

フィッシングサイトの体験

中西渉

watayan@meigaku.ac.jp
名古屋高等学校

第 14 回全高情研全国大会（大阪大会）

1 はじめに

2 実習環境

- 情報教室の環境
- サーバ環境
- 授業用サイト

3 実習

- SMTP, POP3 の観察
- 偽メールの送受信
- 偽サイト
- 生徒の反応

4 まとめ

1. はじめに

情報通信ネットワークは常に重要な要素

SMTP：メールの送信・転送プロトコル

- 送信者の確認をしない

→ 送信者を詐称できる

偽メールによる偽サイトへの誘導を体験させてみよう
(要するにフィッシング)

1 はじめに

2 実習環境

- 情報教室の環境
- サーバ環境
- 授業用サイト

3 実習

- SMTP, POP3 の観察
- 偽メールの送受信
- 偽サイト
- 生徒の反応

4 まとめ

2.1 情報教室の環境

勤務校について

- 1887年創立
- キリスト教主義
- 男子校
- 併設型中高一貫校（中6クラス，高12クラス）

情報教室について

- 入学時にアカウント作成（OpenLDAP で管理）
- 3 教室（48 + 1 台）

OS	Debian GNU/Linux
メールソフト	Sylpheed
Web ブラウザ	Firefox
教員画面転送	VNC
オフィスソフト	LibreOffice
	→ Google ドキュメント (?)

- 生徒は iPad を所有（2021～）
- 普通教室に Wi-Fi（2021～）

2.2 サーバ環境

サーバ：オンプレミス

OS	Debian GNU/Linux
Web サーバ	Apache
SMTP サーバ	Postfix
POP3 サーバ	Dovecot

偽サイトのサーバ：レンタルサーバ

2.3 授業用サイト

校内 Web サーバに授業用サイト

- moodle で構築
- 授業資料提供, 課題提出, 小テスト, ...
- 授業解説動画 (2020 年度～)
 - 2020 : 埋め込み動画
 - 2021 : YouTube の再生リスト



2020 年度



2021 年度

1 はじめに

2 実習環境

- 情報教室の環境
- サーバ環境
- 授業用サイト

3 実習

- SMTP, POP3 の観察
- 偽メールの送受信
- 偽サイト
- 生徒の反応

4 まとめ

3.1 SMTP, POP3 の観察

Sylpheed のログウィンドウ



The screenshot shows a window titled "プロトコルログ" (Protocol Log) with a scroll bar on the right. The log content is as follows:

```
* POP3サーバ: localhost に接続中...  
[11:35:48] POP3< +OK Solid POP3 server ready <23310.1625970948@pan>  
[11:35:48] POP3> USER watayan  
[11:35:48] POP3< +OK username accepted  
[11:35:48] POP3> PASS *****  
[11:35:48] POP3< +OK authentication successful  
[11:35:48] POP3> STAT  
[11:35:48] POP3< +OK 220 24874375  
[11:35:48] POP3> UIDL  
[11:35:48] POP3< +OK  
[11:35:48] POP3> LIST  
[11:35:48] POP3< +OK scan listing follows
```

POP3 について

- パスワードは*****で表示
 - 本当はそのままネットワークを流れる
- 盗聴の危険
- 以前は APOP
 - 今は通信自体を暗号化

SMTP について

- ユーザ名, パスワードなし
- 本人確認しない
- 「なりすまし」可能

3.2 偽メールの送受信

偽メールを眼の前で送る

- 定番ネタ
- (念のため) 他愛ない内容

同僚I氏の提案:「ホントに偽サイト作っちゃったらどうかな」

- リアルな状況設定
- フィッシングの話にもつながる

→「よし、やろう」

偽メールを送信

```
mitomn
root@kali:~# netcat 192.168.1.100.nagoya-gakuin.ed.jp 25
220 192.168.1.100.nagoya-gakuin.ed.jp ESMTD Postfix (Debian/GNU)
HELO nagoya-gakuin.ed.jp
250 192.168.1.100.nagoya-gakuin.ed.jp
MAIL FROM: support@nagoya-gakuin.ed.jp
250 2.1.0 Ok
RCPT TO: 192.168.1.100.nagoya-gakuin.ed.jp
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Content-type: text/plain; charset=UTF-8
From: サポート委員会 <support@nagoya-gakuin.ed.jp>
To: A組生徒諸君 <192.168.1.100.nagoya-gakuin.ed.jp>
Subject: 【緊急】ミラーサーバの設置

最近授業用サイトの動作が重いのでミラーサーバを設置しました。
http://nagoya-gakuin.192.168.1.100

--
名古屋高校ネットワークサポート委員会 <support@nagoya-gakuin.ed.jp>
.
250 2.0.0 Ok: queued as D1DA1440086
QUIT
221 2.0.0 Bye
root@kali:~#
```

- 偽メールであることは念を押す
 - 「これから偽メール送るからな」
 - 「ネット（略）委員会なんてないぞ」
 - 「『Ok』って出てるけどこのメールアドレスも嘘だぞ」
 - 「最近授業用サイトが重いのは本当だけどな」
- SMTP 直打ち
 - ホントはメールソフトの設定で簡単にできる
 - 真似しないように
 - 怪しげに見せる演出

3.3 偽サイト



本当の授業用サイト



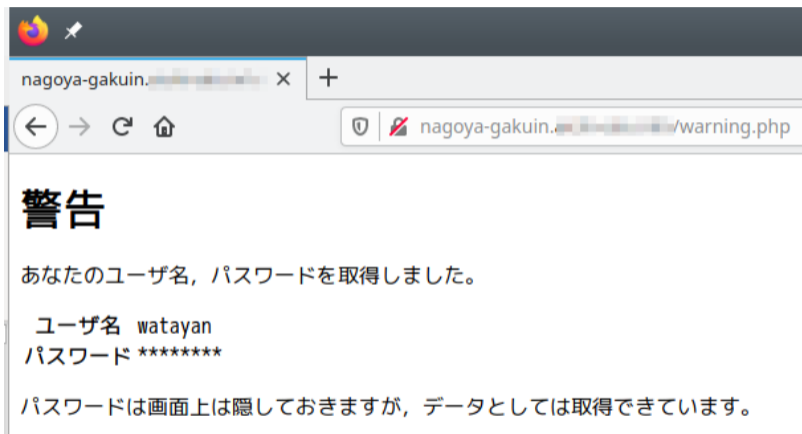
偽サイト

- 本物のHTML, アイコンなどをコピー
- URLも

本物 igw.nagoya-gakuin.ed.jp

偽物 nagoya-gakuin.(略)

偽サイトで「ログイン」すると...



(本当はパスワードは文字数だけカウント)

3.4 生徒の反応

質問：

これと同じメールが
普通に届いたらどうする？



生徒の反応は...

- 様子を伺ってそのまま
- 実際にアクセス
 - 話を聞いていない
 - だまされたフリ

実際のアクセスは...しまった!

アクセスログ設定

情報	保存周期 午前0時頃に前日のアクセスログを保存 保存場所 /home/username/www/logs/access_log_[日付] 保存形式 テキスト形式(前日のアクセスログはgzipで圧縮)
アクセスログの保存	<input type="radio"/> 保存する <input checked="" type="radio"/> 保存しない <input type="checkbox"/> エラーログも保存する
アクセスログの保存期間	<input type="text" value="12"/> ヶ月分
ホスト名の情報	<input type="radio"/> 保存する <input checked="" type="radio"/> 保存しない

1 はじめに

2 実習環境

- 情報教室の環境
- サーバ環境
- 授業用サイト

3 実習

- SMTP, POP3 の観察
- 偽メールの送受信
- 偽サイト
- 生徒の反応

4 まとめ

4. まとめ

- アクセス記録を取り忘れた→次年度こそは
 - セキュリティ意識の格差
 - 「変なの出たんですけど...」
 - 「嘘ってまるわかり」
 - 「だって鍵マークないやん」
- セキュリティの学習は早くやらないと!
- 高校では遅いか?
 - 理屈から説明しないと無意味