［決定版］

基本の4STEP
を徹底解説

新任システム管理者のための

特権ID管理入門書

知らなかったでは済まされない！
管理者権限の利用に潜むリスクと適切な管理方法とは？

NRI Secure Technologies, Ltd.

NRI SECURE

新任システム管理者のための特権ID管理入門書

4月から新社会人となり、今まで経験のない情報システム管理に携わることになる方も多いのではないでしょうか。また、異動や転職を機に、システムを管理する必要性が出た方もいるかと思います。

システム管理の業務を行う中で「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。そのため、システム管理の経験が少ない方も特権ID管理の重要性を理解する必要があります。

本書では、システム管理者に求められる特権ID管理とは何かを説明し、ベストプラクティスとして、ソリューションを用いた特権ID管理方法をわかりやすく解説します。

目次

01　システム管理と特権ID

02　特権ID管理の基本

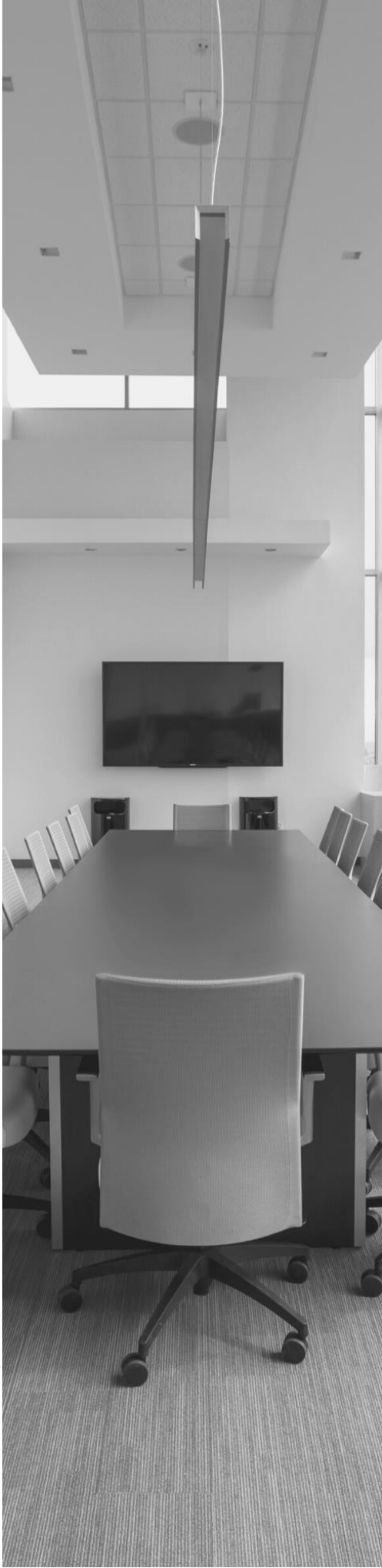
　　STEP1　利用者の特定

　　STEP2　申請承認

　　STEP3　作業の記録

　　STEP4　妥当性の確認

03　ソリューションを導入したベストプラクティス



01

システム管理と特権ID

システム管理とはどのような仕事でしょうか。

情報システム管理者の仕事を端的に言うと、

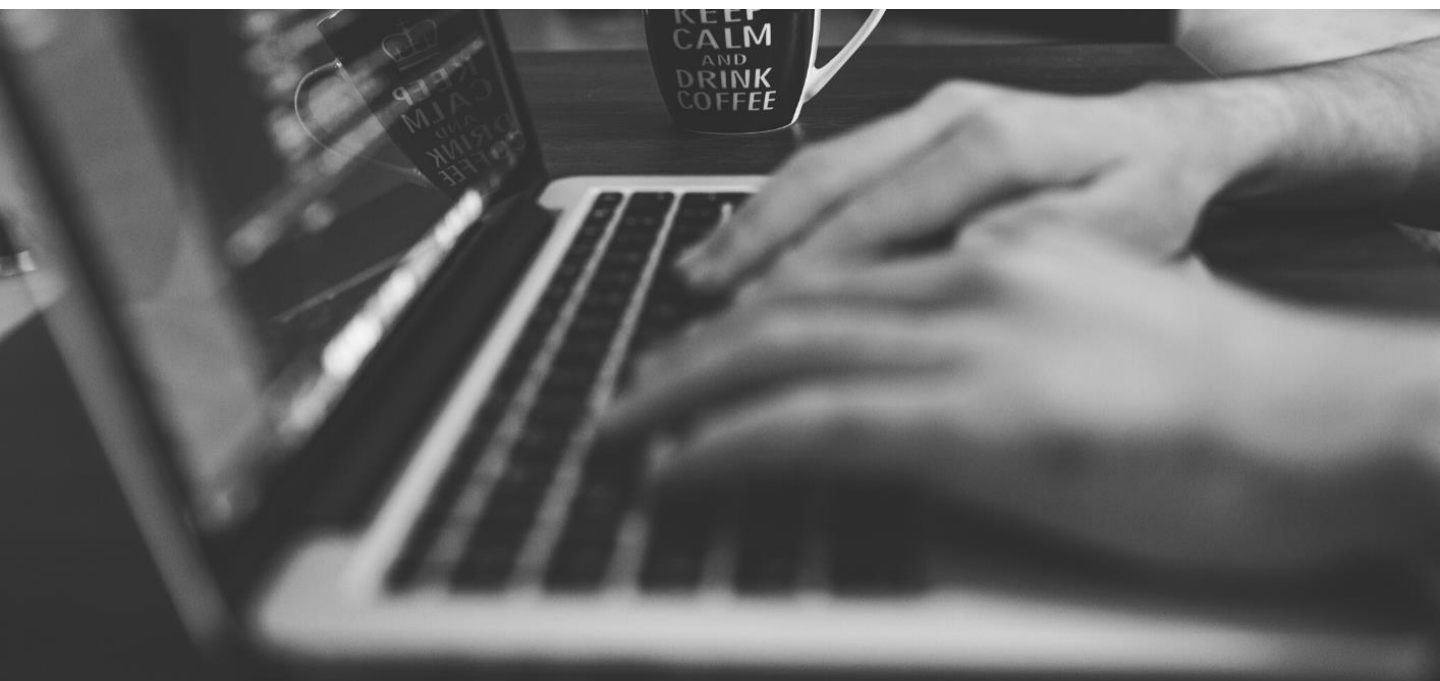
システムを安定的に、かつ、安全に利用してもらうために、システムを維持・保守していく業務

と言えます。

具体的には、情報システムのメンテナンスや障害対応を行うため、システムを構成するサーバへアクセスし、システムの設定変更やログの確認、パッチの適用といった様々な作業を行います。

サーバで操作を行う際は、利用しているアカウントの権限に沿った操作のみが許可されます。アカウントの中にはシステムの起動や停止など、一般のアカウントが持っていない特別な権限をすべて有しているものもあります。これが「特権ID」と呼ばれているものです。

システム管理の作業の際には、この特権IDを利用することが避けられません。



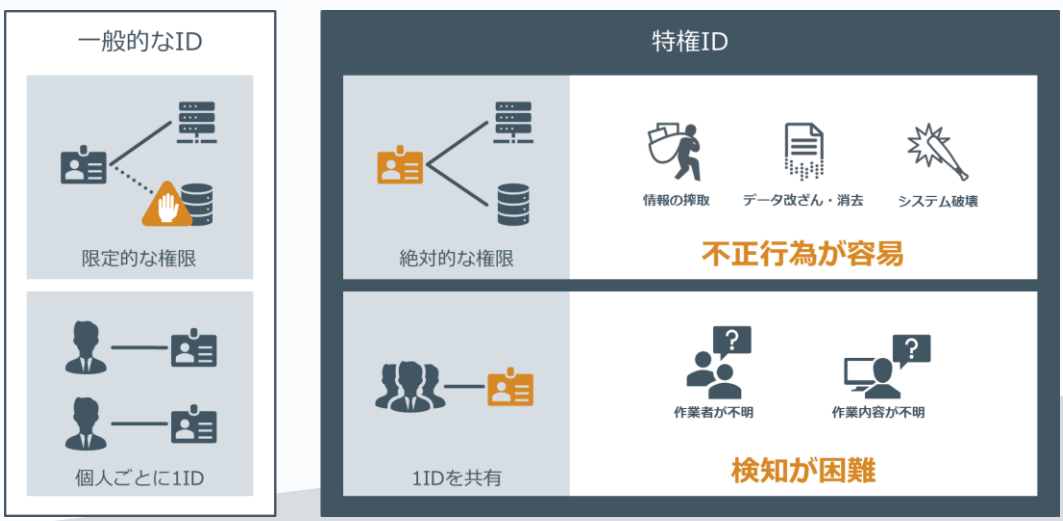
特権IDとは

> システムの維持・管理のために用意され、起動や停止をはじめとするシステムに大きな影響を与えることができる権限

日本ネットワークセキュリティ協会発行の『エンタープライズにおける特権ID管理解説書』（第1版）によれば、特権IDとは “システムの維持・管理のために用意され、起動や停止をはじめとするシステムに大きな影響を与えることができる権限” と定義されています。

つまり、特別な権限がついていることが要件となるため、たとえWindowsにおいて”Administrator”ではなくとも、同等の権限が与えられているIDも特権IDであると言えます。

一般的なIDと特権IDの違い



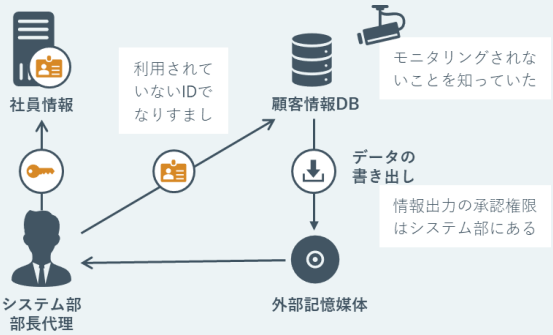
特権ID利用に潜むリスク

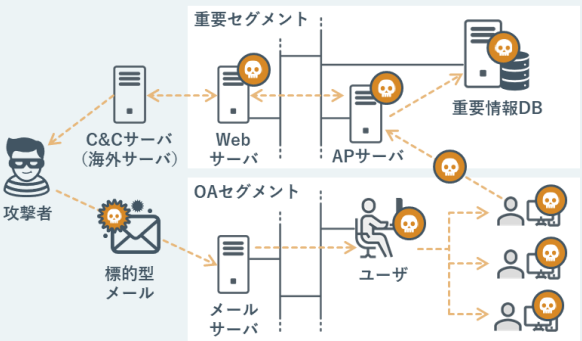
特権IDはあらゆる作業が行えることから、非常に便利なのですが、裏を返すと悪意のある操作／操作ミスによって、情報漏えいやデータの改ざん、サービスの停止などビジネス活動に支障をきたす甚大な被害を及ぼすというリスクも有しています。またそれらの影響は、社会的信用の失墜、損害賠償、事後対応にかかる労力と費用の増大など、将来にわたる多大な損失も伴います。

ならばそのようなアカウントを作らない、または無効化する、という議論もありますが、特権IDは多くのシステムに組み込まれており、その利便性から特権IDを利用した作業が行われているのが実情です。

特権の濫用の例

自身に与えられた特権IDを悪用し、別の社員の個人IDを使って入手した顧客情報を、私的な金銭目的で転売した事件がありました。特権IDを利用することで他人になりすまし、罪を擦り付けることもできてしまうことに注意しましょう。





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、辞書攻撃やブルートフォース攻撃などの手段で特権の搾取を試みることが知られています。特権が搾取されることで、被害は拡大します。

02 特権ID管理の基本

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です。

IT全般統制、J-SOX監査、PCI DSSなどのガイドラインで求められている特権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以下の4STEPにまとめられます。

STEP1　利用者の特定

特権IDを利用した人は「誰か」を特定できる仕組み作りが重要です。
利用者を特定できないと、悪意のある操作が行われた際などの調査が困難になる恐れがあります。
そのため、サーバごとに個人を特定できるID（ユニークなもの）を付与し、そのID経由で特権を利用するといった運用が一般的です。

STEP2　申請承認

特権IDを利用するということはリスクがあるというのは前章の通りです。そのため、特権IDを「いつ」「何のために」利用するのかを明確にした申請を行い、然るべき責任者の承認を受けてはじめて、特権IDを利用することが望ましいと言えます。申請承認のワークフロー（仕組み）は、独自の申請書やメールを利用するなど、企業ごとにやり方は様々です。

STEP3　作業の記録

特権IDを利用した作業に関して、「いつ」「誰が」「何をしたか」記録を残しておくことが重要です。サーバ上に記録されるログで代替するケースが多いですが、事前に申請した通りの作業が行われたのか確認できるよう、操作内容すべてがわかるものを記録しておくことが望ましいです。

STEP4　妥当性の確認

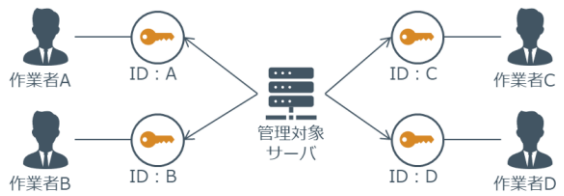
申請の内容と作業の記録を突き合わせ、「申請通りの目的での作業が行われたか」妥当性を確認します。申請内容を理解し、作業の内容を確認する必要があるため、機械的な確認は困難であり、手運用で行われるのが一般的です。

特権ID管理の課題

基本の4STEPをきちんと対応をすることができれば「特権IDの管理は行えている」と言えるのですが、現実的には様々な課題から多大な負荷が発生し、特権ID管理を行うことでコストが多大になってしまうケースや、特権ID管理の仕組み自体が形骸化してしまうケースが見受けられます。

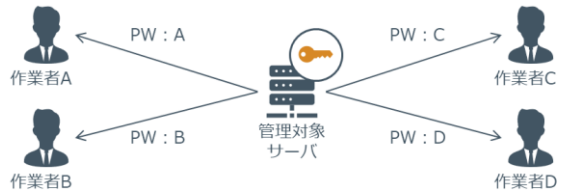
例｜特権IDの利用者を特定する方法：

特権グループIDを個別に作成して個人を特定



サーバ別、利用者別に各IDライフサイクルを管理するため、**負荷が増大**
IDの削除漏れや権限の変更漏れ等に注意

利用の都度パスワード変更して利用者に貸出



パスワード貸出・返却**作業の増加**だけでなく、同一環境での**同時作業も困難**
パスワード変更漏れに注意

03

ソリューションを導入したベストプラクティス

特権ID管理を実施するためには、様々な課題があることを前章で説明しました。
自社の情報システム管理において効率的かつ効果的な特権ID管理を実現するために、特権ID管理専用のソリューションを導入し、現実的な運用を行うことを目指しましょう。

現在販売されている特権ID管理ソリューションは、大きく４つのアクセス方式に分類されます。
これらの違いを押さえることが、ソリューションを導入する上で重要なポイントとなります。

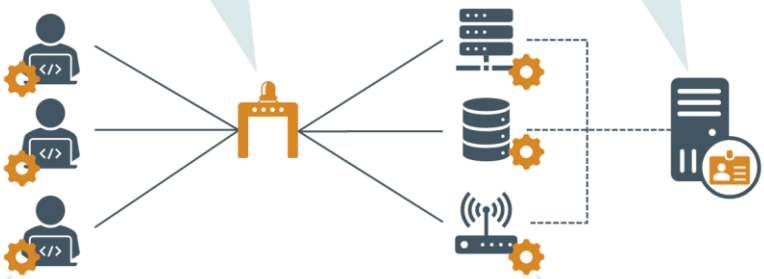
アクセス方式の違い

ゲートウェイ方式

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。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。対象サーバが多い場合や、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

サーバの特権ID棚卸（不正／不要IDチェックなど）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。



クライアント・エージェント型

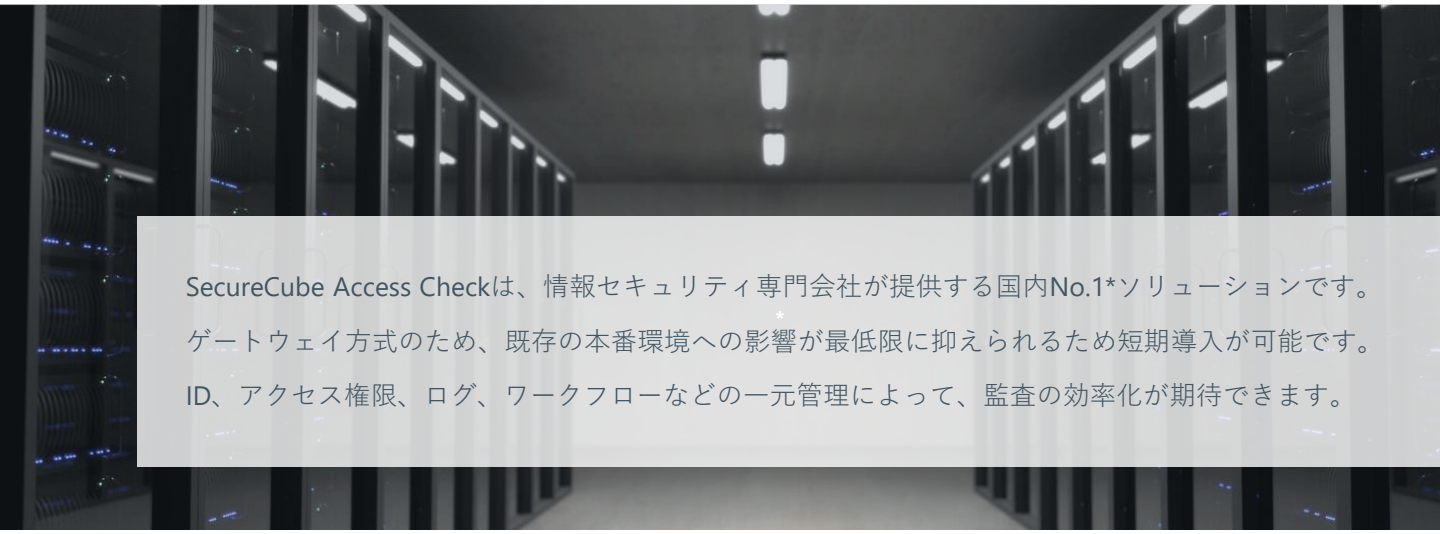
アクセス元のクライアントごとにエージェントをインストールする方式。クライアントごとで、本人認証（特権ID利用者の特定）とログ取得を行う。ログを詳細に取得したい場合や、サーバへの接続用端末が特定されている場合などに最適。

サーバ・エージェント型

アクセス先のサーバごとにエージェントをインストールする方式。サーバごとに個人IDの管理、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、サーバ内で詳細な操作制御を行いたい場合に最適。

ゲートウェイ型の特権ID管理ソリューション

SecureCube Access Check



SecureCube Access Checkは、情報セキュリティ専門会社が提供する国内No.1*ソリューションです。
ゲートウェイ方式のため、既存の本番環境への影響が最低限に抑えられるため短期導入が可能です。
ID、アクセス権限、ログ、ワークフローなどの一元管理によって、監査の効率化が期待できます。

* 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2025」特権ID管理市場：ベンダー別売上金額シェア（2023年度）
SecureCube Access Check, Access Check Essential, Cloud Auditor by Access Check が対象

SecureCube Access Check が選ばれる理由

ゲートウェイ型だから スピード導入

ソフトウェアなどのインストールが不要なため、既存システムや端末への影響を最小限にして、短期間かつコストを抑えて導入することが可能です。

各種ガバナンス対応の 充実した機能

IT全般統制、J-SOX監査、金融庁監査、FISC安全対策基準、PCI DSSなど、各業界における法令基準で求められる特権ID管理を実現できます。

国内のべ600社以上の 導入実績No.1*

大手金融機関をはじめ、流通業、製造業、サービス業、公共機関など業種を問わず様々なお客様に、ご要件に合わせてご利用いただいております。

SecureCube Access Check の詳細はこちら

Website　www.nri-secure.co.jp/service/solution/accesscheck
Email　info@nri-secure.co.jp

SecureCube Access Checkで実効性のある特権ID管理

STEP1 利用者の特定

各サーバに存在する特権IDをSecureCube Access Checkで一元管理することで、ID管理の負荷を大幅に削減することが可能です。特権IDのパスワードを定期的に自動変更する機能も搭載しています。

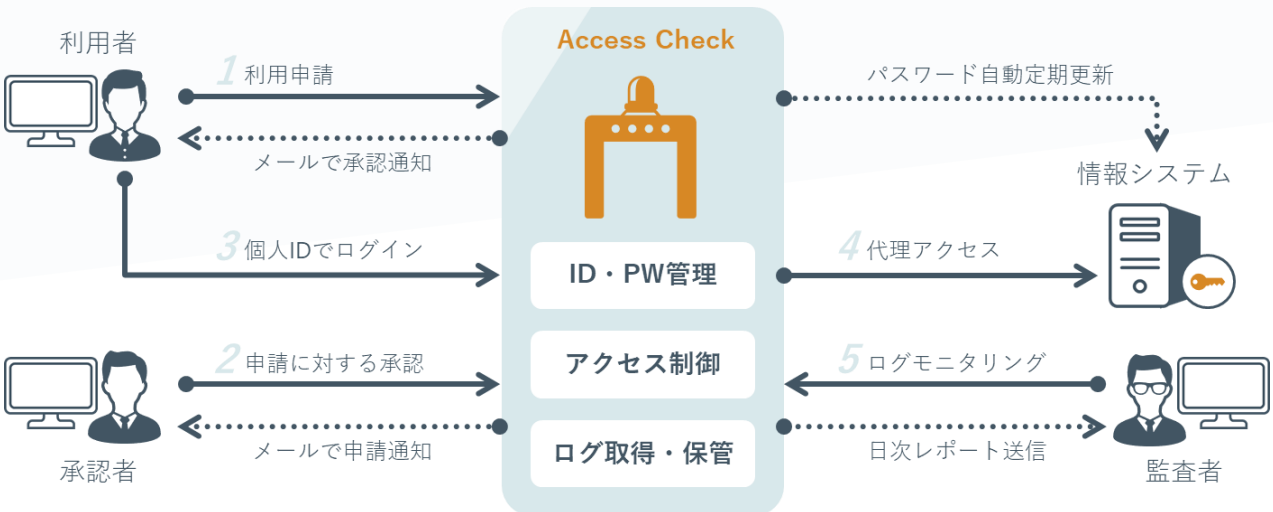
SecureCube Access Checkを経由する際に、個人のIDと特権IDを紐づけて、利用者個人を特定します。

また、SecureCube Access Checkの利用者IDについては、Active Directoryをはじめとした LDAPによる認証連携も可能です。そのため、既に組織で運用している利用者の個人IDをそのまま利用できます。

STEP2 申請承認

SecureCube Access Checkには、申請および承認のワークフロー機能もあります。申請情報が一元管理されているため、検索条件を絞って参照することが可能になります。

また、SecureCube Access CheckではAPI（Application Programming Interface）を提供しており、既存のワークフローシステムなどと連携することも可能です。



SecureCube Access Checkで実効性のある特権ID管理

いつから　いつまで　誰が　どの端末から　どのサーバに　何をしたか

アクセス開始日時	アクセス終了日時	アクセス可否	利用者ID	接続元IPアドレス	接続先IPアドレス	プロトコル	ログイン試行ID	申請番号	操作ログ
2020/03/15 15:47:52	2020/03/15 16:51:10	アクセス許可	user_a	10.0.16.123	10.0.4.32	ssh	root	20200315A0001	
2020/03/15 15:52:09	2020/03/15 16:56:25	アクセス許可	user_b	10.0.16.234	10.0.4.15	rdp	Administrator	20200315A0002	
2020/03/15 15:57:59	2020/03/15 17:00:32	アクセス許可	user_c	10.0.16.101	10.0.4.32	ssh	admin	20200315A0003	
2020/03/15 16:12:18	2020/03/15 16:31:12	アクセス許可	user_a	10.0.16.123	10.0.4.32	ssh	root	20200315A0001	
2020/03/15 16:14:01	2020/03/15 17:14:59	アクセス許可	user_b	10.0.16.234	10.0.4.16	ftp	ftp_user	20200315A0002	

アクセスログ検索結果（イメージ）

STEP3
作業の記録

SecureCube Access Checkでは、「いつ」「誰が」「どの端末から」「どのサーバに」アクセスしたか、だけでなく、そのサーバで「何をしたか」まで含めたログを一元的に記録し、保管します。そのため、SecureCube Access Checkの管理画面から、検索条件を絞って参照できます。

また、ログは暗号化して保管することも可能です。ログのハッシュ値を管理しており、改ざんされている、あるいは改ざんされていないことを証明することができます。

STEP4
妥当性の確認

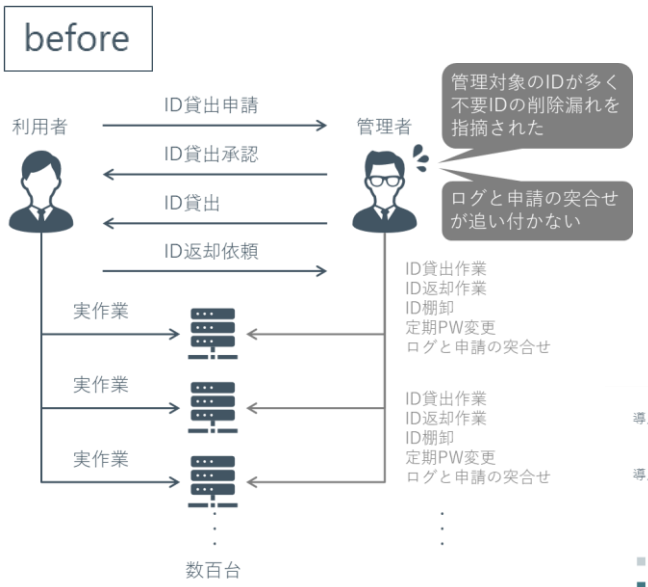
SecureCube Access Checkに保管された申請と、その申請に関連するログが自動的に紐づけられます。そのため、申請とログの突合せ作業は必要なくなり、すぐに申請に基づくログを確認できます。

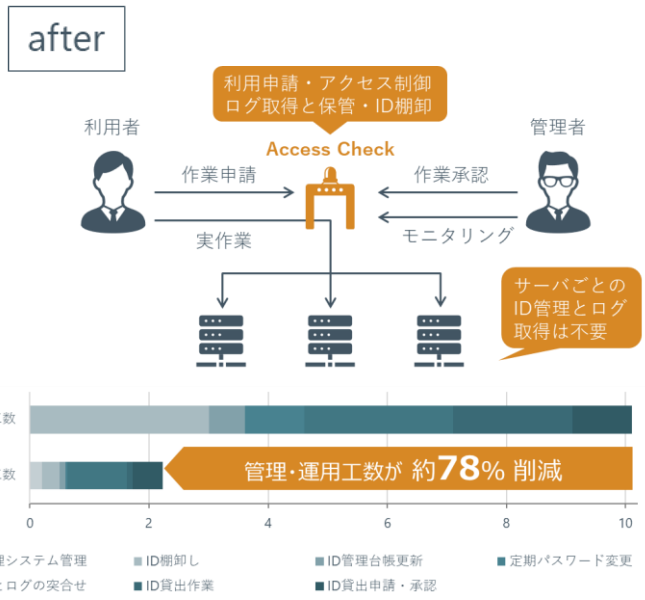
確認を行った証跡を残すための機能も整備されており、妥当性の確認（監査業務）を行うための負荷を大きく低減させることが可能です。

成功事例 | 内部統制の工数が78%削減

ソリューションを導入する前は、手運用で特権IDのパスワード払い出し作業を行っていましたが、短い期間で監査対象サーバが増える中で、多くの作業負荷がかかっており、管理可能なセキュリティレベルに限界があったといいます。

SecureCube Access Checkを導入し、一元的にサーバへのアクセス管理を行うことで、ログの突合せやID棚卸の負荷を大幅に削減することができ、手運用の際の工数の約1/4にまで削減することができました。





まずは
自社の特権ID管理を確認してみましょう

これから初めてシステム管理を行う人は、特権IDというものがピンと来ないかもしれません。

しかしながら、実際に業務を始めるとその便利さに気付き、危険性を認識しながらもリスクを疎かにしてしまい、何らかの事故を起こしてしまうかもしれません。「自分は大丈夫」と思っていても、業務委託先やシステムベンダーへ貸し出す管理者権限のIDはどうでしょうか。

システム管理者として配属された際には、ぜひ自社の特権ID管理が基本の4STEPを実施できているか、見直してみてください。そして、管理負荷やコスト、管理精度などに課題があれば一度特権ID管理ソリューションの導入を検討し、システム管理全体の生産性を向上させていただきたいと考えています。

特権ID管理の基本の4STEP

Appendix：
証跡取得とモニタリングによる現状把握

特権ID管理ソリューションの有用性を理解できても、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把握できる状態にすることをおすすめします。

特権ID管理ソリューション「SecureCube Access Check」のコア機能のみを限定して提供している「Access Check Essential」は、導入のハードルを下げ、現状の可視化から始められるツールです。

「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。これから特権ID管理をはじめる企業は、アクセス統制・証跡取得ソリューションのご活用もご検討ください。

特権ID管理ソリューション導入の課題		Access Check Essential の特長
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！

Access Check Essential の詳細はこちら

Website　www.nri-secure.co.jp/service/solution/access-check-essential
Email　info@nri-secure.co.jp

Access Check

特権ID管理の課題をすべて解決

https://www.nri-secure.co.jp/service/solution/accesscheck