IoT（M2M もしくはスマート家電を含む）ネットワークサービスへの主な脅威候補

Candidates for 'Major Threats for IoT (Including M2M and/or Smart Consumer Electronics Devices) server side services'

近年、コンピュータ以外の（コンピュータ内蔵デバイス）をインターネットに接続して動作させることが一般化している。たとえば、スマート家電と言われているものの多くが様々な情報をインターネット上で交換する。家電製品だけではなく、自動販売機や様々な機器も同様で、M2M(Machine to Machine)もしくは IoT(Internet of Things)という言葉も生まれている。

Recently, many devices other than the computer, also known as smart consumer electronics devices(CED) are connected to the internet and exchanging various information through it. Not only CED but other devises such as vending machines are also connected to the internet. Those are called M2M (Machine to Machine) or IoT (Internet of Things).

こうした機器がインターネットに接続されることで、情報セキュリティ上の新たな問題も生じつつある。こうした機器がインターネット側からの攻撃対象となるような事態への懸念だ。デバイス側のセキュリティについては、ここ数年、様々な議論が行われ、専門家による注意喚起が行われた結果として、いくつかの取り組みも始まっている。

Connecting those 'things' to the internet causes new problems/threats in information security. Therefore, it is a concern about these devices to be attacked from the internet. Thanks to many efforts and discussions by security specialists, there has been start of some movements to improve security of those devices.

しかし、一方でまだ手つかずの問題もある。これらのデバイスの多くが、そのメーカーが提供するサービスを受けるために、クラウド上のサービスに接続されている。これらのサービスは多岐にわたり、日常的なデータ交換から、デバイスのソフトウエアの更新までを担っている。

On the other hand, some threats are still remaining. For example, many of those devices are connected to and given control by service provider by its makers from cloud. Those services may provide various functions from daily data exchange to software update for devices.

こうした、サービスのセキュリティが侵害された場合、その影響は単一のデバイスが侵害された場合に比べて遙かに大きなものとなる。攻撃が成功することで、攻撃者は非常に多

数のデバイスを制御出来る可能性があるからだ。コンピュータアプリケーションの多くが、最近では同様のしくみを持っており、実際、サービスサイトが侵害された事による被害も報告されている。対象がデバイスの場合は、アプリケーション以上にユーザが気づきにくいという特徴もあり、より長時間侵害が持続する可能性もある。

If those services are breached, results are much worse than causing a single device, because the attacker may have control over a large number of devices when the attack is succeeded. Many of recent computer applications are same, but it can be much worse and last longer if a service for device is breached, and would be hard for the users to realize.

日本クラウドセキュリティアライアンスとそのワーキンググループは、この問題に取り組むべく、こうしたサービスがさらされるであろう脅威の洗い出しに着手した。以下は、その議論のための材料として提供される、脅威の候補である。

Cloud Security Alliance Japan Chapter and its working group has started the discussion about this issue, and at the first stage we are going to figure out those threats for services. Threats described below are candidates for following discussion.

脅威の候補
Candidates of Threat

１．サービスの妨害、停止
1. Denial of Services

もし、デバイスがその動作に必須の情報をサービスから得ている場合、サービスの停止またはレスポンスの低下により不具合を引き起こす可能性がある。こうした障害は、サービスに依存している大量のデバイスに、ほぼ同時に発生する可能性が有り、社会的な混乱をもたらす可能性がある。

If those devices retrieve information or data which is crucial for its function, failure or degraded response of services may cause device failure. It may happen concurrently to a huge number of devices and it may cause social confusion.

２．誤った情報の流布
2. Propagation of false information

デバイスが受け取る情報をサーバ側で改ざんすることで、攻撃者が意図した情報を様々な形で流布できる可能性がある。これによる社会混乱などが引き起こされる可能性がある。

Attacker may be able to propagate incorrect or false information by manipulating them at source. It may also cause social confusion.

３．不正なデータによる機器の乗っ取りや妨害
3. Disturbing or Hijacking devices using manipulated data

デバイスが、サーバから受け取ったデータによりその動作を決定する場合、そのデータをサーバ側で改ざんすることにより、デバイスの動作を妨害したり、意図的に特定の動作を

させたりすることができる可能性がある。

If devices determine its action by data received from the server, the attacker may disturb or worsen the control devices by manipulating data at source.

４．収集された様々な情報の漏洩や悪用
4. Data breach and malicious use of collected data in server

サーバにはデバイスから収集された大量のデータが格納されている場合がある。ユーザ情報もしくは匿名情報にかかわらず、こうした情報が漏洩したり、それらを悪用されることで、様々な問題が生じうる。

There are sometimes huge amount of collected data in servers. No matter if it is named or anonymized, breach or malicious use of those data may cause various problems.

５．スクリプト、アプリケーションコードの改ざん
5. Malicious change on application code or script

多くのデバイスがサーバ側から受け取るアプリケーションやスクリプトコードを動作させる仕組みを有している。これらのコードをサーバ側で変更することで、攻撃者はデバイスに対して任意の動作を実行できる可能性がある。

Many devices have features to run application or script code provided by server. Attacker may execute their own code on devices to do something by changing application or code at source.

６．デバイスに配布するシステムソフトウエア（ファームウエア）改ざん
6. Malicious change to system software (firmware) to be delivered to devices

デバイスのシステムソフトウエア（ファームウエア）の自動更新機能を利用して、攻撃者は改ざんされたコードをデバイスに配布できる。これにより、攻撃者はデバイスの制御を完全に奪うことができ、デバイスを様々な用途に使用することができる。

Attacker can distribute manipulated or their own system software (firmware) to devices. Attacker may get full control of devices and do various things with those devices.

７．不正なデバイスもしくは個別に乗っ取られたデバイスからのサーバ侵害
7. Attack against services from unauthorized or locally hijacked devices

サービスのデバイス認証が不完全な場合や回避手段がある場合、もしくは正規のデバイスがなんらかの方法で乗っ取られた場合、攻撃者がそれらを利用してサービスに対し有効な攻撃を行うことができる可能性がある。この攻撃が成功した場合、１～６に述べたすべての脅威をもたらす可能性がある。

If the service do not authorize devices properly (including existence of possible evasion technique) or even a legitimate device, and if hijacked, the attacker may use those devices for effective attack to the service. All threats described above can be brought if this attack succeed.

８．他サービスとのデータ授受インターフェイスに対する侵害
8. Abuse of interface for data exchange with other services

IoT 化のビジネス目的のひとつが、多くのデバイスから収集されたデータの活用であり、今後、様々なサービス間でデータの相互利用が活発になると考えられる。こうした他のサービスや他事業者とのインターフェイスの不正利用や攻撃により、サービスが侵害される可能性がある。

Since one of major business objective to deploy IoT is to collect and analyze useful customer data. In the age of Big Data, those data are transferred between different services or service providers. This type of interfaces (or API) may be abused or attacked to breach security of services.

ここに挙げた脅威には、攻撃等の目的もしくは結果、手段が混在している。このワーキンググループでは、次のステップとして、こうしたカテゴリによる分類を行うと同時に、様々なサービスとの関係を明らかにすることによって、IoT へのサービスを提供する事業者が自らのリスクを正しく評価できるようなフレームワークを構築していく。

Listed threats are still mixture of objectives, attack methods, attack outcome. Our working group is aiming to create useful framework for IoT service providers by categorizing and analyzing those threats and clarifying relationships between various services and threats.

これらは、多くの脅威の中の一部かもしれない。我々は、今後、さらに検討を進め、こうした脅威に対する有効な対策を提言していく。

These might be only a part of various threats. We'll continue this research and propose effective measures against those threats.

一般社団法人　日本クラウドセキュリティアライアンス
IoT クラウドサービスワーキンググループ

Cloud Security Alliance Japan Chapter Inc.
IoT Cloud Service Working Group