ORACLE

貴社のソフトウェアはサイバー犯罪に対応しきれますか？

サードパーティのサポートやセルフメンテナンスでは、完全に犯罪から保護することは出来ません—本当のソリューションがここにあります。

サイバー犯罪は実在します

23兆ドル

2027年までに予測される世界中のサイバー犯罪被害の年間コスト[1]

サイバー攻撃やデータ漏えいは指数関数的に増え続けています[2]

2024年のデータ漏えい被害の世界平均コスト[3]

488万ドル

ランサムウェア攻撃

あらゆる業界に影響を及ぼす絶え間ない脅威[4]

多くのビジネスがこの影響から立ち直ることができません

- 機密的専有情報
- 業務中断
- システムおよびファイルの修復
- 罰金や訴訟
- 企業に対する評価やブランドの被害
- 顧客や社員の信頼

サードパーティのサポートプロバイダーや、セルフメンテナンスセキュリティ方法にごまかされないようにしましょう

1 「仮想パッチ」は実際のパッチではない

仮想パッチは応急処置であり、ソフトウェアを実際にパッチしたりアップデートするものではありません。

- 暫定的ソリューション
- 根本的な問題の放置
- 脆弱性の全容の無視

米国 国土安全保障省

「潜在的な脅威に対して適切な予防措 置が取られているかを確認する、強固で継続的なパッチ管理プロセスを確立することは、全ての組織にとって不可欠な事項です。」

https://www.cisa.gov/

2 「総合的なセキュリティ」は完全ではない；ファイアウォールは万全ではない

ペリメータに集中したセキュリティ戦略では、ソフトウェアは攻撃に対して脆弱になります。

- 内部漏洩の影響を受けやすい
- ネットワークの脅威に対する可視性の制限
- ソフトウェアの実際のセキュリティを無視

EU一般データ保護規則

データプライバシーを高め、個人データおよびデータ処理のセキュリティを確保する様々な規則

- ☑ 欧州連合居住者のデータを扱う全ての組織に該当
- ☑ 2018年5月25日施行
- ☑ 非遵守および違反の場合は多額の違反金が発生することがある

https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en

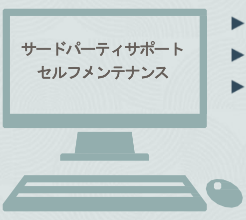
3 セルフメンテナンス＝潜在的責任

自社のメンテナンスは、ソフトウェアを重要なセキュリティアップデートから隔離してしまう恐れがあります。

- 多くの脆弱性を（法的に）修正する力がない
- 新規パッチやアップデートへアクセスできない
- 確実にメンテナンスや保護を行う際の制限されたリソース

要点

セキュリティパッチは、Oracleを含めた企業ソフトウェアの保護に必要不可欠なものです。コードにアクセス出来ないと、そのためのパッチを開発することができません。これによって貴社のソフトウェアは攻撃に対して脆弱になり、また貴社ビジネスをリスクに晒すことになります。



- 不十分なセキュリティ更新
- 不十分なセキュリティ修正
- 不十分な脆弱性に対する保護

Oracle サポートで、Oracle のソフトウェアを保護しましょう

Oracle サポートは、貴社のOracle ソフトウェアがミッションクリティカルなセキュリティアップデートや保護を法的に受ける最適な方法です。

Oracle はソースコードを作成、所有

- 脆弱性および発生する脅威の発信源の認識および対処ができます
- 信頼できるソースのセキュリティアップデートを実行します

Oracle は全レベルに対してセキュリティを提供

- ソフトウェアスタックの全ての階層をパッチします
- 全てのスタックへの回帰テストを行います

Oracle にはツール、経験そして知識があります

- 積極的な変更管理のプロセス
- 統一したリリース管理のプロセス
- 信頼された継続的かつ前例のないイノベーション

Oracle を最大限活用しましょう。

貴社ビジネスが脅威に直面した際、信頼され、安全かつ包括的なサポートに代わるものはありません。

Oracle Premier Support

ソース：
1. https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020
2. https://www.wipro.com/securitymagazine.com/articles/100335-cyberattack-attempts-increased-104-in-2023
3. https://www.ibm.com/reports/data-breach
4. https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf