統合ID管理入門

(株) NTTデータ

山田　達司

本日の内容

- 自己紹介
- 統合ID管理とは
- 主要概念の説明
- 統合ID管理における課題
  - アカウント管理
  - 認証
  - 認可
  - 属性情報管理
  - ライフサイクル管理
  - 証跡管理

自己紹介

山田　達司
(株) NTTデータ　ﾋﾞｼﾞﾈｿｽﾘｭｰｼｮﾝ事業本部　ﾈｯﾄﾜｰｸｿﾘｭｰｼｮﾝﾋﾞｼﾞﾈｽﾕﾆｯﾄ
ｵﾌｨｽｿﾘｭｰｼｮﾝ担当　課長　ｼﾆｱITｽﾍﾟｼｬﾘｽﾄ(ｾｷｭﾘﾃｨ)

■1997年～　情報ｼｽﾃﾑ部において施策推進およびｼｽﾃﾑ開発･運用に従事
- ｾｷｭﾘﾃｨ対策：ｼﾝｸﾞﾙｻｲﾝｵﾝ、ID管理、PKI、ｼﾝｸﾗｲｱﾝﾄ
- 情報共有：ﾎﾟｰﾀﾙ、ﾒｰﾘﾝｸﾞﾘｽﾄ、文書共有ｼｽﾃﾑ
- モバイル：携帯電話によるｲﾝﾄﾗﾈｯﾄｱｸｾｽ
- ｸﾞﾙｰﾌﾟ経営：NTTﾃﾞｰﾀｸﾞﾙｰﾌﾟ向け仮想ﾈｯﾄﾜｰｸ

■2004年～　VANADISｿﾘｭｰｼｮﾝの企画･開発およびそれを適用したSIに従事
- 統合ID管理製品：VANADIS Identity Manager/VANADIS SSO
- SaaS/クラウド構築基盤：VANADIS SaaS Platform　他

■業務外ではモバイルデバイスの普及に努める。1995年より米国製PDAであるPalmの日本語化ソフト(J-OS)開発、書籍執筆、開発者コミュニティの育成などに努める。

- 自己紹介
- **統合ID管理とは**
- 主要概念の説明
- 管理の統合
  - アカウント管理
  - 認証
  - 認可
  - 属性情報管理
  - ライフサイクル管理
  - 証跡管理

なぜ統合ID管理が必要なのか

コンプライアンスの動向

情報の改ざん、漏洩などによる事件、事故が多発

↓

J-SOX法など法規制強化

↓

ITによる内部統制の必要性

↓

■適切な人と権限の管理

ITシステムの動向

汎用機による中央処理型

↓

C/S、Webの普及

↓

IT運用の分散化、負担増加

↓

■利便性、運用効率低下
■情報の信頼性、安全性低下

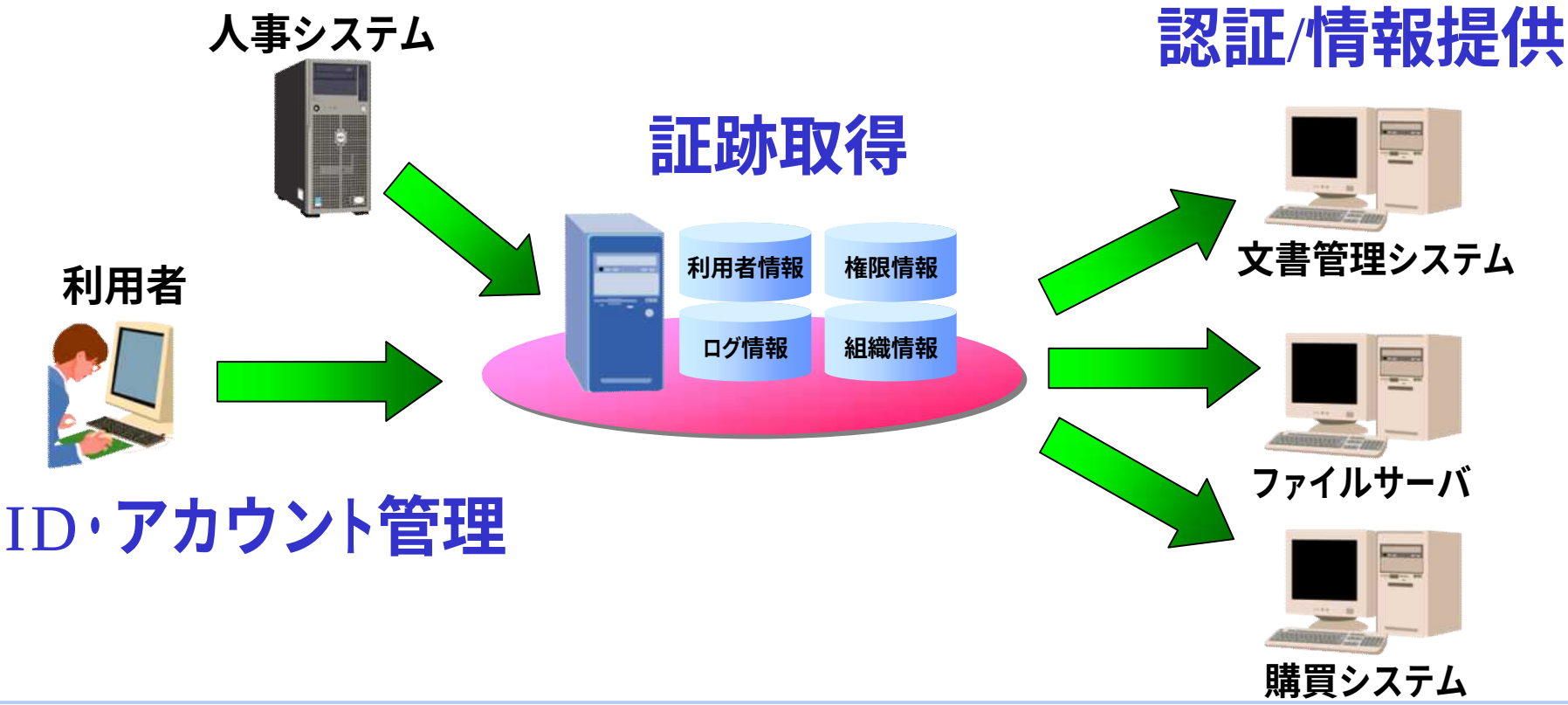
管理すべき項目の増加

全体最適化が必要 → **統合ID管理**

管理対象システムの増加

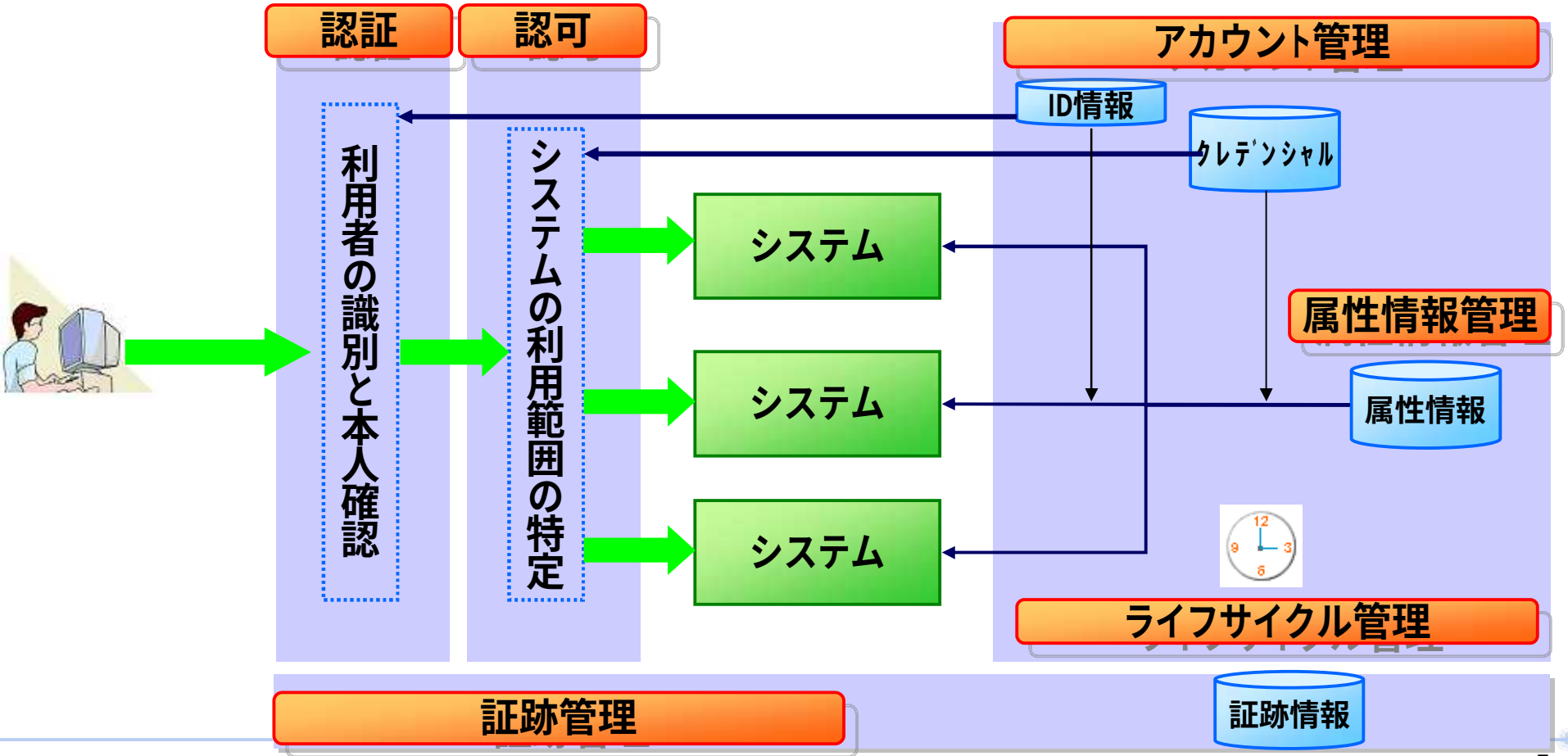
統合ID管理とは

統合ID管理とは、必要な証跡を取得しつ、企業内のポリシーに基づき定義されたプロセスに沿ってID･アカウント情報の管理を行い、業務システムに認証機能及び情報提供を行うこと

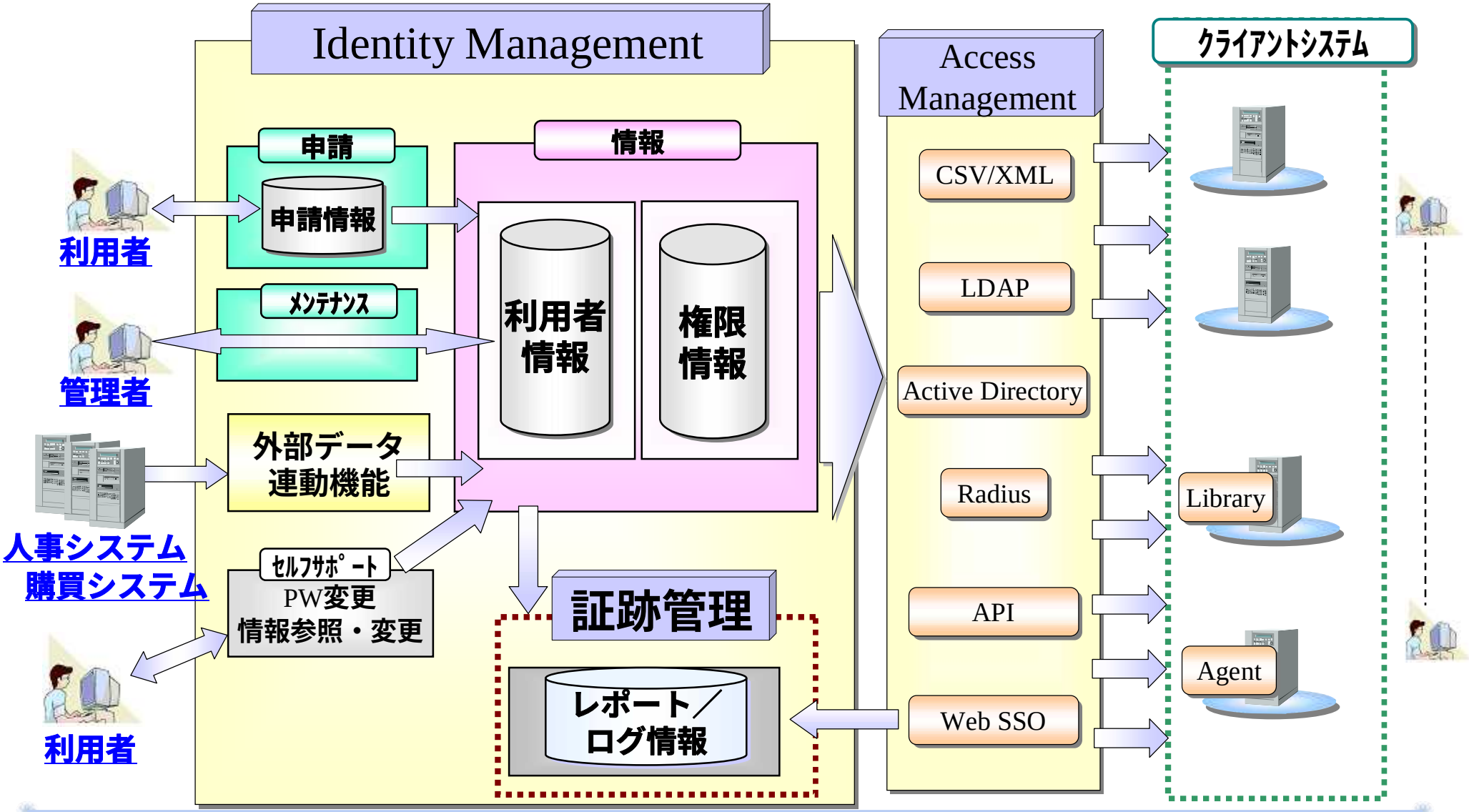


統合ID管理を構成する６つの機能

統合ID管理を実現するためには「アカウント管理」、「認証」、「認可」、「属性情報管理」、「ライフサイクル管理」、「証跡管理」からなる6機能が必要である。統合ID管理とシステムはID情報の更新時とユーザのシステム利用時に連携を行う。



統合ID管理の代表的な機能構成



1. 自己紹介
2. 統合ID管理とは
3. 主要概念の説明
4. 管理の統合
   - アカウント管理
   - 認証
   - 認可
   - 属性情報管理
   - ライフサイクル管理
   - 証跡管理

IDとは？

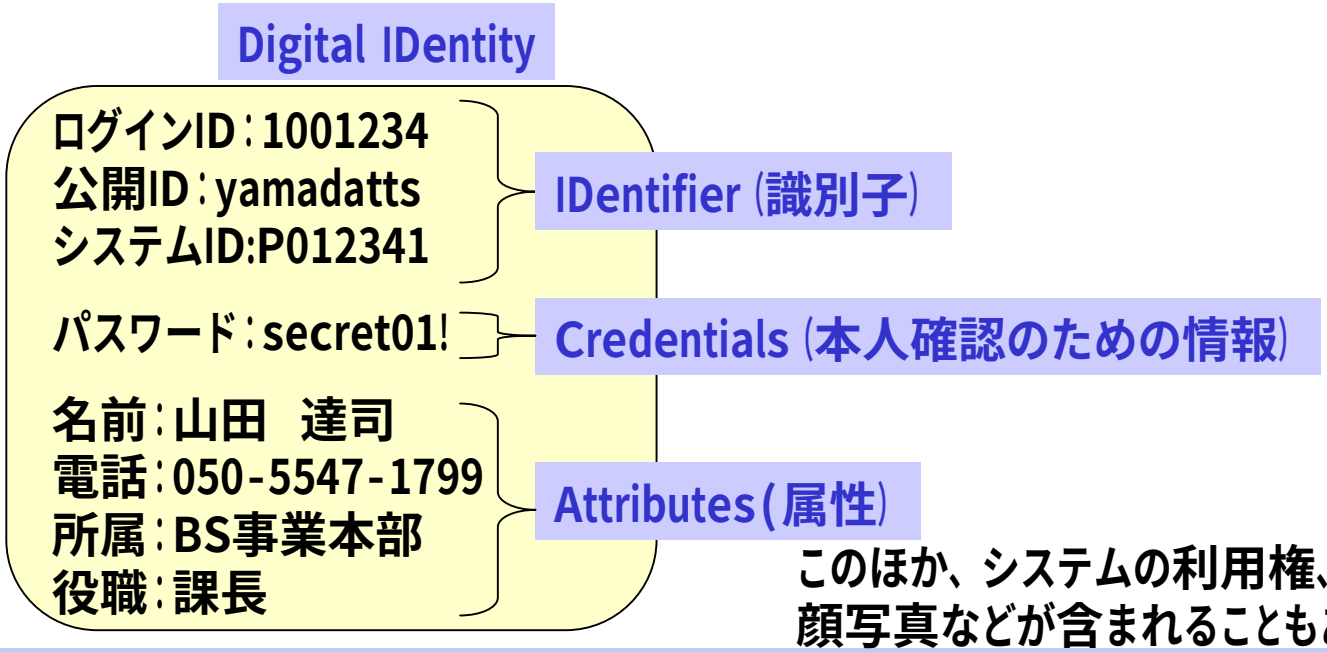
■IDには2つの意味があり、混同されることが多い。

Digital IDentity（デジタルアイデンティティ）

・・・ITシステムにおける利用者の投影のこと 。ID管理のIDはこちら

IDentifier(アイデンティファイア)

・・・利用者を特定するための識別子のこと。用途に応じて複数持つことも可能



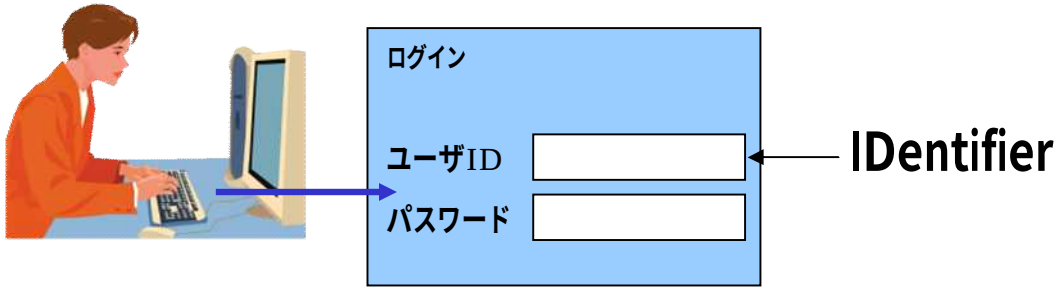
このほか、システムの利用権、資格情報、
顔写真などが含まれることもある。

使い分けられるID

2つのIDはコンテキストにより使い分けられているが、誤解の元となることも多い。

本資料ではデジタル・アイデンティティを「アカウント」と呼ぶ

「IDを入力してください」	IDentifier
「システム上にIDを作りました」	Digital IDentity
「社員番号をIDとして使っています」	IDentifier
「あなたのIDは無効になりました」	Digital IDentity
「社員と協力会社社員は異なるIDを使います」	IDentifier
「IDの払い出しをお願いします」	????
「人事システムと連動してIDを管理しています」	????

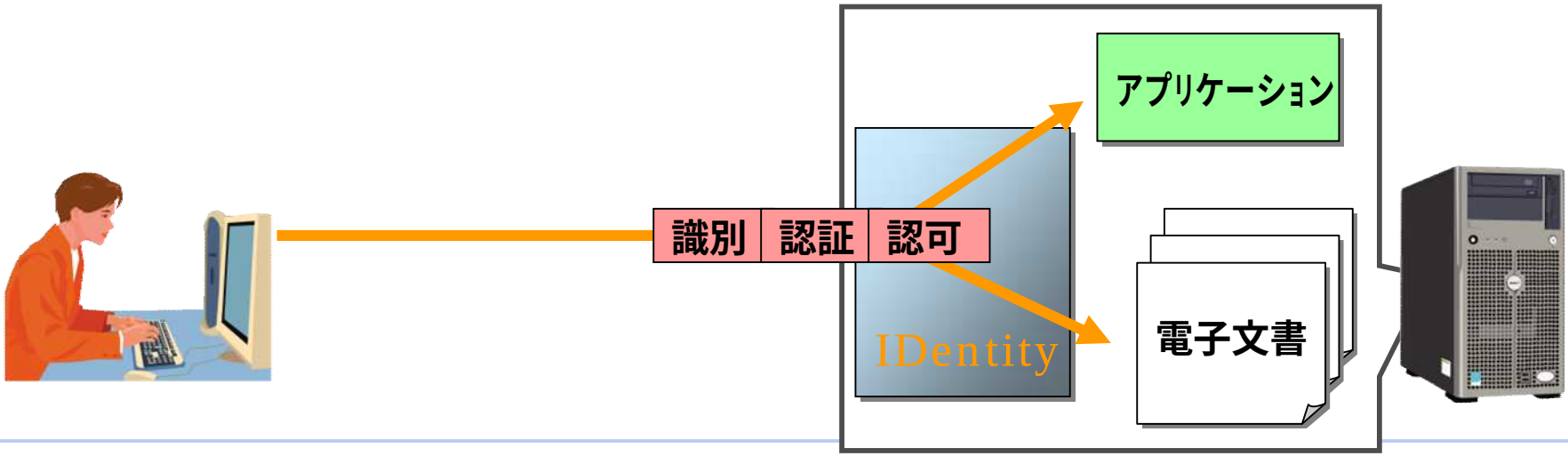


アカウント（Digital Identity）の用途

アカウント（Digital Identity）の主な用途はシステム内の機能や情報を利用させることである。

利用者は以下のプロセスを経てシステム内の機能や情報を利用する

- 識別：Identification
- 認証：Authentication
- 認可: Authorization

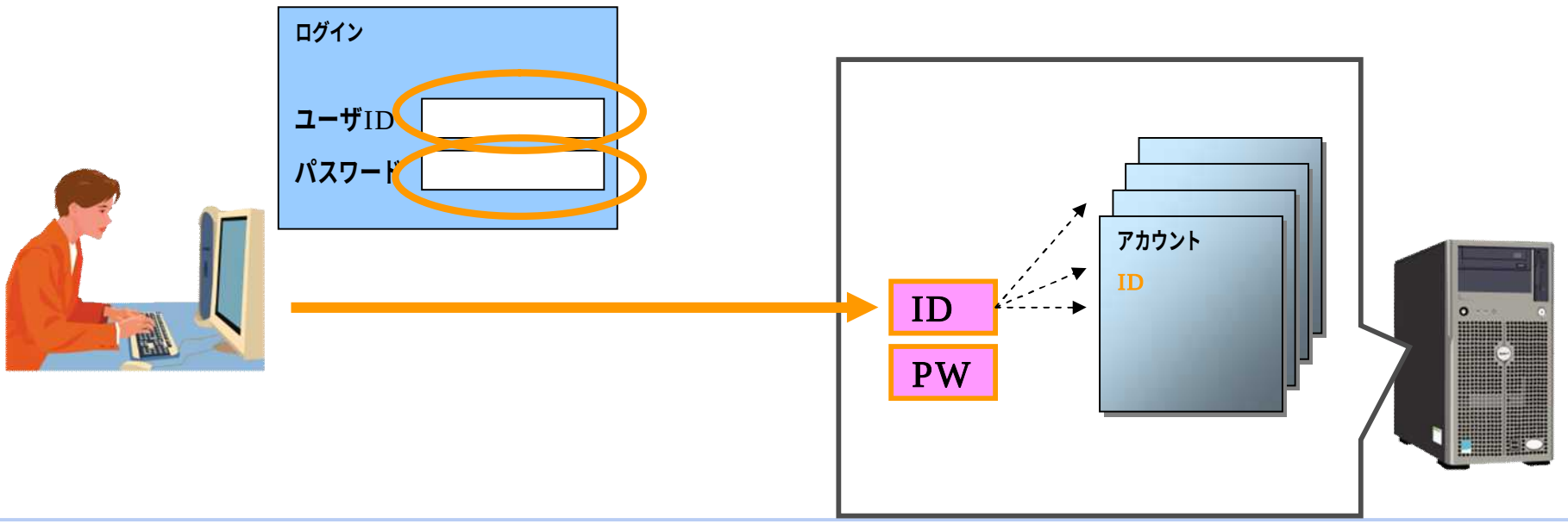


識別(Identification)とは

- 利用者がITシステムにアクセス

  →　誰？　(「識別」)

■ 利用者が誰であるか見分けること



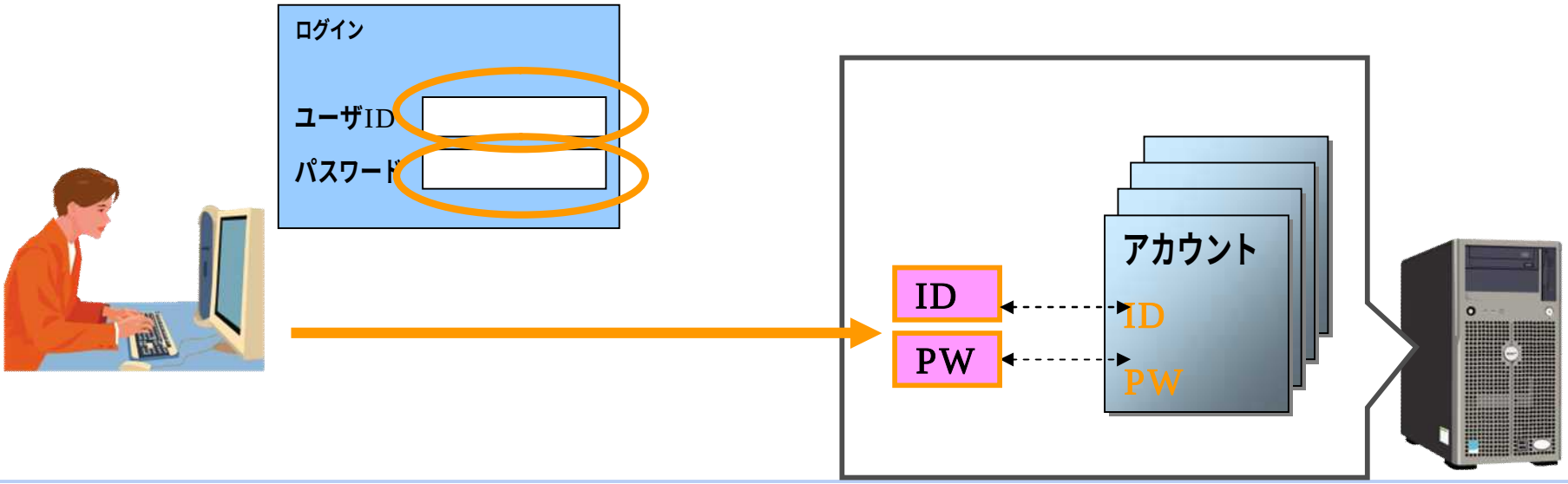
認証(Authentication)とは

- 「識別」により誰がアクセスしてきたか判明

  →　本人か？　(「認証」)

■ 利用者の「識別」を行った上で利用者が本人であるか確かめること

※　認証にはパスワード以外にもICカード認証や生体認証など様々な方式がある

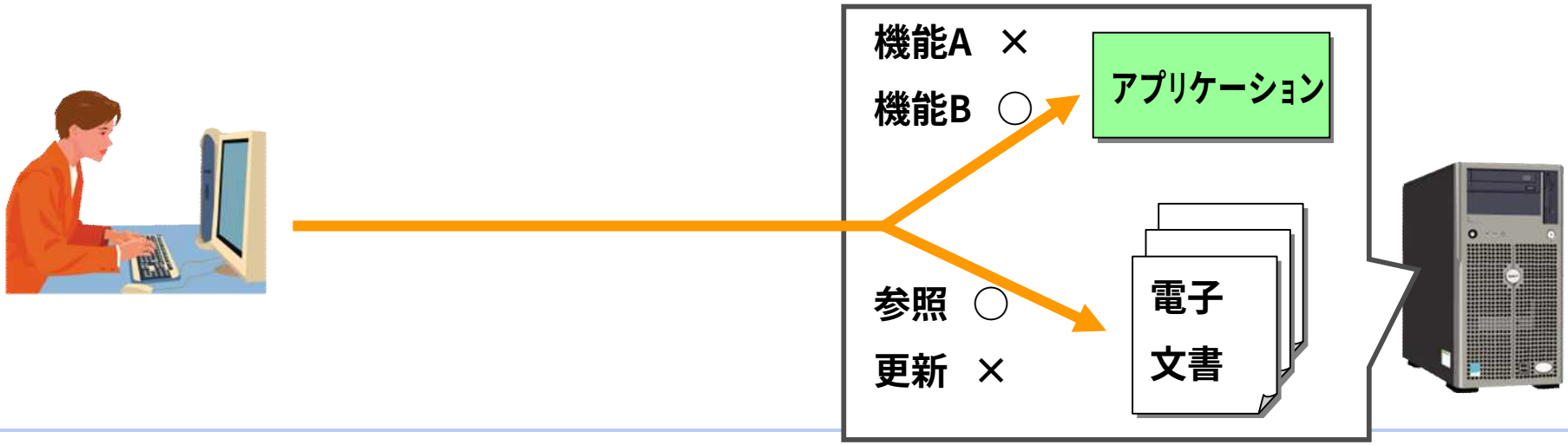


認可(Authorization)とは

- 「認証」により本人だと判明

  →　何でもやらせていいか？　(「認可」)

■ 「認証」された利用者がシステムを利用する際に、機能・情報をどこまで利用させるかを決定すること



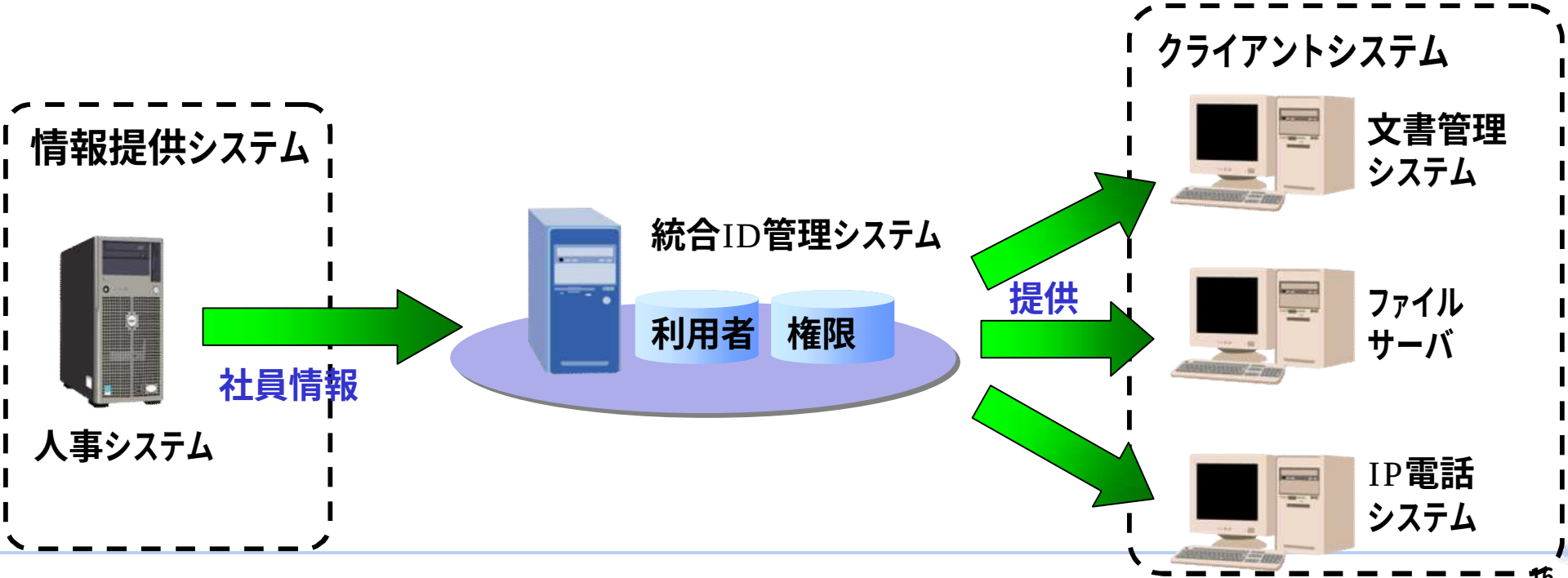
連携するシステム

- 「統合ID管理」システムは利用者や組織に関する基本情報を人事システムなどから取得

■ ID管理情報の源泉となるシステム → 情報提供システム

- 「統合ID管理」システムはアカウント情報や認証･認可などを各システムに提供

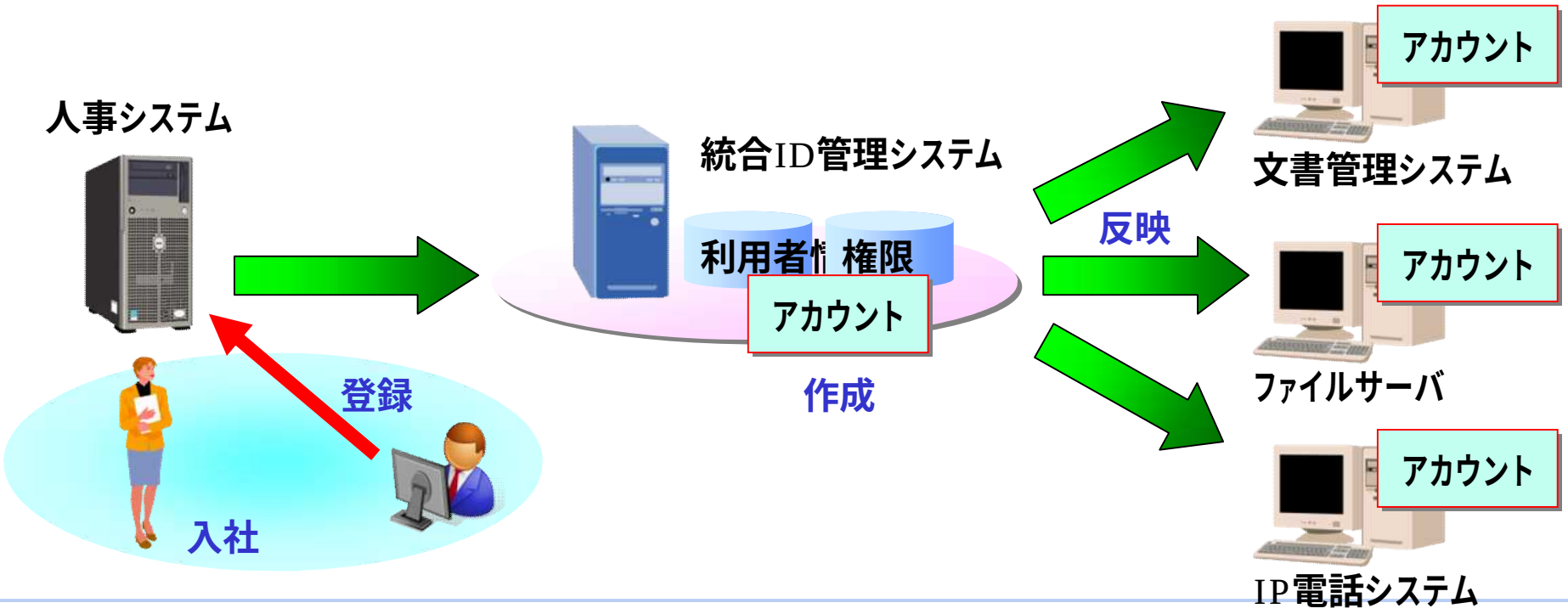
■ ID管理情報や認証、認可の提供先となるシステム → クライアントシステム



プロビジョニング

- 統合ID管理の管理情報の流れ

■ 人事・組織に関するイベントにより統合ID管理システムが管理するアカウントや各種情報の更新を行い、クライアントシステムへ自動反映を行うこと



まとめ：アカウント・IDとは？

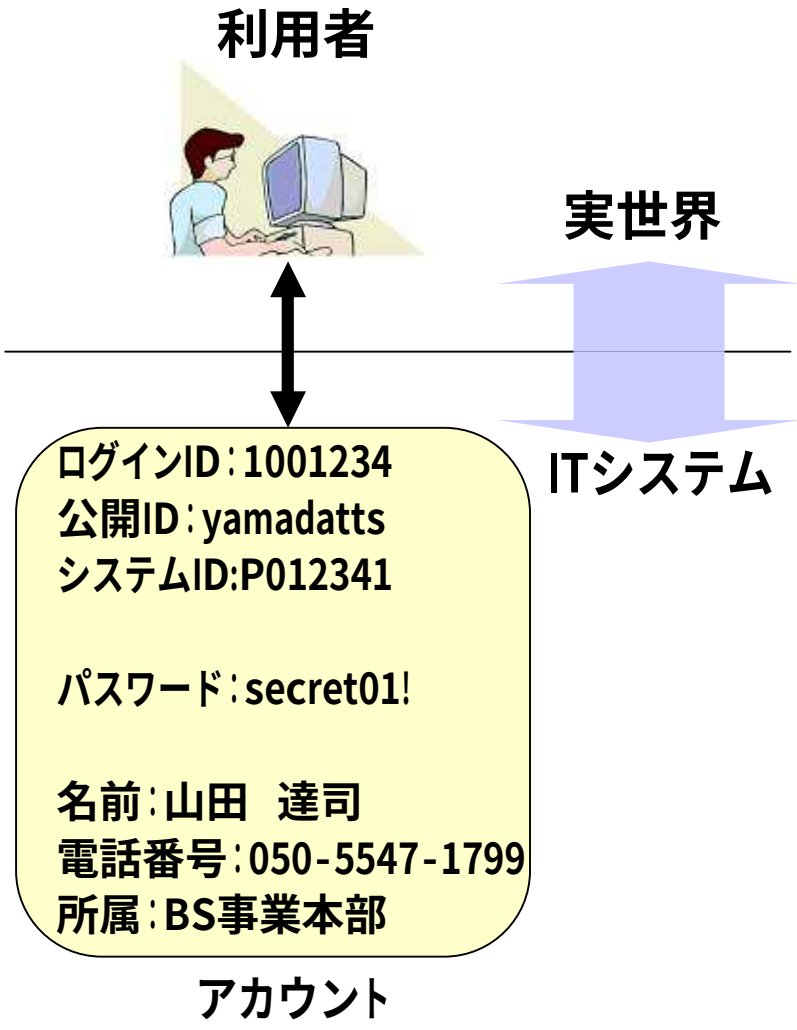
- 利用者：ID統合を行う組織において、正当な理由で社内システムを利用する可能性のある者

- アカウント(Digital Identity)：利用者を電子的に表現したもの。識別子（Identifier)、クレデンシャル（パスワード）、属性情報などを含む。

- ID(Identifier)：　利用者を一意に識別する情報。アカウントのキーとなる情報。用途に応じて複数存在する場合がある

- クレデンシャル：本人確認(認証）に利用される情報。パスワード、ICカード、生体情報などがある。

- 属性情報：利用者に付随して管理される情報
（例：役職、所属、名前、電話番号等）



まとめ：識別/認証/認可

- 識別：Identification

ある利用者が特定の個人であることを伝えること。

- 認証：Authentication

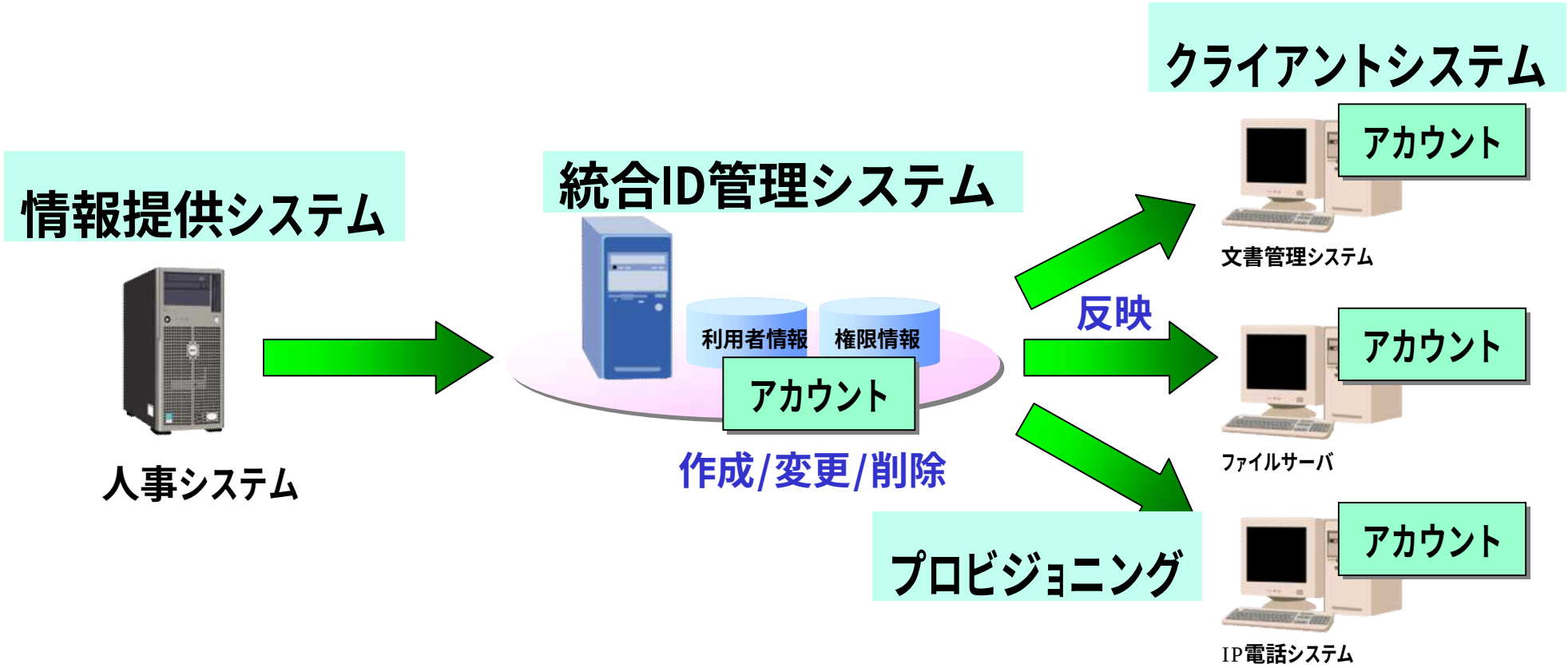
利用者が識別により伝えられた個人であることを確認し、利用者の正当性を証明すること。

- 認可：Authorization

認証された利用者のシステムの利用可否、利用可能な機能、利用可能な情報の範囲等を定めること。

識別(Identification)と認証(Authentication)はあわせて認証と呼ばれることも多い。
認証(Authentication)、認可 (Authorization)に課金 (Accounting)を加えAAAと呼ばれることもある。

まとめ：システムと連携



1. 自己紹介
2. 統合ID管理とは
3. 主要な概念の説明
4. 管理の統合
   - **アカウント管理**
   - 認証
   - 認可
   - 属性情報管理
   - ライフサイクル管理
   - 証跡管理

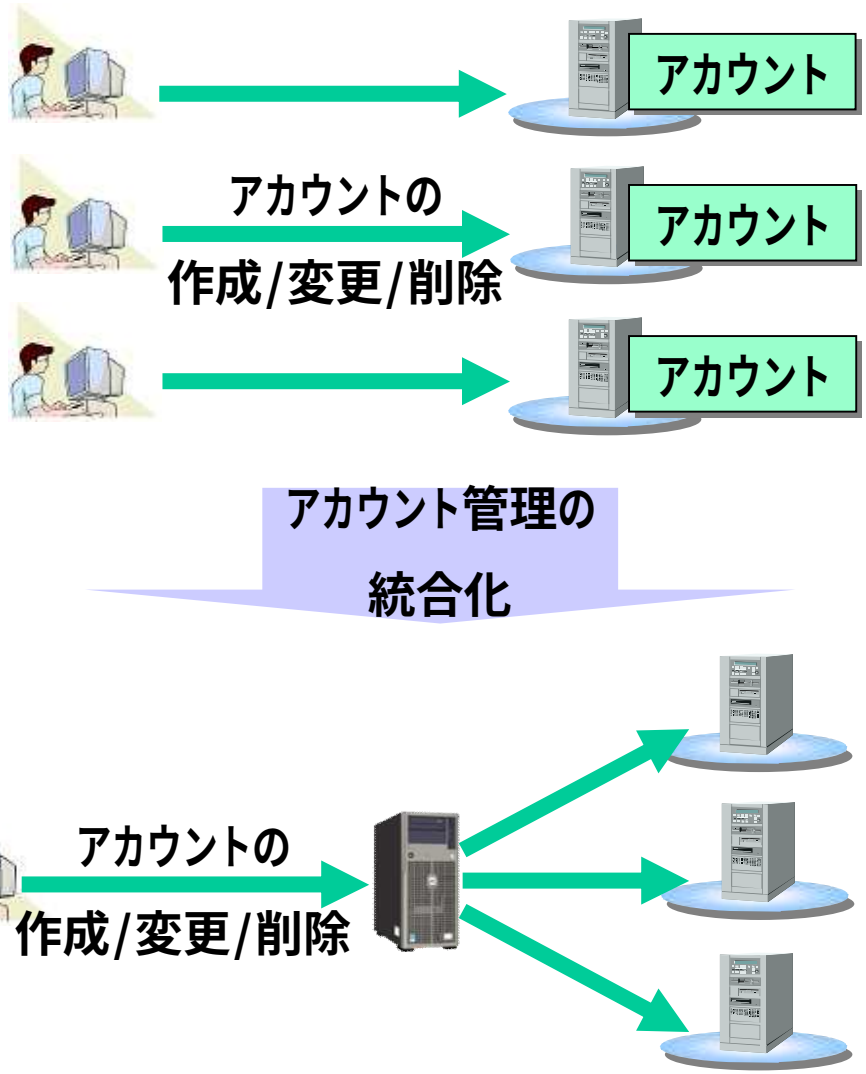
アカウント管理の統合化とは

■アカウント管理とは

システムの利用者の変更に伴い、アカウントの作成、修正、削除等を行うこと。

■アカウント管理の統合化とは

業務システムにおいて個別に行われていたアカウント管理を複数システム間で連動して実施すること。



アカウント管理の統合における課題

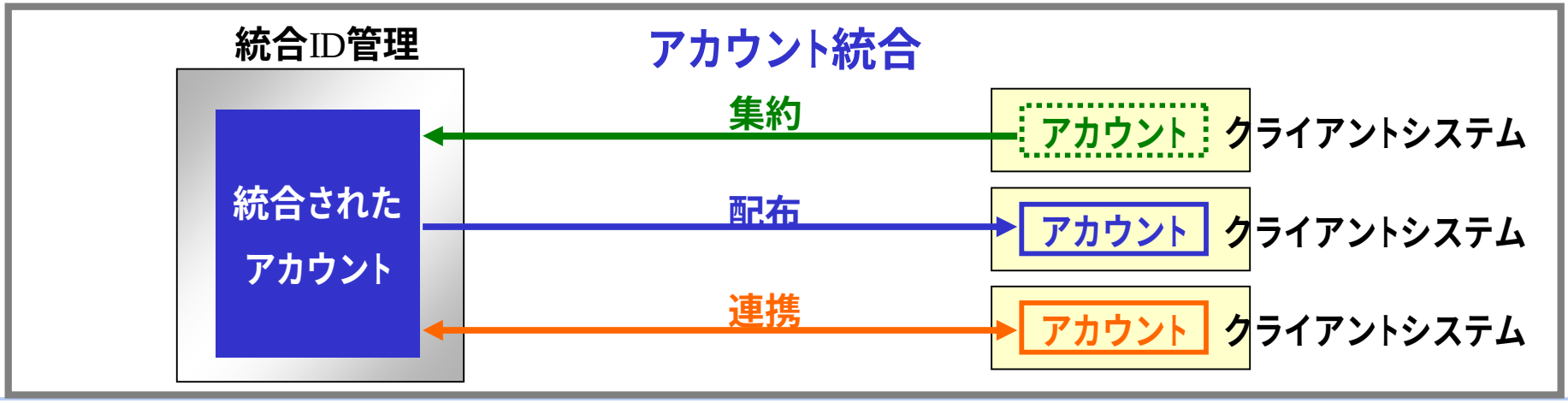
アカウント管理の統合においては、以下の課題を検討し、方針を策定し、システム上に実装する必要がある。

- 統合方式
- ID体系
- 利用者の分類
- 利用者を管理する期間

統合方式 （1／3）

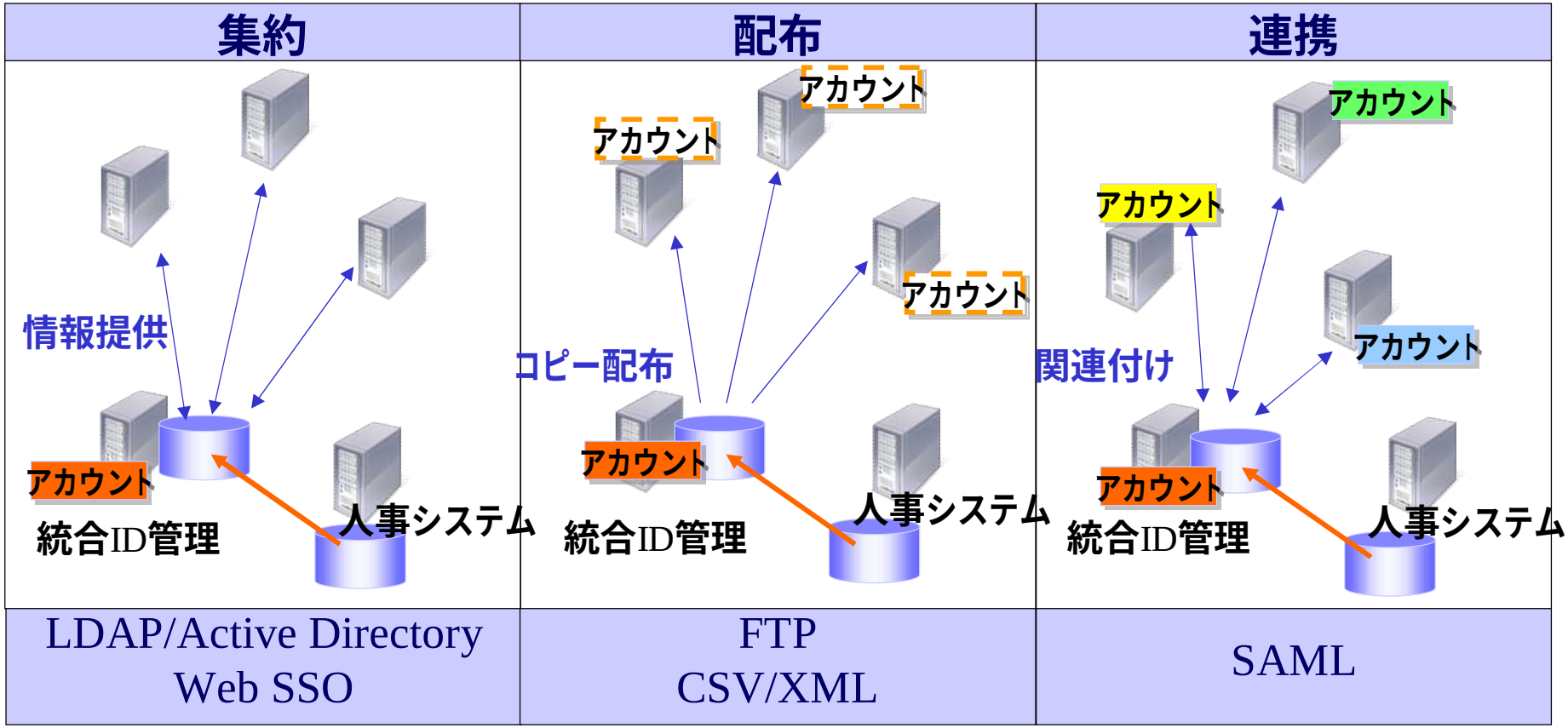
「アカウント管理の統合」には3つの方式がある

- 集約 ・・・ 統合ID管理がアカウントを一元管理し、必要に応じて情報を提供
- 配布 ・・・ 統合ID管理がアカウントを一元管理し、コピーをｸﾗｲｱﾝﾄｼｽﾃﾑに配布
- 連携 ・・・ 統合ID管理とｸﾗｲｱﾝﾄｼｽﾃﾑが異なるアカウントを保持し、相互を関連付ける



統合方式 （2／3）

各システムはその特徴に従い、「集約」、「配布」、「連携」のうち適切な方式によりアカウント統合されている必要がある。



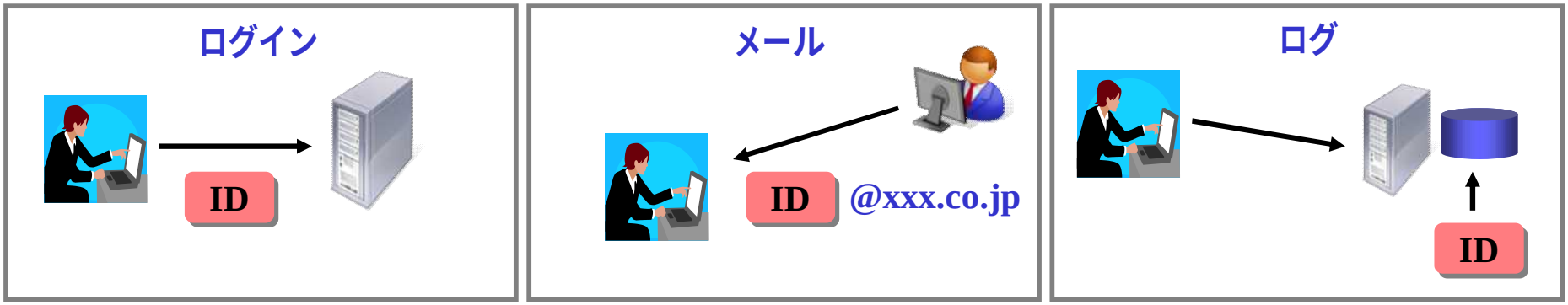
統合方式　（3／3）

統合方式それぞれの特徴は以下の通り。

方式	集約	配布	連携
メリット	情報漏洩リスクが低い 情報の変更が即座にシステムに反映される	技術的な難易度が低く適用可能なシステムが多い。	管理ポリシー、ID体系などが異なるシステム群の統合が可能
デメリット	システムの構造によっては技術的に実現困難。 統合ID管理システムが停止するとシステム全体が停止	システム管理者による利用者情報盗難・悪用のリスクあり。 盗難・悪用時の影響範囲が大きい。	システムごとの管理ポリシーの違いに個別対応が必要。
適した環境	クライアントシステムも含めて再構築する場合など。	連携するクライアントシステムが独自にアカウント管理が必要であるが、カスタマイズが可能な場合。	イントラのシステムとSaaSなど同一ポリシーの適用が困難な場合

ID体系　（1／3）

IDの用途はシステム利用時の認証、利用者による他利用者の識別、システム間での利用者の識別など様々なものがある、異なる用途に対してひとつのIDを用いると、利便性の低下、セキュリティリスクの増大などの問題が懸念される



成りすましを防ぐため、IDは非公開が望ましい

変更することも有効

IDは人に伝えることが目的

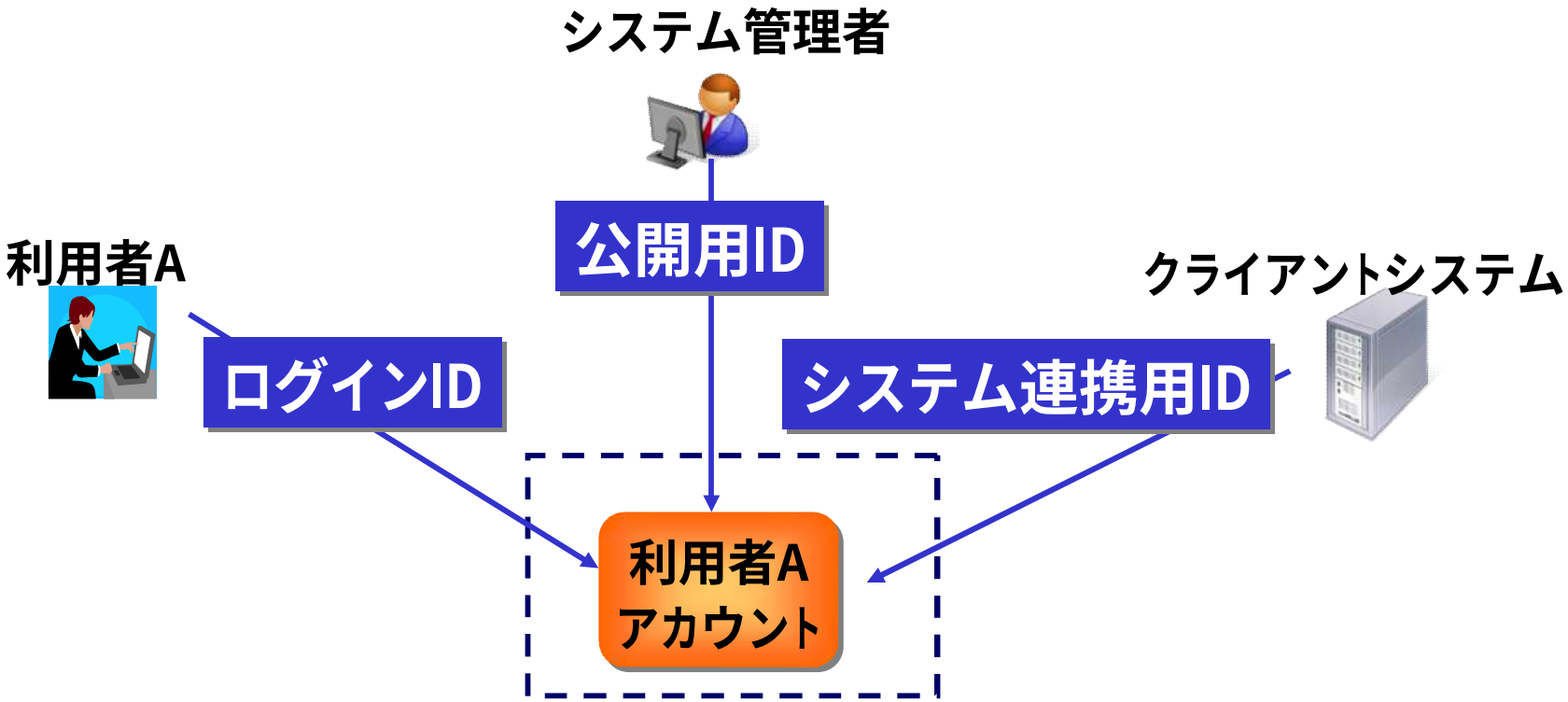
識別が容易な体系が望ましい

システムで利用が容易な固定桁数が望ましい

変更は不可

ID体系　（2／3）

用途に応じて適切な特徴を持つ最小限の種類のIDが各アカウントごとに定義されている必要がある。



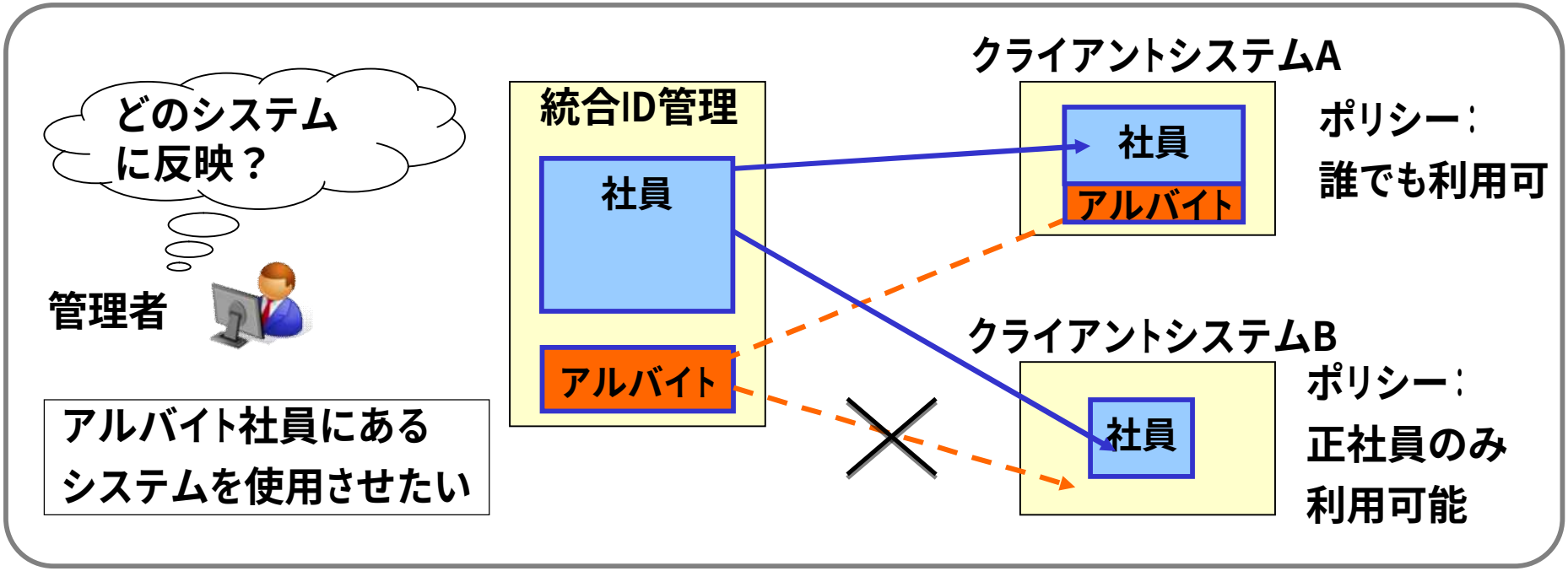
ID体系　（3／3）

アカウント毎に3種類のIDを付与する例

IDの種類	用途	公開可能性	変更可能性	ID体系・例
ログインID	システムへのログイン時にパスワードと組み合わせて利用者を識別・認証する	非公開	可変	それ自身が意味を持たない、あまり長くない半角英数字 「U123456」、 「7654321」など
公開ID	システムの利用者、管理者および外部の人が利用者を一意に特定可能とする（メールアドレス等）	公開	可変	それ自体である程度利用者を特定できる、可変長の半角英数字 「suzuki.taro」、 「tanaka-hanako02」など
システム用ID	連携するシステム間で認証情報、属性情報などを受け渡す際に利用者を識別する（DB上のキー）	公開	不変	固定長で生成した半角英数字など（利用者が識別できる必要はない） 「xU23i041Z」など

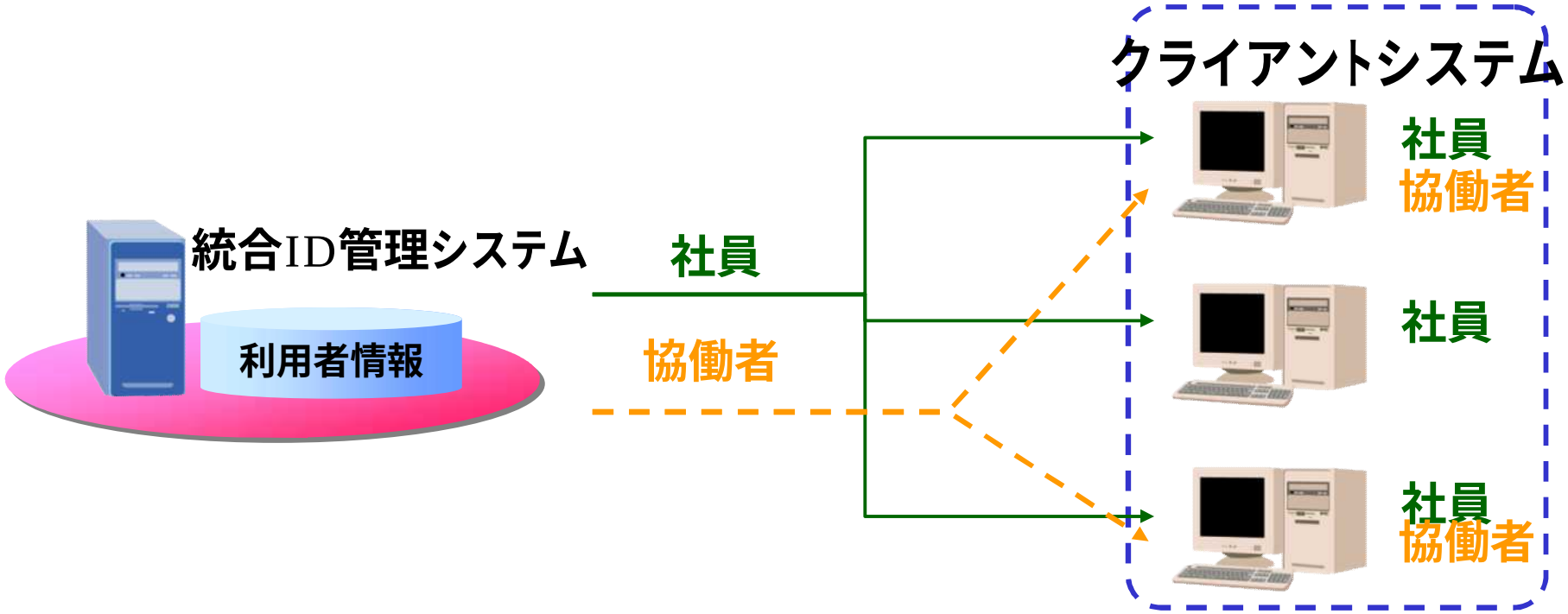
利用者の分類　（1／3）

システムが利用対象となる利用者を明確に決めない場合、新たな種類の利用者を統合ID管理に追加することが難しくなる。



利用者の分類　（2／3）

統合ID管理として、管理対象外とするものも含めて、利用者の範囲・分類を定義し、システムごとの利用ポリシーに従って適切にプロビジョニング（反映）を行うことが必要



利用者の分類　（3／3）

利用対象者の分類例は以下のとおり

利用者の分類	扱い方
社員	基本的には会社と何らか雇用関係にある利用者。「社員」の範囲は企業の規定やポリシーによる。
役員	社員の役職の延長線上として扱う。
協働者	社員とは区別する。協働先の会社や組織との関係を管理する。
退職者	無効な利用者として扱う。再度利用権付与する場合は所定の手続きを必要とする。
その他利用者	例外的に扱う利用者として、取引先営業担当、保険勧誘員、ショールーム来訪者なども対象とすることが考えられる。
システム	クライアントシステムによっては他システムとの連携のためにIDを必要とするケースが考えられる。これらの連携システムを個別に特殊な利用者として扱う。

利用者の管理期間　（1／2）

統合ID管理として、利用者を管理する期間を定めないと、セキュリティリスク、運用負荷の増大を招く恐れがある。

■ 退職、契約終了などで利用者不在となった場合は即座にアカウントを削除する

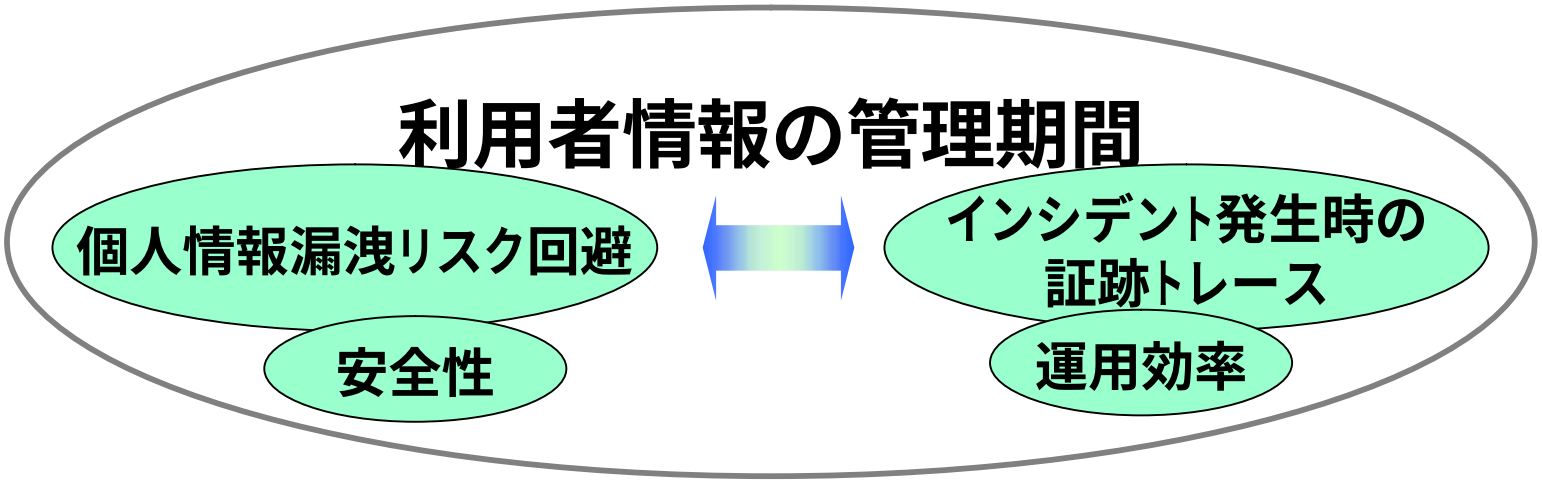
○	個人情報漏洩のリスクを軽減
×	利用者不在となってから発覚するセキュリティインシデントへの対応が困難

■ 退職、契約終了などで利用者不在となった後もアカウント管理を継続する

○	利用者不在となってから発覚するセキュリティインシデントの証跡トレースに有効
×	不在となった利用者の個人情報を保持することで情報漏洩のリスク

利用者の管理期間　（2／2）

利用者アカウントを管理する期間は関連法規と企業のセキュリティポリシーに従い適切に設定されており、期間中は安全に管理され、満了時は全システムの該当アカウントが確実に削除されることが必要

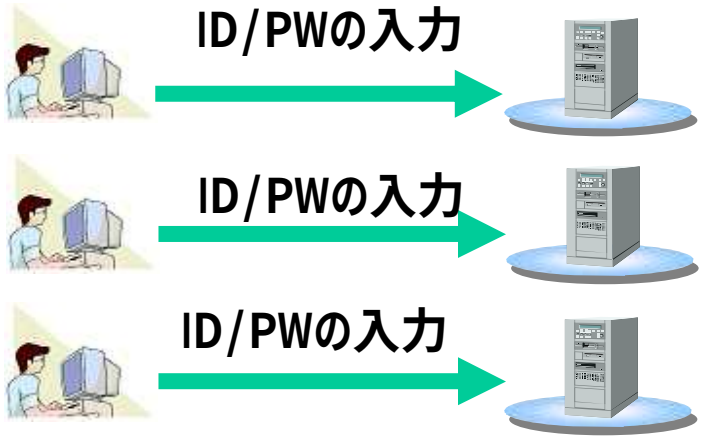


1. 自己紹介
2. 統合ID管理とは
3. 主要な概念の説明
4. 管理の統合
   - アカウント管理
   - **認証**
   - 認可
   - 属性情報管理
   - ライフサイクル管理
   - 証跡管理

認証の統合化とは

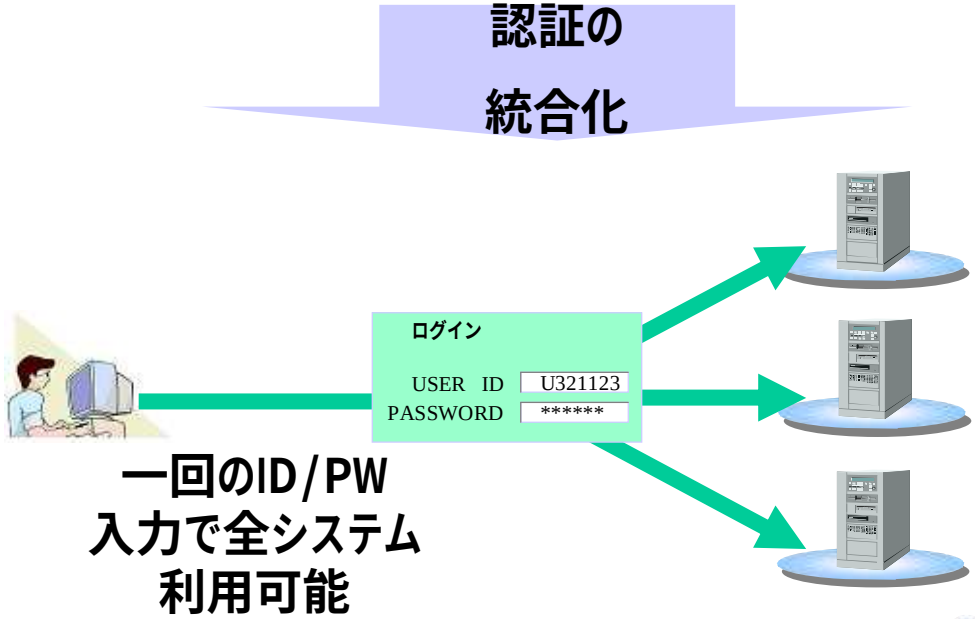
■認証とは

利用者がシステムを利用する際に、
利用者が誰か、本人であるかどうか
を確認すること(識別+認証)



■認証の統合化とは

業務システムにおいて個別に行われ
ていた認証を同一の情報、機能、
ユーザインタフェースなどにより実現
すること



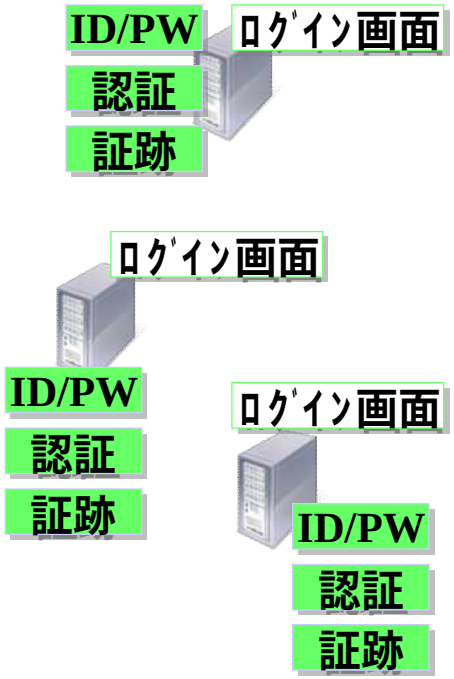
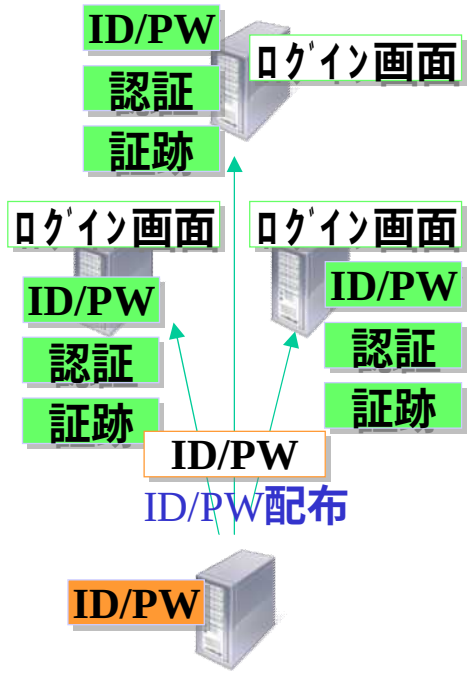
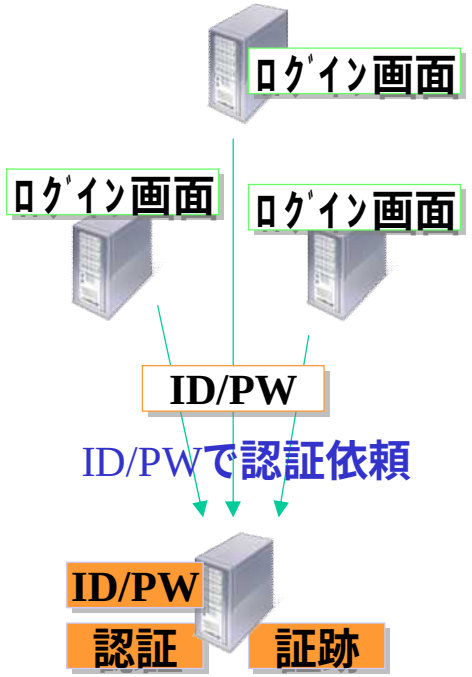
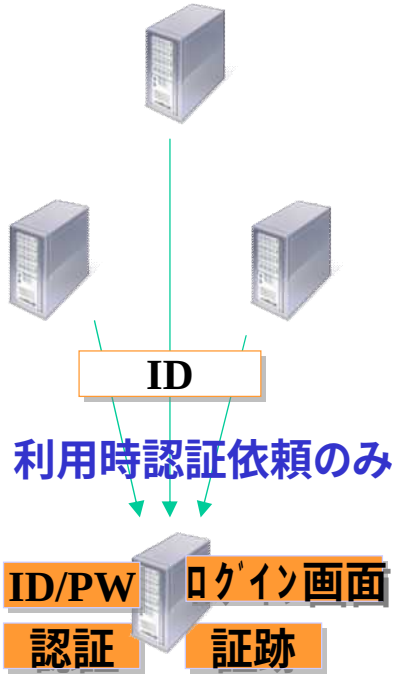
認証統合の課題

認証の統合においては、以下の課題を検討し、方針を策定し、システム上に実装する必要がある。

- 認証統合パターン
- シングルサインオン
- 認証方式

認証統合パターン （1／2）

システムの運用形態やセキュリティポリシーに基づき、最適な方式で認証を統合することが必要である。認証を統合するおもな方式は以下の通り。

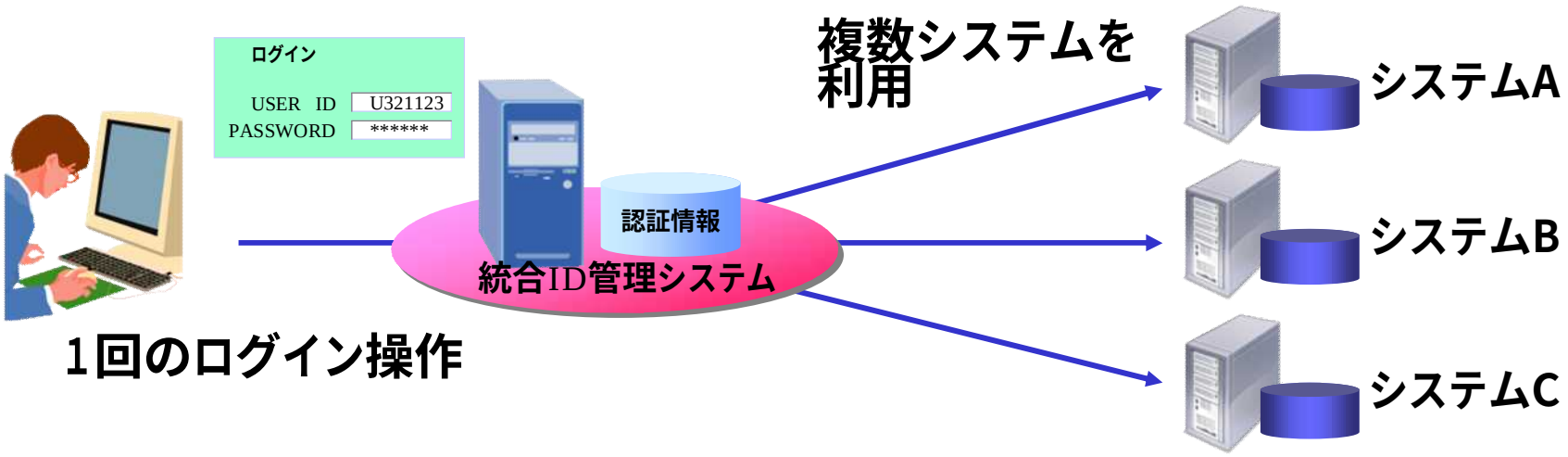
未統合	ID/PW配布	認証サービス	シングルサインオン
			
適用される技術			
-	FTP	LDAP/Active Directory	Web SSO

認証統合パターン　(2／2)

観点	未統合	ID/PW配布	認証サービス	ｼﾝｸﾞﾙｻｲﾝｵﾝ
利便性	C	B	B	A
	システム毎個別のID/PW	統合されたID/PW。システム毎のログイン	同左	1回のログインのみ
安全性	B	C	B+	A
	なりすまし、漏洩などのリスクが大きいが、影響はシステムにとどまる	業務システム管理者による盗難のリスクがある ID/PW盗難時の被害範囲が大きい	各業務システム間でID/PWが流れ、各システムがその蓄積が可能	ID/PWは1箇所でのみ管理、システム間も流れない。認証方式の変更･追加にも柔軟に対応
内部統制	C	B	A	A
	利用者の証跡管理が各システムに分散され、IDもばらばらで問題発生時の調査･分析が困難	問題発生時の利用者の特定はしやすくなるが、認証ログが分散管理される分、調査･分析の効率はよくない	利用者の認証に関する証跡も一元管理され、問題発生時の対応も効率的に行うことができる	同左

シングルサインオン

一回のログイン操作だけで、認証を必要とする複数のシステムを利用できることをシングルサインオンと呼ぶ。主なメリットは「ユーザの利便性向上」「ID/PWの集中管理、証跡の集中取得によるセキュリティ向上」など。



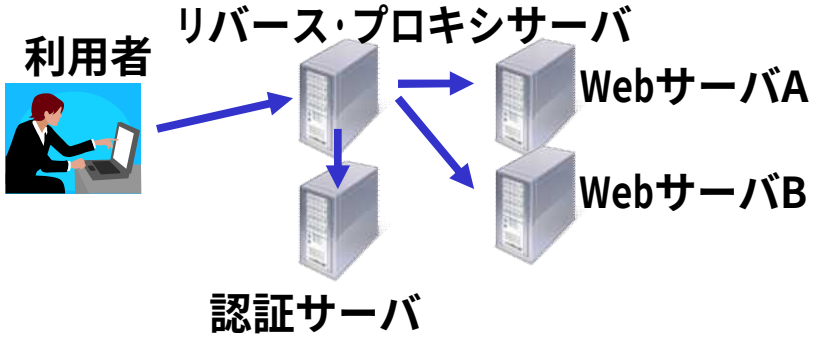
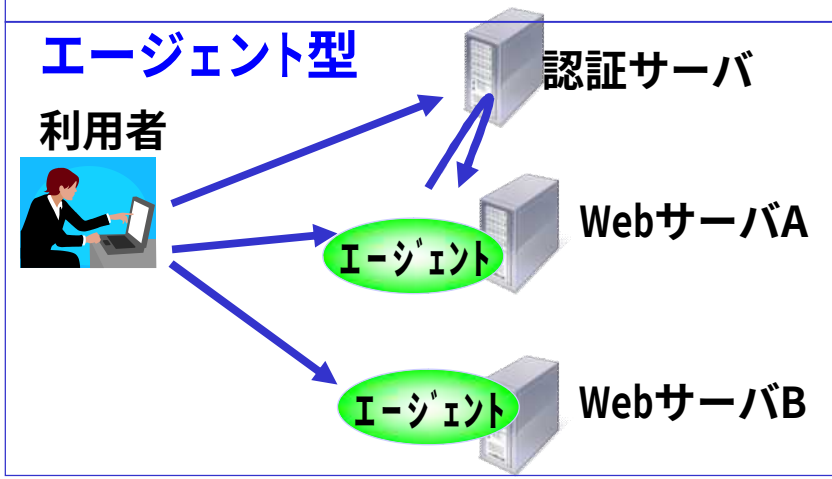
シングルサインオンの実現方式

対象となるシステムの種類により、シングルサインオンの実現方式は大きく3種類に分けられる。

方式名	方式の概要	特徴
WebSSO	プロキシー、フィルターなどにより、Webサーバ全体に認証をかける方式。	認証と同時にACLに基づく認可を制御可能。 静的なコンテンツのアクセス制御が可能
ライブラリ型SSO	アプリケーションにライブラリの形式でSSO機能を付加する方式	アプリケーション単位でのSSOが可能 認証機能を持つAPのみSSO化可能。 静的コンテンツは制御付加
EnterprisseSSO	利用者のPCにｲﾝｽﾄｰﾙしたﾓｼﾞｭｰﾙがｱﾌﾟﾘｹｰｼｮﾝが表示するログイン画面を監視し、ID、パスワードを自動的に入力する方式	既存ｱﾌﾟﾘｹｰｼｮﾝの改造が不要 認証機能を持つAPのみSSO化可能 PCへのﾓｼﾞｭｰﾙｲﾝｽﾄｰﾙが必須

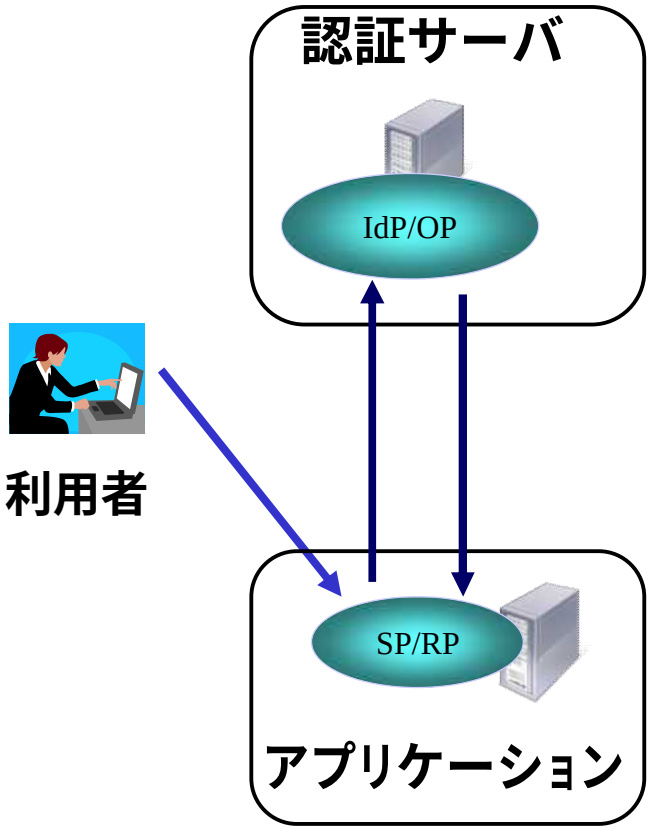
シングルサインオン - Web SSO

Web SSOの主な2方式は以下のとおり

タイプ	説明	メリット	デメリット
リバース・プロキシ型 	利用者のリクエストリバースプロキシサーバが受信し、認証及びアクセス制御を実行	バックエンドにある各サーバに直接アクセスできないため安全性が高い Webサーバの制限がない	リバースプロキシーサーバがパフォーマンスのボトルネックになる可能性がある。
エージェント型 	Webサーバにインストールされたエージェントが Cookieに格納されたログイン状態、属性等によりアクセス制御を実行	ボトルネックになる箇所が少ないためパフォーマンスに優れる	各サーバにエージェント（プラグイン）が必要

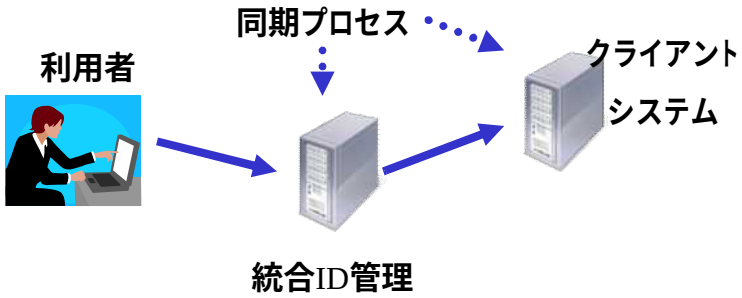
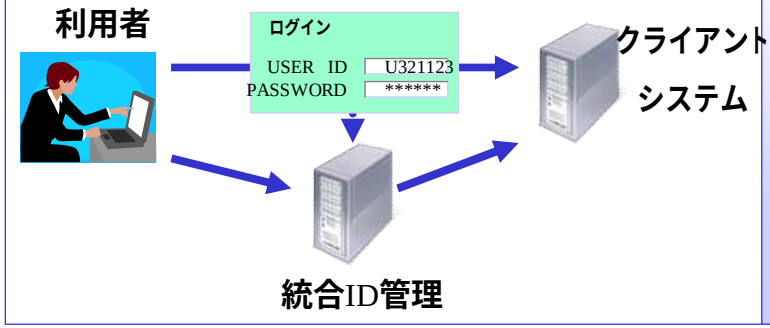
シングルサインオン - ライブラリ型

ライブラリ型SSOの主な2方式は以下のとおり

	方式	説明	特徴
	SAML2.0	OASISが規定。 Trusted Circleと呼ばれる関係付けられた認証サーバ（IdP：Identity Provider)、アプリケーション（SP:Service Provider)間でのSSOが可能	認証情報と通信手段が独立している。 仮名により、異なるID体系のサービス間のSSOが可能 セキュリティの高さからSaaSなどでの実績多
	OpenID	OpenID Foundationにより規定 認証サーバ(OP:OpenID Provider)、アプリケーション（RP:Relaying Party)ともに自由な利用が可能。	実装がシンプルであり、オープンなモジュールが多数存在 インターネット上には多くのOP(Yahoo!、mixi、google等）が存在

シングルサインオン - EnterpriseSSO

Enterprise SSOではｸﾗｲｱﾝﾄｼｽﾃﾑ用ID/PWの管理方法に大きく2種類が存在する

方式	説明	特徴
ID/PW同期型 	パスワード同期プロセスが対象システムのパスワードを自動生成し、ｸﾗｲｱﾝﾄｼｽﾃﾑと統合ID管理の両者に登録する	ｸﾗｲｱﾝﾄｼｽﾃﾑには同期ﾌﾟﾛｾｽが生成するパスワードを設定する仕組みが必要 パスワード更新の頻度を上げることでセキュリティ向上が可能
ID/PW読み取り型 	利用者がクライアントシステムに登録したパスワードを統合ID管理が読み取って記憶する	クライアントシステムに一切の改造、機能追加が不要 ｸﾗｲｱﾝﾄｼｽﾃﾑが表示するすべてのﾛｸﾞｲﾝ画面、パスワード変更画面を登録する必要あり

シングルサインオン

SSOを実現する方式はそれぞれ特徴があり、適切なものの選択が必要

	方式	適した環境	対象システム方式	業務システムへの要件
Web SSO	リバースプロキシ型	インターネット 企業内	Web	APサーバが集約されていること 業務システムのログイン機能が改造可能であること
	エージェント型	企業内	Web	エージェントモジュールのインストールが可能であること 業務システムのログイン機能が改造可能であること
ライブラリ型	ID連携	インターネット SaaS/クラウド	Web	ライブラリの組み込みが可能であること
Enterprise SSO	ID/PW同期型	企業内	Web、C/S	外部からID/PW書き換え可能なインタフェースを持っていること
	ID/PW読み取り型	企業内	Web、C/S	ログイン画面、パスワード変更画面が特定可能なこと。Java/Flash不可などの制限あり

認証方式

認証(本人確認) には精度、利便性などで異なる様々な方式が用いられる。最も広く用いられているのはパスワードである。複数の方式を組み合わせることで、より確実な認証を行うことを二因子認証、二要素認証、多要素認証と呼ぶ。

種類	説明	主な認証方式
知識	本人しか知り得ない情報・知識の確認	パスワード、PIN 質問
身体的特徴	本人のみが持つ身体的特徴の確認 (バイオメトリクス認証)	指紋、虹彩 声紋、網膜
所有	本人のみが所有するものの確認	ICカード、USBトークン 認証カード、OTPトークン 携帯固有ID

認証方式ーその他

その他の認証方式の例

方式	説明	特徴
リスクベース認証	初回認証時にPC、ブラウザ、OS等の環境を記憶。次回以降それらの環境が変更された場合、再度より強固な（第二、第三パスワード、証明書等）認証を実施	アタックを検出することは可能だが、アタックが疑われる際の本人確認の手段を別途用意する必要がある。
イメージマトリクス認証	画面上に毎回ことなるイメージ、数字列を表示。ユーザごとに決められたルールに基づき、その中から情報を読み取る方式	物品、ファイルなどの配布は不要。セキュリティ強度はほどほど
USBメモリー認証	USBメモリー（USBトークンではない）のIDを利用して認証	USBメモリーは汎用品の利用が可能 クライアントへのソフトのインストールが必要
発番号認証	Webでのログインと並行してユーザに電話をかけさせ、サーバ側で発番号にて確認。	ユーザが手持ちの電話、携帯電話を利用できるため、デバイスの配布などが不要。クライアントにソフトの追加も不要

1. 自己紹介
2. 統合ID管理とは
3. 主要な概念の説明
4. 管理の統合
   - アカウント管理
   - 認証
   - **認可**
   - 属性情報管理
   - ライフサイクル管理
   - 証跡管理

認可の統合化とは

■認可とは

利用者がシステムを利用可能か、どの範囲を利用可能かを判断すること。

■認可の統合化とは

業務システムにおいて個別に行われていた認可を、統合管理された情報及び統合ID管理機能上に用意されたメカニズムに基づき、実現すること

認可統合の検討課題

認可の統合においては、以下の課題を検討し、方針を策定し、システム上に実装する必要がある。

- 認可モデル
- 認可の分担

認可モデル

認可を実現する代表的なメカニズムは以下のとおり。

- アクセス制御マトリクス
- ACL (Access Control List)
- RBAC (Role Based Access Control)

認可モデル-アクセス制御マトリックス

利用者に対してリソースごとの利用権と利用レベルを割り当てるメカニズム。

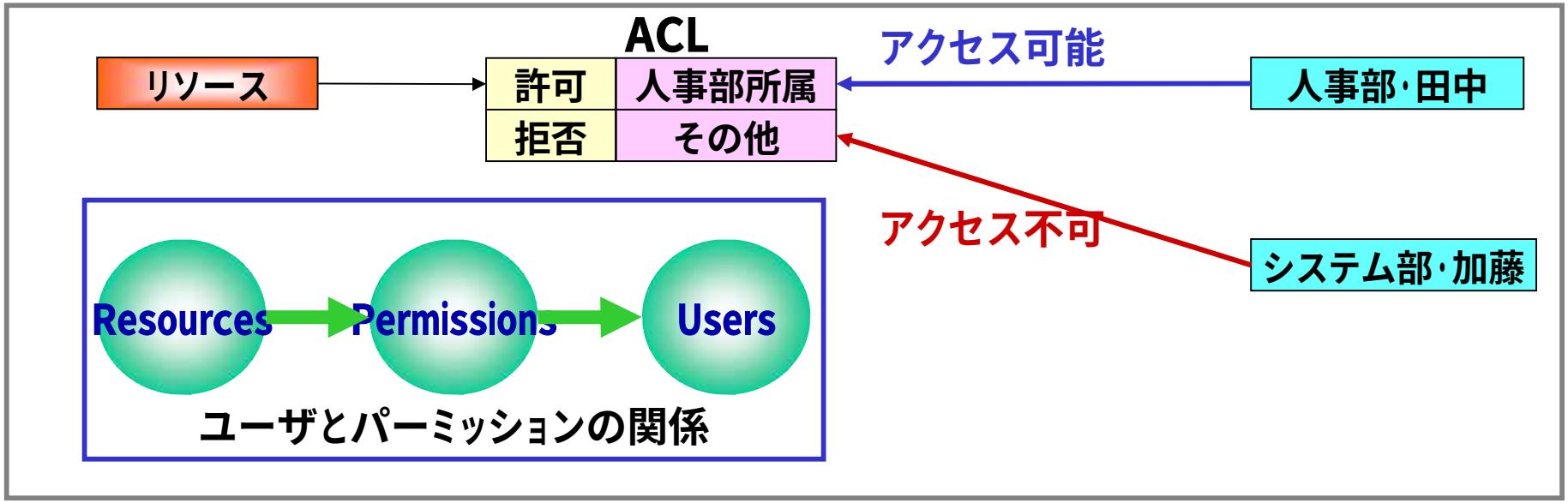
利用権付与の状況が把握しやすく、利用者数やリソース数が少ない環境ではメンテナンスも容易で適しているが、利用者数、リソース数の多い環境では管理負担が増大する。

リソース / 利用者	電子メール	文書管理システム	人事システム	会計システム
ユーザA	○	Admin	×	×
ユーザB	○	一般	登録・参照	×
ユーザC	○	一般	参照	○

認可モデル- ACL（Access Control List）

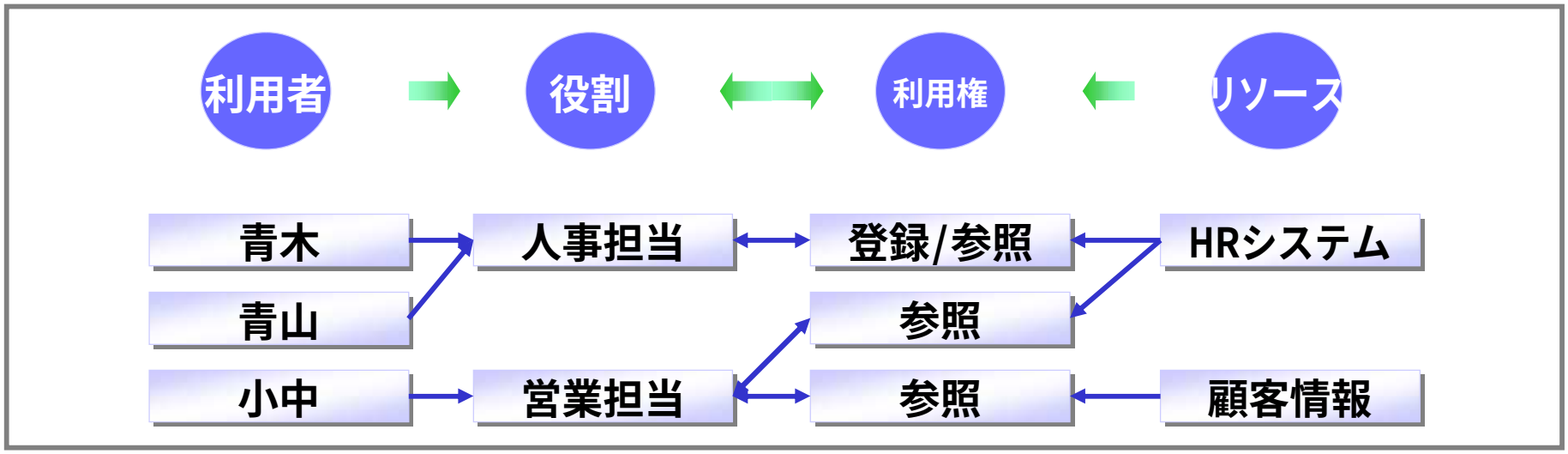
リソースに対して「誰に」「どのような操作を許可／拒否」という属性を定義して認可を行うメカニズム。

複数リソースに対してきめ細やかな利用権設定ができるため、リソース中心に記述した方が効率の良いWebサーバ、ファイルサーバ、文書管理システムなどに適しているが、複雑なルールを記述するとメンテナンス負担が大きくなる恐れあり



認可モデル-RBAC（Role Based Access Control）

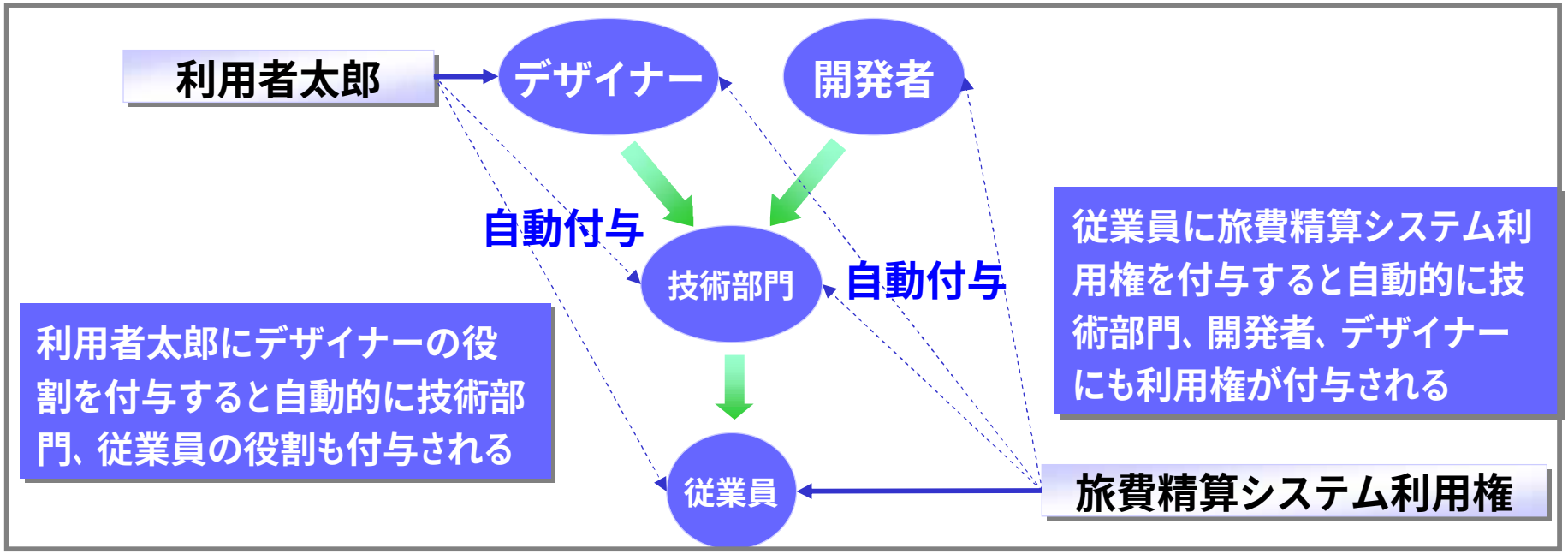
特定の「役割」に対してリソースの利用権を割り当てることで認可を行うメカニズム。役割により多くの利用者を集約して管理可能で、利用者の変化にも柔軟に対応できるため大規模な組織でも効率的に利用権の管理が可能。また、リソースに対して登録や参照といった操作そのものに対する認可が可能であるため、ACLよりも厳密に認可ルールを設定可能



認可モデル-RBAC（Role Based Access Control）

RBACにおける役割は階層構造をとることが可能（階層的RBAC）

上位の役割に割り当てられたユーザは自動的に下位の役割も付与され、下位の役割に割り当てられた権限が自動的に上位の役割にも割り当てられるといった半順序関係を許可することが可能。



認可モデル-主要モデルの比較

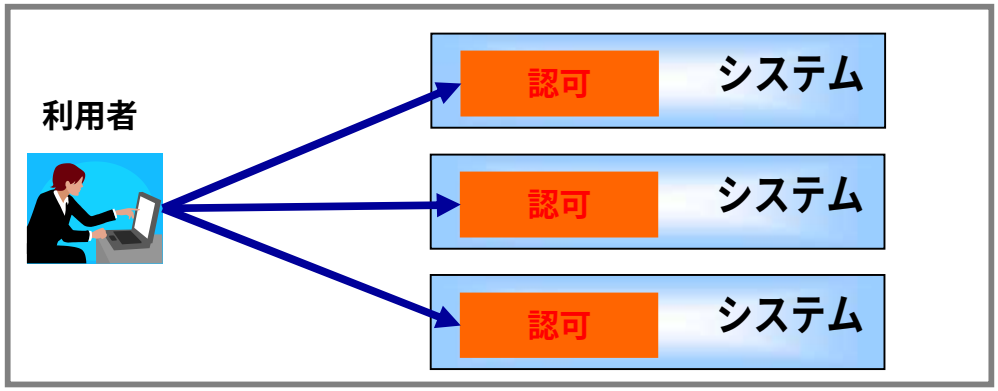
厳密なポリシーの適用、効率的な管理、拡張性などの観点から最適な方式で認可モデルが選択され、利用する必要がある。

モデル	メリット	デメリット	適した用途
アクセス制御マトリクス	利用者ごとの権限が明確で理解しやすい。実装が容易	利用者、リソースの増加ごとに個別に利用権を決定する必要がある	小規模な企業例外の管理
ACL	リソースに対するアクセス権設定を行えば良いので大規模な組織でも効率よくルール設定が可能	情報の増加に伴い、ACLのメンテナンスが困難に 効率的にACLをメンテナンスするには、情報のグループ化、RBACとの組み合わせなどが必要	対象リソースが多い
RBAC	融通が利き、きめ細かな認可ルール設定が可能 人・組織や認可ルールの変更に柔軟に対応できる	組織が複雑になると理解が困難となり、管理負担が大きい 開発コストも大きくなる	対象利用者が多い、組織体系が複雑

認可の分担　（1／2）

認可はｸﾗｲｱﾝﾄｼｽﾃﾑと統合ID管理で分担の境界を適切に設定する必要がある

■ 認可は統合しない

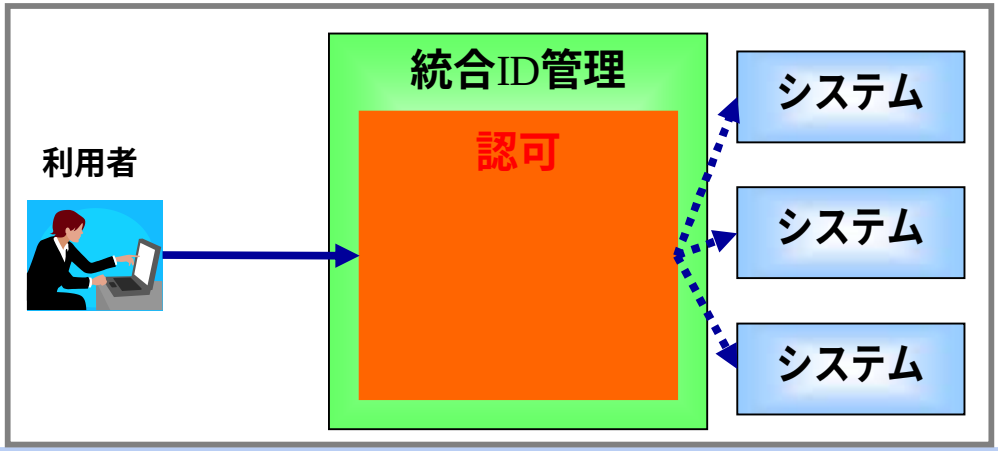


■ 企業として一貫性のない認可

■ 利用者や組織に関する情報変更が反映しきれない

■ 認可情報管理が分散し、信頼性を確保できない

■ 統合ID管理において全ての認可を行う

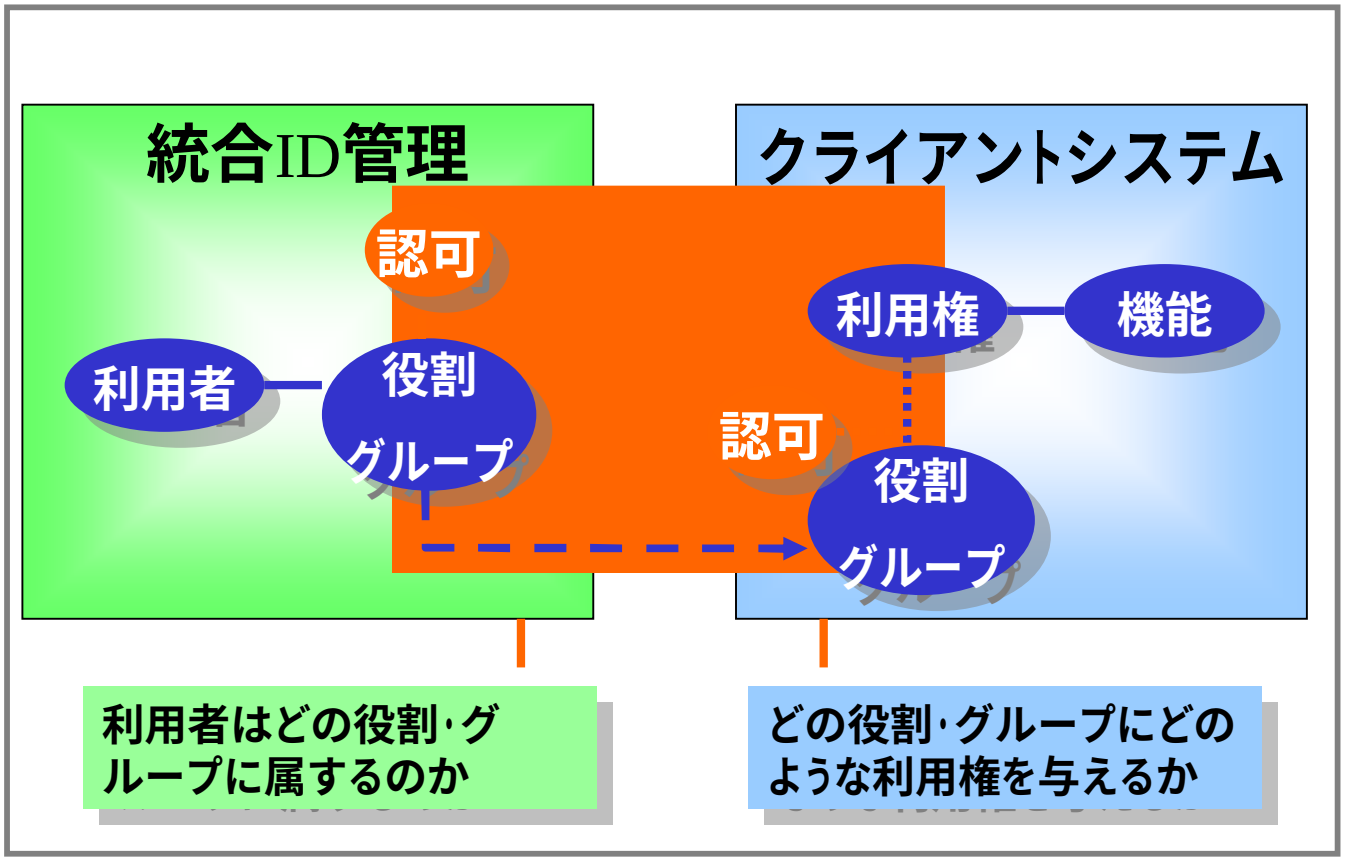


■ システム固有の認可ポリシーの変更が困難

■ システム固有の運用パターンの適用が困難/時間がかかる

認可の分担　（2／2）

分担の一例として、利用者と役割、グループの紐月を統合ID管理側で実施し、役割グループと機能、リソースの紐付けをｸﾗｲｱﾝﾄｼｽﾃﾑで行うモデルがある。



以下の観点で分担を考慮

- 管理情報のメンテナンス
- システム固有のポリシー対応

1. 自己紹介
2. 統合ID管理とは
3. 主要な概念の説明
4. 管理の統合
   - アカウント管理
   - 認証
   - 認可
   - **属性情報**
   - ライフサイクル
   - 証跡管理

属性情報の統合化とは

■属性情報管理の統合化とは

アカウントとひもづけて管理する属性情報(名前、所属、メールアドレス、顔写真) を定義し、様々な情報提供システムから取得し、統合ID管理システム内で管理し、クライアントシステムへ提供すること。

属性情報管理の統合の検討課題

属性情報管理の統合においては、以下の課題を検討し、方針を策定し、システム上に実装する必要がある。

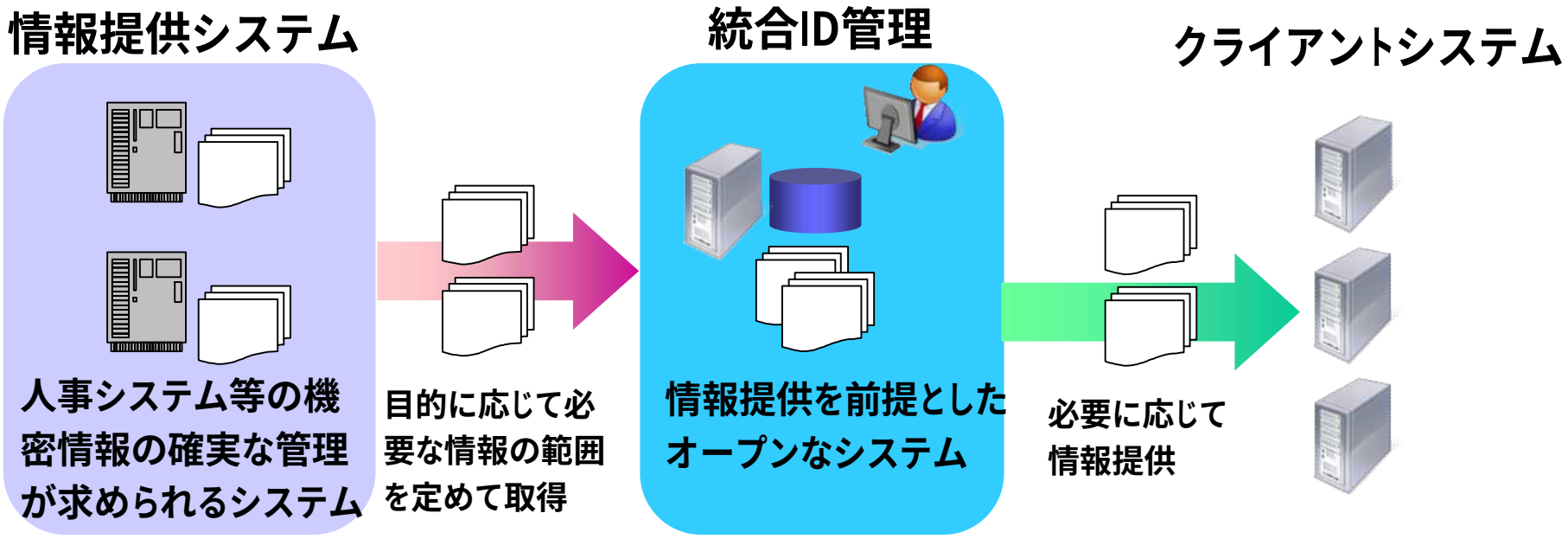
■属性情報の範囲

■属性情報の形式

属性情報の範囲

システムの構築、運用コストを低減するため、統合ID管理にて管理すべき属性情報の管理は以下の観点から決定する必要がある。

- 情報の機敏度、セキュリティレベル
- 情報の活用度合い



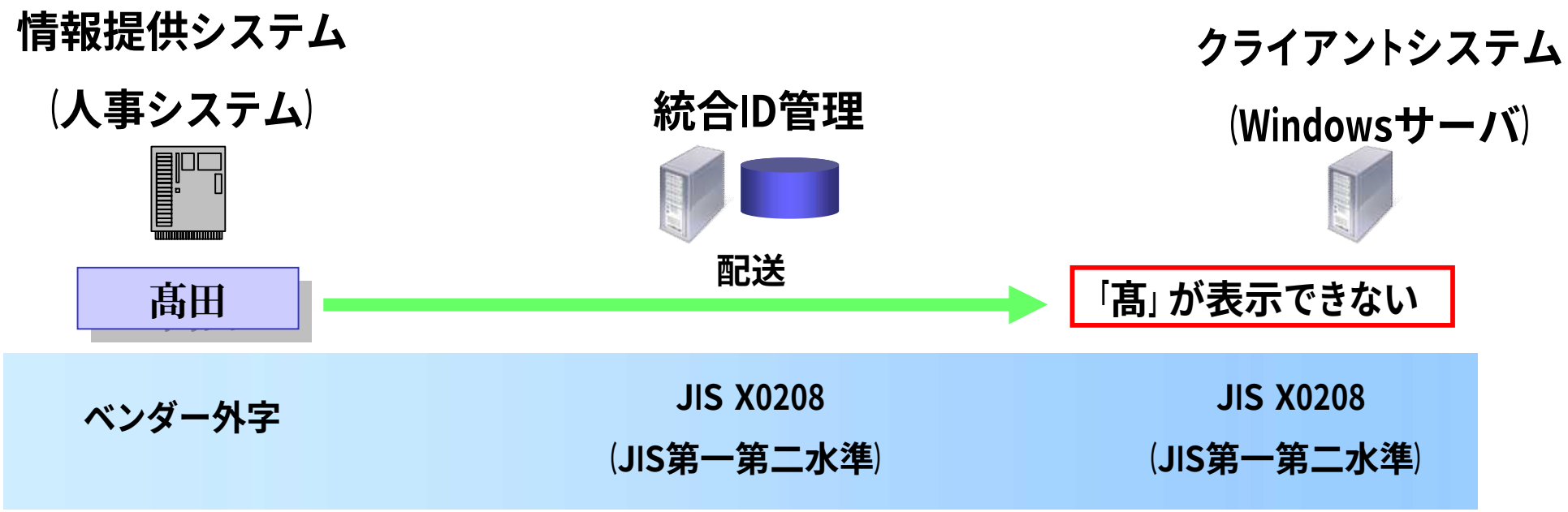
属性情報の範囲

管理対象とする属性情報として、「認可情報」、「コミュニケーション用情報」、「表示用情報」の3種類を対象するという例

管理対象	種類	説明	例
○	認可情報	各システムのアクセス制御において必要となる情報	■ 所属組織 ■ 所属プロジェクト ■ 役職
○	コミュニケーション用情報	利用者同士、システムとのコミュニケーションにおいて必要となる人や資源の識別情報として使用する情報	■ メールアドレス ■ 電話番号
○	表示用情報	連携するクライアントシステム上でおもに利用者に関する表示のために必要となる情報	■ 氏名 ■ 役職名 ■ 所属部署名
×	人事考課情報 給与支給情報	機密性が高く、かつ、クライアントシステムが必要とする可能性が少ないため、管理対象とすべきではない情報	■ 振り込み口座 ■ 保有資格 ■ 保有スキル

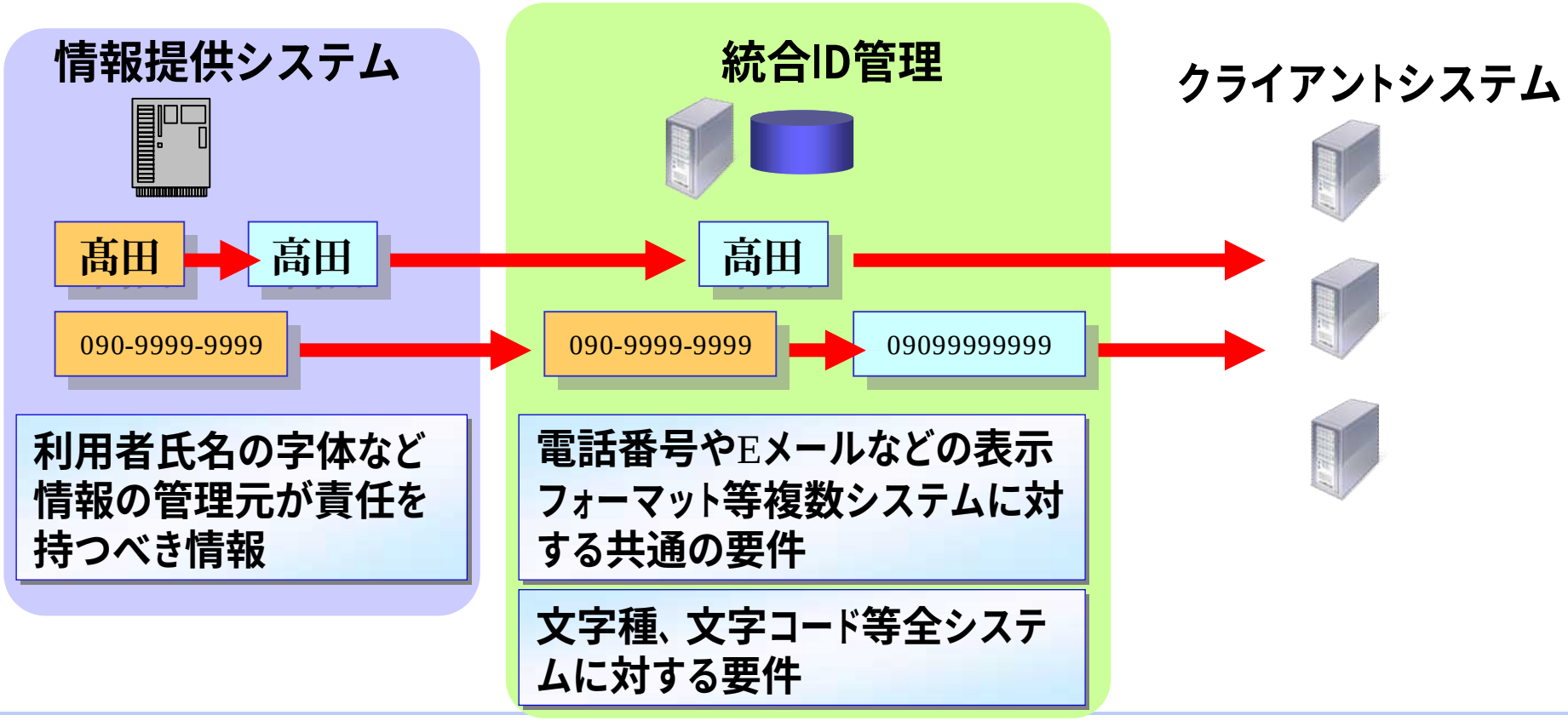
属性情報の形式　（1／2）

情報提供システムから取得した情報をそのままクライアントシステムに提供すると、文字種、字体、フォーマットなどの違いによる不具合・トラブルが発生する可能性がある



属性情報の形式　（2／2）

統合ID管理における共通情報の管理形式が明確化されており、システムの要求する形式に従って適切な場所で変換され、配送される必要がある。特に外字については開発コスト、クライアントシステムでの使い勝手の点から管理すべきではない



1. 自己紹介
2. 統合ID管理とは
3. 主要な概念の説明
4. 管理の統合
   - アカウント管理
   - 認証
   - 認可
   - 属性情報管理
   - **ライフサイクル管理**
   - 証跡管理

ライフサイクル管理の統合化とは

■ライフサイクル管理とは

利用者の状態の変化（入社、異動、退職等）に合わせてアカウントの状態を定義し、状態、および状態の変化に合わせて様々な処理、アクセス制御をおこなうこと。

■ライフサイクル管理の統合化とは

統合ID管理システムにおいてアカウントの状態を定義、管理し、クライアントシステムへ提供する。統合ID管理システム内においてもアカウントの状態の変化に伴い自動的に処理を行うこともある。（権限の付与・はく奪、通知他）

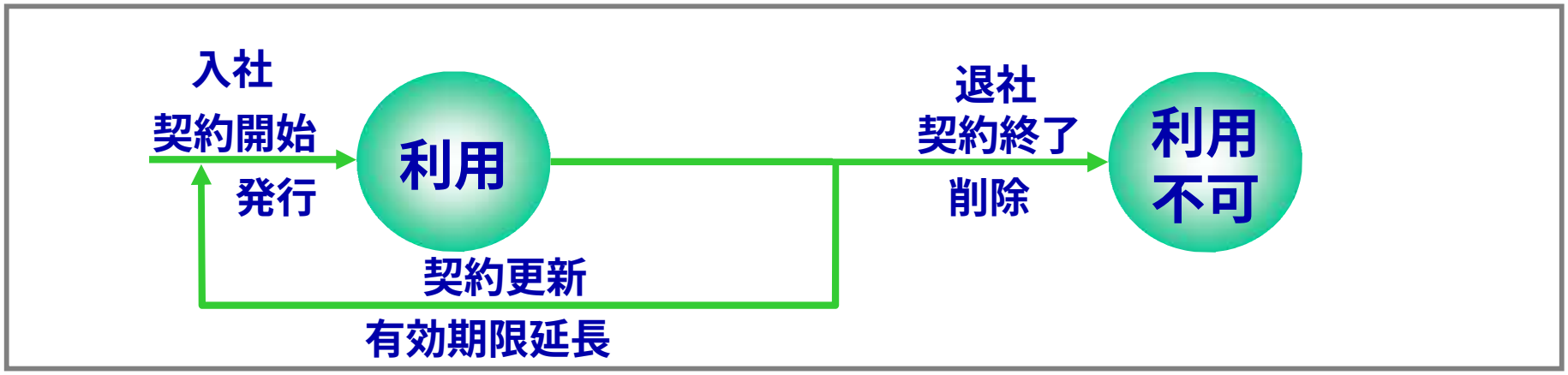
ライフサイクル管理の検討課題

ライフサイクル管理の統合化を行う上では以下の課題を検討する必要がある

- ライフサイクルモデル
- ライフサイクルの同期

シンプルなライフサイクルモデル

最もシンプルなライフサイクルモデルを以下に示す

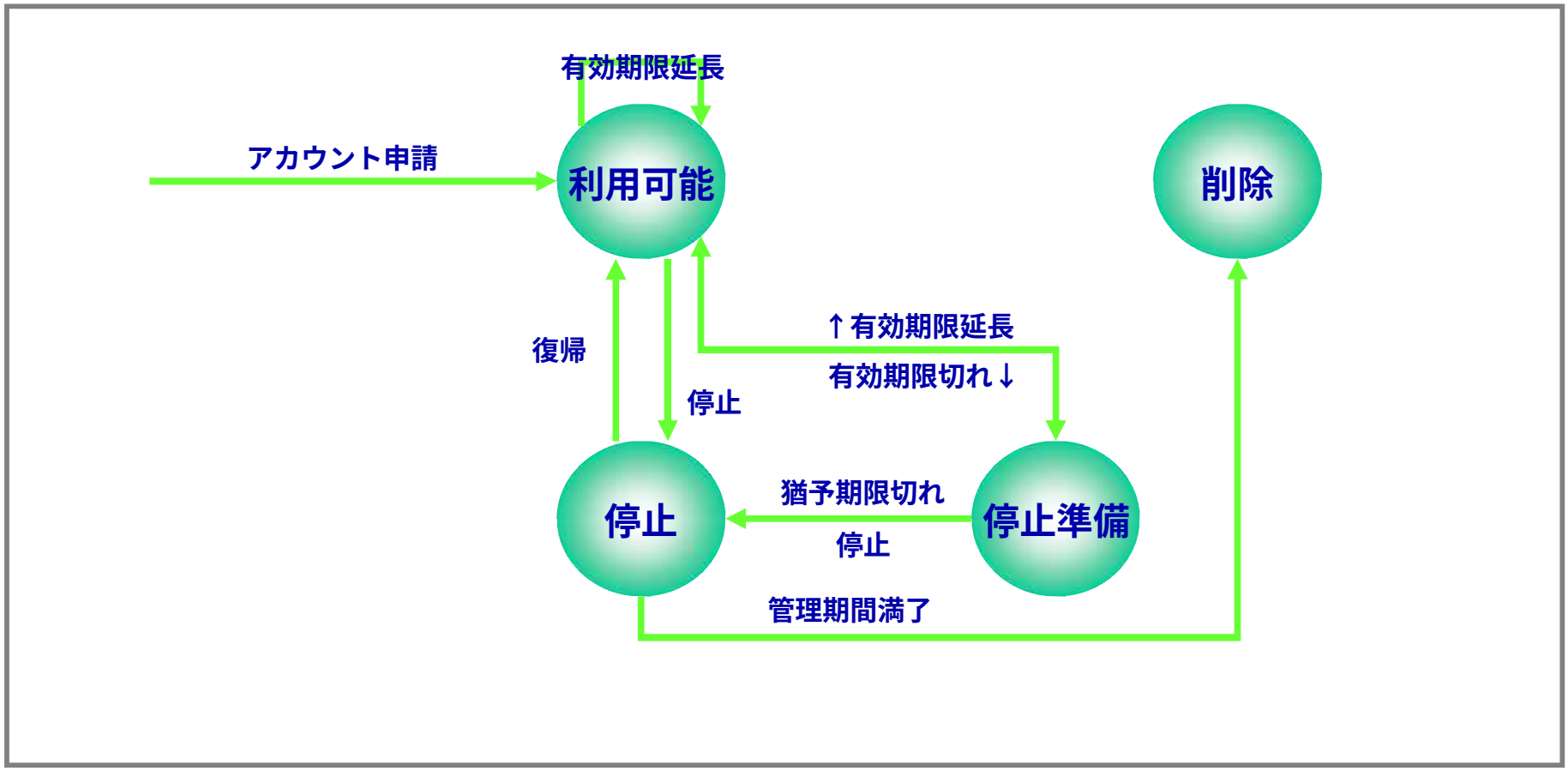


利点
- 不要となったアカウントは迅速に削除し、個人情報を廃棄する（情報漏洩防止）
- ライフサイクル管理がシンプル（管理負担減少、開発コスト低減）

欠点
- 期限延長申請忘れでもアカウントが削除され、発行手続きからやり直し
- 利用者不在となってから発覚するインシデントの証跡トレースが困難
- インシデントが疑われる際の一時的なアカウント停止が困難

ライフサイクルモデル-詳細なモデル

以下はセキュリティの改善、利便性の向上などを実現するライフサイクルモデルの例



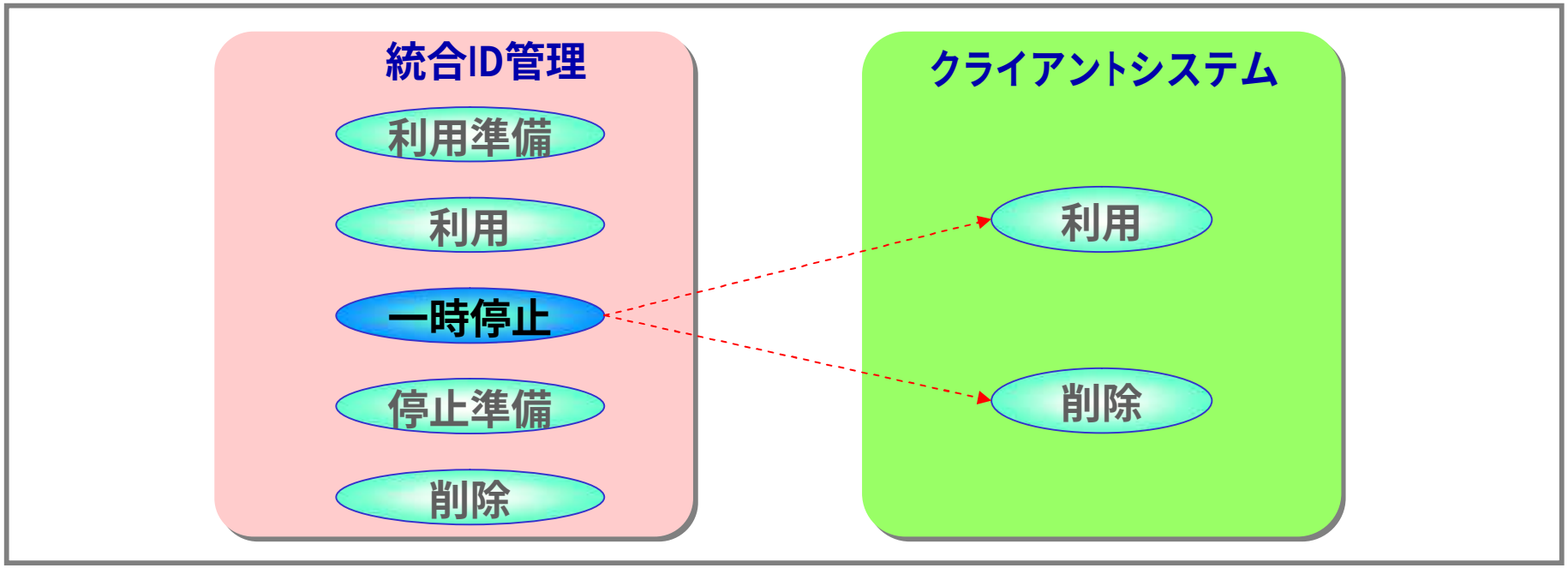
ライフサイクルモデル-詳細なモデル

前頁のライフサイクルモデルにおける各ステータスの意味と状態の例

ステータス	説明	認証可否	アカウント
利用可能	正式なアカウントが発行された状態。アカウントの信頼性によるシステム利用制限はなし。（承認済）	可	有効
停止準備	一時的に当該アカウントの認証を行わない状態。（手動設定、PW入力誤りによるロックなど）	否	有効
停止	アカウントが無効となった状態。（手動停止、再申請への猶予期限切れなど）	否	無効
削除	物理的にアカウントが削除された状態。（期間内に正式なアカウント申請がなかった場合、規定の管理期間が終了した場合など）	ー	ー

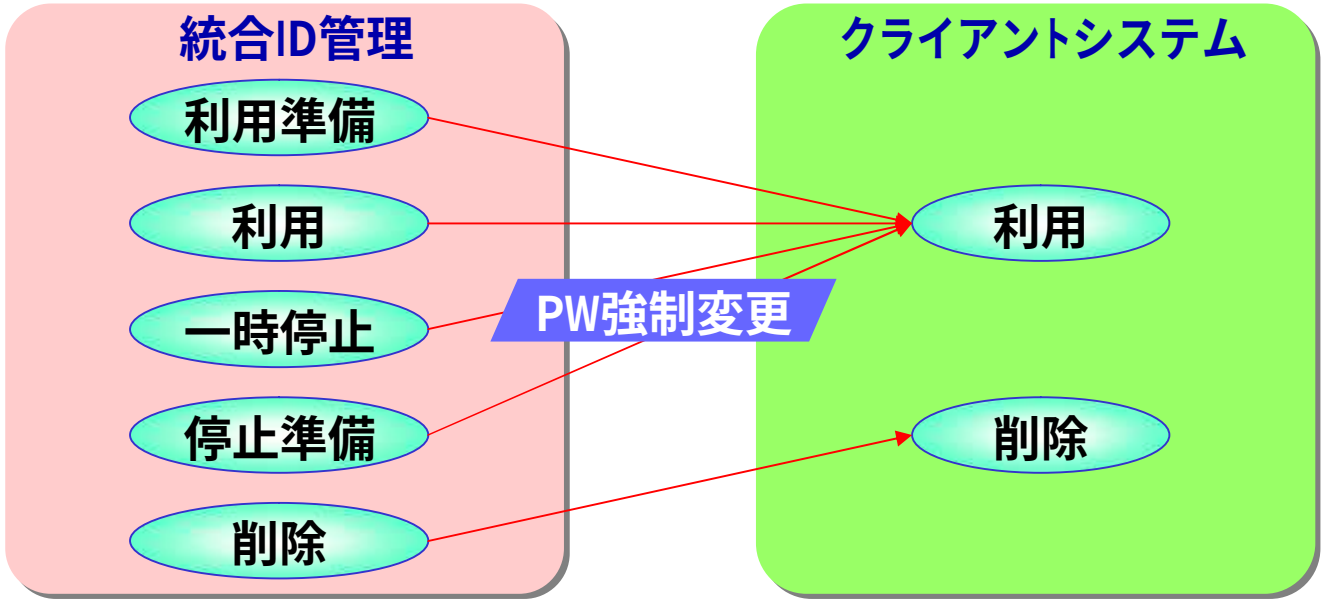
ライフサイクルの同期

統合ID管理で定義したライフサイクルモデルは必ずしもクライアントシステムにおいて実現可能ではない。統合ID管理でのアカウント状態をシステムへどう反映するかはクライアントシステム/レポジトリごとに検討する必要がある。



ライフサイクルの同期

統合ID管理と各システムのライフサイクルの違いは状態の意味に従って適切にマッピングする必要がある。以下の例では一時停止、停止準備などアカウント削除には至らないが利用を停止させる必要がある場合はパスワードをランダムに変更することで同様の状況を用意している。



1. 自己紹介
2. 統合ID管理とは
3. 主要な概念の説明
4. 管理の統合
   - アカウント管理
   - 認証
   - 認可
   - 共通情報
   - ライフサイクル
   - **証跡管理**

証跡管理の統合化とは

■証跡管理とは

様々な目的（業務の正当性証明、システムの正常動作の確認、システムの異常動作時の原因究明等）のため、アカウント管理、認証、認可等統合ID管理にかかわる様々な作業、処理における実施内容、実施者を記録し、統計的な処理を行い、必要な組織に報告すること。

■証跡管理の統合化とは

従来システム個別に実施されていた証跡管理をシステム全体で実施すること

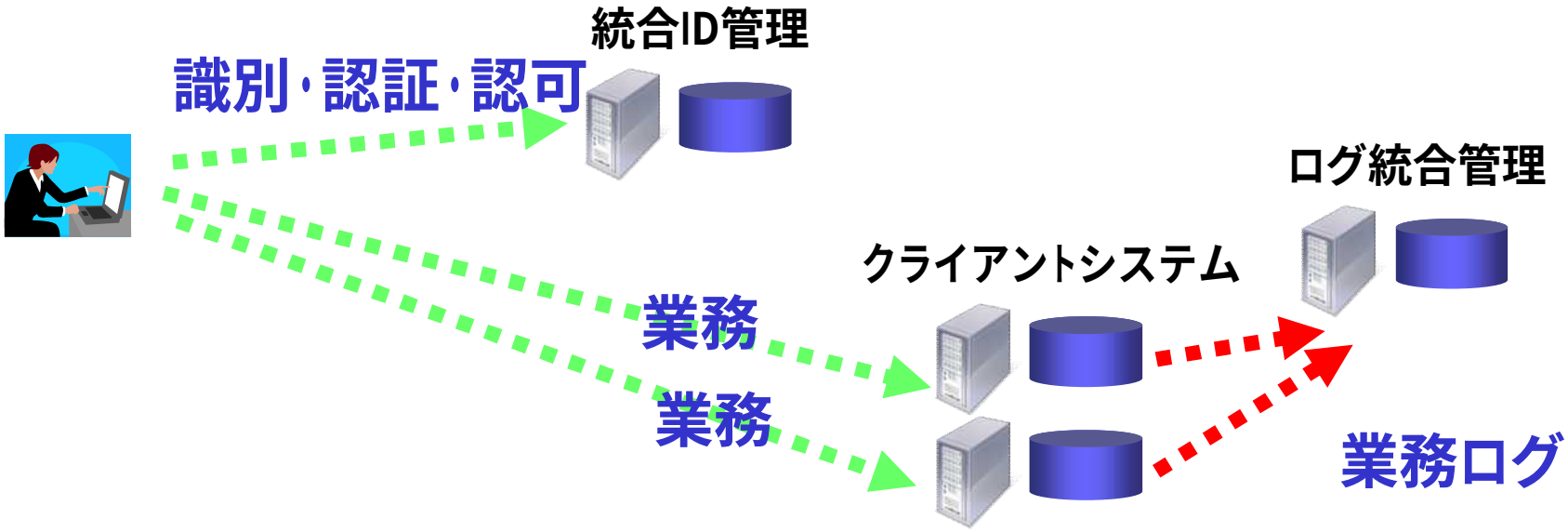
証跡管理の検討課題

証跡管理の統合化を行う上では以下の課題を検討する必要がある

- 証跡管理の分担（業務）
- 証跡管理の分担（ID管理）
- 統合ID管理で取得する情報

証跡管理の分担 (業務)

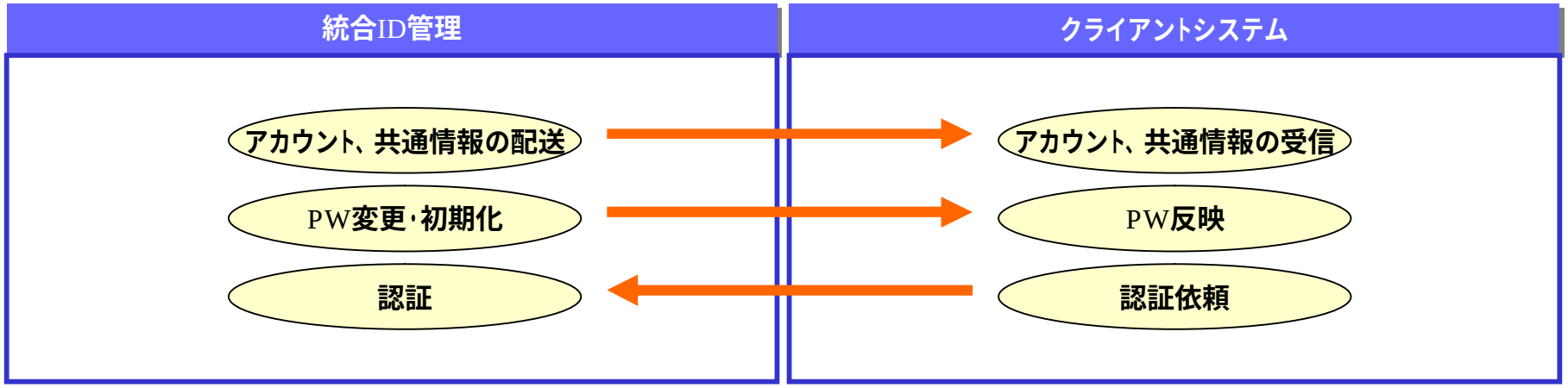
統合ID管理では利用者の識別、認証、認可を行うがクライアントシステムのファイル操作や業務アプリケーションの利用などには関与しないため、統合ID管理とは別に各システムの業務ログを統合管理する仕組みがある



証跡管理の分担（ID管理）

必要な証跡は統合ID管理のみで取得できるとは限らない。ID管理に関する監査証跡は統合ID管理と各システムで役割に基づいた適切な分担で効率的に記録・保管されている必要がある。

■ ID管理の証跡管理分担例



取得するログ

取得するログには監査証跡等必要な情報が漏れなく含まれている必要がある。

以下のような内容について、「いつ」「誰が」「何に対して」「何をした」が確実に記録されることが必要です。

カテゴリ	内容
アカウント管理	プロビジョニング
	アカウント申請、承認
認証	認証操作
	パスワード同期履歴
認可	権限付与
	認可ルール設定
	システムへのアクセス
共通情報管理	情報収集
	情報提供
	メンテナンス
ライフサイクル管理	アカウント生成･状態変化･削除