SSHクライアント

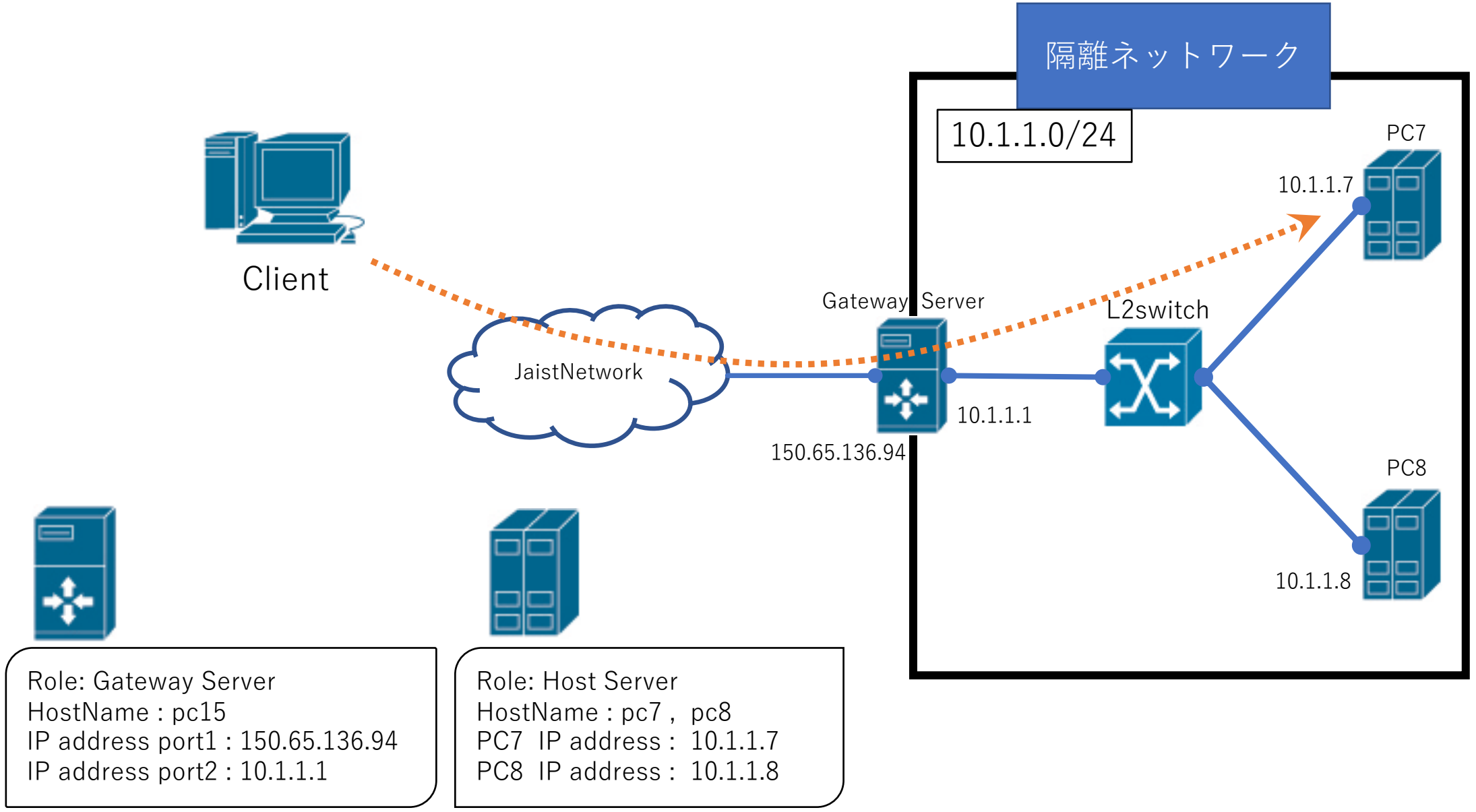
①コマンドプロンプト上で
$telnet 150.65.136.94　と入力
(接続要求)

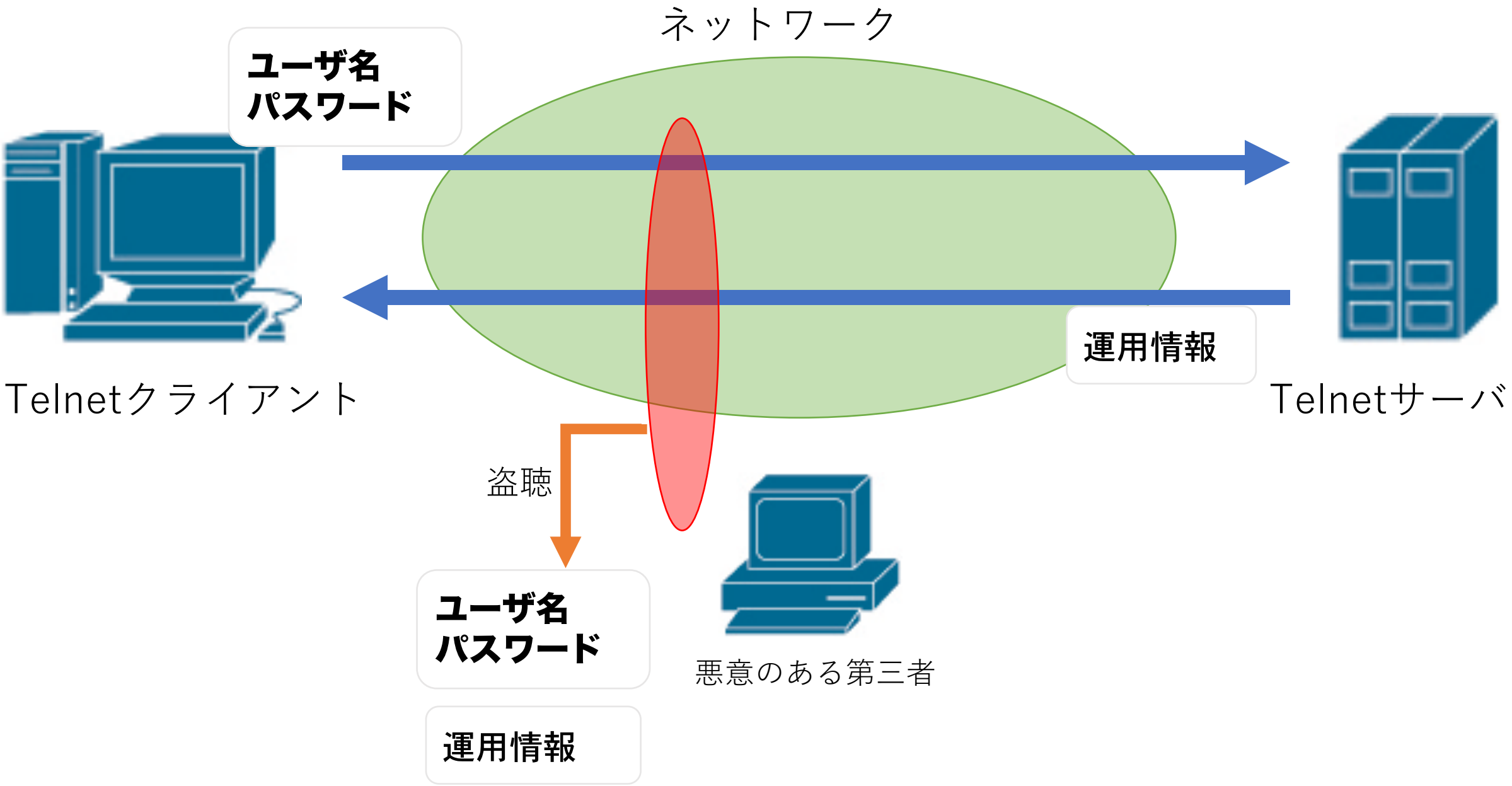
②TCPによるコネクション確立後
Telnetサーバから応答画面表示

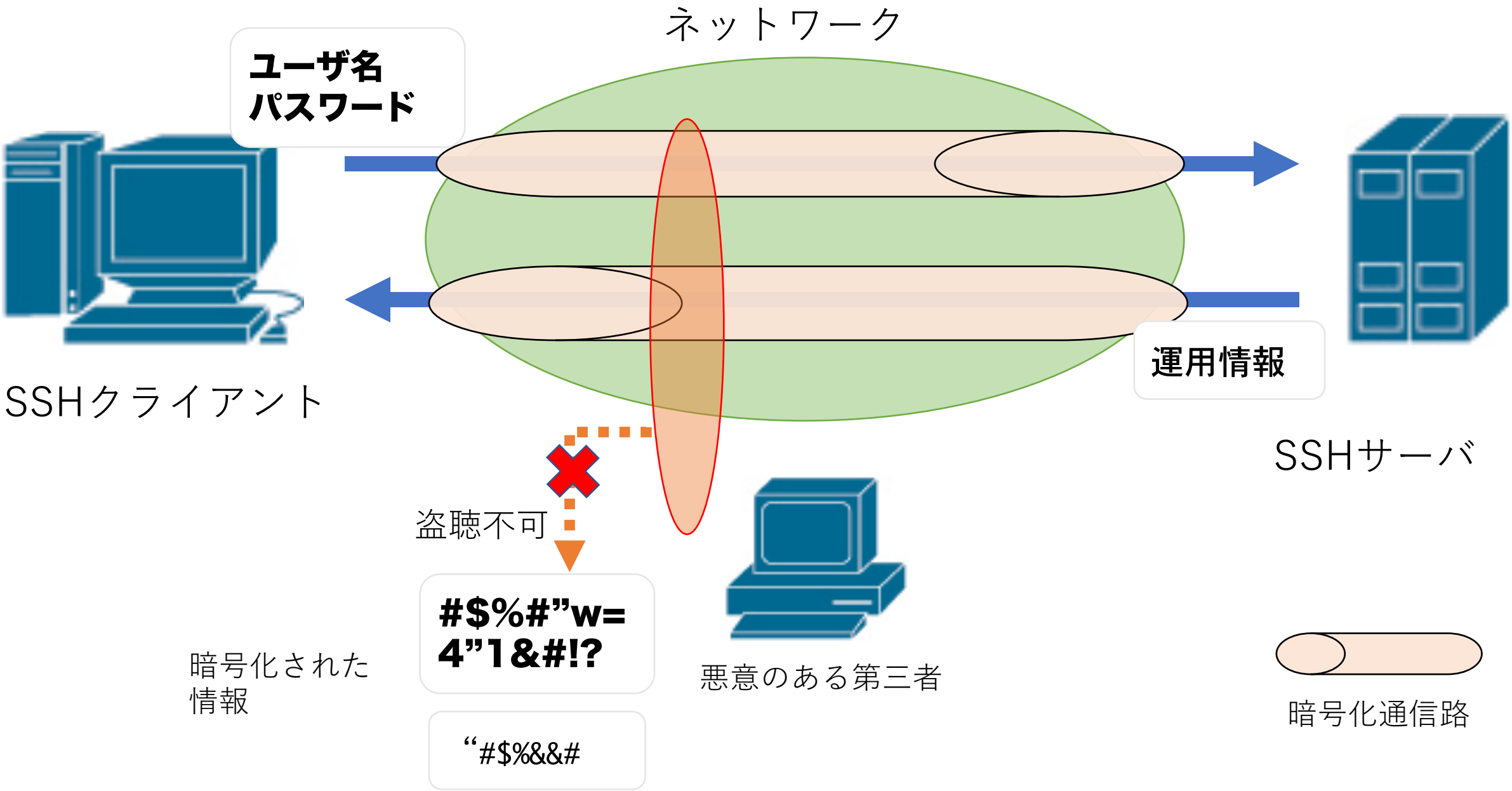
③コマンドプロンプト上でコマンド
入力を行いサーバに対して命令を行う

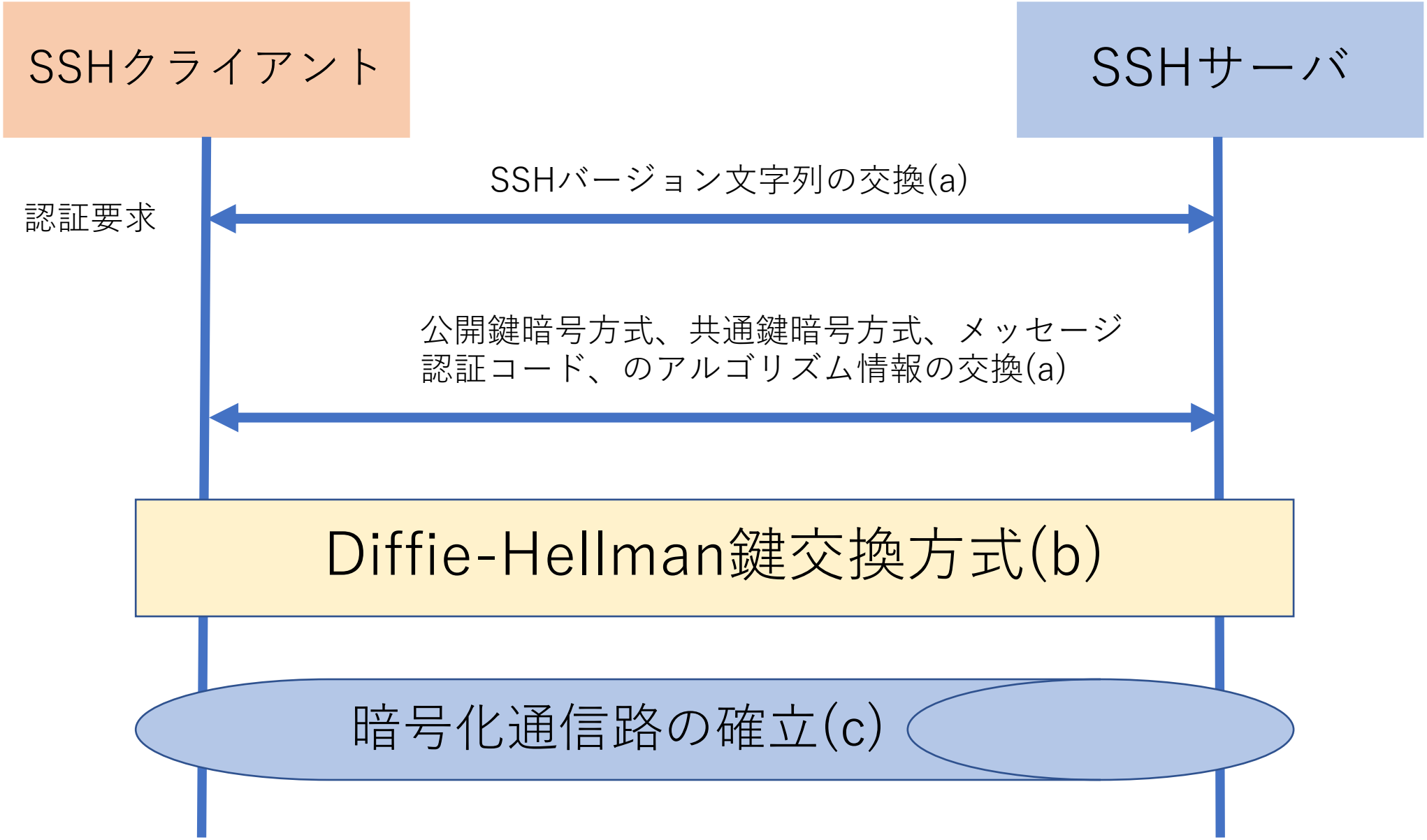
④受信したコマンドに従い処理を行い、
結果をクライアントに対して送信する。

SSHサーバ
IP addres :
150.65.136.94


隔離ネットワーク
10.1.1.0/24
Client
JaistNetwork
Gateway Server
150.65.136.94
10.1.1.1
L2switch
PC7
10.1.1.7
PC8
10.1.1.8
Role: Gateway Server
HostName : pc15
IP address port1 : 150.65.136.94
IP address port2 : 10.1.1.1
Role: Host Server
HostName : pc7 , pc8
PC7 IP address : 10.1.1.7
PC8 IP address : 10.1.1.8


ネットワーク
ユーザ名
パスワード
運用情報
Telnetクライアント
Telnetサーバ
盗聴
ユーザ名
パスワード
運用情報
悪意のある第三者


ネットワーク
ユーザ名
パスワード
SSHクライアント
運用情報
SSHサーバ
盗聴不可
#$%#”w=
4”1&#!?
暗号化された
情報
悪意のある第三者
“#$%&&#
暗号化通信路


SSHクライアント
SSHサーバ
SSHバージョン文字列の交換(a)
認証要求
公開鍵暗号方式、共通鍵暗号方式、メッセージ
認証コード、のアルゴリズム情報の交換(a)
Diffie-Hellman鍵交換方式(b)
暗号化通信路の確立(c)

Telnetクライアント

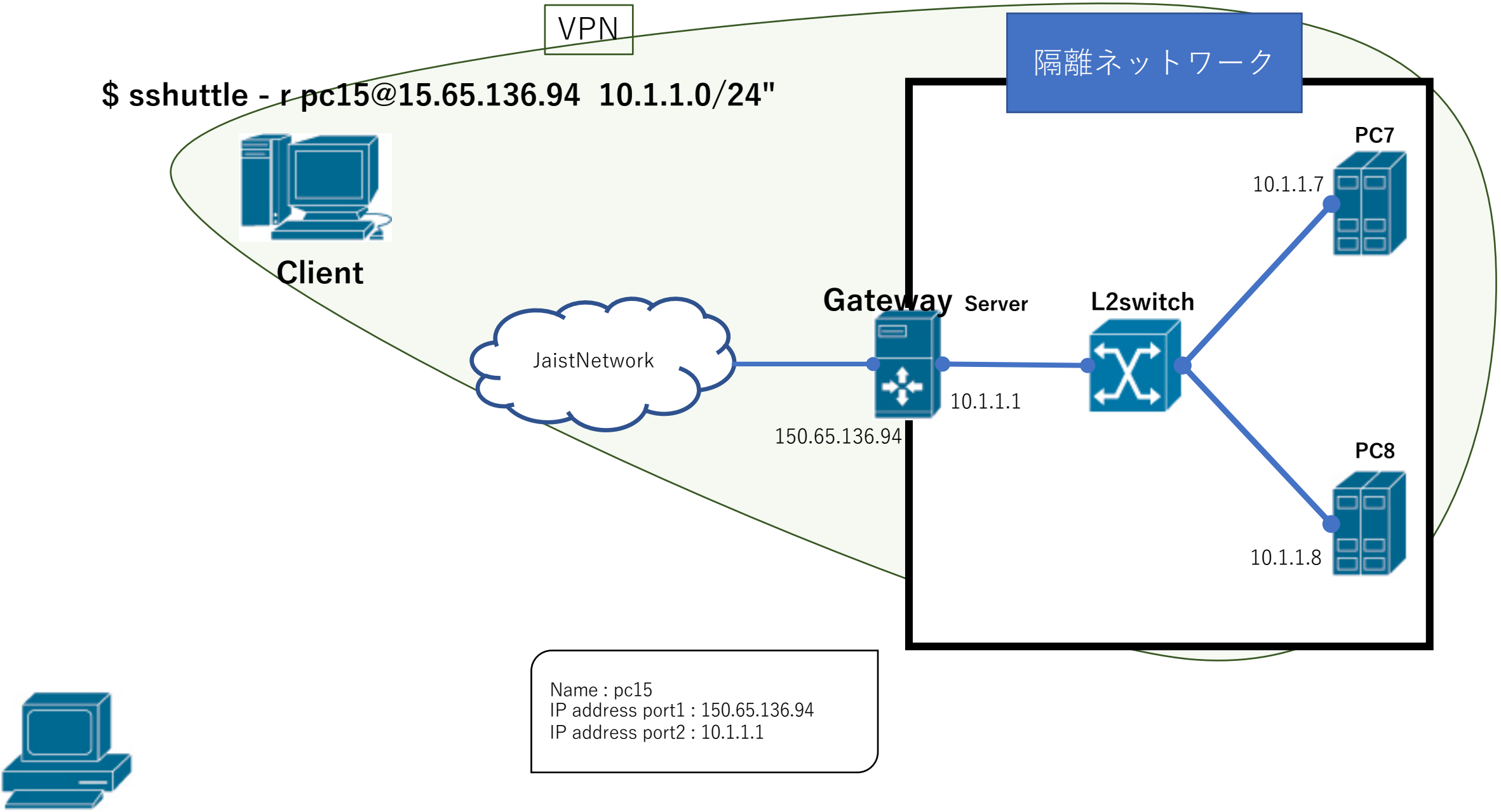
①コマンドプロンプト上で
$telnet 150.65.136.94　と入力
(接続要求)

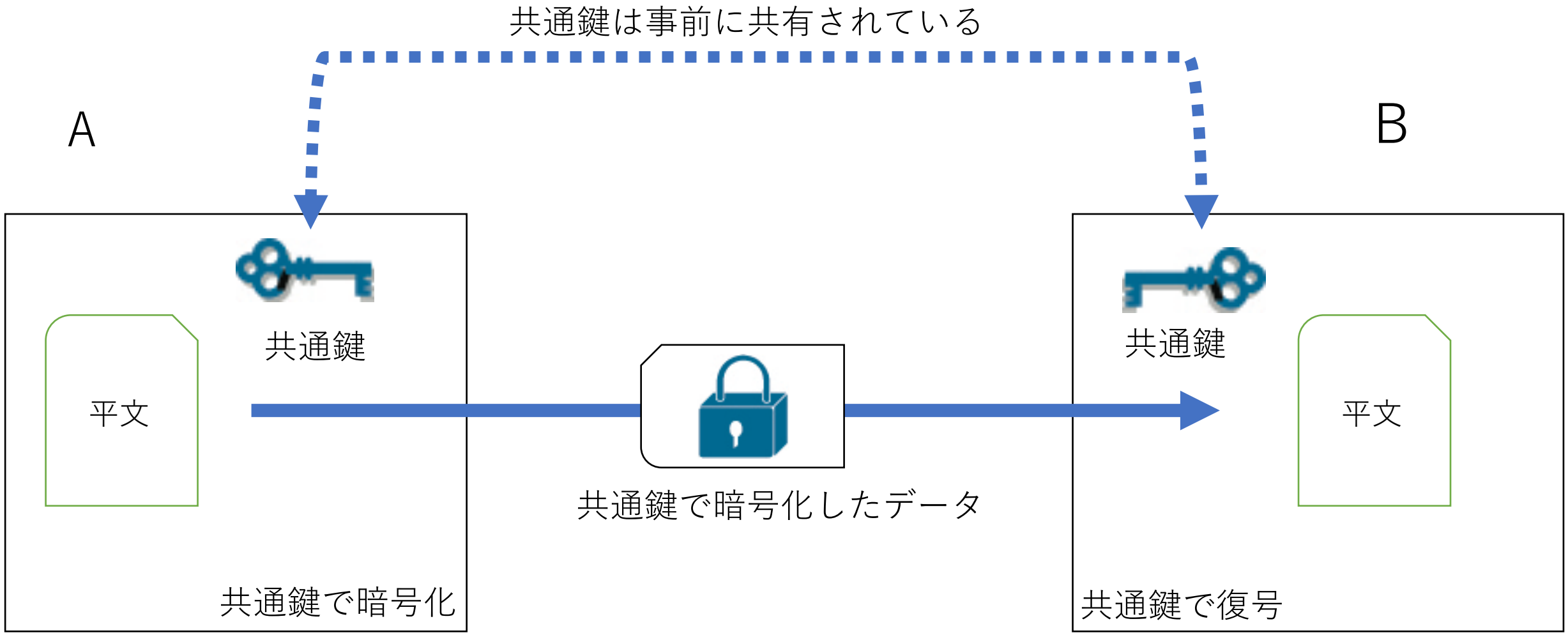
②TCPによるコネクション確立後
Telnetサーバから応答画面表示

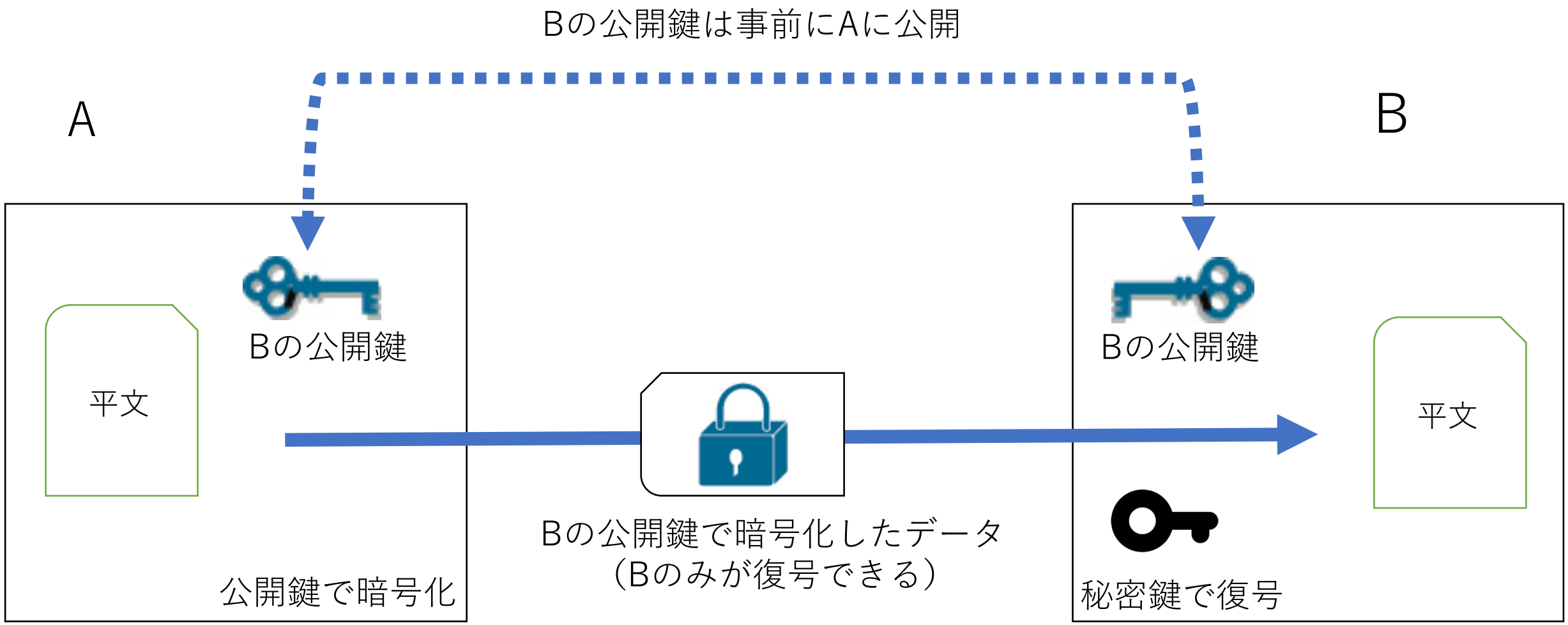
③コマンドプロンプト上でコマンド入力を行い
サーバに対して命令を行う

④受信したコマンドに従い処理を行い、
結果をクライアントに対して送信する。

Telnetサーバ
IP addres :
150.65.136.94


VPN
隔離ネットワーク
$ sshuttle - r pc15@15.65.136.94 10.1.1.0/24"
Client
JaistNetwork
Gateway
Server
L2switch
PC7
10.1.1.7
10.1.1.1
150.65.136.94
PC8
10.1.1.8
Name : pc15
IP address port1 : 150.65.136.94
IP address port2 : 10.1.1.1


共通鍵は事前に共有されている
A
B
共通鍵
平文
共通鍵で暗号化したデータ
共通鍵
平文
共通鍵で暗号化
共通鍵で復号


Bの公開鍵は事前にAに公開
A
B
Bの公開鍵
平文
Bの公開鍵
平文
Bの公開鍵で暗号化したデータ
（Bのみが復号できる）
公開鍵で暗号化
秘密鍵で復号

UNIXサーバ

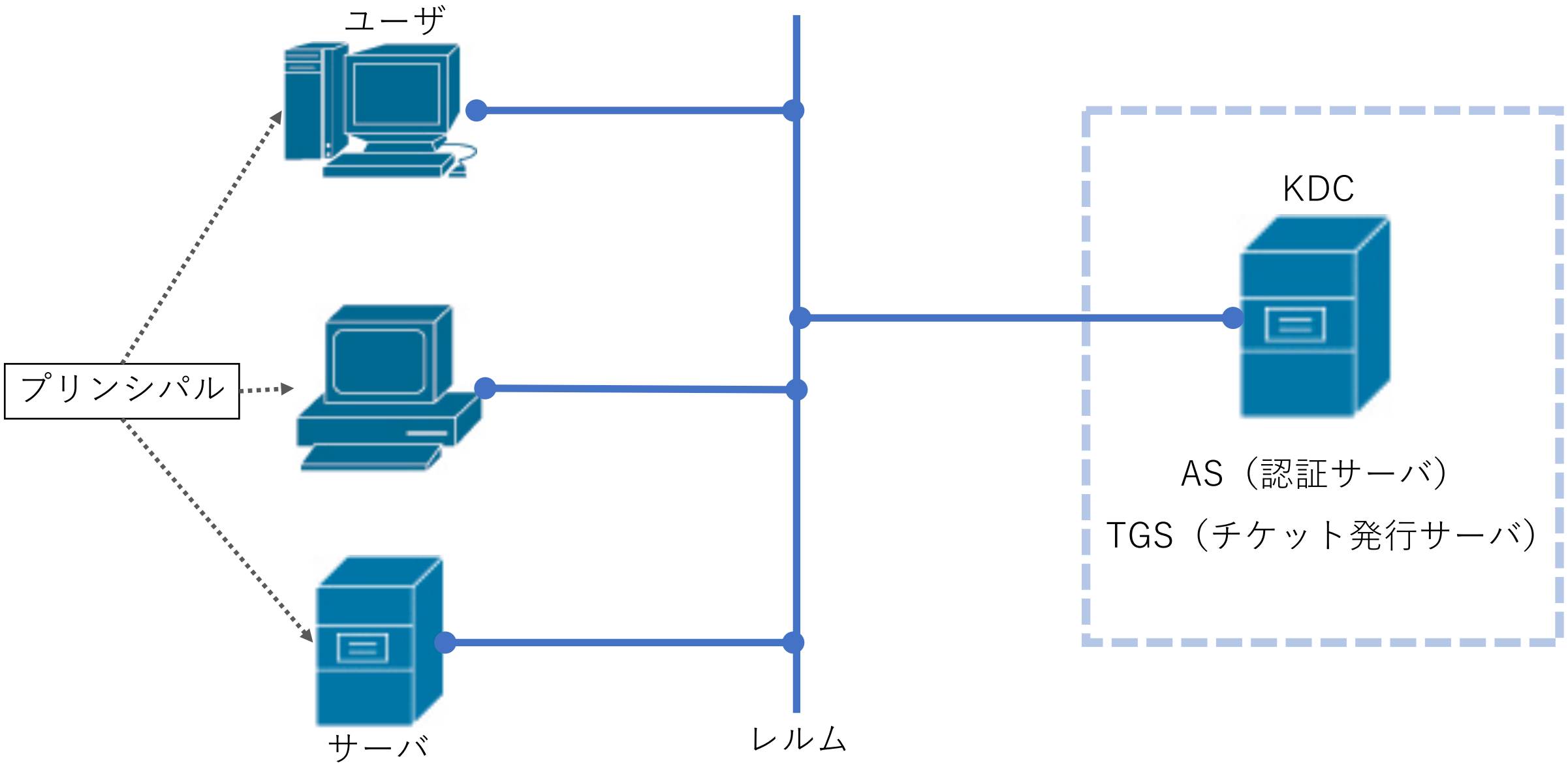
メールクライアント

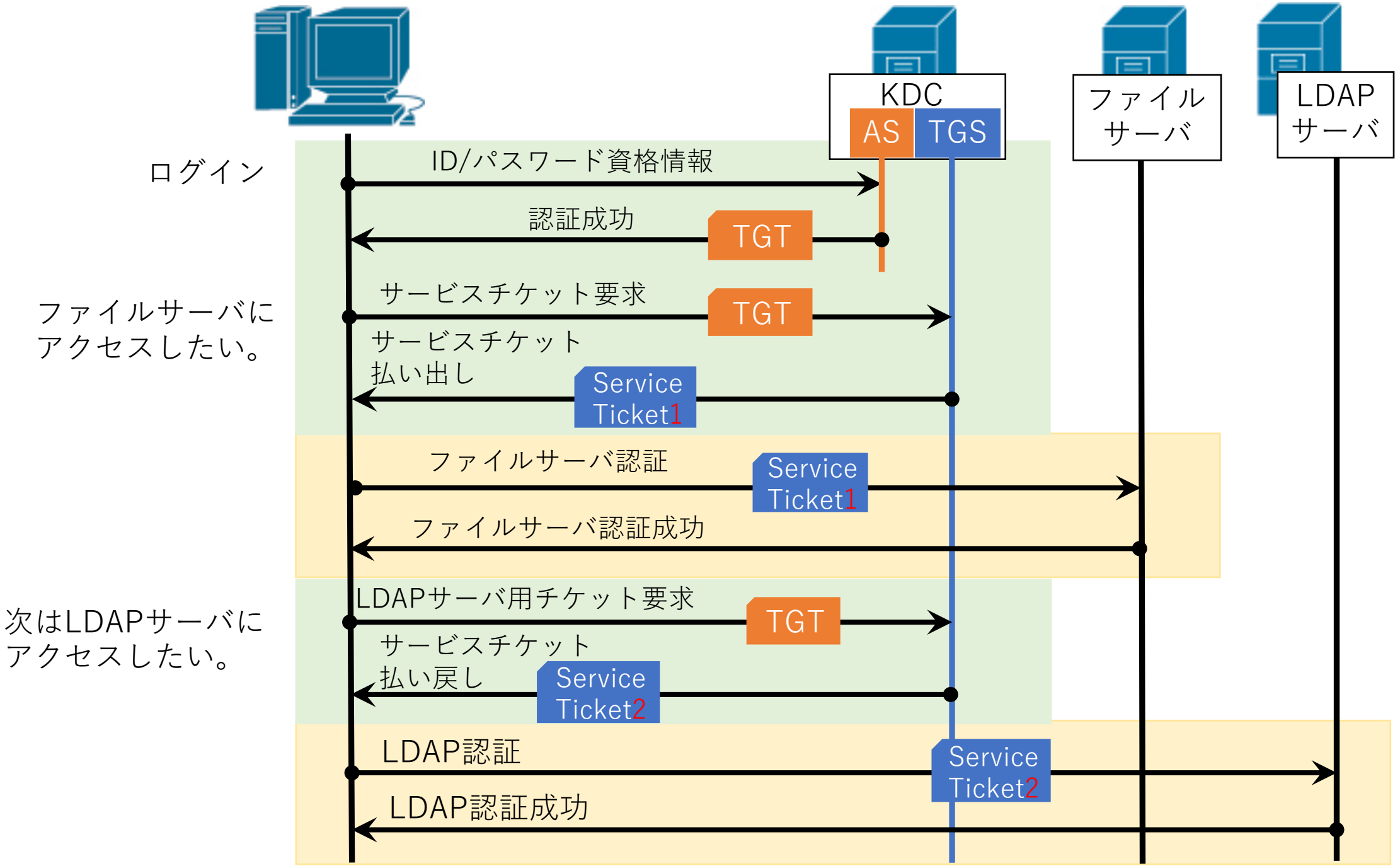
グループ情報
ユーザ情報
ホスト情報
アドレス帳
メールアドレス情報
DNSゾーン情報

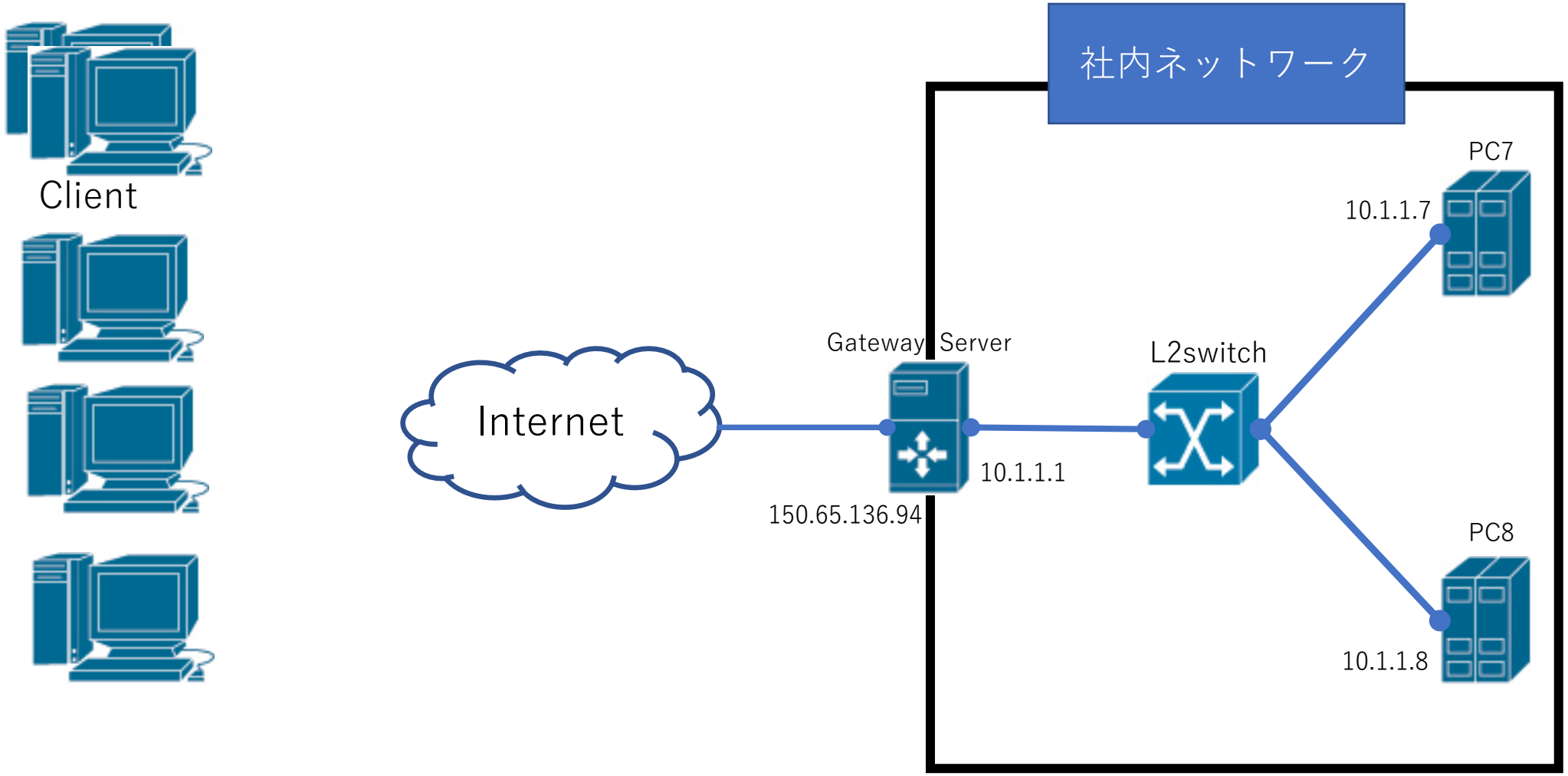
SSHサーバ

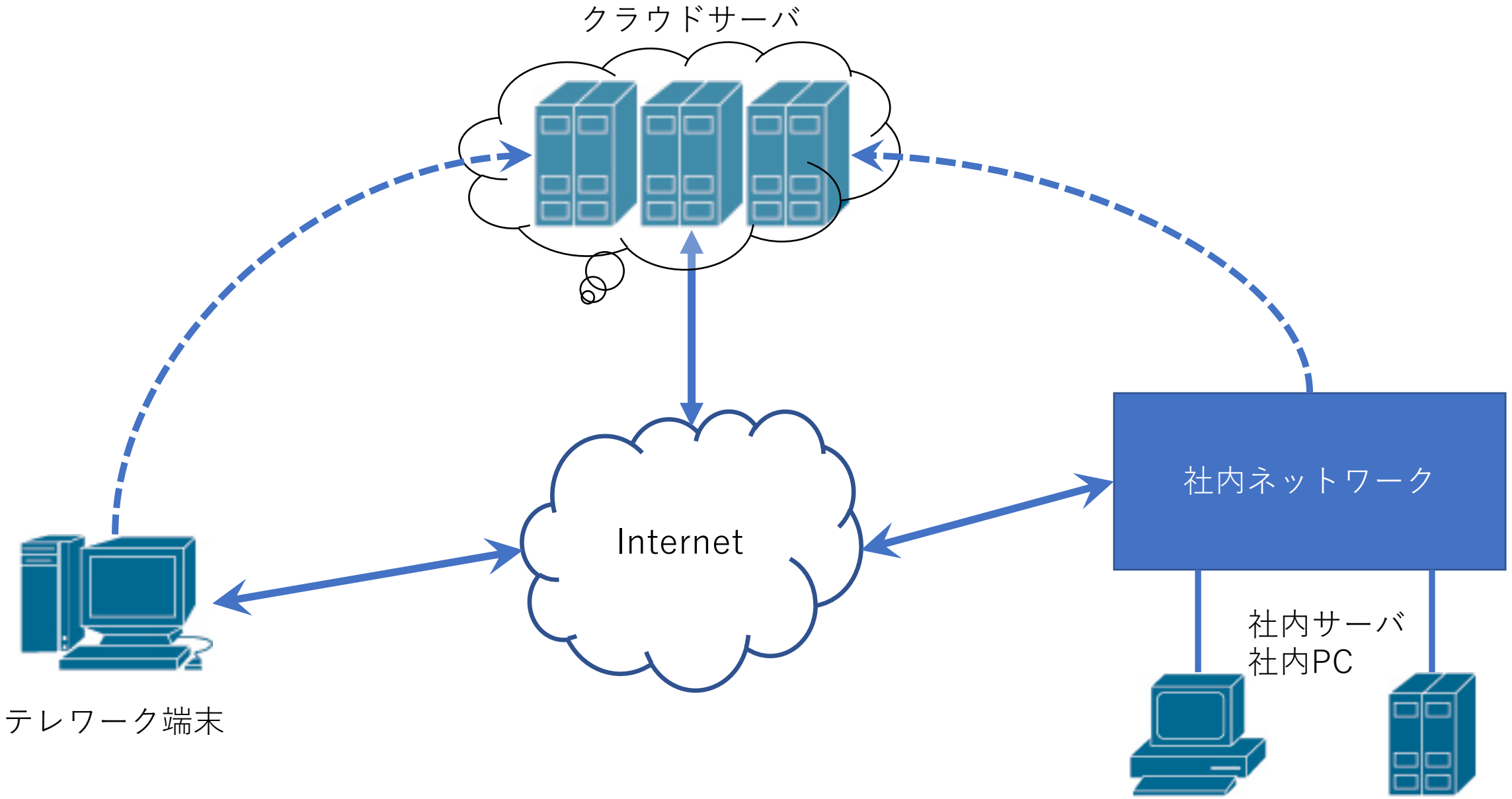
DNSサーバ

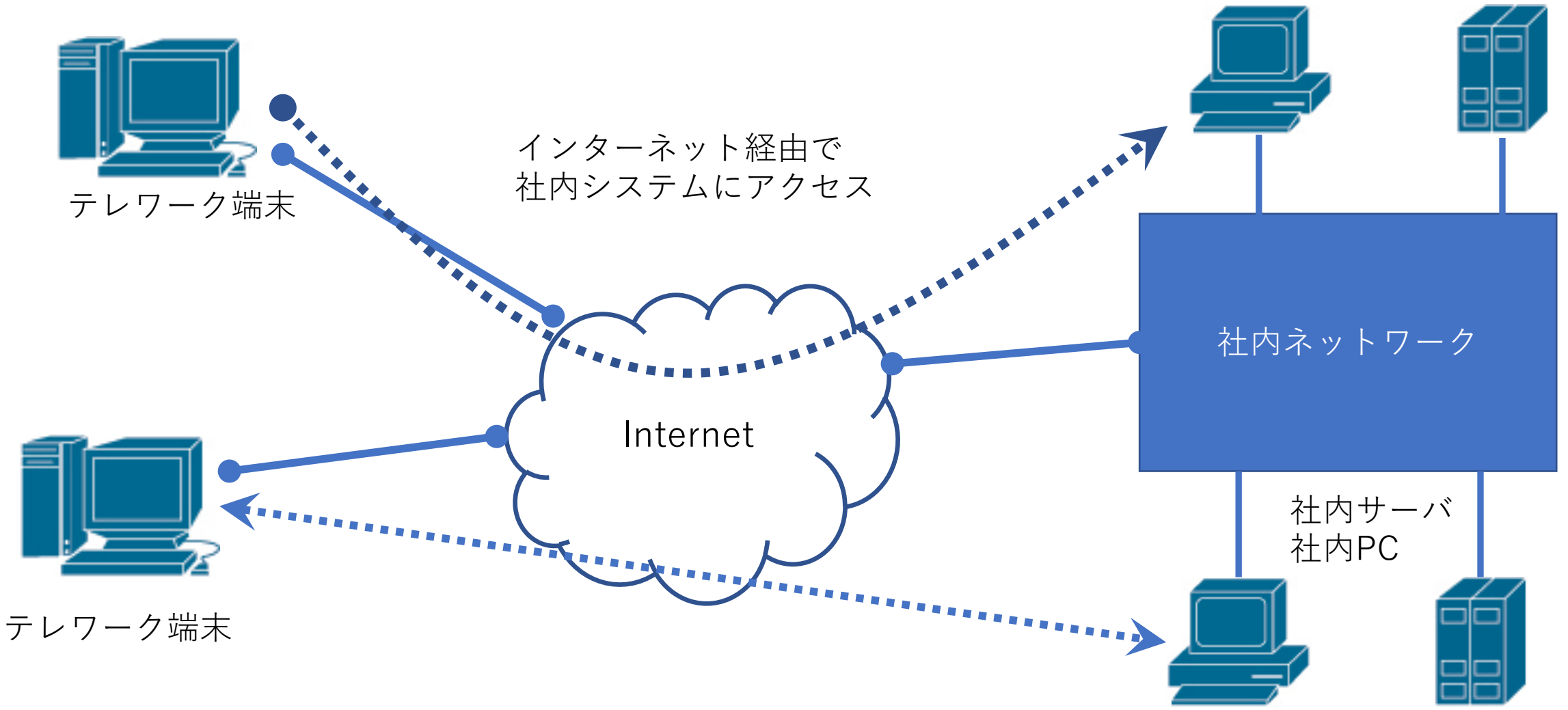
Webサーバ

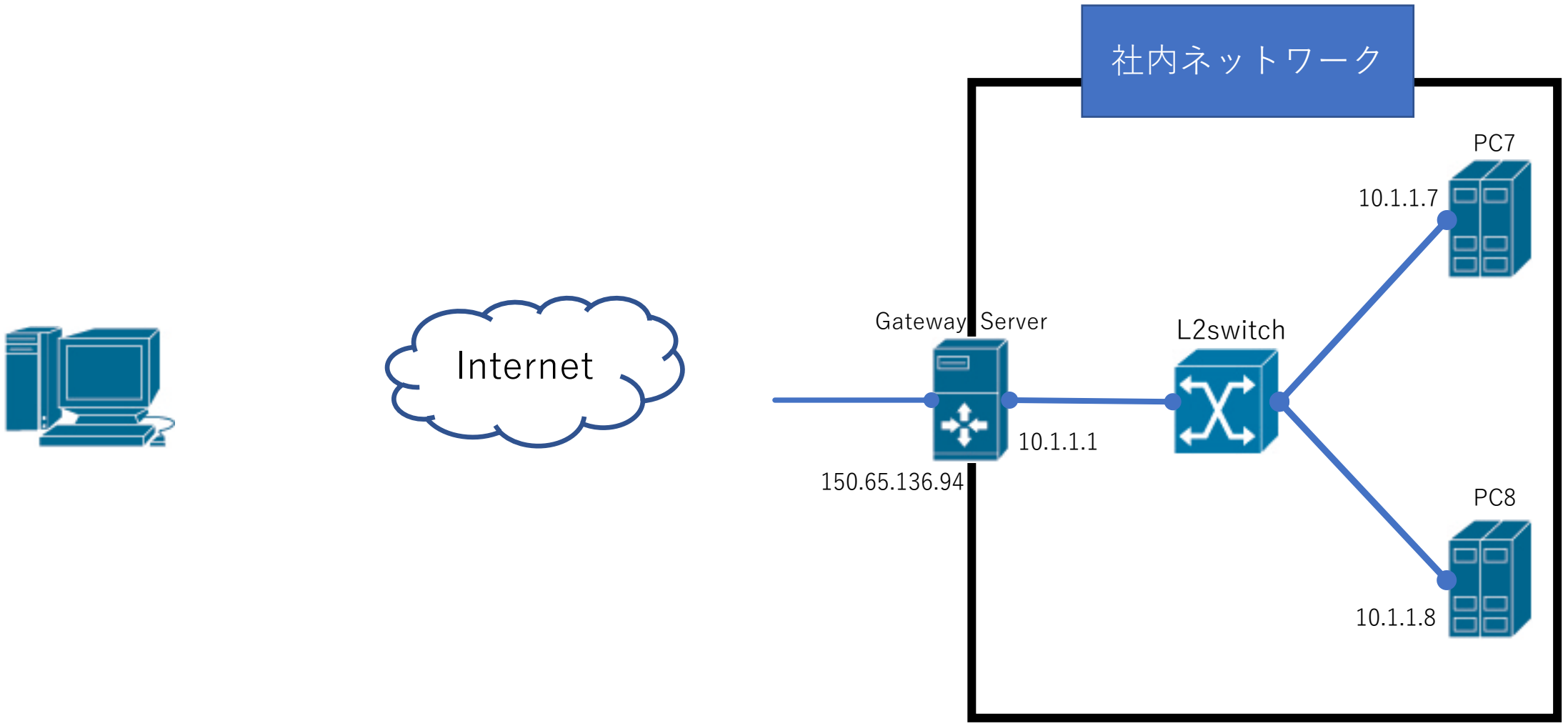

ユーザ
プリンシパル
サーバ
レルム
KDC
AS（認証サーバ）
TGS（チケット発行サーバ）


KDC
AS
TGS
ファイル
サーバ
LDAP
サーバ
ログイン
ID/パスワード資格情報
認証成功
TGT
ファイルサーバに
アクセスしたい。
サービスチケット要求
TGT
サービスチケット
払い出し
Service
Ticket1
ファイルサーバ認証
Service
Ticket1
ファイルサーバ認証成功
次はLDAPサーバに
アクセスしたい。
LDAPサーバ用チケット要求
TGT
サービスチケット
払い戻し
Service
Ticket2
LDAP認証
Service
Ticket2
LDAP認証成功


Client
社内ネットワーク
PC7
10.1.1.7
Internet
Gateway Server
L2switch
10.1.1.1
150.65.136.94
PC8
10.1.1.8


クラウドサーバ
Internet
社内ネットワーク
社内サーバ
社内PC
テレワーク端末


テレワーク端末
インターネット経由で
社内システムにアクセス
Internet
社内ネットワーク
テレワーク端末
社内サーバ
社内PC


社内ネットワーク
PC7
10.1.1.7
Internet
Gateway Server
L2switch
10.1.1.1
150.65.136.94
PC8
10.1.1.8