NRI SECURE

インシデント事例から見えてくる内部不正を効果的に防ぐ対策とは

2024年2月27日（火）

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

部長　大谷 佳裕

目　次

目　次

会社概要

NRIセキュアテクノロジーズは野村総合研究所を母体とする
企業情報セキュリティのリーディングカンパニー

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
社員数	連結：750名、単体：638名
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
認証取得	ISO/IEC 27001認証取得　IS 75215 / ISO 27001

セキュリティコンサルティング

サイバーセキュリティ
コンサルティングサービス5分野*1

**マーケット
シェアNo.1*2**

ITR Market View2023
（2022年度）

マネージドセキュリティ

ジャパン マネージド
セキュリティサービス

**プロバイダー
オブザイヤー 受賞**

Frost & Sullivan
（2017～2021年）

セキュリティソリューション

特権ID管理ソリューション
「Access Check」シリーズ*3
特権ID管理市場

**8年連続
シェアNo.1*4**

ITR Market View2023
（2014～2021年度）

セキュリティソリューション

統合IAMソリューション
「Uni-ID Libra」
CIAM市場

**6年連続
シェアNo.1*4**

ITR Market View2023
（2016～2021年度）

出典：*1 次の5分野 ▶セキュリティコンサルティング・プランニングサービス市場 ▶セキュリティ脆弱性診断サービス市場 ▶IoT/OTセキュリティ脆弱性診断サービス市場 ▶セキュリティ監査サービス市場 ▶BCP／BCM対策構築運用支援サービス市場
*2 ITR「ITR Market View：サイバー・セキュリティ・コンサルティング・サービス市場2023」2022年度　*3 「Access Check」シリーズ： SecureCube Access Check, Access Check Essential, Cloud Auditor by Access Check が対象
*4 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」2021年度　：以上すべてベンダー別売上金額ベース

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

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**

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。

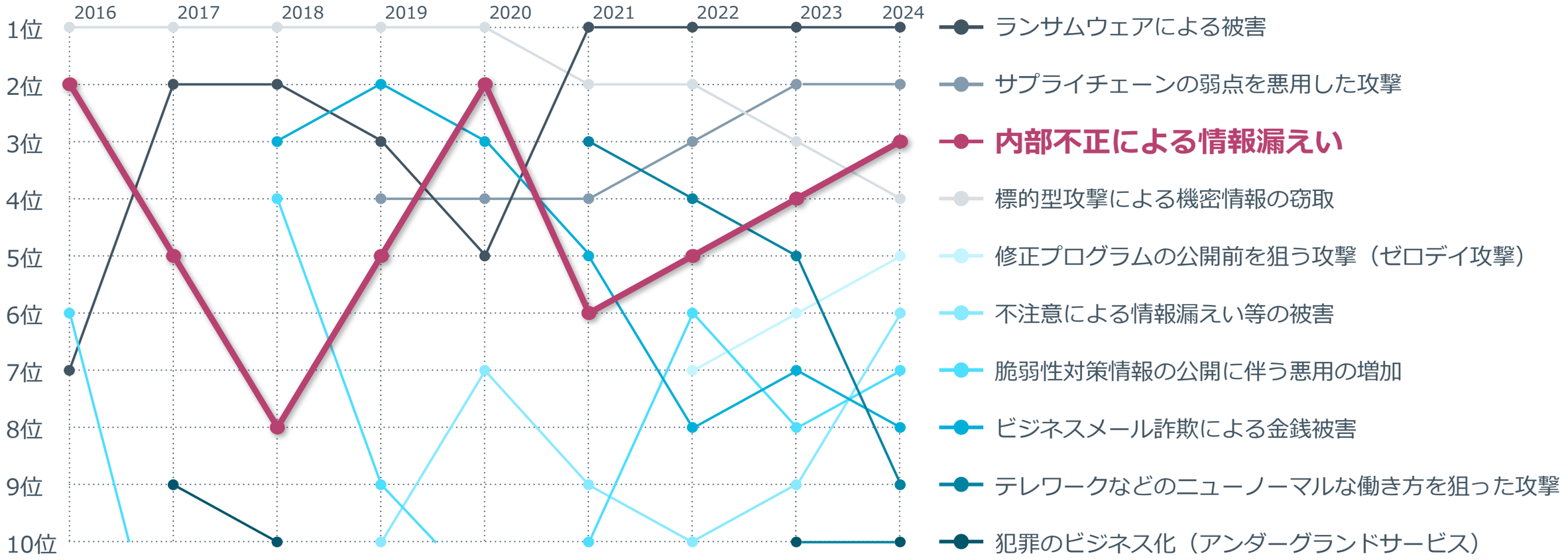
豊かな未来づくりのために
挑戦を続けるお客さまとともに
誰もが安全に安心して
ITの魅力を自由に楽しめる社会をつくる。

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

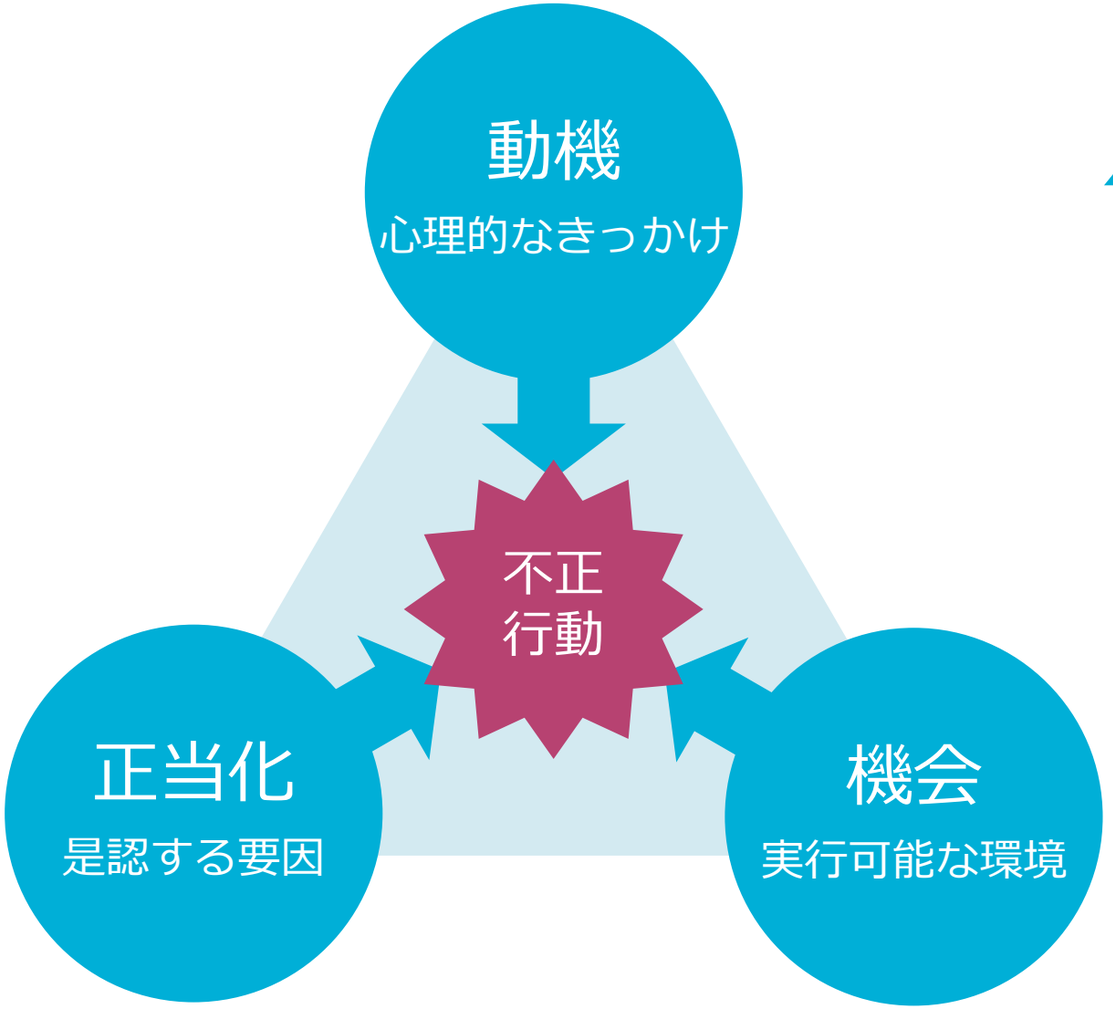
内部不正によって引き起こされる影響は、一時的なビジネス活動への支障だけでなく、社会的信用の失墜、損害賠償、事後対応にかかる労力や費用の増大等、多大な損失が考えられる

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

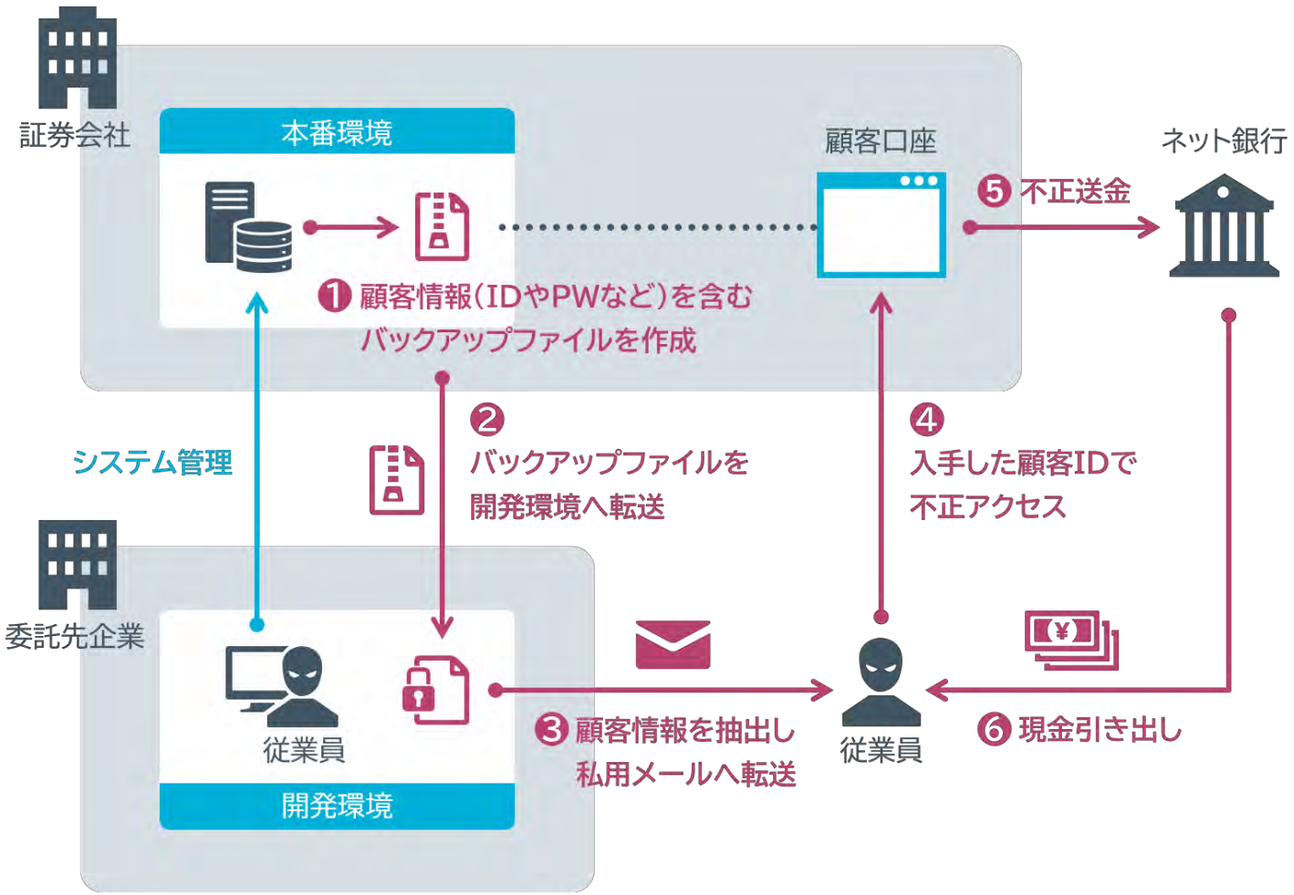
不正のトライアングルを崩すには　–内部不正防止の基本原則–

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

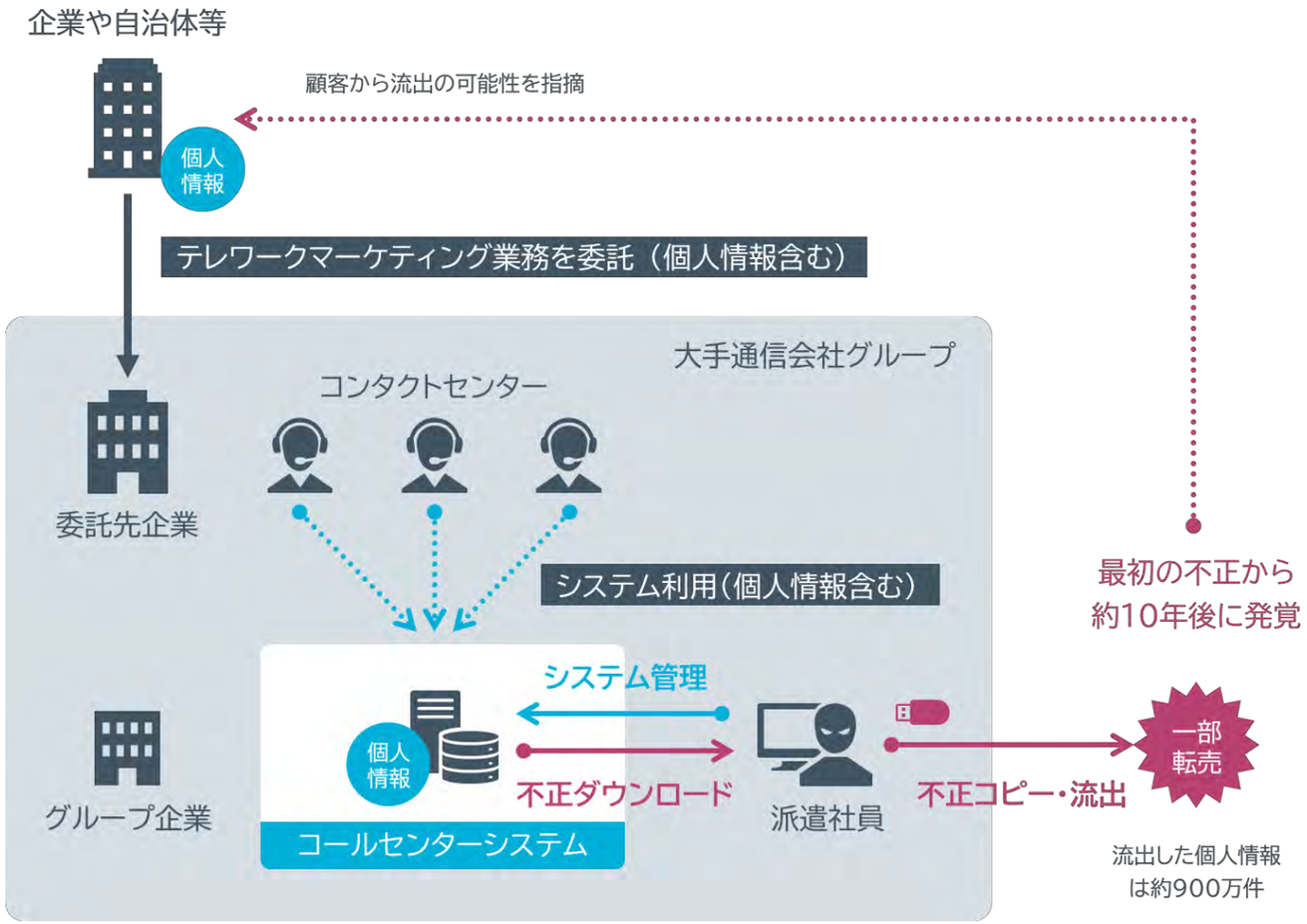
2017年から約2年半にかけて、証券取引システムの開発・保守を担っていた委託先の元従業員が、顧客情報を不正利用し、約2億円を不正出金

→ **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

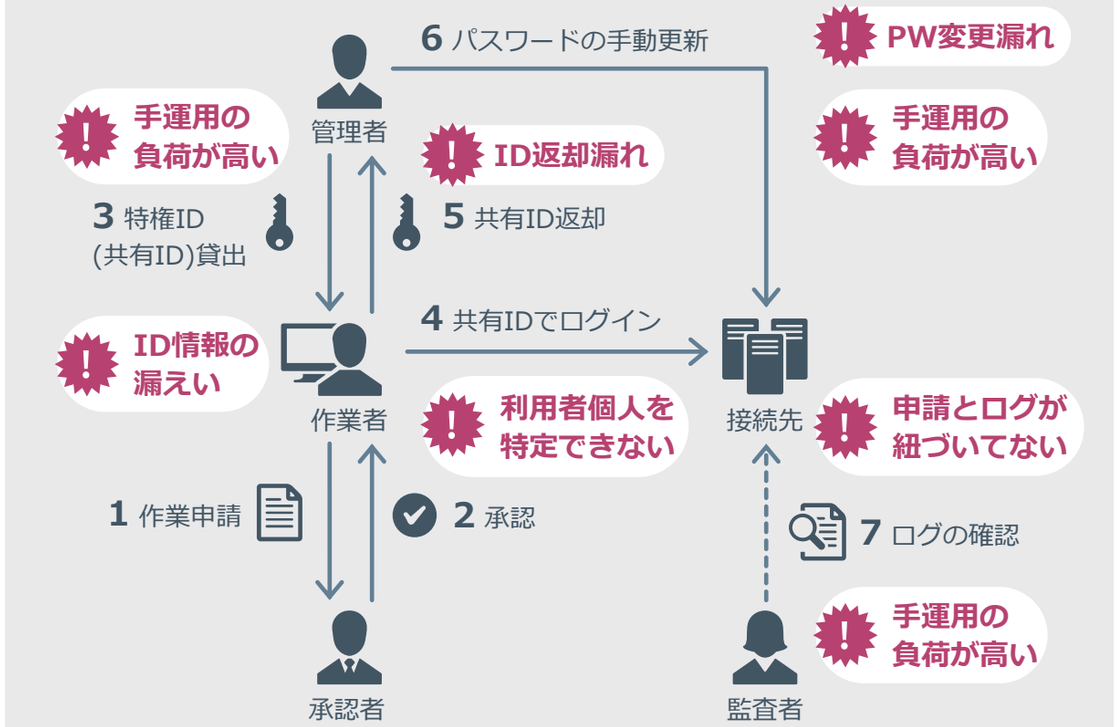
自社の運用やリスク評価に応じて、段階的に対応を進める

	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
弱	✓ 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
統制レベル	✓ 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	✓ 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

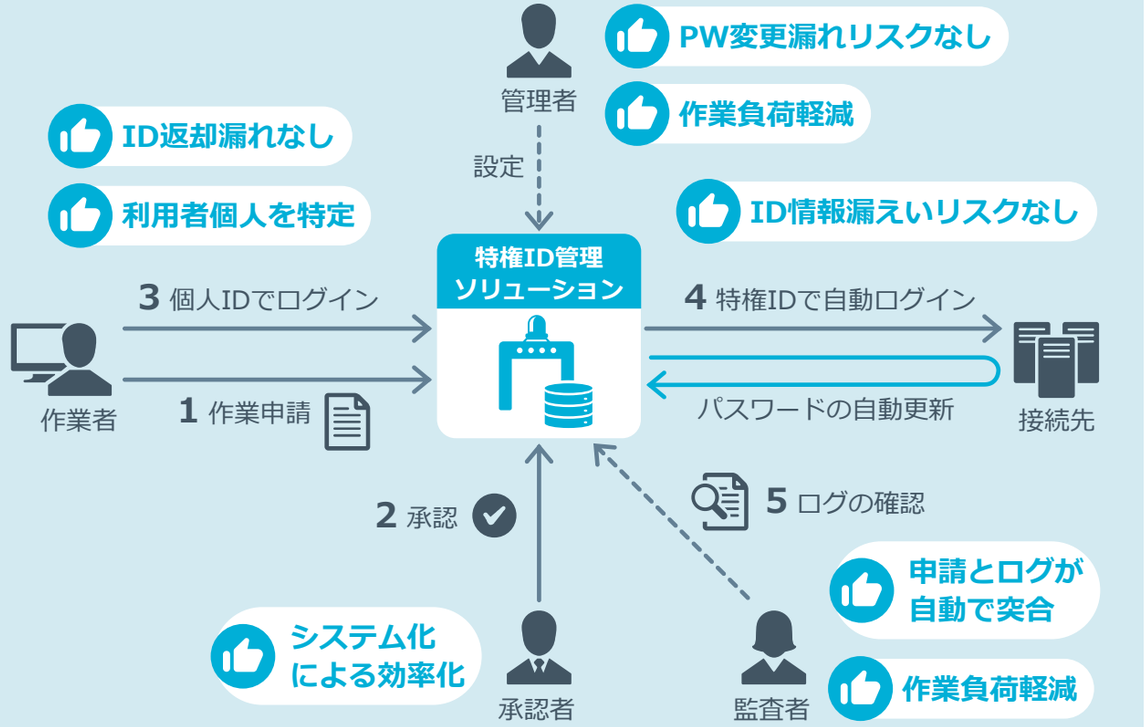
特権ID管理ソリューションを用いて内部不正対策を効率的に実現

- 手運用でも最低限の対策は可能だが、管理負荷等の課題が残る
- 特権ID管理ソリューションを用いることで、運用工数の削減や作業漏れ・ミスなどの防止が期待できる

手運用に残る課題

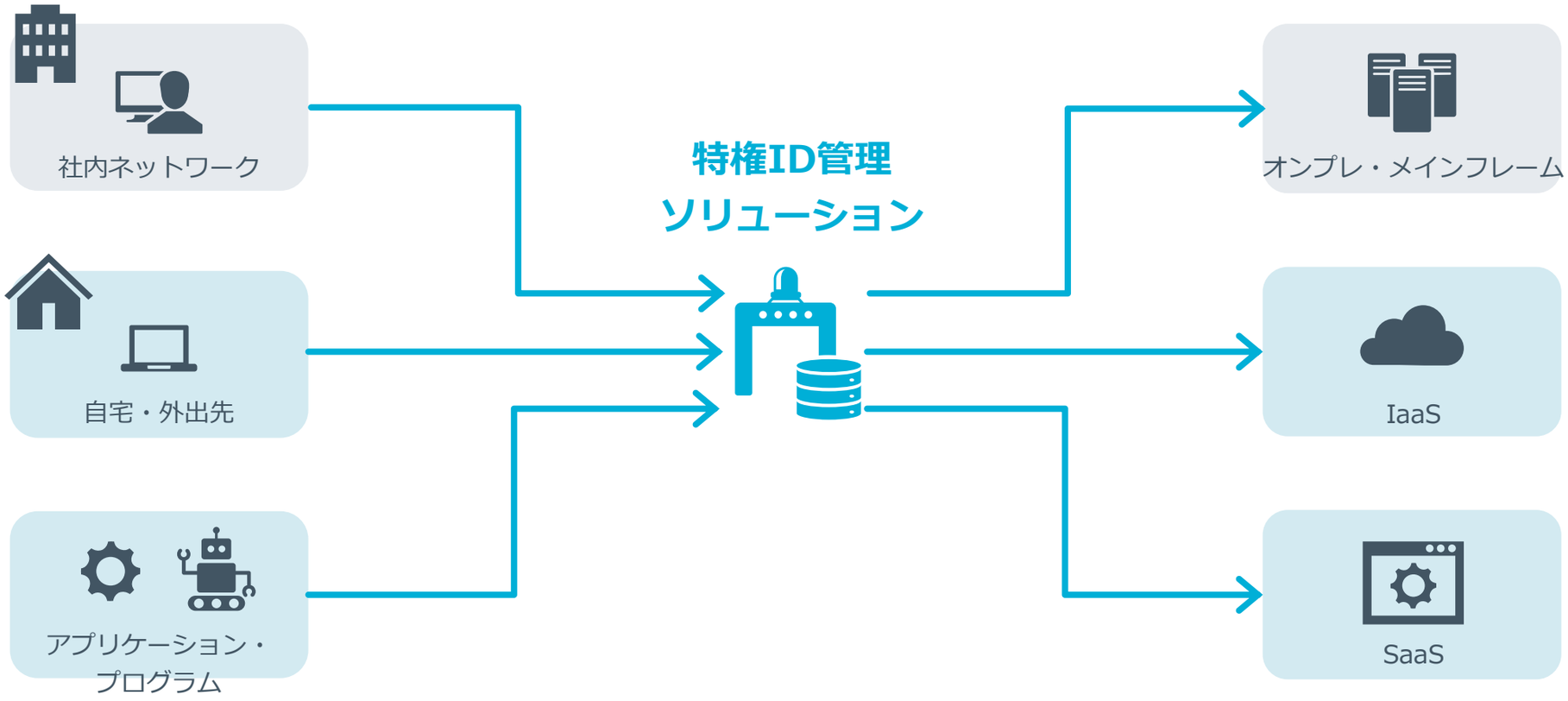


特権ID管理ソリューション利用のメリット



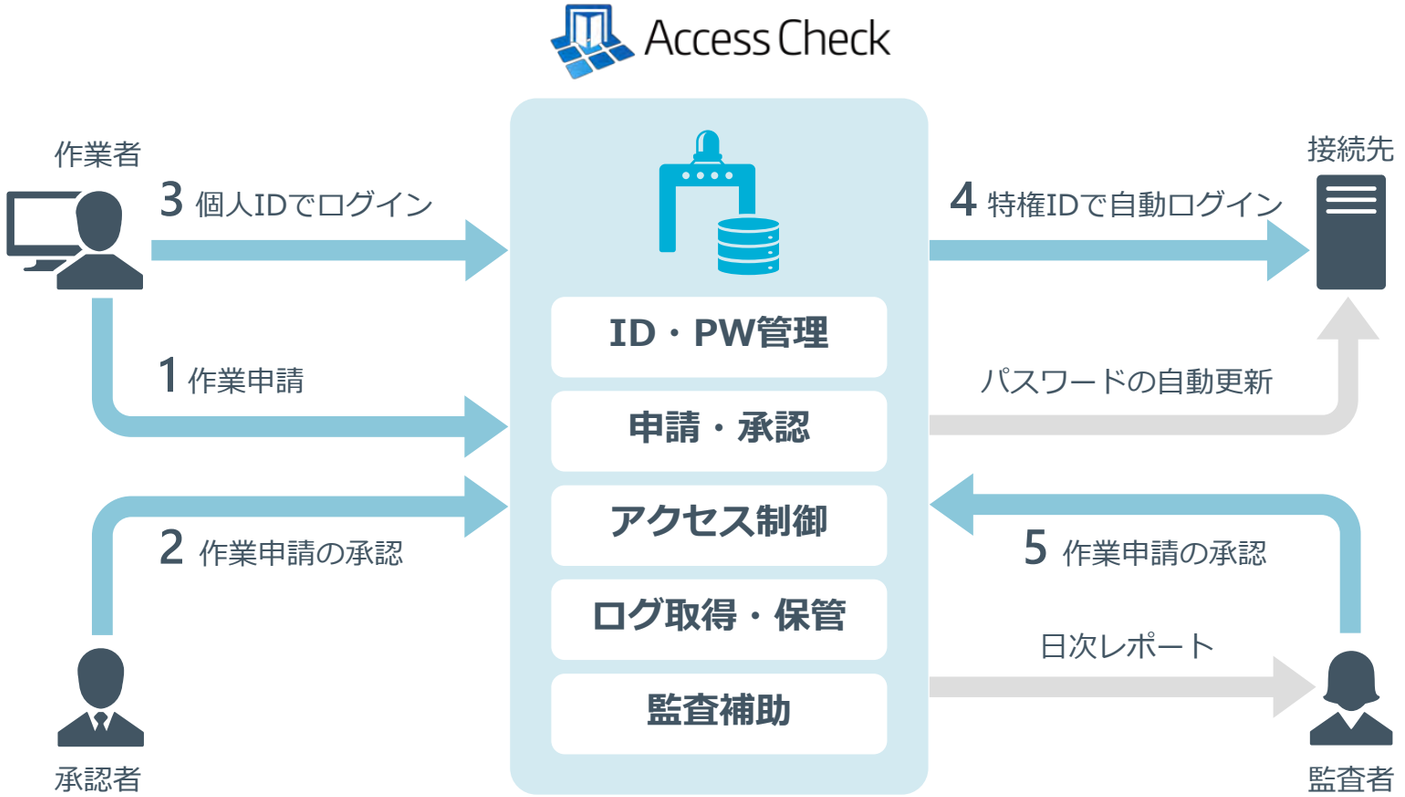
特権ID管理ソリューションならシステム環境の複雑化にも対応

- クラウドサービスの利用拡大、リモートワークへの切り替え、アプリケーションによる管理者権限の利用等、システム環境は大きく変化しているため、特権ID管理で考えるべき範囲も広がっている
- 自社の運用に適用できることはもちろん、拡張性も視野に入れたソリューション選定が望まれる



（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

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
- 内部不正時に利用されやすい「**特権ID**」の管理を行うことで、内部不正の機会を減らすことが可能
- 昨今のシステム環境では、これまで考慮していなかった「**特権ID**」とその利用機会が存在
- 効率良く**特権ID管理**を行うために、専用ソリューションの導入をご検討ください

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