# Sanesecurityのこと

小島　肇
龍谷大学理工学部

# before

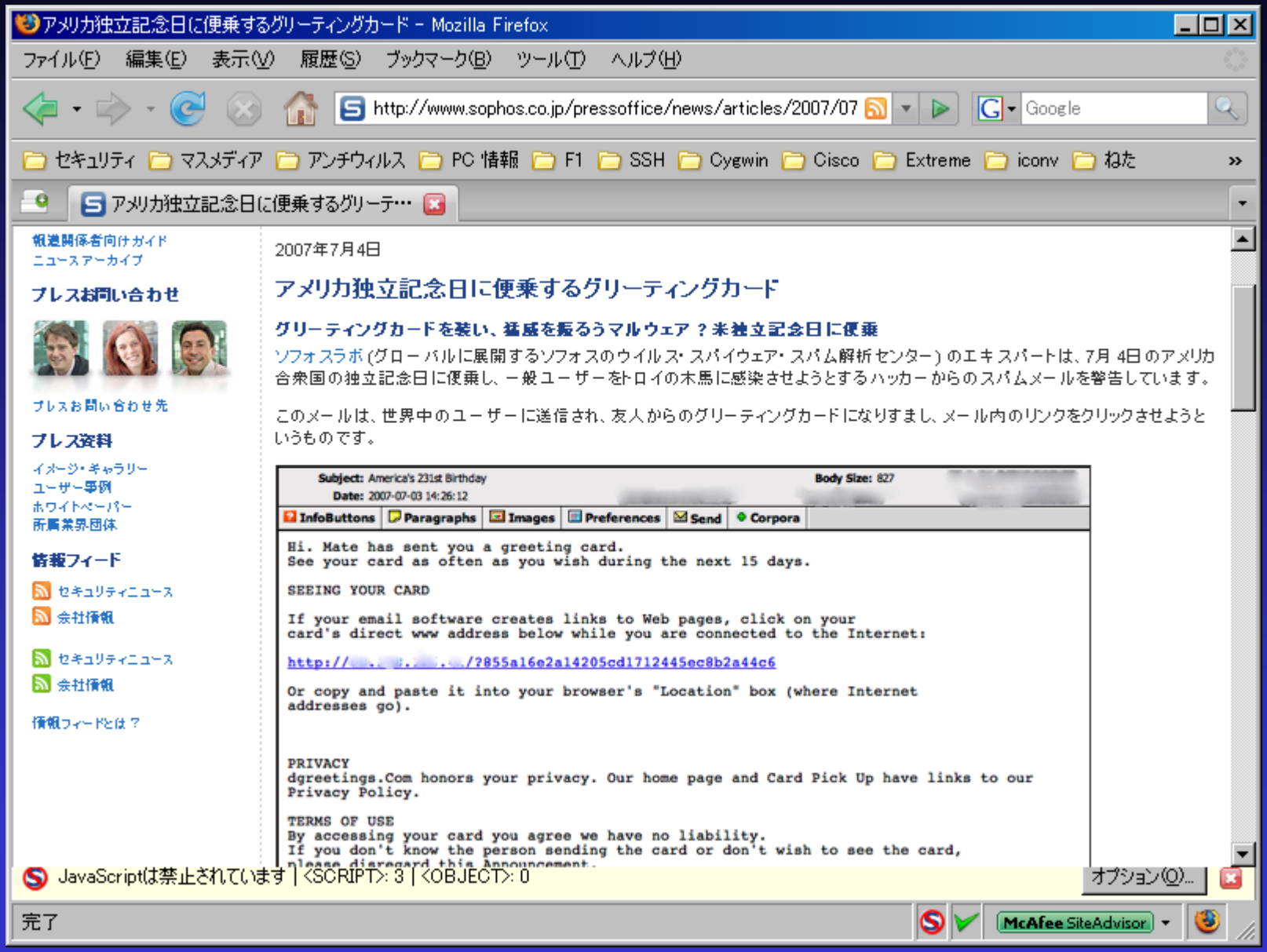
- FreeBSD + postfix 2.2 + amavisd-new + S25R
  - sophos (sophie) + clamav (clamd)

# amavisd-new

- MTA とコンテンツチェッカー（アンチウイルスやアンチスパム）とのインターフェイスとなるプログラム
  - 複数のアンチウイルスプログラムを併用できる
- amavisd-new が MIME を分解し、各パートをコンテンツチェッカーで検査する
- http://www.ijs.si/software/amavisd/

# E-card spam 襲来

- ある日、ウイルスサイトへのリンクが書かれたメールが大量に届き始めた
- それ自体はウイルスじゃないのでそのまま届く




http://www.sophos.co.jp/pressoffice/news/articles/2007/07/july4.html

# 2007.07.04 15:42:51 +0900

- 学内から学外へのメールが Email.Phishing.RB-1221 として検出された
  - 当時の e-card ねたの検出名
- その後も同様事例が数回発生
- なぜ学外→学内の時点で検出されなかったのか?

# 検出されたメールを分析

- メール本文にフィッシングメール全体（メールヘッダ＋メール本文）が記載されているような転送メール
- ClamAV のフィッシング検出ルールはメールヘッダも見ているのか?

# after (phase 1)

- FreeBSD + postfix 2.3 以降 + amavisd-new + S25R
  - sophos (sophie) + clamav (clamd)
  - postfix milter interface + clamav-milter
  - 実際には postfix 2.4 を使用

# インストール

- /etc/mail/sendmail.mc に以下を追加
  - INPUT_MAIL_FILTER(`clmilter',
    `S=local:/var/run/clamav/clmilter.sock, F=,T=S:4m;R:4m')dnl
    define(`confINPUT_MAIL_FILTERS', `clmilter')
- cd /etc/mail; make install
- /etc/rc.conf に以下を追加
  - clamav_milter_enable="YES"
    clamav_milter_flags="-H -N -n -P --local --outgoing ¥
    --max-children=10 --quarantine-dir=/var/spool/quarantine ¥
    --external --timeout=0"

# インストール

- /var/spool/quarantine を作成
  - mkdir /var/spool/quarantine
    chown clamav:clamav /var/spool/quarantine
    chmod 700 /var/spool/quarantine
- /usr/local/etc/rc.d/clamav-milter.sh に以下を追加
  - start_postcmd=start_postcmd
    start_postcmd()
    {
    echo "5 sec waiting for ${clamav_milter_socket}... "
    sleep 5
    chgrp postfix $clamav_milter_socket
    chmod g+rwx $clamav_milter_socket
    }

# インストール

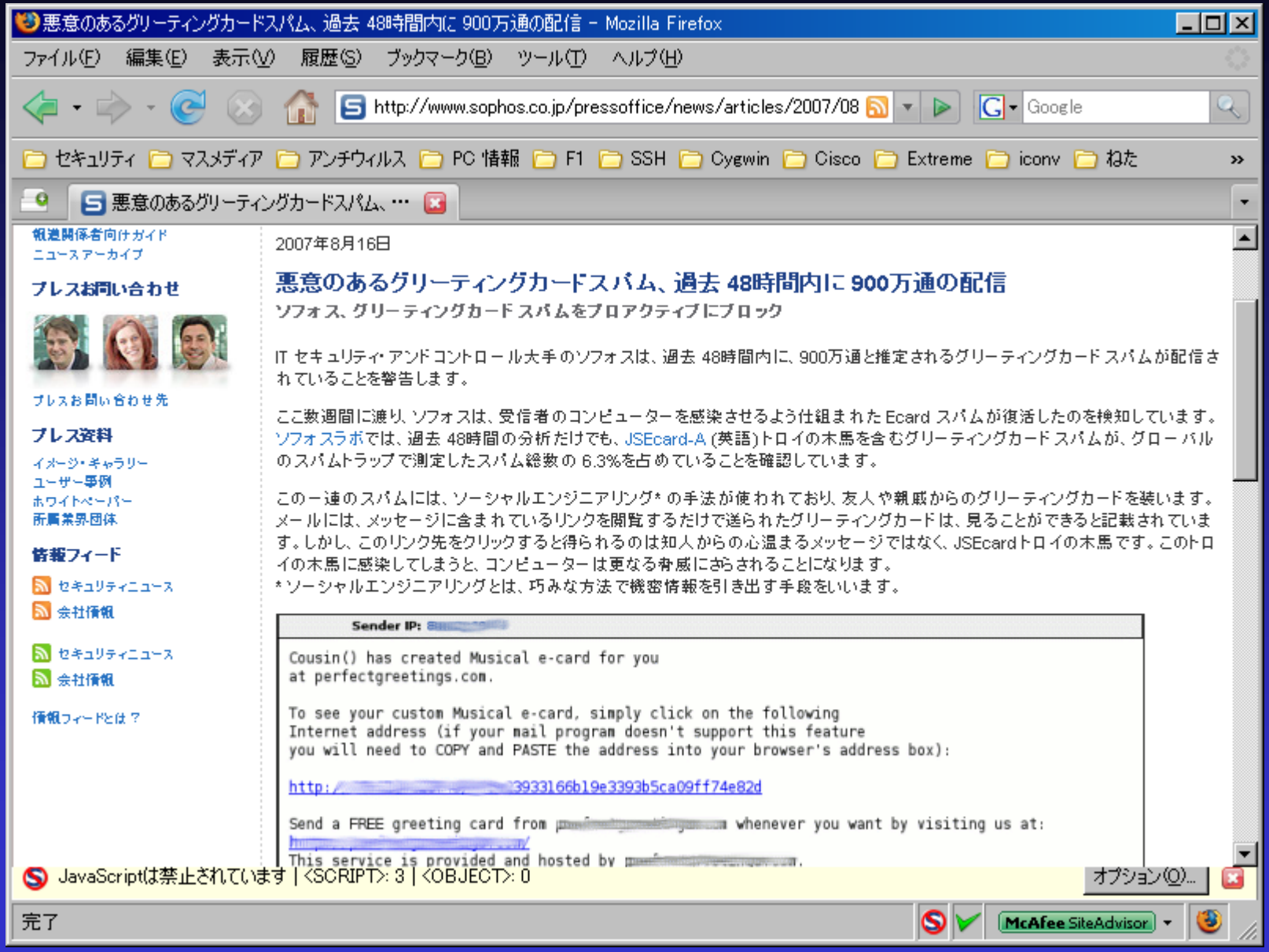
- /usr/local/etc/postfix/main.cf に以下を追加
  - smtpd_milters = unix:/var/run/clamav/clmilter.sock
    milter_default_action = accept
- /usr/local/etc/postfix/master.cfに以下を追加
  - 127.0.0.1:10025 inet n - n - - smtpd
    ……
    -o smtpd_milters=
- clamav-milter を起動し、postfix reload

# 結果

- ClamAV で対応されているものについては正常に検出されるようになった模様

しかし……

# 8月にまたもや
# e-card spam
# 大流行




http://www.sophos.co.jp/pressoffice/news/articles/2007/08/malicious-ecard.html

# spam 対策の重要性の増大

- ウイルス対策としての spam 対策が必要だと悟る
- しかし
  - 素の ClamAV の spam 対応は弱い
  - 金はない
  - 誤検出は困る

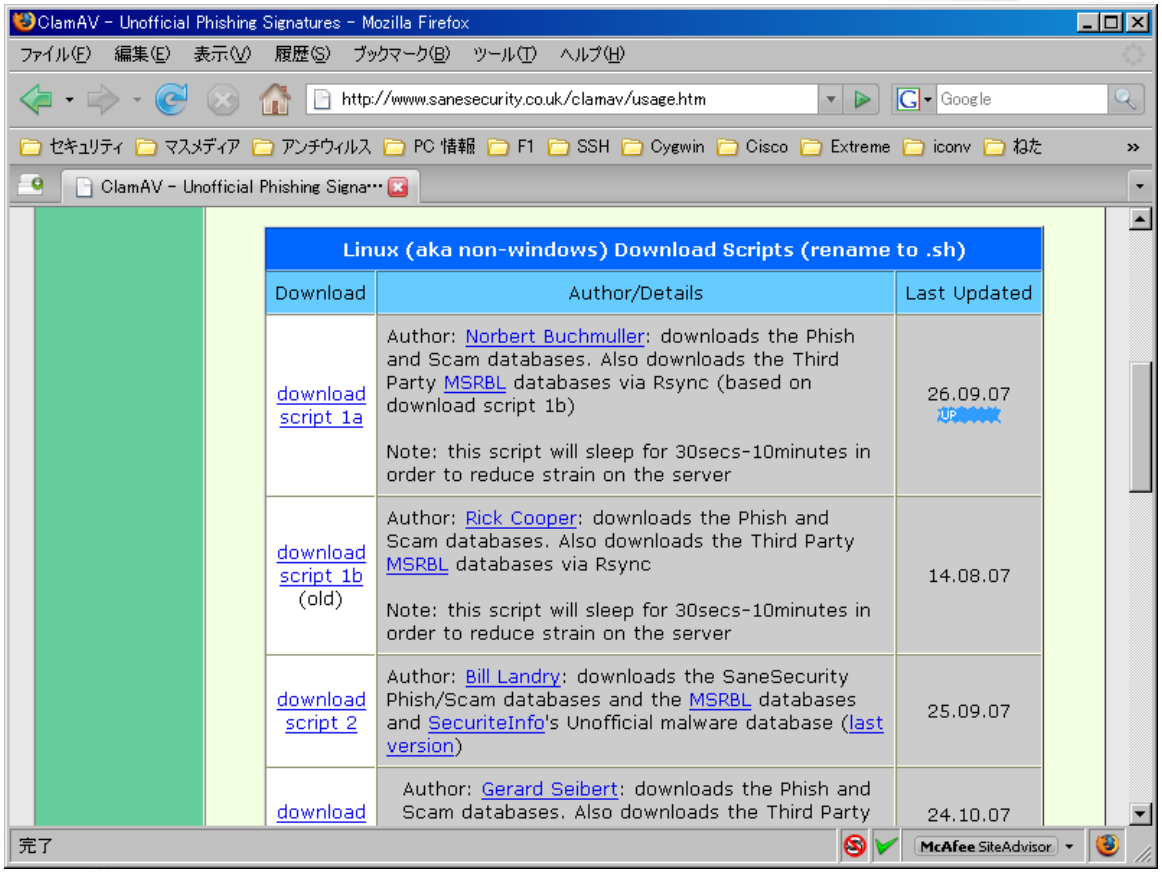
そこで……


http://www.sanesecurity.co.uk/

# Sanesecurity

- ClamAV で利用できる、spam 検出用の独自のシグネチャを提供
- 無料
- ダウンロードするだけで利用できる

# ダウンロードスクリプト




http://www.sanesecurity.co.uk/clamav/usage.htm

# ダウンロードスクリプト

- 複数のスクリプトが提供されている
  - Windows 用もある
- いずれにも MSRBL という RBL データのダウンロードが含まれている
  - 手元では、その部分はコメントアウトして利用

# after (phase 2)

- FreeBSD + postfix 2.3 以降+ amavisd-new + S25R
  - sophos (sophie) + clamav (clamd)
  - postfix milter interface + clamav-milter
  - Sanesecurity

# 使用感

- 英語圏の spam にはそれなりに有効
  - stock spam とか
- CJK spam にはめっぽう弱い
- 誤検出は確認していない

# 質問？