ITA_システム構成/環境構築ガイド

ActiveDirectory連携編

ー第1.2版 ー

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写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。
- Oracle、MySQLは、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。
- MariaDBは、MariaDB 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

はじめに

本書では、ITA で ActiveDirectory 連携（以下、「AD 連携」）機能を
利用頂く為に必要なシステム構成と環境構築について説明します。

AD 連携機能を利用するにあたっては、ITA 基本機能が構築済であることが前提です。ITA 基本機能の構築に関しては、「システム構成／環境構築ガイド_基本編」をご覧ください。

1 機能

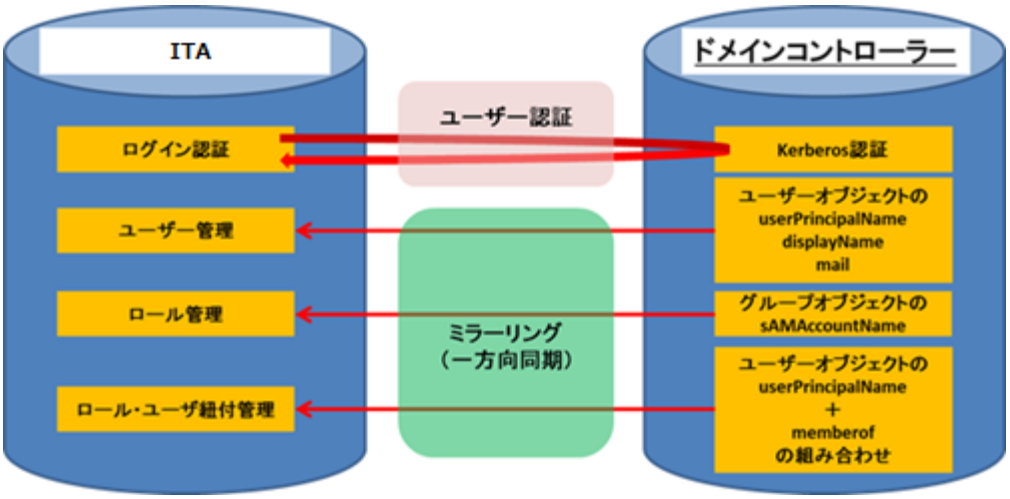
AD 連携機能は、以下の機能を提供します。

表 1-1 機能名

No	機能名	用途	WEB コンテンツ	BackYard コンテンツ
1	AD 認証(kerberos 認証機能)機能	ITA から AD に対して AD 認証（Kerberos 認証） を行います。	○	
2	ミラーリング機能	AD 上のユーザー情報およびグループ情報を 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」にミラーリングを します。（一方向同期）		○

2　システム構成

AD 連携機能は、組織でお使いのドメインを構成するドメインコントローラーと連携します。



※ userPrincipalName … ActiveDirectory 上のログイン ID
※ displayName … 表示名
※ sAMAccountName … オブジェクト名（上図では、グループオブジェクトの名称）
※ memberof … ユーザーが所属するグループ名

3 システム要件

AD 連携機能は、ITA システムのシステム要件に準拠するため、「システム構成／環境構築ガイド_基本編」を
参照してください。ここでは Backyard の要件を記載します。

●BackYard

表 3-1　表 AD 連携機能 Backyard システム要件

パッケージ	バージョン	注意事項
PHP	5.6	

表 3-2　表 AD 連携機能 必要外部モジュール

外部ﾓｼﾞｭｰﾙ	バージョン	注意事項
PEAR	1.10.3	

4　外部認証設定ファイルの準備

4.1　外部認証設定ファイルについて

ITA では、以下の2つの条件を満たしている場合に、自動的に AD 連携機能が有効になります。
①所定のディレクトリに外部認証設定ファイルが存在する
②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

AD 連携機能を有効にするには、所定のディレクトリに外部認証設定ファイルを配備する必要があります。
詳細は、 4.2 外部認証設定ファイルの配備をご参照ください。

また、外部認証設定ファイルの記述方法についても所定の形式が決まっています。
所定の形式以外で記述されている場合はエラーになります。

詳細は、 4.3 外部認証設定ファイルの記述をご参照ください。

4.2　外部認証設定ファイルの配備

ファイル名と配備先のディレクトリは下記のとおりにしてください。

■ファイル名
・ExternalAuthSettings.ini

■配備先のディレクトリ
・~/ita-root/confs/webconfs/

4.3 外部認証設定ファイルの記述

外部認証設定ファイルには、「セクション」「キー」設定項目として記述します。

以下は設定例です。
各セクションおよび各キーの詳細は表 4.3-1 ExternalAuthSetting.ini 設定値 早見表をご参照ください。

```
[Authentication_method]
AuthMode = 1

[Replication_Connect]
ConnectionUser = "Administrator"
UserPassword = "Password"
basedn = " ou=hogeUsers , dc= hoge,dc=local"

[DomainController_1]
host = ldap://127.0.0.1
port = 389
basedn = "ou=hogeUsers , dc=hoge , dc=local"
reconnection_count = 3
connect_protocolversion = 3
connect_timelimit = 30
search_timelimit = 30

[LocalAuthUserId]
IdList = "6 ,12"

[LocalRoleId]
IdList = "3 , 23"
```

各セクションおよび各キーについては下記の表をご参照ください。

※ connect_protocolversion 以外は全て必須の要素となります。

表 4.3-1 ExternalAuthSetting.ini 設定値 早見表

セクション	キー	説明
Authentication_method	AuthMode	認証方式を設定します。 ITA では通常「1」を設定してください。
Replication_Connect	ConnectionUser	ミラーリング機能において、AD 上の情報を探索する為の AD ユーザーを指定します。 ミラーリング対象の全ての AD 情報を探索できる権限を 持つユーザーを指定して下さい。
	UserPassword	「ConnectionUser」要素で指定した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。 記述法について「LDAP 識別名の記述ルール」に基づきます。 ドメイン名を構成する DC は指定必須となります。 探索範囲の指定については、任意で OU のみ指定可能です。 **※ITA では、OU 以外で探索範囲は指定できません。**
DomainController_1 *1	host	連携する AD を構成する DomainController のホスト を指定します。
	port	連携する AD を構成する DomainController のポート を指定します。
	basedn	※ Replication_Connect の場合と同様の内容を指定
	reconnection_count	通信不調でサーバーとの接続に失敗した場合に、 自動的に再接続を試行する回数を指定します。 指定された回数内に接続できなかった場合、ログイン画面上に エラーメッセージを返します。
	connect_protocolversion	LDAP バージョンを指定できます。 **※指定がない場合は、「3」で処理を実行します。**
	connect_timelimit	DomainController への接続待機時間を指定します。 指定された時間内に接続できなかった場合、失敗となります。
	search_timelimit	AD における Kerberos 認証処理の待機時間を指定します。 指定された時間内に認証できなかった場合、失敗となります。
LocalAuthUserId	IdList	ITA 上のユーザーの内、AD 連携の対象外とするユーザーを 指定できます。**（※ITA のユーザーID で指定します。）** カンマ区切りで複数指定することができます。
LocalRoleId	IdList	ITA 上のロールの内、AD 連携の対象外とするロールを 指定できます。**（※ITA のロール ID で指定します。）** カンマ区切りで複数指定することができます。

*1 DomainController は最大で 3 つまで指定できます。その場合は、「DomainController_2」ならびに「DomainController_3」としてセクションを追記してください。キーは「DomainController_1」と同一です。
複数指定した場合は、各 DomainController に対して順番に処理を行いますが、成功した段階で次の DomainController に対しては処理を行いません。

- **ドメインが異なる DomainController を指定することはできません。**