パスワード変更対応デバイス一覧

Operating Systems	Microsoft, IBM, Oracle, HP, Redhat, Ubuntu, Fedora, CentOS, Novell, Vmware, Apple, Citrix, EMC NetApp, BigIP/F5, Juniper
Windows Applications	Windows Services, Windows Scheduled Tasks, IIS Application Pool, IIS Directory Security (Anonymous User), Windows Registry COM+, Cluster Service
Data Base	Oracle, SQL Server, DB2, MySQL, Sybase, ODBC
Applications	SAP, IBM, BEA, JBOSS, Oracle, CyberArk, Tomcat, HP, TIBCO, Cisco, BMC, Sensage, Infomatica, Tenomos, SoftwareAG, Xerox
Security Appliances	Checkpoint, Nokia, Cisco, Juniper, Fortinet, Blue Coat, Palo Alto, IBM, SourceFire, TippingPoint, WatchGuard, Acme Packet, Critical Path, Symantec, Safenet, ProofPoint, McAfee
NW Device	Cisco, Juniper, Nortel, Alcatel, F5, HP, 3com, Enterasys, Meinberg, Citrix, Riverbed, Netscout, Aruba, Avaya, Bluecoat, Brocade, Radware, Yamaha, Voltaire, BTI Photonic Systems, RFL lectronics, Applied Innovation, Symmetricom, WAAS, Fujitsu, Nokia, McAfee
Directories and Credential Storage	Microsoft, Oracle, Novell, Unix vendors, RSA/FoxT, CA, Symantec, IBM
Remote Control and Monitoring Devices	IBM, HP, Dell, Oracle , Digi, Cyclades, Fujitsu
Storage	NetApp, EMC, IBM, HP
SaaS/Web Sites	Facebook, Gmail, Linkedin, Twitter, Amazon(AWS), Microsoft(Azure, Office365), Pinterest
OT/SCADA	Industrial Defender, GE, RuggedCom

※ お客様の環境によってはカスタマイズが必要な場合がございます。また、記載の内容は予告なく変更する場合があります、詳細はお問い合わせください。

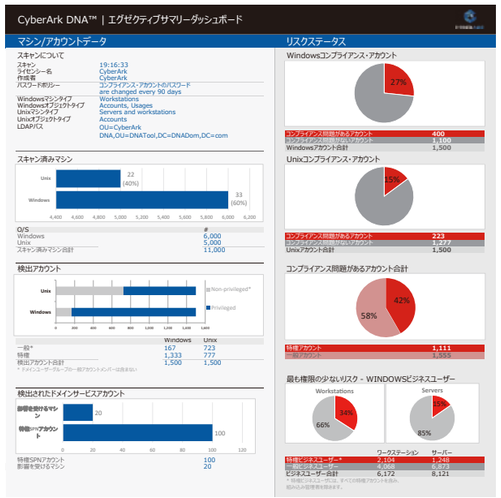
特権アカウント管理状況調査ツール

Discovery and Audit（DNA）

DNA (Discovery and Audit) は、サーバ・端末に登録されているアカウントを洗い出し、管理状況やリスクを調査します。

- サーバに存在するアカウントと SSH 鍵の洗い出し
- 長期間パスワード変更されていないアカウント
- Pass-The-Hash によるアカウント盗難のリスク
- ハードコードされた特権アカウントの抽出
- ゴールデンチケット攻撃のリスク
- AWS 環境に対するスキャン

本ツールは、特権アカウント管理を検討されているお客様に無償で提供いたします。詳しくは弊社までお問い合わせください。



※本製品の仕様、価格等は予告なく変更する場合があります。

お問い合わせ

フューチャーセキュアウェイブ株式会社

〒141-0032 東京都品川区大崎2-9-3　大崎ウエストシティビル
【Tel】03-5634-7655　【E-mail】contact@securewave.co.jp
https://www.securewave.co.jp/

FUTURE SECURE WAVE

CYBERARK®

グローバル スタンダード セキュリティで特権アカウントを管理 / 保護

PRIVILEGED ACCESS MANAGER

サイバー攻撃の 80% 以上で悪用されている特権アカウント。
特権アカウントを管理 / 保護することで情報資産を被害から守る。

特権アカウントの管理、制御、監査を可能とする **CORE PRIVILEGED ACCESS SECURITY**

CYBERARK

CyberArkのアイデンティティセキュリティ製品は、70,000社以上、Fortune 100の59%が導入、Global 2000の35%以上に採用されています。

- 特権アカウント利用者、管理デバイスの一元管理による運用管理業務の効率化を実現
- 特権アカウントを利用したアクティビティの監視と記録
- パスワード保護による、セキュアなアクセス環境の提供
- 権限とアカウント情報の分離

特権アカウント保護の重要性

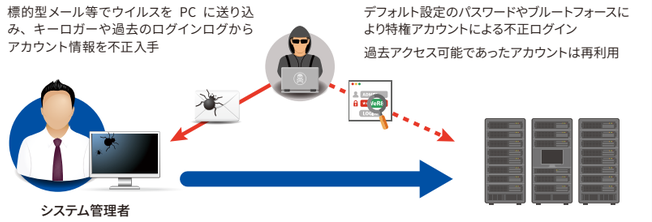
- あらゆるシステムに特権アカウントは存在する -
- 攻撃者は特権アカウントの奪取を狙っている -

Administrator や root などに代表される特権アカウントは、あらゆるシステム・デバイスに存在します。システムの管理 / 運用上不可欠なものですが、特権アカウントを利用するとシステム上で可能な行為がすべて実行可能となるため、サイバー攻撃者は特権アカウントの奪取を狙っています。

CyberArk 社の調査によるとサイバー攻撃の 80% 以上で特権アカウントが悪用されていると報告されています。

特権アカウントに関するリスク（例）

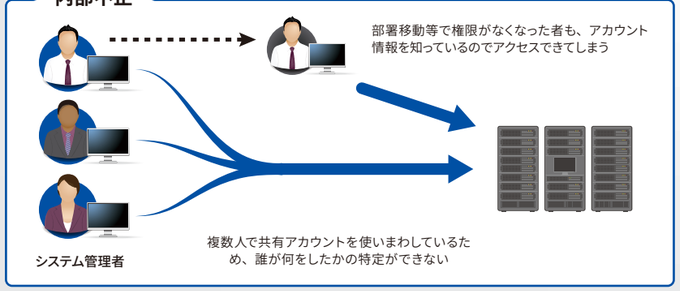
外部脅威



問題：

- 管理者 PC 上で特権アカウント情報を入力するため、必ず情報が残ってしまう。
- 定期的なパスワード変更やランダムな文字列設定は運用負荷が高く、手動での実行が難しい。

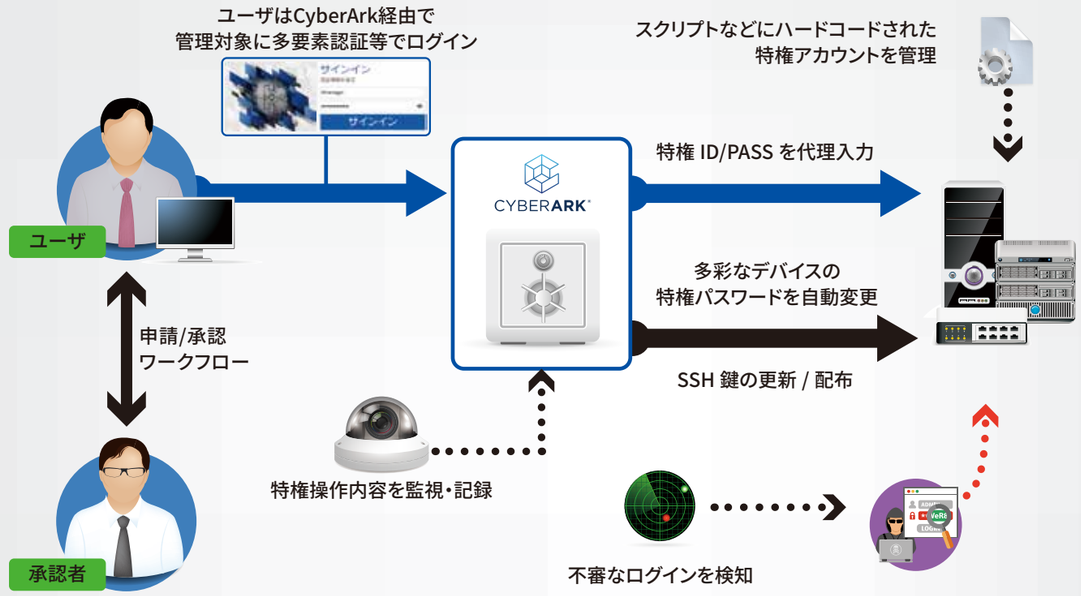
内部不正



問題：

- 個人ごとのアカウントを設定すると、維持管理に係る工数が増大する。
- 手動による管理ではアカウントの消し忘れなど、作業ミスが発生する。
- ログを取得できていないため、内部不正が発覚する可能性が低く、抑止効果が無い。
- 不要な権限を与えてしまうケースがある。

CyberArk 機能概要図



■主な機能

CyberArk PAM は特権アカウントの管理 / 保護に必要な機能を備え、お客様のシステムに存在する特権アカウントを強固に守ります。

- 特権アカウントのパスワード自動変更
- SSH 鍵の自動更新 / 配布
- 特権アカウントユーザの権限管理
- 特権利用のための承認ワークフロー
- レポートの自動作成 / 出力
- 対象システムへの接続の一元化
- 操作内容の動画 / テキストによる記録
- RDP/SSH だけでなく多様な管理に対応
- 不信な特権利用 / 操作の検知 / アラート
- ハードコートされた特権アカウントの管理