SafeNet

Internet of Things (IoT)

信頼できる基盤の構築

ガイドブック

目次

はじめに

Internet of Things (IoT)の展望

「Internet of Things（IoT）（デバイス=「もの」によるインターネット利用）」とは、既存のインターネットインフラ内で、一意に識別可能なデバイスが相互通信できる時代が到来したことを表現しています。ますますネットワーク接続を増していく私たちの生活に、より優れた知見と制御をもたらします。2020年までに全世界でおよそ500億[1]のデバイスが接続されると予測され、Internet of Things（IoT）は急速に実現しようとしています。

技術によって創出される価値と、新たな市場機会の可能性を考慮すると、Internet of Things（IoT）は今後10年で企業に14.4兆ドルの純利益をもたらすと推定されます[2]。あらゆる業界の組織が、この新時代によって提供される機会をとらえようとしており、独自のIoT戦略を開発・実施し始めています。

間違いなくInternet of Things（IoT）は大変革をもたらすものとなりますが、同時にセキュリティの考え方も変化させると見られています。保護を必要とするデータとデバイスの規模は、想像できないほどの数に膨れ上がっていきます。漏洩による結果の大きさを考えると、IoTの将来は、セキュリティ、信頼、データ整合性の基盤を構築できるかどうかにかかっていることは明らかです。

1 http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
2 http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf

Internet of Things（IoT）は何が違うのか?

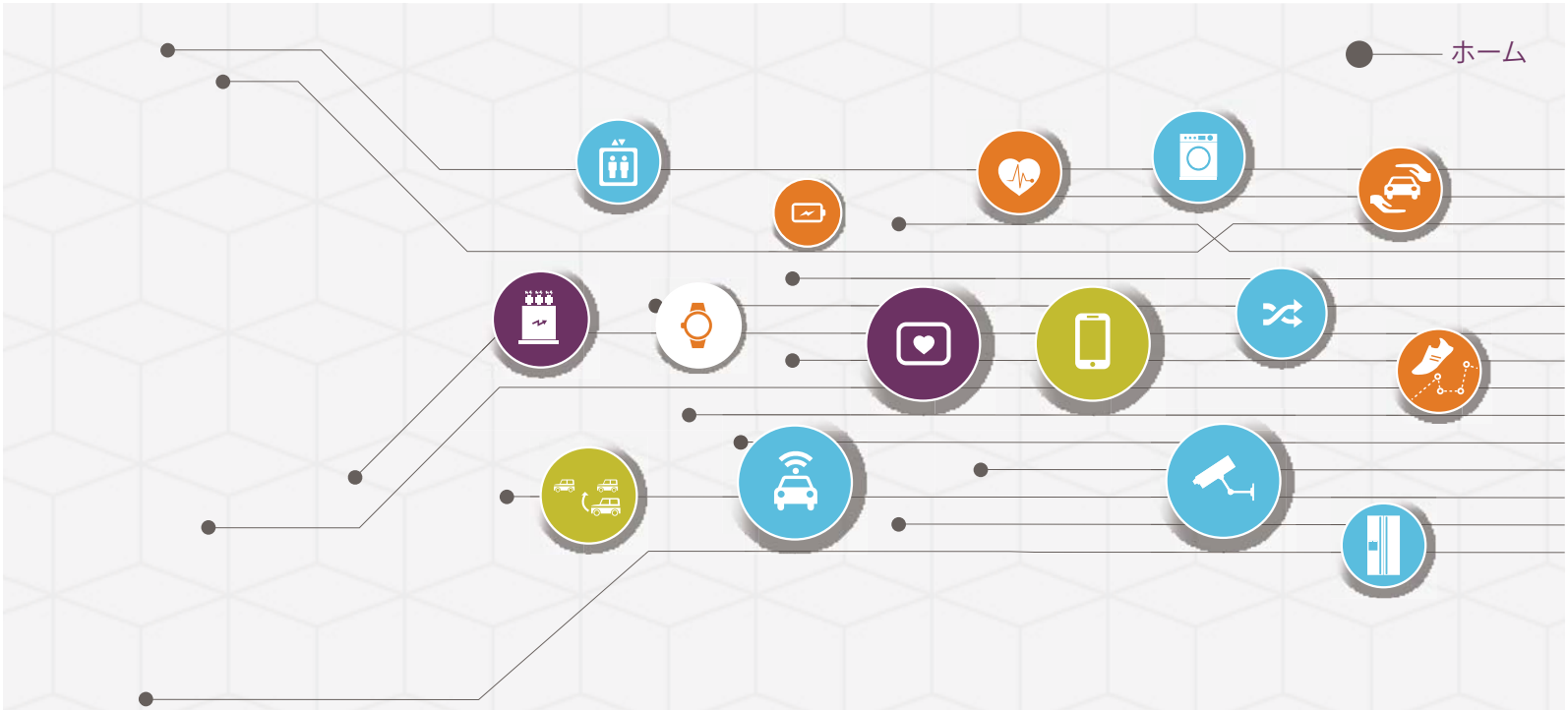
Internet of Things（IoT） は、数多くの様々な技術動向の頂点を代表するものです。IoTの導入は、モバイルコンピューティングへの移行を加速させ、クラウドへの依存を拡大させ、ビッグデータの価値を強固なものにします。では、Internet of Things（IoT）は、技術の観点からは何が違うのでしょうか?

あらゆる場所にあるIoTとデータ

モビリティはすでに実現しています。2000年代初めは、米国の成人人口のわずか半数強しか携帯電話を所持していませんでした。その後、所持率は90%以上にまで増加しました。モバイル技術の普及は、モビリティの次なる進化を円滑に進めました。今や誰もが、世界中のどこからでもデータやサービスにアクセスできることを当然のごとく期待しています。Internet of Things（IoT） の範囲は、自宅と会社という従来の境界を越え、さらに多くのデータと制御を移動することで、この問題を深刻化しています。

クラウドに配慮した設計

今日、クラウドはほとんどの企業でIT戦略の重要な要素であるだけでなく、当面の主要な技術動向の中心にあると見られます。この事実はInternet of Things（IoT）も確実に当てはまり、IoTにとってクラウド基盤は、大量のデバイス、接続、データを受け入れるためだけでなく、独自の革新的なソリューションを構築しようとする多数の中小企業や新興企業が求めるリソースを提供するためにも必要とされています。



ビッグデータがビッグディールに

Internet of Things（IoT）とは、データを収集し、ビジネスの取り組み方を強化させるためにデータを役立たせることです。デバイスから押し寄せる途方もない量のデータは、IoTソリューションプロバイダーに大きな課題を突き付けています。ビッグデータソリューションは、データを分析し、関連する傾向とパターンを発見する能力を提供することで、この課題を乗り越えることに貢献します。

IPを越えた通信

長年、インターネット通信は、通信相手を識別するためにIPアドレスに大きく依存してきました。IoTの一部のユースケースでは、より優れたセキュリティとより効率的な通信を、限られたパワーのデバイスを使用して実現できる新種の通信技術が必要になります。

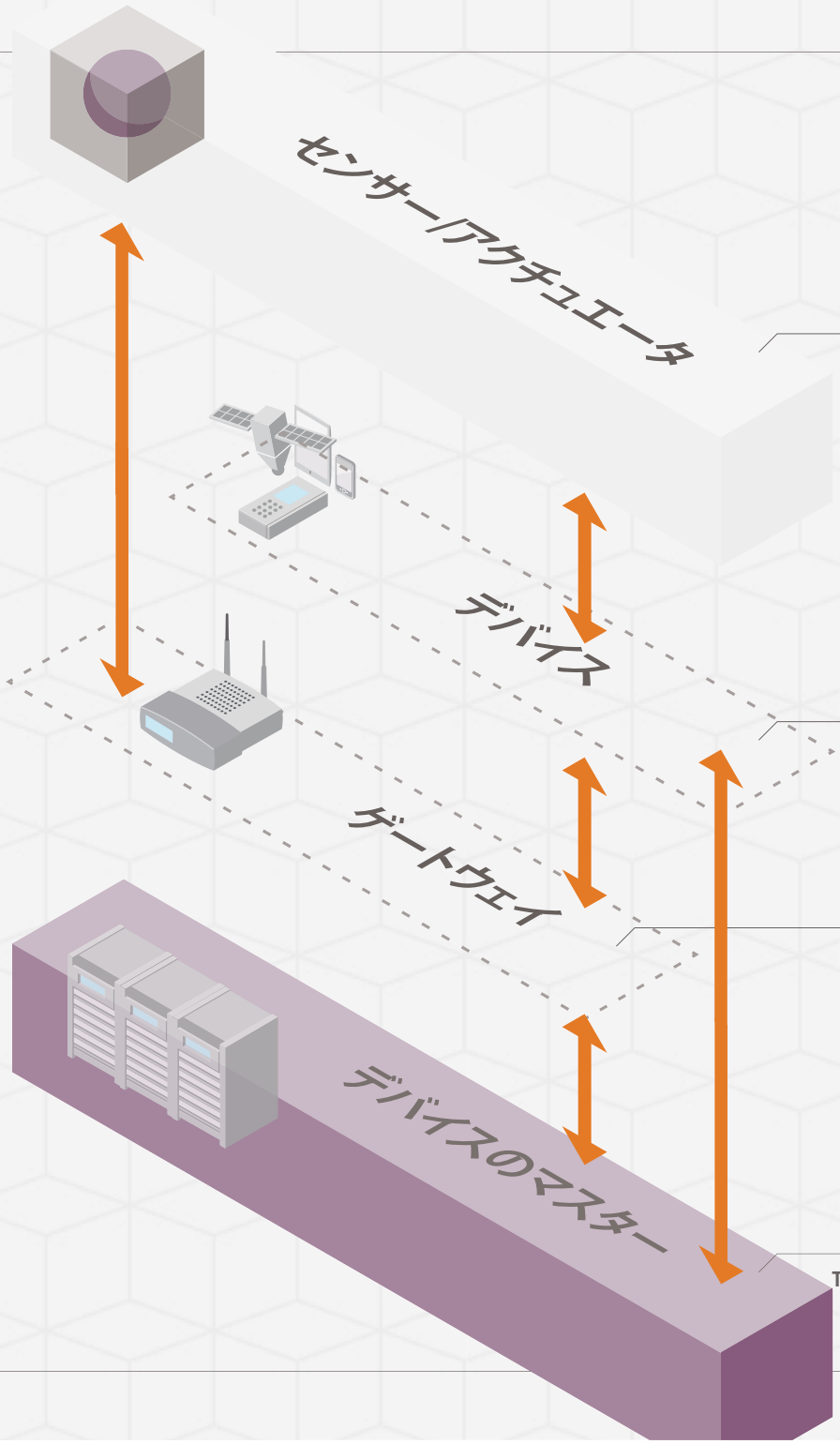
Internet of Things（IoT）の構成要素

センサー / アクチュエータ
センサーとアクチュエータは、データを監視、収集し、Internet of Things（IoT）の「THINGS（モノ）」を制御するツールです。

デバイス
簡単に言うと、デバイスは「THINGS（モノ）」です。センサーとアクチュエータを使用することで、これらのデバイスは想像を超えるほど直観的かつ効率的になります。

ゲートウェイ
IoTゲートウェイは、効率性の向上、直観的なデータの管理と分類、セキュリティ向上のために、デバイスのインテリジェントな通信を可能にします。

デバイスのマスターおよびサービスプロバイダー
Internet of Things（IoT）のすべてのデバイスやサービスにはマスターが必要です。マスターは、デバイスメーカー、クラウドサービスプロバイダー、またはIoTソリューションプロバイダーとなります。マスターの役割は、デバイスを発行・管理すること、またデータ分析を容易にすることです。



Things（モノ）の監視、
モノからのデータ収集、
Things（モノ）の制御

Things（モノ）

Things（モノ）の
通信をサポート

Things（モノ）の発行と管理、
Things（モノ）からの
データの分析

慎重な推進：IoTでのセキュリティ侵害

Internet of Things（IoT）は、データやシステムに対する脅威がこれまでになく大きくなっている中で出現しました。毎日平均13件の企業セキュリティ侵害があり、1日におよそ1000万、すなわち1時間に420,000もの記録が紛失しています。

新たな接続デバイスが発売されると、セキュリティ研究者はその脆弱性を明らかにするという課題に取り組み、適切なセキュリティなしにデバイスを接続することの潜在的な危険性を世界に広げています。次にいくつかの例を示します。

接続された自動車の操作

セキュリティ専門家のChris Valasek氏とCharlie Miller氏は、自動車の診断ポートに繋いだノートパソコンを使用してトヨタ・プリウスとフォード・エスケープをハッキングし、接続された自動車の脆弱性を明らかにして世間の注目を浴びました。この研究では、自動車のヘッドライト、ハンドル、ブレーキの操作が可能でした。

医療機器に対する脅威

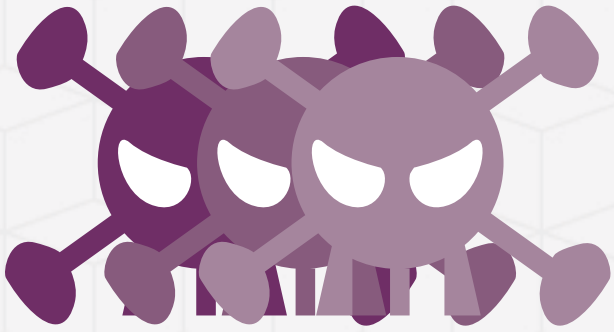
2014年4月、Scott Erven氏とそのセキュリティ研究者チームは、医療機器の脆弱性に関する2年にわたる研究結果を発表しました。この研究は、患者の健康と安全に重大な脅威を与える可能性がある主要なセキュリティ欠陥を明らかにしました。チームは薬剤注入ポンプの投与量レベルを制御する装置や除細動器などの医療機器を遠隔操作できることを発見しました。

スマートグリッドの危険性

2012年、米国国土安全保障省は、強固なスマートグリッドとルータのプロバイダーであるRuggedComのデバイスに欠陥があることを発見しました。エンドユーザーとRuggedComデバイス間のトラフィックを復号化することで、攻撃者は送電網を危険にさらす攻撃を開始できる恐れがあります。

3つの主要な攻撃ターゲット

Internet of Things（IoT）に対して起こり得る攻撃は、攻撃のターゲットを基に次の3つの主要カテゴリに分類できます。**デバイスに対する攻撃**、**デバイスとマスター間の通信に対する攻撃**、**マスターに対する攻撃**です。



デバイスに対する攻撃

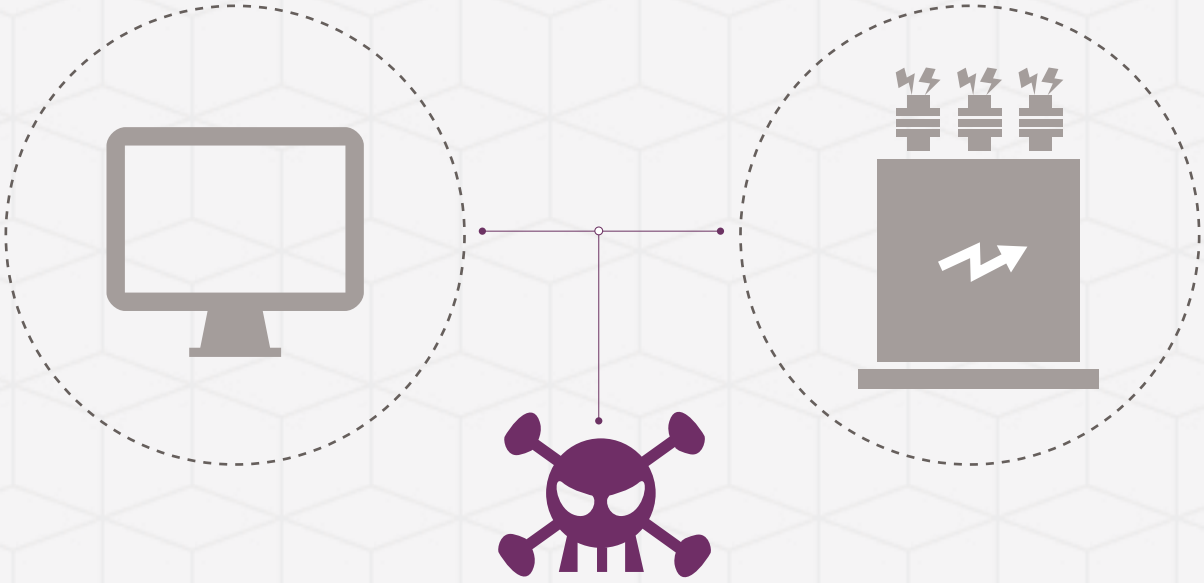
攻撃をたくらむ者にとって、デバイスはいくつかの理由により興味深いターゲットになります。まずデバイスの多くは、その機能の単純な性質によってもたらされる固有の価値を持ちます。たとえば、接続された監視カメラが侵害を受けた場合は、その場所の警戒態勢に関する重大な情報を提供する恐れがあります。

次に、デバイスは物事を制御し管理する信頼された機能を持つため、物事に影響を与えられるという価値があります。これは、自宅や会社の照明を制御するような単純なものから、身体に害を及ぼす恐れのある方法で自動車や医療機器を制御するような悪質なものまであります。

最後に、デバイスにはそれに委ねられた役割に基づく価値があります。たとえば、スマートグリッドは、接続されたメーターが本物かつ正確であると信用されています。ハッカーは1つのメーターを操作して、電気代を減らしたり自宅や会社への電力供給を否定しようとしたりします。それどころか、もし十分な数のスマートメーターが操作された場合、より広範囲の送電網を不安定にしてしまう恐れがあります。

通信に対する攻撃

攻撃の一般的な方法のひとつとして、通信中のメッセージの監視や改ざんが含まれます。メッセージは移動中に傍受・取得・操作されるため、IoT環境を移動するデータの量とセンシティビティはこの種の攻撃を特に危険なものにします。これらすべての脅威が、伝送される情報やデータの信用性、インフラ全体に対する大きな信頼性を危険にさらします。たとえば、自宅や会社から公益事業会社までのエネルギー消費に関する情報は、それ自体が数多くの脅威につながります。例としては次のようなものがあります。財産を奪おうと計画する者が、自宅や会社の不在や活動の時間を確かめようとエネルギー使用を追跡する恐れがあります。また、公益事業会社に伝送されるデータを操作して情報を改ざんする恐れがあります。



デバイスのマスターに対する攻撃

メーカー、クラウドサービスプロバイダー、IoTソリューションプロバイダーに対する攻撃は、最大の被害を及ぼす可能性があります。これらのメーカーやプロバイダーは、大量のデータを一任されており、その一部は極めてセンシティブな性質を持ちます。さらに、このデータはIoTプロバイダーにとって分析の中核となる戦略的なビジネス資産であるため、価値が高く、データが漏洩した場合は重大な競争力の低下をもたらします。

デバイスへのサービスの中断も脅威をもたらします。デバイスの多くが機能を発揮するために、マスターとの通信能力に依存しているからです。

マスターへの攻撃は一度に多数のデバイスを操作する機会を示しており、その一部はすでに現場に配備されている可能性があります。たとえば、ファームウェア/ソフトウェアを頻繁に更新するプロバイダーは、そのメカニズムによって、悪質なコードをデバイスに取り込んでしまう危険にさらしている恐れがあります。

IoTのセキュアな基盤の構築

IoTは多くの点で大変革をもたらすものになる可能性を秘めていますが、セキュリティの観点からはほとんど変化がありません。最も基本的なレベルでは、Internet of Things（IoT）のセキュリティは、デバイスとそのマスターを識別して、デバイスとマスターが管理し共有するデータを保護することを意味しています。

信頼できるデバイス

信頼できるデバイスとは、確実に識別でき、メーカーやプロバイダーと関連付けできるものです。デバイスは、同タイプの他のデバイスとともに、マスターとも通信可能でなければなりません。

デバイスの識別

信頼できるデバイス

- 確実な識別
- メーカー／プロバイダーとの関連付け
- マスターや他のデバイスとの安全な通信

セキュリティニーズ

- アイデンティティを確立してサービスや他のデバイスに対する認証を容易にする、製造時点で各デバイスに発行されるデバイスID証明書

信頼できるマスター

信頼できるマスターとは、従属デバイスと安全に通信し、コードが本物であり改ざんされていないことを保証する方法でデバイスにファームウェア／ソフトウェアアップデートを発行するものです。

マスターの識別

信頼できるマスター

- デバイスと安全に通信
- 信頼できるファームウェア/ソフトウェアの発行

セキュリティニーズ

- デジタル証明書で署名されたコードを使用したファームウェア/ソフトウェアアップデートのコード署名
- SSL証明書を使用した現場のデバイスとのSSL通信

データの整合性

クラウドおよびIoT環境を移動する機密データは、傍受を防止するために暗号化が必要です。同様に、保存データは盗難を防止するために、透過的かつシームレスな暗号化が必要です。

データの整合性

データ暗号化

- 保存機密データの透過的かつシームレスな暗号化
- 移動中データの暗号化

セキュリティニーズ

- パフォーマンスに影響を与えることなく、ビッグデータクラスタに保存機密データをロックダウン
- IoTおよびクラウド環境を移動するデータの保護

Internet of Things（IoT）に対する信頼できるアイデンティティの確立

公開鍵暗号（PKC）は、互いに面識がないユーザー間で信頼できるセキュアな通信を実現するために特別に開発されました。つまり公開鍵暗号は、アイデンティティに対する信頼を提供する手段です。Internet of Things（IoT）が一意に識別可能なデバイスのネットワーク上に構築されていると考えると、公開鍵暗号はIoTにおいて信頼できるアイデンティティを確立する上で極めて大きな役割を果たします。

公開鍵暗号は、データの暗号化に用いられる2つの異なる数値間の特別な固有関係の概念に基づきます。数値の1つは公開され（公開鍵）、もう1つは非公開にされます（秘密鍵）。この2つが対になっている場合にのみ、その関係が本物であると見なされます。暗号化と復号化に別個の鍵を使用するため、非対称暗号化とも呼ばれています。

しかし、乗り越えなければならないハードルがさらにもう1つあります。対象となる鍵が本当にその所有権を主張している人物のものであることを確認する必要があります。これは、その鍵が本当にその人物のものであることを保証する、デジタル証明書を発行する認証局（CA）によって効果的に行われます。

デジタル証明書を仮想パスポートと考えてください。パスポートには、審査機関が本人の身元を確認しやすいように、本人の顔写真、名前、国籍、生年月日、出生地などが記載されています。同じようにデジタル証明書には、対応する公開鍵について、デバイスやシステムのアイデンティティを確立し確認するのに役立つ、いくつかのフィールドが含まれています。

デジタル証明書

- ✓ 発行認証局を識別する
- ✓ 証明書の所有者を識別する
- ✓ 証明書の所有者の公開鍵を組み込む
- ✓ 認証局の固有の秘密鍵でデジタル署名される

数百億もの証明書がモノのインターネットの一部として発行されています。これらの証明書は、デバイスの識別、ファームウェア/ソフトウェアアップデートの署名、暗号化通信の容易化に使用されます。公開鍵暗号の使用とデジタル証明書の発行を管理するために必要な公開鍵基盤（PKI）の規模は膨大なものになります。幸い、現在ではPKIのセキュリティ、効率性、管理のしやすさを強化できる信頼性の高い実証済みソリューションセットが市場に出ています。

IoTの公開鍵基盤のベストプラクティス

前のページで説明したアイデンティティ基盤全体は、公開鍵と秘密鍵を基礎としています。公開鍵は自由に入手できるようにする必要があるため、問題ありません。しかし、秘密鍵は非公開かつ安全に保持する必要があります。さもないと、アイデンティティへの信頼が損なわれてしまいます。

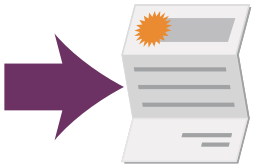
したがって、公開鍵と秘密鍵の安全な生成と保管は最重要事項です。選択肢は、使用するオペレーティングシステムで動作可能なソフトウェアで実行するか、あるいはシステムに安全に接続されたハードウェアの信頼のルート内で実行することです。

暗号鍵が他のシステムコンポーネントと同じサーバー上に保管された場合、その暗号鍵へのアクセスは極めて容易になり、システムを危険にさらします。これはソフトウェアで暗号鍵を保管する暗号化ソリューションの大きな弱点です。

米国国立標準技術研究所（NIST）は、信頼のルートを、1つ以上のセキュリティクリティカルな機能を実行するために本質的に信頼できるコンポーネントとして定義しています。暗号鍵の保護、デバイス認証の実行、ソフトウェアの検証が3つの例です。これらのコンポーネントはセキュリティに配慮した設計でなくてはならず、NISTによれば、理想的に実装され、耐タンパ性のハードウェアによって保護されなくてはなりません。信頼のルートは、サーバー上のソフトウェアと暗号鍵マテリアルの間に障壁を築きます。このアプローチであれば、機密の暗号鍵にアクセスしようとするハッカーの攻撃意欲を大幅に削ぐことができます。

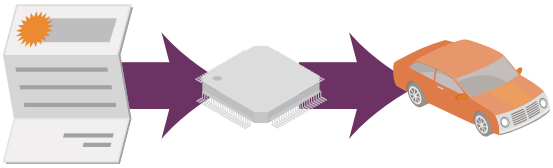
1. ID／証明書作成

証明書発行元
シリアルナンバー
有効期限開始日
有効期限終了日
公開鍵
デジタル署名



デバイスID

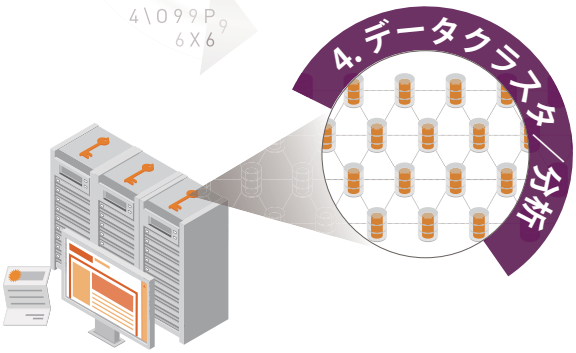
2. デバイスメーカー／IDとともに提供

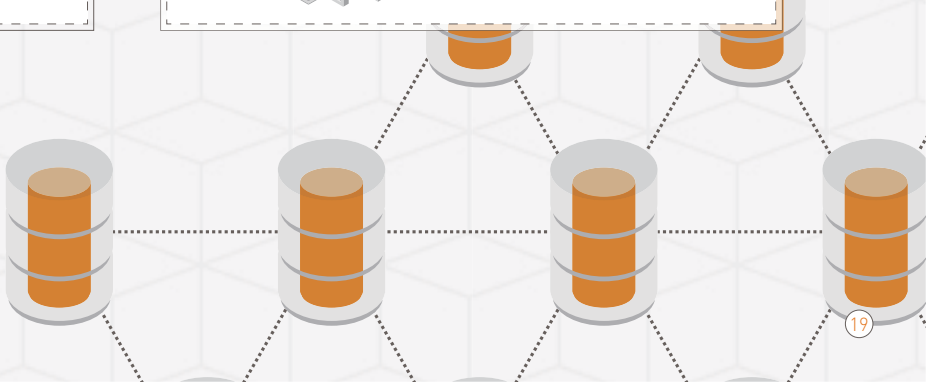


デバイスID　　デバイスA

3. デバイス間／デバイスとデバイスのマスター間の通信

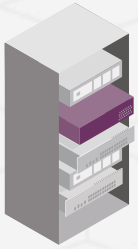
デバイスA　　デバイスB





暗号化による データの保護

Internet of Things（IoT）では、収集・伝送・保存されるデータの機密性を保つために、暗号化によるデータの保護が必要となります。また暗号化は、デバイスとクラウド間、デバイスとモバイルアプリケーション間を通過するデータを保護する役割を果たします。



Data-at-Rest（保存データ）の保護: ビッグデータの暗号化

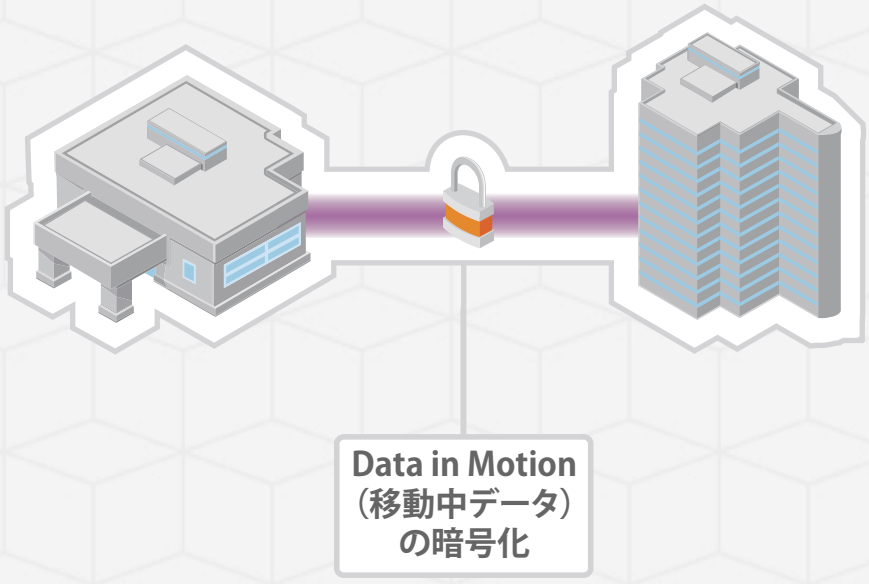
ビッグデータとは、要はスケーラブルでコスト効率の良いストレージの提供と、データを役立てるための大規模なデータセットの高速処理のことです。残念ながら、このデータの保護は組織にとって重大な課題となっています。通常、このデータは数百から数千のデータノードに散在するクラスタに保管されます。このうちのほとんどは保護されておらず、各データノードが悪質な侵入者や犯罪者の潜在的なエントリーポイントになっており、不正なユーザーやサービスがアクセスすると、機密データがはっきり見える状態のままで置かれています。これは、組織にとって重大で、かつコストがかかる可能性のあるリスクです。

組織は、ビッグデータの価値を発見するためにスケーラビリティと効率性を十分に利用することと、組織の高価値な情報を保護することの間で、綱渡りを演じることを強いられています。この課題を乗り越えるには、パフォーマンスに影響を与えずに、ビッグデータクラスタの機密の保存データをロックダウンできるようにしておく必要があります。そのためには、これらの分散したノードで機密データを保護できる、透過的で自動化されたファイルシステムレベルの暗号化が必要です。

Data-in-Motion（移動中データ）の保護: 通信の暗号化

IoTエコシステムを移動するデータの保護は、特有の課題を示します。デバイスを出入りするデータの多くがパブリックネットワーク上で通信されるため、通信は、インターネットで他の通信を保護するのとほぼ同じ方法で保護する必要があります。TLS（Transport Layer Security）とSSL（Secure Socket Layer）はこの目的に利用できる確立した暗号化プロトコルです。このアプローチは、課題がないわけではありません。それは、非対称暗号がパフォーマンスに与える負荷です。楕円曲線暗号（ECC）の登場と、その標準としての導入は、この課題を乗り越える上で大きな役割を果たします。

さらに暗号化は、メーカー、クラウドサービスプロバイダー、IoTソリューションプロバイダーのバックエンドインフラレベルでも必要です。データはある場所から別の場所へ移動するため、光ファイバ盗聴などの攻撃に対して非常に脆弱です。データはネットワークを流れるため、ハッカーは検出されずにエバネセントファイバ結合デバイスをケーブルに接続できます。ハッカーはネットワーク上で実行されるすべてのアクティビティを記録し、気付かれることなくデータを取得し、盗みます。暗号化が十分でない場合、この種の攻撃はデータの変更にも利用できるため、システム全体の制御をのっとる可能性があります。



M2M通信モジュール
LETおよび3Gモジュール

オートモーティブ、インダストリアル分野での国内採用プロジェクトの立ち上げ、製品化サポートでの下記の実績があります。

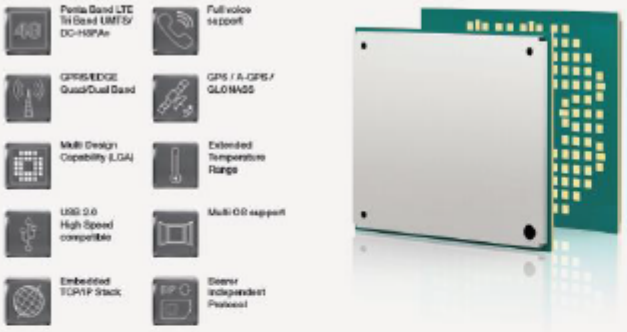
- 建機・農機のグローバル監視（大手複数社採用）
- ハンディーターミナル/R-PDA（複数社採用）
- 車載トラッキング・EV監視（多数採用）

携帯電話無線ネットワーク（GSM,GPRS,UMTS,LTE・・・）

LTE

Cinterion® PLS8 Wireless Module
First Industrial 4G LGA Module in the Market

PLS8



HSPA+

Cinterion® PHS8 Wireless Module
The Thinnest 3G LGA Module in the Market

PHS8

3G

Cinterion® PDS8 Wireless Module
Global 3G with Java™ embedded and GPS

PDS8

Dual/Quad Band
Cat 1 LTE single mode, Linux

ELS5/3

ライセンス管理モジュール Sentinel Embedded

Sentinelのソフトウェアライセンス管理ソリューションにより、
IoTデバイスでの下記の対応が可能となります。

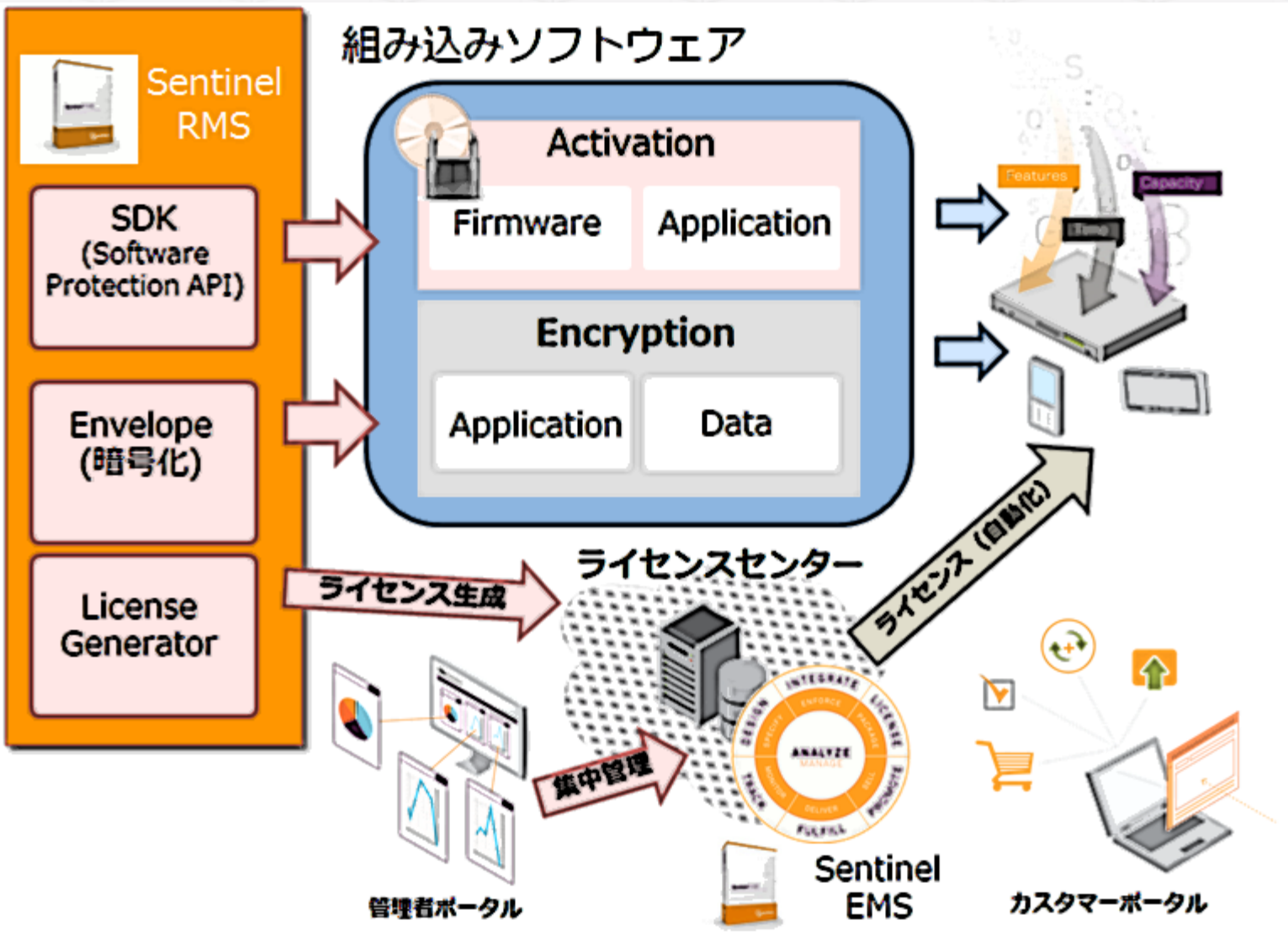
- デバイスのクローニングでのファームウェアの不正使用防止
- プログラムの改ざんおよびリバースエンジニアリング対策
- ソフトウェアのバージョン管理
  （セキュリティパッチなどへの迅速かつ漏れのない対応）
- IoTデバイスとERPおよびビックデータを連携可能

①プログラムソースに
ライセンスAPIを
組み込む

②機能の組み合わせにより
様々なライセンス体系を
生成

③機能のアップグレード、
リニューアル、サポート処理を
効率的に実施

組み込みデバイス向けライセンス管理ソリューション



すべての物は他の全ての物と関係している

-レオナルド・ダ・ヴィンチ

日本セーフネット株式会社

東京都港区新橋6-17-17　御成門センタービル 8F
Tel: 03-5776-2751
Email: jp-info@safenet-inc.com
HP: http://WWW.safeNet-inc.jp