資料７－２

NOTICEの活動について

NOTiCE

令和６年５月10日
事務局

❶ NOTICEの活動概要

サイバー攻撃による被害事例

CASE 01 2016年

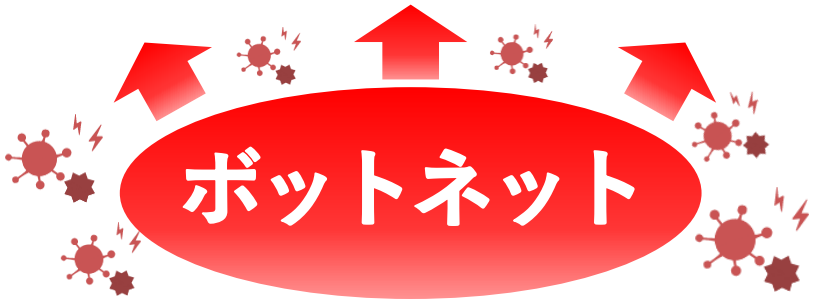
「Mirai」に数百万台以上のIoT機器が感染し、
世界中のウェブサイトやオンラインサービスが停止

CASE 02 2018年

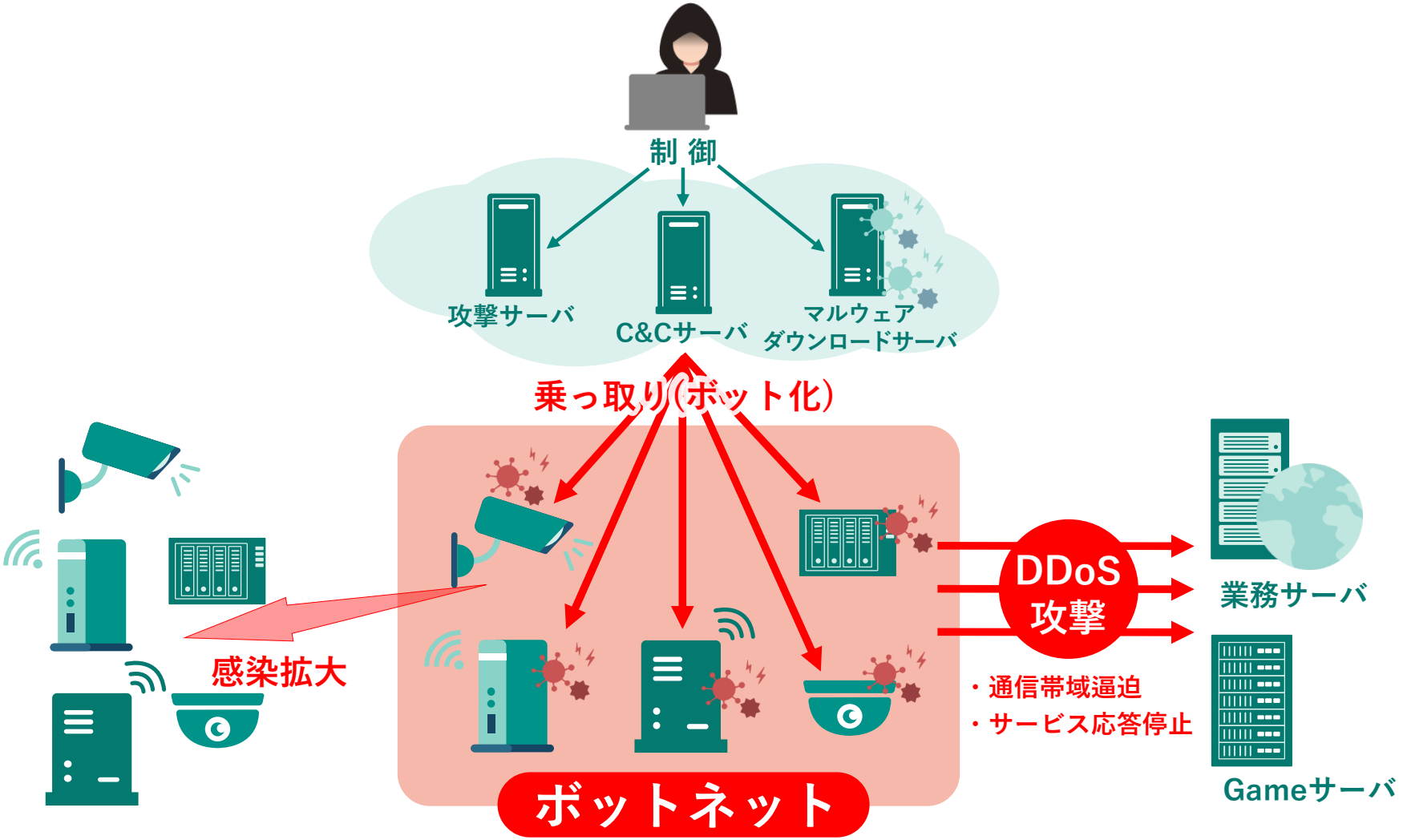
IoT機器を使用不能に陥らせるおそれのある
「VPNFilter」が世界中で50万台以上に感染

CASE 03 2022年

マンション用のWi-Fiルーターが「Fodcha」に感染し、
通信停止や速度制限の被害が発生



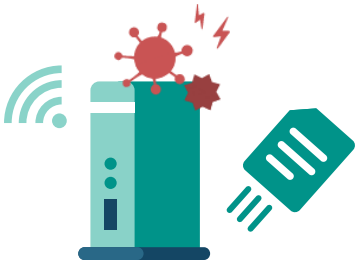
「ボットネット」とは


制 御
攻撃サーバ
C&Cサーバ
マルウェア
ダウンロードサーバ
乗っ取り（ボット化）
感染拡大
DDoS
攻撃
・通信帯域逼迫
・サービス応答停止
業務サーバ
Gameサーバ
ボットネット

IoT機器の乗っ取りによる被害例

ルーターが乗っ取られ、サイバー攻撃の踏み台にされてしまう

2021年8月から9月にかけて、過去最大級のサイバー攻撃が世界各地で相次いで発生した。新種のボットネット「Meris」によるもので、標的に大量のデータトラフィックを送り付けてサービス不能状態に陥れるDDoS攻撃が25万台のルーターから仕掛けられていた。



ルーターが攻撃され、個人情報などが盗まれる

X氏は、知らないうちに 数万円が銀行口座から不正送金されていた。原因は家庭用ルータのDNS設定が改変されていたこと。DNS設定を変更することでサイバー犯罪者は、X氏の通信をすべて傍受し、銀行口座の認証情報を含むさまざまな情報を入手していたとみられる。

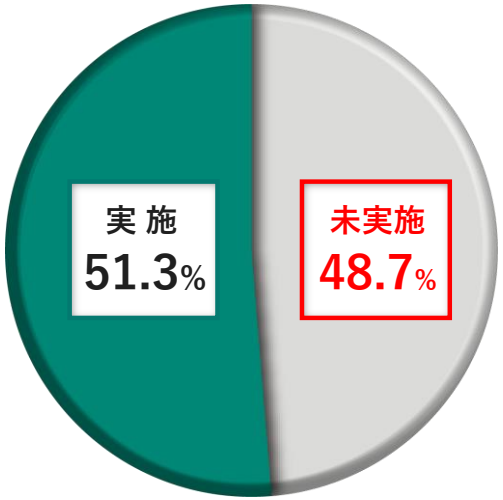
ネットワークカメラの映像が第三者に覗かれる

学校防犯システムと保育所見守りカメラにおいて、マルウェア感染の特徴のある通信を国立研究開発法人情報通信研究機構（NICT）が観測した。十分なセキュリティ対策が行われていないことにより、マルウェアに感染し、どちらも第三者から映像が閲覧できる状態になっていた。また、保育所ではインターネットが使えない状態となっていた。

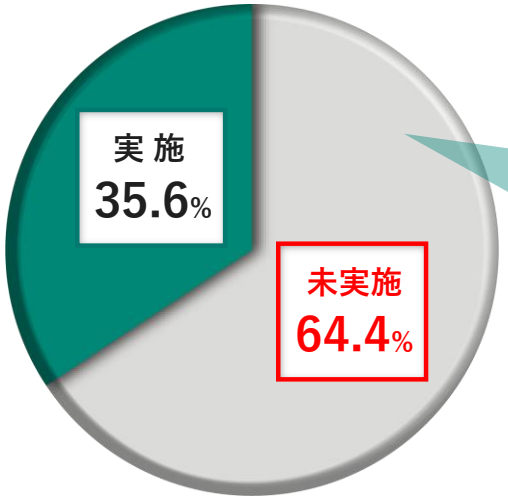
対策の難しさ①

一般生活者のIoT機器セキュリティ対策実施率

全　体



ITリテラシー低層



「ゲートウェイ」「ポート」「ファームウェア」「マルウェア」「グローバルIPアドレス」「サイバー攻撃」「プロトコル」の用語のうち１つ以上で「知らない」と回答した人

理 由（記術式）

“リスクの内容を詳しく知らない”

“何をしたらいいのかわからない”

多くの生活者が

リスクを知らない　　**対策法を知らない**

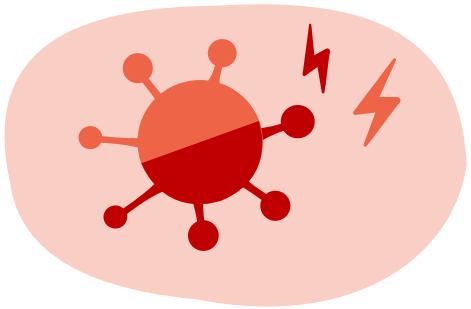
※サンプル数：個人ユーザー2000ss／法人ユーザー（セキュリティ部門担当者）200ss
※NOTICE「一般生活者に対するIoT機器セキュリティ対策意識アンケート調査」（2023年9月実施）

対策の難しさ②

国内

マルウェア感染IoT機器検知数

（≒ボット化している可能性のあるIoT機器検知数）



最大 1,419 件/日

ボットネットの特徴 → 乗っ取られに気づきにくい/24時間稼働している

ボット化するIoT機器 → ルーター/監視カメラシステム（ネットワークカメラ）

* 2024年3月の観測結果

NOTICEの活動の３本柱

目　的

IoT機器のセキュリティ対策向上を推進することにより、

ボットネットによる**サイバー攻撃の発生や被害を未然に防ぐ**

活動内容

活動01 → 脆弱なIoT機器の **観測**

活動02 → IoT機器のリスクと対策への **意識啓発**

活動03 → リスクが高いIoT機器管理者への **注意喚起**

活動①「観測」

活動01 観測

1 脆弱性のあるIoT機器を観測

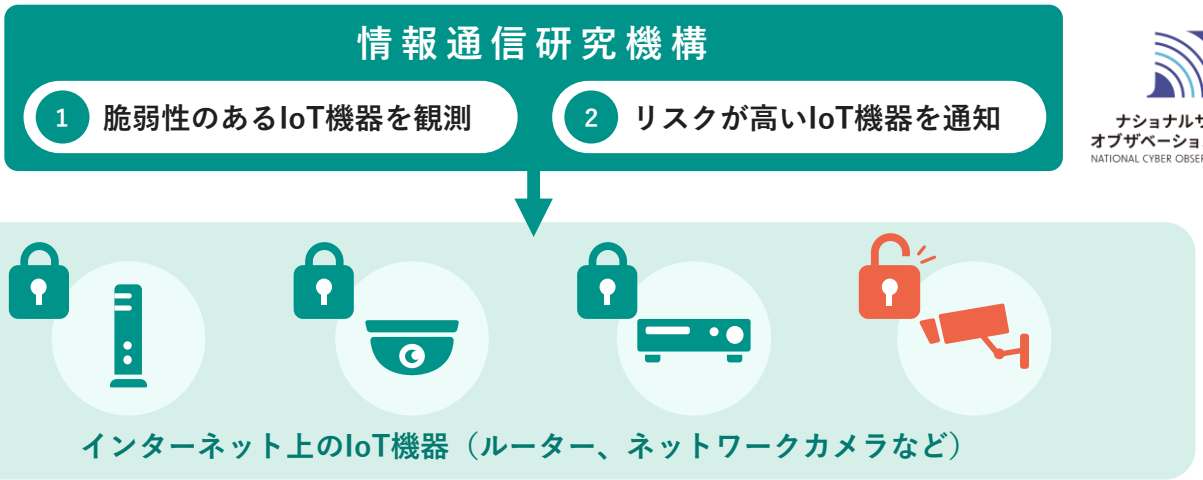
NICTが、参加ISPのネットワークに直接接続されているIoT機器を対象に、「脆弱性のあるIoT機器」があるかどうかを定期的に観測

※「脆弱性のあるIoT機器」＝ 推測されやすい管理者パスワードが設定されている／ファームウェアがアップデートされていないIoT機器

2 リスクが高いIoT機器を通知

①で観測したIoT機器のうち、悪用される恐れのある/既にサイバー攻撃に悪用されているIoT機器を「リスクが高いIoT機器」としてISPへ通知

※「リスクが高いIoT機器」＝ (1) その脆弱性が乗っ取りに繋がりうる、かつその脆弱性を突いた攻撃が既に報告されているIoT機器
(2) 既にマルウェアに感染しているIoT機器



活動①「観測」

活動01 観測

IoT機器観測総数

1.12 億件

参加インターネットサービスプロバイダ（ISP）のIPアドレスに対して観測している総数

容易に推測可能な ID・管理者パスワードである IoT機器

月 **10,137** 件

ファームウェアに 高リスク脆弱性を有するIoT機器

月 **15,019** 件

マルウェア感染IoT機器検知数

最大 **1,419** 件/日

* 2024年3月の観測結果

活動③「注意喚起」

活動03 注意喚起

1. ISPが、リスクが高いIoT機器の利用者に対して、電子メールや郵便で**注意喚起**を実施
2. 注意喚起を受けた管理者は、**「設定変更」**か**「該当する機器の買い替え」**が必要
3. 「NOTICEサポートセンター」が、注意喚起を受けた人への**ユーザーサポート**を提供

活動③「注意喚起」

2023年度の注意喚起対象数

	4月	5月	6月	7月	8月	9月
マルウェア感染IoT機器（１日当たり最大値）	565	1,021	1,200	1,009	1,238	997
	10月	11月	12月	1月	2月	3月
	6,300	3,792	780	2,100	1,244	1,419

	4月	5月	6月	7月	8月	9月
容易に推測可能なID・管理者パスワードであるIoT機器	4,685	4,888	5,063	5,122	5,055	5,162
	10月	11月	12月	1月	2月	3月
	5,162	5,181	5,190	5,443	5,492	5,402

※2024年4月以降は上記に加え「ファームウェアに高リスク脆弱性を有するIoT機器」についても注意喚起予定

❷ 令和６年度からの新しいNOTICE

NOTICEの歩み①

2016年10月 → **マルウェア「Mirai」による大規模なDDoS攻撃による ネットワーク障害の発生**

多数のIoT機器で構成されるボットネット（マルウェア「Mirai」の感染により乗っ取られたIoT機器群）からDDoS攻撃が実行され、米国の大手Webサービスが数時間に渡り、アクセスできない事態が発生しました。

↓

2017年9月 → **米国クラウド事業者に対する大規模なDDoS攻撃被害**

Googleの数千のIPアドレスを標的として、過去最大規模（最大2.5Tbps）のDDoS攻撃が発生。DNSなどを用いたリフレクション攻撃が6カ月にわたり続きました。

↓

2019年2月 → **NOTICEの発足へ**

→ **「ID・管理者パスワードに脆弱性のあるIoT機器」がメインスコープ**

NOTICEの歩み②

2022年9月 日本国内で感染したIoTボットネットによる海外への攻撃

日本国内でマンション入居者用の無料Wi-Fiサービス（全国で約30万世帯が利用）に使用していたWi-FiルーターがIoTボット（「Fodcha」と推定）に感染し、2022年9月20日から28日まで、海外に対する大規模なDDoS攻撃に悪用されました。これにより、上位の通信回線の停止や速度制限が行われました。

2023年8月 FBIによるQakbotのテイクダウン

米国を含む複数の国家が協力し、十数年にわたり大規模な感染基盤を世界中に広げてきた多機能マルウェア「Qakbot」を悪用したボットネットのテイクダウンに成功。「Qakbot」は全世界で70万台以上のデバイスに感染したマルウェアで、ランサムウェアなどの別のマルウェアを追加でダウンロードし感染させるなど、システムへの侵入窓口として多く使われていました。

- 「ファームウェアに脆弱性のあるIoT機器」の乗っ取りが増加
- サイバー攻撃者側も高度に組織化されるようになった

「ID・管理者パスワードの脆弱性」に対処するだけでは不十分

環境の変化

インターネットに接続されるIoT機器が**増加傾向**にある

↳ ID・管理者パスワードの脆弱性だけでなく、
ファームウェア脆弱性を突く乗っ取りが顕在化するなど、
リスクがあるIoT機器検知は増加傾向にある

↳ 観測結果に基づく事後対策だけでなく、
乗っ取られないための予防対策が進むように**意識啓発活動を強化**
セキュリティ対策の必要性を強く喚起する必要がある

2024年4月 → **“新NOTICE”の発足**

新しいNOTICEのミッション

プロジェクトミッション

ルーター等の乗っ取りの予防対策の推進、及び乗っ取られたルーター等のセキュリティ対策の見直しの推進によりIoTボットネットの活動を抑制し、これに起因する**サイバー攻撃の発生と被害を軽減**する。

ゴール

- ✓ インターネットに接続されたルーター等が適切に管理されている状態を実現する
- ✓ 高リスク脆弱性を選定し、これを有するルーター等を特定する能力を維持する
- ✓ 高リスク脆弱性を有するルーター等の管理者へ注意喚起する能力を維持する
- ✓ 特に深刻な高リスク脆弱性については、ステークホルダーによる連携対処を徹底する

令和6年度からの新たな取り組み

令和6年4月1日「国立研究開発法人情報通信研究機構法の一部を改正する等の法律」施行　※一部規定を除く

観測の強化

IoT機器の乗っ取りにつながる脆弱性を幅広く観測

▼「ID・管理者パスワードに脆弱性のあるIoT機器」を引き続き観測

▼「脆弱性があるファームウェア等を搭載しているIoT機器」、
「既にマルウェアに感染しているIoT機器」も観測対象に追加

意識啓発の強化

IoT機器セキュリティ対策への「必要性に関する気づき」の醸成
IoT機器セキュリティ対策への「心理的ハードル」の低減

▼ロゴ・ホームページの刷新/デジタル広告配信等の広報活動強化

▼ISP/SIer/メーカーなどステークホルダーとの連携を強化

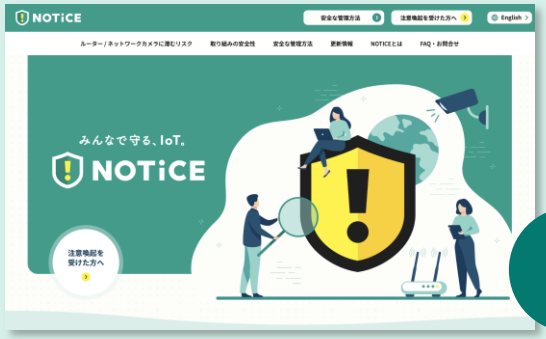
意識啓発の強化

旧ロゴ

NOTICE
National Operation Towards IoT Clean Environment

新ロゴ

NOTiCE



HP

フライヤー

国民の皆様に知っていただきたいこと

セキュリティ対策を行わずに

IoT機器を放置すると

気づかぬうちに**乗っ取られる**こと

適切に **定期的**に IoT機器を管理すれば

ボットネットによる被害は予防できる

IoT機器の管理者にお願いしたいこと

安全な管理ができているかのチェック項目

設置時

- ☑ 1 推測されにくい複雑な管理者パスワードに変更してください
- ☑ 2 ファームウェアが最新版でない場合はアップデートしてください
- ☑ 3 使用しない機能や設定は無効にしてください

定期的

- ☑ 4 ファームウェアが最新版でない場合はアップデートしてください
- ☑ 5 サポートが終了したルーターやネットワークカメラは買い替えをご検討ください

NOTICEプロジェクト体制の充実

NOTICEプロジェクト ステアリングコミッティー

総務省

国立研究開発法人
情報通信研究機構
（NICT）

ナショナルサイバーオブザベーションセンター
NATIONAL CYBER OBSERVATION CENTER

一般社団法人
ICT-ISAC

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

インターネットサービスプロバイダ（ISP）

ルーター/ネットワークカメラ 各製造メーカー
（令和6年度より参画）

ご清聴ありがとうございました