

# DLPAにおける サイバーセキュリティ対策に向けた 活動紹介

DLPA（デジタルライフ推進協会）  
2023年 3月 16日（木）



# 目次

1. DLPA概要
2. ネットワーク機器の要件
3. Wi-Fiルーターと脆弱性リスク
4. DLPA推奨Wi-Fiルーターについて
5. DLPAからの訴求活動



# 1. DLPA概要

【名称】 一般社団法人 デジタルライフ推進協会（略称：DLPA）

【設立】 2010年2月1日

【設立趣旨】 ユーザーの利便性を守り、デジタルライフの健全な発展を推進する。

【活動実績】 **技術WG：**

- ・サイバーセキュリティTG(2017/5～継続)／エンドオブサービスTG(2018/7～2019/12末)  
※ 最新のサイバー攻撃・脅威に目を向けた活動継続中 → 「DLPA推奨Wi-Fiルーター」の提案

**普及WG：**

- ・普及に向けた広報活動 → 「DLPA推奨Wi-Fiルーター」の訴求活動

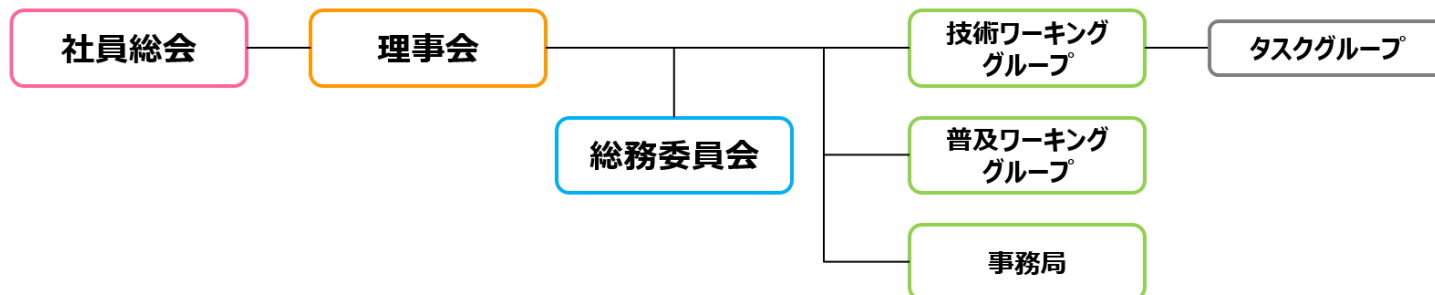
【会員】 14社（2022年8月時点）

サイバーセキュリティ／エンドオブサービスの活動は、株式会社アイ・オー・データ機器、NECプラットフォームズ株式会社、エレコム株式会社、株式会社バッファロー

国内ルーターメーカーの4社が加盟し、サイバーセキュリティの脆弱性対応について推進している。

※ 横浜国立大学の吉岡准教授に、顧問としてご指導を頂いています。

【組織】



## 2. ネットワーク機器の要件

個人・家庭向けWi-Fiルーターと、企業向けネットワーク（法人ルーター）とは求められる要件が異なる。前者は、ネットワークに詳しくない居住者が設定する場合でも、安全にお使い頂けるように設計されている。

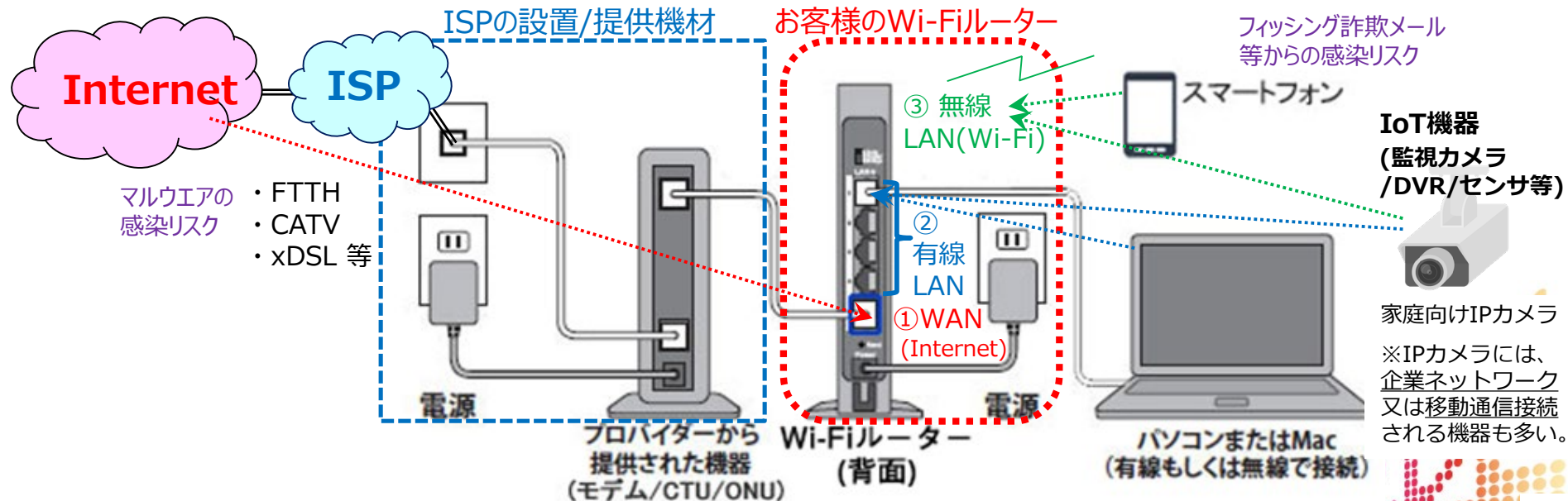
要件	個人・家庭向けWi-Fiルーター	企業向けネットワーク（法人ルーター）
設置者	主に居住者（又は設定サービス）	設置設定事業者（システムインテグレーター等）
設置機器	Wi-Fiルーター（届かない場合、中継機等）	拠点ごとにルーター（VPNやFireWall等を設置） 部門毎にVLAN等でアクセス制御（スイッチングハブ等） Wi-Fi接続はエリア毎に法人向けアクセスポイントを設置
保守	お客様（メーカーは問合せ対応、FAQ案内） ソフトウェア/ファームウェア更新での対応 基本、 <u>保証期間内は無償対応</u>	主に設置設定事業者が保守契約に基づき対応 <u>サポート費用がかかる</u> （無償期間設定あり）
設計	居住者が設置・設定しやすい点を重視 ➡ できるだけ難しい設定・操作を避ける	システムインテグレーターが、ネットワークシステム全体を設計し、各装置は設計通りに動作することが重視される
セキュリティ	Wi-Fiルーターが中心。（※PC/タブレット/スマートフォン等LAN内からの感染も懸念）	ネットワーク設計を通し、ネットワークシステム全体でセキュリティを担保する

※ ネットワークシステムを構成する、各製品に脆弱性が見つかった場合、対象機器の機能上の対策は、製造メーカーでの対応が必要です。

## 3. Wi-Fiルーターと脆弱性リスク

Wi-Fiルーターには、① WAN(Internet)、② 有線LAN、③無線LAN (Wi-Fi)の3種類のインターフェースを持ち、各インターフェースから侵入（ログイン）されるとルータの設定が変更され、攻撃の踏み台にされる可能性があります。

Wi-FiルーターのI/F	主な脆弱性（リスク）	攻撃エリア	主な攻撃事例
① WAN (Internet)	回線側からの侵入	Internet網	Telnet等のWAN側ポートを出荷時設定で閉じているが、開かれるとWeb設定ページへログイン、ルータ設定が変更される
② 有線LAN	PC等、接続機器からの侵入	主に宅内	宅内PC等からWeb設定へログインし、ルータ設定が変更される
③無線LAN (Wi-Fi)	スマートフォン等、Wi-Fi機器からの侵入	Wi-Fi通信範囲	Wi-Fiへ接続してログインし、宅外からルータ設定が変更される



## 4. DLPA推奨Wi-Fiルーターについて

### 1. 既知脆弱性への対応

Wi-FiルーターI/F	主な攻撃事例	DLPA推奨ルーター
① WAN (Internet)	Telnet等のWAN側ポートを出荷時設定で閉じているが、Web設定へログインし、ルータ設定を変更してポートを開ける	★ WAN側ポートは出荷時閉じておりTelnet/Web不可 (a)Web設定ログインID/PWが個体毎に異なり変更不可
② 有線LAN	宅内PC等からWeb設定へログインし、ルータ設定を変更する	(a)Web設定ログインID/PWが個体毎に異なり変更不可
③無線LAN (Wi-Fi)	Wi-Fiへ接続してログインし、宅外からルータ設定を変更する	(a)Web設定ログインID/PWが個体毎に異なり変更不可

### 2. 今後発生し得る脆弱性への対応

各メーカーは新たな脆弱性が公開されたとき、可能な限りFW修正でその脆弱性に対応します。

→ 脆弱性へ対応した (b)FWは自動更新機能がついているので、お客様のWi-Fiルータは自動的に更新・対策されます。

#### DLPA推奨Wi-Fiルーター

最新のWi-Fiルーターは、出荷時からセキュリティ対策機能が搭載されているので、安全にご利用いただけます。

(b) ファームウェアの自動更新に対応



> 対応機種については末尾にある各社リンクページでご確認ください。

(a) 管理画面へのログインIDもしくはパスワードの固有化



2019/12/18 DLPAよりプレス発表

【引用】ご家庭でWi-Fiルーターをより安全にお使い頂くために ([https://dlpa.jp/wifi\\_support/](https://dlpa.jp/wifi_support/))

**4社のDLPA推奨Wi-Fiルーターは、今までに1台もNOTICEで検出されていません (2023/3/16時点)**

DLPA加盟4社からも「安全にご利用頂く」ための案内を提供しています。

(株)アイ・オー・データ機器

<https://www.iodata.jp/product/network/info/wifi/safety.htm>

NECプラットフォームズ(株)

<https://www.aterm.jp/product/atermstation/info/2019/info1218.html>

エレコム(株)

[http://qa.elecom.co.jp/faq\\_detail.html?id=8202](http://qa.elecom.co.jp/faq_detail.html?id=8202)

(株)バッファロー

<https://www.buffalo.jp/topics/select/detail/wi-fi.html>



# 5. DLPAからの訴求活動(1)

## 1. DLPAサイトにて、家庭用Wi-Fiルーターの安全な使い方を案内

ご家庭でWi-Fiルーターをより安全にお使い頂くために

「自宅のネットワークは自分で守ろう！」

お家のWi-Fiルーター設置したきりになっていませんか？

Wi-Fiルーターは、一度設置し稼働すると管理が行き届きにくく、そのまま長期利用されていることがあります。メンテナンスがされていないWi-Fiルーターは年々増え続けるサイバー攻撃の被害に遭う恐れがあります。被害に遭わないためにも、お客様ご自身が適切にセキュリティ対策をすることが重要です。大切なデータ・生活を守るために、4つの項目に注意しましょう。

セキュリティ対策のポイント

- 1 最新ファームウェアでの運用
- 2 より安全なパスワード設定
- 3 修理/サポートの期限について
- 4 脆弱性問題に関する更新プログラムの提供について

セキュリティ対策がされているDLPA推奨Wi-Fiルーターがオススメよ！

2019年12月より、4つのセキュリティ対策ポイントを掲げ、一般ユーザーへ案内。



その中でも重要項目を2つ選定し、これらが出荷時状態から対応しているWi-Fiルーターを安全な商品として「DLPA推奨Wi-Fiルーター」と称している。

※ 2019年12月時点で、加盟4社の現行品Wi-FiルーターはすべてDLPA推奨Wi-Fiルーターの基準を満たしています。

DLPA推奨Wi-Fiルーター

ファームウェアの自動更新に対応

管理画面へのログインIDもしくはパスワードの固有化

# 5. DLPAからの訴求活動(2)

## 2. 外部サイトと連携し、家庭用Wi-Fiルーターの安全な使い方を案内

### ▼インプレス様 INTERNET Watch(記事広告)

団体名義ではなく、よりユーザーの馴染みがあるメーカーが主体となり、家庭内のルーターの見直し及び買い替えについて呼びかけた。



**実家のWi-Fiルーターもより安全に！ 年末年始の帰省時に対策を**  
 メーカーの垣根を越えて国内大手4社が提言する「Wi-Fiルーターをより安全に使うための方法」とは  
 清水 理史 2019年12月25日 06:00

「IoT機器を狙ったサイバー攻撃」の増加により、Wi-Fiルーターのセキュリティ対策が急務となってきた。そんな中、一般社団法人デジタルライフ推進協会(DLPA)から、メーカーの垣根を越えた共通の提言が発表された。

Wi-Fiルーターをサイバー攻撃から守るには、どのような点に注意すればいいのか？今回は、DLPAに参加する株式会社アイ・オー・データ機器、NECプラットフォームズ株式会社、エレコム株式会社、株式会社パッパローの4社から、そのポイントを聞いた。

年末年始の休暇のタイミングで、自宅はもちろんのこと、帰省した実家のWi-Fiルーターについて確認するのでもいいかもしれない。

### ▼NISC様 サイバーセキュリティ月間 特設ページ (2022年～)

サイト内でご案内された「家庭内Wi-Fiルーターの設定・利用」については、DLPAよりコンテンツを提供。同じ内容を掲載することで、ユーザー意識の統一化を図る。



**基本的なセキュリティ対策**  
 誰もが安心してITの活動を享受するためには、国境を越えてサイバー空間を共有、これらの空間に接続している機器があります。

**家庭用無線LANルーターの設定・利用**  
 誰もが安心してITの活動を享受するためには、国境を越えてサイバー空間を共有、これらの空間を共有、これらの空間に接続している機器があります。

**ご家庭でWi-Fiルーターをより安全にお使い頂くために**  
 「自宅のネットワークは自分で守ろう!」

**セキュリティ対策のポイント**

- 1 ファームウェアのアップデート設定について
- 2 管理画面パスワードの設定について
- 3 修理/サポートの期限について
- 4 脆弱性問題に関する更新プログラムの提供について
- 5 連絡/問合せ先



## 5. DLPAからの訴求活動(3)

### 3. 動画にて、家庭用Wi-Fiルーターの安全な使い方を案内（現在制作中）

コロナ禍において、リモートワーク・リモート授業が進み、Wi-Fiルーターの買い替え市場は伸びたが、それでも長期にわたりWi-Fiルーターを使い続けているユーザーがいる。そんなユーザーに、**動作寿命**ではなく、**セキュリティ寿命**があることを啓発することで、DLPAが推奨する、安心・安全なWi-Fiルーターへの買い替えの重要性をPRする動画を作成。

公開：2023年3月末予定

動画時間：2分30秒程度



第3者が、アンケート調査をもとに、生活者の悩みや疑問を、DLPAに取材し解決に導く動画構成。  
疑問をなげかけることで「気づき」を与える。

主体を生活者におき、同じルーターを長期で使いつづける危険性、セキュリティ意識の低さの危険性などを説明しつつ、その問題をすべて解決しているのが「DLPA推奨Wi-Fiルーター」であることPR。

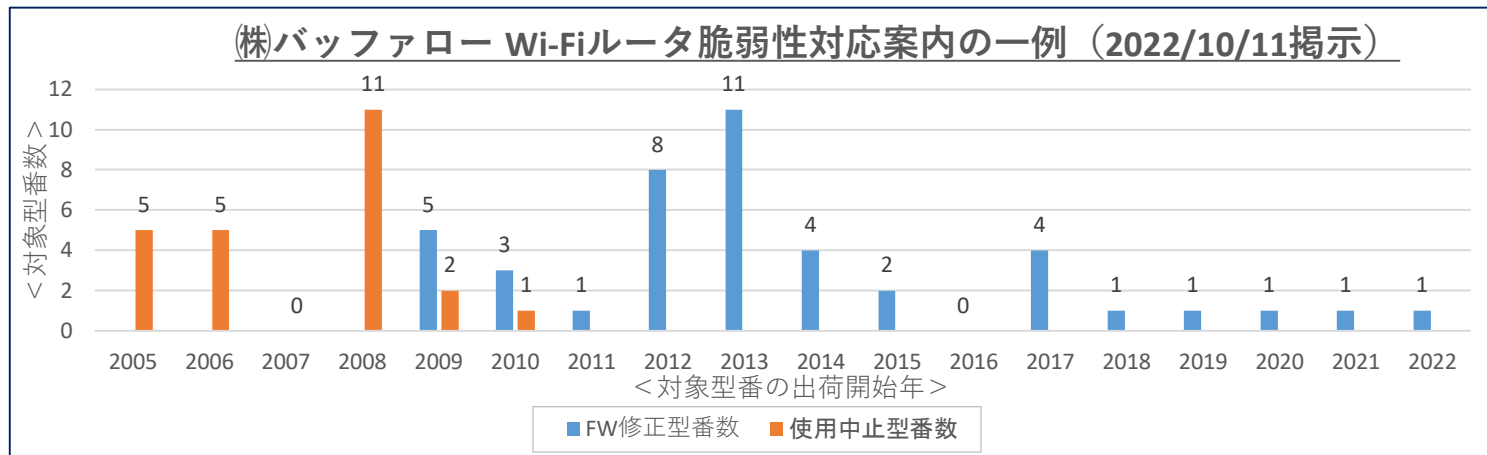
## (参考) バッファローの脆弱性対応事例

DLPA加盟のルーターメーカー 4 社における「Wi-Fiルータ保証期間は 1 年」であるが、お客様が安全にWi-Fiルーターをお使いいただけるように、脆弱性が見つかった際は、可能な範囲で販売終了型番についても脆弱性対応ファームウェア（FW）をお客様にダウンロード提供すると共に、【重要なお知らせ】として掲示し、お客様へ情報を提供しています。

対象：2022年に新たに発見された脆弱性 3 件（対応事例の一つとして）

対応：2009年に販売開始（販売終了から10年程経過）した型番まで遡ってファームウェアの改版を行い、2022年10月までに、これら脆弱性 3 件への対応を実施。

どうしても対応できなかった2010年以前に販売開始した型番は、お客様へ使用中止を案内。



【引用】ルーター等の一部商品における複数の脆弱性とその対処方法 (<https://www.buffalo.jp/news/detail/20221011-01.html>)