

■ 対応ログ一覧

- ◆: GFI EventManagerでルール定義されています。
- : GFI EventsManagerにMIBが搭載されています。
- : 新たにルール定義ができます。MIBをGFI EventsManagerに取り込みます。

	Windows events	W3C Logs	Syslog messages	SNMP Traps
Access / Identity / Policy / Management				
CA eTrust SiteMinder (Netegrity)				●
Cisco Access Registrar - RADIUS access policy server				●
Cisco Secure Access Control Server (ACS)				●
IBM Tivoli Access Manager				●
Oracle Access Manager (NetPoint /Oblis)				○
RSA ACE Server / RSA Secure ID				○
SecurVantage				○
Anti-virus				
AMaViS			○	
ClamAV			○	
Grisoft AVG	○			
Kaspersky ScanEngine	○			
McAfee	○			
McAfee Total Protection for Enterprise				○
Sophos	○			
SpamAssasin			○	
Symantec Antivirus Corporate Edition				○
Symantec ScanEngine	○			
TrendMicro Office Scan				○
TrendMicro InterScan Web Security				○
TrendMicro VirusWall				○
TrendMicro InterScan Messaging Security				○
Anti virus management / security management software				
F-Secure Anti Virus				○
McAfee Policy Orchestrator				○
Symantec Enterprise Security Architecture				○
Symantec System Center				○
TrendMicro Control Manager				○
Databases				
IBM DB2	○		○	
Microsoft SQL Server	◆			
MySQL	○			
Oracle SQL Server	○		○	
PostgreSQL	○		○	
Data Security				
Ingrian DataSecure				○
Tivoli Storage Manager				○
Vormetric Data Security Expert				○
Directory Services				
Microsoft Active Directory	○			
OpenLdap			○	
DNS \ DHCP Servers				
Bind			○	
Dhcpd			○	
Microsoft DHCP Server	○			
Microsoft DNS Server	○			

	Windows events	W3C Logs	Syslog messages	SNMP Traps
Email Filtering /email server				
CypherTrust IronMail				○
Lotus Domino				○
Proventia MailFilter				○
Honeypots				
Honeyd				○
ManTrap				○
Symantec Decoy Server				○
Specter				○
IDS /IPS				
BlackIce suite				○
Border Guard				○
Cisco IPS 4200 Sensors series (device)				●
Cisco Secure IDS				●
Cisco Security Agent				●
Dragon network sensors (device)				○
Juniper IDP			◆	●
McAfee Entercpt				○
McAfee IntruShield (appliance)				○
NFR-NID (sensor)				○
Prelude Hybrid				○
Primary Response				○
Proventia IPS (appliance)				○
RealSecure Server Sensor				○
Snort				○
Sourcefire Intrusion sensor				○
Sourcerfire RNA				○
Symantec Critical System Protection				○
Symantec ITA				○
Symantec ManHunt				○
Symantec NetProwler				○
Symantec Network Security 7100				●
TippingPoint IPS (50, 200, 200E,600E, 1200E, 2400E, 5000E)				○

	Windows events	W3C Logs	Syslog messages	SNMP Traps
Integrated security				
Juniper Secure Service Gateway SSG 300 series UTM Appliances			◆	●
Sidewinder				●
SonicWall				●
Mail Servers				
Exim			○	
Microsoft Exchange Server	◆	○		
Netscape Messaging Server			○	
Postfix			○	
Sendmail			○	
Routers \ Switches \ Firewalls				
3Com 5000 and 6000 families				●
3Com 4500 and higher series				●
Allied Telesis 8xxx series				●
Allied Telesis 9xxx series				●
Allied Telesis AT-AR-700 series				◆●
Allied Telesis AT-AR400 series				●
Allied Telesis Rapier series				●
Allied Telesis Secure VPN router				●
Allied Telesis SwitchBlade series				●
Astaro Linux Firewall		○	○	
Baracuda			○	
CheckPoint FW-1			○	
Cisco 2800 series and above				●
Cisco ASA family			◆	●
Cisco Catalyst family				◆●
Cisco CATOS Switches			○	
Cisco IOS Routers			○	◆●
Cisco PIX Firewalls			◆	●
CyberGuard TSP Family 1000				●
Dell PowerConnect series				●
HP ProCurve Family				●
HP ProCurve Secure Router				●
Ipchains			○	
IPCop		○	○	
Ipf			○	
Iptables			○	
Juniper Networks E-Series				●
Juniper Networks Firewall family			◆	●
Juniper Networks J-Series			◆	●
Juniper Networks M-Series			◆	●
Juniper Networks NetScreen			◆	
Loop Telecom IP6500 VPN Router				○
M0n0wall			○	
Netgear ProSafe Layer 2 family				●
Netgear ProSafe Layer 3 family				●
NetGear ProSafe VPN Firewall Router				●
Nokia Checkpoint IPSO Firewall			○	
Nortel Secure Router 4134				○
Pf			○	
Pfsense			○	
Smoothwall			○	
Symantec Enterprise Firewall				●

	Windows events	W3C Logs	Syslog messages	SNMP Traps
Network Behaviour Analysis				
PeakFlow				●
StealthWatch				○
Network /devices management				
CiscoWorks				○
Juniper NetScreen Security Manager			◆	○
NFR Central Management Server				○
Proventia Management Siteprotector				○
Sourcefire Defense Center				○
Operating Systems				
Microsoft Windows 2000 SP4 Operating System to Microsoft Vista and Microsoft 2008 Server	◆			
Unix \ Linux Distributions			◆	
Proxy Servers				
Microsoft ISA Server	◆			
Squid		○	○	
Sun Java System Web Proxy	○	○	○	
Remote Access				
PCAnywhere				●
Security Cameras				
AKCP security probe				●
Assus mimic				○
Sensors				
Fan sensors - AKCP security probe				●
Humidity sensors - AKCP sensorProbe				●
Motion sensors - AKCP security probe				●
Pression sensors - AKCP sensorProbe				●
Temperature sensors - AKCP sensorProbe				●
Voltage sensors - AKCP sensorprobe DC				●
VPN				
Alcatel Secure SVPN Gateway 7137				○
Check Point VPN-1				●
Cisco VPN 3* Concentrators series				●
Juniper Networks SSL VPN Appliances			◆	●
Web Security				
Websense Enterprise				○
Web Servers				
Apache		○	○	
Zeus		○	○	
Microsoft IIS	◆	◆		
Sun Java System Web Server			○	
Sun One Web Server		○	○	
Netscape Fasttrack Commerce >Enterprise		○	○	
Netscape iPlanet		○	○	
NCSA		○		
WLAN Security				
AirDefense Guard				○
Axial AirMagnet Enterprise				○
Cisco Aironet 1200 Series				●