SafeNet

SENTINEL
SOFTWARE
MONETIZATION
SOLUTIONS

“モノのインターネット”時代のソフトウェアライセンス／エンタイトルメント管理

ホワイトペーパー

IoT（Internet of Things：モノのインターネット）の可能性に注目が集まっています。IoTをベースとした新しいアプリケーションを構築し、自社のソリューションの機能を強化することは、OEM事業を手がける多くのソフトウェア企業にとって最優先事項となっています。

たとえば、インテリジェントな組み込みデバイスを介してビッグデータを取得または分析し、新たな考察を得る――そういった仕組みの先進的なIoTアプリケーション／サービスを開発することで、企業は大きな収益が見込むことができます。素晴らしい話ですが、もちろんいくつかの課題もあります。

とりわけ、セキュリティの問題は避けては通れません。インターネットに常時接続し通信するソリューションにおいて一定レベルのセキュリティを確保することは、組み込み系の開発者／エンジニアにとって最大の障壁となります。

本ホワイトペーパーでは、このようないくつもの課題をクリアして、IoTアプリケーションをしっかりと収益化していく方法について考察します。ここで、有効な解決策としてとりあげるのは、高度なソフトウェアライセンス／エンタイトルメント管理のアプローチです。このアプローチによって企業は、IoTアプリケーションのセキュリティレベルと収益化の両方を強化することが可能になります。さらに、ソフトウェアライセンス／エンタイトルメント管理ソリューションに備わる「フィーチャーベースのライセンシング」が、IoTアプリケーションが求めるスタイルで、最適なビッグデータを生成できることも示しています。

IoTの世界には、収益化の機会が実に豊富に存在しています。MarketsandMarketsの予測によると、IoT市場と関連するM2M（Machine-to-Machine）通信市場の規模は、2017年までに2,900億ドルに達し、2012年から2017年までの年平均成長率（CAGR）は30.1%になると目されています。またIDATEは、2020年までにスマートフォンから車、冷蔵庫、衣服に及ぶ、800億台ものデバイスがインターネットに接続されると予想しています。一方、IDCの予測はもう少し慎重で、インストールベースでの全世界のIoTの CAGRは17.5%まで成長し、2013年末時点の91億台から、2020年には281億台に達すると見積もっています。

IoT市場には、アプリケーション、分析、サービス、アプリケーションイネーブルメントプラットフォーム、コネクティビティ、インテリジェントデバイス（サイバーフィジカルシステムを含む）などの多様な技術分野を含み、これらの技術は既存のIPベースの接続の下、人が介在することなく通信を行います。IDCによると、2013年時点で1兆9,300億ドル相当だったこの市場が、2020年には7兆700億ドル相当にまで成長し、その際にインストール台数の90%を先進地域が占めると予測されています。

今後、IoT製品はますます差別化が進み、とりわけスマート分析やスマートアプリケーションを組み込んだ包括的なソリューションとして市場競争が激化していくでしょう。Transparency Market Researchの研究では、全世界のビッグデータ市場は2012年から2018年にかけてのCAGRが40.5%に達し、63億ドルから483億ドルに激増すると見積もられています。

Gartnerの最新の技術ハイプサイクルによると、市場が一定のアプローチに落ち着いてきたビッグデータは現在、成長曲線のピークを過ぎたフェーズだと見られています。ここで言うアプローチとは、基本的に、新しいテクノロジーとプラクティスは既存のソリューションに追加されるという傾向を指しています。組織が新しい事業や収益チャネルを開拓していくうえで、ビッグデータについては、その利用価値に対して現実的なスタンスが取られることになります。

一方で、IoTアプリケーションは現在、成熟したビジネスモデルに向かっていく渦中にあります。では、IoTアプリケーションは、実際にどのような領域で利用されるのでしょうか。また、どのようなタイプのデータに誰が対価を払いたいと考えるのでしょうか。

多様な利点を持つ、複数のアプリケーション領域

IoT自体がそうであるように、IoTアプリケーションは実に広範な市場です。専門家や個人などのエンドユーザーだけでなく、サービスプロバイダー側にとっても多種多様な利点をもたらすと期待されています。たとえば、気象観測計は気候動向分析のためのビッグデータを提供します。在宅ケア用の製品は、高齢者がより長く自宅で過ごせるようにします。スマートパッケージやスマートコンテナは物流の改善に貢献します。

市場のセグメントが異なれば、需要もまた異なります。代表的なものでは、IoTデバイス知能、セキュリティ、収益化、そしてビッグデータの作成などの需要です。以下に2つの例を挙げます。

- 産業用機械は、可視化およびリアルタイム機械制御用のハイレベルな組み込み型の知能を備えています。この分野が浸透してきた結果、産業用機械や関連する知的財産を、窃盗や改ざんから保護する必要性が高まっています。さらに、多数のセンサーが接続されていることから、産業用機械は大量のビッグデータを創りだすことが可能であり、そこから生み出される膨大なデータをも安全に保護する必要があります。それには、オンデマンドのソフトウェアイネーブル機能を備えたカスタマイズ型のソリューションがあれば、データおよび利用状況の分析が容易になり、大きな収益化の機会がOEM事業にもたらされるでしょう。
- 一方、建物内のスマートサーモスタットやスマートランプには、複雑な組み込み知能である必要はありません。したがって、IoTデバイスレベルで求められるセキュリティも非常に低く代わりに、収益化の可能性も低くなっています。しかしながら、周辺機器のマルチクライアント機能といった特別な管理機能が付加価値を生むかたちで、収益化のオプションが見つかる場合もあります。加えて、サーモスタットとランプは特性上、ビッグデータを創りだす要素が非常に高いため、顧客の個人情報が窃取されないよう、ベンダーはデータの安全を保つための手段を、慎重に講じる必要があります。

以下の表に示すように、知能のレベルが非常に高いIoTデバイスと低いデバイスとがあり、その間に、幅広いIoTアプライアンスが存在します。

インテリジェントIoTアプリケーション	デバイスインテリジェンス	収益化[1]	セキュリティ[2]	ビッグデータ
産業用機械	***	***	***	**
スマートビデオ監視	***	***	***	***
自動販売機／売店	***	***	***	*
デジタル広告	***	***	**	***
医療用画像形成ステーション	***	**	***	*
スマートファーミング（農業）	***	**	***	**
フリート管理	***	*	**	**
携帯電話ベースのIoTアプリ	**	***	***	***
家庭用ロボットの住宅用ゲートウェイ	**	**	**	**
スマートグリッドアプリケーション	**	**	**	**
設備管理機器	**	**	**	**
気象観測計	**	*	*	***
病院設備ロジスティクス	**	*	**	*
入室管理	**	*	**	**
スマート家電	**	*	*	***
在宅ケアゲートウェイ	*	*	**	*
監督および機能使用モニタリング	***	***	***	***
メンテナンスおよび保証アプリ	**	***	**	***

[1] OEM向け／モジュラーアプリによる
[2] デバイス保護や知的財産保護
上記すべてのアプリケーション用アドオン

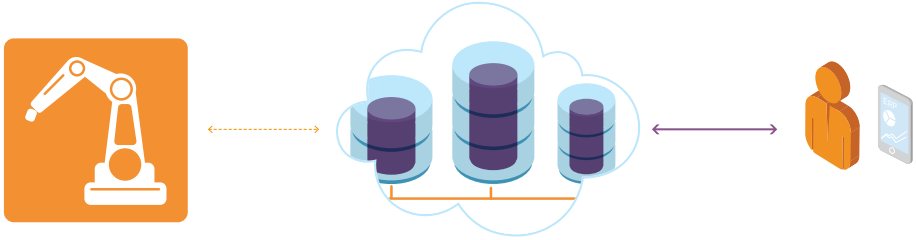
IoTアプリケーションの共通の利点とは

これまでに紹介したさまざまなIoTアプリケーションは、ユーザーが得られる恩恵だけでなく、ベンダーにとっても、収益化の手法やセキュリティの実装、ビッグデータといった観点ごとに大きく異なります。

その一方で、IoTの活用そのものが、すべてのIoTアプリケーションの展開にもたらす、共通もしくは不変の利点もあります。例として、IoTデバイスにおける状態データのモニタリングがあげられます。この利点は最終的に、予知保全サービスにつながり、収益化の機会となるでしょう。その際には、エンドユーザーもアプリケーションの可用性向上やTCO（総所有コスト）の削減といった恩恵を受けることができます。

さらに、OEM／サービスプロバイダーは、ビッグデータによって、他よりも修理頻度が高いコンポーネントを把握でき、この情報を次世代製品の設計改善に活かすことができます。ビッグデータは、OEMの組み込みハードウェアベンダーのビジネスモデルさえ変えることが可能です。なぜなら、デバイスのモニタリングに独自の組み込みクラウドを提供することができるからです。このタイプのサービスは、OEM向けの追加のソフトウェアやサービスを加えることで、ハードウェアベンダーのビジネスモデルを拡充する可能性を秘めています。そしてOEMベンダーは、これらのプラットフォームやサービスを自社のビジネスモデルに効果的に活用できるのです。

技術要件



キャプション：IoTアプリケーションの構築に必要なものは、基本的に3つ。1つ目が「モノ」そのもの、つまりIoTデバイス。2つ目が組み込み（クラウド）サーバーで、最後の3つ目がクライアントです。

IoTアプリケーションの構築に必要なものは、基本的に3つだけです。1つ目が「モノ」そのもので、つまりIoTデバイスです。2つ目が組み込み（クラウド）サーバーで、最後にクライアントがあげられます。

ただし詳しく見ると、IoTがもっと複雑な世界であることに気づくでしょう。たとえば、IoTデバイスは自身がゲートウェイを備えているか、もしくは別のゲートウェイを使ってインターネットにアクセスし、1台だけでなく複数のアプリケーションサーバーにデータを送信します。これらのサーバー（多くの場合プライベート、パブリックまたはハイブリッドクラウドサーバー）は広範な情報配信のためのメインの基盤となり、オンラインダッシュボード、携帯電話アプリ、あるいはSMS経由で人またはインテリジェントデバイスに情報を送信します。接続、通信、そして組み込み知能という点で、広範な管理が必要になるわけです。では、実際のIoTデバイスにはどの程度の知能が必要なのでしょうか。

「インテリジェントなモノ」の定義

IoTデバイスのすべてに高度な知能が必要というわけではありません。昨今、データ処理能力を持たないRFIDフォームのIoTデバイスが郵便小包に組み込まれ、物流の最適化やステータス、追跡情報の提供に役立っていることはご存じでしょう。自動車の盗難防止用の位置情報データを提供するIoTデバイスが必要とするのも限定的な知能であり、ほとんどの場合、GPS機能を備えたGSMチップで十分です。多くの場合、大量のIoTプロジェクトで使用される周辺機器に、複雑な知能は必要とされません。

ただし、このようなタイプのアプリケーションでは、「IoTエッジデバイス」が所定の位置にすでに追加されていることが前提となります。エッジデバイスは、その名のとおり、インターネットのエッジに配備され、シンプルなIoTゲートウェイよりも高度な知能を供給します。

エッジデバイスは、ローカルに分散されたすべてのデバイスからのデータをホストする組み込みWebサーバーを供給し、クラウドとの通信を管理します。先に説明したRFIDパッケージの追跡用ロジスティクス車両や、ホームオートメーション向けのスマートハウス用ゲートウェイなどで事例を見ることができます。これらのインテリジェントなIoTエッジデバイスが、組み込みクラウドと周辺IoT機器とを接続します。場合によっては、クライアントデバイスと直接通信することもあります。スマートフォンやタブレットとの通信がその例です。

＜要約＞ IoT市場には何十億というデバイスが存在していますが、デバイスによっては限定的な知能が備えられています。ただし、膨大な数や種類のIoTデバイス／IoTエッジデバイスは、ソフトウェアの仕組みに高度な統合知能を必要としています。ソフトウェアベンダーは、こうしたソフトウェアをセキュアに保護する必要があります。

必須となるセキュリティの強化

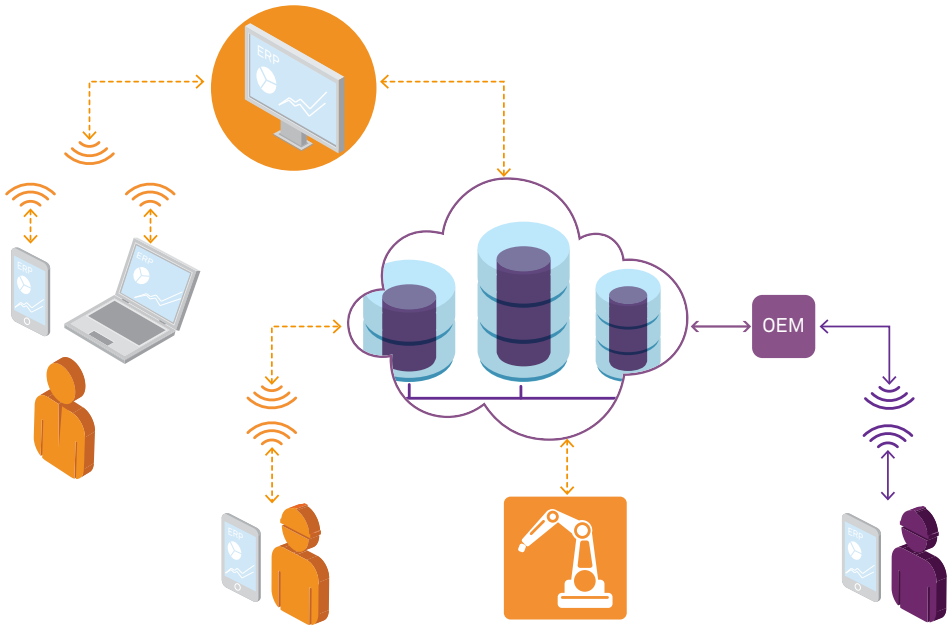
接続状態のインテリジェントIoT（エッジ）デバイスにとって、セキュリティの強化は必須です。それにはさまざまな理由があります。

誰かがスマートメーターのデータをハッキングして、光熱費を不正にゼロにしようとしている状況を想像してみてください。この行為がエネルギー供給会社に多大な損失を与えることは間違いありませんが、相対的に見れば、まだ被害の少ないケースにすぎないと言えます。

さらに悲惨な結果を招くケースもあります。マシンの不正操作は、非生産的なダウンタイムを発生させるだけにはとどまりません。たとえば、非常停止装置や安全手順においてハッキングされた場合、最悪の場合、オペレーターが怪我をすることもありえます。IoTデバイスを不正な操作から守るだけでなく、知的財産の保護もまた重要な課題となってくるのです。

セキュリティ強化の要求が増している要因の1つとして、以前であればインターネットに接続するはずもなかった機器がネット上に現れてきていることが挙げられます。この動きが、広範かつ大量な機器の設置と相まってインタフェースの数を急速に押し上げ、データの破損が起こりうる状況を生み出しているのです。そうなると、最高レベルのセキュリティが欠かせないことは明白です。

強固なセキュリティ対策は、インテリジェントIoT（エッジ）デバイスにとってのみの重要課題ではありません。サービス担当者がマシンや機器、設備に接続されたIoTデバイスからデータを収集する際に使用するユーザークライアントとともに、組み込み（クラウド）サーバーアプリケーションもカバーされなければなりません。そのためには、インテリジェントIoTデバイス上で動作するソフトウェアのバージョンを確認するだけでなく、ソフトウェアが特定のデバイス上だけで動作するように制御する必要があります。さらに、ソフトウェアを特定のデバイスに紐付けて、他の権限のないデバイスにインストールできないようにしなければなりません。最後に、誰がクラウド経由でアプリケーションにログオンしたのかを把握できるようにすることも必要です。



キャプション：IoTアプリケーションでは、さまざまなデバイスにおける多数のセキュリティ問題を解決することが求められます。OEMエンジニアの多くは、ITではなくロボット工学を専門としているため、問題解決の大半が新しい経験となります。

OEMエンジニアの多くは、ITではなくロボット工学を専門としているため、これらの問題の大半が新しい経験となります。VDCが最近まとめた市場調査研究からも、組み込みシステムエンジニアがネットワーク接続されるシステムを構築するうえで、セキュリティが最大の障壁になることがわかっています。また、組み込み系エンジニアの3人に2人が、自社の顧客にとってセキュリティが重要、または非常に重要であると認めています。要するに、多種多様なデバイスにおいて、さまざまな観点から多くのセキュリティ問題を解決しなければならないということです。

セキュリティ対策のためのパッケージ

利用できる保護対策はいくつも存在します。たとえば、メカ的な保護は、密閉されたハウジングやボードのほか、現金自動支払機（ATM）のテクノロジーで使用されるような、改ざんをトリガーとして自己破壊するメカニズムによって実現しています。また、セキュリティパッケージで求められるその他の機能として、通信インタフェースを保護し、データとデータ通信を暗号化する必要性が考えられます。そして何よりも、IoTアプリケーションの収益化の観点では、ソフトウェアライセンス／エンタイトルメント管理のアプローチが重要なことは言うまでもありません。

USBポート経由などのローカルアクセスからアプリケーションを保護する一番シンプルな方法は、まずそれらをアクセス可能な状態にしないことです。これは、密閉されたハウジング内に設置することや、そもそもハードウェア設計に組み込まないことで実現できるでしょう。ただし、どのインテリジェントシステムにも、少なくとも1つのネットワーク接続があります。このチャネルを経由するIoT通信の安全を保つには、ネットワーク接続を介した外部からの攻撃に対抗するファイアウォールをインストールする必要があります。さらに、VPN（仮想プライベートネットワーク）接続を使うとともに、WhiteScriptingやSecureBootといった内部セキュリティ対策を実施して、マルウェアが実行されるのを未然に防ぐことができれば理想的です。

現状の危険を考えてみると、アプリケーションと生成されるデータの両方を、暗号化によって保護することが必要であることは明らかです。データをインテリジェントIoTデバイス上で暗号化することはもちろん、送信中の暗号化も欠かせません。ただしこれらは、セキュリティ対策における氷山の一角にすぎません。すべてのデバイスにおけるデータの整合性と均一性という観点から見た、セキュアなデータ送信は別の問題であり、なぜIoTアプリケーションにおいてセキュリティが重要になってくるのかを明確に示しています。では、開発者がこの課題に迅速かつ効果的に対処するには、どうしたらよいのでしょうか。

キャプション：ライセンス／エンタイトルメント管理とアプリケーションコードの暗号化によって、各インテリジェントIoT（エッジ）デバイスの中核となる機能が保護されるだけでなく、組み込み（クラウド）サーバーおよびクライアント上のアプリケーションも安全に保護されます。

「IoTアプリケーションの心臓部」となるセキュリティ機構

IoTのすべてのレベル（インテリジェントデバイス、組み込みクラウドサーバーおよびクライアント）で導入可能な、高度なソフトウェアライセンス／エンタイトルメント管理ソリューションが、現存する技術的な課題をきわめてシンプルにしてくれます。そうしたソリューションは、ライセンスの不正な使用や配布からアプリケーション資産を守り、知的財産の盗難や改ざん、リバースエンジニアリングによる被害を防ぎます。

すでにビジネスIT分野では、ライセンス／エンタイトルメント管理ソリューションが広く使われています。たとえば、ERPのような基幹業務アプリケーションのソフトウェアライセンスなど、エンタープライズ向けソリューションの保護、現金自動支払機、ストリーミングポータル、モバイルアプリなどでの活用が有名です。また、ライセンス／エンタイトルメント管理ソリューションは、組み込み分野のソフトウェアベンダーでも導入され、ツールのセキュアな保護のために使用されています。こうした状況から、ライセンス／エンタイトルメント管理ソリューションをインテリジェントなIoTアプリケーションに適用することに価値を見出し、導入を検討することは当然の流れだと言えるでしょう。

コードレベルでデバイスをプロテクト

ユーザーおよびアプリケーションレベルでのライセンス／エンタイトルメント管理のアプローチは、いわばコインの一方の面にすぎません。もう片方の面は、インテリジェントデバイス自体です。OEMベンダーにとって、自社のインテリジェントIoTデバイスをコードレベルでプロテクトして、破壊行為や不正操作を防ぐことは必須の対策です。機能の安全性や保証請求を考えると、デバイスの組み込みパラメータ設定を保護することが必要といえます。

ハードウェアベースの統合暗号化コンポーネントを備えたソリューションであれば、最強のプロテクションを実現できます。たとえば、差分電力解析（DPA）や電子顕微鏡検査法を使ったリバースエンジニアリングなど、悪意を持った高度なハードウェア攻撃に対しては、安全性に定評のあるSmartCardテクノロジーのもとに統合されたハードウェア ベースのプロテクションキーが、現在、利用できる、最高レベルのセキュリティで対策を講じます。

キャッシュ内でのコード暗号化

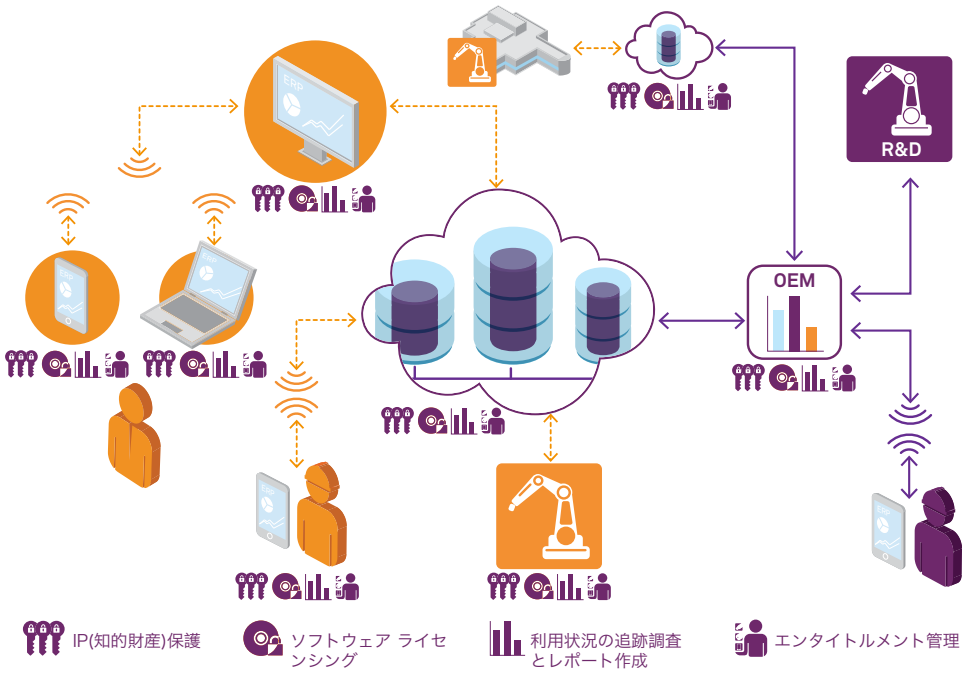
アプリケーションとハードウェアキーとの間に分離不可能な結束を形成する、専用のチップテクノロジーを採用した暗号化の仕組みがあります。これを用いた暗号化機能を付加することで、キャッシュ内のコードを常に暗号化しておくことが可能になります。その結果、コードは「知的財産を標的とする泥棒」がアクセスできない仕組みに変わります。このようなハードウェア ベースの暗号化キーは、ファイアウォールやVPN、暗号化通信とともに非常に重要な中核となるセキュリティ機能を果たし、IoTに接続したインテリジェント組み込みデバイスを安全にプロテクトします。もちろん、専用のセキュリティハードウェアを使用したハイレベルなセキュリティが、すべてのアプリケーションに必要なわけではありません。開発者は、状況に応じてハードウェア ベースのキーとソフトウェア ベースのキーを選択して、対象のアプリケーションにとって最適なセキュリティを構成することになります。

キャプション：小さなチップがもたらす大きなセキュリティ。ハードウェア ベースの暗号化キーは、コードを常に攻撃から守り、信頼性の高いプロテクションを実現します

セキュリティの複雑さを解消する

上述のようなハイレベルのプロテクション以外にも、ソフトウェア ライセンス／エンタイトルメント管理ソリューションに備わる注目機能として、きめ細かな管理機能が挙げられます。この管理機能は、組み込みIoTデバイスや組み込み（クラウド）サーバー、そしてモバイルアプリを含むさまざまなクライアントデバイスに適用できます。たとえば、マシンや機器上のメンテナンスアプリケーション全体への継続的なプロテクションも可能です。

ライセンス／エンタイトルメント管理ソリューションに備わるすぐれた管理機能は、アプリケーションの周辺全体をも監視できます。この結果、IoTアプリケーションに接続する可能性のある、あらゆるインテリジェントデバイスや、デバイス上で使用するアプリケーションをプロテクトできるというわけです。その際、ベースとなるOSやプロセッサのアーキテクチャ／プラットフォームの種類は問いません。ソフトウェア開発者は、多様なセキュリティの課題を単一のソリューションで解決でき、その複雑さを解消できるようになるのです。



キャプション：単一のソフトウェア保護およびライセンス管理ソリューションが、想定されるあらゆるデバイスをプロテクトすることで、セキュリティの複雑さを解消します。

フィーチャ単位レベルの追跡モニタリング

ライセンス／エンタイトルメント管理ソリューションの利点は、これだけではありません。ソリューションは、最も一般的なライセンシングモデル（サブスクリプション、時刻ベース、期間限定）をサポートしています。IT分野においては、スタティック（静的）なライフタイムライセンスを管理するだけでなく、個々のフィーチャ単位のレベルで一定の期間や使用量について有効化するといった、詳細な追跡モニタリングが可能なソリューションが支持されています。

これまでに説明した、豊富な管理機能を備え、フィーチャ単位の追跡が可能なライセンス／エンタイトルメント管理ソリューションを導入したとき、IoTアプリケーションの開発者は、アプリケーション内でのユーザーの行動モニタリングに必要なビッグデータの生成も可能になります。この先新的なモニタリングは、エンドユーザー側で行われる、特定のボタンの使用状況といった些細な状況すらカバーすることができます。

フィーチャ単位レベルでソフトウェア／エンタイトルメント管理が行えることで、開発者やエンジニアは強力なツールを手に入れたことになります。たとえば、メーカーはエンドユーザーの使用状況に基づいてカスタマイズしたメンテナンスサービスや保証管理サービスを提供できるようになります。

では、そうした価値のあるサービスを、どのような方針に基づいて、提供するのがよいのでしょうか。

保証とは、本質的には、販売者と購買者の双方に向けたリスクマネジメントです。リスクマネジメントは時間で測定されることが一般的です。1年間で200回使用された洗濯機の故障のリスクは、使用回数が50回の洗濯機と比べて格段に高くなります。そのため、販売と購買の双方にとっての解決策として、「この製品はX回の使用に耐えます」と耐用性に関する保証を行うことになります。

さらなる側面として、ライセンス管理に基づくビッグデータが、エンドユーザーのアプリケーション使用状況とソフトウェアの機能に関して、価値ある見識を提供することをあげられます。これは、将来の製品開発に役立つ知識ともいえます。このような有効な知見によって、機能の有効／無効を判断し、コンシューマーや、コストに敏感な専門家レベルのユーザーの市場からプレミアマーケットまで、幅広い市場向けのパッケージを作成することが可能になります。この結果、適切なライセンス管理によってIoT投資の収益化に向けた基盤を固めることができるのです。

キャプション：「いつ、どのくらいの頻度で、どの機能が使用されるのか？」――使用状況の追跡は、製品開発に価値ある見識を提供します。

同時に、ライセンス／エンタイトルメント管理ソリューションは、認証に代表される重要なセキュリティ機能をクラウド環境で実行するプラットフォームを提供します。この特徴が、IoTに取り組むコミュニティにおいてもホットな話題としてとりあげられています。

「いつ、誰がアプリケーションへのアクセスを承認されるのか？」――これは、エネルギー分野のスマートグリッドアプライアンスのようなIoTアプリケーションの多くにおいて非常に重要な問題となっています。ライセンス／エンタイトルメント管理ソリューションは、ビッグデータの提供だけでなく、その評価という点でも重要な機能を実行します。そして、このソリューションの主要な役割である特定の機能の有効化が収益に結びつくことから、IoTへの投資を回収するプラットフォームが提供されるのです。

シンプルなインテグレーション

ライセンス／エンタイトルメント管理ソリューションは、保護を必要とする、運用中のデバイス数の影響を受けません。立ち上げたばかりの企業のように、現場に数台のデバイスしかない環境でも、何万台ものデバイスが設置されているエンタープライズの環境でも、これらのデバイスは等しくアプリケーションに活用されます。

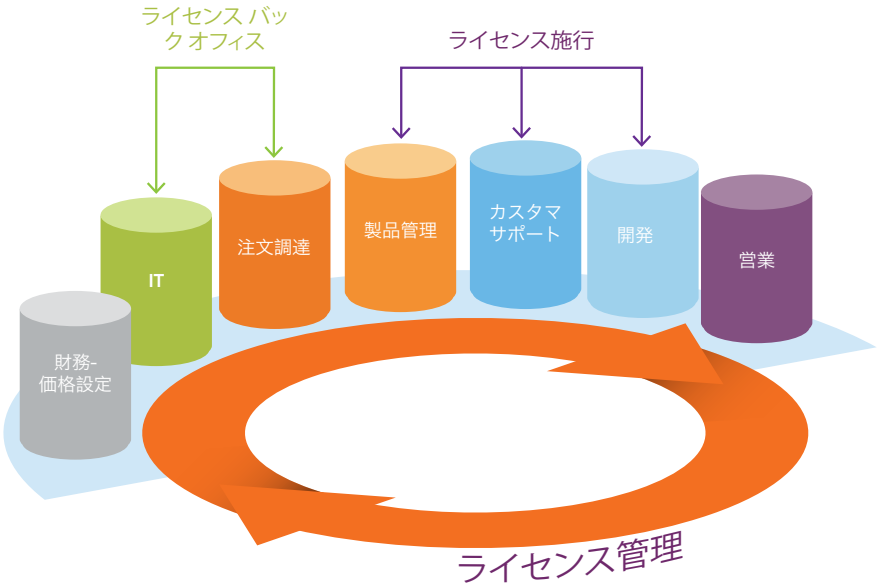
ライセンスの作成、プロビジョニング、有効化、更新および使用状況のモニタリングといった種々のタスクは、アプリケーションに容易に統合できます。さらに、ライセンス／エンタイトルメント管理ソリューションは、サードパーティ製のソフトウェア ライセンシングにも利用できるため、OEMベンダーは単一のツールでOSライセンシングを管理できます。また、同ソリューションはERP、CRM、請求／マーケティング自動化システムへのシームレスな統合も考慮して設計されています。そのため、製品の発送やカスタマー サービス／サポートなどの処理の自動化を実現します。これが最終的には、運用コストの削減に貢献し、ひいては顧客満足度の最適化につながります。こうしたことから、ライセンス／エンタイトルメント管理ソリューションが、IoTアプリケーションの導入ツールとして、非常に重要かつ必要不可欠な役割を果たすことをご理解いただけるでしょう。

ソフトウェア ライセンシングを実装する

ソフトウェア開発ライフサイクルのどのようなステージでも、OEMベンダーはライセンス／エンタイトルメント管理ソリューションの導入を開始できます。最も効率のいいタイミングは、最初のステージから使用することです。不可能な場合、あとからでも導入できますが、作業がいくぶん複雑になってしまいます。

いずれの場合でも、利用可能なさまざまな選択肢の中から何を始めるのかを理解しておくことが必要です。そして、どの方法を選んだとしても、テクノロジーの観点だけで考えるのではなく「全体像」を描くこと。つまり、ライセンス／エンタイトルメント管理ソリューションを単なるツールとしてではなく、最終的には新しいビジネスモデルへの扉を開くツールとしてとらえることが大切です。

一部のビジネスにとって、ソフトウェア ライセンシングがグレーゾーンである理由は？



キャプション：ライセンス／エンタイトルメント管理のための適切な戦略の策定には、多くのステークホルダーが関与しています。

まず、一例を挙げましょう。物流とITのインテグレーションに向けたソリューションを模索している企業は、プロセスのインテグレーションに関するいくつかの問い（システムをスタンドアロンで運用するか、それともERPシステムに組み入れるか）への回答を用意しなければなりません。早い段階でこのような重要事項を決定しないと、インテグレーションのプロセスの最後で、膨大な作業を強いられることになります。

さらに、企業はフレキシビリティとセキュリティの間で、適度なバランスをとることが必要です。これは、新しいビジネスの創出にあたり、どのように差別化や標準化を行うかという、企業の方針に対する問いかけともいえます。さまざまな組織から多様な要求がある中で、正しい構造化と優先順位付けが行われなかった場合、管理側が重要な機能へ適正に配慮できなかったり、配慮が遅すぎて市場投入が遅れたりする可能性があります。加えて留意すべきは、最悪のケースに備え、準備期間中に十分な議論を行わなかった場合、あとからコストのかかる対策を行わざるをえなくなることです。

現在のビジネスモデルについて考えることは一要素にすぎません。将来のビジネスモデルを予想することは、ソフトウェア収益化ソリューションを導入するのと同じように重要です。

例として、ライセンシングをオフラインで現場に導入することを考えてみましょう。現場での導入が増え続け、管理がますます複雑になることを考えると、ライセンスとアプリケーションを常にオンラインで保有することが推奨されます。これは、組み込みデバイスをシンクライアントとして設計することにもつながります。

さて、これは本当に私たちが望む、確実に機能する方法なのでしょうか？　それとも他のアプローチが必要になるのでしょうか？　IoT以前の産業機械では珍しくなかった、DaaS (Devices as a Service) については、どのように考えるべきでしょうか？　さらに、コンシューマーデバイスへのライセンシングについてはどうでしょうか？　携帯電話やタブレット用のダッシュボードを提供する場合、これらについてもまた、適正な管理が必要になります。

考えられるさまざまなシナリオはすべて、新しいビジネスモデルにフィットしていることが必要です。そこにはライセンス／エンタイトルメント管理下で扱うビッグデータも含まれます。これらの実情をすべて考慮すると、IoTアプリケーションの現場への導入にはどれくらいの時間が必要かを簡単に把握できるようにすること、またそれは専門家が行わなければならないということが理解できるでしょう。なぜなら、これらのIoTアプリケーションには、ただ1つだけではなく2〜3、場合によってはそれ以上の複数のライセンス／エンタイトルメントプラットフォームが含まれていて、それぞれに対して管理や収益化そして保護が実施されなくてはならないからです。

ライセンス／エンタイトルメント管理の専門家やコンサルタントへの相談は、早ければ早いほどいい結果が期待できます。IoTマーケットへ参入したいと考えている企業は、この結果、自社の革新的なIoTアプライアンスへ取り組み、効果的かつ利益を生み出す事業に向けた、スムーズなスタートを切ることができるのです。最適な実行戦略の詳細については、2番目のホワイトペーパー「ソフトウェア ライセンシングの権利を初めて得るには」をご覧ください。

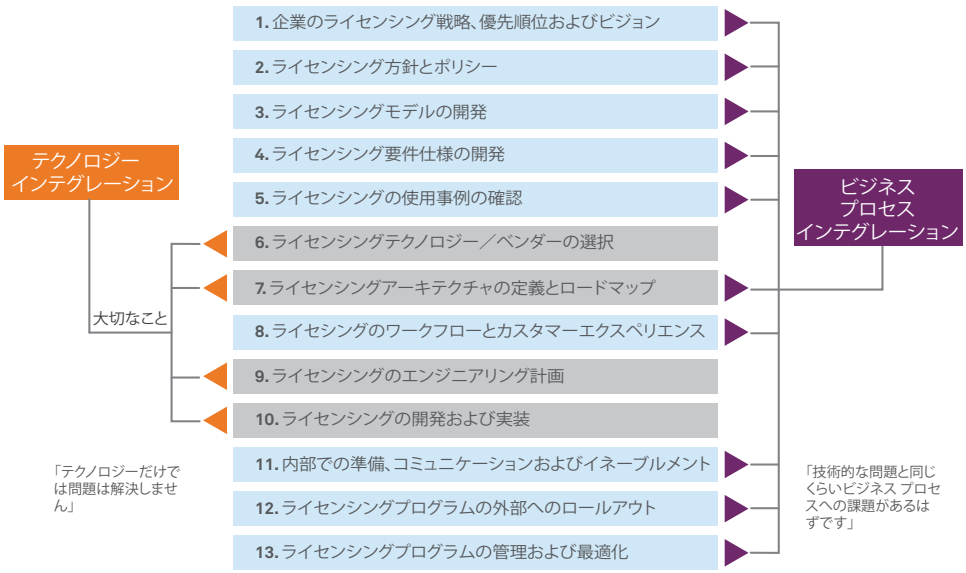
IoTでサプライチェーン全体に新たなビジネスモデルを実現する

多くのOEMベンダーはビジネスモデルを拡大しつつあり、純粋なハードウェアベンダーからハードウェア、ソフトウェア、そしてサービスベンダーへとビジネスモデルを移行しています。

ビジネスモデルの変革を経験しているのは、OEMベンダーだけではありません。組み込みボードメーカーやシステムベンダーもまた、自社のハードウェアに対する独自のメンテナンスプラットフォームを提供するため、デバイスを組み込んでクラウドに移行しています。エンドユーザー、OEMベンダー、組み込みハードウェアベンダーのいずれのユーザーであっても関係はありません。

これらのハードウェアのモニタリングおよび予知保全管理用のAPIには、リバースエンジニアリングからの保護も必要です。その結果、今や組み込み系ハードウェアベンダーにとっても、柔軟なハードウェアまたはソフトウェア ベースの暗号化エンジンを持つ、ライセンス／エンタイトルメント管理ソリューションが必須となっているのです。

ビジネス インテグレーション



キャプション：ライセンス／エンタイトルメント管理ソリューションの導入は、ビジネスプロセスのインテグレーションに比べればシンプルな作業です

組み込みソフトウェアベンダー向けの収益化アプローチ

Basically every IoT application needs an appropriate license and entitlement management
ここまで述べてきたように、あらゆるIoTアプリケーションの開発には、ライセンス／エンタイトルメント管理ソリューションの機能が必要不可欠となるでしょう。OEMベンダーやビジネスアプリケーションの開発者は、市販のソリューションを購入することで簡単に導入できます。

一方、独立系の組み込みソフトウェアベンダー（IESV）はOEMベンダーとは異なり、エンジニアリング環境にフィーチャを容易に統合するためのテクノロジーを自らが提供する立場にあります。その実現を支援するのが、ライセンス／エンタイトルメント管理ソリューションが提供するプラグイン機能です。

SafeNetを代表とするライセンス／エンタイトルメント管理ソリューションベンダーは、IESVプラットフォーム専用のプラグインの提供をはじめ、さまざまな形でIESVが付加価値のあるプラットフォームを実現できるようにサポートしています。このようなサポートのもと、自社の顧客に提供していると同等のテクノロジーを使って、IESVは自社のエンジニアリングソフトウェアの保護や収益化に取り組むことができます。ライセンス／エンタイトルメント管理ソリューションは、活用を進めていくことで、最終的にIoTサプライチェーン全体で活用していくことを可能にします。

SafeNet, Inc.について

1983年に創設されたSafeNet, Inc.は、世界で最も大規模な情報セキュリティベンダーの1社であり、組織における最もセンシティブなデータの保護という観点において、世界中のマーケットリーダーから大きな支持を得ています。

SafeNetのデータセントリックアプローチは、データセンターからクラウドまでの、あらゆる場所に格納された価値の高いビジネス情報の安全を、ライフサイクル全般にわたって確保することに重点を置いています。センシティブなデータの保護とアクセスコントロール、リスク管理、コンプライアンスの確保、そして仮想／クラウド環境のセキュリティ保護において、25,000を超える企業や政府機関といったお客さまが、SafeNetに信頼を寄せています。

SafeNetのテクノロジーやソリューションの詳細は、Twitter、LinkedIn、Facebook、YouTube、Google+などのソーシャルメディアでもご覧いただけます。

SafeNetソフトウェア収益化ソリューション

SafeNetは、オンプレミス、組み込み、クラウドのソフトウェアベンダーに向けたライセンス／エンタイトルメント管理ソリューションで業界をリードするプロバイダーです。SafeNetのSentinelは、安全かつ柔軟なアプローチにより、お客さまの今後のビジネスを保証する収益化ソリューションとして、ソフトウェア業界で最も信頼されているブランドです

詳細については、こちらのWebページをご覧ください。www.safenet-inc.jp/software-monetization-solutions

会話に参加する

→ Facebook
www.facebook.com/licensinglive

→ Twitter
twitter.com/LicensingLive

→ LinkedIn
bit.ly/LinkedInLicensingLive

→ Sentinel ビデオクラウド
sentinelvideos.safenet-inc.com/

→ LicensingLive
licensinglive.com

お問い合わせ先: すべてのオフィスの所在地と連絡先情報につきましては、以下をご覧ください**www.safenet-inc.jp**
フォローする: www.safenet-inc.com/connected