

ネット社会の信頼性

—オンラインで安心して生きるために—

国立情報学研究所
トラスト・デジタルID基盤研究開発センター
佐藤周行

2025-10-15
@NII 市民講座

この時間、お話しすること

- 現代の生活はネットなしでは考えられません
- ネットという「基盤」が安心して使えるようになるにはいろいろな仕組みが必要です
- 技術的な保証
 - 今回、必要に応じて最低限のことはお話しします
- 制度的な保証
 - これが今回の中心的なテーマです
- 「ネット社会」と「実社会」には微妙なずれがあります。その「ずれ」にも注目して、どのような仕組みがネット社会で作られているのかを見ていきます

「実社会」とは

- 少し、オンラインとは関係ないことをしゃべりましょう
- われわれが実社会で（曲がりなりにも）安心して生活するためには何が必要でしょうか？
 - 生活のためのインフラには何があるでしょうか
 - 水道
 - 電気
 - ガス
 - 通信
 - 交通
 - インフラの維持に多くの努力が割かれています
 - 維持には多くの場合公共からの支出が当然とされています

公共からの支出をしぶるとどうなるか

- 1980年代、イギリスでは「サッチャリズム」のもと、多くのインフラを民間に払い下げて（維持整備の費用を）公共から切り離す試みがなされました
 - 大学も…
- 同時期、日本では「中曽根民活」のもと、同様の試みがなされました
- 日本では現状でも、インフラの維持整備費用を民間に任せる動きがあります
 - 鉄道は（東京に住んでいるとわかりませんが）いろいろ辛い状況に陥っています
 - 水道は、人口減少と相まって、現在苦境に立っています

根拠なしにいい加減なことを言っではいけないですね

● JR北海道の例

- 2013年以降、石勝線での重大事故（ATS未設置区間での脱線火災など）を契機に、安全管理体制の不備が露呈。
- 2016年、国土交通省が維持困難な線区リストを公表
 - 特に宗谷本線、留萌本線、根室本線で利用者減少と設備老朽化が深刻であることが指摘される
- このケースでは間に合って、「JR北海道グループ長期経営ビジョン未来2031」や「中期経営計画2026」の策定により、長期的な整備の覚悟が示され、現在は一息ついている

● 水道事業の例

- 「水道事業及び下水道事業の現状と課題」（総務省 2024）
 - 設備の老朽化と更新のための投資の不足、人口減少などで維持が困難になっていることが報告される

ネット社会のインフラ

- もちろん、ネットワークは重要な（インフラ）です。
- ずいぶん前から携帯電話網もそこに加わるようになりました
- インターネットに支えられる社会生活全般をネット社会と言うのならば、ネット社会は実社会を含む勢いを見せています
 - ネット社会限定のサービス等
- そこで「安心して」生活するには、何が必要でしょうか？
- ネットワークと言うインフラを維持するのは、ケーブルと交換機だけの問題ではなくなりました

ネット社会での「安心」とは

- もちろん、ネット社会でも法律は適用されますから、法律の守る範囲で安心して行動することができます
- 経済的自由（契約の保護）
- 基本的人権の保護
 - これが、ネット社会では別の意味を持ってきました

ネット社会の信頼はどう組み立てられているか

- たとえば、クレジットカードの番号をネットに流すなどと言うことは普通に行われているわけで、
- 番号を盗まれると、経済的な被害を被る可能性がありますから、これを送るときは、他人に見られない保証が必要です
- インターネットは、この点について非常に脆弱なアーキテクチャを持っていました
 - 盗聴を技術的に防ぐことができない
 - なりすましをする技術的なハードルが低い

TLSの保証

- ところででてきたのがTLS (SSL) という技術です
- インターネットでは、セキュリティを考えるとときに、以下のよ
うな仮定をおきます
「攻撃者 (adversary) はネットワーク上のすべての通信を傍受・改ざ
ん・再送・偽造できる」
- Dolev-Yao攻撃者モデル (1983年) と言います
- Yao先生は、ACMという学会でTuring賞と言う立派な賞をも
らっています。そこで写真を確認することができます

https://amturing.acm.org/award_winners/yao_1611524.cfm



MORE ACM AWARDS



A.M. TURING AWARD LAUREATES BY...

- ALPHABETICAL LISTING
- YEAR OF THE AWARD
- RESEARCH SUBJECT



ANDREW CHI-CHIH YAO

China – 2000

CITATION

In recognition of his fundamental contributions to the theory of computation, including the complexity-based theory of pseudorandom number generation, cryptography, and communication complexity.

SHORT ANNOTATED BIBLIOGRAPHY

ACM TURING AWARD LECTURE VIDEO

RESEARCH SUBJECTS

BIRTH:

1946, Shanghai, China

EDUCATION:

B.S. (Physics, National University of Taiwan, 1967); A.M. (Physics, Harvard University, 1969); Ph.D. (Physics, Harvard University, 1972); Ph.D. (Computer Science, University of Illinois Urbana-Champaign, 1975).

EXPERIENCE:

Andrew Chi-Chih Yao was born in Shanghai, China, on December 24, 1946. After moving with his family to Hong Kong for two years he immigrated to Taiwan. In 1967 he received a B.S. in Physics from the National University of Taiwan. He then started graduate studies in Physics at Harvard University, where he received an A.M. in 1969 and a Ph.D. in 1972 under the supervision of Sheldon Glashow, winner of the 1979 Nobel Prize in Physics. He subsequently entered the Ph.D. program in Computer Science at the University of Illinois Urbana-Champaign, and received his degree just two years later, in 1975. Yao completed his dissertation, *A Study of Concrete Computational Complexity*, under the supervision of [Chung Laung Liu](#).

TLSの特徴

- TLSはTransport Layer Securityの略です（誰かに聞かれたら教えてあげましょう）
- TLSは、Dolev-Yaoモデルの下で、相手と安全に通信するための手段を提供します
 - TLSは、通信を暗号化します
 - TLSは、相手の名前を識別することができます
- TLSのおかげで、クレジットカード情報や個人情報などの大切な情報をやりとりできるようになりました
- みなさんの身近にあるTLSとしてHTTPSがあります
 - HTTPS = HTTP over SSL (SSLはTLSの古い名前)

https://trustdigitalidcenter.jp/

https://trustdigitalidcenter.jp

トラスト・デジタルID基盤研究開発センター

ホーム ▾ 開発・研究 ▾ 標準・規格 ▾ 関連情報 ▾ 学認対応IdPホスティングサービス お問

目次

概要

認証の使命：インターネットトラスト実現のために

お知らせ

概要

NIIは、従来の認証事業（[学認](#)、[UPKI電子証明書発行サービス](#)、[!](#)）しつつ、学術・産業界からの認証基盤のより一層の利便性、安全性、トラスト・デジタルID基盤研究開発センターにおいて、学術生の学術活動の高度化を支援するための認証基盤技術の研究開発

- 産学連携を促進するID（アイデンティティ）基盤・認証認可
- 融合領域研究を促進するコミュニティ間連携強化技術の研究
- トラスト技術、デジタルIDに関係する広範囲にわたる研究開発
- 国際標準に準拠したトラスト・フェデレーション運用技術の研究

トラスト・デジタルID基盤研究開発センターを我が国における認証基盤の中心として、大学・研究機関のみならずベンダとの協働を促進し、

- これによって trustdigitalidcenter.jp というサーバと暗号化を通じて安全に通信できることを保証しています

- …本当？

実は、危険性は完全になくなったわけではなくて

- 技術的な攻撃にはいろいろありますが、特に以下のものが知られています
- trustdigitalidcenter.jpという名前のサーバと本当に通信できているのか？
- TLS通信では、「このサーバの名前はこれこれである」ということを証明するデータを使います
⇒サーバ証明書（聞いたことがありますか？）
- サーバ証明書はプログラムを使えば発行できるわけで…
- 悪い人が邪悪な目的でサーバ証明書を発行したらどうなるか？

ちなみに...

- サーバ証明書をみると
ですね...

全般(G) 詳細(D)

発行先

共通名 (CN)	www.trustdigitalidcenter.jp
組織 (O)	<Not Part Of Certificate>
組織単位 (OU)	<Not Part Of Certificate>

発行者

共通名 (CN)	GlobalSign GCC R3 DV TLS CA 2020
組織 (O)	GlobalSign nv-sa
組織単位 (OU)	<Not Part Of Certificate>

有効期間

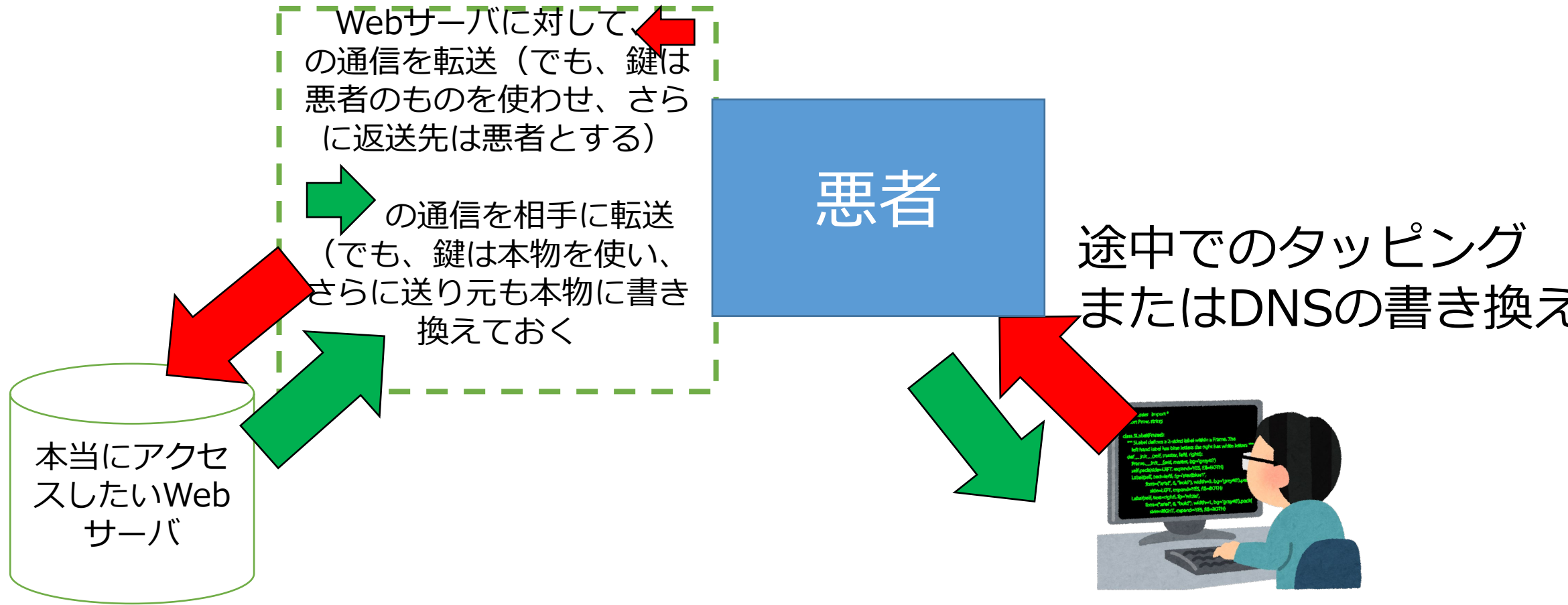
発行日	2025年5月9日金曜日 17:55:09
有効期限	2026年6月10日水曜日 17:55:08

SHA-256 フィンガープリント

証明書	b91341fc1e9cbcce6d803dcd6d625c54ec744d3185dc1c77d58b0 cebb98c7fe7
公開キー	60364e96b377a3872e298e4f9ca3e90e78c1fd833e6dcdada39a6c 3428da94ed

【中間者攻撃・MITM】

- (Man In The Middle Attack)



そんなことはありえない？

- サーバ証明書を発行する所が乗っ取られたり、勝手にサーバ証明書を発行したりすると、「名前の証明」が心許なくなってきました
- 「またまた～心配しすぎですよ」という声が聞こえる
- 過去の例：
 - 2011年Comodo社：発行側が乗っ取られて、Google等のサーバ証明書が不正に発行された
 - 2011年DigiNotar社：発行側が乗っ取られて、Gmail関係のサーバ証明書が不正に発行され、イラン国内でGmail関係の通信が傍受された（らしい）

解決のために

- これは暗号の構成の問題でTLSがDolev-Yaoの仮定に対して脆弱（ぜいじゃく）というわけではないのですが
- 「では、サーバ証明書の記載内容を社会的に保証しましょう」という方向に進むのが「インフラ」です
- 保証するには以下が必要です
 - 発行元のセキュリティの確保（悪者が侵入できないようにする）
 - 発行に際しての発行先の身元の徹底的な審査
 - Google以外の会社にGoogleに関係した証明をするのは社会的な信頼を損ねる

PKI

- このように作られたのがPKIです
Public Key Infrastructure
- 具体的にどう運用されているか（ブラウザの視点）？
 1. ブラウザベンダーは、「信頼できるサーバ証明書発行機関」のリストを作ります
 2. ブラウザベンダーは、そのリストをブラウザが参照できるようにし、サーバ証明書を見るたびに、それが「信頼できる機関」から発行されているかどうか確認します
 3. 確認されたら、通信することにOKを出します
 4. ブラウザベンダーは、定期的にアップデートをかけます。その時点でリストが更新されます

PKIの実際

- 発行側はこうです
 1. サーバ証明書で「証明する範囲」を決めます
 2. その範囲内で、発行を求めるところを審査します
 3. 審査に通ったらサーバ証明書を発行します（有効期限付き）
 4. 何らかの理由で有効期限が切れる前に事項が証明できなくなったらその証明書の有効性を取り消します。有効性が取り消された証明書のリストを作って公開します
 5. 定期的に監査を受け、自分たちの運用が正しくなされていることを外部に主張します
- 大変な努力で維持されている「インフラ」なんです
 - 発行側の努力
 - ブラウザ側の視覚化

ブラウザ

- ブラウザも、インフラ的な性格を持つソフトです
- ブラウザを使ってサーバにアクセスする
- ブラウザを使ってデータをダウンロードする
- ブラウザを使って (Javascript) プログラムを実行する
- ブラウザを使って…
- 現在、ブラウザを作る (リリースする) ことができる会社は限られています
 - 仕様が膨大になり、体力のないところに対応できない
 - Chrome, Edge, Safari

ところで

- 「信頼できるサーバ証明書発行機関」をPKIの言葉では Certification Authority (CA)
- この「Authority」というのが、今日のもう一つのキーワードです
- ところでPKIは、セキュリティ分野に属すると思いますか？
- 答えは半分YESです

PKIをどのような面から論じるか

- 使われている暗号は安全ですか？
- 通信プロトコルとしてのTLSは安全ですか？

- …のような、技術的な安全性を論じるのがセキュリティです
- 一方、今までお話ししてきた話はそういうこと（だけ）ではなくて

- そのCAは信頼できますか？
- ブラウザはその信頼を反映していますか？

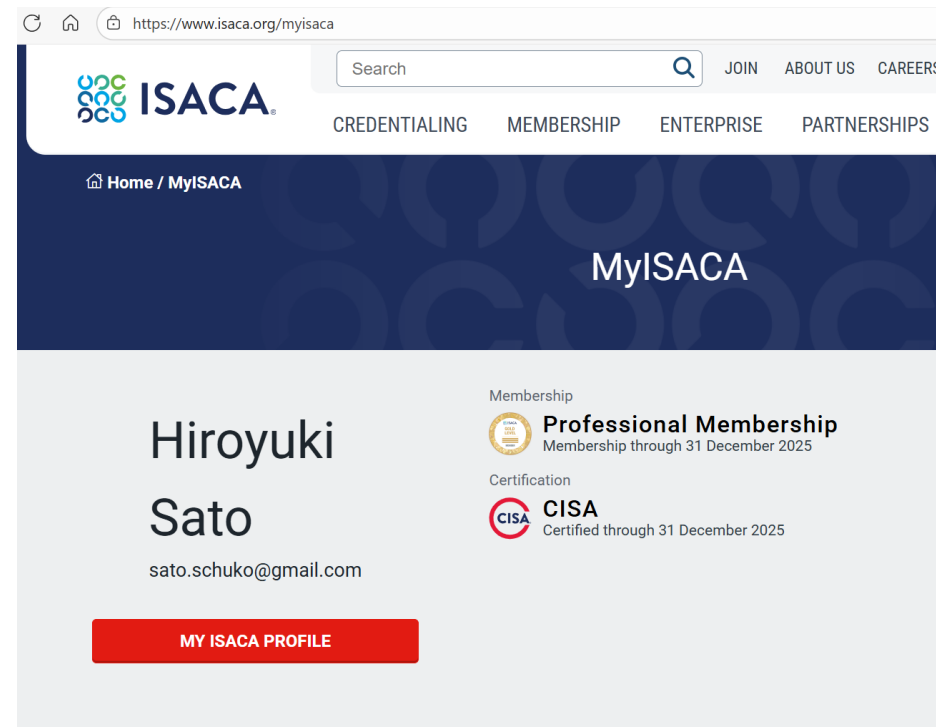
- という「信頼できるという判断」がテーマになってきました

ネット社会におけるオーソリティ

- 「信頼の起点」を「トラストアンカー」といったりします
 - （向きが逆？）
- 実社会でも、まったく同じ仕組みが動いていることが想像できますか？
- 「オーソリティ」
 - 色々な意味がありますが、ここでは「専門家や公共機関など、信頼のおけるなにか」
 - 行政機関はオーソリティのひとつです「当局」（この訳語が割り当てられた場合、主に警察機関のこととして使われます）

オーソリティの作り方

- 民間のオーソリティもあります
- 試験を行って、資格を与える機関は「オーソリティ」として働かないと、その資格の価値が認められません
- たとえば、佐藤は以下の資格を持っています。監査業界では、国際的な資格として一定の権威を認められています
- 民間団体なんですが…
 - 右は <https://www.isaca.org/>



The screenshot shows the MyISACA profile page for Hiroyuki Sato. The page includes the ISACA logo, a search bar, and navigation links for JOIN, ABOUT US, CAREERS, CREDENTIALING, MEMBERSHIP, ENTERPRISE, and PARTNERSHIPS. The profile section displays the name Hiroyuki Sato, the email address sato.schuko@gmail.com, and two credentials: Professional Membership (valid through 31 December 2025) and CISA Certification (certified through 31 December 2025). A red button labeled 'MY ISACA PROFILE' is located at the bottom of the profile section.

オーソリティの作り方

1. 権威を持っている「専門家」が集まる
 1. たとえば、システム監査資格、会計監査資格。
 2. ある事柄について「こうあるべきだ」という基準を作る
 3. 自らが、それについて「権威」であると内外に主張する
 1. コミュニティの支持が必要。会計監査資格は国の保証がある
 4. 対象が、その基準を満たしているかどうかを自ら判定する
 1. 資格試験はその有力な方法のひとつ
 5. 基準を満たしていると判定したら、その判断を「認定」(Certification) として、公表する
- これらが社会のインフラの一部として機能しています
 - 「認定」は、社会生活のコストを下げる有力な手段です

PKIについてもCertificationはあって

- Certification Authorityが満たすべきセキュリティ基準、運用基準が定められています
 - CA/Browser Forum Baseline Requirement
 - 主要ブラウザベンダは、「信頼できるCAのリスト」を作るとき、CAがこの基準を守り、認定されていることを強制します
 - これは「業界団体」が強制力を持つ認定を行う典型的な例です
- この運用と監視が結構厳しくて…
 - NIIは大学向けに電子証明書の発行を行っていますが
 - 結構気を遣って運用しています
 - このピリピリした運用は「トラスト業務」の本質的な性質の一つでしょう

クレジットカード業界にも認定はありまして

- PCIDSS (Payment Card Industry Data Security Standard)
- クレジットカード大手5社が定める、CCを扱うサービス提供業者が順守すべきbaseline requirement
- これも、認定を出します
- 大手のEC企業はほとんどこの認定をとっています

ところが…

- Amazon(物販部門)は実は準拠を唱っていないわけですが、決済基盤を自分で持っているところは、ビジネス上別の戦略があるのかもしれない

小さめのところでも

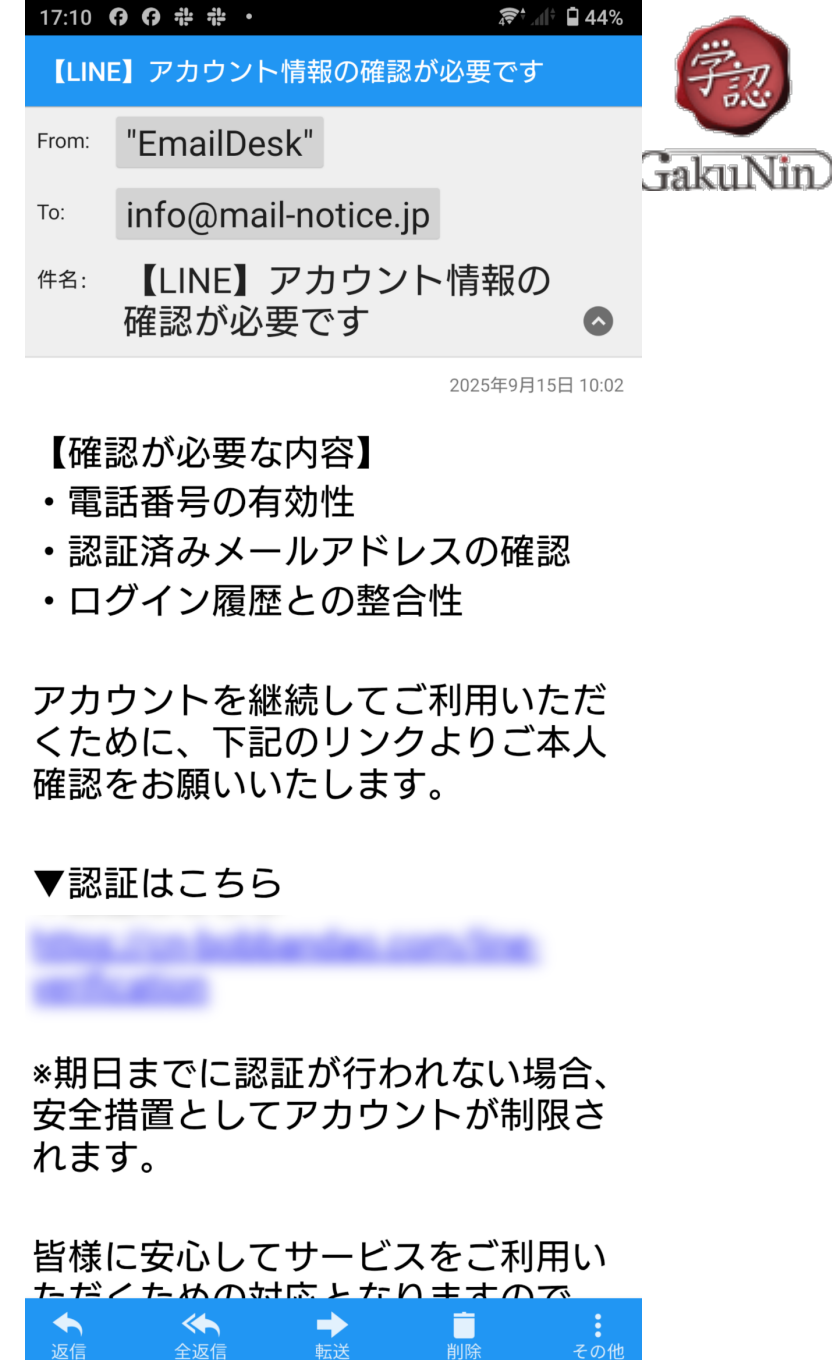
- 日本酒の等級は国税庁が認定します←国の関与大
- さっきのISACAという団体は、シカゴに本拠を置く民間団体です
 - 監査に関係する人たちのコミュニティが権威を認めている
- 「権威」という意味でいつも引き合いに出されるものとして「モンドセレクション」がありますが
 - 認定の詳細はよくしりませんので、これ以上の発言を控えます

インターネットトラスト

- インターネットで、この手の「オーソリティ」はどれくらいあるか？
 - 後で典型例をいくつかあげましょう
- インターネットの中で、「オーソリティ」を起点として、人間やシステムが他を信頼するようになるシステムを「インターネットトラスト」と言います
 - PKIはその典型例です
 - ログインの認証に関係するトラストは最後にお話しします
- 「最後は信じるしかない」というのがトラストですが、その度合いを高めるための方法論はいろいろ提案されています
 - 監査

それをかいくぐる動き

- 「フィッシング」ってご存知ですか？
- 「トラスト」の観点（インターネットに限らず）から、フィッシングを見てみましょう。
- 最近では、Webメール系のものはフィッシングメールを自動的に削除するものが多く、あまり観察できません。携帯メールはフィッシングの巣窟かなあ…（私の場合）



シャレにならなかつたのが2025年の証券業界

← → ↻ https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html



文字サイズ

サイト内検索

ホーム	金融庁について ▼	報道・広報 ▼	政策・審議会 ▼	法令・指針等 ▼	金融機関情報 ▼
-----	--------------	------------	-------------	-------------	-------------

[ホーム](#) > [報道・広報](#) > [金融庁からのお願い・注意喚起](#) > インターネット取引サービスへの不正アクセス・不正取引による被害が急増

✕ **ポスト**

令和7年4月3日
(令和7年9月8日更新)
金融庁

インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています

- 実在する証券会社のウェブサイトを使った偽のウェブサイト（フィッシングサイト）等で窃取した顧客情報（ログインIDやパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

オンラインでの不正取引件数（2025）

	2月	3月	4月	5月	6月	7月
不正取引アクセス件数	97	2320	5424	3342	1794	1055
不正取引件数	34	935	2986	2383	870	894
不正売却(億)	0.8	175	1558	1124	226	250
不正買付(億)	0.8	147	1366	1008	173	223

https://www.fsa.go.jp/ordinary/chuui/chuui_phishing/20250908.pdf から一部引用

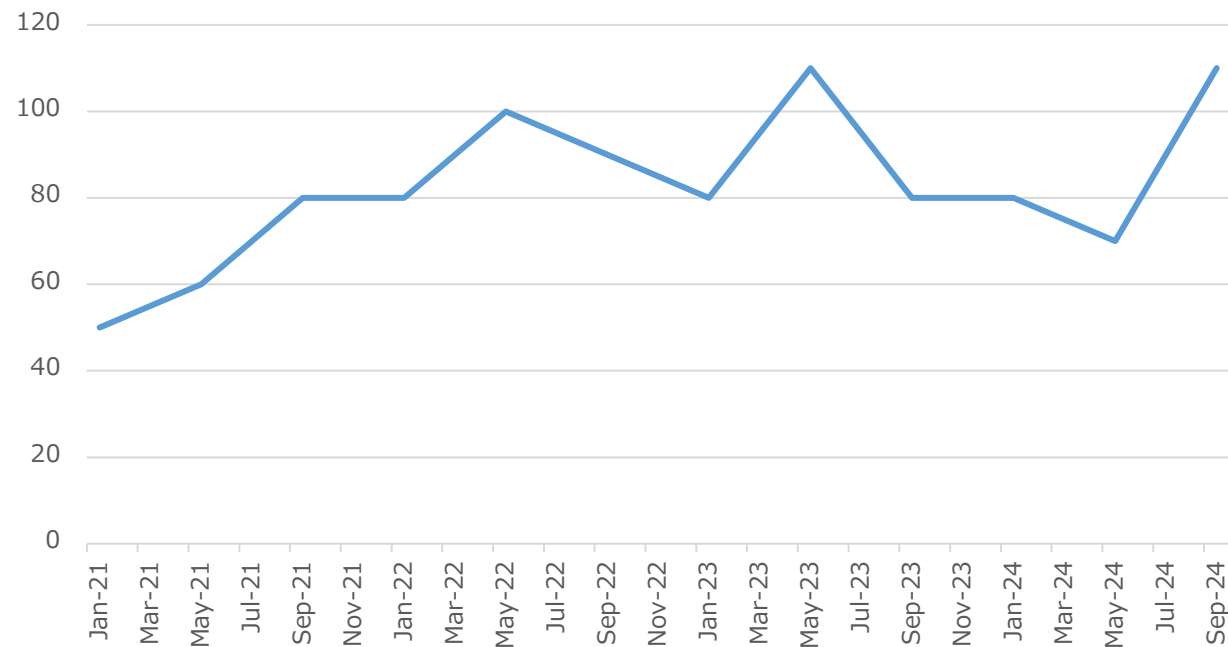
フィッシング対策協議会のレポート

- フィッシング対策協議会が毎年発表している「フィッシングレポートxxxx」を見ると、フィッシングの動向を理解することができます
 - フィッシングレポート2025は
https://www.antiphishing.jp/report/phishing_report_2025.pdf
で公開されています。
 - その中の「国内のブランド名を悪用された企業の件数」に注目してみます。

ブランド名を悪用された企業の件数

- 「フィッシングレポート2025」の「図1-3国内のブランド名を悪用された企業の件数」をもとに計算

ブランド名を悪用された国内企業数



フィッシングを技術面からみると

- フィッシングは、技術的には「ブラウザが便利すぎる」という機能上の欠点、「メールが（メールアドレスを持っている）誰にでも届く」という機能の本質をついてきます
 - 最近では、ブラウザでURLをクリックしてもすぐにはそのURLにジャンプしない仕様になってきました
 - 現在のほとんどのWebメールは「あやしい」と判断したメールを自動的にゴミ箱にいれたり、勝手に削除したりします
 - 送信元の拒否リストも運用されています
 - 送信元に、「ちゃんとした」サイトであることの証明を求めることもはじまりました（DMARCって聞いたことがありますか？）
 - メール上でのURLのコピーや貼り付けにも制限がかかりはじめました

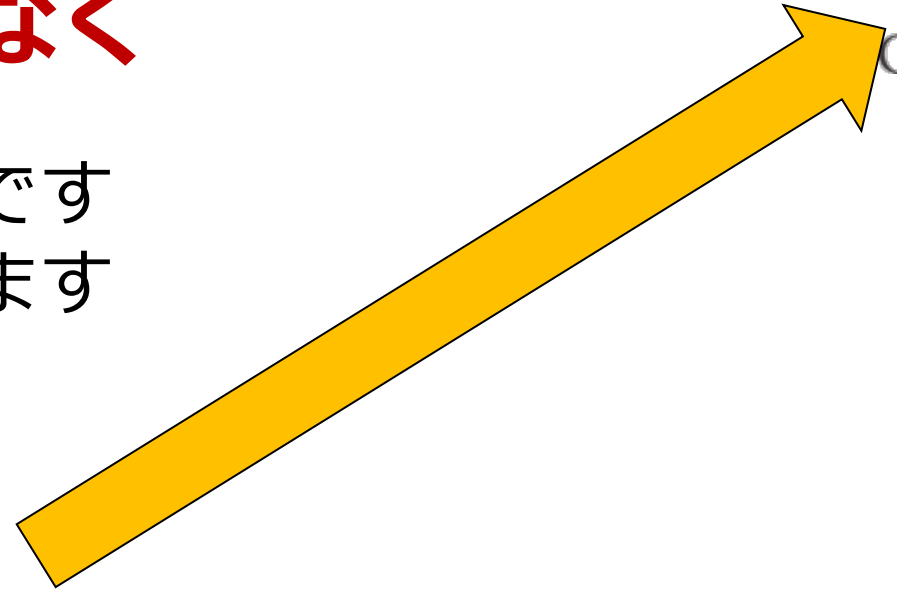
フィッシングを心理面から見ると

- 「メールの文面を信じてしまう」ように仕向けられると、もうそれはフィッシングの入り口
 - 忙しい、眠いなどで、判断力が低下している
 - 文面がそれらしい
 - 安心できそうな会社のプレミアムなサービスをうたっている
- この「安心できそうな」というのが、その会社が長年培ってきた社会的な信用です（評判）
- フィッシングは、社会の信用（トラスト）の体系にただ乗りするのが基本です
- PKIのような技術でサポートされているものをかいくぐり、人間の行動にそのまま訴える作戦をとります

手をこまねいているわけではなく

- 「信頼」を端的に表現するのがロゴです
- ネット上の詐欺によく使われたりします

- 佐藤が関係するサービスのロゴです
- ロゴは登録することができます（NIIが登録商標しています）
- 登録した上で、利用条件を課すことができます



▶ 関連情報

▶ 学認ロゴや商標の利用に関するご案内

学認ロゴや商標の利用に関するご案内

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
平成24年12月10日

学認ブランド使用ガイドライン Ver1.1

本ガイドラインは、大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（以下、「NII」といいます）が所有する「学認」に係るロゴおよび登録商標（以下、「学認ブランド」といいます）の非独占的な使用許諾の範囲、使用方法、使用許諾対象となる学認ブランドおよびガイドラインの変更等について説明するものです。NIIは、次の条件のもとにおきまして、大学、研究機関等に属する学術関係者および学認にSPを登録する機関（以下、「学術関係者等」といいます）ならびに学術関係者等以外のその他の使用者（以下、「その他の使用者」といいます）に対しまして、学認ブランドを無償で使用することを許諾いたします。

ロゴを保護するための証明書

- ネット上で「ロゴ」を保護する、または利用者が登録者であることを証明することをやり始めるようになりました
- VMC (Verified Mark Certificate), CMC (Common Mark Certificate) の2種類があります



- メールで顕著
 - 業務上のメール（会社からの送信）であることを証明するために、ロゴ込みの証明書を貼付することができるようになりました（Gmailで対応済み）
 - ⇒これがフィッシング対策にきけばよいのですが…
- Xでも、本人確認マーク（青い、例のやつ）は昔からあるわけで

普通のWebサイトにログインする場合でも

- ログインしている人が本人かどうかの問題は古くから指摘されてきました
- 本人なのに他人を装う、匿名で行動する、等々
- 「裏垢」「捨て垢」などの俗語があります
(佐藤はほとんどやらないのですが) SNSでは大きな問題になっているようで…
- 「裏垢誤爆」なる言葉もこのスライドを作る過程の調査で知りました
- 少し真面目な話をしましょう…

ショッピングサイトや研究用サイトでは

- ショッピングサイト：
 - 誰でもアカウントを作っています…
 - クレジットカード登録してね
 - ⇒そのクレジットカードを使う人がアカウントを作った人であることの確認が必要（経済的な被害の場になるのはショッピングサイトは好みません）
 - ⇒じゃあ、携帯の番号も登録してください。ログインする場合はその携帯にワンタイムPWを送ります
- SNS
 - 誰でも登録しています
 - PWが破られて、他人が自分になりすまして変なこと書くのはいやでしょう？（SNSサイトは無用のトラブルに巻き込まれたくありません）
 - ⇒携帯番号を登録して下さい（以下同様）

銀行はこれらと本質的に異なります

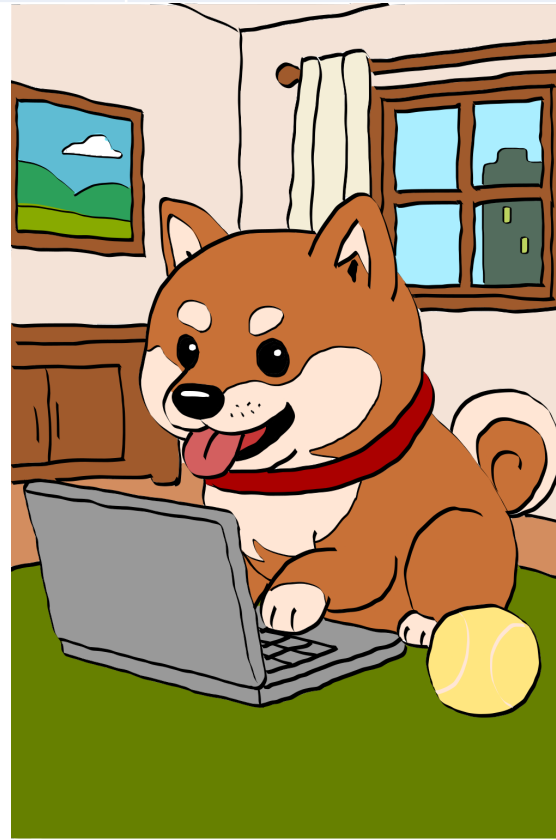
- 銀行はAML（Anti Money Laundering）法で厳しく規制されています
- 誰でも口座を作れるか？
 - 本人書類（Identity Document）を身元確認に用います⇒提出を要求されたことがあると思います
 - 銀行はそれをもとに以下に代表される審査を行います
 - 口座数の調査（一人で複数の口座を持っていると、それだけで怪しまれる）
 - 金融犯罪歴（口座の売買、口座を通したML等金融犯罪等）の調査
 - 審査に通ると口座開設が認められます
 - 口座を使って取引を行う場合、特にオンラインの場合はパスワードだけで取引を認めることはありません（ワンタイムPW、マイナカードの提示などを求められることがある）

教育研究用のサーバの場合

- 銀行ほどではないですが
- 大学では、学内のリソースを学外者が使うのは禁止です
 - 誰が「学外」かはともかくとして
- 大学では、入学試験からつながる本人の身元確認の徹底がなされています
 - 高校の成績書の書き方は文科省の強い指導下にあります
 - 高校の運用について、社会的に強い信頼があります
- その上で、成績の閲覧等シェアにならない機微データが多くあるので、多くの大学ではパスワードのみでのログインを認めない傾向にあります
 - まだ、パスワードのみでのログインを許容している大学はもちろんあります
 - スマホが普及した今、ログイン強化のハードルは劇的に下がりました

まとめると

	SNS	オンラインショッピング	大学	銀行
身元確認	緩くてOK	緩くてOK	きつい（高校から）	とてもきつい（AML法の要請）
ログイン時当人確認	緩め⇒きつめに推移（トラブル防止）	きつめに推移（CCの保護）	きつめに推移（成績データ等の保護）	とてもきつい（金融資産の保護）



サービスの対象者が本人かどうかわからない（犬の可能性を排除できない⇒インターネットドッグなどといったりします）ことを排除する必要性とその度合いはサービスによって異なります

最近のIT環境では

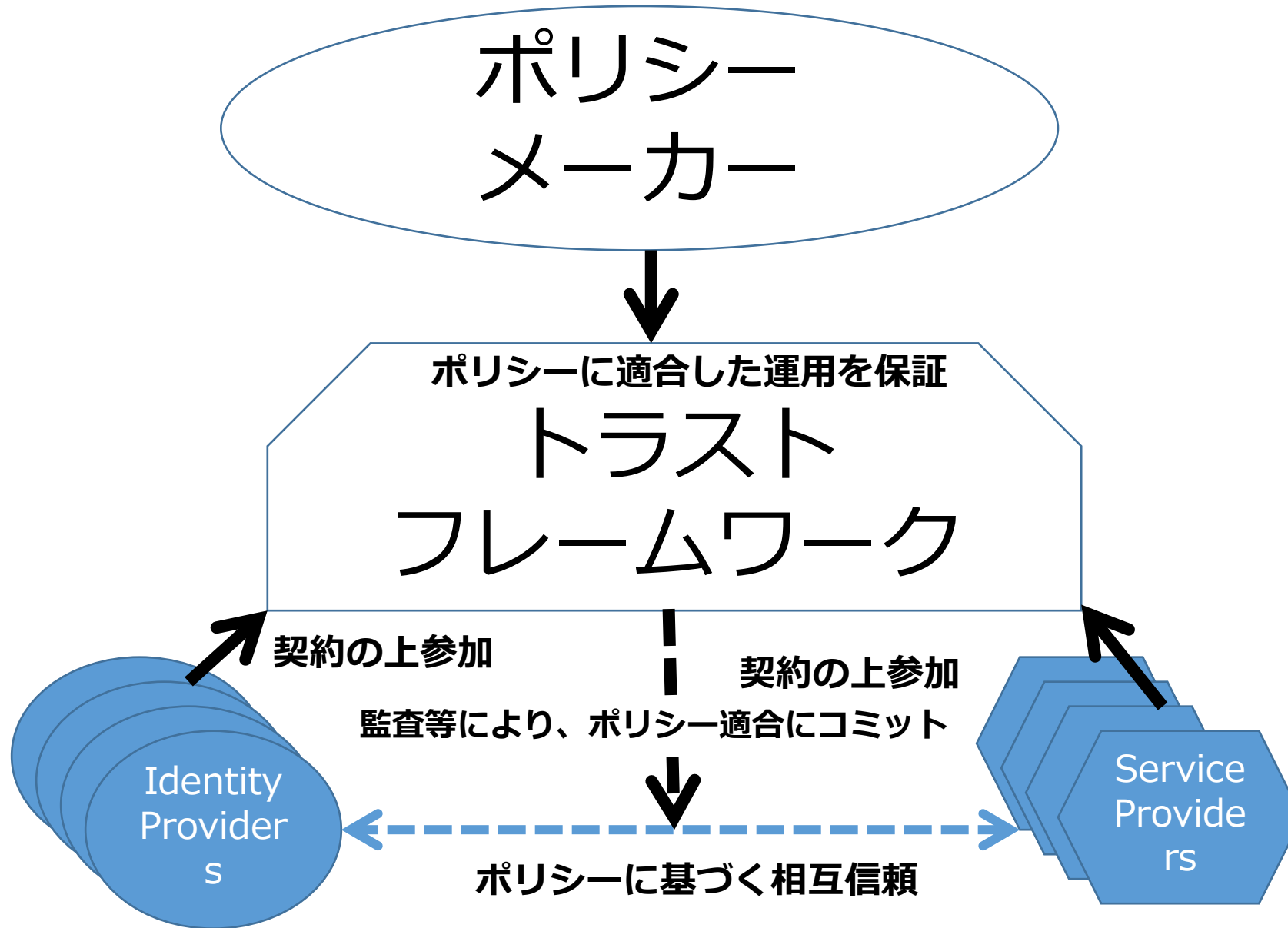
- サービスのログインに際して、他のアカウントでログインすることを許すことが当然になりました
 - 当日、例を出すことが許されれば、実演します
- 大学でも、一回ログインすれば、学内のリソースを再度ログインすることなく利用可能にしていることが多くなっています
 - 成績閲覧
 - LMS
 - ...
- (注意) Google, Apple, MSでは、自分たちでツールを提供し、そこにアカウントでのログインを要求することが多くあります。仕組みは同じですが、大学の場合は、別々に作られたサービスまでを統合して利用可能にすることが多くあります

IdP (CSP)

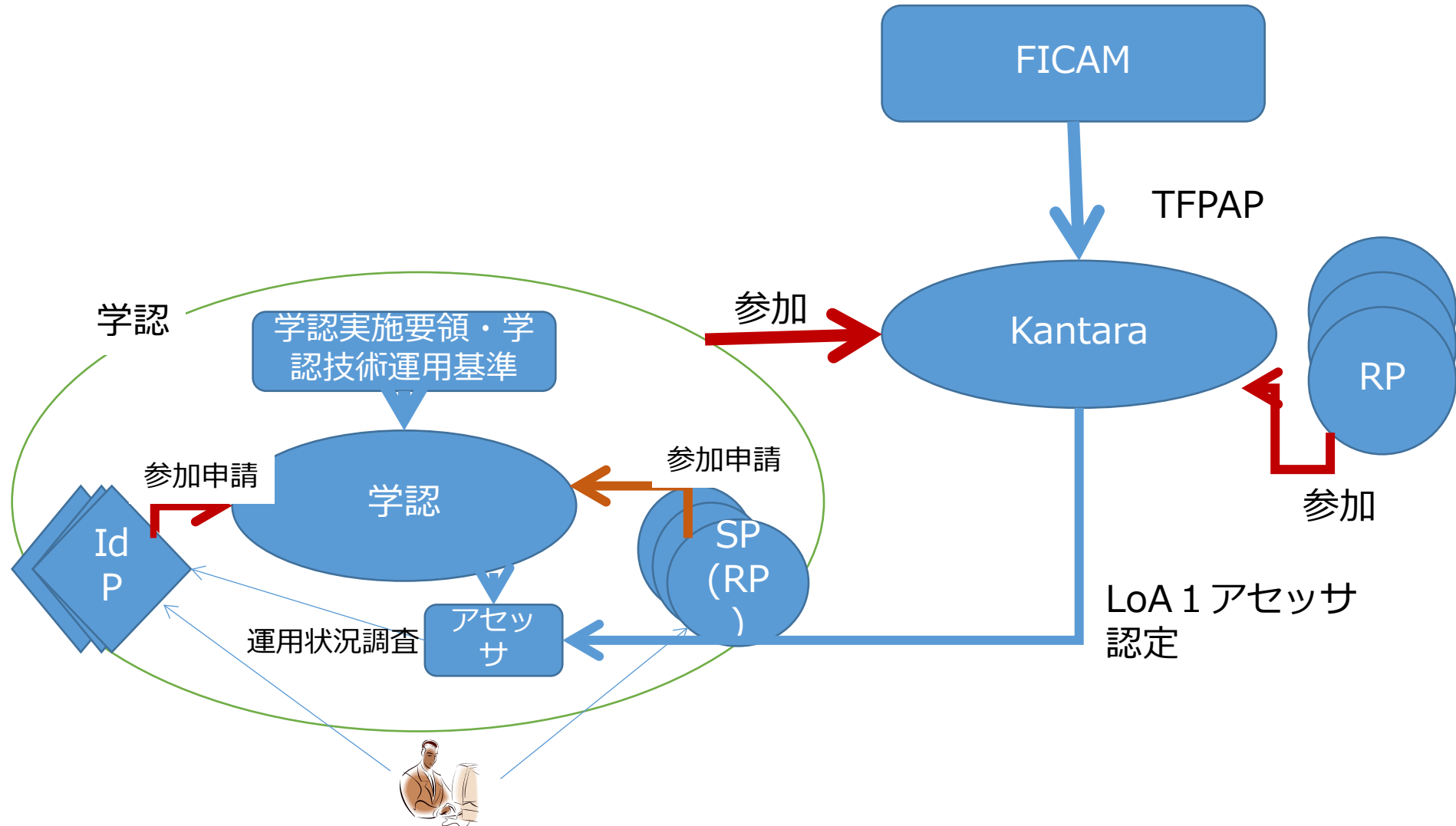
- ところででてきた考えが「ログインとサービスの分離」です
- アカウムの運用保守は一か所で（サービスごとにアカウントを作って運用するのはコストもかかるし面倒だ）⇒Identity Provider (IdP), 又は Credential Service Provider (CSP)
- サービス側は、ログインの管理をアカウントの運用を行っているところに明け渡すことになります
- ⇒アカウントの管理はちゃんとしているんでしょよね（当然の疑念）
 - アカウムの運用する側だって、「サービスで変な情報を抜き取っていないでしょよね」
 - 学外のサービスを利用するときは特に
- これらの疑念を払拭することが求められました

方法論

- アカウムの運用についてのポリシーを定めます
 - アカウムの持つ人は学内に限る
 - 人事DBや学務DBのデータを上流として機械的に作る（作成更新削除）
 - サービスの運用についてのポリシーを定めます
 - 個人情報の取り扱いについて
 - その他、データのセキュリティ管理について
 - これらのポリシーを参加予定者に見せて、賛同する所と契約を結びます
 - ポリシーが守られていることを、定期的な監査を行うことで保証します
- ⇒このようにつくられた制度を「インターネットにおけるトラストフレームワーク」と言います



国際標準への参加



まとめの言葉

- インターネットで「信頼」を作っていくには、セキュリティ技術に支えられた「信頼する」という行為が必要になります
- PKIをその典型としてとりあげました
- 信頼をすり抜けるフィッシング対策にも、PKIが使われるようになりました
- アカウントの管理が他と分離されるサービス形態が普通になり、「アカウントの品質」の問題を「トラストフレームワーク」で解決しようとしてしました