

NIIオープンフォーラム2016 IDaaSの概要と ご利用いただくための取り組み(苦労話)

2016年5月27日

エクスジェン・ネットワークス(株)
代表取締役 江川淳一

1. Identityの捉え方(eic2016より)
 2. クラウドの普及とフェデレーション
 3. IDaaS概要
 4. Extic(Exgen Trusted Identity Center)
 5. IDaaSをご利用いただくために
(参考)
- エンタープライズ市場におけるステルスIDaaS戦略

1. Identityの捉え方(eic2016より)

THE MOMENTS AHEAD FOR IDENTITY



Ian Glazer

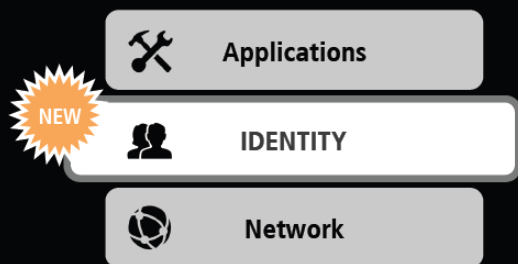
Senior Director, Identity
Salesforce

Ian Glazer is the Senior Director for Identity, at Salesforce. His responsibilities include product strategy and identity standards work. Prior to that, he was a research vice president and agenda manager on the Identity and Privacy Strategies team at Gartner where he oversaw the entire...

1. Identityの捉え方(eic2016より)

THE MOMENTS AHEAD FOR IDENTITY

- ①Identity業界は今、「TCP/IP Moment」を迎えている
~ネットワーク業界でTCP/IPそのものに代金を支払わなくなった瞬間



Identity must be embedded
(e.g. TCP/IP)

CIS2013で、Andre Durandのキーノートでの発表

1. Identityの捉え方(eic2016より)

THE MOMENTS AHEAD FOR IDENTITY

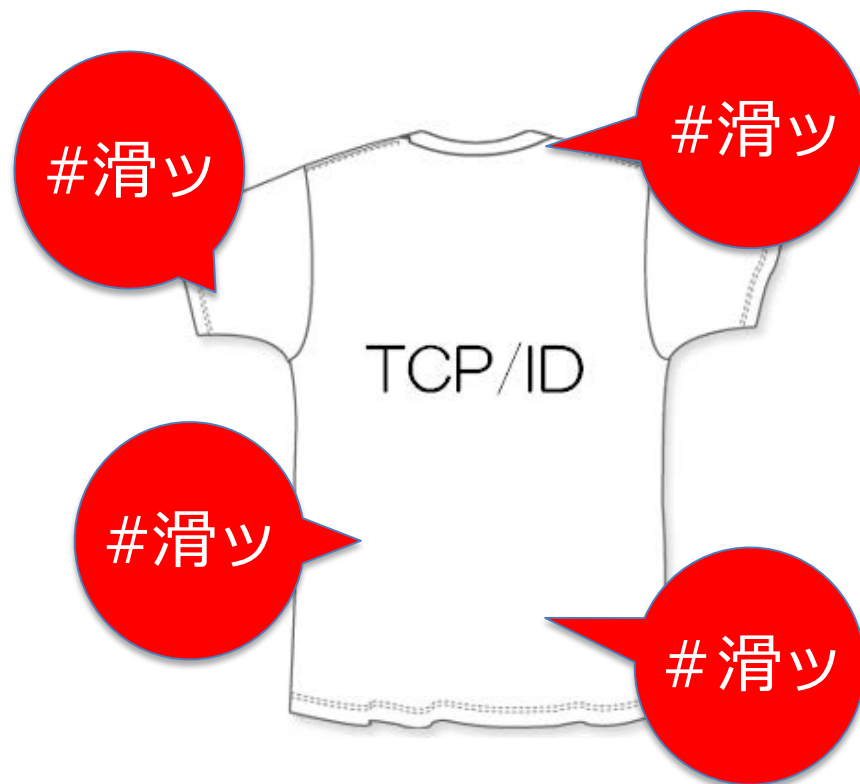
- ①Identity業界は今、「TCP/IP Moment」を迎えている
~ネットワーク業界でTCP/IPそのものに代金を支払わなくなった瞬間

[OpenID TechNight Vol.10] CIS2013報告 参考資料

2013.9.4

egawa

第7層: アプリケーション層 アプリケーション間でのデータのやり取りを担当	
第6層: プレゼンテーション層 データ変換 (ASCII・EBCDIC などの相互変換) と圧縮を規定する	第4層: アプリケーション 例: HTTP・FTP・DNS
第5層: セッション層 ログイン・ログアウトなどのセッションの手順を規定する	
第4層: トランスポート層 再送・輻輳処理・ピア間の信頼性のあるエンドツーエンドの通信を担当。	第3層: トランスポート 例: TCP・UDP
第3層: ネットワーク層 ネットワークの経路選択・中継作業を担当。	第2層: インターネット 例: IP・ICMP・ARP・RARP
第2層: データリンク層 1つのネットワークに接続された複数のコンピュータ間でのデータを伝送を担当。	第1層: ネットワークインタフェース 例: Ethernet・PPP
第1層: 物理層 回線の上でデータ送受信を担当。回線に送信する電気的な変換やピンの形状・ケーブル特性などを規定。	第0層: ハードウェア 例: UTP ケーブル・RC-232C



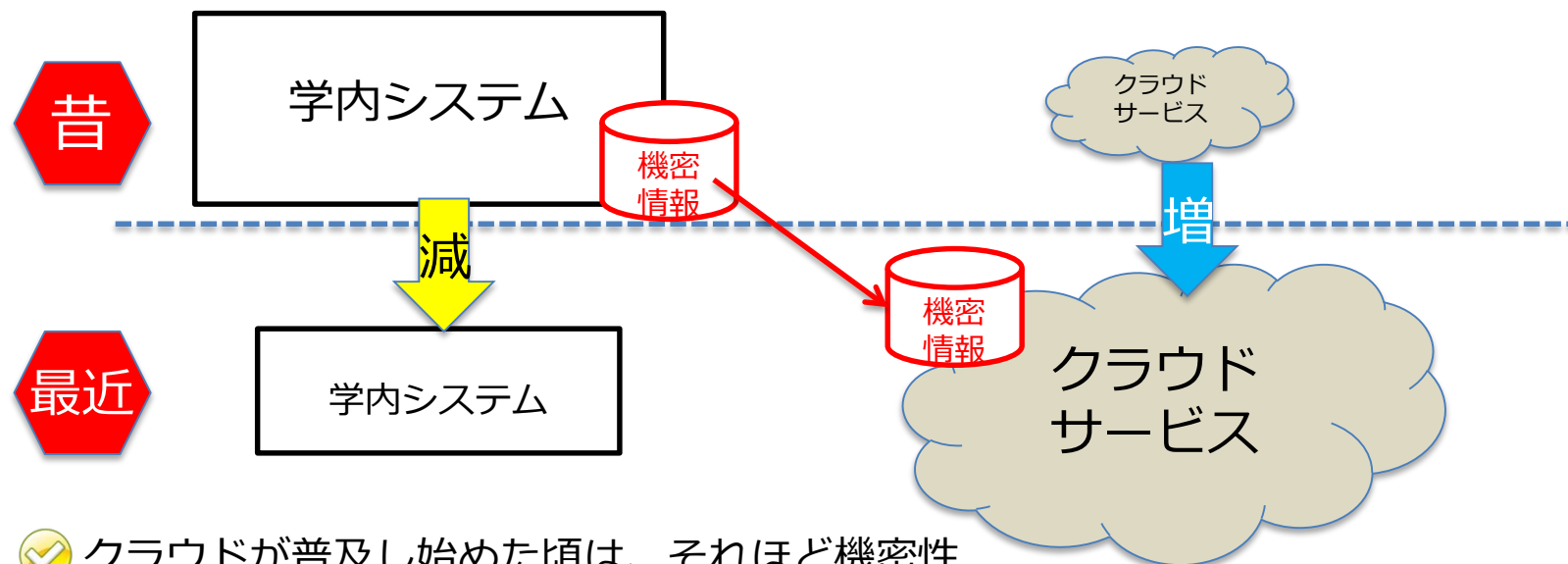
CIS2013報告会での私の発表

THE MOMENTS AHEAD FOR IDENTITY

- ①Identity業界は今、「TCP/IP Moment」を迎えている
～ネットワーク業界でTCP/IPそのものに代金を支払わなくなった瞬間
- ②具体的にどういう瞬間なのか。
 - (1) Standards-based identity
 - ・ Identityに関する技術は標準化ベースになる
～SAML、OpenID Connect、OAuth、SCIM
 - (2) Outcomes-based identity
 - ・ Identityに関するビジネスでは、本当の成果を求められる
～IDを管理すること、認証基盤を構築することで何が実現されるか？
 - 1. リスク低減(mitigate risk)
 - 2. ビジネスに直接貢献する事(increase customer delight)
 - (3) Professionalized identity
 - ・ Identityの専門化という職業が成り立つ
～今までは、セキュリティやプライバシーの専門家はいたが
Identityの専門家はいなかった。
～セキュリティやプライバシーを考えるにもIdentityから考える

2. クラウドの普及とフェデレーション

2.1 クラウドの普及と新たなセキュリティ対策の必要性



- ☑ クラウドが普及し始めた頃は、それほど機密性の高くない情報を扱うシステムのみクラウドサービスに移行するケースが多かった。
- ☑ 最近ではミッションクリティカルな業務のクラウドサービス利用が進む。
 - ・ 機密情報をクラウド事業者に預けざるを得ない

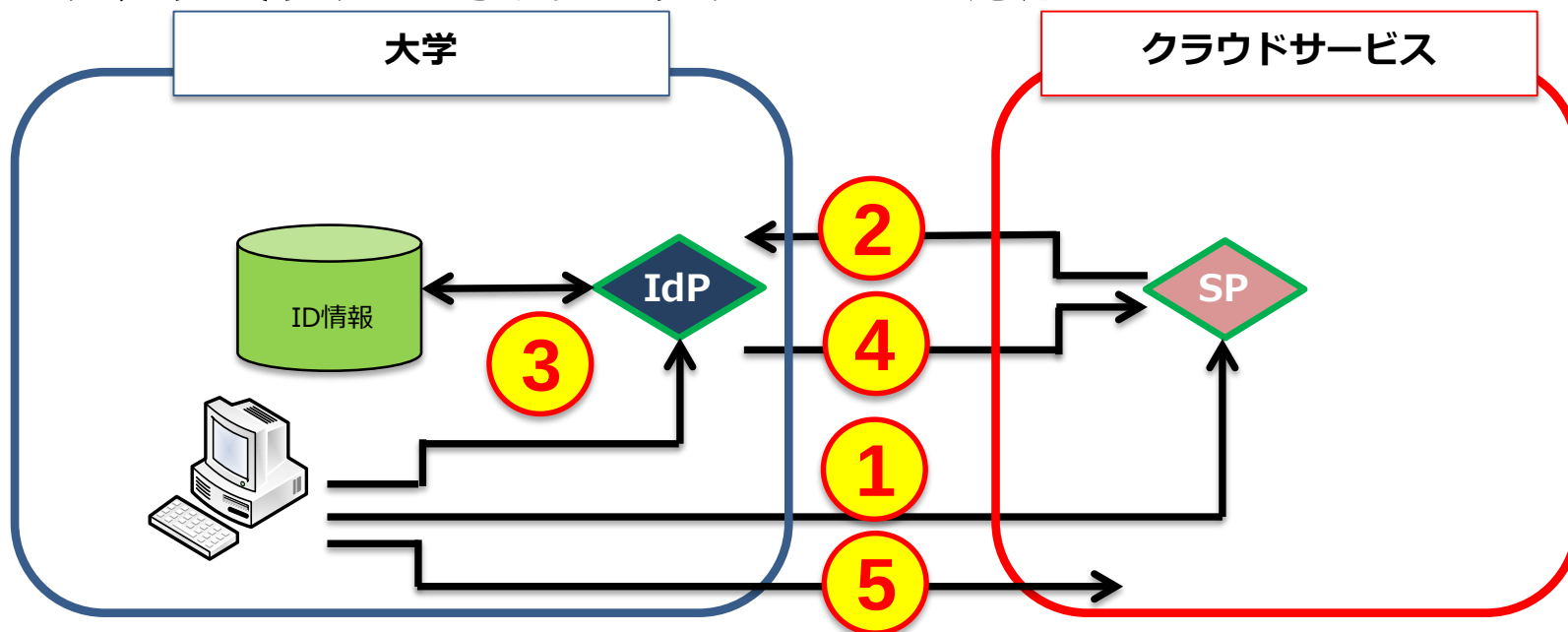
- ☑ (クラウド時代のセキュリティ対策のポイント)
 - ・ **セキュリティポリシーのコントロールを残す**

○ ID情報を大学内に残す

認証基盤を整備し
フェデレーション技術を活用

2. クラウドの普及とフェデレーション

2.2 アカデミックITでのフェデレーション応用

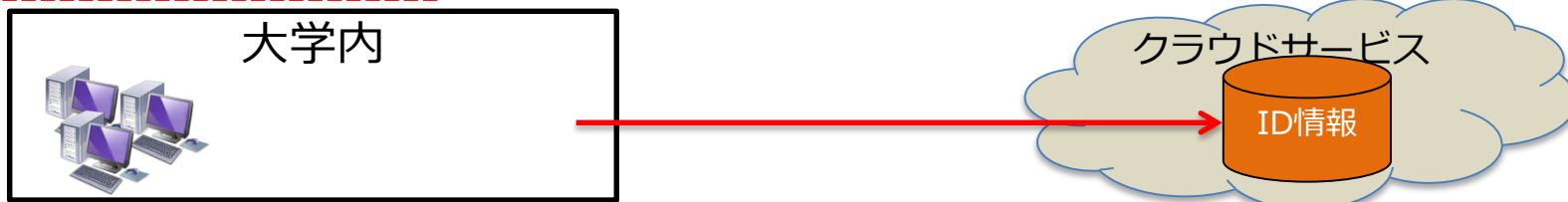


- ①【アクセス試行】 クラウドサービスへのアクセス
- ②【認証要求】 クラウドサービス事業者から利用企業への認証処理の委譲
- ③【認証処理】 エンドユーザによる認証処理
- ④【IDトークン返却】 クラウドサービスへの認証結果の連携
- ⑤【クラウドサービス利用】 エンドユーザによるクラウドサービス利用

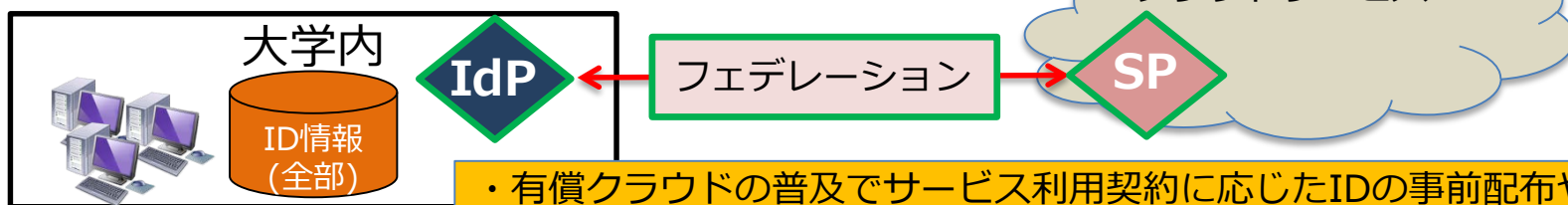
2. クラウドの普及とフェデレーション

2.2 アカデミックITでのフェデレーション応用

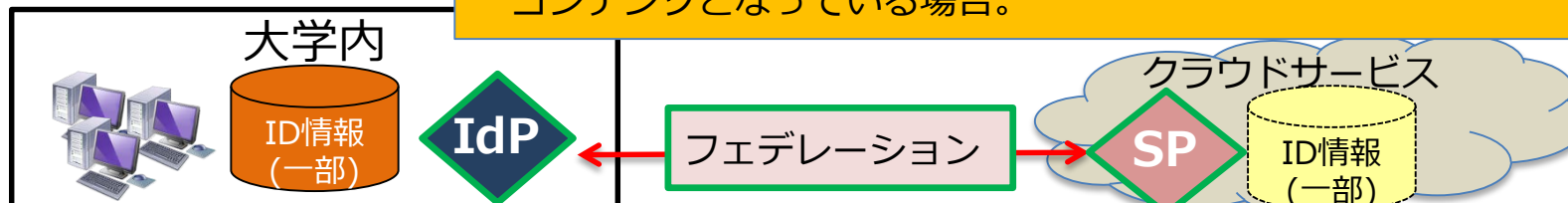
ローカル認証方式



フェデレーションによる認証情報連携



- ・有償クラウドの普及でサービス利用契約に応じたIDの事前配布やアクティベーションが必要な場合。
- ・スケジュール共有システムのようにID情報自体がアプリケーションのコンテンツとなっている場合。

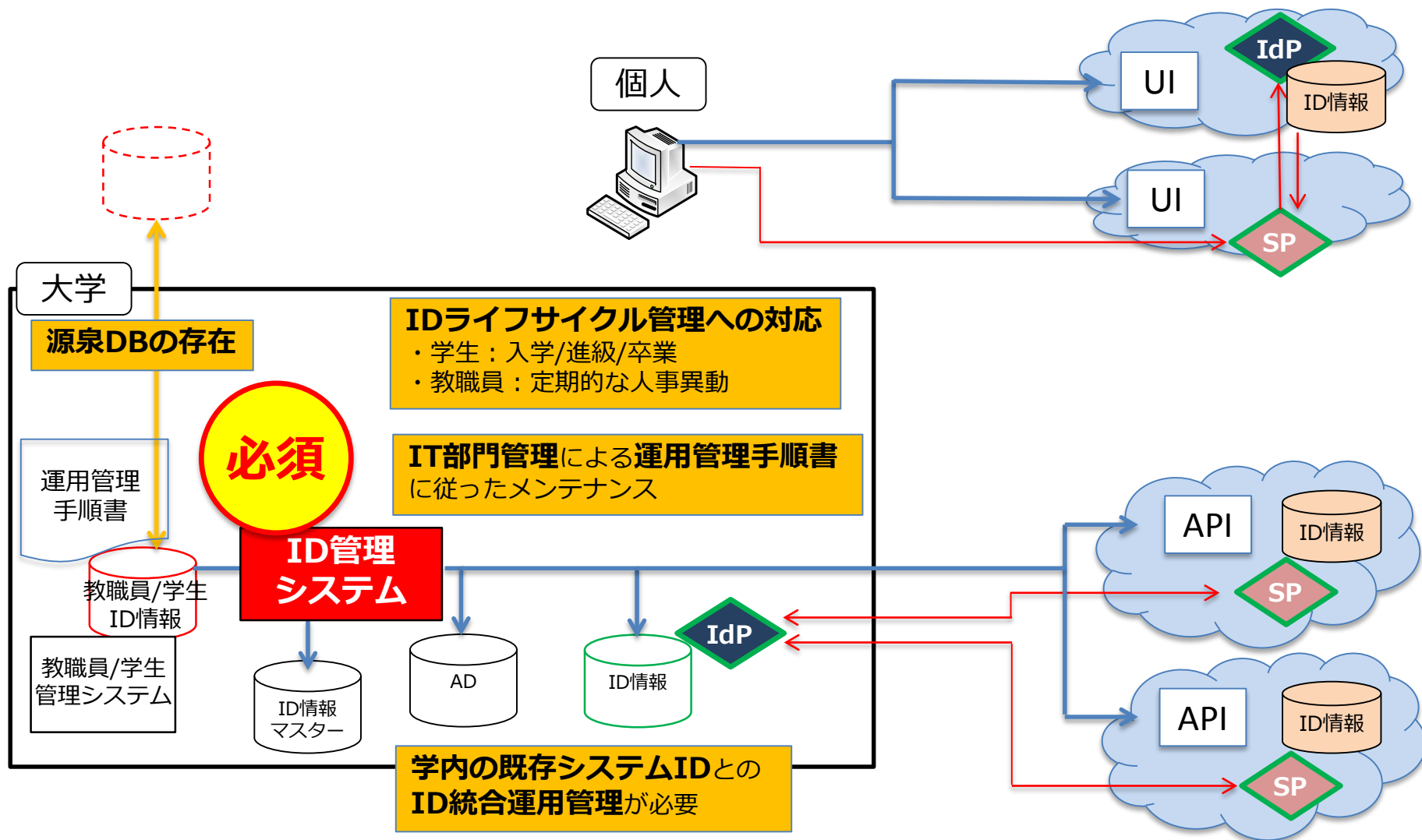


ID情報を大学内に残す

ID情報の一部はクラウドサービスに渡し、セキュリティポリシーの及ぶ範囲内にID情報の一部を残す。

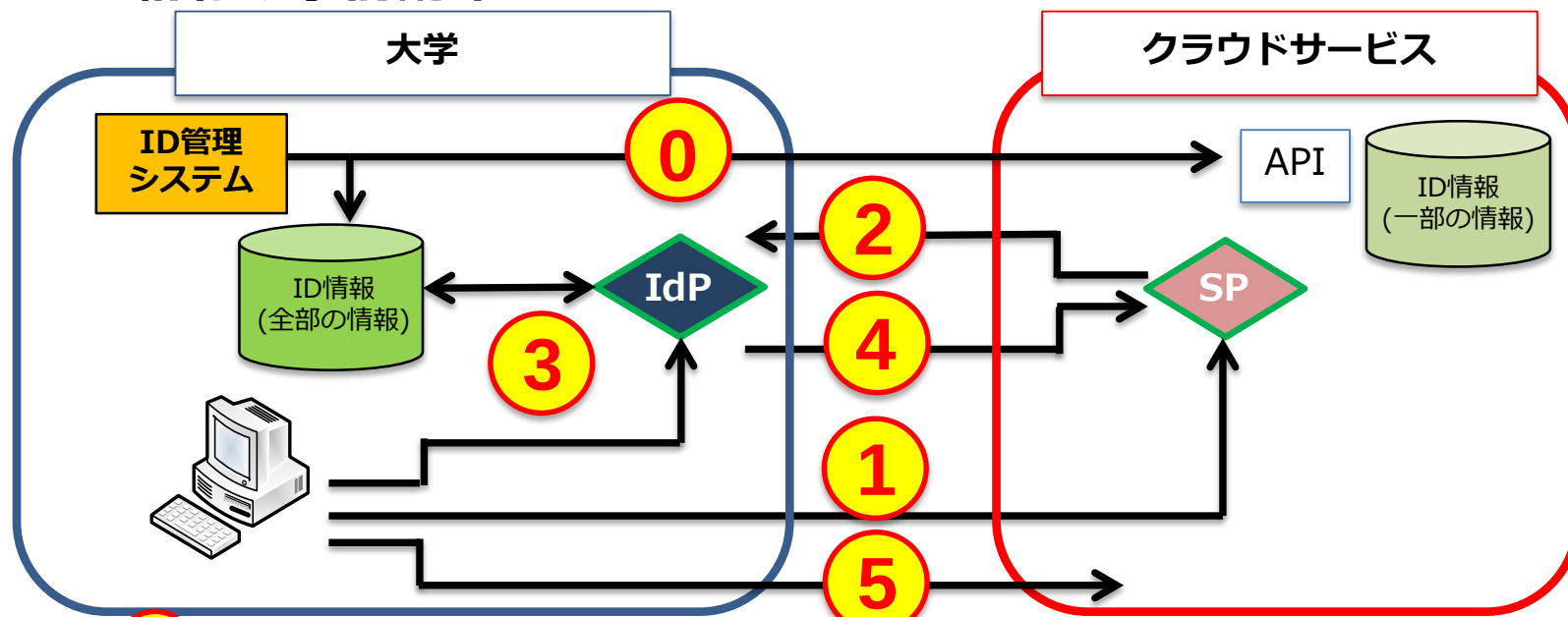
2. クラウドの普及とフェデレーション

2.3 ID情報の事前配布



2. クラウドの普及とフェデレーション

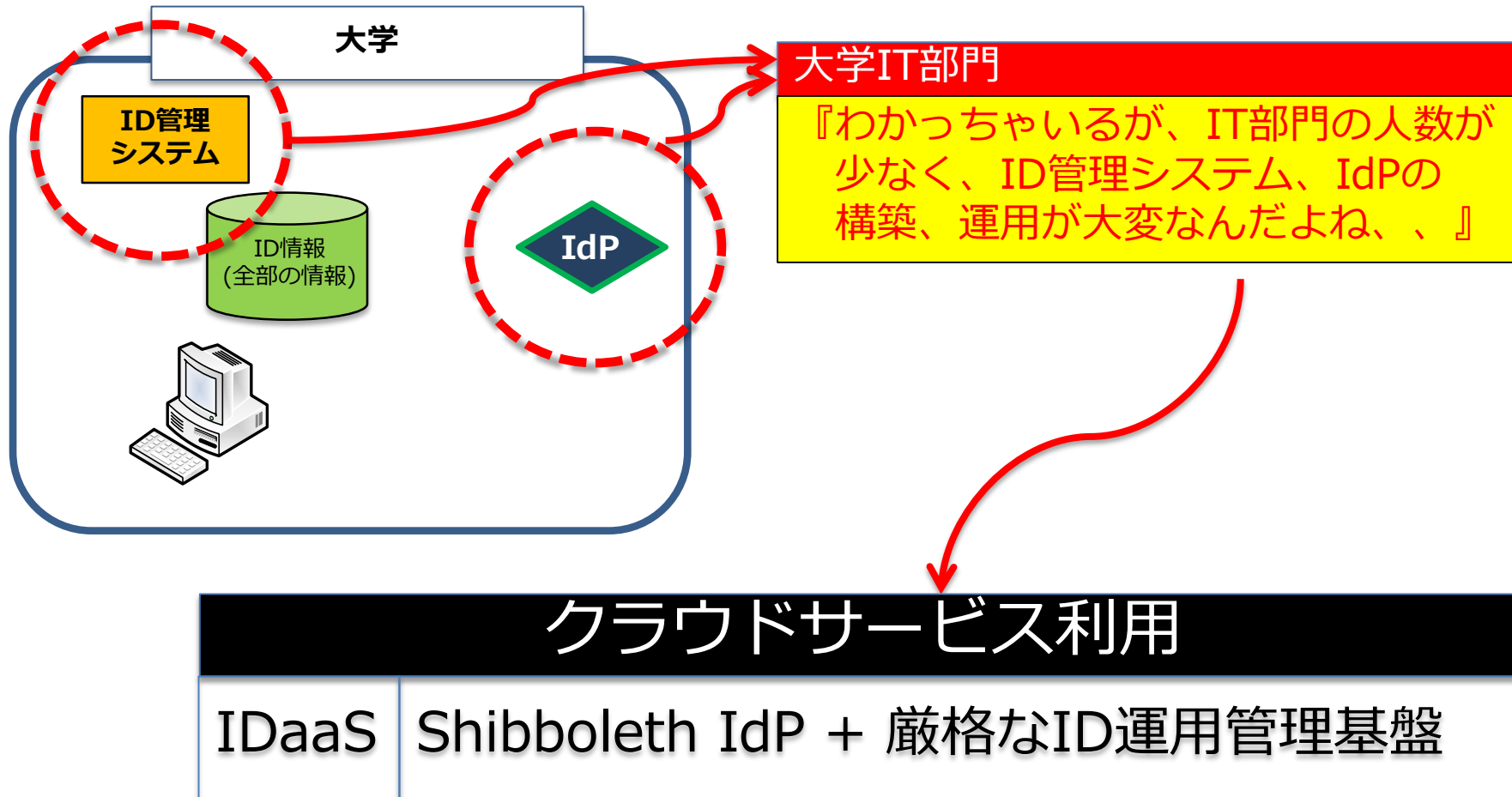
2.3 ID情報の事前配布



- ① 【アクセス試行】 クラウドサービスへのアクセス
- ② 【認証要求】 クラウドサービス事業者から利用企業への認証処理の委譲
- ③ 【認証処理】 エンドユーザによる認証処理
- ④ 【IDトークン返却】 クラウドサービスへの認証結果の連携
- ⑤ 【クラウドサービス利用】 エンドユーザによるクラウドサービス利用

2. クラウドの普及とフェデレーション

2.4 ID管理システム & IdP構築を検討する大学に事情



3. IDaaS概要

3.1 IDaaSの主要機能

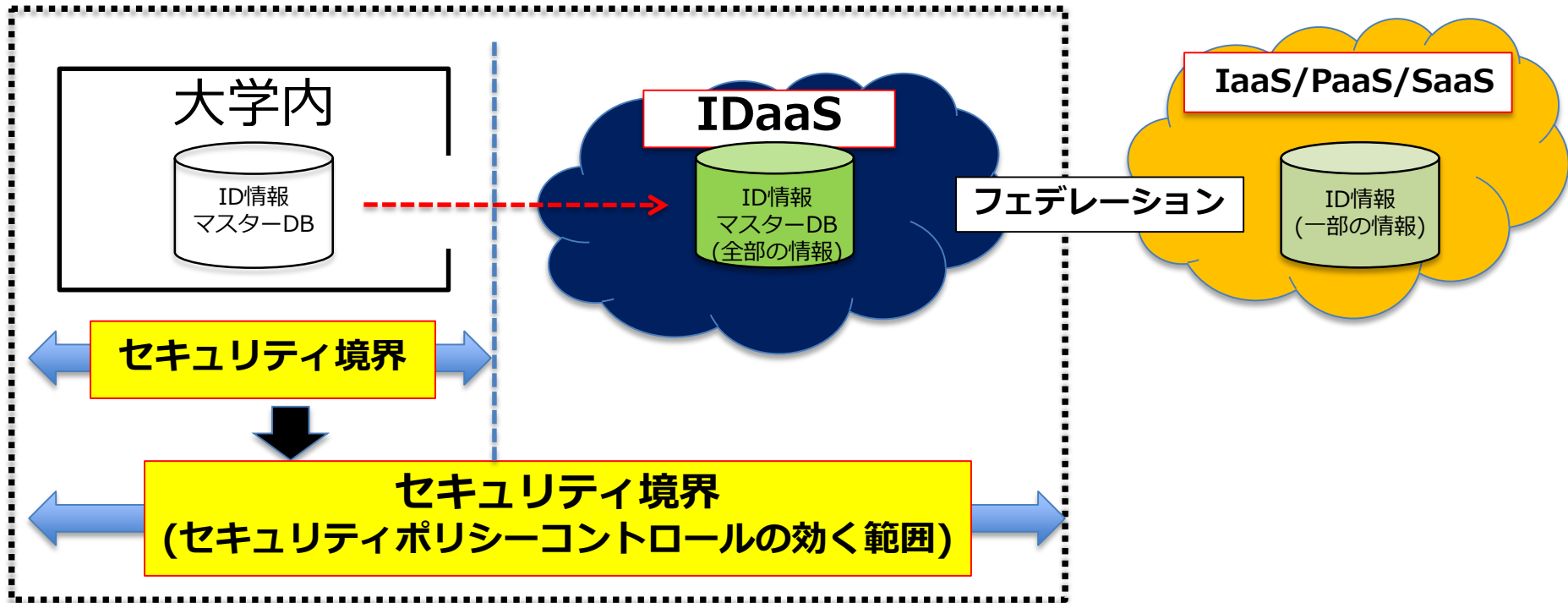
IDaaSとは

- ・ Identity as a Service
- ・ ID管理機能とフェデレーションをベースとしたシングル・サインオン機能をクラウドサービスとして提供する(下図①~④が主要機能)
- ・ インフラ&サービス監視はIDaaSの構成要素として重要
(次ページ「IDaaS選定のポイント」参照)



3. IDaaS概要

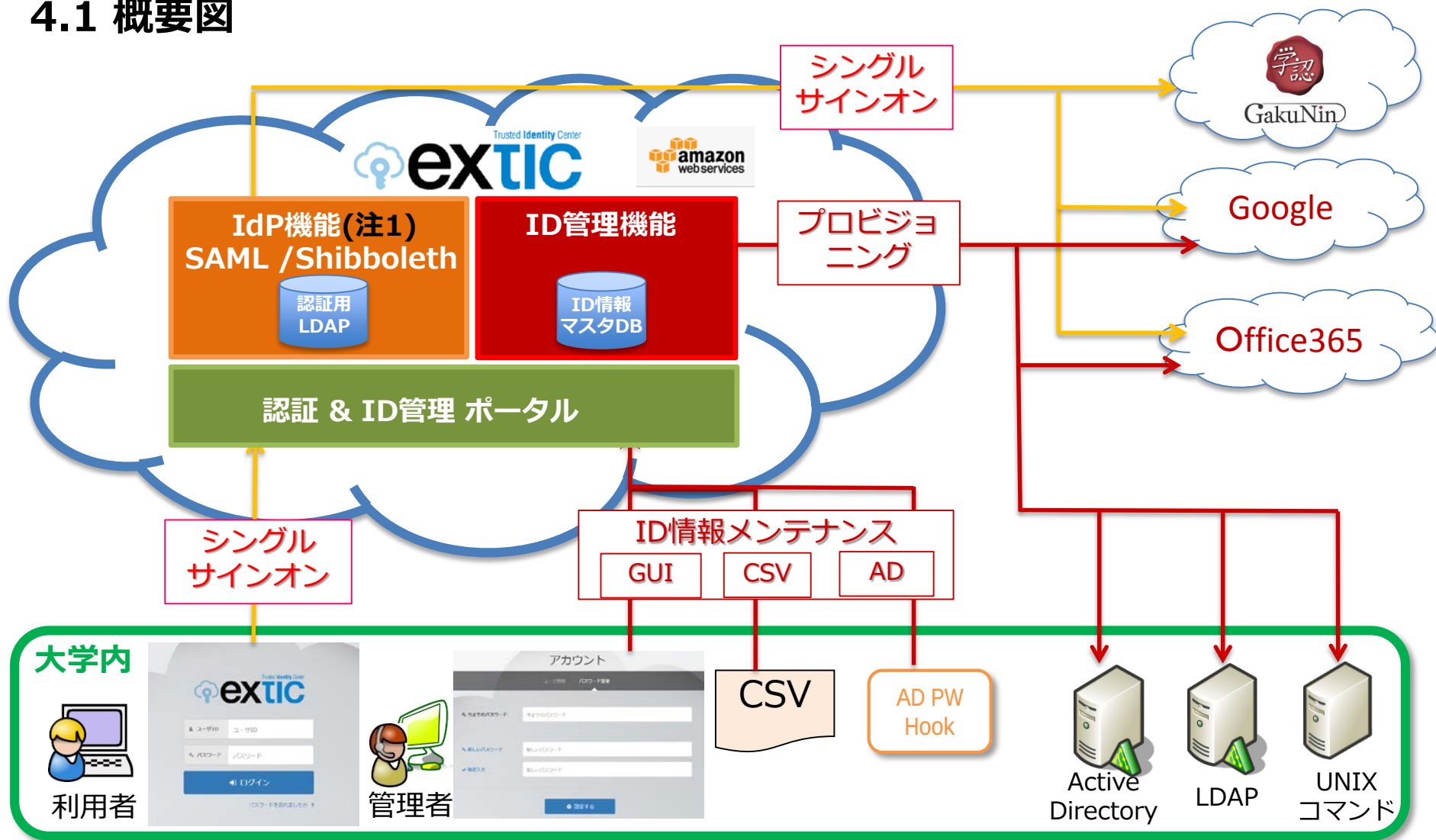
3.2 IDaaS選定のポイント



- ・ IDaaSでは大学のID&パスワードを含むID情報を預かります。大学がIDaaSを選択する場合、そのセキュリティレベルが重要なポイントとなります。大学内と同等もしくはそれ以上のセキュリティレベルが維持できることの説明が必要です。

4. Extic(Exgen Trusted Identity Center)

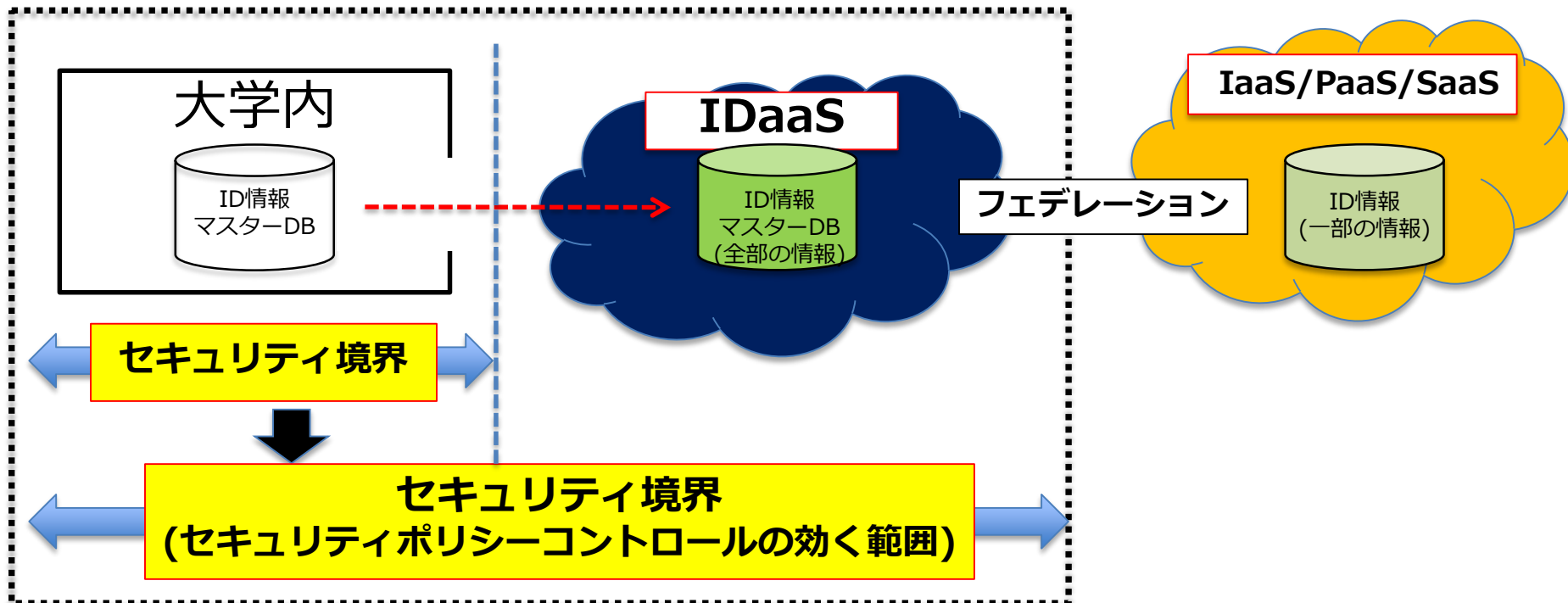
4.1 概要図



(注1)2016年7月リリース予定

4. Extic(Exgen Trusted Identity Center)

4.2 Exticのセキュリティ



- ・ IDaaSでは大学のID&パスワードを含むID情報を預かります。
大学がIDaaSを選択する場合、そのセキュリティレベルが重要なポイントとなります。
大学内と同等もしくはそれ以上のセキュリティレベルが維持できることの説明が必要です。

①ソフト

DeepSecurity

②サービス

24/365監視

③監視業務の運用

PCIDSS準拠

④障害対応時の開発元の運用

ISMS取得予定

4. Extic(Exgen Trusted Identity Center)

4.3 導入事例

- **お客様概要**

- お客様名：文教大学
- ユーザー数：約 10,000 ユーザー

- **ご要求事項**

- ID 管理に関わるサーバーや拡張時のメンテナンスコストを抑えたい。
- ID 管理の対象外となっている Office 365 も統合管理したい。
- LDAP Manager で実現している運用をできるだけ引き継ぎたい。

- **導入効果**

- Extic 採用による ID 管理関連サーバーのメンテナンスコストを削減できました。
- Office 365 x 2 ドメインも ID 統合管理対象システムとすることにより、学内の ID を統合管理することができました。
- これまでに培ってきた LDAP Manager のノウハウが反映されている Extic であるため、LDAP Managerで行っている運用をあまり変えることなく、移行が実現できました。

4. Extic(Exgen Trusted Identity Center)

4.3 導入事例

- お客様概要

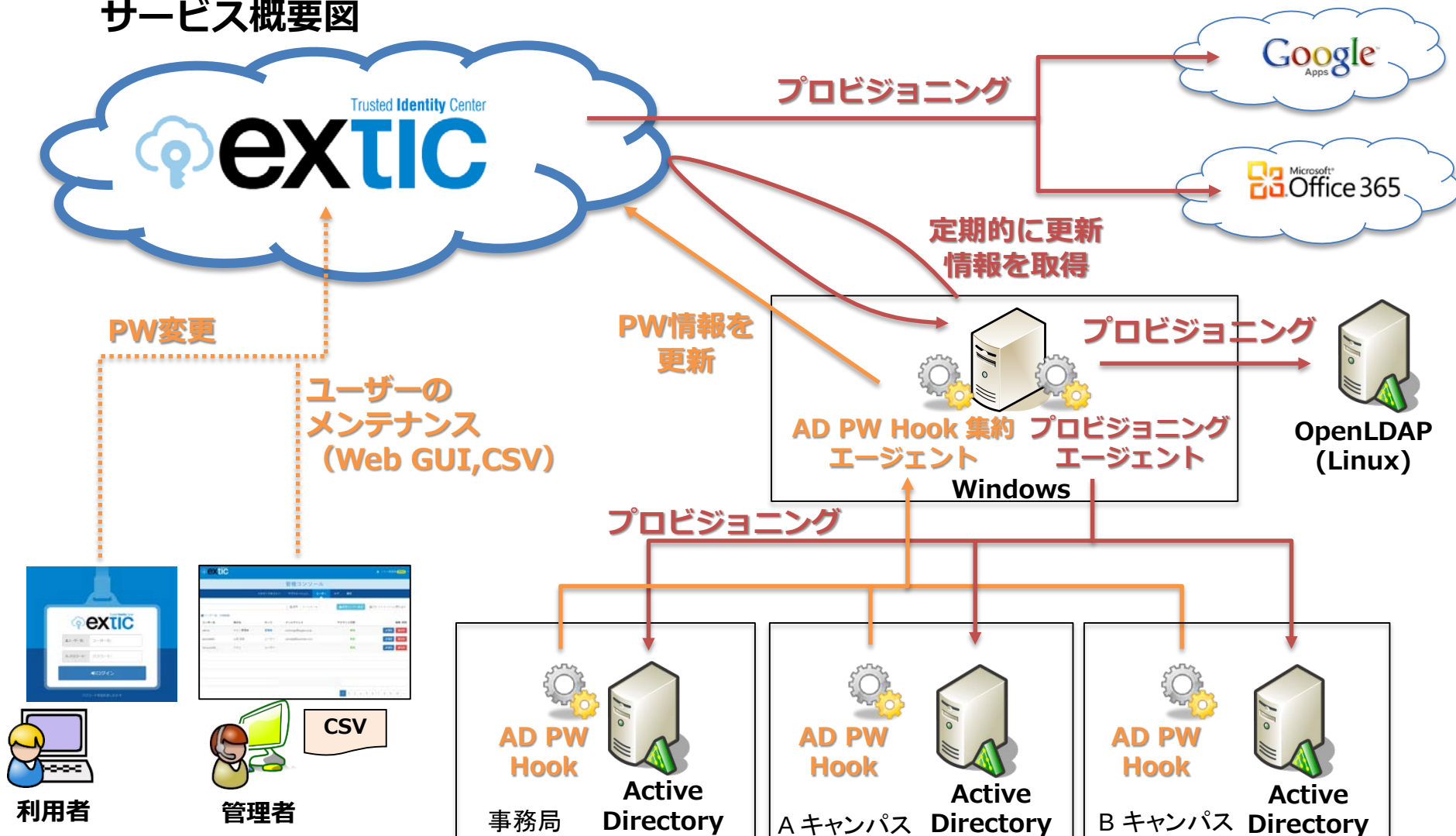
- 機能構成

- Extic ライセンス数 : 5,001 ~ 10,000 ユーザーライセンス
 - 連携システム
 - Office 365 x 2 ドメイン
 - Google Apps x 3 ドメイン
 - オンプレミス連携
 - » Active Directory x 3 ドメイン
 - » OpenLDAP x 1
 - » AD パスワードフック
 - » パスワード通知書印刷機能

4. Extic(Exgen Trusted Identity Center)

4.3 導入事例

サービス概要図



5. IDaaSをご利用いただくために

5.1 アカデミックIT環境におけるSaaS普及の取り組み

大学
広島大
クラウド利用
ガイドライン

クラウドサービス利用時の
注意事項や実施内容の明確化

IaaS/PaaS/SaaS

NII
学認クラウド
チェックリスト

クラウドサービス事業者の
可視化

NII支援方策 (2)クラウド導入支援 実験中

大学がクラウドを導入するための支援サービス

- 大学がクラウドを導入する際に確認すべきチェックリスト（信頼性、セキュリティ、契約条件等）を策定し、チェックリストに基づくクラウド（事業者・サービス）の検証結果を大学に提供。
- クラウドサービス調達における課題整理と解決策を検討。

大学・研究機関

- ・チェックリストと調査結果を用いた仕様策定
- ・クラウドの調達



学認クラウド

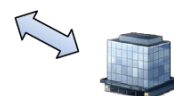
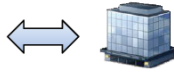
チェックリスト 評価結果



- ・チェックリストの作成
- ・クラウドの評価
- ・アカデミックディスカウント検討

クラウド事業者

- ・チェックリストに基づく自社クラウドの評価
- ・参考価格提示



Kento Aida, National Institute of Informatics

5. IDaaSをご利用いただくために

5.2 SaaS利用を検討する大学の事情

- ・ある大学がIDaaS利用を検討したとき、**広島大が作成したクラウドサービス利用ガイドライン**の以下の項目をどう適用するかが課題に。

①要件 独立性の高さ

預ける情報のリスクを判定し、マルチテナント型サービスの利用可否を判定する。

②要件 通信経路の安全性

預ける情報のリスクを判定し、インターネットを介してクラウドへアクセスすることの可否を判定する。

預ける情報＝ID情報は重要度IIかIIIか、判断するのが難しい

そもそも、ID情報をSaaSに預けるにはセキュリティポリシーの変更が必要

NG IDaaS利用＝他校で前例ない

OK Office365等のメガSaaS＝他校で前例ある
パッケージソフト on AWS(SINET直結)＝セキュリティポリシーOK

5. IDaaSをご利用いただくために

5.3 USにおけるSaaS普及の取り組み

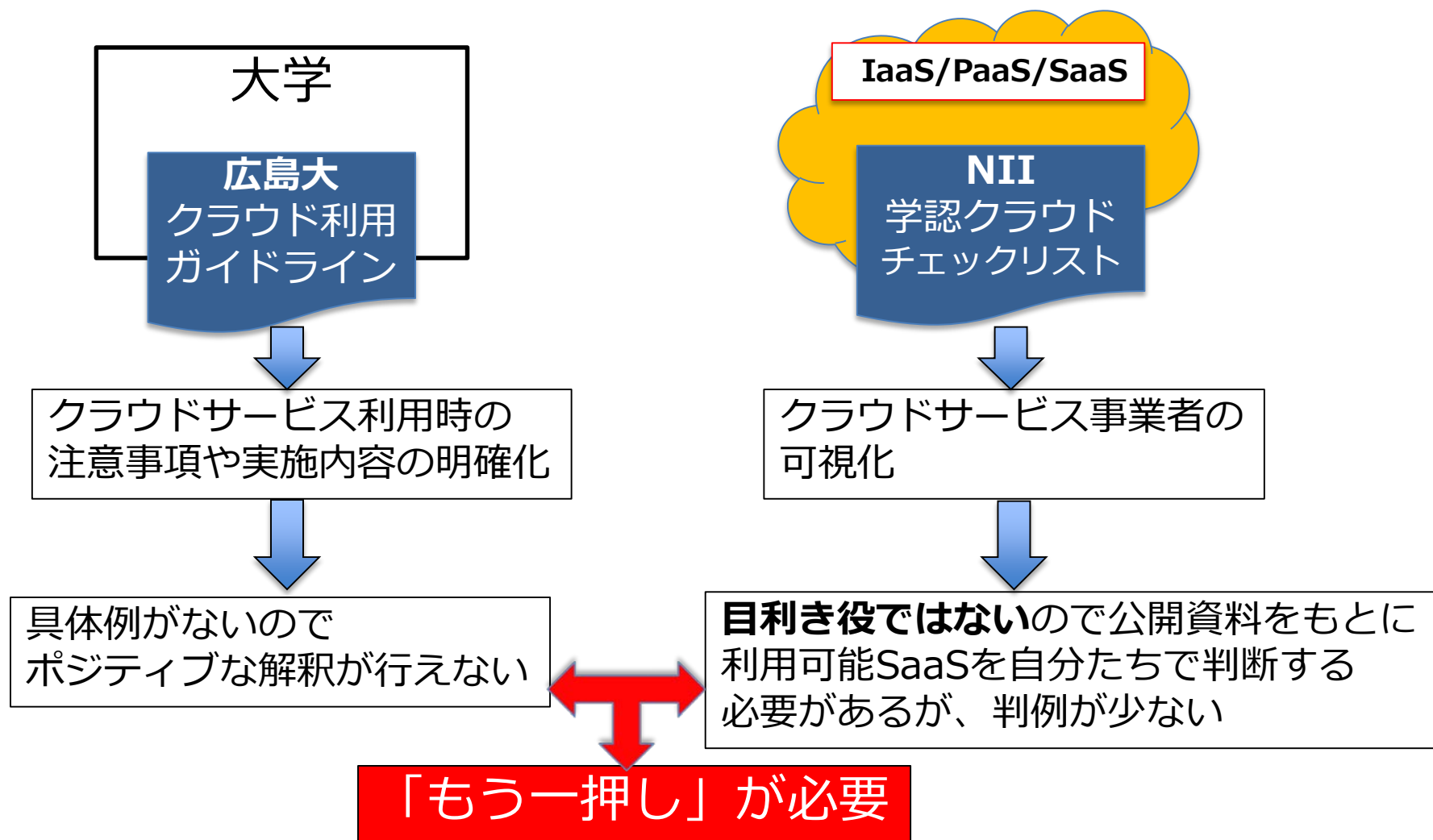
- Internet2 NET+



NAME	TYPE	PHASE	ELIGIBLE SUBSCRIBERS
2FA	S&I		
Akamai Security Services	S&I		
Bitglass Cloud Security Access Broker	S&I		
CloudLock	S&I		Internet2 Member
DocuSign	S&I		Internet2 Member
Duo Security	S&I		
eduroam	S&I		Internet2 Member or Other R&E Participant
Fidelis XPS	S&I		
Fischer Ignite-Federation Service	S&I		Internet2 Member or Other R&E Participant
InCommon Certificate Service	S&I		
KeyNexus	S&I		Internet2 Member
LastPass	S&I		Internet2 Member or Other R&E Participant
Lookout Mobile Threat Protection	S&I		
Netskope	S&I		
SafeNet	S&I		Internet2 Member or Other R&E Participant
Securio Cloud Protect	S&I		
Skyhigh	S&I		Internet2 Member
Splunk Enterprise On Premise	S&I		Internet2 Member
Toopher	S&I		
Vera	S&I		

5. IDaaSをご利用いただくために

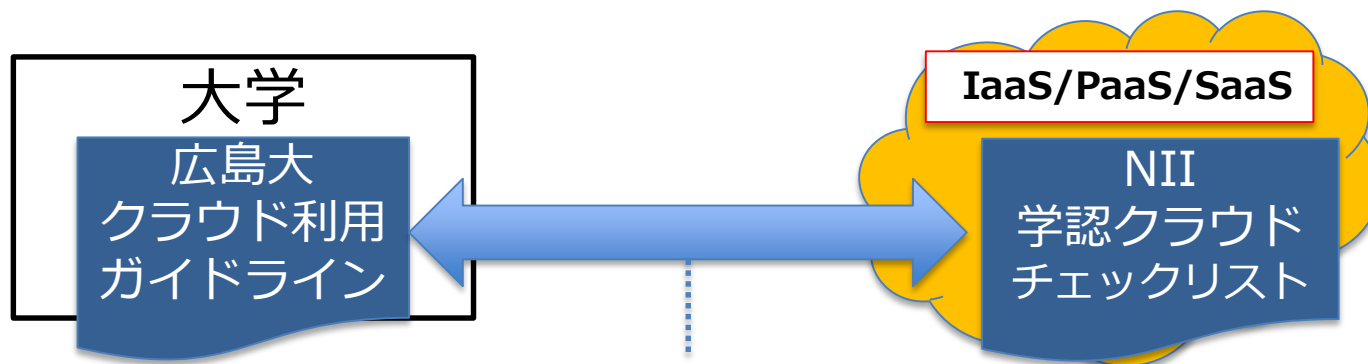
5.4 IDaaS普及には「もう一押し」が必要



5. IDaaSをご利用いただくために

5.5 AXIES認証部会での試み (正規の)口コミ確立

Identity Eco System
作りを先行する



Identity目線で具体的な製品やサービスを当てはめて解釈する。

部会に参加しているメーカーの製品やクラウド事業者のサービスを検証できるように整備する。

この一例がIDaaS

評価環境提供
のベースになる

部会に参加している大学に評価してもらい、評価結果を公表する。

SaaS利用可能なセキュリティポリシーのサンプル文を作成する。

・ OPTiM Store(2016年 3 月 9 日発表)



①様々なSaaSの品定め

②様々なSaaSのセキュアな環境の提供

③様々なSaaSの効率的利用環境の提供

* ハイブリッドクラウド(SaaS、プライベートクラウド、オンプレを組み合わせた)利用をお客様がそれぞれの要件に合わせて行うのではなく、あらかじめクラウド事業者がトータルソリューションとして提供する。

• CASB

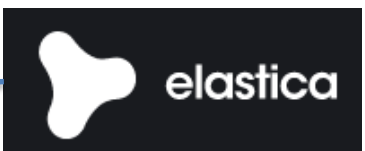
- Cloud Access Security Broker
- クラウドサービスと企業ユーザの間に位置し、クラウドへのアクセスのセキュリティを確保する様々な機能を有するソフトまたはサービス
- 暗号化、監査、データ漏えい防止、アクセス制御、不正なふるまい検知。
- ガートナーの予想では今年の市場規模が\$100M、2018年には\$400Mに達する。
- 既に10社を超えるCASBベンダーが存在している。



total data protection



Trust in the Cloud™



elastica

BLUE COAT

Perspecsys