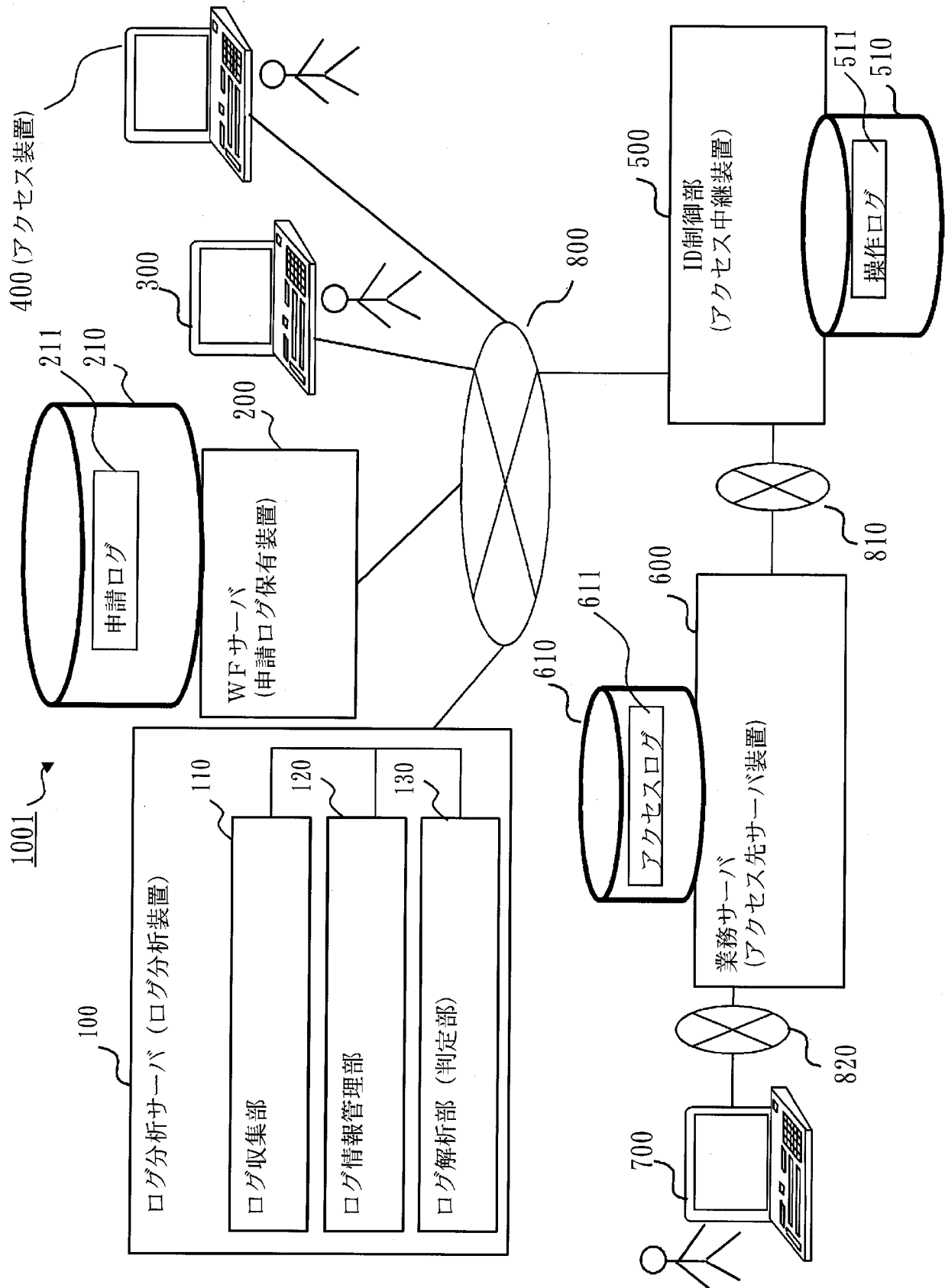
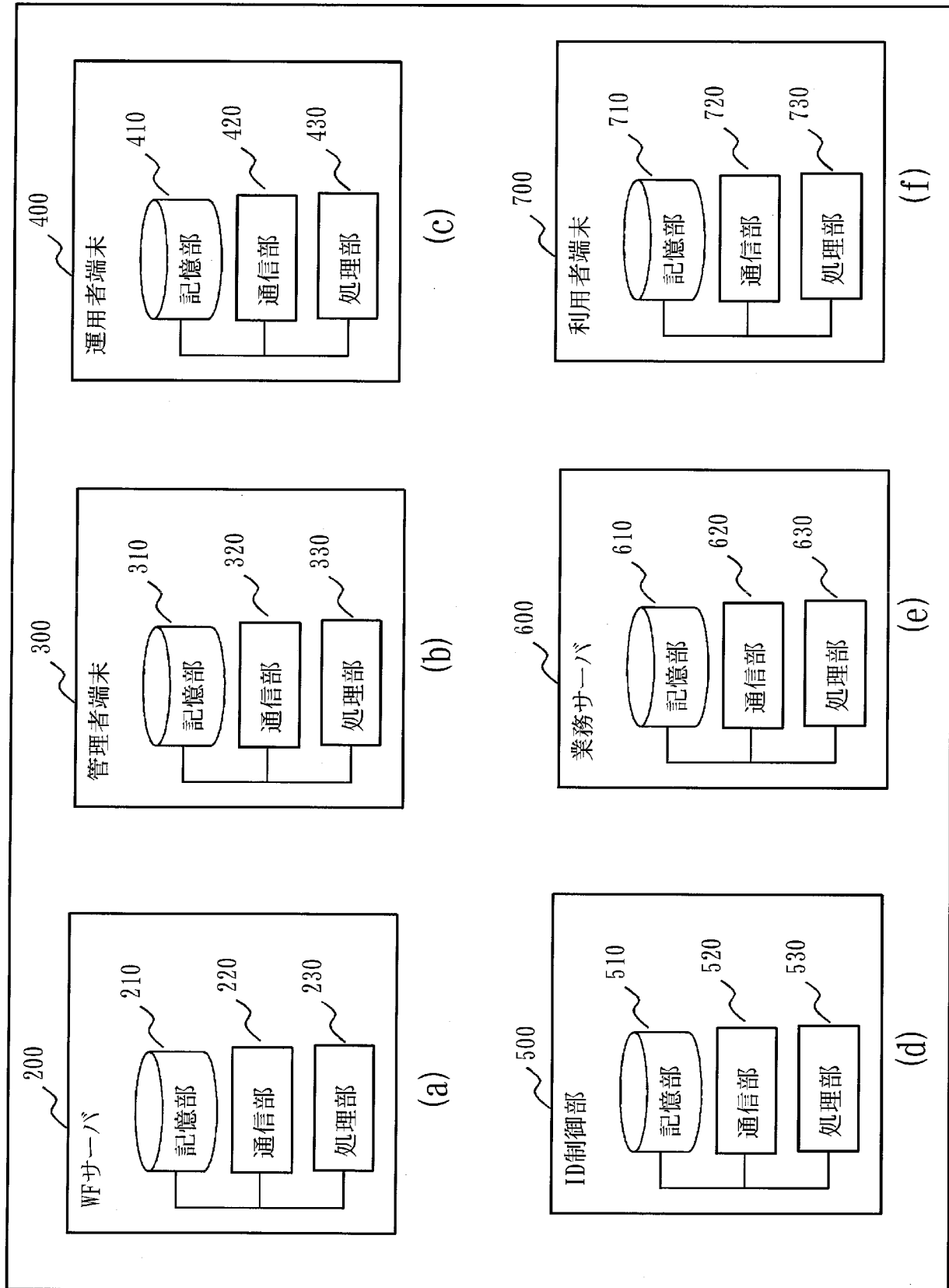


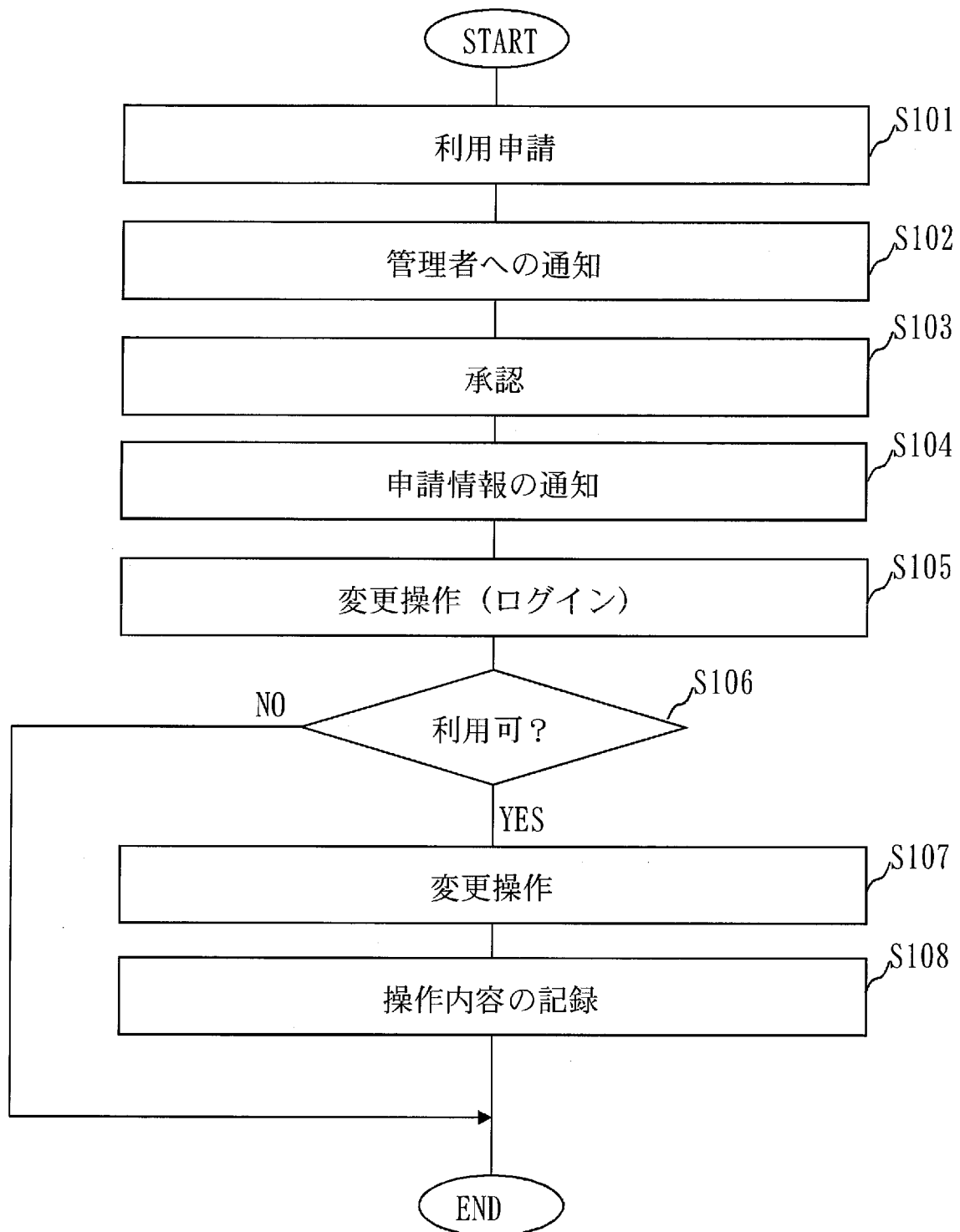
[図1]



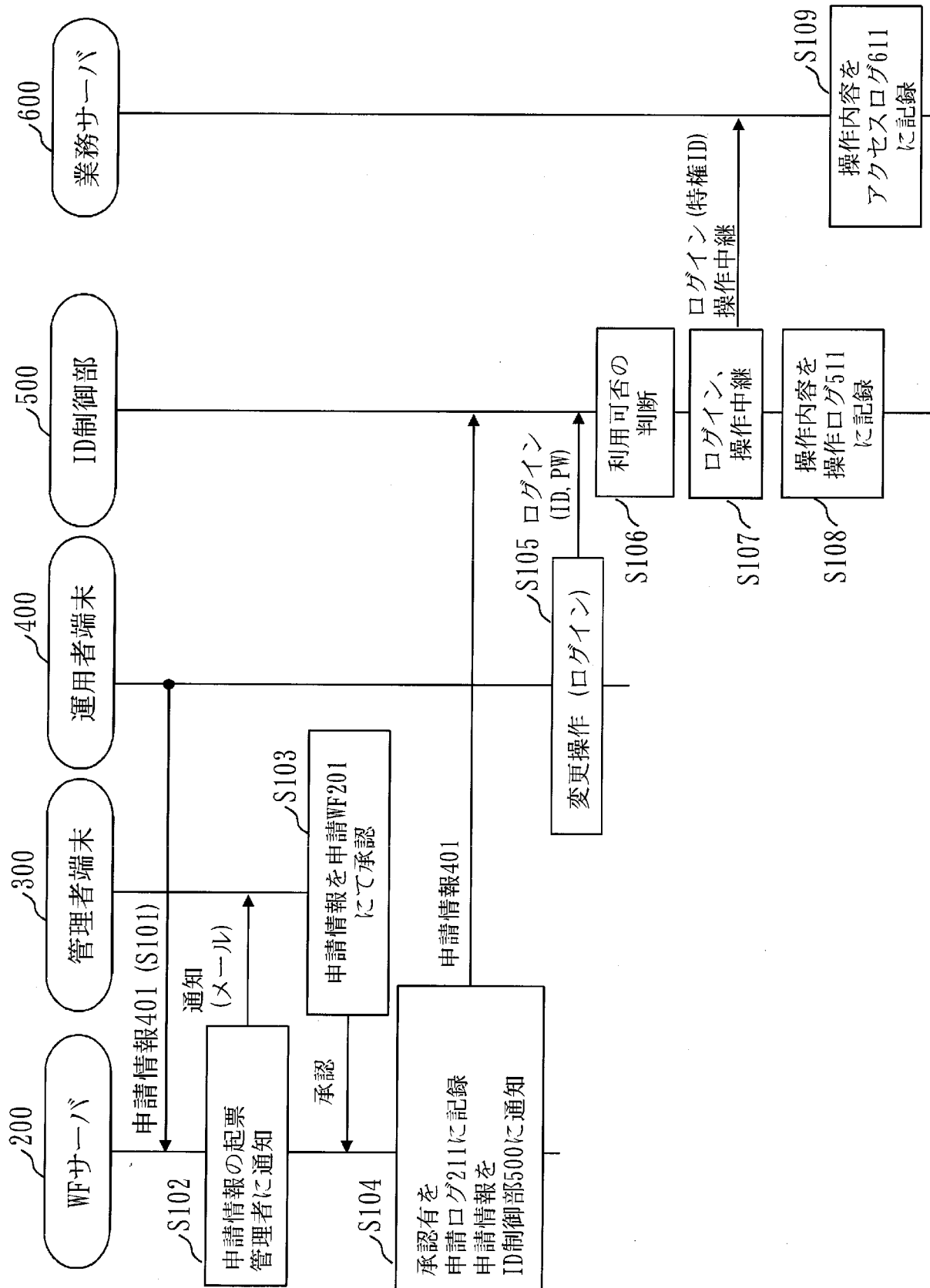
[図2]



[図3]



[図4]



[図5]

401

項目	内容
11 特権ID	業務サーバに対してログインするアカウント
12 利用者情報	運用者Yを識別する識別子
13 業務サーバ識別子	ログインする業務サーバのホスト名などの識別子
14 利用期間	申請内容に従った操作の実施予定の期間
15 利用予定コマンド／ プロトコル	業務サーバにアクセスするプロトコル。 業務サーバへの実行予定の作業（コマンド）

[図6]

401

11	項目	
12	特権ID	Admin01
13	利用者情報	Takanashi
14	業務サーバ	Host01
15	利用期間	2014/01/01 08:00:00 to 2014/01/01 13:00:00
	利用予定コマンド/ プロトコル	RDP

[図7]

211

項目	内容
11 特権ID	業務サーバに対してログインするアカウント
12 利用者情報	運用者を識別するためのIDなど
13 業務サーバ	ログインする業務サーバのホスト名などの識別子
14 利用期間	申請内容に従った操作を、いつからいつまでの予定で実施するか
15 利用予定コマンド／プロトコル	業務サーバに対して、どのようなプロトコルでアクセスするか。 また、どのような作業（コマンド）を実行するか
16 承認状況	承認済み or 未承認 or 却下

[図8]

211

#特権ID、利用者情報、業務サーバ、利用期間（開始）、利用期間（終了）、
プロトコル、コマンド、承認状態（見出し行）
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 . . . (省略), NG

[図9]

511

項目	内容
11-5 特権ID	業務サーバに対してログインするアカウント
12-5 利用者情報	運用者Yを識別する識別子。
14-5 利用期間	
17-5 操作内容	※利用プロトコルによって異なる telnet等の場合には、利用コマンドを記録 RDPプロトコルの場合には、通過するRDPから画面 イメージ等を記録

[図10]

511

#特権ID、利用者ID、利用開始日時、利用終了日時、プロトコル、操作内容
Admin01, Takanashi, 2014/01/01 08:03:12+0900 (JST), 2014/01/01
10:08:03+0900 (JST), RDP, file://○○○ (操作内容の記録動画へのリンク)

[図11]

611

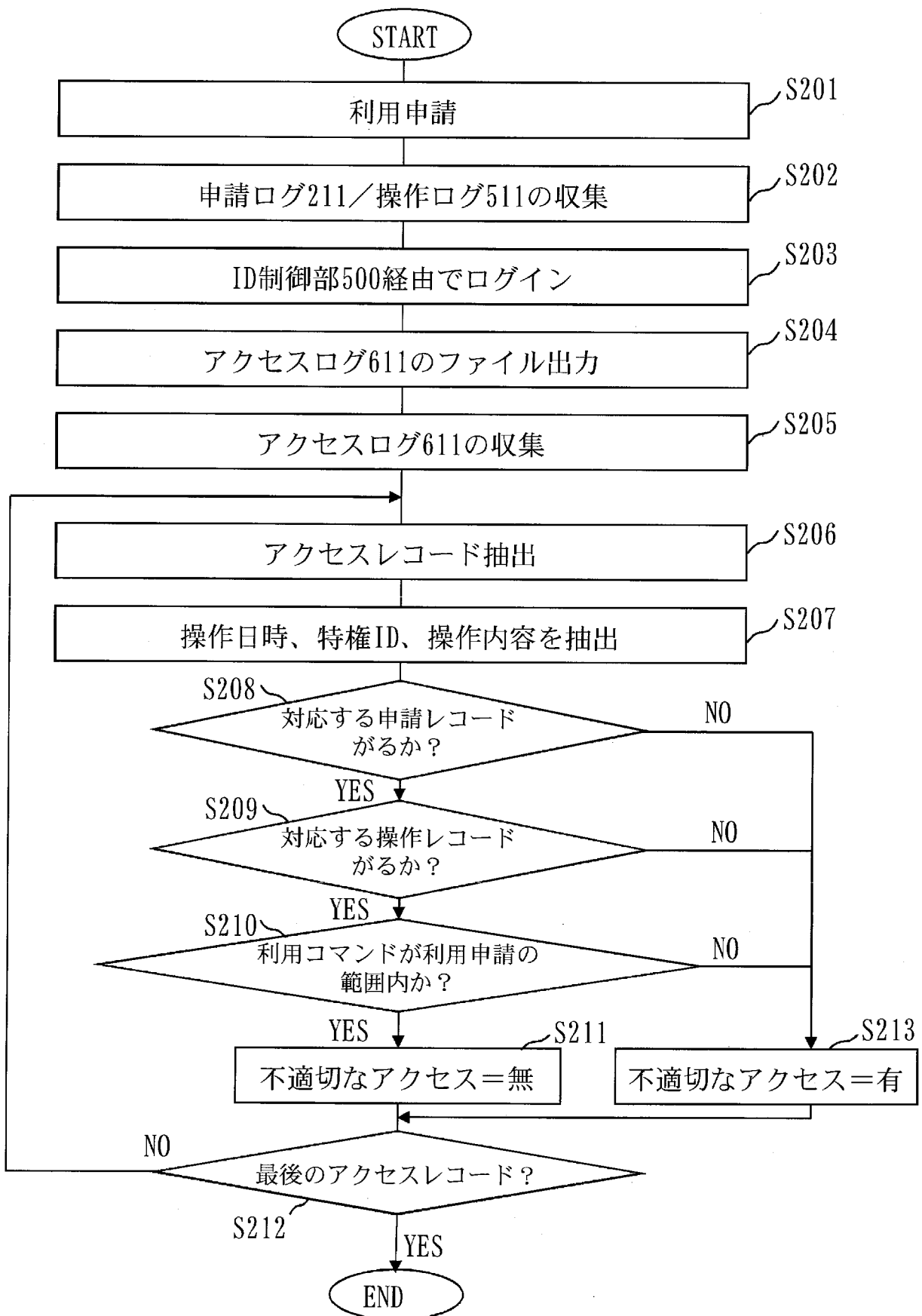
項目	内容
11-6 利用者ID (特権ID)	
17-6 操作内容	ログインなどの操作や、実行したコマンド等の情報
14-6 操作日時	上記の操作を実施した日時

[図12]

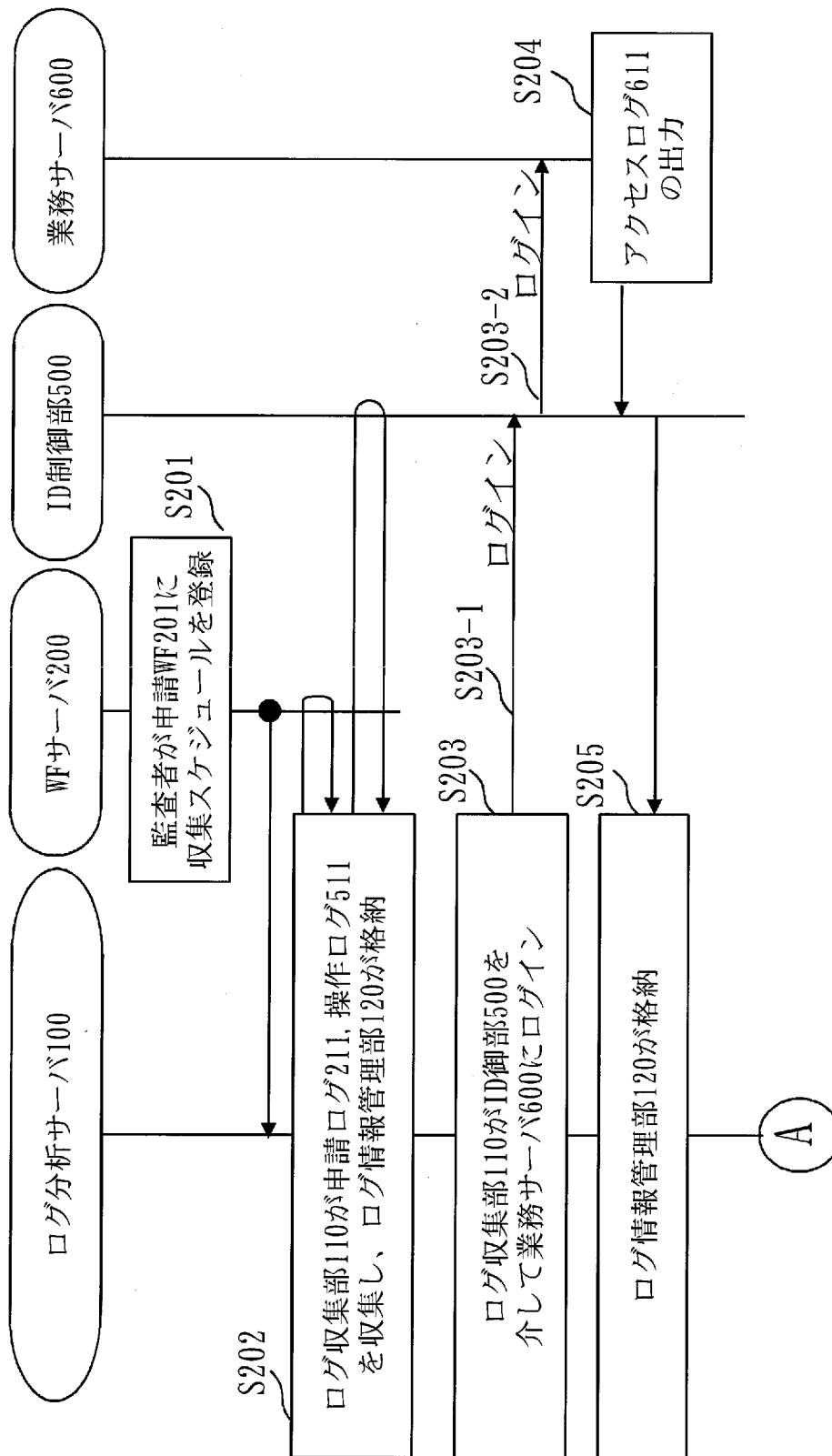
611

#日時 (JST), イベントID, カテゴリ, 詳細
2014/01/01 08:03:14, 0001 (正常にログオンしました), ログオン, Admin . . .
2014/01/01 08:04:19, 0500 (ファイルオープン), ファイルアクセス, Admin ○○
ファイル
2014/01/01 10:08:04, 0002 (正常にログオフしました), ログオン, Admin . . .

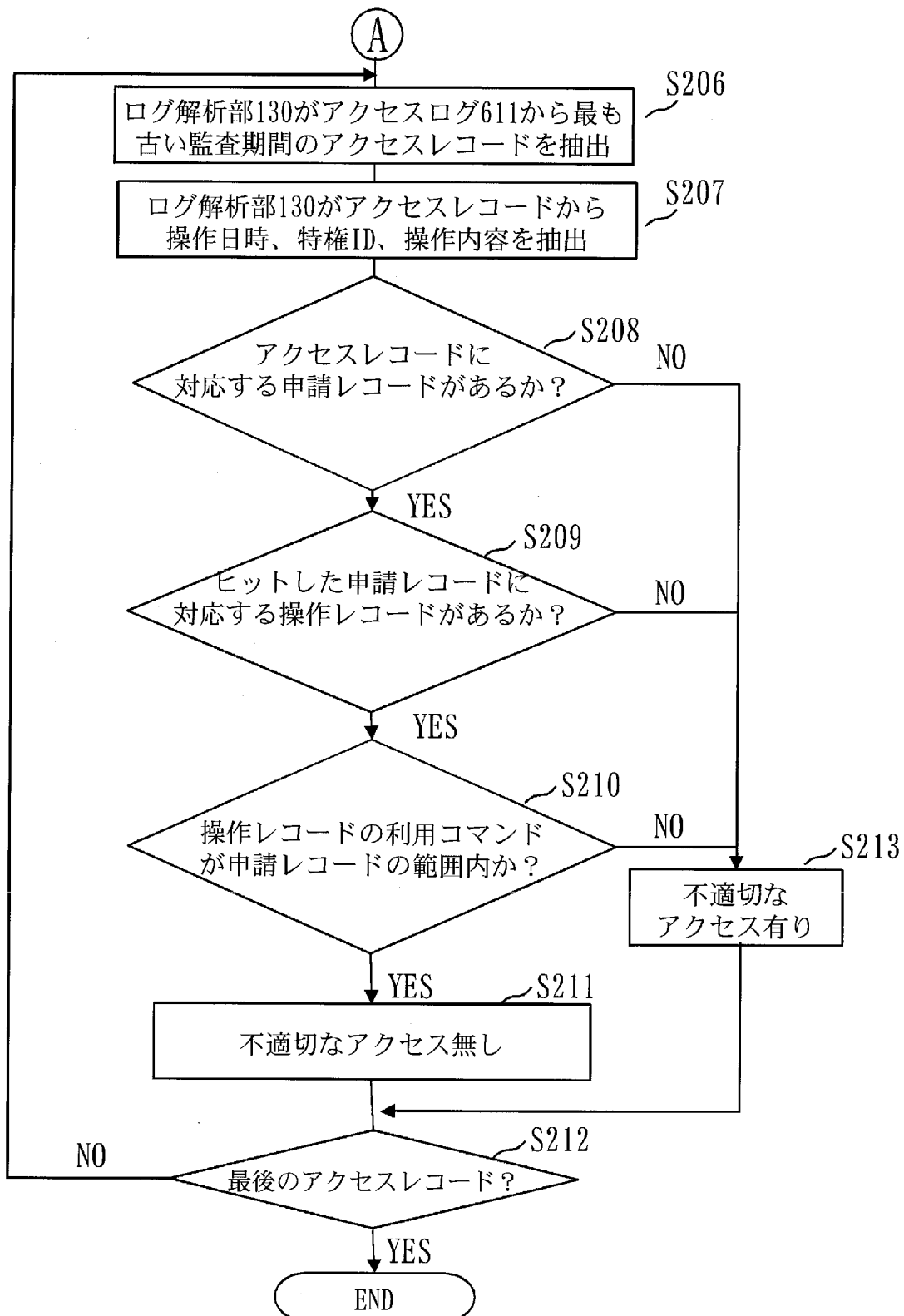
[図13]



[図14]



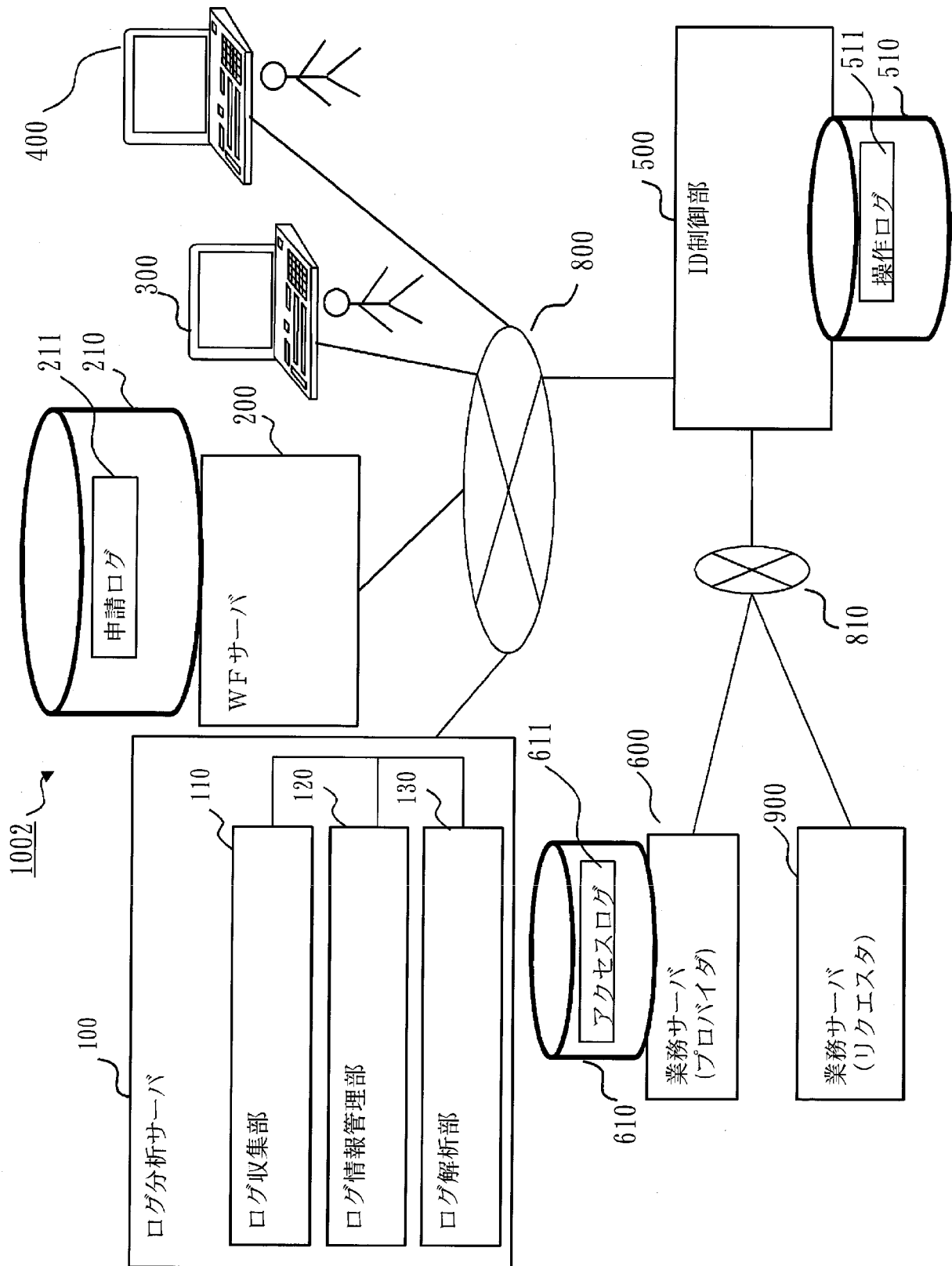
[図15]



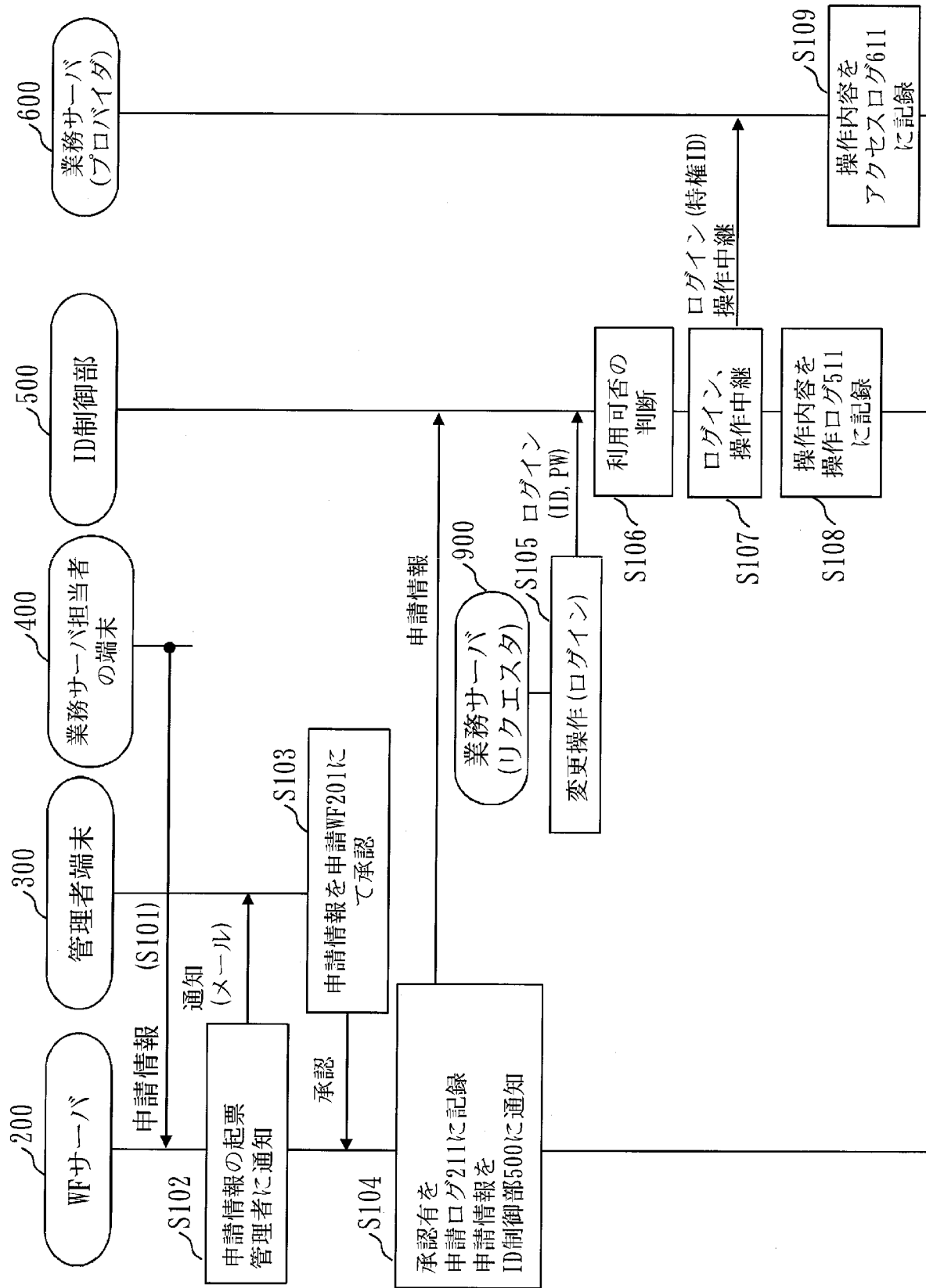
[図16]

操作者	状態	申請ログ211	操作ログ511	アクセスログ611
運用者／ログ 分析サーバ	適切	○	○	○
	不適切（未申請）	×	×	×
	不適切（不正経路）	○	×	○
外部犯行者	不適切	△※1	×	○

[図17]



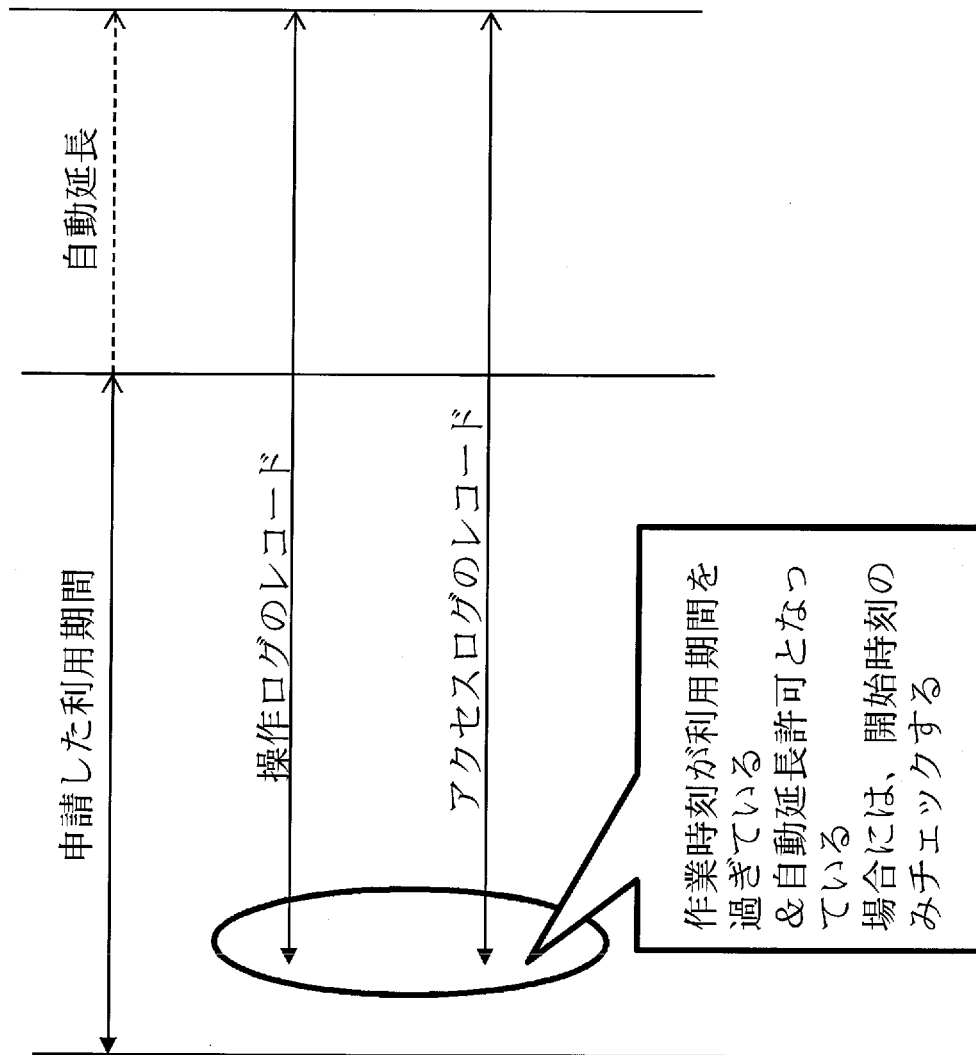
[図18]



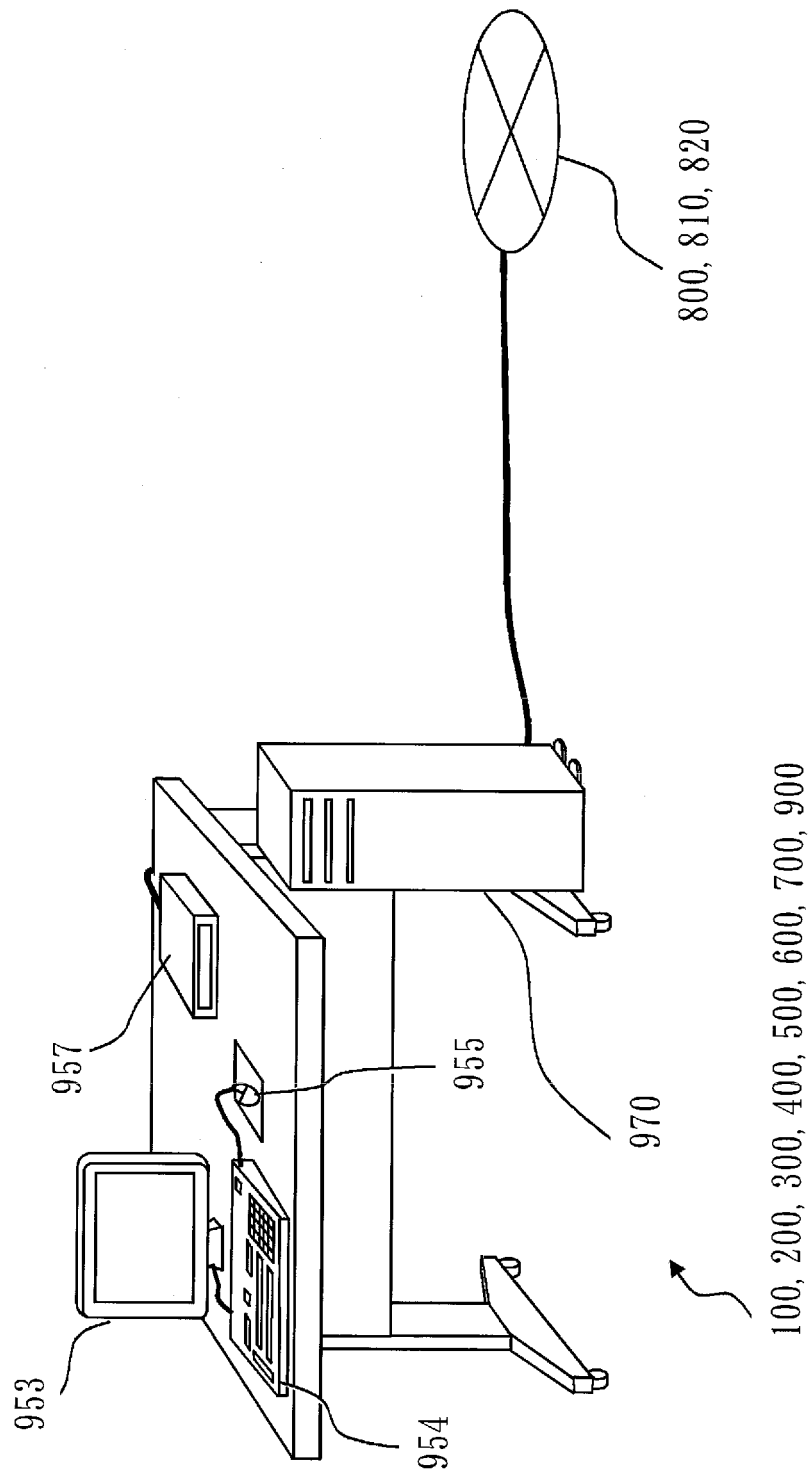
[図19]

操作者	状態	申請ログ211	操作ログ511	アクセスログ611
運用者／ 業務サーバーバ (リクエスタ)	適切	○	○	○
	不適切 (未申請)	×	×	×
	不適切 (不正経路)	○	×	○
	不適切	△※1	×	○
外部犯行者				

[図20]



[図21]



[図22]

