Windows Server 2008 の

サポート終了(EoS)対策の背景と手段

LAC 株式会社ラック

目次

はじめに

マイクロソフト社のサーバ向けオペレーティングシステム「Windows Server 2008」は、2008 年 2 月に日本での販売を開始した製品です。Windows テクノロジで、仮想化技術を初めて実装し、パブリッククラウドの利用に及び腰であった企業が、プライベートクラウドの導入・構築の需要増により急速に普及した製品です。

Windows Server 2008 が登場して 12 年が経過した 2020 年 1 月 14 日に、ついにマイクロソフト社によるサポートが終了となります。

マイクロソフト社および多くの SI 企業は、多くの企業で今なお稼働し続けていている Windows Server 2008 のサポート終了について、その周知と対策を促してきましたが、今なお 20 万台以上のサーバが運用を続けているとみられます。
そこで、Windows Server 2008 のサポート終了の背景と、具体的な対応方法について改めてまとめました。

「サポート」と「サポート終了(EOS:End Of Support)」とは何か

マイクロソフト社は、製品の販売開始から製品のメンテナンスの期間を定義しています。
サポート期間は製品のカテゴリーにより異なっており、ビジネス利用者向け、開発者向け、およびデスクトップ向け、オペレーティングシステム製品の場合、一般的なメンテナンス期間は、メインストリームサポートが最低 5 年間、さらに延長サポート期間が最低 5 年、合わせて最低 10 年の継続となっています。一方で、コンシューマー向け製品などは、延長サポートは提供されず最低 5 年間のサポート期間となります。

注意すべきは、サポート継続の期間のカウントアップは、マイクロソフト社が販売を開始した時点から計算され、ユーザーがライセンスを購入した時期とは無関係であることです。例えば販売後 5 年経過した Windows 製品の場合、5 年のサポート期間はありますが、それ以降はマイクロソフト社の判断によりサポートが打ち切られる可能性があります。
本件で取り上げる Windows Server 2008 のメンテナンス期間は、販売開始から 12 年となっており、最低 10 年とされる期間を超え継続されているのは、多くの企業が導入した製品であり、市場の状況に配慮したものと考えられます。

この最低 10 年のサポート期間は、他社のソフトウェア製品のサポート期間と比較しても、決して短いものではありません。マイクロソフト社が各種製品のライフサイクルについて発表した際に市場の混乱はありましたが、メンテナンス期間をあらかじめ提示する流れは業界の標準的な手法となりました。

マイクロソフト社のいう「サポート」とは、次のような製品改良活動を差しています。

- 機能のアドオン
- 性能の改善
- 設定の変更
- 不具合の解消

この「不具合の解消」に含まれるのが、製品のセキュリティ上の欠陥である「脆弱性対応」です。
ソフトウェア製品は、非常に複雑な実装がされているため、多くの不具合が含まれた状態で提供され、不具合を解消しながら品質を高めていきます。しかしこの不具合の中には、サイバー攻撃に悪用されることで、深刻な被害につながる性質のものも存在し、特別な対応を必要とします。これがセキュリティアップデートと呼ばれます。
そして上記 4 点について改良されたものは、一定の期間を経て大規模な単一パッケージ「サービスパック Service Pack」として提供されます。このサービスパックは、メインストリームサポートの期間中に複数回提供されます。

ところがこのサービスパックという存在は、製品のメンテナンスにおいて大きな負担となっています。これはセキュリティアップデートを配信する場合、修正プログラムはサービスパックそれぞれに合わせて開発とテストを行う必要があるためです。マイクロソフト社は、製品のアップデートによる互換性上の悪影響（デグレードやサイドエフェクトと呼ばれる）を回避するため、サービスパックごとに異なるセキュリティアップデートを開発し、代表的なプログラム言語における互換性テストを行った上で、配信をしています。

これらの労力を軽減するために、ライフサイクルにはサービスパックポリシーというものが存在し、最新のサービスパックが提供されてから約 24 か月は、古いサービスパックに対してもセキュリティアップデートを提供されますが、サービスパックポリシーの期間を過ぎると、セキュリティアップデートなどは提供が停止されます。
この 24 か月という期間は、サービスパックを適用に向けた猶予期間と位置付けられ、ユーザーが互換性の検証するために考慮されたものです。サイバー攻撃への備えのためにセキュリティアップデートを適用すると、今まで動いていた機能が動かなくなった、という事例は枚挙にいとまがありません。ましてやサービスパックのように大規模なシステム変更は綿密な互換性テストを行った上で実施されます。そして、最新の製品に移行することは、慎重な検討と検証の上で実施されるべきものです。

サポート終了後に使用し続けてはいけない理由

Windows Server 2008 に限らず、サポートが終了した製品を使用し続けることに対して、多くの企業が警告を発しています。
多くのソフトウェア製品は、製品を利用することができる「使用ライセンス」の契約をしており、ほぼすべての契約においては、サポートが終了した製品の利用を制限する条項はありません。メーカーがメンテナンスを終了した製品を利用する場合、そのリスクを理解したうえで使用を続けることは可能です。
ではなぜ、ソフトウェア製品に関して、メーカーや IT 企業はサポートが終了した製品の使用を止めるよう訴えているのでしょうか。それには、いくつかの理由があります。

理由 1：残存するセキュリティホールがサイバー攻撃の突破口として悪用される可能性がある
サイバー攻撃は、自然発生的に起こるものではありません。背後には明らかに悪意のある人物や組織がいて、何らかの意図をもって攻撃行為を行います。製品の安全上の欠陥である脆弱性は、過去から何度もサイバー攻撃の手段として悪用されています。セキュリティアップデートが適用されていない、またはネットワーク経路上でのセキュリティ対策が行われていない場合、脆弱性を突いたサイバー攻撃は深刻な被害につながります。

2017 年 5 月に深刻な被害を引き起こした「WannaCry」は、マイクロソフト社の OS に搭載されている SMB 通信機能に含まれる脆弱性を悪用し、企業内で感染を広げました。悪用された脆弱性は、「MS17-010:Microsoft Windows SMB サーバのセキュリティ上の脆弱性」で、Windows xp 以降の Windows が影響を受けましたが、その当時 Windows xp や Windows Serve 2003 といったサポートが終了した製品では、脆弱性が放置されていたことから被害が拡大しました。

多くの製品は、過去の製品との互換性を維持するため、古くからあるライブラリーと呼ばれる機能群を利用しています。例えば、Windows Server 2008 の場合、そのツールは Windows 2000 Server よりも古いバージョンから引き継いだコードも多く残っており、おそらく最新の Windows Server 2019 にも引き継がれているとみられます。
つまり、今後 Windows Server 2019 上で発見された脆弱性は、同様の機能が実装されている過去の製品、例えば Windows Server 2008 にも含まれている可能性を否定できません。
2018 年 8 月にセキュリティアップデートとして提供された CVE-2018-8341 については、Windows カーネルに潜む脆弱性について述べられていますが、影響を受ける Windows は、クライアントの Windows7 から Windows Server 2016 まで全バージョンに渡ります。

さらに、すでにサポートを終了している Windows xp や Windows Server 2003 にもこの脆弱性は残存していると考えられ、現在もこれらの製品を使用し続けていることはリスクが高いと考えられます。

なお、マイクロソフト社は、サポートが終了した製品に対しても、実害につながる脆弱性に対しては、例外的にセキュリティアップデートを提供したことがあります。しかし、それらの例外対応を期待して、サポート終了製品を使用し続けることはお勧めできません。

理由 2：最新の技術によるオペレーティングシステム保護機能が十分ではない

サイバー攻撃が日々巧妙化していることはよく知られており、メーカーも製品のセキュリティ品質を高める取り組みを行っていますが、人間が開発した大規模かつ複雑なシステムの場合、脆弱性の存在を完全に排除することは困難です。そのため、脆弱性をゼロにするのではなく、たとえサイバー攻撃が行われたとしても被害を最小限に抑えるための機能が搭載されています。

例えば、Windows Server 2016/2019 の場合、次のような脆弱性を悪用したサイバー攻撃に対するセキュリティ対策機能が実装されています。

Just Enough Administration (JEA)
Windows PowerShell で管理する権限の制限する機能

Credential Guard
特権を持つシステムソフトウェア以外の動作を制御する機能

制御フロー ガード(CFG)
メモリ破損の脆弱性に対処するセキュリティ機能

Windows Defender Advanced Threat Protection (ATP)
ホストへの侵入防御機能

これらの機能は、脆弱性を悪用したサイバー攻撃が、システムに深刻なダメージを与えることを制限する機能です。
マイクロソフトが公表するセキュリティ情報を見ると、Windows Server 2016/2019と、それ以前の製品において深刻度の評価が違う場合がありますが、それはこれら機能を有効にしたことによる回避策が提供されているためです。
これらの技術は、時代に即して機能を拡張したもので、古いアーキティクチャの製品に実装することはできません。そして昨今の「被害前提のセキュリティ対策」において、これらの機能の活用が必要となっています。

理由 3：システム全体での整合性

企業は、Windows のオペレーティングシステムを利用したいのではなく、情報システムは業務システムの基盤として利用していることでしょう。業務アプリケーションなどは、パッケージとして販売されたもののほか、自社で開発したものなど多岐にわたりますが、オペレーティングシステムのサポート終了は、システム全体の運用管理の整合性に影響を与えます。実際には、Windows Server 2008 のサポート期間にアプリケーションのメンテナンス期間が過ぎていたり、その逆のケースもあります。
今利用しているシステムが、事業活動において重要な役割を果たしているのであれば、メンテナンスの行き届いた製品で確実な運用を行うことが望まれます。

Windows Server 2008 を利用する企業が取るべきアクション

このように、サポートが終了した Windows Server 2008 に関するリスクが眼前に迫る中、今なお利用を続けるユーザーが取れるアクションにかかる時間と費用と考えると、現実的な選択肢は限られます。
以下にユーザーが取るべき対策を、有効な順に説明します。

対策 1：Windows Server 2008 を Microsoft Azure 環境に移行し、3 年の猶予を得る

2020 年 1 月 14 日のサポート終了日まで 1 年を切り、重要なシステムを確実に移行する計画を一から始めることは現実的に難しくなってきました。国内にはまだ非常に多くの Windows Server 2008 が稼働していることを考慮し、マイクロソフト社は延命策を提案しています。それが、オンプレミス環境で稼働している Windows Server 2008 の Microsoft Azure への移行です。Microsoft Azure は、仮想マシン環境を提供するパブリッククラウドサービスですが、Azure への移行によりセキュリティアップデートを 3 年間継続して提供されることになります。
現在使用している Windows Server 2008 環境を、移行ツールを使用してパッケージ化し、Azure 上へ転送することでスピーディーにサーバ移転は完了します。
しかし、オンプレミス環境に構築されたサーバ環境を Azure に移行するだけで問題は解決しません。移行するサーバが単体で動作する場合であれば、社内からの通信経路の確保だけで済みますが、他のシステムとの連携がある場合には、システム全体の移行計画が必要となり、費用も増加します。
システム全体の整合性を考慮し、移行計画をする場合、数か月の検討期間と移行作業期間が必要となることから、Azure への移行であってもあまり猶予は残されていません。
ただし、Azure への移行により延命される 3 年は、次のシステムへの移行期間と理解し新しいシステムへの移行計画を立てるべきです。

対策 2：拡張セキュリティ更新プログラムを契約し、セキュリティアップデートを入手する

マイクロソフト社は、2018 年 8 月にオンプレミス環境で Windows Server 2008 を利用する企業を対象に、2019 年 3 月 1 日より「拡張セキュリティ更新プログラム」を有償で提供しています。
この拡張セキュリティ更新プログラムは、移行の猶予が必要な Windows Server 2008 のライセンス金額の 75%を支払うことで、1 年間の延命支援を受けられるものです。そして拡張セキュリティ更新プログラムの期間は、3 年間と有限となっておりそれ以降のサービスはありません。
対策 1 にあるように、Azure 環境へ移行するよりも高額となりますが、今使い続けている環境を維持できることは魅力的ですが、サーバ OS の移行やシステムの刷新の期限が 3 年であることは変わりません。
ラックとしては、ハードウェアトラブルや管理運用コストに優れる Azure 環境への移行を推奨します。

対策 3：セキュリティ対策機能を導入し防御する

次に考えられることは、Windows Server 2008 へのサイバー攻撃を防御するセキュリティ対策ソリューションを導入することです。セキュリティアップデートは、特定の脆弱性の修復のために提供される不具合の修正であり、本来はサイバー攻撃がサーバに届かなければ問題にはなりません。
以前より、脆弱性を悪用したサイバー攻撃をネットワーク上で検知し防御する製品がありますが、それを活用することでセキュリティ対策を強化します。

この対策は、サーバの構成を変えずにサイバー攻撃を防ぐことができることから有効であると思われがちですが、根本的な脆弱性対策ではなく、あくまでもリカバリー的な対策であることと、脆弱性への攻撃を必ず防ぐことができるとは限らない点が懸念されます。
また、導入には安定して稼働するネットワークの経路上に設置することになり、不具合の有無の検証や機器の購入費用に加え、保守や運用ノウハウを習得する必要があり、それらの投資に見合った効果があるかどうかを検討する必要があります。

対策 4：Windows Server 2008 を、Windows Server 2016/2019 にアップグレードする
最後に、最新のセキュリティ技術が実装され、今後も継続的にメンテナンスが行われる新しいバージョンの Windows Server に移行するという選択肢があります。
しかし、プラットフォームのアップグレードを数か月のうちに実施することは現実的ではありません。
Windows Server 2008 から Windows Server 2016/2019 へのアップグレードは、いったん Windows Server 2012 へのアップグレードを行った上で、2016/2019 へのアップグレードをしなければならず、それだけ内部の構造が変化しています。つまり、現在稼働しているシステムの互換性が著しく低く、その検証が重要となります。
また、現環境で利用しているミドルウェアはアプリケーションが、最新の Windows テクノロジに対応してない可能性が高く、その場合には周辺環境のバージョンアップなども必要となります。それにより IT 投資金額も増大することが予測されます。

以上を踏まえ、結論としては、Windows Server 2008 の当面のセキュリティ確保のため、3 年のメンテナンス期間延長のために Microsoft Azure 環境へ移行計画を実行し、2020 年以降はシステムのリプレース計画を検討することをお勧めいたします。

本件に関してラックが行える支援

ラックは、セキュリティ対策に関する技術と知見を強みとした、システムインテグレーターです。クラウド環境でのシステム構築やシステム開発の経験を活かして、Windows Server 2008 の EoS 問題の解決を支援いたします。

前述した対策 1～4 に関しては、難易度（リスク）、必要時間、必要予算の違いはありますが、すべて対応することは可能です。しかしながら、Windows Server 2008 のサポート終了によりリスクを回避しつつ、安定稼働できる環境が短期間かつ低価格で入手でき、新しいシステムへの移行の期間を確保できる手段としては、対策 1 の「Azure 環境への移行」を強くお勧めします。

ラックが提供する「セキュリティ診断付 Azure 移行支援サービス」は、オンプレミス環境もしくは他のクラウド環境から Azure 環境への移行の計画、実施をサポートします。もちろん、複数サーバを連携して稼働するシステム全体の移行にも対応いたします。また、Azure 移行後のシステムのセキュリティ診断を行い、セキュリティ対策の支援を行います。

セキュリティ診断付 Azure 移行支援サービス　サービス概要

サービス名	内容概要
計画フェーズ	対象システム、サーバ機器のシステム構成、ネットワーク構築の把握
	Azure 環境へのマイグレーション設計（ネットワーク設計、キャパシティプランニング、アプリケーション構成、カスタマイズ内容の把握）
	クラウドへの VPN 接続・閉域網接続するためのネットワーク設計
移行フェーズ	移行用サーバの設置
	移行先環境の構築
	クラウドへの VPN 接続・閉域網接続するためのネットワーク構築
	データ同期
	移行テスト
	移行実施
	システム移行確認
	簡易セキュリティ診断
支援フェーズ	運用支援
	作業環境の破棄及び原状復帰
オプションサービス	ユーザーサポートサービス
	Azure 環境移行後のアドバンスドセキュリティ診断およびリスクアセスメント
	プラットフォームマイグレーション、システムリプレースに関する支援

以上

２０１９年６月 27 日　発行