

# IoT時代のネットワークソリューション



## はじめに

従来ネットワークに接続されていなかった自動車や検針器などの機器が、通信機能を持つ Internet of Things（以下、IoT）デバイスとして今後爆発的に増え、その数は国内においても 2019 年には 9 億台を超えると予想されています<sup>1</sup>。IoT デバイスの普及により、工場や農場における生産性向上や、お客さまニーズの迅速な把握などが期待される一方、通信機能を持つデバイスが増加することにより、不正アクセスによる情報流出や乗っ取りによる誤動作などのセキュリティリスクの拡大が懸念されています。IoT デバイスはパソコンやスマートデバイスと比較して個々の性能に限りがあるため、セキュリティ対策ソフトウェアをインストールすることが困難であり、さらに前述の通り数も膨大であるため、デバイスごとの対応では限界が見えてきます。

IoT デバイスに対するセキュリティインシデントはすでに発生しています。道路の電光掲示板に不正アクセスされ注意を促す文字表示が変更された米国の事例や、インターネットから接続できるネットワークカメラの映像が一覧でサイト上に公開された事例<sup>2</sup>など、さまざまな種類の IoT デバイス

を対象とした事例が報告されています。

特に注目されたのが米国で発生した Point of Sales（以下 POS）システムに対する不正アクセスの事例です。POS レジにマルウェアを感染させることで、クレジットカード情報や顧客情報が流出しました。米国においては小売店だけでなく、レストランや駐車場など、広範囲において事例が報告され、既に日本国内においても侵入を検知した事例が報告されています。

このように、今後普及が見込まれる IoT デバイスですが、セキュリティリスクへの対策が急務となっています。

## IoT に対するセキュリティ要件

それではどのような対策を行えばいいのでしょうか。POS システムを例に不正アクセス方法とその対策をみてみます（図 1）。前述の事例における手順は以下の通りです。

- ① パソコンに対する標的型攻撃などによりマルウェアを感染させます。
- ② 感染したパソコンはパソコンの持つアクセス情報などにより周囲の端末に感



<sup>1</sup> 出典：IDC Japan プレスリリース「国内 IoT（Internet of Things）市場予測を発表」（2015 年 2 月 5 日）

<sup>2</sup> Insecam（閉鎖）

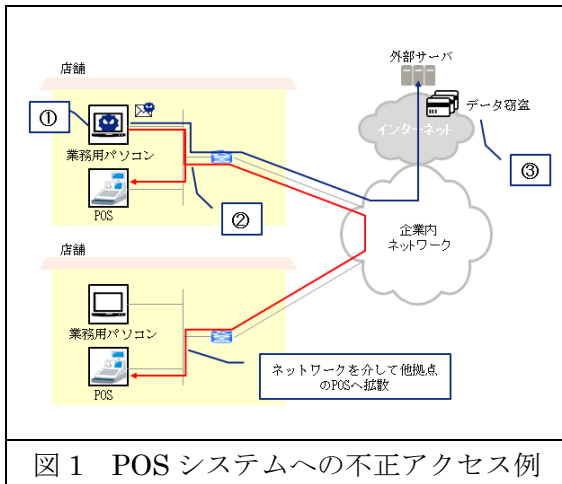


図1 POSシステムへの不正アクセス例

感染を拡大していきます。その過程でPOSシステムにも感染し、POSレジに対してはメモリー情報をリークするマルウェアを感染させます。

- ③ マルウェアにてPOSレジのメモリー上に展開されたクレジットカード情報が不正にアクセスされ、感染したパソコンを介してインターネットに通信されます。

このように、インターネットとの直接通信を許可していない場合においても、不正アクセスにより情報流出する恐れがあります。

このような不正アクセスに対するセキュリティ各社からの提言には、主にデバイスによる対策とネットワークによる対策が挙げられています。デバイスによる対策として、ハードウェアベースの暗号化の導入やセキュリティ対策ソフトウェアの導入などが挙げられていますが、すでに各店舗に展開しているPOSシステムを全て更改するには莫大なコストと時間がかかってしまいます。

## ネットワークによる対策

ネットワークによる対策では、主に2カ所でセキュリティ向上を図ることができま



す。

一つ目がインターネットとの境界線における入口・出口対策です。マルウェアが添付されたメールを検知するメールアンチウイルスや標的型攻撃を回避するためのサンドボックスにより、パソコンへのマルウェアの感染を防いだり、IDS/IPSによりマルウェアに感染してしまったパソコンと外部サーバとの不正通信を検知したりすることで、マルウェア感染前後の対策を行うことができます。ウイルス対策の導入率は92.9%である一方、IDS/IPSの導入率は32.7%にとどまっています<sup>3</sup>。感染を防ぐだけでなく、万が一感染してしまった場合でも被害を最小限に抑える対策を進めるためにはIDS/IPSの導入が効果的です。

二つ目がパソコンとPOSシステムとの通信を防ぐ対策です。パソコンとPOSシステムを直接通信できないようにすることにより、パソコン経由でマルウェアがPOSシステムに感染するリスクを低減することができます。小売店やレストランなどの場合、LAN環境が小規模であるため、やむをえずパソコンとPOSシステムを同一のセグメントに接続しているケースが想定されます。リスクを低減するために、パソコンとPOS

<sup>3</sup> 日米企業の情報セキュリティ投資動向, MM総研, 12/2013

システムのネットワーク分離は有効な対策と考えられます。

これらのネットワークによる対策だけでは USB 経由のマルウェア感染など、完全なセキュリティ対策とはいえませんが、機器の利用に対する運用ポリシーの整理・徹底と組み合わせることで、対策をより強固にすることができます。

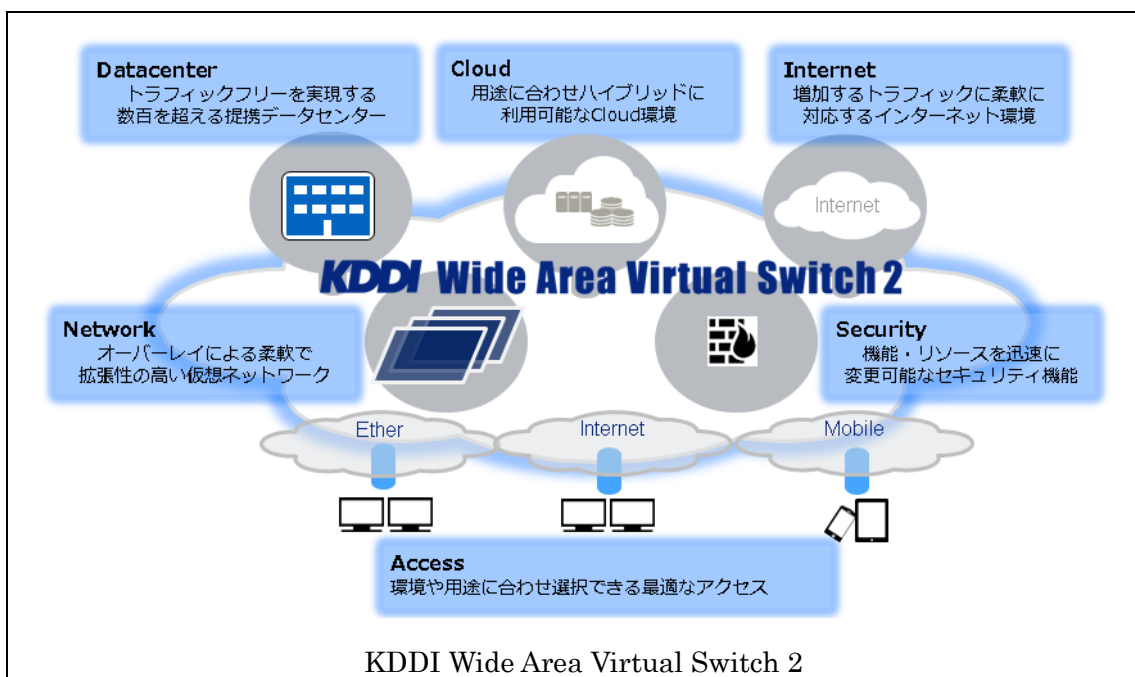
## KDDI Wide Area Virtual Switch 2

KDDI では 2014 年 9 月より Software Defined Networking (以下 SDN) 技術を用いたネットワークサービスとして「KDDI Wide Area Virtual Switch 2 (以下 KDDI WVS2)」を提供しています。KDDI WVS2 は広域イーサネットと IP-VPN を統合したレイヤ 2/レイヤ 3 混合のイントラネットサービスを提供するだけでなく、そのイントラネット上で利用できるファイアウォールや、インターネット接続およびインターネット通信のセキュリティを確保する



セキュリティアプライアンスを提供しています。2015 年 6 月からはこれらセキュリティ機能に加えて、任意の VLAN や IP アドレスを用いてネットワークを分離する仮想ネットワーク機能の提供を開始します。

KDDI WVS2 セキュリティアプライアンスでは、インターネットファイアウォール、IDS/IPS、Web アンチウイルス、メールアンチウイルス、URL フィルタリングと、それらを一括提供する UTM を提供しています。これらの機能はカスタマーコントローラを用いて、クラウド同様に購入・帯域変更・解約の契約処理やセキュリティポリシーの変更をオンデマンドに実施することが



できます。これによりトラフィック増加に伴う増強や、セキュリティインシデント対策を迅速に行うことができます。

KDDI WVS2 仮想ネットワークでは、既存のイントラネットにオーバーレイした仮想ネットワークをオンデマンドに作成・変更・削除することができます。従来であれば、ネットワークを分離したい場合、広域イーサネット上に VLAN で分離するか、物理的に別のアクセス回線を敷設して分離するしかありませんでした。VLAN で分離した場合、同一アクセス回線上に複数のネットワークを構築できるため、コストメリットがあるものの、広域ネットワークのルーティング設計を行わなくてはなりません。一方、物理的に複数のネットワークを構築した場合、用途に応じて広域イーサネットと IP-VPN を構築できますが、複数のアクセス回線を敷設するため初期投資コストや運用コストが上昇してしまう課題がありました。KDDI WVS2 仮想ネットワークを利用することにより、同一のアクセス回線上に広域イーサネットと IP-VPN を混在させることができるようになります。さらに、レイヤ 3 ネットワークの場合には、VLAN による分離だけでなく、送信元・宛先アドレスによりさらに細かくネットワークを分離することができるようになります。これにより、従来コストのために同一のネットワークで利用していた端末を、簡単に分離することができます。

## KDDI WVS2 仮想ネットワークによる対策

KDDI WVS2 仮想ネットワークを利用することで、各拠点の LAN 構成を変更せずに

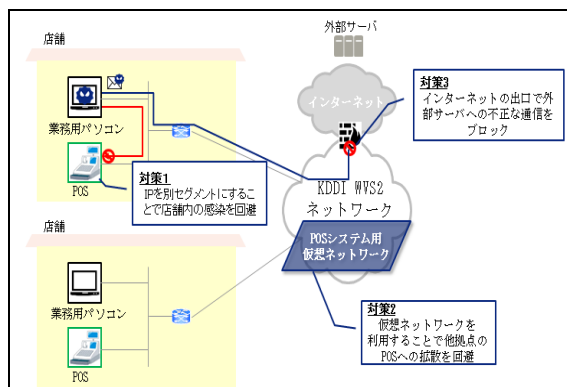


図 2 KDDI WVS2 仮想ネットワークによる対策

セキュリティ対策を行うことができます (図 2)。従来通り同一 LAN 上にパソコンと POS システムを接続したまま、それぞれの IP サブネットを異なるものにすることで、疎通可能な IP アドレスへの総当たり攻撃による POS システムの検知を回避し PC から POS システムへのマルウェアの感染を防ぎます。既存の LAN 環境で同様の対策を実施する場合、経路情報を分離して保持できる高価なルータへの置換や、別に新たなルータを設置し物理的に接続を分ける必要があります。小規模拠点には見合わないコストと導入までの時間がかかりますが、KDDI WVS2 仮想ネットワークではコストをかけずに短期間での対策が可能です。具体的には、アドレス配布は L3VPN より行い、POS システムは MAC アドレスで識別を行うことで、パソコンとは異なる IP サブ






ネットのアドレスを配布します。そのうえで、仮想ネットワークでは IP アドレス単位で接続するネットワークの分離を行います。パソコンに割り当てられる IP アドレスの範囲からの通信については、L3VPN に転送し、既存のイントラ環境にアクセスさせます。POS システムに割り当てられる IP アドレスの範囲からの通信については、仮想ネットワークを転送先とします。これにより、万が一パソコンに侵入され、同一拠点の POS システムに不正アクセスされたとしても、その POS システムを踏み台としない限り、別拠点の POS にアクセスすることが出来ず、不正アクセスが広まるリスクを低減します。


さらに、KDDI WVS2 セキュリティアプライアンスにより、各拠点からインターネットへ抜ける通信を監視することで、侵入されたパソコンや POS システムから外部のサーバへの通信を検知、防御することができます。

今後増加が見込まれる IoT デバイスに対するセキュリティ対策が火急の問題となってきました。KDDI は KDDI WVS2 で提供する仮想ネットワークおよびセキュリティアプライアンスを用いることにより、低コストで迅速なセキュリティ対策の実現に向けたお手伝いをいたします。

KDDI ホームページ : <http://www.kddi.com/business/pr/spcloud/>

KDDI WVS2 のお問い合わせは KDDI および KDDI まとめてオフィスグループ営業担当者、または法人お客さまセンターにご連絡ください。

 0077-7007(無料)

 0120-921-919(無料)

受付時間 : 9:00~18:00 (土・日・祝日・年末年始を除く)