

改訂新版「サーバ技術者養成講座」よくある質問(第3版)

- 第2日 利用技術の基礎-Windows

- Q1.Windows ネットワークの設定(P29~P34)行ったところ、P33のYahooへのPINGが通
りません。対処方法は？

- 第3日 利用技術の基礎-UNIX/Linux(1)

- Q1.リスト3-5 シェルの練習でシェルスクリプト ./shell1 を実行した際、表示した漢字部分が
文字化けします。

- 第6日 サーバ導入技術の習得(2)

- Q1.第6日-2 環境設定:P99 リスト6-3で、Domain=[I6290nj]がDomain=[EXAMPLE]となっ
てしまい、どうしても smb: ¥>のコマンドプロンプトが出てきません。
- Q2.第6日-2 環境設定:評価プログラムがうまく動作しない。
- Q3.第6日-2 環境設定:CentOS 5.6 をインストールして評価プログラムを実行するとセグメ
ンテーションエラーになる。

- 第7日 サーバアプリケーションの仕組みと構築

- Q1.第7日-2 DNS サーバ:リスト7-9でDNS 操作確認を行ったところ no TTL specified; と
いうエラーが表示された。

- 第10日 samba とスーパーサーバ

- Q1.第10日-1 samba:smbclient で Windows 7 の共有フォルダへアクセスすると "session
setup failed: SUCCESS - 0" が表示されて接続できない。

- 第12日 セキュリティ・システムの仕組みと構築

- Q1.第12日-2 SSH-V1: ページ225で書籍の通り行っても、TeraTermでアクセスしようと
すると以下のエラーが表示され、アクセスが出来ません。
- Q2.第12日-2 SSH-V1: TeraTerm V.4.66では図12-4、12-5、12-7で異なります。この
TeraTermは使用できないですか？また、どのような設定を行えば使用できますか？
- Q3.第12日-2 SSH-V1: ssh-1.2.14-win32binとバッチファイルをUSBメモリ内に入れて
から本書のとおりバッチファイルを起動しましたが、エラーで接続ができませんでした。
- Q4.第12日-2 SSH-V1: Teraterm+TTSSHで起動してから、ssh1.2.14を起動させ、パスワ
ードを入力すると接続ができるようになりました。
- Q5.第12日-2 SSH-V1: クライアント側に Teraterm(ポート転送設定)が無くとも実行できる
ようにするには、どのように行えば良いのでしょうか？

- 第13日 SSL

- [Q1.第 13 日 SSL:SSL メールの設定中、smtps を追加するのですかそれとも変更するのですか？](#)
 - [Q2.第 13 日 SSL:設定完了して stunnel を起動する設定にするのですが stunnel の稼動確認ができません。](#)
 - [Q3.第 13 日 SSL:2 度ほど繰り返しましたが、該当ページでエラーが発生し、結果が得られません。](#)
 - [Q4.第 13 日 SSL:SSL 完了後の評価プログラム実行で \[10:FAIL\] - 'stunnel/smtps' \('未実行/未成功/未完了？-ログでは不明'\) のエラーとなりました。\(1\)](#)
 - [Q5.第 13 日 SSL:SSL 完了後の評価プログラム実行で \[10:FAIL\] - 'stunnel/smtps' \('未実行/未成功/未完了？-ログでは不明'\) のエラーとなりました。\(2\)](#)
- [第 20 日 データベースサーバとその応用](#)
 - [Q1.第 20 日-1 データベースサーバ:リスト 20-3 MySQL 動作環境の設定でコマンドエラーとなりました。](#)
 - [Q2.第 20 日-1 データベースサーバ:リスト 20-3 MySQL 動作環境の設定で mysqld ended で Done してしまいます。](#)
- [その他の情報問い合わせ](#)
 - [Q1.本書の出版後の情報の追加や更新はどうなっていますか。](#)
 - [Q2.ネットワーク関係の仕事をしていますが、実際の構築の経験がありません。この本に関連した研修講座がありますか。](#)
 - [Q3.この本の内容を実際の現場に適用できますか。](#)
 - [Q4.技術的なものは身に付いても理論的なものが身に付かないのではないか。](#)
 - [Q5.ネットワークやサーバの理論について知るための書籍や資料にはどのようなものがありますか。](#)
 - [Q6.第 25 日の2で解説しているクラスタリングについての書籍がありますか。](#)
 - [Q7.その他、参考になるサイトにはどのようなものがありますか。](#)

第 2 日 利用技術の基礎-Windows

Q1.

Windows ネットワークの設定 (P29~P34) 行ったところ、P33 の Yahoo への PING が通りません。対処方法は？

A1. インターネット接続の場合、ゲートウェイ設定を行って下さい。

第 3 日 利用技術の基礎-UNIX/Linux(1)

Q1.

リスト 3-5 シェルの練習でシェルスクリプト ./shell1 を実行した際、

①LS -AL を実行して表示した漢字部分が文字化けします。

②合計 16 の「合計」が文字化け

③ファイル属性の 11 月 の「月」が文字化け

./shell1 ではなくコマンドとして ls -al を実行した場合は文字化けしません。

A1. 「cat>shell1」の最初の行の csh が bash の間違いです。

P60ーリスト 3-5 中段 shell 作成

[user1@h2g dir2]\$ cat>shell1 ←ファイル shell1 (「エル・エル・数字の 1」) を作成する

誤) #!/bin/csh ←shell1 の 1 行目入力 (†34)

正) #!/bin/bash←shell1 の 1 行目入力 (†34)

P61ーリスト 3-5 上段 shell 内容確認

[user1@h2g dir2]\$ more shell1 ←shell1 の内容を確認する

誤) #!/bin/csh

正) #!/bin/bash

第 6 日 サーバ導入技術の習得(2)

Q1.

第 6 日-2 環境設定 : P99 リスト 6-3 で、Domain=[I6290nj]が Domain=[EXAMPLE]となつてしまい、どうしても smb: ¥>のコマンドプロンプトが出てきません。

A1.Domain が EXAMPLE となっているということなので、

①コマンド smbclient のパラメータ (' ' でくくった文字列) の先頭¥の後の Windows PC 名に EXAMPLE と指定していませんか？

②つまり、Windows PC 名は正しいですか？

③共有フォルダを作成して共有設定してありますか (その共有名を指定していますか) ？

Q2.

第 6 日-2 環境設定：評価プログラムがうまく動作しない。

A2. サーバ設定評価ユーティリティパッケージのバージョン番号に 'w' がついている CentOS 用の評価プログラムを使用する。

Q3.

第 6 日-2 環境設定：CentOS 5.6 をインストールして評価プログラムを実行すると以下のようなセグメンテーションエラーになる。

“セグメンテーション違反です (コアダンプ)”

A3. サーバ設定評価ユーティリティパッケージの eval バージョン 12w と evals バージョン 13w は CentOS5.5 のみ対応です（パッケージ内 README.1st 参照）で CentOS5.6 以降には対応していません。CentOS5.6 以降で使用すると記述のエラーになります。

evals バージョン 14-final-w（CentOS5.6 以降および Scientific Linux などの RHEL クローンのバージョン 6 以降にも対応）を使用して下さい。なお、README.1st と License_Agreement を必ず読んで下さい。

第 7 日 サーバアプリケーションの仕組みと構築

Q1.

第 7 日-2 DNS サーバ：リスト 7-9 で DNS 操作確認を行ったところ

「db.example:1: no TTL specified; using SOA MINTTL instead zone example.com/IN: loaded serial 1」

というエラーが表示された。

A1. /var/named/chroot/var/named/master/db.example の 1 行目に「\$TTL」がないというエラーメッセージです。

第 10 日 samba とスーパーサーバ

Q1.

第10日-1 samba : smbclient で Windows 7 の共有フォルダへアクセスすると “session setup failed: SUCCESS - 0” が表示されて接続できない。

A1. この現象は、以下で説明するような特定の環境で発生する samba のバグです。
したがって、この事象への対策としては、

- ①本書で smbclient を使用するところでは smbclient は使用せずに、ファイル送受信が必要な場合は USB などのツールを使用する
- ②その他の処理を行ってから smbclient を使用する

のいずれか、あるいは、両方を使用して下さい。

なお、②の方法は第26日の運用管理の項で行うとより理解しやすいので、当面は①を使用する方法をお薦めします。

1) トラブルの詳細

samba のバージョン 3.5.4 以前の smbclient で Windows PC に接続するとき、相手先 PC の OS が Windows 7 で、かつ、その PC で「Microsoft (Windows) Live Sign-in Assistant」を使用していると、接続時に、以下のエラーメッセージが表示されて接続できない。
“session setup failed: SUCCESS - 0”

Windows 7 の「Microsoft Live Sign-in Assistant」は、Windows Live Messenger や Windows Live メールなど9つのソフトパッケージ「Windows Live Essentials 2011 (旧「Windows Live おすすめパック」)」(や Windows Live Messenger パッケージ、あるいは、Live Sign-in Assistant パッケージ単独)などに含まれるものです。Windows Live Sign-in Assistant は Windows Live ID を管理するサインインサービスで、Windows 7 では Windows Live ID と Windows 7 ユーザーアカウントを結びつけ、同一 Windows Live ID のコンピュータユーザ間でのファイル共有を管理しています。そこが、smbclient によるファイル共有アクセスとの接点で、samba 側 (smbclient) に問題があります。

2) バグレポート

以下のバグレポートがあげられています。

- ①Red Hat Bugzilla - Bug 651722
(https://bugzilla.redhat.com/show_bug.cgi?id=651722)
- ②The Samba-Bugzilla - Bug 7577
(https://bugzilla.samba.org/show_bug.cgi?id=7577)

3) 対策

以下のような、いくつかの対策がありますが、本書の第25日までは smbclient が唯一の方法ではないので余計なトラブルを起こさないためにも①を推奨します (実際の現場では USB などのオフラインツールを推奨)。

①smbclient 以外を使用する

Linux からは smbclient 以外のツール USB など Windows との間のファイル送受信を行う方法を推奨します（実際のセキュリティの観点からも USB などオフラインツールが望ましい）。

②パッチをあてる

CentOS 5 の samba にはバージョン 3.0 の samba-3.0.x とバージョン 3.5 の samba3x-3.5.x とがありますが、本書で使用している CentOS 5.5 の samba-3.0.33 には以下のパッチをあてる必要があります。

- ・ spnego patch for 3.0.x

Red Hat Bugzilla - Bug 651722 のページの「Attachments」欄にあるパッチ
(<https://bugzilla.redhat.com/attachment.cgi?id=459350>)

【注】パッチ手順の詳細は技評サポートページ参照。

③バージョン 3.5 以降の samba (samba3x-3.x.x) を使用する

samba のバージョン 3.5 以降については CentOS 5.6 の samba3x-3.5.4-0.70.el5
(<http://mirror.centos.org/centos/5.6/os/i386/CentOS/>)
においてバグ fix されています。

④Windows Live ID Sing-in Assistant を削除するかサービス停止する

先述のように、Windows Live ID による Microsoft の複数の Live サービスを使用したり、PC 間のファイル共有を行う場合に必要なものなので、いずれも不要であれば削除（*1）、あるいは、必要に応じて（または、念のため）smbclient 使用時に一時的にサービス停止します（*2）

- ・ 削除

コントロールパネル→プログラムの追加と削除を開く
Windows Live ID サインイン アシスタント＝削除

- ・ サービス停止

コントロールパネル→管理ツール→サービス
Windows Live ID Sing-in Assistant サービス
＝自動スタートアップで開始状態→停止、または、手動設定&停止)

（*1）削除後、再インストールも可能（単独パッケージもあり）

（*2）実際の結果検証は未確認です。

4) 関連情報

本書では説明していませんが smbclient 使用時には、以下のようなことも関係してきます。

①smbclient 接続のユーザ名

root で smbclient 使用時の接続ユーザ名は何も指定しないと、相手 Windows では Everyone（すべてのユーザ）または Guest の対象とみなされ、「-U ユーザ名」を指定するとその「ユーザ名」で接続してきたとみなされます。Everyone または Guest の場合には、smbclient の「Password:」には何も入力する必要はありませんが、ユーザ名指定の場合は、注意が必要です。Windows 上でそのユーザアカウントにパスワードを設定していない場合、smbclient の「Password:」には何も入力しないこととなりますが、そうすると接続はできますが、GET/PUT/DIR などの操作はすべて “NT_STATUS_ACCESS_DENIED” で拒否されます。つまり、wmbclient で「ユーザ名」接続する場合には、Windows 上で必ずそのユーザアカウントにパスワード設定（し、smbclient で「Password:」入力）しなければなりません。

②smbclient からアクセスする XP/Vista/7 の共有フォルダのセキュリティ設定

smbclient の相手 PC の共有フォルダの設定で「共有とセキュリティ」の「セキュリティ」ページのグループ名/ユーザー名欄と「共有」ページの「アクセス許可」のグループ名/ユーザー名欄にあるユーザ名が関係してきます。共有のデフォルト設定は「アクセス許可」が Everyone で「セキュリティ」では使用ユーザとシステム関係ユーザです。したがって、上記（1）の「ユーザ名」指定しない場合は、Everyone または Guest を「セキュリティ」に追加しておきます。一方「ユーザ名」指定する場合は、そのユーザ名「アクセス許可」と「セキュリティ」に追加します。なお、「アクセス許可」と「セキュリティ」でのそれぞれのユーザのアクセス許可にも注意が必要です（読み込み、書き込み、...）。

第 12 日 セキュリティ・システムの仕組みと構築

Q1.

第 12 日-2 SSH-V1：ページ 225 で書籍の通り行っても、TeraTerm でアクセスしようとする
と以下のエラーが表示され、アクセスが出来ません。

（エラー内容）

SSH2 秘密鍵の読み込みに失敗しました

error:0906D06C:PEM routines:PEM_read_bio: no start line

A1. SSH-V2 が使用されているためです。SSH-V1 で実行して下さい。

Q2.

第 12 日-2 SSH-V1 : TeraTerm V. 4. 66 では図 12-4、12-5、12-7 で異なります。この TeraTerm は使用できないですか？また、どのような設定を行えば使用できますか？

A2. 接続時のサービス SSH で SSH バージョン (V) を SSH1 を選択すれば正しく接続できます。ただし、RSA-1 プライベートキー identity が正しい前提です。identity が正しい（壊れていない）かどうかを見るために、P223 から P224 のリスト 12-7 の⑪⑮⑳の ls や mdir で identity のファイル属性（名前やサイズ、および、日時）で確実なコピーを確認しています。

新旧 Tera Term の利用上の違いは上記、SSH バージョン選択があるかどうか大きな違いです（もちろん、画面上の多少の違いはありますが）。この Version 4. 68 でも上記のように問題なく接続できることを確認しています。

【備考】 identity を含むすべてのファイルのサーバから USB や FD へのコピー時の破損
ファイルを USB や FD にコピーする際に、破損することは現実起きています。それは、以下のような場合です。

- ・ USB など mount/umount で着脱をシステムに知らせる場合、mount した後の実際の装着や umount 前に実際の取り出し、あるいは、umount コマンド時に USB メモリのランプが点滅している時の取り出し、を行ったような場合に正確なコピーができていないことがある。
- ・ FD の場合、mcopy が正常に動作しないで①のファイル属性で違いが見られる。属性が同じ場合でも PC でのファイル入出力が異常な場合がある。また、FD をフォーマットしたときに終了および「閉じる」を行って、絵ジェクトボタンを押すときに FD ドライブの駆動ランプがついていたような場合、あるいは、FD を長く使用していたような場合、その FD に対する書き込みが PC では正しくても UNIX/Linux では（書き込みは正常のように見えても）実際には正しくない場合がある。

以上のような問題を確認する（トラブルシュート）時は以下の手順で明確になります。

サーバから PC へ持ってきた当該のファイルを逆の操作で PC からサーバへ持って行き、diff で比較する。これで、何も表示がなければ同じで、さもないと違う（破損）ということがわかる。

Q3.

第 12 日-2 SSH-V1 : sssh-1. 2. 14-win32bin とバッチファイルを USB メモリ内に入れてから本書のとおりバッチファイルを起動しましたが、エラーで接続ができませんでした。

A3. エラーがリスト 12-11 の④⑤どちらのバッチの話かわかりませんが、④が接続できないのであれば、⑤の後に④を実行していない、つまり、リスト 12-12 の①→にの順に行っていないか、または、①で正しく接続していない、あるいは、①②でエラーがある（リスト 12-11 の④⑤の入力に間違いがある）などが原因と考えられます。

Q4.

第12日-2 SSH-V1 : TeraTerm+TTSSHで起動してから、ssh1.2.14を起動させ、パスフレーズを入力すると接続ができるようになりました。

A4. この意味がよくわかりませんが、TeraTermPro+TTSSH と ssh-telnet.bat (ssh-1.2.14) は全く異なるものであり、相関関係は全くありません。関係あるとすれば、「identity」のみです。

「identity」の存在場所 (USB 内にあり、USB を PC から取り外したり、PC に入れたりしていた、など) が関係しているような印象があります。

Q5.

第12日-2 SSH-V1 : クライアント側に TeraTerm (ポート転送設定) が無くとも実行できるようにするには、どのように行えば良いのでしょうか？

A5. リスト12-11の⑤の設定の内、「-L 23:localhost:23」の部分です。

第13日 SSL

Q1.

第13日 SSL : SSLメールの設定中、

1 stunnel(smtps)の設定で[smtps]の設定をするようになっていますが、stunnel.confでは、[ssmtp]になっているが、smtpsを追加するのですかそれとも変更するのですか？

A1. P245のリスト13-13の上から4行目の「vi stunnel.conf」の説明ー「(((以下のmoreのように変更)))」ーにあるように、つぎの「more stunnel.conf」で表示されるように変更します。

Q2.

第13日 SSL : 設定完了してstunnelを起動する設定にするのですがstunnelの稼働確認ができません。

```
ps ax|grep stunnel
```

```
2837 pts/1 R+ 0:00 grep stunnel
```

と表示します。

```
tail /var/log/stunnel.log を確認したら
500 clients allow
Error binding pop3s to 0.0.0.0:995
bind: Address already in use (98)
```

となります。

243 ページまでは何事もなく正常に動作していました。

A2. このエラーメッセージは「pop3s の 995」が重複されている（先にどこかで=dovecot ですが、設定されているのに、ここ=stunnel でまた設定した）という意味です。
つまり、stunnel.conf に以下の設定が残っていることを示します。

```
[pop3s]
accept  = 995
connect = 110
```

前の質問への回答と同様ですが、「more stunnel.conf」で表示されるように（そのままこれと全く同じように、表示されていない部分は削除して）変更します。

Q3.

第 13 日 SSL : (ページ 248)

2 度ほど繰り返して本書操作内容を実施しましたが、該当ページでエラーが発生し、結果が得られません。

自分の入力誤りと思い、確認し、再実施しました。やはり、エラーが発生して、メール送信できません

```
[root@h2g dovecot]# cd /etc/stunnel
[root@h2g stunnel]# /usr/sbin/stunnel /etc/stunnel/stunnel.conf
[root@h2g stunnel]# ps ax|grep stunnel
4427 pts/1    R+        0:00 grep stunnel
[root@h2g stunnel]# tail /var/log/stunnel.log
2011.05.11 15:57:47 LOG5[4344:3086661328]: stunnel 4.15 on i686-redhat-linux-gnu
with OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008
2011.05.11 15:57:47 LOG5[4344:3086661328]: Threading:PTHREAD SSL:ENGINE
Sockets:POLL, IPv6 Auth:LIBWRAP
2011.05.11 15:57:47 LOG5[4344:3086661328]: 500 clients allowed
2011.05.11 15:57:47 LOG3[4344:3086661328]: Error binding pop3s to 0.0.0.0:995
2011.05.11 15:57:47 LOG3[4344:3086661328]: bind: Address already in use (98)
2011.05.11 16:17:24 LOG5[4425:3086026448]: stunnel 4.15 on i686-redhat-linux-gnu
with OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008
2011.05.11 16:17:24 LOG5[4425:3086026448]: Threading:PTHREAD SSL:ENGINE
Sockets:POLL, IPv6 Auth:LIBWRAP
2011.05.11 16:17:24 LOG5[4425:3086026448]: 500 clients allowed
```

```
2011.05.11 16:17:24 LOG3[4425:3086026448]: Error binding pop3s to 0.0.0.0:995
2011.05.11 16:17:24 LOG3[4425:3086026448]: bind: Address already in use (98)
[root@h2g stunnel]#
```

A3. stunnel のログ (/var/log/stunnel.log) にあるように、

```
Error binding pop3s to 0.0.0.0:995
```

```
bind: Address already in use (98)
```

stunnel で pop3s (995) を使用しようとしたが、既に (他で)、pop3s (995) が動作していた、というエラーメッセージです。「他」とは P246 の「1.4.3 dovecot/pop3s の設定手順 3」(リスト 13-14)

です。書籍の手順で言えば、pop3s (SSL 受信) は dovecot (dovecot.conf) で smtps (SSL 送信) は stunnel (stunnel.conf) で行い、pop3s は stunnel では使用しないのですが、間違って、pop3s を stunnel で設定してしまうと pop3s が重複して上記エラーとなります。stunnel では P245 の「1.4.2 stunnel (smtps) の設定手順 2」(リスト 13-13) にあるように、「smtps だけ」の設定で、pop3s は設定しません。リスト

13-13 の stunnel.conf の設定はリストの more コマンドのように、「; Service-level configuration」部分は [smtps] 設定だけを残し、[pop3s] など他の全ては削除します。

こうした、「Error binding」/「bind: Address already in use (98)」のエラーはよくある間違いです。同じサービス/ポート番号 (pop3s とか smtps など、/etc/services にあるサービス名とポート番号) の有効化が重複して起こるものなので、そのような同じ設定を行うアプリケーション (例えば、ここで、dovecot/stunnel/xinetd など) がある場合にはその重複設定に注意して下さい。

Q4.

第 13 日 SSL : SSL 完了後の評価プログラム実行で [10:FAIL] - 'stunnel/smtps' ('未実行/未成功/未完了?-ログでは不明') のエラーとなりました。

"/root/work/evalsh -c" を実行したところ、[SSL] チェック項目に関して、上記 [10] 以外は完了していた状況です。(1~9, 11~14 は正常完了)

"1.5.1 smtps の stunnel 及び xinetd の設定"を確認しても、不備は無いように見受けられます。

A4. 第 13 日 SSL 完了後、評価プログラム eval で「[10:FAIL] - 'stunnel/smtps' ('未実行/未成功/未完了?-ログでは不明')」と表示される問題について

(「http://www.network-mentor.com/new_server_28days.html」に関連情報あり)

1. 概要

この現象は「MS-IE/OE (Internet Explorer/Outlook Express) の処理上の問題」が基本にあり、その結果として、ときおり stunnel のログに異常を示すものが記録されてしまうことが主因です。評価プログラム eval はそれ故異常 (ではないか?) と見ています。

以降でこの問題の状況を説明しますが、主因の「MS-IE/OE の処理上の問題」については、TCP および TLS/SSL のプロトコル詳細に関係するので最後の【参考】で説明しています。

2. 問題の状況

最初に、第 13 日の P250「リスト 13-17 クライアントからのテストとログの確認」の /var/log/stunnel.log の最終 2 行で以下のように訂正があります。

(誤)

```
2010.07.16 20:44:42 LOG3[4098:3086735056]: SSL_read: Connection reset by peer
(104)
```

```
2010.07.16 20:44:42 LOG5[4098:3086735056]: Connection reset: 369 bytes sent to
SSL, 640 bytes sent to socket
```

(正)

```
2010.07.16 20:44:42 LOG5[4098:3086735056]: Connection closed: 369 bytes sent to
SSL, 640 bytes sent to socket
```

旧 (誤) リストは stunnel/smtps 送信で何らかのトラブルが発生したときのログで、新 (正) リストは完全に正常処理されたときのログです。旧 (誤) リストでもこのデータ送信自体は正しく送信されているのですが、送信後やクローズ処理で問題があると考えられます。

これについてはこの説明の最後の【参考】に詳しく解説していますが、送信拒否されたメールが送信トレイにある OE (Outlook Express) を再起動して「インターネットセキュリティ警告」で「はい」で再送信を行ったときや、システムやネットワークに負荷がかかっているときに証明書表示して「はい」で送信を行ったときなどがよくあるケースです。

3. 評価プログラムの動作と smtps の正常処理

評価プログラム eval では正常に終了していないことから警告メッセージ「[10:FAIL] - 'stunnel/smtps' ('未実行/未成功/未完了?-ログでは不明')」を表示して「Fail」としています。

stunnel のログ (/var/log/stunnel.log) で「Connection reset」(上記旧リスト)ではなく、「Connection closed」(上記新リスト)とあれば正常です。smtps 送信を 2、3 度試行すると正常になります(それでも、最後の説明にあるように MS-IE/OE 自体の問題で異常が続くときがあります)。

評価プログラム eval では「Connection reset」でもデータが送られていれば「正常」と判断する選択肢もありますが、そのデータが「完全にすべて」送られているかどうかは TCP の「reset」(異常時のリセット)の意味からも判断できないのでこの設定(警告 FAIL)にしています。

なお、サーバ(stunnel)側でこの MS-IE/OE 自体の問題に対処することも可能です(最後の【参考】参照)。

【参考】TCP、および、TLS/SSL におけるクローズ手順と「MS-IE/OE の処理上の問題」

1. TLS/TCP プロトコルのクローズ手順

①TLS/SSL のクローズ手順は、TLS の仕様「RFC5246-The Transport Layer Security (TLS) Protocol Version 1.2」の「7.2.1. Closure Alerts」に下記のように記述されている。

他の致命的なアラートが送られていない限り、どちらも、コネクションの書き込みをクローズする前に close_notify アラートを送信することが要求される。

(Unless some other fatal alert has been transmitted, each party is required to send a close_notify alert before closing the write side of the connection.)

②TCP の正常時のクローズ手順は、TCP の仕様「RFC0793 (標準 STD0007) Transmission Control Protocol」の「3.5. Closing a Connection」で下記のように記述されている。

TCP A		TCP B
1. ESTABLISHED		ESTABLISHED
2. (Close)		
FIN-WAIT-1	-->	--> CLOSE-WAIT
3. FIN-WAIT-2	<--	<-- CLOSE-WAIT
4.		(Close)
TIME-WAIT	<--	<-- LAST-ACK
5. TIME-WAIT	-->	--> CLOSED
6. (2 MSL)		
CLOSED		

したがって、正常な TLS/TCP のクローズ手順は、「クライアントおよびサーバの両者が、TLS では close_notify アラートでクローズし、TCP でも FIN/ACK の送受信でクローズする」ということがプロトコル仕様である。

なお、TCP では異常時に RST (リセット) を送信してクローズすることができる (*) が、正常時は FIN/ACK の双方向送受信 (「3-ウェイハンドシェイク」)。

(*) RFC1122 (標準 STD0003) -Requirements for Internet Hosts - Communication Layers

「4.2.2.13 Closing a Connection: RFC-793 Section 3.5」

2. MS-IE/OE の TLS/TCP のクローズ手順

MS-IE/OE の TLS/TCP 処理では、「close_notify アラート」を送信せずに、TCP クローズを行う。しかも、その TCP クローズでも、FIN/ACK 送信ではなく、RST (リセット) 送信でクローズすることもある。

3. クライアント OE とサーバ stunnel との smtps 送信の問題

以上のように、サーバ側の stunnel はクローズ時にプロトコルに正しく対応して、TLS では close_notify アラートでクローズし（相手の close_notify アラートで受信してから）、TCP でも FIN/ACK の送受信でクローズしようとする。一方、クライアント OE は close_notify アラートの送信をせずに TCP クローズに入る。このとき、OE 側 TCP が FIN/ACK を送信すれば、サーバ stunnel の TCP は FIN/ACK で応答して正常なクローズとして処理するが、OE 側 TCP が RST を送信すると、サーバ stunnel の TCP は異常終了としてクローズしてしまう。stunnel のログには、正常時は「Connection closed」、リセット時は「Connection reset」と記録される。

4. MS-IE/OE の close_notify アラートなしのクローズに対応するための stunnel の設定

以上のような問題を回避するために、stunnel では以下の設定が可能になっている。

（「man stunnel」から）

TIMEOUTclose = seconds

time to wait for close_notify (set to 0 for buggy MSIE)

これは、MS-IE/OE そのものの問題に対処するためにこの値を 0 にセットして、close_notify アラートを受け取ることなく、stunnel が TCP クローズに移行できるようにする回避策である。

=====

Q5.

第 13 日 SSL : SSL 完了後の評価プログラム実行で [10:FAIL] - 'stunnel/smtps' ('未実行/未成功/未完了?-ログでは不明') のエラーとなりました。

送受信ログには以下のような記録が残っています。

[/var/log/maillog]

h2g dovecot: pop3-login: Login: user=, method=PLAIN, ~

h2g dovecot: POP3(user1): Disconnected: Logged out ~

[/var/log/stunnel.log]

stunnel connected from ~

Connection closed: 442 bytes sent to SSL, ~

[/var/log/service.log]

START: smtps pid=3189 ~

EXIT: smtps status=0 pid=3189 ~

A5. 第 13 日の SSL メールには、「1. 4 スタンドアロンモードによる SSL メールの設定と利用」および「1. 5 inetd モードによる SSL メールの設定と利用」の 2 つの方法があります。

ご質問の中の下記の stunnel ログ

stunnel connected from ~

は「1. 5」 ((x)inetd モードによるメール送信 (xinetd/smtps) = 「1.5/1.5.1」) の方で記録されたログです。

一方、エラーメッセージ

'stunnel/smtps' (' 未実行/未成功/未完了? - ログでは不明

は「1. 4」の方に対するエラーメッセージです。

つまり、「1. 4」の方が問題となっています。「1. 4」が正しく実行されていれば、stunnel.log には

smtps connected from 192.168.0.8:4364

Connection closed: 443 bytes sent to SSL, 4246 bytes sent to socket

と記録されているはずですが。

状況としては、スタンドアロンモードによるメール送信 (stunnel/smtps) = 「1.4/1.4.2」が正しく完了していない (あるいは、メール送受信を実行していない) のではないかと推測されます。

手順として、xinetd の smtps を disable (xinetd を再起動) してから、stunnel を再起動してテストし、それから、つぎに、「killall stunnel」して、再度 xinetd の smtps を disable 無効にして、テストする、になります。

なお、stunnel/xinetd の smtps 送信では、以下のように SSL だけではなく、ソケット (smtp) にもデータ送信されたことを確認して下さい。

Connection closed: 443 bytes sent to SSL, 4246 bytes sent to socket

証明書の確認でキャンセルするとソケットには0バイト送信になります。

第 20 日 データベースサーバとその応用

Q1.

第 20 日-1 データベースサーバ: リスト 20-3 MySQL 動作環境の設定

MySQL 動作環境の設定において my.cnf を編集し、safe_mysqld -u mysql & (③) を起動させましたがコマンドエラーになりました。

A1. コマンドは「mysqld_safe -u mysql &」のまちがいです。

Q2.

第 20 日-1 データベースサーバ: リスト 20-3 MySQL 動作環境の設定

下記のように mysqld ended で Done してしまいます。

A2. P363 の「②' mysql ディレクトリ所有者/グループ設定」が行われていないようです。これを実行すれば、この「 [1]+ Done」が表示されずに、以降も正常に処理されます。

その他の情報問い合わせ

Q1.

本書の出版後の情報の追加や更新はどうなっていますか。

A1. 書籍のサポートページに情報があります。また、著者企業（[有限会社ネットワーク・メンター](#)）の[書籍ページ](#)では逐次、関連情報が追加・更新されています。

Q2.

ネットワーク関係の仕事をしていますが、実際の構築の経験がありません。この本に関連した研修講座がありますか。

A2. 現在、まだありません。全国向けのインターネット経由での通信研修であれば著者企業（[有限会社ネットワーク・メンター](#)）の方で行っているものがあります。[インターネット通信研修「サーバ技術者養成講座」](#)を参照下さい。

日本全国どこからでも、24時間いつでも、自宅・自席の Windows PC から著者企業が提供する最高の ICT サーバ技術の修得が可能です。

Q3.

この本の内容を実際の現場に適用できますか。

A3. 実際に企業内のサーバに適用している例は多数あります。ただし、第 21 日から第 27 日（第 24 日と第 25 日は除く）の強化と応用を適切に行って下さい。

Q4.

技術的なものは身に付いても理論的なものが身に付かないのではないかと。

A4. 本書では、ネットワークのサーバ構築・運用管理の基本的な実作業部分に特化することで、サーバ技術者としての利用運用技術を短期間に習得できるようにしています。実際の

教育研修をまとめた本書により、そうした実績を得ている例が多数あります。理論的な部分や応用部分については現場に入って作業していく中で必然的に（必要に迫られて）習得されてゆくので後回しにしています。とは言っても、読者がサーバ利用者として使用していた中では得られない初歩的・基本的な部分については一定の解説をしています。例えば、DNSやsambaの仕組みなどです。経験的に見ても、本書の最初に、あるいは、本書と一緒に、詳細理論を教育したことが何度かありますが、いずれのケースでも、1年ほどたつとその内容をほとんど忘れてしまうのが実状です。

Q5.

ネットワークやサーバの理論について知るための書籍や資料にはどのようなものがありますか。

A5. 著者関係では、通信技術のプロトコルについて詳細解説した「通信プロトコル事典」やインターネット技術について詳細解説した「インターネットRFC事典」などがあります。ネットワーク技術全般であれば、「ネットワーク・スーパーテキスト上巻（理論編）」があります。

Q6.

第25日の2で解説しているクラスタリングについての書籍がありますか。

A6. 第25日の2は、著者の別書籍「Linux 高信頼サーバ構築ガイド～クラスタリング編」のさわり部分をもとに解説しています。また、情報処理学会での著者の講演資料ももとにしています。

Q7.

その他、参考になるサイトにはどのようなものがありますか。

A7. 以下のような公的組織サイトが有用でしょう。

[ANSI（米国規格協会）](#)

[APNIC](#)

[ARIN](#)

[CERT（コンピュータ緊急対応センター）](#)

[IAB（インターネット・アーキテクチャ委員会）](#)

[IANA（インターネットアドレス管理委員会）](#)

[ICANN](#)

[IEEE](#)

[IESG（インターネット技術標準化運営グループ）](#)

[IETF（インターネット技術標準化委員会）](#)

[IPA セキュリティ・センター](#)
[ISOC（インターネット学会）](#)
[ISO（国際標準化機構）](#)
[ITU（国際電気通信連合）](#)
[JPCERT（日本版 CERT）](#)
[JIPDEC（情報処理開発協会）](#)
[JPNIC](#)
[Purdue 大学 COAST ライブラリ](#)
[rpmfind.netRPM リポジトリ](#)
[TheOpenGroup](#)
[TIA（米国電気通信工業会）](#)
[W3C（WWW コンソーシャム）](#)
[WIDE プロジェクト](#)
[インターネット協会（IAJapan）](#)
[ジャパン ICANN フォーラム](#)
[Realtime BlackholeList Japan](#)
[情報処理振興事業協会（IPA）](#)
[情報通信技術委員会（TTC）](#)
[日本データ通信協会](#)
[日本レジストリサービス](#)