安全なニンテンドーDSの使い方？

宮本 久仁男 a.k.a wakatono
wakatono@todo.gr.jp

ニンテンドーDS Lite
×WiFi
×Internet
～どうやって使おう～

宮本 久仁男 a.k.a wakatono
wakatono@todo.gr.jp

ニンテンドーDS Liteの無線LAN機能

- WiFi準拠（802.11b/g）
  - WEP 64bit/128bit/152bit で暗号化
- TCP/IPプロトコルスタックを装備
  - 軽量なスタック
- ネットワーク対応のゲームに使える
  - 無線LANアクセスポイント経由でインターネットアクセス／AdhocモードでDS同士の通信

一方WEP自体は？

- 言われてるほど強くはない
  - むしろ脆弱
  - 詳細は割愛
- WEP 152bitを使う？
  - 他の機械との共存の問題がある
  - それ以前に、鍵長が長くなってもヤバそう
    - （詳細は検証必要）
- じゃあ、WEPに頼らないところで安全にする方法は？
  - WPAは使えない

着目するポイント

- ニンテンドーDS（以下DS）同士の通信は範疇外
  - DSをつぶされる分には別にいいや（暴言）
- DS - 無線LAN AP – インターネットの場合
  - 通信先は固定
    - P2Pで端末間通信をするということはないだろう
  - プロトコルはゲームによってまちまち
- その通信は通したい
  - それ以外は通したくない

無線LAN APを無断で使われて困ること

- どこかへのアタックの踏み台にされる
- Spamなどを出されてしまう
- 家庭内のマシンをクラックされる危険性
- etc…

これらを防ぐためには？

通信を制限する手段(1)

- L2で制限
  - MACアドレスで制限
- L3で制限
  - IPアドレスで制限
- L4で制限
  - プロトコルやポート番号で制限
- L5以上で制限
  - L4のペイロード見て制限

…それ以外は？

通信を制限する手段(2)

- ヒューリスティック解析による制限
  - 通信の挙動を見て、それによる制限を施す
- DSの解析を行うにあたって立てた仮説は次のページに

DSの通信に関する仮説

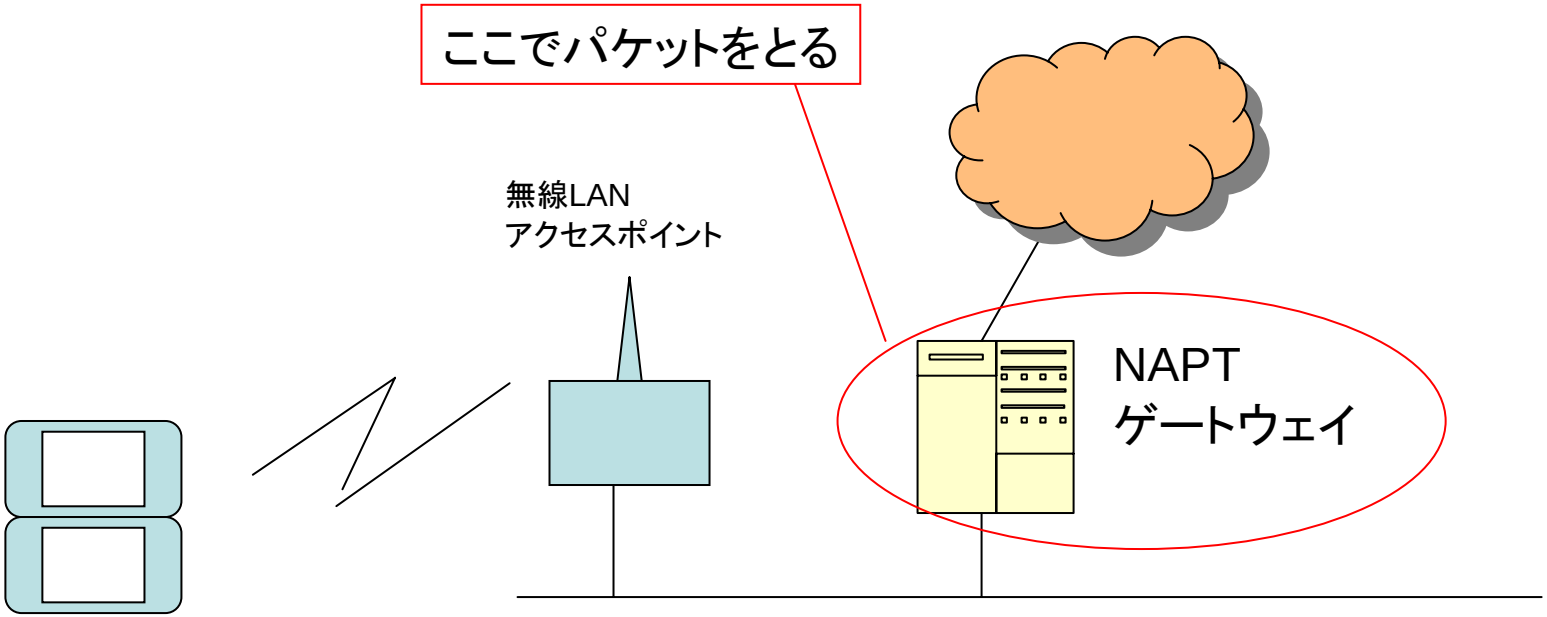
- 任天堂ブランドのゲームは通信先が固定
  - DNS Lookupや通信先は固定
    →固定の通信先は、実はトンネルのピア
  - 特定のポート番号を使っている
    →どこの家庭でもあるようなブロードバンドルータの内側からも通信可能
- 任天堂ブランド以外のゲームも通信先が固定
  - 通信先がどこであるか？は、ゲームの本質には関係ない
  - 場合によっては、通信先は（任天堂ブランドのゲームと）いっしょの可能性

実際に試してみる

- 具体的には？
  - 実際にゲームを動かしてみて、通信先を観測する
  - 直接DSが通信するようなケースは知らない

- まずやること
  - とりあえずどんなところと通信してるか？の把握
  - ホントに限定できるのであれば、それらのアドレス以外と通信できないようにしておけば問題なし

検証環境



- 電波法の兼ね合いがあるので、無線LANをダイレクトにモニタしない
  - 「偶然」自分のAPを使う「わけわからん人」のパケットをデコードしたくないし

解析でやってること

- ぶっちゃけやってることは

Man-in-the-Middle（中間者攻撃）

みたいなこと

自分ち限定

検証ソフトウェア

- マリ〇カート DS
- テ〇リス DS

結果は？

- とりあえずキャプチャデータを見てみましょう

パケットキャプチャの結果とその意味

- その時の通信先は以下のとおり

conntest.nintendowifi.net.
gpcm.gs.nintendowifi.net.
mariokartds.ms17.gs.nintendowifi.net.
nas.nintendowifi.net.

conntest.nintendowifi.net.
gamestats.gs.nintendowifi.net.
gpcm.gs.nintendowifi.net.
nas.nintendowifi.net.
tetrisds.master.gs.nintendowifi.net.
tetrisds.ms2.gs.nintendowifi.net.

実際の接続先は？

- いくつかあった
  - 単純に「全て同じつなぎ先」ではない模様
  - 少なくとも、ゲームごとに異なるFQDNが指定されている部分はある

持ってないソフトもある程度は...

- NINTENDO 役○DS

ゲームごとに異なるFQDN

- tetrisds.master.gs.nintendowifi.net
  mariokartds.master.gs.nintendowifi.net
  yakumands.master.gs.nintendowifi.net
  - 上記3つは全て同じアドレスを指す
- tetrisds.ms2.gs.nintendowifi.net
  mariokartds.ms17.gs.nintendowifi.net
  yakumands.ms5.gs.nintendowifi.net
  - 上記3つは同じアドレスを指す

ゲームによらず同じFQDN

- conntest.nintendowifi.net
  - 接続チェック用のアドレス
- gamestats.gs.nintendowifi.net
  - ゲームの結果を提供するサーバ
  - IIS5で構成されている
- gpcm.gs.nintendowifi.net
- nas.nintendowifi.net

提案する構成

- DS用のAPは独立で構成
  - 最大の鍵長を設定することで、クラック避け
  - DSのみに使わせることで、通信先の大幅な制限を可能にする
    - 前述のサーバに対するアクセスおよびDNSに対するアクセすのみを実施
    - DNS自体も固定でアドレス解決を行うように構成
- アウトバウンドの通信を制限
  - DSが通信するサーバとの間での通信のみ認める
  - DSが使うポート番号のみのアウトバウンド通信を認める

上記2つを満足できれば、「そこそこ」安全に出来るのではないか

ポート番号は実効的には難しい（多岐にわたるため面倒）

残存リスク

- 同一ネットワークに属するマシンが何かされる懸念
  - 対策：APのWAN側から直接アクセス可能な領域に、コンピュータを置かない
- 制限した上で通信可能なマシンに対する不正アクセスの懸念
  - IDSなどを設置することで、攻撃の予兆検知
  - それで通信可能なのは、ゲーム用のサーバ
    - それもリスクです
- 善良な（w）DSそのものの破壊／踏台化の懸念
  - DSに脆弱性が発見された場合
  - 成仏してください（汗

結論

- 少し大掛かりだが、WEPのみに頼る以上にはセキュアにすることが可能
  - 投資は少々
    - 無線LANルータが1ついる（FONルータで代替可？）
- 通信先に対するインシデント発生は、**「通信先になんらかの脆弱性がある場合」**には避けられない
  - そこまでは責任持てんよorz

参考

- Nintendo Wi-Fi Connection
  http://www.tetrisconcept.com/wiki/index.php/Nintendo_WiFi_Connection