Rhysidaによるベルリン州政府攻撃の分析——攻撃者の力量推定と防御側への教訓

リークサイト掲載情報および公開報道に基づく脅威インテリジェンス・レポート

2026年9月7日（第2版：リークサイト上のフォルダ構造情報を追加）

要旨

2026年8月28日、ランサムウェアグループ「Rhysida（リシーダ）」は自らのダークウェブ・リークサイトに「Berlin, Germany」と題するエントリーを掲載し、ベルリン州（ドイツの首都であり連邦州の一つ）の行政ネットワークから約5.79TB・約144万ファイルを窃取したと主張した。ベルリン州政府は同日中に恐喝を受けている事実を公式に認め、身代金（30BTC、約200万ユーロ相当）の支払いを拒否。9月4日のオークション期限経過後、Rhysidaは主張するデータの全量をダークウェブ上で無条件公開した。

本レポートは、(1) リークサイトの掲載内容・侵害範囲の主張・認証情報の窃取水準などから攻撃者Rhysidaの技術的力量を推定し、(2) 本事案から得られる防御側（特に自治体・官公庁のシステム構成）への教訓を整理することを目的とする。分析にあたっては、Rhysidaの主張（リークサイト上の未検証情報）と、ベルリン州政府・報道機関による確認済み情報を明確に区別する。

注記（OPSEC）：本調査はリークサイトの公開ページの記述および信頼できる報道の内容のみに基づいており、流出データ本体のダウンロード・閲覧は行っていない。

---

1. 事案の時系列（確認された事実ベース）

日付	出来事	情報の性質
2026年8月7日頃〜12日	フォレンジック調査により、この期間にデータの外部流出が開始していたと特定	報道（捜査当局情報源）
8月14日	ベルリン州のIT部門が侵入を検知。都市開発・住宅担当部局、およびモビリティ・交通・環境担当部局の2部局をネットワークから切り離し	報道
8月23日	上記2部局のネットワーク復旧（隔離期間は約9日間。住宅手当支給や家族支援業務に遅延が発生）	報道
8月28日	Rhysidaがリークサイトに「Berlin, Germany」を掲載。30BTC（当時レートで約200万ユーロ、230〜240万ドル相当）を要求し、7日間のカウントダウンを設定。同日、Der Spiegelが攻撃主体を報道し、ベルリン市長（Kai Wegner）が緊急州議会後に恐喝を受けている旨を公式に認め、支払い拒否を表明	公式発表・報道
8月31日	州政府がデータ窃取の事実を正式確認	公式発表
9月4日	オークション期限到達、支払いなし	報道
9月4日以降	Rhysidaが主張するデータ全量（約5.7〜5.79TB）をダークウェブ上で無条件公開	リークサイト（未検証）

ベルリン州刑事警察局（LKA）、検察、および連邦レベルのセキュリティ機関が捜査を継続している。州政府は「個人データまたはその他の非公開データが含まれている可能性は否定できない」とする一方、流出量・件数について独自の確定数値を公表していない。**現在公開されている詳細な内訳（ファイル数、カテゴリ別件数、個人数など）はすべてRhysida自身のリークサイト掲載情報に由来し、州政府による独立した検**

証は行われていない、という点は本分析全体を通じて重要な前提となる。

なお、ベルリン州は2026年9月20日に州議会（Abgeordnetenhaus）選挙を控えており、本事案は選挙直前という政治的に敏感なタイミングで発生・公表された。

---

2. Rhysidaというランサムウェアグループについて

- **沿革**：2023年5月頃に活動を開始。教育機関を中心に攻撃していたVice Society（DEV-0832）との技術的類似性が指摘されており、その後継ないし関連グループと分析されている。
- **運営形態**：Ransomware-as-a-Service（RaaS）。中核グループがランサムウェア基盤を維持し、実行を担うアフィリエイトに利益分配する形態。
- **標的傾向**：教育、医療、製造、情報通信、政府機関、重要インフラを中心に、2026年8月時点で世界約39か国・280件超の被害を公称。過去の著名な被害組織には英国図書館（British Library）、コロンバス市（米国）、シアトル港湾局などがある。
- **直近動向**：2026年5月にはシュトゥットガルト市当局への攻撃を主張（要求額約33万ユーロ）しているが、こちらはデータ窃取の事実自体が当局により確認されておらず、リークサイト掲載＝実被害確定ではない好例となっている。
- **既知のTTP（CISA/FBI/MS-ISAC合同勧告 AA23-319A、2025年4月更新）**：
  - 初期侵入は主にVPNなど外部公開リモートサービス経由。多くの事例で正規の（窃取済みの）認証情報を用いたログインであり、MFA未導入のVPNが突破口になった事例が報告されている。
  - Netlogonの脆弱性（CVE-2020-1472／Zerologon）の悪用。
  - フィッシングによる初期アクセス。
  - 横方向移動にPsExec等の正規運用ツールを悪用（Living-off-the-land）。
  - 二重恐喝（データ窃取→暗号化→非払い時はリークサイトで公開・オークション）モデル。

以上より、Rhysidaは技術的に極めて高度な独自エクスプロイトを開発する「先端型」グループというより、**認証情報の窃取・悪用と正規ツールの流用を軸とした、再現性の高い”ログインして居座る”型の侵入を得意とする組織**と位置づけられる。

---

3. 目的(1)：攻撃者の力量推定

3.1 リークサイト掲載情報から読み取れる内容（Rhysidaの主張・未検証）

Rhysidaの掲載ページには、以下のカテゴリ別ファイル集計が示されている（既存の合計約144万ファイルに対する内訳）。

カテゴリ	件数（Rhysida主張）
地図・地理情報（Maps/Geo）	124,823
法務・苦情処理関連	77,939
財務関連	55,553
契約書	46,522
人事（HR）	27,299
政府監督関連	13,142
機密文書	11,777
インフラ関連	8,110
パスワード関連	5,941
医療・健康情報	2,738
連絡先情報	2,287

さらに、個人情報として電子メールアドレス16,389件、電話番号11,963件、対象個人12,076名、IBAN（国際銀行口座番号）148件が含まれると主張。加えて、GebäudeAtlas（施設管理系システムとみられる）や決済代行PAYONEの支払データベース、個人用「パスワード保管庫」、Z_ADMIN権限を持つデータベースアカウントなど、**平文の認証情報**が窃取されたとしている。懲戒案件（VG Berlin行政裁判所係属中の訴訟を含む）、州刑事警察局・州の治安機関（Staatsschutz）が関与する事案、連邦参議院（Bundesrat）委員会の秘密指定解除に関する通信記録、機密保護（Geheimschutz）区分文書、上下水道などKRITIS（重要インフラ）関連の脆弱性分析文書といった、**機微度の極めて高いカテゴリ**の存在も明記されている。

3.1.1 リークサイト上のドキュメント一覧（フォルダ構造）から得られた追加情報

リークサイトには「Document (part 1)」～「Document (part 3)」として、窃取データのフォルダツリーを閲覧できるブラウザが用意されている。今回、そのうちpart 2のみ読み込みに成功し（part 1・3はタイムアウト）、ルートフォルダ「data」直下の第一階層フォルダ名一覧を確認できた（フォルダ名のみの閲覧にとどめ、内部ファイルの展開・ダウンロードは行っていない）。

確認できたフォルダ名は以下の通り：`$RECYCLE.BIN`、`6B_AO_Personelles`、`BE-Personal`、`Berichte`、`Bso`、`Controlling`、`Gruppen`、`Karten`、`Microsoft SQL Server`、`PST-Backup`、`RBS`、`Saveris`、`Users-Archiv`、`YADE_INFO`、`haushaltsdb_senstadtdb28`、`temp`、`ALL_FILES`

この一覧単体はRhysida側が用意した閲覧用インターフェース上の表示であり、ファイル内容そのものではないが、以下の点で先の分析を補強・具体化する状況証拠となる。

- **`haushaltsdb_senstadtdb28`**：「haushaltsdb」は予算データベース（Haushaltsdatenbank）、「senstadtdb」は都市開発・住宅担当上院部局（Senatsverwaltung für Stadtentwicklung）のデータベースを指すとみられる略称であり、末尾の「28」はサーバ／インスタンス番号と推測される。これは、公式報道で最初に異常を検知し8月14日にネットワークから切り離された2部局の一つ（都市開発・住宅担当部局）と一致する。リークサイト側の主張と、州政府が公式に認めた被害部局の情報が、フォルダ名という形で部分的に符合している点は注目に値する。
- **`Microsoft SQL Server`**：一般的な文書ファイルの集積ではなく、SQL Serverのデータディレクトリ（データベースファイル本体またはバックアップ）そのものが持ち出された可能性を示唆する。これが事実であれば、ファイル共有への到達にとどまらず、**データベースサーバ上のローカル管理者権限またはサービスアカウント権限にまで到達していたこと**を意味し、3.2節(c)で述べた横展開の深さをさらに裏付ける。
- **`PST-Backup`**：Outlookメールボックスのバックアップアーカイブであり、Rhysida側の要約に記載されていた「PSTアーカイブ」と符合する。
- **`Saveris`**：Testo社のワイヤレス環境監視（温度・湿度等）システム「Saveris」に由来すると思われるフォルダ名。仮に該当システムのデータであれば、建物管理・冷蔵冷凍設備・実験室環境などのIoT/OT系監視データが、一般文書と同じ共有ドライブ上に存在していたことになり、4.3節で述べたKRITIS・OT系データの分離の必要性を裏付ける材料となる。
- **`6B_AO_Personelles`**／**`BE-Personal`**／**`Bso`**／**`Controlling`**／**`Gruppen`**／**`Karten`**：人事、財務・管理、地理情報など、複数部局・複数業務領域のフォルダが**単一のルート「data」以下に並列に配置**されている構造がうかがえる。これは特定システムの部分的侵害ではなく、**部局横断の共有ファイルサーバ（ネットワークドライブ）単位での侵害**であったことを強く示唆する。

留意点：以上はいずれもフォルダ名という表層情報にとどまり、ファイル内容・件数・実際の格納データを検証したものではない。また、リークサイト運営側（Rhysida）が閲覧者に見せる目的で用意した表示であるため、実際のデータ構造を正確に反映しているとは限らない点にも留意する必要がある。

3.2 力量評価

以上の主張内容と、ベルリン州が独自に確認・公表している事実（侵入開始が8月7日頃、検知が8月14日、隔離対象が2部局にとどまり全庁ネットワークの即時遮断には至らなかった等）を照らし合わせると、以下の評価が導かれる。

(a) 侵入自体の技術的高度さは限定的である可能性が高い CISA勧告が示す通り、Rhysidaはゼロデイやアフ BOFなど高度な独自兵器よりも、VPN等の外部公開サービスへの正規（窃取済み）認証情報での「ログイン」を主要な初期侵入経路とする。ベルリン州の事案でも、報道は「侵入」というより「認証情報の悪用による侵入」を示唆する記述が中心であり、少なくとも公開情報からは高度なゼロデイ悪用を示す証拠は確認できない。

(b) 滞留期間中の探索・トリアージ能力は高く評価すべきである 実際の侵入開始（8月7日頃）から検知（8月14日）まで約1週間、リークサイト掲載（8月28日）まで約3週間の滞留があったとみられる。この間に約144万ファイルを走査し、地図・法務・財務・契約・人事・監督・機密・インフラ・パスワード・医療・連絡先という11カテゴリに整理して提示している点は注目に値する。これほど短期間で大量データを意味のある単位に自動分類する能力（キーワード・拡張子・フォルダ構造ベースの自動仕分けツールの使用が示唆される）は、**データ窃取後の”戦利品”を恐喝材料として最大化するための専門的なトリアージ・パイプラインを持つグループ**であることを示す。これはRhysidaに限らず近年の二重恐喝型RaaSアフィリエイトに共通する「ビジネス化」の表れであり、個々の実行者の技術力というより組織としての運用成熟度の高さと解釈すべきである。

(c) 権限昇格・横展開の深さを示唆する状況証拠 「パスワード保管庫」「Z_ADMIN権限のデータベースアカウント」「幹部の個人情報（IBAN、身分証、銀行カード）」まで到達している点は、単一システムの表層的な侵害にとどまらず、**管理者権限領域・複数部局にまたがる横展開**に成功したことを強く示唆する。ただし、これらはすべてRhysida自身の主張であり、州政府による独立検証を経ていない点には留意が必要である（リークサイトの記載は被害を誇張し交渉を有利に進めるための”マーケティング”的機能を併せ持つことが一般に指摘されている）。この点は、3.1.1で述べたフォルダ構造上の状況証拠（SQL Serverデータの直接窃取が疑われる点、部局横断の共有ドライブ構造、都市開発・住宅担当部局との名称上の符合）によっても補強される。

(d) オークション形式の運用は組織としての成熟を示す 支払い期限経過後、直ちに全データを無条件公開するのではなく、まずオークション形式を試みた点（「2 auctions online」の表示など）は、被害組織以外の第三者（データブローカー等）への売却も見据えた、複数の収益化経路を持つ運用体制を示している。

総合評価：Rhysidaは、単発の高度な技術的ブレークスルーよりも、**認証情報窃取を起点とした侵入の再現性、大量データの分類・恐喝素材化のオペレーション能力、複数の収益化チャネルを持つビジネスモデルの成熟度**において高い力量を持つ組織と評価できる。逆に言えば、多要素認証の徹底やVPNアクセスの監視といった基本的対策の欠如が突破口になっている可能性が高く、「防ぎようのない超高度な攻撃」ではなく「典型的な二重恐喝型RaaSの手口が、大規模な官公庁ネットワークに対しても通用してしまった」事例と位置づけるのが妥当である。

---

4. 目的(2)：防御側（システム構成等）への教訓

4.1 検知〜隔離までの時間差（Dwell Time）の短縮

報道によれば、データ流出の開始（8月7日頃）から検知（8月14日）までに約1週間、検知から2部局の切り離しにとどまった点も含め、**全庁的な封じ込めには時間を要した**ことが示されている。特定の2部局のみを切り離す判断は業務継続を優先した結果とみられるが、住宅手当支給などの行政サービスに遅延が生じており、「部分隔離とサービス継続」のトレードオフを平時から設計しておく必要性を示す事例である。

- 教訓：異常な大量データ転送（Exfiltration）を検知するDLP／ネットワーク監視の強化と、検知から隔離までの初動対応時間（MTTC: Mean Time to Contain）短縮を組織目標として明示すること。
- 教訓：緊急時に「どの部局・システムを、どの業務影響を許容して切り離すか」の判断基準を事前にプレイブック化しておくこと。

4.2 認証情報の管理——平文保管・特権共有アカウントの排除

Rhysidaの主張が事実であれば、決済システム（PAYONE）や施設管理システム（GebäudeAtlas）の認証情報、個人の「パスワード保管庫」、共有的な管理者アカウント（Z_ADMIN）が平文または容易にアクセス可能な形で存在していたことになる。これはCISA勧告が指摘する「窃取済み正規認証情報によるログイ

ン」という初期侵入手口と、被害拡大後の横展開の両方を成立させる典型的な脆弱要因である。

- 教訓：パスワードマネージャー・シークレット管理基盤（Vault等）への一元化と、平文でのパスワード保存の根絶。
- 教訓：外部公開VPN・リモートアクセスへの多要素認証（MFA）の例外なき徹底。CISA勧告はMFA未導入VPNが突破口となった事例を繰り返し指摘している。
- 教訓：共有管理者アカウント（Z_ADMIN的な汎用特権アカウント）の廃止と、個人に紐づいた特権アクセス管理（PAM）・最小権限原則の適用。

4.3 ネットワークセグメンテーションとKRITIS（重要インフラ）データの分離

上下水道の脆弱性分析文書のような重要インフラ（KRITIS）関連データが、一般の行政文書と同一のネットワーク・アクセス権限下に置かれていたと疑われる点は深刻である。重要インフラの脆弱性情報は、それ自体が二次攻撃（実際の水道システムへの攻撃）の踏み台となり得る「機密性の中でも別格」の情報である。

- 教訓：KRITIS関連文書・機密指定（Geheimschutz／VS区分）文書は、一般行政ネットワークから論理的・可能であれば物理的に分離し、アクセスログを個別に監査すること。
- 教訓：マイクロセグメンテーションにより、一つの部局の侵害が全庁的な東西（Lateral）方向の移動につながらない設計とすること。

4.4 「攻撃者の分類ラベル」を模倣した自組織のデータガバナンス

皮肉なことに、Rhysidaは窃取データを「地図・法務・財務・契約・人事・監督・機密・インフラ・パスワード・医療・連絡先」という実務的な11分類で整理し提示した。これは裏を返せば、**攻撃者の方が防御側よりもデータの所在・機微度を正確に把握していた可能性がある**ことを意味する。

- 教訓：組織側でデータ分類（Data Classification）とデータマッピング（どこに何が、誰がアクセスできる状態で存在するか）を平時から整備し、機微データ（医療情報、金融情報、身分証明書類、重要インフラ情報等）を優先的に保護・監視対象とすること。
- 教訓：DLPツールの分類ルールを、攻撃者が実際に狙う区分（認証情報、財務、個人情報、重要インフラ）に合わせて優先度付けすること。

4.5 バックアップ・法的対応・コミュニケーション体制

ベルリン州は身代金の支払いを拒否し、公式に恐喝の事実を早期に認めた。この透明性の高い対応（8月28日という早い段階での公式表明）は、Just Culture的観点からも評価に値し、他の自治体が参照すべき危機管理コミュニケーションの一例となる。一方で、GDPR第32条・第9条・第33条、ドイツの機密保護関連法規（VSA/StGB）、KRITIS/BSIG法制上の義務など、複数の法的枠組みに同時に抵触し得る事案であり、法務・広報・技術部門の即応連携体制が不可欠であることも示された。

- 教訓：身代金非払い方針を平時から明文化し、経営層（首長・幹部）が迅速に意思決定できる体制を整えること。
- 教訓：個人データ・重要インフラ・国家機密が同一インシデントに混在するケースを想定し、GDPR等のデータ保護法制とKRITIS等の重要インフラ法制の双方に同時対応できる法務体制を平時から準備すること。
- 教訓：オフライン・イミュータブル（改ざん不可能）なバックアップの整備により、身代金非払いを選択しても行政サービスを早期復旧できる体制を確保すること（本レポートの範囲では復旧状況の詳細は未確認）。

4.6 共有ネットワークドライブの一元化リスク

3.1.1で確認したフォルダ構造は、人事・財務・地理情報・環境監視・データベースバックアップといった性質の異なる複数部局のデータが、単一の共有ファイルサーバ（ルート「data」）の下に並列配置されていた可能性を示している。**部局ごとにアクセス権限が分離されていたとしても、同一の物理／論理ストレージ基盤・同一の管理者権限ドメインの配下にあれば、一度の権限奪取で全部局のデータに到達し得る。**

- 教訓：部局横断の共有ファイルサーバを運用する場合でも、部局単位でストレージボリューム・バックアップドメイン・管理者権限ドメインを分離し、単一の侵害が全庁的なデータ露出につながらない構成とすること。
- 教訓：データベースサーバのファイルシステムレベルのバックアップ（.bak等）を、一般のファイル共有と同じネットワークドライブ上に置かないこと。データベースバックアップは専用のバックアップ基盤・暗号化・アクセス制御下で管理すること。
- 教訓：ビル管理・環境監視（IoT/OT）系システムのデータも、一般業務用ファイルサーバとは独立した管理下に置くこと。

---

5. 未確認事項・分析の限界

- 本レポートで示したカテゴリ別ファイル数・個人情報件数などの詳細は、**すべてRhysida自身のリークサイト掲載情報に基づく未検証の主張**である。ベルリン州政府は「個人データ等が含まれる可能性は否定できない」との認定にとどめており、独立したフォレンジック調査に基づく確定数値は本稿執筆時点で公表されていない。過去の大規模リークサイト事案では、攻撃者側の主張する件数が事後の公式調査で下方修正される例が多いことにも留意が必要である。
- 初期侵入の具体的な手口（フィッシングか、VPN認証情報の窃取か、他の脆弱性の悪用か）は、本稿執筆時点の公開報道からは特定できていない。
- 流出データが実際にダークウェブ上で無条件公開された後の悪用状況（フィッシング・なりすまし等の二次被害）については、継続的なモニタリングが必要である。
- 3.1.1で言及したフォルダツリー情報は、リークサイト提供の閲覧ツール（part 2）から得られた最上位階層のみであり、part 1・part 3はタイムアウトにより未確認である。フォルダ内部の詳細な構成・ファイル一覧は今回の調査範囲に含まれていない。

出典

- CISA/FBI/MS-ISAC, “#StopRansomware: Rhysida Ransomware” (AA23-319A, 2023年11月15日発行、2025年4月30日更新)
- CybelAngel, “Rhysida Ransomware: Attack Methods, IOCs and Defence 2026”
- SecurityAffairs, “Berlin Ransomware Leak Exposes State Secrets”
- BleepingComputer, “Berlin confirms data theft after Rhysida ransomware attack claims”
- TechTimes, “Berlin’s Seven-Day Ransomware Isolation Gap Let Rhysida Steal Critical Infrastructure Data”
- 各種報道（Reuters配信を含む、Kai Wegnerベルリン市長および内務担当上院議員Iris Sprangerの共同声明に基づく報道）
- Rhysidaダークウェブ・リークサイト掲載ページ（「Berlin, Germany」エントリー、閲覧のみ・データダウンロードは実施せず）

本レポートはOSINT（オープンソース・インテリジェンス）および公開リークサイトの掲載情報のみに基づく分析であり、被害組織との接触や非公開情報の入手は行っていない。