学科内無線 LAN 構築
-ネットワーク利用認証ゲートウェイ Opengate 運用例-

九州工業大学
松元隆二

matsumoto(at)tech-i.kyutech.ac.jp

概 要

無線 LAN はセキュリティを甘くすると部外者の不正利用の温床になりやすいため、セキュリティ対策を高めに設定する事が多いと考えられるが、学科で導入した無線 LAN を非常に厳しい設定にしたところ、利用者が極めて少ない状況に陥ってしまった。利用率改善のため、佐賀大学で開発されたネットワーク利用認証ゲートウェイ Opengate を導入し、利用率の向上に成功した。
Key Words: 無線 LAN, Opengate

1 旧環境

私が運用を任されている学科の無線 LAN は H21 年度以前は以下のような運用を行っていた。

- MAC アドレスを申請した機材のみ利用可。
- 学生が利用する場合は指導教員の責任の基、教員を経由して MAC アドレスの申請を行う。
- 学外への直接通信は禁止。proxy 経由のみ。
- 通信ログは無し。学外のみ proxy がログを記録する。
- アンテナ設置場所はセミナー室 4 箇所。
- 利用時間制限無し。

という形で運用を行っていた。本学科の構成は職員約 30 名、学生は 1 学年あたり約 90 名であるが、無線 LAN 利用者は職員 4 名のみという惨状であった。うち 1 名は卒論の時だけ臨時にという対応であった。学生の利用申請は無かった。

一部より、簡単に使えるなら利用したいという意見があったが、「教室の黒板に WEP パスワードを書く」というような意見であった。この運用ではセキュリティインシデントが発生した時に利用者が特定できない。少なくとも利用者が特定できる無線 LAN 環境は死守すべきである。

2 新環境

利用率の改善のため、H22 年度に以下のような運用変更を行った。

- MAC アドレスの事前登録廃止。ネットワーク利用認証ゲートウェイ Opengate を使ったユーザ ID/パスワードを使った認証に変更。本学統合認証と連携した。Opengate については後述。
- 学科の計算機担当教員の了解の基、学科の学生が教員を介さずに直接利用申請を出す事を許可。
- 学外への通信は旧来 proxy のみであったが、学外への直接通信を一部解禁。http, https, pop, pop3s, imap, imaps, submission, smtps は直接通信を許可。頻繁に portscan に使われる smtp と ssh は学科内 (≠学内) に制限。ssh で学科外に出たい場合は、学科共通の UNIX 端末にログインしてから利用。
- 無線 LAN のルータの出口に Firewall を接続し、全ての通信を記録する。
- アンテナ設置箇所を増やし、学科共通の教室は全て無線 LAN エリア内にした。
- 利用時間制限は深夜 12 時〜朝 7 時は運用停止。学内規則で研究室に泊まる事は禁止されている。

環境更新後ユーザ数は増加し、H22 年 12 月現在、職員の利用数が 6 名、学生は 13 名利用している。複数台利用しているユーザも多く、現時点で 64 個の MAC アドレスが利用されたようである。

3 Opengate

Opengate は佐賀大学で開発された Web ブラウザ上でユーザ認証を行い、ネットワークの利用許可を与えるゲートウェイである [1]。

利用者側から見た利用形態は、次のようになる。Opengate 配下の無線 LAN に PC などを接続して、Web ブラウザを起動すると、http 通信の横取りが行われ、ユーザ認証のための Web ページに自動転送される。ユーザ認証に成功すると、通信が開放され、一般のネットワーク利用が可能になる。認証状態を Web ブラウザが保持し、Web ブラウザを起動している間だけ通信が可能になる。Web ブラウザを閉じると通信が遮断される。

管理者側からみた Opengate の構成は次のようになる。FreeBSD でルータを構築し、無線 LAN のネットワークと一般のネットワークの間に設置する。FreeBSD のルータ上で動作する Opengate がネットワークを監視している。無線 LAN 側に新規に通信してきた MAC アドレスが出現した場合 http 通信の横取りを行い、Web ブラウザでユーザ認証を行い通信の許可の可否を判断する。なお、無線 LAN に限らず有線 LAN でも利用可能である。

同等の機能を持つハードウエアやソフトウエアは数社から発売されているが、非常に高価である。しかし Opengate は GPL で公開されているため、安価に構築できる。

3.1 導入時の問題点

FreeBSD でルータを構築できるスキルのある管理者が存在するかという問題に尽きる。FreeBSD の ipfw の設定を理解して設定できる管理者でないと導入は難しいだろう。今回の導入ではソフトウエアをインストールしただけでは素直に動作しなかったため、Firewall のルールのデバック作業が入った。 ネットでググってコピペで対応している管理者には難しい。

Opengate のユーザ認証の backend として LDAP, pop, ftp などが利用可能である。本学科では ftp サーバを構築して認証に用いた。ftp サーバは利用者制限機能を提供している場合が多く Opengate に都合が良い。学科内の誰もがログインできる端末に ftp サーバを構築し、無線 LAN 利用申請があったユーザ ID に対して ftp 利用許可をあたえる方法で構築した。

(補足: ftp サーバは IP アドレスベースのアクセス制限をお勧めします。)

3.2 導入後の問題点

頻繁に利用しているユーザより、認証に失敗するという連絡が入った。調べるとゾンビ化した Opengate の daemon が残っていた。安直な対策であるが毎朝 reboot をかける運用に変更した。現在 crontab は以下のようにしている。深夜は運用停止しているため深夜にルータ機能を停止し、早朝再起動している。

crontab

```
10 0 * * * /sbin/sysctl net.inet.ip.forwarding=0
30 6 * * * /sbin/sysctl net.inet.ip.forwarding=1
40 6 * * * /sbin/shutdown -r +3
```

次に、H22/12/15 付けの Windows セキュリティ更新以降、IE の文字コード認識のルール変更で JIS コードで作成されているユーザ認証ページが文字化けするようになった。文字コードを UTF-8 に変更した。

4 パチモン無線 LAN 対策

無線 LAN は実配線が見えないため、偽物の無線 LAN を立てる事が簡単である。接続先が偽物の無線 LAN である可能性を否定できない。大学などの無線 LAN は非常に多くのユーザが WEP パスワードを共有しているため、なおさら危険である。

偽物の無線 LAN につないで偽物の認証画面で認証作業を行うとパスワードが漏洩する。

偽物対策のため、認証を https のみにし、SSL 証明書でオレオレ証明書を止め、UPKI[2] で発行したブラウザが認証可能な証明書を用いている。利用者に向けては、SSL 証明書回りで警告がが出た場合は認証しないよう注意喚起している。

某大学の無線 LAN マニュアルで、オレオレ証明書で運用して SSL エラーが出ても無視するよう指示しているを読んだ事がある。少なくとも UPKI 参加校は SSL の証明書の入手が容易なので、至急改善して欲しい。

参考文献

[1] Opengate ホームページ,
URL: http://www.cc.saga-u.ac.jp/opengate/

[2] UPKI イニシアティブ,
URL: https://upki-portal.nii.ac.jp/