

お客様名

Unicorn ID Manager

コマンドライン仕様書



OSSTech

オープンソース・ソリューション・テクノロジー(株)

文書番号: XXXXX

作成者: 野村 健太郎

作成日: 2011年 3月 1日

リビジョン: 1.2

目次

1. 概要	1
1.1 目的	1
2. Unicorn IDM コマンドライン仕様	2
2.1 コマンドライン操作概要	2
2.2 ユーザー登録	3
2.3 ユーザー更新	3
2.4 ユーザー削除	4
2.5 ユーザーの無効化、有効化	5
2.6 ユーザー一覧取得	5
2.7 CSV ファイルの書式について	6
2.8 Google Apps ニックネームの登録	6
2.9 コマンド返り値について	6
2.10 コマンドの実行完了タイミングについて	7
2.10.1 unicornidm-account-csvhandle	7
2.10.2 unicornidm-account-userlist	7
2.10.3 googleapps-nickname-csvadd	7
3. Unicorn ID Manager のログ	8
3.1 ログ出力ディレクトリ	8
3.2 ログファイル名の書式	8
3.2.1 基本書式	8
3.2.2 操作種別について	9
3.2.3 操作対象について	9
3.2.4 ログファイル出力パターン	9
3.3 ログ出力内容	11
3.3.1 ユーザー一覧取得コマンド以外のコマンド	11
3.3.2 ユーザー一覧取得コマンド	11
3.4 ログファイルサンプル	12
4. Google Apps ニックネーム登録ログ	13
4.1 ログ出力ディレクトリ	13
4.2 ログファイル名の書式	13
4.3 ログ出力内容	13
4.4 ログファイルサンプル	13

5. ログファイル名の取得方法	15
6. 改版履歴	16

1. 概要

本文書 Unicorn ID Manager(以下、Unicorn IDM)のコマンドライン仕様書です。

1.1 目的

Unicorn IDM の機能を外部ツールなどから利用する際の仕様を記します。

2. Unicorn IDM コマンドライン仕様

本章では、Unicorn IDM のコマンドラインインタフェースの仕様について説明します。

2.1 コマンドライン操作概要

Unicorn ID Manager のコマンドラインインタフェースでは操作を行うことが可能です。1～5 の操作については、それぞれの操作ごとに CSV ファイルを作成する必要があります。

1. ユーザー登録
2. ユーザー更新
3. ユーザー削除
4. ユーザー無効化
5. ユーザー有効化
6. ユーザー一覧の取得

Unicorn ID Manager で使用する CSV ファイルで指定できる項目として、以下のものがあります。

ヘッダ名	説明
username	ユーザー名。Google Apps へのログイン、LDAP 認証に使用される。
sn	姓
givenName	名
password	パスワード
uidNumber	UNIX の uid を指定
gidNumber	UNIX の gid を指定
unixHomeDirectory	UNIX のホームディレクトリを指定
mail	メールアドレス

2.2 ユーザー登録

Google Apps と LDAP にユーザーを登録するための CSV ファイルは、次のフォーマットとなります。

username	sn	givenName	password	uidNumber	gidNumber	unixHomeDirectory	mail
ytakeda	武田	保真	Xee1shei	1000	2000	/home/1000/ytakeda	ytakeda@example.com
tyamada	山田	太郎	Saeroh1h	1001	2000	/home/1000/tyamada	tyamada@example.com

- 1 行目は、ヘッダとして必要です。（大文字、小文字の区別があります）
- CSV ファイルは、UTF-8 で作成する必要があります。（Shift-JIS などで作成した場合は、Linux 上で iconv コマンドで変換可能です。）

Google Apps のみにユーザーを登録する組織の場合、次の CSV ファイルとなります。

username	sn	givenName	password
ytakeda	武田	保真	Xee1shei
tyamada	山田	太郎	Saeroh1h

Unicorn ID Manager でのユーザー登録コマンドは、次の書式です。

```
# /opt/osstech/sbin/unicornidm-account-csvhandle -t <組織名> -o useradd -f <csv ファイル>
```

組織名は、Unicorn ID Manager の初期設定時に設定します。

2.3 ユーザー更新

Google Apps と LDAP にユーザーを登録するための CSV ファイルは、次のフォーマットとなります。

username	sn	givenName	password	uidNumber	gidNumber	unixHomeDirectory	mail
ytakeda	武田	保真	newpass	2000	2000	/home/1000/ytakeda	ytakeda@new.example.com

			word1				e.com
tyamada	山田	太郎	newpass word2	2001	2000	/home/1000/tyamada	tyamada@new.examp e.com

- 1行目は、ヘッダとして必要です。（大文字、小文字の区別があります）
- CSV ファイルは、UTF-8 で作成する必要があります。（Shift-JIS などで作成した場合は、Linux 上で iconv コマンドで変換可能です。）
- Google Apps で変更可能な属性は、「sn」、「givenName」、「password」の3つのみです。

ユーザー更新時は、変更対象のフィールドのみ記載した CSV ファイルを利用することができます。また、値が設定されていないフィールドは、Google Apps や LDAP に登録されている内容は更新されません。

例えば、パスワードのみを一括更新したい場合、次の CSV ファイルを作成します。

username	password
ytakeda	aen5Egho
tyamada	Vohni3iy

Unicorn ID Manager でのユーザー情報の更新コマンドは、次の書式です。

```
# /opt/osstech/sbin/unicornidm-account-csvhandle -t <組織名> -o usermod -f <csv ファイル>
```

2.4 ユーザー削除

ユーザーを削除するための CSV ファイルは、次のフォーマットとなります。

username	unixHomeDirectory
ytakeda	/home/1000/ytakeda
tyamada	/home/2000/tyamada

Unicorn ID Manager でのユーザーの削除コマンドは、次の書式です。

```
# /opt/osstech/sbin/unicornidm-account-csvhandle -t <組織名> -o userdel -f <csv ファイル>
```

2.5 ユーザーの無効化、有効化

無効化、有効化を行う際には、対象となるユーザーのリストとなる CSV ファイルをそれぞれ作成します。

username
ytakeda
tyamada

Unicorn ID Manager でのユーザーの無効化コマンドは、次の書式です。

```
# /opt/osstech/sbin/unicornidm-account-csvhandle -t <組織名> -o userdisable -f <csv ファイル>
```

Unicorn ID Manager でのユーザーの有効化コマンドは、次の書式です。

```
# /opt/osstech/sbin/unicornidm-account-csvhandle -t <組織名> -o userenable -f <csv ファイル>
```

2.6 ユーザー一覧取得

対象組織のユーザー一覧を取得し、CSV ファイルとして出力します。コマンドは、次の書式です。

```
# /opt/osstech/sbin/unicornidm-account-userlist -t <組織名> -f <出力 csv ファイル>
```

出力 CSV ファイルには以下の書式でユーザー一覧が出力されます。

username	属性…	対象サーバー 1	対象サーバー…
ユーザー名	…	アカウントの登録状態	アカウントの登録状態

- CSV ファイルに日本語が含まれる場合、文字コードは Shift-JIS となります。
- 「対象サーバー」には UnicornIDM の管理単位である「組織」に登録されている全てのサーバーが出力されます。
- 「アカウントの登録状態」には次のステータスが表示されます。

ステータス	意味
enable	対象サーバーにアカウントが登録されており、有効である
disable	対象サーバーにアカウントが登録されているが、無効である
None	対象サーバーにアカウントが登録されていない

以下に例を示します。

```
username,sn,givenName,LDAP,student.ga.example.co.jp,staff.ga.example.co.jp
ytakeda,武田,保真,enable,enable,None
tyamada,山田,太郎,disable,disable,None
sato,佐藤,花子,enable,None,None
```

2.7 CSV ファイルの書式について

各種コマンドの入力に使用する CSV ファイルの書式は RFC に準拠しています(RFC4180)。RFC に、カラムのデータをダブルクォーテーションで囲む必要がある場合の説明などが記載されているため、CSV の書式に関しては RFC4180 をご参照ください。

- <http://www.ietf.org/rfc/rfc4180.txt>

2.8 Google Apps ニックネームの登録

Unicorn ID Manager の機能ではありませんが、Google Apps にニックネームを登録するためのコマンドインターフェースを用意しています。

このコマンドを利用することで、ユーザー登録時に Google Apps にニックネームの登録を行うことが可能です。

ニックネーム登録のための CSV フォーマットは次の通りです。

username	nickname
ytakeda	yasuma.takeda
tyamada	taro.yamada

- 1 行目はヘッダとして必要です。

ニックネームの登録コマンドは、次の書式です。

```
# /opt/osstech/sbin/googleapps-nickname-csvadd -d <Google Apps ドメイン名> -f <csv ファイル>
```

2.9 コマンド返り値について

いずれのコマンドも、返り値として以下の値を返します。

- 0 … 正常終了(ただし、コマンドによっては処理はバックグラウンドで進行する)

- 1 … 異常終了

2.10 コマンドの実行完了タイミングについて

|| 2.10.1 unicornidm-account-csvhandle

unicornidm-account-csvhandle コマンドは実行するとすぐにプロンプトに制御が戻りますが、実際の処理はバックグラウンドで進行します。そのため、処理が完了したかどうかの判定はログファイルへの書き込みの完了(正確には、ログファイルのファイルクローズ)から判断する必要があります。

ログファイルへの書き込みの完了を検知するために、「5 ログファイル名の取得方法」で説明するように、書き込みが完了したログファイルの名前を特定のファイルに書き出すようにしています。

unicornidm-account-csvhandle コマンド実行完了の判定は、実行した操作のログファイルへの書き込みの完了から判断してください。

|| 2.10.2 unicornidm-account-userlist

ユーザー一覧取得コマンドである unicornidm-account-userlist は、ユーザー一覧を取得し、指定したファイルに出力するまでプロンプトに制御が戻りません。処理が完了したかどうかの判断は、コマンド実行の完了から判断してください。

|| 2.10.3 googleapps-nickname-csvadd

googleapps-nickname-csvadd コマンドは、Google Apps へのニックネーム登録処理が完了するまでプロンプトに制御が戻りません。処理が完了したかどうかの判断は、以下のどちらかから判断してください。

1. コマンド実行の完了
2. ログファイルへの書き込み完了(unicornidm-account-csvhandle と同様)

googleapps-nickname-csvadd コマンドの場合も、「5 ログファイル名の取得方法」で説明するように、書き込みが完了したログファイルの名前を特定のファイルに書き出すようにしています。

3. Unicorn ID Manager のログ

本章ではUnicorn IDM のログについて説明します。

3.1 ログ出力ディレクトリ

ログファイルは以下のディレクトリに出力されます。

- /opt/osstech/var/lib/unicornIDM/results/組織名

「組織名」は、Unicorn IDM の初期設定時に登録した管理単位としての組織を意味します。

3.2 ログファイル名の書式

ログファイル名の書式について説明します。

3.2.1 基本書式

ログファイルのファイル名書式は以下のようになります。

年月日-時刻_操作種別_操作対象.result

各項目の詳細は以下の表のようになります。

項目	詳細
年月日	書式：yyyymmdd 例：20100325（2010年3月25日）
時刻	書式：hhmmss 例：185401（18時54分1秒）
操作種別	• useradd：ユーザー登録 • useraddhook：ホームディレクトリ作成 • usermod：ユーザー更新 • userdel：ユーザー削除 • userdelhook：ホームディレクトリ削除 • userdisable：ユーザー無効化 • userenable：ユーザー有効化 • userlist：ユーザー一覧取得
操作対象	• ldapserver：LDAP サーバー • ActiveDirectory：Active Directory • 学部生 Google Apps ドメイン名

	・ 卒業生 Google Apps ドメイン名 ・ 組織名（ホームディレクトリ作成/削除時のみ）
--	---

3.2.2 操作種別について

操作種別の「useraddhook」と「userdelhook」は、ホームディレクトリの自動作成/削除機能を有効にしている組織において、ユーザー登録とユーザー削除を実行した場合にのみ出力されます。これらは、Unicorn IDMが自動的にホームディレクトリの作成/削除を実行した際のログとなります。ホームディレクトリの自動作成/削除機能を無効に設定した組織では、操作種別が「useraddhook」と「userdelhook」のログは出力されません。

3.2.3 操作対象について

Unicorn IDM 上の一つの組織に対する操作であっても、ログファイルはその組織に登録されているLDAP サーバーや Google Apps などの操作対象毎に出力されます。

ただし、ホームディレクトリの自動作成/削除のログは、操作対象が「組織名」となります(ホームディレクトリの自動作成/削除 はUnicorn IDM の組織毎に設定するため)。

3.2.4 ログファイル出力パターン

例として、以下の組織が登録されていると仮定します。

組織名	登録されている操作対象
Studens	・ LDAP サーバー(ldapserver) ・ 学部生 GoogleApps ドメイン
AD	・ ActiveDirectory
Graduate	・ 卒業生 GoogleApps ドメイン

以下にログファイルの出力パターンをまとめます。

組織名	操作	出力ファイル
Students	ユーザー登録	年月日-時刻_useradd_学部生 GoogleApps ドメイン名.result 年月日-時刻_useradd_ldapserver.result 年月日-時刻_useraddhook_Students.result

	ユーザー更新	年月日-時刻_usermod_学部生 GoogleApps ドメイン名.result 年月日-時刻_usermod_ldapserver.result
	ユーザー削除	年月日-時刻_userdel_学部生 GoogleApps ドメイン名.result 年月日-時刻_userdel_ldapserver.result 年月日-時刻_userdelhook_Students.result
	ユーザー無効化	年月日-時刻_userdisable_学部生 GoogleApps ドメイン名.result 年月日-時刻_userdisable_ldapserver.result
	ユーザー有効化	年月日-時刻_userenable_学部生 GoogleApps ドメイン名.result 年月日-時刻_userenable_ldapserver.result
	ユーザー一覧取得	年月日-時刻_userlist_学部生 GoogleApps ドメイン名.result 年月日-時刻_userlist_ldapserver.result
AD	ユーザー登録	年月日-時刻_useradd_ActiveDirectory.result
	ユーザー更新	年月日-時刻_usermod_ActiveDirectory.result
	ユーザー削除	年月日-時刻_userdel_ActiveDirectory.result
	ユーザー無効化	年月日-時刻_userdisable_ActiveDirectory.result
	ユーザー有効化	年月日-時刻_userenable_ActiveDirectory.result
	ユーザー一覧取得	年月日-時刻_userlist_ActiveDirectory.result
Graduate	ユーザー登録	年月日-時刻_useradd_卒業生 GoogleApps ドメイン名.result
	ユーザー更新	年月日-時刻_usermod_卒業生 GoogleApps ドメイン名.result
	ユーザー削除	年月日-時刻_userdel_卒業生 GoogleApps ドメイン名.result
	ユーザー無効化	年月日-時刻_userdisable_卒業生 GoogleApps ドメイン名.result
	ユーザー有効化	年月日-時刻_userenable_卒業生 GoogleApps ドメイン名.result
	ユーザー一覧取得	年月日-時刻_userlist_卒業生 GoogleApps ドメイン名.result

3.3 ログ出力内容

3.3.1 ユーザー一覧取得コマンド以外のコマンド

ユーザー一覧取得コマンド以外のコマンドでは、いずれの操作においても以下のようなログが出力されます。

```
ytakeda,OK ← 操作に成功したユーザー
tyamada,User already exists ← 操作に失敗したユーザーとその原因
```

カラム	意味
第一カラム	ユーザー名
第二カラム	登録結果 ・ OK：操作成功 ・ OK 以外：操作失敗の原因

ログファイルから「,OK」を含まない行を抽出することで、操作に失敗したユーザーを検出することが可能です。

3.3.2 ユーザー一覧取得コマンド

ユーザー一覧取得コマンドでは、ログファイルに各サーバー/各 Google Apps ドメインのユーザー一覧が出力されます。出力 CSV ファイルには以下の書式でユーザー一覧が出力されます。

username	属性…	active
ユーザー名	…	アカウントの登録状態

「active」のカラムには次のステータスが表示されます。

ステータス	意味
True	アカウントが有効である
False	アカウントが無効である

以下に例を示します。

```
username,sn,givenName,active
ytakeda,武田,保真,True
tyamada,山田,太郎,False
```

3.4 ログファイルサンプル

Studens 組織におけるユーザー登録時のログファイルサンプルです。以下のファイルにログが出力されます。

- LDAP サーバーへのユーザー登録結果
 - `/opt/osstech/var/lib/unicornIDM/results/Studens/20100325-185458_useradd_ldapserver.result`
- ホームディレクトリの自動作成結果
 - `/opt/osstech/var/lib/unicornIDM/results/Studens/20100325-185458_useraddhook_Studens.result`
- Google Apps へのユーザー登録結果
 - `/opt/osstech/var/lib/unicornIDM/results/Studens/20100325-185458_useradd_gapps.example.com.result`

4. Google Apps ニックネーム登録ログ

Google Apps にニックネームを登録するコマンドのログについて説明します。

4.1 ログ出力ディレクトリ

ログファイルは以下のディレクトリに出力されます。

- /opt/osstech/var/log/googleappsutils/results

4.2 ログファイル名の書式

ログファイルのファイル名書式

```
年月日-時刻_nicknameadd_ドメイン名-result.csv
```

年月日、時刻の書式は「3.2.1.基本書式」と同じです。

4.3 ログ出力内容

以下のようなログが出力されます。

```
ytakeda,OK ← ニックネーム登録に成功したユーザー  
tyamada,EntityExists(1300) ← ニックネーム登録に失敗したユーザーとその原因
```

カラム	意味
第一カラム	ユーザー名
第二カラム	登録結果 ・ OK：ニックネーム登録成功 ・ OK 以外：ニックネーム登録失敗の原因(Google Apps ライブラリが出力)

ログファイルから「,OK」を含まない行を抽出することで、ニックネーム登録に失敗したユーザーを検出することが可能です。

4.4 ログファイルサンプル

Google Apps にニックネームを登録した際のログファイルのサンプルです。

- /opt/osstech/var/log/googleappsutils/results/20100216-110955-nicknameadd-

gapps.example.com-result.csv

5. ログファイル名の取得方法

ログファイルはユーザー登録・更新・削除などの操作の度に新規作成され、ファイル名に年月日時刻を含みます。そのため、外部ツールなどからログ確認を行う際には、ログファイル名の取得が煩雑になります。

以下のファイルに、実行した操作によって生成されたログファイルのファイル名が上書き方式で書き出されます。外部ツールなどから操作実行後のログを確認したい場合は、このファイルからログファイル名を取得すると便利です。Google Apps ニックネーム登録コマンドのログファイル名も以下のファイルに出力されます。

- `/opt/osstech/var/lib/unicornIDM/logfilelist`

ファイル内容は以下のようになります。

```
/opt/osstech/var/lib/unicornIDM/results/Studens/20100325-193629_useradd_ldapserver.result  
/opt/osstech/var/lib/unicornIDM/results/Studens/20100325-193629_useraddhook_Studens.result
```

このファイルの内容は変更・削除しても問題ありません。

例えば、外部ツールから Unicorn IDM コマンド/Google Apps ニックネーム登録コマンドを実行する際に、コマンド実行前に `/opt/osstech/var/lib/unicornIDM/logfilelist` の内容を削除しておき、コマンド実行後に、`/opt/osstech/var/lib/unicornIDM/logfilelist` のファイルサイズが 0 より大きな値になっていればコマンドの実行が完了したと判断する、といった使用も可能です。

6. 改版履歴

- 2010 年 3 月 26 日 野村 健太郎
 - 初版作成
- 2010 年 5 月 19 日 野村 健太郎
 - ユーザー一覧取得コマンドを追加
 - コマンドの返り値の説明を追加
- 2011 年 3 月 1 日 野村 健太郎
 - Unicorn IDM 2.X 対応