様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月　 ２ 日現在

機関番号：１２５０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ１１２９０

研究課題名（和文）安全性と利便性を備えた情報連携システム

研究課題名（英文）Secure infomation sharing system with user-friendliness

研究代表者
多田　充（Tada, Mitsuru）

千葉大学・大学院理学研究院・教授

研究者番号：２０３０３３３１

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究では，独立に運用されている複数のサービスシステムに対して，新たに制御センターを設置することにより，同一ユーザが所有する属性情報を安全に連携させることができるシステムを構成した。制御センターを中心とするスター型の構成にすることにより，N個のサービスシステムのうち任意の２つのシステム間で情報連携を行う際，ＯＡｕｔｈなどの従来の方法だとユーザの登録の手間がＯ（Ｎ＾２）であるのに対し，本システムの場合はＯ（Ｎ）で済む。また，ユーザが一般的に所有しているスマートデバイスを用いることにより，ユーザと制御センター間の認証を複数・多要素によるものにするなど，強固なものにすることができる。

研究成果の学術的意義や社会的意義
特定のサービスシステムだけが持つ情報を他のサービスシステムにおいても適切に利用できる仕組みの構築は，別々の組織により運用されいる場合だけでなく，同一または提携している組織で運用されているサービスシステム間でも有用であると思われる。実際，同一組織内で異なるＩＤ体系による複数のシステムがある場合，組織のユーザはそれぞれのシステムに保有されている自身の情報を複数のサービスを使い分けて利用しなければならない。本研究の成果は，そのような状況を解決する１つの手法となると思われる。また，複数の制御センターを階層的に設置することにより，大規模な組織内のシステムを論理的に階層的に統合することが可能である。

研究成果の概要（英文）：Our research has proposed the construction for an information sharing system which enables to make attribute data for a user registered in plural service systems independently managed shared among those systems, by newly installing a control server. The star-type construction with the control server as the center has decreased the sharing setting labor for one user from O(n to O(n), comparing with the way we usually adopt such as OAuth. Furthermore, we can strengthen the authentication between a user and the control server by using a smart device a user usually possess with which the authentication can be by double or multi-factor.

研究分野：暗号理論，情報セキュリティ

キーワード：情報連携　複数所有物認証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) 現在，ネットワーク上のサービスシステムを利用するにあたり，会員登録時点で，サービスシステム側が，ユーザの本人証明やそのサービスを受ける 資格/権限 等を確認することがある。(例えば，ユーザの免許証や住民票の写し，資格証明書や健康診断書 など) これらはユーザの属性に該当するが，異なる組織が運用する異なるサービスシステム間でユーザの属性証明することは容易ではなく，実際にはユーザ自身が一方のサービスシステムに発行してもらった証明書を，他方のシステムに提出するような形になっていることが多い。しかし，これは安全性や信頼性，利便性の観点で問題があると言わざるを得ない。

(2) 経済産業省は，安全性の観点から，ポリシーやルールを明確にした上で，信頼できる組織を認定し，それらを連携される「ID 連携トラストフレームワーク」の仕組みを構築する必要性を訴え，現在，日本情報経済社会推進協会(JIPDEC)を中心として，多くの民会企業および大学の技術者や研究者が，その実現に向けて活発に議論している。ネットワーク上で，ID 情報も含めてユーザ情報(属性)の連携を推進することにより，行政組織，民間企業等における本人確認や属性情報収集の効率性が高まり，また，本人確認や属性情報の管理が専門的に行われることで，個人情報管理の安全性が向上することが期待できる。更には，本人の同意に基づき，複数のサービスシステムが連携することで，複合的かつきめ細かなサービスの提供が期待できる。

２．研究の目的

(1) 我々の研究グループが，経済産業省主催の「ID 連携トラストフレームワークビジネスモデルコンテスト」において奨励賞を受賞した「共通 1-day パスワード発行センタ構想」のアイデアを発展させ，ネットワーク上で安全かつ円滑にユーザ情報を複数のサービスシステム間で連携(情報連携)する仕組みの構築，その安全性・利便性の調査，および，構築したプロトコルの実装実験による検証を行う。

(2) 我々が構築したシステムにおける「ユーザの携帯端末 ⇔ 制御センター 間」の認証について，前述の段階では「ユーザの記憶情報(パスワード)および所有物(携帯端末)」という 2 要素によるものを想定していたが，その手段について，安全性を損なわずに，より利便性の高い認証プロトコルを構築する。

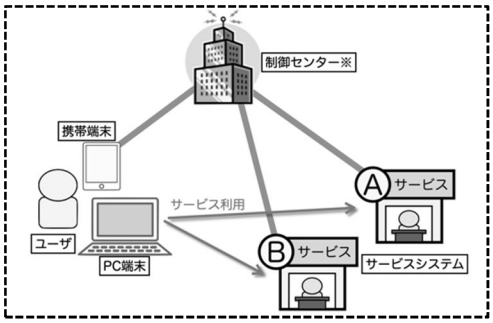
３．研究の方法

(1) 経済産業省は，ID 連携トラストフレームワークの一環として，ユーザの情報を連携させる「デジタル Watashi アプリ」の取り組みを発表している。それにおいて，情報連携はユーザを中心としたスター型になっているが，本研究では，新たに設置する制御センターを中心としたスター型になるようにシステムを構成する。このようにすることで，各サービスシステム間の仕様の違いや，技術的仕様変更，サービスシステムの追加・削除 等を全て制御センターが吸収し，他のエンティティに影響しないようにできる。このことは，ユーザが使用する携帯端末アプリについても同様である。接続されているサービスシステムが新たに 増えた/減った，または，接続されているサービスシステムのうちの１つが仕様変更しただけで，ユーザはそのサービスシステムを利用しない場合であっても，アプリ更新など，システム構成の変更に伴う作業をしなければならない。しかし，本申請研究のシステムの場合は，中間に配置される制御センターがそれらの変更を吸収するため，サービスシステムの変更に伴うユーザの作業は発生しない。これらは，運用する上で重要な利点となり得る。

(2) ２(1)の「共通 1-day パスワード発行センタ構想」においては，複数のサービスシステム間において，その都度発行されるパスワードが共有される。本研究で考える情報連携システムでは，ユーザの属性情報が共有される。その違いは，共有される情報の出発点（共有される情報を元々保有しているシステム，あるいは，その情報を生成するシステム）であり，前者の場合は制御センターであり，後者の場合はその属性情報を保有しているサービスシステムである。そのため，前者のためのプロトコルに，どの属性情報を共有するか，どのサービスシステムと共有するかなどを決定するための通信を追加する必要がある。本研究では，そのプロセスを一般化（モデル化）する。

４．研究成果

(1) 情報連携システムのプロトコル



本研究による情報連携システムは，右図のように，ユーザ（PC 端末およびスマートデバイス），サービスシステム（簡単のため，A と B の 2 つとする），制御センターからなる。それぞれのエンティティ間の通信は公開鍵証明書を利用した https などの安全な通信路とする。

ユーザはサービスシステム A，B において，固有のユーザ ID（それぞれ uID_A，uID_B とする）を割り当てられているものとする。A において，ユーザは属性情報($att_1^A,\cdots,att_M^A$)を持っているものとする。また，B において（$att_1^B,\cdots,att_N^B$）をもっているものとする。

情報連携プロトコルは，登録フェーズ および 情報連携フェーズの 2 つからなる。さらに，登録フェーズは 2 つのステップ（登録フェーズ 1 および 2）に分けられる。詳細については参考文献[1]により国際会議で論文発表しているが，ここではその概略を述べる。

登録フェーズ 1 において，A は uID_A に紐付けされた一意的な文字列（管理 ID）mID_A を生成し，制御センターに mID_A のためのアカウント作成を依頼する。制御センターは，mID_A に紐付けされた一意的な文字列（アプリケーション ID）aID_A を生成し，aID_A のアカウントのための認証情報（電子署名や MAC など）を含んだ登録チケット T を作成し A に返す。（T は必ずしも aID_A の文字列を含む必要はない）A は安全な方法で T をユーザに渡す。

登録フェーズ 2 において，ユーザは自身が所有するスマートデバイスを用いて，T を制御センターに送る。（スマートデバイスには，本システムのための動作を行う専用アプリがインストールされているものとする。）制御センターは，T の正当性を検証した上で，ユーザのスマートデバイスを認証するための証明書（アクセスパス P_A）を作成し，スマートデバイスに返す。P_A はスマートデバイス内でその機器でのみ利用できる状態で保存される。ユーザ（スマートデバイス）と制御センター間は，登録で用いた機器でのみ認証をパスできる状態，つまり，所有物認証が可能な状態になる。

サービスシステムA

項目	ユーザID	管理ID	属性1	･･･	属性M
値	uID_A	mID_A	att_1^A	･･･	att_M^A

（Bについても同様）

制御センター

項目	アプリケーションID	対象サービスシステム	管理ID
値	aID_A	A	mID_A
	aID_B	B	mID_B

ユーザのスマートデバイス

項目	アプリケーションID	対象サービスシステム	アクセスパス
値	aID_A	A	P_A
	aID_B	B	P_B

登録フェーズを実行することにより，ユーザには 3 種類の ID 文字列が割り当てられることになる。ユーザ・サービスシステム間の uID_A，サービスシステム・制御センター間の mID_A，制御センター・ユーザ間の aID_A である。なお，サービスシステム B についても，同様のプロセスを行うことにより，それぞれのエンティティには，右図のようにデータが登録される。

情報連携フェーズ において，ユーザが A に保存されている自身の属性情報 att_i^A をサービスシステム B に連携させるとする。

ユーザは，スマートデバイス（内の専用アプリ）を用いて，A から B に情報連携させる旨を送る（＊）。その際，関係するサービスシステムに対応するアクセスパス P_A および P_B を用いて認証する。

制御センターは，A および B に問い合わせて，それぞれのサービスシステムで扱っている属性情報のリスト（L_A，L_B とする）を得て，L（$=L_A \cap L_B$）をユーザ（のスマートデバイス）に送り返す。ユーザは，A における属性 i^A が L に入っていることを確認し，その属性値を B に連携させる旨を制御センターに送る。（このとき，その属性は B にも登録されている属性 j^B となる。）もし，属性 i^A が L に入っていない場合は，連携不可能ということでプロトコルを終了させる。

制御センターは，P_A に対応する aID_A に紐付いている mID_A と，属性 i^A をサービスシステム A に送り，その属性値 α（$=att_i^A$）を得る。そして，P_B に対応する aID_B に紐付いている mID_B と，属性 j^B，および，その属性値 α をサービスシステム B に送り，B は mID_B に対応しているユーザアカウント uID_B の属性 j^B に値 α を登録する。

情報連携フェーズにおいて，ユーザの属性値 α が制御センターに晒されるのを防ぐ場合は，A が α を制御センターに送る際，それに暗号化処理を施す必要がある。登録フェーズ 1 において，サービスシステムがユーザに登録チケットを渡すとき，ユーザ（スマートデバイス）とサービスシステムの間で鍵（k_A,k_B とする）を共有することができることに着目する。情報連携フェーズ

の（＊）の段階において，ユーザは AB 間のセッションキーk を設定し，k を k_A で暗号化したもの e_A，および，それに対する MAC m_A，同様に k を k_B で暗号化したもの e_B，および，それに帯する MAC m_B を作成し，（e_A,m_A）および（e_B,m_B）を制御センター経由で A および B に送る。A が B にαを連携させるときは，αを k で暗号化すればよい。そのようにすることで，ユーザの属性情報そのものが制御センターのログに記録されることを防ぐことができる。

(2) ユーザ（スマートデバイス）・制御センター間の認証について

登録フェーズ 2 において，ユーザが制御センターに登録手続きを行う際，ユーザ固有のパスワードを設定することにより，記憶情報および操作機器による 2 要素認証が可能となる。しかし，スマートデバイスは小型であることが多く，そのような機器に対してパスワードを入力するのはユーザにとって煩わしい作業であることが多い。そこで，本研究においては，ユーザの複数の所有物による認証について，そのプロトコルを構築した。ここではその概略を述べる。

登録フェーズ 1 において，制御センターは自身がその正しさを検証できる何らかの認証情報（S とする）を生成し，登録チケットとともに S をサービスシステム A に送る。A は，S の情報が書き込まれた IC カード等の物理的媒体 C を作成し，登録チケットと C を安全な方法でユーザに渡す。ユーザは，登録チケットと上記媒体 C を用いて登録手続きを行う。

情報連携フェーズにおいて，ユーザは 登録フェーズ 2 で使用したスマートデバイス（にインストールされている専用アプリ）で上記媒体 C に書き込まれている認証情報 S を読み込み，制御センターに情報連携リクエストを送る。このようにすることで，制御センターは通信相手が，登録に使用したものと同一のデバイスを使用（所有）していること，および，サービスシステムから渡された上記カード等の媒体を所有していることの 2 つを検証することができ，より高い精度で本人認証ができると期待できる。なお，スマートデバイスに指紋認証や顔認証などのバイオメトリクスによるロックがかかっていれば，それも認証要素となり，さらに高い精度で認証することができる。

(3) アクセスパスの安全性について

登録フェース 2 で，制御センターから送られてきたアクセスパスについて，ユーザはそれをデバイスの耐タンパー領域に保存したり，機器固有の情報で暗号化したりするなど，そのアクセスパスが他のデバイスでは利用できないようにする必要がある。これについては，我々の研究グループがすでに論文発表している手法などで解決できることが解っている。

(4) 複数所有物認証の利便性向上について

上記(2)で述べた複数所有物認証であるが，サービスシステムから独自に送られてきたカード等の媒体 C を常に携帯することになると，ユーザの利便性が損なわれると思われる。そのため，本人の身分証明ができる（運転免許証やマイナンバーカードなど，公ではあるものの）第三者発行の IC カード媒体（ここでは D とする）を C の代わりに用いることができるよう，複数所有物認証のプロトコルを改良した。これについては[2]で公表している。

登録フェーズが終了した時点でユーザ認証に使用できる媒体は，アクセスパス P とサービスシステム発行のカード C であるが，この時点では，P と C をシェアとする(2,2)-閾値秘密分散を構成する。このとき復元される（秘密分散としての）秘密情報を u とし，制御センターのみがそれを保存する。制御センターは，ユーザから P と C が送られてきたら，その 2 つから u が復元できるかを検証することによりユーザ認証を行う。

ユーザが，自身の身分を保障できる別の媒体 D を登録する際，制御センターは P と C で認証した後，P,C,D をシェアとする(2,3)-閾値秘密分散を構築し，そこで復元される秘密情報を更新する。それ以降は，ユーザは P,C,D のうち 2 つがあれば認証をパスすることができる。制御センター側で P の送付を必須とすることにより，ユーザは使用する機器および身分証 D で情報連携のリクエストを送ることができる。（なお，ユーザが登録できる身分証の個数については，特に制限はない。）

ユーザがスマートデバイスを交換する際は，C と D のみで認証できるため，その認証を行った上で，新たにアクセスパス P’を生成し，ユーザ（スマートデバイス）に送る。そのため，一見煩わしい機種変更の操作もスムーズに行うことができる。

(5) 実装実験について

(1)～(3)に述べた情報連携プロトコルについて，我々の研究グループは，その動作確認のための実験的システムを構築した。2 つのサービスシステム，制御センター，ユーザのスマートデバイスの動作をシミュレータするプログラムを作成した。サーバ（サービスシステムと制御センター）は Linux，Apache2 を用い，プログラミング言語は php を用いた。スマートデバイスのシミュレータについては，php を用い，PC のブラウザで動作させた。なお，スマートデバイスと制御センターの間の認証は，アクセスパスを用いた機器認証と便宜上パスワードの認証を併用している。

[1] M. Tada: “Attribute sharing systems of the star type”, Proceedings of The 4th International Conference on Signal Processing and Information Security (ISAPIS) 2021, pp.33-36, 2021.
[2] 多田, 糸井:「認証システムおよび認証方法」, 特許第 6994209 号 (2021), 特願 2020-217877.

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 M. Tada	４．巻 4
２．論文標題 Attribute sharing systems of the star type	５．発行年 2021年
３．雑誌名 Proceedings of The 4th International Conference on Signal Processing and Information Security (ISAPIS)	６．最初と最後の頁 33-36
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ICSPIS53734.2021.9652425	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 M. Tada
２．発表標題 Attribute sharing systems of the star type
３．学会等名 The 4th International Conference on Signal Processing and Information Security (ISAPIS) 2021（国際学会）
４．発表年 2021年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称 機種変更支援システム及び方法	発明者 多田，糸井	権利者 千葉大学，株式会社セフティーアングル
産業財産権の種類、番号 特許、特願2018-109505	出願年 2018年	国内・外国の別 国内

〔取得〕　計3件

産業財産権の名称 認証リクエストシステム及び認証リクエスト方法	発明者 多田，糸井	権利者 千葉大学，株式会社セフティーアングル
産業財産権の種類、番号 特許、特許第6760631号	取得年 2020年	国内・外国の別 国内

産業財産権の名称 認証システム及び認証方法	発明者 多田，糸井	権利者 千葉大学，株式会社セフティーアングル
産業財産権の種類、番号 特許、特許第6994209号	取得年 2021年	国内・外国の別 国内

産業財産権の名称 複数のサービスシステムを制御するサーバシステム及び方法	発明者 多田	権利者 千葉大学
産業財産権の種類、番号 特許、特許6199506号	取得年 2020年	国内・外国の別 国内

〔その他〕

－

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	糸井　正幸 (Itoi Masayuki)	株式会社セフティーアングル・代表取締役	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関