第 1 回 ネットワークセキュリティゼミ

ゼミ担当者　：　福田 正輝，青木 大，鍵谷 武宏
指導院生　：　吉井 健吾，天白 進也，山崎 弘貴
開催日　：　2006 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ー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一つを識別する番号である．今使われている IPv4 のアドレスは 32 ビットで構成されており，8 ビットずつ区切って「172.20.11.2」のように 10 進数で表現されている．IP アドレスの中身を大きく分けると，ネットワークの番号を指し示す前半のネットワークアドレス部分と，個々のコンピュータを示す後半のホストアドレス部分の 2 つに分かれる．ネットワークアドレス部分とホストアドレス部分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 及び Table 2 に示した 5 つのクラスに分けられている．

Table 1　IP アドレスクラス (境界)

クラス名	ネットワークアドレス部分
クラス A	先頭 1 ビットを除いた上位 7 ビット
クラス B	先頭 2 ビットを除いた上位 14 ビット
クラス C	先頭 3 ビットを除い上位 21 ビット
クラス D	上位 4 ビットを除いた全部分
クラス E	上位 4 ビットを除いた全部分

Table 2　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	240.0.0.0〜255.255.255.255

このうち，クラス D のアドレスはマルチキャストアドレス，クラス E のアドレスは実験的な目的のための予約アドレスであり，通常の端末には使用されない．また，Table 3 に挙げたアドレスは特別な用途で使用されるために予約されており，これらのアドレスも一般の端末用の IP アドレスとしては使用できない．

Table 3　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

  ブロードキャストによる通信を行う際に使用されるアドレスである．

- 先頭 8 ビットが 01111111 のアドレス

  あるコンピュータにおいて，そのコンピュータ上で動作しているサーバソフトウェアに接続する際に，そのコンピュータの正式な IP アドレス以外に「自分自身」を示す IP アドレスを使って接続するために使用されるアドレスである．

Table 3 の予約された IP アドレス以外はすべてユーザが自由に利用できることになっているが，インターネットに接続するような場合には，ほかのホストと IP アドレスが衝突しないようにしなければならない．一般的には，インターネットに接続するホストには**グローバル IP アドレス**を付け，組織内部のネットワークでは，**プライベート IP アドレス**を付ける．

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，インターネットの中での住所に当たり，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出来ない (Table 4).

Table 4　各クラスのプライベートアドレス領域

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

プライベート IP アドレスは，サブネットワーク番号とホスト番号の 2 部分の組み合わせにより表記される．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番号を示し，何ビットがホスト番号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).

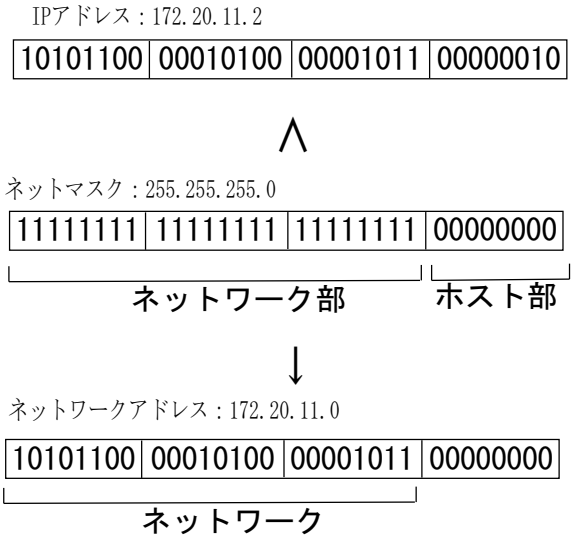

Fig. 1　サブネットマスク

1.2　ルータとアドレス変換

プライベート IP アドレスはあくまでも LAN 内用のものにすぎないため，これを利用する端末は直接インターネットに接続することが出来ない．そこで，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になる．この機能を担うのがルータである．ルータのアドレス変換の仕組みは，パケット中継するときに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アドレス「172.20.11.2」からグローバルアドレス「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).

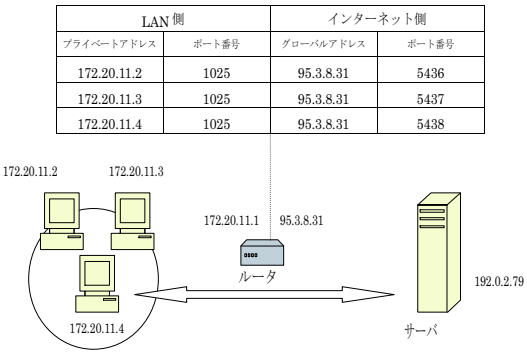

Fig. 2　ルータの仕組み

2　DNS サーバ

2.1　DNS サーバの役割

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．

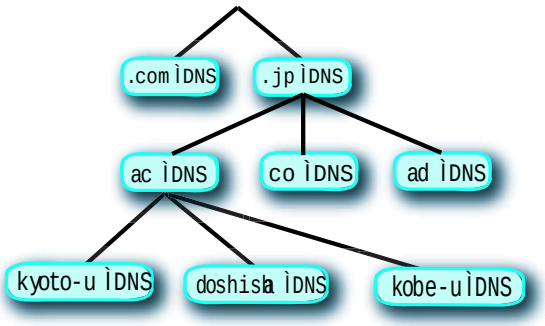

Fig. 3　DNS サーバの階層構造

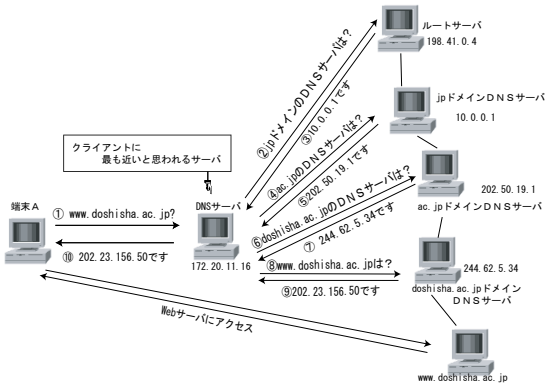

Fig. 4　DNS サーバの仕組み

2.3　DNS サーバの具体例

DNS サーバの動作に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二つの場合がある．ここでは同志社のサーバ（www.doshisha.ac.jp）にアクセスするときを例に挙げて，DNS サーバの動作についての具体例を示す．クライアントが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，クライアントが設定した優先 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 アドレスが登録してあるならば，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 5 の動作を行う．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，「www.doshisha.ac.jp」の IP アドレスが登録されていなかったため，ほかの DNS サーバに問い合わせる．
2. 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．
3. 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．
4. 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．
5. 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．

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を許可したり，外部からの不正なアクセスを遮断するために用いられる．

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 LAN 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よいものかどうかを調査して，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．この結果，インターネットから送られてきたデータについても，プロキシサーバはクライアントとインターネット・サーバの間を仲立ちして，やり取りされるデータを監視し，問題のあるアクセスを未然に防ぐ.(Fig.5).

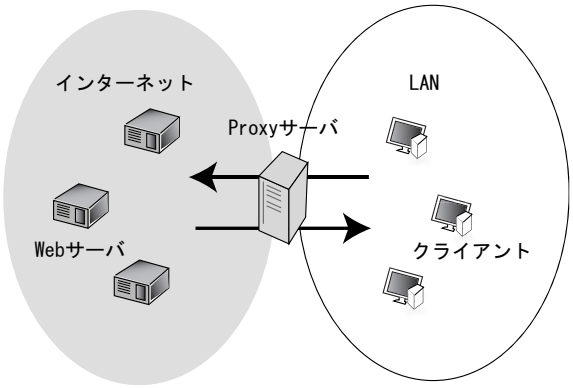

Fig. 5　プロキシサーバの仕組み

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が，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という機能を持ったプロキシサーバを用いる場合，ユーザがこのコンテンツへアクセスしようとした場合，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) の場所を指し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. 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)

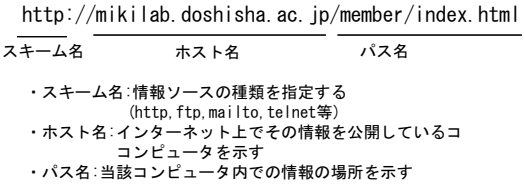

Fig. 6 URL の構成

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パーミッションである．Fig. 7 や Fig. 8 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，先頭のファイルの型を表すビットを除いた 9 ビットを 3 ビットずつ区切った各部分が，左から「所有者」,「グループ」,「その他」を表している．その 3 つに対して,「読み込み」,「書き込み」,「実行」の 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 5 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，ディレクトリの場合，Table 6 のようになり，パーミッションの先頭のファイルの型には d が入り，”drwxr--r--”のようになる (Fig. 8).

Table 5 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 6 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

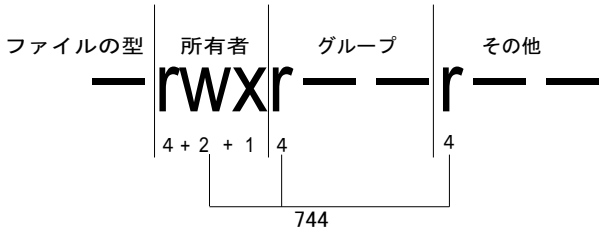

Fig. 7 パーミッションの表記

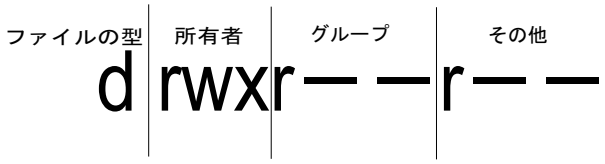

Fig. 8 ディレクトリのパーミッションの表記

6 共通鍵暗号方式

共通鍵暗号方式とは暗号化と復号化に同じ鍵を用いる暗号方式のことで，暗号文の送信者と受信者で同じ鍵を共有する必要があるため,「共有鍵暗号」または「共通鍵暗号」とも呼ばれる．暗号文を送受信する前に，あらかじめ安全な経路を使って共通の鍵を共有する必要がある．公開鍵暗号が発明されるまでは，暗号といえば共通

鍵暗号のことであった．共通鍵暗号方式は扱いが簡単であり，処理速度が速い半面，相手先ごとに固有の鍵を作成しなければならないこと，あらかじめ安全な方法で相手に鍵を渡さなければならないことから，限られた特定の相手とのやり取りに向いている．このシステムの概要を Fig. 9 に示す．

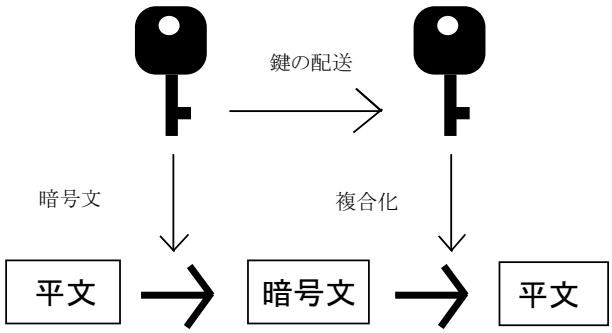

Fig. 9　共通鍵暗号方式

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，非対称暗号とも呼ばれる．1 つ目の鍵は他人に広く公開するため**公開鍵**と呼ばれ，2 つ目の鍵は本人だけがわかるように厳重に管理されるため**秘密鍵**と呼ばれる．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，公開鍵の共有が容易であること．通信する相手の数に関係なく，公開鍵が 1 つでよいことなど，安全性が高い．このシステムの概要を Fig. 10 に示す．

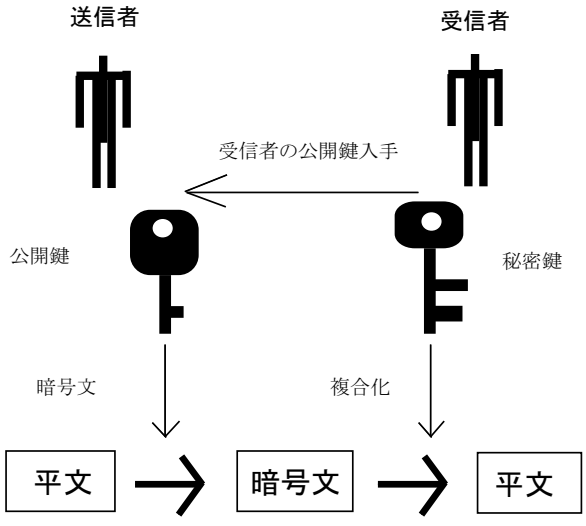

Fig. 10　公開鍵暗号方式

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．telnet や ftp でも同様の操作が可能だが，これらのプログラムでは，ネットワークを流れるデータは暗号化されていないため，世界中が接続可能なインターネット環境で用いるのは危険であると考えられる．そのため，これらの問題を解消するため，SSH が用いられる．SSH 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**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，ユーザの個人情報を盗むといった攻撃を防ぐために有効である．ホスト認証の流れを以下に示す．

1. 乱数によって finger print というデータを生成し，公開鍵で暗号化してサーバに送信
2. サーバは，サーバ秘密鍵で暗号化してサーバに送信する
3. finger print を比較することで，ホストの認証を行う

8.3　通信内容の暗号化

SSH はホスト認証が終った後クライアントは通信の暗号・復号を行うための共通鍵を作り，公開鍵暗号方式によってサーバに共通鍵を送信する．以後の通信はこの共通鍵による暗号化によって守られる．これは公開鍵による暗号化処理が共通鍵によるものより時間がかかるからである．SSH はこのようにお互いの認証には公開鍵暗号を，そして実際の通信には共通鍵暗号を使うことで安全で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，ホスト認証と同様の公開鍵の認証をユーザ単位で行う方法がある．SSH2 ではユーザ側が鍵の準備をしている場合にはこの鍵を用いた認証，準備していなければパスワード認証を行う．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，秘密鍵のペアを作成し，サーバに登録しておく
  2. アクセスするユーザ名をサーバに送る
  3. 乱数を生成し，登録されているユーザの公開鍵で乱数を暗号化し，クライアントに送信
  4. パスフレーズの入力によって秘密鍵を復号化し，受信したデータを秘密鍵で復号化する
  5. 復号化したデータのハッシュ値をサーバへ送信
  6. 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のでユーザ毎に公開鍵を作成したほうが安全である．そこで，ユーザの秘密鍵は暗号化して保存し，それを用いるとき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．また，このしくみではユーザの秘密鍵が盗まれた場合，自由にサーバと通信することができる．そこで，ユーザの秘密鍵は暗号化して保存し，それを用いるとき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 SSH 認証の手順を示す (Fig. 12).

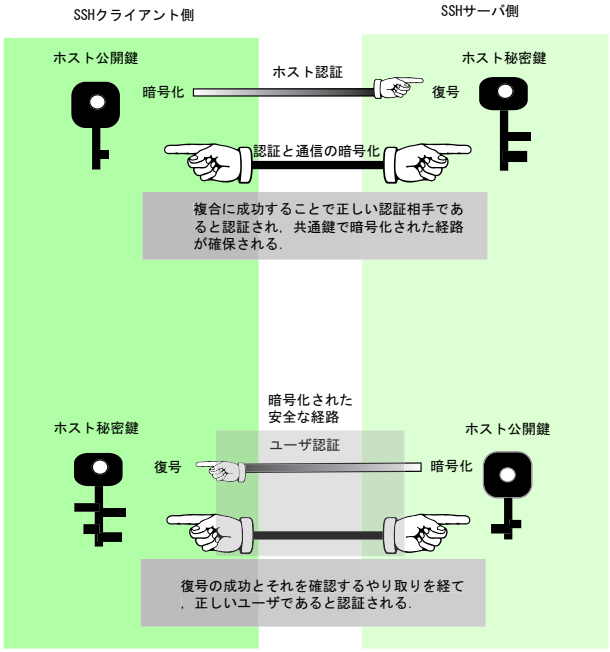

Fig. 11　SSH 認証の手順

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，暗号化できない通信の間に立って暗号化経路を SSH が作ってくれる機能である．つまり，ポートフォワーディングによって暗号化されていない通信の暗号化も可能になる．Fig. 12 にその概要をしめす.

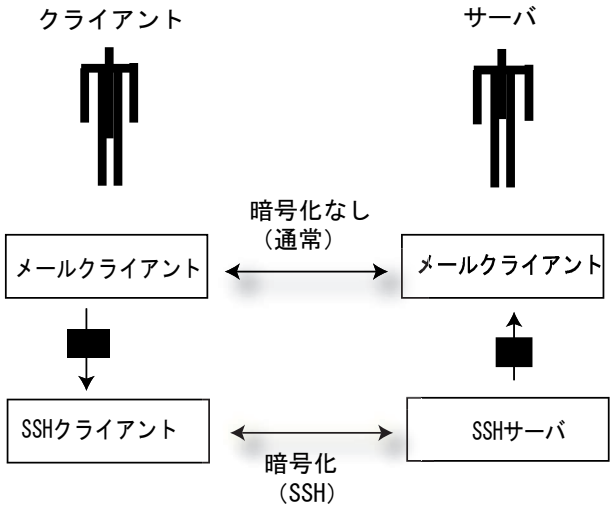

Fig. 12　ポートフォワーディング

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，この通信は暗号化されていないのでパスワードなどを平文でネットワークに流してしまっている．そこで Fig. 12 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．

たとえば，8025 番ポートに送られてきたデータを，mikilab の 25 番ポートに SSH で送りたい場合は，

L8025:mikilab.doshisha.ac.jp:25

のように設定すればよい．そして，8025 ポートにメールクライアントからデータを送るように設定しておけば SSH によってデータの送受信が行える．