2）統合ID管理製品「Soliton ID Manager」ご紹介

～AD管理において使える機能の紹介～

平成27年11月18日
株式会社 ソリトンシステムズ
ID Manager担当
倉田和人

Soliton ID Managerの概要

ID管理システムの役割

1．必要最小限のアクセス権限付与

2．統合された認証・認可の仕組み
（認証基盤）

3．アクセスログの取得・統合管理
（ログ管理基盤）

4．アクセス権限の確認＆是正

全プロセスの
監視・監査

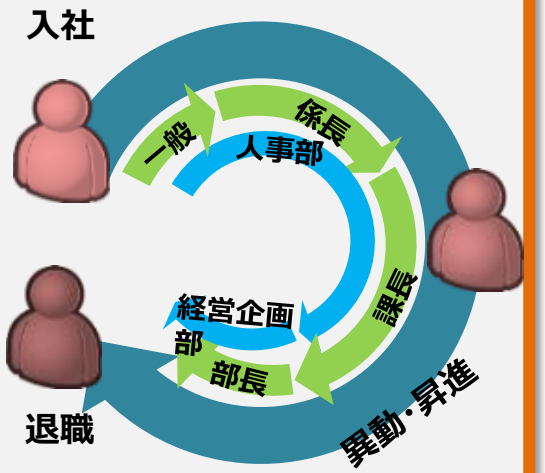
ID ManagerによるID管理

■ セキュリティの視点＝必要最小限のアクセス権限

– 必要なアクセス権のみを付与し、不要になった権限はすぐに削除・是正する

対応付け

IDライフサイクル管理



情報資産アクセス管理

アクセスポリシー

情報資産の把握と分類

自動割当と申請制御

権限可視化とライフサイクル管理

利用開始

権限変更

利用終了

アクセス権限の可視化

Soliton ID Manager

IDentity管理		情報資産アクセス管理
○	誰が	○
○	どんなIDで	○
―	どの情報資産を	○
―	どんな権限で	○
―	どの期間	○
―	どんな理由で	○

ステップアップ

管理者は楽になったけど、セキュリティ対策としては不十分なんだよなあ。

適切なアクセス権限管理ができるから、セキュリティ対策としても十分だ！

使えるのかを管理できる

情報資産アクセス管理の概要

1）マスター管理

- ID管理システムが利用する３つのマスター
  - ①情報資産マスター
  - ②組織マスター
  - ③社員マスター

①情報資産マスター管理

■ 情報資産マスターの役割

- 情報資産の分類や管理者の登録
- ロールやアクセス権限を管理したい対象の登録
- ライセンスや貸し出し管理をしたい資産の登録

■ 情報資産マスターで管理可能な情報資産の例

ADグループ

共有フォルダ

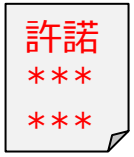
ロール

アプリケーション

メーリングリスト

デバイス

ライセンス

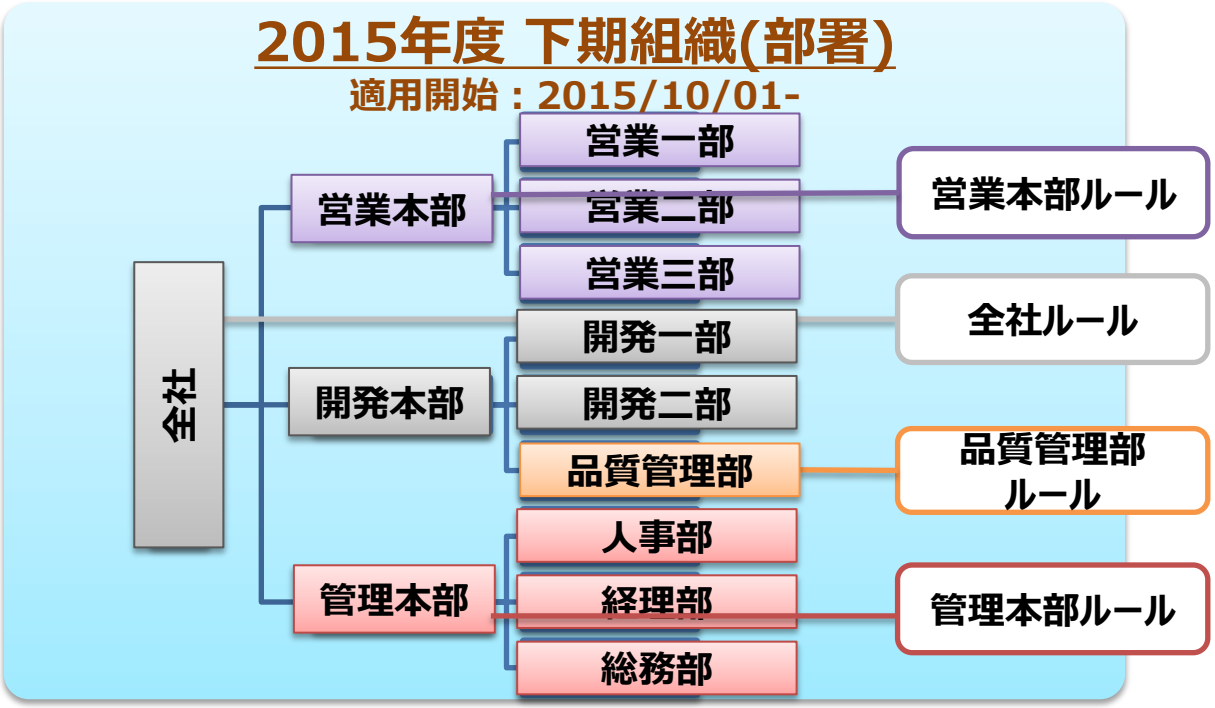


②組織マスター管理

■ 組織マスターの役割

- 組織情報のコードマスター
- 組織ルールの適用先
- ワークフローにおける申請可否制御や承認経路

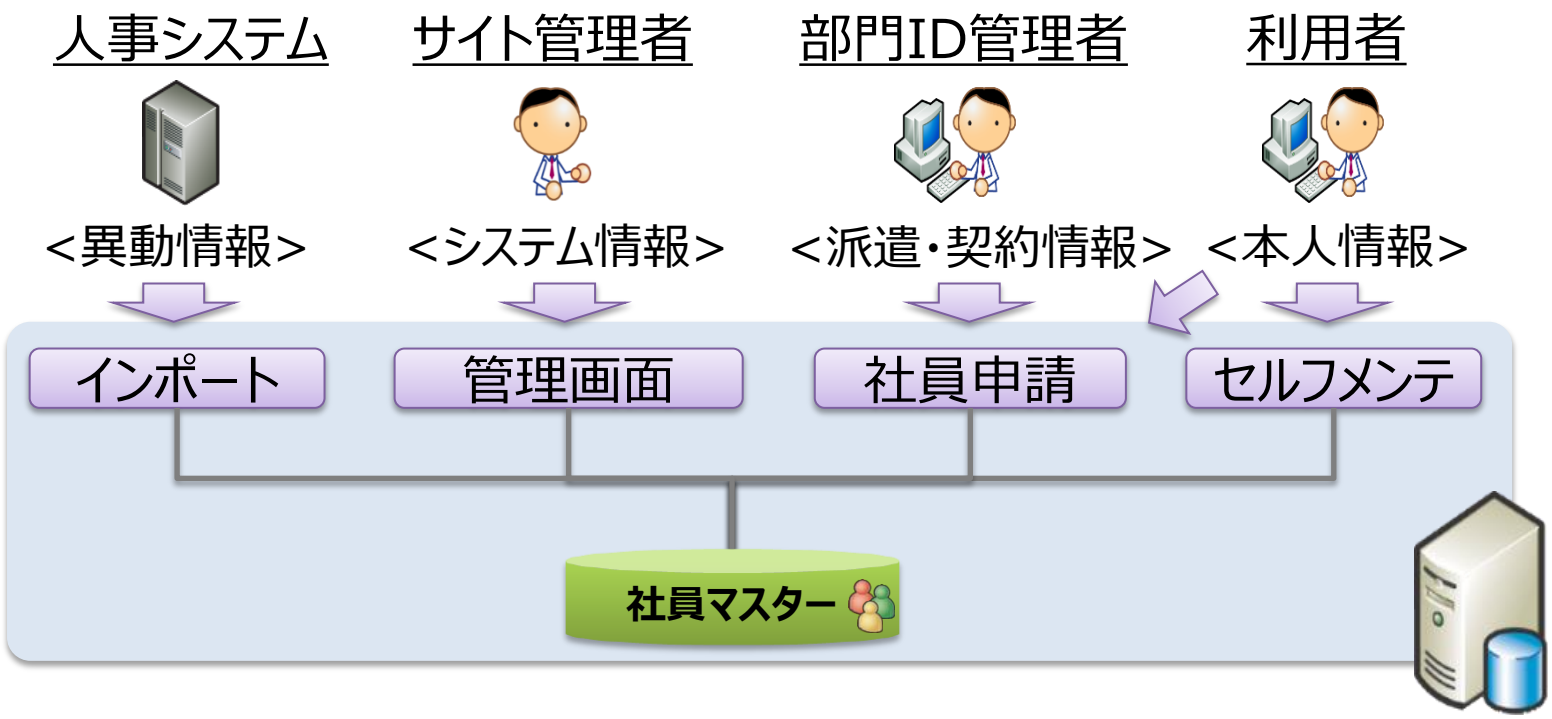
【部署マスターと組織ルール】



③社員マスター管理

■ 社員マスターの役割

- 統合ID管理システムにログインするIDの管理
- プロビジョニングに必要な社員属性の管理
- 通知先メールアドレスの管理



2）アクセス権限管理

■2種類のアクセス権限管理方法

①組織ルールによる権限管理

・人事異動に合わせて自動付与・削除

②ワークフローによる権限管理

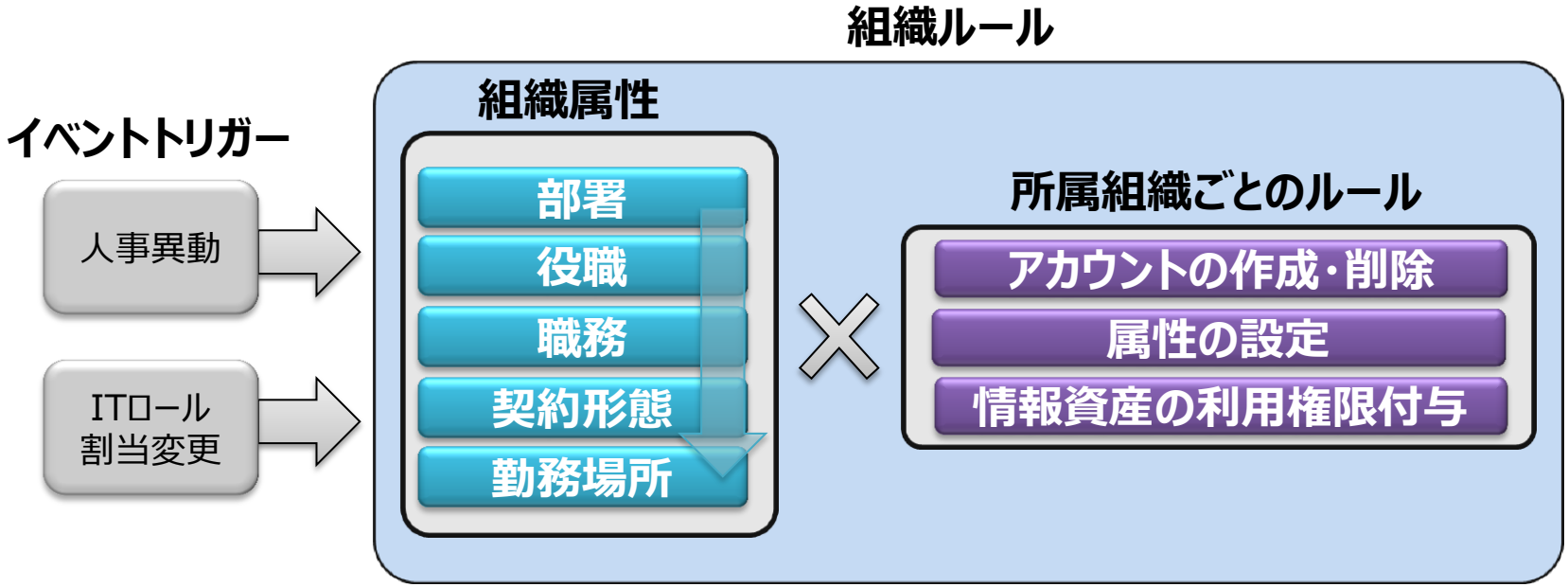
・組織ルールでは自動付与できないもの

・組織ルールで付与した権限の変更

①組織ルールによる権限管理

■ 組織ルールの役割

- 人事異動への自動対応
  - 部署異動処理、昇進処理、兼務処理、引継処理
- IT部門で管理する組織属性（ITロール）を用いた管理
  - 標準提供の組織属性を独自のITロールとして利用する事が可能



人事異動への自動対応

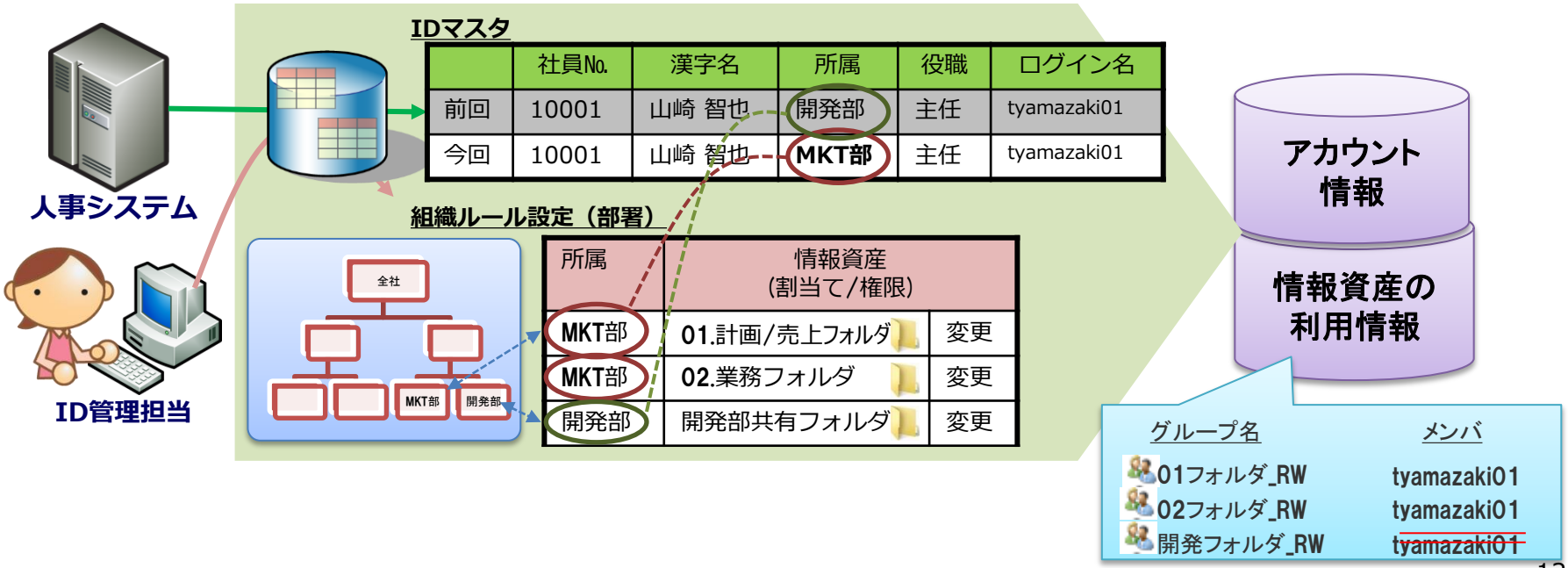
■ 社員マスターの更新を検知して自動更新

① 人事異動情報から所属組織の変更を検知

② 新所属組織の組織ルールを適用

③ 旧所属組織で割り当てた権限を引継期間経過後に適用終了

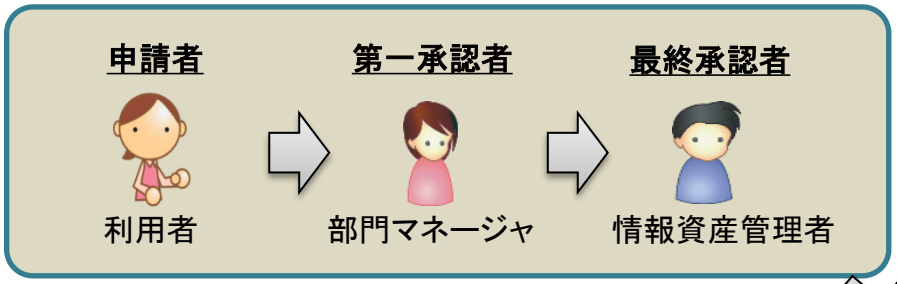
ファイルサーバのアクセス権管理例）



②ワークフローによる権限管理

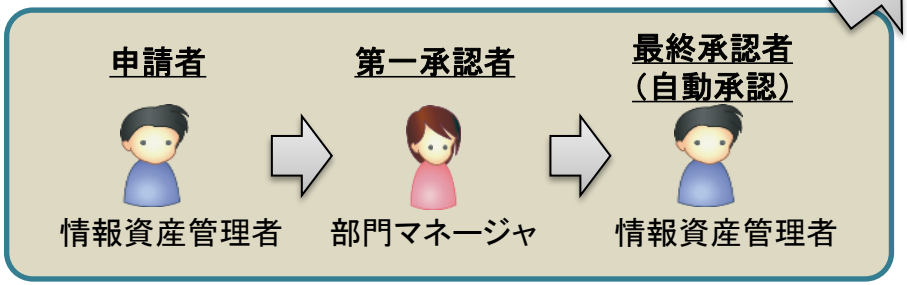
1.利用者による申請

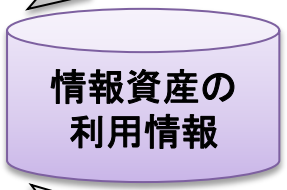
申請者　：利用者
対象者　：利用者
情報資産：(利用したいもの)
利用条件：
　利用権限　：
　利用開始日：
　理由終了日：
申請理由：
承認理由：



2.情報資産管理者による代理申請

申請者　：情報資産管理者
対象者　：利用者
情報資産：(管理対象のもの)
利用条件：
　利用権限　：
　利用開始日：
　理由終了日：
申請理由：
承認理由：

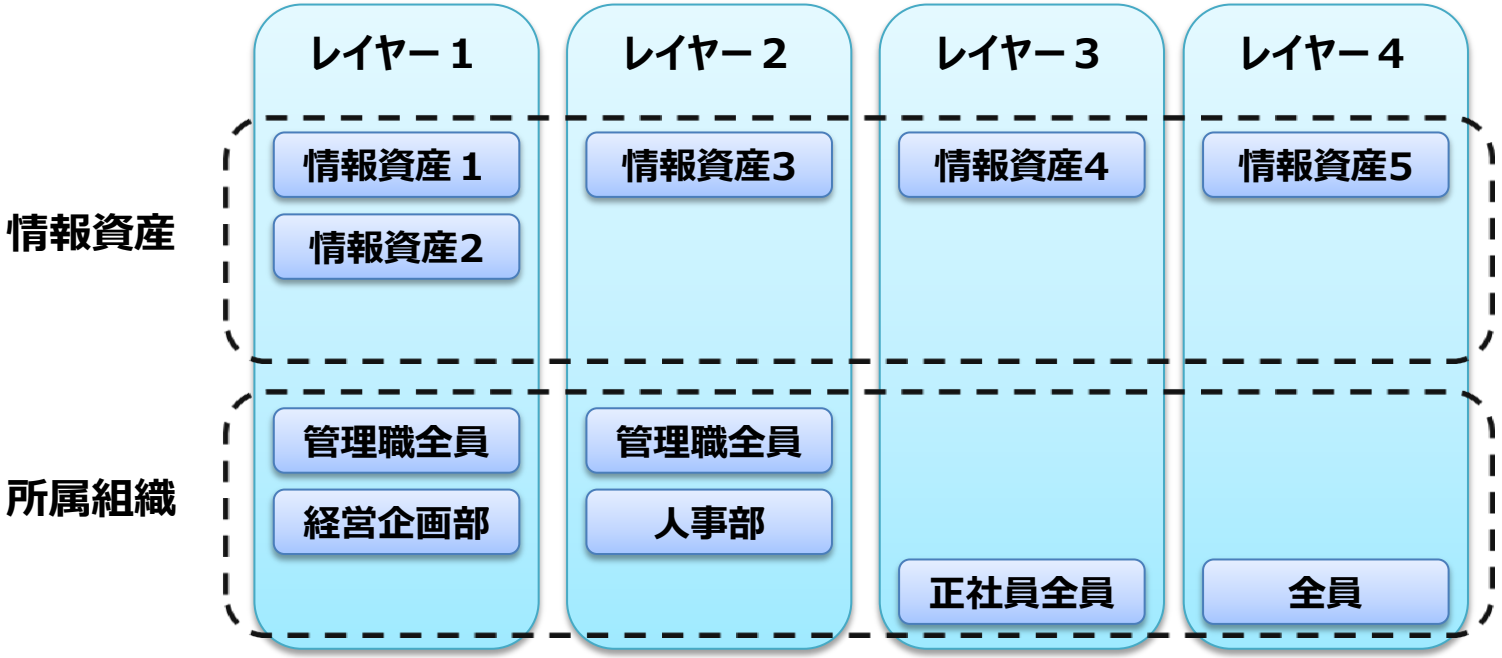




②ワークフローによる権限管理

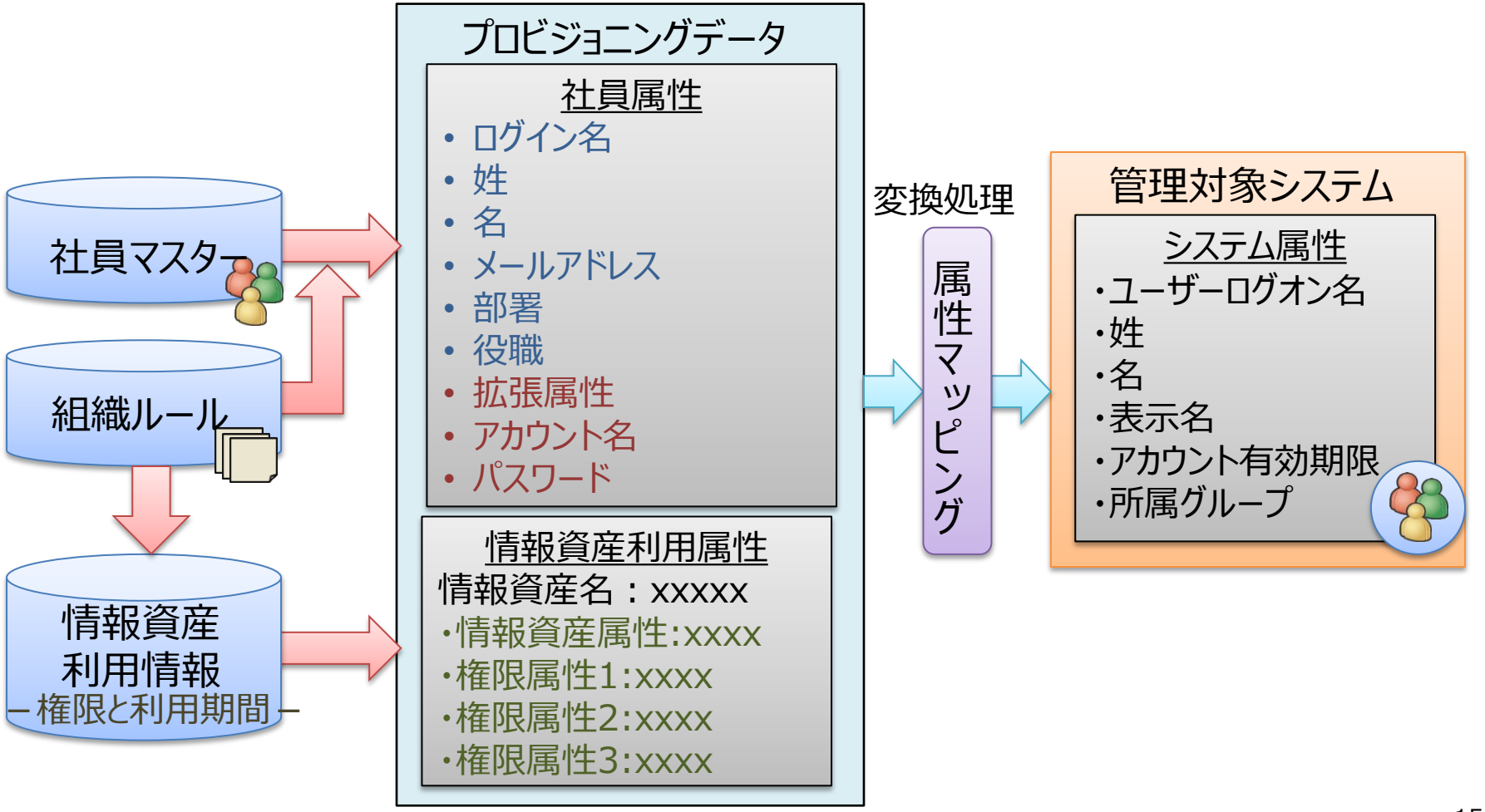
■ 情報資産を分類し申請可能な情報資産を制御

- 重要度や機密度などに応じてセキュリティレイヤーを作成
- 情報資産をセキュリティレイヤーに分類
- セキュリティレイヤーごとに利用可能者の条件を設定



3）自動プロビジョニング

社員マスターや情報資産利用情報を元に管理対象システムにアカウント情報を配信



複雑なプロビジョニングも簡単

■ 属性マッピングで出来る事

- 条件分岐
  - ルールに「If/Elseif/Else」を使用することで、条件分岐が可能。
- 不要文字削除
  - trimメソッドにより、文字列の前後から不要なスペース等の指定した文字を削除
- 大文字/小文字変換
  - lower/upper/properメソッドにより、大文字・小文字変換が可能
- ランダム文字列生成
  - randomメソッドにより、ランダム文字列を生成

設定例）

属性	設定	出力
アカウント有効	#{if}(<退職フラグ>)==“0”)1#{elseif} (<退職フラグ>)==“1”)0#{else}1#{end}	退職フラグが1なら0 退職フラグが0なら1 退職フラグが0か1以外なら1
性別	#{if}(<性別フラグ>==“0”)男性 #{elseif}(${EXT_ATTR_0003}==“1”)女性#{end}	性別フラグが0なら”男性” 性別フラグが1なら”女性”
氏名	<姓>.trim(“ ”) <名>.trim(“ ”)	“ 阿井出 ”+” 絵夢 “→”阿井出 絵夢”
ログオン名	<ユーザーID>.lower	“SOLITON”→”soliton”
パスワード	${COMMON.random(abcdef),5}	abdce

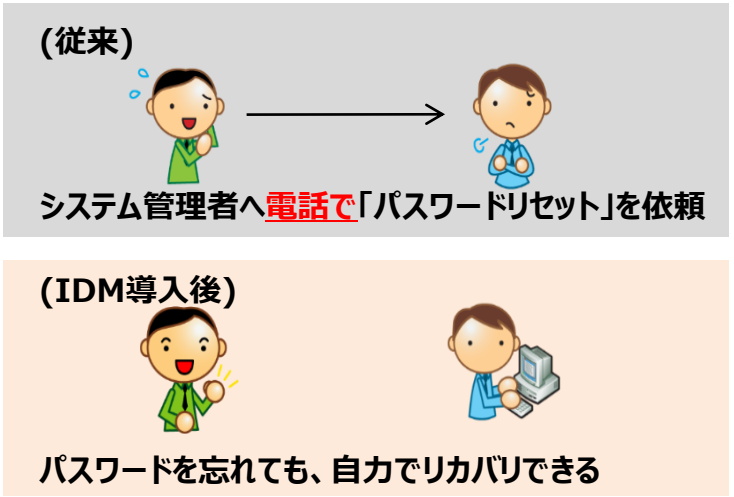
ジョブスケジューラの搭載

- 全処理をジョブとしてスケジュール実行可能
  - インポート処理
  - 各種マスター上での適用開始・終了処理
  - 情報資産の利用開始・終了処理
  - メール通知処理
  - アカウント同期処理　など

4）認証情報の管理

■パスワードの一元管理

- パスワードポリシ機能
  - パスワードの複雑さを定義
- パスワードの一括変更
  - ID管理システム上で全システムパスワードを一括変更
- パスワードのセルフリセット
  - メール連携によりパスワードリセット



5）ログ管理と可視化

■ 取得できるログ一覧

取得単位	ログ種類	内容	備考
システム	システム管理ログ	システム管理者の操作記録	サイトの設定、システム管理者登録、アクセス制御設定等
	システムログ	システムの動作ログ	syslogサーバーへ送信可
	ログインログ	システム管理者のログイン履歴	いつ、誰が、どこから、どのような権限でログインしたのか？
サイト	アカウント配信ログ	連携先システムへの処理結果を記録	いつ、どのシステムの、どのIDに、どのような変更を行ったのか？履歴と現在のステータス
	サイト管理ログ	サイト管理者の操作記録	サイト設定(ユーザー管理、ルール設定、パスワードポリシーなど)に対して、いつ、誰が、どんな変更を行ったのか？
	社員操作ログ	社員マスターの更新履歴	社員マスター対して、いつ、どんな変更を行ったのか？
	情報資産利用ログ	**情報資産の利用権限の履歴(情報資産別)**	**どの情報資産に、誰が、どの期間、どのような権限が付与されているか**
		情報資産の利用権限の履歴(個人別)	**誰に、どの情報資産に対して、どの期間、どのような権限が付与されているか**
	ログインログ	サイト管理者のログイン履歴	いつ、誰が、どこから、どのような権限でログインしたのか？

ログの活用①権限棚卸し

情報資産管理者に「**誰に、どのような権限で、いつまで、どのような理由で付与されたのか**」を可視化することで、アクセス権限の棚卸を実現

ファイルサーバのフォルダアクセス権管理の例）

新規利用申請 | 利用変更申請 | エクスポート | すべて | 検索キーワードを入力して下さい | 検索

ログイン名 ▼▲	氏名▼▲	部署(主)▼▲	利用状況 ▼▲	利用開始日 ▼▲	利用終了日 ▼▲	利用開始事由 ▼▲
tyamazaki01	山崎　智也	マーケティング部	利用終了	2013/04/01	2014/03/31	組織(部署：開発部)
tyamazaki01	山崎　智也	マーケティング部	利用中	2014/04/01		組織(部署：マーケティング部)
khiraishi01	平石　和男	営業部	利用中	2014/05/01	2014/09/30	申請
kkuroda01	黒田　官兵衛	開発部	利用中	2014/04/01		組織(役職：課長)
smatsui01	松井　繁	開発部	利用開始前	2015/10/01		申請
tkoishikawa01	小石川　哲也	マーケティング部	利用終了	2012/04/01	2013/11/30	組織(部署：マーケティング部)

利用権限の詳細がわかる

申請内容の詳細がわかる

ログの活用②利用者に可視化

利用者に**「どの情報資産に、どの権限で、いつまでアクセス可能か」**まで可視化することで、利用期間の延長や権限変更など申請によって自己解決が可能

すべて　検索キーワードを入力して下さい　検索

情報資産名 ▼▲	情報資産タイプ▼▲	利用状況 ▼▲	利用開始日 ▼▲	利用終了日 ▼▲	利用開始事由 ▼▲
01.計画/売上フォルダ	共有フォルダ	利用終了	2013/04/01	2014/03/31	組織(部署 : 開発部)
01.計画/売上フォルダ	共有フォルダ	利用中	2014/04/01		組織(部署 : マーケティング部)
02.業務フォルダ	共有フォルダ	利用中	2014/04/01		組織(部署 : マーケティング部)
マーケティング部G	ADグループ	利用中	2014/04/01		組織(部署 : マーケティング部)
A社プロジェクトML	メーリングリスト	利用中	2014/04/01		組織(部署 : マーケティング部)
顧客情報管理	CRMシステム	利用開始前	2014/09/01	2014/12/31	申請

社員情報の可視化と棚卸

部門マネージャや社員情報管理担当者に、**「指定部署の社員情報を可視化」**することで利用部門による社員情報の棚卸しを効率よく行うことが可能

社員情報一覧画面イメージ

ログイン名	氏名	メールアドレス	(主)部署	(主)役職
kkurata	倉田和人	kkurata@idm-demo2.local	営業部	部長
tasanuma	浅沼正	tasanuma@idm-demo2.local	営業部/営業1課	課長
mhanafusa	華房誠	mhanafusa@idm-demo2.loca		
thaken	派遣太郎	thaken@idm-demo2.local		

ログイン名	kkurata
入社日	1994/4/1
退社日	
姓	倉田
名	和人
メールアドレス	kkurata@idm-demo2.local
（主）部署	営業部
（副）部署	
（主）役職	部長
（副）役職	
ＡＤアカウント	kkurata
APアカウント1	Kkurata
APアカウント２	Kazuhito.kurata

権限管理イメージ

Soliton

人事異動に連動した権限管理

人事異動

組織ルール

期間管理

社員

組織

情報資産

情報資産の利用情報

開始

変更

終了

権限付与
変更・削除

申請に基づいた権限管理

申請

承認

確認と是正

申請制御

セキュリティ
レイヤ

情報資産管理者

	氏名	部署(主)	利用状況	利用開始日	利用終了日	利用開始申由
ysaki01	山崎 智也	マーケティング部	利用終了	2013/04/01	2014/03/31	組織(部署：開発部)
tyamazaki01	山崎 智也	マーケティング部	利用中	2014/04/01		組織(部署：マーケティング部)
thiraishi01	平石 和男	営業部	利用中	2014/05/01	2014/09/30	申請
tkuroda01	黒田 官兵衛	開発部	利用中	2014/04/01		組織(役職：課長)
smatsui01	松井 繁	開発部	利用開始前	2015/10/01		申請
tkoishikawa01	小石川 哲也	マーケティング部	利用終了	2012/04/01	2013/11/30	組織(部署：マーケティング部)

ROLE：営業担当

権限：変更

役割に応じたアクセス管理を実現

情報資産管理者 	アクセス許可条件を決め、定期的に棚卸を行う （申請条件や権限付与ルールの定義と権限棚卸し）
部門マネージャ 	業務上必要な権限であることを判断する （承認に基づくアカウント権限付与）
運用担当 **（サイト管理者）** 	各システムに正確に設定を反映する （ルールによる自動設定や差分自動チェック）
IT監査担当 	統制状況を監査する （操作・変更履歴のログや各エビデンス確認）
利用者 	付与された権限を把握し、許可された情報資産のみに アクセスする

AD管理において使える機能

AD管理において使える機能

- 単体機能
  - アカウント管理
  - グループ管理
  - パスワード管理
  - スキーマ拡張属性管理
  - ライセンス管理
- システム連携
  - 認証基盤連携
  - ログ管理連携

アカウント管理（1/2）

- 人事イベント対応（人事システム連携）
  - 入社
    - アカウントの作成
  - 部署異動／昇格・降格
    - アカウントの属性変更（＆グループ変更）
  - 属性変更
    - アカウントの属性変更
  - 出向／休職
    - アカウントの無効化
      - 無効化属性を設定
      - アカウント有効期限を設定
  - 退社
    - 一定期間アカウントを無効化してから、アカウントを削除

アカウント管理（2/2）

■人事管理外社員登録

- 契約開始
  - 社員新規登録(代理)申請
    - 入力内容に合わせてアカウントを自動作成
- 社員情報棚卸
  - 所属部門の社員情報を確認
- 契約終了
  - 社員情報変更(代理)申請
    - 契約終了日を入力して申請
    - 契約終了日に合わせてアカウントを削除

グループ管理

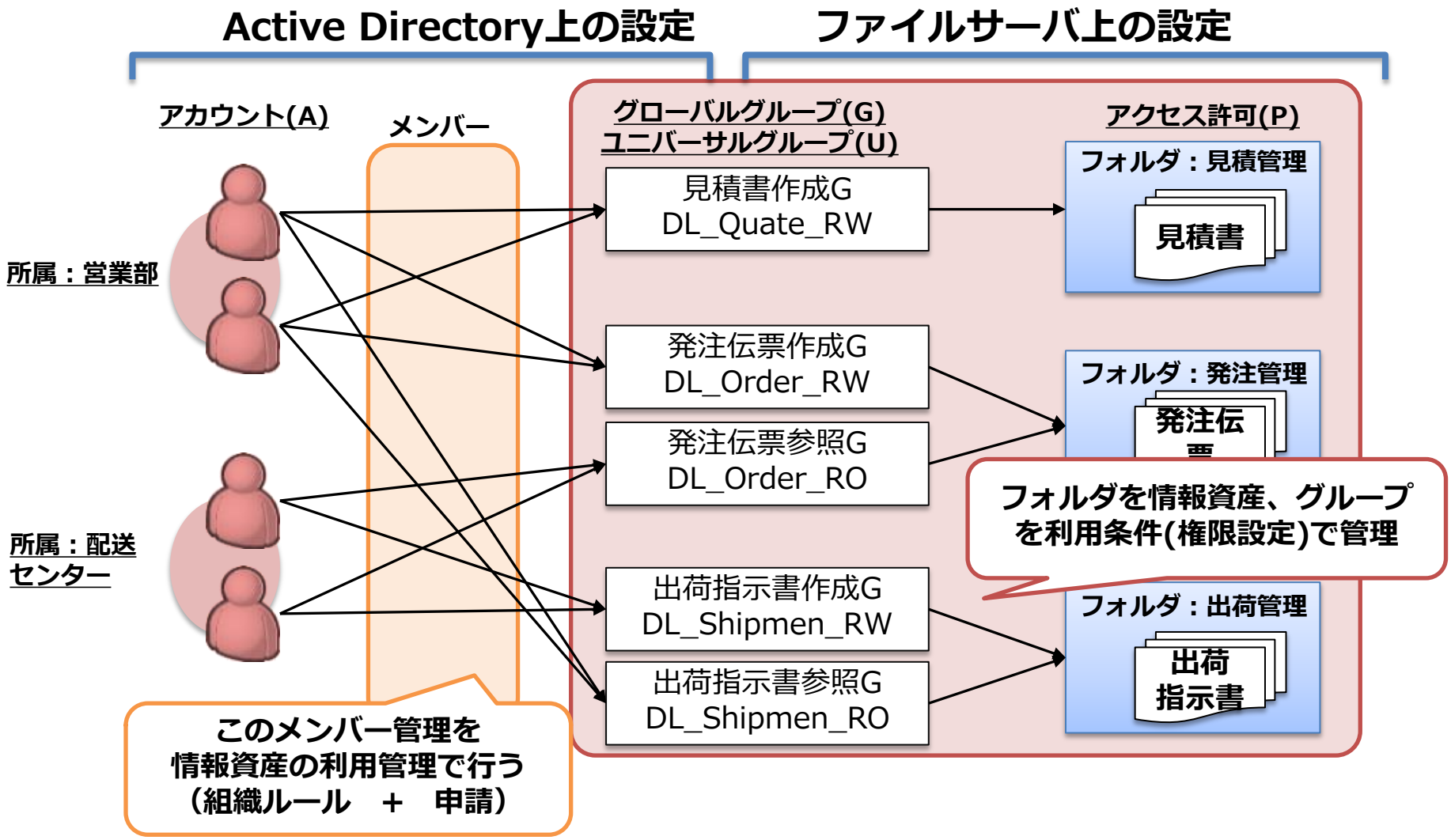
■ 人事イベント対応

- 部門のセキュリティグループの自動更新
  - 部署ごとのセキュリティグループを情報資産として作成
  - 発令日に合わせた新所属部署グループへのメンバー追加
  - 引継期間終了後の旧所属部署グループからのメンバー削除
  - 兼務所属部門も含めた自動更新

■ ワークフロー対応

- ファイルサーバアクセス権用グループの管理
  - 管理対象フォルダを情報資産として登録
  - フォルダのアクセス権をグループで設定
  - 情報資産とグループを属性マッピングで紐付
    - アクセス権種別が複数ある場合は情報資産に種別ごとにグループを紐付

アクセス権管理の概要


Active Directory上の設定
ファイルサーバ上の設定
アカウント(A)
メンバー
グローバルグループ(G)
ユニバーサルグループ(U)
アクセス許可(P)
所属：営業部
所属：配送センター
見積書作成G
DL_Quate_RW
発注伝票作成G
DL_Order_RW
発注伝票参照G
DL_Order_RO
出荷指示書作成G
DL_Shipmen_RW
出荷指示書参照G
DL_Shipmen_RO
フォルダ：見積管理
見積書
フォルダ：発注管理
発注伝票
フォルダ：出荷管理
出荷指示書
フォルダを情報資産、グループを利用条件(権限設定)で管理
このメンバー管理を
情報資産の利用管理で行う
（組織ルール　＋　申請）

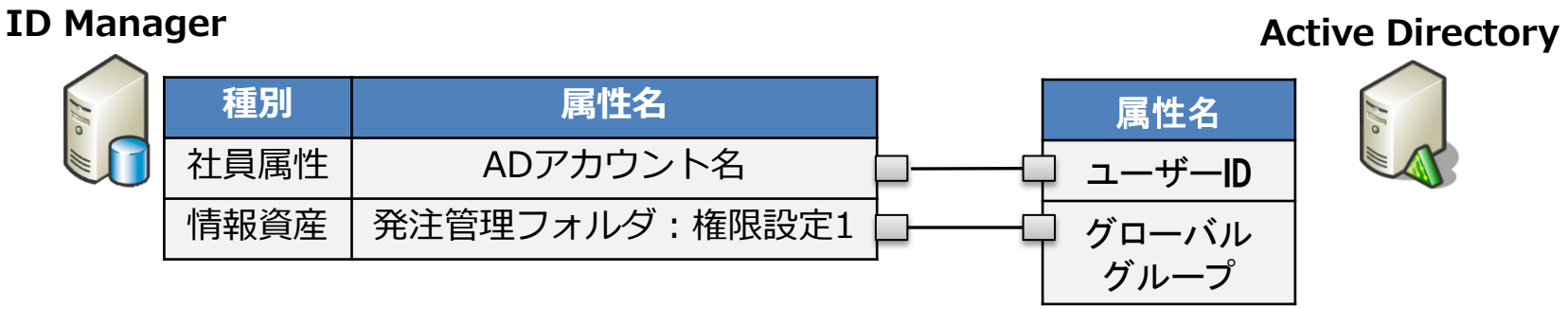
フォルダを情報資産として登録

■ 情報資産を登録する

情報資産名	権限設定		権限	
	種別	権限設定名	権限	権限値
発注管理フォルダ	権限設定1 (選択)	アクセス権	作成	DL_Order_RW
			参照	DL_Order_RO

アクセス権の選択肢

■ 属性をマッピングする（アカウント同期設定）



アクセス権の付与方法

■ 人事異動に合わせて自動設定

– 部署の組織ルールで設定

情報資産名	権限設定1
見積管理フォルダ	作成：RW
発注管理フォルダ	作成：RW

名前：山崎智也
ログインID：Tyamazaki01
所属：営業部

■ 申請に合わせて設定

– 必要に応じて情報資産利用申請を行う

情報資産タイプ	共有フォルダ
情報資産名	出荷管理フォルダ
情報資産管理者	浅沼　正
情報資産セット名	配送センター所管

アクセス権	
利用開始日	
利用終了日	

パスワード管理

- WEBからのパスワード変更
  - ID管理システムの利用者ポータル上で、パスワード変更
  - ドメインログオンパスワードだけでなく、設定された複数システムのパスワードも一括変更
- Windowsドメインパスワード変更連携
  - Windowsドメイン上で変更した新しいパスワード情報をID管理システム上に自動同期
- 上席者への依頼によるパスワードリセット
  - 社員情報の代理変更申請でパスワードを初期化
- パスワードのセルフリセット
  - パスワード忘れ時に、

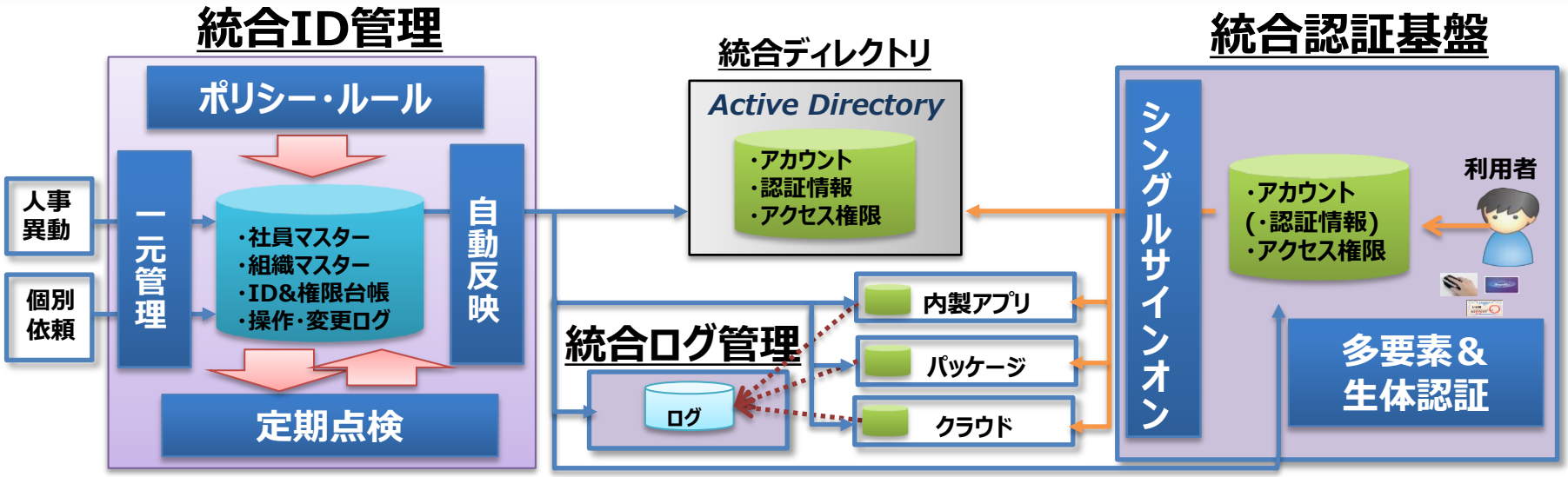
スキーマ拡張属性管理

- Exchange Online用属性の管理
  - ディレクトリ同期環境
    - オンプレミスのAD上でスキーマ拡張
    - ID管理システムで拡張した属性を設定
  - クラウドID環境
    - ID管理システムでExchange Online属性を設定
      - ExchangeOnlineライセンスを適用するとメールボックスが自動作成され更新できるようになる
      - メールボックス作成には時間が掛かる為(30秒~1分程度)、直ぐに実行すると処理はエラーになるので注意が必要

ライセンス管理

- Office365のライセンス管理
  - 利用ユーザーへのライセンス適用
    - 適用するライセンス契約を選択
    - ライセンス契約内で利用する機能を選択
      - Exchange Onlineを有効にするとメールボックスが自動作成される
  - 情報資産としてライセンス管理
    - ライセンスを情報資産として登録
    - 組織ルール、申請によってライセンスを付与
      - 申請付与の場合、付与可能なライセンス数を設定可能
- ライセンスの棚卸
  - ライセンス管理者を情報資産管理者として登録
  - いつでも、ライセンス適用情報を閲覧・検索可能

システム連携



- 統合認証基盤連携
  - 多要素認証や生体認証で、Windowsログオンやアプリケーション認証を強化
  - 各アプリケーションへの認証はシングルサインオンに
  - ランダムパスワードなど、パスワードを複雑化＆隠ぺい化して認証強化

- 統合ログ管理連携
  - 統合ID管理が管理する情報を利用して、名寄せに必要な統合ID情報、所属部署情報などをログに追加する事で、高度なログ解析・活用が可能

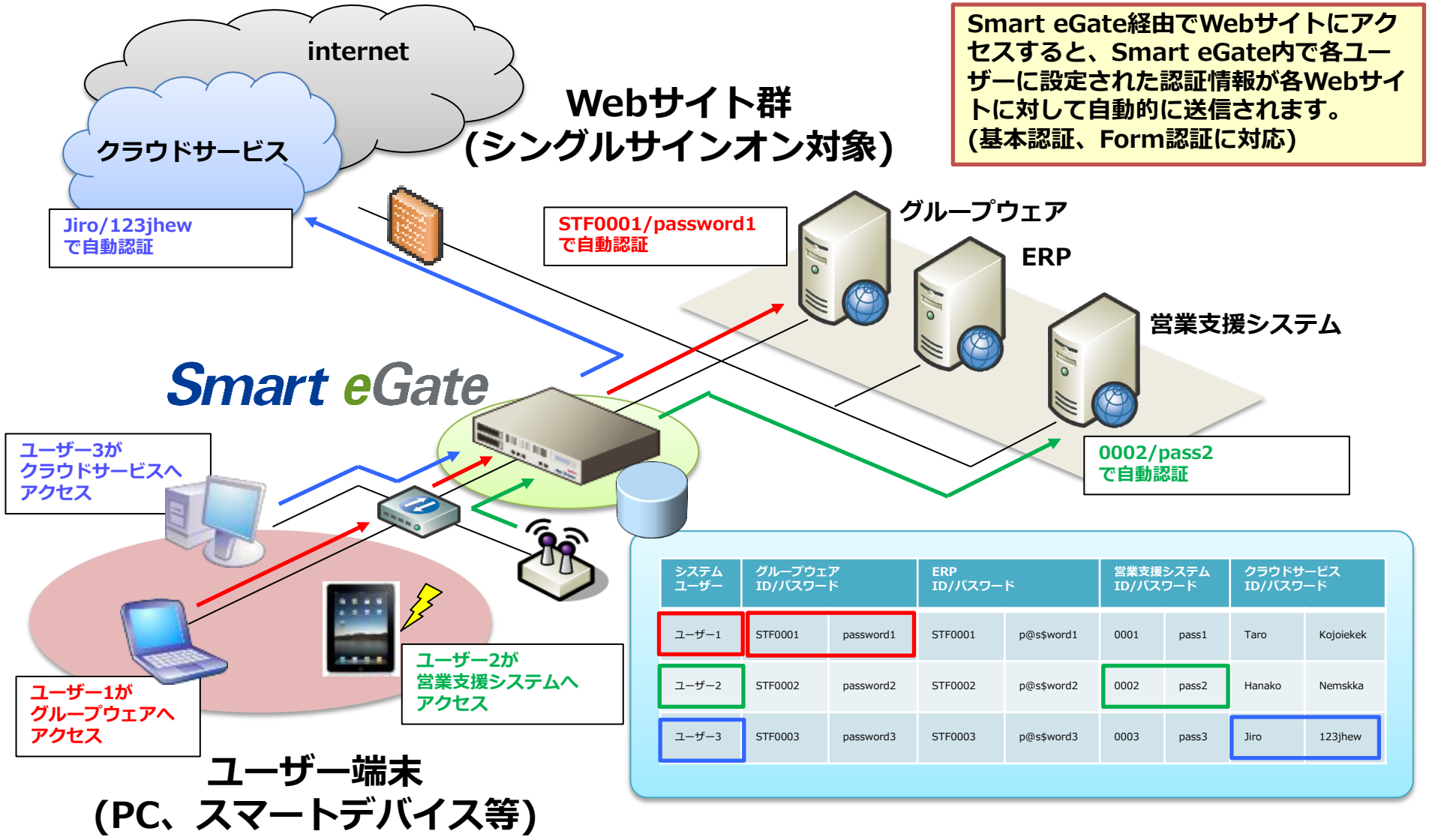
統合認証基盤連携

- Smart eGate連携
  - Active Directoryと連携して、WEBアプリケーションへのシングルサインオンを実現
  - WEBアプリケーションへのアクセス制御を実現

- SmartOn ID連携
  - Windowsログオン認証をICカードや生体情報を使って認証強化
  - .Netアプリケーション、DOMINO、WEBアプリケーションへのシングルサインオンを実現
  - PC利用における各種アクセス制御を実現

Smart eGateによるSSO

Smart eGate経由でWebサイトにアクセスすると、Smart eGate内で各ユーザーに設定された認証情報が各Webサイトに対して自動的に送信されます。
(基本認証、Form認証に対応)



システム ユーザー	グループウェア ID/パスワード		ERP ID/パスワード		営業支援システム ID/パスワード		クラウドサービス ID/パスワード	
ユーザー1	STF0001	password1	STF0001	p@s$word1	0001	pass1	Taro	Kojoiekek
ユーザー2	STF0002	password2	STF0002	p@s$word2	0002	pass2	Hanako	Nemskka
ユーザー3	STF0003	password3	STF0003	p@s$word3	0003	pass3	Jiro	123jhew

システム連携：統合ログ管理

Soliton

■ アクセスログと属性マスターを使ったログ分析

- 複数ログの串刺し検索可能
  ＝＞問題発生時に何が起きたのか時系列に経過がわかる
- マネージャが自部署ログを確認可能
  ＝＞業務に不要な操作・アクセスがあれば発見可能

AD監査ログ

日時	ユーザーID	ログ内容
2015/11/1 10:00	1111111	*******
2015/11/1 10:15	2222222	*******
2015/11/1 10:30	3333333	*******
2015/11/1 11:00	4444444	*******

PC操作ログ管理

InfoTrace PLUS

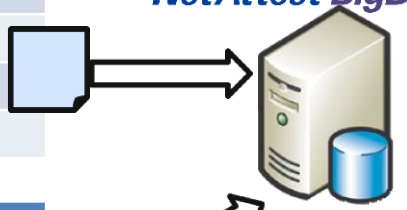
日時	ユーザーID	ログ内容
2015/11/1 9:55	smatsuui	*******
2015/11/1 10:10	Tyamazaki	*******
2015/11/1 10:15	khiraishi	*******
2015/11/1 11:20	Kkurata	*******

ID管理システム

Soliton ID Manager

姓名	統合ID	部署名	ログA	ログB
山崎智也	t.yamazaki	営業部	1111111	Tyamazaki
倉田和人	k.kurata	総務部	2222222	Kkurata
松井繁	s.matsui	開発部	3333333	Smatsui
平石和夫	k.hiraishi	営業部	4444444	khiraishi

NetAttest BigData



・ログごとに異なるユーザーIDを名寄せ
・ログ解析に必要なその時点での属性を
ログに追加

日時	姓名	部署名	ソース	ログ内容
2015/11/1 9:55	松井繁	開発部	ログB	*******
2015/11/1 10:00	山崎智也	営業部	ログA	*******
2015/11/1 10:10	山崎智也	営業部	ログB	*******
2015/11/1 10:15	倉田和人	総務部	ログA	*******
2015/11/1 10:15	平石和夫	総務部	ログB	*******
2015/11/1 10:30	松井繁	開発部	ログA	*******
2015/11/1 11:00	平石和夫	営業部	ログA	*******
2015/11/1 11:20	倉田和人	総務部	ログB	*******