まえがき ……3

第1章
ネットワークセキュリティとSSH 15

1.1 セキュリティとは ……15
1.2 インターネットにおける脅威とその対策 ……16
1.2.1 なりすまし ……17
1.2.2 盗聴 ……18
1.2.3 改ざん ……20
1.2.4 ホストのなりすまし ……21
1.2.5 中間者攻撃 ……23
1.2.6 侵入 ……24
1.2.7 サービス不能攻撃 ……25
1.3 盗聴や改ざんなどの脅威に対して脆弱なプロトコル ……26
1.3.1 TELNET、LOGIN、SHELL ……26
1.3.2 FTP ……27
1.3.3 HTTP ……27
1.3.4 POP3、IMAP4 ……28
1.3.5 X Window System ……28
1.4 SSH ……28
1.4.1 SSHの実装 ……29
1.4.2 SSHでできること ……30
1.4.3 SSHでできないこと ……31

1.5 セキュリティポリシー ……33
1.5.1 セキュリティと利便性のトレードオフ ……33
1.5.2 セキュリティポリシーとは ……34
1.5.3 個人としてのセキュリティポリシー ……35

第2章
SSHプロトコル 39

2.1 暗号技術 ……39
2.1.1 暗号 ……40
2.1.2 共通鍵暗号（対称鍵暗号） ……41
2.1.3 公開鍵アルゴリズム ……42
2.1.4 鍵交換アルゴリズム ……44
2.1.5 一方向ハッシュ関数 ……44
2.1.6 MAC（メッセージ認証コード） ……45
2.1.7 暗号の強さ ……46
2.2 SSHプロトコルバージョン2の概要 ……47
2.2.1 SSHプロトコルのバージョン ……47
2.3 SSHプロトコルバージョン2の概要 ……48
2.3.1 安全な通信路（トランスポート）の提供 ……48
2.3.2 ユーザ認証 ……49
2.3.3 接続 ……49
2.4 SSHプロトコルバージョン2の詳細 ……49
2.4.1 プロトコルアーキテクチャ ……49
2.4.2 トランスポート層プロトコル ……50
2.4.3 ユーザ認証プロトコル ……53
2.4.4 コネクションプロトコル ……59
2.4.5 他のプロトコル ……60
2.5 OpenSSHにおける工夫：特権分離 ……61
2.6 SSL/TLSとKerberos ……61
2.6.1 SSL/TLS ……61
2.6.2 Kerberos ……62

第3章
SSHの基本的な利用法 65

3.1 sshによるリモートログイン ……66
3.1.1 サーバのホスト公開鍵の登録と確認 ……68
3.2 sshによるリモートホストでのコマンドの実行 ……74
3.3 scpによるファイル転送 ……75
3.3.1 リモートホストのファイル・ディレクトリの指定方法 ……75
3.3.2 scpコマンドの利用 ……76
3.3.3 ディレクトリの再帰的なコピー ……77
3.3.4 scpにおけるエラー ……78
3.3.5 scpのオプション ……79
3.4 sftpによる対話的なファイル転送 ……80
3.4.1 sftpコマンドによる接続 ……80
3.4.2 sftpのコマンド ……81
3.4.3 sftpのコマンドライン引数 ……85
3.4.4 バッチモードの利用 ……86
3.4.5 lftp ……86
3.5 rsyncによるファイル転送 ……88
3.5.1 rsyncを利用したファイルの同期 ……89
3.5.2 rsyncを利用したホスト間でのファイルの同期 ……90
3.5.3 rsyncのオプション ……91

3.6 公開鍵認証の利用 …… 93
3.6.1 鍵の作成 …… 94
3.6.2 リモートホストでの公開鍵の登録 …… 95
3.6.3 公開鍵認証によるログイン …… 96
3.6.4 秘密鍵ファイルにパスフレーズを付けないとどうなるか 97
3.7 エージェント（ssh-agent）の利用 …… 98
3.7.1 ssh-agent の起動 …… 98
3.7.2 ssh-add による鍵の登録、確認、削除 …… 100
3.7.3 ssh-agent を利用した公開鍵認証 …… 102
3.7.4 ssh-agent の停止 …… 103
3.7.5 ssh-agent に関連する環境変数 …… 103
3.7.6 ssh-agent と ssh-add のその他の機能 …… 105
3.7.7 ssh-agent と X Window System …… 107
3.7.8 エージェントの転送 …… 109
3.8 SSH デーモン …… 112
3.8.1 SSH デーモンの設定 …… 112
3.8.2 SSH デーモンの開始、終了、再起動 …… 113

第 4 章
SSH をより便利に使う 115

4.1 ポートの転送 …… 115
4.1.1 ポートの転送とは? …… 115
4.1.2 ポートの転送の利用例 …… 117
4.1.3 SSH のポート転送 …… 118
4.1.4 その他のトンネリング・VPN ソフトウェア …… 130
4.2 X Window System の転送 …… 131
4.2.1 SSH による X11 の転送の概要 …… 131
4.2.2 OpenSSH による X Window System の転送 …… 133
4.3 通信の圧縮 …… 135
4.3.1 サーバ側の設定 …… 135
4.3.2 圧縮を有効にして接続する …… 135
4.4 SSH 経由で SSH を使う …… 136
4.4.1 転送したポートをさらに転送する …… 137
4.5 エージェントを利用できない場合の SSH 接続の自動化 138
4.5.1 パスフレーズなしの秘密鍵ファイルを利用する接続 … 140
4.5.2 コマンドを指定する公開鍵認証の応用例 …… 142
4.6 特定のユーザのパスワードによる認証を禁止する設定 147
4.7 バージョン管理システムと SSH …… 149
4.7.1 CVS …… 149
4.7.2 Subversion …… 150
4.7.3 GNU arch …… 150

第 5 章
SSH の利用・運用ポリシー 151

5.1 SSH クライアントの利用に関するポリシー …… 151
5.1.1 パスワードによる認証よりも公開鍵認証を利用する … 151
5.1.2 公開鍵認証での鍵の管理 …… 152
5.1.3 エージェントの転送 …… 153
5.2 SSH クライアントの設定（ssh_config） …… 153
5.2.1 ssh_config ファイルの構造 …… 154
5.2.2 設定項目の解説 …… 155
5.2.3 ssh_config の設定例 …… 158
5.2.4 SOCKS・HTTP プロキシの利用（ProxyCommand） 159

5.3 SSH サービスの運用ポリシー …… 162
5.3.1 脆弱性が発見された際の対処 …… 162
5.3.2 接続元ホストの制限 …… 164
5.3.3 ホスト秘密鍵ファイルの管理 …… 165
5.3.4 sshd のログ …… 166
5.4 SSH デーモンの設定（sshd_config） …… 167
5.4.1 root でのログイン（PermitRootLogin） …… 167
5.4.2 PAM を利用するか（UsePAM） …… 168
5.4.3 パスワードによる認証を利用するか …… 168
5.4.4 サポートするプロトコル（Protocol） …… 169
5.4.5 sshd_config の設定例 …… 169
5.5 トラブルシューティング …… 170
5.5.1 問題個所のみつけかた …… 170
5.5.2 自力では解決できない場合 …… 174

第 6 章
Windows での SSH 175

6.1 Cygwin での OpenSSH の利用 …… 175
6.1.1 Cygwin のインストール …… 175
6.1.2 OpenSSH クライアントの利用 …… 177
6.1.3 SSH サービスの登録 …… 180
6.2 PuTTY …… 182
6.2.1 PuTTY のインストール …… 182
6.2.2 PuTTY での接続 …… 183
6.2.3 PuTTY の設定 …… 185
6.2.4 PuTTY での公開鍵認証の利用 …… 187
6.2.5 エージェント（Pagent）の利用 …… 191
6.2.6 PuTTY のその他のコマンドの概説 …… 193
6.3 Windows 上のフリーな SFTP クライアント …… 194
6.3.1 FileZilla …… 194
6.3.2 WinSCP …… 197
6.3.3 FileZilla・WinSCP での日本語ファイル名の取り扱い・198
6.4 その他の SSH の実装 …… 200
6.4.1 F-Secure SSH …… 200
6.4.2 TeraTerm と ttssh …… 200
6.4.3 VaraTerm …… 200
6.4.4 Mac OS での SSH …… 201
6.4.5 Java による SSH の実装 …… 201
6.4.6 Palm・PocketPC での SSH …… 201

索引 …… 203