金融機関等を狙った DDoS 攻撃を観測、脅迫型 DDoS 攻撃も警戒が必要
ダークネット観測レポート（FY2020 2Q）

BB ソフトサービス株式会社
株式会社クルウィット

BB ソフトサービス株式会社（以下、「BBSS」）と株式会社クルウィット（以下、「クルウィット」）は、IoT 機器やサイバー攻撃の実態を可視化するため、ダークネット観測リポート（2020 年 7 月～9 月分）を発行します。

https://securie.jp/usecase/iotreport/fy2020_2q.html

■観測パケット数

2020 年 7～9 月期におけるダークネット宛のパケット数については、図 1 の観測結果となりました。探索目的と思われる UDP パケットのスキャンが多く見受けられ、また金融機関等を狙ったと思われる DDoS 攻撃の通信も観測されました。特に 2020 年 8 月以降からは、金銭を支払わなければ DDoS 攻撃を行うといったランサム DDoS 攻撃が、複数のサイバー攻撃者グループにより行われているため、警戒が必要です。

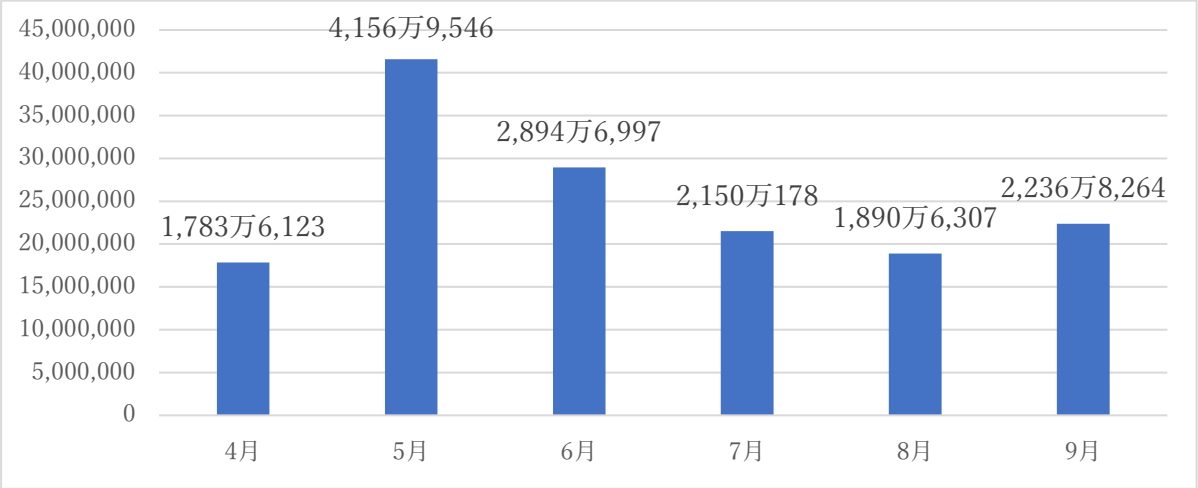


図 1　観測パケット数

■観測ホスト数

当該期間におけるダークネット宛に通信をしたホスト数については、9 月に探索または調査目的であろうと思われる通信を行う機器の増加を観測しました。

	4月	5月	6月	7月	8月	9月
ホスト数	45万 6,127	377万 2,713	46万 7,461	45万 1,330	40万 7,424	60万720
国内ホスト数(*)	2,313	93,005	2,546	3,066	3,128	2,500

図 2　観測ホスト数

*国内ホスト数：IP アドレスを逆引きして.jp ドメインだったもの。

■宛先ポート番号

当該期間におけるダークネット宛への宛先ポート番号の観測状況については、445/TCP(microsoft-ds)を狙った通信を観測しており、7 月下旬と 9 月上旬に一時的な通信量の増加を確認しました。次に 1433/TCP（ms-sql-s）は、Windows のデータベースサーバーを狙った通信であり、445/TCP と同様に PC を対象とした通信も従来から続いています。そして、22/TCP(ssh)、23/TCP(telnet)、80/TCP(http)については、IoT 機器(ルーター等)を狙った通信であり、実際には IoT 機器に対する通信が多く観測されています。

順位	4月	5月	6月	7月	8月	9月
1	23/TCP	23/TCP	445/TCP	445/TCP	445/TCP	445/TCP
2	1433/TCP	445/TCP	23/TCP	23/TCP	23/TCP	23/TCP
3	445/TCP	1433/TCP	1433/TCP	1433/TCP	1433/TCP	1433/TCP
4	52869/TCP	80/TCP	52869/TCP	80/TCP	22/TCP	22/TCP
5	80/TCP	22/TCP	80/TCP	22/TCP	80/TCP	80/TCP

図 3　宛先ポート番号

■送信元の国別観測状況

当該期間におけるダークネット宛に通信をした国別状況については、図 4 の観測結果となりました。

順位	4月	5月	6月	7月	8月	9月

1	アメリカ(US)	アメリカ(US)	不明(N/A)	不明(N/A)	不明(N/A)	アメリカ(US)
2	不明(N/A)	中国(CN)	スイス(CH)	アメリカ(US)	アメリカ(US)	不明(N/A)
3	中国(CN)	不明(N/A)	アメリカ(US)	中国(CN)	中国(CN)	セーシェル(SC)
4	ロシア(RU)	ロシア(RU)	セーシェル(SC)	セーシェル(SC)	セーシェル(SC)	中国(CN)
5	セーシェル(SC)	セーシェル(SC)	中国(CN)	ロシア(RU)	ロシア(RU)	ロシア(RU)

図 4　送信元の国別観測状況

■考察

この 3 カ月の傾向として、攻撃者は PC のネットワークやサーバーを狙ってセキュリティホールを探す探索・調査を行っている傾向があります。見境なしに攻撃できる対象を探しており、セキュリティ対策を怠ってしまうと侵入されてしまう可能性があります。また最近の傾向として金銭を払わないと DDoS 攻撃を行うといったランサムウエアに似た脅迫型の攻撃も出てきており注意が必要です。

今回の観測データで、DDoS 攻撃の元となっている機器について詳細に確認できておりませんが、セキュリティ対策の取られていない IoT 機器も DDoS 攻撃に利用されていると考えられます。過去には IoT 機器の脆弱性を狙うマルウエア「Mirai」に ISP ルーターが感染し、ユーザーがインターネット接続できなくなったり、ボットネット化した IoT 機器がサイバー攻撃に利用されるという事例がありました。このような IoT ボットネットの派生は現在も作られ続けています。家庭内の IoT 機器が多様化し、在宅勤務で家庭のインターネット環境の安定性・安全性への需要も高まる中、ホームネットワークと IoT 機器を安全に保つ対策が求められます。

■IoT 機器を攻撃から守るためには？

1. IoT 機器をしっかり調べて購入する。

安くてセキュリティ対策がしっかり施されていない製品もあるため、メーカーホームページでセキュリティ対策を実施しているか？　もしくはセキュリティパッチ情報が定期的に更新されているかどうかを確認しましょう。

2. 初期パスワードを変更する

多くのルーターや IoT 機器には、メーカーが初期パスワードを設定しています。このパスワードを変更しないまま放置しておくと、不正侵入の原因となるため、必ず変更するようにしてください。パスワードは 8 文字以上で作成し、大文字・小文字・数字・特殊文字を使用すると強度が高くなります。

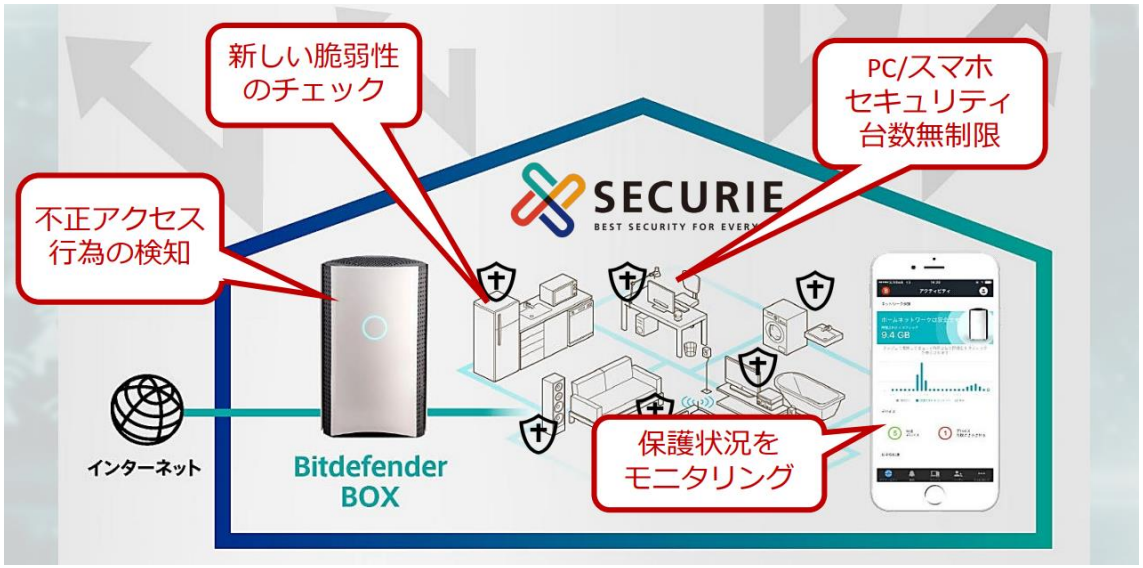
3. セキュリティ更新や修正情報を確認する

メーカーが発表している最新のセキュリティパッチ情報を常に確認し、OS やファームウェアを最新に保つようにしてください。または脆弱性診断ツールを使用して、自動的にこれらの情報を確認でき

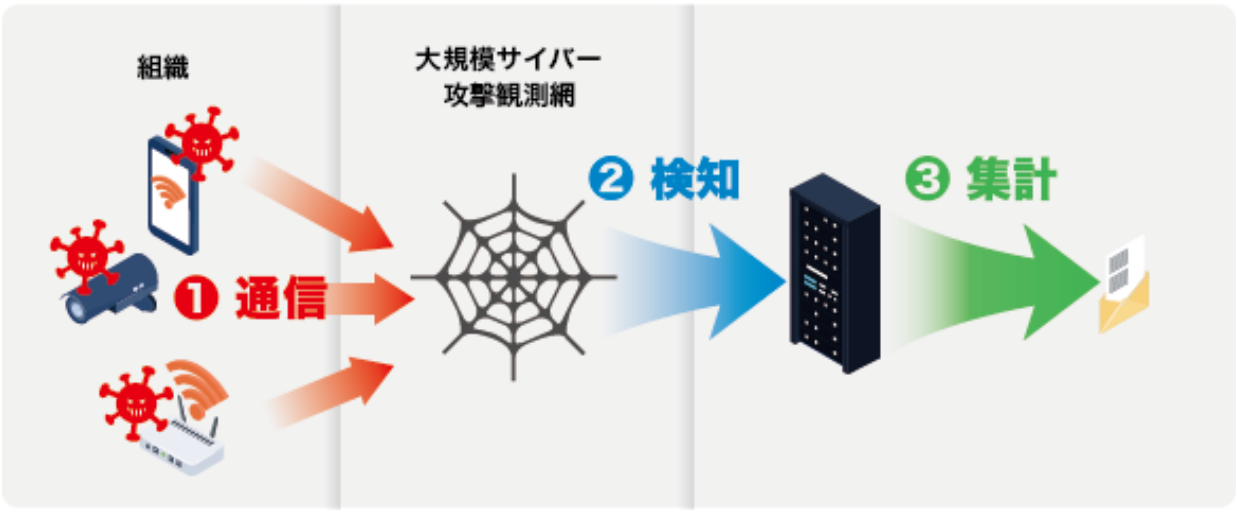
るようにすると便利です。

4. IoT 機器専用の Wi-Fi ネットワークを作る
IoT 機器用にもう 1 台ルーターを用意し、個人情報など重要な情報を保存している PC やリモートワークで使用する PC 等と、IoT 機器の Wi-Fi ネットワークを分けておきます。この方法により、万が一 IoT 機器がハッキングされた場合でも、個人情報に侵入される心配はありません。多くのルーターは、ゲストネットワークを設定できるようになっていますので、この機能も活用しましょう。

5. 専用のソリューション（セキュリティ機能付き Wi-Fi ルーター）を導入する
SECURIE powered by Bitdefender は、IoT 機器、PC、タブレット、スマートフォンなどをまとめて保護します。弱いパスワードなどのデバイスの脆弱性を自動的にスキャンする脆弱性診断や、普段の動きを把握し、異なる通信をした場合に検知する異常検知、攻撃の侵入検知など、ホームネットワークを侵入から防ぐ機能が搭載されています。さらに、高性能セキュリティソフトが台数無制限でご利用いただけますので、外出中でもモバイルデバイスを守ることができます。



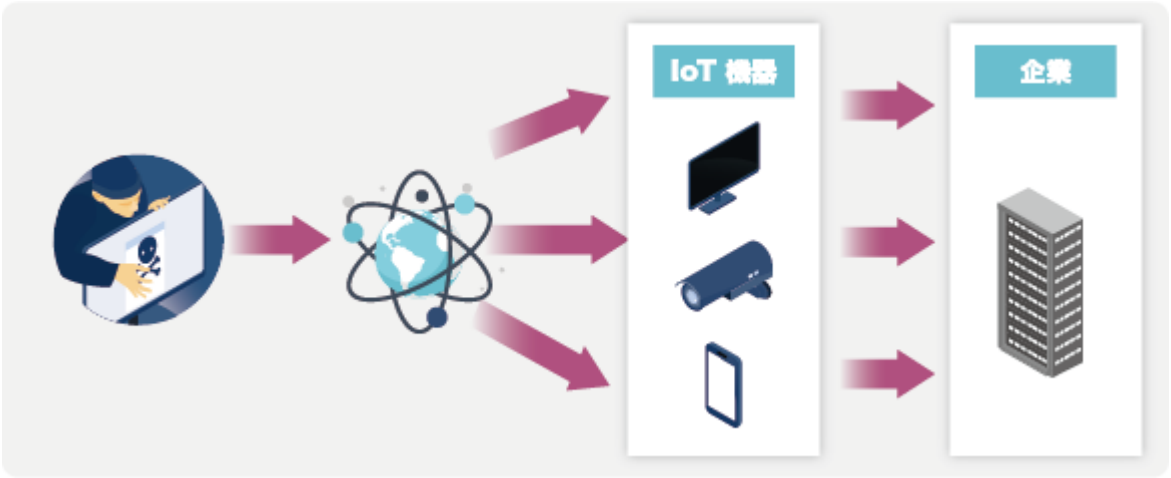
■ダークネット観測レポートとは
クルウィットが運用しているダークネット観測サービス「SITE VISOR」で計測したデータをもとに、IoT 機器などへの攻撃傾向を把握します。だれも利用していない IP アドレスをネット上に配置、その IP アドレスにどのような攻撃を想定したアクセスをしてきたか？を調査し、攻撃の傾向をレポート致します。



■IoT 機器への攻撃

IoT 機器を攻撃する専用のウイルスがあり代表的なマルウエア「Mirai」と言われるものがあります。スマートスピーカーなどの IoT 機器を踏み台にして、企業などを攻撃します。

たとえ IoT 機器がマルウエアに感染したとしても、実被害がでる可能性は低いが、犯罪者の犯罪の片棒を担ぐこととなります。場合によっては警察からの事情聴取などで拘束・端末の没収をされる可能性もあります。



■IoT 機器への攻撃の種類

犯罪者はポートを利用して攻撃を仕掛けてきます。ポートとは機器同士が通信を行うときのドア（出入口）のようなもので番号がつけられています。犯罪者がよく使うのは「遠隔操作ができる」ポートです。これを悪用すれば、IoT 機器を含めたパソコンや IoT 機器を操作することができます。

犯罪者が IoT 機器を攻撃するためにアクセスしてくる代表的なポート

ポート番号	役割
ポート22	管理用コマンドを使った遠隔操作をする (ssh)
ポート23	管理用コマンドを使った遠隔操作をする(telnet)
ポート80	ルーターなどの管理画面へアクセスする (http)
ポート81	ルーターなどの管理画面へアクセスする(http)
ポート8080	Webカメラやルーターなどのログイン画面へアクセスする(http)
ポート5555	Android開発用環境からIoT機器アクセスする(ADB)

IoT 機器はインターネットにつながっている機器という認識が薄く、ログイン ID やパスワードを購入時のまま変更してなかったり、変更していても簡単なものに設定してしまっていたりすることも多いようです。犯罪者はそのような機器を狙っています。

■BB ソフトサービス株式会社について

ソフトバンクグループにおいて、セキュリティ製品を主軸とするソフトウェアサービスを、ISP や携帯電話会社などの通信事業者を通じて提供しています。サービス提供のみならず、フィッシング対策協議会やその他の社外団体を通じた情報セキュリティに関する啓発活動にも積極的に取り組んでいます。一般消費者のサイバー犯罪被害を減らし、よりよいインターネット利用環境を全てのユーザーに提供することで社会貢献を果たしてまいります。

■株式会社クルウィットについて

「インターネットサービス」と「情報セキュリティ」の 2 つの事業を中心に、誰でも安心してインターネットが利用できるよう研究開発を行っています。その研究開発で培った技術やノウハウをもとにダークネット監視サービス「SITEVISOR」を開発・運用しています。

事業を通じてお客様に末永く満足いただけるサービスを提供していくと同時に企業価値・信用度・認知度の向上に務めてまいります。

＜会社概要＞

社名：　BB ソフトサービス株式会社

所在地：　東京都中央区銀座 6-18-2　野村不動産銀座ビル 14 階

社長：　代表取締役社長 兼 CEO　瀧　進太郎

設立日：　2006 年 1 月 17 日

株主：　SB C&S 株式会社　100%

事業内容：　ブロードバンドを利用したコンシューマー・SOHO 用アプリケーションサービス、およびオリジナルアプリケーションサービスの企画・開発・販売・運営

URL：　https://www.bbss.co.jp/home.html

＜お問い合わせ先＞
BBSS 広報事務局（株式会社カーツメディアコミュニケーション内）
担当：堀川、大塚　TEL：03-6261-7413