JNSA

NPO 日本ネットワークセキュリティ協会

標準化部会　デジタルアイデンティティ WG

【改定新版】

特権 ID 管理ガイドライン　解説編

２０２３年3月３１日　発行

留意事項

このレポートの利用に際しては、以下の条件を遵守してください。

このレポートに含まれる一切の内容に関する著作権は、レポート作成者に帰属し、日本の著作権法や国際条約などで保護されています。

著作権法上、認められた場合を除き、著作権者の許可なく、このレポートの全部又は一部を、複製、転載、販売、その他の二次利用行為を行うことを禁じます。

これに違反する行為を行った場合には、関係法令に基づき、民事、刑事を問わず法的責任を負うことがあります。

レポート作成者は、このレポートの内容の正確性、安全性、有用性等について、一切の保証を与えるものではありません。また、このレポートに含まれる情報及び内容の利用によって、直接・間接的に生じた損害について一切の責任を負わないものとします。

このレポートの使用に当たっては、以上にご同意いただいた上、ご自身の責任のもとご活用いただきますようお願いいたします。

目次

ご挨拶

本書は 2016 年度に発行した、「エンタープライズにおける特権 ID 管理解説書（第１版）」について、これまでに多くのご意見やご指摘をいただいたものを反映すべく再度内容について検討を行い、新たな形で発行するものである。

今回の解説書は 2 部構成として、１部は「解説編」２部は「実践編」とした。「解説編」では、特権 ID 管理の重要性や特権 ID の捉え方、インシデント事例などを紹介した。「実践編」では、実際に特権 ID を行うための仕組みや運用方法について解説予定である。なお、「実践編」については現状未完成であるため、完成した際にはぜひ続けてご拝読いただきたい。

これから、特権 ID 管理を導入検討する人には、プロジェクトの推進の準備として、また、現在特権 ID 管理システムを導入中の人にとっては、現在のプロジェクトをよりよくするためのチェック・ヒント集として、ご活用していただけると考えている。

また、この分野について詳細に書かれた書籍がほとんど出版されておらず、その意味でも本書の内容は多くの企業に役立つ内容となっている。

なお、本書は「日本ネットワークセキュリティ協会（JNSA）」の「デジタルアイデンティティ管理ワーキンググループ」のサブグループにて検討した内容となっている。本書があらゆる企業において、特権 ID 管理の適切な導入・運用に貢献できれば幸いである。

標準化部会　デジタルアイデンティティ管理　ワーキンググループ　リーダ　宮川 晃一

第 1 章　特権 ID とは

1.1　システムにおける特権 ID とは

システムに対する攻撃者は、攻撃対象のシステムへアクセスや操作を行うために、特権を奪取することを試みる。設定済みの許可されている特権 ID を利用してアクセスされた場合、システムからは、特権 ID の利用者が正規の権限を持っているか判断できない。そのため、取り扱いには一般利用者向けのユーザーID（以後、一般 ID）以上に、注意が必要である。

特権とは特別な権限のことであり、辞書によると「特定の（身分や階級に属する）人に特別に与えられる優越的な権利。」となっている。一方で、情報システムにおける権限とは、システム内のリソースやファイルへのアクセス権やプログラムの実行権、他のユーザーやプロセス等とのデータの共有権限などが考えられる。それらの権限に対して、一般のユーザーより特別に与えられる優越的な権利が、情報システムにおける特権となる。

種別	利用目的	保持する権限
一般 ID	通常業務で使用	通常業務で使用する必要最低限の権限
特権 ID	特別な操作が必要な業務で使用	全ての権限（全権）、あるいは全権に準ずる権限（高権限）

表 1-1 一般 ID と特権 ID の相違点（比較）

例えば「利用目的」で比較すると、一般 ID は利用者が通常業務で使用する。一方特権 ID は一般 ID では操作することができない特別な業務を実施する場合に使用する。OS やミドルウェアにセキュリティパッチを適用する場合などが該当する。

「保持する権限」で比較すると、一般 ID は通常業務で使用する権限、必要最低限の権限のみを保持する。通常業務で使用しない権限はそもそも不要であり、不要な権限の付与により誤操作や想定外の利用（不正利用含む）が発生する可能性があるためである。一方特権 ID は当該領域におけるすべての権限を持っていたり（全権）、ある

いは全権に準ずる権限を持っていたりする（高権限）。これにより一般 ID ではできない特別な操作を実施することができる。

特権 ID	説明
root/Administrator	Linux/Windows 等の OS やハイパーバイザにおいて、あらゆる操作に対する権限を持つ ※ビルトイン管理者アカウントともいう
Administrators グループに所属する ID	Windows OS において、あらゆる操作に対する権限を持つ
Windows Server Operators、Windows Account Operators、Backup Operators のようなグループに所属する ID	Windows OS において、特定の機能を利用する場合に必要な操作に対する権限を持つ（アカウント管理権限、バックアップ権限など）
sa	Microsoft SQL Server（データベース）において、あらゆる操作に対する権限を持つ
SYS、SYSTEM、SYSADMIN などのグループに所属する ID	Oracle Database（データベース）において、あらゆる操作に対する権限、あるいは特定の機能を利用する場合に必要な操作に対する権限を持つ（バックアップ権限など）
enable コマンドによる特権行使	ネットワーク機器において、あらゆる操作に対する権限を持つ（enable コマンドを使用することで、通常モードから特権モードに移行する）
AWS、Azure、GCP 等のクラウドサービス登録時のメールアドレス	当該クラウドサービスにおいて、あらゆる操作に対する権限を持つ
アプリケーションの管理者 ID （アプライアンスを含む）	アプライアンスやアプリケーションにおいてあらゆる、操作に対する権限を持つ

表 1-2 特権 ID の例とその説明

特権 ID は高権限を持っており、あらゆる操作ができるため、様々な脅威に晒されている。

脅威の分類	脅威の内容	リスク
内部脅威	正当な権限を持つ人による特権 ID 不適切利用（人為的ミス、不正利用など）	• 機密情報･個人情報などの利用価値のあるデータの窃取:機密性に対するリスク • 誤ったデータ変更（削除、データ更新など）：完全性に対するリスク • 想定外のサービス停止:可用性に対するリスク
	正当な権限を持たない人による特権 ID 不正利用	
外部脅威	不正アクセスによる特権 ID 不正利用	

表 1-3 脅威の分類とリスク

1.2　特権 ID の特徴

特権 ID は、システムの導入時やシステムそのものの設定変更時に利用される。具体的には、root や Administrator、admin など OS やミドルウェアにあらかじめ組み込まれたユーザーカウント、SYS や SYSTEM、sa など DBMS（データベースマネジメントシステム）のアカウント、manager などネットワーク機器やストレージ機器のアカウントなどが挙げられる。（表 1-2 参照）また、現在のシステムでは、権限管理機能が実装されているものが多く、システムの管理に関わる権限を付与した任意の ID も特権 ID となる。一般ユーザー向けの ID とは異なり、広範囲で強い権限を与えられた特権 ID には、あらかじめ組み込まれているなど、いくつか実装のパターンがある。製品に実装されている特権および特権 ID のパターンを表 1-4 に示す。

ID がハードコーディングされている（固定 ID）	パスワード	パスワード無し
		デフォルト（既定）パスワードが設定されている
		初期設定時にパスワード登録を行う
	ID	ID の追加登録
		ハードコーディング/ビルトインされている ID の無効化
		ハードコーディング/ビルトインされている ID の削除
デフォルト（既定）ID が登録されている	パスワード	パスワード無し
		デフォルト（既定）パスワードが設定されている
		初期設定時にパスワード登録を行う
	ID	デフォルト ID の変更
		ID の追加登録
		ハードコーディング/ビルトインされている ID の無効化
		ハードコーディング/ビルトインされている ID の削除
ID をユーザーが設定する	パスワード	パスワード無しでの登録
	ID	複数 ID の登録

表 1-4 製品に実装されている特権および特権 ID のパターン

1.2.1. 一般 ID と特権 ID の違い

特権 ID は、一般 ID と比較して権限の範囲が広いため、操作ミスや故意の操作による影響範囲も広くなる。また、前述したようにシステムにあらかじめ組み込まれているため、ID そのものが情報として公開されてしまっていることが多くパスワード攻撃を受けやすい。さらには、運用上で共有して使われることが多く、いつ誰が利用したか特定しにくい環境が発生しやすい。

一般 ID と比較した場合の特権 ID の特徴	影　響
権限の範囲が広い	不正アクセスや誤動作等が発生した場合、一般 ID に比べ、大きな被害になりやすい
デフォルト（既定）の ID として用意されている	ID が知られているため、パスワード攻撃を受けやすい
運用上、共有する ID となりやすい	利用者の識別が難しいため、監査ができない。パスワードが変更しにくい

表 1-5 一般 ID と比較した場合の特権 ID の特徴

上記のことから、特権 ID の誤った運用による脅威として次の点があげられる。

誤用：単純なミスによる障害発生

乱用：過度な操作

故意：悪意を持った操作

監査不能：誰がいつ操作したか不明

また、特権 ID のライフサイクルは、通常の ID 管理における ID ライフサイクルの視点にプラスして、システムの採用から廃棄までの視点も必要であることを意識しておく必要がある。特にビルトインされた特権 ID は、システム管理者が変更になった場合でも存続する ID となり、利用者視点でのライフサイクルとは時間軸が異なるからである。

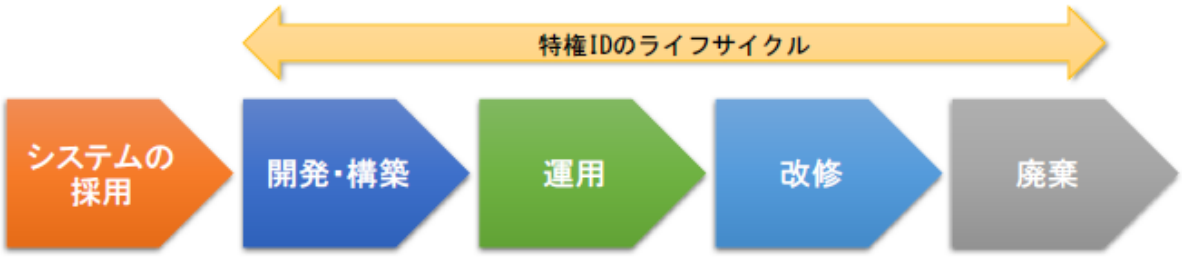


図 1-1 特権 ID のライフサイクル

1.2.2. 特権 ID が奪取された場合の影響度

奪取された特権 ID がどのレイヤで利用されているものかによって、システムに与える影響度が大きく異なる。一般的に、より下位レイヤー（ハードウェア基盤に近い層）の ID が奪取された場合には、それよりも上位のレイヤへの制御・改ざん・破壊などが可能となるため、システムへの影響度は相対的に大きいと言える。

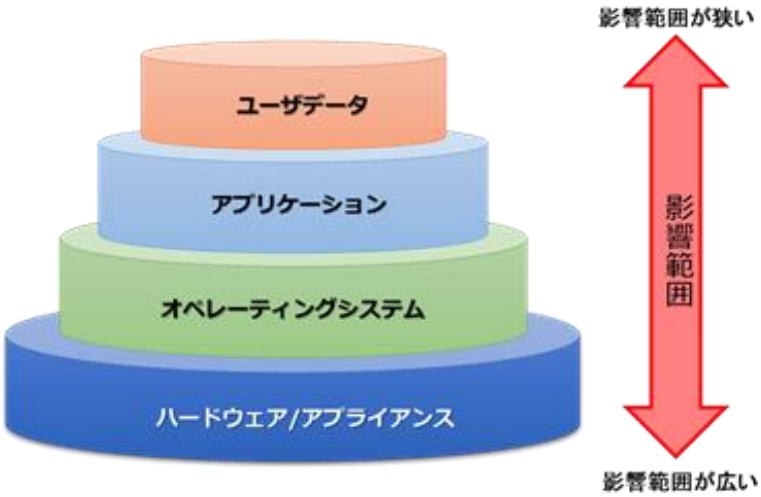


図 1-2 システムのレイヤと特権 ID の影響範囲

1.2.3. 利用用途の観点でのセキュリティリスク

保守要員など、本来は、運用上の権限範囲を狭く小さく定義するべきメンバーに対して、ハードウェアや OS の障害発生時を想定し、特権 ID またはそれに相当する権限を保持する ID を割り振らざる得ない状況が発生する。システム的な制限だけではなく、「社内規定」、「運用手順書」、「承認フローの遵守」など運用ルールの確立、さらにはログ管理によるトレーサビリティの確保により、想定外の作業事故や故意の不正アクセスなどを抑制する努力も必要となる。

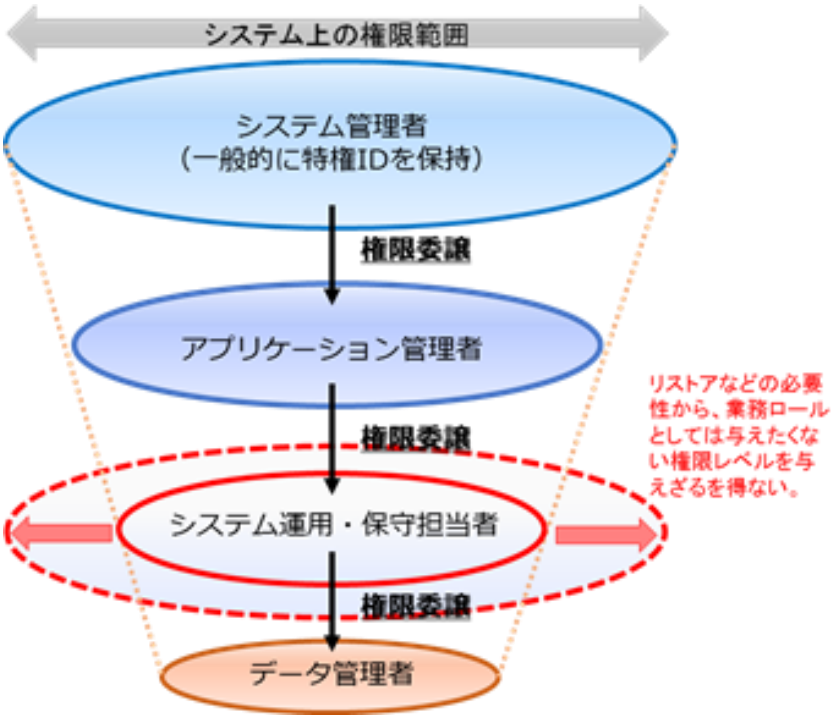


図 1-3 システムのレイヤと特権 ID の影響範囲

第 2 章　特権 ID 管理の課題と管理策

2.1.　特権 ID に関わるリスク

本章では、特権 ID に関わるリスクとその管理策について述べる。特権 ID は利用者にとっては便利に利用できる一方、特権 ID 特有のリスクが存在する。リスクは一般的に「発生可能性」と「影響度」で評価できるが、本書では特権 ID 特有のリスクを検討するにあたり、構成する要素を「脅威」、「脆弱性」、「資産」に分解して検討を行う。

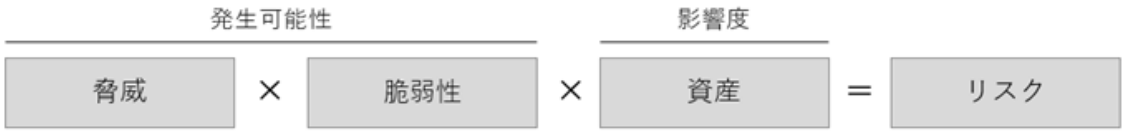


図 2-1. リスクの要素

特権 ID に関わる「脅威」

脅威は一般的に組織側でコントロールすることが難しい要素である。脅威は環境的要因、人的ミス要因、意図的要因を背景に発生するが、特権 ID に関わる脅威としては以下の項目を例として挙げることができる。

種別	脅威の例
環境的要因	✧　システムのクラウド化による攻撃面の増加
人的ミス要因	✧　特権 ID 利用中のオペレーションミス ✧　特権 ID 利用者による機密書類や機密データの紛失
意図的要因	✧　組織に不満を持つ特権 ID 保有社員による内部不正 ✧　マルウェアによる特権 ID／パスワードの摂取

表 2-1. 脅威の例

特権 ID に関わる「脆弱性」

脆弱性は一般的に組織側でコントロールが可能な要素である。本書で対象とする脆弱性、管理策がパッチの適用となるようなソフトウェアバグ等による脆弱性は検討の対象とせず、日々の運用プロセスや組織の慣習に起因して発生する運用の脆弱性を対象とする。特権 ID に関わる脆弱性としては以下の項目を例として挙げることができる。

種別	脆弱性の例
運用不備	✧ 製品にビルトインされているアカウントを使用 ✧ 構築/設定作業時にベンダーが設定したパスワードを継続使用 ✧ 不特定多数のユーザーが使用 ✧ 何でもできる便利なアカウントとして常用 ✧ 連携用として複数のシステムで共有 ✧ 長期間同じパスワードで利用 ✧ 同じパスワードを複数のシステムで使いまわし ✧ 類推しやすいパスワードを設定 ✧ システムの多様化による特権 ID の把握漏れ

表 2-2. 脆弱性の例

特権 ID に関わる「資産」

資産は一般的に組織が守るべき対象を指す。特権 ID に関わる資産としては以下の項目を例として挙げることができる。

種別	資産の例
内的	✧ 特権 ID 利用者がアクセスできる機密情報 ✧ 特権 ID 利用者が設定したシステム設定
外的	✧ 組織が提供するサービス

表 2-3. 資産の例

特権 ID に関わる「リスク」

ここまでに列挙した脅威、脆弱性、資産を元に、特権 ID に関わるリスクを洗い出すことができる。特権 ID に関わるリスクは、セキュリティの 3 要素である機密性、完全性、可用性に加えて、組織のイメージ毀損や評価・評判の低下といったレピュテーションに対するリスクにも波及する。

種別	リスクの例
機密性	✧ 機密情報・個人情報などの利用価値のあるデータの窃取
完全性	✧ 誤ったデータ変更
可用性	✧ 想定外のサービス停止
レピュテーション	✧ 組織のイメージ毀損や評価・評判の低下

表 2-4 リスクの例

特権 ID 特有のリスクを、それらの発生要素である「脅威」、「脆弱性」、「資産」の要素で整理すると以下の通り整理することができる。

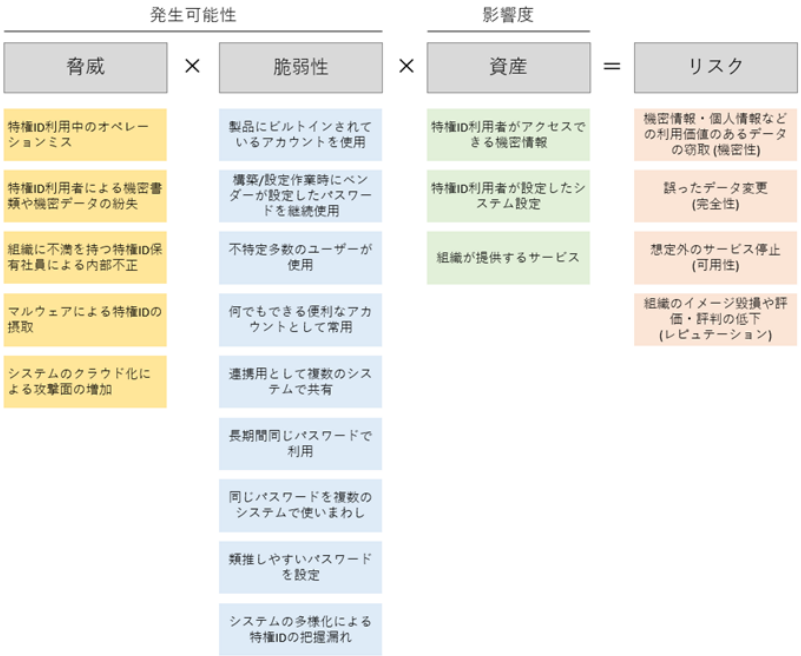


図 2-2 「脅威」「脆弱性」「資産」の整理例

次にリスクを構成する３つの要素のうち、組織側でコントロールが可能な要素である「脆弱性」毎にその背景と対策を述べる。

2.1.1. ビルトイン管理者アカウントの利用

ネットワーク機器やアプライアンス機器、OS も含めたソフトウェアなどの製品には、出荷時から組み込まれた特権 ID が用意されており、多くの場合は、それらのアカウントを利用して最初の構築を行う。出荷時から組み込まれた特権 ID はその利用場面の性格上、すべての権限をもっており、通常の運用には不要な権限も含まれているが、便利なためそのまま運用フェーズでも利用し続けてしまうことが考えられる。

また、最近の製品はセキュリティの観点から、新規の管理者用 ID や権限分掌、監査用 ID 設定などの機能が実装されているが、あらたに特権 ID を設定すると管理上の手間が多少なりとも発生するため、運用フェーズでもそのまま組み込みの特権 ID を使い続けてしまうことが考えられる。

内容	**製品にビルトインされている特権を持った ID は、初期パスワードを含めインターネット上に情報として公開されてしまっていることが少なくない。** **設定・構築のため、すべての権限をもった特権 ID のため、運用時において必要以上に権限を付与してしまう。**
理由/背景	**あらたに ID を設定することに手間がかかる** **設定した特権 ID の利用頻度が低いため、失念してしまう恐れがあるのでマニュアルにも記載されている ID を利用したい。** **製品上、設定できない仕様となっている。**
対策	**パスワードは初期値から必ず変更（空白＝NULL の場合は設定）する** **システム上、無効化が可能な場合はビルトインの特権 ID を無効化する** **パスワードの持ち主を決め、変更後のパスワードをわからないように隠匿する**

表 2-5 ビルトイン管理者アカウントの脆弱性

2.1.2. 構築/設定作業時パスワードの継続利用

開発業者、構築業者に作業を依頼し、作業に利用していた特権 ID をそのままの設定で使い続ける、逆に運用フェーズに入って利用するための特権 ID 用パスワードを構築業者に設定依頼しているなどの現状が見受けられる。大規模なプロジェクトであれば開発環境と本番環境が厳密に管理され、前述のようなことはあまりないと考えられるが、小規模であるもののサーバー台数が多い割に管理者が少人数な場合などに起こりがちである。障害が発生した場合に、業者にすぐにシステムへアクセスし調査を依頼したいなどの事情もあり、構築時の設定をそのままにしておくようなケースも考えられる。

内容	**パスワードを知っているベンダー側のエンジニアの把握が困難になる。そのため、パスワードがどのように伝搬するか制御ができない。別の作業時に勝手にアクセスされても把握がしにくい状況に陥る。**
理由/背景	**変更することが手間である。** **変更することが必要であることを失念していた。** **いざという際にベンダーに調査を依頼したいのでそのままにしておきたい。** **パスワードの管理をベンダーに任せている。** **ID/パスワードを払い出す仕組みがない。**
対策	**作業ごとに ID を払い出し、作業墓はベンダーに払い出した ID を無効/削除する、もしくはパスワードを変更するなどの運用を行い、意図しないところでアクセスされることを防ぐ**

表 2-6 構築/設定作業時パスワードの継続利用時の脆弱性

2.1.3. 不特定多数の利用者

特権 ID は一般 ID とは異なるライフサイクルを持つ面もあり、システムのライフサイクルの中で管理者の変更が発生するなど運用上の理由から、完全な共有利用の排除は困難である。また、管理を担当するユーザー毎に改めて管理用特権 ID を発行する手間や、特権 ID を増やすことへの心理的抵抗感もあり、システムにあらかじめ用意された特権 ID の管理を担当するメンバーで共有しているケースは多く見受けられる。

内容	ID を共有してしまうと、実際に誰が利用したか把握できなくなる。万が一不正アクセスが起きた場合、利用者の特定が困難である。
理由/背景	管理者個別に ID を発行することが手間である。 特権を持った ID を多く発行することに抵抗がある。
対策	一般ユーザーとしてログインした後、特権を付与する機能（sudo や runas）を活用する。 貸し出しの管理台帳で管理する。

表 2-7 共有 ID による不特定多数利用による脆弱性

2.1.4. 特権 ID の常用

運用上、特権が不要の場合でも常に特権 ID でアクセスしているケースである。「管理者が操作（オペレーション）毎に ID を使い分けることが煩わしい」など操作性/利便性による特権 ID を常用の背景が考えられる。

内容	何のためにその特権 ID でアクセスしてきたのか特定することが困難。 アプリケーション・プログラムがアクセスする ID と同様の ID で管理者がアクセスした場合にアクセスの要因をトレースすることが困難。 オペレーション上不必要な権限を持つ ID の利用による人的ミスで障害を誘発する可能性が高まる。
理由/背景	オペレーション（作業）ごとに ID を使い分けるには手間がかかる。 アプリケーション・プログラムも特権 ID アカウントを利用しているため、あまり意識していない。ID を分けるにしても、アプリケーションごとにどのような権限を与えれば良いかわからない。利用のたびに特権 ID の利用申請を行うことが面倒である。
対策	特権を持つ ID を付与するユーザーは必要最低限とする。 複数名での ID の使い回しをやめる。 あらかじめ想定できるオペレーション権限を策定し、適切なタイミングで適切な管理者に対してのみ最低限の権限を付与する。

表 2-7 特権 ID 常用による脆弱性

2.1.5. システム連携用 ID

古くに開発され、実装されたシステムで見受けられるケースである。システム自体に連携用 ID として相手側の特権 ID を埋め込んでしまっているような実装になっているため、容易に変更ができない。さらには認証用のパスワードまで埋め込んでいる場合、パスワード変更すらできず、他のシステムまで影響を及ぼしていることが考えられる。このケースの場合、残念ながらシステムの改修や更新のタイミングで是正する以外に対処はできないものとなる。

内容	**ID とパスワードが連携対象のシステム側にわたるため、そこからパスワードが漏えいする可能性がある。** **複数のシステムで特権 ID を共有してしまうと、パスワードの変更に対応できない使い方をするシステムが一つでも存在する場合、パスワードの変更そのものが困難になり、漏えいのリスクが高まる。**
理由/背景	**連携用の ID の利用ルールを事前に定めておらず、それぞれ勝手にパスワードまでプログラムに書き込んでしまっている。** **他システムで、処理に必要な権限を把握しておらず、特権 ID でとりあえずなんとかしたい。** **連携用 ID に求められる権限が分かっていたとしても、専用 ID を準備できない。**
対策	**パスワードを使う場合は、定期変更可能な実装を行い、パスワードの変更プロセスを決めておく。あるいは、証明書認証を使い証明書の更新プロセスを決めておくなど連携用 ID の利用ルールを事前に決める。** **パスワードを補完する場合は、暗号化やファイルへのアクセス制御などを行う。**

表 2-8 システム連携用 ID 利用による脆弱性

2.1.6. 特権 ID へ設定するパスワード

特権 ID に設定するパスワード運用に当たっての問題点は、一般 ID との本質的な違いはそれほど大きく無いが、「特権 ID そのものを共有されることが多い」、「ビルトインされている特権 ID である」という前述の運用と組み合わされて課題が顕著に現れると考えられる。特権 ID のパスワードの設定状況の例を次にあげる。

・　　長期間同じパスワードで利用している
・　　複数のシステムの特権 ID に同じパスワードを設定している
・　　特権 ID に簡単な（類推しやすい脆弱な）パスワードを設定している

2.1.6.1.　長期間同じパスワードでの利用

特権 ID を長期間同じパスワードで運用している背景として、「一度設定したパスワードを変更すると周知に手間がかかる」、「変更した際のシステムへの影響度が不明なため、変更できない」などの理由が考えられる。一つ目の課題は、特権 ID を複数名で共有していることで原因として挙げられる。

内容	**異動や退職により、管理者の任が解かれた人がアクセスできる手段を知っている状況になる。トラブルによる退職者の逆恨みによる不正アクセスの事件などが実際に起きている。**
理由/背景	**一度設定したパスワードを変更すると周知に手間がかかる。** **変更した際のシステムへの影響度が不明なため、変更できない。** **管理対象のサーバーやシステムが多く、定期的にパスワードを変更するという運用が出来ない。**
対策	**パスワード自体を解読される可能性を減らすため、または解読される、知られてしまったため進入を許すなどの被害を最小限に抑えるという点で、パスワードの利用後に変更（使い捨て）することが有効である。** **連続したアクセス試行に回数制限を設定する方策も有効である。**

表 2-9 長期間同じパスワード利用による脆弱性

2.1.6.2.　複数システムの特権 ID に対して共通のパスワードを設定

サーバーやネットワーク機器などが数十台ある場合、それぞれで異なるパスワードを設定するには、その分「パスワードを考える必要がある」、「覚えきれない」など管理に手間がかかる。そのため共通のパスワードを使いまわしてしまいがちである。

内容	一つのシステムの特権 ID のパスワードが漏れてしまうと、複数のシステムの特権が奪われることになる。
理由/背景	それぞれのシステムで個別に特権 ID のパスワードを設定すると管理に手間がかかる。
対策	各システムで個別のパスワードを設定することで被害を最小限に食い止めることができる。パスワードの一部にホスト名の頭文字をつけるなど、使い回しを防止しながらも管理しやすい生成ルールを考える方法などがある。

表 2-10 複数システムの特権 ID に対して共通のパスワードによる脆弱性

2.1.6.3. 類推しやすいパスワードを設定

特権 ID に限った問題ではないが、前述の複数名での共有している問題とも関連し、覚えやすい簡単なパスワードを設定してしまうという背景が考えられる。

内容	インターネット上には、パスワード解析のためのツールや辞書が出回っており、脆弱なパスワードではすぐに解読されてしまう可能性が高く、不正アクセスを防ぐ効果が下がる。
理由/背景	特権 ID に複雑なパスワードを設定すると失念してしまう。 システムの仕様でパスワードに設定可能な文字種や文字数の制限がある。
対策	類推しにくいパスワードを設定する（SplashData 社”Worst Passswords” List 等にランクインしているパスワードは設定しない）。複雑さを維持しながら管理しやすいパスワード生成方法などを利用して、パスワードを設定する。システム仕様上の制限がある場合は、ネットワークや物理的（サーバールームへの入退室）な制限を組み合わせて管理する

表 2-11 類推しやすいパスワード利用による脆弱性

2.1.7. システムの多様化による特権 ID の把握漏れ

各種システムのクラウド化やデジタルトランスフォーメーション（DX）化によるクラウドサービス（IaaS、PaaS、SaaS）の急速な利用に伴い、IAM ユーザーに代表される特権 ID を保有するユーザーが乱立する事態が考えられる。その場合、特権 ID を適切に把握し管理することが難しくなる。

内容	特権 ID が乱立することで、把握できていない特権 ID が存在してしまう可能性がある。把握できていない特権 ID は、利用者の管理やパスワード変更といった管理運用の対象外となってしまう。
理由/背景	クラウド利用に不慣れなシステム管理者がクラウド特有の特権 ID を十分に理解しないまま恣意的に利用している場合に発生する。また、SaaS の利用拡大によりサービス利用者が特権 ID を利用している状況も考えられる。
対策	特定のユーザーのみに特権 ID を払い出すことが効果的である。また、二要素認証による本人確認の強化も効果的である。

表 2-12 システムの多様化による特権 ID の把握漏れによる脆弱性

2.2. 特権 ID の管理策

2.2.1. 理想と現実のギャップ

本来は、特権 ID の権限を細かく分割し、特権の利用を開始するタイミングで作業や操作に最低限必要な「コマンド」や「データ」のみの権限を付与し、利用を終了するタイミングで権限を剥奪することにより、誤用・乱用・故意によるシステムへの影響、情報漏えい等を最小限に抑えることが望まれる。

最小特権や強制アクセス制御等を実現する方法として Trusted OS の導入があるが、現在のところ、実際に利用されるケースはあまり多くない。サービス追加やシステム変更等を行う際の煩雑さ、対応するプラットフォームの少なさが、Trusted OS が利用されない要因の一つとして考えられる。

また、特権 ID 利用者（管理者）が少ない場合、特権 ID 利用者は複数の権限の ID を利用するため、権限を細かく分割しても効果が少ないと思われる。

2.2.2. 特権 ID の管理策のポイント

特権 ID は、システムの維持（メンテナンス）に利用されるため、管理者/作業者に必要なアクセス権を付与する必要がある。一方で、必要以上の権限を付与してしまうことによる誤用や乱用を防止する対策/管理策が必要である。

実際にはシステムにあらかじめ組み込まれた特権 ID を複数の管理者/作業者が共有して運用されているケースが多く見受けられる。システムに組み込まれた特権 ID の共有を避け、管理者、作業者それぞれのアカウントを作成して運用すべきである。少なくともいつ誰が特権 ID を利用してアクセスしたか履歴の管理が必要である。また、特権 ID を利用する際には、正しい手続きとして、利用者の申請と作業範囲と内容の把握、それらに対する承認・許可の一連のフローが必要である。

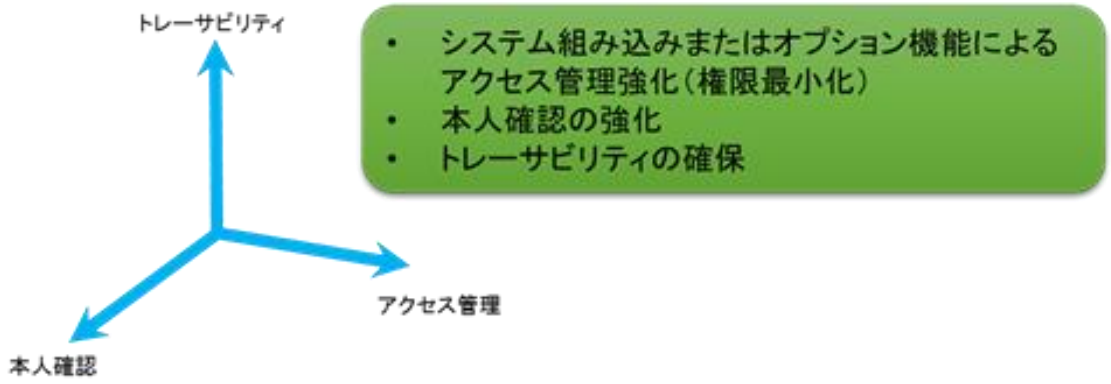


図 2.3 特権 ID の管理策のポイント

2.2.3. 特権 ID の利用における現状と管理策の関係

前項「2.1 特権 ID に関わるリスク」であげた 6 つの利用の現状と管理策のポイントの関係性を確認する。

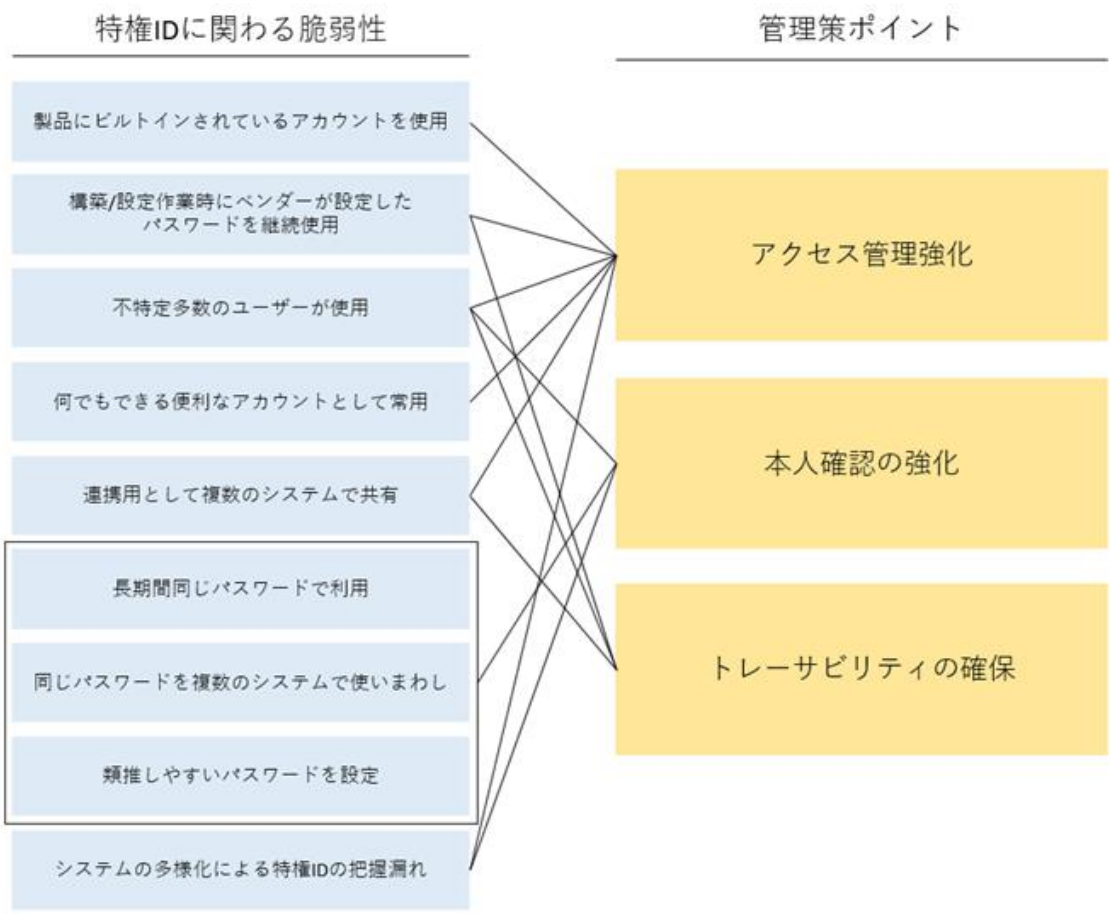


図 2.4 特権 ID に関わる脆弱性と管理策ポイントの関係

2.2.4. アクセス管理の強化

特権を利用するシステムへのアクセスを強化するための方法としては、社屋や部屋へのアクセスを制御する「物理的なアクセス強化」と、ネットワーク機器やアプライアンス機器、OS も含めたソフトウェアなどの製品に対してアクセスを制御する「システムによるアクセス強化」がある。これらの方法を効率的に組み合わせて対策することが効果的である。

アクセス強化方法	アクセスを制御するための方法例
物理的なアクセス強化	ビル、データセンターの入退場を管理する
	サーバールームへの入退室を管理する
	システムを利用できる端末を限定する
システムによるアクセス強化	端末のログインユーザーを限定する。
	特定のユーザーのみに特権を付与する。
	特権を利用する度に認証情報を変更する。

表 2-2 特権を利用するシステムへのアクセスを強化するための方法

2.2.4.1. 物理的なアクセス強化

現在、オフィスビルやサーバールームへのアクセス管理は、入退時に実施することが多い。オフィスビルでは、出入り口で入退場ゲートや警備員による社員証の認証を行い、適切な人間のみを社屋へ入ることを許可する。また、サーバールームでは、鍵やICカードによる入退管理を実施し、適切な人間のみをサーバールームへ入ることを許可する。

機密性の高い情報を管理している施設については、指紋、静脈、虹彩、顔などによるバイオメトリクス（生体）認証が使われることもある。

2.2.5. 本人確認の強化

パスワードによる認証は、ほとんどのシステムで搭載されており、導入が容易であることから、多くの環境において利用されている。しかし、パスワードの漏えい（盗み見、パスワード攻撃、パスワード管理の不備など）により不正に利用されるリスクも大きい。その結果、本人確認の正確性において、問題が生じる危険性がある。

セキュリティ事故が発生した場合、正確な本人確認ができないと、調査が遅れるだけではなく、被害が拡大する危険性がある。特に特権IDに関しては、影響がさらに大きくなる。また、特権IDの利用はシステムへの影響が大きいことから、監査においても本人確認の正確性が要求されるケースが多い。

本人確認を強化する手段の例として、多要素認証(二要素認証)による本人確認が挙げられる。

最近では、スマートフォンのアプリケーションを利用した本人確認の手法などが提供されている

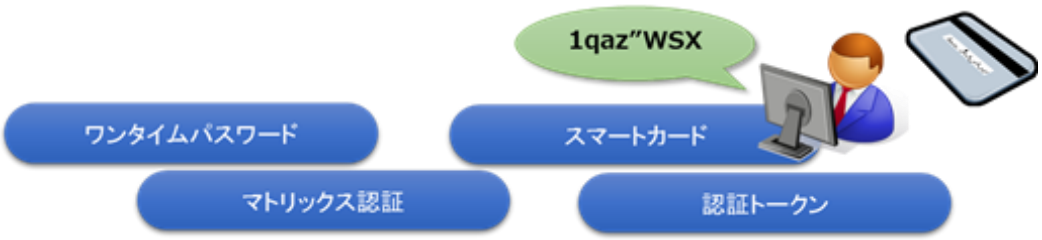


図 2.5 本人確認の方法

2.2.6. トレーサビリティの確保

平常時は、特権 ID が適切に利用されているか監査でき、非常時には事故の究明のためにトレーサビリティの確保が重要である。同時に故意による不正に対する抑止力としての位置づけとしても重要である。

トレーサビリティの確保の手段としては、特権 ID の貸出し記録台帳などを用意し運用にて人手を介して行う方法や、システムを導入する方法が考えられる。システムと運用チームが小規模であれば、費用対効果の面で記録台帳を使った運用でも良いが、システムが大規模または運用を担当するメンバーが大人数で業者などの他社の担当者もかかわるような場合は、トレーサビリティの確保のみならず運用コスト、監査コストを低減するためにも、特権 ID を管理するシステムの導入が不可欠である。

特権 ID 管理システムには、作業者および作業端末と作業対象となるシステムの間にゲートウェイとして配置し、制御を行うタイプ、作業端末に導入するタイプ、特権 ID 管理対象のサーバーに導入するタイプなどがあげられる。これらは基本的に、いつ誰がどのサーバーにアクセスしたかを作業時のログを記録し、保存している機能を持っており、トレーサビリティの確保が可能となっている。非常時の事故究明のために

は、作業内容を記録し、保存しておくことも重要である。なお、特権 ID 管理システムの詳細は本ガイドラインの「実践編」を参照いただきたい。

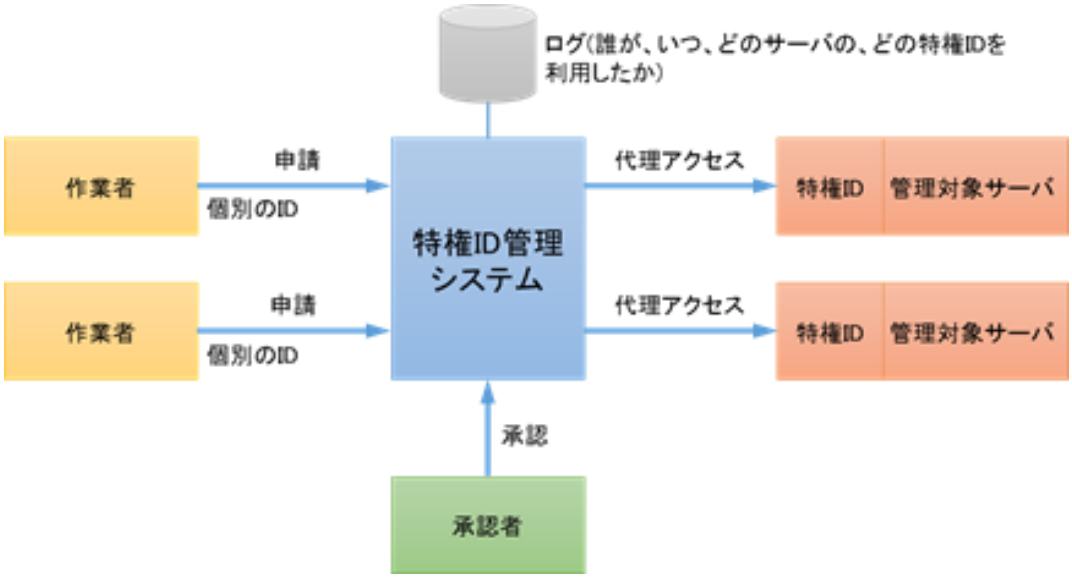


図 2.6 特権 ID システムの概要

第３章インシデント事例集

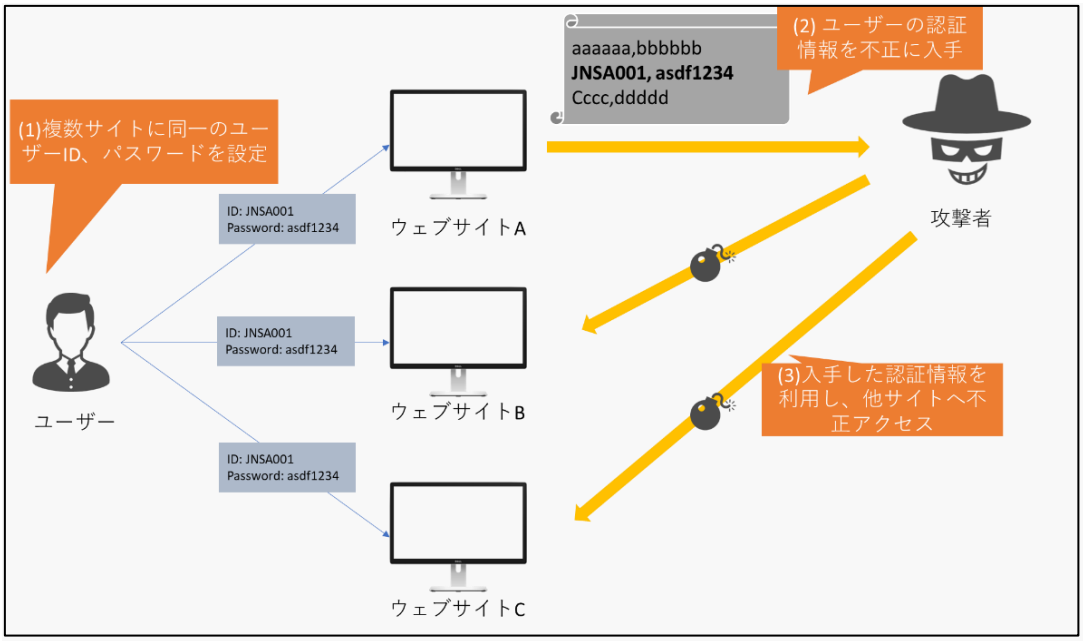
3.1　ネットワーク機器への攻撃事例

2022 年 5 月、シスコは従業員が利用する Google Chrome ブラウザに保存された認証情報が漏洩したことに起因したセキュリティ侵害を受けた。シスコの従業員は、シスコ社で利用する認証情報を個人的な Google アカウントでログインした Google Chrome ブラウザに保存して利用していた為、シスコ社で利用するパスワードがプライベートの Google アカウントに同期されている状態であった。攻撃者は、シスコの従業員のプライベートの Google アカウントを侵害することに成功し同期されていた認証情報を取得し Cisco VPN への認証に成功した事例である。

引用元：Cisco Talos shares insights related to recent cyber-attack on Cisco
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html

3.2　パスワードリスト攻撃の事例

パスワードリスト攻撃について、攻撃手法ならびに実際のインシデント事例を紹介する。パスワードリスト攻撃は主にインターネットに公開されているウェブサイトに不正にアクセスするための攻撃手法の一つである。攻撃者は何らかの不正な手段を用いて入手した認証情報のリストを攻撃に利用する。このリストの入手手段は様々なもの存在するが、不正アクセス先のウェブサイトとは異なるサイトの脆弱性を利用して入手するなどが考えられる。ランダムにパスワードを試行する総当たり方式と異なり、実際に使われているユーザーID とパスワードを用いるため、ログイン成功の確率が高いといった特徴が挙げられる。特にウェブサイトの利用者が複数サイトで同一の ID/パスワードを使いまわしている場合に、攻撃の成功率が上昇する。そのため、本攻撃に対する対策として、サイト間でのパスワードの使いまわしをしないことが有効である。



パスワードリスト攻撃による実際のインシデント事例として、株式会社ニトリホールディングスが提供する「ニトリアプリ」サービスにて発生した事例が挙げられる。攻撃者はニトリアプリからニトリアプリの認証プログラムに対し、不正に入手した大量のユーザーID（メール アドレス）とパスワード情報を用いて、アクセスしたことが確認されている。これにより、約 13 万 2,000 アカウントについて、個人情報を閲覧された可能性があるとされている。

引用元：「ニトリアプリ」への不正アクセスによる個人情報流出の可能性に関するお詫びとお知らせ

https://www.nitorihd.co.jp/news/items/644dc27180ca40016761ce9c03d0f201_172.pdf

3.3 Web サイトの改ざん事例

2019 年 1 月 10 日に和歌山県の当時 南紀白浜観光局（現 南紀白浜観光協会）は、ホームページが何者かに不正アクセスされ、不正な書き込みをされる被害を受けたと発表した。発表によると 2018 年 12 月 31 日～2019 年 1 月 1 日にわたり、不正な書き込みが行われるなどの被害が確認された。その後、復旧した 1 月 10 日に発表されたサイバー攻撃の事例である。

引用元：ホームページ改ざんに関するご報告とお詫び：南紀白浜観光協会

http://www.nankishirahama.jp/news/detail.php?news_id=111

一部報道では、サイトは CMS で構築されており、その管理画面に対して、外部から管理者の ID とパスワードを利用され、顔写真や児童ポルノなど無関係の内容が掲載されるという被害に遭ったとされている。また、当時の南紀白浜観光局は公式の発表では触れられていないものの、この事件で悪用された管理者 ID とパスワードは推測が容易（ログイン ID：nanki、パスワード：shirahama）にできるものが設定されており、管理者画面の URL とともに、掲示板サイトに投稿されインターネット上に晒されていたと言われている。

引用元：2019-01-16 南紀白浜観光局の Web サイト改ざんについてまとめてみた

https://piyolog.hatenadiary.jp/entry/20190116/1547586873

このことが事実であるとすると、攻撃者はパスワードクラッキングもそれほど時間がかからず成功し、管理者権限を奪取できたと考えられる。

Appendex　各種標準化基準による特権 ID 管理

PCI DSS v4.0

以下は「Payment Card Industry データセキュリティ基準 要件とテスト手順 v4.0」（PCI Security Standards Council, LLC. 2022 年 3 月）における特権ユーザー関連と思われる要件について紹介するものである。原文には各要件の目的やテスト手順などが詳細に記述されていること、また特権と関連性のある記述が他にも存在すること（例．ベンダーのデフォルトアカウントユーザーテムアカウントに関する記述など）から、詳細は原文を参照いただきたい。

要件 7：システムコンポーネントおよびカード会員データへのアクセスを、業務上必要な適用範囲（Need to Know）によって制限する
7.2　システムコンポーネントやデータへのアクセスが適切に定義され、割り当てられている。
7.2.2 特権ユーザーを含むユーザーには、以下に基づいてアクセスが割り当てられます。 ・　職務分類と機能。 ・　職責を果たすために必要な最小限の特権

要件 8：ユーザーの識別とシステムコンポーネントへのアクセスの認証
8.2　ユーザーと管理者の識別と関連するアカウントは、アカウントのライフサイクルを通じて厳密に管理されている。
8.2.2　グループアカウント、共有アカウント、汎用アカウント、またはその他の共有された認証情報は、例外的に必要な場合のみ使用し、以下のように管理される。 例外的に必要な場合を除き、アカウントの利用を禁止する。 ・　使用は例外的な状況に必要な時間に制限される。 ・　使用を正当化するビジネス上の理由が文書化されている。 ・　使用は、経営陣によって明示的に承認される。 ・　アカウントへのアクセスが許可される前に、個々のユーザーの身元が確認される。 ・　実行されたすべてのアクションが、個々のユーザーに起因するものである。

要件 10：システムコンポーネントおよびカード会員データへのすべてのアクセスをログに記録し、監視すること
10.2　異常や疑わしい活動の検出および、イベントのフォレンジック分析をサポートするために、監査ログが実装されている。
10.2.1.5　監査ログは、以下のような識別情報および認証情報へのすべての変更を記録する。 ・　新しいアカウントの作成 ・　特権の昇格 ・　管理者アクセス権を持つアカウントに対するすべての変更、追加、または削除

ISO 27001 での特権管理

以下、特権ユーザー、その管理について記載された要件である。それぞれの項目の詳細においては、各文書の原文を参照のこと。

ISO/IEC 27001:2013

情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項

(Information technology -- Security techniques -- Information security management systems – Requirements)

情報セキュリティマネジメントシステム（ISMS）適合性評価制度は、国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者適合性評価制度である。

ISMS 適合性評価制度において、第三者である認証機関が本制度の認証を希望する組織の適合性を評価するための基準である ISO/IEC 27001:2013 において特権管理に関しての要件を紹介したものである。項目の詳細においては、原文を参照いただきたい。

ISO Standards (https://www.iso.org/isoiec-27001-information-security.html)

一般財団法人日本規格協会の書籍販売サイト（https://webdesk.jsa.or.jp/）

A11.2.2 特権管理
管理策： 特権の割り当て及び利用は、制限し、管理することが望ましい。

システム管理基準(平成 30 年 4 月 20 日)

本基準は、どのような組織体においても情報システムの管理において共通して留意すべき基本的事項を体系化･一般化したものである。 以下はシステム管理基準においての特権アクセス管理、ログ管理の項目を紹介したものである。項目の詳細においては、原文を参照いただきたい。

経済産業省 システム監査制度について

https://www.meti.go.jp/policy/netsecurity/sys-kansa/

Ⅴ．運用・利用フェーズ
3.2 アクセス管理 (1) 運用管理者は、情報セキュリティ方針に基づいて、運用システムへのアクセス管理ルールを作成し、情報システム部門長の承認を得て、適切に運用すること。 (2) 運用管理者は、データへのアクセスコントロール及びモニタリングを、実施すること。 (3) 上記以外のアクセス管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。
5.ログ管理 (1) 運用管理者は、ログを取得し、定期的に分析すること。

システム管理基準　追補版（財務報告に係る IT 統制ガイダンス）

財務報告に係る内部統制の整備運用に際して、「システム管理基準等」に基づいて構築されている情報システムを活用し、 財務報告に係る内部統制で求められている「IT への対応」を行っている、行うとしている企業において、 「システム管理基準等」と「IT への対応」との間の具体的な対応関係を明らかにする必要があり、そのような企業に対して、主要なケースを想定しつつ、IT 統制に関する概念、 経営者評価、導入ガイダンス等を提供するものである。

以下はシステム管理基準　追補版においての特権 ID 管理の項目を紹介したものである。項目の詳細においては、原文を参照いただきたい。

経済産業省 システム監査制度について

https://www.meti.go.jp/policy/netsecurity/sys-kansa/

システム管理基準 追補版
3-(3)-②-ホ 特権 ID の付与にあたっては、担当者や利用期間を限定し、その ID に対応する業務にのみ利用していること。 ・特権については、運用基準があり、特権の付与に際して、最小限にとどめていること。利用が終わって、不要になれば、すぐに特権を停止する。 ・特権IDを調査して、正しい職務に適切に付与されていることを確かめる。 ・特権IDが、すべての機能を利用できる場合には、スプリットパスワードや相互監視等（ デュアルコントロールとも呼ばれる）の別の統制が併用されていることを確かめる。

NIST SP800-53 Rev5

組織と情報システムのためのセキュリティおよびプライバシー管理策

Security and Privacy Controls for Information Systems and Organizations

組織およびシステムのセキュリティとプライバシーの要件を満たすための包括的かつ柔軟なガイドであり、変化する脅威、脆弱性、要件、および技術に基づいて、現在および今後の保護ニーズを満たすセキュリティおよびプライバシー管理策を含む包括的かつ柔軟なカタログを提供している

以下は NIST SP800-53 Rev5 においての特権アクセス管理、ログ管理の項目を紹介したものである。項目の詳細においては、原文を参照いただきたい。

セキュリティ関連 NIST 文書：IPA 独立行政法人 情報処理推進機構

https://www.ipa.go.jp/security/publications/nist/

3.1 アクセス制御
AC-2 アカウント管理 (6) アカウント管理 ｜ 動的権限管理 ［設定：組織が定める動的 権限 管理ケイパビリティ ］を実装する。 (7) アカウント管理 ｜ 特権ユーザーカウント

(a) ［選択：役割ベースのアクセスに関する基本的なスキーム：属性ベースのアクセスに関する基本的なスキーム］に従って、特権ユーザーカウントを作成し管理する。 (b) 特権的役割または属性設定を監視する。 (c) 役割または属性の変更を監視する。 (d) 特権的役割または属性の設定が適切でなくなった場合にアクセスを無効にする。 AC-6 最小特権 (5) 最小特権 ｜ 特権アカウント システム上の特権アカウントを［設定：組織が定める職員または役割 ］に制限する。
3.3 監査 および 説明責任
AU-6 監査記録のレビュー、分析、 および 報告 (8)監査記録のレビュー、分析、および報告 ｜ 特権コマンドの全文分析 システムの物理的に異なるコンポーネントまたはサブシステム、またはその分析専用の他のシステムで、ロギングされた特権コマンドの全文分析を実行する。
3.7 識別および認証
IA-2 識別および認証（組織のユーザー） (1)識別及び認証（組織のユーザー） ｜ 特権アカウントへの多要素認証 特権アカウントにアクセスするための多要素認証を実装する。

あとがき

本書の執筆にあたっては以下のメンバーにご尽力をいただいた。

この場をお借りして謝辞を申し上げる。

【検討・執筆メンバー】

宮川　晃一（WG リーダー）	日本電気株式会社
菊地　周平	CyberArk Software 株式会社
染谷　浩子	CyberArk Software 株式会社
大竹　章裕	株式会社ラック
斎藤　知明	TIS 株式会社
松井　祐輔	日本電気株式会社
吉本　紀浩	デロイトトーマツサイバー合同会社
今堀　秀史	株式会社 SHIFT
金子　敬祐	SCSK 株式会社

（順序不同）

なお、本 WG の活動内容およびメンバーは以下の紹介ページを参照いただきたい。

【デジタルアイデンティティ WG 紹介ページ】

https://www.jnsa.org/active/std_idm.html