家庭向けIoT機器、ルータを守ろう

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

- 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=xbn8SZIib90

- 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)

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)

4. 続き (ルータ設定その2)

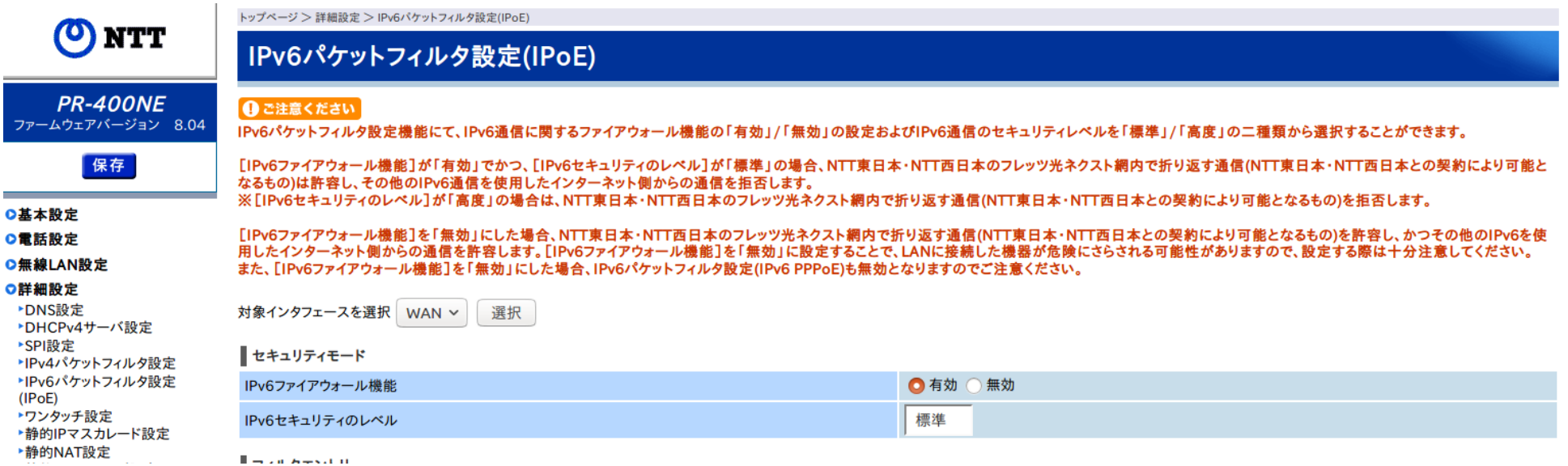
- この機種では、変換対象ポートと宛先ポートを別にできない (port 80で複数Webサーバを置けない)
  - 192.168.0.254 (Linuxサーバ)、7(ネットワークカメラ)
  - 4 (Panasonic ビデオ、port 80なので変換できない)

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
☑ 01	UDP	domain	192.168.0.254	domain
☑ 02	TCP	22	192.168.0.254	22
☑ 03	TCP	smtp	192.168.0.254	smtp
☑ 04	TCP	www	192.168.0.254	www
☑ 05	TCP	pop3	192.168.0.254	pop3
☑ 06	TCP	587	192.168.0.254	587
☑ 07	TCP	8080	192.168.0.250	8080
☑ 08	TCP	https	192.168.0.254	https
☑ 09	TCP	8888	192.168.0.7	8888
☐ 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



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
-

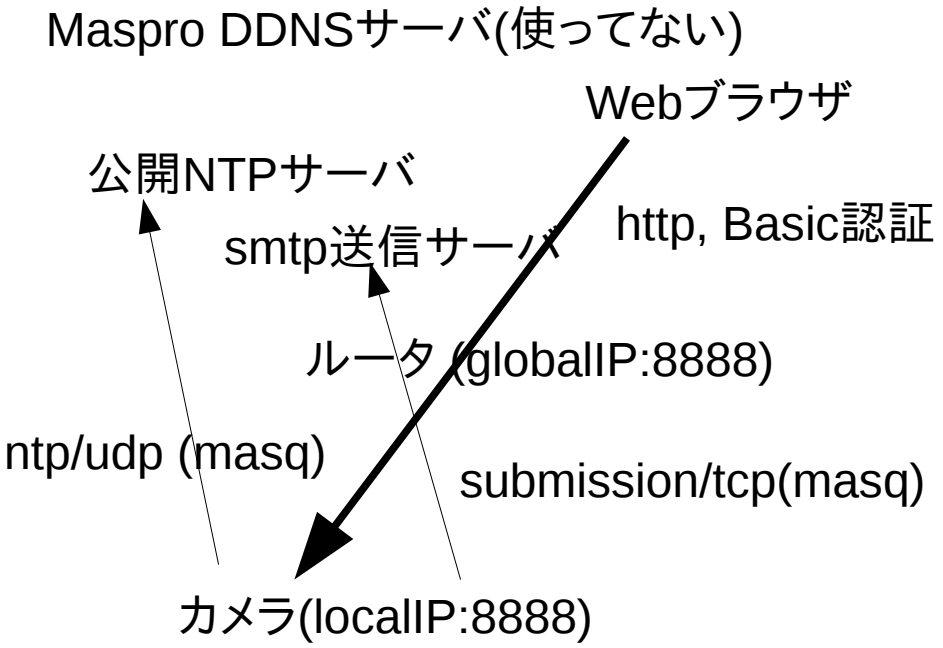
5. ある家庭での利用例(時間あれば実演)

- 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

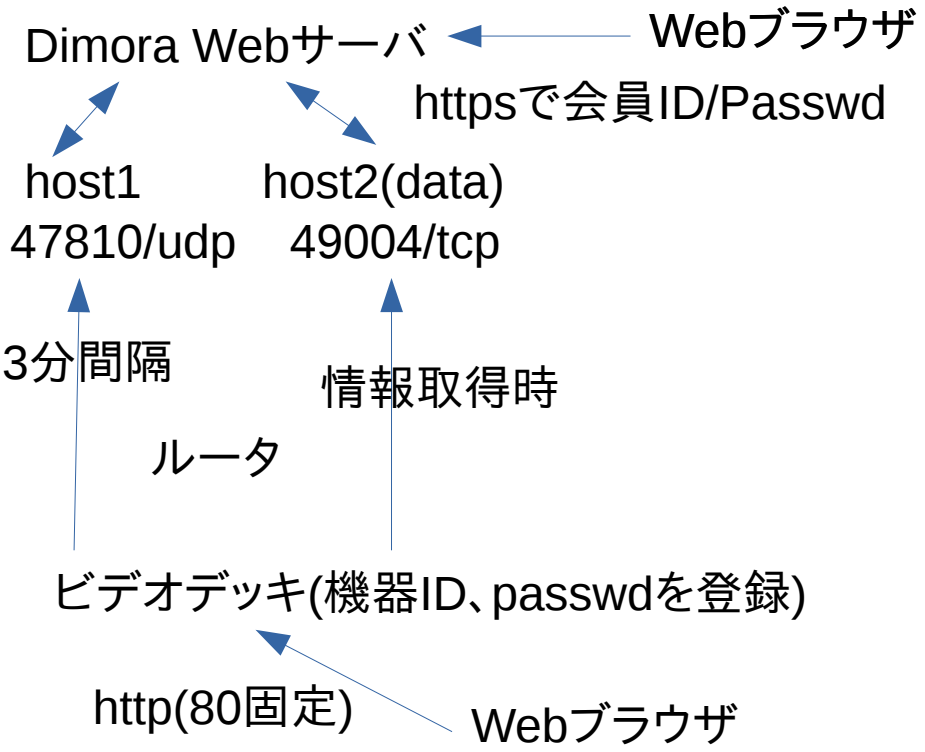
- Port forwarding(http)
  - 矢印は通信開始方向



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 forwading不要

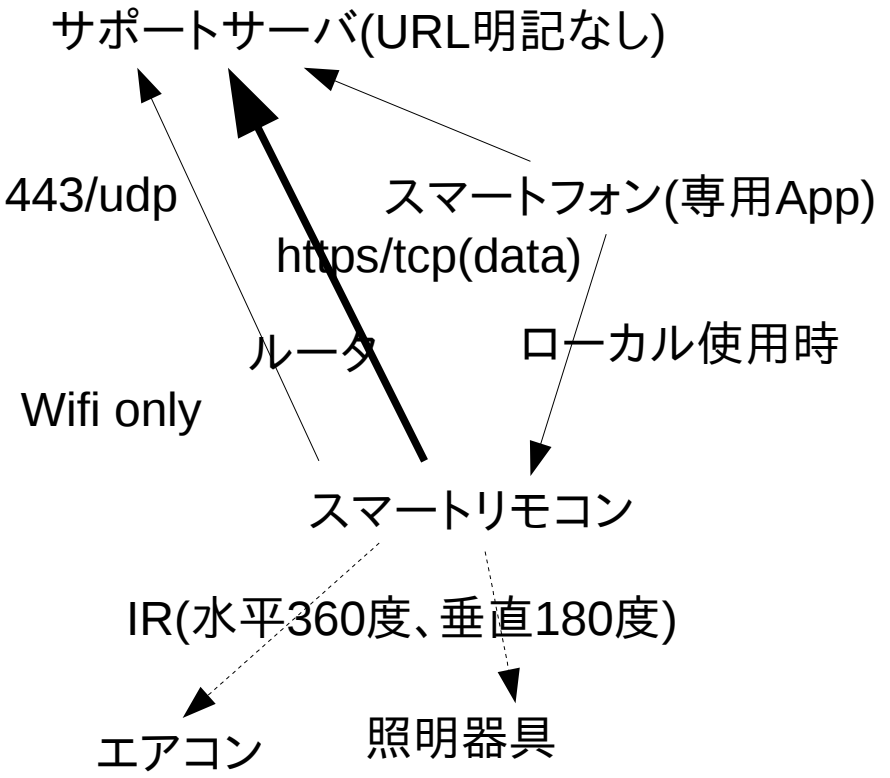


5. 続き(スマートリモコン)

- 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
  - プリセットから近いのを選択
  - または手動(やや難)
- 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?)
- FAQでは以下だが443だけ観測された

```
TCP     : 60001/60011
UDP     : 50001/50002/50003
SNTP    : 123
SSL/TLS : 443/8883
```

- Port forwarding不要



5. 続き(リモコン2)


家電リモコン一覧
家電リモコン(1)
家外有効


家電リモコン(1)
エアコン
2018/11/11 09:11計測
更新
温度
湿度
照度
23.3 ℃
47 %
226lx
0
50
0
100
0
1000


エアコン
冷房
暖房
除湿
自動
送風
温度
風量
30℃
静か
16℃
自動
17℃
1
停止
運転開始

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)

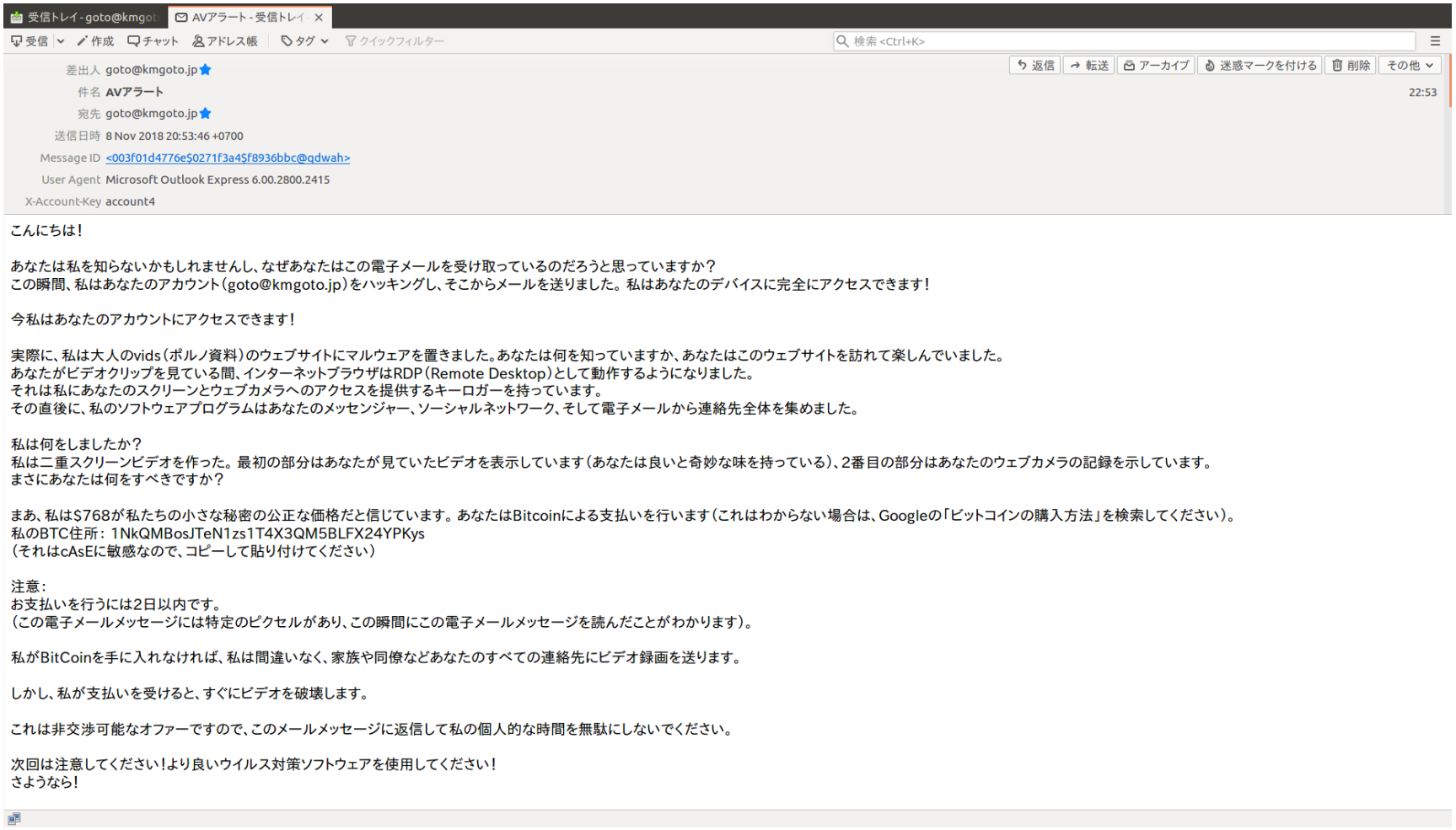
- SMSでも来るようになった詐欺メッセージ
  - 請求先の名前くらい書いてよね
  - 発信者名称、電話番号は嘘つき可
-

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)

おまけ (その2: email)

- 日本語: BitCoinで払えと言われてもねえ



受信トレイ - goto@kmgot　AVアラート - 受信トレイ

受信　作成　チャット　アドレス帳　タグ　クイックフィルター　検索 <Ctrl+K>

返信　転送　アーカイブ　迷惑マークを付ける　削除　その他

差出人 goto@kmgoto.jp
件名 AVアラート　22:53
宛先 goto@kmgoto.jp
送信日時 8 Nov 2018 20:53:46 +0700
Message ID <003f01d4776e$0271f3a4$f8936bbc@qdwah>
User Agent Microsoft Outlook Express 6.00.2800.2415
X-Account-Key account4

こんにちは！

あなたは私を知らないかもしれませんし、なぜあなたはこの電子メールを受け取っているのだろうと思っていますか？
この瞬間、私はあなたのアカウント（goto@kmgoto.jp）をハッキングし、そこからメールを送りました。私はあなたのデバイスに完全にアクセスできます！

今私はあなたのアカウントにアクセスできます！

実際に、私は大人のvids（ポルノ資料）のウェブサイトにマルウェアを置きました。あなたは何を知っていますか、あなたはこのウェブサイトを訪れて楽しんでいました。
あなたがビデオクリップを見ている間、インターネットブラウザはRDP（Remote Desktop）として動作するようになりました。
それは私にあなたのスクリーンとウェブカメラへのアクセスを提供するキーロガーを持っています。
その直後に、私のソフトウェアプログラムはあなたのメッセンジャー、ソーシャルネットワーク、そして電子メールから連絡先全体を集めました。

私は何をしましたか？
私は二重スクリーンビデオを作った。最初の部分はあなたが見ていたビデオを表示しています（あなたは良いと奇妙な味を持っている）、2番目の部分はあなたのウェブカメラの記録を示しています。
まさにあなたは何をすべきですか？

まあ、私は$768が私たちの小さな秘密の公正な価格だと信じています。あなたはBitcoinによる支払いを行います（これはわからない場合は、Googleの「ビットコインの購入方法」を検索してください）。
私のBTC住所：1NkQMBosJTeN1zs1T4X3QM5BLFX24YPKys
（それはcAsEに敏感なので、コピーして貼り付けてください）

注意：
お支払いを行うには2日以内です。
（この電子メールメッセージには特定のピクセルがあり、この瞬間にこの電子メールメッセージを読んだことがわかります）。

私がBitCoinを手に入れなければ、私は間違いなく、家族や同僚などあなたのすべての連絡先にビデオ録画を送ります。

しかし、私が支払いを受けると、すぐにビデオを破壊します。

これは非交渉可能なオファーですので、このメールメッセージに返信して私の個人的な時間を無駄にしないでください。

次回は注意してください！より良いウイルス対策ソフトウェアを使用してください！
さようなら！

おまけ (その2分析)

- メイ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: 自分のメイルサーバ行 (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)
- 実験で使用した製品
  - 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