



# ITA\_利用手順マニュアル

管理コンソール

—第1.1版—

## 免責事項

本書の内容はすべて日本電気株式会社が所有する著作権に保護されています。

本書の内容の一部または全部を無断で転載および複製することは禁止されています。

本書の内容は将来予告なしに変更することがあります。

日本電気株式会社は、本書の技術的もしくは編集上の間違い、欠落について、一切責任を負いません。

日本電気株式会社は、本書の内容に関し、その正確性、有用性、確実性その他いかなる保証もいたしません。

## 商標

- ・ LinuxはLinus Torvalds氏の米国およびその他の国における登録商標または商標です。
- ・ Red Hatは、Red Hat, Inc.の米国およびその他の国における登録商標または商標です。
- ・ Apache、Apache Tomcat、Tomcatは、Apache Software Foundationの登録商標または商標です。
- ・ Ansibleは、Red Hat, Inc.の登録商標または商標です。
- ・ Active Directoryは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

その他、本書に記載のシステム名、会社名、製品名は、各社の登録商標もしくは商標です。

なお、® マーク、TMマークは本書に明記しておりません。

※本書では「Exastro IT Automation」を「ITA」として記載します。

## 目次

目次.....	2
はじめに .....	4
1 ITA システム 管理コンソールの概要 .....	5
1.1 ITA 管理コンソールについて .....	5
1.1.1 画面説明 ログイン、パスワード登録.....	6
(1) ログイン画面 .....	6
(2) パスワード変更 .....	6
(3) ログアウト画面(もう一度ログインする) .....	6
1.1.2 画面説明 ITA 管理コンソール .....	7
(1) メインメニュー .....	7
(2) システム設定 .....	8
(3) メニューグループ管理.....	9
(4) メニュー管理 .....	12
(5) ロール管理 .....	15
(6) ユーザー管理.....	16
(7) ロール・メニュー紐付管理.....	17
(8) ロール・ユーザ紐付管理.....	18
(9) IP アドレスフィルタ管理 .....	19
(10) メニューエクスポート.....	20
(11) エクスポート/インポート管理 .....	23
(12) ITA バージョン確認.....	24
(13) オペレーション削除管理 .....	25
(14) ファイル削除管理 .....	27
1.2 BackYard コンテンツ .....	28
1.2.1 BackYard 処理一覧 .....	28
1.2.2 BackYard 処理説明 .....	28
(1) メール送信 .....	28
(2) ロール紐付確認＋クリーニング .....	33
(3) 投入オペレーション確認＋クリーニング .....	33
(4) ファイル確認＋クリーニング .....	33
(5) メニューインポート実行.....	33
(6) メニューインポートクリーニング .....	33
(7) ActiveDirectory 情報ミラーリング .....	33
1.3 標準 REST 機能の利用 .....	34
1.3.1 リクエストの形式 .....	34
1.3.2 利用可能なメソッドとコマンド .....	35
1.4 ActiveDirectory 連携機能の利用 .....	45
1.4.1 利用の開始.....	45
1.4.2 機能概要 .....	46
(1) AD 情報ミラーリング機能 .....	46
1.4.3 AD 情報ミラーリング機能 .....	エラー! ブックマークが定義されていません。
(1) AD 認証(Kerberos 認証)機能.....	46
1.4.4 AD 情報ミラーリング機能 .....	47
1.4.5 AD 認証(Kerberos 認証)機能.....	49
1.4.6 本機能の例外について .....	50

(1)	連携対象外レコード.....	50
(2)	AD 認証対象外 (ITA 内部認証) .....	50
2	運用操作 .....	51
2.1	インストールの開始 .....	51
2.2	オペレーション作業履歴の定期削除 .....	51
2.3	ログレベルの変更.....	53
2.4	メンテナンス .....	54
2.4.1	ITA システム 独立型プロセスの起動/停止/再起動 .....	54
3	Appendix .....	55
3.1	トラブルシューティング .....	55

## はじめに

---

本書は、ITA システムの管理コンソールの概要および操作方法について記載したものです。

## 1 ITA システム 管理コンソールの概要

本章では ITA を操作するための管理コンソールについて説明します。

### 1.1 ITA 管理コンソールについて

ITA 管理コンソールでは、ITA を利用するユーザー（アカウント）、操作メニューの実行権限の登録／更新／削除を行います。

また、ITA 初期メニュー以外に、利用部門が独自の情報を ITA のデータベース上で管理する場合、管理レベルにあった個別メニューの作成もできます。

個別メニューの登録／変更／削除をご使用される際は、製品サポートへお問い合わせください。

表 1.1-1 Web コンテンツメニュー/画面一覧

No	メニューグループ	メニュー・画面
1	共通部	ログイン画面
2		パスワード変更画面
3		ログアウト画面
4	ITA 管理コンソール	メインメニュー
5		システム設定
6		メニューグループ管理
7		メニュー管理
8		コンテンツファイル管理
9		ロール管理
10		ユーザー管理
11		ロール・メニュー紐付管理
12		ロール・ユーザ紐付管理
13		IP アドレスフィルタ管理（デフォルトでは非表示）
14		メニューエクスポート
15		メニューインポート
16		エクスポート/インポート管理
17		オペレーション削除管理（デフォルトでは非表示）
18		ファイル削除管理（デフォルトでは非表示）

### 1.1.1 画面説明 ログイン、パスワード登録

#### (1) ログイン画面

ITA システムのメニュー画面に未ログインでアクセスした場合、「ログイン画面」が表示されます。



図 1.1-1 ITA ログイン画面

ITA システムのインストール直後は必ず次のログインIDとパスワードでログインしてください。

ログイン ID : administrator

初期パスワード : password

インストール後に初めてログインした際は「パスワード変更画面」に遷移します。

#### (2) パスワード変更

ログインユーザーは任意のタイミングで自身のパスワードを変更できます。

各メニュー画面右上の「パスワード変更」ボタンから「パスワード変更画面」に遷移し、パスワード変更を行ってください。



図 1.1-2 ITA パスワード変更画面

#### (3) ログアウト画面(もう一度ログインする)

各メニュー画面右上「ログアウト」ボタンをクリックすると、システムからログアウトします。

表示されている「もう一度ログインする」リンクをクリックすると、ログイン画面に遷移します。



図 1.1-3 ITA ログアウト画面

## 1.1.2 画面説明 ITA 管理コンソール

### (1) メインメニュー

メインメニューは、各メニューグループのメインメニューへの URL リンクを表示しており、押下することで指定のメニューグループのメインメニューへ遷移できます。

表示されるメインメニュー、並びにマニュアル一覧画面で表示されるマニュアルは、**インストールしたドライバーのみ**表示されます。



図 1.1-4 メインメニュー画面



## (2) システム設定

ITA システム導入・運用時に設定すべき各種情報の登録／更新／廃止を行います。

### 【注意】

サブメニューの「システム設定」は、製品サポート向けのメニューですので、使用しないでください。

設定値を変更されると、ITA の動作は保証されません。

Exastro  
IT Automation

管理コンソール

Menu

メインメニュー

システム設定

メニューグループ管理

メニュー管理

ロール管理

ユーザ管理

ロール・メニュー紐付管理

ロール・ユーザ紐付管理

メニューエクスポート

メニューインポート

エクスポート/インポート管理

バージョン確認

説明

表示フィルタ

一覧/更新

更新	廃止	設定値	項目ID	項目名	項目値	設定値	注釈
更新	廃止	2,100,000,001	IP_FILTER	IPアドレス規制			IPアドレスを利用したアクセス規制の有効/無効を選択 規制する場合のホワイトリストはIPアドレスフィルタ管理 ブランク：無効 1:有効
更新	廃止	2,100,000,002	FORBIDDEN_UPLOAD	アップロード禁止拡張子	.exe;.com;.php;.cgi;.sh;.sql;.vbs;.js;.pl;.ini;.htaccess		ファイルアップロードを禁止する拡張子 (半角セミコロン区切り)
更新	廃止	2,100,000,003	PWL_EXPIRY	アカウントロック継続期間 (秒)	0		アカウントロック起点日時からロック状態を継続する期間 正の数(整数のみ)：上記の通り ゼロ：ロックしない 負の数：ロックされたアカウントは永久にロック状態
更新	廃止	2,100,000,004	PWL_THRESHOLD	パスワード誤り閾値(回数)	3		アカウントをロックするためのパスワード失敗回数 正の数(整数のみ)：上記の通り ゼロ；設定不可 負の数(整数のみ)：アカウントロック機能がOFFになる
更新	廃止	2,100,000,005	PWL_COUNT_MAX	パスワード誤りカウント上限(回数)	5		パスワードの連続誤りをカウントする上限回数 正の数(整数のみ)：上記の通り ゼロ以下：誤りがカウントされない
更新	廃止	2,100,000,006	PW_REUSE_FORBID	パスワード再登録防止期間 (日)	180		同一パスワードの再登録を防止する期間(日数) 正の数(整数のみ)：上記の通り ゼロ以下：再登録防止期間は無くなり同一パスワードが再
更新	廃止	2,100,000,007	PASSWORD_EXPIRY	パスワード有効期間(日)	90		パスワードの有効期間(日数) 正の数(整数のみ)：上記の通り ゼロ以下：永久に有効(利用可能) となる
更新	廃止	2,100,000,008	AUTH_IDLE_EXPIRY	認証継続期間：未操作 (秒)	3600		未操作時に認証(セッション)を継続する期間 (秒) 正の数(整数のみ)：上記の通り (ただしphp.iniの「session.gc_maxlifetime」で指定の値 ゼロ以下：設定不可
更新	廃止	2,100,000,009	AUTH_SES_EXPIRY	認証継続期間：最長 (秒)	10800		認証(セッション)を継続する最長期間 (秒) (ただしphp.iniの「session.gc_maxlifetime」で指定の値 ゼロ以下：設定不可

フィルタ結果件数: 9

Excel出力

管理画面に接続

図 1.1-5 管理コンソール画面

### (3) メニューグループ管理

メニュー(子)はメニューグループ(親)に属します。この画面で親となるメニューグループの登録／更新／廃止を行います。

メニューグループ名称は、**一意**である必要があります。

更新	廃止	メニューグループID	メニューグループ名称	表示順番	パネル用画像	メニュー情報	備考
更新	廃止	1	入力用	1,000		メニュー情報	
更新	廃止	2	参照用	1,100		メニュー情報	
更新	廃止	2,100,000,001	Exastro IT Automation			メニュー情報	ユーザ向け共通メニューグループ。
更新	廃止	2,100,000,002	管理コンソール	10	kanri.png	メニュー情報	システム管理者向けメニューグループ。
更新	廃止	2,100,000,003	基本コンソール	20	kihon.png	メニュー情報	基本コンソール
更新	廃止	2,100,011,501	資材管理 管理	30	szai_kanri.png	メニュー情報	資材管理 管理
更新	廃止	2,100,011,502	資材管理 払出払戻	40	szai_harai.png	メニュー情報	資材管理 払出払戻
更新	廃止	2,100,011,601	パラメータシート作成	51	sheet.png	メニュー情報	パラメータシート作成
更新	廃止	2,100,011,602	マスタ作成	50	master.png	メニュー情報	マスタ作成
更新	廃止	2,100,011,609	パラメータシート(組)ホスト分解	59		メニュー情報	パラメータシート(組)ホスト分解
更新	廃止	2,100,011,701	ホストグループ管理	60	host_group.png	メニュー情報	ホストグループ管理
更新	廃止	2,100,020,000	Ansible共通	70	anscmn.png	メニュー情報	Ansible共通
更新	廃止	2,100,020,001	Ansible-Legacy	80	anslsc.png	メニュー情報	Ansible-Legacy
更新	廃止	2,100,020,002	Ansible-Pioneer	90	anspcr.png	メニュー情報	Ansible-Pioneer
更新	廃止	2,100,020,003	Ansible-LegacyRole	100	anslr.png	メニュー情報	Ansible-LegacyRole
更新	廃止	2,100,030,001	Cobbler	110	cobbler.png	メニュー情報	Cobbler
更新	廃止	2,100,060,001	DSC	140	dsc.png	メニュー情報	DSC
更新	廃止	2,100,070,001	OpenStack	150	openstack.png	メニュー情報	OpenStack

フィルタ結果件数: 18

Excel出力

図 1.1-6 メニューグループ管理画面

ここで、各サブメニューの操作について説明します。操作は、他のメニューにおいても共通です。  
データ更新系の操作のため、システム管理者でログインしてください。

#### (登録内容の更新／廃止 - 1件ごと更新／廃止／復活)

メニューグループを1件1件更新／廃止／復活する場合の操作です。

##### ① 「一覧/更新」サブメニューに登録情報を表示

「表示フィルタ」に検索条件を入力し、Enterキーか[フィルタ]ボタンをクリックします。

- 1) 登録内容を変更する — [更新] ボタンで編集モードにし、値を変更
- 2) 項目を無効にする — [廃止] ボタンをクリック
- 3) 無効(廃止)の項目を有効にする — [復活] ボタンをクリック

##### ② 実行確認のポップアップ画面が表示され、[OK]または[キャンセル]をクリックします。

#### (追加登録 - 1件ずつ登録)

メニューグループを1件1件登録する場合の操作です。

- ① [登録] サブメニューを開き、[登録開始] ボタンをクリックして登録フォームを表示します。
- ② 「メニューグループ名称」を入力し、[登録] ボタンをクリックします。

※ メニューグループ名称は重複登録できません。

※ 「表示順序」は任意ですが、空白の場合はメニューグループがメインメニューに表示されません。

※ 「表示順序」の昇順にメインメニューに表示されます。「表示順序」が同じ場合は、

「メニューグループID」の昇順で表示されます。

※ 「備考」は任意です。

図 1.1-7 メニューグループ管理画面(登録)

(登録内容の更新／廃止- まとめて更新／廃止)

一度に複数のメニューグループを登録する場合の操作です。

- ① [全件ダウンロードとファイルアップロード編集] サブメニューを開き、[全件ダウンロード(Excel)] で新規登録用シートをダウンロードします。
- ② 以下の各項目を入力してファイルを保存します。
  - 実行処理種別= 登録／更新／廃止／復活 を選択
    - ・メニューグループ名称 = 変更後の名称
    - ・表示順序 = 変更後の内容
    - ・備考 = 変更後の内容

- ③ [ファイルを選択] ボタンで②のファイルを指定し、[ファイルアップロード] でアップロードを行います。

※「実行処理種別」が選択されていなかったり、正しい処理種別を選択していない場合、登録が実行されません。

(追加登録 - まとめて登録)

一度に複数のメニューグループを登録する場合の操作です。

- ① [全件ダウンロードとファイルアップロード編集] サブメニューを開き、[新規登録用ダウンロード(Excel)] で新規登録用シートをダウンロードします。
- ② 以下の各項目を入力してファイルを保存します。
  - ・実行処理種別 = 登録
  - ・メニューグループ名称 = 新規に登録するメニューグループ名称
  - ・表示順序 = メニューグループの表示順序
- ③ [ファイルを選択] ボタンで②のファイルを指定し、[ファイルアップロード]でアップロードを行います。
 

※「実行処理種別」を「登録」以外にすると、登録が実行されません。

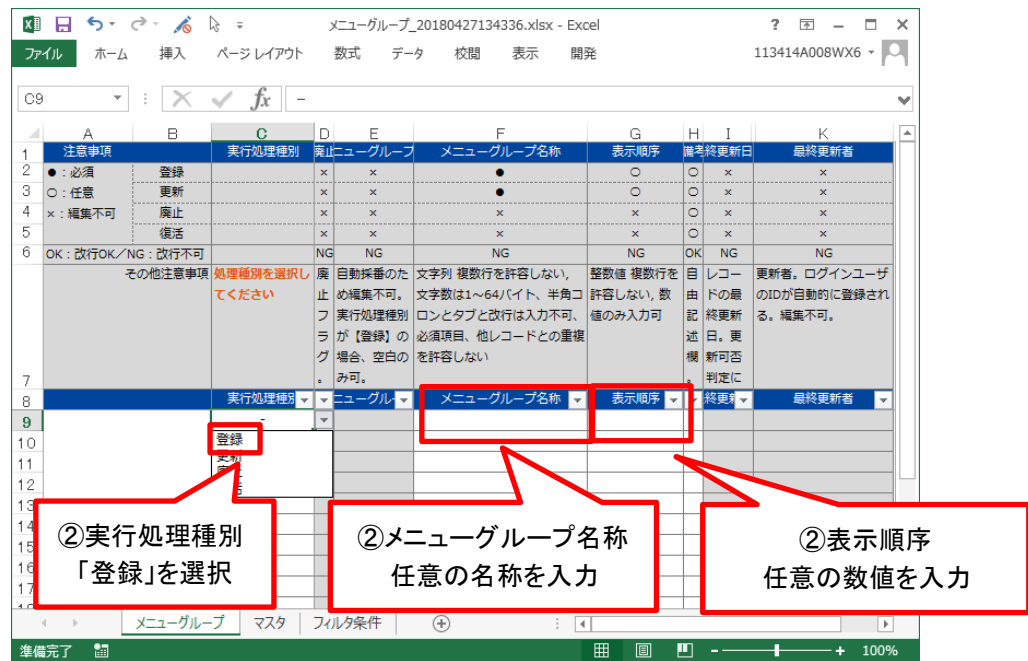


図 1.1-8 メニューグループ管理画面

※ メニューグループの登録を行うと、作成したメニューグループ配下に自動的に「メインメニュー」が登録されて、「システム管理者」ロールのユーザで参照することが可能となります。

具体的には、以下のメニューに自動的にデータが登録されます。

- ・「メニュー管理」メニュー
- ・「コンテンツファイル管理」メニュー
- ・「ロール・メニュー紐付管理」メニュー

#### (4) メニュー管理

この画面でコンテンツの機能(メニュー)の登録／更新／廃止を行います。  
メニュー名称は一意である必要があります。

##### ① メニューに対するロール情報・コンテンツファイルの確認

「一覧/更新」サブメニューから、その機能に対するロール情報とコンテンツファイルの対応を確認できます。

Exastro IT Automation 管理コンソール										
Menu										
メインメニュー										
システム設定										
メニューグループ管理										
メニュー管理										
ロール管理										
ユーザ管理										
ロール・メニュー紐付管理										
ロール・ユーザ紐付管理										
メニューエクスポート										
メニューインポート										
エクスポート/インポート管理										
バージョン確認										
説明										
表示フィルタ										
一覧/更新										
更新	廃止	メニューID	メニューグループ		メニュー名称	認証要否	サービス提供中	メニューグループ内表示順序	ロール情報	操作
			ID	名称						
更新	廃止	1	1	入力用	代入値登録	要	サービス提供中	1	ロール情報	する
更新	廃止	2	2	参照用	代入値登録	要	サービス提供中	1	ロール情報	する
更新	廃止	2,100,000,101	2100000001	Exastro IT Automation	ログイン画面	不要	サービス提供中	1	ロール情報	しない
更新	廃止	2,100,000,102	2100000001	Exastro IT Automation	システムエラー	不要	サービス提供中	2	ロール情報	しない
更新	廃止	2,100,000,103	2100000001	Exastro IT Automation	不正操作によるアクセス警告	不要	サービス提供中	3	ロール情報	しない
更新	廃止	2,100,000,104	2100000001	Exastro IT Automation	不正端末からのアクセス警告	不要	サービス提供中	4	ロール情報	しない
更新	廃止	2,100,000,105	2100000001	Exastro IT Automation	ログインID一覧	不要	サービス提供中	5	ロール情報	しない
更新	廃止	2,100,000,106	2100000001	Exastro IT Automation	パスワード変更	不要	サービス提供中	6	ロール情報	しない
更新	廃止	2,100,000,107	2100000001	Exastro IT Automation	アカウントロックエラー	不要	サービス提供中	7	ロール情報	しない
更新	廃止	2,100,000,202	2100000002	管理コンソール	システム設定	要	サービス提供中	2	ロール情報	する
更新	廃止	2,100,000,203	2100000002	管理コンソール	IPアドレスフィルタ管理	要	サービス提供中	3	ロール情報	する
更新	廃止	2,100,000,204	2100000002	管理コンソール	メニューグループ管理	要	サービス提供中	4	ロール情報	する
更新	廃止	2,100,000,205	2100000002	管理コンソール	メニュー管理	要	サービス提供中	5	ロール情報	する
更新	廃止	2,100,000,207	2100000002	管理コンソール	ロール管理	要	サービス提供中	7	ロール情報	する

#### 1.1-9 メニュー管理

ロール情報

△閉じる

メニュー情報

廃止	メニューID	メニューグループID	メニュー名称	認証要否	メニューグループ内表示順序	備考	最終更新日時	最終更新者	
	2100000208	2100000002	管理コンソール	ユーザ管理	要	8	廃止不可	2015/04/01 10:00:00	システム管理者

ロール情報

ロールID	アクセス権限	ロール名称
1	メンテナンス可	システム管理者

メンテナンス

図 1.1-10 ロール情報画面(メニュー管理)

## ② パラメータ

メニューの登録情報には次の項目があります。

表 1.1-2 「メニュー管理」のパラメータ

	項目名	説明
1	認証可否	不要: ログインせずにアクセス可能 要 : ログイン後のみアクセス可能
2	サービス状態	サービス提供中: アクティブ状態。一般ユーザーがアクセス可能 メニュー開発中: システム管理者のみアクセス可能
3	メニューグループ内表示順序	メニューグループのサブメニューで表示する順序。昇順で上から表示される。
4	オートフィルタチェック	メニュー表示時に「オートフィルタ」のチェックボックスにチェックを入れるかどうかの設定
5	初回フィルタ	メニュー表示時に「フィルタ」を押下した状態で表示するかどうかの設定
6	Web 表示最大行数	[一覧/更新]に表示する最大行数
7	Web 表示前確認行数	[一覧/更新]に出力する前に確認ダイアログを表示する最大行数
8	Excel 出力最大行数	Excel 出力する最大行数

認証可否	サービス状態	メニューグループ内表示順序	オートフィルタチェック	初回フィルタ	Web表示最大行数	Web表示前確認行数	Excel出力最大行数
① プルダウン検索	② プルダウン検索	③ プルダウン検索	④ プルダウン検索	⑤ プルダウン検索	⑥ プルダウン検索	⑦ プルダウン検索	⑧ プルダウン検索

図 1.1-11 メニュー登録画面(メニュー管理)

【Web 表示最大行数】と【Web 表示前確認行数】には次のような関係があります。

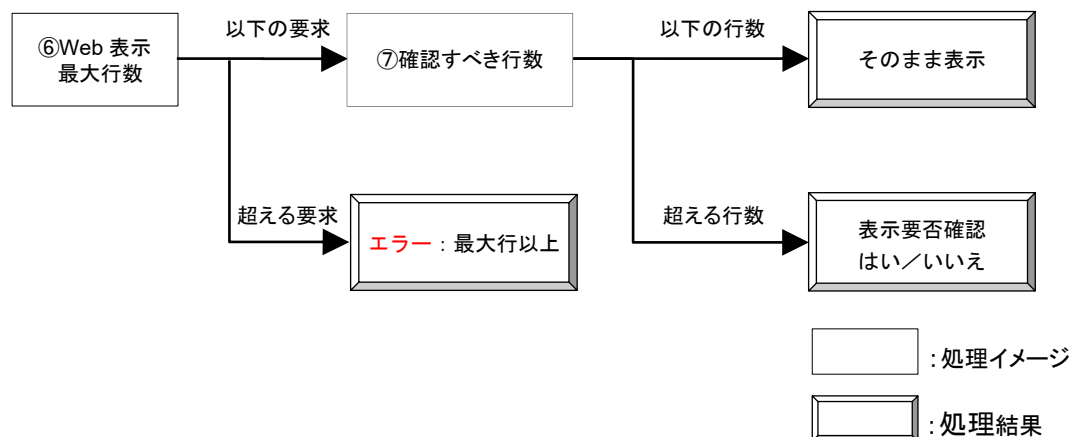


図 1.1-12 Web 表示最大行数の処理概要

【Excel 出力最大行数】を超えている場合、そのメニューの「全件ダウンロードとファイルアップロード編集」の項目の表示が、以下のように変化します。



図 1.1-13 エラー表示画面(メニュー管理)

この画面からダウンロードできるファイルは、Excel ではなく独自フォーマットの CSV です。このファイルを使って編集、アップロードを行いたい場合は、「独自フォーマット編集 Excel 作成ツール」のボタンでツールをダウンロードし、ダウンロードされたファイルの中にある「ReadMe」ファイルの説明に従って操作してください。

## (5) ロール管理

ロールの登録／更新／廃止を行います。

また、そのロールを持つユーザーや対応付けられているメニューを確認のみ行えます。

ロール名は一意である必要があります。

The screenshot displays the 'Exastro IT Automation 管理コンソール' (Management Console) interface. The left sidebar contains a 'Menu' section with options like 'メインメニュー', 'システム設定', 'メニューグループ管理', 'メニュー管理', 'ロール管理' (highlighted), 'ユーザ管理', 'ロール・メニュー紐付管理', 'ロール・ユーザ紐付管理', 'メニューエクスポート', 'メニューインポート', 'エクスポート/インポート管理', and 'バージョン確認'. The main content area is titled 'ロール管理' (Role Management) and includes a '説明' (Description) section, a '表示フィルタ' (Display Filter) section with search criteria for role ID, name, and status, and a table of roles. The table has columns for '更新' (Update), '廃止' (Delete), 'ロールID', 'ロール名', 'ユーザ情報', 'メニュー情報', '権限', '最終更新日時', and '最終更新者'. One role is listed: 'システム管理者' (System Administrator) with ID '1'. Below the table is an 'Excel出力' (Excel Export) button. The bottom section contains links to '登録' (Registration), '全件ダウンロードとファイルアップロード編集' (Full Download and File Upload Edit), 'ユーザ情報' (User Information), 'メニュー情報' (Menu Information), and '変更履歴' (Change History).

図 1.1-14 コンテンツファイル管理画面



## (6) ユーザー管理

ユーザー(アカウント)の登録/更新/廃止を行います。

また、「ロール情報」ボタンから、ユーザーとロール(実行権限)の紐付のメンテナンスができます。

アカウントロックがかかった場合、この画面から解除可能です。

ログイン ID は一意である必要があります。

The screenshot shows the Exastro IT Automation management console. The left sidebar contains a menu with options like 'メニュー管理' and 'ロール管理'. The main area is titled 'ユーザ管理' (User Management). It features a search bar with filters for '廃止' (Deletion), 'ユーザID', 'ログインID', 'ユーザ名', 'メールアドレス', 'PW最終更新日時', 'PWカウンタ', and 'ロック日時'. Below the search bar is a table of users. The first user is 'administrator' with a login ID of '1'. The 'ロール情報' (Role Information) button is highlighted with a red box. Below the table, there is a section for '一覧/更新' (List/Update) and a table of roles. The first role is 'システム管理者' (System Administrator) with a role ID of '1'. The 'ロール情報' button is highlighted with a red box.

更新	廃止	ユーザID	ログインID	ログインPW	ユーザ名	メールアドレス	ロール情報	PW最終更新日時	PWカウンタ	ロック日時	ロック解除	権限	最終更新日時	最終更新者
更新	廃止	1	administrator	*****	システム管理者	sample@xxx.bbb.co.jp	ロール情報	2019/07/17 17:22:14			ロック解除	システム管理者	2019/07/17 17:22:14	システム管理者

図 1.1-15 ロール設定画面への遷移操作画面(ユーザ管理)

## (7) ロール・メニュー紐付管理

各メニューとロール対応付けの登録／更新／廃止を行います。

ロールに紐付かないメニュー画面はメニューグループに表示されません。

The screenshot shows the 'Exastro IT Automation 管理コンソール' interface. The left sidebar contains navigation links like 'メニュー管理', 'ロール管理', and 'ユーザ管理'. The main area is titled 'ロール・メニュー紐付管理'. It features a '表示フィルタ' (Display Filter) section with dropdowns for '検索コード' and '検索条件'. Below this is a table with columns for 'ID', '名称', 'メニューグループ', and 'メニュー'. The table lists various roles and their associated menu items, including 'システム管理者' and 'システム設定'.

図 1.1-16 ロール・メニュー紐付管理画面

「(4)メニュー管理」「(5)ロール管理」で登録したロールとメニューがリストボックスに表示される(下図 ①,②)ので、それぞれを選択し、紐付タイプ(下図 ③)を選択します。

The screenshot shows the '登録' (Registration) form. It has three red boxes highlighting the selection areas: ① for 'ロール (ID:名称)\*', ② for 'メニューグループ:メニュー\*', and ③ for '紐付'. The form also includes a '自動入力' (Auto-fill) section and a '※\*は必須項目です。' (Note: \* is a required item) warning. At the bottom are '戻る' (Back) and '登録' (Register) buttons.

図 1.1-17 グループメニュー権限の設定画面(ロール・メニュー紐付管理)

## (8) ロール・ユーザ紐付管理

各ユーザー（アカウント）とロール（実行権限）対応付けの登録／更新／廃止を行います。  
 ロールに紐付かないユーザー（アカウント）は各メニュー画面にアクセスできません

The screenshot shows the 'ロール・ユーザ紐付管理' (Role-User Assignment Management) screen in the Exastro IT Automation management console. The interface includes a sidebar menu with options like 'メニュー管理', 'ロール管理', and 'ユーザ管理'. The main content area has a '表示フィルタ' (Display Filter) section with various dropdowns and input fields. Below this is a table with columns for '更新', '廃止', 'ID', 'ロールID', 'ロール名称', 'ユーザID', 'ユーザログインID', '権限', '最終更新日時', and '最終更新者'. A single row is visible for 'システム管理者' (System Administrator). At the bottom, there are buttons for '登録' (Register), '更新' (Update), and '廃止' (Delete), along with a note about required fields.

図 1.1-18 ロール・ユーザ紐付管理画面

「(5)ロール管理」ならびに「(6)ユーザー管理」で登録したロールとユーザーがリストボックスに表示される（下図 ①，②）ので、それぞれを選択します。

The screenshot shows the 'ユーザ権限の設定画面 (ロール・ユーザ設定画面)' (User Permission Setting screen). It features two dropdown menus for selecting a role and a user, both highlighted with red boxes and numbered 1 and 2 respectively. Below the dropdowns are buttons for '戻る' (Back) and '登録' (Register). A note at the bottom states: '※ \*は必須項目です。' (Note: \* indicates required items).

図 1.1-19 ユーザー権限の設定画面 (ロール・ユーザ設定画面)

### (9) IP アドレスフィルタ管理

ITA システムに接続を許可するユーザー端末の登録／更新／廃止を行います。

当機能は、導入初期は無効のため、メニューに表示されていません。

利用する場合は、以下の手順で有効にしてください。

- ① 「ロール・メニュー紐付管理」を開く
- ② 「表示フィルタ」→「メニューグループ」のプルダウンから「管理コンソール」を選択する
- ③ 「IP アドレスフィルタ管理」を「復活」する
- ④ 画面をリロードする

IPv4 形式のアドレスを登録し、「システム設定」で「IP アドレス規制」を有効にすると、登録した端末からのみアクセス可能になります。

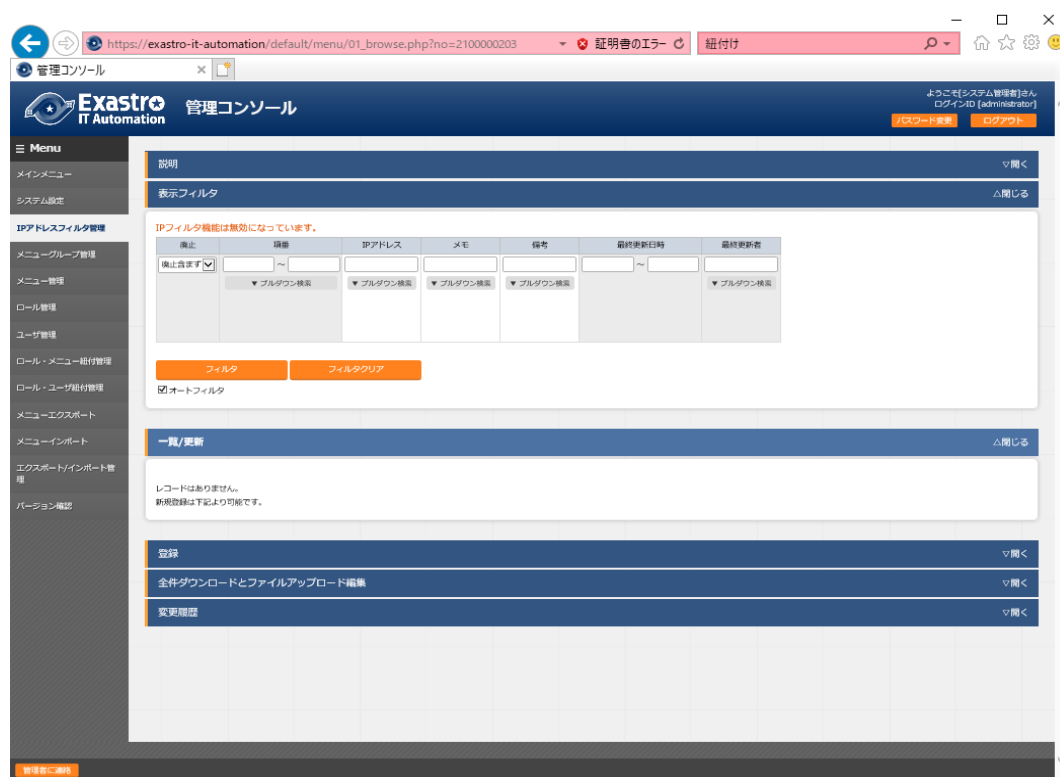


図 1.1-20 IP アドレスフィルタ管理画面

※ 「システム設定」で「IP アドレス規制」が無効の場合、「IP フィルタ機能は無効になっています。」メッセージが表示されます。

#### 【注意】

接続可能な端末を登録後に「システム設定」の「IP アドレス規制」を有効にしてください。  
有効端末を登録せず「IP アドレス規制」を有効にすると、ITA システム自体に接続できなくなります。

## (10) メニューエクスポート

ITA システムに登録されているデータを、メニューごとにエクスポートします。

※データを別の ITA 環境に移す場合、すべてのメニューを対象に移動しないとデータの整合性が壊れる可能性があります。

### ① エクスポートするメニューを選択する

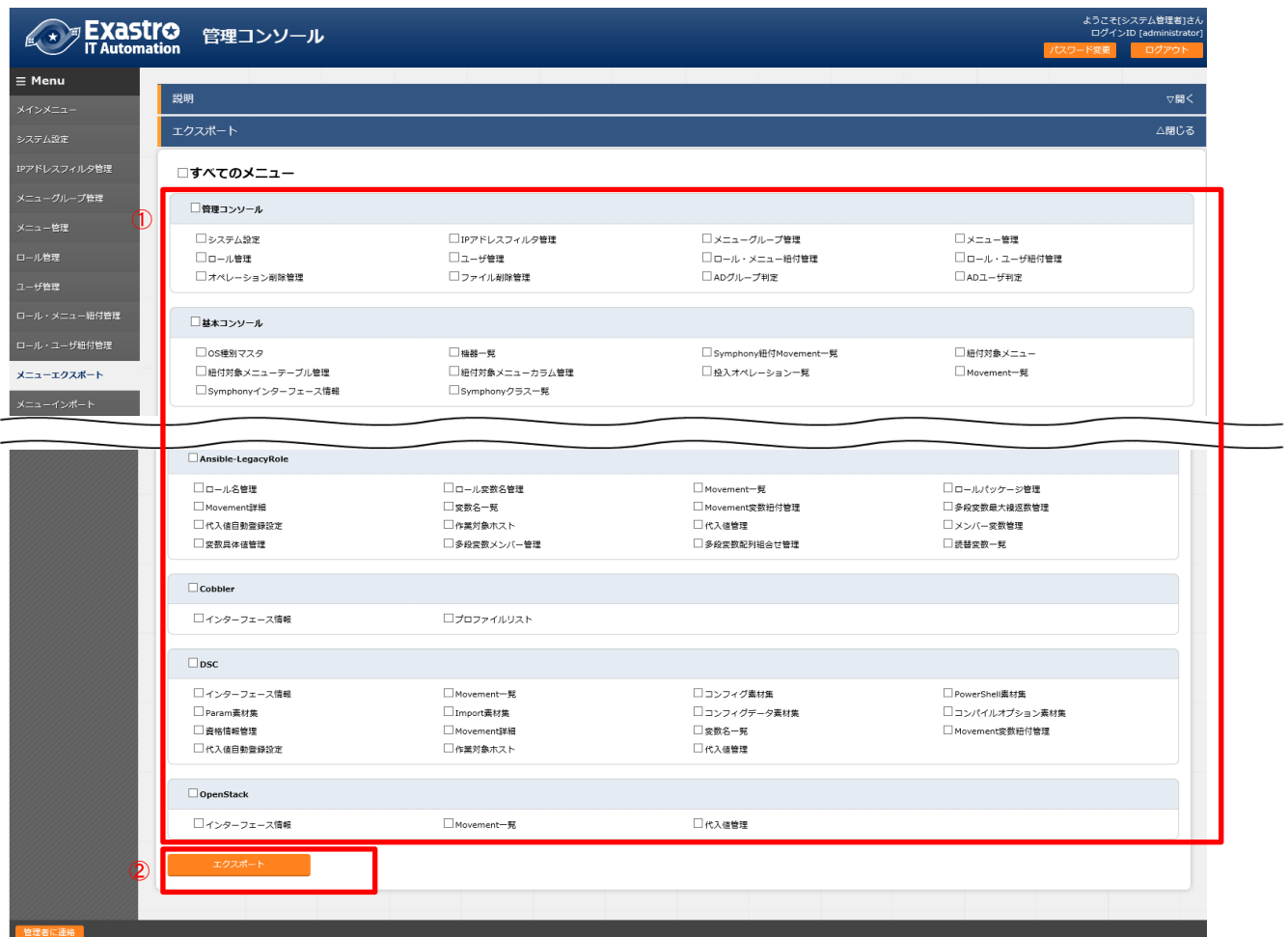
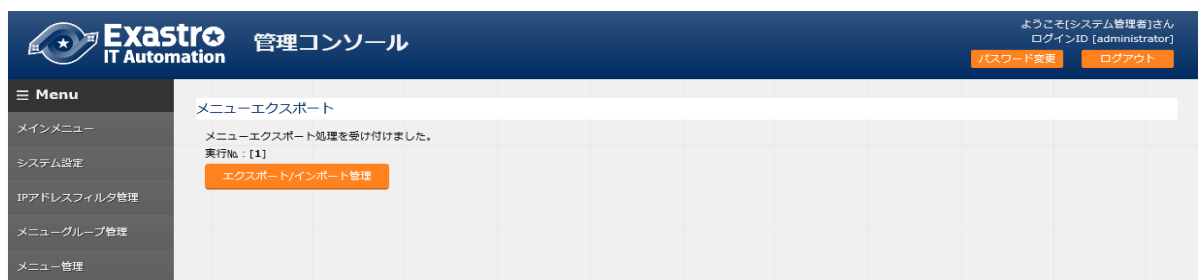


図 1.1-21 メニューエクスポート画面(1)

### ② メニューを選択後、エクスポートボタンをクリックする

エクスポート処理の実行Noが表示されるので、エクスポート/インポート管理画面で処理のステータスを確認してください。



## メニューインポート

「(10)メニューエクスポート」で保存した kym ファイルをアップロードします。

- ① アップロードする kym ファイルを選択する
- ② アップロードボタンをクリックする



図 1.1-22 メニューインポート画面(1)

- ③ インポートするメニューを選択する  
チェックボックスがチェックされているメニューがインポートされます。  
インポートする必要がないメニューは、チェックは外してください。

- ④ インポートボタンをクリックする  
廃止データをインポートしない場合は「インポート(廃止を除く)」をクリックする



図 1.1-23 メニューインポート画面(2)

- ⑤ メニューインポートボタンをクリックする  
インポート処理の実行No.が表示されるので、エクスポート/インポート管理画面で処理のステータスを確認してください。



図 1.1-24 メニューインポート画面(3)

### (11) エクスポート/インポート管理

エクスポートとインポートのステータスを確認します。

ステータスは、「未実行」、「実行中」、「完了」の順に変わります。

処理種別は、「エクスポート」または「インポート」が表示されます。

インポート種別は、処理種別が「インポート」の場合に「通常」または「廃止を除く」が表示されます。

フィルタボタンをクリックしてステータスが「完了」になったことを確認してください。

インポート処理でエラーが発生した場合は、ステータスが「完了(異常)」になります。

The screenshot displays the 'Exastro IT Automation 管理コンソール' (Management Console). The left sidebar contains a 'Menu' with various system management options. The main area shows the 'エクスポート/インポート管理' (Export/Import Management) section. It includes a table with columns for '実行ID' (Execution ID), 'ステータス' (Status), '処理種別' (Process Type), 'インポート種別' (Import Type), 'ファイル名' (File Name), '最終更新日時' (Last Update Time), and '最終更新者' (Last Updated By). Two records are listed, both with a status of '完了' (Completed). The second record is an 'インポート' (Import) of type '通常' (Normal). Red boxes highlight the 'ステータス' and '処理種別' columns for the second record. Below the table, there is a 'フィルタ結果件数: 2' (Filter Result Count: 2) and an 'Excel出力' (Excel Output) button. The bottom of the page shows '全件ダウンロード' (Download All) and '変更履歴' (Change History) buttons.

実行ID	ステータス	処理種別	インポート種別	ファイル名	最終更新日時	最終更新者
1	完了	エクスポート		ita_exportdata_20190601045655.kym	2019/06/01 04:56:55	データポータビリティプロシージャ
2	完了	インポート	通常	2_ita_exportdata_20190601045655.kym	2019/06/01 05:12:46	データポータビリティプロシージャ

図 1.1-25 エクスポート/インポート管理画面



## (12) ITA バージョン確認

ITA の各機能のバージョンを確認します。  
インストール済みの機能のみ確認できます。

The screenshot displays the Exastro IT Automation Management Console interface. The top header features the Exastro logo and the text '管理コンソール'. A left-hand menu lists various system management options. The main content area is titled 'バージョン情報' (Version Information) and contains a table listing installed components and their versions. At the bottom of the interface, there is a button labeled '管理者に連絡' (Contact Administrator).

ドライバ	バージョン
Base	Exastro IT Automation Base functions version 1.1
Ansible	Exastro IT Automation Ansible Driver version 1.1
Cobbler	Exastro IT Automation Cobbler Driver version 1.1
Create_param	Exastro IT Automation Create_param version 1.1
DSC	Exastro IT Automation DSC Driver version 1.1
Hostgroup	Exastro IT Automation Hostgroup version 1.1
Hostgroup2	Exastro IT Automation Hostgroup2 version 1.1
Hostgroup3	Exastro IT Automation Hostgroup3 version 1.1
Material	Exastro IT Automation Material version 1.1
Material2	Exastro IT Automation Material2 version 1.1
Material3	Exastro IT Automation Material3 version 1.1
Material5	Exastro IT Automation Material5 version 1.1
OpenStack	Exastro IT Automation OpenStack Driver version 1.1

図 1.1-267 ITA バージョン確認画面

### (13) オペレーション削除管理

基本コンソール[投入オペレーション一覧]に登録されているオペレーションの実施予定日に紐づくデータを、指定した「論理削除日数」と「物理削除日数」に基づき削除する設定を行います。

「論理削除日数」を過ぎた場合は廃止、「物理削除日数」を過ぎた場合は DB から削除します。

当機能は、導入初期は無効のため、メニューに表示されていません。

利用する場合は、以下の手順で有効にしてください。

- ① 「ロール・メニュー紐付管理」を開く
- ② 「表示フィルタ」→「メニューグループ」のプルダウンから「管理コンソール」を選択する
- ③ 「オペレーション削除管理」を「復活」する
- ④ 画面をリロードする

The screenshot displays the 'Management Console' (管理コンソール) of Exastro IT Automation. The left sidebar contains a 'Menu' (メニュー) section with various management options. The main area is titled 'Operation Deletion Management' (オペレーション削除管理) and features a 'Filters' (フィルタ) section with dropdown menus for 'Deletion Status' (廃止), 'Item Number' (項番), 'Logical Deletion Days' (論理削除日数), 'Physical Deletion Days' (物理削除日数), 'Table Name' (テーブル名), and 'Main Column Name' (主キーカラム名). Below the filters are 'Filter' (フィルタ) and 'Clear Filter' (フィルタクリア) buttons. A table of operations is visible, with columns corresponding to the filter criteria. The bottom of the page has a 'Connect to Administrator' (管理者に連絡) button.

図 1.1-278 オペレーション削除管理画面

画面の項目一覧は以下のとおりです。

表 1.2-3 登録画面項目一覧(投入オペレーション一覧)

項目	説明	入力 必須	入力形式	制約事項
論理削除日数	マシン日時を基準にして、オペレーションの実施予定日が指定した日数日数を経過していたら、論理削除(廃止)を行います。	○	手動入力	数値
物理削除日数	マシン日時を基準にして、オペレーションの実施予定日が指定した日数日数を経過していたら、物理削除(DB からレコード削除)を行います。	○	手動入力	数値
テーブル名	削除対象のテーブル名を指定します。	○	手動入力	最大長 256 バイト
主キーカラム名	テーブルの主キーのカラム名を指定します。	○	手動入力	最大長 256 バイト
オペレーション ID カラム名	テーブルでオペレーション ID を保持しているカラム名を指定します。	○	手動入力	最大長 256 バイト
データストレージパス取得 SQL	履歴データパス 1~4 でインタフェース情報のデータストレージ配下のパスを指定している場合、インタフェース情報のデータストレージ情報を取得する SELECT 文を記載します。データストレージ配下のパスを指定していない場合は省略可能です。  exp) select ANSIBLE_STORAGE_PATH_LNX AS <b>PATH</b> from B_ANSIBLE_IF_INFO where DISUSE_FLAG='0' ※必ずエイリアス名に PATH を設定してください。	-	手動入力	最大長 1024 バイト
履歴データパス 1	履歴データパス 1(省略可能) 作業インスタンスディレクトリの投入データ履歴や結果データ履歴など、~/ita-root/配下のパスの場合は、~/ita-root/からの相対パスを記載します。  exp) Ansible Legacy 投入データ履歴の場合 uploadfiles/2100020113/FILE_INPUT Ansible Legacy 結果データ履歴の場合 uploadfiles/2100020113 /FILE_RESULT 作業インスタンスディレクトリ(データストレージ)など、インタフェース情報のデータストレージ配下のパスの場合はデータストレージを示すキーワード「/__data_relay_storage__」を付けたパスを記載します。  exp) Ansible Legacy 作業インスタンスディレクトリの場合 /__data_relay_storage__/legacy/ns/ ~/ita-root/配下またはデータストレージ配下以外のパスの場合は絶対パスを記載します。  exp) /var/log/hoge 履歴データパス 2~履歴データパス 4 も同様	-	手動入力	最大長 1024 バイト
履歴データパス 2	履歴データパス 2(省略可能)	-	手動入力	最大長 1024 バイト
履歴データパス 3	履歴データパス 3(省略可能)	-	手動入力	最大長 1024 バイト
履歴データパス 4	履歴データパス 4(省略可能)	-	手動入力	最大長 1024 バイト
備考	自由記述欄です	-	手動入力	最大長 4000 バイト

## (14) ファイル削除管理

サーバ上のファイルの最終更新日を確認して、保存期間が過ぎているファイルを削除する設定を行います。  
当機能は、導入初期は無効のため、メニューに表示されていません。  
利用する場合は、以下の手順で有効にしてください。

- ① 「ロール・メニュー紐付管理」を開く
- ② 「表示フィルタ」→「メニューグループ」のプルダウンから「管理コンソール」を選択する
- ③ 「ファイル削除管理」を「復活」する
- ④ 画面をリロードする

The screenshot shows the '管理コンソール' (Management Console) interface. The sidebar menu on the left includes 'Menu', 'メインメニュー', 'システム設定', 'IPアドレスフィルタ管理', 'メニューグループ管理', 'メニュー管理', 'ロール管理', 'ユーザ管理', 'ロール・メニュー紐付管理', 'ロール・ユーザ紐付管理', 'メニューエクスポート', 'メニューインポート', 'エクスポート/インポート管理', 'オペレーション削除管理', 'ファイル削除管理', and 'バージョン確認'. The main content area has a '説明' (Description) section, a '表示フィルタ' (Display Filter) section with a dropdown for 'メニューグループ' (Menu Group) set to '管理コンソール', and a table for '登録' (Registration). The table has columns for '項目' (Item), '削除日数' (Deletion Period), '削除対象ディレクトリ' (Deletion Target Directory), '削除対象ファイル' (Deletion Target File), 'サブディレクトリ削除有無' (Subdirectory Deletion Yes/No), and '備考' (Remarks). The '削除日数' column has a dropdown set to '廃止含まず' (Exclude discontinued). The '登録' section has a '自動入力' (Automatic Input) button and a '登録' (Register) button.

図 1.1-29 ファイル削除管理画面

画面の項目一覧は以下のとおりです。

表 1.2-4 登録画面項目一覧(投入オペレーション一覧)

項目	説明	入力必須	入力形式	制約事項
削除日数	最終更新日を基準にして、設定した日数を経過していたら、削除を行います。	○	手動入力	数値
削除対象ディレクトリ	削除対象ファイルが格納されているディレクトリを設定します。	○	手動入力	最大長 1024 バイト
削除対象ファイル	削除対象のファイル名を指定します。ワイルドカードでの設定が可能です。	○	手動入力	最大長 1024 バイト
サブディレクトリ削除有無	削除対象ディレクトリ直下のディレクトリも削除するかどうか設定する。「あり」の場合、削除対象ディレクトリ直下のディレクトリの名前と最終更新日を確認して、削除対象であれば削除します。	○	リスト選択	あり／なし

## 1.2 BackYard コンテンツ

ここでは、ITA 基本機能での BackYard コンテンツについて説明します。  
BackYard はサーバー内で独立して動作する常駐プロセス化した機能です。Web ブラウザ上で操作する Web コンテンツとは異なり、ユーザーは BackYard の存在を意識することはありません。  
処理の開始・停止等の制御はコマンドラインで実行してください。

### 1.2.1 BackYard 処理一覧

BackYard の処理の一覧を以下に記述します。

表 1.2-1 BackYard 機能

No	処理名称	ファイル名(※)	備考
1	メール送信	ky_mail※1	必要が無ければ停止可
2	ロール紐付確認＋クリーニング	ky_std_checkcondition-linklist※1	常駐
3	投入オペレーション確認＋クリーニング	ky_execinstance_dataautoclean-workflow.sh※2	Cron 起動
4	ファイル確認＋クリーニング	ky_file_autoclean-workflow.sh※3	Cron 起動
5	メニューインポート実行	ky_data_portability_execute-workflow	常駐
6	メニューインポートクリーニング	ky_data_portability_dataautoclean-workflow.sh	Cron 起動
7	ActiveDirectory 情報ミラーリング	ky_activedirectory_roleuser_replication-workflow.php※7	常駐

※1 ファイル配置ディレクトリは ~/ita-root/backyards/webdbcore

※2、5、6、7 ファイル配置ディレクトリは ~/ita-root/backyards/ita-base

※3、4 ファイル配置ディレクトリは ~/ita-root/backyards/common

### 1.2.2 BackYard 処理説明

BackYard の処理について説明を以下より記述します。

#### (1) メール送信

メール送信は、ユーザーが作成したメールのテンプレートに送信元、送信先アドレスや本文内の変数を動的に置換し、自動送信する処理です。

メール送信はテンプレートリスト、テンプレート、送信依頼ファイルという 3 つのファイル(詳細後述)を参照し、実行の要否を判断しながら処理を行います。

送信パターンは フリー型、セーフ型、フリーフォーマット型の 3 パターンがあります。

それぞれのパターンによる各ファイルの要不要、必要事項は次の表のとおりです。

表 1.2-2 送信タイプ別参照ファイルへの記載事項

ファイル名 送信タイプ	テンプレート	テンプレートリスト				送信依頼ファイル			
	ファイル中の項目	テンプレート ID	置き換え 文言数	from, to	cc	タイトル	from, to	cc	置き換え 文字列
	位置	1 列目	2 列目	3 列目	4 列目	1 行目	2,3 行目	4 行目	5 行目以降
フリー型	必要	必須	数値 (0 以上)	不要		必須	必須	任意	指定分の 文字列
セーフ型			X 固定	必須	任意		不要		不要
フリーフォーマット型	不要(※)								

※ メール本文は送信依頼ファイルに記述します。

次に、各ファイルの説明とサンプルを提示します。

【重要】各ファイルは、文字コード[UTF-8]／改行(LF)で編集してください。

#### ① テンプレートリスト

- ・ファイル名 : sysmail.list
- ・配置ディレクトリ : ~/ita-root/confs/backyardconfs/

メールテンプレートで使用する変数数や送信先アドレスなどをリストするファイルです。

このリストを元に送信処理が行われます。

#### ■ テンプレートリスト記述例

	1	2	3	4	5
フリー型	001	3			
セーフ型	002	3	from_add@ita.com	to_add@ita.com	cc_add@ita.jp
	003	7	from_add@ita.com	to1@ita.com,to2@ita.com	null
フリーフォーマット型	004	X	from_004@ita.com	to_004@ita.com	null

↑ ↑ ↑ ↑ タブ区切り

図 1.2-1 テンプレートリスト 記述例

表 1.2-3 テンプレートリストの必須パラメーター一覧表

No	項目	必須	補足
1	テンプレート ID	○	001~999 (000 は予約済のため使用不可)
2	置き換え文言数	○	可変文字列数。例) 日付、人名など
3	送信元メールアドレス	△	送信依頼ファイルに記述しない場合は必須
4	送信先メールアドレス	△	同上
5	cc アドレス	×	不要の場合は「null」を指定

※ ④複数指定する場合はコンマ区切り

#### ② テンプレート

- ・ファイル名 : sysmail\_body\_nnn.txt
- ・配置ディレクトリ : ~/ita-root/confs/backyardconfs/

メールの本体です。ファイル名の[ nnn ] は「テンプレート ID」を入れてください。

例) ○ sysmail\_body\_001.txt

× sysmail\_body\_1.txt

メール本文と、可変部分があれば置換用の変数(%%001%% ~ %%999%%)を記述します。  
変数は、テンプレートリストファイルに指定した「置き換え文言数」分の連番にします。

#### ■ テンプレート記述例 [OK]

To:%%001%% 各位  
管理部よりお知らせです。  
%%003%%のパスワードが%%002%%日変更されていません。  
7日以内に新しいパスワードを設定してください。

順序の入れ替わりは OK

※ 置き換え文言数 = 3

#### ■ テンプレート記述例 [NG]

To:%%001%% 各位  
管理部よりお知らせです。  
%%002%%のパスワードが%%005%%日変更されていません。  
7日以内に新しいパスワードを設定してください。

連番ではないため NG

### ③ 送信依頼ファイル

- ・ ファイル名 : sysmail\_nnn\_任意の半角英数字.txt
- ・ 配置ディレクトリ : ~/ita-root/temp/ky\_mail\_queues/ky\_sysmail\_0\_queue/

テンプレートに差し込む文字列を記載します。ファイル名の[ nnn ] は「テンプレート ID」を入れてください。[ nnn ]以降はファイルが一意になるよう任意の半角文字列を入れてください。

例) ファイル命名の例

- sysmail\_001\_20140813123025\_123456789
- sysmail\_001\_a001.txt
- × sysmail\_001\_
- × sysmail\_001\_.txt

テンプレートリスト、テンプレートを用意後、このファイルを配置ディレクトリに置くことで、メールが送信されます。

メール送信の際、置き換え文字をテンプレート中の変数に差し込みます。

送信依頼ファイルは、メール送信後、送信状況によって以下のディレクトリに移動します。

送信成功 → ~/ita-root/temp/ky\_mail\_queues/ky\_sysmail\_1\_success

送信失敗 → ~/ita-root/temp/ky\_mail\_queues/ky\_sysmail\_2\_error

#### ■ 送信依頼ファイルフォーマット

送信依頼ファイルは、行ごとに意味が決まっています。

- 1 行目 ... メールタイトル
- 2 行目 ... 送信元メールアドレス
- 3 行目 ... 送信先メールアドレス(複数指定の場合はコンマで区切る)
- 4 行目 ... cc メールアドレス(不要の場合は空行)
- 5 行目 ~ ... 置き換え文字列

※ 2~4 行目はフリー型のみ必要

※ 5 行目以降の文字列行数が、テンプレートの変数数およびテンプレートリスト②置き換え文言数と同じでない場合、エラーになります。

「①テンプレートリスト」「テンプレート」を例に、送信依頼ファイル記述例を提示します。

#### ■ 送信依頼ファイル記述例

1) フリー型例: テンプレート ID = 001

sysmail\_001\_20160401\_0001.txt

```
パスワード変更依頼 ..... > メールタイトル
admin@ita.jp ..... > 送信元アドレス
ml_dev1@ita.jp ..... > 送信先アドレス
ml_sup1@ita.jp ..... > cc アドレス
システム部 ..... > %%001%% 置換文字列
90 ..... > %%002%% 置換文字列
開発部ポータル ..... > %%003%% 置換文字列
```

送信されたメール: 送信依頼ファイルから置換された箇所(赤字)

パスワード変更依頼  
from: admin@ita.jp  
to: ml\_dev1@ita.jp  
cc: ml\_sup1@ita.jp  
To: システム部 各位  
管理部よりお知らせです。  
開発部ポータルのパスワードが 90 日変更されていません。  
7 日以内に新しいパスワードを設定してください。

2) セーフ型例: テンプレート ID = 002

sysmail\_002\_20160401\_0001.txt

パスワード変更依頼 ..... > メールタイトル  
システム部 ..... > %%001%% 置換文字列  
90 ..... > %%002%% 置換文字列  
開発部ポータル ..... > %%003%% 置換文字列

※ メールアドレスはテンプレートリストファイルに指定

送信されたメール: 送信依頼ファイルから置換されたか所(赤字)

テンプレートリストから置換されたか所(青字)

パスワード変更依頼  
from: from\_add@ita.com  
to: to\_add@ita.com  
cc: cc\_add@ita.com  
To: システム部 各位  
管理部よりお知らせです。  
開発部ポータルのパスワードが 90 日変更されていません。  
7 日以内に新しいパスワードを設定してください。

3) フリーフォーマット型: テンプレート ID = 004

sysmail\_004\_20160401\_0001.txt

パスワード変更依頼  
To: システム部 各位  
管理部よりお知らせです。  
開発部ポータルのパスワードが 90 日変更されていません。  
7 日以内に新しいパスワードを設定してください。

送信されたメール: テンプレートリストから置換されたか所(青字)

パスワード変更依頼  
from: from\_004@ita.com  
to: to\_004@ita.com  
cc:  
To: システム部 各位  
管理部よりお知らせです。  
開発部ポータルのパスワードが 90 日変更されていません。  
7 日以内に新しいパスワードを設定してください。



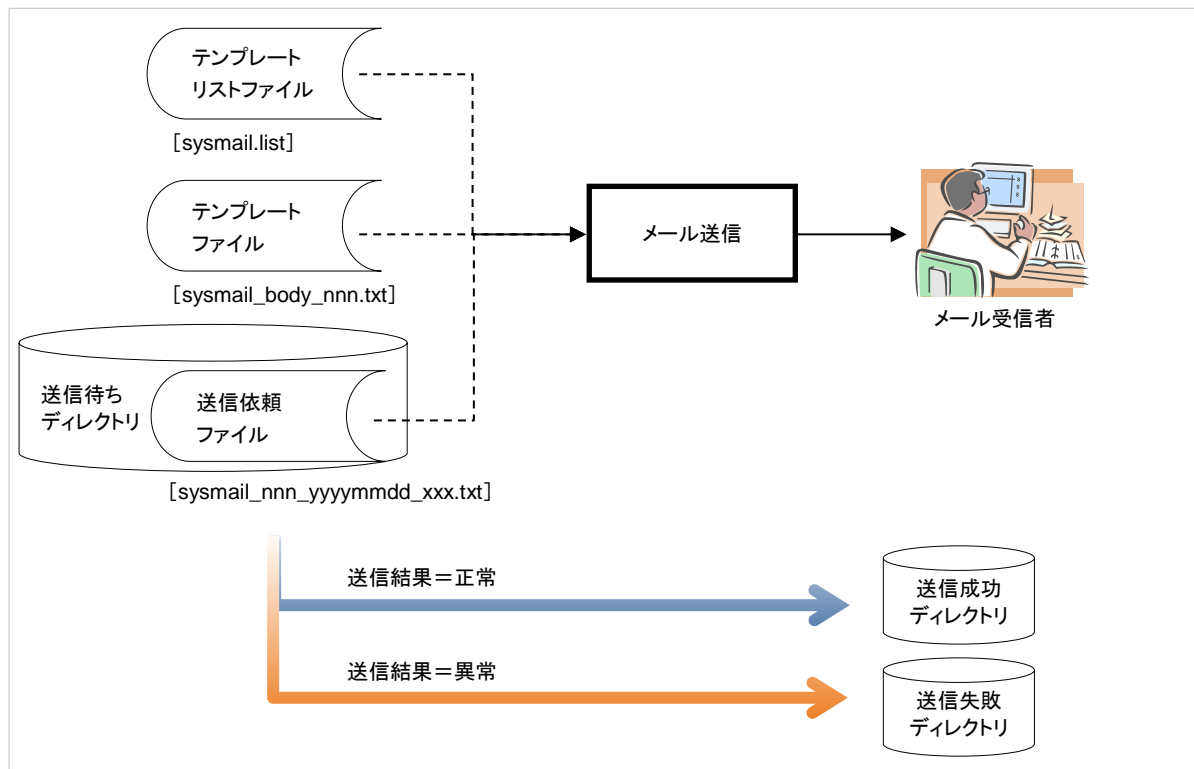


図 1.2-2 メール送信の動作イメージ

#### ④ メール送信までの操作手順

テンプレート ID 決定～送信までの手順を説明します。

ファイルのフォーマットや命名などは、「p29 ①テンプレートリスト ～ p30 ③送信依頼ファイル」を参照してください。

##### 1)テンプレートリストファイルの編集とテンプレート ID の決定

テンプレートリストファイルを編集で開き、テンプレート ID を決定します（重複しない番号）。  
行を追加し、1 列目に決定した ID を記述します。

フリー型、セーフ型の場合で可変の文字列を利用したい場合、置換文字数分を 2 列目に記述します。

送信モードにより、メールアドレスも記述します。

##### 2)テンプレートファイル作成(フリーフォーマット型以外)

メール本文を記述します。

可変部分がある場合、変数で記述します。

※可変部分がない場合、テンプレートファイルは不要です。

##### 3)送信依頼ファイル作成

##### 4)所定ディレクトリへファイル配置

- ・ テンプレートリスト → ~/ita-root/conf/ky\_backyardconf/
- ・ テンプレート → ~/ita-root/conf/ky\_backyardconf/
- ・ 送信依頼ファイル → ~/ita-root/temp/ky\_mail\_queues/ky\_sysmail\_0\_queue/

##### (2) ロール紐付確認＋クリーニング

ロール紐付リスト(ロール・ユーザ／ロール・メニュー)の内容を確認し、ロールとユーザ、ロールとメニューで無効な紐付け関係が存在したら、その情報を消去する処理です。

独立型の常駐プロセスとして動作します。

##### (3) 投入オペレーション確認＋クリーニング

「オペレーション削除管理」メニューの設定に基づいてデータの削除を行います。

##### (4) ファイル確認＋クリーニング

「ファイル削除管理」メニューの設定に基づいてファイルの削除を行います。

##### (5) メニューインポート実行

「メニューインポート」メニューで実行された情報を基に、メニューインポートを実行します。  
実行結果は「エクスポート/インポート管理」メニューで確認できます。

##### (6) メニューインポートクリーニング

メニューインポート実行で使用した一時ファイルを一定期間経過後に削除する。

##### (7) ActiveDirectory 情報ミラーリング

後述の ActiveDirectory 連携機能において、ミラーリング(一方向同期)処理を行います。

※ActiveDirectory 連携機能についての詳細は、「1.4ActiveDirectory 連携機能の利用」をご参照ください。

## 1.3 標準 REST 機能の利用

外部プログラムから REST API を利用して、ITA で管理されているリソースに対し、操作を行うことが可能です。以下に、呼び出し規約を示します。

### 1.3.1 リクエストの形式

ITA の REST API では、ITA 上の各メニューのパスに対して HTTP リクエストを発行します。

パス:

https://<HostName>:<Port>/default/menu/07\_rest\_api\_ver1.php?no=(各メニューのメニューID)  
例) https:// exastroServer:443/default/menu/07\_rest\_api\_ver1.php?no=2100000202

HTTP ヘッダ:

以下の表にあるものが利用可能です。

表 1.3-1 HTTP ヘッダパラメーター一覧

HTTP ヘッダ	説明
Host	ITA の RestAPI サーバーのホスト名または IP アドレスとポート番号をコロン(:)区切りで指定する。
Method	原則:POST、を指定すること。 例外:ITA で認証不要と設定したメニューにアクセスする場合のみ、GET、を指定することが可能。
Content-Type	“application/json”を指定する。 Method が GET の場合は指定しなくてもよい。
Authorization	ITA の認証要メニューにアクセスする場合は、 「ログイン ID」と「パスワード」* を、半角コロン(:)で結合して、base64encode をした値、を指定。 Method が GET の場合は指定しなくてもよい。
X-Command	Method が POST の場合にのみ設定可能。 【INFO】、【FILTER】、【EDIT】のいずれかを設定できる。

HTTP ヘッダの文字列は大文字でも小文字でも問題ありません。

\* ITA のパスワードが期限切れとなっていた場合、RestAPI は Error となります。

Web システムのログイン画面から、パスワードを変更してからリクエストを行ってください。

但し、ActiveDirectory 連携機能を利用している場合は、ActiveDirectory 上で管理される認証情報に従います。(※ActiveDirectory 連携機能の連携対象外ユーザーは、この限りではありません)

**ActiveDirectory 連携機能の詳細は、「1.4ActiveDirectory 連携機能の利用」をご参照ください。**

HTTP ヘッダの例:

ログイン ID が[test\_loginid]で、パスワードが[test\_password]の場合

test\_loginid: test\_password を、base64encode で暗号化

→[qTlmqS9fo2qcozyxBaEyp3EspTSmp3qipzD=]

Host:<HostName>:<Port>

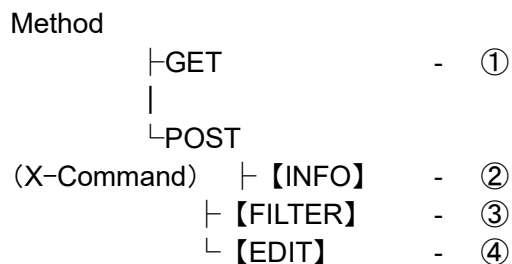
Content-Type:application/json

Authorization: qTlmqS9fo2qcozyxBaEyp3EspTSmp3qipzD=

X-Command: INFO

### 1.3.2 利用可能なメソッドとコマンド

利用可能なメソッドとコマンドの階層は以下のとおりです。



#### ① GET (Method)

列情報(列番号と列名)および、通常ステータス(廃止または活性中)の全レコードの行数とレコード内容を返却します。

・HTTP ヘッダ

表 1.3-2 HTTP ヘッダパラメーター一覧

HTTP ヘッダ	値
Method	GET

・content パラメータ  
なし

・レスポンス

#### 1)レコード行数

(JSON 形式)

キー{resultdata} -> キー{CONTENTS} -> キー{RECORD\_LENGTH}の中に、数値として格納されます。

#### 2)列情報(列番号と列名)

(JSON 形式)

キー{resultdata} -> キー{CONTENTS} -> キー{BODY} -> キー{0}の中に、0 から始まる数値を、キーとする配列として格納されます。

表 1.3-3 レスポンスパラメーター一覧(列情報)

列番号	列名
0	一列目
1	二列目
⋮	⋮

#### 3)レコード情報

(JSON 形式)(1 行につき 1 個の配列(列番号と列別データ))

キー{resultdata} -> キー{CONTENTS} -> キー{BODY} -> キー{(1 以降、該当レコードの存在行数を上限とする数値))の中に、0 から始まる数値をキーとする配列として格納されます。

表 1.3-4 レスポンスパラメーター一覧(レコード情報)

列番号	列データ
0	一列目データ配列
1	二列目データ配列
⋮	⋮

Method: Get でレスポンスされるデータの表と、Json の階層構造を以下に示します。

Json 格納時の階層構造

```

resultdata
└─CONTENTS
  └─RECORD_LENGTH: 3
    └─BODY
      └─0
        │ └─0: A
        │ └─1: I
        │ └─2: U
      └─1
        │ └─0: あ
        │ └─1: い
        │ └─2: う
      └─2
        │ └─0: か
        │ └─1: き
        │ └─2: く
      └─3
        │ └─0: さ
        │ └─1: し
        │ └─2: す

```

表 1.3-1 返されるデータ一覧

	0	1	2
0	A	I	U
1	あ	い	う
2	か	き	く
3	さ	し	す

## ② INFO(X-Command)

列情報のみを取得します。

X-Command(FILTER)または X-Command(EDIT)を実行する際に必要な情報を取得することができます。

・HTTP ヘッダ

表 1.3-2 HTTP ヘッダパラメーター一覧

HTTP ヘッダ	値
Method	POST
X-Command	INFO

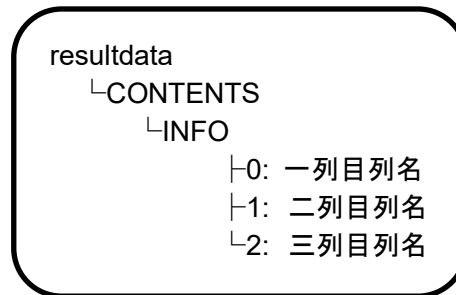
・content パラメータ  
なし

・レスポンス

1)列情報(列番号と列名)

(JSON 形式)

キー{resultdata} -> キー{CONTENTS} -> キー{INFO}の中に、  
0 から始まる数値をキーとする配列として格納されます。



### ③ FILTER(X-Command)

パラメータで指定した条件に合致したレコードの、列情報(列番号と列名)および、  
通常ステータス(廃止または活性中)の全レコードの行数とレコード内容を返却します。

表 1.3-3 HTTP ヘッダパラメーター一覧

HTTP ヘッダ	値
Method	POST
X-Command	FILTER

#### ・content パラメータ

##### 1) フィルタ形式

操作したい Web ページの表示フィルタでフィルタをかけられる列と形式に従い、  
列ごとに以下をフィルタの種類として指定可能です。

- ・NORMAL - 通常の LIKE 検索
- ・RANGE - 1~5 等の範囲検索

また、Web ページの表示フィルタにプルダウンが表示されている列については、  
LIST(複数の完全一致条件による OR 検索。複数条件を配列に格納し指定)設定可能です。

##### 2) 指定形式

JSON 形式で指定。フィルタ種類ごとの形式で、フィルタ条件を格納します。

JSON 形式にする前段階では、1つの連想配列の中に、列番号ごとの連想配列を入れ子にする形で指定します。複数の列番号ごとの連想配列を格納した場合、AND で繋いだ意味になります。

さらに列番号ごとの連想配列の中にフィルタ条件の形式と条件をセットにした連想配列を格納してください。列番号ごとの連想配列に複数のフィルタ条件の連想配列を格納した場合、OR でつないだ意味になります。

## パラメータの記述例

### PHP の場合 例(1)

列番号 2 が列名【項番】(主キーのカラム列)、列番号 4 が【備考】のコンテンツの場合で、  
【項番】が 5 以上かつ、【備考】に「あいう」が入っているレコードを抽出したい場合  
↓ 抽出イメージ

	列番号 1	列番号 2	列番号 3	列番号 4
列名	【列名 1】	【項番】	【列名 3】	【備考】
1	*****	1	*****	あいうえお
2	*****	2	*****	かきくけこ
3	*****	3	*****	あいうえお
4	*****	4	*****	かきくけこ
5	*****	5	*****	かきくけこ
6	*****	6	*****	あいうえお
⋮	⋮	⋮	⋮	⋮

```
$aryFilter = array(2=>array('RANGE'=>array('START'=>'5')),
                  4=>array('NORMAL'=>'あいう')
                );
```

// \$strParaJsonEncoded を Http リクエストの context として ReST へ送信

```
$strParaJsonEncoded = json_encode($aryFilter,
                                   JSON_UNESCAPED_UNICODE | JSON_NUMERIC_CHECK
                                );
```

### PHP の場合 例(2)

列番号 2 が列名【項番】(主キーのカラム列)、のコンテンツの場合で、

【項番】が 10 から 99 の範囲、または、【項番】が 1 または 2 または 5、のレコードを抽出したい場合。

↓ 抽出イメージ

	列番号 1	列番号 2	...
列名	【列名 1】	【項番】	...
1	*****	1	...
2	*****	2	...
3	*****	3	...
4	*****	4	...
5	*****	5	...
⋮	⋮	⋮	...
10	*****	10	...
⋮	⋮	⋮	...
99	*****	99	...
⋮	⋮	⋮	...

```
$aryFilter = array(2=>array('RANGE'=>array('START'=>'10',
                                           'END'=>'99'
                                           ),
                        'LIST'=>array(0=>'1',
                                     1=>'2',
                                     2=>'5'
                                     )
                        )
);
// $strParaJsonEncoded を Http リクエストの context として ReST へ送信
$strParaJsonEncoded = json_encode($aryFilter,
                                   JSON_UNESCAPED_UNICODE | JSON_NUMERIC_CHECK
                                   );
```

### PHP の場合 例(3)

列番号 2 が列名【項番】(主キーのカラム列)、列番号 5 が列名【最終更新日付】(日付型/日時型)のコンテンツの場合で、

【項番】が 1 から 100 で、かつ、【最終更新日付】が 2016 年 8 月 01 日(00:00:00)から 2016 年 12 月 31 日(23:59:59)の範囲のレコードを抽出したい場合

```
$aryFilter = array(2=>array('RANGE'=>array('START'=>'1',
                                           'END'=>'100'
                                           ),
                        5=>array('RANGE'=>array('START'=>'2016/08/01 00:00:00',
                                               'END'=>'2016/12/31 23:59:59'
                                               )
                        )
);
// $strParaJsonEncoded を Http リクエストの context として ReST へ送信
$strParaJsonEncoded = json_encode($aryFilter,
                                   JSON_UNESCAPED_UNICODE | JSON_NUMERIC_CHECK
                                   );
```



## ・レスポンス

### 1)レコード行数

(JSON 形式)

キー{resultdata} -> キー{CONTENTS} -> キー{RECORD\_LENGTH}の中に、数値として格納されます。

### 2)列情報(列番号と列名)

(JSON 形式)

キー{resultdata} -> キー{CONTENTS} -> キー{BODY} -> キー{0}の中に、0 から始まる数値を、キーとする配列として格納される。

表 1.3-4 レスポンスパラメーター一覧(列情報)

列番号	列名
0	一列目
1	二列目
⋮	⋮

### 3)レコード情報

(JSON 形式)(1 行につき 1 個の配列(列番号と列別データ))

キー{resultdata} -> キー{CONTENTS} -> キー{BODY} -> キー{(1 以降、該当レコードの存在行数を上限とする数値))の中に、0 から始まる数値をキーとする配列として格納される。

表 1.3-5 レスポンスパラメーター一覧(レコード情報)

列番号	列データ	説明
0	一列目データ	
1	二列目データ	
⋮	⋮	

※Json 格納時の階層構造は、Method:GET と同様です。

## ④ EDIT(X-Command)

レコードの登録、既存レコードの更新、廃止、復活を行います。

・HTTP ヘッダ

表 1.3-6 HTTP ヘッダパラメーター一覧

HTTP ヘッダ	値
Method	POST
X-Command	EDIT

## ・パラメータ

### 1)指定形式

JSON 形式で指定してください。

INFO で取得できる列情報をもとに、1レコードにつき1つの配列で指定し、1レコードを格納した配列を要素とする配列を、JSON 形式でエンコードしたものを HTTP リクエストの context として送信してください。

列番号 0 の列名【処理種別】には、[登録]、[更新]、[廃止]、[復活]のいずれかを指定してください。

PHP の場合    例(1)    登録
<p>列番号 0 が列名【処理種別】、列番号 1 が【廃止】、列番号 2 が【項番】（主キー役のカラム列）、</p> <p>．．．（中略）．．．</p> <p>列番号 10 が【備考】、列番号 11 が【最終更新日時】、列番号 12 が【更新用の最終更新日時】、列番号 13 が【最終更新者】、のコンテンツの場合に、</p> <p>2 レコードを追加する場合、</p> <pre> \$aryUpdate = array(array(0=&gt;'登録', 1=&gt;"", 2=&gt;"", . . . （中略） . . .                         10=&gt;'1 レコード目の備考欄', 11=&gt;"", 12=&gt;"", 13=&gt;""                     ),                     array(0=&gt;'登録', 2=&gt;"", 2=&gt;"", . . . （中略） . . .                         10=&gt;'2 レコード目の備考欄', 11=&gt;"", 12=&gt;"", 13=&gt;""                     )                 );  // \$strParaJsonEncoded を Http リクエストの context として ReST へ送信 \$strParaJsonEncoded = json_encode(\$aryUpdate,                                    JSON_UNESCAPED_UNICODE   JSON_NUMERIC_CHECK                                 ); </pre>
PHP の場合    例(2)    更新
<p>列番号 0 が列名【処理種別】、列番号 1 が【廃止】、列番号 2 が【項番】（主キー役のカラム列）、</p> <p>．．．（中略）．．．</p> <p>列番号 9 が【備考】、列番号 10 が【最終更新日時】、</p> <p>列番号 11 が【更新用の最終更新日時】、列番号 12 が【最終更新者】、のコンテンツの場合に、</p> <p>【項番】10 のレコードを更新する場合、</p> <pre> \$aryUpdate = array(array(0=&gt;'更新', 1=&gt;"", 2=&gt;"10", . . . （中略） . . .                         9=&gt;'備考欄',                         10=&gt;'2016/08/01 12:30:45',                         11=&gt;'【更新用の最終更新日時】', ※                         12=&gt;'管理者'                     )                 );  // \$strParaJsonEncoded を Http リクエストの context として ReST へ送信 \$strParaJsonEncoded = json_encode(\$aryUpdate,                                    JSON_UNESCAPED_UNICODE   JSON_NUMERIC_CHECK                                 ); </pre>

※Method: GET、X-Command: FILTER で取得した、【更新用の最終更新日時】をセットしてください。このデータによって、追い越し更新を防止しています。  
【更新用の最終更新日時】は、“  ”で始まっています。

・レスポンス

1)各レコードの処理結果

(JSON 形式)

キー{resultdata} -> キー{LIST} -> キー{NORMAL} -> キー{register、update、delete、error}の中に、配列として格納されます。

表 1.3-7 Key パラメーター一覧

key	値の型	
name	文字列	処理結果種類の名前
ct	数値	(処理結果ごとの) レコード件数

2)各レコードの処理結果

(JSON 形式)

キー{resultdata} -> キー{LIST} -> キー{RAW} -> キー{パラメータとして渡したレコード番号(列情報を送信しなくてよい)デフォルト設定では、0、から始まる)}}の中に、0 から始まる数値を、キーとする配列として格納されます。

表 1.3-8 Key パラメーター一覧

key	値の型	
0	文字列	結果コード(別表を参照)
1	文字列	詳細コード(別表を参照)
2	文字列	エラーメッセージ

・結果レスポンス階層表

resultdata

└LIST

└NORMAL

| └register: {name:,ct:}

| └update: {name:,ct:}

| └delete: {name:,ct:}

| └error: {name:,ct:}

|

└RAW

└0: {0:,1:,2:}

└1: {0:,1:,2:}

└2: {0:,1:,2:}

└ .

└ .

└ .

.

.

別表:結果コード／詳細コード 一覧

処理種別	結果コード	詳細コード	説明
登録	000	201	登録の成功。
登録	002	000	必須項目が未入力。
登録	002	000	レコードと重複している項目がある。
登録	002	000	重複禁止に違反しているレコードが存在している。
登録	002	000	入力値の長さが規定のバイト数を超えている。
登録	002	000	入力値[NULL バイト文字等が含まれた値]が不正。
登録	002	000	半角整数以外が入力された。
登録	002	000	値が範囲外。
登録	002	000	入力された値が最小値を下回っているか最大値を上回っている。
登録	002	000	入力条件を満たしていない。
登録	002	000	数値以外が入力された。
登録	002	000	タブと改行が入力された。
登録	002	000	タブが入力された。
登録	002	000	入力値が範囲外。
登録	002	000	入力値が、PHP 関数(checkdate)で正常に処理できる範囲外。
登録	002	000	利用できない値が選択された。
登録	002	000	登録時に指定できない項目(主キー)が指定された。
登録	-	-	メンテナンス権限がない。
更新	000	200	更新の成功。
更新	002	000	必須項目が未入力。
更新	002	000	レコードと重複している項目がある。
更新	002	000	重複禁止に違反しているレコードが存在している。
更新	002	000	入力値の長さが規定のバイト数を超えている。
更新	002	000	入力値[NULL バイト文字等が含まれた値]が不正。
更新	002	000	半角整数以外が入力された。
更新	002	000	値が範囲外。
更新	002	000	入力された値が最小値を下回っているか最大値を上回っている。
更新	002	000	入力条件を満たしていない。
更新	002	000	数値以外が入力された。
更新	002	000	タブと改行が入力された。
更新	002	000	タブが入力された。
更新	002	000	入力値が範囲外。
更新	002	000	入力値が、PHP 関数(checkdate)で正常に処理できる範囲外。
更新	002	000	利用できない値が選択された。
更新	003	000	別セッションからレコードが更新されたため、更新の実行が中止された。
更新	003	000	廃止済レコードへの更新が実行されようとした。
更新	101	000	更新対象の行が特定できなかった。
更新	-	-	メンテナンス権限がない。
廃止	000	210	廃止の成功。
廃止	002	000	入力値の長さが規定のバイト数を超えている。
廃止	002	000	入力値[NULL バイト文字等が含まれた値]が不正。
廃止	002	000	入力された値が最小値を下回っているか最大値を上回っている。
廃止	002	000	入力条件を満たしていない。
廃止	002	000	タブが入力された。

処理種別	結果コード	詳細コード	説明
廃止	003	000	別セッションからレコードが更新されたため、廃止の実行が中止された。
廃止	003	000	廃止済レコードへの廃止が実行されようとした。
廃止	101	000	廃止対象の行が特定できなかった。
廃止	-	-	メンテナンス権限がない。
復活	000	200	復活の成功。
復活	002	000	必須項目が未入力。
復活	002	000	復活の場合、更新できない項目が更新されようとした。
復活	002	000	レコードと重複している項目がある。
復活	002	000	重複禁止に違反しているレコードが存在している。
復活	002	000	入力値の長さが規定のバイト数を超過している。
復活	002	000	入力値[NULL バイト文字等が含まれた値]が不正。
復活	002	000	入力された値が最小値を下回っているか最大値を上回っている。
復活	002	000	入力条件を満たしていない。
復活	002	000	タブが入力された。
復活	003	000	別セッションからレコードが更新されたため、復活の実行が中止された。
復活	003	000	復活済レコードへの復活が実行されようとした。
復活	101	000	復活対象の行が特定できなかった。
復活	-	-	メンテナンス権限がない。
表示	-	-	バリデーションエラー。
表示	-	-	次のいずれか(全レコード,廃止含まず,廃止のみ)が選択されていない。
-	000	000	処理スキップして、次のレコードへ。

## 1.4 ActiveDirectory 連携機能の利用

ActiveDirectory (以下、AD といいます) をご利用されている場合、お使いの AD ドメインを構成するドメインコントローラーと ITA を連携させることができます。

後述の環境要件を満たすだけで、AD 側の設定は何ら変更せずに ITA 側の設定のみで連携を開始できます。

ITA 側の環境構築および設定方法の詳細は、「システム構成／環境構築ガイド\_ActiveDirectory 連携 編」を別紙マニュアルとして用意させて頂いておりますので、そちらをご参照ください。

**※ なお、本節で用いる用語の内、以下の用語は全て以下の意味で用いるものとします。**

- ・(用語) サインイン ID → (意味) AD 上の属性「userPrincipalName」の@より左側の値
- ・(用語) グループ名 → (意味) セキュリティグループの「sAMAccountName」の値

### 1.4.1 利用の開始

#### 【環境要件】

本機能をご利用頂くには、AD 側は以下の要件を満たしている必要があります。

- ・Windows Server 2000 以降である
- ・ITA と連携する AD 上のユーザーには、userPrincipalName の設定がされている

**※ITA では、ログイン認証時のログイン名は「userPrincipalName」のみをサポートしています。**

#### 【AD 連携機能の有効化】

次の2つの条件を満たしている限り、自動で有効になります。

- ① 以下に示す所定のディレクトリに後述の「外部認証設定ファイル」が存在している

(所定ディレクトリ)

- ・~/ita-root/conf/webconfs/

- ② 後述の「外部認証設定ファイル」の内容において、有効な行が少なくとも1行はある

#### 【外部認証設定ファイルの準備】

外部認証設定ファイルの以下①～③について、適切に述する必要があります。

##### ① ファイル名

ファイル名は必ず以下の名前である必要があります。

(ファイル名)

- ・ExternalAuthSettings.ini

##### ② 接続先 DomainController の指定

■セクション:『DomainController\_1 (DomainController\_2) (DomainController\_3)』

- ・host --- 連携先の DomainController の host を指定します。
- ・port --- 上記で指定の DomainController へ接続する際に使用するポートを指定します。

後述の「1.4.2 機能概要」で紹介する機能のいずれにおいても、接続先の DomainController の host および接続に使用する port は上記の設定値を使用します。

### ③ ミラーリング用ユーザーの指定

#### ■セクション『Replication\_Connect』

- ・ConnectionUser --- ミラーリング処理で AD 上の情報を探索する為のユーザーを指定します。
- ・UserPassword --- 上記で使用するユーザーのパスワードを指定します。
- ・basedn --- ドメインのベース dn を指定します。(探索範囲を指定の場合、OU も指定)

ここで指定されたユーザーがミラーリング処理において AD 上の探索を行います。  
その為、ConnectionUser には AD 上の探索権限を持つユーザーを指定する必要があります。

**※注:これらの設定に誤りがある場合でも、外部認証設定ファイルが存在する限り本機能は有効になります。この場合、後述の「連携対象外ユーザー」且つ、同じく後述の「連携対象外ロール」を権限として持つユーザー以外は ITA にログインできなくなります。**

## 1.4.2 機能概要

本機能は、次に挙げる2つの機能を提供します。

### (1) AD 情報ミラーリング機能

AD ユーザーで ITA にログインする為には、ITA 上の「ユーザー管理」および「ロール管理」ならびに「ロール・ユーザ紐付管理」の 3 テーブルに対してもレコードを登録する必要があります。

AD 情報のミラーリング機能は、これらのテーブルに対して後述する所定の AD 情報を基にレコードの自動登録および更新をします。

一度登録されたロールは AD 連携機能が有効である限り常にミラーリング(一方向同期)される為、AD 上で変更した内容は ITA 上の当該レコードにも反映されます。

ミラーリング機能については、「0

## 1.4.3 AD 情報ミラーリング機能

」で詳述します。

### (1) AD 認証(Kerberos 認証)機能

ログイン試行時の認証処理に、連携先 AD の Kerberos 認証機能を利用します。

AD 連携機能が有効である限り、自動的に AD 認証となります。

AD 認証機能については、「1.4.5 AD 認証(Kerberos 認証)」で詳述します。

#### 1.4.4 AD 情報ミラーリング機能

AD 連携機能では、AD 上のユーザーと所属するセキュリティグループの関係を権限として扱います。  
(後述の連携対象外ユーザーを除きます)

ミラーリング機能は、AD 上のユーザーと所属するセキュリティグループの関係を自動的に ITA 上へ反映する機能です。

##### 【登録および更新】

以下のものを所定の AD 情報として ITA 上にミラーリングします。

まだ ITA 上に登録されたことのない AD 情報の場合には「登録」処理を行い、一度でも登録されたことがある AD 情報の場合には「更新」\*1処理を行います。

##### ① AD 上のユーザー情報 → ITA 上の「ユーザー管理」

- ・サインイン ID — ログイン ID
- ・表示名 \*2 — ログイン名
- ・電子メール \*3 — メールアドレス

##### ② AD 上のセキュリティグループ情報 → ITA 上の「ロール管理」

- ・グループ名 — ロール名称

##### ③ AD 上のユーザーが所属するセキュリティグループ情報 → ITA 上の「ロール・ユーザ紐付管理」

- ・「②」の ITA 上に登録されたロール ID と名称 — ロール(ID:名称) \*4
- ・「②」にある「①」の ITA に登録されたユーザ ID と名称 — ユーザ(ユーザ ID:ログイン ID)

※注：OU は権限として扱いません。よって、ITA 上のロール名としても扱われません。

※注：「ロール・メニュー紐付管理」については、手動で設定する必要があります。

ミラーリングされたレコードの最終更新者には「ActiveDirectory ユーザ同期プロシージャ」が設定されます。

このミラーリング処理は、AD 連携機能が有効である限り常に実行されます。  
したがって、ITA 上でレコードの上記①～③を更新しても、AD 情報で再度上書き更新されます。

また、廃止および復活処理についても AD 上の有効／無効の状態に基づきミラーリングをします。  
廃止および復活の詳細については、本項で後述します。

※AD 連携機能を有効にした状態のまま ITA 上でレコードを作成および編集する場合には、  
後述の『特別ユーザー』および『特別ロール』の設定をする必要があります。  
詳細は、「1.4.6 本機能の例外について」をご参照下さい。

\*1 上記①～③の情報に変更がない場合は、更新処理は行われません。

\*2 AD 上で設定されていない場合は、自動的にサインイン ID と同一のものを ITA 上に設定します。

\*3 AD 上で設定されていない場合は、自動的にダミー値を ITA 上に設定します。

\*4 AD 上でユーザーが1人も所属していないグループの場合は、レコードが作成されません。



### 【廃止】

以下の場合、ITA 上の当該レコードが活性中であればミラーリング処理でそれを廃止処理します。

- ・AD 上からユーザーまたはセキュリティグループを削除した
- ・AD 上のユーザーアカウントを無効にした
- ・AD 上でユーザーの「userPrincipalName」を削除した
- ・AD 上でグループのタイプをセキュリティグループから配布グループに変更した

### 【復活】

以下の場合、ITA 上の当該レコードが廃止中であればミラーリング処理でそれを復活処理します。

- ・AD 上から削除されていてユーザーまたはセキュリティグループが復元された <sup>\*5</sup>
- ・AD 上でアカウントが無効にしていたユーザーに対し、再度アカウントを有効化した。
- ・AD 上で「userPrincipalName」が削除していたユーザーに対し、再度「userPrincipalName」設定した
- ・AD 上でグループタイプを配布グループにしていたグループを再度セキュリティグループに変更した。

表 1.4-1 ケース別 廃止／復活処理の区別一覧表

AD 上の情報操作内容	ITA 上のレコード活性状態(ミラーリング処理前)	
	廃止中	活性中
ユーザーまたはグループの削除	何もしない	廃止
ユーザーアカウントの無効	何もしない	廃止
ユーザーuserPrincipanName を削除	何もしない	廃止
グループタイプの変更(セキュリティ → 配布)	何もしない	廃止
ユーザーまたはグループの復元	復活	何もしない
ユーザーアカウントの有効	復活	何もしない
ユーザーuserPrincipanName を再設定	復活	何もしない
グループタイプの変更(配布 → セキュリティ)	復活	何もしない

<sup>5</sup> AD 自体のバックアップを使って復元した場合やサーバーOS のフルバックアップを使って復元した場合など

#### 1.4.5 AD 認証(Kerberos 認証)機能

AD 連携機能が有効である場合にはお使いのドメインに対して Kerberos 認証を行う為、普段 AD 上でお使いのサインイン ID およびパスワードをそのままご利用ください。

但し、以下のものに 1 つでも該当するユーザーは、本機能でログイン頂けません。

- ・連携対象外ユーザー\*<sup>6</sup>（次項で詳述）
- ・AD 上で「Kerberos 事前認証を必要としない」フラグが ON のユーザー
- ・AD 上で「ユーザーは次回ログオン時にパスワード変更が必要」フラグが ON のユーザー
- ・AD 上で「アカウントロック」状態であるユーザー
- ・ITA のログインに、サインイン ID 以外のログオン情報を用いようとしたユーザー
- ・何らかの理由で「ユーザー管理」に登録されていないユーザー
- ・何らかの理由で「ロール・ユーザ紐付管理」に紐付く権限が登録されていないユーザー

また、認証処理そのものは通過した場合でも、「ロール・メニュー紐付管理」でメニューへのアクセス権限を何ら紐付けられていないユーザーは、「不正アクセス画面」に遷移されます。

**※注: AD 連携機能が有効の場合、ITA 上でログインに失敗した場合でも AD 上のロックアウトカウンターにカウントが入ります。(次項で詳述する「連携対象外ユーザー」を除く)**

---

<sup>6</sup> ITA 内部認証(ITA 上で管理されるログイン ID とパスワードに基づく認証)にてログインして下さい。

#### 1.4.6 本機能の例外について

「0」

AD 情報ミラーリング機能」および「1.4.5 AD 認証 (Kerberos 認証) 機能」のいずれにおいても例外があります。

本項では、例外について説明します。

##### (1) 連携対象外レコード

ITA 上で作成した「ユーザー管理」レコード、「ロール管理」レコード、「ロール・ユーザ紐付管理」レコードは、原則としてミラーリング処理の際に自動的に廃止されます。

但し、例外として①～⑤の場合には AD 連携機能の連携対象外扱いとし、廃止されません。

- ④ ITA デフォルト(ユーザーID:1)のシステム管理者ユーザーの「ユーザー管理」レコード
- ⑤ ITA デフォルト(ロール ID:1)のシステム管理者ロールの「ロール管理」レコード
- ⑥ 特別ユーザーに指定されている「ユーザー管理」レコード
- ⑦ 特別ロールに指定されている「ロール管理」レコード
- ⑧ ユーザーまたはロールのどちらか一方でも特別指定されている「ロール・ユーザ紐付管理」レコード

なお、AD ユーザーのサインイン ID が 連携対象外ユーザー <sup>\*7</sup> のログイン ID と重複した場合は、当該の AD ユーザーの情報は ITA 上にミラーリングされません。

同様に、AD 上のグループ名が 連携対象外ロール <sup>\*8</sup> のロール名と重複した場合は、当該のグループ名は ITA 上にミラーリングされません。

**※特別ユーザーおよび特別ロールについては、外部認証設定ファイルで設定可能です。**

なお、機能の性質上、特別ユーザーおよび特別ロールの設定には AD からミラーリングしたレコードも指定できますが、推奨はされません。

特別ユーザーおよび特別ロールの設定機能は、あくまでも ITA 上で作成したレコードをミラーリング処理の対象から除外した場合にのみ利用されることを想定して提供しています。

**※AD からミラーリングしたレコードを特別ユーザーおよび特別ロールに設定した場合は、廃止がされないだけでなく、更新および復活もされなくなります。**

##### (2) AD 認証対象外 (ITA 内部認証)

連携対象外ユーザーは、AD 連携機能が有効中であつたとしても、常に ITA 上で管理されるログイン ID とパスワードに基づいて認証処理が行われます。(ITA 内部認証)

**※元々は AD からミラーリングされたユーザーであっても特別ユーザーに指定した場合は、ITA 内部認証となります。**

<sup>\*7</sup> 上記①③を合わせたユーザー

<sup>\*8</sup> 上記②④を合わせたロール

## 2 運用操作

ITA システムに対する操作は、ユーザーによるブラウザ画面からの入力だけではなく、ssh コンソールや FTP ソフトを使ったシステム運用・保守による操作もあります。運用・保守の操作対象は次のとおりです。

- インストール関連
- オペレーション作業履歴の定期削除
- ログレベルの変更
- メンテナンス

### 2.1 インストールの開始

インストール時の事後作業については、別マニュアル「インストールマニュアル」の 3 項動作確認をご参照ください。

### 2.2 オペレーション作業履歴の定期削除

投入オペレーション一覧に登録されているオペレーションで、実施日が設定されているオペレーションに紐づく作業履歴は、指定した保存期間を過ぎると削除されます。(廃止扱いとされます。)

作業履歴には以下のものがあります。

- ・ITA - Symphony で管理している情報
- ・各オーケストレータのドライバー - Ansible driver で管理している情報

保存期間は以下のファイルによって指定できます。

```
・ITA
~/ita-root/conf/yardconf/ita_base/keep_day_length.txt
・Ansible
~/ita-root/conf/yardconf/ansible_driver/keep_day_length.txt
・ドライバー共通
~/ita-root/conf/yardconf/ita_base/dataautoclean_conf.txt
```

この機能は、Cron に登録されている日時処理によって作動します。

Cron には、コマンド{ `crontab -e` } により以下の行が登録されており、実行時間を指定することができます。

・ITA

```
mm hh * * * su - -c '/exastro/ita-root/backyards/ita_base/ky_std_symphony-dataautoclean.sh'
```

・Ansible

```
mm hh * * * su - -c '/exastro/ita-root/backyards/ansible_driver/ky_ansible_dataautoclean-workflow.sh'
```

・ドライバー共通

```
mm hh * * * su - -c '/exastro/ita-root/backyardconfs/commn/ky_execinstance_dataautoclean-workflow.sh  
confs/backyardconfs/ita_base/dataautoclean_conf.txt'
```

mm:起動する時間(分)

hh:起動する時間(時)

## 2.3 ログレベルの変更

ITA システム 独立型プロセスのログレベルの変更方法は次のとおりです。

### ■ 対象ファイル

~/ita-root/backyards/webdbcore/ky\_mail  
~/ita-root/backyards/webdbcore/ky\_std\_checkcondition-linklist  
~/ita-root/backyards/ita\_base/ky\_std\_symphony-dataautoclean.sh  
~/ita-root/backyardconfs/commn/ky\_execinstance\_dataautoclean-workflow.sh

#### ① NORMAL レベル

「LOG\_LEVEL='NORMAL'」を有効にします。

```
# ログ出力レベル
#  DEBUG : 解析レベルでログ出力
#  NORMAL : クリティカルな場合のみログ出力
#LOG_LEVEL='DEBUG'
LOG_LEVEL='NORMAL'
```

#### ② DEBUG レベル

「LOG\_LEVEL='DEBUG'」を有効にします。

```
# ログ出力レベル
#  DEBUG : 解析レベルでログ出力
#  NORMAL : クリティカルな場合のみログ出力
LOG_LEVEL='DEBUG'
#LOG_LEVEL='NORMAL'
```

※ ログレベル変更は、プロセス再起動(Restart)後に有効になります。(「[2.4 メンテナンス](#)」参照)

## 2.4 メンテナンス

### 2.4.1 ITA システム 独立型プロセスの起動/停止/再起動

メール送信機能を例示します。

ロール紐付確認＋クリーニングの場合は、「ky\_mail」を「ky\_std\_checkcondition-linklist」に読み替えてください。

#### ① プロセス起動

```
$ service ky_mail start ↵
```

#### ② プロセス停止

```
$ service ky_mail stop ↵
```

#### ③ プロセス再起動

```
$ service ky_mail restart ↵
```

## 3 Appendix

### 3.1 トラブルシューティング

No	内容
Q-1	表示の動作が重くなる 大型サイズのファイルダウンロードに時間かかりすぎる 処理がタイムアウトになる PHP スクリプトが強制終了する
A-1	PHP のメモリ設定が足りないことが考えられます。 PHP 設定ファイル「php.ini」内の次のパラメータの値を見直して、割り当て可能な最大値を設定してください。  ・memory_limit                  PHP に割り当て可能なメモリ  ファイルのアップロードで同様な事象も発生する可能性があるため、次のパラメータ値の見直しもあわせて行ってください。  ・post_max_size                  post データに許可される最大サイズ ・upload_max_filesize          ファイルあたりの最大サイズ
Q-2	「ita-root」(ITA システムのルートディレクトリ)の作成の注意点を教えてください。
A-2	ディレクトリ位置は、「絶対パス」と、ブラウザで指定する「ファイル名」の 2 つを合わせて 1,024 文字以内で収まるように配慮してください。 全体のパス名が長い場合、サーバーの動作に悪影響(遅い／フリーズ)を与える可能性があります。
Q-3	ITA システムでは Web 画面上の「表示フィルター」サブメニューでキーワード検索や曖昧検索が可能です。RDBMS が <b>Oracle の場合</b> 、ワイルドカード記号(たとえば"*"、や"#") <b>のみを指定する曖昧検索は期待とおりの結果が得られないことがあります。</b>
A-3	Oracle で記号の曖昧検索を行いたい場合、記号の前後に文字列をあわせて入力・検索を行ってください。 (例) × : 「*」 ○ : 「あ*」、「い*は」など
Q-4	アカウントロックされてログイン出来ない場合



No	内容
A-4	<p>ログインを何回か失敗するとアカウントがロックされます。 ロックがかかる失敗回数は「システム設定」内のパラメータの設定によって変更します。</p> <p>・PWL_THRESHOLD パスワード誤り閾値(回数)</p> <p>またアカウントロックの継続期間も「システム設定」内のパラメータの設定によって変更可能です。</p> <p>・PWL_EXPIRY アカウントロック継続期間(秒)</p> <p>※パラメータ「PWL_EXPIRY」の値をゼロ(0)にすると、ログインを何回失敗してもロックは掛かりません。</p>
Q-5	AD 連携機能で、外部認証設定ファイルに複数の DomainController の設定する時に、異なるドメインの DomainController を設定できますか。
A-5	<p>設定できません。</p> <p>ITA では AD 連携時に内部処理として AD のドメイン一意キーである SID を取得しています。異なるドメイン間では SID が重複する可能性がある為、異なるドメインの DomainController を設定した場合には ITA 側に AD 情報を同期できなくなります。</p>
Q-6	一度 ITA と連携した AD ドメインを再構築したところ、AD 連携ができなくなりました。
A-6	<p>再構築した場合(バックアップした場合も含む)は、内部処理で取得した SID が ITA 上の DB 内で重複する場合があります。 重複が発生した時点で、AD 連携機能の処理が正しく行われなくなります。</p> <p>一度 ITA と連携した AD ドメインを再構築後に再度 ITA と連携した場合は、お手数ですが ITA そのものも再構築してください。</p>
Q-7	一度 AD 連携を有効にしたものの、不要になったので無効にしました。しかし、ミラーリング処理で ITA 上に登録されたユーザー・レコードならびにロール・レコードが廃止されません。
A-7	<p>仕様となります。</p> <p>お手数ですが、画面上から手動で廃止して頂くか、ファイルアップロード機能を利用頂いて一括廃止するなどして下さい。</p>
Q-8	ITA 上にミラーリングされている AD ユーザーなのにも関わらず、ITA にログインできないユーザーがいます。
A-8	<p>ITA 上にミラーリングされている AD ユーザーだったとしても、外部認証設定ファイルに記述された内容で以下の①と②に相違があり且つ①で指定された範囲外のユーザーはログインできません。</p> <p>①『DomainController_1(DomainController_2)(DomainController_3)』の【basedn】 ②『Replication_Connect』の【basedn】</p> <p>詳細は、「システム構成／環境構築ガイド_ActiveDirectory 連携編」をご参照ください)</p>
Q-9	OU で探索範囲を指定する時に、複数の OU を指定することはできますか。

No	内容
A-9	<p>できません。</p> <p>複数の OU を指定されたい場合には、それら上位となるレイヤーに OU を更に作成して頂き、その上位の OU を探索範囲として指定してください。</p>
Q-10	Azure ActiveDirectory(以下、Azure AD と言います)に対して ITA の AD 連携機能を使うことはできますか。
A-10	できません。
Q-11	「Azure AD Connect」で Azure AD と同期している AD に対して ITA の AD 連携機能を使っている時、Azure AD で作成および編集したグループのグループ名が ITA 上のロール名に反映されない時があります。
A-11	<p>AD 連携機能において取得するグループ名称は、グループの sAMAccountName です。</p> <p>AD の製品仕様として、Azure AD 上で作成および編集したグループ名が必ずしも AD の sAMAccountName に反映されるわけではない為、反映されなかった場合には ITA 上のロール名にも反映されません。</p> <p>※AD の詳細な仕様については Microsoft 社のサポートおよび公式ドキュメント等をご参照ください。</p>