NTT DATA
Trusted Global Innovator

認証基盤ソリューションのご紹介

VANADIS® Identity Manager

VANADIS® SecureJoin

NTTデータ先端技術株式会社
サイバーセキュリティ事業本部セキュリティイノベーション事業部DXセキュリティソリューション担当

01

製品概要

御社で、以下のようなお困りごとはございませんか？

テレワーク需要による、ゼロトラストネットワーク・クラウドサービスの利用急増

ID管理が煩雑化

- サービスごとにログインが必要で利便性が悪い
- 新しいシステム構築のたびに、独自IDが発生している
- システムID管理が一元化されておらずアクセス制御を厳格に管理出来ていない

高度なセキュリティ対策が必要に

- ID窃取を狙ったサイバー攻撃も高度化しており対策が不十分に感じる
- ID権限不備や幽霊IDによる重要な企業情報の流出リスクが気になる
- 関連法制度が技術的要件を満たしていない

導入に対する課題

- ID管理製品は海外製品が多く、自社に適応できるか不安
- ID管理システム導入の必要性は理解できるが、予算の都合で導入ができない

認証基盤ソリューションVANADISは、以下のような問題解決をします。

01

不適切なID管理が引き起こすセキュリティリスクを予防！

◆徹底したライフサイクル管理により幽霊IDの不正利用による個人情報・企業重要情報の流出を防ぎます
◆セキュリティポリシーに従ったID、パスワード設定やパスワードの定期的な変更などの運用が可能です

02

国内の法制度やプライバシーマーク制度に対応した統合ID管理を実現！

◆プライバシーマーク制度で求められている職務権限に対応したアクセス範囲の設定や最新の状態で
個人情報管理が可能です
◆改正個人情報保護法で拡大された保有個人データの開示、利用停止等の範囲にも対応します
◆履歴管理によるユーザの操作証跡を監査できるようにします（国内版SOX法が求めるトレーサビリティに対応）

03

ID運用の統合化による管理運用コストの低減！

◆ID変更による各システムへの登録・変更作業が一度に可能です
◆新しいシステムを構築するときに、独自IDを管理する必要がありません

認証基盤ソリューションVANADISの製品概要を以下に記します。

①認証基盤機能 VANADIS® Identity Manager

統合ID管理サービス

企業内で管理するID情報やアクセス権限の
承認プロセス等を一元管理しアクセス権を統一します。

ID及び権限の登録や人事マスターとの連携、
認証機能との連携などが可能です。

- **一元管理による運用コスト削減**
- **短期間の構築が可能**
- **日本企業に合わせた効果的なID管理運用**
- **多用なシステムとの連携**

②シングルサインオン機能 VANADIS®SecureJoin

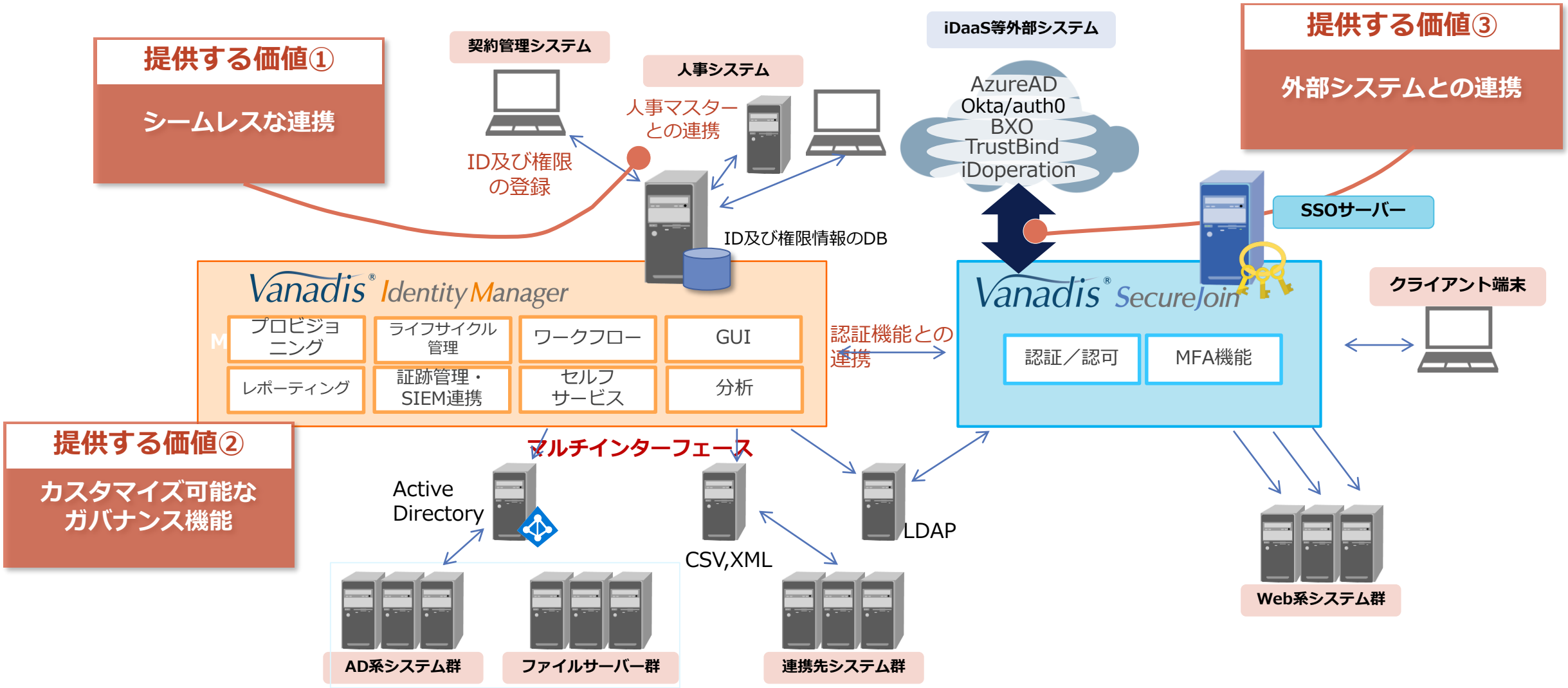
認証/認可サービス

ユーザが本人であるかの確認を実施し、ID情報を基に
アクセス権を付与します。

各業務システムに組み込まれたSSOエージェントにより、
認証及びアクセスログを記録します。

- **パスワードが一本化されユーザの利便性UP**
- **少ない既存環境の変更で導入可能**
- **ログ管理によるセキュリティ管理向上**
- **多要素認証によるセキュリティ強化**

認証基盤システム全体イメージ図を以下に記載します。



02

認証基盤システム
VANADIS Identity Manager

認証基盤システム Vanadis® IdentityManager の特徴

01 純国産のID管理製品として、
日本独自の商習慣をサポート

02 確立したフレームワークにより、
短期間での構築が可能

03 各種インターフェースに対応しており、
様々なシステムとの連携が可能

04 利用ユーザー数のみに依存する
シンプル・リーズナブルな料金体系

05 20年以上の運用実績による
信頼性の高いソフトウェア

総務省のシステムGIMAに導入！

ID・権限の一元管理から、マルチインターフェースまで

ID・権限の一元管理

ネットワーク上に分散配置する
複数システムのIDと権限を一元管理

プロビジョニング

利用者情報のメンテナンスを行う登録や
属性の変更に連動して、
必要に応じたイベントを自動的に実行

権限自動管理のイベントでは、接続する
各システムへ権限付与や停止などを自動実施

IDのライフサイクル管理

定期的なIDの棚卸し機能等により、
IDライフサイクル機能
（生成から消滅まで）を実現

証跡の記録とSIEM連携

現在のIDのステータスなどの出力や
IDの作成／廃棄、権限の付与／変更などの
記録とレポートを作成が可能

SIEM連携による分析機能の提供

GUIによる管理

GUIでの管理対象の選定や
フォーマット作成が**お客様側でも可能**

SEによるカスタマイズ対応が不要になり
スムーズに管理設定の変更が容易に実現

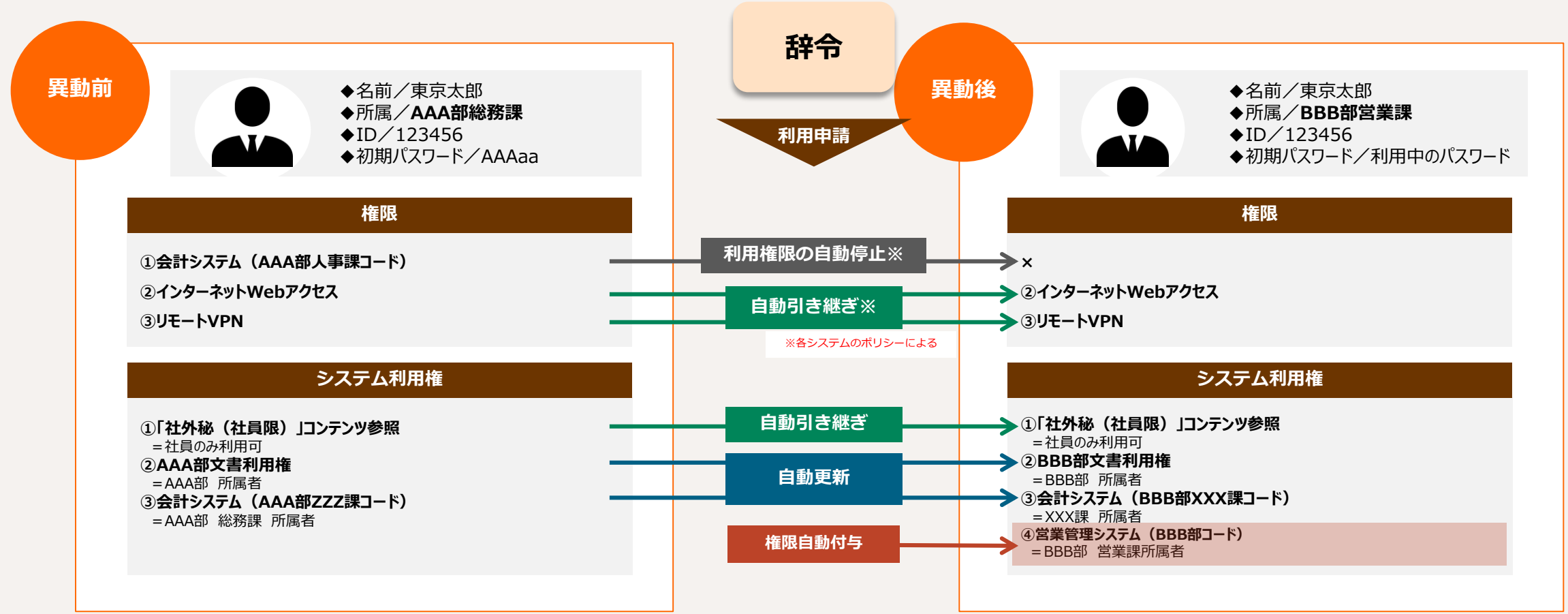
マルチインターフェース

RESTAPI、LDAP、ファイル（XML,CSV）等
主要な連携インターフェイスに対応しており
多種多様なシステムにおいて利用可能

登録や属性変更に連動し、イベントを自動的に行います。

プロビジョニングとは、**利用者情報のメンテナンスを行う登録や属性の変更に連動して、必要に応じたイベントを自動的に行う機能**です。
プロビジョニングの権限自動機能では、認証基盤に接続する各システムへの権限の付与や停止などの自動反映を実現します。

実行イベント例



2-5. VANADIS® Identity Managerの機能一覧

機能名		詳細
管理者支援機能	各種情報管理	利用者、組織、グループ、権限及びVIM内部で保持しているマスタ情報の各種新規登録、検索参照、変更及び削除を実施
	GUIシステム管理	人事データ等の情報設定やプロビジョニング設定、バッチ処理設定が標準機能でGUIによるユーザ設定が可能
	パスワード初期化、変更	管理者は管理している利用者のパスワード初期化が可能であり、利用者自身はパスワードの初期化、変更が可能
利用者支援機能	自身の情報管理	利用者自身の情報を確認、更新可能
	各種通知のメール送信	利用者に対する各種通知をメールにより送信可能
システム連動	AD・LDAP連動	利用者情報（パスワード情報、権限情報、及び所属グループを含む）をAD及びLDAPに連動可能
	XML・CSVファイル入出力	利用者情報、権限情報等をXMLファイル、及びCSVファイルにて指定ディレクトリへの入出力が可能 （外部システムとのファイル授受などに使用）
	RESTAPI、SOAP対応	RESTAPI、SOAPによって外部システムと利用者情報、権限情報等の提供・取込が可能 （既存の人事情報管理システムから人事情報の入出力する際などに使用）
	Web・SSO連携	VANADIS®SecureJoin等のシステムと連携してWebシステムへのシングルサインオンを実現可能
プロビジョニング	ライフサイクル管理	利用者情報の棚卸しや事前に設定した期日に応じて定型処理やID有効化／無効化、利用権の設定等を自動的に実施
	権限自動管理	利用者の増減、属性の変更に連動して、接続する各システムへの権限の付与や停止などを自動的に実施
申請ワークフロー		Webメニュー及びワークフロー機能により利用者の権限変更申請及び管理者の審査・承認が可能 ワークフロー機能部分をローコード開発で作成することも可能
証跡監査･レポート機能		現在のIDの状態（生存ID、休止ID、権限設定状態等の出力やIDの作成／破棄、権限の付与／変更）などの 記録及びレポート出力が可能

03

シングルサインオンシステム
VANADIS SecureJoin

シングルサインオンシステム Vanadis® SecureJoin の特徴

01

ハイブリットなSSO方式により
規模やSSO先サーバ/OSに依存せずSSOが可能

02

SecureJoin機能のみに絞った料金体系によって
より安価に利用が可能

03

統合Windows認証、MFAといった
複数の認証方式をサポート

04

VIMと同じく20年以上の運用実績による
信頼性の高いソフトウェア

既存システムに柔軟に対応し、シングルサインオンを実現

独自方式

独自方式**エージェントインストール型**
リバースプロキシ方式を用い、
導入・運用コストを抑えた構築を実現

独自方式では一般的な２つのSSO方式が
組み合わさり、双方のメリットを両立

外部サービスとの連携

- ActiveDirectoryを代表に**様々なID管理サーバを認証レポジトリとして利用可能**
- 統合Windows認証を用い、**Windowsログイン時に業務システムへの自動ログイン**を実現
- クラウドサービス（**SAML, OIDC対応**）へのSSOを実現

構成の多様性

多様な構成を組むことができ、
既存システムの変更を抑えた導入が可能

- 既存認証システムとの連携
- マルチドメイン対応
- ID統合がなされていない環境への対応

多要素認証

OTP・ICカード・USBデバイス・指静脈などの
認証情報による多要素認証でより安全な認証を実現

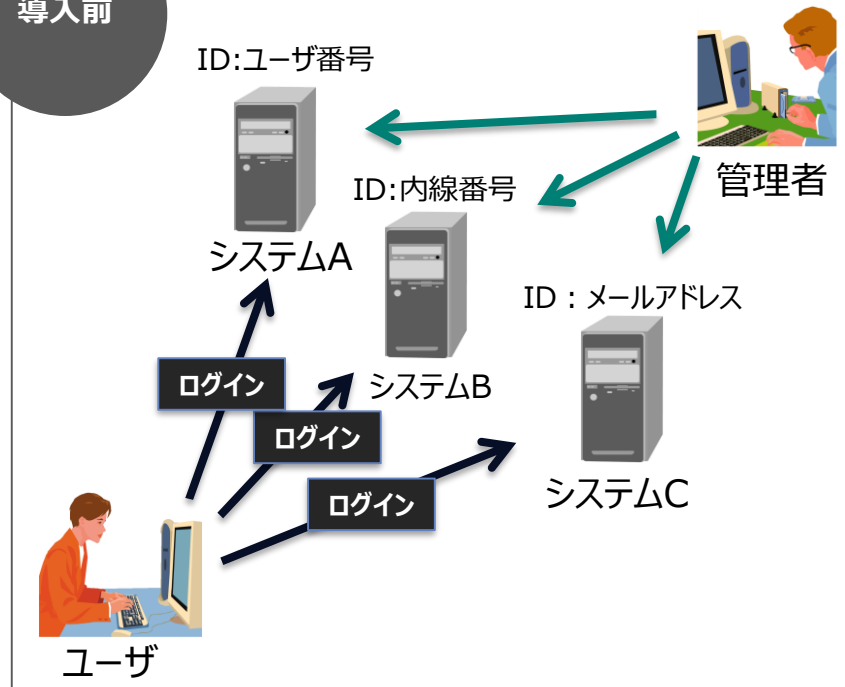
株式会社 NTT データのOTPサービス、**BizXaaS®**
Authenticationに標準対応

※ OTP：ワンタイムパスワード

既存システムへのアクセス制御を一元化し、SSOを実現します。

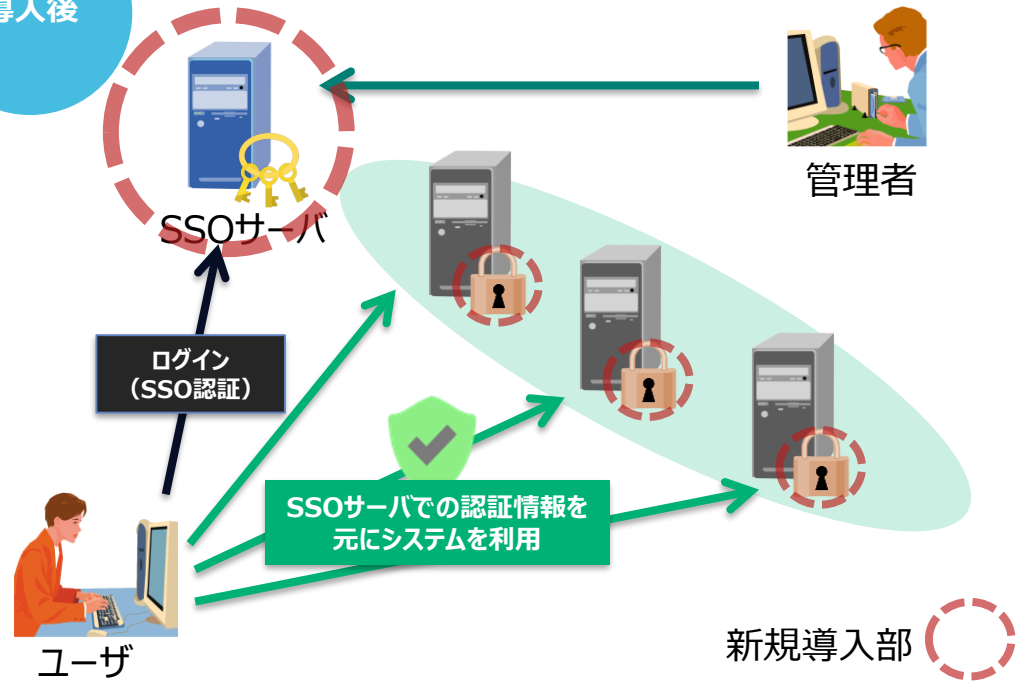
一般的なSSO実現手法である「エージェントインストール方式」と「リバースプロキシ方式」を組み合わせた独自方式である
「エージェント型リバースプロキシ方式」を用いて、既存のネットワーク構造に手を加えることなく導入でき、
負荷分散によりレスポンスの良いSSOを実現します。

導入前



ユーザー	管理者
業務システムごとに異なるIDでログイン	業務システムごとにユーザー管理

導入後



SSOサーバ（SecureJoin®）

ID/パスワードの検証を行い、アクセスチケット（ユーザ情報を持つCookie）を払い出すサーバ。ユーザ情報管理も行う。

SSOエージェント（SecureJoin®）

SSO対象のシステムへ導入するアクセスポイント。単体でリバースプロキシとして動作するため、導入が容易。

ユーザー	管理者
一度SSOサーバで認証後、追加認証不要	SSOサーバでユーザー情報を一元管理

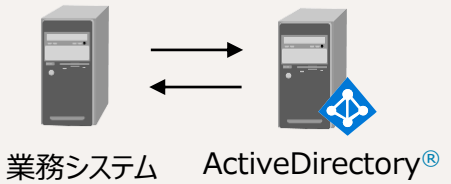
多様な外部システムと連携し、より効率的なSSOを実現します。

既存のActiveDirectory®の利用や、統合Windows認証を使用した自動ログイン・クラウドサービスへのSSOに対応しており、
高い経済性・利便性を実現します。

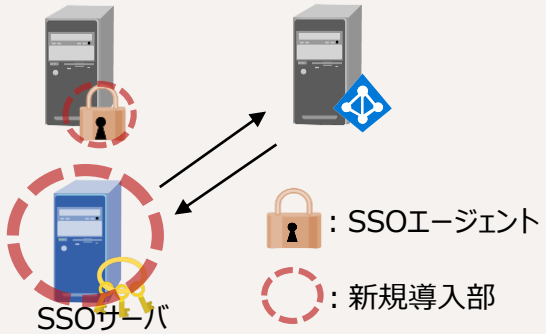
ActiveDirectory®

SecureJoinはActiveDirectory®やLDAPサーバを認証時のレポジトリとして利用することができるため、既存ユーザ管理サーバがSecureJoinに対応している場合、導入コストを抑えることが可能です。

・導入前



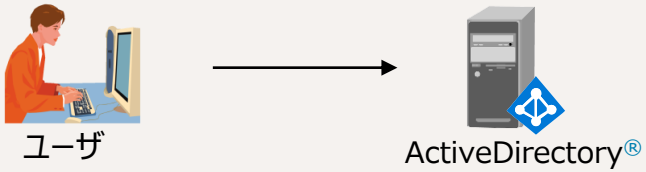
・導入後



統合Windows認証

統合Windows認証を使用し、Windowsのログオン時に自動的にSSO認証を行うことで、よりスムーズなシステムへのアクセスをサポートします。

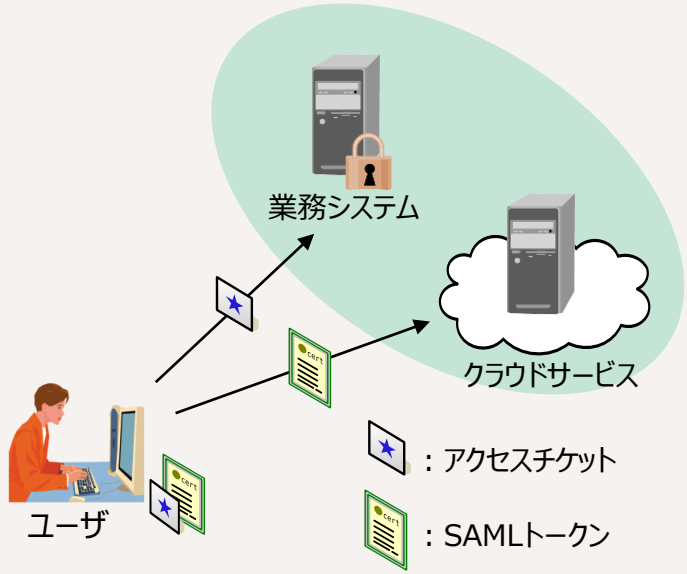
①Windowsログオン



②業務システムへアクセス可能（自動認証）

クラウドサービス

SecureJoinはSAML認証に対応する外部サービスとの連携が可能です。インターネットドメイン間でユーザ認証を行なう標準規格であるSAML認証を通じ、多様なクラウドサービスとオンプレミスの業務システム間でのSSOを実現します。



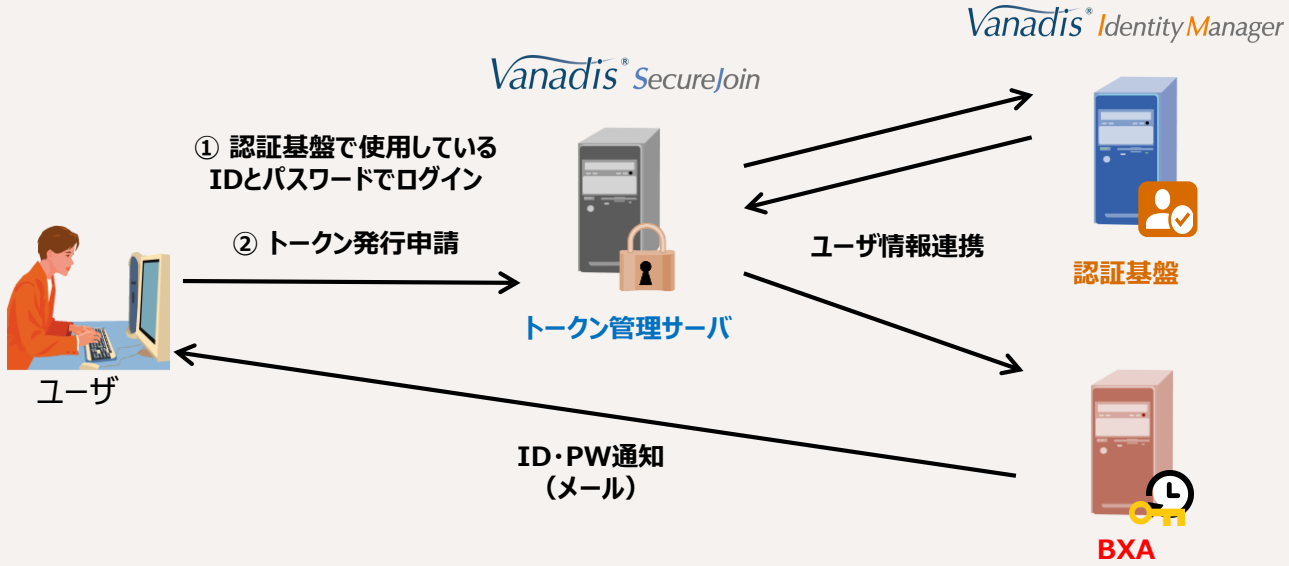
BXAとの連携により、スムーズな多要素認証の導入を実現します。

株式会社 NTT データが提供する、ワンタイムパスワード／トランザクションサイニングによる本人認証サービス
「BizXaaS® Authentication」に標準対応し、多要素認証をスムーズに実現します。

利用申請

① トークン管理サーバにログインし、BXA連携に必要なトークンの発行申請を行います。トークン管理サーバはVIMと連携しており、通常使用しているIDとパスワードでログインが可能です。

② ログイン後はトークンの発行申請を行います。VanadisとBXAが連携し自動でBXAアカウントが生成されるため、スムーズな申請が可能です。申請完了後、BXAで使用するIDと初期パスワードがメールにて送付されます。



BXA設定

① 端末にアプリケーションをインストールし、メールで受け取ったIDと初期パスワードでログインします。

② 初回ログイン時に求められる初期設定を済ませると設定完了です。

3-6. VANADIS® SecureJoinの機能一覧

機能名		詳細
シングルサインオン（SSO）	マルチドメイン機能	複数のドメイン（例.test.co.jp,test.com,Ttest.co.uk）間で、SSOを実現可能
	Windows統合認証機能	Windowsログオン時の情報をもとに、業務システムへのSSOが可能
	シングルサインアウト機能	複数ドメインでの運用をしていても一度で全てのドメインからログアウト可能
	ユーザ属性情報連携機能	アクセスしてきたユーザの属性情報を、アクセスチケット(Cookie)により業務システムへ提供する機能
	プラグイン機能（オプション）	エージェントプラグインを作成し、任意の業務システムに対して柔軟に接続可能
	クラウド連携機能（オプション）	SAMLを用いてクラウドサービスとのSSOが実現可能
認証・認可	標準認証	IDとパスワード、電子証明書、ICカード、統合Windows認証によりユーザ認証が可能
	カスタム認証	カスタムモジュールの作成により、標準方式に準拠しない任意デバイスでのユーザ認証が可能
	高度ACL機能	複数条件の指定により、複雑なアクセスコントロールリスト（ACL）での認可を行うことが可能
認証データベース	LDAP認証	LDAPサーバと接続し、認証及びユーザー情報の取得が可能
	PKI認証	CA証明書およびCRLを使用してユーザ認証が可能
	カスタム認証用データベース	外部データベース接続用のモジュールの作成により、任意のデータベースを認証用リポジトリに使用可能
セキュリティ	アクセスチケット保護機能	アクセスチケットは暗号化され、証明書を使用して改ざんを防止されている また盗聴しリプレイされたとしてもIPアドレスチェック機能により異なるIPアドレスのアクセスを拒否することが可能
	SSL機能	SSOサーバ、エージェントともにSSLをサポートしており、エージェントとWebシステム間でもSSL化が可能
証跡監査		誰がいつ認証したかのアクセスログを取得可能であり、同様に誰がいつ業務システムを利用したかの認可アクセスログも取得可能

04

実績

高度なID管理が必要なお客様にたくさんのご利用をいただいています。

社名／システム名	ユーザー数	備考
総務省 政府職員認証基盤システム	450,000人	・認証基盤を中心とした各省庁システムの横断的な最適化を実現。 ・省庁内システムのSSOを実現。
A保険会社 総合認証基盤システム	60,000人	・携帯電話による社内メール閲覧。
B自治体	50,000人	・ポータル製品と組み合わせSSOを実現。
C製造会社 個人認証基盤システム	35,000人	・グループ会社（グローバル含）の統合ID管理基盤を実現。 ・多様な方式でのデータ連携を実現。
NTTデータ 全社認証基盤システム	30,000人	・認証基盤を中心とした社内システム全体最適化を実現。 ・約300システムのSSO化を実現。
D通信会社	30,000人	・社内システムのSSOを実現。

ユーザ数、数千～数万の規模のお客様中心にご利用いただいています。

社名／システム名	ユーザー数	備考
E銀行 統合ID管理システム	30,000人	・社内システムのSSOを実現。
F自治体	15,000人	・庁内システム内のSSOを実現。
G会社	10,000人	・ポータル製品「intra-mart」と組み合わせてSSOを実現。
H広告会社	8,000人	・社内システムのSSOを実現。
I自治体 職員認証基盤システム	4,000人	・認証基盤を中心とした庁内システムの横断的な最適化を実現。 ・庁内システムのSSOを実現。
J通信社 ID管理システム	3,000人	・統合ID管理基盤の構築、携帯電話からの社内システムアクセスを実現。
K通信会社	3,000人	・社内システムのSSOを実現。

NTT DATA

Trusted Global Innovator