

パーソナルサイズのマルチエージェント統合環境 airWeb の開発

Development of Personal-sized Multi-Agent Integrated Platform: airWeb

飯塚 豊¹⁾ 富樫 良成²⁾ 加地 正典³⁾
Yutaka IIZUKA Yoshishige TOGASHI Masanori KAJI

- 1) 株式会社エアフロント (〒158-0096 東京都世田谷区玉川台 2 - 2 - 1 ヤマウラビル 2 F
E-mail: iizuka@airfront.co.jp)
- 2) 株式会社エアフロント (〒158-0096 東京都世田谷区玉川台 2 - 2 - 1 ヤマウラビル 2 F
E-mail: togashi@airfront.co.jp)
- 3) 株式会社エアフロント (〒158-0096 東京都世田谷区玉川台 2 - 2 - 1 ヤマウラビル 2 F
E-mail: kaji@airfront.co.jp)

ABSTRACT. This describes the development of Personal-sized Multi-Agent Integrated Platform named airWeb. airWeb is a Web-based information aggregation software and has functionality to execute multi-agent. The platform also includes Agent Development Kit, Agent Distribution Server and practical agents. In this project, we have developed secured agent distribution functionality with new Agent Distribution Server.

1. 背景

Web が本格的に普及し始めてから 5 年以上経過し、インターネット上に蓄えられる情報は現在も加速度的に増えている。しかし、新しいサイトの発見や、決まったサイトの定点観測、コミュニティサイトへの参加、必要な情報の保存など、ほとんどのユーザは手作業で行っているのが実情である。一部自動処理（ロボットや購読機能など）が行われているケースもあるが、たくわえる情報のフォーマットがまちまちであり、操作性も統一されていない。とくに個人の環境の場合、情報の保管場所が一元化されていないことによる情報の再利用が困難となっているケースも多い。

これは HTML が論理構造ではなく主としてデザインに重点を置いて記述するために使われていること、すなわち Web のデータが正規化されていない点に負う部分が多い。HTML は、その簡易な書き方とブラウザ上での表現力の高さから広く利用されてきたが、文書管理という本来の SGML の持っていた意味はほとんど失われてしまった。XML などのドキュメントの論理構造と表現を分離する手段や、WSDL に代表される Web サービスのような新しい形態の情報流通手段は現れてきているが、主流は依然として HTML と HTTP サーバにとどまっている。

このような状況を踏まえ、必要な情報を取得する手続きの複雑化、一貫性のない情報の氾濫を解決する手段のひとつとして、エージェント技術が注目されている。エージェント技術とは、コンピュータ上に実現された人間の情報処理を代行する機構の総称である。エージェントは範囲が広い用語であるが、このプロジェクトでは、特にインターネットエージェント（インターネット上での情報検索・統合・配信の支援）を中心として取り扱う。

2. 目的

本プロジェクトは、同名の平成 12 年度実施プロジェクト成果を受け、セキュリティ機能の向上や、サーバの大幅な強化、キラーエージェントの開発、対応プロトコルの拡大、携帯端末との連携、ユーザインタフェースの一層の向上など、エージェント環境をより広いユーザに知って使ってもらい、競争力のあるプラットフォームに育てあげることを目的としている。

3. 開発内容

以下に、開発した機能の中から特徴的な成果について述べる。

(1) airWeb 本体の機能強化

パブリックベータ版として公開した airWeb について、様々な反応を得ることができた。その中から、さらにエージェントを強力に信頼できるものにするため、次の機能アップを実施した。

a) セキュリティ機能の向上

パッケージ自体をアップロードしてもらい、スタッフのチェックを通して承認し、配布サーバを証明する署名を付与する方式を新たに導入した。新しい airWeb では、ユーザが設定するセキュリティレベルにより、署名の無いパッケージをインストールしないよう制限することも可能となった。

この署名は公開鍵暗号方式をベースにした独自の署名方式であり、鍵変更や複数の配布サーバ（署名を行う認証者）への対応も考慮された設計となっている。また、これに合わせて新しく設計したパッケージ形式は、開発者向けにも公開し、エージェント開発のテストや新たな付加情報を用いた応用事例の試作にも活用されるよう展開していく予定である。

b) ユーザビリティの向上

airWeb をパブリックベータとして配布開始し、これまでに多くのユーザに利用されさまざまなフィードバックを得てきた。この中から、特に注力すべきいくつかの改善を含む非常に多くの改修を加えた。

(ア) ログブラウザ機能の向上

airWeb には、汎用的に利用できる高機能なログデータベースが搭載されており、フロントエンドとなる情報ブラウザ（ログブラウザ）もまた収集した情報を最大限効果的に表示できるように任意にエージェントとして作成できるようにになっている。しかしブラウザを一から組み上げるのは大変な作業であり、一般的な機能を搭載したタイトルリストを提供することで、データベースのアクセスやタイトルリストの表示を省力化できるようにしている。このタイトルリストに、共通で追加して利用価値のある機能を追加して高機能化した。具体的には、以下のような機能群である。

- ・ 未読・既読の任意設定、チェックマーク操作
- ・ 検索と結果のハイライト表示
- ・ 高度なツリー表示操作
- ・ 情報の新しさによる背景色グラデーション
- ・ 記事のコピー、削除
- ・ リストカラムの任意入れ替え、調整状態の保存復元

(イ) キャビネットの操作性向上

キャビネットそのものの概念がわかりにくいという声も寄せられた背景に、追加する方法が限定され、固定の場所にしかアイテムが表示されず、フォルダやアイテムの作成もユーザが自由にできないという使いにくさがあった。

キャビネットはユーザが自分の好きなように情報を整理し配置する場所という位置づけを明確にし、フォルダの作成やアイテムの移動が自由に行えるよう改良を行った。また、アイテムを追加する際も、キャビネット上で指定した位置にアイテムが作成されるよう、「アイテムの追加」処理の内部インターフェースを改良した。「アイテムの追加」のためのエージェントを作成する必要があったのもエージェント開発の敷居を高くしていたので、合わせて簡易な追加方法を利用できるようにした。

(ウ) タブバーの導入

airWeb では、収集した情報毎に、その情報を表示するのに最適なブラウザが実行されるようになっていた。しかし複数の情報を順次開いていくとブラウザが多数開いている状態になり、ウィンドウの選択が思うようにできなくなっていた。ショートカットキーによるウィンドウの順次選択といった一般的な操作方法のサポートに加え、今回、開かれているウィンドウをタブ形式で表示する、メインウィンドウの機能を追加した。これにより、開いているウィンドウが常時一覧でき、切り替えも1クリックで行えるようになり利便性が向上した。



(エ) 予約機能のインターフェース整備

airWeb には、巡回と予約の2通りの自動処理の機能がある。巡回は、設定された要件で毎回処理を実行するのに対し、予約は必要に応じて発生するインターネットの利用を手助けしてくれるものである。典型的な事例として掲示板が挙げられる。通常、巡回により掲示板から新規に投稿されたメッセージを読み取ってきて、ブラウザでその情報を閲覧する。閲覧している記事に対してコメントを書いたり、新規に投稿を作成したりする場合は、投稿のための編集エージェントが起動して投稿を作成し、その実際の処理は予約として保存され、次回インターネットに接続した際自動的に送信することができるようになるものである。

この予約に関しては、仕組みの説明がほとんどないことに加え、それらを確認する手段もなければ、エージェントによって予約処理を実行した際の後処理の方法もまちまちであったため、たとえば投稿に失敗した際の下書きがどうなるのかといった事象がわかりにくいものであった。

本開発において、airWeb 本体で保留状態の管理を明確に定義し、必要なAPIの整備を行った。さらに、予約・保留・実行済みのユーザが作成した情報も管理確認できるエージェントを標準で用意した。

また、エージェント開発を増強するために、Air VM の機能アップおよび ASDK (AirWeb Software Development Kit) の改良を行っている。高機能なエージェントをより効率よく開発できる機能が多数サポートされている。あわせて、エージェント開発の標準パターンを既定し、必要な機能のエージェントだけを作ればよいように、汎用的で高機能な標準エージェントとインターフェースを整理し、標準化を行った。今後開発者コミュニティを通して随時公開していく予定である。

(2) サーバ機能の強化

パッケージファイルに署名を付加、不正アクセスによるパッケージファイルの改ざん、ウイルスなどの被害によるパッケージファイルの破損などを検出し、不正なパッケージのインストールを防止することが可能になった結果、安全性が向上した。

また、パッケージファイルに署名を付加するため、新しいパッケージファイルの形式を採用し、パッケージ情報、デベロッパ情報などをパッケージファイル自体に埋め込む事が可能になった。これによりディスクからパッケージをインストールするなど、ネットワークのエージェント情報サーバに依存しないパッケージファイルの流通が可能になった。新しいパッケージファイルの書式は拡張可能であり、今後様々な情報をパッケージファイルに付加することができる。

ADS のシステムを構成する各要素に対する改良、変更点は以下のようにになっている。

a) ADS サーバプログラム

ADS のサーバプログラムにはデベロッパからファイルの直接転送による登録を受け付ける機能、ファイルを新しい形式のパッケージファイルに変換する機能、さらに airClub スタッフによる安全性検証を経て公開される時点でパッケージファイルに署名を付加する機能が追加さ

れた。

b) ADS パッケージマネージャ

ADS のユーザ向けクライアントプログラムであるパッケージマネージャには新しい形式のパッケージファイルを扱う機能、パッケージの署名を検証する機能が追加され、airWeb 本体にインストール済みパッケージの情報を管理する機能が備わったため、従来はパッケージマネージャが独自に行っていたインストール済みパッケージの情報管理を airWeb 本体の機能で行うよう変更されている。

c) ADS エージェントパブリッシャ

ADS のデベロッパ向けクライアントプログラムであるエージェントパブリッシャは新しいサーバプログラムに対しファイルを直接転送して登録する機能が追加された。従来のファイルの位置情報のみ送信する登録方法への対応は終了した。

d) パッケージ署名

従来の ADS はデベロッパから登録されたエージェントをスタッフが検査し、安全性において問題ないもののみユーザに公開する事で、悪意を持ったエージェントからユーザの環境を保護してきた。

しかし、エージェントパッケージファイルをデベロッパが用意したスペースで公開しているため、安全性の検査が終わった後でパッケージファイルを差し替える事が可能であり、セキュリティ確保の方法として有効に機能していたとは言い難いものであった。

新しい方法では、airClub のスタッフが登録されたエージェントの安全性を検証してから公開する部分は変わらないが、公開されるパッケージには安全性検証済みであることを証明する署名を付加するため、改ざん、破損を検出し不正なパッケージのインストールを防止できる。

また、パッケージファイルに署名を付加する必要上、パッケージファイルは airClub 側に保存するよう変更されているため、パッケージが改ざん、破壊される危険がさらに減少している。

またダウンロード中の通信エラーが原因でパッケージファイルが破損した場合も署名の検証によってこれを検出可能なため、破損したパッケージをインストールする危険を回避することも可能となっている。

パッケージファイルに付加される署名は公開鍵暗号アルゴリズムによって保護され、証拠の残らないパッケージファイルの改ざんは極めて困難であり、ほぼ不可能である。

airClub がデベロッパ、あるいは特定のパッケージを信用することを、パッケージに対する安全性検証済みの署名によって表明する。ユーザは airClub を信用することによってデベロッパ、またはそのパッケージを間接的に信用することができる。

ユーザは airClub を信用することができれば ADS で配布されるエージェントを安全に利用することができる。

ユーザの立場から見れば、ユーザと airClub との一对一、しかもユーザが airClub を信用できるか否かのみが問題となるシンプルな信用モデルである。

署名に利用されている公開鍵暗号アルゴリズムに使用される鍵も airClub の公開鍵のみを airWeb 本体が管理しており、公開鍵暗号アルゴリズムにつきものの鍵の管理をユーザが意識しなくて済む。

e) パッケージファイルサーバ

従来の ADS はエージェント情報サーバを中心に構成されており、エージェント情報サーバはデベロッパが公開しているパッケージファイルの所在をパッケージ情報とともに登録するいわばリンク情報のサーバであった。

このため、デベロッパが自分のパッケージファイル公開のサイトを移転や構成変更をしたい場合には再登録が必要であり、エージェント情報サーバに登録されたリンク情報との整合性に問題をきたし、ユーザがパッケージファイルをダウンロードできなくなる事故が多発した。

また、公開するパッケージファイルの保護のため安全性検証済みの署名を付加し、ユーザのセキュリティを確保する必要も生じた。

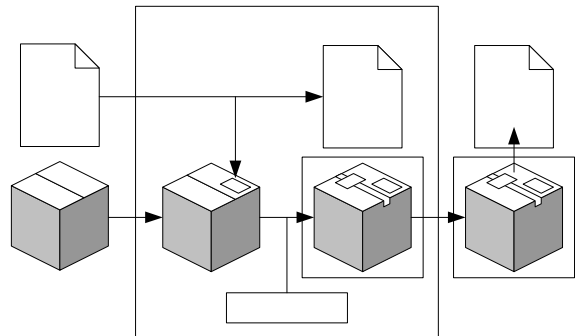
新しい ADS はエージェント情報サーバにパッケージファイルサーバの機能を併設し、デベロッパからファイルの直接転送を受け付け、パッケージファイルを airClub のサーバに保存するよう変更された。

これにより、デベロッパがパッケージを公開するための制限が緩和され、デベロッパは公開パッケージファイルを自分で管理する必要がなくなり、ユーザがパッケージファイルをダウンロードできなくなるような問題は解消された。

またパッケージファイルに新しい形式を採用し、サーバ側で各種情報を付加することが可能になった。これを利用してパッケージファイルの安全性を検証済みである事を証明する署名を付加している。

(3) セキュリティの強化

新しい ADS におけるパッケージの登録から公開までの各状況をセキュリティの観点から詳しく見ると、以下ようになる。



デベロッパはファイルをパッケージ情報とともに ADS のサーバに転送する。この時、ファイルに対する改ざんや破損の防止はデベロッパにその責任がある。従来の ADS ではパッケージファイルはこの状態のままユーザに公開されていた。

ADS のサーバプログラムは転送されたファイルから新しいパッケージファイル形式を作成し、同時に転送されたパッケージ情報を埋め込む。パッケージ情報はデータベースに登録され、作成されたパッケージファイルはサーバに保管される。この時点から転送されたファイルは ADS のサーバによって保護されるようになる。

airClub のスタッフによる安全性検証をパスし、パッケージがユーザに公開される時に ADS のサーバプログラムはパッケージファイルに安全性検証をパスした事を証

明する署名を付加する。
これによりパッケージファイル自身が改ざんや破損に対する耐性を持つようになる。

安全性検証済みを証明する署名はハッシュアルゴリズムで生成されたダイジェストを公開鍵暗号アルゴリズムで暗号化したものを使用する。

ハッシュアルゴリズムは既に複数実装され、選択可能な状態となっている（公開に危険を伴う情報であるためここではどのようなアルゴリズムを使用しているのか明記しない）。

公開鍵暗号アルゴリズムも実装され使用されている（ハッシュアルゴリズム同様ここでは明記しない）。

鍵長は可変でサーバ、airWeb 本体を含むクライアントの双方とも任意の鍵長を扱うことができる。

暗号化の鍵に現在は 128 ビット以上の長さの鍵を使用している。サーバの処理能力やブロードバンドの普及、低価格化した大容量外部記憶装置を考慮すれば鍵長を長くすることも可能であるが、パッケージ署名の性格を考慮すると、128 ビットでも十分な安全性を得られると考えられる。

ハッシュアルゴリズムと公開鍵暗号アルゴリズムは鍵ごとに選択可能であり、万一アルゴリズムの脆弱性が発見されたような場合に他のアルゴリズムに切り替える事が可能になっている。

（４）キラーエージェントの開発

前年度の事業では４４本のエージェントを開発し、パブリックベータ版として airWeb にバンドルして配布を行った。またその後の airClub コミュニティではネット上の作者によるエージェントが次々と開発され、平成 14 年 2 月現在で ADS には 74 本のエージェントが登録されている。

さまざまなサイトへの対応というニーズとともに、収集した情報をより効果的にブラウズしたり管理するニーズが顕著に高いことも明らかとなっている。

本開発では、ニーズの高いいくつかのエージェントについて改良を行った。以下に、新規に作成したヘッドライン巡回エージェントについて述べる。

a) ヘッドライン巡回エージェント

ホームページ収集が汎用的な Web サイトイメージの複製を行うのに対し、新着情報やプレスリリースといったヘッドライン構成になっている情報では収集した情報の一覧性に欠ける。（図 1）

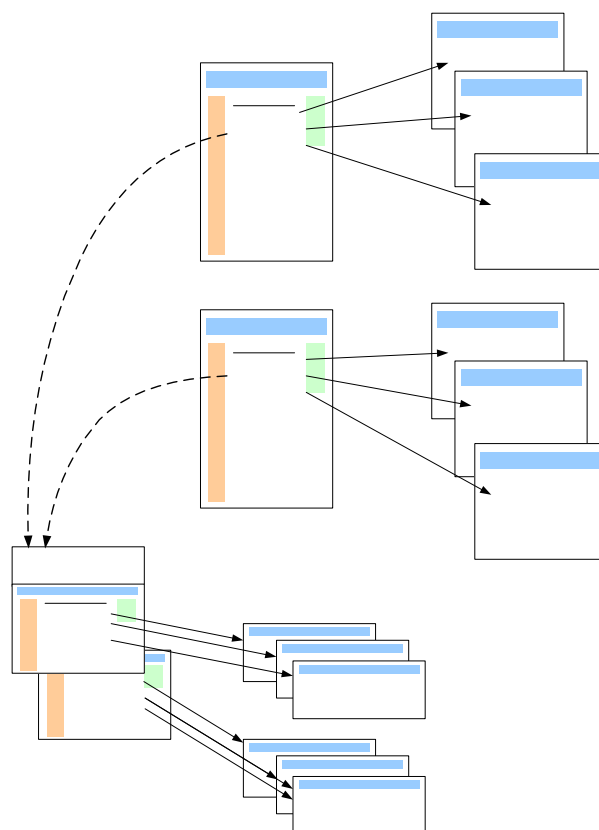


図 1 ホームページ収集での収集イメージ

そこで、ページ構成に特化した収集エージェントの一例として、ヘッドライン形式のページ構成から記事を収集するエージェントを開発した。

ヘッドライン型ページ収集エージェントは、ニュースキャストエージェントのノウハウとホームページ収集エージェントの機能を組み合わせて、ニュース速報や新着ソフトレビューなど、見出しから記事がリンクされる構成のほとんどのページに対応できる。

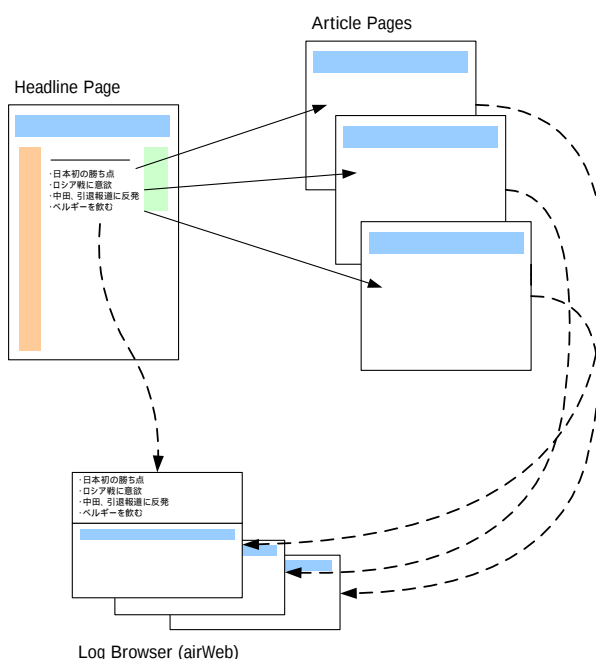


図 2 ヘッドライン収集でのログイメージ

これまでに要望が多かった地方紙のニュースキャストや
株価速報なども収集でき、定義ファイルを流通させるこ
とでエージェント作者とは違った層の情報作成のコミュ
ニティが形成されることも期待できる。

5．参加企業及び機関

飯塚豊

株式会社エアフロント

契約件名

「パーソナルサイズのマルチエージェント統合環境
airWeb」

6．参考文献

[1] ウィリアム・スターリングス：暗号とネットワーク
セキュリティ,ピアソン・エデュケーション,2001

[2] BRUCE SCHNEIER : APPLIED CRYPTOGRAPHY,
John Wiley & Sons, Inc.N.Y.(2001)