protiviti®
Face the Future with Confidence

2021年5月19日「プロティビティ・CyberArk共催ウェブセミナー企業のセキュリティ強化を加速させるアクセス管理の進め方」ご質問とプロティビティの回答

No.	頂いたご質問	Protiviti回答
1	他社での同様のサービスが多々あるかと思いますが、本サービスの独自性&強みがあればご教示いただけますか。	①管理対象が、サーバ、一部のネットワーク機器・DBに限定されず、ビジネスアプリケーション、IaaS/SaaS、RPA、DevOpsツール、端末等に渡り多様なこと、 ②統制・セキュリティ機能として、特権IDの保存・変更、アクセス履歴の取得だけでなく、アプリケーション埋め込みパスワードの排除、不正特権アクセスのリアルタイム検知・防御、最小特権の強制等により、セキュリティレベルを上げられること、の2点です。
2	CyberArkのソリューションはクラウドでの提供に限りますか。オンプレ版というのは存在しますか。	オンプレミスのソフトウェアも提供しています。
3	「特権ID管理」と「特権アクセス管理」の違い（方法、成果物など）を教えて下さい。	両者に明確な違いはございません。 海外ではPAM（Privilege Access Management）と呼ばれていることが多く、CyberArk社様も「特権アクセス管理」の表現に統一されているため、特権アクセス管理という言葉を用いました。 日本で言う「特権ID管理」もIDそのものを超えてアクセスに視点が置かれるようになっています。
4	特権IDの定期的な棚卸を手間少なく行える自動プロセス管理的な機能はありますか。	CyberArkの導入により、管理対象の特権IDに何があり、どう使われているかが常時把握できますので、棚卸自体が不要となります。
5	弊社独自のワークフローシステムによる特権IDの申請書に記載の利用者と、CyberArkでモニタリングする実際の特権IDの利用者が合致していることを確認する方法は有りますか。	利用者がCyberArkにアクセスする際に、ワークフローシステムで発行した承認キーを入力させるようにし、ワークフローシステムのログ上の被承認者と、CyberArkのアクセスログ上の利用者を突合する仕組みを作ることで可能です。 外部製品との連携については、PluginやAPIを持っており、作り込みにて柔軟に対応することが可能です。

No.	頂いたご質問	Protiviti回答
6	今回ご紹介いただいたCyberArk社の特権アクセス管理ソリューションを監査で利用することは一般的ですか。	CyberArk社様からご紹介いただいたように、不正特権アクセスをリアルタイムで検知・防止したり、日々の特権アクセスの運用に使われたり、クラウドサービスやDevOpS環境等へ管理対象を拡大するため、直接の運用は１線部門や２線部門で行うことが一般的な利用です。 監査部門としては、このツールを用いて特権アクセス管理に関するリスクが抑えられているかを監査することになります。ツールが管理対象とするシステムのカバレッジや、運用で用いられているレポート、日々のオペレーションが適切に行われているか等の観点で監査することになります。
7	２章でご説明いただいた「特権ID管理を構築するためのステップ」において、ステップ１の現状の把握は、どのような分析を行いますか。	貴社の規程類・ルールや、インタビューによる業務フローの分析等から、特権アクセス管理の態勢を、プロティビティが保有するリスク管理態勢のフレームワークを適用し、ステップ２の目指す姿の明確化を視野において現状分析を行います。 また、貴社の管理対象となる特権IDを簡易的に棚卸するCyberArk社のツールを適用し、管理対象の特権IDを明らかにするアプローチもございます。
8	CyberArk特権アクセス管理製品の提供形態を教えてください。	オンプレミスのソフトウェア提供、およびSaaSとしてご提供しております。
9	CyberArk特権アクセス管理製品はどのIaaSに対応してますか。	AWS, Azure, GCPです。
10	CyberArk特権アクセス管理製品の導入が、なぜDX推進と関連するのですか。	システム間連携でのパスワード管理をマニュアル管理としないことで、システムの自動化を促進するためです。