一般社団法人
デジタルライフ推進協会
Digital Life Promotion Association

資料3－3－1

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

一般社団法人
デジタルライフ推進協会
Digital Life Promotion Association

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

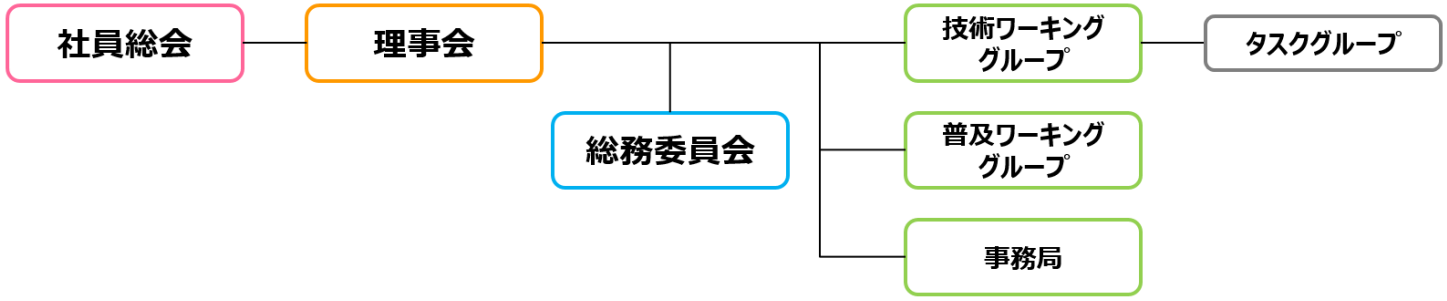
【会員】14社（2022年8月時点）

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。

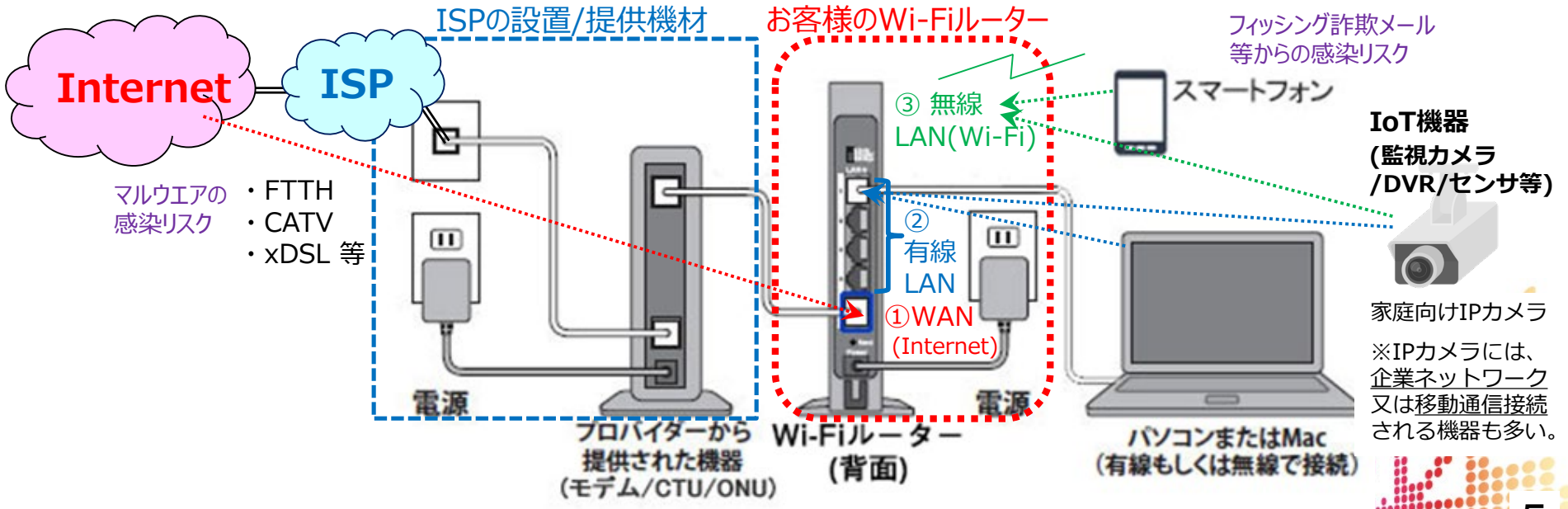
要件	**個人・家庭向けWi-Fiルーター**	企業向けネットワーク（法人ルーター）
設置者	主に居住者（又は設定サービス）	設置設定事業者（システムインテグレーター等）
設置機器	Wi-Fiルーター（届かない場合、中継機等）	拠点ごとにルーター（VPNやFireWall等を設置） 部門毎にVLAN等でアクセス制御（スイッチングハブ等） Wi-Fi接続はエリア毎に法人向けアクセスポイントを設置
保守	お客様（メーカは問合せ対応、FAQ案内） ソフトウエア/ファームウエア更新での対応 基本、保証期間内は無償対応	主に設置設定事業者が保守契約に基づき対応 サポート費用がかかる（無償期間設定あり）
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



一般社団法人
デジタルライフ推進協会
Digital Life Promotion Association

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。

【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/）

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。

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

エレコム㈱
http://qa.elecom.co.jp/faq_detail.html?id=8202

㈱バッファロー
https://www.buffalo.jp/topics/select/detail/wi-fi.html

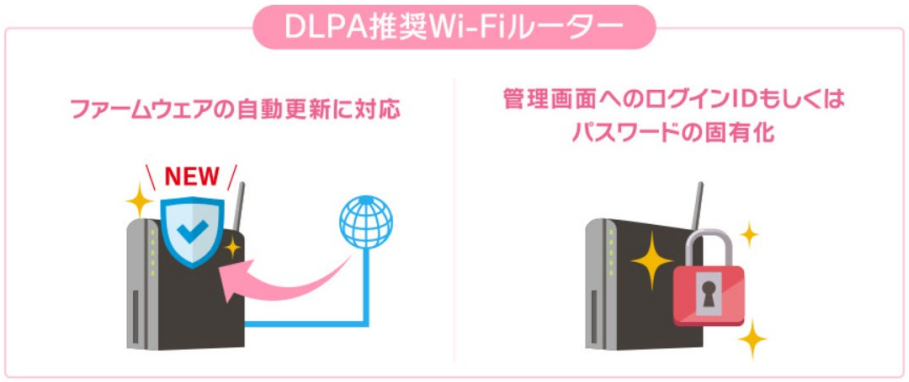
5．DLPAからの訴求活動(1)

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

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。**



一般社団法人
デジタルライフ推進協会
Digital Life Promotion Association

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。

https://internet.watch.impress.co.jp/docs/interview/1224449.html

▼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。

https://security-portal.nisc.go.jp/cybersecuritymonth/2022/

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 があることを啓発しすることで、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

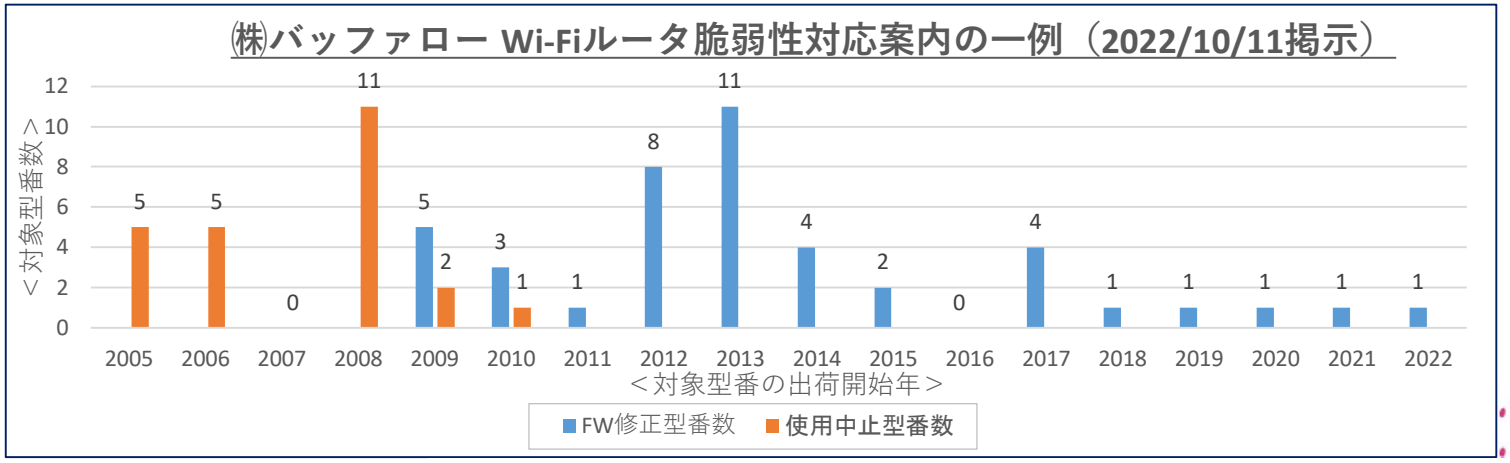
動画時間：2分30秒程度

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エア（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エアの改版を
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）