「マルチメディア，分散，協調とモバイル
(DICOMO2019) シンポジウム」 令和元年7月

# 学内サービスパスワードレス化の実現性の検討

加藤 大弥[1] 藤尾 正和[2] 林 達也[1] 砂原 秀樹[1]

**概要：** 本研究ではその中でも学生・教員を対象とした学内サービスをパスワードレス化するにあたってその実現性の検討を行う。さまざまな認証要素や認証プロトコルの堅牢性だけではなく、教育機関という特性、登録・利用・紛失等の管理運用、社会的なデファクトスタンダードといった現実性にもフォーカスすることで、学内パスワードレス化に向けた調査を行った。また、調査結果をもとに開発・運用を行っている慶應義塾大学メディアデザイン研究科学内認証基盤 KMD-Auth を紹介する。本研究は慶應義塾大学と日立製作所との共同研究の成果を活用したものである。

# Feasibility of Password-less Authentication in Campus Services

DAIYA KATO[1] MASAKAZU FUJIO[2] TATSUYA HAYASHI[1] HIDEKI SUNAHARA[1]

## 1. はじめに

インターネット上でサービスを適切に利用するために利用者が誰であるのかという本人確認が必要不可欠であり、それに伴う、本人を証明するためのクレデンシャルも守るべき重要な情報である。その中でも一般的に広く利用されているクレデンシャルはパスワードだろう。しかし、2017年に修正された NIST SP800-63-3[4] でも取り上げられているように、パスワードの生成・利用・管理には解決が困難な問題が多くあり、クレデンシャルの不正取得・解析・ソーシャルエンジニアリング等の要因から個人情報の流出やサービスの不正使用の問題が社会問題となっている。

多くの大学においても、授業での出席確認や履修登録、大学独自のサービスを利用するためにユーザー名とパスワードを学生に対して発行しているため、大学内においても同様の問題が多く発生している。その中には、大学及び大学生という特色から発生する問題もあり、例として、

- 脆弱なパスワードの生成・使いまわし
- 学生同士のパスワード共有
- 学生主動のサービスにおけるパスワードの管理

を挙げる。最初の二つに関しては、パスワードの認証要素としての性質と情報リテラシやセキュリティの知識が未熟であることが主な原因として考えられ、2018 年に情報処理推進機構 (IPA) の調査結果 [5] でもみられるように、”長いパスワードを利用している”に関しては、10 代:35.4%,20 代:29.2%が実施しておらず、”使いまわしをしていない”に関しては、10 代:55.6%,20 代:56.0%が使いまわしていると回答している。また、4 段階評価 (レベル 1=未熟) されているパソコン習熟度との関連性については、習熟レベルが低いほどよくない傾向にあることが示されている。パスワード共有に関しては、問題意識の調査において”友人から代理操作を依頼されたので、友人の ID とパスワードを使ってログインした”という質問に対して、パソコン利用時では、10 代:55.8%,20 代:45.0%、スマートデバイス利用時では、10 代:45.7%,20 代:42.3%が”問題があると思う”と回答しており、全体的に問題の意識が低く、特に 20 代に至っては過半数に満たないものになっている。これは、アカウント情報を友人間で共有することで授業の出席を代行するといった大学特有の状況が大きく起因しているのではないかと考える。学生主動のパスワードの管理については、クラウドサービスの充実や個人での Web サービス開発の加速が著しい今日において、学園祭参加登録、学内サービスをスクレイピング等で収集し集約したサイト、勉強会や研究室のホームページ等の Web サイトを作成し、学生がユーザーのアカウント情報を管理という状況が生まれ始めている。これらのサービスで利用されるパスワードは先に述べた通り学内で使いまわされている可能性が高いことと漏洩元のサービスから学生の属性情報を簡単に絞り込まれてし

[1] 慶應義塾大学大学院 メディアデザイン研究科
[2] 日立製作所 研究開発グループ

まうという問題を孕んでおり、各大学 ITC 等で管理している範疇を逸脱しているため防ぎようのないリスクになっている。

本研究ではこれらの問題を、

- クレデンシャル情報にパスワードを含んでいる
- 未熟な管理者によるクレデンシャル情報の管理

とし、学内サービスにおいて問題の根本でもあるパスワードを利用しない認証の導入を実現するための検討を行う。

## 2. 関連研究

### 2.1 脆弱なパスワードの生成

Micheller らは [1]、自身の所属している大学において、学生の所属している学部・専攻科ごとの生成されるパスワードの強度の違いやパスワード生成ポリシー厳格に定めた場合の推測しやすいパスワードを生成してしまうことが調査によって示されている。結論として、パスワードを個々人に生成させることは難しいと考え MTurk を利用した生成ポリシーに基づいたパスワードを自動生成する仕組みを提案してしている。このことから、パスワードを適切に利用することは難しく利用し続けることはリスクが大きいことが考察できる。

### 2.2 学生間のパスワード共有

熊谷らは [2]、大学生間でのパスワードの共有と友人関係が密接に関連しているのではないかという調査を行っており、網羅性が高いとは言い難い部分はあるものの友人貢献を伴うセキュリティ無効感が意識的セキュリティ行動に負の影響を強く与えることが判明している。この対策としては教育が考えられるが、影響力やコストは未知数であり、意識的に正の影響へシフトさせることが可能なのかは判明していないのが現状である。

### 2.3 パスワードレスへの取組み

森井らは [3]、Shibboleth の外部認証に FIDO を利用することでパスワードレスな環境を構築し認証連携の検証を行っている。これにより、パスワードのようなクレデンシャル情報が通信経路流れないことで安全性を確認している。この研究では、すでに学内で用意されているサービスを利用することをスコープとしているため学生が独自に展開しているサービスに対しては対応していない。また、登録・認証フェイズでは MITM 攻撃等でクレデンシャルが盗まれることを指摘している通り、登録する、および登録されている情報を盗まれるリスクが懸念されている。

## 3. 学内サービスの現状と対策

### 3.1 学生主動サービスの展開とリスク

近年の学内サービスは、大学側が提供管理している授業支援や成績開示等のサービスが提供されているものと、学園祭出店登録や学内の e-learning 等のサービスをスクレイピングし提供している学生が自主的に構築したサービスが混在している。その中でも学生が自主的に構築したサービスにおいて、ユーザーの大学内で利用しているパスワードの使いまわしと、管理者が未熟なため発生するクレデンシャル情報漏洩のリスクが存在しており、これによって大学側で発行したクレデンシャルが大学側が提供しているリソース外から漏洩する可能性が生まれる。しかし図 1 の通り、学生が構築しているサービスは学内のリソースを利用しているとは限らず、クラウド上に構築している場合等においては大学側が直接的に管理することは困難である。

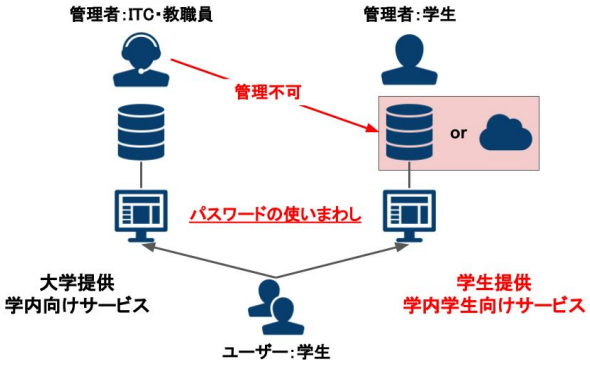



図 1 学内サービスにおけるクレデンシャル漏洩のリスク

### 3.2 学生主動のサービスに対して取り得る対策

以上のような学生主動のサービスに対して、一概にサービスの構築・展開を抑圧・禁止するというこういは、学生の学習と向上心を著しく阻害してしまう可能性がある。そのため、取り得る対策として、

- 管理・運用・構築ポリシーの指導を行う
- サービス構築用インフラの提供
- クレデンシャル情報を管理させない

について考察した。1 つ目に関しては専門家が指導をした場合のコストがあまりにも大きく、指導後の効果が得られるかどうかを判断できない部分がある。2 つ目に関しては、インフラ構築の際に発生する大学側の金銭的・人的リソースの増加・管理運用の拡充が負担になり、また、構築したインフラを学生がどの程度使うかという費用対効果が現実的ではないと考察した。3 つ目に関しては、構築されたサービスに対して、パスワードといった直接的なクレデンシャル用法を利用させないという考え方であるが、この手法に関しては、構築を行う学生が Basic 認証以外の方法で行わなければならないため学生主動で実現することは難しいと考察した。しかし、認証部分を提供もしくは代行することで解決できると考察し、本研究の指針とした。

## 4. パスワードレス認証の実現性

### 4.1 パスワードに代わる認証要素の調査

パスワードレス認証を学内で実現するにあたり、パスワードの代わりとなる認証要素の調査と検証を行う。検証する内容は、使用性、運用性、導入コストとした。使用性については、サービスの管理者およびユーザーに積極的に利用してもらうための指針、運用・再発行については、大学側の管理者の人月は有限なものであり、安定的に継続的に利用できるもことを意味しており、認証器の再発行等も含まれている。導入コストについては、学内という環境上、高価な認証器を全学生に配布することは困難であり実現性を担保するためのものである。また、本研究では各認証器や認証要素の認証強度については、NIST SP800-63-3B[4]を基準に検証を行い、定められている認証器を利用するため検証しないものとした。同様に複数の認証要素を活用した多要素認証に関しても検証していない。

パスワードに代わる認証要素の検討・考察した結果を表1に示す。各認証要素の検討項目と概要については下記に箇条書きでまとめる。※印に関しては次項の導入コストに記載する。

**表 1** 認証要素の調査と考察

| ✓ | 認証器 | 使用性 | 運用性 | 導入コスト |
|---|---|---|---|---|
| 除外 | 記憶シークレット | 高 | 高 | 低 |
| | ルックアップシークレット | 低 | 高 | 低 |
| | 経路外デバイス | 中 | 中 | 依存※ |
| ✓ | 単一要素 OTP デバイス | 中 | 中 | 依存※ |
| | 多要素 OTP デバイス | 中 | 低 | 依存※ |
| | 単一要素暗号ソフトウェア | 中 | 低 | 中 |
| ✓ | 単一要素暗号デバイス | 高 | 中 | 高 |
| | 多要素暗号ソフトウェア | 低 | 低 | 中 |
| ✓ | 多要素暗号デバイス | 中 | 中 | 依存※ |

- 記憶シークレット
  - 認証例：パスワード
  - 使用性：記憶から呼び出すため利用しやすい
  - 運用性：クレデンシャルの保管に難がある。再発行にコストはかからない
  - 導入コスト：ユーザーの記憶を利用するため無料

- ルックアップシークレット
  - 認証例：乱数表
  - 使用性：毎回ランダムな表から選択するためユーザビリティは劣る
  - 運用性：再発行に関してはパスワードと同様
  - 導入コスト：ユーザーの記憶を利用するため無料

- 経路外デバイス
  - 認証例：SMS、QR コード
  - 使用性：携帯電話やスマートフォンを利用するがクリック
  - 運用性：実装コストが多少かかる、デバイスの基本的な機能で可能
  - 導入コスト：学生のスマートフォンに依存

- 単一要素 OTP デバイス
  - 認証例：OTP デバイス、スマートフォン等のソフトウェア OTP
  - 使用性：特定のアプリのインストールが必要
  - 運用性：個々人のデバイスの設定を行わなければならない。デバイスを保有しなければならない
  - 導入コスト：1 個 ￥1,000 - 2,000

- 多要素 OTP デバイス
  - 認証例：スマートフォン等の指紋認証が搭載されている OTP デバイス
  - 使用性：単一要素 OTP デバイスと同様
  - 運用性：機能を有しているデバイス保有率が低く、対応範囲が狭い
  - 導入コスト：学生のスマートフォンに依存

- 単一要素暗号ソフトウェア
  - 認証例：端末毎のクライアント証明書
  - 使用性：認証開始までの準備が高負荷
  - 運用性：各デバイスのセキュアなストレージ部に保存する必要があり、紛失した際の再発行にコストが発生
  - 導入コスト：クライアント証明書の発行手法に準ずる

- 単一要素暗号デバイス
  - 認証例：FIDO 対応 USB ドングル
  - 使用性：USB デバイスを保持タップするのみと比較的良い
  - 運用性：USB ドングルは FIDO 対応 Server を構築する必要あり
  - 導入コスト：1 個 3,000 - 8,000

- 多要素暗号ソフトウェア
  - 認証例：生体認証等で有効化されるクライアント証明書
  - 使用性：単一要素暗号ソフトウェアと同様ではあり、生体認証を行う必要がある
  - 運用性：生体認証を導入するためのコストが高い
  - 導入コスト：認証デバイスに準じる

- 多要素暗号デバイス

– 認証例：FIDO 対応スマートフォン
– 使用性：単一要素暗号デバイスと同様ではあるが、生体認証を行う必要がある
– 運用性：生体認証を導入するためのコストが高い
– 導入コスト：学生のスマートフォンに依存

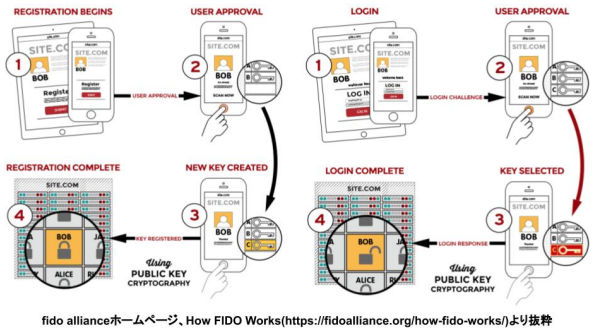
これらの考察からチェックがついているものを本研究で用いる認証要素とした。単一要素 OTP デバイス・単一要素暗号デバイス・多要素暗号デバイスを選定した理由としては、新しい認証を導入するにあたりコストをかけられない部分が大きく影響している。例として 2000 円の認証デバイスを配布することを考えた場合、10,000 人の学生が所属している大学組織においては、20,000,000 円の費用を捻出することになる。そこで、総務省の情報通信白書 [6] によると 20 代のスマートフォンの普及率は 2016 年度の段階で普及率が 94.2%という調査結果が明らかになっている。そのためコストをかけることなく大部分の学生に対して対応が可能であると想定しスマートフォンを認証要素として利用することを前提とした。

### 4.2 認証プロトコルの調査

現在、大学内で利用されている代表的な認証プロトコルとしては、学認や Shibboleth で利用されている SAML があるが、RP-IdP 間の事前設定があることによりプロトコルとしての堅牢性を担保している。しかし SAML はその複雑性から導入が困難であるといわれており、また、OWASP2017[7] において XML eXternal Entity 攻撃の危険性が高く認証情報を XML でやり取りすることを非推奨としているため、利用を視野には入れていない。本研究にでは、学生のサービス管理者にクレデンシャル情報を保管するリスクを低下させるために、Openid Connect(OIDC) と FIDO の利用を検討した。

OIDC は URI ベースで認証を行うことで気軽に認証を行うことが可能になっている。また、認証に使うクレデンシャル情報は OIDC 認証サーバーのみに保管されており、学生主動のサービスに対してはトークンと呼ばれる別途発行される認証情報を用いるため、クレデンシャル情報を保存管理するリスクを抑えることが可能である。

FIDO[8] は、パスワード利用せずに認証を高速に安全に行うことを目的とし、図 2 利用しているデバイスで生体認証を行うことで事前に格納しているに秘密鍵を呼び出し、PKI で認証を行うことが可能になる。また、近年 FIDO2 という Web ブラウザで利用することを目的として W3C 標準となった webauthn[9] がある。この方式を用いることでサービス管理者は PKI と同様の公開鍵を保管するのみで良いため情報漏洩時のリスクを低減することができる。



fido allianceホームページ、How FIDO Works(https://fidoalliance.org/how-fido-works/)より抜粋

図 2 FIDO の登録と認証の基本的な flow

## 5. プロトタイプ認証基盤の展開と運用

調査・検討結果から本研究では、

- 認証要素
  – 単一要素 OTP デバイス, 単一要素暗号デバイス, 多要素暗号デバイス
- 認証プロトコル
  – OIDC, FIDO, FIDO2

を要件とし、これらを満たす認証を実現するために実際にプロトタイプとして認証基盤の展開と運用を行った。

### 5.1 認証基盤およびフレームワークの選定

認証サーバーを構築するにあたり、オープンソースな認証基盤および認証フレームワークを用いることとして調査・選定を行った。選定基準としては、

- 前項の要件を満たしている、もしくは、おおよそ満たしている
- 脆弱性の早期発見、継続的な運用を行う必要があるため開発コミュニティが活発
- 学生に対して認証を提供するためフリーな開発・提供が可能なライセンスである

を重要視し、セキュリティ面から、OpenID Foundation が認定した Certified OpenID Connect Implementations[10] から選定する。候補として選定した認証フレームワークを表 2 に示す。この中から、開発コミュニティが活発である

表 2 認証サーバーの候補

| 名称 | ライセンス | 認定者 |
|---|---|---|
| MITREid Connect[11] | Apache License 2.0 | Justin Richer |
| Keycloak[12] | Apache License 2.0 | Red Hat |
| ORY Hydra[13] | Apache License, 2.0 | ORY GmbH |

ことと FIDO や webauthn 等の最新の認証要素に対する取り組みについても言及していることから Keycloak をメインフレームとして開発することとした。

### 5.2 開発・運用中の認証基盤の紹介

慶應義塾大学メディアデザイン研究科内に展開・運用している KMD-Auth について紹介する。まず、KMD-Auth の構成および特徴を以下に示す。

- 提供開始日
  - 2019/4/29
- 利用サービス数
  - 1
- 認証基盤
  - Keycloak 5.0.1(latest:6.0.1)
- 安定提供している認証要素
  - ユーザー/パスワード
  - ワンタイムパスワード (TOTP)
  - FIDO U2F
- 試用提供している認証要素
  - webauthn Yubikey
- 開発中の認証要素
  - webauthn Android
  - webauthn 指静脈認証

認証基盤では、サービスで認証を行う際に Web ブラウザ上で特定の URI に誘導することで、図 3 に示すような認証サービスを提供している。サービス管理者は、認証時に指定された URI にアクセスし、認証成功後に URI に JWT[14] で格納されている token 情報を利用することで検証とアクセスコントロールを行うことが可能になっており、各自サービスに認証サーバーを構築することなく認証を行うことができる。

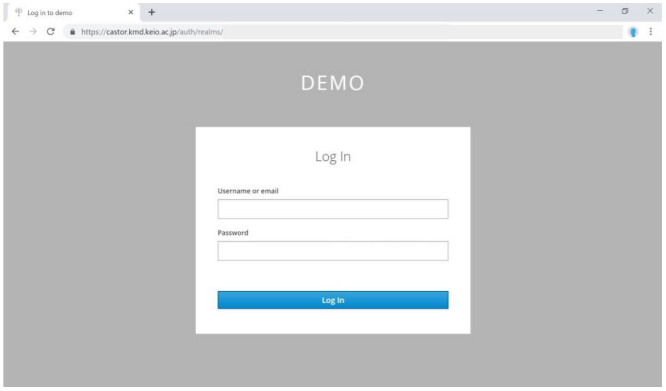



**図 3** 提供している実際の認証画面の例

現状としては、本研究科の学生が開発運用している研究用途の Web サービスに対して認証を提供しており、図 4 に示しているような認証 flow となっている。提供している認証要素としては、ユーザー名/スマートフォンにインストールされているソフトウェア OTP のみを利用しており、事前に別途 Keycloak に OTP デバイスを登録しているユーザーのみを対象に利用している。

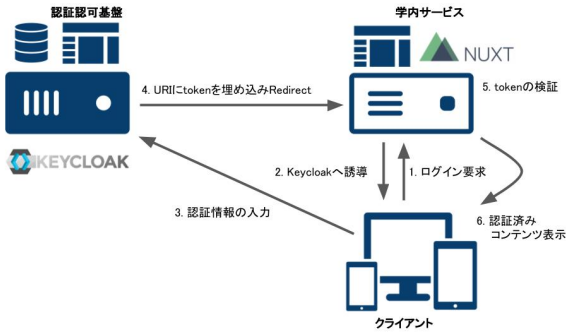



**図 4** 実際の学内サービスでの利用

今後のマイルストーンとしては既存の学内サービスである、研究科ホームページ、研究科独自の学習支援システムの各認証サーバーを廃止、ユーザー情報を移植したのちに認証を提供することを予定している。

## 6. 課題

本研究での調査を通して得られた課題について述べる。

### 6.1 認証要素について

学内においてパスワードに代わる認証要素を導入することは比較的可能なのではないかと考える。理由としては、指紋認証のような学生が普段利用している認証に置き換えるため利用を開始する障壁が少ないこと、Web ブラウザを利用する場合、標準機能として実装されている認証要素が多くユーザーの環境に依存しにくいためである。反面、OTP などデバイスごとの設定が必要になる場合においては学生が使いこなすことが可能であるかという課題は残る。

### 6.2 認証の提供について

学生のサービスに認証を提供することに関しては課題が多く残っている。まず、そもそもとして学生に利用してもらわなければならないという課題があり、学生に対して広く告知し学生がサービスを構築を行う際の実装の候補に挙がる必要がある。そのためには、構築が容易になることだけではなく、利用した場合に得られるメリットを明確にするべきである。また、学生がクレデンシャル情報である token の取り回しなどの OIDC 準拠の専門的な実装をしなければならないこともあり、これに関しては設計要件のドキュメントおよび Proof of Concept 実装を提供することが重要になってくると考えている。

### 6.3 運用について

認証基盤の実運用を通して、ユーザー登録、デバイスを持っていない人への対応という課題が見えてきた。学生のユーザー登録に対しては登録者が学生であるか否かを判断しなければならず、現状としては学籍番号等の学生のみが保持する情報を利用することが考えられるが、ユーザーに

対する負担が大きくなってしまう。そこで、学生に全員に対し事前に一時的なアカウントを発行し、ユーザー登録専用サービスにおいて OTP や FIDO のクレデンシャルを登録していもらう方法を検証する予定である。スマートフォン等の認証デバイスを保持していないユーザーに対しては、可能な限り全学生に対応することを考えた場合、学生証などの NFC カードを利用することが考えられたが、認証を行うための NFC リーダーが必要なという問題や、解決方法として、学内に NFC リーダーと認証クライアントポイントを常設し SSO を通して一定期間中の認証を賄うことを検討しているが具体的な解決の見通しは立っていない。

## 7. おわりに

本研究では、学内サービスにおいてパスワードを利用しない認証を導入するためパスワード以外の実現性がある認証要素、プロトコルについて検討を行った。また、実際に認証基盤の導入および運用を開始し実サービスに対して認証の提供を試験的に行っている旨を示した。今後は、スマートフォンなどのユーザーが保持している機材に頼らず、指静脈認証器や学生証等の NFC カードの利用についても検討し、全ユーザーがパスワード以外の認証方式を行うことが可能な環境を整えることを検討していく。また、認証だけではなく生体情報等の効率的なユーザー登録についても検討する必要がある。

### 参考文献


[1] Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur, ”Measuring Password Guessability for an Entire University”,CCS ’13,p173-186

[2] 熊谷匠純, 菊地拓翔, 澤信吾, 加藤菜美絵, 関良明, ” —”, 電子情報通信学会論文誌 D,Vol.J101-D,No.10,pp.1438-1442

[3] 森井理智, 谷岡広樹, 大平健司, 佐野雅彦, 松浦健二, 関陽介, 上田哲史, ”パスワードレス認証方式を用いた認証連携に関する研究”, 研究報告インターネットと運用技術(IOT),2017-IOT-37,vol5,p1-6

[4] Digital Identity Guidelines Authentication and Lifecycle Management，入手先 ⟨https://pages.nist.gov/800-63-3/sp800-63b.html⟩（参照 2019-05-06）.

[5] 「2018 年度情報セキュリティに対する意識調査」報告書について，入手先 ⟨https://www.ipa.go.jp/security/fy30/reports/ishiki/index.html⟩（参照 2019-05-06）.

[6] 総務省 | 平成 29 年版 情報通信白書，入手先 ⟨http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/n1100000.pdf⟩（参照 2019-05-06）.

[7] Top 10-2017 Top 10，入手先 ⟨https://www.owasp.org/index.php/Top_10-2017_Top_10⟩（参照 2019-05-06）.

[8] FIDO Alliance ”Alliance Overview, Changing the Nature of Authentication”，入手先 ⟨https://fidoalliance.org/overview/⟩（参照 2019-05-06）.

[9] Web Authentication: An API for accessing Public Key Credentials Level 1，入手先 ⟨https://www.w3.org/TR/webauthn/⟩（参照 2019-05-06）.

[10] Certified OpenID Connect Implementations，入手先 ⟨https://openid.net/developers/certified/⟩（参照 2019-05-06）.

[11] OpenID-Connect-Java-Spring-Server，入手先 ⟨https://github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server⟩（参照 2019-05-06）.

[12] Keycloak，入手先 ⟨https://github.com/keycloak/keycloak⟩（参照 2019-05-06）.

[13] Hydra，入手先 ⟨https://github.com/ory/hydra⟩（参照 2019-05-06）.

[14] RFC7519 JSON Web Token (JWT)，入手先 ⟨https://tools.ietf.org/html/rfc7519⟩（参照 2019-05-06）.