事例で語る！内部不正対策のポイントとは
～すぐ導入できるアクセス制御・ログ取得ツールを紹介～

2024年5月23日（木）

NRIセキュアテクノロジーズ
ソフトウェア第二事業本部
統制ソリューション事業部

大塚　直哉

目　次

目　次

会社概要

（2024年4月時点）

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 サイバーセキュリティハブ大阪：大阪府大阪市北区 中之島フェスティバルタワー・ウエスト 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	建脇 俊一		
専務取締役	池田 泰徳	常務取締役	西内 喜一
取締役	小林 賢治、武田 則幸、山口 隆夫、能勢 幸嗣	監査役	坂田 太久仁
社員数	連結：813名、単体：697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

サービス・ソリューション提供体制

社会やニーズの変化、技術動向に応じたサービス・製品を4つのコア事業で提供

戦略ITイノベーションと研究開発

戦略ITイノベーション — 政策動向やマーケットニーズの洞察によるソリューション創発

研究開発センター — 先進技術の探索・評価、およびサービス開発の推進・統括

4コア事業

コンサルティング

顧客密着型の問題解決支援

ストラテジーコンサルティング事業本部
マネジメントコンサルティング事業本部
サイバーコンサルティング事業本部

DXセキュリティ

デジタルトランスフォーメーション
をセキュリティで支援

DXセキュリティコンサルティング事業本部
DXセキュリティプラットフォーム事業本部

**マネージド
セキュリティサービス**

24時間365日の
セキュリティ監視サービス

マネージドセキュリティサービス事業本部
マネージドセキュリティサービス開発本部

ソフトウェア

日本市場に合わせた自社開発の
セキュリティソリューション

ソフトウェア第一事業本部
ソフトウェア第二事業本部

企業のセキュリティ対策をトータルで支援する 5つの提供サービスカテゴリ

コンサルティング	セキュリティ診断	SOC・マネージド セキュリティサービス	セキュリティ 製品・ソリューション	セキュリティ 教育・研修

主な提供サービス・製品一覧

（2024年4月時点）

コンサルティング

リスクアセスメント
- 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
- 工場ファストセキュリティアセスメント
- MITRE ATT&CKを用いたサイバー攻撃対策の評価
- 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
- セキュリティ対策レポート
- セキュリティ監査
- CRI Profileを活用したサイバーセキュリティアセスメント
- クラウドセキュリティ評価
- サイバーセキュリティ経営ガイドライン対応支援
- ローコード/ノーコード開発基盤セキュリティ評価
- リスクベースアセスメント
- IMDRFガイダンスに基づいたセキュリティアセスメント
- AI品質・適合性検証

リスクマネジメント
- 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
- サプライチェーン・セキュリティコンサルティング
- 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
- プライバシーリスク評価・パーソナルデータ管理システム化検討支援
- AIリスクガバナンス構築支援

脅威インテリジェンス
- マネージド脅威情報分析

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
- 半導体業界向けSEMIセキュリティ規格準拠支援
- 防衛産業サイバーセキュリティ基準準拠性評価
- SWIFT CSCFの準拠性評価

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
- セキュリティ業務改革支援
- デバイス脆弱性監視分析
- SEC Team Services
- SBOM導入支援

設計開発支援
- DevSecOps実行支援
- 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

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
- AIセキュリティ診断（AI Red Team）

IoT/OT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

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
- Mandiant Advantage Security Validation ペネトレーションテスト

SOC・マネージドセキュリティサービス

NeoSOC（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（共用SOC）
- SIEM監視

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
- メールセキュリティ管理サービス(Proofpoint Email Protection)
- マネージドITDRサービス
- 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
- マネージドネットワークスサービス

Web・アプリケーション 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
- パブリッククラウドセキュリティマネージドサービス

OT/IoTセキュリティ監視
- マネージドNDR（Nozomi Networks for OT/IoT）

マネージドNWサービス
- 拠点WAN接続サービス
- SD-WAN接続サービス
- マルチクラウド接続サービス
- 高度運用監視サービス

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
- Access Check Essential
- Okta
- YubiKey
- CrowdStrike Falcon Identity Protection
- ジョーシス
- Start In

リモートアクセス
- CACHATTO
- MagicConnect

メール・Webセキュリティ
- m-FILTER MailAdviser
- Cofense
- Proofpoint
- Proofpoint Email Fraud Defense (EFD)
- DMARCレポート可視化

文書・ファイルセキュリティ
- クリプト便
- POSTUB
- Box
- FinalCode
- 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
- パブリッククラウドセキュリティマネージドサービス
- Adaptive Shield
- i-FILTER@Cloud

リスク分析・可視化
- Proofpoint ITM
- illumio
- Secure SketCH

脅威インテリジェンス
- IntSights
- Recorded Future
- GR360
- RiskIQ

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

IoT/OTセキュリティ
- マネージドNDR（Nozomi Networks for OT/IoT）
- SCADAfenceプラットフォーム
- 工場ファストセキュリティアセスメント

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
- CCSP CBKトレーニング

セキュリティ人材育成
- セキュアEggs

安全・安心なIT社会を実現するために

NRIセキュアは
世界最高水準の情報セキュリティを提供するため
技術と知見を磨き続けています。

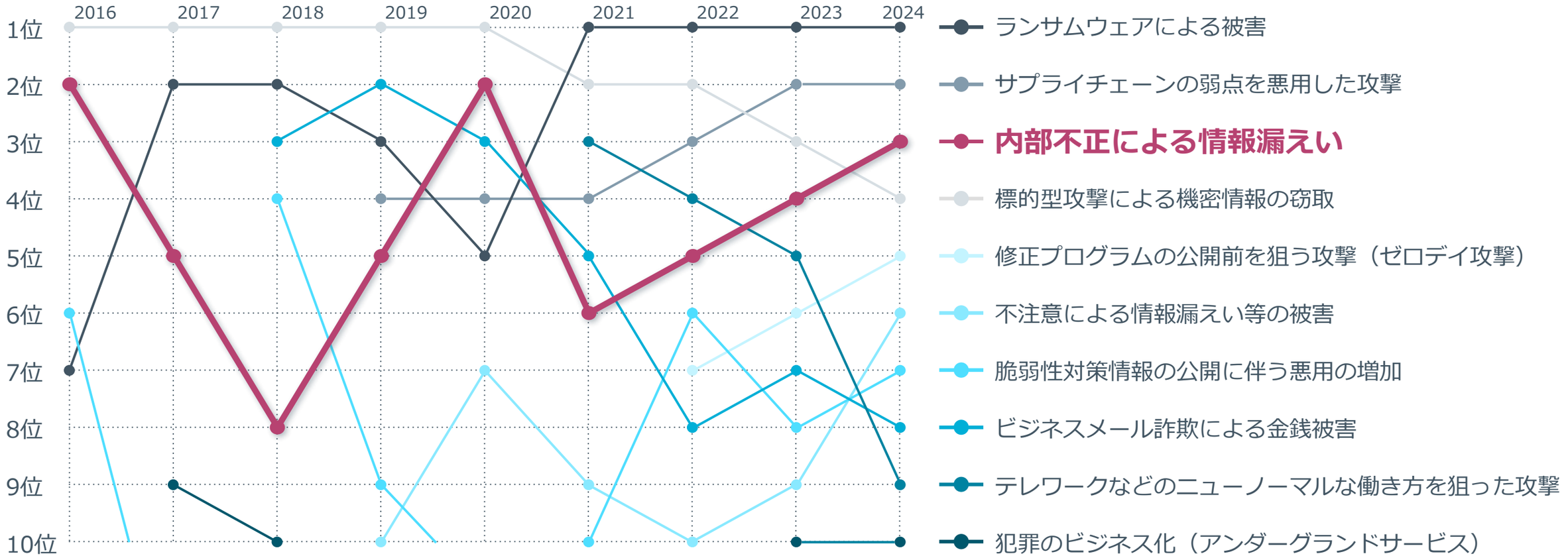
豊かな未来づくりのために
挑戦を続けるお客さまとともに
誰もが安全に安心して
ITの魅力を自由に楽しめる社会をつくる。

ー これが、NRIセキュアの使命です。

目　次

内部不正による情報漏えいの脅威の推移

「情報セキュリティ10大脅威（組織）」では、過去9年間「内部不正による情報漏えい」が継続ランクイン



※IPA「情報セキュリティ10大脅威 2024：組織編」および、IPAが発表している過去の情報セキュリティ10大脅威の順位を基にNRIセキュアが作成
https://www.ipa.go.jp/security/10threats/10threats2024.html

内部不正によるセキュリティインシデントの影響

内部不正によって引き起こされる影響は、一時的なビジネス活動への支障だけでなく、社会的信用の失墜、損害賠償、事後対応にかかる労力や費用の増大等、多大な損失が考えられる

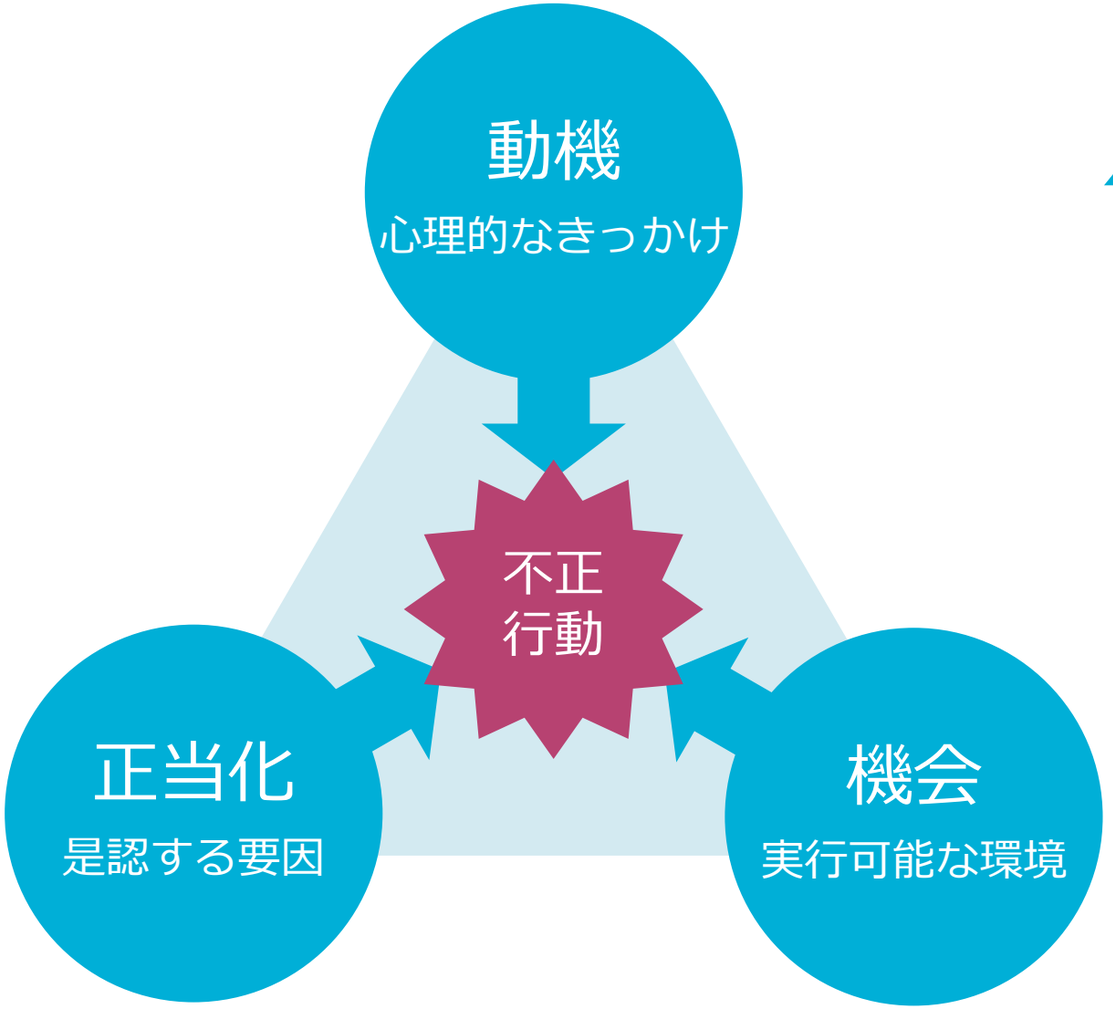
公表されている内部不正によるセキュリティインシデント

報道時期	不正行為者	概要
2021年1月	大手通信会社 退職者	技術情報を転職先に不正に持ち出し、約1000億円の損害賠償を求めて民事訴訟を提起
2021年3月	大手証券会社 委託先社員	管理しているシステムから、210件の顧客情報を不正に持ち出し、約2億円を不正に出金
2022年6月	自治体 再々委託先社員	市民の個人情報約46万件が入ったUSBメモリを紛失、市は委託先に約3,000万円の損害賠償を請求
2022年9月	大手飲食チェーン 退職者	営業秘密を不正に持ち出し、5億円（63億円以上の損害金額の一部請求）の損害賠償を求め提訴
2023年3月	大手通信会社 委託先派遣社員	開発していたデータ管理システムから個人情報約596万件を個人保有のクラウドサービスへ保存
2023年7月	大手通信会社 再委託先派遣社員	管理しているシステムから顧客情報約900万件を不正入手、一部個人情報が名簿業者に流通

報道されている情報を基にNRIセキュアが作成

目　次

不正が起こるメカニズム　–不正のトライアングル–



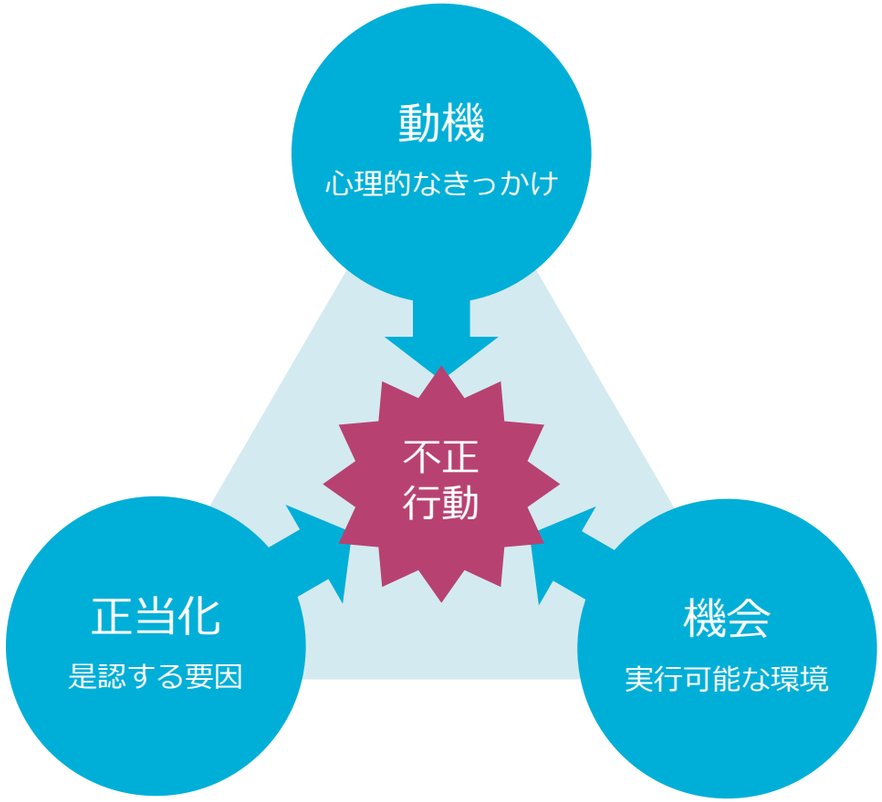
組織犯罪研究者 ドナルド・R・クレッシーが提唱
不正のトライアングル

各要素がそろったときに不正が発生する
可能性が高まると言われている

内部不正を防止する対策
＝トライアングルを崩す対策

不正が起こるメカニズム　–不正のトライアングル–

- **1960年代に、米国経済学者であり犯罪学者でもあるドナルド・クレッシーによって提唱された**
- **動機・機会・正当化の3つの要素が成り立つとき、個人が不正行為に走るリスクが高まる**



機会

- **不正行為を行う機会が存在するかどうか**
- **内部統制や監査の不備、管理プロセスの弱点などが知られている**と、不正行為のリスクは高まる

動機

- 不正行為に至るきっかけや心理的な圧力
- 金銭的な課題を感じている、組織に不満を持っているなどが代表的なきっかけ

正当化

- 自身の行動化を正当化できるか
- “報酬が少ないから”、“他の人もやっている”など内部不正を自身の中で正当化し、罪悪感を減らすことで行為を行いやすくなる

不正のトライアングルを崩すには　–内部不正防止の基本原則–

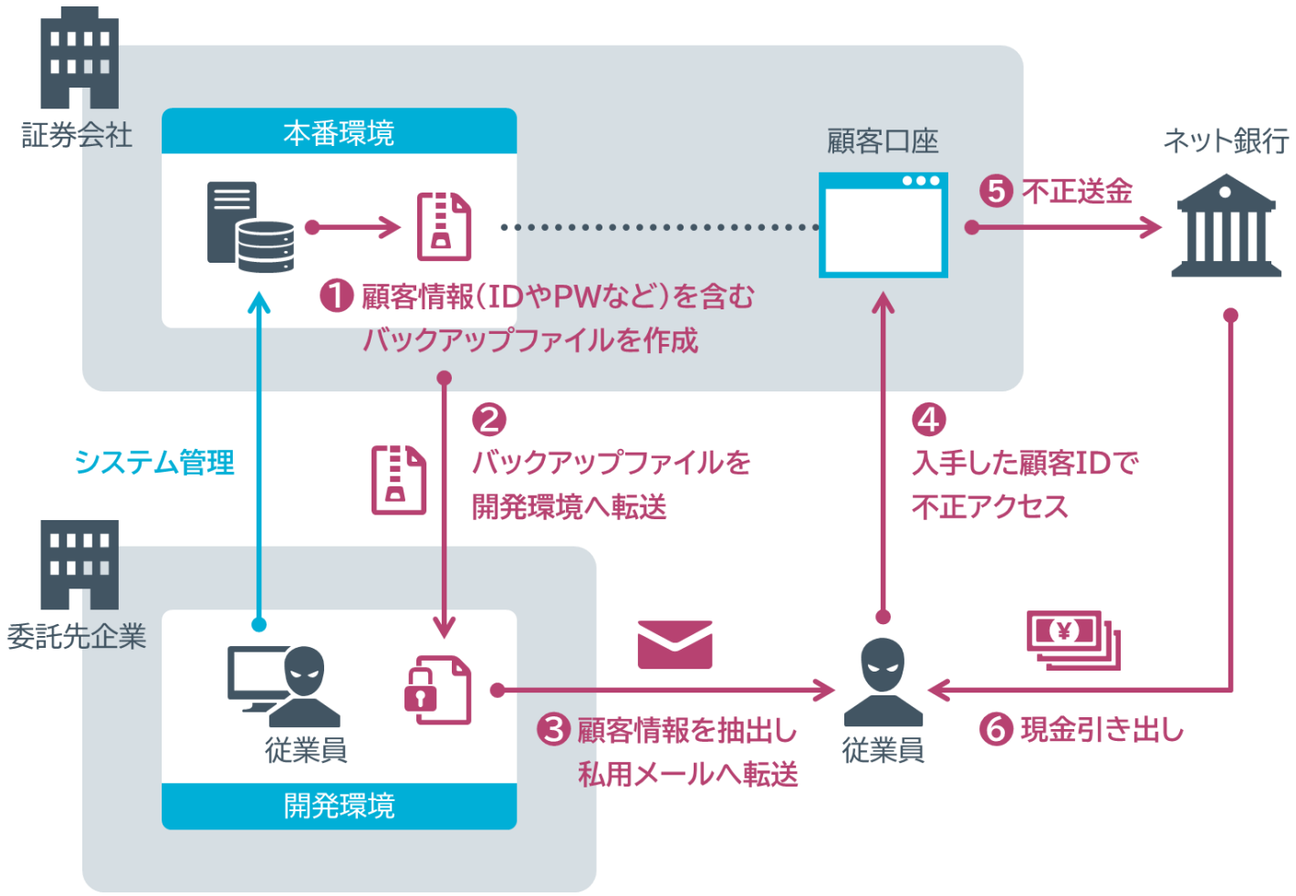
IPAのガイドラインに記載されている内部不正防止の基本原則は、不正のトライアングルを崩すことと対応

機会の削減	**犯行を難しくする**（やりにくくする） 対策を強化することで犯罪行為を難しくする **捕まるリスクを高める**（やると見つかる） 管理や監視を強化することで捕まるリスクを高める **犯行の見返りを減らす**（割に合わない） 標的を隠したり、排除したり、利益を得にくくすることで犯行を防ぐ
動機の削減	**犯行の誘因を減らす**（その気にさせない） 犯罪を行う気持ちにさせないことで犯行を抑止する
正当化の削減	**犯罪の弁明をさせない**（言い訳させない） 犯行者による自らの行為の正当化理由を排除する

IPA「組織における内部不正防止ガイドライン」より作成
https://www.ipa.go.jp/security/guide/insider.html

目　次

証券会社の委託先元社員による不正出金事件



報道されている情報を基にNRIセキュアが作成

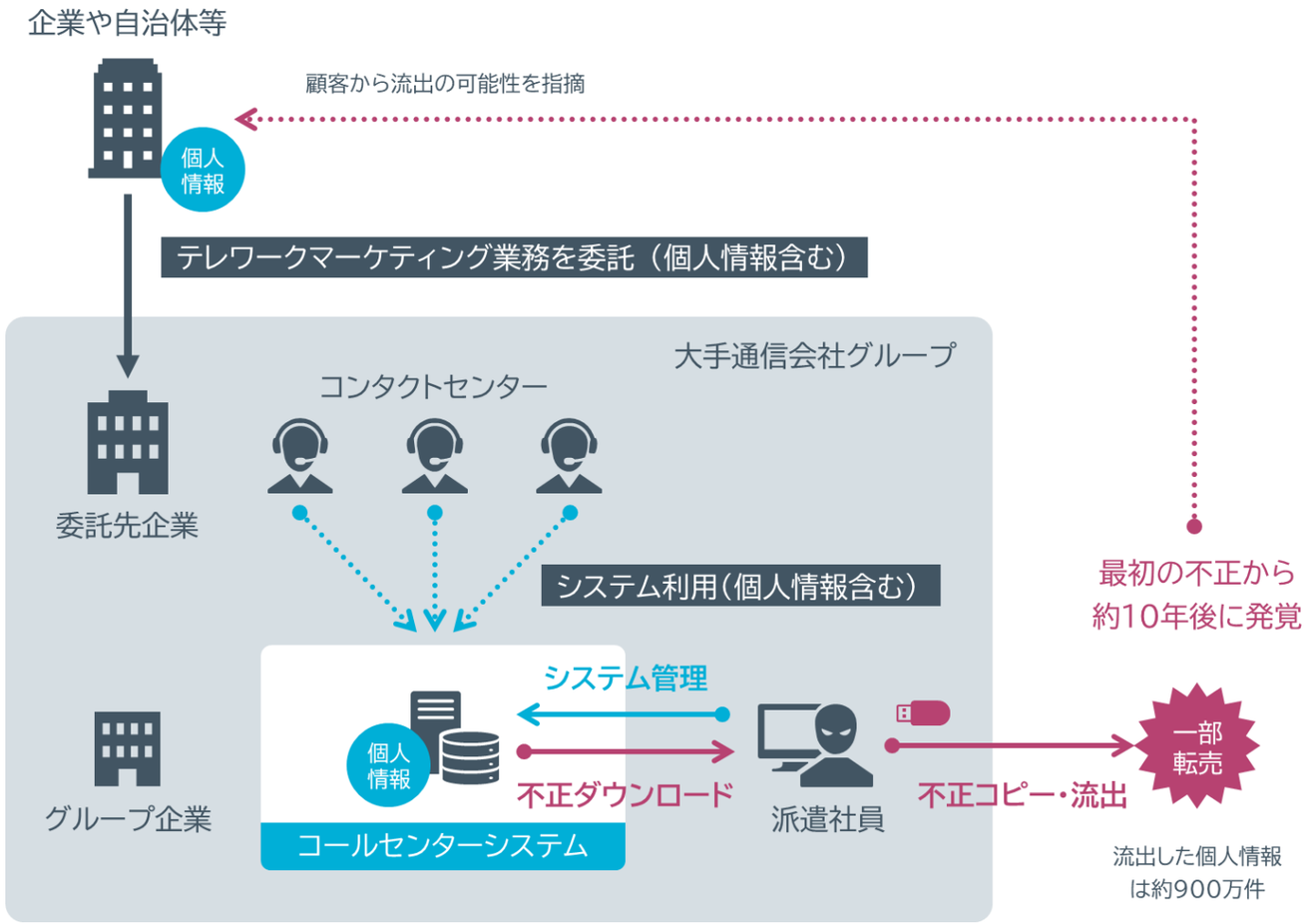
2017年から約2年半にかけて、証券取引システムの開発・保守を担っていた委託先の元従業員が、顧客情報を不正利用し、約2億円を不正出金

→ **2020年に、顧客からの問い合わせにより発覚**

機会

- ✓ 19年にわたりシステムを担当しており、熟練のエンジニア（システムに精通）
- ✓ 本番環境と開発環境の両方にアクセスできる権限を保持
- ✓ 本番環境から顧客情報を含むファイル転送が可能
- ✓ 本番環境から取得されたファイルの内容の確認は十分にされていないことを把握

大手通信会社の子会社による情報漏えい事件



報道されている情報を基にNRIセキュアが作成

2013年ごろから約10年かけて、コールセンターのシステムを保守・運用を担う元派遣社員が、個人情報約900万件を不正に持ち出し、第三者に流出

→ **2023年に、警察による捜査が実施され発覚**

機会

- ✓ 15年もの間、システムに携わるベテランエンジニア（システムに精通）
- ✓ システムに保管された情報を保守作業端末へダウンロード可能
- ✓ 保守作業端末から外部記憶媒体へデータの持ち出しが可能
- ✓ データ持ち出しの検知が不十分
- ✓ 各種ログのモニタリングが不十分

2つの事件の共通点

長期間システム管理に
従事し、権限が集中

管理者権限を悪用して
重要情報にアクセス

情報の持ち出しを制限・
検知する仕組みがない

本番環境からの情報の
持ち出しを容易に実行

作業の操作記録の
モニタリングが不十分

長期間犯行を検知できず
被害が拡大

2つの事件の共通点

長期間システム管理に
従事し、権限が集中

管理者権限を悪用して
重要情報にアクセス

特権ID・権限の適切な管理

犯行を難しくする

情報の持ち出しを制限・
検知する仕組みがない

本番環境からの情報の
持ち出しを容易に実行

情報持ち出しの制御と確認

犯行の見返りを減らす

作業の操作記録の
モニタリングが不十分

長期間犯行を検知できず
被害が拡大

ログ管理とモニタリング

捕まるリスクを高める

3つの内部不正対策と統制レベル

自社の運用やリスク評価に応じて、段階的に対応を進める

統制レベル
弱
強

1 特権ID・権限の適切な管理	2 情報持ち出しの制御と確認	3 ログ管理とモニタリング
✓ 開発と運用の権限分掌 ✓ 職務に応じたアクセス権の付与 ✓ IDや付与した権限の定期的な棚卸	✓ 申請・承認に基づいたファイル持ち出しの制限 ✓ 持ち出したファイルの内容を含めた操作記録	✓ システム管理者権限を利用した個人を特定して記録 ✓ 利用申請とログを紐づけて保管
✓ 申請・承認に基づいたID払い出し、アクセス制御 ✓ アクセス経路の限定	✓ 情報を持ち出す作業においては2名以上での操作を必須化 ✓ 持ち出した情報の内容を定期的にモニタリング	✓ 操作の記録を含むログの定期的なモニタリング ✓ 不審なログに関する利用者へのヒアリングを実施
✓ 強力な認証（多要素認証）によるアクセス制御 ✓ パスワードの秘匿化	✓ 重要情報の持ち出しをシステム的に検知・遮断	✓ 合理的なロジックに基づくモニタリング対象の絞り込み ✓ 怪しい操作の自動検出

目　次

現場からよく聞く課題

システム開発や短期的なプロジェクトの現場では、厳格なアクセス統制は難しい

セキュリティ

現場に任せているため抜け漏れがある

逐次的に環境構築され、メンテナンス作業も多いことから、現場任せになるため、管理漏れが発生

運用負荷

運用負荷が高く業務効率が低下している

作業の都度、操作ログを作業者自身が取得し、ファイルサーバに蓄積しているが、ログサイズも大きく効率が悪い

コスト

コストやリソース不足で十分な対応ができない

高価なソリューションを購入するだけの投資対効果は見込めず、複雑な設定を運用維持できる体制も取れない

Access Check Essential で効率的にアクセス統制を強化

Access Check Essentialでは、効率的なアクセス統制を短期間・低コストで実現することが可能

セキュリティ

セキュリティ向上

共有IDを利用している場合でも作業者個人を特定できるほか、パスワードの秘匿化、アクセス制御、ログの取得漏れ防止、不正の早期発見などに貢献

運用負荷

運用負荷を軽減

エージェントのインストールが不要なゲートウェイ型のため、操作端末やサーバへの影響を最小限に抑え、メンバの入れ替えなどにも柔軟に対応

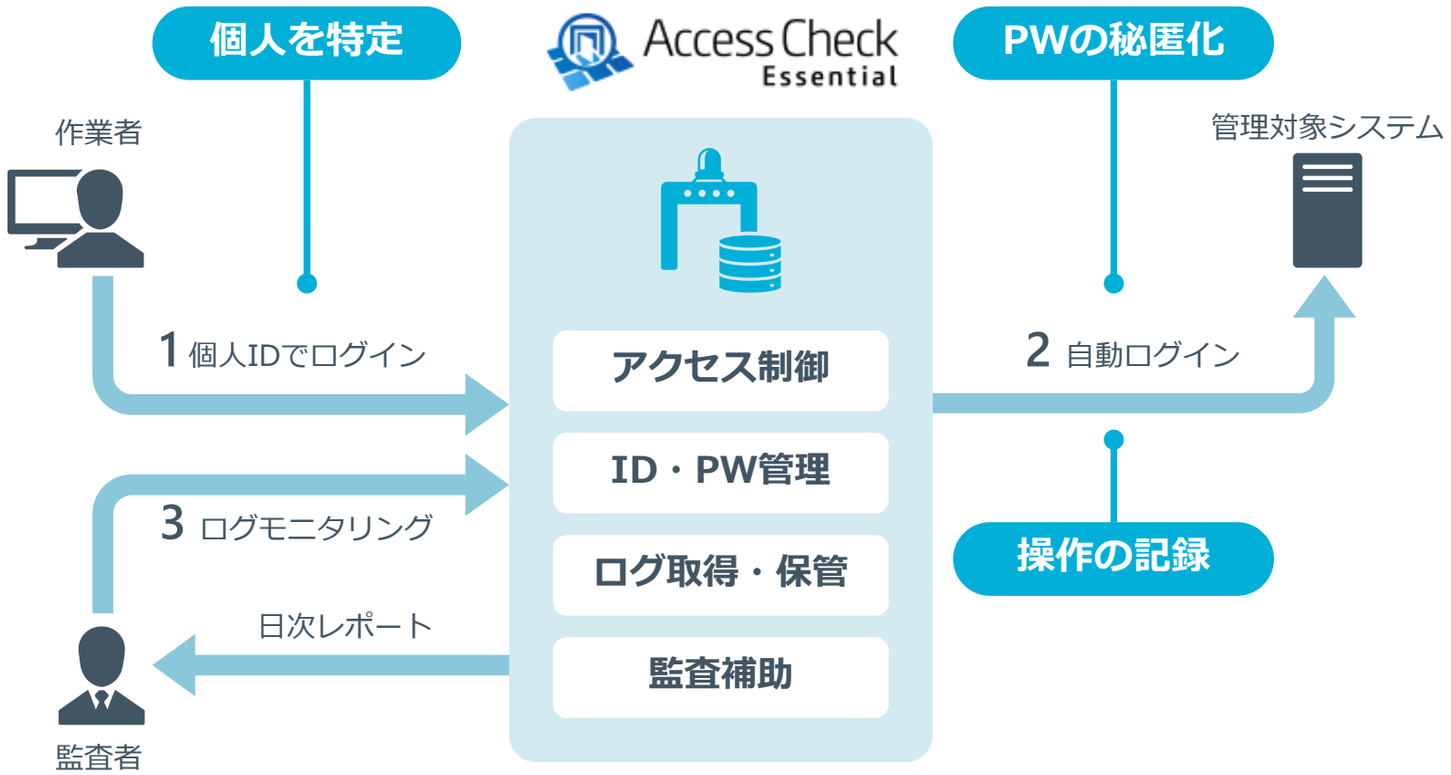
コスト

低コストで統制強化を実現

アクセス統制に必要な最小限の機能を提供、管理対象機器数のレンジに応じた価格設定で利用者の増減に影響されない

Access Check Essential とは

- Access Check Essential は、ゲートウェイ型のアクセス制御・ログ取得ソリューション
- ゲートウェイを通過するだけで、作業者個人の特定とPWの秘匿化、操作の記録が可能



3つの特長

ゲートウェイ型なので
導入・運用が容易

サブスクリプション型で
初期費用を抑えた
導入が可能

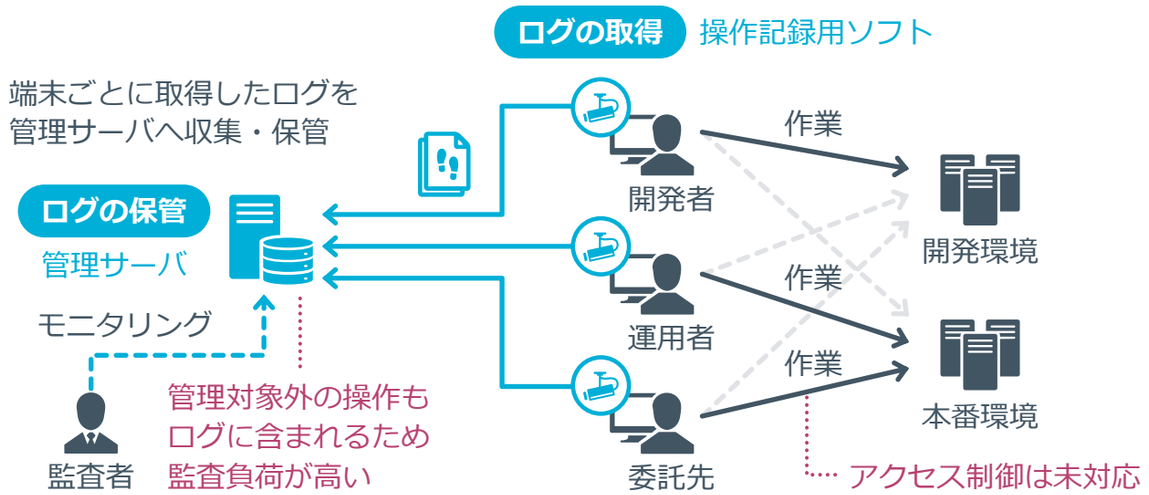
パスワードの秘匿化や
ログの改ざん防止など
セキュリティ機能も充実

特長1｜ゲートウェイ型のため導入・運用が容易

- **作業者端末にエージェント（専用ソフトウェア）をインストールして操作ログを取得するソリューションの場合、導入後の運用負荷が高くなる傾向がある**
- **ゲートウェイ型のソリューションは、運用負荷を最低限に抑えることが可能**

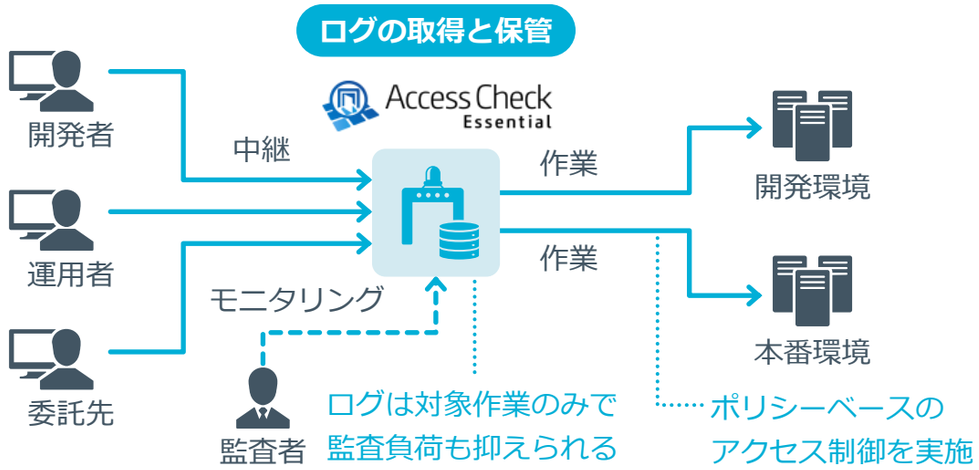
エージェント型のシステム証跡管理ツール

導入時：影響調査、動作確認の負荷が高い
運用時：ソフトの配布・管理、アップデート対応の負荷が高い
→ **ユーザが多い／人の入替えが多い場合には運用負荷が高くなる**



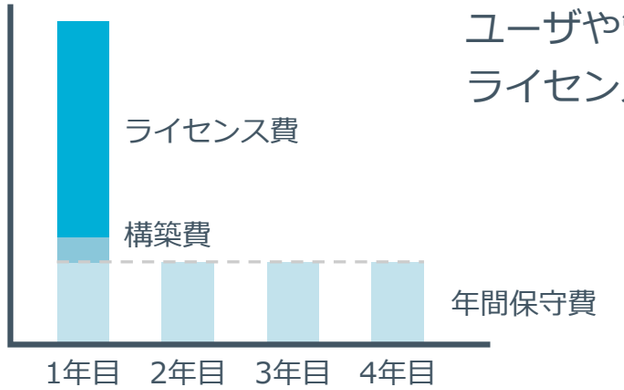
ゲートウェイ型のAccess Check Essential

導入時：既存環境への影響は最小限、動作確認の負荷も低い
運用時：ソフト配布の必要なし、中継サーバのみのメンテナンス
→ **ユーザが多い／人の入替えが多い場合でも運用負荷を抑えられる**

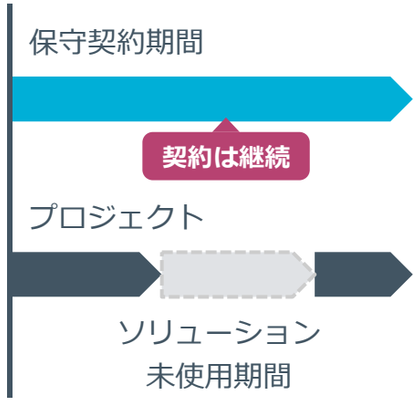


特長2｜サブスク型で初期費用を抑えた導入が可能

買い切り



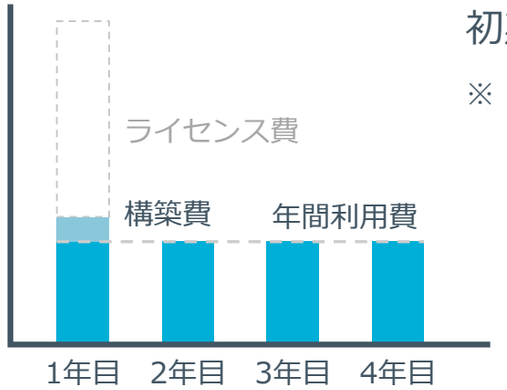
ユーザや管理対象機器が多いと
ライセンスを含めた初期費用が高い



プロジェクトが終了した場合にも
再度利用することを想定して
保守契約を解約しづらい

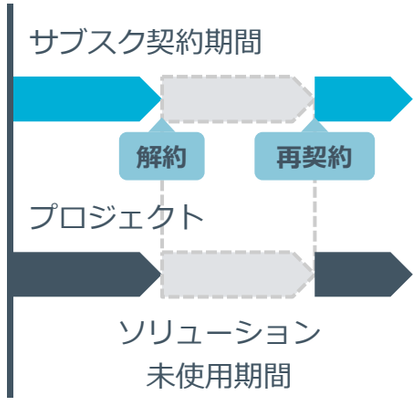
※ 解約後に再度保守契約を結びたい場合、解約日からの遡及契約ができず、ライセンスの買いなおしが必要となるケースもある

サブスクリプション



初期費用が抑えられる

※ ただし、サブスクリプションの年間利用費は買い切りの年間保守費よりも割高となる



1年単位で契約するため
プロジェクト状況に応じて解約できる

※ 再度利用する際には再契約が必要

特長3｜パスワード秘匿化やログの改ざん検知等セキュリティ機能も充実

パスワード秘匿化

- 退職者・異動者も共有しているIDのパスワードを知っている状態

- 利用者にパスワードを開示することなく共有IDを利用可能

ログの暗号化保存
ログの改ざん検知

- 操作の記録は作業者個人に任せているためログの抜け漏れが発生
- ログを加工していても分からない

- 操作の内容は作業時に自動記録
- ログは暗号化して保存され、改ざんを検知した場合、アラートを通知

Access Check Essential の主な機能

アクセス制御

- ユーザの特定
- ポリシーベースのアクセス制御
- リアルタイム遮断

ID・パスワード管理

- パスワード秘匿化

ログ取得・保管

- アクセスログと操作ログの取得
- 取得したログの保護
  （ログの暗号化と改ざん通知）

監査補助

- 日次レポート
- ダッシュボード
- キーワード検知

Access Check Essential 主な機能①　アクセス制御

Access Check Essentialがゲートウェイとなりアクセス制御を実施

ユーザの特定（認証）

特権IDなど、複数の利用者がIDを共有している場合でも、Access Check Essentialで個人認証を行うため、ユーザを特定できます。

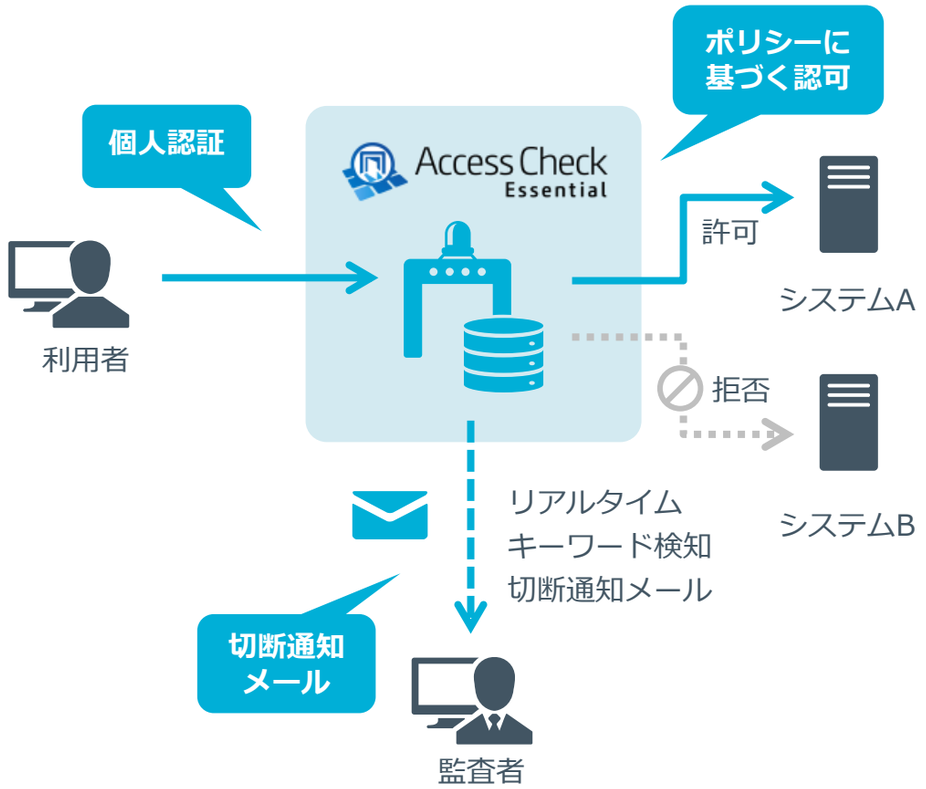
ポリシーベースのアクセス制御（認可）

ID/パスワードにより個人の「認証」を行い、事前のポリシー設定に基づきその先のシステムへアクセスして良いか「認可」を行います。

ポリシーは、利用者（ユーザ）と接続先のシステム（ノード）を紐づけて設定し、ユーザに対してノードへのアクセス権限を定義したものです。
ユーザは、ポリシーで紐づけされていない（許可されていない）ノードへアクセスすることはできません。

リアルタイム遮断

事前に登録されたキーワード（危険なコマンドなど）が作業中に確認された場合、リアルタイムに通信を遮断することが可能です。（検知だけも可）



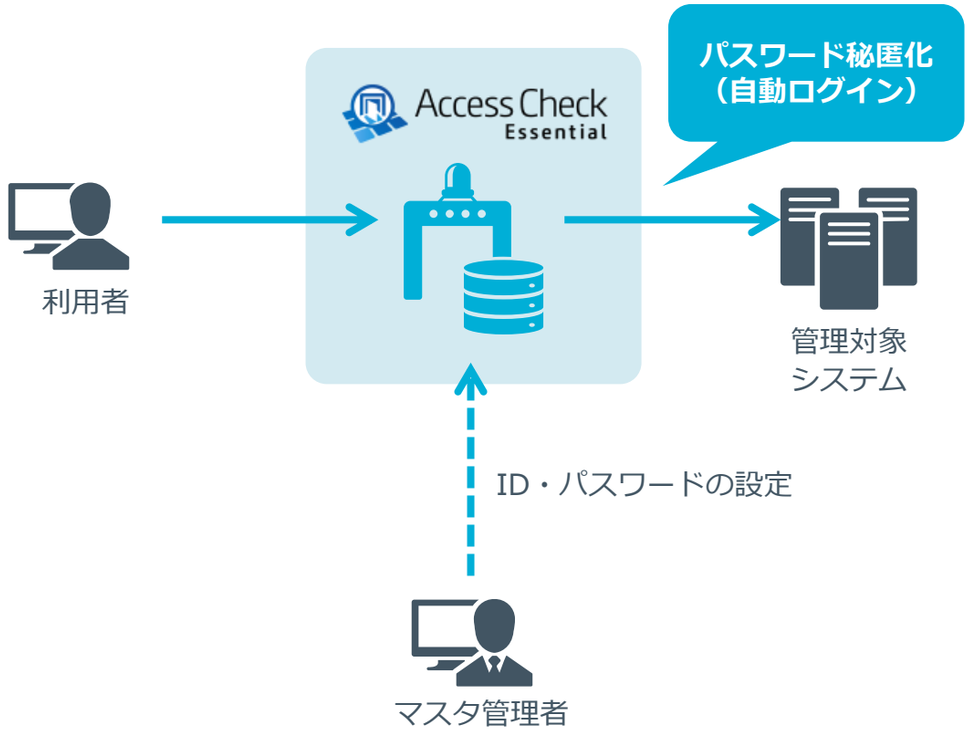
※ 登録可能なポリシー数上限は最大10です。

Access Check Essential 主な機能②　ID・パスワード管理

Access Check Essential上で、管理対象システムのIDとパスワードを一元管理

パスワードの秘匿化

Access Check Essentialを経由してアクセスする場合、Access Check Essentialが代理で管理対象システムへのログイン処理を行うため、利用者にパスワードを開示することなく、管理対象システムへ接続いただけます。パスワードはマスタ管理者のみ閲覧することができ、パスワードの漏えいリスクを軽減します。



Access Check Essential 主な機能③　ログ取得・保管

Access Check Essentialを経由して行った操作をまるごと記録するため、有事の際にも簡単に追跡可能

アクセスログと操作ログの取得

アクセスの概要をまとめた「アクセスログ」と、実際の操作内容を記録した
「操作ログ」の2種類のログを取得することができます。

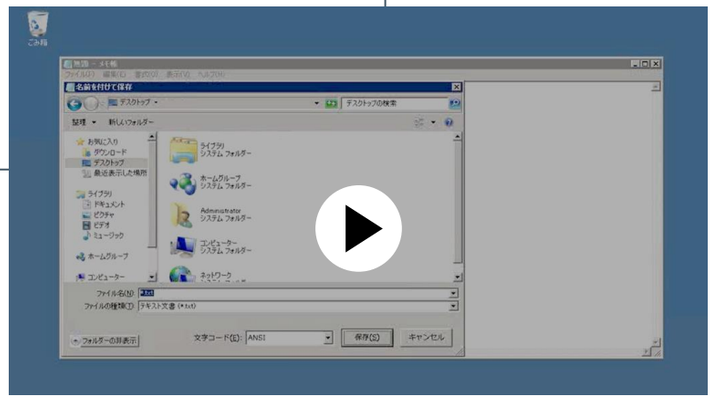
操作ログは、プロトコルに応じて形式が異なります。
SSH接続の場合、コンソール画面に表示されたテキスト形式で取得されます。
RDP接続の場合、画面操作を動画で記録します。
SCP接続の場合、コマンドログと転送したファイル実体を記録します。

取得したログの保護

ログは暗号化して保存されます。また、ログの改ざん検知機能を備えています。
取得したログは監査担当者だけが参照でき、内部監査のモニタリングや
内部統制の証明として有効です。

SSH接続の操作ログ（イメージ）

```
1  ↓
2  ↓
3  【登録されているキーワード】(いずれかのキーワードを含む)↓
4  1.exit↓
5  2.ls↓
6  3.pwd↓
7  ↓
8  【キーワードを含むレコード】↓
9  24:[admin@node01 ~]$ ls↓
10 29:[admin@node01 ~]$ pwd↓
11 33:[admin@node01 ~]$ exit↓
12 ↓
13 ↓
14 ↓
15 yes↓
16 Warning: Permanently added '172.20.197.11' (RSA) to the list of known hosts.↓
17 This access will not login automatically. please enter the password.↓
18 admin@172.20.197.11's password: ↓
19 Last login: Thu Aug 28 10:24:15 2014 from 172.20.197.4↓
20 [admin@node01 ~]$ ↓
21 [admin@node01 ~]$ ↓
22 [admin@node01 ~]$ ↓
23 [admin@node01 ~]$ ↓
24 [admin@node01 ~]$ ls↓
25 test.txt↓
26 [admin@node01 ~]$ ↓
27 [admin@node01 ~]$ ↓
28 [admin@node01 ~]$ ↓
29 [admin@node01 ~]$ pwd↓
30 /home/admin↓
31 [admin@node01 ~]$ ↓
```



RDP接続の操作ログ（イメージ）

（補足）有事の際にすぐに該当のログを検索可能

画面を録画するだけでなく、アクセス日時やユーザから検索することが可能

検索したい期間、利用者やプロトコル、接続元/接続先IPアドレスなどで検索対象を絞り込むことができます。

実際の操作内容は、ファイルとしてダウンロードすることで確認できます。

Access Check Essential 主な機能④　監査補助

日次レポートによる集計や不正検知機能など、監査業務を支援

日次レポート機能

指定された監査者向けに、アクセスログの一覧をメールで配信します。
（レポートはPDFファイル形式、またはCSVファイル形式です。）

アクセス時の操作ログに、事前に登録した検知キーワード（危険なコマンドなど）が含まれているかも、レポートから確認することができます。

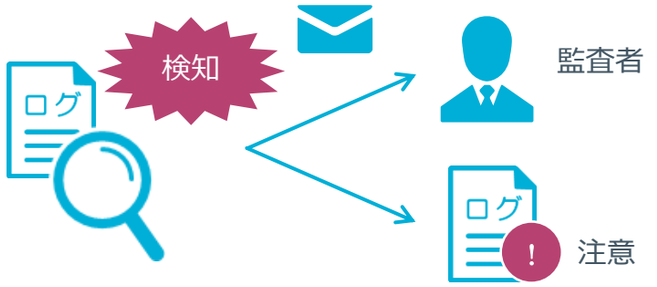
ダッシュボード機能

取得・保管しているログの中からセキュリティ違反につながりやすい情報を抽出し、管理者・監査者のダッシュボード上に表示します。

不正検知機能

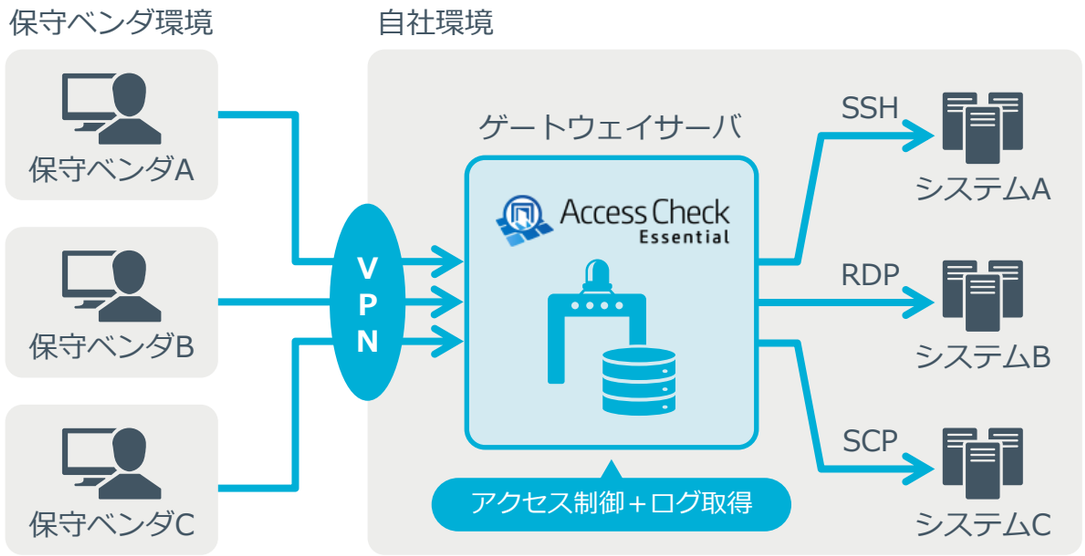
取得した操作ログに事前に登録したキーワード（危険なコマンドなど）が含まれていないかをチェックし、含まれている場合には、その都度、監査者へ通知します。

保存されている操作ログに対して、改ざん、または削除されていないか確認し、管理者にその結果を通知します。



Access Check Essential 活用事例

リモートアクセスの管理



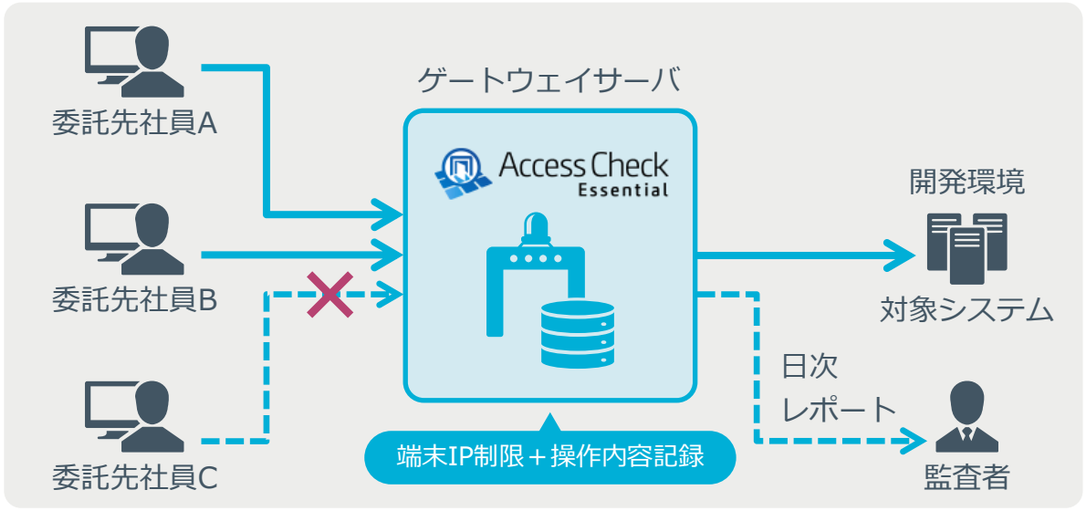
アクセスできるシステムを最小限に制御

各保守ベンダがアクセスできる対象のシステムを制御し、不正なアクセス制御を防止します。

すべての作業内容を記録・保管

操作の内容だけでなく、RDP接続時にクリップボード共有で取得したファイルやSCP接続時の転送したファイルの実体もログとして取得します。

委託先社員のアクセス管理



端末のIP制限により不正なアクセスを拒否

ポリシー設定により、特定のIPアドレスからの接続のみ許可することで、特定端末以外からのアクセスを拒否することができます。

日次レポートによるアクセス状況の把握

取得したアクセスログを日次でレポート配信することができます。
また、不正なキーワードが含まれる場合にはそれを検知します。

Access Check Essential の導入の流れ

1. 注文書送付
2. 弊社より提供する VMイメージを受領
3. VMイメージを 仮想基盤で展開
4. ネットワーク設定、 利用者登録して完了

Access Check Essentialの VMイメージ

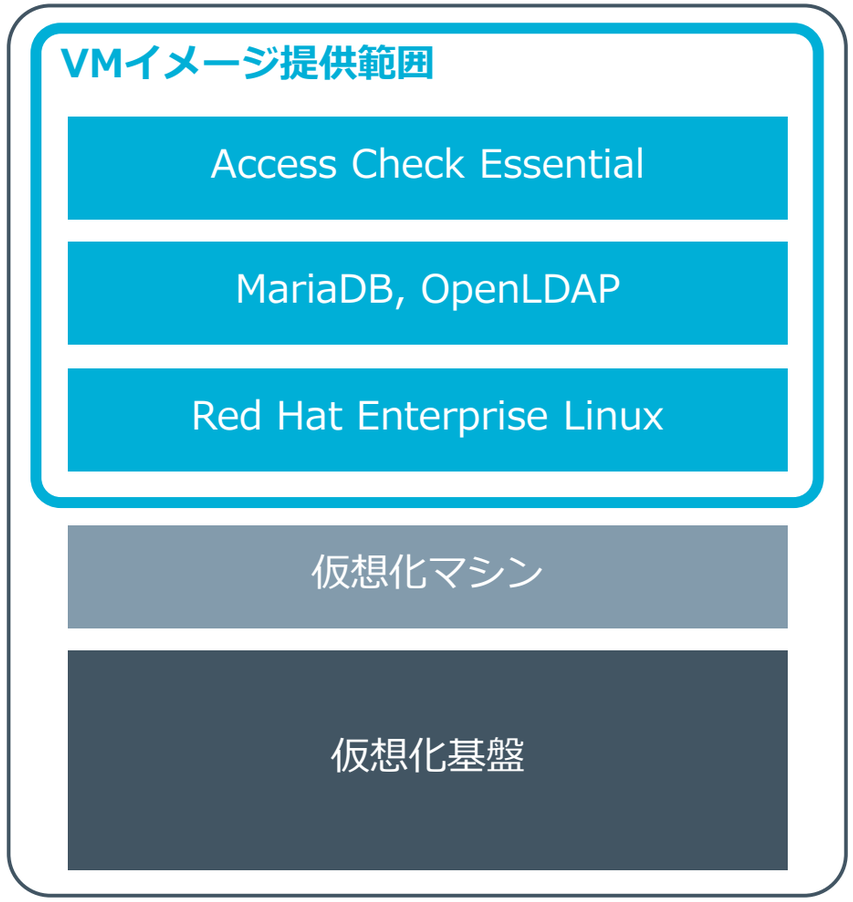
- **VMWare/AWS**に対応しています。
- Red Hat Enterprise Linux上に作成するため、**お客様にてサブスクリプションライセンスをご用意ください。**
- 各設定項目（例：パスワードポリシーやログ保存期間など）は弊社にてデフォルト値を入力して作成します。**必要に応じて、自社の設定に変更ください。**
- ベースとなる1ポリシー、および、全システムに接続可能なIPアドレス（0.0.0.0/0）を設定した1接続ノードをあらかじめ登録しておきます。**利用者/管理者アカウントの登録をお願いします。**

Access Check Essentialの 導入支援

- **QA対応のみ**のAccess Check Essential専用導入パックをご利用いただけます。
- VMイメージのデプロイ手順、および利用を開始するにあたって必要な設定の簡易手順書を提供しますので、**お客様にて導入作業を実施します。**

- **最低限必要な作業(想定)：**
  - ・VMイメージのデプロイ
  - ・ネットワーク設定（設定ツール提供予定）
  - ・ユーザ/管理者のアカウント登録
  - ・稼働確認

Access Check Essential の動作環境



※　シングル構成のみ可能

Access Check　Essential 動作環境

仮想化基盤	VMWare / AWS
OS	Red Hat Enterprise Linux Server **8**（8.8）※1
CPU	**2.50**GHz × **8**Core 以上
メモリ	**16**GB 以上※2
HDD	**500**GB 以上※3
ネットワーク	**1**つ以上のNIC

※1　Red Hat Enterprise Linuxのサブスクリプションライセンスはお客様にてご用意をお願いします。

※2　RDP中継が多い、またはSCP中継でサイズの大きい（数百MB以上の）ファイルを転送する場合には、大きめのメモリ量が必要です。

※3　ログ保存の要件によっては増設が必要です。

（ご参考）統制レベルとソリューションマッピング

	Phase1	Phase2	Phase3
管理対象機器	重要システムのみ	重要システム以外の機器も徐々に管理対象に加えていく	AWSやAzure等のクラウドサービスの特権も管理対象に加える
アクセス制御	ユーザの属性を基に、アクセス制御の範囲を広めに設定する	アクセスできる範囲をユーザ毎に必要最小限にする	認証強化を目的に、二要素認証に切り替える
ワークフロー	作業のための申請・承認はなし	作業のための申請・承認を行う	多段承認を取り入れ、申請内容の確認強度をあげる
ID・パスワード管理	アクセス管理のみ、管理対象機器のID・パスワード管理はなし	管理対象機器のID・パスワードを管理し、パスワードを秘匿化	パスワードの秘匿化だけでなく、パスワード定期更新も実施する
システム構成	シングル構成	冗長構成に変更する	DR環境も用意する

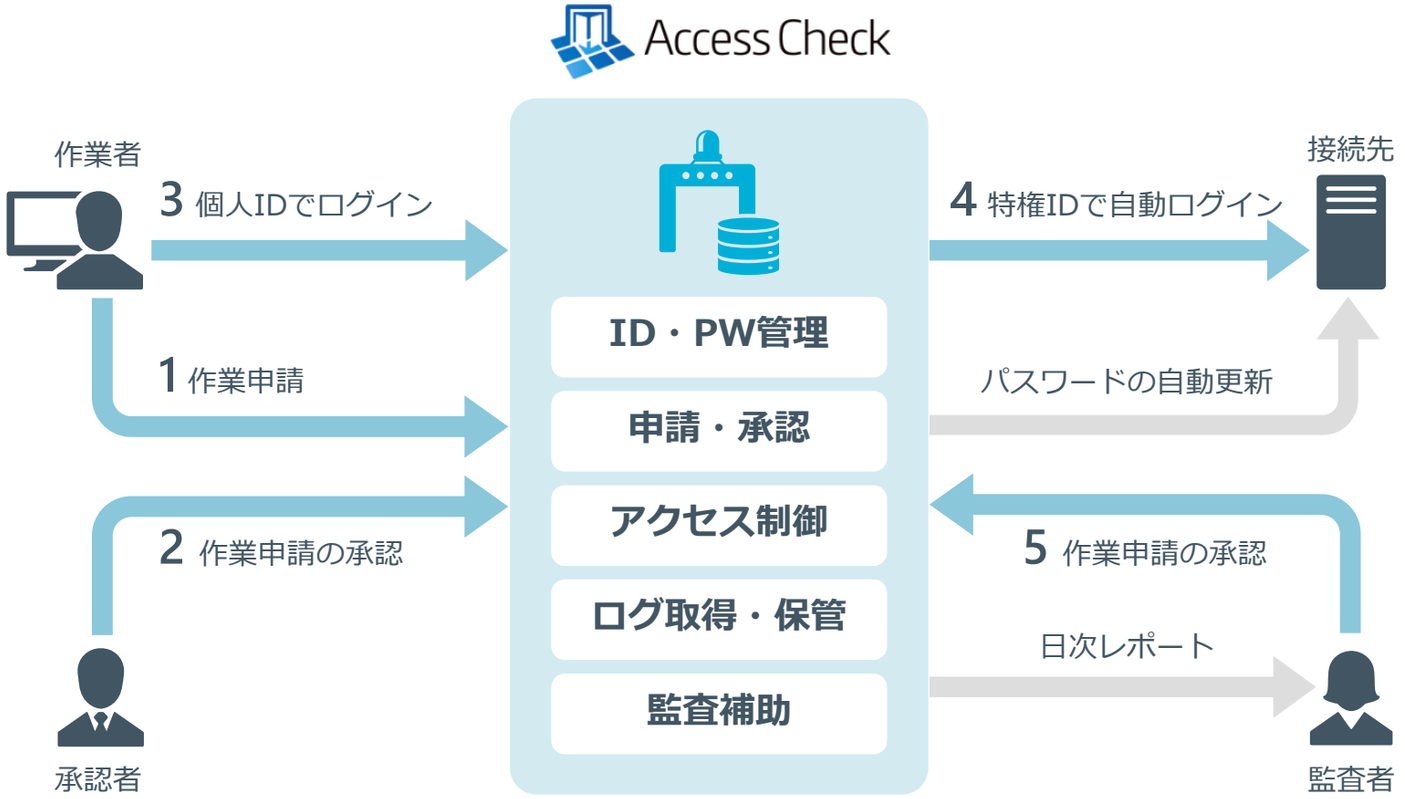
Access Check Essential

Access Check

Access Check
＋有償オプション

（ご参考）SecureCube Access Checkの特長

- NRIセキュアが金融機関のシステム保守業務のため開発した、安全性の高い特権ID管理ソリューション
- 下記3つの特長があるほか、専門エンジニアによるきめ細やかな保守サポートも好評



3つの特長

ゲートウェイ型なので
導入・運用が容易

充実した機能と
制約条件が少なく
多様な環境での利用可能

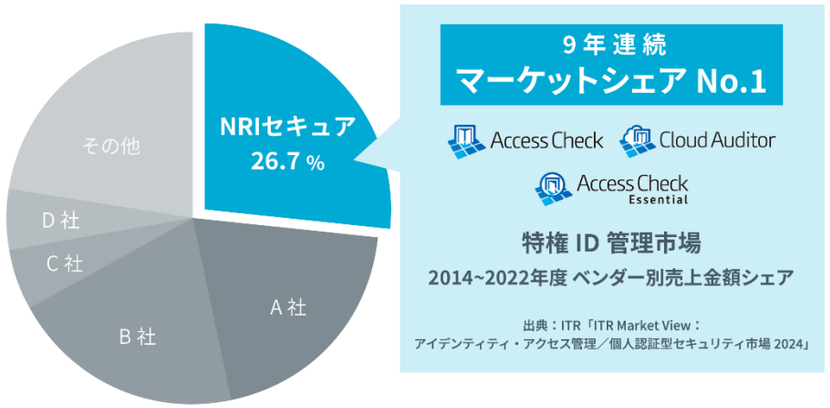
多くのお客様に支持され
市場シェアNo.1※と
豊富な導入実績

※ 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, Access Check Essential, Cloud Auditor by Access Check が対象

（ご参考）Access Checkシリーズの外部評価

市場シェア・品質について、以下の外部評価をいただいており、安心して導入可能

特権ID管理市場 9年連続トップシェア



株式会社アイ・ティ・アールが行った特権ID管理市場に関する最新調査※1において、**9年連続でマーケットシェアNo.1**※2を獲得しています。

※1 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2024」特権ID管理市場：ベンダー別売上金額シェア（2022年度）に掲載。 SecureCube Access Check, Access Check Essential, Cloud Auditor by Access Check が対象。

※2 特権ID管理市場における2014～2022年度のベンダー別売上金額によるマーケットシェア。

カンパニーオブザイヤー：日本の特権アクセス管理業界で最高水準と認定

米大手リサーチ・コンサルティング会社、フロスト＆サリバンが主宰する「2023 フロスト＆サリバン ベストプラクティス アワード」において、**日本の特権アクセス管理市場の分野で最高位の表彰（Japan Privileged Access Management Company of the Year Award**※）を受けました。

※ フロスト＆サリバン社が発行したレポート「2023 カンパニーオブザイヤーアワード　日本特権アクセス管理市場（NRIセキュア）」に掲載。

目　次

内部不正を防ぐため、対策の見直しを行い、犯行の機会を減らすことが重要

- 内部不正によるセキュリティインシデントは繰り返し発生している
- 内部不正を防ぐには、不正のトライアングルの動機・機会・正当化を崩すことが重要
- システム管理において「アクセス制御」と「ログ取得」により、内部不正の機会を減らすことが可能
- 効率良くアクセス制御・ログ取得を行うために、専用ソリューションの活用がおすすめ
- Access Check Essentialは、効率的なアクセス統制を短期間・低コストで実現可能

特権ID管理ソリューション
「SecureCube Access Check」
について詳しく知りたい方は、
毎月開催の定期セミナーにも、
ぜひご参加ください

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

お申込みは
こちらから

NRI SECURE