ORACLE

ソフトウェアパッチは安全の維持に不可欠です：対策はお済みですか？

ご自身のセキュリティ戦略は安全で包括的でしょうか？
危険な橋を渡らないでください。

「オラクルのサポートは、オラクル以外のサードパーティーのソフトウェアサポート業者が提供するサービスをはるかに超える水準で、機能とセキュリティを提供します」[1]

なぜパッチは必要か？

技術分野の世界的な調査会社、Omdia（オムディア）の年次調査では、最も重要なトレンドの上位3件は**セキュリティ・ID・プライバシー**の管理であるとしています。

ソフトウェアパッチの適用とメンテナンスを適切に実施しなければ、会社の収益と評判を危険にさらすことになります。

直面する可能性のある脅威：

- 盗難
- 経済的損失
- ブランドの信用失墜ダメージ
- 詐欺
- 罰金

パッチ適用は、プロアクティブな保護戦略の重要な手段であり、優れた**IT**セキュリティガバナンスにとって不可欠です。ソフトウェアの定期的なパッチ適用とメンテナンスの確実な実施は、すべての企業にとっての必須要件です。

「ベンダーソフトウェアのパッチを速やかに適用することは、存在している未対策の　セキュリティ脆弱性から生じるリスクを回避するために不可欠な基盤です」[2]

パッチ適用の利点

定期的なソフトウェアパッチの適用を実施する理由は多数あります。その中でもこの2つが重要であるとオラクルは考えています。

1. **強力なソフトウェアセキュリティを維持する:** 厳格なソフトウェアセキュリティとメンテナンスプログラムは、継続的な警戒と維持が必要です。
2. **ITガバナンスとコンプライアンスのニーズを満たす**: 定期的なソフトウェアのパッチ適用と保守サービスなしに、コンプライアンスの強力な基盤と文化は存在しえません。

「ベンダー提供のパッチで［あなたの］資産を最新の状態に保つことは、ソフトウェア関連の脅威から保護するという点において最も基本的でタイムリーな手段です」[3]

連邦取引委員会（FTC）は、サードパーティソフトウェアの更新やパッチ適用を実施すること、ベンダーからのセキュリティ警告に注意してすみやかに対応することを推奨しています。

ソフトウェアパッチ戦略はどのように組み込むべきか？

以下は、より**強力なセキュリティ**につながるパッチ適用ガイドラインです：

1. 健全な組織にとってパッチ適用が不可な要素であるという**認識**を習慣づける。
2. **ビジネスリスクと技術リスク**に基づいてパッチに優先順位を付ける。
3. **定期的なセキュリティメンテナンス**の重要な部分として確実にパッチを適用する。
4. リスク回避のため、パッチの適用は必ず**ソフトウェアベンダー**立ち合いのもとに実施する。

「ソフトウェアベンダーは自社製品のパッチ適用・サポート・セキュリティ保護に関して最も多くの経験と専門知識を持つため、企業は緊密に連携する必要があります」[4]

なぜ信頼できるパートナーが重要なのか？

企業は信頼できるプロバイダーと提携して、**ソフトウェアのセキュリティを最新の状態に保ち、潜在的な脆弱性**に対処するための手順を実施しなければなりません。

オラクルのような信頼できるパートナーを見極めるうえで役立つ**3つの特性**をご紹介しましょう。

信頼性

企業のIT環境でデータを守るための知識と専門性を備えている。

企業クラスのセキュリティとサポートを扱うことにおいて長年の経験がある。

安全性

ITスタック全体のセキュリティ保護において経験がある。

プロアクティブでリアルタイムのサポートリソースを提供する専門家である。

包括的

絶えず進化し改善されるセキュリティとサポートの完全な統合セットを提供している。

ITセキュリティとコンプライアンスを中心とする文化の確立を支援できる。

サードパーティサポートで欠けているものは何か？

1. セキュリティ修正：

サードパーティベンダーが主要なセキュリティ修正を提供できない理由は以下の通りです：

- **オラクルのソースコードを部分的に変更することができない。**
- **オラクルが修正する脆弱性の技術的な詳細に精通していない。**

2. 継続的なセキュリティ保証の取り組み：

Oracle Supportのお客様が、オラクルのセキュリティ保証の取り組みにより、サードパーティサポートの顧客には得られない方法で利益を得る理由は以下の通りです：

- **過去の修正とパッチは、後からリリースされる各オラクルソフトウェアに組み込まれている。**

「サードパーティサービスプロバイダーの不十分な来歴では、潜在的なリスクが発生するだけでなく、ソフトウェアの標準的な開発経路から逸脱しているため、所有コストが増え、後の段階で回帰コストが発生する可能性があります」[5]

結論

オラクルを含むエンタープライズソフトウェアを保護するには、セキュリティソフトウェアのパッチ適用が不可欠です。**コードへの十分な権限を持たない場合、コードにアクセスしたり更新したりすることはできません。**これにより、ソフトウェアが攻撃されやすくなり、ビジネスを危険にさらすことになります。

サードパーティサポートとセルフメンテナンスとは：

- **不十分なセキュリティ更新**
- **不十分なセキュリティ修正**
- **不十分な脆弱性の排除**

オラクルで強力なセキュリティを実現しましょう

ITガバナンスとコンプライアンスのニーズを満たしながら、オラクルソフトウェアの重要なセキュリティ更新と保護を確保しましょう。オラクルなら次のことが可能になります：

- **定期的なパッチ適用スケジュール**と全社的なITセキュリティに重点を置き、システムの脆弱性を減らし安全性を高めることを保証します。
- ソースに**信頼できるセキュリティアップデート**を実施
- **プロアクティブな変更管理**プロセス

Omdiaの全レポートを読む

Oracle Premier Supportにアクセス

[1] [5] Omdia. (2023). Sustainable Software Patching: Critical for Solid Security, Reduced Risk, and Meeting Compliance Challenges.　(持続可能なソフトウェアパッチ適用: 強固なセキュリティ、リスクの軽減、およびコンプライアンスへの対応に不可欠)