Customer Confidential

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
ソリューション事業本部
第三ソリューション事業部

御社で、以下のようなお困りごとはございませんか？

- □ システムのID管理が、放置状態になってしまっている
- □ システムの管理が部門ごとに分かれており、効率が悪い
- □ 幽霊IDがあり、重要な企業情報の流出リスクが気になる
- □ ID管理システム導入の必要性はわかるが、予算の都合でできない
- □ ID管理製品は海外製品が多く、自社に適応できるか不安
- □ 日本版SOX法やプライバシーマーク制度のレベルに達していない
- □ 新しいシステム構築のたびに、独自IDが発生している

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。

①不適切なID管理が引き起こすセキュリティリスクを防ぐ

◆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適性な運用が可能です

②日本版SOX法やプライバシーマーク制度での統合ID管理機能実現

◆職務権限に対応したアクセス範囲、権限のレベルを定める必要があります
◆IDの発行や変更、削除の承認プロセスを確立し、履歴管理により、後から監査できるようにします

③ID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

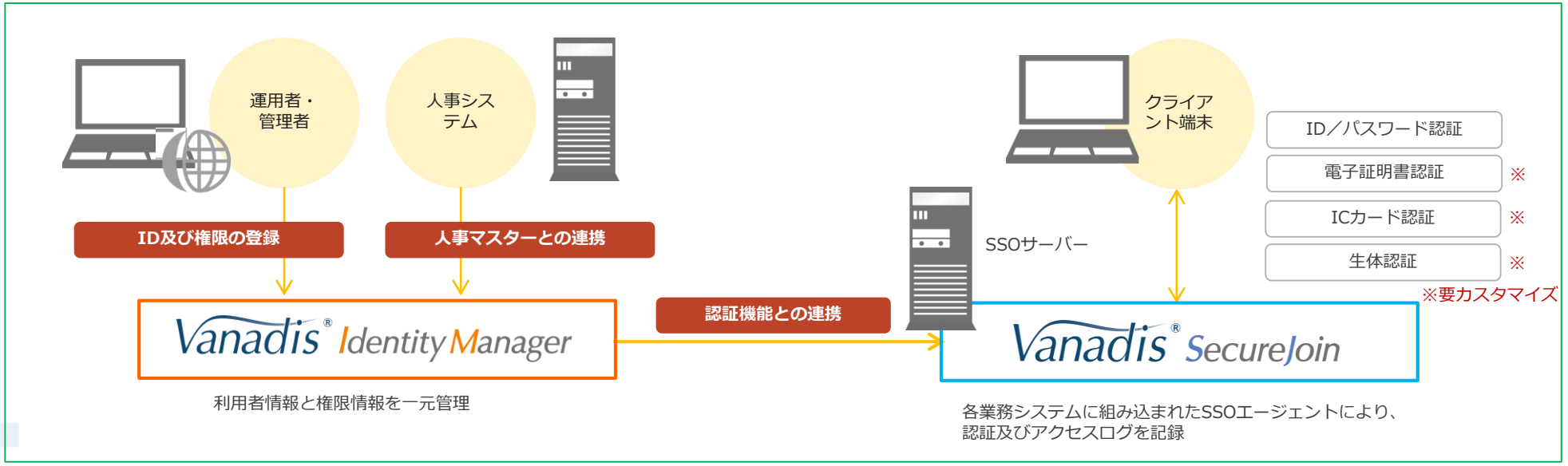
認証基盤ソリューションVANADISの製品概要を以下に記します。

①認証基盤機能→VANADIS® Identity Manager

運用負荷・コスト削減	セキュリティリスクの低減	効果的なITリソース投資
個々に管理を行っていた作業を一元化することで、運用コストを劇的に削減できます。	セキュリティ対策（パスワード変更等）を厳格化することができ、リスク低減できます。	個々の認証機能を一元化することで、各システムの認証機能をなくし、スリム化します。

②シングルサインオン機能→VANADIS®SecureJoin

作業効率＆利便性向上	セキュリティ強度の向上	厳密なセキュリティ管理
一度の認証通過で、アクセス権のある全てのWebページにアクセス可能になります。	ICカード、USBキー等を使用した認証に対応し、SSOの実現とセキュリティ強度を両立。	認証ログの一元的な取得が可能となり、不正なアクセス検出が容易となります。



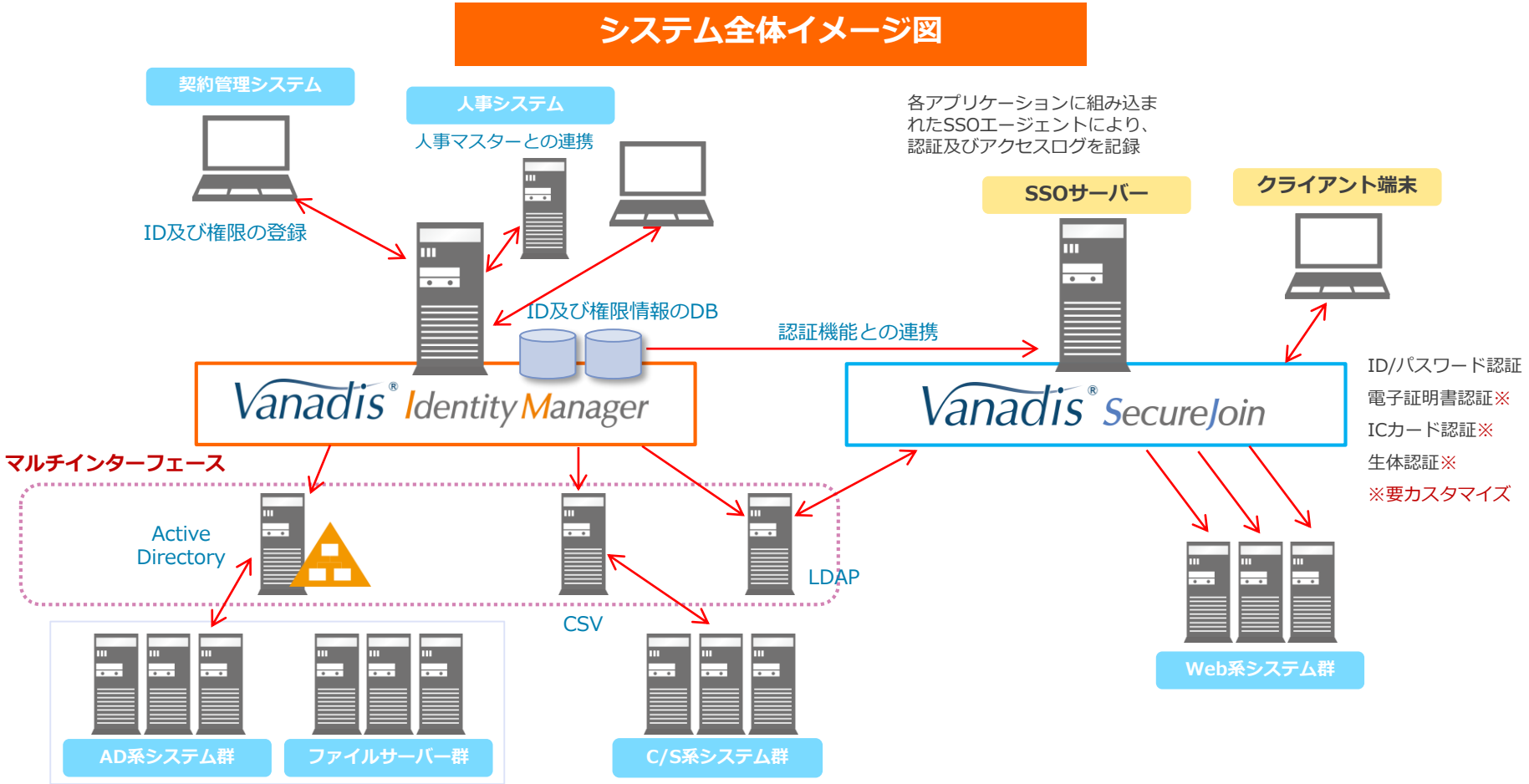
認証基盤ソリューションVANADISの概要は、以下の通りです。

認証基盤システム（VANADIS Identity Manager）

- 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します
- 様々なシステムとの連携を可能とするインターフェイスを搭載
- 確立したフレームワークにより、短期間での構築が可能
- NTTデータの自社ソフトがベースのため、ライセンス費用も安価
- 10年以上の運用実績による信頼性の高いソフトウェアです

→総務省が導入を決めた職員等利用者共通認証基盤（GIMA）で採用！

認証基盤システム全体イメージ図を以下に記載します。



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と権限を一元管理する

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行う。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的に行う

セルフサービス

エンドユーザーが自分自身でパスワードのリセットやプロフィールの変更が可能に。ヘルプデスクへの過剰な問い合わせなどを防ぐ

証跡の記録

現在のIDの状態（生存ID、休止ID、権限設定状態）などを出力。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

IDのライフサイクル管理

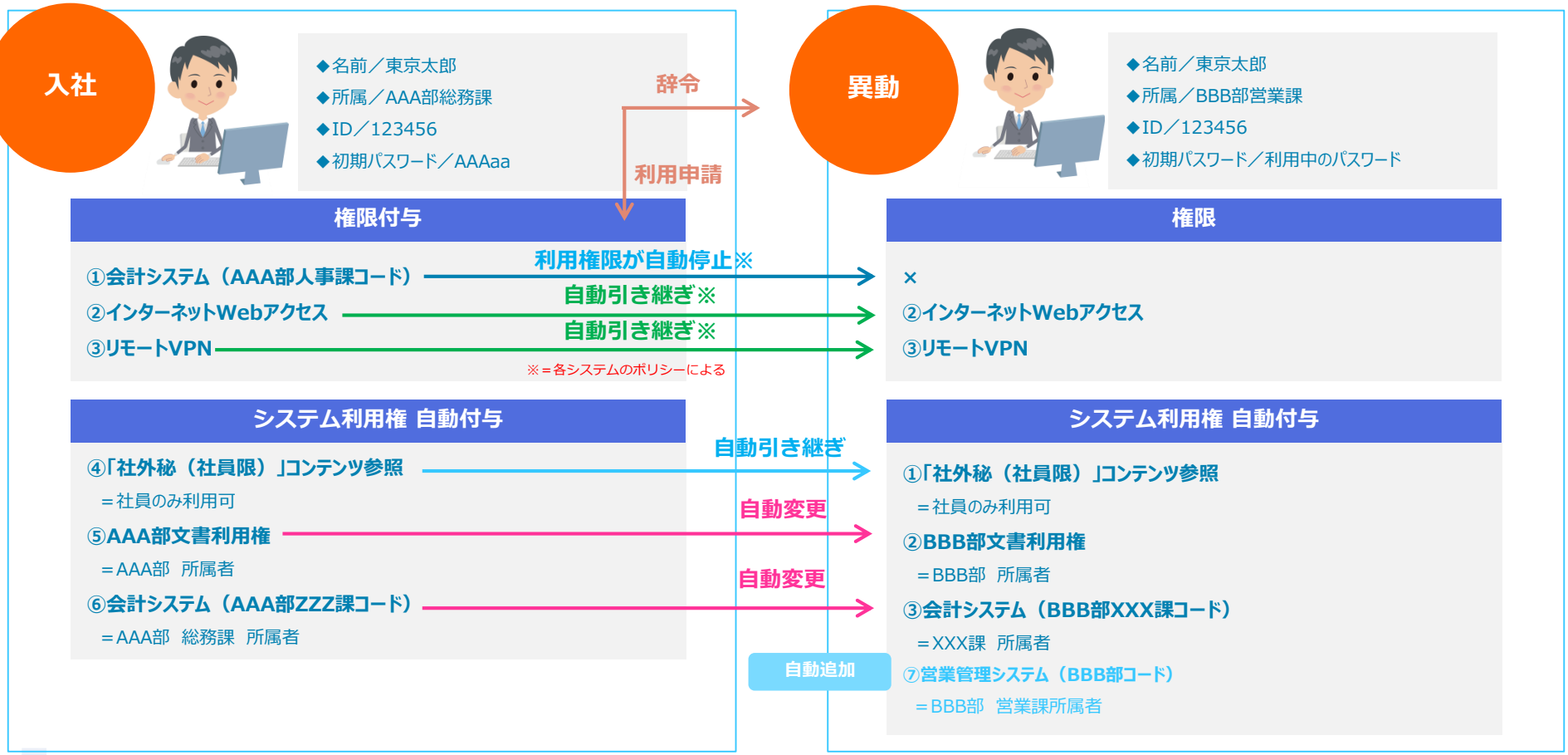
定期的なIDの棚卸し機能等により、IDライフサイクル機能（生成から消滅まで）を実現する

マルチインターフェース

LDAP、SOAP、ファイル（XML、CSV）等、主要な連携インターフェイスに対応することで、多種多様なシステムにおいても利用可能

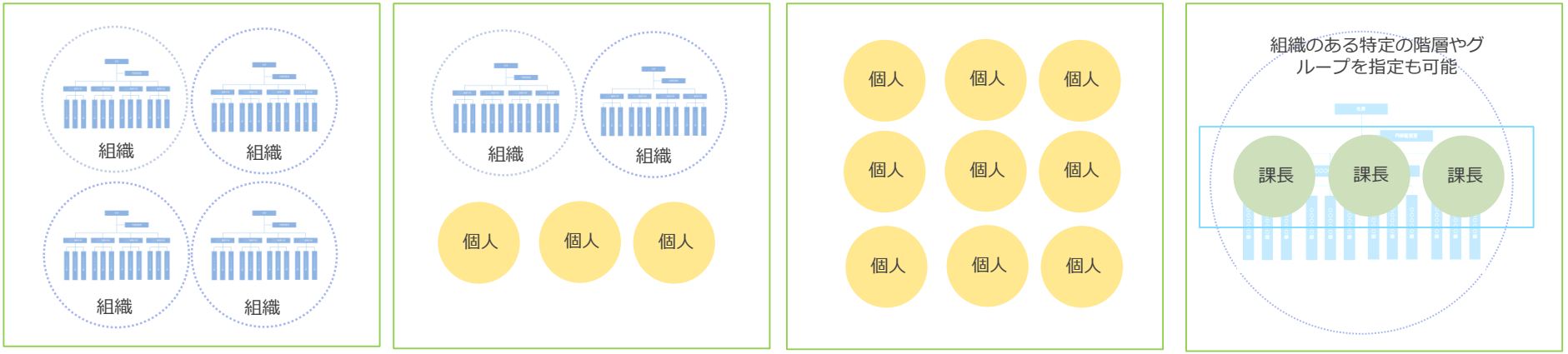
登録や属性変更に連動し、イベントを自動的に行います。

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。



権限設定は、人、役職、組織の他に、グループ指定が可能

権限設定については、人、役職、組織のほかにグループを定義できるようにすることが必要と考えています。



システムへのログイン権付与の方法

人	個人を特定して、ログイン権限を付与
グループ	プロジェクトやWGなど、人事システムで管理されていない任意の「人」の集まり／人や組織、特定役職の集まり
組織	特定組織に対しての、ログイン権限の付与
役職	特定役職に対しての、ログイン権限の付与

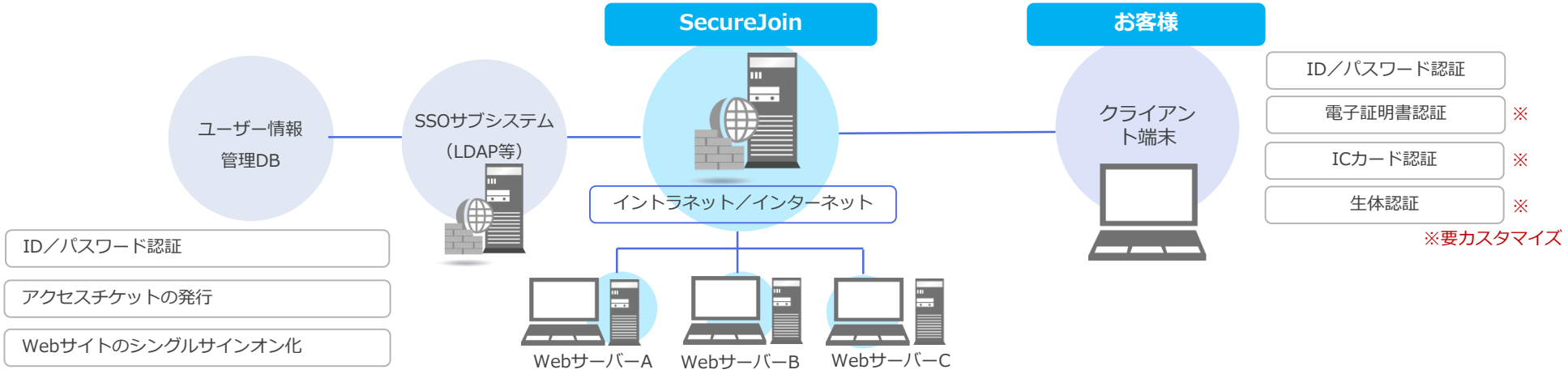
2-4. VANADIS® Identity Managerの機能一覧

機能名		詳細
管理者支援機能	利用者情報管理	利用者の新規登録および、利用者情報の検索参照、変更、削除を行う
	権限情報管理	権限の新規登録および、権限情報の検索参照、変更、削除を行う
	グループ情報管理	グループの新規登録および、グループ毎にその属性情報の変更とメンバーの追加、変更、削除を行う
	組織情報管理	組織の新規登録および、組織情報の検索参照、変更、削除を行う
	マスタ情報管理	VIM内部で保持しているマスタ情報の参照および、追加、変更、削除を行う
	パスワード初期化	利用者自身または管理者が管理する利用者のパスワードの初期化を行う
利用者支援機能	パスワード変更	利用者自身のパスワードの変更を行う
	セルフサービス	本人の情報を確認し、更新する機能
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に連動する
	XML・CSVファイル入出力	利用者情報、権限情報などを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を行う（外部システムとのファイル授受などに使用）
	SOAP提供・取込	外部システムからSOAPによる利用者情報、権限情報などの提供および取込を行う。（既存の人事情報管理システムなどからVIMのSOAP提供・取込機能による人事情報の入出力などに使用）
	Web・SSO連携	VANADIS®SecureJoinと連携してWebシステムへのシングルサインオンを実現
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および、イベントに応じて定型的な処理を自動的に行う機能
	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行う
	タイマー機能	あらかじめ設定した期日に、IDの有効化／無効化、利用権の設定を自動的に行う
共通機能	ユーザー通知	利用者に対する各種通知をメールにより通知する
	ログ出力	ログを採取し出力する
	Webオンラインメニュー	利用者が所有するVIM利用権限の変更に対する申請を行い、管理者が審査・承認を行う
申請ワークフロー（オプション）		利用者がアクセス権の変更に対する申請を行い、管理者が審査・承認を行う
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／変更などの記録とレポートを作成する

エージェント型リバースプロキシ方式で容易な導入運用が実現

SecureJoinは、弊社が開発したWebのシングルサインオン製品で、広範囲なアプリケーションに適用できます

シングルサインオンのイメージ



特　徴

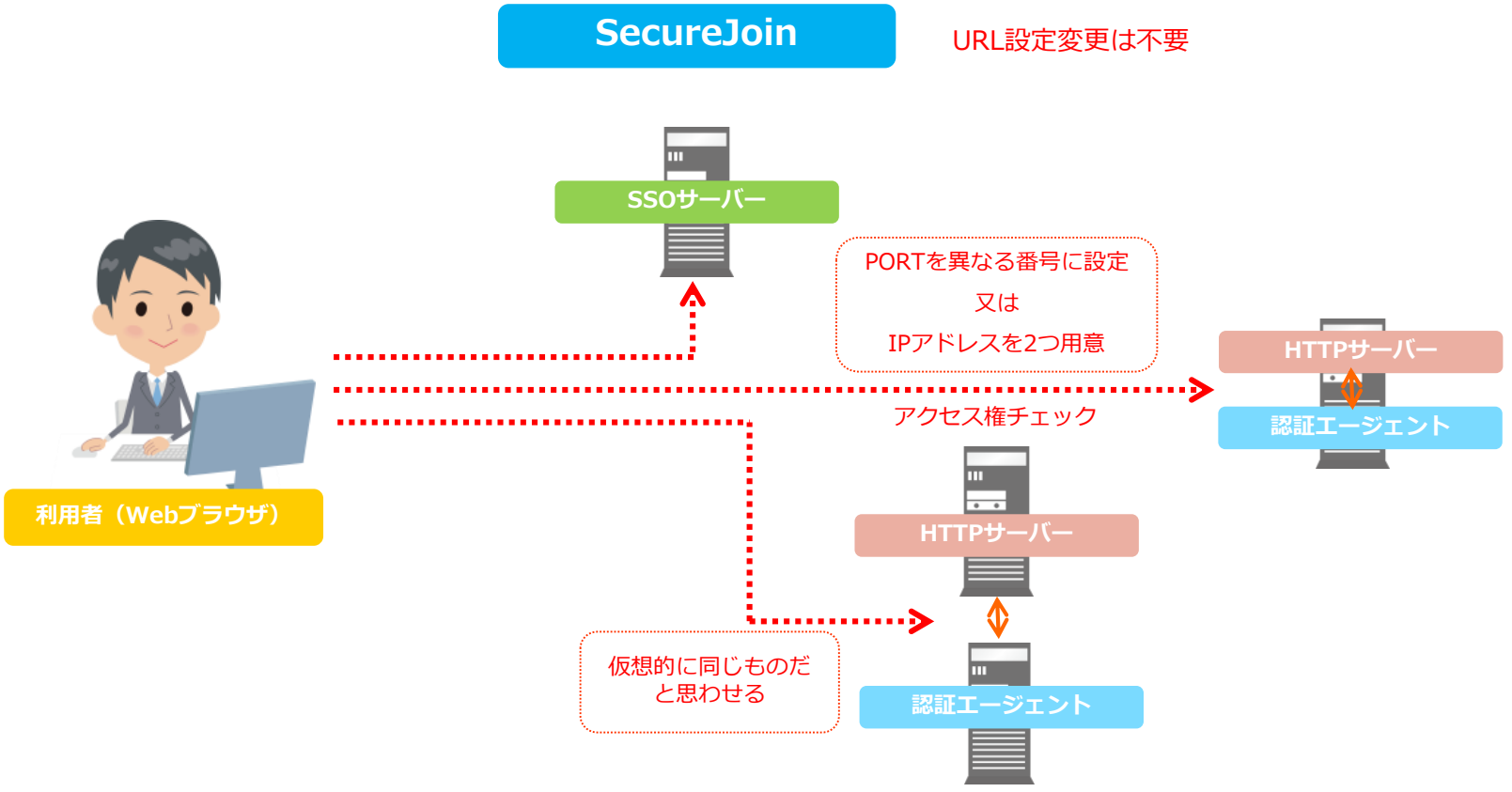
◆Webサーバーの OS、ソフトを選ばないため、既存システムからの移行がスムーズに実現します。
◆Webサーバーの分散配置構成に対応し、Webサーバ、ホストOSの種類を問わない汎用性の高いソフトウェアです。
◆特定部署等、サーバー単位での導入が簡単に実施できるため、段階を追っての導入が可能です。
◆PC及びバイオメトリクスでのシングルサインオンにも、対応しています。

「エージェント型リバースプロキシ方式」は、現在主流の方式の長所を持ち短所を改修した方式です

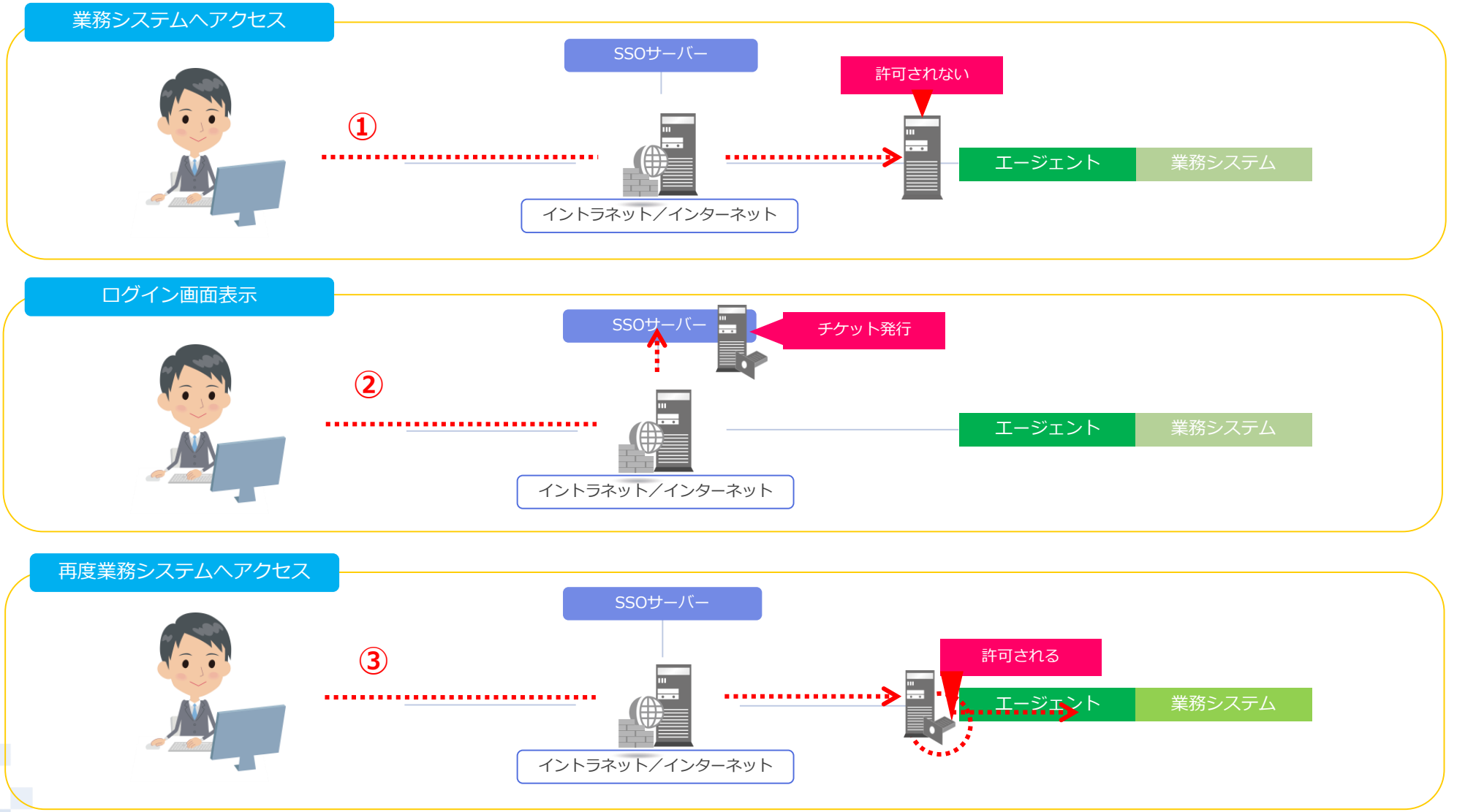
方式	実現方式	長所	短所
リバースプロキシ方式 （一般的な方式1）	・全ての通信負荷は、そこでアクセス制御を行う	・セキュリティレベルが高い ・エージェント不要 ・Webサーバーに制約を受けない ・ASPサービスに適用が容易	・認証サーバーに負荷が集中 ・全てのアクセスが認証サーバーを通る ・Webブラウザの設定が必要 ・大規模ユーザーに適さない ・Webサーバーの分散配置構成に適さない
エージェントインストール方式 （一般的な方式2）	・ユーザーの属性情報(部署、役職、メールアドレス等）を暗号化してアクセスチケット送信しWebサーバーの認証プラグインがアクセスチケットを元にアクセス制御を行う ・認証プラグインとWebサーバー間の通信はAPI	・負荷が集中しない ・各エージェントが直接アクセスを受ける ・大規模ユーザーに対応可能 ・Webサーバーの分散配置構成に対応可能 ・複数ドメイン対応が容易	・Webサーバー台毎に認証モジュールのインストールが必要 ・Webサーバーに制約を受ける
エージェント型リバースプロキシ方式 （NTTデータ方式）	・ユーザーの属性情報（部署、役職、メールアドレス等） アクセスチケットを送信し、認証モジュールがアクセスチケットを元にアクセス制御を行う ・SSOエージェントとWebサーバー間の通信はHTTPであり、いわば認証モジュールがプロキシとして動作する	・負荷が集中しない ・各エージェントが直接アクセスを受ける ・大規模ユーザに対応可能 ・Webサーバーの分散配置構成に対応可能 ・Webサーバー、ホストOSの種類を問わない ・Webサーバーに制約を受けない ・ASPサービスに適用が容易 ・複数ドメイン対応が容易	・Webサーバー台毎に認証モジュールのインストールが必要

「エージェント型リバースプロキシ方式」は、現在主流の方式の長所を持ち短所を改修した方式です

エージェント型リバースプロキシ方式

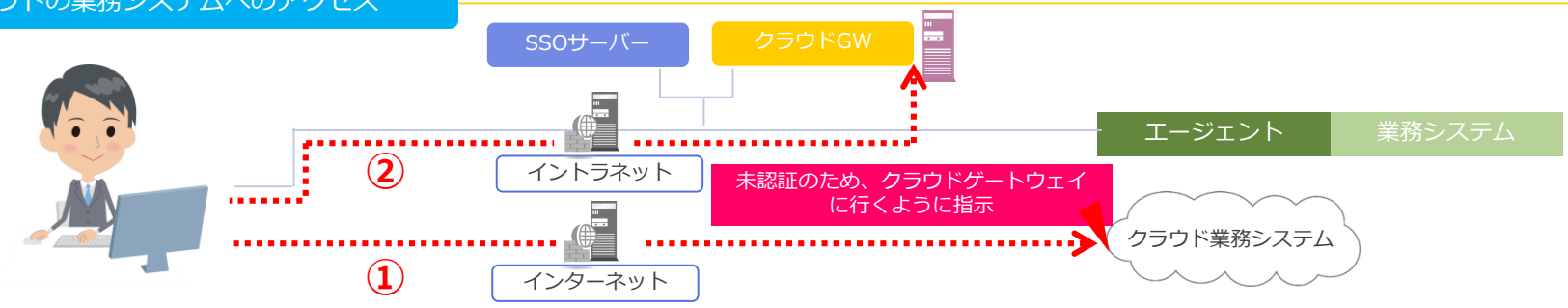


3-4. VANADIS® SecureJoin アクセスフロー

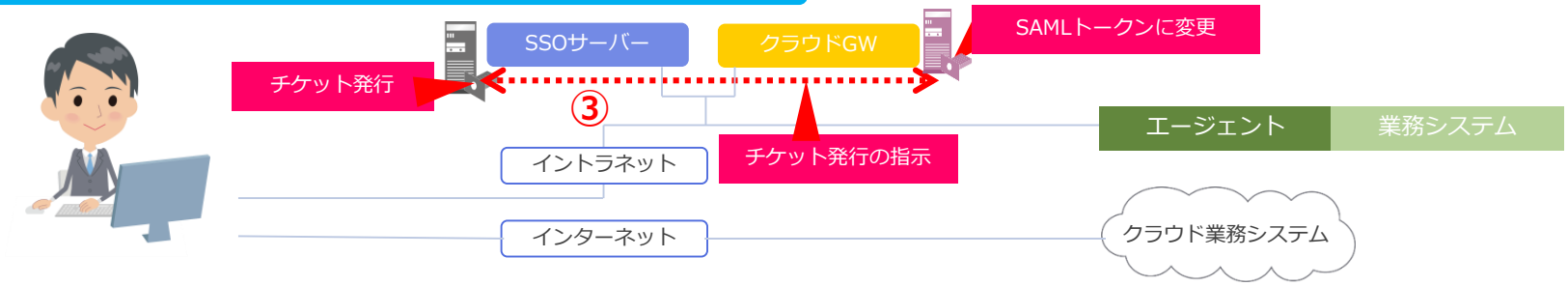


3-5.クラウド ゲートウェイ　アクセスフロー

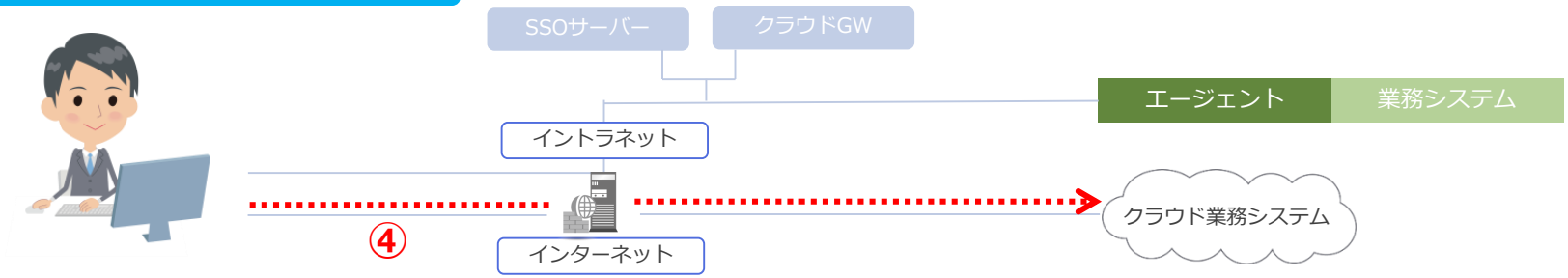
クラウドの業務システムへのアクセス



SSOサーバーがチケット発行後、クラウドゲートウェイでSAMLトークンに変更される



SAMLトークンで業務スタート



Windowsログイン状態→SecureJoin認証連携

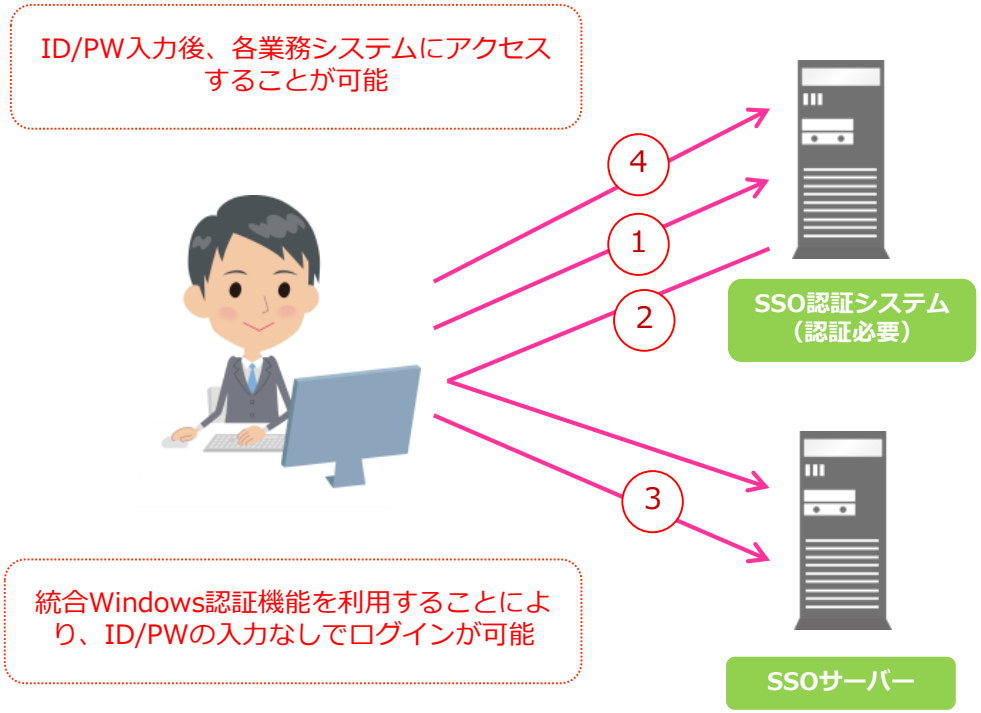
■WindowsログインSecureJoin認証連携

① SSO認証が必要なサイトにアクセス
② SSOサーバーにリダイレクトされる
③ 統合Windows認証機能を利用することにより自動ログイン
④ 新たにID/PWを入力することなく業務システムを利用できる

■注意点

統合Windows認証を利用するにあたり以下の制限がある

- ブラウザはIEに限る
- SSOサーバーへのアクセスにプロキシサーバを利用しない
- SSOサーバーをIEで「イントラネット」ゾーンに含める



3-7.VANADIS® SecureJoinの機能一覧①

機能分類	区分	詳細
シングルサインオン	エージェント型リバースプロキシ方式	・WebサーバーのOS、Webサーバ等に依存しない方式 ・大規模組織に段階的に導入が可能 ・異種Webサーバーが混在する環境への適用が可能 ※Webサーバーのシングルサインオンを実現（HTTPプロトコルが対象） ・C／S、メインフレーム等のSSO化対応は、SIが発生 ※連携するサーバーに「SecureJoin」のモジュールをインストールする必要あり ※パスワードは、LDAPに依存するため、既存のLDAPサーバーがあることが前提
	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を実現する機能
	Windows統合認証機能	Windowsドメインのログインをもって、WebのSSOを引き継ぐ機能
	シングルサインアウト機能	複数ドメインを運用していても、一度に全てログアウトできる機能
	情報提供機能	アクセスしてきたユーザーの情報を、アクセスチケット(Cookie)によりAPへ提供する機能
	エージェント独立機能	エージェントがサポートしないWebサーバーにおいて、エージェントを独立して設置できる機能
	プラグイン（要開発）	エージェントプラグインの作成により、任意のWebアプリケーションに対して柔軟性のある接続を行うことができる機能
認証	パスワード認証機能	アクセスしてきたユーザーをIDとPWにより、許可されたユーザーであることを確認する機能
	電子証明書認証機能	アクセスしてきたユーザーを電子証明書より、許可されたユーザーであることを確認する機能
	ICカード認証機能（PKI）	アクセスしてきたユーザーをICカードに格納された証明書により、許可されたユーザーであることを確認する機能
	生体認証機能	アクセスしてきたユーザーを指紋により、許可されたユーザーであることを確認する機能
	カスタム認証（要開発）	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のデバイスに対応させることが可能
認証データベース	LDAP認証機能	LDAPサーバーと接続して認証及びユーザー情報の取得を行う機能
	PKI認証機能	CA局の証明書によりユーザーを認証する機能、CA証明書およびCRLを使用
	カスタム認証（要開発）	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できる機能

3-8.VANADIS® SecureJoinの機能一覧②

機能分類	区分	詳細
認可	認可	アクセスしてきたユーザが、Webページにアクセスする権限を持っているか確認する機能
	高度ACL機能	複数条件の指定などにより、複雑なアクセスコントロールリストにより認可を行う機能
セキュリティ	改ざん防止機能	証明書を使用してアクセスチケットの改ざんを防止する機能
	SSL機能	SSOサーバー、AgentともにSSLをサポートする機能、エージェントとWebサーバー間もSSL化可能
	アクセスチケット暗号化機能	アクセスチケットを暗号化する機能
	IPアドレスチェック	アクセスチケットを盗聴し、リプレイしても、IPアドレスが異なれば拒否する機能
可用性	ログインサーバーのスケールアウト機能	ログイン量及び信頼性条件に応じてログインサーバーをスケールアウトできる機能
	負荷分散Webサーバ対応機能	負荷分散構成になっているWebサーバーに適用
運用機能	アクセスログ	アクセスログを取得する機能
	Web設定機能	Webインターフェイスによりエージェントの設定の変更が可能
	リモート設定	リモートからログの参照、エージェントの設定変更が可能
	テスト機能	任意ユーザによるログインを模すことでSSO対応アプリケーションのテストを支援する機能
オプション	認証連携	Liberty Alliance（SAML2.0）に対応し、複数のドメインにおけるSSO、同規格に対応した外部システムとのSSOが実現する機能
	VIM連携	VANADIS Identity Managerとの連携機能

認証基盤ソリューション分野でID数で国内トップシェアです。

事例	社名／システム名	ユーザー数	備考
1	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。
2	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。
3	B自治体	50,000人	・ポータル製品と組み合わせSSOを実現。
4	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。
5	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。
6	D通信会社	30,000人	・社内システムのSSOを実現。

構築実績以外にも、2万規模のID管理コンサルティング実績有

事例	社名／システム名	ユーザー数	備考
7	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。
8	F自治体	15,000人	・庁内システム内のSSOを実現。
9	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。
10	H広告会社	8,000人	・社内システムのSSOを実現。
11	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。
12	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。
13	K通信会社	3,000人	・社内システムのSSOを実現。

NTT DATA

Trusted Global Innovator