～ ID 管理システム用フレームワーク ～

Ver.2.0

標準仕様説明書

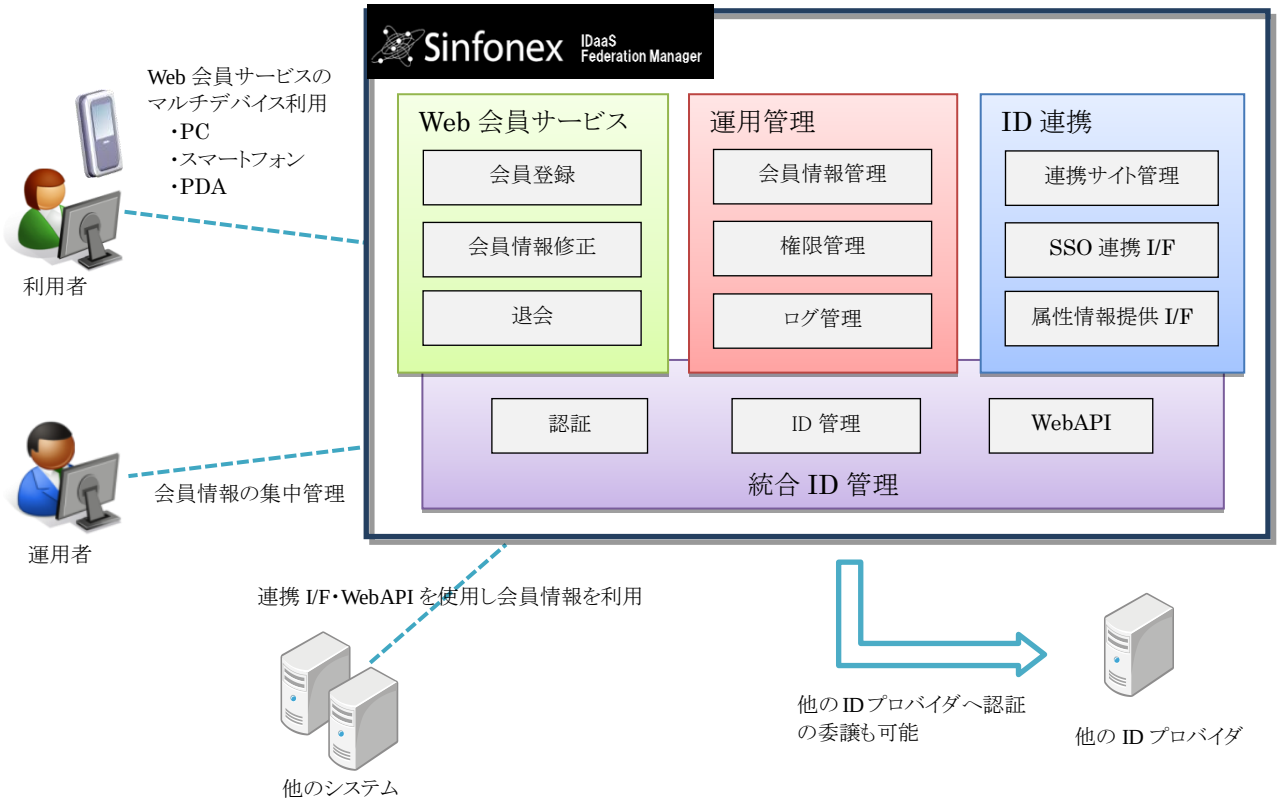
NTT DATA

変える力を、ともに生み出す。

目次

1. Sinfonex IDaaS/Federation Manager とは

「Sinfonex IDaaS／Federation Manager」とは、NTT データが提供するサービス連携プラットフォーム「Sinfonex」から Web 会員管理のためのコア機能を切り出した、ID 管理システムのためのフレームワークです。ID 管理のための機能を API 提供するため、既存システムや新システムを「Sinfonex IDaaS／Federation Manager」に接続し、その機能を利用することが可能です。
「Sinfonex IDaaS／Federation Manager」を使用することで、ユーザのログイン情報と属性情報を一元管理、各種情報の操作権限や変更履歴を管理することが可能となり、運用コストやセキュリティリスクの軽減が実現できます。



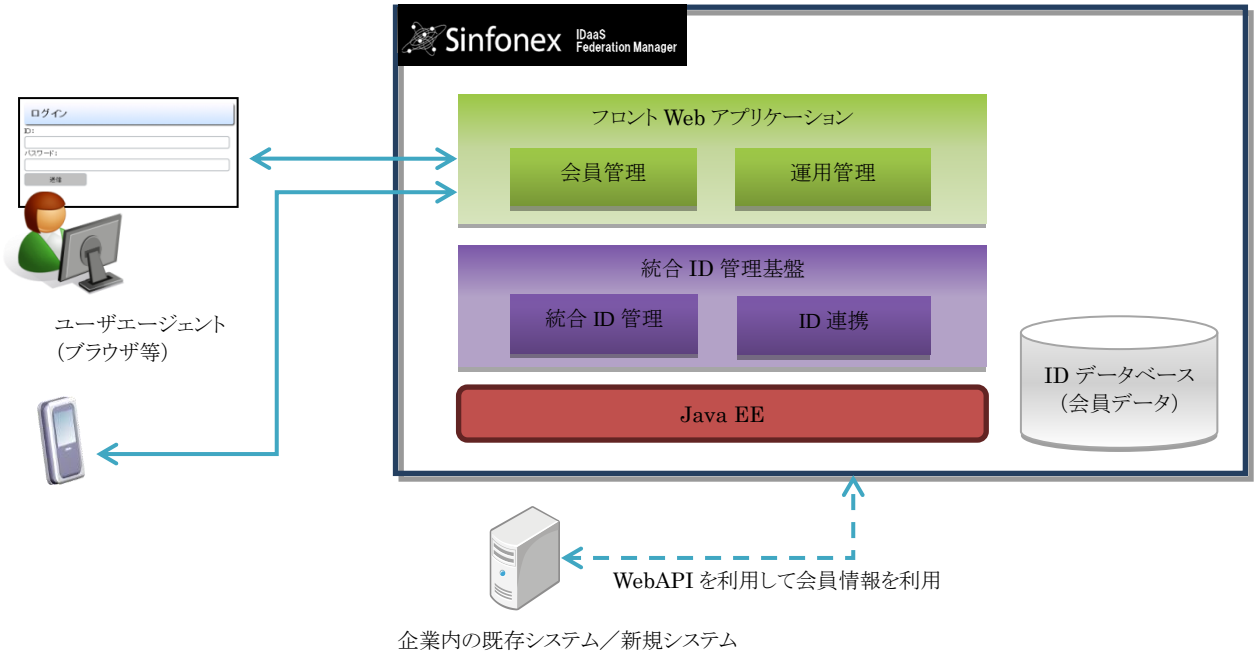
「Sinfonex IDaaS／Federation Manager」では、Web 会員システムを構築するために必要となる、以下の機能を提供します。

Web 会員サービス Sinfonex IDaaS	会員（利用者）向けポータルを短期間で構築するための各種機能をフレームワークとして提供します。会員情報管理、操作履歴の保存、メール送信などの各種機能が HTTP インタフェースで提供されるため、最小限のプログラム開発で会員向けサイトを構築することができます。
運用管理 Sinfonex IDaaS／ Federation Manager	運用者の操作権限設定、会員情報の照会・修正、操作履歴の照会など、運用管理のための充実した機能で会員情報の集中管理を実現します。
ID 連携 Sinfonex Federation Manager	ID 連携のための各種 I/F がシングルサインオンや属性情報流通を実現します。サイト間の ID 連携における国際標準仕様である SAML2.0 や OpenID 等に対応しており、大手ポータルサイトなどとも短期間でシングルサインオン接続することが可能です。

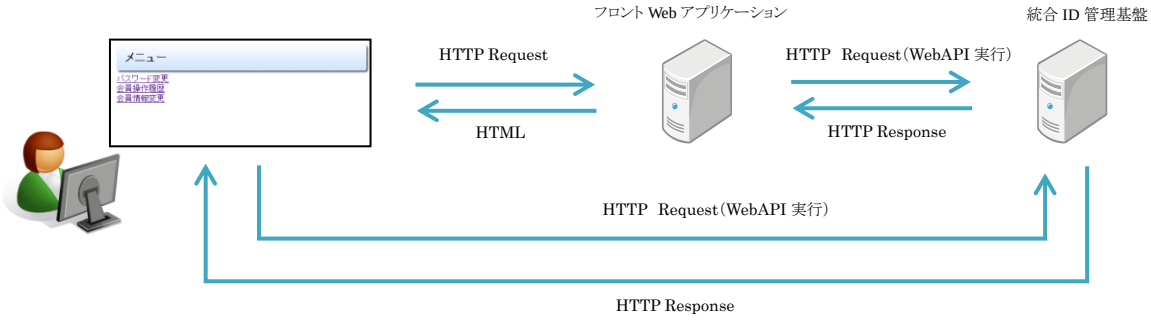
上記機能を実現するためのコア機能として、認証、ID 管理、WebAPI などの統合 ID 管理機能も備えています。

2. アーキテクチャ

「Sinfonex IDaaS／Federation Manager」の構成は、ID 管理のための機能をフレームワーク化した統合 ID 管理基盤と、ユーザにプレゼンテーションを提供するためのフロント Web アプリケーションに大別されます。
フロント Web アプリケーションは標準でシンプルなテンプレート画面を提供します。
統合 ID 管理基盤では、ID 管理業務に必要な機能を WebAPI としてフロント Web アプリケーションに提供します。各機能を API 化しているため、他の既存システムや新規システムから WebAPI を使用し ID 管理のための機能を利用するとことができます。



WebAPI の実行は HTTP リクエストで行い、結果を HTTP レスポンスで取得します。HTTP ベースの API 実装のため、ブラウザから JavaScript で WebAPI を実行する Ajax での実装など、フロント Web アプリケーションで柔軟に実装方法を選択することができます。



3. 特徴

Point1. シンプルで高性能な ID データベース

一般的なイントラネット向け ID 管理システムでは高機能ゆえにそのデータが複雑なリレーションを生み、しばしばパフォーマンスの低下を招きます。「Sinfonex IDaaS／Federation Manager」の ID データベースは、Web 会員管理に最適化されたシンプルな設計のため高性能な機能提供が可能となっており、大規模ユーザの ID と属性情報を管理できます。

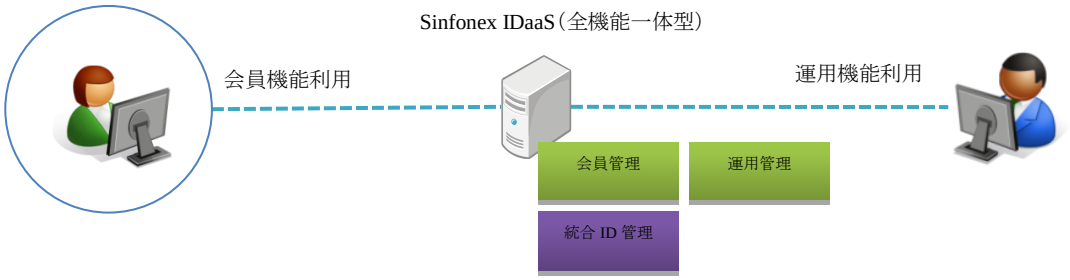
	Sinfonex IDaaS Federation Manager	一般的なイントラネット向け ID 管理システム
機能	提供機能を Web 会員管理に特化	高機能 ・ワークフロー ・組織管理 ・レポート etc…
データベースの特徴	Web 会員管理に最適化されたデータベース設計で高性能。標準構成で 5000 万会員の情報を管理可能。	データ構造が複雑になりやすくデータ量が増えやすいため、データベースアクセスがボトルネックとなりパフォーマンスの低下を招きやすい。

Point2.　拡張性を考慮した柔軟なアプリケーション構成

各種機能を WebAPI や外部 I/F として提供し機能間の依存度を低くする設計となっているため、システム全体のサイジングやプレゼンテーションレイヤの拡張、他システムの接続などが容易に行えるようになっています。

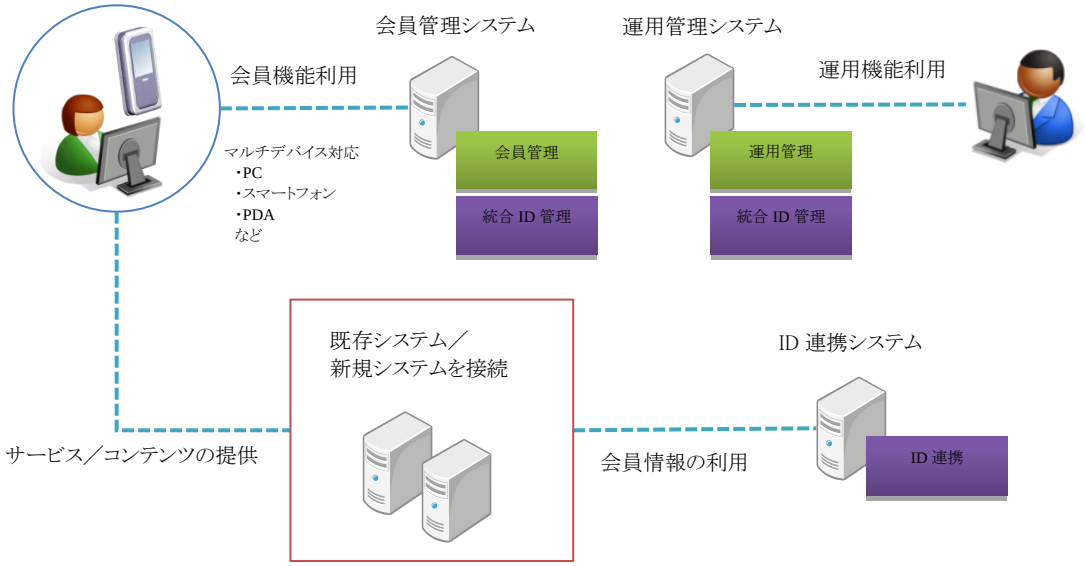
■小規模向けシステム構成例

全機能（ID 連携オプションを除く）が1台のサーバで稼働する小規模向けシステム構成例です。



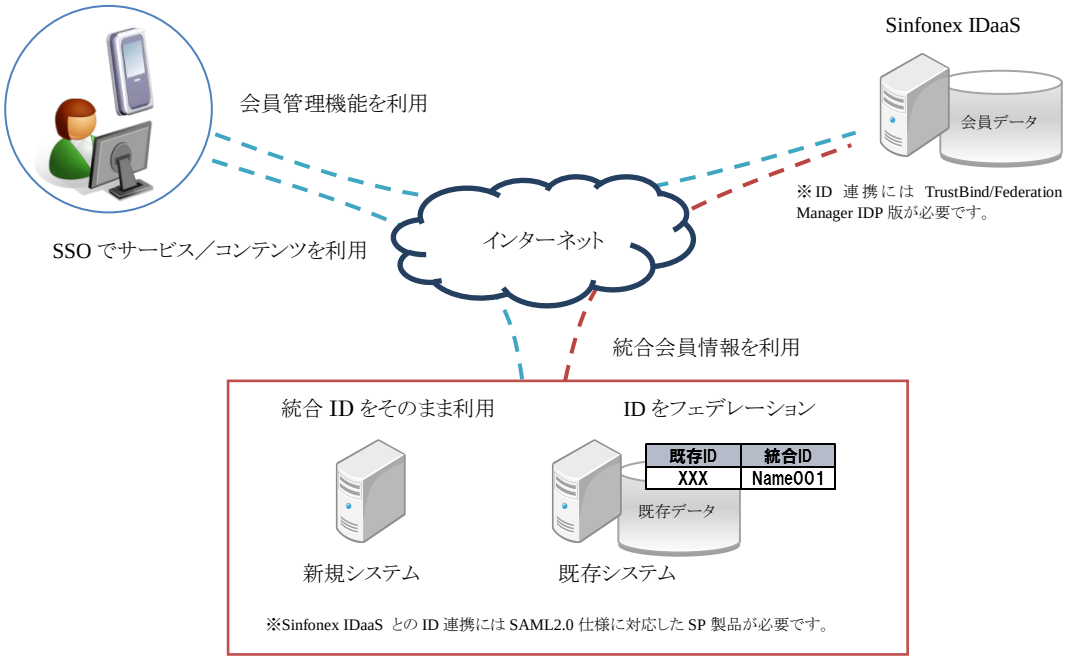
■大規模向けシステム構成例

各機能を別々のサーバで稼働させる大規模向けシステム構成例です。小規模向けシステム構成からの移行も可能です。

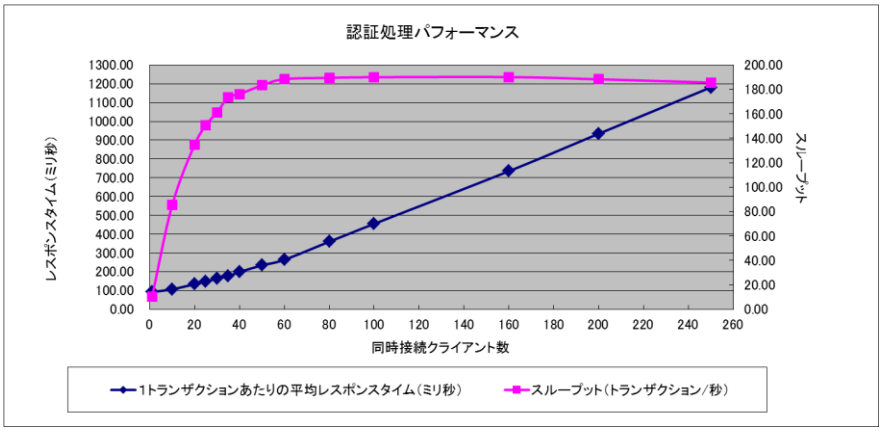


Point3. 国際標準仕様に準拠した ID 連携

「Sinfonex IDaaS」の統合 ID 管理基盤は、国際的な認定機関である Kantara Initiative の相互接続性試験に合格した TrustBind/Federation Manager※1 と連携することで、SAML2.0※2 の技術を使用したシングルサインオン（SSO）、シングルログアウト（SLO）、属性情報提供機能を高い品質で提供します。SAML2.0 仕様で ID 連携を行うため、異なるドメインのシステム間でも安全に認証情報と属性情報を交換し、SSO・SLO することが可能です。また、SAML2.0 によるシングルサインオンはアイデンティティ・フェデレーション※3 により実現されるため、既に ID を管理している既存システムを接続し、ID を連携させることが可能です。



■統合 ID 管理サーバ 1 台（CPU：4core、メモリ：4G）での認証処理パフォーマンス参考値



※上記はサーバ 1 台構成の参考値です。サーバ環境をスケールアウトすることでさらに性能向上が可能です。

※1 TrustBind/Federation Manager は NTT ソフトウェア株式会社の製品です。Sinfonex IDaaS／Federation Manager は当該商品の OEM です。

※2 SAML2.0 はユーザの認証や属性、認可に関する情報を記述するマークアップ言語で、Web サイトや Web サービスの間でこれらの情報を交換することで、一度の認証で複数のサービスが利用できるシングルサインオンを実現できます。

※3 アイデンティティ・フェデレーションは、別々に管理された ID 情報を連携させる概念です。

4. 機能

会員管理

「Sinfonex IDaaS／Federation Manager」の会員管理機能は、Web 会員管理に特化したラインナップで軽量・高性能な機能を WebAPI としてご提供します。各会員管理 WebAPI を使用し、業務を実現するための画面テンプレートをご提供します。
会員登録から会員情報修正、リマインダによるパスワード再発行など、会員自らのセルフメンテナンスを可能とし、運用管理コストを軽減します。

■会員管理 WebAPI 一覧

機能名称		概要
会員登録	会員情報登録	新規会員情報を登録します。
パスワード再発行	パスワード再発行	登録されているメールアドレスにパスワード変更用 URL を送信します。 (「秘密の質問」表示、回答入力)
	パスワード再発行受付	パスワード再発行用メールに記載したリンク URL から遷移してパスワードを変更します。 (ID、新 PWD 入力)
	パスワード変更	パスワードの変更を行います。
会員認証	ログイン	ID/PW で認証を行い、サーバ側セッションを作成します。
	ログアウト	サーバ側セッションの破棄を行います。
会員情報変更	会員情報照会	会員情報を照会します。
	会員情報変更	会員情報の変更を行います。
会員退会	会員退会	会員の退会処理を行います。

■会員管理画面テンプレート
会員管理 WebAPI を使用し、業務を実現するための画面テンプレートをご提供します。

運用管理

「Sinfonex IDaaS／Federation Manager」の運用管理機能は、運用に必要な充実した機能を取りそろえ WebAPI としてご提供します。各運用管理 WebAPI を使用し、業務を実現するための画面テンプレートをご提供します。
会員情報のエクスポート機能などの利便性に加え、オペレータの権限設定、操作履歴管理など情報漏洩対策やセキュリティ監査も考慮しています。

■運用管理機能一覧

機能名称		概要
管理者認証	ログイン	ID/PW で認証を行い、サーバ側セッションを作成します。
	ログアウト	ログアウト処理を実施し、サーバ側セッションの破棄を行います。
	管理者パスワード変更	パスワードの変更を行います。
	管理者パスワード初期化	パスワードの初期化を行います。
管理者管理	管理者一覧照会	管理者情報を一覧照会します。
	管理者詳細照会	管理者情報を照会します。
	管理者変更	管理者情報の変更を行います。
	管理者削除	管理者を削除します。
	管理者登録	管理者を登録します。
会員管理	会員情報一覧照会	会員の一覧を照会します。
	会員情報詳細照会	会員の詳細を照会します。
	会員情報変更	会員情報を変更します。
	会員情報削除	会員を削除します。
	パスワード初期化	登録されているメールアドレスにパスワード変更用 URL を送信します。
履歴管理	会員情報出力履歴照会	会員情報出力履歴を照会します。
	アクセスログ照会	会員の各種処理履歴を照会します。
	エラーログ照会	会員のエラーログを照会します。
	操作ログ照会	管理者の各種操作履歴を照会します。

■運用管理画面テンプレート
運用管理 WebAPI を使用し、業務を実現するための画面テンプレートをご提供します。

ID 連携

「Sinfonex IDaaS／Federation Manager」は TrustBind/Federation Manager と連携し、SAML2.0 の IdP 機能を接続システムに外部 I/F として提供します。
※ID 連携機能はオプションとなります。ID 連携機能を有効にするためには TrustBind/Federation Manager が必要となります。

■ID 連携 I/F 一覧

機能名称	概要
シングルサインオン	SAML2.0 仕様に準じたシングルサインオン機能を提供します。利用者が利用するサービス（接続システム）が「Sinfonex IDaaS／Federation Manager」のシングルサインオン機能を利用することで、同様にシングルサインオン機能を利用する他のサービスにシングルサインオンすることが可能となります。
シングルログアウト	SAML2.0 仕様に準じたシングルログアウト機能を提供します。利用者が利用するサービス（接続システム）が「Sinfonex IDaaS／Federation Manager」のシングルログアウト機能を利用することで、同様にシングルログアウト機能を利用する他のサービスからシングルログアウトすることが可能となります。
属性情報提供	SAML2.0 仕様のシングルサインオン時、属性情報問い合わせ（AttributeQuery 要素）を使用した IdP から SP への属性情報提供をサポートします。

■ID 連携管理機能一覧

機能名称	概要
連携サイト登録	Sinfonex IDaaS／Federation Manager に接続して ID 連携できるサイトシステムを登録します。
連携サイト一覧	Sinfonex IDaaS／Federation Manager に接続して ID 連携できるサイトシステムの一覧を表示します。

5. システム要件

■動作環境

ハードウェア	CPU	Intel Xeon CPU 1.86GHz 以上推奨
	メモリ	2GB 以上
	ハードディスク容量	30GB 以上
ソフトウェア	OS	Red Hat Enterprise Linux v5 以降 Windows Server® 2003 以降
	Web サーバ	Apache HTTP Server 2.2 以降 Microsoft IIS 6.0 以降
	アプリケーションサーバ	Apache Tomcat 6.0 以降 Oracle WebLogic Server 10g 以降
	ランタイム環境	Java SE 6 以上
RDBMS	Oracle	Oracle10g Release1 Oracle10g Release2 Oracle11g Release1 Oracle11g Release2
	PostgreSQL	PostgreSQL 8.4 以降

Sinfonex IDaaS／Federation Manager **標準仕様説明書**

2012 年 4 月発行

発行者　株式会社エヌ・ティ・ティ・データ
リージョナルビジネス事業本部 e-コミュニティ事業部 クラウドサービス担当
東京都江東区豊洲 3-3-9
豊洲センタービルアネックス
TEL.050-5546-2449