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

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）

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

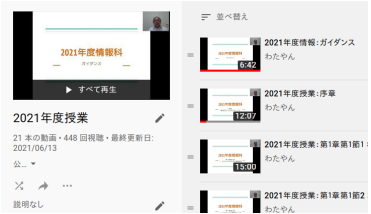
2.3 授業用サイト

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

3.1 SMTP, POP3 の観察

Sylpheed のログウィンドウ

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

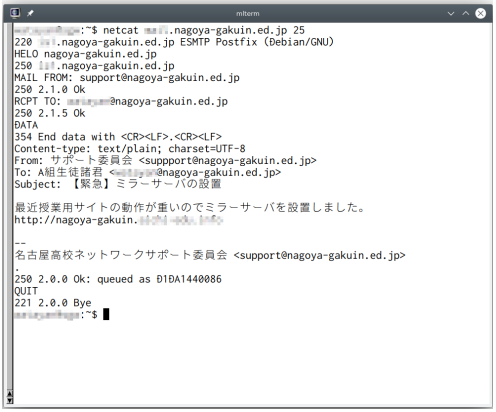
- 定番ネタ
- （念のため）他愛ない内容

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



- 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

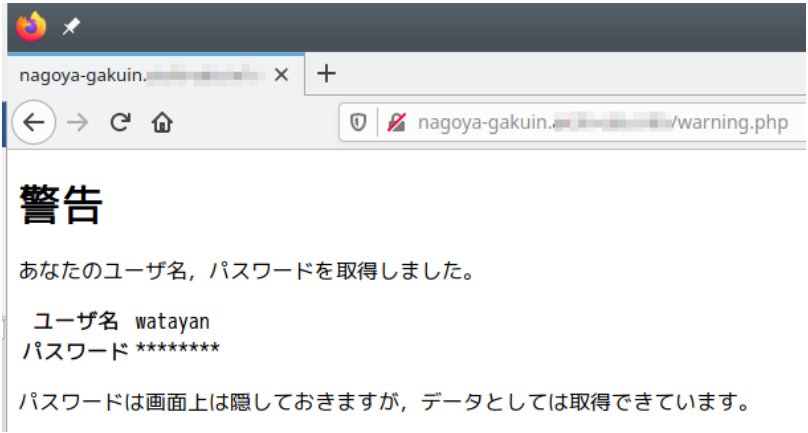
3.3 偽サイト

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：

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!

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