2018 年 6 月 22 日

サービス＆セキュリティ株式会社 e-Gate センター

IoT 機器に対するサイバー攻撃の脅威と対策

1. 背景

コンピュータや携帯電話だけでなく、あらゆる機器によって「IoT（Internet of Things、モノのインターネット）」が形成される社会になろうとしています。総務省の情報通信白書では世界の IoT 機器の数が 2020 年には 300 億台に達するとされています。一方、機器がインターネットにつながることでサイバー攻撃の対象となり、被害数は増加し続けています。独立行政法人情報処理推進機構（IPA）が発表した「情報セキュリティ 10 大脅威　2018」では IoT 機器に関する脅威が挙げられています。IoT 機器を狙ったサイバー攻撃の対策は喫緊の課題です。

e-Gate センターにおいても IoT 機器に対するサイバー攻撃が確認されています。図 1 は e-Gate センターの監視するシステムにおける IoT 機器への攻撃イベント数の推移です。2018 年 1 月以降、イベント数が増加している傾向がよみとれます。

【図 1　IoT 機器に対する攻撃イベント数の推移】

これらの攻撃イベントは、IoT 機器をターゲットにしたマルウェア「Mirai」の亜種を利用したものと考えられます。あらゆる機器がインターネットにつながる社会において、IoT 機器に対するサイバー攻撃の問題は避けて通ることができません。重要な情報を盗まれる被害にあったり、踏み台として攻撃に加担させられ加害者となる可能性があります。正しい情報を把握して早期に対応することが必要です。

2. IoT 機器に対するサイバー攻撃のトレンドと対策例

IoT 機器の中でサイバー攻撃の対象とされることが多いのはルータやアクセスポイント、ネットワークカメラなどです。2016 年以降、「Mirai」は IoT 機器を乗っ取って踏み台にする DDoS 攻撃（Distributed Denial of Service、分散型サービス不能攻撃）に利用されてきました。 2017 年から 2018 年にかけては「Mirai」の亜種である「Satori」や「Wicked」などが現れ、IoT 機器に侵入し遠隔でコマンドを実行するなどの攻撃活動を行っています。

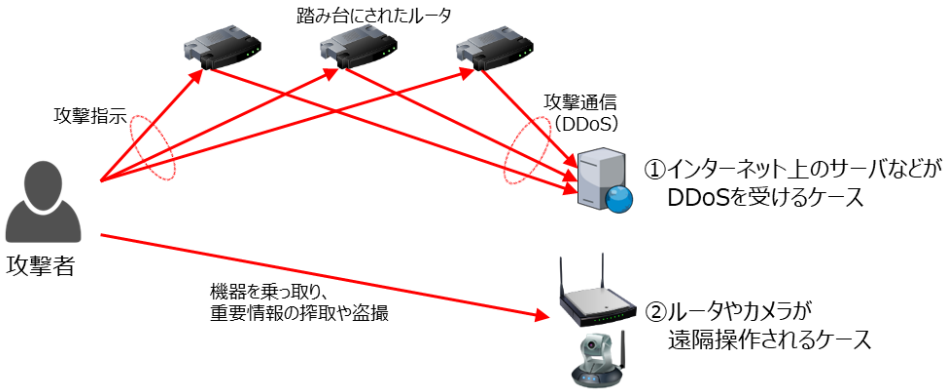
以下では IoT 機器に対する攻撃の例と対策について説明します。

⑴ ルータやカメラを狙った攻撃

IoT 機器への攻撃に共通していることは、初期設定値をはじめとする簡単な ID とパスワードでのログインを試みることです。ログイン成功後、機器がどのように攻撃に利用されるかが異なります。

① DDoS 攻撃の踏み台になるケース：図 2 の①のようにルータなどの IoT 機器を踏み台としてインターネット上のサーバを攻撃対象とするものです。ルータは直接被害を受けるのではなく、踏み台となって攻撃に加担する加害者となります。攻撃者は複数のルータを踏み台として利用し、特定のサーバに対して DDoS 攻撃を行います。2016 年に確認された事案では実に 38 万台以上の IoT 機器が踏み台になり 620Gbps の大規模な攻撃が行われました。

② 遠隔操作で情報搾取・盗撮するケース：図 2 の②のようにルータやカメラを対象とするものです。攻撃者は簡単な ID とパスワードでのアクセスによって、IoT 機器を乗っ取ろうとします。ログインに成功すると、対象がルータの場合は内部ネットワークへの不正な侵入を可能にし重要な情報を盗むなどの攻撃が可能です。対象がカメラである場合は盗撮等の被害が発生します。2018 年には自治体が河川監視のために設置したカメラの映像に攻撃者のメッセージが表示されるという事案がありました。



【図 2　IoT 機器に対するサイバー攻撃の例】

⑵ IoT 機器に対するサイバー攻撃の対策例

① 上述のような攻撃を対策するには、まず機器の管理者パスワードを初期値から変更することです。英数字や記号を混在させ、できるだけ長いパスワード（目安として 8 文字以上）を設定してください。また、機器のソフトウェアを脆弱性対策済のバージョンに更新します。CVE（共通脆弱性識別子）情報や機器ベンダのウェブサイトを参照して脆弱性の有無を確認し、対策済のソフトウェアがリリースされている場合は速やかに更新してください。

② 機器の脆弱性に対策したソフトウェアに更新できない場合や機器のハードウェアなどの制約で対策が不可能な場合、FW（ファイアウォール）や UTM（統合脅威管理）、IPS（侵入防御システム）といったセキュリティ対策装置を利用します。これらの機器をインターネットと IoT 機器の経路上に設置することで、悪意ある攻撃を検知、遮断することができます。

⑶ 参考情報

情報通信白書（総務省）
http://www.soumu.go.jp/johotsusintokei/whitepaper/index.html

情報セキュリティ 10 大脅威 2018（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/vuln/10threats2018.html

Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威（Japan Vulnerability Notes）
https://jvn.jp/ta/JVNTA95530271/

3. e-Gate の活用について

サイバー攻撃を早期に発見する為には、前述の対策例のようにセキュリティ機器を導入し、それらの機器を運用監視することが重要です。SSK の総合セキュリティサービス「e-Gate」では、最新の分析システムを活用し精度の高い検知、また専任のアナリストによる分析を行っております。「e-Gate」のセキュリティ監視サービスをご活用頂くことにより迅速なセキュリティインシデント対応が可能となります。

■総合セキュリティサービス
SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター”この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。
【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp