

家庭向けIoT機器、ルーターを守ろう

インターネット安全教室(ウインクあいち)
追加プログラム (初級から上級向け)

2018年11月25日(日) 11-12am
東海インターネット協議会 副理事長
<http://www.tokai-ic.or.jp/>
南山大学国際教養学部 後藤 邦夫
goto at nanzan-u.ac.jp



目次

- 1. IPAの新作ビデオ紹介 (倍速で)
- 2. パスワードを変更しよう (初級)
- 3. ネットワークのセキュリティチェック (中級)
- 4. UPnPとルータ、無線AP詳細設定 (上級)
- 5. ある家庭での利用例 (一部中上級)
- まとめ
- おまけ – 最近の詐欺メッセージ例、偽警告(一部中級)
- 参考文献リスト

1. IPAの新作ビデオ紹介

- あなたの家も狙われている？ 家庭教師が...(約14分、2倍速で)

<https://www.youtube.com/watch?v=xbn8SZlib90>

- IPAの情報セキュリティ啓発ビデオ一覧

<https://www.ipa.go.jp/security/keihatsu/videos/index.html>

1. 続き(教訓)

- ルータの電源は確実に (可用性)
 - ホームゲートウェイはルータ、IP電話等の箱
 - 無線LANアクセスポイントは別設置可
- DDoS Attack (Distributed Denial of Service Attack)
 - 自分に直接害がなくても踏み台になるのはまずい
- Firmware – softwareとhardwareの中間
- ネットワークカメラのパスワード設定が重要
 - 丸見えカメラ <https://www.insecam.org/> (Insecam)

2. パスワードを変更しよう(初級)

- すべての機器の管理パスワード (http://192.168.1.1/等)
 - ルータ
 - 無線LANアクセスポイント (SSID、キーは1台ずつ違うなら、そのままでもよい)
 - ネットワークカメラ、スマートリモコンなど、特にインターネットから通信開始できる機器 (初期設定で見えるようになる)
- 変更操作例
 - 各機器のIPアドレスを調べる (取扱説明書参照 or ping, arp, nmap)
 - 初期パスワードで "http://IPアドレス/" にloginして、設定

3. ネットワークのセキュリティチェック (中級)

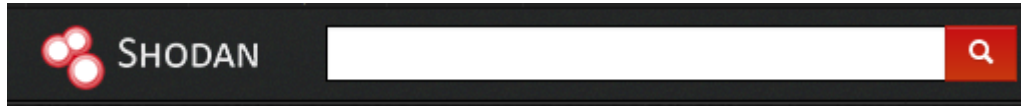
- インターネットからのチェック (外部Webサイト利用)
 - 1) 自宅のグローバルIPアドレス(v4とv6)確認
https://test-ipv6.com/index.html.ja_JP
 - IPv6アドレスが見えなくても、近くの網内で有効かも
 - 2) インターネットからルータのUPnPが使えないことを確認 <https://www.grc.com/x/ne.dll?bh0bkyd2>
(ShieldsUp) 結果が以下ならOK (だめなら危険なルータ)

THE EQUIPMENT AT THE TARGET IP ADDRESS
DID NOT RESPOND TO OUR UPnP PROBES!

(That's good news!)

3. 続き

- インターネットから自宅をポートスキャン
 - 自宅で、自分のIPアドレスを指定して実行
 - 勤務先等外部から実行しない



- 具体例: Shodan <https://www.shodan.io/>
 - 自宅ルータのグローバルIPアドレスを入れて検索
 - v6の場合は、aaaa:bbbb:cccc:dddd::/64 等
- LAN内でポートスキャン (nmap等) <https://nmap.org/>
 - 自分でインストール (Linux, macOSは簡単)
 - Windowsは面倒そう

4. UPnPとルータ、無線APの詳細設定 (上級)

- Universal Plug and Play (通信プロトコル)
 - LAN内の機器を発見、利用
 - 便利だが認証なし
 - ほとんどのルータがport forwarding要求を受理
 - Port forwarding (port開放) するとWAN側からLAN内機器に直接通信できる (便利だが危険)
 - 上級者はルータのUPnPを無効にして、静的設定を!
 - WAN側のUPnPが有効なルータは欠陥品

4. 続き (ルータ設定その1)

- UPnPの「使用する」のチェックを外す(高度な設定)



PR-400NE
ファームウェアバージョン 8.04

保存

- 基本設定
- 電話設定
- 無線LAN設定
- 詳細設定
 - DNS設定
 - DHCPv4サーバ設定
 - SPI設定
 - IPv4パケットフィルタ設定
 - IPv6パケットフィルタ設定 (IPoE)
 - ワンタッチ設定
 - 静的IPマスカレード設定
 - 静的NAT設定
 - 静的ルーティング設定
 - VPNサーバ設定
 - 高度な設定
- メンテナンス
- 情報

トップページ > 詳細設定 > 高度な設定

高度な設定

ご注意ください
設定変更は即時に有効となります。[設定] ボタンをクリックしたあと、本商品にアクセスできなくなる場合がありますので、その場合は、WebブラウザをWebブラウザを開きなおしてください。

《高度な設定》画面の[WAN→LAN中継設定]と《静的IPマスカレード設定》画面の内容が競合した場合は、《高度な設定》画面の[WAN→LAN中継設定]を行くと、通話・通信が切断されることがあります。

高度な設定

LANポート通信設定	自動設定	(LAN1)
	自動設定	(LAN2)
	自動設定	(LAN3)
	自動設定	(LAN4)
LAN側MDI/MDI-Xモード	MDI-X固定	
セキュリティ保護機能	<input checked="" type="checkbox"/> 使用する	

ブリッジ設定

PPPoEブリッジ	<input checked="" type="checkbox"/> 使用する
PPPoEブリッジ自動切断	<input type="checkbox"/> 使用する
PPPoEブリッジ自動切断するまでの時間(秒)	1800

UPnP設定

UPnP設定	<input type="checkbox"/> 使用する
--------	-------------------------------

WAN→LAN中継設定

4. 続き (ルータ設定その2)

- この機種では、変換対象ポートと宛先ポートを別にできない (port 80で複数Webサーバを置けない)
 - 192.168.0.254 (Linuxサーバ)、7(ネットワークカメラ)
 - 4 (Panasonic ビデオ、port 80なので変換できない)


NATエントリ

01~

エントリ番号	変換対象プロトコル	変換対象ポート	宛先アドレス	宛先ポート
<input checked="" type="checkbox"/> 01	UDP	domain	192.168.0.254	domain
<input checked="" type="checkbox"/> 02	TCP	22	192.168.0.254	22
<input checked="" type="checkbox"/> 03	TCP	smtp	192.168.0.254	smtp
<input checked="" type="checkbox"/> 04	TCP	www	192.168.0.254	www
<input checked="" type="checkbox"/> 05	TCP	pop3	192.168.0.254	pop3
<input checked="" type="checkbox"/> 06	TCP	587	192.168.0.254	587
<input checked="" type="checkbox"/> 07	TCP	8080	192.168.0.250	8080
<input checked="" type="checkbox"/> 08	TCP	https	192.168.0.254	https
<input checked="" type="checkbox"/> 09	TCP	8888	192.168.0.7	8888
<input type="checkbox"/> 10	TCP	8880	192.168.0.4	8880

4. 続き (ルータ設定その3)

- IPv6フィルタの初期設定確認
- IPv6サービス未公開なので「標準」でOK

**NTT**

PR-400NE
ファームウェアバージョン 8.04

保存

- 基本設定
- 電話設定
- 無線LAN設定
- 詳細設定
 - DNS設定
 - DHCPv4サーバ設定
 - SPI設定
 - IPv4パケットフィルタ設定
 - IPv6パケットフィルタ設定 (IPoE)
 - ワンタッチ設定
 - 静的IPマスカレード設定
 - 静的NAT設定

トップページ > 詳細設定 > IPv6パケットフィルタ設定(IPoE)

IPv6パケットフィルタ設定(IPoE)

ご注意ください

IPv6パケットフィルタ設定機能にて、IPv6通信に関するファイアウォール機能の「有効」/「無効」の設定およびIPv6通信のセキュリティレベルを「標準」/「高度」の二種類から選択することができます。

[IPv6ファイアウォール機能]が「有効」でかつ、[IPv6セキュリティのレベル]が「標準」の場合、NTT東日本・NTT西日本のフレッツ光ネクスト網内で折り返す通信(NTT東日本・NTT西日本との契約により可能となるもの)は許可し、その他のIPv6通信を使用したインターネット側からの通信を拒否します。
※ [IPv6セキュリティのレベル]が「高度」の場合は、NTT東日本・NTT西日本のフレッツ光ネクスト網内で折り返す通信(NTT東日本・NTT西日本との契約により可能となるもの)を拒否します。

[IPv6ファイアウォール機能]を「無効」にした場合、NTT東日本・NTT西日本のフレッツ光ネクスト網内で折り返す通信(NTT東日本・NTT西日本との契約により可能となるもの)を許可し、かつその他のIPv6を使用したインターネット側からの通信を許可します。[IPv6ファイアウォール機能]を「無効」に設定することで、LANに接続した機器が危険にさらされる可能性がありますので、設定する際は十分注意してください。
また、[IPv6ファイアウォール機能]を「無効」にした場合、IPv6パケットフィルタ設定(IPv6 PPPoE)も無効となりますのでご注意ください。

対象インタフェースを選択 WAN ▾ 選択

セキュリティモード

IPv6ファイアウォール機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
IPv6セキュリティのレベル	標準

IPv6パケットフィルタ設定 (IPv6 PPPoE)

4. 続き (無線AP追加設定項目)

- 侵入者へのハードルを上げる
 - MACアドレス登録制、ESSIDスティルス
- 会社では、認証サーバで個人認証できるWPA/WPA2 Enterprise

WRC-733GHBK

設定メニュー

▶モード変更

▶無線設定

▶WAN&LAN設定

▶LED省電力設定

▶ファイアウォール設定

▶アクセスコントロール

▶システム設定

言語設定

言語設定 ▼

アクセスコントロール

特定の機器について、接続を許可する・許可しないを設定します。登録できる端末数は、最大 50 です。有線/無線 両方の機器が対象になります。また、「許可」と「拒否」を混在させる設定はできません。

※APモードでは有線接続したクライアントの制御はできません。

アクセスコントロール機能: ☒ 有効 ☐ 無効

コントロールモード: 接続許可 ▼

MACアドレス: (記入例: 0090fe0123ab)

コメント: (最大20文字、半角英数のみ)

【接続許可】: 設定した機器の接続を許可します。設定していない機器については接続することができません。
【接続拒否】: 設定した機器の接続を拒否します。設定していない機器は全て接続することができます。

追加

アクセスコントロール:

MACアドレス	コメント	ステータス	選択
fc:d8:48:1a:f2:07	iPod-KG	接続許可	<input type="checkbox"/>
40:b8:37:cf:96:1b	Xperia-SO20H-KG	接続許可	<input type="checkbox"/>
68:a3:c4:ab:94:7c	thinkpad-KG	接続許可	<input type="checkbox"/>
c0:33:5e:1b:74:37	SurfacePro3-KG	接続許可	<input type="checkbox"/>
48:43:7c:ae:70:53	iPhone-Reoto	接続許可	<input type="checkbox"/>

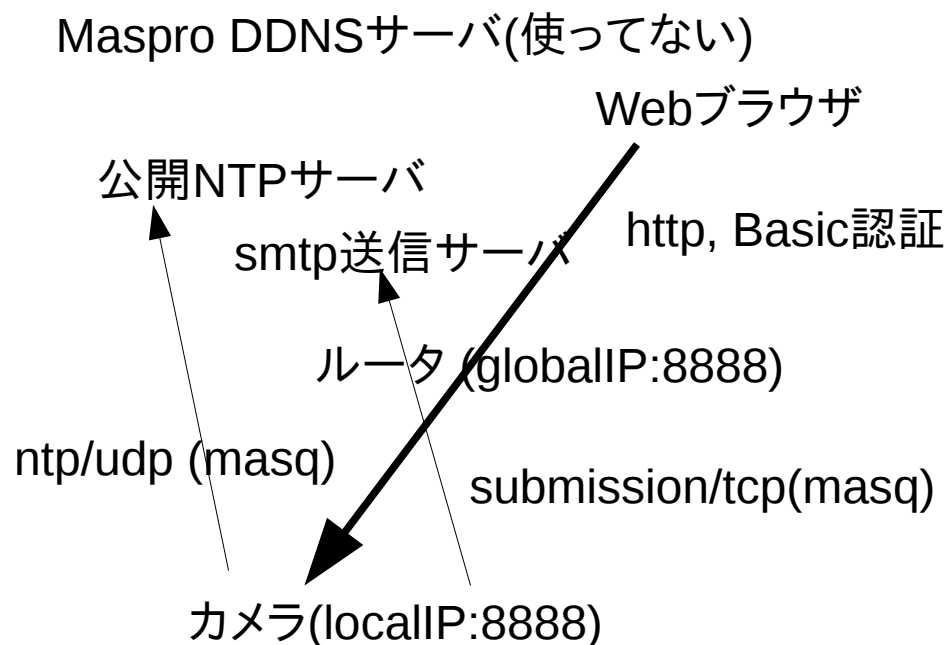
5. ある家庭での利用例(時間あれば実演)

- ネットワーク構成
 - ホームゲートウェイ(レンタル) IPv4グローバルアドレス固定、IPv6サービスあり
 - 宅内1000BASE-T + 無線AP
 - インターネットから使うIoT機器のLANアドレスは手動設定(ルータのDHCP貸出範囲外に)
- コンピュータ等
 - デスクトップPC (Linuxサーバ、Mac miniサーバ)
 - ノートPC、スマートフォン等 (Wifi MACアドレス登録数10以上)
- 外部から利用するIoT機器
 - ネットワークカメラ (http port 8888で公開、パスワード認証、ペット見守り用、Linux2.6.x)
 - ビデオレコーダ (2010、dimoraで録画予約、公開不要、ストリーミング機能なし、Linux2.6.x)
 - スマートリモコン (留守のときに停電したら、冷房付けたい、公開必要、Linux2.6.x)
- IoT機器の設定 – ほとんどの場合専用アプリケーションは不要、LinuxのFirefox等でOK

5. 続き (ペット見守り)

- Maspro電工 見張っチャオ (Win10以前)
<http://www.maspro.co.jp/products/security/hs2/>
- httpだけで使える(5コマ/秒までの簡易動画) – PCまたはスマートフォン
- SMTP、NTP、センサ、暗視、静止画記録、
- DDNSでFQDN固定(提供あり)
- わが家ではhttp://自宅ドメイン:8888/ LANではlocalIP:8888/(ルータでポートを変えられないので仕方なく)
- httpsなし(サーバ証明書設定管理の手間が無理?)
- 初期設定IDとパスワードを変更しないと危ない

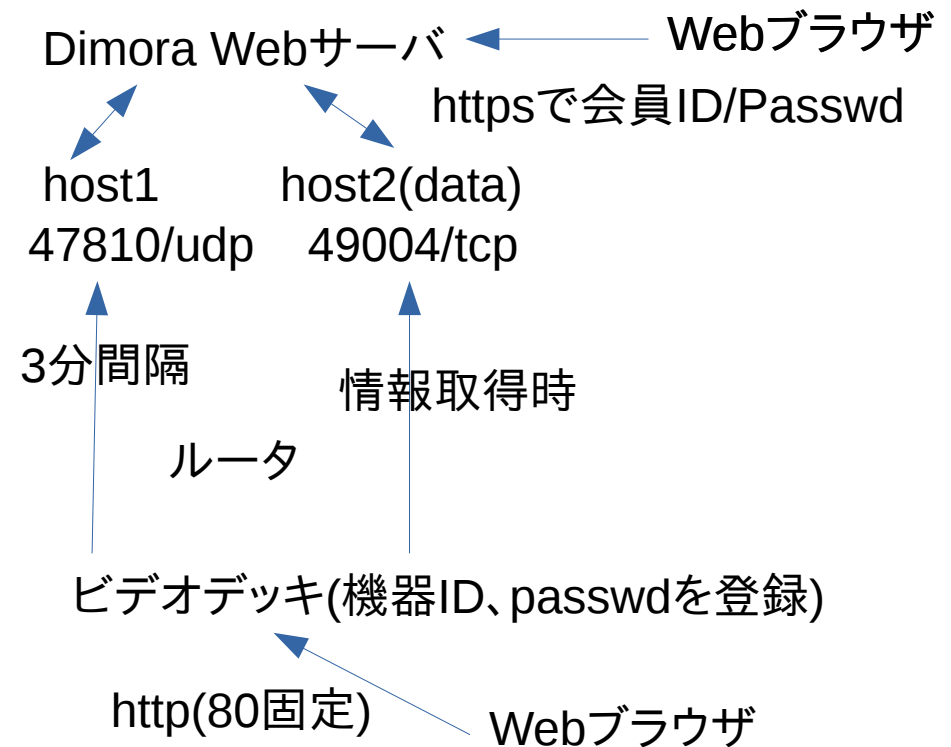
- Port forwarding(http)
 - 矢印は通信開始方向



5. 続き (ビデオ)

- Panasonic DMR-BZT600 (2011ころ)
- 機器パスワードを本体リモコンで設定
- `http://192.168.0.X/`
 - 直接外から使うためにはport forwarding必要(非推奨)
- <https://dimora.jp/login/>
 - Club Panasonicユーザ登録
 - 機器IDとパスワード登録
 - 基本機能無料
- 右図はパケットキャプチャ結果からの推定(矢印は通信開始方向)

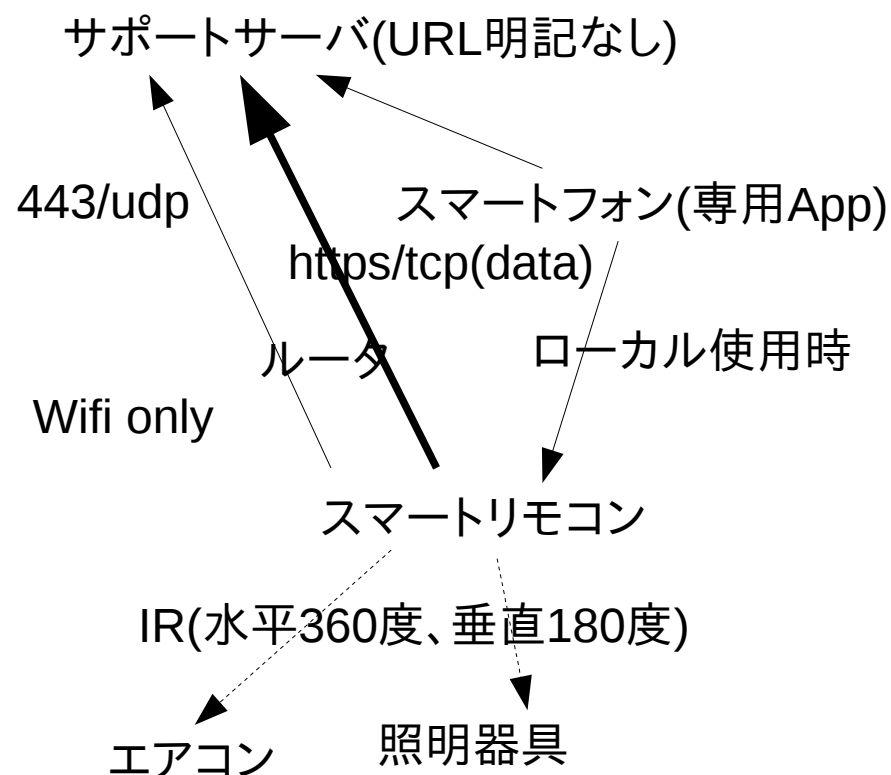
- Port forwarding不要



5. 続き(スマートリモコン)

- RS-WFIREX3
- Android/iOS専用App
- 利用アカウント作成(認証コードをemail受信)
- 専用App(同一Wifi)で本体設定(IPアドレス固定不要)
- 以後、どこからでもアクセス可
- リモコン登録 – リ
- 送信先 (詳細不明)
 - hostname.1e100.net (443/udp, https/tcp, GoogleのIPアドレス)
 - 他にfacebook.com (http, https/tcpでAPI?)

• Port forwarding不要



5. 続き(リモコン2)



まとめ

- まずは管理パスワードを変更
 - しかし、ファームウェアに埋め込まれた別のidとパスワードで使える場合がある(欠陥商品)
- 売り切りでサポートが短そうな製品は買い替え
- サーバ仲介利用パターン(ビデオ等)では、インターネット公開不要
- 今日の内容が大体わかる人に製品マニュアルを読んでもらう
 - 会社では技術力がある業者に納品設置してもらう
- 試してみたい機器 – 最新のインターホン

おまけ (その1: SMS)

- SMSでも来るようになった詐欺メッセージ
 - 請求先の名前くらい書いてよね
 - 発信者名称、電話番号は嘘つき可



おまけ (その1左例分析)

- sagawa-zak.com – Android用マルウェア (受け取ったのはiPhoneユーザでしたが)

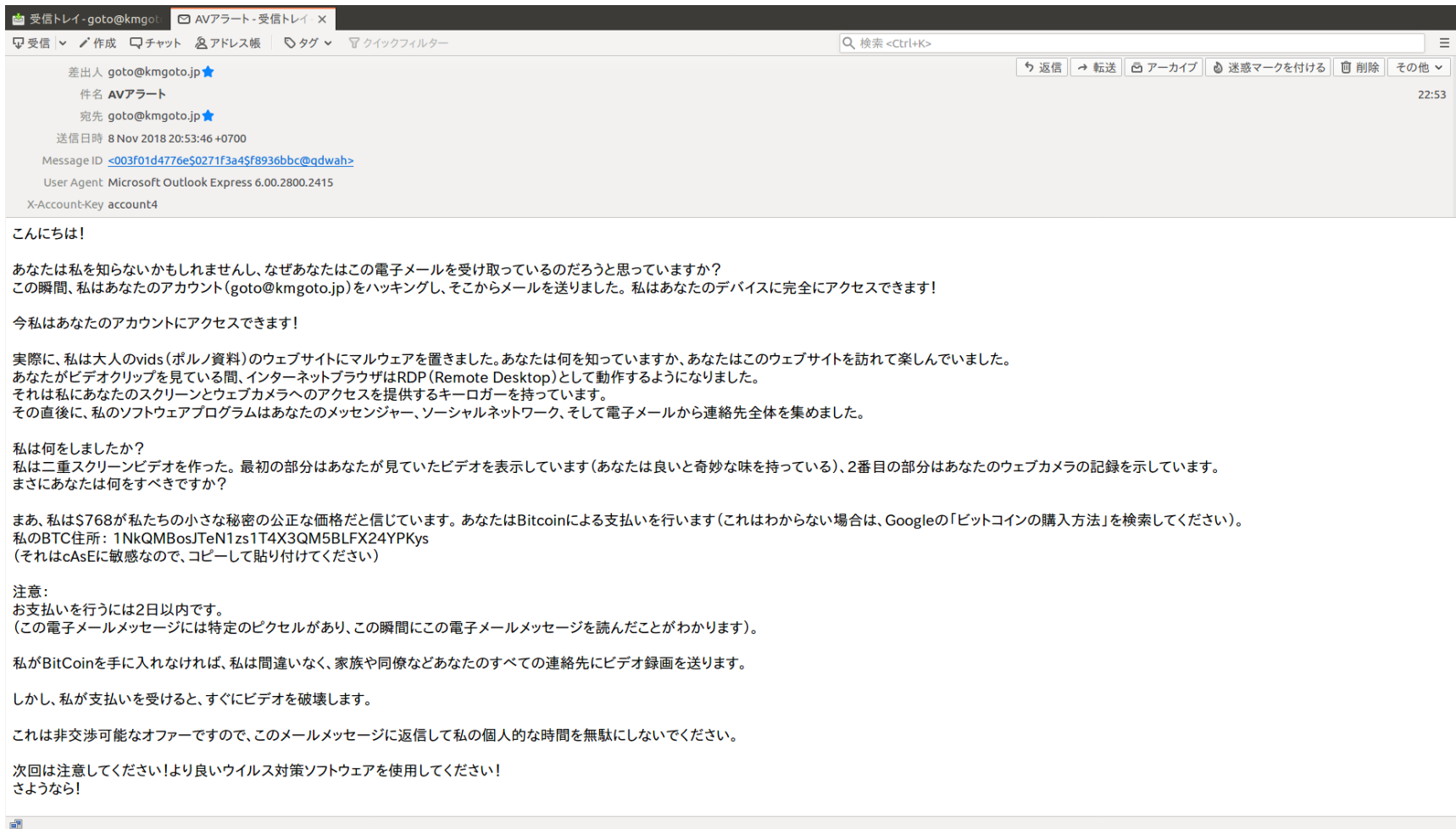
The image shows a Google Safe Browsing warning page for the website **sagawa-zak.com**. The page has a red header with a warning icon and the text "この先は詐欺サイトです" (This is a scam site ahead). Below this, it states: "このページは、危険なソフトウェアをインストールしようとしているため、Firefox によりブロックされています。" (This page is blocked by Firefox because it is trying to install dangerous software). The provider of the warning is listed as "Google Safe Browsing".

Overlaid on this is an Android file manager dialog titled "sagawa.apk を開く" (Open sagawa.apk). The dialog shows the file "sagawa.apk" with details: "ファイルの種類: Android パッケージ (2.3 MB)" and "ファイルの場所: http://sagawa-zak.com". It asks how to handle the file, with options: "プログラムで開く(O):" (selected), "ファイルを保存する(S)", and "今後この種類のファイルは同様に処理する(A)". The "プログラムで開く(O):" option is set to "OpenJDK Java 8 Runtime (既定)".

At the bottom of the warning page, there is a navigation bar with several links: "法人のお客さま", "再配達のご依頼", "貨物追跡サービス", "WEBトータルサポート", "料金検索", and "営業所検索". A red button labeled "インストール" (Install) is also visible.

おまけ (その2: email)

- 日本語: BitCoinで払えと言われてもねえ



おまけ (その2分析)

- メールヘッダが読めれば色々わかる
 - 残念: スマートフォンではヘッダが読めない、内容で判断
 - Received: 自分のメールサーバ行 (unknownは△)
 - Date: 地域が推定できる(JST = UTC + 9h)

```
Delivered-To: goto@kmgoto.jp
Received: from 72.75.186.123.broad.fs.ln.dynamic.163data.com.cn (unknown [123.186.75.72])
    by FL9-119-243-80-3.aic.mesh.ad.jp (Postfix) with ESMTP id C4E971140246
    for <goto@kmgoto.jp>; Thu,  8 Nov 2018 15:26:08 +0900 (JST)
Message-ID: <003f01d4776e$0271f3a4$f8936bbc@qdwah>
From: <goto@kmgoto.jp>
To: <goto@kmgoto.jp>
Subject: =?utf-8?B?QVbjgqLjg6njg7zjg4g=?=
Date: 8 Nov 2018 20:53:46 +0700
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----_NextPart_000_003C_01D4776E.027039CB"
```

おまけ (その3: 偽警告)

- ビデオ: <https://www.youtube.com/watch?v=sm1UMc97zRc> (2倍速で)
 - マルウェアを入れさせる
 - 役に立たないサポート契約
- 対処 (アクションしなければ実害なし、落ち着いて)
 - Webブラウザの停止 (WebブラウザのJavaScriptコード実行でしょう)
 - OS再起動
 - 最後の手段: 電源ボタン長押しで停止
 - 再起動してもだめならWebブラウザのキャッシュを消す (特にスマートフォン)
- だまされた場合 (経験に基づく)
 - ネットワーク接続を切る
 - クレジットカードなら支払わないと連絡(250 USD、翌日で間に合った、カード再発行も依頼)
 - リモート制御アプリケーションを削除(極悪でなければ自分で消せる)
 - PCを点検(業者委託、このケースではマルウェアなし)
 - 必要あれば消費者センターに相談(このケースでは不要だった)
- IPAの解説(2018年5月): <https://www.ipa.go.jp/files/000066767.pdf>

参考文献等

- IPAの資料

- "映像で知る情報セキュリティ～映像コンテンツ一覧～," <https://www.ipa.go.jp/security/keihatsu/videos/index.html> (最終更新 2018年4月3日)
 - "あなたの家も狙われている!? 家庭教師が教えるネット家電セキュリティ対策(ビデオ)"(2018年4月)
 - "その警告メッセージ、信じて大丈夫? ブラウザの“偽警告”にご用心!(ビデオ)" (2017年4月)
- 山崎 知嗣, "偽警告に騙されないで! ～巧妙化する手口とその対策～," <https://www.ipa.go.jp/files/000066767.pdf> (2018年5月)

- Webサイト

- Insecam, "Insecam - World biggest online cameras directory," <https://www.insecam.org/> (アクセス 2018年11月)
- Biglobe/Fullroute, "Test your IPv6," <https://test-ipv6.com/> (アクセス 2018年11月)
- Gibson Research Corp., "ShieldsUp!," <https://www.grc.com/x/ne.dll?bh0bkyd2> (アクセス 2018年11月)
- Shodan, "The search engine for Security", <https://www.shodan.io/> (アクセス2018年11月)
- Nmap.org, "Nmap: the network mapper -- Free Security Scanner," <https://nmap.org/> (アクセス 2018年11月)
- Panasonic, "Dimora", <https://dimora.jp/> (アクセス 2018年11月)

- 実験で使用了製品

- PR-400NE NTT西日本 レンタルホームゲートウェイ (ファームウェア ver.8.04 2016年8月)
- WRC-733GH(BK) ELECOM (ファームウェア 1.56 2017年5月、自動更新)
- HS2CRC2 マスプロ電工 (ファームウェア更新情報なし)
- DMR-BZT600 Panasonic (ファームウェア 1.53 2013年12月、自動更新)
- RS-WFIREX3 ラトックシステム (ファームウェアバージョン不明)

以上