

Fig. 1

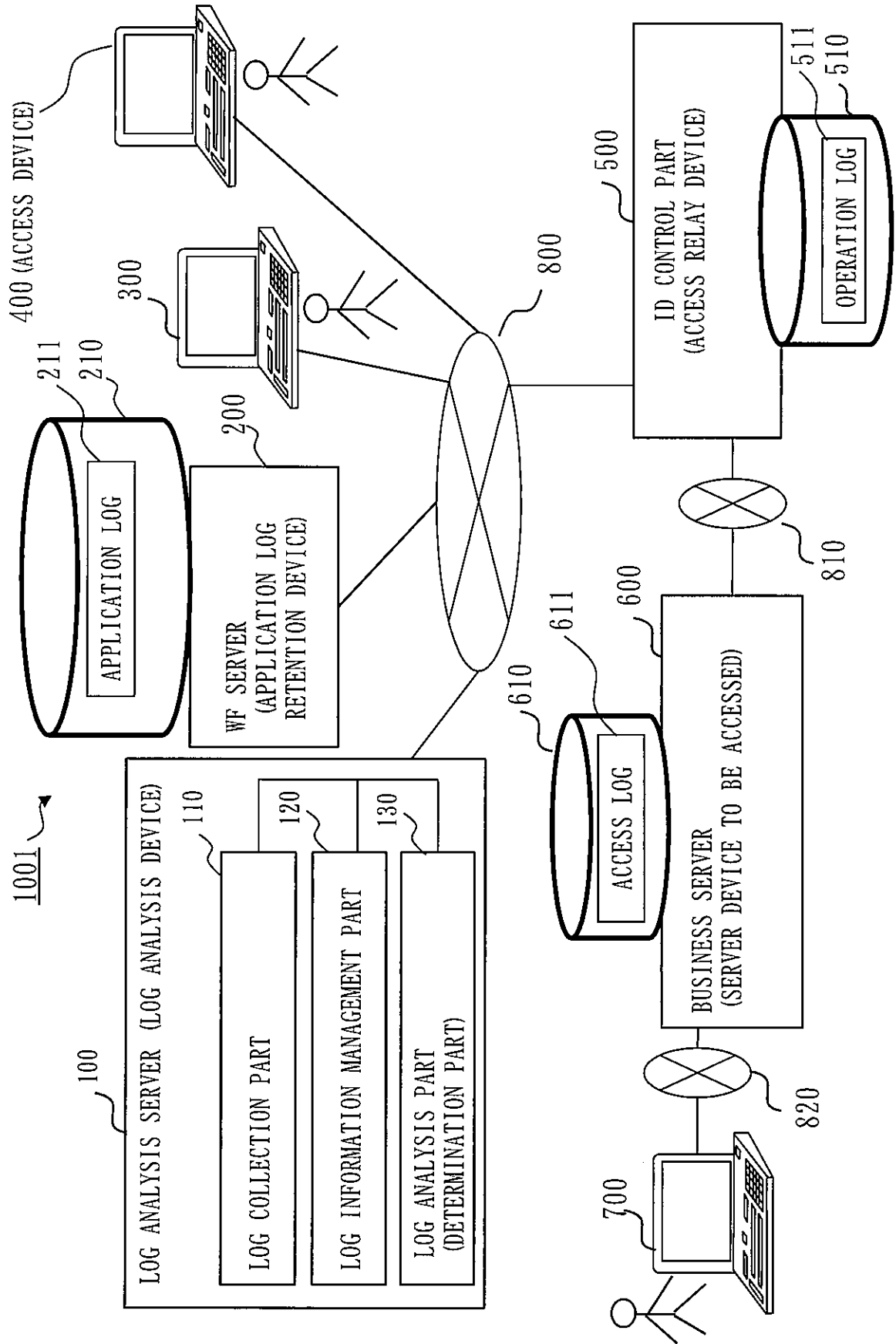


Fig.2

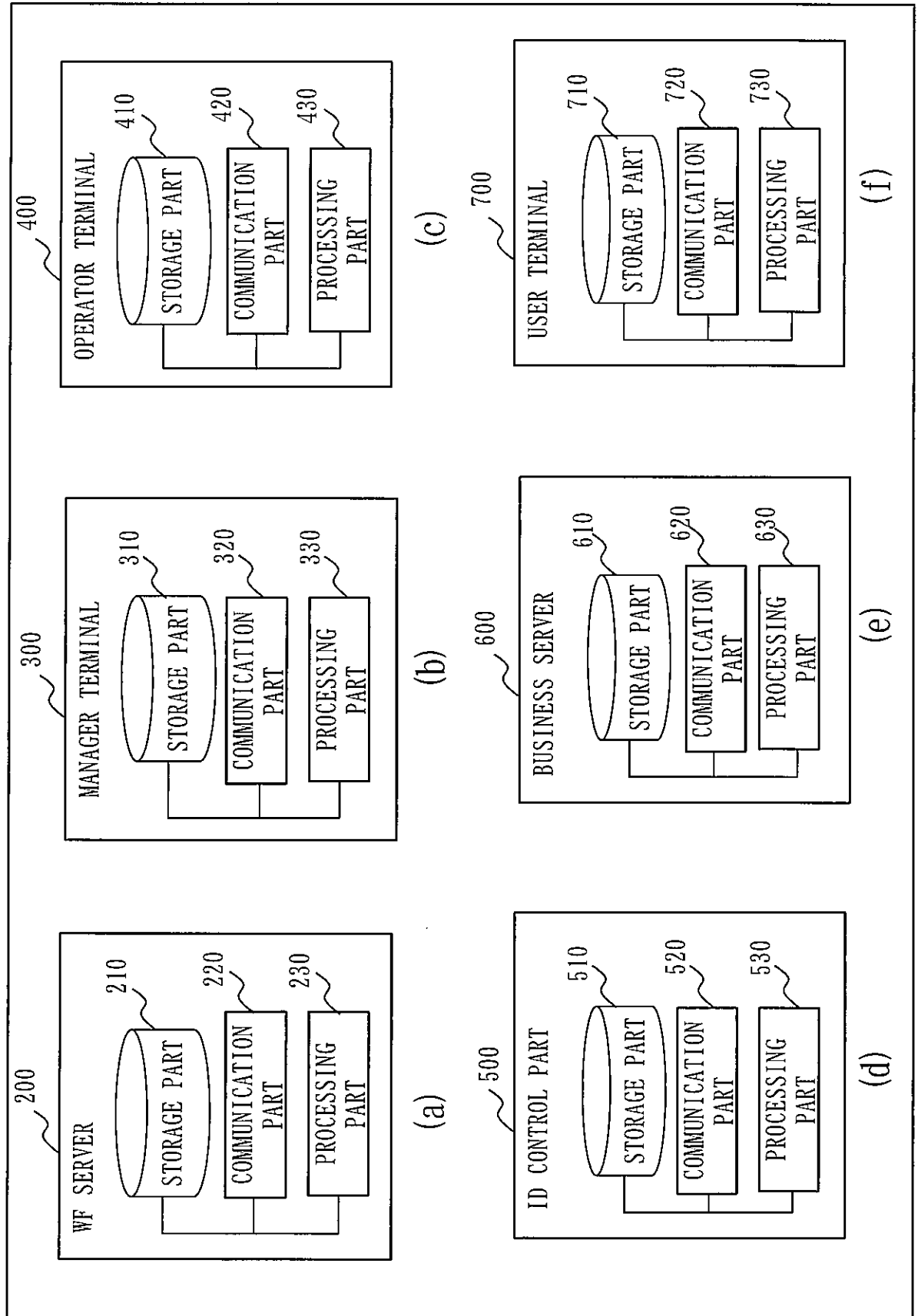


Fig.3

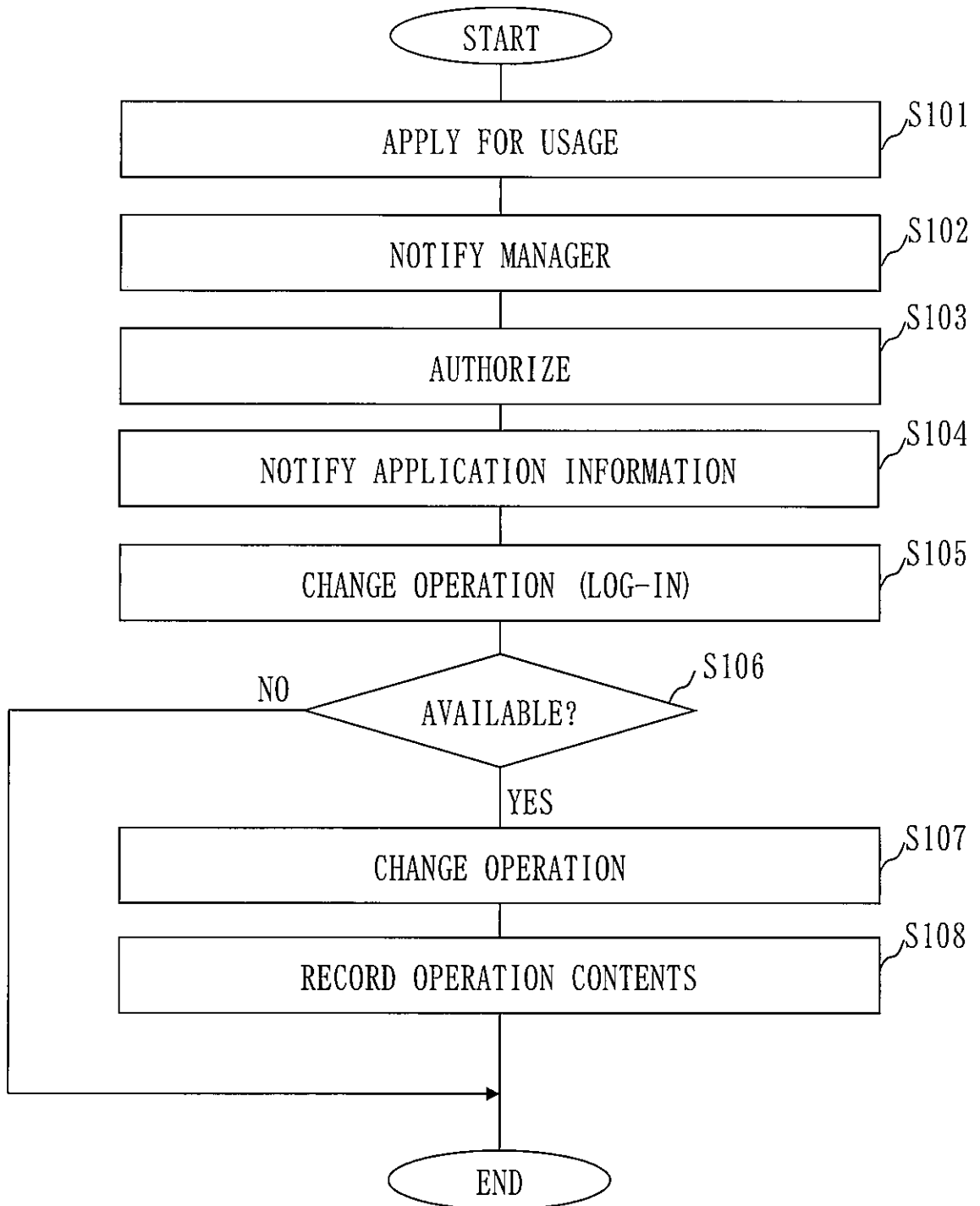


Fig. 4

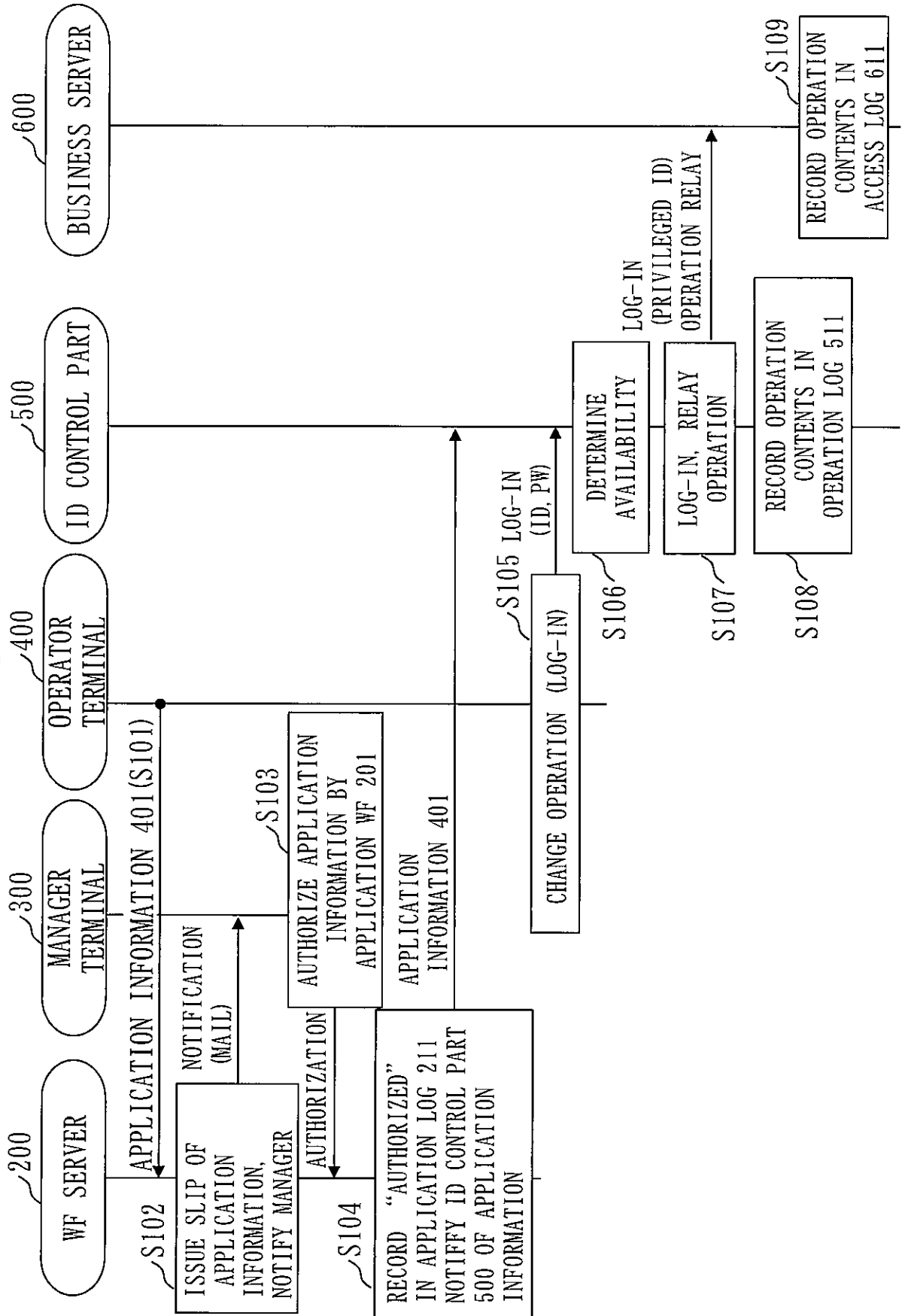


Fig. 5

401

ITEM	CONTENTS
11 PRIVILEGED ID	ACCOUNT FOR LOG-IN TO BUSINESS SERVER
12 USER INFORMATION	IDENTIFIER TO IDENTIFY OPERATOR Y
13 BUSINESS SERVER IDENTIFIER	IDENTIFIER SUCH AS HOST NAME OF BUSINESS SERVER TO BE LOGGED IN
14 PERIOD OF USE	PLANNED PERIOD OF OPERATION TO BE CARRIED OUT ACCORDING TO APPLICATION CONTENTS
15 COMMAND/PROTOCOL TO BE USED	PROTOCOL TO ACCESS BUSINESS SERVER. OPERATION TO BE CARRIED OUT ON BUSINESS SERVER (COMMAND)

Fig. 6

401	
11	ITEM
12	PRIVILEGED ID
13	Admin01
14	USER INFORMATION
15	Takanashi
	BUSINESS SERVER
	Host01
	PERIOD OF USE
	2014/01/01 08:00:00 to 2014/01/01 13:00:00
	COMMAND/PROTOCOL TO BE USED
	RDP

Fig. 7

ITEM	CONTENTS
PRIVILEGED ID	ACCOUNT FOR LOG-IN TO BUSINESS SERVER
USER INFORMATION	SUCH AS ID TO IDENTIFY OPERATOR
BUSINESS SERVER	IDENTIFIER SUCH AS HOST NAME OF BUSINESS SERVER TO BE LOGGED IN
PERIOD OF USE	FROM WHEN TO WHEN IS OPERATION CARRIED OUT ACCORDING TO APPLICATION CONTENTS?
COMMAND/PROTOCOL TO BE USED	WHICH PROTOCOL IS USED TO ACCESS TO BUSINESS SERVER? WHICH OPERATION (COMMAND) IS CARRIED OUT?
AUTHORIZATION STATUS	AUTHORIZED OR UNAUTHORIZED OR DISMISSAL

Fig. 8

211

#PRIVILEGED ID, USER INFORMATION, BUSINESS SERVER, PERIOD OF USE (START), PERIOD OF USE
(END), PROTOCOL, COMMAND, AUTHORIZATION STATUS (HEADING LINE)
Admin01, Takanashi, Host01, 2014/01/01 08:00:00+0900 (JST), 2014/01/01
13:00:00+0900 (JST),
Admin02, Matsuzaka, Host01, 2014/01/01 09:00:00+0900 (JST), 2014/01/01
10:00:00+0900 (JST), Telnet, yum . . . (OMITTED), NG

Fig. 9

511

ITEM	CONTENTS
11-5 PRIVILEGED ID	ACCOUNT FOR LOG-IN TO BUSINESS SERVER
12-5 USER INFORMATION	IDENTIFIER TO IDENTIFY OPERATOR Y
14-5 PERIOD OF USE	
17-5 OPERATION CONTENTS	※VARY ACCORDING TO PROTOCOL TO BE USED IN CASE OF telnet, ETC., RECORD COMMAND TO BE USED IN CASE OF RDP PROTOCOL, RECORD SCREEN IMAGE, ETC. FROM RDP TO BE PASSED

Fig. 10

511

#PRIVILEGED ID, USER ID, DATE AND TIME OF START OF USE, DATE AND TIME OF END OF USE,
PROTOCOL, OPERATION CONTENTS
Admin01, Takanashi, 2014/01/01 08:03:12+0900 (JST), 2014/01/01
10:08:03+0900 (JST), RDP, file://○○○ (LINK TO RECORDED VIDEO OF OPERATION CONTENTS)

Fig. 11

	ITEM	CONTENTS
11-6	USER ID (PRIVILEGED ID)	
17-6	OPERATION CONTENTS	INFORMATION OF OPERATION SUCH AS LOG-IN AND EXECUTED COMMAND, ETC.
14-6	DATE AND TIME OF OPERATION	DATE AND TIME OF IMPLEMENTING THE ABOVE OPERATION

Fig. 12

611

#	DATE AND TIME (JST)	EVENT ID	CATEGORY	DETAILS
	2014/01/01 08:03:14	0001	(LOGGED ON NORMALLY)	LOG-ON, Admin . . .
	2014/01/01 08:04:19	0500	(FILE OPEN)	FILE ACCESS, Admin ○○
	FILE			
	2014/01/01 10:08:04	0002	(LOGGED OFF NORMALLY)	LOG-OFF, Admin . . .

Fig.13

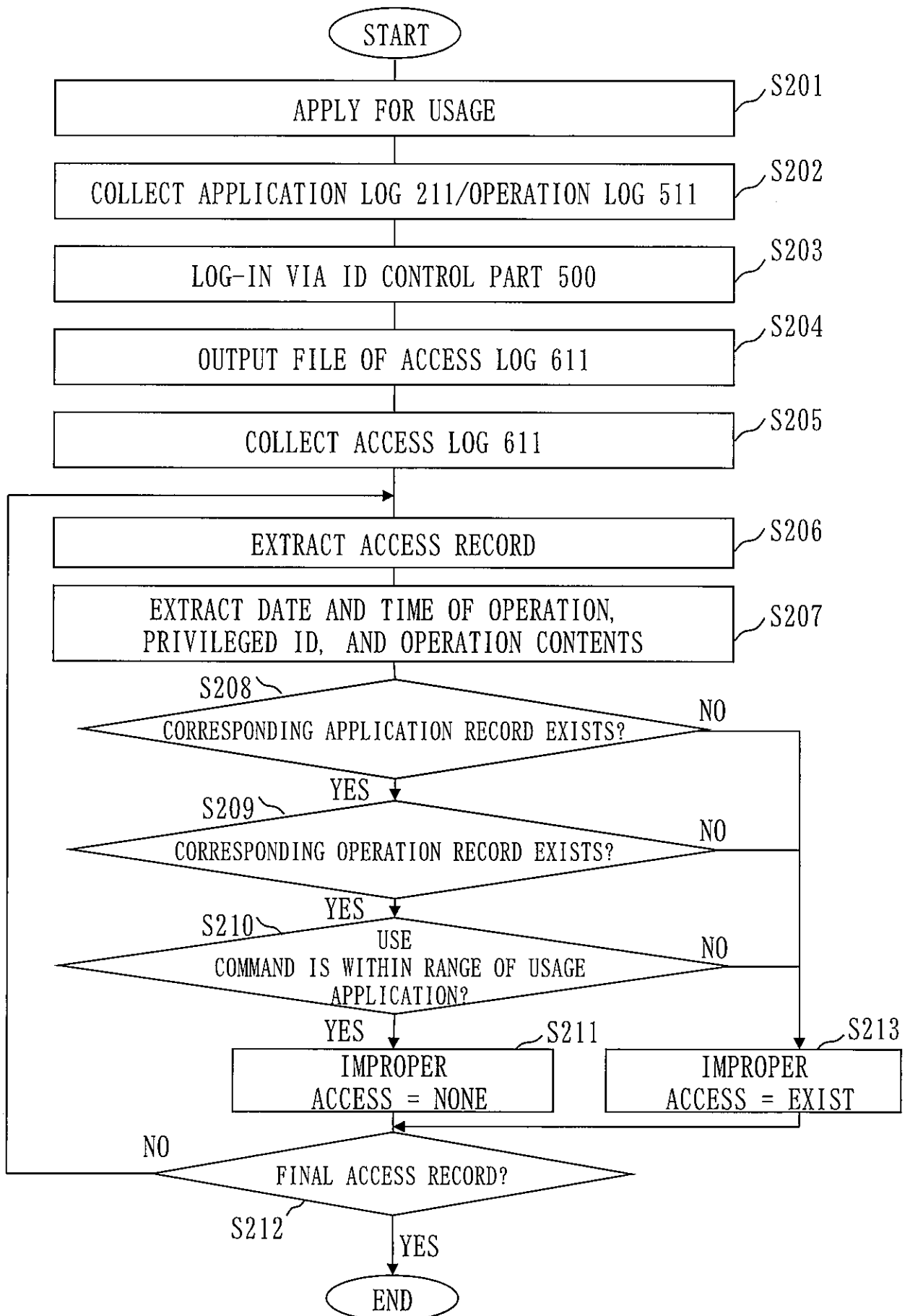


Fig. 14

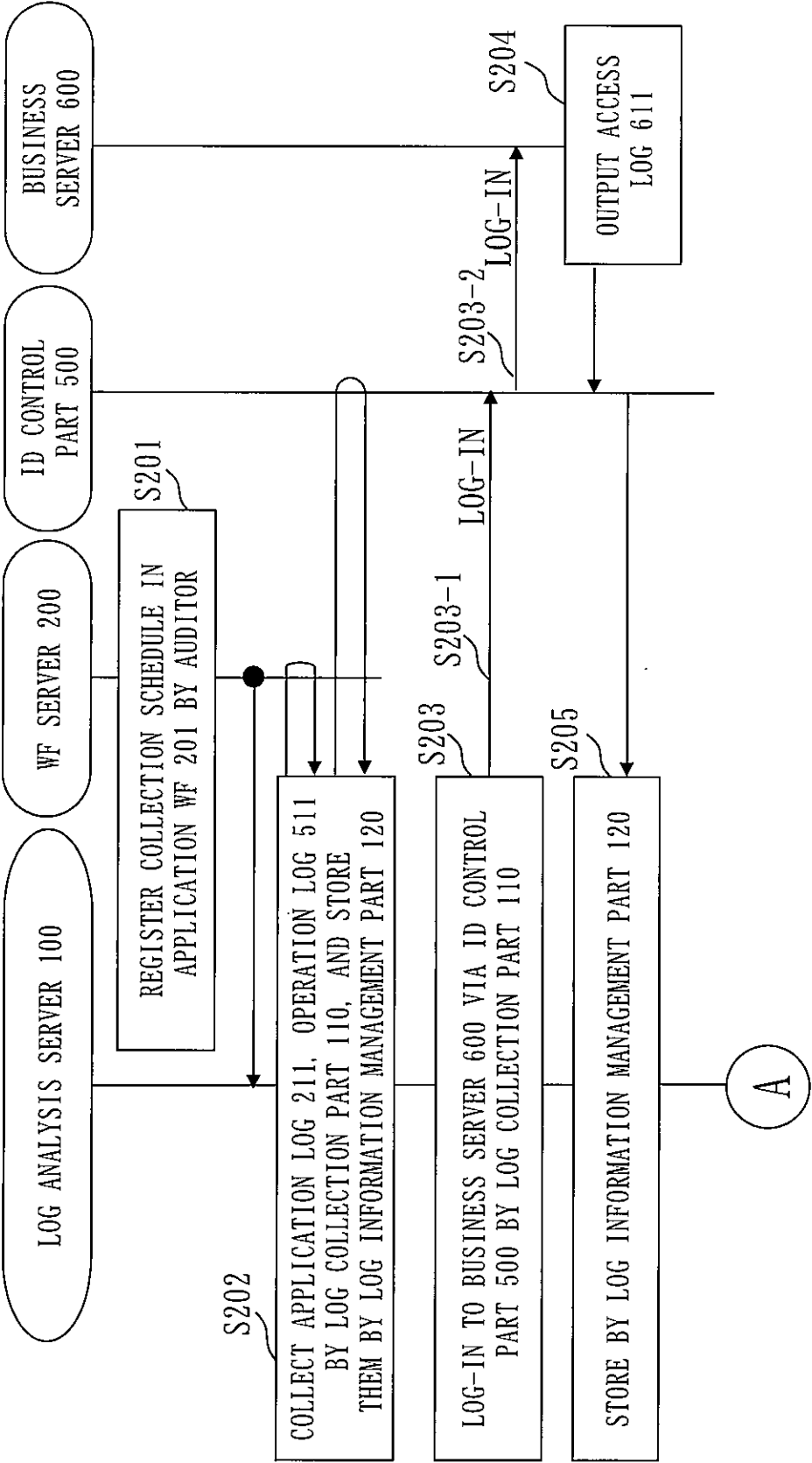


Fig.15

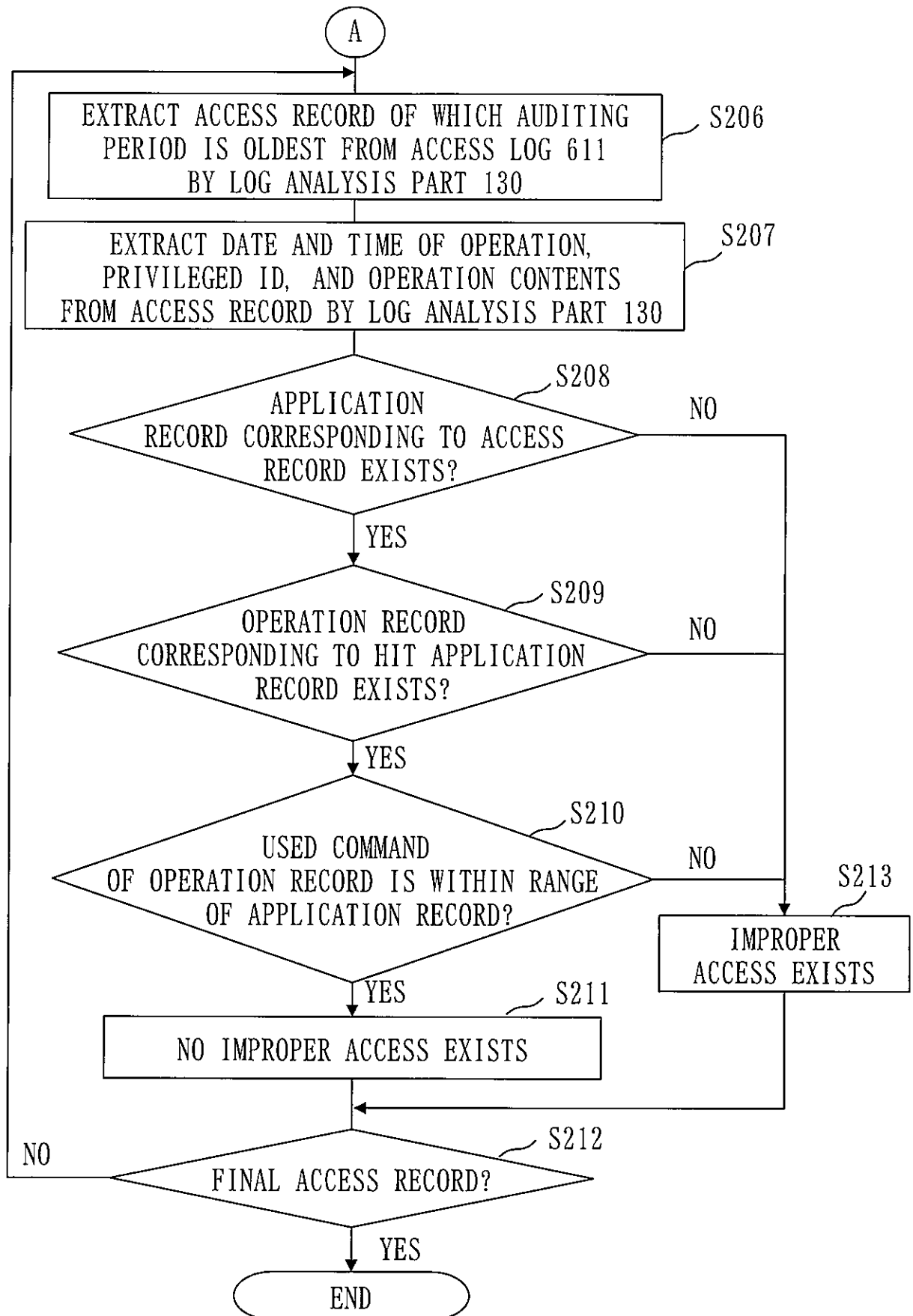


Fig.16

PERSON WHO OPERATES	STATUS	APPLICATION LOG 211	OPERATION LOG 511	ACCESS LOG 611
OPERATOR/LOG ANALYSIS SERVER	PROPER	○	○	○
	IMPROPER (UNAPPLIED)	×	×	×
	IMPROPER (WRONG ROUTE)	○	×	○
EXTERNAL PERPETRATOR	IMPROPER	△*1	×	○

Fig. 17

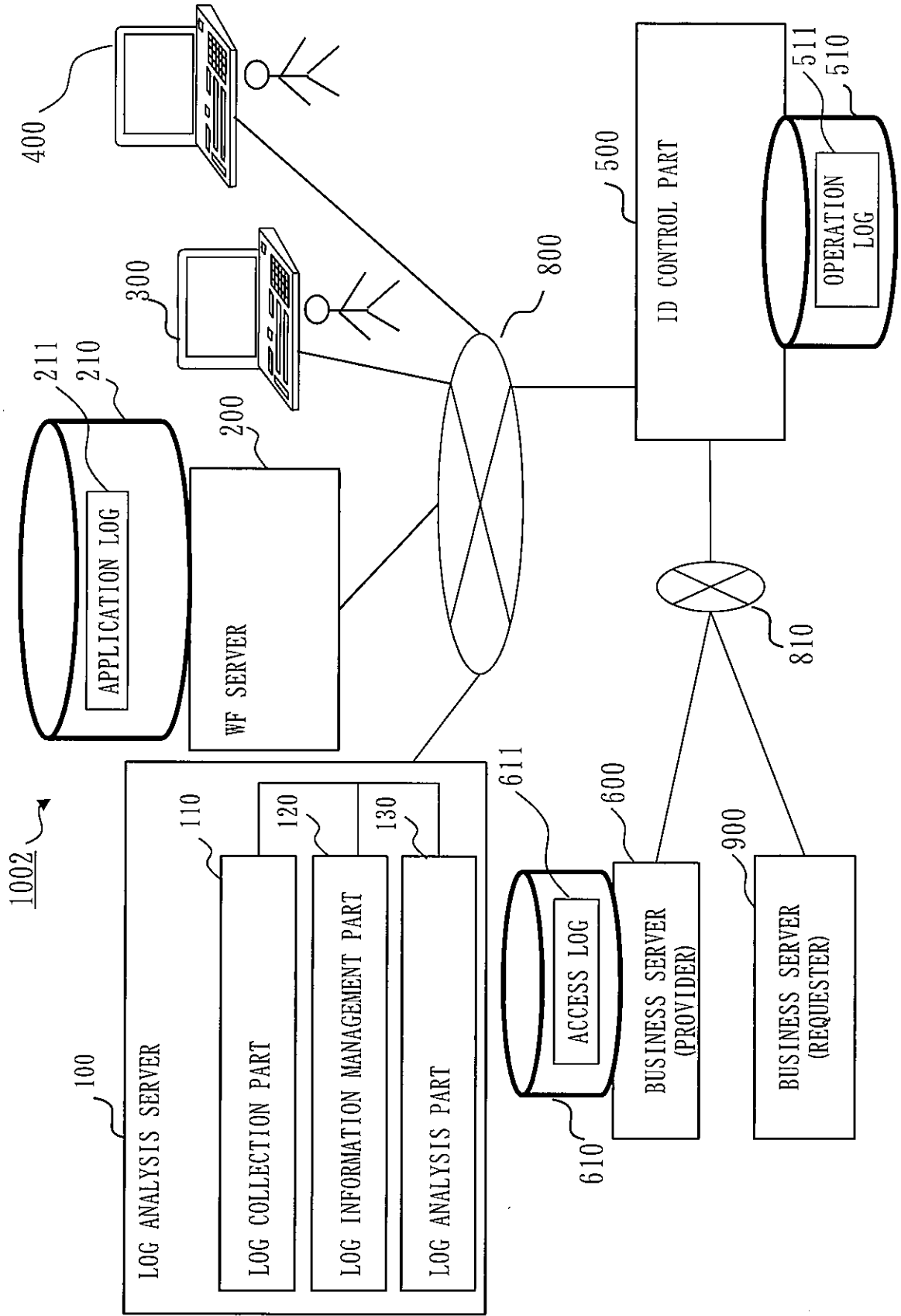


Fig.18

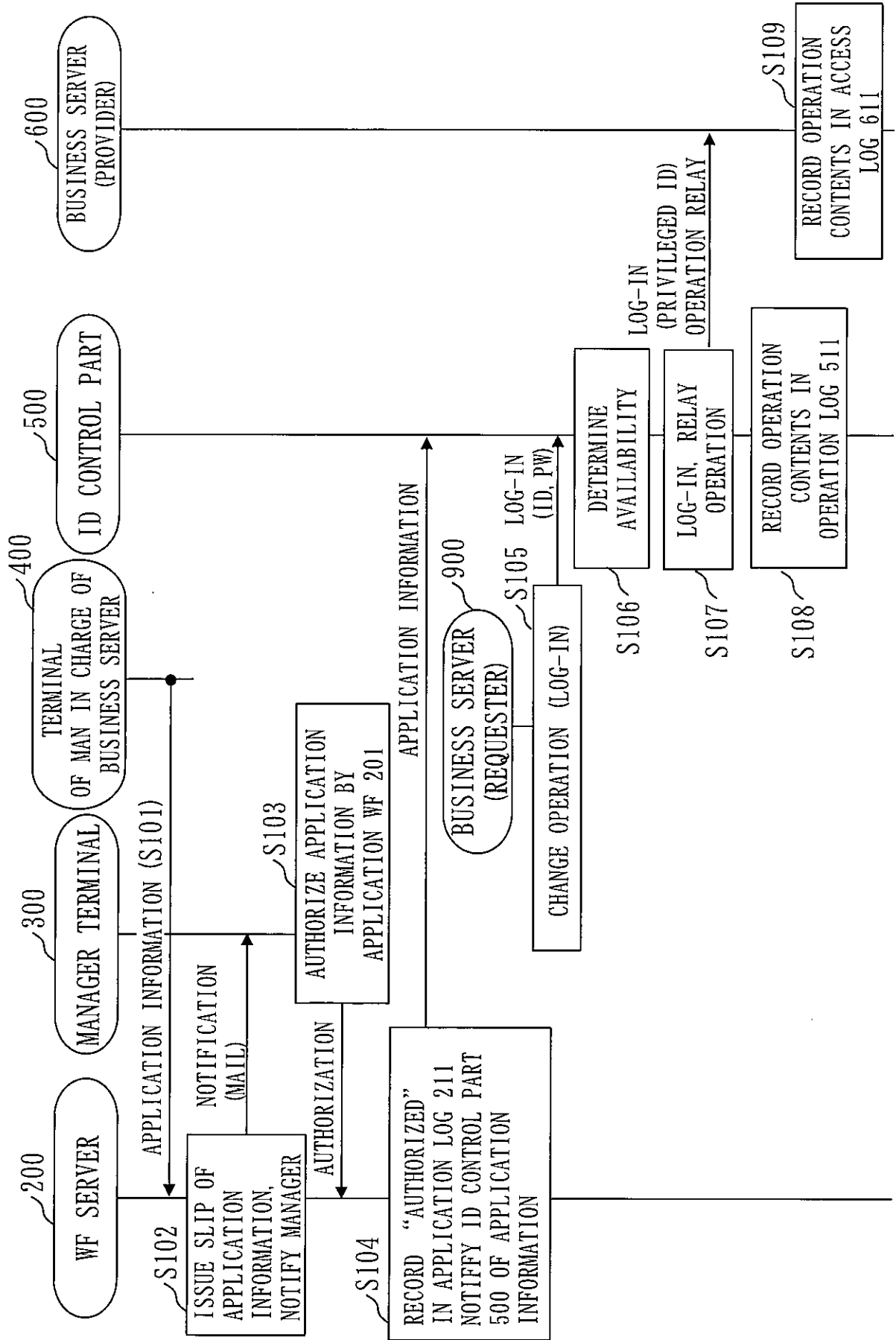


Fig. 19

PERSON WHO OPERATES	STATUS	APPLICATION LOG 211	OPERATION LOG 511	ACCESS LOG 611
OPERATOR/BUSINESS SERVER (REQUESTER)	PROPER	○	○	○
	IMPROPER (UNAPPLIED)	×	×	×
	IMPROPER (WRONG ROUTE)	○	×	○
EXTERNAL PERPETRATOR	IMPROPER	△*1	×	○

Fig. 20

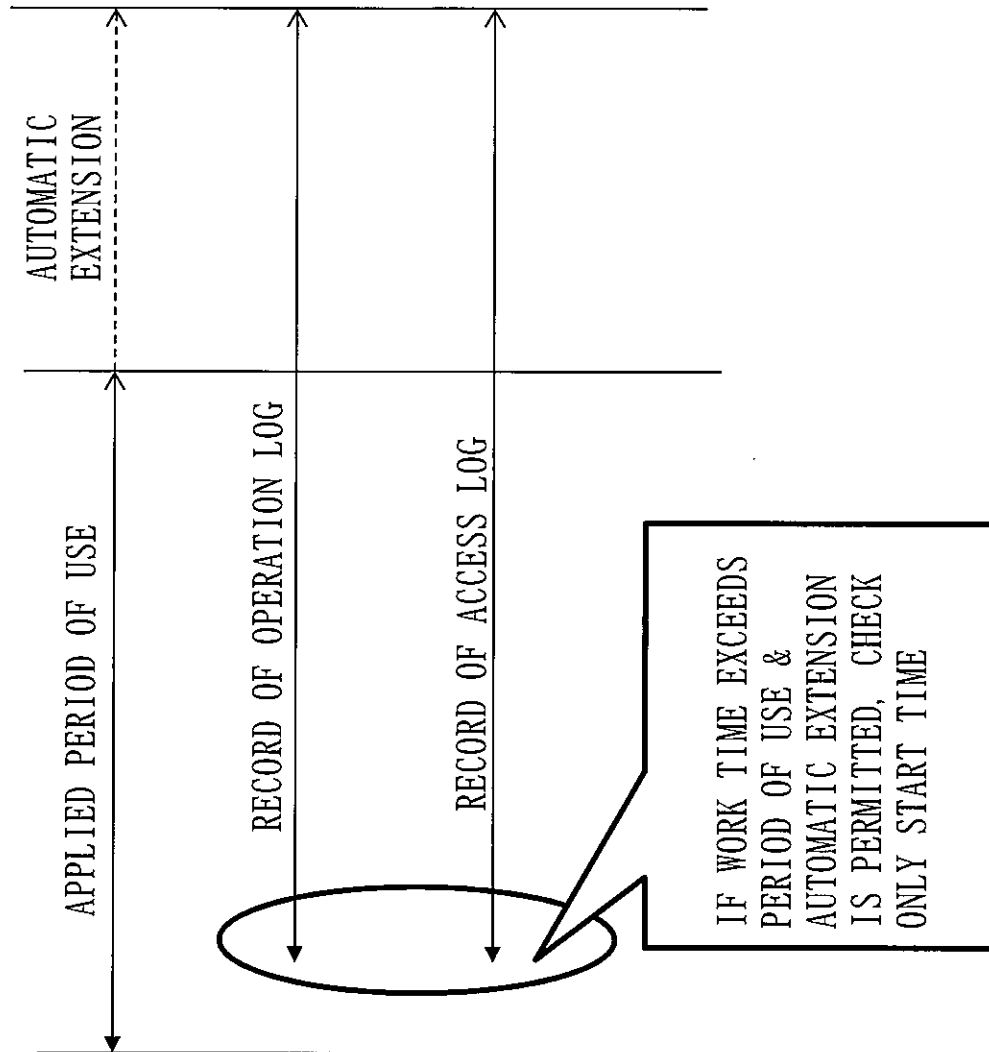


Fig. 21

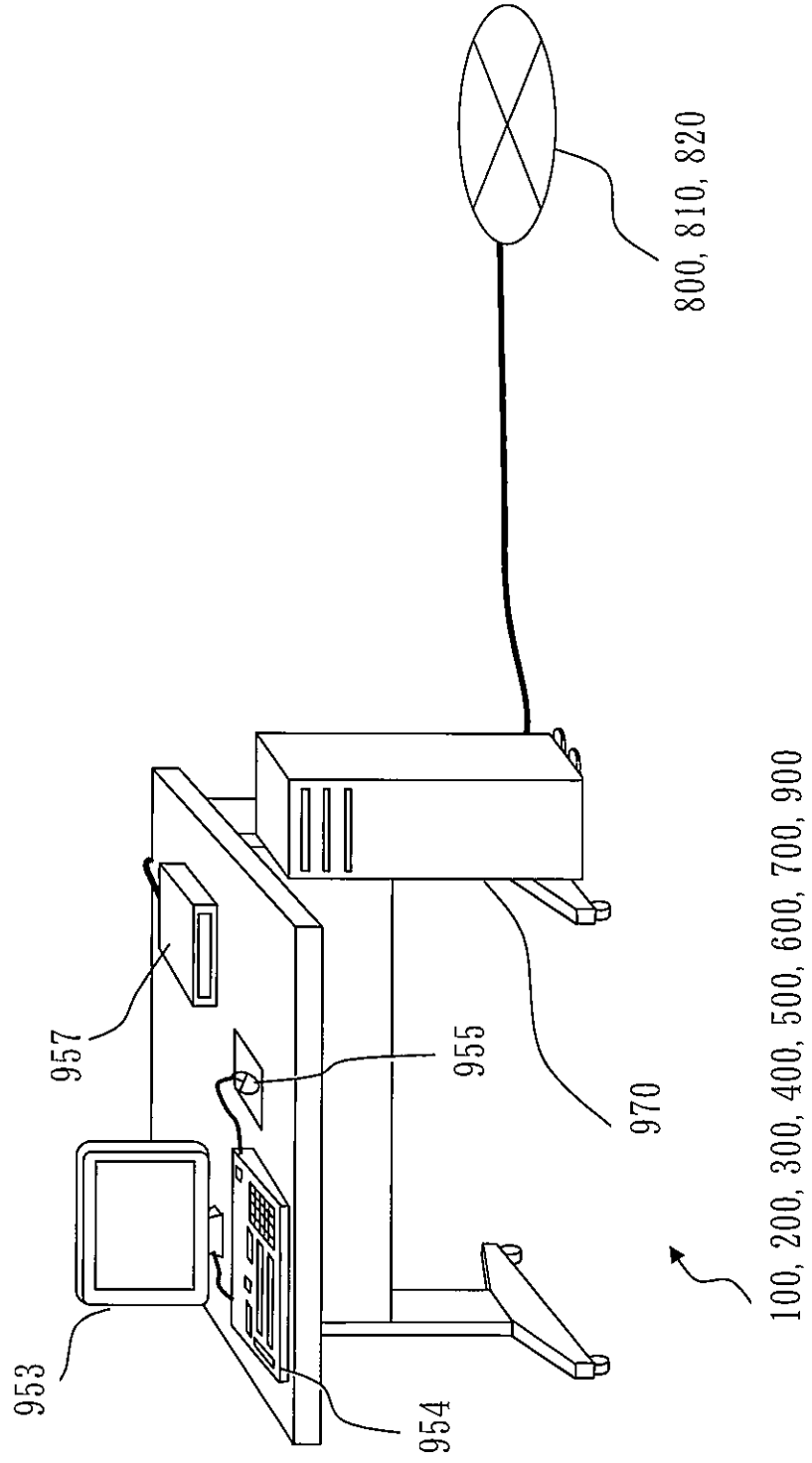


Fig. 22

100, 200, 300, 400, 500, 600, 700, 900

