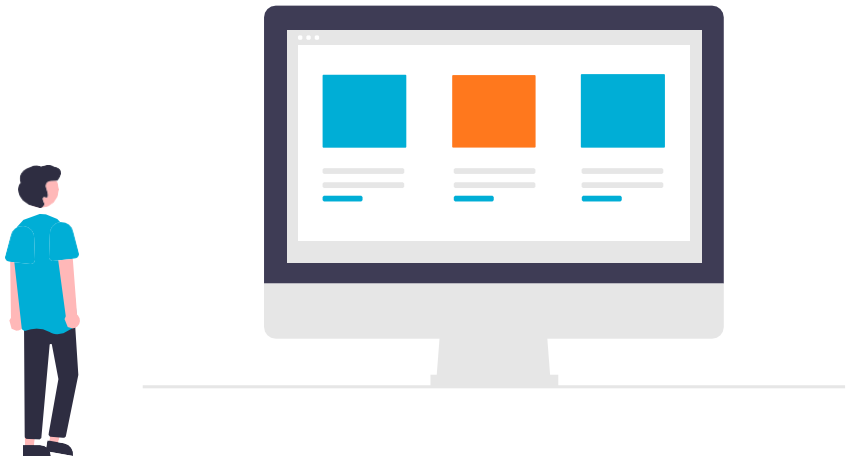
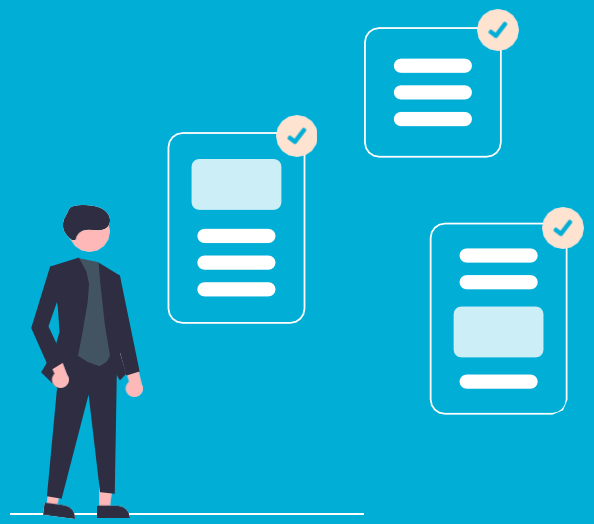
NRI SECURE



特権ID管理ツールを検討するときに確認するべき50のチェックリスト

NRIセキュアテクノロジーズ株式会社

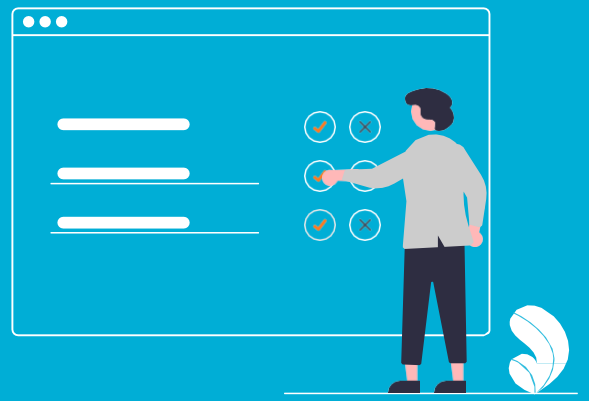


はじめに

セキュリティリスクが高まる昨今、システム運用や重要なデータの管理権限を持つ「特権ID」をより厳格に管理する必要性が高まっています。一方で、テレワークを始めとした多様な働き方が広がる中で、安全性に加え、運用効率の高い仕組みが求められるようになっています。

「特権ID管理ツール」を導入することで、機密データの漏えいや改ざんなど、不正アクセスのリスクを軽減することができ、より効率的・効果的な運用が可能となります。
現在では、さまざまな特権ID管理ツールが販売されており、各ツールによって実現できることに違いがあります。自社に適した製品を選ぶためには、まず比較するべき項目を挙げることが必要です。

そこで本資料では、特権ID管理ツールを導入する際に検討しておきたい要点を網羅的にチェックリスト形式でまとめました。自社の特権ID管理要件をまとめる、あるいは、複数のツールを比較する際に本チェックリストが参考になれば幸いです。



目次

特権ID管理ツールの基本ステップと機能

01

特権IDは一般的なIDとは異なり、**システムの変更や重要なデータへのアクセス権限**を持ちます。そのため、権限付与から作業内容の確認までを厳密に管理することが欠かせません。そこで有効な手段となるのが**特権ID管理ツールの導入**です。

ツールによって搭載する機能や実現できることは異なりますが、導入する目的を明確にしたうえで、ツールの基本的な仕組みや役割を理解して選定することが重要です。まずは、適切な特権ID管理を実現するために必要となる、基本的な要素からみていきましょう。

特権ID管理の基本の4ステップ

特権ID管理の基本的なプロセスは次の4つのステップで構成されます。
「利用者の特定」「申請と承認」は、利用者を特定することでリスクを抑制する予防的統制の観点、**「作業の記録」「妥当性の確認」**は素早い把握と監査につながる発見的統制の観点を基にしています。

Step1

利用者の特定

特権IDは利用者間で共有して使用することがあるIDです。まずは**特権IDを利用しようとしている利用者が「誰なのか」を特定**します。

Step2

申請と承認

特権IDを「いつ」使うのか、「何のために」使うのかなど、利用する目的を明確にし、申請と承認のプロセスを行います。

Step3

作業の記録

特権IDを用いた作業内容を記録しておきます。**「いつ」「誰が」「何をしたか」を確認できる内容を履歴として残します。**

Step4

妥当性の確認

申請時の内容と作業の記録を突き合わせて**「申請通りの内容で作業を行ったかどうか」を確認し、その整合性を検証**します。

「特権ID」を適切に管理することは、セキュリティを高める上で非常に重要です。
システム管理者に求められる特権ID管理について、より詳しくは下記ページより資料をダウンロードしてご覧ください。

新任システム管理者のための特権ID管理入門書

特権ID管理ツールの5つの基本機能

特権ID管理は厳格な管理が必要になるため、ワークフローの管理から監査までの工数が多くなります。その解決には、下記の主要な5つの基本機能を効率よく実施できる特権ID管理ツールの活用が有効です。

機能1：特権ID管理

特権IDのパスワードの自動変更や有効期限設定などのPPM機能※、ID情報の収集と出力といった管理機能です。

※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

機能2：ワークフロー

特権ID利用時の申請から承認までのプロセスをシステム化することで、担当者の業務負担を軽減します。事後承認や多段階承認にも対応していることが理想です。

機能3：アクセス制御

申請の承認状況に応じて、アクセス制御を行います。製品によっては、ユーザがアクセスできるサーバや利用可能なプロトコルなどをポリシーとしてあらかじめ登録して、ポリシーに基づくアクセス制御も可能です。

機能4：ログ取得･管理

特権ID利用時の作業内容を記録し、申請時の作業内容と突き合わせます。ログの閲覧権限の設定、保存時の暗号化などにも対応していることが理想です。

機能5：監査支援

定期レポートの出力、危険コマンドの発行通知、申請外の持ち出しファイルの検出などによって、監査や内部統制の業務を支援します。

特権ID管理ツール導入の前に確認すべきチェックリスト 02

さまざまな特権ID管理ツールが販売されていますが、先述の5つの基本機能だけでも実現方法は各特権ID管理ツールによって違いがあるため、自社に適した製品を選択するためには詳細な要件の検討が欠かせません。
以降では5つの機能とその他の機能、非機能要件に分類して、確認すべきチェック項目を紹介します。全ての項目が必須というわけではなく、自社に適した特権ID管理ツールを選択する際にどの項目が必須か、または、あると望ましいか、もしくは不要かを考慮しながら参考にしてみてください。

チェック項目1　特権ID管理

管理したい特権ID・管理者アカウントに対応している

特権ID管理ツールによって管理・制御できるOSやサービスは異なります。まずは自社の管理対象となるOSやシステム、サービスを漏れなくカバーできるかどうかを確認します。

特権パスワードの自動定期変更が可能

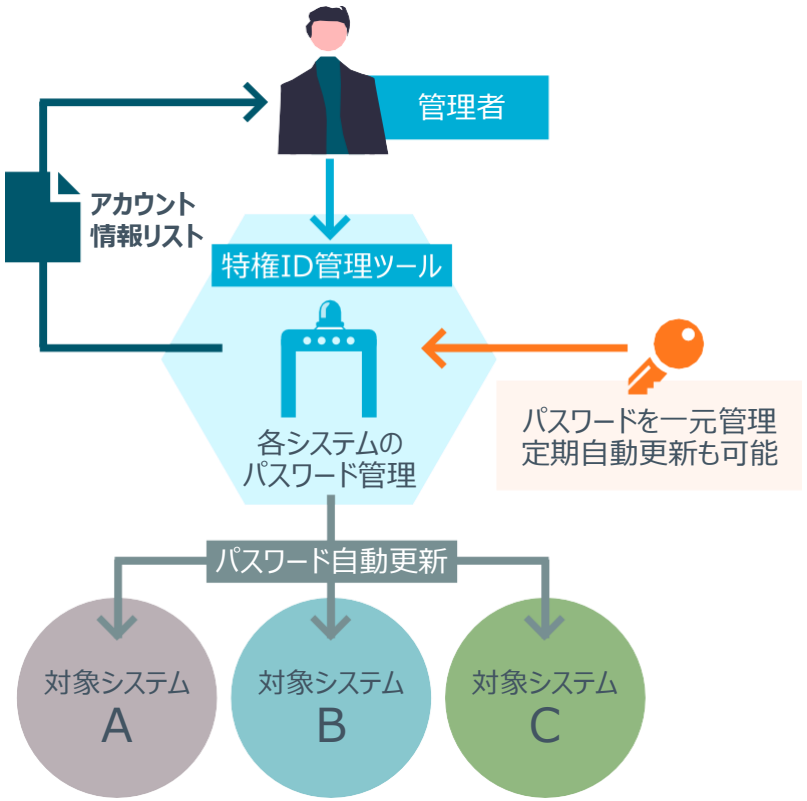
不正な利用を防止する上では、パスワードを定期的に変更することが重要となります。運用負荷の軽減や安全性の向上のためには、パスワードの自動更新機能を備えていることが望まれます。

特権パスワードは暗号化されて保存される

特権ID管理ツール上でパスワードを管理する場合には、そのパスワードが安全に保管できるか確認します。

パスワード変更できない特権IDの管理もできる

特権IDの特性によっては定期的なパスワード変更ができないケースもあります。その場合は、外部へのパスワード漏えいを防ぎ、セキュアに特権ID・パスワードを管理できる機能を備えていることが重要となります。



チェック項目2　ワークフロー①

- [ ] **細かい作業時間の設定が可能**

  不正な利用を防ぐためには、特権ID利用時の作業時間を細かく設定できるかどうかが重要です。申請する負荷を軽減する上では、定期申請ができることも重要な検討事項となります。

- [ ] **利用する特権IDを絞って申請できる**

  管理対象のシステムに応じて複数の特権IDを管理する場合は、利用する特権IDを限定する絞り込みの機能があるかどうかも重要です。また、そもそも利用を許可されていない特権IDは申請時に表示させないことも必要となります。

- [ ] **代理申請が可能**

  異なる組織の利用者に対する権限付与や緊急時対応などが必要になる場合、特権IDの利用を代理申請する機能があると役立ちます。

- [ ] **複数人での作業を一度に申請できる**

  一人の利用者ではなく複数の利用者が同時に特権IDを必要とするケースも考えられます。その場合、複数人数分をまとめて申請できる機能があると負荷軽減につながります。

- [ ] **過去の申請を再利用できる**

  過去の申請から必要な情報を書き換える形で新たな申請を作成することで、申請時の入力負荷を下げることが可能です。

チェック項目2　ワークフロー②

自己承認を制御できる

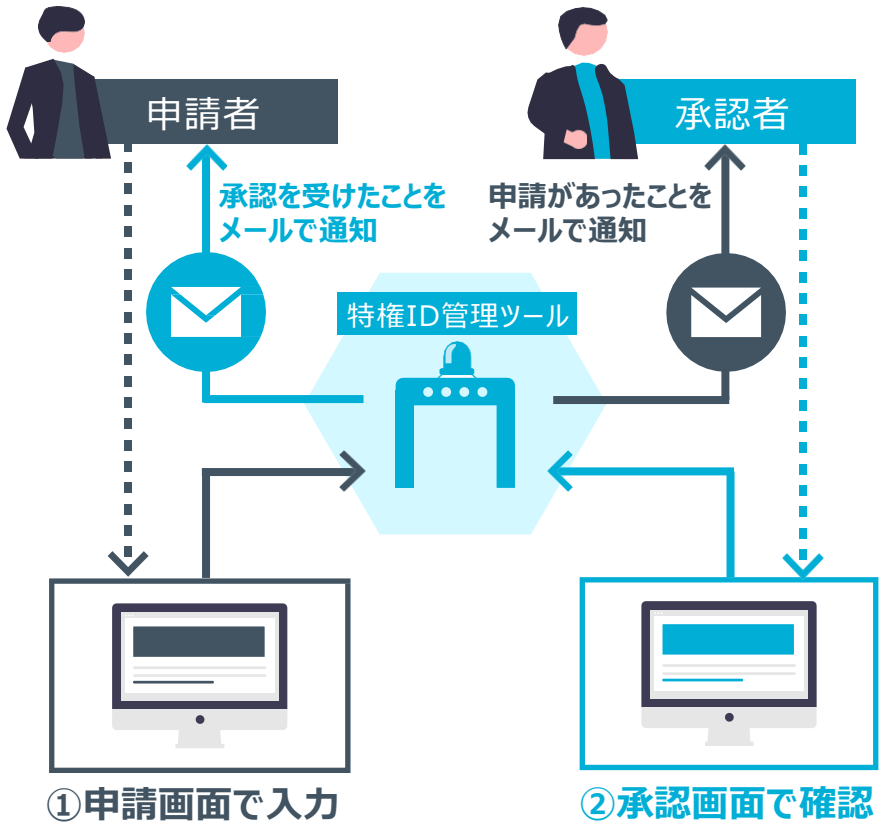
承認の権限を持つ利用者が、自ら作業をするために申請を出すケースも考えられます。
そのため、不正利用を防ぎ、安全性を確保するためには、自己承認を制御する機能が必要となります。

自社の承認フローを設定できる

「多段階承認をする」「グループ承認をする」など自社の運用に応じて柔軟に承認フローを設定できる機能があるかどうかも重要です。
また、作業内容ごとに承認フローを変更できるか、確認します。

緊急時のアクセスに対応できる

迅速な対処が求められる緊急時に本来の承認者が不在の時もあると思います。
その場合でもアクセスを許可できる仕様であれば、応急的な対処が可能となります。



チェック項目3　特権IDの利用・アクセス制御①

普段利用しているクライアントツールを利用できる

SSHクライアントなど、普段利用しているクライアントツールを特権ID管理ツールの運用に使えるのかどうかの確認が必要です。また、使用できない場合にはどのような影響があるのか、許容範囲であるかを確認します。

アクセスした個人を識別できる

特権IDを複数人で共有している場合、誰が特権IDを使ってアクセスをしたのか、個人を識別する機能を備えている必要があります。

アクセス元の端末を制御できる

IPアドレスやMACアドレス、クライアント証明書の有無による制御など、特権IDによるアクセスを許可する端末を制御できる機能があれば、外部の利用者による不正なアクセスを防止することができます。

承認された作業者・時間帯・対象機器のみにアクセスできる

アクセスの許可を承認した利用者やシステム・機器のみに限定し、さらにアクセス可能な時間帯も制限する機能があれば、目的外での利用を抑止できます。申請した時間を過ぎた場合に、強制的に利用が停止（切断）されるのか、ログイン状態は保持されるのかも確認します。

チェック項目3　特権IDの利用・アクセス制御②

承認された特権ID・プロトコルのみが利用できるよう制御できる

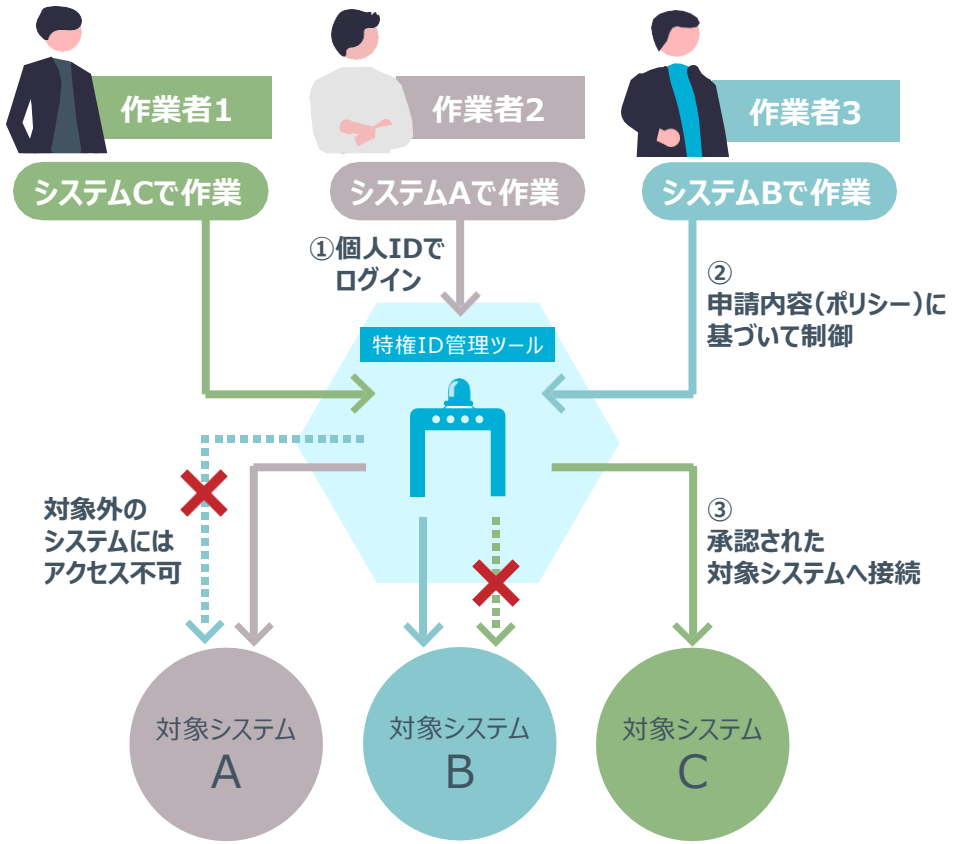
利用する特権IDやシステムとの接続に使うプロトコルを申請時に絞り込めれば、本来の目的とは異なる利用を抑止することができます。

複数人が同時に管理対象システムへログインできる

複数人での作業が必要になることもあるため、複数の作業者が同時に同じ特権IDを利用できるかも重要です。
また、同時に同じ特権IDを利用したとしても、利用した個人を識別できる必要があります。

作業者に対して特権パスワードを秘匿化できる

作業者に対して特権IDの利用の承認を与える際、特権IDのパスワードを秘匿化する機能を活用できれば、パスワードの漏えいや、許可されていない時間帯での不正利用を抑止できます。



チェック項目4　ログ取得・管理①

- [ ] **自社で定めているログ保存期間に対応できる**

  監査や内部統制のためにログ管理のポリシーを設定している場合は、それに準じてログの保存期間を設定できる柔軟性が必要になります。

- [ ] **アクセス概要だけでなく実際の操作内容を記録できる**

  作業者や接続先の機器へのアクセスログだけでなく、操作内容や転送したファイルなど具体的な作業内容をログとして残しておく機能があれば、監査や内部統制の強化につながります。

- [ ] **ログ取得できない作業が存在しない**

  作業内容をログとして残せない領域があると不正利用に使われる可能性を残してしまうことになるため、漏れなくログが取得できるツールであるかどうかも重要です。

- [ ] **ログの閲覧を限られた人のみに設定できる**

  監査や内部統制に使われるログは閲覧権限を制限しておくことが必要です。そのため、取得したログの閲覧者を制限できるか、確認します。

- [ ] **ログの改ざんを検知する仕組みがある**

  悪意のある利用者は、自身の不正な操作の痕跡を消すためにログの改ざんを試みます。そうした悪意ある行動を検知する機能を備えていれば、不正な操作を早期に発見し、被害拡大を防止できます。

チェック項目4　ログ取得・管理②

ログを暗号化して保存することができる

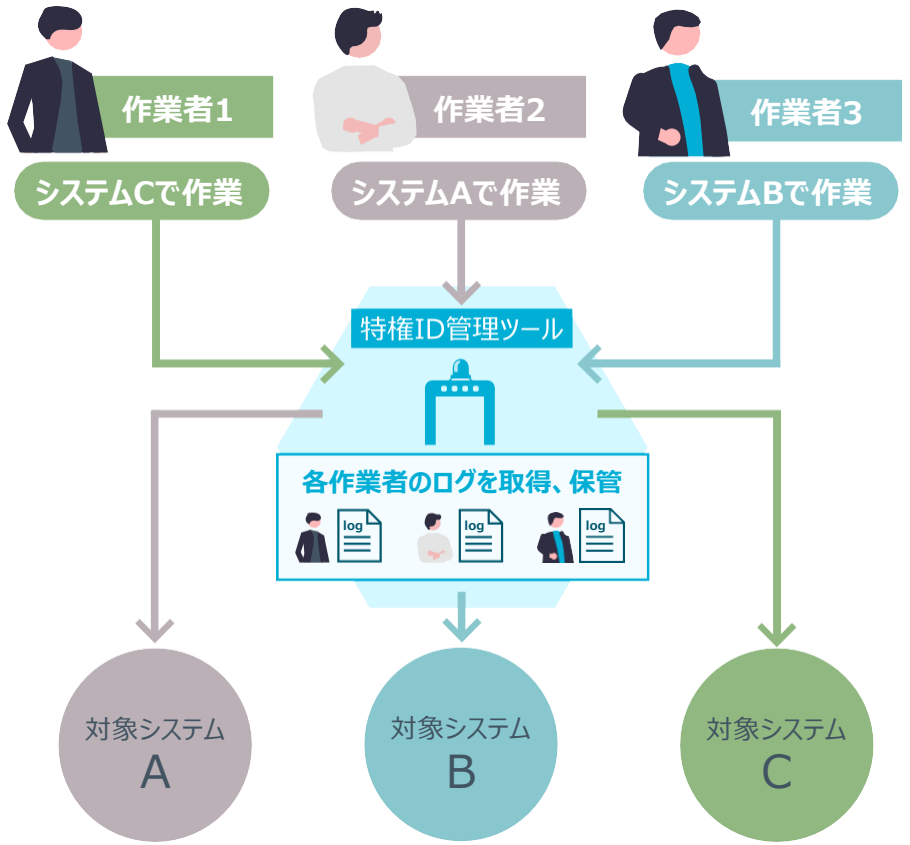
ログへの閲覧権限を設定できるかどうかに加え、ログを暗号化し保存する機能があることで、改ざんなど不正な操作のリスクを減らすことができます。ログ自体に重要な情報を含んでいる可能性もあるため、この観点でも暗号化できることが重要です。

持ち出し・持ち込みファイル実体を記録できる

不正なファイルの持ち出しや持ち込みがないかどうか、ログとして記録しておく機能があれば、特権ID管理のセキュリティをより高めることができます。

取得したログを外部ストレージへバックアップできる

本来の保存期間を超えてログを保持する、または有事に備えた冗長性確保のためにバックアップを外部ストレージに保存する機能があれば、事業の信頼性をより高めることができます。
また、長期間ログを保存する必要がある場合には、外部ストレージへログを配信する機能があると便利です。



チェック項目5　監査支援①

- ☑ **申請とログが自動で突合される**

  申請時の内容と操作ログを自動的に突き合わせることができれば、適切な監査業務と効率性向上が実現できます。

- ☑ **特権IDの棚卸が可能**

  特権IDの棚卸機能があれば、使用されていない特権IDの把握や不正に作成された特権IDの有無を確認するための作業負荷を軽減できます。

- ☑ **ログのキーワード検索ができる**

  作業中に不正な操作が行われていないかどうかを確認したい場合は、特定のキーワードによるログの検索機能を備えていることで業務効率の向上と安全性の確保を実現できます。

- ☑ **定期的なレポート発行が可能**

  収集する操作ログに関して日次や週次といった定期的なレポート出力をする機能があれば、監査業務の効率化が図れます。

- ☑ **申請外アクセスを検知できる**

  申請と承認のフローを踏んでいないアクセスによる危険を抑止するには、申請外のアクセスなどの不正な操作を検知した時に通知する機能が必要です。

チェック項目5　監査支援②

不正なコマンド実行を検知できる

不正な操作があった場合に、事前に登録した危険なコマンドをログから検知し、通知する機能があれば、不正操作の抑止、および早期発見につながります。

不正なファイル持ち出しを検知できる

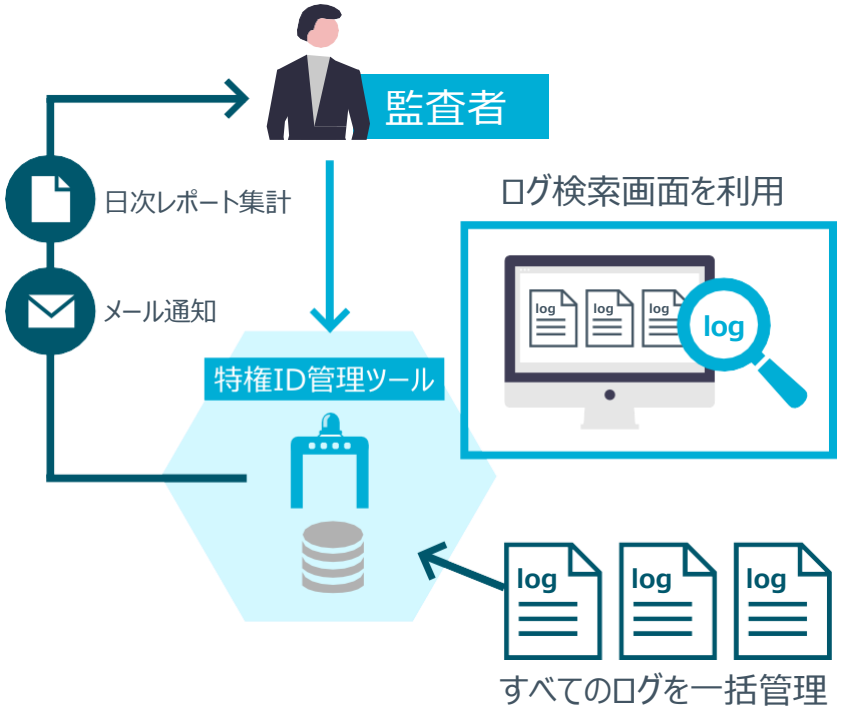
事前に申請したファイル以外の持ち出しがあった場合、それを検知し、メールで通知する機能があることで、不正な持ち出しが発生した際に早期の発見が可能となります。

個人情報など重要情報の持ち出しを検知できる

マイナンバーやクレジットカード情報、個人情報などの重要情報が持ち出されたことを検知する機能があれば、重要情報が不正に持ち出されても早期に発見し、被害の発生を抑止できます。

申請やログの内容を監査したことを記録に残すことができる

監査対応の証跡を残すことも必要です。内容を閲覧し、作業の妥当性を確認したことをツール上に記録できるか、確認します。



チェック項目6　その他機能

- [ ] **自社のActive Directoryと連携できる**

  作業者のユーザ認証の際、社内で運用している既存のActive Directoryを連携させて使用できれば、認証の一元化が実現できます。シングルサインオン（SSO）の機能があると便利です。

- [ ] **自社のワークフローや統合ログ製品との連携が可能**

  社内でワークフロー製品や統合ログ製品を使用している場合、それらの製品と特権ID管理ツールを連携させることができれば、既存の仕組みを生かして特権ID管理の一元化が可能です。さらにAPI連携ができれば拡張性、柔軟性がより高くなります。

- [ ] **作業者の個人認証について多要素認証できる**

  作業者を特定する認証の際、多要素認証の仕組みを導入できれば、なりすましを防ぎ情報漏えいのリスクを最小化できます。

- [ ] **作業者アカウントの棚卸が可能**

  本来削除するべき作業者アカウントが残っていると不正利用のリスクが高まります。アカウントの有効期限や棚卸機能があると便利です。

- [ ] **特権ID管理ツール自身の管理者アカウントについても操作内容を記録・モニタリングできる**

  特権ID管理ツール自身のシステム管理の権限を持つアカウントについても、その操作を記録し・モニタリングできることが必要です。

チェック項目7　非機能要件①

- [ ] **エージェントレスで利用できる**

  特権ID管理ツールを導入する際に、サーバやクライアントPCに専用のソフトウェアをインストールすることなく利用開始できれば、既存システムへの影響を小さく抑えることができ、短期間での導入や、運用負荷の軽減につながります。

- [ ] **冗長化構成ができる**

  冗長化の構成を組むことができるツールであれば、障害発生時など有事の際でも重要な特権ID管理の運用を継続させることができます。

- [ ] **発生しうる同時接続に対応できる**

  障害発生など有事の際には、特権IDの利用が集中することも考えられます。その場合に考えられる最大の同時複数接続に対処できるツールかどうかも重要です。

- [ ] **拡張が容易**

  管理対象のシステムが増える可能性がある場合は、スケールアウトまたはスケールアップによる拡張が容易にできるツールであることも重要となります。

- [ ] **エンドtoエンドで通信がすべて暗号化されている**

  端末とサーバの通信だけでなく、外部連携ツールとの通信、特権ID管理ツールの内部通信がすべて暗号化されていることを確認します。

チェック項目7　非機能要件②

- [ ] **多言語に対応している**

  日本語や英語での表示はもちろん、マニュアルも必要な言語での提供があるかどうかも忘れてはいけない確認事項です。

- [ ] **必要な言語でのサポート窓口がある**

  海外製のソリューションを導入した際には、テクニカルサポートを含めて日本語での窓口があると問い合わせがスムーズです。
  サポート対応時間にも留意し、日本時間での対応が可能か確認します。

- [ ] **サポート窓口の営業時間外にもサポートが可能**

  夜間休日にツールを利用することが多い場合、通常のサポート窓口の営業時間外のサポート体制もあることを確認します。

- [ ] **ツールに不具合・脆弱性が発見された場合、修正アップデートまたはパッチが提供される**

  特権ID管理ツールに不具合や脆弱性が発見された場合、業務に支障がでないよう、アップデートもしくはパッチ適用が必要です。ツール自身のメンテナンス作業を行う体制を確認し、バージョンアップやパッチ提供の頻度が自社にとって適切か確認します。

導入・運用を考慮するとエージェントレスがおすすめ 03

特権ID管理ツールは、大きく「ゲートウェイ方式」と「エージェント方式」の2つに分類できます。
ゲートウェイ方式は、利用者とサーバの間に関所（ゲートウェイ）を設置して一元管理する方式です。エージェント方式は、サーバやクライアントPCに専用のエージェントをインストールする必要があり、導入時の手間がかかる傾向にあります。

ゲートウェイ方式の特権ID管理ツールは「エージェントレス」である点がメリットです。エージェント方式の場合は対象サーバやクライアントPCの台数分だけエージェントをインストールする必要があるため、管理対象サーバやクライアントPCが多ければ多いほど導入時の手間が増大します。しかし、エージェントレスであれば管理対象の端末も少なく済むため、システム更新時や機器・ユーザの増減があった場合にも大きな運用負荷が発生することはありません。

NRIセキュアの「**SecureCube Access Check**」は、ゲートウェイ方式を採用した「エージェントレス」の特権ID管理ツールです。セキュリティと運用効率を高めるための多彩な機能を備えています。アクセス制御やログ管理における細かな設定が可能であることはもちろん、管理者操作がログとして記録できることも大きな特徴です。「既存システムへの影響を最小限に抑えつつ、日々の運用において作業効率と安全性を高めたい」。そんなツールをお探しの場合は、ぜひ「SecureCube Access Check」をご活用ください。

市場シェアNo.1*の**特権ID管理ツール**

最短1ヶ月で導入可能　管理工数最大78%削減

Access Check

エージェントレスで
既存システムへの影響を最小に

* 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2023」特権ID管理市場：ベンダー別売上金額シェア（2021年度）SecureCube Access Check，Cloud Auditor by Access Check が対象

まずは証跡取得とモニタリングによる現状把握から始めよう

特権ID管理ツールの有用性は理解できるものの、いざシステム保守・運用の業務に取り入れるとなると、細やかな運用設計が必要になり、導入に慎重になる企業は少なくありません。ネットワークの状態やセグメント分けなどがどうなっているか分からない状態から、いきなり100点満点を目指すのは困難です。
そんな時、まずは証跡取得とモニタリングによる現状把握から始め、誰がどこにアクセスして何をしているかをモニタリングできる状態にすることをおすすめします。

特権ID管理ツール「SecureCube Access Check」のコア機能のみ限定して提供している「**Access Check Essential**」では、導入のハードルをさらに下げ、現状の可視化から始められるツールです。まずは証跡取得・モニタリングから開始し、利用状況を可視化した上で、必要に応じて特権IDを適切に管理していくといったように、段階的にアクセス統制を進めていくことができます。

「Access Check Essential」が提供する機能は、アクセス統制に欠かすことのできない「アクセス制御」「ログ取得・管理」「監査支援」です。
「SecureCube Access Check」同様、ゲートウェイ方式を採用しているため、管理者の運用負荷を最小限に抑えることが可能です。
特権ID管理ツールを検討していてもなかなか導入に至らない、そんな課題をお持ちの際には、ぜひ「Access Check Essential」もご検討ください。

運用開始までに時間がかかる	→	すぐに使い始められる！
運用を維持する体制が取れない	→	運用負荷が軽減！
導入するための予算が立てられない	→	初期費用が抑えられる！

特権IDの内部統制に不可欠なアクセス制御・証跡取得に特化

Access Check Essential

Access Check　　Access Check Essential

SecureCube Access Check や **Access Check Essential** についてもっと知りたい方はこちら

資料請求 ›　　定期セミナー申込 ›　　試用版申込 ›

SecureCub Access Check製品サイトへ ›　　Access Check Essential製品サイトへ ›

NRI SECURE

www.nri-secure.co.jp/　　info@nri-secure.co.jp