ネットワークセキュリティゼミ

ゼミ担当者　：　田中 美里，山田 幸史朗
指導院生　：　天白 進也，鍵谷 武宏
開催日　：　2007 年 4 月 13 日

ゼミ内容: 本ゼミでは，TCP/IP プロトコルで通信する際に必要となる IP アドレスやプロキシサーバ，ルータの仕組みや DNS の仕組みといったような，ネットワークの基礎知識，そして SSH を用いたセキュリティの向上への取り組みとして，ポートフォワーディングや暗号方式の技術について学ぶ．

1　IP アドレス

1.1　IP アドレスの仕組み

IP アドレスとは，ネットワークに接続した機器一つを識別する番号である．OSI 基本参照モデルのネットワーク層で使用され，この数値がインターネット上で重複することはない．現在使われている IPv4 のアドレスは 32 ビットで構成されており，それを 8 ビットずつ区切って,「172.20.11.2」のように 4 つの 10 進数で表現されている．IP アドレスは前半のネットワークの番号を指し示すネットワーク部と後半の個々のコンピュータを示すホスト部から構成される．また，この二つの境界の位置によって，ネットワークに接続できるコンピュータの数が変わる．その境界の位置はネットワークの規模によって，Table 1 に示した 3 つのクラスに分けられる．

Table 1　IP アドレスクラス (領域)

クラス	先頭 8 ビット	アドレス領域
A	0xxxxxxx	0.0.0.0〜127.255.255.255
B	10xxxxxx	128.0.0.0〜191.255.255.255
C	110xxxxx	192.0.0.0〜223.255.255.255
D	1110xxxx	224.0.0.0〜239.255.255.255
E	1111xxxx	240.0.0.0〜225.255.255.255

クラス A のアドレスは，先頭 1 ビット (0) を除いた上位 7 ビットがネットワークアドレスとなり，24 ビットがホスト部となるため約 1677 万台の接続が可能である．同じようにクラス B のアドレスは，先頭 2 ビット (10) を除いた上位 14 ビットがネットワークアドレスとなり，65534 台の接続が可能であり，クラス C のアドレスは，先頭 3 ビット (110) を除いた上位 21 ビットがホスト部となり，254 台の接続が可能である．クラス D は任意の数台に一度で情報を伝達する通信するマルチキャストアドレス，クラス E は実験的な目的のための予約アドレスであり，通常の端末には利用されない．また，以下に挙げるアドレスは特別な用途で使用される為に予約されており，一般の端末用の IP アドレスとしては使用できない．

Table 2　特別なアドレス

x.x.x.0 など	ホストアドレス部分が全て 0
x.x.x.255 など	ホストアドレス部分が全て 1
127.x.x.x	先頭 8 ビットが 01111111

- ホストアドレス部分が全て 0 のアドレス

  そのネットワークそのものを表すアドレスである．

- ホストアドレス部分が全て 1 のアドレス

  ネットワークに対するブロードキャストアドレスとして用いられる．

- 先頭 8 ビットが 01111111 のアドレス

  その機器自身を表すローカルループバックアドレスとして用いられる．

また，IP アドレスはグローバル IP アドレスとプライベート IP アドレスに分けられる．グローバル IP アドレスとは，インターネットに接続された機器に一意に割り当てられた IP アドレスである．このアドレスは，インターネット上の住所に当たり，インターネット上で通信を行うためには必ず必要である．プライベート IP アドレスとは，直接インターネットに接続しないコンピュータ（LAN 上のコンピュータなど）のアドレスとして自由に利用できる IP アドレスである．プライベート IP アドレスとして使用できるアドレスは，各クラスについてあらかじめ決められており，この領域のアドレスはグローバル IP アドレスとして使用することはできない．(Table 3).

プライベート IP アドレスは，サブネットワークアドレスとホストアドレスの組み合わせによって表記される．合計は 32 ビットになるが，内訳は固定されていない．32 ビット中の左何ビットがサブネットワークアドレ

Table 3　各クラスのプライベート IP アドレス領域

クラス名	領域
クラス A	10.0.0.0〜10.255.255.255
クラス B	172.16.0.0〜172.31.255.255
クラス C	192.168.0.0〜192.168.255.255

スを示し，何ビットがホストアドレスを示すかといった両者のビット配分は，サブネットマスクという値で決める．そのため，32 ビットのプライベート IP アドレスだけでは，IP アドレスの内容を正しく表現できない．つまり，IP アドレスとネットマスクの 2 つがワンセットとなって初めてネットワーク番号とホスト番号の値を正しく表現できる．

例えば,「172.20.11.2」という IP アドレスを「255.255.255.0」というサブネットマスク値を使って分割する．するとこの IP アドレスが示すのは,「172.20.11.0」というサブネットワークアドレス上にある，ホストアドレス「2」の端末ということがわかる (Fig.1)．

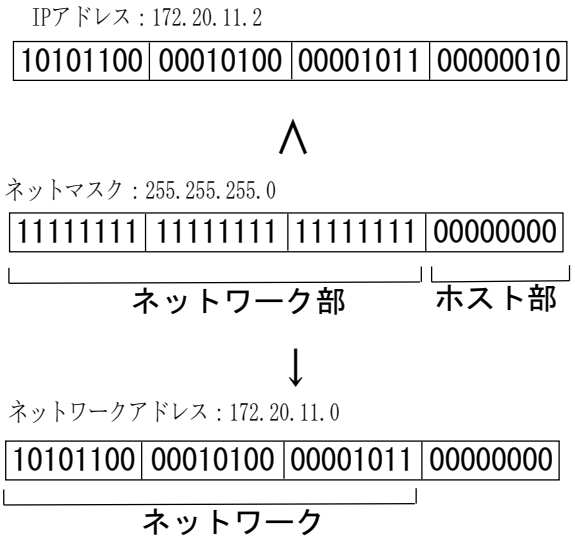

Fig. 1　サブネットマスク

1.2　ルータとアドレス変換

ルータとは，コンピュータ・ネットワークにおいて，異なる網間の中継・接続を行う通信機器である．OSI 基本参照モデルにおけるネットワーク層で動作する．ルータの役割には，LAN 間を中継するルーティング機能，アクセスリスト機能（フィルタリング），IP 変換などがある．

プライベート IP アドレスは，あくまでも LAN 内のものにすぎない．そこで，プライベート IP アドレスを割りあてられたノードがインターネットで通信を行う場合，プライベート IP アドレスとグローバル IP アドレスを相互に変換する仕組みが必要となる．代表的な技術として NAT と IP マスカレードが挙げられ，いずれもルータによってアドレス変換が行われる．

NAT では，グローバル IP アドレスとプライベート IP アドレスが 1:1 に割り当てられる．IP マスカレードはルータがパケット中継をする際，パケットに記載されている IP アドレスとポート番号を書き換えるものである．例えば，プライベート IP アドレス「172.20.11.2」のマシンから，グローバル IP アドレス「192.0.2.79」の Web サーバにアクセスするとき，ルータによってプライベート IP アドレス「172.20.11.2」からグローバル IP アドレス「95.3.8.31」に置き換える．そして，書き換える前のプライベート IP アドレスとポート番号，書き換えた後のグローバル IP アドレスとポート番号をワンセットにしてルータ内部にある対応表に記録しておく．よって相手の Web サーバに届くパケットには送り先のアドレスにルータのグローバル IP アドレスとポート番号が記載されており，Web サーバもルータのグローバル IP アドレスとポート宛にパケットを送ることになる (Fig.2)．

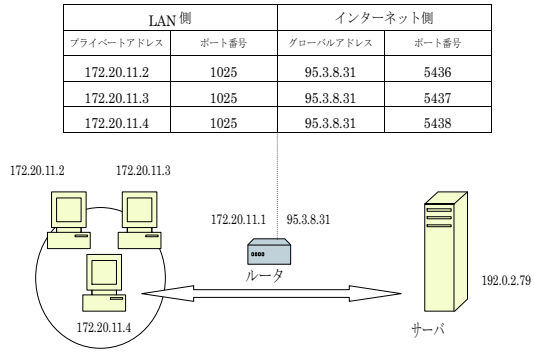

Fig. 2　ルータの仕組み

1.3　IP アドレス枯渇問題

インターネットの普及に伴い，現在使用されている IPv4 では，近い将来に IP アドレスが不足してしまうことが予想されている．そこで現在，アドレス空間の桁数を増大させた IPv6 が提案されている．ネットワークアドレスの長さを IPv4 の 32 ビットから 128 ビットにすることで，約 4.3×10^9 個しか無かった IP アドレスを約 3.4×10^{38} 個までサポートすることができる．よって，全ノードがグローバル IP アドレスを持つことができる．しかし，前述した NAT や IP マスカレードがもつ「インターネットと直接接続しない」というセキュリティ上のメリットが消える為，それらの解決や対策が今後の課題となっている．

2　DNS サーバ

2.1　DNS サーバの役割

DNS は，クライアントが Web サーバ等にアクセスする際に必要な Web サーバの IP アドレスを知るために作られた．インターネット上では IP アドレスでコンピュータの住所を示すため，クライアントが Web サーバ等にアクセスするためには，Web サーバの IP アドレスを知る必要がある．与えられたドメイン名からその IP アドレスを調べ，それを教えることが DNS サーバの役割である．

2.2　DNS サーバの構造

DNS は，“www.doshisha.ac.jp”のようなホスト名 (www) とドメイン名 (doshisha.ac.jp) を，IP アドレスに変換するための一覧表を管理している．いわば，インターネット上の電話帳のような役割を果たしている．しかし，1 つの DNS サーバが世界中のサーバの IP アドレスを管理しているわけではなく，多数の DNS サーバが Fig.3 のような木構造を成して分散管理している．

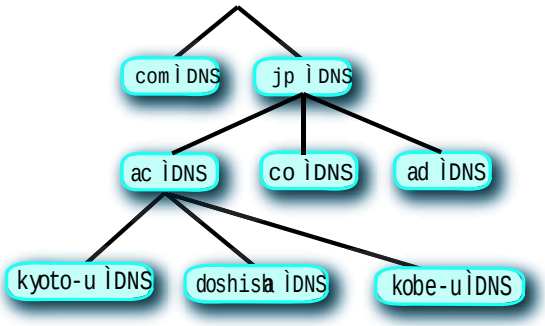

Fig. 3　DNS サーバの階層構造

2.3　DNS サーバの具体例

DNS サーバの動作はクライアントが設定した優先 DNS サーバが，クライアントの要求するサーバのアドレスを持っている場合と持っていない場合の 2 つに分かれる．ここでは同志社のサーバにアクセスする場合，まず同志社の IP アドレスを，クライアントが指定した優先 DNS サーバに問い合わせる．そして優先 DNS サーバに同志社の IP アドレスが登録されている場合は，優先 DNS サーバは同志社の IP アドレスを返す．しかし優先 DNS サーバに同志社の IP アドレスが登録されていない場合は，以下の 1 から 4 のように他の DNS への問い合わせを行う．また，その動作を図にしたものを Fig.4 に示す．

1. 優先 DNS サーバは，ルートドメインサーバに jp ドメインの DNS サーバの IP アドレスを問い合わせる．
2. 優先 DNS サーバは，jp ドメインに ac.jp ドメインの DNS サーバの IP アドレスを問い合わせる．
3. 優先 DNS サーバは，ac.jp に doshisha.ac.jp のサーバの IP アドレスを問い合わせる．
4. 優先 DNS サーバは，doshisha.ac.jp に www.doshisha.ac.jp のサーバを問い合わせ，クライアントに www.doshisha.ac.jp の IP アドレスを返す．

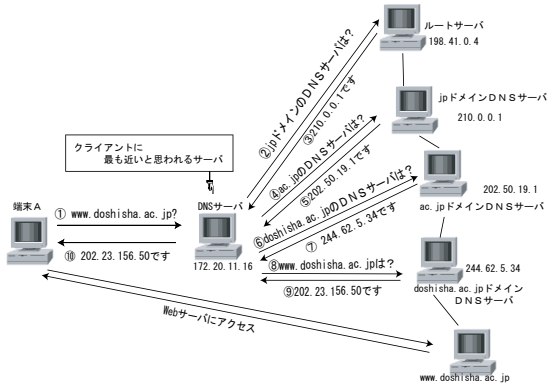

Fig. 4　DNS サーバの仕組み

3　プロキシサーバ

3.1　プロキシサーバの概要

プロキシサーバとは，プロキシ（代理）という言葉が示す通り，内部のネットワークのコンピュータに変わってインターネットとの接続を行うコンピュータのことである．ネットワークに出入りするアクセスを一元管理し，内部から特定の種類の接続のみの許可，外部からの不正なアクセスを遮断，データの高速化などを行うために用いられる．

3.2　プロキシサーバの機能

前述の役割を果たすため，プロキシサーバはフィルタリング機能を持ち，データのモニタリング，改変，通信の妨害が可能である．プロキシサーバは内部ネットワークのクライアントからインターネットへの通信要求を一度受け取り，それをインターネットに送り出して良いか判断し，問題がなければそのクライアントに代わってインターネットにデータを送出する．(Fig.5) プロキシサーバを利用せずに Web ページを閲覧する場合，ユーザのコンピュータが WWW サーバに直接アクセスするため，ユーザの IP アドレスやホスト名，ブラウザや OS の種類といった個人情報が要求先 WWW サーバと Web ページの管理者に伝わってしまうことになる．しかし，プロキシを利用することで，これを防ぐことができる．また，過去にサーバが受信したコンテンツを一時的に保存しておくキャッシング機能を持ったプロキシサーバを用いる

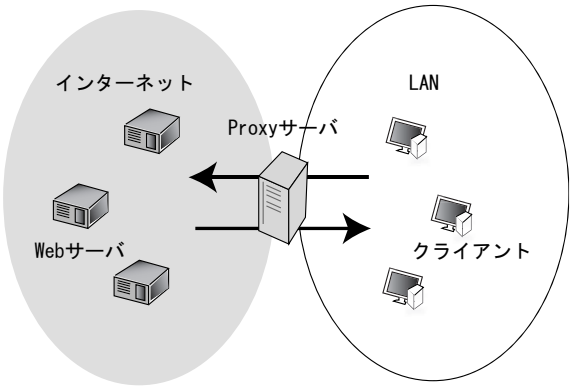

Fig. 5　プロキシサーバの仕組み

場合，ユーザがそのコンテンツへアクセスした時，プロキシサーバは自分の保有するデータを直接送り返すため，ユーザは素早くコンテンツを取得することができる．

4　URL

URL(Uniform Resource Locator) とは，インターネット上に存在する情報資源 (文書や画像など) の場所を示す記述方式のことで，インターネット上における情報の「住所」を示す.URL は一般的に Fig. 6 のように，スキーム名，ホスト名，パス名で表される.(他に，ポート番号やユーザ名，パスワードがつく場合がある)

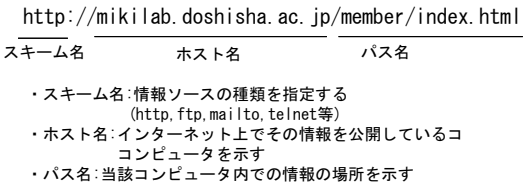

Fig. 6　URL の構成

Fig. 6 の URL では mikilab.doshisha.ac.jp というコンピュータ上の/member/で示される場所の index.html というファイルが示され，このファイルには HTTP でアクセスすればよいことが示されている．

5　パーミッション

パーミッションとはハードディスクなどに保存されているファイルやディレクトリに対するユーザのアクセス権のことである．一般に，UNIX システムにおけるアクセス権を指す言葉として用いられる．UNIX システムにおけるパーミッションは，ファイル/ディレクトリの「所有者」，同じマシンを利用できるユーザ全体を意味する「グループ」，この 2 つ以外の「その他のユーザ」に対して，それぞれ「読み込み」「書き込み」「実行」の権限を与えるかどうかを設定できる．サーバとして使用するコンピュータは多くのユーザが同時に利用し，他ユーザによるファイルの改変，削除を防ぐため，パーミッションの設定が必要になる．

UNIX コマンドで”ls -l”コマンドを入力すると，ファイルの所有者や作成日時など多くの情報が表示されるが，一番左に”-rwxr--r--”のように表示される部分がある．これがパーミッションである．Fig. 7 に示すように”r”や”w”はそれぞれが 1 ビットに対応しており，先頭ビットはファイルの型を表しており,「-」は通常ファイル,「d」はディレクトリになる．

先頭ビットを除く 9 ビットを 3 ビットずつに区切った各部分が，左から「所有者」,「グループ」,「その他」のアクセス権限である．各々の持つ 3 ビットに対しては，左から「読み込み」,「書き込み」,「実行」という 3 つのアクセス権限を表している．パーミッションは各部分ごとに許可する権限の値を足し算したもので表す．ファイルのアクセス権限を Table 4 に示す．例えば「読み取り」と「実行」の権限を与える場合は 4+1 で 5 になり，すべての権限を与える場合は 4+2+1 で 7 となる．つまり，”-rwxr--r--”という文字列は”744”という数値に置き換えることができる (Fig. 7)．また対象がディレクトリの場合，Table 5 のようになる．

Table 4　ファイルのアクセス権限

権限	表示	8 進数表記
読み取り権限	r (read)	4
書き込み権限	w (write)	2
実行権限	x (execute)	1

Table 5　ディレクトリのアクセス権限

r	ディレクトリ情報読み取り権限
w	ファイル作成権限
x	カレントディレクトリ変換権限

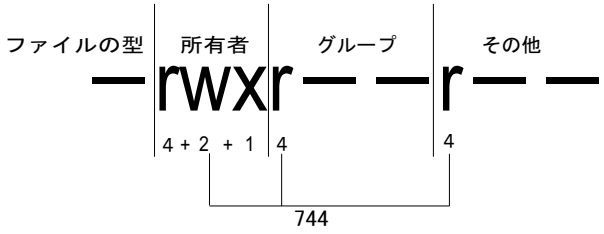

Fig. 7　パーミッションの表記

6　共通鍵暗号方式

共通鍵暗号方式 (Common key cryptosystem) とは暗号化と復号化に同じ鍵を用いる，または鍵の一方から他方が用意に入手可能な暗号方式である．共有鍵暗号方式,

秘密鍵暗号方式とも呼ばれ，公開鍵暗号方式が発明されるまでは，暗号と言えば共通鍵暗号方式のことであった．代表的なアルゴリズムには DES，AES がある．

共通鍵暗号方式は計算量が少なく処理速度が速い反面，鍵の配布・管理負担が大きい．配布については，盗聴を避けるため，安全な配布方法を用意する必要がある．また，通信先ごとに固有の鍵を作成しなければならないため，通信相手が増える度に鍵管理の負担が増大する．このシステムの概要を Fig. 8 に示す．

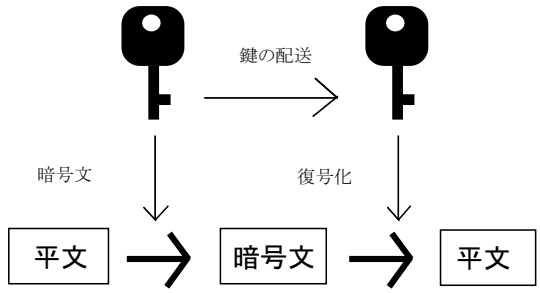

Fig. 8　共通鍵暗号方式

7　公開鍵暗号方式

公開鍵暗号方式とは，対になる 2 つの鍵を使ってデータの暗号化・復号化を行なう暗号方式のことで，RSA などが代表的なアルゴリズムとして挙げられる．1 つ目の鍵は**公開鍵**と呼ばれ，広く一般的に公開される．2 つ目の鍵は**秘密鍵**と呼ばれ，本人のみがわかるように厳重に管理される．秘密鍵で暗号化されたデータは対応する公開鍵でしか復号できず，公開鍵で暗号化されたデータは対応する秘密鍵でしか復号できない．

暗号化と復号化に用いる鍵が同じ共通鍵暗号方式に比べ，処理に時間がかかる．しかし公開鍵の共有が容易であること．受信者側は通信先の数に関係なく，秘密鍵と公開鍵の対を 1 つ持てば良いことなど，管理面の負担は少ない．このシステムの概要を Fig. 9 に示す．

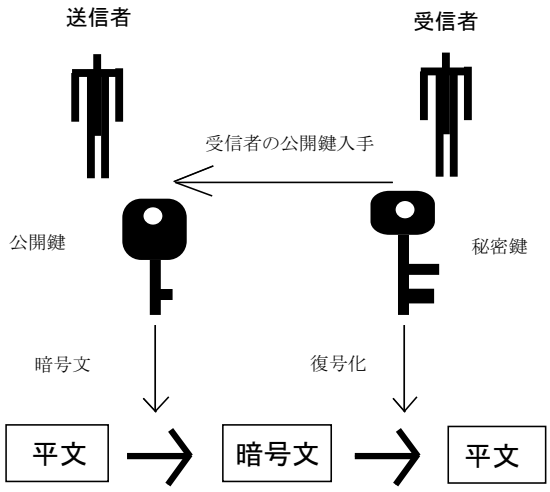

Fig. 9　公開鍵暗号方式

8　SSH について

8.1　SSH の概要

SSH（Secure SHell）とはネットワークを介して別のコンピュータにログインし，遠隔地のマシンでコマンド操作をするためのプログラムである．ネットワーク上を流れるデータは暗号化されるため，インターネット経由でも一連の操作を安全に行うことができる．SSH と SSH2 という 2 つのバージョンが存在するが，前者には脆弱性が発見されているため，利用は推奨されていない．また，暗号化しない SMTP や FTP の通信路を暗号化するポートフォワーディングの機能も有する．SSH では，以下に示す「ホスト認証」「通信内容の暗号化」「ユーザ認証」の 3 つの仕組みにより通信のセキュリティを確保している．

8.2　ホスト認証

SSH は通信を行う際に相手となる**サーバ**（リモートホスト）が正しいマシンであることを確認する．これはサーバに「なりすまし」てアクセスを受け付け，ユーザ（ローカルホスト）の個人情報を盗むといった攻撃を防ぐのに有効である．公開鍵暗号方式を用いたホスト認証の流れを以下に示す．

1. ユーザは乱数によって finger print というデータを作成し，公開鍵で暗号化してサーバに送信
2. サーバは受信した finger print を秘密鍵で復号して，ユーザに送り返す
3. サーバから受信したデータと finger print を比較する事で，ホストの認証を行う

8.3　通信内容の暗号化

SSH ではホスト認証が終わった後，ユーザ側が使い捨ての共通鍵を作り，公開鍵で暗号化してサーバに送信する．以降やりとりされるデータは，この共通鍵によって暗号化される．このように処理時間の短い共通鍵を，公開鍵暗号方式で送信する方式をハイブリッド方式といい，SSH はこの方式を利用する事で，安全かつ高速な通信を行うように設計されている．

8.4　ユーザ認証

ホスト認証が終わった後はユーザ認証を行う．ユーザ認証にはパスワード認証と公開鍵暗号方式による認証がある．SSH2 ではユーザ側が公開鍵を準備している場合にはこの公開鍵を用いた認証，準備していなければパス

ワード認証を行う．パスワードの認証を行う場合、ホスト認証後に作成した共通鍵によってパスワードを暗号化している。

以下にそれぞれの手順を示す.

- パスワード認証

1. 各ユーザにあらかじめ割り当てられたパスワードを用いて認証を行う

- 公開鍵認証

1. 公開鍵と秘密鍵の対を作成し，サーバには公開鍵を登録し，ユーザはパスフレーズによって暗号化された秘密鍵を所有する
2. ユーザはアクセスするサーバにユーザ名を送信
3. サーバは乱数を生成し，登録されているユーザの公開鍵によって暗号化し，ユーザに送信
4. ユーザはパスフレーズの入力によって秘密鍵を復号し，サーバからの受信データをその秘密鍵で復号
5. 受信したデータのハッシュ値をサーバへ送信
6. サーバは元の乱数のハッシュ値と受信したハッシュ値を照合し，ユーザを認証する．

認証の安全性の見地に立てばネットワークにパスワードを流さずにすむ公開鍵認証の方が安全である．しかし，ユーザの秘密鍵が盗まれる場合，およびユーザのローカルマシンが勝手に操作される場合，無断でログインされる可能性がある．そのため，ユーザの秘密鍵は常時は暗号化して保存し，認証の際にパスフレーズによって復号するという手法がとられている．以下にユーザ認証に公開鍵を用いた SSH の認証手順を示す.

8.5　ポートフォワーディング

ポートフォワーディングとは，特定のポートから受け取ったデータを他のポートへ転送することをいう．SSH におけるポートフォワーディング機能といえばトランスポート層の通信を暗号化する機能のことである．Fig. 11 にその概要をしめす.

ここでは，具体例としてメールクライアントと，メールサーバの送受信を扱う．メールの送受信には **POP**, **SMTP** がよく利用されるが，これらのプロトコルでは通信経路が暗号化されていないのでパスワードなどを平文で流してしまっている．そこで Fig. 11 のようにメールクライアントとメールサーバの間に SSH を組み込むことで暗号化して送受信を行うことができる.

ポートフォワーディングを行うためには,「自分のどのポートに送られてきたデータを」,「どの相手の」,「どのポートに」フォワーディングをするかを設定する必要がある．例えば putty の「SSH ポートフォワーディングのオプション（カテゴリ：接続→ SSH →トンネル)」において以下のように設定した場合、

L8025　　mikilab.doshisha.ac.jp:25

このとき，ユーザがローカルホストの 8025 番のポートにアクセスすると，mikilab の 25 番にアクセスすることになる．より具体的に言えば，ユーザがローカルホストの SSH クライアントの 8025 番ポートにアクセスすると，SSH クライアントは暗号化されたセキュアな通信路を確立し，リモートホストである mikilab の SSH サーバの 25 番にアクセスしてデータのやりとりを行う.

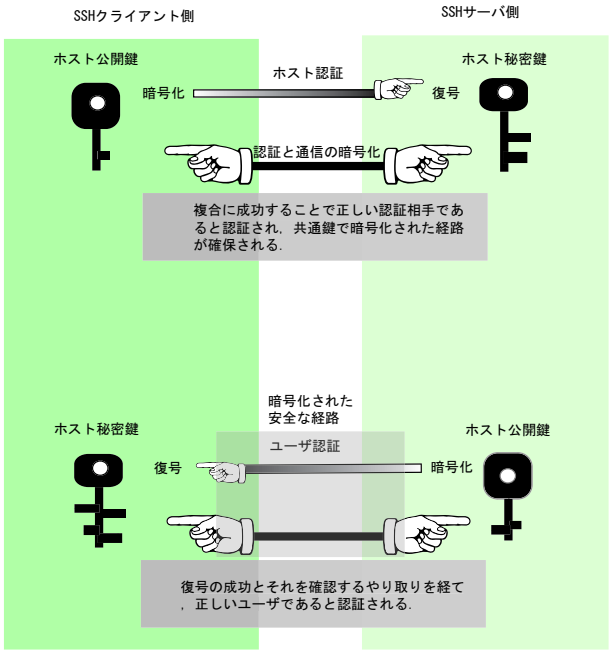

Fig. 10　SSH 認証の手順

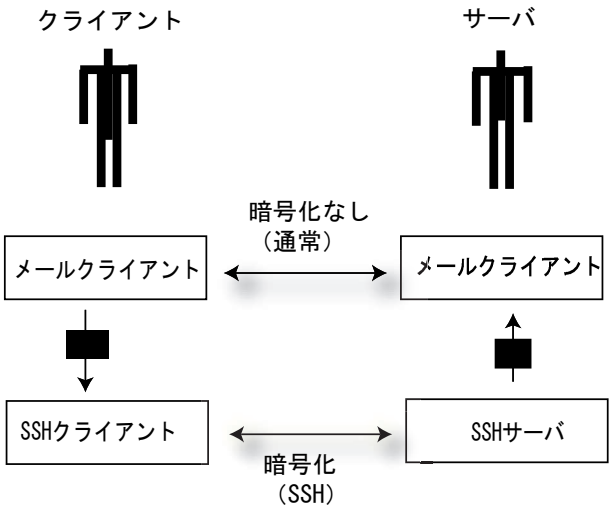

Fig. 11　ポートフォワーディング