The Defacers Challenge

山形大学工学部技術部
総合情報処理センター米沢分室　鈴木　勝人

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、文部科学省から対策するようにとの連絡があった。これに対応するため工学部内へのアナウンス・ネットワーク使用の縮小・サーバーへのパッチの適用・ネットワーク監視等の対策を行った。幸い攻撃による被害はなく終了した。

1　はじめに

2003年7月3日､海外のサイトにおいて､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。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、文部科学省から正式な対応依頼があったこともあり、手抜き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。
・直ちに分室所属職員及び工学部の評議員(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。
・コンテストまでに時間があったため、Webサーバ等へのパッチ等の作業を行った。
・コンテスト当日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

3-1　情報の信憑性の確認

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。

3-2　具体的な対応策

工学部の評議員（2名）および分室職員で検討。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。

（1）セキュリティーポリシーに関する部分
　ⅰ）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。設置している個人の責任に帰する。ただし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、公式 Web サーバのゾーン）は守る。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7月7日の昼までは、接続を外してもらう。

v）インサイド → DMZ1 のパケットのアクセスを制限する。

（2）サーバ等に対する作業

ⅰ）DNS サーバ、Web サーバ、メールサーバは最小限で運用し、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設定。

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。

（3）全ユーザに対する防衛策のアナウンス

ⅰ）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日（月）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、放送でアナウンスし、対応が終了ししだい、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

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。攻撃対象が Web server であったので、主にファイアウォールおよび Web サーバ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、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。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）。非合法な行動をとる人種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

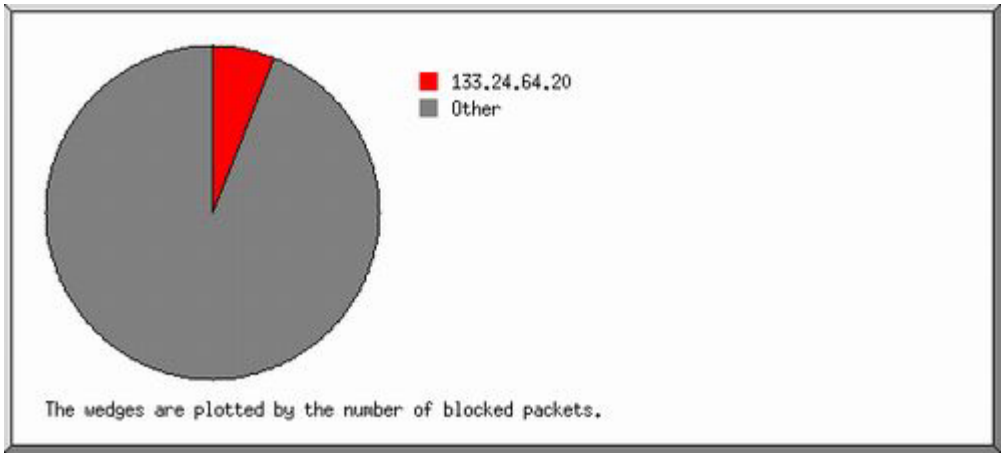
ファイアーウォールのログから攻撃の様子を解析した。表１に攻撃を受けた主なポートを示す。http サービスの 80 番ポートはもちろんであるが、137、139 など Windows 特有のポートが多く攻撃

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。
攻撃はキャンパス内ほぼ全てのアドレスに対して行われたが、特に WINS サーバ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 Serve
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	Micrfosoft-SQL-Monitor
2425			IP message

グラフ１：攻撃先



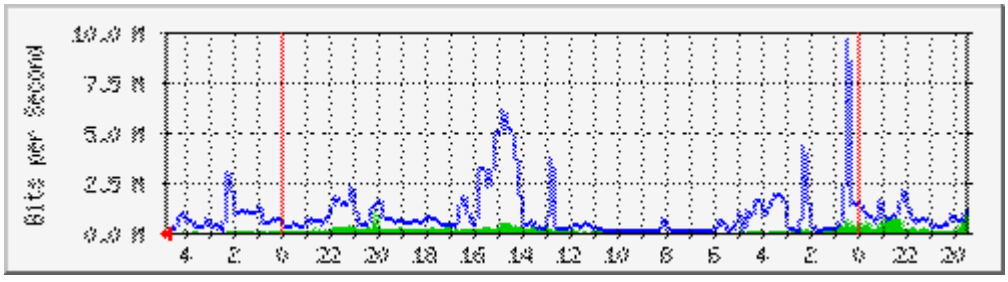


図１：7 月 5 日（土）20 時頃（右端）から 7 月 7 日（月）4 時頃（左端）の間の米沢キャンパスの通信量（5 分間平均）。線：米沢キャンパスに入ってくるトラフィック。塗りつぶし：米沢キャンパスから出ていくトラフィック。

4-3　接続禁止処置の解除

一晩監視を続け、センター管理の機器の安全も確認し、不正アクセスの件数も減ってきたのを監視しながら一般ユーザへのアナウンスのタイミングを計り、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。

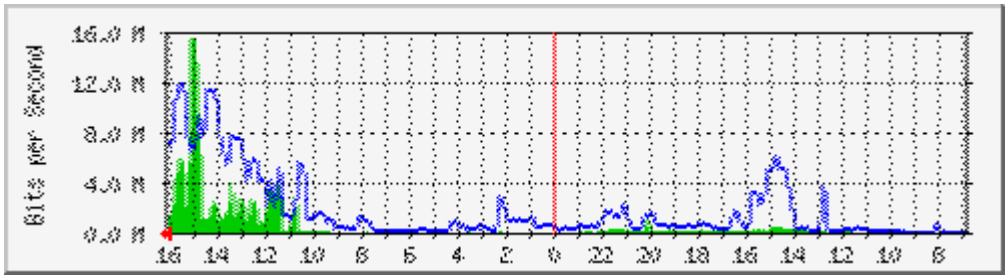


図２：7 月 7 日（日）8 時頃（右端）から 7 月 8 日（月）16 時頃（左端）の間の米沢キャンパスの通信量（5 分間平均)。線：米沢キャンパスに入ってくるトラフィック。塗りつぶし：米沢キャンパスから出ていくトラフィック。

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。