AiLockランサムウエアによる日本交通侵害事案
リーク目録（インデックス）分析報告書

対象ファイル: nihon-kotsu_lst20260811.zip（リークサイト掲載の窃取データ目録／データ本体は含まれない）

作成日: 2026年8月11日 ｜ 分析種別: 公開目録に基づく到達範囲・攻撃者力量の推定と防御側教訓の抽出

本報告書の目的

本報告書は、AiLockランサムウエアグループのリークサイトに掲載された「目録（ファイルツリー一覧）」を静的に分析し、(1) 攻撃者がネットワーク内のどこまで到達し得たか、(2) その手法・力量として何が推定できるか、(3) 防御側が今後のシステム構成・権限管理に活かすべき教訓は何か、を整理したものである。窃取されたとされるデータそのもの（文書・画像・データベース等の中身）は本分析には一切含まれておらず、目録に記載されたパス名・拡張子・サイズ・ディレクトリ構造のみを分析対象としている。

目次

1. エグゼクティブサマリー

2026年8月、AiLockランサムウエアグループは日本交通を標的とした攻撃を主張し、リークサイト上に窃取データの「目録」（`nihon-kotsu_lst20260811.zip`、展開後 `nihon-kotsu.lst`、約54MB・約57万行）を公開した。本目録を機械的に解析した結果、以下の点が確認された。

項目	目録記載内容からの推定値
目録に記載されたファイル数	約52.3万ファイル（フォルダ数 約4.8万）
目録記載サイズの合計	約2.9TB（テラバイト）
到達が確認できるルート区分	全社共有ドライブ、約60拠点・部門別共有フォルダ、SQLサーバーのフルバックアップ領域、運転免許証等の個人識別データ専用フォルダ、$RECYCLE.BIN（ごみ箱）
最大単一ファイルサイズ	256GB（SQLデータベースのフルバックアップ、2ファイル）
データの新しさ	ファイル名から2026年（攻撃直近）の給与・契約データを含むことを確認

最重要所見: 攻撃者は特定の端末やフォルダに限定されず、**全社の部門別ファイル共有（約60拠点）とSQLサーバーの完全バックアップ領域の双方に到達**していたと推定される。これは単一エンドポイントの侵害にとどまらず、ファイルサーバー管理者相当、またはドメイン管理者相当の高い権限を攻撃者が獲得していたことを強く示唆する。加えて運転免許証画像・マイナンバー関連書類・給与明細・源泉徴収票等、個人情報保護法上の要配慮性が高いデータ群への到達も確認された。

2. 分析対象データに関する留保事項

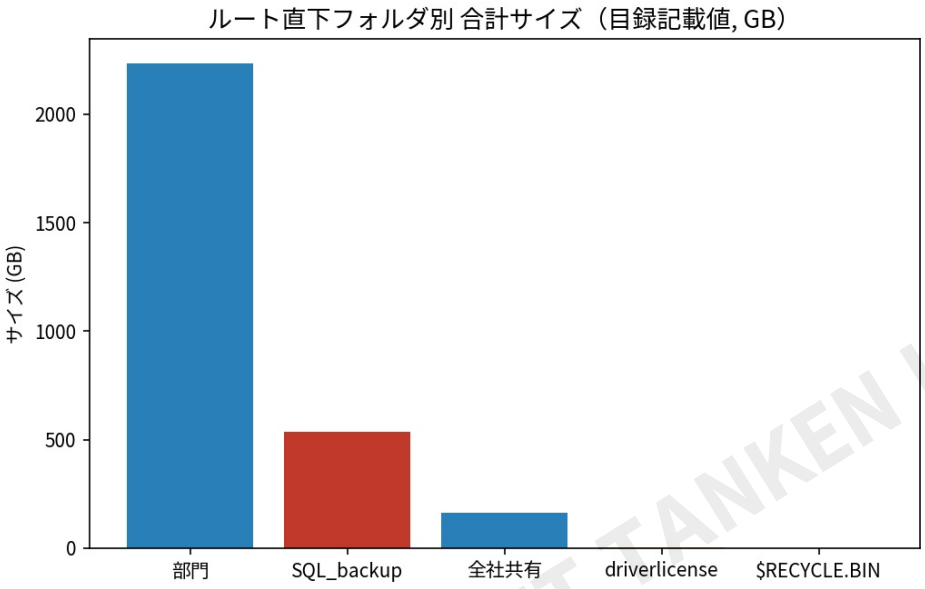
- 本目録は攻撃者（AiLock側）が自らリークサイトに掲載した一覧であり、**実際に窃取したデータの完全性・正確性を第三者が検証したものではない**。誇張、選別的掲載、あるいは実際にはコピーせずアクセスのみ行ったファイルの記載が含まれる可能性を否定できない。
- したがって本報告書の「到達範囲」は、**目録に基づく推定（下限の目安）**であり、実際の侵害範囲はこれより狭い、あるいは広い可能性がある。
- 本分析ではファイルの中身（内容）には一切アクセスしておらず、パス名・ファイル名・拡張子・記載サイズ・ディレクトリ階層構造のみを機械的に集計している。
- 個人名を含むファイル名が多数含まれるが、本報告書では第三者（従業員・乗務員等）のプライバシー保護の観点から、個人名は具体例として引用せず、データ種別・件数レベルで扱う。

3. 目録の基礎統計

3.1 ルート構造

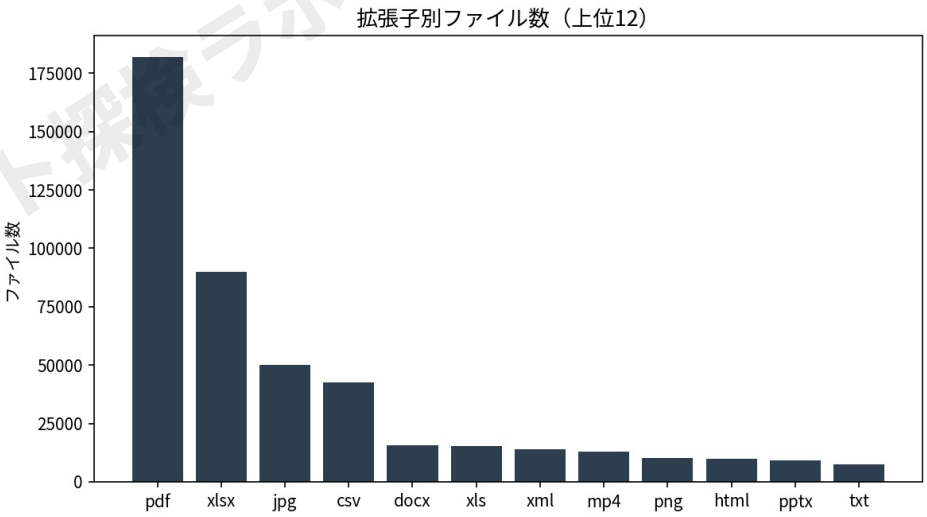
目録のルート直下は5つの区分から構成されており、いずれも同一の目録内に併記されていた。

ルート直下フォルダ	ファイル数	合計サイズ（記載値）	内容の推定
部門	419,968	約2,233.8 GB	拠点・部門別の業務共有フォルダ（約60拠点）
全社共有	99,026	約161.8 GB	全社共通の共有ドライブ（給与・人事・IT関連含む）
SQL_backup	8	約536.6 GB	基幹システムのSQLサーバー フルバックアップ（.bak）
driverlicense	3,937	約3.4 GB	乗務員等の運転免許証画像専用フォルダ
$RECYCLE.BIN	3	<0.01 GB	Windowsごみ箱（削除ファイルの痕跡）



3.2 拡張子別の内訳（上位）

ファイル種別からは、一般文書に加えて基幹業務システム固有のバイナリ形式が多数含まれることが確認できる。



拡張子	件数	推定される内容
pdf	182,047	請求書・証明書・帳票類（スキャン文書含む）
xlsx / xls / xlsm	109,640	Excel業務資料（給与集計・分析表等）
jpg / jpeg / png / heic	63,006	写真・スキャン画像（運転免許証画像を含む）
csv	42,493	基幹システムからの出力データ（給与・勤怠等）
docx / doc	20,270	Word文書（契約書・議事録等）
mp4 / wmv / mov / avi	21,506	動画（研修動画、ドライブレコーダー映像等）
db / dat / dat2 / neo / tvr / dsce / obc	約10,900	業務システム固有形式（デジタコ・ドラレコ・会計/給与ソフトのバックアップ）

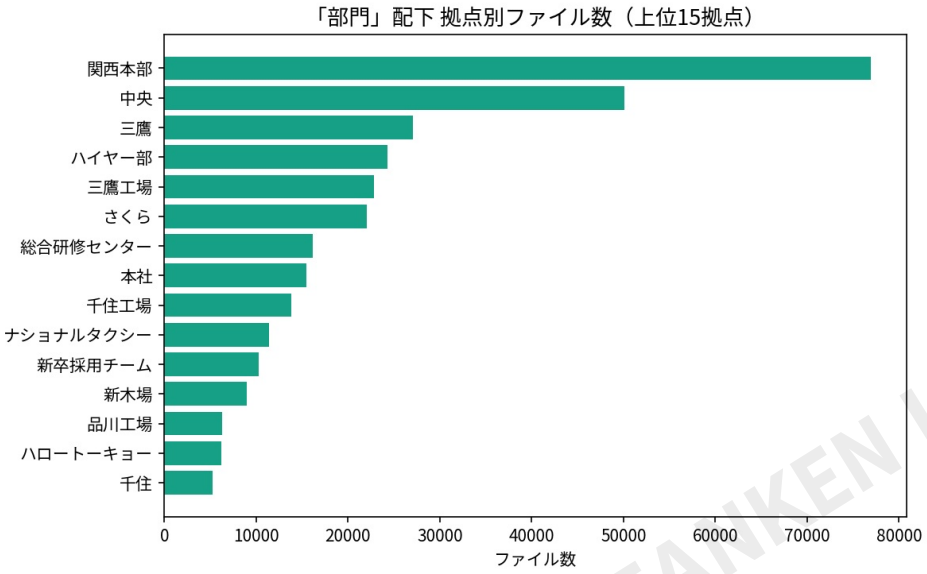
3.3 データの時系列

ファイル名中の年号出現数を集計すると、2020年〜2026年まで継続的にデータが存在し、**2026年（攻撃直近）の給与・契約関連ファイルが約2.3万件**確認できる。これは攻撃者が古い保管データだけでなく、攻撃時点に近い「生きた」業務データにアクセスしていたことを示す。

4. 攻撃者の到達範囲（スコープ）の分析

4.1 全部門・全拠点の共有フォルダへの到達

「部門」フォルダ配下には、本社・ハイヤー部・各営業所・整備工場・関西地区（神戸・京都・梅田・難波・高槻・西淀川・三宮・守口・茨木・堺 等）まで、**約60拠点分の共有フォルダ（Share【拠点名】形式）**がすべて目録に含まれていた。



所見: 通常、拠点別共有フォルダはActive Directoryのグループ／ACLにより当該拠点の従業員のみアクセス可能に制限されるのが一般的である。全拠点分がまとめて窃取・目録化されている状況は、(a) 単一の高権限アカウント（ドメイン管理者、バックアップ管理者、あるいはファイルサーバーのローカル管理者）が奪取された、(b) ファイルサーバー自体（OSレベル）が侵害され、ACLを介さずファイルシステムに直接アクセスされた、のいずれか、あるいは両方が生じたことを強く示唆する。

4.2 基幹データベースのフルバックアップへの到達

`SQL_backup` フォルダには、以下の8つの `.bak`（SQL Serverバックアップ）ファイルが直下に存在していた。

ファイル名	記載サイズ	推定用途
`ORANGE.bak`	256 GB	基幹業務データベース（フルバックアップ）
`BANANA.bak`	256 GB	基幹業務データベース（フルバックアップ）
`APPLE.bak`	24 GB	基幹業務データベース
`PLUM.bak`	398 MB	業務データベース
`ReportServer.bak / ReportServerTempDB.bak`	89 MB / 8.2 MB	SQL Server Reporting Services（SSRS）標準DB
`ASPState.bak`	124 MB	ASP.NETセッション状態管理DB（Webアプリケーション基盤の存在を示す）
`ListenerDB.bak`	4.2 MB	Always On可用性グループ等のリスナー関連DBの可能性

重大所見: `ReportServer` 系DBの存在はSQL Server Reporting Servicesが稼働していたことを、`ASPState` の存在はASP.NETベースの社内Webアプリケーションが存在したことを示す。256GB級のフルバックアップが2本、合計500GB超がバックアップ用共有（と見られる場所）に平置きされていたことは、**バックアップの保管場所・アクセス権限設計に重大な弱点があった**ことを意味する。一般に本番DBサーバーへの侵入なしにこの規模のバックアップへ到達するには、バックアップ格納先の共有フォルダ、バックアップ管理サーバー、あるいはバックアップ運用アカウントの権限が窃取された可能性が高い。

4.3 個人情報の集中フォルダへの到達

- **運転免許証画像**: `driverlicense` フォルダに乗務員番号レンジ別（例: 26434〜35000、35001〜40000 等）にサブフォルダが分けられ、氏名を含むファイル名で表裏の画像が保管されていた。政府発行身分証の画像という機微性の高い情報が、専用の一箇所に集約されていたため、単一フォルダへのアクセスで大量のID画像が一括取得可能な状態だったと推定される。
- **給与・人事データ**: 「弥生給与」「N-pay」等のフォルダ配下に、源泉徴収票、給与差押結果リスト、健康保険・年金関連データ、口座情報、マイナンバー登録シートなど、要配慮性の高い人事給与データが多数含まれていた（関連キーワードでの検出件数は延べ10万件超）。
- **会計データ**: 本社経理課の「勘定奉行」（OBC）バックアップフォルダが含まれ、経理・会計システムへの到達も確認された。

- **採用関連書類**: 履歴書・診断書など、応募者・従業員の機微な個人情報を含む書類も広範囲に含まれていた。

4.4 内部ネットワーク構成情報の露出

目録内のショートカット（.lnk）ファイル名から、以下のような内部ネットワーク・システム構成情報が読み取れる。

種別	読み取れる情報
ファイルサーバーIPアドレス	共有フォルダショートカットの大半が同一IP（`192.168.30.1`）を参照しており、単一の中央ファイルサーバーに拠点別共有が集約されていたことを示す。一部ショートカットは別IP（`192.168.23.45`）を参照しており、複数サーバー構成であったことも示唆される。
基幹ERP	「Glovia iZ」（国産ERP）のログインショートカットが`ap1`（APサーバー）・`db1`（DBサーバー）の2台構成で存在。内部ホスト命名規則の一端が露出。
リモートアクセス	FortiClient（VPNクライアント）のショートカット、および複数の個人フォルダに「FortiClient接続情報.txt」という名称のファイルが存在。VPN関連情報がテキストファイルとして平文管理されていた可能性を示唆する。
その他SaaS/業務システム	Mattermost（社内チャット）、Zoom、IEYASU（勤怠管理）、N-Portal、業務支援システム等、オンプレミスとクラウドが混在した環境であったことが確認できる。

4.5 $RECYCLE.BIN に残る複数ドメイン痕跡

目録中の`$RECYCLE.BIN`には、異なる2系統のWindowsセキュリティ識別子（SID）体系が確認された。

```
S-1-5-21-1887545528-1784076478-4020714316-500 （および -8600）
S-1-5-21-4242897574-2485501222-363680262-500
```

SIDのドメイン識別子部分（先頭の数値群）が異なることから、**少なくとも2つの異なるドメイン／ローカル管理体系に属すホストの痕跡が同一の目録内に混在している**と考えられる。これは (a) 複数のファイルサーバー・ホストから収集したデータを1つの目録にまとめて公開している、(b) 過去のドメイン移行・M&A等の履歴が残っている、のいずれかを示唆し、少なくとも攻撃が単一ホストにとどまらず複数システムに及んだ可能性を裏付ける傍証となる。

5. 攻撃手法・力量の推定

5.1 AiLockグループの一般的特徴（公開情報より）

AiLockは2025年3月頃に初めて確認されたRaaS（Ransomware-as-a-Service）型グループであり、二重恐喝（データ窃取＋暗号化、支払わない場合は規制当局や競合他社への通報も示唆）を特徴とする。マルウェアはC/C++で書かれ、ChaCha20（ファイル暗号化）とNTRUEncrypt（メタデータ保護）を組み合わせたハイブリッド暗号方式を採用し、IOCP（I/Oコンプリーションポート）による複数スレッド設計（パストラバーサルスレッドと暗号化スレッドの分離）で高速処理を行う。公開されているMITRE ATT&CK技術には、`T1135`（ネットワーク共有の探索）、`T1134.001`（トークン偽装/窃取）、`T1082`（システム情報探索）、`T1486`（データの暗号化による影響）、`T1489`（サービス停止）等が含まれる。初期侵入手法は業界的に確定情報が乏しいが、同種のRaaSグループ全般ではVPN／RDP等リモートアクセスサービスの認証情報窃取・悪用が主要な侵入経路として頻繁に報告されている。

5.2 本件目録から推定される力量

観点	推定内容
権限レベル	約60拠点分の共有フォルダとSQLバックアップ領域の双方に到達していることから、単一ユーザー端末の侵害にとどまらず、**ファイルサーバーまたはドメインレベルの高権限**を獲得していた可能性が高い（AiLockの既知手法であるT1134.001トークン窃取と整合的）。
内部探索(Discovery)の徹底度	T1135（ネットワーク共有探索）に合致する形で、本社・拠点・工場・健康保険組合まで漏れなく列挙されており、探索が自動化ツールまたは十分な時間をかけた手動偵察により網羅的に行われたことを示す。
ステージング/持ち出し対象の選定	単なる無差別コピーではなく、SQLバックアップ、給与、個人情報（運転免許証）等、金銭的・regulatory的に恐喝価値の高いデータ群が明確に含まれており、二重恐喝を意識したデータ選定が行われた可能性がある。
滞留期間（Dwell Time）	2026年直近データへのアクセス痕跡があることから、少なくとも攻撃直前まで内部に留まりデータへアクセス可能な状態にあったと考えられる。目録だけでは正確な滞留期間は特定できないが、広範囲な列挙・大容量データの持ち出しには相応の時間を要したと推定される。
初期侵入経路	目録単体からは特定不可。ただし社内共有フォルダにVPNクライアント（FortiClient）や接続情報ファイルが多数存在することから、リモートアクセス経路（VPN/RDP）の認証情報窃取・悪用が有力な仮説の一つとして考えられる（確定情報ではない）。

> 本目録には暗号化やランサムノートに関する記載（例: Readme.txt等）は含まれておらず、これは目録が「暗号化前に持ち出したデータの一覧」であるため妥当である。すなわちこの目録は、AiLockの攻撃ライフサイクルにおける**データ探索・ステージング・持ち出し（Discovery→Collection→Exfiltration）段階の成果物**であり、その後の暗号化（Impact）フェーズとは別の証跡として扱うべきである。

6. 防御側への教訓と推奨対策

本目録から得られる示唆に基づき、今後のシステム構成・権限管理において特に優先度の高い教訓を以下に整理する。

6.1 重大 ファイル共有の平坦化・過剰な水平展開の是正

> **問題:** 単一の中央ファイルサーバー（192.168.30.1）に全拠点・全部門の共有フォルダが集約され、結果として一度の侵害で全社データへの到達を許した。

- 部門・拠点単位でのACL（アクセス制御リスト）を「作成時点の建前」ではなく定期的に棚卸し、実際に業務上必要な最小範囲に限定する。
- 特に人事・給与・個人情報・会計データについては、一般業務共有と物理的／論理的に分離した専用ボリューム・専用ACLで管理する。
- ファイルサーバーの水平展開（1台のサーバーに全社の共有を集約する構成）を見直し、機密度の高いデータ領域は独立したサーバー・ドメイン・信頼境界に分離する（マイクロセグメンテーション）。

6.2 重大 バックアップの隔離・不変化

> **問題:** 数百GB規模のSQLフルバックアップが一般アクセス経路から到達可能な場所に平置きされていた。

- バックアップの保管先は本番ネットワークから論理的・可能であれば物理的に分離し、通常の管理者アカウントでは読み取れない構成（イミュータブル/WORMストレージ、オフラインバックアップ、専用バックアップドメイン）とする。
- バックアップ運用アカウントは本番AD管理者アカウントと分離し、多要素認証・強力な資格情報管理を適用する。
- バックアップファイルへのアクセス自体を監査ログ対象とし、通常時に発生し得ない大容量読み取り・コピーを検知するアラートを設定する。

6.3 高 特権アカウント管理の強化

> **問題:** 全社規模のフォルダ横断アクセスとバックアップ領域への到達は、ドメイン管理者相当またはそれに準ずる高権限アカウントの奪取を強く示唆する。

- 階層化管理モデル（Tier 0/1/2）を導入し、ドメイン管理者権限を持つアカウントが一般ワークステーションで使用されない運用とする。
- PAM（特権アクセス管理）ソリューションの導入、LAPS（ローカル管理者パスワードの自動ローテーション）の適用。
- AiLockの既知手口であるトークン窃取（T1134.001）対策として、Credential Guard等のトークン保護機構、EDRによる異常なトークン利用の検知を強化する。

6.4 高 リモートアクセス（VPN/RDP）の強靭化

- VPNクライアントへの多要素認証（MFA）を全アカウントに例外なく適用する。
- VPNアプライアンスのファームウェア・既知脆弱性の速やかなパッチ適用と定期的な設定監査。
- 「FortiClient接続情報.txt」のような接続情報・資格情報をテキストファイルで共有フォルダに平文保存する運用を禁止し、パスワードマネージャー等の適切な保管手段へ移行する。
- RDPの直接インターネット公開を廃止し、踏み台（Jump Server）・ゼロトラストアクセス経由に統一する。

6.5 高 個人情報・機微情報の管理強化

- 運転免許証画像等の身分証データは、一般共有フォルダではなく、暗号化・アクセスログ取得・多要素認証が適用された専用の文書管理システム（DMS）またはVaultで管理する。
- マイナンバー、給与、健康保険等の要配慮個人情報は「特定個人情報等取扱規程」等の社内規程どおりの技術的アクセス制御（暗号化・権限分離・アクセスログ）が実際に機能しているか定期監査する。
- 個人データを含むファイルへのDLP（データ損失防止）ツールの適用を検討し、大量の個人情報ファイルの外部への一括コピー・送信を検知・遮断する。

6.6 中 内部探索・大量データアクセスの検知

- 短時間に多数の共有フォルダへ横断的にアクセスする挙動（T1135 ネットワーク共有探索に相当）を検知するため、SMBアクセスログの集中監視・UEBA（ユーザー行動分析）の導入を検討する。
- 各主要共有フォルダにハニートークン（おとりファイル）を設置し、アクセス発生時に即時アラートする仕組みを構築する。
- 短期間での大量ファイル読み取り・外部への大容量転送（数十GB〜数百GB規模）を検知するネットワーク監視（DLP／NDR）を強化する。

6.7 中 データ最小化・保存期間の見直し

- 2020年以降の給与・契約・研修動画等が現用共有上に残置されていたことを踏まえ、業務上必要な保存期間を超えた古いデータはオフライン・アーカイブ環境へ退避し、平時のアタックサーフェスを縮小する。
- ファイルサーバー上のデータ棚卸し（データマッピング）を定期的に実施し、機密度分類（公開／社外秘／機密／極秘）をラベル付けして管理する。

6.8 中 インシデント対応体制の整備

- バックアップからの復旧手順を定期的に訓練し、実際に「使える」ことを検証する（バックアップの有無だけでなく復元可能性の検証）。

- ランサムウエア対応を想定したインシデントレスポンス計画・外部専門ベンダーとの事前契約（リテイナー契約）を整備する。
- 本件のように複数ドメイン／複数ホストの痕跡が疑われる場合に備え、フォレンジック調査範囲をファイルサーバー単体に限定せず、関連する全ドメインコントローラー・バックアップサーバーまで拡張する体制を準備する。

7. 総括

本目録の分析から、攻撃者は単一端末やひとつの部門にとどまらず、**全社規模のファイル共有と基幹データベースのバックアップという「最も価値の高い領域」の双方に到達していた**と推定される。これは、境界防御（VPN/ファイアウォール）の突破後、内部での権限昇格・横展開を阻む仕組み（セグメンテーション、最小権限、特権アカウント保護）が十分に機能していなかった可能性を示している。防御側にとっての教訓は、単一の侵入点対策だけでなく、**「侵入されても被害が全社・全システムに拡大しない」構造（ゼロトラスト・セグメンテーション・バックアップの隔離）**への転換が急務であるという点に集約される。
