

# CyberArk

## 導入支援/運用支援サービス

### 特権アカウントの管理・防護を実現

標的型攻撃や内部不正への対策で最も重要視される対策として、特権アカウントの管理・防護があります。J SOX 法、PCI DSS、NIST SP800 171、システム管理基準（経済産業省）等の様々なガイドラインや、内部統制監査の基準として、特権アカウント管理は非常に重要となります。

企業を狙った攻撃や不正アクセスが急増している一方、特権アクセス管理がカバーすべき領域は拡大しており、これまでのような情報システム部門や担当者による限定的な管理ではない強力なセキュリティが求められています。

### 製品の特長

CyberArkは、特権アカウントにおける一元的な「管理」「利用」「監査」を提供します。

#### 1. 特権アカウントの管理

- 特権アカウントのパスワードを一元管理し、パスワードを定期的に自動更新します。利用者は特権アカウント情報を持たないため、パスワード漏洩リスクが低減されます。
- 特権アカウント・パスワード情報は暗号化されVault（金庫）サーバに安全に保管されます。
- 基本機能において管理対象の機器にエージェントなどの導入が不要です。

#### 2. 特権アカウントの利用

- 管理対象の機器への自動接続（利用者によるパスワード手動入力不要）を提供します。利用者は自身のIDでポータルにログインし、ポータル経由で管理対象の機器にアクセスします。
- 特権アカウント使用時の申請、承認のワークフロー機能を提供します。都度のアクセス承認、実施作業の制御も可能です。
- 外部スクリプトやアプリケーションが利用する埋め込みパスワードを利用する特権アカウントもカバーします。（※要オプションライセンス）

#### 3. 特権アカウントの監査

- 特権アカウントの利用履歴をレポート出力でき、監査に利用可能です。
- CyberArkを経由しない不正アクセスを検知します。
- 通常運用を自動的に学習し不振と判断したアクセス、閾値を超えたアクセスを検知します。

### 導入への課題

CyberArkの導入には求められる環境や細かな設定作業など技術的なノウハウが必要になります。

#### 課題 1

##### 適切な要件定義・システム連携の検討、権限の考慮などさまざまな検討が必要

- 既存環境に導入するために連携が必要なシステムが複雑すぎてわからない。
- ソフトウェアインストールや構築設定が多岐に渡り把握しきれない。
- 承認ワークフローやグループなど権限に関わる検討がどうしてもいかわからない。
- 対障害性など安定的な利用のための具体的な構成が設計しきれない。

#### 課題 2

##### 導入後の適切なチューニングや組織改編による変更が必要。

- 導入後に利用者からさまざまな要望が上がってくるため随時調査が必要。
- 社内異動やグループ統合などに併せた権限の変更が必要。
- メーカーからのセキュリティパッチなどメンテナンスに多くの稼働が取られる。
- 障害が発生した場合に、にどのように対処すればよいかかわからず不安。

# デジタルアーツコンサルティングに依頼するメリット

## 多くの実績をもつ技術者による導入・構築を全面サポート

- 導入に必要な各種システム連携事項のご提示から構築作業まで一括で対応。
- お客様のご希望に沿った動作設定を細かく実施することが可能。
- 運用を見据えさまざまなドキュメントのご提供。

## 継続的な安定利用向け長期的にサポート

- CyberArkの日々の運用に関わる設定変更などのご支援。
- 安定稼働のためのメンテナンス対応。
- 運用で必要となるスキルアップのトレーニングや各種お問合せに対応。

## サービス内容

CyberArkのご支援として大きく2つの工程に分けて提供いたします。

### 導入支援

お客様システム連携を行うための要件定義から詳細な設計および構築や試験までのご支援を行います。

### 運用支援

CyberArkの導入完了後の運用面でのご支援を行います。メンテナンス対応に加え、ご要望に併せてレポート抽出やパッチ適用なども対応いたします。

### 導入支援

	工程	サービス内容
1	要件定義	<ul style="list-style-type: none"><li>特権アカウントの利用・管理状況のヒアリングを行いCyberArkによる管理可否を実施</li><li>既存のシステム環境のヒアリングを行い既存システムとのCyberArk間での通信方式や認証連携を検討</li><li>特権アカウントの利用シーンに沿った機能の選択や設定内容を検討</li></ul>
2	設計・構築	<ul style="list-style-type: none"><li>要件に沿ったインフラ設計やCyberArkソフトウェア設計の実施</li><li>設計の内容に基づきインフラ基盤の構築や基本的な設定を実施</li><li>既存の特権アカウントの初期登録を代行して実施</li></ul>
3	試験	<ul style="list-style-type: none"><li>想定通りに動作しているかの確認</li><li>障害時など不測の事態を考慮した切り替わり試験</li></ul>
4	管理者向け説明	<ul style="list-style-type: none"><li>管理者向けに必要な作業に関するトレーニング</li><li>管理者向け手順書などドキュメント作成</li></ul>

### 運用支援

	業務範囲	サービス内容
1	設定代行	特権アカウントの追加や削除などの対応
2	脆弱性・不具合対応	<ul style="list-style-type: none"><li>定期的に発生する脆弱性や不具合パッチの調査・適用</li><li>EOLなどによるソフトウェアバージョンアップの支援</li></ul>
3	お問い合わせ・障害対応	<ul style="list-style-type: none"><li>CyberArkに関するお問い合わせの調査・回答</li><li>不具合・障害など不測の事態における解決までのご支援</li></ul>

### 本サービスに対するお問い合わせ先

デジタルアーツコンサルティング CISOサービス事業部  
ismap-pro@con.daj.co.jp



デジタルアーツコンサルティング株式会社  
東京都千代田区大手町1-5-1 大手町ファーストスクエア ウエストタワー14F  
Tel: 03-6206-3421