資料1-4

「サイバーセキュリティ意識・行動強化プログラム」に基づく総務省の取組

総務省　サイバーセキュリティ統括官室

公衆無線LAN（Wi-Fi）関係ガイドラインの改定

- 総務省では、公衆無線LANの提供者・利用者向けにガイドラインを作成しており、周知啓発に活用。
- 現行版と比べ、WPA3等の新技術も出てきていることから、現在、内容の見直しを実施中。
- 改定版ができた場合、Wi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に改めて周知予定。

提供者向け

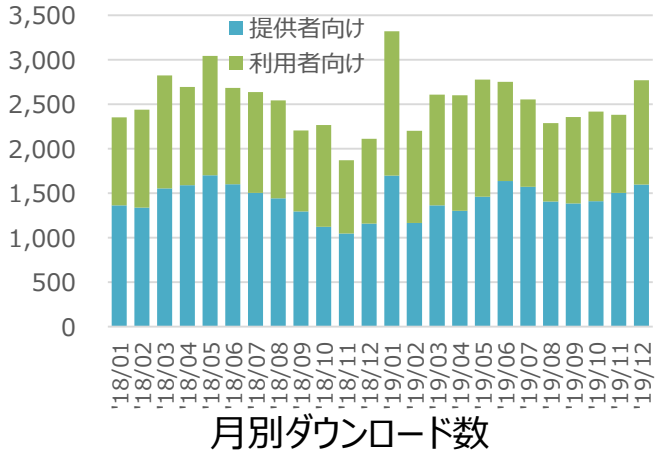
利用者向け

「Wi-Fi提供者向け セキュリティ対策の手引き」の見直し

現行版（2016年８月版）について、次の観点から見直しを実施中

- ✓新技術動向（WPA3、Enhanced Open、Wi-Fi 6等）を反映
- ✓対象者の明確化（自店利用者のみへの提供も対象）
- ✓偽アクセスポイント対策について追記
- ✓提供環境に応じたセキュリティ対策が必要であることを明示
- ✓セキュリティ対策状況の利用者への周知が必要であることを明確化

年間約３万件のWeb閲覧数



「Wi-Fi利用者向け 簡易マニュアル」の見直し

現行版（2015年３月版）について、次の観点から見直しを実施中

- ✓新技術動向（WPA3、Enhanced Open、Wi-Fi 6等）を反映
- ✓「公衆利用」と、限定的な「家庭・職場利用」の差異を明確化
- ✓TLS(SSL)による上位レイヤーでの暗号化について追記
- ✓無線LANルータ等の管理用ID・パスワードの設定変更について追記

公衆無線LAN（Wi-Fi）の利用に関する周知啓発

- 公衆無線LANの利用者のセキュリティ対策に関する周知啓発を目的として、**オンライン動画講座**を開講。（2020年２月10日～3月23日）
- 無線LANのセキュリティ対策に関する**ショートムービー**を作成し**SNSを通じて周知**予定（本年３月）。

オンライン動画講座

- ✓有識者が、公衆無線LAN利用時のリスクや、適切なセキュリティ対策を動画(全10回)により紹介
- ✓オンライン講座プラットフォーム「gacco」にて配信
  https://gacco.org/wifi-security/
  （2020年２月10日～３月23日）

第１回：もっとつながる・使える公衆無線LAN＜Wi-Fiの技術＞
第２回：とっても危険！「野良Wi-Fi」
第３回：そのWi-Fi、本物ですか？
第４回：さまざまな公衆無線LANサービスを知ろう
第５回：Wi-Fiの接続と暗号化の仕組み
第６回：安全なWeb利用の方法
第７回：自分で重要な通信内容を守る
第８回：より安全・安心にWi-Fiを使うために
第９回(追加講義)：Wi-Fi規格の最新動向
第10回(追加講義)：自宅や外出先で行う最新のセキュリティ対策とは

SNSを用いた周知啓発

- ✓無線LANのセキュリティ対策に関し、20秒程度の動画コンテンツを作成（全３種）
- ✓若年層を含む利用者への周知のため、SNSを通じて作成動画を周知
- ✓動画から上記オンライン動画講座にリンクを張ることで相乗効果を期待

＜動画① 知らない接続先を使わない＞

その他、「動画② HTTPSの利用・確認」「動画③ 管理用パスワード等の適切な設定」を作成中

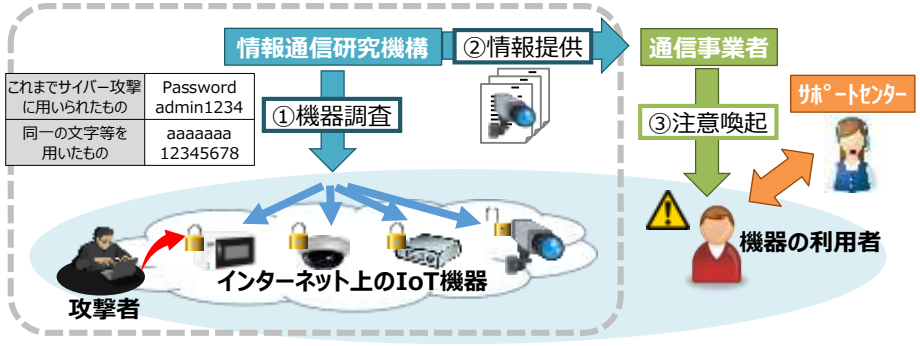
IoT機器調査及び利用者への注意喚起（NOTICE）

- 情報通信研究機構（NICT）が**サイバー攻撃に悪用されるおそれのあるIoT機器**を調査し、インターネットプロバイダを通じた利用者への注意喚起を行う取組「**NOTICE**」を2019年２月より実施。
- NOTICEの取組に加え、**マルウェアに感染しているIoT機器**をNICTの「**NICTER**」プロジェクトで得られた情報を基に特定し、インターネットプロバイダから利用者へ注意喚起を行う取組を2019年６月より開始。

（１）NOTICEプロジェクトの推進

（調査対象）パスワード設定等に不備があり、サイバー攻撃に悪用されるおそれのあるIoT機器

① NICTがインターネット上のIoT機器に、容易に推測されるパスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を特定。
② 当該機器の情報をインターネットプロバイダ（ISP）に通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施。



2019年12月までの取組結果

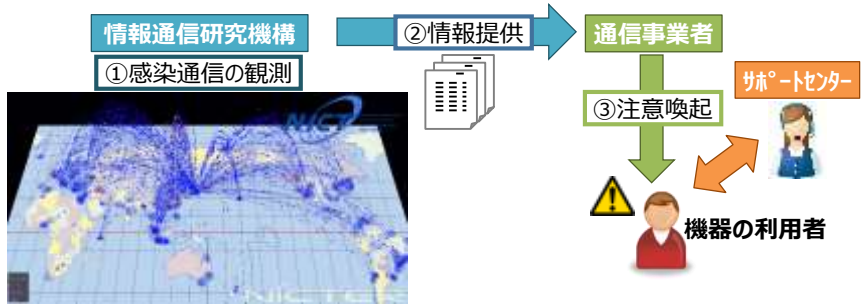
ID・パスワードが入力可能であったもの　約111,000件（直近での調査）

上記の内、ID・パスワードによりログインでき、注意喚起の対象となったもの　延べ1,328件

（２）マルウェアに感染しているIoT機器の利用者への注意喚起の推進

（調査対象）既にMirai等のマルウェアに感染しているIoT機器

① NICTが「NICTER」プロジェクトにおけるダークネット※に向けて送信された通信を分析することでマルウェアに感染したIoT機器を特定。
※NICTがサイバー攻撃の大規模観測に利用しているIPアドレス群
② 当該機器の情報をインターネットプロバイダ（ISP）に通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施



2019年12月までの取組結果

ISPに対する通知の対象となったもの　60～598件（１日当たり）

※2019年12月時点で41社（約1.1億IPアドレス）が参加

NOTICEに係る利用者支援

- **サポートセンター**を設置し、**専用Webサイト**の開設や**コールセンター**による問合せ対応を通じて利用者に適切なセキュリティ対策等を案内。
- 利用者からの問合せ対応に当たっては、各行政相談窓口や**消費生活センター**等と連携の上実施。

専用Webサイト

https://notice.go.jp

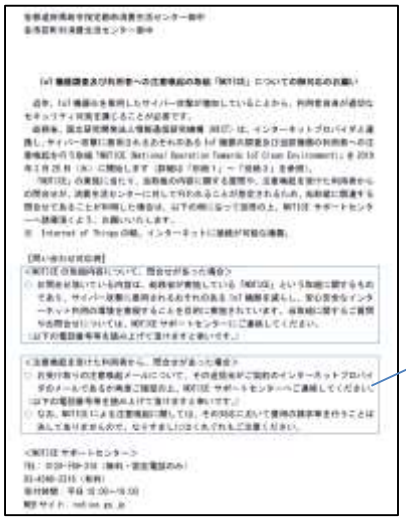
・問い合わせフォームを併設
・よくある質問（FAQ）を掲載
・英語版での情報発信も実施

コールセンター

０１２０－７６９－３１８（無料・固定電話のみ）
０３－４３４６－３３１８（有料）
受付時間：10:00～18:00（年末年始除く）

※注意喚起対象者のみならず、NOTICEの取組内容に関する問い合わせにも対応

各消費生活センター等との連携



平成31年3月13日発出

各消費生活センター等に対し、NOTICEに関する問い合わせがあった場合にサポートセンター（コールセンター）に誘導していただくよう、例文を示して依頼

＜注意喚起を受けた利用者から、問合せがあった場合＞

○ お受け取りの注意喚起メールについて、その送信元がご契約のインターネットプロバイダのメールであるか再度ご確認の上、NOTICEサポートセンターへご連絡してください。（以下の電話番号等を読み上げて頂けますと幸いです。）

○ なお、NOTICEによる注意喚起に関しては、その対応において費用の請求等を行うことは決してありませんので、なりすましにはくれぐれもご注意ください。

NOTICEに係る周知広報

- IoT機器のセキュリティ対策の必要性、NOTICEの取組の広報のため、**ポスター**や**リーフレット**作成し、家電量販店やサイバーセキュリティ関係イベント（セミナー等）で配布。
- 加えて、**新聞広告**や**サイネージ広告**、**政府広報**等を通じてNOTICEの取組を周知。

ポスター・リーフレット

各所での**ポスター掲示**を実施（2019年２月）

- 大手家電量販店（計約3000店舗）
  エディオン系列、ケーズデンキ系列、上新電機、ビックカメラ系列、ヤマダ電機系列
- 地方公共団体（約500団体）
- 東京メトロ駅構内（10駅）
- 電車中吊広告（東京メトロ全線、JR山手線等）

セキュリティ関連イベント等で**リーフレット配布**

新聞広告

全国日刊紙（2019年2月）

サイネージ広告

全国主要39駅
（2019年2月）

政府広報（ラジオ）

全国（TOKYO FM系列）
（2019年12月）

その他

- 総務省広報誌
  （2019年5月、2020年3月）
- 総務省報道発表
  （取組状況を四半期ごとに）
- 業界誌への寄稿　等