

アイデンティティ管理ソリューション

CSL  Guard

&

 ActCenter

NTTソフトウェア株式会社

<http://www.ntts.co.jp/>

<http://www.nttsoft.com/>

1. 製品のご紹介

2. ソリューションの機能

- 2. 1. シングルサインオン
- 2. 2. アクセス制御
- 2. 3. アカウト一括管理
- 2. 4. ポリシ権限管理

3. ソリューションの特長

- 3. 1. ソリューションのサマリー
- 3. 2. ソリューションの特長



4. 主な機能

- 4. 1. 利用者向け機能
- 4. 2. 運用管理者向け機能
- 4. 3. 運用管理画面

5. システム構成

- 5. 1. 全体製品モジュール構成
- 5. 2. システム構成例
- 5. 3. 対応プラットフォーム

1. 製品のご紹介

「アイデンティティ管理ソリューション」を構成する2つの製品群

“**CSLGuard** (コンソールガード)”



CSLGuardCS, CSLGuardWEB, CSLGuard Identity Manager

クライアント/サーバ系システム、Web系システムのシングルサインオン認証、アクセス制御環境を統一的に実現し、利便性の向上と統制環境構築を同時に実現します。

また、アクセスログの一元取得により、監査の容易性も高めます。

“**ACTCenter** (アクトセンター)”



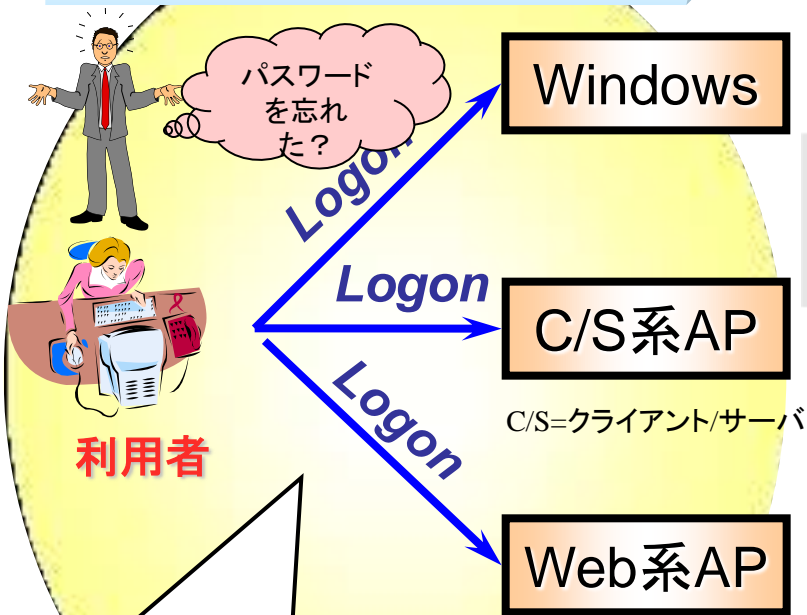
ユーザアカウントとアクセス権限を、所属組織などのポリシーベースで集中管理し、大量アカウント管理の容易化と運用コストの削減を実現します。

AD, UNIX, Windows, Linux, LDAP、Oracleなどに格納された多彩なアカウント情報の集中管理が行えます。

2.1 シングルサインオン CSLGuard

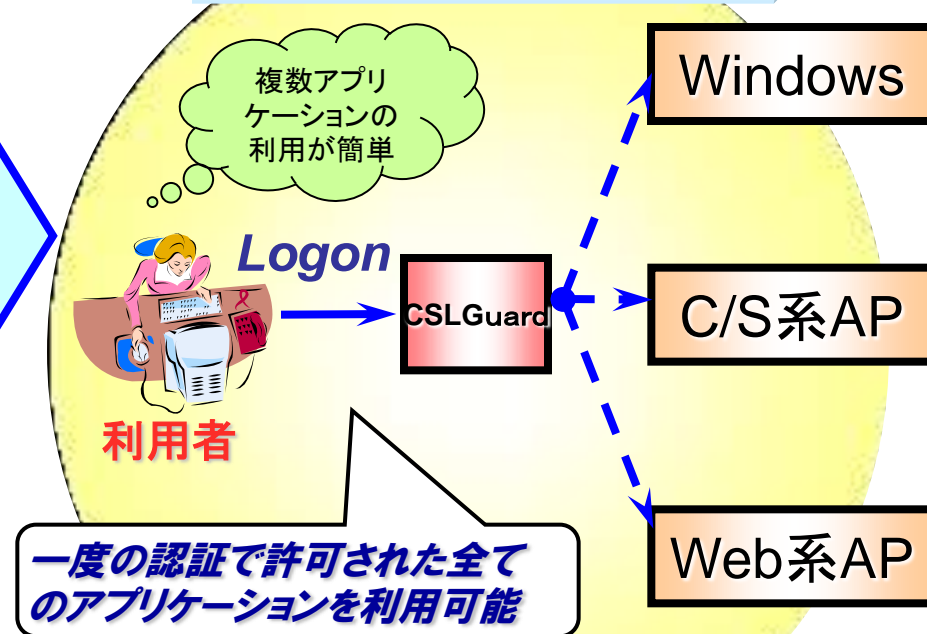
CSLGuardは、アプリケーションの認証を統合し、利便性と内部統制環境を実現します

通常のログイン



各アプリケーションごとにそれぞれのID/パスワードでログイン

シングルサインオン

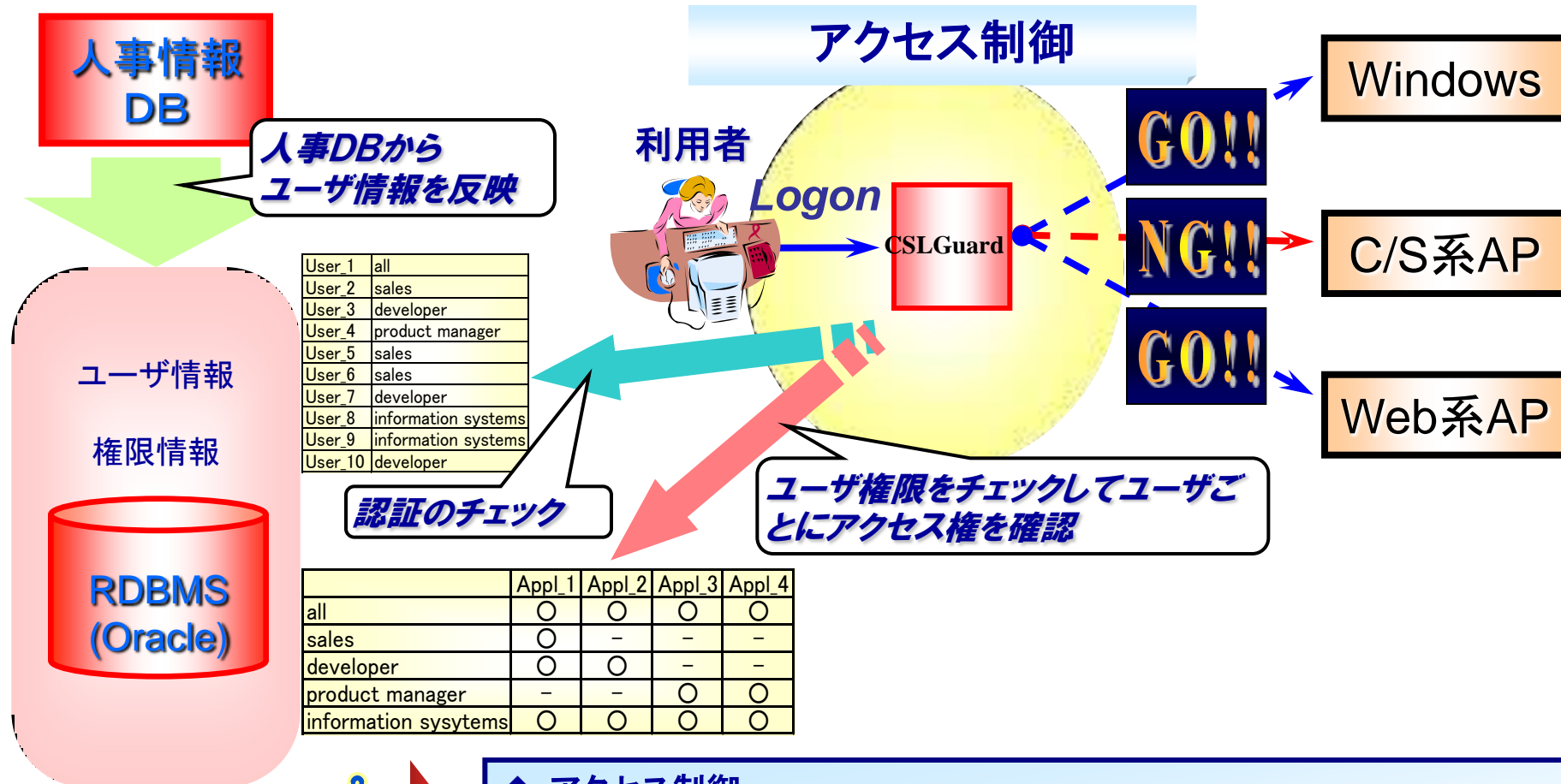


何ができる？

- ◆ アプリケーションの認証がひとつにまとまる
 - 利用者の利便性が高まり、**アクセス権限の管理も徹底**できる。
 - 認証のログが一元化でき、**監査もしやすい**。
- ◆ **クライアントサーバ系のアプリケーションも統合** (独自機能)
 - メタフレームやTelnetなども連携

2.2 アクセス制御機能 CSLGuard

許可された人が、許可されたアプリケーションのみを利用可能にします



何ができるのか？

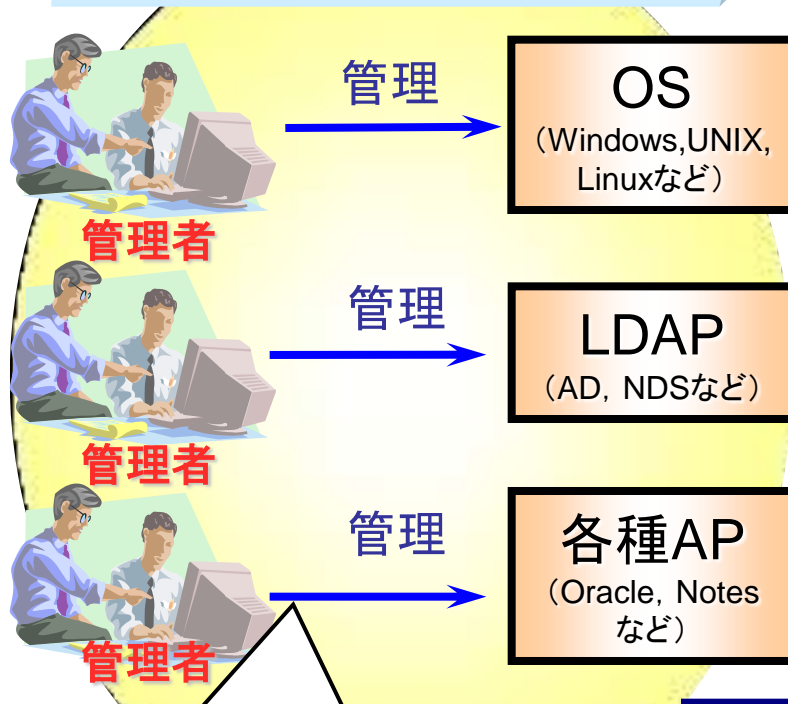
◆ アクセス制御

- (URLディレクトリ単位、アプリケーション単位で、属性にて権限振り分け)
- 権限のある人だけがアクセス可能
- アクセス権限管理の徹底で不正アカウントによる情報漏えいを防止

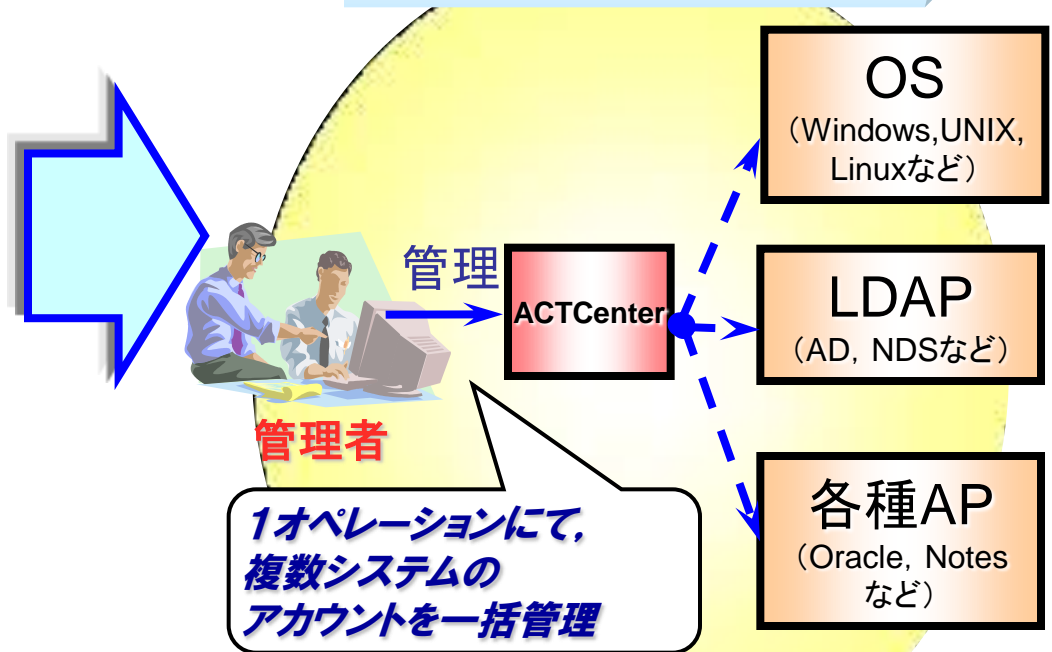
2.3 アカント一括管理 ACTCenter

ACTCenterは、アカウントを一括管理し、低コストで強固なセキュリティ基盤を築きます

通常のアカント管理



アカウント一括管理



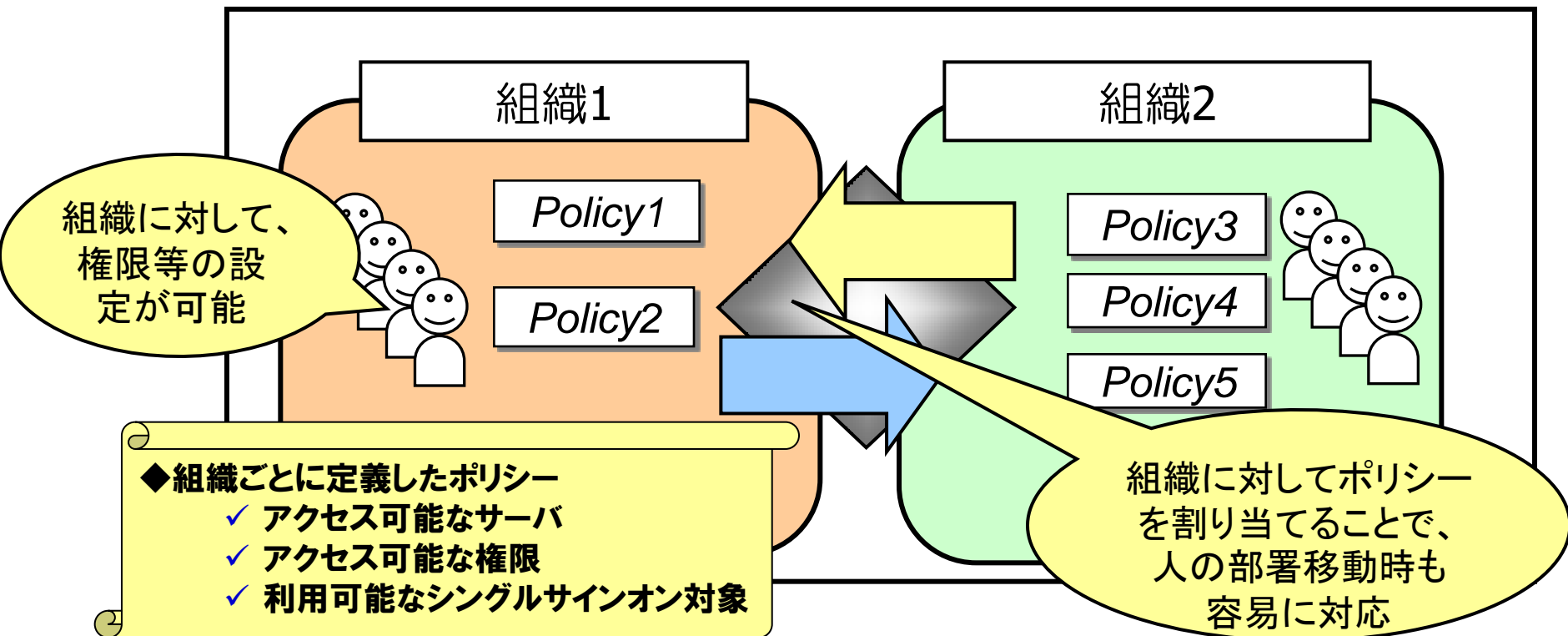
何ができるのか？

- ◆ アカント情報を一括登録, 変更, 削除
— 各サーバや業務アプリケーションの**アカウント運用が容易に**
— 一括管理で、**ゴーストアカウントを撲滅**
- ◆ スケジュール予約運用
— 人事異動等、多くの異動の場合、あらかじめアカウントの利用開始や削除を自動設定することで、運用負荷を軽減
- ◆ **管理アカウントと実アカウントとの自動差分調査(監査対応)**

2. 4. ポリシー権限管理

Mobile

組織を階層管理して、組織自体にポリシーを設定



何ができるのか？

- ◆ ポリシーごとに権限を設定
- ◆ **運用負担の削減を実現**
 - 組織ごとにポリシーを設定し、アクセスできるアプリケーション決定
 - 人事異動による**権限付け替えも瞬時に実現**
- ◆ ポリシーによる運用で、管理者はアカウントの管理・変更が楽になり**確実な管理を実現**

3. 1. ソリューションサマリー

CSLGuard (コンソールガード)

- ◆シングルサインオン (Web系、クライアント/サーバ系)
- ◆内部統制対応 (アクセス制御・監査ログ管理)

ID管理ソリューション

認証統合サーバ



ユーザ情報同期

ユーザ管理データベース

アカウント管理サーバ

アカウント連携



社内システム(サーバ)

人事システム

業務システム

グループウェアシステム

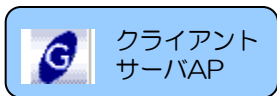
ネットワーク機器

DBMS (Oracleなど)
新たな管理対象群

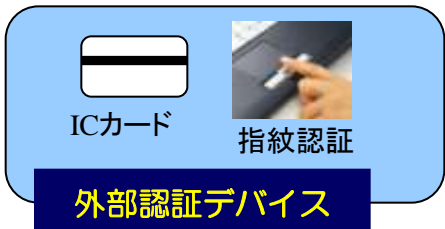
ACTCenter(アクトセンター)

- ◆アイデンティティ管理 (アカウント一括管理・スケジュール管理)
- ◆内部統制対応 (不正アカウントチェック)

ブラウザ/携帯端末



連携



ICカード

指紋認証

外部認証デバイス

3. 2. ソリューションの特長(1)

➤ 純国産製品、自社での万全サポート

- ◆ コールセンタの設置、顧客からのお問合せに対する迅速な対応
- ◆ お客様からのご要望を製品改善要求へと迅速に取り込み(カスタマイズ実績も多数あり)

➤ シングルサインオン、アクセス制御、アカウント管理をまとめて提供可能

- ◆ 設定により、CSLGuardとACTCenterの連携が容易
 - ◆ ACTCenterで管理するアカウントをCSLGuardのシングルサインオンで利用可能
 - ◆ CSLGuardでパスワード変更実施時、ACTCenterで管理するアカウントのパスワードも自動変更可能
- ◆ 運用者向け管理機能が充実
 - ◆ パスワードランダム変更機能(定期スケジュールの自動実行が可能)
 - ◆ アカウント監査チェック機能(ACTCenterで管理するサーバ上のアカウント差分チェック)

➤ シングルサインオン対象範囲が広い

- ◆ C/S系アプリケーション： Windows, 各種C/S系AP, telnetコンソール, 各種OS, 各種LDAP
- ◆ Web系アプリケーション： ブラウザのForm認証、Basic認証画面に対するSSO

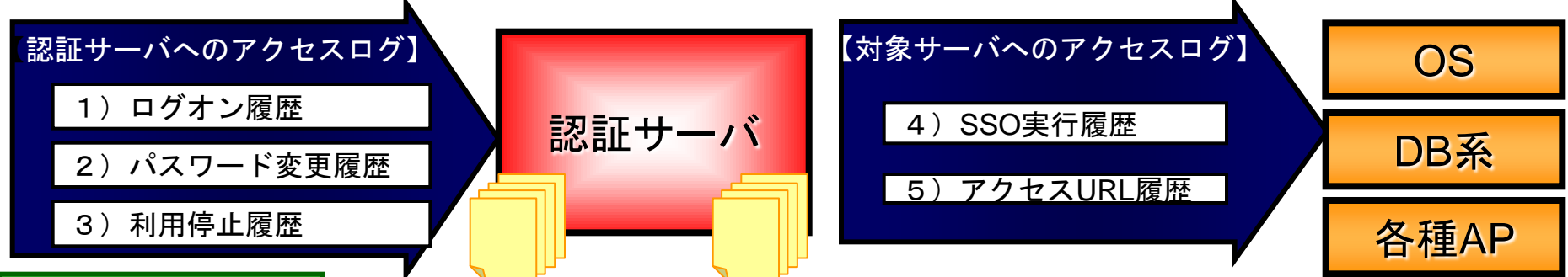
➤ 様々な認証方式、各種規約への対応に取組み

- ◆ X.509証明書認証対応、ICカード、指紋認証等との連携
- ◆ モバイル端末サポート
- ◆ Liberty Alliance, SAMLにも対応可能

3. 2. ソリューションの特長 (2)

▶ 監査ログ一元取得

◆ユーザ認証, SSO履歴, セキュリティ情報更新などの作業履歴を一括管理



1) ログイン履歴

結果（成功、失敗）とその理由
失敗時の理由内容

- ①ID/パスワード間違い
- ②設定されたログインポリシーに違反している
 - ・許可されたログイン有効期間をすぎている
 - ・許可された認証方式以外の方式でログインを試みた
例) 指紋認証のみ許可のユーザが、
ID,パスワードで認証を試みた等
 - ・ログインが許可された時間帯・曜日以外のログイン
 - ・ログインできる開始日以前のログイン
 - ・ログインできる期間の終了日をすぎた状態でログイン

2) パスワード変更履歴

シングルサインオンに用いるパスワードをユーザが変更をした結果（成功、失敗）とその理由

3) 利用停止履歴

パスワードポリシーに違反したユーザに対して利用停止を実行したログ

4) SSO実行（アプリケーションへのログイン）履歴

C/S系アプリケーションに対してSSOを実行した履歴
(Windowsへのログインを合わせて行う、一段認証の場合には、Windows端 未起動時の実行履歴が取得)

Web系APに対してBasic認証、Form認証SSOを実施した履歴

- ・誰が（認証後はシングルサインオンに用いたIDがログに記録される）
- ・いつ（日時 [YYYY/MM/DD hh:mm:ss]）
- ・どこから（職員PCのIPアドレス又はホスト名）
- ・どのシステムに（アプリケーションの識別名称）
- ・どのアカウントで（アプリケーションへのログインに使用したID）

5) アクセスURL履歴 【Web系のみ】

シングルサインオンサーバ（CSLGuardWEB）を経由してWeb系APへアクセスした際の、httpメソッド(GET,POST等)、URL履歴

3. 2. ソリューションの特長(3)

➤ 必要ファイルの自動配信

- ◆ SSO対象システム追加、バージョンアップなどにおけるファイル更新（CSLGuardCS Clientモジュール、スクリプトファイル）は利用者がCSLGuardへログオンすることで自動実行～端末への再配布などの運用コスト削減

➤ システムダウン時の利用継続機能 (キャッシュ機能)

- ◆ 認証サーバアクセス不可時における認証、シングルサインオンが継続可能 (過去の認証、シングルサインオン履歴を元を実施)

➤ スケジュール実行結果のメール通知 (ACTCenter SCM)

- ◆ スケジューリングによるアカウント管理の実行結果を指定されたメールアドレスへメール通知

➤ 抽出結果のPDF出力

- ◆ 一括処理のエクスポートによる出力結果及びターゲットの差分アカウント抽出結果をPDFファイルに出力 (PDFファイルをパスワードで保護することも可能)

➤ システム連携を意識したインターフェースを提供

- ◆ お客様のご要件、移行、導入に対して、CSVファイルベースの一括処理インターフェース提供
- ◆ 他ソリューション (ID管理、シングルサインオン) との連携も可能

3. 2. ソリューションの特長 (4)

➤ Webサーバ連携 <CSLGuardWEB>

- ◆ 後段Webサーバに対して、利用者の属性情報を通知可能

➤ アクセス制御 <CSLGuardWEB>

- ◆ Webサーバの各URLにアクセス権の設定を実施
- ◆ 各種アクセス制御条件設定
 - ◆ 未認証でアクセス可 (Public)
 - ◆ 認証済みユーザのみ (Allusers)
 - ◆ 特定認証者 (ユーザ単位)
 - ◆ アクセス制御単位をグループで管理して、URLへのアクセス許可をグループごとに設定 (1グループに複数ユーザを設定可能)
 - ◆ 属性情報によるアクセス制御


➤ シングルアカウント機能 <CSLGuardWEB, ACTCenter>

- ◆ SSO用ID, パスワードとSSO対象システムのアカウント, パスワードを同値にして、利用者からリアルタイムにパスワード変更することが可能。

4. 1. 利用者向け機能 (1)

➤ 認証

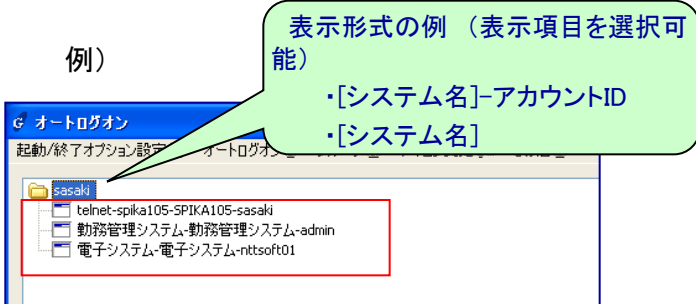
- ◆ お客様の端末利用形態にあわせ、3種類の認証方式を標準で用意
- ◆ 利用者ごとに許可する認証方式を選択可能

比較観点	一段認証	Windows認証連携	二段認証
OSへの ログオン	従来のWindowsログオン画面の代わりに CSLGuardのログオン画面が表示される 	従来のWindowsログオン画面から実施 ※Windows認証連携: WindowsのログオンIDと同じIDでCSLGuardに ログオンする場合、ID情報を取得する必要がある	
前提条件	・WindowsへのログオンID、パスワードを認証基盤 へ登録しておく (ACTCenterによる管理が可能)	左記前提が不要	
特長	PC立ち上げ時の一回の認証により、シングルサインオン環境となる		Windowsの認証後、認証基盤 へログオンが必要 (二回の認証行為が必要)
	別のIDで利用する場合、Windowsログオフが必要 ⇒主に個人PC(一人一台)環境で利用		別のIDで利用する場合、 Windowsのログオフが不要 ⇒共用端末でも利用可能
	端末にインストール済みのアプリケーションと競合 しないかチェックが必要 (WindowsのGINAをCSLGuardが用意するGINAと 書き換えるため、競合しないかどうか)	左記の検証が不要	

4. 1. 利用者向け機能 (2)

▶ シングルサインオン(SSO)

- ◆ 実行契機をシステム単位で選択可能 (混在も可)
 - ◆ SSOランチャーからの起動
 - ◆ 従来通りの起動 (デスクトップショートカット、ブラウザのお気に入り 等)
- ◆ 同一システムへ複数アカウントでのログオンが可能

比較観点	メニュー実行型	ウィンドウ監視型
SSO実行契機	SSOランチャーからの起動 例)  <p>表示形式の例 (表示項目を選択可能)</p> <ul style="list-style-type: none"> ・[システム名]-アカウントID ・[システム名] 	従来通りの起動 (デスクトップショートカット、ブラウザのお気に入り等)
特長	アプリケーションの起動をCSLGuardが代行 ログオン画面に対してSSO実施	アプリケーションの起動は利用者自身が実施 CSLGuardがSSO対象ログオン画面が出力されたことを検知し SSO実施
	<ul style="list-style-type: none"> ・利用可能な業務システムが一覧化されるため分かりやすい ・同一システムに対して複数のID(一般利用者/管理者権限等)を持つ場合にもSSO可能 	起動方法が従来通りであるため、利用者に対して馴染みやすい
	起動に時間がかかるシステムの場合、確実にログオンを行うための待ち時間が一律かかってしまう	SSO対象システムのログオン画面タイトルが重なっている場合、タイトル変更または運用制約が発生する

4. 2. 運用管理者向け機能

▶ ブラウザベースの一元管理

- ◆ 運用管理者の作業シーンを想定した画面構成
- ◆ ポリシー設定(ログオンポリシー、パスワードポリシー)
- ◆ ユーザに関する情報管理(追加/変更/削除/参照)
- ◆ シングルサインオン対象アカウント管理(追加/変更/削除/参照)

▶ 情報検索

- ◆ 過去に実行した検索条件より再実行が可能(クイック検索)
- ◆ ポリシーに該当するユーザ検索 例) 現在利用停止中のユーザ検索

▶ 各種運用作業

- ◆ 大量の人事異動を意識した一括処理の実行(所定書式のCSVファイルを指定)
- ◆ 定期スケジュールの登録/実行 (アカウントパスワードランダム変更 等)
- ◆ 利用者配信ファイルの登録(シングルサインオン用スクリプトファイル等)

▶ 稼働状況照会

- ◆ 現在ログオン中のユーザー一覧
- ◆ スケジュール実行履歴
- ◆ パッケージ動作ログ、一括処理実行結果の参照

▶ 監査チェック

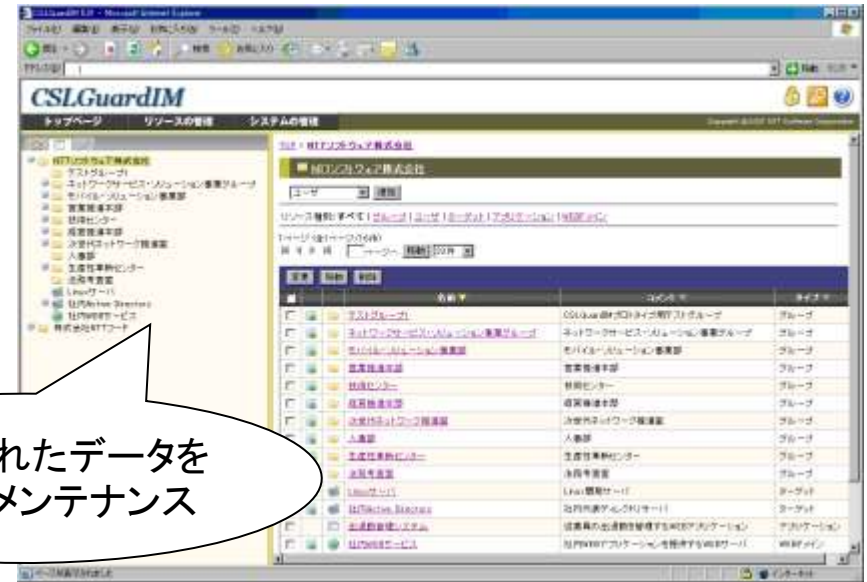
- ◆ アカウント管理先の不正アカウントをチェック

4. 3. 運用管理画面 (1)

作業シーンを想定した画面構成



使用頻度の高い
操作メニュー(ユーザ追加、検索等)



階層化されたデータを
参照し、メンテナンス



各種メンテナンス作業、
システム稼働状況参照
メニューを一覧化

4. 3. 運用管理画面 (2)

情報検索画面

The screenshot shows the CSLGuardIM 5.01 web application interface. The browser title is "CSLGuardIM 5.01 - Microsoft Internet Explorer". The page has a navigation bar with "トップページ", "リソースの管理", and "システムの管理". On the left, there are sections for "ログイン情報" (Login Info) and "よく使う操作" (Frequently Used Operations). The main content area is titled "クイック検索" (Quick Search) and "ユーザ検索" (User Search). Under "ユーザ検索", there are sections for "基本条件" (Basic Conditions), "セキュリティ条件" (Security Conditions), and "追加条件" (Additional Conditions). A dropdown menu is open over the "基本条件" section, showing options like "次の文字列に等しい" (Equal to the next string) and "次の文字列で始まる" (Starts with the next string). A search button "この条件で検索を実行する" (Execute search with these conditions) is at the bottom. On the right, there is a sidebar with system statistics like "接続先データベース" (Connected Database) and "登録ユーザー数" (Registered User Count).

過去に実施した
検索条件を選
択可能

各種検索条件
に該当するデー
タを検索

4. 3. 運用管理画面 (3)

監査チェック結果画面

The screenshot shows the CSLGuardIM 5.01 web application interface. The browser window title is "CSLGuardIM 5.01 - Microsoft Internet Explorer". The application has a navigation menu with "トップページ", "リソースの管理", and "システムの管理". The main content area is titled "ターゲットアカウント差分情報" and contains two tables of account information.

▼ターゲットにのみ存在するアカウント
1ページ (全1ページ/4件)

削除	すべて削除	アカウント名
<input type="checkbox"/>	<input type="checkbox"/>	onlyTarget1
<input type="checkbox"/>	<input type="checkbox"/>	onlyTarget2
<input type="checkbox"/>	<input type="checkbox"/>	onlyTarget3
<input type="checkbox"/>	<input type="checkbox"/>	onlyTarget4

▼データストアにのみ存在するアカウント
1ページ (全1ページ/10件)

削除	すべて削除	アカウント名
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore1
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore2
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore3
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore4
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore5
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore6
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore7
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore8
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore9
<input type="checkbox"/>	<input type="checkbox"/>	onlyDatastore10

認証サーバと実サーバの
差分をチェックすることで、
実サーバに直接作成され
た不正アカウントの有無を
チェック

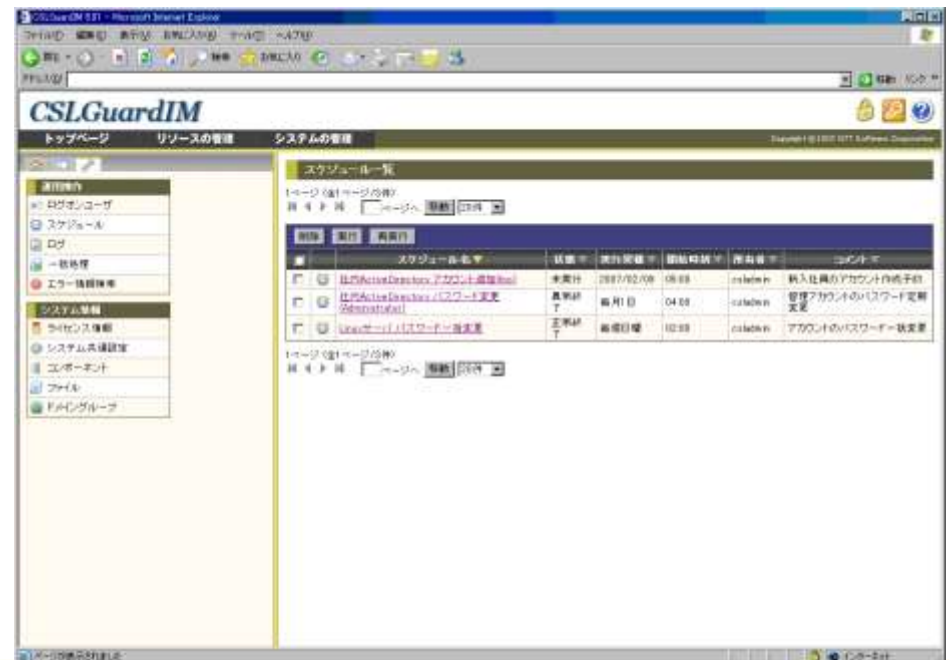
4. 3. 運用管理画面 (5)

稼働状況照会

一括処理結果



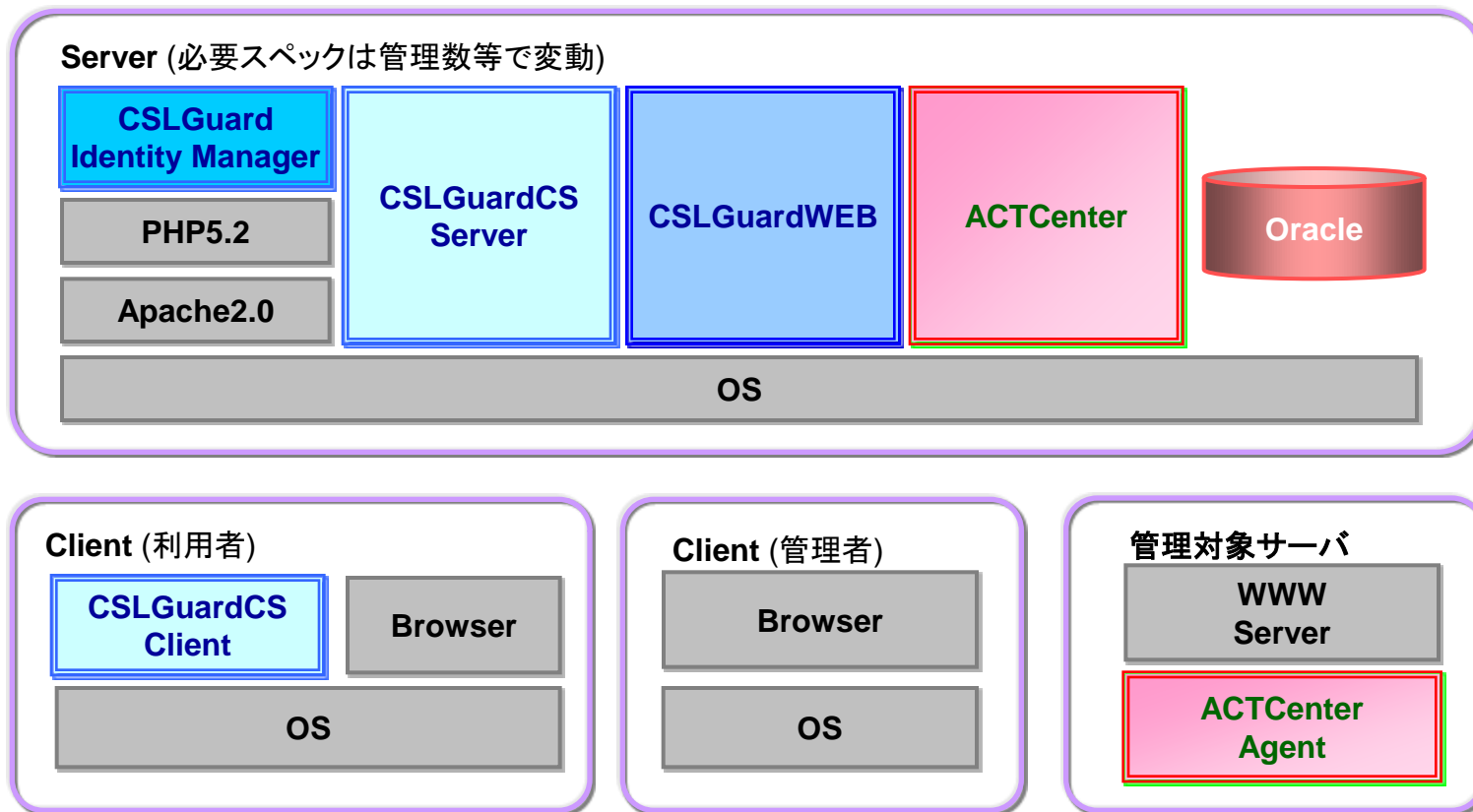
スケジュール一覧/実行結果



5. システム構成

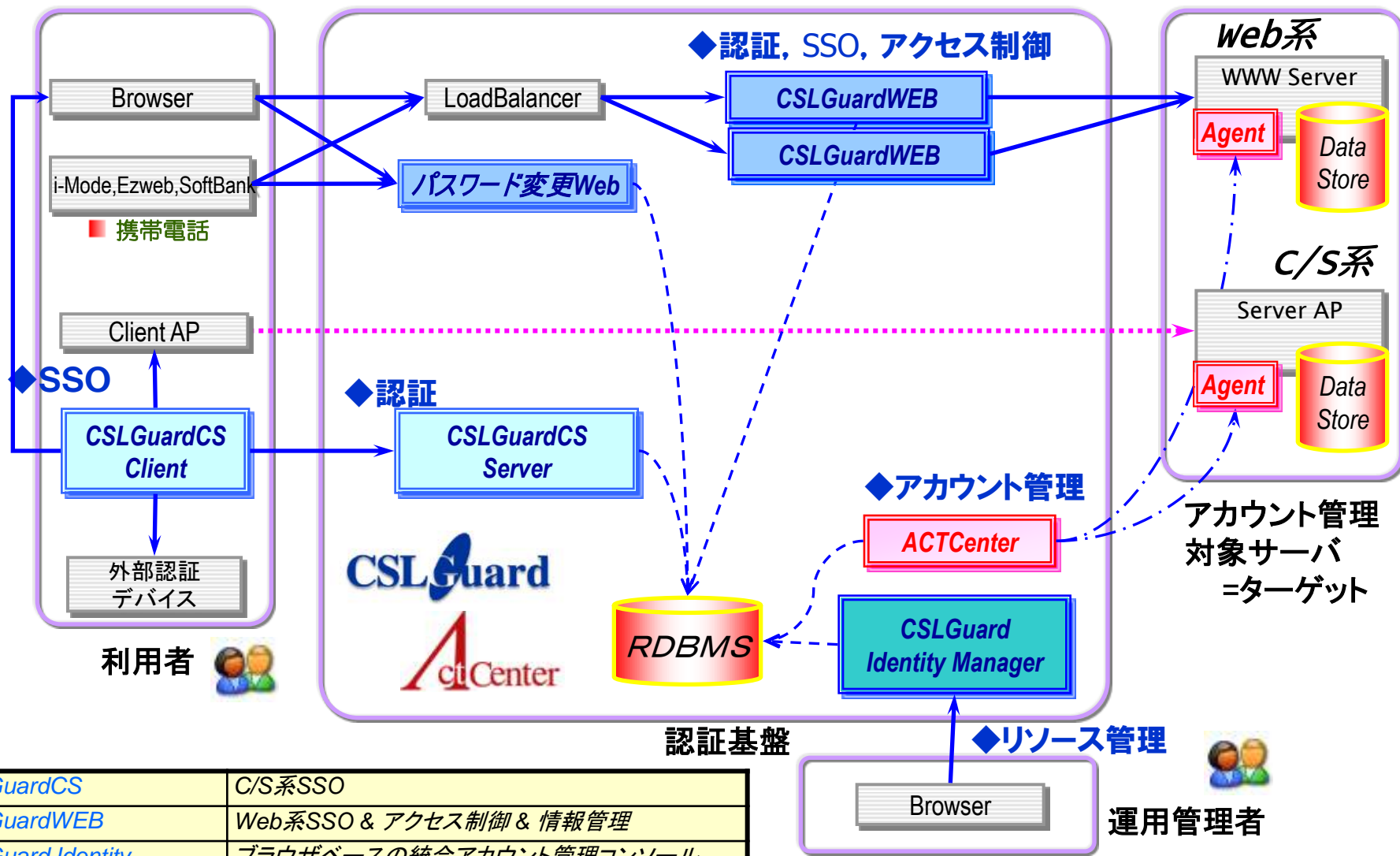
Mobile

■ システム最小構成



- この構成は必要最小限の構成であり、実際にはお客様の要件により台数は異なります。
- 対応OSにつきましては「5. 3. 対応プラットフォーム」を参照願います。

5. 1. 全体製品モジュール構成



CSLGuardCS	C/S系SSO
CSLGuardWEB	Web系SSO & アクセス制御 & 情報管理
CSLGuard Identity Manager	ブラウザベースの統合アカウント管理コンソール
ACTCenter	エージェントを介したアカウント管理

接続対象コンポーネント

5. 2. システム構成例

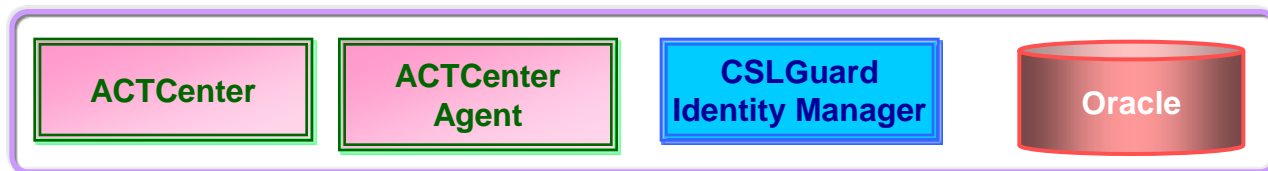
➤ C/S系認証 & SSO



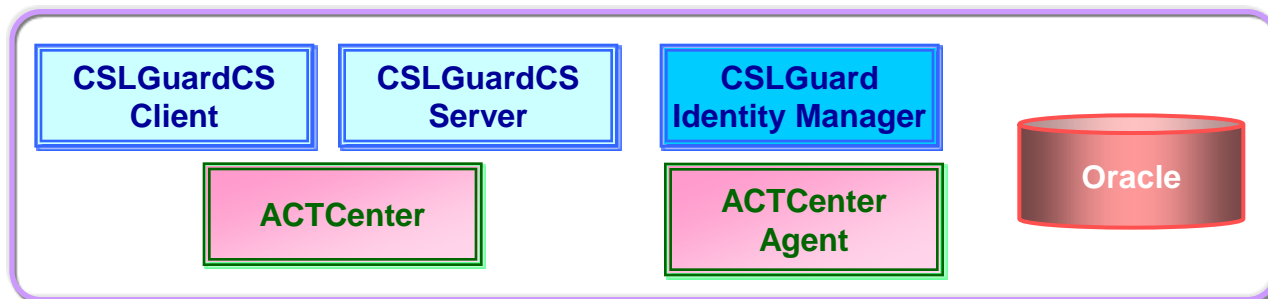
➤ Web系認証 & SSO & アクセスコントロール



➤ アカウント管理



➤ C/S系SSO&アカウント管理連携



5. 3. 対応プラットフォーム

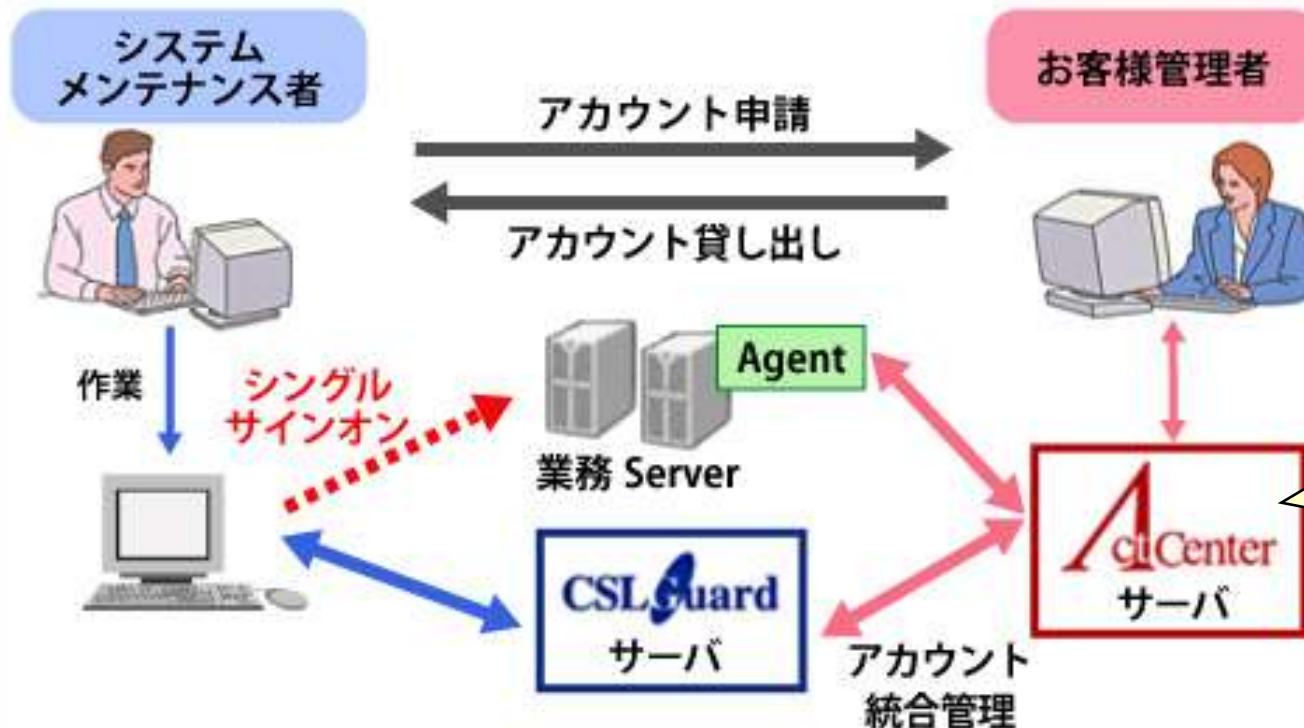
製品名	Ver.	対応プラットフォーム	製品オプション	必要となる製品(お客様用意)	
ACTCenter	5	Server	Redhat Linux ES 4, 5 Windows 2003 R2 Windows 2008		
		Agent	Windows NT4.0, 2000, 2003, XP HI-UX/WE2 06-20 Solaris 7, 8, 9, 10 HP-UX 10.20, 11.0, 11iv2 AIX 4.3, 5.2, 5.3 Redhat Linux AS2.1, 3, 4 ES 3, 4 Novell eDirectory 8.7.3 Sun Java System directory Server 5.2		
CSLGuardCS	5	Server	Redhat Linux ES 4 Windows 2003 R2 Windows 2008		
		Client	Windows 2000 Professional, Windows XP Professional Windows Vista		
CSLGuardWEB	5	-	Redhat Linux ES 4 Windows 2003 R2 Windows 2008	◆SSL ◆クライアント認証	◆サーバ証明書 (SSL使用時)
CSLGuard Identity Manager	5	-	Redhat Linux ES 4 Windows 2003 R2 Windows 2008		◆ブラウザ(IE5.5以上) ◆Apache 2.0 ◆PHP 5.2
RDBMS	-	-	Oracle 10g Standard Edition One Oracle 11g Standard Edition One		

〈参考〉アイデンティティ管理ソリューション 事例

内部統制用に、ニーズの高まる、システムのルート権限など特権IDの厳密な管理を容易に実現

〈導入モデル〉 特権アカウント管理モデル

ポイント：特権 ID の厳密な管理



システム保守の必要な、ある日のある時間帯のみ自動で管理者権限を払い出し

<参考>IT内部統制向け情報セキュリティソリューション

内部統制強化に必須のセキュリティ

◇アクセス制御

(不正アクセス防止、職務分掌)

◇ログ監査

(不正アクセス検出、正当性監査)

◇データ保護、暗号

(盗聴、改ざん防止)

■アイデンティティ管理ソリューション

コンソールガード
「**CSLGuard**、アクトセンター**ACTCenter**」

サビー センセージ
■ログ収集・監査 「**SAVVY**、**SenSage**」

サイファークラフト
■暗号化ソリューション「**CipherCraft®シリーズ**」

■文書持ち出し管理ソリューション



利用者

社内・社外統制

アクセス制御

データの
持ち出し制御

データの暗号

監査ログ収集

データ保護・暗号

アクセス制御
アイデンティティ管理
「**CSLGuard**、**ACTCenter**」

ログ監査

ログ収集・監査
「**SAVVY**、**SenSage**」

データ保護・暗号
・暗号化ソリューション
「**CipherCraft®シリーズ**」
・文書持ち出し管理
ソリューション