



Adobe Flash Media Interactive Server 3.5 を使用した大規模なストリーミングの デプロイメント計画

7/6/09

目次

- 1 メディアストリーミング用の大規模デプロイメントの概要
- 4 処理能力の計画とオプション
- 6 デプロイメントのアーキテクチャ
- 17 ストレージとキャッシュ
- 18 ライブストリーミング
- 20 コンテンツの保護対策
- 21 トラブルシューティング
- 23 用語集

このドキュメントでは、Flash Media Server 3.5 のデプロイメントを実行する際の原則について解説します。ダイナミックストリーミングおよび DVR 機能に関するデプロイメントオプションについては、このドキュメントの今後のバージョンで扱う予定です。

メディアストリーミング用の大規模なデプロイメントの概要

大規模なデプロイメントの概要

Flash Media Interactive Server (FMIS) を大規模にデプロイすることで、高い品質が要求される Flash プラットフォームへのストリーミングに対応することができます。大規模なデプロイメントでは、複数のサーバーを相互にリンクしてサービスの処理能力と品質を向上させることで、メディアフローの途絶を減らし、ユーザーエクスペリエンスを改善することができます。

大規模なデプロイメントを効率的に計画するためには、データセンター（ローカルまたはリモート）の選択、帯域幅の問題、ストレージとキャッシュの管理、認証とセキュリティ、ライブストリーミングに関する考慮事項、およびトラブルシューティングなどの問題について検討する必要があります。このドキュメントでは、このような問題を解決し、使用するネットワークに最適な選択を行うために役立つ情報を提供します。

大規模なデプロイメントでは、複数のテナントを使用して複数のユーザーにサービスを提供します。場合によっては、複数のデータセンターにまたがる多数のデプロイメントが使用されます。

Flash Media Server では、大規模なデプロイメントに対する柔軟なソリューションが用意されており、2 種類の構成を選ぶことができます。Flash Media Interactive Server は、ネイティブのオリジン/エッジ構成、またはオリジン単独クラスター構成で設定できます。ここでは、それぞれの構成の利点について概要を説明します。

ライブとビデオオンデマンドのデプロイメントの違い

大規模なデプロイメントの効率を高めるには、配信するコンテンツの種類を検討する必要があります。ライブ（“ステートフル”）コンテンツとビデオオンデマンド（“ステートレス”）コンテンツは、それぞれキャッシュとディスクストレージに対する影響が異なり、必要となるロードバランシング処理のレベルも異なるため、別々の方法で処理する必要があります。

ビデオオンデマンド（VOD）ストリームは、一般的な DNS または GEO ロードバランシングを使用して負荷分散することができます。DNS ロードバランシングでは、ユーザーの DNS サーバーの場所に最も近いサーバーに要求を送ります。GEO ロードバランシングでは、ユーザーの実際の IP アドレスに最も近いサーバーに要求を送ります。

ライブストリームは 1 箇所から送信されるため、高度なロードバランシング処理が必要になります。多くの場合は、サーバーサイド ActionScript を使用してプロキシをセットアップします。その場合、Flash Media Live Encoder (FMLE) またはサードパーティのライブエンコーダーからのライブストリームの受け入れ先として、プライマリサーバーとバックアップサーバーのグループを定義する必要があります。このストリームが ActionScript を使用したプロキシ処理を経て、エッジサーバーに送られます。

待機中の処理能力を活用することもお勧めします。ライブストリームに使用されていないアイドル状態の処理能力を VOD に活用し、大規模なライブイベントに対応できるようにネットワークを拡張することができます。

また、ライブストリームをデプロイする際には、FMLE などのエンコーダーからサーバーへのパブリッシュが可能になるようにアクセスコントロールを設定することと、DoS 攻撃と入力過負荷を防止するために権限を設定することが重要です。

大規模なデプロイメントの計画について詳しくは、2 日間の実践的なトレーニングクラスを受講を検討してください。詳しくは、http://www.adobe.com/support/training/instructor_led_curriculum/fm3largescaleddeployment.html を参照してください。

ライブストリームは、VOD よりも少ないストレージ容量で利用できます。ただし、FMS 3.5 の DVR 機能を使用した場合は例外です。DVR を使用する場合、ストリーミングのナビゲーションを可能にするためにライブストリーム全体をアーカイブする必要があるため、十分なディスク容量が必要になります。ただし、一般的には、ライブストリームに必要なハードディスク容量はごくわずかであるか、まったく不要です。

キャッシュ処理も、ライブストリームコンテンツと VOD コンテンツでは異なります。キャッシュ処理は、ネットワーク効率、サーバー負荷、全体的なサービス品質に大きく影響します。VOD の場合、マルチビットレートストリーミングを使用すると、サーバーとネットワークの負荷が増大します。例えば、ユーザーがストリームを視聴しているときに帯域幅が変化する場合、ストリームが滑らかに切り替えられるように、すべてのビットレートバージョンのストリームをキャッシュしておく必要があります。それほど大量のデータは RAM に格納できないため、コンテンツ対応型の高度なキャッシュ機能を実装する必要があります。また、セグメントキャッシュを設定することで、エッジで提供されるビデオ部分を管理することができます。キャッシュの設定と管理について詳しくは、このホワイトペーパーの「ストレージとキャッシュ」を参照してください。

プロトコルのサポート

Flash Media Server では、Transmission Control Protocol (TCP) を経由した Adobe Real-time Messaging Protocol (RTMP) を使用して、接続されたクライアントと通信します。RTMP 接続により、ビデオ、オーディオ、データの双方向通信を管理します。Flash Media Server 3.5 の RTMP には、次の表に示すように 5 種類の設定があります。

名前	ポート	暗号化	説明
RTMP	1935	なし	標準の RTMP
HTTP	80	なし	(オプション) Apache Web サーバーがインストールされている場合、FMS はプロトコルに基づきポート 80 の要求を HTTP または RTMP にプロキシ処理します。
RTMP/T	80	なし	HTTP (カプセル化された RTMP パケットを使用)
RTMPS	443	あり	安全な SSL を介した RTMP には証明書の管理が必要
RTMPTS	80	あり	安全な SSL を介した RTMP (HTTP 内にトンネリング)
RTMPE	1935	あり	パフォーマンスの高い暗号化された RTMP
RTMPTE	80	あり	HTTP 内にトンネリングされた暗号化 RTMP

サーバーのデプロイメントのニーズに合わせて RTMP ポートを変更できます。

標準の RTMP プロトコルを使用した場合に、最も高いパフォーマンスが得られます。

RTMP/T または RTMPTE を使用した場合、RTMP を許可していないネットワークやポート 1935 をブロックしているネットワークのユーザーにも配信できるようになります。ただし、RTMP/T トンネリングを実行すると Flash Media Server の処理能力が減少し、RTMP (トンネリングされない) トラフィックが 30% 発生し、CPU 使用率が上昇します。

RTMPE の場合も CPU 使用率が上昇しますが、70% 未満の CPU 使用率でも 1 Gbps ネットワークインターフェイスがサチュレーションに達するため、CPU への負荷は SSL 暗号化よりも軽微です。

ハードウェアに関する考慮事項

帯域幅の消費が激しい大規模なホスティングではどれでも同じですが、Flash Media Server のデプロイメントでも、高速なディスクアクセス、豊富な RAM、高速なプロセッサ速度が推奨されます。次の表に示す構成でも、パフォーマンス上の問題を生じることなく、1 Gbps 以上のネットワーク接続がサチュレーションに達します。

デプロイメント	プロセッサ	RAM	RAIDの種類
小規模、1対多	デュアルコア 1 個	2 ~ 4 GB	RAID 1、5 または 6
中規模、1対多または多対多	クアッドコア 1 個	4 ~ 8 GB	RAID 1、5 または 6
大規模、1対多または多対多、平均的な共有オブジェクトの使用状況、インタラクティブ要素	クアッドコア 1 ~ 2 個	4 ~ 16 GB	RAID 1、10、5、50 または 6
最大規模、1対多、多対多、最大レベルの共有オブジェクトの使用状況、多彩なインタラクティブ要素	クアッドコア 1 ~ 2 個	16 ~ 32 GB	RAID 1、10、5、50 または 6

通常は、可能な限り高速なハードディスク (10,000 ~ 15,000 RPM) を選択する必要があります。

RAM

FMS では、RAM を使用して録画済みストリーム、インタラクティブコンテンツ、データなどのコンテンツをキャッシュするため、RAM を潤沢に用意しておくことが重要です。RAM が不足した場合、FMS ではハードディスクを使用してコンテンツをキャッシュするため、パフォーマンスが低下します。Flash Media Server では、キャッシュを 256 キロバイトのブロック単位で RAM またはハードディスクに格納するため、データに高速でアクセスすることができます。オリジンではキャッシュを RAM に格納し、エッジではハードディスクを使用してキャッシュすることで、オリジンの負荷を軽減することができます。Vhost.xml 設定ファイルの <CacheDir> タグを使用して、録画済みデータストリームをエッジ上のローカルハードディスクにキャッシュするように設定することで、ストリームが要求されるたびにオリジンからストリームにアクセスする必要がなくなります。

Flash Media Server では、キャッシュが RAM またはハードドライブに 256 キロバイトのブロックで保存されるので、情報にすばやくアクセスできます。オリジンの負荷を軽減するために、オリジンサーバーはキャッシュを RAM に保存し、エッジサーバーはハードドライブキャッシュを使用します。

CPU

接続の処理、サーバーサイドコードの実行、サーバー操作の管理を効率的に行うには、CPU の速度も重要です。CPU が過負荷になると、パフォーマンスが低下し、接続時間の増大と再バッドイベントの頻発を招くと共に、待ち時間が発生する可能性があります。一般的に、CPU またはコアが 1 つ増えると、パフォーマンスが 80% 上昇すると予想されます。デュアルコア CPU を 2 基搭載するコンピューターは、クアッドコア CPU を 1 基搭載するコンピューターよりも高いパフォーマンスを発揮します。最低でも、3.2GHz Intel® Pentium® 4 CPU をお勧めします。

RAM または CPU の使用率が頻繁に 75% を超える場合には、ハードウェアのアップグレードを真剣に検討してください。

大規模な FMS デプロイメント用に独自にハードウェアを購入する際には、同一のハードウェア構成を複数購入することをお勧めします。そうすることで、ハードウェアのクラッシュや障害が発生した場合に、ハードウェアの交換が容易になります。

アドビでは特定のハードウェアの認定は行っていませんが、統合ハードウェアソリューションを備えたサーバーが必要な場合には、CISCO Internet Streamer (Content Delivery Server) をお勧めします。このソリューションのハードウェアは、Flash Media Server を使用したストリーミングに最適化して設定されています。

ネットワークインターフェイス

FMS 3.5 では、わずか 20% の CPU 使用率* で 1 Gbps のネットワークインターフェイスカードがサチュレーションに達するため、複数のネットワークカードを追加してサーバーのネットワーク処理能力を向上させることを検討してもよいでしょう。複数のネットワークカードを使用すると、サーバーあたりの処理能力が 1.4 Gbps を超える可能性があります(各 NIC の使用率を 70% として計算)。これを、Linux では「ボンディング」、Windows では「チーミング」と呼びます。FMS ではオペレーティングシステムを経由してハードウェアリソースを利用するため、FMS に特別な設定を加える必要はありません。

ネットワークインターフェイスのアップグレードを計画する際に検討する問題点は、以下のとおりです。

- データセンターのネットワーク接続には、サーバーのネットワーク処理能力をサポートできるだけの帯域幅が必要です。
- ハードディスクの速度の限界がボトルネックになる可能性があります。ほとんどの SATA ハードディスクはバースト時のスループットが 3 Gbps に達しますが、通常維持されるスループットは 1 ~ 2 Gbps 程度です。高速回転 (10,000 RPM 以上) の SAS ハードディスクを使用すると、アクセス時間とスループットの改善に効果がある場合があります。FMS ではデータを効率的に RAM にキャッシュするため、ハードディスクの入出力動作が大量に発生しない限り、ハードディスクの速度が問題にならない可能性もあります。大量の入出力動作が発生する状況としては、同時に数百人のユーザーがビデオを録画したり、同時に数百~数千人のユーザーがビデオを再生したりするような、負荷の大きい録画再生アプリケーションを使用する場合があります。
- 複数の NIC カードを使用する場合、合計スループットを融合することで、1 Gbps の限界を超えます。使用率が 100% に達しないネットワークインターフェイスも、処理能力計画では発生します。
- Flash Media Server は、複数のネットワークカードを別々のリソースとして管理するように設定することもできます。ストリーミングをアダプターレベルで準備でき、特定のメディアや通信の配信を別々のネットワークカードにバインドすることができます。このソリューションを使用する際には、データが別々のネットワークカードにバインドされるため、サーバー全体で接続が永続的に維持されないことに注意してください。接続が永続的に維持されない問題は、リアルタイムのデータ共有やライブストリーミングなどのステータフルなアプリケーションに影響します。
- ネットワークの使用率が高まると (使用可能なネットワーク帯域幅の 70%)、CPU とメモリのオーバーヘッドが増加し、実際のネットワーク処理能力に関係なくパフォーマンスが低下する場合があります。

データセンター/コロケーション施設

IT インフラストラクチャは、アウトソーシングするか、社内でホスティングするかを選択できます。

社内でデプロイメントを行う場合、直接的な管理が必要になりますが、資格を持つ IT 管理者がいるのであれば、サーバーやインフラストラクチャをよりきめ細かく管理することができます。

ハードウェアのコストに加え、保守、管理、電力および帯域幅のコストも考慮する必要があります。多くの場合、社内における帯域幅と電力のコストは、外部データセンターにおけるコストよりも小さくなります。これは、中間業者に費用を上乗せされないためです。ただし、外部データセンターではハードウェアコストと保守が重視されており、多くの場合は大規模な固定インフラストラクチャを備え、高いネットワーク処理能力を実現しています。

* 平均 300 kbps のストリームが Linux Red Hat で実行されています。詳しくは、Flash Media Server 3.5 のホワイトペーパーを参照してください。

外部のデータセンターまたはコロケーション施設を検討する際には、次の点を考慮します。

- **ネットワークの信頼性。**帯域幅を提供するキャリアはどの会社か、その評判はどうかを確認します。そのキャリアはティア1でしょうか、ティア2でしょうか。または、さらに下の階層でしょうか。ティア1のキャリアでなくても、優れたパフォーマンスが得られる場合があります。一般的に、下層のネットワークでは他のプロバイダーにデータ転送の使用料を支払っています。そのため、ユーザーの使用料が高くなる場合がありますが、最終的にはティア1と同じ品質を達成することができます。
- **フェイルオーバーとセキュリティ。**データセンターに、予備のバックボーン接続と、フェイルオーバー発電機を備えた電源グリッド接続が用意されていますか。データセンター施設に、セキュリティシステム、消火設備および効果的なHVACが備えられていますか。
- **サポート。**すべてのデータセンターにNOCスタッフが年中無休の24時間体制で常駐し、年中無休24時間のテクニカルサポートが提供されていますか。すべてのサポート担当者がユーザーの母国語を流暢に話せますか。コールセンターはどこに置かれていますか。通常の勤務時間帯に連絡が取りやすいように、サポートスタッフはユーザーに近いタイムゾーンに配置されている必要があります。
- **トラブルチケット。**サポートチケットに対する平均応答時間はどれくらいですか。平均チケット応答時間が24時間以内である必要があります。リアルタイムでの応答が理想です。
- **サーバーとネットワークの保守。**サーバー、ネットワーク、電源などの障害が発生したときの平均解決時間はどれくらいですか。管理に定評のあるデータセンタープロバイダーでは、サービスレベル契約条項に、サーバーの修理または交換を4時間以内で実施するというポリシーを記載しています。すべての施設に予備のネットワークと電源システムが用意されていますが、大規模な障害が発生することはまれであり、発生したとしても2～4時間で解決します。

オペレーティングシステム

Flash Media Serverは、WindowsまたはLinuxのオペレーティングシステムにインストールすることができます。

Microsoft® Windows Server 2008 および Windows Server® 2003 Service Pack 2 がサポートされます。Windows へのデプロイメントはLinuxよりもセットアップと管理が容易であり、経験のある管理者も豊富です。

Red Hat Linux 4 または 5.2 にデプロイメントした場合、Windows へのデプロイメントと比較すると、ライブストリームにおけるCPUのパフォーマンスが10～15%向上し、録画済みストリームのCPUパフォーマンスが25～35%向上します。

最新のシステム要件およびオペレーティングシステム要件については、http://www.adobe.com/go/fms_jp をご覧ください。

処理能力の計画とオプション

大規模なFMSデプロイメントを効果的に計画するには、ネットワーク、サーバーハードウェアおよびFMSソフトウェアを最適化する必要があります。

最大限のパフォーマンスを目指した計画

1台のサーバーによるデプロイメントでは、コンテンツの量やサーバーのトラフィックが大幅に増加したり、瞬間的に急増したりすると、すぐに対応できなくなります。1台のサーバーのピークスループットは約700Mbpsに限られており、通常の動作オーバーヘッドのための余裕が残されています。サーバーが限界値に常時達していると、FMSのログに、接続が頻繁に切断されたり拒否されたりしたことが記録されます。帯域幅の要件を計算する方法については、「Calculating Bandwidth Needs for Flash Media Server 3」(英語) (http://www.adobe.com/devnet/flashmediaserver/articles/calculating_bandwidth.html) を参照してください。

分散したデプロイメント

デプロイメントの前に、地域的な分散の可能性を考慮してください。基本のユーザー層が様々な地域に分散している場合、高品質のサービスを維持するために、複数のデータセンターによるデプロイメントが必要になる場合があります。ライブWebサーバーを既に導入している場合は、ユーザーのトラフィックの統計情報を分析してください。既に何らかの分析や市場調査を実施している場合は、それも加味してトラフィックを予測します。

地域の違いが待ち時間に影響し、サービスの低下を招く場合があります。サーバーとクライアントの間の待ち時間が増加すると、スループットの制限が厳しくなり、再バッファの発生が増加する可能性があります。さらに、一部の国では公共のインターネットに対して、ファイアウォールや帯域幅制限、ポートのブロックなど、様々な制限が課せられています。

一般的なデプロイメントは、2～12の任意の地域から構成できます。1つの地域は、米国の東海岸または西海岸のように大きな領域として定義することができます。一部のCDNは全世界に展開していますが、ほとんどのCDNは北米地域、ヨーロッパ地域、アジア太平洋地域など、1つの地域に特化しています。

国際的に展開する理想的な専用サーバープロバイダーまたはコロケーションプロバイダーを探すことは、難しい場合があります。こちらが理解する言語をサポート担当者が話せることと、こちらの勤務時間帯にサポート担当者が対応できることを確認してください。

Flash Media Server は、複数のネットワークカードをサポートして、サーバーの処理能力を高めることができます。通常は、アウトバウンドネットワーク全体の70%が使用可能な帯域幅として分類されます。

帯域幅の要件を計算する場合のガイドラインについては、「Calculating Bandwidth Needs for Flash Media Server 3」(英語) (http://www.adobe.com/devnet/flashmediaserver/articles/calculating_bandwidth.html) を参照してください。

コアプロセスについて

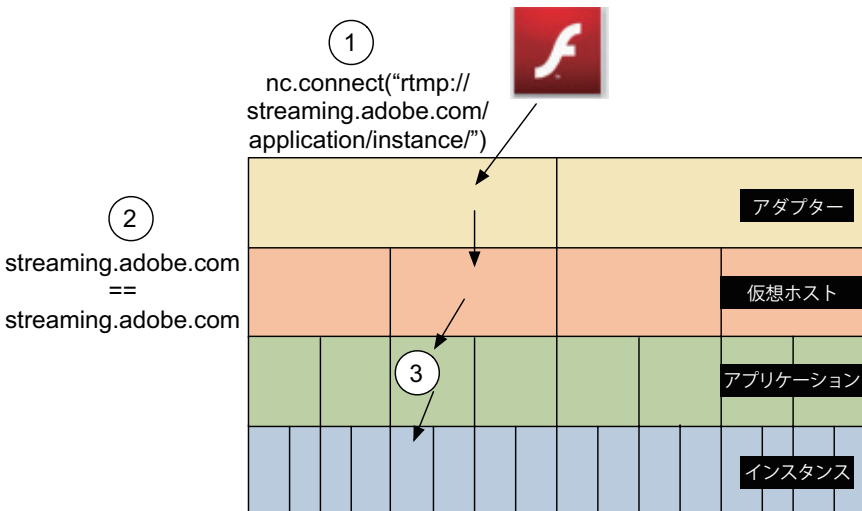
FMS 3.5 は、64 ビットオペレーティングシステム上で 32 ビットモードで動作する 32 ビットプロセスです。サポートファイルの長さは 2 GB を超えており、32 ビットプロセスの一般的なファイルアドレス制限を超過しています。

Flash Media Server では複数のプロセスが動作します。デフォルトのインストール設定では、マスター、エッジ、コア、Admin の 4 つのプロセスが動作しています。マスタープロセスは、必要に応じてコアプロセスを開始する監視機能です。マスタープロセスは一度に 1 つしか実行できませんが、コアプロセスは一度に複数実行できます。

Flash Media Interactive Server 3.5 では、複数のサーバープロセスを柔軟に設定できます。「プロセススコープ」を利用して、Flash Media Server の動作を分散し、サーバーパフォーマンスを最適化し、サービス品質を向上させます。プロセススコープを適切に設定することで、接続処理とメモリ使用状況を効率化するだけでなく、形式が正しくないスクリプトや悪意のある攻撃を切り離すことができます。つまり、1 つのプロセスがクラッシュしても、他のプロセスは影響を受けません。プロセスを分割すると、以下のことが可能になります。

- Flash Media Server が従来より短時間で接続を受諾できるようになります。
- Flash Media Server がより多くのビデオデータおよびオーディオデータを RAM に格納できるようになります。
- メモリの 2 GB の制限が拡張されます。
- 形式が正しくないスクリプトが実行されたときやサービス妨害 (DoS) 攻撃が発生したときに、プロセスを切り離します。

スコープの基本設定は Application.xml ファイルで設定されます。プロセス数、プロセススコープ、プロセスの実行時間、コアプロセスが無効になるまでに許可されるプロセス障害の数を指定できます。プロセススコープには、Adaptor、Vhost、Application、Instance および None の 5 つのオプションがあります。コアプロセスとプロセススコープについて詳しくは、Adobe Flash Media Server 3.5 のテクニカルホワイトペーパー (英語) を参照してください。



VHost の設定は簡単です。FMS コンピューターのアダプターディレクトリの中に、各 VHost に対応する専用ディレクトリが用意されています。各 VHost は、DNS (Domain Name Server) エントリに割り当てるか、サーバーの IP アドレスを指定する WINS (Windows Internet Name Service) アドレスや hosts ファイルなどの名前解決手段に割り当てる必要があります。また、各アダプターにはカスタム VHost ディレクトリだけでなく、_defaultVHost_directory も含まれています。存在しない VHost にクライアントが接続しようとすると、サーバーはそのクライアントと _defaultVHost_ の接続を試行します。

デプロイメントのアーキテクチャ

Flash Media Server では、オリジン／エッジ構成による実質的なプラグアンドプレイのデプロイメントから、オリジン単独クラスターデプロイメントによる、柔軟な設定が可能で堅牢性の高いデプロイメントまで、様々な大規模デプロイメントが可能になっています。

オリジンとエッジについて

使用するネットワークに最適のデプロイメントアーキテクチャを選択するには、まずオリジン／エッジ構成のロードバランシングの基本概念について理解しておくことが重要です。

オリジン／エッジ構成は、企業や小規模 CDN などの大規模な内部デプロイメントに最適なソリューションです。この構成では、あらかじめ実装されているキャッシュ管理機能を利用するため、セットアップが容易です。簡単な設定の変更だけで、Flash Media Interactive Server (FMIS) をエッジサーバー（プロキシとも呼ばれます）として設定することができます。エッジ（プロキシ）構成では、ローカルディスクとメモリキャッシュが自動的に管理されるため、手動で管理する必要がありません。キャッシュはオンデマンドで管理されるため、最も需要の高いメディアセグメントは要求されると即座に提供されます。キャッシュ機能により、応答時間が増加し、待ち時間が減少し、全体的なサービス品質が向上するため、ユーザーとコンテンツの距離が縮まります。

エッジサーバーは、オリジンとして指定された FMIS からキャッシュを構築します。オリジン単独構成（デフォルト）は、中央実行ポイントであり、ファイルストレージを処理します。論理処理とデータ保存は、すべてオリジンで行われます。エッジサーバーはオリジンに接続して、接続、CPU および帯域幅を管理します。例えば、エッジを使用してストリームを数千人のユーザーに再配布することができますが、オリジンへの接続は 1 つのみで済みます。これにより、オリジンを保護し、必要な帯域幅、CPU 負荷およびメモリ使用量を減らします。また、エッジサーバーではカスタム C++ プラグインを使用して認証を管理することもできます。

オリジン／エッジ構成では、複数の場所に置かれたデータセンターがサポートされます。これにより、配信ネットワークの安定性と冗長性が向上します。このような構成は、アップタイム、信頼性、全体的なサービス品質の向上に役立ちます。オリジン／エッジ構成は分散に適した性質を持つことから、フェイルオーバーサーバーを離れた場所に置くことができ、データセンターに大規模な障害が発生した場合でも（停電、自然災害、火災など）、完全にサービスが停止することを避けられます。

オリジン／エッジ構成を使用したライブストリーミングでは、ライブコンテンツの再ブロードキャスト元であるオリジンとエッジサーバーの間に必要な接続が 1 つで済むため、ネットワーク全体の処理能力が向上します。詳しくは、このホワイトペーパーの「デプロイメントのアーキテクチャ」を参照してください。また、オリジンとエッジの接続の詳細とチュートリアルについては、<http://www.adobe.com/jp/support/flashmediaserver/> にある Adobe Flash Media Server 3.5 のドキュメントを参照してください。

オリジン単独クラスター構成のデプロイメントは、サーバーが 1 ～ 2 台のデプロイメントに適しています。また、専門の技術スタッフがサポートする、大規模な CDN デプロイメントにも使用できます。オリジンサーバーは、配信ネットワーク用にカスタマイズされたエッジの役割を実行するために使用できます。この構成を行うには、ロードバランシングやキャッシュの管理など、ネットワークに関する専門知識が必要となります。C++ プラグインやカスタムキャッシュ管理の知識など、Flash Media Interactive Server の動作に関する実用的な知識があれば、FMIS を効率的に拡張するために役立ちます。

オリジン／エッジ構成と同じく、オリジン単独クラスターデプロイメントは、グローバルに確立することも、1 つのデータセンターから確立することもできます。クラスターデプロイメントでは、スマートキャッシングと局所的な配信ポイント（Point of Presence、POP と呼ばれます）を利用して、選択された場所で強化された処理能力を管理することができます。FMIS は様々なサーバーハードウェア構成やプラットフォームで動作し、需要の少ない地域におけるコストを管理するために役立ちます。

オリジン単独クラスターデプロイメントは、非常に小規模のデプロイメントに向いていますが、使用されるキャッシュをきめ細かく制御できるため、大規模なデプロイメントにも推奨されます。

キャッシュはオンデマンドで管理されるので、最も人気のあるメディアセグメントが要求時にすぐに利用可能です。キャッシュは、最終的にコンテンツを視聴者の近くに配置することで、応答時間を短縮し、待ち時間を短くして、全体的なサービス品質を向上させます。

クラスターデプロイメントとエッジ/オリジンデプロイメントの違い

デプロイメントの種類	長所	短所
オリジン/エッジ構成	<ul style="list-style-type: none"> • サーバーは、複数の場所で簡単にデプロイし、相互に接続することができます。 • フェイルオーバー機能を使用して、単一障害点を最小化できます。 • FMS 内部キャッシュを使用します。 	<ul style="list-style-type: none"> • 手動のキャッシュのロードはサポートされていません。 • 大規模な場合には適していません。
オリジン単独クラスター	<ul style="list-style-type: none"> • CDN デプロイメント用に大規模な処理能力を提供できます。 • カスタムのロードバランシングソリューションを作成できます。 • カスタマイズされたサーバーの管理および監視を実装できます。 • カスタムキャッシュコントロールが可能です。 	<ul style="list-style-type: none"> • キャッシュ管理の豊富な知識が必要です。 • C++ やサーバーサイド ActionScript を使用してキャッシュを管理する必要があります。 • 認証の詳しい知識が必要です。

オリジン/エッジ構成の大きな利点の一つは、アドビの効率に優れたキャッシュ管理ソリューションおよびページコレクションソリューションを利用できることです。顧客はこのソリューションを利用して、人気の高いコンテンツをエンドユーザーが入手しやすくなるように設定できます。さらに、この構成では待ち時間が減少し、ディスクアクセスへの依存が減るため、ネットワークをより効率的に使用できます。

オリジン/エッジのサーバー構成では、ネットワーク上の多数のコンピューターにサーバーの負荷を分散することで、パフォーマンスを向上させます。オリジン/エッジデプロイメントでは、クライアントからのすべての接続要求がエッジサーバーにリダイレクトされます。また、大規模なプライベートネットワークをサポートする場合は、この構成を使用してリソースを最大限に活用できます。リモートオフィスにエッジサーバーを配置すると、メディアファイルがエッジのローカルにキャッシュされるため、ストリームが要求されるたびにオリジン（ホスト）サーバーにアクセスする必要がなくなります。

通常、オリジン/エッジデプロイメントは単方向ストリーミングサービスに最適です。リアルタイム通信を行うためにカスタムサーバーサイドアプリケーションを使用している場合は、接続要求はオリジンサーバーに代わってエッジサーバーで厳密に処理されます。その後、クライアント接続がオリジンサーバーにラウンドトリップされ、アプリケーションが実行されます。

エッジサーバーでクライアント要求が受信されると、処理できるタスクを処理した後、他に要求されているデータがあれば、オリジンサーバーに接続します。オリジンサーバーで要求が処理されると、データがエッジサーバーに戻され、さらにそのデータがクライアントに送信されます。クライアント側からは、オリジンサーバーで実行されているアプリケーションに対して直接接続されているように見えます。

エッジサーバーは、接続のオーバーヘッド処理や認証などの管理作業を行う、いわば「交通整理役」として機能し、オリジンサーバーの貴重なシステムリソースやネットワークリソースが浪費されることを防ぎます。接続や接続試行が発生するたびに、その接続を介した実際のストリームデータフロー以外でもリソースが消費されます。接続の数や頻度が増大すると負荷が過度に大きくなり、サーバーのパフォーマンスが低下するおそれがあります。エッジサーバーによって多数のクライアントからの接続を多重化し、オリジンサーバーへの一つの接続に集約することで、負荷が大幅に低減します。エッジサーバーとオリジンサーバー間の通信はすべて、クライアントに対して透過的に行われます。

また、エッジサーバーでは、オリジンサーバーから受信した記録済みのメディアコンテンツをキャッシュに格納し、そのエッジサーバーに接続している他のクライアントにもそのコンテンツを提供することで、オリジンサーバーへの負荷をさらに低減します。

設定の意思決定は、コンテンツのキャッシュに関する知識とスキル、および C++ を使用する能力に基づいて行う必要があります。キャッシュに対するカスタムコントロールが必要ない場合は、エッジサーバーテクノロジーを利用できます。

オリジン／エッジ構成におけるキャッシュの動作

オリジン／エッジ構成では、エッジサーバーでローカルディスクキャッシュが管理され、視聴済みのビデオの一部（セグメント）のみが格納されます。（従来のバージョンの FMS とは異なり）ファイル全体をキャッシュせず、視聴済みのセグメントのみをキャッシュすることで、ディスクキャッシュの管理を効率化しています。キャッシュされたセグメントは、オリジンからプライベート RTMP チャンネルを経由して要求されます。その要求の方法は、HTTP 1.1 のバイト範囲要求と似ています。特に高品質のマルチビットレートビデオを扱う場合、合計ファイルサイズが簡単に 1 GB を超えることがあるため、このような形式のキャッシュ管理が重要となります。このサイズのファイルが送られると、ディスクキャッシュがすぐにいっぱいになります。

例えば、ストリームの再生中に、ストリームの一部（セグメント）がクライアントから要求されたとします。FMS エッジサーバーのメモリ内キャッシュで、そのセグメントが検索されます。キャッシュ内でそのセグメントが見つからなかった場合、ソースファイルからのロードが試行されます。ローカルファイルがエッジサーバー上に存在しない場合には、オリジンにそのファイルが要求されます。その後、エッジサーバーでそのセグメントがセグメントキャッシュに挿入されます。セグメントキャッシュがいっぱいの場合、キャッシュ内のセグメントを削除して新しいセグメントを挿入できるようにします。新しいセグメントを挿入できるだけの領域が確保されるまで、LRU の原則に従ってセグメントが削除されます。LRU とは **Least Recently Used** の略で、「最近、最も使用されていないもの」を意味します。セグメントが現在使用中の場合、削除することはできません。すべてのセグメントが使用中であり、新しいセグメントを追加できるだけの領域が確保できない場合、セグメントのロードは失敗し、そのセグメントを要求したストリームの再生が途中で停止します。

FMS では、ガベージコレクションを利用してセグメントの削除を管理します。FMS の管理者は、ディスクキャッシュのガベージコレクションを管理するために、各エッジサーバーの最大キャッシュサイズを指定できます。FMS でキャッシュサイズがそのサイズに到達すると、原則的に LRU の順序に基づいて、ファイルのガベージコレクションが開始されます。ファイルセグメントは、サブディレクトリ（バケット）にグループ化された後、LRU の順序で並べ替えられます。ガベージコレクションが開始されると、最も古いバケットが最初に削除されます。バケット数は設定でき、デフォルトでは 8 個です。バケットを増やすと、削除がきめ細かく実行されるようになりますが、同時にバケット間でファイルの入れ替えが頻繁に発生するため、ディスクの入出力が増大します。

キャッシュについて詳しくは、このドキュメントの「エッジキャッシュ」を参照してください。

構成のオプション

Flash Media Server の大規模なデプロイメントでは、オリジン／エッジとオリジン単独クラスターという 2 種類の構成を選択できます。

オリジン／エッジ構成

Flash Media Interactive Server には、オリジン／エッジ機能が実装されています。

オリジン／エッジ構成は、企業や小規模 CDN などの組織における大規模なデプロイメントに最適です。多くの場合、実装されているファイルアクセス機能を使用して、発展途上のバックエンドストレージシステムと組み合わせて使用されます。オリジン／エッジのソリューションは、ほとんどの顧客の問題を解決する優れたソリューションです。ただし、顧客がキャッシュの管理に関する高度な知識を持っており、サーバーの負荷をきめ細かく管理することを希望している場合は、オリジン単独クラスターソリューションを採用し、キャッシュ処理およびアクセスコントロール処理を実行するカスタムプラグインと組み合わせることをお勧めします。（大規模なデプロイメントにオリジン単独クラスター構成を使用することは、経験豊富なストリーム管理者または大規模 CDN のみにお勧めします。）

オリジン／エッジ構成の場合、ファイル名の競合を避けるために、すべてのオリジンサーバーおよびエッジサーバーで同一のオペレーティングシステムとディスクフォーマットを使用する必要があります。ファイル名が競合した場合、デプロイメントが壊れる可能性があります。一般的に、エッジサーバーとオリジンサーバーの推奨比率は 5 対 1 です。フェイルオーバー用のオリジンサーバーも実装しておくことをお勧めします。

オリジン／エッジ構成の大きな利点の 1 つは、セットアップが容易なことです。エッジサーバーは、テキストエディターで `vhost.xml` 設定ファイルを編集するだけで設定できます。次の変更を加えます。

1. Mode 設定を探し、値を **remote** に変更します。
2. Anonymous 設定を探し、値を **true** に変更します。この設定により、FMS サーバーが暗黙的なインストールに設定されます。明示的なインストールに設定するには、この値を **false** に設定します。（暗黙的なインストールでは、エンドユーザーに表示される URL を変更する必要がないため、通常は暗黙的なインストールが推奨されます。）
3. RouteEntry 設定を探し、値を変更します。1 つ目の値は、エッジサーバーの仮想サーバー IP アドレスとポートです。2 つ目の値は、オリジンサーバーの仮想サーバー IP アドレスとポートです。例えば、RTMPS プロトコルを使用していて、エッジの仮想 IP アドレスが 10.20.0.0、オリジンの仮想 IP アドレスが 10.234.56.78 の場合、RouteEntry 設定は次のようになります。

```
<RouteEntry>10.20.0.0:443;10.234.56.78:443</RouteEntry>
```

- ローカルエッジキャッシュを有効にするには、CacheDir 設定を探し、その値を **true** に変更します。この設定はオプションです。

オリジン／エッジデプロイメントの設定について詳しくは、Flash Media Server 3.5 のドキュメントを参照してください。

オリジン単独クラスター構成

オリジン単独クラスター構成を使用すると、高度にカスタマイズされたデプロイメントで、管理されたスケールビリティを実現できます。この構成の場合、クライアントのトラフィックを分散するために、ロードバランサーの背後に複数のオリジンサーバーが配置されます。複数のオリジンサーバーを配置することで、信頼性の高いアプリケーションスケーリングが実現します。また、冗長性が高まり、単一障害点をなくすことができます。

オリジン単独クラスターは一般的に、クライアントが特定のアプリケーションインスタンス内から相互に通信する必要がないライブストリーミングや VOD ストリーミングに最適です。クラスター化は、Flash Media Streaming Server または Flash Media Interactive Server を使用して実行できます。

この種の構成では、C++ プラグインを使用して独自のキャッシュ管理ソリューションを開発し、Flash Media Server に実装する必要があります。コンテンツはすべて、内部または遠隔地のストレージに保存されます。ファイル（またはファイルセグメント）を取得してキャッシュするカスタムファイルプラグインを開発することで、コンテンツへのアクセス速度を速めることができます。このソリューションは、堅牢性の高いバックエンドストレージシステムを備えたネットワークに、キャッシュとファイルストレージに関する専門知識を持つ IT スタッフが常駐している場合に適しています。

使用するロードバランサーに応じて FMS の設定に加える調整は変わりますが、必ず調整する基本設定もいくつかあります。それは、アイドル状態の接続を維持する時間（キープアライブ時間）、cookie のサポート、およびルートエントリです。

デフォルトでは、アイドル状態の接続は無期限に維持されます。接続ベースのアプリケーションの場合、通常は無期限に接続を維持する方が有利ですが、大規模なデプロイメントには向いていません。開いている接続を未使用のままにすることは、サーバーリソースの無駄遣いとなるため、アイドル状態の接続は適切な時間内に閉じることをお勧めします。それには、server.xml ファイルを編集します。**AutoCloseIdleClients** を **true** に変更し、**CheckInterval** および **MaxIdleTime** の値をアプリケーションに適した時間に設定します。（最初は 20 に設定しておき、必要に応じて最適なパフォーマンスが出るように調整することをお勧めします。）

オリジン単独クラスターデプロイメントの場合、cookie を使用して個々のユーザーを適切なホストに割り当てる必要があります。その際、セッションを維持するために、FMS の cookie サポートを有効にする必要があります。デフォルトで、FMS の cookie サポートは無効になっています。cookie サポートを有効にするには、adaptor.xml ファイルを開き、**SetCookie** の設定を **true** に変更します。

最後に、クライアントの要求に回答して FMS サーバーから送信される HOST ヘッダーを設定する必要があります。オリジン単独クラスターデプロイメントの場合、このヘッダーにロードバランサーの仮想サーバーの IP アドレスを設定する必要があります。この変更を行うには、vhost.xml ファイルを開き、ロードバランサーの仮想サーバーの IP アドレスとポート番号に合わせて **RouteEntry** の設定を変更します。

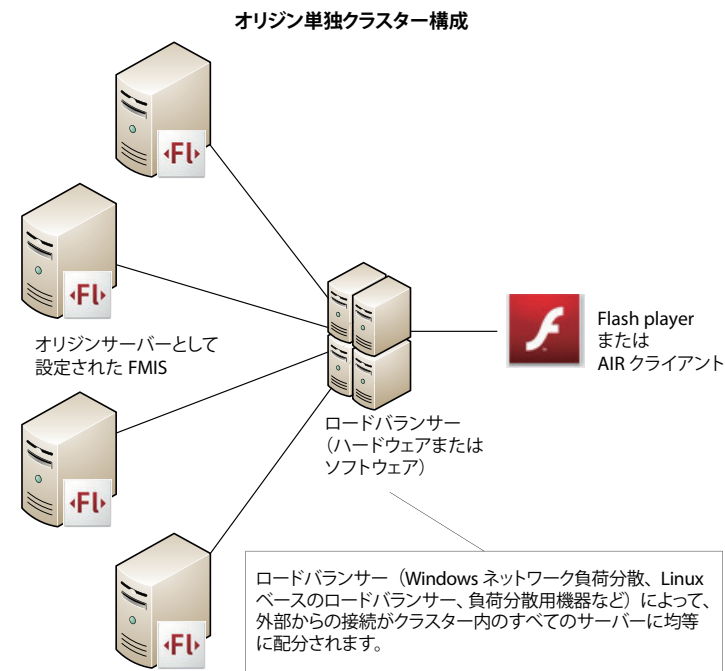
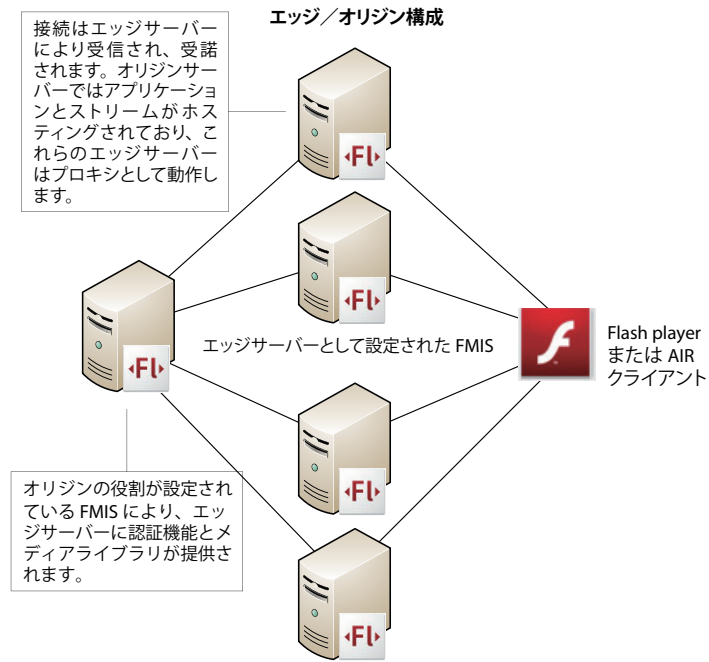
典型的なロードバランシングのアプローチ

DNS ロードバランシングにより、ユーザーの DNS サーバーによって最も近いサーバーに要求を送ることができます。

地域のロードバランシングにより、IP アドレスに相対的なサーバーに対して要求を送ることができます。通常、従業員は共通の DNS サーバーを使用しているので、現在のインターネットではより効果的です。

コンテンツ対応のロードバランシングにより、コンテンツが保存されているサーバーに要求を直接送ることができます。

デプロイメントの比較



複数のテナントの準備

Flash Media Server には、強力な仮想化機能が備えられており、別々のユーザーアカウントを複数準備する作業を簡単に実行することができます。複数のテナントの場合、アプリケーションレベルで準備することをお勧めします。サーバー上の各アプリケーションディレクトリには専用の設定ファイルが格納されているため、各アプリケーションに合わせた設定を定義することができます。また、クライアントアカウントにサーバーアクセス特権がある場合、複数のクライアントアカウントをクライアント自身のアプリケーションに割り当てることをお勧めします。これにより、各クライアントのコンテンツが分離されて安全が確保され、カスタムサーバーサイドコードがサンドボックスに格納されます。それぞれのコアプロセスを特定の数のアプリケーションに制限することで、不正なプロセスによって停止するアプリケーションの数を限定することができます。アプリケーションレイヤーに複数のテナントを設定することにより、次の項目をユーザー単位で制御できるようになります。

- クライアント帯域幅の制限
- プロセススコープ
- 使用可能なプロトコル

アドビでは、複数のテナントをアプリケーションレベルで準備することを推奨します。

- コンテンツ保護 (ACL / SWF 検証 / RTMPE)
- スクリプトの自動ロード
- メモリ割り当て
- 仮想ディレクトリの場所
- キャッシュ
- 最適化
- DVR コントロール
- 共有オブジェクトコントロール

プロセススコープの設定に基づいて、複数のテナントにサーバーリソースを割り当てることもできます。スコープは、顧客のアカウントを準備する方法に応じて選択します。Flash Media Server は、次のスコープでコアプロセスを生成するように設定することができます。

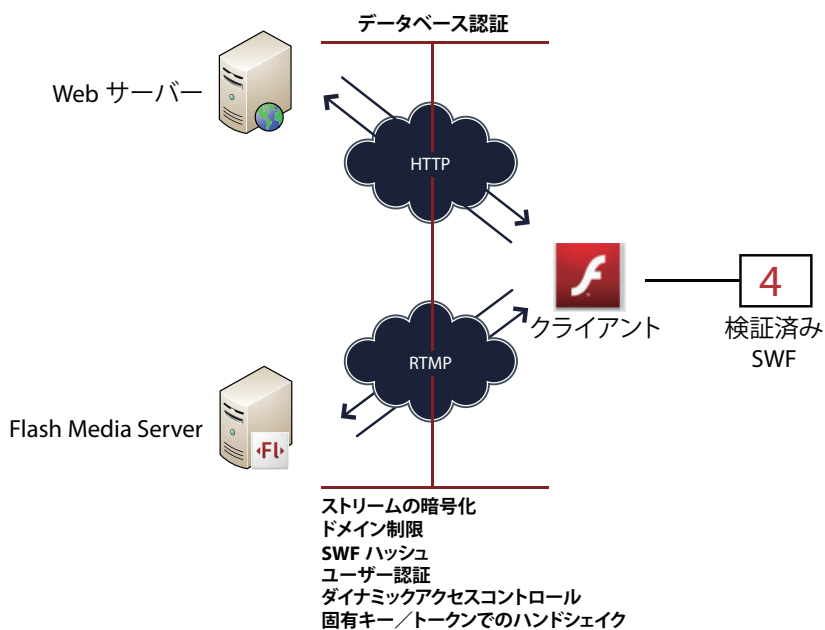
- **Adaptor**. クライアント相互の通信が必要なステート付きのアプリケーション (チャット、ライブビデオ、ゲーム、データ共有ソリューションなど) に最適です。
- **VHost**. 様々なサブドメインのユーザーに固有の設定を適用する場合に役立ちます。
- **Application**. 推奨設定です。各アプリケーションが専用のプロセス内で実行されます。大量のメモリがあり、様々なアプリケーションから多数の接続要求がある場合に役立ちます。
- **Instance**. スコープを最もきめ細かく分散します。

各プロセスで 4 GB もの仮想メモリを使用できるため、あまり多くのプロセスを生成することはお勧めできません。プロセススコープについて詳しくは、Adobe Flash Media Server 3.5 のテクニカルホワイトペーパー (英語) を参照してください。

アクセスコントロールと認証

ストリーミング本来のセキュリティに加えて、Flash Media Server には、きめ細かいアクセスコントロールを可能にする数々の機能が備えられています。次の図表に示すように、様々な手法を利用できます。

Flash Media Server のセキュリティ



詳細情報

プロセススコープについて詳しくは、公式な Flash Media Server 3.5 のホワイトペーパー (英語) (http://www.adobe.com/products/flashmediaserver/pdfs/FlashMediaServer3_WhitePaper_ue_v1.pdf) を参照してください。

アクセスコントロール方法	利点	実装
ファイアウォールおよびポートのフィルタリング	ポートスキャン、サービス妨害 (DoS) 攻撃、総当たりログインスクリプトおよびウイルスを防止します。	サーバーのオペレーティングシステムでファイアウォールまたはポートフィルタリングを使用して、FMS が動作しているサーバーの未使用の TCP ポートをすべてブロックします。
ユーザー名/パスワードの認証	特定のユーザーアクセスレベルの設定およびユーザーアクセスデータの記録が可能です。	ColdFusion や PHP などのバックエンドスクリプトおよび ActionScript を使用して、ユーザーデータベースを検証します。
トークンベースの認証	トークンハンドシェイクに基づく安全な認証を提供します。これは単純なアクセスコントロールソリューションとして利用できます。	Web サービス (SOAP)、Flash Remoting、XML、HTTP POST または単純なファイルアクセスに統合してクライアントを検証します。
アクセスプラグイン	要求を接続前にインターセプトして、サーバーリソースの節約や追加のセキュリティを実現できるようにします。より高いレベルのサーバー条件 (現在接続されているユーザー数など) に基づいて、接続の承諾、拒否またはリダイレクトを行えるようにします。データベースに対する認証も可能です。	アクセスプラグインを開発します。
認証プラグイン	接続後、ただし接続の承諾およびコードの実行が行われる前に、要求をインターセプトします。続いて、接続の承諾、拒否またはリダイレクトを行い、カスタムのサーバーサイド ActionScript 関数を呼び出すことができます。	1 つまたは多数の認証プラグインを開発します。
ドメインのブロック	Flash Media Server のストリームおよびリソースにアクセスするユーザーを厳密に制御します。	アダプター設定ファイルまたは VHost 設定ファイルで、ドメインのホワイトリスト (またはブラックリスト) を作成します。
SWF 検証	許可された SWF への FMS アクセスを制限し、アクセスコンテンツおよびサーバーリソースへの許可されていない試行を防止します。	アプリケーションの Flash Media Server SWF ディレクトリに許可された SWF ファイルを配置し、Application.xml の機能をオンにします。

ファイアウォールとポートフィルタリング

ファイアウォールは、あらゆるサーバー設定において有益な追加機能です。ハッカーの侵入を食い止め、重要なデータへのアクセスを防ぎ、サーバーへの攻撃を防止します。

未使用の TCP ポートをすべてブロックすることが推奨されています。ファイアウォールを使用しない場合、またはファイアウォールへのアクセス権を持っていない場合、Windows と Linux はいずれもポートをフィルタ処理する機能を提供しており、接続を解除してポートスキャナーを阻止することができます。

Flash Media Server に対して開かれるデフォルトのポートは 80、443 および 1935 です。ポート 1111 は、リモートの admin サーバーアクセス用に開いておく必要があります。Windows でターミナルサービスを使用している場合、ポート 3389 を開いておくことは非常に重要です。Linux サーバーでは、ポート 22 を SSH ターミナルアクセス用に開いておく必要があります。その他の一般的なポートには、rsync 用の 873、FTP 用の 20 と 21、SFTP 用の 22 などがあります。

一般的な攻撃には、ポートスキャン、サービス妨害 (DoS) 攻撃、分散サービス妨害 (DDoS) 攻撃、総当たりログインスクリプト、ウイルスなどがあります。これらの攻撃には、基本的なセキュリティ計画で対処できます。

SSAS、アクセスプラグインまたは認証プラグインによるユーザー認証

Flash Media Server 3.5 で利用可能なユーザー認証の手法は、カスタムサーバーサイド ActionScript、アクセスプラグインの記述、認証プラグインの使用などです。

サーバーサイド **ActionScript** により、単純なユーザー名/パスワード、暗号化されたトークン (MD5 ハッシュ) または固有キーを実装できます。さらに、サーバーサイドでは、Web サービス (SOAP)、Flash Remoting、XML、HTTP Post または単純なファイルアクセスを Flash Media Server に組み込んで、送信されるデータに基づいてクライアントを検証することができます。この認証スキームは、ログイン情報をデータベースと照合するだけの簡単なものにすることもできますし、ColdFusion を使用した SSL ベースのトークンシステムを作成するような複雑なものにすることもできます。

アクセスプラグインを使用することにより、要求がサーバーのスクリプト層に到達する前にサーバーへの接続をインターセプトし、ユーザーを認証して、データベースのクエリおよび更新、指定された数の接続のみの受諾、特定のファイルまたはディレクトリに限定されたアクセス許可などのタスクを実行するカスタムロジックを実装します。Flash Media Interactive Server インストールにつき、アクセスプラグインは1つのみです。

認証プラグインは、サーバーイベントへのアクセスを許可します。このプラグインをスタックして、外部からの接続の要求に対して順次処理を実行することができます。接続が確立された後で接続が受諾されなかった場合は、認証プラグインによって、接続の許可のような基本的なロジックだけでなく、地理的な場所やサブスクリプションレベルに対して特別な配信の規則を適用するという複雑なロジックも実装できます。

ドメインまたは IP によるアクセスの制限

許可されていないドメインおよびネットワークでリソースが使用されないようにすることは、サーバーをロックする最初の段階の手順の1つです。デフォルトでは、クライアントはすべてのドメインまたは IP アドレスから Flash Media Server に接続できますが、これにはセキュリティリスクが伴います。アダプター設定ファイルまたは VHost 設定ファイルで、許可されたホスト名、ドメイン名および完全または部分的な IP アドレスのホワイトリストを作成できます。

SWF 検証

SWF 検証は、Flash Media Server 3.5 のセキュリティ機能です。この機能により、どの SWF ファイルに対してサーバーへの接続を許可するかを制御できます。この機能を使用しない場合は、Replay Media Catcher ソフトウェアのような許可されていないクライアント、オープンソース RTMP のクライアントまたはプロキシ、SWF ファイル（適切な接続文字列およびアプリケーション名を指定）が無制限にサーバーに接続できるので、ストリームへのアクセスやサーバーリソースの不正使用が発生します。SWF 検証により、サーバーに接続する権限を持つ特定の SWF ファイルを指定できます。この機能を有効にするには、許可された SWF のコピーを FMS アプリケーションディレクトリに格納して、Application.xml ファイルで機能を有効にするだけです。次に、SWF が接続を試行すると、FMS では接続を受諾する前に、ファイルがアプリケーションディレクトリ内の SWF ファイルの1つと完全に一致するかどうかを検証します。検証データがキャッシュに保持される時間の長さや、許可された SWF ファイルの更新の有無をサーバーが確認する頻度、さらに例外 (Flash Media Live Encoder など) があるかどうかのチェックが行われるようにサーバーを設定できます。

サーバーの状態と監視

Flash Media Server は、サーバーの状態やパフォーマンスを監視する様々な方法を提供します。最も単純なチェックでは以下を検証します。

- サーバーオペレーティングシステムが稼働しているか
- FMS が実行されているか
- 接続が許諾されているか

さらに詳しい状態の確認では、以下の情報を確認します。

- メモリ使用量
- CPU 使用率
- ディスクアクセス
- ネットワークのパフォーマンスおよび使用率
- 現在の接続数
- キャッシュ使用率
- 現在再生中のストリームの数

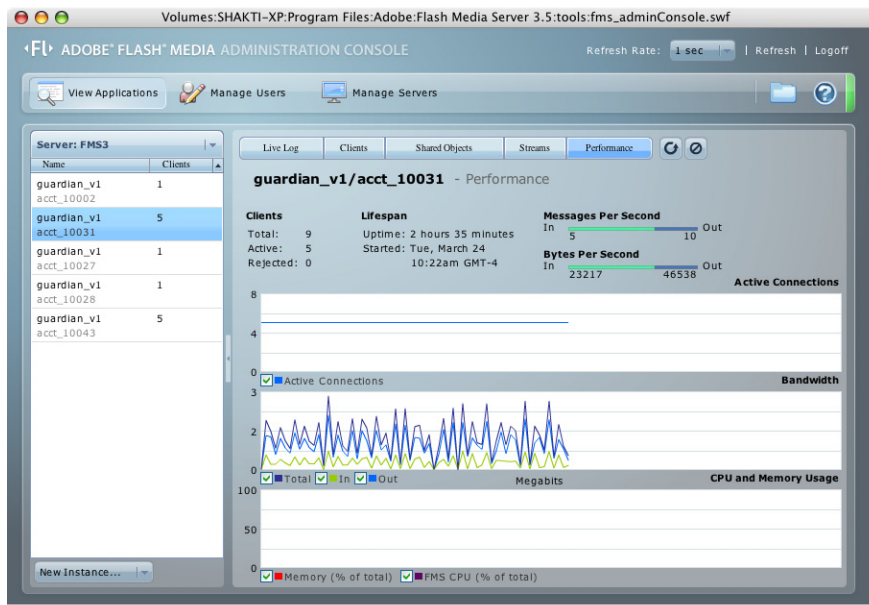
これらのサーバーの詳細は、Administration Console、Administration API、FMSCheck ユーティリティなどのプラグインを使用して参照できます。また、サードパーティソフトウェアを使用して FMS を監視することもできます。Nagios、Zenoss、Groundwork Open Source、Hyperic HQ はすべて、無料のオープンソースです。サポート、追加の機能、トレーニング、限定コンサルティングなどを含む「Enterprise」バージョンも購入できます。これらのアプリケーションは、SNMP クエリー、エージェントアプリケーション、WMI クエリーなど様々な手法を提供します。また、ping の実行でサーバー、アプリケーション、サービスのステータスを追跡し、サーバーの問題を検出した場合はサーバー管理者に自動的に通知します。

大規模な FMS デプロイメントの効率的な管理のために推奨される、標準的なツールもいくつかあります。アクティブディレクトリを使用すると、単一の管理ポリシーでサーバーをすべてまとめることができますので、ネットワーク全体でポリシー変更をすばやく効率的に実施できます。管理インターフェイス、KVM over IP、ターミナルサービス、VNC および SSH コマンドラインはすべて、毎日のサーバー管理に有益なツールです。

プラグイン

Flash Media Server 3.5 の特徴の 1 つは、管理者が保守と管理をより効率的に行うために使用できるプラグインアーキテクチャです。アプリケーションへのアクセスの制限または変更、ストリームおよびサービスのための認証層の作成およびファイル入出力システムの実装を行えるように、C++ プラグインを開発できます。詳しい説明、チュートリアル、サンプルプラグインについては、Flash Media Server 3.5 のドキュメント、またはこのドキュメントで後述する「プラグインについて」セクションを参照してください。

Administration Console



Flash Media Server Administration Console は、サーバーまたは仮想ホストの現在の統計を表示するとき便利な SWF ファイルです。アプリケーションのデバッグに有用なトレースイベントのライブログや、アクティブなクライアント、共有オブジェクト、ストリームのリストも提供します。管理者はパフォーマンスのセクションにより、アクティブな接続、帯域幅の使用量、CPU / メモリの統計についてリアルタイムの統計を参照できます。これらの統計を使用して、サーバーの効率性と使用率を判断することができます。Administration Console は Flash Media Server のインストールに付属しており、任意のコンピュータでローカルに実行でき、Web サーバーでホストできます。Administration API を使用して、デフォルトではポート 1111 で FMS Administration Server に接続します。

Administration API

FMS Administration API は、50 のコマンドで構成されています。これらのコマンドで、FMS の監視、管理および制御を行う独自のカスタム管理ツールを作成できます。カスタムアプリケーションでは、ローカルまたはリモートでアクセスして多数の管理タスクを実行できます。これらのツールは、RTMP または RTMPE（デフォルトのポート 1111 経由）を使用して Adobe Flash Player や Adobe AIR クライアントで、または HTTP を使用して Web クライアントで実行できます。

Administration API を使用すると、管理者アカウントや仮想ホストアカウントの管理、アプリケーションの作成と削除、サーバーの開始と停止、アプリケーションおよびインスタンスのロードとアンロード、ガベージコレクションなどのサーバー機能を実行できます。

Administration API を使用するには、Flash Media Server と Flash Media Administration Server が両方とも実行されている必要があります。詳しくは、『Flash Media Server Administration API Reference』を参照してください。

システムの監視

Nagios:

<http://www.nagios.org>

Zenoss

<http://www.zenoss.com>

Groundwork オープンソース

<http://www.groundworkopensource.com/>

Hyperic HQ:

<http://www.hyperic.com/>

FMSCheck ユーティリティ

FMSCheck ユーティリティは、Windows および Linux で利用できる、スクリプティング可能な無料のコマンドラインツールであり、サーバステータスの確定や問題の診断に使用できます。これはコマンドラインツールなので、スクリプト言語（Cscript、Perl、bash、csh、VBScript、Python など）を使用して任意の自動化システムに統合できます。このユーティリティを使用して、以下のチェックを実行します。

- ストリームのパブリッシュまたは再生
- サーバースイドストリームの再生
- サーバが実行中かどうかの判断
- 現在のサーバ応答時間の測定
- fmscore プロセスが応答していないかを判断
- 1つのアプリケーションのインスタンスに、またはすべてのアクティブなアプリケーションインスタンスに接続

FMSCheck ユーティリティにアクセスするには、コマンドプロンプトから Flash Media Server 3.5 がインストールされている tools サブフォルダーに移動し、以下のように適切なパラメーターを指定して FMSCheck.exe（Linux では ./fmscheck）を呼び出します。

```
fmscheck --host localhost --port 1935 --app myApp --logfile "c:\Program Files\Adobe Flash Media Server 3.5\fmsCheck01.log --play "C:\Program Files\Flash Media Server 3.5\Test.flv" 0 20
```

結果は、FMSCheck ログファイル、または FMS Administration Console で参照できます。FMSCheck ユーティリティの概要および必要なパラメータについて詳しくは、『Flash Media Server 3.5 Configuration and Administration Guide』（英語）を参照してください。

ログファイルについて

Flash Media Server 3.5 には、特定のアプリケーションに合わせて詳細にカスタマイズできる、強力なログ保存機能が用意されています。この機能は、一般的に、課金、サービス品質の監視、トラブルシューティングなどに使用されます。すべてのログファイルは、W3C 拡張ログファイル形式を使用しており、標準的なツールで解析できます。ログのリアルタイムでの参照、ログ分析ツールによる解析またはスプレッドシートプログラムへのファイルのインポートが可能です。

以下に示す 4 種類のログファイルがあります。

- **アクセスログ。** サーバリソースへのアクセスに対するユーザーの要求を追跡します。デフォルトでは、サーバごとに 1 つのアクセスログがありますが、各仮想ホストに応じて設定できます。
- **アプリケーションログ。** 主にアプリケーションのデバッグに使用されます。各アプリケーションインスタンスに対して別個のログファイルが作成されます。
- **診断ログ。** サーバの操作およびプロセスを追跡します。
- **プラグインログ。** メッセージおよびイベントを記録します。

C++ プラグインを使用してカスタムのログ保存を設定することもできます。カスタムログでは、サーバの重要な問題や、クライアントごとの詳細な情報が報告され、さらにはパブリッシュシステム ID が参照されます。

設定ディレクトリのルートレベルに保存された Logger.xml ファイルにより、Flash Media Server ログファイルの設定を制御します。このファイルを編集して、ログ保存するデータ、ログファイルの名前付けの方法、ログファイルの保存先、ローテーションの頻度のすべてを設定できます。ログファイルのデフォルトの場所は、サーバをインストールしたディレクトリ内の logs ディレクトリです（RootInstall/logs）。

Server.xml の Logging セクションでログファイルを有効化または無効化します。Logger.xml には実際のログファイル設定が含まれています。通常のデプロイメントでは、FMS は 1 秒ごとに数ギガバイトのログを生成できるので、堅牢なログ管理システムを処理能力の計画の一部にする必要があります。ログ管理システムは、サードパーティプロバイダーから入手することも、ニーズに合わせて独自に構築することもできます。

プラグインおよびアプリケーションについて

他のビデオ配信テクノロジーではあらかじめブランディングが固定されたプレイヤーを視聴者に表示することのみ可能ですが、Flash プラットフォームでは、多彩なインタラクティブ機能を備える完全にカスタマイズされたインターフェイスを作成できます。また、リアルタイムのデータ共有、サーバーサイドプラグイン、ログ保存および監視アプリケーションプログラミングインターフェイス (API) により、デベロッパーや IT チームが大規模なリッチメディアアプリケーションを開発および管理するためのツールが提供されます。

Flash Media Server のアプリケーションは、クライアント SWF およびサーバー上の関連付けられたサービス、つまりカスタムアプリケーションで構成されます。クライアント SWF は、ブラウザーの Flash Player、デスクトップの AIR、各種デバイス上の Flash Lite で実行できます。FMS には、2 つの構築済みアプリケーションつまりサービスが付属しています。VOD はオンデマンドのビデオ用に、Live はライブブロードキャストに使用されます。これらのサービスにより、すぐに FMS 経由でのストリーミングを開始できます。サーバーサイドプログラミングは必要ありません。Flash Media Interactive Server で、独自のサーバーサイド ActionScript コードを記述してカスタムアプリケーションを作成することもできます。

カスタムアプリケーションに加えて、Flash Media Interactive Server では C++ で記述されたプラグインが提供されます。このプラグインにより、サーバー自体の機能を拡張できます。プラグインはアクセスセキュリティのチェック、コンテンツの地域特定の許可、クライアントに関する統計データの追跡およびネットワークベースのファイル操作を実行します。Flash Media Server 3.5 には、すぐに使用を開始できるように、新しいサンプルのプラグインが付属しています。

一般的に以下のようなケースで使用されます。

C++プラグインの用途	説明
リモートファイルの取得	ネットワーク上のローカルではないファイルにアクセスします。HTTP バイト範囲要求 (セグメント化されたロード) または FTP を使用してソリューションを開発することにより実装できます。
キャッシュ管理	ガベージコレクションの管理およびキャッシュヒットの監視に使用できます。ネットワーク上のエッジでオリジンサーバーのメモリおよびディスクキャッシュを管理することにより、独自のカスタムエッジサーバーの作成にも使用できます。
アクセスコントロール (ACL)	LDAP、アクティブディレクトリ、カスタムプロビジョニング (タイムトークンなど) のソリューションを活用して、ストリームへのアクセスを制限します。
カスタムのログ保存	FMS の基本的なログ機能を拡張し、追加の重要な問題を追跡して、警告やアラームを生成できるようにします。
サーバーの監視	サーバーの状態を確認し、エラーや障害に対処する管理および通知のソリューションを作成します (警告の作成、メモリ管理ルーチンの確立、ルーターへの通知など)。
高度なクライアント/接続の監視	接続レベルでサービス品質を監視および管理します。シークなどの特定のアクション、特定のストリームへのアクセス、ダイナミックストリーミングまたは DVR 最大期間の許可/禁止に使用できます。

プラグインは 3 種類に分類されます。ファイル、認証およびアクセスです。

プラグインの分類	説明
ファイル	FMS とオペレーティングシステムのファイル入出力メカニズムの間で非同期のインターフェイスを提供し、どこでどのようにサーバーがファイルシステムからコンテンツを読み取るかを完全に制御できるようにします。
認証	様々なセキュリティおよび管理者機能、またはサービス品質 (QoS) の監視に使用されます。複数の認証プラグインを使用することができ、これらは順次実行されます。再生の認証、ストリームでのパブリッシュまたはシーク、クライアントの接続/接続解除、サーバーサイド ActionScript でのメソッドの呼び出し、地理的な場所またはサブスクリプションレベルに基づくストリームの配信、特定のストリームへのユーザーアクセスの時間および有効期間の制限などの用途があります。認証プラグインはエッジおよびオリジンのデプロイメントで使用できますが、機能は各ケースで異なります。詳しくは、Flash Media Server に関するドキュメントを参照してください。
アクセス	セキュリティの別の層をサーバーに追加します。コアプロセス (fmscore) で動作する認証プラグインと異なり、アクセスプラグインはエッジプロセス (fmsedge) で動作するので、サーバーのスクリプト層に到着する前に接続をインターセプトできます。サーバーに接続されているユーザー数や帯域幅の使用量、またはユーザーがデータベース内に存在するかなどの基準に従って、接続要求の受諾、拒否またはリダイレクトを行うようにプラグインをコーディングできます。その他の用途には、ファイルおよびフォルダーに対する読み書きアクセスの設定、ビデオビットマップデータへのアクセスの許可およびクライアントプロパティの検査などがあります。サーバーごとにアクセスプラグインが 1 つのみ可能です。

エッジサーバーのアクセスプラグインにより、オリジンサーバーのスクリプト層に到着する前に接続をインターセプトできます。アクセスプラグインは C++ で記述されたサーバープラグインであり、インターセプトした接続を受諾、拒否またはリダイレクトするかを決定します。アクセスプラグイン内に、クライアントの接続要求を処理するためのカスタムロジックを実装できます。例えば、アカウントデータベースでクライアントログインに対するクエリーを実行し、クライアント接続が受諾された後でデータベースレコードを更新するか、または現在接続されている特定の数のクライアントよりも少ない場合のみ、要求を受諾することができます。また、サーバーのファイルおよびフォルダーの読み書きアクセスの設定、オーディオおよびビデオのビットマップデータへのアクセス権限の設定、アクセスプラグインによるクライアントのプロパティの検査を行うこともできます。アクセスプラグインは Flash Media Interactive Server で利用可能ですが、クライアントサイドで Flash Player 6 以降を使用する必要があります。アクセスプラグインは、Flash Media Interactive Server のインストールにつき 1 つのみ許可されます。

認証プラグインも C++ で記述されたサーバープラグインであり、サーバーイベントへのクライアントアクセスを認証します。これらのプラグインは、接続が確立された後、受諾される前に動作します。認証プラグインは以下を実行できます。

- サーバへの接続を許可します。
- サーバからクライアントを切断します。
- 再生、パブリッシュまたはストリーム内のシークを許可します。
- サーバーサイド ActionScript のメソッドを呼び出します。
- 視聴者の現在地、サブスクリプションレベル、ストリームの送信元に基づいて、クライアントにコンテンツを配信します。
- 特定のストリームへのユーザアクセスの時間や接続期間を制限します。
- 論理ストリームパスを物理ストリームパスにマッピングします。例えば、クライアントが「foo.flv」というストリームを要求したものの、このクライアントがサービスのプレミアムメンバーでない場合は、低品質バージョンのコンテンツしか受信できないので「low.flv」をクライアントに提供することが可能です。

アクセスプラグインと異なり、外部からのイベントに対して順次処理が行われるため、複数の認証プラグインを使用できます。例えば、最初のプラグインでクライアント接続を認証し、次のプラグインでは低品質バージョンではなく高解像度バージョンのストリーム再生を認証します。

ストレージとキャッシュ

ファイルのストレージシステムおよびコンテンツのキャッシュの適正な計画は、大規模なデプロイメントの基本です。コンテンツファイルの保存には多数の方法があり、大規模なデプロイメント用のファイル配信アーキテクチャを構築する場合は多くの考慮事項があります。

ストレージオプション

FMS デプロイメント用のコンテンツストレージには、ローカルストレージまたはリモートストレージという 2 つの主要なアプローチがあります。

ローカルストレージでは、FMS のデフォルトストレージを使用するか、または設定ファイルを使用してサーバーやローカルネットワーク上の中央ストレージディレクトリにマッピングします。アプリケーションのメディアファイルは、以下の場所に保存できます。

- デフォルトの `applicationName\streams\instanceName` フォルダー
- `Application.xml` の `<storageDir>` タグで定義される代替りの場所
- `Vhost.xml` または `Application.xml` の `<VirtualDirectory>` タグで定義される追加の場所

これは最も単純なデプロイ方法ですが、FMS で大量のコンテンツをサポートする大規模シナリオでは不十分な場合がよくあります。ローカルストレージは、ユーザーごとのコンテンツの分離に問題があり、柔軟性に乏しく、規模の調整が困難になる傾向が見られます。このような理由から、ほとんどの CDN ではリモートストレージソリューションを採用しています。

リモートストレージは、より堅牢かつ柔軟なアプローチです。このシナリオでは、すべてのサーバーが中央の外部コンテンツリポジトリのコンテンツを要求します。リモートストレージには 2 種類あります。「近く」と「遠く」です。近くのストレージはネットワークドライブとして簡単にマウントできますが、遠くのストレージはデプロイ時にファイルプラグインが必要です。ネットワークでの最適なパフォーマンスのために、ファイルプラグインを微調整することは非常に重要です。重要なベストプラクティスには以下のものがあります。

- スレッドをブロックしません。
- FMS に対するファイルデータの要求および取得をできるだけ迅速に実行します。

- HTTP 範囲要求を使用します。
- データをオンデマンドで提供できるように、可能な限り大量のデータについて大規模な先読みおよびキャッシュをローカルで実行します。

コンテンツストレージおよびファイルプラグインのプログラミングについて詳しくは、Flash Media Server 3.5 のドキュメントを参照してください。

エッジキャッシュ

コンテンツのキャッシュは、最終的な再生環境に重大な影響を与えるので、大規模なデプロイメントの重要な要素です。理想的なキャッシュソリューションは、ネットワーク全体で各サーバーのメモリ内に 100% のコンテンツをキャッシュすることです。もちろん、これは非現実的です。実際の目標は、最も頻繁に要求されるコンテンツを可能な限りエンドユーザーの近くに保存して、ファイルシステムのコンテンツへの要求数を制限することです。

FMS デプロイメントでは、コンテンツを複数のポイントでキャッシュできます。FMS 内のビルトイン FLV キャッシュは、最も基本的なキャッシュポイントであり、既にサーバーメモリに提供されているコンテンツを保存します。これにより、ディスクアクセスの頻度は少なくなります。ただし、サーバーの RAM の総容量および Windows の 32 ビットプロセスの 4 GB の仮想メモリ空間の容量によって効果が左右されます。アプリケーションをコアプロセスに割り当てる方法を設定することにより、FLV キャッシュのパフォーマンスを最適化できます。

FMS で利用可能な次のレベルのキャッシュは、エッジキャッシュです。エッジサーバーでは、ストリームセグメントをエンドユーザーの近くでキャッシュできます。これにより、待ち時間が少なくなり、サービス品質が向上します。ストリームセグメントはサーバーメモリに保存されますが、ディスクに保存するように設定することもできます。エッジキャッシュデプロイメントでは、古いコンテンツをページするためのポリシーを作成する必要があります。ただし、キャッシュのスマリングが発生する場合があります。

オリジン単独キャッシュの処理では、FLV キャッシュを設定する必要があります。さらに、各オリジンサーバーに強力なバックエンドストレージシステムおよび適切に調節されたファイルプラグインが必要です。

メモリ管理

Flash Media Server 3.5 は、キャッシュ動作が強化されており、メモリ管理および全体的なサーバーパフォーマンスを向上させます。サーバーの fms.ini ファイルで SERVER.FLVCACHE_MAXSIZE パラメーターを変更することにより、キャッシュで使用される RAM 容量の上限を設定できます。デフォルト値は 500 MB です。

さらに、キャッシュはファイル全体ではなく、セグメントつまりブロックに基づいているので、キャッシュ動作の効率が大幅に向上します。キャッシュがいっぱいになると、サーバーは、最近最も使用されていないものから順に未使用のブロックを削除します。これらのブロックのサイズは、fms.ini ファイルの APP.DEFAULT_CHUNKSIZE パラメーターで設定できます。大きな値にするほど CPU 使用量が減りますが、狭い帯域幅の接続でクライアントのパフォーマンスが低下し、サーバーのパフォーマンスが低下する可能性があります。例えば、キャッシュサイズが利用可能なメモリよりも大きい場合、またはサーバープロセスが OS メモリの制限を超えている場合は、サーバープロセスが終了することがあります。逆に値を低く設定しすぎると、理論的にすべてのブロックが使用中になり、新しいストリームブロック用に交換できません。このような場合は、新しいセグメントを要求しているストリームの再生が停止します。

メモリ管理の微調整について詳しくは、Flash Media Server のドキュメントを参照してください。

ライブストリーミング

ライブストリーミングは、Flash Media Server の強力な機能ですが、大規模なデプロイメントではいくつか興味深い問題が発生する可能性があります。アドビでは、マルチポイントパブリッシュや LiveStreamCast アプリケーションなど、いくつかのソリューションを提供しています。

受け入れ先

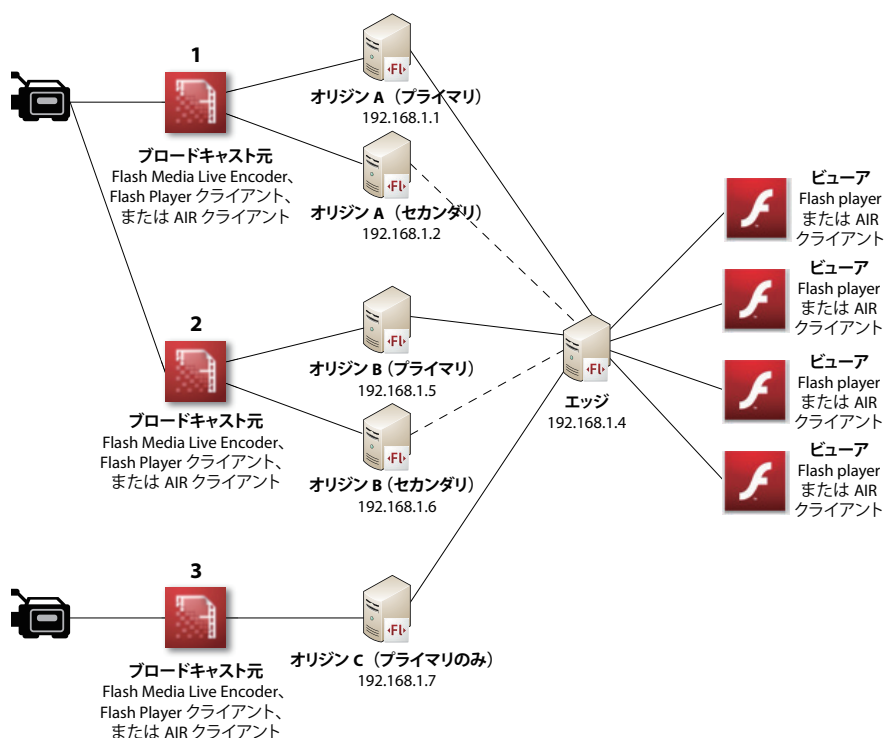
Flash Media Server では、受け入れ先として動作するライブサービスが提供されるので、独自のライブストリームを直ちにブロードキャストできます。カスタムスクリプトやサーバー設定は不要ですこのライブサービスは FMS アプリケーションフォルダーに配置されており、次に示すような ActionScript の接続 URI を使用してアクセスできます。

rtmp://myFMShost.com/live

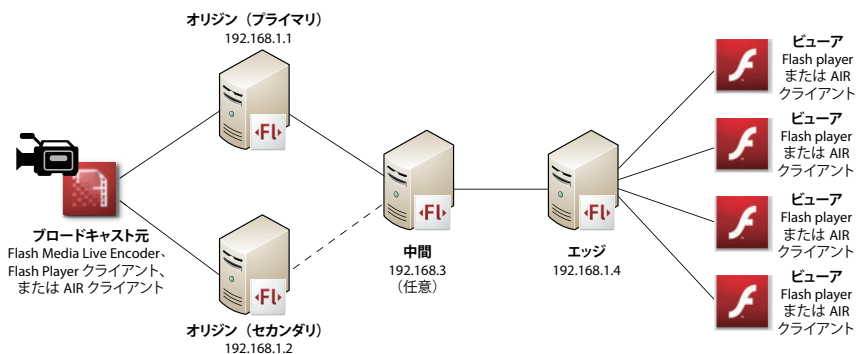
ライブストリームは、Flash Media Server 3.5 経由で Flash Player の PC カメラのソースから、Flash Media Live Encoder から、またはサードパーティのライブエンコーダーからブロードキャストできます。標準のデプロイメントでは、ストリームは FMS で実行されているサーバーにソースから直接送信されます。クライアントは、その同じサーバーに接続してストリームを表示します。したがって、ブロードキャストの規模が制限されるので、大規模なデプロイメントには適していません。ライブブロードキャストの柔軟性とスケーラビリティを向上させるために、Flash Media Interactive Server 3 以降で利用可能なマルチポイントパブリッシュ機能を実装できます。マルチポイントパブリッシュを使用して、Flash Media Server または Flash Media Live Encoder でオリジンサーバーへのフィードを制御できるので、大規模なブロードキャストを処理できます。これにより、ブロードキャスト元はデータメッセージをストリームに組み込むことができ、カスタムアプリケーションを CDN サーバーにデプロイせずにサーバーサイドコードを実装できます。

LiveStreamCast の使用

LiveStreamCast は、Flash Media Interactive Server アプリケーション向けのスケーラビリティをすぐに実現できる、構築済みアプリケーション構造です。オリジンサーバーノード、中間サーバーノードおよびエッジサーバーノードで構成されています。この 3 層構造内の各ノードは、サーバーサイド ActionScript (.asc) で記述された FMS アプリケーションであり、オリジン単独モードで設定された固有の FMS サーバーで動作します。



複数のオリジングループおよび複数のエンコーダーを持つ LiveStreamCast。このシナリオでは、セカンダリオリジンはエンコーダー 1 および 2 から利用可能ですが、エンコーダー 3 からは利用できません。



オプションの中間ノードを持つ LiveStreamCast。このシナリオでは、中間サーバーがエッジサーバーノードアプリケーションと共にインストールされます。エッジノードがプライマリサーバーおよびセカンダリサーバーを同じサーバーとして参照することに注意してください。

ライブアプリケーションスケーリングに伴って複雑さが増すので、NetStream.publish() および NetStream.play() コマンドを使用して直接サブスクライブすることは信頼性が低い可能性があります。LiveStreamCast の分散ノード構造は、サーバーでパブリッシュされるライブストリームをすべて追跡し、パブリッシュ情報をサブスクライバーに渡すことを可能にして、この問題に対処します。これは、大規模なブロードキャストのはるかに効率的で信頼性の高い方法です。次の表では、LiveStreamCast アプリケーション構造の各要素の機能を詳細に説明しています。

ノード	説明	機能
オリジンサーバーノード	このサーバーサイド FMS アプリケーションは、パブリッシャーからビデオストリームを受信し、データを複数の中間サーバーノードに配信します。	パブリッシャーからの接続を受諾し、パブリッシャーのリストを維持することができます。 中間ノードからの接続を受諾し、パブリッシャーが追加または移動されたときに中間ノードに通知します。 中間ノードからの再生コマンドを受諾し、データを中間ノードに配信します。
中間サーバーノード	このサーバーサイド FMS アプリケーションは、オリジンサーバーノードからビデオストリームを受信し、データを複数のエッジサーバーノードに渡します。これは、配信ネットワークの中間層です。	host.ini の設定テーブルからオリジンサーバーの IP を読み取ることができます。 設定テーブル内のすべてのオリジンノードに接続し、接続が解除された場合は再接続します。 オリジンノードからの通知を受信し、各オリジンノードのアクティブなパブリッシャーのリストを維持します。 オリジンノードに対して、再生コマンドの送信およびデータの受信を行います。 接続/ストリームのエラーをエッジノードに報告します。
エッジサーバーノード	このサーバーサイド FMS アプリケーションは、クライアントからの接続要求を受信し、中間サーバーノードのデータをクライアントに配信します。	host.ini の設定テーブルから中間サーバーの IP を読み取ることができます。 設定テーブル内のすべての中間ノードに接続し、接続が解除された場合は再接続します。 中間ノードからの通知を受信し、各中間ノードのアクティブなパブリッシャーのリストを維持します。 中間ノードに対して、再生コマンドの送信およびデータの受信を行います。 接続/ストリームのエラーをエッジノードに報告します。

LiveStreamCast は、www.adobe.com/go/fms_tools/ から無料でダウンロードできます。

コンテンツの保護対策

ストリーミングには固有のコンテンツ保護がありますが、Flash Media Server には追加のセキュリティオプションがあります。

RTMPE のデプロイメントと RTMP の制限

Flash Media Server では暗号化された RTMP (RTMPE) がデフォルトで有効になっているので、証明書进行管理することなく暗号化された接続でストリームを送信できます。安全な 128 ビットの暗号化を提供する RTMPE は、SSL よりも速く簡単なデプロイメントが可能なので、一般的に推奨される暗号化の形式です。(ただし、一部のロードバランサーでは、SSL プロセスをオフロードして FMS マシン全体の暗号化による負荷を軽減することで、SSL をより効率的なオプションにしています。) RTMPE は Flash Player 9 以降でサポートされています。

コンテンツに対してストリームの暗号化を実装するには、アプリケーションへの接続時にプロトコルを指定するだけです。

- SSL
NetConnection.connect("rtmps://yourFMSserver.com");
- トンネリングされた SSL
NetConnection.connect("rtmpts://yourFMSserver.com");
- 暗号化された RTMP
NetConnection.connect("rtmpe://yourFMSserver.com");
- トンネリングされた暗号化 RTMP
NetConnection.connect("rtmpte://yourFMSserver.com");

RTMPE はアダプターレベルで有効化または無効化できますが、エッジサーバーとオリジンサーバー間での暗号化接続には使用できません。

RTMPE を使用するとき標準の RTMP アクセスを無効化して、暗号化されていない接続を禁止することは非常に重要です。

コンテンツ保護リソース

How to protect video content (Flash Media Server) TechNote
<http://www.adobe.com/go/kb405456>

Video content protection measures enabled by FMS 3 Whitepaper
http://www.adobe.com/devnet/flashmediaserver/articles/protecting_video_fms.pdf

SWF 検証

FMS サーバーの別のレベルのセキュリティは、SWF 検証です。この機能は、許可されていないクライアントアプリケーションからコンテンツへのアクセスを防止します。許可された SWF ファイルのコピーはサーバー(またはリモートファイルリポジトリ)に配置され、許可されたファイルのいずれかに一致した SWF ファイルでのみ接続要求が受諾されます。SWF フォルダーの場所、エージェント除外リスト (例えば、Flash Media Live Encoder)、SWF フォルダーのスキャンの間隔および SWF キャッシュの有効期限を設定できます。

SWF 検証のデフォルト設定には、大規模なデプロイメントにおける課題があります。複数のサーバーの複数のアプリケーションに対する許可された SWF ファイルの配信の管理は、困難な作業です。このタスクを単純化するには、server.xml ファイルでグローバルな SWF 検証フォルダーを設定します。または、より迅速な変更を容易にするために、キャッシュの有効期限のデフォルト値を小さくすることを検討します。

1 つの広範なセキュリティリスクであるストリームリッピングにより、視聴者はストリームのデータに直接アクセスして記録できます。RTMPE を SWF 検証と組み合わせて使用することで、ストリームリッピングを防ぐことができます。

トラブルシューティング

問題	説明	解決策
ビデオラグと同期の問題	ビデオが途切れたり処理速度が遅かったりするか、またはオーディオの同期が切れています。	<p>CPU、メモリまたはネットワークの制限値に達している可能性があります。不適切なエンコーディングの実施、過度に高いビットレート、不十分なアプリケーション設計も、ビデオおよびオーディオのラグと非同期化の原因になります。</p> <p>サーバーの CPU の負荷が大きくなった場合、キューに格納する新しいプロセスが徐々に増えて、待ち時間がしだいに大きくなります。マルチコアおよびマルチ層のプロセッサは、シングルコアプロセッサよりもパフォーマンスに優れていますが、すべてのコアの使用率が高い場合に CPU 過負荷が発生する可能性があります。</p> <p>多数の一意のビデオが要求された場合や共有オブジェクトの使用が多くなった場合は、物理メモリの不足が発生してメモリのページングが必要になるので、処理速度が低下して非効率な状態になり、サーバーがクラッシュするおそれもあります。</p> <p>大量のビデオをストリーミングする場合は、ネットワークの制限も問題になります。サーバーのネットワークカードが飽和状態になると、パケットが破棄される場合があります、ストリーミングのパフォーマンスが低下します。複数のネットワークカードを使用することにより、ネットワーク負荷を分散させて、サーバーのストリーミング容量を増加させることができます。</p> <p>適正なエンコーディングの実施は、スムーズなビデオ再生に不可欠です。ビットレートが高すぎると、サーバーまたはクライアントが帯域幅を処理できずに再生が途切れる場合があります。また、固定ビットレート (CBR) を使用した、ビデオストリーミングのエンコードが推奨されています。FMS 3.5 のダイナミックストリーミング機能を使用した場合、視聴者の帯域幅を検出して適切なビットレートでストリームを提供し、さらに現在のネットワーク状況に応じて動的に調整することにより、全体的なサービス品質を向上させることもできます。</p> <p>適正なアプリケーションアーキテクチャは、最適なサーバーパフォーマンスを確実に達成するために重要です。クライアントアプリケーションの不適切なコーディングは、CPU の過度な使用、非効率なメモリ割り当て、および全般的なパフォーマンス低下を引き起こす場合があります。例えば、不要なループを回避し、イベントリスナーを適正に有効化および無効化し、不要になったストリームを閉じることは重要です。</p>
ビデオラグと同期の問題	ライブストリームで数秒間のラグが発生します。	ライブストリームパブリッシュの問題は、一般的にパブリッシャーからサーバーへの不十分な帯域幅が原因です。最速の有線インターネット接続を通じてパブリッシュすることをお勧めします。共有接続は不安定なので、専用の接続であることを確認してください。サーバーの過負荷によって待ち時間が発生する可能性もあります。
ビデオラグと同期の問題	オンデマンドストリームが閉じられたり停止するか、または再生されません。	クライアントの Flash Player のバージョンとのビデオコーデックの互換性を確認してください。H.264 ビデオは、Flash Player 9 以降でのみ再生されます。固有のビデオでのみ失敗が発生する場合は、FLVCheck ユーティリティで検査して、破損していないことを確認してください。このユーティリティは、ビデオのコーデックプロファイルと Flash Player との互換性もチェックします。また、前述したパフォーマンスの低下について考えられる原因もチェックします。

問題	説明	解決策
ビデオラグと同期の問題	一部のビデオ再生で問題が発生し、その他の受信したストリームは正常に再生されます。	FMS 対応アプリケーションを使用するには、少なくともブロードバンド接続が必要です。スムーズなビデオストリーミングおよびビデオチャットへの参加のためには、通常、512 Kbps 以上（ダウンロード時）の速度をお勧めします。 FMS は帯域幅の検出およびダイナミックストリーミングを提供しているため、接続速度が遅い場合はビデオの品質が低くなる可能性があります。つまり、接続速度の異なる様々なユーザーに対応しています。
サーバーのクラッシュ	サーバーがフリーズまたはクラッシュします。	サーバーのクラッシュは、通常、メモリリークまたはメディアファイルの破損によって発生します。サーバーのクラッシュの根本原因を特定するには、まず、すべての FMS ログファイルを検査します。問題が発生した時刻をメモし、問題が発生した時点からサーバーのクラッシュまでログに記録されたイベントを文書化します。オペレーティングシステムのログを調べると、クラッシュの詳細が明らかになります（Windows ではイベントログ、RedHat Linux ディストリビューションでは /var/log/messages）。クラッシュまたはハングのダンプデータを取得することも役に立ちます。Windows では ADPlus (http://support.microsoft.com/kb/28650)、Linux では pstack を使用します。 パフォーマンスデータを収集することによっても、サーバーのハングまたはクラッシュの詳細がわかります。メモリ使用率、CPU 使用率、接続数およびスワップ空間の容量は、いずれも根本原因を特定するのに重要な情報です。障害の原因となった動作またはイベントをすべて文書化します。
サーバーのトラブルシューティング	アプリケーションが応答を停止しました、または接続が確立できません。	まず、FMS Administration Console にログを記録し、アクティブな接続があるかどうかをチェックします。アクティブな接続がある場合は、問題が発生している仮想ホストを再起動します。アクティブな接続がない場合は、仮想ホストの停止および再起動を試行します。問題が解決しない場合は、FMS ログファイルをチェックして、応答のない動作に関する詳細な記録を探します。次に、Windows のイベントログまたは Linux の /var/log/messages をチェックして、拒否された接続の有無を確認し、理由が記録されているかを確認します。接続が拒否される一般的な理由として、リソース制限超過が考えられます。リソース制限超過のエラーは、サーバーの接続数、共有オブジェクト数またはインスタンス数が上限を超えたことを示しています。仮想ホストに制限を設定している場合は、制限の値を大きくする必要があります。アプリケーションログのその他のエラーは、通常、アプリケーション自体の問題、またはユーザーによるアプリケーションへの入力による問題を示しています。アプリケーションのトレース機能や外部ログを使用し、FMS Administration Console でライブトレースフィードバックをチェックします。SWF 検証を使用している場合、この機能が主な原因である場合があります。クライアント SWF が、許可された SWF に一致していることを確認してください。
サーバーのトラブルシューティング	サーバーの応答が遅く、RDP/VNC/SSH が非常に停滞しています。	CPU、メモリおよびネットワークの使用量を確認してください。これらのいずれが高い場合でも、サーバーの処理が遅くなり応答しなくなります。再起動するか、アプリケーションを閉じる必要があります。リソース使用量の高い状態が続く、または急激に上昇してすぐに最大値に達するような場合は、特定の FMS アプリケーションの問題か、関連のない外部プログラムの問題が発生している可能性があります。使用量の高い状態が続くと、最終的にハードウェアにダメージを与える可能性があるため、すぐに調査して問題を解決する必要があります。他のすべての原因が除外された後は、ハードウェアテストが必要な場合もあります。
サーバーのトラブルシューティング	クライアント接続が受諾されていますが、処理が非常に遅いか、または解決されません。	接続の問題が発生するのは、ロードバランサーが適切に動作していない場合や、大量の同時接続要求がある場合などです。クライアントエンドでは、インターネット接続の問題や、ファイアウォールのポートブロックが考えられます。FMS の access.log ファイルでは、接続問題の詳細を参照できます。FMS 3 以降では、ログ保存がデフォルトでオンになっています。また、FMS サーバーステータスの診断ユーティリティ（FMSCheck）は接続問題の診断に便利です。 ActionScript によるイベントハンドラステータスコードのトレースも、接続問題の診断に有用です（AS2 では onStatus、AS3 では netStatus）。また、Ethereal Wireshark、tcpdump、Charles などの接続監視ユーティリティも試してみてください。多くの場合、接続の「長さ」は接続パフォーマンスに影響します。地理的な場所、ホップの数、全体的な待ち時間などがすべて要因になります。RTMP トンネリング（RTMPT）接続は、通常は標準の RTMP 接続よりも遅いことにも注意してください。

アドビへのお問い合わせ

アドビサポートは、デプロイメントに関する専門的な支援を得る機会として非常に有用です。サポートチームへのお問い合わせの際には、以下のガイドラインに従ってください。

- すべてのお客様からのお問い合わせはテクニカルサポートに送られます。
- さらに支援が必要な場合は、Worldwide Escalations Engineer に送られて詳しい分析が行われます。
- アドビのバグ報告システムに問題がログ保存され、エンジニアリングにエスカレートされます。そこで、適切なエンジニアリングの部署によって評価および処理されます。
- 最も高度なレベルの質問は、製品管理の部署によって処理されます。

アドビでは、いくつかのプレミアムサポートプランを提供しています。Bronze、Silver、Gold、Platinum から選択していただけます。機能と価格の詳細を参照する場合、またはアドビのセールスに詳細を問い合わせるには、<http://www.adobe.com/jp/support/programs/> にアクセスしてください。

アドビサポートにお問い合わせの前に、問題に関するできるだけ多くの情報を集めることが重要です。少なくとも、以下の情報を準備してください。

- FMS のバージョンおよび正確なビルド番号
- プラットフォーム、オペレーティングシステムおよびサービスパック (Windows) またはカーネル (Linux)
- FMS に対するシステム要件を満たしていることの確認 (<http://www.adobe.com/jp/products/flashmediainteractive/systemreqs/>)
- 問題の発生場所 (ライブ、VOD またはインタラクティブアプリケーション)

その他に、以下のような質問に答える準備をしておくことも有用です。

- 新規デプロイメントですか、または既存のものですか。
- 最近、その問題の原因となるような変更を行いましたか。
- 設定はどうなっていますか (ロードバランサー、NIC、エッジ/オリジン)
- 問題の再現に必要な手順の詳細はどのようなものですか。

可能であれば、ログファイル、クラッシュまたはハングのダンプ、パフォーマンスデータ、FLA ファイル、クライアント用の ActionScript、サーバーサイド ActionScript、FMS 設定ファイルなどをアドビに提供することも非常に有用です。

用語集

基本の技術的な定義

Adobe AIR : デベロッパーが HTML、AJAX、Flash、Flex などの既存の Web 開発スキルを使用し、リッチなインターネットアプリケーションを構築してデスクトップにデプロイできるようにするための、クロスプラットフォームツールです。

Flash Lite 3 : VP6 および Spark コーデックをサポートするモバイル Flash プレイヤーであり、Flash Media Server への RTMP 接続が可能です。

Flash Media Live Encoder : Flash Media Server に接続する無料の Windows ベースのデスクトップアプリケーションです。ライブビデオおよびオーディオを Flash Player にストリーミングできます。

Flex : Adobe Flex は、Flash Player および AIR で動作する多彩なインターフェイスアプリケーションを作成するための、クロスプラットフォームのオープンソースフレームワークです。これらのアプリケーションは、すべての主要なブラウザおよびオペレーティングシステムで同様に動作します。

Live : Flash Media Live Encoder または Flash Player を使用する Live Flash ストリーミングです。

RTMP (Real Time Message Protocol) : Flash Player のクライアントと Flash Media Server 間の通信に用いる、アドビ独自のプロトコルです。

RTMPE : 暗号化された RTMP です。次世代の RTMP (Real Time Messaging Protocol) であり、SSL 暗号化プロトコルでのセキュリティおよびパフォーマンスを向上させます。

SSL (Secure Sockets Layer) : インターネットでの安全な通信を提供する暗号プロトコルです。SSL は、RTMPS によってストリームおよびデータの暗号化に利用されます。

SWF 検証 : この機能により、管理者はクライアントアプリケーションの検証を目的として、参照 SWF アプリケーションファイルを Flash Media Server に提供します。参照 SWF のバイトコードは、接続要求の送信元のクライアント SWF と比較され、バイトコードが一致した場合は接続が許可されます。バイトコードが一致しない場合、接続は自動的に拒否されます。

FMS コミュニティリソース

FMS Experts

<http://adobe.com/communities/experts/>

FMS User Group

<http://groups.adobe.com/groups/2d1f7135c6/>

Flashcomguru

<http://flashcomguru.com>

FMSGuru

<http://fmsguru.com>

FlashConnections

<http://flashconnections.com>

Flash Media List

<http://flashcomguru.com/flashmedialist/>

詳細情報

サポートパッケージについて詳しくは、<http://www.adobe.com/jp/support/flashmediaserver/> を参照してください。

キャッシュのスミアリング：多数のサーバーでコンテンツの同じ部分が不必要に繰り返された場合に発生します。例えば、10人のユーザーが4GBのビデオを再生しようとして、コンテンツを認識しないロードバランサーにより10台の異なるサーバーに送られたとします。その結果、10台のサーバーでそれぞれ4GBのファイルのコピーを維持する必要があるため、ディスクの総容量の40GBが使用されることになります。これらの10人のユーザーが1台のサーバーに送られた場合は、そのサーバーの4GBのディスク容量だけが使用され、残りの9台のサーバーで合計36GBが節約できます。キャッシュスミアリングにより、無駄なキャッシュ容量が発生し、キャッシュ使用率またはキャッシュの効率性が低下します。

クライアント：Flash Playerで動作するSWF、Adobe AIR、Flash Media Serverに接続するFlash Lite 3です。

構成のオプション：XMLファイルで定義されます。これらのオプションにより、サーバー管理者はFlash Media Serverのパフォーマンスおよび機能を微調整できます。

コーデック：ビデオファイルまたはオーディオファイルをエンコードする形式です。Flashでは、ビデオにはSorenson Spark、On2 VP6-S、On2 VP6-E、H.264コーデックを、オーディオにはNellymoser、MP3、AACを使用します。コーデックは「コードデコード」の略です。特定のコーデックが用いられたビデオを再生するには、プレイヤー上に当該コーデックのデコード機能部分が用意されている必要があります。

コンテンツ：Flash Media Serverからストリーミングされるビデオまたはオーディオのデータです。

コンテンツ配信ネットワーク (CDN)：ストリーミングサービスおよび帯域幅をユーザーに提供する企業です。ユーザーは固有のサーバーをセットアップおよびインストールする必要はありません。

サーバーサイド ActionScript (SSAS)：Javascript 1.5 ベースの言語です。開発者はこの言語を使用し、FMSサーバーの様々な機能を活用して、より高度なレベルの制御を追加できます。通常は、複雑なインタラクティブアプリケーションで機能を拡張するために使用されます。

サービス品質 (QoS)：ストリーム再生パフォーマンスであり、ユーザーの再生環境の質に影響を与えます。

セキュリティオプション：サーバー管理者が効率的にサーバーの安全性を確保するためのFMSのオプションです。このオプションには、SWF検証、ドメインコントロールの参照、RTMPEなどが含まれています。

接続：クライアントにビデオをストリーミング配信する際には、1つの接続が用いられます。複数のクライアントが同時にストリーミングを行うことを、同時接続と呼びます。

デジタル著作権管理 (DRM)：メディアに適用される使用の規則および保護であり、盗用や不正共有を防ぎます。

パブリッシュポイント：ユーザーがビデオやオーディオコンテンツを格納したり、ライブビデオをパブリッシュしたりすることができる、Flash Media Server上のディレクトリです。

ビデオオンデマンド (VOD)：録画済みのFlashビデオストリーミングの配信を表すために使用される用語です。

プラグイン：FMSでは、組み込みのC++ APIを使用してC++プラグインを作成および統合することができます。これにより、サーバー管理者および開発者はFMSの機能を拡張できます。

プロトコル：2つの処理エンドポイント間の通信を可能にする規則または標準です。RTMPは、SWFクライアントとFMSの通信を可能にするプロトコルです。

ポート：アプリケーションまたはプロセス固有の通信エンドポイントです。トランスポートプロトコルでは、どのサービス通信を受信するかを定義できます。FMSはポート1935で通信します。

アドビ システムズ 株式会社
〒141-0032 東京都品川区大崎1-11-2 ゲートシティ大崎 イーストタワー
www.adobe.com/jp
Adobe Systems Incorporated
345 Park Avenue, San Jose, CA 95110-2704 USA
www.adobe.com

Adobe, the Adobe logo, Acrobat, Clearly Adobe Imaging, the Clearly Adobe Imaging logo, Illustrator, ImageReady, Photoshop, and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Mac and Macintosh are trademarks of Apple Computer, Inc., registered in the United States and other countries. PowerPC is a registered trademark of IBM Corporation in the United States. Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2009 Adobe Systems Incorporated. All rights reserved.
Printed in Japan.

91010001 11/09