

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)

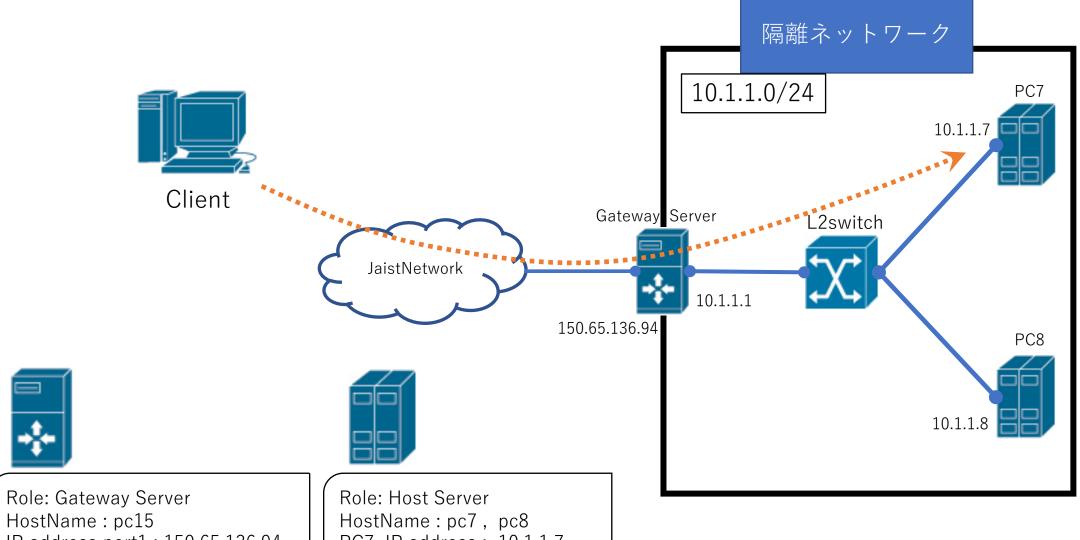
②TCPによるコネクション確立後 Telnetサーバから応答画面表示

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。



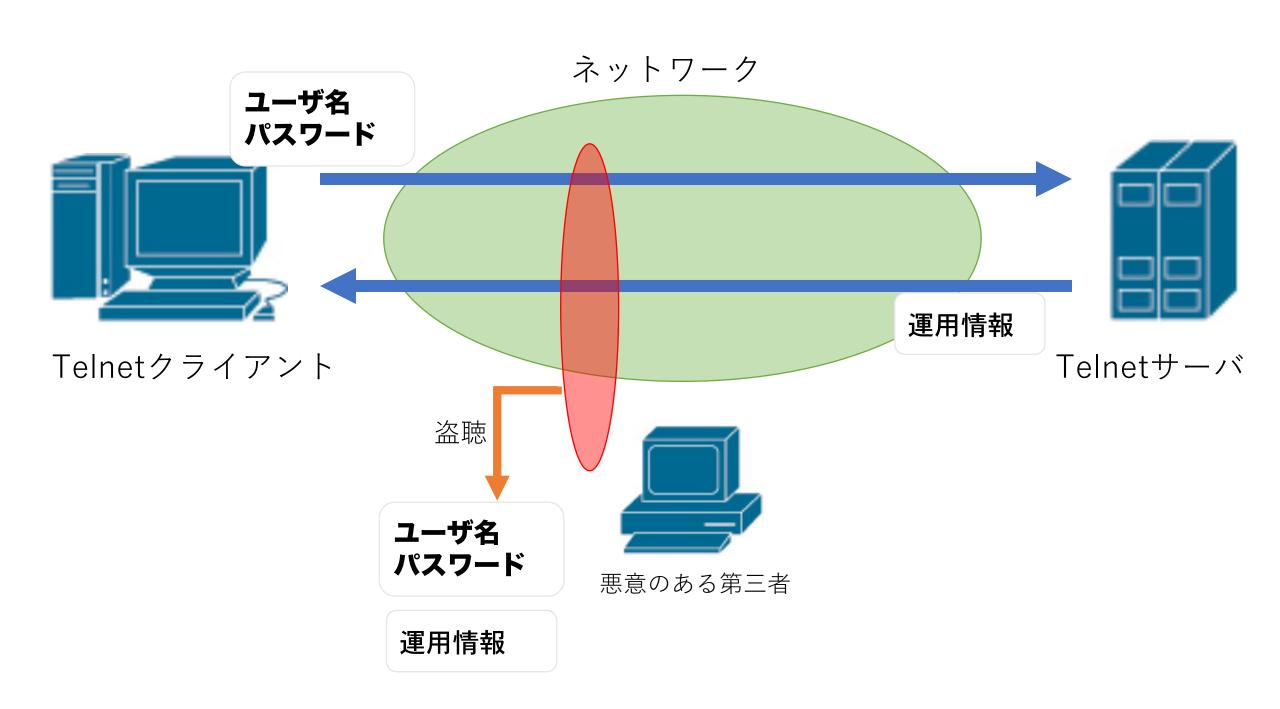
SSHサーバ IP addres: 150.65.136.94

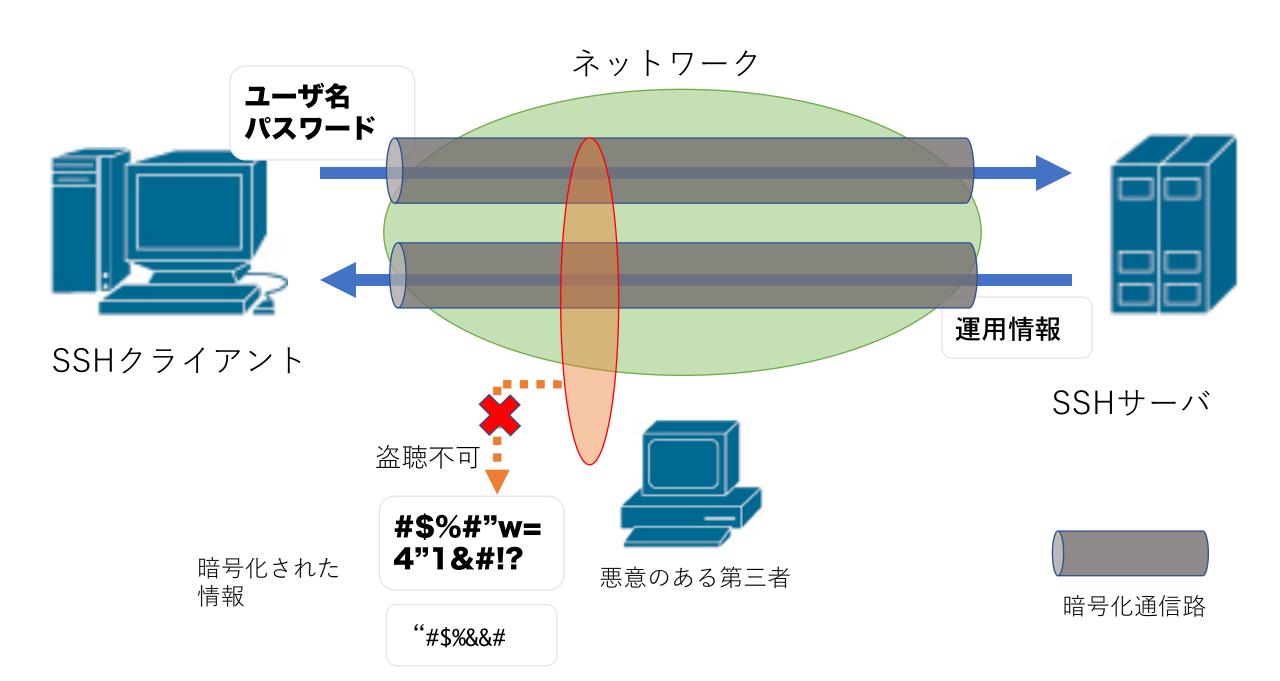


IP address port1 : 150.65.136.94

IP address port2: 10.1.1.1

PC7 IP address: 10.1.1.7 PC8 IP address: 10.1.1.8





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)

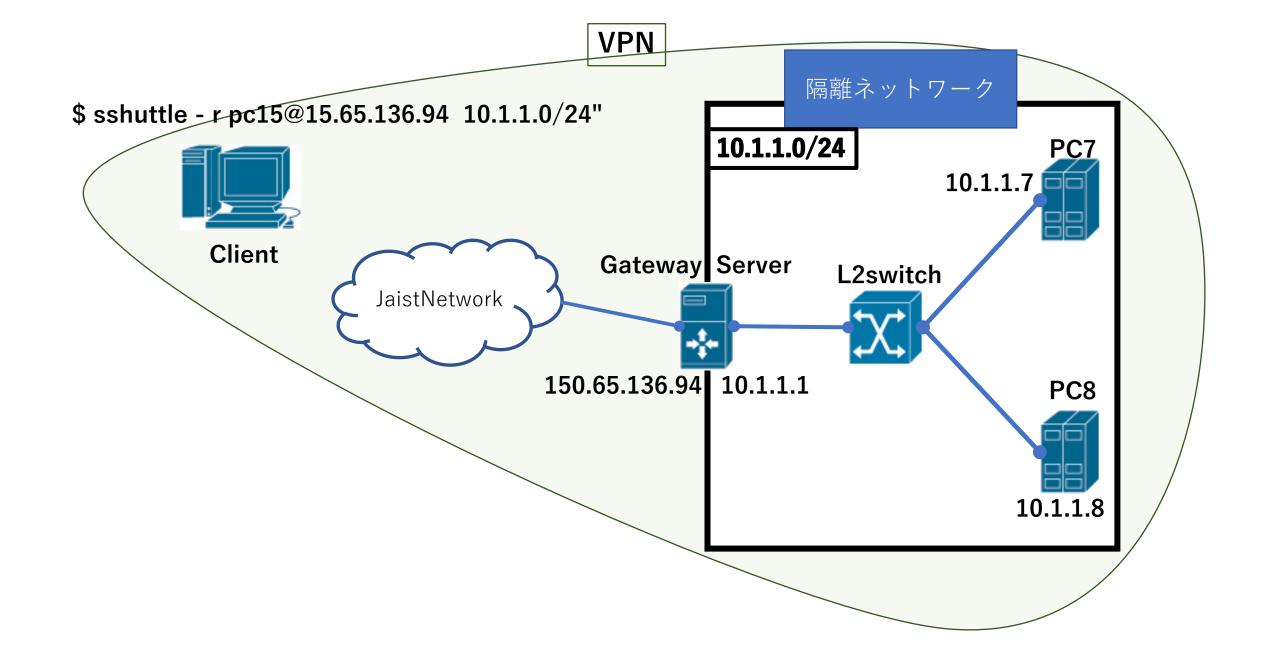
②TCPによるコネクション確立後 Telnetサーバから応答画面表示

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

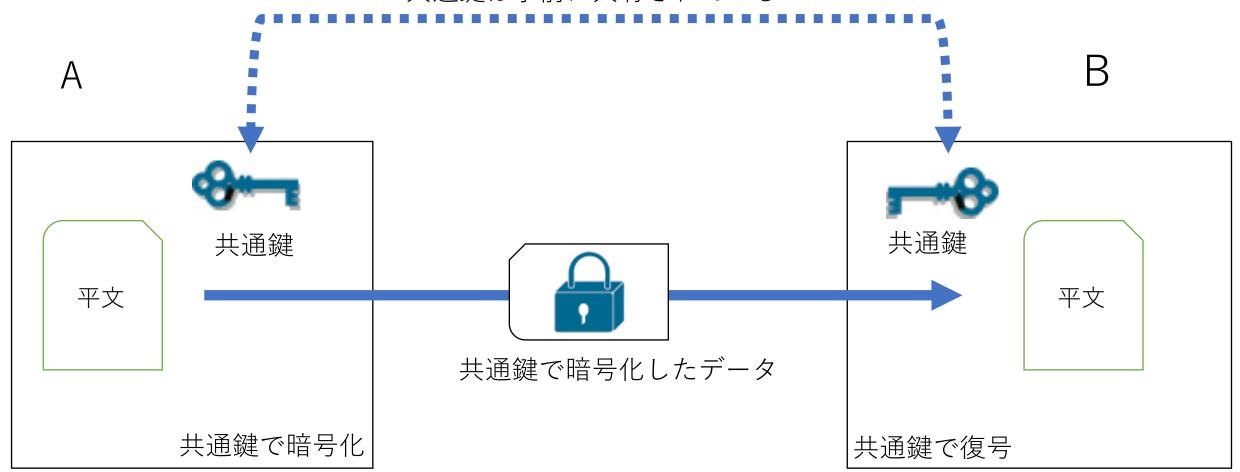
④受信したコマンドに従い処理を行い、 結果をクライアントに対して送信する。



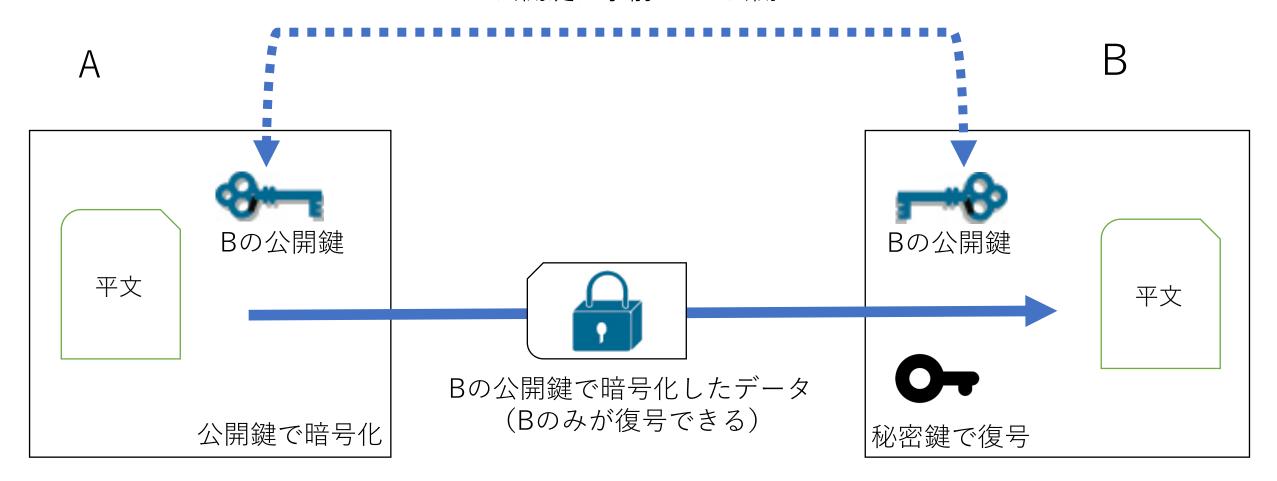
Telnetサーバ IP addres: 150.65.136.94

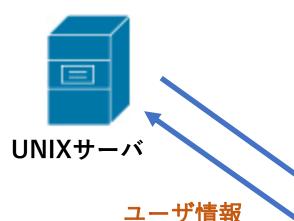


共通鍵は事前に共有されている



Bの公開鍵は事前にAに公開





アドレス情報の問い合せ



メールクライアント

ユーザ情報の問い合せ

LDAP Server

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 公開鍵情報の 問い合わせ



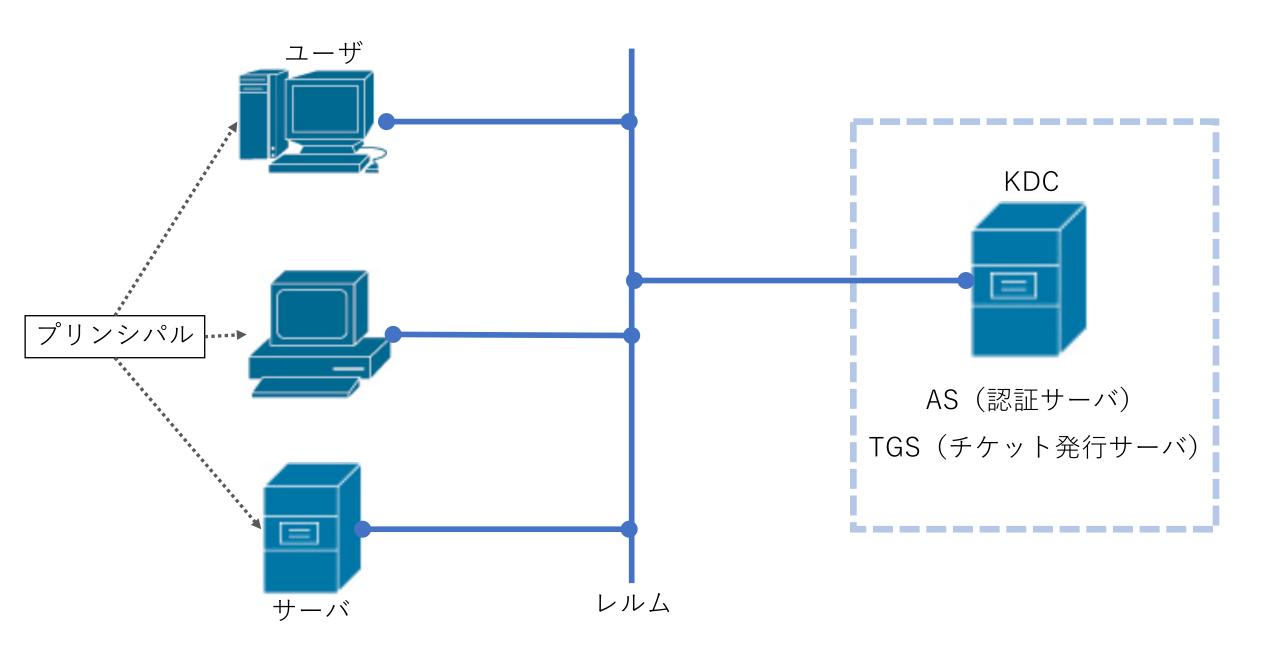


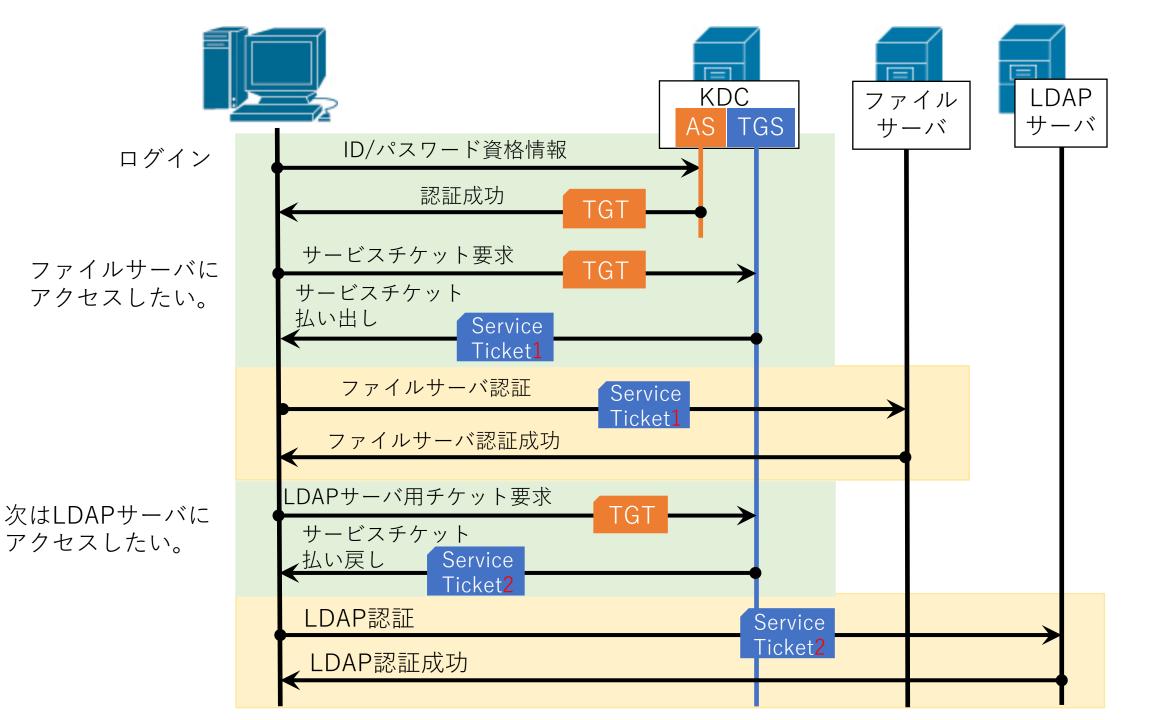
DNSゾーン情報の 問い合わせ

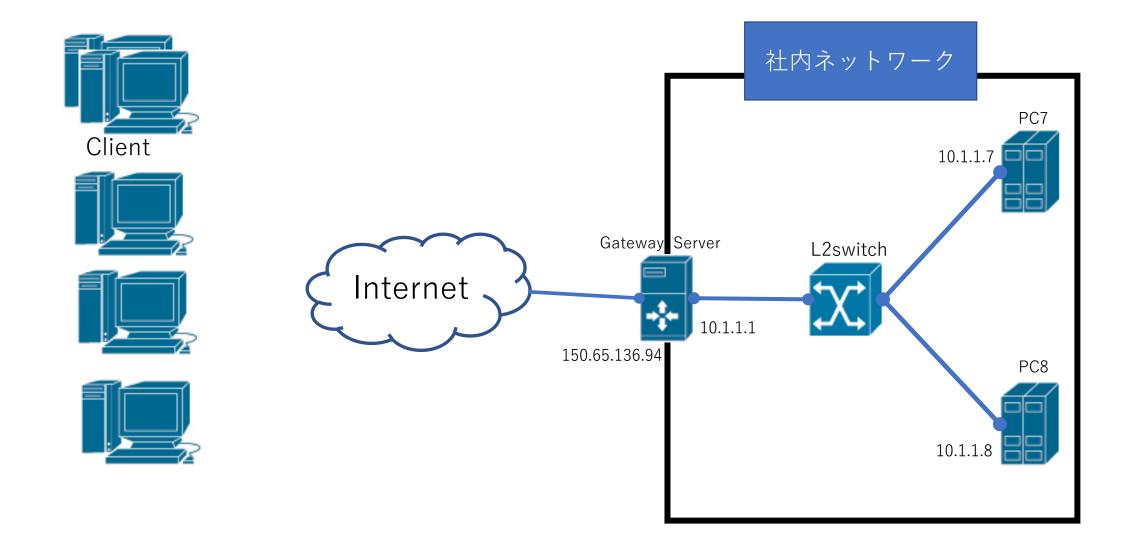
認証情報の問い合わせ

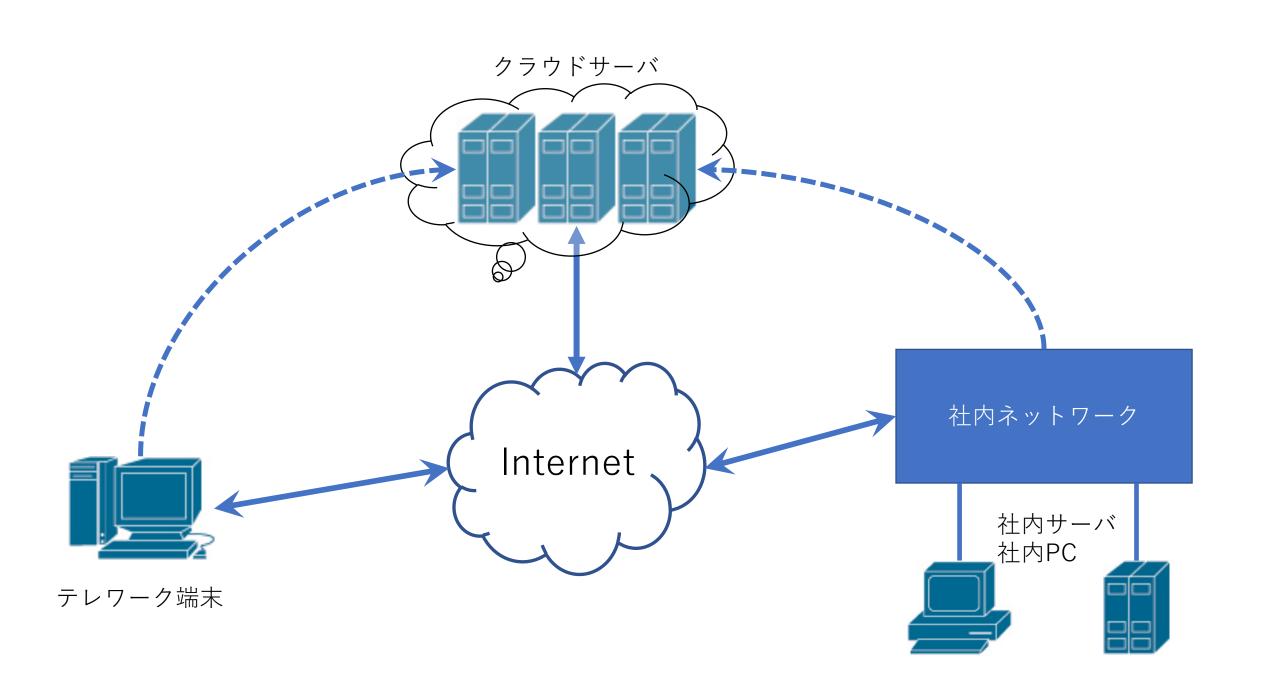


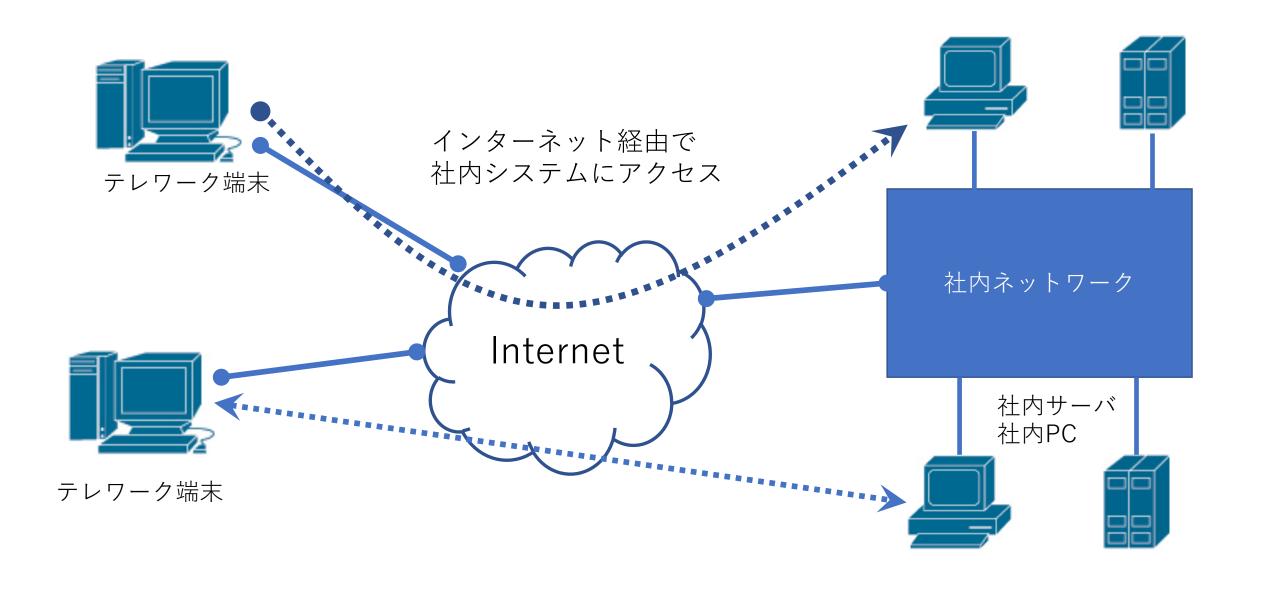
Webサーバ

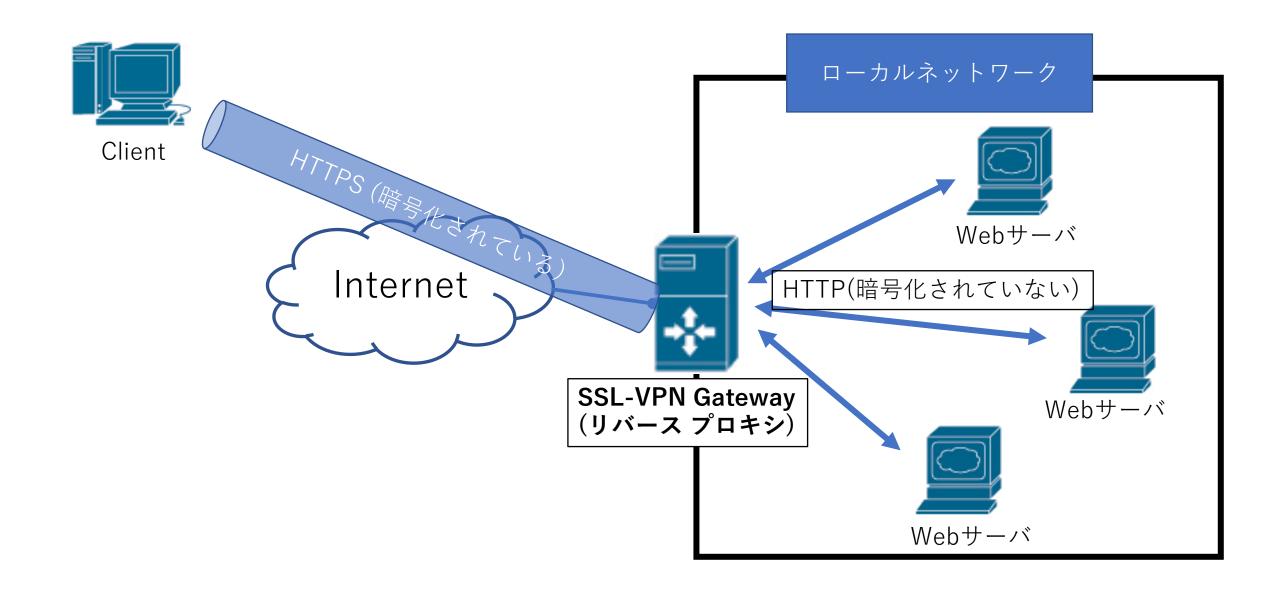


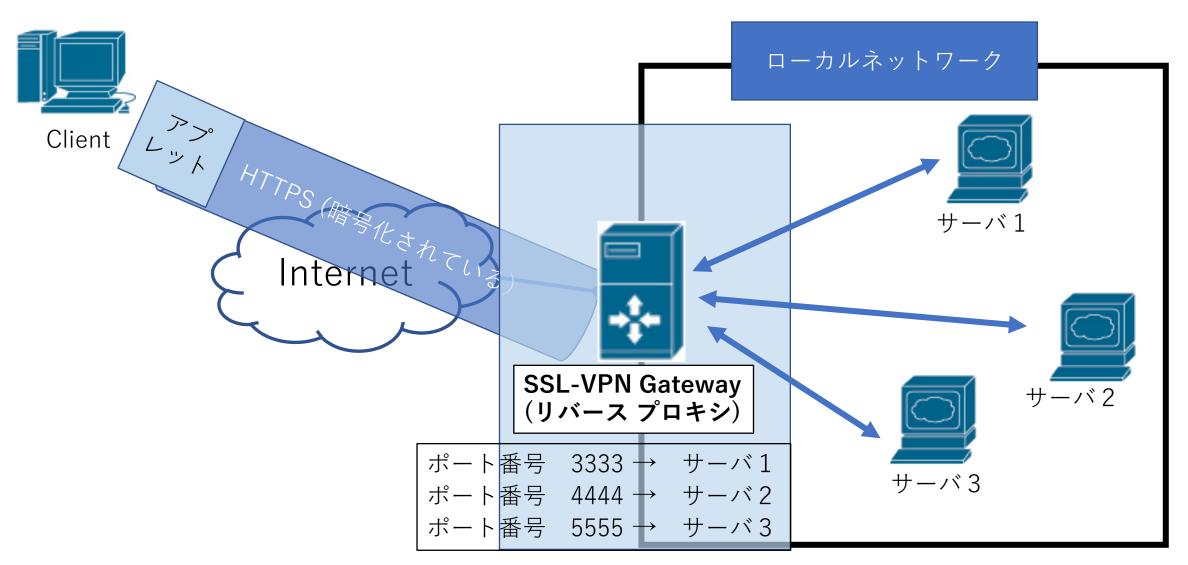












事前に対応付けておく

