

# ADOBE® AIR™ 1.5 の セキュリティ

## 著作権情報

© 2008 Adobe Systems Incorporated. All rights reserved.

Adobe® AIR™ 1.5 のセキュリティ

本マニュアルがエンドユーザ使用許諾契約を含むソフトウェアと共に提供される場合、本マニュアルおよびその中に記載されているソフトウェアは、エンドユーザ使用許諾契約にもとづいて提供されるものであり、当該エンドユーザ使用許諾契約の契約条件に従ってのみ使用または複製することが可能となるものです。当該エンドユーザ使用許諾契約により許可されている場合を除き、本マニュアルのいかなる部分といえども、**Adobe Systems Incorporated**（アドビ システムズ社）の書面による事前の許可なしに、電子的、機械的、録音、その他いかなる形式・手段であれ、複製、検索システムへの保存または伝送を行うことはできません。本マニュアルの内容は、エンドユーザ使用許諾契約を含むソフトウェアと共に提供されていない場合であっても、著作権法により保護されていることにご留意ください。

本マニュアルに記載される内容は、あくまでも参照用としてのみ使用されること、また、なんら予告なしに変更されることを条件として、提供されるものであり、従って、当該情報が、アドビ システムズ社による確約として解釈されてはなりません。アドビ システムズ社は、本マニュアルにおけるいかなる誤りまたは不正確な記述に対しても、いかなる義務や責任を負うものではありません。

新しいアートワークを創作するためにテンプレートとして取り込もうとする既存のアートワークまたは画像は、著作権法により保護されている可能性のあるものであることをご留意ください。当該アートワークまたは画像を新しいアートワークに許可なく取り込んだ場合、著作権者の権利を侵害することがあります。従って、著作権者から必要とするすべての許可を必ず取得してください。

例として使用されている会社名は、実在の会社・組織を示すものではありません。

Adobe, the Adobe logo, ActionScript, and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Mac is a trademark of Apple Inc., registered in the United States and other countries. Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

This work is licensed under the Creative Commons Attribution Non-Commercial 3.0 License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/3.0/us/>

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

MPEG Layer-3 audio compression technology licensed by Fraunhofer IIS and Thomson Multimedia (<http://www.mp3licensing.com>).

Portions of this product contain code licensed from Nellymoser ([www.nellymoser.com](http://www.nellymoser.com)).

Video compression and decompression is powered by On2 TrueMotion video technology. © 1992-2005 On2 Technologies, Inc. All Rights Reserved. <http://www.on2.com>.

This product includes software developed by the OpenSymphony Group (<http://www.opensymphony.com/>)

This product contains either BSAFE and/or TIPEM software by RSA Security, Inc.

**Sorenson  
Spark**

Sorenson Spark™ video compression and decompression technology licensed from Sorenson Media, Inc.

This product includes software developed by the IronSmith Project (<http://www.ironsmith.org/>).

Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA.

Notice to U.S. Government End Users. The Software and Documentation are “Commercial Items,” as that term is defined at 48 C.F.R. §2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA. For U.S. Government End Users, Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

# 目次

## Adobe AIR 1.5 のセキュリティ

概要 .....	1
アプリケーションのインストールとアップデート .....	1
コード署名 .....	3
セキュリティサンドボックス .....	4
ファイルシステムへのアクセス .....	5
信頼されないコンテンツの安全な使用 .....	6
HTML セキュリティ .....	6
その他のセキュリティに関する考慮事項 .....	7

# Adobe AIR 1.5 のセキュリティ

セキュリティは、アドビ システムズ社、ユーザ、システム管理者およびアプリケーション開発者にとって、重要な関心事の 1 つです。このような理由から、Adobe® AIR™ には、ユーザやアプリケーション開発者を保護するためのセキュリティ規則やコントロールのセットが用意されています。このホワイトペーパーでは、Adobe AIR アプリケーションを使用および開発する際のセキュリティに関する考慮事項について説明します。

## 概要

AIR のセキュリティモデルは、Flash® Player で実行される SWF コンテンツやブラウザで実行される HTML コンテンツのセキュリティモデルを発展させたものですが、セキュリティコントラクトはブラウザのコンテンツに適用されるセキュリティコントラクトとは異なります。このコントラクトは、開発者に、ブラウザベースのアプリケーションには十分すぎるほど自由にリッチエクスペリエンスを実現できる豊富な機能を提供します。

AIR アプリケーションは、ネイティブアプリケーションと同じユーザ権限で実行されます。一般的に、これらの権限では、ファイルの読み取りや書き込み、画面への描画、ネットワークとの通信など、オペレーティングシステム機能に広範囲にアクセスできます。ネイティブアプリケーションに適用されるオペレーティングシステムの制限（ユーザ固有の権限など）は、AIR アプリケーションにも同等に適用されます。

AIR アプリケーションは、コンパイル済みバイトコード（SWF コンテンツ）または変換されるスクリプト（JavaScript、HTML）のいずれかを使用して作成されているので、ランタイムでメモリを管理できます。これにより、メモリ管理に関連する脆弱性（バッファオーバーフローやメモリの破損など）によって AIR アプリケーションが影響を受ける可能性を最小限に抑えることができます。これらは、ネイティブコードで作成されたデスクトップアプリケーションに影響を与える最も一般的な脆弱性の一部です。

**注意：**このホワイトペーパーでは、Adobe AIR でのセキュリティに関連する事項について説明します。開発者向けドキュメントの「AIR のセキュリティ」の章には、セキュリティで保護された AIR アプリケーションの開発に関する技術的な詳細や、AIR API を使用する際の考慮事項が示されています。

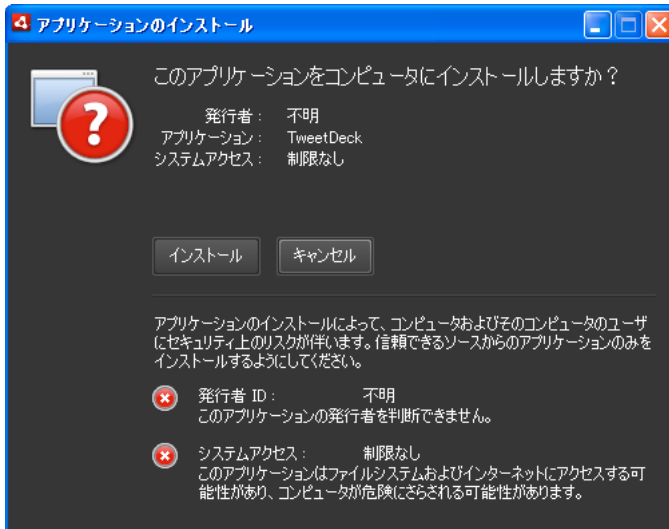
- Flex 開発者向け ([http://www.adobe.com/go/learn\\_air\\_flex\\_jp](http://www.adobe.com/go/learn_air_flex_jp))
- Flash 開発者向け ([http://www.adobe.com/go/learn\\_air\\_flash\\_jp](http://www.adobe.com/go/learn_air_flash_jp))
- Ajax 開発者 ([http://www.adobe.com/go/learn\\_air\\_html\\_jp](http://www.adobe.com/go/learn_air_html_jp))

## アプリケーションのインストールとアップデート

AIR アプリケーションは、拡張子が air の AIR インストーラファイルを使用して配布されます。Adobe AIR がインストールされている環境で AIR ファイルを開く場合、ランタイムによってアプリケーションのインストールプロセスが制御および管理されます。

**注意：**開発者は、バージョン、アプリケーション名、発行者ソースを指定できますが、アプリケーションのインストールの最初のワークフロー自体は変更できません。Adobe AIR によって管理される安全で合理化された一貫性のあるインストール手順をすべてのアプリケーションで共有できるので、この制限はユーザにとって有利になります。アプリケーションのカスタマイズが必要な場合は、アプリケーションを初めて実行するときに指定できます。

デフォルトのアプリケーションインストーラによって、セキュリティ関連の情報がユーザに示されます。AIR のインストール中に発行者名が表示されるのは、信頼できる証明書、またはインストールされているコンピュータで信頼されている証明書にチェーン化されている証明書を使用して AIR アプリケーションに署名している場合です。それ以外の場合、発行者名は「不明」として表示されます。これにより、ユーザは、十分な情報に基づいてアプリケーションをインストールするかどうかを決定できます。



SWF ファイルで最初に Flash Player ブラウザプラグインをインストールする必要があるのと同様に、AIR アプリケーションでも最初にランタイムをユーザのコンピュータにインストールする必要があります。

ランタイムは 2 つの方法でインストールできます。1 つはシームレスインストール機能を使用する方法で、もう 1 つは手でインストールする方法です。

- シームレスインストール機能を使用すると、開発者は、Adobe AIR をインストールしていないユーザに合理化されたインストールエクスペリエンスを提供できます。シームレスインストールでは、開発者は Web ページに SWF ファイルを埋め込み、その SWF ファイルでインストール対象の AIR アプリケーションの名前を示します。ユーザが SWF ファイルをクリックしてアプリケーションをインストールするときに、SWF ファイルによってランタイムの有無が確認されます。ランタイムが検出されない場合、ランタイムはインストールされて、開発者のアプリケーションのインストールプロセスですぐに有効化されます。ユーザには、インストールをキャンセルするためのオプションも提供されます。
- ユーザが AIR ファイルをインストールする前にランタイムを手動でダウンロードしてインストールすることもできます。この場合、開発者は様々な方法（電子メールや Web サイト上の HTML リンクなど）で AIR ファイルを配布できます。AIR ファイルを開くと、ランタイムが有効化され、アプリケーションのインストール処理が開始されます。

AIR のセキュリティモデルでは、ユーザが AIR アプリケーションをインストールするかどうかを決定できます。AIR インストーラでは、ユーザがこの信用判断をより簡単に行うことができるように、ネイティブアプリケーションのインストールテクノロジーにいくつかの改良が行われています。

- ランタイムは、AIR アプリケーションが Web ブラウザ内のリンクからインストールされる場合でも、すべてのオペレーティングシステムで一貫したインストールエクスペリエンスを提供します。ネイティブアプリケーションのインストールエクスペリエンスは、セキュリティ情報がすべて提供される場合、セキュリティ情報を提供するブラウザまたは他のアプリケーションに依存します。
- AIR アプリケーションインストーラはアプリケーションのソースを識別し（ソースを検証できない場合は、インストーラが確認）、ユーザがインストールの続行を許可した場合にアプリケーションで利用可能になる権限に関する情報を提供します。

- ランタイムは、AIR アプリケーションのインストールプロセスを管理します。AIR アプリケーションは、ランタイムが使用するインストールプロセスを操作できません。

一般的に、ユーザは信頼していないソースや、検証できないソースから提供されたデスクトップアプリケーション（AIR アプリケーションを含む）をインストールする必要はありません。他のインストール可能なアプリケーションと同様に、ネイティブアプリケーションのセキュリティに関する立証責任は、AIR アプリケーションにも同等に当てはまります。

## AIR アプリケーションのアップデート

ソフトウェアアップデートの開発と展開は、ネイティブコードアプリケーションの中でも最も大きなセキュリティ問題の 1 つです。インストール済みの AIR アプリケーションで、リモートの場所にアップデート AIR ファイルがあるかどうかを確認できます。アップデートが必要な場合、AIR ファイルがダウンロード、インストールされ、アプリケーションが再起動します。開発者向けドキュメントでは、この方法を使用して、新しい機能を提供するだけでなく、潜在的なセキュリティの脆弱性に対処するための詳細を説明しています。

## AIR アプリケーションの削除

ユーザは AIR アプリケーションを次の方法で削除できます。

- Windows：「プログラムの追加と削除」パネルを使用してアプリケーションを削除します。
- Macintosh：インストール場所からアプリケーションファイルを削除します。

AIR アプリケーションを削除すると、アプリケーションディレクトリ内のすべてのファイルが削除されます。ただし、アプリケーションがアプリケーションディレクトリ以外のディレクトリに書き込んだファイルは削除されません。AIR アプリケーションを削除すると、AIR アプリケーションがアプリケーションディレクトリ以外のディレクトリに行った変更は元に戻りません。

## コード署名

Adobe AIR では、すべての AIR アプリケーションが電子署名されている必要があります。コード署名は、ソフトウェアの整合性と発行者の ID を保証するために、コードに電子署名するプロセスです。開発者は、証明機関（CA）から発行された証明書を使用するか、自己署名入り証明書を作成することによって、AIR アプリケーションに署名できます。

認定されている証明機関（CA）が発行した証明書を使用して AIR ファイルに電子署名すると、インストールしているアプリケーションが誤ってまたは悪意を持って変更されていないことをユーザに確実に保証することができます。認定された証明機関（CA）が発行した証明書を使用して AIR ファイルに電子署名すると、開発者は署名者（発行者）と見なされます。AIR では、Verisign および Thawte 証明機関によって発行されたコード署名証明書が認識されます。開発者が Verisign または Thawte の証明書を使用して AIR ファイルに署名している場合、AIR アプリケーションインストーラによってインストール中に発行者名が表示されます。

AIR アプリケーションインストーラによってインストール中に発行者名が表示されるのは、信頼できる証明書、またはインストールされているコンピュータで信頼されている証明書にチェーン化されている証明書を使用して AIR アプリケーションに署名している場合です。証明機関（CA）では、信頼性の高い証明書を発行する前に、実績のあるプロセスを使用して発行者または開発者の ID を検証します。

開発者は、自分自身で作成した、自己署名入り証明書を使用して AIR アプリケーションに署名することもできます。ただし、AIR アプリケーションインストーラでは、このようなアプリケーションは発行者が検証されていないアプリケーションとして表示されます。

AIR ファイルに署名が行われると、電子署名がインストールファイルに含まれます。署名には、署名後に AIR ファイルが変更されていないことを検証するために使用されるパッケージのダイジェストと、発行者 ID を検証するために使用する署名証明書に関する情報が含まれます。

AIR では、オペレーティングシステムの証明書ストアを通じてサポートされる公開キーインフラストラクチャ (PKI) を使用します。AIR アプリケーションがインストールされているコンピュータでは、発行側の情報を検証するために、AIR アプリケーションの署名に使用されている証明書そのものを信頼するか、信頼できる証明機関の証明書にリンクしている証明書のチェーンを信頼する必要があります。

AIR ファイルが、信頼できるルート証明書 (およびこれには通常すべての自己署名入り証明書が含まれる) のいずれにもチェーン化されていない証明書で署名されている場合、発行者側の情報は検証できません。AIR は、AIR ファイルが署名後に変更されていないか確認できますが、ファイルの実際の作成者および署名者を検証することはできません。

コード署名プロセスおよび使用できる証明書の形式について詳しくは、開発者向けドキュメントを参照してください。

## セキュリティサンドボックス

AIR には、AIR アプリケーションの各ファイルの権限を定義する包括的なセキュリティアーキテクチャが用意されています。これには、アプリケーションと共にインストールされるファイルと、アプリケーションによって読み込まれるその他のファイルの両方が含まれます。権限はその生成元に従ってファイルに付与され、サンドボックスと呼ばれる論理的なセキュリティグループに割り当てられます。

アプリケーションと共にインストールされるファイルはアプリケーションディレクトリと呼ばれるディレクトリに配置されます。このため、デフォルトではすべての AIR API にアクセスできるアプリケーションサンドボックスと呼ばれるセキュリティサンドボックスに配置されます。AIR API の中には、アプリケーションリソースディレクトリ以外のソースのコンテンツ (つまり、アプリケーションと共にインストールされたものではないファイル) から利用できるようにした場合に、多大なセキュリティリスクを発生させる API が含まれます。

サンドボックスの AIR セキュリティモデルは、Flash Player セキュリティモデルと追加のアプリケーションサンドボックスで構成されています。アプリケーションサンドボックスに含まれないファイルには、Flash Player セキュリティモデルで指定されているセキュリティ制限と同様のセキュリティ制限が適用されます。

ランタイムはこれらのセキュリティサンドボックスを使用して、ファイルがアクセスするデータの範囲や、ファイルが実行する処理を定義します。ローカルのセキュリティを維持するために、各サンドボックス内のファイルは他のサンドボックスのファイルと分離されています。例えば、外部のインターネット URL から AIR アプリケーションに読み込まれた SWF ファイルはリモートサンドボックスに配置されます。デフォルトでは、このファイルは、アプリケーションサンドボックスに割り当てられるアプリケーションディレクトリ内のファイルに対してスクリプトを実行するための権限を持ちません。

### 非アプリケーションサンドボックス内のコンテンツの権限

アプリケーションがインストールされると、AIR インストーラファイルに含まれているすべてのファイルがユーザのコンピュータのアプリケーションディレクトリにインストールされます。アプリケーションの実行時にアプリケーションディレクトリツリー内のすべてのファイルがアプリケーションサンドボックスに割り当てられます。アプリケーションサンドボックス内のコンテンツには、ローカルファイルシステムとのやり取りを含め、AIR アプリケーションで使用できる完全な権限が与えられます。

AIR アプリケーションの多くは、ローカルにインストールされたこれらのファイルのみを使用してアプリケーションを実行します。ただし、AIR アプリケーションがアプリケーションディレクトリ内のファイルだけに制限されるわけではなく、どのソースのどの種類のファイルでも読み込むことができます。これにはユーザのコンピュータのローカルファイルだけでなく、ローカルネットワークやインターネットなど使用可能な外部ソースのファイルも含まれます。ファイルの種類はセキュリティ制限に影響しません。読み込まれた HTML ファイルは、同じソースから読み込まれた SWF ファイルと同じセキュリティ権限を持ちます (ただし、アプリケーションサンドボックス内のコンテンツでは、サンドボックスの外部から JavaScript ファイルを読み込むことはできません。詳しくは、開発者向けドキュメントを参照してください)。

アプリケーションセキュリティサンドボックス内のコンテンツは、他のサンドボックス内のコンテンツでは使用できない AIR API にアクセスできます。例えば、アプリケーションセキュリティサンドボックス内のコンテンツのみが、ローカルファイルシステムに対して読み取りおよび書き込みを実行できます。

JavaScript の手法には、ストリングを動的に実行可能コードに変換できるものがあります。アプリケーションセキュリティサンドボックス内のコンテンツは、コードがアプリケーション URL から読み込んでいるときにのみこれらの手法を使用できます。アプリケーションサンドボックス内でこれらの手法を使用すると、セキュリティリスクが発生します。例えば、ネットワークサンドボックスから読み込まれた文字列をアプリケーションで不用意に実行する可能性があります。また、その文字列には、ユーザのコンピュータのファイルの削除または変更を行ったり、信頼できないネットワークドメインにローカルファイルのコンテンツを報告したりする悪質なコードが含まれている場合があります。詳しくは、開発者向けドキュメントを参照してください。

## 非アプリケーションサンドボックス内のコンテンツの権限

ネットワークやインターネットから読み込んだファイルは、非アプリケーションサンドボックスに割り当てられます。このようなコンテンツは、Web ブラウザ (Flash Player) 内で実行される SWF コンテンツや、Web ブラウザ内で実行される HTML コンテンツと同じ権限および制限で動作します。

アプリケーションセキュリティサンドボックスのコンテンツとは異なり、非アプリケーションセキュリティサンドボックスの HTML コードは、JavaScript のメソッドを使用して、動的に生成されたコードをいつでも実行できます。

非アプリケーションサンドボックス内のコードは、アプリケーションの機能を提供する、権限が付与された AIR API にアクセスできません。

詳しくは、開発者向けドキュメントを参照してください。

## ファイルシステムへのアクセス

Web ブラウザで実行中のアプリケーションは、ユーザのローカルファイルシステムとのやり取りのみが制限されます。

Web ブラウザは、Web コンテンツを読み込んでもユーザのコンピュータが改ざんされないことを保証するセキュリティポリシーを実装します。例えば、ブラウザで Flash Player を使って実行されている SWF ファイルは、ユーザのコンピュータに既に存在するファイルと直接やり取りできません。共有オブジェクトはユーザの環境設定およびその他のデータを管理する目的でユーザのコンピュータに書き込むことができますが、これはファイルシステム操作の制限になります。AIR アプリケーションはネイティブにインストールされるので、エンドユーザとは異なるセキュリティコントラクトを備えています。このアプリケーションとエンドユーザとのコントラクトは、ネイティブアプリケーションと同様にインストール時に作成され、アプリケーションがローカルファイルシステムに対して読み取りや書き込みを実行する機能が含まれます。

この自由度には開発者の大きな責任が伴います。アプリケーションの予想外の不安定さは、アプリケーションの機能だけでなく、ユーザのコンピュータの完全性も危険にさらします。開発者向けドキュメントの「AIR のセキュリティ」の章では、ベストプラクティスについて説明しています。

ユーザのコンピュータに対する管理者の制限がない限り、AIR アプリケーションには、ユーザのハードドライブ上のどの場所にも書き込むことができる権限が付与されます。ただし、開発者は、ランタイムが各アプリケーションに提供する、ユーザおよびアプリケーション固有のアプリケーション記憶領域ディレクトリを使用することをお勧めします。AIR API には、開発者がアプリケーション記憶領域ディレクトリ内のデータを読み取りおよび書き込みするための便利なメソッドが用意されています。ランタイムは、各アプリケーションおよびユーザに固有な暗号化されたローカルデータ記憶領域も提供します。これにより、アプリケーションでは、他のアプリケーションまたはユーザによって簡単に解読されないように暗号化された形式で、ユーザのローカルハードディスクに格納されたデータを保存および取得できるようになります。各 AIR アプリケーションに対して個別の暗号化されたローカルストアが使用され、各 AIR アプリケーションは各ユーザに対して個別の暗号化されたローカルストアを使用します。アプリケーションでは、Web サービスに対するログイン資格情報など、セキュリティ

で保護する必要がある情報を格納するために暗号化されたローカルストアを使用できます。AIR は、暗号化されたローカルストアを各ユーザーに関連付けるために、Windows では DPAPI を使用し、Macintosh では KeyChain を使用します。暗号化されたローカルストアは AES-CBC 128 ビット暗号化を使用します。

## 信頼されないコンテンツの安全な使用

アプリケーションサンドボックスに割り当てられていないコンテンツは、ランタイムのセキュリティ基準を満たす場合のみ AIR アプリケーションに追加のスクリプト機能を提供できます。ここでは、非アプリケーションコンテンツでの AIR セキュリティコントラクトについて説明します。

AIR アプリケーションは、Flash Player のブラウザプラグインが信頼されないコンテンツのスクリプトによるアクセスを制限するよりも厳格に、非アプリケーションコンテンツのスクリプトによるアクセスを制限します。例えば、ブラウザ内の Flash Player では、SWF ファイルで `System.allowDomain()` メソッドを呼び出して、指定したドメインから読み込まれた SWF コンテンツへのスクリプトによるアクセスを許可することができます。このメソッドの呼び出しは、ユーザーのファイルシステム内の非アプリケーションファイルへの不適切なアクセスを許可することになるので、アプリケーションセキュリティサンドボックス内のコンテンツについては許可されていません。

アプリケーションコンテンツと非アプリケーションコンテンツとの間をスクリプト化する AIR アプリケーションではさらに複雑なセキュリティの調整が行われます。アプリケーションサンドボックス内に含まれていないファイルは、サンドボックスブリッジを使用したアプリケーションサンドボックス内のファイルのプロパティとメソッドへのアクセスのみが許可されます。サンドボックスブリッジはアプリケーションコンテンツと非アプリケーションコンテンツ間のゲートウェイとして機能し、2つのファイル間の明示的な操作を可能にします。サンドボックスブリッジを正しく使用すると、セキュリティの追加のレイヤーが提供され、非アプリケーションコンテンツが、アプリケーションコンテンツの一部となるオブジェクト参照にアクセスするのを制限します。

サンドボックスブリッジのメリットについて、例を使って説明します。AIR ミュージックストアアプリケーションは、独自の SWF ファイルを作成する必要のある広告主に API を提供し、ストアアプリケーションはこのファイルを使用して通信できます。ストアは、ストアが提供するアーティストと CD を探すためのメソッドを広告主に提供する必要がありますが、セキュリティ上の理由でサードパーティの SWF ファイルからメソッドとプロパティを分離する必要があります。

サンドボックスブリッジはこの機能を提供できます。デフォルトでは、ランタイムで外部から AIR アプリケーションに読み込まれたコンテンツには、メインアプリケーションのどのメソッドまたはプロパティへのアクセス権もありません。カスタムのサンドボックスブリッジ実装を使用すると、開発者はこれらのメソッドやプロパティを公開せずにリモートコンテンツにサービスを提供できます。サンドボックスブリッジは信頼されるコンテンツと信頼されないコンテンツ間の制限された通路となります。

サンドボックスブリッジの使用について詳しくは、開発者向けドキュメントの「AIR のセキュリティ」の章を参照してください。

## HTML セキュリティ

HTML コンテンツでは、主に JavaScript による動的に生成されるコードの作成機能のために、SWF ベースのコンテンツとは異なるセキュリティの考慮事項があります。eval() 関数を呼び出すときに作成されるような、動的に生成されたコードがアプリケーションサンドボックス内で許可されると、セキュリティリスクが発生することがあります。例えば、ネットワークサンドボックスから読み込まれた文字列をアプリケーションで不用意に実行する可能性があります。また、その文字列には、ユーザーのコンピュータのファイルの削除または変更を行ったり、信頼できないネットワークドメインにローカルファイルのコンテンツを報告したりする悪質なコードが含まれている場合があります。

動的なコードを生成するには、次のような方法があります。

- eval() 関数を呼び出します。

- innerHTML プロパティを設定するか、または DOM 関数を呼び出してスクリプトタグを挿入してリソース外のスクリプトを直接読み込みます。
- innerHTML プロパティを設定するか、または DOM 関数を呼び出して、(src を使用してスクリプトを読み込むのではなく) インラインコードを含む script タグを挿入します。
- アプリケーションサンドボックス内のコンテンツについて、script タグの src を、アプリケーションリソースディレクトリ以外にあるファイルに設定します。
- javascript URL スキームを使用します (href="javascript:alert("Test")" など)。

アプリケーションセキュリティサンドボックス内のコードは、アプリケーションディレクトリからコンテンツを読み込んでいるときにのみこれらのメソッドを使用できます。これによって、すべての AIR API にアクセスできるアプリケーションサンドボックス内のコードが、潜在的に信頼されないソースのスクリプトを実行することを防止できます。

非アプリケーションセキュリティサンドボックスのコンテンツは、これらのメソッドを使用して動的コードを生成できます。ただし、直接 AIR API にアクセスできるわけではありません。AIR のサンドボックスブリッジ機能によって、非アプリケーションセキュリティサンドボックス内のコードが、アプリケーションコードによって制限および決定された方法で、アプリケーションサンドボックス内のコードとやり取りするための手段が提供されます。

AIR アプリケーションは、(ファイルやネットワークのソースから読み込むのではなく) HTML スtring 変数から HTML コンテンツを生成できます。ただしデフォルトでは、String によって生成された HTML コンテンツには、アプリケーションサンドボックスの権限が付与されません。これにより、潜在的に安全でないインターネットのソースから取得される String コンテンツに、アプリケーションが不用意にアクセスしないようにします。

HTML セキュリティについて詳しくは、開発者向けドキュメントの「AIR のセキュリティ」の章を参照してください。

- Flex 開発者向け ([http://www.adobe.com/go/learn\\_air\\_flex\\_jp](http://www.adobe.com/go/learn_air_flex_jp))
- Flash 開発者向け ([http://www.adobe.com/go/learn\\_air\\_flash\\_jp](http://www.adobe.com/go/learn_air_flash_jp))
- Ajax 開発者向け ([http://www.adobe.com/go/learn\\_air\\_html\\_jp](http://www.adobe.com/go/learn_air_html_jp))

「Adobe AIR HTML のセキュリティ」ホワイトペーパーも参照してください ([http://www.adobe.com/go/learn\\_air\\_htmlsecurity\\_wp\\_jp](http://www.adobe.com/go/learn_air_htmlsecurity_wp_jp))。

## その他のセキュリティに関する考慮事項

AIR アプリケーションが Web テクノロジーを使用して構築されていても、開発者はそれらの AIR アプリケーションがブラウザのセキュリティモデル内で機能していないことに気づくことが重要です。つまり、故意にまたは誤ってローカルシステムに損害を与える可能性がある AIR アプリケーションを構築する場合があります。AIR はリスクを最小化しようと試みますが、脆弱性が取り込まれる可能性はまだあります。ここでは、重要なセキュリティ上の潜在的なリスクについて説明します。開発者向けのドキュメントでは、このようなリスクを回避するアプリケーションを構築するためのベストプラクティスを示しています。

### ファイルをアプリケーションセキュリティサンドボックスにインポートした場合のリスク

アプリケーションサンドボックスがランタイムのすべての権限を持つコンテンツ。開発者は次の点に注意する必要があります。

- ファイルは必要な場合のみ AIR ファイル (インストール済みアプリケーション内) に含めます。
- スクリプトファイルは、動作が完全に把握され、信頼される場合のみ AIR ファイル (インストール済みアプリケーション内) に含めます。

- ネットワークソースのデータを AIR API のメソッドのパラメータとして使用しないでください。これによりコードが実行される可能性があります。

Adobe AIR では、アプリケーションサンドボックス内のコンテンツがネットワークソースのデータをコードとして使用することによって、悪意のあるコードが誤って実行されることを防ぎます。これには、ActionScript Loader.loadBytes() メソッドや JavaScript eval() 関数の使用が含まれます。

## 外部ソースを使用してパスを判断する場合のリスク

AIR アプリケーションは、外部のデータまたはコンテンツを使用すると、改ざんされる可能性があります。このため、アプリケーションでネットワークまたはファイルシステムのデータを使用する場合は特に注意する必要があります。信頼の責任は最終的には開発者と、開発者が作成するネットワーク接続にあります。外部データの読み込みは本来リスクを伴うものであるため、機密データの操作への入力には使用しないでください。開発者は次の操作を行わないことをお勧めします。

- ネットワークソースのデータを使用したファイル名の決定
- ネットワークソースのデータを使用した、アプリケーションでの個人情報の送信に使用される URL の作成

## 保護されていない資格情報を使用、保存または送信する場合のリスク

ユーザ資格情報をユーザのローカルファイルシステムに保存することは本来リスクを伴い、これらの資格情報が改ざんされる可能性があります。開発者は次の点に注意する必要があります。

- 資格情報をローカルに保存する必要がある場合は、ローカルファイルシステムに書き込むときに資格情報を暗号化します。Adobe AIR は、インストール済みの各アプリケーションに固有の暗号化された記憶領域を提供します。詳しくは、開発者向けのドキュメントを参照してください。
- ネットワークソースが信頼されない場合は、暗号化されていないユーザ資格情報をネットワークソースに送信しないでください。
- 資格情報の作成時にデフォルトのパスワードを指定しないでください。パスワードはユーザ自身が作成できるようにしてください。デフォルトを使用するユーザはその資格情報を、デフォルトパスワードを知っている攻撃者に公開することになります。

## ダウングレード攻撃のリスク

アプリケーションのインストール処理中に、ランタイムはアプリケーションのバージョンが現在インストールされていないことを確認します。アプリケーションが既にインストールされている場合、ランタイムは既存のアプリケーションのバージョンストリングを、インストールしようとしているバージョンと比較します。このストリングが異なる場合、ユーザはインストールのアップグレードを選択できます。ランタイムは、新しくインストールされるバージョンが古いバージョンよりも新しいことを保証するわけではなく、それが異なるバージョンであるということだけを保証します。攻撃者は古いバージョンをユーザに配布して、セキュリティの弱点をくぐり抜ける可能性があります。このリスクは軽減することができ、リスクを回避するためのバージョンスキームおよびアップデート確認の実装に関するベストプラクティスについては、開発者向けのドキュメントを参照してください。