第 1 回 ネットワークセキュリティゼミ

ゼミ担当者　：　天白進也，山本健友，瀬戸川滋彰
指導院生　　：　市川親司，吉井健吾，千野晋平
開催日　　：　2005 年 4 月 19 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 アドレスの中身は大きく分けると，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 つのクラスにわけられている．

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，そのため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
0.0.0.0	全てのビットが 0

- 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．

- 全てのビットが 0 のアドレス

  ルーティングの際にデフォルトのネットワークを示すために使用されるアドレスである．

デフォルトのネットワークとは，ルーティングテーブル上に次にデータを転送する対象となるネットワークがない際に指定する規定のネットワークのことである．

Table 3 の予約された IP アドレス以外はすべてユーザー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，つまり，今まで述べてきた IP アドレスのことである．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ことになっている．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のである．

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).

1.2　ルータとアドレス変換

プライベート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，プライベートアドレスとグローバル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アドレスとポート番号，書き換えた後のグローバル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は送り先アドレスにルータのグローバル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).

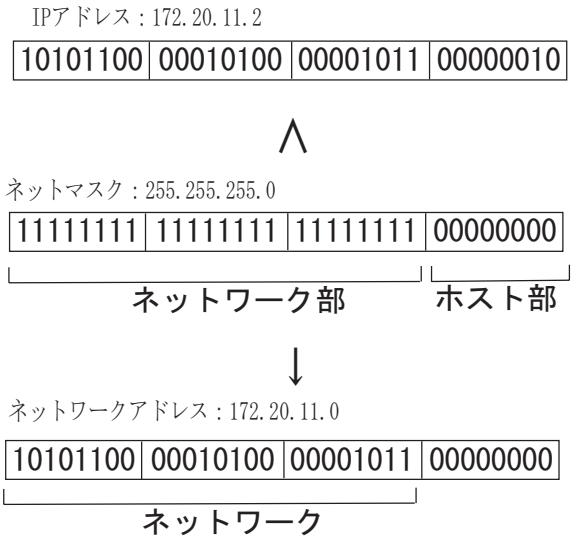

Fig. 1　サブネットマスク

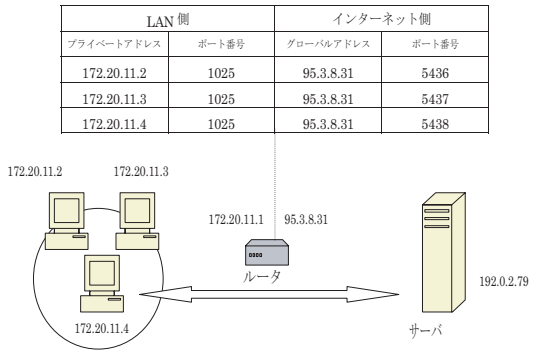

Fig. 2　ルータの仕組み

2　DNS サーバ

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．

以下, 具体的なやりとりを例にDNSの役割を見てゆく. クライアントがmikilabのサーバにアクセスしようとするとき,「mikilab.doshisha.ac.jp」のIPアドレスを，クライアントが設定した優先DNSサーバ「170.20.11.16」に問い合わせると，DNSサーバは登録してある「mikilab.doshisha.ac.jp」のアドレスをクライアントに返すのである．しかし，必ずしもクライアントが設定したDNSサーバがクライアントが要求するサーバのIPアドレスを持っているとは限らない．そのときは，ほかのDNSサーバに問い合わせることになる．このときの動作を解説する．まず，クライアントがブラウザで「www.doshisha.ac.jp」にアクセスしようとして，優先DNSサーバに問い合わせるとする．しかし，優先DNSサーバには「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ことになる．DNSサーバは階層構造になっており，ドメインの右に行くほど上位の階層になる．つまり,「www.doshisha.ac.jp」ではjpが一番上位の階層になるが，そのもう一つ上にルートドメインサーバがある．このように階層化したドメインの一つ一つがDNSサーバの担当範囲を表す単位となる．具体的には，下位のドメインを担当するDNSサーバを，すぐ上に位置するDNSサーバに登録する．そして，その上位のDNSサーバをさらに上位のDNSサーバに登録する，というように順に登録してゆく．つまり，www.doshisha.ac.jpというドメインを担当するDNSサーバをdoshisha.ac.jpのDNSサーバに登録し，doshisha.ac.jpのDNSサーバをac.jpドメインのDNSサーバに，といった順に登録していくのである．よってルートドメインDNSサーバはjpドメインのDNSサーバを登録しているのである．このルートドメインのDNSサーバをDNSサーバ全てに登録することによって，全てのDNSサーバをつなぐことが出来るのである．クライアントが設定した優先DNSサーバは，jpドメインのDNSサーバのIPアドレスをルートドメインに問い合わせ，次にac.jpドメインのDNSサーバのIPアドレスをjpドメインに問い合わせ，doshisha.ac.jpのサーバのIPアドレスを，ac.jpに問い合わせ，そしてwww.doshisha.ac.jpのサーバをdoshisha.ac.jpに問い合わせることで，クライアントにwww.doshisha.ac.jpのIPアドレスを返せるようになるのである．

3　プロキシサーバ

プロキシサーバとは，内部ネットワークからインターネットに接続する際，高速なアクセスを実現し，セキュリティを確保するために設置されるサーバである.「プロキシ」とは「代理」という意味であり，その言葉が示す通りインターネット上の目的のコンテンツをユーザのコンピュータの代わりにとってきてくれるのである (Fig.4).

プロキシサーバの機能は，以下の二つである．

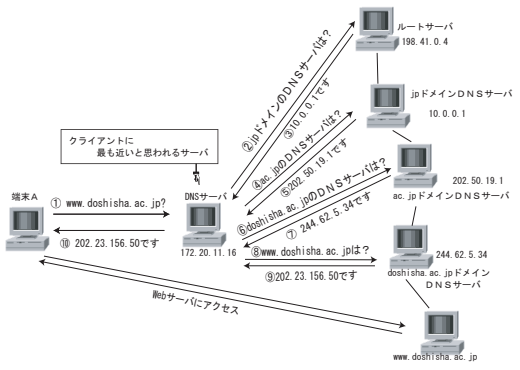

Fig. 3　DNSサーバの仕組み

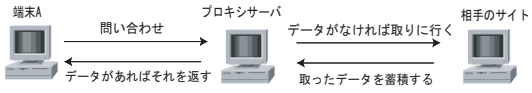

Fig. 4　プロキシサーバの仕組み

- キャッシュ機能

  プロキシサーバはキャッシュ機能を実装しており，過去にサーバから受信したコンテンツを一時的にプロキシサーバ自身のディスク内に蓄積しておくことができる．ユーザから同一コンテンツへのアクセス要求があった場合，プロキシサーバーにキャッシュされたコンテンツを参照させるので，ユーザはコンテンツを素早く取得することが可能となる．また，その場合プロキシサーバは本来のサーバにアクセスしなくて済むため，そのサーバに掛かる負荷を軽減することができる．このようにプロキシをキャッシュサーバとして利用することによって，遠くのサーバに何度もアクセスしなくて済むため，結果的にネットワークのトラフィック (回線使用量) を軽減できる．

- セキュリティ機能

  プロキシサーバはWebブラウザなどのクライアントとWWWサーバ等の外部サーバ間に位置し，接続されたクライアントからの要求を受付，代理でインターネットと通信する．そのため，これらの間でやりとりされる全てのデータのフィルタリングができる．つまりデータのモニタリング，改変，妨害が自由にできる．それに加えてクライアントが相手側のサーバに直接アクセスせずに済むため，ユーザの様々な個人情報 (IPアドレスやホスト名など) を外部サーバに伝えることなくコンテンツ閲覧ができ，匿名性の確保が可能となる．また，外部からの進入を防御するというファイアウォールの機能も併せ持ち，セキュリティの確保を実現している．

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，インターネットにおける情報の「住所」にあたる．URL は以下の 3 つの部分からなっている．

- URL の種類
  (http，ftp，mailto，file など)
- Web ページを提供している Web サーバのコンピュータの名前
  (www.doshisha.ac.jp，mikilab.doshisha.ac.jp など)
- Web サーバの中での Web ページの位置
  (/zaigaku/jugyo/index.html，/dia/index.html など)

例えば，以下のような URL がある．

http://www.doshisha.ac.jp/zaigaku/jugyo/index.html

この URL は HTTP という方法で提供している www.doshisha.ac.jp というコンピュータの中で/zaigaku/jugyo/index.html という位置にあるウェブページを示している．また，www.doshisha.ac.jp や mikilab.doshisha.ac.jp のようなコンピュータの名前をドメイン名 (ホスト名と呼ばれることもある) という．ドメイン名は「ホスト部＋ドメイン部」で構成されており，www や mikilab はホスト部，doshisha.ac.jp がドメイン部にあたる．ドメイン名はインターネット上の IP アドレスのままでは人間には覚えにくいため，分かりやすくするためにつけた名前である．

5 パーミッション

パーミッションとはコンピュータの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が設定できる．

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．”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」,「その他のユーザ」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すのである．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て計算する．権限は Table 5 に示している．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．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．実際に Fig. 5，Fig. 6 にファイル，及びディレクトリのパーミッションの表記例を示す．

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

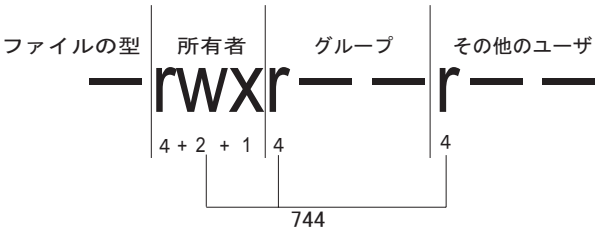

Fig. 5　パーミッションの表記

Fig. 6　ディレクトリのパーミッションの表記

6 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．このシステムの概要を Fig. 7 に示す．

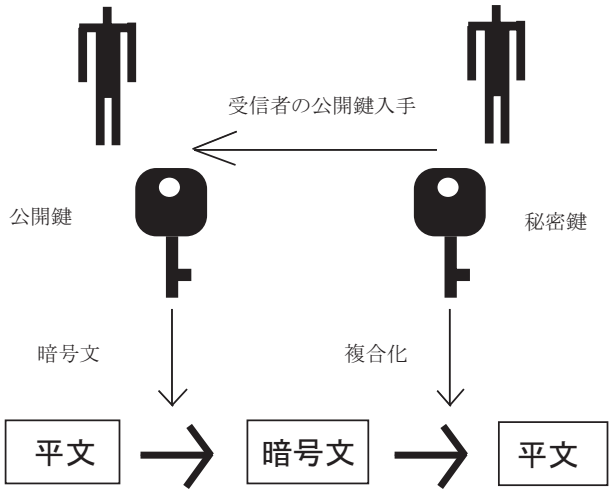

Fig. 7　公開鍵暗号方式

暗号化と復号化を同じ鍵で行なう**共通鍵暗号方式**に比べ，鍵を安全な経路で輸送する必要がないため，鍵の管理が楽で安全性が高い．

7　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. 8 に示す．

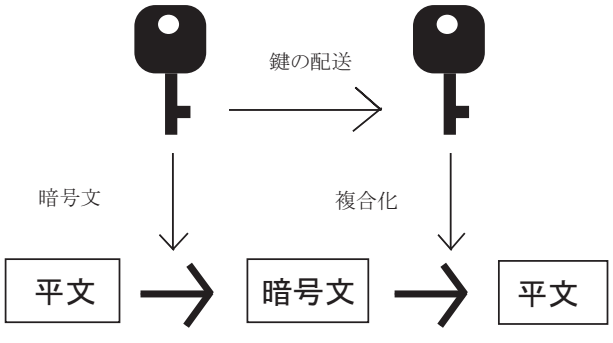

Fig. 8　共通鍵暗号方式

8　SSH について

8.1　SSH の概要

ネットワークを利用して，別のマシンにログインしたり，ファイルを転送する際に telnet や ftp を用いることができる．しかし，これらの方法ではネットワークを流れる情報は暗号化されず，データは平文のまま送信されている．つまり，もし途中にこのデータを盗み見ている人がいた場合にはすべての内容が筒抜けになってしまうのである．このような状況は世界中のユーザが接続可能なインターネット環境では非常に危険である．よって信頼できないネットワーク環境では通信が暗号化されているコマンドによる通信を利用するべきである．このような環境を提供するのが SSH(Secure SHell) である．

8.2　SSH の仕組み

SSH の認証および暗号化には公開鍵暗号と言う暗号化技術が使われている.SSH ではこの暗号方式により，大まかに言って次の 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．

8.3　ホスト認証

まず，SSH は通信を行う際に相手となる**リモートホスト（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．SSH はインストール時点でそのホストを認証するための公開鍵と秘密鍵を作成する．そして，初めてアクセスしてきた相手に対して自分の公開鍵を渡す．次に，**ローカルホスト (クライアント)** は公開鍵を使ってランダムに生成したデータを暗号化してリモートホスト (公開鍵を渡したホスト) に送る．リモートホストはそのデータを自分の秘密鍵で復号し，それをローカルホストに送り返す．この結果，ローカルホスト上で暗号化する前のデータと送り返されたデータが一致すれば正しい鍵を持つ通信相手であることが保証される．認証の様子を Fig. 9 にしめす．

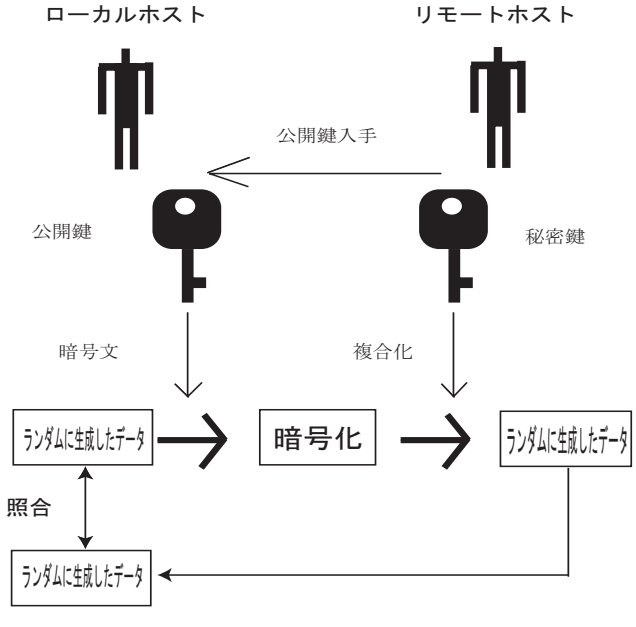

Fig. 9　ホスト認証

8.4　通信内容の暗号化

SSH はホスト認証が終った後ローカルホストは通信の暗号・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リモートホスト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処理の早い通信を行うように設計されている．

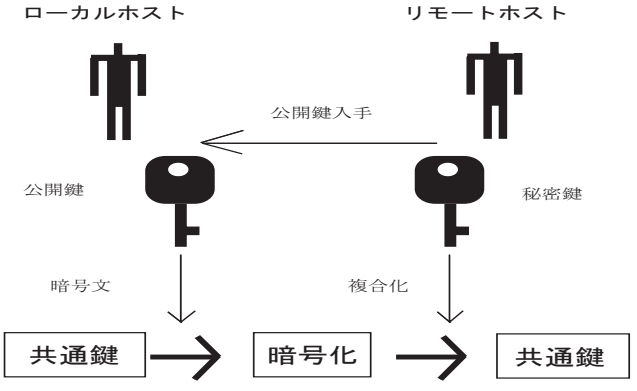

Fig. 10　共通鍵の共有

8.5　ユーザー認証

ホスト間の認証が終った後はユーザー認証を行う．ユーザー認証にはパスワード認証と，ホスト認証で行ったような公開鍵の認証をユーザー単位で行う方法がある．SSH2 ではユーザー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ようにしている．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ー毎に鍵を作成したほうが安全である．パスワードによる認証方式は，ユーザーにあらかじめ割り当てられたパスワードによって認証を行うものである．ユーザが鍵の準備をしている場合の認証は，ホスト認証の方法とほぼ同じ手続きによって行われる．ユーザーの認証ではホスト認証のときとは逆にリモートホストにユーザが準備した公開鍵を使い，ローカルホストのユーザ秘密鍵が正しいものかどうかを調べる．調べる方法はホスト認証のときと同じようにリモートホストの公開鍵を使って暗号化したデータをローカルホストの秘密鍵で復号できるかどうかで判定する．しかし，このままではもしユーザー秘密鍵を盗まれたり，ユーザのローカルマシンを勝手に操作したりすることでログインできてしまう可能性がある．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．

8.6　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. 11 にその概要をしめす．

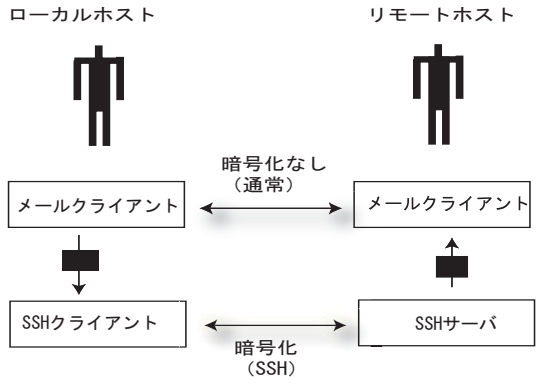

Fig. 11　ポートフォワーディング

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. 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．

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．

8.7　scp を用いたファイル転送

scp とは，SSH を用いたファイル転送コマンドである．従来，UNIX にはリモートホストにファイルを転送する方法として **rcp** コマンドが使われていたが，rcp はデータが暗号化されないために途中の通信路でデータが盗聴される危険性がある．それに対して scp は SSH を用いて暗号化された経路を用いてデータを転送することができるため，途中で盗聴される心配がなくなる．以下に，その利用方法について説明する．

scp [オプション] [転送したいファイル名] [転送先のパス]

ローカルホストからリモートへファイルを転送するためには，[転送したいファイル名] にローカルホストにあるファイルを指定し，[転送先のパス] にリモートホストのパスを指定する．リモートホストを転送先のパスとして指定する場合，以下のように記述する．

[ユーザー名]@[ホスト名]:[パス]

補足資料

- マルチキャスト

  ネットワーク内で、複数の相手を指定して同じデータを送信すること。これに対し、不特定多数の相手に向かってデータを送信することを「ブロードキャスト」、単一のアドレスを指定して特定の相手にデータを送信することを「ユニキャスト」という。TCP/IP ネットワークでは、複数のあて先を指定して一回データを送信すれば、通信経路上のルータがあて先に応じて自動的にデータを複製してくれるので、回線を圧迫することなく効率よく配信することができる。インターネットで映像配信を行なう場合などに使われる。

- ブロードキャスト

  ネットワーク内で、不特定多数の相手に向かってデータを送信すること。ネットワーク全体を意味する特殊なアドレスを指定することによって行なう。TCP/IP では、ネットワークに接続して設定情報を自動取得する際に、設定情報を持っているサーバを探す場合など、限られた用途に使用する。単一のアドレスを指定して特定の相手にデータを送信することを「ユニキャスト」と呼び、複数の相手を指定してデータを送信することを「マルチキャスト」という。

- ファイアウォール

  組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステム。また、そのようなシステムが組みこまれたコンピュータ。企業などのネットワークでは、インターネットなどの外部ネットワークを通じて第三者が侵入し、データやプログラムの盗み見・改ざん・破壊などが行なわれることのないように、外部との境界を流れるデータを監視し、不正なアクセスを検出・遮断する必要がある。このような機能を実現するシステムがファイヤーウォールである。多くの場合はソフトウェアの形で提供され、コンピュータに組みこんで使用するが、高い性能が要求されるため、専用のハードウェアが用いられる場合もある。

- ルータ

  ネットワーク上を流れるデータを他のネットワークに中継する機器。OSI 参照モデルでいうネットワーク層 (第 3 層) やトランスポート層 (第 4 層) の一部のプロトコルを解析して転送を行なう。ネットワーク層のアドレスを見て、どの経路を通して転送すべきかを判断する経路選択機能を持つ。また、自分の

対応しているプロトコル以外のデータはすべて破棄する。複数のプロトコルに対応したルータをマルチプロトコルルータと呼ぶ。

- アカウント

  コンピュータやネットワーク上の資源を利用できる権利のこと，または利用する際に必要な ID のこと．

- TCP/IP【Transmission Control Protocol/Internet Protocol】

  インターネットやイントラネットで標準的に使われるプロトコル．米国防総省が，核攻撃で部分的に破壊されても全体が停止することのないコンピュータネットワークを開発する過程で生まれた．UNIX に標準で実装されたため急速に普及し，現在世界で最も普及している．OSI 参照モデルでは IP が第 3 層 (ネットワーク層)，TCP が第 4 層 (トランスポート層) にあたり，HTTP や FTP などの基盤となるプロトコルである．

- プロトコル

  複数のデバイスやコンピュータシステムが互いに通信するための規約．たとえばコンピュータシステムに SCSI デバイスを接続すると，両者は SCSI インターフェイスで定義された手順に従ってデバイスの初期化やデータ転送などを行なう．この場合の手順の取り決めをプロトコルと呼ぶ．また 2 つのコンピュータをネットワークで接続するとき，両者が通信するために使用する手順もプロトコルである．

- ポート (port)

  インターネット上の通信において，複数の相手と同時に接続を行なうために IP アドレスの下に設けられたサブ (補助) アドレス．TCP/IP で通信を行なうコンピュータはネットワーク内での住所にあたる IP アドレスを持っているが，複数のコンピュータと同時に通信するために，補助アドレスとして複数のポートを持っている．ポートの指定には 0 から 65535 までの数字が使われるため,「ポート番号」とも呼ばれる．IP アドレスとポートを組み合わせたネットワークアドレスを「ソケット」と呼び，実際にはデータの送受信はソケット単位で行われる．

- Telnet (テルネット)

  インターネットやイントラネットなどの TCP/IP ネットワークにおいて，ネットワークにつながれたコンピュータを遠隔操作するための標準方式．また，そのために使用されるプロトコル．Telnet サーバを立ち上げてあるコンピュータにネットワークにつながれたほかのコンピュータから Telnet クライアントを使ってログオンし，そのコンピュータの目の前にいるのと同じように操作することができる．

- ssh【Secure SHell】

  主に UNIX コンピュータで利用される，ネットワークを介して別のコンピュータにログインしたり，遠隔地のマシンでコマンドを実行したり，他のマシンへファイルを移動したりするためプログラム．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なうことができる．SSH のプロトコルには「バージョン 1（SSH1）」と「バージョン 2（SSH2)」があり，両者には互換性がない．バージョンによる大きな違いは，SSH1 では公開鍵暗号化方式に「RSA」を、SSH2 では「DSA」を使用していることである．

- ホスト

  パソコン通信で中心となるコンピュータのこと．メニュー表示などの処理や，フォーラム，電子メールなど各種データの記録はホストコンピュータが行なっている．利用者はホストコンピュータにアクセスして，パソコン通信で提供されている各種サービスを利用する．

- サーバ

  コンピュータネットワークにおいて，クライアントコンピュータに対し，自身の持っている機能やデータを提供するコンピュータのこと．インターネットにおける WWW サーバなどが該当する．また，クライアントソフトウェアに対し，自身の持っている機能やデータを提供するソフトウェアのこと．

- POP

  メールサーバ上のメールを読み出すときに使う手順．インターネットやイントラネット上で，電子メールを保存しているサーバからメールを受信するためのプロトコル．

- SMTP 【Simple Mail Transfer Protocol】

  インターネットやイントラネットで電子メールを送信するためのプロトコル．サーバ間でメールのやり取りをしたり，クライアントがサーバにメールを送信する際に用いられる．

- クライアント

  ネットワーク上のサービスを提供する役割を持つサーバ（提供者）に対して，ネットワークに接続してサービスを利用する側のコンピュータをクライアント（依頼者）という．

- FTP

  ネットワーク上のクライアントとホストコンピュータとの間で，ファイルの転送を行なうためのプロトコル（またはそれを実装したコマンド）．UNIX では，この FTP プロトコルを実装した ftp コマンドが標準で提供される．

- RSA

  Ronald Rivest 氏，Adi Shamir 氏，Leonard Adleman 氏の 3 人が 1978 年に開発した公開鍵暗号方式の一つ．開発者の名前をとって名付けられた．公開鍵暗号の標準として広く普及している．

  itemDES 1960 年代後半に IBM 社によって開発された秘密鍵暗号化アルゴリズムで,1977 年にアメリカ政府標準技術局 (NIST) によって連邦情報処理基準に採用された. 現在ではあまりにも暗号強度が低すぎるため、Triple DES など, 別の暗号方式が使用されるようになっている．

- 公開鍵 (public key)

  公開鍵暗号方式で使用される一対の鍵の組のうち, 一般に公開されるほうの鍵.

- 秘密鍵 (secret key)

  公開鍵暗号方式で使用される一対の鍵の組のうち, 一般に公開されない鍵.

- 秘密鍵暗号暗号化と復号化に同じ鍵を用いる暗号方式．共通鍵暗号の別名.