# BigFix
# はじめに

# Special notice

Before using this information and the product it supports, read the information in Notices (on page 40).

# Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

# 目次

# 第 1 章. 概要

BigFix は、コンプライアンス、エンドポイント、およびセキュリティーの管理について、迅速かつ直感的なソリューションを提供する製品スイートです。この製品により、組織は単一のインフラストラクチャー、単一のコンソール、および単一の種類のエージェントを使用して、物理エンドポイントと仮想エンドポイントの表示および管理を行うことができます。

BigFix は、以下の機能を提供します。

- 連続的なエンドポイント自己アセスメントおよびポリシー実施のための単一のインテリジェント・エージェント。
- 単一の管理コンソールからの、リアルタイムの可視性と制御。
- 位置、接続タイプ、または状況と関係なしに、何十万ものエンドポイントを管理。
- 正確なタイプのエンドポイント構成またはユーザーの種類を、特定アクションの目標として設定。
- 複雑性とコストの削減、正確性の改善、および生産性向上の管理。
- パッチ管理、ソフトウェア配布、および OS デプロイメント。
- 異機種混合のプラットフォームのサポート。
- モバイル・デバイスの管理。
- 米国連邦情報・技術局 (NIST) の標準に基づく自動エンドポイント・アセスメントおよび脆弱性修復。
- マルウェアその他の脆弱性からのリアルタイム保護。
- サーバー自動化。

ビジネスと環境のニーズに応じて、このスイートに属する特定の製品のライセンスを購入し、これらの機能の一部またはすべてを選択し実装することができます。

ライセンス交付は、管理対象のエンドポイントの数およびスイートから選択された製品に応じて、1 年ごとのサブスクリプションによって行われます。

すべての製品は相互に互換性があり、BigFix コンソールを使用して、ご使用のネットワーク内のどこからでもアクセス可能です。

通常、 BigFixのインストールは次のパートから構成されています。

- BigFix プラットフォーム (（ページ） *3)*
- 1 つ以上のBigFix アプリケーション (（ページ） *7)*

製品の詳細は、以下を参照してください。

- サンプル・アーキテクチャー (（ページ） *10)*
- コンテンツのタイプ (（ページ） *12)*
- コンテンツを適用するターゲットの識別方法 (（ページ） *14)*

# 第 2 章. BigFix プラットフォーム

すべての BigFix アプリケーションは、BigFix プラットフォーム上で実行されます。

BigFix のプラットフォームは、全体的な IT インフラストラクチャーの中核部分として機能する、多層構造のテクノロジー・プラットフォームです。このプラットフォームは、IT インフラストラクチャーの管理作業を管理対象デバイスそのものであるエージェントに配布する、コンテンツ駆動型の動的なメッセージングおよび管理システムです。

このプラットフォームでは、専用ネットワークまたはパブリック・ネットワークを介して、最大で 250,000 までの物理コンピューターと仮想コンピューター (サーバー・デスクトップ、ローミング・ラップトップ、携帯電話、POS 装置、現金自動預け払い機、セルフサービス・キオスクなど) を管理することができます。

このプラットフォームでサポートされるのは、Microsoft Windows、UNIX、Linux、および Mac OS です。

BigFix プラットフォームは、以下の機能および利点を備えています。

**単一のインテリジェント・エージェント**

10 M バイト未満の RAM で作動し、管理する必要のあるすべてのコンピューターにインストールする必要があります。このエージェントは、ネットワークに接続されているかどうかにかかわらず、規定されたポリシーと対比して、エンドポイントの状態を絶えず査定します。ターゲットがポリシーまたはチェックリストに準拠していないことをエージェントが検出すると、すぐにサーバーに通知し、構成済みの修復タスクを実行した後、直ちにタスクの状況および結果をサーバーに通知します。ほとんどの場合、エージェントは、ユーザーからの直接介入を一切必要としないサイレント・モードで動作します。ただし、ユーザー応答を要求する必要がある場合、このプログラムでは画面にプロンプトを表示することもできます。BigFix エージェントがインストールされたコンピューターも、クライアントと呼ばれます。

**単一のコンソール**

エンドポイント保護、システム・ライフサイクル管理、セキュリティー構成および脆弱性の管理など、どのような特定のソリューションを使用する場合でも、そのソリューションは単一のコンソールから管理されます。必要な権

限を持つオペレーターであれば、コンソールを使用して、ネットワークのその他の部分に影響を与えることなく、フィックスを必要とするコンピューターのみにそれを迅速かつ容易に配布することができます。

**単一のサーバー**

個々のクライアントとの間の情報の流れを調整し、その結果をデータベースに保存します。ポリシー・ベースのコンテンツを管理し、環境内のすべての装置に対してオペレーターがリアルタイム可視性を維持し、制御できるようにします。このコンテンツは *Fixlet* というメッセージで配信され、クラウド・ベースの「コンテンツ・デリバリー」サービスを使用して継続的に更新されます。ほとんどの分析、処理、および実施作業はサーバーでなくエージェントによって行われるため、単一のサーバーで最大 250.000 までのエンドポイントをサポートできます。複数のサーバーを採用すれば、高可用性を実現できます。

**1 つ以上のリレー (オプション)**

分散デバイスおよびポリシー・コンテンツの管理を容易にします。リレーとは、リレー・サービスを使用して拡張されたクライアントのことです。ホスト・コンピューターを保護するためのすべてのクライアント・アクションを実行し、さらに子クライアントおよび子リレー対して、コンテンツおよびソフトウェアのダウンロードを配信します。リレーを使用すると、各ネットワーク・コンピューターがサーバーに直接接続する必要がなくなるので、負荷を大幅に軽減することができます。数百のクライアントがダウンロードのために 1 台のリレーを指定することができるので、同様にサーバーに対する要求は 1 つのみになります。リレーは他のリレーにも同様に接続できるため、効率はさらに高まります。エージェントをリレーにプロモートするために要する時間は数分であり、専用のハードウェアやネットワーク構成を変更する必要はありません。

**2 次サーバー (オプション)**

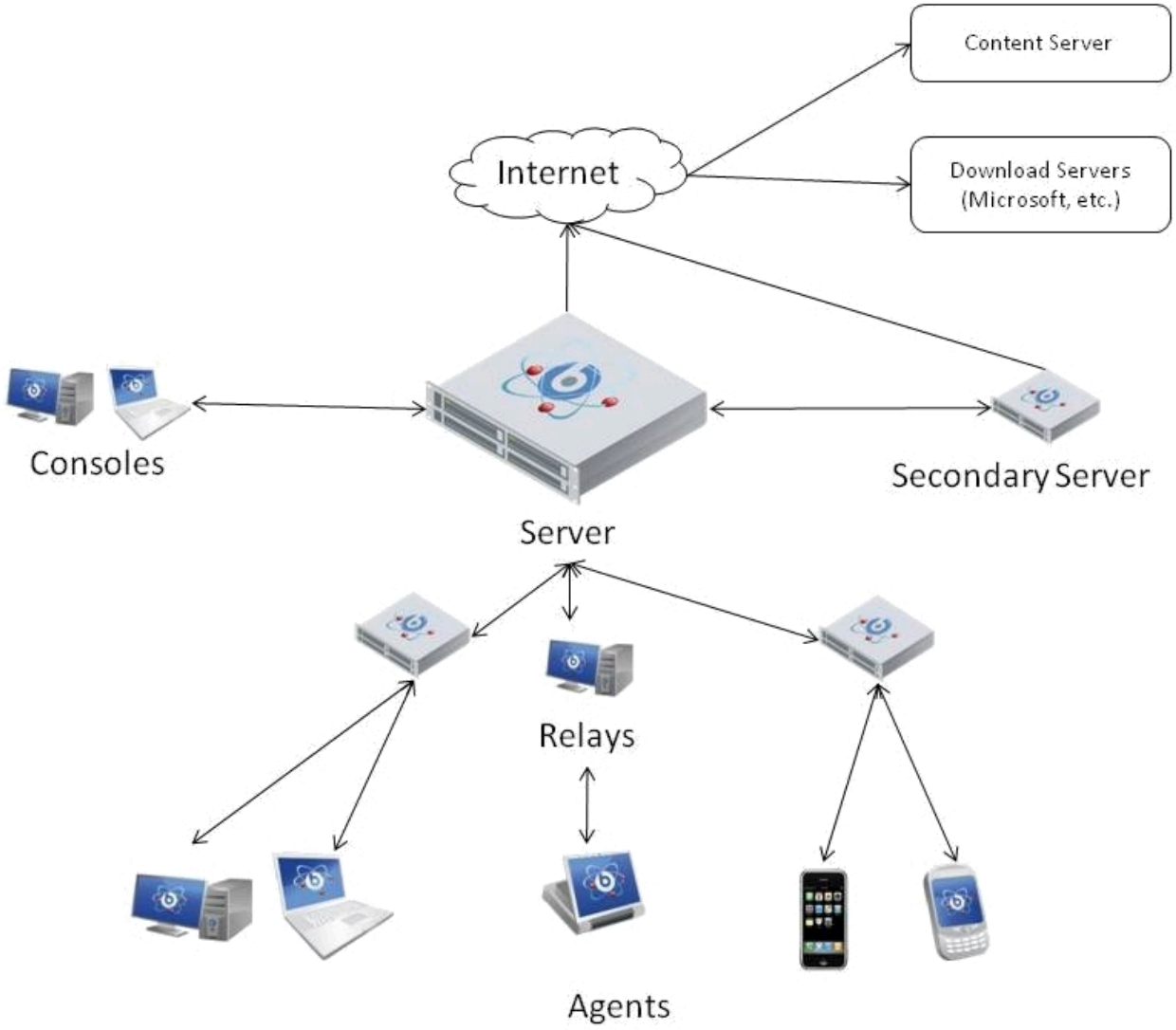
災害復旧用にサーバー情報を複製する、災害用サーバー・アーキテクチャー (DSA) サーバー。ある BigFix サーバーで障害が発生しても、他の BigFix サーバーが、元のサーバーの全機能を備えた BigFix サーバーとして自動的に引き継ぎます。

### Web レポート

Web レポート・プログラムを使用すると、以下のことが可能になります。

- データのチャートやグラフを生成し、ハードコピーが得られます。
- ネットワーク内のすべての Fixlet アクティビティーの監査証跡の維持が容易になります。
- データをエクスポートして、スプレッドシートまたはデータベースでさらに操作することができます。
- 組織にインストールされている予備の BigFix サーバーからの情報を集約します。

このインターフェースは Web ブラウザーで実行され、一連のユーザーはこれを使用してコンピューターの状態を表示することができますが、これらのユーザーにこれらのコンピューターを変更する権限が付与されることはありません。


Content Server
Internet
Download Servers
(Microsoft, etc.)
Consoles
Secondary Server
Server
Relays
Agents

# 第 3 章. BigFix アプリケーション

BigFix ソリューションは、精度と生産性を高めながら、統合されたセキュリティーと運用管理、効率化および簡素化されたエンドポイント管理を提供する複数のアプリケーション製品で構成されています。

**BigFix Lifecycle**

このアプリケーションを使用すると、管理者は、エンドポイントの状態を正確に表示して問題を自動的に修復する、エージェント・ベースのツールを使用できるようになります。

BigFix Lifecycle には、以下のアプリケーションが含まれます。

**OS Deployment**

単一の一元化された場所からネットワーク全体に新規ワークステーションやサーバーを迅速にデプロイするための、統合された包括的なソリューションを提供します。

**電源管理**

ネットワーク内のコンピューターの消費電力設定を管理およびモニターします。また、この製品は、ダッシュボード、ウィザード、および Web レポートを使用して設定した社内の省電力ポリシーを管理および適用します。

**Remote Control**

適用環境内のワークステーションおよびサーバーの引き継ぎとモニターをリモートで実行します。

**Server Automation**

プロビジョニング・ワークフローを自動化します。サーバーやコンピューターなどのさまざまなエンドポイントにわたって、Fixlet、タスク、およびベースラインのシーケンスを自動化できます。

**ソフトウェア配布**

単一の一元化された場所からネットワーク全体にソフトウェアを迅速にデプロイするための、統合された包括的なソリューションを提供します。これは、コスト効率の高い運用管理機能、およびソフトウェアの配信とインストールのプロセスの可視性を提供します。

**BigFix Patch**

このアプリケーションを使用すると、すべての分散エンドポイントに対し、自動化された単純なパッチ・プロセスを使用できるようになります。この製品は、オペレーティング・システム・パッチとソフトウェア・アプリケーション・パッチの両方を管理します。

**BigFix Compliance**

このアプリケーションを使用すると、エンドポイントが保護され、修復が自動化されます。また、セキュリティー・コンプライアンス標準を満たしていることが規制機関に対して保証されます。

**BigFix Inventory**

このアプリケーションを使用すると、モニター対象のコンピューターをスキャンして、以下のことが行えます。

- インストール済みのソフトウェアを識別する。
- スキャンでディスカバーされた署名をソフトウェア・カタログと突き合わせる。
- レポートを作成する。
- その結果を、契約に定められたコストおよび資格に関する情報と比較する。

追加ライセンスを購入することにより、BigFix ソリューションに属するアプリケーションを後で必要になった際に追加することができます。購入した製品は、自動的に BigFix コンソールで使用できるようになります。ソリューションに属するアプリケーションを追加するにあたり、追加のソフトウェアをインストールしたり、新たなハードウェアを購入した

りする必要はありません。Asset Discovery と Inventory のみ、新規コンポーネントのインストールを必要としますが、このインストールは BigFix 自身により行われます。

**注:** Asset Discovery はBigFixプラットフォームのコンポーネントの 1 つで、ご使用のネットワーク内にある管理されていない資産を識別できるようにします。

多くのお客様は、Patch などの単一のアプリケーションから使用を開始し、その後、製品ソリューションの機能全体の価値が分かり始めたら、新規ライセンスを購入して、製品を適用する範囲を拡大します。

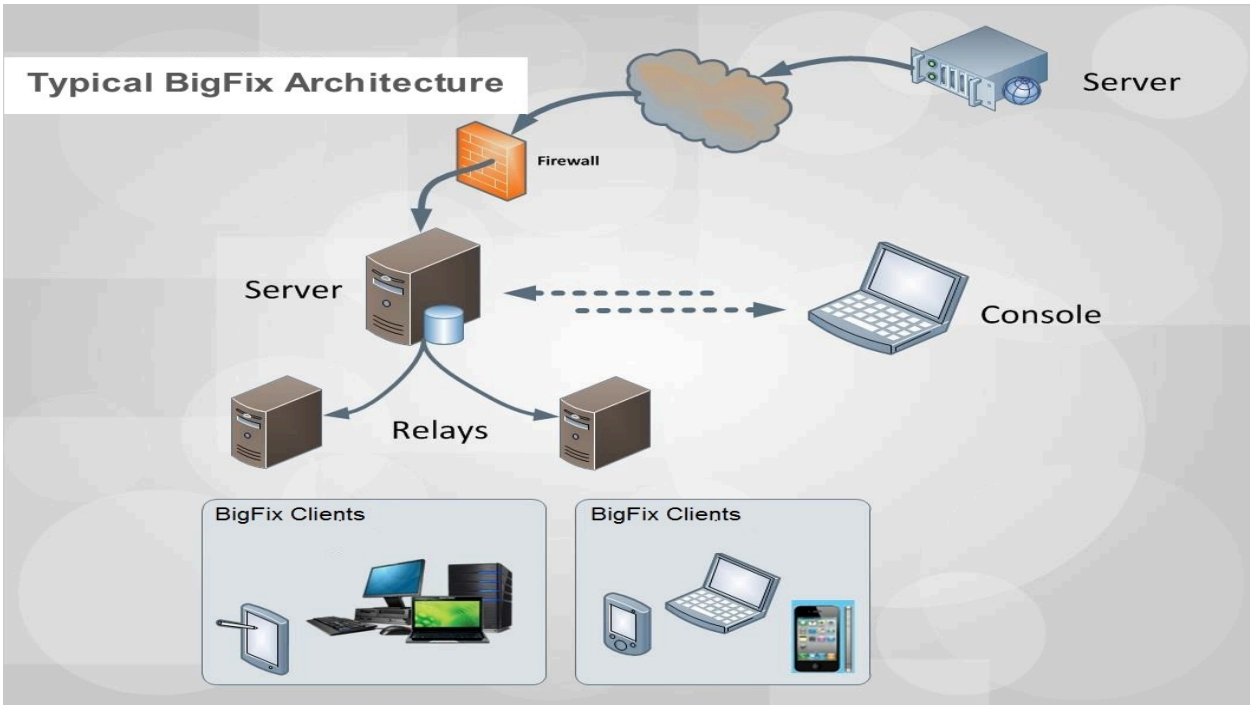
いくつかの機能は、BigFix 製品ソリューション内の複数のアプリケーションに共通しています。例えば、下の図に示すように、OS およびソフトウェア・アプリケーションのパッチを適用する機能は、Patch アプリケーションのみならず、Compliance アプリケーションおよび Lifecycle アプリケーションでも使用することができます。パッチを管理するためのこうしたライセンスは、いずれも購入が可能です。

これらのアプリケーションはすべて、エージェントでの連続的な評価と、リポジトリーからデータを取得してターゲットに送る収集プロセスを利用しています。

# 第 4 章. サンプル・アーキテクチャー

サンプル・アーキテクチャーは、ご使用の環境の計画を立てるのに役立ちます。

標準的なインストール済み環境には、インターネットから Fixlet を収集する BigFix サーバーが少なくとも 1 つ存在します。これらのメッセージは、コンソール・オペレーターで表示したり、リレーに配信したりできます。リレーは、クライアントにデータを転送します。各クライアントはそのローカル・コンピューターを検査し、関連する Fixlet をリレーに折り返し報告します。リレーは、そのデータを圧縮してサーバーに返します。




コンソールはこのアクティビティーを監視します。サーバーに接続し、ビューを定期的に更新して、ネットワークに関する変更または新しい情報を反映させます。脆弱性が見つかった場合は、コンソール・オペレーターは該当するコンピューターを対象としてパッチやその他のフィックスを適用します。該当するすべてのコンピューターにフィックスが配信され、1 台ずつバグと脆弱性を解消していく進行状況を、ほぼリアルタイムで追跡できます。

BigFix は、遠方のオフィスに VPN を介して接続できる柔軟性があるほか、在宅勤務者や外回りの営業スタッフが、DMZ 内のファイアウォールで保護されたリレーにインターネット

を介して接続することも可能にします。このシンプルな階層は拡張と深化が可能であり、実質的にあらゆるサイズのネットワークに対応することができます。

# 第 5 章. コンテンツのタイプ

BigFix では、コンテンツに基づいています。コンテンツの総称用語は、ターゲットに配布するデータ、またはターゲットで実行する命令、またはターゲットで実行する照会を表す場合があります。

BigFix 実装環境は、以下のさまざまなタイプのコンテンツに基づいています。

**アクション**

アクションは選択されたターゲットで実行されるスクリプトです。アクションは、ポリシー違反および機密漏れの修正、構成ステップの実行、または一般に、ターゲットに対する操作やコマンドの実行のために使用されます。Fixlet、タスク、およびベースラインにはアクションが含まれ、それらの修復作業はアクションによって実行されます。

**Fixlet**

Fixlet とは、ターゲット・システムの BigFix エージェントがその状況を判断し、脆弱性やポリシー・ルールの非準拠といった問題を特定し、解決のための修正アクションを実行するために使用する指示が記述された文書のことです。

**タスク**

タスクとは、ターゲット・システムの BigFix エージェントが、コマンドや構成アクティビティーをローカルで実行するために使用する指示が記述された文書のことです。

**ベースライン**

ベースラインは、Fixlet とタスクのデプロイメント・コンテナーです。1 つ以上のターゲットに対して、コンテンツ・セットを同時に適用する場合に使用できます。コンテンツは、ベースラインの記述で指定されたシーケンスに基づいて適用されます。例えば、ベースラインは以下を含む場合があります。

1. 製品をインストールするための Fixlet。
2. 製品を必要なレベルへアップグレードする Fixlet。
3. インストールされた製品を構成するタスク。

ベースラインがデプロイされる際、所定のシーケンスに従ってコンテンツが適用されます。

**分析**

分析はプロパティー式のコレクションであり、オペレーターはこれを使用することで、ネットワーク上のBigFixクライアント・コンピューターの各種プロパティーを表示および要約できます。

これらのタイプのコンテンツには、BigFix コンソールからアクセスできます。BigFix スイートに属する各アプリケーションは、これらのコンテンツを使用してアクティビティーを実行します。ユーザーは、独自のニーズを満たすように、カスタム・コンテンツを作成することができます。例えば、カスタム Fixlet を作成して、独自に開発したアプリケーションにパッチを適用したり、ポリシー・ルールを適用したりすることができます。カスタム・コンテンツを作成するには、特定の許可が必要です。

コンテンツはコンテンツ・サイトにあります。これらのコンテンツは、適時、自動的に更新されます。利用可能なコンテンツ・サイトのセットは、購入した BigFix 製品ライセンスによって異なります。必要な許可を持っている場合は、独自のカスタム・コンテンツ・サイトを作成し、カスタム・コンテンツを収集することができます。

# 第 6 章. コンテンツを適用するターゲットの識別方法

BigFix は、コンテンツを適用するターゲットを識別するのに役立ちます。

BigFix の主な特長の 1 つは、コンテンツの適用先となるターゲット、つまりコンテンツを必要とするコンピューターを判別する機能です。この機能は関連式を使用して実現されます。関連式はコンテンツ定義の一部であり、管理対象クライアントのハードウェアおよびソフトウェアのプロパティーを調べて、パッチや保守アクティビティーなどがそれを必要とするコンピューターのみに適用され、その他のコンピューターには適用されないようにすることを目的としています。

コンテンツを定義するには、そのコンテンツのターゲットとなる一連のコンピューターを「適用可能なコンピューター」タブで指定します。関連度の評価により、この一連のコンピューターが絞り込まれ、そのコンテンツを真に適用する必要のあるコンピューターのみが選択されます。


関連式はすべてのコンテンツ・タイプに対して同じ方法で使用されますが、以下のようにコンテンツ・タイプに応じてさまざまな動作がトリガーされます。

**関連するアクション**

この場合、アクション・スクリプト言語を使用してアクションの記述に指定された命令を実行することにより、違反が修復されます。アクションは、実行時に「アクションの実行」ダイアログでカスタマイズできる関連句を取り込みます。

**関連する Fixlet**

コンピューターがポリシー・ルールに準拠していない場合です。Fixlet が必要な場合、Fixlet 定義に含まれるアクションを実行して、問題を修復できます。

アクションの実行後に関連性がもう一度評価され、脆弱性が修復されたかどうか確認されます。

例えば、Fixlet を使用して Symantec Endpoint Protection をインストールすることができます。この Fixlet は、Symantec Endpoint Protection がインストールされていないコンピューターに関連付けられています。Fixlet がすべての該当するコンピューターにインストールされると、関連性のマークは付かなくなります。その後、「適用可能なコンピューター」タブに指定された 1 つ以上のコンピューターから Symantec Endpoint Protection がアンインストールされると、Fixlet に再び関連性のマークが付きます。

**関連するタスク**

コンピューターに構成標準または構成要件の違反があるか、メンテナンス・アクティビティーを実行する必要がある場合です。

例えば、タスクを使用して Symantec Endpoint Protection を始動したりします。このタスクが該当するのは、Symantec Endpoint Protection が非アクティブになっているコンピューターです。

このタスクが該当する場合、タスク定義に含まれるアクションを実行して、問題を修正することができます。アクションのすべてのステップが完了すると、タスクには、そのコンピューターには該当しないことを示すマークが付けられます。関連式が再度評価されることはありません。ベスト・プラクティスとして、アクションが正常に完了したかどうかを判別するために成功基準を使用して、修復の試みが問題の解決につながるようにすることが推奨されます。

**関連するベースライン**

この場合、このベースラインに含まれる 1 つ以上の Fixlet が、Fixlet の記述とベースラインの「適用可能なコンピューター」タブの両方に指定されている関連式の基準を満たす、1 つ以上のコンピューターに必要です。ベースラインの「適用可能なコンピューター」タブに何も指定されていない場合、Fixlet およびタスクの適用条件に制限は適用されません。

例えば、Windows および Linux オペレーティング・システムの Fixlet およびタスクがベースラインに含まれているものの、ベースラインの「適用可能な

コンピューター」において Windows コンピューターのみが関連すると指定されている場合、Windows に適用可能な Fixlet およびタスクのみが対象となります。

**注:** ベースラインにタスクが含まれる場合でも、Fixlet の動作は適用されます。

**関連する分析**

照会間隔に従ってプロパティー照会を実行し、結果をサーバーに送信します。この結果は BigFix コンソールに表示されます。

コンピューターが新規に収集された文書の関連性 (例えば Fixlet や分析) を評価して、結果を送信すると、その結果は BigFix コンソールに表示されます。初回の評価の後は、コンピューターは変更のみをレポートします。これは、同じ結果のレポートにネットワーク帯域幅を使用してもメリットがないためです。

関連式は、人間が読んで理解できる「Relevance Language」という専用言語で作成されます。

カスタム・コンテンツ許可を持っている場合、新規の関連式を作成したり、あるいは既存の式を変更することで、必要に応じたコンテンツが実行されるように調整することができます。オペレーターへの許可の割り当てに関する詳細は、許可されるアクティビティーと許可とのマッピング (（ページ）　　)を参照してください。

# 第 7 章. パッチ管理のシナリオ

以下のトピックにリストされた手順に従って、新しくインストールされたBigFixサーバー上のパッチ管理アプリケーションを使用して、パッチを適用する方法を確認してください。すべての手順は BigFix コンソールから実行します。

このシナリオは、Windows オペレーティング・システムに適用されます。同じ手順に従って、他のオペレーティング・システムでもパッチを有効にして、適用することができます。

このシナリオは、以下の 2 つのパートに分かれています。

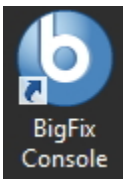


## Windows パッチ用のパッチ管理の構成

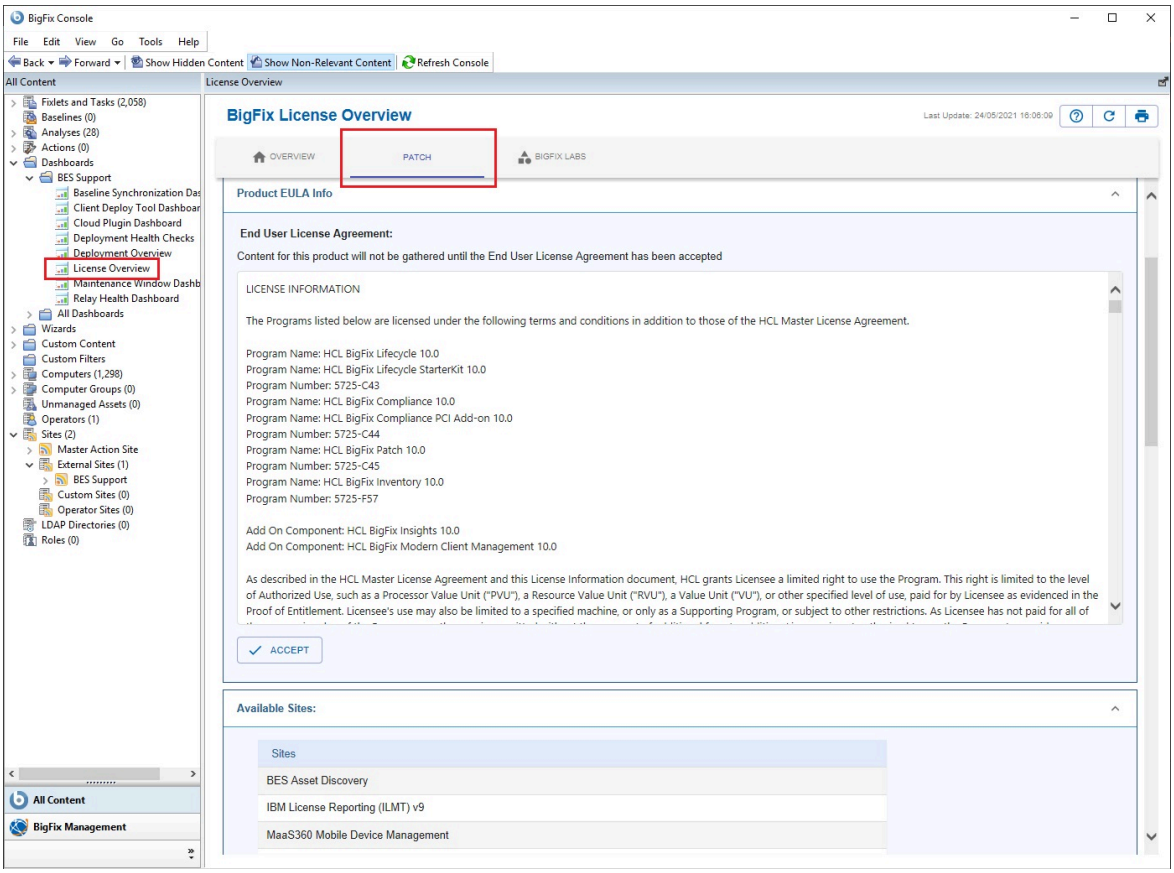
インストール後に、BigFix 製品は、特定の管理サイトおよびメンテナンス・サイトをサブスクライブするように自動的にセットアップされます。これにより、それらのサイトから企業内にコンテンツが自動的に流れ込み、BigFix クライアントを実行しているすべてのコンピューターで、それらのコンテンツの関連度が評価されます。

以下の手順を実行して、パッチ管理サイトをサブスクライブします。

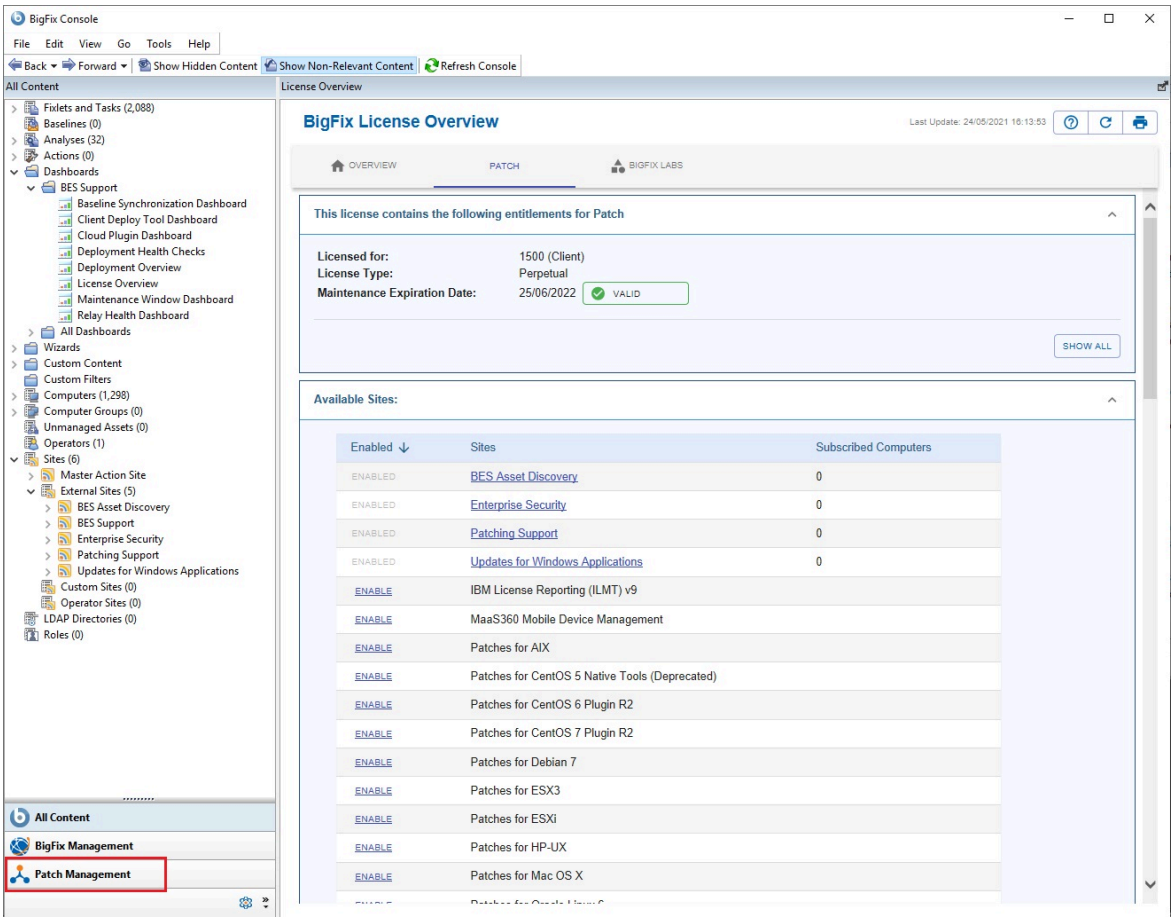
1. 次のアイコンをダブルクリックして、BigFix コンソールを開きます。




2. **「ライセンスの概要」**ダッシュボードをクリックします。
3. 「パッチ管理」タブを選択します。

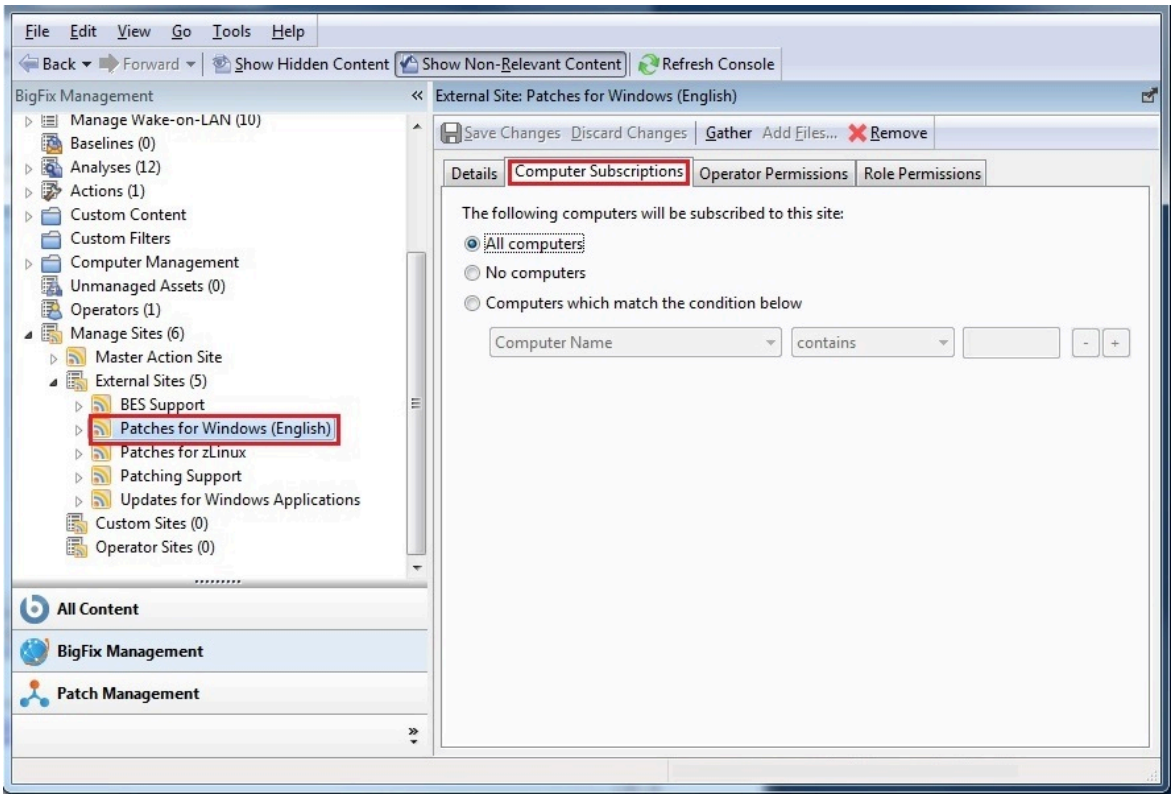



4. パッチ管理のご使用条件を読んで同意します。
5. **「利用可能なサイト」**で、**「BES Asset Discovery」**、**「Patches for Windows (英語)」**、**「パッチ・サポート」**、および**「Windows アプリケーションの更新」**の横にある**「有効化」**をクリックし、パッチ管理 Web サイトからのダウンロード・コンテンツを有効にします。




これで、パッチ管理サイトがドメイン・パネルの**「サイトを管理」**ノードにリストされます。

6. **「サイトを管理」**ノードを開いて、**「Patches for Windows (英語)」**を選択します。
7. サイト・ダイアログで、**「コンピューターのサブスクリプション」**タブをクリックしてから**「すべてのコンピューター」**を選択します。

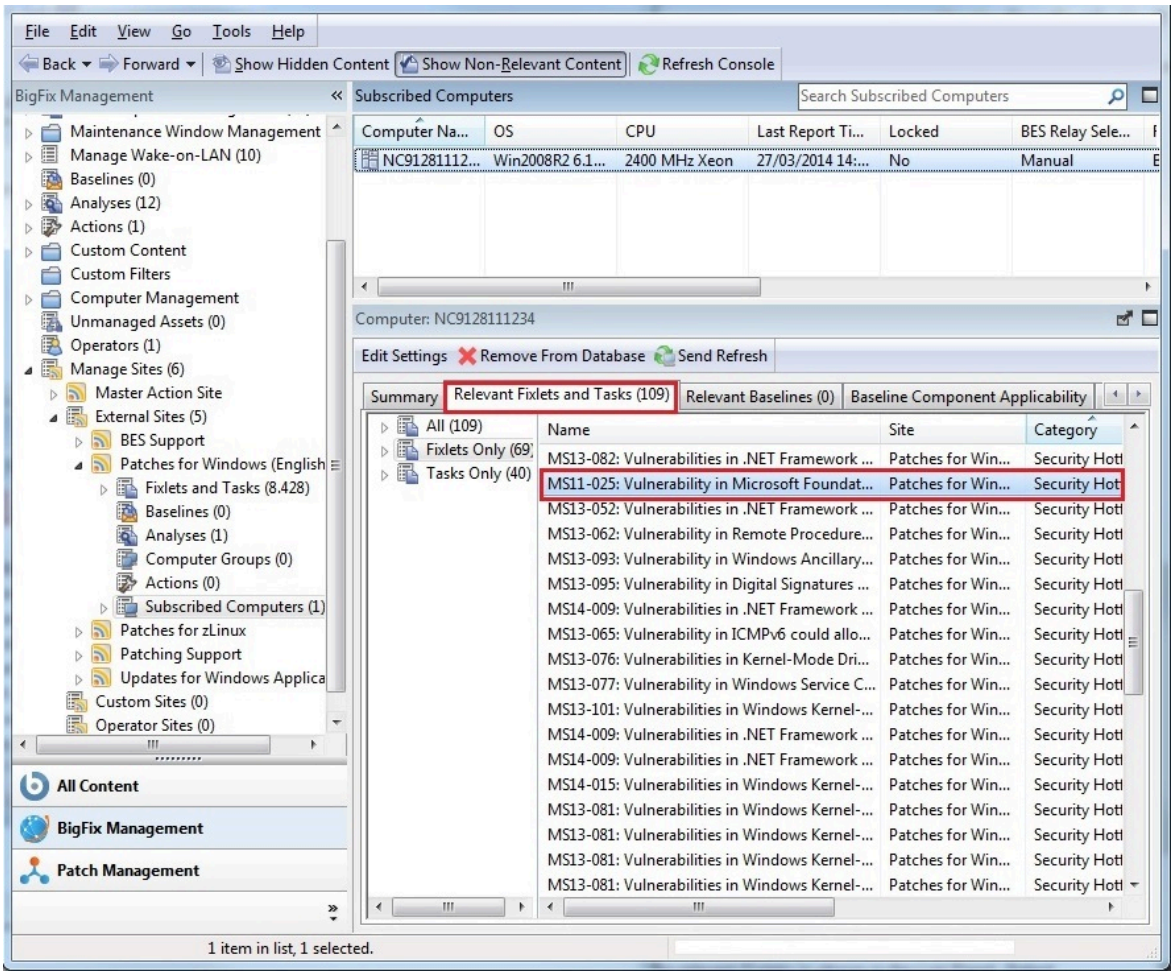



8. 収集プロセスが自動的に実行されるまで待機するか、**「収集」**をクリックして選択したサイトから使用可能なコンテンツのダウンロードを開始できます。
9. 収集プロセスが完了すると、**「Patches for Windows (英語)」**サブツリーに新規コンテンツが取り込まれます。

# Windows パッチの適用

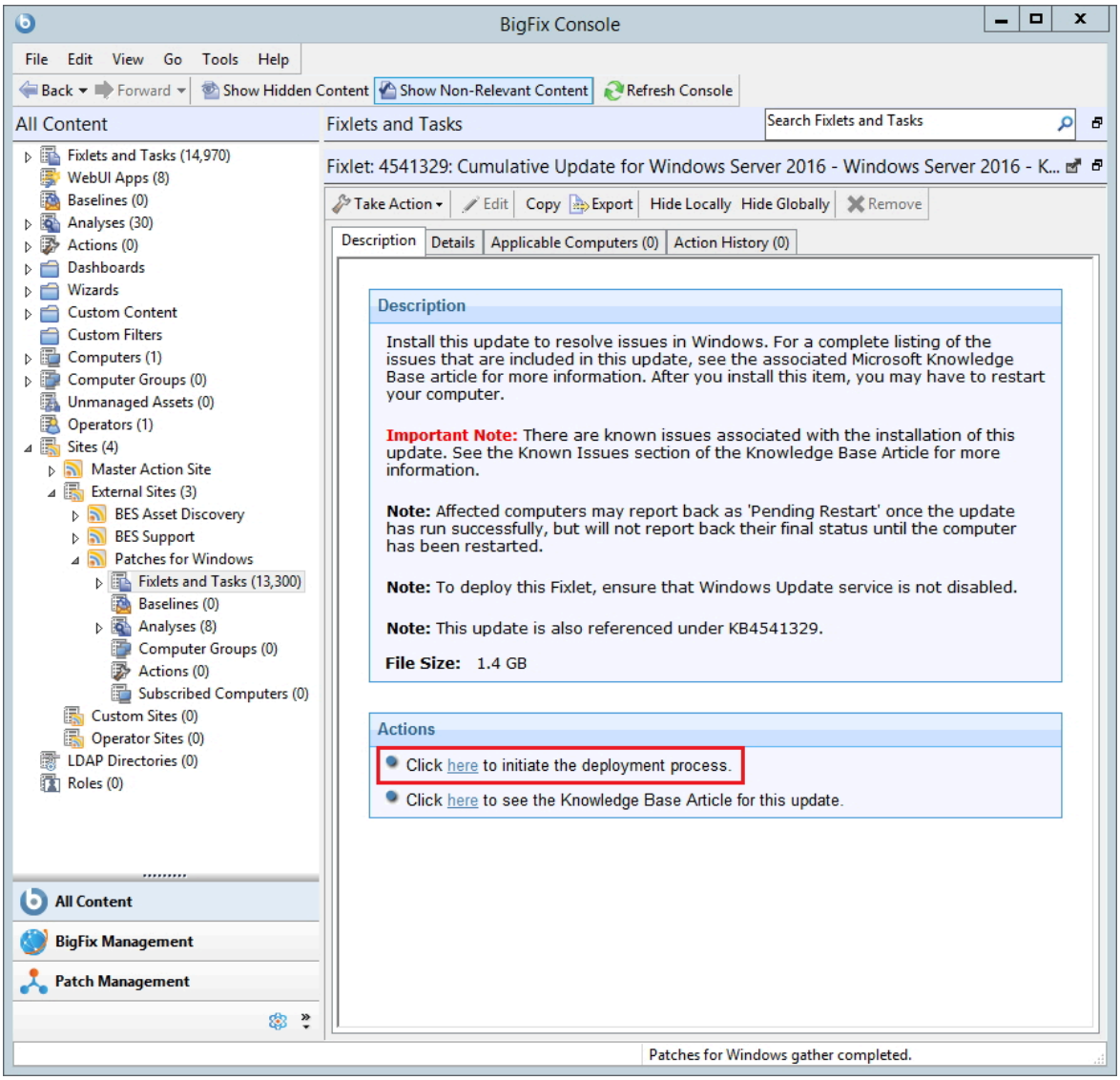
以下の手順をコンソールから実行して、Windows パッチを適用します。

1. **「Patches for Windows (英語)」**サブツリーを展開し、**「サブスクライブしたコンピューター」**をクリックします。**リスト・パネル**に、サーバー・システムにインストールされたクライアントを表すエントリーが表示されます。
2. **「関連する Fixlets とタスク」**タブを選択して、選択したクライアントに関連する Fixlets のリストを表示します。

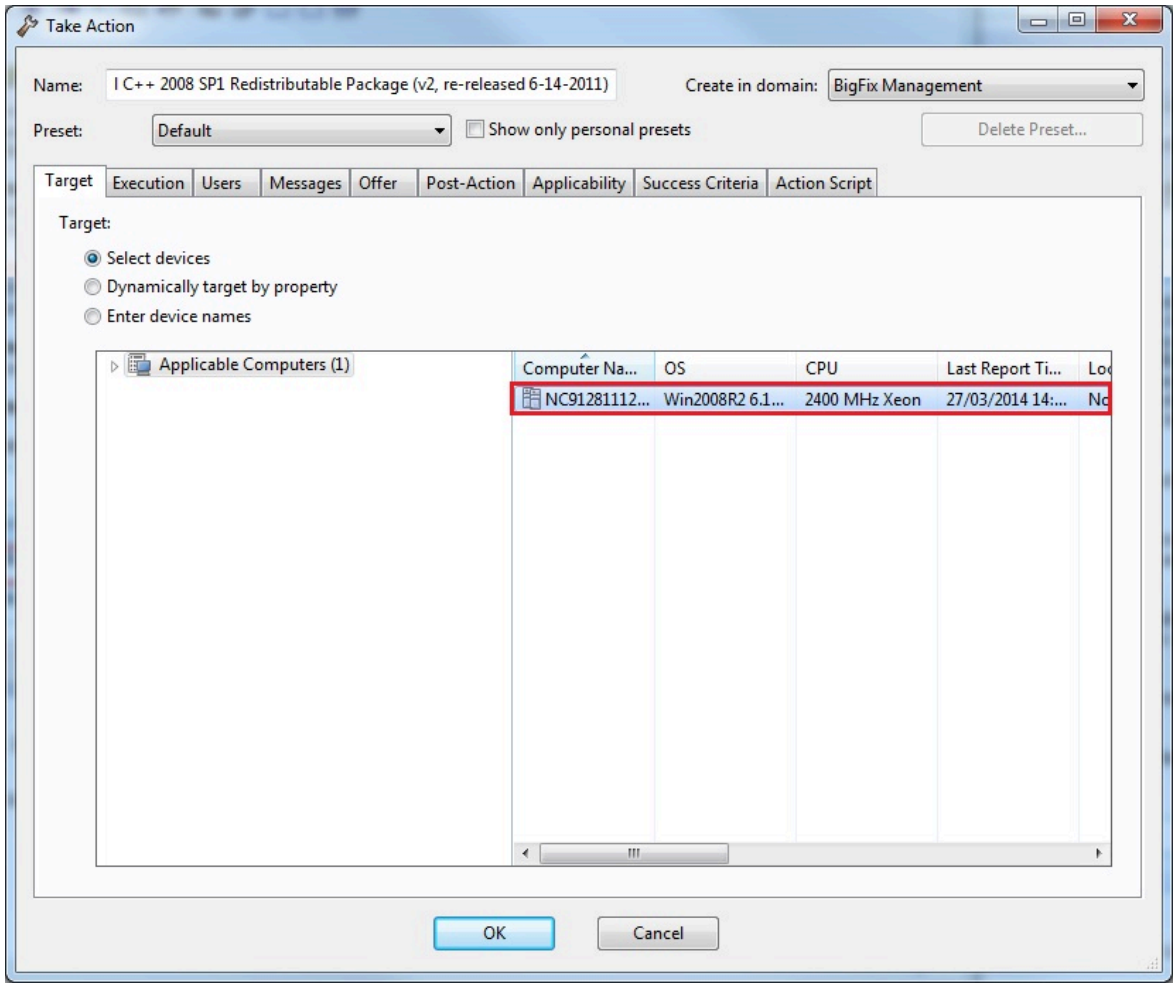



Fixlet がクライアントに関連するのは、Fixlet で参照されたコンテンツをクライアントがインストールする必要がある場合です。コンテンツをインストールする必要性については、Fixlet に指定された事前定義条件のセットを使用して、クライアント上で自動的に評価されます。

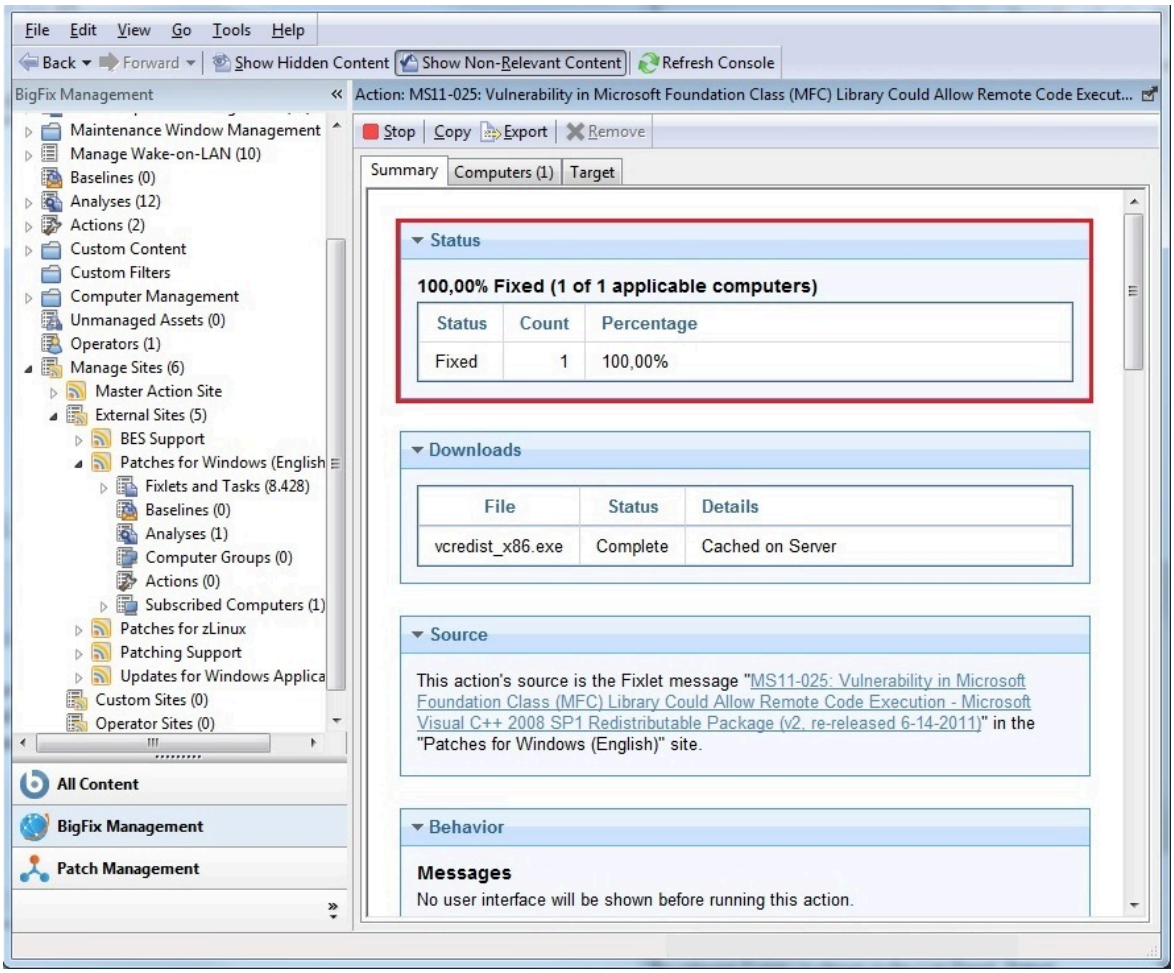
3. 「Fixlet」をダブルクリックして、Fixlet の説明にアクセスします。
4. **「アクション」**ペインで、適用プロセスの開始を選択します。




5. **「アクションの実行」**パネルが開きます。このパネルでクライアントを選択してから、**「OK」**をクリックして適用を開始します。




6. **「アクション」**パネルへ自動的にリダイレクトされます。状況ペインに、Fixlet 適用の進捗状況が表示されます。状況は**「未評価」**から**「評価中」**に変わり、クライアントの脆弱性が正常に修正されると**「修正済み」**に変わります。脆弱性の除去は、「アクション」の**「成功条件」**タブで指定された事前定義条件のセットを使用して、クライアント上で自動的に評価されます。




7. 脆弱性が除去された後は、クライアントにその Fixlet を再度適用する必要はありません。Fixlet はそのクライアントに関連がないマークが付けられます。

# Appendix A. Glossary

This glossary provides terms and definitions for the Modern Client Management for BigFix software and products.

The following cross-references are used in this glossary:

- *See* refers you from a non-preferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

A *(on page 25)* B *(on page 26)* C *(on page 27)* D *(on page 29)* E *(on page 31)* F *(on page 31)* G *(on page 31)* L *(on page 31)* M *(on page 32)* N *(on page 33)* O *(on page 33)* P *(on page 34)* R *(on page 34)* S *(on page 34)* T *(on page 37)* U *(on page 37)* V *(on page 37)* W *(on page 38)*

## A

**action**

1. See Fixlet *(on page 31)*.
2. A set of Action Script commands that perform an operation or administrative task, such as installing a patch or rebooting a device.

**Action Script**

Language used to perform an action on an endpoint.

**agent**

See BigFix agent *(on page 26)*.

**ambiguous software**

Software that has an executable file that looks like another executable file, or that exists in more than one place in a catalog (Microsoft Word as a standalone product or bundled with Microsoft Office).

**audit patch**

A patch used to detect conditions that cannot be remediated and require the attention of an administrator. Audit patches contain no actions and cannot be deployed.

**automatic computer group**

A computer group for which membership is determined at run time by comparing the properties of a given device against the criteria set for group membership. The set of devices in an automatic group is dynamic, meaning that the group can and does change. See also computer group *(on page 27)*.

# B

**baseline**

A collection of actions that are deployed together. A baseline is typically used to simplify a deployment or to control the order in which a set of actions are applied. See also deployment group *(on page 29)*.

**BigFix agent**

The BigFix code on an endpoint that enables management and monitoring by BigFix.

**BigFix client**

See BigFix agent *(on page 26)*.

**BigFix console**

The primary BigFix administrative interface. The console provides a full set of capabilities to BigFix administrators.

**BYOD**

Bring Your Own Device (BYOD) refers to employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.

# C

**client**

A software program or computer that requests services from a server. See also server *(on page 35)*.

**client time**

The local time on a BigFix client device.

**Cloud**

A set of compute and storage instances or services that are running in containers or on virtual machines.

**Common Vulnerabilities and Exposures Identification Number (CVE ID)**

A number that identifies a specific entry in the National Vulnerability Database. A vendor's patch document often includes the CVE ID, when it is available. See also National Vulnerability Database *(on page 33)*.

**Common Vulnerabilities and Exposures system (CVE)**

A reference of officially known network vulnerabilities, which is part of the National Vulnerabilities Database (NVD), maintained by the US National Institute of Standards and Technology (NIST).

**component**

An individual action within a deployment that has more than one action. See also deployment group *(on page 29)*.

**computer group**

A group of related computers. An administrator can create computer groups to organize systems into meaningful categories, and to facilitate deployment of content to multiple computers. See also automatic computer group *(on page 26)* and manual computer group *(on page 32)*.

**console**

See BigFix console *(on page 26)*.

**content**

Digitally-signed files that contain data, rules, queries, criteria, and other instructions, packaged for deployment across a network. BigFix agents use the detection criteria (Relevance statements) and action instructions (Action Script statements) in content to detect vulnerabilities and enforce network policies.

**content relevance**

A determination of whether a patch or piece of software is eligible for deployment to one or more devices. See also device relevance *(on page 30)*.

**Coordinated Universal Time (UTC)**

The international standard of time that is kept by atomic clocks around the world.

**corrupt patch**

A patch that flags an operator when corrections made by an earlier patch have been changed or compromised. This situation can occur when an earlier service pack or application overwrites later files, which results in patched files that are not current. The corrupt patch flags the situation and can be used to re-apply the later patch.

**custom content**

BigFix code that is created by a customer for use on their own network, for example, a custom patch or baseline.

**CVE**

See Common Vulnerabilities and Exposures system *(on page 27)*.

**CVE ID**

See Common Vulnerabilities and Exposures Identification Number *(on page 27)*.

# D

**data stream**

A string of information that serves as a source of package data.

**default action**

The action designated to run when a Fixlet is deployed. When no default action is defined, the operator is prompted to choose between several actions or to make an informed decision about a single action.

**definitive package**

A string of data that serves as the primary method for identifying the presence of software on a computer.

**deploy**

To dispatch content to one or more endpoints for execution to accomplish an operation or task, for example, to install software or update a patch.

**deployment**

Information about content that is dispatched to one or more endpoints, a specific instance of dispatched content.

**deployment group**

The collection of actions created when an operator selects more than one action for a deployment, or a baseline is deployed. See also baseline *(on page 26)*, component *(on page 27)*, deployment window *(on page 30)*, and multiple action group *(on page 33)*.

**deployment state**

The eligibility of a deployment to run on endpoints. The state includes parameters that the operator sets, such as 'Start at 1AM, end at 3AM.'

**deployment status**

Cumulative results of all targeted devices, expressed as a percentage of deployment success.

**deployment type**

An indication of whether a deployment involved one action or multiple actions.

**deployment window**

The period during which a deployment's actions are eligible to run. For example, if a Fixlet has a deployment window of 3 days and an eligible device that has been offline reports in to BigFix within the 3-day window, it gets the Fixlet. If the device comes back online after the 3-day window expires, it does not get the Fixlet. See also deployment group *(on page 29)*.

**device**

An endpoint, for example, a laptop, desktop, server, or virtual machine that BigFix manages; an endpoint running the BigFix Agent.

**device holder**

The person using a BigFix-managed computer.

**device property**

Information about a device collected by BigFix, including details about its hardware, operating system, network status, settings, and BigFix client. Custom properties can also be assigned to a device.

**device relevance**

A determination of whether a piece of BigFix content applies to applies to a device, for example, where a patch should be applied, software installed, or a baseline run. See also content relevance *(on page 28)*.

**device result**

The state of a deployment, including the result, on a particular endpoint.

**Disaster Server Architecture (DSA)**

An architecture that links multiple servers to provide full redundancy in case of failure.

**DSA**

See Disaster Server Architecture *(on page 30)*.

**dynamically targeted**

Pertaining to using a computer group to target a deployment.

# E

**endpoint**

A networked device running the BigFix agent.

# F

**filter**

To reduce a list of items to those that share specific attributes.

**Fixlet**

A piece of BigFix content that contains Relevance and Action Script statements bundled together to perform an operation or task. Fixlets are the basic building blocks of BigFix content. A Fixlet provides instructions to the BigFix agent to perform a network management or reporting action.

**Full Disk Encryption**

To reduce a list of items to those that share specific attributes.

# G

**group deployment**

A type of deployment in which multiple actions were deployed to one or more devices.

# L

**locked**

An endpoint state that prevents most of the BigFix actions from running until the device is unlocked.

# M

**MAG**

See multiple action group *(on page 33)*.

**management rights**

The limitation of console operators to a specified group of computers. Only a site administrator or a master operator can assign management rights.

**manual computer group**

A computer group for which membership is determined through selection by an operator. The set of devices in a manual group is static, meaning they do not change. See also computer group *(on page 27)*.

**master operator**

A console operator with administrative rights. A master operator can do everything that a site administrator can do, except creating operators.

**masthead**

A collection of files that contain the parameters of the BigFix process, including URLs to Fixlet content. The BigFix agent brings content into the enterprise based on subscribed mastheads.

**MCM and BigFix Mobile**

Refers to the offering by Bigfix that is common for both Modern Client Management to manage laptops (Windows and macOS) and BigFix Mobile to manage mobile devices (Android, iOS, and iPadOS).

**mirror server**

A BigFix server required if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.

**Multicloud**

The utilization of distinct sets of cloud services, typically from multiple vendors, where specific applications are confined to a single cloud instance.

**multiple action group (MAG)**

A BigFix object that is created when multiple actions are deployed together, as in a baseline. A MAG contains multiple Fixlets or tasks. See also deployment group *(on page 29)*.

# N

**National Vulnerability Database (NVD)**

A catalog of officially known information security vulnerabilities and exposures, which is maintained by the National Institute of Standards and Technology (NIST). See also Common Vulnerabilities and Exposures Identification Number *(on page 27)*.

**NVD**

See National Vulnerability Database *(on page 33)*.

# O

**offer**

A deployment option that allows a device holder to accept or decline a BigFix action and to exercise some control over when it runs. For example, a device holder can decide whether to install a software application, and whether to run the installation at night or during the day.

**open-ended deployment**

A deployment with no end or expiration date; one that runs continuously, checking whether the computers on a network comply.

**operator**

A person who uses the BigFix WebUI, or portions of the BigFix console.

# P

**patch**

A piece of code added to vendor software to fix a problem, as an immediate solution that is provided to users between two releases.

**patch category**

A description of a patch's type and general area of operation, for example, a bug fix or a service pack.

**patch severity**

The level of risk imposed by a network threat or vulnerability and, by extension, the importance of applying its patch.

# R

**relay**

A client that is running special server software. Relays spare the server and the network by minimizing direct server-client downloads and by compressing upstream data.

**Relevance**

BigFix query language that is used to determine the applicability of a piece of content to a specified endpoint. Relevance asks yes or no questions and evaluates the results. The result of a Relevance query determines whether an action can or should be applied. Relevance is paired with Action Script in Fixlets.

# S

**SCAP**

See Security Content Automation Protocol *(on page 35)*.

**SCAP check**

A specific configuration check within a Security Content Automation Protocol (SCAP) checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

**SCAP checklist**

A configuration checklist that is written in a machine-readable language (XCCDF). Security Content Automation Protocol (SCAP) checklists have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services.

**SCAP content**

A repository that consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

**SCAP enumeration**

A list of all known security related software flaws (CVEs), known software configuration issues (CCEs), and standard vendor and product names (CPEs).

**SCAP mapping**

The interrelationship of enumerations that provides standards-based impact measurements for software flaws and configuration issues.

**Security Content Automation Protocol (SCAP)**

A set of standards that is used to automate, measure, and manage vulnerability and compliance by the National Institute of Standards and Technology (NIST).

**server**

A software program or a computer that provides services to other software programs or other computers. See also client *(on page 27)*.

**signing password**

A password that is used by a console operator to sign an action for deployment.

**single deployment**

A type of deployment where a single action was deployed to one or more devices.

**site**

A collection of BigFix content. A site organizes similar content together.

**site administrator**

The person who is in charge of installing BigFix and authorizing and creating new console operators.

**software package**

A collection of Fixlets that install a software product on a device. Software packages are uploaded to BigFix by an operator for distribution. A BigFix software package includes the installation files, Fixlets to install the files, and information about the package (metadata).

**SQL Server**

A full-scale database engine from Microsoft that can be acquired and installed into the BigFix system to satisfy more than the basic reporting and data storage needs.

**standard deployment**

A deployment of BigFix that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all Client computers have direct access to a single internal server.

**statistically targeted**

Pertaining to the method used to target a deployment to a device or piece of content. Statically targeted devices are selected manually by an operator.

**superseded patch**

A type of patch that notifies an operator when an earlier version of a patch has been replaced by a later version. This occurs when a later patch updates the same files as an earlier one. Superseded patches flag vulnerabilities that can be remediated by a later patch. A superseded patch cannot be deployed.

**system power state**

A definition of the overall power consumption of a system. BigFix Power Management tracks four main power states Active, Idle, Standby or Hibernation, and Power Off.

# T

**target**

To match content with devices in a deployment, either by selecting the content for deployment, or selecting the devices to receive content.

**targeting**

The method used to specify the endpoints in a deployment.

**task**

A type of Fixlet designed for re-use, for example, to perform an ongoing maintenance task.

# U

**UTC**

See Coordinated Universal Time *(on page 28)*.

# V

**virtual private network (VPN)**

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

**VPN**

See virtual private network *(on page 37)*.

**vulnerability**

A security exposure in an operating system, system software, or application software component.

# W

**Wake-from-Standby**

A mode that allows an application to turn a computer on from standby mode during predefined times, without the need for Wake on LAN.

**Wake on LAN**

A technology that enables a user to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, users of this technology can remotely turn on a server and control it across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

**WAN**

See wide area network *(on page 38)*.

**wide area network (WAN)**

A network that provides communication services among devices in a geographic area larger than that served by a local area network (LAN) or a metropolitan area network (MAN).

# Appendix B. Support

For more information about this product, see the following resources:

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube
- BigFix Tech Advisors channel on YouTube
- BigFix Forum

# Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or

any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

# Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

# Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

## Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

## Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

## Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

## Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.