EXGEN NETWORKS

管理と連携の基礎

知らなきゃ損するクラウド時代のID運用
～管理から連携まで～

USE INNOVATIVE TECHNOLOGY.

2016年11月30日

エクスジェン・ネットワークス株式会社
江川淳一

1. システム増殖とID管理

・「認証/認可」と「ID管理」の役割

・アプリケーションに「認証/認可」は何故必要か？

部署や役職に応じた適切な**アクセス権限管理**を行うため。

『アクセス権限管理』
＝『認証/認可のしくみ』＋『新鮮で正しいID情報』

・アプリケーションに「ID管理」は何故必要か？

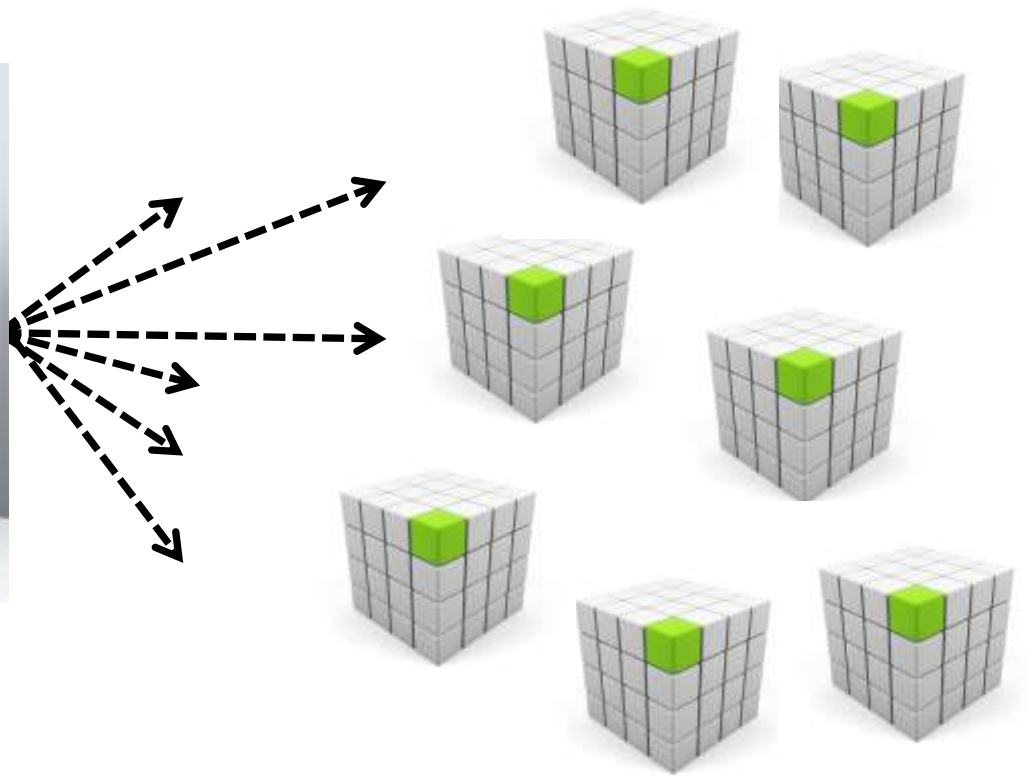
組織変更/人事異動情報を迅速にID情報に反映するため。

1. システム増殖とID管理

・システムの増殖

・組織の中でシステムは増殖するもの。

アプリの中に「認証」のしくみと「ID管理」のしくみが
一緒に存在したまま、システムが増殖すると、、



1. システム増殖とID管理

・**ID情報の鮮度を維持するのが困難に**

・**ID情報に対する組織変更/人事異動情報の反映処理が煩雑になる。**

①人事異動に伴う、アクセス権限の迅速な変更
②退職に伴う、アクセス権限の迅速な無効化・削除
③派遣社員、協力会社社員等の一時利用ユーザの管理

↓

・**部署や役職に応じた適切な**
アクセス権限管理が困難になる。

↓

・**ID運用管理業務の効率化が必要に。**

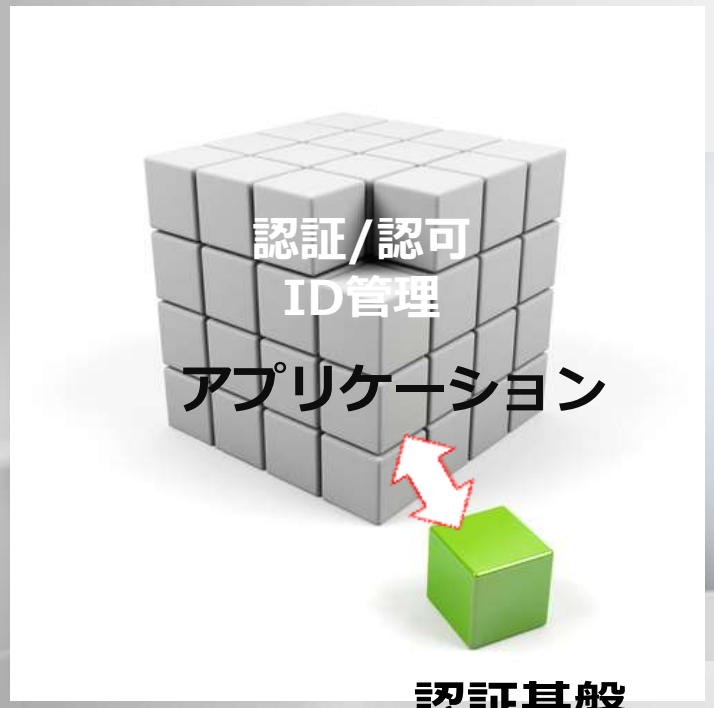
↓

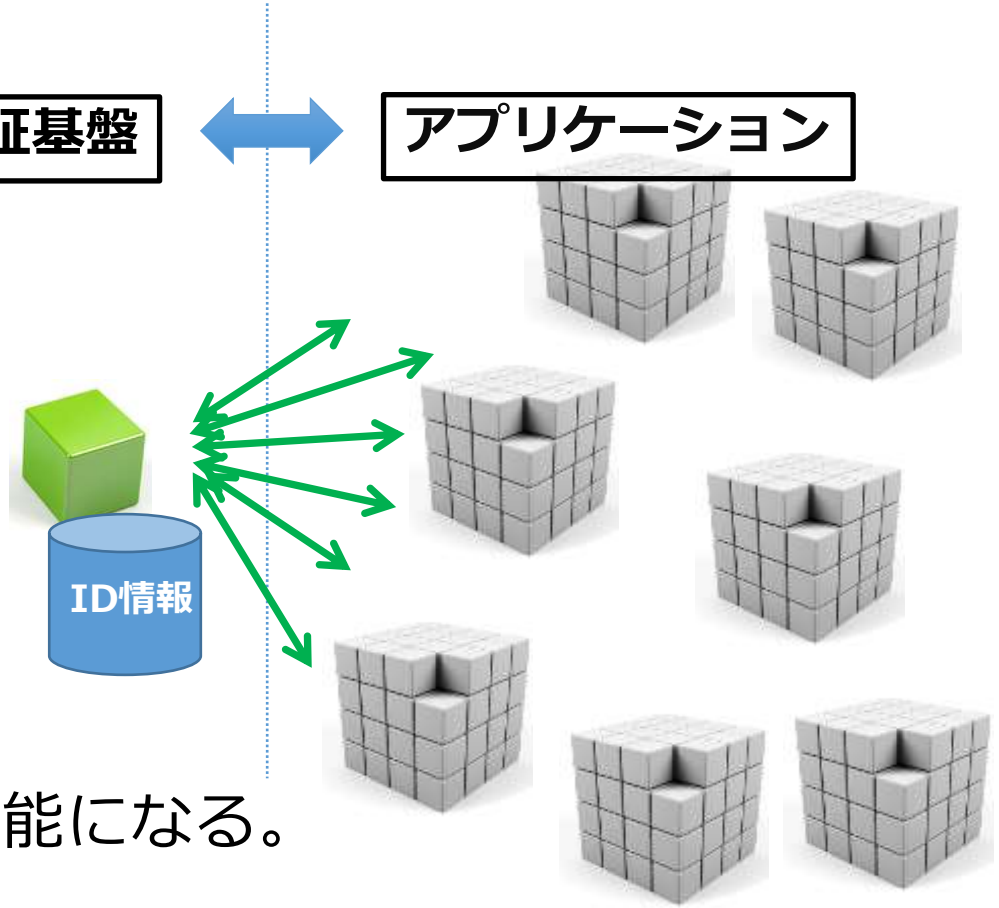
・**認証基盤システムの整備**

1. システム増殖とID管理

・認証基盤システムとは

・「認証」のしくみと「ID管理」のしくみを
認証基盤システムとして、アプリケーションから切り離す。





・「ID情報」の再利用が可能になる。

1. システム増殖とID管理

・認証基盤システムの3要素

基本構成

ID情報マスターDB

ID情報管理システム

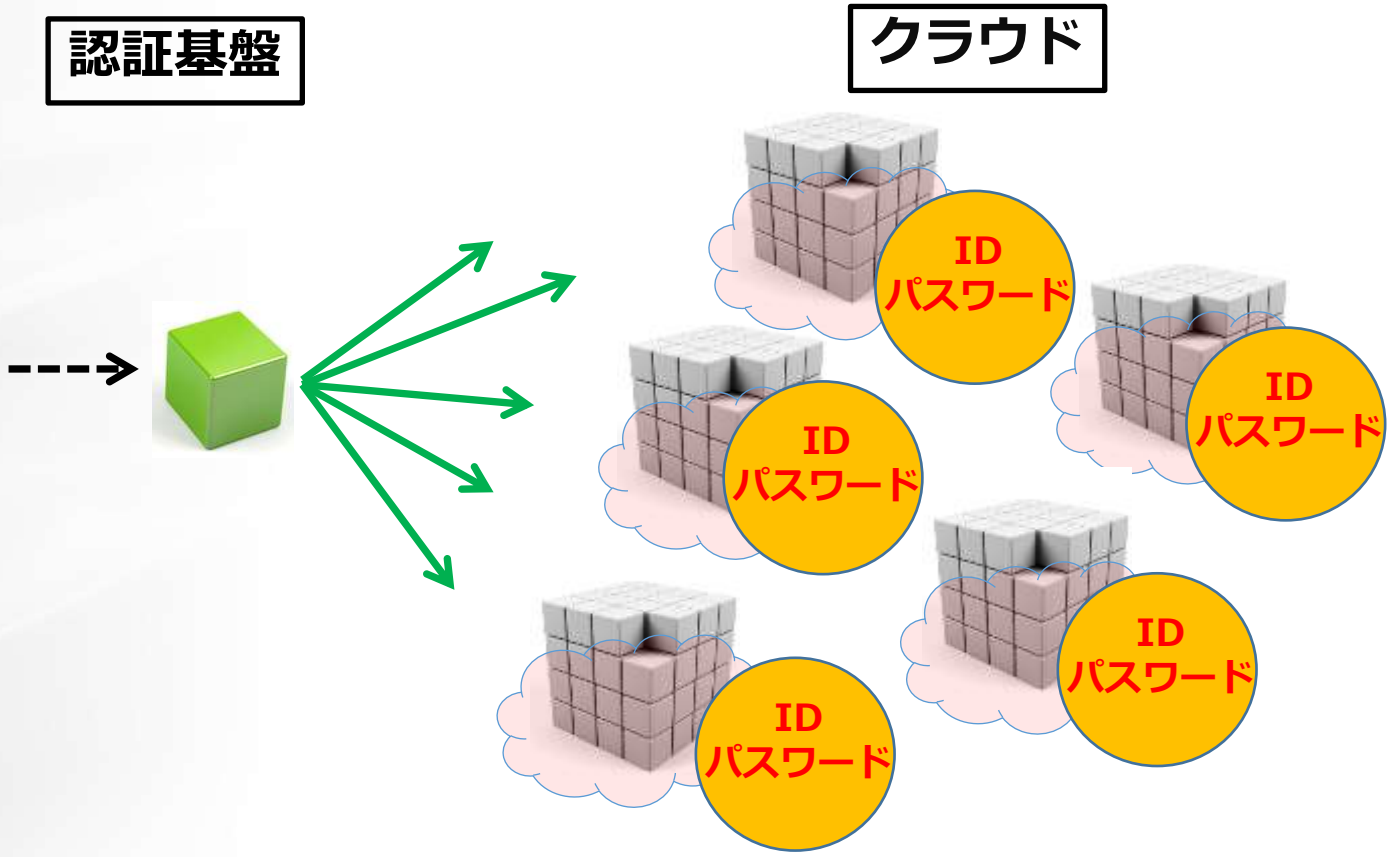
認証システム

2. クラウド増殖とID連携

・クラウドの増殖

・最近は社内システムだけではなくクラウドの利用が増えている。

・ローカル認証方式では、「IDとパスワード」が社外に出て行く。



2. クラウド増殖とID連携

・**IDとパスワードのセットが社外に出ると**

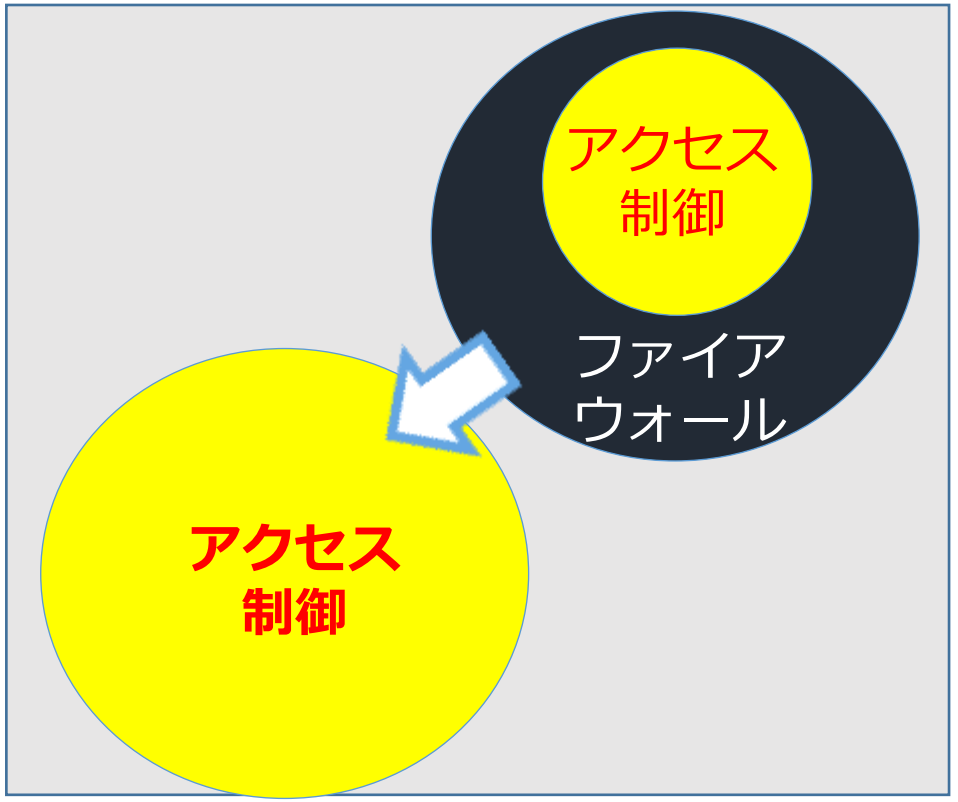
・**セキュリティポリシーコントロールが困難に。**
パスワードポリシーや機密情報のリスクレベルに応じた認証手段の採用が困難になる。

・**ID/パスワードの漏えいリスク。**
セキュリティレベルの低いクラウドから、IDとパスワードのセットが漏えいするリスクがある。

・**IDとパスワードのセット**をクラウド事業者に預けることなく、認証を行いたい。

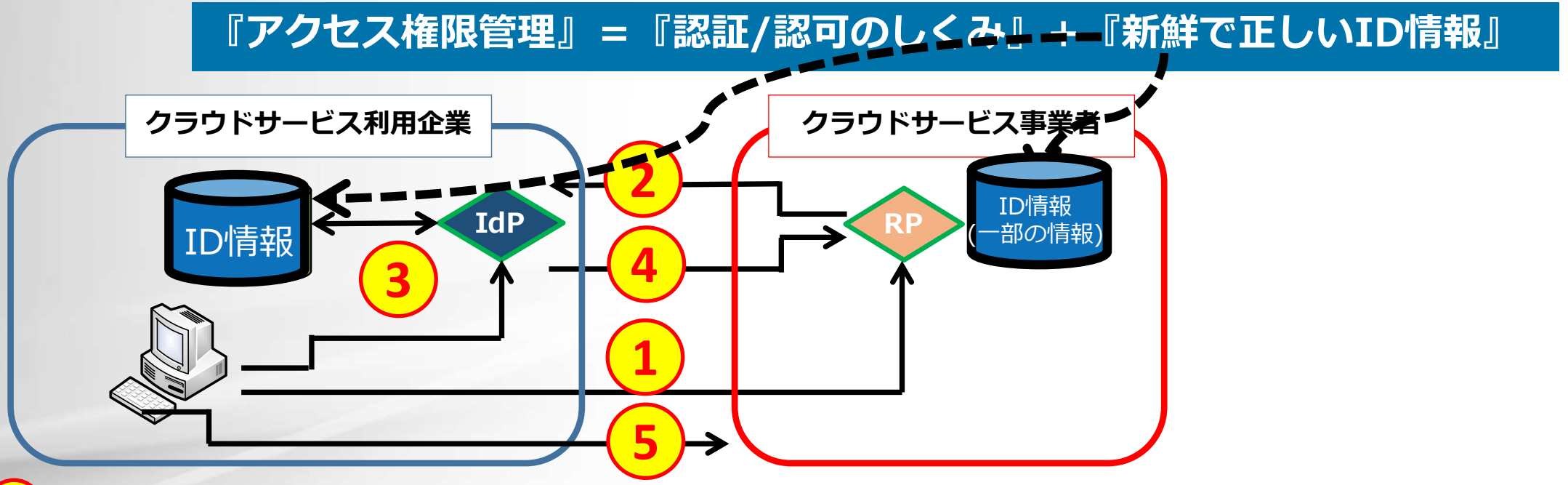
・**フェデレーション技術の認証利用**

Identity is the new Perimeter



2. クラウド増殖とID連携

・フェデレーション技術のエンタープライズ認証利用



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

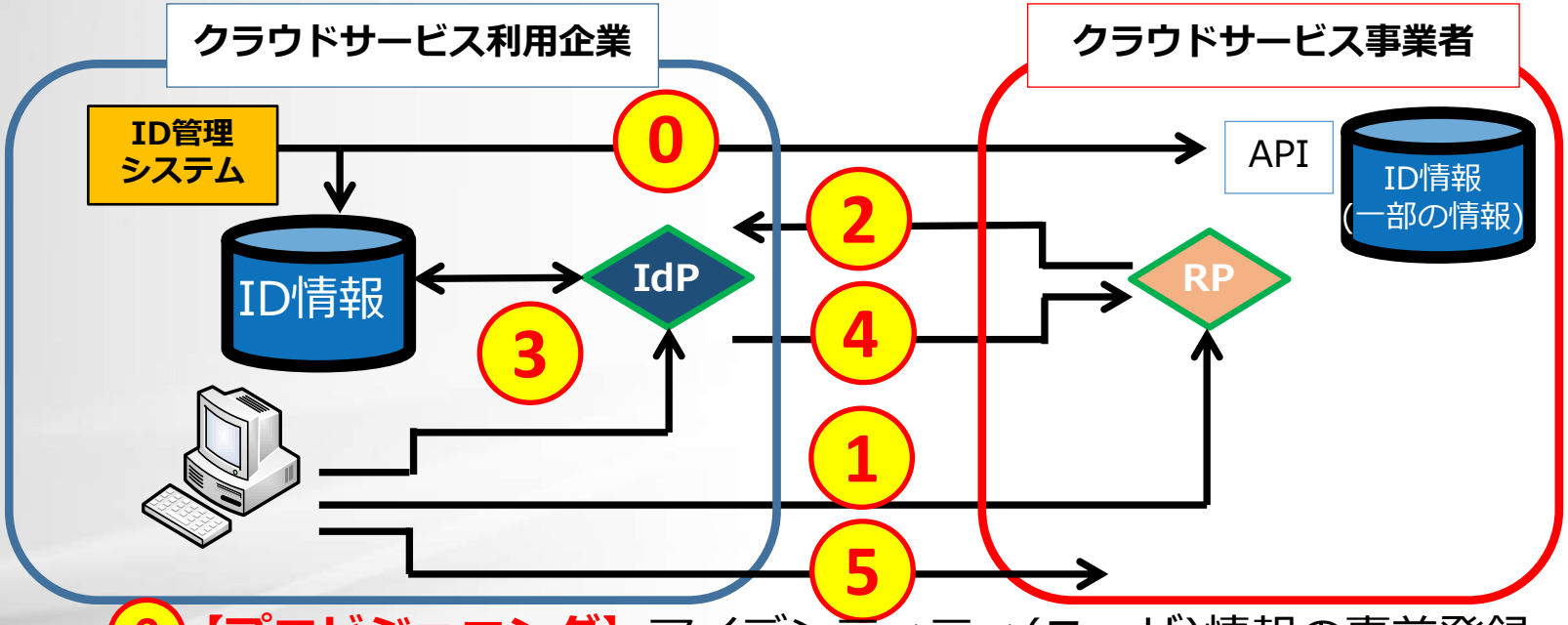
3 **【認証処理】** エンドユーザによる認証処理

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. クラウド増殖とID連携

・フェデレーション技術のエンタープライズ認証利用



0【プロビジョニング】アイデンティティ(ユーザ)情報の事前登録

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

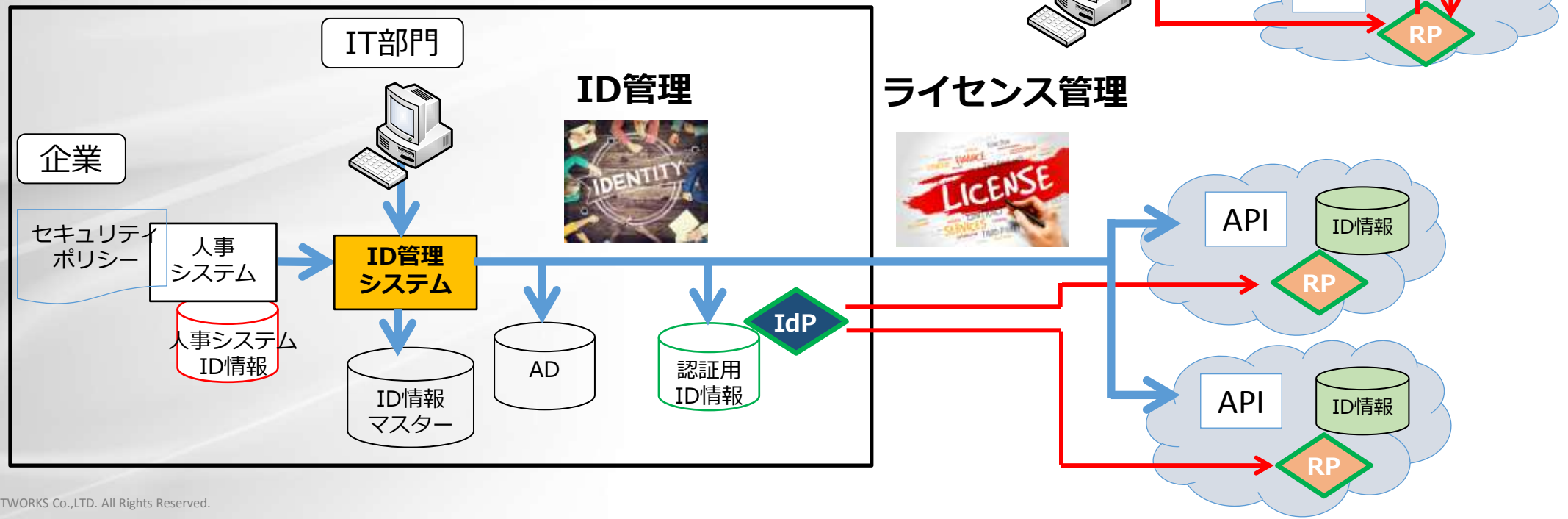
4【IDトークン返却】クラウドサービスへの認証結果の連携

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. クラウド増殖とID連携

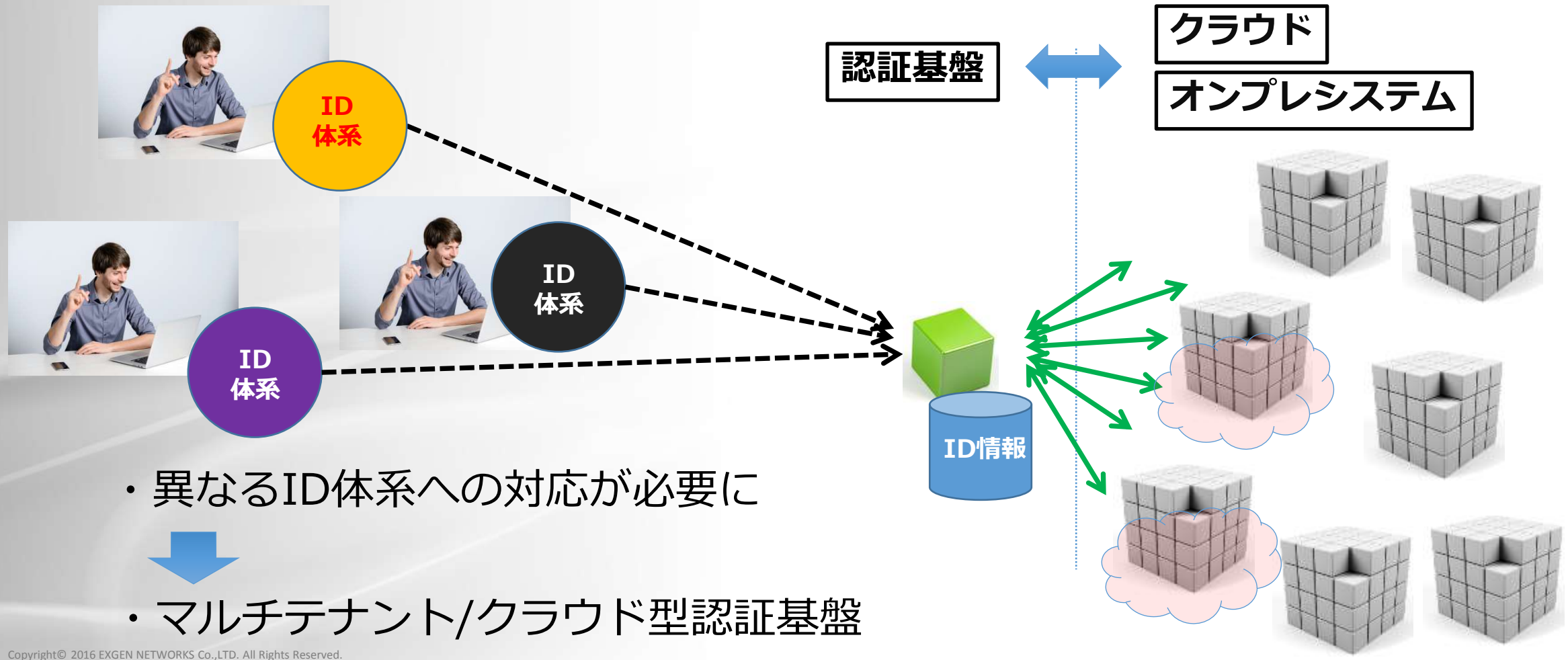
・エンタープライズ市場のID連携はプロビジョニング併用

- 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。
- 営業支援システムやスケジュール共有システムのようにID情報自体が業務アプリのコンテンツとなっている場合が多い。
- IT部門が従業員のID情報をメンテナンスする。(新鮮な状態に保つ。)



3. 組織増殖とIDaaS

- **組織の増殖**
  - グローバル化やM&A等によって組織も増殖。

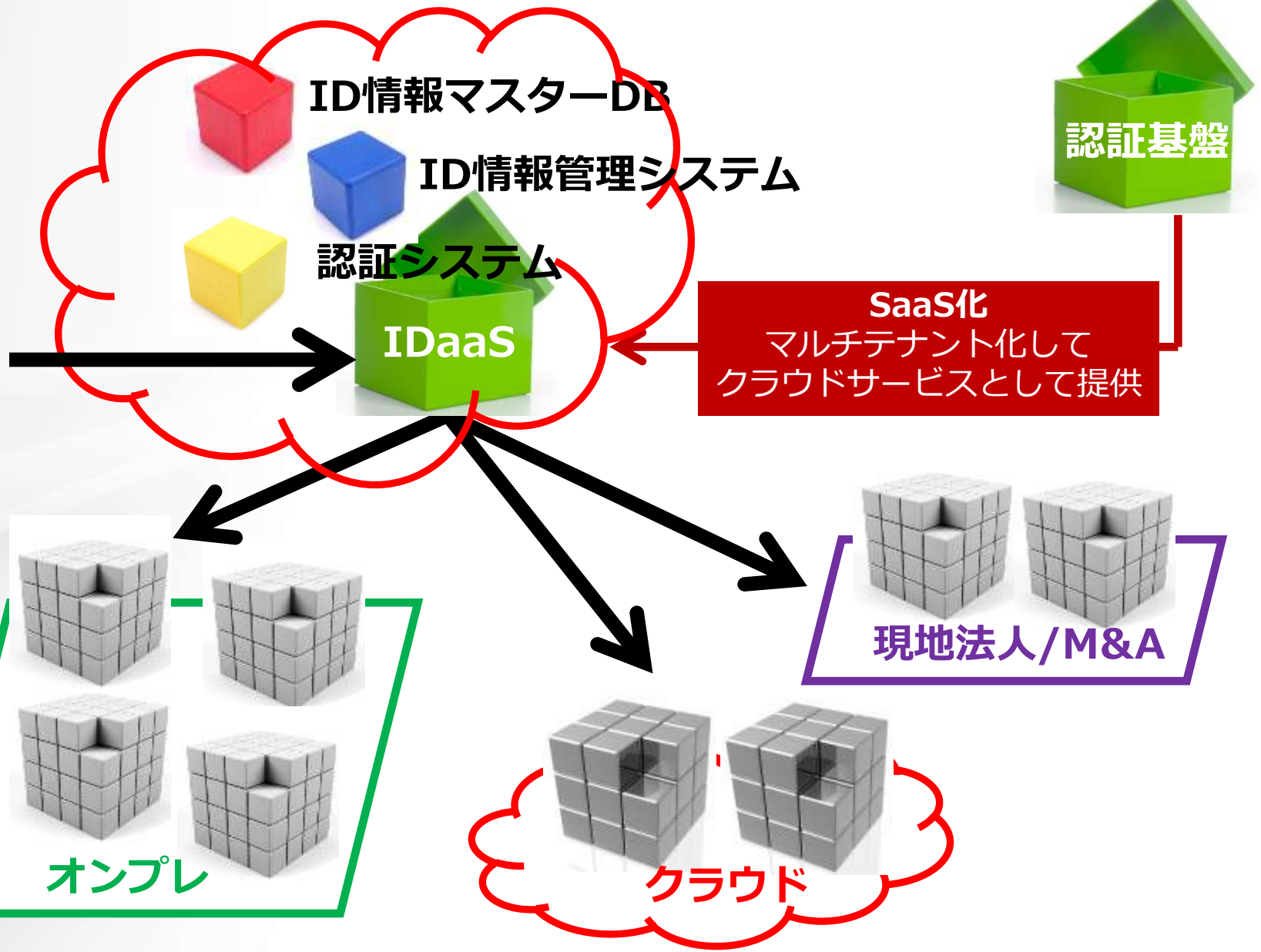


  - 異なるID体系への対応が必要に

  - マルチテナント/クラウド型認証基盤

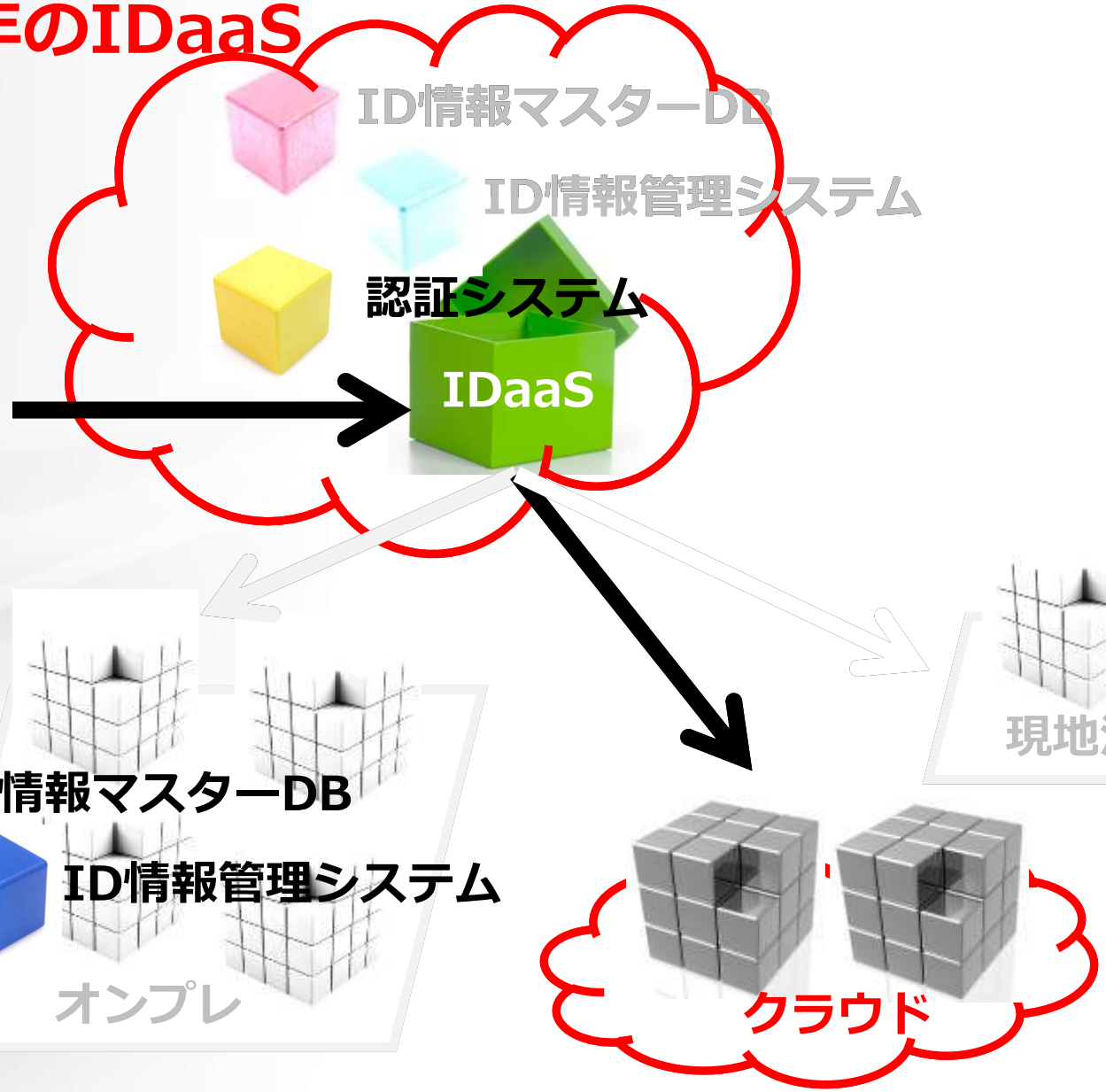
3. 組織増殖とIDaaS

・**IDaaS**



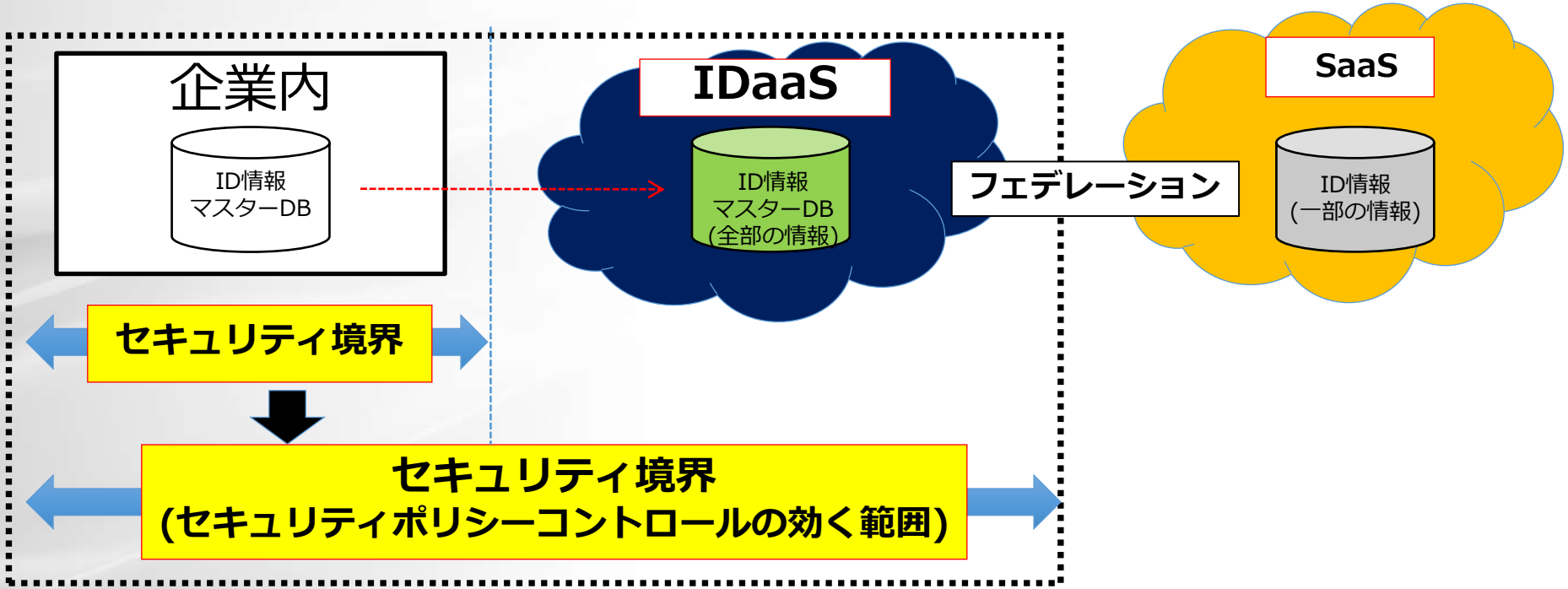
3. 組織増殖とIDaaS

・いわゆる2016年のIDaaS



3. 組織増殖とIDaaS

- **IDaaSのセキュリティ**
  - アクセス制御を行う場所＝IDaaSは安全か
  - 企業にとっては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企業内と**同等もしくはそれ以上**であることが必要。



3. 組織増殖とIDaaS

・IDaaSのセキュリティ

(例) Trusted ID Center eXTIC

統合型セキュリティソリューションを導入し、
24時間/365日体制でのインフラ＆サービス遠隔監視を実施。
これを、基本サービスとして提供。

①統合型セキュリティソリューション

- DeeP Security(トレンドマイクロ社)

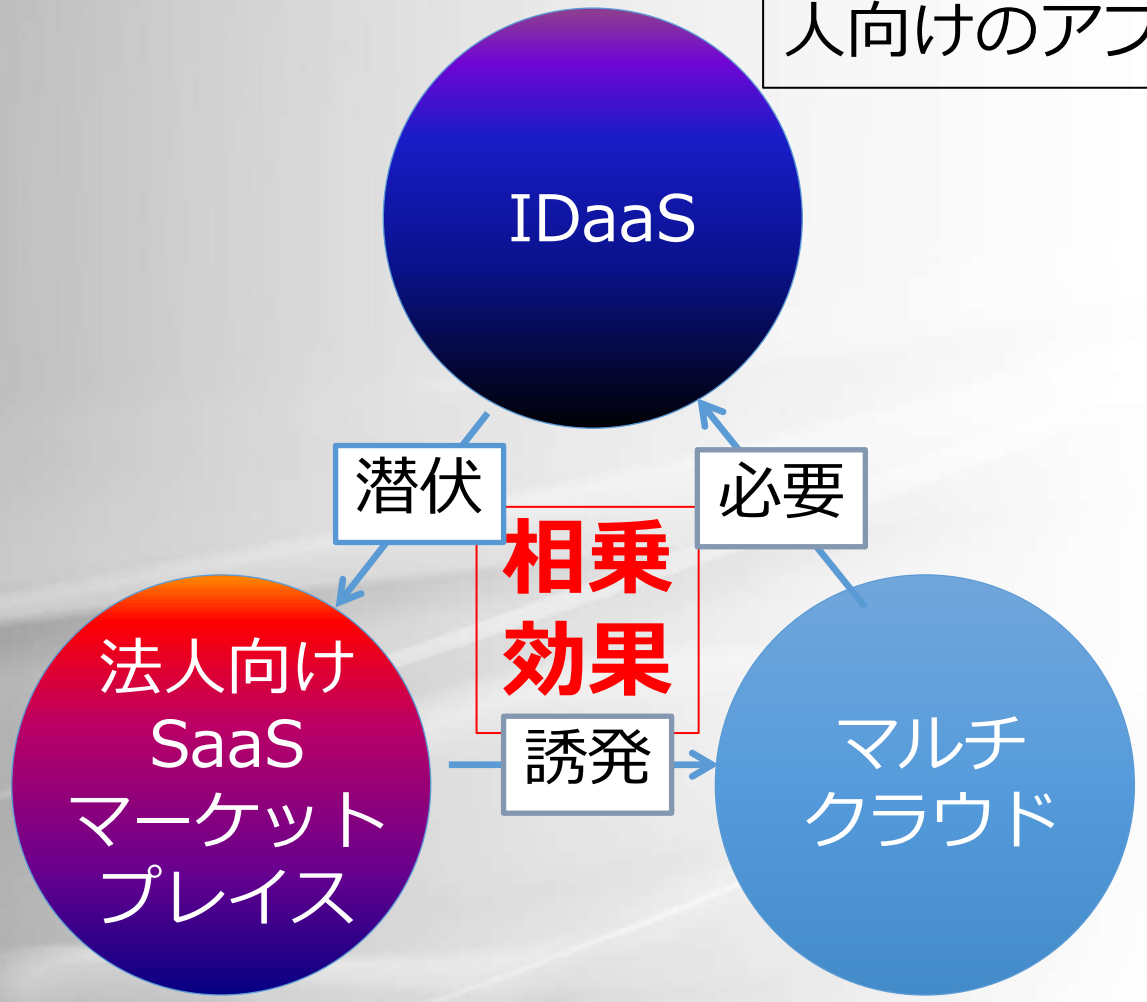
②24時間/365日体制のインフラ ＆ サービス遠隔監視

- PCIDSSに準拠した運用監視を行うセキュリティチームが、日々の脆弱性情報をチェックし、顧客の大切なユーザ情報を安全な状態に保つ。

3. 組織増殖とIDaaS

・**IDaaSの応用**

仕事の業務効率を上げることを目標とした、さまざまなビジネスシーンで利用できる、高品質かつセキュアな法人向けのアプリマーケットプレイス。



4. 様々な増殖と『連携と管理(認証基盤整備)』

・システム増殖、クラウド増殖、組織増殖、、、つまり**変化**。
これらの変化に対してIT部門は、いつでも適切な対応が行えるように準備を整えておくことが必要。
変化そのものに対して迅速かつ柔軟な対応が行えるように、
インフラとしてアクセス制御のしくみをしっかり整備しておくことが極めて重要。

X