

App-V セキュリティのベスト プラクティス

**App-V セキュリティのベスト プラクティス**

このドキュメントでは、App-V インフラストラクチャに組み込むセキュリティを設計する際のスタート地点になる情報を管理者に提供します。次のドキュメントでは、現在の App-V で使用可能な推奨されるセキュリティ構成について説明します。

Copyright © 2008 MICROSOFT CORPORATION

[はじめに 4](#_Toc211854592)

[App-V コンポーネントおよびサービス 5](#_Toc211854593)

[App-V インフラストラクチャのコンポーネントの一覧 5](#_Toc211854594)

[作業の前に 8](#_Toc211854595)

[環境のセキュリティ保護 8](#_Toc211854596)

[オペレーティング システム 8](#_Toc211854597)

[SQL Server 8](#_Toc211854598)

[ネットワーク インフラストラクチャ 9](#_Toc211854599)

[Application Virtualization の通信のセキュリティ保護 10](#_Toc211854600)

[サーバー間 10](#_Toc211854601)

[データ ストア 10](#_Toc211854602)

[コンテンツ 10](#_Toc211854603)

[クライアントとサーバー間 11](#_Toc211854604)

[公開の更新 11](#_Toc211854605)

[RTSPS 用の App-V Management Server および Streaming Server の構成 12](#_Toc211854606)

[HTTPS を使用して App-V の運用をサポートする IIS の構成 13](#_Toc211854607)

[App-V Client からパッケージのストリーミング用の Management Server への通信 13](#_Toc211854608)

[Management Console から Management Service への通信 13](#_Toc211854609)

[App-V Server のセキュリティ 14](#_Toc211854610)

[アプリケーション レベルのセキュリティ 14](#_Toc211854611)

[App-V Client のセキュリティ 16](#_Toc211854612)

[承認 16](#_Toc211854613)

[ADM テンプレート 17](#_Toc211854614)

[レジストリ 17](#_Toc211854615)

[クライアントのウイルス スキャン 17](#_Toc211854616)

[移動プロファイル / フォルダのリダイレクト 17](#_Toc211854617)

[App-V シーケンスのセキュリティ 19](#_Toc211854618)

[Sequencer でのウイルス スキャン 19](#_Toc211854619)

[ファイルに対する ACL のキャプチャ (NTFS) 19](#_Toc211854620)

[Sequencer がレジストリ ACL をキャプチャしない 20](#_Toc211854621)

[アプリケーション サービス 21](#_Toc211854622)

[永続的なセキュリティ情報 21](#_Toc211854623)

[インターネット用のシナリオ 22](#_Toc211854624)

[App-V サーバーを ISA の背後に配置 23](#_Toc211854625)

[App-V サーバーを DMZ に配置 24](#_Toc211854626)

[クライアントのインターネット用の考慮事項 26](#_Toc211854627)

[まとめ 27](#_Toc211854628)

# **はじめに**

現在のインフラストラクチャ管理者にとって大きな課題の 1 つは、セキュリティで保護され、かつ生産性が高く、サポート可能な環境をどのように提供するかということです。多くの組織では Microsoft Application Virtualization 4.5 (App-V) の計画と展開を開始しており、インフラストラクチャ管理者にとって、管理および運用タスクのセキュリティ機能とベスト プラクティスを理解することが重要になっています。App-V システムのセキュリティでは、ソフトウェアと、ソフトウェアを運用する環境を適切に設定することが必要です。このドキュメントでは、セキュリティの面から、App-V のさまざまなコンポーネントを構成する方法について説明し、その指針を示します。このドキュメントで説明されているセキュリティの推奨事項を伴わないシステムを展開する前に、管理者はコンポーネントの露出と攻撃にさらされる領域を十分に検討する必要があります。

App-V 4.5 の開発は、次のようなセキュリティ イニシアティブを含む、標準的なマイクロソフト セキュリティ開発ライフサイクルに従っています。

* 信頼できるコンピューティング (TwC)
* Secure Windows Initiative (SWI)
* セキュリティ開発ライフサイクル (SDL)

これらの開発プラクティスおよび設計目標によって、企業でサポート可能な多くの新しい機能とシナリオが提供されています。App-V 4.5 のセキュリティ機能および強化機能には、次のようなものが含まれます。

* インターネット向け機能のサポート。
* Kerberos 認証および承認の採用。
* "既定でのセキュリティ保護" 構成。高度なセキュリティ設定はすべて、標準状態のインストールで既定で設定されます。
* セキュリティで保護されたログ ファイルへのアクセスおよびログ ファイルのサイズの管理。
* App-V Desktop Client に対するセキュリティで保護されたユーザー アクセス許可。
* シーケンス処理の一部としてファイル ベースの ACL をキャプチャ。

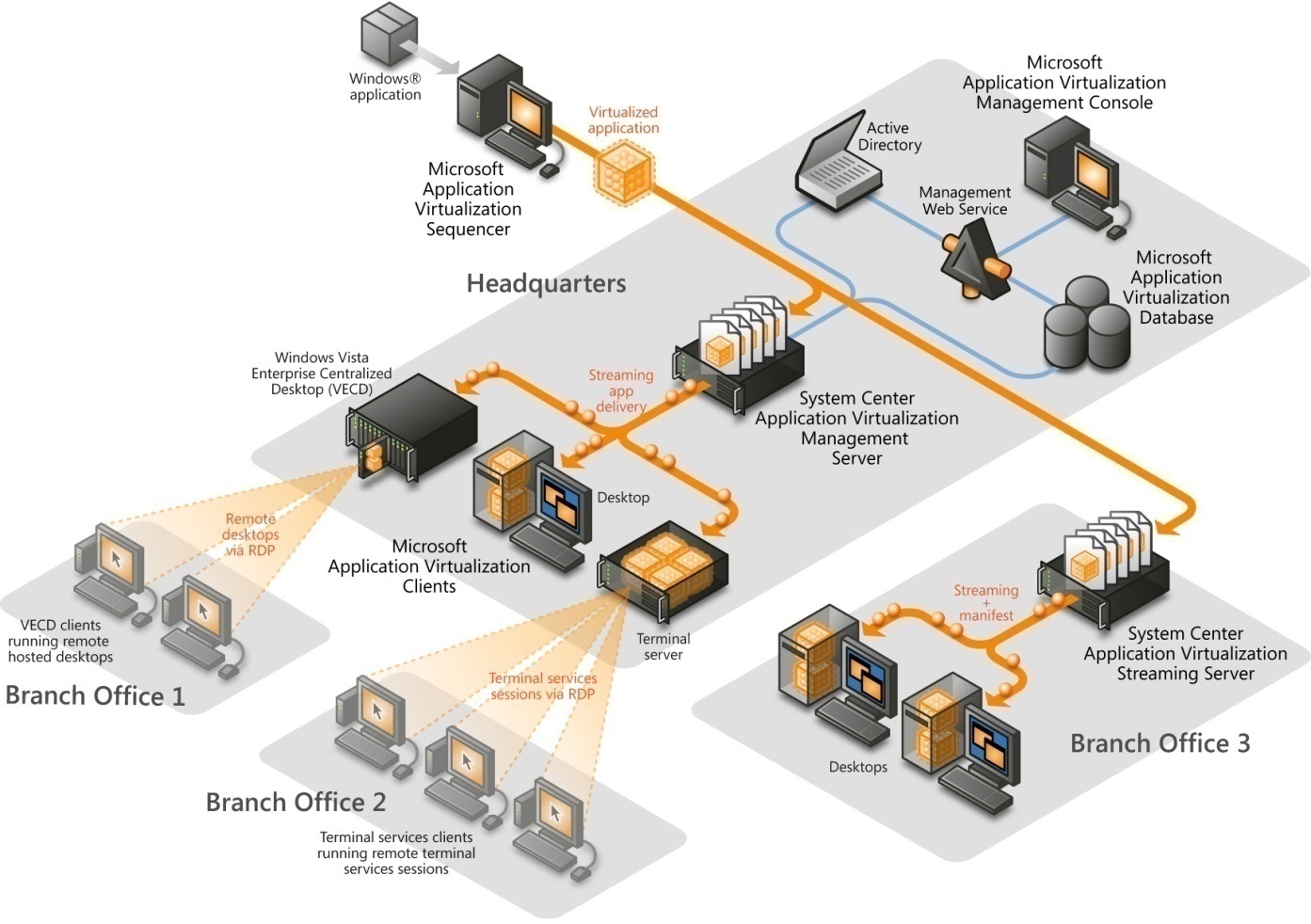
前述の機能および強化機能の多くは、実装するセキュリティ機能を管理者が選択する必要があるか、または選択することができます。これらの機能については後で説明します。このような構成を必要としない機能や、構成できない機能については、このドキュメントでは詳細を説明しません。App-V をセキュリティで保護するための詳細な手順については、『App-V セキュリティ運用ガイド』 (<http://go.microsoft.com/fwlink/?LinkId=127120>) を参照してください。

セキュリティで保護された App-V 環境を実装する際の最も大きな前提条件の 1 つは、サーバーとクライアントとの間でセキュリティで保護された通信を可能にする証明書です。証明書は、App-V インフラストラクチャで行われる多くの種類のネットワーク通信をセキュリティで保護するために使用されます。詳細については、証明書の作成や展開をサポートするための環境設定についてのリンクを参照してください。この作業はよく知られたものであるため、このドキュメントでは App-V に固有の手順について説明します。

## **App-V コンポーネントおよびサービス**

App-V インフラストラクチャをセキュリティで保護するには、この環境を構成するコンポーネントを理解しておく必要があります。この新しいバージョンの App-V (旧 "SoftGrid") では、いくつかのコンポーネントやサービスの名前が変更されています。また、新しいストリーミング専用のサーバーもインフラストラクチャに追加されました。図 1 は、このホワイト ペーパーで説明するコンポーネントを示したものです。

図 1 : App-V インフラストラクチャの図



### App-V インフラストラクチャのコンポーネントの一覧

#### App-V Management Server (旧 Virtual Application Server)

このコンポーネントは、App-V Client へのパッケージ コンテンツのストリーミング、およびショートカットやファイルの種類の関連付けの作成を処理します。

App-V Management Server は、アクティブ アップグレード、ライセンス管理、およびレポート作成に使用できるデータベースをサポートしています。

#### App-V Streaming Server (新規)

このコンポーネントは、ブランチ オフィスなど、クライアントにパッケージ コンテンツをストリーミングする際に Management Server に戻るリンクが許可されない環境で、クライアントへのストリーミング用のパッケージをホストします。

このサーバーには、ストリーミング機能のみが含まれ、Application Virtualization Management Console も、Application Virtualization Management Web Service も提供されません。

#### App-V データ ストア

このコンポーネントは、SQL データベースに格納され、アプリケーション仮想化インフラストラクチャに関する情報を保持します。

このストア内の情報には、すべてのアプリケーション レコード、アプリケーション割り当て、およびアプリケーション仮想化環境の管理を担当するグループが含まれます。

#### App-V Management Service (旧 Management Web Service)

このコンポーネントは、アプリケーション仮想化データ ストアに対する読み取り/書き込み要求の通信を処理します。

このコンポーネントは、App-V Management Server と共にインストールすることも、IIS がインストールされている別のコンピュータにインストールすることもできます。

#### App-V Management Console

App-V Server 管理用の MMC 3.0 スナップイン管理ユーティリティです。

このコンポーネントは、App-V Server と共にインストールすることも、MMC 3.0 と .NET 2.0 がインストールされている別のワークステーションにインストールすることもできます。

#### App-V Sequencer

このコンポーネントは、仮想アプリケーション パッケージを作成するために、アプリケーションのインストールを監視およびキャプチャします。

このコンポーネントの出力は、アプリケーションのアイコン、アプリケーション定義情報が含まれている OSD ファイル、パッケージ マニフェスト ファイル、アプリケーション プログラムのコンテンツ ファイルが含まれている SFT ファイルで構成されます。App-V インフラストラクチャを使用せずにパッケージをインストールするための MSI を作成することもできます。

#### App-V Client

このコンポーネントは、Application Virtualization Desktop Client または Application Virtualization Terminal Services Client にインストールされます。仮想化されたアプリケーション用の仮想環境を提供します。

App-V Client は、キャッシュへのパッケージのストリーミング、公開の更新、および Application Virtualization Server との処理を管理します。

セキュリティで保護された App-V 環境を計画する場合は、複数の異なるインフラストラクチャ モデルが考えられます。これらのモデルでは、前述のコンポーネントのいくつかが使用されますが、すべてのコンポーネントが使用されるわけではありません。App-V インフラストラクチャ モデルの詳細については、『App-V の計画と展開ガイド』 (英語) または『[App-V インフラストラクチャの計画と設計ガイド](http://technet.microsoft.com/en-us/library/bb897450(TechNet.10).aspx)』 (英語) を参照してください。

# **作業の前に**

環境のセキュリティを強化するには、環境内で潜在的な脅威にさらされている部分をすべて調べる必要があります。App-V インフラストラクチャのセキュリティを向上させるには、App-V 固有のセキュリティ機能と、基になるインフラストラクチャの標準的なセキュリティの手法を使用する必要があります。App-V インフラストラクチャでは、アプリケーションの起動に固有にデータ、構成情報、およびその他のセキュリティ関連の機密情報がネットワーク上で送信されるので、中間者攻撃などのセキュリティ上の脅威の影響を受ける可能性があります。App-V によって送信されるデータのセキュリティを確保するには、これらの通信をセキュリティで保護することが必要です。IIS、Active Directory、および SQL などのサービスの基になるインフラストラクチャをセキュリティで保護することによって、App-V インフラストラクチャの全体的なセキュリティが向上します。このドキュメントでは、一般的な指針と、インフラストラクチャのセキュリティ保護の詳細を説明するドキュメントへのリンクを示します。

## **環境のセキュリティ保護**

App-V インフラストラクチャは、以下のコンポーネントに大きく依存しています。

### オペレーティング システム

App-V インフラストラクチャがインストールされるオペレーティング システムを強固にすることは、最も総合的なセキュリティ ソリューションを提供する上で重要な手順です。適切なセキュリティが実装されていない場合、オペレーティング システムが App-V インフラストラクチャの弱点になる可能性があります。オペレーティング システムをセキュリティで保護する作業の多くは、現在の IT の世界では一般的な手法です。サーバーのオペレーティング システムのセキュリティ保護に関する詳細なガイダンスについては、以下の 2 つのガイドを参照してください。

[Window Server 2003 セキュリティ ガイド (英語)](http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en)

[Windows Server 2008 セキュリティ ガイド (英語)](http://www.microsoft.com/downloads/details.aspx?FamilyID=fb8b981f-227c-4af6-a44b-b115696a80ac&displaylang=en)

評価する必要がある一般的なセキュリティの考慮事項には、次のようなものがあります。

* オペレーティング システムの修正プログラムの適用
* サーバーの物理的なセキュリティ保護
* 攻撃にさらされる領域の縮小
* 既定のアクセス許可および権限の使用の縮小
* ファイル サーバーの強化
* Web サーバーの強化

### SQL Server

App-V では、SQL Server を利用して構成や使用状況の情報を格納します。使用環境に App-V をインストールする前に、SQL Server で一般的なセキュリティ強化を実行してください。詳細については、『SQL Server 2005 セキュリティ ベスト プラクティス ガイド (英語)』 (<http://www.microsoft.com/technet/prodtechnol/sql/2005/sql2005secbestpract.mspx>) を参照してください。評価する必要がある一般的なセキュリティの考慮事項には、次のようなものがあります。

* 攻撃にさらされる領域の縮小
* 認証モード
* ネットワーク接続
* サービス アカウントの選択と管理

### ネットワーク インフラストラクチャ

ネットワーク インフラストラクチャのリスクを軽減することは、重要であると同時に、通常は困難な作業です。一般的に、信頼されていないユーザーは、ワイヤードおよびワイヤレス接続によって組織のネットワークにアクセスします。このようなユーザーは、(無意識のうちにであっても) ネットワークや App-V インフラストラクチャに対する潜在的な脅威になります。このガイドでは、ネットワーク インフラストラクチャのセキュリティ保護に関するガイダンスは示しませんが、App-V インフラストラクチャの構成によって、ネットワーク上に存在する脅威を最小限に抑えるためのガイダンスを示します。

### 

# **Application Virtualization の通信のセキュリティ保護**

App-V では、インフラストラクチャのさまざまなコンポーネント間で、複数の種類の通信方法を実装しています。セキュリティを強化する作業では、リスクを評価し、そのリスクを軽減する必要があります。App-V インフラストラクチャを計画するときに、サーバー間の通信およびクライアントとサーバー間の通信をセキュリティで保護することによって、既存のネットワークに存在しているリスクが軽減される場合があります。

## **サーバー間**

### データ ストア

Application Virtualization Management Server および Management Service は、TCP ポート 1433 上で SQL 接続を利用してデータ ストアと通信します。Management Server では、データ ストアを使用してアプリケーションや構成データを取得し、使用状況情報をデータベースに書き込みます。Management Service は、App-V インフラストラクチャを構成する管理者に代わって、データ ストアと通信します。データ ストアには機密情報が格納されているので、このデータに対する脅威を排除することは重要です。

App-V Management Server、Management Service、およびデータ ストアの間の通信を IPSec によってセキュリティで保護することをお勧めします。具体的には、データ ストア (SQL) と Management Server の間、およびデータ ストア (SQL) と Management Service の間の通信チャネルをセキュリティで保護するポリシーを作成します。もう 1 つのオプションとして、IPSec によるサーバーとドメインの分離を展開し、App-V インフラストラクチャのすべてのコンポーネントが、セキュリティで保護されたチャネルでのみ通信するように構成する方法もあります。IPSec の実装の詳細については、以下のリンクを参照してください。

Windows Server 2003

<http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/default.mspx> (英語)

Windows Server 2008

<http://technet.microsoft.com/en-us/library/cc732283.aspx> (英語)

### コンテンツ

App-V Management Server のインストールによって、コンテンツ ディレクトリの場所が構成されます。このディレクトリは、Management Server や Streaming Server がストリーミングするパッケージを取得できるように、仮想化されたアプリケーション パッケージが配置される場所です。この場所はサーバーのローカルに設定することも、リモートのネットワーク共有に配置することもできます。また、SAN ベースの環境を使用している場合は、リモート記憶域という選択肢もあります。したがって、IPSec を実装して、リモートのコンテンツ ディレクトリの場所との通信をセキュリティで保護してください。

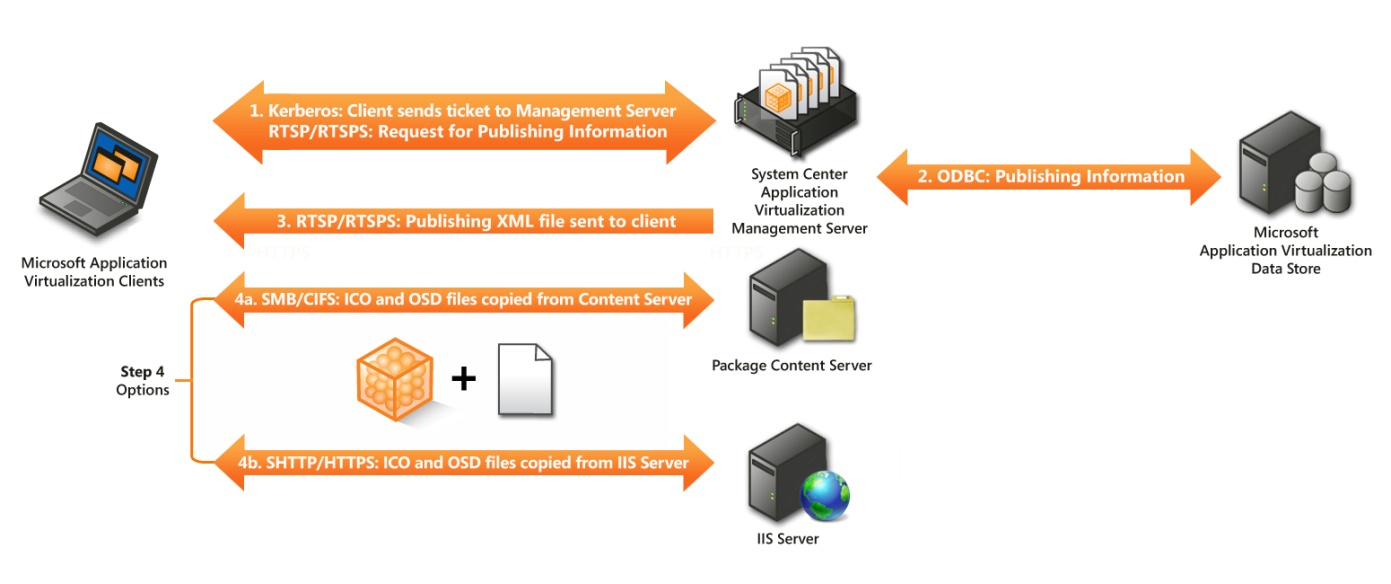
パッケージをクライアントにストリーミングする際のもう 1 つのオプションとして、IIS サーバー上の仮想ディレクトリを使用する方法があります。コンテンツ用に作成された仮想ディレクトリがリモート ソース上に配置されている場合は、IIS サーバーとリモート記憶域の間の通信を IPSec を使用してセキュリティで保護することをお勧めします。

## **クライアントとサーバー間**

### 公開の更新

接続された App-V インフラストラクチャでは、クライアントは、公開の更新を実行するサーバーと通信します。公開の更新は、既定ではユーザーのログオン時に実行されますが、ユーザーが開始することも、一定の時間間隔で実行されるように構成することもできます。公開の更新はログオン ユーザーの資格情報の下で実行され、アプリケーション パッケージに関する情報が適切な公開のためにクライアントに渡されます。App-V Client と App-V Management Server の間で発生する通信をセキュリティで保護し、公開情報がセキュリティで保護されていないチャネルで送信されないようにすることが重要です。公開データは XML ファイル形式で Management Server からクライアントに送信されます。XML ファイルには組み込みのセキュリティはなく、OSD ファイルへのパスが含まれています。この情報が悪用されると、第三者が悪意のある OSD ファイルを使用して、アプリケーションを起動するように App-V クライアントをリダイレクトすることが可能になります。公開の更新は 2 つの手順で実行されます。

図 2 : 公開の更新のトラフィック



1. アプリケーション公開情報を受信します。クライアントは、この情報で、Management Server に対して公開されているアプリケーションの一覧を要求します。この情報が、以下のプロトコルを使用して、XML ファイル形式でクライアントに送信されます。

* RTSP/RTSPS

メモ : RTSPS を使用する場合、トランスポート層セキュリティ (TLS) が使用され、サーバー認証のみがサポートされます。クライアントとサーバーの間での相互証明書認証はサポートされません。クライアントは、セキュリティで保護されたストリーミングのために、サーバーの ID のみを検証します。

* HTTP/HTTPS

メモ : App-V Management Server は、HTTP/HTTPS 上で公開の更新要求を受け付けません。

1. XML ファイル内の公開情報には、ICO ファイルと OSD ファイルの場所が含まれています。これらの情報が、ショートカットとファイルの種類の関連付けを公開するために、以下のプロトコルを使用してクライアントにコピーされます。
   * SMB/CIFS
   * HTTP/HTTPS

公開の更新の最初の手順で、通信をセキュリティで保護するには、RTPS または HTTPS を使用します。最初の手順の通信方法の選択は、公開サーバーをクライアントに追加するときに行われます。2 番目の手順では、SMB/CIFS 共有には IPSec が、Web サーバーには HTTPS が使用されます。2 番目の手順の通信方法の選択は、データベース内でアプリケーション レコードが作成されたときに行われます。

メモ : IIS を使用して ICO ファイルと OSD ファイルを公開する場合は、OSD = TXT の MIME の種類を構成する必要があります。構成されていないと、IIS でこれらのファイルが提供されません。

### RTSPS 用の App-V Management Server および Streaming Server の構成

App-V Management Server や Streaming Server をインストールまたは構成して、強化されたセキュリティ (TLS など) を使用するには、App-V サーバーに X.509 V3 証明書が用意されている必要があります。セキュリティで保護された Management Server や Streaming Server をインストールまたは構成するための準備をするには、いくつかの作業を完了する必要があります。セキュリティで保護された App-V Management Server や Streaming Server の証明書を展開および構成するための技術的な要件を以下に示します。

* **証明書が有効である必要があります。**証明書が有効ではない場合、クライアントは接続を終了します。
* **証明書に適切な拡張キー使用法 (EKU) - サーバー認証 (OID 1.3.6.1.5.5.7.3.1) が含まれている必要があります。**証明書にこの EKU が含まれていない場合、クライアントは接続を終了します。
* **証明書の FQDN がインストール先のサーバーと一致している必要があります。**たとえば、クライアントが RTSPS://Myserver.mycompany.com/content/MyApp.sft を呼び出し、証明書の [発行先] フィールドが Fooserver1.mycompany.com に設定されている場合、myserver.mycompany.com と Fooserver1.mycompany.com が同じサーバーである (同じ IP アドレスに解決される) 場合でも、クライアントはサーバーに接続されず、セッションは終了します。

メモ : App-V をネットワーク負荷分散クラスタで使用する場合、RTSPS をサポートするために、証明書はサブジェクト代替名 (SAN: Subject Alternate Name) を使用して構成されている必要があります。SAN を使用した証明機関の構成および証明書の作成については、<http://support.microsoft.com/kb/931351> を参照してください。

* **クライアント (およびサーバー) はルート CA を信頼する必要があります。**App-V Server に証明書を発行する証明機関 (CA) は、サーバーに接続するクライアントによって信頼されている必要があります。信頼されていない場合、クライアントは接続を終了します。
* **証明書の秘密キーのアクセス許可が、サーバーの App-V Service によるアクセスを許可するように変更されている必要があります。**既定では、App-V Management Server および Streaming Server サービスは、ネットワーク サービス アカウントで実行されます。サーバー上で PKCS#10 が生成されるときに、秘密キーが作成されます。このキーにアクセスできるのは、Local System および Administrators グループだけです。この既定の ACL によって、App-V サーバーはセキュリティで保護された接続を受け付けることができません。秘密キーに対する適切な ACL を構成する詳細な手順については、『App-V セキュリティ運用ガイド』を参照してください。

メモ : 公開キー基盤の構成の詳細については、<http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx> を参照してください。

メモ : 管理者は証明書の有効性を監視して、App-V やその他のサービスに対して発行された証明書の有効期限が切れないようにする必要があります。

### HTTPS を使用して App-V の運用をサポートする IIS の構成

App-V は、特定のインフラストラクチャ構成で IIS サーバーを使用します。HTTPS をサポートするように IIS サーバーを構成する作業は一般的な作業です。詳細については、<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/596cdf5a-c852-4b79-b55a-708e5283ced5.mspx?mfr=true> (英語) を参照してください。

### App-V Client からパッケージのストリーミング用の Management Server への通信

ユーザーが最初にアプリケーションを起動するとき、またはクライアントで自動読み込みパラメータが設定されている場合、アプリケーション パッケージがサーバーからクライアントのキャッシュにストリーミング (移動) されます。この処理では、RTSP/RTSPS、HTTP/HTTPS、および SMB/CIFS プロトコルがサポートされています。クライアントで Application Source Root または OverrideURL の設定が構成されていない限り、使用されるプロトコルは OSD ファイルによって制御されます。

したがって、このドキュメントで既に説明したように、高度なセキュリティを実現するために、RTSPS、HTTPS、および SMB/CIFS 用の IPSec 上で通信が行われるように構成します。使用する通信方法の選択の詳細については、『Application Virtualization システムの計画と展開ガイド』 (<http://go.microsoft.com/fwlink/?LinkId=122063>) を参照してください。

メモ : IIS を使用してパッケージ (SFT ファイル) を公開する場合は、SFT = Binary の MIME の種類を構成する必要があります。構成されていないと、IIS からクライアントにパッケージが提供されません。

### Management Console から Management Service への通信

App-V Management Console によって、管理者はデータ ストアに変更を加えることができます。ただし、Management Console は Management Service を通じて通信する必要があります。したがって、「[HTTPS を使用して App-V の運用をサポートする IIS の構成](#_HTTPS_を使用して_App-V)」で説明したように、Management Console から Management Service への通信で HTTPS を使用するように構成します。

## **App-V Server のセキュリティ**

このドキュメントで既に説明したように、サーバーのインストールでは、既定で最高レベルのセキュリティが設定されます。ただし、一部のコンポーネントは、インストールの一部として構成されていない、基になるインフラストラクチャのコンポーネントに依存しています。以下に示すインストール後の手順を実行することによって、App-V インフラストラクチャのセキュリティが強化されます。

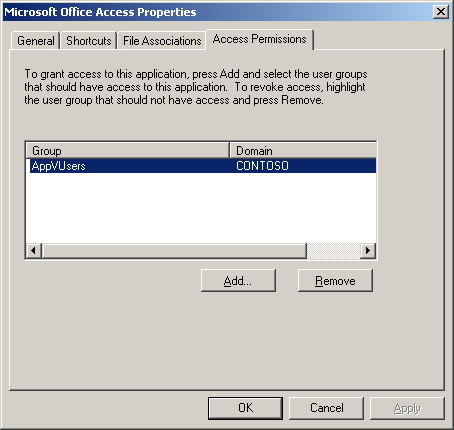
コンテンツ ディレクトリには、クライアントにストリーミングされるすべてのパッケージが格納されます。これらのリソースは、潜在的なセキュリティの脅威を排除するために、できる限り安全である必要があります。

* **UNC ベースの公開やストリーミング :** この場所のアクセス許可は、環境によって最も制限されている必要があります。NTFS のアクセス許可を使用して、コンテンツ ディレクトリに最も制限された ACL を実装します (ユーザー = 読み取り、管理者 = 読み取りおよび書き込み)。
* **公開やストリーミングに IIS を使用 :** Windows 統合認証のみをサポートするように IIS を構成します。IIS サーバーへの匿名アクセス権を削除し、NTFS アクセス許可を使用してディレクトリへのアクセスを制限します。
* **RTSP/RTSPS によるアプリケーション パッケージのストリーミング :** 認証を要求するように App-V プロバイダ ポリシーを構成し、アクセス許可を適用し、必要なグループのみがプロバイダ ポリシーにアクセスできるように構成します。データベース内で適切なアクセス許可を使用してアプリケーションを構成します。

データ ストア内のデータに対する潜在的な脅威を排除し、悪意のあるアプリケーションがインフラストラクチャ内に公開されることを回避するために、App-V 管理者のセットは最小限にとどめるようにします。

## **アプリケーション レベルのセキュリティ**

パッケージ内の個々のアプリケーションに対してアクセス許可を設定できますが、実際にはセキュリティはパッケージ レベルで設定されます。割り当てられていないアプリケーションはユーザーのデスクトップに公開されませんが、ユーザーはパッケージに対するアクセス許可に基づいてそのアプリケーションを実行できます。パッケージ内の一部のアプリケーションに対するアクセス許可しか持たないユーザーが、パッケージ内の他のアプリケーションを起動できるというようなシナリオが考えられます。このような現象が発生するのは、ユーザーがアプリケーション追加のアクセス許可を持っている場合や、クライアント上の管理者である場合です。ユーザーが同じパッケージ内の最低 1 つのアプリケーションへのアクセス権を持っている場合、クライアント上のショートカットを作成または使用して、アクセス権を持っていないアプリケーションを起動できます。



## **App-V Client のセキュリティ**

App-V Client では、以前のバージョンの製品にはなかった多くのセキュリティ強化機能が追加されています。これらの変更は、導入してすぐの状態で、またはクライアント設定の構成によって、最高レベルのセキュリティを実現するために行われました。

既定では、App-V Client には、ユーザーが公開の更新を実行したり、アプリケーションをストリーミングしたりするために必要なアクセス許可のみが構成されています。App-V Client に用意されているその他のセキュリティ強化機能には、次のようなものがあります。

* 既定では、OSD キャッシュの更新は、公開の更新プロセスによってのみ許可されます。
* ログ ファイル (sftlog.txt) は、クライアントへのローカル管理者のアクセス権を持つアカウントによってのみアクセスできます。
* ログ ファイルに最大サイズが設定されました。
* ログ ファイルはアーカイブの設定によって管理されます。
* システム イベントがログに記録されるようになりました。

既定では、クライアントのインストールによって、OSD ファイルの FTA が登録されます。これによって、ユーザーは、公開されたショートカットの代わりに、OSD ファイルから直接アプリケーションを移動できます。クライアント上のアクセス許可がアプリケーション追加のアクセス許可を制限するように設定されているが、ユーザーが管理者である場合、セキュリティに関連するシナリオが現実になる可能性があります。このようなシナリオでは、ユーザーは OSD を電子メールで送信したり、悪意のある OSD を含む Web サイトを閲覧したりすることができます。ユーザーがこの方法で OSD ファイルを開く場合、ユーザーはアプリケーションを起動および追加したり、アプリケーション追加のアクセス許可を迂回することができます。これは、ローカル管理者が、App-V Client 用に設定されたアクセス許可セットを迂回するからです。OSD の FTA について登録を解除するだけで、これを防止できます。また、ユーザーが OSD ファイルを使用してアプリケーションを直接起動する理由がない場合は、この拡張機能を、電子メール システムやクライアントを通じてブロックしたり、ファイアウォールによってブロックしたりすることができます。これらのオプションを構成する作業の詳細については、以下のリンクを参照してください。

[http://support.microsoft.com/kb/837388](http://support.microsoft.com/kb/887620)

### 承認

App-V Client のインストール時に、管理者はキャッシュされたアプリケーションについて承認を要求するようにシステムを構成できます。これは、サーバーからストリーミングされたアプリケーションが、起動の前に App-V インフラストラクチャからの承認を要求することを意味します。ただし、App-V インフラストラクチャが利用できない場合 (App-V インフラストラクチャが停止している場合や、クライアントが App-V インフラストラクチャから分離されている場合)、アプリケーションはパッケージの最後の承認を使用します (これは肯定的な場合と、否定的な場合があります)。App-V インフラストラクチャが利用できなくなる前に、ユーザーがアプリケーションを正常に起動していなかった場合は、App-V インフラストラクチャと通信し、承認を受け取ることができるようになるまで、アプリケーションを起動できません。

RequireAuthorizationIfCached レジストリ設定を (またはセットアップ時にオプションをオフにして) 承認を要求しないように設定することは、インフラストラクチャが利用可能な場合は承認が試行され、結果の承認 (肯定または否定) が適用されることを意味します。App-V インフラストラクチャが利用できない場合は、以前に正常に承認されていたアプリケーションだけではなく、以前にキャッシュされていたすべてのアプリケーションが起動されます。また、ユーザーがアクセス許可によってクライアントをオフライン作業モードに変更するアクセス許可を持っている場合や、ユーザーがローカル管理者である場合は、ユーザーは App-V インフラストラクチャが利用できない場合と同様に、すべてのキャッシュされたパッケージを開くことができます。

### ADM テンプレート

App-V では、グループ ポリシーを通じて最も一般的なクライアント設定を構成するために使用できる ADM テンプレートが導入されています。このテンプレートによって、管理者は集中管理された管理モデルから、多くのクライアント設定を実装したり、変更したりすることができます。ADM テンプレートで利用可能な設定の一部がセキュリティに関連しています。

ADM テンプレートを使用する際の重要な考慮事項の 1 つは、設定がグループ ポリシーのユーザー設定であり、完全に管理されたグループ ポリシーではないという点です。この動作についての理解を深め、組織内で適切にクライアントを展開するために必要な、ADM テンプレートの解説および固有の設定については、App-V ADM テンプレートに関するホワイト ペーパー (<http://go.microsoft.com/fwlink/?LinkId=127120>) を参照してください。

### レジストリ

App-V Client では、レジストリを使用してクライアントの構成を格納します。既定では、キーおよび値は、特権のない (管理者以外の) ユーザーから保護され、ユーザーがキーや値を改ざんしたり、クライアント上のセキュリティ アクセス許可を変更したりすることを防止できます。App-V Client のレジストリ キーの一覧については、<http://go.microsoft.com/fwlink/?LinkID=121528> を参照してください。

メモ : App-V Client のレジストリ キーはすべて HKEY\_LOCAL\_MACHINE ベースであるため、コンピュータ全体に影響します。

### クライアントのウイルス スキャン

App-V Client PC 上で実行されるウイルス対策ソフトウェアでは、仮想環境で実行されている感染したプロセスを検出してレポートすることができます。ただし、ウイルス対策ソフトウェアでは、仮想環境内に存在するファイルのウイルスを削除することはできません。仮想環境でウイルスが検出された場合、ウイルス対策ソフトウェアは構成された操作 (隔離や修復) を実行しようとしますが、その操作はユーザーごとの記憶域で完了し、実際のパッケージには影響しません。ウイルス スキャン ソフトウェアでは、sftfs.fsd ファイルを例外として構成する必要があります。このファイルは、App-V Client 上でパッケージを格納するキャッシュ ファイルです。

メモ : 展開されたアプリケーションやパッケージでウイルスが検出された場合は、ウイルスを含まない置換用のパッケージを作成できるまで、本稼働環境から削除してください。

### 移動プロファイル / フォルダのリダイレクト

App-V では、パッケージに対するユーザー固有の変更は、ユーザーのプロファイルの Application Data 内の usrvol\_sftfs\_v1.pkg ファイルに格納されます。このプロファイルまたはリダイレクトされた Application Data フォルダはクライアントとサーバーの間で送信されるので、クライアントとサーバーの間の通信をセキュリティで保護することが不可欠です。エンドポイント間の通信をセキュリティで保護するための IPSec ポリシーの使用については、このドキュメントの「[データ ストア](#_データ_ストア)」を参照してください。

## **App-V シーケンスのセキュリティ**

App-V 用のアプリケーションのパッケージ化やシーケンスは、通常、App-V インフラストラクチャで最も大きい継続的なタスクです。継続的なタスクとして、アプリケーションのシーケンス時に従うポリシーやプロシージャを作成するときには十分な検討が必要です。

### Sequencer でのウイルス スキャン

推奨される方法は、シーケンス処理時には、Sequencer ワークステーションでウイルス対策ソフトウェアやマルウェア検出ソフトウェアをすべて無効にすることです。この作業は、シーケンス処理を高速化したり、ウイルス対策ソフトウェアやマルウェア対策ソフトウェアのコンポーネントがシーケンス中に検出され、仮想アプリケーション パッケージに含められることを防止したりするために必要です。

従来の方法でソフトウェアをコンピュータ (Sequencer 以外) にインストールし、正常にインストールされた後で、コンピュータのウイルスをスキャンします。ウイルスが検出された場合は、ソフトウェアの製造元に感染しているソース ファイルを通知し、ウイルスの含まれていない更新されたインストール ソースを要求します。必要に応じて、インストール フェーズの後で Sequencer をスキャンして、ウイルスが見つかった場合は、前述のようにソフトウェアの製造元に連絡する必要があります。

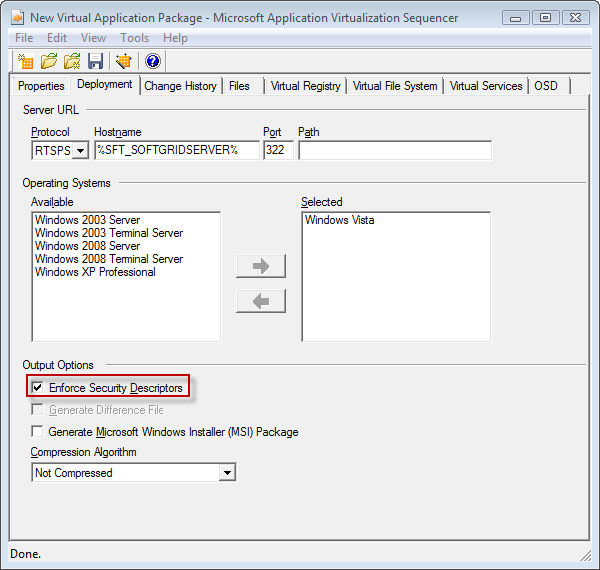
メモ : アプリケーション内でウイルスが検出された場合は、展開しないでください。

### ファイルに対する ACL のキャプチャ (NTFS)

App-V Sequencer は、製品のインストール時に監視されるファイルの NTFS アクセス許可または ACL をキャプチャします。この機能によって、シーケンス担当のエンジニアは、アプリケーションをローカルにインストールし、仮想化していない場合と同様に、アプリケーションの動作をより正確にキャプチャすることができます。一部のシナリオでは、アプリケーション ファイル内でユーザーがアクセスすることを想定していない情報を、アプリケーションが格納する場合があります。アプリケーションは、アプリケーション内部のファイルに資格情報を格納する場合があります。パッケージに ACL が適用されていない場合、ユーザーがこの情報を表示し、アプリケーションの外部で使用する可能性があります。

メモ : セキュリティ固有の情報を格納するアプリケーションは、仮想化するアプリケーションとして最適ではありません。多くのアプリケーションがこのような処理を行うので、これらの場所をセキュリティで保護することは、このデータのセキュリティを確保することになります。

インストール フェーズで、シーケンス担当エンジニアは、必要に応じてファイルの既定のアクセス許可を変更できます。シーケンス処理が完了した後、パッケージを保存する前に、シーケンス担当エンジニアは、アプリケーションのインストール時にキャプチャされるセキュリティ記述子を適用するかどうかを選択できます。実行するアプリケーションを正しく仮想化するために他に方法がない場合を除いて、セキュリティ記述子を適用することをお勧めします。



App-V のこのリリース以前は、シーケンス処理の一部として ACL はキャプチャされていませんでした。このため、通常は管理者特権を必要とする特定のアプリケーションを、低い特権のユーザーとして実行することができました。App-V のこの新しい機能では、アプリケーションは従来のインストールと同様に実行され、アプリケーション開発者によって組み込まれたセキュリティに準拠することができます。

### Sequencer がレジストリ ACL をキャプチャしない

Sequencer はシーケンスの監視インストール フェーズで NTFS の ACL をキャプチャしますが、レジストリの ACL はキャプチャしません。ユーザーは、サービス以外の仮想アプリケーションのすべてのレジストリ キーに対してフル アクセス権を持ちます。ただし、ユーザーが仮想アプリケーションのレジストリを変更しても、その変更は固有のストア (uservol\_sftfs\_v1.pkg) に格納され、他のユーザーには影響しません。

### アプリケーション サービス

App-V では、仮想化されたアプリケーションの一部であるアプリケーション サービスをサポートしています。シーケンス処理中にアプリケーション サービスを仮想化できますが、仮想環境でアプリケーション サービスを実行できるセキュリティ コンテキストは制限されます。仮想環境でサポートされているセキュリティ コンテキストは、Local System、Local Service、または Network Service だけです。シーケンス処理中に、アプリケーション サービスについて、サポートされている 3 つ以外のセキュリティ コンテキストが指定されている場合、仮想環境では Local System セキュリティ コンテキストが適用されます。アプリケーション サービスが Local Service または Network Service を使用するように構成されている場合は、仮想環境でもこれらのセキュリティ コンテキストが使用されます。サービス アカウントの構成は、シーケンス処理中にこの 3 つのセキュリティ コンテキストを使用して実行できます。

### 永続的なセキュリティ情報

アプリケーションをシーケンスするときに、シーケンス担当エンジニアは、ユーザーが実行するようにアプリケーションをインストールすることも、監視しながらアプリケーションをインストールするための自動化された方法を開発することもできます。シーケンスのこのフェーズでは、パッケージから除外されているすべてのものが、パッケージの一部としてキャプチャされます。これは、アプリケーションを仮想化して実行するのに必要なアセットが含まれるようにするためです。一部のアプリケーションでは、インストール中に重要なセキュリティ情報 (パスワードなど) が格納されます。セキュリティ情報が保護されていない状態のままであると、パッケージにアクセスできる他のユーザーによってアクセスされる場合があります。インストール中に、アプリケーションのインストール プログラムによってパスワードやその他の重要なセキュリティ情報を要求される場合は、マニュアルを調べて、永続的ではない (インストール後に削除される) こと、または永続的である場合は保護される (暗号化される) ことを確認します。

## **インターネット用のシナリオ**

App-V 4.5 はインターネット用のサーバーのシナリオをサポートしており、企業ネットワークに接続していないユーザーや、企業ネットワーク外部のユーザーも App-V を使用できます。以下のシナリオは、セキュリティに関して最善の選択肢を示しています。

App-V のインターネット用インフラストラクチャは、このドキュメントで既に説明したセキュリティで保護された接続上でサポートされます。いずれのシナリオをサポートする場合でも、Management Server 上の RTSPS と、IIS サーバー上の HTTPS の両方が必要です。RTSPS は、インターネット ベースのクライアントについて公開の更新をサポートすると共に、必要に応じてアプリケーション パッケージのストリーミングもサポートできます。HTTPS はクライアントへの ICO ファイルと OSD ファイルのコピーをサポートし、必要に応じてアプリケーション パッケージのストリーミングをサポートします。パッケージのストリーミングに RTSPS と HTTPS のいずれを使用するかは、環境で必要な機能と、目的のパフォーマンスによって決まります。RTSPS は一部の環境で必要になるアクティブ アップグレードをサポートしています。一方、HTTPS はクライアント数が多い場合のパフォーマンスが RTSPS よりもよくなります。組織のセキュリティの要件を適切にサポートするには、Management Server を IIS サーバーから分離することをお勧めします。

メモ : App-V のインターネット用のシナリオで、RTSP または HTTP を使用することはサポートされていません。インターネット上の通信チャネルがセキュリティで保護されていない場合、中間者攻撃を受ける可能性があるからです。

インターネット ベースのクライアント用に App-V インフラストラクチャを設定する場合は、次の 2 つのシナリオをお勧めします。

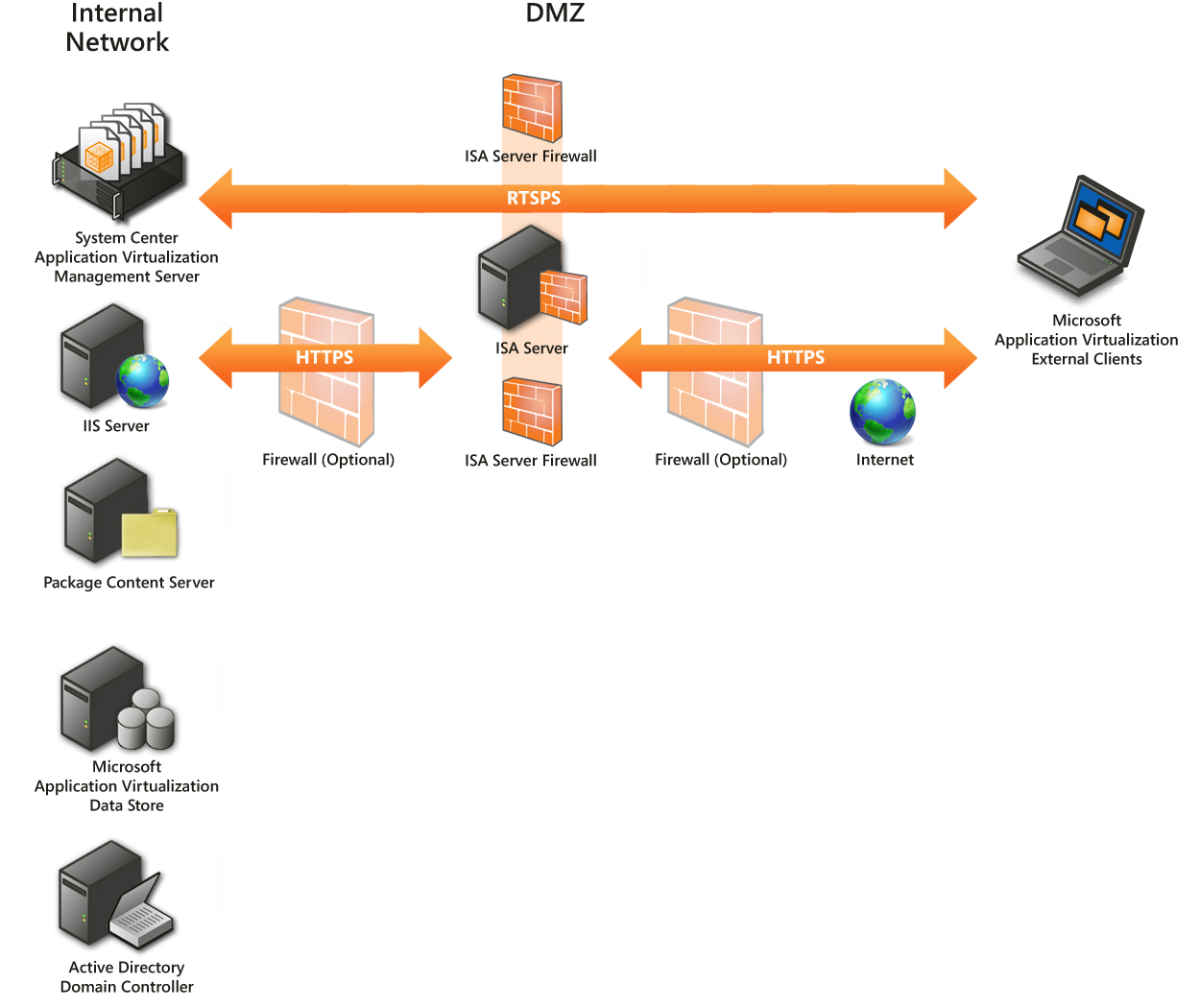
* App-V サーバーを ISA の背後に配置
* App-V サーバーを DMZ に配置

### App-V サーバーを ISA の背後に配置

このシナリオは、インターネット用サーバーをサポートするのに最適なセキュリティ ソリューションです。ISA のリバース プロキシ機能やサーバー公開機能を使用することによって、管理者は App-V サーバー インフラストラクチャ全体を企業ネットワーク内部で保守管理できます。これによって、すべてのユーザー (内部ユーザーとインターネット ベースのユーザーの両方) が、同じ App-V サーバーにアクセスできます。その結果、インフラストラクチャを保守管理するための管理者の負担が軽減されます。ISA のリバース プロキシ機能やサーバー公開機能によって、インターネットからのトラフィックを ISA サーバーで受信でき、ISA サーバーは企業インフラストラクチャ内で要求を完了します。

このシナリオでは、ISA サーバーがインターネットからの RTSPS と HTTPS の両方のトラフィックを受信でき、内部ネットワークに対して RTSPS および HTTPS の要求を実行できることが必要です。ISA サーバーの前後で追加のファイアウォール機器を使用する場合は、アクセスを可能にするために適切なプロトコルやアドレスを指定する必要があります。

図 3 : ISA の背後の App-V サーバー



### App-V サーバーを DMZ に配置

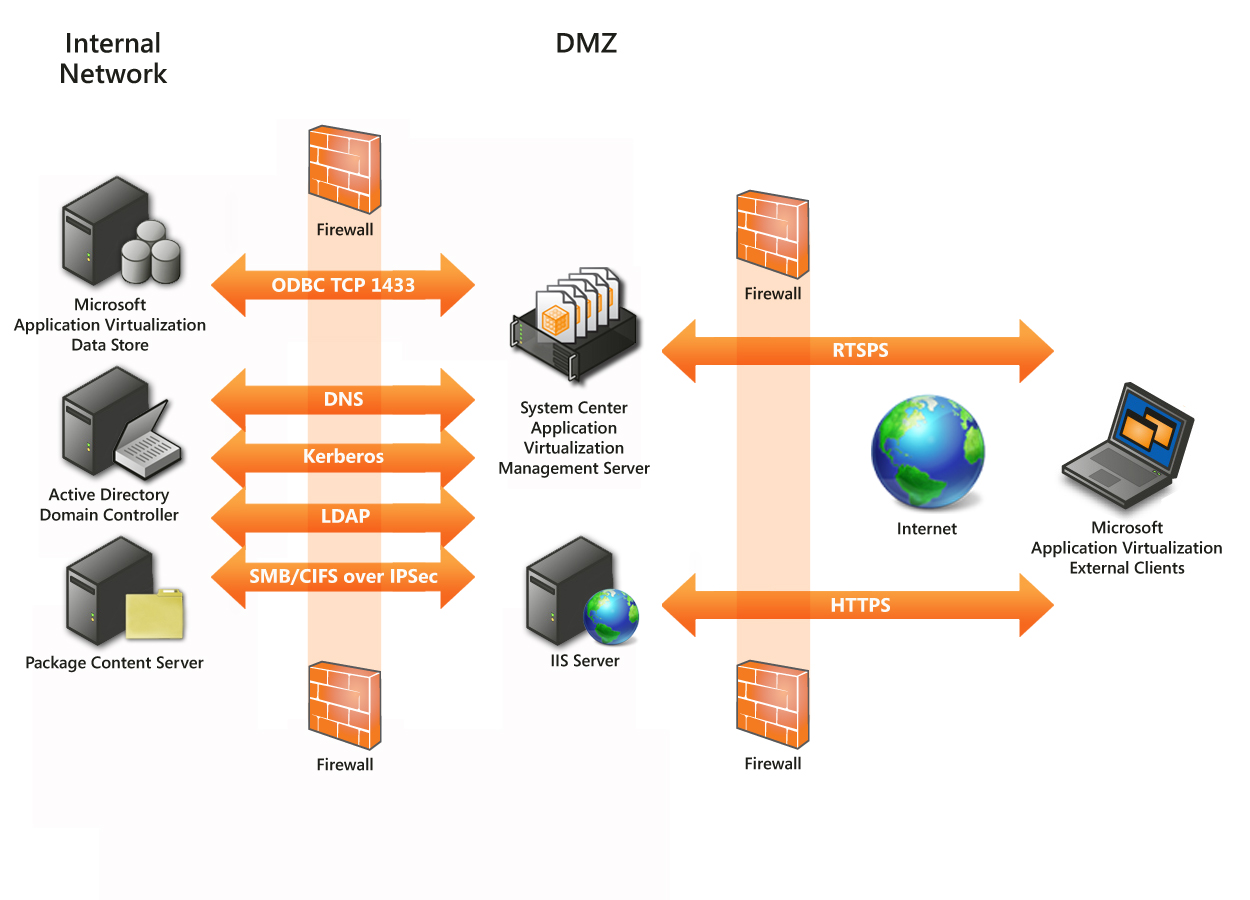
もう 1 つのシナリオでは、App-V Management Servers を DMZ 内に配置します。Management Server と IIS サーバーをサポートするには、公開およびストリーミング用のプロトコルである RTSPS と HTTPS を、インターネットから DMZ への方向で許可する必要があります。また、Management Server と IIS サーバーをサポートするインフラストラクチャ関連のトラフィックを、DMZ から内部ネットワークへの方向で許可する必要があります。このシナリオでは、DMZ から内部ネットワークへのトラフィックが正しく構成されていることを確認するために、管理者の負担が増加します。

この環境のもう 1 つの問題は、Management Server と IIS サーバーが DMZ にある場合、内部のクライアント コンピュータが DMZ にアクセスできるようにしたり、内部ネットワークに追加の App-V インフラストラクチャ サーバーを配置したりする必要があることです。これによって、App-V ソリューションの管理の負担が増加します。ただし、ISA サーバーのない環境では、これが最適なソリューションです。

**DMZ から内部ネットワークに対して必要なトラフィック**

* SQL
* コンテンツ ディレクトリが内部ネットワークにある場合は SMB/CIFS
* Kerberos
* DNS
* LDAP

図 4 : DMZ 内の App-V Management Server および IIS Server



## **クライアントのインターネット用の考慮事項**

**ドメインに参加しているクライアント**

内部ネットワーク上のユーザーは、App-V インフラストラクチャのすべてのコンポーネントにアクセスできます。ユーザーが内部ネットワークから離れると、一部のサービスは利用できなくなります。既定では、App-V Client は、認証と承認のために Active Directory によって発行された Kerberos チケットを使用します。多くのインフラストラクチャでは、インターネット ユーザーがこの操作を実行できるように、インターネット上にドメイン コントローラを配置することはありません。クライアントは、チケットが認証および承認で有効である間は (既定では 10 時間)、Active Directory から発行されたチケットを使用します。ユーザーが Active Directory から切断されている間にチケットの有効期限が切れ、ユーザーはチケットを更新することができない場合は、App-V Client はキャッシュされた資格情報を使用して NTLM 認証に戻ります。

**ドメインに参加していないクライアント**

App-V Client が機能するために、Active Directory によって管理する必要はありません。このため、組織は App-V を使用して、パートナー組織に仮想化されたアプリケーションを提供したり、マネージ サービスの一部として仮想化されたアプリケーションを提供したり、ドメイン管理されていないコンピュータをサポートしたりすることができます。ユーザーが自宅勤務の従業員であり、そのコンピュータが企業のドメインに参加していない場合でも、App-V でこのようなユーザーにアプリケーションを配布できます。ユーザーを認証および承認して、公開の更新を実行したり、アプリケーションをストリーミングしたりできるようにするには、App-V 環境にアクセスできるコンピュータ上にそのユーザーのユーザー名とパスワードを "格納" し、アプリケーションに対する適切なアクセス許可を付与する手順を実行する必要があります。

# **まとめ**

このドキュメントでは、セキュリティで保護された App-V インフラストラクチャを設計するための概念とガイダンスを示しました。実装の詳細については、『App-V セキュリティ運用ガイド』を参照してください。