スピーカー紹介

潮村 剛 （しおむら たけし）

1990年代半ば、食品メーカーからITベンチャーに飛び込む。
国内の主要通信サービス事業者を中心に認証系システム案件を数多く担当し鍛えられる。

2008年、かもめエンジニアリング社を設立。
統合認証基盤やビッグデータ処理など、通信サービス事業向けのシステムで
多くの導入実績を上げつつ、2017年にはSSO分野で「KAMOME SSO」を提供開始。
SSOやID分野のセミナーで年間30回程度講師を担当。

2019年、一般企業のID管理の課題を解決するためKeyspider社を設立。
「クラウドID管理サービス Keyspider」の提供を開始。

2021年、テレワークのセキュリティ強化を推進するため、
ゼロトラスト接続サービス「Keygateway C1」を発表

2022年、日本企業へのゼロトラストセキュリティの普及を目的として、
ITベンダーやSI事業者を中心とした19社で「ゼロトラストアライアンス」を設立。

オライリー・ジャパンより刊行のIT技術書籍のプロデュース。
『RADIUS – ユーザ認証セキュリティプロトコル』（2003年）
『Diameter プロトコルガイド』（2015年）

趣味　料理と読書。歴史小説とSFが好き。

画像引用：
オライリー・ジャパン

「ユーザーの認証・認可」「ID管理」を中心としたチーム

■ 通信キャリア向け 大規模認証システム

- ➢ 携帯電話サービス 基幹認証システム
  - 国内通信事業者　4,500万ユーザ
- ➢ 企業顧客向けVPNサービス 認証基盤
  - 国内総合電機メーカー　100万ユーザ
- ➢ 社内LANアクセス　認証基盤
  - 国内大手移動体通信事業者　20万ユーザ
- ➢ Webフィルタリングサービス
  - 認証エンジンセキュリティベンダー OEM提供

etc.・・・

■ エンタープライズ市場向け シングルサインオン（SSO） & ID管理システム

- ➢ IDaaSサービス 認証基盤
  - 通信事業者　約2,000社
- ➢ 社内業務アプリ SSOシステム
  - 家電メーカー　7,000ユーザー　など
- ➢ 学内システム SSOシステム
  - 大学　15,000ユーザー　など
- ➢ OEM提供先

NTT AT　FUJITSU　HCNET エイチ・シー・ネットワークス株式会社　Stylez 株式会社 スタイルズ　Marubeni Network Solutions　IP3

KAMOME Engineering

セキュリティの土台は
「利用者のID情報管理」から

KAMOME Engineering

コミュニケーション・情報共有が広がるほど･･･

利用者の増加

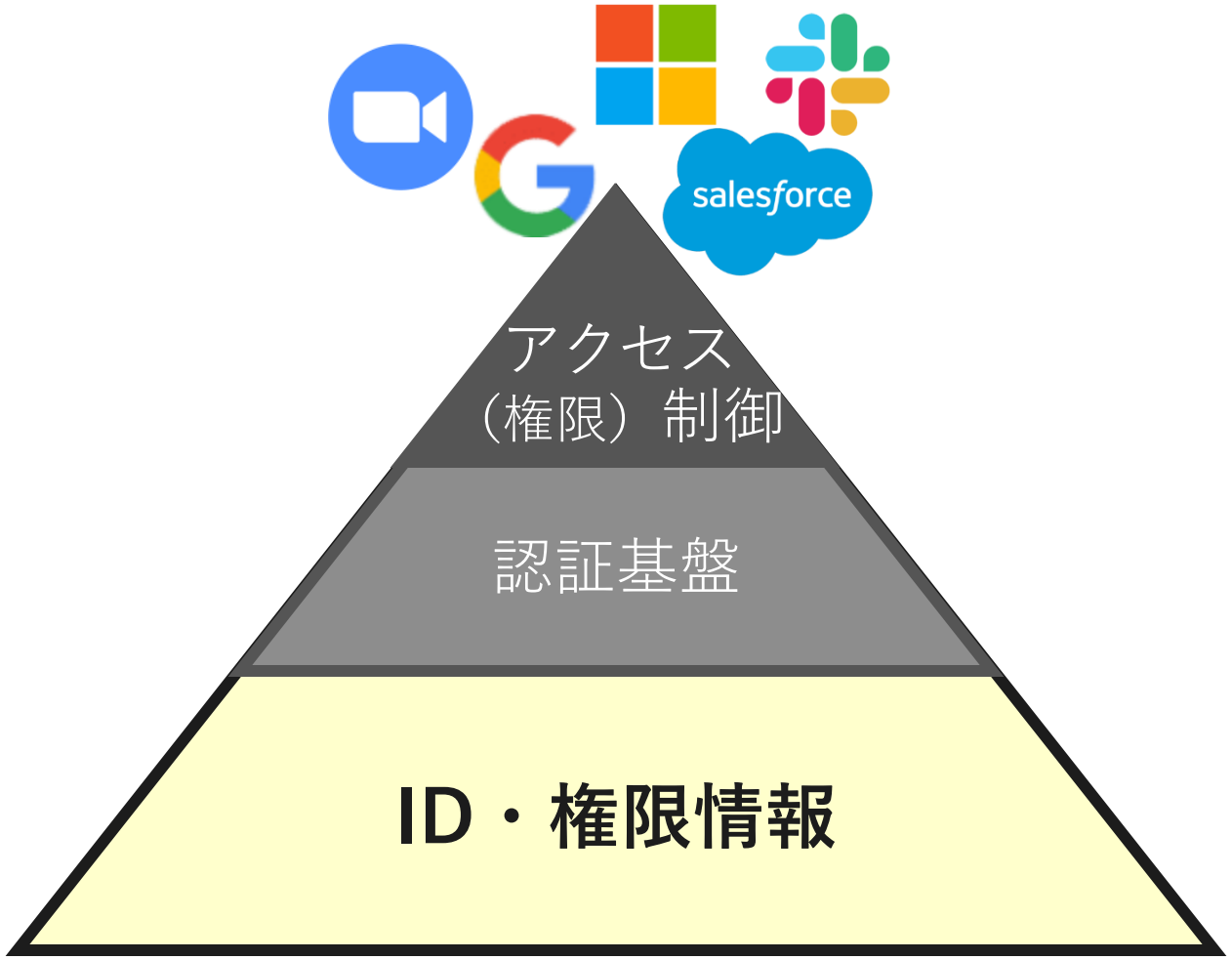
利用・連携システムの増加

ID、パスワード、所属、利用権限 …

利用者情報・権限情報の、正確・タイムリーな管理が重要に

KAMOME Engineering

ID管理は、すべてのセキュリティの根幹



KAMOME Engineering

ID情報管理の導入目的とは？

セキュリティ

メンテナンス漏れによるセキュリティリスクの抑制

- **退職者ID や 利用者不明のIDを使った システムの不正利用・情報漏洩**
- **過大な権限割当てによる機密情報の不正参照**
- **脆弱なパスワードによる不正アクセス**

IT全般統制

「内外からのアクセス管理等のシステムの安全性の確保」が要求する下記事項への対応

- アカウント発行・変更・削除を適時に実施
- 定期的な棚卸しの実施と承認
- 定期的なログのモニタリング

利便性

利用者・運用担当者ともに、アカウントに関する運用負荷を軽減

- 人事異動情報を発令日に即日反映
- パスワード変更・リセットをセルフサービス
- 各種調査・監査対応

個人情報保護

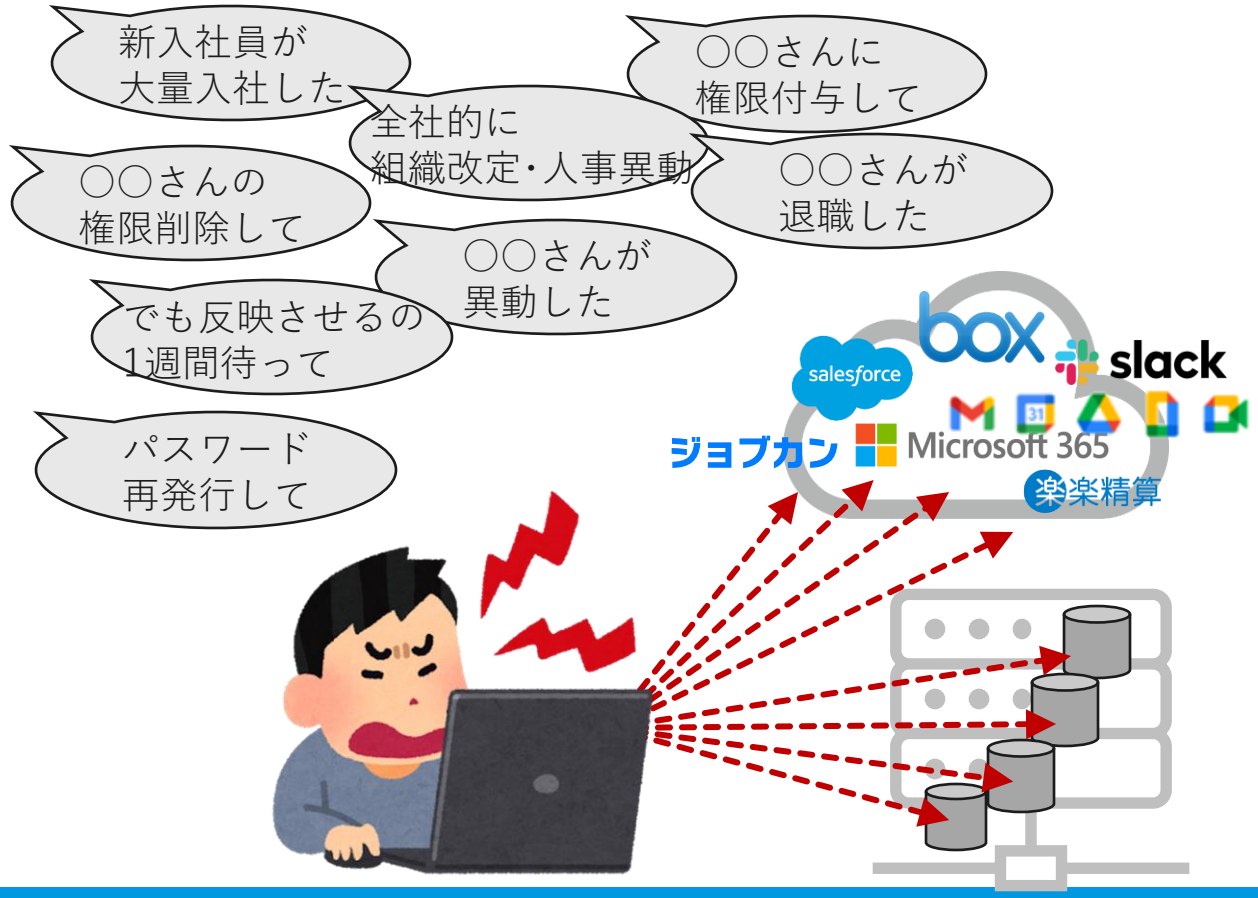
2022年4月、改正個人情報保護法が施行

- 2017年の改正で従業員の個人情報保護が強化
- データの利活用促進を図る一方、違反時の厳罰化も
- 短期保有のデータも対象

KAMOME Engineering

でも、大変ですよね･･･

■ 各システムのID情報のメンテナンスがバラバラだと…



- とにかくメンテナンスが大変！
  - **メンテ漏れ**がなくならない
  - 運用の**人的コスト**がかさむ
- **なくなった権限**や**退職者の情報**が残っていると、不正アクセスの誘因に
  - **監査**の際にも必ず注目されるポイント
- ログもバラバラになってしまう
  - 「**いつ、誰に、どんな**メンテナンスを？」
  - 有事の際に迅速な対応ができない
  - 監査への対応もまた大変になる

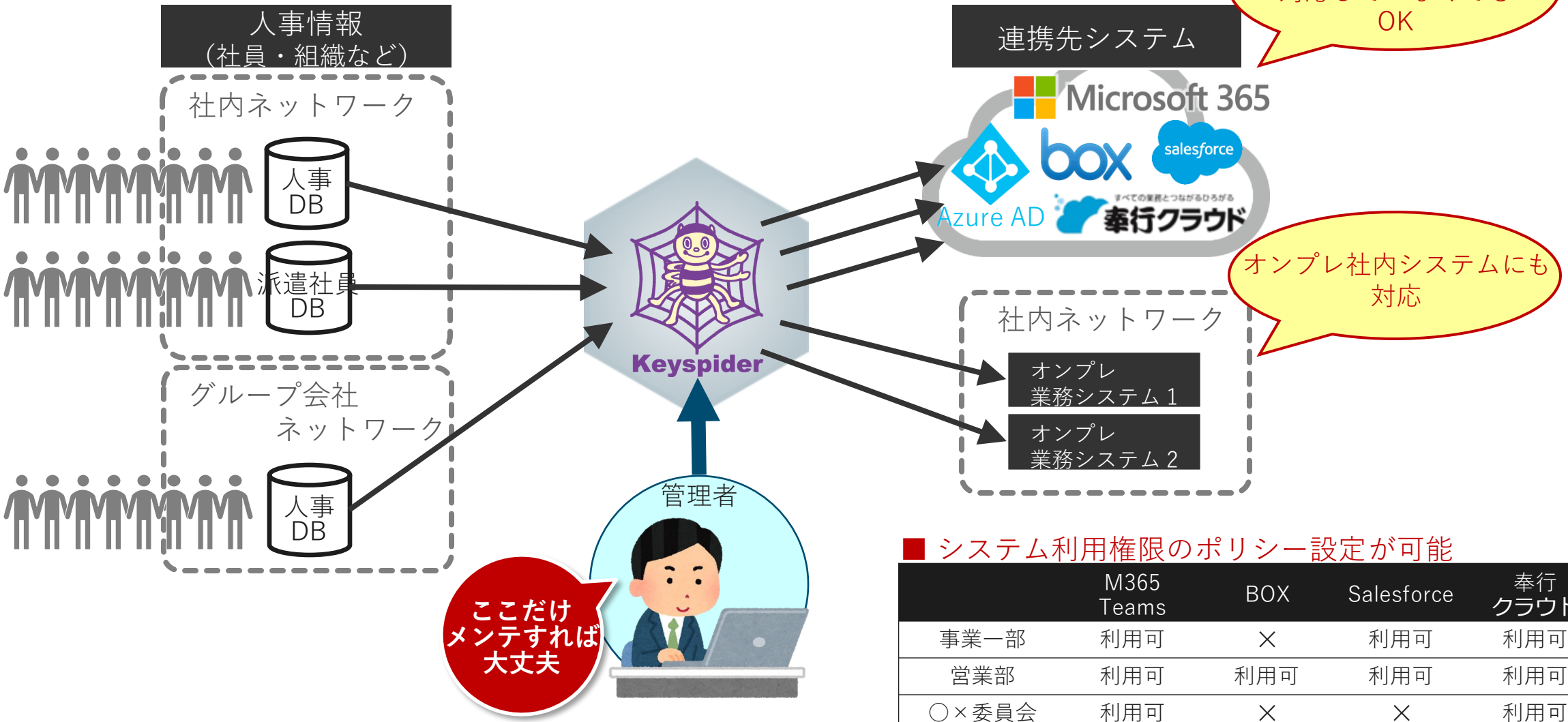
KAMOME Engineering

日本企業の人事運用に適した
国産・ID管理クラウドサービス

ID情報を一元管理、各システムへ自動的に同期

KAMOME Engineering

Keyspider を活用したID管理業務



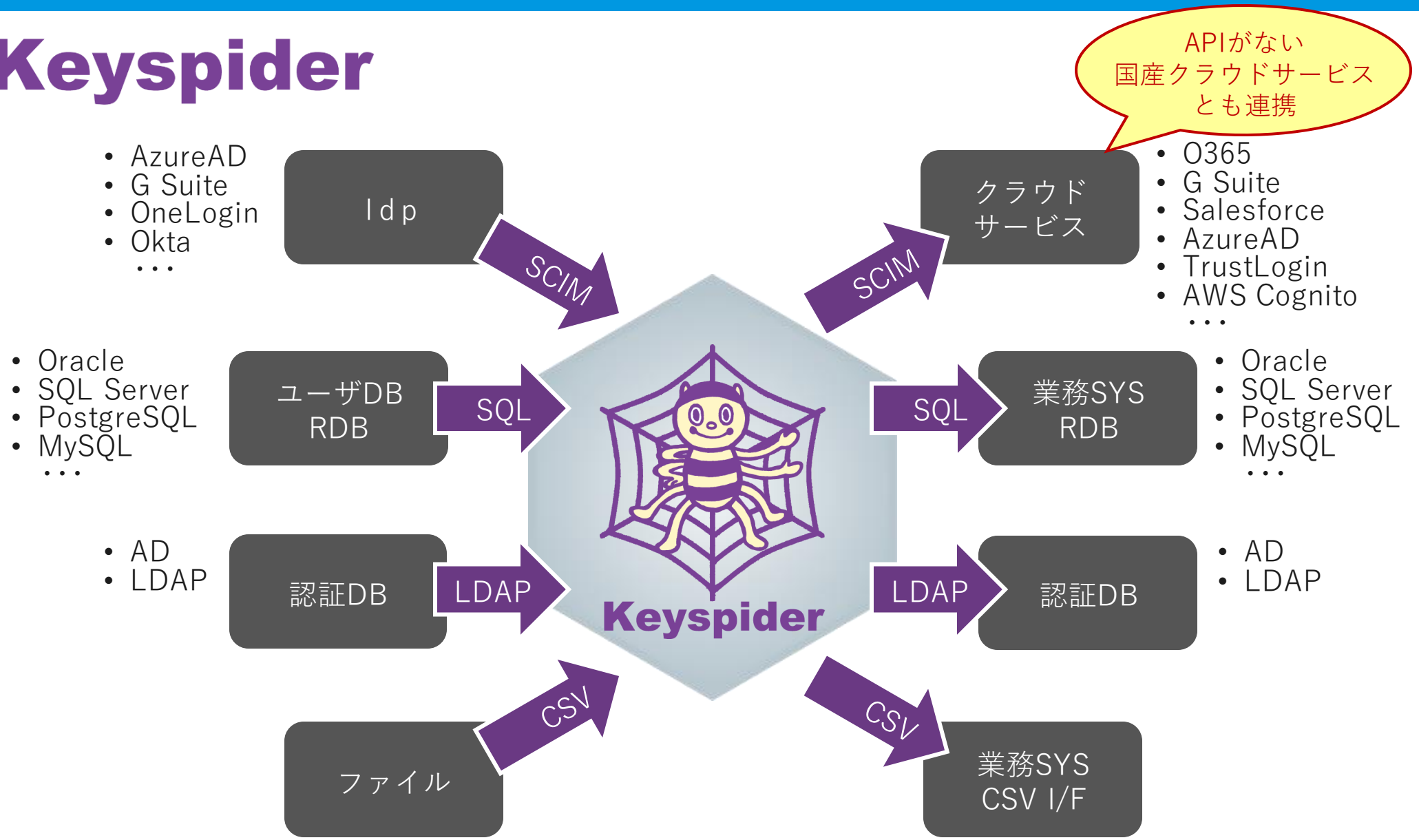
■ システム利用権限のポリシー設定が可能

	M365 Teams	BOX	Salesforce	奉行クラウド
事業一部	利用可	×	利用可	利用可
営業部	利用可	利用可	利用可	利用可
○×委員会	利用可	×	×	利用可

主要プロトコルすべてに対応し、多様なシステムと連携

KAMOME Engineering

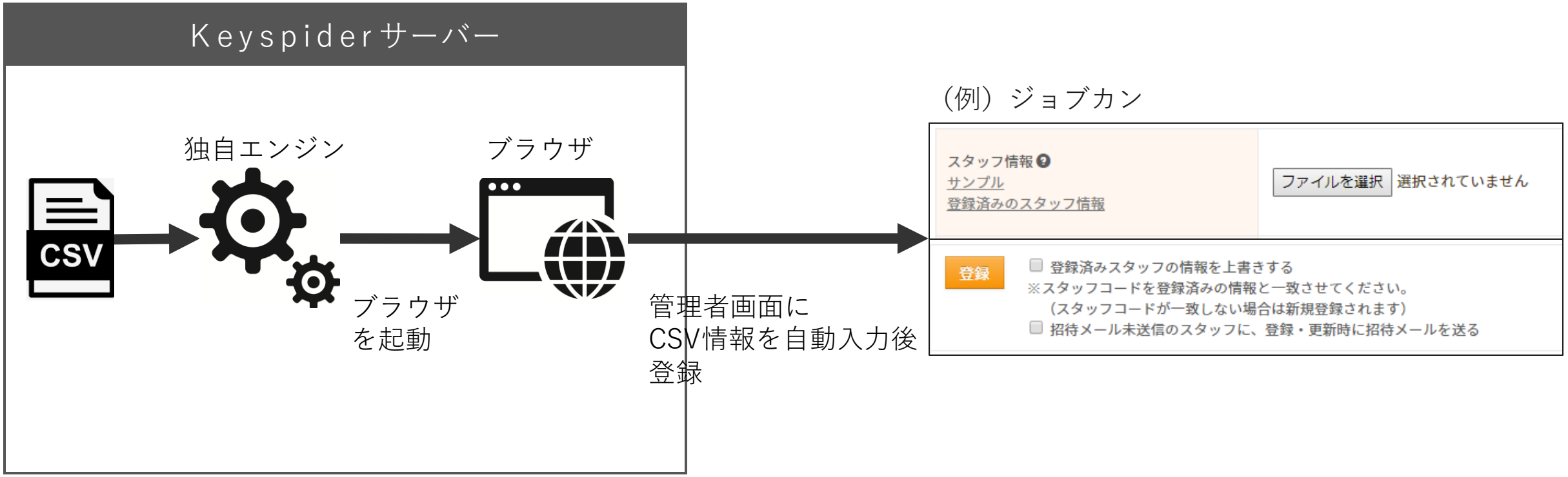
Keyspider



APIがない国産クラウドとも、独自APIにより連携可能

KAMOME Engineering

Keyspider



独自のRPA(オープンソース)技術により、
SCIMなどの**APIが無いクラウドサービス**や、スクラッチ開発された**オンプレミスのシステム**などに対しても
自動的にデータの同期が可能です。

日本企業に必要な「ID管理」を実現

KAMOME Engineering

Keyspider

データ取込

日本組織対応

マスター管理

組織の人事を
連携先に伝える

連携先に
IDを配信する

プロビジョニング
（データ同期）

属性編集・マッピング

Keyspider

組織の
アカウント運用を
支援する

パスワード管理

承認ワークフロー

棚卸データ作成

監査証跡作成

どれだけ**組織の人事・運用に寄り添っている**かが重要

日本企業向けの独自機能

KAMOME Engineering

Keyspider

所属兼務対応

- ユーザー情報に
  兼務部署項目を標準で用意
- 「組織マスター」で簡単入力
- ユーザー情報から
  権限・所属グループを自動判定

一つのIDへ
「主務」「兼務」
両方の権限を割り当て

引継ぎ期間

- 「引継ぎ期間」を設定
- その期間は異動前の権限を保持
- 期間経過後に自動で権限削除

データから判断できない
権限の割り当て

未来発令

- 未来日発令の情報を登録
- 組織マスターも未来日発令対応
- 実際の発令前に
  データを事前チェック

月末月初の運用負荷を軽減

その他の主要機能

KAMOME Engineering

Keyspider

※ 一部実装中のものを含みます

機能名	内容
社員番号、メールアドレスなどの生成（関数機能）	ルールに基づき、自動的に社員番号やメールアドレスを生成
有効期限によるアカウント削除・権限削除	予め有効期限（例えば6か月など）を決めて、アカウントを登録したり権限を付与する（期限後に自動的に削除）
新規アカウント登録時の自動権限付与	新規アカウント登録時に、予め指定されたポリシーに従って自動的に権限を付与
承認ワークフロー	アカウント登録や権限付与について、マネージャー等の承認を経てから実行する
差分チェック	KeyspiderのDBと、プロビジョニング先の状態に差分が無いかをチェック
異常値アラート	プロビジョニング用のデータ作成時、通常とは異なる大量の差分が発生した場合などに警告
棚卸データ作成	システム上のアカウントや権限の状態と実際の現場との乖離をチェックする 棚卸業務のために必要なデータを生成
監査証跡	Keyspider Manager（画面）において、いつ、誰が、どのような操作を行ったのか データを記録

IDaaSに搭載のID管理機能　との比較

KAMOME Engineering

Keyspider

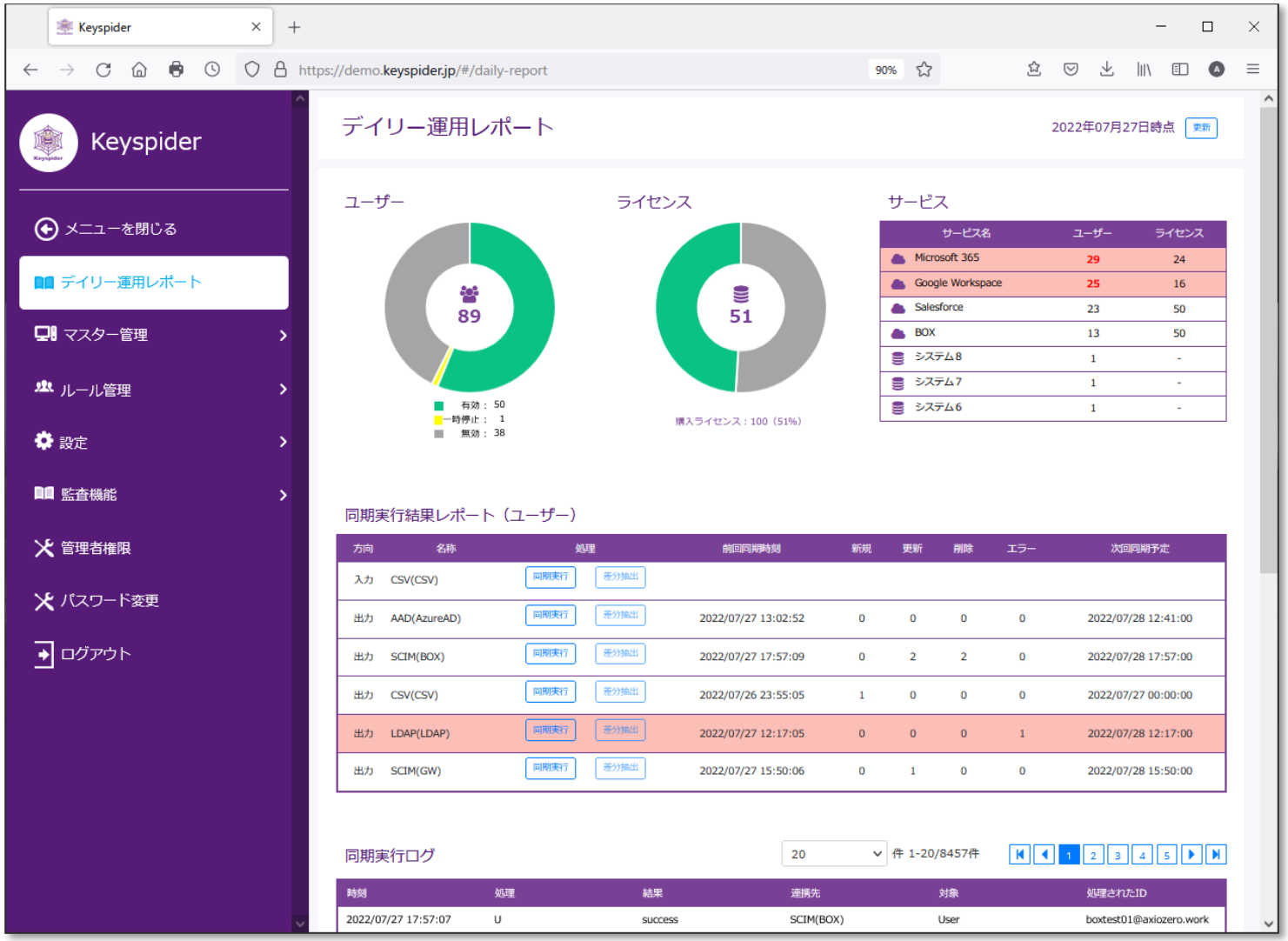
機能		Keyspider	IDaaSのID管理
IDの配信	SaaS	◎	○
	オンプレミス	◎	△
人事イベントの伝搬	源泉システム連携	◎	△
	日本組織対応	◎	△
アカウント運用支援	セルフサービス	◎	○
	棚卸し	◎	△

◎…サービス標準機能内提供＋多機能　○…サービス標準機能内提供　△…オプション購入・別途SI・開発が必要

充実した日本語GUI

Keyspider 管理画面の例

- 各種マスタの検索、参照、更新、パスワードポリシーの管理などが可能です。
- 操作はすべて記録されます。
- 一般ユーザーが自らパスワードリセットできる画面も提供します。

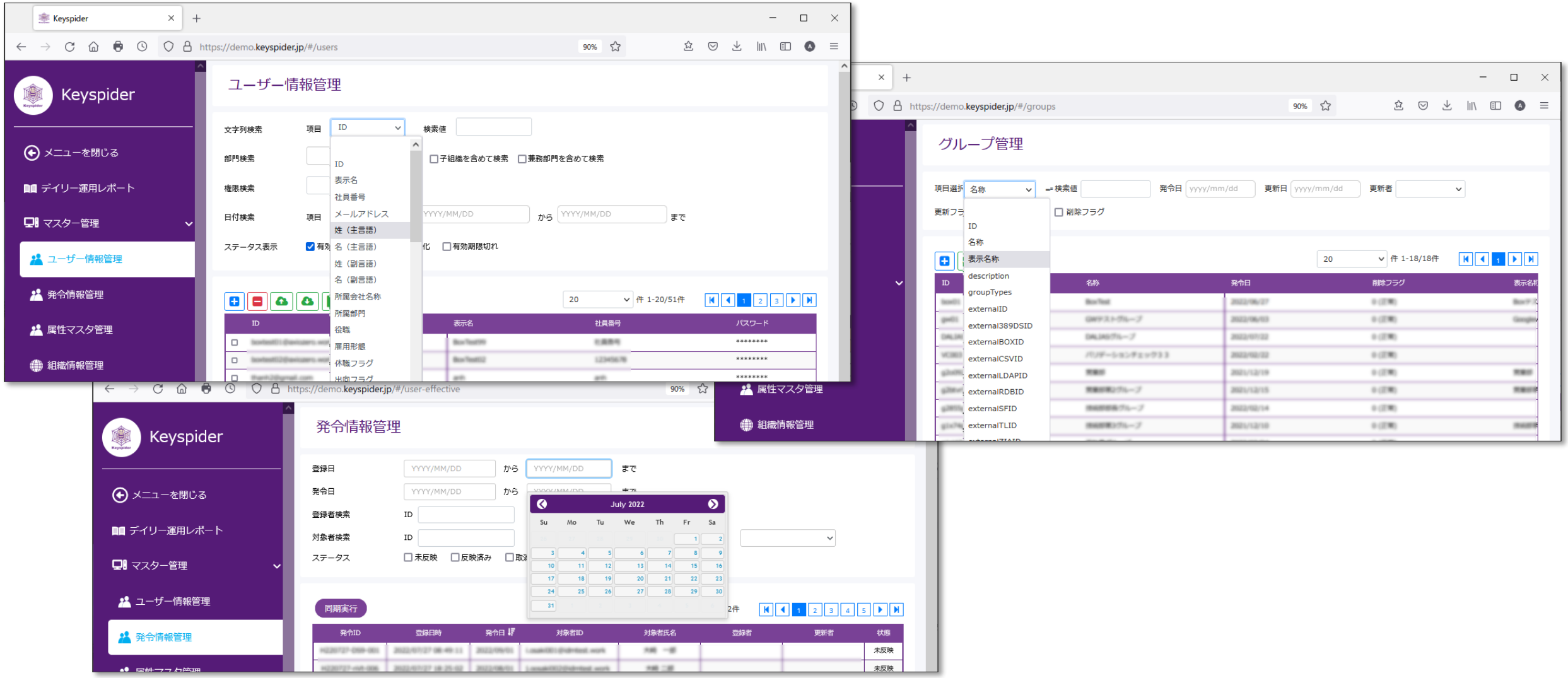


充実した日本語GUI

KAMOME Engineering

Keyspider 管理画面の例

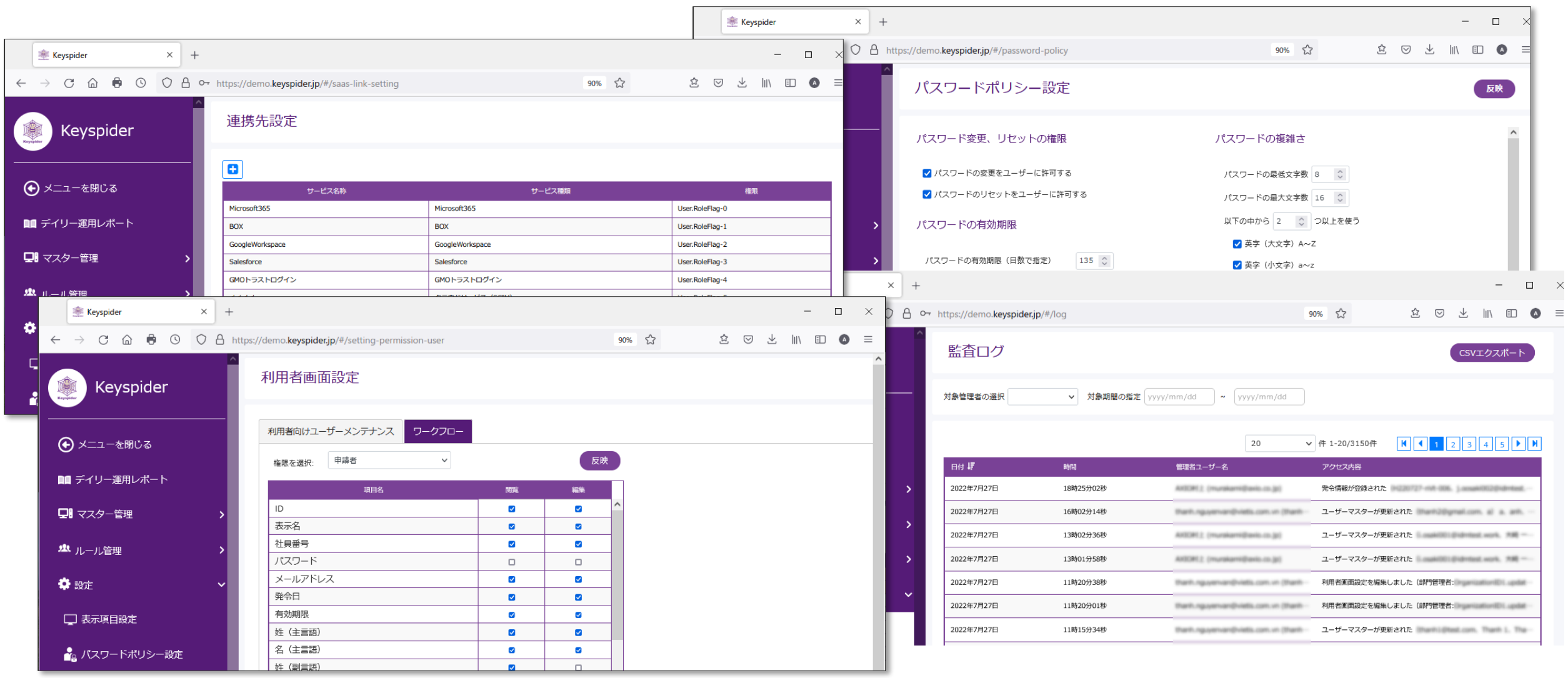
- 各種マスタの検索、参照、更新、パスワードポリシーの管理などが可能です。
- 操作はすべて記録されます。
- 一般ユーザーが自らパスワードリセットできる画面も提供します。



充実した日本語GUI

Keyspider 管理画面の例

- 各種マスタの検索、参照、更新、パスワードポリシーの管理などが可能です。
- 操作はすべて記録されます。
- 一般ユーザーが自らパスワードリセットできる画面も提供します。



連携システム検証状況 （続々検証中）

KAMOME Engineering

Keyspider

※ 一部検証中のものを含みます

No.	名称	種別	方向		方式
01	AD/LDAP	オンプレ	入力	出力	LDAP
02	AzureAD	SaaS	入力		SCIM
03	AzureAD/Microsoft365	SaaS		出力	GraphAPI
04	BOX	SaaS		出力	独自API
05	CSVファイル	オンプレ	入力	出力	CSV
06	GoogleWorks	SaaS	入力	出力	SCIM
07	IIJ ID	SaaS	入力	出力	SCIM
08	Okta	SaaS	入力	出力	SCIM
09	OneLogin	SaaS	入力	出力	SCIM
10	RDB/Oracle	オンプレ	入力	出力	SQL
11	Salesforce	SaaS		出力	SCIM

No.	名称	種別	方向	方式
12	SAP	SaaS	出力	SCIM
13	Slack	SaaS	出力	SCIM
14	SmartHR	SaaS	出力	RPA
15	TrustLogin	SaaS	出力	SCIM
16	Zoom	SaaS	出力	SCIM
17	コンカー	SaaS	出力	SCIM
18	サイボウズ・キントーン	SaaS	出力	RPA
19	ジョブカン	SaaS	出力	RPA
20	楽楽精算	SaaS	出力	RPA
21	奉行クラウド	SaaS	出力	RPA

まとめ

KAMOME Engineering

- セキュリティの土台となるのは、適切なID管理です。
- 手作業による個別メンテナンスは、人的負荷が大きいだけでなく
  漏れ・ミス等からのセキュリティインシデントを招きやすくなります。
- 源泉データから各システムへ、ID・権限情報のプロビジョニングを
  一括して行うサービス「Keyspider」が便利です。
- 特に日本企業に適した国産サービスです。

ぜひご要望ください

詳細説明
課題ヒアリング

デモ
評価サイト

概算お見積り

■ ご連絡先

- かもめインサイドセールスチーム　i-sales@kamome-e.com
- お問い合わせフォーム　https://solution.kamome-e.com/contact/

ブログ記事をアップしています。あわせてご参照ください。
「ID管理に必要なSCIMとは？」「ID管理システム4選の機能・特徴を比較！」 等
https://solution.kamome-e.com/blog/

かもめエンジニアリング株式会社
KAMOME Engineering
日本でいちばん仕事が大好きなチームです！