“The Defacers Challenge” に対する山形大学米沢キャンパスでの対応

Countermeasures for “The Defacers Challenge” at Yamagata university Yonezawa campus

奥山澄雄 7，鈴木勝人, 伊藤智博, 仁科辰夫, 青木和恵
Sumio Okuyama, Katsuto 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

概要

2003 年 7 月 3 日，“The Defacers Challenge” なる，いわゆる「クラッカー」による WEB ページ改ざんコンテストがあるとの情報提供があり，文部科学省本省から対策するようにとの通達があった．これに対応するため，山形大学米沢キャンパスではキャンパス内へのアナウンス・ネットワーク使用の縮小・サーバーへのパッチの適用・ネットワークの監視等の対策を行った．さいわい，“The Defacers Challenge” による被害はなく終了した．

キーワード

The defacers challenge，ホームページ改ざん

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・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．
- 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) で対応策を検討を行った．
- 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．
- 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．

3 対応策の検討

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．

（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, WEB サーバー, メールサーバーは最小限で運用し，最新のパッチを当てる．
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．
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．

（c）全ユーザに対する防衛策のアナウンス

i. 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．
ii. 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．
iii. 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．
iv. 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．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．

表 1: 攻撃を受けた主なポート．

番 号	プロトコル	サービス	内 容
53	tcp/udp	domain	Domain Name Service
80	tcp/udp	http	World Wide Web
137	tcp/udp	netbios-ns	NETBIOS Name Service
139	tcp/udp	netbios-ns	NETBIOS Name Service
445	tcp/udp	microsoft-ds	Microsoft-DS
1434	tcp/udp	ms-sql-m	Microsoft-SQL-Monitor
2425			IP message

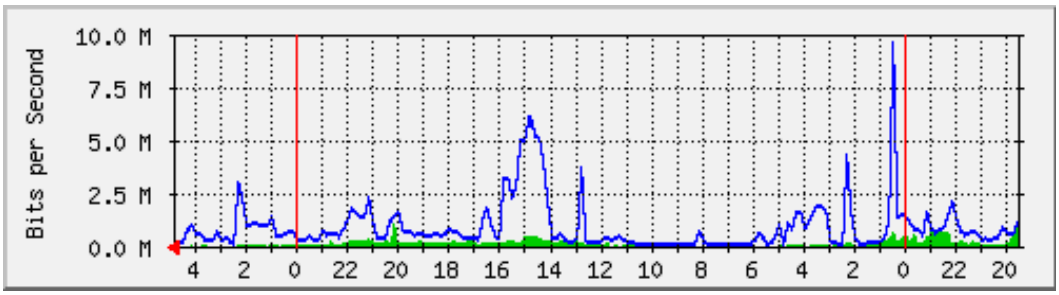

図 1: 7 月 5 日 (土)20 時頃 (右端) から 7 月 7 日 (月)4 時頃 (左端) の間の米沢キャンパスの通信量 (5 分間平均)．線: 米沢キャンパスに入ってくるトラフィック．塗りつぶし: 米沢キャンパスから出ていくトラフィック．

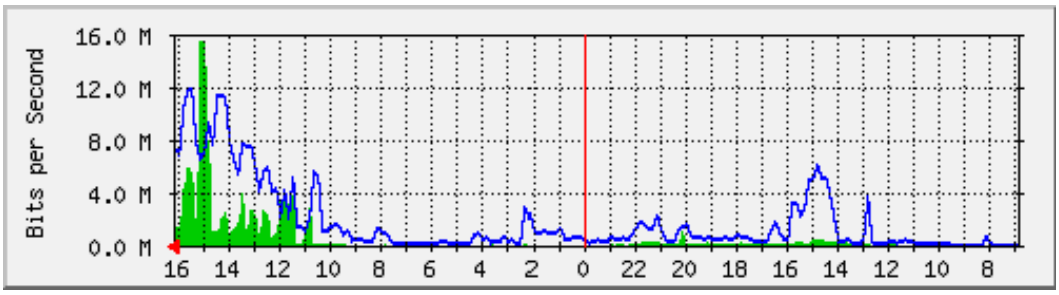

図 2: 7 月 7 日 (日)8 時頃 (右端) から 7 月 8 日 (月)16 時頃 (左端) の間の米沢キャンパスの通信量 (5 分間平均)．線: 米沢キャンパスに入ってくるトラフィック．塗りつぶし: 米沢キャンパスから出ていくトラフィック．

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．

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．.

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．