

標的型メールがやってきた

寺田真敏 ((株) 日立製作所)

標的型メールの対応経緯

2008年6月5日、コンピュータセキュリティ(CSEC)研究会が主催するコンピュータセキュリティシンポジウム2008(CSS2008)のCFP(Call For Papers)を騙ったウイルスメール^{☆1}が出回った。ウイルスメールは、特定の組織やコミュニティに狙いを定めてメールの文面などをカスタマイズする標的型メールであった。幸い各組織が導入していたアンチウイルスソフトにより検知されたため大事には至らなかった。今回のマルウェア特集に寄せて、当時、CSEC研究会主査であった筆者の視点から、CSS2008のCFPを騙った標的型メールの対応経緯について紹介する¹⁾。

攻撃活動の変遷

●見えなくなってきた攻撃活動の全容

2000年以降のインシデントの変遷をまとめると表-1のようになる。あくまでも主観的な視点からまとめた表であり、必ずしもすべての攻撃活動を網羅しているものではない。しかし、ここ10年間の攻撃活動の変遷を見る限り、短いサイクルで新たな攻撃活動が生まれ、一度確立した攻撃活動は決してなくなることはない。さらに攻撃活動を通じた技術の継承と徹底したカスタマイズ化によって、攻撃活動の全容が見えないという状況に追い込まれているような感じがある²⁾。

●大量流布型から標的型へ

標的型攻撃という用語が広がり始めたのは2005年で米US-CERTが発行した「TA05-189A: Targeted Trojan Email Attacks」という注意喚起文書がきっかけとなった³⁾。Targeted Attack=標的型攻撃は、特定の組織やコミュニ

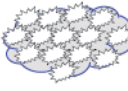
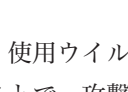
年代	特徴	被害の模式図
2000年 ～2001年	均一的かつ広範囲にわたる単発被害 Webサイトのページ書き換え	
2000年 ～2005年	均一的かつ広範囲にわたる連鎖型被害 マルウェア添付型メールの流布 ワームの流布	
2005年～	類似した局所的な被害 SQLインジェクションによるWebサイト攻撃 Winny, Shareによる情報流出 フィッシング、スパイウェア、ボットなど	
2006年～	すべてが異なる局所的な被害 標的型攻撃	

表-1 2000年以降の攻撃活動の変遷

ティに狙いを定めて、文面、添付ファイル、使用ウイルスなどを相手にあわせてカスタマイズすることで、攻撃活動検出率を下げ、攻撃成功率を高める手法である。

ここで、2004年に流布したW32/Netsky(ネットスカイ)と比較してみる。W32/Netskyは、電子メールの添付ファイルとして広がった電子メール流布型のマルウェアである。その当時、マルウェア開発者同士の競争もあったか、W32/Netskyとその対抗馬であるW32/Bagle(ベグル)の発生種別数は、多いときで双方合わせて約30種/月(2004年3月)となった。主にpif(MS-DOSアプリケーションへのショートカット)という拡張子の付いたファイルを添付することを特徴としていた。

同じ電子メールを介して流布したマルウェアであっても、CSS2008のCFPを騙った標的型メールと2004年に流行ったW32/Netskyが添付されたメールには、表-2に示すような違いがある。標的型メールは、怪しさを感ぜさせない普通のメールであり、報告件数(≒配布件数)も少なく、さらに、感染後も目立つような活動はしないやっかいな攻撃手法である。

標的型メールがやってきた

●2008年6月5日11:47 事のはじまり

CSS2008のCFPを騙ったウイルスメールが送付され

☆1 本事案の第一報が「CSS2008のCFPを騙ったウイルスメール」として報告されたことから、本稿では受信したマルウェアの添付された標的型メールのことをウイルスメールと記述する。

項目	マルウェア添付メールの昔	マルウェア添付メールの今
流布時期	2004 年	2008 年
タイプ	大量流布型	標的型
添付ファイル名	your_product.pif など	css2008-cfp.pdf
検出マルウェア名	W32/Netsky	TROJ_PIDIEF.DU
メール受信画面	「See the attached file for details. (詳細は添付ファイルを見てね)」と書かれている。亜種によって文面や添付ファイル名は異なるが、メール本文は明らかに怪しさの残る文面である(図-1)。	メール本文に記載されている CSS2008 の開催目的、開催時期、場所などは、CSS2008 の発表募集要項である CFP から切り貼りして作成された文面であり、怪しさをまったく感じさせない(図-2)。
報告件数	2008 年に IPA に報告された届出件数 4,867 件	CSEC 研究会で確認した該当メール受信数 5 件
感染後の活動	自分自身の分身を多数作成するために、マルウェア添付メールを大量に送信する。	攻撃者が用意したサーバから有害なプログラム等をダウンロードしたり、情報をアップロードする。

表-2 マルウェア添付メールの今と昔の比較

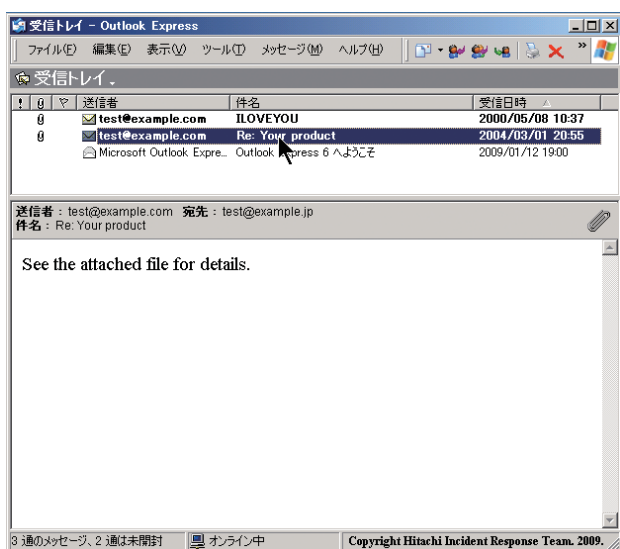


図-1 W32/Netsky が添付されたメール受信画面

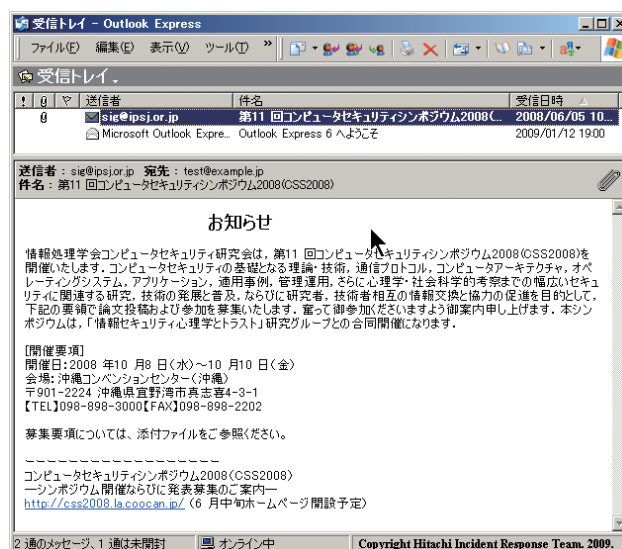


図-2 CSS2008 の CFP を騙った標的型メールの受信画面

たことは、CSEC 研究会関係者から主査・幹事宛への第一報と、知り合いからの連絡で知ることとなった。やはり情報入手経路は多いに限る。心の中では、攻撃者に対して『余計なことを！』『CSEC 研究会への挑戦？』などと思う反面、インシデントレスポンスチームに所属している身として、この貴重な経験をどうやって活用しようかと考えている自分がいた。

Subject: (csec-adm 1844) CSS2008 の CFP を騙ったウイルスメール([Fwd:Fwd: 第11 回コンピュータセキュリティシンポジウム 2008 (CSS2008)])
Date: Thu, 05 Jun 2008 11:47:42 +0900

とりあえず、第一報です。

添付のような、CSS2008 の CFP を騙ったウイルスメールがあるようです。弊社のウイルスチェックにひっかかりました。

- 送信元 sig@ipsj.or.jp は詐称されているようです。
- メッセージヘッダに基づく送信元 210.108.157.54 を whois で引くと、韓国方面です。

まだ詳細は把握できておりませんが、取り急ぎエスカレーションまで。

● 2008 年 6 月 5 日 12:40 注意喚起活動

ウイルスメールには、感染のための攻撃コードを埋め込んだ PDF (css2008-cfp.pdf) が添付されていた。Web 掲載していた CSS2008 の CFP (css2008-cfp.pdf) をダウンロードして攻撃コードを埋め込んだと考えられる。ただし、この時点でできることといえば、CSEC 研究会関係者に、ウイルスメールが出回っていることと、今後発生し得る類似の攻撃活動による被害を抑えるため、電子メールによる CFP 配布はテキスト版 CFP に制限することくらいであった。その当時のメールを見返すと、次のような気持ちであったようだ。

Date: Thu, 12 Jun 2008 18:48:11 JST

寺田です。
CSEC HP に掲載している PDF(*)は、そのままです。
なぜなら、削除すると負けた気がしてくやしいからです。

*) CSS2008 の CFP として用意したオリジナル PDF ファイル

● 2008年6月9日 情報収集開始

幸い各組織が導入していたアンチウイルスソフトにより検知されたため大事には至らなかったこと、数日間様子を見ていたが第2波もないことから、今回発生したウイルスメール受信の実態調査に重点を移した。しかし、CSEC 研究会関係者から情報を募っても最終的に確認できた受信件数は4組織、わずかに5件である。また、いずれもほぼ同時刻（2008年6月5日10:45前後）に、同一送信元（韓国，210.108.157.54）から発信されたという情報のみであった。残念ながら、これだけの情報では何もできない。

このままでは引き下がれないので、今後、CSEC 研究会関係の CFP を騙ったウイルスメールが出回らないようにするための手立てを考えることにした。たどりついた結論は、今回の攻撃活動が標的型攻撃をベースとしたメール（以降、標的型メール）であったことから、①守る側も複数組織が協力して攻撃者の手口を明らかにする活動を試みる、②攻撃者の手口を徹底的に公開することとした。特に、複数組織が協力するとした背景には、標的型攻撃が各組織の個別事案となることが多いため、実態把握のための情報交換をしにくい。この課題を打破したいという思いがあった。

もちろん、この目的を達成するためには、検体（マルウェア添付メール）を回収する必要がある。検体を回収できると、CSS2008 と同時期に開催する MWS2008（マルウェア対策研究人材育成ワークショップ）の研究素材に利用できるかもしれないという気持ちがあったことは言うまでもない。

● 2008年6月12日 検体確保

CSS2008 の CFP を騙った標的型メール5件のうち、2件は日立ドメイン宛に送付されていたことから、すぐに、CSEC 研究会主査の帽子を脱ぎ、日立インシデントレスポンスチームの帽子にかぶりなおした。検体を確保できなければ攻撃者の手口を明らかにできず、標的型メ

ールの実態を伝えることもできない。やるべきことは、メール運用部署に協力を依頼し、ログサーバから該当メールを確保することである。

● 2008年7月25日 研究会運営委員会

7月25日の CSEC 研究会運営委員会において、CSS2008 の CFP を騙ったウイルスメールの対応経緯を報告するとともに、対応経緯の公開を提案し、関係各位の了解を得た。たかがウイルスメールの受信ではあるが、標的型の場合には、『気が付いているぞ!』ということをも明らかにすることは、数少ない攻撃活動を検出していることを意味するので、攻撃者に対するわずかな抵抗であっても効果を期待できると信じている。

CSEC 研究会運営委員会会議録 -第50回-

日時：2008年7月25日(金) 12:00-13:00
場所：福岡システムLSI総合開発センター

- (10) CSS2008 CFP を騙ったウイルスメールの対処：寺田@日立
ウイルスメールへの対処として、次のような対処提案があった。
ーウイルスメールを受信した組織に、ウイルスメールの検体提供を依頼する。
ーウイルスメールによる被害をIPA、JPCERT/CCに報告する。
ー情報処理学会コンピュータセキュリティ研究会関係者に対して、検体の調査を依頼する。
ーこれらの経過を、CSEC 研究会のHPですべて公開する。
(含む、CSS2008のナイトセッションでの経過報告)

● 2008年8月4日 検体提供の依頼開始

CSS2008 の CFP を騙ったウイルスメールを受信した関係者に、検体提供の依頼を開始する。5件のうち、2件はすでにアンチウイルスソフトがメール自身を削除してしまったため回収不能、1件はログとして残っていたが組織外への提供不可という状況で、すでに日立で確保した検体に期待するしかなかった。

いくら検体を組織内で確保できたといっても、必ずしもその検体を組織外に提供できるわけではない。実は、ここを守る側の弱点がある。攻撃側は情報、ツールを交換／共有できるが、防護側に至っては情報セキュリティの壁がその交換／共有を阻んでしまうことがある。これは、攻撃活動の全容を見えにくくする方向にプラスに働き、攻撃者に有利な状況を作りだすことになってしまう。

● 2008年8月26日 検体回収の実現

CSS2008 の CFP を騙ったウイルスメールが公開情報であったことが幸いし、検体回収、すなわち、日立から CSEC 研究会への検体提供が実現した。検体提供につきましては、システム開発研究所の所長であった前田所長のご支援に感謝いたします。



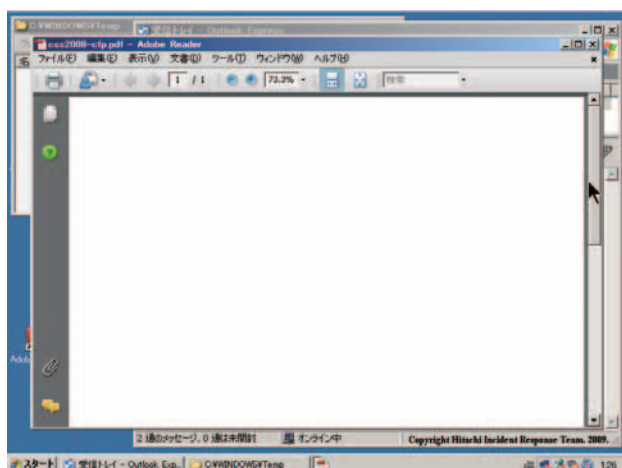


図-3 白紙のPDF表示



図-5 CSS2008のオリジナルCFPのPDF表示

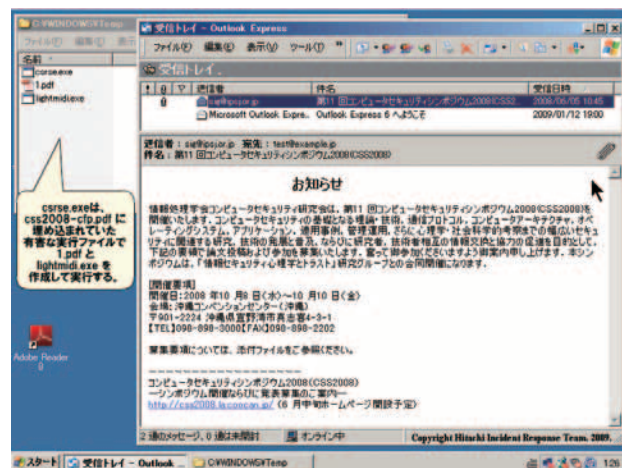


図-4 csrse.exe, 1.pdf, lightmidi.exeの作成

(c) CSS2008 の CFP の PDF 表示

csrse.exeによって作成されたCSS2008のオリジナルCFPのPDFファイル(C:\WINDOWS\Temp\1.pdf)を表示する。表示の際に、一度Adobe Readerのプロセスを終了するため、白紙のPDF(css2008-cfp.pdf)表示が消え、改めてCSS2008のオリジナルCFPがPDF(1.pdf)表示される(図-5)。

(2) 感染後の活動に関する解析結果

csrse.exeによって作成されたlightmidi.exeは、レジストリ改変とファイルのダウンロードを行うサービスをPCに登録する。その後の活動として、WebサイトからHTTP手順で新たなファイルをダウンロードし、実行する。ダウンロードするファイルはオンラインゲームのIDとパスワードを盗む仕様であり、アンチウイルスソフトが既知マルウェアとして検知したことから、使い回しされている可能性が高いということが分かった。

● 対応経緯の公開

「②攻撃者の手口を徹底的に公開する」については、攻撃者を牽制することも目的の1つにあるが、守る側の立場からも、標的型攻撃の実態の一端を明らかにし、対応の一事例として参考となることを期待したものである。多くの事実を公開するため実施した活動について表-3に示す。特に、CSS2008ナイトセッションにおいて青木一史氏の発表した検体解析結果報告が、ナイトセッション優秀発表第3位に輝いたことを付け加えておきたい。

● 2008年9月1日 検体解析の依頼開始

「①守る側も複数組織が協力して攻撃者の手口を明らかにする活動を試みる」を実現するため、CSEC研究会からNTT情報流通プラットフォーム研究所に検体解析を依頼した⁴⁾。解析結果は、次の通りである。

(1) 感染動作に関する解析結果

(a) 白紙のPDF表示

メールに添付されているPDF(css2008-cfp.pdf)を開くと、PDF内に埋め込まれたJavaScript経由で攻撃コードが実行され、白紙のPDFが表示される(図-3)。

(b) マルウェア感染

攻撃コードは、Adobe Readerに存在する脆弱性(JVND-2008-001095)を利用して、C:\WINDOWS\Temp\csrse.exeを作成し、実行する。csrse.exeは、CSS2008のオリジナルCFPのPDFファイル(C:\WINDOWS\Temp\1.pdf)と、実行ファイル(C:\WINDOWS\Temp\lightmidi.exe)を作成する(図-4)。

日付	対応活動
2008 月 7 月 25 日	CSS2008 の CFP を騙ったウイルスメールに関する対応経緯の Web 掲載を開始
2008 月 10 月 8 日	CSS2008 ナイトセッションにおいて検体解析結果の報告（発表者：NTT 情報流通プラットフォーム研究所 青木一史氏）
2008 年 10 月 12 日	IPA, JPCERT コーディネーションセンターへの報告
2008 年 10 月 28 日	検体解析結果を Web 掲載
2008 年 12 月 3 日	受信したウイルスメールの画面スナップショットを Web 掲載
2009 年 1 月 26 日	CSS2008 の CFP を騙ったウイルスメール受信の仮想体験デモを Web 掲載

表-3 対応経緯の情報公開活動

次の一步に向けて

対応経緯の公開による効果かどうかは分からないが、幸いにして、CSS2009 では CFP を騙ったウイルスメールが出回ることにはなかった。

標的型攻撃に関する多くの調査報告で「不審なメール」という用語を使って注意喚起を促している。実際に標的型攻撃で利用されるメールは、CSS2008 の CFP を騙ったメールを見る限り、怪しさを感じさせない普通のメー

ルであった。まずは、普通のメールが攻撃に利用されているという認識を持つことが、対策のための第一歩として重要だと感じている。次の一步として、見えなくなってきた攻撃活動の全容に歯止めをかける協力体制を MWS（マルウェア対策研究人材育成ワークショップ）を通して検討していきたいと考えている。

最後に、この場をお借りして、CSS2008 の CFP を騙ったウイルスメールへの対応にご協力をいただいた関係組織の皆様にお礼申し上げます。

参考文献

- 1) CSEC 研究会：CSS2008 の CFP を騙ったウイルスメールに関する情報，<https://www.sdl.hitachi.co.jp/csec/css2008-cfp-secinfo.html>
- 2) IPA：情報セキュリティ白書 2009 第 II 部 10 大脅威，<http://www.ipa.go.jp/security/vuln/documents/10threats2009.pdf>
- 3) US-CERT：TA05-189A：Targeted Trojan Email Attacks，<http://www.us-cert.gov/cas/techalerts/TA05-189A.html>
- 4) 新米セキュリティ担当者が行く！CSIRT 奮闘記 現場訪問編：日立製作所の「HIRT」，日経 NETWORK 1 月号，日経 BP 社，No.117，pp.92-95（2010）。

（平成 22 年 1 月 17 日受付）

寺田真敏（正会員）

masato.terada.rd@hitachi.com

（株）日立製作所システム開発研究所主管研究員／Hitachi Incident Response Team チーフコーディネーションデザイナー。コンピュータネットワーク、ネットワークセキュリティの研究開発に従事。2006 年から 2008 年 CSEC 研究会主査。

