インシデント調査報告書（JPCERT/CC 準拠版・サンプル）

TLP:CLEAR | 自動解析報告（決定論的ルールエンジン版・サンプル） | ケースID: CASE-SAMPLE-202611 | 作成: 2026-11-23 09:00:00 JST | 総合判定: 緊急

目次（クリックで各章へ移動）	
本資料の取扱い・留意事項	付録A. IoC一覧（無害化済み）
1. 調査概要	付録B. 侵害・疑いのあるアカウント・端末一覧
2. エグゼクティブサマリー・調査結果概要	付録C. MITRE ATT&CK対応表
3. 調査結果（攻撃フェーズ・観点別）	付録D. 関連ファイル・持ち出し疑い・再現観点
4. 対象別調査結果詳細（端末別）	付録E. 証拠保全記録・データ消去証明
5. 対応状況・推奨対策・再発防止策	

本資料の取扱い・留意事項

- 基準タイムゾーン: 本報告書内の時刻は特記ない限り日本標準時（JST / UTC+09:00）です（内部保持および JSON/CSV は UTC+00:00 基準）。
- 攻撃関連IP・ドメイン・URLへのアクセス禁止: 誤アクセスによる感染・露見防止のため defang 形式（例: 203[.]0[.]113[.]10、hxxps://example[.]com/）で記載しています。絶対に直接アクセスしないでください。
- 取扱い範囲・免責: 本資料は提出された限定証跡に対する自動ルール照合見解であり、完全性・網羅性を保証するものではありません。共有範囲にご注意ください。
- 元の証跡内容の保全: 調査の正確性を保つため、パス・アカウント名・メールアドレス等はマスクせず原本どおり出力しています。外部共有時は必要に応じてご自身でマスキングしてください。
- 問い合わせ先: https://forensic.ba-essa.com （バエッサ / ba-essa）

1. 調査概要

1.1 調査にかかる経緯・申告事項

ファイルサーバー SRV-FILE01 にて深夜帯に不審な負荷上昇と見覚えのない圧縮ファイルが確認されたため、保守アカウント利用履歴を中心に調査を実施（架空サンプル事例）。

1.2 ヒアリング内容（提出時入力情報）

項目	内容
発覚日時	2026-11-21 08:30 JST
発覚のきっかけ	不審なログイン・操作痕跡 / システム管理者の目視確認
実施済み初動対応	該当アカウント無効化検討、証拠ログの保全
今回の調査目的	侵入経路の確認，被害範囲・横展開の確認，情報漏えい有無の確認，封じ込め・推奨対策の整理
未提出・対象外補足	外部プロキシおよびファイアウォールの通信詳細ログは未提出

1.3 調査範囲外（本サービスの対象外項目）

対象外項目	理由
物理機器の保全情報・作業写真・ライブレスポンス実行記録	利用者側でエクスポートした証跡ファイルをオンライン提出する仕組みのため、機器外観・製造番号・複製作業立会い・稼働端末へのライブコマンド記録は取得対象外です。
外部脅威インテリジェンス・ダークウェブ／リークサイト照会・攻撃アクター帰属	外部サービスへ調査対象データを送信しないZero-retention方針および誤帰属（Attribution誤認）防止のため、外部脅威DB照会や攻撃グループ特定は対象外です。
マルウェア検体本体の動的・静的詳細解析（リバースエンジニアリング）	イベントログ・ファイルシステム・OSアーティファクトの自動照合基盤であり、実行ファイル単体のサンドボックス解析や逆アセンブル解析は対象外です。
LLMを用いた複数ログ横断の物語的侵入経路推論	本報告書は決定論的ルールエンジンによる再現可能な検知結果に基づいて作成されており、個別環境文脈を踏まえた自由推論は対象外です。

1.4 調査対象・提供データ一覧

証拠ID	ファイル / パス	種別	記録期間（JST）	行数 / 状態
E-01	Security.evtx	Windows イベントログ（EVTX）	2026-11-18 00:00 〜 2026-11-21 09:00	9820行（解析完了）
E-02	Microsoft-Windows-Sysmon%4Operational.evtx	実行痕跡 / Sysmon ログ	2026-11-20 00:00 〜 2026-11-21 09:00	1840行（解析完了）
E-03	auth.log	システムログ（Syslog）	2026-11-20 00:00 〜 2026-11-21 09:00	820行（解析完了）

1.5 使用ツール・パーサー一覧

ツール / パーサー	用途
Windows イベントログパーサー / シグネチャ照合ルール	Windows イベントログ（EVTX）の構造化パースおよび既知脅威シグネチャ照合
バエッサ サイバー攻撃ログ分析 決定論的ルールエンジン	攻撃手法・不審挙動の自動照合（外部AI不使用）

2. エグゼクティブサマリー・調査結果概要

総合評価: 緊急 （有効検知 4 件 / 総検知 4 件 / 除外 0 件 ／ 内訳: 緊急 1・高 2・中 1・低 0）

注: 本報告書は提出ログに対する自動ルール照合結果です。侵害の確定には運用記録との照合が必要です。

2.1 調査目的別の確認状況・判定可否

調査目的	確認結果および判定できない理由
侵入経路の確認	外部IP 198[.]51[.]100[.]42 からのRDPログイン成功痕跡を1件確認。VPN/FWログ未提出のため接続経路詳細は別途要確認。
被害範囲・横展開の確認	提出端末1台（SRV-FILE01）上で永続化タスク登録およびLSASS参照痕跡を確認。他端末の未提出ログは調査対象外。
情報漏えい有無の確認	一時領域への7z圧縮ファイル作成を検知。外部通信ログ未提出のため実際の外部送信有無は別途確認が必要です。
推奨対策の把握	検知4件および不足証跡に基づき、第5章へ優先度順の封じ込め手順を整理しました。

2.2 主要インシデントタイムライン（抜粋 / JST）

日時（JST）	端末	事象概要	根拠
2026-11-20 23:12:08	SRV-FILE01	198[.]51[.]100[.]42 から svc_backup でRDPログイン成功	E-01
2026-11-20 23:18:45	SRV-FILE01	定期実行タスク ¥Microsoft¥SyncJob 登録	E-01
2026-11-20 23:25:19	SRV-FILE01	lsass.exe プロセスへの異常読み取り参照	E-01
2026-11-20 23:41:02	SRV-FILE01	一時フォルダ内への export_202611.7z 作成	E-02

3. 調査結果（攻撃フェーズ・観点別）

3.1 初期侵入・外部接点

確認状況: 検知あり（1件）

危険度 / ID	端末 / 時刻（JST）	確認事項	根拠ID
[高] F-002	SRV-FILE01 2026-11-20 23:12:08	外部からの遠隔ログイン成功（RDP） — 198[.]51[.]100[.]42 から svc_backup でのログイン成功。	E-01

3.2 永続化・権限維持

確認状況: 検知あり（1件）

危険度 / ID	端末 / 時刻（JST）	確認事項	根拠ID
[高] F-003	SRV-FILE01 2026-11-20 23:18:45	不審な定期実行タスクの登録 — C:¥ProgramData¥Updater¥sync.ps1 を起動するタスクを新規作成。	E-01, E-02

3.3 認証情報窃取の疑い

確認状況: 検知あり（1件）

危険度 / ID	端末 / 時刻（JST）	確認事項	根拠ID
[緊急] F-001	SRV-FILE01 2026-11-20 23:25:19	認証情報メモリ参照（LSASS）の疑い — svc_backup アカウントから lsass.exe への読み取りアクセスを検知。	E-01

3.4 収集・情報持ち出し

確認状況: 検知あり（1件）

判断できない理由: 通信先別の送信容量を確認するため、FW/プロキシログとの突合を推奨します。

危険度 / ID	端末 / 時刻（JST）	確認事項	根拠ID
[中] F-004	SRV-FILE01 2026-11-20 23:41:02	一時フォルダへの圧縮ファイル作成 — 一時フォルダ内へ export_202611.7z を作成した痕跡。	E-02

4. 対象別調査結果詳細（端末別）

端末: SRV-FILE01

状態: 緊急対応を推奨 ／ 最大危険度: 緊急 ／ 関連アカウント: svc_backup, tanaka.taro ／ 根拠ID: E-01, E-02

- [緊急] 2026-11-20 23:25:19 認証情報メモリ参照（LSASS）の疑い（根拠: E-01）
- [高] 2026-11-20 23:12:08 外部からの遠隔ログイン成功（RDP）（根拠: E-01）
- [高] 2026-11-20 23:18:45 不審な定期実行タスクの登録（根拠: E-01, E-02）
- [中] 2026-11-20 23:41:02 一時フォルダへの圧縮ファイル作成（根拠: E-02）

5. 対応状況・推奨対策・再発防止策

報告済み初動対応: 該当アカウント無効化検討、証拠ログの保全

優先度 / 対象	対応検知ID	対策内容と期待効果	実施時注意事項
緊急（即時） [封じ込め] SRV-FILE01 / svc_backup	F-001, F-002	端末のネットワーク隔離と svc_backup アカウントの即時無効化・鍵変更 効果: 攻撃者による追加操作・横展開の即時停止	揮発性情報保持のため、隔離前に電源断は行わないでください
高（24時間以内） [根絶・範囲確認] SRV-FILE01	F-003, F-004	¥Microsoft¥SyncJob 削除および FW/VPN での 198[.]51[.]100[.]42 通信確認 効果: 再侵入の足場除去と持ち出し実態の把握	タスク本体および sync.ps1 は保全後に削除してください

優先度の判断基準

優先度	目安	判断基準
緊急（即時）	発見後 1〜4 時間以内	認証情報窃取・進行中の外部侵入が疑われる事項
高（短期）	24〜72 時間以内	永続化設定や不審ファイル操作の除去・調査
中（中期）	1〜2 週間以内	ログ取得拡充や設定見直しによる再発防止

付録A. IoC一覧（無害化済み）

種別	観測値（誤アクセス防止表記）	端末	根拠ID
IPアドレス	198[.]51[.]100[.]42	SRV-FILE01	E-01
IPアドレス	203[.]0[.]113[.]77	SRV-FILE01	E-02
ファイルパス	C:¥ProgramData¥Updater¥sync.ps1	SRV-FILE01	E-01
アカウント	svc_backup	SRV-FILE01	E-01

付録B. 侵害・疑いのあるアカウント・端末一覧

端末一覧

端末名	状態 / 件数	根拠ID	推奨対応
SRV-FILE01	緊急対応を推奨（4件）	E-01, E-02	端末隔離、svc_backup無効化および同期タスク確認

アカウント一覧

アカウント	状態 / 端末	根拠ID	推奨対応
svc_backup	不正利用の疑い（優先対処）（SRV-FILE01）	E-01, E-02	アカウント無効化・パスワード再設定・権限監査
tanaka.taro	要確認（SRV-FILE01）	E-02	圧縮ファイル作成の業務実施有無を本人に確認

付録C. MITRE ATT&CK対応表

戦術（Tactic）	技術ID / 名称	端末	確認事象 / 根拠
認証情報アクセス（credential-access）	T1003.001 / LSASS Memory	SRV-FILE01	lsass.exe 参照の異常検知［F-001 / E-01］
初期アクセス（initial-access）	T1078 / Valid Accounts	SRV-FILE01	社外IPからのRDP成功［F-002 / E-01］
永続化（persistence）	T1053.005 / Scheduled Task	SRV-FILE01	不審なスケジュールタスク作成［F-003 / E-01］
収集（collection）	T1560.001 / Archive via Utility	SRV-FILE01	7z 一時圧縮ファイル生成［F-004 / E-02］

付録D. 関連ファイル・持ち出し疑い・再現観点

持ち出し・アーカイブ疑い関連ファイル

ファイルパス	端末	ルール / 根拠
C:¥Users¥tanaka.taro¥AppData¥Local¥Temp¥export_202611.7z	SRV-FILE01	win.sysmon.archive_staging (E-02)

検知ルールの再現観点（ハンティング参照）

ルールID	危険度	検知タイトル
win.security.lsass_dump_suspected	緊急	認証情報メモリ参照（LSASS）の疑い
win.security.rdp_external_logon	高	外部からの遠隔ログイン成功（RDP）
win.security.scheduled_task_created	高	不審な定期実行タスクの登録

同梱成果物: report.pdf / report.json / timeline.csv / report_jpcert.pdf / report_jpcert.md

付録E. 証拠保全記録・データ消去証明

証拠ID	ファイル名	サイズ	SHA-256	取込（JST）
E-01	Security.evtx	14.2 MB	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	2026-11-23 09:00:12
E-02	Microsoft-Windows-Sysmon%4Operational.evtx	4.8 MB	8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92	2026-11-23 09:00:14
E-03	auth.log	0.6 MB	4b227777d4dd1fc61c6f884f48641d02b4d121d3fd328cb08b5531fcacdabf8a	2026-11-23 09:00:15

- Chain of Custody 検証: 記録数 6 件 / 整合性: 正常（OK） / 先頭ハッシュ: 9f86d081884c7d659a2feaa0…
- Zero-retention 消去方針: 生証跡は解析完了後に自動消去（報告書も24時間後に完全廃棄（問い合わせ対応用の非機密管理メタデータのみ別保管））
- 消去証明書: basis=zero_retention_immediate_purge / 署名検証=OK / keyset=sha256:sample-custody-key-202611