ネットワーク管理支援ツールの紹介と不正アクセスの現状について

笠原, 義晃
九州大学情報基盤センター

https://doi.org/10.15017/1470491

出版情報：九州大学情報基盤センター広報 : 学内共同利用版. 1 (2), pp.59-68, 2001-10. 九州大学情報基盤センター
バージョン：
権利関係：

ネットワーク管理支援ツールの紹介と不正アクセスの現状について

笠原 義晃*

今年度の初めに，学内ネットワークの管理支援機器として，情報基盤センターに「Kinnetics」と「Dragon IDS」という二つの機器が導入されました。この項では，この二つの機器がどういう機能を持ち，またどういった役に立つかについて解説します。また，「Dragon IDS」の運用を通して明らかになってきた，学内ネットワークを取り巻く不正アクセスの現状について，いくつかの例を通して見て行きます。

1 Kinnetics

「Kinnetics[1]」は，ハード/ソフト一体型のネットワーク管理支援システムです。米国 Peregrine Systems 社[2]が開発し，日本ではダイキン工業 (株)[3]などが販売しています。ネットワーク地図を自動生成し，各ネットワーク機器の状態やネットワークの利用率などを収集・報告する装置です。

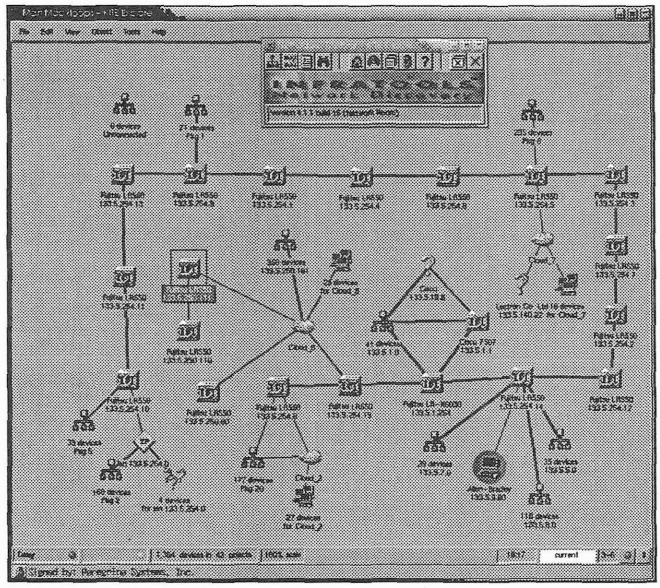

図 1: Kinnetics によるネットワーク地図

*九州大学情報基盤センター
E-mail : kasahara@nc.kyushu-u.ac.jp
[1]2001 年 10 月から商品名が IND(IntraTools Network Discovery) に変更されます。
[2]http://www.peregrine.com/
[3]http://www.comtec.daikin.co.jp/

九州大学の学内ネットワークのような大規模なネットワークを管理する場合，まずネットワーク機器の多さとその接続の複雑さが問題になります。ネットワークの構成図を作成するだけでも大変です。通常は手作業でネットワーク図を描いたりするわけですが，各機器の設定を確認しつつ作らなければならず，非常に手間がかかります。しかし「Kinnetics」を使うと指定したネットワークの機器を走査し，図1のように自動的にネットワーク地図を作成してくれます[4]。ルータやスイッチングハブのような重要な機器以外の端末は自動的にまとめて表示されるため，見通しのよい地図になっています。もちろん，まとめられている部分も必要に応じて展開表示する事ができます。

また，「Kinnetics」は定期的に各機器から情報を収集しており，ネットワーク過負荷や機器の停止などのさまざまな管理項目について，ネットワーク地図上に状況を表示する事が可能です。例えば，過負荷な経路を赤い線で表示したり，停止した機器を赤い丸で囲んだりしてくれます。これにより，ネットワークの状況が一目瞭然となり，何かトラブルが発生した場合にも迅速に対応が可能になります。各機器のネットワークインターフェイスを通過したトラフィックやパケット数なども記録されており，図2のように表示する事ができます。利用者からネットワークの不調を訴えられた時などに，過去に遡って流量の記録を調べる事が可能です。

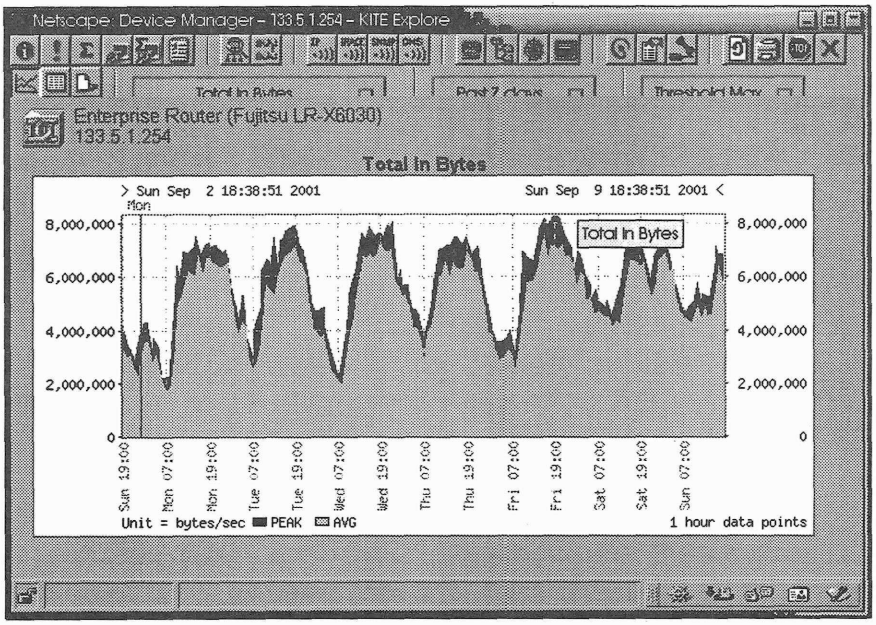

図 2: 箱崎 FDDI ループ出口ルータを通過したトラフィック総量のグラフ

[4]ただし，機器の配置は手で調整する必要があります。

「Kinnetics」は多くのネットワーク機器が対応している業界標準のSNMP[5]というプロトコルでほとんどの管理情報を集めるようになっており，使用しているネットワーク機器のメーカーを選びません。基本的には管理したいアドレスの範囲を指定するだけで，あとは全自動で情報を収集してくれます。本学のネットワークでも，使用している機器は1つの企業の物に統一されているわけではありませんから，この点は非常に重要と言えます。SNMPに応答しないようなハブがあっても，自動的に周辺の情報からネットワーク構成を推測して図にしてくれます[6]。

ユーザインターフェイスはJavaを活用したウェブブラウザベースで，特別なツールを必要としないのも特徴です。一般の利用者に公開しているわけではありませんが，管理者としても通常のブラウザがあれば使えるというのは非常に助かります。

現在は，情報基盤センター内に設置されている機器，および箱崎キャンパス内のFDDIバックボーンの機器を監視対象として運用しています。状況に応じて，問題のあるネットワークの詳細な調査を行う際などには監視範囲を拡大して運用する予定です。ギガビット級ネットワークが導入されるとさらに機器が増えますので，「Kinnetics」の活躍する場面も増えてくるものと思います。

2 Dragon IDS

「IDS」とは，Intrusion Detection System，すなわち侵入検知装置のことです。大別して，サーバにインストールしてファイルの改竄やログファイルの内容を監視する物(ホスト型)と，ネットワークに接続してトラフィックを監視し，ネットワークを経由しての不正使用等を検知する物(ネットワーク型)があります。

「Dragon IDS」は，Enterasys Networks社[7]が開発し，日本ではInternational Network Security Inc. 社[8]等が販売しているIDSです。ホスト型の「Dragon Squire」，ネットワーク型「Dragon Sensor」，そして統合管理用サーバ「Dragon Server」で構成されます。九州大学では2001年4月に，学内ネットワークから外部に出ていく部分のネットワークにネットワーク型の「Dragon Sensor」を設置しました。

ネットワーク型侵入検知の原理は，ネットワークを流れるトラフィックの中から，サーバへの攻撃や不正利用に含まれる特定のパターン(文字列など)を検索して拾い上げるという物です。図3に簡単な例を示します。この図ではphfというCGIスクリプトを攻撃する通信がIDSで検出されています。ウェブサーバに対してのパケットの中に「`GET /cgi-bin/phf`」という文字列が含まれているかどうかを調べる事により，攻撃を受けている事がわかります[9]。どのような規則でパケットを検索するかを記述した物を「シグニチャ」と呼びます。IDSにおける攻撃検知能力はシグニチャに

[5]Simple Network Management Protocol
[6]ハブが接続されている上位の機器がSNMPに応答するハブやルータである必要があります。
[7]`http://www.enterasys.com/`
[8]`http://www.insi.co.jp/`
[9]成功したかどうかは，この例だけではわかりません。

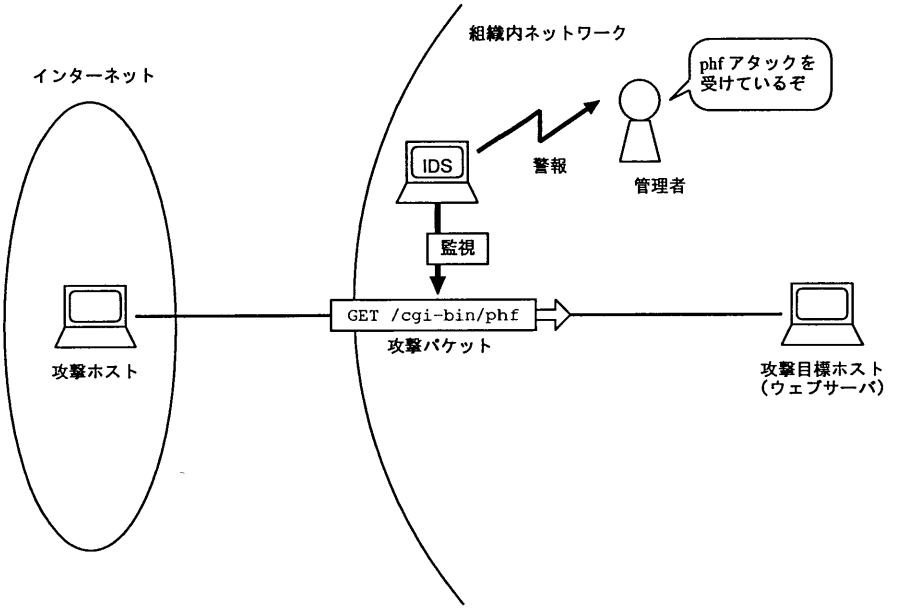

図 3: IDS の動作原理

かなり左右されます。「Dragon IDS」は，開発元から 1,200 種類を越える豊富なシグニチャが提供されており，攻撃やさまざまな不正使用の検出に利用できます。開発元が積極的に新しいシグニチャを公開しており，更新されたシグニチャを毎日チェックして自動でダウンロードする機能があるため，新しい攻撃にも迅速に対応できます。シグニチャの書式が公開されており，ユーザ側で自由に修正・追加ができるため，柔軟に運用できるのも特徴です。また，高速な動作も売りで，200Mbps の通信でもほとんどデータを取りこぼすことなくチェックする事が可能とのことです。

「Dragon IDS」を導入した事により，外部から学内のホストへの攻撃や侵入を迅速に発見する事が可能になりました。例えば，CodeRed による攻撃の跡は図 4 のように見る事ができます。この図の [IIS:IDA-ISAPI-OVERFLOW] というのがシグニチャの名前で，Microsoft Internet Information Service というサーバソフトウェアに含まれる ida.dll に存在するバッファオーバーフローに対する攻撃を発見するシグニチャです。この図では，外から中への攻撃は記録されていますが中から外への攻撃が記録されていないため，学内に感染ホストが無いらしい事がわかります。

IDS の仕組み上，IDS の出力結果を見て人間が解釈しないと侵入かどうか判断できない事が多いため，自動的に管理者のみなさんに連絡をするという事は難しいのですが，それでも IDS が無かった時に比べて格段に状況が把握できるようになりました。学内から学外への攻撃も検出しますので，学内に既に侵入を受けたホストがあって，

外部に攻撃をしている物も発見できます。なお，学内で攻撃ツールらしき物を動かすとまる見えですので，そのような行動は謹しんでいただきますよう，よろしくお願いします。

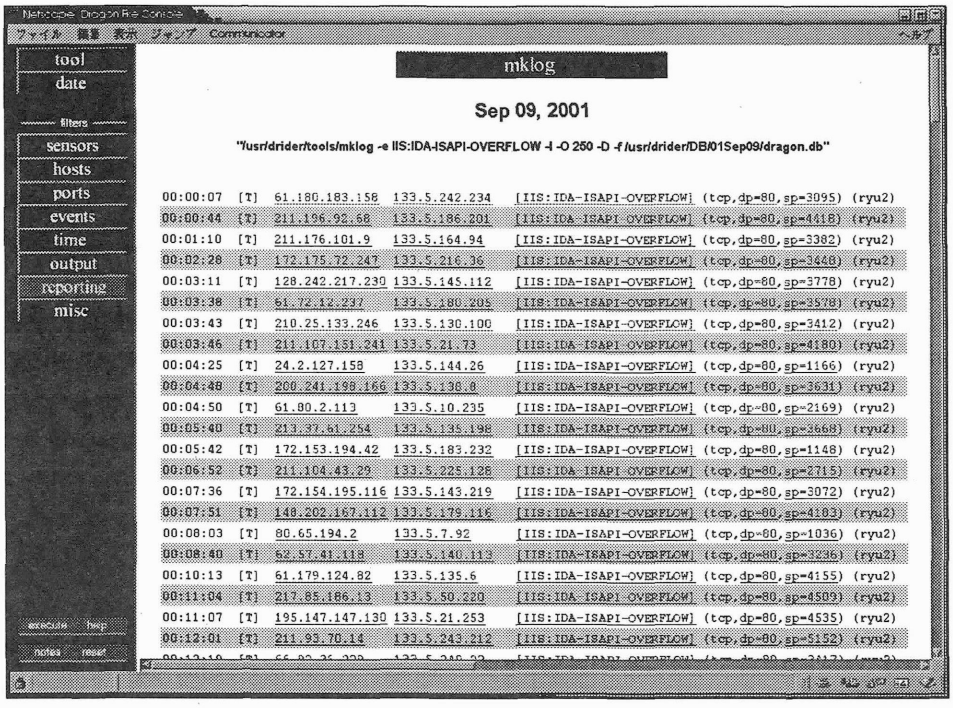

図 4: CodeRed による外部からの攻撃パケット記録

3 学内ネットワークを取りまく不正アクセスの現状

この節では,「Dragon IDS」によって検出・記録された情報を調査する事によりわかってきたネットワークにおける不正アクセスの現状について，いくつか例を挙げて報告します。

3.1 ホスト走査

ある組織のネットワークを攻撃目標とする場合，通常まずそのネットワークのどのIPアドレスでどのようなサーバが動いているかを知る必要があります。このような目的で行なわれるのが，いわゆるポートスキャンと呼ばれるものです。目標とするネットワークやホストに対してポートスキャンをかける事によって，攻撃の足がかりを探すのです。

一般にポートスキャンと言う場合，実際には二つの異なる種類の走査 (スキャン) を合わせて指している事があります。図 5 に模式図を示します。まず，ある特定のホストについて，どのポートが開いているかを調べる走査があります。ここではこれを「ポート走査」と呼ぶ事にします。特定の IP アドレスに対し，例えばポート番号の 1 番から 15,000 番までに順に接続要求を出す，というような物です。たいていの場合，ポート番号とサービスは 23 が telnet，25 が smtp(メールサーバ) といった具合に一対一に対応しているため，ポート走査によってそのサーバが何をサービスしているかがわかるというわけです。特定のホストを攻撃対象にしたい場合に足掛かりを探す場合などに使われます。

これに対して，特定のポート番号について，あるネットワークに含まれる個々の IP アドレスに接続要求を出す走査があります。ここではこれを「ホスト走査」と呼ぶ事にします。例えば，telnet で接続可能なホストを探すために，相手の IP アドレスを変えていって 23 番ポートに接続要求を出してみるわけです。これによって，あるサービスに対する攻撃手段を知っている時に，どこでもいいからその攻撃ができそうなホストを見つける事ができます。相手がどこでも構わないような，無差別な攻撃などで使われます。

「Dragon IDS」には，このような走査をある程度検出する機能があります。「ある程度」というのは，感度を上げると本当は走査でない通常の通信を走査と誤認識して意味のない出力が増えてしまい，そうならないように感度を下げると今度は非常にゆっくりした走査を検知できないという問題があるからです。とは言え，誤認識が起こらない程度に調整した IDS でも相当の走査が検出されています。九大では，特にホスト走査を非常に多く受けている事が，IDS の出力からわかっています。

図 6 は，2001 年 5 月頭から 7 月末にかけて，九大のネットワークが受けたホスト

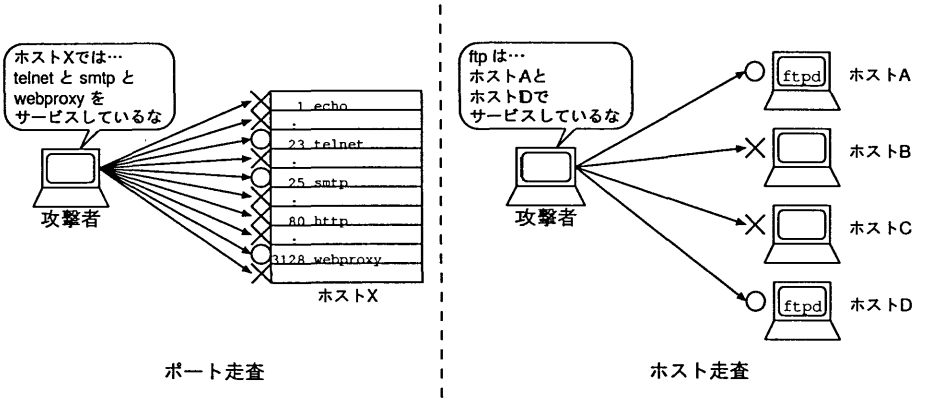

図 5: ポート走査とホスト走査

走査を集計したグラフです。折線は左の数値，+印は右の数値を読んでください。折線は，ある1日にホスト走査の対象となった，九大内のIPアドレスののべ総数を示しています。+印は，ある1日にホスト走査をかけてきた，異なる送信IPアドレスの総数です。全くホスト走査を受けていない日もありますが，多い日にはのべ70万アドレスを越える範囲が走査されている事がわかります。全体で平均を取ると，だいたい毎日4台の異なる相手から，のべ20万アドレスが走査されている事になります。

九大のネットワークは，だいたい6万強のアドレス空間を持っています。ホスト走査は使われていないIPアドレスにも来ますので，大雑把に言って全てのホストが毎日3回，なんらかのポートをチェックされているという計算になります。ちなみに，よく調べられているポートは多い物から順に，21(FTP)・53(DNS)・111(RPC)・25(SMTP)・80(HTTP)でした。これらのサービスはかなりの頻度で外から走査されている事になり，穴があるとすぐに悪用される可能性があります。

これらのサービスはRPCを除いて学外から通信できる必要のあるサービスであるため，今の所九大の入口で通信を遮断する事ができません[10]。したがって，これらのサービスは特に，不要なら動かさないこと，必要ならセキュリティ対策をしっかりすることが重要です。

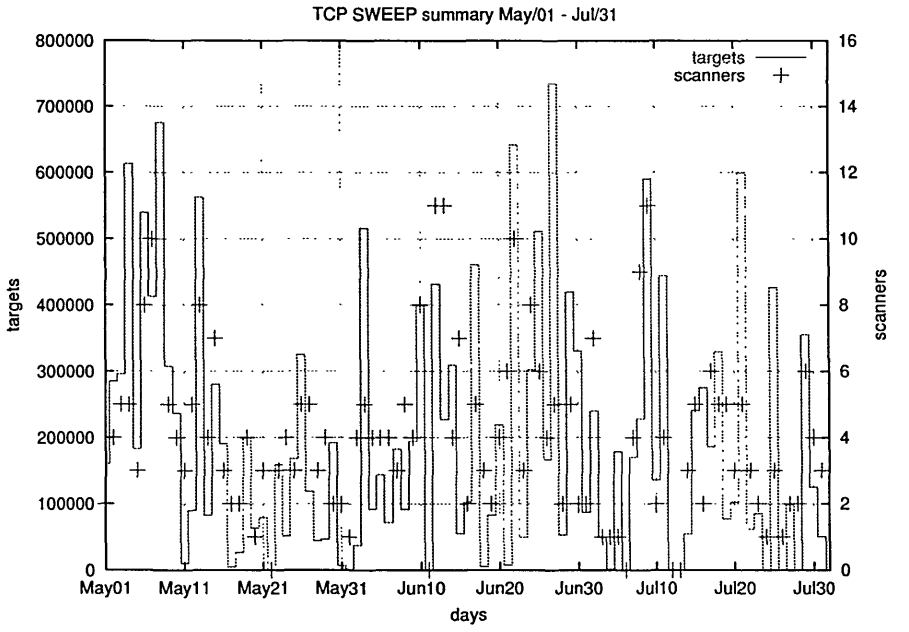

図 6: ホスト走査ののべ総数と走査元ホスト

[10]RPCのポートは入口で落としているため，スキャンはできても通信はできないようになっています。

3.2 CodeRed

最近世間を騒がせている CodeRed というワーム，御存知の方も多いかと思います。このワームは Windows NT/2000 で動作する Microsoft IIS(Internet Information Service) というサーバソフトに存在するセキュリティホールを利用して，ネットワークを介して自分のコピーを他のホストに伝染させ，増殖するワームです。もう少し具体的に言うと，IIS のウェブサーバに含まれる，Indexing Service という機能に存在するセキュリティホールを利用します。ただし，Indexing Service を動かしているかどうかには関係なく，セキュリティホールを修正するパッチを当てていないと感染する可能性があります。

Windows 2000 では Professional 版にもこの IIS が付属しており，知らずにインストールしてワームに感染してしまい他に被害を広げている例が多発しています。本人にサーバを動かしている自覚がないため，発見や対処が遅れる原因になっています。

このワームは感染相手の IP アドレスをほぼ無作為に選び，相手が IIS を動かしているかどうかに関係なく接続して感染しようとします。ほとんどの場合それは失敗するわけですが，たまたまセキュリティパッチを当てていない IIS にぶつかると，感染してしまうというわけです。そんな大雑把な事で感染を広げられるのだろうかと思わ

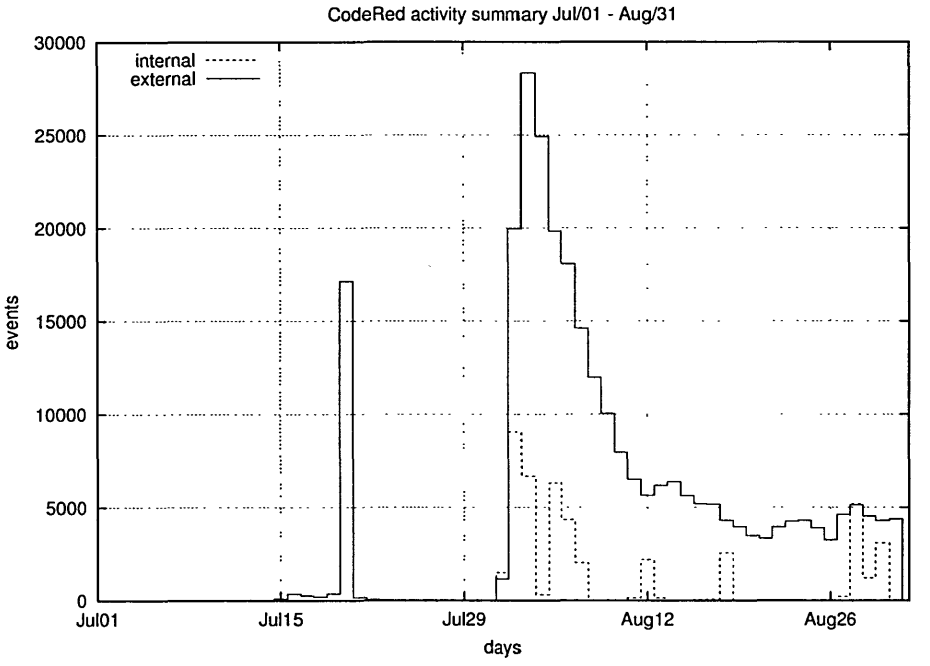

図 7: CodeRed 通信数

れるかもしれませんが，7月19日の大流行の時には，一説では世界中で9時間に25万台のIISが感染したと言われています。このワームが利用するセキュリティホールは1ヶ月も前にパッチが提供されていたにもかかわらず，ワームが非常に速い速度で拡散するのに十分な数だけセキュリティパッチを適用していないホストがあったという事です。

「Dragon IDS」のシグニチャの中に，このワームが利用するセキュリティホールへの攻撃パケットを検出する物がありました。このシグニチャはワームの出現前から設定されていたため，CodeRedが最初に出現した時からの攻撃数を調べる事ができました。これを利用して九大内外のCodeRedワーム関連の通信数をグラフにしたのが図7です。

実線は，外部から内部のホストに向けての接続数，点線は，内部から外部のホストに向けての接続数です。すなわち，点線のグラフがある日は九大内にCodeRed感染ホストがあった，という事になります[11]。IDSの活躍により，内部の感染ホストはほとんどその日のうちに発見され，管理者へ連絡されました。しかし，9月に入っても1週間に1台程度の割合で新しい感染ホストが見つかっており，完全に制圧できていません。

7月に流行したオリジナルのCodeRedは，毎月20日になると感染をやめるような作りになっていました。図7を見てもわかるように19日の大攻勢の後急に通信数が減っている事がわかります。本来，CodeRedは一旦感染行動をやめると月が変わっても復活しないのですが，時計が狂っているホストなどによって再感染が起こったため8月になってまた大発生しました。残念ながら7月19日の大流行は教訓として生かされなかったというわけです。また，8月5日前後に，同じセキュリティホールを利用する全く異なるワーム(CodeRed II・CodeRed v3などと呼ばれている)が発生し，さらに事態を悪化させました。新種は20日に停止するようにはなっておらず，また感染したホストのウェブサーバに裏口を作り，後から任意のコマンドを実行できるようにするという悪質な作りになっています。また，攻撃頻度がオリジナルのCodeRedよりかなり高いため，現在ではほとんどの攻撃がCodeRed II由来の物となっています。

このグラフに出ている数値は，実際に何らかの形で80番ポート(HTTP)にサーバが動いているホストに対する通信の数です(IISとは限りません)。実際にウェブサーバへの接続に成功しないと攻撃パケットが来ないため，IDSでCodeRedの攻撃と判定できないからで，実際の接続要求はこの数十倍やってきているはずです。IDSのログ調査から，九大内でCodeRedからのパケットを受けたホスト数(＝ウェブサーバが動いているホスト数)は1,000台強である事がわかっています。つまり，平均すると一番多い日で1台につき約30回/日，8月末でも一日に約5回の攻撃が来ている計算になります。セキュリティパッチを当てていないIISをネットワークにつなぐと，その日のうちに確実に感染してしまうでしょう。

[11] シグニチャの設定により，7月中は学内の感染ホストを検出できていません。

CodeRed ワームについては，Microsoft のページに詳細な情報が掲載されています。http://www.microsoft.com/japan/technet/security/codeptch.asp などを参照の上，対策していただきますようよろしくお願いします。特に Windows 2000 については，サーバにするつもりのない Professional と言えども感染の危険性がありますので，対策を忘れないようにお願いします。

3.3　まとめ

この節では，IDS の記録を元に，ホスト走査と，CodeRed ワームの活動を見てみました。これらの事からわかるように，学内のネットワークにホストを接続するという事は，苛烈な攻撃に身をさらす事になっているのが現状です。CodeRed は Microsoft Windows にしか関係のないワームでしたが，実際には Linux に感染するワーム，Solaris に感染するワーム，手作業で攻撃をしかける人々など，さまざまな方法での攻撃が IDS によって観測されています。

IDS は防犯ブザーや監視カメラと同じで，侵入を発見する事はできますが防ぐ事はできない物です。センターでは，IDS を活用して侵入の早期発見と解決のために今後も活動して行きますが，これにはネットワークの利用者である皆さんの協力が不可欠です。センターから連絡を受けたら，速やかに対策すると共に，同じ問題が起こらないようその他のホストにも対策をしていただきますよう，よろしくお願いします。

侵入事例の 9 割以上は，既知のセキュリティホールを利用した物である事がわかっています。つまり，きちんと対策をしていれば，ほとんどの不正侵入は未然に防げるのです。実際に侵入を受けてしまうと，多大な労力をかけて修復する必要があります。ホスト走査の現状を見てもわかるように，「こんな所まで攻撃には来ないだろう」という予測は全く間違っています。CodeRed のような，感染する事だけを目的に感染するような攻撃ツールがこれからさらに増えてくる事は想像に難くありません。ホストをネットワークにつないだまま放置したりしないよう，十分に御注意願います。

関連情報

CERT/CC
　http://www.cert.org/
JPCERT/CC
　http://www.jpcert.or.jp/
Microsoft TechNet Online
　http://www.microsoft.com/japan/technet/
SecurityFocus
　http://www.securityfocus.com/