山形大学紀要（工学）第28巻　第１号　平成16年２月
Bull. Yamagata Univ. (Eng.) Vol.28 No.1 Feb. 2004

ＷＥＢページ改ざんコンテスト “The Defacers Challenge”への対応報告

奥山　澄雄・鈴木　勝人・伊藤　智博・仁科　辰夫・青木　和恵

Countermeasures for “The Defacers Challenge” at Yamagata University Yonezawa Campus

Sumio Okuyama, Katsuhito Suzuki, Tomohiro Ito, Tatsuo Nishina, and Kazue Aoki

山形大学総合情報処理センター，〒992-8510 山形県米沢市城南4-3-16
Computing Service Center, Yamagata University
4-3-16 Jonan, Yonezawa 992-8510, Japan

（平成15年10月２日受理）

Abstract

On July/7/2003, “The Defacers Challenge”, which was cracking contests for Web pages was held. By way of countermeasures, we performed an announcement for the peopele in the campus, reduction of network usage, application of patchs for computers, watching for the network. As a result, no damage was found on the campus computers.

１　はじめに

2003年７月３日，海外のサイト（http://www.defacers-challenge.com）において，2003年７月６日（日）に，「改ざんコンテスト」を開催するという情報が文部科学省から通知された．山形大学米沢キャンパスでは，内部のネットワークおよびコンピュータを管理している，山形大学総合情報処理センター米沢分室（以下，米沢分室と記す）が対応した．対応策を考える際，「ホームページの改ざん行為は，世の中では日常的に行われていることであり，特別な対応をする必要はないのではないか」という声もあったが，文部科学省本省から正式な対応依頼があったこともあり，手抜きをせずに対応を行った．この，改ざんコンテストは，ＷＥＢサイトを攻撃しトップページをのっとって別のものにしてしまうもので，改ざんしたページの数により勝敗を決めようとするものであった．

２　経　緯

・７月３日（木）14時50分頃，文部科学省から「ホームページ等に係る不正アクセス行為等の可能性に関する情報について」と題した事務連絡が届いた．資料１にその全文を示す．
・直ちに米沢分室所属の職員および米沢キャンパスの評議員（２名）で対応策の検討を行った．
・７月４日，キャンパス内へのアナウンスを行った．基本的に紙ベースで行い，e-mail は補助手段とした．通知文書の全文を資料２に示す．
・改ざんまでに時間があったため，WEB サーバーへのパッチ等の作業を行った．
・当日の７月６日（日）は出勤し，ネットワークの監視を行った．
・７月７日（月）正午に放送を用いてキャンパス内の警戒態勢を解除した．また資料３に示した通知文書を教職員に配布し，事情の説明を行った．

3 対応策の検討

米沢分室所属の職員および米沢キャンパスの評議員とで検討を行った内容を以下に示す．

実際のアナウンスの全文は資料2の通りである．

1．情報の信憑性の確認．基本的な情報に誤りがあっては何事も無駄になってしまうので，情報源である文部科学省に電話にて確認を行った．担当官から「業務上必要なサーバー以外は停止し，動かす必要があるものにはパッチをあてるなどをして欲しい」旨を確認した．

2．具体的な対応策を米沢キャンパスの評議員（2名）および総合情報処理センター米沢分室職員で検討した．両評議員に承認を得た対応策は，セキュリティーポリシーに関する部分と，セキュリティーアップのためのサーバ等に対する作業，全ユーザに対する防衛策のアナウンスの3点となった．[2,3,4]

(a) セキュリティーポリシーに関する部分

ⅰ．米沢分室管理の機器は守る．

ⅱ．DMZ0（非武装ゾーン）は特に対処しない．（書類上，何かが起きても設置者の責任に帰するため）．ただし念のため7月7日の昼までは，接続を外してもらう．

ⅲ．DMZ1（公式メールサーバー，公式WEBサーバーのゾーン）は守る．米沢分室管理の計算機は守るが，個人でDMZ1に置いている計算機は個人の責任に帰することとし7月7日の昼までは，接続を外してもらう．

ⅳ．インサイド（ファイアーウォールの内側）はファイアーウォールで守られているので特別な対処はしない．ただし念のため月曜日のお昼までは，接続を外してもらう．

ⅴ．インサイド→DMZ1のパケットを制限する．

(b) サーバ等に対する作業

ⅰ．DNS サーバー[5]，WEBサーバー[6]，メールサーバー[2]は最小限で運用し，最新のパッチを当てる．具体的に行った作業を列記する．

・工学部トップページWEBサーバーのApacheをバージョンアップし，sshデーモンを停止した．

・汎用サーバーのsshデーモンを停止した．

・WEBホスティングサーバーのApacheのバージョンアップを行った．

・上記以外のサーバーについてはssh，sendmailのバージョンが最新のものであるかを確認した．

ⅱ．各サーバ上の必要なデータのバックアップを取る．

ⅲ．インサイド→DMZ1のパケットのアクセスを制限するように機器を設定する．[7]

ⅳ．7月5日にファイアーウォールの電源を切り，再起動する．これはファイアーウォール上にキャッシュされたコネクション情報を一度すべて忘れさせ，ほんの少しでもリスクを減少させるためである．[8]

(c) 全ユーザに対する防衛策のアナウンス

ⅰ．資料2示す文書を紙およびメールにて配布する．この文書では，「不正アクセスであること」は明記せずぼかした形にした．この理由は，攻撃を仕掛けてくるクラッカー（攻撃者）たちは，アナウンスした時点ですでにどこかにバックドアを仕込むための仕掛けを用意していると思われるためである．正確な情報を伝えた場合，ユーザーが興味本位でこれらの仕掛け・罠にアクセスしてしまい，バックドアを仕込まれる可能性が高い．あらかじめ攻撃者が情報を流しておくということ自体，この種類の効果を狙っていると考えられる．個人レベルでのセキュリティの甘さ，人間をいかに騙すか，が攻撃者の腕の見せ所だとも考えられる．このリスクを犯してまで正確な情報を提示するのは危険であると考え，ぼかした形で伝えることとした．

ⅱ．米沢分室が管理する計算機以外のすべての計算機を学内ネットワークに接続することを7月5日（土）の夕方から7月7

日12:30まで禁止する．

iii. 接続禁止期間中の連絡はEmail の使用は不可能であるので，電話を利用することを明記する．

iv. ７月７日12:30までにクラッキングされずにすんだ場合には，放送を用いて接続禁止令の解除をアナウンスする．クラッキングされた場合には，７月７日12:30の時点でテストに問題が発生した旨，館内放送などでアナウンスし，対応が終了ししだい，館内放送で学内ネットワーク接続禁止令の解除をアナウンスする．

v. 学内ネットワーク接続禁止令が解除されてからのアクセス状況を監視し，あらかじめ仕込まれていたかもしれないバックドアなどの動作による攻撃状況をモニターする．実際にはインサイドからのバックドアによる攻撃が一番怖い．

4　改ざんコンテスト当日の対応及びログの解析

当初，改ざんコンテントは７月６日に始まり，６時間行われる予定という情報のみであったので，おそらく米国時間の７月６日であろうと推測し，７月６日13時に出勤し攻撃のモニターを開始した．攻撃対象がＷＥＢサーバーであったので，主にファイアウォールおよびＷＥＢサーバーのログをモニターすることにした．

4．1　当日の対応

７月６日14時30分頃　http://www.defacers-challenge.com のページでコンテストの時間帯がエストニア時刻の９時から24時であることを確認した．ＪＳＴでは７月６日（日）15時から７月７日（月）６時の間である（サマータイム）．もともと非合法な行動をとる人たちであるのであくまでも目安の時間である．

4．2　攻撃の様子

ファイアーウォールのログから攻撃の様子を解析した．表１に攻撃を受けた主なポートを示す．一番多かったのは17300ポートに対する攻撃で，これはkuan2と呼ばれるWindows上で活動するトロイの木馬型ワームが使用するポートである．このほか，httpサービスの80番ポートはもちろんであるが，137，139などWindows特有のポートが多く攻撃された．攻撃のピーク時には毎秒250件以上の不正アクセスがあった．攻撃は米沢キャンパス内のほぼ全てのアドレスに対して行われたが，特にWINSサーバーが狙い撃ちされていた．この原因は不明であるがWINSサーバの情報がクライアント経由で外部に流れている可能性が考えられる．また，米沢キャンパスにあるDNSサーバー，ＷＥＢサーバー，メールサーバーを狙った明確な攻撃は特に観察されなかった．

表１：攻撃を受けた主なポート．

番号	サービス	内　容	割合(%)
17300		Win32 ワーム(kuan2)	28.55
137	netbios-ns	NETBIOS Name Service	19.86
80	http	World Wide Web	16.14
445	microsoft-ds	Microsoft-DS	16.03
139	netbios-ssn	NETBIOS Name Service	5.32
21	ftp	ftp service	3.49
25	smtp	SMTP service	3.44
1434	ms-sql-m	Microsoft-SQL-Monitor	0.97
53	domain	Domain Name Service	0.56

4．3　接続禁止処置の解除

一晩監視を続けたのち，米沢分室管理の機器の安全を確認し，不正アクセスの件数が減ってきたことを確認した．一般ユーザへのアナウンスは，３・４校時終了のチャイムを待って12時３分頃，接続禁止解除のアナウンスを放送で流した．解除前にネットワークに接続しても良いかと問い合わせがあった教職員は7 名であった．資料3 に教職員に配布した「ご協力のお礼」の全文を示す．この文書中で経過を正しく伝えた．

図１に７月５日（土）20時頃から７月７日（月）４時頃の間の米沢・小白川間の通信量を示す．学内ネットワークへの接続禁止処置のお願いが功を奏して通信量が激減した．

図２に７月７日（日）８時頃（右端）から７月８日（月）16時頃（左端）の間の米沢キャンパスの通信量を示す．接続禁止処置解除を行った７月８日（月）12時頃から急速に通信量が増加している．

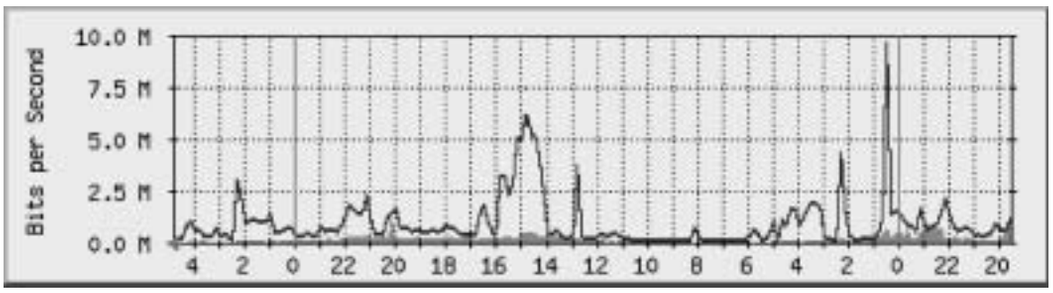

図１：７月５日（土）20時頃(右端）から７月７日（月）４時頃（左端）の間の米沢キャンパスの通信量（５分間平均）．線：米沢キャンパスに入ってくるトラフィック．塗りつぶし：米沢キャンパスから出ていくトラフィック．

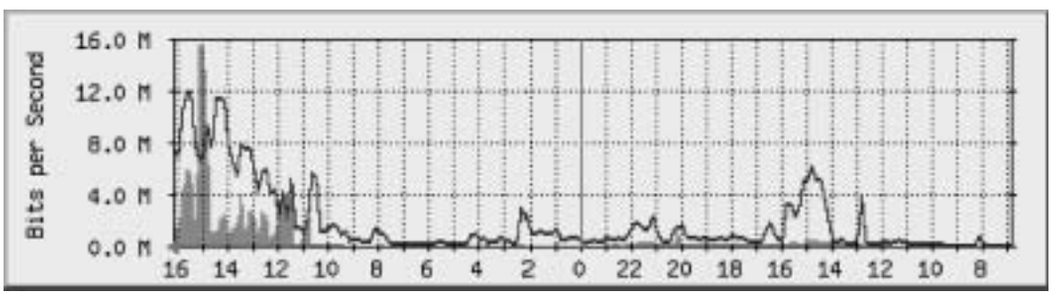

図２：７月７日（日）８時頃(右端）から７月８日（月）16時頃（左端）の間の米沢キャンパスの通信量（５分間平均）．線：米沢キャンパスに入ってくるトラフィック．塗りつぶし：米沢キャンパスから出ていくトラフィック．

5 まとめ

幸い今回の攻撃に対しては被害もなく無事運用することができた．日常的に各種サーバの維持管理をすることが肝要であろう．またこれからますます重要になるであろう，ネットワークに関する緊急対応に関して有用な情報収集を行うことができた．

6 参考文献

1）奥山澄雄，鈴木勝人，伊藤智博，仁科辰夫，青木和恵:“The Defacers Challenge に対する山形大学米沢キャンパスでの対応”，学術情報処理研究，vol.7（2003）65．

2）M．Kaeo:“ネットワークセキュリティ設計ガイド”，（ソフトバンクパブリッシング，東京，2000）．

3）久米原栄:“TCP/IPセキュリティ”，（ソフトバンクパブリッシング，東京，2000）．

4）白井雄一郎，白濱直哉，又江原恭彦，柳岡裕美:“不正アクセスの手法と防御”，（ソフトバンクパブリッシング，東京，2001）．

5）P．Albitz，and C．Liu:“DNS & Bind”，（オライリー・ジャパン，東京，2002）．

6）秋本らいむ，寺尾英作:“Apache-WWW サーバーの構築と管理”，（ソフトバンクパブリッシング，東京，2002）．

7）Allan Leinwand:“Cisco ルータ設定ガイド”，（ソフトバンク，東京，1998）．

8）D．W．Chapman Jr.，and A．Fox:“Cisco PIX Firewall 実装ガイド”，（ソフトバンクパブリッシング，東京，2003）．

事務連絡
平成15年７月３日

各関係機関情報セキュリティ担当者殿

文部科学省大臣官房政策課情報化推進室

ホームページ等に係る不正アクセス行為等の可能性に関する情報について

内閣官房情報セキュリティ対策推進室より，海外のサイト（http:/ww.defacers-challenge.com）において，「改ざんコンテスト」を本年７月６日に開催する旨の記載がなされているとの情報提供がありました。各関係機関におかれましては，各種サーバ等の情報セキュリティの確保に遺漏の無いよう，至急対応方よろしくお願いします。なお，関係すると思われる事案が発生した場合には当室への報告方，よろしくお願いいたします。

文部科学省大臣官房政策課情報化推進室
情報システム第二係
電話番号03-xxxx-xxxx(内線xxxx)
電子メール＊＊＊＊＊@mext.go.jp

資　料：１

－YUnetへの接続禁止処置への協力のお願い－

工学部全教職員ならびに学生各位

総合情報処理センター米沢分室長の仁科です。皆様には、常日頃から総合情報処理センターの活動にご協力いただき、ありがとうございます。さて、急な話で申し訳ございませんが、皆様へのアナウンスと協力のお願いがございます。本日も８号館のノード装置のスイッチが故障し、ネットワークの運用に支障をきたしましたことをお詫び申し上げます。加えて、昨今では情報セキュリティーを固める必要性がますます増加し、ネットワークの運用自体も厳しさを増しております。このような情勢に鑑み、以下に示します日程で、山形大学の学内情報ネットワークであるYUnetの安定運用と総合情報処理センターが管理するサーバ群の高度なセキュリティーチェックを執り行うことが決まりました。これは、独法化に向けた情報セキュリティーポリシーの制定にも関連し、今後の山形大学の未来を担うネットワーク関連の運用・管理技術のチェックと評価を目的とするものです。この運用試験・評価は、センターが管理する計算機に対して、高度なセキュリティーチェックを行うものであり、チェックテストに伴い、YUnetに接続されている計算機のデータ等が紛失・破壊される恐れがあります。つきましては、この期間中は、YUnetへの皆様の計算機の接続をすべて禁止することとなりました。このセキュリティーチェックは、メールやウェブアクセスをはじめとする広範なチェックであり、作業終了の通知をネットワークを利用して行うことができません。このため、作業が終わりしだい、館内放送などで接続禁止処置の解除をアナウンスいたしますが、それまでは皆様の計算機をYUnetから外して下さいますようお願い申し上げます。

記

日　時：７月５日夕刻から来週初めの７月７日月曜日12:30のお昼時まで（予定）館内放送などで接続禁止処置解除のアナウンスがあるまで

目　的：YUnetの安定運用に関する調査試験・評価と、総合情報処理センターが管理するサーバ群の高度

なセキュリティーチェック・評価のため
対　象：全ての計算機・プリンターなどの機器（ＤＭＺ０～インサイドまでの各階層における全て）総合情報処理センターが管理する機器を除く
処　置：YUnetへの接続を禁止する個々の機器のネットワークカードへの接続を外しても良いが、各部屋にある情報コンセントへの接続を外すことを推奨
終了時のアナウンス：館内放送によるアナウンス
業務遂行上の連絡方法：電話による連絡、あるいは携帯電話のメールを推奨する
注意１：本調査試験・評価の過程において、皆様の計算機がYUnetに接続されていたために発生するかもしれないトラブルに関して、総合情報処理センターでは一切の責任を負いません
注意２：計算機上のデータのバックアップは、作業開始までに各自で完了しておくこと
注意３：学生への周知徹底もお願いします（各指導教官の義務と責任です）
注意４：本件に関するお問い合わせは総合情報処理センターまで電話にてお願いします
注意５：この文書のコピー、再配布、転送を禁止します

以上

資　料：２

－「YUnet への接続禁止処置」ご協力のお礼－

工学部全教職員ならびに学生各位

総合情報処理センター米沢分室長の仁科です。皆様には、常日頃から総合情報処理センターの活動にご協力いただき、ありがとうございます。７月５日（土）夕刻から７月７日（月）12時頃まで行われた「セキュリティーチェック」は無事終了いたしました．すでにご存知の方もいらっしゃるかと思いますが，このチェックは事前にもたらされた不正アクセス情報に対応するためのものでした．ピーク時には毎秒250件以上の不正アクセスがありましたが，米沢地区は皆様のご協力により，いまのところ無事であるようです．他大学では不測の事態に備えるため，公式なサーバーを停止したところも少なくありませんでした．経過の詳細については下記の通りですが，今後も同様な事態があると考えられますので，ご協力をお願いする次第です．

経　過

１．７月３日，文部科学省大臣官房政策課情報化推進室から「ホームページ等に係る不正アクセス行為等の可能性に関する情報」がメールで配信された．
２．情報が真のものであるかどうか，文部科学省に電話にて確認．担当官から「業務上必要なサーバー以外は停止し，動かす必要があるものにはパッチをあてるなどをして欲しい」旨を確認．
３．大場・東山両評議員および総合情報処理センター米沢分室職員で対応を検討し，先のアナウンスを流すことに決定．
４．アナウンスの書式については，皆さんが罠(改ざんされたホームページにおかれたトロイの木馬など)にかからないようにするため，ぼかした形で行うよう配慮した．
５．不正アクセスに対処するためにサーバーへのパッチの適用や，ネットワーク設定の見直しを行った．
６．不正アクセスが広範に行われるとされた７月６～７日は米沢分室職員がネットワークを監視し，不測の事態に備えた．

以上

資　料：３