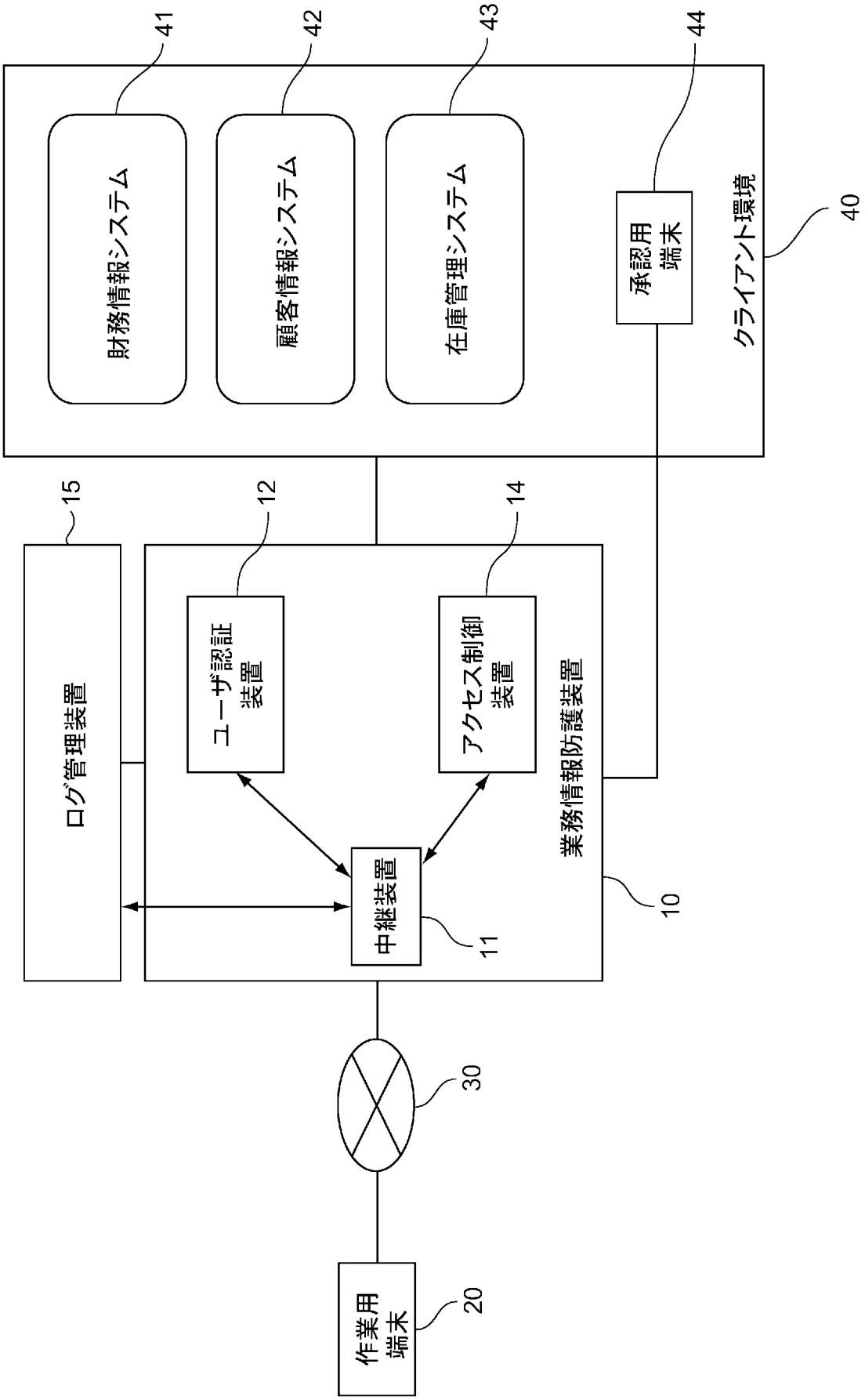
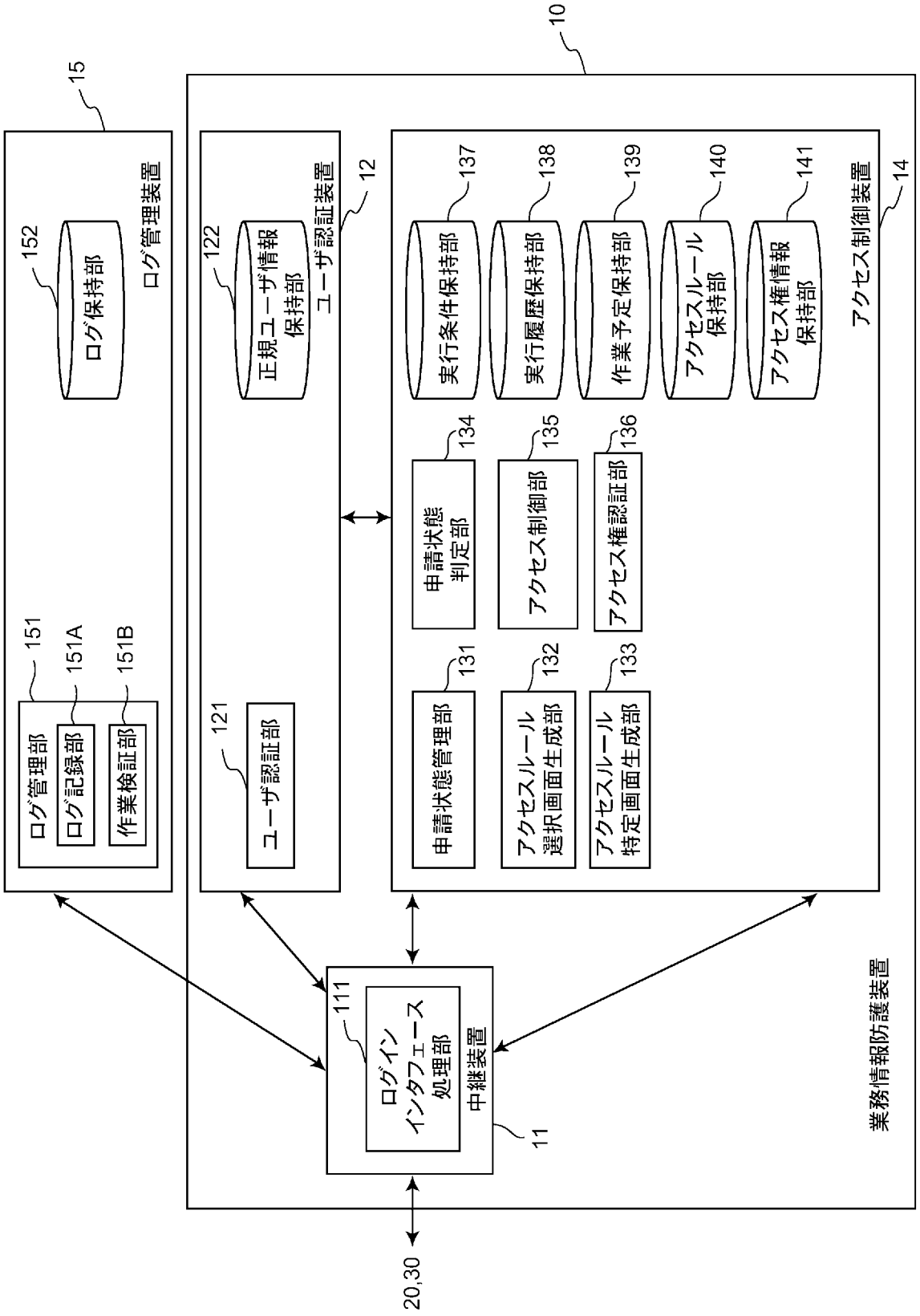
[図1]


41
42
43
44
財務情報システム
顧客情報システム
在庫管理システム
承認用端末
クライアント環境
40
15
12
14
ログ管理装置
ユーザ認証装置
アクセス制御装置
業務情報防護装置
中継装置
11
10
30
作業用端末
20

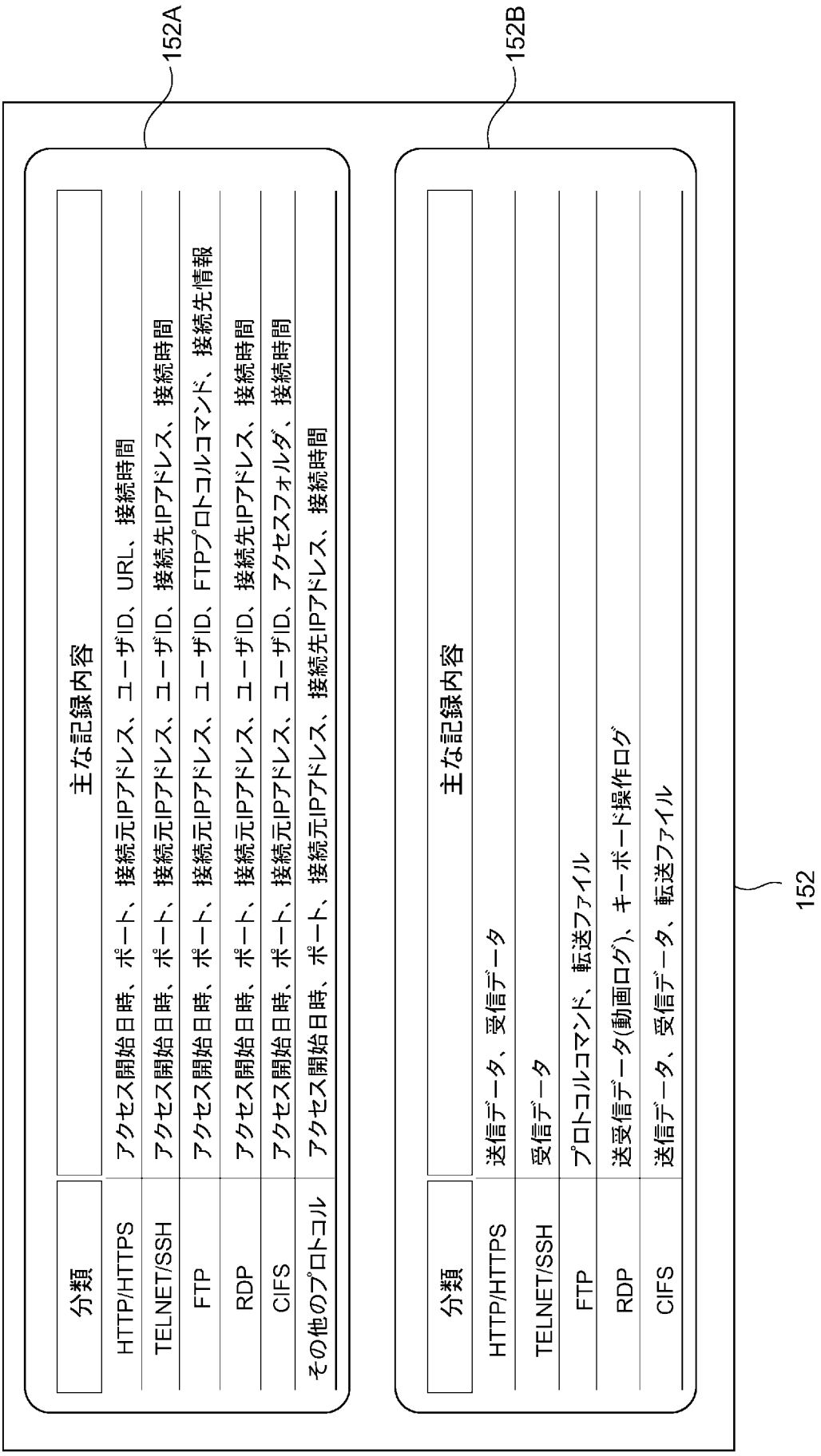
[図2]


10
15
ログ管理装置
152
ログ保持部
151
ログ管理部
151A
ログ記録部
151B
作業検証部
12
ユーザ認証装置
122
正規ユーザ情報保持部
121
ユーザ認証部
14
アクセス制御装置
137
実行条件保持部
138
実行履歴保持部
139
作業予定保持部
140
アクセスルール保持部
141
アクセス権情報保持部
134
申請状態判定部
135
アクセス制御部
136
アクセス権認証部
131
申請状態管理部
132
アクセスルール選択画面生成部
133
アクセスルール特定画面生成部
111
ログインインタフェース処理部
中継装置
11
業務情報防護装置
20,30

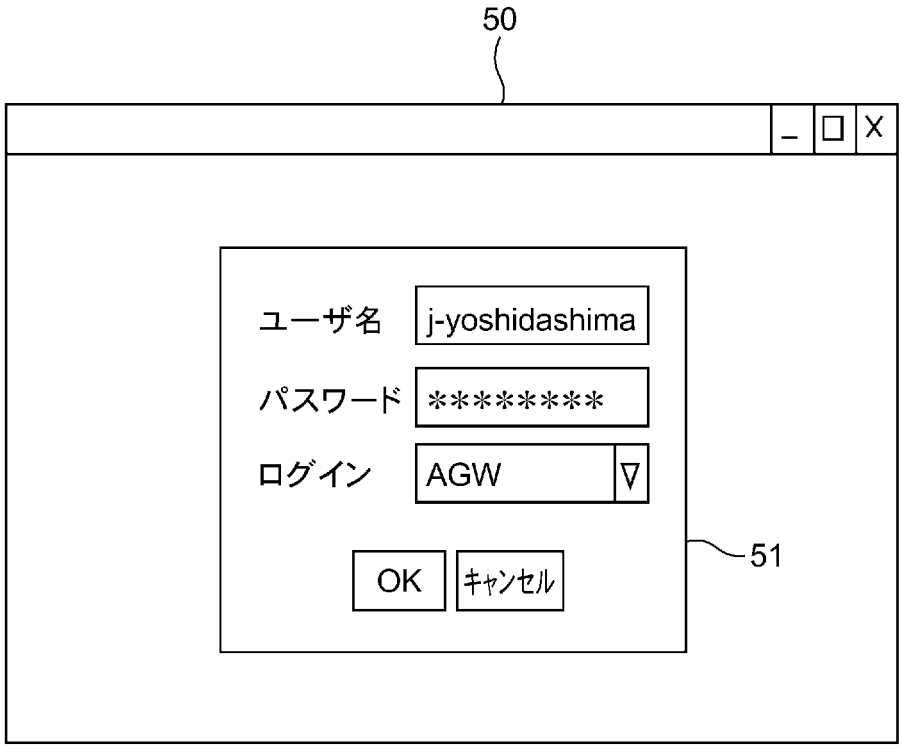
[図3]

137A アクセスルールID	137B 年月日	137C 時間	137D 作業種別	137E 承認要否	137F アクセスルール名
1	営業日	6:00→16:00	01:障害対応 02:調査		アクセスルールA
2	営業日	6:00→16:00	03:稼動監視 04:リリース作業	○ ○	アクセスルールB
3	営業日	16:00→6:00	01:障害対応 02:調査 03:稼動監視 04:リリース作業	○	アクセスルールC
4	2006/9/26	12:00→13:00	03:稼動監視	○	アクセスルールB
5	非営業日	終日	01:障害対応 02:調査 03:稼動監視 04:リリース作業	○	アクセスルールC
⋮	⋮	⋮	⋮	⋮	⋮

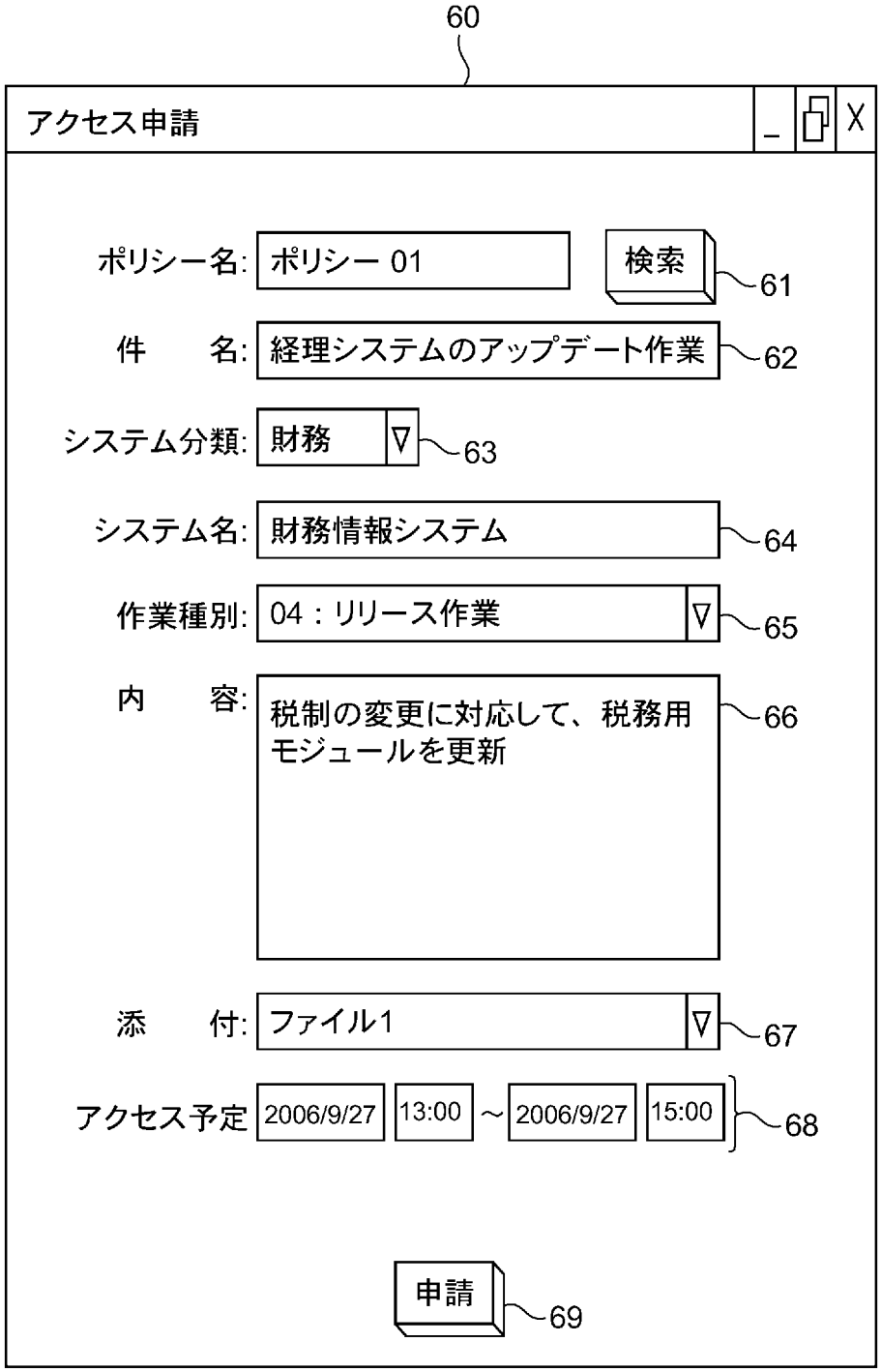
[図4]


152A
152B
152
分類
主な記録内容
HTTP/HTTPS
アクセス開始日時、ポート、接続元IPアドレス、ユーザID、URL、接続時間
TELNET/SSH
アクセス開始日時、ポート、接続元IPアドレス、ユーザID、接続先IPアドレス、接続時間
FTP
アクセス開始日時、ポート、接続元IPアドレス、ユーザID、FTPプロトコルコマンド、接続先情報
RDP
アクセス開始日時、ポート、接続元IPアドレス、ユーザID、接続先IPアドレス、接続時間
CIFS
アクセス開始日時、ポート、接続元IPアドレス、ユーザID、アクセスフォルダ、接続時間
その他のプロトコル
アクセス開始日時、ポート、接続元IPアドレス、接続先IPアドレス、接続時間
分類
主な記録内容
HTTP/HTTPS
送信データ、受信データ
TELNET/SSH
受信データ
FTP
プロトコルコマンド、転送ファイル
RDP
送受信データ(動画ログ)、キーボード操作ログ
CIFS
送信データ、受信データ、転送ファイル

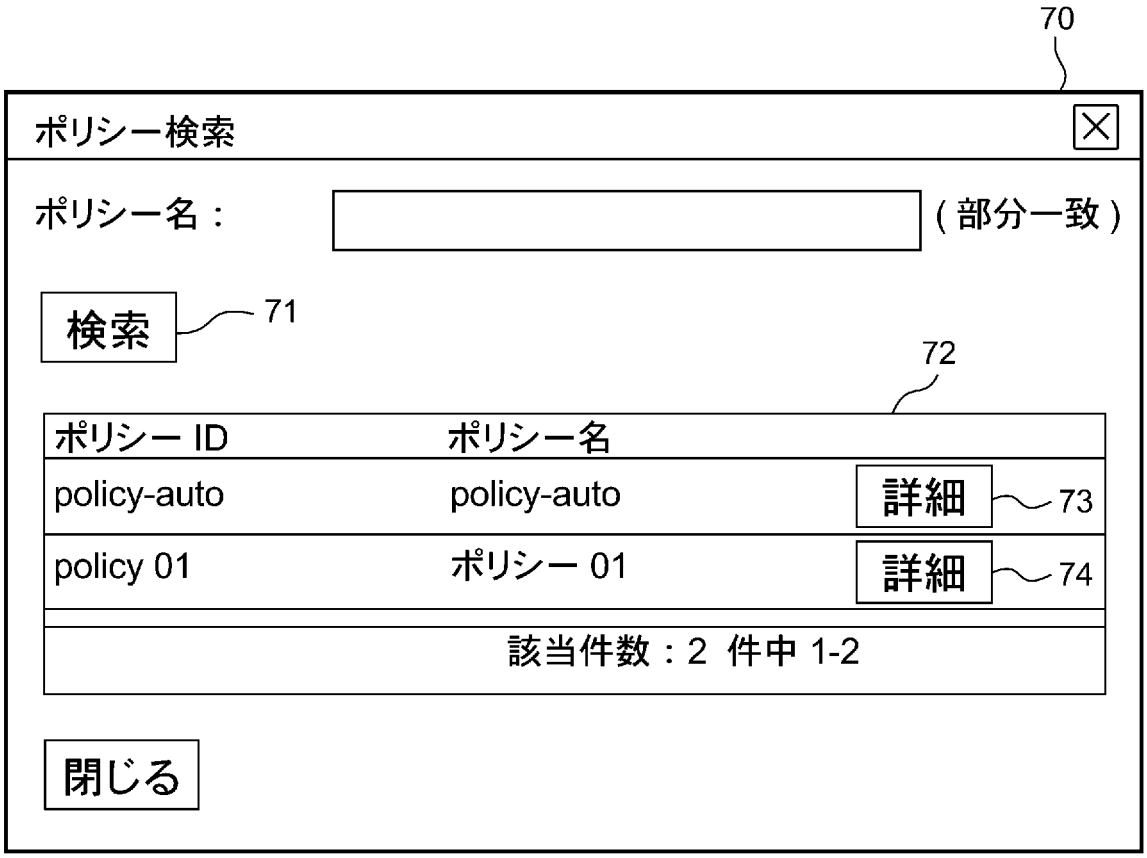
[図5]



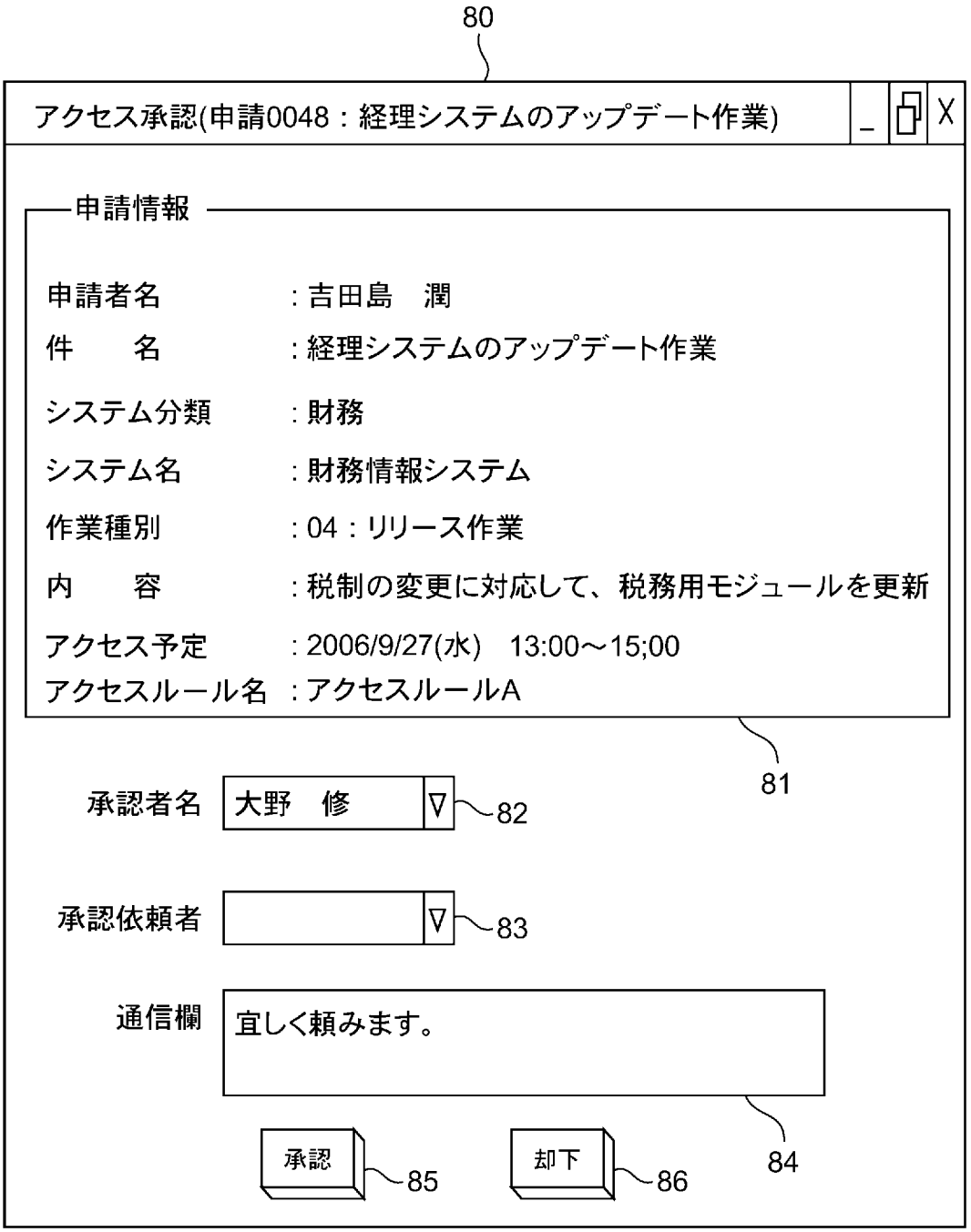
[図6]


60
アクセス申請
ポリシー名:
ポリシー 01
検索
61
件　　名:
経理システムのアップデート作業
62
システム分類:
財務
63
システム名:
財務情報システム
64
作業種別:
04：リリース作業
65
内　　容:
税制の変更に対応して、税務用モジュールを更新
66
添　　付:
ファイル1
67
アクセス予定
2006/9/27
13:00
～
2006/9/27
15:00
68
申請
69

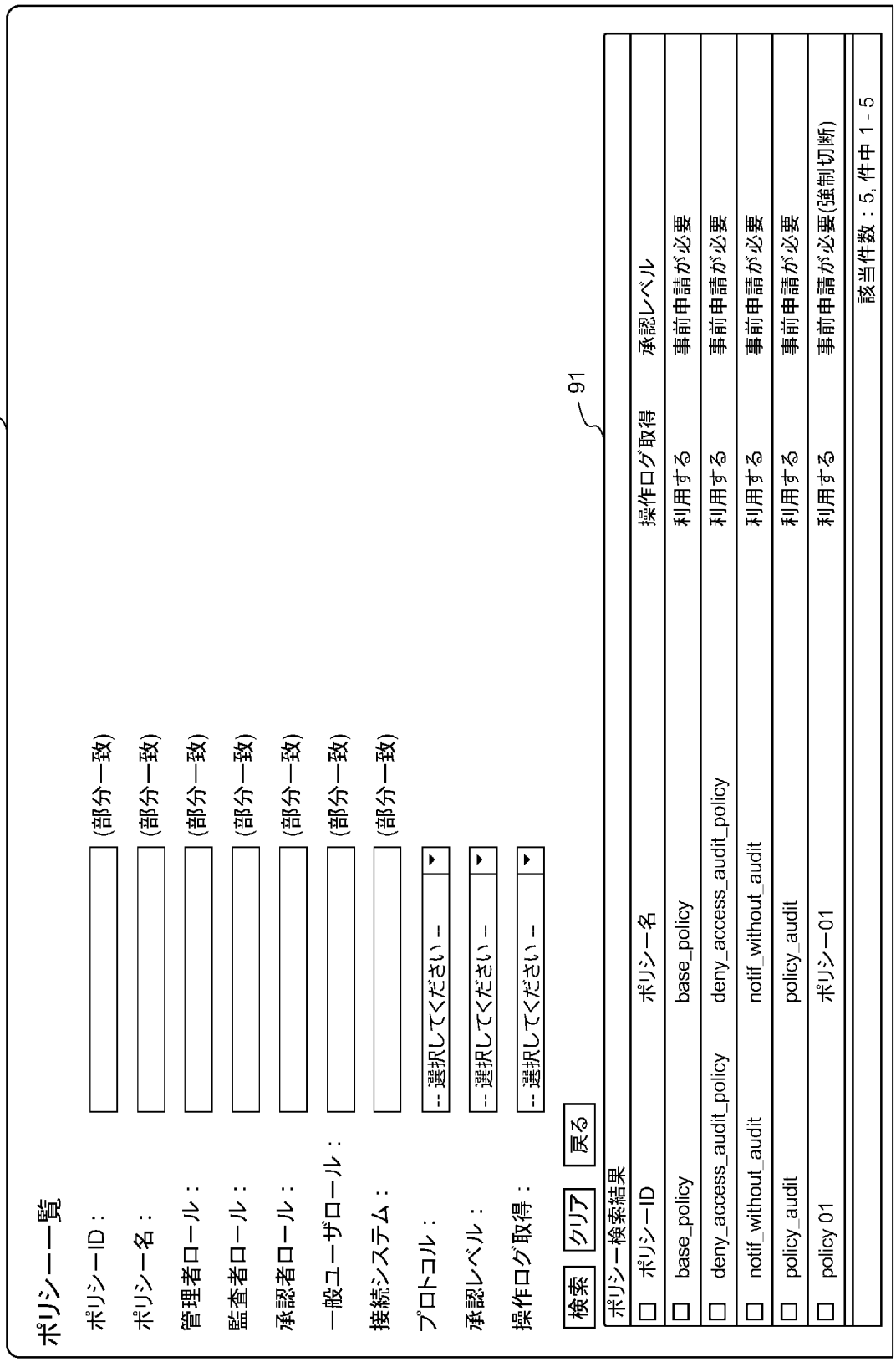
[図7]


70
ポリシー検索
ポリシー名：
（部分一致）
検索
71
72
ポリシー ID
ポリシー名
policy-auto
policy-auto
詳細
73
policy 01
ポリシー 01
詳細
74
該当件数：2 件中 1-2
閉じる

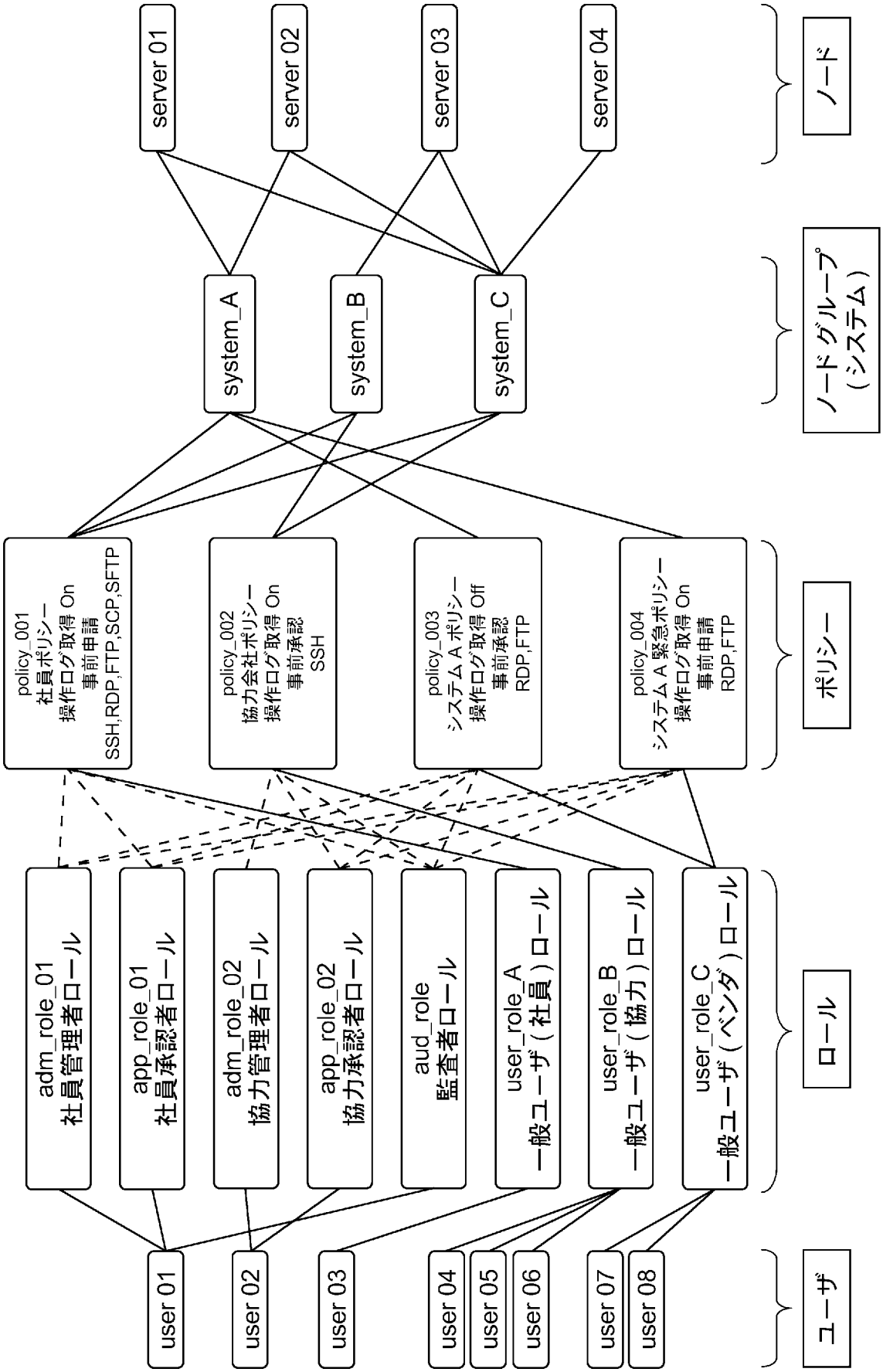
[図8]


80
アクセス承認(申請0048：経理システムのアップデート作業)
申請情報
申請者名 ：吉田島　潤
件　　名 ：経理システムのアップデート作業
システム分類 ：財務
システム名 ：財務情報システム
作業種別 ：04：リリース作業
内　　容 ：税制の変更に対応して、税務用モジュールを更新
アクセス予定 ：2006/9/27(水)　13:00～15;00
アクセスルール名 ：アクセスルールA
81
承認者名
大野　修
82
承認依頼者
83
通信欄
宜しく頼みます。
84
承認
85
却下
86

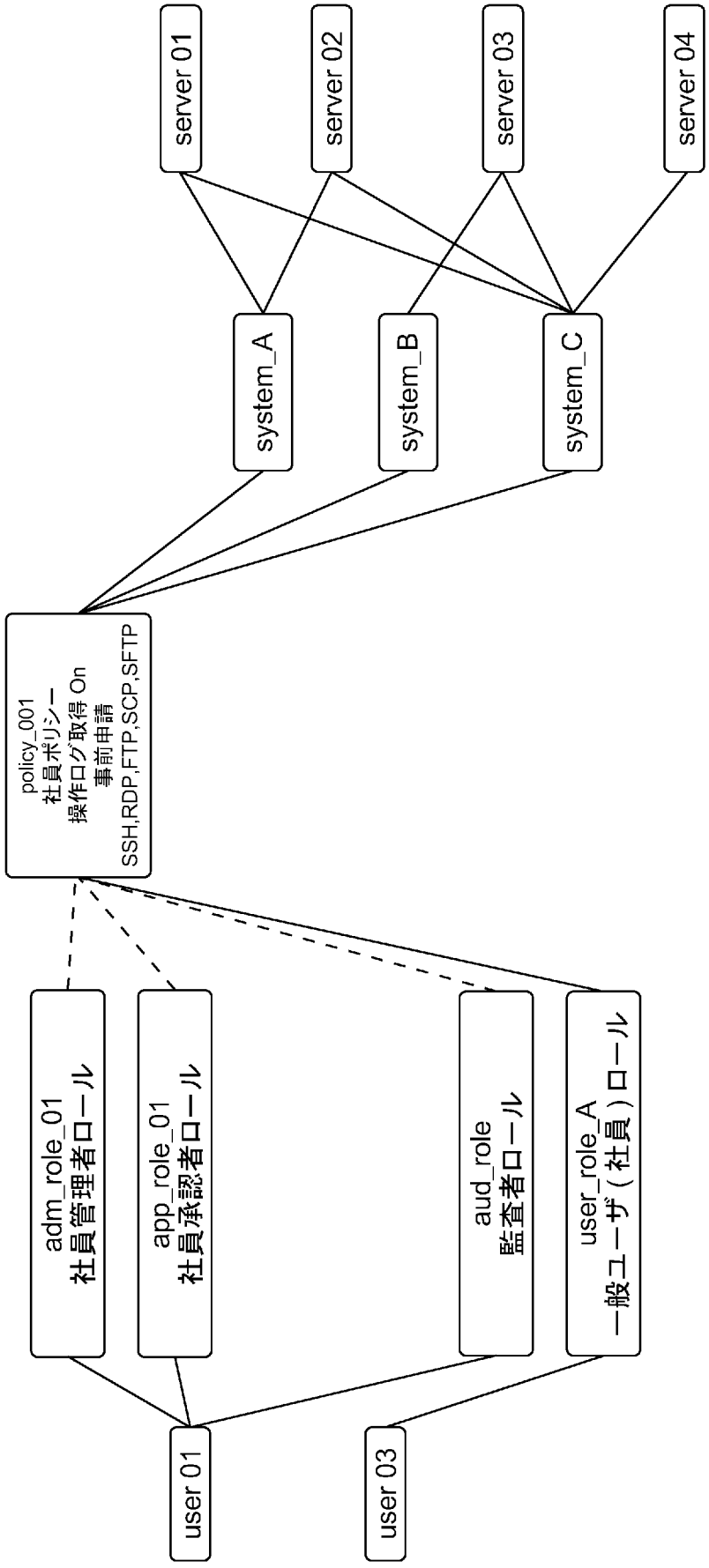
[図9]


90
ポリシー一覧
ポリシーID：
(部分一致)
ポリシー名：
(部分一致)
管理者ロール：
(部分一致)
監査者ロール：
(部分一致)
承認者ロール：
(部分一致)
一般ユーザロール：
(部分一致)
接続システム：
(部分一致)
プロトコル：
-- 選択してください --
承認レベル：
-- 選択してください --
操作ログ取得：
-- 選択してください --
検索
クリア
戻る
91
ポリシー検索結果
ポリシーID
ポリシー名
操作ログ取得
承認レベル
base_policy
base_policy
利用する
事前申請が必要
deny_access_audit_policy
deny_access_audit_policy
利用する
事前申請が必要
notif_without_audit
notif_without_audit
利用する
事前申請が必要
policy_audit
policy_audit
利用する
事前申請が必要
policy 01
ポリシー01
利用する
事前申請が必要(強制切断)
該当件数：5, 件中 1 - 5

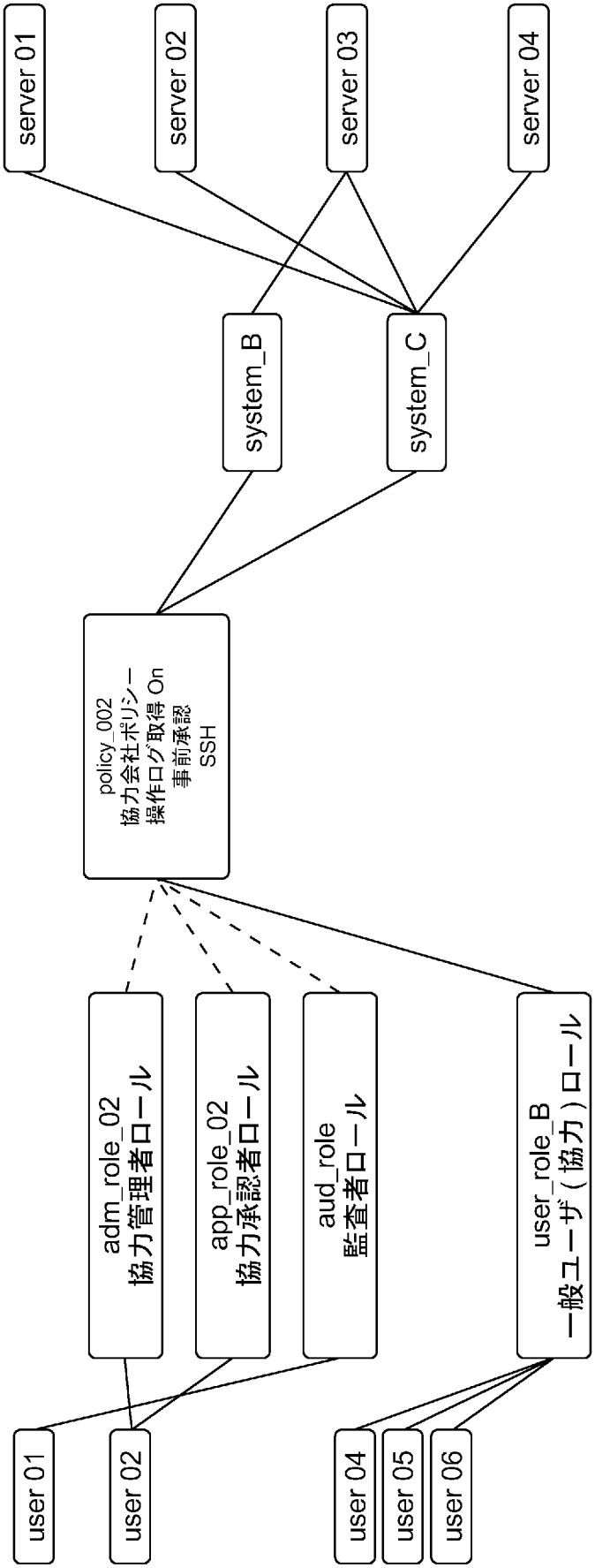
[図10]


server 01
server 02
server 03
server 04
ノード
system_A
system_B
system_C
ノードグループ（システム）
policy_001
社員ポリシー
操作ログ取得 On
事前申請
SSH,RDP,FTP,SCP,SFTP
policy_002
協力会社ポリシー
操作ログ取得 On
事前承認
SSH
policy_003
システムＡポリシー
操作ログ取得 Off
事前承認
RDP,FTP
policy_004
システムＡ緊急ポリシー
操作ログ取得 On
事前申請
RDP,FTP
ポリシー
adm_role_01
社員管理者ロール
app_role_01
社員承認者ロール
adm_role_02
協力管理者ロール
app_role_02
協力承認者ロール
aud_role
監査者ロール
user_role_A
一般ユーザ（社員）ロール
user_role_B
一般ユーザ（協力）ロール
user_role_C
一般ユーザ（ベンダ）ロール
ロール
user 01
user 02
user 03
user 04
user 05
user 06
user 07
user 08
ユーザ

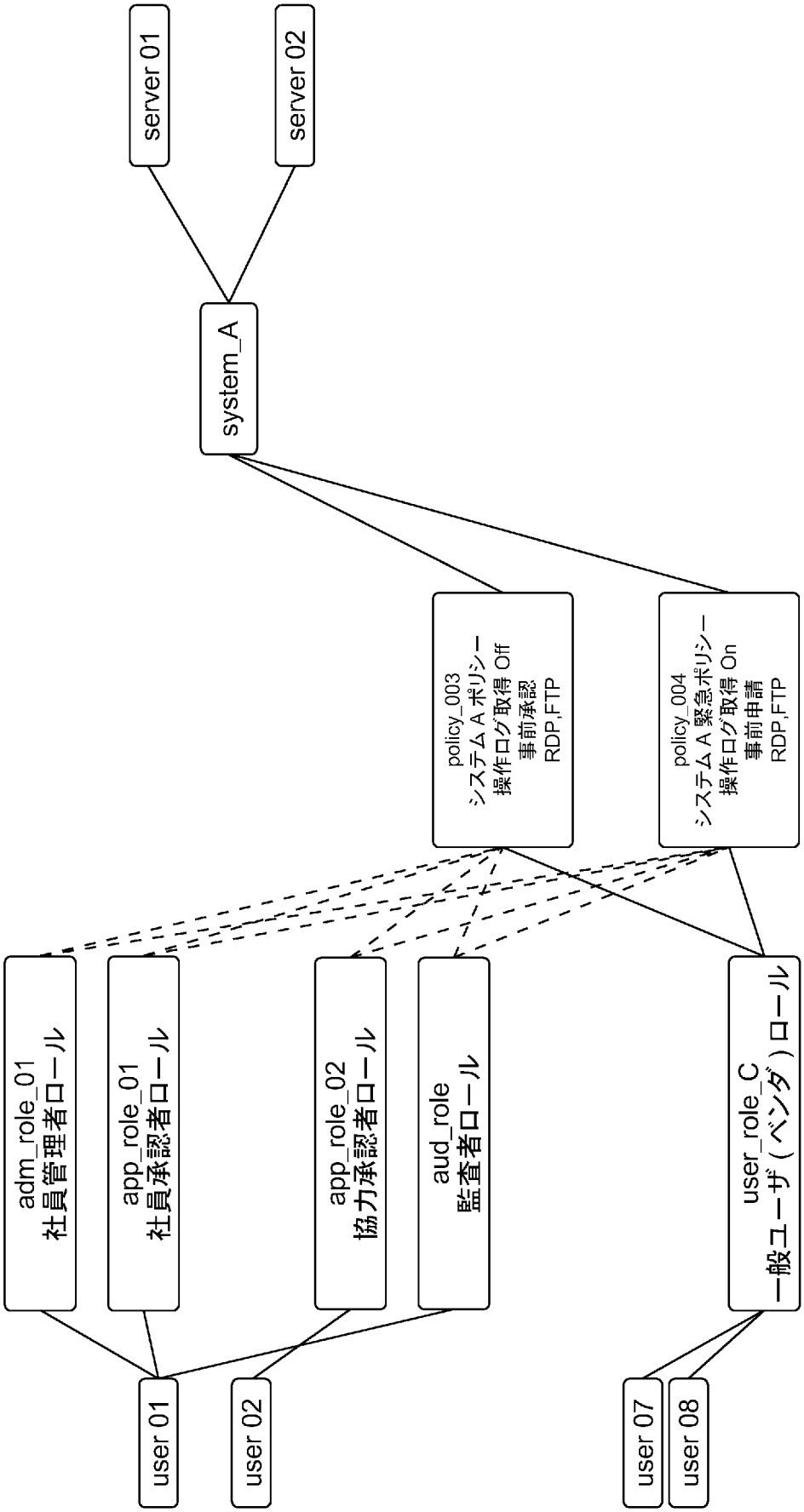
[図11]


server 01
server 02
server 03
server 04
system_A
system_B
system_C
policy_001
社員ポリシー
操作ログ取得 On
事前申請
SSH,RDP,FTP,SCP,SFTP
adm_role_01
社員管理者ロール
app_role_01
社員承認者ロール
aud_role
監査者ロール
user_role_A
一般ユーザ（社員）ロール
user 01
user 03

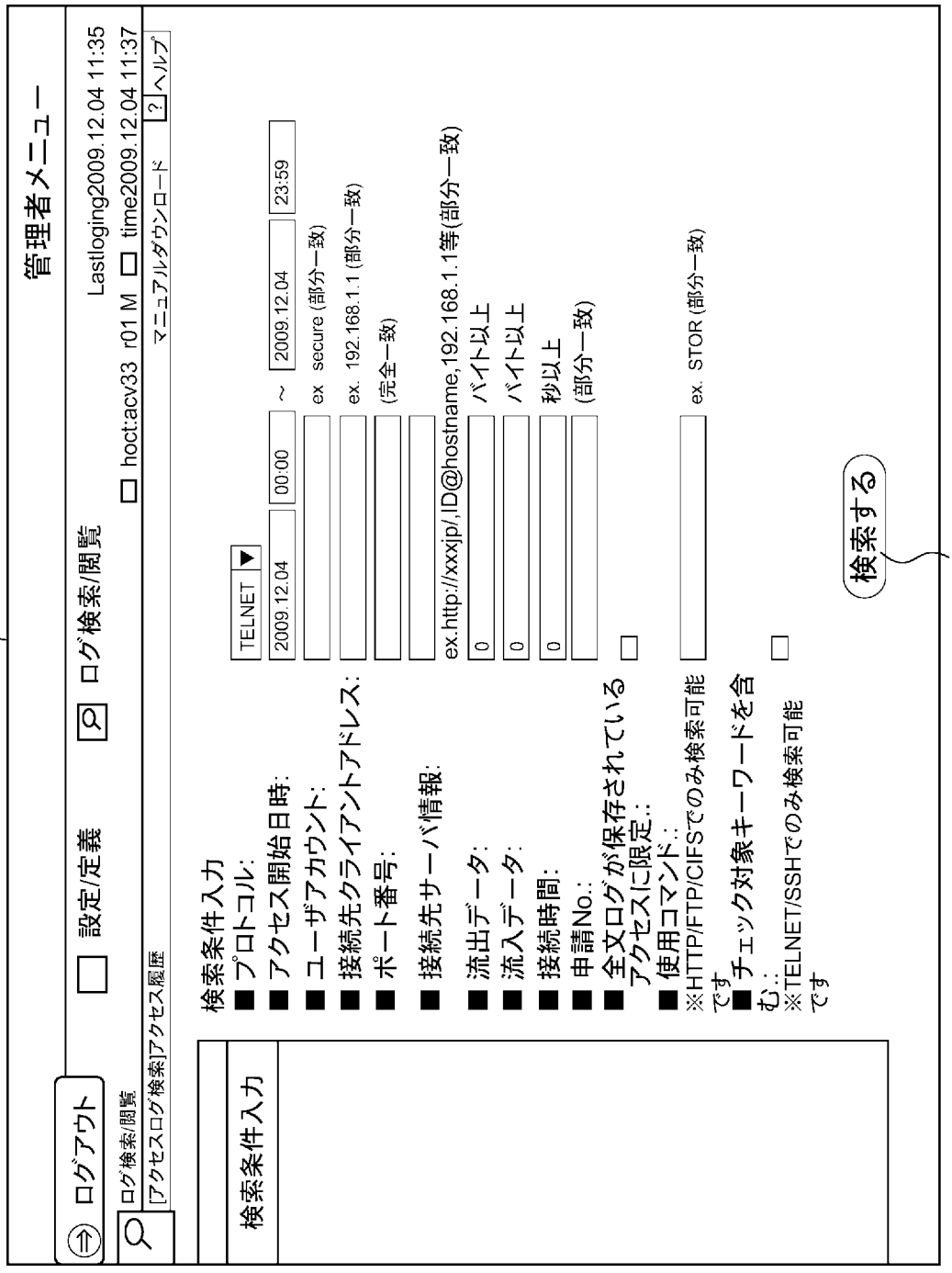
[図12]


server 01
server 02
server 03
server 04
system_B
system_C
policy_002
協力会社ポリシー
操作ログ取得 On
事前承認
SSH
adm_role_02
協力管理者ロール
app_role_02
協力承認者ロール
aud_role
監査者ロール
user_role_B
一般ユーザ（協力）ロール
user 01
user 02
user 04
user 05
user 06

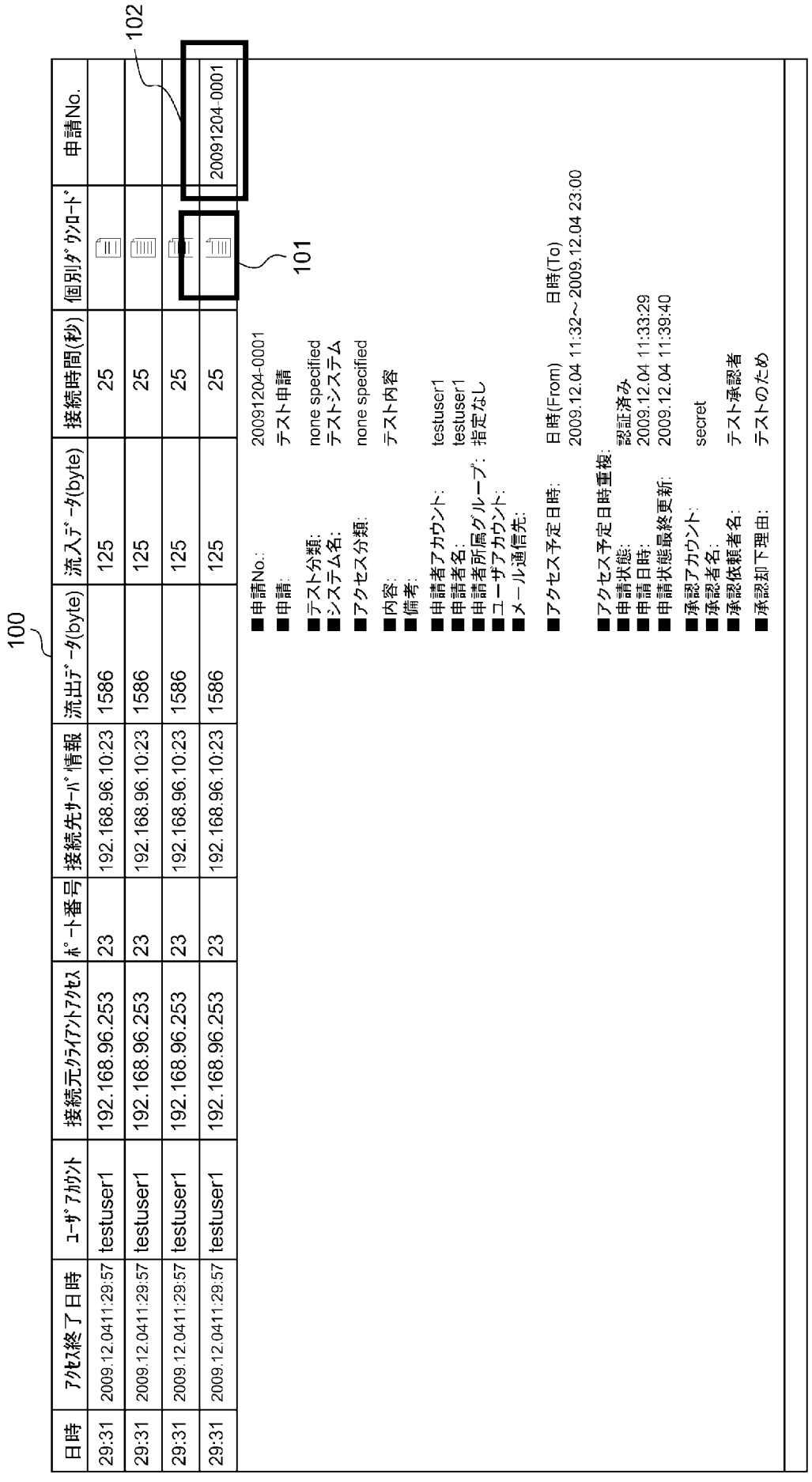
[図13]


server 01
server 02
system_A
policy_003
システムＡポリシー
操作ログ取得 Off
事前承認
RDP,FTP
policy_004
システムＡ緊急ポリシー
操作ログ取得 On
事前申請
RDP,FTP
adm_role_01
社員管理者ロール
app_role_01
社員承認者ロール
app_role_02
協力承認者ロール
aud_role
監査者ロール
user_role_C
一般ユーザ（ベンダ）ロール
user 01
user 02
user 07
user 08

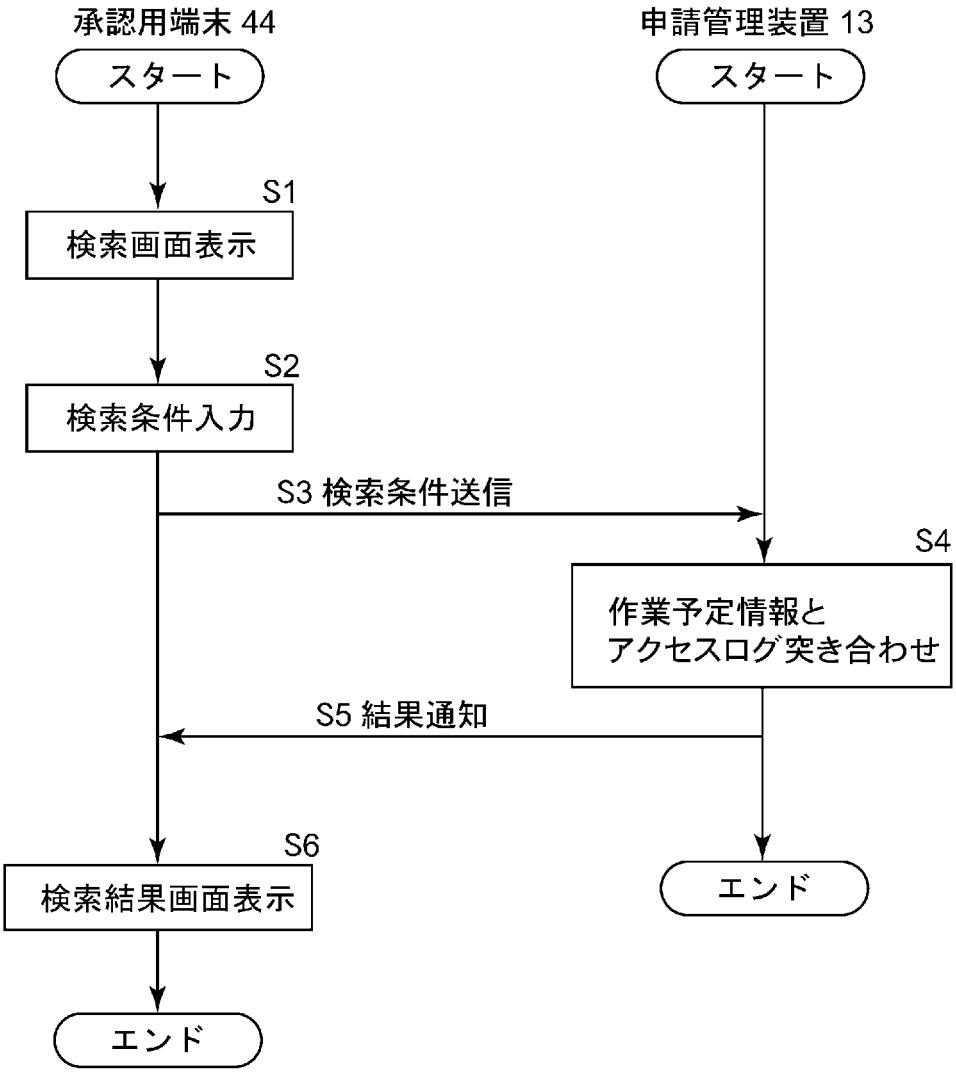
[図14]


90
管理者メニュー
ログアウト
設定/定義
ログ検索/閲覧
Lastloging2009.12.04 11:35
hoct:acv33 r01 M time2009.12.04 11:37
ログ検索/閲覧
アクセスログ検索|アクセス履歴
マニュアルダウンロード
ヘルプ
検索条件入力
検索条件入力
■プロトコル:
TELNET
■アクセス開始日時:
2009.12.04
00:00
~
2009.12.04
23:59
■ユーザアカウント:
ex secure (部分一致)
■接続先クライアントアドレス:
ex. 192.168.1.1 (部分一致)
■ポート番号:
(完全一致)
■接続先サーバ情報:
ex.http://xxxjp/,ID@hostname,192.168.1.1等(部分一致)
■流出データ:
0
バイト以上
■流入データ:
0
バイト以上
■接続時間:
0
秒以上
■申請No.:
(部分一致)
■全文ログが保存されている
アクセスに限定.:
■使用コマンド.:
※HTTP/FTP/CIFSでのみ検索可能です
ex. STOR (部分一致)
■チェック対象キーワードを含む.:
※TELNET/SSHでのみ検索可能です
検索する
91

[図15]


100
102
101
日時
アクセス終了日時
ユーザアカウント
接続元クライアントアクセス
ポート番号
接続先サーバ情報
流出データ(byte)
流入データ(byte)
接続時間(秒)
個別ダウンロード
申請No.
29:31 2009.12.0411:29:57 testuser1 192.168.96.253 23 192.168.96.10:23 1586 125 25 20091204-0001
■申請No.: 20091204-0001
■申請: テスト申請
■テスト分類: none specified
■システム名: テストシステム
■アクセス分類: none specified
■内容: テスト内容
■備考:
■申請者アカウント: testuser1
■申請者名: testuser1
■申請者所属グループ: 指定なし
■ユーザアカウント:
■メール通信先:
■アクセス予定日時: 日時(From) 日時(To)
2009.12.04 11:32～2009.12.04 23:00
■アクセス予定日時重複:
■申請状態: 認証済み
■申請日時: 2009.12.04 11:33:29
■申請状態最終更新: 2009.12.04 11:39:40
■承認アカウント: secret
■承認者名:
■承認依頼者名: テスト承認者
■承認却下理由: テストのため

[図16]


承認用端末 44
スタート
S1
検索画面表示
S2
検索条件入力
S3 検索条件送信
S6
検索結果画面表示
エンド
申請管理装置 13
スタート
S4
作業予定情報と
アクセスログ突き合わせ
S5 結果通知
エンド