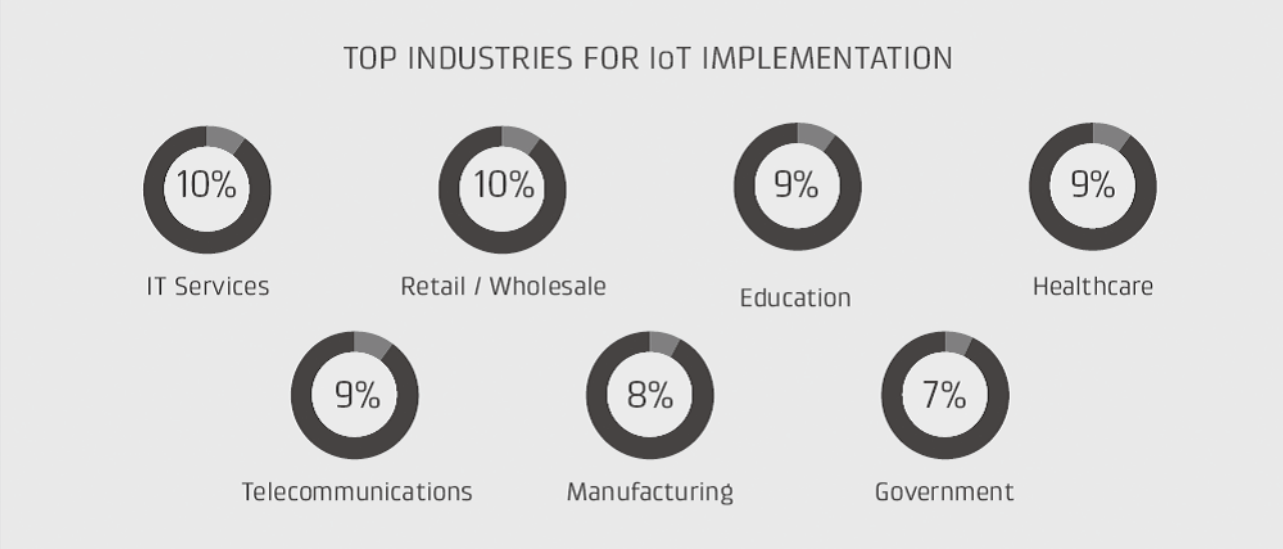
IoTセキュリティとセキュリティ製品の動向

Value Creation Frontier 代表
衣川　俊章

今回は、「最新米国サイバーセキュリティ事情」ということで、IoTセキュリティとセキュリティ製品の動向を書かせていただきたいと思います。ここで書かせていただいている情報は、筆者が米国でのカンファレンス・セミナーでの参加と、調査資料などをベースにまとめさせていただいております。

IoTセキュリティ

ある調査によると、IoT技術を何らかの形で利用している組織は32%、1年以内には導入しようと計画している組織まで含めると69%となっています。特に大企業で、かつ分散され広範囲でデバイスが存在し（例えば、電気メーターや自動車など）、かつそれがビジネスに不可欠な要素になっている組織での導入が進んでいるようです。



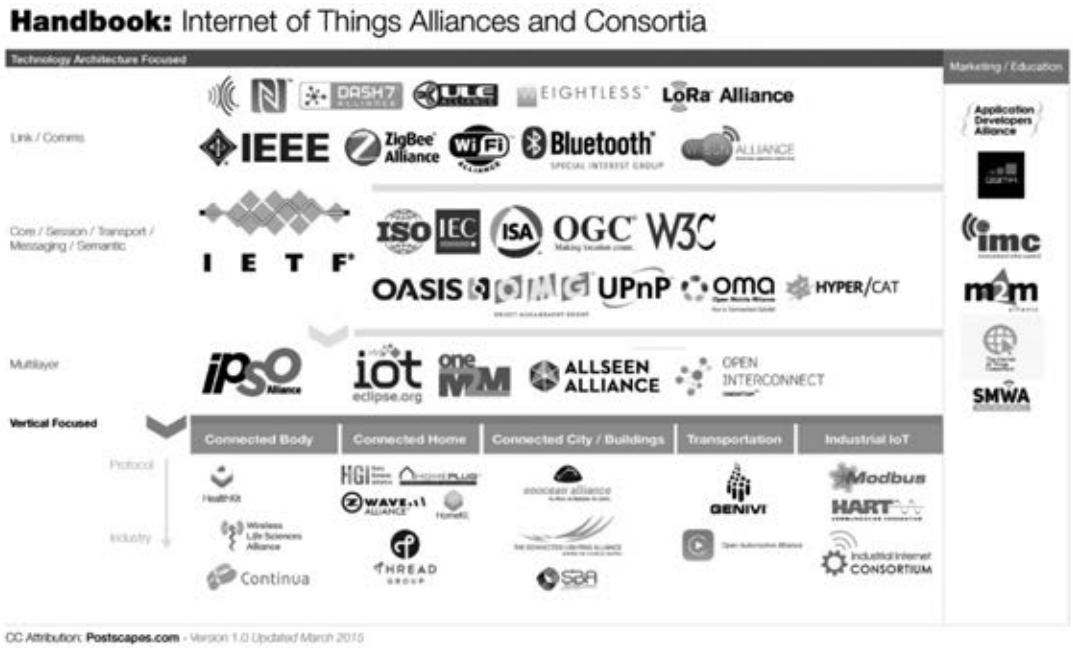
導入に際しての最大の懸念事項はセキュリティで、IoT特有のネットワークインフラの構築が必要であると言われています。

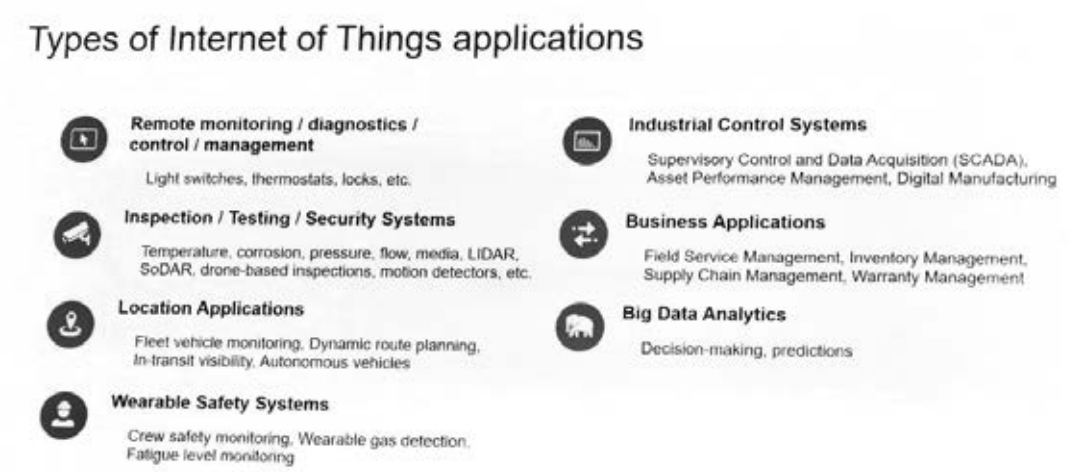
一方で、IoTにおける脅威としては、66%のIoTネットワークではセキュリティ違反が発生しており、DDoS通信のうち10%がIoTシステムを狙ったものであるとも言われています。残念ながら、IoTデバイスは70%が非暗号化ネットワークを利用し、50%では認証が弱く、結果66%では攻撃を許してしまっているという数字も出ています。

前述を踏まえ、セキュリティ対策に関しては、ネットワーク・エンドポイントモニタリングに関して注力しているベンダーが多くなって来ています。また、ネットワークアクセスにおいても、今までのインターネットではコネクションをまず優先し、その上での認証という考え方になっていますが、IoTネットワークでは、認証をまず実施し、その上でコネクションを許可するという発想に基づく構築が必要であると言われています。また、IoTネットワーク構築に際しては、論理・物理的に分離されたネットワークを考えるべきであるとも言われています。

ただ、IoTのそもそもの課題として、業界全体が混沌としている状況です。エッジデバイスは種類、数とも増加し続けており、それに呼応する為の複雑で細分化されたアプリケーション、多様なプロトコルや形態の存在、それらのコネクティビティの安全性を含めた確保も検討を進めていかなければいけない状況であります。それに関しての標

準やガイドラインがまだ充分に整備されていない（様々な団体などが設立されていて、整備への取り組みは始まっていますが）のも現状です。





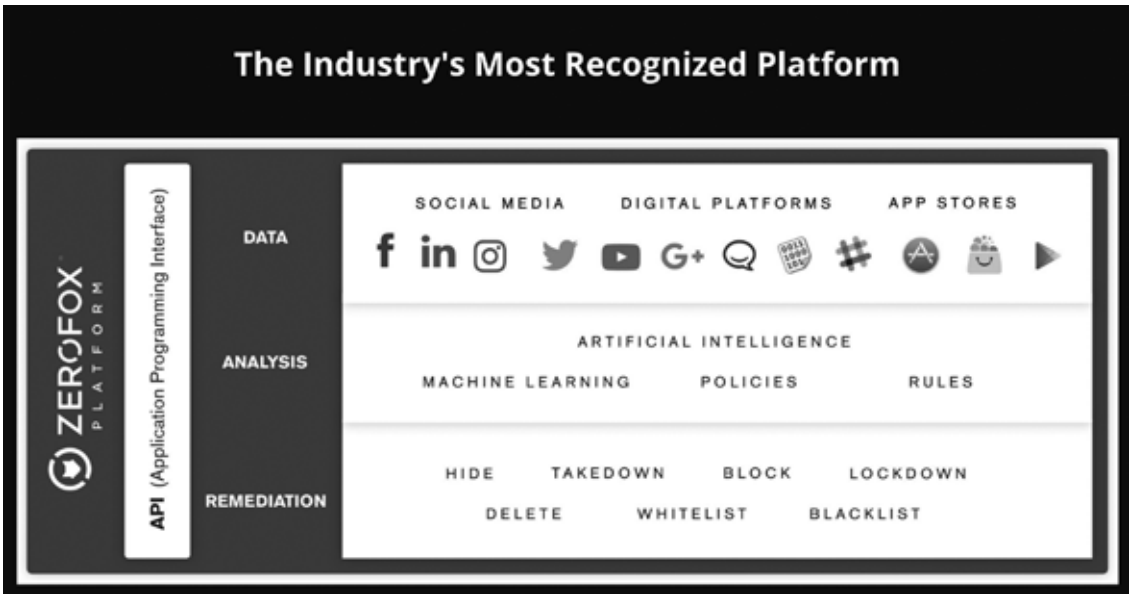
セキュリティという観点では、センサー・エンドポイントレベルでのビルトインをどこまでやれるかが課題とも言われています。昨今では、Raspberry Piなどの普及によって、低スペックエッジデバイスにおけるセキュリティビルトインが今までより加速していくのではとの予測があります。あとはリアルタイムでのネットワーク・デバイス運用管理も必要要素であると考えられています。

セキュリティ製品動向

一時期、セキュリティ製品がエンドポイント保護にシフトしていき始めた時期がありました。今でもエンドポイントセキュリティエリアへのベンダー進出、特にAI活用を売りとしているベンダーは継続しており、むしろ飽和状態かつ、製品毎の差別化が分かりづらくなってきているように感じられます。そこで、次世代IDSを中心としたネットワークレベルセキュリティの復活が見受けられるようになって来ています。更に、エンドポイントとネットワーク製品との連携をするケースが増えてきています。これによって差異化を図ったり、包括的なセキュリティ提供を図ることを各社が目指していることと考えられます。

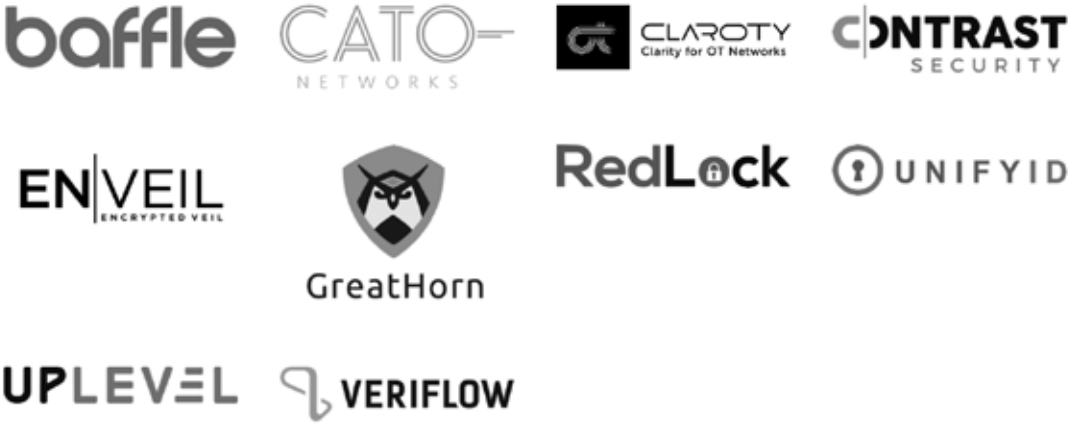
エンドポイントに限らずセキュリティ製品へのAI活用は引き続き継続しており、アンチフィッシングツール、ネットワーク検疫・分析製品、脆弱性検査ツール、面白い所では、ソシアルメディアモニタリングツールでの利用などが出てきています。

＊例：ソシアルメディアモニタリングツールーZeroFox



ただ、革新的なアイデアや技術活用での新製品が出てきていないのも現状です。この4月開催のRSAでのInnovation Sandbox表彰企業がどのようが技術なのかには、興味があります。

＊2017年Innovation Sandbox選出スタートアップ企業



直接製品動向とは直接関係ありませんが、スタートアップ企業関連の直近話題としては、2015年度のRSA Innovation Sandboxの最優秀企業であるインシデントレスポンスオーケストレーションのパイオニアであるPhantom CyberがSplunkに買収されました。もう一つの話題として、スタートアップ企業が米国政府案件に入り込むケースは中々見られませんでしたが、先日Cybereasonが米国政府セキュリティ評価標準・認証であるFedRAMP申請を始めたというニュースが入りました。この認証取得には10ヶ月、かつ1億円近い費用が掛かるのが、スタートアップ取得は進んでいなかった大きな理由でした。これに他のスタートアップが容易に追随するとは思えませんが、1社でもこの取組みを始めたことは、政府におけるセキュリティ対策にスタートアップの先進技術が活用される活路を開いたという意味で大きいと見られています。

参考文献：

1. Cradlepoint “State of IoT 2018” (https://cradlepoint.com/white-paper/state-iot-2018)
2. Postscapes IoT Alliance and Consortium (https://www.postscapes.com/internet-of-things-alliances-roundup/)
3. ZeroFoxホームページ (https://www.zerofox.com/platform/)
4. RSA Conference 2017 Innovation Sandbox (https://www.rsaconference.com/events/us17/agenda/innovation-sandbox-contest