●Windows Server 2003 サポート終了とは

2015 年 7 月 15 日(日本時間)にマイクロソフト社が提供している OS「Windows Server 2003」のサポートが終了します。

●Windows Server 2003 のサポート終了後は？

OS のサポート終了後は、新たな脆弱性が発見されても修正プログラムが提供されないため、脆弱性を悪用した攻撃を受け、「サーバーが乗っ取られる」「業務が停止する」「機密情報が漏洩する」などの被害に遭う可能性があります。また、脆弱性は昨今問題となっている内部不正への悪用も懸念されるため、企業・組織のリスク回避の観点から、「Windows Server 2003」を利用するシステムは後継システムへの移行が求められます。

サポート終了の影響

・セキュリティ更新プログラムの停止

・問題発生時のマイクロソフトのサポートが受けられない

・他メーカーの製品サポート終了の可能性

●ソフトウェアのライフサイクルを意識した計画的なシステム運用を

企業・組織の管理者は自組織のシステムに使用しているソフトウェアのライフサイクルを常に念頭に、安全な運用の維持を心掛けておく必要があります。サポート終了がきっかけで直ちに被害に遭うわけではありませんが、事業へのリスクを回避するために、いまからでも移行計画を立案し、後継システムへ可能な限り早く移行させることが望まれます。

●サポートが継続しているサーバーOS とそのサポート期間

・Windows Server 2008 R2

サポート終了予定日 2020 年 1 月 15 日（日本時間）まで（2015 年 4 月現在の情報）

・Windows Server 2012 R2

サポート終了予定日 2023 年 1 月 11 日（日本時間）まで（2015 年 4 月現在の情報）

●FileMaker Server 14 対応サーバーオペレーティングシステム

1）Windows Server 2012 R2 Standard Edition
(更新プログラム 2919355 をインストール済み)

2）Windows Server 2012 Standard Edition

3）Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition

4）OS X Yosemite 10.10

5）OS X Mavericks 10.9

●Windows Server 2003 サポート終了に関する情報

マイクロソフト社でも Windows Server 2003 サポート終了に伴うセキュリティ上のリスクや移行相談窓口のページを公開していますので、あわせてご確認ください。

Windows Server 2003 移行相談窓口

無償コール センター サービス

TEL：0120-39-8185　受付時間: 9:00 ~ 17:30

営業日: 月曜日～金曜日(日本マイクロソフト社指定休業日を除く)

（補足）
・Windows OS のサポート
　Windows OS のサポートには、「メインストリーム サポート」と「延長サポート」の 2 種類が存在し、「メインストリーム サポート」は、現役製品としてのサポート期間で、セキュリティ更新だけではなく、OS としての不具合対応であったり無償サポートが提供されている期間です。これに対し、「延長サポート」は退役前のサポート期間で、セキュリティ更新と有償サポート以外のサポートが停止します。つまり、Windows Server 2003 および、Windows Server 2003 R2 は、現在「延長サポート」期間中であり、すべての延長サポートが 2015 年 7 月 14 日（日本時間では 15 日）に終了することになっています。
　延長サポートが終了すると、まず延長サポートで提供されていた「セキュリティ更新」と「有償サポート」のサービスが停止します。マイクロソフトから毎月提供されている Windows Update などが停止され、何か問題が起きた時のサポートも受けられられなくなります。また、Windows Server 上で動作しているソフトウェアや周辺ハードウェアを提供している他のメーカーも、マイクロソフトの公式サポート終了に合わせて、各種サポートを終了する可能性が挙げられます。

最新のセキュリティ脅威は、想像以上に高度化、進化しており、ウイルス対策ソフトやファイアウォールだけでは決して十分ではありません。あなたの会社でも、まだこんな誤解していませんか？
・残っているのは古いファイルサーバーのみで、リスクは低い
　たとえ重要な情報が保存されていなくても、古いファイル サーバーは、攻撃者の格好のターゲットです。密かに侵入した攻撃者は、ファイル サーバーにマルウェアを置きます。すると、社内のユーザーが次々とアクセスして感染が拡大。半年もすれば、管理者権限を持つユーザーが感染し、その ID とパスワードが盗まれます。そうなれば、社内のあらゆるデータが危険にさらされます。その中に取引先や銀行口座の情報も含まれていたら･･･。現実に、同様の手口で口座情報を盗まれ、不正送金の被害にあったり、取引先から委託された個人情報が漏えいし、取引停止となり、倒産に至るケースも増えています。
・マルウェア対策ソフトを入れているから問題ない
　たとえサーバーの OS のサポートが終了していても、マルウェア対策ソフトを導入し、パターン ファイルを最新にしているから大丈夫だと思っていませんか? それで防ぐことができるのは、マルウェア全体の 9 割だと言われています。残念ながら、残り 1 割は防げません。マルウェアが爆発的に増えているのに加え、標的型攻撃で使われる特定企業をねらったマルウェアは、パターン ファイルで検知できないのです。たとえ 1 割でも防げなければ、感染はシステム全体に広がってしまいます。残り 1 割のマルウェアを防ぐことは、とても難しいのが現実です。
・ファイアウォールがしっかりしているから大丈夫
　ファイアウォールを設置しているから侵入されない、と考えていませんか? 確かにファイアウォールは、外部からの不正侵入を防ぐ有効な手段です。より高度な IPS、Web ア

プリケーション用の WAF などのツールも開発されています。しかし今、最も脅威となっているのは、内部からの侵入です。大規模な標的型攻撃で、犯行グループが内部に協力者を送り込み、システムを内部感染させることもあります。事前に取引業者や社内の人間関係を調べ、不自然ではないメールを送り付け、システムを感染させることもあります。ねらわれているのは、むしろ人なのです。

・延命措置のソリューションを導入すれば何とかなる

Windows Server 2003 のサポート終了に向けて、さまざまな延命ソリューションが登場しています。このため、こうしたソリューションを導入すれば問題ないと思っていませんか? しかし、これらは新しいサーバーに移行するまでの一時的な対策にすぎません。今から 12 年前にリリースされた Windows Server 2003 は、いわば玄関の鍵しかない古い家のようなものです。そしてサポート終了後は、壁に穴が見つかっても修復されません。延命用ソリューションとは、この家を柵で囲む対策であり、家そのものの強度を上げることはできないのです。

・最新の OS ほど、セキュリティのリスクも低い

Windows Server 2003 がリリースされたのは 2003 年 6 月です。当時のセキュリティの脅威は、自身の技術をアピールしたり、世の中を騒がせたりすることを目的とした愉快犯が中心でした。このため、OS のセキュリティも、こうした脅威に対抗できる水準にとどまっています。しかし、当時と今では、IT 技術は劇的に進化し、セキュリティ上の脅威も、金銭目的や機密情報をねらった組織犯罪へと変質しています。したがって、当時の OS を現在利用することは、非常に危険と言わざるをえません。現実に、新しい OS であるほどマルウェアの感染率は低くなることが、客観的なデータとして示されています。

・攻撃の高度化に対応し、OS も進化を続けています

現在、攻撃の手法は高度化、複雑化、大規模化しています。たとえば、金銭を目的とする標的型攻撃では、攻撃者が膨大なコストをかけて独自のウイルスを開発し、ターゲット企業の取引先や人間関係を調べ上げ、内部に協力者を送り込んでシステムを感染させることも珍しくありません。こうした脅威に対抗するため、Windows は常に新しい技術を取り込んで、セキュリティを強化し続けています。新しい Windows が登場すると、どうしても操作性や快適性などの目に見える機能に注目が集まりますが、実は目には見えないセキュリティ機能の強化に、膨大な投資が行われているのです。

・管理者権限を適切に管理できるアーキテクチャをご用意

最新の Windows では、「多層防御」という考え方に立ってセキュリティ機能を提供しています。Windows Server 2003 では、管理者権限が漏えいすると、すべての権限が乗っ取られてしまいます。しかし、多層防御の考え方に立つ最新の Windows では、管理者権限を細かく区切り、たとえ 1 つの権限が乗っ取られても、できることを限定することで情報資産を守ります。建物でいえば、玄関の鍵しかなかったのが Windows Server 2003 です。玄関を突破されたら、すべての部屋に侵入されてしまいます。一方、最新の Windows は、玄関だけでなく、部屋ごとに鍵がかけられるので、被害を最小限に抑えられるのです。