Lenovo

Lenovo XClarity Essentials

UpdateXpress ユーザー・ガイド

バージョン 4.4.0

注

本書および本書で紹介する製品をご使用になる前に、41 ページの 付録 B「注記」に記載されている情報をお読みください。

本書は、Lenovo XClarity® Essentials UpdateXpress および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

第 24 版 (2024 年 2 月)

目次

表

このガイドについて

Lenovo XClarity Essentials UpdateXpress (これ以降 UpdateXpress アプリケーションと呼びます) は、ご使用のサーバーに、UpdateXpress System Packs (UXSPs) や個別更新を適用するアプリケーションです。本ガイドでは、UpdateXpress アプリケーションをダウンロードして使用する方法について説明します。

本ガイドが対象とする読者

本書は、ファームウェアおよびデバイス・ドライバーの保守をよく理解しているシステム管理者またはシステム管理の担当者向けです。

規則および用語

太字の「注」、「重要」、または「注意」で始まっているパラグラフは、重要な情報を強調する特定の意味を持ちます。

注：これらの注記には、注意事項、説明、助言が書かれています。

重要：これらの注記には、不都合な、または困難な状態を避けるのに役立つ情報または助言が書かれています。

注意：これらの注記は、プログラム、デバイス、またはデータに損傷を及ぼすおそれのあることを示します。「重要」の注記は、損傷を起こすおそれのある指示や状態の記述の直前に書かれています。

本書でコマンドを入力するよう指示された場合は、コマンドを入力してから Enter を押します。

サポートされている Web サイト

このセクションでは、サポート Web リソースについて説明します。

- Lenovo XClarity Essentials Web サイト

  ThinkSystem および System x サーバーの複数のシステム管理ツールをダウンロードするには、この Web サイトを使用します。
- Lenovo XClarity Essentials UpdateXpress

  UpdateXpress アプリケーションをダウンロードするには、この Web サイトを使用します。

以下の Web サイトでは、製品の互換性とサポート、保証とライセンス、およびさまざまな技術リソースに関する情報を提供します。
- Lenovo Flex System サポート製品およびサービス
- ServerProven Web サイト
- Lenovo サーバー、ストレージ、およびネットワーキング・リソース・ライブラリー

第 1 章　技術的な概要

Lenovo XClarity Essentials UpdateXpress (これ以降 UpdateXpress アプリケーションと呼びます) を使用して、UpdateXpress System Packs (UXSPs) や個別更新を取得し、ご使用のローカル・システムまたはリモート・システムに適用できます。UpdateXpress アプリケーションは、UpdateXpress System Pack (UXSP) 更新パッケージおよび個別更新を取得してデプロイします。UXSP にはファームウェアおよびデバイス・ドライバーの更新が含まれています。

次のセクションでは、UpdateXpress アプリケーションの 4 つの主要機能を簡単に説明します。詳しくは、9 ページの 第 3 章「UpdateXpress アプリケーションの使用」を参照してください。

ローカル・サーバーの更新
UpdateXpress アプリケーションが現在実行されているローカル・マシンを更新します。マシン・タイプを検出し、更新を取得し自動的に適用します。

リモート・サーバーの更新
マシン上で実行されているベースボード管理コントローラー (BMC) を使用してリモート・マシンを更新します。ターゲットのリモート・マシンに更新を転送するために、簡易ファイル転送プロトコル (SFTP) サーバーが必要です。

更新のリポジトリーの作成
Lenovo サポート Web サイトから更新を取得するマシン・タイプを 1 つ以上選択します。指定されたフォルダーに更新がダウンロードされますが、更新は適用されません。後で UpdateXpress アプリケーションを使用して、Lenovo サポート Web サイトからでなく指定のフォルダーから更新を取得するように指示することにより、これらの更新を適用できます。

リモート RAID 構成
BMC サービスを使用して RAID アレイを構成します。

UpdateXpress System Pack (UXSP)

UXSP は、System x および ThinkSystem サーバー向けのファームウェアとドライバーのオンライン更新の統合テスト済みバンドルです。UXSP は、サポートの最初の 3 年間は半年ごとに、最後の 3 年間は 1 年ごとにリリースされます。

UXSP は、指定のシステムのドライバーとファームウェアのすべてのオンライン更新をダウンロードしてインストーするプロセスを簡素化します。UXSP を使用すると、常に Lenovo によってまとめてテストされバンドルされた完全で最新の更新セットを使用できます。

UXSP はマシン・タイプとオペレーティング・システムの組み合わせに対して作成されます。各 Windows® オペレーティング・システムや各 Linux ディストリビューションに対して、別々の UXSP が提供されます。たとえば、ある特定のマシン・タイプに対して複数の UXSP が存在する可能性があります。また、Windows オペレーティング・システムや各 Linux ディストリビューションの更新がある可能性もあります。

また、アウト・オブ・バンド方式でシステムを更新できるプラットフォーム UXSP の一種もあります。プラットフォーム UXSP にはオペレーティング・システムは含まれません。

UXSP 形式
UXSP は XML ファイルで配信されます。UXSP の命名規則は次の形式です。
lnvgy_utl_uxsp_*version_operatingsystem_arch*.xml
例: `lnvgy_utl_uxsp_a3sp27a-1.00_windows_32-64.xml`

UpdateXpress アプリケーションを使用した UXSP 更新の適用

UpdateXpress アプリケーションを使用して、ご使用のマシンに UXSP 更新を適用できます。UpdateXpress アプリケーションは更新を適用するマシンのインベントリーを作成し、適用できる更新パッケージがあるかどうかを指定されたロケーションに対して照会します。インベントリーと適用可能な更新リストを比較して、適用する更新のセットを推奨し、その後それらの更新をマシンにデプロイします。

UpdateXpress アプリケーションを使用して UXSP を適用するには、以下を行います。

1. UpdateXpress アプリケーションを Lenovo サポート Web サイトからダウンロードします。
2. UpdateXpress アプリケーションを実行します。「**ローカル・マシンの更新**」または「**リモート・マシンの更新**」を選択します。
3. 「**Lenovo サポート Web サイトの確認**」を選択します。
4. 「**UpdateXpress アプリケーション・システム・パック (UXSP)**」を選択します。

更新を Lenovo サポート Web サイトから直接ダウンロードすることもできます。XML ファイルとともに更新ペイロードを忘れずにダウンロードしてください。各 UXSP のダウンロードに同じ宛先フォルダーを選択すると便利です。異なるマシン・タイプ用の複数のシステム・パックを同じフォルダーにダウンロードできます。UpdateXpress アプリケーションを実行すると、マシン・タイプが検出され、そのマシン・タイプ用の正しいコンテンツが使用されます。場合によっては、システム・パック間で共通のファイルがあることがあります。既にフォルダーにある共通ファイルは再度ダウンロードされることはありません。そのため、ダウンロードにかかる全体時間が減少します。

UXSP をバンドルとして処理する

UpdateXpress アプリケーションは UXSP をダウンロードして適用するように設計されています。UXSP は UXSP XML ファイルで指定されている個別更新のコレクションです。

UpdateXpress アプリケーションを実行するときに、UXSP を使用するか個別更新を使用するかを選択できます。多くの場合、UXSP の使用が推奨されますが、個別更新を使用すると、どの更新を使用するかを非常に柔軟に選択できます。

更新の要件の処理

このトピックでは、更新の要件の取得および適用方法について説明します。

更新を正常に適用するには、その更新のすべての前提条件および必要条件も取得して適用する必要があります。UpdateXpress アプリケーションは前提条件や必要条件を自動的に確認、取得、および適用します。更新では多くの場合、正常に適用されるには事前に前提条件ファイルを適用する必要があります。または、適用された更新を正常に使用するために必要条件パッケージを含める必要がある場合もあります。更新プロセスを簡素化するために、UpdateXpress アプリケーションは更新ファイルに含まれる情報を使用して指定された更新に必須のパッケージを識別します。その後、UpdateXpress アプリケーションはこれらの必須パッケージを適用します。

前提条件ファイル

Lenovo によって提供される更新パッケージには、正常に更新を適用するために事前に適用する必要がある前提条件ファイルの情報が含まれています。更新を指定すると、UpdateXpress アプリケーションはこの情報を読み取り、前提条件パッケージを検索します。

デフォルトでは、UpdateXpress アプリケーションは更新パッケージを取得して評価し、前提条件が満たされているかどうかを判別して、必要に応じて指定された更新を適用する前に前提条件ファイルを自動的に適用します。ユーザーは、前提条件ファイルを適用しないことも選択できます。ただし、これを行うと更新が正常に適用されない可能性があります。

前提条件パッケージに前提条件または必要条件がある場合、それらも同様に取得、評価、適用されます。

必要条件ファイル

一部の更新では、必要条件ファイルが必要です。これは更新を正常に完了するために適用する必要がある追加パッケージですが、指定された更新の前に適用する必要はありません。

デフォルトでは、UpdateXpress アプリケーションは必要条件パッケージを更新の一部として識別、評価、適用します。

必要条件パッケージに前提条件または必要条件がある場合、それらも同様に取得、評価、適用されます。

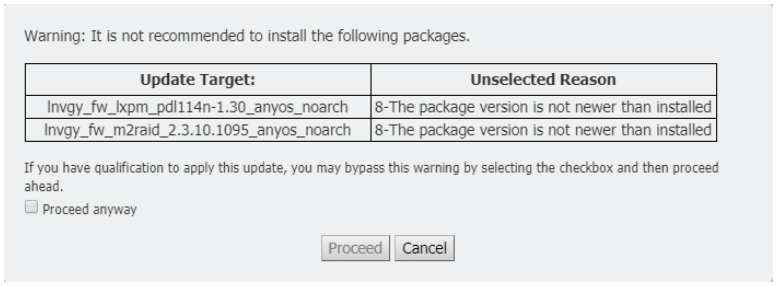
例

たとえば、前提条件と必要条件の両方がある更新の場合を考えてみます。デフォルトでは、UpdateXpress アプリケーションは以下の手順を実行します。

1. 更新を確実に完了させるために、UpdateXpress アプリケーションは最初に更新をダウンロードします。
2. 前提条件ファイルがダウンロードされます。
3. 必要条件ファイルがダウンロードされます。
4. 前提条件ファイルまたは必要条件ファイルは、システムの現在の状態に対して評価されます。これらの条件が適用済みで、システムが既に必要なレベルにある場合、この条件は無視されます。
5. 必要な前提条件ファイルが適用されます。
6. 更新が適用されます。
7. 必要な必要条件ファイルが適用されます。

推奨される更新

デフォルトでは、アプリケーション UpdateXpress はシステムをインストールまたはアップグレードするために推奨されるパッケージを選択します。ユーザーは、インストールまたはアップグレードするパッケージを手動で選択することもできます。この場合、ログに次のような警告メッセージが表示されます。



このメッセージが表示された場合は、更新プロセスを中止することをお勧めします。

オペレーティング・システムに依存しない更新

一部の個別更新は、使用されているオペレーティング・システムに関係なく、特定のマシン・タイプに適用されます。これらの個別更新は、オペレーティング・システムに依存しない更新として扱われます。オペレーティング・システム固有の更新を選択するのと同じ方法でオペレーティング・システムに依存しない更新を選択できます。

注：オペレーティング・システム固有の更新を選択する場合、オペレーティング・システムに依存しない更新はパッケージの一部として含まれます。マシン・タイプのオペレーティング・システム更新を選択しない場合にのみ、オペレーティング・システムに依存しない更新を選択します。

欠落している、または完了しなかったインベントリー・データ

場合によってはUpdateXpressアプリケーションがファームウェアまたはドライバーのバージョンを判断できないコンポーネントに更新パッケージが適用されることがあります。この場合、UpdateXpressアプリケーションはコンポーネントのバージョンではなく、更新パッケージのバージョンを表示します。取り付けられているコンポーネントのバージョンが検出されない場合、デフォルトでは更新が選択されません。この場合は、パッケージを推奨更新として手動で選択します。

必要なドライバーのインストール

UpdateXpressアプリケーションは、必要なデバイス・ドライバーをインストールします。

次の場合にUpdateXpressアプリケーションはUXSPのすべてのドライバーをインストールします。
- 現行のデバイス・ドライバーがUXSP内の使用可能なデバイス・ドライバーより古い。
- UpdateXpressアプリケーションが現行のデバイス・ドライバーのバージョンを判別できない。これは通常、デバイス・ドライバーがインストールされていない場合に発生します。

  注：インストールされているデバイス・ドライバーのバージョンが検出されない場合、UpdateXpressアプリケーションは「**未検出**」と表示します。

この動作を利用して、ファームウェア更新に必要な次のデバイス・ドライバーをインストールできます。
- Intelligent Peripheral Management Interface (IPMI)
- IPMIマッピング・レイヤー

第 2 章 ハードウェアとソフトウェアの要件

UpdateXpress アプリケーションの使用を開始する前に、ハードウェア、オペレーティング・システム、およびローカル・オペレーティング・システムの特権要件を確認してください。UpdateXpress アプリケーションを実行するシステムには、少なくとも 1 GB のランダム・アクセス・メモリー (RAM) が必要です。

サポートされるサーバー・モデル

UpdateXpress アプリケーションは、使用可能な UXSP に含まれる Windows および Linux デバイス・ドライバーおよびファームウェアをサポートします。現在サポートされているコンポーネントのデバイス・ドライバーおよびファームウェアのリストは、各システム・パックに含まれる UpdateXpress アプリケーション readme ファイルに含まれています。

表 1. サポートされる Lenovo システム

シリーズ	サーバー・モデル	
ThinkEdge	• SE350 V2 (7DA9) • SE360 V2 (7DAM)	• SE450 (7D8T) • SE455 V3 (7DBY)
ThinkSystem	• DX1100U ゲートウェイ (7D49) • DX1100U パフォーマンス/容量 (7D4A) • DXN2000 ストレージ (7D5W) • SD530 (7X21) • SD530 V3 (7DD3、7DDA) • SD550 V3 (7DD2、7DD9) • SD555 V3 (7DDM、7DDN) • SD630 V2 (7D1K) • SD650 DWC (7X58) • SD650 V2 (7D1M) • SD650 V3 (7D7M) • SD650-I V3 (7D7L) • SD650-N V3 (7D7N) • SD665 V3 (7D9P) • SD665-N V3 (7DAZ) • SD670 V2 (7D1N) • SE350 (7Z46、7D1X、7D27) • SN550 (7X16) • SN550 V2 (7Z69) • SN850 (7X15) • SR150/SR158 (7Y54、7Y55) • SR250 (7Y51、7Y52) • SR250 V2 (7D7R、7D7Q) • SR250 V3 (7DCM、7DCL) • SR258 V2 (7D7S) • SR258 V3 (7DCN) • SR530 (7X07、7X08) • SR550 (7X03、7X04) • SR570 (7Y02、7Y03) • SR590 (7X98、7X99) • SR630 (7X01、7X02) • SR630 V2 (7Z70、7Z71) • SR630 V3 (7D72、7D73、7D74)	• SR635 (7Y98、7Y99)[1] • SR635 V3 (7D9G、7D9H) • SR645 (7D2X、7D2Y) • SR645 V3 (7D9C、7D9D) • SR650 (7D4K、7X05、7X06) • SR650 V2 (7D15、7Z72、7Z73) • SR650 V3 (7D75、7D76、7D77) • SR655 (7Y00、7Z01)[1] • SR655 V3 (7D9E、7D9F) • SR665 (7D2V、7D2W) • SR665 V3 (7D9A、7D9B) • SR670 (7D4L、7Y36、7Y37、7Y38) • SR670 V2 (7Z22、7Z23) • SR675 V3 (7D9Q、7D9R) • SR850 (7X18、7X19) • SR850 V2 (7D31、7D32、7D33) • SR850 V3 (7D96、7D97、7D98) • SR850P (7D2H、7D2F、7D2G) • SR860 (7X69、7X70) • SR860 V2 (7Z59、7Z60、7D42) • SR860 V3 (7D93、7D94、7D95) • SR950 (7X11、7X12、7X13) • SR950 V3 (7DC4、7DC5、7DC6) • ST250 (7Y45、7Y46) • ST250 V2 (7D8F、7D8G) • ST250 V3 (7DCF、7DCE) • ST258 V2 (7D8H) • ST258 V3 (7DCG) • ST550 (7X09、7X10) • ST558 (7Y15、7Y16) • ST650 V2/ST658 V2 (7Z74、7Z75、7Z76) • ST650 V3 (7D7A、7D7B) • ST658 V3 (7D7C)
ThinkServer	• DN8848 V2 (7D6A、7D8U) • SE550 V2 (7D68) • SR588/SR590 (7D4M) • SR588 V2/SR590 V2 (7D53)	• SR660 V2/SR668 V2 (7D6L) • SR860P (7D5D) • WH5900 アプライアンス (7D5V)

表 1. サポートされる Lenovo システム (続き)

シリーズ	サーバー・モデル	
WenTian	• WA5480 G3/WA5488 G3 (7DE7) • WR3220 G2/WR3228 G2 (7DEC)	• WR5220 G3/WR5228 G3 (7D8Y)
ソリューション	• ThinkAgile VX シリーズ (7D28、7D2Z、7D43、7DDK、7Y12、7Y13、7Y14、7Y92、7Y93、7Y94、7Z12、7Z13、7Z62、7Z63) • ThinkAgile MX シリーズ (7D19、7D1B、7D1H、7D5R、7D5S、7D5T、7D66、7D67、7D6B、7DGG、7Z20)	• ThinkAgile HX シリーズ (7D20、7D2T、7D46、7D4R、7D5U、7X82、7X83、7X84、7Y88、7Y89、7Y90、7Y95、7Y96、7Z03、7Z04、7Z05、7Z08、7Z09、7D0W、7D0Y、7D0Z、7D11、7D52、7Z82、7Z84、7Z85)
System x	• HX 3310 アプライアンス (8693) • HX 5510/7510 アプライアンス (8695) • nx360 M5 (5465、5467) • x240 計算ノード (7162、2588) • x240 M5 計算ノード (2591、9532) • x280 X6/x480 X6/x880 X6 計算ノード (4258、7196)[2] • x440 (7167, 2590)	• x3250 M6 (3633、3943) • x3500 M5 (5464) • x3550 M5 (5463、8869) • x3650 M5 (5462、8871) • x3750 M4 (8753) • x3850 X6/x3950 X6 (6241)[2]
注： 1. このサーバー・モデルは AMD 1 ソケット・プロセッサー・ベースです。 2. このサーバー・モデルは単一ノードと複数ノードの両方をサポートします。		

サポートされているオペレーティング・システム

UpdateXpress アプリケーションは Linux および Windows オペレーティング・システムでサポートされています。

Windows

UpdateXpress アプリケーションは、64 ビットのオペレーティング・システムでサポートされています。UpdateXpress アプリケーションでサポートされているオペレーティング・システムを識別するには、次の表の情報を使用します。

表 2. サポートされる Windows オペレーティング・システム

オペレーティング・システム	ローカル更新	リモート更新	ローカル・リポジトリー	リモート RAID 構成
ワークステーション向け Microsoft Windows 10/11 Pro (21H2/22H2)	あり 注	あり	あり	あり
Microsoft Windows Server 2016	あり	あり	あり	あり
Microsoft Windows Server 2019	あり	あり	あり	あり
Microsoft Windows Server 2022	あり	あり	あり	あり

注：ワークステーション向け Microsoft Windows 10/11 Pro (21H2/22H2) をサポートするサーバー・モデルは、ローカル更新機能にもアクセスできます。

Linux

UpdateXpress アプリケーションは次のバージョンの Linux オペレーティング・システムでサポートされています。

表 3. サポートされる Linux オペレーティング・システム

オペレーティング・システム	ローカル更新	リモート更新	ローカル・リポジトリー	リモート RAID 構成
Red Hat Enterprise Linux 7.X (7.6 以降のバージョン)	あり	あり	あり	あり
Red Hat Enterprise Linux 8.X	あり	あり	あり	あり
Red Hat Enterprise Linux 9.X	あり	あり	あり	あり
SUSE Linux Enterprise Server 15.X	あり	あり	あり	あり

注：

- Linux オペレーティング・システムで UpdateXpress アプリケーションを実行する場合は、500 MB のフリー・ディスク・スペースが推奨されます。
- UpdateXpress アプリケーションはファジー・オペレーティング・システム・チェックをサポートしています。現在のオペレーティング・システムが UXSP 内のファームウェア・パッケージをサポートしていない場合、そのファームウェア・パッケージが UpdateXpress アプリケーションの比較結果に表示される場合があります。
- Linux OS の `ifconfig` コマンドによっては、UpdateXpress が RHEL 7.0 以降のバージョンにインストールされていない場合があります。RHEL 7.0 以降のバージョンでファームウェアを更新するには、ネット・ツールをインストールする必要があります。
- Linux デバイス・ドライバーの更新には特定のパッケージが必要です。以下のパッケージがインストールされている必要があります。
  - Red Hat Enterprise Linux: rpm-build、perl、および bash
  - SUSE Enterprise Linux: perl および bash
- 以下のオペレーティング・システムでは、代わりに UpdateXpress 4.3.0 を使用できます。
  - SUSE 12.5
- 以下のオペレーティング・システムでは、代わりに UpdateXpress 4.1.0 を使用できます。
  - RedHat 7.5
  - SUSE 12.4
- 以下のオペレーティング・システムでは、代わりに UpdateXpress 3.4.0 を使用できます。
  - RedHat 7.0/7.1/7.2/7.3/7.4
  - SUSE 12.0/12.1/12.2/12.3
  - Windows 7/8
  - Windows Server 2008R2/2012/2012R2

オペレーティング・システム特権

UpdateXpress アプリケーションを実行するには、ユーザーが管理者特権または root と同等のオペレーティング・システム特権を持っている必要があります。権限が足りないユーザーがプログラムを実行しようとすると、UpdateXpress アプリケーションはエラーを返します。

UpdateXpress アプリケーションとその抽出、および機密性の高いログは、権限を持つユーザーのみがアクセスできるを安全な場所に保存します。

第 3 章 UpdateXpress アプリケーションの使用

UpdateXpress アプリケーションを使用して、更新を手動で適用できます。UpdateXpress アプリケーションを実行する際は、1024 x 768 以上の画面解像度が推奨されます。UpdateXpress アプリケーションを実行するには、圧縮ファイルを解凍してご使用のオペレーティング・システム用の実行可能ファイルを起動します。インストールは不要です。

Windows

Windows オペレーティング・システムの場合、UpdateXpress アプリケーションの名前は次のとおりです。

```
lnvgy_utl_lxce_ux{ build id }_4.x.x_windows_x86-64.zip
```

UpdateXpress アプリケーションの各リリースは、バージョン番号で Windows ZIP ファイル名を識別できます。Windows ZIP ファイルは **lnvgy_utl_lxce_ux{ build id }_{ version }_windows_i386.zip** と指定されます。ここで *lnvgy_utl_lxce_ux* は zip ファイルの名前であり、*build id* は Build 番号を、*version* は UpdateXpress アプリケーションのバージョン番号を示します。

Linux

Linux オペレーティング・システムの場合、UpdateXpress アプリケーションの名前は次のとおりです。

オペレーティング・システム	UpdateXpress アプリケーションの名前
Red Hat Enterprise Linux 7.X/8.X/9.X AMD64/EM64T 以降	`lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz`
SUSE Linux Enterprise Server 12.X/15.X AMD64/EM64T 以降	`lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz`

UpdateXpress アプリケーションの名前は、Windows オペレーティング・システムと Linux オペレーティング・システムでは異なります。便宜上、本書では以降 Windows と Linux 両方のオペレーティング・システム用の UpdateXpress アプリケーションの名前として *<Zipfile>* を使用します。

UpdateXpress アプリケーションの起動

UpdateXpress アプリケーションを使用して、最新の UXSP および個別更新を取得できます。

UpdateXpress アプリケーションを起動するには、以下を行います。

- **Windows の場合**:
  1. *<Zipfile>* をローカル・フォルダーに解凍します。
  2. 次のいずれかを行います。
     - **lxce_ux.exe** をダブルクリックします。
     - **lxce_ux.exe** を右クリックして、ポップアップ・メニューの「**管理者として実行**」をクリックします。
- **Linux の場合**:

  ターミナルに以下のコマンドを入力します。

  ```
  tar xvf <Zipfile>
  ./start_lxce_ux.sh
  ```

ローカル・サーバーの Web サイトからの更新

UpdateXpress アプリケーションは Web サイトから取得した UXSP または個別更新を使用してローカル・マシンを更新できます。

このタスクを完了するには、以下の前提条件を満たす必要があります。
- UpdateXpress アプリケーションが更新するローカル・マシン上で実行されている。
- マシンがサポートされているオペレーティング・システムを実行している。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。

Web サイトからローカル・マシンを更新するには、以下を行います。
1. UpdateXpress アプリケーションを起動します。9 ページの「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**ローカル・サーバーの管理**」を選択します。「**BMC アクセス情報の入力**」を選択した場合、このウィンドウに BMC 情報を入力して「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ターゲット・サーバーでの更新の実行**」を選択し、「**次へ**」をクリックします。
5. 「更新設定」ウィンドウで、以下の操作を 1 つ以上行います。
   - バックアップ・システム・ファームウェアをアップグレードするには、「**BMC (および該当する場合は UEFI)のバックアップ・イメージのみを更新する**」を選択して、「**次へ**」をクリックします。
   - ファームウェアをダウングレードするには、「**バックレベル・ファームウェアへの更新を有効にする**」を選択して、「**次へ**」をクリックします。
6. 「更新ロケーション」ウィンドウで「**Lenovo サポート Web サイトの確認**」を選択して、「**次へ**」をクリックします。
7. 「更新タイプ」ウィンドウで、ターゲット更新タイプを選択して、「**次へ**」をクリックします。
8. 「ターゲット・ディレクトリー」ウィンドウでは、更新をダウンロードする場所を指定するか、デフォルトの場所のままにして、「**次へ**」をクリックします。
9. 「インターネット・アクセス」ページで、ユーザーのセキュリティー・アクセスに特別な要件がない場合は、「**テスト接続**」をクリックしてターゲット URL のネットワーク接続を確認し、「**次へ**」をクリックします。
   セキュリティーに関する他の懸念事項がある場合は、「**テスト接続**」をクリックする前に、以下の操作を 1 つ以上行います。
   - 「**プロキシ・サーバー**」を構成します。
     a. Web への接続に HTTP/HTTPS プロキシが必要な場合は「**プロキシ・サーバー**」を選択し、以下のフィールドに入力します。

プロキシ・タイプ	プロキシ・サーバーのプロキシ・タイプ。
IP アドレスまたはホスト名	プロキシ・サーバーのホスト名、IP アドレス、またはドメイン名。
ポート	プロキシ・サーバーのポート番号。

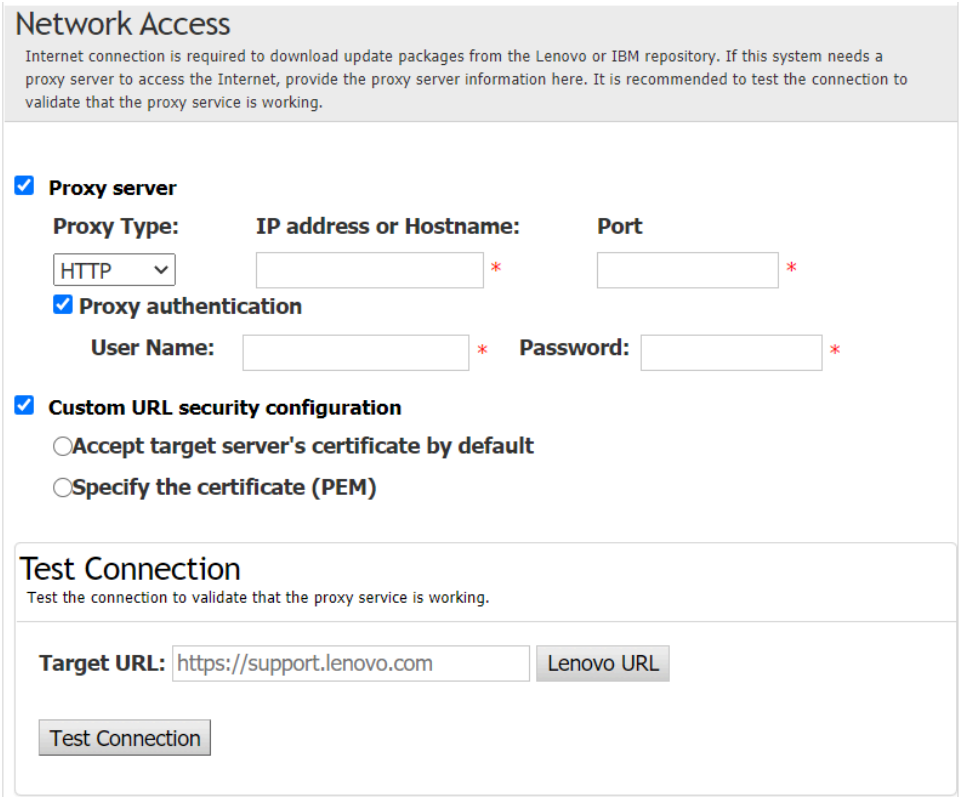
     b. プロキシ・サーバーへの認証に資格情報を指定する必要がある場合は「**プロキシ認証**」を選択し、以下のフィールドに入力します。

ユーザー名	プロキシ・サーバーへの認証用のユーザー名。
パスワード	指定されたユーザー名のパスワード。

   - 「**カスタム URL セキュリティー構成**」の構成

     リバース・プロキシが必要な場合は「**カスタム URL セキュリティー構成**」を選択し、以下のいずれかのオプションを選択します。
     – **デフォルトでターゲット・サーバーの証明書を受け入れる**

– **証明書 (PEM) を指定する**



10. 「推奨される更新」ウィンドウで、以下の操作を 1 つ以上行います。
    - すべての更新パッケージを表示するには、「**未検出のデバイスの更新を表示する**」を選択します。
    - コンポーネントを更新するには、ターゲット・コンポーネントを選択し、「**次へ**」をクリックします。
11. 「更新の取得」ウィンドウの取得表に、パッケージの取得の進行状況が表示されます。進行状況が完了したら、「**次へ**」をクリックします。
12. 「更新の実行」ウィンドウで、「**更新を開始しポップ・ウィンドウで続行を確認する**」をクリックします。実行テーブルには、パッケージのアップグレードの進行状況が表示されます。アップグレードの進行状況が完了したら、「**次へ**」をクリックします。
13. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、「**閉じる**」をクリックして終了します。

ローカル・サーバーのローカル・ディレクトリーからの更新

UpdateXpress アプリケーションはローカル・フォルダーから取得した UXSP または個別更新を使用してローカル・マシンを更新できます。

このタスクを完了するには、以下の前提条件を満たす必要があります。
- UpdateXpress アプリケーションが更新するローカル・マシン上で実行されている。
- マシンがサポートされているオペレーティング・システムを実行している。サポートされているオペレーティング・システムについて詳しくは、6 ページの 「サポートされているオペレーティング・システム」を参照してください。
- マウントされた ISO を有効なローカル・ディレクトリーとして使用しないでください。使用すると、更新プロセス中にアンマウントされ、フラッシュの障害が発生する場合があります。

ローカル・ディレクトリーからローカル・マシンを更新するには、以下を行います。
1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。

2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**ローカル・サーバーの管理**」を選択して「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ターゲット・サーバーでの更新の実行**」を選択し、「**次へ**」をクリックします。
5. 「更新設定」ウィンドウで、以下の操作を 1 つ以上行います。
   - BMC または UEFI のバックアップ・イメージを更新するには、「**BMC (および該当する場合は UEFI)のバックアップ・イメージのみを更新する**」を選択して、「**次へ**」をクリックします。
   - ファームウェアをダウングレードするには、「**バックレベル・ファームウェアへの更新を有効にする**」を選択して、「**次へ**」をクリックします。
6. 「更新ロケーション」ウィンドウで、「**ローカル・ディレクトリーを検索**」を選択します。ローカル・フォルダーを指定するには、以下のいずれかを行います。
   - 「**参照**」をクリックし、ターゲット・フォルダーを選択して、「**次へ**」をクリックします。
   - 「**参照**」ボタンの横にあるフィールドにフォルダーのパスを入力して、「**次へ**」をクリックします。
7. 「更新タイプ」ウィンドウで、ターゲット更新タイプを選択して、「**次へ**」をクリックします。
8. 「推奨される更新」ウィンドウで、以下のいずれかを実行します。
   - すべての更新パッケージを表示するには、「**アダプターが検出されない更新を表示する**」を選択します。
   - インストール済みのドライバーとファームウェアのバージョンを、最新バージョンと比較するには、「**開始**」をクリックします。進行状況が完了したら、ターゲット・パッケージを 1 つ以上選択し、「**次へ**」をクリックします。
   - ローカル・システムにインストールされているデバイスのバージョンを最新バージョンと比較するには、「**インストール済みデバイスのみ**」を選択し、「**開始**」をクリックします。進行状況が完了したら、ターゲット・パッケージを 1 つ以上選択し、「**次へ**」をクリックします。
9. 「更新の実行」ウィンドウで、「**更新を開始しポップ・ウィンドウで続行を確認する**」をクリックします。実行テーブルには、パッケージのアップグレードの進行状況が表示されます。アップグレードの進行状況が完了したら、「**次へ**」をクリックします。
10. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、「**閉じる**」をクリックして終了します。

リモート・サーバーの Web サイトからの更新

UpdateXpress アプリケーションは Web サイトから取得した UXSP または個別更新を使用してリモート・マシンを更新できます。

このタスクを完了するには、以下の前提条件を満たす必要があります。

UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているマシンで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。

Web サイトからリモート・マシンを更新するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - **(設定) IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - **(設定) ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - **(設定) パスワード**: ターゲット・システムの BMC パスワードです。
   - **(設定) ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

注：BMC サーバー証明書を確認しない場合、「**デフォルトで BMC サーバーの証明書を承認します**」を選択して「**次へ**」をクリックします。

4. 「タスク」ウィンドウで、「**ターゲット・サーバーでの更新の実行**」を選択し、「**次へ**」をクリックします。
5. 「更新設定」ウィンドウで、1 つまたは複数のオプションを選択します。「**BMC サーバーではなく別個のリモート・サーバーを使用する**」が選択されている場合、以下の情報を入力します。
   - (SFTP/HTTP/HTTPS/FTP 設定) **IP アドレスまたはホスト名**: サーバーの IP アドレスまたはホスト名です。
   - (SFTP/HTTP/HTTPS/FTP 設定) **ユーザー名**: サーバーのユーザー名です。
   - (SFTP/HTTP/HTTPS/FTP 設定) **パスワード**: サーバーのパスワードです。
   - (SFTP/HTTP/HTTPS/FTP 設定) **ポート**: サーバーのポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。
   - (SFTP/HTTP/HTTPS/FTP 設定) **ディレクトリー**: 更新パッケージをコピーするサーバーのロケーションです。

     注：SFTP/HTTP/HTTPS/FTP サーバーの絶対パスを入力します。FTP サーバーは、5 ページの「サポートされるサーバー・モデル」で上付き文字 2 (注 2) によってマークされた ThinkServer にのみ使用されます。
6. SFTP サーバーの鍵フィンガープリントを構成するには、以下のいずれかを実行します。
   - SFTP サーバーの鍵フィンガープリントを確認するには、「**はい**」をクリックします。
   - SFTP/HTTPS サーバーの鍵フィンガープリントを確認しない場合、「**SFTP サーバーの鍵フィンガープリントをスキップする**」を選択して「**次へ**」をクリックします。
7. 以下の操作を 1 つ以上行います。
   - ファームウェアをダウングレードするには、「**バックレベル・ファームウェアへの更新を有効にする**」を選択して、「**次へ**」をクリックします。
   - バックアップ・システム・ファームウェアをアップグレードするには、「**BMC (および該当する場合は UEFI)のバックアップ・イメージのみを更新する**」を選択して、「**次へ**」をクリックします。
8. 「更新ロケーション」ウィンドウで「**Lenovo サポート Web サイトの確認**」を選択して、「**次へ**」をクリックします。
9. 「ターゲット・ディレクトリー」ウィンドウでは、更新をダウンロードする場所を指定するか、デフォルトの場所のままにして、「**次へ**」をクリックします。
10. 「インターネット・アクセス」ページで、ユーザーのセキュリティー・アクセスに特別な要件がない場合は、「**テスト接続**」をクリックしてターゲット URL のネットワーク接続を確認し、「**次へ**」をクリックします。
    セキュリティーに関する他の懸念事項がある場合は、「**テスト接続**」をクリックする前に、次のように、セキュリティー要件に応じて「**プロキシ・サーバー**」および/または「**カスタム URL セキュリティー構成**」を構成します。
    - **プロキシ・サーバー**
      a. Web への接続に HTTP/HTTPS プロキシが必要な場合は「**プロキシ・サーバー**」を選択し、以下のフィールドに入力します。

プロキシ・タイプ	プロキシ・サーバーのプロキシ・タイプ。
IP アドレスまたはホスト名	プロキシ・サーバーのホスト名、IP アドレス、またはドメイン名。
ポート	プロキシ・サーバーのポート番号。

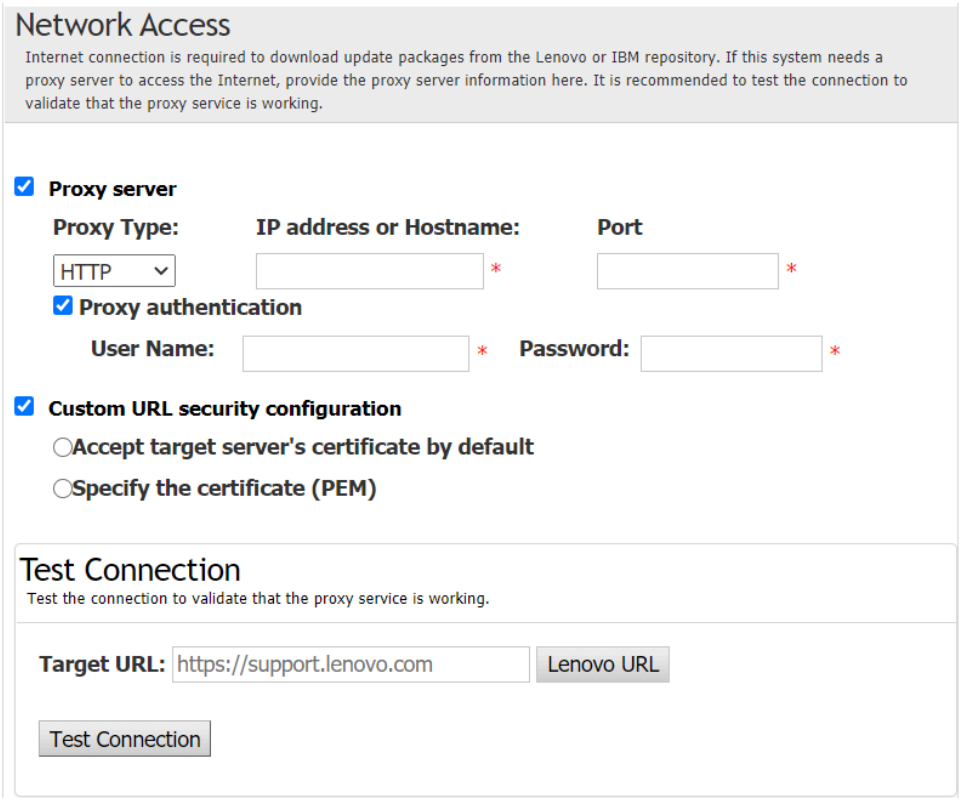
      b. プロキシ・サーバーへの認証に資格情報を指定する必要がある場合は「**プロキシ認証**」を選択し、以下のフィールドに入力します。

ユーザー名	プロキシ・サーバーへの認証用のユーザー名。
パスワード	指定されたユーザー名のパスワード。

    - **カスタム URL セキュリティー構成**

      リバース・プロキシが必要な場合は「**カスタム URL セキュリティー構成**」を選択し、以下のいずれかのオプションを選択します。

– **デフォルトでターゲット・サーバーの証明書を受け入れる**
– **証明書 (PEM) を指定する**



11. 「更新タイプ」ウィンドウで、ターゲット更新タイプを選択して、「**次へ**」をクリックします。
12. 「推奨される更新」ウィンドウで、以下の操作を 1 つ以上行います。
    - すべての更新パッケージを表示するには、「**未検出のデバイスの更新を表示する**」を選択します。
    - コンポーネントを更新するには、ターゲット・コンポーネントを選択し、「**次へ**」をクリックします。
13. 「更新の取得」ウィンドウの取得表に、パッケージの取得の進行状況が表示されます。進行状況が完了したら、「**次へ**」をクリックします。
14. 「更新の実行」ウィンドウで、「**更新を開始しポップ・ウィンドウで続行を確認する**」をクリックします。実行テーブルには、パッケージのアップグレードの進行状況が表示されます。アップグレードの進行状況が完了したら、「**次へ**」をクリックします。
15. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

リモート・サーバーのローカル・ディレクトリーからの更新

UpdateXpress アプリケーションはローカル・フォルダーから取得した UXSP または個別更新を使用してリモート・マシンを更新できます。

このタスクを完了するには、以下の前提条件を満たす必要があります。

UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているマシンで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。

ローカル・ディレクトリーからリモート・マシンを更新するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの「UpdateXpress アプリケーションの起動」を参照してください。

2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書と SFTP/HTTPS サーバーの鍵フィンガープリントを検査しない場合は、「**BMC サーバーの証明書および SFTP/HTTPS サーバーの鍵フィンガープリントをデフォルトで受け入れます**」というメッセージの前にあるチェックボックスにチェックを入れ、「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ターゲット・サーバーでの更新の実行**」を選択し、「**次へ**」をクリックします。
5. 「更新設定」ウィンドウで、「**別個のリモート・サーバーを使用する**」が選択されている場合、以下の情報を入力します。
   - (SFTP/HTTP/HTTPS/FTP 設定) **IP アドレスまたはホスト名**: サーバーの IP アドレスまたはホスト名です。
   - (SFTP/HTTP/HTTPS/FTP 設定) **ユーザー名**: サーバーのユーザー名です。
   - (SFTP/HTTP/HTTPS/FTP 設定) **パスワード**: サーバーのパスワードです。
   - (SFTP/HTTP/HTTPS/FTP 設定) **ポート**: サーバーのポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。
   - (SFTP/HTTP/HTTPS/FTP 設定) **ディレクトリー**: 更新パッケージをコピーするサーバーのロケーションです。

     注：SFTP/HTTP/HTTPS/FTP サーバーの絶対パスを入力します。FTP サーバーは、5 ページの 「サポートされるサーバー・モデル」で上付き文字 2 (注 2) によってマークされた ThinkServer にのみ使用されます。
6. SFTP サーバーの鍵フィンガープリントを構成するには、以下のいずれかを実行します。
   - SFTP サーバーの鍵フィンガープリントを確認するには、「**はい**」をクリックします。
   - SFTP/HTTPS サーバーの鍵フィンガープリントを確認しない場合、「**SFTP サーバーの鍵フィンガープリントをスキップする**」を選択して「**次へ**」をクリックします。
7. 以下の操作を 1 つ以上行います。
   - ファームウェアをダウングレードするには、「**バックレベル・ファームウェアへの更新を有効にする**」を選択して、「**次へ**」をクリックします。
   - バックアップ・システム・ファームウェアをアップグレードするには、「**BMC (および該当する場合は UEFI)のバックアップ・イメージのみを更新する**」を選択して、「**次へ**」をクリックします。
8. 「更新ロケーション」ウィンドウで、「**ローカル・ディレクトリーを検索**」を選択します。ローカル・フォルダーを指定するには、以下のいずれかを行います。
   - 「**参照**」をクリックし、目的のフォルダーを選択して、「**次へ**」をクリックします。
   - 「**参照**」ボタンの横にあるフィールドにフォルダーのパスを入力して、「**次へ**」をクリックします。
9. 「更新タイプ」ウィンドウで、ターゲット更新タイプを選択して、「**次へ**」をクリックします。
10. 「推奨される更新」ウィンドウで、「**開始**」をクリックして、インストール済みファームウェアのバージョンを、最新バージョンと比較します。進行状況が完了したら、ターゲット・パッケージを 1 つ以上選択し、「**次へ**」をクリックします。

    注：すべての更新パッケージを表示するには、「**アダプターが検出されない更新を表示する**」を選択してから「**開始**」をクリックします。
11. 「更新の実行」ウィンドウで、「**更新を開始しポップ・ウィンドウで続行を確認する**」をクリックします。実行テーブルには、パッケージのアップグレードの進行状況が表示されます。アップグレードの進行状況が完了したら、「**次へ**」をクリックします。
12. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

リモート・サーバーの BIOS の構成

UpdateXpress アプリケーションは、リモート・サーバーの BIOS 設定の構成をサポートしています。

前提条件:

リモート・サーバーの BIOS 構成機能は、ThinkServer/WenTian サーバーでのみサポートされます。サポートされているオペレーティング・システムについて詳しくは、6 ページの 「サポートされているオペレーティング・システム」を参照してください。

BIOS を設定するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書と SFTP/HTTPS サーバーの鍵フィンガープリントを検査しない場合は、「**BMC サーバーの証明書および SFTP/HTTPS サーバーの鍵フィンガープリントをデフォルトで受け入れます**」というメッセージの前にあるチェックボックスにチェックを入れ、「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**BIOS 構成**」を選択し、「**次へ**」をクリックします。
5. 「構成モード」ウィンドウで、「**共通 BIOS 構成**」または「**BIOS 構成ファイルのインポート**」を選択し、「**次へ**」をクリックします。
6. 次のいずれかを行います。
   - 前の手順で「**BIOS 構成ファイルのインポート**」が選択されている場合は、この手順をスキップします。
   - 前の手順で「**共通 BIOS 構成**」が選択されている場合は、現在の値を 1 つ以上選択し、「**次へ**」をクリックします。
7. 「BIOS 変更ビュー」ウィンドウで、データが「**表示**」、「**チェック**」、および「**確認**」に変更されます。「**次へ**」をクリックします。
8. 「BIOS 構成のエクスポート」ウィンドウで、構成をファイルとしてエクスポートします。エクスポートしたファイルの場所を指定し、「**次へ**」をクリックします。
9. 「実行中の構成」ウィンドウで、「**手動で再起動**」または「**直ちに再起動**」を選択し、「**スタート**」をクリックします。タスクが完了したら、「**次へ**」をクリックします。
10. 「終了」ウィンドウで、「**ログの表示**」をクリックして構成ログを確認し、「**閉じる**」をクリックして終了します。

リモート・サーバーのログの収集

UpdateXpress アプリケーションは、リモート・サーバーのログの収集をサポートします。

前提条件:

リモート・サーバーの収集機能は、ThinkServer サーバー/WenTian サーバーでのみサポートされます。サポートされているオペレーティング・システムについて詳しくは、6 ページの 「サポートされているオペレーティング・システム」を参照してください。

ログを収集するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書と SFTP/HTTPS サーバーの鍵フィンガープリントを検査しない場合は、「**BMC サーバーの証明書および SFTP/HTTPS サーバーの鍵フィンガープリントをデフォルトで受け入れます**」というメッセージの前にあるチェックボックスにチェックを入れ、「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ログの収集**」を選択し、「**次へ**」をクリックします。
5. 「ログの収集モード」ウィンドウで、「**BMC ログの収集**」または「**FFDC ログの収集**」、あるいはその両方を選択し、「**次へ**」をクリックします。
6. 「ログの収集結果」ウィンドウで、結果を確認し、「**次へ**」をクリックします。
7. 「終了」ウィンドウで、 をクリックして詳細なログを確認し、「**閉じる**」をクリックして終了します。

Web サイトからの複数のリモート・サーバーの更新

UpdateXpress アプリケーションは、Web サイトからのリモート・サーバーの一括更新をサポートしています。

注：Web サイトから単一のリモート・サーバーを更新するには、12 ページの 「リモート・サーバーの Web サイトからの更新」を参照してください。

前提条件:

リモート・サーバーのマルチ更新機能は、ThinkServer サーバーおよび WenTian サーバーでのみサポートされます。サポートされるサーバーの詳細については、5 ページの 「サポートされるサーバー・モデル」を参照してください。

Web サイトから複数のリモート・サーバーを更新するには、以下を行います。
1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**マルチサーバーの管理**」を選択し、「**次へ**」をクリックします。
4. 「マルチサーバーの管理」ウィンドウで、「**サーバー・プールへの新しいサーバーの追加**」を選択し、以下の操作を 1 つ以上行い、最後に「**次へ**」をクリックします。
   - 新しいサーバーをサーバー・プールに追加するには、IP アドレス範囲を入力し、BMC の情報領域で「**検出**」をクリックして、サーバー・プール・リストから 1 つ以上のターゲット・サーバーを選択します。
   - サーバー・プール・リストからサーバーを削除するには、1 つ以上のターゲット・サーバーを選択し、「**選択済みサーバーを削除**」をクリックします。
   - ユーザー名とパスワードがサーバーに対して正しいかどうかを確認するには、1 つ以上のターゲット・サーバーを選択し、「**選択済みサーバーをスキャン**」をクリックします。
   - 管理用に共通の BMC 資格情報を使用するには、「**管理用に共通の BMC 資格情報を使用する**」を選択し、ユーザー名とパスワードを入力します。
   - 現在のサーバーのサーバー・プール・リストをエクスポートするには、「**エクスポート**」をクリックします。サーバー・プール・リストは、`configure.json` ファイルに保存されます。

- 他のサーバーにサーバー・プール・リストをインポートするには、「**インポート**」をクリックし、configure.json ターゲット・ファイルを選択します。

5. 「**次へ**」をクリックすると、証明書を更新する必要があるかどうかを確認するようユーザーに通知するメッセージが表示されます。「**同意する**」をクリックして、証明書を更新します。

   注：ユーザーが初めてログインした場合、またはパスワードが期限切れである場合は、「パスワードの変更」ウィンドウでパスワードを変更します。
6. 「タスク」ウィンドウで、「**ターゲット・サーバーでの更新の実行**」を選択し、「**次へ**」をクリックします。
7. 「更新設定」ウィンドウで、1 つまたは複数のオプションを選択します。「**BMC サーバーではなく別個のリモート・サーバーを使用する**」が選択されている場合、以下の情報を入力します。
   - (HTTPS/FTP 設定) **IP アドレスまたはホスト名**: サーバーの IP アドレスまたはホスト名です。
   - (HTTPS/FTP 設定) **ユーザー名**: サーバーのユーザー名です。
   - (HTTPS/FTP 設定) **パスワード**: サーバーのパスワードです。
   - (HTTPS/FTP 設定) **ポート**: サーバーのポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。
   - (HTTPS/FTP 設定) **ディレクトリー**: 更新パッケージをコピーするサーバーのロケーションです。

     注：HTTPS/FTP サーバーの絶対パスを入力します。FTP サーバーは、5 ページの「サポートされるサーバー・モデル」で上付き文字 2 (注 2) によってマークされた ThinkServer にのみ使用されます。
8. HTTPS サーバー・キーのフィンガープリントを構成するには、以下のいずれかを実行します。
   - HTTPS サーバー・キーのフィンガープリントを確認するには、「**はい**」をクリックします。
   - HTTPS サーバー・キーのフィンガープリントを確認しない場合、「**HTTPS サーバー・キーのフィンガープリントをスキップする**」を選択して「**次へ**」をクリックします。
9. 「更新ロケーション」ウィンドウで「**Lenovo サポート Web サイトの確認**」を選択して、「**次へ**」をクリックします。
10. 「ターゲット・ディレクトリー」ウィンドウでは、更新をダウンロードする場所を指定するか、デフォルトの場所のままにして、「**次へ**」をクリックします。
11. 「インターネット・アクセス」ページで、ユーザーのセキュリティー・アクセスに特別な要件がない場合は、「**テスト接続**」をクリックしてターゲット URL のネットワーク接続を確認し、「**次へ**」をクリックします。
    セキュリティーに関する他の懸念事項がある場合は、「**テスト接続**」をクリックする前に、次のように、セキュリティー要件に応じて「**プロキシ・サーバー**」および/または「**カスタム URL セキュリティー構成**」を構成します。
    - **プロキシ・サーバー**
      a. Web への接続に HTTP/HTTPS プロキシが必要な場合は「**プロキシ・サーバー**」を選択し、以下のフィールドに入力します。

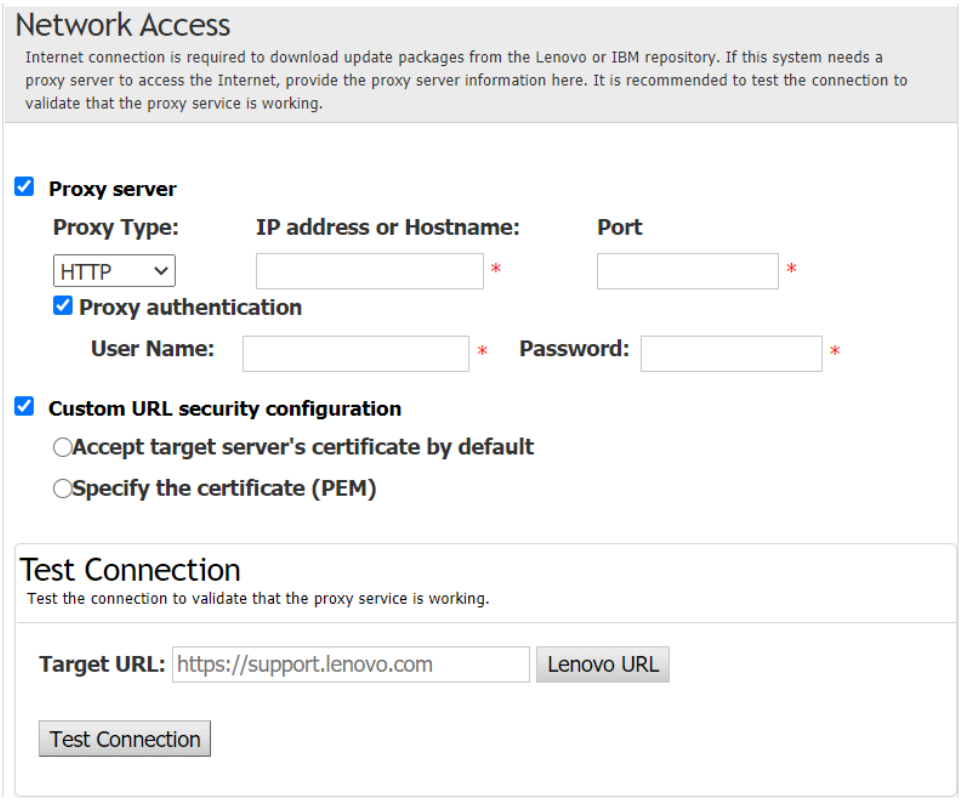
プロキシ・タイプ	プロキシ・サーバーのプロキシ・タイプ。
IP アドレスまたはホスト名	プロキシ・サーバーのホスト名、IP アドレス、またはドメイン名。
ポート	プロキシ・サーバーのポート番号。

      b. プロキシ・サーバーへの認証に資格情報を指定する必要がある場合は「**プロキシ認証**」を選択し、以下のフィールドに入力します。

ユーザー名	プロキシ・サーバーへの認証用のユーザー名。
パスワード	指定されたユーザー名のパスワード。

    - **カスタム URL セキュリティー構成**

      リバース・プロキシが必要な場合は「**カスタム URL セキュリティー構成**」を選択し、以下のいずれかのオプションを選択します。
      – **デフォルトでターゲット・サーバーの証明書を受け入れる**
      – **証明書 (PEM) を指定する**



12. 「更新タイプ」ウィンドウで、ターゲット更新タイプを選択して、「**次へ**」をクリックします。
13. 「推奨される更新」ウィンドウで「**開始**」をクリックして、ファームウェアのバージョンを、最新バージョンと比較します。進行状況が完了したら、ターゲット・パッケージを 1 つ以上選択し、「**次へ**」をクリックします。

    注：すべての更新パッケージを表示するには、「**アダプターが検出されない更新を表示する**」を選択してから「**開始**」をクリックします。
14. 「更新の取得」ウィンドウの取得表に、パッケージの取得の進行状況が表示されます。進行状況が完了したら、「**次へ**」をクリックします。
15. 「更新の実行」ウィンドウで、「**更新を開始しポップ・ウィンドウで続行を確認する**」をクリックします。実行テーブルには、パッケージのアップグレードの進行状況が表示されます。アップグレードの進行状況が完了したら、「**次へ**」をクリックします。
16. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

ローカル・ディレクトリーからの複数のリモート・サーバーの更新

UpdateXpress アプリケーションは、ローカル・フォルダーからのリモート・サーバーの一括更新をサポートしています。

注：ローカル・フォルダーから単一のリモート・サーバーを更新するには、14 ページの 「リモート・サーバーのローカル・ディレクトリーからの更新」を参照してください。

前提条件:

リモート・サーバーのマルチ更新機能は、ThinkServer サーバーおよび WenTian サーバーでのみサポートされます。サポートされるサーバーの詳細については、5 ページの 「サポートされるサーバー・モデル」を参照してください。

ローカル・ディレクトリーから複数のリモート・サーバーを更新するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**マルチサーバーの管理**」を選択し、「**次へ**」をクリックします。
4. 「マルチサーバーの管理」ウィンドウで、「**サーバー・プールへの新しいサーバーの追加**」を選択し、以下の操作を 1 つ以上行い、最後に「**次へ**」をクリックします。
   - 新しいサーバーをサーバー・プールに追加するには、IP アドレス範囲を入力し、BMC の情報領域で「**検出**」をクリックして、サーバー・プール・リストから 1 つ以上のターゲット・サーバーを選択します。
   - サーバー・プール・リストからサーバーを削除するには、1 つ以上のターゲット・サーバーを選択し、「**選択済みサーバーを削除**」をクリックします。
   - ユーザー名とパスワードがサーバーに対して正しいかどうかを確認するには、1 つ以上のターゲット・サーバーを選択し、「**選択済みサーバーをスキャン**」をクリックします。
   - 管理用に共通の BMC 資格情報を使用するには、「**管理用に共通の BMC 資格情報を使用する**」を選択し、ユーザー名とパスワードを入力します。
   - 現在のサーバーのサーバー・プール・リストをエクスポートするには、「**エクスポート**」をクリックします。サーバー・プール・リストは、`configure.json` ファイルに保存されます。
   - 他のサーバーにサーバー・プール・リストをインポートするには、「**インポート**」をクリックし、`configure.json` ターゲット・ファイルを選択します。
5. 「**次へ**」をクリックすると、証明書を更新する必要があるかどうかを確認するようユーザーに通知するメッセージが表示されます。「**同意する**」をクリックして、証明書を更新します。

   注：ユーザーが初めてログインした場合、またはパスワードが期限切れである場合は、「パスワードの変更」ウィンドウでパスワードを変更します。
6. 「タスク」ウィンドウで、「**ターゲット・サーバーでの更新の実行**」を選択し、「**次へ**」をクリックします。
7. 「更新設定」ウィンドウで、1 つまたは複数のオプションを選択します。「**BMC サーバーではなく別個のリモート・サーバーを使用する**」が選択されている場合、以下の情報を入力します。
   - (HTTPS/FTP 設定) **IP アドレスまたはホスト名**: サーバーの IP アドレスまたはホスト名です。
   - (HTTPS/FTP 設定) **ユーザー名**: サーバーのユーザー名です。
   - (HTTPS/FTP 設定) **パスワード**: サーバーのパスワードです。
   - (HTTPS/FTP 設定) **ポート**: サーバーのポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。
   - (HTTPS/FTP 設定) **ディレクトリー**: 更新パッケージをコピーするサーバーのロケーションです。

     注：HTTPS/FTP サーバーの絶対パスを入力します。FTP サーバーは、5 ページの 「サポートされるサーバー・モデル」で上付き文字 2 (注 2) によってマークされた ThinkServer にのみ使用されます。
8. 「更新ロケーション」ウィンドウで、「**ローカル・ディレクトリーを検索**」を選択します。ローカル・フォルダーを指定するには、以下のいずれかを行います。
   - 「**参照**」をクリックし、目的のフォルダーを選択して、「**次へ**」をクリックします。
   - 「**参照**」ボタンの横にあるフィールドにフォルダーのパスを入力して、「**次へ**」をクリックします。
9. 「更新タイプ」ウィンドウで、ターゲット更新タイプを選択して、「**次へ**」をクリックします。
10. 「推奨される更新」ウィンドウで、「**開始**」をクリックして、インストール済みファームウェアのバージョンを、最新バージョンと比較します。進行状況が完了したら、ターゲット・パッケージを 1 つ以上選択し、「**次へ**」をクリックします。

    注：すべての更新パッケージを表示するには、「**アダプターが検出されない更新を表示する**」を選択してから「**開始**」をクリックします。
11. 「更新の実行」ウィンドウで、「**更新を開始しポップ・ウィンドウで続行を確認する**」をクリックします。実行テーブルには、パッケージのアップグレードの進行状況が表示されます。アップグレードの進行状況が完了したら、「**次へ**」をクリックします。
12. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

複数のリモート・サーバーでの BIOS の構成

UpdateXpress アプリケーションは、複数のリモート・サーバーの BIOS 設定の一括構成をサポートしています。

前提条件:

リモート・サーバーのマルチ構成機能は、ThinkServer/WenTian サーバーでのみサポートされます。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。

BIOS を設定するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**マルチサーバーの管理**」を選択し、「**次へ**」をクリックします。
4. 「マルチサーバーの管理」ウィンドウで、「**サーバー・プールへの新しいサーバーの追加**」を選択し、以下の操作を 1 つ以上行って、「**次へ**」をクリックします。
   - 新しいサーバーをサーバー・プールに追加するには、IP アドレス範囲を入力し、BMC の情報領域で「**検出**」をクリックして、サーバー・プール・リストから 1 つ以上のターゲット・サーバーを選択します。
   - サーバー・プール・リストからサーバーを削除するには、1 つ以上のターゲット・サーバーを選択し、「**選択済みサーバーを削除**」をクリックします。
   - ユーザー名とパスワードがサーバーに対して正しいかどうかを確認するには、1 つ以上のターゲット・サーバーを選択し、「**選択済みサーバーをスキャン**」をクリックします。
   - 管理用に共通の BMC 資格情報を使用するには、「**管理用に共通の BMC 資格情報を使用する**」を選択し、ユーザー名とパスワードを入力します。
   - 現在のサーバーのサーバー・プール・リストをエクスポートするには、「**エクスポート**」をクリックします。サーバー・プール・リストは、`configure.json` ファイルに保存されます。
   - 他のサーバーにサーバー・プール・リストをインポートするには、「**インポート**」をクリックし、`configure.json` ターゲット・ファイルを選択します。
5. 「**次へ**」をクリックすると、証明書を更新する必要があるかどうかを確認するようユーザーに通知するメッセージが表示されます。「**同意する**」をクリックして、証明書を更新します。

   注：ユーザーが初めてログインした場合、またはパスワードが期限切れである場合は、「パスワードの変更」ウィンドウでパスワードを変更します。
6. 「タスク」ウィンドウで、「**BIOS 構成**」を選択し、「**次へ**」をクリックします。

   注：この BIOS 構成機能は、同じマシン・タイプのサーバーでのみサポートされます。
7. 「構成モード」ウィンドウで、「**共通 BIOS 構成**」または「**BIOS 構成ファイルのインポート**」を選択し、「**次へ**」をクリックします。
8. 次のいずれかを行います。
   - 前の手順で「**BIOS 構成ファイルのインポート**」が選択されている場合は、この手順をスキップします。
   - 前の手順で「**共通 BIOS 構成**」が選択されている場合は、現在の値を 1 つ以上選択し、「**次へ**」をクリックします。
9. 「BIOS 変更ビュー」ウィンドウで、変更された BIOS 設定を確認し、「**次へ**」をクリックします。
10. 「BIOS 構成のエクスポート」ウィンドウで、構成をファイルとしてエクスポートします。エクスポートしたファイルの場所を指定し、「**次へ**」をクリックします。
11. 「実行中の構成」ウィンドウで、「**手動で再起動**」または「**直ちに再起動**」を選択し、「**スタート**」をクリックします。タスクが完了したら、「**次へ**」をクリックします。
12. 「終了」ウィンドウで、「**ログの表示**」をクリックして構成ログを確認し、「**閉じる**」をクリックして終了します。

複数のリモート・サーバーのログの収集

UpdateXpress アプリケーションは、リモート・サーバーのログの一括収集をサポートしています。

前提条件:

リモート・サーバーのマルチ収集機能は、ThinkServer/WenTian サーバーでのみサポートされます。サポートされているオペレーティング・システムについて詳しくは、6 ページの 「サポートされているオペレーティング・システム」を参照してください。

ログを収集するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**マルチサーバーの管理**」を選択し、「**次へ**」をクリックします。
4. 「マルチサーバーの管理」ウィンドウで、「**サーバー・プールへの新しいサーバーの追加**」を選択し、以下の操作を 1 つ以上行って、「**次へ**」をクリックします。
   - 新しいサーバーをサーバー・プールに追加するには、IP アドレス範囲を入力し、BMC の情報領域で「**検出**」をクリックして、サーバー・プール・リストから 1 つ以上のターゲット・サーバーを選択します。
   - サーバー・プール・リストからサーバーを削除するには、1 つ以上のターゲット・サーバーを選択し、「**選択済みサーバーを削除**」をクリックします。
   - ユーザー名とパスワードがサーバーに対して正しいかどうかを確認するには、1 つ以上のターゲット・サーバーを選択し、「**選択済みサーバーをスキャン**」をクリックします。
   - 管理用に共通の BMC 資格情報を使用するには、「**管理用に共通の BMC 資格情報を使用する**」を選択し、ユーザー名とパスワードを入力します。
   - 現在のサーバーのサーバー・プール・リストをエクスポートするには、「**エクスポート**」をクリックします。サーバー・プール・リストは、`configure.json` ファイルに保存されます。
   - 他のサーバーにサーバー・プール・リストをインポートするには、「**インポート**」をクリックし、`configure.json` ターゲット・ファイルを選択します。
5. 「**次へ**」をクリックすると、証明書を更新する必要があるかどうかを確認するようユーザーに通知するメッセージが表示されます。「**同意する**」をクリックして、証明書を更新します。

   注：ユーザーが初めてログインした場合、またはパスワードが期限切れである場合は、「パスワードの変更」ウィンドウでパスワードを変更します。
6. 「タスク」ウィンドウで、「**ログの収集**」を選択し、「**次へ**」をクリックします。
7. 「ログの収集モード」ウィンドウで、「**BMC ログの収集**」または「**FFDC ログの収集**」、あるいはその両方を選択し、ログ出力ディレクトリーを指定して、「**次へ**」をクリックします。
8. 「ログの収集結果」ウィンドウで、結果を確認し、「**次へ**」をクリックします。
9. 「終了」ウィンドウで、  をクリックして構成ログを確認し、「**閉じる**」をクリックして終了します。

更新のリポジトリーの作成

UpdateXpress アプリケーションは Web サイトから取得した UXSP または個別更新のリポジトリーを作成できます。

このタスクを完了するには、以下の前提条件を満たす必要があります。

- UpdateXpress アプリケーションがリポジトリーを作成するローカル・マシン上で実行されている。
- マシンがサポートされているオペレーティング・システムを実行している。サポートされているオペレーティング・システムについて詳しくは、6 ページの 「サポートされているオペレーティング・システム」を参照してください。

更新リポジトリーを作成するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**更新のリポジトリーの作成**」を選択して「**次へ**」をクリックします。
4. 「更新タイプ」ウィンドウで、ターゲット更新タイプを選択して、「**次へ**」をクリックします。
   - 「**UpdateXpress System Packs (UXSP)**」を選択して UXSP を更新します。「**UpdateXpress System Packs (UXSP)**」を選択した場合は「更新の選択」ウィンドウがスキップされますが、すべての UXSP パッケージがダウンロードされます。
   - 個別パックを更新するには「**最新の使用可能な個別の更新**」を選択します。「**最新の使用可能な個別の更新**」を選択した場合、次の手順で「更新の選択」ウィンドウが表示され、ユーザーはターゲット・パッケージを選択する必要があります。
5. 「インターネット・アクセス」ページで、セキュリティー・アクセスに特別な要件がない場合は、「**テスト接続**」をクリックしてターゲット URL のネットワーク接続を確認し、「**次へ**」をクリックします。
   セキュリティーに関する他の懸念事項がある場合は、「**テスト接続**」をクリックする前に、次のように、セキュリティー要件に応じて「**プロキシ・サーバー**」および/または「**カスタム URL セキュリティー構成**」を構成します。
   - **プロキシ・サーバー**
     a. Web への接続に HTTP/HTTPS プロキシが必要な場合は「**プロキシ・サーバー**」を選択し、以下のフィールドに入力します。

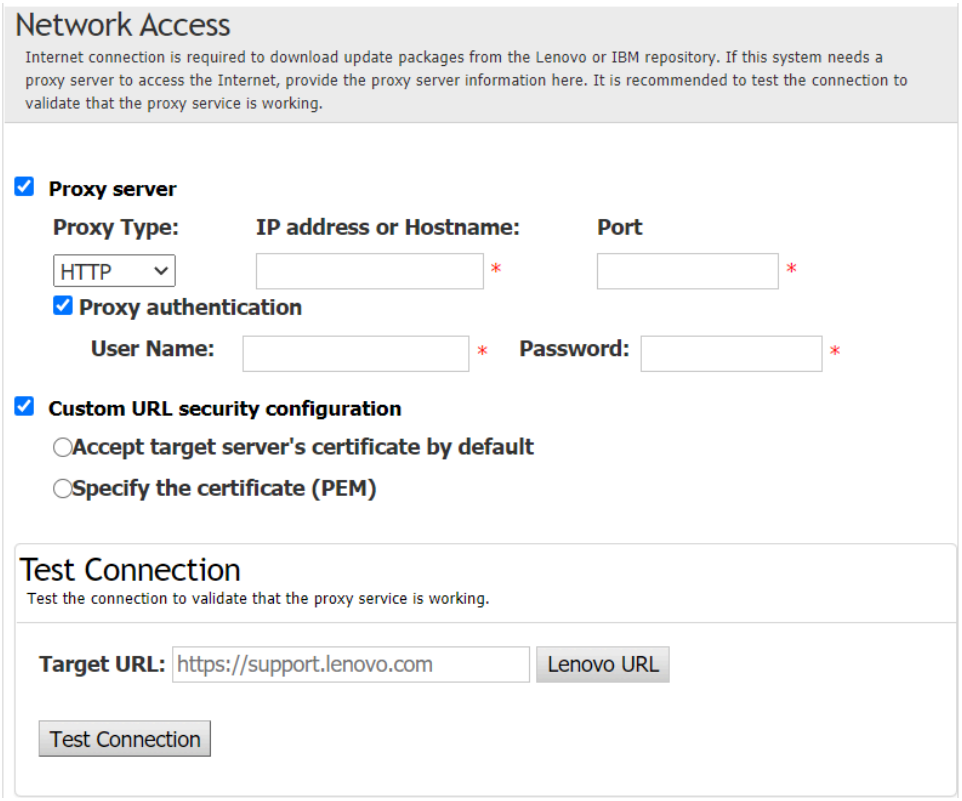
プロキシ・タイプ	プロキシ・サーバーのプロキシ・タイプ。
IP アドレスまたはホスト名	プロキシ・サーバーのホスト名、IP アドレス、またはドメイン名。
ポート	プロキシ・サーバーのポート番号。

     b. プロキシ・サーバーへの認証に資格情報を指定する必要がある場合は「**プロキシ認証**」を選択し、以下のフィールドに入力します。

ユーザー名	プロキシ・サーバーへの認証用のユーザー名。
パスワード	指定されたユーザー名のパスワード。

   - **カスタム URL セキュリティー構成**

     リバース・プロキシが必要な場合は「**カスタム URL セキュリティー構成**」を選択し、以下のいずれかのオプションを選択します。
     – **デフォルトでターゲット・サーバーの証明書を受け入れる**
     – **証明書 (PEM) を指定する**



6. 「マシン・タイプ」ウィンドウで、ターゲット・マシン・タイプを選択し、「**次へ**」をクリックします。
   - リストされているすべてのマシン・タイプを選択するには、ヘッダーのチェック・ボックスを選択します。
   - マシン・タイプを追加するには、「**追加**」をクリックして、マシン・タイプを指定します。
   - マシン・タイプを削除するには、リストからマシン・タイプを選択して、「**削除**」をクリックします。
   - マシン・タイプ・リストを最新バージョンに更新するには、「**リストを更新**」をクリックします。
   - マシン・タイプ・リストをリセットするには、「**リストをリセット**」をクリックします。
7. 「オペレーティング・システム」ウィンドウで、ターゲット・オペレーティング・システムを選択し、「**次へ**」をクリックします。
8. 「ターゲット・ディレクトリー」ウィンドウでは、更新をダウンロードする場所を指定するか、デフォルトの場所のままにして、「**次へ**」をクリックします。
9. (オプション)「**最新の使用可能な個別の更新**」を選択します。「更新の選択」ウィンドウが表示されます。ターゲット更新を選択して「**次へ**」をクリックします。
10. 「更新の取得」ウィンドウの取得表に、パッケージの取得の進行状況が表示されます。進行状況が完了したら、「**次へ**」をクリックします。
11. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

リモート・サーバーの RAID アレイの構成

UpdateXpress アプリケーションは、RAID 情報の収集、RAID アレイの作成、ディスク・ステータスの構成、コントローラーの構成のクリアなど、リモート・サーバー用の RAID 構成を行うことができます。

前提条件:

UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているサーバーで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。

RAID アレイを設定するには、次の手順に従います。

1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。関連情報を表示するウィンドウがポップアップ表示されたら、「OK」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書と SFTP/HTTPS サーバーの鍵フィンガープリントを検査しない場合は、「**BMC サーバーの証明書および SFTP/HTTPS サーバーの鍵フィンガープリントをデフォルトで受け入れます**」というメッセージの前にあるチェックボックスにチェックを入れ、「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**リモート RAID 構成**」または「**ターゲット・サーバーでの更新の実行**」、あるいは両方の項目を選択して、「**次へ**」をクリックします。
5. 「RAID 構成」ウィンドウで、UpdateXpress は最初にリモート・サーバーの RAID 情報を収集します。収集が完了すると、RAID 情報がウィンドウに表示されます。
   - コントローラーの構成をクリアするには、「**コントローラーのクリア**」をクリックします。
   - ドライブ・ステータスを JBOD に変更するには、「**JBOD にする**」をクリックします。
   - ドライブのステータスを「未構成の正常ドライブ」に変更するには、「**正常にする**」をクリックします。
6. 「RAID 構成」ウィンドウで、コントローラー用のアレイを作成するには、「**アレイの作成**」をクリックします。
   a. ウィザード・ウィンドウで、RAID レベルの選択、アレイのスパン、メンバー、ホット・スペアの追加、ボリュームの作成、ディスク・パラメーターの設定を行います。
   b. 要約情報が表示されたら、「**作成**」をクリックしてストレージ・アレイの作成を開始します。
   c. プロセスが完了したら、「**収集**」または「**最新表示**」をクリックして RAID 情報を再度収集します。
   d. 他に必要な操作がない場合は、「**次へ**」をクリックします。
7. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

リモート・サーバーに対するステージングされた更新の実行

UpdateXpress アプリケーションは、リモート・サーバーに対するステージングされた更新の実行をサポートします。

このタスクを完了するには、以下の前提条件を満たす必要があります。

- UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているサーバーで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの 「サポートされているオペレーティング・システム」を参照してください。

リモート・サーバーに対するステージングされた更新を実行するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。

- (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

注：ユーザーが BMC サーバーの証明書を確認しない場合は、「**デフォルトで BMC サーバーの証明書を承認します**」を選択して「**次へ**」をクリックします。

4. 「タスク」ウィンドウで、「**ターゲット・サーバーでの更新の実行**」を選択し、「**次へ**」をクリックします。
5. 「更新設定」ウィンドウで、1 つまたは複数のオプションを選択し、「**次へ**」をクリックします。

注：
- 「**BMC サーバーではなく別個のリモート・サーバーを使用する**」が選択されている場合、以下の情報を入力します。
  - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
  - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
  - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
  - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。
  - (設定) **ディレクトリー**: SFTP サーバーの絶対パスです。そのディレクトリーに、更新ファイルがアップロードされます。ディレクトリーがアクセス可能であることを確認してください。例: /payload
- SFTP/HTTPS サーバーの鍵フィンガープリントを確認しない場合は、「**SFTP サーバーの鍵フィンガープリントをスキップする**」を選択します。

6. 「更新ロケーション」ウィンドウで「**Lenovo サポート Web サイトの確認**」を選択して、「**次へ**」をクリックします。
7. 「ターゲット・ディレクトリー」ウィンドウでは、更新をダウンロードする場所を指定するか、デフォルトの場所のままにして、「**次へ**」をクリックします。
8. 「インターネット・アクセス」ページで、ユーザーのセキュリティー・アクセスに特別な要件がない場合は、「**テスト接続**」をクリックしてターゲット URL のネットワーク接続を確認し、「**次へ**」をクリックします。
   セキュリティーに関する他の懸念事項がある場合は、「**テスト接続**」をクリックする前に、次のように、セキュリティー要件に応じて「**プロキシ・サーバー**」および/または「**カスタム URL セキュリティー構成**」を構成します。
   - **プロキシ・サーバー**
     a. Web への接続に HTTP/HTTPS プロキシが必要な場合は「**プロキシ・サーバー**」を選択し、以下のフィールドに入力します。

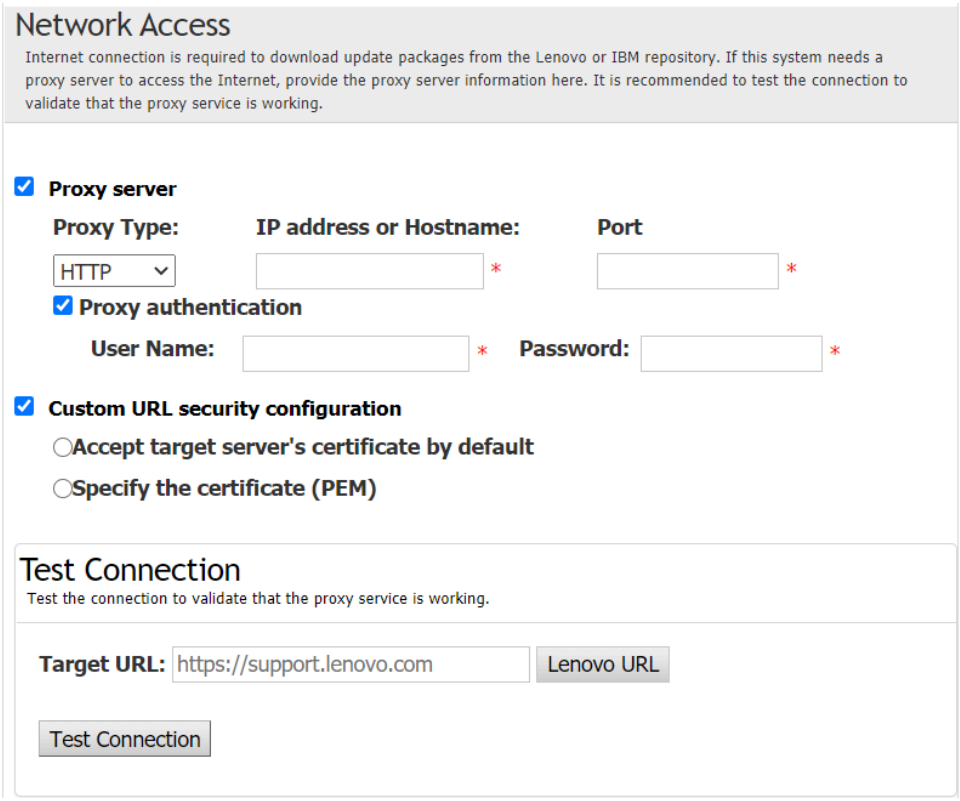
プロキシ・タイプ	プロキシ・サーバーのプロキシ・タイプ。
IP アドレスまたはホスト名	プロキシ・サーバーのホスト名、IP アドレス、またはドメイン名。
ポート	プロキシ・サーバーのポート番号。

     b. プロキシ・サーバーへの認証に資格情報を指定する必要がある場合は「**プロキシ認証**」を選択し、以下のフィールドに入力します。

ユーザー名	プロキシ・サーバーへの認証用のユーザー名。
パスワード	指定されたユーザー名のパスワード。

   - **カスタム URL セキュリティー構成**

     リバース・プロキシが必要な場合は「**カスタム URL セキュリティー構成**」を選択し、以下のいずれかのオプションを選択します。
     - **デフォルトでターゲット・サーバーの証明書を受け入れる**
     - **証明書 (PEM) を指定する**



9. 「更新タイプ」ウィンドウで、ターゲット更新タイプを選択して、「**次へ**」をクリックします。
10. 「推奨される更新」ウィンドウで、以下の操作を 1 つ以上行います。
    - すべての更新パッケージを表示するには、「**未検出のデバイスの更新を表示する**」を選択します。
    - コンポーネントを更新するには、ターゲット・コンポーネントを選択し、「**次へ**」をクリックします。
11. 「更新の取得」ウィンドウの取得表に、パッケージの取得の進行状況が表示されます。進行状況が完了したら、「**次へ**」をクリックします。
12. 「実行中の更新」ウィンドウで、「**更新の開始**」 → 「**はい**」 → 「**次へ**」をクリックします。

    注：バンドル・パッケージを含むファームウェアを更新するには、「**バンドル・パッケージを含むファームウェアを更新する。このチェックボックスと下位オプションは XCC2 のみをサポートします。**」を選択し、適用時間を設定します。
    - **リセット時**: 次回システムが再起動する際にパッケージを更新します。
    - **即時**: パッケージをすぐに更新します。システムがすぐに再起動される可能性があります。
    - **更新要求時**: ステージングされた更新の管理または OneCLI コマンドの実行によってパッケージを更新します。
13. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

リモート・サーバーに対するステージングされた更新の管理

UpdateXpress アプリケーションは、リモート・サーバーに対するすべてのステージングされた更新の開始、キャンセル、および表示をサポートします。

このタスクを完了するには、以下の前提条件を満たす必要があります。

- UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているサーバーで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。

リモート・サーバーに対するステージングされた更新を管理するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書を確認しない場合は、「**デフォルトで BMC サーバーの証明書を承認します**」を選択して「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ステージングされた更新の管理**」を選択して「**次へ**」をクリックします。
5. 「タスク管理」ウィンドウで、以下のいずれかを実行して「**次へ**」をクリックします。
   - タスク情報を取得するには、タスク ID を入力して  をクリックします。保留中のタスクのタスク ID が自動的に入力されます。
   - 更新を開始するには、ターゲット・タスクの「**スタート**」をクリックします。
   - 更新をキャンセルするには、ターゲット・タスクの「**キャンセル**」をクリックします。
6. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

SED 認証キーの管理

ThinkEdge サーバーは、認証キーを使用して自己暗号化ドライブ (SED) へのアクセスを提供します。UpdateXpress アプリケーションは、生成、バックアップ、リカバリーなど、SED 認証キー (AK) の管理をサポートします。

前提条件:
- UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているサーバーで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの 「サポートされているオペレーティング・システム」を参照してください。
- この機能は、ThinkEdge サーバーがロック解除されている場合にのみサポートされます。サポートされるサーバーについて詳しくは、5 ページの 「サポートされるサーバー・モデル」の ThinkEdge シリーズを参照してください。

SED 認証キーを管理するには、以下を行います。
1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書を確認しない場合は、「**デフォルトで BMC サーバーの証明書を承認します**」を選択して「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ThinkEdge サーバーでのセキュリティー機能の構成**」を選択し、「**次へ**」をクリックします。
5. 「ThinkEdge サーバーのセキュリティー機能」ウィンドウで、「**SED 認証キーの管理**」を選択し、「**次へ**」をクリックします。
6. 「SED 認証キー (AK) 管理」ウィンドウで、以下のいずれかを実行します。

- SED AK を生成するには、「**SED 暗号化の有効化**」を選択するか (SED AK が無効になっている場合)、「**SED AK の変更**」を選択します (SED AK が有効になっている場合)。「**方式**」ドロップダウン・リストでターゲット方式を選択し、「**再生成**」をクリックします。

  注：データの損失に備えて、AK をバックアップすることをお勧めします。ユーザーは、AK をバックアップした後にのみその他のオプションを選択できます。
- SED AK をバックアップするには、「**SED AK のバックアップ**」を選択し、バックアップ・ファイルの場所とパスワードを入力して、「**開始**」をクリックします。UpdateXpress は、SED AK 情報を含むバックアップ・ファイルを保存します。
- SED AK をリカバリーするには、「**SED AK のリカバリー**」を選択し、以下のいずれかを実行します。
  - バックアップ・ファイルを使用してリカバリーするには、「**方式**」ドロップダウン・リストで「**バックアップ・ファイルから SED AK をリカバリーする**」を選択します。次に、「**参照**」をクリックしてバックアップ・ファイルを選択し、パスワードを入力して、「**復元を開始**」をクリックします。
  - パスフレーズを使用してリカバリーするには、「**方式**」ドロップダウン・リストで「**パスフレーズを使用して SED AK をリカバリーする**」を選択し、パスフレーズを入力して、「**復元を開始**」をクリックします。

7. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

ThinkShield ポータルでのサーバーの登録

ThinkEdge サーバーの所有権は Lenovo ThinkShield Key Vault Portal で登録できます。その後、UpdateXpress はポータルを使用してロックダウンされたサーバーをアクティブにすることができます。

前提条件:
- UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているサーバーで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。
- この機能は ThinkEdge サーバーでのみサポートされます。サポートされるサーバーについて詳しくは、5 ページの「サポートされるサーバー・モデル」の ThinkEdge シリーズを参照してください。

ThinkShield ポータルでサーバーを登録するには、以下を行います。
1. UpdateXpress アプリケーションを起動します。9 ページの「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書を確認しない場合は、「**デフォルトで BMC サーバーの証明書を承認します**」を選択して「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ThinkEdge サーバーでのセキュリティー機能の構成**」を選択し、「**次へ**」をクリックします。
5. 「ThinkEdge サーバーのセキュリティー機能」ウィンドウで、「**ThinkShield ポータルでのサーバーの登録**」を選択し、「**次へ**」をクリックします。
6. 「インターネット・アクセス」ウィンドウで、以下のいずれかを実行します。
   - ユーザーのセキュリティー・アクセスに特別な要件がない場合は、「**テスト接続**」をクリックしてターゲット URL のネットワーク接続を確認し、「**次へ**」をクリックします。

- セキュリティーに関する他の懸念事項がある場合は、以下の 1 つ以上を構成し、「**テスト接続**」をクリックします。
  - **プロキシ・サーバー**: HTTP/HTTPS プロキシを介してネットワークにアクセスします。
    a. 「**プロキシ・サーバー**」を選択し、以下のフィールドに入力します。

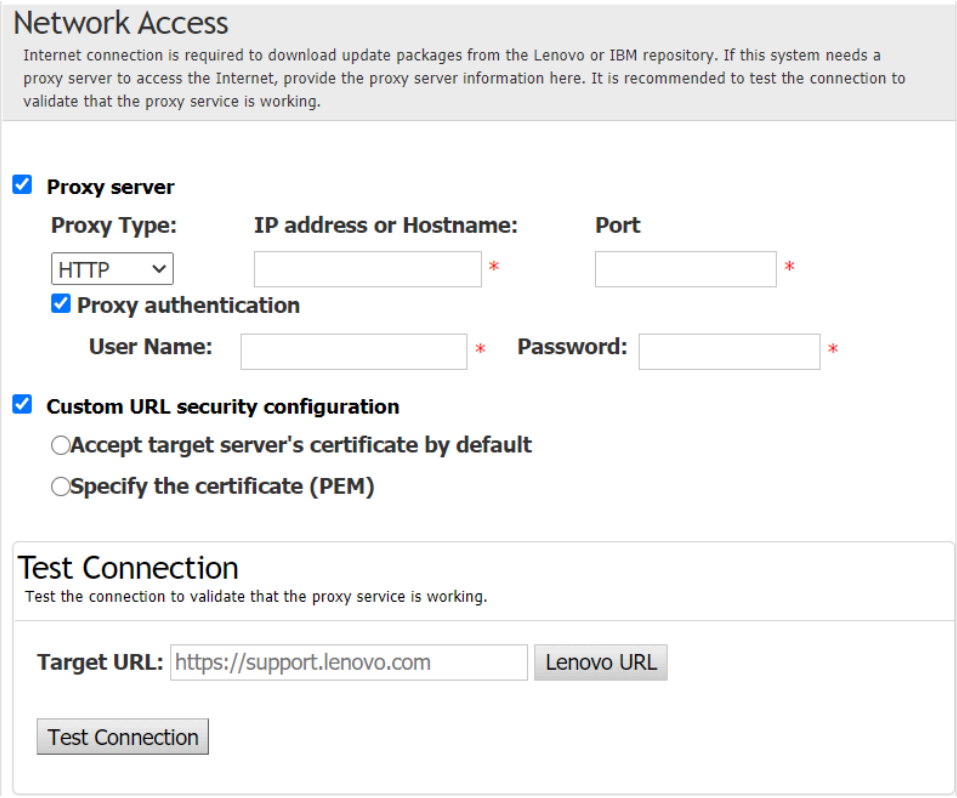
プロキシ・タイプ	プロキシ・サーバーのプロキシ・タイプ。
IP アドレスまたはホスト名	プロキシ・サーバーのホスト名、IP アドレス、またはドメイン名。
ポート	プロキシ・サーバーのポート番号。

    b. プロキシ・サーバーへの認証に資格情報を指定する必要がある場合は「**プロキシ認証**」を選択し、以下のフィールドに入力します。

ユーザー名	プロキシ・サーバーへの認証用のユーザー名。
パスワード	指定されたユーザー名のパスワード。

  - **カスタム URL セキュリティー構成**: リバース・プロキシを介してネットワークにアクセスします。

    以下のいずれかを選択します。
    - デフォルトでターゲット・サーバーの証明書を受け入れる
    - 証明書 (PEM) を指定する



7. 「サーバーの登録」ウィンドウで、ThinkShield Key Vault Portal の組織 ID、ユーザー名、およびパスワードを入力して、「**登録**」をクリックします。
8. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

ロックダウン制御モードのアップグレード

ThinkEdge サーバーには、不正のイベントを検出するセキュリティー・センサーが装備されています。これは、不正検出でもサーバーをロックダウンします。UpdateXpress では、XClarity Controller によるサーバーのアクティブ化から ThinkShield ポータルによるサーバーの管理への、サーバー・ロックダウン制御モードのアップグレードをサポートしています。

前提条件:
- UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているサーバーで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。
- この機能は ThinkEdge サーバーでのみサポートされます。サポートされるサーバーについて詳しくは、5 ページの「サポートされるサーバー・モデル」の ThinkEdge シリーズを参照してください。

ロックダウン制御モードをアップグレードするには、以下を行います。
1. UpdateXpress アプリケーションを起動します。9 ページの「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書を確認しない場合は、「**デフォルトで BMC サーバーの証明書を承認します**」を選択して「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ThinkEdge サーバーでのセキュリティー機能の構成**」を選択し、「**次へ**」をクリックします。
5. 「ThinkEdge サーバーのセキュリティー機能」ウィンドウで、「**システム・ロックダウン制御**」を選択し、「**次へ**」をクリックします。次に、以下のいずれかのオプションで、ThinkShield Key Vault Portal にサーバーの所有権を登録するかどうかを選択し、もう一度「**次へ**」をクリックします。
   - 「**はい、今すぐサーバーを登録します**」を選択し、手順 6 に進みます。
   - 「**いいえ、ThinkShield Key Vault Portal でサーバーを登録しないで続行します**」を選択し、手順 8 に進みます。
6. 「インターネット・アクセス」ウィンドウで、以下のいずれかを実行します。
   - ユーザーのセキュリティー・アクセスに特別な要件がない場合は、「**テスト接続**」をクリックしてターゲット URL のネットワーク接続を確認し、「**次へ**」をクリックします。
   - セキュリティーに関する他の懸念事項がある場合は、以下の 1 つ以上を構成し、「**テスト接続**」をクリックします。
     – **プロキシ・サーバー**: HTTP/HTTPS プロキシを介してネットワークにアクセスします。
       a. 「**プロキシ・サーバー**」を選択し、以下のフィールドに入力します。

プロキシ・タイプ	プロキシ・サーバーのプロキシ・タイプ。
IP アドレスまたはホスト名	プロキシ・サーバーのホスト名、IP アドレス、またはドメイン名。
ポート	プロキシ・サーバーのポート番号。

       b. プロキシ・サーバーへの認証に資格情報を指定する必要がある場合は「**プロキシ認証**」を選択し、以下のフィールドに入力します。

ユーザー名	プロキシ・サーバーへの認証用のユーザー名。
パスワード	指定されたユーザー名のパスワード。

– **カスタム URL セキュリティー構成**: リバース・プロキシを介してネットワークにアクセスします。

以下のいずれかを選択します。
– デフォルトでターゲット・サーバーの証明書を受け入れる
– 証明書 (PEM) を指定する

7. 「ThinkShield Portal アカウントの検証」ウィンドウで、ThinkShield Key Vault Portal の組織 ID、ユーザー名、およびパスワードを入力して、「**検証**」をクリックします。検証が完了したら、「**次へ**」をクリックします。

注：情報入力が有効である必要があります。有効でないと、「**次へ**」ボタンは有効に*なりません*。

8. 「システム・ロックダウン制御」ウィンドウで、「**YES**」と手動で入力し、「**OK**」をクリックします。アップグレード・プロセスが完了したら、「**次へ**」をクリックします。
9. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

ロックダウン・モードでのサーバーのアクティブ化

ThinkEdge サーバーには、不正のイベントを検出するセキュリティー・センサーが装備されています。これは、不正検出でもサーバーをロックダウンします。UpdateXpress は、ThinkShield Key Vault Portal または XClarity Controller を使用してロックダウンされたサーバーのアクティブ化をサポートします。

前提条件:
- UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているサーバーで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。
- この機能は ThinkEdge サーバーでのみサポートされます。サポートされるサーバーについて詳しくは、5 ページの「サポートされるサーバー・モデル」の ThinkEdge シリーズを参照してください。

サーバーをロックダウン・モードでアクティブにするには、以下を行います。
1. UpdateXpress アプリケーションを起動します。9 ページの「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書を確認しない場合は、「**デフォルトで BMC サーバーの証明書を承認します**」を選択して「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ThinkEdge サーバーでのセキュリティー機能の構成**」を選択し、「**次へ**」をクリックします。
5. 「ThinkEdge サーバーのセキュリティー機能」ウィンドウで、「**ThinkShield ポータルでのサーバーのアクティブ化**」を選択し、「**次へ**」をクリックします。

   注：デフォルトのシステム・ロックダウン制御は XClarity Controller で管理されます。ロックダウン制御が ThinkShield ポータルで管理されている場合、ユーザーは ThinkShield Key Vault Portal によって認証された後でのみ、ロックダウン・モードでサーバーをアクティブにすることができます。
6. 「インターネット・アクセス」ウィンドウで、ユーザーのセキュリティー・アクセスに特別な要件がない場合は、「**テスト接続**」をクリックしてターゲット URL のネットワーク接続を確認し、「**次へ**」をクリックします。
   セキュリティーに関する他の懸念事項がある場合は、「**テスト接続**」をクリックする前に、次の

ように、セキュリティー要件に応じて「**プロキシ・サーバー**」および/または「**カスタム URL セキュリティー構成**」を構成します。

- **プロキシ・サーバー**
  a. Web への接続に HTTP/HTTPS プロキシが必要な場合は「**プロキシ・サーバー**」を選択し、以下のフィールドに入力します。

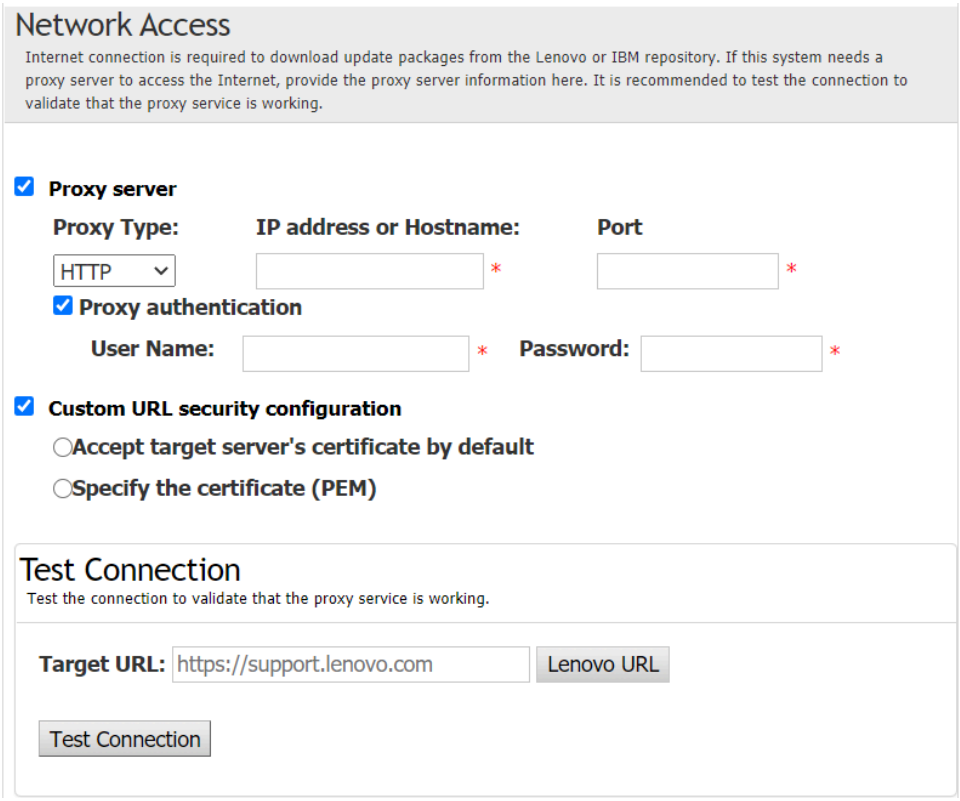
プロキシ・タイプ	プロキシ・サーバーのプロキシ・タイプ。
IP アドレスまたはホスト名	プロキシ・サーバーのホスト名、IP アドレス、またはドメイン名。
ポート	プロキシ・サーバーのポート番号。

  b. プロキシ・サーバーへの認証に資格情報を指定する必要がある場合は「**プロキシ認証**」を選択し、以下のフィールドに入力します。

ユーザー名	プロキシ・サーバーへの認証用のユーザー名。
パスワード	指定されたユーザー名のパスワード。

- **カスタム URL セキュリティー構成**

  リバース・プロキシが必要な場合は「**カスタム URL セキュリティー構成**」を選択し、以下のいずれかのオプションを選択します。
  – **デフォルトでターゲット・サーバーの証明書を受け入れる**
  – **証明書 (PEM) を指定する**



7. 「サーバーのアクティブ化」ウィンドウで、ThinkShield Key Vault Portal 組織 ID、ユーザー名、およびパスワードを入力して、「**アクティブ化**」をクリックします。アクティベーション・プロセスが完了したら、「**次へ**」をクリックします。

   注：サーバーが XClarity Controller によって管理されている場合、ユーザーは ThinkShield Key Vault Portal の情報を入力する必要は*ありません*。

8. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

セキュリティー・センサーの構成

ThinkEdge サーバーには、改ざんイベントを検出するセキュリティー・センサーが装備されています。UpdateXpress は、動作検出センサーおよびシャーシ侵入検出センサーのしきい値の有効化、無効化、および変更をサポートしています。

前提条件:
- UpdateXpress アプリケーションが、サポートされているオペレーティング・システムがインストールされているサーバーで実行されている。サポートされているオペレーティング・システムについて詳しくは、6 ページの「サポートされているオペレーティング・システム」を参照してください。
- この機能は ThinkEdge サーバーでのみサポートされます。サポートされるサーバーについて詳しくは、5 ページの「サポートされるサーバー・モデル」の ThinkEdge シリーズを参照してください。

セキュリティー・センサーを構成するには、以下を実行します。
1. UpdateXpress アプリケーションを起動します。9 ページの「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**リモート・サーバーの管理**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
   - (設定) **IP アドレスまたはホスト名**: ターゲット・システムの BMC IP アドレスまたはホスト名です。
   - (設定) **ユーザー名**: ターゲット・システムの BMC ユーザー名です。
   - (設定) **パスワード**: ターゲット・システムの BMC パスワードです。
   - (設定) **ポート**: BMC CIM または RSET ポート番号です。ユーザーが入力しない場合は、デフォルトのポートが使用されます。

   注：ユーザーが BMC サーバーの証明書を確認しない場合は、「**デフォルトで BMC サーバーの証明書を承認します**」を選択して「**次へ**」をクリックします。
4. 「タスク」ウィンドウで、「**ThinkEdge サーバーでのセキュリティー機能の構成**」を選択し、「**次へ**」をクリックします。
5. 「ThinkEdge サーバーのセキュリティー機能」ウィンドウで、「**セキュリティー・センサーの構成**」を選択し、「**次へ**」をクリックします。
6. 「セキュリティー・センサーの構成」ウィンドウで、以下のいずれかを実行して、「**次へ**」をクリックします。
   - 「**動作検出**」または「**シャーシ侵入検出**」を有効または無効にするには、ドロップダウン・リストからオプションを選択するか、スイッチ・ボタンをクリックしてステータスを切り替えます。

     注：データ損失に備えて、項目を選択する前に AK をバックアップすることをお勧めします。
   - 動作検出のステップ・カウントをリセットするには、「**ステップ・カウンターのリセット**」をクリックします。UpdateXpress はステップ・カウントを 0 にリセットします。
   - 動作検出をロックダウンするためのしきい値のステップを変更するには、「**ロックダウンのしきい値**」のターゲット・ステップ・レベルを選択します。

     注：セキュリティー・センサーによって改ざんイベントが検出されると、ThinkEdge サーバーはロックダウンされます。
7. 「終了」ウィンドウで、「**ログの表示**」をクリックしてアップグレード・ログを確認し、生成されたコマンドをコピーして保存した後、「**閉じる**」をクリックして終了します。

イーサネットの直接接続でのサーバーの管理

UpdateXpress アプリケーションは、イーサネットの直接接続でのサーバーの管理をサポートしています。ネットワーク・ケーブルが接続されている場合、UpdateXpress はデフォルトの BMC IP および資格情報を使用してサーバー BMC へのアクセスを試します。

イーサネットの直接接続でサーバーを管理するには、以下を行います。

1. UpdateXpress アプリケーションを起動します。9 ページの 「UpdateXpress アプリケーションの起動」を参照してください。
2. 「ウェルカム」ウィンドウで「**次へ**」をクリックします。
3. 「ターゲット・サーバー」ウィンドウで、「**イーサネットの直接接続**」を選択し、以下の情報を入力して「**次へ**」をクリックします。
4. 「イーサネットの直接接続設定」ウィンドウで、以下を行います。
   a. 「「使用可能なネットワーク・アダプター」」テーブルからターゲット・アダプターを選択します。
   b. デフォルトの IP アドレスが **192.168.70.125** であることを確認します。
   c. ユーザー名およびパスワードを入力します。
   d. **テスト接続 → 次へ**または「**次へ**」をクリックします。
5. 「タスク」ウィンドウで、以下のいずれかを選択します。
   - **ターゲット・サーバーでの更新の実行**。詳しくは、14 ページの 「リモート・サーバーのローカル・ディレクトリーからの更新」で手順 4 とそれ以降の手順を参照してください。
   - **ステージングされた更新の管理**。詳しくは、27 ページの 「リモート・サーバーに対するステージングされた更新の管理」で手順 4 とそれ以降の手順を参照してください。
   - **リモート RAID 構成**。詳しくは、24 ページの 「リモート・サーバーの RAID アレイの構成」で手順 4 とそれ以降の手順を参照してください。
   - **ThinkEdge サーバーでセキュリティー機能を構成します**。詳しくは、次のセクションで手順 4 とそれ以降の手順を参照してください。
     – 28 ページの 「SED 認証キーの管理」
     – 29 ページの 「ThinkShield ポータルでのサーバーの登録」
     – 31 ページの 「ロックダウン制御モードのアップグレード」
     – 32 ページの 「ロックダウン・モードでのサーバーのアクティブ化」
     – 34 ページの 「セキュリティー・センサーの構成」

「終了」ウィンドウでの OneCLI コマンドの表示

UpdateXpress は、GUI ウィザードで OneCLI コマンドを起動することで更新を実行します。UpdateXpress 2.7.0 以降のバージョンでは、これらのコマンドは「終了」ウィンドウの新しいメッセージ・ボックスに表示されます。コマンドを保存して使用すると、CLI モードで同じ機能を呼び出すことができます。

OneCLI コマンドの例:

```
<LXCE OneCLI> update flash --uselocalimg --imm USERID:***@xx.xxx.xxx.xxx --dir
D:\build\Onegui\105980\lnvgy_utl_lxce_ux01k-2.7.0_windows_i386\workingdir --output
D:\build\Onegui\105980\lnvgy_utl_lxce_ux01k-2.7.0_windows_i386\Lenovo_Support\ --platform --log 5
```

第 4 章　トラブルシューティング

この章では、UpdateXpress アプリケーションに問題が発生した場合の対処方法について説明します。

制限および問題

- **Linux で UpdateXpress を実行するプロセスにおいてカスタム・プロキシー/URL セキュリティー構成の証明書を指定するとき、ユーザーが「参照」を 2 回クリックした場合、UpdateXpress インターフェースに参照ウィンドウが表示されない場合があります。**

  「インターネット・アクセス」ページの「**プロキシ・タイプ**」ドロップダウン・リストで「HTTPS」を選択し、「**カスタム・プロキシー・セキュリティー構成**」と「**カスタム URL セキュリティー構成**」を選択し、「**参照...**」をクリックして両方の選択項目の証明書を指定します。ユーザーが「参照」を 2 回クリックすると、参照ウィンドウが表示されない場合があります。

  回避策: 以下の操作を 1 つ以上行います。
  - バックグラウンドの参照ウィンドウに手動で切り替えます。
  - ウィンドウ・サイズを調整し、バックグラウンドの参照ウィンドウを表示します。
  - 代わりに Windows で UpdateXpress を使用します。
- **インボックス・ドライバーからアウト・オブ・ボックス・ドライバーにアップグレードする際、UpdateXpress が一部のデバイスでアウト・オブ・ボックス・ドライバーをデフォルトとして設定できません。**

  UpdateXpress は、更新タスクを実行するために OneCLI を呼び出します。OneCLI は、インボックス・ドライバーとアウト・オブ・ボックス・ドライバーの一致していないバージョンを比較して、更新に使用する正しいバージョンを選択できませんでした。この場合、UpdateXpress はアウト・オブ・ボックス・ドライバーを更新対象として選択できません。ユーザーが、対象となるアウト・オブ・ボックス・ドライバーを手動で選択し、インボックス・ドライバーをオーバーライドする必要があります。
- **すべての UpdateXpress パスは、標準英語の英数字を使用する必要があります。**

  すべての UpdateXpress パスは、標準英語の英数字を使用する必要があり、スペース、特殊文字、または英語以外の言語の文字を含めることはできません。

回避策

現在、UpdateXpress アプリケーションに既知の問題または回避策はありません。

共存および互換性

UpdateXpress アプリケーションは OneCLI に基づいていますが、システムの他のプログラムとの対話は行いません。UpdateXpress アプリケーションと OneCLI を同時に実行しないでください。

付録 A　UpdateXpress のアクセシビリティー機能

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーが情報、技術、製品を快適に使用できるようにサポートします。

以下のリストには、UpdateXpress アプリケーションの主要なアクセシビリティー機能を記載しています。
- キーボードのみによる操作
- 画面読み上げ機能によって通常使用されるインターフェース

キーボード・ナビゲーション

キーボードを使用してグラフィカル・ユーザー・インターフェース (GUI) 間を移動できます。

以下のキーボード・ショートカットが Windows および Linux 両方のオペレーティング・システムに適用できます。

ショートカット	機能
タブ	次のコントロールに移動します。
Shift+タブ	前のコントロールに移動します。
左矢印	1 文字戻ります。
右矢印	1 文字進みます。
Backspace	カーソルの左にある文字を削除します。
Delete	カーソルの下にある文字を削除します。
上矢印	ラジオ・ボタンのフォーカスと選択を上方向に移動します。
下矢印	ラジオ・ボタンのフォーカスと選択を下方向に移動します。
スペース	オプションを選択またはクリアします。

スクリーン・リーダー技術

スクリーン・リーダー技術は主にソフトウェア・プログラム・インターフェース、ヘルプ情報システム、および各種オンライン・ドキュメントに適しています。スクリーン・リーダーについて詳しくは、以下を参照してください。
- JAWS スクリーン・リーダーの使用:

  http://www.freedomscientific.com/Products/Blindness/JAWS
- NVDA スクリーン・リーダーの使用:

  http://www.nvaccess.org/

Lenovo とアクセシビリティー

アクセシビリティーに対する Lenovo の取り組みについて詳しくは、http://www.lenovo.com/lenovo/us/en/accessibility.html を参照してください。

付録 B　注記

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、Lenovo の営業担当員にお尋ねください。

本書で Lenovo 製品、プログラム、またはサービスに言及していても、その Lenovo 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、Lenovo の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、他の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

Lenovo は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について 実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

Lenovo は、本書を特定物として「現存するままの状態で」提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。Lenovo は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書で説明される製品は、誤動作により人的な傷害または死亡を招く可能性のある移植またはその他の生命維持アプリケーションで使用されることを意図していません。本書に記載される情報が、Lenovo 製品仕様または保証に影響を与える、またはこれらを変更することはありません。本書の内容は、Lenovo またはサード・パーティーの知的所有権のもとで明示または黙示のライセンスまたは損害補償として機能するものではありません。本書に記載されている情報はすべて特定の環境で得られたものであり、例として提示されるものです。他の操作環境で得られた結果は、異なる可能性があります。

Lenovo は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本書において Lenovo 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この Lenovo 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

商標

Lenovo、Flex System、System x、NeXtScale System は Lenovo の商標です。Intel および Intel Xeon は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。Internet Explorer、Microsoft、および Windows は、Microsoft Corporation の米国およびその他の国における商標です。Linux は、Linus Torvalds の米国およびその他の国における商標です。その他すべての商標は、それぞれの所有者の知的財産です。

重要事項

プロセッサーの速度とは、マイクロプロセッサーの内蔵クロックの速度を意味しますが、他の要因もアプリケーション・パフォーマンスに影響します。

主記憶装置、実記憶域と仮想記憶域、またはチャネル転送量を表す場合、KB は 1,024 バイト、MB は 1,048,576 バイト、GB は 1,073,741,824 バイトを意味します。

ハードディスク・ドライブの容量、または通信ボリュームを表すとき、MB は 1,000,000 バイトを意味し、GB は 1,000,000,000 バイトを意味します。ユーザーがアクセス可能な総容量は、オペレーティング環境によって異なる可能性があります。

Lenovo は、他社製品に関して一切の保証責任を負いません。他社製品のサポートがある場合は、Lenovo ではなく第三者によって提供されます。

いくつかのソフトウェアは、その小売り版 (利用可能である場合) とは異なる場合があり、ユーザー・マニュアルまたはすべてのプログラム機能が含まれていない場合があります。

索引

ふ

へ

よ