NIIオープンフォーラム2017

EXGEN NETWORKS

学認　―トラストの現在と未来―

IDaaSは学認アンケートに耐えられるのか

2017年6月7日

EXGEN 江川

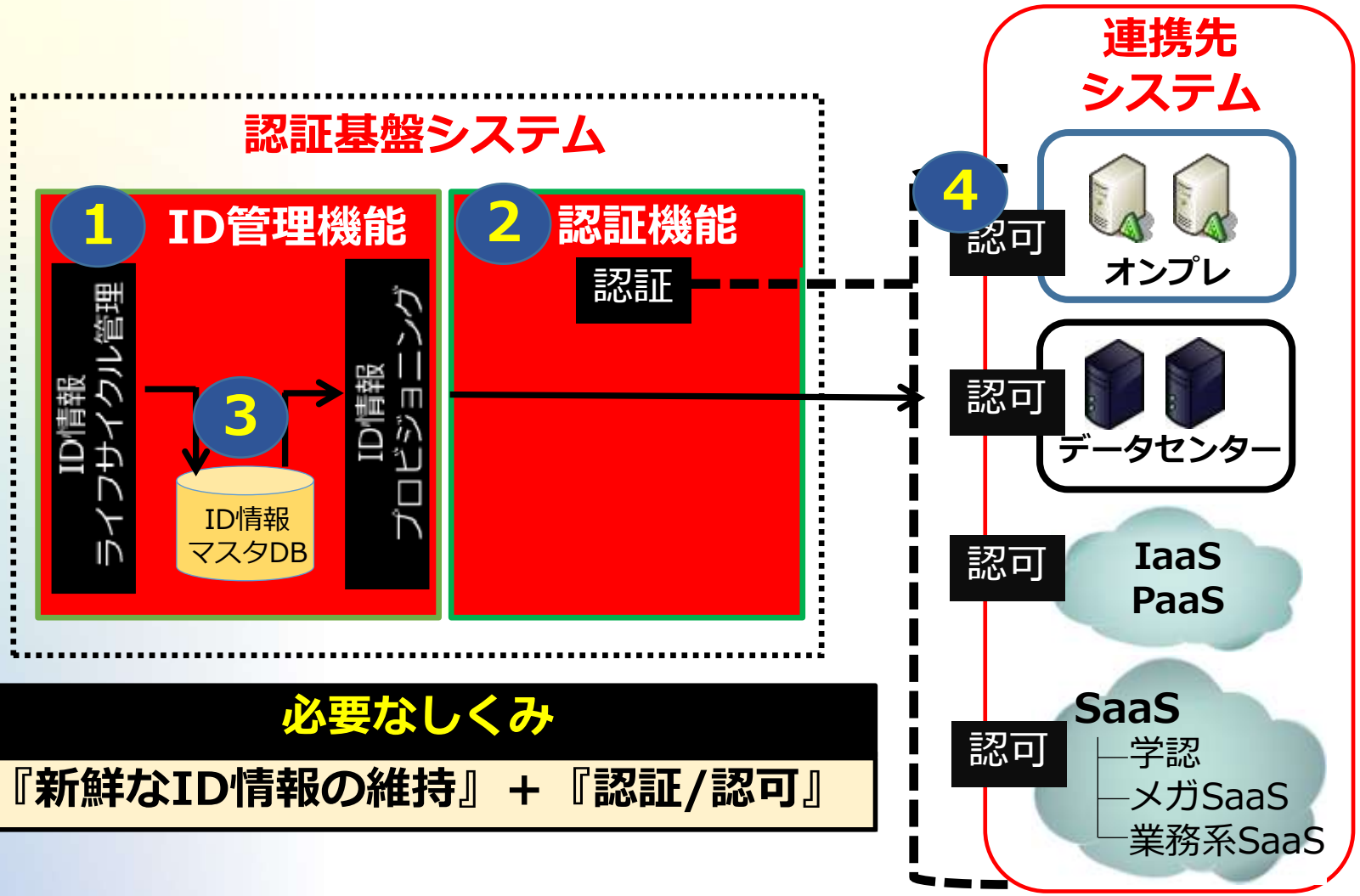
USE INNOVATIVE TECHNOLOGY.

1. 認証基盤システム構成と認証/認可

機能構成と実装場所

1.認証基盤システム
- ①ID管理機能(IDM)
- ②認証機能(IdP)
- ③ID情報マスタDB

2.連携先システム
- ④認可機能



認証基盤構築の目的

適切なアクセス権限管理の維持

必要なしくみ

『新鮮なID情報の維持』 + 『認証/認可』

2. 認証基盤システムにおけるID管理システムの役割

① 認証/認可のしくみに対して、ID情報の鮮度を保つしくみが必要

② ID情報 & 属性情報の事前配布が必要

(1) 認可のための属性情報の事前配布

(2) コンテンツとしてのID & 属性情報の事前配布

(スケジュール共有システムのようにアプリケーションによっては
ID情報自体がコンテンツとなっている場合が多い)

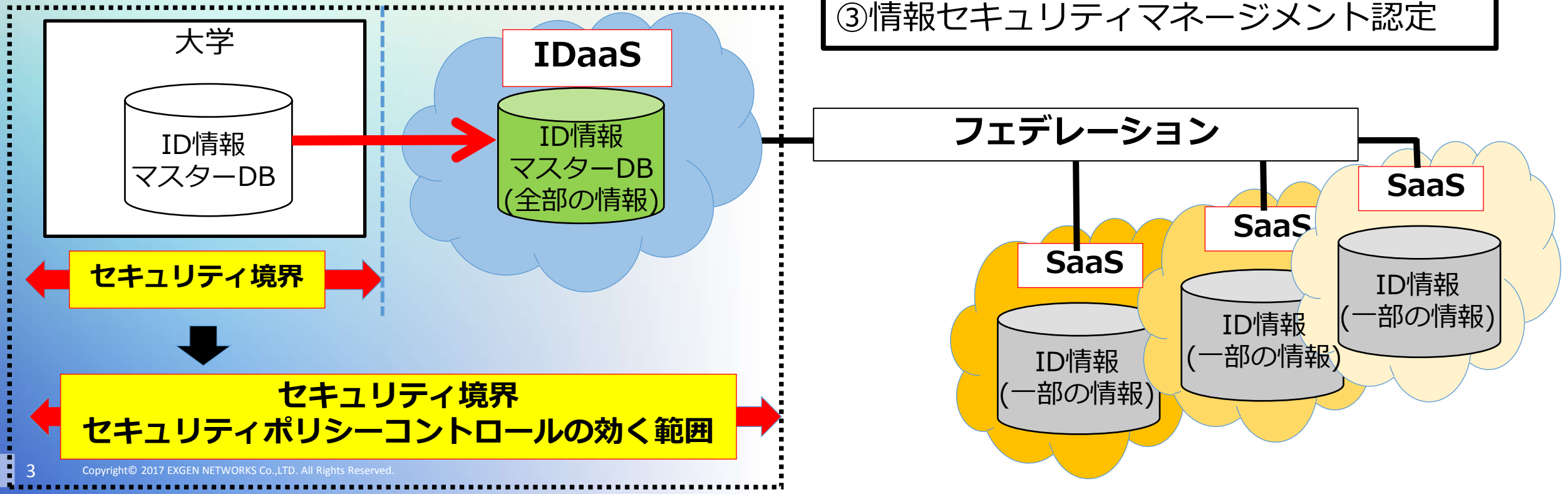
(3) サービス利用契約に応じたライセンス数分のIDの事前配布

**③ 教職員/学生のID情報をIT部門が一括してメンテナンスを行うため
メンテナンス効率の向上のしくみが必要**

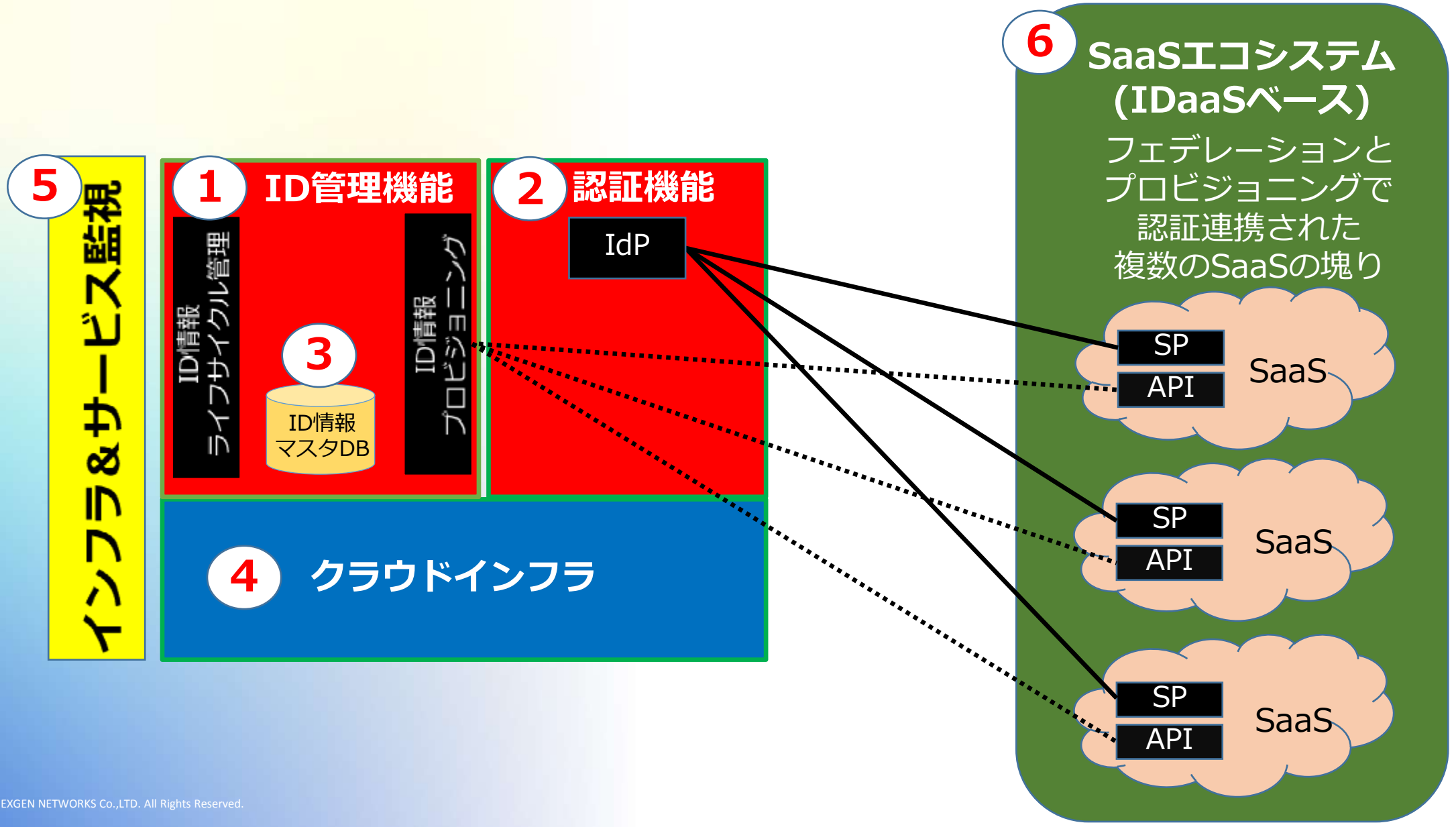
3. IDaaSにおけるサービス監視の必要性

・ID情報マスターDBを保管する場所、IdPで認証を行う場所の安全性が課題。
・大学にとってはIDaaSまでがセキュリティ境界内。
・IDaaSのセキュリティレベルは大学と同等もしくはそれ以上であることが必要。

①統合型セキュリティツールを実装
②24/365の**インフラ & サービス監視**
③情報セキュリティマネージメント認定

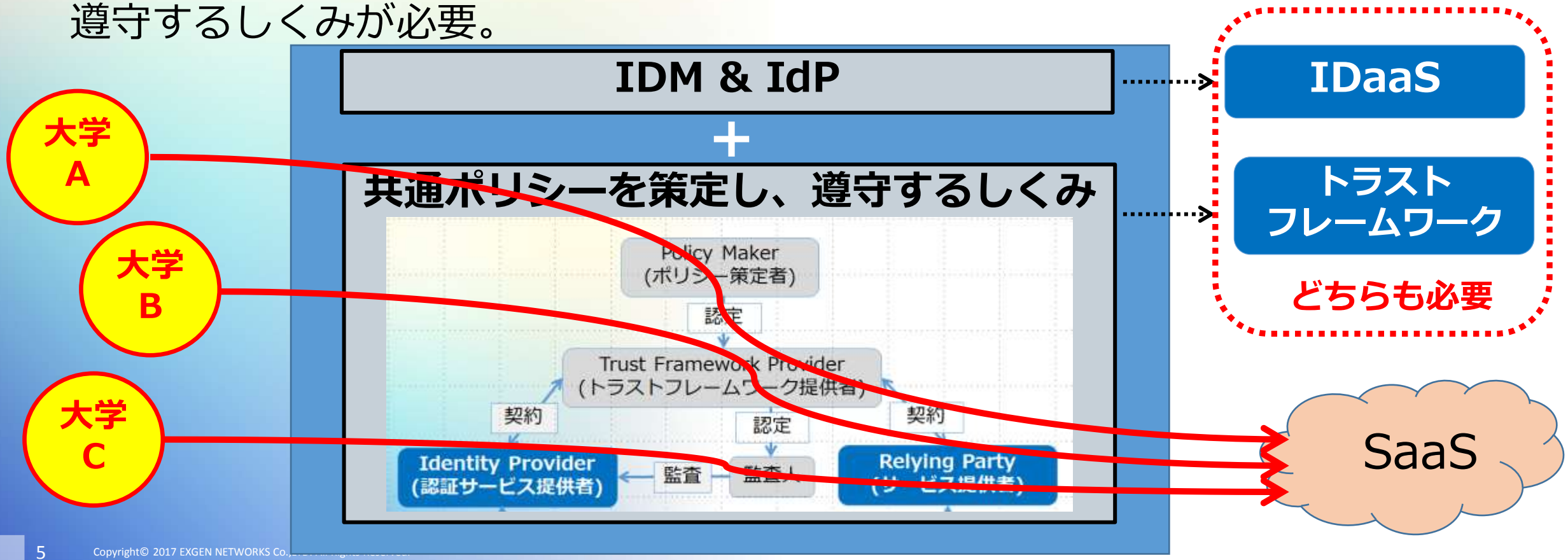


4. IDaaSの構成



5. トラストフレームワークとIDaaS

・複数の大学が、セキュアに情報共有を行う(例：学認SPを利用する)ためには、認証基盤システムが必要。
・さらに、各大学でセキュリティマネージメントレベルを統一する必要があり、そのためには共通のセキュリティポリシーやID運用管理ポリシーを策定し、遵守するしくみが必要。



6. 学認アンケート対応のIDaaSとは

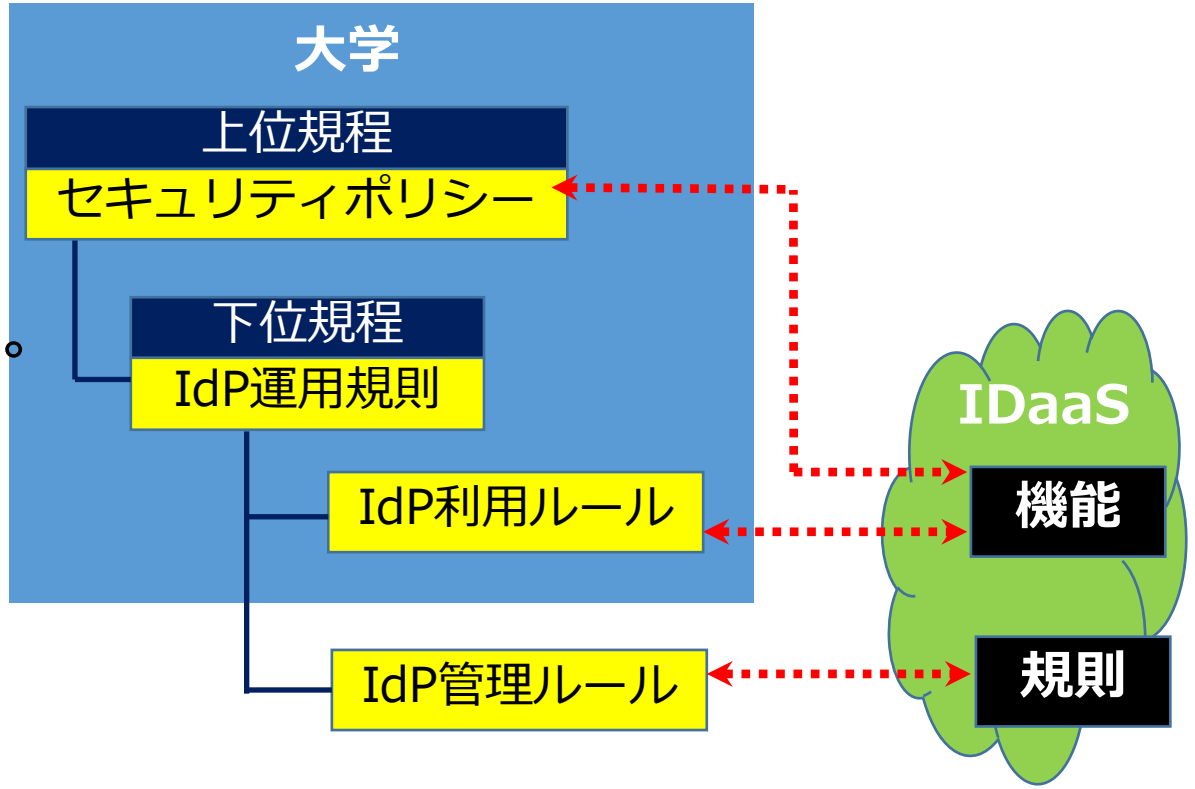
6.1. ガバナンス

(ポジティブな回答のポイント)

・IdP運用規則が定められている。
・その上位規程として、セキュリティポリシーが定められている。

(学認対応のIDaaSとは)

①大学のセキュリティポリシーに沿った、
　セキュリティ機能設定ができる。
②大学のIdP運用規則の利用ルールに
　沿った、ID運用管理の機能設定ができる。
③IDaaSのIdP運用管理ルールが、
　大学のセキュリティポリシーの下位規程
　として整合性が保たれている。
　→(Exticの場合)
　IdP運用管理規則の公開(準備中)
　ISMS取得(準備中)

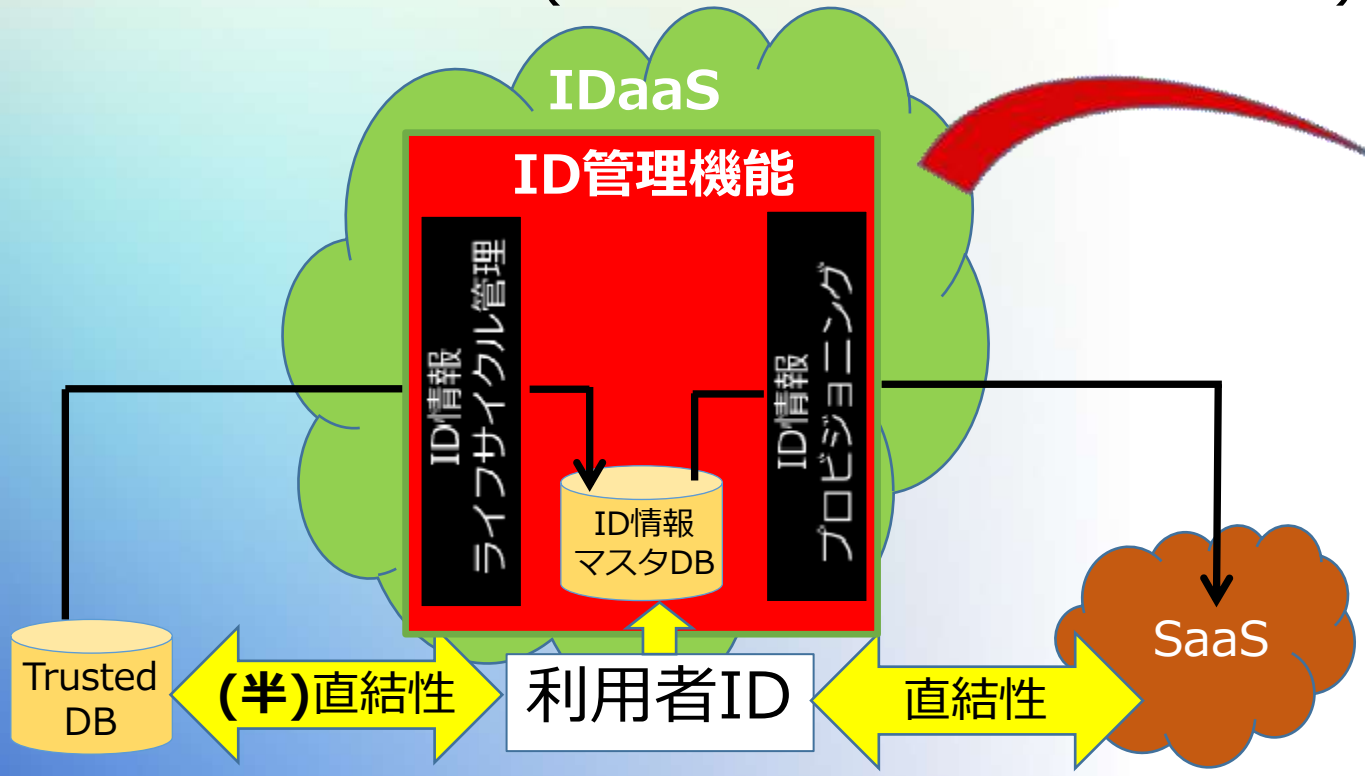


6. 学認アンケート対応のIDaaSとは

6.2. テクニカル① 『利用者IDと属性の管理・運用』

(ポジティブな回答のポイント)

・利用者IDが、学務データや人事データ等、大学内で信頼できるDB(Trusted DB)で作成され、**(半)**直結している。
・IDライフサイクル(特に破棄、停止のプロセス)が、きちんと回っている。



(学認対応のIDaaSとは)

(半)直結性を担保する
ID管理機能が実装されている

6. 学認アンケート対応のIDaaSとは

6.2. テクニカル① 『利用者IDと属性の管理・運用

(学認対応のIDaaSとは) ＝(半)直結性を担保するID管理機能

①ID情報ライフサイクル管理機能

(1)学認が推奨する属性情報をメンテナンスできる(次ページ参照)。

(2)変なIDが紛れ込むことを防止する (オペミス低減、統制外オペの抑止)。

(3)部局管理者に正当で適切なメンテナンス権限を与える。

→**(Exticの場合)**CSVメンテナンス機能、 管理者権限の委譲機能
管理者用ID情報メンテナンス画面、**ログ管理機能**

②ID情報プロビジョニング機能

・SP毎に必要な属性情報を送出できる。

→**(Exticの場合)**Office365連携等のプロビジョニング機能(注)
(注) 必要な属性情報の送出は認証機能(フェデレーション)でも行っている

6. 学認アンケート対応のIDaaSとは

6.2. テクニカル① 『利用者IDと属性の管理・運用』

(Exticで管理できる属性情報)

- mail
- sn
- o
- ou
- givenName
- displayName
- eduPersonAffiliation
- eduPersonPrincipalName
- eduPersonEntitlement
- eduPersonScopedAffiliation
- eduPersonTargetedID
- jasn
- jaGivenName
- jaDisplayName
- jao
- jaou

(Exticで管理できない属性情報)

- isMemberOf
- gakuninScopedPersonalUniqueCode
- eduPersonAssurance
- eduPersonUniqueId
- eduPersonOrcid

6. 学認アンケート対応のIDaaSとは

6.2. テクニカル②　『派遣職員や臨時職員の取扱い』

(ポジティブな回答のポイント)

・Trusted DBに含まれない派遣職員や臨時利用者に対する利用者IDについて、
(1)組織メンバーとそれ以外を区別している。
(2)臨時利用者はアカウント有効期限を設定して管理している。
(3)属性に応じてSPの利用を制御している。
・共有アカウントを禁止している。

(学認対応のIDaaSとは)

①ID情報ライフサイクル管理機能
(1)eduPersonAffiliationについて、staff、student等以外の値の設定ができる。
(2)臨時利用者はテンポラリーアカウトとして有効期限付きIDとして管理が可能。

6. 学認アンケート対応のIDaaSとは

6.2. テクニカル② 『派遣職員や臨時職員の取扱い』

(学認対応のIDaaSとは)

②ID情報プロビジョニング機能

・利用者IDの属性情報に応じて、SPに対する連携可否の制御が可能。

→**(Exticの場合)**Office365連携等のプロビジョニング機能(注)

③認証機能

・利用者IDの属性情報に応じて、SPに対するアクセス可否の制御が可能。

→**(Exticの場合)**認証ポータル画面(2017年12月リリース予定)

～属性情報により、SSO可能なアイコン表示を制御することが可能

～利用者ID x SP毎にSSOの可否を設定することが可能

(注) 利用者IDの特定の属性情報(例：eduPersonAffiliation)により、SPへのアカウント情報連携(アクティベーション等)を自動化するためには、Exticの前処理として、該当属性情報(例：Office365連携フラグ)を予めメンテナンスしておく必要がある。

6. 学認アンケート対応のIDaaSとは

6.2. テクニカル③ 『プルーフィングとセキュリティ』

(ポジティブな回答のポイント)

・IDやクレデンシャルの配布は本人確認を行った上で書面で行っている。
・全学セキュリティポリシーに沿ったパスワードポリシーの設定を行っている。

(学認対応のIDaaSとは)

①ID情報ライフサイクル管理機能
　(1)ID通知書の出力が可能。
　　→**(Exticの場合)**
　　CSVメンテナンス機能
　　管理者用ID情報メンテナンス画面
　(2)パスワードポリシーチェック機能
　　がある。

(Exticで設定可能パスワードポリシー)

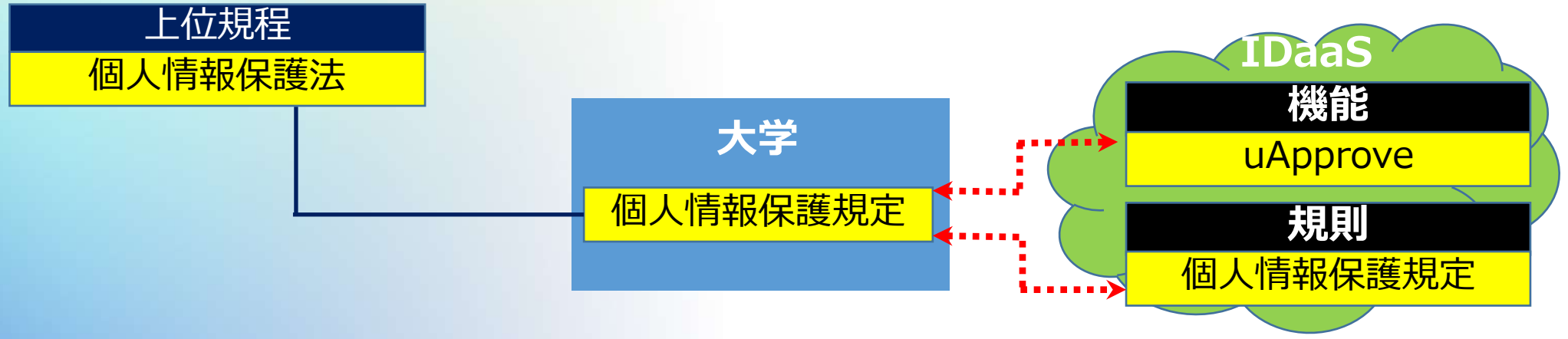
・Active Directory と同様のパスワードの複雑さの設定
・最小の長さ／最大の長さ
・入力必須文字タイプ
・入力禁止文字
・過去に設定したパスワードの再利用を禁止
・有効期限
・有効期限切れ前に通知する期間
・認証の失敗回数が指定回数に達した場合に
　アカウントのロックアウト
・アカウントをロックアウトする期間

6. 学認アンケート対応のIDaaSとは

6.3. プライバシー

(ポジティブな回答のポイント)

・個人情報保護に関する法令に従い、学内でも規程が定められている。
・認証機能により送出される属性情報について、利用者の同意を取得する仕組みがある。



6. 学認アンケート対応のIDaaSとは

6.3. プライバシー

(学認対応のIDaaSとは)

①大学の個人情報保護規定に沿った、属性情報送出同意機能(uApprove等)が、
ID管理機能のひとつとして実装されている。
→(Exticの場合)uApprove実装

②IDaaSの個人情報保護規定が、大学の個人情報保護規定と整合性が保たれている。
→(Exticの場合)個人情報保護規定の公開(準備中)

(今後の検討課題)
・ID管理機能のプロビジョニング機能により送出される属性情報の保護方法。