小山工業高等専門学校研究紀要
第 37 号 (2005) 169 － 178

CGIを用いたパスワード変更ツールMPCCについて

南斉 清巳* 井手尾 光臣** 石塚 大智***

*小山工業高等専門学校 電子制御工学科
**小山工業高等専門学校 技術室
***日本IBM (平成16年小山高専電子制御工学科卒業)

1. はじめに

本校では、全学生を対象にメール利用希望者に対して、アカウントを付与している．メールサーバはLinuxで運用されており、利用者はパスワードを変更する場合、telnetを利用してメールサーバにリモートログインし、さらにunixコマンドを使用する必要があった．

このため、Linuxの操作に慣れていない利用者にとっては、大変使いづらいものであった．また、メールユーザのリモートログインを許可する必要があるため、セキュリティの点からも好ましくない．これらの問題点を解決するため、Webブラウザ上からパスワードを変更するためのツール (Mail user Password Change Cgi 以下MPCCと呼ぶ) を作成したので報告する．

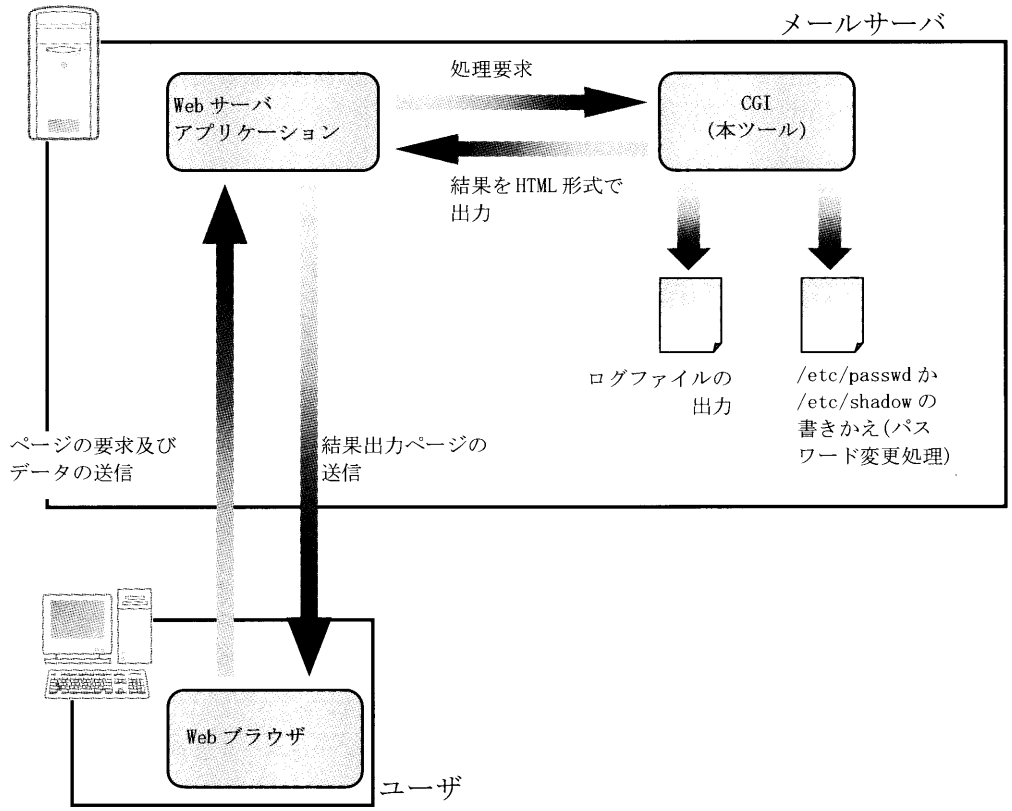


図1 処理の流れ

2．システム概要

Web 上からパスワードを変更させるために、CGI(Common Gateway Interface)を使用する．CGI プログラムには C++を使用した．また、プログラム中でユーザの認証やパスワードの変更を行うために PAM(Pluggable Authentication Modules)を使用している．

パスワードを変更するために次の２つのモードを用意した．

（1） 一般ユーザモード
一般ユーザが自分のパスワードを変更するためのモードである．現在使用しているパスワードで認証を行う．

（2） 管理者モード
利用者が自分のパスワードを忘れてしまったときに、管理者が新たなパスワードを発行するためのモードである．ここで言う管理者は必ずしも root ユーザでなくとも良い．

本ツールの処理の流れを図１に示す．本システムは CGI を使用するので、メールサーバ上で Web サーバが動作している必要がある．これには Apache1.3 を使用している．また、サーバとクライアント間の通信の安全性のために SSL を使用し、暗号化通信を行っている．SSL 通信をサポートするモジュールとしては mod_ssl を使用している．

ツールの処理の流れについて簡単に説明する．まず、パスワードを変更しようとするユーザは、Web ブラウザを利用してパスワードを変更するホスト（メールサーバ）の Web サーバに入力フォームページを表示する．ユーザは入力フォームに、ユーザ名やパスワードなどの情報を入力したら、それらの情報を Web サーバに送信する．

Web サーバはそれらの情報をもとに、CGI プログラムに対して処理要求を行う．ツールの処理過程においてエラーが起きなければ（発生しうるエラーについては後で述べる）、パスワードの変更処理が行われる．パスワード変更処理とは、具体的には/etc/passwd の内容の変更(シャドウパスワードが無効の場合)、もしくは/etc/shadow の内容の変更(シャドウパスワードが有効の場合)が行われることである．このとき、処理状況をログファイルに出力する．

ツールは処理結果を HTML 形式で出力し、その HTML 形式の結果出力ページがユーザへと返される．

表１　MPCC 関連ファイル一覧

ファイル名	ファイルの説明
index.html	MPCC のメニューページ．MPCC 一般ユーザモード・MPCC 管理者モード・ヘルプへのリンクがある．
mpcc-t1.html	MPCC 一般ユーザモードの入力フォームページ．
mpcc-t1.cgi	MPCC 一般ユーザモードの処理を行う CGI ファイル．
mpcc-t1_(日付).log	MPCC 一般ユーザモードのログファイル．日付ごとに生成される．(日付)にはログファイルが生成された日付が入る．
mpcc-t2.html	MPCC 管理者モードの入力フォームページ．
mpcc-t2.cgi	MPCC 管理者モードの処理を行う CGI ファイル．
mpcc-t2_(日付).log	MPCC 管理者モードのログファイル．日付ごとに生成される．(日付)にはログファイルが生成された日付が入る．
inter.html	MPCC の入力フォームページや結果出力ページから MPCC メニューページへ戻る際の中間リンクファイル．入力フォームページや結果出力ページでは SSL 通信をサポートし、MPCC メニューページでは SSL 通信をサポートしないようにするために用いる．
help.html	MPCC に関する簡易ヘルプページ．
mailadmin.conf	MPCC 管理者モードにおける、メールユーザ管理者を設定するファイル．
gif ファイル 16 種	各種ボタン用の画像ファイル．

※HTMLファイルではJAVAScriptを使用しているので、Webブラウザ側では
JAVAScriptを有効にしておく必要がある

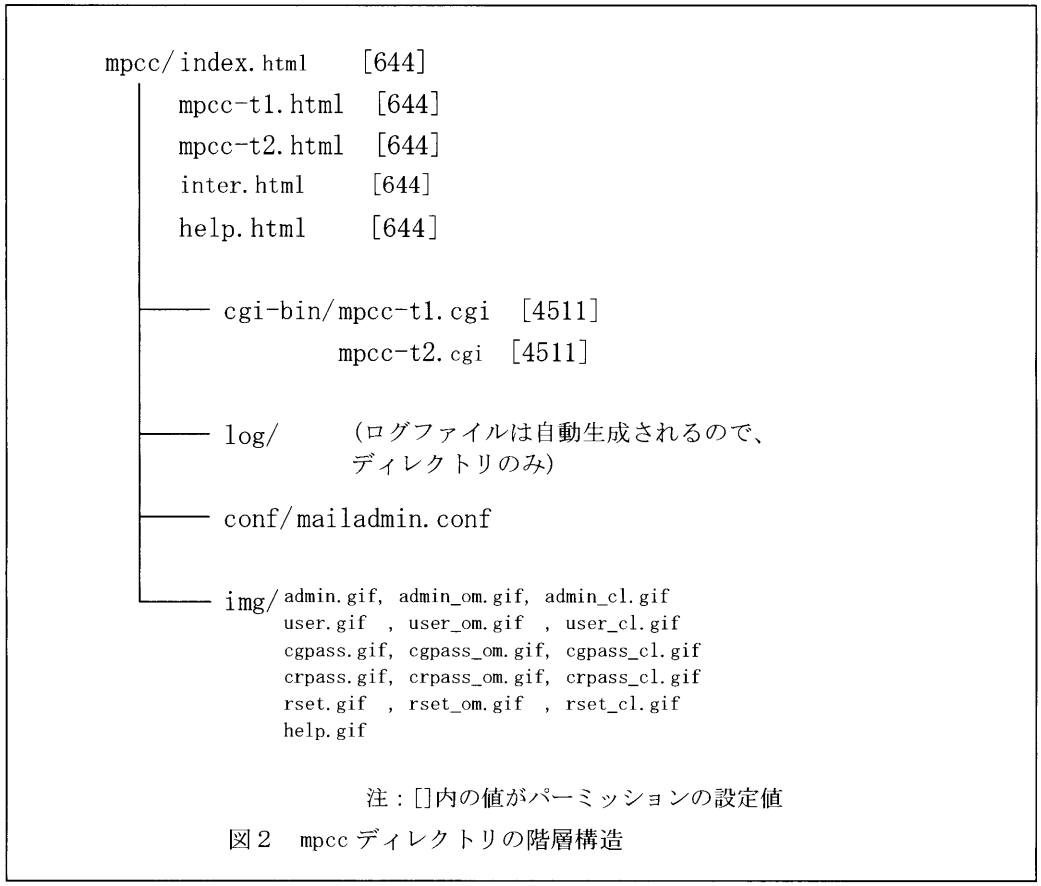


図2 mpccディレクトリの階層構造

mpccディレクトリを/var/www/内にコピーして、ツールが動作するようにApacheの設定ファイルにmpccディレクトリに対するエイリアスやオプションを設定する．このときの設定ファイルの変更内容を次に示す．

－Apacheの設定ファイルhttpd.confの変更内容－

<IfModule mod_alias.c> ～ </IfModule>内に次の文を追加する．

```
Alias /mpcc/ “/var/www/mpcc/”

<Directory “/var/www/mpcc” >
    Options FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

ScriptAlias /mpcc/cgi-bin/ “/var/www/mpcc/cgi-bin/”
```

```
<Directory “/var/www/mpcc/cgi-bin” >
    Options ExecCGI
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

また、同じ設定ファイル内でコメントアウトされている
#AddHandler cgi-script .cgi
を次のように変更する.
AddHandler cgi-script .cgi
設定が完了したらApacheをSSL対応で起動、もしくは再起動する.

3．実装

表1に示す各モジュールを、メールサーバへ実装した．メールサーバで使用したソフトウェアは次の通りである.ApacheやSSLモジュールはRed Hat Linux 7.2 インストールCD内に含まれているRPMパッケージを利用した.

OS：	Red Hat Linux 7.2
Webサーバアプリケーション：	Apache 1.3.20-16
SSLモジュール：	mod_ssl 2.8.4-9

開発機でコンパイル済みのCGIファイルを含め、MPCC に関するファイルは開発機での試験運用時と同様に、mpcc ディレクトリにまとめてメールサーバにコピーする.開発機での試験運用時とは異なり、コピー先は/home/httpd/html/となっている．パーミッションの設定値は試験運用時と同様である.ただし、HTML ファイル（index.html，inter.html)内のリンクをメールサーバにあわせて変更する必要がある.

Apache の設定変更も試験運用時とほぼ同様であるが、mpcc ディレクトリがある階層が異なるため、試験運用時の設定とは若干異なる．具体的には、/var/wwwを/home/httpd/htmlとする必要がある．また、lddコマンドにより、作成したCGIファイルが必要としているライブラリを調べると、以下のようなライブラリが必要とされていることがわかった.

- libpam.so.0
- libstdc++-libc6.2-2.so.3
- libm.so.6
- libc.so.6
- libdl.so.2
- /lib/ld-linux.so.2

したがって、もし不足しているライブラリがあればメールサーバにインストールする必要がある.

また、Webサーバアプリケーションであるapacheをrootユーザで起動していると、間違った古いパスワードでもパスワード変更ができてしまうという現象が、一般ユーザモードにおいて確認できた．これは、Apacheをrootユーザで起動していると、CGIを実行するユーザがrootとなってしまうためであると考えられる．そのため、root ユーザによるパスワード変更時と同様に、ユーザの古いパスワードに対する認証が緩和され、間違った古いパスワードでもパスワード変更ができてしまう．Apacheをrootユーザで起動するには多少の設定が必要なため、通常はほとんど起こり得ないことではあるが、このようなことを防ぐために、ツールを使用する場合はApacheをroot以外のユーザで起動する必要がある.

4．評価

2004年4月から運用を開始しているがトラブルも無く動作している.メールアカウントを発行したときのユーザ教育においても従来のunixコマンドによるパスワード変更に比べて格段に楽になったといえる.

5．まとめ

CGIを用いることで、ユーザがWebブラウザ上からLinuxホストのユーザパスワード変更を行うツールを作成することができた.ただし、セキュリティに関係するパスワード変更を行うツールなので、セキュリティポリシーを的確に制定し、使用する際には注意を払うことが重要である.

参考文献等

Haruhiko Okumura's Home Page（奥村晴彦氏のホームページ）
http://www.matsusaka-u.ac.jp/~okumura/
エンタープライズ：Linux Tips http://www.itmedia.co.jp/help/tips/linux/
Linuxメモ http://bitarts.jp/tech/linux/
とほほのWWW入門 http://tohoho.wakusei.ne.jp/www.htm
猫でもわかるプログラミング http://www.kumei.ne.jp/c_lang/
レッドハット株式会社_オープンソースとともに
http://www.jp.redhat.com/
HP-UXリファレンス(マンページ) http://docs.hp.com/ja/hpuxosmanpages.html
リナックス・コマンド集 http://www.yaizu.net/linux/linux-command.htm
IT用語辞典e-Words http://e-words.jp/

サーバ構築研究会 著：「Red Hat Linux 9で作るネットワークサーバ構築ガイド」 秀和システム(2003)

付録 MPCC の使用方法

A. 1　MPCC メニューページについて

MPCC（本ツール）を使用する際には、Web ブラウザのアドレスバーに

http://(ホスト名もしくは IP アドレス)/mpcc/　または

http://(ホスト名もしくは IP アドレス)/mpcc/index.html

と入力する．すると、MPCC のメニューページが開かれる（図 A.1 参照）．

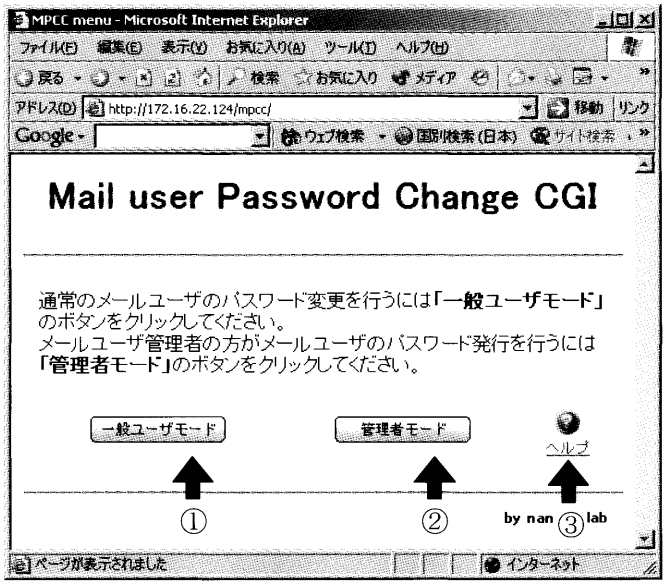


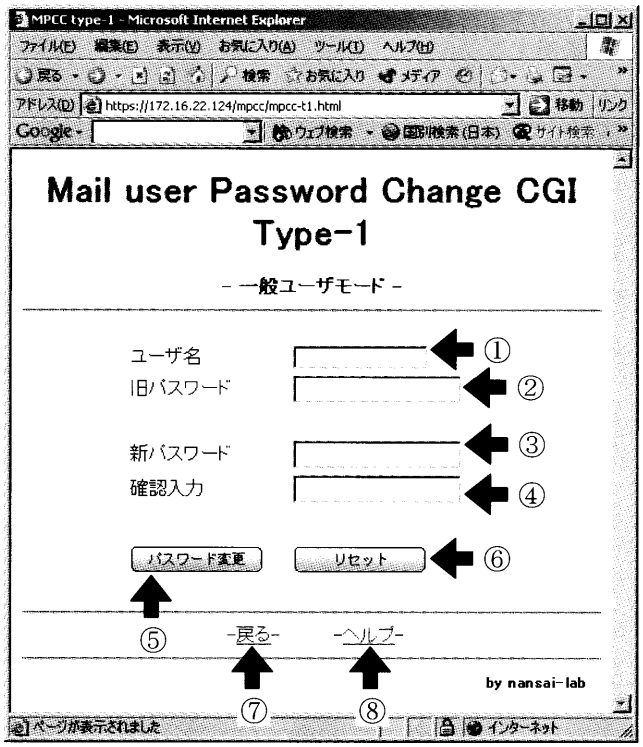
図 A.1　MPCC メニューページ

①のボタンをクリックすると、MPCC 一般ユーザモードの入力フォームページへジャンプすることができる．②のボタンをクリックすると、MPCC 管理者モードの入力フォームページへジャンプすることができる．また、③のリンクをクリックすると、MPCC に関するヘルプページを見ることができる．

A. 2　MPCC 一般ユーザモードについて

MPCC 一般ユーザモードでは、一般のメールユーザのパスワード変更を行うことができる．ただし、パスワードを変更するには、パスワードを変更するユーザのユーザ名と、そのユーザの古いパスワードが必要となる．

MPCC 一般ユーザモードの入力フォームページを図 A.2 に示す．また、表 A.1 に入力フォームページの各入力欄について説明する（カッコ内の数字は図 A.2 に対応）．



図A.2　MPCC一般ユーザモード入力フォー

表A.1　MPCC一般ユーザモード入力フォームの入力欄

入力欄	入力欄の説明
ユーザ名（①）	パスワードを変更するユーザのユーザ名を入力する.
旧パスワード（②）	パスワードを変更するユーザの古いパスワード（それまで使用していたパスワード）を入力する.
新パスワード（③）	新しいパスワードを入力する.
確認入力（④）	新しいパスワードの確認のため、新しいパスワードをもう一度入力する.

各入力欄への入力が完了したら、「パスワード変更」ボタン（⑤）をクリックすることでパスワード変更処理が開始される. 入力した内容をクリアするには、「リセット」ボタン（⑥）をクリックする. ⑦のリンクをクリックすると、MPCCメニューページへ戻ることができる. また、⑧をクリックするとMPCCに関するヘルプページを見ることができる.

A. 3　MPCC管理者モードについて

MPCC管理者モードでは、メールユーザに対する管理権限を持っているユーザ（メールユーザ管理者）が、メールユーザに対するパスワード変更（新しいパスワードの発行）を行うことができる. 新しいパスワードはMPCCが生成する、ランダムなパスワードとなる. ユーザに対するパスワード変更を行うには、メールユーザ管理者のユーザ名とパスワードが必要となる.

MPCC 管理者モードの入力フォームページを図 A.3 に示す．また、表 A.2 に入力フォームページの各入力欄について説明する．

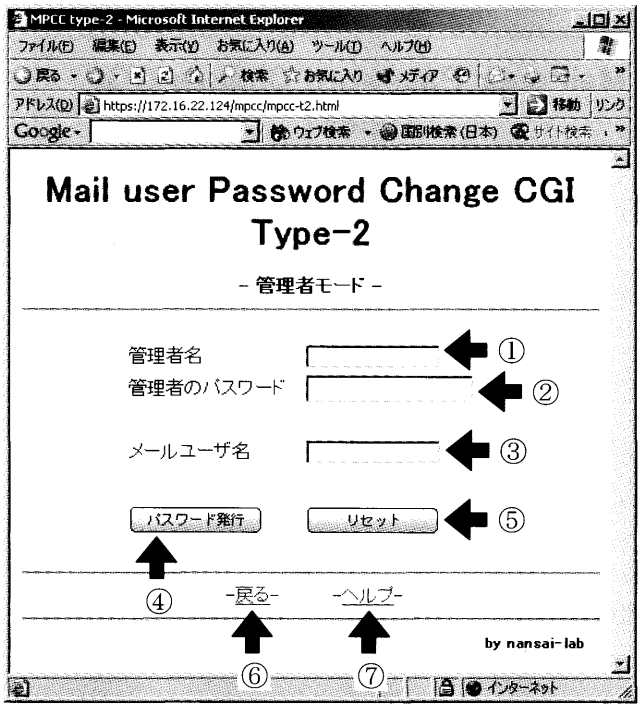


図 A.3　MPCC 管理者モード入力フォー

表 A.2　MPCC 管理者モードの入力欄

入力欄	入力欄の説明
管理者名（①）	メールユーザ管理者のユーザ名を入力する．
管理者のパスワード（②）	メールユーザ管理者のパスワードを入力する．
メールユーザ名（③）	パスワードを変更（新しいパスワードを発行）するユーザのユーザ名を入力する．

各入力欄への入力が完了したら、「パスワード変更」ボタン（④）をクリックすることでユーザに対するパスワード変更処理が開始される．入力した内容をクリアするには、「リセット」ボタン（⑤）をクリックする．⑥のリンクをクリックすると、MPCC メニューページへ戻ることができる．また、⑦のリンクをクリックすると、MPCC に関するヘルプページを見ることができる．

ユーザに対して新しく発行されたパスワードは、結果出力ページに表示される．

A. 4　メールユーザ管理者設定ファイル mailadmin.conf について

MPCC 管理者モードにおけるメールユーザ管理者の設定は mpcc/conf/mailadmin.conf で行う．例として、mailadmin01 と mailadmin02 というユーザをメールユーザ管理者に設定する場合の、mailadmin.conf への設定は次のようになる．

-mailadmin.conf設定例-

```
## MPCC Administrator  ##
## Config File         ##
## Max 10 Admins       ##
mailadmin01                  } ここへメールユーザ管理者
mailadmin02                  } のユーザ名を記述する
## Config File End     ##
```

上の例のように、メールユーザ管理者名は ##Max 10 Admins## ～ ##Config File End## の間に記述する．メールユーザ管理者は最大10名まで設定することができる．

A. 5 MPCCのログファイルについて

MPCCのログファイルは、MPCCを利用した日付ごとにmpcc/logディレクトリ内に自動生成される．MPCC一般ユーザモードのログファイル名がmpcc-t1_(日付).log、MPCC管理者モードのログファイル名がmpcc-t2_(日付).logとなっている（例えば、2004年2月19日の、MPCC一般ユーザモードのログファイル名はmpcc-t1_20040219.logとなる）．

以下に、MPCC一般ユーザモードのログファイル出力例を示す．

-MPCC一般ユーザモードのログファイル出力例-

```
#
# MPCC type-1 log.
#
# Log format is ...
# Date; User name; S-Success, F-Failure
#

Fri Feb 27 10:40:42 2004; No Set; F     －(a)
Fri Feb 27 10:41:28 2004; mailuser; F   －(b)
Fri Feb 27 10:42:04 2004; mailuser; S   －(c)
```

MPCC一般ユーザモードのログファイルには

①ツールを使用した日時

②ツールを使用したユーザのユーザ名（入力されなかった場合は”No Set”）

③パスワード変更処理が成功したか失敗したか（成功なら”S”，失敗なら”F”）

が記録される．先の出力例では(a)がユーザ名が指定されずにパスワード変更処理が失敗したログ、(b)がmailuserがパスワード変更を行ったが失敗したログ、(c)がmailuserがパスワード変更を行って成功したログとなっている．

また、MPCC管理者モードのログファイル出力例を以下に示す．

-MPCC管理者モードのログファイル出力例-

```
#
# MPCC type-2 log.
#
# Log format is ...
# Date; MailAdmin name; S or F; User name; S, F or None
# S-Success, F-Failure, None-Not Change
#

Fri Feb 27 10:41:49 2004; mailadmin>mailadmin; S; user>mailuser; S   －(a)
Fri Feb 27 10:49:02 2004; mailadmin>Not Set; F; user>Not Set; None   －(b)
Fri Feb 27 10:49:27 2004; mailadmin>mailadmin; F; user>testuser; None   －(c)
```

```
Fri Feb 27 10:50:04 2004; mailadmin>mailuser; F; user>testuser; None－(d)
Fri Feb 27 10:50:40 2004; mailadmin>mailadmin; S; user>testuser; F　－(e)
```

MPCC 管理者モードのログファイルには
①ツールを使用した日時
②メールユーザ管理者のユーザ名（mailadmin>の部分へ記録される．入力されなかった場合は”No Set”）
③メールユーザ管理者の認証に成功したか失敗したか（成功なら”S”，失敗なら”F”）
④パスワード変更対象となったユーザのユーザ名（user>の部分へ記録される．入力されなかった場合は”No Set”）
⑤パスワード変更対象となったユーザに対するパスワード変更処理が成功したか失敗したか（成功なら”S”，失敗なら”F”．メールユーザ管理者の認証失敗時など、パスワード変更処理が行われなかった場合は”None”）
が記録される．先の出力例は次のような状態のログである．

(a)　メールユーザ管理者 mailadmin がメールユーザ mailuser に対してパスワード変更処理を行い、メールユーザ管理者の認証、メールユーザに対するパスワード変更がともに成功した．
(b)　メールユーザ管理者、パスワード変更対象のメールユーザがともに設定されず、処理を行わなかった．
(c)　メールユーザ管理者 mailadmin に対する認証が何らかの原因で失敗した．
(d)　メールユーザ管理者 mailuser に対する認証に失敗した．
(e)　メールユーザ管理者 mailadmin に対する認証には成功したが、メールユーザ testuser に対するパスワード変更処理が失敗した．

「受理年月日　2004 年9月30日」