Garoon
SSOとAD連携 説明資料

サイボウズ株式会社

Garoon

本資料について

- 本文書の取り扱いについて
  この文書内における掲載情報の二次利用においては、ご自身の判断と責任の下に行ってください。サイボウズ株式会社は、それらの情報をご利用になることにより発生したあらゆる商業的損害・損失を含め一切の直接的、間接的、特殊的、付随的または結果的損失、損害について責任を負いません。本文書を一部引用して作成した文書には、次のような当社の著作権表示文を記載してください。「この文書は、サイボウズ株式会社による『GaroonSSOとAD連携 説明資料』を一部引用しています。」

- 商標について
  記載された商品名、各製品名は各社の登録商標または商標です。また、当社製品には他社の著作物が含まれていることがあります。個別の商標・著作物に関する注記については、弊社のWebサイトを参照してください。
  https://cybozu.co.jp/logotypes/other-trademark/

目次

本資料ではクラウド版GaroonとパッケージGaroonでSSOに利用できる認証方式、およびAD連携を行う方法をご説明します。

1. クラウド版GaroonのSSOとAD連携
    i. SSOで利用できる認証方式
    ii. AD連携

2. パッケージ版GaroonのSSOとAD連携
    i. SSOで利用できる認証方式
    ii. AD連携

SSO　：シングルサインオン
AD　：Active Directory連携
※Active DirectoryはMicrosoftが提供するディレクトリサービスです

クラウド版 Garoon

SSOとAD連携

クラウド版Garoon のSSOとAD連携　目次

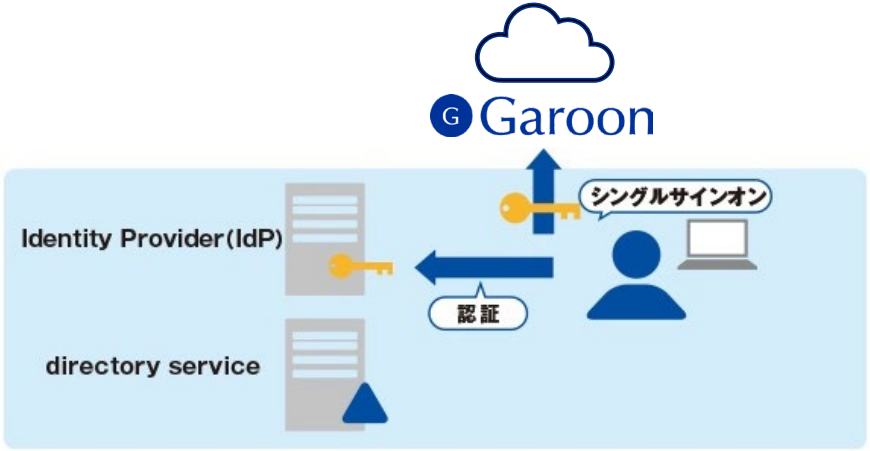
クラウド版 Garoon

SSOで利用できる認証方式

SSOで利用できる認証方式

クラウド版Garoonで他システムとSSOを行う場合はSAML認証を利用します。

- SAML認証
  異なるセキュリティドメイン間で認証情報を連携するためのXMLベースの標準仕様です。



詳しくは以下のページをご覧ください。
https://jp.cybozu.help/general/ja/admin/list_saml.html

クラウド版 Garoon

AD連携の方法

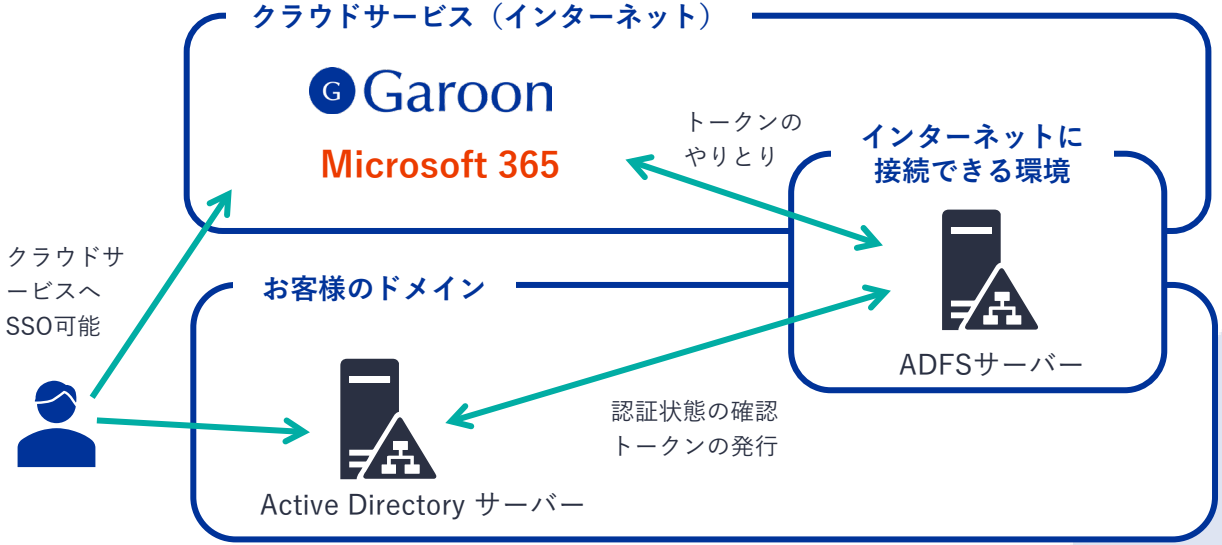
AD連携

AD連携については「認証」と「ユーザー連携」にわけて検討する必要があります。

- ADによる認証
  ADに登録されているユーザー情報を利用して認証を行うことです。
  以下の2つの方法があります。
  - ADFSを利用する
  - Microsoft Entra ID（旧 AzureAD）を利用する
- ADによるユーザー連携
  ADに登録されているユーザー情報をGaroonに登録することです。
  以下の3つの方法があります。
  - 連携ソリューションを利用する
  - Azure Functionsを利用する
  - プロビジョニング機能を利用する

ADによる認証 －ADフェデレーションサービス(ADFS)を利用－

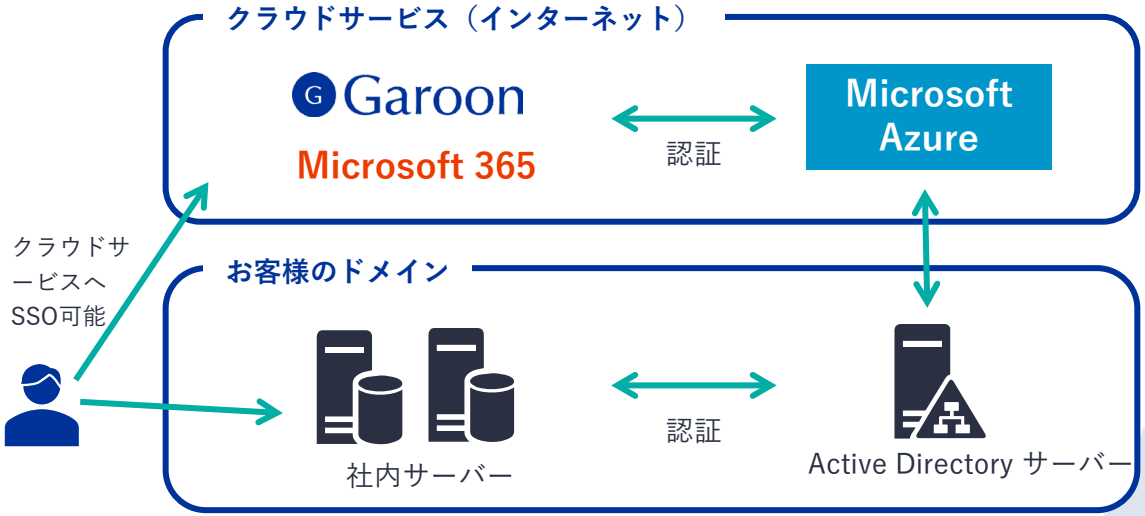
社内のADからインターネットを経由して認証を行い、オンプレミスだけではなく クラウドサービスも含めたSSOを実現する方式です。



詳しくは以下のページをご覧ください。
https://cybozu.dev/ja/id/a54158b14a50830f29070350/

ADによる認証 – Microsoft Entra ID（旧 AzureAD）を利用 –

IDやアクセスを管理するクラウド型のソリューション、 Microsoft Entra ID（旧 AzureAD）を利用してSSOを実現する方式です。



詳しくは以下のページをご覧ください。
https://cybozu.dev/ja/id/945cd23374ba72897798dd60/

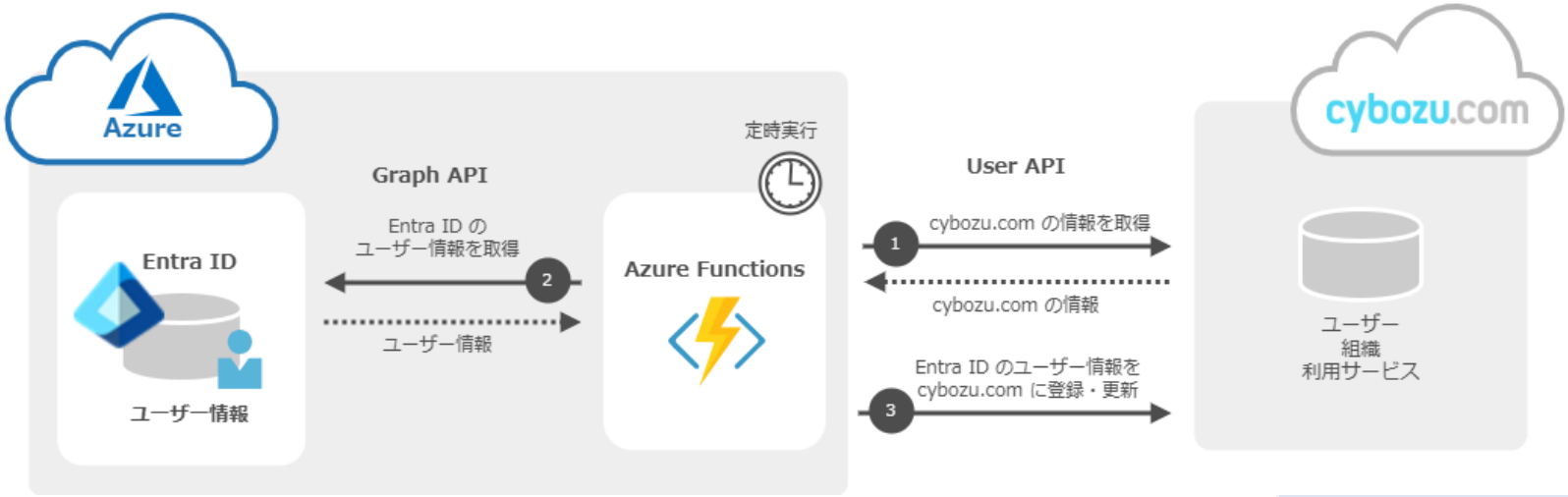
ADによるユーザー連携 －連携ソリューションを利用－

オフィシャルパートナーから、ユーザー連携の連携ソリューションが提供されています。

クラウド版 GaroonとのSSOやユーザー連携に利用できる連携ソリューションは以下をご覧ください。
https://www.cybozu.com/jp/service/solution/

ADによるユーザー連携 – Azure Functionsを利用する –

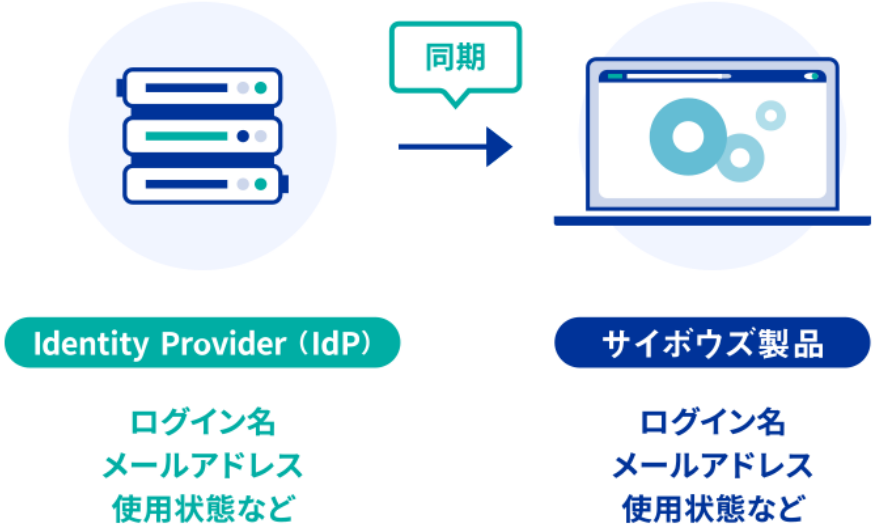
Azure Functions を使って、定期的に Microsoft Entra ID（旧 AzureAD）から cybozu.com（サイボウズのクラウドサービス） へ自動でユーザー情報の登録を行う方法です。



詳しくは以下のページをご覧ください。
https://cybozu.dev/ja/id/6de47b1a28248f27c3750ee5/

ADによるユーザー連携 －プロビジョニング機能を利用－

SCIMによるユーザープロビジョニングを標準搭載し、構築済みのIdentity Provider(IdP)で管理しているアカウント情報を、サイボウズのクラウドサービスに同期する方法です。



詳しくは以下のページをご覧ください。
https://jp.cybozu.help/general/ja/id/020260.html

パッケージ版 Garoon

SSOとAD連携

パッケージ版Garoon SSOとAD連携　目次

パッケージ版 Garoon

SSOで利用できる認証方式

SSOで利用できる認証方式

パッケージ版 Garoonで利用できる認証方式には以下の3つがあります。

- 標準認証（必要な情報を POST させる）
- 統合 Windows 認証（環境変数認証）
- オープン統合認証 ver.2（Cookieを利用した認証）

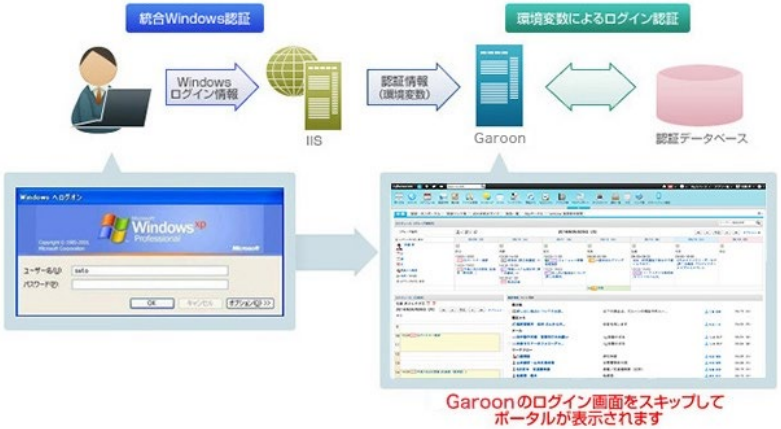
標準認証は、Garoonのユーザー情報を使用して認証する方法です。「統合Windows認証」と「オープン統合認証 ver.2」については次ページ以降で詳しくご説明します。

パッケージ版 Garoon

統合 Windows 認証

統合 Windows 認証

「統合 Windows 認証」とは、マイクロソフト社による認証形式で、ドメインの認証情報を利用し、マイクロソフト社製 Webサーバーのインターネットインフォメーションサービス（以下IIS)とブラウザを認証させるものです。これを利用すると、Windows 端末にログインするだけで、 Garoonに自動的にログインすることが可能です。



詳細・構築についてはサイボウズ オフィシャル パートナーへご相談ください。
https://partner.cybozu.co.jp/

「統合 Windows 認証」の設定方法と利用例

「システム管理画面(基本システム)」-「認証」-「ログイン認証」より「ログイン認証を追加する」をクリックし、「環境変数認証」をログイン認証形式に選択して、以下の設定を追加します。

例えば以下のような運用が可能です。

- Windows 端末のスタートアップ機能を利用し、Windows 端末に一度ログイン後、自動的にGaroonのログイン後の画面を表示させる。
- 統合 Windows 認証を利用可能な Web サービスへSSOを行う。Garoonのリンク集にリンクを貼るだけで、特別な仕組みを導入しなくともリンク先のサービスが利用できる。

パッケージ版 Garoon

オープン統合認証ver.2

オープン統合認証ver.2

「オープン統合認証 ver2」とはGaroon独自のドメインCookie（※）による認証方式です。他のシステムで「オープン統合認証 ver.2」形式の Cookie を発行または認証することによって、サイボウズ製品と他のシステムの間でシングルサインオンが可能になります。「オープン統合認証 ver.2」を使用するにあたっては、以下の条件を満たしている必要があります。

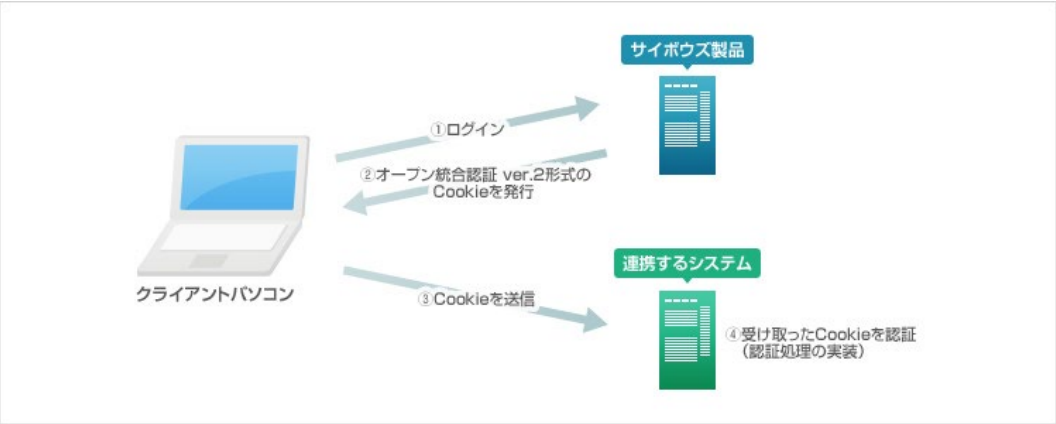
- 「Garoon」および他システムが動作するサーバーが
  互いにFQDN（完全修飾ドメイン名）で名前解決できる
- 「Garoon」および他システムが動作するサーバーが全て同一のドメインに存在する
- 「Garoon」および他システムのユーザーのログイン名が同一である

「オープン統合認証 ver.2」を使用してGaroonと他システムと認証情報を連携する場合は、Garoonをシングルサインオンのマスターとする形態と、スレーブとする形態があります。また、両方の形態を実装することによって、マルチマスターでシングルサインオンを実現することもできます。

詳細・構築についてはサイボウズ オフィシャル パートナーへご相談ください。
https://partner.cybozu.co.jp/

「オープン統合認証ver.2」を利用したSSO（マスター）

「オープン統合認証 ver.2」を使用してGaroonと他システムと認証情報を連携する場合は、Garoonをシングルサインオンのマスターとする形態と、スレーブとする形態があります。以下はGaroonをマスターとした場合です。



■必要な作業

・「Garoon」に「オープン統合認証 ver.2」を設定する

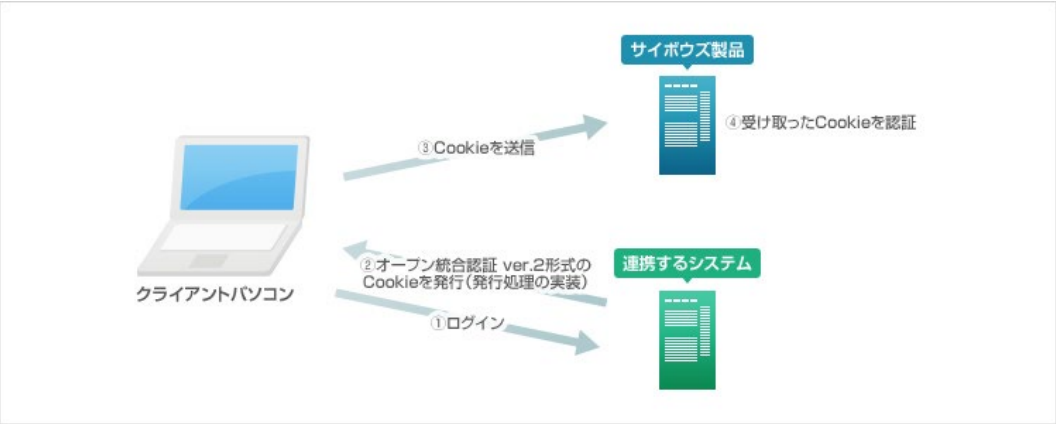
・「Garoon」と連携するシステムに、「オープン統合認証 ver.2」形式のCookieで認証する機能を実装する

詳細については、サイボウズ オフィシャル パートナーへご相談ください。

https://partner.cybozu.co.jp/

「オープン統合認証ver.2」を利用したSSO（スレーブ）

「オープン統合認証 ver.2」を使用してGaroonと他システムと認証情報を連携する場合は、Garoonをシングルサインオンのマスターとする形態と、スレーブとする形態があります。以下はGaroonをスレーブとした場合です。



■必要な作業

・「Garoon」に「オープン統合認証 ver.2」を設定する

・「Garoon」と連携するシステムに、「オープン統合認証 ver.2」形式のCookieで認証する機能を実装する

詳細については、サイボウズ オフィシャル パートナーへご相談ください。

https://partner.cybozu.co.jp/

パッケージ版 Garoon

AD連携の方法

AD連携

AD連携については「認証」と「ユーザー連携」にわけて検討する必要があります。

- ADによる認証
  ADに登録されているユーザー情報を利用して認証を行うことです。
  以下の方法で実現できます。
  - Garoonのシステム管理でADを認証用のサーバーとして登録する
- ADによるユーザー連携
  ADに登録されているユーザー情報をGaroonに登録することです。
  以下の2つの方法があります。
  - サイボウズが提供する「ガルーン 2 連携API」を利用する
  - 連携ソリューションを利用する

ADによる認証

GaroonはLDAPv3 の規格に対応しており、認証情報を保持するデータベースとして任意のLDAP サーバーを使用することができます。 LDAPサーバーとしてADを利用した場合、Garoonの利用者パスワードをADにて管理することができます。

上記設定を行う場合、Garoonのユーザー情報とADのログイン名を同じにして登録する必要があります。

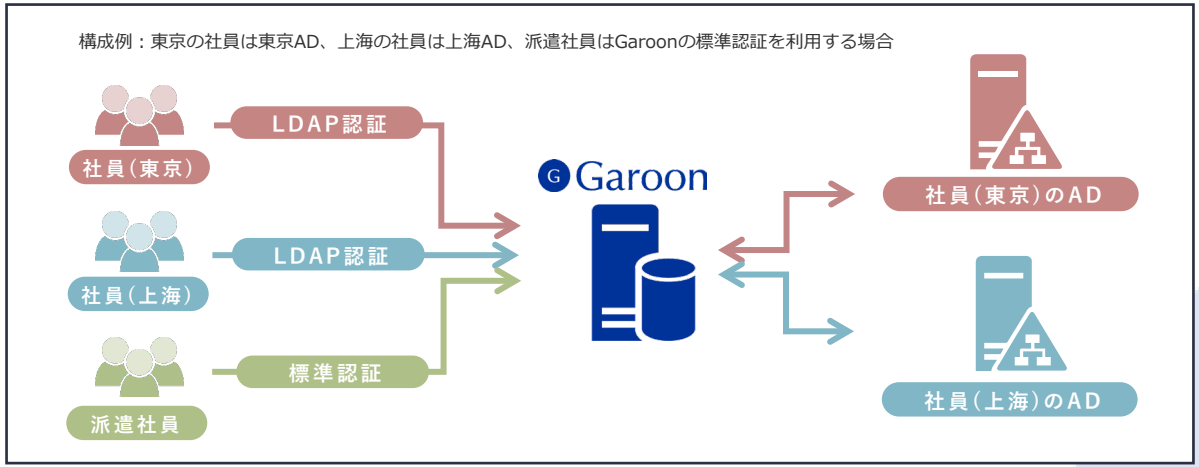
ログイン名で同一ユーザーかを判断するためです。

詳細・構築についてはサイボウズ オフィシャル パートナーへご相談ください。

https://partner.cybozu.co.jp/

ADによる認証 －複数認証－

Garoonの標準認証とLDAP認証（複数可）を組み合わせて利用することもできます。たとえば、派遣社員はGaroonの標準認証を利用する一方、正社員はLDAP認証を利用してADと連携する、というような運用が可能です。



詳細・構築についてはサイボウズ オフィシャル パートナーへご相談ください。
https://partner.cybozu.co.jp/

ADによるユーザー連携 －「ガルーン 2 連携API」を利用－

サイボウズが提供する「ガルーン 2 連携API」を利用することでADで管理するユーザー情報をGaroonに一括登録が可能です。

詳細・構築についてはサイボウズ オフィシャル パートナーへご相談ください。
https://partner.cybozu.co.jp/

ADによるユーザー連携 －連携ソリューションを利用－

オフィシャルパートナーが提供するID統合管理製品を利用してユーザー連携を行うこともできます。連携ソリューションを利用することでGaroon以外の他システムも含めたユーザー情報を一元管理が容易になります。

詳しくは以下のページをご覧ください。
https://garoon.cybozu.co.jp/function/expand/

付録：
「統合 Windows 認証」
「オープン統合認証 ver.2」の応用

付録

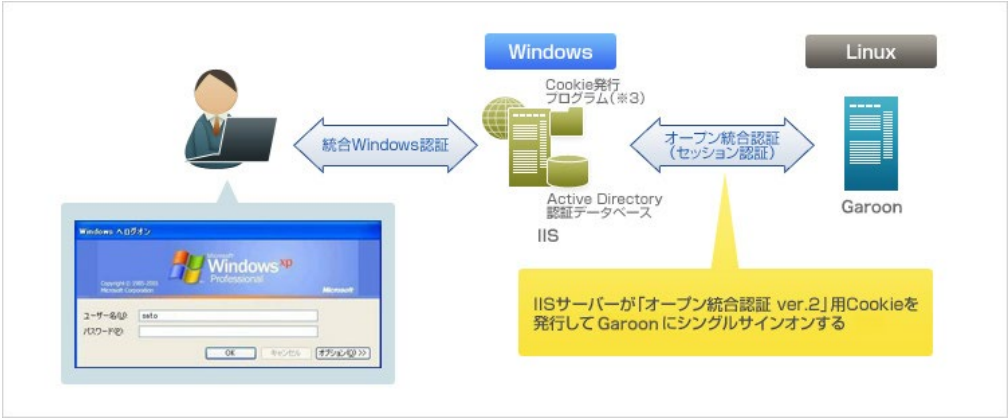
「統合 Windows 認証」「オープン統合認証 ver.2」を利用した認証の応用例をご紹介します。

1. **Linux上のGaroonで「統合 Windows 認証」を利用**
2. **Garoonを経由して「統合 Windows 認証」を利用**

Linux上のGaroonで「統合 Windows 認証」を利用

■概要

Linux OS では IISが対応していないため、Garoonを Linux OS で運用する場合は通常「統合 Windows 認証」が利用できません。 しかし「オープン統合認証 ver.2」と「統合 Windows 認証」を組み合わせることで、Linux 上で運用しているGaroonに「統合 Windows 認証」でのシームレスなログインが実現できます。
クライアント PC がまず認証用の IIS にアクセスし「オープン統合認証 ver.2」を利用して、Cookie を発行します※。その Cookie を利用してGaroonにシングルサインオンを行います。

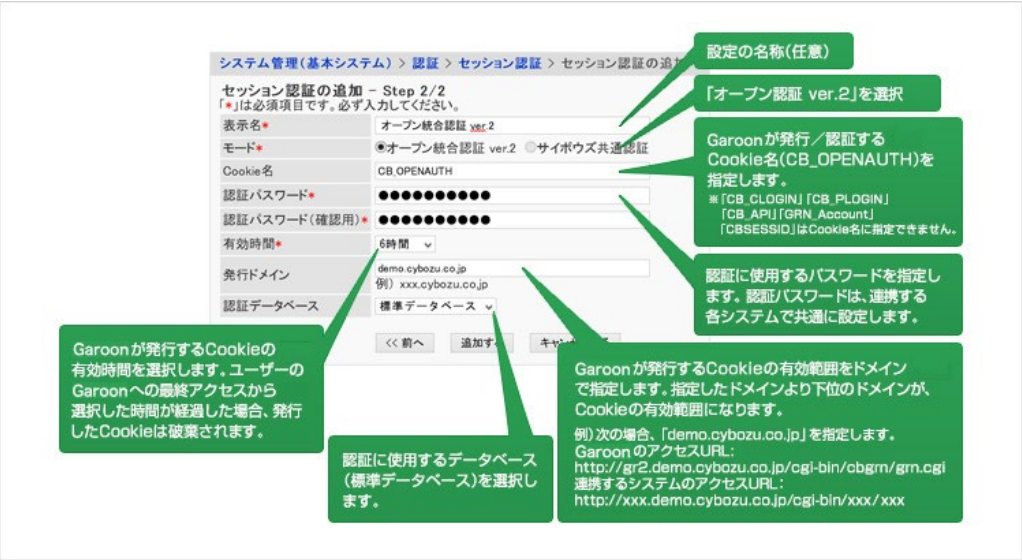


詳細についてはサイボウズ オフィシャル パートナーへご相談ください。
https://partner.cybozu.co.jp/

Linux上のGaroonで「統合 Windows 認証」を利用

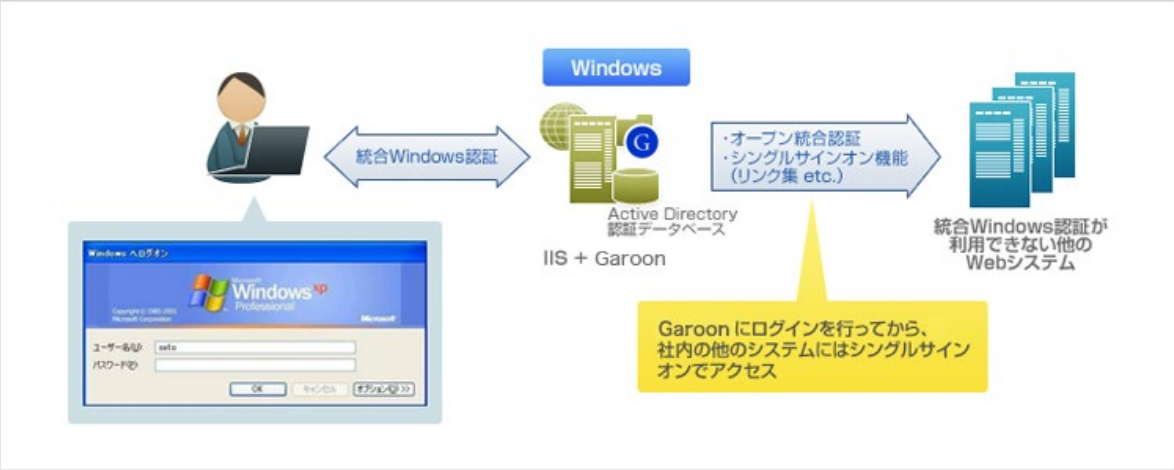
■設定画面

「システム管理画面(基本システム)」-「認証」-「セッション認証」より「セッション認証を追加する」をクリックします。「オープン統合認証 ver2」をセッション認証形式に選択して、以下の設定を追加します。



Garoonを経由して「統合 Windows 認証」を利用

「統合 Windows 認証」を利用する場合、スレーブ側のシステムは統合 Windows 認証に対応している必要があります。統合 Windows 認証に対応していないシステムがある場合、Garoonを経由させることで、擬似的に統合 Windows 認証を利用したシングルサインオンの仕組みを構築できます。
まず、「統合 Windows 認証」を利用してGaroonにログインします。その後Garoonの標準機能である「オープン統合認証 ver.2」もしくは「シングルサインオン」機能を利用します。 Garoonを経由して「統合 Windows 認証」が利用できない他のWebシステムへSSOが可能になります。



END