



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



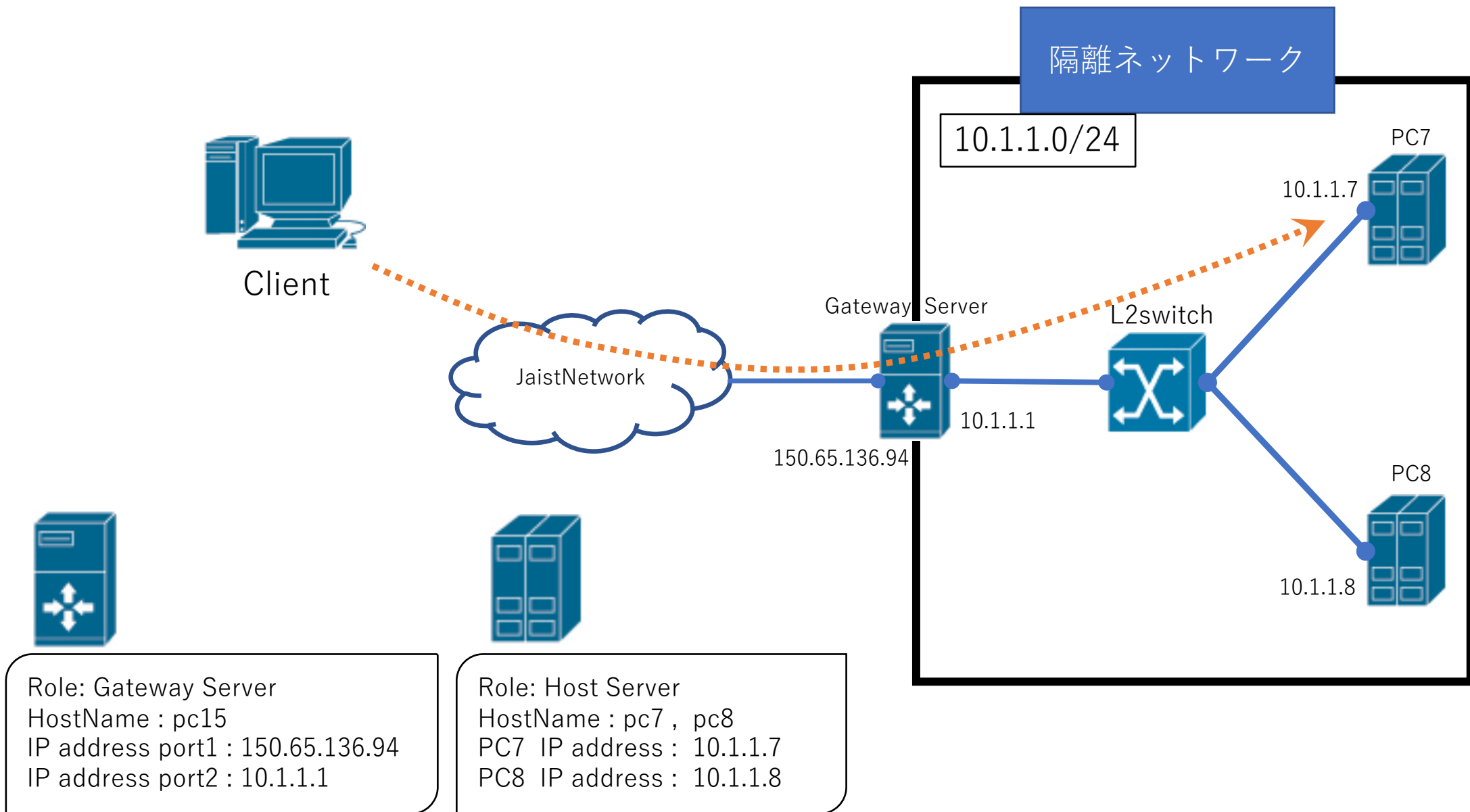
③コマンドプロンプト上でコマンド  
入力を行いサーバに対して命令を行う

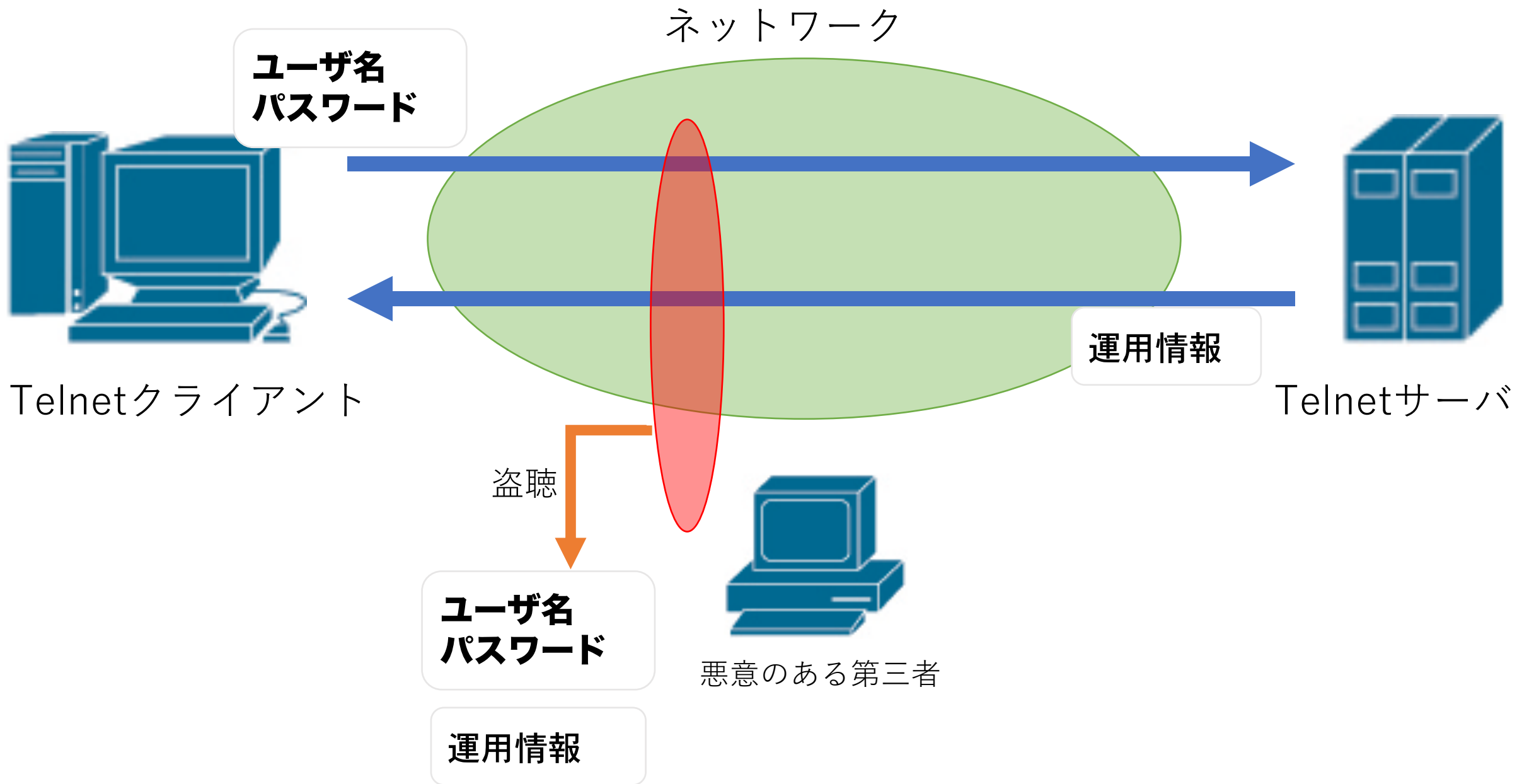


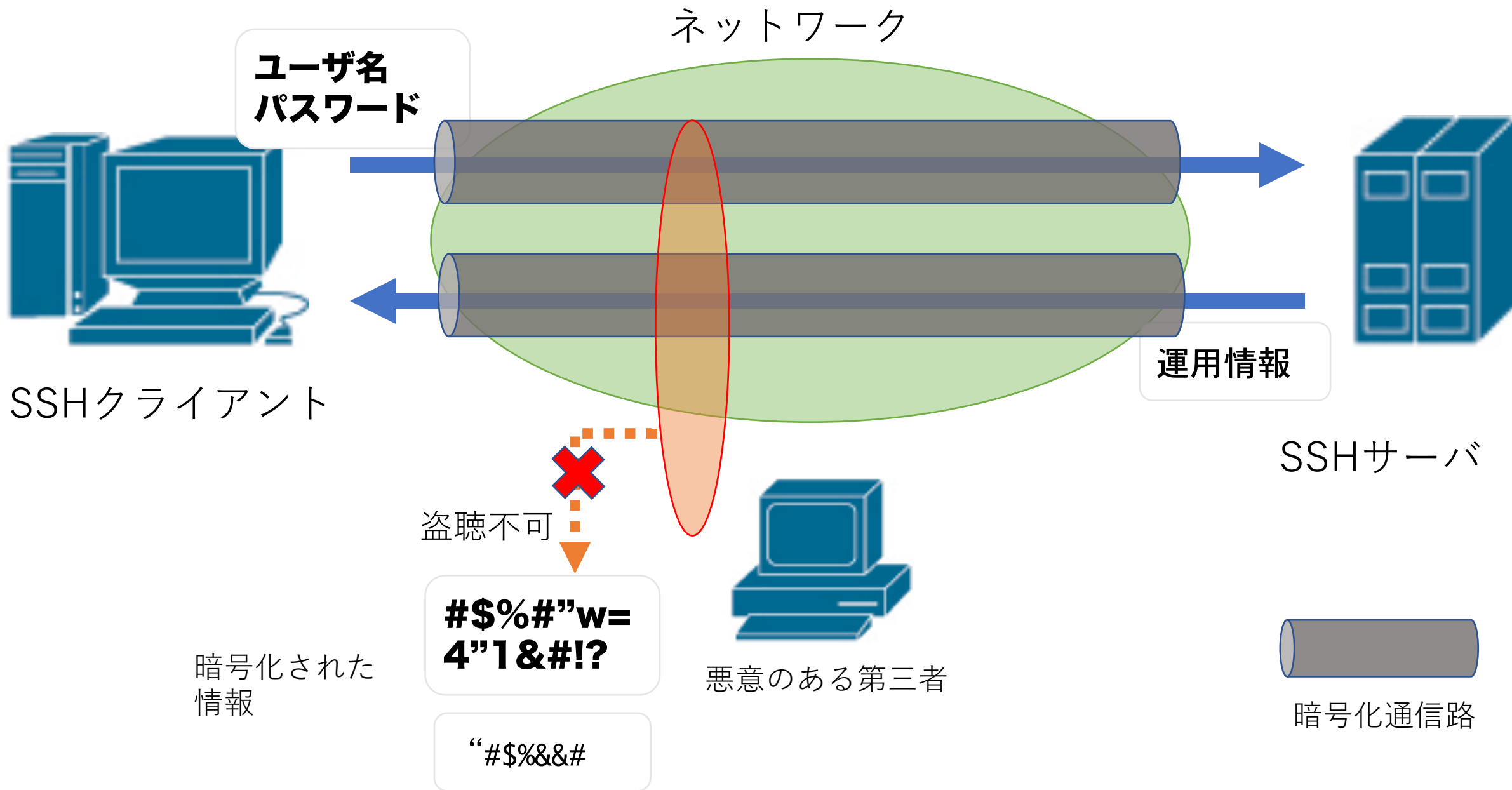
④受信したコマンドに従い処理を行い、  
結果をクライアントに対して送信する。



SSHサーバ  
IP address :  
150.65.136.94







SSHクライアント

SSHサーバ

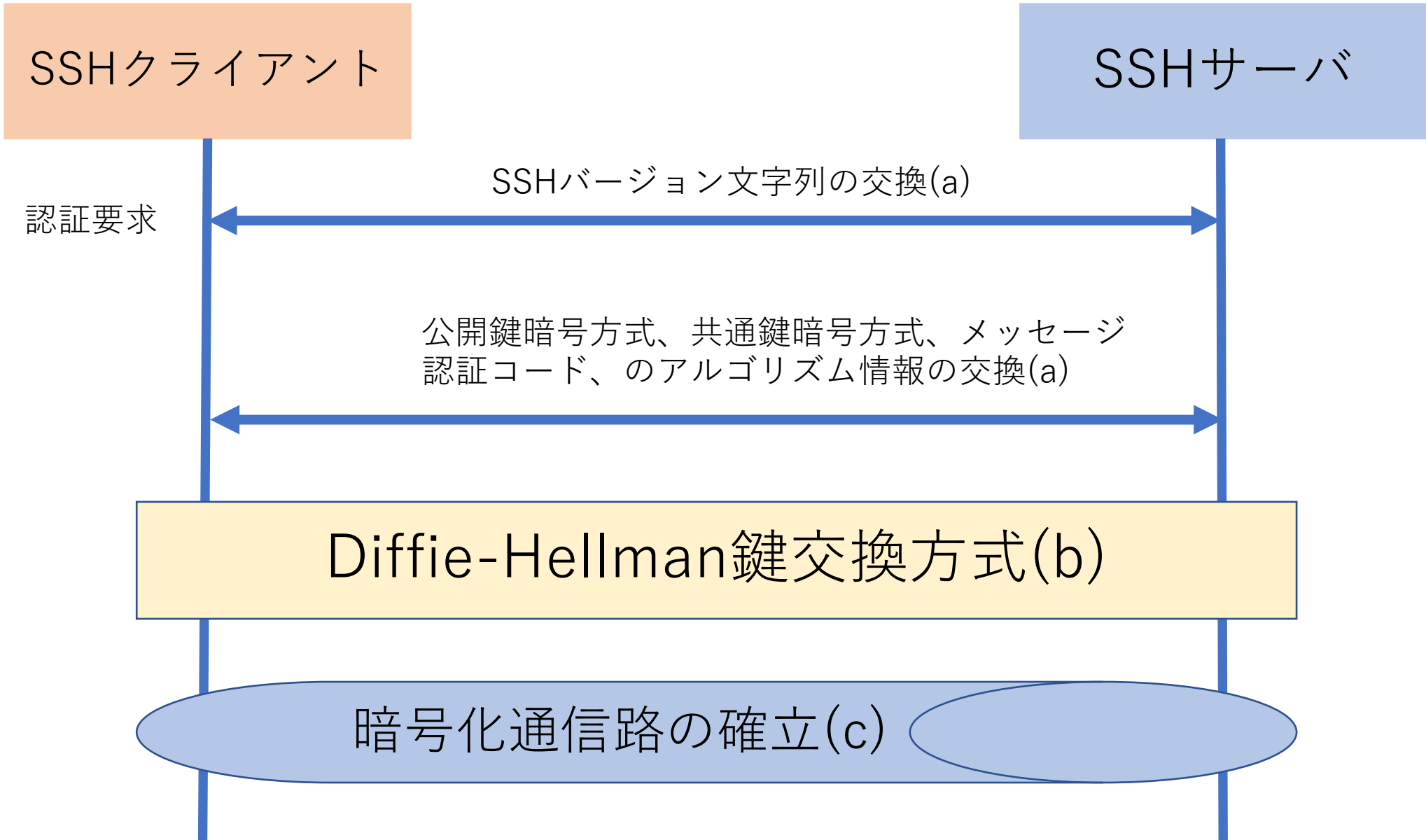
認証要求

SSHバージョン文字列の交換(a)

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。



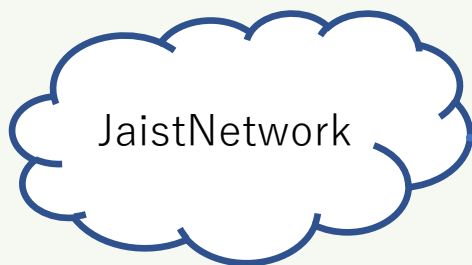
Telnetサーバ  
IP address :  
150.65.136.94

VPN

\$ sshuttle -r pc15@15.65.136.94 10.1.1.0/24"



Client



JaistNetwork

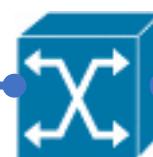
Gateway Server



150.65.136.94

10.1.1.1

L2switch



隔離ネットワーク

10.1.1.0/24

PC7

10.1.1.7



PC8

10.1.1.8



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



共通鍵で暗号化したデータ



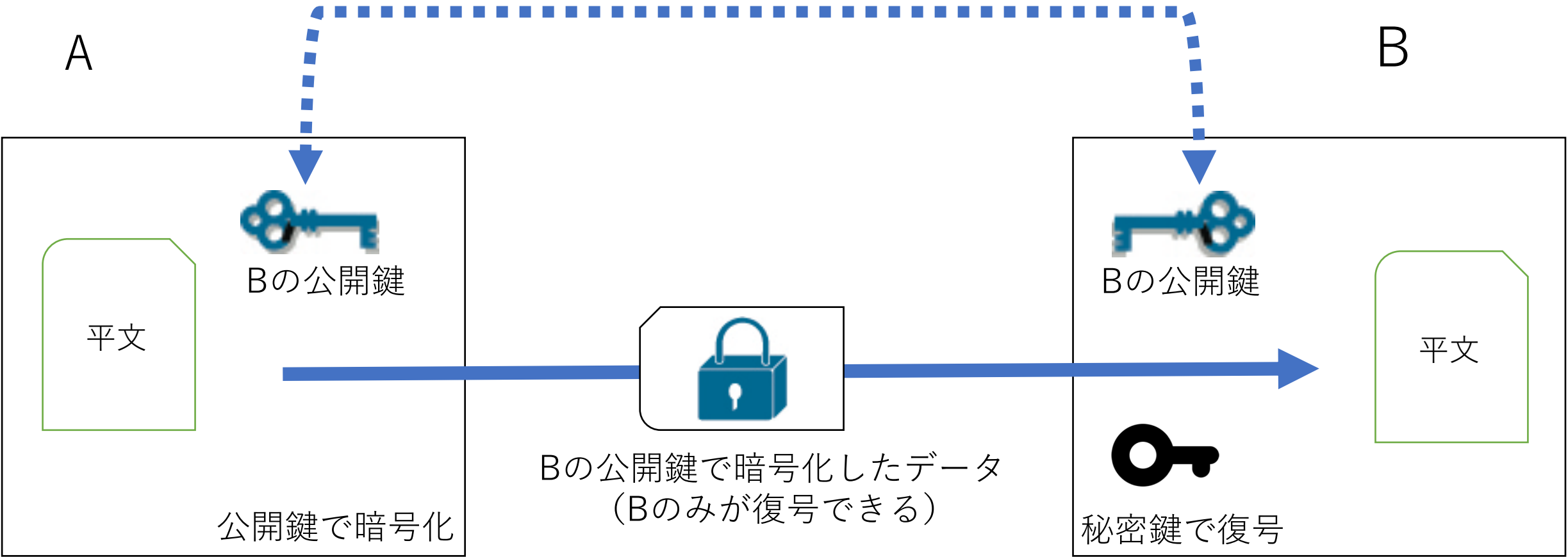
共通鍵

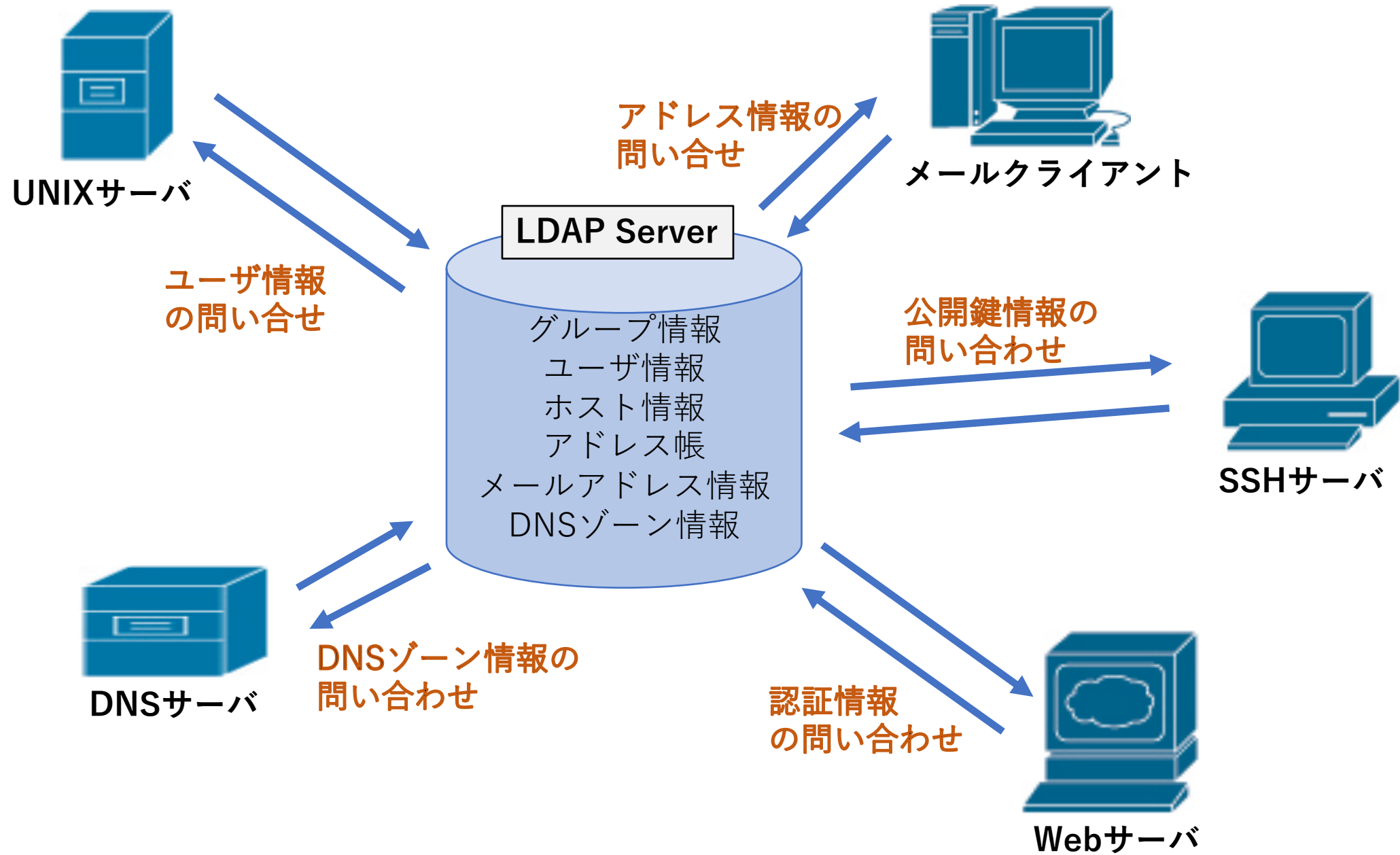
平文

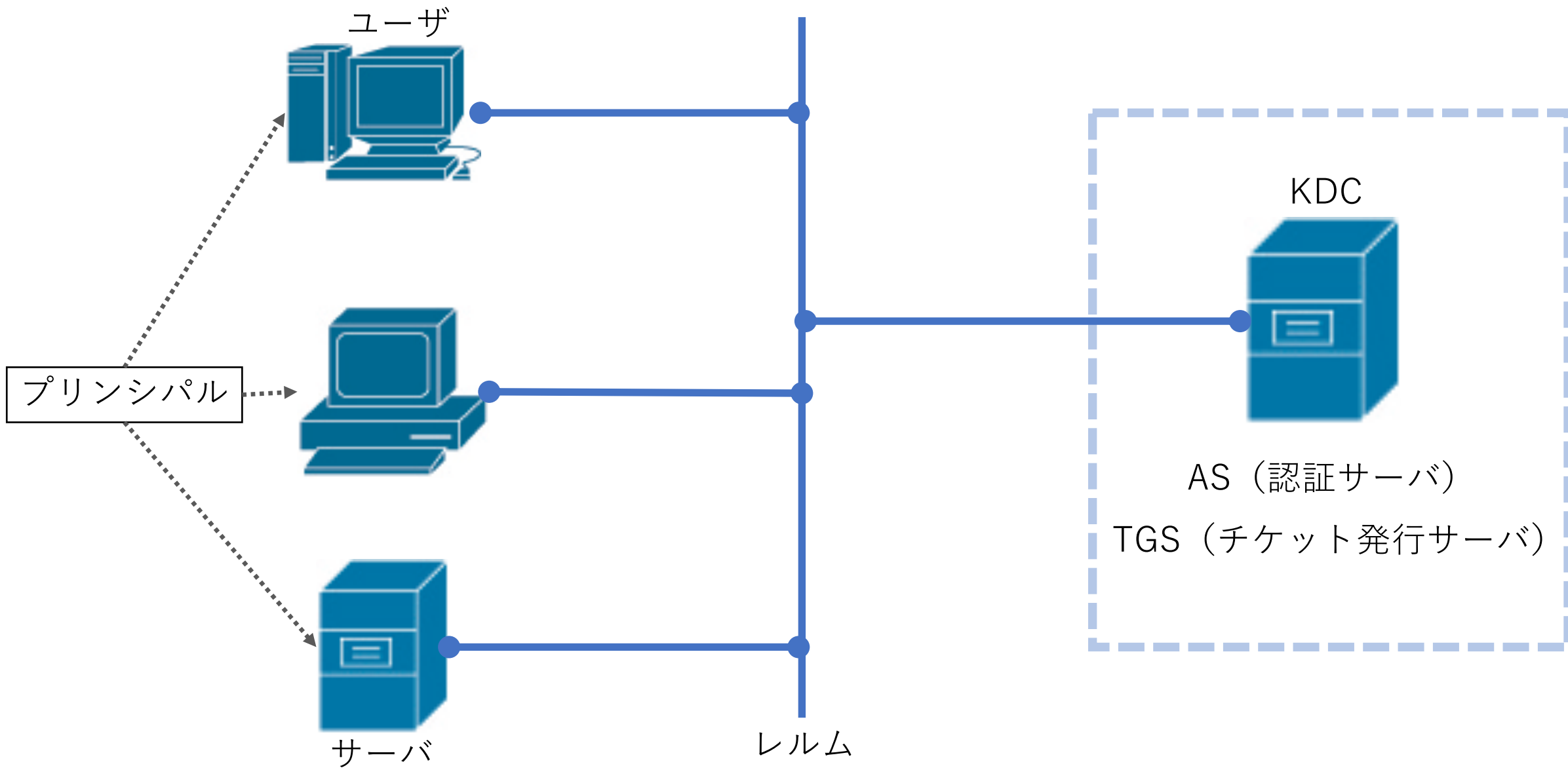
共通鍵で復号



Bの公開鍵は事前にAに公開

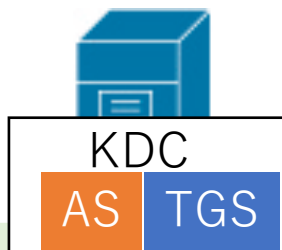






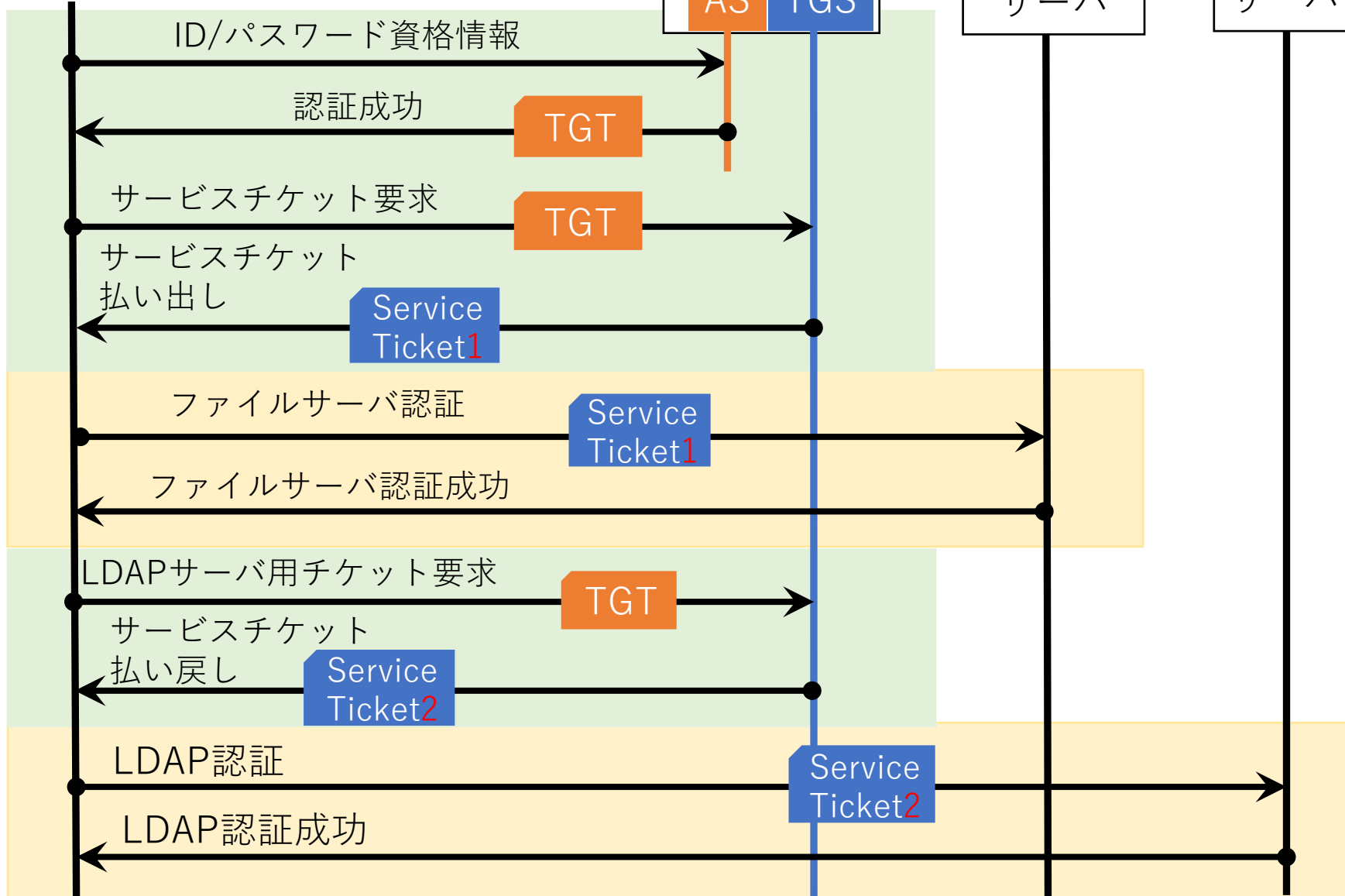


ログイン



ファイルサーバに  
アクセスしたい。

次はLDAPサーバに  
アクセスしたい。





Client



Internet

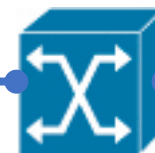
Gateway Server



10.1.1.1

150.65.136.94

L2switch



社内ネットワーク

PC7

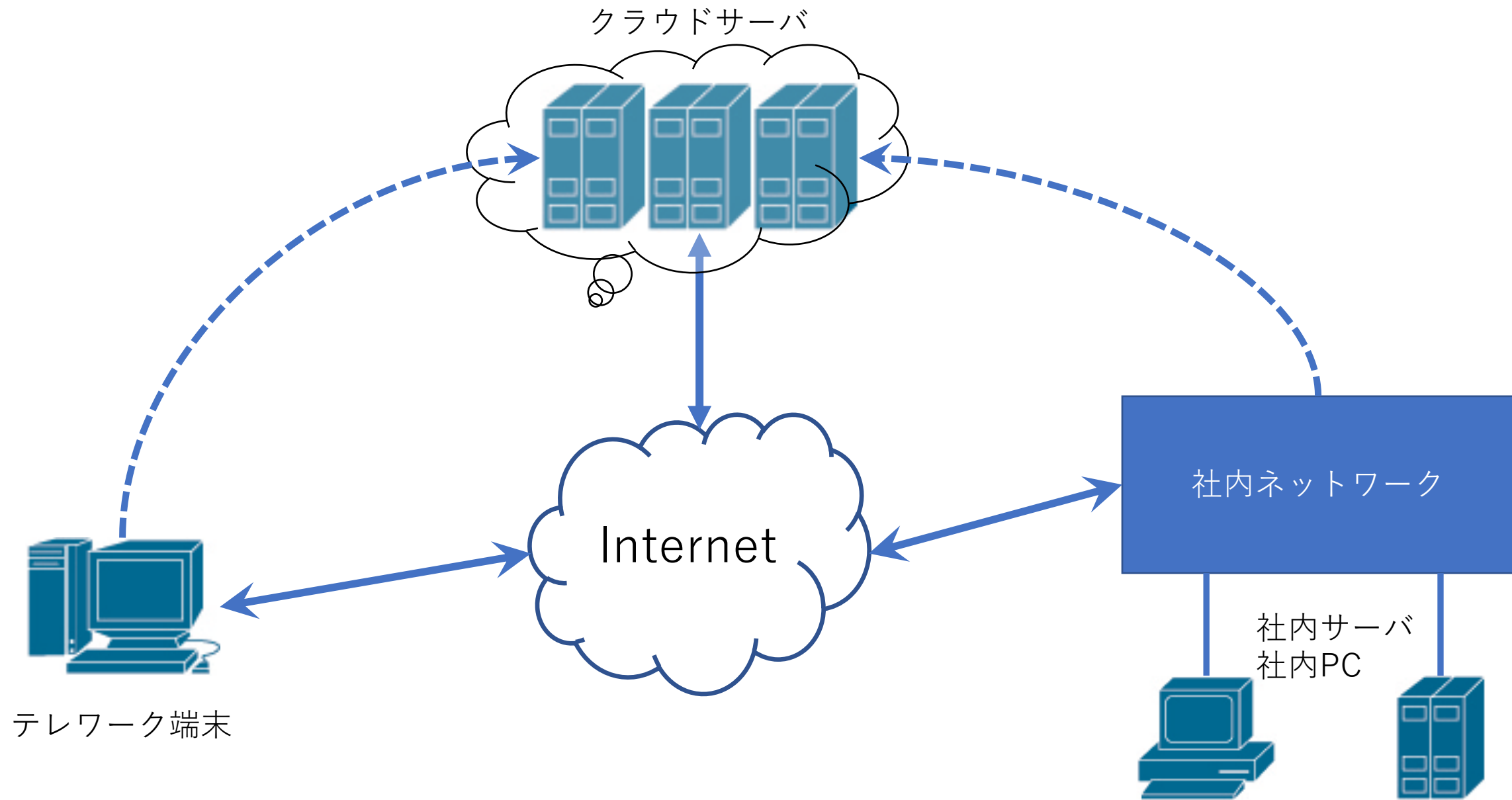


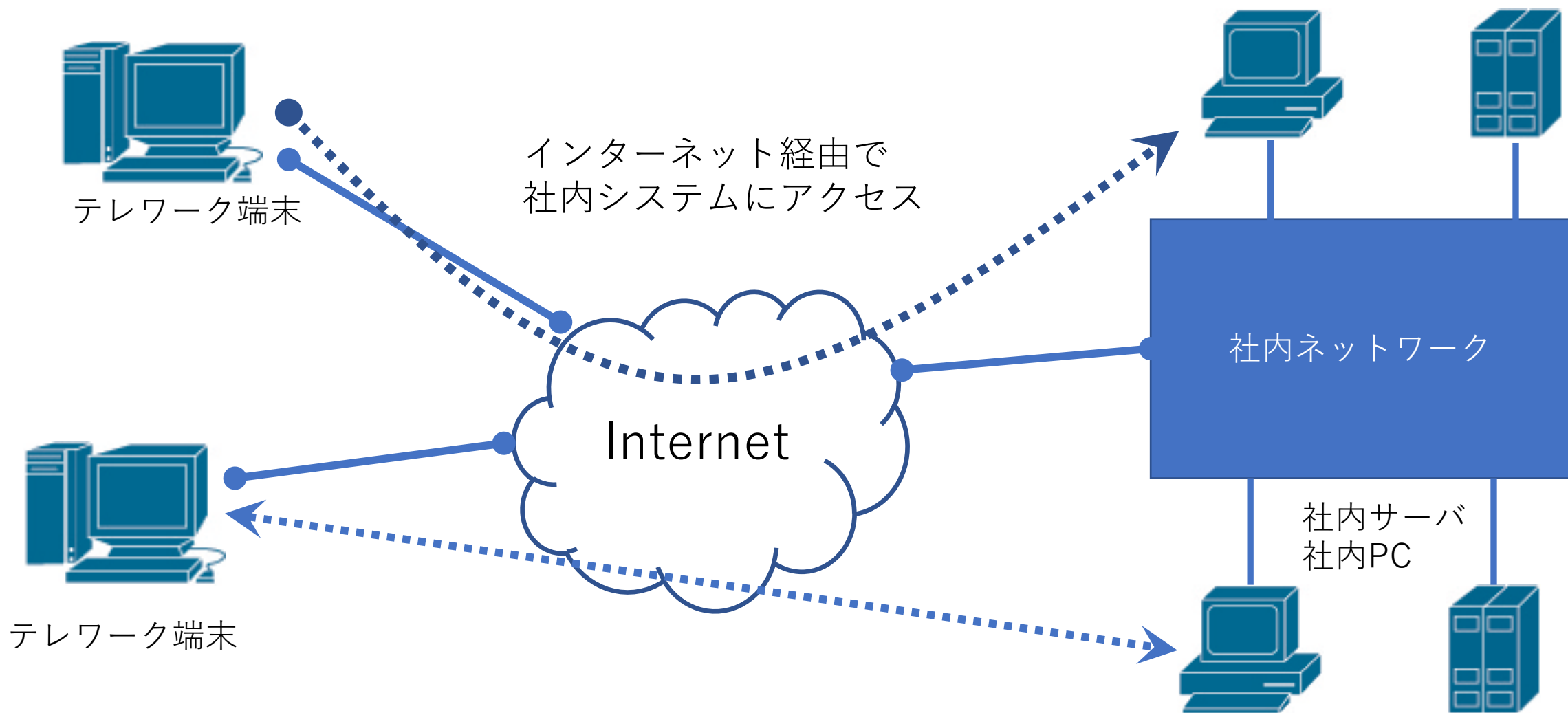
10.1.1.7

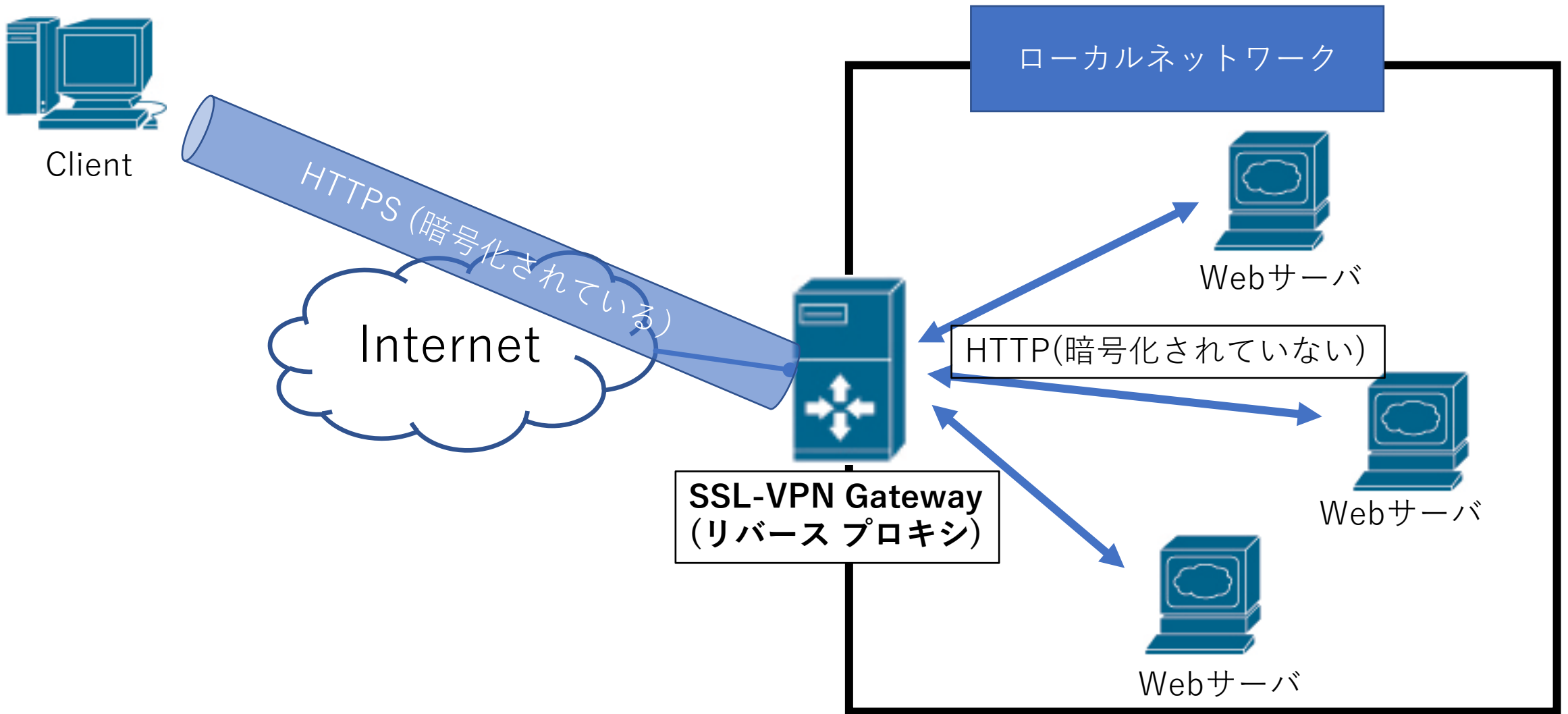
PC8



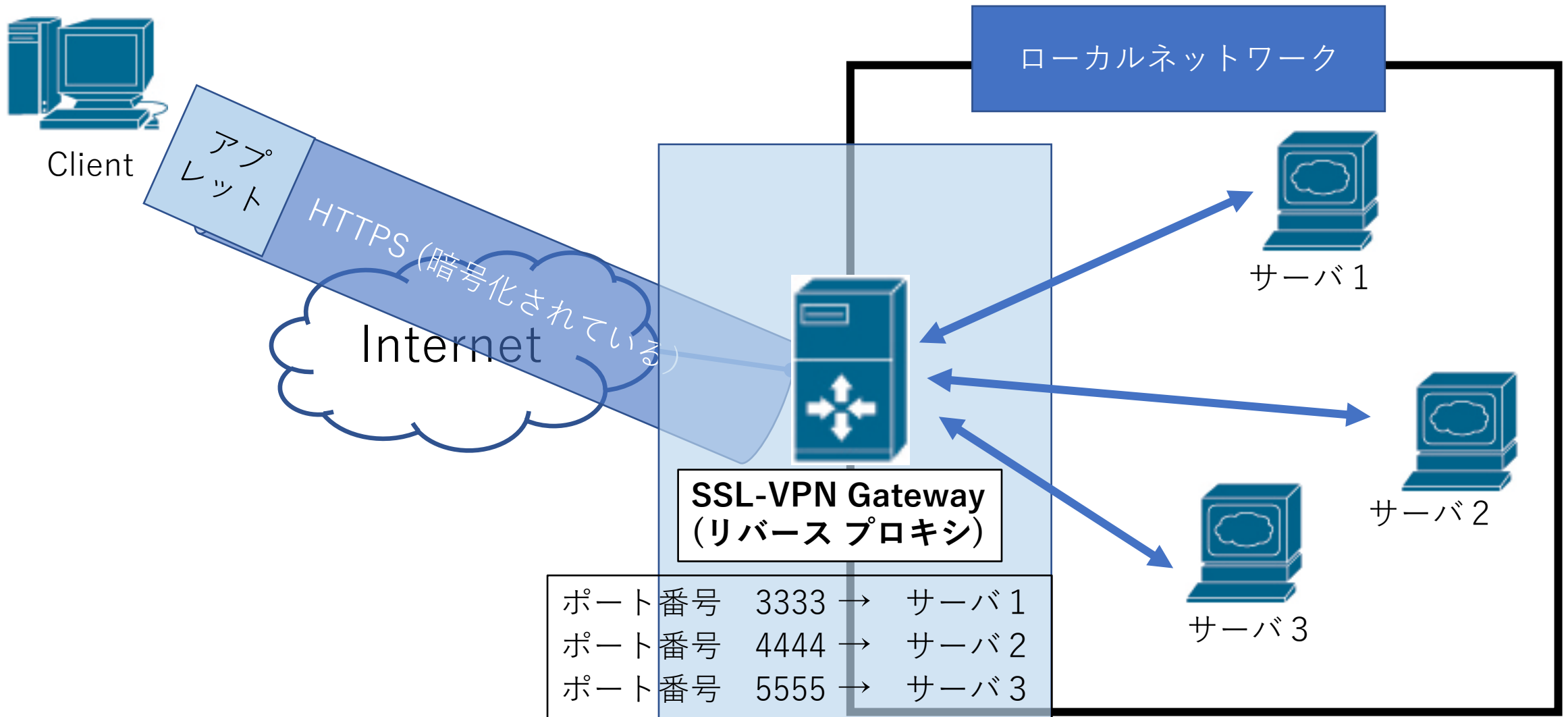
10.1.1.8











事前に対応付けておく

