することができます。設定では、コードへのアクセス制御、コードのオリジンおよび完全性の検証、ファームウェアのロールバック回避（特に旧プラットフォームや資源に制約のあるプラットフォームを対象）がサポートされています。

エッジのセキュリティ強化

産業ロボット、最新のコンシューマ・デバイス、自動運転車など、複雑でプロセッサ・インテンシブなIoTデバイスは、クラウドからネットワークのエッジへと広がっており、デバイス内部でもよりエッジに近い処理が増えつつあります。エッジ・コンピューティングにより、大量のデータによるクラウド接続の負担を軽減し、特にリアルタイム・システムにおいては、レイテンシを抑えることで、処理のスピードアップを図ることができます。センシティブな詳細情報を取り除いた後のデータを収集情報としてアップロードするため、効率化とプライバシー保護の強化にもつながります。

NXPのセキュリティICの役割は、エッジ・デバイスを守ることです。クラウド接続を行わないスタンドアロン環境でも、また外部接続を行う場合においても、他ノードとのやりとりを安全に管理します。

高い操作性

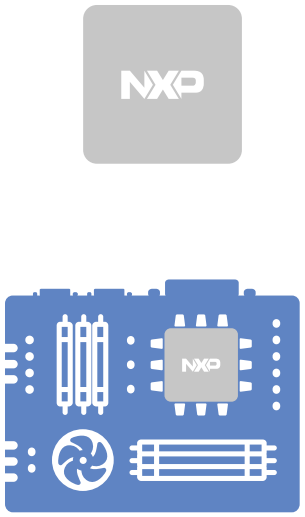
NXPのセキュリティ・ソリューションは、セキュリティを確保するために必要な処理を省略することなく、短時間で効率的に実行します。不正アクセスを防止し、データを守る仕組みを提供し、それらの機能を事前にソリューションに組み込ませることにより、少ない手順で実装を可能にします。

2021年初頭には
IoTコンピューティングの43%が
エッジで行われるようになると、
IDC は予想しています。

操作は、簡単な3ステップ

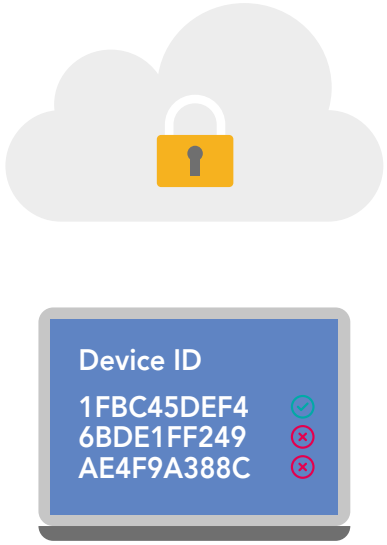
NXPのセキュリティICには、デバイスが社内外のクラウドにセキュアに接続するのに必要なカギを保存する機能があるため、3つの手順を踏むだけで接続ができます。事前に統合化されたオンチップ・アプリケーションには、セキュアなアクセスに必要なセキュリティ・コードがすでに入っているのです。

1.



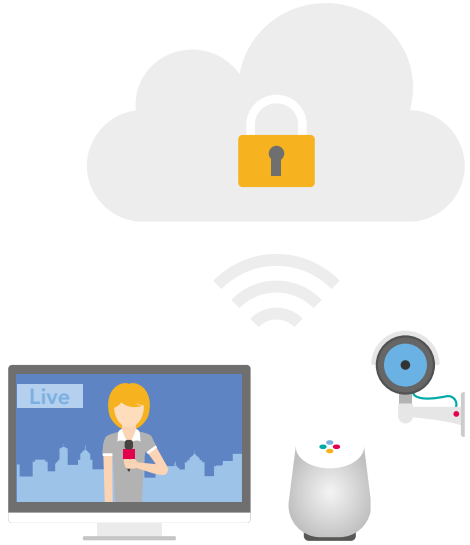
NXP **セキュリティ IC**を
ボードに組み込む

2.



認証機関の証明書をアップロード、
またはクラウド・ダッシュボードのデバイスIDを選択

3.



IoTデバイスをオンにし、
初期設定を**自動的**かつ**セキュア**に行うようにする

ゼロタッチ鍵管理

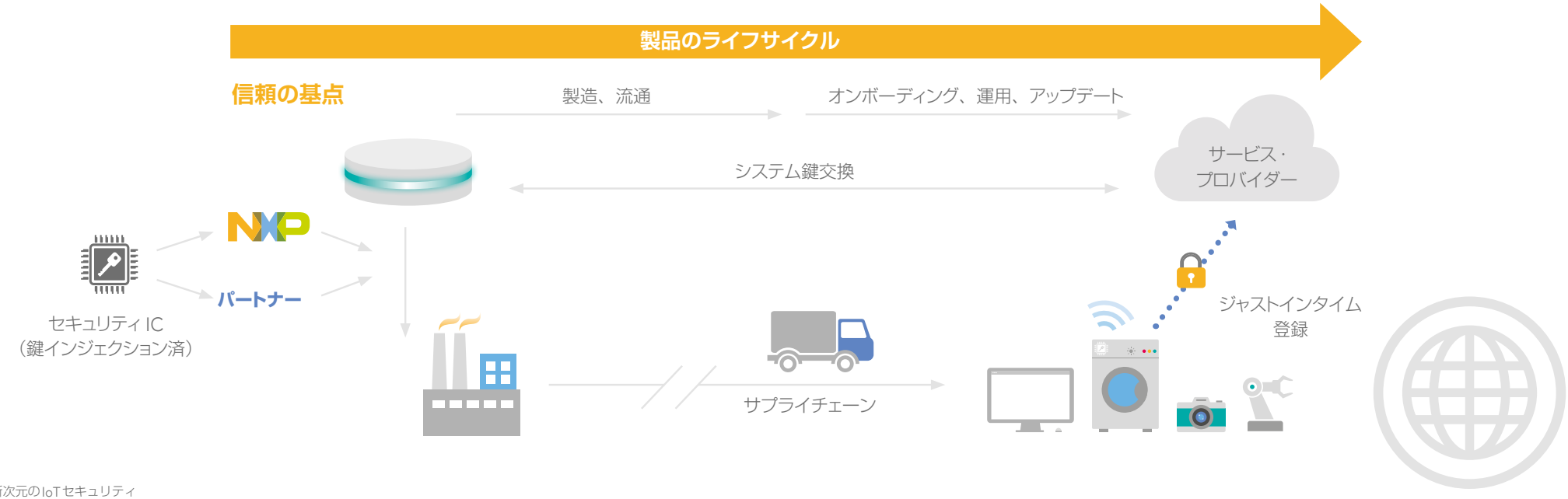
アクセスのセキュア化に必要な鍵と資格情報の生成は、比較的複雑なプロセスであるため、適切に行わないと脆弱性につながる可能性があります。マニュアル処理によるプロビジョニングでは間違いが起きやすく、デバイスの数が増えると対応が困難になります。また鍵の保全のため、鍵の書き込みは信頼性の高い環境下で行わなくてはなりません。つまり厳重なアクセス管理、人員の入念なスクリーニング、サイバー攻撃や認証情報の盗難を防ぐセキュアなITシステムなど、セキュリティが整った施設が必要です。チップ・レベルで実行するNXPのセキュア・トラスト・プロビジョニング・サービスがあれば、OEMの保有コストと鍵管理の複雑さが軽減され、IoTデバイスの初期設定もスムースにできるようになります。プログラミング・センターとの提携によりNXPは規模の大小を問わずあらゆるIoTデバイスへの実装を支援します。また、プロビジョニング・サービスを使えば、同一サービスに複数のサードパーティーOEMデバイスを接続する場合、サービス・プロバイダーとの鍵共有の調整をする手間が省けます。

迅速な統合

開発キットは主要ユースケースのサンプルコードや詳細なアプリケーション・ノート、そしてi.MXやKinetisマイクロコントローラの開発キットとの互換性とともに、コネクティビティ・スタックと統合されているので、開発者は設計プロセスをすぐに開始することができます。デバッグ・バージョンや手軽に利用できるサンプル・アプリケーションで、システム・インテグレーションの仕上げも簡単に行うことができます。

クラウド・プロバイダーとの協業で、エッジからクラウドまで広範囲にわたるセキュリティ・ソリューションを提供できるようになりました。特定のクラウド・プロバイダーとの連携作業専用の事前に統合されたソリューションは、複雑さを最小限にとどめ、IoTデバイスのセキュリティ開発に要する時間を短縮し、広範なエコシステム全体を通じてデバイスを守ります。

NXPセキュリティ・ソリューションで、エコシステム全体が守られます



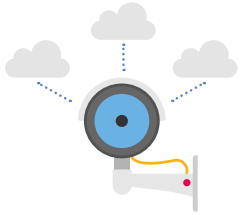
一か所で多面的なセキュリティを

統合が簡単、
ゼロタッチ・ソリューション

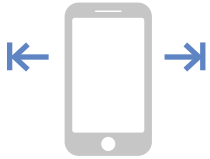
事前に実装された
セキュリティと
システムレベル・パフォーマンス

受賞実績で証明された
堅牢な手法

規模の大小を問わず
迅速に対応



マルチアプリケーション・
プラットフォームで
新規ビジネスモデルを創出



デバイスからエッジ、
クラウドに至る
エンドツーエンドのセキュリティ

製品ハイライト	
クラウド・サービスおよび エッジ・コンピューティング・ プラットフォームへのセキュアな接続	A710xCH（Amazon Web Servicesおよび プライベート・クラウド） A710xCL（Alibaba Cloud Services in China）
デバイス・オリジンの証明	A1006
計測インフラ	A70CU（英国） A80SM（ドイツ）

最先端をゆくNXP

IoTセキュリティの対象は1つではなく、また、どれをとってもまったく同じものはありません。だからこそ、NXPはデバイスが実際に稼働している期間を超えて、IoTのライフサイクルにおけるあらゆるステージ、あらゆる種類のIoTエコシステムに対するセキュリティ対策に取り組んでいます。高い処理技術と最新の接続性、堅牢なセキュリティを備えたNXPのポートフォリオはIoT開発のワンストップ・ショップといえます。多種多様な業界にセキュリティ・ソリューションを提供してきた実績に基づき、パートナー企業、OEM、システム・インテグレーター、サービス・プロバイダーなどの大手のエコシステム・プレーヤーと長期にわたる関係を築き上げてきました。NXPのソリューションは、エコシステムに貢献するモノをセキュリティに対する脅威から保護するように作られています。そして、NXPは一つ一つの新たな課題への挑戦から得られた経験より今日のIoTに最適なソリューションを生み出しています。

- **コモン・クライテリアが認証した製品を広範囲に取り揃え、セキュリティ業界をリード**
- **セキュアなマイクロコントローラにおける業界最先端の技術**
- **広範囲なソリューションを1社でカバー**
- **広範囲なエコシステム・パートナーとの関係**
- **規模を問わない機敏な対応**
- **新しいビジネスモデルを支えるマルチアプリケーション・プラットフォーム**

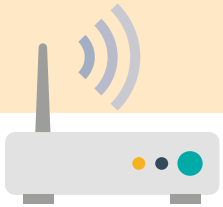
05 NXPセキュリティ

日常に
セキュリティを

NXPのシリコンベースのセキュリティ・ソリューションの用途は多岐にわたり、スマート・シティやスマート・エネルギーから、ホーム・オートメーション、パーソナルケア、インダストリー4.0、テレマティックスといったスマート・モビリティに至るまでさまざまなIoTアプリケーションに使われています。デバイスの接続とデータの秘匿性をセキュアに守るNXPのソリューションが日々の生活でどのように使われているのか、その実例をいくつか取り上げます。

「当社のスマート・ゲートウェイにNXPのセキュリティを組み込んだことで、顧客データの安全性と秘匿性を維持するという目標が達成でき、GDPRコンプライアンスにさらに一歩近づきました」

Dr. Neuhaus Telekommunication



スマートホーム

ENTRスマートロックでアクセス制御をセキュアに

高度な安全性を誇るセキュリティ・ロッキングやアクセス制御のソリューションのプロバイダーとして世界的に有名なMul-T-Lock社の**スマートロック「ENTR」**は、スマートフォンや指紋、個人コード、遠隔操作により自宅の玄関ドアを開けることができるサービスです。鍵を作ったり無効にしたりと、アクセス管理が自由自在にできます。認証情報を紛失したときはアクセスを取り消すこともできます。システムは電池式ですが、NXPの低電力セキュリティ・ソリューションを使っているので、セキュアなチャネル上でのBluetooth Low Energy (BLE) 接続が可能に。オフライン状態でも安心してモバイル・デバイスが使えます。

スマート・シティ

ドイツ: スマート・エネルギー・ゲートウェイに お墨付きのセキュリティを

NXPはDr. Neuhaus TelekommunicationやPower Plus Communicationといった**スマートメータリング・ゲートウェイ**のプロバイダーとの協働で、ドイツの情報セキュリティの政府機関であるBSIが発行した機密保持プロファイルの厳しい基準を満たしたセキュリティ・ソリューションを手がけました。NXPの埋め込み式セキュリティ・モジュールが、エネルギーやサービスのプロバイダーが報告する消費者用計測データへのアクセスや、計測データの転送を守っています。GDPRに準拠した設定で装備が進められました。

ユーティリティ計測

英国: セキュアなゼロタッチ試運転

長年にわたる国家プロジェクトの一環であるスマートグリッド・インフラは、1億個以上ものデバイス、住宅区域ハブ、ガスや電気メーター、家庭内のディスプレーなどを配して、エネルギー管理の最適化を目指しています。NXPの技術がそのインフラの大部分を守っており、NXPのセキュアな接続チップセットがハブやメーターの動作状況を国のデータ通信センターにゼロタッチで提供しています。セットアップに要する時間が分刻みで多大なコストとなるため、導入が簡単かつ迅速に行えることが重要です。NXPの画期的な手法は、優れたセキュア性能とシンプルさを併せ持ったものとして高い評価を受け、2014年度のスマート・メータリング欧州・英国サミットにおいて、サイバー・セキュリティのイノベーション賞を受賞したことで広く業界の注目を集めました。

明日への躍進を目指して

IoTセキュリティを実現するNXPの革新的ソリューションの
詳細につきましては、ウェブサイト
nxp.com/internet-of-thingsをご覧ください。

リリース：2018年2月（抄訳：2018年5月）