JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

クラウド時代のアイデンティティ管理

セキュリティにおけるアイデンティティ管理WG
伊藤忠テクノソリューションズ株式会社
富士榮　尚寛

2011 年 1 月 25 日

WG紹介（これまでの活動）

- 「内部統制におけるアイデンティティ管理WG」として2005年度より活動
  - 主にIT全般統制とアイデンティティ管理の関連を討議
- 2008年度より「セキュリティにおけるアイデンティティ管理WG」として活動
  - 内部統制に限らず広くアイデンティティ管理について討議
  - システム化や組織における導入指針、事例のとりまとめ
- 成果物：「内部統制におけるアイデンティティ管理解説書」（現在第2版）
  - アイデンティティ管理の意義
  - IT内部統制におけるアイデンティティ管理の位置づけ
  - アイデンティティ管理システム導入指針
- キーマンズネット
  - 2度と失敗しない「アイデンティティ管理」
  - クラウドとも連携「アイデンティティ管理」
- 2009年度 JNSA賞WGの部

本日の話のスコープ

クラウド　×　アイデンティティ管理

- 利用する側：　提供する側
- 企業や組織：　個人
- セキュリティ：　コスト・効率化

アイデンティティとは

アイデンティティとは？

Entity / Subject（人、コンピュータ 等の「主体」）に関わる様々な属性、好み、形質の集合体

構成要素	解説	例
属性	後天的に取得された主体に関わる情報（後から変化する）	名前、社員番号、電話番号、メールアドレス
好み	主体の嗜好に関わる情報	甘いものが好き
形質	主体の先天的な特有の性質（後から変化しにくい）	生年月日、性別
関係性	他の主体との関係に関わる情報（一部属性と重複）	XX大学卒業、YY部所属

「ID」とは「アイデンティティ」であり、番号や識別子だけを指すのではない

アイデンティティとは

デジタル・アイデンティティとは？

・アイデンティティをデジタル空間に投影したもの
・デジタル空間における「立場・身分」

インターネット・アイデンティティとは？

・デジタル・アイデンティティのうち、インターネット上に生息するもの（Facebook IDとはtwitter IDなど）

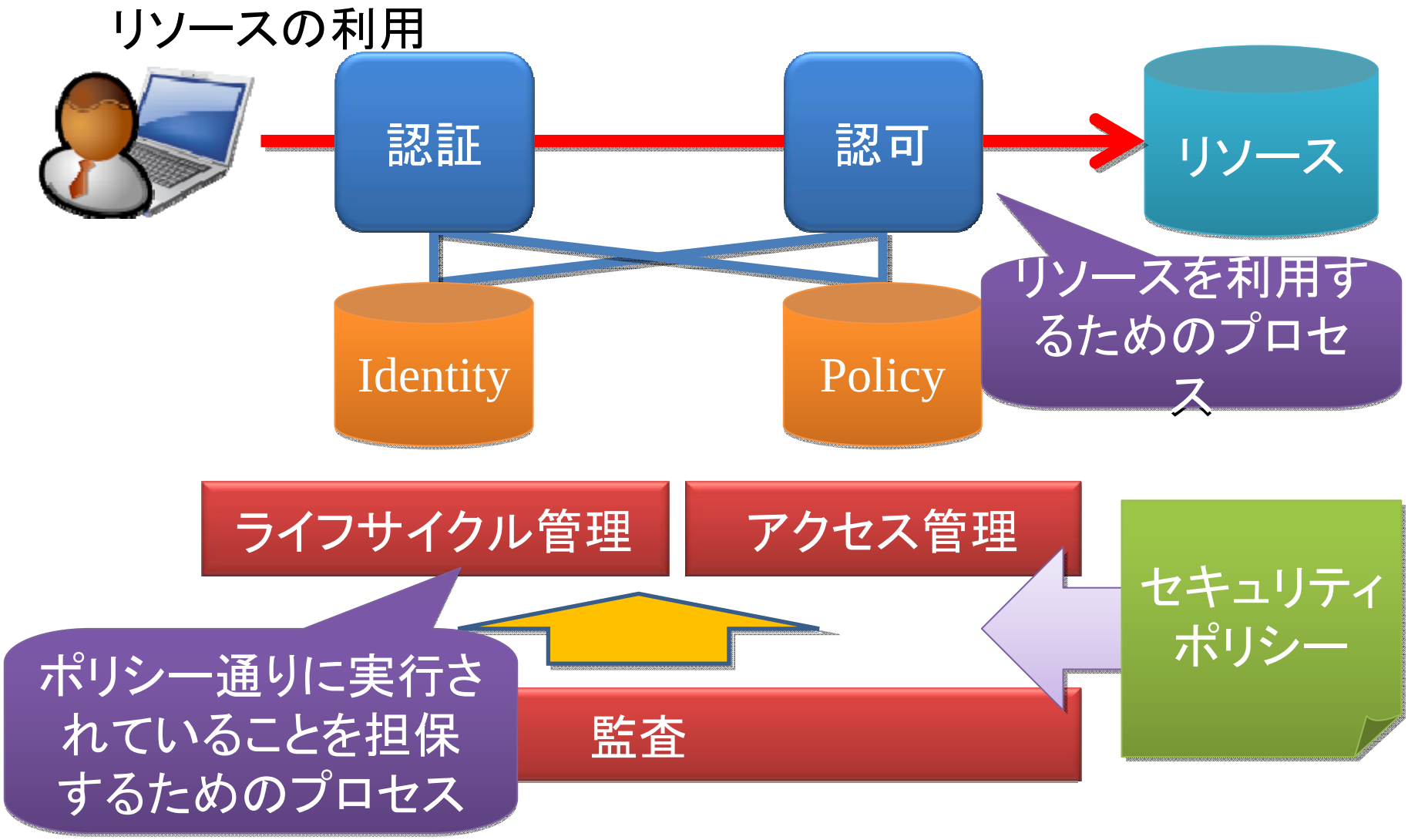
→今回扱うのは、「企業や組織が扱う（管理する）デジタル・アイデンティティ」。クラウドだからと言ってすべてのアイデンティティがインターネット上に引っ越す訳ではない。

アイデンティティ管理とは

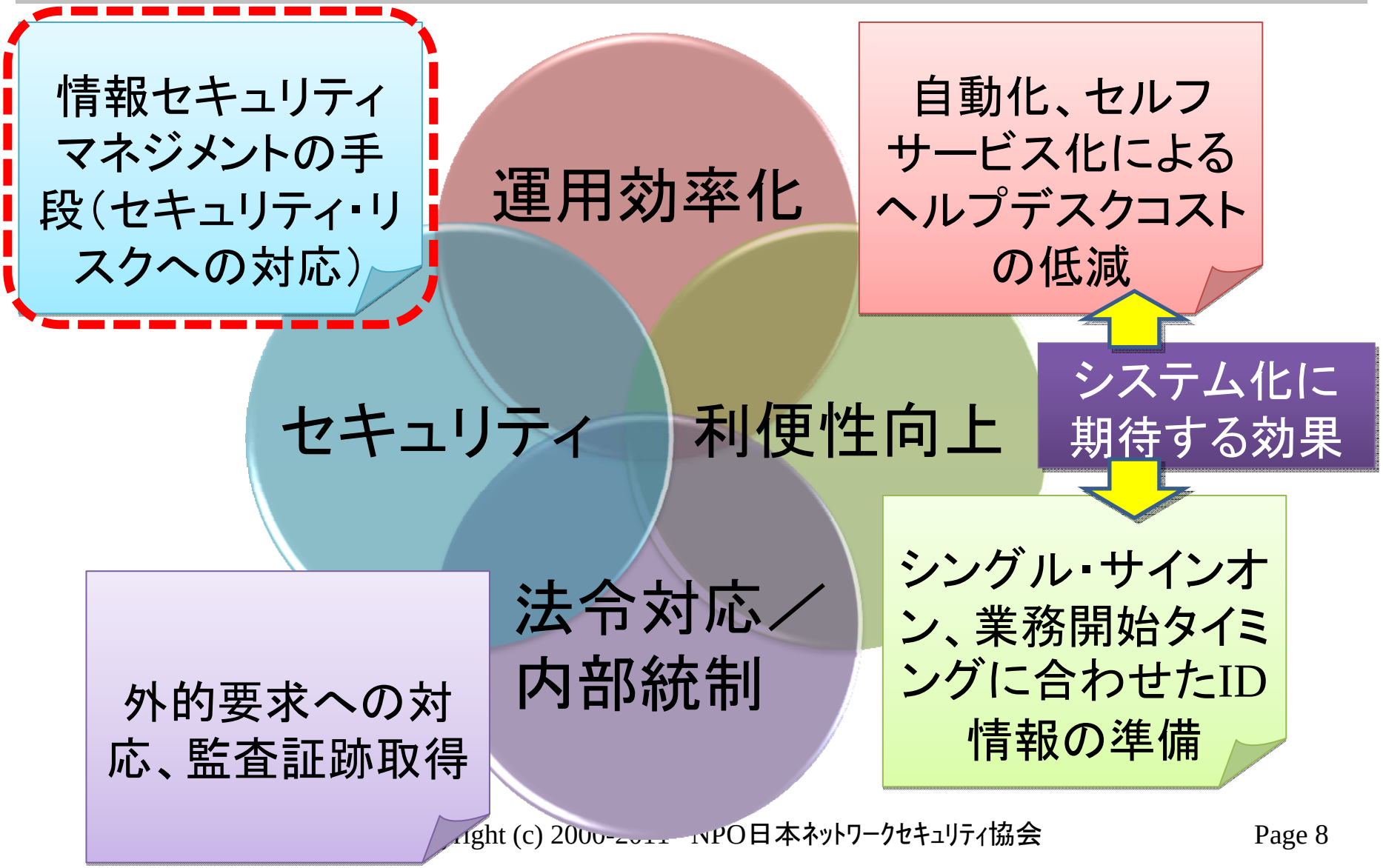
誤解を恐れずに書くと、組織におけるアイデンティティ管理とは
「ユーザが各種リソースを利用するプロセスが組織のセキュリティポリシーやルール通りに実行されていることを担保／保証するためのプロセス（の一部）」

構成要素	解説	関連キーワード
ライフサイクル管理	• いつ、どこに作成し、変更し、削除するか？ • 誰がそれらの変更を承認するのか？	プロビジョニング
アクセス管理	• 利用者とデジタル・アイデンティティをどのように紐付けるのか？ • どのデジタル・アイデンティティにどんなリソースを利用させるのか？	認証（SSO）・認可 ロール・権限管理 フェデレーション
監査	• 適正にデジタル・アイデンティティのライフサイクルやアクセスが管理されていることをどのように証明するのか？	アテステーション

アイデンティティ管理とは



アイデンティティ管理の目的は？



クラウドでは

【ポイント】

•クラウドだから、と言って**情報セキュリティ管理ポリシー・ルールが変わるわけではない**。前提事項や周辺環境が異なるだけである。

•**適切なタイミングで適切なリソースに対してアイデンティティ情報を提供することが引き続き重要**である。そのリソースがクラウド上に存在する可能性がある、というだけである。

•ただし、これまで組織内にクローズされていた為に受容していた**リスクの発生率や影響度合いは変化する可能性**がある。

新たなリスク？

ENISAが2009年11月に公表したリスク評価より

【方針や組織的なリスク】

R.1 Lock-in
R.2 Loss of governance
R.3 Compliance challenges
R.4 Loss of business reputation due to co-tenant activities
R.5 Cloud service termination or failure
R.6 Cloud provider acquisition
R.7 Supply chain failure

【技術的リスク】

R.8 Resource exhaustion (under or over provisioning)
R.9 Isolation failure
R.10 Cloud provider malicious insider – abuse of high privilege roles
R.11 Management interface compromise (manipulation, availability of infrastructure)
R.12 Interception data in transit
R.13 Data leakage on up/download, intra-cloud
R.14 Insecure or ineffective deletion of data
R.15 Distributed denial of service (DDoS)
R.16 Economic denial of service (EDoS)
R.17 Loss of encryption keys
R.18 Undertaking malicious probes or scans
R.19 Compromise service engine
R.20 Conflicts between customer hardening procedures and cloud environment

【法的リスク】

R.21 Subpoena and e-discovery
R.22 Risk from changes of jurisdiction
R.23 Data protection risks
R.24 Licensing risks

【クラウド特有ではないが特に考慮すべきリスク】

R.25 Network breaks
R.26 Network management (ie. Network congestion / mis-connection / non-optimal use)
R.27 Modifying network traffic
R.28 Privilege escalation
R.29 Social engineering attacks (ie. Impersonation)
R.30 Loss or compromise of operational logs
R.31 Loss or compromise of security logs (manipulation of forensic investigation)
R.32 Backups lost, stolen
R.33 Unauthorized access to premises (including physical access to machines and other facilities)
R.34 Theft of computer equipment
R.35 Natural disasters

新たなリスク？

■R.2「ガバナンスの喪失」

•プロビジョニング先リソースへの直接のコントロールを失ってしまうため、SLAや契約形態による事前コントロール、およびリスクが顕在した場合の対応やコンテンジェンシープランなどの事後コントロールの整備が必要

•リスクの転嫁が意味をなさないケースの存在の認識（社会的コストとして跳ね返ってくる場合など）

•標準化されたAPIなどを使ってクラウド上のアイデンティティ・ライフサイクルやアクセス状態を社内からシステム的に管理

■ R.10「クラウド・プロバイダー内部者の特権濫用」

■ R.11「管理者機能の悪用」

■ R.28「権限奪取」

■ R.33「権限無きアクセス」

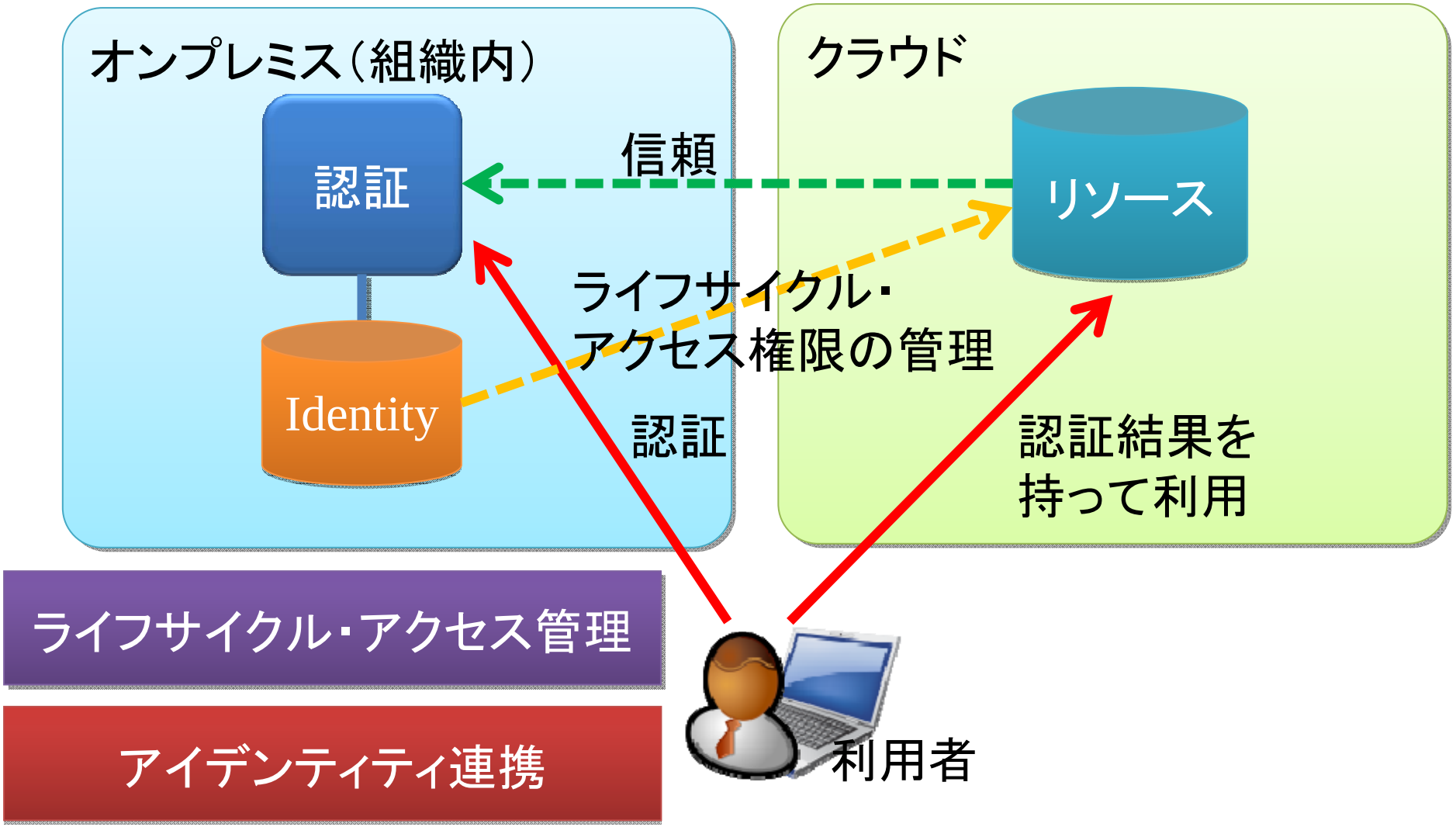
•サービス提供者側の特権管理状況の把握が必要

•アクセス管理機能（認証・認可）の切り離し、オンプレミス連携（アイデンティティ連携）

■ R.21「法令による命令や証拠保全」

•サービス提供者側のポリシーの把握が必要

リスクへの対応の例



まとめ

- 新たなリスクの存在を認識する必要あり
- 引き続き管理は重要（変化の激しい環境下において管理プロセスをいかに維持するか？が大切）
- アイデンティティ連携などで企業内のアイデンティティ管理プロセスを効率的にクラウドへ広げることが可能
- システム的な対応以外についても検討が必要（SLA、コンテンジェンシー等）

今後のWG活動紹介

- 成果物の書籍化（2011年4月予定：インプレスR＆D出版）
  「クラウド環境におけるアイデンティティ管理ガイドブック」（仮）
- WG紹介の英文化
- ロール管理の在り方に関する討議

WGメンバ

WGリーダー　：　日本ビジネスシステムズ株式会社　宮川　晃一

WGメンバ　：

伊藤忠テクノソリューションズ株式会社
富士榮　尚寛、松山 雄一郎
株式会社マインド・トゥー・アクション
中島　浩光
NRIセキュアテクノロジーズ株式会社
山口　雅史
NTTコムウェア株式会社
駒沢 健、前園　暁子、松岡　浩平
株式会社シグマクシス
篠原　信之
東芝ソリューション株式会社
小林 智恵子
日本IBM株式会社
丹羽　奈津子、中本 雅寛
日本IBMシステムズ・エンジニアリング株式会社
酒井美香
日本オラクル株式会社
大森 潤
日本CA株式会社
小坂　嘉誉
日本電気株式会社
桑田 雅彦、竹下 勉、中村 有一
株式会社ネットマークス
高木 経夫、大竹 章裕、栃沢 直樹
富士通関西中部ネットテック株式会社
今堀　秀史、福原　幸一
株式会社富士通ソーシアルサイエンスラボラトリ
恵美　玲央奈
マイクロソフト株式会社
安納　順一
三菱電機株式会社 情報技術総合研究所
原田　篤史
富士通株式会社
岩田　洋一 、佳山こうせつ
株式会社インテック
木村 慎吾
株式会社ディアイティ
鈴木　隆一