2016 年 3 月 25 日
株式会社セキュアソフト

SecureSoft コンテナシリーズでの AD サーバ連携について

はじめに

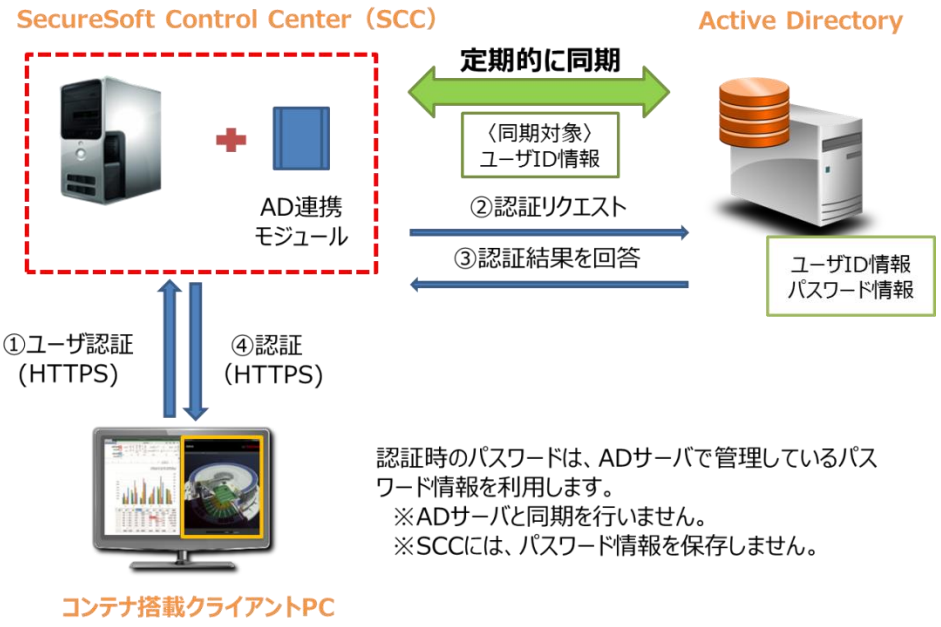
SecureSoft コンテナシリーズでは、コンテナユーザ認証を既存のシステムで利用している Active Directory サーバ(以下“AD サーバ”)のユーザ情報と連携する機能を提供しています。この連携機能により、コンテナシステム導入時のエンドユーザ認証情報管理について一元化が可能となり運用者の負担を軽減できます。

■AD サーバとの連携について

SecureSoft コンテナシステムでユーザ ID 管理を行う SecureSoft Control Center（以下“SCC”）では、ユーザの既存環境で運用されている AD サーバと連携をさせるために、「Active Directory 連携モジュール」(以下 “AD 連携モジュール”)をオプションで提供しています。SCC に AD 連携モジュールを追加導入することで、SCC と AD サーバ間でのユーザ ID 情報連携が可能になります。パスワード情報の保持方法の違いにより以下の 2 つの方式があります。

■連携方式 1

認証リクエストを受けた SCC が AD サーバにユーザ ID 情報、パスワード情報を確認する方式です。SCC と AD サーバ間ではユーザ ID 情報は定期的に同期しつつ、認証時にはパスワード情報を AD サーバへ毎回問い合わせします。本方式ではユーザ ID 情報とパスワード情報の両方を AD サーバ側情報に委ねることで一元管理化されるメリットがあります。



【図 1】AD サーバとの連携方式 1

[図 1　動作概要]

① ユーザは AD サーバで管理されているユーザ自身の ID、パスワードを利用してコンテナにログインします。コンテナ搭載クライアント PC は HTTPS を利用して SCC サーバへログインリクエストを送信します。

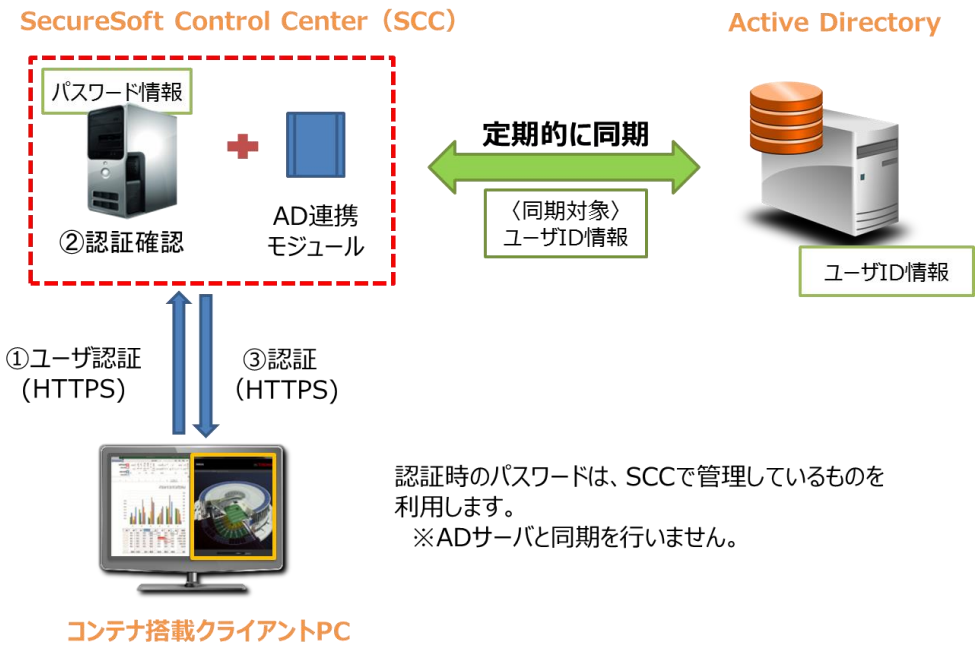
② コンテナ搭載クライアント PC からログインリクエストを受けた SCC サーバは AD 連携モジュールを使って AD サーバに認証リクエストを送ります。

③ SCC から認証リクエストを受けた AD サーバは認証結果を SCC に応答します。

④ AD サーバからの認証結果に従い、SCC はクライアントへログイン許可・拒否の応答をします。

■連携方式 2

SCC がユーザ ID 情報のみ AD サーバと定期的にユーザ ID 情報を同期し、パスワード情報は SCC 側で独自に管理する方式です。Windows システム環境とコンテナ環境のユーザ ID 管理についてポリシーが異なる等の状況に対応が可能となります。



【図 2】AD サーバとの連携方式 2

[図 2　動作概要]

① ユーザは AD サーバで管理されているユーザ自身の ID と SCC で管理しているパスワードを利用し、利用してコンテナにログインします。コンテナ搭載クライアント PC は HTTPS を利用して SCC サーバへログインリクエストを送信します。

② コンテナ搭載クライアント PC からログインリクエストを受けた SCC サーバは、AD サーバと定期的に同期されているユーザ ID 情報とローカルに管理しているパスワード情報を確認します。

③ 認証情報の確認結果に従い、SCC はクライアントへログイン許可・拒否の応答をします。

以上