



SG3600LM, SG3600LG, SG3600LJ

V8. 2, V8. 3

LDAP 連携機能説明書

2019 年 10 月 第 2 版

目次

1章	概要	1
1.1.	機能概要	1
1.2.	LDAP連携機能を利用する条件	1
1.3.	用語	2
2章	LDAP連携設定	3
2.1.	ログオンスクリプトの配置	5
2.2.	自己署名証明書の作成	7
2.3.	LDAP識別名の登録	8
2.4.	LDAP(SG)ユーザの登録	9
2.5.	LDAPグループの作成	10
2.6.	所属LDAP(SG)ユーザの設定	12
2.7.	LDAPルールの設定	14
2.8.	LDAP連携利用の設定	19
3章	注意事項	20

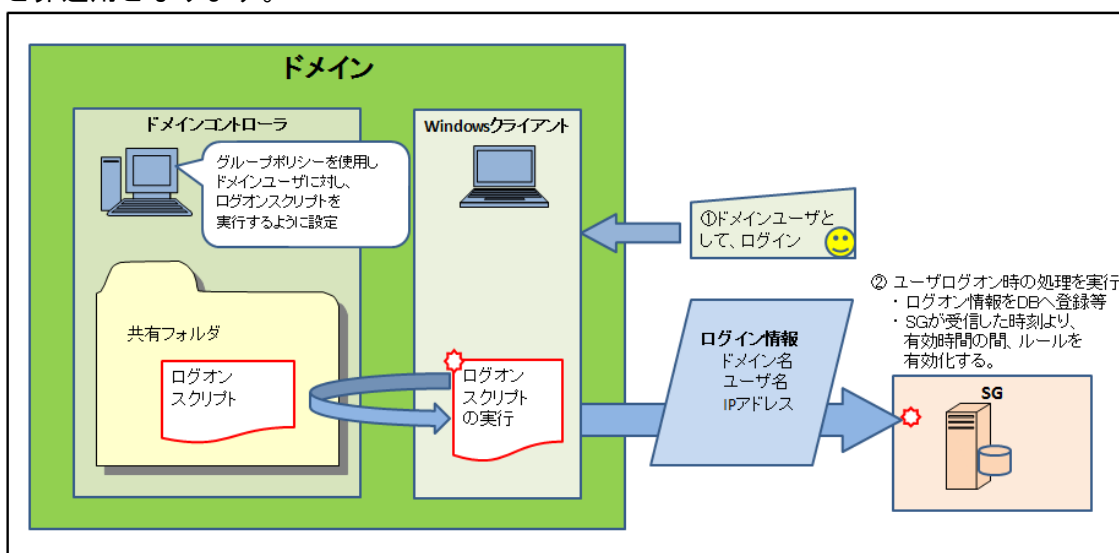
1章 概要

本章では、SG で LDAP 連携機能を利用する場合の動作や条件について説明します。

1.1. 機能概要

LDAP連携機能を利用すると、LDAPサーバに登録されたユーザ名でファイアウォールを利用することができますようになります。

SGにLDAPサーバの識別子を登録することで、LDAPサーバからユーザ名の一覧を取得できるようになります。このユーザ名の一覧からユーザを選択することでSGへ登録できます。ユーザがログインすると、SGへ「ログインしたユーザ名」と「ログインしたPCのIPアドレス」を通知します。SGは、通知されたユーザ名に紐付くルールを適用します。このルールは、通知されたIPアドレスが発信元となる通信に対して有効となり、有効時間を経過すると非適用となります。



1.2. LDAP連携機能を利用する条件

SG で LDAP 連携機能を利用する場合、次の条件を満たしている必要があります。

- Windows Server 2012もしくはWindows Server 2012 R2でドメインを構築し、Active Directoryでユーザを管理していること
- ユーザがログインするPCは、Windows Server 2012、Windows Server 2012 R2、Windows 7、Windows 8、Windows 8.1、Windows Vistaのいずれかであること
- SG-LDAPサーバ間および、SG-ユーザがログインしたPC間が通信可能であること

※ Windows、Windows Server 2012、Windows Server 2012R2、Windows 7、Windows 8、Windows 8.1およびWindows Vista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。

1.3. 用語

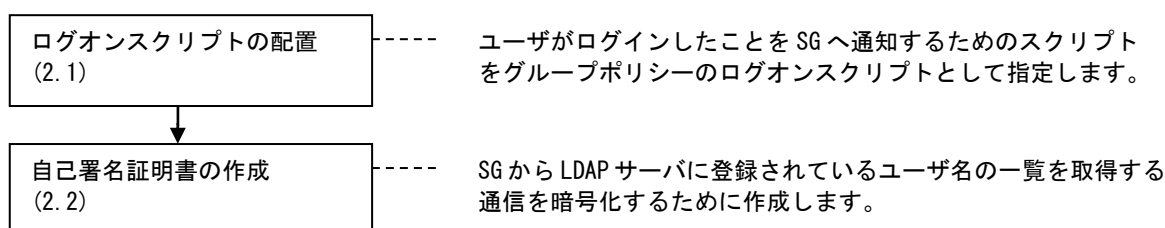
用語	意味
LDAP サーバ	本書においては、ドメインコントローラかつ Active Directory でユーザを管理しているサーバを指します。
LDAP 識別名	SG 上で使用する用語となります。 Active Directory 上のユーザやコンピュータを格納するオブジェクト。デフォルトで設定されている Users や組織単位 (ou) を指します。
LDAP (SG) ユーザ	SG 上で使用する用語となります。 LDAP サーバに登録されているユーザの中で、SG に登録しているユーザを指します。
所属 LDAP (SG) ユーザ	SG 上で使用する用語となります。 LDAP グループに所属している LDAP (SG) ユーザを指します。

2章 LDAP連携設定

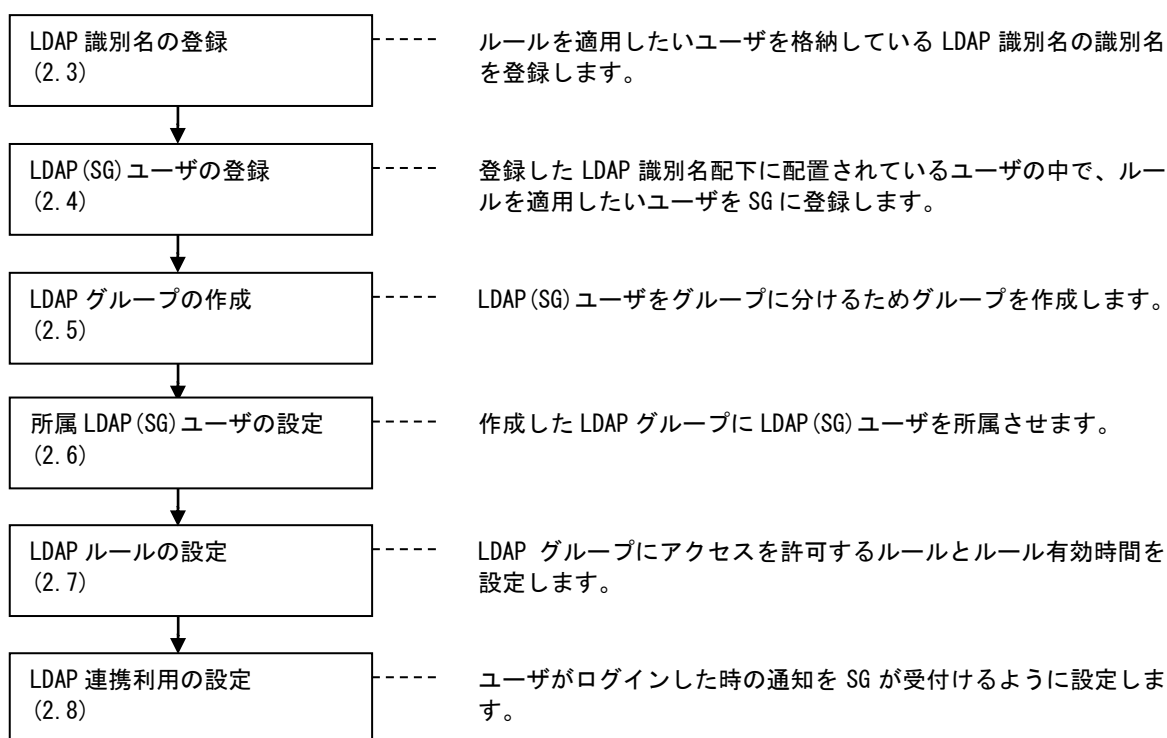
本章では、SG で LDAP 連携機能を利用するための手順について説明します。

LDAP サーバ側と SG 側のそれぞれの主な設定の流れは以下のとおりです。

LDAP サーバ側



SG 側



これ以降は、以下のようなケースを想定し、設定する手順を説明します。お客様環境にあわせて適宜読み替えてください。

【目的】

情報システム課の全ての職員は、情報システムサーバとインターネットに接続できるようにします。ただし、管理職員のみ人事サーバにも接続できるようにします。

【LDAP】

LDAP は以下の状態を想定とします。

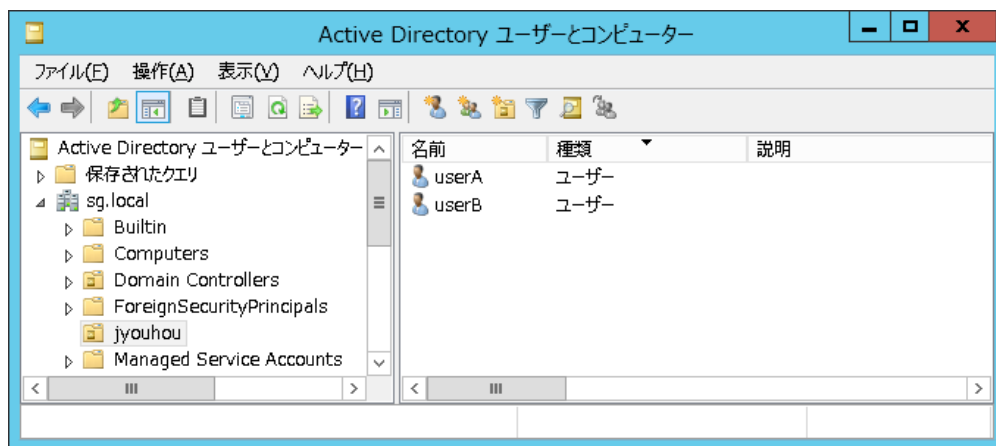
ルートドメイン : sg.local

情報システム課 (ou)

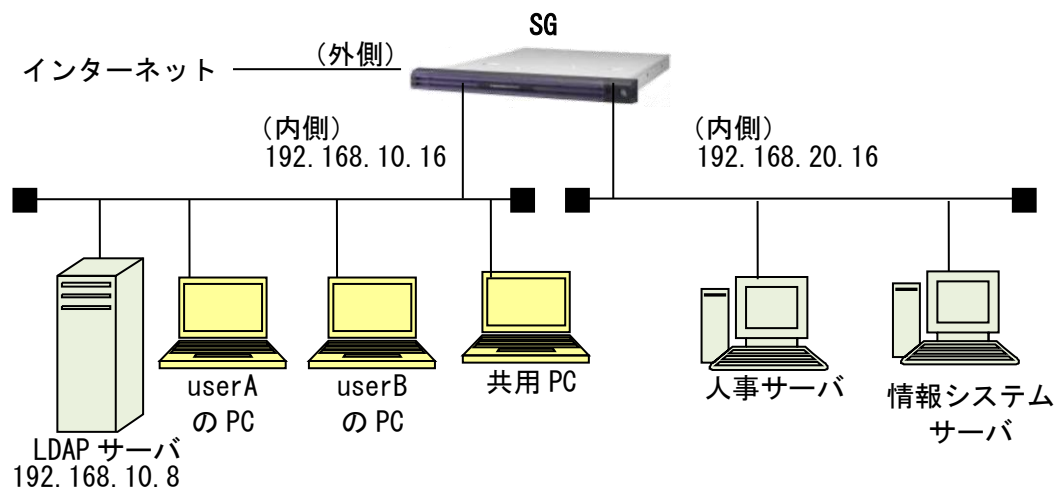
識別名 : ou=jyouhou,dc=sg,dc=local

所属するユーザ名 : userA、userB

userA は管理職員、userB は一般職員とします。



【機器の配置】



2.1. ログオンスクリプトの配置

SG でユーザのログインを検知できるように、ログイン情報をログインした PC から暗号化して送信するため に LDAP サーバの共有フォルダに、ログオンスクリプトとして、「SGLogonScript.vbs」と「GetLogonInfo.exe」を格納します。共有フォルダは、ログインする PC からアクセス可能である必要があります。

ログオンスクリプトを格納後に、送信先の SG の IP アドレス部分を変更します。ポート番号部分は

LDAP 連携利用の設定 で設定したポートになります。ログイン情報を取得する GetLogonInfo.exe のパスを格納したフォルダ名に変更します。本ケースの場合は以下のように変更します。

(SGLogonScript.vbs)

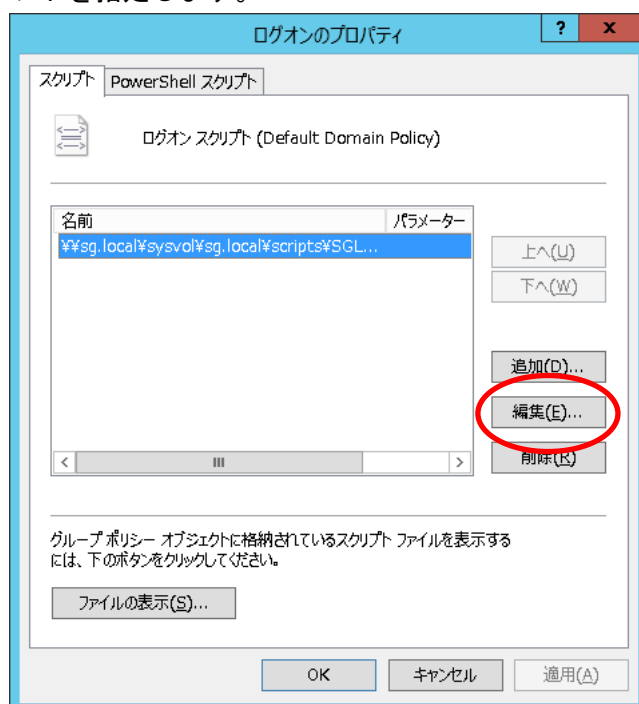
```
strURL = "https://192.168.10.16:453/ldap/"
```

IP アドレス ポート番号

```
strCmd = "%sg.local%sysvol%sg.local%scripts%GetLogonInfo.exe"
```

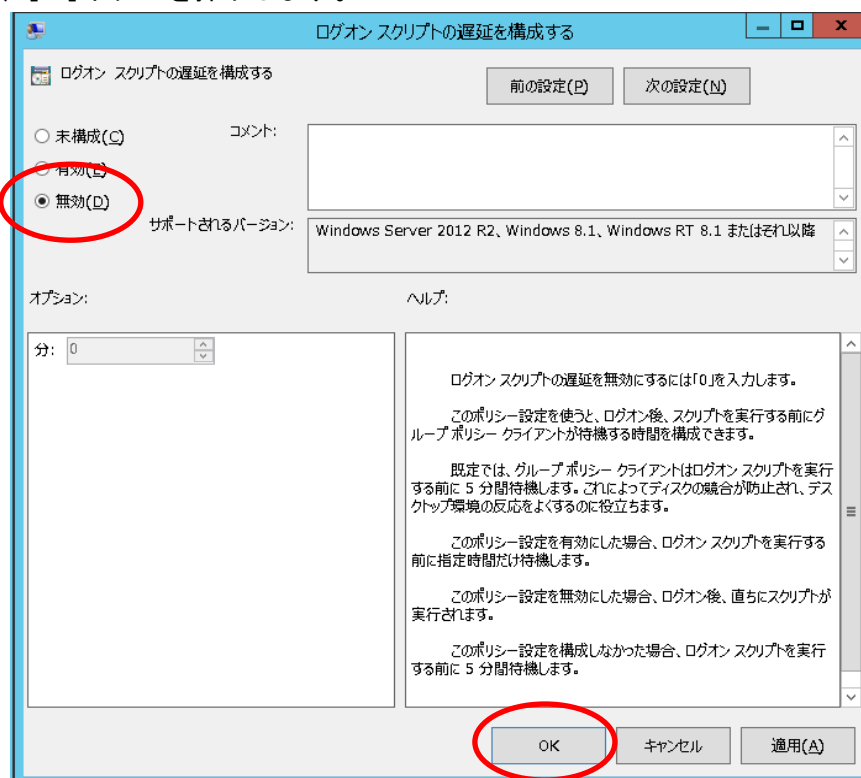
GetLogonInfo.exe を格納したフォルダ名

LDAP サーバでグループポリシー管理を開き、ドメイン名配下の[Default Domain Policy]を右クリックし[編集]を選択し、グループポリシー管理エディターを開きます。画面左側の[ユーザの構成][ポリシー][Windows の設定][スクリプト (ログオン/ログオフ)]を順に選択し、画面中央の[ログオン]をダブルクリックし[ログオンのプロパティ]画面を開きます。[追加]ボタンを押下し、表示される画面の[参照]ボタンを押下し、格納したログオンスクリプトを指定します。



LDAP サーバが Windows Server 2012 R2 の場合、ログオンスクリプトの実行のタイミングがログインから 5 分後となる設定がデフォルトとなっています。実行タイミングをログイン時にするためには以下の設定を行います。

LDAP サーバでグループポリシー管理エディターを開き、画面左側の[コンピュータの構成][ポリシー][管理テンプレート][システム][グループポリシー]を順に選択し、[ログオンスクリプトの遅延を構成する]をダブルクリックします。表示された画面で、[無効]を選択し、[OK]ボタンを押下します。



LDAP サーバが Windows Server 2012 の場合且つログインする PC が Windows 8.1 または Windows Server 2012R2 の場合、ログオンスクリプトの実行のタイミングがログインから 5 分後となる設定がデフォルトとなっています。実行タイミングをログイン時にする為にはログインする PC で上記と同様の設定を行います。

2.2. 自己署名証明書の作成

SG が LDAP サーバのユーザ名の一覧を取得する時に、暗号化して受信するために LDAP サーバに自己署名証明書が必要となります。既に LDAP サーバに自己署名証明書がある場合は、あらたに自己署名証明書を作成する必要はありません。

インターネットインフォメーションサービス (IIS) マネージャーを開き、画面左側に表示されている LDAP サーバ名を選択します。画面中央に表示される機能の[サーバー証明書]をダブルクリックします。画面右側に表示されている[自己署名入り証明書を作成...]をクリックします。

[自己署名入り証明書の作成] 画面の各項目を入力し[OK]ボタンを押下します。フレンドリ名は任意、証明書ストアは[個人]を選択します。

2.3. LDAP識別名の登録

ルールを適用したいユーザが配置されている LDAP 識別名を SG に登録します。

登録後に LDAP 識別名は更新できません。更新したい場合は、LDAP 識別名を削除後に登録する必要があります。LDAP 識別名を削除すると、LDAP 識別名に紐づく LDAP (SG) ユーザ情報、LDAP グループ情報および LDAP グループルールが削除されます。

- (1) [ファイアウォール] > [詳細設定] > [LDAP 連携設定] > [LDAP 識別名 新規] 画面の各項目を入力後、[登録] ボタンを押下します。各項目の詳細は、表 1 LDAP 識別名 設定項目一覧 を参照ください。

LDAP識別名 新規

[ファイアウォール](#) > [詳細設定](#) > [LDAP連携設定](#) > LDAP識別名 新規

[ヘルプ](#)

LDAP識別名	
LDAP識別名	ou=jyouhou,dc=sg,dc=local
ホスト名	192.168.10.8
サーバポート	636
バインドユーザ名	Administrator
パスワード	●●●●●●●●
再パスワード	●●●●●●●●
コメント(改行不可)	情報システム課

登録

表 1 LDAP識別名 設定項目一覧

項目名	設定内容
* LDAP 識別名	ルールを適用したいユーザが配置されている LDAP 識別名を識別名の表記方法で入力します。本ケースでは「ou=jyouhou,dc=sg,dc=local」のように入力します。
* ホスト名	LDAP サーバの名前もしくは IP アドレスを入力します。
* サーバポート	LDAP サーバからユーザー一覧を取得するポート番号は 636 となります。設定の変更はできません。
* バインドユーザ名	LDAP サーバにログイン可能なユーザ名を入力します。
* パスワード	バインドユーザ名で入力したユーザ名のパスワードを入力します。
* 再パスワード	バインドユーザ名で入力したユーザ名のパスワードをもう一度入力します。
コメント(改行不可)	LDAP 識別名に関するコメントを入力します。

※ 各項目先頭のアスタリスク（*）は必須項目

2. 4. LDAP(SG)ユーザの登録

ルールを適用したいLDAP上のユーザをSGに登録します。
本ケースでは、userA（管理職員）とuserB（一般職員）に登録します。

- (1) [ファイアウォール] > [詳細設定] > [LDAP 連携設定] 画面の[LDAP (SG) ユーザ]アイコンをクリックします。



LDAP連携設定

[ファイアウォール](#) > [詳細設定](#) > LDAP連携設定

[\[ヘルプ\]](#)

LDAP識別名、LDAP(SG)ユーザ、LDAPグループの順に設定を行ってください。

LDAP識別名を
選択したLDAP識別名を

LDAP識別名	コメント	LDAP(SG)ユーザ	LDAPグループ
<input type="checkbox"/> ou=jyouhou,dc=sg,dc=local	情報システム課		

☐ 全選択/解除

- (2) [LDAP (SG) ユーザ設定] 画面に表示されているLDAPに登録されているユーザでSGに登録したいユーザをチェックし、[設定]ボタンを押下します。

LDAP(SG)ユーザ設定

[ファイアウォール](#) > [詳細設定](#) > [LDAP連携設定](#) > LDAP(SG)ユーザ設定

[\[ヘルプ\]](#)

LDAP識別名: ou=jyouhou,dc=sg,dc=local

LDAPサーバ登録ユーザの中から、LDAP(SG)ユーザとして登録したいユーザをチェックしてください。(サポート対象外の文字についてはヘルプを参照。)

LDAPサーバ登録ユーザ	フィルタ
<input checked="" type="checkbox"/> userA	ou=jyouhou
<input checked="" type="checkbox"/> userB	ou=jyouhou

☐ 全選択/解除

2.5. LDAPグループの作成

LDAP (SG) ユーザをグループに分けるためのグループを登録します。

本ケースでは、情報システム課の全職員用のグループと管理職員用の 2 つのグループを作成します。それぞれ LDAP グループ名は、「情報システム課（全職員用）」、「情報システム課（管理職用）」とします。ここでは、全職員用のグループの作成を説明します。

- (1) [ファイアウォール] > [詳細設定] > [LDAP 連携設定] 画面の [LDAP グループ] アイコンをクリックします。

LDAP連携設定

[ファイアウォール](#) > [詳細設定](#) > LDAP連携設定

[ヘルプ](#)

LDAP識別名、LDAP(SG)ユーザ、LDAPグループの順に設定を行ってください。

LDAP識別名を

選択したLDAP識別名を

LDAP識別名	コメント	LDAP(SG)ユーザ	LDAPグループ
<input type="checkbox"/> ou=jyouhou,dc=sg,dc=local	情報システム課		

☐ 全選択/解除

- (2) [追加] ボタンを押下します。

LDAPグループ設定

[ファイアウォール](#) > [詳細設定](#) > [LDAP連携設定](#) > LDAPグループ設定

[ヘルプ](#)

LDAP識別名: [ou=jyouhou,dc=sg,dc=local](#)

LDAPグループを

選択したLDAPグループを

LDAPグループ名	コメント	所属LDAP(SG)ユーザ
LDAPグループが登録されていません		

☐ 全選択/解除

- (3) [LDAP グループ情報追加]画面にて各項目を入力後、[登録]ボタンを押下します。各項目の詳細は、表 2 LDAP グループ 設定項目一覧 を参照ください。

LDAPグループ情報追加

[ファイアウォール](#) > [詳細設定](#) > [LDAP連携設定](#) > [LDAPグループ設定](#) > 新規追加 [\[ヘルプ\]](#)

LDAP識別名: ou=jyouhou,dc=sg,dc=local

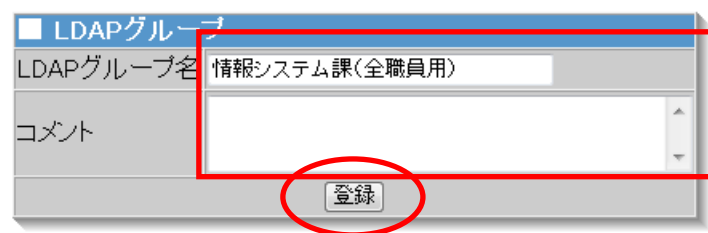


表 2 LDAPグループ 設定項目一覧

項目名	設定内容
* LDAP グループ名	任意の名前を入力します。
コメント	LDAP グループに関するコメントを入力します。

※ 各項目先頭のアスタリスク（*）は必須項目

2. 6. 所属LDAP(SG)ユーザの設定

LDAP (SG) ユーザを、LDAP グループに所属させます。

本ケースでは、userA（管理職員）を全職員用のグループと管理職員用のグループの両方に所属させ、userB（一般職員）を全職員用のグループに所属させます。

LDAP グループルールは、LDAP グループに設定することになりますので、適用させたいユーザが1人であっても LDAP グループに所属させる必要があります。

表 3 LDAPグループ名、所属LDAP (SG) ユーザ、LDAPルールの関係

LDAP グループ名	所属 LDAP (SG) ユーザ	LDAP グループルール
情報システム課（全職員用）	userA、userB	情報システムサーバおよびインターネットへのアクセス許可
情報システム課（管理職員用）	userA	人事サーバへのアクセス許可



- (1) [ファイアウォール] > [詳細設定] > [LDAP 連携設定] > [LDAP グループ設定] 画面の[所属 LDAP (SG) ユーザ]アイコンをクリックします。

LDAPグループ設定

[ファイアウォール](#) > [詳細設定](#) > [LDAP連携設定](#) > LDAPグループ設定 [\[ヘルプ\]](#)

LDAP識別名: ou=jyohou,dc=sg,dc=local

LDAPグループを [追加](#)
選択したLDAPグループを [削除](#)

LDAPグループ名	コメント	所属LDAP(SG)ユーザ
<input type="checkbox"/> 情報システム課(全職員用)		
<input type="checkbox"/> 情報システム課(管理職員用)		

☐ 全選択/解除

- (2) [所属 LDAP (SG) ユーザ設定] 画面で所属させたい LDAP (SG) ユーザをチェックし、[設定] ボタンを押下します。

(全職員用のグループでの設定)

所属LDAP(SG)ユーザ設定

[ファイアウォール](#) > [詳細設定](#) > [LDAP連携設定](#) > [LDAPグループ設定](#) > 所属LDAP(SG)ユーザ設定 [ヘルプ](#)

LDAP識別名: ou=jyouhou,dc=sg,dc=local
LDAPグループ名: 情報システム課(全職員用)

LDAP(SG)ユーザの中から、LDAPグループに所属させるユーザをチェックしてください。

LDAP(SG)ユーザ名	フィルタ
<input checked="" type="checkbox"/> userA	ou=jyouhou
<input checked="" type="checkbox"/> userB	ou=jyouhou

☐ 全選択/解除

[設定](#)

(管理職員用のグループでの設定)

所属LDAP(SG)ユーザ設定

[ファイアウォール](#) > [詳細設定](#) > [LDAP連携設定](#) > [LDAPグループ設定](#) > 所属LDAP(SG)ユーザ設定 [ヘルプ](#)

LDAP識別名: ou=jyouhou,dc=sg,dc=local
LDAPグループ名: 情報システム課(管理職用)

LDAP(SG)ユーザの中から、LDAPグループに所属させるユーザをチェックしてください。

LDAP(SG)ユーザ名	フィルタ
<input checked="" type="checkbox"/> userA	ou=jyouhou
<input type="checkbox"/> userB	ou=jyouhou

☐ 全選択/解除

[設定](#)

2.7. LDAPルールの設定

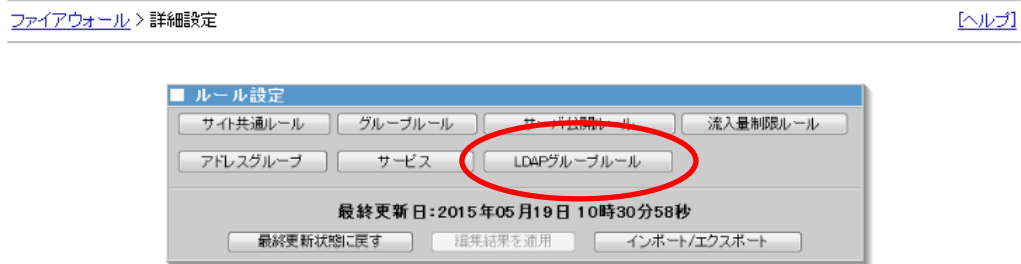
LDAP グループに、ルールとルール有効時間を設定します。ルール有効時間は、ユーザがログインして適用されるルールが有効となる時間となります。有効時間が経過する前に再度ログインするとその時点から有効時間が経過するまで有効となります。

また共用 PC に、管理職員と一般職員の 2 人がログインしている場合、共用 PC には管理職員用のルールと全職員用のルールが適用されていますので、一般職員が人事サーバにアクセスできることに注意してください。

本ケースでは、全職員用のグループにインターネットと情報システムへのアクセスを許可するルールを、管理職員用のグループに人事サーバへのアクセスを許可するルールを設定します。

ここでは全職員用のグループにインターネットへのアクセスを許可するルールについて説明します。

- (1) [ファイアウォール] > [詳細設定] 画面の[LDAP グループルール]ボタンを押下します。



- (2) [ルール設定(LDAP 識別名選択)] 画面で LDAP 識別名を選択し、[追加]ボタンを押下します。

ルール設定(LDAP識別名選択)



- (3) [ルール設定 (LDAP グループ)] 画面の [追加] ボタンを押下します。

ルール設定 (LDAP グループ)

ファイアウォール > 詳細設定 > ルール設定 (LDAP グループ) [ヘルプ]

かんたん設定 (ネットワーク構成) の確認

LDAP 識別名: ou=jyohou,dc=sg,dc=local

ルールの追加・削除・更新を行った場合は、詳細設定トップ画面の「編集結果を適用」ボタンをクリックしてください。

一覧末尾に LDAP グループルールを **追加** (削除)

選択した LDAP グループルールを (削除)

1 頁に表示する LDAP グループ 20 件 反映

全件中 件目を表示

← 前の件 | 次の件 →

No.	発信元	宛先	通信種別	処理	記録	コメント
LDAP グループルールが登録されていません。						

☐ 全選択/解除

← 前の件 || 次の件 →

- (4) [LDAP グループ選択] 画面で LDAP グループ名を選択し、[追加] ボタンを押下します。

LDAP グループ選択

ファイアウォール > 詳細設定 > ルール設定 (LDAP グループ) > LDAP グループ選択 [ヘルプ]

LDAP 識別名: ou=jyohou,dc=sg,dc=local

選択した LDAP グループのグループルールを **追加**

LDAP グループ名	コメント
<input checked="" type="radio"/> 情報システム課 (全職員用)	
<input type="radio"/> 情報システム課 (管理職用)	

- (5) [LDAP グループルール] 画面の [追加] ボタンを押下します。

LDAP グループルール

ファイアウォール > 詳細設定 > ルール設定 (LDAP グループ) > LDAP グループルール [ヘルプ]

LDAP 識別名: ou=jyohou,dc=sg,dc=local

LDAP グループ名: 情報システム課 (全職員用)

☐ **ルール有効時間**

10 時間

一覧末尾に LDAP グループルールを **追加** (削除)

選択した LDAP グループルールを (削除)

No.	発信元	宛先	通信種別	処理	記録	コメント
LDAP グループルールが登録されていません。						

☐ 全選択/解除

登録

- (6) [LDAP グループルール 設定追加] 画面で各項目を入力し、[登録]ボタンを押下します。各項目の詳細は、表 4 LDAP グループルール 設定項目一覧 を参照ください。

LDAPグループルール 設定追加

ファイアウォール > 詳細設定 > ルール設定(LDAPグループ) > LDAPグループルール > 設定追加 [\[ヘルプ\]](#)

LDAP識別名: ou=jyohou.dc=sg.dc=local
LDAPグループ名: 情報システム課(全職員用)

■ 処理

許可 →

■ 発信元

ユーザが使用中のホスト

■ 宛先

☐ ユーザ指定
☒ 外部
☐ 内部
☐ DMZ
☐ 任意
☐ ファイアウォール自身

☐ 上記指定以外

■ 通信種別

☒ ユーザ指定
☐ 任意

■ 記録

☐ なし
☒ ログ
☐ アラート+ログ

■ コメント

表 4 LDAPグループルール 設定項目一覧

項目名		設定内容
処理		許可のみとなります。設定の変更はできません。
発信元		ユーザがログインした PC を発信元とする通信にルールを適用します。設定の変更はできません。
* 宛先	ユーザ指定	通信を許可する宛先を IP アドレスかアドレスグループで指定します。アドレスグループについては、画面右上 [ヘルプ] を参照してください。
	外部	外部ネットワークへの通信を許可します。
	内部	内部ネットワークへの通信を許可します。
	DMZ	DMZ への通信を許可します。
	任意	宛先に関わらず通信を許可します。
	ファイアウォール自身	ファイアウォール自身への通信を許可します。
* 通信種別	ユーザ指定	右側のリストボックスからプロトコル種別を選択し、[←] ボタンを押下するか、テキストエリアに直接プロトコル種別を直接入力します。
	任意	通信種別に関わらず通信を許可します。
* 記録	なし	ログもアラートも残しません。
	ログ	通信のログを残します。
	アラート+ログ	通信のログを残すとともにアラート情報も残します。
コメント		任意のコメントを入力できます。

※ 各項目先頭のアスタリスク（*）は必須項目

- (7) [LDAP グループルール] 画面でルール有効時間を入力し、[登録] ボタンを押下します。

LDAPグループルール

ファイアウォール > 詳細設定 > ルール設定(LDAPグループ) > LDAPグループルール [ヘルプ](#)

LDAP識別名: ou=jyouhou,dc=sg,dc=local
LDAPグループ名: 情報システム課(全職員用)

ルール有効時間
10 時間

一覧末尾にLDAPグループルールを [追加](#)
選択したLDAPグループルールを [削除](#)

No.	発信元	宛先	通信種別	処理	記録	コメント
<input type="checkbox"/> 1	ユーザが使用中のホスト	外部	http https			

☐ 全選択/解除

[登録](#)

- (8) [LDAP グループルール] 画面の[ルール設定 (LDAP グループ) に戻る]ボタンを押下します。

LDAPグループルール

ファイアウォール > 詳細設定 > ルール設定(LDAPグループ) > LDAPグループルール > 登録結果 [ヘルプ](#)

LDAP識別名: ou=jyouhou,dc=sg,dc=local
LDAPグループ名: 情報システム課(全職員用)

LDAPグループルールを設定しました。

[ルール設定\(LDAPグループ\)に戻る](#)

- (9) [ルール設定 (LDAP グループ)] 画面の[詳細設定]リンクを押下します。

ルール設定(LDAPグループ)

ファイアウォール > [詳細設定](#) > ルール設定(LDAPグループ) [ヘルプ](#)

[かんたん設定\(ネットワーク構成\)の確認](#)

LDAP識別名: ou=jyouhou,dc=sg,dc=local

ルールの追加・削除・更新を行った場合は、詳細設定トップ画面の「編集結果を適用」ボタンをクリックしてください。

一覧末尾にLDAPグループルールを [追加](#)
選択したLDAPグループルールを [削除](#)

1頁に表示するLDAPグループ 20 件 [反映](#)

全1件中1件目を表示 ← 前の20件 | 次の20件 →

No.	発信元	宛先	通信種別	処理	記録	コメント
[001]	情報システム課(全職員用)	ルール有効時間: 10時間	このLDAPグループルール全体を削除			
<input type="checkbox"/> 1	ユーザが使用中のホスト	外部	http https			

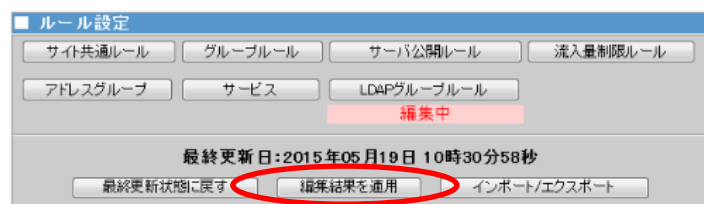
☐ 全選択/解除 ← 前の20件 | 1 | 次の20件 →

(10) [詳細設定] 画面の[編集結果を適用]ボタンを押下します。

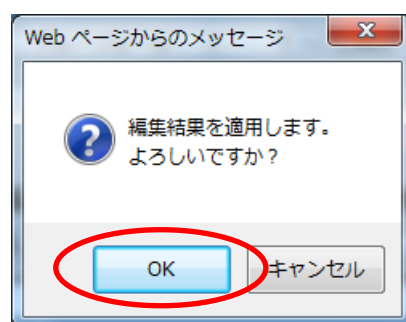
詳細設定

[ファイアウォール](#) > 詳細設定

[ヘルプ](#)



(11) [OK]ボタンを押下します。



2. 8. LDAP連携利用の設定

ユーザがログインした時の通知を SG が受け取るように設定します。

- (1) [ファイアウォール] > [詳細設定] > [LDAP 連携利用設定] 画面で各項目を入力し、[更新] ボタンを押下します。各項目の詳細は、表 4 LDAP グループルール 設定項目一覧 を参照ください。

LDAP連携利用設定

[ファイアウォール](#) > [詳細設定](#) > LDAP連携利用設定

[ヘルプ](#)

LDAP連携利用設定

☐ LDAP連携を利用しない
 ☒ LDAP連携を利用する

LDAPユーザのログイン通知を受け取るポート番号を
 とする

どこからの通知を許可しますか？
 ☒ 内部ネットワークからのみ許可する
 ☐ すべてのネットワークから許可する

表 5 LDAP連携利用設定 設定項目一覧

項目名		設定内容
* 利用設定	LDAP 連携を利用しない	ユーザがログインした時の通知を受け取りません。LDAP 連携機能は動作しません。
	LDAP 連携を利用する	ユーザがログインした時の通知を受け取ります。LDAP 連携機能は動作します。
通知を受け取るポート番号		LDAP ユーザのログイン通知の受付を行うウェブのポート番号を指定する。
通知を許可	内部ネットワークからのみ許可する	LDAP ユーザのログイン通知を、内部ネットワークからのみ受け付けます。
	すべてのネットワークから許可する	LDAP ユーザのログイン通知を、どこからでも受け付けます。

※ 各項目先頭のアスタリスク（*）は必須項目

3章 注意事項

- LDAP連携機能を利用して登録できるLDAP上のユーザ情報（ユーザ名、及びLDAP識別名）に、【半角英数字、半角ハイフン、半角アンダスコア、半角ピリオド以外の文字】が使用されている場合はサポート対象外です。使用された場合は予期せぬ動作となる場合があります。
- LDAPサーバのユーザ名が64文字以上の場合、SGに登録することができません。
- インターネットインフォメーションサービス（IIS）マネージャーで作成した自己署名証明書の有効期限は1年となります。1年以内に再度、自己署名証明書を作成する必要があります。
- ユーザがログインしてからLDAPルールの有効時間を経過するとルールが非適用となります。再び適用するためには、再度ログインする必要があります。
- ユーザがログインすると有効時間が経過するまでルールが適用されたままの状態となります。共有で使用するPCで、有効時間が経過する前に他のユーザがログインすると、適用されたままのルールによるアクセスが可能となります。
- LDAPルールで許可されているアクセスであっても、サイト共通ルールで許可されていない場合、アクセスすることはできません。
- LDAPサーバのユーザを削除あるいは別のLDAP識別名に移動させた後に、[LDAP (SG) ユーザ設定]画面もしくは[所属LDAP (SG) ユーザ設定]画面に遷移すると、SG上のLDAP識別名配下に登録したLDAP (SG) ユーザは自動的に削除されます。