

LIBERTY ALLIANCE PROJECT ホワイトペーパー

Liberty Alliance と WS-Federation : 比較概要

2003 年 10 月 14 日

エグゼクティブサマリー

このホワイトペーパーは、アイデンティティの基本的な理解や、Liberty Alliance 仕様と提案されている WS-Federation 技術案とを対比した高度な概要を必要とする企業読者と技術戦略の決定者を対象としています。文書中の WS-Federation の分析には、2003 年 9 月現在で公開されている情報が基準として使用されていることに注意してください。このホワイトペーパーでは、以下の事項を取り扱います。

- なぜ業務プロセスや Web サービスは根本的にアイデンティティに左右されるのか、なぜ連携アイデンティティ管理上の問題や可能性に対応する上で、一連のオープンな仕様やビジネスガイドラインが最適なのか。
- 連携アイデンティティ管理に向けた Liberty Alliance Project の業務重視のアプローチ、およびそのアプローチや製品を支える推進力および業界のサポート。
- Liberty Alliance Project と WS-Federation 技術ホワイトペーパーで提案されている事項との共通要素。
- Liberty Alliance Project 仕様と、WS-Federation を含む第三者からの新たな提案との融合の呼びかけ。

アイデンティティ：高い価値の関係を保つための中核事項

アイデンティティは、顧客やビジネスパートナーとの関係から、貴重なデータや情報にアクセスする従業員や機器の必要性の把握に至るまで、価値の高いビジネス関係の中核をなしています。アイデンティティには、価値の高い Web サービスを開発、展開するために欠かせない属性と特性が含まれます。企業は、アイデンティティを管理するにあたり、さまざまな認証および認可メカニズムの技術的影響に加え、アイデンティティとデータの管理にかかわる現行、新規のビジネスおよびポリシーの問題を考慮しなければなりません。アイデンティティを効果的に管理することにより、コストを削減し、セキュリティを強化し、拡大し続けるアイデンティティ盗難の脅威を防止し、新たなサービス、収益モデル、およびビジネス機会を実現することができます。

取引やデータがオンラインに移行し続けるに従って、「オフライン」世界で一般化しているアイデンティティ関係もオンライン世界に移行しなければなりません。その場合、データや金融取引のためのより強力な認証の必要性や、個人、顧客、または従業員のデータを管理するための新しい法律や規制を順守する必要性などの新たな問題が生じます。顧客サービスと顧客満足は、今後も重要です。そのため主要企業は、その構成要素（従業員、ビジネスパートナー、および特に消費者）が複数のユーザー名とパスワードの組み合わせという負担なしに、できる限り簡単に対象のオンラインサービスにアクセスできるようなシングルサインオン（SSO）システムを模索しています。モバイル機器や端末からのアクセスなどの一部のシナリオでは、このような負担は、多くのユーザーが利用する上で大きな障害となります。

多くの企業は、シングルサインオンの概念を自社と社内部門の Web サイトだけでなく、パートナーの Web サイトにも拡張しつつあります。これは、連携アイデンティティ管理の好例です。このようなシステムを導入する際には、関連するアイデンティティデータをどこでどのようにして保管、共有するか、またデータ交換や商取引にかかわる法律上、規制上の問題にどのように対処するかを考慮しなければなりません。

最も重要な点は、このような構想を世界規模で簡単に導入するには、さまざまな業種の企業が合意する一連の共通した技術仕様と事業慣行が必要となることです。そのような基準がなければ、連携アイデンティティサービスを開発、展開する際に、コスト増大や複雑化の障壁が生じてネットワークの効果が限定され、幅広い相互運用が妨げられます。

このようなオープンスタンダードの必要性に対応するため、2001 年 9 月に Liberty Alliance が設立されました。Liberty Alliance は、連携アイデンティティサービスのため

の綿密に構成された強固な仕様を発表してきました。最近、技術ベンダー5社（IBM、Microsoft、RSA、VeriSign、および BEA）は、この分野における特定の問題に対処する別の方法を概説した「Web Services Federation Language（WS-Federation）」という技術ホワイトペーパーを発表しました。この仕様案の情報から判断して、Liberty Alliance Project の仕様と重複する可能性があることは明らかです。この重複については、このホワイトペーパーの後半で詳しく説明します。

業界標準に向けた業務重視の Liberty のアプローチ

Liberty Alliance には、技術、金融サービス、通信、モバイルサービス、政府、製造を含む多くの産業セクターが参加しています。Liberty Alliance Project は、アイデンティティと連携アイデンティティ管理にかかわる技術、ビジネス、およびポリシーの問題に意欲的に取り組んでいる唯一の世界的組織です。

「[連携アイデンティティの] ビジネスの問題は、技術的な問題よりも複雑である」
-Burton Group、「ID の連携 - その理由と時期（Federating ID - Why and When）」、
2003年7月

Liberty では、連携アイデンティティ管理の標準的な手法の策定に着手した時点で、技術がこの課題の一部に過ぎないことを認識していました。そのため Liberty は、市場要求文書（MRD：Market Requirement Document）に記載されたビジネスの利用事例を各仕様の根拠とし、ビジネスの問題を開発と成果の中核に据えました。このような市場要求には、ビジネス、ポリシー、および規制のニーズを満たすアイデンティティ管理ソリューション向け技術の用途が反映されています。Alliance は、これらの要求の基準から作業を開始し、W3C や OASIS などの他のオープンな業界団体からの技術を活用しようと取り組んでいます。そのため、Alliance の技術仕様では、そのような団体による SAML、WS-Security、SOAP、XML などの成果や作業を再利用し、基盤にしています。

一般に、ビジネス関係を構築する際には、何らかの形式の契約上の合意によって、その関係が支えられます。Alliance ではこの点を念頭に置き、企業が連携ネットワークアイデンティティの利用に依存したビジネス関係に参加する際に必要な契約見直しの量を減らし、そのような契約上の合意の参考となるビジネスガイドラインを策定しました。最初の一連のガイドラインでは、責任、リスク、相互信頼、準拠などの問題に重点を置きました。今後のビジネスガイドラインでは、より詳細に特定の業界や地域に焦点を当てる予定です。

Liberty Alliance の採用、推進力、および実証済みの相互運用性

Liberty Alliance は当初から、検証、実証済みのオープンな標準を目指して取り組んでいます。綿密に構成された Liberty ID-FF(アイデンティティ連携フレームワーク)仕様は、複数ベンダーによる 18 か月間の広範な協力、パブリックレビュー、および多くの相互運用試験を経て、2002 年 7 月に発表されました。同様に、Liberty Alliance の作業の第 2 フェーズと共に発表された ID-WSF(アイデンティティ Web サービスフレームワーク)は、ベンダー界と主要なエンドユーザー企業を代表する参加企業による 1 年以上の活発な取り組みを反映しています。

Liberty Alliance の包括的かつ厳密なアプローチは、業界全体の充実したサポートと採用を促しました。2003 年 7 月現在、企業が連携アイデンティティ管理に向けて Liberty プロトコルを導入できるような製品とサービスを発表している技術ベンダーは、20 社以上に上ります。General Motors や American Express などの多くの主要企業は、内部で Liberty の実装を開始しました。2003 年末までに、いくつかの新たな製品や内部導入の完了および出荷が予定されており、この仕様の世界的なサポートが継続的に拡大していることが窺えます。

オープンスタンダードの開発に向けた進行中の取り組み

Liberty Alliance は、連携アイデンティティに向けた包括的な一連の標準を策定、展開するという使命を反映し、補完的な取り組みを行っている組織と協力しています。たとえば Alliance は、(Liberty 1.1 仕様の一部である)アイデンティティ連携フレームワークプロトコルを SAML 2.0 の検討材料として OASIS に提供しました。さらに、Liberty は、Open Mobile Alliance (OMA)、Open Group、OASIS などの業界標準に取り組む組織との話し合いに参加しています。

WS-Federation 技術ホワイトペーパーの発表を受け、Alliance では、重複箇所と見直し箇所の評価を行い、考えられる融合点を見極めるために、分析を実施しました。

明らかに、融合の可能性は存在します。先述したとおり、Liberty は、他のオープンスタンダード組織から提供される技術の再利用を模索する技術的作業に関して、強力なポリシーを採用しています。Liberty Alliance の参加企業は、この業界内の他の企業が同様のポリシーを採用するよう呼びかけています。そうすることで、業界やアイデンティティベ

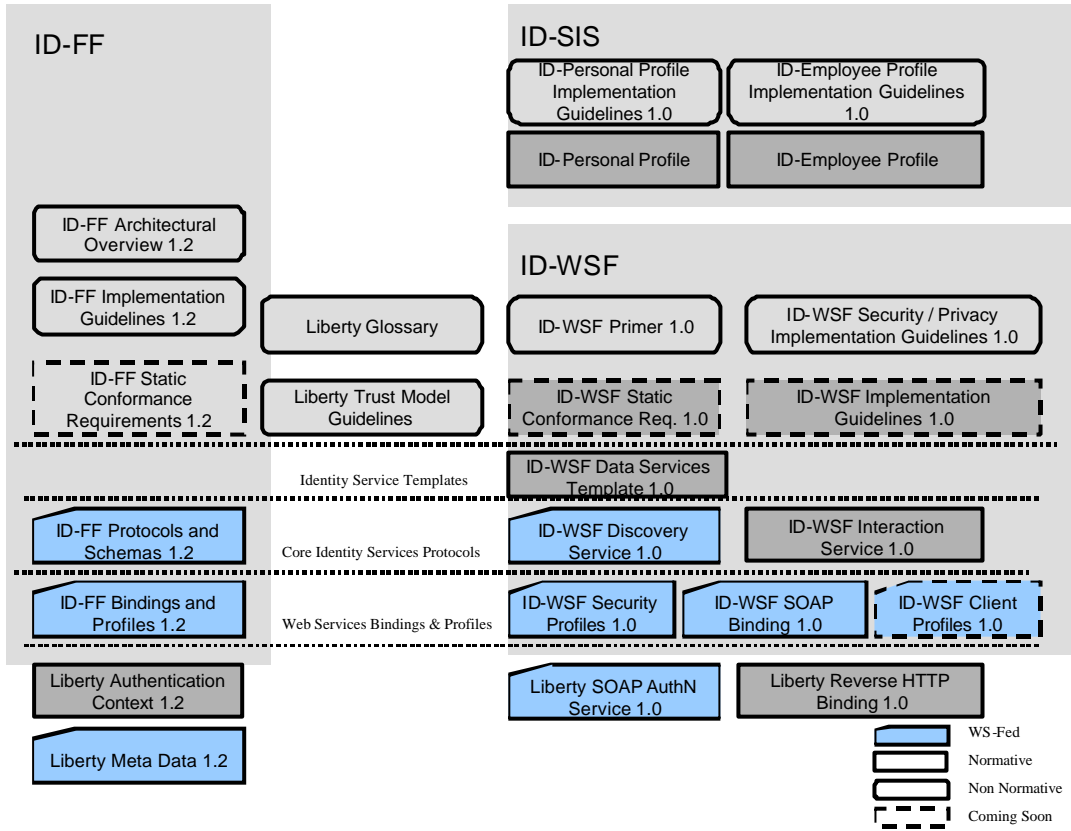
スの Web サービスの展開を阻害するような相反する取り組みを抑制することができます。

Liberty Alliance 仕様と WS-Federation 仕様の比較分析

WS-Federation ホワイトペーパーの調査によると、より新しいこの取り組みでは、連携アイデンティティサービスを導入する別の方法として、全部とは言わないまでも一部 Liberty Alliance 仕様を模倣しているように見受けられます。

以下は、Liberty 仕様のコンポーネントの詳細図です。強調表示（左上角が欠けた青いボックス）は、Liberty アーキテクチャのコンポーネントのうち、技術ホワイトペーパーに記載されたように WS-Federation でも何らかの対応が予定されているものです。これらの重複する技術コンポーネントの詳細な比較については、この文書末に表形式で示します。WS-Federation は依然として開発の初期段階にあり、発展途上のため、サポートされるアイデンティティ情報の性質はまだはっきりしていません。このことは、この2つの仕様の厳密な範囲を比較する上で、評価に関わる問題となります。

Liberty Alliance Project のフェーズ 2 仕様案



プライバシー

アイデンティティのプライバシーを尊重することは Liberty Alliance の基本方針であり、すべての種類のビジネスおよびアイデンティティ実装(すなわち B2E、B2B、および B2C)の重点です。Liberty Alliance では、政府、消費者、およびプライバシー保護団体のリーダーと積極的に協調する公共ポリシー専門家グループ (Public Policy Expert Group) を設置しています。現行および新規のプライバシー問題および規制に関するこの進行中の作業は、このような問題に敏感に反応する仕様やビジネスガイドラインの策定にプラスの影響を与えています。

Liberty の ID-WSF 仕様の目的は、属性情報に関するアクセス管理ポリシーを推奨し、公開された属性に関する用途指示子の提示を許可することによって、プライバシーを確保することです。この技術により、Liberty 仕様のユーザーは、個人アイデンティティ情報を交換せずに、選択を行った顧客のアカウントを連携またはリンクさせることができます。Liberty 仕様をサポートするアイデンティティの実装においてユーザーがアカウントを連携させる場合、仮名リンクの概念に沿って、その関係に固有のランダムな識別子が生成され、グローバルな識別子を根本的に回避すると共にそのプロセスに対するセキュリティの階層が追加されます。Liberty Alliance は、この「仮名リンク」アプローチに関して、2002 年 10 月の Digital ID World でデジタルアイデンティティ業界賞 (Digital Identity Industry Award) を授与されました。

現時点で、WS-Federation の提案では、(仮名の暗号化などの) プライバシーのメカニズムが Liberty Alliance 仕様ほど規定されていません。WS-Federation は、個人識別情報 (PII) に対するオプションのアクセス管理について WS-Policy (そしておそらく、詳細不明の WS-Privacy) に従っています。WS-Federation では、(オプションの) プライバシー保護識別子の管理に仮名サービス (Pseudonym Service) が採用されています。

仕様の共通点と相違点

仕様レベルで見ると、Liberty の連携フレームワーク (ID-FF、ID-WSF、および ID-SIS) と WS-Federation は、以下のようにいくつかの中核的な原則やメカニズムを共有していません。

1. 基本的なメッセージングプロトコルのプロファイルによるブラウザクライアントとスマートクライアントの区別 (ただし、これらのクライアントの性質はおそらく異なる)
2. セキュリティトークンの発行による信頼の仲介

3. プライバシーが管理された属性の共有

4. 連携サインアウトによる基本的なセッション管理

ただし、これらの原則の適用方法は、主にアプローチや基礎となる技術で異なります。以下の表に、これらの相違点を詳しく示します。

	特徴/機能	Liberty Alliance Project	WS-Federation
同様の技術的アプローチを採用する重複箇所	クライアントプロファイル	ブラウザクライアントおよびスマートクライアントの両方について、クライアントプロファイルを規定	ブラウザクライアントおよびスマートクライアントの両方について、クライアントプロファイルを規定
	SSO 管理の流れ	SSO 管理の流れでは、フロントおよびバックチャネルの両方のメカニズムを規定	SSO 管理の流れでは、フロントチャネルメカニズムを規定し、強く推奨するが、「ポイントベース」のバックチャネルメカニズムの使用には反対

	特徴/機能	Liberty Alliance Project	WS-Federation +
異なる技術的アプローチを採用する重複箇所	アカウント連携	アイデンティティのマッピングによるアカウント連携は、(主要なプライバシー機能である)オペイク識別子によって実現	アイデンティティのマッピングによるアカウント連携は、仮名サービスによって実現
	プライバシー	プライバシー管理は仕様に記載されている(アクセス管理ポリシー、用途指示子、および仮名を推奨)	アクセス管理に関して WS-Policy (そしておそらく WS-Privacy) に従うことによって、オプションでプライバシーをサポート
	セキュリティトークン	プロバイダ間での認証および認可セキュリティトークンの通知に関しては、SAML アセッションを拡張	セキュリティトークンの通知に関しては、WS-Security の X509v3 および Kerberos プロファイルがベース

	ビジネスおよびポリシーの問題	ビジネスガイドラインと認証コンテキストを通じた信頼の確立に関連するビジネスの問題に対応	現時点では、ビジネスの信頼問題には対処していない
	基礎となる技術	基礎となる技術は、SAMLをベースに拡張し、トランスポートおよびメッセージのセキュリティについてはSSLとWS-Securityに依存	基礎となる技術は、WS-Trust、WS-Policy、およびWS-Metadataをベースとし、トランスポートおよびメッセージのセキュリティについてはSSLとWS-Securityに依存

	特徴/機能	Liberty Alliance Project	WS-Federation
LibertyとWS-Federationの大まかな相違点	アプローチ	ベンダー、エンドユーザー、および非営利団体を含むオープンスタンダード組織が策定	Microsoft、IBM、VeriSign、BEA、およびRSA Securityが策定
	範囲	連携アイデンティティサービスにかかわる技術、ビジネス、およびポリシーの問題を全般的に取り扱う	連携アイデンティティサービスに関する技術的仕様が対象
	成熟度	2年間にわたって共同で策定された成熟した仕様であり、発表の時点でLiberty仕様をサポートする実装は2003年10月以上	草案の初期段階であり、現時点では利用可能なベンダー実装はなし
	仕様へのパブリックレビュー/アクセス	仕様については、多くのベンダーとエンドユーザーによる広範なパブリックレビューと多くの相互運用試験を実施	パブリックレビューや評価のメカニズムはなし

	実装コスト	製品やサービスへの仕様の実装は無料 http://www.projectliberty.org/specs/ipr.html	仕様の閲覧は無料、実装および配布コストは不明(ホワイトペーパーには次のように記載:「作成者は、明示的または黙示的を問わず、特許権を含めて、所有または管理するいかなる知的所有権のライセンスも許可しません」 http://www-106.ibm.com/development/webservices/library/ws-fed/
--	-------	--	--

結論

2年を経た Liberty Alliance Project は、連携アイデンティティ管理に向けたオープンな業界標準の必要性に取り組みます。Liberty は、WS-Federation を提案している技術ベンダーの関心と取り組みを認識し、Liberty Alliance 仕様の今後の発展に対する作成者からの情報を歓迎します。Liberty は、これらのベンダーが、160 を超える Liberty Alliance の参加組織によってすでに達成された大きな進展を考慮し、融合ソリューションの総合的なメリット(オープンな業界標準、規模の経済、製品開発の短縮化、使用する技術に左右されない同じユーザー体験、採用の迅速化など)を評価するよう期待します。

このような業界全体のメリットを実現するため、Liberty Alliance は、融合に向けた道を検討するための公開ワークショップを呼びかけます。Liberty Alliance は、このようなミーティングの推進、共同主催、および参加の意思があり、参加企業のためにできる限り早期の開催を望んでいます。

付録：Liberty Alliance と WS-Federation 仕様の詳細な技術分析：

分類	コンポーネント	Liberty	WS-Federation +
リンク	アカウントのリンク	ID 連携フレームワーク	あり。仮名サービスのセットメッセージによる
シングルサインオン	認証リクエスト	SAML リクエスト	WS-Trust トークン発行リクエスト
	認証レスポンス	SAML レスポンス	WS-Trust トークン発行レスポンス
	アサーション	SAML 認証ステートメント	任意のトークン
	認証の詳細	認証コンテキストはリクエストとレスポンスに規定される場合あり	
	プロファイル	ブラウザアーティファクト、フォーム POST、LEC	バリエーションのある Passive および Active プロファイル
セッション	IDP によって開始されるシングルログアウト	あり	あり
	SP によって開始されるシングルログアウト	あり	あり
	セッションのクレデンシャル		WS-SecureConversation
プライバシー	オペイク識別子	あり	オプション（オペイクではない永続的な識別子が使用される場合あり）
	管理	NameRegistration プロトコル	あり。仮名サービスのセットメッセージによる
	公開される属性に関するポリシー	用途指示子	
	暗号化された識別子および URI	あり	
認可	認可リクエスト	黙示的	WS-Trust

分類	コンポーネント	Liberty	WS-Federation +
	認可レスポンス	黙示的	WS-Trust
	属性（ロール）		あり
信頼	法律上の合意	認証コンテキストから参照可能	
	ビジネス上の合意	認証コンテキストから参照可能	
	提携	あり	
	イントロダクション	下記を参照	
	トークンの交換/マッピング		WS-Trust
セキュリティ	メッセージのセキュリティ	XML 署名/XML 暗号化 /WS-Securityの保護されたメッセージ	XML 署名/XML 暗号化 /WS-Securityの保護されたメッセージ
メタデータ	発行	DNS および既知の場所。UDDI ディレクトリで発行される場合あり	
	取り出し	DNS および既知の場所	
	スキーマ	ID-WSF メタデータ	WS-MetadataExchange
ディスカバリー	主体者の IDP	共通ドメインクッキー	
	発行	ID-WSF DiscoveryLookupUpdate	UDDI
	照会	ID-WSF DiscoveryLookupRequest	UDDI
	セキュリティポリシー		WS-SecurityPolicy
イントロダクション	信頼の仲介	あり	WS-Trust
	主体者の連携の通知	あり	
	信頼の終了の通知	あり	
情報の共有	アクセス	あり。アイデンティティサービス	属性サービス
	保管		UDDI

分類	コンポーネント	Liberty	WS-Federation +
	プライバシーポリシー	プライバシーポリシー記述言語	WS-Privacy か？
	データ操作	WSF データサービステンプレート	WS-Federation ではなし。Net My Services HSDL では可能性あり
	データのインターフェース	ID 個人プロフィール	WS-Federation ではなし。Net My Services では可能性ありか？
	仲介	あり	
ユーザーのインタラクション	ユーザーの承諾	ID-WSF インタラクションサービス	
	連携の終了	あり	