



Liberty 技術用語集

バージョン 1.2

作成者

Thomas Wason, IEEE ISTO

協力者

- . Carolina Canales-Valenzuela, Ericsson
- . John Kemp, IEEE ISTO
- . Elisa Korentayer, IEEE ISTO
- . John Linn, RSA Security, Inc.
- . Peter Davis, Neustar, Inc.

概要

Liberty Alliance Projectの用語集。Liberty Alliance仕様に使用されている重要な用語、略語、および頭字語

ファイル名: liberty-glossary-v1.2-JP.pdf

Copyright © 2003 Liberty Alliance Project

1 告知

2 Copyright © 2002, 2003 ActivCard; American Express Travel Related Services; America Online,
3 Inc.; Bank of America; Bell Canada; Catavault; Cingular Wireless; Cisco Systems, Inc.; Citigroup;
4 Communicator, Inc.; Consignia; Cyberun Corporation; Deloitte & Touche LLP; Earthlink, Inc.;
5 Electronic Data Systems, Inc.; Entrust, Inc.; Ericsson; Fidelity Investments; France Telecom;
6 Gemplus; General Motors; Hewlett-Packard Company; i2 Technologies, Inc.; Intuit Inc.; MasterCard
7 International; NEC Corporation; Netegrity; NeuStar; Nextel Communications; Nippon Telegraph
8 and Telephone Company; Nokia Corporation; Novell, Inc.; NTT DoCoMo, Inc.; OneName
9 Corporation; Openwave Systems Inc.; PricewaterhouseCoopers LLP; Register.com; RSA Security
10 Inc; Sabre Holdings Corporation; SAP AG; SchlumbergerSema; SK Telecom; Sony Corporation;
11 Sun Microsystems, Inc.; Symlabs, Inc.; Trustgenix; United Airlines; VeriSign, Inc.; Visa
12 International; Vodafone Group Plc; Wave Systems;. All rights reserved.

13

14 本書は、Liberty Alliance の参加企業によって作成されました。本書は、この仕様の実装以外
15 の目的で使用することはできません。この仕様を他で引用することは禁止されています。
16 それ以外の用途でこの文書の複製を希望する場合は、Liberty Alliance まで使用許可について
17 お問い合わせください。

18

19 この仕様の特定要素の実装には、特許権など、第三者が所有する知的所有権の使用許諾権
20 が必要な場合があります。それ以外において本仕様の策定に協力した企業は、かかる第三
21 者の知的所有権の有無を確認することまたは確認しなかったことについて一切責任を負い
22 ません。この仕様は、「無保証で」提供されるものであり、Liberty Alliance の参加企業は、
23 明示的または黙示的を問わず、商品性、第三者の知的所有権を侵害しないこと、特定目的
24 に対する適合性についていかなる保証もいたしません。この仕様の実装にあたっては、
25 Liberty Alliance Project の Web サイト (<http://www.projectliberty.org/>) にアクセスして、Liberty
26 Alliance 理事会がこれまでに受け取っている「Necessary Claims Disclosure Notices(必要な特許
27 請求範囲の開示に関する告知)」の情報をご確認ください。

28

29 (日本語訳はしがき)

30 この文書の日本語訳においては、原文(英語)で表現されている内容について RFC 文献の
31 日本語訳等を参考にできるだけ正確を期すよう務めました。あくまで Liberty 仕様の理解
32 の参考とするにとどめ、Liberty 仕様の実装を検討され、知的所有権を確認する場合、必ず
33 原文や参考文献を参照いただくようお願いいたします。

34 翻訳にあたった Liberty Alliance 参加企業は原文と同様、本文書に係る翻訳の正確性、翻訳
35 された仕様の商品性、第三者の知的所有権に対する非侵害性、特定目的に対する適合性な
36 どを一切保証しません。

37

38 Liberty Alliance Project
39 Licensing Administrator
40 c/o IEEE-ISTO
41 445 Hoes Lane
42 Piscataway, NJ 08855-1331, USA
43 info@projectliberty.org

44

45 **目次**

46	1. はじめに	6
47	2. 定義	7
48	3. 参考文献	20

49 1. はじめに

50 この文書は、Liberty Alliance Project で取り扱う用語の標準リファレンスを提供し、そ
51 れによってインターネット上のアイデンティティソリューション、とくに、Liberty
52 Alliance により定義されるソリューションについて議論する際に、共通の意味で用語が理
53 解されるようにすることを目的としています。

54
55 この文書は、ネットワークアイデンティティに関する議論に使用されるすべての用語を完
56 全に網羅した公式なものではなく、Liberty で取り扱う範囲の概念の定義を幅広くまとめた
57 ものです。このような文脈で頻繁に使用されていても日常的な意味で用いられる多くの用
58 語は、ここに記載していません。さらに、Liberty に関連する多くの用語は、セキュリティ
59 やプライバシーに関するものです。そのため、この文書の典拠として[RFC2828]を採用し、
60 ここで定義されておらず、[RFC2828]で RECOMMENDED の定義として記載されている用語
61 が標準となります。注：関係者にとって必要な用語が 1 つにまとめた用語集を一連の
62 Liberty 文書に添付できるように、この文書に[RFC2828]から引用したいいくつかの定義（出典
63 を明記）を含めました。

64
65 最後に、この用語集は現時点での文書であるため、常に改訂される可能性があります。内
66 容および書式に関するコメントは、Liberty Technology Working Group
67 (technology@projectliberty.org) までお寄せください。

68 **2. 定義**

69 **AAC**

70 「認証アサーションコンテキスト」を参照。

71

72 **アクセスコントロール**

73 要求されたアクセスをリソースに仲介する行為で、要求者の特権属性と要求されたリソ
74 スのコントロール属性に基づいて行われる。

75

76 **アカウント**

77 定期的な取引やサービスの提供に関して、主体者とサービスプロバイダ間で交わされた正
78 式な契約。

79

80 **アカウントのリンク**

81 「アイデンティティ連携」を参照。

82

83 **AD**

84 「認証ドメイン」を参照。

85

86 **アフィリエイト**

87 アフィリエイトとは、プロバイダ ID で記述した 1 つまたは複数のエンティティの集ま
88 りであり、その中でメンバーとして Liberty の対話を行うことができる。アフィリエイト
89 ャンは、1 つのアフィリエイト ID で照会し、プロバイダ ID によって特定された 1 つの
90 エンティティがこれを管理する。アフィリエイトに参加するメンバーは、アフィリエイト
91 のメンバーとして (アフィリエイト ID を使用) または単独で (プロバイダ ID
92 を使用) サービスを呼び出すことができる。「アフィリエイト」と「アフィリエイト
93 グループ」は同義。

94

95 **アフィリエイトグループ**

96 「アフィリエイト」を参照。

97

98 **AP**

99 「属性プロバイダ」を参照。

100

101 **APL**

102 属性プロバイダ (AP) は、ID-PP 情報を提供する。ID-PP プロバイダとも言う。AP は、ID-PP
103 をホスティングする ID-WSF Web サービスである。

104

105 **アーティファクト、SAML**

106 完全な SAML アサーションを指し示すためのランダムで小さな数値。SAML アーティファ
107 クトは、ブラウザの URL クエリ文字列によってサイト間で渡される。[SAMLBind11],
108 [SAMLCore11]

109

110 **アサーション**

111 主体者側で行われる認証行為、主体者の属性情報、または特定のリソースについて主体者

112 に適用する権限許諾に関して、SAML オーソリティにより生成されるデータ。

113

114 **属性**

115 主体者を識別する特徴。一般に、主体者の属性によって主体者そのものを表すとされる。

116

117 **属性クラス**

118 あらかじめ定義された属性のセット。たとえば、主体者名の構成要素（プレフィクス、フ
119 ァーストネーム、ミドルネーム、ラストネーム、およびサフィックス）などがある。Liberty
120 のエンティティは、これらのクラスを標準化することができる。

121

122 **属性コンテナ**

123 予想使用パターンに従ってグループ化した属性の集まりによって構成されるモジュールを
124 指す。

125

126 **属性プロバイダ (AP)**

127 属性プロバイダ (AP) は、ID-PP (アイデンティティパーソナルプロファイル) 情報を提供
128 する。ID-PP プロバイダとも言う。AP は、ID-PP をホスティングする ID-WSF Web サービ
129 スである。

130

131 **認証された主体者**

132 アイデンティティプロバイダからアイデンティティ認証を受けた主体者。

133

134 **認証 (AuthN)**

135 通信者が主体者の名前で「対話」する資格を持っているかどうかを検証するプロセス。

136

137 **認証オーソリティ**

138 認証アサーションを作成するシステムエンティティ。 [SAMLGloss]

139

140 **認証アサーションコンテキスト (AAC)**

141 資格付与の判断を下す前に、サービスプロバイダが認証アサーション自体に加えて要求す
142 る可能性のある情報。

143

144 **認証ドメイン (AD)**

145 認証ドメイン (AD) とは、Liberty に対応するエンティティの公式コミュニティであり、既
146 知の共通ルールセットに従って対話が行われる。

147

148 **認証セッション**

149 A が B を認証した後から、A が B の ID アサーションの信頼を中止して再認証を要求するま
150 での時間。単に「セッション」と呼ばれることもあり、主体者による正常なログインから
151 ログアウトまでの状態を指す。

152

153 **認証クオリティ**

154 サービスプロバイダがアイデンティティプロバイダから受け取った認証アサーションにお
155 くことができる、保証レベル。

156

157 **認可 (AuthZ)**

158 適用されるアクセス制御情報を査定することによって、対象ユーザーが特定のリソースに
159 対する特定のタイプのアクセス権を有しているかどうかを判断するプロセス。通常、認証
160 コンテキストに沿って認可を行う。認証されたユーザーに、異なるタイプのアクセス実行
161 権限が付与される場合がある。([SAMLGloss]より)

162

163 **証明書管理**

164 証明書のライフサイクルの間に、デジタル証明書の発行者が果たす以下のような機能。
165 [RFC2828]

- 166 ・ 証明書にバインドするデータ項目の取得と確認。
- 167 ・ 証明書の符号化と証明書への署名。
- 168 ・ ディレクトリまたはレポジトリでの証明書の保管。
- 169 ・ 証明書の再発行と鍵更新、内容更新。
- 170 ・ 証明書の取り消しと CRL の発行。

171

172 **証明書ポリシー (CP)**

173 特定のコミュニティやアプリケーションのクラスに対する証明書の適用範囲を示す一連の
174 規則。たとえば、証明書ポリシーでは、所定の価格帯の B2B 取引における参加者の認証に
175 は特定の種類の証明書が適切であると指示される場合がある。証明書運用規定と証明書ポ
176 リシーの根本的な違いは、前者は証明書発行機関が「所有」するのに対し、後者は発行さ
177 れた証明書を使用するエンティティが所有することである。証明書ユーザーが証明書ポリ
178 シーを定義し、(異なる証明書運用規定を保有する) 証明機関がその証明書ポリシーに特定
179 の証明書が適切であることを証明する。

180

181 **証明書運用規定 (CPS)**

182 証明機関が証明書の発行時に適用する運用規定を記述したもの。証明書運用規定は、信頼
183 性の高いシステムの詳細と、証明書の発行時に採用する運用規定を証明機関が宣言する形
184 で提示される。

185

186 **証明書失効リスト (CRL)**

187 発行者によって有効期限切れ以前に取り消されたデジタル証明書を列挙したデータ構造。
188 [RFC2828]

189

190 **ces**

191 Case Exact String の略。ある属性を自由形式の文字列から成るものとして定義するために使
192 用する用語。完全一致では、この属性の比較で大文字と小文字を区別する。「cis」も参照。

193

194 **トラストサークル (circle of trust)**

195 ユーザーが安全でシームレスな環境で取引できるような、Liberty アーキテクチャおよび運
196 用協定に基づくビジネス関係を持っているサービスプロバイダとアイデンティティプロバ
197 イダとの連携。

198

199 **cis**

200 Case Inexact String の略。ある属性を自由形式の文字列から成るものとして定義するために
201 使用する用語。不完全一致では、この属性の比較で大文字と小文字を区別しない。「ces」も

202 参照。

203

204 **クッキー**

205 通常 Web を利用した個人のローカルコンピュータに保存されるもので、ユーザー名や現在の
206 の日時を含む情報の集合を指す。主として以前にサイトを訪問したり、登録したことがあ
207 る利用者を Web サイトが識別するために利用される。

208

209 **CoT**

210 「トラストサークル (Circle of Trust)」を参照。

211

212 **CP**

213 「証明書ポリシー」を参照。

214

215 **CPS**

216 「証明書運用規定」を参照。

217

218 **CRL**

219 「証明書失効リスト」を参照。

220

221 **クレデンシャル**

222 表明された事実が正しいことを証明する既知のデータ。

223

224 **データ**

225 主体者がアイデンティティプロバイダやサービスプロバイダに提示するあらゆる情報。

226

227 **アイデンティティ連携の解除**

228 今後アイデンティティプロバイダがサービスプロバイダに主体者のアイデンティティを提
229 供したり、サービスプロバイダがアイデンティティプロバイダからユーザーのアイデンテ
230 イティを受け取ることがないように、アイデンティティプロバイダとサービスプロバイダ
231 間でのユーザーアカウントのリンクを解除すること。

232

233 **委任**

234 あるシステムエンティティに、主体者に代わってアイデンティティサービスにアクセスさ
235 せること。

236

237 **デジタル証明書**

238 電子的に署名されたアサーション。基礎となるアサーションの発行元と同じ主体者が証明
239 書に署名しなければならない。

240

241 **デジタル署名**

242 秘密鍵と署名対象のメッセージ内容に大きく依存するデータ構造。デジタル署名は、対応
243 する公開鍵でしか確認できない。注：多くの点で、デジタル署名は手書きの署名と同義で
244 はない。注：国際的な法律では、デジタル署名の定義はさまざまである。「公開鍵暗号方式」
245 も参照。

246

247 **ディスカバリサービス**

248 属性プロバイダを特定するための Liberty のサービス。
249

250 **DNS (Domain Name System)**

251 主にインターネットでホスト名をインターネットアドレスに変換するために使用される、
252 分散型の複製された汎用のデータ照会サービス。
253

254 **ECML**

255 「 Electronic Commerce Modeling Language 」を参照。
256

257 **Electronic Commerce Modeling Language (ECML)**

258 複数ベンダーから提供される電子財布のような自動化ソフトウェアが、統一規格で必要デ
259 ータを提供できるようにするための階層的な支払い用のデータ構造の一式。
260

261 **エンドポイント**

262 「 エントリポイント 」の口語。
263

264 **エンティティから提供されるデータ**

265 エンティティから Liberty トラストサークルのメンバーに直接提供されるあらゆるデータ。
266

267 **エントリポイント**

268 サービスを利用するために使用できる、SOAP (RPC) アドレスと機能名。Liberty エントリ
269 ポイントには、ディスカバリサービスにおいて検出される対象を指す。
270

271 **連携させる**

272 2 つ以上のエンティティをリンクまたはバインドすること。
273

274 **連携アーキテクチャ (認証)**

275 Liberty トラストサークル内の加盟者間で主体者にサービスを提供する複数エンティティを
276 サポートするアーキテクチャ。
277

278 **連携**

279 任意の数のサービスプロバイダおよびアイデンティティプロバイダで構成される提携関係。
280

281 **HTTP (Hypertext Transport Protocol)**

282 分散協調型ハイパーメディア情報システム用のアプリケーションレベルのプロトコル。
283 [RFC2616]
284

285 **ID-PP**

286 ID 個人プロフィール (ID-PP) とは、プライベートと職場の領域を問わず、主体者に関する
287 アイデンティティ情報のこと。
288

289 **アイデンティティ**

290 エンティティの本質のことであり、しばしばその特性によって表される。
291

292 **アイデンティティ連携**

293 トラストサークル内のさまざまな Liberty Alliance エンティティにおいて、主体者の複数ア
294 カウントを関連付けたり、バインドすること。

295

296 **アイデンティティプロバイダ (IdP)**

297 主体者のアイデンティティ情報を生成、保管、管理し、主体者の認証をトラストサークル
298 内の他のサービスプロバイダに提供する Liberty 対応のエンティティ。

299

300 **アイデンティティサービス**

301 1つまたは複数のアイデンティティに関する情報を収集、更新し、それらアイデンティテ
302 ィのために何らかの行為を行うよう特定のリソースに作用する、Web サービスの抽象的観念。

303

304 **呼び出しアイデンティティ**

305 メッセージ処理時にサービスをリクエストする側であり、SAML アサーションの主体。

306

307 **IdP**

308 「アイデンティティプロバイダ」を参照。

309

310 **IPsec (Internet Protocol Security)**

311 パブリックなネットワークにおけるデータ通信の機密性、完全性、および真正性を確保す
312 るためのオープンスタンダードのフレームワーク。

313

314 **Kerberos**

315 信頼できる第三者機関による認証プロトコル。[RFC1510]を参照。

316

317 **Liberty Alliance ガイドライン**

318 Liberty Alliance によって定義され、Liberty 仕様を最大限に実装するために準拠することを推
319 奨されているポリシー。

320

321 **Liberty Alliance 原則**

322 アイデンティティプロバイダまたはサービスプロバイダが Liberty 規格に準拠であるために
323 契約上合意しなければならないという約束事項。

324

325 **Liberty アーキテクチャ**

326 連携したアイデンティティによるシングルサインオンが可能な専門のプログラムや仕様を
327 サポートするアーキテクチャ。

328

329 **LEC**

330 「Liberty 対応クライアント」を参照。

331

332 **LECP**

333 「Liberty 対応クライアントまたはプロキシ」を参照。

334

335 **LEP**

336 「Liberty 対応プロキシ」を参照。

337

338 **Liberty 対応クライアント (LEC)**

339 主体者がサービスプロバイダで利用することを希望するアイデンティティプロバイダに関
340 する情報を保有するか、または情報の取得方法を知っているエンティティを指す。

341

342 **Liberty 対応クライアントまたはプロキシ (LECP)**

343 Liberty 対応クライアントとは、主体者がサービスプロバイダで利用を希望するアイデンテ
344 ィティプロバイダに関する情報を保有するか、または情報の取得方法を知っているクライ
345 アントを指す。Liberty 対応プロキシとは、Liberty 対応クライアントをエミュレートする
346 HTTP プロキシ (一般的には WAP ゲートウェイ) を指す。

347

348 **Liberty 対応プロバイダ**

349 本書においてのみ適用される定義として、Liberty 対応プロバイダとは、主体者の個人識別
350 情報 (PII) を収集、転送、または受信する属性プロバイダ (AP)、ディスカバリサービス
351 (DS)、サービスプロバイダ (SP)、アイデンティティプロバイダ (IdP) のいずれかである。

352

353 **Liberty 対応クライアント/プロキシプロファイル**

354 このプロファイルでは、Liberty 対応クライアントまたはプロキシ (場合によってはその両
355 方)、サービスプロバイダ、アイデンティティプロバイダの間のやり取りを指定します。

356

357 **Liberty 対応プロキシ (LEP)**

358 Liberty 対応プロキシとは、Liberty 対応クライアントをエミュレートする HTTP プロキシ (典
359 型的には、WAP ゲートウェイ) を指す。

360

361 **Liberty 対応ユーザーエージェント/デバイス (LUAD)**

362 Liberty 仕様の 1 つまたは複数のプロファイルに対して特有のサポートを有するユーザーエ
363ージェントまたはデバイス。標準の Web ブラウザは、Liberty で定義する多くのシナリオに
364 用いることができるが、Liberty プロトコル特有のサポートがされないため、LUAD とはな
365 らないことに留意する必要がある。

366 特有機能のいかなる要求も、LUAD の定義のみに基づくシステムエンティティの存在を意
367 図するものではない。むしろ LUAD は、特有機能を実装する Liberty 仕様で定義される 1 つ
368 または複数の Liberty システムエンティティの役割を実行してもよい。たとえば、
369 LUAD-LECP は、Liberty LECP プロファイルをサポートするユーザーエージェントまたはデ
370 バイスであり、LUAD-DS であれば、Liberty ID-WSF ディスカバリサービスを提供するユー
371 ザーエージェントまたはデバイスが定義されることになる。

372

373 **ログイン**

374 主体者が、システムリソースを利用できるセッションへのアクセスを取得する行為。
375 [RFC2828]

376

377 **ログアウト**

378 セッションの終了。

379

380 **LUAD**

381 「Liberty 対応ユーザーエージェント/デバイス」を参照。

382

383 **MEP**

384 MEP (Message Exchange Pattern: メッセージ交換パターン) は、SOAP ノード間で行われる
385 メッセージ交換のパターンを設定するテンプレートを指す。 ([SOAPv1.2]を参照)

386

387 **メタデータ**

388 アプリケーションまたは環境内で管理される他のデータに関する情報または記録を提供す
389 る定義データ。

390

391 **ミニマム最大値**

392 特定フィールドの最大値またはサイズとしてサポートされるべき最小値。たとえば、URL
393 のミニマム最大値は 256 文字であり、このフィールドに対応するすべてのシステムでは、
394 少なくとも 256 文字がサポートされなければならないが、それ以上の文字数をサポートす
395 ることができる。

396

397 **名前空間**

398 すべての名前が一意となるような名前の集合。

399

400 **ネットワークアイデンティティ**

401 主体者のすべての既存アカウントから構成される属性のグローバルセットの抽象概念。

402

403 **ノンス**

404 ノンスとは、同じ目的のために 1 度しか使用されない値を指す。ノンスには、タイムスタ
405 ンプ、Web ページの訪問カウンタ、ファイルの不正な再生や複製を制限または防止するた
406 めの特殊なマーカーなどがある。

407

408 **否認防止**

409 ある行為や情報に関わったことを主体者が法的に否認
410 できないようにすること。

411

412 **非推移的プロキシ機能**

413 信頼できる機関のポリシーに従い、別のエンティティのために行使できる機能。この機能
414 は、移転しない。

415

416 **オベイクハンドル**

417 特定のアイデンティティプロバイダとサービスプロバイダ間でしか意味をなさない文字列。

418

419 **PAOS**

420 SOAP のための逆方向の HTTP バインディング[SOAP v 1.2]。通常の HTTP バインディン
421 グとの主な相違点は、SOAP 要求が HTTP 応答にバインドされ、またその逆も同様にバイ
422 ンドされるという点である。

423

424 **パスワード**

425 認証情報として用いられる機密データ値 (通常は文字列)。 [RFC2828]

426

427 **PDP**

428 「ポリシー決定点」を参照。

429

430 **PEP**

431 「ポリシー実行点」を参照

432

433 **許可**

434 ユーザーがアクセスできるデータや使用できるメニューオプションおよびコマンドについ
435 て、各ユーザーに許諾された権限を指す。

436

437 **個人識別情報 (PII)**

438 ある人物を特定したり、その位置を捜し出したりするためのデータを指し、主に名前、住
439 所、電話番号、電子メールアドレス、銀行口座、または社会保障番号のようなその他の固
440 有の識別子から構成される。

441

442 **PII**

443 「個人識別情報」を参照。

444

445 **PIN (個人識別番号)**

446 [RFC2828]を参照。基本的には、パスワードと同じもの。一般に、サイズと内容は一部の文
447 字や数字に限定される。

448

449 **PKI**

450 「公開鍵基盤」を参照。

451

452 **ポリシー**

453 論理的に定義された、実行可能かつテスト可能な行動 (ビヘイバー) ルールのセット。

454

455 **ポリシー決定点 (PDP)**

456 該当するポリシーとリクエスト側のエンティティを表す情報に照らして決定リクエストを
457 評価し、認可決定を返すシステムエンティティ。

458

459 **ポリシー実行点 (PEP)**

460 決定リクエストを生成し、認可決定を実施することにより、アクセス制御を行うシステム
461 エンティティ。認可決定が PEP に送られる場合、ポリシー実行点がリクエストを生成する
462 必要はない。

463

464 **主体者**

465 主体者とは、連携アイデンティティを取得でき、決定を下すことができ、認証された行為
466 を自身のために行うことができるようなエンティティを指す。主体者には、個人ユーザー、
467 個人のグループ、企業、その他の法人、Liberty アーキテクチャの構成要素などがある。

468

469 **プライバシー**

470 主体の希望に応じた、ライフサイクル全体にわたる個人情報の適切な取り扱い。

471

472 **プロフィール**

473 あるアイデンティティで認証を受けるために必要な識別とデータ以外に、そのアイデンティティのために保管される広範な属性から構成されるデータ。少なくとも、このような属性のいくつか（住所、嗜好、カード番号など）は主体者によって提示される。

476

477 **専有データ**

478 ある組織に固有の保護データのこと。

479

480 **プロキシ**

481 他者を代理することを認定されたエンティティ。

482

483 **仮名**

484 所定の信頼当事者に対して主体者を確認するために、信頼当事者間でのみ有効となるようにアイデンティティプロバイダまたはサービスプロバイダによって割り当てられる任意の名前。

487

488 **公開鍵基盤 (PKI)**

489 主体者を含むコミュニティのために、非対称暗号アプリケーションにおいて証明書管理、アーカイブ管理、鍵管理、およびトークン管理の機能を果たす証明機関（また、オプションとして登録機関やその他の支援サーバおよびエージェント）のシステム。[RFC2828]

492

493 **公開鍵暗号方式**

494 2種類の鍵を使用する暗号方式。1つ目の鍵は必ず秘密に管理され、それと一意に対応する
495 2つ目の鍵は公開される。1つ目の鍵（秘密鍵）を使用して作成されたメッセージは、2つ
496 目の鍵（公開鍵）を使用して「確実な」方法で一意に確認できる。確認の確実性が非常に
497 高いため、このようなメッセージはデジタル署名と呼ばれる。最後に、公開鍵を使用して
498 作成されたメッセージは、対応する秘密鍵でしか復号化することができない。「デジタル署名」を参照。

500

501 **受信者**

502 メッセージを受信し、メッセージの最終的な処理者となるエンティティ。

503

504 **RELS**

505 「Rights Expression Languages (権利記述言語)」を参照。

506

507 **信頼当事者**

508 要求されたサービスを提供するかどうかの判断に際して要求メッセージと関連するアサーションを信用する、メッセージの受信者。

510

511 **Remote Procedure Call Protocol (RPC)**

512 プログラマーが明示的に動作を記述しなくても、あるホストで動作しているプログラムに別のホストで実行されるコードを生成させることが可能なプロトコル。

514

515 **否認**

516 義務や責任を拒絶したり、放棄したりすること。

517

518 **要求者**

519 処理を行うために受信者にメッセージを送信するエンティティ。通常、要求者はメッセー
520 ジの作成者でもある。

521

522 **リソース**

523 特定のアイデンティティ（1つまたは複数）にかかわるデータ、または、特定のアイデンテ
524 ィティや複数のアイデンティティから成るグループのために機能するサービスを指す。た
525 とえば、特定のアイデンティティに関する予定を含むカレンダーがその例である。

526

527 **リソースオフファリング**

528 リソースとサービスインスタンスの関連付け。

529

530 **Resource Owner Interaction (ROI)**

531 Resource Owner Interaction の略。Resource Owner Interaction サービスは、リソース所有者と
532 のやり取りを公開する Liberty アイデンティティサービスを指す。これにより、クライアン
533 ト（通常は WSP。WSP が ROI サービスに対しては WSC として機能する）はリソース所有
534 者に同意、認可決定などの問い合わせを行うことができる。

535

536 **Rights Expression Languages (REL:権利記述言語)**

537 使用方法の指示を伝えるための機械言語。REL の使用によって情報プロバイダは、情報交
538 換の前に意図したとおりに情報が使用されることを要求し、特定のトランザクション中に
539 やり取りされる情報について承認された使用方法を指示することができる。

540

541 **ROI**

542 「Resource Owner Interaction」を参照。

543

544 **RPC**

545 「Remote Procedure Call Protocol」を参照。

546

547 **SAML (Security Assertion Markup Language)**

548 セキュリティシステム間で認証および認可されたデータを交換するための XML 規格。
549 <http://www.oasis-open.org/committees/security/#documents> を参照。

550

551 **SAML オーソリティ**

552 SAML ドメインモデルにおいてアサーションを発行する抽象的なシステムエンティティ。
553 ([SAMLGloss]を参照)

554

555 **送信者**

556 最初の SOAP 送信者。送信者のアイデンティティが呼び出しアイデンティティと異なる場
557 合、その送信者はプロキシである。

558

559 **サービス**

560 特定のサービスまたは情報を提供するために指定されたエントリポイントの集まり。

561

562 **サービスインスタンス**

563 特定タイプのアイデンティティサービスの物理的なインスタンス作成を指す。サービスイ
564 ンスタンスとは、別個のプロトコルエンドポイントにおける実行中 Web サービスのことで
565 ある。

566

567 **サービスプロバイダ (SP)**

568 主体者にサービスや商品を提供するエンティティ。

569

570 **シングルサインオン (SSO)**

571 アイデンティティプロバイダ A との間に存在する認証セッションの証明を使用して、アイ
572 デンティティプロバイダ B との新たな認証セッションを作成できること。

573

574 **スマートカード**

575 1 つまたは複数の IC チップを内蔵し、コンピュータの CPU、メモリ、および入出力インタ
576 ーフェースの機能を果たす、耐タンパ性を持つクレジットカード大のデバイス。

577

578 **SOAP (Simple Object Access Protocol)**

579 Web で情報やリクエストを伝えるために用いられる XML エンベロープおよびデータエンコ
580 ーディング技術。一般的には、Web サービスで使用されるプロトコルと考えられる。実際
581 には、HTTP や FTP などのより低レベルの Web プロトコルに使用されるエンベロープのカ
582 プセル化形式のことである。[SOAP]を参照。

583

584 **SP**

585 「サービスプロバイダ」を参照。

586

587 **SSL (Secure Sockets Layer Protocol)**

588 コネクション型のエンドツーエンドの暗号を使用してクライアント (通常、Web ブラウザ)
589 とサーバ間のトラフィックにデータ守秘性サービスとデータ完全性サービスを提供し、オ
590 プションでクライアントとサーバ間のピアエンティティ認証を行うことも可能な (Netscape
591 Communications, Inc. によって開発された) インターネットプロトコル。Transport Layer
592 Security を参照。[RFC2828]

593

594 **SSO**

595 「シングルサインオン」を参照。

596

597 **TLS (Transport Layer Security Protocol)**

598 SSL プロトコルを発展させたもの。TLS プロトコルによって、インターネット経由の通信
599 のプライバシーを確保することができる。このプロトコルを使用すると、盗聴、改ざん、
600 またはメッセージ偽造を防止しながら、クライアントアプリケーションとサーバアプリケ
601 ーション間で通信することができる。[RFC2246]を参照。

602

603 **トラストサークル (trust circle)**

604 「トラストサークル (circle of trust)」を参照。

605

606 **信頼できるオーソリティ**

607 Liberty においては、アサーションの発行および保証を担う、信頼できる第三者機関 (TTP)
608 を指す。

609

610 **TTP**

611 信頼できる第三者機関 (Trusted third party の略)

612

613 **URI (Uniform Resource Identifier)**

614 抽象的または物理的リソースを識別するための短い文字列。[RFC2396]には、絶対および相
615 対形式を含むURIの一般構文と、それらの使用についてのガイドラインが定義されている。

616

617 **URL (Uniform Resource Locator)**

618 URIのサブセット。URLは、名前やその他の属性によってリソースを識別するのではなく、
619 直接的なアクセスメカニズムの表現 (たとえばネットワーク上の位置) を通じてリソース
620 を識別する。[RFC2396]

621

622 **URN (Uniform Resource Names)**

623 場所に依存しない永続的なリソース識別子として用いられ、(URNのプロパティを共有す
624 る) 他の名前空間を容易にURN空間に対応させるための名前。[RFC2141]を参照。

625

626 **ユーザーエージェント**

627 ユーザーのために Web コンテンツを読み込んで表示するソフトウェア。

628

629 **ユーザーインターフェース**

630 ユーザーエージェントによって提供されるコントロール (メニュー、ボタン、プロンプト
631 など) やメカニズム (選択やフォーカスなど)。

632

633 **VPN (Virtual Private Network)**

634 ネットワークを利用する各ユーザーのプライバシーと認証を確保しながら、インターネッ
635 ト経由で運用できるネットワーク。

636

637 **WAP (Wireless Application Protocol)**

638 無線デバイスを使用するモバイルユーザーが簡単に情報やサービスにアクセスし、これら
639 を利用できるようにするオープンな国際仕様。

640

641 **Web サービス**

642 インターネットプロトコルを使用し、プログラムに使用されるように設計されたサービス
643 を提供するサービス。

644

645 **Web サービスコンシューマ (WSC)**

646 Web サービスを利用してデータにアクセスするエンティティ。

647

648 **Web サービスプロバイダ (WSP)**

649 Web サービスを通じてデータを提供するエンティティ。

650

651 **WML (Wireless Markup Language)**

652 XML に基づくマークアップ言語であり、携帯電話やポケットベルなどの狭帯域デバイスで
653 コンテンツやユーザーインターフェースを指定するのに用いられる。

654

655 **WSC**

656 「Web サービスコンシューマ」を参照。

657

658 **WSDL (Web Services Description Language)**

659 Web サービスのインターフェースを記述する一般的な技術。http://www.w3.org/TR/wsdl/を参
660 照。

661

662 **WSP**

663 「Web サービスプロバイダ」を参照。

664

665 **XML (eXtensible Markup Language)**

666 情報や文書を Web で交換できるようにエンコードするための W3C 技術。[XML],
667 [XMLCanon], [XMLDsig], [xmlenc-core], [Schema1], [Schema2]を参照。

668

669 **XML アドレッシング**

670 (XML コーディングを使用して、) 別のサービスにあるデータを検索して参照する方法。

671

672 **ZIC (Zero Install Client)**

673 Liberty 専用の拡張機能を有しない、一般的に使用される HTTP ベースのユーザーエージェ
674 ント。たとえば、標準的な Web ブラウザは ZIC である。

675 **参考文献**

676 **標準**

- 677 [LibertyBindProf] Kemp, John , Wason, Tom, eds. "Liberty ID-FF Bindings and
678 Profiles Specification," Version 1.2, Liberty Alliance Project (12 November
679 2003). <http://www.projectliberty/specs>
- 680 [LibertyMetadata] Davis, Peter, eds. "Liberty Metadata Description and Discovery
681 Specification," Version 1.0, Liberty Alliance Project (12 November 2003).
682 <http://www.projectliberty/specs>
- 683 [LibertyProtSchema] , Cantor, Scott, Kemp, John, eds. "Liberty ID-FF Protocols and
684 Schema Specification, " Version 1.2, Liberty Alliance Project (12 November
685 2003). <http://www.projectliberty/specs>
- 686 [RFC1510] Kohl, J., Neuman, , C., eds. (September 1993). "The Kerberos Network
687 Authentication Service (V5)," RFC 1510, Internet Engineering Task Force
688 <http://www.rfc-editor.org/rfc/rfc1510.txt>
- 689 [RFC2119] Bradner, S., eds. "Key words for use in RFCs to Indicate Requirement
690 Levels," RFC 2119, The Internet Engineering Task Force (March 1997).
691 <ftp://ftp.rfc-editor.org/in-notes/rfc2119.txt>
- 692 [RFC2141] Moats, R., eds. (May 1997). "URN Syntax," RFC 2141, Internet
693 Engineering Task Force <http://www.rfc-editor.org/rfc/rfc2141.txt> [20 December
694 2002]
- 695 [RFC2246] Dierks, T., Allen, C., , , , eds. (January 1999). "The TLS Protocol,"
696 Version 1.0 RFC 2246, Internet Engineering Task Force
697 <http://www.rfc-editor.org/rfc/rfc2246.txt>> [20 December 2002].
- 698 [RFC2396] Berners-Lee, T., Fielding, R., Masinter, L., eds. (August 1998). "Uniform
699 Resource Identifiers (URI): Generic Syntax," RFC 2396, The Internet
700 Engineering Task Force <http://www.rfc-editor.org/rfc/rfc2396.txt> [18 December
701 2002].
- 702 [RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P.,
703 Berners-Lee, T., eds. (June 1999). "Hypertext Transfer Protocol – HTTP/1.1,"
704 RFC 2616, The Internet Engineering Task Force
705 <http://www.rfc-editor.org/rfc/rfc2616.txt> [18 December 2002].
- 706 [RFC2828] Shirey, R., eds. (May 2000). "Internet Security Glossary," RFC 2828.,
707 Internet Engineering Task Force <http://www.rfc-editor.org/rfc/rfc2828.txt> [20
708 December 2002].
- 709 [RFC3280] Housley, R., eds. (April 2002). "Internet X.509 Public Key Infrastructure
710 Certificate and Certifi- cate Revocation List (CRL) Profile," RFC 3280, The
711 Internet Engineering Task Force <http://www.rfc-editor.org/rfc/rfc3280.txt>
- 712 [SAMLBind11] Maler, E., Mishra, P., Philpott, R., eds. (27 May 2003). "Bindings and
713 Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1,"
714 OASIS Committee Specification, ver- sion 1.1, Organization for the
715 Advancement of Structured Information Standards
716 http://www.oasis-open.org/committees/documents.php?wg_abbrev=security
- 717 [SAMLCore11] Maler, E., Mishra, P., Philpott, R., eds. (27 May 2003). "Assertions and

- 718 Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1,"
719 OASIS Committee Specification, version 1.1, Organization for the
720 Advancement of Structured Information Standards
721 http://www.oasis-open.org/committees/documents.php?wg_abbrev=security
722 [SAMLGloss] Hodges, J., Maler, E., eds. (05 November 2002). "Glossary for the
723 OASIS Security Assertion Markup Language (SAML)," Version 1.0, OASIS
724 Standard, Organization for the Advancement of Structured Information
725 Standards <http://www.oasis-open.org/committees/security/#documents>
726 [Schema1] Thompson, H.S., Beech, D., Maloney, M., Mendleson, N., eds. (May 2002).
727 "XML Schema Part 1: Structures," Recommendation, World Wide Web
728 Consortium <http://www.w3.org/TR/xmlschema-1/>
729 [Schema2] Biron, P.V., Malhotra, A., eds. (May 2002). "XML Schema Part 2:
730 Datatypes," Recommendation, World Wide Web Consortium
731 <http://www.w3.org/TR/xmlschema-2/>
732 [SOAPv1.2] "SOAP Version 1.2 Part 1: Messaging Framework," Gudgin, Martin,
733 Hadley, Marc, Mendelsohn, Noah, Moreau, Jean-Jacques, Nielsen, Henrik
734 Frystyk, eds. World Wide Web Consortium W3C Proposed Recommendation
735 (07 May 2003). <http://www.w3.org/TR/2003/PR-soap12-part1-20030507/>
736 [<http://www.w3.org/TR/2003/PR-soap12-part1-20030507/>]
737 [WSDLv1.1] "Web Services Description Language (WSDL) 1.1," Christensen, Erik,
738 Curbera, Francisco, Meredith, Greg, Weerawarana, Sanjiva, eds. World Wide
739 Web Consortium W3C Note (15 March 2001).
740 <http://www.w3.org/TR/2001/NOTE-wsdl-20010315>
741 [<http://www.w3.org/TR/2001/NOTE-wsdl-20010315>]
742 [XML] Bray, T., Paoli, J., Sperberg-McQueen, C.M., Maler, Eve, eds. (Oct 2000).
743 "Extensible Markup Language (XML) 1.0 (Second Edition)," Recommendation,
744 World Wide Web Consortium <http://www.w3.org/TR/2000/REC-xml-20001006>
745 [XMLDsig] Eastlake, D., Reagle, J., Solo, D., eds. (12 Feb 20002). "XML-Signature
746 Syntax and Processing," Recommendation, World Wide Web Consortium
747 <http://www.w3.org/TR/xmlsig-core>
748 [XMLCanon] Boyer, J., Eastlake, D., Reagle, J., eds. (18 July 2002). "Exclusive XML
749 Canonicalization," Recommendation, World Wide Web Consortium
750 <http://www.w3.org/TR/xml-exc-c14n>
751 [xmlesc-core] Eastlake, Donald, Reagle, Joseph, eds. (December 2002). "XML
752 Encryption Syntax and Processing," W3C Recommendation, World Wide Web
753 Consortium <http://www.w3.org/TR/xmlesc-core/>
754