ESI Data Security Service Specification

Ver1.2

Professional Service Division

Xerox e-Discovery

1. Data Security Overview

Professional Service Division

Xerox e-Discovery

1.1. Overview of ESI Data Security

Ji2 protects a client's ESI (electrically secured information) using a multistage defense with various security measures applied to the information system (network, server and terminal) as well as physically. The main features of Ji2's ESI data security are as follows:

Coverage of the ESI security	The area which needs security operation	Ji2's offerings
Physical security measures for the datacenter	Datacenter with a high security rating	Service levels at or exceeding "Tier 3" as defined by the Japan Data Center Council（JDCC）
	Physical security such as entrance and exit control	Secured reception entrance monitored 24 /7 by the center's personnel. Entrance and exit to the data center monitored by surveillance camera s and accessed only via biometrics authentication
	Third party certification of the security management	ISO27001 certification obtained for iDC (off-site) datacenter.
Communication network	Virtual Private Network（VPN)	Handle ESI data in an exclusive, encrypted network using IPsec (IP Security).
	Firewall	Control and block outside communication ports except required ones (443 and 3389 ports)
	Intrusion Detection System (IDS) equipped, managed Intrusion Prevention System (IPS) is an active option	Detected unauthorized computer access will be blocked. Managed IPS, powered by IBM X-force, is also available for an additional fee.
	Encryption as the measures to prevent falsification or tampering with data and information leakage	AES encryption, HMAC certification and SSL communication with high security strength
Server	OS Security Settings	Minimal administrator-level authorization (Windows) / mandatory access control.
	Access restriction and control	Access restriction at the IP level plus role-based access restrictions
	Data protection and backup	Disk redundancy using RAID6, asynchronous backup, and forensic reproduction of original ESI
Application	Separation of ESI files and processing/review DB	Isolate the data to use for each process from the storage of the client's ESI files
	Authority settings at the applications level	Role-based access authority settings limit case access and access to application features.
	Keep the ESI data within iDC through all processes	"Terminal Server" in the datacenter transmits only the necessary screen to the user's terminal through Remote Desktop Protocol (RDP)
Business terminal	Virtual desktop	Access to applications from normal Windows desktop within the RDP environment
	Measures for virus and malware	Commercial anti-virus software is equipped; a whitelist measure is available for an additional fee.
Laboratory or review center	Physical security : entrance and exit control	Entrance and exit from the data laboratory or the review center is controlled via electronic ID card, 24-hour monitoring with the surveillance cameras, and restrictions on what personal belongings may be carried into a room (cell phones, USB drives, etc. are prohibited)
	Exclusive network	Access to the LAN within the laboratory or review center only via direct-wired connection (no WiFi)

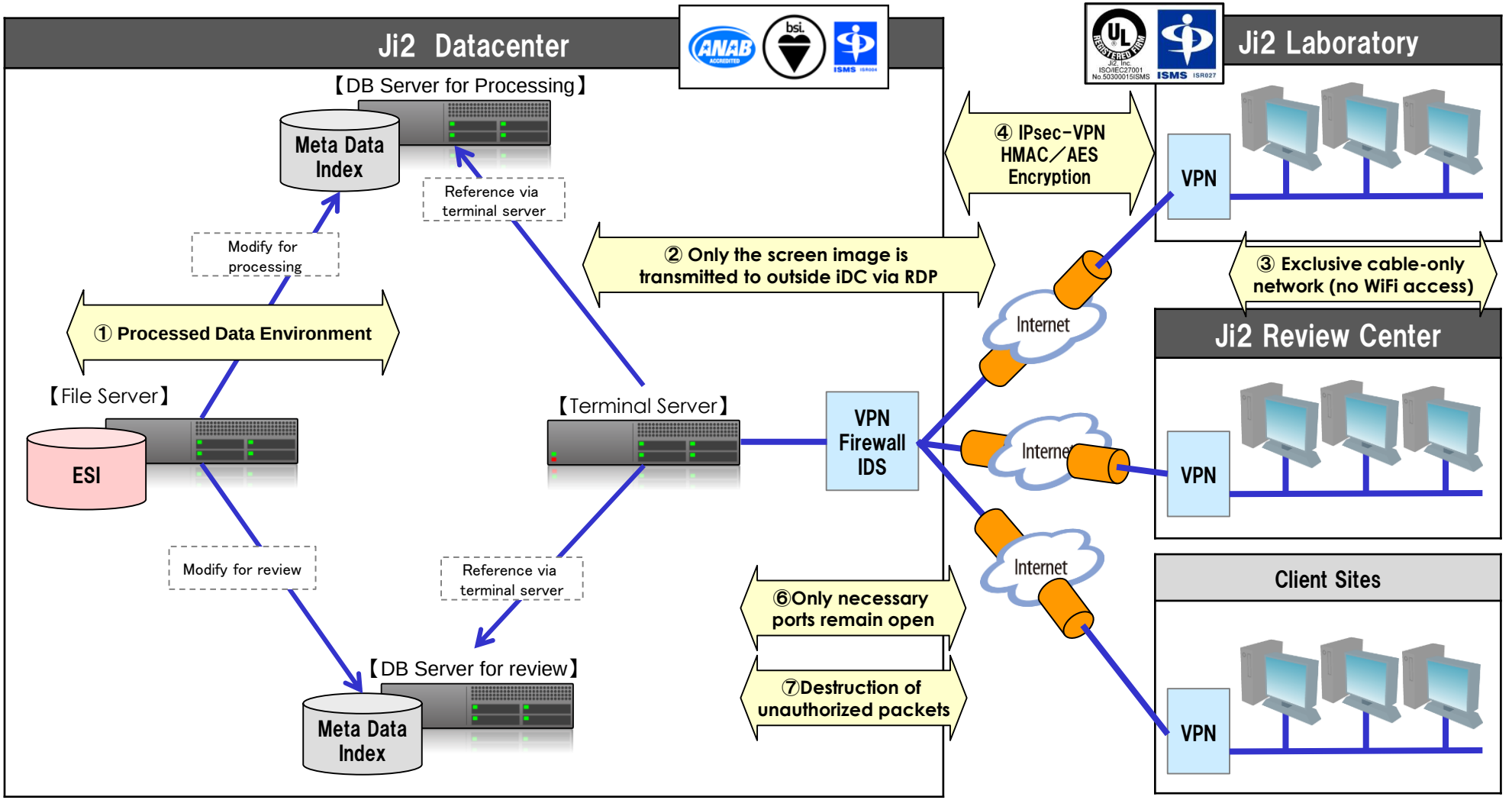
1.2. Data security requirements

Ji2 defined six security requirements to design its data security system for ESI (electronically stored information) held on behalf of clients for electronic discovery. Generally, information security cannot become 100% safe regardless of the level of effort; however, Ji2 designs its system to be as robust as possible.

ESI data security requirements	Assumed risks	Phenomenal examples of data security	Countermeasures
Avoid involuntary system shutdown	Operation ceases due to external / internal factors or ESI data disappears and ESI data cannot be processed.	・Communication down due to DoS (Denial of Service) or external DDoS (Distributed Denial of Service) attack ・System shutdown due to an attack using an OS security hole ・System shutdown caused by unauthorized computer access ・Shutdown due to intentional termination of functions, a breakdown, or equipment destruction	Attack prevention Fragility analysis and measurement Redundancy of systems
Prevention of spoofing attack and subsequent DoS/DDoS attack	An outsider accesses ESI data or the processing data	・ Cracking / wiretapping of user ID and password ・ Session hijacking ・ Subsequent DoS/DDoS attack from spoofed ISP address.	Personal authentication Terminal authentication HASH technology
Prevent Data Manipulation	ESI data itself or the processing data suffers from tampering (mainly due to an external factor)	・ Tampering with the data over the communication path ・ Tampering with ESI data and the processing / analysis data ・ Tampering with various log files	Physical security Encryption HASH technology Data is protected from direct access Intrusion prevention for outside communication Use of third party authentication
Prevention of data leakage	Due to an external factor, ESI data itself or the processing data are intercepted and stolen.	・ Interception and theft on the communication path ・ Theft or reproduction of ESI data due to outside intrusion ・ Information leakage during normal operation (using authorized credentials) ・ Information leakage through human mistake	Physical security Encryption Data is protected from direct access Prevention of external communication breach Use of third party monitoring
Fragility Analysis and Measurement	An outsider accesses ESI data using a security flaw.	・ Unauthorized access using weaknesses of the application ・ Inappropriate configuration, failure to apply patches for OS, middleware, etc.	Fragility inspection Regular application of software patches
Internal Error or Attack	An internal person (within Ji2 or client location) leaks, or manipulates ESI data intentionally or by mistake.	・ Limit information breach, data tampering, etc., caused intentionally by internal individuals. ・ Prevent data breach, setting errors, etc. due to operational mistakes of internal individuals.	Internal access monitoring Authority management Audit of the operation logs

1.3. Security overview of the network system from the perspective of ESI

Ji2 network system conception diagram for the client's ESI data's environment. ① ESI data for processing and review ② may only be transmitted as a screen image to other machines ③ to wired-only LAN networks ④ using encrypted IPsec-VPN. On the datacenter side, ⑥only the necessary ports remain open and ⑦ if unauthorized communication is detected, the data packet is destroyed.



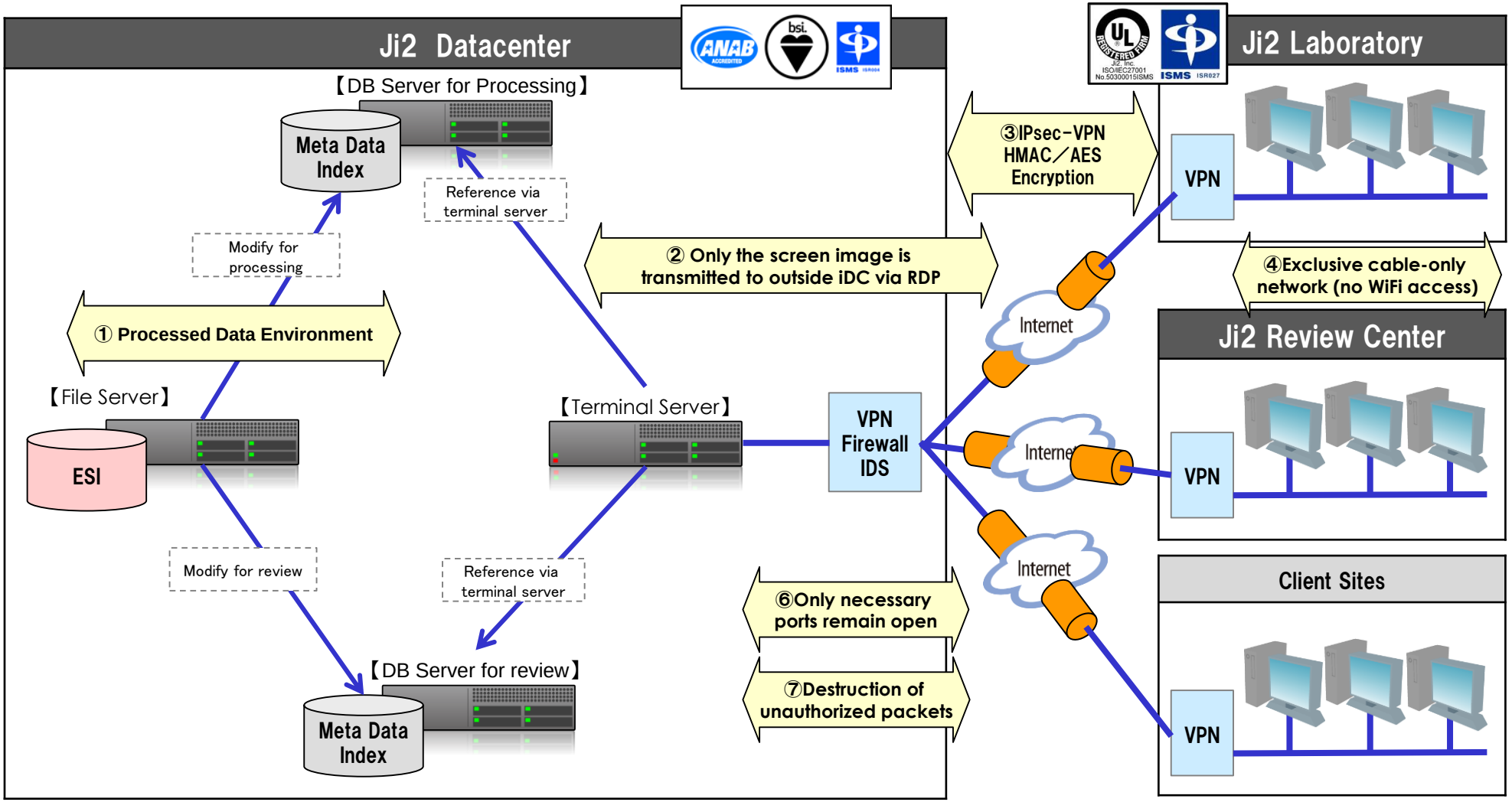
2. Network and Computer System Security

Professional Service Division

Xerox e-Discovery

2.1 Overview

As seen previously in diagram 1.3, the following is a client's ESI data within the Ji2 network system environment. ① ESI data for processing and review ② may only be transmitted as a screen image to other machines ③ through IPsec's virtual exclusive network after encryption . ④It is then only available within Ji2 via wired-only LAN networks. On the datacenter side, ⑥ only the necessary ports are opened and ⑦ if unauthorized communication is detected, the data packet is destroyed.



2.2. Security Roles for eDiscovery Application

2.2.1. Access based on the balance of user needs and data security

Role-based authorization for each feature and function is generally determined as follows

Permission		Administrator	Project Manager	Reviewer
Advanced Tools	ND Similarity Viewer	●	●	
	Concept Analyzer	●	●	
	Relationship Analyzer	●	●	
	Build ND Similarity Viewer	●		
	Email Thread Analyzer	●	●	
	Build Email Thread Analyzer	●		
	Assisted Review	●		
Delivery	Delivery	●		
Global	Access Project	●	●	●
	Customize Layout	●	●	●
	Modify Options	●	●	●
	Edit Project	●		
Processing	Edit Project	●		
	Catalog and Stage	●		
	Extract	●		
	Dedupe	●		
	Customize Slipsheet Template	●		
	Manage Custom Fields	●		
	Edit Custom Fields	●		
	Execute Maintenance Scripts	●		
	Manage Maintenance Scripts	●		

2.2. Security Roles for eDiscovery Application

Permission		Administrator	Project Manager	Reviewer
Review	Access View	●	●	●
	Access View Folder	●	●	●
	Print Documents	●	●	
	Tag Documents	●	●	●
	Access Issue Tag Category	●	●	●
	Redaction	●	●	●
	Save Documents	●	●	
	Automated Review User			
	Linear Review	●	●	●
	Remove Documents from View	●	●	
	Open Native	●	●	●
	Reset Tags	●	●	
Security Manager	Manage User	●		
	Manage Company	●		
	Access Company	●		
	Add Permission	●		
	Manage Role	●		
	Access Role	●		
	See User	●	●	
	Security Manager	●		
Edit View	Build View	●	●	
	Rebuild View	●	●	
	Manage Organization Codes	●	●	
	Move View	●	●	
	Access Scope	●	●	
	Lock/Unlock View	●	●	
	View Manager	●	●	
	Manage System Views	●	●	

2.3. Communication Gateway Security Specifications

Function and performance of the communication gateway including security-related specifications. Also includes details regarding the dynamic packet filtering firewall and IDS which detects unauthorized access or breach.

2.3.1 Main functional specifications of the communication gateway

Functional classification	Item	Specifications
Basic communication function	Throughput	Up to 1Gbit/s
	IPsec throughput	Up to 200Mbit/s
	IPv6 connection type	Native, tunnel, dual stack, RA proxy, DHCPv6-PD
	Routed Protocols	IP, IPv6
	IP routing protocol	RIP, RIP2, OSPF, BGP4（EBGP, IBGP）
	IPv6 routing protocol	RIPng
	Number of route entries	Up to 10,000
	Recommended numbers of OSPF Neighbors and routes	30 Neighbors: 5,000 routes
	Number of BGP4 routes	Up to 5,000
	WAN protocol	PPP, PPPoE, MP, Frame Relay
	The number of the PPPoE sessions	20
	Certification	RADIUS, PAP/CHAP, MS-CHAP/MS-CHAPv2, ISDN authentication based on IP Address
	Management protocol	SNMP（v1, v2c, v3）
Band control	QoS function (control system)	Priority queueing, Bandwidth control (Dynamic Traffic Control), CBQ, WFQ, Dynamic Class Control, VPN QoS, bandwidth detection, load notification
	QoS function (classification method)	IP address, protocol, port number, ToS field
	QoS function (cooperation with the net side QoS function)	ToS → CoS conversion
Closed network	Function for closed network services	Tag VLAN, IPv6 multicast (MLDv1, MLDv2, MLD proxy)
	Tag VLAN (IEEE 802.1Q)	32ID for each LAN

2.3. Communication Gateway Security Specifications

Functional classification	Item	Specifications
Firewall	Static packet filtering (IPv4/IPv6)	Uses IP address, port, protocol (Established, TCP flag), source / destination, IN/OUT on the LAN side /WAN side
	Dynamic packet filtering (IPv4/IPv6)	Basics application (TCP, UDP), applied application (FTP, TFTP, DNS, WWW, SMTP, POP3, TELNET), free definition, applied to IN/OUT on the LAN side /WAN side
	The number of the dynamic filter sessions	20,000
IDS	Detection of unauthorized access and invasion (IPv4)	Applied to IN/OUT on LAN side /WAN side; 31 types of unauthorized access such as IP header, IP option header, ICMP, UDP, TCP, the FTP are detectable; and email notice function of an unauthorized access detection
VPN	VPN function	IPsec (VPN function: NAT traversal, XAUTH)+AES128/256, 3DES, DES (encryption function: hardware processing) +IKE/IKEv2 (main mode, aggressive mode), PPTP (VPN function) +RC4 (encryption function), L2TP/IPsec
	Number of connections to VPN (IPsec)	100 (maximum number: 100)
	Number of connections to VPN (PPTP)	4 (maximum number: 100)
	Number of connections to VPN (IPsec + PPTP)	100 (maximum number: 100)
NAT	Address conversion (NAT Descriptor)	NAT, IP masquerade, static NAT, static IP masquerade, DMZ host function, a PPTP pass-through (multi sessions), IPsec pass-through (1 session), FTP, trace route, ping, SIP-NAT, restrictions function of number of IP masquerade conversion sessions
	The number of the NAT sessions	20,000
Log	Logging function	Stored to the memory, output in SYSLOG, output (encryption function included) to an external memory (microSD, USB memory), function to save logs during power interruption/failure, function to save reboot logs
	Log contents	Packet filtered, call control, performance of various security functions (items blocked by router firewall, etc.)
	Log memory capacity	Up to 10,000 logs
Other security	Security-related extended function	URL filtering (outside database reference type, internal database reference type, web reputation function), DHCP terminal certification function, Winny filter (Winny Version2), Share filter (Share version 1.0 EX2), MAC address filtering

2.3. Communication Gateway Security Specifications

2.3.2. Detection of unauthorized access and intrusion (IDS)

This function works to detect and notify administrators when the system detects a packet with the purpose of intrusion or attack. However, it is difficult to judge correctly whether an invasion has occurred or not, and guaranteed detection is impossible.

Ji2's communication gateway package detects intrusions and attacks by comparing the pattern (signature) of the unauthorized packet to known attack patterns. The pattern comparison is processed packet by packet, and the implementation conducts inspection based on the connection status by inspecting the state of system component potentially under attack such as the ports. This system's effectiveness is maximized when it is used with a dynamic filter. For example, if dynamic filter is defined to use SMTP, based on this information the system detects unauthorized access in connection to SMTP. However, this system detects packets which are not filtered by the dynamic filter (e.g. IP header and ICMP) regardless of the dynamic filter's settings. In addition, basically TCP and UDP can be detected without defining a dynamic filter.

Under Ji2's communication gateway's IDS settings, packets detected under the following criteria are all deleted.

Classification	Item	Judgment condition
IP header	Unknown IP protocol	When protocol field is more than 143 (101 before Rev.10.00.56)
	Land attack	When the IP source address is the same as the destination IP address.
	Short IP header	When the length of the IP header is shorter than the one recorded in the length field
	Malformed IP packet	When a computer receives packets with incorrect header length.
IP option header	Malformed IP opt	When the structure of the option header is invalid
	Security IP opt	When security and handling restriction headers are received.
	Loose routing IP opt	When a loose source routing header is received.
	Record route IP opt	When a record route header is received.
	Stream ID IP opt	When a stream identifier header is received.
	Strict routing IP opt	When a strict source routing header is received.
	Timestamp IP opt	When an internet timestamp header is received.

2.3. Communication Gateway Security Specifications

Classification	Item	Judgment condition
Fragment	Fragment storm	When a large quantity of fragments is received
	Large fragment offset	When the value in the offset field of a fragment is large.
	Too many fragments	When packets are split into too many fragments.
	Teardrop	When attacked by Teardrop or similar tools.
	Same fragment offset	When the values in the offset field of fragments are the same.
	Invalid fragment	When other fragments received are impossible to re-assemble.
ICMP	ICMP source quench	When a source quench is received.
	ICMP timestamp request	When a timestamp request is received.
	ICMP timestamp reply	When a timestamp reply is received.
	ICMP info request	When an information request is received.
	ICMP info reply	When an information reply is received.
	ICMP mask request	When an address mask request is received.
	ICMP mask reply	When an address mask reply is received.
	ICMP too large	When an ICMP of 1,025 bytes or greater is received.
UDP	UDP short header	When the value in the length field of UDP is smaller than 8.
	UDP bomb	When the value in the length field of UDP header is too large.
TCP	TCP no bits set	When nothing is set to a flag.
	TCP SYN and FIN	When SYN and FIN are set at the same time.
	TCP FIN and no ACK	When FIN without ACK is received.
FTP	FTP improper port	A port number specified by PORT and PASV command is not in the range of 1024 to 65535.

3. Security

Professional Service Division

Xerox e-Discovery

3.1. Security: Datacenter

Ji2 uses "the facility standard" that the Japanese Datacenter Association established as a criteria required for secure storage of ESI data. Ji2 selects datacenters with the highest evaluation based upon the following criteria. Ji2's current datacenter is graded "Tier 3" with the following specifications:

Management item	Object	Security specifications	Remarks, photograph, etc.
Access control	Site	Guard-monitored systems and environment	
	Building	Human receptionist Chip card required Biometric vein certification Biometrically secured portals (pictured)	
	Server room	Chip card secured	
	Rack	Key secured	
Security monitoring	Site	Surveillance cameras (monitored and recorded)	
	Building	Surveillance camera (monitored and recorded)	
	Server Room	Surveillance camera (monitored and recorded)	
	Rack	Surveillance cameras are not installed for each aisle.	
Main Distribution Frame (MDF) room, Network room	Separation	Separated, exclusive space is assigned.	
	Redundancy	Redundancy has been confirmed.	
Communications cable and power supply cable	Isolation	Isolation has been confirmed.	
Server operation monitoring	NOC (network operation center) Internal organization of the datacenter	Monitored internet usage 24/7, 365 days per year	
Audit	Information security operation	ISO/IEC 27001	Third party audit

3.2. Security: eDiscovery Laboratory

Ji2 keeps the client's original source data in its eDiscovery laboratory and extracted ESI data in the datacenter. Physical admission to the laboratory is restricted to a sub-set of Ji2 employees and source data is kept in a key-secured locker. Security specifications are as follows.

Management item	Object	Security specifications	Remarks, photograph, etc.
Access control	Site, building	Guard-monitored systems	
	Ji2 floor	Floor specific IC chip card and key.	SECOM Security Systems
	e Discovery laboratory	ID card with IC chip embedded	Access limited to specific personnel. Entrance as well as Entry and Exit logs are also recorded electronically.
	Locker for the ESI data in the laboratory	key	
Security monitoring	Site, building	Surveillance camera (monitored and recorded)	
	Ji2 Floor	Surveillance camera (monitored and recorded)	
	e Discovery laboratory	Surveillance camera (monitored and recorded)	
e Discovery laboratory Local area network	Division	Fully isolated room divided from the rest of the facility.	
	Redundancy	n/a	
e Discovery Laboratory operation monitoring	Ji2's internal operational organization	Monitored by the Professional Service Division	
Audit	Information security operation	ISO/IEC 27001	Third party audit

3.3. Security: Review Center

The data center only transmits ESI data as "a screen for reading“ to the review center. Reviewers must leave personal electronic equipment in a locker external to the review center to prevent photography using cell-phone cameras. The security specifications are as follows.

Management item	Object	Security specifications	Remarks, photograph, etc.
Access control	Site, building	Guard-monitored systems	
	Ji2 floor	Floor specific IC chip card and key.	SECOM Security Systems
	Each room of the review center	ID card with IC chip embedded	Access controlled on a room-by-room basis. Entry and exit logs are recorded electronically.
	Private cell-phones, USB Drives, etc.	Prohibited	To be kept in an external, locked locker
Security monitoring	Site, building	Surveillance camera (monitored and recorded)	
	Ji2 Floor	Surveillance camera (monitored and recorded)	
	Each review room	Surveillance cameras in all rooms (monitored and recorded)	
Review center Local area network	Division	Independent, exclusive room	
	Redundancy	n/a	
Review center operation monitoring	Ji2’s internal operational organization	Monitored by the Professional Service Division	
Audit	Information security operation	ISO/IEC 27001	Third party audit

4. Information Security Management System

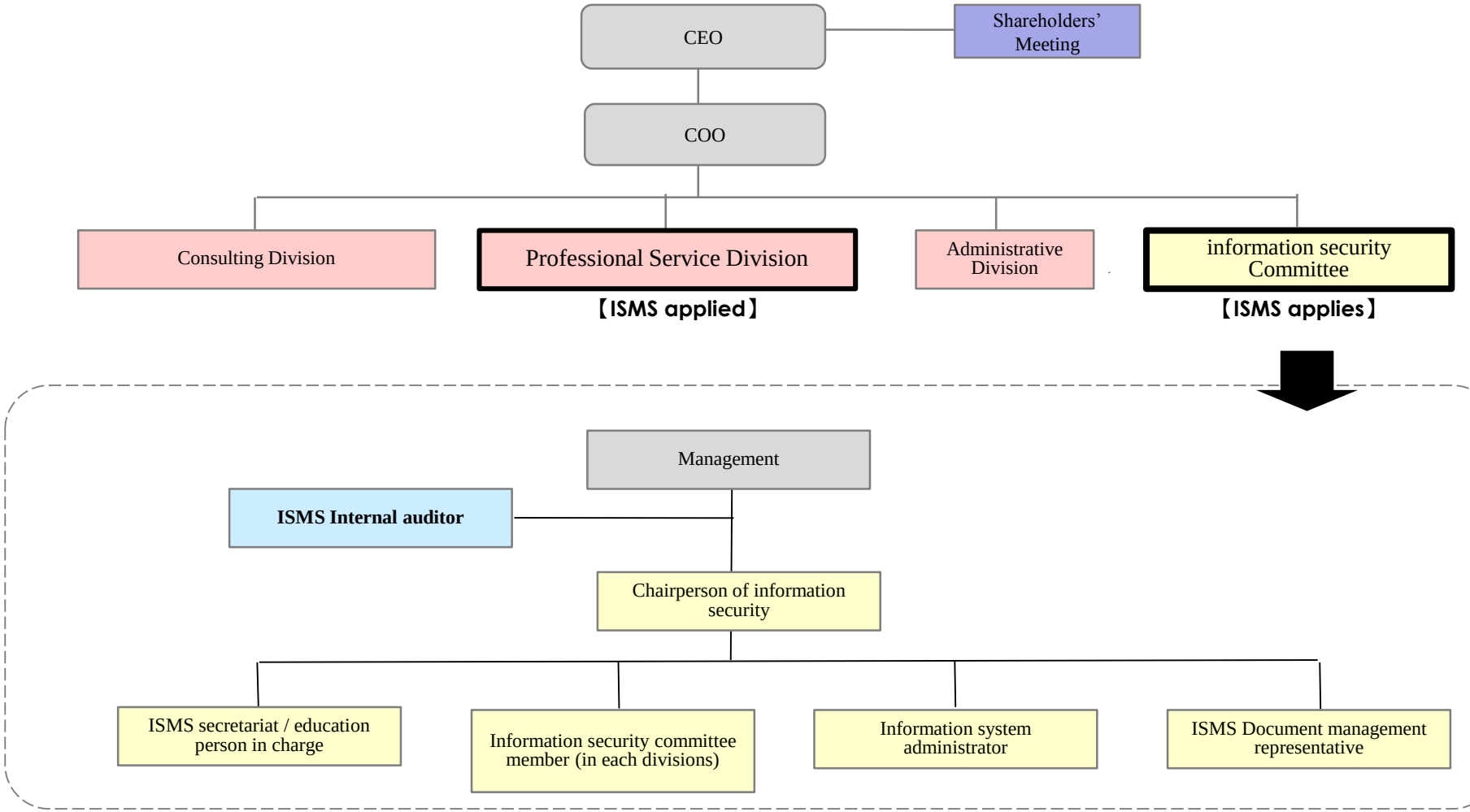
Professional Service Division

Xerox e-Discovery

4.1. The coverage and the maintenance system of ISO/IEC27001

Ji2 obtained JIS Q27001:20014(ISO/IEC 27,001:2013) in April, 2014 and has built a management system (ISMS) for information security management. The following is the scope of ISMS and the implementation of the management system.

Ji2's company organizations and the coverage of application



4.2. Information security management systems: Subcontractors

For some cases, scanned paper document, or translation services may be required and Ji2 may subcontract the work. In addition, Ji2 uses a datacenter to store ESI and treats it as a subcontractor relationship. Each subcontractor's information-security-related certification is summarized as follows.

Requirements	Subcontractor name	The outside certification obtained on the information security	Remarks
ESI data storage	Xerox Corporation (U.S.) (litigation support services)	SSAE16 SOC1 Type II certification ISO/IEC 27001:2005 certification	
	IDC frontier Co., Ltd. (datacenter business)	ISO/IEC27001:2005（JIS Q 27001:2006）certification	
Paper data computerization services	Xebec Co., Ltd.	P mark (JIS Q 15,001:2006) certification	
	Fuji Xerox Co., Ltd. Global service sales division	ISO/IEC27001:2005（JIS Q 27001:2006）certification	
Translation and review services	Honyaku corporation	P mark (JIS Q 15,001:2006) certification	
Review services	With Co. Ltd.	P mark (JIS Q 15,001:2006) certification	
	More Selections Co. Ltd.	N/A	Ji2 Information Security Committee audited March 2015: subcontractor questionnaire April 2015: on-site audit
Electronic mail system operation	Microsoft Corporation （Office365 service）	SSAE16 SOC1 Type II certification ISO/IEC 27001:2005 certification Safe Harbor certification between US and EU US FISMA2002 certification	
【Reference】Parent company	Soliton Systems K.K.	ISO/IEC27001:2014（JIS Q 27001:2013）certification P mark (JIS Q 15,001:2006) certification	