논제 부정 Access에 대한 Firewall의 과제와 대책

변성준* · 서정석** · 최원석***

요 약

Firewall은 다양한 부정Access의 방지책으로서 확실히 유효한 수단이지만 이 Firewall은 사용자로부터 지시된 설정을 충실히 실행하는 것으로 설정 오류,소프트웨어의 정지,허가된 룰을 악용한 침입 등 반드시 사용자가 바라는 작용을 무조건적 상태에서 보증해 주는 것은 아니다.따라서 사용자는 도입 후에도 운용시에 Access log를 감시하고 본래의 Security Policy에 반하는 행위를 매일 매일 체크하지 않으면 안될 상황에 처해 있다.

본 연구는 이러한 부정Access에 대한 이와 같은 Firewall의 현상에 대한 과제 중에서 "부정Access를 어떻게 하면 일찍,정확히 체크할 수 있는가?"라는 주제를 선택하여 Firewall의 한계와 그 대응책을 실제로 부정Access를 시험해 보는 것으로 검증하기로 하였다. 실험결과에서 (1)Port Scan이나 전자메일 폭탄(서비스정지공격)등은 Firewall로 방지하는 것은 불가능하거나 혹은 Checking이 곤란하다.(2)공격마다 로그 수집을 했음에도 관계없이 Firewall의 로그는 번잡하므로 단시간에 사태의 발견이 대단히 곤란하다고 하는 Firewall의 한계를 인식하였다.그리고 그 대책으로서 우리는 체크 툴의 유효성에 착안하여 조사한 결과,결국 무엇이 부정Access인가에 대해서는 어디까지나 이용하는 측이 판단하여 Firewall 상에 설정하지 않으면 안되지만 체크 툴은 이 부정Access 정보를 데이터베이스로서 갖고 있음으로써 ' 무엇이 부정Access인가 ' 를 이용자 대신에 판단하고 툴에 따라서는 설정을 자동적으로 변경하여 부정 Access의 저지율을 향상시킨다.이처럼 체크 툴은 Firewall의 수비능력을 보강하는 위치에 있다고 생각할 수 있다.

1. 머리말

현재 인터넷은 급속한 성장을 계속하고 있다.신문 · TV 등 이제까지의 미디어를 통한 정보제공의 신속함과 정보취득의 시기와 장소를 자유로이 선택할 편리성에서 많은 기업이 인터넷 상에 새로운 " 창구 " 를 개설하고 있다.한편,인터넷 이용자 측에서도이 " 창구 " 에 언제라도 어디에서라도 가볍게 access할 수 있으므로 이 편리성이 두개의 날을 가진 칼이 되어 초대하지 않은 손님의 침입을 쉽게 허락하고 있다.

즉, 이 흐름에서 사회적 문제 중 하나로 되어 있는 것이 인터넷 부정Access이다.

인터넷의 세계(사회)에는 실세계(사회)와 같이 그러한 부정을 단속할 기구는 아직 정비되어 있지 않다.인터넷에 입각한 새로운 법률이나 보험 등도 정비되고는 있지만,실제로 인터넷 사회의 확대를 추구하지 않고서 유효한 억지책이란 있을 수 없다.

이러한 상황 하에서 그 편리성을 빨리 도입하고 싶은 기업은 스스로의 책임으로 정보를 지키지 않으면 안 된다.그리고 현재,부정Access대책의 대표적 방지책으로서 먼저 들 수 있는 것이 Firewall이다.

Firewall은 다양한 부정Access의 방지책으로서 확

* IBM

** 나사렛대학교 전산정보학과 조교수

*** 중부대학교 컴퓨터안전관리학과

실히 유효한 수단이며 기업측은 이를 도입함으로써 ' 부정Access 대책완성 ' 으로 잡는 경우도 적지 않다.그러나 이Firewall은 사용자로부터 지시된 설정을 충실히 실행하는 것으로 설정오류,소프트웨어의 정지,허가된 룰을 악용한 침입 등에 대해 반드시 사용자가 바라는 작용을 무조건적 상태에서 보증해 주는 것이 아니다.따라서 사용자는 도입 후에도 운용으로서Access log를 감시하고 본래의 Security Policy에 반하는 행위를 매일 매일 체크하지 않으면 안될 상황에 처해 있다.이러한 운용은 최종적으로 관리할 인재의 Skill에 Security level을 의존하지 않을 수 없다.

본 연구는 이러한 부정Access에 대한 Firewall의 현상 과제를 실제로 부정Access를 실천해 보아 검증하고 그 결과를 토대로 Firewall을 사용한 부정Access대책의 범위와 한계를 확실히 하려는 것이다.

2. 부정 Access란

2.1 부정 Access의 종류

현재 인터넷에 접속되는 단말이 증가함에 따라서 부정Access도 증가하고 있다 간단히 부정Access라 해도 다양한 종류가 존재한다.크게 나누면,다음과 같이 분류 할 수가 있다.

(1) 부정침입 :부정하게 네트웍이나 서버에 로그인하는 경우.

프로그램의 실행,타 사이트에 대한 공격의 발판,기밀정보에 대한 부정 Access 등이 수행된다.

(2)서비스 정지 :DoS(Denial of Service)Attack 이라 부른다.

표적 기기를 정지시키거나 네트웍의 traffic을 증대시키는 등 네트웍의 기능을 마비시킨다.

메일폭탄 등이 있다.

(3) 서비스 방해 :홈페이지 영역 탈취 · 게시판훼손 등 사이트가 제공할 서비스를 정상으로 실행할 수 없게 한다.

(4) 도난 · 도청 :ID 정보 · 패스워드 파일 · 기밀데이터 등을 도난하고 부정열람· 이용한다.

사용자정보의 매매 등이 발생될 경우도 있다.

(5) 파괴/개정 :호스트 내와 네트웍 상의 파일이나 데이터를 파괴 혹은 개정한다.

하드디스크의 파괴 등 두려운 결과를 초래하는 경우도 있다.

2.2 부정 Access의 현상

위와 같이 부정Access에는 다양한 종류 · 수법이 존재한다.99년의 4월~6월에 실제부정Access가 수행되었다고 보고된 건수만 해도 표1과 같이 상당한 건수에 이르고있다.

단,이것은 JPCERT에 보고된 것뿐이므로 실제 부정Access는 이보다 훨씬 많을 것으로 생각된다.

이와 관련하여 JPCERT란,일본 국내 조직 및 사용자에 대해 인터넷을 경유한 시스템 부정침입,파괴,방해 또는 그것을 목적으로 한 부정Access로 그 영향이 광범위하게 미칠 가능성이 있는 것에 대해 피해 접수와 대응,피해의 실태조사,피해상황 · 침입경로 분석,재발 방지를 위한 대책의 검토와 조언 등을 수행하는 단체이다.

표 1.1999년 4월부터 6월 사이의 부정Access 보고건수

부정 Access 사례	건수 (10건이상)
시스템에 존재하는 서비스/약점 탐사(probe.scan)	103건
전자메일의 부정한 중계, 전자메일폭탄 등	35건
시스템에 대한 부정침입 및 관리자 권한 사칭	25건
Mountd 서버를 악용한 공격	19건
네트웍이나 호스트 운용을 방해하려는 공격	10건
Web 서버의 cgi-bin 프로그램을 악용한 공격	
프록시 서버의 부정이용	
POP 서버를 악용한 공격	
Automountd를 악용한 공격	
Anonymous FTP 서비스의 부정이용	
IMAP 서버 프로그램을 악용한 공격	
바이러스, 트로이의 목마	

2.3 부정 Access 대책

일반적으로 인터넷에 접속되어 있는 컴퓨터는 주야로 이러한 위험에 노출되어 있다.

이들의 부정Access 대책으로서 대표적인 것을 표 2에 게재하였다. Firewall은 대부분의 부정Access에 대응하고 있지만,그 효과는 부정Access의 종류에 따라 다르며 부정 침입에 대해 가장 유효한 수단으로 되어 있다.

표 2. 부정Access 대책의 수비범위(◎는 효과큼,0 는 효과있음)

부 정	부정침입	서비스정지	서비스정지	도난도청	파괴개정
(1) Firewall의 이용	◎	0	0	0	0
(2) 사용자 인증(on time password, radius 등)	◎				
(3) 암호화				◎	0
(4) 전자서명					◎
(5) OS나 개별 서버 프로그램에 대한 최신 patch의 적용	◎	0	0		
(6) OS의 hardening(불필요한 프로세스를 정지한다.)	◎	0	0		

3. Firewall의 Security

Firewall은 외부와 내부의 네트웍의 접점에 위치하고 내부 네트웍을 외부 네트웍으로
부터 의 다양한 위협에서 지켜주는 것이다.Firewall이 제공하는 기능에는 다음과 같은 것이 있다.

- Packet Filtering기능
- Gateway(Proxy)기능
- Log 기능
- Alarm 기능
- User 인증기능
- NAT 기능
- VPN

(1) Packet Filtering 기능

IP Packet의 IP Header, TCP/UDP Header 등의 정보를 토대로 한 제어방법으로 Firewall을 통과할 Packet을 제한하는 것이다. Packet을 통과시킬지의 여부는 송신원 혹은 송신측의 address와

port번호 등으로 판단한다.네트웍 층에서 Packet의 제어를 하므로 빠른 처리가 가능하다.이 수법은 많은 벤더에 의해 확장이 수행되어 ' State full packet inspection ' 이라는 기술이 널리 사용되고 있다.

(2) Gateway(Proxy)기능

1) Application Gateway형

각 application(telnet,ftp,http등)마다 Gateway daemon을 실행해 두고 이 daemon 이 사용자의 대리인(proxy)으로서 행동한다.Web 컨텐츠의 Cache, URL의 제한 등 세밀한 제어가 가능하다.

2) Circuit Level Gateway형

Socket level로 packet 전송을 하는 SOCKS 서버로 불리는 데몬에 의해 실현된다.

사용자는 packet의 전송을 SOCKS 서버에 의뢰하기 때문에 사용자측 프로그램(WWW 브라우저 등)에 SOCKS 대응 라이브러리를 구성할 필요가 있다.

(시장에 나온 주요 브라우저는 대응되어 있음)

(3) 로그 기능

이상 발생시에 무엇이 발생했는지를 trace하기 위한 데이터 로그를 남긴다.

(4) 이상 발생시의 알람 기능

이상 발생시에 관리자에게 통고하는 기능.호출기 발신기능 등이 있다.

(5) 사용자 인증기능

사용자 마다 Firewall 통과를 제어하게 된다면 사용자 인증이 필요해진다.

(6) NAT(Network Address Translation)기능

외부 네트웍에 대해 내부 네트웍 어드레스를 변환하는 기능이다.

외부에 대해 내부 어드레스를 은폐할 수가 있다.

(7) VPN(Virtual Private Network)

인터넷 등 Security 보증이 없는 외부 네트웍을 이용하여 기밀 데이터를 송수신할 경우,도청 · 사칭의 방지책으로서 쌍방에서 외부 네트웍의 출입구 (Firewall 등)에서 데이터를 암호화하는 방법을 취한다.

4. Firewall의 기능 검정 (실험)

4.1 실험목적

이제까지 서술한 바와 같이 외부 네트웍으로부터 내부 네트웍을 지키는 Security Tool로서의 Firewall은 일반적으로 널리 도입되어 있다.그러나 기본적으로는 2.3에서 설명한 대로 " 부정침입 " 을 막는 것이며 일단 침입을 허가하면 공격을 피하기는 어렵다.

따라서 침입된 공격에 대해 어떻게 일찍 대책을 취하는가가 중요한 과제가 된다. 그러기 위해서는 어떤 방법으로든 일찍,정확히,부정Access를 체크할 필요가 있다. 그래서 본 프로젝트 팀에서는 다음 두가지 사항에 착안하여 Firewall의 Security기능을 검증하기로 하였다.

(1) 부정Access가 있었던 것을 사용자는 어떻게 체크할 수 있는가?

(2) Firewall을 통과해 버린 부정 Accees는 어디까지 체크할 수 있는가?

이 경우에 사용할 Firewall의 기능으로서는 ' 로그 기능 ' 에 목표를 맞추고 검증을 실행하였다. 그리고 이 실험결과에서 Firewall이 가진 Security 기능의 장점 · 단점 · 한계를 확실하게 하기로 하였다.

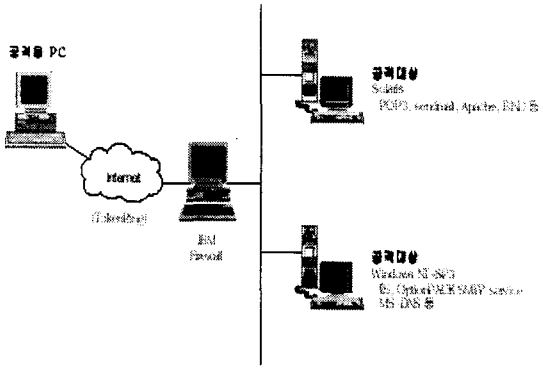
4.2 실험구성

실험구성을 그림 1에 나타내었다. Firewall에는 IBM e-Network Firewall을 사용하였다.

준비된 설비의 사정상, TokenRing측을 외부 네트

웍으로 가정하고 공격대상을 DMZ에 한정하였기 때문에 굳이 사내 네트웍은 만들지 않았다.

그림 1 :실험구성 (1)



4.3 실험내용

비무장 지역인 DMZ상의 서버를 공격하여 다음을 확인하였다.

(1) 부정Access가 있었다는 것을 Access Log 상에서 판단할 수 있는가?

(2) 그 부정Access의 종류(수단)가 Access Log로 판별할 수 있는가?

(3) 부정Access는 성공했는가?

또,IP address에 의한 TCP/IP Packet의 Dump도 실행하고 Access Log와의 체크결과 차이를 확인하였다.(단,공격대상이 Windows NT의 경우에만)

4.3.1 실험 항목

이번 실험에서는 인터넷 상에서 실제로 수행되는 경우가 많은 공격 방법인 Port Scan과 DoS Attack을 중심으로 3가지 패턴을 실시하였다.이때,실험 1 이외의 Firewall에서는 어떠한 제한도 되어 있지 않았지만, Firewall을 통과하는 Packet의 Log는 모두 취득하도록 설정하였다.

(1) 부정한 Remote Login (telnet)의 방지와 체크

(2) Port Scan

(3) Service 정지공격(DoS)

(4) 상용 툴에 의한 유사공격

실험 1 :부정한 Remote Login (telnet)의 방지와 체크

Remote Maintenance 등의 목적에서 주로 UNIX 시스템에서 사용되는 telnet에 관해 Firewall에서 부정Access의 방지,및 체크가 가능한지의 여부를 테스트한다.

테스트 패턴으로서는 다음 두가지를 설정했다.

1)Firewall 상에서 아무것도 제한하지 않는다.

2)Firewall 상에서 Packet Filtering

(Port 2 3의 outbound를 금지)

실험 2 :Port Scan의 체크

악의적인 제3자가 부정한 Attack을 수행할 사전작업으로서 Port Scan이라 불리는 내부 서버에 대한 access가능한 port 번호를 순서에 따라 체크하는 행동을 한다는 것이 잘 알려져 있다.

이번에는 NSA(Network Security Auditor)라는 IBM e-Network Firewall에 부속된Security Check Tool을 사용하여 이 Port Scan을 유사적으로 재현하여 이것이 Firewall상에서,또 Realtime 공격 체크 툴에서는 어떻게 체크할 수 있는 지를 테스트해 보았다.

실험 3 :서비스 정지공격(DoS)의 실시

현재 Internet 상에는 다양한 DoS 툴이라 부르는 네트웍 경유로 시스템에 장애를 주는 프로그램이 존재한다.이번에는 이들 DoS의 대표적인 것부터 세가지를 선택하여 각각에 대해 Firewall의 Log를 취득하였다. 덧붙여서 최근 특히 문제가 되고 있는 전자메일 폭탄(SPAM)툴에 관한 테스트를 실시하였다.

1)특정 프로토콜을 사용한 공격

프로그램명 :winnuke

발신원 주소 :위조불가

사용할 프로토콜 :TCP(port 139)

공격대상 :주로 Microsoft계 OS

개요 : NetBIOS port 139에 대해 OOB[Out Of Band] packet을 송신한다. NT/95에서는 이에 대한 처리가 불충분하기 때문에 hang up하는 등의 장애가 발생한다. NT에서는 SP3에서 대처완료.

2)부정한 IP Packet의 송신(1)

프로그램명 :teardrop

발신원 주소 :위조가능

사용할 프로토콜 :TCP/UDP(임의 :139를 지정)

공격대상 :OS 일반

개요 :IP의 Fragments data를 송신할 때 이전 Packet과 나중 Packet에서 overlap하는 packet을 송신한다. 전술한 Winnuke도 마찬가지. Windows나 일부의 시스템에서는 대처가 불충분하므로 hang up하는 등의 장애가 발생할 가능성이 있다. NT에서는 SP3에서 대처완료.

3)부정한 IP Packet의 송신(2)

프로그램명 :Nestea

발신원 주소 :위조가능

사용할 프로토콜 :TCP/UDP(임의 :35254(랜덤값))

공격대상 :OS 일반

개요 :2)에서 실험한 TearDrop을 토대로 Fragments Pattern을 변경한 것. NT에서는 SP3+HotFix 또는 SP4에서 대처완료.

4)제어 프로토콜(ICMP)을 사용한 공격

프로그램명 :winfreez

발신원 주소 :위조가능

사용할 프로토콜 :ICMP(Redirect)

공격대상 :주로 Microsoft계 OS

개요 :ICMP의 갱신요구를 연속 송신한다. Win95/NT에서는 이에 따라 CPU의 사용률이 높아져 GUI 조작이 불가능해지는 등 일시적으로 hang up하는 것과 같은 상태가 된다. 고속 LAN이나 CPU 점유율이 낮은 NIC에서는 영향이 발생하기 어렵다.

5)전자메일 폭탄(SPAM)

프로그램명 :mailbomb

발신원 주소 :mail address만 위조가능 (발신IP는 위조불가)

사용할 프로토콜 :smtp(25)

공격대상 :메일 서버

개요 :어떤 특정한 Mail address에 대해 대량의 Mail을 송신한다.

실험 4 :상용 툴에 의한 유사공격

상용 Security Check Tool로서 ISS사의 Internet Scanner라는 툴이 있다.

이번에는 이 툴 중에서도 Firewall에 특화된 부분에 한정된 Firewall Scanner를 사용하여 실제로 어떤 공격을 실행하고 있는지, Firewall상의 로그에는 어떤 형태로 취득할 수 있는지에 대한 테스트를 실시하였다.

4.3.2 실험순서

공격용과 체크측(피공격측)의 두 팀으로 나누고 연계된 다음의 작업을 실시하였다.

(1)공격측과 체크측에 신호를 보내고 공격을 개시한다.

(2)체크측은 신호와 함께 Access Log 상의 표시를 체크 한다.

(3)공격측,체크측 (피공격측)은 부정Access의 결과를 확인한다.

(4)나중에 출력된 각종 로그(파일)를 실제로 추적해 봄으로써 부정Access의 상황을 어디까지 파악할 수 있는지를 평가한다.

4.3.3 채취한 데이터

각각의 실험에 대해

(1)Firewall의 Access Log

(2)IP Address/tcpdump/NT Network Monitor에 의한 TCP/IP packet의 dump

(3)Attack tool의 Command line log

의 3가지 사항을 실험 로그로서 채취하였다.각 로그는 후일 분석을 통하여 체크의 여부에 관한 판단을 수행하는 데에 사용하였다.

4.4 실험결과

실험결과를 표 3 ~표 6에 표시하였다.실험 1의 부정한 Remote Login의 방지와 체크(표 3)에서는 Firewall의 Packet Filter에서 금지된 telnet에 대한 access가 제한되어 로그에서 그 부정Access가 판별 가능하였다. 실험 2의 Port Scan(표 4)은 AccessLog, IP Trace에서 체크 할 수가 있었다.실험 3의 서비스 정지공격(DoS)에 관해서는 통상의 패턴과 다른 Packet 송신 기록으로부터 부정이 행해지고 있다는 것을 어느 정도 판단할 수 있는데 그것이 어떤 공격인지 판별할 수 없으므로 방어대책을 강구하는 것이 불가능하다.이 공격에 대해서는 IP trace도 대부분 무력하다.실험 4의 상용 툴에 의한 유사공격도 부정에 대한 판단,수법의 판별에 관해서는 대부분 마찬가지의 결과이며 방대한 로그나 IP trace의 데이터로부터 판단하는 것은 대부분 불가능하였다.

표 3.실험 1 부정한 Remote Login(telnet)의 방지와 체크

부정 access	공격 대상	Packet Filtering	Log에 의한 부정Access의 체크				IP trace에 의한 체크여부	부정 Access를 받은 호스트의 결과
			Access Log의 확정	부정의 판단	수법 판별	Realtime 체크		
[illegible] telnet	Solaris	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	telnet 성공
[illegible] telnet	Solaris	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	telnet 불가

표 4.실험 2 Port Scan

부정 access	공격 대상	Log에 의한 부정Access의 체크				IP trace에 의한 체크여부	부정 Access를 받은 호스트의 결과
		Access Log의 확정	부정의 판단	수법 판별	Realtime 체크		
PortScan (Network Security Auditor)	WinNT (Windows NT)	[illegible]	[illegible]	[illegible]	X	[illegible]	[illegible]
	Solaris	[illegible]	[illegible]	[illegible]	X	[illegible]	[illegible]

표 5.실험 3 서비스 정지 공격 (DoS)

부정 access	공격 대상	Log에 의한 부정Access의 체크				IP trace에 의한 체크*1	부정 Access를 받은 호스트의 결과
		Access Log의 특징	부정의 판단	수법 판별	Realtime 체크		
Winnuke	WinNT	수신측Port번호 TCP139에 대해 일방적으로 반복하여 데이터가 송부되어 있다.	0	×	×	×	아무것도 발생하지 않는다.
Teardrop	WinNT	수신측Port번호 UDP139에 대해 데이터가 한 개 흘러 들어오고 UDP Port 0이 한 개 흐르는 한 방향뿐인 데이터 흐름이다.	0	×	×	×	아무것도 발생하지 않는다.
Nestea	WinNT	UDP 데이터가 두 개 흘러 들어오고 UDP Port 0(송신측, 수신측 둘 다 0)이 한 개 흐르는 한 방향뿐인 데이터 흐름이다.	△	×	×	×	서비스정지 (시스템다운)
Winfreez	WinNT	ICMP TYPE=5 가 일방적이고도 계속적으로 송부되고 있다.	0	△	△	0 (ICMP 캡처성공)	서비스정지(20초간 freeze)
SPAM	WinNT & Solaris	수신측 port번호 TCP25의 packet이 차례차례로 대량으로 송부되어 있다.	△	×	×	×	거대 메일수신에 의한 메일서비스 방해

표 6.실험 4 상용 툴에 의한 유사 공격

부정 access	공격 대상	Log에 의한 부정Access의 체크				IP trace에 의한 체크*1	부정 Access를 받은 호스트의 결과
		Access Log의 특징	부정의 판단	수법 판별	Realtime 체크		
상용 Security Check Tool에 의한 유사공격(Firewall Scanner)	Firewall (AIX)	수신측 port번호가 순번대로 Up하여 또 특정 port(TCP21, 25, 80 등)에 반복하여 접속을 시작하고 있다. 또, telnet이나 ftp와 같은 User ID로 로그인을 시도하여 실패하였다.	0	△	×	-	서비스 등의 port번호의 누출
	WinNT & Solaris	수신측 port번호가 순번대로 up하고 있고 또 특정 port(TCP21,25,80 등)에 반복해서 접속을 시작하고 있다	0	△	×	0 (TCP25/53/80에서 캡처성공)	서비스등의 port번호 및 OS, 서비스 등의 버전정보 등의 누출

TCP port 번호 ··· 20(FTP-DATA),21(FTP),23(TELNET),25(SMTP),53(DOMAIN), 80(WWW),139(NETBIOS session service)

UDP port 번호 ··· 137(NETBIOS name service),139(NETBIOS session service)

ICMP type ··· 5(Redirect),8(Echo)

*1 :IP address는 Port 번호 등의 조건에 따라 캡처를 실시하므로 그 조건에 맞지 않을 경우 캡처에 실패한다.따라서 X는 본 실험에 있어서는 캡처에 실패한 것을 가리킨다.

<표에서의 기호 의미>

- Packet Filtering
  - 0 ··· 성공
  - − ··· 미실시
- 부정의 판단
  - 0 ··· 극히 특징적이며 판별/판단이 가능하다.
  - △ ··· 견해에 따라서는 부정Access 등의 상황에만 판별한다.
  - × ··· 로그로서는 모든 판별/판단이 안된다.
- 수법판별
  - 0 ··· 비교적 명확하게 판별할 수 있다.
  - △ ··· 구체적으로 어떤 부정Access인지는 판별할 수 없다.
  - × ··· 로그로서는 모든 판별/판단이 안된다.
- Real time 체크
  - 0 ··· 만약 24시간 · 365일 로그를 보고 있다면 체크할 수 있다.
  - △ ··· 만약 24시간 · 365일 로그를 보고 있어도 간과할 가능성이 높다.
  - × ··· 로그로서는 모든 판별/판단이 안된다.
- IP trace에 의한 체크
  - 0 ··· 본 실험에서 캡처한 포트번호 등의 조건이 합치하여 캡처에 성공.
  - × ··· 본 실험에서 캡처한 포트번호 등의 조건이 합치하지 않아 캡처에 실패.
  - − ··· 미실시

5.5 Firewall의 과제 및 대책

5.1 Firewall의 과제

이번 실험에서 다음 두가지 사항이 확인되었다.

(1)Port Scan이나 전자메일폭탄(서비스정지 공격)등은 Firewall에서는 방지할 수없거나 혹은 체크가 곤란하다는 것.

(2)공격마다 로그 수집을 했음에도 불구하고 Firewall의 로그는 복잡하므로 단시간에 사건의 발견이 매우 곤란하다는 것.

제한된 시간과 환경에서의 실험과 달리 실제 환경에서는 인터넷 상의 불특정다수의
access가 있어 그것을 감시하지 않으면 안된다.
4장의 결과에서 Firewall 이라 해도
기술적 · 운용적인 과제를 안고 있음을 새삼 인식하였다.
운용담당자 레벨에서 어떠한 부정Access를 받고 있는지를 Firewall의 로그로 판단하는 것은 매우 어렵고 부정Access가 되고 있음에도 불구하고 운용담당자가 모두 깨닫지 못할 가능성도 있어 경우에 따라서는 공격을 받고 치명적인 결과를 초래하게 될 경우도 생각될 수 있다. 이러한 Firewall의 과제에 대응할 방법으로서 다음을 들 수 있다.

(1)로그해석 툴 등을 이용하여 로그해석을 빈번히 실행하여 항상 감시한다.

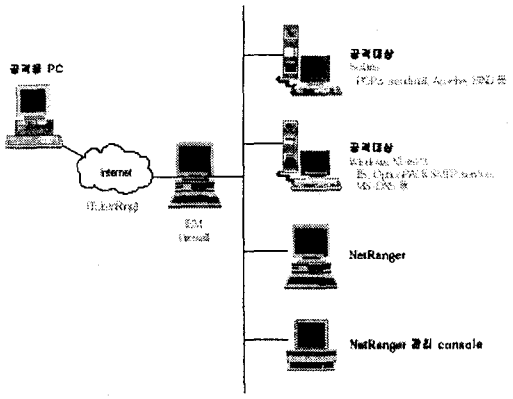
(2)Real time의 부정Access의 체크 툴(이하, 체크 툴)을 사용하여 체크한다.

(1)은 Access log에서 어떤 공격이 되고 있는지를 해석하는 툴이다.이 툴의 이용으로 운용담당자는 Security에 대한 스킬이 별로 없어도 어떤 공격이 있었는지를 어느정도 알 수가 있게 된다.단,이 툴은 어디까지나 로그의 해석 툴이므로 즉시성은 부족하고 Real time으로 체크하는 것은 불가능하다.그에 비해 (2)는 Real time으로 어떤 부정Access가 되었는지를 체크할 수 있다는 이점이 있다. 본 팀에서는 이 체크툴의 유효성을 조사하였다.

5.2 체크 툴의 사용

현재, 체크 툴 시장에서 ISS사의 Real Secure와 CISCO SYSTEMS사의 NetRanger의 비율이 높고 이 두가지 제품은 일부 기능을 제외하면 대부분 동등한 기능을 갖고 있다.
이번에는 NetRanger를 그림 2와 같이 공격 대상 서버인 어느 네트웍 세그먼트(DMZ)에 설치하고 4장과 같은 실험을 수행하였다.

그림 2.실험 구성(2)



5.3 실험결과

표7 ~표9에 실험결과를 표시한다.4장의 결과와 비교할 수 있도록 Firewall의Access log에서는 체크할 수 없었던 부정Access가 전부 체크되어 있다.더구나 어떤 종류의 부정Access인지도 정확히 통지되고 있다.또,전술한 바와 같이 체크 툴은 부정Access가 있다면,디스플레이 상에 Real time으로 통지해 준다.이 결과를 보면 체크 툴은 5.1 에서 서술한 Firewall을 가진 Security상의 두가지 문제에 대한 해결책이 될 것으로 생각된다.

표 7. 실험 2 Port Scan

부정 access	공격 대상	Log에 의한 부정Access의 체크			NetRanger	
		부정의 판단	수법 판별	Realtime 체크	체크상황	Realtime 체크
PortScan (Network Security Auditor)	WinNT (Windows NT)	○	○	×	TCP Port Sweep의 일 수천의 대량 TCP Connection Request 등 아이콘 출력으로 통지	○
	Solaris	○	○	×	상동	○

표 8. 실험 3 서비스 정지 공격(DoS)

부정 access	공격 대상	Log에 의한 부정Access의 체크			NetRanger	
		부정의 판단	수법 판별	Realtime 체크	체크상황	Realtime 체크
Winnuke	WinNT		×	✓	NetBios Out of Bound를 체크한 것을 아이콘 출력으로 통지	○
Teardrop	WinNT		×	×	IP Fragments Overlap을 체크한 것을 아이콘 출력으로 통지	○
Nestea	WinNT	△	×	×	IP Fragments Overlap을 체크한 것을 아이콘 출력으로 통지	○
Winfreez	WinNT		△	△	수천의 대량 ICMP Redirect를 체크한 것을 아이콘으로 통지	○
SPAM	WinNT & Solaris	○	×	×	Qmail Length Crash를 체크한 것을 아이콘으로 통지	○

표 9. 실험 4 상용 툴에 의한 유사공격

부정 access	공격 대상	Log에 의한 부정Access의 체크			NetRanger	
		부정의 판단	수법 판별	Realtime 체크	체크상황	Realtime 체크
상용 Security Check tool 에 의한 유사공격 (Firewall Scanner)	WinNT & Solaris	○	△	×	TCP Connection Request, TCP Port Sweep, ICMP Unreachable, Tftp password, DNS Request, Windows Registry Access, MailRecon, Bad from, Bad Recpt, Auth Failure FTP 등을 다수의 부정Access 체크한 것을 아이콘으로 통지	○

<표에서의 기호 의미>

- 부정 판단/수법판별/Real time 체크 (Firewall Access Log)

  ○ ,△,× ··· 4.4 참조

- Real time 체크(NetRanger)

  ○ ··· 부정Access와 그 내용을 즉시 체크할 수가 있다.

5.4 체크툴의 유효성

이번에 우리가 실험에 사용했던 IBM eNetwork FireWall에서는 부정Access의 체크는 Access Log를 보는 것 밖에 없다.그러나 이 로그상의 기록 내용은 표시가 추상적이고 기록량이 많아 해독에는 전문지식과 노력을 요하므로 부정Access의 발견에는 대체로 시간이 걸린다.또, 이 방법에서는 운용담당자가 부정Access 수법(정보)에 정통해 있지 않으면 그 사실이 부정Access인지 어떤지의 판단을 내리는 것이 어렵다.이에 대해 체크 툴은 다음 기능을 갖고 있어 그러한 운용담당자의 부담을 경감 시킬 수 가 있다.

- 부정 Access의 종류를 데이터베이스에 보유
- Real time으로 보고
- GUI에 의해 이해하기 쉽게 보고
- 부정Access를 레벨별로 보고

그 외에 Firewall만의 운용 시에 비해 다음 행동을 불러오기까지의 시간이 단축된다는 효과가 있다.

- 운용 Policy에 따른 대응
- Firewall의 vendor에 대한 보고
- Firewall의 설정 수정
- Firewall에 대한 patch적응(Firewall의 bug,새롭게 발견된 약점 등의 경우)
- 동작검증(문제수정의 확인)

오히려,이번에 사용한 NetRanger는 체크한 부정Access로부터 Router(Cisco로 제한함)의 설정을 자동적으로 변경할 수도 있다.

이러한 점을 살펴 본다면 체크 툴은 Firewall의 문제에 대처함과 동시에 운용 담당자의 부담을 경감시키는 유효한 수단이 될 것으로 생각한다.

5.5 Firewall + 체크 툴의 운용상의 주의점과 그 Positioning

그러나 체크 툴은 기존의 부정 Access에만 대응하고 있어 바이러스 체크 툴의 패턴파일과 마찬가지로 부정 Access의 데이터베이스를 항상 최신의 상태로 유지하지 않는다면 새로운 공격에는 대처할 수 없다.그리고 말할 것도 없이 최신의 데이터베이스는 새로운 공격이 발생하고 비로서 갱신되는 것이다.

이번 연구에서 판명된 Firewall의 수비범위는 ' LAN간 접속된 외부 네트웍에서 내부네트웍으로의 부정침입을 Block화 하는 것 ' 이다.그러나 무엇이 부정침입인가에 대해서는 어디까지나 이용하는 측이 판단하여 Firewall상에 설정하지 않으면 안된다.즉이용자 측은 온갖 부정Access 정보를 채취,분석하고 운용 Policy에 따라 적절한 설정을 Firewall에 실시하지 않으면 안되는 것이다.체크 툴은 이 부정Access 정보를 데이터베이스로서 갖고 있음으로써 ' 무엇이 부정 Access인가 ' 를 이용자를 대신하여 판단하고 툴에 따라서는 설정을 자동적으로 변경하고 부정Access,의 저지율을 향상시키는 (NetRanger는 CISCO Router에 대해 이 자동설정 변경기능을 갖고 있지만 시간 형편상 실험에서 확인할 수 없었다.) 이것으로써 체크 툴은 Firewall의 수비능력을 보강하는 자리를 굳히게 되었다고 생각할 수가 있다.

한편,이 Firewall의 수비범위 외의 부정Access에 대해서는 별도의 대응이 필요해진다.

예를 들면,서버의 Maintenance용으로 설치된 모뎀이나 TA 등을 경유하여 직접서버에 공격을 시도하는 attack에 대해서는 무력하다.이 공격은 Firewall을 통하지 않을 뿐 아니라 서버에 설치된 서브넷에 설치된 체크 툴에도 일체 packet을 보내지 않는다.이것을 방지하기 위해서는 내부 네트웍에서의 모뎀이나 TA 등의 이용상황을 감시한다.또,기기의 이용자체를 금지한다는 것도 하지 않으면 안된다.또,내부 혹은 DMZ에 설치된 머신에 대해서도 Firewall을 도입했다 해서 안심하는 것이 아니라 동작하고 있는 OS나 프로그램의 Security hole이 없는지를 검증할 필요가 있다.

5.6 Firewall에 의한 부정 Access 대책의 맹점

마지막으로 부정Access에 대해서 또 하나 간과했던 것을 고찰해 보고 싶다.부정 Access란 외부에서 내부로 허가되지 않은 Access라고 하는 ' 통념 ' 이 있다. Firewall 자체도 이 개념에서 등장한 툴이다. 그러나 실제는 내부에 있는 ' 신뢰된 ' 사용자에 의한 공격도 존재한다.

예를 들면,회사에 원한을 가진 사람이 그만두기 전에 시스템 파괴 · 서비스 정지를 해버리는,타인의 패스워드를 훔쳐서 도용하는,사람의 신용을 실추시키는 메일을 보내는 등이 있다.특히 도용의 경우는 귀찮도록 서버의 로그를 체크하여도 그 사람이 메일을 보냈다는 사실이 기록되어 있을 뿐이다. 이와 같이 예를 들어 내부에 있다 해도 Cracking에 흥미가 없는 사람이나 성실한 사람만으로 구성되고 있다는 보증은 없다. 규모가 크게 커지면 커질수록 다양한 인간이 있는 것처럼 그에 따라서 ' 위험한 ' 인간이 있을 가능성, 공격을 간과할 가능성도 증가한다.

최근에는 두려울 정도로 Packet 도청 툴이나 Cracking 툴이 다수 출하되고 있어 누구라도 간단히 입수하여 사용할 수가 있다.이것이 흥미없는 사람이나 성실한 사람을 cracker로 만들어 버릴 가능성을 포함하고 있다.

' 인증된 ' ' 신뢰의 구축 ' 사용자 이외는 네트웍에 접속되지 않는 것이 안전하며 또한 이상뿐이지만 현재의 TCP/IP(Ipv4)를 메인 프로토콜로 할 경우,현재로서는 불가능하다고 생각한다. 인증을 엄격하게 할 암호화라는 방법에서도 불

충분한 경우는 해당 네트웍을 일반 사용자의 Access를 불가능하게 할 곳으로 옮겨 설치하는 방법 밖에 없을 것이다.

6. 맺음말

우리 NS01은 Firewall을 중핵으로 놓은 Security를 주제로 1년 남짓 연구를 계속해왔다.
이 분야의 Skill은 인터넷 접속하고 있는 기업에 따라서는 필수적이며 앞으로도 더욱 힘을 주지 않으면 안될 것이다.
e-Business라고 하는 단어가 유행하고 있는 것처럼 앞으로 점점 인터넷을 이용한 전자상거래가 유행할 것은 틀림없지만 거기서 중요해진 것은 Security이다.부정침입을 허락하지 않는 장치 만들기가 필수적이다.이것을 게을리하여 부정침입을 당했던 기업은 이미지 저하를 면치 못하고, 헤아릴 수 없는 사회적 손실을 입힐 것이다.
반면, Security · Security만으로 시스템을 꽁꽁 묶어버리는 것도 생각해 본다.역시 여러 가지 면에서 어느 정도까지 지켜지지 않으면 안될 정보인가를 확실히 해둘 필요도 생기게 된다.이 Security Policy가 가장 기본임을 잊어서는 안된다. 또,이미 외부로 눈을 돌려 버린 듯 하지만 내부에 대한 고려도 필요하다는 것도 잊어서는 안된다.이 모두를 포함하여 현재로서는 각 기업의 인터넷시스템 운용 도입에 있어서 Security에 대한 힘을 가진 것이 아직 본격화되고 있지 않다라는 것이 현재의 모습일 것이다.그런 의미에서 본 연구 테마는 대단히 유효한 것이었다고 확신한다.
마지막으로 시스템은 기계에서 지킨다 해도 그것에 관계된 사람 한 사람 한 사람에 대한 Security가 철저하지 않으면 안된다.시스템상 참조마저 불가능한 문서가 태연히 인쇄되어 데스크상에 놓여 있다.이것이야말로 Security Policy이며 개선이 필수인 것이다.
앞으로의 과제에서는 이러한 기본적인 Security mind는 종료한다.
논문을 모두 작성한 지금,이 1년 동안의 우리 활동을 돌아보고 좋았던 것은 멤버와의 교류를 통해 Internet Security에 대한 흥미도 점점 늘어나 대단히 뜻 있는 시간을 가질 수 있었다는 것이다. 또,고객,상사 · 부하,선배 · 후배라는 비유가 일체 없이 중간감각에서 경쟁회사의 사람들과 만났을 때도 대단히 중요한 경험이었다.또한 가이드쉐어가 없었다면 맛볼 수 없을 체험이었을 것이다.이와 같은 장을 마련하고 있던 일본 GUIDE/SHARE 위원회의 전부,그리고 실험환경을 흔쾌히 제공해 주셨던 河岡Advisor 및 유니어덱스사의 모두에게 이 장을 빌어 감사의 뜻을 표하고 본 연구를 끝맺고자 한다.

참고문헌

[1] 닛케이 오픈 시스템
1998 년 6 월호 (닛케이 BP 사)

[2] 인터넷 테크놀로지
1999 년 8 월호 (닛케이 BP 사)

[3] Cracking 대책 Final Guide
Anonymous 著,1999년 (燔泳社)

[4] 포인트 도해식 인터넷 RFC사전 笠松英松감수,멀티미디어 통신연구회편 1995년(아스키출판사)

[5] 양해 TCP/IP W.Richard Stevens 著,井上尙司監譯,1997년 (소프트뱅크북스)

[6] Practical Unix &Internet Security Second edition Simon Garfinkel and Gene Spafford 著,1996년 (O 'Reilly &Associations Inc.,)

[7] http://www.jpcert.or.jp/stmt2.html

[8]http://www.jpcert.or.jp/nl/99-0003-99-0003-01.html