ネットの上の“あなた”

～ 安全・便利な本人認証と個人識別の今 ～

中村　素典 / 国立情報学研究所

2013年8月28日

パスワード、いくつ使っていますか？

- ネットバンキング
  - 銀行口座ごとにパスワード
- ネットショッピング
  - ショッピングサイトごとにパスワード
- スマートフォン、タブレット
  - Andoroidの初期設定にGoogleのアカウント
  - iPhoneやiPadでiTunes Storeを利用する際のアカウント
    - iCloud
  - Windows8もMicrosoftのアカウントを作ろうとする

- 他人でなく、“あなた”自身であることを確認したい
  - 性善説では成り立たないネット社会

パスワードは何のため？

- 目的
  - サービスやリソースに**アクセスする権限を持つ**ことを証明する
- 方法
  - 権限を持っていることを証明するための**固有情報の提示**
- 固有情報に求められる特性
  - 容易に**推測**できないこと
  - 容易に**複製（なりすまし）**できないこと
  - 容易に**漏洩**しないこと
  - 利便性を大きく損なわないこと

  など

良いパスワードとは？

- 自分が覚えやすく、他人に類推されにくいもの

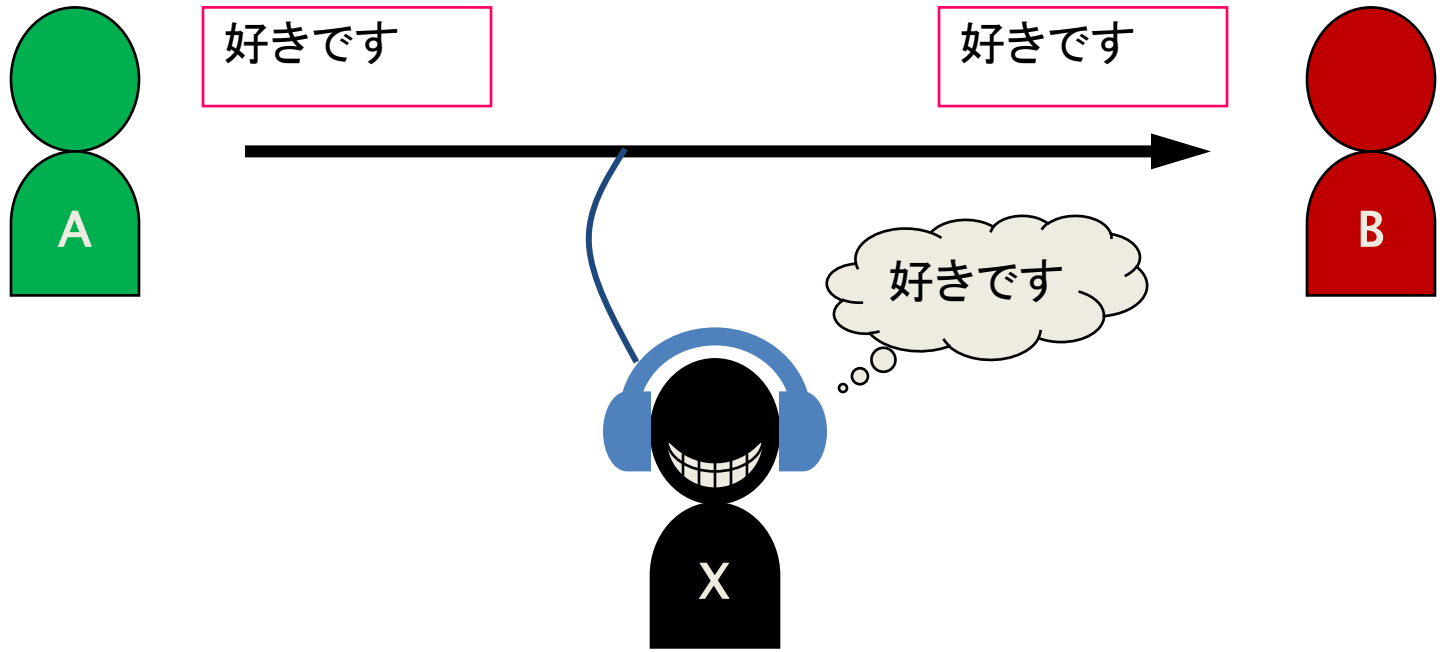
- 危険なパスワード
  - ユーザ名と同じ（ジョー アカウント）
  - 忘れないようにメモに残す、パソコンに貼る
    - 見られたり落としたらどうする？
  - 短い
    - 計算機で総当たり（ブルートフォース）攻撃すれば解ける
  - 辞書に載っている（有名人の名前なども）
    - 様々な種類の辞書が充実
  - 身の回りの情報（氏名、誕生日、住所、電話番号、ペット）
    - 調べる気になればわかる（ソーシャルエンジニアリング）

インターネット上のセキュリティ脅威

1. 盗聴
2. 改竄（かいざん）
3. 成りすまし
4. （否認）

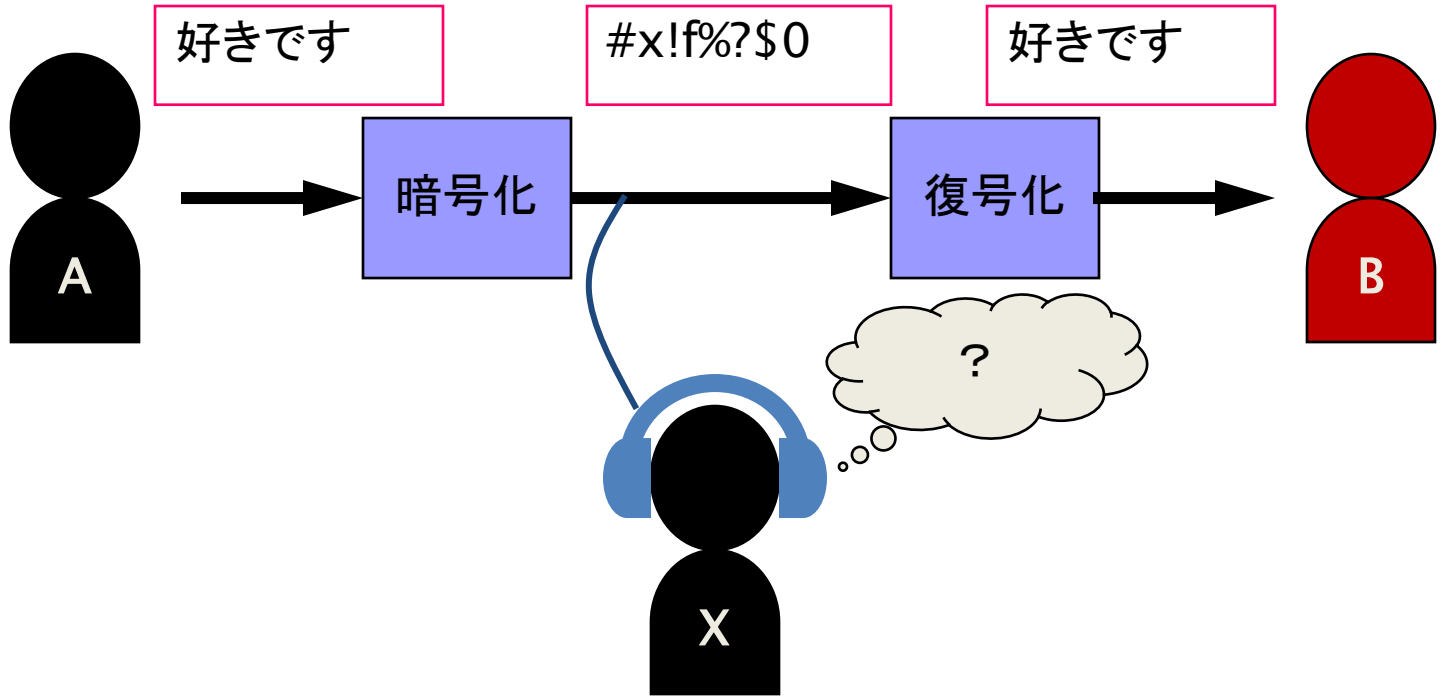
盗聴

- 暗号化していないと…



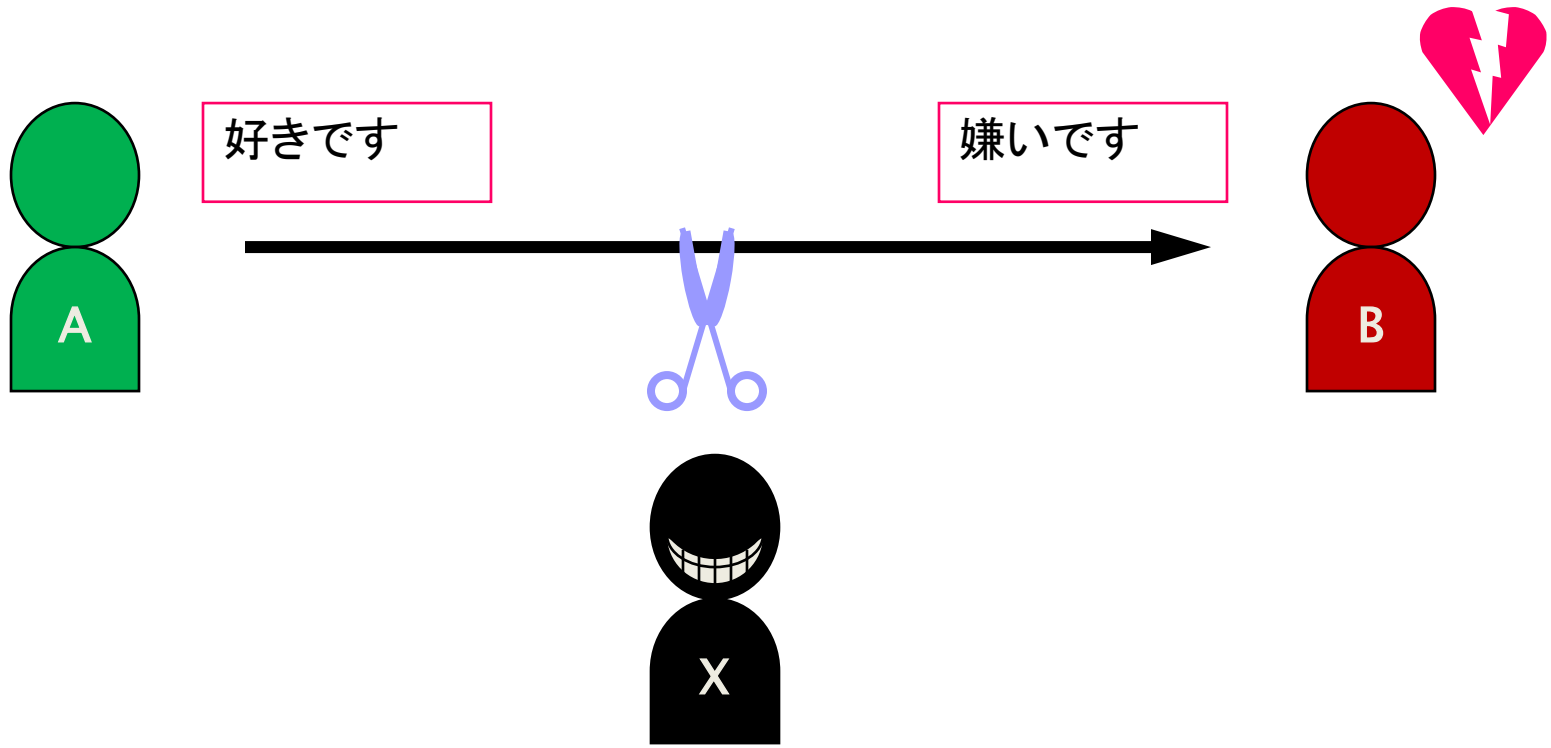
盗聴の防止

- 暗号化によって盗聴を防ぐ



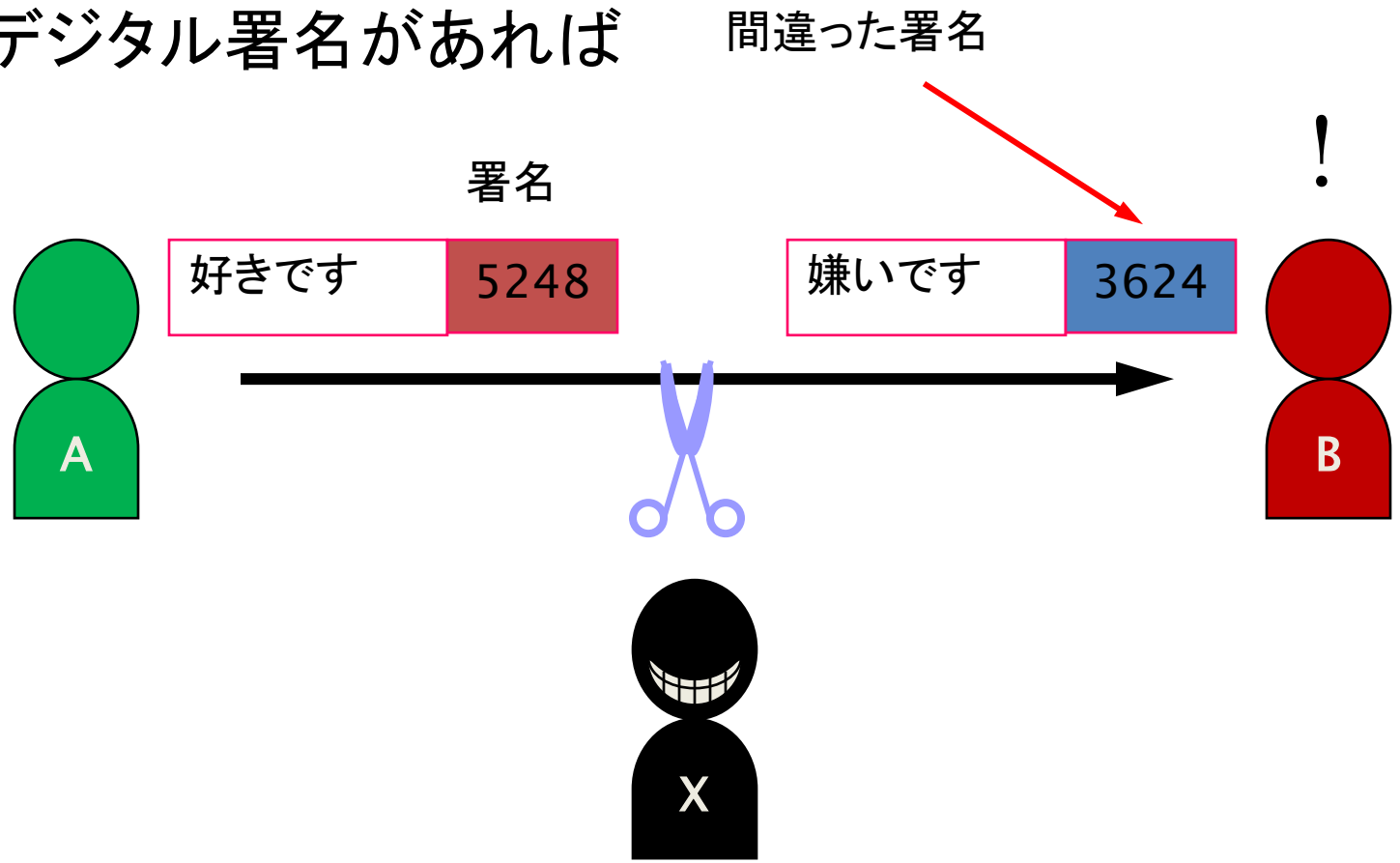
改竄

- デジタル署名していないと…



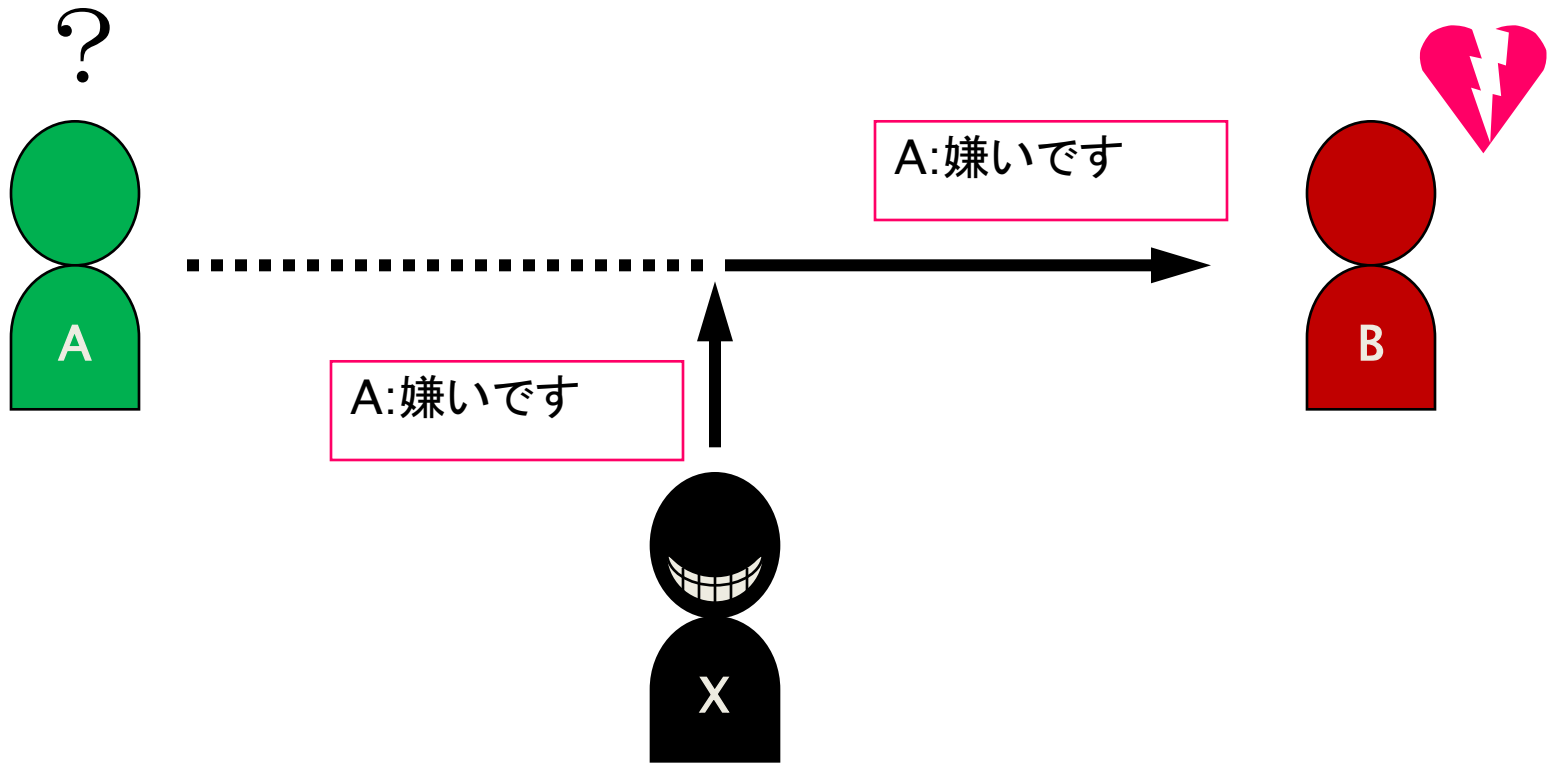
改竄の防止

- デジタル署名があれば



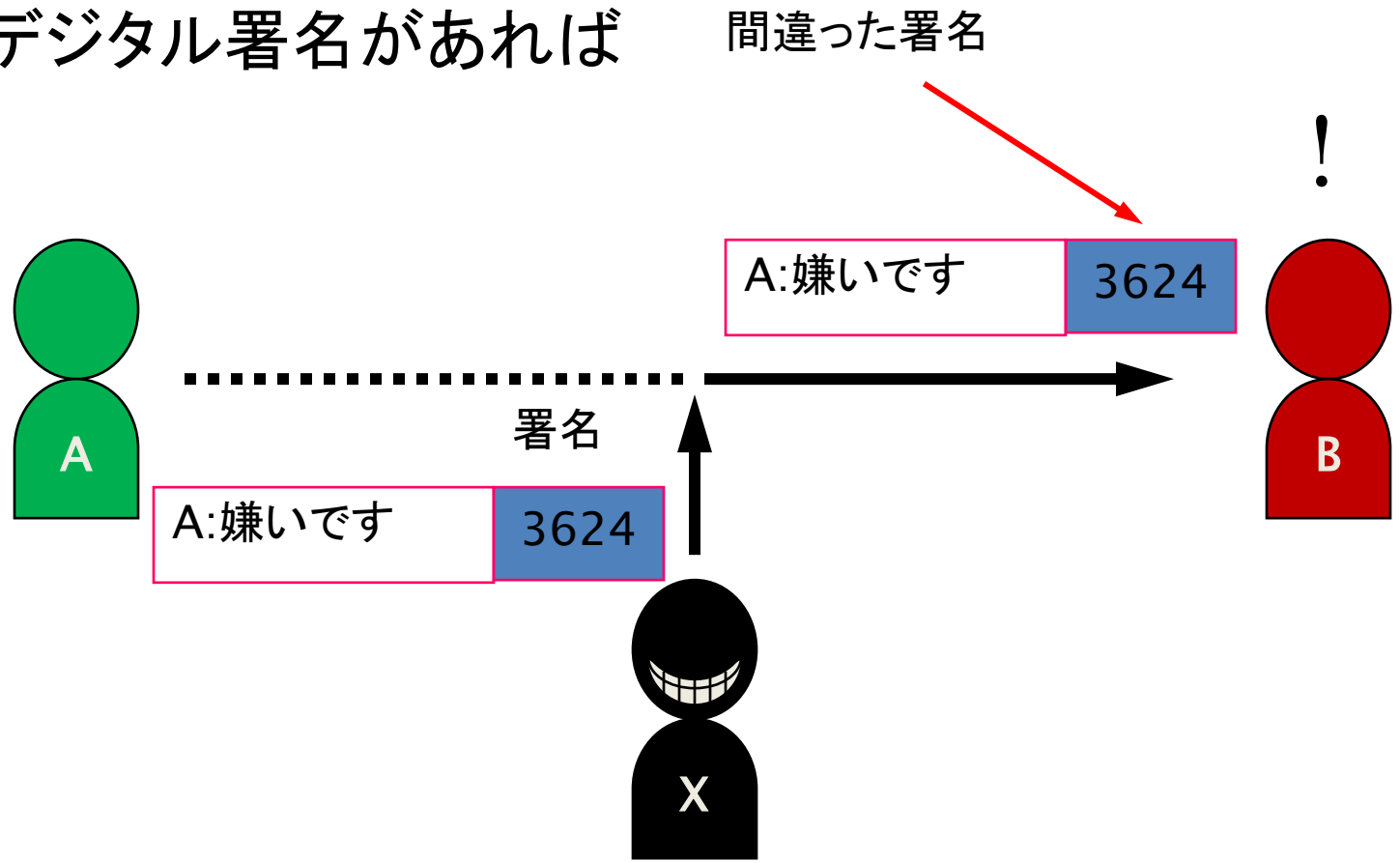
なりすまし

- デジタル署名していないと…



なりすましの防止

- デジタル署名があれば



対策をかいくぐる悪者

- 盗聴
  - 「暗号化されていない」無線LANの危険性
- ショルダーハック（気づかれないように画面を見る）
- キーロガー、スクリーンショット
  - スパイウェアのウィルス感染
- フィッシング（メール等で不正サイトへ誘導）
  - パスワードの確認や変更を要求
- サイトへの不正侵入（パスワードリスト等の取得）
  - 別のサイトへのアクセスにも利用
- リバースブルートフォース
  - 同じパスワードを、ユーザ名を変えながら試す
    - パスワードを連続して間違えたら使えなくなるサイトへの対策
  - ユーザ名(ID)の選定も重要

インターネットでのパスワード盗聴対策（クレジットカード情報なども同様）

- HTTPS (SSL)によるWebページの保護
  - 公開鍵暗号方式を用いた暗号化
    - 対となる「公開鍵」と「私有鍵」の組合せ

緑になるEV証明書は、より厳密な機関認証

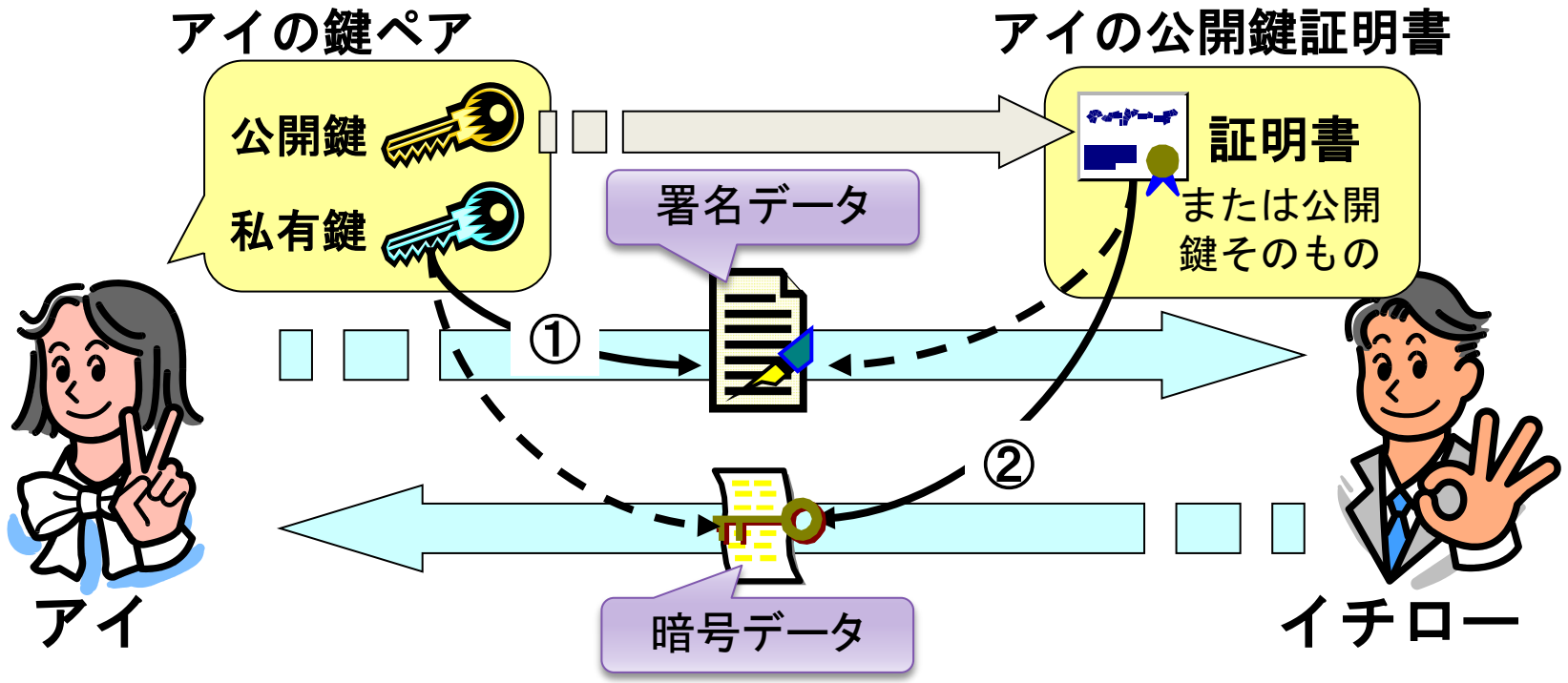
- 暗号通信は相手の識別と両者間の合意が重要
  - 鍵マークが出れば、ほぼ盗聴の危険はない
  - しかし、相手が正しい（信頼できる）とは限らない
    - 似た名前のそっくりサイトによるフィッシング
    - EV証明書（アドレスバーが緑になる）と、随分安心

公開鍵暗号方式による暗号化と署名

- デコードには、対となる鍵が必要、という特性を利用

① 署　名：私有鍵でエンコード→公開鍵でデコード

② 暗号化：公開鍵でエンコード→私有鍵でデコード



パスワードに求められる難解さ

- 周辺情報から類推できないこと
  - 基本4情報（氏名、生年月日、性別、住所）
  - ペットの名前
- 辞書に載っていそうにないもの
  - 辞書は年々充実する
- 総当たり（ブルートフォース）攻撃で破られないもの
  - Lockdown.co.ukが2009年に行った試算
    - 8文字の大小英数字および記号を含むパスワード
      - 高性能PCで23年間、スーパーコンピューターで83.5日
    - 8文字の大小英数字を含むパスワード
      - 高性能PCで253日間、スーパーコンピューターで60.5時間
    - 6文字の大小いずれかの英字だけのパスワード
      - Pentium 100MHzのPCで5分間～8.5時間
  - コンピュータは日進月歩で高性能化する

サイト毎に異なるパスワードの作り方の一例

- 好きな言葉、ことわざ、童謡、歌謡曲の一節をベースに

もーもたろさん　ももたろさん　おこしにつけた

↓

mo-motarosan　momotarosan　okoshinitsuketa

↓

“m-mtr3　mmtr3　oksntkt”

↓ (Google用)

“m-mtr3　Google　oksntkt”

同じ方法が広まるとルール化されて安全性が下がるので、
自分なりの方式を考えましょう！

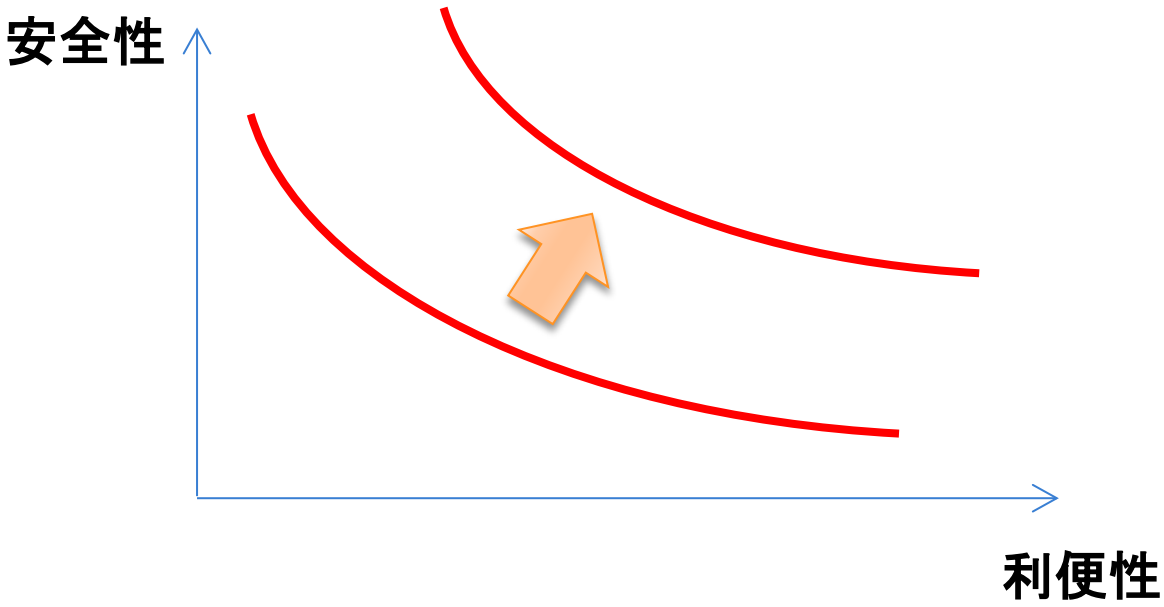
参考：ヒカリ＆つばさの情報セキュリティ3択教室(NII)

パスワード管理について

- 定期的に変更すべき？
  - 頻繁な変更で、パスワードが次第に簡易なものになりがち
    - 弱くなるくらいなら、変えない方がマシ？
- パスワードのサイト毎の使い分け
  - どのパスワードか分からなくなって、いろいろ試すのは危険
    - 一般的なWeb認証だと、相手サイトは生のパスワードを受け取る!
- パスワード管理ソフト（サイト）
  - どこまで信頼できる？
  - 一度に全てのパスワードの狙われる危険性？
  - よく理解した上で利用しましょう

セキュリティにおけるトレードオフ（二律背反）

- 安全性×利便性＝一定



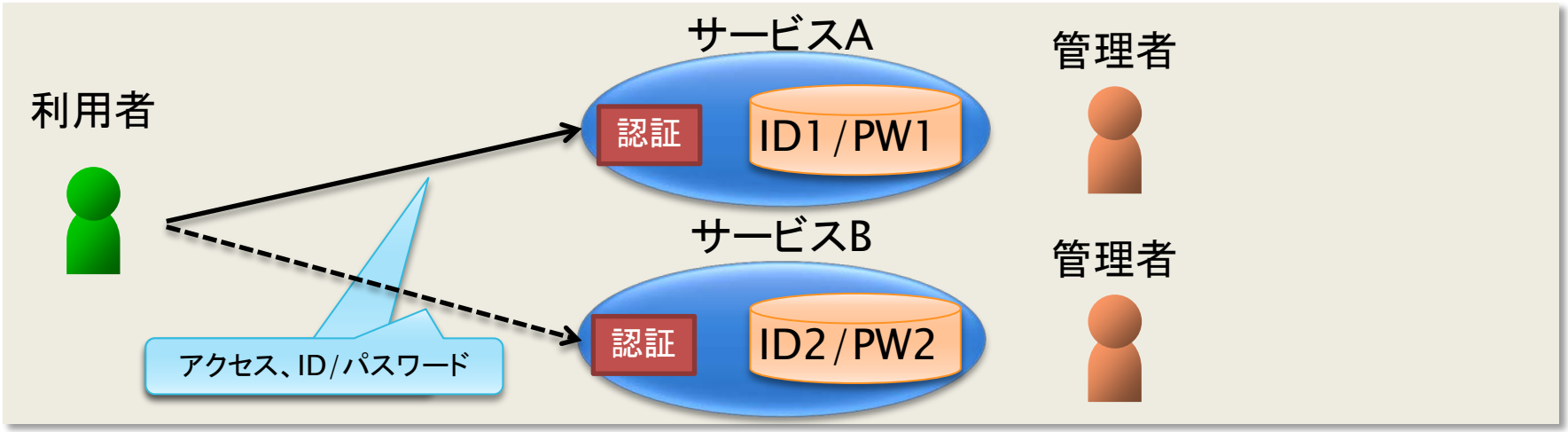
- 技術革新による向上

電子化の推進による様々なサービスの乱立

- 増え続ける大学のキャンパス内オンラインサービス
  - 電子メール
  - 履修登録
  - Eラーニング
  - 単位認定
  - 証明書発行
  - 蔵書検索
  - 業績管理
  - 出張申請
  - 予算管理
  - 施設利用予約
- サービス毎に発行されるIDとパスワード
  - 覚えきれず、セキュリティ低下につながる
  - 管理の手間が煩雑
- 企業でも状況は変わらない

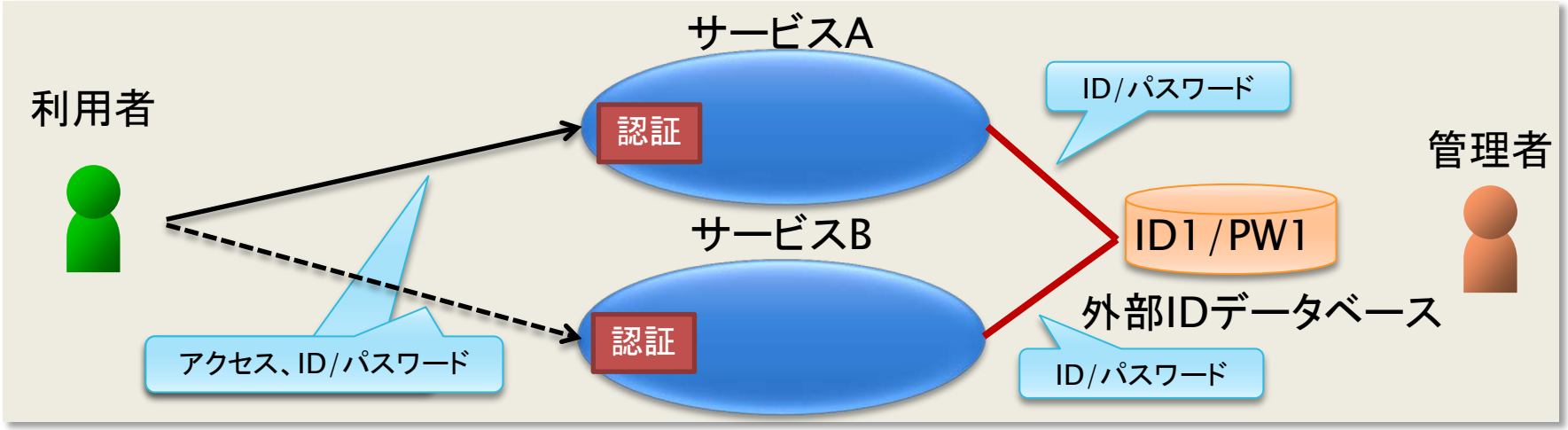
認証統合（一組織の場合）

- ユーザ毎のIDを統一
- IDデータベースを統合



認証統合（一組織の場合）

- ユーザ毎のIDを統一
- IDデータベースを統合
  - 同じIDとパスワードを利用
  - 管理の手間が減ってユーザも管理者も嬉しい

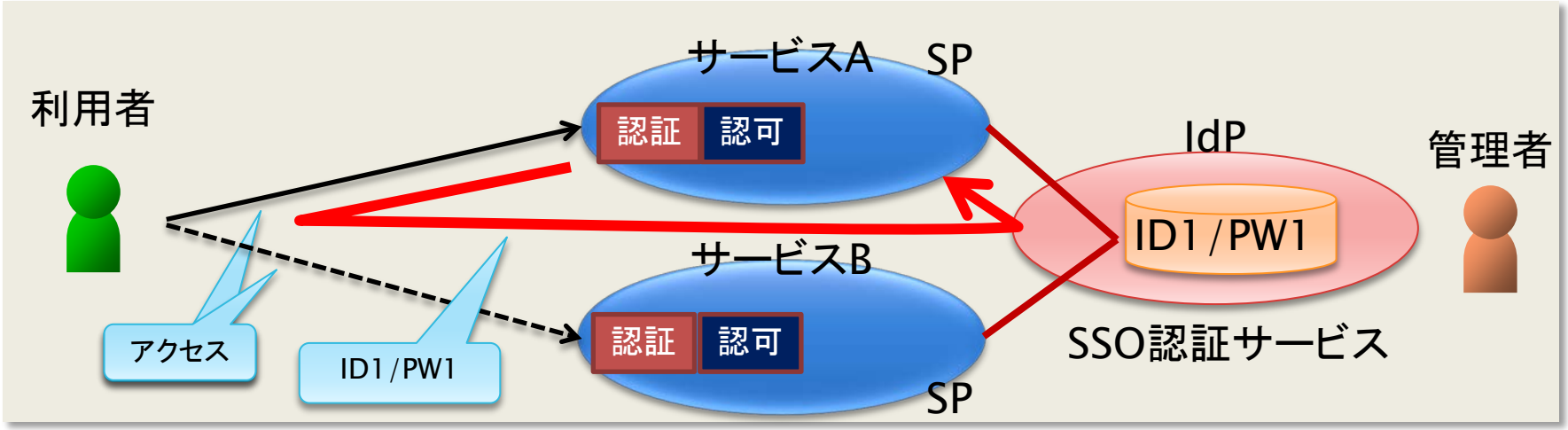


認証統合しても残る危険性

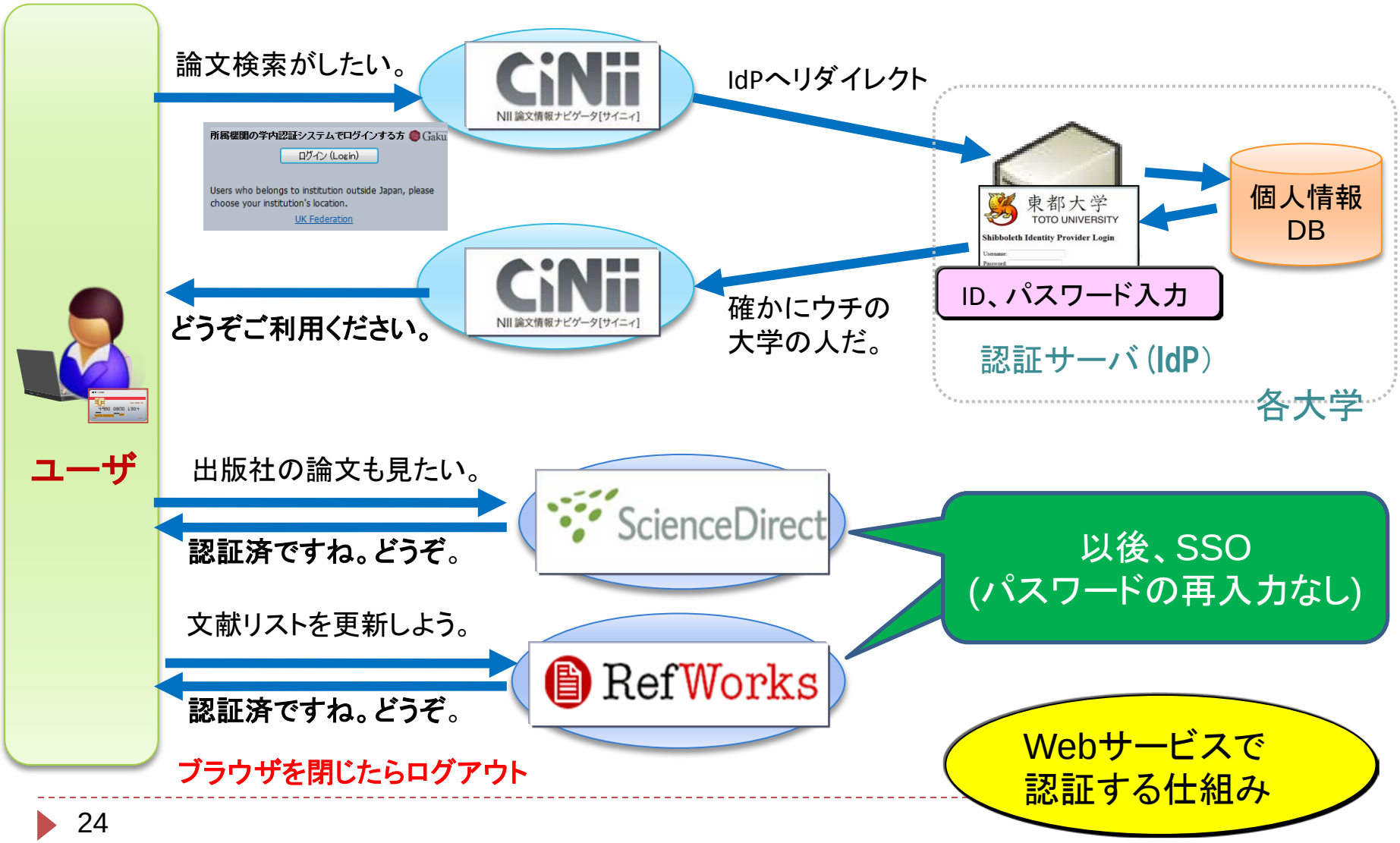
- パスワードは、従来通り各サービスに直接投入される
  - パスワードの不必要なやりとり（盗聴の危険が増える）
    - どこかで漏れると、他のサービスにもアクセスされうる
  - サイト毎にパスワード入力画面（ログイン画面）が異なる
    - フィッシングの危険性

シングル・サイン・オン (SSO: Single-Sign-on)

- 認証処理の部分もサービスから切り出し集約
  - パスワードは、「サービス」には渡らない
- 「ワンストップ」認証
  - 認証済み状態を覚えることで、後のパスワード入力を省略
    - 一定の時間内のみ有効
  - 組織内の認証統合のための技術として登場



SSOでの処理の流れ


論文検索がしたい。
CiNii
NII 論文情報ナビゲータ[サイニィ]
所属機関の学内認証システムでログインする方
ログイン (Login)
Users who belongs to institution outside Japan, please choose your institution's location.
UK Federation
IdPへリダイレクト
東都大学
TOTO UNIVERSITY
Shibboleth Identity Provider Login
個人情報
DB
ID、パスワード入力
認証サーバ（IdP）
各大学
確かにウチの
大学の人だ。
どうぞご利用ください。
ユーザ
出版社の論文も見たい。
ScienceDirect
認証済ですね。どうぞ。
以後、SSO
(パスワードの再入力なし)
文献リストを更新しよう。
RefWorks
認証済ですね。どうぞ。
ブラウザを閉じたらログアウト
Webサービスで
認証する仕組み

ところで、どうしてパスワード？

- “あなた”であることを確かめる方法の一つ

- 確かめる方法は、パスワードだけではない

Source: http://www.npa.go.jp/annai/license_renewal/home.html

Source: http://www.nikkei.co.jp/topic5/2004newpro/yusyut.html

Source: http://juki-card.com/about/

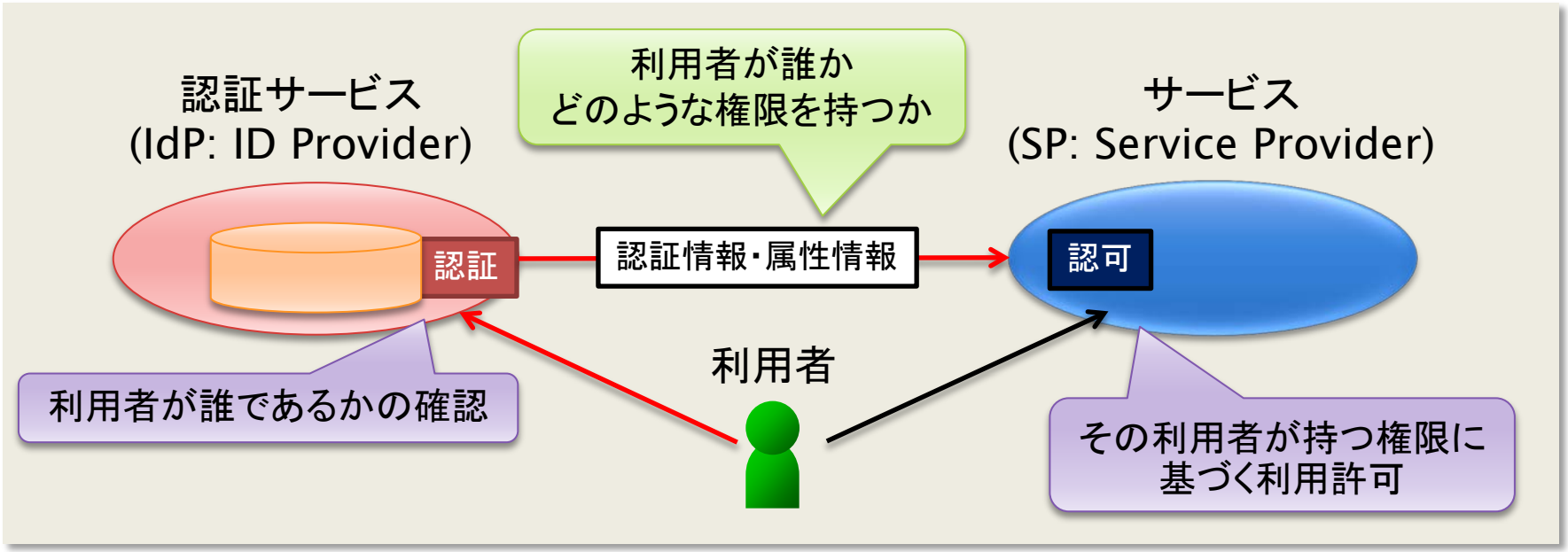
“あなた”について、確実に知りたいこと

- 本人性
  - “あなた”自身の意思によるものであること
  - 他人による勝手な成りすましでないこと
    - “あなた”だけの情報（指紋、顔写真、パスワード、…）
- 実在性
  - “あなた”が実際に存在する人であること
  - 架空の存在でないこと
    - “あなた”に対応する識別子（符号）などが使われる
- 真正性（非改ざん性）
  - “あなた”に対応する識別子が正しいものであること
    - 本人性と実在性の対応付け

多くの場合、区別無く扱われるが、実際には異なる

認証と認可の分離

- 認証
  - 利用者が誰であるかの確認
- 認可
  - その利用者が持つ権限に対応した利用許可



SSO（認証と認可の分離）で得られる安全性

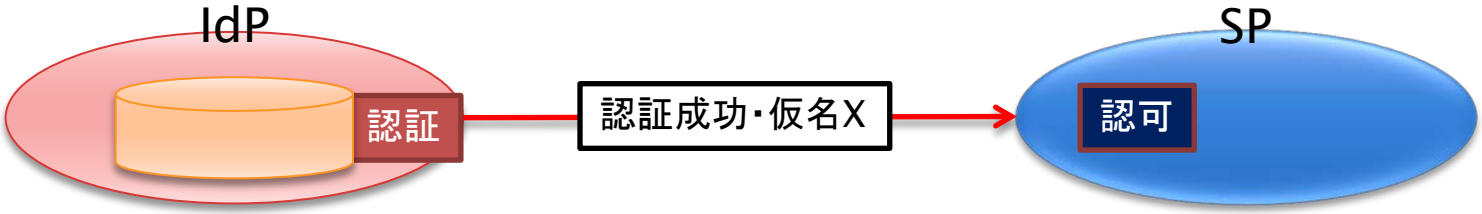
- パスワードはサービスに渡らない
  - セキュリティ水準の統一
- 怪しいサーバの排除
  - 連携するサイトのリストを管理
    - フィッシング対策
- プライバシー保護の可能性
  - 属性情報の送信制御
  - 匿名、仮名でのアクセスも実現可能
    - もちろん、全てのサーバの協力で利用者を特定可能

匿名アクセス、仮名アクセス

- 通常アクセス

- 匿名アクセス
  - ID情報を送らないので、実際に誰かはわからない

- 仮名アクセス (PPID: Pairwise Pseudonymous Identifier)
  - SP毎に異なるIDを送ることで、SP間での行動履歴の収集を防止
    - プライバシー保護



SSOの新たな使いみち

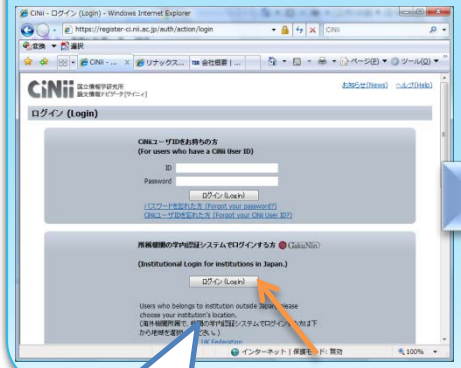
- 組織をまたがったID連携
  - 「フェデレーション」

- 背景
  - SSO規格（プロトコル）の標準化
    - 組織毎に異なった規格だと相互接続が困難
    - SAML (Simple Authentication Mark-up Language)
      - XMLベースの書式
    - OpenID
  - SaaS (Software as a Service)やクラウドの登場と普及
    - ネットワーク越しに様々なサービスを利用することが当たり前に

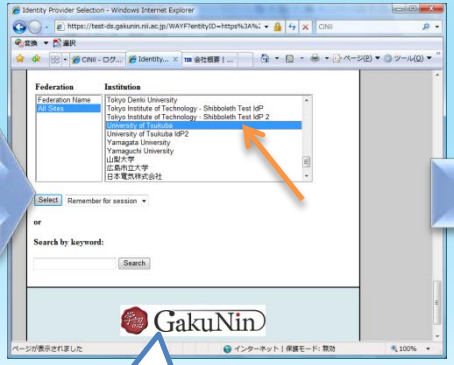
フェデレーションにおける認証手順

成功！

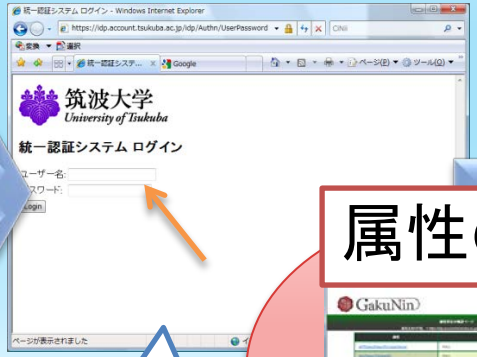
1. 学認認証を選択



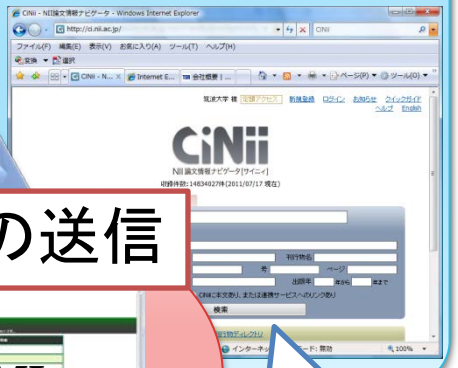
2. 所属機関を選択



3. ID/PWを入力



4. 認証完了(SPに戻る)



属性の送信

SAML
(属性)

SP
(Service Provider)

DS
(Discovery Service)

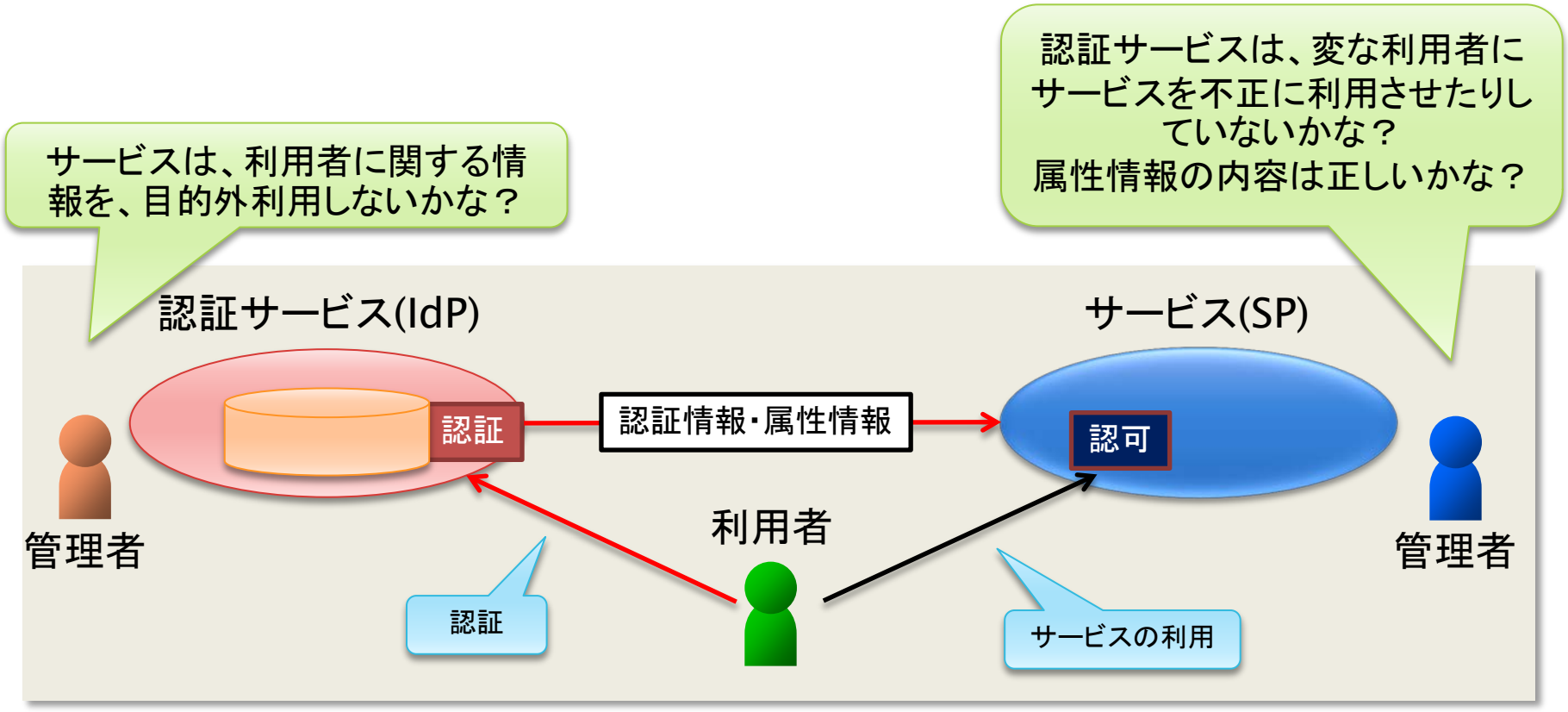
SP

IdP
(Identity Provider)

SP
(Service Provider)

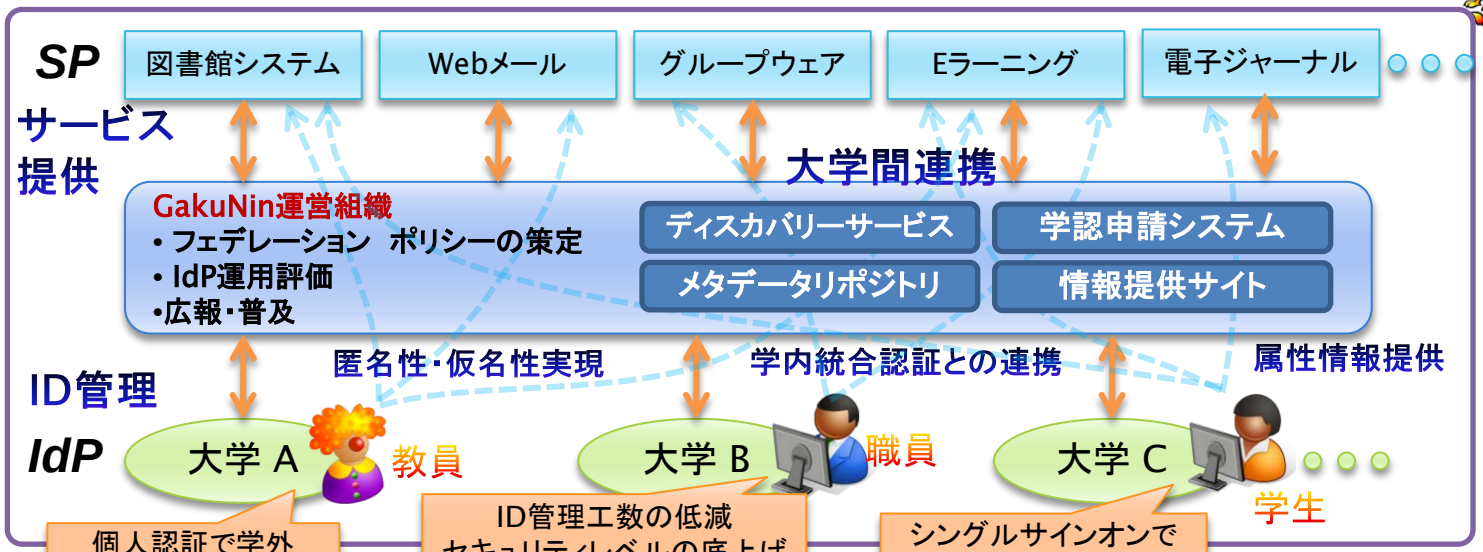
SSO技術の組織間利用での信頼

- 異なる組織が個別に管理するため、相互の信頼が重要



学術認証フェデレーション「学認」

- シングルサインオン(SSO)技術に基づく学術研究支援IT基盤の構築
- IdP･SP相互の信頼を持続する信頼フレームワークの提供
- 国際連携･産学連携による利便性向上、付加価値の実現、新サービスの創出
- 多様なニーズに応え、利便性･セキュリティを向上させる技術開発



コンテンツ系サービス

各種基盤系サービス

Foodle

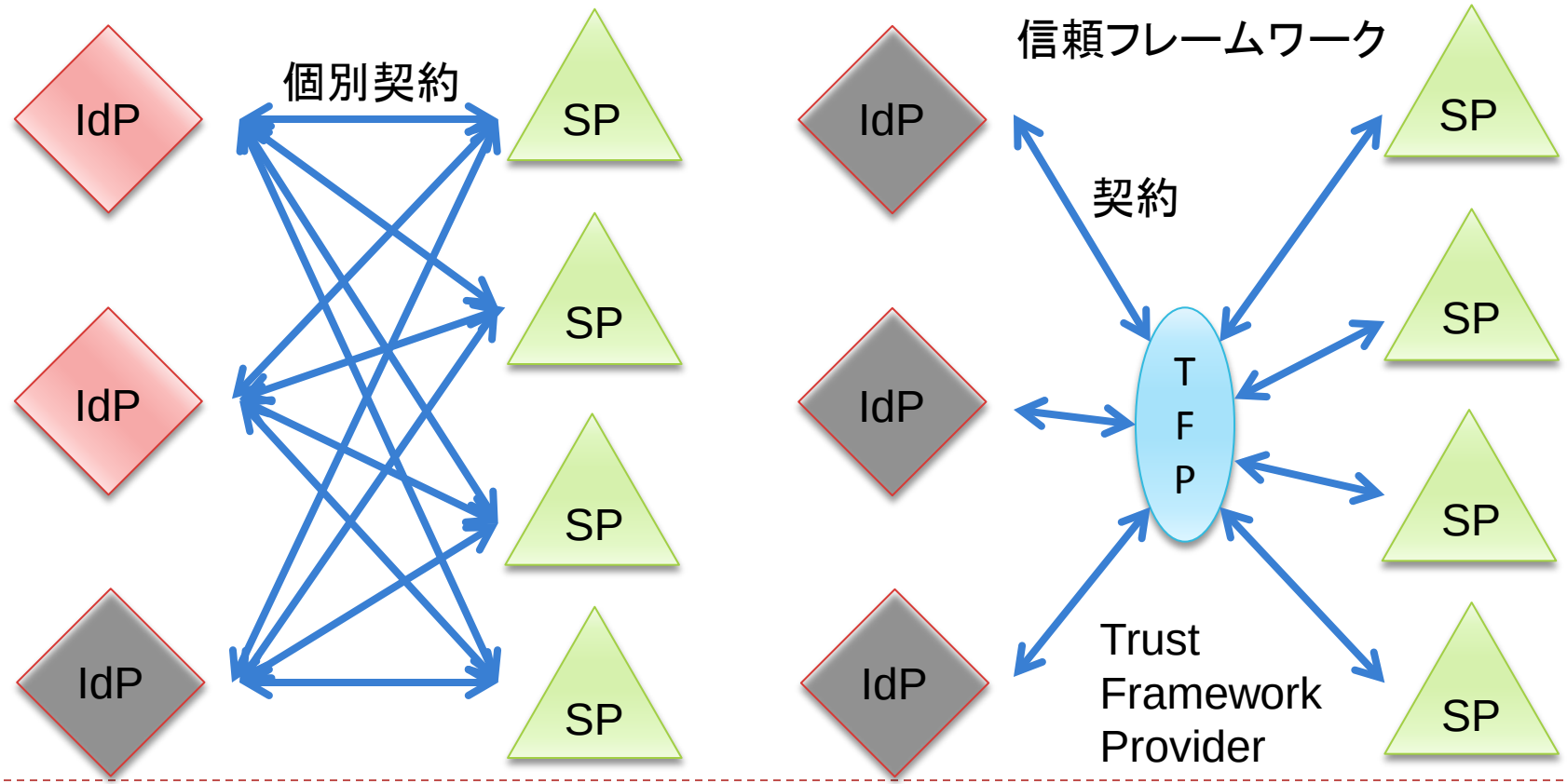
民間でも広がるSSO技術

- ID連携機能を提供するプロバイダ
  - Facebook
  - Google
  - mixi
  - Twitter
  - Yahoo! Japan

  など…
- 利用プロトコル
  - OpenID 2.0 (2007)
  - OAuth 2.0 (2012)
  - OpenID Connect (2013?)

信頼フレームワークの効果

- 一律のポリシーに基づく信頼フレームワークの導入により、個別契約でのN×Mの関係が、N＋Mの関係に削減



学認とOpenIDとの連携の可能性

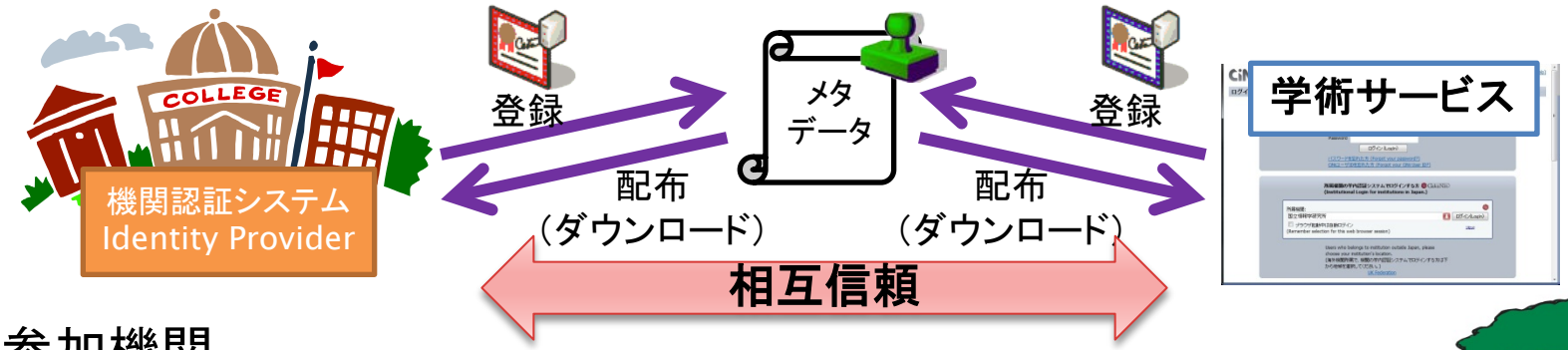
- 民間デファクトであるOpenID対応のサービスが、学認IdPで認証して利用できるようになれば、**学認（大学）向けのサービス**がさらに広がる
  - 学認にて**プロトコルゲートウェイ**によるOpenID Connect対応

- 民間（OpenID OP）から 学認対応SP へのアクセスが可能になれば、**産学協同研究の情報基盤**としての活用や**保護者向けサービス**へも展開できる
  - Google/Yahooなどのアカデミックサービスを利用している大学の、学認参加も容易に

学認による認証連携の礎

GakuNin ポリシーに準拠し参加機関間の認証連携を実現

- 学術認証フェデレーション実施要領（平成24年3月22日 改正）
- 学術認証フェデレーション システム運用基準 (Ver.1.2)（平成23年8月24日 改正）



- 参加機関
  - ポリシーに準拠することにより学認に参加可能
- 事務局
  - 参加が承認されたIdPとSPの情報はメタデータに登録
- IdP,SPサーバ
  - メタデータに登録されたIdPとSPだけが互いに接続することができる

学認システム運用基準で定めるIdPの要件

- 組織の構成員であることの保証
  - 卒業、退職などによる異動の適切な反映
  - 名誉教授、OB、図書館の地域内利用者、その他ゲスト等の扱い
- 識別子再利用についての考慮
  - 同一識別子を利用する場合は、一定期間あける
- ユーザの同一性の保証
  - パスワード配布時の本人確認
  - 適切に管理された役職アカウント
- 個人情報保護への対応
  - 国公立大学ではオプトインが原則
- ログの保存
  - インシデント対応のための、eduPersonTargetdIDやtransient-idの記録

機関として責任を持った IDおよび属性の保証

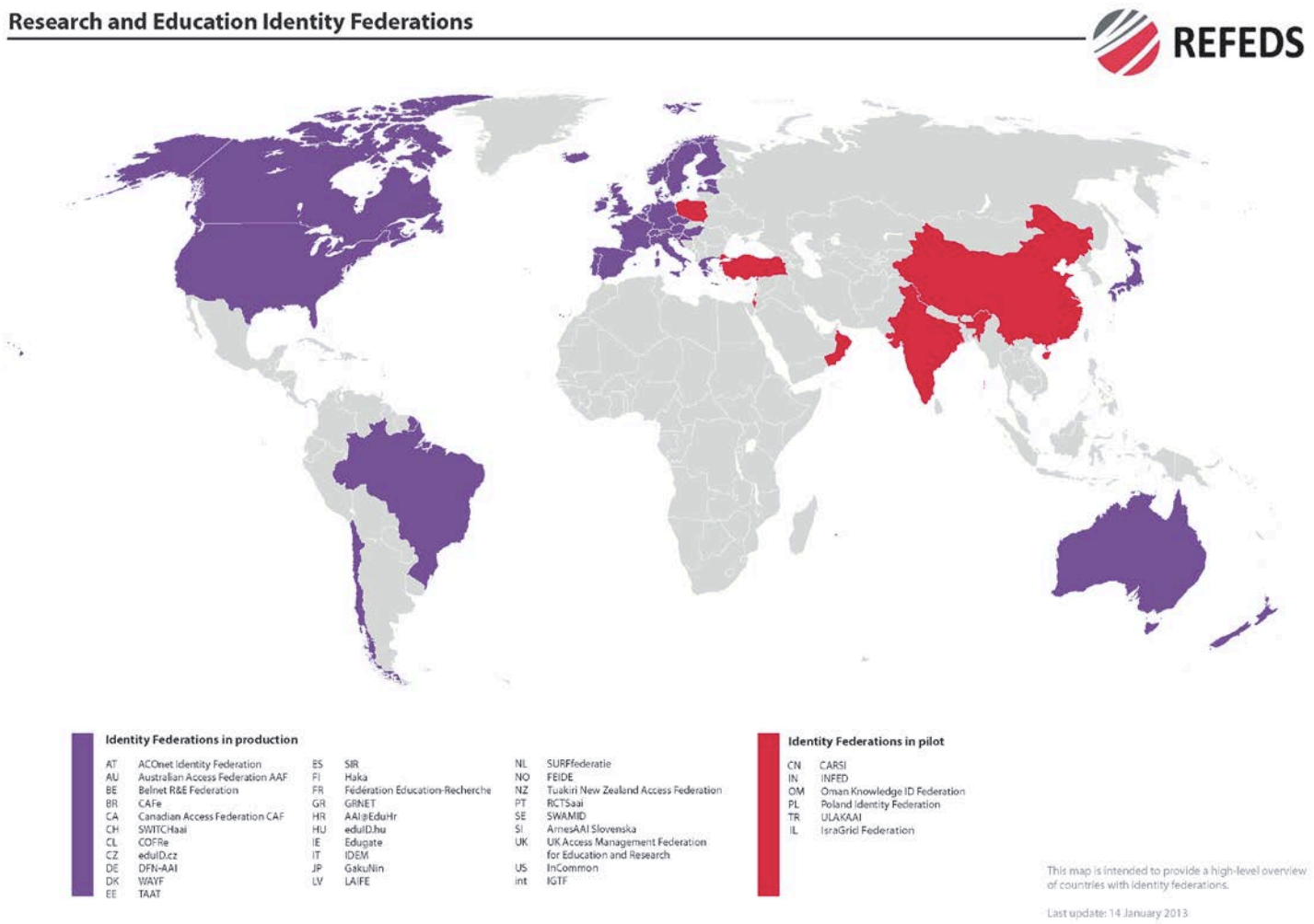
⇒定期アンケート（毎年）によるチェックとフィードバックで維持

- IdP of The Year 2012 を大阪大学が受賞

フェデレーションのメリット

- 管理コストの削減
  - ユーザ管理が不要
  - クラウド利用の促進
- セキュリティレベルの向上
  - セキュリティ基準への準拠が容易
  - SPにおいてパスワードを扱わずに済む
    - 決裁情報も分離すればさらに安心
- 利便性の向上
  - シングルサインオン技術の活用
  - サービス間連携（マッシュアップ）の推進
- 大学間交流の支援
  - 単位互換授業、共同研究など
- 新たなサービスの発掘
  - サービスのスタートアップの迅速化

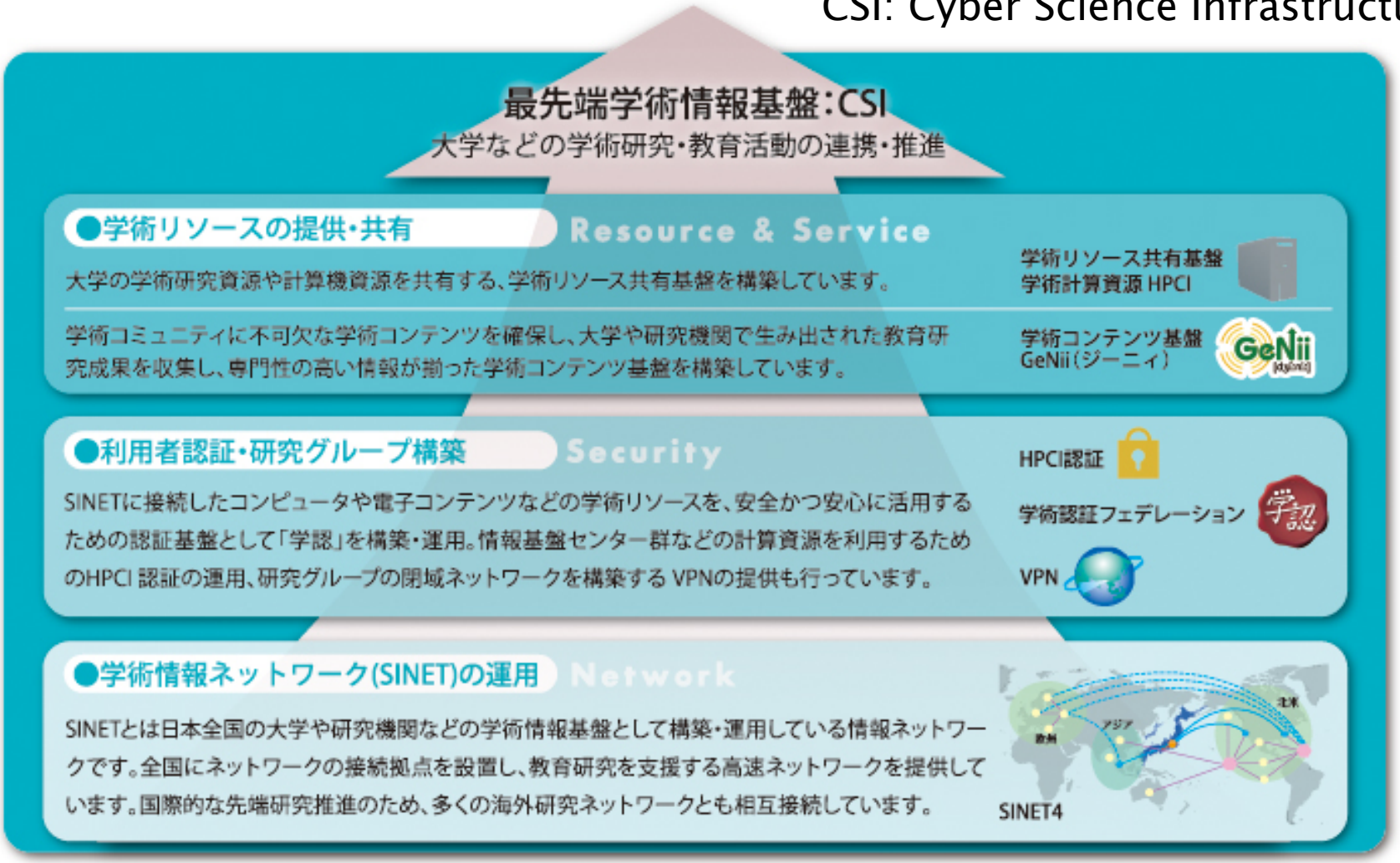
学術フェデレーションの広がり



Source: https://refeds.org/docs/REFEDSmap.pdf

NIIによるCSIの整備

CSI: Cyber Science Infrastructure



学認で扱う属性情報（IdPからSPへ送出）

属性	内容
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名（日本語）
OrganizationalUnit (ou)	組織内所属名称
jaOrganizationalUnit (jaou)	組織内所属名称（日本語）
eduPersonPrincipalName (eppn)	フェデレーション内の共通識別子
eduPersonTargetedID	フェデレーション内の仮名識別子
eduPersonAffiliation	職種
eduPersonScopedAffiliation	職種（@scopeつき）
eduPersonEntitlement	資格
SurName (sn)	氏名（姓）
jaSurName (jasn)	氏名（姓）（日本語）
GivenName	氏名（名）
jaGivenName	氏名（名）（日本語）
displayName	氏名（表示名）
jaDisplayName	氏名（表示名）（日本語）
mail	メールアドレス
gakuninScopedPersonalUniqueCode	学生・職員番号（@scopeつき）

実際に使われる属性情報の例

サービスA (1項目必須)

eduPersonPrincipalName(必須)

サービスB (1項目必須)

eduPersonAffiliation (必須)
eduPersonTargetedID

サービスC (必須項目なし)

eduPersonEntitlement
eduPersonAffiliation

必要最低限のみを送出

(参考) https://www.gakunin.jp/docs/fed/technical/attribute

送信する属性情報の選択による プライバシー保護

- 送信が必須でない属性情報に関して、ユーザが送信の可否を個別に選択できる
- 将来の挙動について指定できる

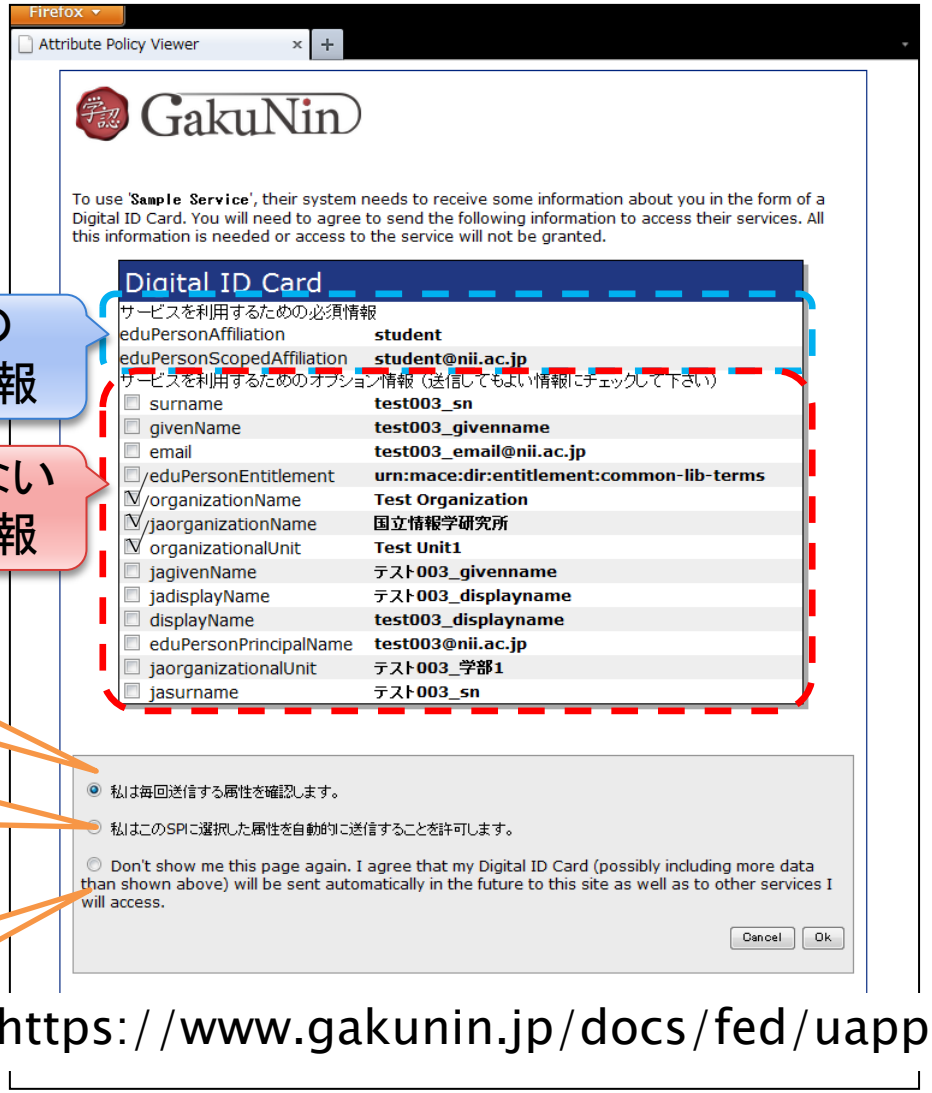
必須の属性情報

必須でない属性情報

次回の同一SPアクセス時も再び同意が必要

同一SPについては将来の同一内容の送信について同意

全てのSPに対して全ての属性情報を送ることを同意



https://www.gakunin.jp/docs/fed/uappro

SNS等の連携とプライバシー

- SSO等の連携技術の普及により、ますます便利に
  - ログインだけでなく、様々な情報の連携が可能

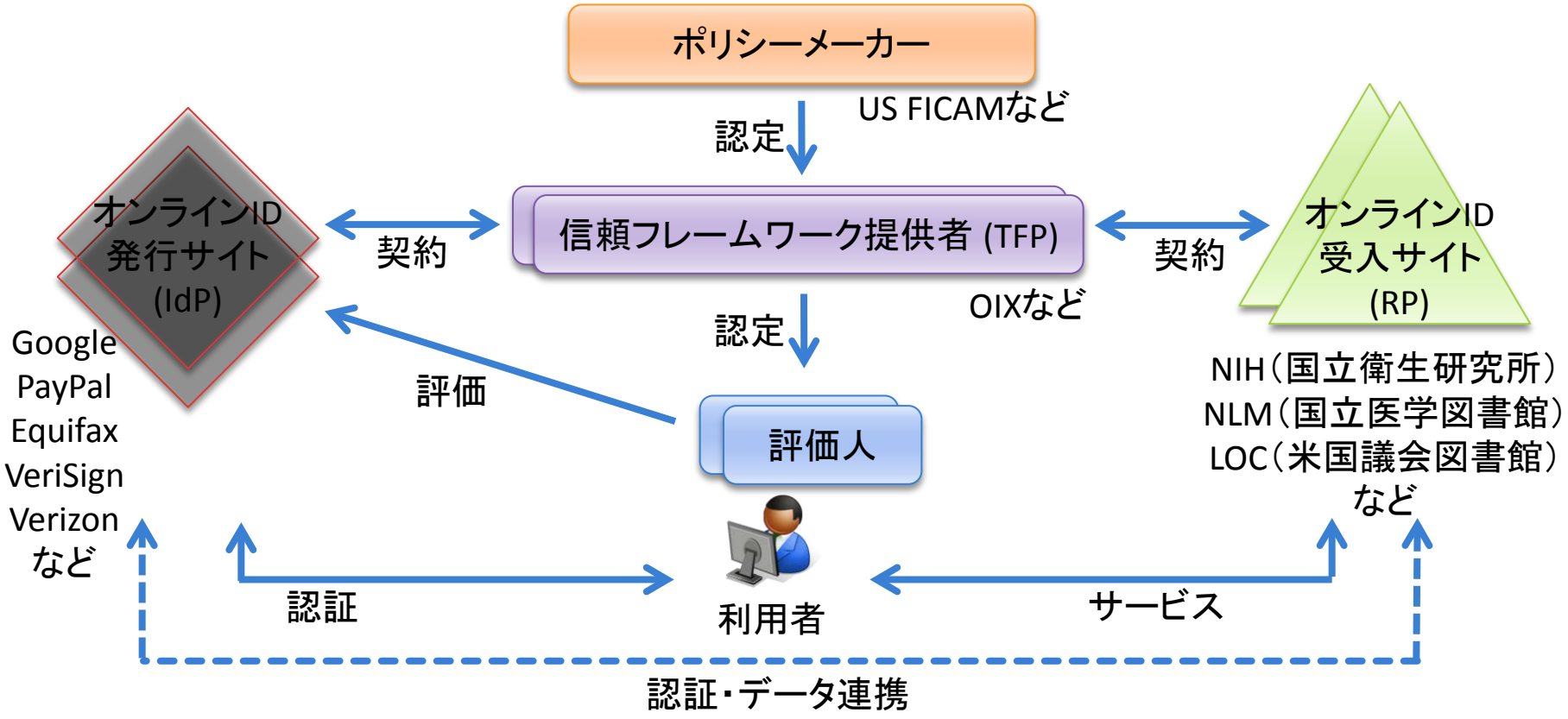
- SNS系サービスには様々な個人情報が蓄積されていく
  - 情報の公開範囲の設定に注意
  - アプリケーションや他のサービスとの連携で個人情報が渡る
  - 公開・非公開を細かく指定できない場合が多い
    - 要求をすべて了承しないとアプリが利用できない等

参考:「SNSの安全な歩き方～セキュリティとプライバシーの課題と対策～」

- JNSA（日本ネットワークセキュリティ協会）
- http://www.jnsa.org/result/2012/sns.html

信頼性の評価

- トラストフレームワーク
  - 米国の例 (LoA 1)



保証レベル (Level of Assurance)

- 4つの保証レベルを規定
  - レベル1：whitehouse.govのWebサイトでのオンラインディスカッションに参加
  - レベル2：社会保障Webサイトを通じて自身の住所記録を変更
  - レベル3：特許弁理士が特許商標局に対し、機密の特許情報を電子的に提出
  - レベル4：法執行官が、犯罪歴が格納されている法執行データベースにアクセス

- LoA 1
  - 米国連邦政府内のサービス（SP）に、外部の認証システム（IdP）を用いてアクセスする場合に求められるレベル
    - PubMedなどの、米国NIH（国立衛生研究所）提供の95のサービスへの接続
  - プライバシー保護（余計な個人情報は送らない）の観点もある

認証サーバに求められる安全基準

- 日本政府におけるガイドライン （米国 国立標準技術研究所 NIST SP800-63に準じる）
  - オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（概要版）[PDF]より引用
  - http://www.kantei.go.jp/jp/singi/it2/guide/

＜主な対策基準＞

保証レベル	登録	発行・管理	トークン	認証プロセス	署名等プロセス
レベル4	**（窓口）** • 写真付き身分証明1種の提示 • 申請情報の台帳照合 • 重複登録ではないことの確認	• 手渡し、本人限定受取郵便、によるトークン発行	• レベル3の基準に加え、耐タンパ性が確保されたハードウェアトークンを利用すること	• レベル3と同等の基準	• 電子政府推奨暗号リストに記載の署名方式 • 電子署名用の証明書の用途は電子署名限定
レベル3	**（窓口）** • 写真付き身分証明1種（or他2種）の提示 • 申請情報の台帳（又は公的証明書）照合 **（郵送 or オンライン）** • 申請書に対する電子署名 • 申請情報の台帳（又は公的証明書）照合	• レベル4の方法に加え、書留郵便、書留郵便＋ダウンロード、電子署名＋ダウンロード、によるトークン発行	• レベル2の基準に加え、複数の認証要素を利用すること	• レベル2と同等の基準に加え、フィッシングの脅威に対する耐性	• 電子政府推奨暗号リストに記載の署名方式
レベル2	**（窓口）** • 写真付き身分証明1種（or他2種）の提示 **（郵送 or オンライン）** • 申請情報に他機関の登録情報（クレジットカード番号等）を含めて申告	• レベル3の方法に加え、分割配付（一方を郵送）、メール通知後のダウンロード、によるトークン発行	• 認証情報の推測確率が16384分の1未満であること	• レベル1と同等の基準に加え、盗聴、セッション・ハイジャック、中間者攻撃の脅威に対する耐性	
レベル1	**（窓口 or 郵送 or オンライン）** • 身元確認は不要 • メールアドレスの到達確認	• レベル2の発行方法に加え、電子メールによる送付、ダウンロード、によるトークン発行	• 認証情報の推測確率が1024分の1未満であること	• オンライン上の推測、リプレイ攻撃の脅威に対する耐性	

パソコン1台によるアクセスの限界

- 難しいパスワードでも、ウィルス感染すれば盗まれる
  - 毎回パスワードを変えると効果的

- パスワード漏洩、リプレイアタック対策
  - リスクベース
    - いつもと違うネットワークからのアクセスに注意を払う
  - ワンタイムパスワード
  - デジタル証明書（公開鍵暗号方式）
    - 秘密鍵が漏れない仕組み（ハードウェアで実現）
  - 携帯電話の活用

認証強化のメリット

- パスワード流出の可能性低減
  - 悪意によるもの
  - ユーザの不注意によるもの
  - セキュリティ意識の向上
    - 意図的に他人に教えてしまうこと（代理作業の依頼）の抑制
  - 共有アカウント（共有パスワード）の廃止
    - 認証と認可の分離により実現可能
- パスワード流出時の対応コストの低減
- 確実な本人認証を必要とするサービスへの対応

多要素(2要素)認証による安全性向上

- 2つの要素(モノと記憶など)が揃って初めて認証が成立
  - ICカード＋PIN
  - ICカード＋生体認証
  - セキュリティトークン＋PIN

などなど

http://rsa.com/company/news/releases/images/SID800&SID7002.jpg

http://www.nikkei.co.jp/topic5/2004newpro/yusyut.html

http://japan.rsa.com/node.aspx?id=1313

認証方式のいろいろ

- マトリックス認証
  - マトリックス自体が秘密、位置情報が秘密
- ワンタイム（使い捨て）パスワード
- 生体認証（指紋、静脈、…）
- 電子証明書

	1	2	3	4	5
1	5	0	G	T	V
2	A	3	E	2	R
3	8	D	K	P	U
4	Z	4	J	M	9
5	Q	F	L	X	7

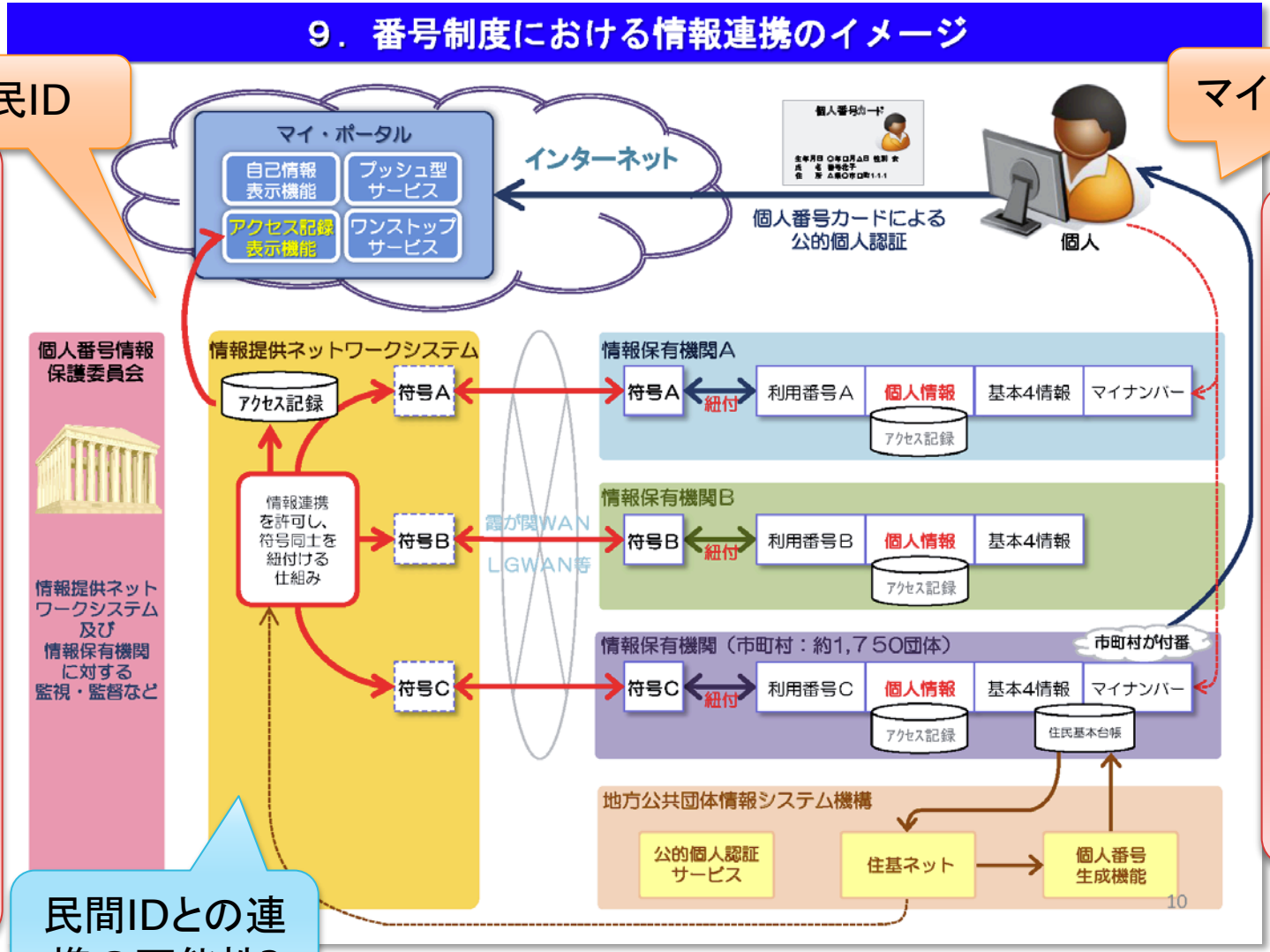
容易に導入できる要件

- 発行（登録）、配布コストが低い
- ユーザ操作が簡単
- 新たな持ち物が増えない（特殊デバイス不要、紛失しにくい）
- 特殊なソフトウェアが不要
- 利用場所を選ばない
  - 汎用、多用途なものが望ましい
    - 複数ドメインでも共有可能であればなお良い

ログアウトの重要性

- 高度な認証をしても、ログイン後に遠隔操作されては意味がない
  - ログアウト処理で、サービス利用の終了を宣言することは重要
- Webブラウザのサービスは、ブラウザを終了させる
  - サイト毎に仕様が異なるので、よく確認する
    - ログイン状態を保持する機能を有効にすると便利だけれど…
  - ポイントはクッキー
    - ブラウザのクッキーで同一端末かどうかを確認している
    - ブラウザーの終了によりクッキーが削除される

国民IDとマイナンバー



出典：マイナンバー法案の概要とシステムについて（社会情報流通基盤研究センター）
Source: http://asist.ssr.titech.ac.jp/wp-content/uploads/2abe.pdf

まとめ

- ネットワーク社会において個人認証は非常に重要
- パスワードには限界がある
- SSO技術に基づくIDフェデレーションの広がり
- より高度な認証技術の導入によるサービスの充実へ