JEITA 知識情報処理技術に関するシンポジウム
集めないビッグデータ（2） －個人データの安全な活用に向けて－

OpenID Connectと「同意」にもとづくパーソナルデータ「購読」

2014年４月２４日

株式会社　野村総合研究所
上席研究員　崎村夏彦

Nat Sakimura
Chairman, OpenID Foundation

トップページ >

JEITA 知識情報処理技術に関するシンポジウム

集めないビッグデータ(2) －個人データの安全な活用に向けて－

　個人データの管理における安全性とは、本人に不利益なデータ利用を防ぐということです。これは、(1)データ利用を許可する者(複数可)の認証を厳しくし、(2)本人の利益に即して判断する人を許可者に含め、(3)一度に漏洩するデータを少なくすることにより実現できます((2)は(3)を含意します)。もちろん集中管理((1)のみ)より本人による分散管理((1)+(2)+(3))の方が安全です。
　一方、個人データの管理における利便性には、個人的利便性(B2Cサービスの本来の価値)と社会的利便性があります。前者は本人に役立つことで、後者は本人を含むとは限らない多くの人々の役に立つことです。
　安全性と個人的利便性を高めるには本人が常に関わる仕方で個人データを管理するのが望ましいわけですが、データ利用の可否を本人がすべて直接判断するのは煩雑でしょうし、また社会的利便性を高めるにも、データ利用の許可にいちいち本人が直接関わらない方が良いかも知れません。本シンポジウムでは、安全性と利便性をバランス良く両立させながら個人データを活用する方法について、技術や制度などの観点から議論します。

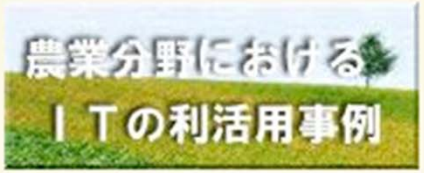
■ 日 時　２０１４年4月２４日（木）１０：００～１７：００

■ 場 所　東京大学山上会館 大会議室
　　http://www.u-tokyo.ac.jp/campusmap/cam01_00_02_j.html

■ 主 催　一般社団法人電子情報技術産業協会　知識情報処理技術専門委員会

■ 定 員　１００名（定員になりしだい締め切らせて頂きます。）

■ 聴講料　無料



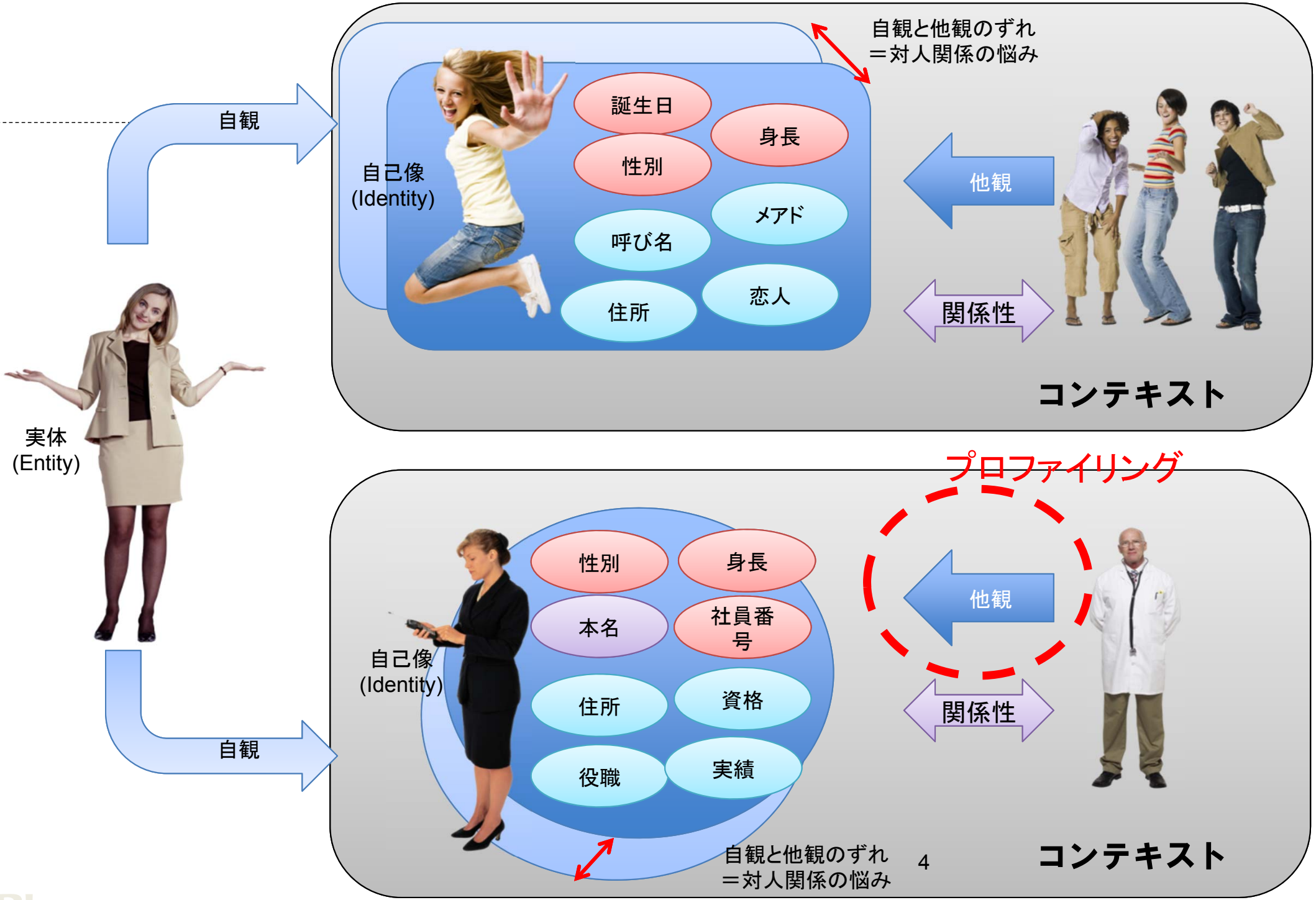
個人データの管理における安全性とは、本人に不利益なデータ利用を防ぐということです。これは、(1)データ利用を許可する者(複数可)の認証を厳しくし、(2)本人の利益に即して判断する人を許可者に含め、(3)一度に漏洩するデータを少なくすることにより実現できます((2)は(3)を含意します)。もちろん集中管理((1)のみ)より本人による分散管理((1)+(2)+(3))の方が安全です。

一方、個人データの管理における利便性には、個人的利便性(B2Cサービスの本来の価値)と社会的利便性があります。前者は本人に役立つことで、後者は本人を含むとは限らない多くの人々の役に立つことです。

安全性と個人的利便性を高めるには本人が常に関わる仕方で個人データを管理するのが望ましいわけですが、データ利用の可否を本人がすべて直接判断するのは煩雑でしょうし、また社会的利便性を高めるにも、データ利用の許可にいちいち本人が直接関わらない方が良いかも知れません。本シンポジウムでは、安全性と利便性をバランス良く両立させながら個人データを活用する方法について、技術や制度などの観点から議論します。

（出所）JEITA 知識情報処理技術に関するシンポジウム 集めないビッグデータ(2) －個人データの安全な活用に向けて－
http://home.jeita.or.jp/cgi-bin/page/detail.cgi?n=668&ca=1

プライバシーの尊重

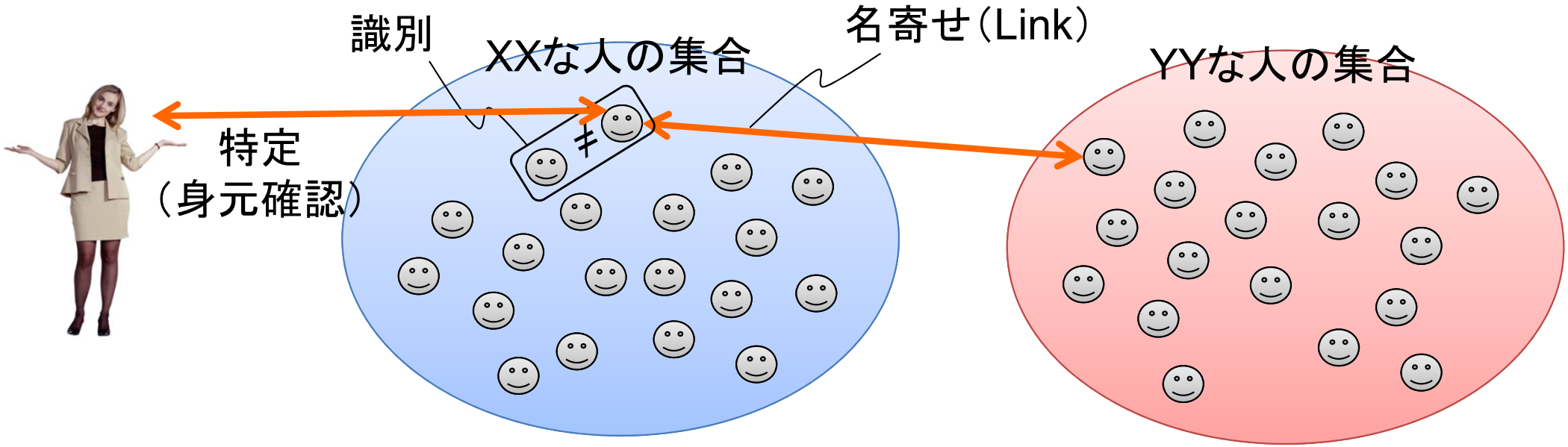


昨今よく取り上げられる「コントロール」

■ 名寄せ不能化 →

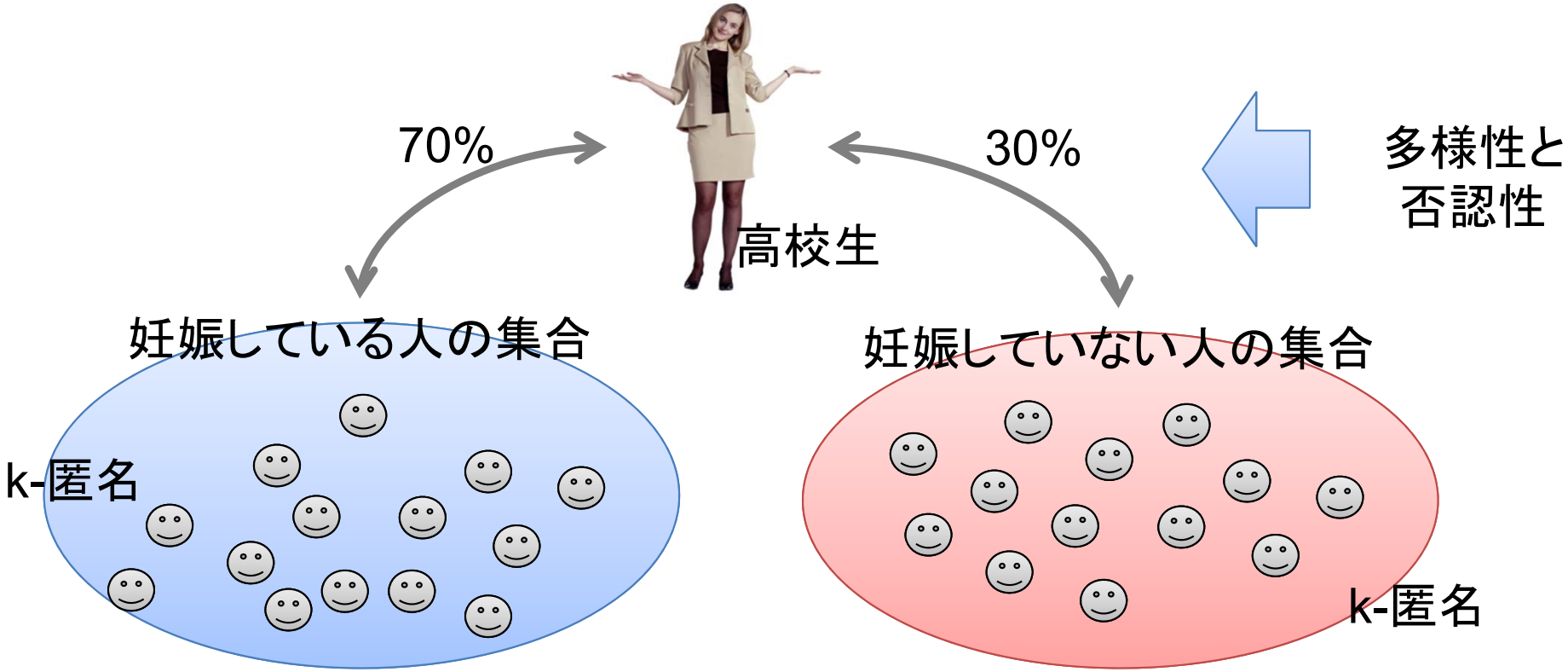
- 相手先別仮名化(PPID)
- 非特定化
- 非識別化

名寄せが出来なければ、
複数の属性をくっつけて
新たな「像」をつくることが
難しくなる。



非識別化は十分ではない

- しかし、高い確率でXXな人の集合に入っているとわかれば、相変わらず差別されたり、自己イメージが崩れるなど被害をこうむり得る。
- したがって、「非識別化」しても、相変わらずプライバシー侵害は起きる。



データの種類を制御するのではなく、行為を制御しなければならない。

行為に対するガイドラインとして、
いわゆる「プライバシー原則」がかかげられてきた

OECD8原則

1. 目的明確化の原則
2. 利用制限の原則
3. 収集制限の原則
4. データ内容の原則
5. 安全保護の原則
6. 公開の原則
7. 個人参加の原則
8. 責任の原則

EU指令　公正情報処理規定

1. 公正かつ適法な処理
2. 目的明確化
3. 適切なデータ
4. 正確なデータ
5. 個人の参加とアクセス
6. 必要期間のみ
7. 監督機関の設置とデータ管理者の公開

ISO/IEC 29100 プライバシー原則

1. 同意と選択
2. 目的の正当性と規定
3. 収集の制限
4. データ最小化
5. 利用、保持、開示の制限
6. 正確性と品質
7. オープンさ、透明性、通知
8. 個人の参加とアクセス
9. 説明責任
10. 情報セキュリティ
11. プライバシー法令遵守

ISO/IEC 29100:2011のプライバシー原則概観

原則	解説
1. 同意と選択	意味ある同意を得なさい →明示的な同意とは限らない。きちんと「理解」を得ることが重要。 文脈に沿うようにし、予想外のことをおこさない。同意した場合、同意しなかった場合に「どのようなことが起きるか」を伝える。「同意する」以外の選択肢を提供する
2. 目的の正当性と規定	利用目的が正当でなければならない。詳しく規定されなければならない。 新たな用途を追加するときには、都度、同意を得ること。
3. 収集の制限	必要最低限のデータしか求めてはならない。
4. データ最小化	収集したデータは、必要最低限の処理しかしない。同データには、必要最低限の人しか触らないようにする。（→　望まない自己像の生成などを防ぐ。）
5. 利用、保持、開示の制限	必要最低限の期間しか保持してはならない。 利用目的が達せられた後、法的要件などで保持する必要が有る場合には、そのデータをロックしてアクセスできないようにする。 データの開示は利用目的を達するのに必要最低限のものにしなければならない

（出所）ISO/IEC 29100 をもとにNRI作成

原則	解説
6. 正確性と品質	データが正確でないと、その人にとって不利なイメージが形成されてしまう恐れがあるので、データの品質を確保しなければならない。
7. オープンさ、透明性、通知	パーソナルデータを処理する主体のポリシー、処理したということ、ポリシーの変更、処理をやめさせる方法などを個人に対してきちんと伝える。
8. 個人の参加とアクセス	各社がどのようなデータを保持しているかなどを見て、必要に応じて修正を行うことができること。
9. 説明責任	情報の取り扱いについての説明責任を確保すること。
10. 情報セキュリティ	取得したパーソナルデータは安全に管理すること。
11. プライバシー法令遵守	関連法令を遵守しなさい。個人情報保護法だけでなく、様々な関連法規を含むことに留意する必要あり。

（出所）ISO/IEC 29100 をもとにNRI作成

苦節４年半...2014/2/26

■ OpenID Connect をリリースしました。

インターネットのアイデンティティ層

1. データ利用を許可するものを認証を厳しくし、
2. （錯誤による同意を減らすために）本人の利益に則して判断する人を許可者に含め、
3. 一度に漏洩するデータを少なくする

プライバシーに配慮したパーソナルデータ連携を行うためには

1. データ利用を許可するものを認証を厳しくし、
2. （錯誤による同意を減らすために）本人の利益に則して判断する人を許可者に含め、
   a. データ利用をするものを認証し、
   b. そのデータ利用者がプライバシー原則の遵守をコミットしていることを確認し、
   c. 必要ならば本人の明示的同意を取得する
3. 一度に漏洩するデータを少なくする
   a. 最低限のデータ取得
   b. 最低限のデータ保持
   c. 分散データ
4. いつでもデータ提供・利用を停止することができるように同意と許可の管理を行う

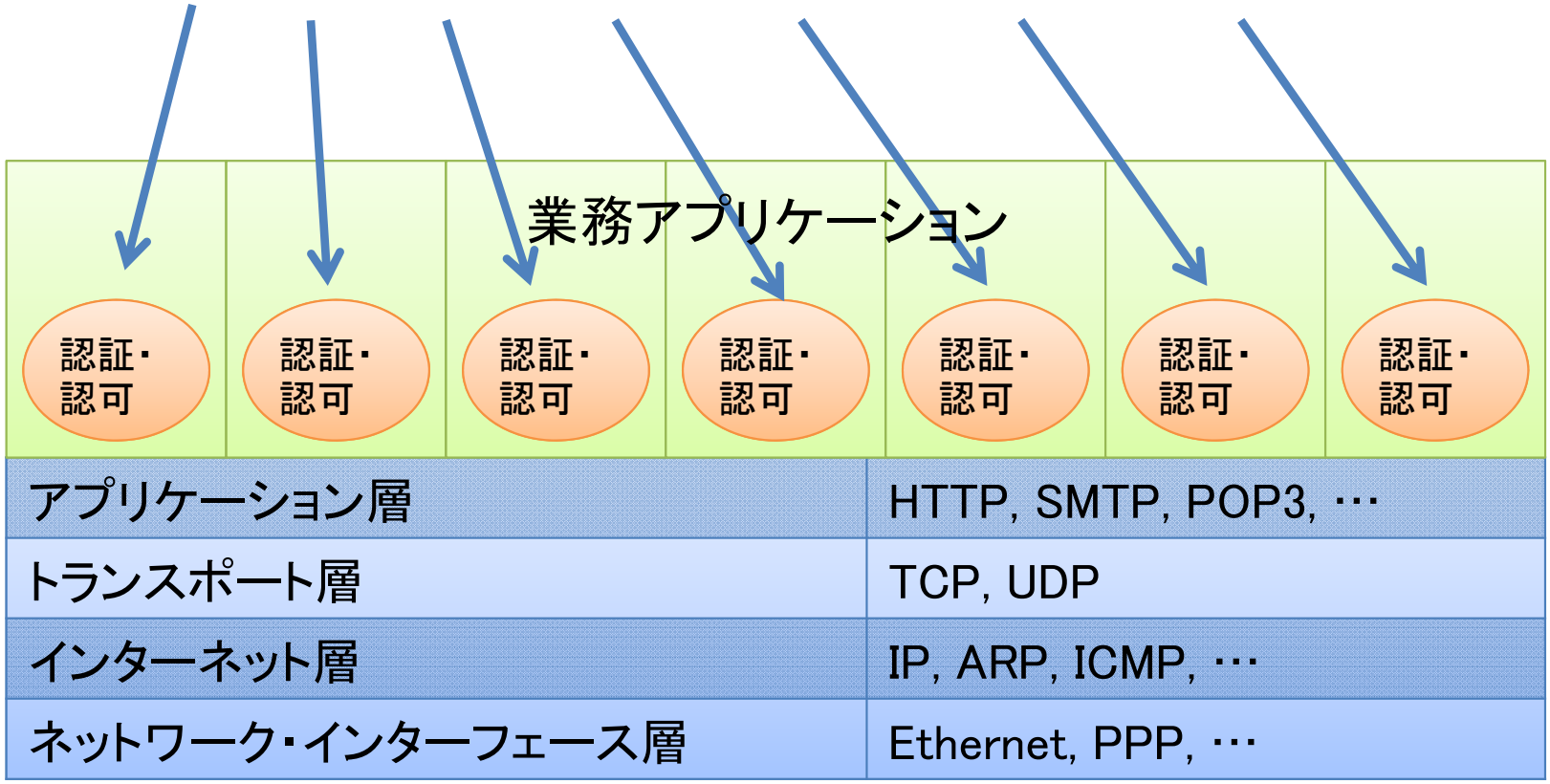
インターネットのアイデンティティ層？

TCP/IP参照モデル

アプリケーション層	HTTP, SMTP, POP3, …
トランスポート層	TCP, UDP
インターネット層	IP, ARP, ICMP, …
ネットワーク・インターフェース層	Ethernet, PPP, …

業務アプリケーション

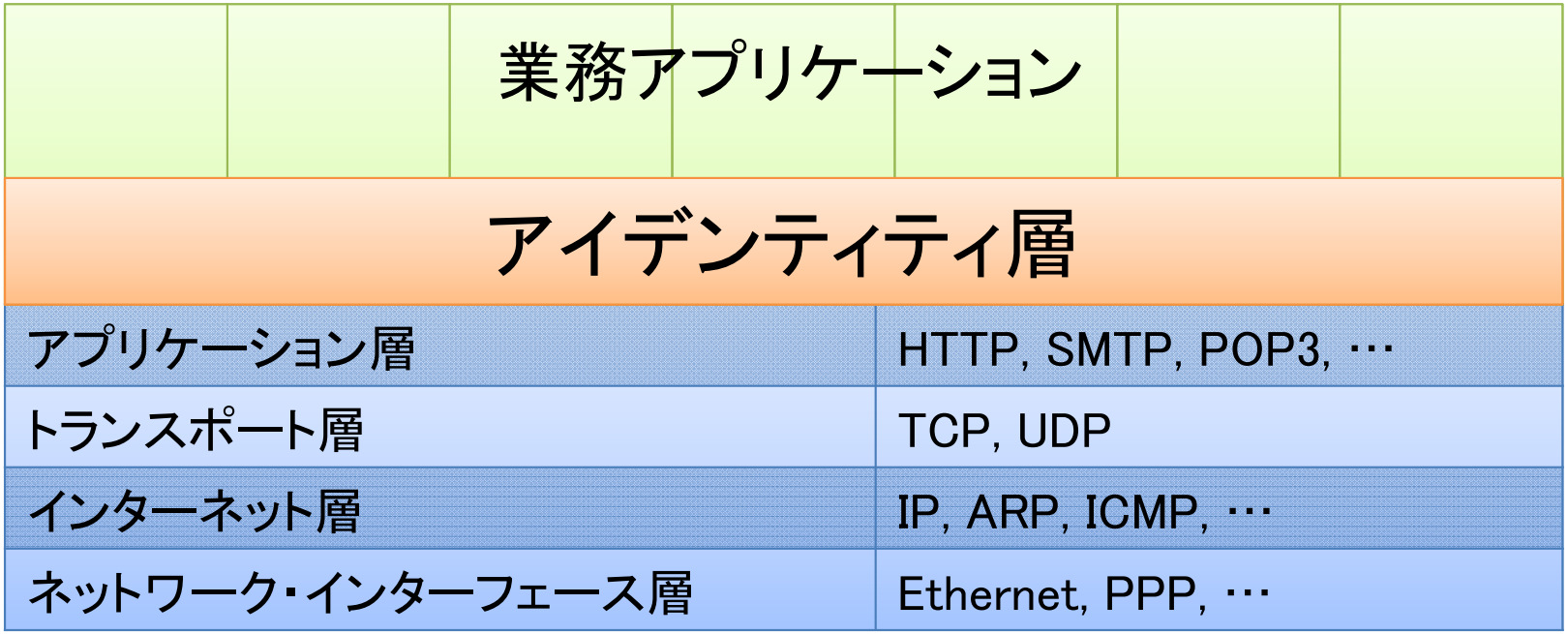
インターネット上でのセキュリティの問題の95%以上が、この「認証・認可」がヘボなことに由来



アンチ・ウイルスの父：ピーター・ティペット

セキュリティを強化するという観点では、アンチウイルスやらファイヤーウォールやら他の全てのセキュリティ機能を完璧にしたとしても、アイデンティティ機能をちょっとだけ進化させるので得られる利益に遠く及ばない

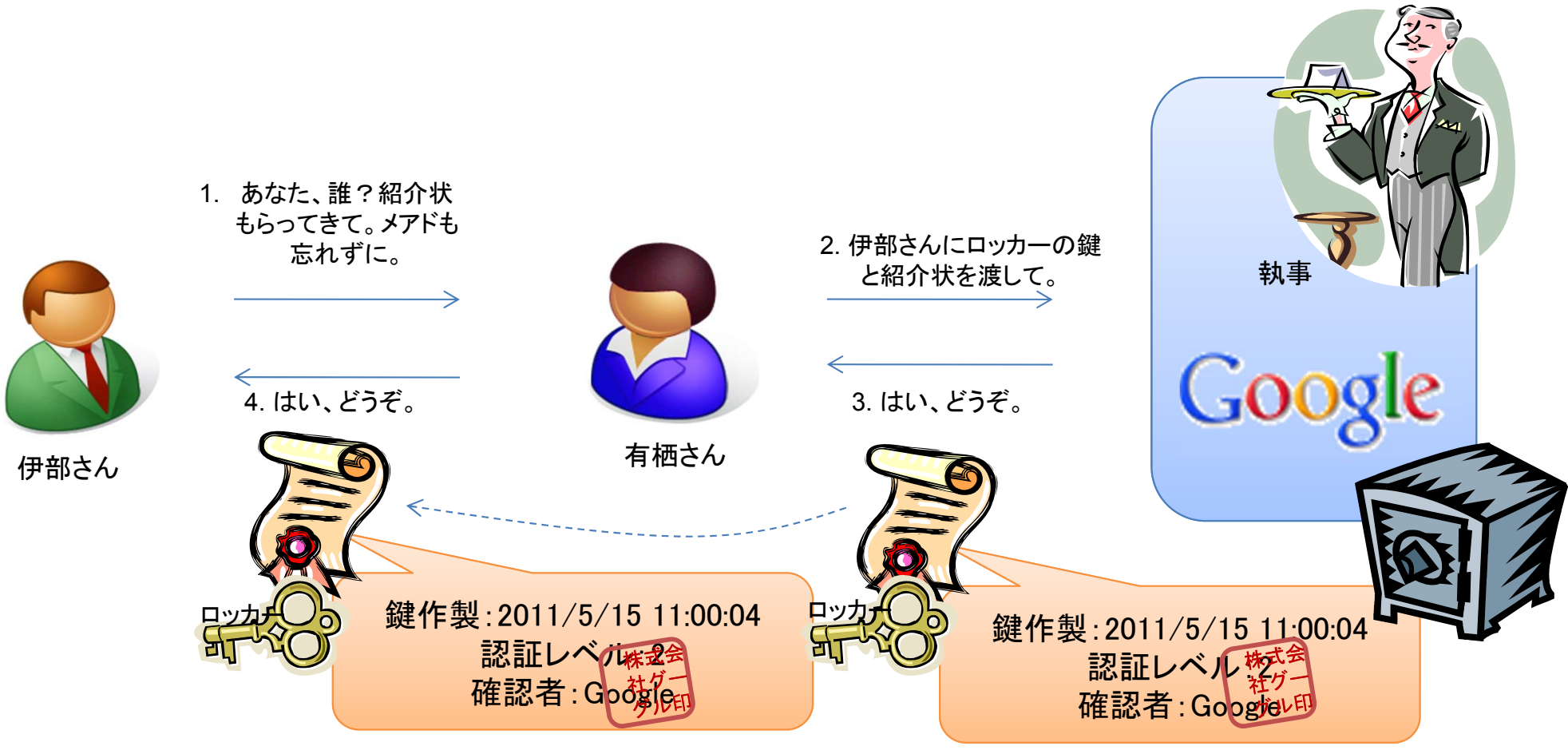
アイデンティティ層への外出し



認証・認可・同意管理・アイデンティティ（＝属性の集合）提供

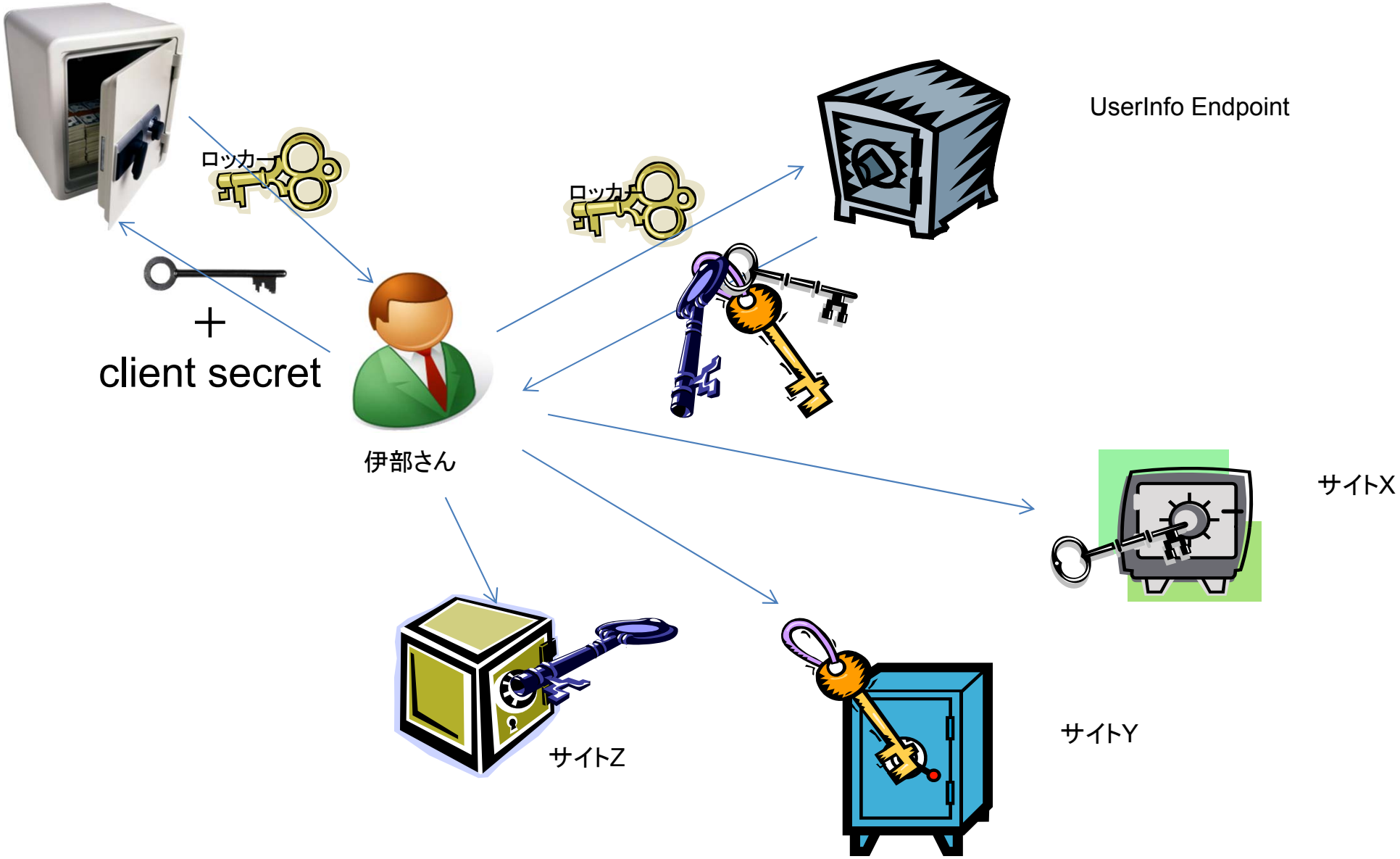
OpenID Connectってどんなもの？

「鍵」と「紹介状」の取得

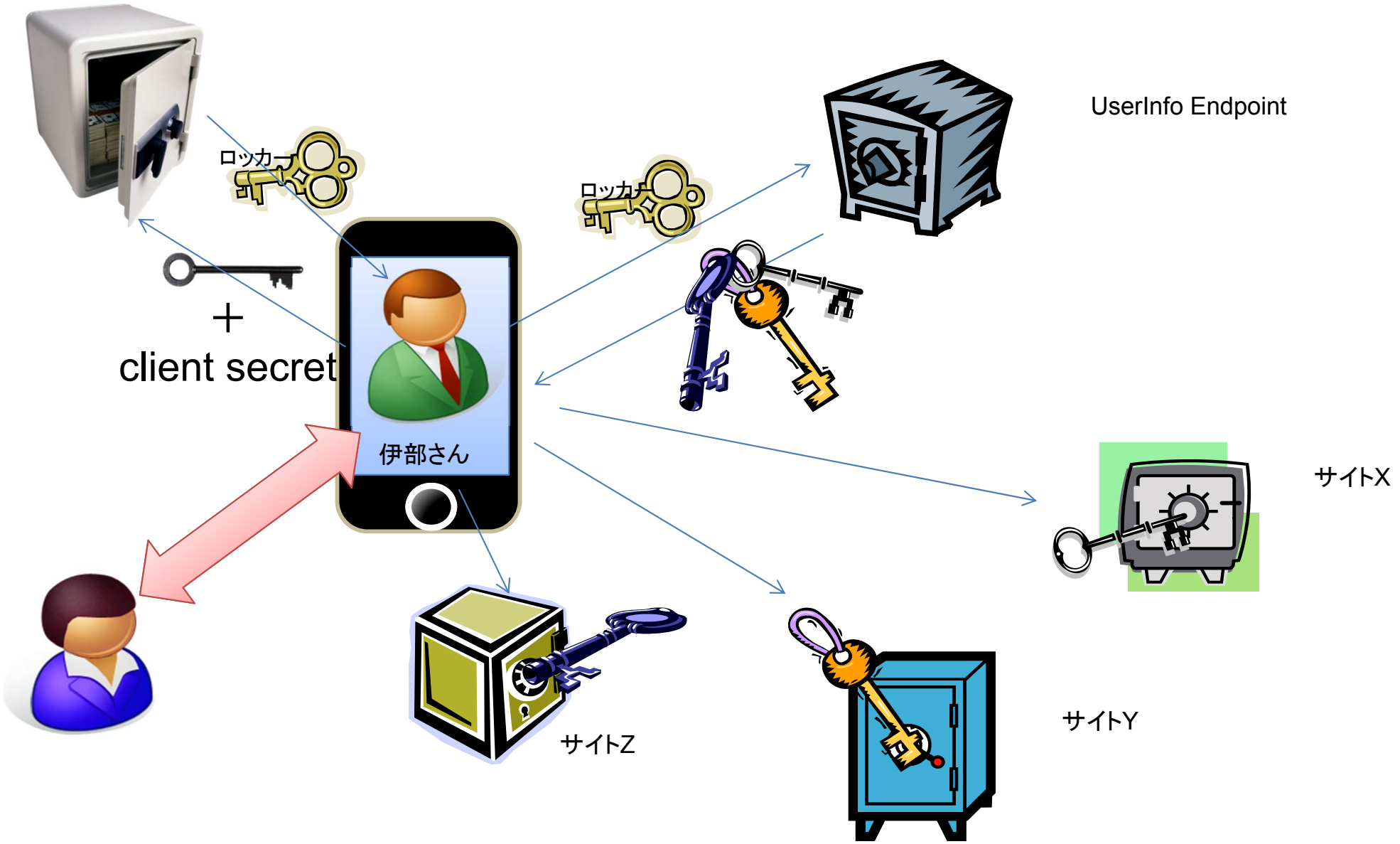


「鍵」＝Access Token　「紹介状」＝ID Token (JWS)

鍵を使った追加情報の（オフラインでの）取得



鍵を使った追加情報の（オフラインでの）取得



1. データ利用を許可するものを厳しく認証し、

- データ利用を許可するもの：本人、代理人、管理者 etc.
  - 本人以外の場合、そのものが権限を持っているのをどのように確認するかは課題。
- 厳しく認証（Core: 3.1.2.3）
  - 認証手段は規定しない。（任意のものを利用可能）
  - ただし、認証レベルの表現は定義している（Core: 5.5.1.1）
    - ISO/IEC 29115 の LoA を規定している

2. (錯誤による同意を減らすために)本人の利益に則して判断する人を許可者に含め、

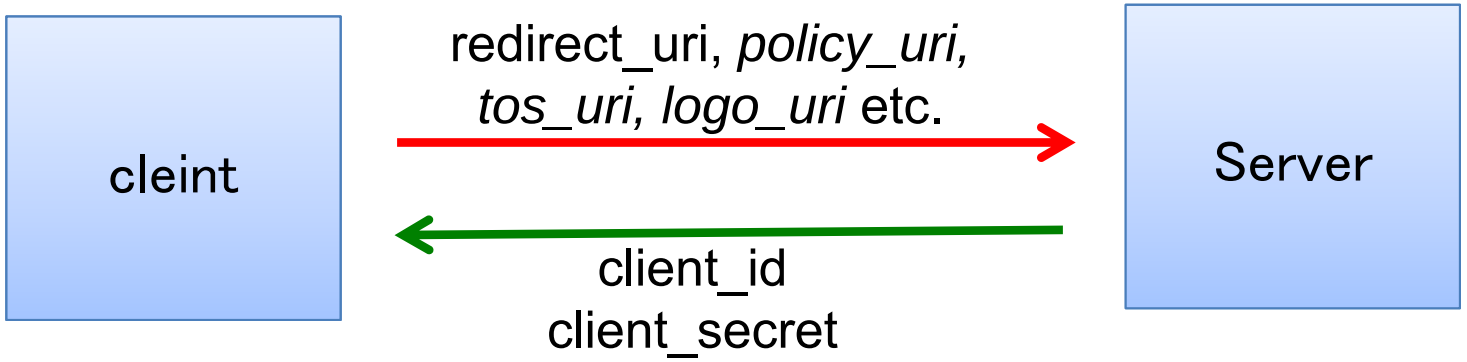
- OpenID Connect では、「許可」は「Authorization Server」において行われる。
- Authorization Server では、
  a. データ利用をするものを認証し、
  b. そのデータ利用者がプライバシー原則の遵守をコミットしていることを確認*1し、
  c. 必要ならば、主体の明示的同意を取得する。

*1 いくら技術的手段を施しても、ここが崩れたら何もならない

2a.データ利用をするものを認証

■ データ利用者はあらかじめ(同意・認可)サーバに登録

- DynReg: 2. Client Metadata



■ データ要求時には、client_id, client_secret で認証

- Core: 3.1.2.1 Authentication Request, 3.1.3.1 Token Request

2b. そのデータ利用者がプライバシー原則の遵守をコミットしていることを確認し、

- policy_uri, tos_uriの内容のトラストフレームワークによる確認と公表(リスティング)
  - トラストフレームワークの指定した policy_uri を採用すると話は簡単
  - これを登録時にコミットしているので、
    - 故意に従わなかった場合→トラストフレームワークによる、詐欺としての訴追
    - 過失の場合→トラストフレームワークの契約にもとづく賠償 etc.
    - などの「エンフォースメント」が効く
- 認可サーバは、
  - clientが「妥当な」policy_uri を登録していること
  - clientが「Good Standing」であること

を確認すれば良い。

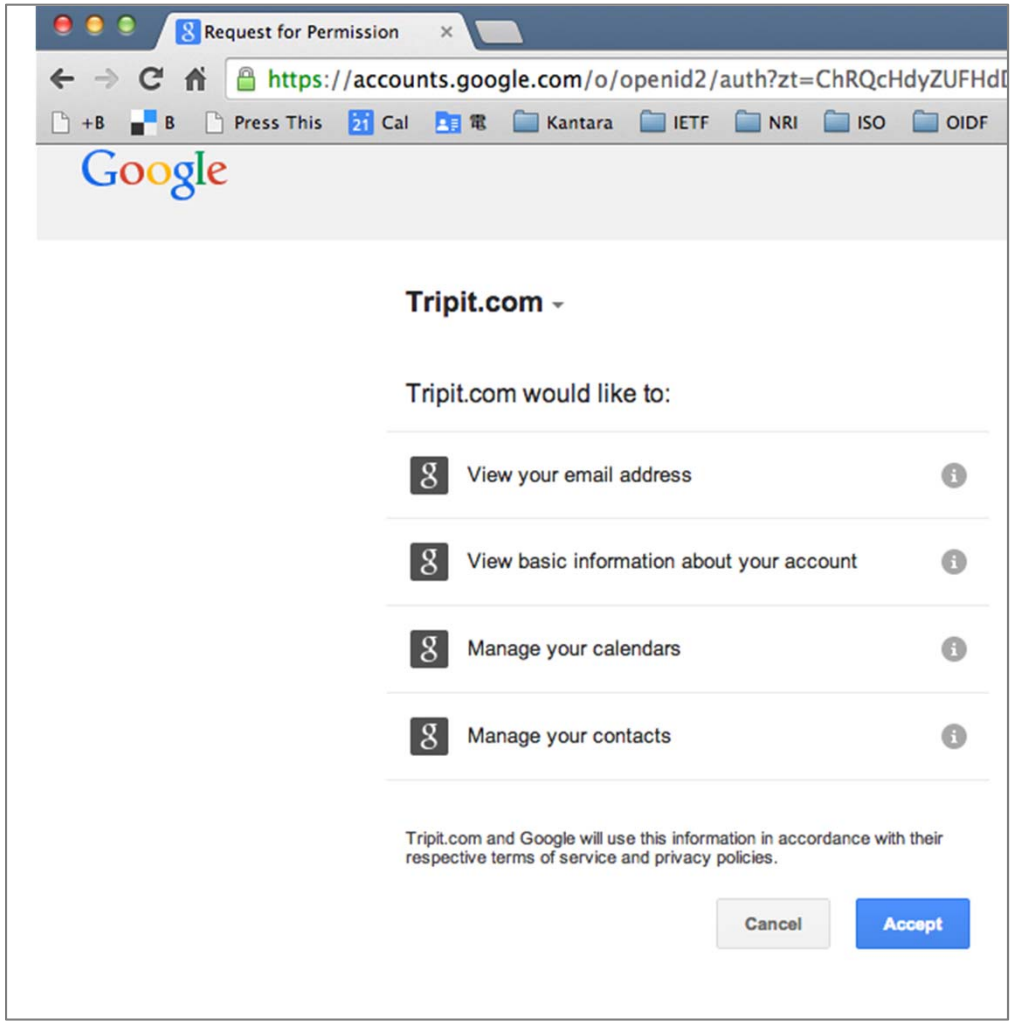
ルール

執行力

技術的対策

※ これは、運用面なので、トラストフレームワークが規定すべきこと。
プロトコルとしてのOpenID Connectは、このユースケースを実装できるように設計されている。

2c. 必要ならば明示的同意を取得する



- Core: 3.1.2.4「他の”Conditions for processing”が満たされていない限り、ユーザの同意を取得しなければならない。」
- ただし・・
  - ユーザのクリックが「意味ある同意」であるかどうかには議論がある。
  - 経産省 IT融合フォーラム・パーソナルデータWG資料など参照

3. 一度に漏洩するデータを少なくする

a. 最低限のデータ取得

- 取得するデータを細かく制御できれば、最低限のデータ取得のみに留めることができる
  - → OpenID Connect では、リクエストごとに属性単位で制御可能（Core: 5.5, 6）

b. 最低限のデータ保持

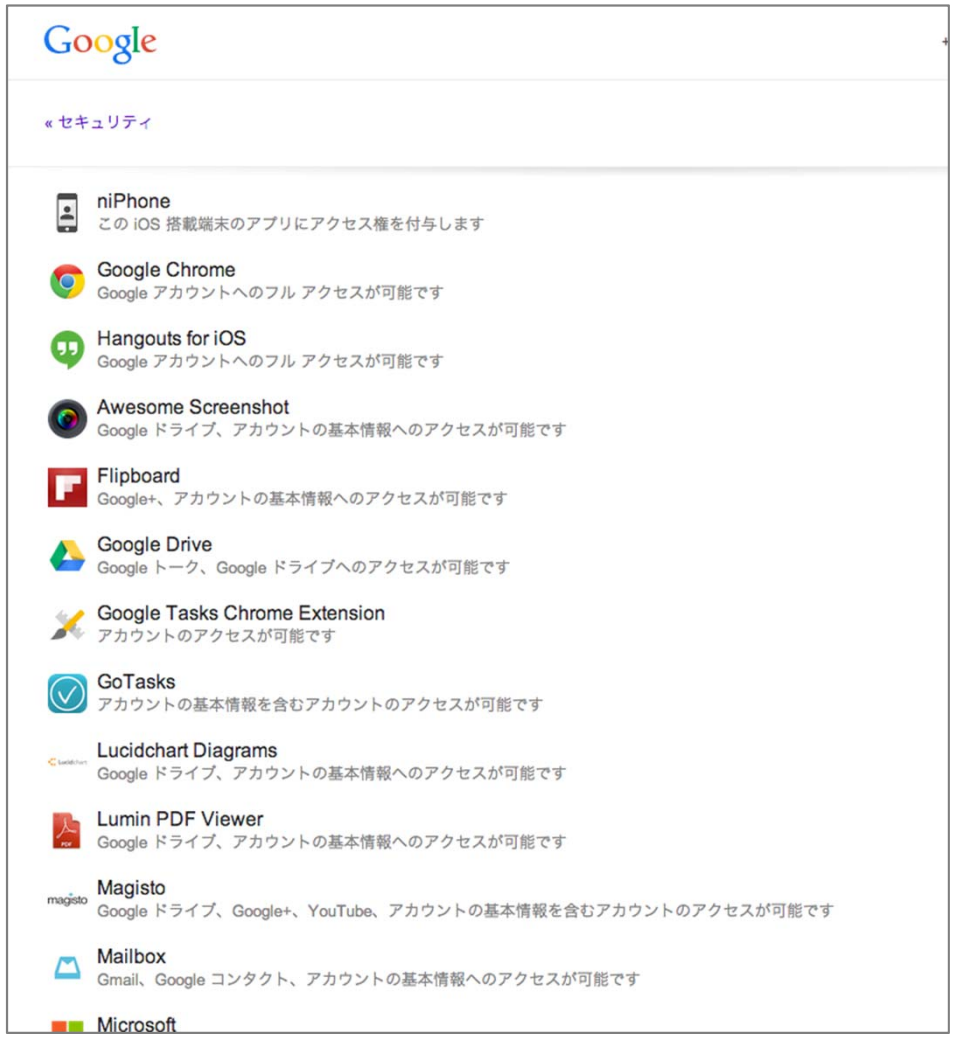
- 「（ユーザが）オフライン（の時のデータ）アクセス」＝「データ購読」ができれば、必要時にデータ取得ができるので、データを保持する必要性が減る
  - → OpenID Connectでは、「Offline」アクセス許可の取得が可能。この権現に基づいて発行された「鍵(access token)」を使う。（Core: 11）

c. 分散データ

- OpenID Connectでは、分散Claimsをサポート。ネットワーク上に散らばったデータソースに対するアクセス許可を発行可能。（Core: 5.6.2）

4. いつでもデータ提供・利用を停止することができるように同意と許可の管理を行う

- データ提供先を手動で管理できているのは2％未満*1
- 許可サーバがデータ提供先一覧を管理、いつでも切断可能に
- そのためには、データ保存期間を短くして、随時再取得させるようにしておく必要がある
  - ● → データ購読
- Core: 16.18「The Authorization Server SHOULD provide a mechanism for the End-User to revoke Access Tokens」



*1 野村総合研究所調査(2008)

わすれてはいけないこと

- OpenID Connectはプロトコルです。
  - 満たすことを可能にしているだけで、
    実際のサービスで上記が守られるかどうかは実装によります。
- プライバシー・トラストフレームワークと組合せてこそ、その真価を発揮します。
- ツール（技術）だけで解決しようとしてはいけません。
  つねにルールとの組合せを考えるべきです。
- 目的を見失わないようにしましょう。守るべきは「個人の尊厳」であり、「本人に不利益がないようにすること」です。
  - 非識別化とか、データの流出防止などは、手段に過ぎません。