製造業DXカンファレンス 2022

OTネットワークに求められる特権ID管理とは

～重要システムの特権を守るベストプラクティスソリューションのご紹介～

2022年1月28日

NRIセキュアテクノロジーズ株式会社
ソフトウェア事業本部
ソフトウェアビジネス三部

和田 真治

目　次

会社情報

（2021年12月1日現在）

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 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		
代表取締役社長	柿木 彰		
取締役	池田 泰徳、柴田 実、竹本 具城、山口 隆夫	監査役	坂田 太久仁
社員数	連結：590名、単体：497名		
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

3つの強み

パイオニアならではの「高い技術力と豊富なノウハウ」に裏打ちされた業界随一の強み

情報セキュリティの
トータルソリューション

企業が直面する情報セキュリティのあらゆる課題を
ワンストップで解決します。

グローバルサポート力

海外のIT事情やレギュレーションにおける知見と、
世界中のNRIグループ拠点を活用し、
企業のグローバル展開を支援します。

最先端の技術と知見

継続的な調査研究と豊富な経験を活かし、最先端で
高品質なセキュリティソリューションを提供しま
す。

主要な提供サービス・製品一覧

（2021年12月1日現在）

コンサルティング

リスクマネジメント
- セキュリティ監査
- 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
- セキュリティ対策レポート
- 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
- マネージド脅威情報分析
- 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
- 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
- サプライチェーン・セキュリティコンサルティング
- MITRE ATT&CKを用いたサイバー攻撃対策の評価

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

PCI準拠支援
- PCI DSS SAQ対応支援
- PCI DSS SAQ準拠パッケージ
- 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

設計開発支援
- 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
- PFIクレジットカード情報漏えい調査

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

IoT/OTセキュリティ診断
- 無線通信セキュリティ診断
- 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
- 車両システムセキュリティ診断

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

マネージドセキュリティサービス・SOC

SOC（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（NeoSOC）

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
- 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運用支援
- 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

公開Web環境 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
- Deep Security管理

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
- Okta
- YubiKey

リモートアクセス
- CACHATTO
- MagicConnect

メール・Webセキュリティ
- m-FILTER MailAdviser
- Proofpoint
- Global Relay Archive
- Incapsula
- Cofense

文書・ファイルセキュリティ
- クリプト便
- POSTUB
- Box
- FinalCode
- Contents EXpert / Digital Form
- Contents EXpert / XML Assist

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

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

リスク分析・可視化
- IntSights
- Recorded Future
- GR360
- RiskIQ
- ObserveIT
- Secure SketCH

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

IoT/OTセキュリティ
- SCADAfenceプラットフォーム

セキュリティ教育・研修

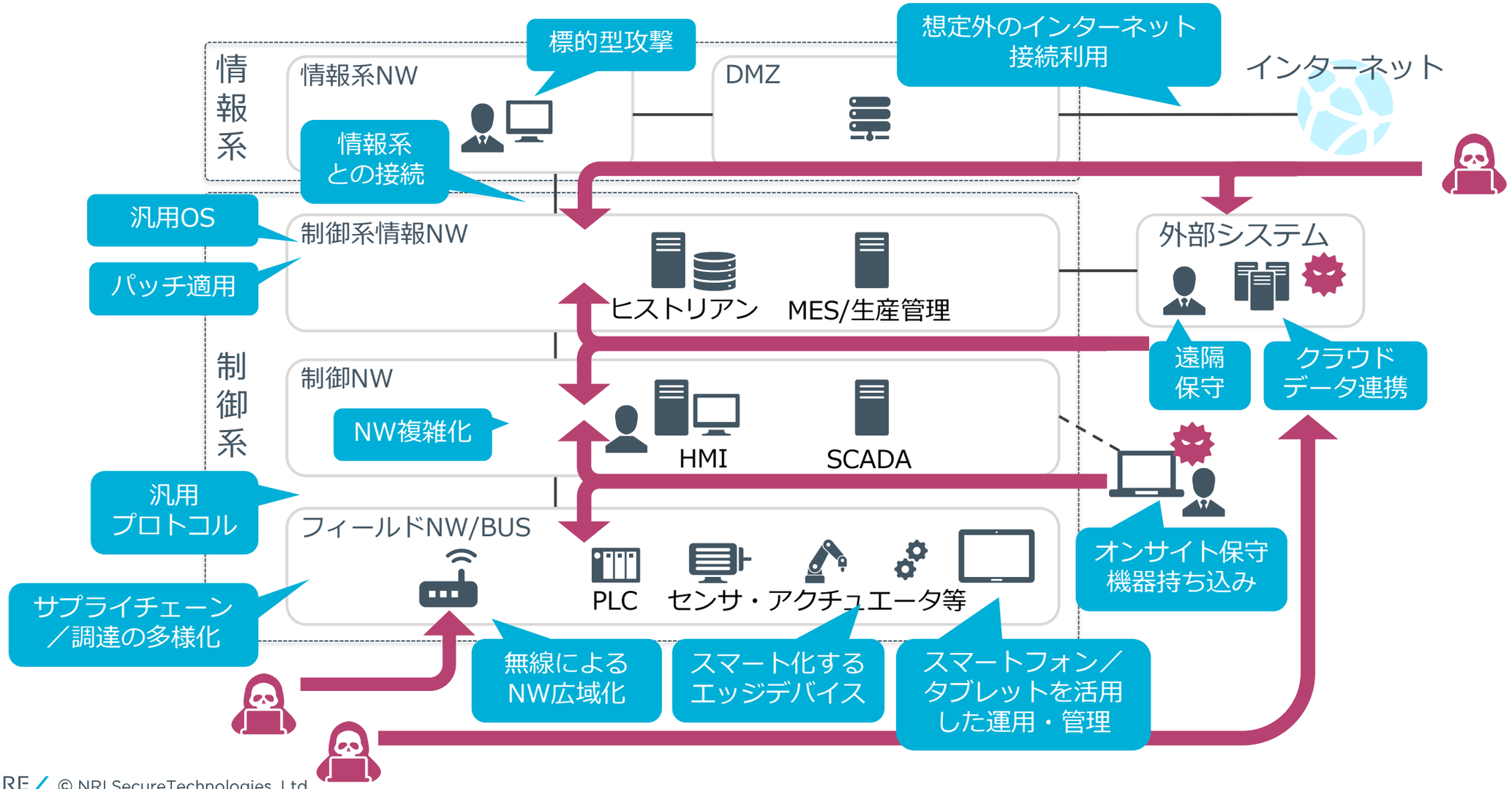
セキュリティ資格取得支援
- SANSトレーニング
- CISSP CBKトレーニング

セキュリティ人材育成
- セキュアEggs

OTセキュリティが必要とされる背景

OTネットワークを取り巻くセキュリティリスク

- 工場の制御システムを安定稼働させるためには、様々なセキュリティリスクの考慮が必要となっている



製造業の変化

- 製造業のインフラの変化・プロセスの変化によりサイバーセキュリティのリスクは大きくなっている

製造インフラの変化

- **ネットワークのオープン化**
  データ連携や遠隔保守を目的とした外部システムとの接続、
  IoT機器やセンサの情報をクラウドに集約、
  社内の情報系システムとの連携、等
- **OS/プロトコルの汎用化**
  独自のOSや通信プロトコルから
  汎用OSやTCP/IPの汎用プロトコルへの移行

製造プロセスの変化

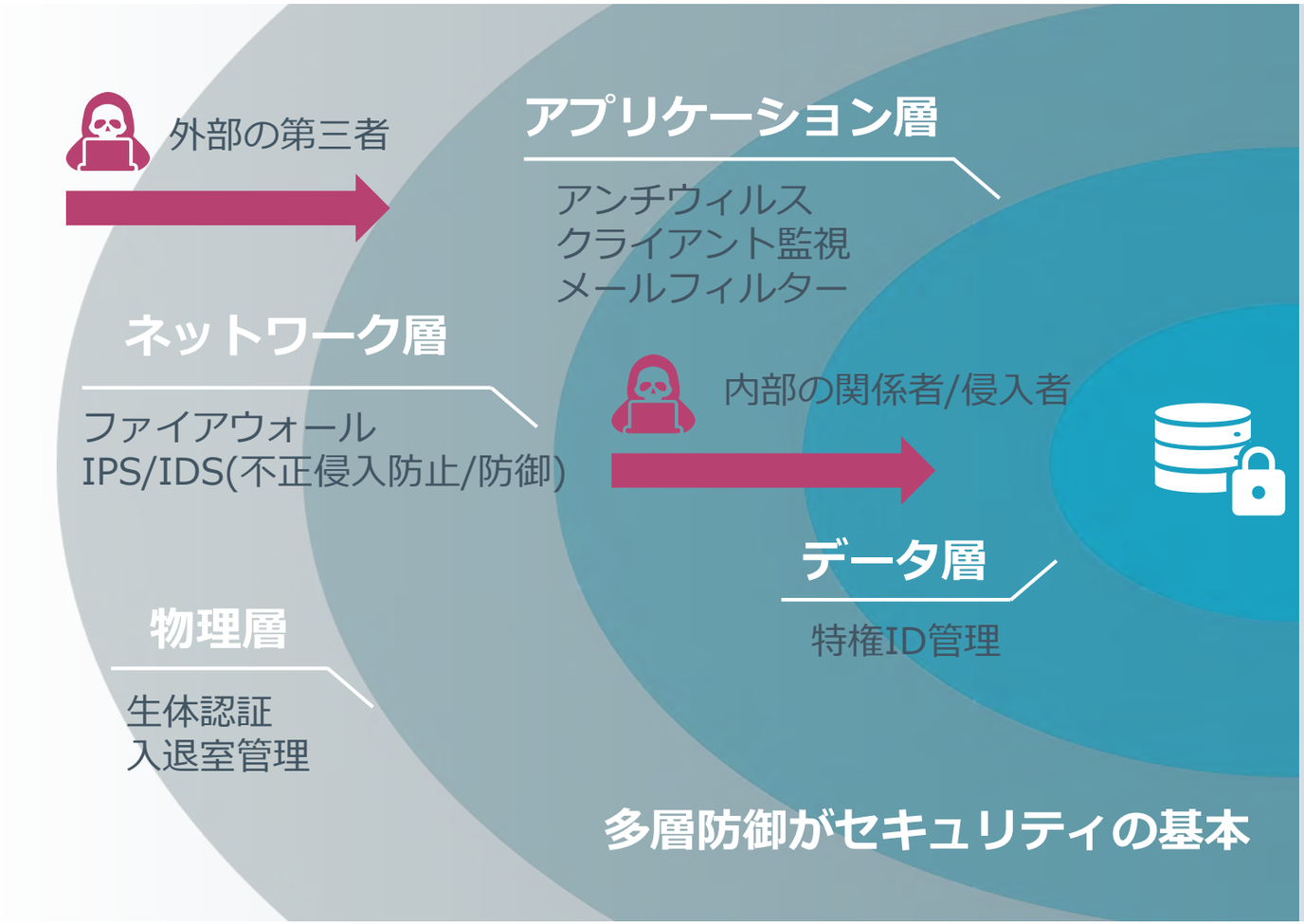
- **テレワーク活用**
  時差出勤、週休3日制の導入など、3密回避が行われる中、
  「事業継続」と「生産性向上」の視点から
  生産現場においても遠隔保守、監視、制御の仕組みを導入
- **プロセス全体のデジタル化**
  設計から管理、製造までをすべてコンピュータが担い、
  品質の維持や製造効率を上げる**DX化**がさらに加速

サイバーセキュリティへの影響

- **脆弱性の増加、攻撃の容易化に**繋がり、**攻撃者に狙われやすくなる**
- **金銭目的のサイバー攻撃(ランサムウェア)が増加**しており、
  ランサム(身代金)要求に応じやすい標的として、**製造業が狙われやすくなっている**

まず対策するべきセキュリティリスクとは

- 最優先で対策が必要となるのは、外部攻撃や内部不正で第一に狙われる「特権ID」の管理



外部攻撃や内部不正で一番に狙われるのが

・どんな情報にもアクセスできる

・どんな操作も可能である

システムの最高権限を持つ「**特権ID**」

OTネットワークを守る最後の砦として

特権ID管理は必須

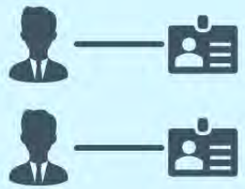
特権ID管理とは

特権IDとは

- システムの維持・管理のために用意された、システムに大きな影響を与えられる権限を持つアカウント

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

情報の搾取

データ改ざん・消去

システム破壊

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ー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

特権IDの不正利用によって、**多大な損害**をもたらす原因になりえる

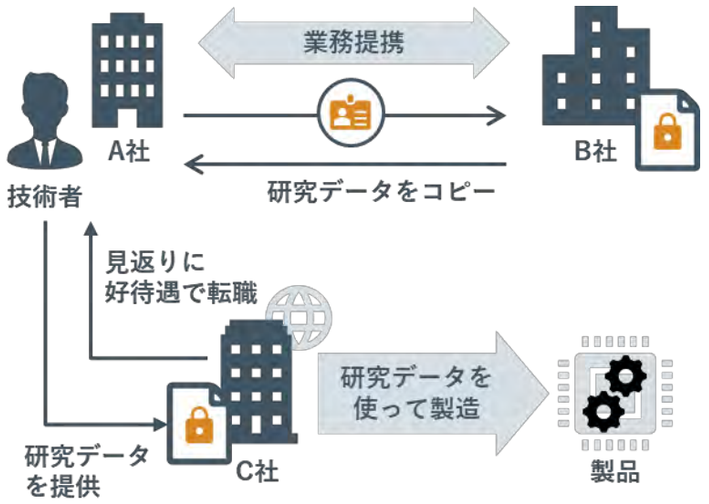
製造業における特権ID管理の課題

- 製造業のお客様からは以下のようなお問い合わせをいただいている

企業規模（従業員数）	実際に問い合わせいただいた特権ID管理にまつわる課題
10,000人以上	各拠点や工場から集めてくるログ形式の統一による**監査対応の効率化**
10,000人以上	電力系の**監査への対応**（工場内の情報LANから制御LANへの通信制御）
1,000~4,999人	**監査法人からの指摘**
10,000人以上	**クラウドサービスの特権ID管理**が新たに必要となった
10,000人以上	**海外拠点までの内部統制**を聞かせ、情報漏洩や**ランサムウェア**の被害を防ぎたい
1,000~4,999人	**工場におけるサイバー攻撃**の実害事例も後を絶たないが、自社も被害を受けないか心配

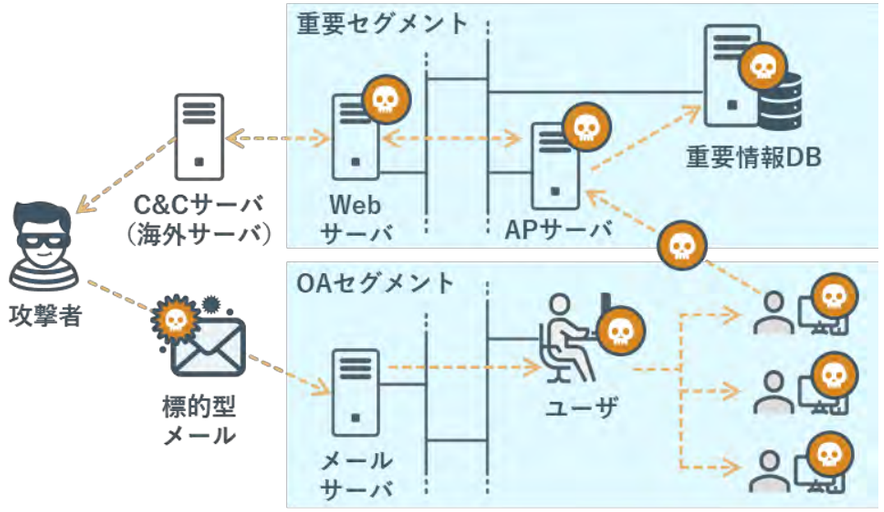
特権IDの不適切な管理による不正利用の例

- 近年、製造業においてもセキュリティインシデントは増大傾向



特権の濫用の例

自身に与えられたアクセス権を利用し、提携先の研究データを不正に持ち出し、転職先の海外企業へ漏えいした事件。この技術流出の後、B社とC社の技術格差は急速に縮まったとされている。



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の不適切な管理がもたらす損失

- 特権IDを悪用されることで、ビジネス活動に支障を来すのはもちろん、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、中長期的に多大な損失が生じる
- 重要なインフラやサービスへの侵入は、事業収益の損失だけでなく人命を脅かす被害をもたらす恐れもある

安全性	生産ライン暴走	➡	人命に関わる事故
可用性	生産ライン停止	➡	出荷停止
完全性	改ざん、破壊	➡	リコール
機密性	情報漏洩	➡	技術流出

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

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るが、
共通して言えることは4STEPにまとめられる

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

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管理ソリューション SecureCube Access Check を利用したアクセス制御

SecureCube Access Checkの特徴

NRIセキュアが設計・開発する特権ID管理ソリューション

SecureCube Access Check

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。

IT全般統制、J-SOX監査、FISC安全対策基準、金融庁監査、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。

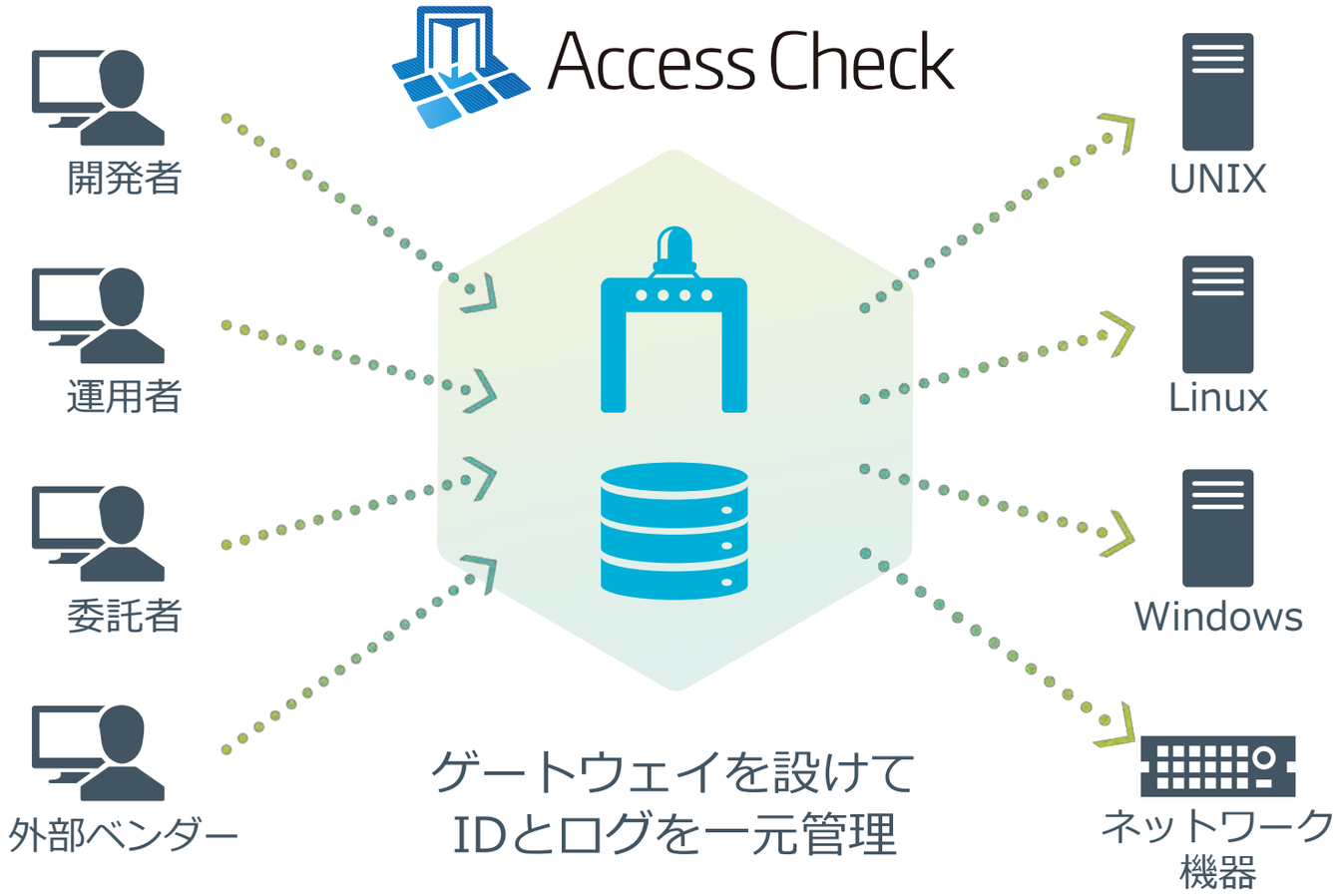
大手金融機関をはじめ、流通業、製造業、サービス業、公共機関など業種を問わず様々なお客様に、ご要件に合わせてご利用いただいております。

※ 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2021」
特権ID管理市場：ベンダー別売上金額シェア（2019年度）
SecureCube Access Check，Cloud Auditor by Access Check が対象

SecureCube Access Checkの特長1

ゲートウェイ型だから
スピード導入

完全エージェントレスで厳格な特権ID管理を実現



エージェントレスで
既存システムへの
影響を最小に

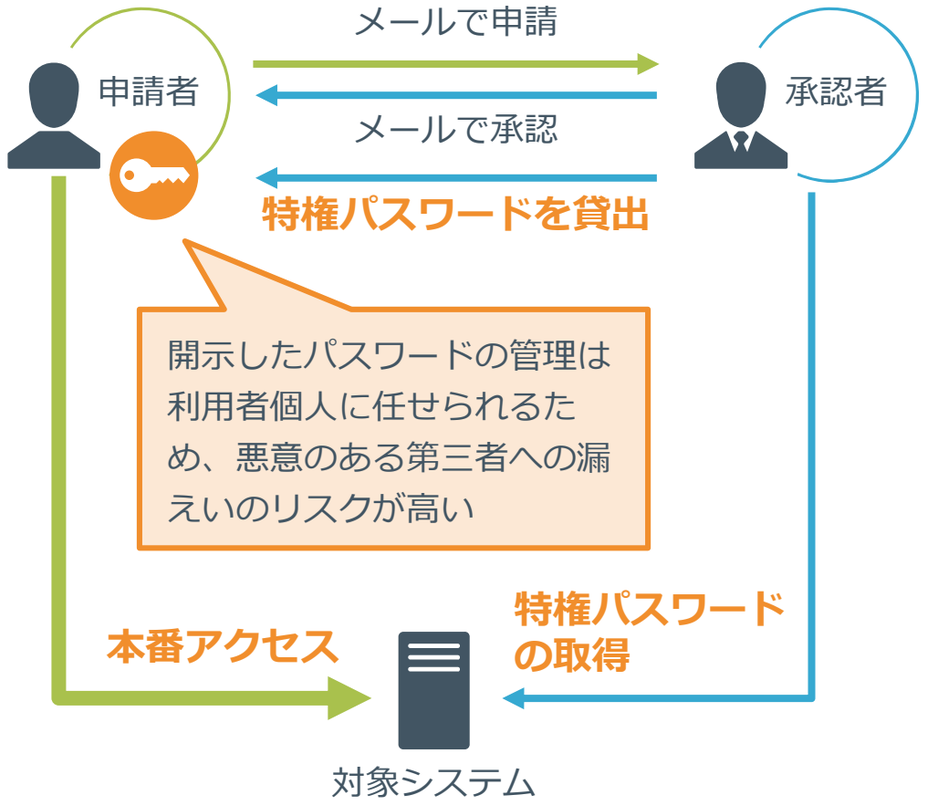
ゲートウェイを介さない直接ログインに対しては特権パスワード管理機能で制御可能です。

SecureCube Access Checkの特長2

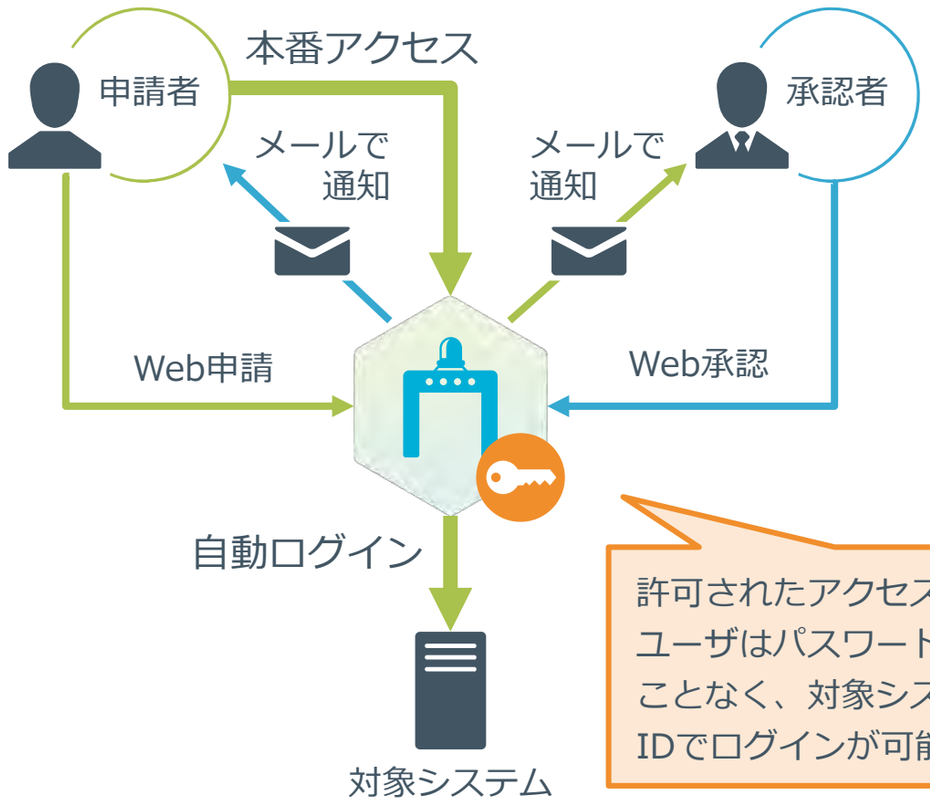
各種ガバナンス対応の
充実した機能

各業界に精通したコンサルタントと連携し、**求められる機能をいち早く提供**

従来の利用者へ特権IDのパスワード開示する方法では第三者への漏えいリスクが高い



パスワードを入力することなく自動でログインできるため、漏えいリスクが少ない



特許取得済

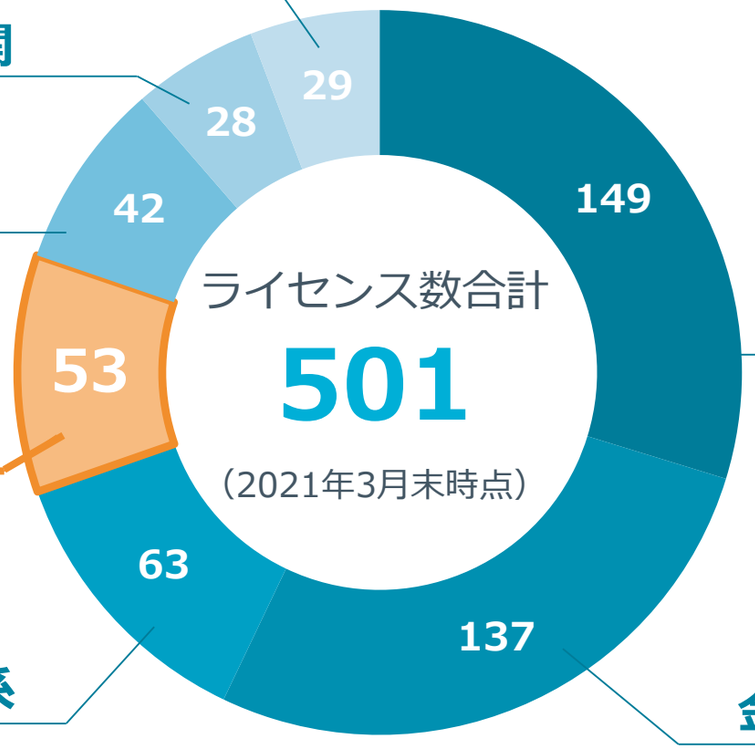
許可されたアクセスであれば、ユーザはパスワードを入力することなく、対象システムの特権IDでログインが可能

特許技術（特許第5797060号）にて実装

SecureCube Access Checkの特長3

国内のべ500社以上の
導入実績No.1※

15年以上の販売実績で、国内外のべ501ライセンスを出荷



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2021」
特権ID管理市場：ベンダー別売上金額シェア（2019年度）
SecureCube Access Check，Cloud Auditor by Access Check が対象

SecureCube Access Checkの主な機能

特権ID管理に必要な機能をすべて備えた**オールインワンソリューション**

ID管理

特権IDのパスワード自動変更や有効期限設定、ID情報を収集しCSV出力することが可能

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しており、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

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を実施、閲覧権限のある監査者のみ検索・閲覧が可能

監査補助

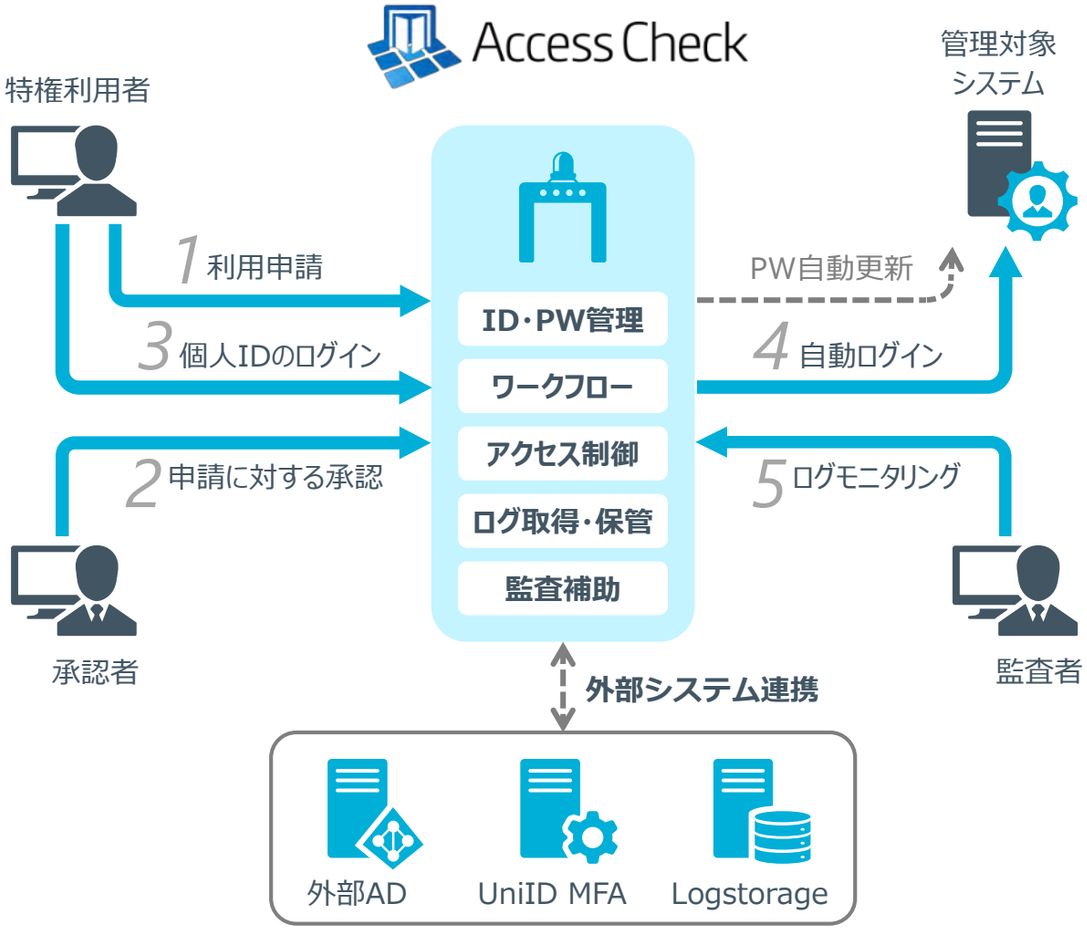
定期レポート出力の他、危険コマンドの発行通知、申請外持ち出しファイルの検出機能などを提供

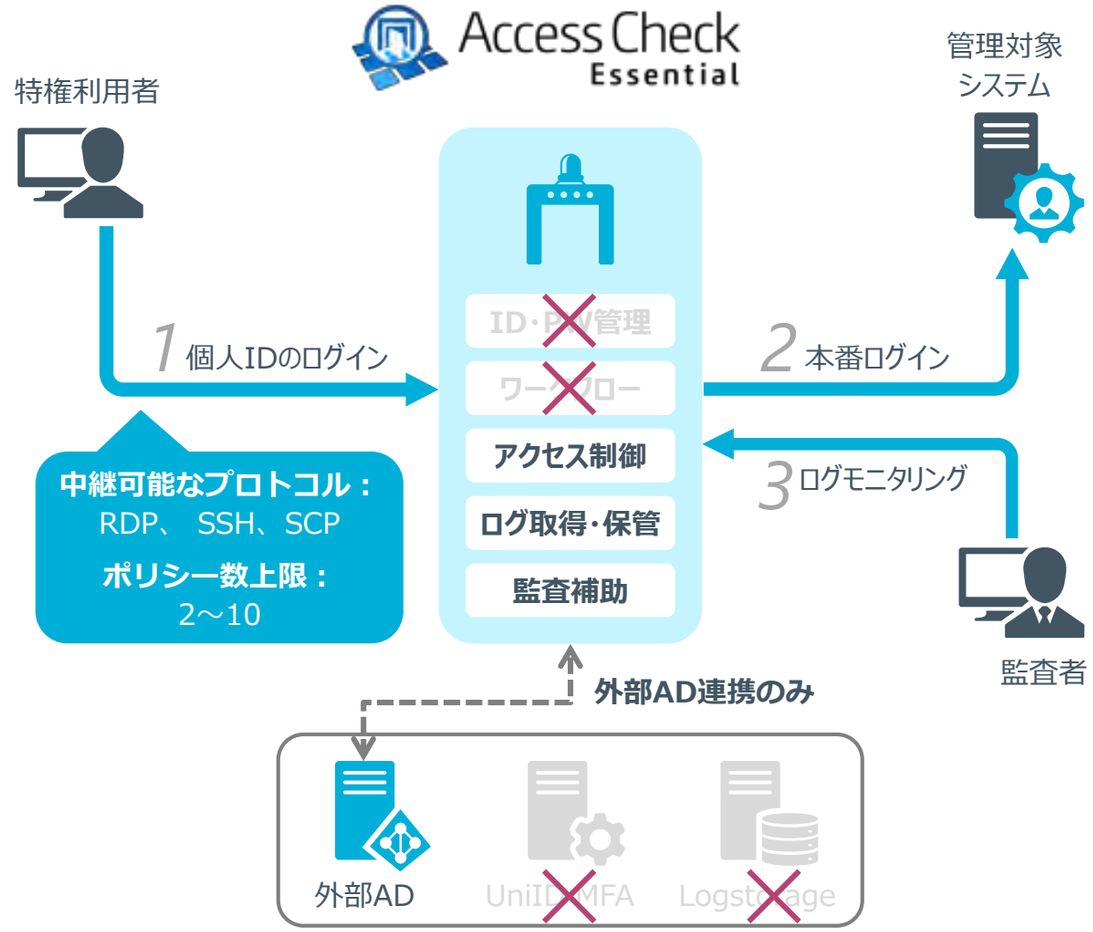
特権ID管理ソリューション

Access Check

コア機能に限定したAccess Check Essentialでスモールスタートも可能に

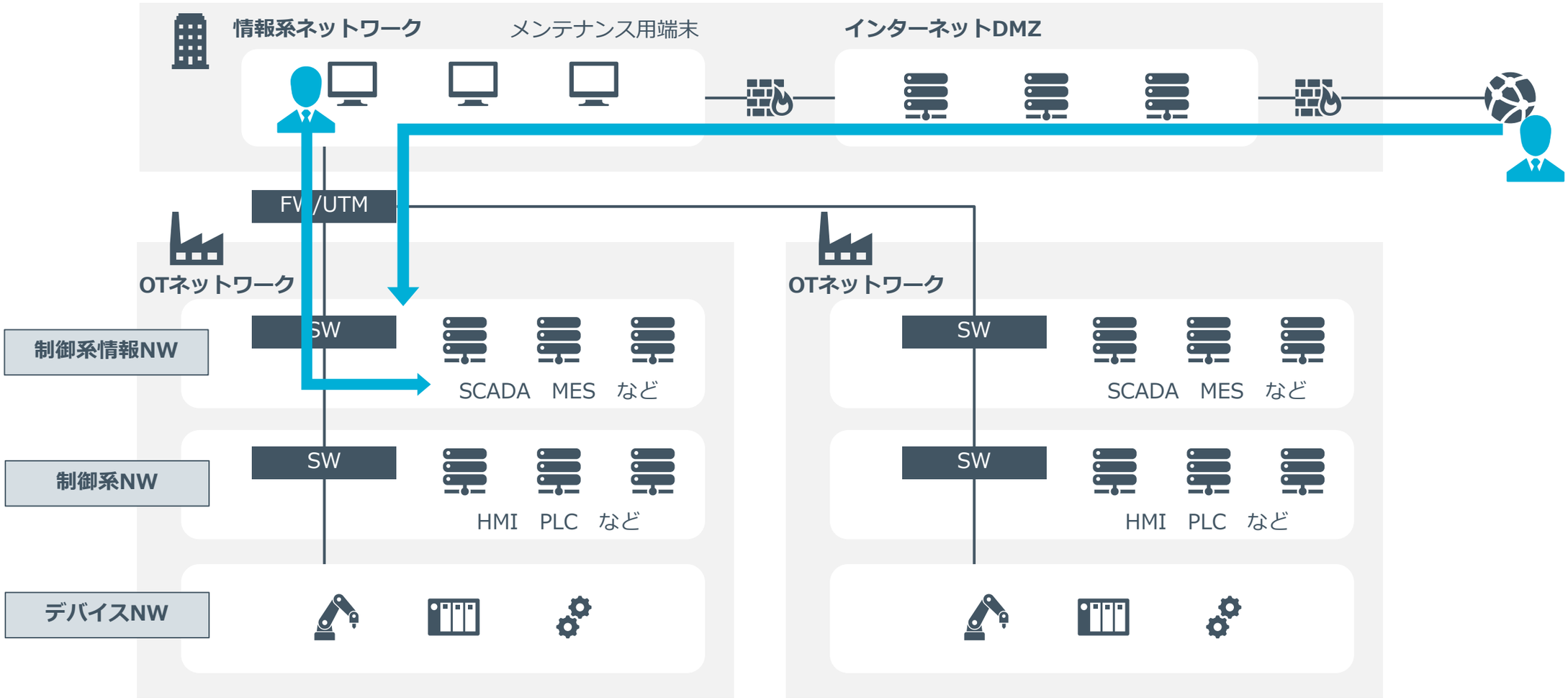
- 特権ID管理ソリューション SecureCube Access Check の機能のうち、アクセス統制に欠かせない
  アクセス制御、ログ取得・保管、監査補助の3つに限定して低価格で提供





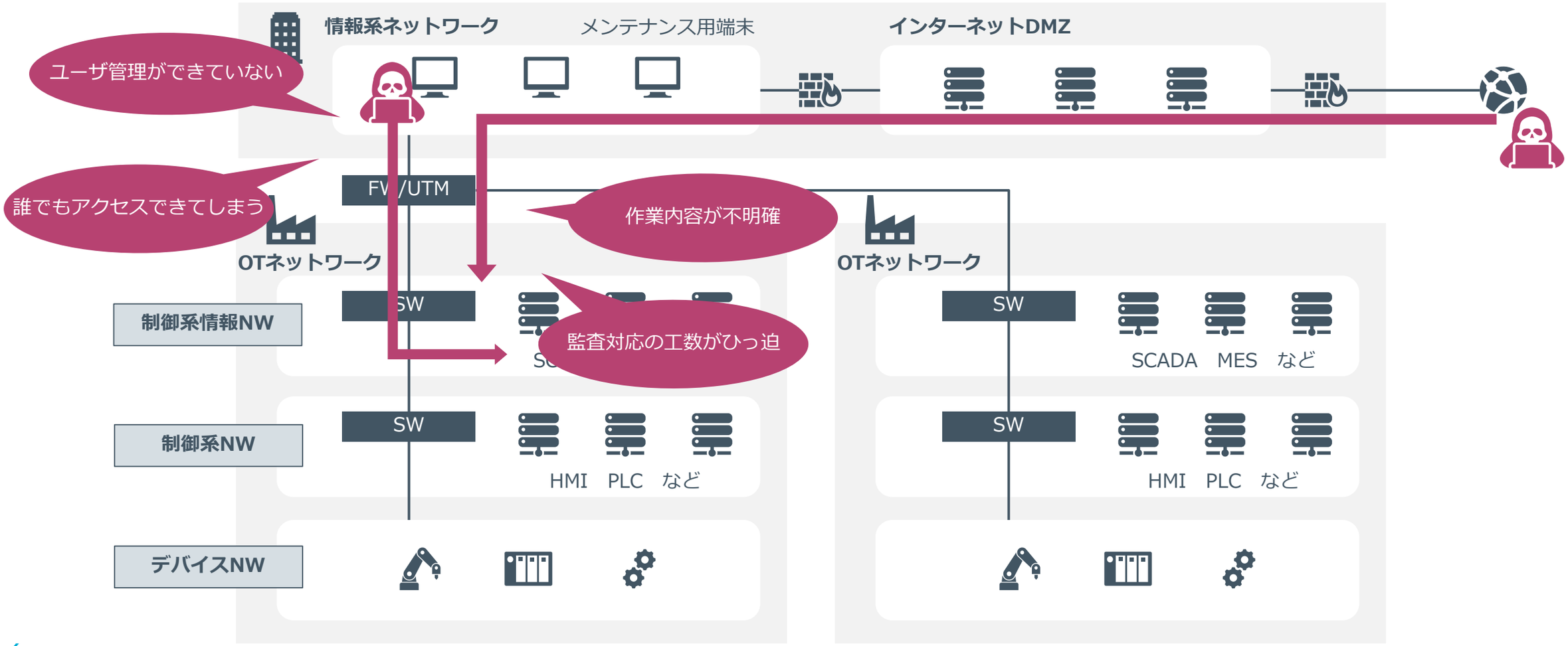
製造業におけるシステム構成例

- 工場にはシステム管理サーバ、データ収集サーバ、データ分析サーバ等が導入され、それらをリモートから操作するケースが増えており、以下のような構成が想定される



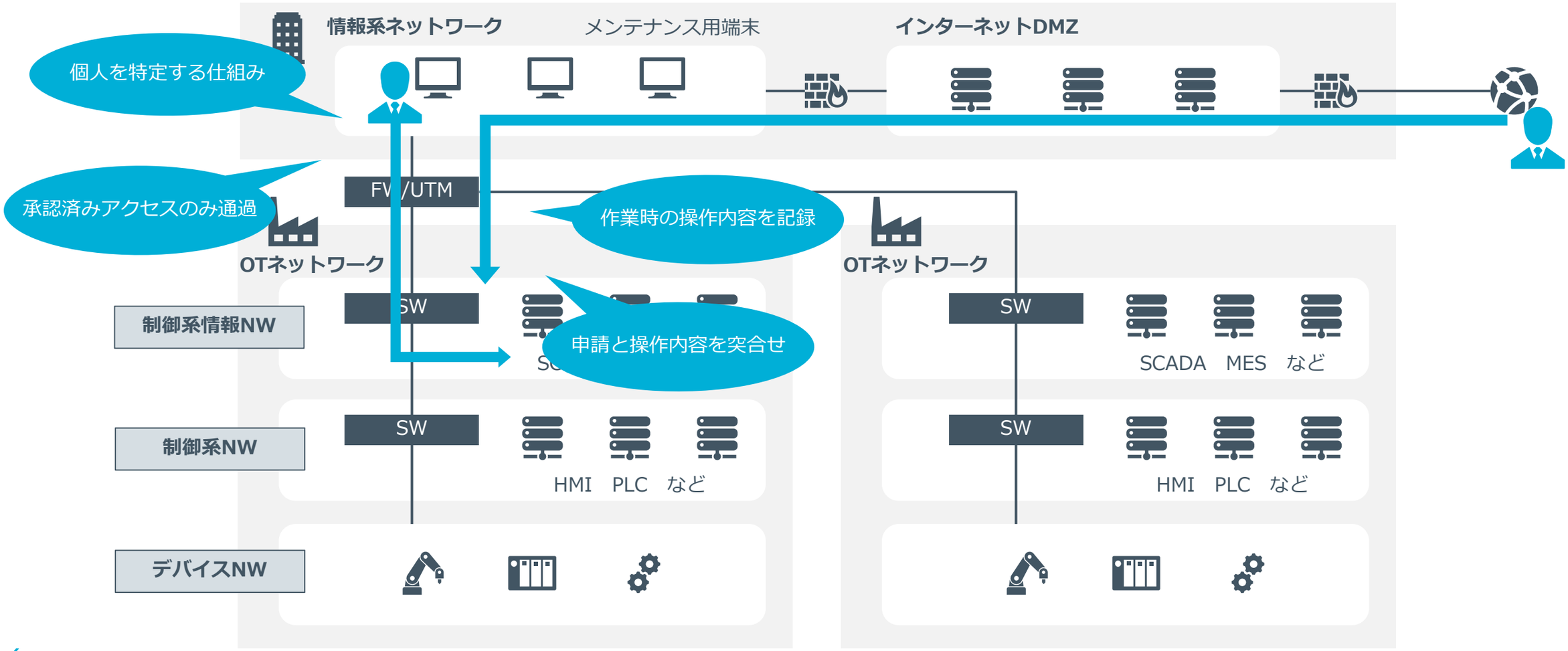
存在する内部不正/外部攻撃のリスク

- 内部不正や外部攻撃で特権IDが奪取され、情報漏洩、ランサムウェアによる生産ラインの停止が発生した場合、作業内容が特定できない、被害の検知が遅れることが想定される



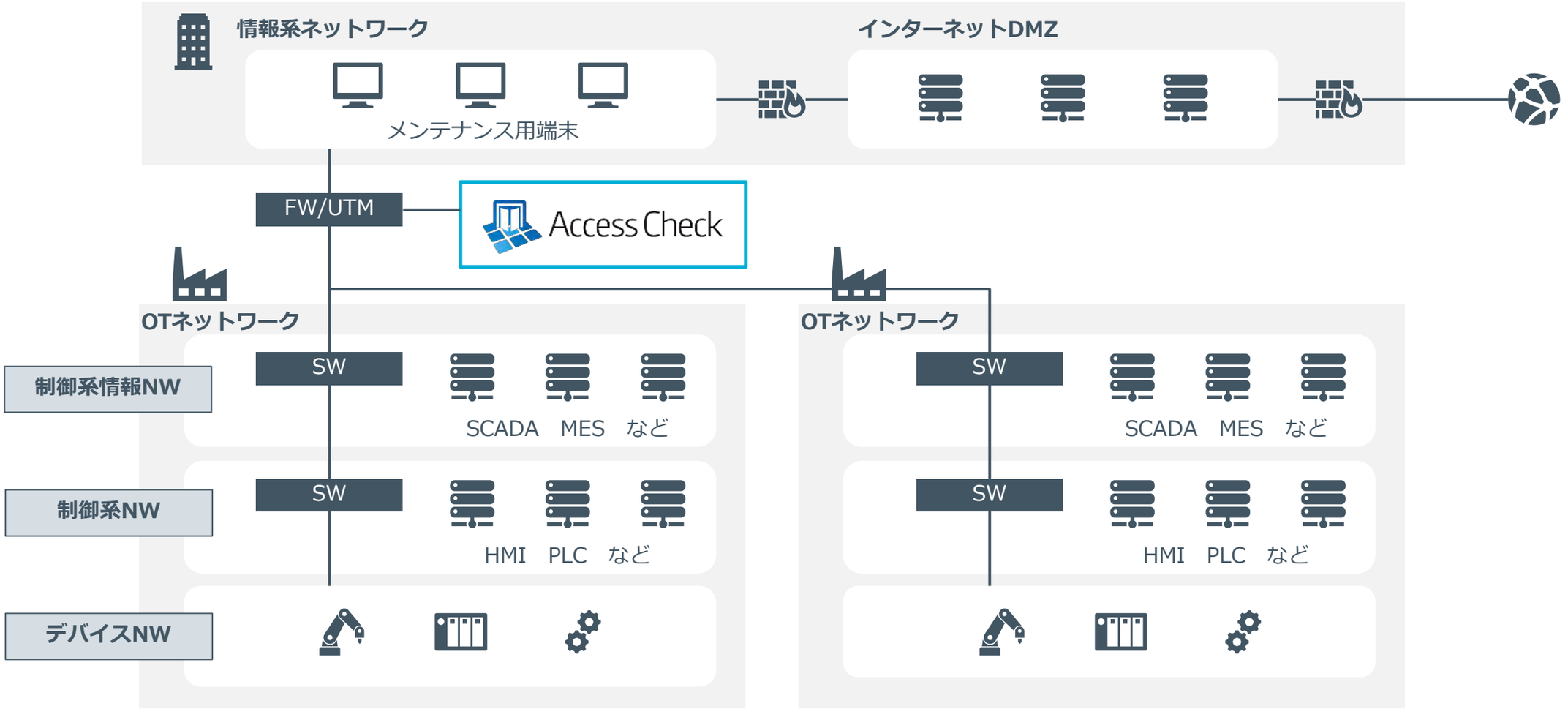
特権の悪用を防ぐためのアプローチ

- 特権ID管理の基本の4STEP（個人の特定、アクセス時の申請承認、操作記録、モニタリング）に沿って運用することが重要

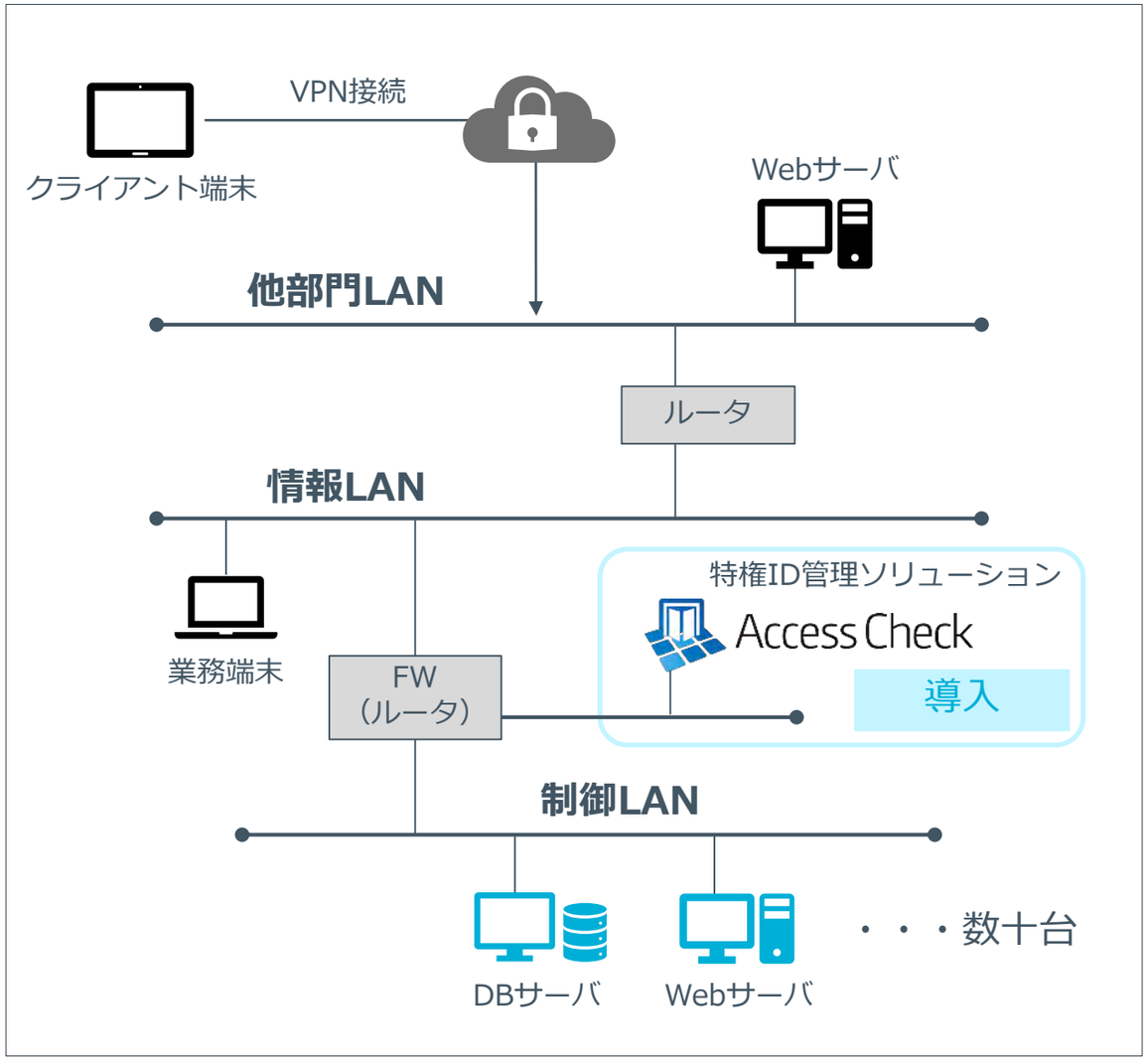


効果的かつ効率的なアクセス統制を実現

- SecureCube Access Checkを利用することで、工場内のネットワークセキュリティを効果的かつ効率的に確保することが可能



実際の活用例



目的

- 内部統制

主な導入要件

- 制御LANへのすべてのアクセス管理・制御
- アプリの改変、エージェント導入が不要

- ✓ 制御LANへの通信に対して、認証・認可を実施
  (Linux/WindowsへのTelnet / SSH / FTP / HTTP / RDP)
- ✓ 操作内容はログとして記録され、一元的に保管
- ✓ 短期間で全ての要件を満たせた

まとめ

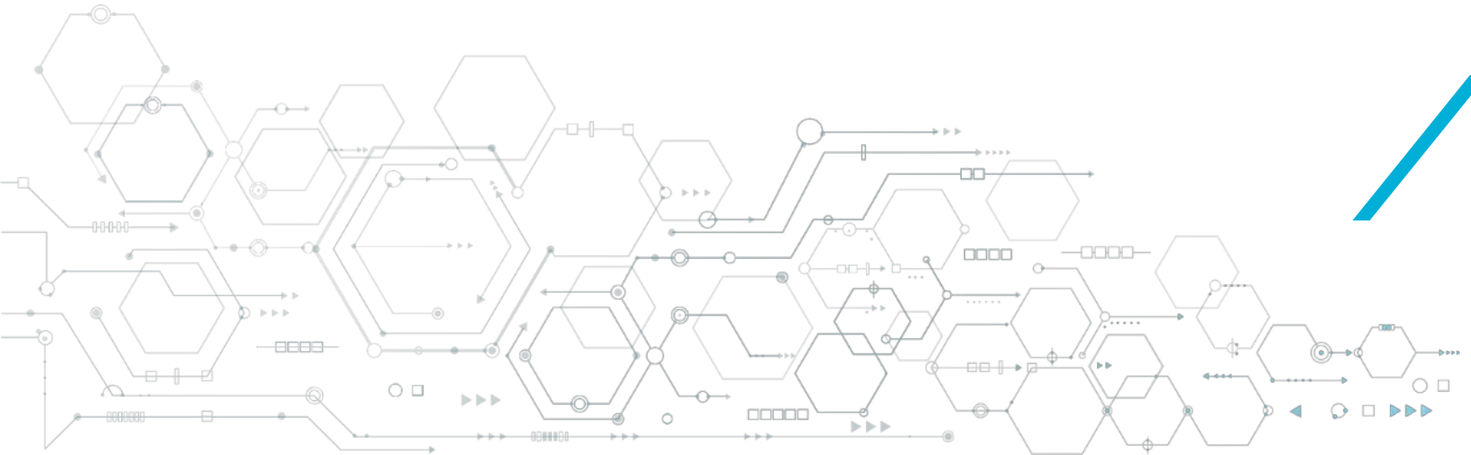
重要データを守るために必要なセキュリティとは

- 内部不正対策・サイバー攻撃対策として特権IDは管理すべき重要項目
- 製造インフラや製造プロセスの変化が進む中、OTネットワークにおいても特権ID管理は必須
- 特権ID管理の基本は、利用者の特定、申請・承認、作業の記録、妥当性の確認の一貫した実施
- システム管理者が特権IDを利用する際は、申請と承認、ログ取得・管理を徹底
- 完全ゲートウェイ型のアクセス管理製品「**SecureCube Access Check**」では
  特権ID管理、アクセス統制を効果的、効率的に実現し、OTネットワークのセキュリティを確保
- 「**Access Check Essential**」で、まずは証跡取得による現状把握からスタート

2月16日（水）11:00～ Access Check Essential 紹介セミナー受付中！

コア機能のみを搭載した Access Check Essential の機能や活用方法について徹底解説

https://www.nri-secure.co.jp/seminar/2022/ac_essential0216



NRI SECURE