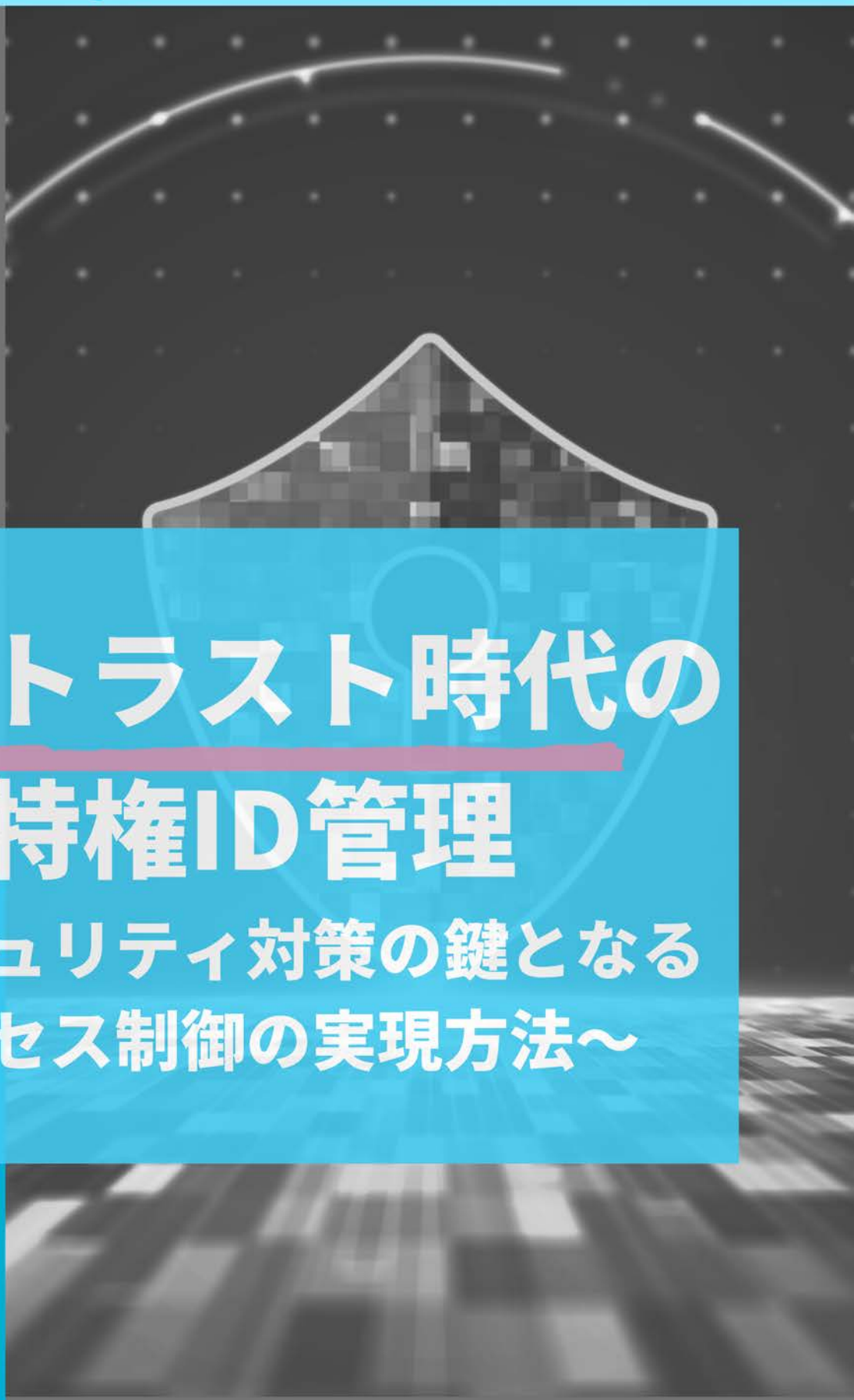
NRI SECURE



ゼロトラスト時代の特権ID管理

～セキュリティ対策の鍵となるアクセス制御の実現方法～

はじめに

これまで、特権ID管理は、内部統制を主な目的として行われる傾向がありましたが、昨今では、セキュリティ対策としても重要視されるようになっています。

その背景として、サイバー攻撃や内部不正の増大はもちろん、クラウドサービスの利用拡大、新型コロナウイルス（COVID-19）感染症の拡大に伴うテレワークの急増が挙げられます。セキュリティリスクが高まる中、特権ID管理に求められることが大きく変化しているのです。

一方、働く環境の多様化に伴い、これまでのセキュリティ対策だけでは対応が困難になった今、ゼロトラストに注目が集まっています。

本書では、その理由を説明した上で、ゼロトラストを前提としたセキュリティ対策において、今後、特権ID管理に必要な条件は何かを解説します。

目次

01 セキュリティリスクの高まりとゼロトラスト

1.1. 「セキュリティの抜け道」の増大

近年、ハードウェア・ソフトウェアの購入をはじめとする初期費用や、ハードウェアをメンテナンスする手間を削減するため、クラウドサービスを利用する企業が増えています。総務省の令和3年「情報通信に関する現状報告」（令和3年版情報通信白書）によれば、その割合は一部利用も含めると約7割にのぼります。

また、新型コロナウイルス（COVID-19）感染症の拡大に伴い、ここ数年で、テレワークを導入する企業が急増しています。NRIセキュアが毎年行っている調査では、日本企業1,616社のうち80%が、新型コロナウイルス感染症拡大以降にテレワークを開始していたことが分かりました（「NRI Secure Insight 2021」より抜粋）。コロナ禍によりテレワークが急速に浸透した結果、働く場所（ワークプレイス） の分散が加速しています。

これまで、機密情報をはじめとする企業の重要資産は社内に存在し、アクセスも社内から行うのが大半でした。しかし、昨今では、クラウドストレージをはじめ、社外に保存されることが多くなっています。しかも、働き方の多様化に伴い、さまざまな場所・端末からアクセスされるケースが急増しています。

その結果、致命的な損害を引き起こす「セキュリティの抜け道」の発生リスクが増大しています。従来のセキュリティ対策では、もはや企業の重要資産を守ることが難しくなっているのです。

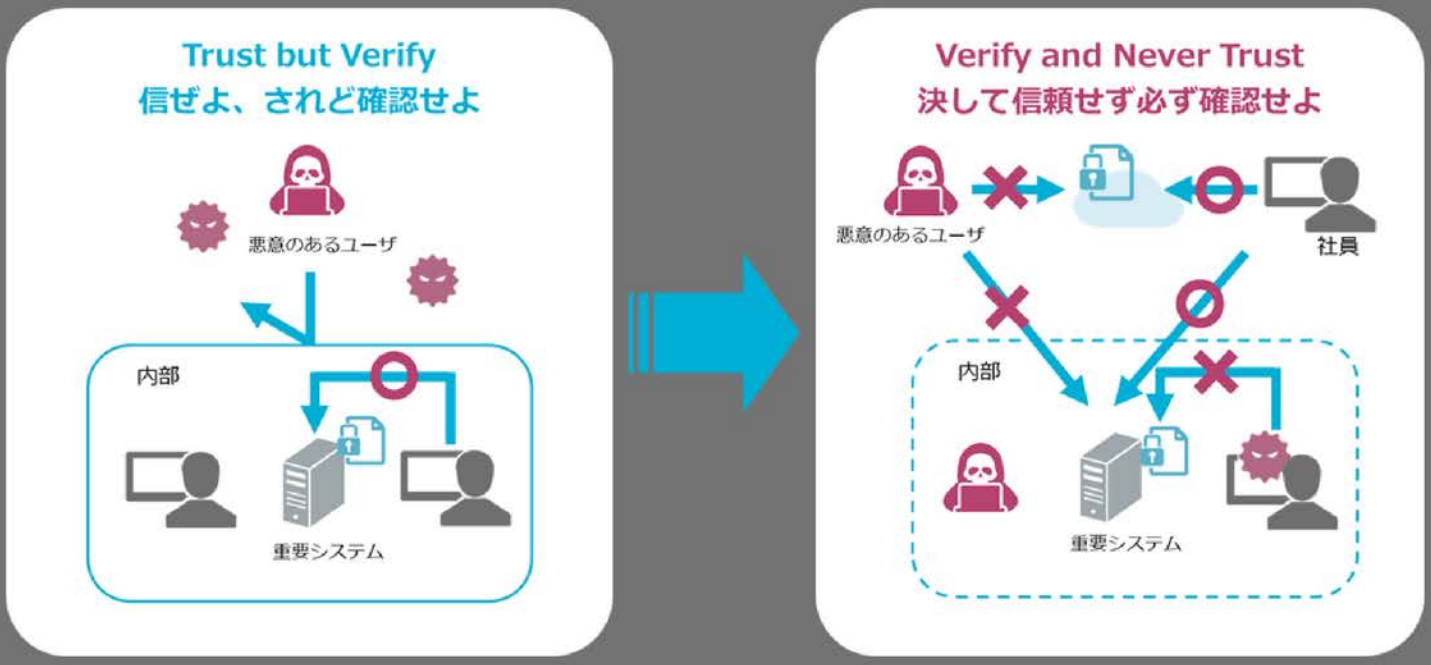
このようなビジネス環境の急速な変化に伴い、ゼロトラストへの注目度が急激に高まっています。その理由について次項で見ていきましょう。

01

1.1. ゼロトラストが注目を集める理由

ゼロトラストは、2010年に米国の調査会社であるForrester Research社が提唱したセキュリティモデルです。「決して信頼せず必ず確認せよ（Verify but never trust）」を前提としています。守るべき重要資産へのアクセスはすべて信用せずに監視・検証することで、脅威を防ぐという考え方です。

一方、従来から一般的に知られているのは「境界防御モデル」です。こちらは「信ぜよ、されど確認せよ（Trust but verify）」を前提としています。信用する領域と信用しない領域の二つに境界を分け、不審なID・アクセスといった、境界外部からの脅威を検証することで、境界内部への侵害を防ぐという考え方です。企業の重要資産が社内にあることが前提のセキュリティモデルだと言えるでしょう。



【図１】境界防御モデルからゼロトラストモデルへ

ただし、昨今では、前項で示したとおり、重要資産がクラウドサービスなど社外に保存されることが増え、働き方の多様化により、様々な場所・端末からアクセスされる頻度が高まっています。その結果、セキュリティの抜け道が増大している時代なのです。

以上のことから、IDやアクセスポイントにかかわらず、すべてのアクセスを常に監視するという、ゼロトラストの考え方が注目されています。

従来の手法では重要資産を守ることが困難になっている今、ゼロトラストを前提としたサイバーセキュリティ対策の構築が急務です。それは、特権IDを使ったアクセスの管理においても同じことが言えます。

次章からは、ゼロトラスト時代に求められる特権ID管理のあり方について、現状を概観した上で、順を追って解説します。

02

特権ID管理の現状と今後

2.1. 特権ID管理の重要性と現状

特権IDは、WindowsのAdministratorやLinux/UNIXのrootに該当する、高い権限をもつIDのことです。システムのシャットダウン、ユーザ権限の変更、機密情報へのアクセスなど、システムに対して大きな影響を与える操作が可能です。さらにログの削除など、侵害した痕跡を消すこともできます。

システム	特権ID名
Windows	Administrator
Linux/Unix	root
Oracle	sys
SQL Server	sa

【表1】システムと特権ID名の組み合わせ例

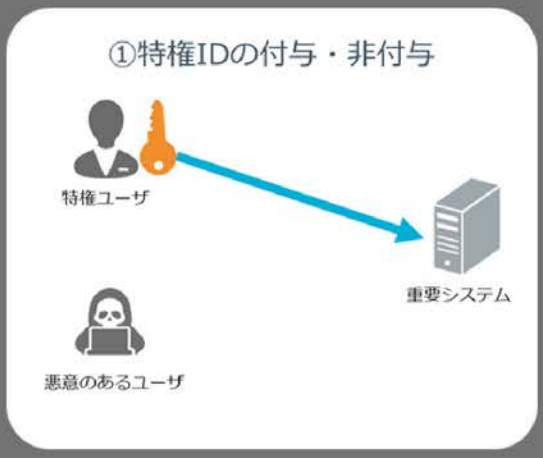
そのため、サイバー攻撃や内部不正の際に最も狙われるIDです。万が一特権IDを窃取・悪用されてしまうと、企業は甚大な被害を受けることになります。

それにもかかわらず、複数ユーザでの使い回し、初期設定パスワードのままでの使用など、特権IDが適切に管理されていない企業が多く見られます。今後、内外の攻撃から身を守るには、特権IDをどのように管理すれば良いのでしょうか。

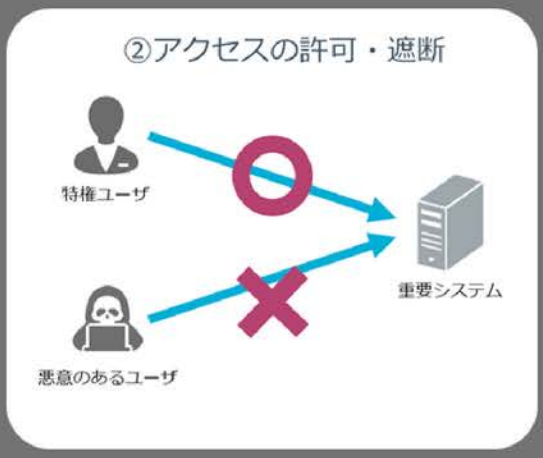
2.2. 特権ID管理に必要な2つの対応

特権ID管理には、本来、次の2つの対応が必要です。

① 特権IDのアカウント（Administrator、root等）を適切に管理すること
② 特権IDを利用した本番環境へのアクセスを制御すること



①は、特権IDについて、利用を許可するユーザ・範囲の管理、誰がいつ利用したかの特定、利用者が規定の申請・承認手続きを踏んでいるかの確認、付与する権限を最小限にすることなどを指します。いわゆるID管理にあたるものです。



一方、②は、特権IDを利用したシステムへのアクセスそのものを制御することを指します。一つ一つのアクセスを監視し、許可されたアクセスかどうかをチェックし、不正なアクセスである場合には遮断などの対応を行います。

【図２】特権ID管理における2つの対応

これまでの特権ID管理は、内部統制が主な目的であり、①の対策が優先されてきました。②のアクセス制御については、まだ手をつけていない企業が今でも多く見られます。

しかし、サイバー攻撃や内部不正から身を守るセキュリティ対策が急務の今、特権ID管理の方法を改めて見直すことが求められています。

2.3. 今後の特権ID管理に不可欠なアクセス制御

昨今、働く環境の急速な変化に伴い、「セキュリティの抜け道」が増大した結果、特権IDそのものが窃取されるケースが急増しています。そのため、正しいIDによる操作でも、安全とは言えなくなっています。

前述のとおり、従来の特権ID管理では、特権IDの付与を厳密にコントロールすることで攻撃から身を守る方法が主流でした。しかし、今やそれだけでは不十分だと言えるでしょう。これからは、すべてのアクセスを検査した上で許可・遮断する「アクセス制御」が不可欠なのです。

【図３】アクセス制御の有無による違い

この方法なら、万が一特権IDが窃取・悪用されたとしても、不審なアクセスそのものを遮断することで、攻撃者から重要情報を守ることができます。このアプローチは、IDやアクセスポイントにかかわらず、すべてのアクセスを常に監視するというゼロトラストの考え方とも合致します。

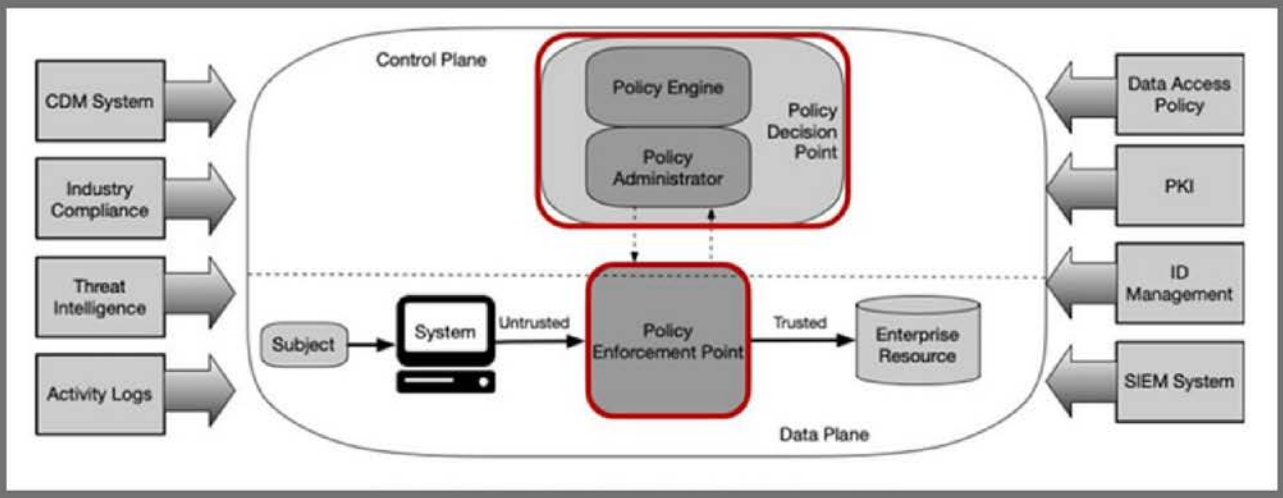
次章からは、ゼロトラストにおけるアクセス制御の考え方を概観した上で、これからの特権ID管理に求められる条件について見ていきます。

03 ゼロトラストにおけるアクセス制御の考え方

3.1. アクセス制御に必要な要素

ゼロトラストを定義・解説するものとして、NIST（National Institute of Standards and Technology：米国立標準技術研究所）が発行したガイドライン「NIST SP 800-207」があります。

この中で、ゼロトラストの論理コンポーネントが図示されています（図4）。主要素となるのは、赤枠で囲んだ、「Policy Decision Point（PDP、ポリシー決定ポイント）」と「Policy Enforcement Point（PEP、ポリシー施行ポイント）」です。



【図4】ゼロトラストの論理コンポーネント

アクセス要求元（ユーザ・システム）が企業リソースに接続する際、PDPでそのアクセスの許可・遮断を判断し、PEPで接続の有効化・終了などを行います。

では、PDPはどのようなポリシーに基づいて判断するのでしょうか。次項で見ていきましょう。

3.2. ゼロトラスト7つの原則とアクセス制御

「NIST SP 800-207」では、「ゼロトラスト7つの原則」が提唱されています。その中で、No.4、6、7がアクセス制御に関連する内容です。

No.	内容
1	すべてのデータソースとコンピューティングサービスをリソースとみなす
2	ネットワークの場所に関係なく、すべての通信を保護する
3	企業リソースへのアクセスは、セッション単位で付与する
4	リソースへのアクセスは、動的なポリシーにより決定する
5	すべての資産の整合性とセキュリティ動作を監視し、測定する
6	リソースの認証と認可は動的に行い、アクセスが許可される前に厳密に実施する
7	可能な限り多くの情報を収集し、セキュリティを高めるために利用する

【表２】ゼロトラスト7つの原則

この原則から、ゼロトラストモデルでは、リソースへのアクセス可否の判断をPDPで行う際に、出来るだけ多くの情報を集めた上で、動的に変化する要素を用いる必要があるとわかります。

具体的には、アクセス要求元について、信頼度、セキュリティ対策の実施状況、信頼度が変化する要因（時間帯・場所等）など、変動する要素に基づいて判断する必要があるのです。

では、今後の特権ID管理がこの条件を満たすには、具体的に何を行えば良いでしょうか。次章で見ていきましょう。

04 ゼロトラスト時代の特権ID管理を実現する方法

特権IDは、システムに大きな影響を与える操作が可能な、高い権限を持つIDです。そのため、特権ID管理におけるアクセス制御は、とりわけ厳密に行われる必要があります。

本章では、その方法について、「ゼロトラストが提唱するアクセス制御に必要な要素を満たす方法」という観点で、順を追って解説していきます。

4.1. 特権ID管理製品の利用

前述のとおり、ゼロトラストの考え方では、一つ一つのアクセスを常に監視し、できるだけ多くの、且つ動的な要素を用いてアクセス可否を判断・制御することを提唱しています。ただし、特権ID管理において、それを手作業で行うのは困難です。

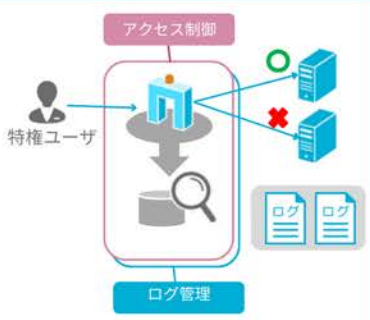
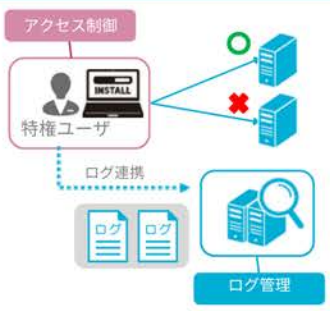
従って、ゼロトラストにおけるアクセス制御に必要な要素を満たすには、特権ID管理製品の利用が不可欠です。では、どのような製品を選べば良いでしょうか。

4.2. ゲートウェイ方式とエージェント方式の違い

現在の特権ID管理製品は、大きく分けると、ゲートウェイ方式とエージェント方式の二つに分類できます。各方式によって、アクセス制御が可能な範囲・方法が異なります。

ゲートウェイ方式では、重要システムと特権ユーザの間にゲートウェイを設置することで、重要システムへのアクセスを一元管理します。重要システムに入る前に必ずゲートウェイを通過するため、ID・アクセスポイントにかかわらず、すべてのアクセスを検査・制御することが可能です。

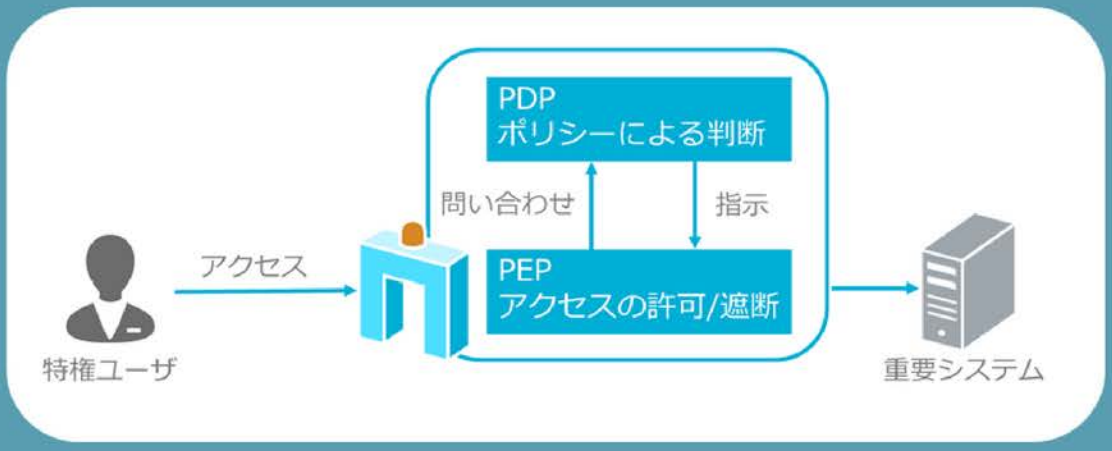
一方、エージェント方式では、特権ユーザが利用するクライアント端末と本番サーバにエージェントをインストールすることで、アクセス制御を行います。特権IDの払い出しや利用可否を行うことで、不審者が重要システムに侵入するのを防ぎ、統制を図る際に利用される方式です。

方式	ゲートウェイ方式	エージェント方式	
		クライアント・エージェント	サーバ・エージェント
特徴	ユーザと本番サーバの間にゲートウェイを設置し、アクセス制御とログを一元管理。エージェントのインストールは不要	クライアント端末にエージェントをインストールし、アクセス制御とログ取得を実施。ログは監査のために別コンポーネントへ収集	接続先サーバごとにエージェントをインストールし、アクセス制御を実施。ログは監査のために別コンポーネントへ収集
構成			

【図５】ゲートウェイ方式とエージェント方式の違い

4.3 製品を選ぶポイント

ゲートウェイ方式で開発された製品の場合、すべてのアクセスに対し、企業の重要システムへ到達する前に検査し、許可・遮断を行うことが可能です。そのため、ゼロトラストの論理コンポーネントで定められた、PDP（ポリシー決定ポイント）とPEP（ポリシー制御ポイント）を備えた構成で、特権アクセス管理を行うことができます。



【図６】ゲートウェイ方式のPDPとPEPの役割

一方、エージェント方式には、特権IDの払い出しを行ったユーザによるアクセスなのかを検査した上で、許可・遮断を行う製品があります。その場合、アクセス制御の判断基準がIDに関する情報に限られるため、ポリシーと合致しているのかを判断するのに十分な情報が得られるとは言えません。

さらに、利用端末にエージェントをインストールすることでアクセスを制御する方式のため、インストールしていない端末から侵入された場合、防御できないという問題があります。

以上のことから、ゼロトラストにおけるアクセス制御に必要な要素を満たすには、ゲートウェイ方式をはじめとする、特権IDを使ったすべてのアクセスを検査・制御できる製品を選ぶのがおすすめです。

なお、NRIセキュアでは、長年、ゲートウェイ方式の特権ID管理製品「SecureCube Access Check（セキュアキューブ・アクセスチェック、以下「Access Check」）」を提供しています。

Access Checkでは、特権IDの利用可否に限らず、以下のような、さまざまな要素に基づいてアクセス制御を行うことが可能です。ご参照ください。

Access Checkで利用できるポリシーの要素
アクセス実施前に承認が必要か
アクセス開始日時・終了日時
アクセスを実施する端末のIPアドレス
アクセスする本番サーバのIPアドレスまたはホスト名
アクセスする本番サーバのログインアカウント
本番サーバで実施するコマンド（キーワード）
本番サーバにアクセスするプロトコル
持ち出すファイルの名前
クリップボードを利用するか

【表3】Access Checkで利用できるポリシーの要素

05 特権IDによるアクセス制御の事例・利用例

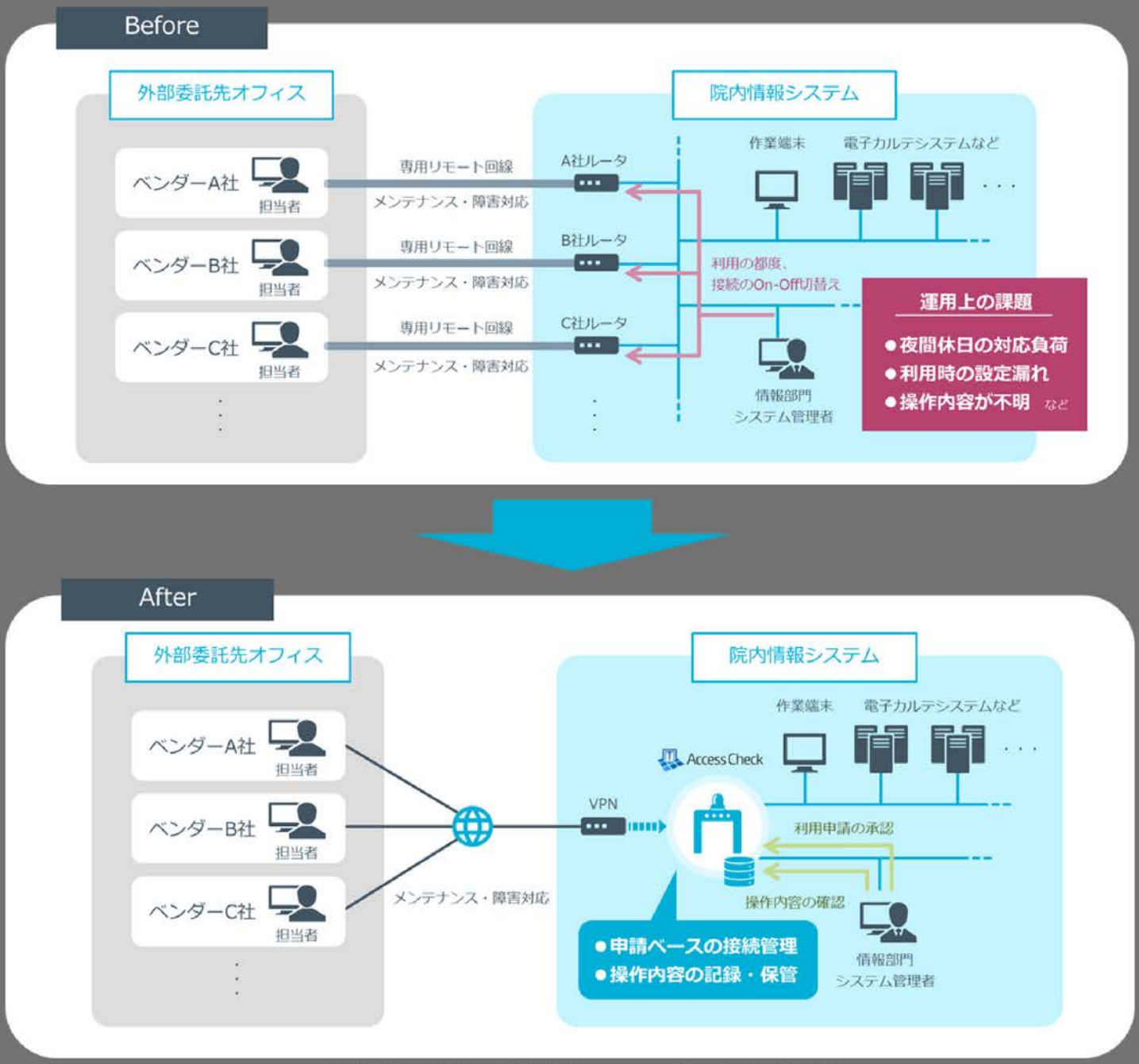
本章では、特権ID管理製品のAccess Checkを活用して、実際にアクセス制御を行った事例と利用例を紹介します。

5.1. リモートアクセス回線のアクセス制御（A病院事例）

西日本にあるA病院では、電子カルテシステムをはじめとする医療業務のデジタル化を進めながら、セキュリティ対策を行ってきました。インターネットには直接接続せず、クローズドな環境に近い形で運用することで、全体のセキュリティを担保。同時に、医師や職員が機密情報を不用意に外へ持ち出さないよう、ネットワークレベルのセキュリティから端末まで、出入口を塞ぐ対策をしてきました。

しかし、リモートメンテナンス回線の対策が難しく、万が一攻撃・不正が行われた場合、早期発見・回避が困難だという課題がありました。A病院の情報システム担当者は、これこそ「セキュリティ上の抜け道」だと捉えていたそうです。

そこで、ネットワークインフラの更改を機に、それまで複数の委託ベンダーがばらばらに用意していたリモートメンテナンス用の回線を一本化し、入口を一つにまとめました。さらに、Access Checkを導入し、委託ベンダーのメンテナンス作業を制御・監視する仕組みを整備したことで、この課題を解決したのです。



【図７】A病院の事例（Access Check導入前後）

A病院がAccess Checkを選んだ主な理由は次の2点です。

① ポリシー設定機能から、きめ細やかなアクセス制御を行えること

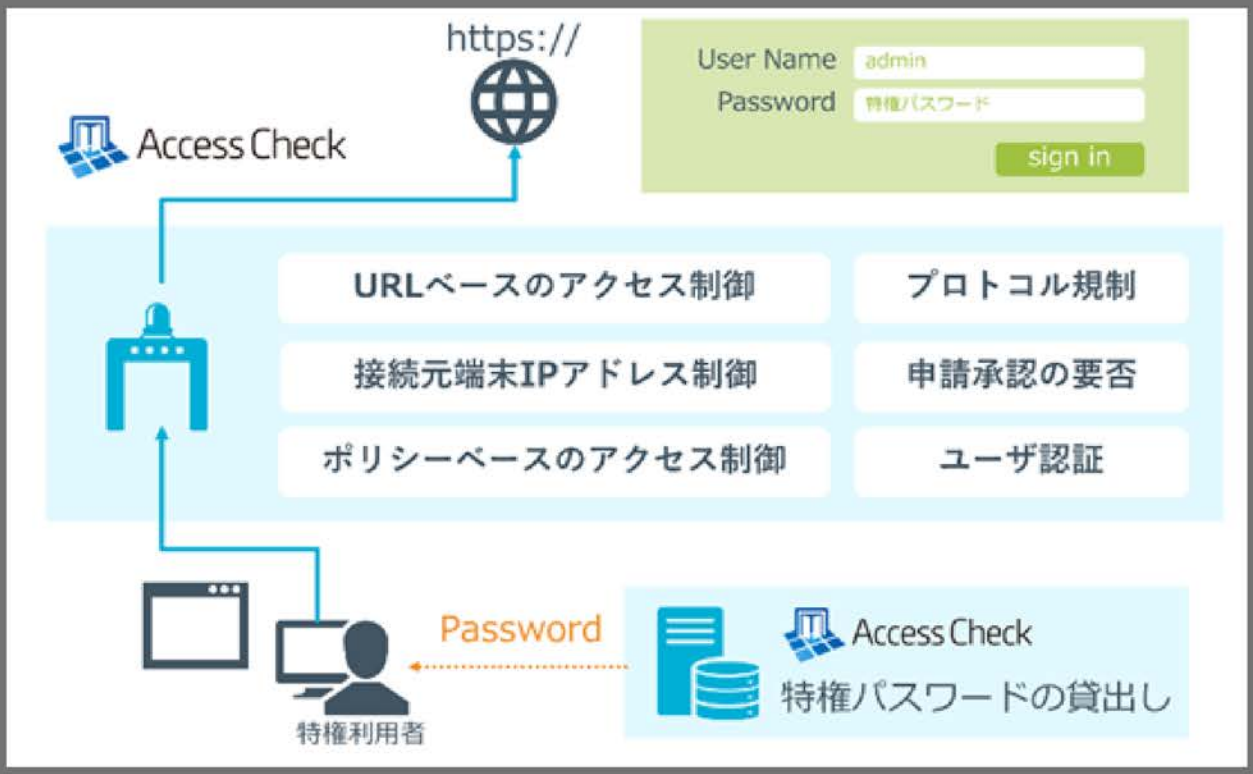
② 申請・承認のワークフローを電子化できること

これは、出来るだけ多くの情報を集めた上で、動的に変化する要素を用いてアクセス制御を行うという、ゼロトラストの考え方に合致した特長でもあると言えるでしょう。

5.2. Webインターフェースのアクセス制御（クラウド利用例）

近年、SaaSサービスやクラウドシステムなど多くのシステムで、Webインターフェースが利用されており、重要システムの場合と同様に厳格なアクセス制御が求められています。

Access Checkでは、アクセス元の端末のIPアドレスと接続先のURLに基づいた、より確実なアクセス制御が可能です。HTTPS中継のリクエストやレスポンスの通信内容を復号化し、解析することもできます。この通信内容はログとして保存でき、情報漏えい時のフォレンジック調査にも利用可能です。



【図８】Webインターフェースのアクセス制御

まとめ

06

これまでの特権ID管理は、内部統制が主な目的でした。しかし、働き方が多様化する今、それだけでは不十分です。「セキュリティの抜け道」が増大しリスクが高まる中、重要資産を守るには、ゼロトラストの考え方に基づいた対策を進める必要があるのです。

そのためには、特権IDの管理に加えて、さまざまな、且つ動的に変化する要素に基づいたアクセス制御が欠かせません。ゼロトラスト時代に求められる特権ID管理を構築するには、ゲートウェイ方式をはじめとする、特権IDを使った重要システムへのアクセスをすべて検査し、制御できる製品を選ぶのが効果的です。

NRIセキュアのAccess Checkは、長年の実績を誇る、ゲートウェイ方式の特権ID管理製品です。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おり、アクセス制御における細かな設定が可能であることが大きな特長です。多様化する環境に対応できる、効率的・効果的なアクセス制御の実現に、ぜひAccess Checkをご活用ください。

参考資料

◆　総務省　情報通信白書
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd242140.html

◆　NIST SP 800-27
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf