

前回(第10回)
「暗号技術とセキュリティ」より

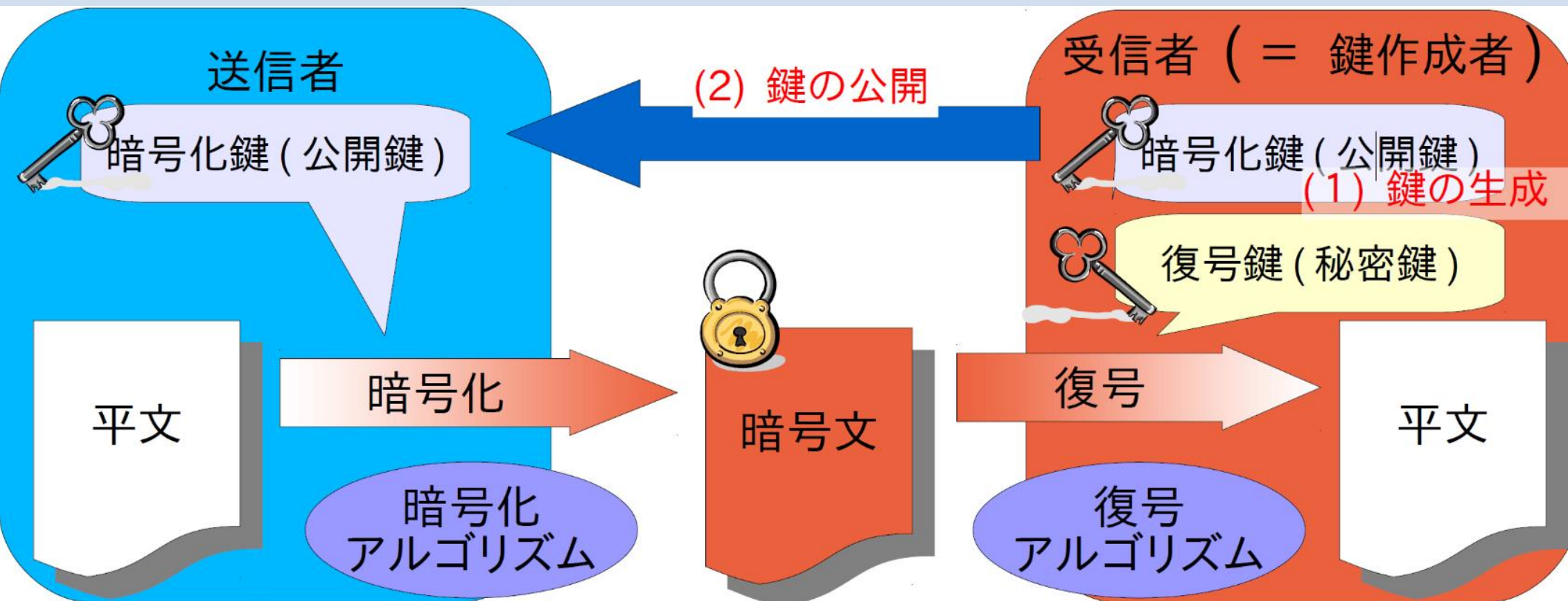
公開鍵暗号

- Stanford 大学 Whitfield Diffie, Martin Hellman が提案 (1976 年)

公開鍵

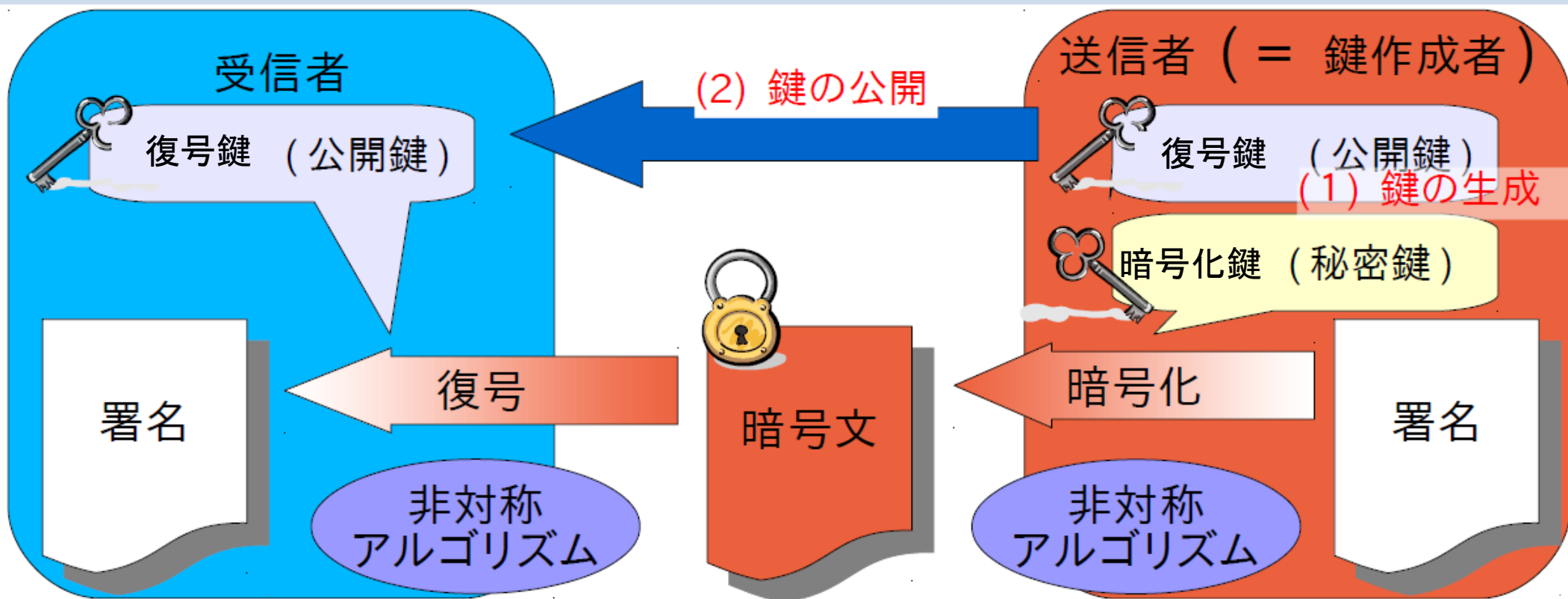
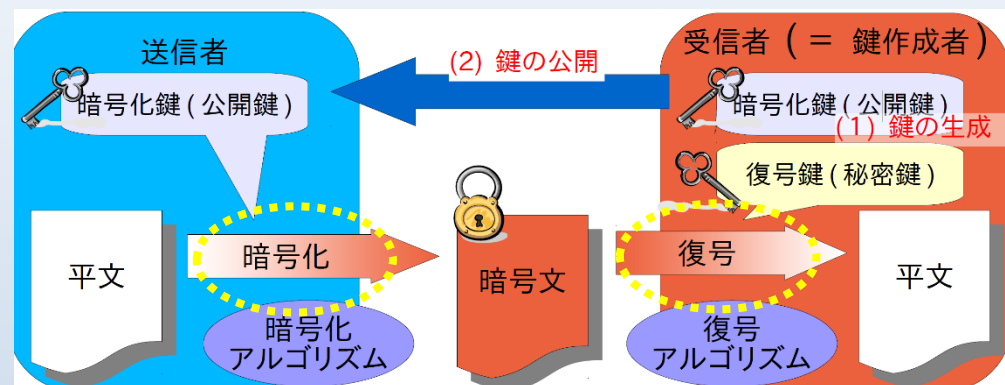
秘密鍵

- ペアになる鍵を作成, 一方を公開, 他方を保管
- 一方の鍵から他方を推測できない



電子署名

- 公開鍵暗号の(逆向き) 使用
 - 秘密鍵で暗号化
 - 公開鍵で復号
 - 組み合わせが不正なら復号不能



セキュアハッシュ関数

- 元データ全体に電子署名せずにダイジェスト化
 - 任意の桁数のデータから、一定の桁数のデータを出力する事が出来る。(ハッシュ値)
 - 出力されたハッシュ値から、元のデータを取り出す事は出来ない。(復元出来ない)
 - 元データのごく一部だけが変更された場合でも、出力されるハッシュ値は大きく変化する。
 - 違う元データから同じハッシュ値が出力される可能性がごく低い。

→ ダイジェストに電子署名してやれば良い

- MD5 RSA Security 社
- SHA-2 米国標準
- RIPEMD160 ヨーロッパ標準 など



情報セキュリティと情報倫理

第11回

さまざまな認証技術

(参考書: 11 情報セキュリティの基盤技術「暗号」
12 暗号と認証を支える制度)

2022/12/16

さまざまな認証技術

- 議論

- パスワードを用いた認証プロトコルや生体認証, 多要素認証などを用いた高度な認証技術 (シラバスより)

- 参考書

- 11.情報セキュリティの基盤技術「暗号」
- 12.暗号と認証を支える制度
 - 特に「2.認証」と「3.認証と暗号」

認証とは

- 対象となっている人や物が、あらかじめ設定された資格を有しているかどうかを確認すること
 - パソコンやスマホを利用している人が、想定された正規の利用者であるか
 - 接続されている機器類が、想定された正規の機器であるか
- アカウント名 (ID) とパスワード
 - 利用者が何者 (ID) であるかを伝え、サービス提供者に確認 (パスワード) させる

利用者: **被認証者**

サービス提供者: **認証者**

認証の目的

- 主体認証
 - 個人や機器そのものを認識する認証
 - 本人確認
- 属性認証
 - 被認証者の資格や属性を確認
 - たばこ自販機で身分証明書などの提示
→ 年齢確認が目的

識別子と認証要素

- 識別子
 - ID, アカウ^ント名, ログイン名, ユーザ名, 会員番号
 - メールアドレスで代用される場合もある
 - 通常は秘密にする必要はない
- 認証要素
 - 代表的なものとしてパスワード

認証者は識別子と認証要素の組を知っている必要がある

→ 認証リポジトリ

利用者認証の方法

- 認証要素

- 知識認証：被認証者だけが知っている固有の知識
 - パスワード, 暗証番号, 公開鍵暗号における秘密鍵, 「秘密の質問」の答え, ジェスチャーなど
- 物体認証：被認証者だけが所有しているとされる物体
 - IDカード, 物理的な鍵, ハードウェアトークン, 印鑑など
- 生体認証：被認証者本人固有の特徴
 - 顔, 声, 指紋, 静脈などの生体情報など

- 認証の厳密さと利用しやすさはトレードオフの関係

- 認証1つのみだと権限がない人に認証してしまう可能性が高くなる
- 複数の方法を組み合わせる認証を義務化すると使い勝手が悪くなる

認証技術

検査符号

- データが正しいか確認するために、データに付加する別データ
 - パリティビット
 - 7ビットのデータに対して1の個数が偶数(または奇数)になるように追加する1ビットのこと
- 0100110 → 0100110¹
- 1011001 → 1011001⁰

検査符号

- チェックサム
 - いくつかの「値の並び」のデータに対して、すべてを加えて256で割った余り(2進数で下位2桁)の値
- チェックデジット
 - データからある方法で計算した結果の数字や文字
 - バーコードの例



一方向性関数・ハッシュ関数

- 一方向性関数

- 次の性質を満たす関数 $h(x)$

- x の値から $h(x)$ の値を求めることは容易
 - $h(x)$ の値から x の値を求めることは困難(事実上不可能)
 - $x_1 \neq x_2$ ならば $h(x_1) \neq h(x_2)$ がほとんどの場合に成り立つ
 - 任意の x に対して「 $h(x) = h(y)$ を満たす y が存在するか判定したり、そのような y の値を求めることが困難(事実上不可能)」である

- ハッシュ関数

- 上記の性質に以下を追加

- $h(x)$ は定義域に対して値域が(とても)小さい

MD5

- 任意の長さのデータに対して計算することができる128ビット(16進数32桁)のハッシュ値
- 一文字違ってもMD5の値は全く異なる
 - MD5(The Open University of Japan)
= 18D08D27 002B1F7D C6577240 1904A4A8
 - MD5(The Open University **O**f Japan)
= 9CEFE4A7 214122DB AD9F43E9 35047284
 - MD5(The Open University **fo** Japan)
= BDEDAB15 575D9C55 A8D57290 65202393

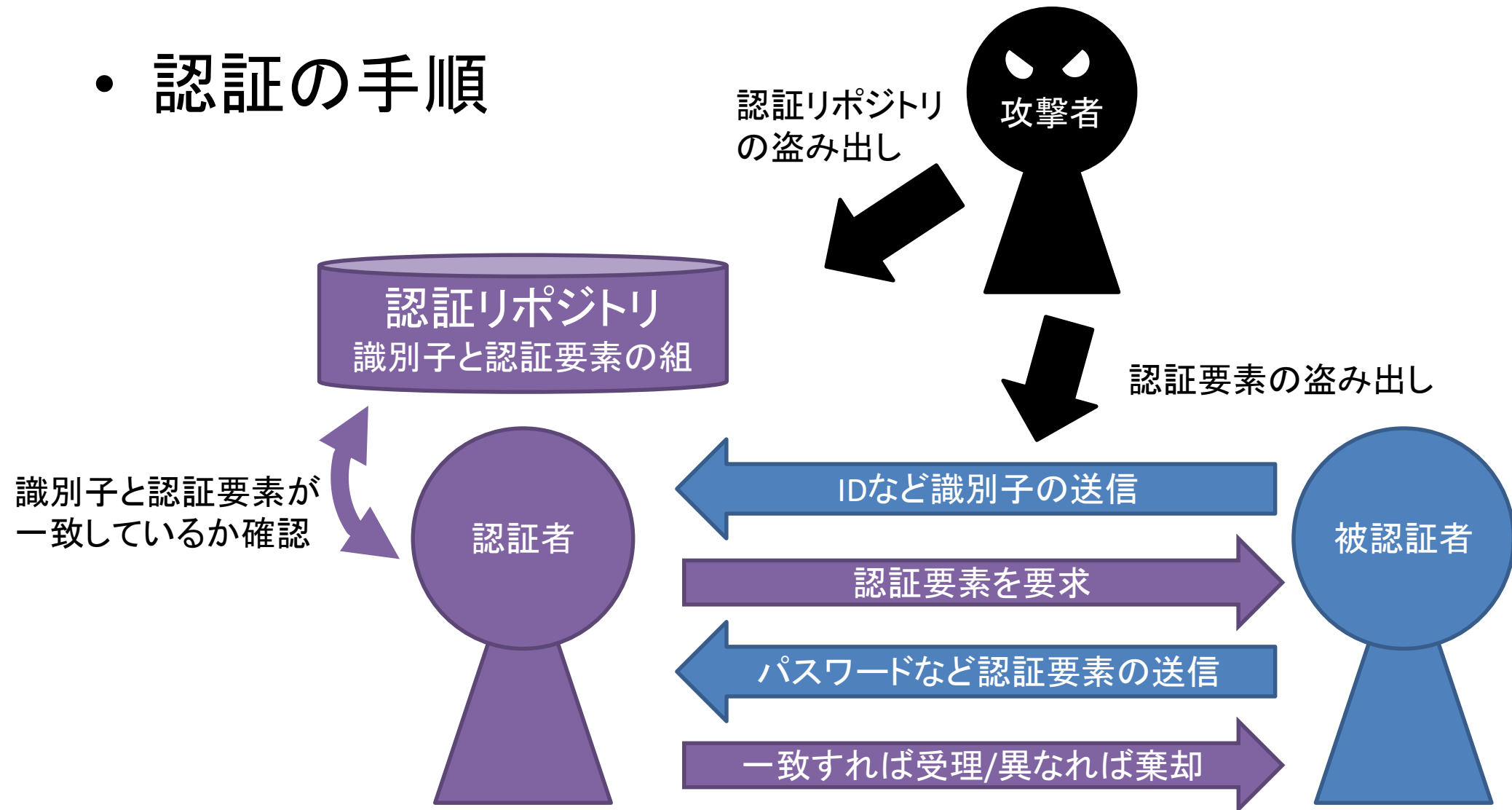
認証とハッシュ値

- パスワード認証の場合
 - 利用者がパスワードを設定
 - 利用者がパスワードを考えて入力
 - システムはそのパスワードのハッシュ値のみ保存
 - 利用者がパスワードを入力してログインするとき
 - 利用者がパスワードとしてある文字列を入力する
 - システムはその文字列のハッシュ値を計算しシステムに保存していたハッシュ値と比較
 - 一致すれば正しいパスワードを入力したとみなす
- 情報漏洩があってもハッシュ値のみのためパスワードそのものの流出を避けることができる

認証プロトコル

認証プロトコル

- 認証の手順



認証プロトコルへの攻撃対策

- SSL (Secure Socket Layer)
 - Web (https) などでの利用
 - 通信路の暗号化
 - IDとパスワードを直接認証者と被認証者との間で通信しても盗聴される危険はない

SSL/TLS 技術

(Secure Socket Layer / Transport Layer Security)

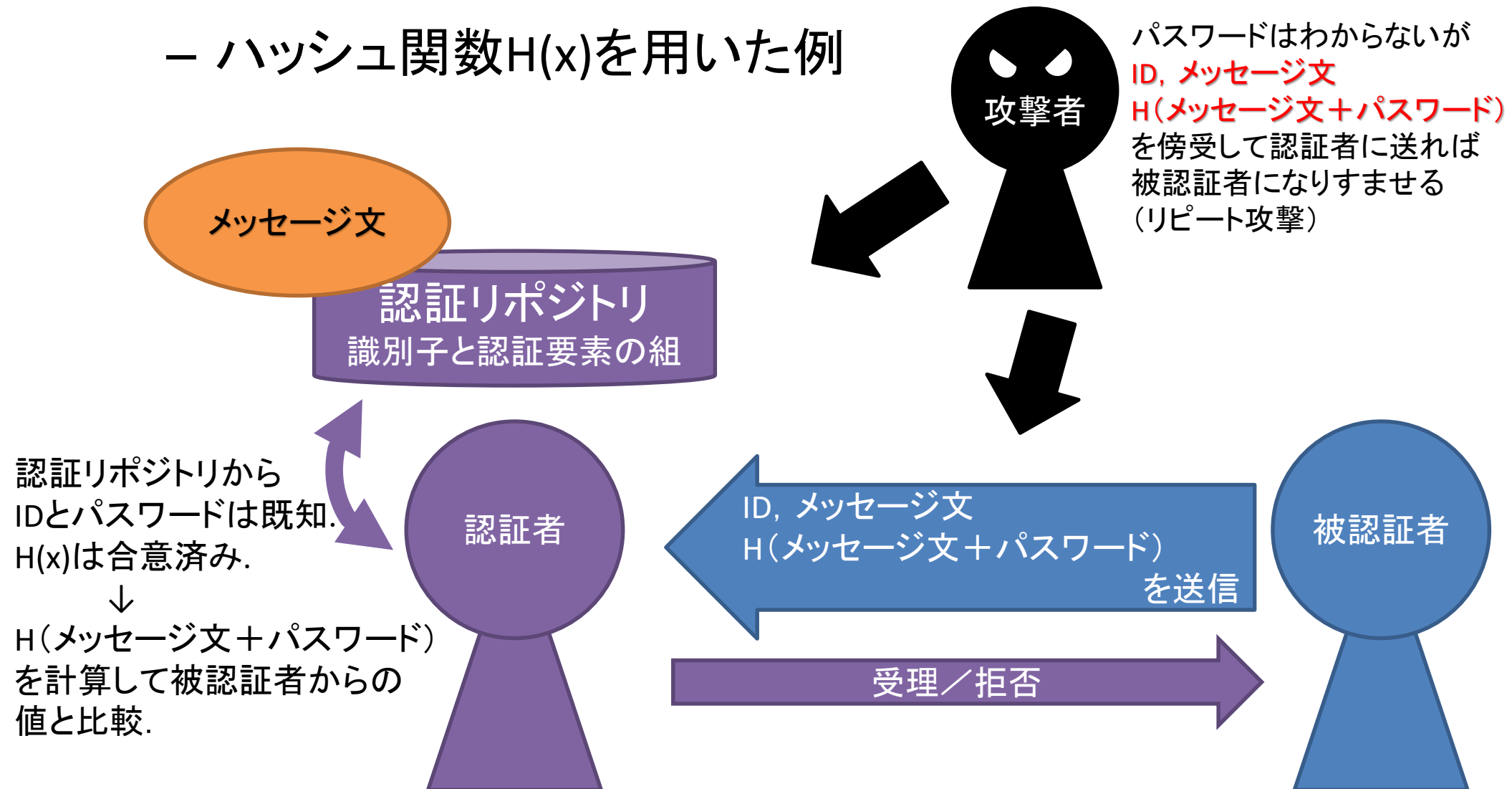
- 公開鍵暗号方式に基づく方式
 - Web (https) などで利用
 - 通信相手の公開鍵を基に暗号化した通信を開始
 - デジタル署名を基に, 公開鍵の正当性を確認
 - CA (RootCA) による確認 → PKI
 - その通信専用の秘密鍵を交換して, 以降の通信を行う
 - 通信には, ハッシュによる改竄検知を併用する
- デジタル署名が正しくない場合 (オレオレ証明書)
 - 偽の通信相手の可能性あり

信頼の鎖

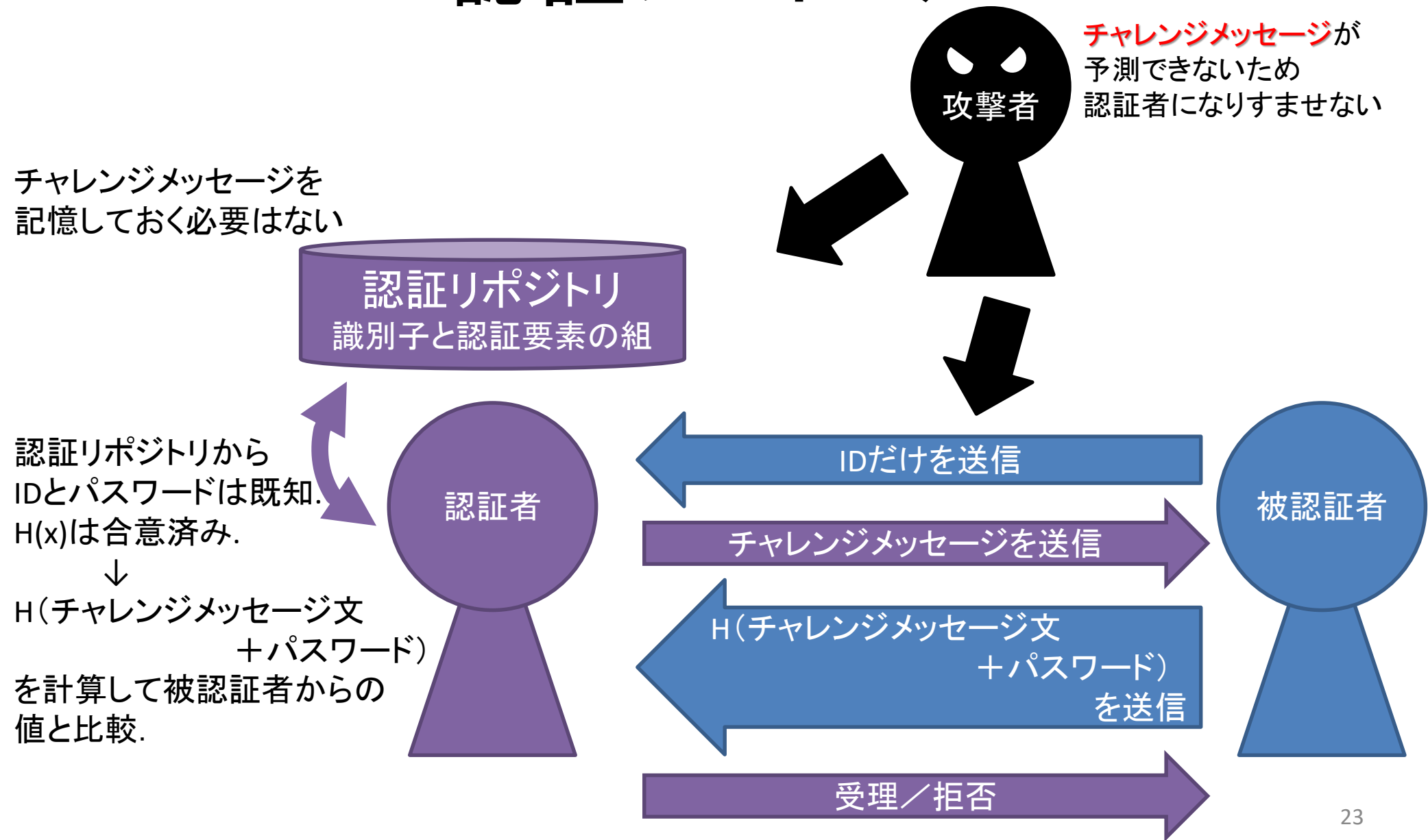
- 問題
 - その認証局が信頼できるものであるかどうか
- Webブラウザ制作者
 - Webブラウザにあらかじめ世界中の認証局やルート認証局（認証局の中でも特に重要なもの）のリストを入れる
 - 認証局を運営する企業に対して認証作業を認める設定をする

認証プロトコルの暗号化

- メッセージ認証コード
 - ハッシュ関数 $H(x)$ を用いた例



チャレンジ・アンド・レスポンス 認証プロトコル



認証プロトコルの脆弱性

- MS-CHAPv2の脆弱性

<https://msrc-blog.microsoft.com/2012/08/20/2743314-ms-ch/>

- マイクロソフト製品で広く使われてきたチャレンジ・アンド・レスポンス認証プロトコル
- 2012年に脆弱性が見つかる
 - 認証のやり取りを傍受, 解析することでパスワードが明らかに

- 危険を回避するには

- 多くの通信プロトコルでは複数の認証プロトコルが選択できるように規格化
- 特定の認証プロトコルに脆弱性が発見された場合には他の認証プロトコルに切り替える

共通鍵暗号方式

- ブロック暗号

- 平文をブロック単位に分割して暗号化を行う
- 実現が比較的容易
 - DES (Data Encryption Standard) 鍵長56bit
 - 1975 年アメリカ商務省標準局で公表
 - 1999年1月, 22時間15分でDESの鍵がやぶられた. 総当たり攻撃
- Triple DES (3DES)
- FEAL NTT が開発
- MULTI 日立製作所が開発. デジタル衛星放送等
- IDEA PGP などで使われる
- RC5 Ronald Rivest が開発. SSL など.
- MISTY 三菱電機が開発. W-CDMA など

パスワードとその管理

パスワード

- 被認証者が記憶した文字列による認証要素
 - 利用方法が平易で分かりやすい
 - 広く普及しているため詳細な説明不要
- 問題点
 - 万一他人に知られたときに被認証者が気づけず漏洩発覚が遅れやすい
 - 容易に推測できる文字列だったり, 異なるサービスに同一のものを使い回す被験者が少なくない

パスワードの傾向

- 2009年10月 無料メールサービスHotmailの1万人分のパスワード漏洩事件より

<https://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/>

- 最多“123456”, 2番目“123456789”
以下10位中5つが数字の単純な並び
- 10位中残り5つが人名
- 全体の19%が数字のみ, 42%が英小文字のみ
- 英大文字小文字, 数字を含むのは6%

パスワードの漏洩

- 総当たり攻撃
- 辞書攻撃
- ソーシャルな攻撃
- フィッシング詐欺による攻撃
 - 攻撃者のWebサイトに巧みに誘導し, IDとパスワードを入力送信するよう仕向ける
- マルウェアによる攻撃
 - 被認証者のキーボード入力内容を詐取したり, PC内のパスワードを盗むようなウイルスを用いる
- 認証リポジトリに対する攻撃
 - 不正アクセスや内部犯行など
 - 他のサービスで同一のIDに対してパスワードによる認証を試行し被害が広がることも

被認証者ができる対抗策

- 総当たり攻撃やソーシャルな攻撃に対応
 - 他人に教えない
 - 簡単に類推できないこと
 - 十分に長い(最低でも8文字以上)
 - サービスごとに違うパスワード

認証者が行うべき認証設計(1)

- 総当たり攻撃対策
 - 1つのIDに対し、一定時間内の認証回数を制限
 - 1分間で10回までの試行制限など
 - 同じIDで何度も間違ったパスワードを試行するアクセスを攻撃とみなし、一定時間そのIDに対する認証を拒否

認証者が行うべき認証設計(2)

- 認証リポジトリ
 - パスワードを格納せずハッシュ値を格納
 - パスワードにソルト値を加えたものからハッシュ値を計算
 - 認証リポジトリ内にパスワードそのものが格納されない
 - ハッシュ値の元となる文字列が長くなるので解析が困難に
 - 同じパスワードでも、ハッシュ値が異なるようにできる
 - IDごとにソルト値は異なることが必要
 - ハッシュ値のデータベースの利用を困難に
 - 攻撃者はSHA-1など有名なハッシュ関数に関して、ある程度の長さの文字列のハッシュ値がまとめられたデータベースを利用することがある

例:

ID	パスワード	ソルト値	ハッシュを求めるための値	ハッシュ値
admin	U3h47aTU	J0w0czvs	U3h47aTUJ0w0czvs	551906b74fb870407383c...

他の認証要素

生体認証（バイオメトリクス認証）

- 人の身体的特徴（顔，声，指紋，静脈パターン，虹彩の模様，網膜のパターンなど）
 - － 他人に模倣されにくい
 - － 失念，紛失の危険がない
- 問題点
 - － 偽造された生体情報は本物との区別が難しい
 - － 流出した場合、被認証者に固有の情報のためパスワードのように変更できない
- セキュリティ確保には他の認証技術と併用

ICカード

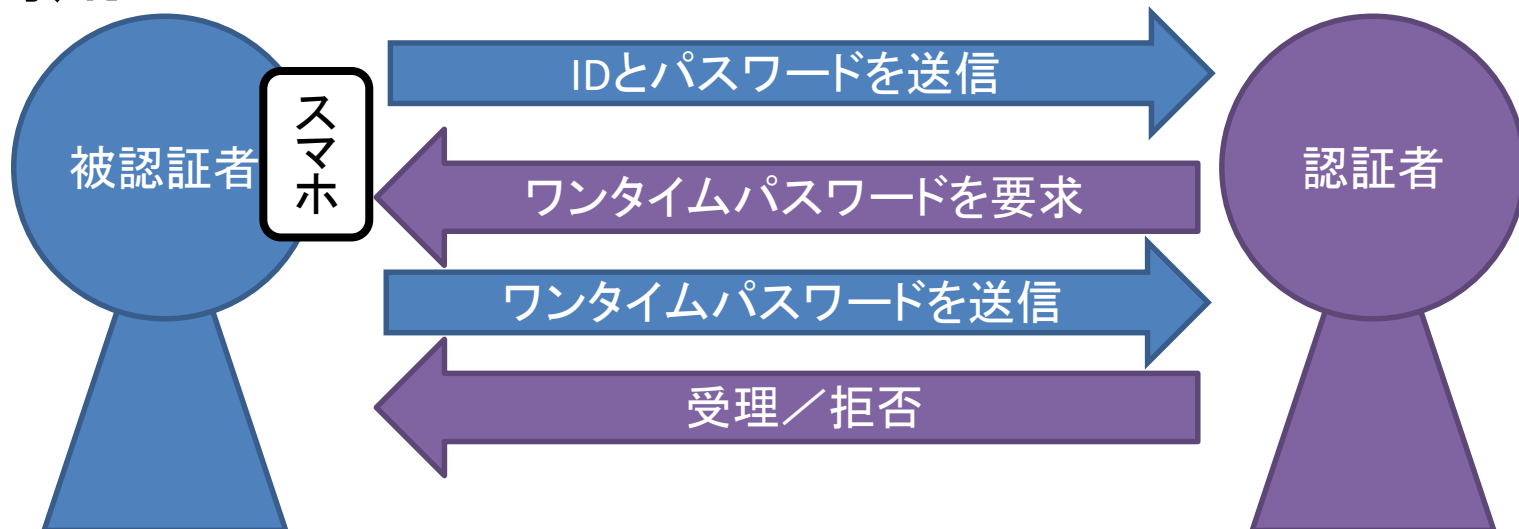
- 微弱電波を利用した発電装置と超小型のコンピュータを組み合わせたカード
 - 鉄道会社の自動改札の場合
 - カードを自動改札に近づけると、電波を受けてコイルで発電
 - 発電した電気(電流)でカード内部のコンピュータを起動
 - 電波から読み取れるデータをもとに計算を行って計算結果を自動改札に送信。盗聴を防ぐため暗号化も
 - 自動改札とカードの間で何回かデータのやり取り
 - 最終的に自動改札を通過することが可能と判断されれば、門が開く。また、ICカードは入場記録(退場記録)や残額・区間などをメモリに書き込む

多要素認証

- 以下の認証要素のうち異なる複数の種類を用いる認証
 - 知識(パスワードなど)
 - 利便性が高い
 - 他人になりすまされやすく、漏洩被害に気付きにくい
 - 物体(ICカード)
 - 盗難紛失に注意
 - 被害自体には気づきやすい
 - 特徴(生体認証)
 - 亡失や盗難の危険がない
 - 偽造や模倣によるなりすましの危険

多要素認証の例

- 二段階認証 - ワンタイムパスワードの場合
 - パスワードによる認証後に被認証者が持つ携帯端末に使い捨てのパスワードを送付する
 - インターネットバンキングでの振込・振替などに利用



暗証カードをご契約いただいていたお客さま

2020年11月以降、暗証カードによるお取引ができなくなります。

1分ごとに更新されるパスワードで安心!



< 暗証カード >



もしくは



< パスワードカード > < パスワードカード >
(スマホアプリ版)

2020年11月をもって、暗証カードのお取扱を終了いたしました。

お取扱終了にともない、テレホンバンキング（自動音声・オペレータ）での以下のサービスを終了いたしました。

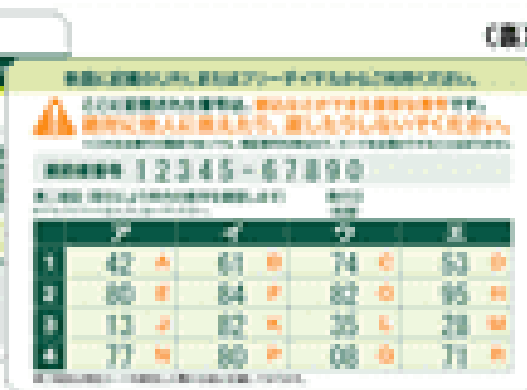
今までご利用いただき、誠にありがとうございました。

今後は、ワンタイムパスワードの利用登録をいただくことにより、テレホンバンキングに代わり、インターネットバンキングでご利用可能となりますので、ワンタイムパスワードの利用登録をお願いいたします。

暗証カード(表)



(裏)



< 暗証カード >



[Q & A（よくあるお問い合わせ）](#) > [その他（お困り・トラブル等）](#) > [金融犯罪関連](#) > 銀行を名乗る不審なEメールが届きましたが、どうしたらいい

ですか？

カテゴリー一覧

+ 各種お手続き

+ 店舗・ATM（手数料・サービス内容）

+ 口座開設・切替

+ 振込・決済

+ インターネットバンキング（三菱UFJダイレクト）

+ クレジットカード・デビットカード

+ 預金・運用商品

+ ローン

+ スマートフォンアプリ

+ その他（お困り・トラブル等）

+ 特別定額給付金（新型コロナウイルス感染症緊急経済対策関連）（6件）

Q & A（よくあるお問い合わせ）

Q ご質問

印刷する

No : 28 公開日時 : 2018/08/27 11:34

銀行を名乗る不審なEメールが届きましたが、どうしたらいいですか？

A ご回答

当行では、セキュリティ上、お客さまに対して、パスワードや暗証番号などの大切な情報を、Eメールでお伺いすることはございません。

このような不審なEメールをお受け取りになった場合は、返信されないようくれぐれもご注意ください。

万が一、パスワードや暗証番号などの大切な情報を返信された場合は至急、以下までのご連絡のうえ、ご利用停止のお手続きをお願いいたします。

■三菱UFJダイレクトのパスワード等を入力された場合

- 毎日9:00～21:00
インターネットバンキングヘルプデスク
0120-543-555 または 042-311-7000（通話料有料）
- 上記以外の時間
三菱UFJ銀行 喪失受付センター
0120-544-565 または 03-5637-0875（通話料有料）
※毎日第2土曜日の21:00から翌朝6:40はご利用いただけません。

統合認証

統合認証

- IDとパスワードなどの認証を複数の情報システムで共通に利用できるようにしたもの
- アイデンティティ連携・フェデレーション
 - 統合認証において、情報システム間で秩序ある情報流通を実現する機構
 - 認証時の個人情報の授受を本人に許可を求める
 - 規格: SAML, OpenIDなど

OpenID

- Google, Facebook, Twitter, Yahoo!などで採用されているアイデンティティ連携規格

The screenshot displays the Google Account management interface. At the top, a blue header bar contains the Google logo and a navigation menu with the option '← アカウントにアクセスできるアプリ' (← Apps that can access your account). Below this, a message states: 'このアプリやサービスには、お使いの Google アカウントへのアクセス権が付与されています。 [ヘルプ](#)' (This app or service has been granted access to your Google account. [Help](#)).

The main content area is divided into two sections. On the left, under the heading 'サードパーティ製アプリ' (Third-party apps), a list of apps is shown with their respective icons and names: Brabio! Project, Lifelog, Qiita, and Wunderlist. Each app entry is followed by the text 'アカウント' (Account). Below this list, a message reads: 'アカウントの基本情報へのアクセスが可能です' (You can access basic account information).

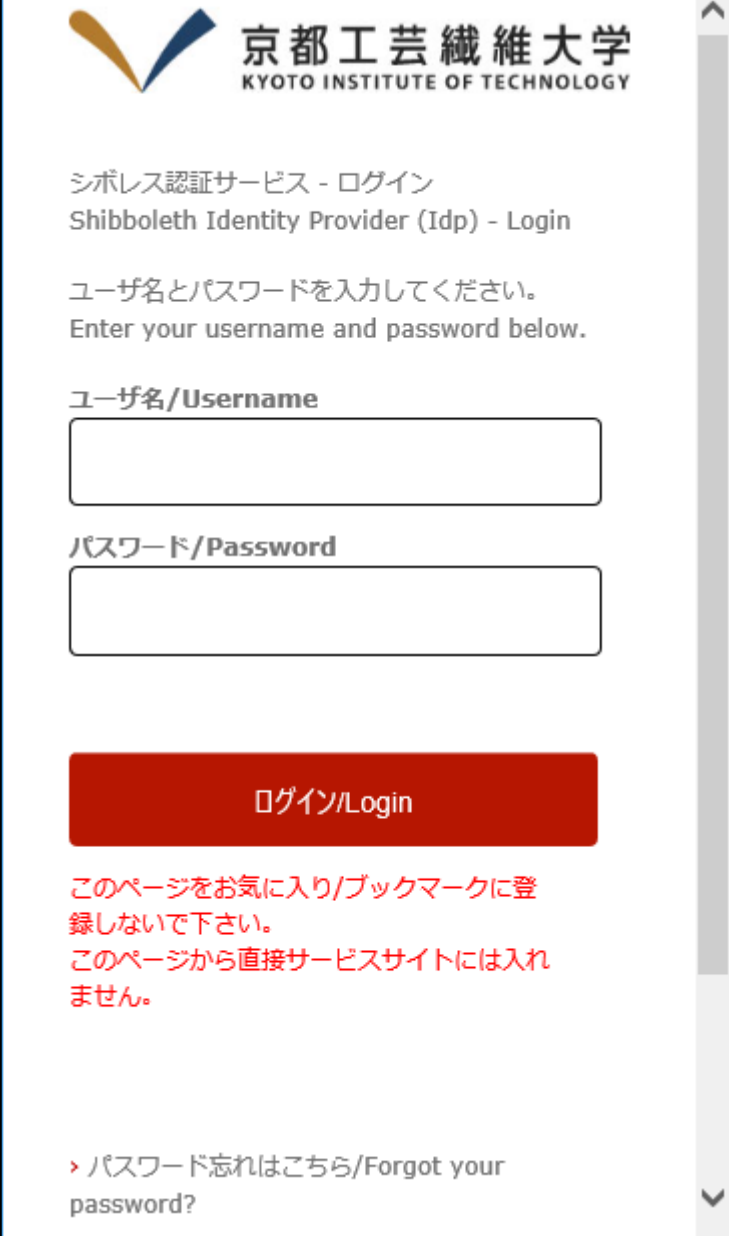
On the right, a modal window titled 'Brabio! Project' is open, showing the 'アカウント設定' (Account settings) page. The page has a dark header with the Brabio! Project logo and the date '12月15日 (金) 11:2'. Below the header, a sidebar menu lists settings: 'アカウント設定' (Account settings), '認証連携設定' (Authentication and linking settings), '通知設定' (Notification settings), and 'お知らせメール配信設定' (Notification email distribution settings). The main content area of the modal shows a table of linked accounts:

Account	Status	Action
Google	連携中 (Linked)	連携を解除 (Unlink)
Facebook	未設定 (Not set)	連携する (Link)
Windows Live ID	未設定 (Not set)	連携する (Link)

本学における統合認証

情報科学センターアカウント(1)

- 学内の多数の情報システムで統合認証を実現
- 認証システムへログインするページが表示されるサービス
 - Webメール
 - e-Learning(Moodle)
 - 認証ポータル(パスワード変更)
 - 認証付き無線LAN・情報コンセント
 - ...



The screenshot shows the Shibboleth login interface for the Kyoto Institute of Technology. At the top is the university's logo and name in Japanese and English. Below this, the text 'Shibboleth Identity Provider (Idp) - Login' is displayed. A prompt asks the user to enter their username and password. There are two input fields: 'ユーザ名/Username' and 'パスワード/Password'. A red 'ログイン/Login' button is positioned below the fields. A red warning message states that the page should not be bookmarked and that direct access to service sites is not possible from this page. At the bottom, there is a link for 'Forgot your password?'.

京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

シボレス認証サービス - ログイン
Shibboleth Identity Provider (Idp) - Login

ユーザ名とパスワードを入力してください。
Enter your username and password below.

ユーザ名/Username

パスワード/Password

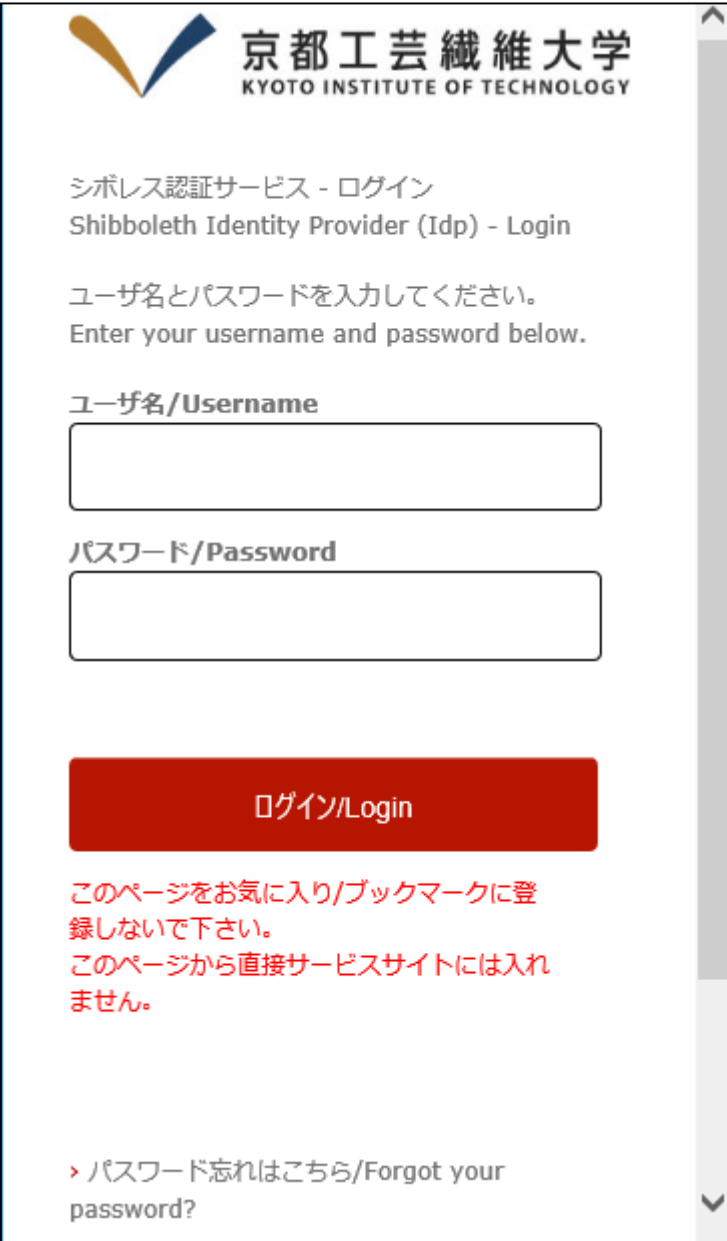
ログイン/Login

このページをお気に入り/ブックマークに登録しないで下さい。
このページから直接サービスサイトには入れません。

パスワード忘れはこちら/Forgot your password?

情報科学センターアカウント(2)

- Shibboleth
 - SAML (セキュリティ・アサーション・マーク付け言語)による統合認証基盤
 - Idp(アイデンティティ・プロバイダ)
 - 利用者情報を提供
 - SP(サービス・プロバイダ)
 - 各情報システム
 - Idpから利用者情報を受け取り利用者にサービスを提供



The screenshot shows the Shibboleth login interface for the Kyoto Institute of Technology. At the top is the university's logo and name in Japanese and English. Below this, the text 'シボレス認証サービス - ログイン' and 'Shibboleth Identity Provider (Idp) - Login' is displayed. A prompt asks the user to enter their username and password. There are two input fields: 'ユーザ名/Username' and 'パスワード/Password'. A red 'ログイン/Login' button is positioned below the fields. A red warning message states that the page should not be bookmarked and that users should not go directly to service sites from this page. At the bottom, there is a link for 'パスワード忘れはこちら/Forgot your password?'.

京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY

シボレス認証サービス - ログイン
Shibboleth Identity Provider (Idp) - Login

ユーザ名とパスワードを入力してください。
Enter your username and password below.

ユーザ名/Username

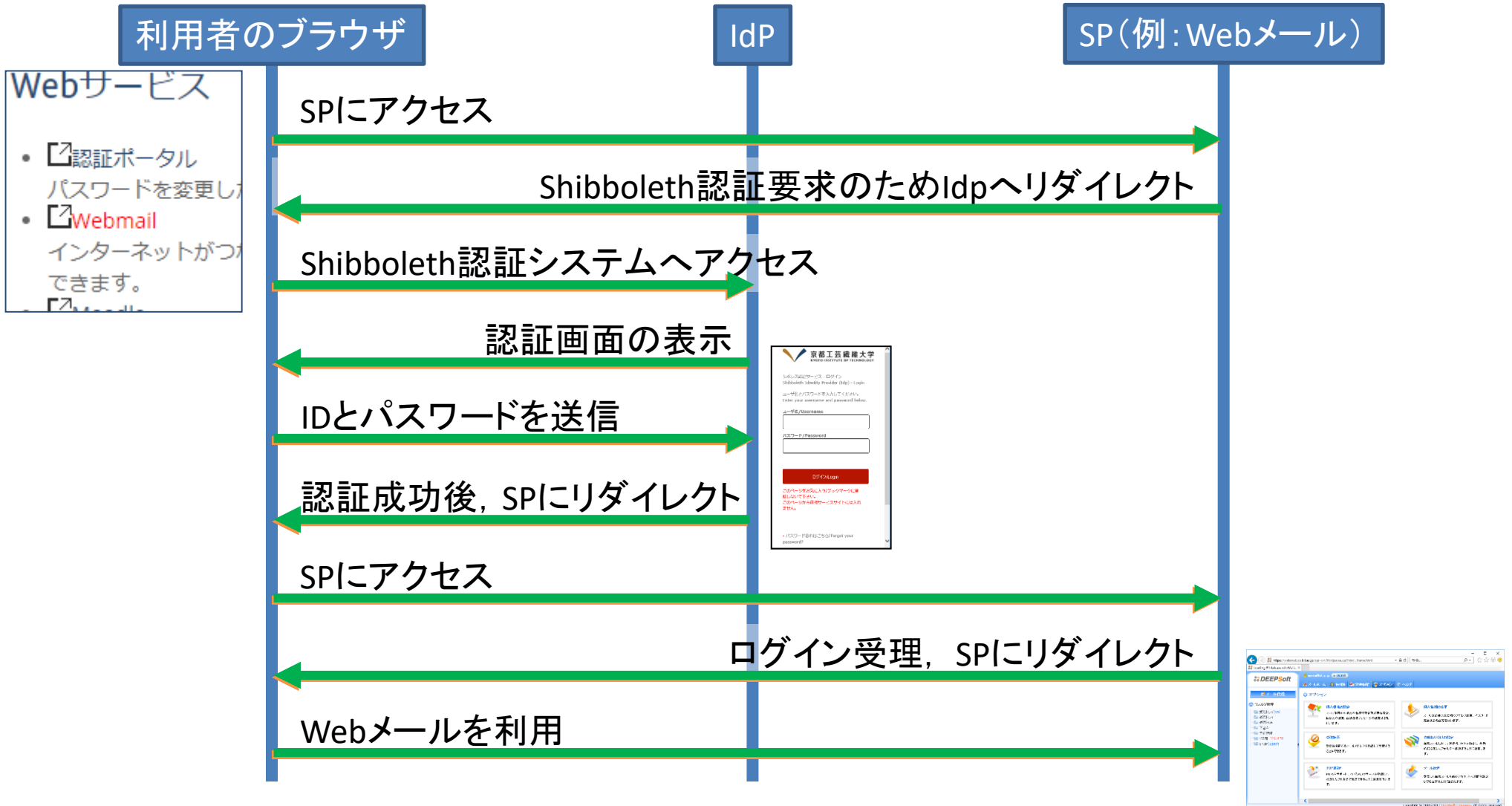
パスワード/Password

ログイン/Login

このページをお気に入り/ブックマークに登録しないで下さい。
このページから直接サービスサイトには入れません。

パスワード忘れはこちら/Forgot your password?

情報科学センターアカウント(3)



共用PC (Windows)

- Active Directory
 - Microsoft社のユーザとコンピュータリソースを管理するコンポーネント群 (ディレクトリサービス)

- 配下の共用PC

- 
- ユーザ名
 - パスワード

情報科学センターアカウントと連携

学術認証フェデレーション(学認: GakuNin)

- 大学や教育機関の間でSAMLに基づくアイデンティティ連携を実現
- 大学内で普段用いているIDとパスワードから他の教育機関のサービスを受けることができる
- 本学で利用可能な学認サービス
 - <https://www.cis.kit.ac.jp/gakunin/> (情報科学センター)

提供	名称	URI	利用資格
国立情報学研究所	FileSender (ファイル共有)	https://filesender.nii.ac.jp/	本学の教員・職員・学生
国立情報学研究所	FaMCUs (テレビ会議多地点接続サービス)	https://famcus.nii.ac.jp/	本学の教員・職員
国立情報学研究所	eduroam認証連携IDサービス	https://federated-id.eduroam.jp/	本学の教員・職員
国立情報学研究所	クラウドゲートウェイ	https://cg.gakunin.jp/	本学の教員・職員・学生
科学技術振興機構	researchmap	http://researchmap.jp/	本学の教員・職員・学生
日経BP社	日経BP記事検索サービスアカデミック版	http://bizboard.nikkeibp.co.jp/academic/	図書館利用資格を満たす教員・職員・学生
Elsevier	ScienceDirect	http://www.sciencedirect.com/	図書館利用資格を満たす教員・職員・学生
	Scopus	https://www.scopus.com	図書館利用資格を満たす教員・職員・学生
John Wiley & Sons	WILEY ONLINE LIBRARY	http://onlinelibrary.wiley.com/	図書館利用資格を満たす教員・職員・学生
Nature	Nature Publishing Group	http://www.nature.com/	図書館利用資格を満たす教員・職員・学生
Royal Society of Chemistry	Royal Society of Chemistry	http://pubs.rsc.org/en/journals	図書館利用資格を満たす教員・職員・学生
Springer Link	Springer	https://link.springer.com/	図書館利用資格を満たす教員・職員・学生
株式会社ディスコ	キャリアタスUC	https://uc-student.jp/kit/	利用資格を満たす教員・職員・学生