テスト レポート
Tolly.

#223114

2023 年 4 月

BlackBerry Ltd.
からの依頼

BlackBerry CylanceENDPOINT (EDR 無効)

リソース効率・有効性に関する Microsoft、Sophos、Trellix との比較分析

EXECUTIVE SUMMARY

現代の企業にとってエンドポイント セキュリティは不可欠ですが、一部のソリューションにおけるシステム リソースの使用状況について考えた場合、そこには隠れたリスクが存在します。物理・仮想を問わず、すべてのコンピューティング システムが強力になる一方、新規および更新されたアプリケーションは、ますます多くのリソースを必要とするようになっています。この現状を踏まえ、BlackBerry は、システム リソースの消費を最小限に抑えながら、オフライン環境でも優れたエンドポイント保護を提供することに重点を置いています。

BlackBerry は、Windows 10 環境における同社の EDR 無効エンドポイント ソリューション「CylanceENDPOINT」の有効性とリソース需要の調査、ならびに複数の競合ソリューションとの比較分析を Tolly に依頼しました。

BlackBerry は、アクセス ポイントから接続/切断するハイブリッド ワーカーや、インターネットに直接接続されていない隔離された制御・運用技術環境において特に重要となる、パフォーマンスへの影響を極めて低く抑えたオフライン保護において優れた実績を上げています。詳細は図 1 を参照してください。

要点

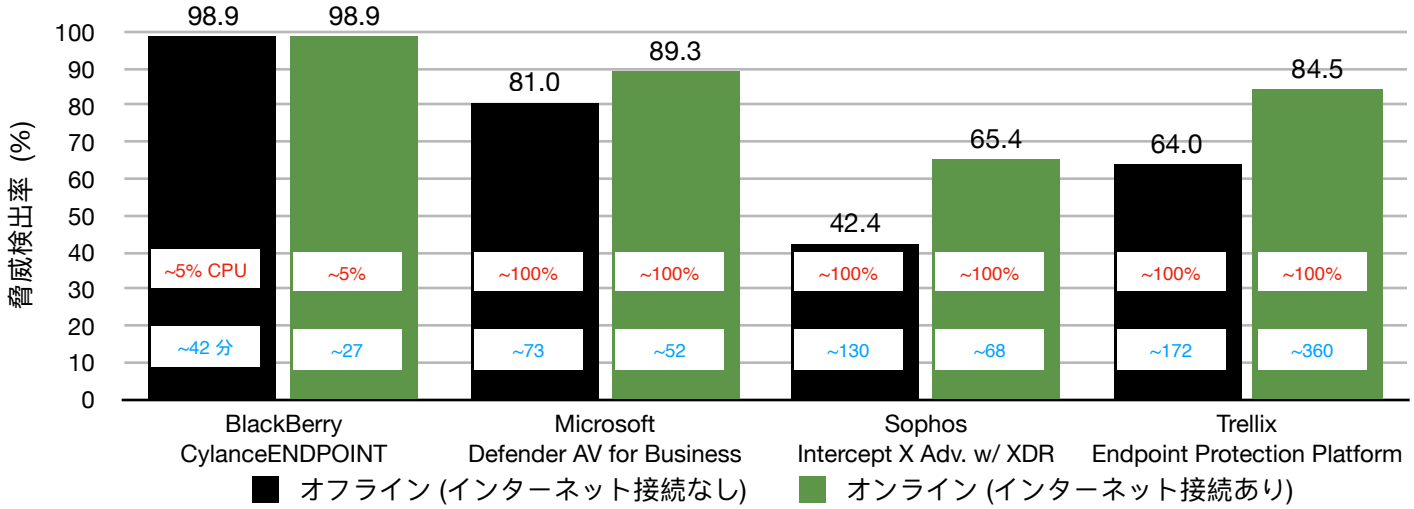
BlackBerry CylanceENDPOINT (EDR 無効):

1. スキャン中の CPU リソース消費を大幅に削減することで、より多くのコンピューター リソースをエンドユーザーやビジネス タスクに割り当てることが可能。
2. オフラインとオンラインの両方で優れた脅威対策機能を提供し、インターネットの接続状況にかかわらず、悪意のあるファイルから確実に保護。
3. マルウェアの侵入によって生じるリソースの継続使用を最小限に抑え、コストのかかるデバイスの再イメージングを排除することで、エンドポイントのライフサイクル延長に貢献。

Windows 10 エンドポイント保護の有効性とリソース使用率

VirusTotal の最新サンプル 1,000 個からなる 2 つのサンプル コレクションをスキャン

（検出率はスキャン後にフォルダーに残ったファイル数から算出）



注意: スキャンは、1,000 個のマルウェア サンプルが含まれるパスワードで保護された「zip」ファイルをシステムが解凍することでトリガーされます。オフライン テストとオンライン テストでは異なるサンプル群を使用しました。各ソリューションで使用したサンプル セットは同一です。実行時間は青字で分単位、また、実行中にエンドポイント保護プロセスによって報告された標準的な CPU 使用率は赤字でパーセント単位で表示されています。これらは VirusTotal の最新サンプルです。サンプルの抽出に使用したクエリについては、「テストの設定および方法」セクションを参照してください。

出典: Tolly、2023 年 3 月

図 1

テスト結果

背景

エンドポイント保護ソリューションは、その性質上、常に存在するため、少量のシステム リソースを常に消費します。エンドポイント セキュリティ ソリューションが CPU などのリソースを過剰に消費した場合、エンドユーザーやビジネス アプリケーションへのレスポンス タイムに影響が生じます。

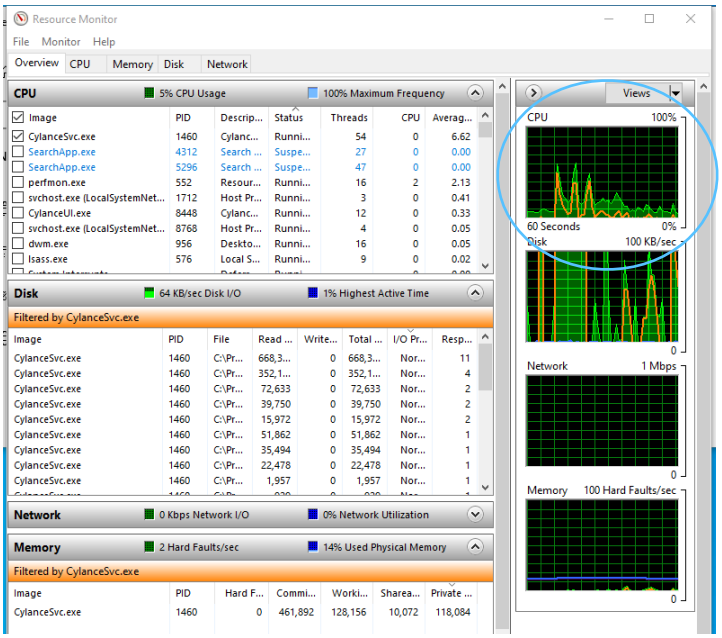
このテストは、目的が非常に限定されているため、極めて端的な結果を得ることができます。Tolly は、一般的な複数のエンドポイント セキュリティ ソリューションにおけるリソース消費量（および有効性）の違いを明らかにするため、Google が運営する VirusTotal ウェブサイトからダウンロードした最新のマルウェア サンプル 1,000 個を含むフォルダーをスキャンした際の脅威検出機能の有効性とリソース消費量を比較評価しました。すべてのテスト結果は、前ページの図 1 に要約されています。新しいサンプルをテストすることはより困難なため、すべてのテストにおいて BlackBerry のテストを最初に実施しました。

有効性 – オフライン テスト

オフライン テストでは、すべてのエンドポイントのインターネット接続を無効にしました。これは、エンドポイントがマルウェアを検証する際に、ローカル情報以外を参照できないようにするためです。

BlackBerry CylanceENDPOINT（EDR 無効）は、マルウェア サンプルの 98.9% を検出しました。これに対し、Microsoft Defender for Business の検出率は 81%、Sophos Intercept X Advanced with XDR は 42.4%、Trellix Endpoint Protection は 64% でした。

BlackBerry CylanceENDPOINT (EDR 無効)
スキャン中の Windows 10 リソース使用率
(Microsoft リソース モニターの報告に基づく)



スキャン途中のリソース スナップショット。BlackBerry の CPU 使用率は平均で約 6%。リソース使用率はテスト全体を通して一定。

出典: Tolly、2023 年 3 月 図 2

BlackBerry Ltd.

CylanceENDPOINT (EDR 無効)

リソース効率および有効性

テスト実施日: *2023 年 3 月*

有効性 – オンライン テスト

オンラインテストは、すべてのエンドポイントのインターネット接続を再度有効にして実施しました。つまり、テスト対象のソリューションは、マルウェアを検証する際に、それぞれの集中型データベースに照会することができます。このテストでは、異なるサンプル セットを使用しました。

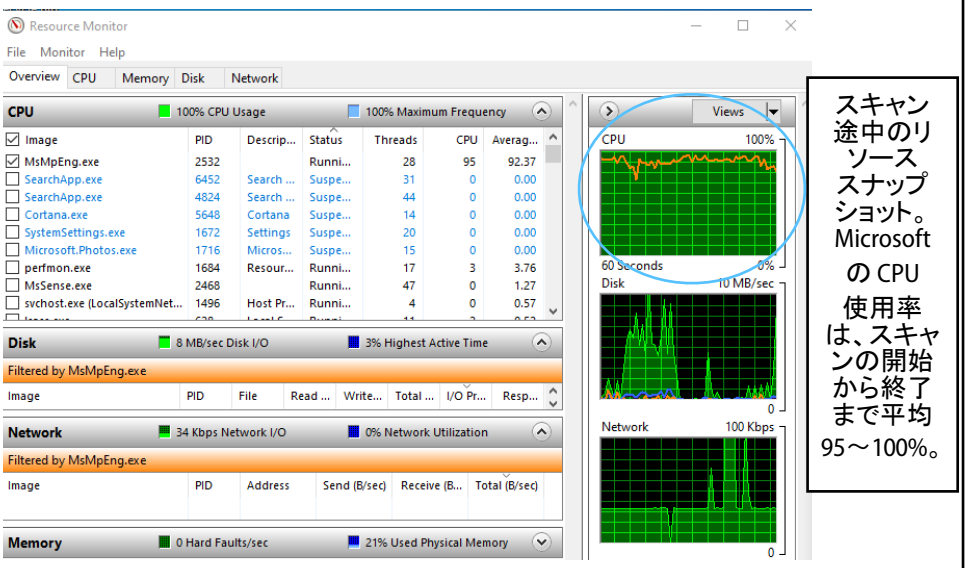
BlackBerry CylanceENDPOINT（EDR 無効）は、オフラインテストと同様、マルウェア サンプルの 98.9% を検出しました。Microsoft Defender for Business は、検出率が 89.3% に向上しました。Sophos Intercept X Advanced with XDR は、サンプルの 65.4% を検出し、約 50% の改善となりました。Trellix Endpoint Protection の検出率は 84.5% でした。

リソース使用率

前述のとおり、このテストでは、エンドポイント ソリューションが貴重な Windows リソースをどのように管理しているかに特に焦点を当てました。

エンドポイント ソリューションは通常バックグラウンドで動作すること、また、マルウェアの到達は予測不可能であることから、リソースの使用状況を正確に把握することは非常に困難です。

Microsoft Defender for Business
スキャン中の Windows 10 リソース使用率
(Microsoft リソース モニターの報告に基づく)



出典: Tolly、2023 年 3 月　　図 3

そのため、このテストでは、テストを推進するための 1,000 個のサンプルが含まれているフォルダーを使用しました。

結果は若干意外なものとなり、BlackBerry と他のベンダーでは、リソース使用率に歴然とした差が認められました。BlackBerry は、テスト全体を通して CPU リソースの使用率を約 6% に抑えており、このような自主的な制約がある中でも、競合ソリューションよりも速くテストを終了しました。詳細は図 2 を参照してください。

他のベンダーの CPU 使用率は、テスト開始直後に 100% に達し、その後もテスト完了まで同じ、またはそれに近い使用率が維持されました。テストの完了には、あるシナリオでは少なくとも 1 つのベンダーが 2 時間以上を要しました。このシナリオは一般的なシナリオではありませんが、テストした他のソリューションが、CPU リソースの使用を抑制することなく、実行しているタスクの継続中、取得できるリソースをすべて使用していることを示しています。最終的には、エンドユーザーがビジネス タスクを実行する際に、パフォーマンスが低下してしまう可能性があります。

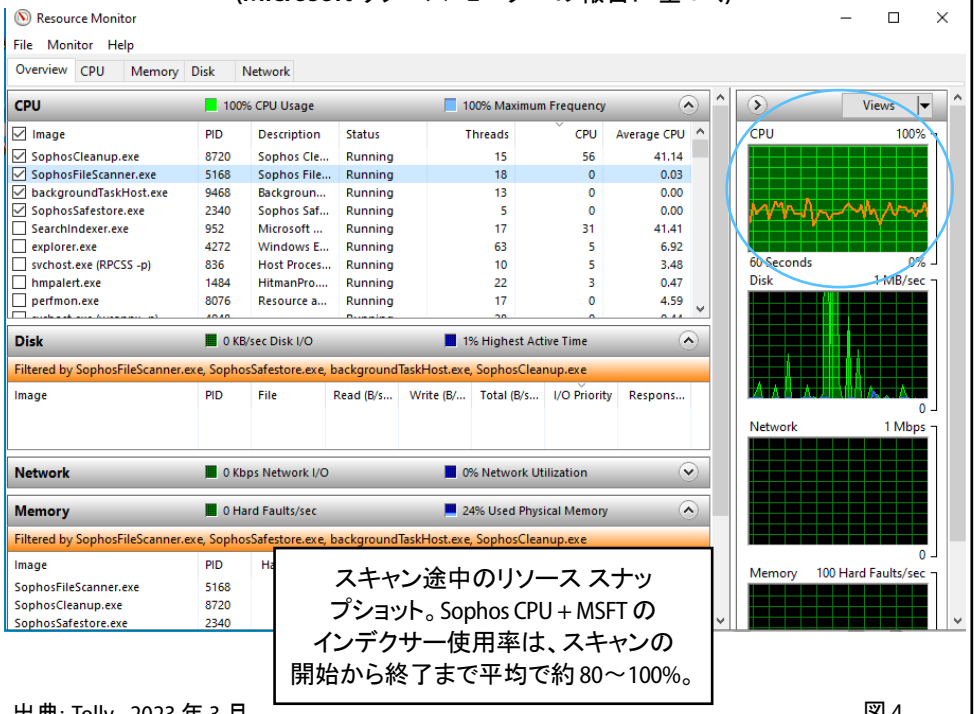
Microsoft

Microsoft の場合、ZIP からマルウェアを「抽出」する際に、核となるセキュリティ プロセス「MsMpEng.exe」が直ちに CPU リソースを取得します。このプロセスは、すべてのマルウェア サンプルの検証が終わるまで、CPU の約 95～100% を消費します。詳細は図 3 を参照してください。スキャン所要時間は、オフライン テストでは約 73 分、オンライン テストでは 52 分でした。

Sophos

Sophos ソリューションも Microsoft と同様、ZIP ファイルからファイルを抽出する時点から約 90～100%の CPU を消費します。Sophos の主な違いは、スキャン中に SophosCleanup.exe、SophosFileScanner.exe、SophosSafestore.exe

Sophos Intercept X Advanced with XDR
スキャン中の Windows 10 リソース使用率
(Microsoft リソース モニターの報告に基づく)



出典: Tolly、2023 年 3 月　　図 4

などの異なるプロセスが呼び出されることです。また、Microsoft SearchIndexer.exe モジュールは、Sophos のスキャン プロセス中はほぼ常に実行されています。テストした他のソリューションでは、このプロセスはこのような形で存在しなかったことから、Tolly のエンジニアチームは、このプロセスが Sophos のエンドポイント ソリューションによって呼び出され、使用されたと推定しています。詳細は図 4 を参照してください。スキャン所要時間は、オフライン テストでは約 130 分、オンライン テストでは 68 分でした。

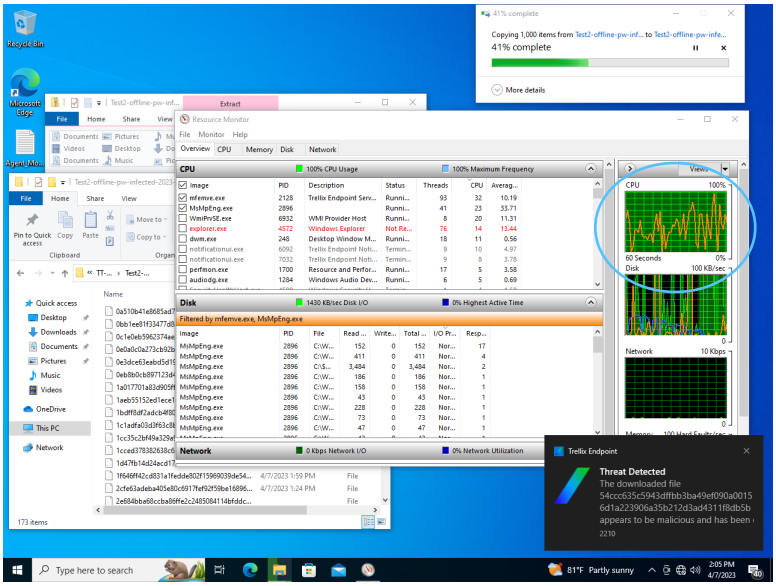
Trellix

Trellix ソリューションもまた、ZIP ファイルからファイルを抽出する時点から約 90～100% の CPU を消費します。Trellix の主な違いは、スキャン中に異なるプロセスが呼び出されることです。Mfemve.exe は、Trellix Endpoint Service のコア プロセス[1] で、Windows 10 に組み込まれた Microsoft Defender のコア プロセスである MsMpEng.exe と連動して動作すると思われます（MsMpEng.exe は、今回のテストに含まれる Microsoft Windows Defender for Business のサブセットでもあります）。

Trellix は、他の Microsoft のシステム プロセスを通して機能すると考えられ、抽出とスキャン プロセス全体で CPU の約 100% を消費しています。実際、Trellix で検出されなかったと思われる一部の脅威は、Microsoft Defender で検出され、そのメッセージに表示されました。どの脅威がどのコンポーネントで検出されたかを特定することは不可能なため、Trellix の結果は Microsoft Defender と合わせたものとなります。

他のソリューションは、抽出を完了してからスキャンを続行するのに対し、Trellix は抽出中にすべてのファイルをスキャンしているようです。CPU を最も消費するプロセスは、テスト全体を通して大きく変化しますが、常に 100% 近くを使用しています。詳細は図 5 を参照してください。スキャン所要時間は、オフライン テストでは約 172 分、オンライン テストでは 360 分でした。どちらのテストでも、Microsoft Defender のプロセスは、テスト終了後も 100% で実行され続けました。

Trellix Endpoint Protection
スキャン中の Windows 10 リソース使用率
(Microsoft リソース モニターの報告に基づく)



スキャン途中のリソース スナップショット。Trellix の CPU 使用率は平均で約 100%。

出典: Tolly、2023 年 3 月 図 5

テストの設定および方法

環境

すべてのテストは、Oracle VirtualBox 6.1 下の仮想化環境で動作する Windows 10 2022H2 64 ビット システムで実施しました。すべての Windows システムは、2023 年 3 月下旬時点で利用可能なすべての更新プログラムで更新しました。更新後は自動アップデート機能を無効にし、テスト中のシステム変更を回避しました。

[1] プロセス名は、同社の前身である「McAfee」の社名にちなんでいます。一部のコンポーネントは、もう 1 つの旧社名である Musaruba に著作権があり、MVISION ソリューションの CASB 要素は、「SkyHigh Networks」というブランド名で提供されています。ブランディングに一貫性がなく、わかりにくい状況となっています。

VirtualBox のホスト システム プロセッサーは、3.7GHz Intel Core i7（96GB DDR4 RAM 搭載）でした。

各仮想デスクトップは、1 台の CPU と 16GB RAM[2] で構成されています。インターネット接続は、仮想化された Gigabit Ethernet ネットワーク アダプターにより確立しました。仮想デスクトップを常時 1 台だけ起動させ、ソリューションを連続的にテストしました。

ソリューションのインストール

テストしたソリューションは、いずれもクラウド管理環境を提供していました。ソリューションごとに、Windows のインストーラーをダウンロードし、エンドポイントをオンボードしました。

Sophos については、エンドポイント保護オプションのみを選択し、暗号化など、その他の機能はインストールしませんでした。

エンドポイントに関しては、特別な構成は行っていません。また、脅威対策データベースはクラウド サービスによって継続的に更新されるため、クライアントのバージョン番号は関係ありません。

ネットワークテスト環境

テストは、Windows システムで、ネットワーク接続状態を変えて 2 回（異なるサンプル セットを使用）実施しました。

オフライン

このテストでは、インターネット接続を提供する Ethernet ネットワーク アダプターを無効にしました。そのため、各エンドポイント保護ソリューションが、マルウェアサンプルの判定を下す際に参照できたのは、ローカル リソースだけでした。

テストは連続的に行われましたが、システムはすべて同時にオフラインにし、テスト開始まで電源をオフにしておきました。

オンライン

このテストでは、Ethernet ネットワーク アダプターを有効にしました。そのため、エンドポイント保護ソリューションは、脅威の判定を下す際に、脅威に関する集中型データベースに照会することができるようになりました。

マルウェア サンプル

すべてのマルウェア サンプルは、テスト開始前の 24 時間以内に VirusTotal コレクションからダウンロードしました。

サンプル セットは、マルウェアとして VirusTotal に提出された 1,000 ファイル（1 ファイル 5MB 未満）で構成されています。各テストにおいて、パスワード保護された約 275MB の圧縮（ZIP）ファイルを生成しました。このファイルはパスワードで保護されているため、エンジニアが手動でスキャン開始をトリガーすることはできません。

サンプルの提供には、「fs:1d+ size:5MB- type:peexepositives:15+ not engines:pup not engines:adware not tag:corrupt not tag:assembly not tag:overlay not tag:nsis not tag:upx not tag:64bits not tag:bobsoft not tag:armadillo not magic:"PE32 executable for MS Windows (unknown subsystem) unknown processor 32-bit」というクエリを使用しました。

テストの手順

マルウェア サンプルをテスト対象のエンドポイント ソリューションにコピーし、シナリオに応じて、ネットワーク接続を有効/無効に設定しました。その後、エンジニアが、テスト対象の Windows システムで「Microsoft リソース モニター」ウィンドウを開きました。

開始時刻は、パスワードが入力され、「extract all」コマンドの処理が開始された時刻を記録しました。終了時刻は、エンドポイント プロセスがテスト対象のマルウェア フォルダーからのファイル削除を停止した時刻を記録しました。

対象フォルダーには 1,000 個のマルウェアのサンプルが含まれており（サンプル数は VirusTotal が決定）、対象フォルダーに残っているファイルがゼロになれば、パーフェクト スコアとなります。脅威検出率の算出には、対象フォルダーに残っているファイル数を使用しました。

Trellix を除き、本番環境における有効性テストは 2023 年 3 月 26 日および 27 日に実施しました。ロジスティクスの問題により、これらの日に Trellix を準備することはできず、Trellix のテストは 2023 年 4 月 7 日および 8 日に実施しました。大部分のテストは、2023 年 3 月下旬に実施したため、結果の引用はこれらの日付のままとなっています。

テスト対象のエンドポイント保護ソリューション

ベンダー	ソリューション
BlackBerry Ltd.	CylanceENDPOINT (EDR 無効)
Microsoft	Defender for Business
Sophos	Intercept X Advanced with XDR
Trellix	Endpoint Protection (MVision)

出典: Tolly、2023 年 3 月 表 1

[2] エンドポイントのインストール中、Sophos のインストーラでは 1 つ以上のコア（CPU）の使用を推奨する警告が表示されました。前述のとおり、テストに使用した CPU は 1 台です。

Tolly について

Tolly Group の企業は、世界的な IT サービスを 30 年間以上にわたり提供し続けています。Tolly は IT 製品、コンポーネント、サービスに関する第三者評価の提供で業界をリードするグローバル企業です。

Tolly に関するご質問は、電子メール (info@tolly.com) または電話 (+1 561.391.5610) でお問い合わせください。

Tolly ウェブサイト:
http://www.tolly.com

利用規約

本書は、特定の用途に対する製品や技術、サービスの追加調査について、その実施が有用であるかどうかを判断するための参考資料として無償で提供されています。製品購入の決定は、ニーズに対する適合性を判断した上でお客様ご自身で行ってください。本書はあくまでも参考資料であり、有資格の IT 技術者や業界専門家の助言の代替となるものではありません。評価の目的は製品の特定機能や性能を説明することであり、テストは実験室の制御された環境で行われています。テストによっては理想的な条件下における性能を検査したものもあるため、実際の性能はそれぞれの状況により異なる場合があります。ご利用のネットワークにおける性能は、実環境のシナリオに従って各自検証してください。

本書の作成にあたり、データの正確性には最善の注意を払いましたが、情報の誤りや過失が含まれている可能性があります。また、本書に掲載されているテスト/監査ではさまざまなテスト　ツールが使用されており、テスト結果を左右するこれらツールの精度は当社の管理外にあります。同様に、スポンサー企業から提供されたデータの正確性についても当社の責任の範疇を超えます。これには、製造中または製造準備段階のソフトウェア/ハードウェアも含まれており、実際に市販される製品はこれらソフトウェア/ハードウェアと同等の品質、あるいは改良された状態で提供されます。本書は「現状有姿」で提供されるものであり、Tolly Enterprises, LLC (以下「Tolly」) は明示的もしくは黙示的の一切の保証を行いません。また、本書に記載されるいかなる情報の正確性、完全性、有用性、適合性についても、直接的もしくは間接的な一切の法的責任を負いません。本書に目を通すことで、本書に含まれる情報の使用は利用者の自己責任であり、これらの情報またはマテリアルによって直接または間接的に生じた損失、損害、費用、その他の結果に対するリスクについて理解しており、その全責任を負うことに同意したことになります。Tolly は本書に含まれる情報を利用または信頼したことで生じた、あるいはこれらの利用や信頼に起因するいかなる損失や危害、怪我、損害についても一切責任を負わず、利用者は Tolly およびその関連会社を免責するものとします。

また Tolly は、本書に記載されている製品や会社について投資する価値があると推奨しているわけではありません。本書に含まれる情報や製品、会社に関連した投資またはプロジェクトに着手する前に、法律、会計、その他の分野の専門家から必ず助言を受けるようにしてください。翻訳版と英語版の内容が異なる場合は、英語版が優先されます。正確性を保証するため、Tolly.com から直接ダウンロードした文書のみを使用してください。文書の全部または一部は、Tolly の具体的な書面による許可なしに複製することはできません。本書に記載されている商標は、それぞれの所有者に帰属します。利用者は、当社以外の活動や製品、サービスに関連して、これらの商標を自らの商標のすべてまたは一部として利用しないこと、ならびに紛らわしい、誤解を招く恐れのある、虚偽の方法、あるいは当社/当社の情報、プロジェクト、開発が糾弾される恐れのある方法でこれらの商標を用いないことに同意するものとします。

cm-1-wt-2023-04-22—Verl