クラウド時代の
エンタープライズ認証の要件

コンシューマ向けインターネットサービスのセキュリティ要件と
エンタープライズ向けクラウドサービスのセキュリティ要件の差について

株式会社プロキューブ
中川路　充

本日の主張

- エンタープライズ向けクラウドサービスの認証要件って、コンシューマ向けの認証要件とは違うんじゃない？
- 「クラウド」と言う言葉から連想して、自分が日頃使っているインターネットサービス（ネットバンキング、SNS、ネットゲーム、路線検索・・・）と同じに考えてませんか？

セキュリティトークン

認証方式の安全性？

- パスワードによる認証でも充分安全なのに、運用負荷も、コストも高いICカードやOTPトークンをなぜ使う必要があるのか？
  - 運用負荷：ICカードやOTPトークンは、最初に配布するとき、紛失したとき、忘れてきた人に対する一時貸し出しなどの運用の負荷が高い（パスワードの運用負荷が低いと思うのは実は錯覚だったりするんだけど・・・）
  - コスト：ICカードやOTPトークンは、1個あたり3000円～

事例1:市役所ID乗っ取り事件

- 2013年某月、警察は元上司のIDで某市役所のネットワークに侵入したとして、不正アクセス禁止法違反容疑で、同市の職員を逮捕した。
- 犯人は、2012年2月～2013年6月の1年以上に渡って部局IDや他人のIDで不正接続を繰り返していた。
- 最後に特定の部局IDで、市長宛てに「人事異動でモチベーションが下がった。期待を裏切らない人事をしてほしい」と批判メールが送られため、市長が市役所に調査を依頼し、発覚した。
- パスワードは、IDと同じであったり、誕生日であったりして推測による乗っ取りが可能なものであった。
- この事件のポイントは批判メールが送られるまで、不正アクセスに気がつかなかったことである。

組織としてのセキュリティ要件

エンタープライズ情報システムのIDとパスワードは個人情報を守るためにあるのではなく、組織の情報資産を守るためのもの

↓

誰一人IDが乗っ取られている人はいないことを担保できる必要がある

↓

コピー耐性のあるセキュリティトークンであれば、全員が手元に持っていれば、乗っ取られていないことが保証できる

事例2:キャッシュカードスキャニング事件

- 犯人は、朝、ゴルフ客が貴重品を預けるところを盗撮し、貴重品ロッカーの暗証番号を盗み読みしました。その後、ゴルフ客がゴルフしている間に貴重品ロッカーから財布を抜き出し、キャッシュカードをスキャニングし、何も盗まずに元に戻しました。
- 後日、スキャニングデータからキャッシュカードを偽造し、銀行のATM でお金を引き出しました。暗証番号は貴重品ロッカーと同じもので試してみることにより、かなり高い率で引き出しに成功したと言われています。
- この事件のキーとなるポイントは、犯人がキャッシュカードのスキャニングだけを行い、何も盗まずに財布をロッカーに戻している点です。このことにより、被害者は自分のキャッシュカードが盗まれていることに気がつかず、犯罪が発覚しにくいという特性がありました。

セキュリティトークンのコピー耐性

- 演算能力：セキュリティトークンと通信する際に、秘密情報を交換せず、ハッシュ値などの演算結果を交換することで、秘密情報が抜き取られることを防ぐ
  - これを実現するためにはセキュリティトークンにハッシュ値を計算する演算能力が必要
- 対タンパ性：内蔵されている秘密情報を抜き取ろうとして分解すると、秘密情報が消去される機能

認証方式の秘密情報コピー耐性

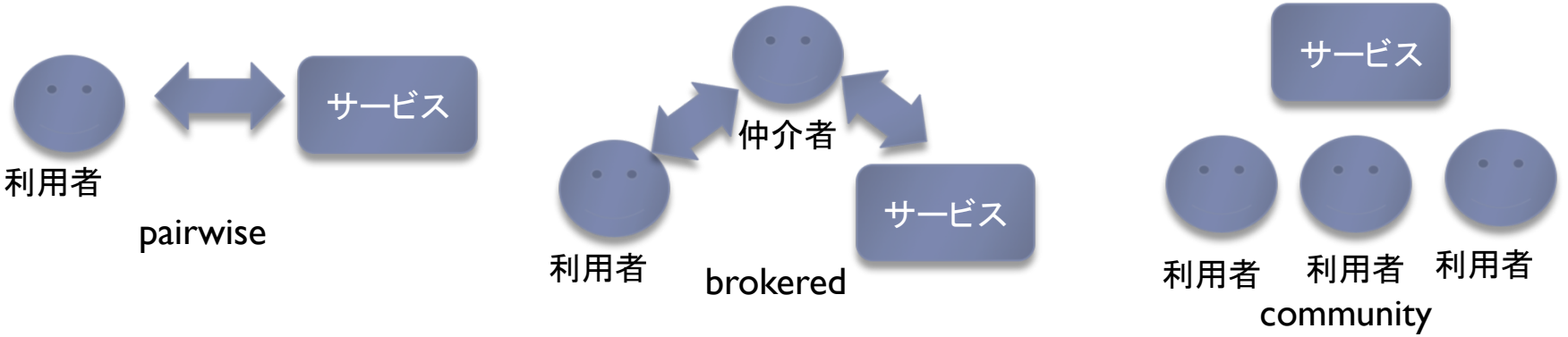
方式	秘密が外に出ない（演算能力がある）	耐タンパ性がある	コピー耐性
パスワード	×	×	×
接触型ICカード	○	○	◎
Felica	△	○	○
生体認証	×	×	×
OTP HW	○	○	◎
OTP SW	○	×	○
ICチップ内蔵USBキー	○	○	◎
暗号化USBキー	×	×	×
イメージマトリックス認証	×	×	×
乱数表	△	×	△
磁気ストライプカード	×	×	×
磁気プリペイドカード	×	×	×

Trust Model

クラウドサービス認証における信頼関係モデル

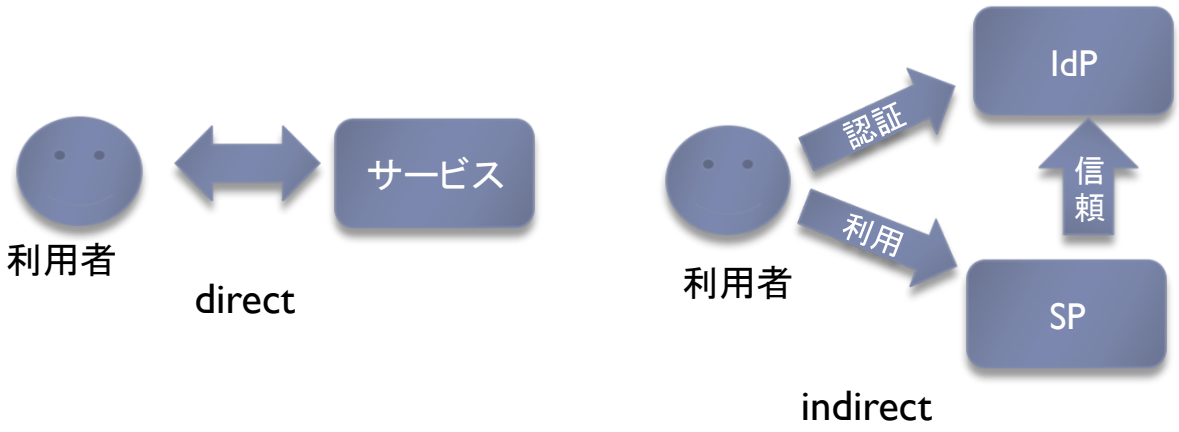
契約関係による信頼関係の分類

関係	説明	例
二者間契約（pairwise）	利用者とサービス提供者の間で直接契約が交わされる形態	インターネットバンキング
仲介契約（brokered）	利用者とサービス提供者の間に仲介者が入り、契約を交わす形態 法人等が契約し、その社員が利用する場合もここに含める	フレッツ（NTT地域IP網） SalesForce，などのビジネス用 SaaS
コミュニティ(community)	契約無く、利用者が無償で提供されるサービスを利用し、その互いの発信内容により、利用者間で信頼関係が構築される形態	Facebook,Twitter, LINE



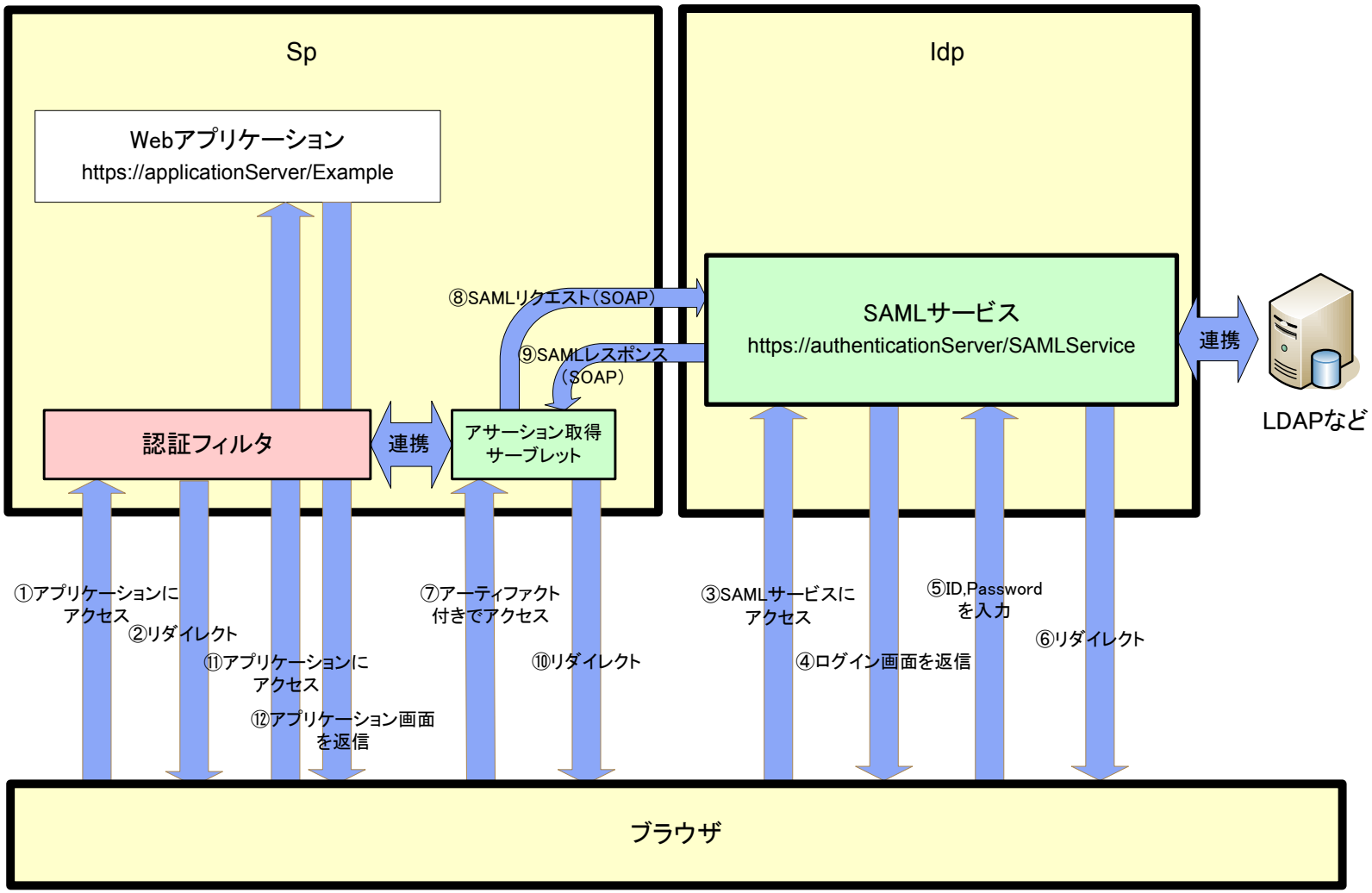
認証技術による信頼関係の分類

関係	説明	例
直接認証（direct）	サービスを提供するシステムが直接利用者の本人確認を行う形態	一般的なWebシステム
間接認証（indirect）	第三者が認証を行い、その証明書をサービス提供者に渡す形式	SAML, Kerberos, PKI



SAMLで indirect 認証

SAML認証手順図



どのような形態が望まれるか？

契約関係	direct	indirect
pairwise （エンタープライズ向けの場合は pairwise はほぼありえない）	一般的	ほとんど例をみない（IdP 提供者のメリットが無い？）
brokered （コンシューマ向けで brokered の例が少ない）	エンタープライズ向けでは現在は主流であるが、indirect に移るべき	SAML+Google Apps, salesForce などの例が出始めており、brokered では理想的なモデル
community （エンタープライズ向けの場合は community はほぼありえない）	一般的	一時、OpenID でシングルサインオンがはやりかけたが、メリットが少ない（SSOだけなら、ブラウザにパスワードを覚えさせても同じ）

エンタープライズ向け indirect のメリット

- IdP 側のメリット
  - A社の IdP は OTP、B社の IdP は IC カードというように、各 IdP の都合で認証方式を決定できる
  - 人事異動の情報を IdP に投入するだけで、クラウド上の全てのシステムに反映される
  - 利用者にシングルサインオン環境を提供できる
- SP 側のメリット
  - パスワード等不要な個人情報を預からなくてすむ
  - ジャストインタイムプロビジョニング＋有効期限切れユーザ削除でユーザ管理機能を省略できる

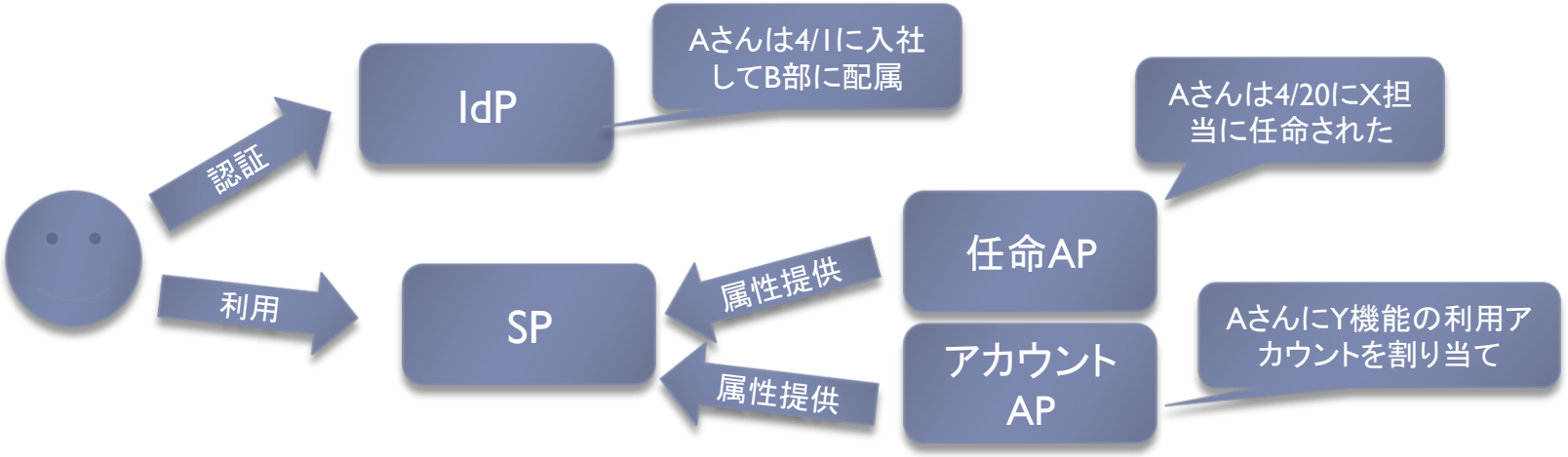
匿名属性認証

匿名属性証明

- 本当はエンタープライズ向けクラウドサービスには個人情報は不要、属性だけ証明できれば良い
  - SAML の Subject ID にはハッシュ値を渡し、クラウドサービスは属性（所属、アプリのアカウントしよう権限の有無、役職など）を参照しながら動作する
- SAML プロトコルでは認証サーバとは別に属性提供サーバ(AP)を立てることが可能
  - ユーザの身元を保証する部門と属性を付与する部門が異なるような場合は、属性だけを提供するサーバを立て、SPのエージェントからそこに問い合わせてもらう

AP(Attribute Provider)

- IdP で認証終了後、SP が AP に対して、SOAP プロトコルで属性を問い合わせる（引数にIdPから受け取ったSAML アサーションの Subject ID を渡す）
- APは自分のデータベースに問い合わせて、属性をSAMLアサーションとして返却
- IdP はユーザの存在や基礎的な属性を管理→人事部門が提供
- SPは役割の任命結果やアカウント保持者を管理→任命権限を持つ部門やシステムアカウントの管理部門が提供

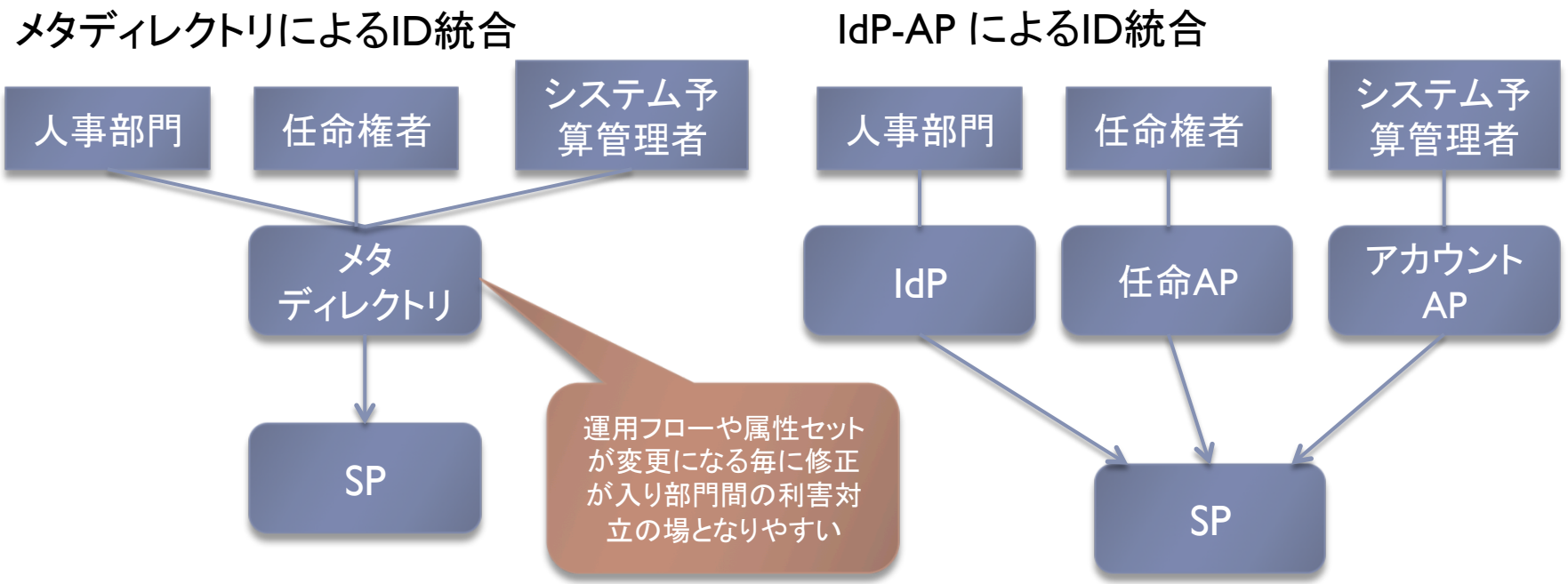


次世代統合認証基盤の構成要素

- JITプロビジョニング：IdPで認証した結果、ユーザが未登録であれば、オンデマンドにユーザを登録する機能
- 有効期限切れユーザの自動削除：オンデマンドに登録したユーザの有効期限が切れた際に自動的にアカウント割り当てを解除する機能
- AP問い合わせ：SP側が必要とする属性をAPに問い合わせる機能

次世代認証基盤ではメタディレクトリ不要

- 統合されたメタディレクトリでは、ユーザの基礎情報をプロビジョニングでSPに配信→JITプロビジョニング（salesforce ならできる）
- 従来のめたディレクトリでは、属性情報を源泉となる部局から収集→SPがAPからオンデマンド取得（できるSPは未出現）
  - って、まだ顧客側もSP側もほど遠いけど・・・Google Apps でもできない



ご清聴ありがとうございました