Wed, 18 Oct 2017 06:55:32 +0000

**NIST 特別出版物800-63C デジタル ID ガイドライン(翻訳版)**

*連携とアサーション*



Paul A. Grassi Justin P. Richer Sarah K. Squire James L. Fenton Ellen M. Nadeau

**Privacy Authors:** Naomi B. Lefkovitz

Jamie M. Danker

**Usability Authors:** Yee-Yin Choong

Kristen K. Greene Mary F. Theofanos

この出版物は以下から無料で入手できる: https://doi.org/10.6028/NIST.SP.800-63c

**NIST 特別出版物 800-63C**

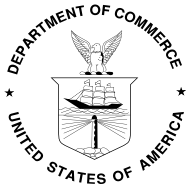
**デジタル ID ガイドライン**

## 連携とアサーション

|  |  |
| --- | --- |
| Paul A. Grassi Ellen M. Nadeau  *Applied Cybersecurity Division Information Technology Laboratory* | James L. Fenton *Altmode Networks Los Altos, Calif.* |
| Justin P. Richer Sarah K. Squire *Bespoke Engineering Billerica, Mass.* |  |
| **Privacy Authors:** Naomi B. Lefkovitz  *Applied Cybersecurity Division Information Technology Laboratory*  Jamie M. Danker *National Protection and Programs Directorate Department of Homeland Security* | **Usability Authors:** Yee-Yin Choong Kristen K. Greene  *Information Access Division Information Technology Laboratory*  Mary F. Theofanos *Office of Data and Informatics Material Measurement Laboratory* |
|  | **翻訳者:** Nov Matake  *YAuth.jp LLC* |

この文書の無料入手先: https://doi.org/10.6028/NIST.SP.800-63c

2017年6月



U.S. Department of Commerce *Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology *Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology*

## **権限**

この出版物は, 2014年の連邦情報セキュリティ現代化法 (Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283) の下で NIST がその法定責任に従って発展させた. NIST は, 連邦情報システムのための最小限の要件を含め, 情報セキュリティの標準およびガイドラインの発展に責任を負うが, その標準とガイドラインは, 全国的なセキュリティシステムにポリシー権限を行使する適切な連邦政府職員の明確な承認がなければ, そうしたシステムに適用されてはならない. このガイドラインは, 行政管理予算局 (OMB) の回状 A-130 の要件と一致している.

この出版物に記載されたいかなることも, 商務長官が法的権限の下で連邦機関に義務付け拘束力を持たせた標準とガイドラインに反駁するために用いられるべきではない. また, これらのガイドラインは, 商務長官, 行政管理予算局長官, またはその他の連邦職員の既存の権限を変更したりそれに取って代わったりするものと解釈されるべきではない. この出版物は, 非政府組織が自由意志に基づいて使用でき, 米国において著作権の対象にならない. しかしながら, 引用で出典として示されることが望ましい.

National Institute of Standards and Technology Special Publication 800-63C

Natl. Inst. Stand. Technol. Spec. Publ. 800-63C, 48 pages (June 2017)

CODEN: NSPUE2

この出版物は以下から無料で入手できる.

https://doi.org/10.6028/NIST.SP.800-63c

この文書では, 試験的な手順や概念を適切に記述する目的でいくつかの商業的なエンティティ, 装置, 材料を特定している場合がある. こうした特定は, NIST による推奨や支持を意味せず, そうしたエンティティ, 装置, 材料がその目的に対して最も有効であることを必ずしも意味していない.

この出版物では, 割り当てられた法的責任に応じてNIST が現在開発中の他の出版物を参照に挙げている場合がある。この出版物に含まれる情報は, 概念と方法論も含め, 付属文書が完成する前でも連邦機関て使用する場合がある. したがって, 現在の要件, ガイドライン, 手順がある場合は, それぞれの出版物が完成するまでそれが有効である. 計画目的と移行目的に対しては, 連邦機関は NIST によるこうした新しい出版物の発展に綿密に従うことを求めてもよい.

各機関は, パブリックコメントの期間中にすべての暫定版を調べ, NIST に意見を提示することが奨励される. 上記の他にもサイバーセキュリティに関する NIST の多くの出版物は, http://csrc.nist.gov/publicationsから入手できる.

**この出版物に関する意見の提出先**:

National Institute of Standards and Technology

Attn: Applied Cybersecurity Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Email: [dig-comments@nist.gov](mailto:dig-comments@nist.gov)

すべての意見は, 情報公開法 (FOIA) の下で公表される.

## **コンピュータシステム技術に関するレポート**

国立標準技術研究所 (National Institute of Standards and Technology, NIST) の情報技術研究所 (Information Technology Laboratory ,ITL) は, 測定と標準に関する全国インフラのための技術的リーダーシップを提供することにより, 米国経済と福祉を促進する. ITL は, 情報技術の発展と生産的利用を押し進めるために, テスト, テスト方法, 参照データ, 概念検証の実装, テクニカル分析を開発している. ITL の責任には, 連邦システムの全国セキュリティ関連情報以外の経済的なセキュリティとプライバシーに対し, マネージメント, 行政, 技術, 物理上の標準とガイドラインの促進が含まれている. 特別出版物 800 シリーズは, 情報システムセキュリティにおける ITL の研究, ガイドライン, 社会福祉の支援努力と, 産業, 政府, 学術組織の共同作業に関するレポートである.

## **概要**

この文書と付属文書の SP 800-63, SP 800-63A, SP 800-63Bは, 連携した身元識別情報システムの実装と連携で使用するアサーションのための技術および手続き上のガイドラインを連邦機関に提供する. この出版物は, SP 800-63-2 の対応するセクションに取って代わる.

これらのガイドラインは, デジタル ID サービスを実装する連邦機関に技術的要件を提供するもので, この目的以外の基準の開発や使用を妨げるものではない. このガイドラインは, 連携した身元情報の使用と身元情報連携を実装するためのアサーションの使用に重点を置いている. 連携により認証情報サービスプロバイダは個別に管理している多くの証明書利用者に対して認証と加入者属性 (随意) を提供することができる. 同様に, 証明書利用者は１つ以上の認証情報サービスプロバイダを利用することができる.

## **キーワード**

アサーション; 認証; 認証情報サービスプロバイダ; デジタル認証 電子認証; 電子認証情報; 連携.

## **謝辞**

SP 800-63 のすべての巻で芸術的な図表を作成してくれた Kaitlin Boeckl と, 貴重な意見を寄せてくれたDigital ID & Authentication Council of Canada (DIACC)のJoni Brennan from the, NISTの Kat Megas および Ben Piccarreta, そしてDeloitte & Touche LLP の Christine Abruzzi および Danna Gabel O’Rourke に感謝している.

これに加え, 原文を執筆してくれた Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus のリーダーシップと革新的考え方に敬意を表したい. こうした方々のたゆまない努力がなければ, 800-63 を今日ある文書に発展させたすばらしい土台は築けなかったであろう.また, プライバシーに関する要件と考慮事項の発展に貢献してくれた連邦プライバシー委員会のデジタル認証タスクフォースの方々に特にお礼を申し上げる.

## **表記法**

「SHALL（しなければならない）」および「SHALL NOT（してはならない)」という用語は, この出版物に厳密に従うことを要求しており, これから逸脱することは許されない.

「SHOULD（すべきである）」および「SHOULD NOT（すべきでない）」という用語は, いくつかある選択肢の中で特に適切なものとして１つが推奨されることを示しており, 他の選択肢については言及も除外もしない. または, ある行動方針が望ましいが必ずしも要求されないことを示す. または,（否定の意味では）ある可能性や行動方針を推奨しないが禁止もしないことを示す.

「MAY（してもよい）」および「NEED NOT（しなくてよい）」という用語は, 出版物の範囲において行動方針が許容できることを示す.

「CAN（できる）」および「CANNOT（できない）」という用語は, 物質的であれ, 物理的であれ, 必然的であれ,可能性や能力があることを示し, 否定の意味では可能性や能力がないことを示す.

# 目次

# Purpose 1

# Introduction 2

# Definitions and Abbreviations 4

# Federation Assurance Levels 5

* 1. Key Management 6
  2. Runtime Decisions 6

# Federation 8

* 1. Federation Models 9
     1. Manual Registration 9
     2. Dynamic Registration 10
     3. Federation Authorities 11
     4. Proxied Federation 12
  2. Privacy Requirements 13
  3. Reauthentication andセッションRequirements in Federated Environments 14

# Assertions 15

* 1. Assertion Binding 16
     1. Bearer Assertions 16
     2. Holder-of-Key Assertions 16
  2. Assertion Protection 17
     1. Assertion Identifier 17
     2. Signed Assertion 18
     3. Encrypted Assertion 18
     4. Audience Restriction 18
  3. Pairwise Pseudonymous Identifiers 18
     1. General Requirements 18
     2. Pairwise Pseudonymous Identifier Generation 19

# Assertion Presentation 20

* 1. Back-Channel Presentation 20
  2. Front-Channel Presentation 22
  3. Protecting Information 23

# Security 24

* 1. Federation Threats 24
  2. Federation Threat Mitigation Strategies 25

# Privacy Considerations 27

* 1. Minimizing Tracking and Profiling 27
  2. Notice and Consent 28
  3. Data Minimization 28
  4. Agency-Specific Privacy Compliance 29
  5. Blinding in Proxied Federation 29

# Usability Considerations 31

* 1. General Usability Considerations 31
  2. Specific Usability Considerations 32
     1. User Perspectives on Online Identity 33
     2. User Perspectives of Trust and Benefits 34
     3. User Models and Beliefs 35

# Examples 36

* 1. Specific Assertion Markup Language (SAML) 36
  2. Kerberos Tickets 36
  3. OpenID Connect 37

# References 39

* 1. General References 39
  2. Standards 39
  3. NIST Special Publication 40

# Federal Information Processing Standards 40

**List of Figures**

Figure 5-1 Federation 8

Figure 5-2 Manual Registration 9

Figure 5-3 Dynamic Registration 10

Figure 5-4 Federation Authority 12

Figure 5-5 Federation Proxy 13

Figure 7-1 Back Channel Presentation 20

# Figure 7-2 Front Channel Presentation 22

**List of Tables**

Table 2-1 Normative and Informative Sections of 800-63C 3

Table 4-1 Federation Assertion Levels 5

Table 8-1 Federation Threats 24

Table 8-2 Mitigating Federation Threats 25

Table 9-1 Federation Proxies 30

**正誤表**

この表は, 特別出版物 800-63-3 で加えられた変更の一覧である. 正誤表の更新には, 編集上または実質上の修正, 明確化, その他のマイナーな変更を含めることができる.

|  |  |  |  |
| --- | --- | --- | --- |
| **日付** | **種類** | **変更** | **場所** |
| 2017-12-01 | 編集上 | セクション 5 のタイトルを “連携” に変更 | セクション 5 |
|  | 実質上 | 属性所有の要件を明確化 | セクション 5.2 |
|  | 実質上 | 言葉づかいを見直して “プライバシー目標” という言葉を入れ, 同意の明示を指定 | セクション 9.1 |
|  | 編集上 | 参照として NISTIR 8062 を追加 | セクション 12.1 |

# 目的

*このセクションは参考情報である.*

[この推奨文書と付随文書 SP 800-63 (sp800-63-3.html), SP 800-63A (sp800-63a.html), SP 800-63B (sp800-63b.html) では, 認証情報サービスプロバイダ (CSP) がデジタル認証を実装する際の技術的ガイドラインを⽰す.](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html)

この文書 SP 800-63C では, 連携した身元識別情報システムにおける身元情報プロバイダ (IdP) と証明書利用者(RP) に対する要件を⽰す. 連携を利⽤すると, ある１つの IdP が, 独⽴して個別管理された複数の RP に対して, アサーションを使用して認証と加入者属性 (随意) を提供することができる. 同様に RP が複数の IdP を利⽤することもできる.

# はじめに

*このセクションは参考情報である..*

連携はネットワーク接続されたシステム間で認証および加入者属性の情報を伝達可能にするプロセスである. 連携シナリオでは, 検証者または CSP は身元情報プロバイダ (IdP) と呼ばれ, RP は IdP が提供する情報を受け取り利⽤する主体となる.

連携した身元情報 (連携 ID) システムは, 上記タスクを完了するためにアサーションを利⽤する.アサーションは, IdP から RP に宛てたステートメントで, 加入者に関する情報が含まれる. 連携技術は, RP と IdP が異なる主体か, 異なる管理下にある場合に利⽤されるのが一般的である. RP はアサーションに含まれる情報を利⽤して加入者を識別し, RP が管理下に置くリソースに加入者がアクセスする際の認証決定を⾏う.通常アサーションは加入者の識別⼦を含み, 過去の RP との通信と加入者を関連付けることを可能にする.アサーションにはさらに属性値や属性参照を含めてもよく, RP での認証決定の際に加入者についてより詳しい特徴を伝える. 補足的な属性は, より⼤規模な連携プロトコルの一部としてアサーションの外で利用できる場合もある. こうした属性値と属性参照は,属性ベースアクセス制御 (ABAC) に対するアクセス権限の決定や, トランザクションの促進 (例えば, 配送先住所) によく使用される.

連携 ID シナリオでは,加入者は RP に対して直接認証するわけではない. その代わり, 連携プロトコルを定義し, 通常は RP からのリクエストに応じたレスポンスとして, IdP が加入者に関連付けられた識別⼦に対するアサーションを⽣成する⼿段を設ける. IdP は [(SP 800-63B, セクション 7 (sp800-63b.html#sec7)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#sec7) に述べたセッション管理を使うかもしれないが) 加入者を責任を持って認証する. このプロセスにより,加入者は個々の RP に対して独⽴した認証情報を所有・管理することなく, 複数の RP からサービスを受けることができる. またシングルサインオンも可能となり, 加入者はひとたび IdP に対して認証すれば, それ以降複数の RP からサービスを受けることもできる.

連携には, セキュリティとプライバシーに関する複雑な要件があり, 注意深い検討が必要な⽐較的複雑なマルチパーティープロトコルが必要である. 特定の連携構造を評価する際は, 構成要素間のインタラクションに分解するとよいかもしれない. ⼀般的に,加入者と IdP の間の認証は SP 800-63B で述べた認証⽅式に基づいて⾏われ, IdP と RP の間の通信は SP 800-63A で述べた⼿順により確⽴された属性とその他の自己表明属性を伝達する. したがって, この文書で提⽰する多くの要件は, これら2つの文書の対応する要件と何らかの関係がある.

以下の表は, この文書のどのセクションが規範であり, どのセクションが参考情報であるかを⽰している.

**表 2-1 800-63C の規範セクションと参考情報セクション**

|  |  |
| --- | --- |
| **セクション名** | **規範/参考情報** |
| 1. 目的 | 参考情報 |
| 2. はじめに | 参考情報 |
| 3. 定義と略語 | 参考情報 |
| 4. 連携保証レベル (FAL) | 規範 |
| 5. 連携 | 規範 |
| 6. アサーション | 規範 |
| 7.アサーション提示 | 規範 |
| 8. セキュリティ | 参考情報 |
| 9. プライバシーの考慮事項 | 参考情報 |
| 10. ユーザビリティの考慮事項 | 参考情報 |
| 11. 例 | 参考情報 |
| 12. 参考文献 | 参考情報 |

# 定義と略語

定義と略語については, すべて [SP 800-63 (sp800-63-3.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.html) 付録 A を参照.

# 連携保証レベル (FAL)

*このセクションは規範である.*

このセクションでは, 許容可能な連携保証レベル (FAL) を定義する. FAL はあるトランザクションにおいてアサーションを構成し保護するための要件について述べたものである. これらのレベルは, あるトランザクションにおいて RP が要求することもあれば, RP と IdP との間の設定で必要とされることもある.

すべてのアサーションはセクション 4 に述べるように連携プロトコルと共に⽤いなければならない (SHALL). すべてのアサーションはセクション 6 に詳説する要件に従わなければならない (SHALL). すべてのアサーションはセクション 7 に述べるいずれかの⽅法で提⽰されなければならない (SHALL). さまざまな連携実装パターンが考えられるが, FAL はよりセキュアな構築オプションを⽰す明確な推奨事項を提供することを意図している. FAL の表に載っていないさまざまな側⾯がありうるが, それらはこの巻の扱うところではない. 最適な FAL の詳しい選択⽅法については [SP 800-63 セクション 6.3 (sp800-63-3.html#FAL\_CYOA)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.html#FAL_CYOA) を参照.

この表は FAL ごとに異なる要件を⽰す. ⼀連の各レベルは, より低いレベルのすべての要件を含み, 満たしている. プロキシを介した連携は, プロキシされるトランザクションの中で最も低いレベルで示されなければならない(SHALL).

#### 表 4-1 連携アサーションレベル

|  |  |
| --- | --- |
| **FAL** | **要件** |
| 1 | ベアラアサーション, IdP が署名 |
| 2 | ベアラアサーション, IdP が署名し RP に暗号化 |
| 3 | 鍵アサーションの保持, IdP が署名し RP に暗号化 |

例えば, FAL1 は特に機能追加の無い OpenID Connect Basic Client プロファイルや Security Assertion Markup Language (SAML) Web SSO Artifact Binding プロファイルに相当する. FAL2 は, それに加えアサーション（例えば, OpenID Connect ID トークンや SAML アサーション）に対する RP の公開鍵による暗号化を要求する. FAL3 では, FAL2 のすべての要件に加え, アサーションに結び付けられた鍵の所有証明を加入者が暗号論的に⾏う必要がある（例えば, 暗号認証コードを利⽤）. FAL3 で登場する鍵は, 加入者が IdP に対して認証する際に利⽤する鍵と同⼀でなくてもよい.

RP はリクエストするものや必要なプロトコルとは無関係に, 連携プロトコルの一部として提⽰されるアサーションの性質を観察すると, 利⽤している FAL を容易に知ることができる. したがって RP は, 特定の認証トランザクションに対して受け⼊れる FAL を決定し, トランザクションがその FAL 要件を満たすことを保証する責任がある.

RP が セクション 7.2 にあるようなフロントチャネル提⽰方法（例えば, OpenID Connect Implicit Client プロファイルや SAML Web SSO プロファイル）を使用している場合, トランザクションで目的の RP 以外の主体やブラウザにアサーションの情報が漏洩することを防ぐため, FAL2 以上が適用されなければならない (SHALL).

さらに IdP は, SP 800-53 に定義されている “中” か “高” 基準のセキュリティ管理やそれに相当する連邦政府標準（例えば, FEDRAMP）や業界標準から,（管理強化を含めるように）適切に調整したセキュリティ管理を採⽤しなければならない (SHALL).

* 1. **鍵の管理**

どの FAL においても, IdP は認可された暗号技術を使用する署名と鍵でアサーションを保護し, RP がその他の RP に対して IdP になりすますことができないよう保証しなければならない (SHALL).アサーションが 対称鍵を使ったデジタル署名で保護されている場合, IdP は同じ公開鍵とプライベート鍵のペアを複数の RP に対する署名に利⽤してもよい (MAY). IdPは, HTTPS で保護された周知の URL を経由するなどして, 検証可能な形で⾃⾝の公開鍵を公開してもよい (MAY). アサーションが共有鍵を⽤いた MAC によって保護されている場合, IdP は RP ごとに異なる共有鍵を使わなければならない (SHALL).

AAL2 で認証を行う政府運営の IdP と, AAL3 で認証を⾏うすべての IdP は, FIPS 140 レベル 1 以上で検証される⼿段を用いて, アサーションの署名と暗号化に使う鍵を保護しなければならない (SHALL).

## **実行時の決定**

連携しているという事実は,情報を提供する許可を得たと解釈してはならない (SHALL NOT).認証を⾏うかどうかや属性を提供するかどうかは, ホワイトリストやブラックリスト, 認可された主体による実行時の決定などによって確定することができる.

IdP は RP のホワイトリストを作成し, そこに含まれる RP に対しては加入者による実行時の決定なしに IdP から認証結果や属性を受け取れるようにしてもよい (MAY). IdP のホワイトリストに含まれるすべての RP は, SP 800-63 シリーズの規定と要件に従わなければならない (SHALL). IdP は, セクション 9.2 にあるように,加入者がホワイトリストを使用できるようにしなければならない (SHALL). IdP は RP のブラックリストを作成し, そこに含まれる RP に対しては加入者からの要求があっても IdP による認証結果や属性を受け取れないようにしてもよい (MAY). ホワイトリストでもブラックリストでも, 利⽤する連携プロトコルに応じて, RP はドメインや確実に一意の識別⼦を⽤いて識別される. どちらのリストにも含まれない RP は, 通常は加入者である認可された主体が認証の実行時を決定するグレーゾーンに配置されなければならない (SHALL). IdP は特定の RP に対する加入者の認証決定を記録してもよい (MAY). ただしその場合は, IdP は記録したアクセスを加入者が将来無効化できるようにしなければならない (SHALL).

RP は IdP のホワイトリストを作成し, そこに含まれる IdP に関しては加入者による実行時の決定なしに認証結果や属性を受け⼊れるようにしてもよい (MAY). RP のホワイトリストに含まれるすべての IdP は, SP 800-63 シリーズの規定と要件に従わなければならない (SHALL). RP は IdP のブラックリストを作成し, そこに含まれる IdP に関しては加入者からの要求があっても認証結果や属性を受け⼊れないようにしてもよい (MAY). ホワイトリストでもブラックリストでも, 利⽤する連携プロトコルに応じて, IdP はドメインや確実に一意の識別⼦を⽤いて識別される. どちらのリストにも含まれない IdP は, 通常は加入者である認可された主体が認証の実行時を決定するグレーゾーンに配置されなければならない (SHALL).. RP は特定の IdP に対する加入者の認証決定を記録してもよい (MAY). ただしその場合は, IdP は記憶したこうしたアクセスを加入者が将来無効化できるようにしなければならない (SHALL).

たとえ相互にホワイトリストに含まれていたとしても, セクション 5.2 に記載する⽬的以外では,加入者に関する情報を IdP と RPの間でやりとりしてはならない (SHALL NOT).

要注意情報が漏洩するリスク（例えば, 肩越しの盗み見）を軽減するため, IdP はデフォルトでは要注意情報をマスクして加入者に提⽰しなければならない (SHALL). IdP は⼀時的にそれらのマスクを外す⼿段を加入者に提供し, 全体の値を見られるようにしなければならない (SHALL). IdP は加入者の苦情や問題 （例えば, 不正確な属性値を加入者が発⾒）の是正のための有効な⼿段を提供しなければならない (SHALL). マスキングと是正についての詳細については, セクション 10 のユーザビリティの考慮事項を参照.

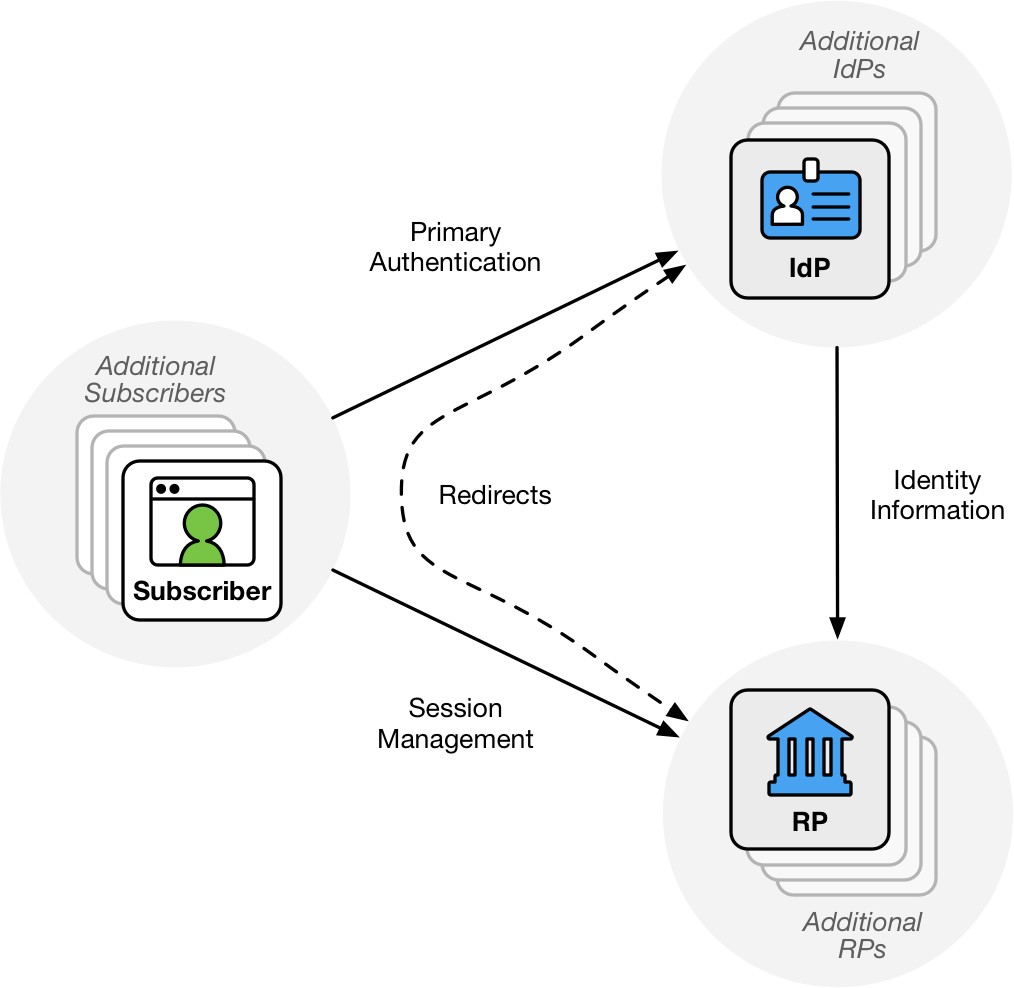
加入者が実行時の決定に関わる場合,加入者は明⽰的な通知を受け取り,自分の属性が RP に送信される前に同意を表明できなければならない (SHALL). 少なくともこの通知は, 最も効果的な通知を提供して確認を得る⽴場にある主体が, セクション 9.2 に従って⾏うべきである (SHOULD). 利⽤するプロトコルでオプショナルな属性が利⽤可能であれば,加入者にはそれらの属性を RP に提供するか否かの選択肢が与えられなければならない (SHALL). IdP はなんらかの記録メカニズムを採⽤し, 同じ RP に対して正確な属性バンドルを再送するようにしてもよい (MAY).

# 連携

*このセクションは規範である.*

連携プロトコルでは, 図 5-1 に⽰すように加入者, IdP, RP の3者の関係が構築される. プロトコルの特性により, どのタイミングでどの主体の間でどんな情報がやりとりされるかは異なる. 一般的に加入者はブラウザを介して IdP と RP の両⽅とやりとりする. RP と IdP の間の通信⽅法は2通りある.

* *フロントチャネル:* 加入者が関わるリダイレクト通信
* *バックチャネル:* RP と IdP のダイレクト通信で, 加入者は関わらない



#### 図 5-1 連携

（図の説明）

左

別の加入者 加入者

中央

第1認証 リダイレクト セッション管理

右

別の IdP IdP 身元情報 RP 別のRP

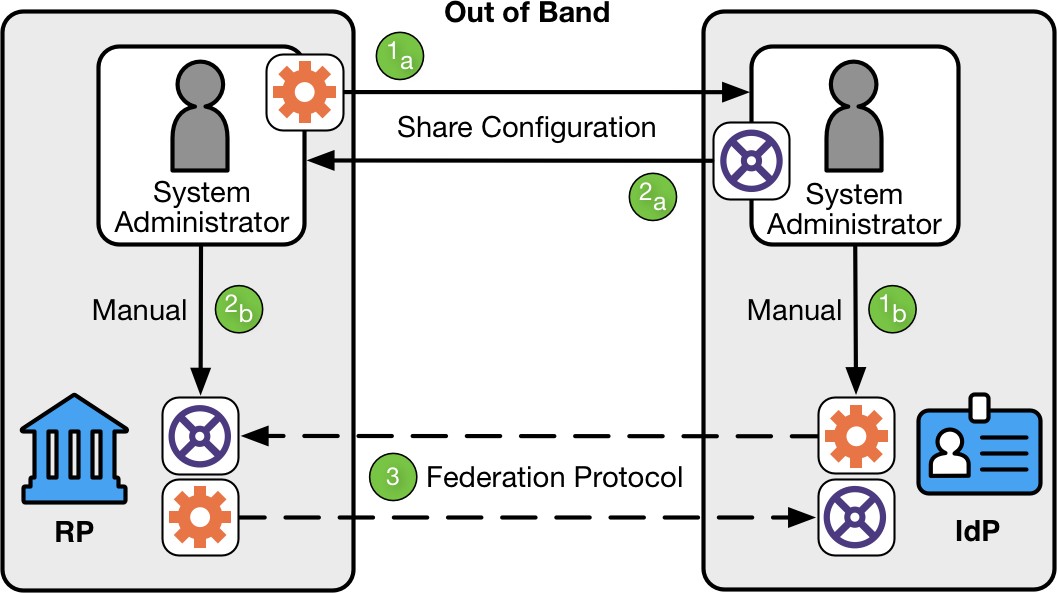
加入者は IdP に対して認証し,認証イベントの結果がネットワーク経由で RP に提⽰される. このトランザクションにおいて, IdP は [SP 800-63B (sp800-63b.html)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html) にあるように認証情報の検証者になる. IdP はこのプロセスの一部として加盟者に関する属性ステートメントを作成することもできる.属性と認証イベントの情報は, セクション 6 にあるようにアサーションを通じて RP に伝送される. 追加の属性については, 認可された認証情報で保護された2番目のプロトコルを通じて利用できるようにしてもよい (MAY).

* 1. **連携モデル**

認証サービスを提供する IdP とそれを利⽤する RP は 連携の参加者として知られる. IdP の視点から⾒れば,連携は⾃⾝がサービスを提供する RP から構成される. RP の視点から⾒れば, 連携は⾃⾝が利⽤する IdP から構成される. このセクションでは,現在使われている⼀般的な ID 連携モデルに対する要件を概説する. 各モデルにおいて,連携参加者の間で関係性が確⽴される.

### **手動登録**

⼿動の登録モデルでは, IdP と RP が相互運⽤する相⼿に関する設定情報を手動で⽤意する. IdP は明⽰的ホワイトリストによって RP を設定し, そこに含まれる RP に関しては認証トランザクション中で認証や属性に関する情報を受け取れるようにしてもよい (MAY). RP がホワイトリストに含まれない場合は, IdP はユーザー情報を提供する前に, 認可された主体（加盟者など）による実行時の決定（セクション 4.2 参照）を要求しなければならない (SHALL).



**図 5-2 手動登録**

（図の説明）

左

システム管理者 手動 RP

中央

アウトオブバンド 構成共有 連携プロトコル

右

システム管理者 手動 IdP

図 5-2 に⽰すとおり, ⼿動登録は以下の3ステップから成る.

1. RP のシステム管理者が RP の属性を IdP のシステム管理者に共有し, IdP のシステム管理者はその属性を RP に関連付ける.
2. IdP のシステム管理者が IdP の属性を RP のシステム管理者に共有し, RP のシステム管理者はその属性を IdP に関連付ける.
3. その後 IdP と RP は標準的な連携プロトコルを使って通信する.

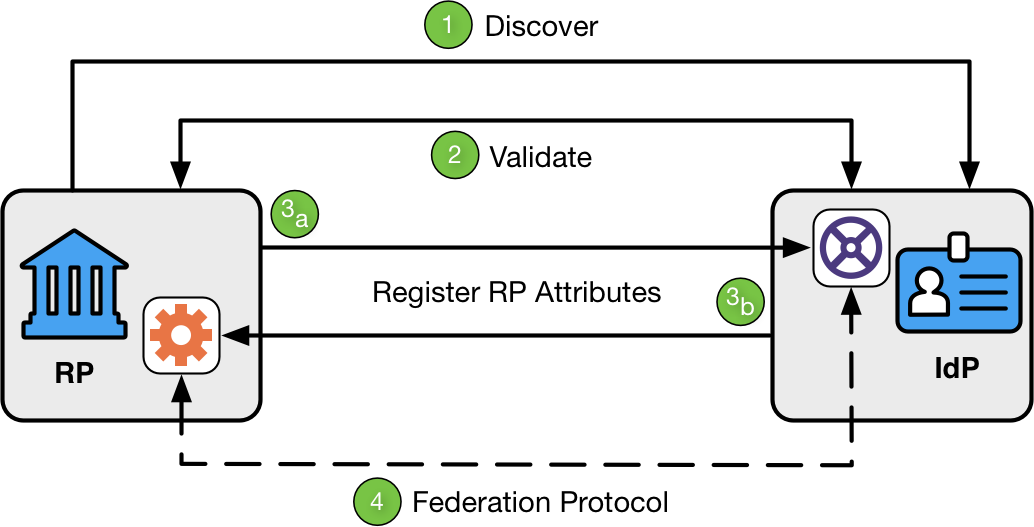
IdP と RP は, ⾃⾝を連携相手のオーソリティとしてもよいし (MAY), セクション 5.1.3 のようにこうしたオーソリティ決定を外部の主体に依頼してもよい (MAY).

鍵情報の伝送を必要とするプロトコルでは, 登録プロセスにおいてセキュアな⽅法で連携された関係性の運⽤に必要な鍵情報を交換しなければならない (SHALL). これには共有シークレットも公開鍵も含まれる. この関係性を⽰すために利⽤される鍵が対称鍵である場合は, 連携参加者のペアに一意でなければならない (SHALL).

連携の関係性に対して, 期待され許容される IAL および AAL に関するパラメーターを確⽴しなければならない (SHALL).

### **動的登録**

連携の動的登録モデルでは,トランザクション実⾏時に連携参加者間でその関係性を取り決めることができる. このプロセスにより, IdP と RP は⼿動登録（セクション 5.1.1 参照）で接続を確⽴することなく, 相互接続することができる. 動的登録をサポートする IdP は, ⾃⾝の設定情報（動的登録のエンドポイントなど）を取得可能にし, システム管理者の関与を最⼩化しなければならない (SHALL).



#### 図 5-3 動的登録

#### （図の説明）

#### １．発見

#### ２．確認

#### ３．RP 属性の登録

#### ４．連携プロトコル

#### 図 5-3 に⽰すとおり, 動的登録は以下の4ステップから成る.

1. 発⾒: RP は IdP の周知な場所に⾏き, IdP のメタデータを発⾒する.
2. 確認: RP と IdP はお互いの正当性を確認する. これには鍵情報やメタデータ, ソフトウェアステートメント, その他の⽅法などが利⽤できる.
3. RP属性の登録: RP は⾃⾝の属性を IdP に送り, IdP はその属性をこの RP に関連付ける.
4. 連携プロトコル: IdP と RP は標準の連携プロトコルを使って通信する.

鍵情報の伝送を必要とするプロトコルでは, 登録プロセスにおいてセキュアな⽅法で連携された関係性の運⽤に必要な鍵情報を交換しなければならない (SHALL). これには共有シークレットも公開鍵も含まれる. この関係性を⽰すために利⽤される鍵が対称鍵である場合は, 連携参加者のペアに一意でなければならない (SHALL).

IdP はユーザー情報を提供する前に, 認可された主体（加入者など）による実行時の決定（セクション 4.2 参照）を要求しなければならない (SHALL). 動的登録を⾏う RP を受け⼊れる IdP は, そうした RP が利⽤できる属性やその他の情報のタイプを制限してもよい (MAY). 動的登録を利⽤できる RP は, 身元情報を受け⼊れる IdP を制限してもよい (MAY).

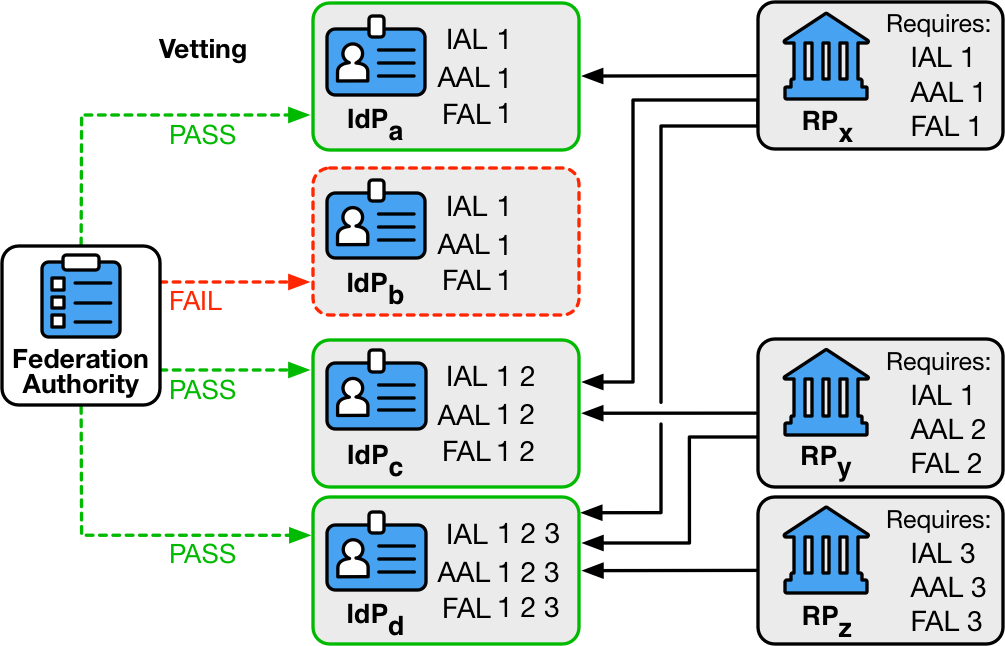
動的登録モデルの参加者は, お互いのことを事前に知らないことがよくある. 可能であれば, 連携参加者が動的に登録した RP の属性のいくつかを暗号論的に検証できるよう, ソフトウェアステートメントにより補強すべきである (SHOULD).ソフトウェアステートメントは RP ソフトウェアに関する属性を列挙したものであり, オーソリティ（IdP ⾃⾝, セクション 5.1.3 にある連携オーソリティ, その他の信頼できる主体）により暗号論的に署名されている. この暗号論的に検証可能なステートメントにより,自己表明属性のみに頼る必要がなくなり, 連携参加者間の通信を確⽴または向上させることができる. （あるプロトコルにおけるソフトウェアステートメントの実装に関する詳細は RFC 7591 セクション 2.3 を参照）

### **連携オーソリティ**

⼀部の連携参加者は, 連携の決定および主体間の関係性構築に関して, *連携オーソリティ*と呼ばれる権限機関に従う. このモデルでは, 連携オーソリティは連携に参加する各主体に対して⼀定レベルの審査を実施し, 所定のセキュリティと完全性基準を遵守しているかを検証するのが⼀般的である. 審査を⾏う場合, 審査レベルは連携のユースケースやモデルごとに一意となる. 図 5-4 の左はこの審査の説明である.

連携オーソリティは, IdP が特定の IAL, AAL, FAL で運営することを承認する. この情報は, 図 5-4 の右にあるように,証明書利用者によって利⽤され, どの身元情報プロバイダがこの RP の要件に合うかの判断材料となる.

連携オーソリティは, ⾃⾝が有効化する連携された関係性に関して, 期待され受け⼊れ可能な IAL, AAL, FAL に関するパラメーターを規定しなければならない (SHALL). 連携オーソリティは, 連携参加者を個別に審査し, 期待されるセキュリティ, 身元情報およびプライバシー基準に準拠しているかを判断しなければならない (SHALL).



#### 図 5-4 連携オーソリティ

（図の説明）

左

連携オーソリティ

審査 合格 不合格 合格 合格

右

要求: 要求: 要求:

IdP と RP の審査には, 最低限以下の項⽬を確認しなければならない (SHALL).

* IdP が⽣成したアサーションがセクション 6の要件に準拠しているか.
* IdP が求める属性データの保持, アグリゲーション, 第三者への開⽰などの要件に RP が準拠しているか.
* RP と IdP の両システムが, 連携プロトコルの承認済みプロファイルを使用しているか.

連携オーソリティは, IdP の設定データを公開したり RP 向けにソフトウェアステートメントを発⾏したりするなど, 参加者間の技術的接続と設定プロセスを⽀援してもよい (MAY).

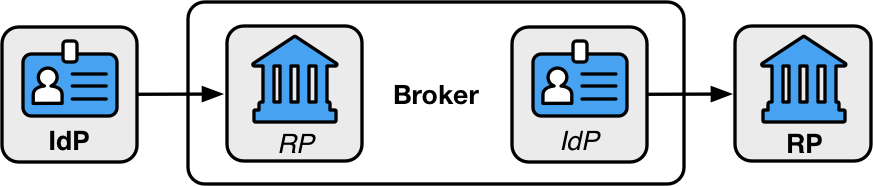
オーソリティに管理された連携は, ほとんどの場合シンプルなメンバーシップモデルを形成する. そのモデルでは, ある主体が連携に参加しているか否かのみを扱う. より洗練された連携においては, 複数のメンバーシップ階層が設けられてもよく(MAY), ある主体が他の主体に⽐べてより⼊念に審査されたかどうかを知ることができる. IdP はある加入者の情報を⼀定以上の階層の RP にのみ受け渡すようにしてもよいし (MAY), RP はある情報を⼀定以上の階層の IdP からのみ受け⼊れるようにしてもよい (MAY).

### **プロキシを利用した連携**

プロキシを利用した連携では, IdP と RP の通信は両者間のダイレクト通信を妨げる形で仲介される. これを実現する⽅法は複数あるが, 共通事項として以下のような項⽬が挙げられる.

* 第三者が連携プロキシ (つまり*ブローカー*) として動作する.
* 通信を振り分けるノードのネットワークが存在する.

プロキシを利⽤する場合, このプロキシは⼀⽅で IdP として機能し, もう⼀⽅では RP として機能する. したがって, IdP と RP に求められるすべての規範要件が, このプロキシにも課せられなければならない (SHALL).



#### 図 5-5 連携プロキシ

（図の説明）

ブローカー

プロキシを利用した連携モデルにはいくつかの利点がある. RP と IdP に共通インタフェースを提供して技術的統合を単純化できる. さらに, プロキシが RP と IdP を互いに効果的に目隠しすることで,互いに加入者リストを保護したい組織間でビジネス上の機密性も実現できる. また,プロキシは セクション 5.2 に述べるようにプライバシーリスクをいくつか低減することもできる.

目隠し技術とその利⽤と 限界については, セクション 9.5 を参照.

## **プライバシー要件**

連携には, それ以外ではトランザクションに関与しない第三者である IdP からの個⼈属性の転送が関係する. さらに, 連携では IdP に加入者の活動が丸見えになる可能性がある. したがって, 連携には特別なプライバシー要件がある.

RP と IdP の間の通信は,加入者がトランザクションを実⾏している IdP に明らかになりうる. 複数の RP と通信することで, IdP は加入者のトランザクションのプロファイルを作成することができる. これは連携なしではなしえない. このアグリゲーションにより,加入者のプライバシー上の利益に必ずしも⼀致しない追跡やプロファイル情報の利⽤が可能となりうる.

IdP は, 身元情報の検証, 認証, 属性アサーション（まとめて “身元情報サービス” と言う）と関連する不正防止, 法律や訴訟手続き, ユーザーからの情報転送依頼に従う目的を除き, ある RP における加入者の活動情報を任意の主体に開⽰したり処理したりする場合は, 追加処理から生じるプライバシーリスクに相当する予測可能性と管理可能性を維持する手段を導入しなければならない (SHALL). こうした手段には, 明確な通知の提供, 加入者の同意の取得, 属性の選択的使用または開示を含めてもよい (MAY). IdP が同意手段を利用する場合は, 追加処理の同意を身元情報サービスの条件にしてはならない (SHALL NOT). IdP は, セクション 6.3 に述べるペア匿名識別子やプライバシーを強化する暗号化プロトコルといった技術的手段を利⽤して,加入者の⾏動の追跡や解析を防止すべきである (SHOULD).

IdP は, 例えば改竄された加入者アカウントの通信といった加入者の活動情報を, セキュリティ⽬的で連携範囲内の他の RP に開⽰してもよい (MAY).

以下の要件は, 特に政府機関に適⽤される.

1. 機関はプライバシー上級担当者 (SAOP) と協議し, プライバシー法の要件が, IdP として機能する機関か RP として機能する機関, またはその両⽅（セクション 9.4 を参照）に適用されるか否かを判断するために分析を実施しなければならない (SHALL).
2. 機関は, 該当する場合は, 記録通知システム (SORN) の適用範囲を公表または識別しなければならない (SHALL).
3. 機関は SAOP と協議し, 電子政府法の要件が, IdP として機能する機関か RP として機能する機関, またはその両⽅に適用されるか否かを判断するために分析を実施しなければならない (SHALL).
4. 機関は, 該当する場合は, プライバシー影響評価 (PIA) の適用範囲を公表または識別しなければならない (SHALL).

## **連携環境における再認証とセッション要件**

連携環境では, RP は⾃⾝のセッションを IdP のセッションとは別に管理する. RP のセッションは RP が IdP からの連携プロトコルを処理するタイミングで開始される. 連携へのログイン時に,加入者が IdP にすでにセッションを持っていてもよく (MAY), そのセッションが RP に対する認証プロセス中で利⽤されてもよい (MAY). IdP は IdP での最新の認証イベントの時刻に関する情報を伝えなければならず (SHALL), RP は⾃⾝のアクセスポリシーの決定にこの情報を利⽤してもよい (MAY). 利⽤する連携プロトコルの性能に応じて, IdP は RP が IdP による加入者の再認証を連携リクエスト中で要求できるようにすべきである (SHOULD).

連携システムは分散を特徴としているため,加入者は IdP と RP のセッションを互いに独⽴して終了させることができる. RP は, 連携にログインができたからといって加入者が IdP においてアクティブなセッションを持っていると仮定してはならない (SHALL NOT). IdP は IdP における加入者セッションの終了がダウンストリーム RP における加入者の任意のセッションに伝わると仮定してはならない (SHALL NOT).

セッション管理要件に関する詳細は [SP 800-63B セクション 7 (sp800-63b.html#sec7)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#sec7) を参照.

# アサーション

*このセクションは規範である.*

認証⽬的で利⽤されるアサーションは, 認証済み加入者に関係するか関連付けられた属性値や属性参照のパッケージ化されたセットで, 連携 ID システム内で IdP から RP に渡される.アサーションに含まれる情報は, アサーションメタデータ,加入者に関する属性値や属性参照, RP が利⽤できるその他の情報 (制約や有効期限など) などさまざまである.アサーションの第⼀の機能は RP に対してユーザーを認証することであるが,アサーションで伝えられる情報は RP がさまざまなユースケースで利⽤できる. 例としては, Web サイトにおける認証やパーソナライゼーションなどが挙げられる. このガイドラインでは, 選択されたソリューションがここに含まれるすべての必須要件を満たす限り, RP のユースケースや識別情報を連携するためのプロトコルもデータペイロードのタイプも制限しない.

アサーションは単⼀の認証イベントのみを表現してもよく (MAY),加入者に関する属性値や属性参照を表現してもよい (MAY).

すべてのアサーションは, 以下にあげるアサーションメタデータを含まなければならない (SHALL).

1. Subject: このアサーションが指し⽰す主体 (つまり, 加入者) の識別⼦.
2. Issuer:アサーションを発⾏した IdP の識別⼦.
3. Audience:アサーションを利⽤することが想定される主体の識別⼦ (つまり, RP)
4. Issuance:アサーションが IdP に発⾏された⽇時を⽰すタイムスタンプ.
5. Expiration:アサーションの有効期限を⽰すタイムスタンプ. RP は有効期限が切れたアサーションを有効なアサーションとして受け⼊れてはならない (SHALL NOT). (つまり, アサーションの有効期限切れであり, RP におけるセッションの有効期限切れではない)
6. Identifier: このアサーション⾃⾝を識別するランダムで一意の値. 攻撃者による以前のアサーションの再利⽤を防ぐために利⽤される.
7. Signature:アサーション全体に対するデジタル署名またはメッセージ認証コード (MAC) で, IdP に関連付けられた鍵の識別⼦や公開鍵を含む.
8. Authentication Time: (利用可能であれば) IdP が最初の認証イベントを通じて加入者を認証した⽇時を⽰すタイムスタンプ.

アサーションはさらに以下の情報を含んでもよい (MAY).

1. Key binding: 公開鍵または加入者が保持する鍵の識別⼦であり, セクション 6.1.2 にあるようにこのアサーションと加入者が保持する鍵との結び付けを証明するために使われる.
2. 属性値と属性参照: 加入者に関する情報
3. 属性メタデータ: １つ以上の加入者属性に関する追加の情報. NIST Internal Report 8112 [NISTIR 8112] に述べられているものなど.

アサーションは, 認証イベントが表明されているときの AAL と, 身元情報の証明済み属性(またはその参照) が表明されているときの IAL を指定すべきである (SHOULD). 指定がなければ RP はこのアサーションにいかなる IAL, AAL も割り当ててはならない (SHALL NOT).

RP は主体の識別⼦をグローバルに一意ではないとして扱わなければならない (SHALL). アサーションの主体の識別⼦の値は, 普通はアサーション発行者が管理するネームスペースに属している. これにより RP は異なる IdP から提⽰された主体を混同することなく複数の IdP と対話することができる.

アサーションには追加の属性を含めてもよい (MAY). セクション 7 では, アサーションに属性を含めて提⽰する際のプライバシー要件を説明している. RP は,アサーションと⼀緒に発⾏された認証情報を利⽤して, 別のトランザクションで IdP から追加の身元情報属性を取得してもよい (MAY). こうした追加属性を取得する能⼒は,アサーションを処理することに等しいと扱ってはならない (SHALL NOT).

詳細は利⽤する連携プロトコルによって異なるが,アサーションは RP における単⼀のログインイベントのみを表すように[利⽤されるべきである (SHOULD). RP がアサーションを利⽤すると, RP によるセッション管理 (SP 800-63B セクション 7 (sp800-63b.html#sec7)) 参照) を開始される. アサーションはそこに含まれる有効期限を超えて利⽤されてはならない (SHALL NOT). しかし](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.html#sec7), RP におけるセッション有効期限は,アサーション⾃体の有効期限よりも先に終了してもよい (MAY). 詳細は セクション 5.3 を参照.

アサーションのライフタイムは発⾏時から有効期限までの間である. このライフタイムは, RP がアサーションを処理して加入者のためにローカルのアプリケーションセッションを開始できるまで⼗分な⻑さが必要だが, 必要以上に⻑くするべきではない. ⻑期間有効なアサーションは詐取やリプレイのリスクが⾼く, ライフタイムの短いアサーションはそうしたリスクを軽減する.アサーションのライフタイムは, RP 上のセッションを制限するために利⽤されてはならない (SHALL NOT). 詳細は セクション 5.3 を参照.

## **アサーションの結び付け**

アサーションの結び付けは, 認証要求者によるアサーションまたはアサーション参照の提⽰は加入者の結び付けに⼗分かどうか, または, アサーションが加入者に結び付けられている追加の証明を RP が要求するのか, という点に基づいて分類することができる.

### **ベアラアサーション**

ベアラアサーションは, いかなる主体でもベアラ (持参人) の身元情報の証明として提⽰することができる. 加入者を⽰す正当なアサーションやアサーション参照を攻撃者が取得したり偽造したりして RP に提⽰することができれば, 攻撃者は RP において加入者になりすますことができる.

加入者になりすますにはベアラアサーションや 参照を所有しているだけでは必ずしも⼗分とは言えない. 例えばアサーションがバックチャネル連携モデル (セクション 7.1 参照) において提⽰される場合,トランザクション中でさらなる管理 (RP の識別やアサーションインジェクション対策など) を行い, RP を不正なアクティビティから保護してもよい (MAY).

### **ホルダオブキーアサーション**

ホルダオブキーアサーションには, 加入者が所持し本人であることを表現する鍵への参照が含まれる. ホルダオブキーアサーション中の鍵の参照は加入者を⽰すものであり, このシステム中のブラウザ, IdP, RP などのいかなる他の主体も⽰すものではない. 鍵への参照はアサーションの発行者によって表明（および署名）されていることに注意が必要である.

RP がホルダオブキーアサーションを受け取ると,加入者はアサーションから参照された鍵を所有していることを直接 RP に証明する.加入者は IdP との間で鍵ベースの認証⽅法を利⽤することもできるが, IdP 上の 最初の認証と RP 上の連携認証は独⽴したものとみなされ, 同じ鍵や関連したセッションが利⽤されるとは想定されない.

加入者が RP に対して鍵所有証明を⾏うとき, 認証要求者はアサーションの正当な主体であることの確実性をある程度証明することになる. 攻撃者は加入者に発⾏されたホルダオブキーアサーションを盗んで利用しようとしても, そこから参照された鍵そのものも盗む必要があるため, 攻撃はいっそう困難になる.

ホルダオブキーアサーションには以下のすべての要件が適⽤される.

1. 加入者は,アサーション⾃体の提⽰に加えて, RP に対して鍵所有を証明しなければならない (SHALL).
2. 加入者が保持する鍵への参照を含むが鍵所有が証明されていない場合, RP はこのアサーションをベアラアサーションとみなさなければならない (SHALL).
3. 所定の鍵への参照は,アサーション内のその他のすべての情報と同レベルで信頼されなければならない (SHALL).
4. アサーションには, ホルダオブキーの提⽰で利⽤するプライベート鍵や対称鍵を暗号化せずに含めてはならない(SHALL NOT).
5. この鍵は加入者が IdP に認証する際に利⽤する鍵と異なってもよい (MAY).
6. この鍵は対称鍵でもよいし, プライベート鍵に対応する公開鍵でもよい (MAY).
7. RP は認証要求者がこの鍵を所有していることを IdP と協力して検証してもよい (MAY). 例えば, 暗号論的なチャレンジに対して認証要求者が計算した署名や MAC を IdP が検証する.

## **アサーションの保護**

結び付けの方法（セクション 6.1 参照）や連携モデル（セクション 5.1 参照）とは別に, 攻撃者が有効なアサーションを偽造したり, 盗んだアサーションをまったく異なる RP に対して再利⽤したりする攻撃を防ぐために, アサーションに⼀連の保護策を施さなければならない (SHALL). 必要な保護策は考慮されるユースケースの詳細で異なるが, ここでは推奨される保護策を列挙する.

### **アサーション識別子**

アサーションは, 対象となる RP が⼀意に識別できるように一意でなければならない (SHALL).アサーションは, ノンス, 発⾏⽇時,アサーション識別子やそれらの組み合わせによって, またはその他のテクニックによってこの一意性を実現してもよい (MAY).

### **署名付きアサーション**

アサーションは IdP によって暗号論的に署名されなければならない (SHALL). RP は, 発行者の鍵に基づいて各アサーションのデジタル署名や MAC を確認しなければならない (SHALL). 署名は,アサーション識別子, 発行者, オーディエンス, 主体, 有効期限を含め,アサーション全体をカバーしなければならない (SHALL).

アサーションの署名は, 非対称鍵を使用するデジタル署名か, RP と発行者の間で共有される対称鍵を⽤いた MAC でなければならない (SHALL). この⽬的のために IdP に利⽤される共有の対称鍵は,アサーションを送信する RP ごとに独⽴していなければならず (SHALL), 通常は RP 登録時に確定される.デジタル署名の検証に⽤いる公開鍵については, IdP がホストする HTTPS URLを通すなどして, RP が実行時にセキュアな⽅法で取得してもよい (MAY). 署名には認可された暗号法を使用しなければならない(SHALL).

### **暗号化アサーション**

アサーションを暗号化する場合, IdP は RP の公開鍵か共有の対称鍵を使ってアサーションのコンテンツを暗号化しなければならない(SHALL). この⽬的のために IdP に利⽤される共有の対称鍵は,アサーションを送信する RP ごとに独⽴していなければならず (SHALL), 通常はRP 登録時に確定される. 暗号化に⽤いる公開鍵については, RP がホストする HTTPS URL を通すなどして, IdP が実行時にセキュアな⽅法で取得してもよい (MAY).

すべてのアサーションの暗号化には, 認可された暗号法を使用しなければならない (SHALL).

アサーションがブラウザなどの第三者を介してやりとりされる場合は,アサーションの暗号化を行わなければならない (SHALL). 例えば SAMLアサーションは XML-Encryption で暗号化でき, OpenID Connect ID Token は JSON Web Encryption (JWE) で暗号化できる. IdP から直接 RP に渡されるアサーションについては, 実際のアサーションを暗号化してもよい (MAY). 暗号化しない場合は, 認証済み保護チャネルで送信しなければならない (SHALL).

注意: アサーションの暗号化は, FAL2 と FAL3 で必須である.

### **オーディエンス制限**

アサーションはオーディエンス制限テクニックを使用し, RP ⾃⾝がアサーションの対象であるかどうかを判断できるようにしなければならない (SHALL). すべての RP は,アサーションのオーディエンスに⾃⾝の識別⼦が含まれているかチェックし, ある RP に対して⽣成されたアサーションが他の RP にインジェクトやリプレイができないようにしなければならない (SHALL).

### **ペア匿名識別子**

状況によっては, IdP 上の加入者アカウントに対する共通の識別⼦を通して, 複数の RP 間でこの加入者が簡単にリンクされないようにすることが望ましい.

### **一般要件**

IdP が RP に対して⽣成するアサーションにペア匿名識別子を利⽤する場合, IdP は セクション 6.3.2 に述べるように各 RP に異なる識別⼦を⽣成しなければならない (SHALL).

複数の RP に対して属性と共にペア匿名識別子を利⽤する場合, RP 同士で身元情報属性を使って相互に関係付けを行い, 加入者を再識別できる場合がある. 例えば2つの独⽴した RP が異なるペア匿名識別子によって識別される同⼀の加入者を観察しているとすると, これらの RP はそれぞれが受け取るアサーション中にペア匿名識別子と共に含まれる名前, メールアドレス, 物理アドレス, その他の識別に⽤いられる属性を⽐較することにより, この加入者が同⼀⼈物であることを知るかもしれない. そうした相互関係はプライバシーポリシーによって禁じられるべきであり (SHOULD), ペア匿名識別子は属性の相互関係の管理作業を増やすことでこうしたポリシーの有効性を⾼めることができる.

プロキシを利用した連携モデルでは, IdP はプロキシによって加入者がアクセスしようとしている RP を知ることができない可能性があるため, 最初の IdP が最後の RP に対してペア匿名識別子を⽣成できないこともある. そのような状況では, ペア匿名識別子は通常は IdP と連携プロキシの間で確定される. プロキシは IdP として機能し, ダウンストリームの RP に対してペア匿名識別子を提供することができる. プロトコルによっては, 身元情報プロトコルを機能させるため, 連携プロキシはペア匿名識別子をアップストリーム IdP から送られてくる関連する識別⼦にマップする必要がある. そのようなケースでは, プロキシは同⼀の加入者を⽰す RP ごとのペア匿名識別子を判別し, 追跡することができる. プロキシは,ペア匿名識別子とその他の識別⼦間のマッピングを第三者に開⽰したり, そのマッピング情報を連携認証とそれに関連する不正防⽌, 法律や訴訟⼿続きの遵守, ユーザーからのこの情報の送信を求める特定の要求への応答以外の⽬的で利⽤したりしてはならない (SHALL NOT).

### **ペア匿名識別子の生成**

ペア匿名識別子には,加入者に関するいかなる識別情報も含めないようにしなければならない (SHALL). また加入者を識別する情報へのアクセスを持つ主体によって推測されないようにしなければならない (SHALL).ペア匿名識別子は, ランダムに⽣成して IdP が加入者に割り当ててもよく (MAY),加入者に関するその他の情報から不可逆で推測不可能な⽅法 (例えばシークレット鍵を利⽤した鍵付きハッシュ関数) で導出してもよい (MAY). 通常この識別⼦は, 対となるエンドポイント間 (例えば, IdP-RP) のみが知っており, このエンドポイント間のみで利⽤されなければならない (SHALL). ただし IdP は以下の場合, RP の要求に従って複数の RP に同⼀の識別⼦を⽣成してもよい (MAY).

* それらの RP が, セキュリティドメインや法的所有権を共有するなど, 運用上相関関係にある正当な理由を説明できる関係性にある.
* 識別⼦を共有するすべての RP が, そのような⽅法で関連付けられることに同意している.

RP はプライバシーリスク評価を実施し, 共通の識別⼦を要求する場合のプライバシーリスクを考慮しなければならない (SHALL). プライバシー上の考慮点についての詳細は セクション 9.2 を参照.

IdP は意図した RP のみが相関関係にあることを保証しなければならない (SHALL). そうでないと, 悪意ある RP が不正に⼀連の相関関係にあるRP になりすまし, これらの RP に対して発⾏された匿名識別子を知る可能性がある.

# アサーションの提示

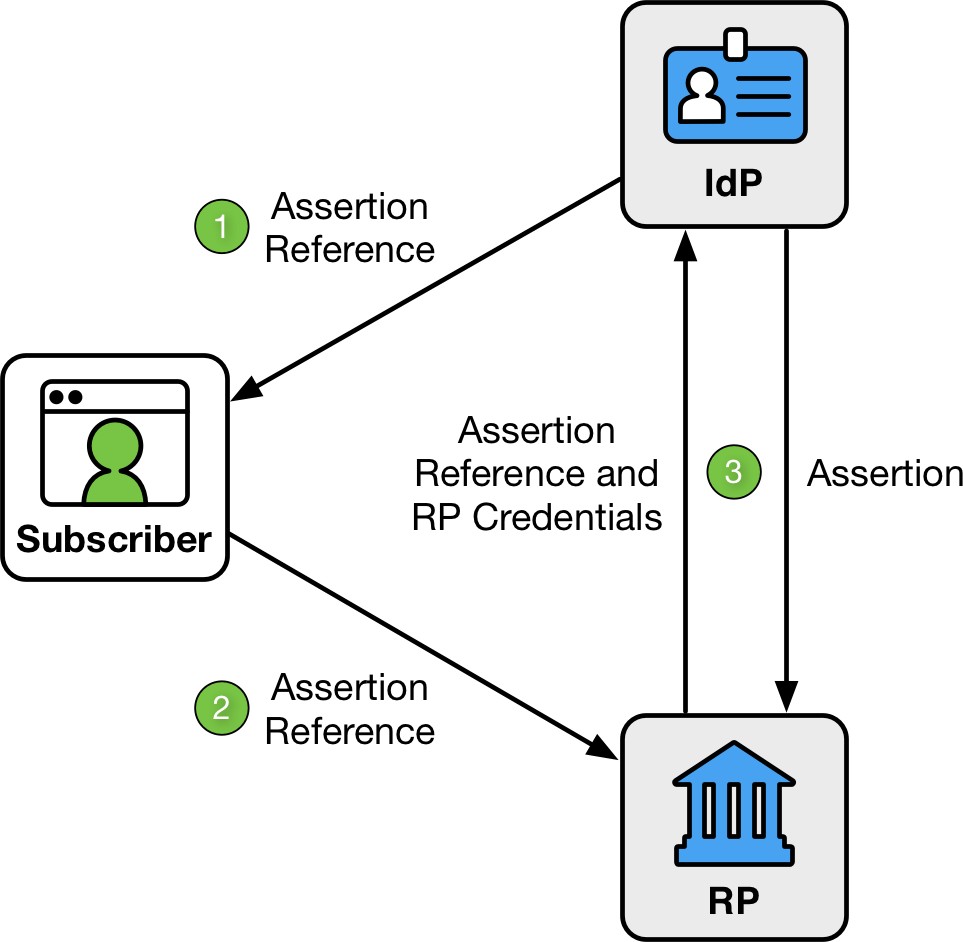
*このセクションは規範である.*

アサーション は IdP から RP に対して*バックチャネル*または*フロントチャネル*で提⽰されてもよい (MAY). それぞれのモデルは一長一短であるが, どちらにおいてもアサーションを正しく検証する必要がある. セクション 5.1.4 にあるように, ある条件下では連携を簡単にするため IdP と RP の間をプロキシを利用した状態でアサーションをやりとりすることもある.

IdP は RP が明⽰的に要求した属性のみを送信しなければならない (SHALL). また RP はプライバシーリスク評価を⾏い, どの属性を要求するかを決定しなければならない (SHALL).

## **バックチャネルでの提示**

バックチャネルモデルでは,加入者はアサーション参照が与えられ, ⼀般的にはフロントチャネルを通してそれを RP に提⽰する.アサーション参照はそれ⾃⾝には加入者に関する情報はなく, 攻撃者による偽造や改竄に耐性がなければならない (SHALL). RP はアサーションを取得するためアサーション参照を IdP に提⽰する. その際 RP は通常は自分自身を IdP に対して認証する.



#### 図 7-1 バックチャネルでの提示

（図の説明）

加盟者

１アサーション参照

２アサーション参照

アサーション参照と RP 認証情報

３アサーション

図 7-1 にあるように, バックチャネルでの提示モデルは以下の3ステップから成る.

1. IdP がアサーション参照をフロントチャネル経由で加入者に送信する.
2. 加入者はアサーション参照をフロントチャネル経由で RP に送信する.
3. RP はアサーション参照と RP ⾃⾝の認証情報をバックチャネル経由で IdP に提⽰する. IdP は認証情報を確認しアサーションを返す.

アサーション参照は以下の必要がある.

1. 単一の RP だけに使用が制限されなければならない (SHALL)
2. 使い捨てでなければならない (SHALL)
3. 有効期限が数秒〜数分と短いべきである (SHOULD)
4. RP の認証といっしょに提⽰されるべきである (SHOULD)

このモデルでは, RP は第三者 (加入者⾃⾝を含む) による傍受・改竄の機会を最小限に抑えてアサーションを IdP に直接要求する.

この⽅法では, 最初の認証トランザクション終了後も, ユーザーを IdP に送り返すことなくバックチャネル通信を繰り返し⾏えるため, RP は IdP にアサーション⾃体には含まれない追加の加入者属性を問い合わせることもできる. この問い合わせにはセクション 6 にあるようにアサーションといっしょに発⾏される認証情報を⽤いる.

ネットワーク経由のトランザクションがより多く必要になるものの, やりとりされる情報はそれを必要としている主体以外に渡されることはない. RP が IdP から直接アサーションを受け取るため, 攻撃箇所は限定される. さらにアサーションを RP に直接インジェクションすることはさらに困難になる.

RP は, クロスサイトスクリプティング対策やその他の方法を活用し, 偽造されたか盗まれたアサーション参照のインジェクションから⾃⾝を保護しなければならない (SHALL).

RP はアサーションに含まれる要素について, 以下のような点を含めて確認しなければならない(SHALL).

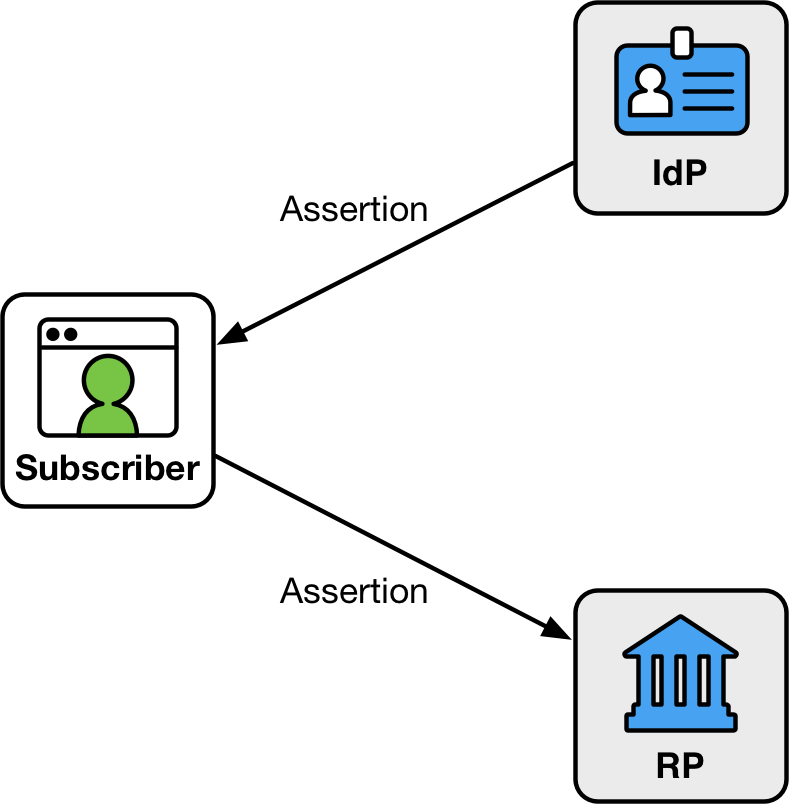
* 発行者の検証:アサーションが RP の想定する IdP から発⾏されている.
* 署名の検証:アサーションの署名が, このアサーションを送信した IdP に関連する鍵と合致する.
* 時間的有効性: 有効期限と発⾏⽇時が現在の⽇時に対して許容範囲内にある.
* オーディエンス制限: 自身がアサーションの受信者として意図されている.

IdP から加入者へ,加入者から RP へとアサーション参照を送信するとき, 認証済み保護チャネルを利⽤しなければならない (SHALL). RP から IdP にアサーション参照を送信するとき, IdP から RP にアサーションを送信するときも同様に, 認証済み保護チャネルを利⽤しなければならない (SHALL).

アサーション参照を提⽰するとき, IdP はアサーション参照を提⽰している主体が認証を要求した主体と同⼀であることを検証しなければならない (SHALL). そのため, IdP は RP に対してアサーション参照提⽰時に⾃⾝を認証するよう求めるか, その他の同様の⽅法 (RP 識別⼿段となるプロトコルの⼀例としては RFC 7636 を参照) が利用できる.

セクション 5.1.4 に述べる 連携プロキシで注意することは, IdP はプロキシに対してアサーション参照とアサーションのオーディエンス制限を⾏い, プロキシはダウンストリームの RP に対して新たに⽣成したアサーション参照やアサーションのオーディエンス制限を⾏うことである.

## **フロントチャネルでの提示**

フロントチャネルモデルでは, IdP は認証の後にアサーションを⽣成して加入者に渡す.加入者は渡されたアサーションを利⽤して, 普通はブラウザのメカニズムを通して RP に⾃⾝を認証する.

#### 図 7-2 フロントチャネルでの提示

（図の説明）

加入者 アサーション アサーション

フロントチャネルモデルでは,アサーションは加入者が閲覧できる. これはアサーションに含まれるシステム情報などの漏洩につながる可能性もある. さらにこのモデルでは, RP が IdP にアサーション提⽰後に追加の属性を問い合わせることがいっそう困難になる.

アサーションは加入者の管理下に置かれることから, フロントチャネルでの提示方法では, 加入者はブラウザをリプレイしてアサーションを複数の RP に送りつけるなどの⼿段によって,アサーションを本来意図されない主体に送りつけることもできる.アサーションが オーディエンス制限により意図しない RP に拒否されたとしても, 意図しない RP へのアサーションの提⽰は加入者に関する情報や加入者のオンライン活動の漏洩につながる可能性がある. 意図して複数の RP に提⽰できるよう設計されたアサーションを⽣成することも可能だが, そのような⼿法はこのアサーションに対するオーディエンス制限を弱め, RP 間における加入者のプライバシーとセキュリティの侵害につながる. したがってそのような複数の RP に対する利⽤は望ましくないが, 代わりに RP はそれぞれ個別のアサーションを取得することが推奨される.

RP は, クロスサイトスクリプティング対策やその他のテクニックを利⽤し, 偽造されたか盗まれたアサーションのインジェクションから⾃⾝を保護しなければならない (SHALL).

RP はアサーションに含まれる要素について, 以下も含めて確認しなければならない(SHALL).

* *発行者の検証*: アサーションが RP の期待する IdP から発⾏されている.
* *署名の検証*: アサーションの署名が, このアサーションを⽣成した IdP に関連する鍵と合致する.
* *時間的有効性*: 有効期限と発⾏⽇時が現在⽇時に対して許容範囲内にある.
* *オーディエンス制限*: 自身がこのアサーションの受信者として意図されている.

IdP から加入者へ,加入者から RP へとアサーションを送信するとき, 認証済み保護チャネルを利⽤しなければならない(SHALL).

セクション 5.1.4 に述べる連携プロキシでは, IdP はプロキシに対してアサーションのオーディエンス制限を⾏い, プロキシはダウンストリームの RP に対して新たに⽣成したアサーションの オーディエンス制限を⾏うことに注意が必要である.

## **情報の保護**

IdP と RP の間の通信は,認証済み保護チャネルを利⽤して保護しなければならない (SHALL).加入者と IdP, そして RP 同士の通信（通常はブラウザ経由）も認証済み保護チャネルを介さなければならない(SHALL).

IdP は, RP がセキュリティポリシーを実施する際に有⽤な情報にアクセスできる可能性もある. こういった情報としては, デバイス ID, 位置情報, システム診断情報, 設定管理などがある. IdP がこうした情報を取得できる場合, セクション 9.2 にあるようにプライバシーに関する加入者の意向の範囲内で, こうした情報をいっしょに RP に渡すことがよいかもしれない.

ユーザーに関する追加の属性は,アサーションとは別に, RP から IdP への認可されたリクエストを通してやり取りされてもよい (MAY). こうした属性へのアクセス権限をアサーションといっしょに発⾏してもよい (MAY). ユーザーに関する情報をこのように分離することで, ユーザーのプライバシー保護に役⽴ち,認証アサーション⾃体に必要不可欠な情報に加えて識別のための属性を限定的に開示することも可能になる.

RP は, セクション 9.3 にあるように, 可能であれば完全な属性値ではなく属性参照を要求しなければならない (SHALL). IdP は属性参照をサポートしなければならない (SHALL).

# セキュリティ

*このセクションは参考情報である..*

連携認証プロセスには, IdP として振る舞う CSP を含めた複数の構成要素間の協調が関係するため, 攻撃者が連携 IDトランザクションを改竄する危険が増加する. このセクションでは連携に対する攻撃とその対策についてまとめる.

## **連携に対する脅威**

連携されていない認証では, 攻撃者の意図は RP が提供するリソースやサービスへのアクセス（またはより⾼度なアクセス）を取得することにある. また, 攻撃者は加入者になりすまそうとすることもある. 潜在的な攻撃者には, 悪意があるか侵害された IdP, RP, ユーザーエージェント（例えば, ブラウザ）, ⼀般的に連携トランザクションの外側にいる主体がなる. 攻撃者は攻撃を成功させるため,アサーションやアサーション参照を傍受したり改竄したりする. さらに, 複数の主体が直接アサーションデータの完全性や機密性を侵害し, 連携プロトコルを無効にしようとするかもしれない. こうしたタイプの脅威を考慮すると, ⾃⾝の権限を超えた権限を取得しようとするあらゆる主体はたとえ認可されていても攻撃者とみなされる.

場合によっては, RP が認識できるように加入者にシークレットを発⾏することもある. この情報を知っているかどうかで,加入者になりすまそうとする攻撃者と本物の加入者を⾒分けられる.ホルダオブキーアサーションのケースでは, このシークレットは連携プロトコルの開始前に IdP との間で確定できよう.

#### Table 8-1 連携に対する脅威

|  |  |  |
| --- | --- | --- |
| **連携に対する脅威/攻撃** | **説明** | **例** |
| アサーションの偽造 /  改竄 | 攻撃者が偽のアサーションを⽣成する. | 侵害を受けた IdP が正しく認証されていない認証要求者の身元情報を表明する. |
| 攻撃者が既存のアサーションを改竄する. | 侵害を受けたプロキシが認証アサーション の AAL を変更する. |
| アサーションの漏洩 | アサーションが第三者に閲覧可能になる. | ネットワークモニタリングにより加入者の記録上の住所が部外者に公開される. |
| IdP による  アサーションの否認 | IdP が後になってトランザクションに署名していないと主張する. | ユーザーが RP で不正なクレジットカード取引に関与し, IdP は彼らをログインさせていないと主張する. |
| 加入者による  アサーションの否認 | 加入者がトランザクションを実⾏していないと主張する. | ユーザー同意 (例えば, 契約) が守られない. |
| アサーションのリダイレクト | アサーションが意図しない状況で利⽤される. | 侵害を受けたユーザーエージェントがアサーションを攻撃者に渡し, 攻撃者がどこか別の場所でそれを利⽤する. |
| アサーションの再利⽤ | アサーションが同じ RP に複数回利⽤される. | 傍受されたアサーションが攻撃者⾃⾝のセッションを認証するために利⽤される. |
| アサーションの置き換え | 攻撃者が別の加入者のためのアサーションを利⽤する. | IdP と RP の間でのセッションハイジャック攻撃 |

* 1. **連携に対する脅威の軽減策**

上記の脅威を緩和するのに役⽴つ対策を表 8-2 に⽰す.

#### 表 8-2連携に対する脅威の軽減策

|  |  |  |
| --- | --- | --- |
| **連携に対する脅威/攻撃** | **脅威の軽減策** | **例** |
| アサーションの偽造/改竄 | IdP がアサーションに暗号論的に署名を施し, RP がそれを検証する. | 4.1, 6 |
| IdP を認証する認証済み保護チャネル経由でアサーションを送信する. | 7.1, 7.2 |
| 推測不能でランダムな識別⼦をアサーションに含める. | 6.2.1 |
| アサーションの漏洩 | RP を認証する認証済み保護チャネル経由でアサーションを送信する. | 7.1, 7.2 |
| アサーションを特定の RP に対して暗号化する. (双⽅向の認証済み保護チャネルで実現可能) | 6.2.3 |
| IdP によるアサーションの否認 | 否認防⽌をサポートする鍵を使用して IdP でアサーションに暗号論的に署名を施し, RP がそれを検証する. | 6.2.2 |
| 加入者によるアサーション の否認 | ホルダオブキーアサーションを発⾏する. 提⽰された鍵所有証明が加入者の関与を⽴証する. | 6.1.2 |
| アサーションのリダイレクト | 署名対象のコンテンツ内に,アサーション発⾏先の RP (“audience”) の 身元情報を含める. RP は⾃⾝が意図された受信者であることを検証する. | 6, 7.1, 7.2 |
| アサーションの再利⽤ | アサーションの有効期限を短くし, 署名対象のコンテンツ内に発⾏⽇時を含める. RP はその有効性を検証する. | 6, 7.1, 7.2 |

1. **プライバシーの考慮事項**

*このセクションは参考情報である..*

## **トラッキングとプロファイリングの軽減**

連携は RP と加入者に多くのメリットをもたらすが,連携参加者を信頼するよう加入者に要求する.セクション 5, 5.1.4, および 6.3 は,加入者に対するトラッキングやプロファイリングの機会増⼤から生じるプライバシーリスクを最小限に抑制するための多くの技術的要件をカバーしている.

例えば複数の RP に対して認証するために同じ IdP を利⽤している加入者がいるとすると, 連携しなかった場合には発⽣しなかった加入者トランザクションのプロファイルを IdP は構築できる. このようなデータは,加入者が予期しないか希望しない⽤途に利用されやすく,加入者が連携サービスを採用することを妨げる可能性もある.

セクション 5.2 は, 身元情報の検証, 認証, 認可, 属性アサーション, これらに関連する不正の軽減以外の目的で属性を処理することから生じるプライバシーリスクと同一基準の予測可能性 (PII と情報システムによるその処理について, 個人と所有者と処理担当者が確実に予測できること) と管理可能性 (変更, 削除, 選択的公開を含め, PII をきめ細かく管理できること) の目標を維持するための措置を講じること, または, 法律や法的手続きを遵守するための措置を講じることを CSP に求めている[NISTIR8062].

CSP には, 身元情報に関係しないサービスを加入者に提供することを含め, 属性処理に対してさまざまな業務上の目的がある. しかし, 身元情報サービス以外の目的で属性を処理することは, 個人がその追加処理を予測していないか気がつかないときにプライバシーリスクを生じさせる. CSP は, 追加処理から生じるプライバシーリスクと同一基準の適切な措置を決めることができる. 例えば, 適用可能な法律, 規制またはポリシーがない場合, 加入者が依頼した身元情報に関係しないサービスを提供するために属性を処理するとき, 通知によって加入者がその処理について確実に推定できることを助ける場合もあろうが (予測可能性), 明確な同意を得る必要はない場合もある. 属性のその他の処理は, 明示的な同意の取得や, 特定の属性の使用や公開を加入者がさらに細かく管理できること (管理可能性) を求める別のプライバシーリスクをもたらす場合もある. 加入者の同意には意味があることが必要である. したがって, CSP が同意を利用するとき, 追加利用を加入者が受け入れることを身元情報サービスを提供する条件にすることはできない.

提案する処理が, 許可された処理や適切なプライバシーリスク軽減措置の範囲外かどうかについて疑問がある場合は, SAOP に意見を求めなければならない.

またセクション 5.2 は, 非関連性 (個人やデバイスを関連付けせずに PII やイベントをシステムの運用要件を超えて処理できること) を提供して加入者のトラッキングとプロファイリングを防止する技術的対策を推奨している[NISTIR8062]. セクション 5.1.4 で述べたプロキシ連携やセクション 6.3 で述べたペア匿名識別子のような技術的対策は, 運⽤要件を超えて加入者をトラッキングしたりプロファイリングしたりすることを一層困難にし,ポリシーの有効性を向上させる.

## **通知と同意**

連携において加入者の信頼を確⽴するには,加入者が⾃⾝の情報がどのように処理されるかについて信頼できる仮定を⽴てられる必要がある. 例えば, どの情報が送信されるのか, そのトランザクションではどの属性が必須でありどれがオプションであるかを理解でき, オプションの属性を RP に送信するか否かの決定権があることが加入者にとって有益であろう. したがって, セクション 7 では,加入者に関する属性が RP に送信される前に加入者に同意を得ることを求めている. セクション 6.3.2 にように, ⼀連の RP が同じペア匿名識別子を共有すべきかどうかを決定する際には, IdP は加入者がそのような RP のグルーピングを理解できることへの配慮と, そのような理解を助ける通知を⾏う役割への配慮が必要になる. 効果的な通知には, ユーザーエクスペリエンスのデザイン標準および研究と, 情報処理により発⽣する可能性のあるプライバシーリスクの評価を考慮する.加入者が情報の処理について抱く信頼性や, 連携に関与するその他の主体の役割など考慮すべき要素は数多い. しかし, 法律を尊重した複雑なプライバシーポリシーや, 相当数の加入者が読んで理解できないような利⽤規約へのリンクは, 決して効果的な通知ではない.

セクション 7 はどの主体が通知を⾏うかは指定していない. 場合によっては 連携に関わる主体が加入者に通知して同意を得るための直接的な接続関係にないこともある. 通知を⾏うよう選択できる主体は複数存在するが,加入者が通知に注意を払い情報に基づいた選択ができることを中⼼にした要因に基づいて決定されている限り, 契約やトラストフレームワークのポリシーによりどの主体が通知して同意を得るのかを事前に決定してもよい.

IdP が セクション 4.2 に述べたように RP のホワイトリストを利⽤している場合, このリストの RP はいずれも認証トランザクションで加入者に提⽰されない. IdP は実行時において加入者に通知を⾏わないため, ホワイトリストにある RP を加入者が利用できるようにし, どの RP がどの加入者属性にアクセスできるか確認できるようにする. IdP は加入者が関与する認証トランザクション外では加入者の認証情報や属性をホワイトリスト上の RP と共有できないため（セクション 5.2 参照）, RP がリスト上に存在することがそのまま加入者の情報が共有されることを意味するわけではない. しかし加入者が IdP を使ってホワイトリスト上の任意の RP にログインすれば, 示された属性は認証トランザクションの一部として共有される.

加入者の実行時の決定が将来のトランザクションを促進するために IdP に保存されている場合は, IdP は加入者に実行時の決定ですでに許可された RP を閲覧したり許可を無効化したりできるようにする必要がある. このリストにはどの属性が許可されているかという情報を含む.

## **データの最少化**

連携は RP に示されるデータを最少化できるため, 結果として加入者のプライバシーは強化される. IdP は⾃⾝のユースケースのために RP の要求を超えて追加の属性を収集するかもしれないが, RP が明⽰的に要求した属性のみが IdP によって送信される. 場合によっては, RP は完全な属性値を要求しない. 例えば, RP は加入者が13歳以上かどうかを知る必要があるが, 完全な⽣年⽉⽇を知る必要はないこともある. 潜在的に注意が必要な PII の収集を最少化するため, RP は属性参照 (例えば,加入者が13歳か否かという, Y/N や Pass/Fail で答えられる質問) を要求することができる. こうすることで RP による潜在的に要注意かつ不要な PII の収集を最少化できる. さらに, セクション 7.3 は可能であれば完全な属性値ではなく属性参照を要求するよう RP に求めている. この RP 要件を満たすため, IdP には属性参照をサポートすることが求められる.

## **機関特定のプライバシー準拠**

セクション 5.2 は, 機関が SAOP に相談してプライバシー準拠要件を決定する要件を定めている. 機関の SAOP をデジタル認証システムの開発初期段階から参加させることは, 1974 年プライバシー法や PIA を実施するための 2002年電子政府法の要件に連携が適用されるかどうかなど, プライバシーリスクの評価/軽減と準拠義務の助言の上で非常に重要である. 例えば, 機関が連携で IdP としてサービスを提供している場合,認証情報は IdP と連携する RP に代わって IdP に管理されることになるため, プライバシー法の要件が適用され, プライバシー法において新規または既存の記録システムによる対応が求められる可能性がある. しかしながら, 機関が第三者の IdP を利⽤する RP の場合, RP から渡されたどのデータが RP として機関に管理されるかによっては (その場合, 機関はそのようなデータをカバーする, より広範でプログラム的な SORN を備える場合がある), デジタル認証はプライバシー法の要件の対象にならない可能性がある.

同様に SAOP は PIA が必要かどうかの決定において機関を支援できる. これらの考慮点は, 連携認証情報の利⽤のためだけにプライバシー法における SORN や PIA の開発が要件になると読むべきではない. 多くの場合,デジタル認証プロセス全体を網羅する PIA と SORN を設計したり, 機関がオンラインアクセスを確⽴しているプログラムやメリットについて議論するさらに広範で計画的な PIA の⼀部としてデジタル認証プロセスを含めたりすることが, もっとも理にかなっていよう.

デジタル認証には多くの構成要素があることから, SAOP に各要素を認識し理解させることが重要である. 例えば, Data Use Agreements (データ使用合意書) や Computer Matching Agreements (コンピュータ致合意書) などの連携した IdP や RP サービスを提供したり利⽤したりする機関にその他のプライバシー要件が適用できる場合がある. SAOP は機関にどの追加要件を適⽤するのか決定する際に⽀援を⾏なうことができる. さらにデジタル認証の個々の要素を完全に理解することで, SAOP は準拠プロセスかその他の⼿段を通してプライバシーリスクを⼊念に評価し, 緩和することができる.

## **プロキシ連携での結び付け**

一般的にプロキシは統合環境を単純化することを主⽬的とし,構造によっては追加の加入者のプライバシー保護を提供しないものもあるが, 結び付け技術を⽤いて多様なレベルのプライバシーを加入者に提供するものもある. プライバシーポリシーにおいて,加入者属性と認証トランザクションデータ（例えば, 末端の IdP および RP の識別⼦）を IdP,RP, 連携プロキシが適切に利⽤することを規定してもよい. 結び付けなどの技術的⼿段は, データ取得をさらに困難にすることにより, そうしたポリシーの有効性を⾼めることができる. 結び付けレベルが上がるほど, 技術上と運⽤上の実装の複雑性は増す. プロキシはトランザクションをいずれかの側の適切な主体にマッピングし,トランザクション内のすべての関係者の鍵を管理する必要がある.

結び付け技術を使っても, 結び付けられた主体は, 提供された属性データやメタデータなどから, タイムスタンプや属性バンドルのサイズ,属性への署名者情報などを解析するなどして, 保護された加入者情報を推測することができる. IdP は追加のプライバシー強化アプローチを検討し, 連携に参加している主体の識別情報の開⽰リスクを減らすことができよう.

以下の表は プロキシ連携で利⽤される結び付けの実装の範囲を⽰したものである. なお, この表は説明を⽬的としたものであり, 網羅的でも技術に特化したものでもない.

#### 表 9-1 連携プロキシ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **プロキシのタイプ** | **RP は IdP を知っている** | **IdP は RP を知っている** | **プロキシは RP と IdP 間の加入を追跡できる** | **プロキシは加入者の属性を閲覧できる** |
| 属性ありでバインドなしのプロキシ | はい | はい | はい | はい |
| バインドなしのプロキシ | はい | はい | はい | N/A |
| 属性ありのダブルバインドプロキシ | いいえ | いいえ | はい | はい |
| ダブルパインドプロキシ | いいえ | いいえ | はい | N/A |
| 属性あり/なしのトリプルバインドプロキシ | いいえ | いいえ | いいえ | いいえ |

1. **ユーザビリティの考慮事項**

*このセクションは参考情報である..*

ISO/IEC 9241-11 はユーザビリティを “特定のユーザーが特定の利⽤状況において, 有効性, 効率性, 満足感を持って特定の⽬的を達成するために製品を利⽤できる程度” と定義している. この定義は, 有効性, 効率性, 満⾜感を達成するために必要な要素として, ユーザー, ⽬標, 利⽤状況に着⽬している. ユーザビリティを達成するには, カギとなるこれらの要素を考慮した全体的なアプローチが必要である.

ユーザビリティの観点からは, 連携 ID システムの最⼤の潜在的メリットの1つとして, ユーザーは複数の認証コードの管理に疲れるという問題への取り組みがあげられる. これまではユーザー名とパスワードの問題であったが, ユーザーが認証コードを管理する必要性が増すにつれ, それが物理的なものでもデジタルなものでも, ユーザビリティの課題が持ち上がるようになった.

認証に対するその他のアプローチの多くには, 広範囲に研究され確⽴されたユーザビリティガイドラインがあるが, 連携 ID はまだ日が浅いため研究結果は不十分で決定性を欠いている. 現在のユーザビリティ研究が進むにつれ, 連携 ID システムに関するユーザビリティガイドラインにはより確実に役立つデータが与えられよう. 例えば, 技術的属性の名前と値をわかりやすい言葉に翻訳するガイダンスをサポートするには, さらなるデータが必要である.

800-63A と 800-63B のユーザビリティのセクションで述べたように, どのような認証⼿法においても全体のユーザーエクスペリエンスは不可⽋である. 連携は多くのユーザーにとってまだ馴染みのない対話型パラダイムであるため, ユーザーエクスペリエンスの問題は特に連携 ID システムによく当てはまる. ユーザーの過去の認証経験は, ユーザーの期待に影響を及ぼしうる.

連携 ID システムにおける全体のユーザーエクスペリエンスは, 可能な限りスムーズかつ容易であるべきである. これは以下のユーザビリティ標準 (ISO 25060 シリーズの標準など) やユーザー対話型デザインのために確⽴された成功事例によって達成できる.

前提

このセクションでは, “ユーザー” とは “認証要求者” または “加入者” を意味し, “エンティティ” とは 連携システムに関与する主体を意味する.

ガイドラインと考慮事項はユーザー視点で記述されている.

アクセシビリティはユーザビリティとは異なり, この巻の扱うところではない. セクション 508 は情報技術の障壁を排除するために制定され, オンライン公開コンテンツに障害者がアクセスできるようにすることを連邦機関に求めている. アクセシビリティのガイドラインについては セクション 508 の法律と標準を参照.

## **一般的なユーザビリティの考慮事項**

連携 ID システムは以下を満たすべきである.

* ユーザーの負担を最小限にする（例えば, フラストレーション, 学習曲線）.
  + 必要なユーザーアクション数を最小限にする.
  + [ユーザーがすばやく容易に同⼀ IdP 上の複数のアカウントを選択できるようにする. 例えば Account Chooser](http://openid.net/wg/ac/) [のようなアプローチでは, ユーザーが IdP リストから利⽤したい IdP](http://openid.net/wg/ac/) を選択して連携プロセスを開始するのではなく, ユーザーが最近アクセスしたアカウントリストからアカウントが選択できる.
  + ユーザーの負担の最⼩化と, ユーザーが⼗分に理解した上で決定できる⼗分な情報提供の必要性とのバランスを取る.
* 馴染みのない技術⽤語や細かな説明を最小限に抑える. （例えば, 基本的なコンセプトが明確に説明できれば, ユーザーは IdPや RP といった⽤語を知る必要はない.）
* IdP と RP で⼀貫性のある統合されたユーザーエクスペリエンスを⽬指す.
* グラフィックス, イラスト, FAQ, チュートリアル, 例などのリソースを提供し, ユーザーが身元情報を理解するのを助ける. そうしたリソースでは, ユーザーの情報がどのように扱われ,トランザクションに携わる各主体（例えば, RP, IdP, ブローカー）がどのような相互関係にあるのかを説明すべきである.
* ユーザーに対して明確で誠実な意味あるコミュニケーションを⾏う. （つまり, コミュニケーションは明⽩で簡単に理解できるべきである）
* 場所やデバイスに関係なくユーザーにオンラインサービスを提供する.
* ユーザーに対して信頼関係を明⽩にし, ⼗分な情報と信頼に基づく決定を容易にする. 信頼関係は動的で状況に依存することが多い. ユーザーは, 特定の属性やトランザクションにおいて, ある IdP と RP を他より信頼するかもしれない. 例えば, 貴重な個人情報（⾦融情報や健康情報など）を含んだ Web サイトでは, ユーザーは連携 ID システムの使用をためらうかもしれない. 個人情報についてユーザーが判断する重要度によっては, ユーザーはソーシャルネットワークプロバイダーを IdP として利用しないこともある. ソーシャルネットワーキングのブロードキャスト的な性質を懸念するからである.
* ユーザーが触れるすべての情報について, [SP 800-63Aのセクション 9 (sp800-63a.html#sec9)](https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.html#sec9) に規定されたユーザビリティの考慮事項に従う.
* どこでどのようにして技術的サポートを受けることができるかを明確に伝える. 例えば, ユーザーにオンラインセルフサービス機能へのリンクやチャット機能, ヘルプデスクサポートの電話番号を提供する.トランザクションに関わる主体間（例えば, RP, IdP, ブローカー）でユーザーをたらい回しにするような技術的⽀援は避ける.
* 適切な状況において, 代表的なユーザーと現実的なタスクに対して, 統合的かつ継続的なユーザビリティ評価を⾏い, ユーザー視点から連携 ID システムが成功することを確実にする.

## **特別なユーザビリティの考慮事項**

このセクションでは, 連携 ID システムに対する特別なユーザビリティ上の考慮点を扱う. このセクションは, 連携 ID システムに関連するすべてのユーザビリティ要素を網羅的にカバーすることを意図するものではない. ここでは, ユーザビリティ研究におけるより広範なテーマである, 身元情報に対するユーザーの認識, ユーザーによる採用, 信頼, 連携 ID 空間の認識に焦点を当てる. 場合によっては実装例を示すこともあるが, 特定のソリューションを規定することはない. ⾔及される実装は, 特定のユーザビリティ上のニーズに対応する⾰新的な技術的アプローチを推奨するための例である. 他の例については, システム設計とコーディング, 仕様, API, 最新の成功事例（OpenID や OAuth など）の標準が参考になる. 実装は画一的なソリューションを防止する多くの要因に大きく左右される.

### **オンライン身元情報に対するユーザーの認識**

ユーザーが連携 ID システムに慣れたとしても, 連携 ID には (特にプライバシーと情報共有の点で) ユーザーのデータ処理⽅法に対する高い信頼性を確⽴するのに必要な別のアプローチが存在する. 身元情報の概念はユーザーと実装者では異なる. ユーザーはログインして⾃⾝のプライベートな空間へのアクセスを得るものとして身元情報を捉えるが, 実装者は認証とアサーション, 保証レベル, サービス提供に必要な身元情報属性の一式という視点で捉える. このように, ユーザーと実装者では身元情報の捉え⽅が異なるため, ユーザーが連携 ID システムに適⽤される身元情報の概念を正確に理解できるよう⼿助けすることが不可⽋である. 優れた身元情報識別モデルは, ユーザーが連携システムの利点とリスクを理解し, こうしたシステムを信頼して採用することを促すための基礎となる.

身元情報の特性の多くは, 連携内と連携間の両⽅でユーザーがどのように身元情報を管理するかに影響を及ぼす. サイバースペースの外で使用状況に基づいて複数の身元情報を管理するのと同じように, ユーザーは⾃⾝の身元情報を連携環境で管理する術を学ぶ必要がある. したがって,身元情報と使用状況がどのように扱われるのかがユーザーに明確でなければならない. そのため, 以下の点が考慮されるべきである.

* 異なるユーザーの役割を区別するため, ユーザーに必要な状況と範囲を提供する. 例えば, ユーザーが⾃⾝の代理として⾏動しているのか, ⾃⾝の雇⽤主など他者の代理として⾏動しているのかなど.
* エンティティを区別するため, ユーザーに一意で意味のある記述的な識別⼦を提供する.
* データ所有権とデータ変更権限のあるユーザーに関する情報をユーザーに提供する. 身元情報とそれに関連するデータは, 複数の主体によって更新/変更が可能な場合もある. 例えば, 医療データは患者のものであるが, ⼀部のデータは病院や医師の診療によってのみ更新される.
* ユーザーが簡単に属性を検証, 閲覧, 更新できるようにする.身元情報とユーザーの役割は静的ではなく動的なものであり, 時間経過と共に変わる (例えば, 年齢, 健康および⾦融データ). 属性を更新したり属性提供を決定したりする機能は, 同時に提供されることもあればそうでないこともある. ユーザーが属性を変更するプロセスが周知され, 文書化され, 容易に実⾏できることを保証する.
* 関連するエンティティがすでに存在しない場合でも, ユーザーにデータを更新する⼿段を提供する.
* ユーザーが⾃⾝の身元情報を完全に削除したり,トランザクション履歴を含むすべての情報を消去したりできるようにする. そうしたアクションを妨げる可能性のある適⽤可能な監査, 法律, ポリシー上の制約を考慮する. 場合によっては, 消去よりも完全な無効化の⽅が適切なこともある.
* サイト/アプリケーションのデータ保持について, 分かりやすいポリシーを見つけやすい場所でユーザーに提供する.
* 組織のデータアクセスポリシーに従って, ユーザーに適切な匿名性や仮名性オプションを提供し, 要望に応じてそうした身元情報オプションを切り替えられるようにする.
* ユーザーに各 IdP および RP 間の接続を管理する⼿段を提供する. これには, 完全な分離, 特定の RP の1つ以上の属性へのアクセス権限の削除を含む.

### **信頼とメリットに関するユーザーの認識**

ユーザーによる連携 ID システムの採用には, 多くの要素が影響を及ぼす可能性がある. どのような技術においても, ユーザーはある要素を他の要素より重視する. ユーザーはある技術の採用を決定する前に, 知り得たメリットとリスクを秤にかけることが多い. ユーザーがよく理解した上で決定できるようにするには, IdP と RP が⼗分な情報を提供することが⾮常に重要である. 信頼と信頼階層 (Tiers of Trust) という概念は連携 ID システムの基本原理であり, ユーザーに採用を促す可能性がある. 最後に, ユーザーエクスペリエンスが向上すると, 連携に対するユーザーの利用が増加し, RP による連携の採用も増加する可能性がある.

このサブセクションでは, 主にユーザーの信頼と, メリットとリスクに関するユーザーの認識に焦点を当てる.

ユーザーによる採用を促進するため, IdP と RP はユーザーとの信頼を確⽴して構築し, 採用によるメリットとリスクをユーザーに理解させる必要がある. 考慮点としては以下が挙げられる.

* ユーザーが⾃⾝の情報の開⽰を管理し, 適切な通知により明⽰的同意を⾏えるようにする（SP 800-63C, セクション 9.2 通知と同意を参照）. 通知の内容, サイズ, 頻度のバランスは, ユーザーが何も考えずにクリックスルーしてしまうことを避けるために必須である.
* 属性共有のためには以下の点を考慮する必要がある.
* 共有される属性と属性値を検証する⼿段をユーザーに提供する. 適切なセキュリティ慣行に従う （セクション 7 参照）.
* 全部かゼロかという徹底的なアプローチではなく, ユーザーが部分的な属性リストに対して同意できるようにする. ユーザーが全情報の共有に同意しない場合でも, ある程度のオンラインアクセスを可能にする.
* ユーザーが共有済属性リストへの同意を更新できるようにする.
* ユーザーに提⽰される不必要な情報を最小限に抑える. 例えば,認証レスポンスの⼀部として RP と共有されるとしても, システムが⽣成した属性（ペア匿名識別子など）を表示しない.
* ユーザーのステップとナビゲーションを最小限に抑える. 例えば,属性共有の同意をプロトコルに組み込み, 連携トランザクションの外の機能としない. こうした例は, OAuth や OpenID Connect といった標準に⾒られる.
* IdP により不正な属性情報を付与された状況からユーザーが回復できるよう, 効果的かつ効率的な是正⼿段を提供する（セクション 7 参照）.
* ユーザーに属性共有の同意を要求する回数を最小限に抑える. 同意要求の頻度を限定することで, 何度も同じ属性の共有要求を受けるユーザーのフラストレーションを避けることができる.
* 制限された利⽤⽬的のためにのみ情報を収集し, 情報開⽰を最小限に抑える (セクション 9.3 参照). ユーザーの明⽰的な同意なしに不必要かつ過剰な情報の収集や開⽰または追跡を⾏うと, ユーザーの信頼は失われる. 例えば, ユーザーに対して現在のトランザクションに関連する属性のみを要求し, RP でユーザーが利用するかどうかわからないトランザクションのために属性を要求しないようにする.
* 連携 ID の利⽤による潜在的メリットとリスクをユーザーにはっきりと誠実に伝える. ユーザーが重視するメリットとしては, 時間節約, 使いやすさ, 管理するパスワード数の減少, 利便性の向上などがある.

リスクに対するユーザーの懸念は, 連携 ID システムの採用意欲に悪影響を与える. ユーザーは, 信頼, プライバシー, セキュリティ, 単一点障害といった点に懸念を抱く可能性がある. 例えば, ひとつの IdP が⼀時的または永続的に利⽤できなくなった場合, ユーザーは複数のアカウントへのアクセスを失うことを恐れるかもしれない. さらに, ユーザーは新しい認証プロセスを学ぶことを心配したり混乱したりする可能性もある. 連携 ID システムの採用を促進するには, 認識されるメリットが認識されるリスクを上回らねばならない.

### **ユーザーモデルと信念**

ユーザーは認識と信念に基づいて特定の結果を期待したり特定の⽅法で⾏動したりする傾向にある. そのような信念, 認識, 傾向は, 社会科学でメンタルモデルと呼ばれる. 例えば, ファストフード店やカフェテリア, 格式の高いレストランなど, ⼈々は店によって⾏動や期待を異にするような⾷事に関するメンタルモデルを持っている. したがって, それぞれの店でどのように振る舞うのが適切かを理解するのにすべての店を知っている必要はない.

連携についてすばらしく完璧なメンタルモデルをユーザーが形成できるよう⽀援することにより, ユーザーはある特定の実装を超えて⼀般化を⾏うことができる. 連携 ID システムがユーザー視点でデザインされていなければ, ユーザーは間違った不完全なメンタルモデルを形成し, こうしたシステムの採用に影響を及ぼすかもしれない. 考慮点としては以下がある.

* ユーザーの誤解を避けるため,トランザクション関係者（例えば, RP, IdP, ブローカー）間の関係性と情報の流れを明確に説明する. ⼀般的⽤語である IdP と RP という語を使⽤するのではなく, 実際のエンティティの名前を使⽤して説明する.
* ⼈⽬をひく視覚的サインや情報を提供し, ⼀⾒無関係なエンティティが相互に関係している理由を理解できるようにする. 例えば, ユーザーは連携 ID システムにおける情報の流れの理解が不⾜しており, オンラインでの個⼈的な⾏動と政府サービスが混じることに関心を持つかもしれない.
* ⼈⽬をひく視覚的サインや情報を提供し, RP が管理を⾃⾝のサイトから IdP にリダイレクトする必要がある際にリダイレクトに関してユーザーに知らせる. 例えば, IdP のユーザーインタフェース内に RP の名前を表⽰し, ⽬的とする RP にアクセスするためにこの IdP にログインしようとしていることをユーザーに知らせる.
* トランザクション関係者（例えば, RP, IdP, ブローカー）の信憑性を判断するため, ユーザーに明確で利⽤しやすい⼿段(例えば, 見て分かる確実性) を提供する. これは, 特にルートドメインが変わる（例えば, .gov から .com）場合など, あるドメインから別のドメインに移る際のユーザーの懸念を緩和するにも役⽴つ. 例えば, IdP の URL を表⽰して, ユーザーが悪意あるサイトにフィッシングされていないことを検証できるようにする.
* 暗黙的なログインと明⽰的なログアウトに関して, ユーザーに視覚的サインを含む明確な情報を提供する. 実装によっては,IdP アカウントで RP にログインすると IdP と RP 双⽅に対して認証されることもある. その場合, ユーザーは RP でのセッションを終了したとしても, 必ずしも IdP のセッションが終了されるわけではなく, IdP から明⽰的に “ログアウト” する必要があることに気づかないかもしれない. IdP のセッションを終了するために明⽰的なログアウトが必要な場合, ユーザーはそれに気づくための明確な情報を必要とする.

# 例

*このセクションは参考情報である..*

以下では3種類のアサーション技術である SAML アサーション, Kerberos チケット, OpenID Connect トークンについて説明する. このリストには, 使用可能なすべてのアサーション技術は含まれないが, 連携 ID システムで⼀般的に利⽤されているものを代表している.

## **セキュリティアサーションマークアップ言語 (Security Assertion Markup Language (SAML))**

SAML は, 信頼関係のあるエンティティ間でインターネットを介して認証と属性情報をやりとりする XML ベースのフレームワークである. 執筆時点で最新の SAML 仕様は, 2005/03/15 発表の SAML v2.0 である.

SAML の構成要素を以下に⽰す.

* アサーションの構造を定義するアサーション XML スキーマ
* アサーションと成果物 (セクション 7.1 で述べたインダイレクトモードで使われるアサーション) をのリクエストに使用する SAML プロトコル
* 基盤となる通信プロトコル (HTTP や SOAP など) を定義し, SAMLアサーションの転送に利⽤できる結び付け

上記の３要素により, “Web ブラウザ SSO” といった特定のユースケースに対応した SAML プロファイルが定義される. SAMLアサーションは XML スキーマにエンコードされ, 3つのタイプのステートメントを伝える.

* *認証ステートメント*: アサーション発行者, 認証済み加入者, 有効期間およびその他の認証に関する情報を含む. 例えば, ある認証アサーションは, 加入者“John” が 2004/06/06 10:32pm にパスワードを使って認証されたことを⽰す.
* *属性ステートメント*: 加入者に関する特定の追加特性を含む. 例えば, 主体“John” は属性“Role” に値“Manager” で関連付けられている.
* *権限ステートメント*: 加入者がアクセス権を持つリソースを⽰す. こうしたリソースには, 特定のデバイス, ファイル, 特定の Web サーバーに関する情報などがある. 例えば, 主体 “John” は与えられたエビデンス “Role” によって “Webserver1002” 上でアクション “Read” が⾏える.

権限ステートメントはこのドキュメントの扱うところではなく, ここでは議論しない.

## **Kerberos チケット**

Kerberos ネットワーク認証サービス [RFC 4120] は, ローカルの共有ネットワーク上のクライアント/サーバーアプリケーションに対して, 対称鍵暗号を利⽤した強固な認証を提供するために設計された. Kerberos の拡張では, プロトコルの特定のステップにおいて公開鍵暗号を利⽤することもできる. Kerberos は加入者と RP の間のセッションデータの機密性と完全性の保護もサポートする. Kerberos はアサーションを利⽤するが, 共有ネットワーク上で使用するために設計されたものであるため, 正確には連携プロトコルとは⾔えない.

Kerberos は, 信頼できない共有ローカルネットワーク上で1つ以上の IdP を利⽤した加入者の認証をサポートしている. IdP が加入者に対して暗号化したランダムなセッションキーを復号できることを⽰すことによって,加入者は暗黙的に IdP に対して認証する (一部の Kerboros には,加入者が明⽰的に IdP に対して認証することを求めるものもあるが, 一般的ではない). 暗号化されたセッションキーに加え, IdP は Kerberos チケットと呼ばれるもう1つの暗号化オブジェクトを⽣成する. このチケットには同じセッションキー,セッションキーが発⾏された加入者の身元情報,セッションキーの有効期限が含まれている. このチケットは, 明⽰的なセットアップフェーズ中に IdP と RP の間で共有される事前に確⽴された鍵によって機密性と完全性を保護している.

セッションキーを使って認証するには,加入者は Kerberos チケットに埋め込まれたセッションキーを保有していることを証明する暗号化データといっしょにチケットを RP に送る.セッションキーは, 新しいチケットを⽣成したり,加入者と RP の間の通信を暗号化して認証したりするために使われる.

このプロセスを開始するため,加入者は認証サーバー (AS) に認証リクエストを送る. AS は加入者の⻑期間有効な認証情報を⽤いて,加入者に対してセッションキーを暗号化する. この⻑期間有効な認証情報は, AS と加入者間の共有秘密鍵でもよいし, Kerberos 派⽣の PKINIT のように公開鍵証明書でもよい.加入者と IdP の間の共有秘密鍵に基づいた Kerberos 派⽣のほとんどは, この鍵をユーザーが⽣成したパスワードから導出する. したがって, Flexible Authentication Secure Tunneling (FAST) [RFC 6113] や似たようなトンネリングや防護メカニズムを利⽤していない限り, 受動的な盗聴者によるオフライン辞書攻撃に対して脆弱である.

セッションキーを加入者に伝送するのに加えて, AS は Ticket Granting Server (TGS) と共有する鍵を使ったチケットを発⾏する. このチケットは, Ticket Granting Ticket (TGT) と呼ばれる. これは検証者が TGT 内のセッションキーを利⽤して, 明⽰的に検証者を認証するかわりにチケットを発⾏することに由来する. TGS は TGT 内のセッションキーを利⽤して加入者に対する新規セッションキーを暗号化し, RP と共有している鍵を使って新規セッションキーに対応するチケットを⽣成する. 加入者はセッションキーを復号し, チケットと新規セッションキーをいっしょに使って RP に対して認証する.

Keriberos認証がパスワードに基づいている場合, このプロトコルは最初のユーザーと KDC とのやりとりを傍受する盗聴者によるオフライン辞書攻撃に対して脆弱であることが知られている. ⼗分な⻑さのパスワードはユーザーにとって厄介なものであるが, より⻑く複雑なパスワードを利⽤すればこの脆弱性は軽減される. ただしパスワードベースのKerberos認証が FAST (または類似の) トンネルで利⽤されている場合, 辞書攻撃を実⾏するには追加で中間者攻撃が必要になる.

## **OpenID Connect**

OpenID Connect [OIDC] は, OAuth 2.0 Authorization Framework および JSON Object Signing and Encryption (JOSE) 暗号システムに基づいた, インターネット規模の 連携 ID および認証プロトコルである.

OpenID Connect は OAuth 2.0 認証プロトコルの上に構築され, RP が加入者の身元情報と認証情報へアクセスすることを加入者が認可できるようにする. OpenID Connect および OAuth 2.0 における RP はクライアントとも呼ばれる.

OpenID Connect のトランザクションが成功すると, IdP は ID トークンという JSON Web Token (JWT) 形式の署名付きアサーションを発⾏する. クライアントは ID トークンを解析し, 加入者および IdP 上での最初の認証イベントに関する情報を取得する. このトークンは, 加入者と認証イベントに関する以下の最低限の情報を含む.

* iss -アサーションを発⾏した IdP を識別する HTTPS URL.
* sub - IdP 固有の Subject 識別⼦であり,加入者を⽰す.
* aud - IdP 固有の Audience 識別⼦であり, IdP におけるこの OAuth 2.0 クライアントの Client 識別⼦に等しい.
* exp - ID トークンの有効期限を⽰すタイムスタンプ. クライアントはこの時刻を過ぎた後にこのトークンを受け⼊れてはならない (SHALL NOT).
* iat - ID トークンの発⾏⽇時を⽰すタイムスタンプ. クライアントはこの時刻より前にこのトークンを受け⼊れてはならない (SHALL NOT).

ID トークンに加え, IdP はクライアントに OAuth 2.0 アクセストークンを発⾏する. このトークンは IdP の UserInfo エンドポイントへのアクセスに利⽤できる. このエンドポイントは主体の属性⼀式を⽰す JSON オブジェクトを返す. このオブジェクトには名前, Eメールアドレス, 住所, 電話番号, その他のユーザー情報が含まれるが, それだけに限らない. ID トークン内の情報が認証イベントを反映したものである⼀⽅で, UserInfo エンドポイントから返される情報は⼀般的に持続性が高いため, より汎⽤的な目的で使用できると考えられる. UserInfo エンドポイントのその他の属性へのアクセスは, 特別に定義された OAuth 2.0 スコープである openid, profile, email, phone, addres のセットにより制御される. さらに offline\_access という追加のスコープがリフレッシュトークンの発⾏を制御するために使われる. リフレッシュトークンを使うと, RP は加入者が不在時でも UserInfo エンドポイントにアクセスできる. したがって, UserInfo エンドポイントへのアクセスは,加入者がそこにいることの証明として RP で認証済みセッションを確立するには不⼗分である.

# 参照文献

*このセクションは参考情報である.*

## **一般**

[FEDRAMP] General Services Administration, *Federal Risk and認証Management Program*, available at: https://www.fedramp.gov/.

[M-03-22] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html.

[NISTIR 8112] NIST Internal Report 8112 (Draft), Attribute *Metadata*, available at: https://pages.nist.gov/NISTIR-8112/NISTIR- 8112.html.

[Section 508] Section 508 Law and Related Laws and Policies (January 30, 2017), available at: https://www.section508.gov/content/learn/laws-and-policies.

## **標準**

[BCP 195] Sheffer, Y., Holz, R., and P. Saint-Andre, *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, https://doi.org/10.17487/RFC7525.

[ISO 9241-11] International Standards Organization, ISO/IEC 9241-11 *Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability*, 1998, available at: https://www.iso.org/standard/16883.html.

[OIDC] Sakimura, N., Bradley, B., Jones, M., de Medeiros, B., and C. Mortimore, *OpenID Connect Core 1.0 incorporating errata set 1*, November, 2014. Available at: https://openid.net/specs/openid-connect-core-1\_0.html.

[RFC 4120] IETF, *The Kerberos Network Authentication Service (V5)*, RFC 4120, DOI 10.17487/RFC4120, July 2005, https://doi.org/10.17487/RFC4120.

[RFC 6113] IETF, *A Generalized Framework for Kerberos Pre-Authentication*, RFC 6113, DOI 10.17487/RFC6113, April 2011, https://doi.org/10.17487/RFC6113.

[RFC 7591] IETF, *OAuth 2.0 Dynamic Client Registration Protocol*, RFC 7591, DOI 10.17487/RFC7591, July 2015,<https://doi.org/10.17487/RFC7591>.

[RFC 7636] IETF, *Proof Key For Code Exchange*, RFC 7636, DOI 10.17487/RFC7636, September 2015, <https://doi.org/10.17487/RFC7636>.

[[SAML] OASIS, *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, March 2008, available at: http://docs.oasis- open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.](file:///C:\Users\shiokawa\AppData\Local\Temp\B2Temp\Attach\%5bSAML%5d%20OASIS,%20Security%20Assertion%20Markup%20Language%20(SAML)%20V2.0%20Technical%20Overview,%20March%202008,%20available%20at:%20http:\docs.oasis-%20open.org\security\saml\Post2.0\sstc-saml-tech-overview-2.0.html)

## **NIST 特別出版物**

[NIST 800 Series Special Publications are available at: http://csrc.nist.gov/publications/nistpubs/index.html (http://csrc.nist.gov/publications/nistpubs/index.html). The following publications may be of particular](http://csrc.nist.gov/publications/nistpubs/index.html) interest to those implementing systems of applications requiring digital authentication.

[SP 800-53] NIST Special Publication 800-53 Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015), http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[[SP 800-63-3] NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.](file:///C:\Users\shiokawa\AppData\Local\Temp\B2Temp\Attach\%5bSP%20800-63-3%5d%20NIST%20Special%20Publication%20800-63-3,%20Digital%20Identity%20Guidelines,%20June%202017,%20https:\doi.org\10.6028\NIST.SP.800-63-3)

[SP 800-63A] NIST Special Publication 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*, June 2017, [https://doi.org/10.6028/NIST.SP.800-63a (https://doi.org/10.6028/NIST.SP.800-63a).](https://doi.org/10.6028/NIST.SP.800-63a)

[SP 800-63B] NIST Special Publication 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, June 2017, https://doi.org/10.6028/NIST.SP.800-63b.

## **連邦情報処理標準**

[FIPS 140-2] Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (with Change Notices through December 3, 2002), https://doi.org/10.6028/NIST.FIPS.140-2.

[Privacy](http://www.nist.gov/public_affairs/privacy.cfm#privpolicy) [Policy (http://www.nist.gov/public\_affairs/privacy.cfm#privpolicy) | Security Notice](http://www.nist.gov/public_affairs/privacy.cfm#secnot) [(http://www.nist.gov/public\_affairs/privacy.cfm#secnot) | Accessibility Statement (http://www.nist.gov/public\_affairs/privacy.cfm#accesstate)](http://www.nist.gov/public_affairs/privacy.cfm#accesstate) [| Send feedback (https://github.com/usnistgov/800-63-3/issues/)  (/800-63-3/comment\_help.html)](https://openid-foundation-japan.github.io/800-63-3/comment_help.html)