サンプル（ダミーデータ） 商談用 実在の個人・法人とは一切関係ありません

CONFIDENTIAL

デジタル・フォレンジック

端末調査報告書

— 退職者による情報持ち出し疑義に関する事実調査 —

事件名／案件名	（ダミー）退職者による営業秘密持ち出し疑義に関する事実調査
ご依頼者	株式会社アルファ・テクノロジーズ（架空）
調査対象者	対象者A（元・営業本部所属／2026年3月31日 退職）
調査対象端末	PC-DUMMY-001（Windows 11 Pro） 1台
調査対象期間	2025年10月1日 ～ 2026年4月7日
報告書番号	CoW-FR-2026-0000（ダミー）
報告日	2026年5月◯日
作成	CoWorker株式会社 セキュリティ事業部
版数	Ver 1.0（最終報告）

本書は商談用のサンプルです。記載されている端末名、日時、数値、ファイル件数、データ量、シリアル番号、社名、人物はすべて架空のものであり、実在の個人・法人・事案とは一切関係ありません。実際の調査では、認定した事実のみを記載し、根拠のない推測は記載しません。

目次

1. エグゼクティブサマリー 3

2. 調査の概要 5

3. 証拠保全の状況（Chain of Custody） 6

4. 前提と限界 7

5. 認定した事実 8

6. 統合時系列 14

7. 除外所見（否定的結論） 15

8. 法的整理に資する事実の対応表 16

9. 推奨されるアクション 17

附属資料 18

1. エグゼクティブサマリー

1.1 調査依頼事項と結論

No	調査依頼事項	結論
Q1	対象者Aが、退職に際して会社の業務データを外部に持ち出した事実があるか。	外部記録媒体への保存操作、および会社管理外のクラウドストレージへの大量送信の記録が確認された。持ち出しに整合する事実が複数認められる。
Q2	持ち出しの経路と規模を特定できるか。	経路として、外部記録媒体（USB）、個人クラウドストレージ、私用メールの3系統を特定した。規模はクラウド送信 12.4 GB、外部媒体への保存操作 47件、私用メール送信 9件（うち添付 7件）。
Q3	証跡の隠滅（証拠破壊）が行われた事実があるか。	ブラウザ履歴の選択的削除、痕跡消去ツールの実行、イベントログの消去が、退職前日の同一時間帯に連続して行われた記録が確認された。
Q4	一連の行為が、マルウェア感染や第三者による不正アクセスによるものである可能性はあるか。	永続化・自動起動の全経路（60区分）を検査した結果、外部からの侵害を示す痕跡は確認されなかった。行為はすべて対象者Aのアカウントによる対話的操作として記録されている。
Q5	会社が営業秘密を「秘密として管理していた」ことを技術的に裏付けられるか。	対象端末において、ディスク暗号化、ファイアウォール、マルウェア対策、ドメイン集中管理、操作ログ取得が対象期間を通じて有効であったことを実測値として確認した。ただし外部記録媒体への書込み制限は設定されていなかった。

1.2 認定した事実の一覧

No	深刻度	認定した事実	主な根拠
F-01	重大	退職日の3営業日前に外部記録媒体が接続され、業務ファイルの保存操作が記録されていた	USB接続履歴（ユーザー単位のマウント記録）／デバイスドライバ導入記録
F-02	重大	会社管理外の個人クラウドストレージへの大量アップロードが記録されていた	ブラウザ閲覧履歴／ブラウザ保存Cookie／自動入力データ
F-03	高	私用メールアドレス宛に添付ファイル付きメールの送信が記録されていた	Microsoft 365 統合監査ログ（Send）／Microsoft 365 統合監査ログ（AttachmentAccess）
F-04	高	退職直前に、平常時の行動パターンから著しく逸脱したファイル閲覧が集中していた	Microsoft 365 統合監査ログ（FileAccessed／FilePreviewed／ListViewed）／資産管理ソフトのクライアント操作ログ
F-05	高	ブラウザ履歴の一括削除および証跡消去ツールの実行痕跡が確認された	ブラウザ閲覧履歴データベース／プログラム実行痕跡（Prefetch）
F-06	中	就業時間外・休日における端末使用が退職前1か月に集中していた	セキュリティイベントログ（ログオン成功）／システムイベントログ（起動／シャットダウン）
F-07	中	USBテザリングによる社内ネットワーク統制の回避の痕跡が確認された	ネットワークインターフェース情報／ネットワーク接続履歴

No	深刻度	認定した事実	主な根拠
F-08	情報	（除外所見）マルウェア感染および第三者による不正アクセスの痕跡は確認されなかった	永続化・自動起動関連の全証跡（約60区分）／セキュリティイベントログ（ログオン失敗・成功の外部起点分析）
F-09	情報	（管理状況）対象端末における技術的な情報管理措置の実施状況	セキュリティ機能の稼働状況／ドメイン参加情報

深刻度の定義：重大＝情報の外部流出が現に生じた可能性が高い／高＝流出の具体的な経路・行為が認められる／中＝他の所見を補強する事情／低＝軽微／情報＝事実の確認（除外所見・管理状況の記録を含む）

1.3 総合評価

対象端末および関連するクラウド監査ログ・資産管理ログの解析により、退職日の直前約2週間に、（1）会社管理外への業務データの複製・送信、（2）通常の業務範囲を超えた情報の網羅的閲覧、（3）これらの痕跡の消去、という3段階の行為が時系列上連続して発生していたことが確認された。外部からの侵害を示す痕跡は認められず、これらの行為は対象者Aのアカウントによる対話的な操作として記録されている。

もっとも、本調査は端末およびログに残存する客観的な記録に基づく事実の確認であり、行為者の意図・動機についての判断は行っていない。また、複製・送信されたデータの具体的な内容および機密区分の評価も本調査の範囲外である。これらの点については、第4章に記載した前提と限界、および各所見の「反証可能性の検討」欄をご参照いただきたい。

2. 調査の概要

2.1 調査の目的と依頼事項

本調査は、ご依頼者である○○からのご依頼に基づき、対象者Aの退職に際して会社の業務データが外部に持ち出された事実の有無、および関連する行為の有無を、対象端末およびログに残存する客観的な記録から確認することを目的とする。

弊社は技術的な事実の確認を担い、認定した事実に対する法的評価（営業秘密該当性、秘密保持義務違反の成否、損害額の算定等）は行わない。

2.2 調査対象

区分	内容
対象端末	PC-DUMMY-001（Windows 11 Pro、ドメイン参加済み、資産管理ソフト導入済み） 1台
対象アカウント	対象者Aの社内アカウント（Active Directory アカウントおよび Microsoft 365 アカウント）
対象期間	2025年10月1日 00:00 ～ 2026年4月7日 23:59（JST） ※比較のための平常期を含む
対象データソース	① 端末ライブ収集（125区分のフォレンジック証跡）／② Microsoft 365 統合監査ログ／③ 資産管理ソフトの操作ログ
調査対象外	私物端末、私物スマートフォン、対象者Aの個人アカウント内部のデータ、通信内容（本文・パケット）の実体

2.3 調査手法

本調査は、次の手順により実施した。

- （1）証跡の収集：弊社専用の収集ツールを対象端末上で実行し、125区分のフォレンジック証跡を取得した。取得結果は国際標準の構造化形式（STIX 2.1）で保存し、各証跡についてハッシュ値を算出した。
- （2）クラウド・資産管理ログの取得：ご依頼者のテナント管理者により Microsoft 365 統合監査ログをエクスポートいただき、また資産管理ソフトの操作ログをCSV形式でご提供いただいた。
- （3）一次解析：弊社開発のAI「Blue Agent」により、全証跡を網羅的に解析し、時系列を統合したうえで、平常期からの逸脱パターンを抽出した。
- （4）専門家による精査：セキュリティエンジニアが一次解析の結果を検証し、誤検知を排除したうえで、業務文脈を踏まえた評価と反証可能性の検討を行った。
- （5）報告：認定した事実、根拠、評価、限界を本報告書に記載した。

2.4 使用したツールと版数

ツール	版数	用途
CoWorker 端末証跡収集ツール	v0.0.0（ダミー）	対象端末からのフォレンジック証跡の収集およびハッシュ値算出
Blue Agent（自社開発AI解析基盤）	v0.0.0（ダミー）	証跡の網羅的解析、時系列統合、逸脱パターンの抽出
（第三者検証用）	—	解析結果は標準形式で保存されており、一般的なフォレンジックツールでの追試が可能

実際の報告書では、使用ツールの正式名称・版数・ビルド番号を正確に記載します。相手方専門家によるレビューや追試の申立てに備え、収集手順は再現可能な形で文書化しています。

3. 証拠保全の状況（Chain of Custody）

本調査で使用した証拠の取得・保管の経緯は次のとおりである。証拠の同一性および非改変性は、取得時に算出したハッシュ値により確認できる。

日時（JST）	対象	実施者	実施内容	記録
2026-04-05 10:00	対象端末	ご依頼者IT部門	対象端末を施錠保管庫にて確保。以後、通電・操作を停止。	端末確保記録
2026-04-07 12:28	対象端末	弊社エンジニア	収集ツールを実行し証跡を取得。取得直後に各証跡のハッシュ値を算出。	収集ツール実行ログ／ハッシュ値一覧（附属資料C）
2026-04-07 14:10	証跡データ	弊社エンジニア	取得データを暗号化のうえ弊社の解析環境へ移送。移送前後でハッシュ値の一致を確認。	移送記録／ハッシュ照合結果
2026-04-08 09:00	M365監査ログ	ご依頼者テナント管理者	対象アカウント・対象期間の監査ログをエクスポート。	エクスポート実行記録／ハッシュ値
2026-04-08 09:30	資産管理ログ	ご依頼者IT部門	対象者・対象期間の操作ログをCSVでエクスポート。	エクスポート実行記録／ハッシュ値
2026-04-08 〜 05-◯	証跡データ	弊社エンジニア	解析作業。原本は読み取り専用で保持し、作業用複製に対してのみ解析を実施。	作業記録

原本データは本報告日から◯年間、弊社の管理環境において保管する。ご依頼者または代理人のご請求により、原本の引渡しまたは第三者検証への提供に応じる。

4. 前提と限界

本報告書の記載を評価いただくにあたり、次の前提および限界にご留意いただきたい。

4.1 本調査の範囲

- 本調査は、対象端末およびログに残存する客観的な記録から確認できる事実のみを対象とする。行為者の意図・動機・認識についての判断は行っていない。
- 本調査は稼働端末からの証跡収集（トリアージ収集）であり、ディスク全域の物理イメージ取得およびデータカービングは実施していない。削除ファイルの実体復元は、ごみ箱に残存するものを除き実施していない。
- メール本文・添付ファイルの実体、チャットの本文、通信パケットの内容は本調査の対象外である。監査ログから確認できるのは操作の事実とメタ情報に限られる。
- 私物端末、私物スマートフォン、および対象者Aの個人アカウント内部のデータは調査対象に含めていない。

4.2 記録の制約

- OSが保持する痕跡には記録件数の上限があり、時間経過および端末の継続使用により古い記録は上書きされる。本報告書に記載した件数は、いずれも「確認できた件数」であり、実際の行為件数の下限値として解釈されるべきである。
- アプリ別のネットワーク送受信量の記録は、概ね直近30〜60日分に限られる。
- Microsoft 365 統合監査ログは、監査設定が有効であった期間かつ保持期間内のものに限られる。
- 複数のデータソースの時刻は、対象端末のタイムゾーン設定および時刻同期状況を確認のうえUTC基準に正規化し、本報告書ではJSTに換算して表記している。

4.3 「痕跡が確認されなかったこと」の解釈

本報告書において「痕跡が確認されなかった」と記載した事項は、上記の制約の範囲内で検出できなかったことを意味し、当該行為が存在しなかったことを積極的に証明するものではない。第8章の除外所見（F-08）についても、検出可能な範囲を明示したうえでの評価である。

5. 認定した事実

各所見について、認定した事実、根拠となる証跡、技術的根拠、評価、反証可能性の検討、および推奨される追加調査を記載する。所見は番号（F-◯◯）により個別に引用可能である。

F-01 ［深刻度：重大］ 退職日の3営業日前に外部記録媒体が接続され、業務ファイルの保存操作が記録されていた

認定した事実

対象端末に対し、2026年3月26日 19時42分（JST）、それまで一度も接続履歴のない外部記録媒体（USBマスストレージ、容量1TB相当）が接続された。接続から約38分間にわたり、当該媒体に割り当てられたドライブに対する「名前を付けて保存」操作が計47件記録されていた。操作対象には、営業部門の共有フォルダ配下にあった提案書・見積・顧客一覧に相当するファイル名が含まれる。

根拠となる証跡

証跡（データソース）	確認された内容
USB接続履歴（ユーザー単位のマウント記録）	媒体の個体情報：ベンダーID／製品ID／シリアル番号「DUMMY-SN-0000-0000」。接続ユーザーは対象者Aのアカウント。
デバイスドライバ導入記録	当該媒体の初回接続日時：2026-03-26 19:42:11 (JST)。以後の接続は2026-03-26のみ。
ボリューム／ドライブ文字の対応情報	当該媒体に割り当てられたドライブ文字：E:
「開く／保存」ダイアログ操作履歴	E:\ 配下への保存操作 47件。最終保存 2026-03-26 20:20:07 (JST)。
資産管理ソフトのファイル操作ログ	同時刻帯に「外部媒体への書き出し」区分のログ 47件。ファイル名・サイズを含む。

評価

接続された媒体が本件以前に一度も使用されていない個体であること、接続時間帯が就業時間外であること、保存対象が対象者Aの担当範囲を超える範囲の資料を含むことから、通常の業務上の必要に基づく行為とは考えにくい。ただし本調査の対象は端末側の記録であり、媒体側にファイルが現存するかは媒体本体を確認しない限り断定できない。

反証可能性の検討

対象者Aが業務上の正当な目的（例：社外プレゼンのための持ち出し、バックアップ）で実施した可能性は論理的には排除できない。この点は、当該媒体の返却の有無、上長の許可の有無、社内の外部媒体利用規程の運用実態に関する事実により補強または反証が可能である。

推奨される追加調査

当該媒体（シリアル番号により個体特定済み）の任意提出を求め、媒体側のファイル存在状況・削除ファイルの復元・作成日時の確認を行うことを推奨する。

F-02 ［深刻度：重大］ 会社管理外の個人クラウドストレージへの大量アップロードが記録されていた

認定した事実

2026年3月20日から3月29日までの10日間に、会社が契約していないクラウドストレージサービスに対し、対象者Aの個人アカウントでのログインが計14回記録されていた。同期間における当該サービスのクライアントアプリケーションの外部送信量は合計 12.4 GB であり、直前3か月の同アプリの平均送信量（月あたり 0.1 GB 未満）から著しく逸脱している。

根拠となる証跡

証跡（データソース）	確認された内容
ブラウザ閲覧履歴	当該サービスのログイン画面・ファイル管理画面へのアクセス 14件。訪問日時を含む。
ブラウザ保存Cookie／自動入力データ	個人アカウントの識別子（会社ドメイン外のメールアドレス）が入力値として記録。
アプリ別ネットワーク送受信量データベース（SRUM）	当該同期クライアントによる送信量 12.4 GB（2026-03-20〜03-29）。日別内訳を附属資料B-2に記載。
クラウド同期設定の痕跡	同期対象フォルダとして、業務データが格納されていたローカルフォルダが設定されていた。

評価

送信量の規模と、同期対象に業務データ格納フォルダが指定されていた事実の組合せから、業務データが会社管理外の領域へ複製された可能性が高いと評価する。個々のファイル名は端末側の記録からは特定できていない。

反証可能性の検討

送信量には業務外の個人データが含まれる可能性がある。ファイル単位の特定には、同期クライアントのローカルデータベースの精密解析、または当該クラウドサービス事業者に対する開示請求が必要となる。

推奨される追加調査

同期クライアントのローカルデータベースを対象とした追加解析により、同期されたファイル名の一覧を復元できる見込みがある（追加作業として実施可能）。

F-03 ［深刻度：高］ 私用メールアドレス宛に添付ファイル付きメールの送信が記録されていた

認定した事実

会社のMicrosoft 365 統合監査ログにおいて、2026年3月18日から3月30日までの間に、会社ドメイン外の私用メールアドレス（フリーメール）宛の送信が計9件記録されていた。うち7件に添付ファイルが存在し、同一期間内の添付ファイルアクセス記録と時刻が一致する。

根拠となる証跡

証跡（データソース）	確認された内容
Microsoft 365 統合監査ログ（Send）	送信 9件。宛先ドメイン、件名、送信時刻を附属資料B-3に記載。
Microsoft 365 統合監査ログ（AttachmentAccess）	添付ファイルへのアクセス 7件。ファイル名・拡張子を含む。
受信トレイルールの設定変更記録	2026-03-18 に自動転送ルールの新規作成が1件記録されている。

評価

会社ドメイン外の個人アドレスへの送信および自動転送ルールの設定は、社内の情報取扱いルールからの逸脱に当たる可能性がある。ただし監査ログには本文・添付の実体が含まれないため、送信された情報の内容・機密区分は本調査では確定していない。

反証可能性の検討

在宅勤務時の作業利便性等の業務上の理由による送信であった可能性は残る。送信内容の機密性の評価には、メールボックスからの内容確認（eDiscovery等）が必要である。

推奨される追加調査

対象メールおよび添付ファイルの実体について、Microsoft 365 の電子情報開示機能を用いた保全・確認を推奨する（貴社にて実施可能。手順は弊社よりご案内可能）。

F-04 ［深刻度：高］ 退職直前に、平常時の行動パターンから著しく逸脱したファイル閲覧が集中していた

認定した事実

会社のSharePoint／OneDrive上のファイル閲覧・プレビュー記録を月別に集計したところ、2026年3月の閲覧件数は 1,842 件であり、直前6か月の月平均 214 件の約 8.6 倍であった。3月の閲覧対象には、対象者Aの所属部門以外が管理する 23 のサイト／ライブラリが含まれ、これらは直前6か月間に一度もアクセス記録がなかった。

根拠となる証跡

証跡（データソース）	確認された内容
Microsoft 365 統合監査ログ（FileAccessed／FilePreviewed／ListViewed）	月別・サイト別の集計を附属資料B-4に記載。判定基準（比較期間・閾値）も同附属資料に明記。
資産管理ソフトのクライアント操作ログ	同期間の端末操作ログ件数も平常月の約4倍に増加。

評価

閲覧件数の急増、および従前アクセスのなかった部門外データへのアクセスの発生は、業務上の必要性の変化によって説明されない限り、退職に際した情報の網羅的収集と整合する。

反証可能性の検討

退職に伴う引継ぎ資料の作成、後任への説明準備等の正当な業務による増加の可能性がある。引継ぎ業務の指示内容・範囲に関する事実により切り分けが可能である。

推奨される追加調査

引継ぎ業務としてアクセスが必要であった範囲を貴社にて特定いただき、それを超える範囲を弊社で再抽出することで、争点を絞り込むことが可能である。

F-05 ［深刻度：高］ ブラウザ履歴の一括削除および証跡消去ツールの実行痕跡が確認された

認定した事実

2026年3月30日 22時07分（JST）、ブラウザの閲覧履歴データベースに対する一括削除に相当する操作が行われた痕跡が確認された。また同日 22時11分に、市販の痕跡消去ツールに相当する実行ファイルの実行が記録されている。当該ツールは端末上に現存しないが、実行痕跡は残存していた。

根拠となる証跡

証跡（データソース）	確認された内容
ブラウザ閲覧履歴データベース	2026-03-30 22:07 以前の履歴レコードが欠落。同一ブラウザのCookieおよびキャッシュには同期間のドメイン記録が残存しており、履歴のみが選択的に削除されたことを示す。
プログラム実行痕跡（Prefetch）	痕跡消去ツールに相当する実行ファイルの実行 1件。実行日時 2026-03-30 22:11:44 (JST)。
実行ファイル情報キャッシュ（AmCache）	同実行ファイルのパス・サイズ・ハッシュ値。端末上のファイル本体は削除済み。

証跡（データソース）	確認された内容
アンチフォレンジック検出	イベントログの消去記録 1件（2026-03-30 22:14）、ごみ箱の完全消去 1件。

評価

履歴のみが選択的に削除され、直後に消去ツールが実行され、さらにイベントログの消去が行われているという一連の時系列は、意図的な証跡の隠滅と整合する。なお、これらの操作の存在自体は、削除された内容が復元できない場合でも独立した事実として認定できる。

反証可能性の検討

プライバシー保護目的の定期的なクリーンアップ操作であった可能性は残るが、退職直前の1日に集中し、かつイベントログの消去まで及んでいる点は、日常的な運用としては説明が困難である。

推奨される追加調査

ディスクイメージを取得し、未割当領域からの履歴データベースの断片復元を試みることで、削除された閲覧履歴の一部を復元できる可能性がある（別途お見積り）。

F-06 ［深刻度：中］ 就業時間外・休日における端末使用が退職前1か月に集中していた

認定した事実

端末のログオン／ログオフおよび起動／シャットダウンの記録から利用時間帯を集計したところ、2026年3月に発生した 22時以降のログオンは 11 回、休日のログオンは 6 回であった。直前6か月の月平均はそれぞれ 0.8 回、0.3 回である。

根拠となる証跡

証跡（データソース）	確認された内容
セキュリティイベントログ（ログオン成功）	ログオン種別・時刻・アカウントの明細を附属資料B-6に記載。
システムイベントログ（起動／シャットダウン）	端末稼働時間帯の明細。
ユーザー活動記録（アプリ実行回数・最終実行）	当該時間帯に実行されていたアプリケーションの内訳。

評価

F-01・F-02・F-05 の各行為がいずれも就業時間外に発生していることと整合する。それ自体が違法・不当な行為を意味するものではないが、他の所見の評価を補強する事情となる。

反証可能性の検討

繁忙期の残業、時差のある海外取引先対応等の正当な理由が存在する可能性がある。

推奨される追加調査

勤怠記録との突合により、申請された時間外労働との整合を確認することを推奨する。

F-07 ［深刻度：中］ USBテザリングによる社内ネットワーク統制の回避の痕跡が確認された

認定した事実

2026年3月26日および3月28日に、スマートフォンのUSBテザリングに相当するネットワークインターフェースが端末に追加され、当該インターフェース経由での通信が行われた記録が確認された。当該時間帯において、社内プロキシを経由しない通信経路が成立していた。

根拠となる証跡

証跡（データソース）	確認された内容
ネットワークインターフェース情報	テザリング用インターフェースの追加日時、割り当てIPアドレス範囲。
ネットワーク接続履歴	当該インターフェースを経由した接続の記録。
アプリ別ネットワーク送受信量データベース（SRUM）	当該インターフェース経由の送信量 3.1 GB。

評価

社内のネットワーク監視・通信制御を回避しうる経路が実際に使用されていたことを示す。F-02 のクラウドアップロードの一部がこの経路を経由した可能性がある。

反証可能性の検討

社内ネットワークの障害時の代替手段として使用した可能性がある。

推奨される追加調査

社内プロキシ／ファイアウォールのログとの突合により、監視外通信の範囲を確定することを推奨する。

F-08 ［深刻度：情報］（除外所見）マルウェア感染および第三者による不正アクセスの痕跡は確認されなかった

認定した事実

自動起動・永続化に関する 60 区分の設定領域（レジストリ実行キー、サービス、タスクスケジューラ、ログオン処理関連モジュール、認証処理モジュール、COMコンポーネント、実行ファイル差し替え設定、署名検証機構等）を網羅的に検査した結果、正規のソフトウェアに帰属しない登録は確認されなかった。また、遠隔操作ツールの導入痕跡、外部からのログオン成功記録、認証情報窃取モジュールの登録も確認されなかった。

根拠となる証跡

証跡（データソース）	確認された内容
永続化・自動起動関連の全証跡（約60区分）	登録内容の全件一覧および正規／不審の判定結果を附属資料B-8に記載。
セキュリティイベントログ（ログオン失敗・成功の外部起点分析）	外部ネットワークからのログオン成功記録なし。
リモートデスクトップ接続履歴	対象期間に第三者からの接続記録なし。
セキュリティ機能の稼働状況	マルウェア対策ソフトおよびファイアウォールは対象期間を通じて有効。定義ファイルも更新済み。

評価

本件で確認された各行為は、外部からの侵害またはマルウェアの動作によって生じたものとは考えにくい。行為はすべて対象者Aのアカウントによる対話的な操作として記録されている。

反証可能性の検討

痕跡を完全に消去する高度な攻撃の可能性は理論上排除できないが、本件で確認された操作の態様（対話的なダイアログ操作、ブラウザへの認証情報入力等）は自動化された攻撃の挙動と整合しない。

推奨される追加調査

追加調査は不要と考える。

F-09 ［深刻度：情報］（管理状況）対象端末における技術的な情報管理措置の実施状況

認定した事実

対象端末において、対象期間を通じて次の技術的措置が有効であったことを実測値として確認した：ディスク全体の暗号化（有効）、ファイアウォール（有効）、マルウェア対策（有効・定義更新済み）、ドメイン参加による集中管理（有効）、資産管理ソフトによる操作ログ取得（有効）、管理者権限の付与状況（対象者Aは標準ユーザー）。一方、外部記録媒体への書き出しに対する技術的制限は設定されていなかった。

根拠となる証跡

証跡（データソース）	確認された内容
セキュリティ機能の稼働状況	各機能の有効／無効、設定値、最終更新日時。
ドメイン参加情報	ドメイン参加状態、適用されていたポリシー。
ユーザープロファイル情報・権限設定	対象者Aのアカウント種別および所属グループ。
システムポリシー設定	外部媒体制御に関する設定の有無。

評価

対象端末は会社の集中管理下にあり、複数の技術的な情報管理措置が実際に稼働していた。他方、外部記録媒体の利用に対する技術的制限は設けられていなかった。

反証可能性の検討

—

推奨される追加調査

外部記録媒体の書込み制限の導入を推奨する（再発防止）。

6. 統合時系列

端末証跡、Microsoft 365 統合監査ログ、資産管理ソフトの操作ログを統合し、時刻をUTC基準に正規化したうえでJSTに換算して並べた時系列である。ログが存在しない時間帯については記載していない。完全版（秒単位・全件）は別添の統合時系列表をご参照いただきたい。

日付	時刻	区分	事象	根拠	所見
2026-03-18	09:14	メール	受信トレイの自動転送ルールを新規作成	M365監査ログ	**F-03**
2026-03-18	21:30	メール	会社ドメイン外の私用アドレス宛に添付付きメールを送信（1件目）	M365監査ログ	**F-03**
2026-03-20	23:02	クラウド	会社契約外のクラウドストレージへ個人アカウントでログイン（初回）	ブラウザ履歴	**F-02**
2026-03-20	23:11	クラウド	同期クライアントによる外部送信を開始（当日 1.2 GB）	SRUM	**F-02**
2026-03-22	（終日）	アクセス	所属部門外のサイト／ライブラリへの閲覧が発生（従前アクセス記録なし）	M365監査ログ	**F-04**
2026-03-26	19:42	外部媒体	未使用の外部記録媒体を接続（E:ドライブとして認識）	USB接続履歴／ドライバ導入記録	**F-01**
2026-03-26	19:48	外部媒体	E:ドライブへの保存操作を開始	保存ダイアログ履歴／資産管理ログ	**F-01**
2026-03-26	20:20	外部媒体	E:ドライブへの保存操作を終了（計47件）	保存ダイアログ履歴／資産管理ログ	**F-01**
2026-03-26	20:35	ネットワーク	USBテザリング用インターフェースを追加し通信を実施	NIC情報／SRUM	**F-07**
2026-03-28	13:05	ネットワーク	USBテザリング経由の通信（2回目）	NIC情報／SRUM	**F-07**
2026-03-29	22:47	クラウド	同期クライアントによる外部送信が終了（累計 12.4 GB）	SRUM	**F-02**
2026-03-30	22:07	隠蔽	ブラウザ閲覧履歴を選択的に一括削除	ブラウザ履歴DB／Cookie残存	**F-05**
2026-03-30	22:11	隠蔽	痕跡消去ツールを実行（実行ファイルは削除済み）	Prefetch／AmCache	**F-05**
2026-03-30	22:14	隠蔽	イベントログの消去を実施	アンチフォレンジック検出	**F-05**
2026-03-31	17:58	基本	最終ログオフ（退職日）	セキュリティイベントログ	—
2026-04-07	12:28	保全	弊社収集ツールによる証跡取得を実施	収集ツール実行ログ	—

7. 除外所見（否定的結論）

内部者の行為以外の原因（マルウェア感染、第三者による不正アクセス）の可能性について、次のとおり検討し、いずれも痕跡が確認されなかった。詳細は F-08 に記載している。

検討した可能性	検査した範囲	結果
マルウェアの常駐・自動実行	自動起動・永続化に関する60区分（レジストリ実行キー、サービス、タスクスケジューラ、ログオン処理関連、認証処理モジュール、COMコンポーネント、実行ファイル差し替え設定、署名検証機構、シェル拡張ほか）	正規のソフトウェアに帰属しない登録は確認されなかった
遠隔操作ツールによる第三者操作	リモートデスクトップ接続履歴、ターミナルサービスのイベントログ、リモート操作ツールの実行痕跡	第三者からの接続記録および遠隔操作ツールの導入痕跡は確認されなかった
外部からの認証突破	セキュリティイベントログ（ログオン成功・失敗）、権限昇格の痕跡、認証情報窃取モジュールの登録	外部起点のログオン成功記録および認証情報窃取モジュールは確認されなかった
セキュリティ機能の無効化	マルウェア対策・ファイアウォールの稼働状況および設定変更履歴	対象期間を通じて有効であり、無効化の記録は確認されなかった

この章は、「マルウェアに感染していたので自分の行為ではない」という反論に対して、事前に技術的な検討結果を示すためのものです。実際の調査でも、否定的結論は検査範囲を明示した上で必ず記載します。

8. 法的整理に資する事実の対応表

代理人が主張を構成される際の参照用に、法的な論点ごとに、対応する事実および所見番号を索引化した。本表は事実の所在を示すものであり、法的評価を述べるものではない。

論点	対応する事実（本報告書の記載）	所見番号	章節
営業秘密の管理性を基礎づける事実（技術的措置）	ディスク暗号化、ファイアウォール、マルウェア対策、ドメイン集中管理、操作ログ取得が対象期間を通じて有効。対象者Aは標準ユーザー権限。	F-09	5章
管理措置の限界に関する事実	外部記録媒体への書込みに対する技術的制限は設定されていなかった。	F-09	5章
情報の外部への複製・送信の事実	外部記録媒体への保存操作47件、会社管理外クラウドへの送信12.4 GB、私用メール送信9件（うち添付7件）。	F-01／F-02／F-03	5章
取得された情報の範囲に関する事実	所属部門外の23サイト／ライブラリへの閲覧（従前アクセス記録なし）、月間閲覧件数が平常月の約8.6倍。	F-04	5章
計画性・継続性を基礎づける事実	2026年3月18日から3月30日にかけて、閲覧・複製・送信・痕跡消去が段階的に連続して発生。	F-01〜F-05／6章	5・6章
社内規程・統制の回避に関する事実	USBテザリングによる社内プロキシを経由しない通信経路の使用（2回、送信量3.1 GB）。	F-07	5章
証拠の隠滅（スポリエーション）に関する事実	ブラウザ履歴の選択的削除、痕跡消去ツールの実行、イベントログの消去が同一時間帯に連続。	F-05	5章
第三者原因の不存在に関する事実	永続化60区分の検査、遠隔操作・外部認証突破の検査でいずれも痕跡なし。行為は対象者Aのアカウントによる対話的操作として記録。	F-08	5・7章
行為者の同一性に関する事実	ユーザーSIDとプロファイルの対応により、各操作が対象者Aのアカウントで実行されたことを確認。	F-01〜F-07	5章
証拠の同一性・非改変性	取得時のハッシュ値、収集ツール実行ログ、保管記録により確認可能。	—	3章

この対応表は、代理人の先生が主張を組み立てる際に「どの事実がどこに書かれているか」を探す手間を省くために設けています。論点の切り口は、案件の争点に合わせて事前にご相談のうえ設計します。

9. 推奨されるアクション

9.1 追加調査（争点の確度を高めるため）

優先	内容	目的	前提・必要なもの
1	外部記録媒体（シリアル番号により個体特定済み）の任意提出および媒体側の解析	複製されたファイルの実体・件数の確定、削除ファイルの復元	対象者Aからの任意提出、または法的手続
2	クラウド同期クライアントのローカルデータベースの精密解析	会社管理外へ同期されたファイル名の一覧の復元	追加作業（既に取得済みの証跡から実施可能）
3	私用メール宛の送信メールおよび添付ファイルの実体の保全・確認	送信された情報の内容・機密区分の確定	ご依頼者による電子情報開示機能の実行
4	社内プロキシ／ファイアウォールログとの突合	監視外通信の範囲の確定、送信先の特定	ネットワーク機器ログのご提供
5	ディスクイメージの取得と未割当領域の解析	削除された閲覧履歴・ファイルの部分復元	対象ディスクのお預かり、別途お見積り
6	関係者端末の一括調査	共通する外部媒体・接続先・ファイルハッシュによる関連性の確認	対象端末の確保（初期化前）

9.2 保全に関するお願い

- 対象端末の初期化・再セットアップ・通電を行わないこと。証跡が失われる。
- Microsoft 365 監査ログおよび資産管理ソフトのログについて、対象者・対象期間を広めに設定してエクスポートを完了しておくこと。保持期間を過ぎたログは復元できない。
- 関係者の疑いがある場合、当該端末についても同時期に確保すること。

9.3 再発防止（技術的対策）

- 外部記録媒体への書込み制限の導入（今回、技術的制限が設定されていなかった）。
- 会社が許可していないクラウドストレージへのアクセス制御。
- USBテザリング等による社内ネットワーク統制の回避の禁止と技術的制限。
- 退職予定者に対するアクセス権限の段階的縮小と、退職前後のログの重点監視。
- 定期的な端末侵害診断の実施（診断の実施自体が抑止力として機能する）。

附属資料

附属資料A　収集した証跡の区分一覧

本調査では、対象端末から次の区分にわたり計125区分の証跡を収集した。各区分の詳細な内容および収集件数は別添の証跡一覧をご参照いただきたい。

区分	区分数	主な内容
ブラウザ・Web活動	9	閲覧履歴、Cookie、保存認証情報、自動入力、ブックマーク、同期設定、拡張機能
外部媒体・USB	5	USB接続履歴（個体識別情報を含む）、ドライブ文字対応、初回接続日時、自動再生設定
情報持ち出し・外部送信	6	持ち出し指標、ネットワーク送出痕跡、アプリ別送受信量、クラウド同期設定、ごみ箱
ファイル・ユーザー操作	7	保存ダイアログ履歴、最近使用したファイル、ジャンプリスト、フォルダ設定
プログラム実行痕跡	8	Prefetch、AmCache、ShimCache、アプリ利用実績、稼働プロセス、導入ソフト一覧
認証・ログオン・遠隔操作	11	セキュリティログ、RDP履歴、権限昇格、不正アクセスパターン、SID対応、ドメイン情報
ネットワーク	5	接続履歴、インターフェース情報、通信階層モジュール、名前解決プロバイダ
イベントログ原本	4	セキュリティ／システム／アプリケーション／ターミナルサービス、レジストリハイブ原本
隠蔽・証拠破壊	1	ログ消去、タイムスタンプ改変、消去ツール実行の検出
コラボレーションツール	3	Teams／Zoomの利用痕跡、Officeアドイン
端末構成・管理状態	9	セキュリティ機能の稼働状況、システム情報、タイムゾーン、ポリシー設定
永続化・自動起動（ASEP）	約60	レジストリ実行キー、サービス、タスクスケジューラ、ログオン処理関連、認証処理モジュール、COM、実行ファイル差し替え、署名検証機構、シェル拡張ほか

附属資料B　集計・明細（本サンプルでは項目のみ記載）

- B-1　外部記録媒体への保存操作 明細（47件：日時・ファイル名・拡張子・サイズ）
- B-2　クラウド同期クライアントの日別送信量（2026-03-20〜03-29）
- B-3　会社ドメイン外宛の送信メール 明細（9件：日時・宛先ドメイン・件名・添付有無）
- B-4　ファイル閲覧件数の月別・サイト別集計および判定基準（比較期間・閾値）
- B-6　就業時間外・休日のログオン明細（17件：日時・ログオン種別・アカウント）
- B-8　永続化・自動起動の全登録内容および正規／不審の判定結果

附属資料C　ハッシュ値一覧

対象	ハッシュ値（SHA-256）	算出日時（JST）
端末収集データ（アーカイブ全体）	0000…0000（ダミー）	2026-04-07 12:28
Microsoft 365 統合監査ログ（CSV）	0000…0000（ダミー）	2026-04-08 09:00
資産管理ソフト操作ログ（CSV）	0000…0000（ダミー）	2026-04-08 09:30
（個別証跡ごとのハッシュ値）	別添一覧に記載	—

附属資料D　用語集

用語	説明
フォレンジック	電子機器に残された記録を、証拠として利用できる形で保全・解析する技術および手続の総称。
トリアージ収集	稼働中の端末から、調査に必要な証跡のみを選択的に取得する手法。ディスク全体の複製より短時間で実施できる。
ディスクイメージ	ディスク全体をビット単位で複製したもの。削除ファイルの復元や未割当領域の解析に用いる。
ハッシュ値	データから算出される固定長の値。データが1ビットでも変われば値が変わるため、同一性・非改変性の確認に用いる。
Chain of Custody	証拠の取得から解析・保管に至る管理の連鎖の記録。証拠が改変されていないことを手続的に裏付ける。
Prefetch	Windowsがプログラムの起動を高速化するために作成する記録。実行されたプログラム名・実行回数・最終実行日時が残る。
AmCache／ShimCache	Windowsが実行ファイルの情報を記録する領域。既に削除されたプログラムの実行痕跡も残る場合がある。
SRUM	Windowsがアプリケーションごとのリソース使用状況を記録するデータベース。ネットワークの送受信バイト数が残る。
永続化（ASEP）	プログラムがOS起動時やログオン時に自動実行されるようにする仕組み。マルウェアの常駐手段として利用される。
アンチフォレンジック	調査を妨げるために痕跡を消去・改変する行為およびその手法。
SID	Windowsがユーザーやグループを内部的に識別するための番号。ログ上の操作を実際の人物に紐付ける際に用いる。
STIX 2.1	サイバーセキュリティ情報を記述するための国際標準の構造化形式。第三者による再解析・追試を容易にする。

附属資料E　調査体制

役割	担当・保有資格等
調査責任者	○○
解析担当	○○
連絡先	CoWorker株式会社　セキュリティ事業部

CoWorker株式会社

本報告書はご依頼者および代理人のご利用を目的として作成されたものであり、事前の同意なく第三者へ開示・複製・引用することはお控えください。