なぜ特権ID管理ツール「SecureCube Access Check」が選ばれるのか

特権ID管理の最新動向と「SecureCube Access Check」のご紹介

NRIセキュアテクノロジーズ株式会社
ソフトウェア第二事業本部
統制ソリューション事業部

特権ID管理の最新動向と「SecureCube Access Check」のご紹介

- はじめに
- 特権ID管理が求められる背景と最新動向
- 特権ID管理を効率的かつ効果的に実現するポイント
- 弊社ソリューションのご紹介と導入効果
- まとめ

特権ID管理の最新動向と「SecureCube Access Check」のご紹介

はじめに

特権ID管理が求められる背景と最新動向

特権ID管理を効率的かつ効果的に実現するポイント

弊社ソリューションのご紹介と導入効果

まとめ

会社概要

（2024年10月時点）

野村総合研究所（NRI）グループにおける情報セキュリティ専門の中核企業

社名	NRIセキュアテクノロジーズ株式会社（略称：NRIセキュア）		
会社所在地	本社：東京都千代田区大手町 東京サンケイビル 横浜ベイオフィス：神奈川県横浜市神奈川区 横浜ダイヤビルディング サイバーセキュリティハブ大阪：大阪府大阪市北区 中之島フェスティバルタワー・ウエスト 北米支社：米国カリフォルニア州アーバイン		
設立年月日	2000年8月1日　※サービス提供開始：1995年		
資本金	4.5億円		
株主	株式会社野村総合研究所		
取締役会長	大元 成和		
代表取締役社長	建脇 俊一		
専務取締役	池田 泰徳	常務取締役	西内 喜一
取締役	小林 賢治、武田 則幸、山口 隆夫、能勢 幸嗣	監査役	桧原 猛
NRIセキュアグループ会社	株式会社ユービーセキュア：東京都中央区 株式会社NDIAS：東京都港区		
提供実績	官公庁、金融機関、流通、製造、製薬、通信、マスコミ など		
認証取得	ISO/IEC 27001認証取得		

IS 75215 / ISO 27001

会社概要｜事業編成と提供サービス

社会やニーズの変化、技術動向に応じたサービス・製品を4つのコア事業で提供

戦略ITイノベーションと研究開発

戦略ITイノベーション　政策動向やマーケットニーズの洞察によるソリューション創発

研究開発センター　先進技術の探索・評価、およびサービス開発の推進・統括

4コア事業

コンサルティング

顧客密着型の問題解決支援

ストラテジーコンサルティング事業本部
マネジメントコンサルティング事業本部
サイバーコンサルティング事業本部

DXセキュリティ

デジタルトランスフォーメーション
をセキュリティで支援

DXセキュリティコンサルティング事業本部
DXセキュリティプラットフォーム事業本部

**マネージド
セキュリティサービス**

24時間365日の
セキュリティ監視サービス

マネージドセキュリティサービス事業本部
マネージドセキュリティサービス開発本部

ソフトウェア

日本市場に合わせた自社開発の
セキュリティソリューション

ソフトウェア第一事業本部
ソフトウェア第二事業本部

企業のセキュリティ対策をトータルで支援する
5つの提供サービスカテゴリ

コンサルティング	セキュリティ診断	SOC・マネージド セキュリティサービス	セキュリティ 製品・ソリューション	セキュリティ 教育・研修

会社概要｜主な提供サービス・製品一覧

（2024年10月時点）

コンサルティング

リスクアセスメント
- セキュリティ対策状況可視化
- グローバルセキュリティアセスメント
- ファストセキュリティアセスメント
- 工場ファストセキュリティアセスメント
- MITRE ATT&CKを用いたサイバー攻撃対策の評価
- 暗号鍵の設計・運用に関する評価支援
- 電子決済セキュリティリスク評価
- セキュリティ対策レポート
- セキュリティ監査
- CRI Profileを活用したサイバーセキュリティアセスメント
- クラウドセキュリティ評価
- サイバーセキュリティ経営ガイドライン対応支援
- ローコード/ノーコード開発基盤セキュリティ評価
- リスクベースアセスメント
- IMDRFガイダンスに基づいたセキュリティアセスメント
- AI品質・適合性検証
- サードパーティ・サイバーセキュリティ・デューデリジェンス
- ソフトウェアサプライチェーンセキュリティ（SSS）評価

リスクマネジメント
- セキュリティポリシー策定支援
- セキュリティガイドライン策定支援
- サプライチェーン・セキュリティコンサルティング
- クラウドセキュリティコンサルティング
- IoTセキュリティコンサルティング
- APIセキュリティコンサルティング
- プライバシーリスク評価・パーソナルデータ管理システム化検討支援
- AIリスクガバナンス構築支援
- 市民開発セキュリティガイドライン策定支援

脅威インテリジェンス
- マネージド脅威情報分析
- マネージドASM

法規制・ガイドライン準拠
- 産業用制御システム向けAchilles認証取得支援
- CIS Controlsによるサイバー攻撃対策の強化支援
- CIS Benchmarksを用いたシステム堅牢化支援
- NIST SP800-171準拠支援
- 医療情報ガイドライン準拠支援
- 半導体業界向けSEMIセキュリティ規格準拠支援
- 防衛産業サイバーセキュリティ基準準拠性評価
- SWIFT CSCFの準拠性評価

PCI準拠支援
- PCI DSS SAQ対応支援
- PCI DSS対策基準書
- PCI DSS / P2PE / 3DS / CP / PIN Security 準拠支援/審査
- PCI DSS準拠／維持支援スキャン
- 非保持化支援

プロジェクト実行支援
- セキュリティ対策支援
- セキュリティ対策構想策定・システム化計画作成支援
- セキュリティ対策推進PMO
- 中長期計画策定支援
- ゼロトラスト・コンサルティング

セキュリティ組織支援
- 組織内CSIRT総合支援
- 組織内PSIRT向け支援
- セキュリティ・カウンセリング
- CIO / CISO支援
- セキュリティ業務改革支援
- デバイス脆弱性監視分析
- SEC Team Services
- SBOM導入支援
- サイバーレジリエンス能力向上
- 経営層向けサイバーセキュリティ研修

設計開発支援
- DevSecOps実行支援
- セキュア設計・開発ガイドライン策定支援
- セキュアアプリケーション設計レビュー
- ソースコード診断
- デジタルサービス向けリスク分析支援

セキュリティ事故対応
- セキュリティ事故対応支援

セキュリティ訓練
- サイバー攻撃対応机上演習
- 工場向けセキュリティ教育・インシデント対応訓練プログラム
- 不審メール対応訓練
- レッドチームオペレーション
- ペネトレーションテスト

セキュリティ診断

セキュリティ診断
- Webアプリケーション診断
- プラットフォーム診断
- スマートフォンアプリケーション診断
- APIセキュリティ診断 / APIセキュリティ設計レビュー
- ブロックチェーン診断
- コンテナ診断
- エンドポイントセキュリティ診断
- クラウド設定評価
- AI Red Team
- AI Blue Team

IoT/OTセキュリティ診断
- OTネットワーク・アセスメント
- デバイス・セキュリティ診断

設計開発支援
- セキュア設計・開発ガイドライン
- セキュアアプリケーション設計レビュー
- ソースコード診断

サイバーアタックシミュレーション
- レッドチームオペレーション
- ペネトレーションテスト
- 不審メール対応訓練
- Mandiant Advantage Security Validation ペネトレーションテスト

SOC・マネージドセキュリティサービス

NeoSOC（セキュリティオペレーションセンター）
- セキュリティログ監視（共用SOC）
- SIEM監視

EDR・MDR（エンドポイント対策）
- マネージドEDR
- マネージドXDR powered by Cortex XDR from Palo Alto Networks
- マネージドEDR（Microsoft Defender for Endpoint）

OA・ワークプレイス環境 運用監視
- メールセキュリティ管理サービス(Proofpoint Email Protection)
- マネージドITDRサービス
- Zscaler Internet Access マネージドサービス
- Zscaler Private Access マネージドサービス
- Netskope Security Cloud管理
- CATO Cloud導入支援
- マネージドセキュリティ powered by Prisma Access from Palo Alto Networks
- Palo Alto PAシリーズ管理
- セキュアインターネット接続
- マネージドネットワークサービス

Web・アプリケーション 運用監視
- クラウド型WAF管理（Imperva Cloud WAF）
- WAF管理
- 統合クラウドセキュリティマネージドサービス powered by Prisma Cloud from Palo Alto Networks
- パブリッククラウドセキュリティマネージドサービス

OT/IoTセキュリティ監視
- マネージドNDR（Nozomi Networks for OT/IoT）

マネージドNWサービス
- 拠点WAN接続サービス
- SD-WAN接続サービス
- マルチクラウド接続サービス
- 高度運用監視サービス

セキュリティ製品・ソリューション

ID管理・認証
- Uni-ID Libra
- Uni-ID MFA
- SecureCube Access Check
- Cloud Auditor by Access Check
- Access Check Essential
- Okta
- YubiKey
- CrowdStrike Falcon Identity Protection
- ジョーシス
- Start In
- HashiCorp Vault

メール・Webセキュリティ
- m-FILTER MailAdviser
- Cofense
- Proofpoint
- Proofpoint Email Fraud Defense(EFD)
- DMARCレポート可視化

文書・ファイルセキュリティ
- クリプト便
- Box
- FinalCode
- Druva
- Contents Expert / XML Assist

エンドポイントセキュリティ
- PC Check Cloud
- Menlo Security
- マネージドEDR
- FFRI Yarai

クラウドセキュリティ管理
- Netskope
- Prisma Cloud
- Zscaler Internet Accessマネージドサービス
- Zscaler Private Accessマネージドサービス
- パブリッククラウドセキュリティマネージドサービス
- Adaptive Shield
- i-FILTER@Cloud

リスク分析・可視化
- Proofpoint ITM
- illumio
- Secure SketCH

脅威インテリジェンス
- IntSights
- Recorded Future
- GR360
- RiskIQ

脆弱性管理
- Contrast Security
- Vex
- VexCloud
- Qualys
- Fortify

IoT/OTセキュリティ
- Nozomi Networks
- SCADAfenceプラットフォーム
- 工場ファストセキュリティアセスメント

AIセキュリティ
- AI Blue Team

セキュリティ教育・研修

セキュリティ資格取得支援
- SANSトレーニング
- CISSP CBKトレーニング
- CCSP CBKトレーニング

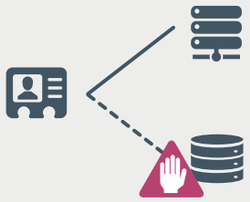
セキュリティ人材育成
- セキュアEggs

特権ID管理の最新動向と「SecureCube Access Check」のご紹介

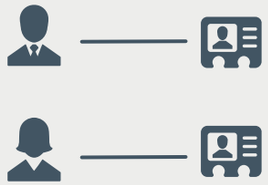
一般的なIDと特権IDの違い

- 「特権ID」とは、通常のユーザよりも特別な権限を有しているIDを指し、システムの起動や停止、設定変更やユーザ権限の管理などを行えるIDが該当

一般的なID

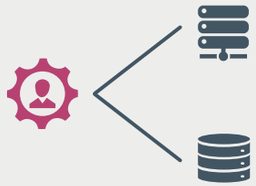


限定的な権限



個人ごとに1ID

特権ID



絶対的な権限

OSやデータベースなどにおいて高権限の特殊な操作（起動や停止）などが可能

システム障害

情報漏えい

データの改ざん・消去

不正行為が容易

1IDを共有

システムにビルトインされている特権IDは利便性が高いがゆえに複数のユーザで使いまわされるケースが多い

作業者が不明

作業内容が不明

検知が困難

管理するべき「特権ID」の多様化

昨今のクラウド利用拡大により、「特権ID」として管理するべき範囲が広がり、さらに権限最小化の原則に従うとその数は膨大になりつつある

従来の特権ID

WindowsやLinux等のサーバに存在する高権限ID
例）　Administrator, root

重要情報を含むデータベースへアクセス可能なID
例）　Oracle sys, SQL Server sa

ネットワーク機器等の設定・運用を行うためのID

DX時代における特権ID

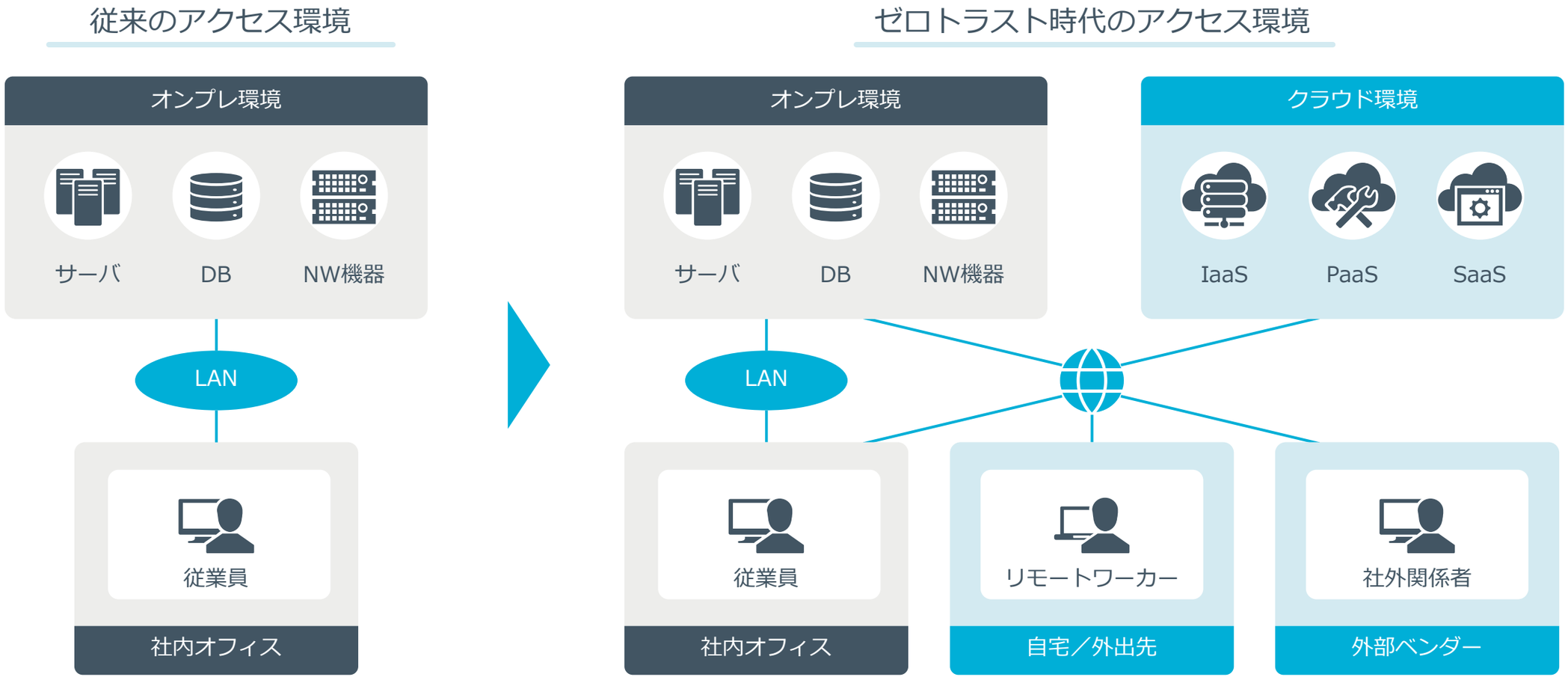
クラウド利用の機会が増え、IaaS、SaaSの管理が可能なアカウントや、その他業務上必要となるサービスの管理アカウントも 特権 として管理するべき

AWS、AzureなどのIaaS管理者アカウント
例）　AWS IAMアカウント

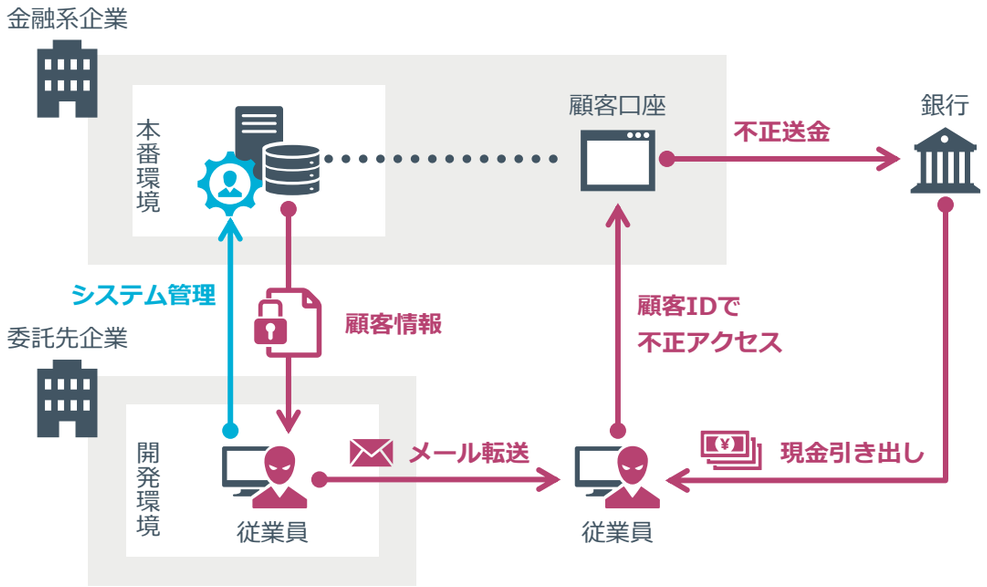
Microsoft365、SalesforceなどのSaaS管理者アカウント
例）　Microsoft365 管理者アカウント
　　Salesforce システム管理者

アクセス環境の多様化

- テレワークの普及により、自宅や外出先からのアクセスや外部ベンダーからのリモートアクセスが増加
- 従来の境界型防御からゼロトラストへ変化する中で、アクセス管理・ID管理の重要性はますます高まる

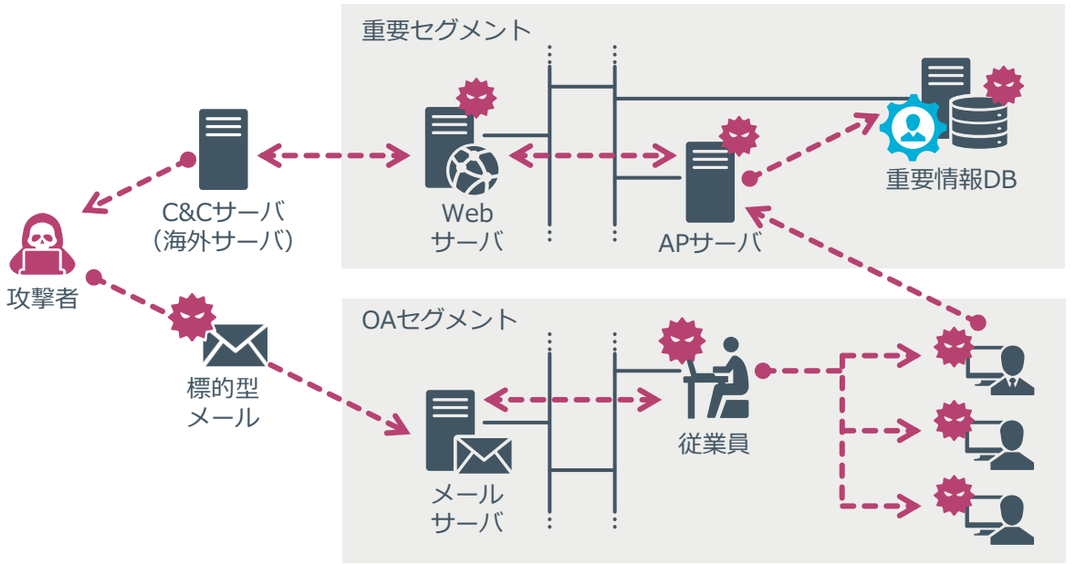


特権IDの不適切な管理による不正利用の例



特権の濫用の例

委託先の大手SIer企業の従業員がシステム管理に利用する
特権IDを悪用して顧客情報を不正取得し、その情報を利用して
個人の口座に不正送金、現金を引き出した事件。



特権の奪取の例

内部犯行だけでなく標的型攻撃においても内部ネットワークへの
侵入が成功すると、辞書攻撃などの手段で**特権の搾取**を試みる。
特権が搾取されることで被害は甚大に。

特権ID管理の最新動向と「SecureCube Access Check」のご紹介

はじめに

特権ID管理が求められる背景と最新動向

特権ID管理を効率的かつ効果的に実現するポイント

弊社ソリューションのご紹介と導入効果

まとめ

特権ID管理の基本の4ステップ

特権ID管理の基本は、次の4STEPを一貫性をもって実施すること

IT全般統制、PCI DSS、金融庁監査などのガイドラインで求められる特権ID管理は、粒の細かさや表現などは異なりますが、共通して言えることは4STEPにまとめられます。

Step1

利用者の特定

特権IDを利用する人は
「**誰か**」を特定する

Step2

申請と承認
アクセス制御

特権IDを「**いつ**」「**何のために**」
利用するのか明確にした
申請を行い、承認を受ける

Step3

作業の記録

特権IDを利用した作業として
「**いつ**」「**誰が**」「**何をしたか**」
を記録する

Step4

妥当性の確認

申請の内容と作業の記録を
突合せて「**申請通りの内容で**
作業を行ったか」を確認する

個人の特定・認証と認可による**予防的統制**

作業の記録とモニタリングによる**発見的統制**

特権IDの管理を手運用で対応した場合に直面する課題

特権ID管理ソリューションを利用せずに手運用で対応した場合、以下のような課題に直面

利用者の特定

- 特権IDを共有しているため、何かあっても利用者の把握や特定ができない

申請・承認
アクセス制御

- システム化されていない （紙運用やExcel運用）ため、運用工数がかかる
- 申請、承認と利用制御がシステム的に紐づいておらず、ルール通りの運用を徹底できない

作業の記録

- ログの保管場所がばらばらのため、確認するのが大変

妥当性の確認

- 申請と対象のログを突合する必要がある。
- 見るべきログを判断するための情報がないため、全件確認するしかない

特権ID管理ソリューション導入による効果

特権ID管理ソリューション導入により、これらの課題は全て解決可能

利用者の特定

- 特権IDを共有しているため、何かあっても利用者の把握や特定ができない
  - → **特権ID管理ソリューションの認証機能で個人特定が可能となる**

申請・承認
アクセス制御

- システム化されていない （紙運用やExcel運用）ため、運用工数がかかる
  - → **システム化により工数を大幅削減**
- 申請、承認と利用制御がシステム的に紐づいておらず、ルール通りの運用を徹底できない
  - → **システム化され、ポリシー違反のアクセスはブロックされる**

作業の記録

- ログの保管場所がばらばらのため、確認するのが大変
  - → **一つの場所に集約されるため、確認が容易になる**

妥当性の確認

- 申請と対象のログを突合する必要がある。
  - → **申請に紐づく形でログが保存されるため、自動で突合可能**
- 見るべきログを判断するための情報がないため、全件確認するしかない
  - → **検知機能やレポート機能を活用することで、重点的にみるべきログを判別可能**

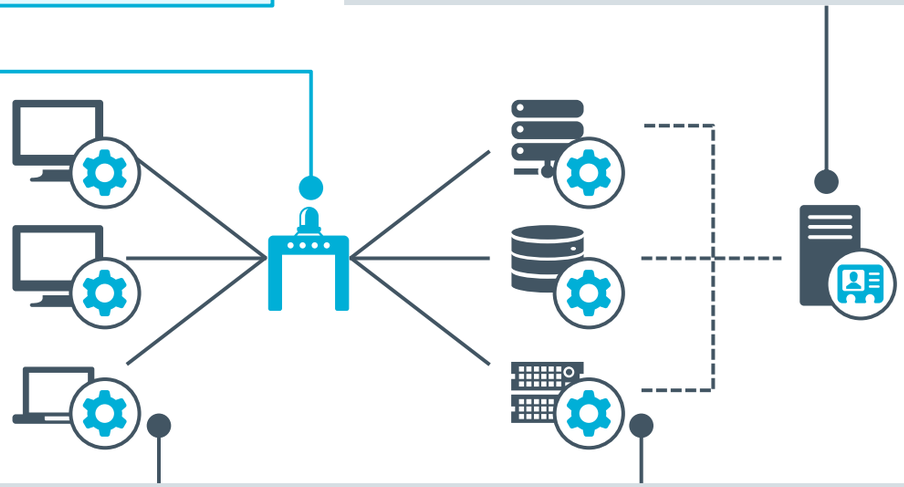
特権ID管理ソリューションの代表的な制御方式

ゲートウェイ方式（完全エージェントレス型）

クライアント端末と管理対象機器の間に関所（ゲートウェイ）を設置して、一元管理する方式。関所上で、個人ID管理、アクセス制御、及びログ管理を統合するため構成がシンプル。**管理対象機器が多い場合や、既存環境への影響を最小限にしたい場合**などに最適。

ID・パスワード貸出方式

管理対象機器の特権ID棚卸とパスワード貸出管理で制御する方式。
アクセス制御用にクライアントエージェントを必要としたり、認証用サーバを別途立てたりする必要がある。**特権IDが少ない場合や、統合ID管理システムが稼動済みの場合**などに最適。



エージェント方式

クライアント・エージェント型

アクセス元のクライアント端末ごとにエージェントをインストールする方式。
クライアントごとで、本人認証（特権ID利用者の特定）とログ取得を行う。**ログを詳細に取得したい場合や、管理対象機器への接続用端末が特定されている場合**などに最適。

サーバ・エージェント型

アクセス先の管理対象機器ごとにエージェントをインストールする方式。
管理対象機器ごとに個人ID管理、操作制御、ログ取得を行う。**物理コンソールでの接続を含めたアクセス制御とログを取得したい場合や、管理対象機器側で詳細な操作制御を行いたい場合**に最適。

ゲートウェイ方式は導入や運用面で優位

比較項目	システム導入	システム運用	アクセス制御	ログ取得
おすすめ **ゲートウェイ方式**	◎ エージェントレスのため導入が容易	◎ 拡張性に優れ、システム構成がシンプルなため運用が容易	○ ゲートウェイでアクセス制御可能、迂回アクセス対策が必要※1	○ エージェントレスで取得可能 迂回アクセス対策が必要※1
サーバ・エージェント型	△ 各サーバへの導入影響がないか調査・検証が必須	△ メンテナンスごとに影響の調査・検証が必須	◎ ローカルログインを含めたきめ細かい制御が可能	◎ ローカルログインを含めたログの取得が可能
クライアント・エージェント型	○ 各クライアントへの導入影響がないか調査・検証が必須※2	△ アクセス制御とログ取得は別製品が必要となり、運用が煩雑	○ エージェント未導入の端末からのアクセス対策が必要	○ エージェント未導入の端末からのアクセスログは取得できない
ID棚卸・貸出方式	△ ID・パスワードの棚卸が必須 パスワード変更できないIDは別対策が必要	○ ID・パスワードの管理（定期棚卸など）が必須、パスワード変更できないIDは別管理	○ パスワード変更できないIDの対策が必要	△ ID貸出・利用のログは取得できるが、操作内容の取得のためには別の仕組みが必要

※1　ネットワーク機器で制限する、特権パスワードを秘匿化する、管理対象機器のログと突合する　等の対策が考えられます。
※2　Windows Terminal Serverを用意し、そこにクライアントエージェントを導入することで導入を簡素化するケースがあります。

特権ID管理の最新動向と「SecureCube Access Check」のご紹介

はじめに

特権ID管理が求められる背景と最新動向

特権ID管理を効率的かつ効果的に実現するポイント

弊社ソリューションのご紹介と導入効果

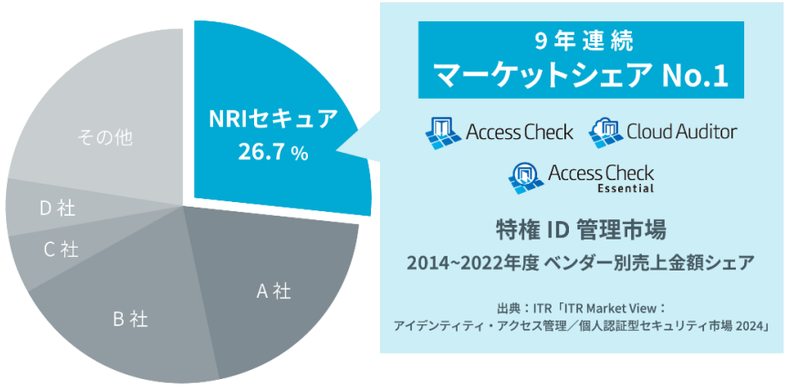
まとめ

SecureCube Access Checkとは

※ ITR「ITR Market View：アイデンティティ・アクセス管理／個人認証型セキュリティ市場2024」特権ID管理市場ベンダー別売上金額シェア（2022年度） SecureCube Access Check, Access Check Essential, Cloud Auditor by Access Check が対象

SecureCube Access Check

NRIセキュアが開発した、安全性の高いゲートウェイ型の特権ID管理ソリューション。
エージェントレスのため、既存環境への影響を最小限に導入することが可能。



様々な業種のお客様の課題を解決

IIJ Internet Initiative Japan / ONE COMPATH / TOWER RECORDS / JEOL
出光 / TOKYU CARD / KDDI Tomorrow. Together / SoftBank
ベネッセコーポレーション / 株式会社東計電算

一部抜粋・順不同

販売代理店

TIS TIS INTEC Group / CTC / Marubeni IT Solutions / Hewlett Packard Enterprise
IIJ Internet Initiative Japan / Computer Science Corporation / GRCS

一部抜粋・順不同

特権ID管理ソリューション SecureCube Access Check の3つの特長

- SecureCube Access Checkは、NRIセキュアが金融機関のシステム保守業務のために開発した、安全性の高いゲートウェイ型の特権ID管理ソリューション
- 下記の3つの特長があるほか、専門エンジニアによるきめ細やかな保守サポートも好評

※ 出典：ITR「ITR Market View：アイデンティティ・アクセス管理／個人認証型セキュリティ市場2024」特権ID管理市場：ベンダー別売上金額シェア（2022年度）
SecureCube Access Check, Access Check Essential, Cloud Auditor by Access Check が対象

ゲートウェイ型だから導入・運用が容易

- 端末や管理対象機器へ専用ソフトを入れることがないため、導入の影響を最小限にして導入可能
- 厳密な運用設計を行わず、まずはログ取得のみで配置するなど、スモールスタートも用意

完全エージェントレスで
既存システムへの
影響を最小に

ゲートウェイを介さない直接ログインに対しては
ID・パスワード管理（PPM）機能で制御可能。

制約条件が少なく多様な環境での利用が可能

- エージェントレスのため、いつも利用している作業クライアントツールをそのまま利用可能
- 管理対象はサーバだけでなく、ネットワーク機器やクラウドサービスなど幅広く対応
- 10種類のプロトコルをサポートし、ファイル転送プロトコルにも対応

作業クライアントに縛られない

ツールなどに縛られず
すべての作業を対象可能に

クラウドにも対応

ネットワーク環境の変化に応じた
柔軟な対応が可能

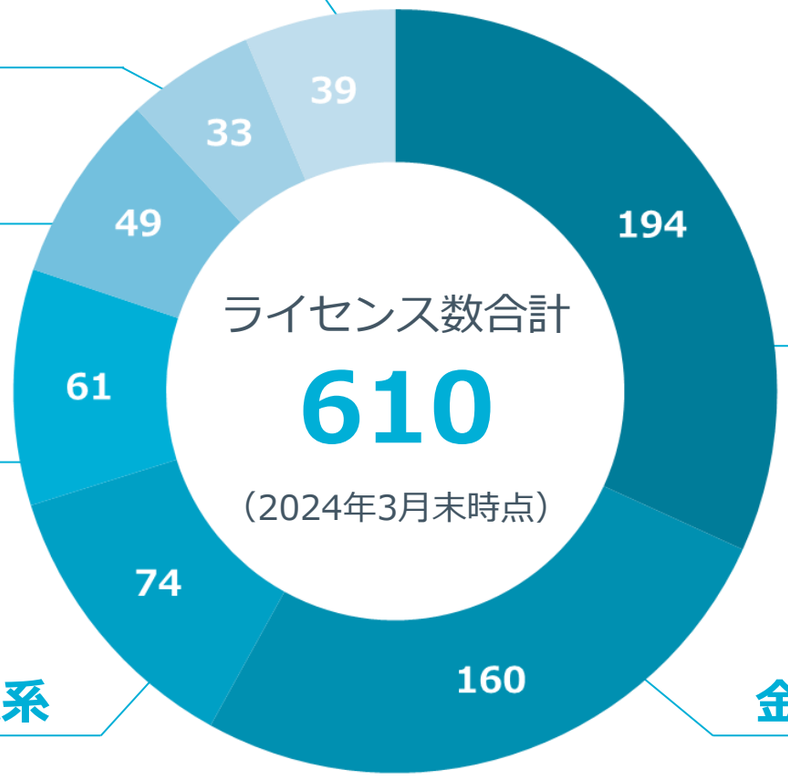
✔RDP ✔Telnet ✔SSH
✔FTP ✔SFTP ✔SCP ✔CIFS
✔HTTP(S) ✔TNS ✔TCP

多くのプロトコルに対応

ファイル転送プロトコルを含む
10種類のプロトコルに対応

多くの企業・組織に支持され市場シェアNo.1※の導入実績

- 上場企業を中心に、業種を問わず、全国610ライセンスの導入実績を誇る
- 特に高いセキュリティを求められる金融の大手証券・保険・銀行などでも採用



情報・IT系
情報処理サービス、
ITコンサル、通信事業　等

金融系
生命保険、損害保険、銀行、
信用金庫、証券、クレジットカード業　等

流通系
運輸、卸売業、百貨店、専門店、
小売スーパー、コンビニエンスストア　等

製造系
石油化学製品製造、製薬、機器製造、
食品製造、ガス・エネルギー　等

サービス系
航空業、旅行業、
教育関連事業　等

公共機関
協会、団体、
特殊法人、官公庁　等

その他
放送、広告、新聞、印刷、
出版、不動産、病院　等

※ 出典：ITR「ITR Market View：アイデンティティ・アクセス管理／個人認証型セキュリティ市場2024」特権ID管理市場：ベンダー別売上金額シェア（2022年度）
SecureCube Access Check, Access Check Essential, Cloud Auditor by Access Check が対象

特権ID管理の業務フロー全体をカバーする5つの機能

特権ID管理のすべての課題を解決するオールインワンソリューション

特権利用前 | 特権利用時 | 特権利用後

ID・パスワード管理

特権IDのパスワード自動更新や有効期限設定ができるほか、ID情報を収集しCSV出力することが可能です。

ワークフロー

申請・承認フローを電子化。事後承認や多段階承認にも対応。既存のワークフローシステムとの連携APIも提供。

アクセス制御

予めアクセスできるサーバやプロトコル等をポリシーとして登録。申請時に選択したポリシーや作業時間に従って制御を実行します。

ログ管理

作業の操作内容は記録され、申請と自動的に突合せされます。閲覧権限のある監査者のみ検索・閲覧できます。

監査補助

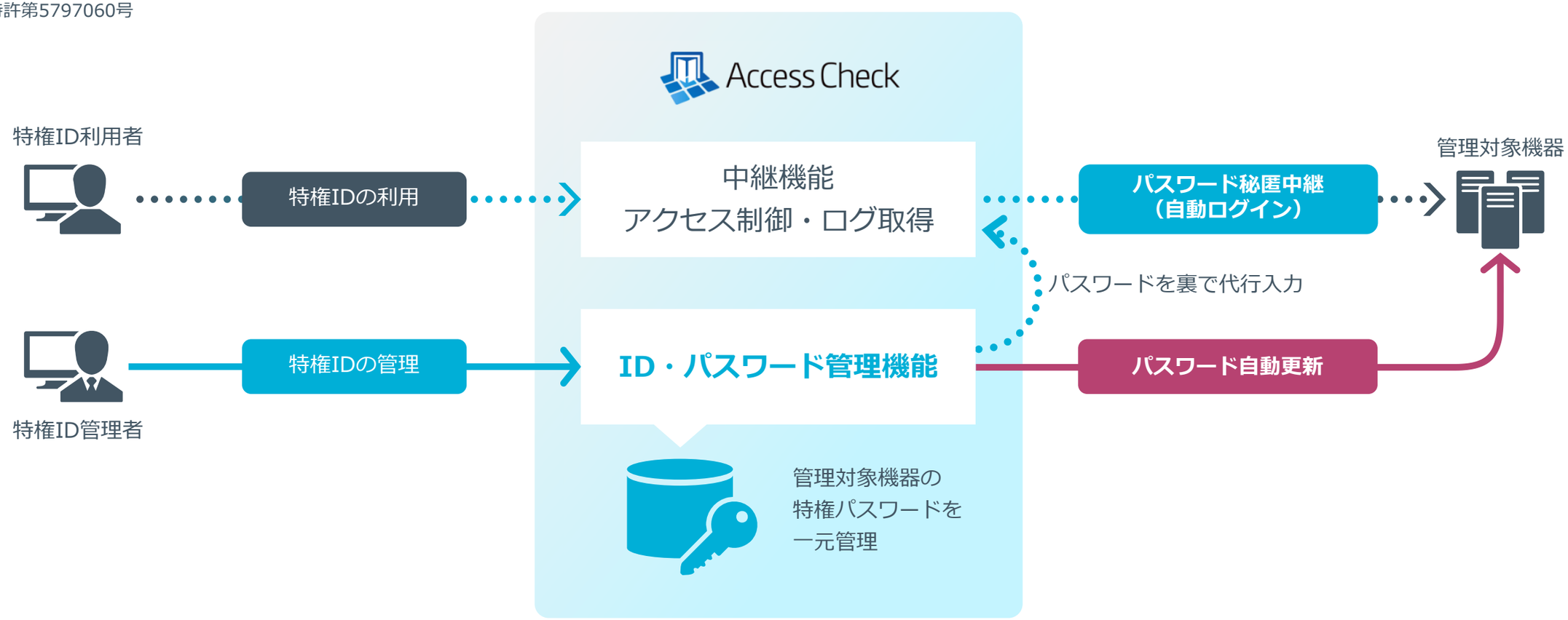
定期レポート出力の他、危険コマンドの発行通知や、申請外持ち出しファイルの検出機能などを提供。

ID・パスワード管理

- **特権IDのパスワード自動更新や有効期限設定などのPPM機能※1やパスワード払い出し機能を搭載**
- **NRIセキュア独自の特許技術※2で特権パスワードを開示せずに、許可された接続先へ自動ログイン可能**

※1　PPM（Privileged Password Management）機能：特権IDのパスワードを変更するなどの管理機能

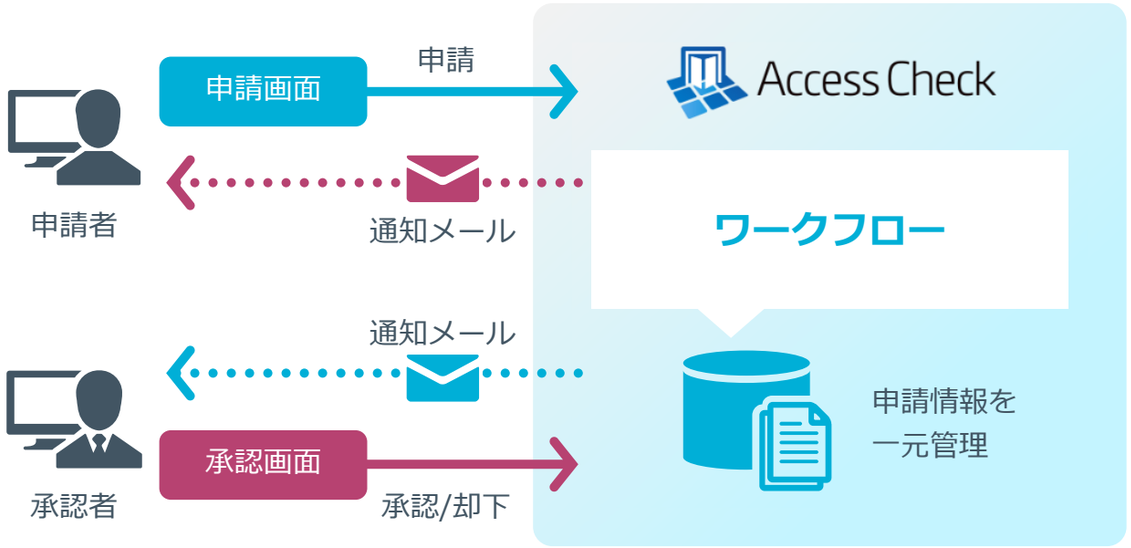
※2　特許第5797060号



ワークフロー

- **特権ID利用における申請から承認までのプロセスをシステム化することで、管理負荷を大幅削減**
- **多段承認や多段グループ承認、事後承認など、自社のルールに合わせた設定が可能※**

※　ServiceNowと申請情報を連携することで、申請内容をさらに細かく設定することも可能です。（Access Check Integrationオプションが必要）



多段承認

指定された承認者が順に承認を行い、承認者全員が承認して初めて「承認済み」となります。

多段グループ承認

指定された各段階の承認者グループの中で一人が順番に承認を行い、すべての段階で承認されて「承認済み」となります。

事後承認

緊急時など、事前に承認者による承認が難しい場合、承認前に作業が可能です。その場合「事後承認」となります。

パスワード払出申請

申請と承認を行うことで、作業者が、作業時に利用する特権IDのパスワードを一時的に参照することが可能です。

テンプレート

よく実施する作業は、申請内容をテンプレートとして保存することが可能です。

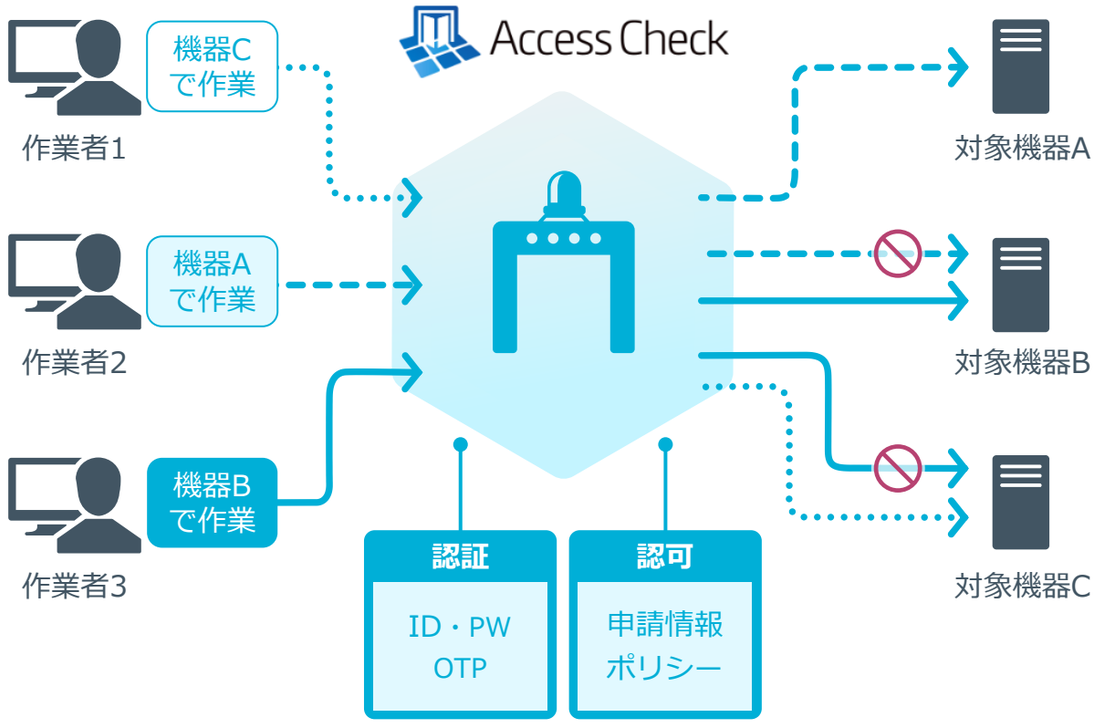
完了報告

作業後、申請内容に対して完了報告（テキスト）を入力することが可能です。

アクセス制御

ID・パスワードとワンタイムパスワード※などによる「認証」と、申請情報あるいはポリシー設定に基づく「認可」によって、管理対象機器へのアクセス可否を判断

※　ワンタイムパスワードを利用した多要素認証には、「高度認証オプション」が必要です。



多要素認証

高度認証オプションを用いることで、SecureCube Access Checkにおける個人認証にワンタイムパスワード（OTP）が必須となります。

New 中継接続許可

中継開始時に、作業者単独では接続できず、別の担当者（再鑑者）による接続許可をもって接続可能になります。

パスワード秘匿中継

中継時に特権パスワードを裏で代行入力して自動ログインさせることで、作業者に特権パスワードを伝える必要がありません。

New 自動特権昇格

SSH中継を利用する際、管理対象機器へ一般ユーザでのログイン後、パスワード入力なしに自動的に特権昇格することが可能です。

アクセス通知

アクセスの開始時、および終了時に、しかるべき承認者へアクセス通知のメールが送信されます。

申請時間超過による強制切断

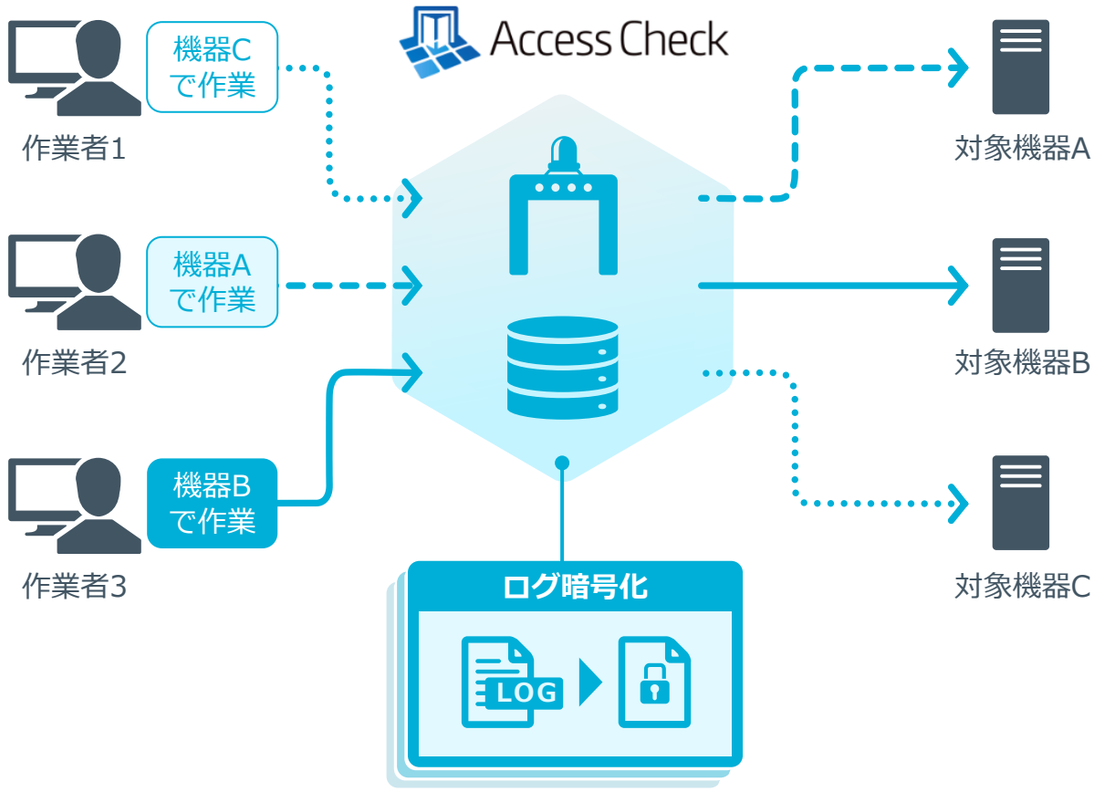
申請時に指定した終了予定時刻を超えると、中継の通信を強制的に切断します。切断しない設定にすることも可能です。

リアルタイムキーワード検知

あらかじめ指定したコマンド（キーワード）が作業中に確認された場合、リアルタイムに通信を遮断することが可能です。

ログ管理

- SecureCube Access Checkを経由したすべての操作が、アクセスログ、操作ログとして取得される
- 取得されたログは暗号化され、ポリシーに紐づく監査者のみが参照できるため内部統制の証明として有効



アクセスログの内容

いつ、誰が、どの端末から、どのサーバへ、どのプロトコルで、どの申請に基づいてアクセスしたか、などのアクセス概要を記録。設定に関わらず、すべての接続で取得される。

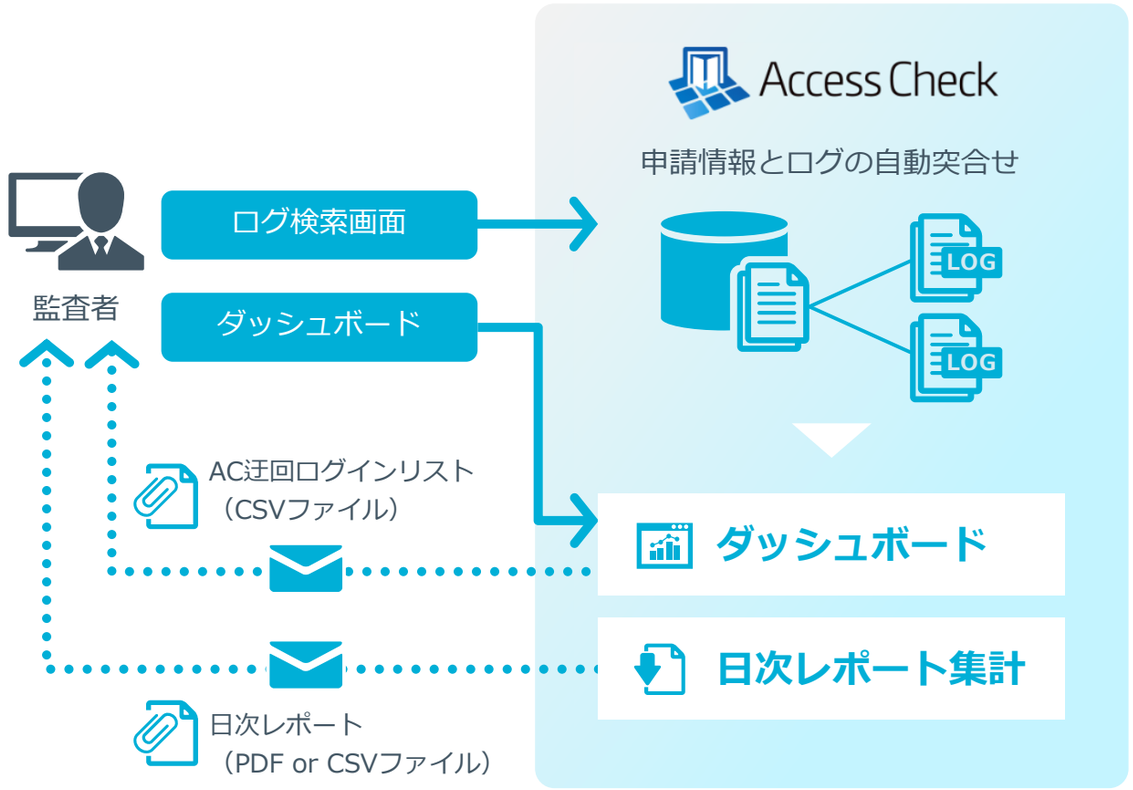
操作ログの内容

アクセス先サーバ／システムでどのような操作を行ったのか、またはどのようなファイルを転送したのか、などの実操作を記録したもの。操作ログの取得有無はポリシーごとに設定する。

プロトコル	操作ログ形式
RDP	リモートデスクトップ上で操作した動画ファイル、クリップボードの転送データ、およびキーボード情報（テキスト）
Telnet / SSH	ターミナルに表示された文字列を記録したテキスト
FTP / SFTP / SCP / CIFS	実際に転送したファイルデータ、およびコマンド（テキスト）
TNS	リクエスト情報（テキスト）
HTTP / HTTPS	リクエスト情報、およびレスポンス情報（テキスト）

監査補助

- 申請情報と実際のアクセスログ、操作ログが紐づけられた状態で記録されているため監査が容易
- 日次レポートやダッシュボードによる集計で、監査業務を支援する機能も標準搭載



日次レポート

- アクセスログ一覧
- アクセス申請一覧
- パスワード払出ログ一覧
- アクセス申請機能による規制履歴
- アクセス申請時間超過アクセス履歴

ダッシュボード

- 接続ノードへのAC迂回ログインリスト
- ログイン失敗総数の推移
- 普段とは異なるIPアドレスからの中継リスト
- 夜間・休日などの利用ユーザリスト　他

各種検知機能

不正操作の早期発見や、ログモニタリングの観点として活用いただけます。

- Access Check迂回ログイン検知
- 要注意キーワード検知
- 不正持ち出しファイル検出
- 重要情報検知（オプション）

確認機能

申請内容と関連するアクセスログを照らし合わせて、申請通りの操作であることが確認された場合に、参照している申請を「確認済み」の状態にします。目視で確認したことを明示的に記録できるため、監査状況を管理することができます。

主なオプション機能

高度認証

SecureCube Access Checkにログインする際にワンタイムパスワード(OTP)の入力を必須化することで、PCIDSS準拠する強固な高度認証を実現します。

※RSA SecureIDを利用する場合、RSA認証サーバが必要です。
※Amazon RDSと高度認証の併用は非サポートです。

AD連携

SecureCube Access Checkのユーザの認証に外部のActive Directoryサーバ、Azure AD DS、またはOpenLDAPのIDとパスワードを利用できます。

※AD連携した場合、CIFS中継は利用できません。

中継自動接続機能

中継接続を開始する際の、SecureCube Access Checkへのログイン、接続先の指定、接続先へのログインを自動で行うツールを利用できます。HTTP(S)のパスワード秘匿中継でも必要です。

動画変換専用サーバ追加

RDP中継で取得されるパケットファイルから動画ファイルへ変換処理を行う専用サーバを構築します。
複数の専用サーバを用意すると、1日に変換可能な時間の上限を増加可能です。

重要情報検知

操作ログを自動分析し、重要情報の持ち出しを検知した際に監査者へ通知します。
パスワード付ファイルなど分析ができなかった場合も、その旨を通知します。

AI動画ログ監査支援

AIを用いた物体検出技術を利用して、動画ログから予め設定された操作を検出し、レポート出力するツールを利用できます。

※ツールの利用には、別途専用サーバが必要です。

ServiceNow連携

servicenow

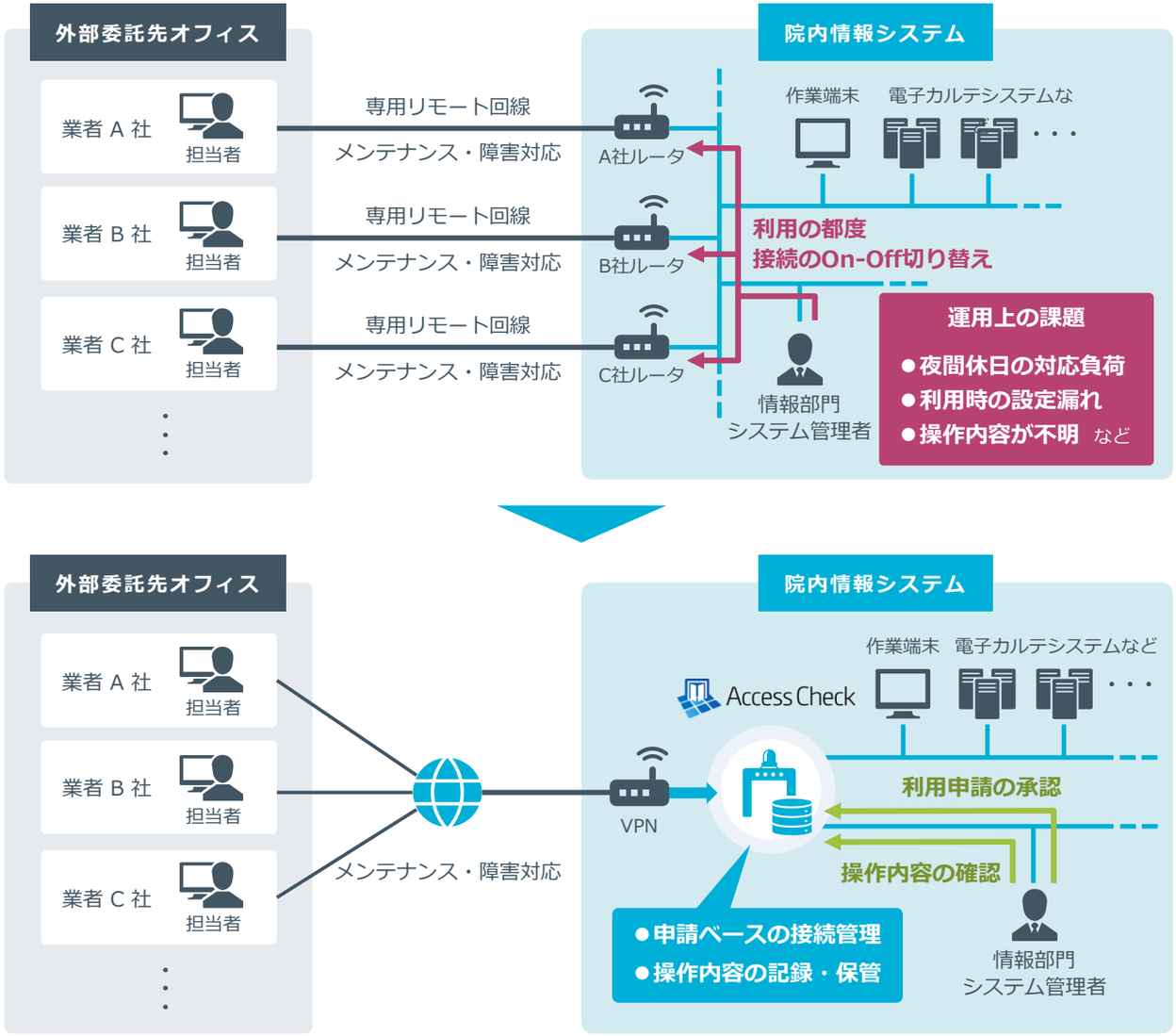
Access Check Integrationによって、特権IDを利用する作業のワークフローをServiceNow ITSMへ集約できます。
Credential Resolver by Access Checkによって、ITOM Discoveryで利用するクレデンシャル情報を安全に保管できます。

統合ログ管理連携

Logstorage

SecureCube Access Checkが記録するアクセスログと、管理対象機器で記録されたシステムログをLogstorage®上に収集して、横断的な検索、分析、レポートを実現します。

ケース1｜病院における活用例



導入目的

外部ベンダーによるリモート作業のアクセス制御

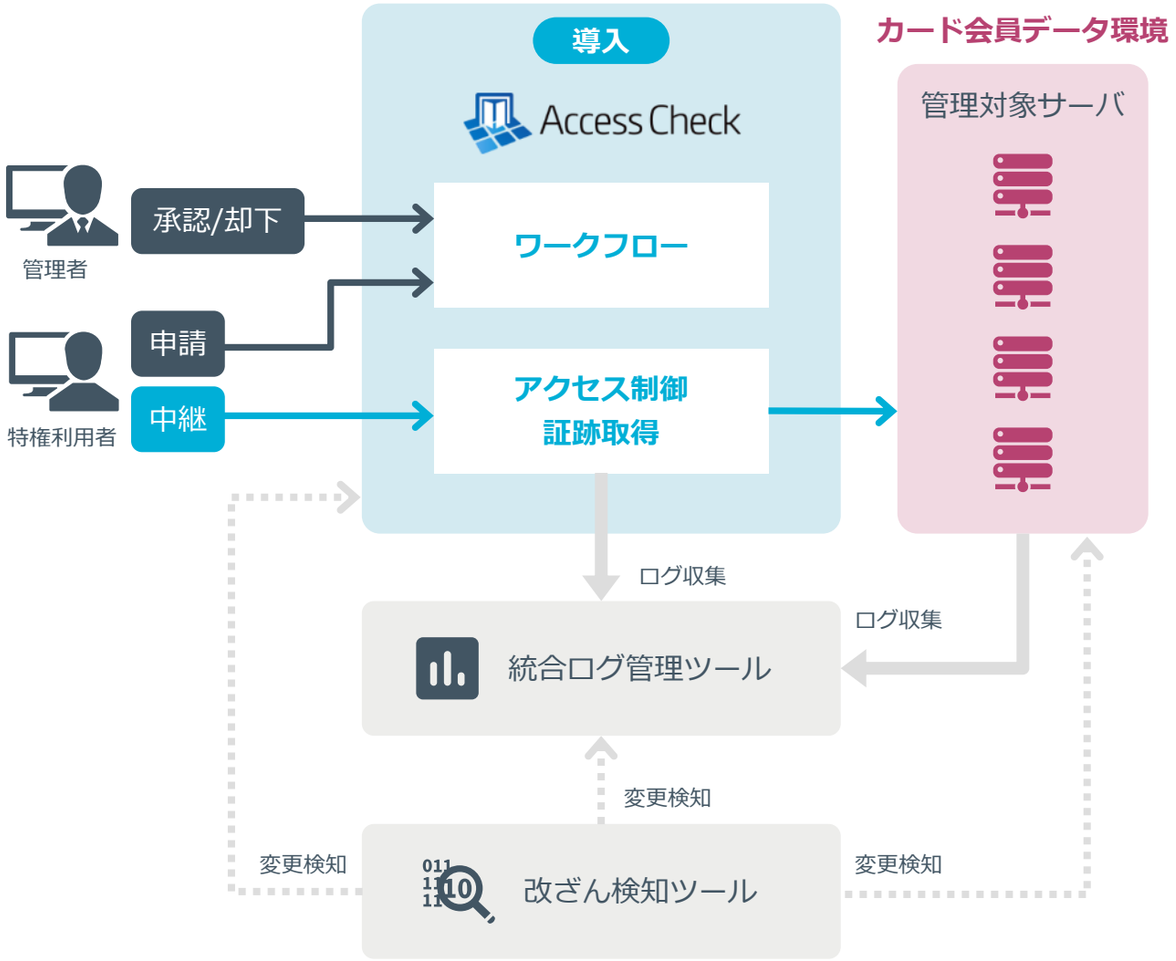
課　題

- ✓ 委託ベンダー専用のルータを、作業の都度、手動でOn-Off対応する管理負荷
- ✓ 緊急メンテナンス作業への対応が困難
- ✓ 作業の証跡は委託ベンダー依存

Point

- ベンダーごとのきめ細やかなアクセス制御を実現
- リモートメンテナンス回線の集約
- システム化による工数削減
- 作業証跡と申請内容の照合の効率化
- 個人情報持ち出しの検知

ケース2｜PCIDSSの求める強力なアクセス制御を実現



導入目的

業界に先駆けたPCIDSS準拠のための「強力なアクセス制御手法」の導入

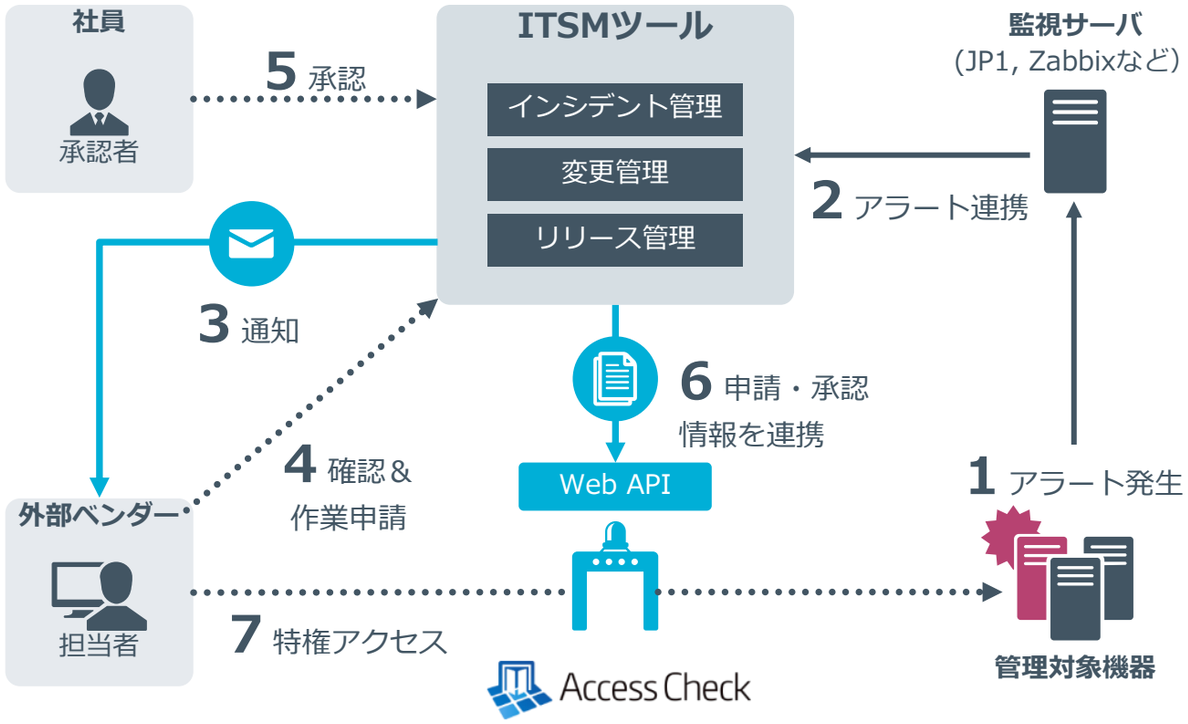
対応要件

- ✓ 要件7：最小権限・職務分掌、アクセス制御
- ✓ 要件8：個人認証（多要素認証）、ID棚卸
- ✓ 要件10：証跡取得・暗号化保存

Point

- カード決済セキュリティ全般に精通したNRIセキュアが開発提供する製品
- 他システムへの影響がないため、短期間で導入
- 厳格なアクセス制御の仕組みを確立し、組織全体のセキュリティ意識も大きく向上

ケース3｜ITSM連携による統制強化



導入目的

ワークフロー統合による運用効率化

対応要件

- ✓ アラート発生を起点にインシデント管理、特権アクセスの申請・承認ワークフローをITSMツール上で完結
- ✓ ITSMツールから行った特権アクセスのワークフローを特権ID管理ソリューションに自動連携

Point

- ワークフロー統合（複数システムに対して、類似の申請・承認作業が不要）による効果
- 運用(申請・承認作業)のコスト削減
- 申請・承認作業の形態化・確認漏れリスクの軽減

特権ID管理の最新動向と「SecureCube Access Check」のご紹介

- はじめに
- 特権ID管理が求められる背景と最新動向
- 特権ID管理を効率的かつ効果的に実現するポイント
- 弊社ソリューションのご紹介と導入効果
- **まとめ**

まとめ

1 クラウド活用の促進やテレワークの普及に伴い、特権ID管理はますます重要に

- 管理すべき特権IDの多様化により、管理の範囲は拡大
- アクセス環境の多様化により、統制レベルは厳格化

2 特権ID管理ソリューションの活用により、効率化・自動化を実現

- 手運用による対策では、セキュリティリスクが残り、運用負荷も高くなるため限界がある
- 変化するIT環境において、厳格な特権ID管理を実現するためには特権ID管理ソリューションが不可欠

3 SecureCube Access Checkは既存環境への影響が少ないゲートウェイ方式。オプションも充実しているため、求める統制レベルに応じて最適な構成を選択可能

- ゲートウェイ方式はエージェントレスのため、導入や運用に優れている
- 顧客要望を反映した独自機能でセキュリティ・利便性を向上

NRI SECURE