

Behind **LockBit** Lite

Learning from Their Negotiations and Activities

はじめに

2025 年 5 月、LockBit ランサムウェア攻撃グループの管理パネルのうち、経験の浅いアフィリエイト向けの「Lite パネル」のデータベースが流出した。本レポートは、MBSD サイバーインテリジェンスグループ (Cyber Intelligence Group : CIG) が当該データベース (Lite パネルのみ) を詳細に分析し、ランサムウェア攻撃グループの活動実態や攻撃者の行動パターンを明らかにすることを目的とする。

本レポートの読み方

- ・ 急いで要点だけ：エグゼクティブサマリー
- ・ 全体像を短時間で：第 I 部 分析概要
- ・ 根拠を含めて検証：第 II 部 詳細分析 + 付録 A・付録 B (前提・制約・章別定義)
- ・ 金額抽出・採用ルールの確認：付録 C (金額抽出・採用ルール)
- ・ 背景説明で参照した外部情報の確認：付録 D (参考文献)

サイバーインテリジェンスグループ (CIG) について



CIG は、三井物産セキュアディレクション (MBSD) でマルウェア解析、ランサムウェアグループの活動実態調査、脅威インテリジェンスの収集・分析を担う専門チームです。独自調査に基づく情報発信のほか、メディアを通じた脅威動向の解説などにも取り組んでいます。

何が起きたか

ランサムウェア攻撃とは一般的に、感染端末のデータを暗号化して使用不能にしたうえで、復旧や情報の非公開と引き換えに身代金を要求するサイバー攻撃である。LockBit は、こうしたランサムウェア攻撃をサービス化して展開してきた代表的な攻撃グループの一つと言える。

2025 年 5 月、LockBit が攻撃の実行や被害組織との交渉に用いていた運用データが流出した。流出データには、被害組織と攻撃者のチャットの記録や、攻撃に使用するランサムウェアの設定情報など、通常明るみにならない攻撃グループの活動実態が多く含まれていた。

本レポートはこの流出データを一次情報として分析し、ランサムウェア攻撃の実態を明らかにするとともに、防御側がランサムウェア対策として取り組むべきポイントを示すことを目的とする。

なお、本レポートの分析対象は、今回の流出範囲である「Lite パネル」(一部の攻撃者が利用)由来のデータに限られるため、分析結果はそのまま LockBit 全体の傾向として捉えることはできない。管理パネルの構成や分析の対象範囲については第 I 部「本レポートの概要」を参照されたい。

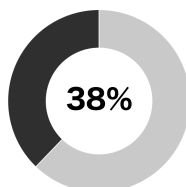
主要な発見

以下に、本レポートの主要な分析結果を整理する。具体的な分析データなどさらに踏み込んだ内容は第 II 部の詳細分析で扱う。

交渉＝支払いではない

チャット記録の分析では、約 38% の被害組織で最終メッセージまでの期間が 24 時間未満であったことが分かった。要求額の確認や攻撃者の対応姿勢の観察など情報収集にとどまるケースが多く、接触が必ずしも支払いの意思を意味するわけではない。

最終メッセージまで24時間未満

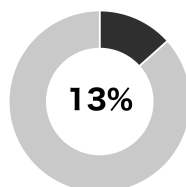


母数: 正規化ドメイン 127 件

支払い率は 1 割強にとどまる

チャットのやり取りから身代金の支払いに至ったと推定できるケースは、全体の約 13% (DB に支払い記録が残る 7 件、チャットの内容から支払いに至ったと推定される 10 件の合計) にとどまる。データの復号や、情報公開の回避を目的として交渉に応じる組織もいる一方で、大半のスレッドは支払いに至らずに終了している。

支払い率 (チャット推定)



母数: 正規化ドメイン 127 件 (内訳: DB確認7件・チャット推定10件)

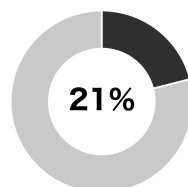
身代金の金額感と交渉の実態

初回要求額の中央値は約 50,000 USD である。攻撃者は「高額な要求＋交渉による減額」を基本戦略とし、減額率は平均で約 37%、最大で約 84%の減額に至った事例もある。

支払い＝復旧ではない

復号ツール提供 19 件 (旧 CIS 地域への無償提供 3 件を含む) 中、復旧を確認できたのは 4 件で、6 件は失敗、9 件は結果不明だった。支払い後にツールを受け取っても、復旧が保証されるわけではない。

復号ツール提供＝復旧ではない

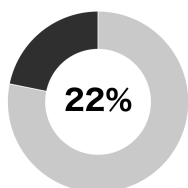


母数: 復号ツール提供 19 件 (無償提供を含む、成功 2・部分成功 2 を合算 / 内訳: 失敗 6 件・結果不明 9 件)

公開リスクは支払いとは独立の判断軸

身代金の支払いが確認できない組織のうち、実際にリークサイトに掲載されたのは約 22% であり、支払い期日を過ぎたら必ずしも即座に掲載されるわけではない。復旧の可否と情報公開リスクは、別の判断軸として扱う必要がある。

支払い未確認群でも掲載は一部



母数: 支払い未確認 110 件

攻撃者ごとに対応能力にばらつきがあり、標的地域にも偏りがある

LockBit にはさまざまな攻撃者が所属しており、攻撃者ごとに返信速度・減額幅・技術的な習熟度は大きく異なる。それぞれの活動量にも偏りが見られ、中には被害組織の約 74% がアジア地域に集中している攻撃者もいた。

侵入経路は VPN 脆弱性・脆弱なパスワード・フィッシング

チャット上で攻撃者自身が明かした主な侵入手口や経路として、脆弱なパスワードや VPN 製品の脆弱性 (Fortinet 等) の悪用、およびフィッシングが挙げられる。これらは、LockBit に限らず攻撃者が侵入の足掛かりを得るための典型的な手段である。

攻撃者の実態把握が防御にもつながる

流出データからは、攻撃者側のインフラにも防御上の不備があったことが確認できる。利用者、すなわち攻撃者のパスワードはハッシュ化等の必要な処理がなされずに平文で保存されており、過去には外部からの探索・攻撃試行と見られるリクエストの記録も見られた。攻撃者であっても、脆弱性や設定不備を放置すれば侵害を受け得る。Operation Cronos による基盤掌握について、LockBit 側は、管理サーバーの PHP を適時更新していなかったことが侵入の一因となった可能性に言及している。このことから防御側にとってもパッチ適用、設定管理、認証情報の保護といった基本対策の継続が重要であると言える。さらに、今回の流出データには、暗号資産アドレス、チャットログ、ビルド設定、アクセス試行記録などが含まれており、資金追跡、攻撃インフラの特定、攻撃手法やアフィリエイトの行動傾向を分析する手がかりとなる。

平時に何を準備すべきか

攻撃者は期限付きの割引や段階的な情報公開予告で時間的圧力をかけることが多い。侵入を未然に防ぐ対策に加え、こうした圧力の下で有事にゼロから方針を固めずに済むよう、以下を平時に整備しておく必要がある。

- **侵入経路への備え**

流出データからも確認できた一般的な初期侵入手口 (VPN 製品の脆弱性、脆弱なパスワード、フィッシング) を踏まえ、パッチ適用・多要素認証・フィッシング対策など、攻撃の入口を防ぐ対策を講じる。

- **交渉や支払いの方針整理**

攻撃者との交渉に応じるか、どのような場合に支払いを検討する余地が生じるかを、あらかじめ対応計画として整理しておく。

- **承認ルートの明文化**

有事の際に責任や決定権を持つ者を明確にすることで、インシデント対応者の負担軽減や意思決定の迅速化が期待できる。

- **優先度の高いデータの選定と復旧計画**

あらかじめ優先度の高いデータを把握し、優先順位に応じた復旧計画を立てておく。攻撃対象は Windows OS だけでなく ESXi・Linux、またバックアップにも至るため、仮想基盤やストレージまで復旧計画の対象に含める。

- **情報公開リスクへの対応計画**

顧客・取引先への通知基準、規制当局への報告義務と期限、メディア対応の想定問答を、システム復旧とは別の対外的な対応策として、あらかじめシナリオ化しておく。

はじめに	1
本レポートの読み方	1
エグゼクティブサマリー	2
何が起きたか	2
主要な発見	2
平時に何を準備すべきか	4
第Ⅰ部 分析概要	9
本レポートの概要	9
主要な分析結果の整理	9
攻撃の全体像：交渉フローと攻撃対象	11
交渉フロー	11
各段階で被害組織が直面する検討事項	11
攻撃対象環境の多様性	11
交渉や支払い検討の実態	12
交渉の期間と内容	12
支払い判断の構造：復旧と公開リスク	12
金額感の目安	12
交渉代理人の活用実態	12
復号の不確実性	13
攻撃者側の実態と、チャットから得られる防御の手がかり	13
アフィリエイト間の不均質な対応	13
攻撃者インフラにおけるセキュリティ上の不備	13
攻撃者がチャットで言及した侵入手口	14
平時の備え	14
承認ルートの明文化とリスクの整理	14
交渉窓口と指揮系統の確立	14
復号失敗・遅延を前提とした復旧計画	14
情報公開リスクへの対応計画	14
基本的な防御対策の継続	14
第Ⅱ部 詳細分析	15
第Ⅱ部の読み方	15
1. LockBit の概要	16
1.1 沿革	16
1.2 RaaS モデルの構造	16
1.3 他のランサムウェア攻撃グループとの関わり	17
1.4 Operation Cronos とその後の動向	17

2. 流出の経緯とデータセット	19
2.1 Lite パネルの背景と 2025 年 5 月の流出	19
2.2 ダンプデータの概要 (検証情報と対象期間)	20
2.3 LockBit RaaS 組織構造の用語定義	20
2.4 データベースの構成 (主要テーブルと参照関係)	21
テーブル間の参照関係	21
同一被害組織の判定ルール	23
記載方針	23
3. 組織構造：Lite パネルの運営体制	24
3.1 参加プロセスと登録状況	24
invites.status の分布	24
オンチェーン検証による invites.status の検討	25
BTC 着金 12 件の詳細分析	25
3.2 アフィリエイトの権限と役割	26
3.3 アフィリエイト活動量の分布	27
ビルド実行の曜日・時間帯傾向	28
アフィリエイト別のチャット件数と被害組織数	28
3.4 参加から活動開始までの期間	29
3.5 アフィリエイト間の差異 (権限・設定)	30
実行者タグ別に見たアカウント設定とビルド設定の傾向	31
3.6 他の攻撃グループとの関連	31
3.7 標的地域の傾向	33
4. 準備フェーズ：ビルドと設定	34
4.1 ビルド数の推移と傾向	34
4.2 対象 OS 別の設定内容	34
ビルドタイプの内訳	35
ビルドタイプ分類の根拠	35
ビルドタイプ別の設定傾向	36
4.3 除外設定とその意図	37
暗号化の除外設定	37
除外設定の内訳	37
除外設定に見られるテンプレート構造と設計意図	39
4.4 停止対象プロセス・サービス	40
5. 交渉フェーズ：チャットに記録されたやりとり	42
5.1 交渉プロセスの全体像	42
5.2 チャットへの参加率	43
5.3 チャット記録期間とメッセージ数の分布	44
5.4 時間帯・曜日・言語の傾向	45
5.5 要求額の提示・減額 (概要)	45

5.6 チャットに見られたパターン	46
テスト復号	46
支払い有無別の訪問回数分布	46
被害組織の反応パターン	47
被害組織の削除要求	51
5.7 攻撃者の交渉術	51
5.8 交渉代理人が関与したケース	56
5.9 その他特徴的な会話	59
5.10 本章のまとめ	63
6. 金銭フェーズ：要求額・合意額・支払い	64
6.1 資金インフラ	64
6.2 要求額の分布と傾向	64
6.3 売上金額と要求額の関係	65
6.4 金額交渉の経過と最終合意	71
6.5 支払い件数と獲得身代金 (推定)	72
6.6 Monero オプションの提示	74
6.7 本章のまとめ	74
7. 復号フェーズ：支払い後のプロセス	76
7.1 支払いから復号ツール提供までの時間	76
7.2 復号結果の分類	82
7.3 復号プロセス中の問題事例	83
7.4 本章のまとめ	88
8. 公開フェーズ：リークサイトへの掲載	89
8.1 掲載までのタイムライン	89
8.2 掲載された組織と掲載されなかった組織	90
8.3 Lite パネルとリークサイト上に現れる被害組織に関する傾向の差異	91
8.4 本章のまとめ	92
9. 運用上の特徴：管理パネルの運営実態	93
9.1 パスワード・パスフレーズ管理の実態	93
ログインパスワードの強度要件	93
パスフレーズ使い回しの実態	94
9.2 管理者依存の運営体制	95
9.3 パネルへの操作エラーと不正アクセス試行	96
外部からの攻撃試行の痕跡	97
リクエスト経路の分布	97
バックエンド構造の露出	98
9.4 データベース設計の特徴	99
スキーマ変更の推移	99

操作ログの分析	100
9.5 本章のまとめ	101
10. チャットに記録された侵入経路・対策に関する言及	102
10.1 初期侵入 (侵入の起点) に関する言及	102
10.2 侵入後活動 (横展開) と対策に関する言及	106
10.3 本章のまとめ	112
巻末付録	113
付録 A 分析の前提と制約	113
データの範囲	113
集計定義	113
判定基準一覧 (支払い・復号・リークサイト掲載)	113
データ終端による打ち切り (右側打ち切り) の影響	114
付録 B データセット概要 (テーブル別レコード数など)	115
【第 II 部共通】 章別分析定義サマリ (完全表)	115
主要テーブル件数一覧 (期間付き)	115
付録 C 金額抽出・採用ルール	116
金額抽出の概要	116
対応通貨と抽出パターン	116
BTC → USD 換算ルール	117
金額の表示上の丸め	117
金額の採用ルール	117
図表における階級表記	117
判定時に参照した情報	117
制約と注意事項	117
付録 D 参考文献	118

第I部 分析概要

本レポートの概要

LockBit は、ランサムウェアの開発・運用基盤を提供し、攻撃の実行を基盤利用者であるアフィリエイトが担う RaaS 型の攻撃グループである。

2025 年 5 月、LockBit の管理パネルが侵害され、約 4.5 か月分の運用データが流出した。流出データには、被害組織との交渉チャット、アフィリエイトのアカウント情報、ランサムウェアのビルド設定、暗号資産アドレスなどが含まれていた。流出したのは「Lite パネル」と呼ばれる管理画面のデータであり、主要なアフィリエイトが利用するメインパネルとは異なる。本章では、この流出データを分析した結果の概要をまとめる。

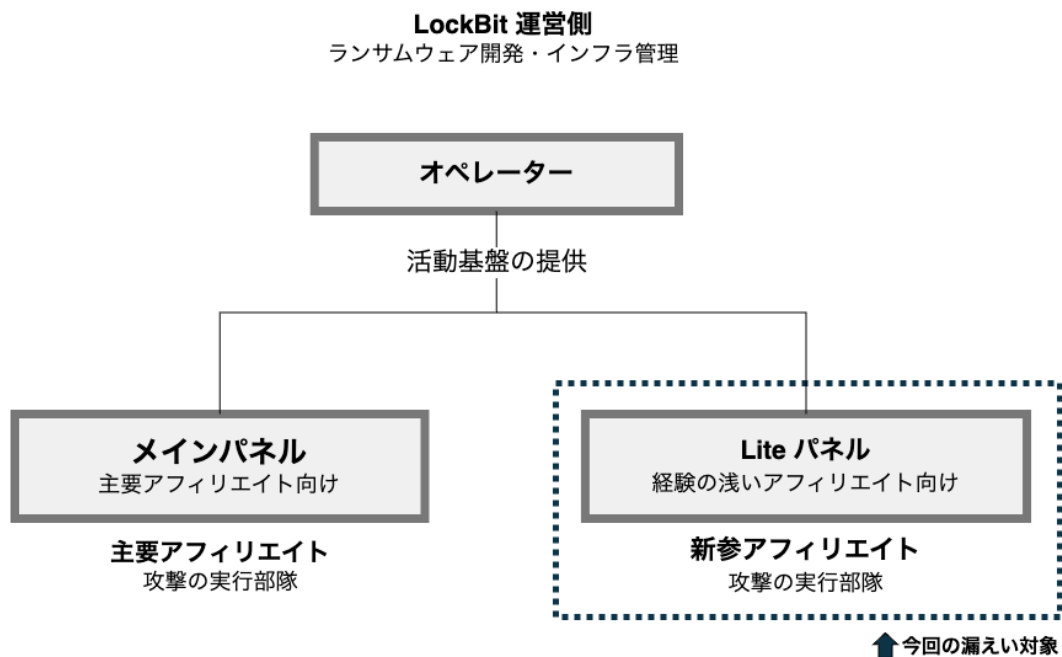


図 I-1-1: LockBit の組織構造と今回の漏えい対象

以下の数値や傾向は、特に断りがない限り Lite パネル由来データから観測できた範囲のものである。したがって、メインパネルを含む LockBit 全体でも同じ傾向が成り立つとは限らない点に留意されたい。また、本レポートで「被害組織」として示す数値は、chats 等の記録を正規化ドメイン単位で名寄せしたものであり、同一の実組織が複数ドメインを運用していた場合はそれぞれ別件として数えている。したがって、実際の法人・組織単位で見た数はこれより少ない可能性がある。(詳細は第 II 部第 2 章第 4 節)

主要な分析結果の整理

本レポートの主要な分析結果を以下に整理する。具体的な分析データなどさらに踏み込んだ内容は第 II 部で扱う。

1. 身代金の支払い率は 1 割強にとどまる

被害組織 (正規化ドメイン 127 件) のうち、支払いが確認できるのは 7 件 (DB フラグ基準)~17 件 (チャット推定基準) である。大半の被害組織は支払いに至らず交渉を終了している。(詳細は第 II 部第 6 章第 5 節)

2. 交渉は支払い意思を意味しない

正規化ドメイン 127 件のうち 48 件 (約 38%) において、最終メッセージまでの期間が 24 時間未満であった。これらの多くは、要求額や被害状況の確認など、情報収集を目的としたものと見られる。チャット

ト参加や交渉開始後、身代金支払いに至るケースは少数である。(詳細は第Ⅱ部第5章第2節)

3. チャット記録期間はケースによって広く分散

チャット記録期間(最初のチャットから最後のチャットまでの経過時間)の中央値はスレッド単位で約12時間、被害組織単位では約67時間であり、中には最長で123日に及ぶ長期のケースも確認できた。期間の長短は、被害組織側の意思決定プロセスやバックアップ状況、復号トラブルなど複合的な要因に左右される。(詳細は第Ⅱ部第5章第3節)

4. 復号ツールは必ずしも機能しない

復号ツール提供が確認された19件のうち、復旧を確認できたのは成功2件、部分成功2件の計4件だった。一方、6件は失敗、9件は結果不明である。このため、確認できた復旧成功の下限は21%だが、結果判明例に限ると40%となる。なお、19件には無償提供3件を含む。(詳細は第Ⅱ部第7章第2節)

5. アフィリエイトによって対応能力が異なる

被害組織が実際に対峙するのは個々のアフィリエイト(攻撃の実行者)である。返信速度、割引の裁量幅、技術的な習熟度はアフィリエイトによって大きく異なり、その実態がチャットデータから明らかになった。(詳細は第Ⅱ部第3章第3節)

6. 復旧と情報公開は別の意思決定軸である

バックアップによる復旧は暗号化被害への対処にとどまり、窃取された情報の公開という脅威は解消しない。そのため、システムを復旧できる場合でも情報公開の阻止を目的に支払いを検討するケースが見られた。(詳細は第Ⅱ部第6章第5節)

7. 支払いの有無だけでは掲載可否を判断できない

支払いが未確認の被害組織110件のうち、リークサイトに実際に掲載されたのは24件(約22%)にとどまる。ただし、これはLiteパネルの対象期間における観測であり、後から掲載されるリスクは拭えない。支払わなければ必ず公開されるというわけではないが、掲載の有無もその時期も攻撃者次第である。(詳細は第Ⅱ部第8章第2節)

8. 攻撃者の基盤も脆弱性を抱えている

流出データを分析したところ、LockBitの管理パネルにはSQLインジェクションを試みた可能性のあるリクエストの記録(攻撃の成功や脆弱性の存在は確認できない)や、パスワードの平文保存が見られた。高度な技術を持つ攻撃者であっても、脆弱性や設定不備を放置すれば侵害を招く。加えて、暗号資産アドレスやチャットログ、ビルド構成などの攻撃者側インフラの実態把握は、資金追跡や攻撃手法の分析につながる重要な手がかりとなる。(詳細は第Ⅱ部第9章第3節)

9. 特定アフィリエイトがアジアを標的としている

アフィリエイトの中には、被害組織が特定の地域に集中している者もいる。特に活発なアフィリエイトの一人が、アジア地域の組織を主要なターゲットにしていたことが分かった。地域的特性は攻撃者の戦略によるところが大きく、日本企業にとっても無視できないリスクである。(詳細は第Ⅱ部第3章第7節)

10. 平時の意思決定体制が有事の対応を左右する

攻撃者が、割引の適用期限と取引そのものの期限をそれぞれ設定し、時間的圧力をかけるケースが多く見られた。こうした圧力の下で有事にゼロから方針を固めるのは極めて困難であり、支払い可否の判断基準、交渉の方針、外部専門家の起用要否は、平時に決めておく必要がある。(詳細は第Ⅱ部第5章第7節)

以降では、これらの要点を「攻撃の全体像」「交渉や支払い検討の実態」「復号の不確実性」「攻撃者側の実態」「平時の備え」の順に整理する。

攻撃の全体像：交渉フローと攻撃対象

本節では、交渉がどのような段階を経て進むのか、また攻撃対象がどの程度の広がりを持つのかを概観する。

交渉フロー

Lite パネルの記録から読み取れる交渉の一般的なフローを以下に示す。ただし、これは支払いに至ったケースで観測された典型的な進行例の一つであり、交渉や支払いを推奨するものではない。

1. 初回通知

攻撃者から被害組織への定型文による最初の接触。

2. 事実確認・証拠提示

侵害の主張やテスト復号の案内が行われ、被害組織が攻撃者の主張内容を確認する段階。

3. 要求額・期限提示

身代金の具体的な金額と支払い期限が提示される。

4. 交渉

割引や条件調整が行われる段階。

5. 支払い

BTC (ビットコイン) や XMR (Monero) などによる送金。

6. 復号・復号後の対応

復号ツールの提供、復号の成否確認、トラブル対応など。(詳細は第 II 部第 5 章第 1 節)

各段階で被害組織が直面する検討事項

交渉は段階ごとに検討すべき事項が変化していく。特に期限を提示された後は、技術的対応と経営判断(法務・規制・対外説明)が同時に進行する。チャットから読み取れる、防御側の検討事項は以下の通りである。(詳細は第 II 部第 5 章第 1 節)

序盤 (通知～証拠提示)

侵害範囲の把握、窃取データに関する攻撃者の主張内容の確認、復旧見込みの初期評価が中心となる。

中盤 (要求額・期限提示～交渉)

情報公開リスクの評価、バックアップからの復旧可否、法務・規制対応の検討が同時並行で進む。

終盤 (支払い～復号)

復号ツールの受領と実行、復号の成否確認、追加対応の要否判断、および再発防止策の設計が求められる。

攻撃対象環境の多様性

Lite パネルに記録されたビルド (ランサムウェアの生成記録) は 1,183 件である。対象は Windows だけでなく、ESXi や Linux 系を含む。種別を推定できたケースでは、Windows が 504 件と最多で、次いで ESXi が 151 件、Linux 系が 143 件であった。

攻撃の対象となる環境は多岐にわたるため、仮想基盤やバックアップ・ストレージなどを含めて復旧計画の対象に含める必要がある。(詳細は第 II 部第 4 章)

交渉や支払い検討の実態

本節では、交渉の期間や金額の傾向、支払い判断にあたって被害組織が直面する論点を整理する。

交渉の期間と内容

Lite パネルの記録では、短時間でチャットが途切れるケースと長期にわたって交渉が続くケースが併存している。チャット記録期間の中央値はスレッド単位で約 12 時間、被害組織単位では約 67 時間であり、中には 123 日に及ぶ長期のケースもあった。

被害組織がチャットを開始する理由は多様であり、侵害範囲の把握、窃取されたとする情報の内容確認、復旧手段の見極めなど、情報収集にとどまるケースも多い。正規化ドメイン 127 件のうち 48 件 (約 38%) は最終メッセージまでの期間が 24 時間未満であり、この事実は接触が支払い意思を意味しないことを示している。

攻撃者は「あと 3 日」「今なら半額」といった期限付きの割引を提示し、被害組織の判断を急がせるケースが見られる。こうした時間的圧力は、社内の意思決定体制が整備されていない組織に対して特に効果的に作用する。有事にゼロから交渉や支払いの可否を検討するのは難しい。どのような目的で交渉に臨むか、どのような場合に支払いを検討するかは、あらかじめ整理しておく必要がある。(詳細は第 II 部第 5 章第 2 節、第 II 部第 5 章第 3 節)

支払い判断の構造：復旧と公開リスク

身代金の支払いに関する判断は、復旧可否、情報公開リスク、法的リスクなど複数の観点から総合的に検討する必要がある。窃取された情報が公開された場合、顧客や取引先への説明責任、規制当局への報告義務、訴訟リスクといった問題に発展し得る。

被害組織 127 件は、支払いが推定される 17 件 (うちデータベース上の支払い済みフラグで確認できるのは 7 件) と、支払いが確認できない 110 件に大別される。

ただし、支払わなければ必ず公開されるわけではない。支払い未確認 110 件のうちリークサイトに掲載されたのは 24 件 (約 22%) にとどまり、残り 86 件は 2026 年 7 月末時点で未掲載である。支払い推定 17 件も同時点では全件が未掲載であった。

一方で、スレッドが終了した時点で未掲載であっても、その後に公開されるリスクは残る。掲載された 24 件のうち 15 件は、2025 年 12 月に LockBit が「LockBit 5.0」としてリークサイトを再構築した際に追加掲載されたものであり、チャット開始から最大約 281 日が経過していた。(詳細は第 II 部第 8 章第 2 節)

支払いの実施・不実施いずれの場合も、事業継続への影響、情報公開リスク、法務・規制上の制約 (制裁対象や反社会的勢力への該当可能性を含む)、コストを複合的に評価する必要がある。判断基準は平時に策定しておくことで、有事の対応を迅速化できる。

金額感の目安

Lite パネルのチャットを分析すると、身代金要求額の中央値は約 50,000 USD であった。ただし、被害組織が交渉の中で減額を要求し、アフィリエイトが割引に応じるというケースも多く見られた。減額率は平均約 37% であり、最大で約 84% の減額に至った事例もあった。

また、支払い手段には BTC に加えて XMR も提示され、XMR 選択時に約 18% 低い価格を提示する例もあった。攻撃者が追跡の難しい手段へ誘導する意図で提示した可能性がある。(詳細は第 II 部第 6 章)

交渉代理人の活用実態

チャットの中には、交渉代理人 (ネゴシエーター) の関与が明らかなケースも見られた。攻撃者とのやりとりを専門家に委ねることで、実務者の負担軽減に加え、交渉の円滑化や条件調整の改善を期待していた可能性がある。

ただし、攻撃者側が代理人の介入を認識した場合、態度が硬化し、身代金の価格交渉が難航する可能性がある。また、過去の経験を元に攻撃者に対して高圧的な態度をとる代理人のチャットも見られており、代理人

の起用が必ずしも効果的に作用するとは限らない。起用の判断基準や代理人に共有する情報の範囲は、あらかじめ整理しておくことが望ましい。(詳細は第Ⅱ部第5章第8節)

復号の不確実性

支払いが完了しても、復号ツールの提供、動作確認、トラブル対応といった工程が続く。Lite パネルのチャット記録からは、この過程で対応遅延や復号失敗が発生する状況が読み取れる。

復号ツールの提供が確認できた 19 件のうち、部分的な成功を含めても復旧が確認できたのは 4 件にとどまる。6 件は復号に失敗し、残る 9 件は結果がチャット上で確認できなかった。なお、この 19 件には旧 CIS 地域の組織への無償提供 3 件を含む。さらに、復号ツールの提供権限はリーダーと見られる特定の人物に集中しているため、リーダーの対応が遅れれば支払い後も待たされる状況が生じる。

たとえ身代金を支払ったとしても、復号・復旧が想定どおり進むとは限らない。こうした遅延や失敗の事例を踏まえると、攻撃者側の対応に依存しない復旧計画が必要である。バックアップや代替手段による復旧ルートの確保、業務影響に基づく優先復旧対象の選定などは、事前に準備しておくことが求められる。(詳細は第Ⅱ部第7章第2節)

攻撃者側の実態と、チャットから得られる防御の手がかり

ここまでは被害組織側の対応を中心に整理した。以下では、攻撃者側の実態を 3 つの視点から述べる。アフィリエイト間の対応能力のばらつき、攻撃者インフラの脆弱性、そしてチャット上で攻撃者自身が伝えた侵入経路である。

アフィリエイト間の不均質な対応

LockBit は RaaS モデルを採用しており、被害組織が実際に対峙するのは個々のアフィリエイト (攻撃の実行者) である。返信速度、割引の裁量幅、技術的な習熟度はアフィリエイトによって大きく異なり、その実態がチャットデータから明らかになった。

また、Lite パネルでは、ビルド数の上位 10 名が全体の約 67% を占めており、アフィリエイト間の活動量の偏りも見られた。

被害組織の所在地域についても、アフィリエイトごとの偏りが確認できる。チャット数および被害組織数が最も多いアフィリエイトでは、被害組織の 74% がアジア地域に集中している。また、被害組織の全件が北米地域に集中しているアフィリエイトも存在しており、ターゲットの選定においてはアフィリエイトの裁量が認められていた可能性がある。

これらの実態を踏まえると、攻撃者側の返信速度や対応レベルに依存せず、被害組織側が独自に意思決定を行い、復旧計画を進めることができるような対応策の設計が重要と言える。(詳細は第Ⅱ部第3章第3節、第Ⅱ部第3章第7節)

攻撃者インフラにおけるセキュリティ上の不備

攻撃者側のインフラにも基本的な不備が散見された。Lite パネルに対して SQL インジェクションを試みた可能性のあるリクエストの記録 (攻撃の成功や脆弱性の存在は確認できない) や、パスワードの平文保存がその例である。この事実は、二つの側面から重要である。

第一に、攻撃者であっても脆弱性や設定不備をきっかけとして攻撃され得ることである。LockBit 側は、管理サーバーの PHP を適時更新していなかったことが、法執行機関による基盤掌握の一因となった可能性に言及している。具体的な侵入手法は、法執行機関から公表されていない。攻撃に精通しているはずの攻撃者でさえ、脆弱性管理や認証情報の保護を怠れば侵害を受ける。この事実は、防御側の組織にとっても、パッチ適用、設定管理、認証情報の保護といった基本的なセキュリティ対策を継続的に実施する重要性を示している。

第二に、暗号資産アドレスやビルド構成、アフィリエイトの行動記録、外部からのアクセス試行記録といっ

た攻撃者側インフラの実態は、法執行機関その他の権限を有する主体による資金追跡・攻撃手法の分析・インフラの監視や無力化の判断材料となり得る。(詳細は第Ⅱ部第9章第3節)

攻撃者がチャットで言及した侵入手口

チャット上では、攻撃者自らが侵入手口に言及する様子も見られた。主な内容は、脆弱なパスワード、VPN製品の脆弱性(Fortinet等)、およびフィッシングである。

また、攻撃者が被害組織に対してセキュリティ対策を助言する場面も見られた。バックアップやNASのADドメインからの分離、全サーバーへのアンチウイルス導入、パスワード強化といった内容であり、こうした助言を「レポート」として文書化し交渉材料に用いていたケースもあった。(詳細は第Ⅱ部第10章)

平時の備え

ここまで見てきた通り、ランサムウェア攻撃による被害への対応では、交渉や支払いの可否、復旧、情報公開リスクといった複数の判断が同時並行で求められる。これらを有事にゼロから検討するのは現実的には困難であるため、インシデントの発生前に整備しておくことが望ましい。

承認ルートの明文化とリスクの整理

攻撃者との交渉や身代金支払いの可否について、判断基準と承認ルートを平時に整備しておくことが望ましい。なお、制裁対象国や反社会的勢力への支払いは、それ自体が法的リスクを伴うことにも留意が必要である。

交渉窓口と指揮系統の確立

攻撃者は期限付きの割引や交渉自体の期限設定で時間的圧力をかけてくることが多く、指揮系統が整っていないければ、実務担当者の負担が増大する。限られた時間の中で適切な判断ができるように、担当者・当番体制・最終承認者を明確にし、インシデント対応訓練などにより、手順通りに対応できる体制を整えることが重要である。

復号失敗・遅延を前提とした復旧計画

復号ツールを受け取っても復旧が確認できたケースは限られている。支払いを選択する場合でも復号ツールの受け取りに時間を要する場合や、復号ツールがまともに機能しない事態が起こり得るため、バックアップ復旧等の手段を並行して整備しておきたい。

情報公開リスクへの対応計画

支払いの有無にかかわらず窃取された情報がリークサイトに掲載されるリスクは存在し、未掲載の状態が永続する保証もない。顧客・取引先への通知基準、規制当局への報告義務、メディア対応の想定問答と公表のひな形を、シナリオとして事前に用意しておくことが望ましい。

基本的な防御対策の継続

有事対応の準備と並行して、侵入そのものを減らすための基本的な防御対策を継続的に実施する必要がある。本レポートで確認した侵入経路の言及は、脆弱なパスワード、VPN製品の脆弱性、フィッシングといった基本的な対策領域に集中していた。攻撃者側のインフラでも同様の不備が確認されており、脆弱性管理や認証情報の保護の重要性は、立場を問わず共通する。パッチ適用、多要素認証、強固なパスワード管理、外部公開サービスの棚卸し、フィッシング対策、バックアップの分離と復旧訓練といった基本施策を、継続して積み上げていくことが重要である。

第Ⅱ部の読み方

第Ⅱ部では、LockBit ランサムウェアの流出パネル (Lite パネル) データを用い、RaaS の運用実態と、被害組織との交渉・支払い・復号・公開までの過程を章別に分析する。第Ⅰ部は結論と示唆を短くまとめたものであり、第Ⅱ部はその根拠となるデータ・計数・具体例を提示する。

なお、第Ⅱ部で示す分析結果は、特に断りがない限り、Lite パネル由来データから観測できた範囲に限られる。主要アフィリエイトが利用するメインパネルは含まれないため、各章で示す傾向や比率をそのまま LockBit 全体のものと解釈することはできない。

また、第Ⅱ部は章ごとに完結するよう構成しているが、分析単位 (組織単位／client_id 単位／レコード単位) や用いたデータ源が章によって異なる。章をまたいで数値を比較する際は、巻末の付録 B(表 B-1) に掲載した章別分析定義サマリを参照されたい。割合 (%) は四捨五入して整数値に統一する (例: 42%)。

各章の概要は以下の通りである。

第 1 章「LockBit の概要」

グループの歴史 (2019 年登場～2025 年の活動継続)、RaaS 組織構造の基本 (オペレーター・アフィリエイトの役割)、他のランサムウェア攻撃グループとの関わり、法執行機関による取り締まり (Operation Cronos) とその後の復活を扱う。

第 2 章「流出の経緯とデータセット」

2025 年 5 月の流出背景 (Lite パネル導入の経緯)、流出ダンプの技術仕様・検証情報、データベース構造・分析の制約条件、RaaS 組織構造の用語定義および記載方針を整理する。第 3 章以降の詳細分析の前提となる情報をまとめている。

第 3 章「組織構造：Lite パネルの運営体制」

アフィリエイトの参加プロセス・権限・活動量の分布、他グループとの関連、標的地域の傾向など、RaaS 組織の内部構造を分析する。

第 4 章「準備フェーズ：ビルドと設定」

ランサムウェアのビルド数の推移、対象 OS 別の設定内容、除外設定・停止対象プロセスなど、攻撃準備段階の実態を扱う。

第 5 章「交渉フェーズ：チャットに記録されたやりとり」

交渉プロセスの全体像、チャット参加率・チャット記録期間・時間帯傾向、被害組織の反応パターン、攻撃者の交渉術、交渉代理人が関与したケース、その他特徴的な会話を分析する。

第 6 章「金銭フェーズ：要求額・合意額・支払い」

BTC アドレスプールを中心とした資金インフラ、要求額の分布、売上金額との関係、金額交渉の経過と最終合意額、支払い件数と獲得身代金の推定値、Monero オプションの提示を扱う。

第 7 章「復号フェーズ：支払い後のプロセス」

支払いから復号ツール提供までの時間、復号結果の分類、復号プロセス中の問題事例を分析する。

第 8 章「公開フェーズ：リークサイトへの掲載」

掲載までのタイムライン、Lite パネル記録とリークサイトデータの突合分析、掲載された組織とされなかった組織の比較を行う。

第 9 章「運用上の特徴：管理パネルの運営実態」

パスワード管理の実態、管理者依存の運営体制、操作エラーと不正アクセス試行、データベース設計の特徴など、攻撃者側の運用実態を分析する。

第 10 章「チャットに記録された侵入経路・対策に関する言及」

チャットログに記録された初期侵入手口 (侵入の起点) および侵入後の横展開・対策に関する言及を整理する。

1. LockBitの概要

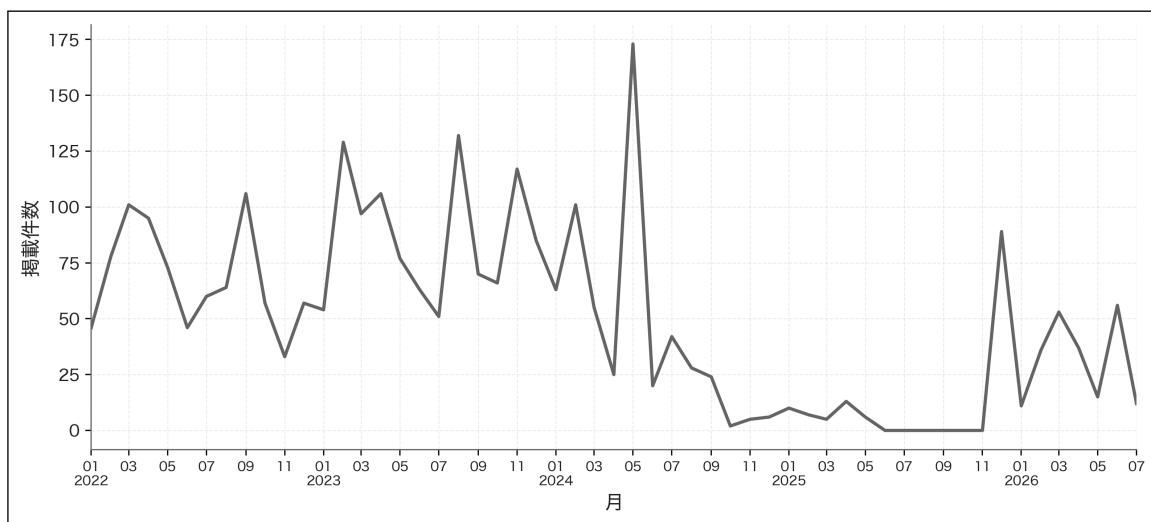
本章では、流出データの詳細な分析に入る前に、LockBitの沿革を整理する。分析対象はCIGが集計したリークサイト掲載データおよび攻撃者が外部公開している情報に限られる。

1.1 沿革

LockBitは2019年に登場し、翌年にはRansomware-as-a-Service (RaaS) モデルへ移行した。その後、2021年の2.0、2022年の3.0と段階的にリブランドを重ね、攻撃手法や運用体制を発展させてきた。2022年9月にはLockBit 3.0のビルダーが流出し、これ以降、LockBitの技術を流用した派生グループの出現が指摘されている。

2024年2月には国際的な法執行機関の連携による取り締まり「Operation Cronos」が実行された(詳細は1.4節)。その後、LockBitは2025年9月にダークウェブフォーラム上で「LockBit 5.0」を掲げて活動再開と新規アフィリエイト募集を表明し、同年12月にはリークサイトが公開され、活動は継続している(付録D)。

図II-1-1に、CIGが集計した2022年1月から2026年7月までの約4年7か月間にわたるリークサイト月別掲載数の推移を示す。2022年から2023年にかけてLockBitの掲載数は攻撃グループ別でトップレベルを維持していたが、2024年2月のOperation Cronos以降は減少に転じた。その後1年以上にわたり低水準が続いたが、2025年9月にLockBitが「LockBit 5.0」を掲げて活動再開を表明し、同年12月にリークサイトが出現している。



図II-1-1: LockBit リークサイト掲載数の推移 (2022年1月～2026年7月)

※ 図II-1-1の掲載件数は月単位の集計であり、実際の被害数と必ずしも一致しない。

1.2 RaaSモデルの構造

LockBitはRaaSモデルを採用しており、オペレーター(運営・ランサムウェア開発を担う)とアフィリエイト(攻撃実行を担う)の間に役割分担がある。本レポートで分析対象となるLiteパネルは、2024年末に導入されたアフィリエイトプログラムであり、従来のメインパネルとは運用体系が異なる。Liteパネルではboss(管理者の役割呼称)への依存度が高く、復号ツールの提供もbossの判断に委ねられていた。

1.3 他のランサムウェア攻撃グループとの関わり

2025 年は、ランサムウェア攻撃グループのリークサイト改ざんや内部データの流出が相次いだ。CIG では、Everest (2025 年 4 月)、LockBit (2025 年 5 月、図 II-1-3)、RansomedVC (2025 年 8 月、図 II-1-2) の 3 件について、リークサイトのトップページが「Don't do crime **CRIME IS BAD** xoxo from Prague」という同一の文面書き換えられていることを確認した。このほか 2025 年 2 月には、BlackBasta の内部チャットログが外部に公開された。LockBit の事案は、これに続く大規模な内部データの流出にあたる。

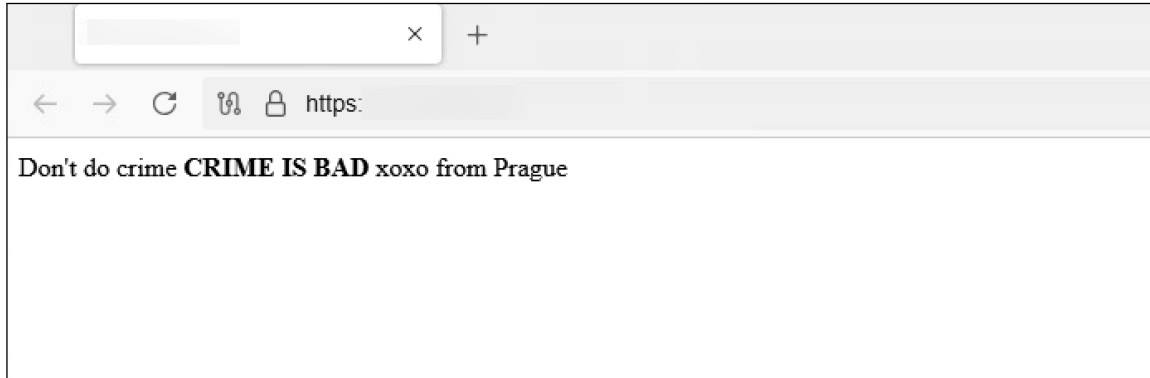


図 II-1-2: RansomedVC リークサイト改ざん時のスクリーンショット

※ CIG にて取得したスクリーンショット

LockBit のケースでは Lite パネル由来と見られる DB ダンプが公開されたため、ビルド設定、交渉チャット、BTC アドレスの割り当て状況など、グループの運営実態を多角的に分析できるデータが公開された。

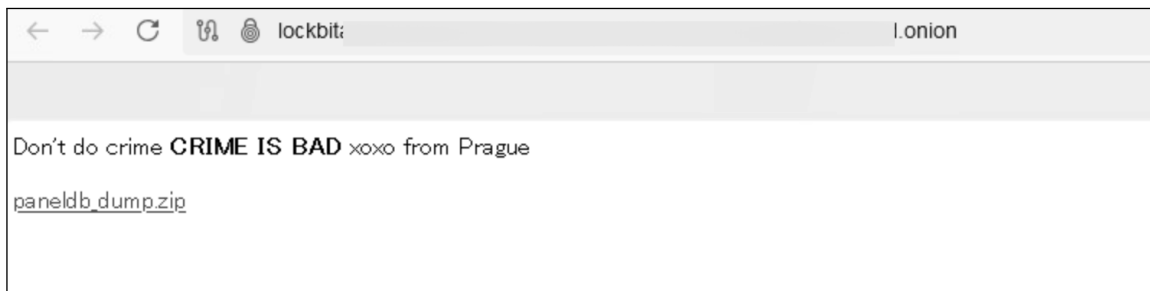


図 II-1-3: LockBit リークサイト改ざん時のスクリーンショット

※ CIG にて取得したスクリーンショット

LockBit は 2019 年に出現し、ランサムウェア攻撃グループとしては比較的長期にわたり活動を続けているグループである。この間、二重脅迫やバグ報奨金の導入、バージョンの刷新を重ねてきたほか、2020 年頃には Maze や RagnarLocker との連携が、2025 年 9 月には DragonForce の提案に LockBit が同意する形で Qilin (Agenda)・LockBit・DragonForce の 3 グループによるランサムウェア「カルテル」結成が発表された (ただし、実際にどこまで運用面での連携が機能しているかは明らかでない) など、ランサムウェア攻撃グループの動向に広く影響を与えてきた。

1.4 Operation Cronos とその後の動向

2024 年 2 月、法執行機関は LockBit のリークサイトを押収し、トップページを書き換えた。この摘発作戦「Operation Cronos」は単発で終わらず、段階的に進行した。同年 5 月には首謀者とされる人物の身元情報が公開され、10 月には開発者の逮捕が発表された経緯がある (付録 D)。LockBit 側は当初、法執行機関による情報公開の度に再掲載を含めて掲載数を急増させるなど、報復的な反応を示した。しかしこうした動きも次第に見られなくなり、2025 年後半にかけてリークサイト上で見られる活動規模は縮小傾向が続いた。そうした中で 2025 年 12 月、LockBit 5.0 のリークサイトが出現し、同月の新規掲載件数は 88 件であった。ただし、リークサイト掲載日は侵害発生から遅れることが多く、新規掲載イコールその月の新規攻撃ではない。実際、Lite パネルと突合できた掲載 24 件のうち 15 件は、2025 年 12 月のリークサイト再構築時に

新規掲載されたものであり、交渉開始から最大約 281 日が経過していた既存案件だった (詳細は第 II 部第 8 章第 2 節)。このサイトは公開直後に OSINT 上で関連インフラ情報が報告されるなど、活動基盤の脆さを示す状況も確認されている。

2. 流出の経緯とデータセット

本章では、Lite パネルの位置づけ、2025 年 5 月の改ざんとダンプ公開の経緯、ダンプデータの範囲、および分析上の制約を整理する。主な分析対象は Lite パネル由来のデータベース (DB) ダンプ (panel_db_dump.sql) であり、対象期間は概ね 2024 年 12 月 18 日から 2025 年 4 月 29 日 (UTC) である。また、CIG にて観測した情報 (リークサイト上の声明やスクリーンショット等) も併せて利用している。

2.1 Lite パネルの背景と 2025 年 5 月の流出

Operation Cronos 後、LockBit のリークサイトでは掲載件数の減少傾向が続いていた。こうした状況下で導入された Lite パネルは、従来のメインパネルが登録に 1 BTC (当時レートで約 9 万~10 万 USD 相当) を要するのに対し、777 USD で参加できる。参加時の実績提示も不要とされており、新規アフィリエイトの参入条件を大幅に緩和したプログラムである。2025 年 5 月 7 日、LockBit のリークサイトのトップページにデータベースのダンプファイルへのリンクが掲示された (図 II-1-3)。第三者による改ざんと見られるが、実行主体は特定されていない。ダンプの生成日時は UTC で 2025 年 4 月 29 日 17:26 であり (2.2 参照)、少なくともこの時点までのデータが含まれる。流出直後、LockBit はリークサイトやハッカーフォーラム上で声明を発し、流出が Lite パネルに限定される旨を主張するとともに、改ざん実行者に関する情報提供者への報酬の支払いを示唆した。

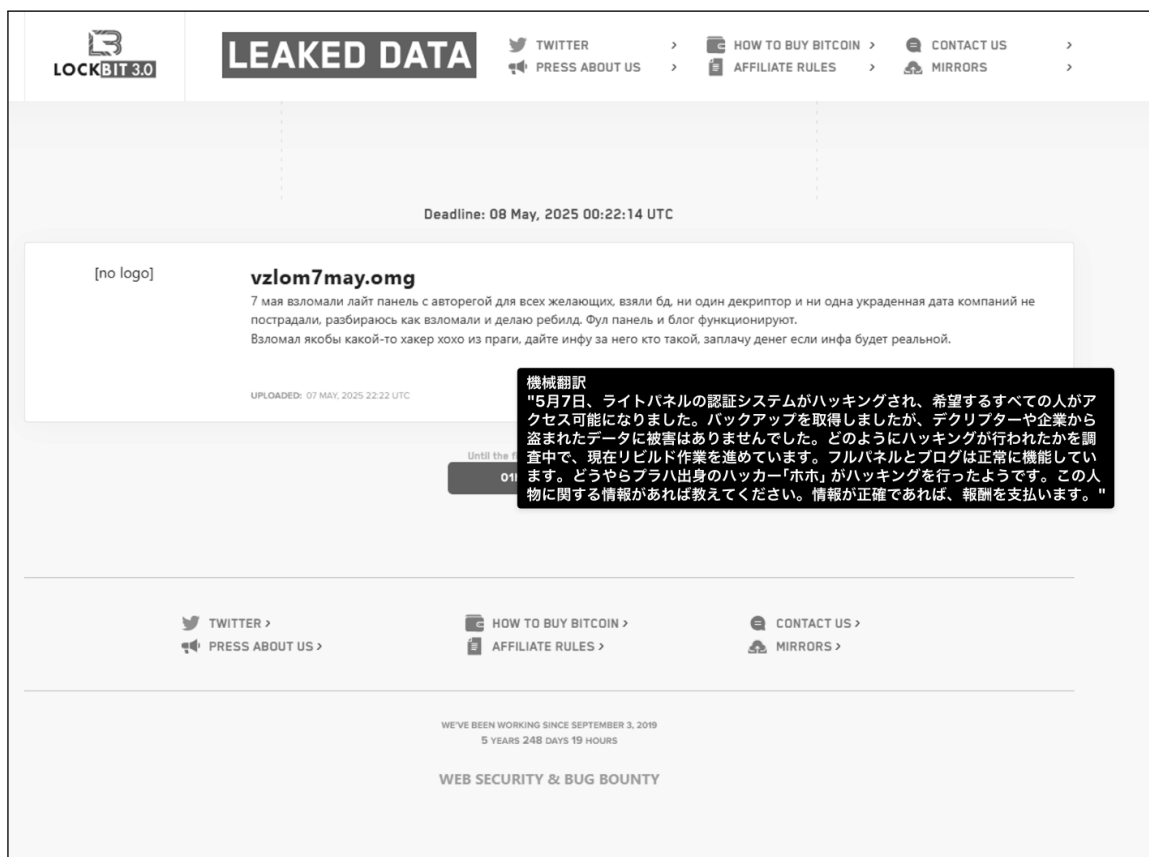


図 II-2-1: 管理パネルデータの流出に対する LockBit 側の反応

※ CIG にて取得したスクリーンショット

2.2 ダンプデータの概要 (検証情報と対象期間)

解析に使用したダンプデータの検証情報を表 II-2-1 に示す。

表 II-2-1：ダンプデータの検証情報

項目	値
ファイル名 (圧縮版)	paneldb_dump.zip
ファイル名 (展開後)	paneldb_dump.sql
圧縮時サイズ	約 7.5 MB
展開後サイズ	約 26 MB
SHA-256 (paneldb_dump.zip)	e00aa8146cf1202d8ba4fffbcf86da3c6d8148a80bb6503d89b0db2aa9cc0997
SHA-256 (paneldb_dump.sql)	4781ec443bb563c0c7b59462d5c25b4d1cfd4ad8a8a9f15aaf1381d4f677c434
生成日時 (ダンプ記載)	Apr 29, 2025 at 05:26 PM (UTC+0)
パネル技術構成	Ubuntu 22.04.1 / MySQL 8.0.41 / PHP 8.1.2

このダンプがカバーする期間は、テーブル内の記録 (作成日時・更新日時等) から概ね 2024 年 12 月 18 日から 2025 年 4 月 29 日までの約 4 か月半と推定される。データベースレコードの改変・欠損・運用上の削除等の可能性を排除できないため、全期間の全記録が完全に保存されているとは断定しない (制約は 2.4 参照)。ダンプには 20 のユーザー定義テーブルが含まれる (空テーブルを含む)。主要テーブルのレコード数を表 II-2-2 に示す。

表 II-2-2：ダンプに含まれるデータ規模 (主要テーブル)

テーブル	レコード数
users	75 件
clients	246 件
chats	4,423 件 (メッセージ単位)
builds	1,183 件
btc_addresses	59,975 件

2.3 LockBit RaaS 組織構造の用語定義

本レポートで使用する LockBit の組織構造に関する用語を以下の通り定義する。

オペレーター (Operator)

LockBit の中核開発者・管理責任者。ランサムウェア本体の開発・保守とインフラ運用を担う。

boss

Lite パネル上のチャットにおける管理者の役割呼称。オペレーター側の人物と推定されるが、本ダンプからはその位置づけを確定できない。Lite パネル上では復号ツールの提供権限と身代金要求額の決定権を持つ。

アフィリエイト (Affiliate)

RaaS 契約者・攻撃実行者。ランサムウェアビルドの取得、攻撃の展開、被害組織との交渉を担う。身代金を獲得した場合は boss へ報告し、手数料を差し引いた収益を受け取る。データベース上は users.id、clients.advid、builds.userid で識別される。本レポートでアフィリエイト名として示す値は、users テーブルの username に記録された名称であり、チャットやビルドの記録に含まれるアフィリエイト ID を users.id と突合して特定したものである。

本ダンプから確認できるのは Lite パネルのアフィリエイト層までであり、メインパネルのオペレーターやアフィリエイトの実態は含まれない。

2.4 データベースの構成 (主要テーブルと参照関係)

本ダンプの全体像は 2.2 節の通りである。各テーブルの詳細なレコード数は巻末の付録 B(表 B-2) にまとめた。以降の分析で使用する主要テーブルの分類と概要を表 II-2-3 に示す。

表 II-2-3：主要テーブルと概要

分類	テーブル	概要
アフィリエイト管理	users / invites	アフィリエイトの登録・招待情報
ビルド管理	builds / builds_configurations	ランサムウェアビルドの記録と設定
被害組織・交渉	clients / chats / visits	被害組織情報、交渉チャット、アクセスログ
アドレス管理	btc_addresses	身代金支払い用の BTC アドレスプール
復号関連	files / pkeys	復号関連ファイル・鍵情報

テーブル間の参照関係

主要テーブル間の参照関係を図 II-2-2 に示す。なお、本ダンプには外部キー制約の定義が含まれない。図中および表 II-2-4 の参照関係は、フィールドの命名規則から推定し、データレベルの結合一致率 (備考列に記載) で検証したものである。

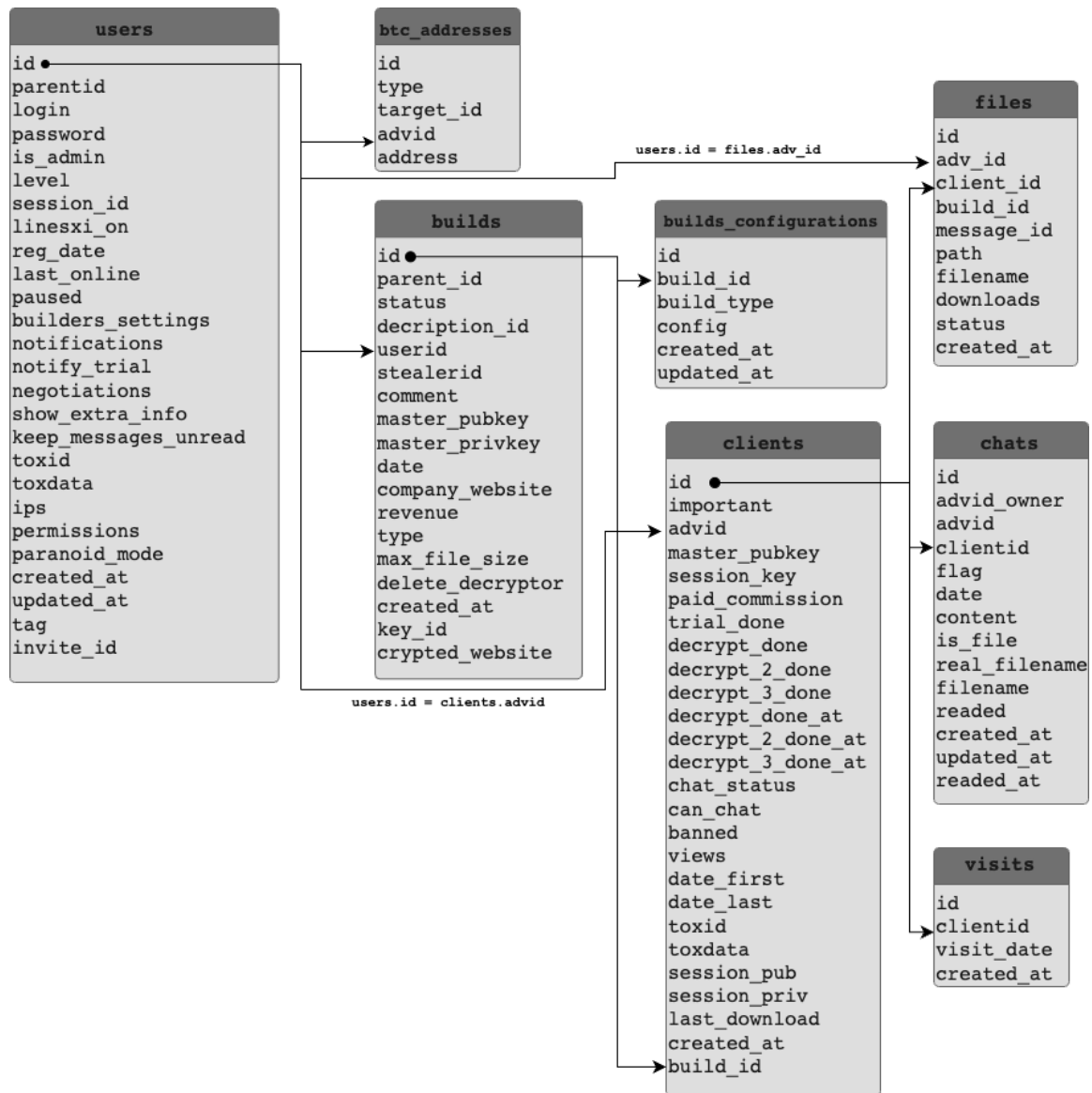


図 II-2-2: 主要テーブルの参照関係

各テーブルの紐付キーと対応関係の詳細を表 II-2-4 に示す。

表 II-2-4 : テーブル間の Join 仕様

親テーブル	子テーブル	紐付キー	対応関係	備考
users	builds	users.id = builds.userid	1 : N	1,183/1,183 が一致
users	clients	users.id = clients.advid	1 : N	246/246 が一致
invites	users	invites.id = users.invite_id	1 : N	73/73 が一致 (invite_id 非ゼロのみ)
users	files	users.id = files.adv_id	1 : N	files の実質的な参照キー
builds	builds_configurations	builds.id = builds_configurations.build_id	1 : 1	1,183/1,183 が一致

親テーブル	子テーブル	紐付キー	対応関係	備考
builds	clients	builds.id = clients.build_id	1 : N	246/246 が一致
builds	pkeys	builds.decrypt_id = pkeys.decryption_id	1 : N	1,095/1,183 が一致 (92.56%)。description_id は原DB上の表記をそのまま記載 (builds 側のみのスペル)
clients	chats	clients.id = chats.clientid	1 : N	4,423/4,423 が一致
clients	visits	clients.id = visits.clientid	1 : N	2,398/2,398 が一致
clients	btc_addresses	clients.id = btc_addresses.target_id	partial	159/59,975 のみ非ゼロ
users	btc_addresses	users.id = btc_addresses.adv_id	partial	159/59,975 のみ非ゼロ

同一被害組織の判定ルール

被害組織の集計単位は builds.company_website を clients.build_id 経由で紐付けたうえで正規化 (http/https スキーム除去、www. 除去、パス部分の除去、小文字化) して生成したユニークドメインである。同一組織が複数ドメインを持つ場合も、ドメインごとに別件としてカウントする。したがって、本レポートで「被害組織数」として示す件数は正規化ドメイン数であり、実際の法人・組織単位の数はこれより少ない可能性がある。テスト目的と判断されるドメイン (example.com、test.com、test.test 等) は件数から除外する。ドメインから組織の同定が困難な場合、国・業種は「Unknown」として扱うが、件数にはカウントする。リークサイト掲載との突合も実施している。

記載方針

被害組織ドメインは正規化後のユニークドメインの算出に使用し、本レポートでは匿名化する。アフィリエイト名 (users.username) は分析上使用するが、実名や実在人物との紐付けは行わない。チャットの引用は教訓・示唆に必要な範囲にとどめ、組織特定につながる固有情報はマスキングする。本レポートの分析上の制約および集計定義 (支払い判定基準、被害組織数の算出方法等) は付録 A にまとめた。

3. 組織構造：Lite パネルの運営体制

本章では、Lite パネルのデータベースに基づき、アフィリエイトの参加から攻撃実行に至るまでの組織運営について分析する。対象テーブルは `invites`、`users`、`builds`、`chats`、`clients` であり、時刻は UTC+0 で統一する。

まず参加プロセスと登録状況を確認し、次にアフィリエイトの権限構造と活動量の分布を整理する。その上で、他グループとの関連や標的地域の傾向を検討し、Lite パネルにおける運営体制の実態を明らかにする。

3.1 参加プロセスと登録状況

`invites` テーブルには、3,693 件に上るレコードがあり、アフィリエイトの登録申請から参加費の支払い、承認までのプロセスが記録されている。

まず図 II-3-1 に、`invites.created_at` を月単位で集計した月別の招待数の推移を示す。Lite パネルの立ち上げ後、一時的に落ちていた招待数は 2025 年 4 月に再度増加し、データ流出直前まで活発な招待活動が続いていたことが分かる。

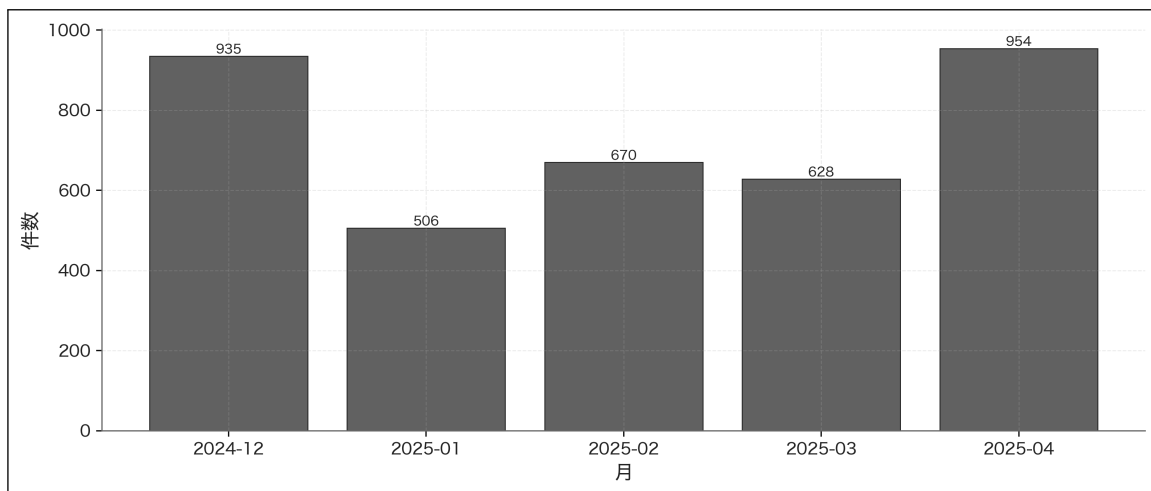


図 II-3-1: 月別招待数の推移 (2024 年 12 月～2025 年 4 月)

`invites.status` の分布

`invites` テーブルには `status` フィールドが存在し、0, 10, 50, 100 の 4 種類の値が記録されていた。フィールド名からは登録プロセスの進行状況を示すものと推測できるが、各値の正確な定義は不明である。図 II-3-2 にその分布を示す。

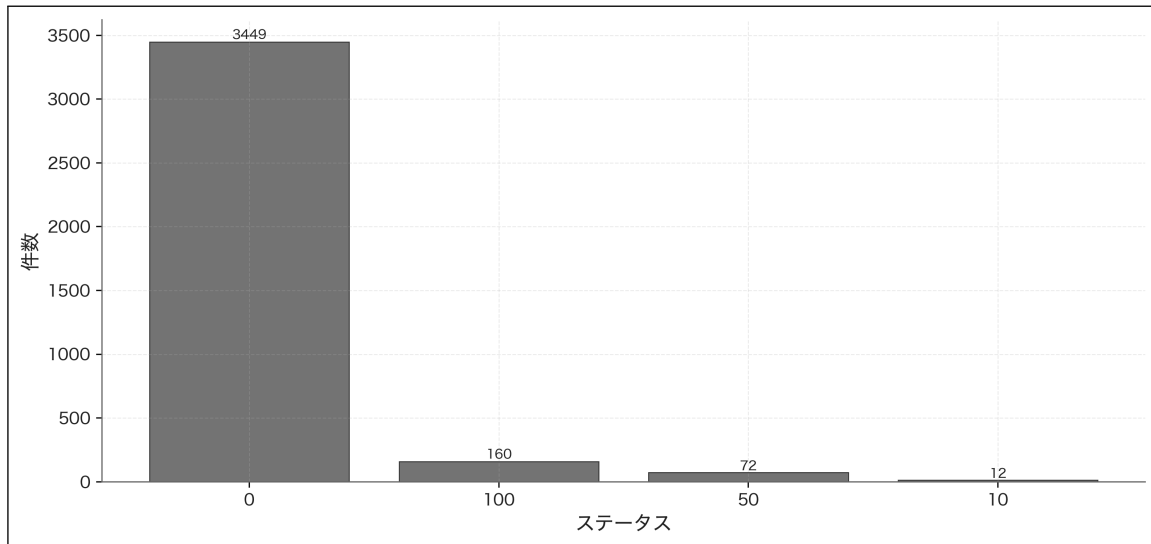


図 II-3-2: invites テーブル中の status 分布

オンチェーン検証による invites.status の検討

status の値が実際に何を意味するかを、オンチェーン着金と突合して検証した。invites の各レコードには BTC または XMR アドレスが割り当てられており、このうち BTC アドレスが記載された 2,338 件について、着金の有無を status の値と照合した。結果を表 II-3-1 に示す。

表 II-3-1: invites.status 別のオンチェーン着金状況

status	件数	BTC 着金確認	着金率
0	2,175	0	0%
10	5	2	40%
50	43	10	23%
100	115	0	0%

status の値と着金率は対応しておらず、status = 100 の 115 件にいたっては全て着金がゼロであった。値が大きいかほど支払い済みを示す、という単純な進捗フラグではないと見られる。BTC で実際に着金を確認できたのは status = 50 の 10 件と status = 10 の 2 件、合計 **12 件** にとどまる。

ただし、BTC 着金がなくても XMR (Monero) など他の経路で支払われた可能性は残るため、12 件はあくまでオンチェーンで確認できた下限である。status が支払いや登録の進捗を何らかの形で反映している可能性も否定はできず、値の解釈には慎重を要する。

BTC 着金 12 件の詳細分析

各招待レコード (invites) の amount には、参加料 777 USD をその時点の BTC/USD レートで換算した BTC 額 (以下「請求額」) が記録されている。着金を確認できた 12 件について、請求額を満たしているか、送金の速さや時期、さらに LockBit オペレーターが受け取った参加費をその後回収したかを調べた。

金額の分布

着金を確認できた 12 件はいずれも請求額を満たしており、不足送金はなかった。内訳は、請求額と完全一致が 6 件、請求額をわずかに上回るもの (+0.01%~+4.22%) が 6 件である。USD 換算 (各着金 TX 時点の BTC 価格で算出) の合計は約 \$9,374 (12 件、約 0.10 BTC)、1 件あたりの平均は \$781、中央値は \$786 である。

送金速度

招待作成から着金確認までの所要時間は平均 28 分、最短 2 分、最長 98 分であり、着金を確認できた

12 件ではいずれも短時間で送金が行われていた。

受取後の資金移動パターン

2024 年 12 月の初期 4 件 (id=8, 339, 422, 876) は 2025 年 3 月 2 日 08:33 (UTC) の同一トランザクションで一括回収されており、LockBit のオペレーターが複数アドレスをまとめて掃き出す運用をしていたことがうかがえる (着金から回収までの滞留期間は約 63~73 日)。一方、2025 年 1 月以降に着金した 8 件 (id=1041 以降) については、2026 年 7 月末時点でも出金は確認されず、残高合計は約 0.0678 BTC であった。これには運用体制の変化や法執行機関による監視への警戒など、複数の要因が考えられるが、本データからは特定できない。

時期分布

2024 年 12 月 (パネル開設直後) に 4 件、2025 年 1 月に 4 件、3 月に 2 件、4 月に 2 件であり、流出直前まで新規参加が続いていた。

3.2 アフィリエイトの権限と役割

Lite パネルのアフィリエイトは復号ツールへのアクセス権を持たず、復号ツールの作成・提供は管理者 (呼称「boss」) に一任されていることがチャット記録から確認できる。そのため、本パネルにおけるアフィリエイトの役割は攻撃の実行と被害組織との交渉に限定される。

チャット記録には、users テーブルと対応すると見られるアフィリエイト ID (adv.id) と、clients テーブルに対応すると見られる被害組織 ID (clients.id) が記録されている。本レポートでは、チャットに記録された adv.id を users テーブルと突合し、該当するアフィリエイト名を特定した。以降の記述やチャット画像に示すアフィリエイト名は、この突合結果に基づく。

また、本レポートでは、アフィリエイト ID (adv.id) と被害組織 ID (clients.id) の組み合わせを 1 つのチャットスレッドとして扱う。ただし、チャット記録からは、同一のアカウントで複数の人物が交代して発言している様子も読み取れる。例えば、被害組織が「技術サポート」や「ボス」の対応を求めた際に、攻撃者側が“boss here” (ボス、入りました) のように自らの立場を名乗ったうえで発言を引き継ぐ場面が見られた。本レポートでは、こうしたチャット上で復号ツールの提供権限を持つと見られる人物の役割呼称として「boss」を使用する (boss の定義は 2.3 節参照)。

こうした役割分担はチャット記録にも直接表れている。あるアフィリエイトは被害組織に対して自分は LockBit オペレーターとは別組織だと明言しており、過去の復号失敗についても「自分の管轄外」と責任を否定している。RaaS の仕組みを自ら説明し、オペレーターや他のアフィリエイトとの関係を線引きするような姿勢とも捉えられる。

アフィリエイトによる責任分担の主張


lofikdis

原文

1. We belong to different organizations; what you said has nothing to do with our team;
2. Lockit organization has hundreds of hacker teams;
3. Please do not communicate with me about content that is not related to this client;
4. You can contact the boss directly through tox;

日本語訳

1.
私たちは別の組織に属しており、あなたの発言は私たちのチームとは関係ありません。
2. Lockit組織には何百ものハッカーチームが存在します。
3. このクライアントに無関係な内容について私とやり取りしないでください。
4. ボスにはToxで直接連絡できます。

2025-04-24 09:24

原文

We have many customers, please don't talk to me about these irrelevant topics, it has nothing to do with our team.
If you are a professional cybersecurity professional, you should understand the operating model of lockbit.
If you are just a middleman scammer. This is the price you have to pay.

日本語訳

私方には多くの顧客がいます。無関係な話題はやめてください。私たちのチームとは関係ありません。もしあなたがプロのサイバーセキュリティ専門家なら、LockBitの運用モデルを理解しているはずです。もし単なる仲介の詐欺師なら、これはあなたが払うべき代償です。

2025-04-24 09:25

原文

I have the evidence in hand, I paid you, and after waiting for a month, you didn't solve the problem, and you banned the page!!

日本語訳

証拠は手元にあります。私は支払いしました。1か月待っても問題は解決せず、あなたたちはページを凍結しました！

Victim

2025-04-24 09:27

原文

Then you send me your boss's tox, and I'll communicate with your boss!

日本語訳

それならあなたの上司のToxを送ってください。あなたの上司と直接やり取りします！

2025-04-24 09:28


lofikdis

原文

Stupid guy.
Lockbit has hundreds of teams. We have never encountered you in this branch.
If you negotiate a solution, then continue to communicate. Otherwise, we refuse to process any of your messages and your customers will lose data forever.

日本語訳

愚かな奴だ。
LockBitには何百ものチームがある。この支部でお前に会ったことはない。
解決策を交渉するなら、やり取りを続ける。そうでないなら、お前のメッセージの処理を拒否するし、お前の顧客は永遠にデータを失う。

2025-04-24 09:28

図 II-3-3: アフィリエイトによる責任分担の主張

3.3 アフィリエイト活動量の分布

ビルドを実行したアフィリエイトは54名、チャット記録上で交渉に関与したアフィリエイトは35名である。users テーブル上の paused フィールドでは paused = 0 (アクティブと推測) が40名、paused = 1 (停止と推測) が35名となっている。パネル上で、アフィリエイトの活動状況まで細かく記録されていた実態がうかがえる。

さらに、ビルド数やチャット件数、被害組織数などの活動量の分布を分析すると、アフィリエイト間で大きなばらつきがあることが分かる。ビルド数で見ると、上位10名が全体の約67% (791/1,183 件) を占めており、チャット件数や被害組織数も同様に一部のアフィリエイトに集中している傾向が見られる。アフィリエイトごとに活動量の偏りがあることは、攻撃者側の運営体制の実態を理解するうえで重要なポイント

である。

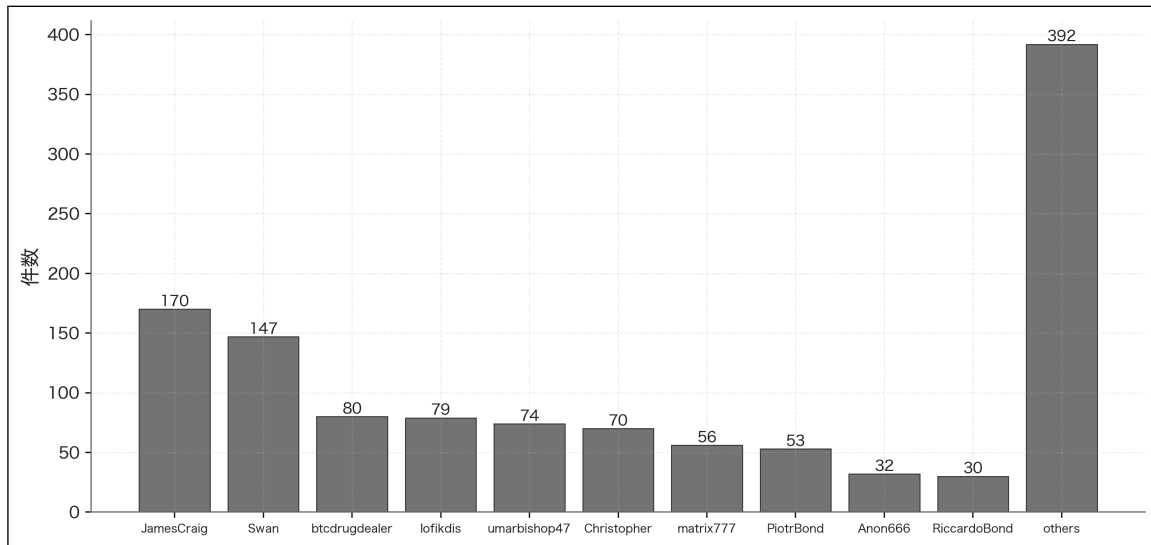


図 II-3-4: アフィリエイト別ビルド件数の分布

ビルド実行の曜日・時間帯傾向

全 1,183 件のビルドについて、created_at を UTC の曜日 × 時間帯に変換して集計した結果を図 II-3-5 に示す。火曜日の UTC 15 時付近にビルド実行が集中し、日曜日は全体的に件数が少ない傾向が見られた。

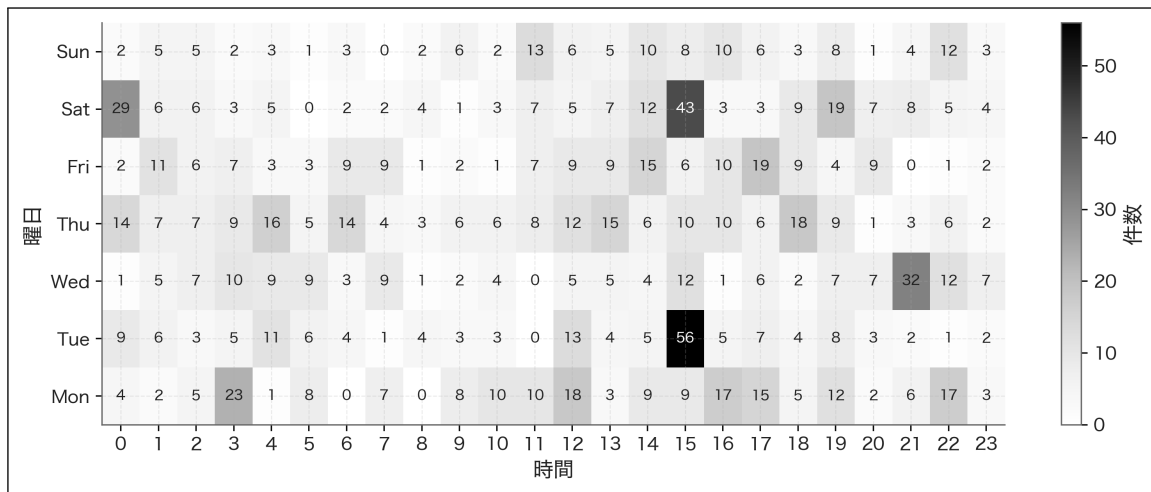


図 II-3-5: ビルド実行の曜日 × 時間帯別ヒートマップ

アフィリエイト別のチャット件数と被害組織数

全 4,423 件のチャットメッセージをアフィリエイト別に集計すると、Christopher が 2,078 件 (全体の 47%) と突出していることが分かる。Christopher に紐付く被害組織は clients テーブル上で 44 件、正規化ドメイン単位では 19 組織であり、いずれもアフィリエイト中で最多である。全体として、被害組織数が多いアフィリエイトほどチャット件数も多い傾向が見られる。図 II-3-6 にチャット件数、図 II-3-7 に被害組織数の分布を示す。

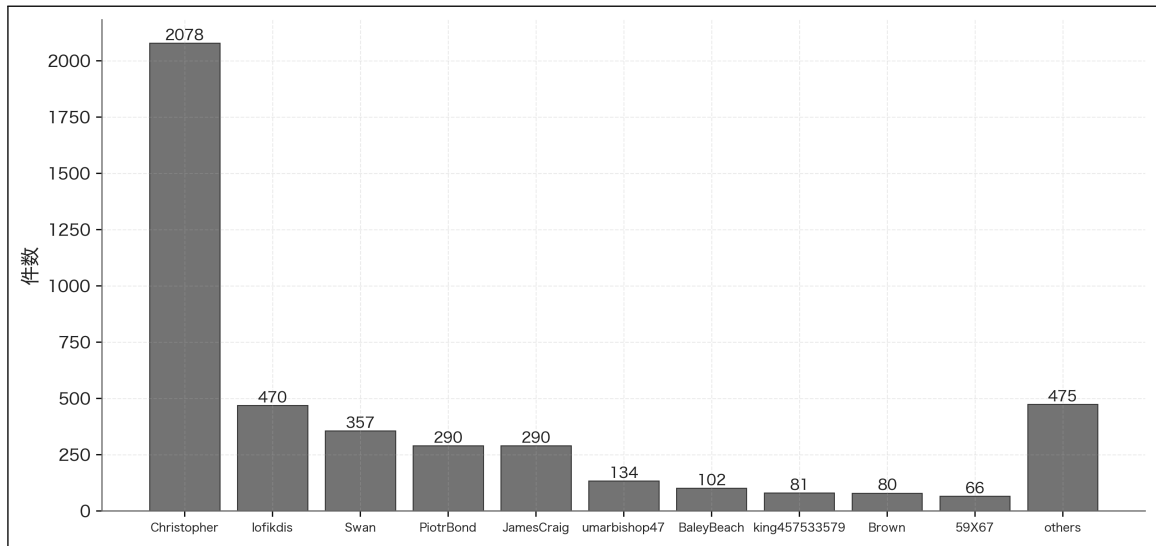


図 II-3-6: アフィリエイト別チャット件数の分布

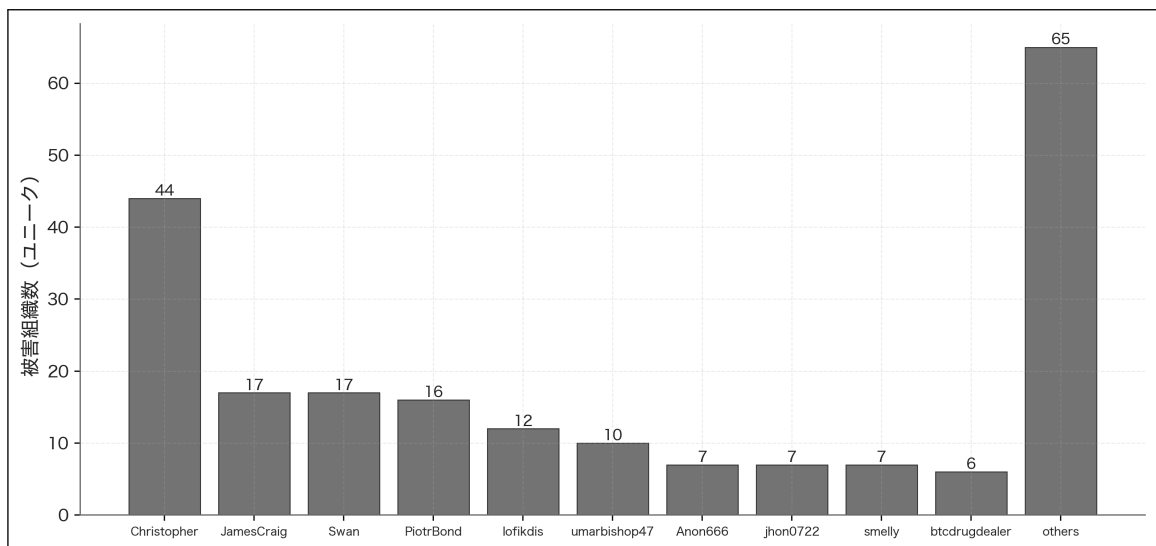


図 II-3-7: アフィリエイト別被害組織数の分布

活動量の多いアフィリエイトには、交渉スタイルにも特徴が見られる。被害組織数が最多の Christopher は返信速度が比較的早く、定型文を多用する傾向がある。LockBit のブランドを前面に出した脅迫が目立ち、復号への疑念を示す被害組織に対しては、LockBit のこれまでの実績を根拠に信頼性を繰り返し主張していた。

一方、ビルド数が最多の JamesCraig は淡々とした事務的な対応が特徴的である。価格交渉では即日支払いを条件とした値下げに応じるケースもあった。減額幅は通常 50%との発言もあるが、7 割近い減額に応じた事例も見られた。

3.4 参加から活動開始までの期間

ビルドを実行したことのある 54 名について、参加 (users.created_at) から初回ビルドまでの経過時間を算出した。35 名 (約 65%) が参加から 24 時間以内、43 名 (約 80%) が 7 日以内に初回ビルドを実行した。一方、登録アカウント 75 名のうち 21 名は一度もビルドを実行しておらず、こうした点も踏まえると、アフィリエイトの活動への積極性や関与の深さには大きな差があることが分かる。図 II-3-8 に 54 名の期間分布を示す。

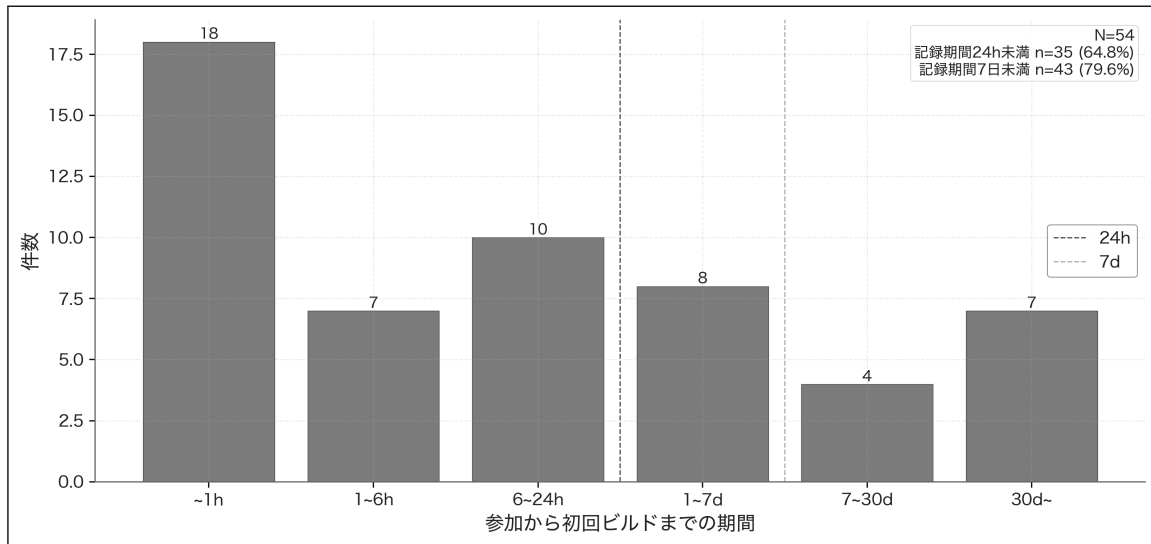


図 II-3-8: 参加から初回ビルドまでの期間分布 (対数スケール)

3.5 アフィリエイト間の差異 (権限・設定)

users テーブルでは、アフィリエイトアカウントごとにタグ、権限リスト (permissions)、ビルダー関連の設定 (builders_settings など) が記録されている。タグは newbie (62 名)、verified (5 名)、タグなし (8 名、うち 2 名は admin を含むコアアカウント) などに分かれており、大半が newbie に分類されている。

ここでいう permissions は、chats、write_chat、builder_chat_generate など、アカウントに付与された画面・機能アクセス権の一覧である。一方、builders_settings は {"10":true,"20":true,...} のような形式で保存されており、ビルドタイプまたはビルダー機能の有効フラグと見られるアカウント単位の設定である。

これに対し、実際の各ビルドで選択された詳細オプションは、builds_configurations.config にビルド単位で記録されている。例えば、暗号化対象、プロセス停止、ネットワーク共有、自己削除、空き領域消去などの設定は、ビルドごとの config から確認できる。

本節で扱う newbie / verified などのタグは、各ビルドに付与されたタグではなく、users テーブルに記録されたアフィリエイトアカウント単位の属性である。一方、ビルドオプションは builds_configurations.config に記録されたビルド単位の設定であり、同一アフィリエイトであってもビルドごとに異なる設定パターンが確認される。

以下では、builds.userid を介して各ビルドを実行者の users.tag と結合し、流出時点のアカウントタグ別に設定傾向を比較する。ただし、タグや権限設定の変更履歴は確認できないため、各ビルド時点のタグ・権限状態を厳密に復元するものではない。

特定のアカウント設定 (linesxi_on [原 DB 上の綴り]、paranoid_mode、negotiations) は、75 アカウント中 2 アカウントのみで有効化されている。名称からそれぞれ ESXi 環境向け機能、慎重なモードに類する設定、交渉関連機能と推測されるが、機能の実態は断定できない。この 2 アカウントはいずれも admin を含むタグなしのコアアカウントであり、一般のアフィリエイト (newbie / verified) には付与されていない。

keep_messages_unread (メッセージ未読保持と推測) という設定も存在するが、全アカウントで値が 0 であり、利用の痕跡はなかった。

実行者タグ別に見たアカウント設定とビルド設定の傾向

newbie と verified の間で、アカウント設定値に明確な機能差は確認できなかった。builders_settings のフラグ数を比較すると、newbie は平均 7.66 個 (中央値 9 個) であるのに対し、verified は平均 5.4 個 (中央値 6.0 個) である。ただし、この差はタグがビルド機能の利用可否を直接決めていることを示すものではない。builders_settings はアカウント単位の設定値であり、ビルドごとの実際のオプション設定とは区別して解釈する必要がある。

実際のビルド設定を見ると、同一アフィリエイトであってもビルドごとに異なるオプション設定が用いられている。複数ビルドを実行したアフィリエイト 51 名のうち、実質的なオプション設定が全ビルドで同一だったのは 2 名のみであり、大半は標的やビルドタイプに応じて設定を変えていた。

一方、運用面では明確な差異がある。停止率 (paused = 1) は verified が 0% (5 名全員がアクティブ) であるのに対し、newbie は約 48% (62 名中 30 名) に達する。アカウント寿命の中央値も verified が約 105.5 日、newbie が約 32.2 日と大きく異なる。

指標	newbie (62 名)	verified (5 名)
builders_settings フラグ数 (平均)	7.66	5.4
builders_settings フラグ数 (中央値)	9	6.0
停止率	約 48% (30 名)	0% (0 名)
アカウント寿命 (中央値)	約 32.2 日	約 105.5 日

以上から、本データではタグがビルドオプションの利用可否を直接決定していたとは確認できない。一方で、停止率やアカウント寿命には差が見られるため、タグはビルド機能そのものよりも、アカウントの運用状態や内部上の位置づけと関係していた可能性がある。

3.6 他の攻撃グループとの関連

チャット記録からは、アフィリエイトが複数の RaaS グループに関与している事例が読み取れた。アフィリエイト「BaleyBeach」は、別のランサムウェア攻撃グループ「RansomHub」の停止を受け、窃取データごと LockBit の Lite パネルに移籍してきたと主張していた。また、「KoreyAllen」というアフィリエイトは別のランサムウェア攻撃グループ「HellCat」と「LockBit」の両方に在籍していたと述べた。RaaS モデルはオペレーターが提供するインフラをアフィリエイトが利用する構造であるため、こうしたグループ間の移動や並行参加が起こりやすい環境であると言える。

※チャット記録をもとにイメージ化したもの

RansomHubからの移籍に関するチャット記録



Victim

原文
Hi, can you explain what is happening?

日本語訳
こんにちは、何が起きているのか説明してもらえますか？

2025-04-02 14:45



BaleyBeach

原文
We were affiliates of RansomHub, now RansomHub closed, we moved here. So existing companies (including yours) which we had to deal with still have chance to prevent their data leak.

日本語訳
私たちはRansomHubのアフィリエイトでしたが、RansomHubが閉鎖され、ここ（LockBit）に移動しました。既存の企業（御社を含む）で対応が必要だった企業は、まだデータ漏洩を防ぐチャンスがあります。

2025-04-02 14:49



Victim

原文
So are you not RansomHub anymore?

日本語訳
では、あなた方はもうRansomHubではないのですか？

2025-04-03 08:13



BaleyBeach

原文
We are the only owners of your data, we - previous affiliates of RansomHub, now LockBit. In any case, this does not concern you. All you need to know that we are the only owners of your data. And our negotiation interrupted payment stage. Final price is 900k as we said.

日本語訳
私たちがあなたの方のデータの唯一の所有者です。元RansomHubアフィリエイト、現在はLockBitです。いずれにせよ、これはあなた方には関係ありません。知っておくべきことは、私たちがあなたの方のデータの唯一の所有者だということです。交渉は支払い段階で中断されました。最終価格は申し上げた通り90万ドルです。

2025-04-03 09:32



Victim

原文
I'm confused because when we were talking on the other channel, you offered us a substantial discount that doesn't seem to be factored into the price you're asking here.

日本語訳
混乱しています。別のチャンネルで話していたとき、かなりの割引を提示されましたが、ここで要求している価格にはそれが反映されていないようです。

2025-04-04 04:45



BaleyBeach

原文
It was 10% if you pay till the end of that month?

日本語訳
その月の終わりまでに支払えば10%でしたか？

2025-04-04 04:47

原文
The only discount we can give you is 10% till the 10th of this month, after price will be again 900k.

日本語訳
唯一提供できる割引は、今月10日までの10%です。それ以降は価格は再び90万ドルになります。

2025-04-04 04:50

図 II-3-9: RansomHub からの移籍に関するチャット記録

チャットのやり取りから、RansomHub から LockBit への移行に伴い、被害組織側が混乱する様子も見受けられた。当該被害組織は LockBit / RansomHub 両グループのリークサイトに重複して掲載されたことが確認できた。



図 II-3-10: HellCat と LockBit の両方に在籍しているアフィリエイトのチャット記録

3.7 標的地域の傾向

被害組織数が多い上位 10 名のアフィリエイトについて、被害組織の拠点となる国を分析し、アフィリエイトごとの地域別分布をヒートマップで示す(図 II-3-11)。アフィリエイト名の横の括弧内の数値は、各アフィリエイトが担当する一意の被害組織数である。

一部のアフィリエイトで地域的な偏りが顕著に表れている。特に Christopher は被害組織 19 件のうち 14 件(約 74%) がアジアに所在しており、地域的な集中が見られる。

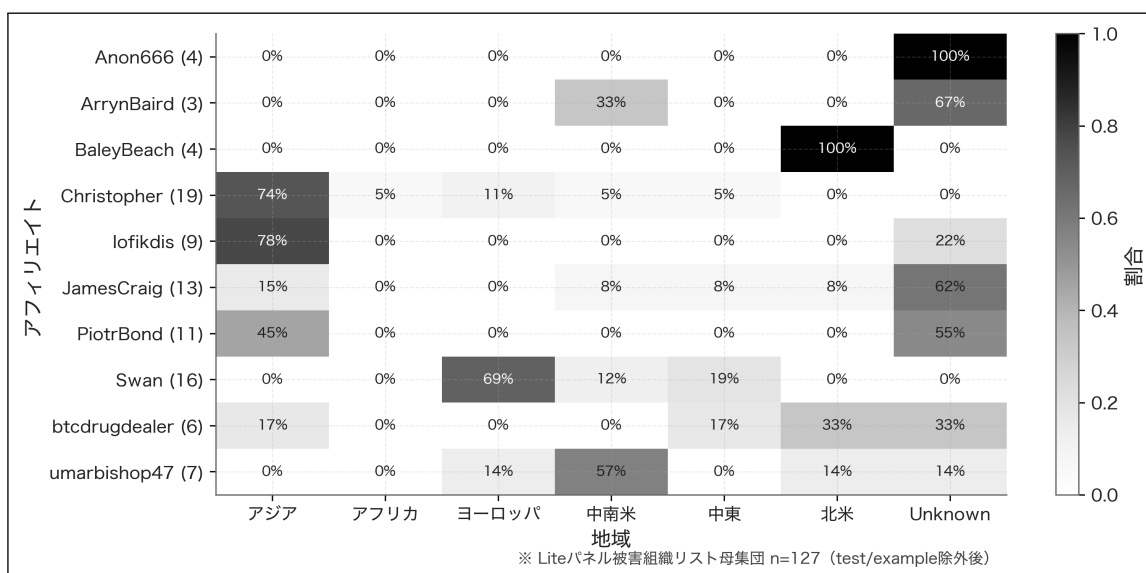


図 II-3-11: アフィリエイトごとの地域別攻撃分布ヒートマップ

こうしたばらつきから、ターゲット選定においてアフィリエイトの裁量が認められていた可能性がある。被害組織の全件が北米に所在するアフィリエイトも存在しており、地域的な傾向はアフィリエイトごとに大きく異なっている。

4. 準備フェーズ：ビルドと設定

本章では、アフィリエイトが攻撃実行のためにビルドしたランサムウェアの実行ファイルに着目し、その設定内容から攻撃準備フェーズの実態を分析する。対象テーブルは `builds`、`builds_configurations`、`clients`、`users`、`pkeys` であり、分析単位は原則としてビルド (`build_id`) である。時刻は UTC+0 に基づく。

ビルドには OS 種別、暗号化対象の除外リスト、プロセス・サービスの停止リストなど、攻撃の挙動を左右する多数の設定項目が含まれている。ビルドタイプ (`type=30/40/46/25/50` 等) や機能の分類は、一次データのキー名・設定パターンに基づく推定を含み、挙動を断定するものではない。母数が図表ごとに異なる場合はその都度明記する。

4.1 ビルド数の推移と傾向

分析対象期間中に記録されたビルドは総数 1,183 件 (`builds` テーブル全レコード) であった。このうち、`builds.type` フィールドから OS・用途を分類できたものは 798 件 (約 67%) である。図表・本文では全件 (1,183 件) と分類可能件数 (798 件) のどちらを母数としているかをその都度明記する。

それぞれのレコードに含まれる日付情報から、図 II-4-1 に日別のビルド数の推移を示す。Lite パネルの立ち上げからデータ流出時点まで、継続的にビルドが行われていたことが分かる。なお、ビルド数が最大となったのは 2025 年 3 月 25 日の 53 件であり、`pkeys` (暗号化に用いる公開鍵情報を格納したテーブル) も同日に 52 件を記録した。両者の件数が完全には一致しないのは、鍵レコードの欠損やビルド処理と鍵生成の記録タイミング差が原因と考えられる。

ただし、ビルドにはテスト設定 (`test.local` など) も含まれるため、ビルド数が実際の攻撃件数と直結するものではない。

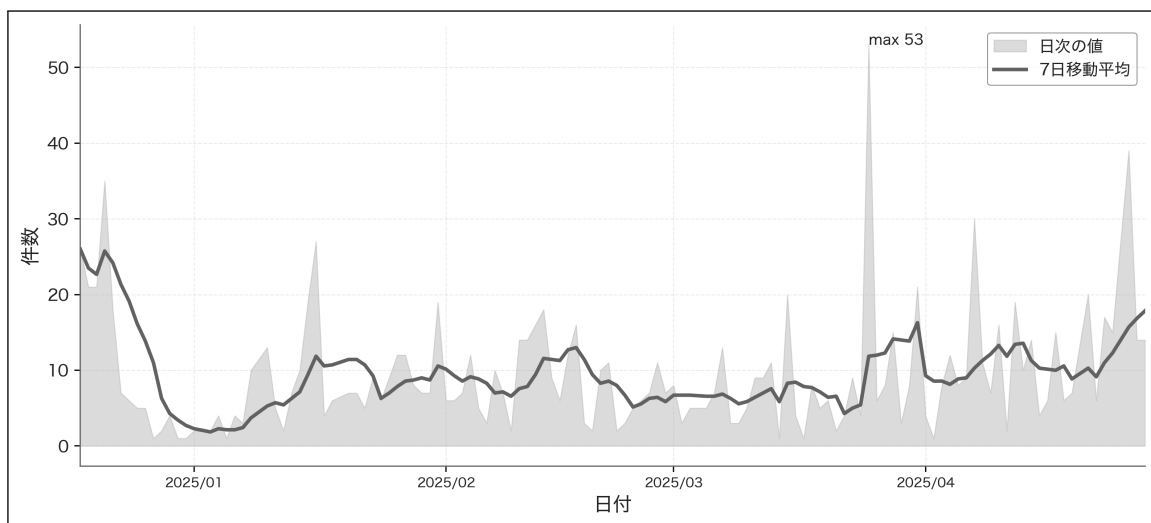


図 II-4-1: ビルド数の日別推移

4.2 対象 OS 別の設定内容

各ビルドには `builds_configurations` テーブルで詳細な設定が定義されている。`builds.type` の値と設定キーの構成から、ビルドタイプと対象 OS の関係は表 II-4-1 の通り推定される。本節では分析対象の中心となる `type = 30` (Windows)、`40` (Linux)、`46` (ESXi) を扱う。

表 II-4-1：ビルドタイプと対象 OS の対応

builds.type	推定される対象	件数	備考
30	Windows	504 件	最多
40	Linux	143 件	
46	ESXi	151 件	
25	不明	297 件	設定スキーマの大部分が不明。一部の設定キー (not_randomize_keys・running_one 等) のみ解釈可能
50	不明	88 件	テストデータを含む

一部のビルド設定には、データを完全に削除するワイプ機能に相当する項目も含まれている。これはキー名に基づく観測であり、実際の挙動は一次データだけでは確定できない。

ビルドタイプの内訳

builds.type の値ごとの件数は表 II-4-1 に示した通りである。図 II-4-2 にビルドタイプ別の内訳を示す。

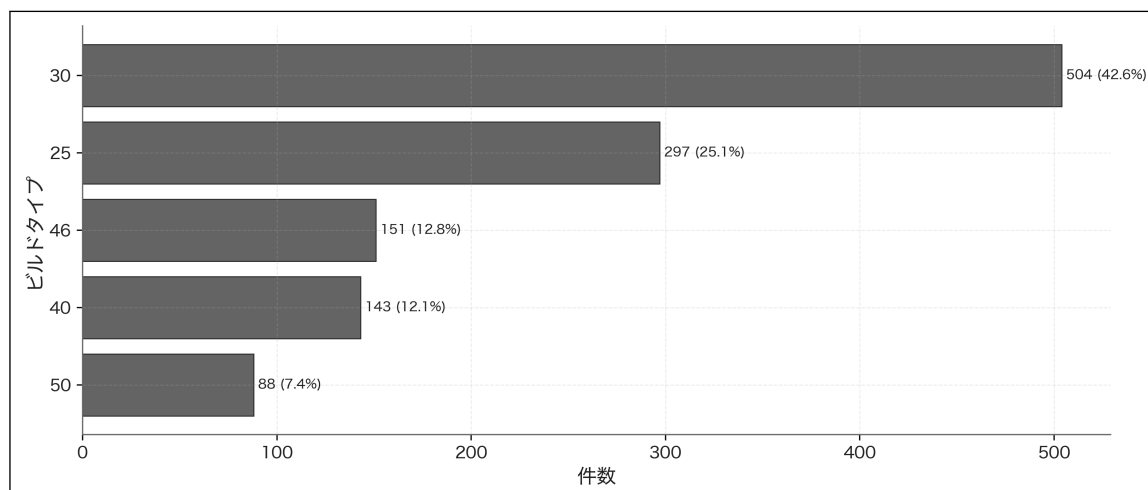


図 II-4-2: ビルドタイプ別内訳

ビルドタイプ分類の根拠

各タイプの分類は builds_configurations.config 内の設定キーパターンに基づく推定である。

type=30 (Windows)

language_check、white_folders といった Windows 固有の設定キーが一貫して含まれる。

type=40 (Linux) / type=46 (ESXi)

いずれも vm_to_skip (VMware vCenter 等)、files_to_skip_vmdk (vmdk 関連) が含まれる。両者の違いは extensions フィールドにある。

type=46 は常に値が入っており、設定ファイル拡張子 (ini, conf, env, json, yaml, yml 等) が指定される傾向がある一方、type=40 の extensions はほぼ空白である。

加えて、復号ツールのファイル名プレフィックス (LBG → type=25、LBB → type=30、LBL → type=40、ESXi → type=46) にも対応関係が見られ、type=40 を Linux 系、type=46 を ESXi 系と解釈する根拠を補強している。

ビルドタイプ別の設定傾向

図 II-4-3 に、ビルドタイプ別の設定キー有効率をヒートマップで示す。設定値が true または 1 である割合を算出し、ビルドタイプ間の差が 15% 以上のキーに限定した。kill_processes_list、kill_service s_list のような文字列リスト型のキーは true/false ではないため対象外としている。

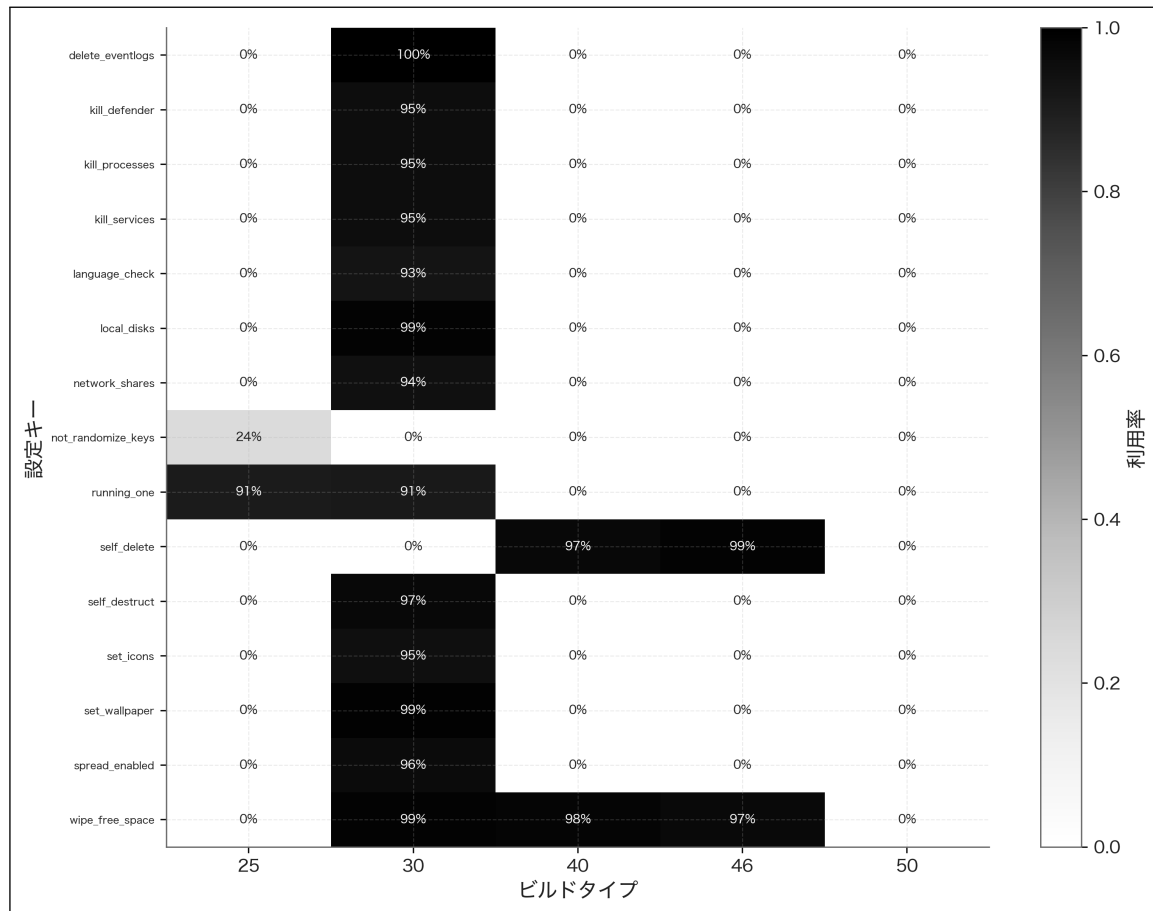


図 II-4-3: ビルドタイプ別設定キー有効率

Windows 向けビルド (type=30) では language_check の有効率が約 93% と高い。特定の言語環境を検出した場合に動作を変更するこの機能が広く採用されている。イベントログやバックアップの削除、プロセス・サービスの停止も高頻度で有効化されている。自己拡散機能 (spread_enabled) も 96% と高頻度で有効化されており、侵入後の横展開を前提とした設定が標準的に組み込まれていたと見られる一方、GPO 経由の展開は低頻度にとどまった。なお、type=25 は大半の設定スキーマが不明だが、not_randomize_key s・running_one など一部のキーは他タイプと共通の形式で読み取れたため、図 II-4-3 にもこれらのキーのみ表示されている。

Linux/ESXi 向けビルド (type=40/46) では、管理 VM や特定のフォルダ・拡張子を暗号化対象から除外する設定が見られるほか、spot_size 等による部分暗号化が選択されるケースも多い。除外設定の具体的な値と傾向については 4.3 で詳述する。

これらの設定傾向から、攻撃者は暗号化の成功率と最低限の運用維持を両立させる方向で、ビルドタイプごとに設定を使い分けられていることが分かる。防御側は、Windows 環境では言語チェック回避やイベントログ削除への対策、仮想化環境では管理基盤の分離・権限設計・バックアップ経路の保護を検討する必要がある。

4.3 除外設定とその意図

本節では、4.2 で触れた Linux/ESXi 向けビルド (type=40/46) の除外設定を詳細に分析する。

暗号化の除外設定

Linux/ESXi 向けビルドの `builds_configurations.config` には、暗号化の除外オプションとして `vm_to_skip` (VM 除外)、`files_to_skip_vmdk` (ファイル・拡張子除外)、`skip_folders` (OS 領域除外) の 3 つのキーがある。プロセス・サービスの停止 (`kill_processes`、`kill_services` 等) は暗号化対象から外すのではなく「暗号化を通すために止める」挙動であるため、4.4 で別途扱う。

図 II-4-4 に、type=40/46 における上記 3 キーの使用率を示す。使用率は各ビルドにおいて当該キーに値が設定されているか (空ではない) を基準に算出した。

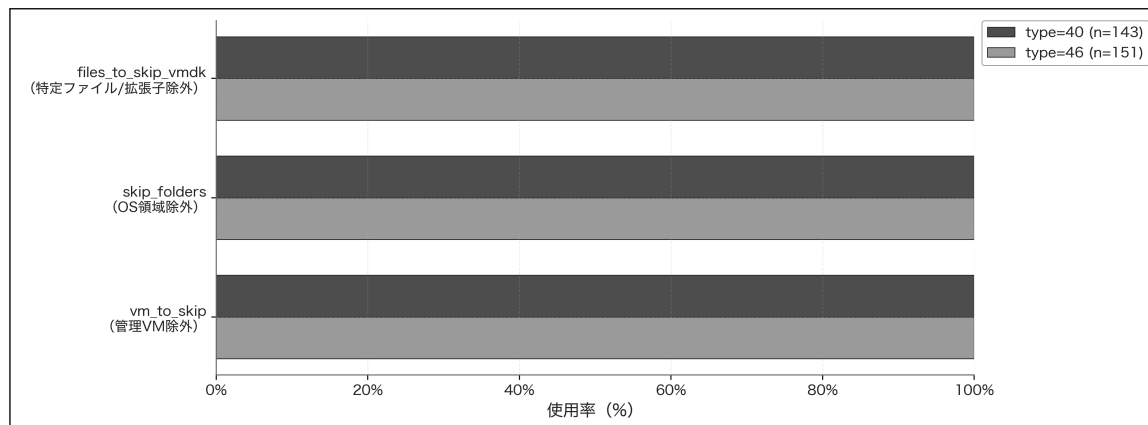


図 II-4-4: 除外設定の使用率 (type=40/46)

除外設定の内訳

続いて、各除外設定の内訳を見ていく。以降の内訳図 (図 II-4-5~II-4-7) では、母数を「当該キーが設定されているビルド」に限定し、各要素の含有率 (その要素を含むビルドの割合) を算出した。含有率が 100% に近い項目が並ぶ場合、共通設定がテンプレートのように利用されていることを示す。

vm_to_skip の内訳

`vm_to_skip` は、暗号化処理の対象から除外する仮想マシン (VM) の名称を指定するフィールドである。図 II-4-5 にその内訳を示す。上位に出現するのは VMwarevCenter (vSphere 環境全体を管理する中核 VM) および VMware-VirtualSAN-Witness (vSAN クラスタのクォーラムを維持する監視 VM) であり、いずれもほぼ同率で含有率が高い。これらの管理系 VM を暗号化すると、vSphere 環境の管理機能や vSAN クラスタの運用に重大な支障が生じる可能性があるため、意図的に除外しているものと考えられる。なお、VMwarevCenter と vCenter 等は表記揺れ (同一対象の別名) の可能性がある。

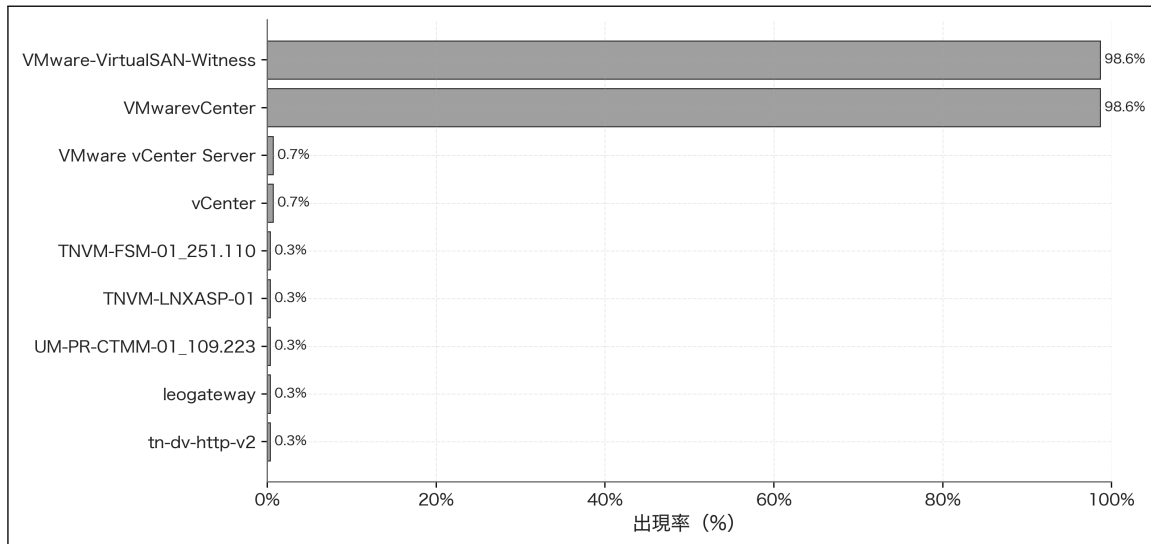


図 II-4-5: vm_to_skip 設定値の内訳

skip_folders の内訳

図 II-4-6 に skip_folders に設定される値の内訳を示す。上位項目は大きく 2 つに分かれる。

1 つ目は etc、dev、bin、usr、lib といった Linux/Unix 系 OS の基本ディレクトリである。これらはシステムの起動や基本動作に不可欠な領域であり、暗号化すると OS 自体が起動不能になる。

2 つ目は bootbank、altbootbank など ESXi 固有の領域である。ESXi のブートイメージや更新モジュールが格納されるこれらのフォルダを除外することで、ハイパーバイザーの起動は維持される。

ビルドタイプ別に集計すると、テンプレート構造がより明確になる。type=40・type=46 の両方で含有率 100% の共通項目は以下の 13 項目である。Linux/Unix 系の基本ディレクトリである etc (設定ファイル)、dev (デバイスファイル)、bin・sbin (実行バイナリ)、usr (システム共通のプログラム格納領域)、include (ヘッダファイル)、lib・lib64 (共有ライブラリ)、proc (カーネル情報)、mbr (マスターブートレコード)、そして ESXi 固有の tardisks (追加モジュール)、bootbank・altbootbank (ブートイメージ) である。いずれもシステム起動や OS 動作に不可欠な領域であり、暗号化すると環境自体が使用不能になるため除外されている。

これに加え、type=40 では scratch (ESXi 一時領域)、store (ESXi ストレージ)、System、boot 等 8 項目が、type=46 では tardisks.noauto が追加される。いずれもタイプ内での含有率はほぼ 100% であり、タイプごとに異なる固定テンプレートが適用されている。

type=40 側に ESXi 固有の除外項目 (scratch・store 等) が type=46 より多く含まれる点は一見不自然だが、type=40 が vCenter Server Appliance のような、ESXi 環境全体を管理する Linux ベースの基盤を対象としている可能性を示唆しており、type=40=Linux・type=46=ESXi という分類と矛盾するものではないと考えられる。ただし、ビルドタイプの分類はキー名・設定パターンに基づく推定であり、実行環境やファイル形式を直接確認したものではない点に留意されたい。

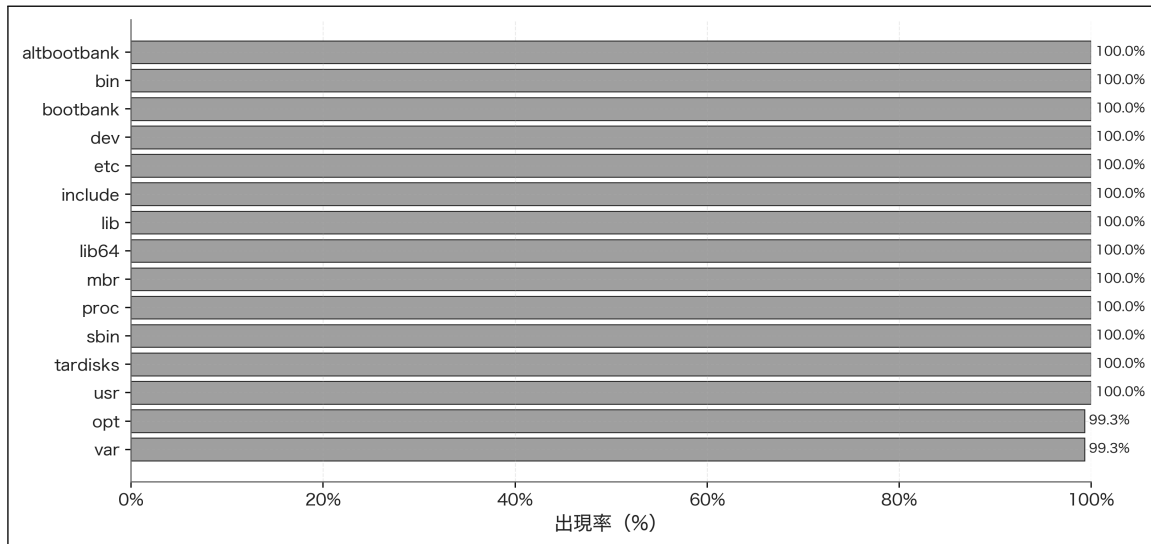


図 II-4-6: skip_folders 設定値の内訳

files_to_skip_vmdk の内訳

files_to_skip_vmdk は、暗号化処理の対象から除外するファイルの拡張子を指定するフィールドである。キー名からは vmdk (仮想ディスク) に特化した設定を連想しやすいが、図 II-4-7 に示すとおり実際に上位に並ぶのは .exe (実行ファイル)、.dll (動的リンクライブラリ)、.sys (システムドライバ) 等の一般的な拡張子である。これらは OS やアプリケーションの動作に不可欠なファイルであり、暗号化するとシステムが動作不能になる。キー名とは裏腹に、OS 基盤のファイル全般を除外する汎用リストとして使用されている可能性がある。

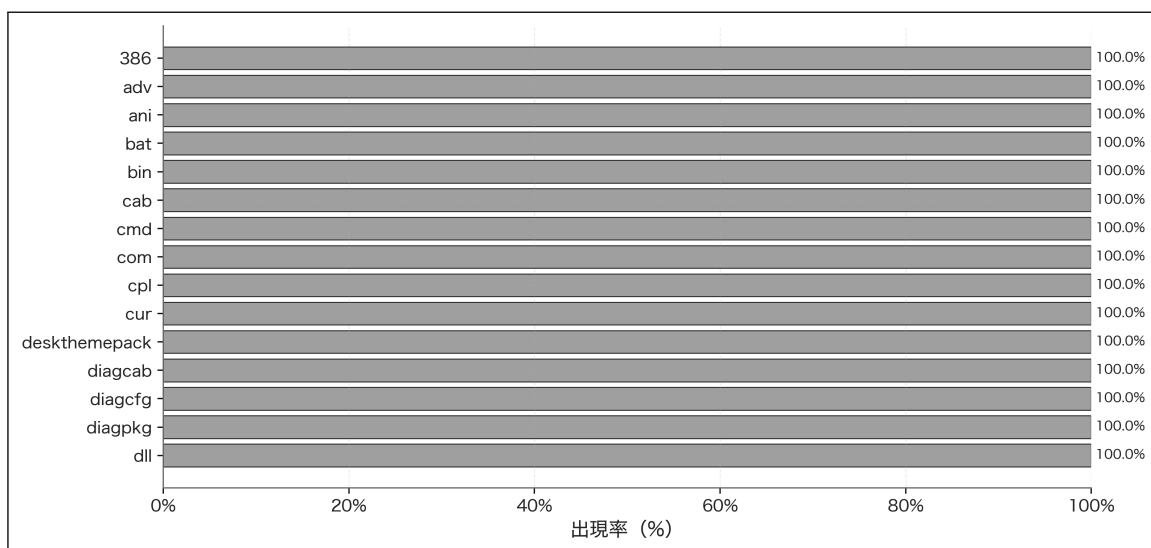


図 II-4-7: files_to_skip_vmdk 設定値の内訳

除外設定に見られるテンプレート構造と設計意図

3つの除外キーに共通して、上位項目の含有率がほぼ均一に高い。アフィリエイトが個別に設計したのではなく、あらかじめ用意された固定テンプレートがそのまま利用されていると見られる。

このほか、type=40/46 の設定には admin_extensions というキーが存在し、vmdk や vbk 等の拡張子がセミコロン区切りで列挙されている。このキーが暗号化ロジック上でどのように動作するのか一次データだけでは断定できないものの、仮想ディスクやバックアップ等の運用上重要なデータ型が一括で列挙されている点は、攻撃者が意識する標的の傾向と捉えることもできる。

以上より、除外設定は固定テンプレートに基づく運用である可能性が高い。

4.4 停止対象プロセス・サービス

ビルド設定には、暗号化の準備段階として停止するプロセスやサービスのリスト (kill_processes_list、kill_services_list) が含まれている。図 II-4-8 に Windows 向けビルド (type=30) の停止対象プロセス上位、図 II-4-9 に停止対象サービス上位を示す。いずれもリスト要素を分割し、使用率の上位を可視化したものである。

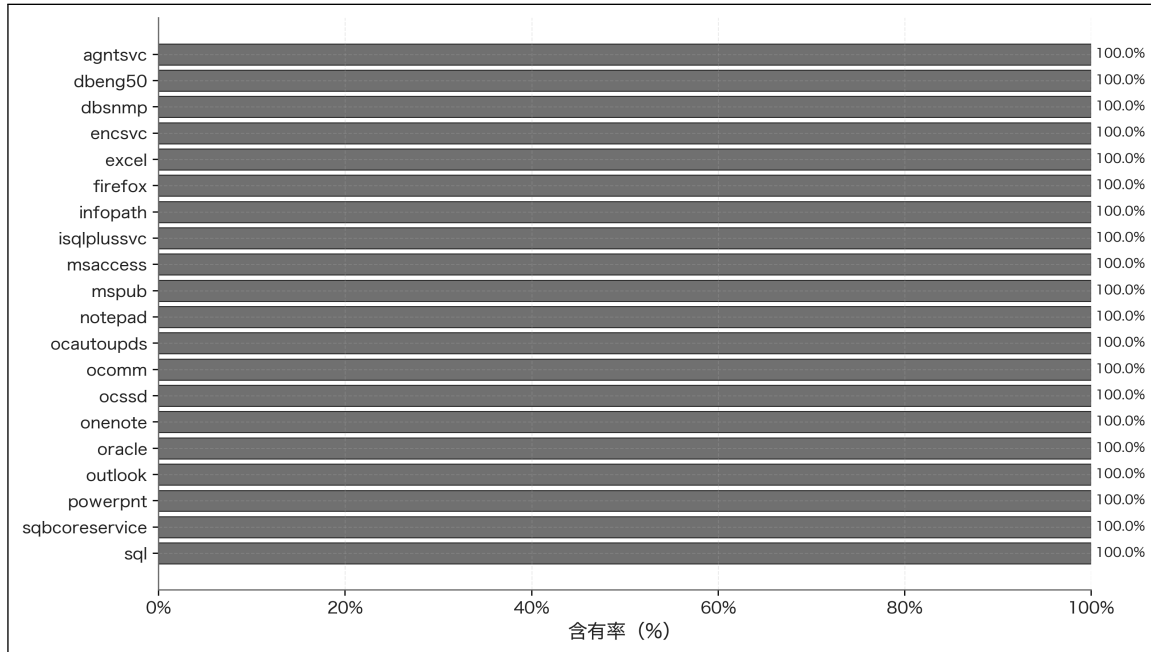


図 II-4-8: 停止対象プロセス上位 (type=30)

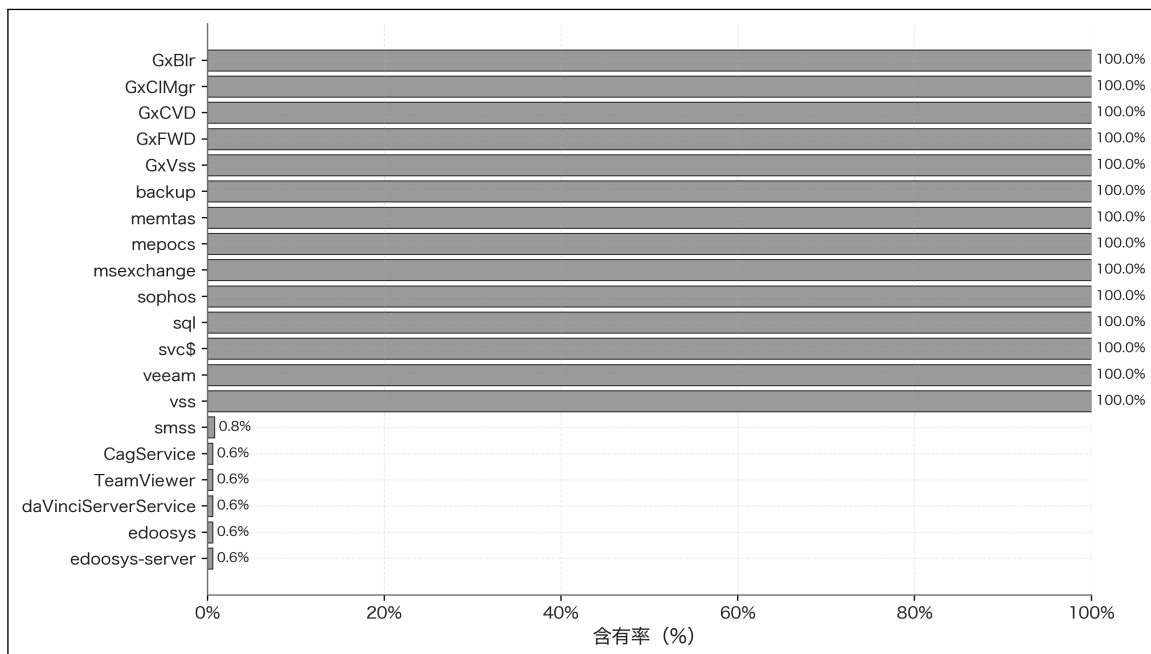


図 II-4-9: 停止対象サービス上位 (type=30)

表 II-4-2：停止対象の主要カテゴリ整理 (type=30)

カテゴリ	代表例 (図 II-4-8/4-9 で頻出)	解釈
データベース	sql, oracle, dbsnmp	DB ファイルのロック解除や業務停止を狙う停止対象
メール	outlook, thunderbird, msexchange	連絡基盤・業務継続系システムへの影響を狙う停止対象
バックアップ	veeam, backup, GxVss	復旧経路の阻害を狙う停止対象
セキュリティ	sophos など	検知・防御機能の弱体化を狙う停止対象

停止対象には、DB・メール・バックアップ・セキュリティに関連する項目が目立つ一方、Excel・PowerPoint など文書編集系の汎用アプリケーションも同様に高い頻度で含まれていた。後者は、ファイルを開いたまま保持しているアプリケーションを終了させることで、そのファイルのロックを解除し、暗号化範囲を広げる狙いがあると考えられる。4.3 の除外設定と同様に、共通テンプレートに基づく設定が使われていた可能性が高い。

これらの停止対象は、暗号化処理を妨げるプロセス (データベースのファイルロック等) を排除すると同時に、業務停止のインパクトを最大化して交渉上の優位を得る設計と見られる。防御側は、暗号化の検知だけでなく、データベース・バックアップ・セキュリティ関連のプロセスやサービスの異常停止を早期検知の指標として監視し、検知時の隔離・権限遮断・バックアップ保護への即時連携を整備しておくことが望ましい。

5. 交渉フェーズ：チャットに記録されたやりとり

本章では、被害組織と攻撃者の間で交わされたチャット記録を分析し、身代金交渉の実態を明らかにする。対象テーブルは clients、chats、visits であり、時刻は UTC+0 に基づく。

Lite パネルには 4,423 件のチャットメッセージが記録されており、初回接触から要求額の提示、減額交渉、支払い、復号ツール提供に至るまでの一連のやりとりが確認できる。

5.1 交渉プロセスの全体像

会話チャットの記録を時系列に沿って整理すると、身代金交渉は主に以下の 6 段階の流れで進行する。本章以降の分析ではこの段階区分を基準として用いる。なお、これは観察されたパターンの整理であり、推奨される交渉手順や支払い判断の指針ではない。

1. 初回通知

攻撃者からのテンプレートメッセージ

2. 事実確認・証拠提示

窃取データの存在証明、テスト復号

3. 要求額・期限の提示

金額と支払い締切の通告

4. 交渉フェーズ

減額、条件調整

5. 支払いフェーズ

送金・確認

6. 復号・復号後の対応

ツール提供・問題対応

チャットは同一のテンプレートで開始される。定型的な初回メッセージにはテスト復号の手順や添付サイズ上限などの注意事項が含まれており、初回接触の対応が定型化されている。図 II-5-1 にその例を示す。

※チャット記録をもとにイメージ化したもの

交渉開始テンプレート文（マスク）



Affiliate

原文

You can attach a few files for test decryption by packing them into an archive with zip, rar, tar, 7zip, 7z, tar.gz extensions of no more than 10 megabytes using the attach button directly in the chat.

If your archive weighs more than 10 megabytes, please use our file sharing service.

http <url : masked> onion http <url : masked> onion http <url : masked> onion For security reasons we do not click on other links you send in chat.

Please wait for a reply, sometimes it takes several hours due to possible time zone differences.

日本語訳

テスト復号化のために、チャット内の添付ボタンを使用して、zip、rar、tar、7zip、7z、tar.gz形式のアーカイブに最大10メガバイトのファイルを数個まとめて添付することができます。

アーカイブのサイズが10メガバイトを超える場合は、当社のファイル共有サービスをご利用ください。

http <url : masked> onion http <url : masked> onion http <url : masked> onion セキュリティ上の理由から、チャットで送信される他のリンクはクリックしないようお願いいたします。

返信をお待ちください。タイムゾーンの違いにより、回答までに数時間かかる場合がございますのでご了承ください。

図 II-5-1: 交渉開始時のテンプレート文 (原文・翻訳、マスク済み)

5.2 チャットへの参加率

被害組織がどの程度チャットに参加したかを確認するため、Lite パネルの記録を集計した。パネル上では同一組織と見られるにもかかわらず複数の client_id で登録されているケースがある。そのため本レポートでは「ID (スレッド) 単位」と「組織 (正規化ドメイン等の一意値) 単位」を分けて整理する。

集計結果は以下の通りである。

- clients テーブルに登録された client_id は 246 件であった。この中にはテストドメイン等も含まれるため、ここでは被害組織そのものではなく、パネル上の登録 ID 数として扱う。
- ダッシュボードへの参加 (アクセス記録あり) は 239 件であり、clients 全レコードに対する参加率は 97% と高い水準であった。
- chats テーブルに登録された client_id の数は 208 件であり、この件数がチャットに参加、すなわち交渉スレッドが作成された ID 数と考えられる。
- これら 208 スレッドにおける client_id を、正規化したドメイン等のユニーク値で名寄せして集約すると、重複やテストデータを除いた一意な組織数は 127 となる (208 スレッド → 127 ドメイン)。
- 以降、この 127 ドメインを一意的被害組織数として扱う。

図 II-5-2 は clients・visits・chats を client_id で突合し、ダッシュボード参加からチャット参加までの段階別件数を集計したものである (分析単位: client_id、母数: clients 全レコード)。



図 II-5-2: 被害組織の段階別内訳

この 127 組織について、最終メッセージまでの期間が 24 時間未満であった組織は 48 件 (約 38%) であり、短時間でチャット記録が途絶えている割合は決して低くない。情報収集やテスト復号を目的として攻撃者とやり取りするケースもあり、チャットへの参加が身代金交渉や支払いの意思に直結しないことが分かる。

5.3 チャット記録期間とメッセージ数の分布

最初のチャットから最後のチャットまでの経過時間をチャット記録期間として算出し、スレッド単位 (208 件) と被害組織単位 (127 組織) の双方で集計した結果を図 II-5-3 に示す。この期間には交渉そのものに加え、支払い後の復号支援に関するやり取りや、双方が発言しない無応答期間も含まれるため、交渉そのものの長さを表す指標ではない。1 つの被害組織が複数スレッドにまたがって交渉を行っているケースが存在するため、被害組織単位の集計はチャット記録期間の実態により近い単位と考えられる。一方、スレッド単位の集計は、個々の会話がどの程度の期間継続していたかを示す指標として意味を持つ。スレッド単位の中央値は約 12.3 時間 (75 パーセンタイル: 約 120 時間)、被害組織単位では約 67 時間 (同: 約 397 時間) であり、最大値はいずれも約 123 日 (約 2,962 時間) であった。

なお、この集計はデータ終端 (2025-04-29) 時点で打ち切られており、追跡期間が短い被害組織ほどチャット記録期間は短く見積もられる可能性がある (感度分析は付録 A 参照)。

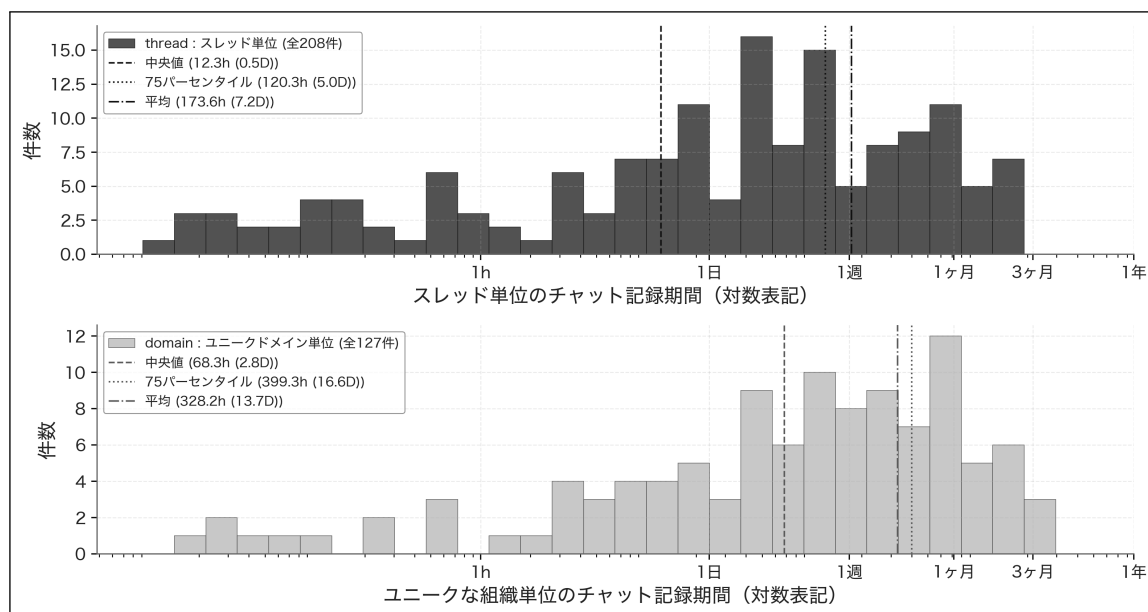


図 II-5-3: チャット記録期間の分布

127 組織単位でのメッセージ数は平均 34.6 件、中央値 10.0 件、75 パーセンタイルは 37.0 件である (図 II-5-4)。

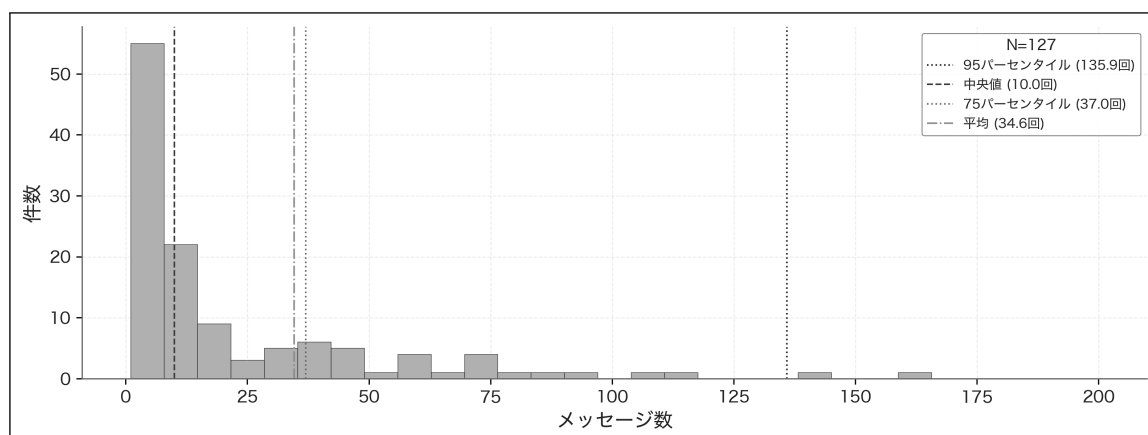


図 II-5-4: チャットメッセージ数の分布 (ユニークドメイン)

チャット記録期間・メッセージ数はいずれも分布の幅が大きく、短期決着と長期化が併存する。社内調整の遅れや復号トラブルによる長期化も見られるため、交渉の進捗に応じた社内承認手順や復号トラブルへの対応手順を事前に整備しておくことが望ましい。

5.4 時間帯・曜日・言語の傾向

chats テーブルに含まれる全 4,423 件のチャットについて、created_at (UTC) を曜日 × 時間帯に変換して件数を集計した (図 II-5-5)。チャットは火曜日から金曜日に集中しており、月曜日・土曜日・日曜日は相対的に活動が少ない。時間帯については UTC 7:00~17:00 に活動が集中する傾向がある。

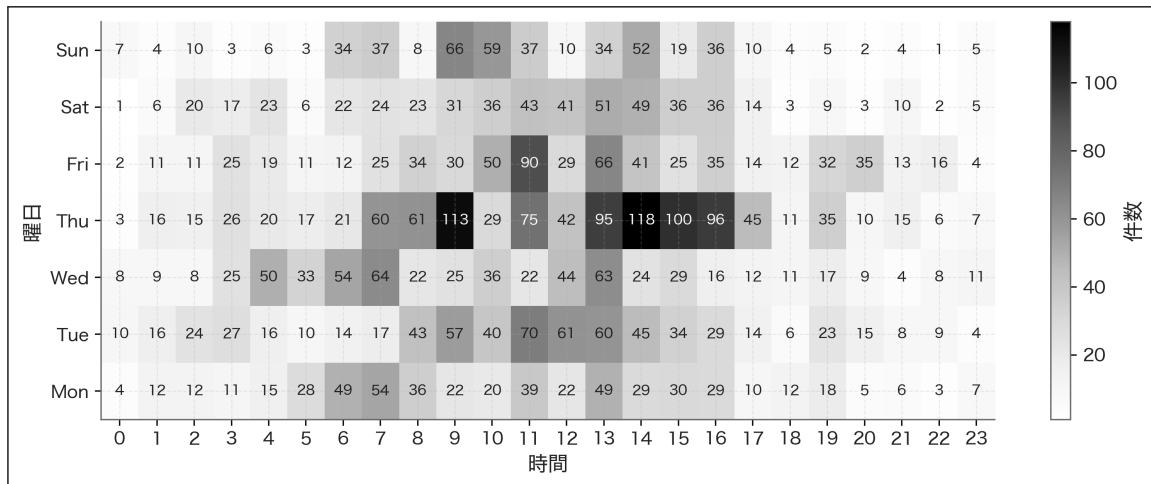


図 II-5-5: チャット活動のヒートマップ (曜日 × 時間帯)

チャット本文に含まれる言語を集計した結果、やり取りは英語が中心であることが分かった。Lite パネル上の被害組織拠点は中国が相対的に多い一方で、被害組織の拠点 (想定言語) に合わせて返信言語を切り替えるような運用は、本データからは見られなかった。図 II-5-6 は chats の全レコードについて message を文字種 (Unicode) で簡易推定し、言語別の件数分布を示したものである。

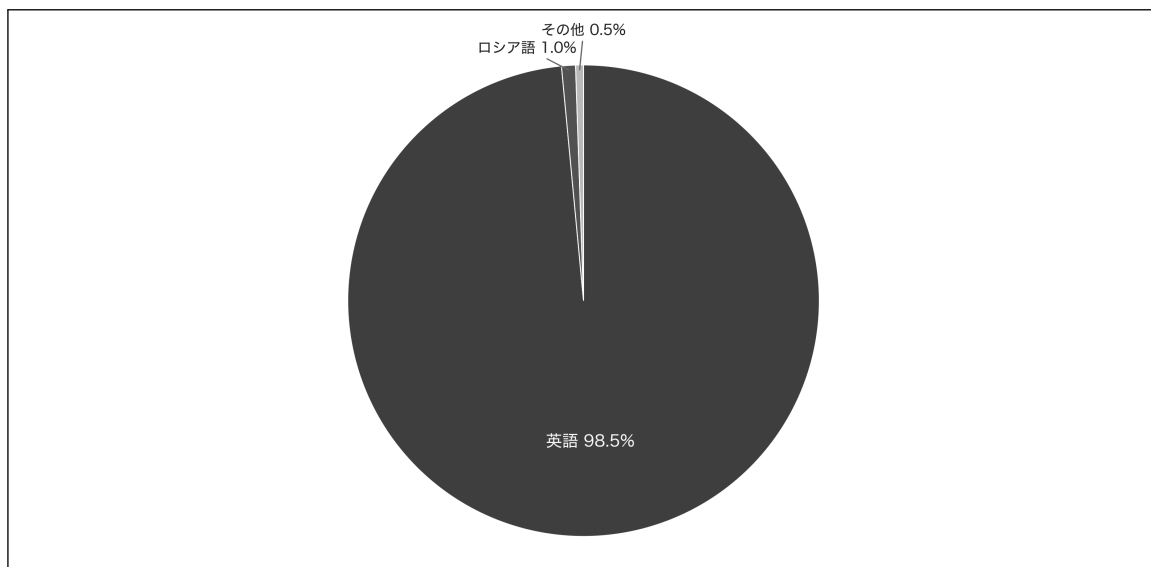


図 II-5-6: チャットの言語分布 (Unicode ベース・簡易推定)

5.5 要求額の提示・減額 (概要)

交渉チャットでは身代金要求から金額交渉、減額に至る一連のやり取りが観測できる。本節では金銭的側面については概要にとどめ、要求額分布・減額率分布の図表は第 6 章 (6.2 節・6.4 節) に集約する。

攻撃者はパネルに被害組織の売上情報を revenue として登録しており、会社規模を調査した上で身代金要求額を決定していたと見られる。

また、多くの交渉チャットで減額交渉が行われていたことも分かった。一部の会話では減額は 50% までの発言もあったが、最大で約 84% の減額に至った取引もあり、アフィリエイトには一定の裁量が与えられ

ていたと見られる。

ただし、過度な値引き要求によって交渉が難航したケースもあった。こうした場面では、アフィリエイトが支払いに難色を示す被害組織を突き放す対応も見られた。

5.6 チャットに見られたパターン

テスト復号

交渉チャットは多くの場合、攻撃者側からテスト復号 (サンプル復号) の手順提示として開始される。被害組織はテスト復号の結果を支払い可否の判断材料の一つとする。一方、復号ツール提供権限を持つと見られる boss の不在を理由にテスト復号対応が遅延するケースもあった。攻撃者側からファイルサイズが小さいことや重要度が低いことを条件として、テスト復号に用いるデータを限定するよう求める例もあった。

テスト復号は意思決定の材料になり得るが、必ず実施されるとは限らず、復旧に必要なデータが返却される保証にもならない。攻撃者が提供するテスト復号には遅延や制限があることを前提とした対応が望ましい。

支払い有無別の訪問回数分布

図 II-5-7・8 は、visits と clients を突合し、支払い判別に訪問回数の分布を比較したものである。支払いを確認・推定できた群では訪問回数が多い傾向が見られ、交渉や復号確認などの手続きが多いことを反映している可能性がある。支払い判定の定義 A (DB フラグ基準) と定義 B (チャット内容からの推定) の 2 系列で可視化しており、いずれも同様の傾向を示している。(定義 A は clients テーブルの paid_commission フラグを基準とするもので、定義 B はチャット内容から支払いの有無を推定したものである。定義 A の 7 件は、定義 B の 17 件に包括される。定義の詳細は付録 A 参照。)

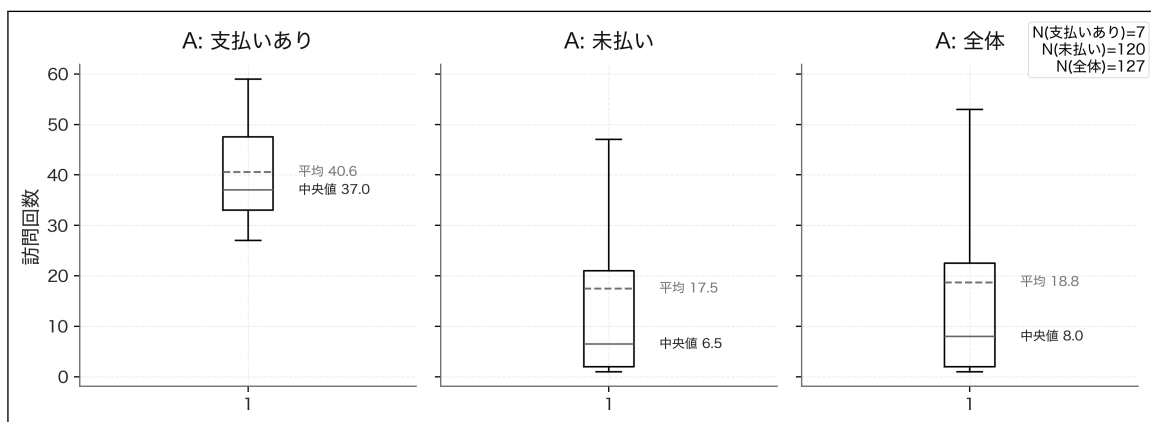


図 II-5-7: 支払い有無別の訪問回数分布 (定義 A : DB フラグ)

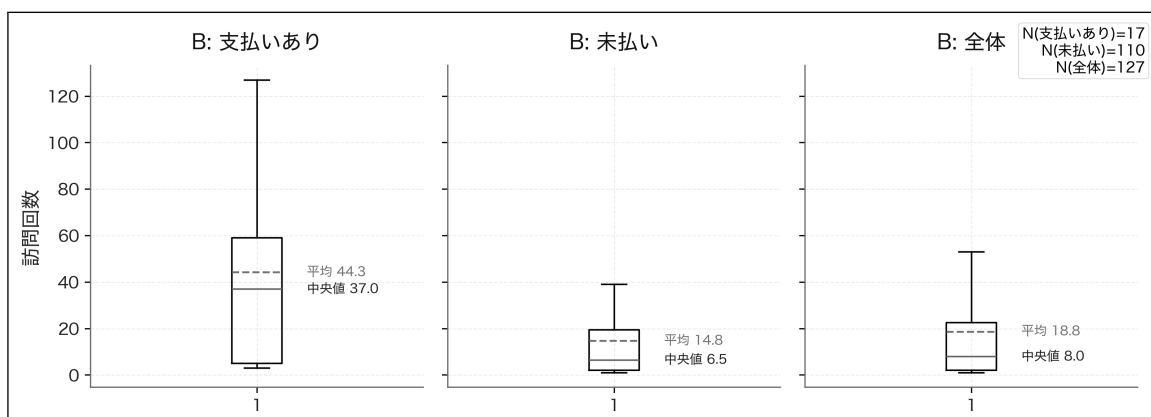


図 II-5-8: 支払い有無別の訪問回数分布 (定義 B : チャット推定)

被害組織の反応パターン

被害組織の反応パターンは、割引交渉型、情報収集型、挑発・感情型、強気姿勢型など多様であった。テスト復号のみ実施し1日でチャットが途絶えたケースも存在する。図 II-5-9～13 にその例を示す。

※チャット記録をもとにイメージ化したもの
(1/2)

被害組織の反応パターン別チャット例 (割引交渉型)

Christopher

原文

hi

日本語訳

やあ

2025-02-05 06:48

原文

40k\$ in bitcoin

日本語訳

ビットコインで4万ドル

2025-02-05 06:48

Christopher

原文

maybe it depends on how quickly you can close discuss

日本語訳

たぶん、あなたがどれだけ早く話し合いを終えられるかにかかっています。

2025-02-05 06:54

原文

10% discount is possible for you

日本語訳

あなたには10%の割引が可能です。

2025-02-05 06:56

原文

hello, A lot of our virtual machines are missing because our controllers are encrypted, so a lot of our virtual machines are not visible

日本語訳

こんにちは。コントローラが暗号化されたため、多くの仮想マシンが見えなくなっており、多数の仮想マシンが見つかりません。

2025-02-08 04:00

Christopher

原文

40k\$ in bitcoin, decrypt all your virtual machines and files

日本語訳

40,000ドル相当のビットコイン。すべての仮想マシンとファイルを復号します

2025-02-08 07:51

Victim

原文

how much for decrypt?

日本語訳

復号の費用はいくらですか？

2025-02-05 06:37

Victim

原文

oh, it is soo high, any discount?

日本語訳

ああ、高すぎます。割引はありませんか？

2025-02-05 06:50

Victim

原文

hello, A lot of our virtual machines are missing because our controllers are encrypted, so a lot of our virtual machines are not visible

日本語訳

こんにちは。コントローラが暗号化されたため、多くの仮想マシンが見えなくなっており、多数の仮想マシンが見つかりません。

2025-02-08 04:00

図 II-5-9: 被害組織の反応パターン別チャット例（割引交渉型・前半、原文抜粋）

47

※チャット記録をもとにイメージ化したもの
(2/2)

被害組織の反応パターン別チャット例 (割引交渉型)

原文
i mean, our controllers are encrypted, so a lot of our virtual machines are not visible
日本語訳
つまり、コントローラーが暗号化されているため、多くの仮想マシンが表示されません。
2025-02-08 08:30

原文
I mean, our system controller is not working, so we can't see the virtual machines, we can't see the files it is managed by the controller, the controller is locked, the files inside esxi are no longer visible
日本語訳
つまり、私たちのシステムコントローラーが動かないため、仮想マシンが見えず、ファイルも見えません。コントローラーで管理されていますが、そのコントローラーがロックされており、ESXi 内のファイルがもう見えません。
2025-02-08 08:32

原文
and you price it is so high, can we talk wiht discount?
日本語訳
それとあなたの提示価格はとても高いです。割引について話せますか？
2025-02-08 08:33

Christopher

原文
i now
日本語訳
知っています
2025-02-08 10:09

Victim

図 II-5-10: 被害組織の反応パターン別チャット例（割引交渉型・後半、原文抜粋）

48

※チャット記録をもとにイメージ化したもの

被害組織の反応パターン別チャット例 (情報収集型)



ZachariasAcosta

原文
Hello

日本語訳
こんにちは

2025-03-24 13:12

原文
Did you take any data? Please generate a list of what was taken

日本語訳
何かデータを持ち出しましたか？持ち出した内容のリストを作成してください。



Victim

2025-03-24 13:20



ZachariasAcosta

原文
<ファイル共有>

日本語訳
<ファイル共有>

2025-03-25 02:19

原文
Here is a part of file tree

日本語訳
ファイルツリーの一部です

2025-03-25 02:20

図 II-5-11: 被害組織の反応パターン別チャット例（情報収集型、原文抜粋）

※チャット記録をもとにイメージ化したもの

被害組織の反応パターン別チャット例 (挑発・感情型)

原文
We waited for a month, and you didn't help us solve the problem, and it was said that the customer damaged the data, and whether the data was damaged or not, can't we see it?

日本語訳
1か月待ちましたが、あなたは問題解決を助けてくれませんでした。顧客がデータを破損したと言われましたが、データが破損しているかどうかは確認できないのですか？



Victim

2025-04-24 09:21

原文
Whenever I receive a customer from you, I will leave a message saying that you are a liar!! Because you don't solve the problem for the customer, you will also close the chat page after payment!!

日本語訳
あなたから客が来るたびに、あなたは嘘つきだとメッセージを残します！なぜなら、あなたは顧客の問題を解決せず、支払い後にチャットページも閉じるからです！！

2025-04-24 09:23

図 II-5-12: 被害組織の反応パターン別チャット例（挑発・感情型、原文抜粋）

被害組織の反応パターン別チャット例 (強気姿勢型)



Swan

原文

If you don't want all this data to become publicly available, then pay the ransom.

日本語訳

このデータを公開されたくないなら、身代金を支払ってください。

2025-04-11 09:03

原文

Sorry guys that must be a misunderstanding because 90% of the topics you are pretending which is containing the gathered data isn't part of the data actually. The ransom is more than 20 times the amount which we had to pay for the work needed to reestablish our hardware functional on reload data. So we can only offer a ransom of max USD 3k because in this case we would be operational quicker. BR, <Masked:Name>

日本語訳

皆さん、すみませんが誤解があるようです。あなた方が主張する収集データの90%は、実際のデータには含まれていません。身代金は、ハードウェアを機能回復しデータを再ロードするための作業費の20倍以上です。ですので、最速の復旧のために最大3,000米ドルしか提示できません。敬具、<Masked:Name>

2025-04-11 16:15



Victim



Swan

原文

Then expect lawsuits from the victims.

日本語訳

では、被害者からの訴訟を覚悟してください。

2025-04-11 17:22

原文

bye bye

日本語訳

さようなら

2025-04-11 17:22

原文

Euer Versuch, mich durch erbärmliche Verschlüsselungstricks und leere Drohungen zum Zahlen zu zwingen, ist gescheitert. Eure Ransomware mag Dateien blockieren, doch Angst verbreitet ihr nicht. Während ihr euch hinter Affiliate-Programmen und anonymen Serverfarmen versteckt, haben internationale Behörden eure Infrastruktur bereits zerschlagen – die Kontrolle über eure Erpresser-Webseiten ist längst verloren. Ihr behauptet, unbesiegt zu sein, doch selbst euer angeblicher «Sprecher» Dmitrij Choroschew steht nun mit einem 10-Millionen-Dollar-Kopfgeld auf der Liste des FBI. Sanktionen machen jede Zahlung an euch zur Straftat, und über 2500 Entschlüsselungsschlüssel liegen bereits in den Händen der Ermittler. Eure «Doppel-Erpressung»? Ein laihes Manöver, das längst durchschaut ist. Statt Lösegeld zu kassieren, werdet ihr bald selbst zahlen – mit eurer Freiheit. Jeder Angriff hinterlässt Spuren, und jedes Opfer, das sich weigert, schwächt eure Macht. Ihr seid keine digitalen Dämonen, nur eine Bande von Dieben, die auf die Verzweiflung anderer angewiesen ist. Meine Daten mögen verschlüsselt sein, doch meine Entschlossenheit ist es nicht. Mit verachtungsvoller Gelassenheit, Die unbeugsame <Masked:Name>

日本語訳

あなたがはじめた暗号化のトリックと空っぽの脅しで私に支払いを強要しようとした試みは失敗した。あなたたちのランサムウェアはファイルを塞ぐかもしれないが、恐怖は広がらない。アフィリエイト・プログラムや匿名のサーバーファームの背後に隠れている間に、国際当局はすでにあなたたちのインフラを粉砕した——恐喝サイトの支配はとうに失われている。自分たちを無敵だと言い張るが、あなたたちのいわゆる「スポークスマン」ドミトリー・ホロシェフでさえ、今やFBIの1000万ドルの賞金首リストに名を連ねている。制裁により、あなたたちへのあらゆる支払いは犯罪となり、2500を超える復号キーはすでに捜査当局の手中にある。あなたたちの「二重恐喝」？とっくに見抜かれた陳腐な手だ。身代金をせしめるどころか、いずれ自分たちが払うことになる——自由という代償を。あらゆる攻撃は痕跡を残し、拒む被害者が一人増えるたび、あなたたちの力は弱まる。あなたたちはデジタルの悪魔などではない。ただ他人の絶望に寄生する盗人の一味だ。私のデータは暗号化されているかもしれない。だが、私の決意は暗号化されていない。軽蔑を込めた静かな確固さをもって。不屈の<Masked:Name>

2025-04-12 06:36



Victim

図 II-5-13: 被害組織の反応パターン別チャット例 (強気姿勢型、原文抜粋)

被害組織の削除要求

交渉チャットには削除要求も見られた。攻撃者側が削除を許諾するメッセージを返していたにもかかわらず、実際にはデータが残存しており、要求後の交渉内容も記録されていた。

※チャット記録をもとにイメージ化したもの

削除要求に関するチャット記録

原文
Can you close these Windows? We don't want our biggest boss to know about these things Or clear the chat messages, this window

日本語訳
このウィンドウを閉じられますか？最上位のボスにこれらのことを知られたくありません。またはチャットメッセージを消してください、このウィンドウを

2025-02-18 02:50

Victim

Christopher

原文
ok

日本語訳
わかりました

2025-02-18 02:55

原文
clearn

日本語訳
消してください

2025-02-18 02:59

Victim

原文
i aready pay you, pls clearn this chat rom or close

日本語訳
すでに支払いました、このチャットルームを消すか閉じてください

2025-02-18 03:00

原文
or close this rom let him cant Can not log in

日本語訳
またはこのルームを閉じて、彼がログインできないようにしてください

2025-02-18 03:05

Christopher

原文
ok ok wait

日本語訳
わかりました、わかりました、待ってください

2025-02-18 03:06

図 II-5-14: 削除要求に関するチャット例（原文抜粋）

5.7 攻撃者の交渉術

チャット記録には、攻撃者が用いる複数の交渉術が見られる。LockBit のブランド知名度を強調する手法、被害組織の売上等の公開情報を根拠に支払い能力を主張する手法、サイバー保険の加入を根拠とする手法などである。

時間的圧力をかける手法も多く見られ、「48 時間以内なら割引」「今決断すれば半額」といった提示で即決を迫るケースが存在する。ただし、これらの傾向はあくまで今回の流出データにおける観察結果であり、全ての交渉において同様の傾向が見られるという保証はない。

図 II-5-15～21 にその例を示す。

※チャット記録をもとにイメージ化したもの
(1/2)

期限や割引を提示して早期決断を迫るチャット例 1



PiotrBond

原文

The only thing we can do is give you a discount on condition that payment is made within three days.

日本語訳

できることは、3日以内にお支払いいただくことを条件に割引を提供することだけです。

2025-04-15 05:03

原文

Also, can we discuss the price and determine the minimum cost that can be offered

日本語訳

また、価格について協議し、提示可能な最低金額を決められますか

2025-04-14 23:06

Victim

原文

offer from client. they won't pay, if amount is over \$10000. consider it and reply. thank you.

日本語訳

クライアントからの提示です。金額が10,000ドルを超えると支払わないとのことです。検討して返信してください。ありがとうございます。

2025-04-15 09:00



PiotrBond

原文

Do they want to get their servers with information back?

日本語訳

相手は、情報が入ったサーバーを取り戻したいのですか？

2025-04-15 09:05

原文

yes. but the value of data isn't over \$10000

日本語訳

はい。ただし、データの価値は10,000ドルを超えません。

2025-04-15 09:27

Victim



PiotrBond

原文

We will wait for a better offer from you.

日本語訳

こちらとしては、あなたからより良い提案を待ちます

2025-04-15 11:37

原文

It's impossible. The client doesn't have that much budget, at most only \$10000

日本語訳

それは不可能です。クライアントにはそこまでの予算がなく、多くても10,000ドルしかありません

2025-04-17 01:08

Victim

原文

You want too much, it's not a big deal

日本語訳

要求が高すぎます。大したことではありません

2025-04-17 01:09

図 II-5-15: 期限や割引を提示して早期決断を迫るチャット例 1（前半、原文抜粋）

52

※チャット記録をもとにイメージ化したもの
(2/2)

期限や割引を提示して早期決断を迫るチャット例 1



PiotrBond

原文

We will meet you halfway and we can close this issue for \$17,000

日本語訳

こちらが歩み寄って、この件を17,000ドルでクローズできます。

2025-04-17 05:28

原文

It's not that we don't want to talk, it's that the Chinese police don't allow them to do this. They have to spend their own money to do this, and in a sense it is also subject to government supervision. The customers really don't have that much money. Do you think 10,000 US dollars is okay? We will communicate and the deal will be done quickly.

日本語訳

話し合いたくないわけではありません。中国の警察が彼らにこれを許可していないのです。彼らは自分たちのお金を使ってこれを行わなければならない、ある意味で政府の監督対象にもなります。顧客には本当にそれほどのお金がありません。10,000米ドルでよいと思いますか？こちらで連絡を取り、取引はすぐに成立します。

2025-04-18 02:57



Victim



PiotrBond

原文

If you pay fast, 12000\$ and we close this issue

日本語訳

早く支払うなら、12,000ドルでこの件をクローズします。

2025-04-18 04:45

図 II-5-16: 期限や割引を提示して早期決断を迫るチャット例 1（後半、原文抜粋）

※チャット記録をもとにイメージ化したもの

期限や割引を提示して早期決断を迫るチャット例 2



affiliate900

原文

We accept bitcoins. €90k if you make payment within 48 hours, after that the price is €130k. This includes 1) decryptor; 2) deletion of stolen data; 3) security suggestions to prevent this from ever happening again; 4) Guarantee to never be attacked again

日本語訳

ビットコインで受け付けます。48時間以内の支払いなら9万ユーロ、その後は13万ユーロです。これには1) 復号ツール 2) 盗まれたデータの削除 3) 再発防止のためのセキュリティ提案 4) 二度と攻撃しない保証が含まれます。

2025-04-28 13:58

原文

maybe you didn't understand: we are a small company and we don't have all that money. we can pay 500/1000 euros, certainly not 90000 euros

日本語訳

あなたは理解していないかもしれませんが、私たちは小さな会社で、そんなお金はありません。500～1000ユーロなら支払えますが、9万ユーロは無理です。

2025-04-28 14:02



Victim

図 II-5-17: 期限や割引を提示して早期決断を迫るチャット例 2（原文抜粋）

53

※チャット記録をもとにイメージ化したもの

期限や割引を提示して早期決断を迫るチャット例 3

PiotrBond

原文
Can

日本語訳
できます。

2025-03-05 16:48

原文
If you pay fast we give discount

日本語訳
早く支払えば割引します

2025-03-05 16:49

Victim

原文
can you give a discount?

日本語訳
割引は可能ですか？

2025-03-05 12:33

図 II-5-18: 期限や割引を提示して早期決断を迫るチャット例 3（原文抜粋）

※チャット記録をもとにイメージ化したもの

被害組織が加入している保険情報に基づいて金銭を要求するチャット例

BaleyBeach

原文
Your insurance covers 5MM. We ask 4MM with discount.

日本語訳
あなた方の保険は500万をカバーしています。割引で400万を要求しています。

2025-04-17 12:43

原文
We're already down 20% from the price listed on the insurance. We are not charity. 9 days left for discount, use your time wisely.

日本語訳
保険に記載された価格から既に20%割引しています。私たちは慈善事業ではありません。割引の期限まで残り9日です。時間を賢く使ってください。

2025-04-18 08:07

Victim

原文
Taking information to my team.

日本語訳
チームに情報を持っていきます。

2025-04-16 05:49

原文
Your final price does not allow much flexibility. We find this amount very difficult to meet.

日本語訳
最終価格では柔軟性がほとんどありません。この金額を満たすのは非常に困難です。

2025-04-17 09:39

図 II-5-19: 保険情報等に言及して金銭を要求するチャット例（原文抜粋）

※チャット記録をもとにイメージ化したもの

自分たちの評判を検索するように促すチャット例

原文

Good day, may we negotiate the amount you have in mind and what in turn would be Lockbit's end of the bargain.

日本語訳

ごきげんよう。あなたが考えている金額について交渉し、見返りにLockBitが何をするのか話し合えますか。

2025-02-11 14:47

Victim

Christopher

原文

120k\$ in bitcoin

日本語訳

12万ドル相当のビットコイン

2025-02-11 15:08

原文

After payment, 100% of your files will be securely deleted and our team won't bother you again. You can trust us by reading about us on the global internet. We value our reputation

日本語訳

支払い後、あなたのファイルは100%安全に削除され、当チームは二度と連絡しません。私たちについてはインターネット上で調べることができます。私たちは評判を大切にしています。

2025-02-11 15:13

図 II-5-20: 評判を検索するよう促すチャット例（原文抜粋）

55



図 II-5-21: 過去の攻撃実績を根拠に支払いを強要するチャット例（原文抜粋）

こうした実例は、有事における冷静な判断のための訓練素材として活用できる。攻撃者の交渉術に感情的に反応せず、想定パターンに沿った対応を取れるよう平時から準備しておくことが望ましい。

5.8 交渉代理人が関与したケース

チャット分析から、明確に交渉代理人（ネゴシエーター）の存在が示されたケースは9件確認できた。表II-5-1は、代理人関与が判定できたスレッドを chats の本文から抽出し、要求額・最終提示額・減額率等を一覧化したものである（交渉の中断等で最終提示額が確認できなかったケースも含む）。交渉代理人によって最大で約84%の減額に至った事例がある一方、代理人が LockBit に対し強い態度を示した結果、やり取りが口論となったケースも見られた。このような場合には、減額交渉、被害範囲の確認、テスト復号など、実質的な協議に支障が生じるため、交渉代理人の関与が必ずしも交渉を有利に進めるとは限らないことが分かる。

表 II-5-1：交渉代理人関与ケースの概要 (9 件)

No	初回要求額	最終提示額	取引成立	減額率	国	業種
1	50,000	－	－	－	ウルグアイ	情報通信
2	294,021	143,933	－	51%	中国	運輸
3	4,840	4,391	○	9%	不明	不明
4	15,000	6,000	○	60%	中国	卸売・小売
5	132,000	－	－	－	中国	製造
6	8,000	－	－	－	不明	不明
7	18,000	－	－	－	不明	不明
8	63,440	10,000	○	84%	不明	不明
9	50,000	－	－	－	中国	地方行政機関

※「取引成立」列の「○」は支払い等による取引成立をチャット上で確認できたことを示す。「－」は成立が確認できなかったことを示し、不成立と断定するものではない(交渉の中断等により最終的な帰結が追えないケースを含む)。

図 II-5-22～25 にその例を示す。

※チャット記録をもとにイメージ化したもの

交渉代理人関与時のチャット例 1

RiccardoBond

原文

I don't know what you are doing. Three people with one ID asked. I have said it many times, but you still don't pay the discount price. Then please pay 0.05BTC. There will be no more discount. You can choose to give up the data.

日本語訳

あなたが何をしているのかわかりません。1つのIDで3人が尋ねました。何度も言いましたが、あなたはまだ割引価格を支払いません。では0.05BTCを支払ってください。これ以上の割引はありません。データを諦めることを選ぶことができます。

2025-02-15 05:10

原文

Customers won't buy BTC, so time is wasted, bro

日本語訳

顧客はBTCを買わないので、時間の無駄なんだ、兄弟。

2025-02-15 05:48

Victim

原文

sorry

日本語訳

ごめんなさい

2025-02-15 05:52

RiccardoBond

原文

Not just your customers

日本語訳

あなた方の顧客だけではなく。

2025-02-15 06:10

原文

sorry, 0.04 pay, bro

日本語訳

すみません、0.04払います、兄弟。

2025-02-15 06:23

Victim

図 II-5-22: 交渉代理人関与時のチャット例 1 (原文抜粋)

交渉代理人関与時のチャット例 2

原文

There is a problem with your decryption program, I paid many times some time ago, and there was basically a problem, and it didn't solve the problem for us, and just closed the page! I don't know where your credibility is for such a high price?????

日本語訳

あなた方の復号プログラムに問題があります。少し前に何度も支払いましたが、基本的に問題があり、私たちの問題は解決せず、ページを閉じただけです！その高い価格に見合う信頼性がどこにあるのかわかりません?????

2025-04-24 09:15



Victim



lofikdis

原文

There are many people in the affiliate program, and we are not sure. Some novice players may execute multiple encryption strategies at the same time. They always execute automatic programs in batches. We are the attackers who catch whales. You can fully believe that our programs are all executed by professional hackers.

日本語訳

アフィリエイトプログラムには多くの人が参加しており、私たちにも確信はありません。初心者は複数の暗号化戦略を同時に実行することがあります。彼らは常に自動プログラムを一括で実行します。私たちは大物を狙う攻撃者です。私たちのプログラムはすべてプロのハッカーが実行していると完全に信じて構いません。

2025-04-24 09:17

原文

After the payment, not only did it not solve the problem, but the communication page was closed!! That's how you deal with it!

日本語訳

支払い後も問題は解決せず、連絡ページまで閉じられました。そういう対応なのですか。

2025-04-24 09:18



Victim



lofikdis

原文

This has nothing to do with us, you can contact the boss directly in the alliance. Our team are all mature professional level hackers.

日本語訳

これは私たちとは関係ありません。アライアンス内のボスに直接連絡できます。私たちのチームは全員、成熟したプロレベルのハッカーです。

2025-04-24 09:19

原文

There are many or even hundreds of affiliates in the affiliate program. What are you talking to us about? We are communicating with this client.

日本語訳

アフィリエイトプログラムには多数、場合によっては何百ものアフィリエイトがいます。私たちに何の話をしているのですか？私たちはこの顧客とやり取りしています。

2025-04-24 09:20

原文

We waited for a month, and you didn't help us solve the problem, and it was said that the customer damaged the data, and whether the data was damaged or not, can't we see it?

日本語訳

1か月待ちましたが、あなたは問題解決を助けてくれませんでした。顧客がデータを破損したと言われましたが、データが破損しているかどうかは確認できないのですか？

2025-04-24 09:21



Victim

図 II-5-23: 交渉代理人関与時のチャット例 2 (原文抜粋)



図 II-5-24: 交渉代理人関与時のチャット例 3（原文抜粋）

やり取りの中で被害組織側が交渉代理人の関与を示し、攻撃者側がそれに反応する場面が見られる。代理人の介入は交渉を有利にする可能性がある一方、攻撃者側の態度硬化など別のリスク要因にもなり得る。これまでも、ランサムウェア攻撃グループが交渉代理人サービスに対し牽制と見られる声明を発した事例が存在する。例えば Everest は 2026 年 1 月、特定の交渉サービスについて被害組織側の評判を損なう旨をリークサイト上で示唆している。

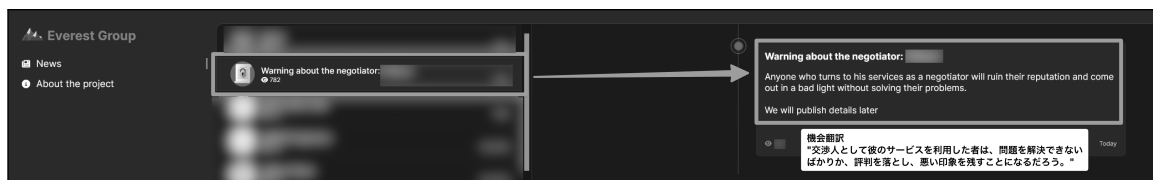


図 II-5-25: Everest のリークサイトに掲載された交渉代理人サービスについての声明

※ 本画像は CIG が取得したスクリーンショット

交渉代理人を利用して減額交渉を有利に進められる可能性もある一方で、攻撃者側が「プロの介入」を牽制する場合もある。交渉代理人を起用するか否かの方針を平時に定め、起用する場合でも、最終判断における責任の所在を明確化しておくことが望ましい。

5.9 その他特徴的な会話

本節では、5.8 節までに含まれないその他の特徴的な会話の例を示す。

制裁対象国に所在しているため金融サービスを利用できず、身代金の支払い手段がないと主張する被害組織が見られた (図 II-5-26)。Bitcoin の購入方法について解説を求める組織がある一方、LockBit 自体が制裁対象であるため金融サービス経由の送金ができないと主張する組織もあった (図 II-5-30)。

また、他国への不満や金銭的な関心から、LockBit への参加に興味を示す被害組織側の担当者も複数見られた (図 II-5-27・28)。こうした発言は、被害組織の従業員が将来的に内部犯行に転じるリスクを示唆するものとして注目に値する。

さらに、自組織への攻撃を回避する目的と見られるやり取りの中で、無関係な第三者企業を攻撃対象として持ちかける発言も見られた(図 II-5-29)。被害対応の窓口担当者が交渉の過程でこうした発言に至る可能性があることは、対応体制や倫理面でのガイドライン整備の必要性を示している。

以下の図 II-5-26～30 に、それらの例を示す。

※チャット記録をもとにイメージ化したもの

その他の特徴的な会話例1

原文

Hello,I am writing to you from Iran. Please believe me when I say I am not a wealthy person or part of any rich organization. I don't have access to international banking systems, and because of global sanctions, I can't even buy Bitcoin legally in my country.The amount you're asking is far beyond anything I could ever afford. Our currency has lost almost all its value — people here are struggling just to survive. Paying 5 BTC per server is not just difficult, it's completely impossible for me. Even saving 0.1 BTC would take years here.This situation has destroyed everything I've worked for. I am desperate and broken. Please understand that I'm not your enemy — I'm just a small person in a very hard place, trying to find a way forward.If there is any way you could help, or reduce the amount, or show any mercy, I would be deeply grateful. I am willing to cooperate or discuss any possible solution that is humanly possible for me.Thank you for reading. I truly hope you will show some mercy.

日本語訳

こんにちは。イランから書いています。私は裕福な人間でも、裕福な組織の一員でもありません。国際的な銀行システムにはアクセスできず、世界的な制裁のため、国内では合法的にビットコインを購入することさえできません。あなたが要求する金額は、私には到底支払えない額です。私たちの通貨はほとんど価値を失い、人々は生き延びるだけで精一杯です。サーバー1台あたり5 BTCの支払いは困難どころか、完全に不可能です。0.1 BTCを貯めるだけでも何年もかかります。この状況は、私が積み上げてきたすべてを壊してしまいました。私は必死で、打ちひしがれています。私はあなたの敵ではありません。ただ、とても厳しい状況にいる小さな人間が、前に進む方法を探しているだけです。もし助けていただけるなら、あるいは金額を下げていただけるなら、どんな慈悲でも深く感謝します。現実的に可能なあらゆる解決策について協力し、話し合う用意があります。読んでいただきありがとうございます。どうか慈悲を示してくださいを心から願っています。

2025-04-11 20:01

原文

We can give you a discount, but you will have to find the money, otherwise we will not reach an agreement.

日本語訳

割引を提供できますが、あなたはお金を見つける必要があります。そうでなければ合意に達することはできません。

2025-04-12 19:30

原文

I want to be completely honest with you: I don't have access to any international banking systems. I don't have a foreign account, and I can't legally buy cryptocurrency like Bitcoin in my country. I live in Iran, and we are under heavy sanctions. Our currency — the Toman — has lost almost all its value. Even earning just a small amount of BTC is a nearly impossible task here.I'm not a business owner with income in dollars or euros. I'm just an individual who has lost everything — 20 servers gone. What you're asking for is simply beyond my means, even with a discount. If there was a way to pay in Toman, I could try to gather something, but I know it may not be useful to you.Please, I am desperate. I'm not trying to avoid responsibility — I just need a chance to recover even part of what I've lost. If you can reduce the amount to something that someone like me could possibly afford, I will do everything I can to make it happen.This is my last hope. I'm asking not as a company or target — just as a human being.

日本語訳

正直にお伝えします。私は国際的な銀行システムに一切アクセスできません。海外口座もなく、私の国ではビットコインのような暗号通貨を合法的に購入できません。私はイランに住んでおり、厳しい制裁下にあります。私たちの通貨であるトマンは価値をほとんど失いました。ここでは少額のBTCを得ることさえほぼ不可能です。私はドルやユーロで収入のある事業主ではありません。私はすべてを失った一個人にすぎません。サーバー20台が消えました。あなたが求めている金額は、割引があっても私の手には負えません。もしトマンで支払える方法があれば何とか集めようとしませんが、あなたにとって役に立たないことは理解しています。どうかお願いします。責任を回避するつもりはありません。失ったものの一部でも取り戻すためのチャンスが必要なだけです。私のような人でも負担できる額に減額していただけるなら、実現のためにできる限りのことをします。これが最後の望みです。企業や標的としてではなく、一人の人間としてお願いしています。

2025-04-14 05:29

原文

Then I won't be able to help you in any way.

日本語訳

それでは、私は何の助けもできません。

2025-04-14 18:33

図 II-5-26: その他の特徴的な会話例 1 (原文抜粋)

60

※チャット記録をもとにイメージ化したもの

その他の特徴的な会話例2

PiotrBond

原文
What are you asking about?

日本語訳
何について尋ねているのですか？

2025-04-04 04:53

原文
这个行业挺好 怎么加入你们？

日本語訳
この業界はなかなか良いですね。どのようにあなた方に参加できますか。

2025-04-04 02:46

Victim

PiotrBond

原文
You can download decryption tool here

日本語訳
こちらから復号ツールをダウンロードできます。

2025-04-04 11:12

原文
我意思是想做你们这个行业是否机会？

日本語訳
私の意味は、あなたたちのこの業界をやることに機会があるかということです？

2025-04-04 05:59

Victim

図 II-5-27: その他の特徴的な会話例 2（原文抜粋）

※チャット記録をもとにイメージ化したもの

その他の特徴的な会話例3

Christopher

原文
we now have open registration in the panel lockbit, but it costs 777\$.

日本語訳
現在、LockBitパネルのオープン登録が可能です、料金は777ドルです。

2025-02-08 13:36

原文
Bro, I want to ask for your advice. If I want to make some extra money on the side but do it safely like you guys, do you have any recommended directions?

日本語訳
相談したいです。副業であなた方のように安全に稼ぐには、どんな方向性がおすすですか？

2025-02-08 09:40

Victim

Christopher

原文
After joining, what can I help with? I don't have any particular skills. If possible, can I join?

日本語訳
参加後、私は何を手伝えますか？特別なスキルはありません。もし可能なら、参加できますか？

2025-02-08 14:33

原文
After joining, what can I help with? I don't have any particular skills. If possible, can I join?

日本語訳
参加後、私は何を手伝えますか？特別なスキルはありません。もし可能なら、参加できますか？

2025-02-08 14:33

Victim

図 II-5-28: その他の特徴的な会話例 3（原文抜粋）

※チャット記録をもとにイメージ化したもの

その他の特徴的な会話例4

原文

If I provide the IP of a mainland Chinese company, can you attack it?

日本語訳

中国本土の企業のIPを提供したら、攻撃できますか？

2025-02-07 01:59

Christopher

原文

we do more china, we have enough companies)

日本語訳

私たちは中国をもっと攻撃しています、十分な企業があります)

2025-02-07 02:03

原文

what china company ?

日本語訳

どの中国企業ですか？

2025-02-07 02:05

Victim

原文

But you must say China is shit!!!!!!

日本語訳

でも、中国はクソだって言わなきゃ！！！！！！

2025-02-07 02:08

原文

It is a publicly listed Chinese company. What information do I need to provide you?

日本語訳

上場している中国企業です。どんな情報を提供すればいいですか？

2025-02-07 02:09

Christopher

原文

we love working with China, they pay well)

日本語訳

私たちは中国との仕事が大好きです、彼らはよく払ってくれます)

2025-02-07 02:11

原文

need site

日本語訳

サイトが必要です

2025-02-07 02:12

図 II-5-29: その他の特徴的な会話例 4 (原文抜粋)

62

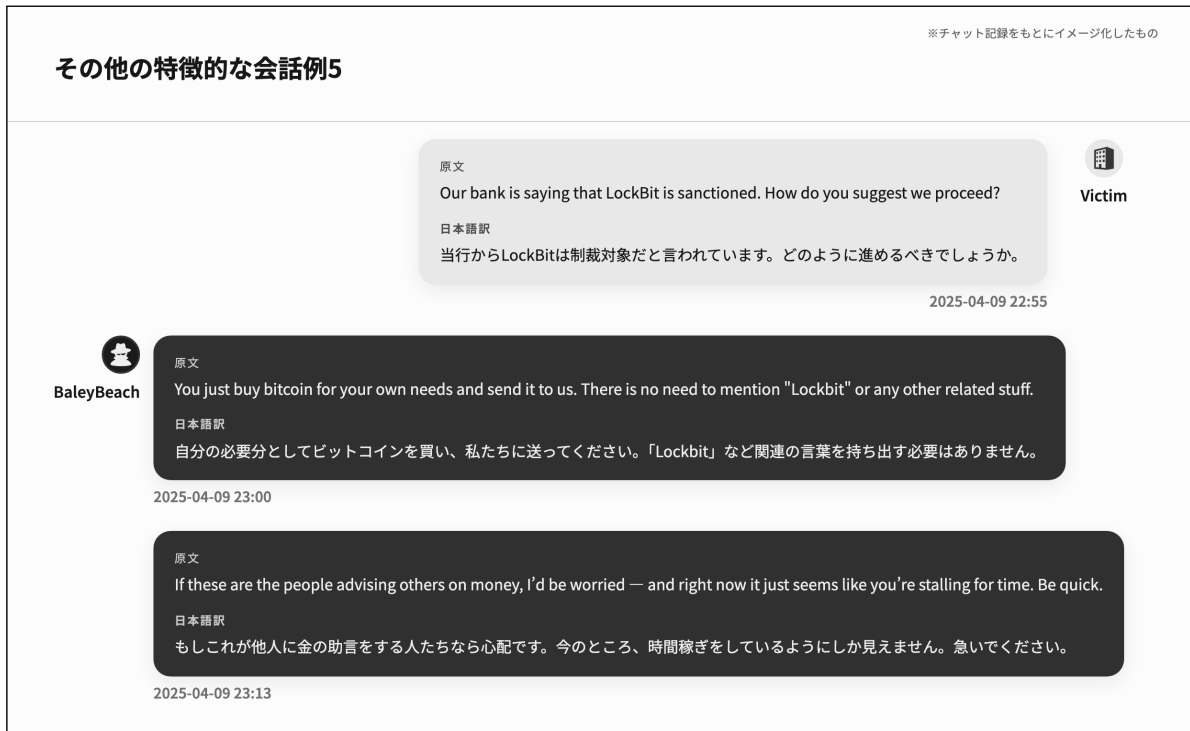


図 II-5-30: その他の特徴的な会話例 5（原文抜粋）

5.10 本章のまとめ

本章では、Lite パネルに記録された交渉チャットを分析し、身代金交渉の実態を整理した。主要な知見を以下に示す。

1. 交渉参加≠支払い意思

clients に登録された 246 件のうち、ダッシュボードへのアクセス記録があるものは 239 件 (97%) であった。一方、重複やテストデータを除いたユニークドメイン単位の 127 組織では、最終メッセージまでの期間が 24 時間未満だった組織が 48 件 (約 38%) であった。最終的な支払いは 7 件 (DB フラグ基準)~17 件 (チャット推定基準) にとどまり、交渉への参加が支払いに直結しないことが分かった。

2. チャット記録期間の大きなばらつき

スレッド単位の中央値は約 12 時間、被害組織単位では約 67 時間であり、最大では約 123 日に及ぶケースもある。短期決着と長期化の両方を想定した体制設計が推奨される。

3. テンプレ化された初回接触

交渉は定型的な初回メッセージで開始され、テスト復号の手順提示など一定のパターンに沿って進行する。

4. 時間的プレッシャーの活用

「48 時間以内なら割引」といった期限提示や、売上・保険情報を根拠にした要求など、複数の交渉術が見られた。

5. 交渉代理人の関与

9 件で交渉代理人の介入があり、最大で約 84% の減額に至った事例がある一方、代理人が攻撃者に対して高圧的な態度を取ることで、攻撃者側の態度が硬化するケースも見られた。

6. 金銭フェーズ：要求額・合意額・支払い

本章では、`chats`・`clients`・`builds`・`btc_addresses`・`invites` およびリークサイト掲載データ (CIG による観測) を用いて、身代金の要求から支払いに至るフェーズを分析する。要求額の傾向や交渉による減額の実態、支払いに至ったケースの帰結、および支払いが復号と掲載状況に与える影響を整理する。分析上の制約は付録 A にまとめた。

6.1 資金インフラ

`btc_addresses` テーブルには 59,975 件のビットコインアドレスが登録されている。このうち被害組織に割り当て済みなのは 159 件 (0.3%未満) に過ぎない。大量のアドレスをプールとして保持し、必要に応じて割り当てる運用と見られる。

各アドレスはアフィリエイトに分配されており、担当する被害組織数が多い場合にはアドレス割り当て数も多くなるという相関が見られる。一部のアドレスは `admin` とアフィリエイトの両方に割り当てられており、収益分配の構造がうかがえる。

図 II-6-1 はアフィリエイトごとの割り当て済みアドレス数を集計したものである。

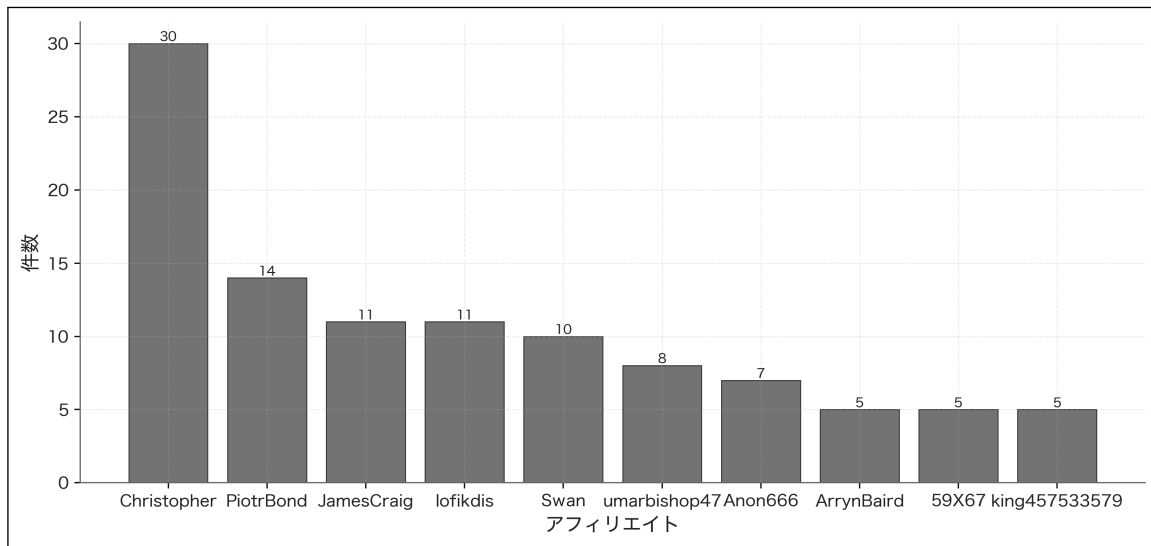


図 II-6-1: アフィリエイトごとの BTC アドレス割り当て数

なお、この `btc_addresses` テーブルに存在せずチャットにのみ出現する BTC アドレスも見られた。プール外のアドレスが使用されていることから、アドレス管理においてもアフィリエイトに裁量が認められていた可能性がある。

`invites` には BTC ウォレット 2,338 件と Monero ウォレット 1,355 件が記録される。BTC 側 (`invites.btc_wallet`) は全件ユニークで `btc_addresses` と重複しない。XMR 側 (`invites.monero_wallet`) も全件ユニークである。

6.2 要求額の分布と傾向

チャットを被害組織 (正規化ドメイン) 単位で集計した結果、要求額の中央値は約 50,000 USD、75 パーセンタイルは約 115,000 USD、平均値は約 208,000 USD であった。90 パーセンタイルは約 400,000 USD であり、高額側に長い裾を持つ分布であった。要求額には大きなばらつきがあることが分かった。なお、この集計では精査対象 127 ドメインのうち身代金要求の実態を反映していない 1 件を除外している (詳細は付録 A 参照)。

本節における要求額は初回要求額 (同一組織内で最初に観測された要求額) を指す。減額交渉が行われたケースについては、初回要求額と最終要求額を用いて減額率を算出した。減額率は初回要求額に対して最終要求額がどの程度下がったかを割合で表したものであり、支払い成立の可否とは別である。金額抽出・採用

ルールの詳細は付録 C を参照されたい。

図 II-6-2 は初回要求額 (USD) の分布を被害組織単位で対数スケールにより示したものである。

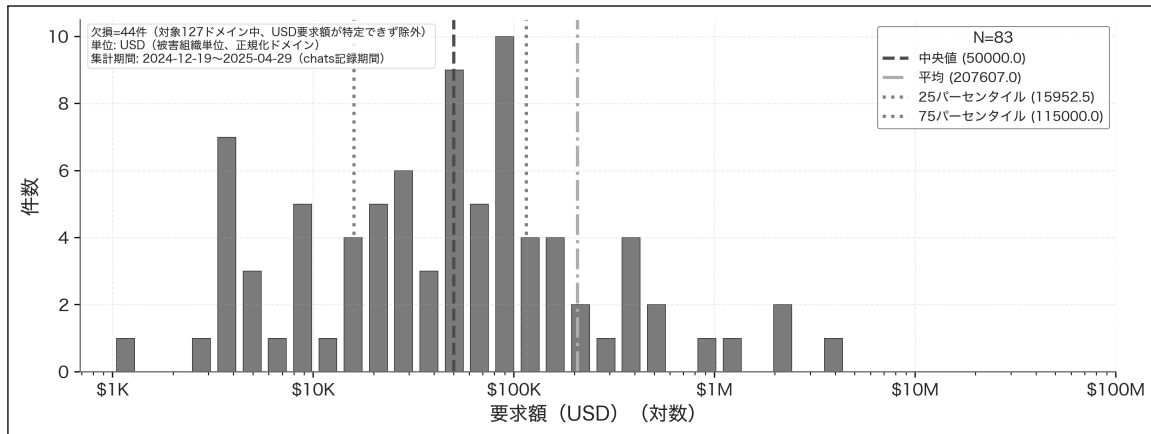


図 II-6-2: 身代金要求額の分布 (対数スケール)

減額率は初回要求額と最終要求額の双方が確認できた被害組織 28 件 (支払い成立・未成立を問わない) を対象に算出した。中央値は約 39%、四分位範囲 (25~75 パーセンタイル) は約 12%~60%であり、ケース間のばらつきが大きく、最小 0%から最大約 84%の減額に至った例まで見られた。平均では約 37%の減額であった。図 II-6-3 はこの 28 件について減額率を集計したものである。

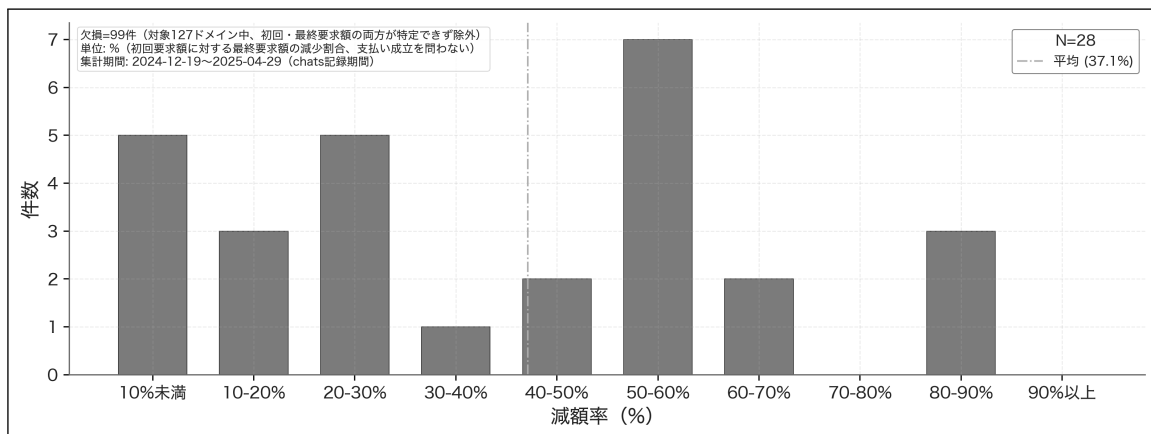


図 II-6-3: 減額率の分布

6.3 売上金額と要求額の関係

builds テーブルには builds.revenue フィールドが存在し、ターゲット企業の推定売上 (攻撃者側の推定・入力値) が記録されている。最も多い設定値は 5kk (500 万 USD) であった。builds.revenue は攻撃者側の入力値であり、正確ではない可能性がある。この正確性が保証されない前提で、revenue カテゴリ別の要求額分布を確認した。builds.revenue と要求額に明確な比例関係は見られず、要求額の決定要因は一次データからは特定できない。

図 II-6-4 は builds.revenue のカテゴリ別に要求額 (USD) の分布を示したものである。要求額は chats から抽出し、被害組織 (正規化ドメイン) 単位で集計している。

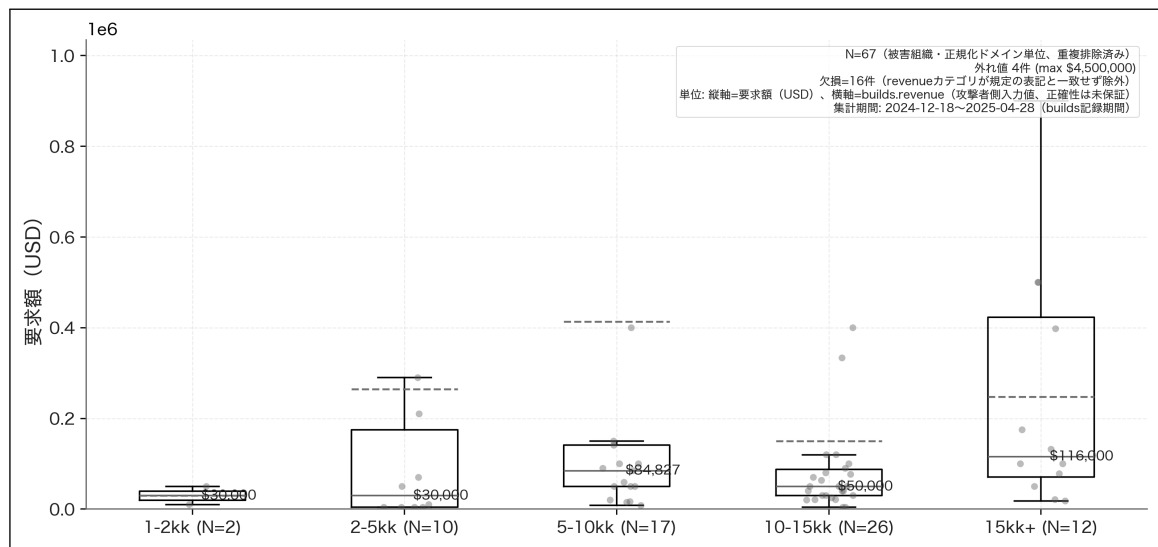


図 II-6-4: revenue フィールド別の身代金要求額分布

要求額の決定要因は一次データからは特定できないが、攻撃者が売上等の公開情報を参照している様子も見られる。図 II-6-5~8 にその例を示す。

要求額決定に関するチャット例 1 : 財務情報をもとした要求額決定


Swan

原文

Please send more files for testing, the corrupted ones are excluded

日本語訳

テスト用にさらにファイルを送ってください。破損しているものは対象外です

2025-04-20 10:24

原文

We will do, its not so easy to find small files how much is the ransom, we would please like to know

日本語訳

やります。ただ、小さいファイルを見つけるのは簡単ではありません。いくらが身代金ですか、教えてください。

2025-04-20 10:25


Victim


Swan

原文

At the moment, our team of lawyers is studying your financial documentation, today we are not ready to name the price for you.

日本語訳

現時点では、当社の弁護士チームがあなたの財務書類を検討しています。本日は価格を提示できません。

2025-04-20 11:21

原文

good morning do you have an update for us?

日本語訳

おはようございます。何か更新はありますか？

2025-04-22 06:12


Victim


Swan

原文

wait

日本語訳

待つて

2025-04-22 09:30

原文

2kk usd

日本語訳

200万USD

2025-04-22 11:17

図 II-6-5: 要求額決定に関するチャット例 1 (財務情報をもとにした要求額決定、原文抜粋)

要求額決定に関するチャット例2：被害組織の売上額を把握しているという主張



Christopher

原文

I know your company revenue, and your system is not cheap, so 70k is not a lot of money for you and the price will not be lower

日本語訳

あなたの会社の売上は把握していますし、システムも安くはありません。だから7万はあなたにとって大金ではなく、値下げはしません。

2025-04-24 11:14

原文

Brother, as a staff member, if I want to solve the problem, the money is not paid by me. But I show my boss that I can indeed do something for the company. Just as I said before, but you don't believe me. Your encryption is indeed not completed, and we haven't. We have indeed fixed a lot, but some that can't be fixed want to be decrypted. Could it be cheaper? A small request

日本語訳

兄弟、従業員として問題を解決したくても、お金は私の持ち出しではありません。ただ、会社のために自分ができることを上司に示したいのです。前にも言いましたが、あなたは信じてくれません。あなたの方の暗号化は確かに完了しておらず、こちらも多くを修復しましたが、直せないものは復号したいのです。もう少し安くできませんか。ささやかなお願いです。

2025-04-24 11:18

原文

You have also seen before that some of the samples we provided did have problems after decryption. I didn't lie, nor was it necessary

日本語訳

こちらが提供したサンプルの中に、復号後に問題があったものがあったのは、あなたも以前に見ています。私は嘘をついていませんし、その必要もありません。

2025-04-24 11:19



Christopher

原文

You can write as much as you want, but it won't change the price

日本語訳

いくらでも書いて構いませんが、価格は変わりません。

2025-04-24 11:20

原文

boss approved, said 70k or nothing

日本語訳

ボスの承認済みです。70kでなければなし、とのこと。

2025-04-24 11:21



Victim

図 II-6-6: 要求額決定に関するチャット例2（被害組織の売上額を把握しているという主張、原文抜粋）

要求額決定に関するチャット例3：被害組織の銀行明細を把握しているという主張

原文

maybe you didn't understand: we are a small company and we don't have all that money. we can pay 500/1000 euros, certainly not 90000 euros

日本語訳

あなたは理解していないかもしれませんが、私たちは小さな会社で、そんなお金はありません。500～1000ユーロなら支払えますが、9万ユーロは無理です。

2025-04-28 14:02

原文

The price is established based on the company's finances, we are aware of the equity in your banks accounts, your revenue and net profits. 1k is not even considerable.

日本語訳

価格は会社の財務に基づいて設定しています。あなたの銀行口座の資本、収益、純利益を把握しています。1000ユーロは論外です。

2025-04-28 14:09

原文

I don't know what you think you know, but we don't have that money. Paying 90,000 euros would mean going into debt and closing the company, does that seem feasible to you. We can get to 2,000 euros

日本語訳

あなたが何を知っていると思っているのか分かりませんが、私たちにはそのお金はありません。9万ユーロを払うと借金を背負って会社を閉じることになりますが、それは現実的ですか。私たちが出せるのは2千ユーロです。

2025-04-28 14:12

原文

Will your own bank statement change your mind? I can get it for you

日本語訳

あなた自身の銀行明細なら考えが変わりますか？用意できます。

2025-04-28 14:28

原文

please go ahead

日本語訳

どうぞ続けてください。

2025-04-28 14:29

Victim

Victim

Victim

Victim

図 II-6-7: 要求額決定に関するチャット例3（被害組織の銀行明細を把握しているという主張、原文抜粋）

69

要求額決定に関するチャット例 4 : 被害組織の財務報告書から要求額の妥当性を主張

原文
could you please how much it will cost to recover my files because we need to know the costs involved.

日本語訳
ファイルの復旧にいくらかかるか教えてください。費用を把握する必要があります。

2024-12-23 13:10

Victim

Christopher

原文
wait, tech support will send your test files

日本語訳
お待ちください。技術サポートがあなたのテストファイルを送ります。

2024-12-23 14:50

原文
price decrypt 80k in bitcoin, for all hosts and files

日本語訳
全ホストとファイルの復号化価格は8万ドル、ビットコインで

2024-12-23 14:51

原文
sir this amount is very high to be paid. We would like to work with you because it will take much time to recover our infrastructure. So some questions from our side 1. Can you please provide a generous discount so it's easier for us to consider your solution?2. How fast the recovery process will take if we work with you ?

日本語訳
その金額はとても高額です。インフラストラクチャの復旧に時間がかかるため、あなたと協力したいと思います。私たちからの質問があります。1. 検討しやすくするため、寛大な割引をしていただけませんか？2. 協力する場合、復旧プロセスはどのくらい早くできますか？

2024-12-23 15:47

Victim

Christopher

原文
we can't offer you a discount

日本語訳
割引は提供できません

2024-12-23 16:08

原文
if you pay quickly and restore the infostructure on the same day

日本語訳
迅速にお支払いいただき、同日にインフラストラクチャを復旧すれば

2024-12-23 16:12

原文
I saw your financial report, our price is not big for you

日本語訳
あなたの財務報告書を見ました。私たちの価格はあなたにとって大きくありません

2024-12-23 16:14

図 II-6-8: 要求額決定に関するチャット例 4 (財務報告書から要求額の妥当性を主張、原文抜粋)

自社の公開情報 (IR・採用・事業規模等) が攻撃者に把握されている前提で、想定される要求額レンジや交渉シナリオを事前に検討しておくことが望ましい。

6.4 金額交渉の経過と最終合意

主な交渉の流れは、高額な要求から始まり減額交渉を経て合意に至るというものであり、減額交渉は多くのケースで見られた。減額率や要求額帯ごとの支払い確認割合を分析した。

支払いの有無は、DB 上のフラグとチャット上の支払い完了表現の二つの観点から判定した。以降では、支払い判定を次の二つに分けて扱う。

表 II-6-1：支払い判定の定義と件数

定義	件数	根拠
定義 A (DB フラグ基準)	7 件	<code>clients.paid_commission > 0</code>
定義 B (チャット推定基準)	17 件	チャット上で支払い完了メッセージが見られたユニーク組織

※ 定義 A は `client_id` 単位、定義 B はユニークドメイン単位である。定義 A の 7 件を `clients.build_id → builds.company_website` 経由で正規化ドメインに写像すると、重複なく 7 件の異なる被害組織 (ドメイン) に対応し、いずれも定義 B の分母である 127 ドメインに含まれる。したがって 7 件・17 件は同一の 127 ドメインを分母とする値として扱うことができ、以降の支払い率 6~13% はこの写像後の値である。

本節の支払い確認は、被害組織単位で交渉結果を捉えるため、チャット内容から支払い完了を推定した定義 B を基本とする。支払い判定の詳細は付録 A で整理する。

図 II-6-9 は `chats` から抽出した要求額と支払い判定を被害組織 (正規化ドメイン) 単位で集計し、要求額帯別の支払い確認割合を示したものである。母数が小さい帯は不確実性が大きい。金額抽出の詳細は付録 C を、支払い判定の詳細は付録 A を参照されたい。

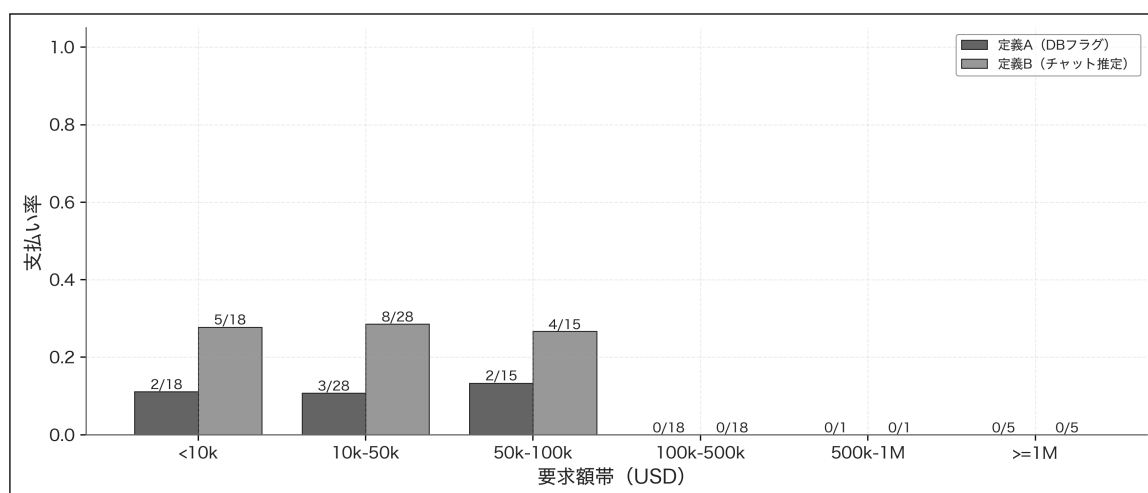


図 II-6-9: 要求額帯別の支払い確認割合

本データにおいては、初回要求額が 10 万 USD を超える区分で支払い確認例は見られなかった。ただし、各区分の母数が小さいため、要求額と支払いの統計的関連または因果関係を示すものではない。

減額率に明確な上限が設定されていない点も見られた。5 割を上限とすると述べるアフィリエイトがいる一方、それを大きく超える減額を許容する者もいた。図 II-6-10 にその例を示す。



図 II-6-10: 割引上限に関するチャット例（原文抜粋）

減額率はアフィリエイトの裁量に依存していると見られるが、全ての攻撃グループが同様とは限らない。「減額がある前提」で交渉に臨むのではなく、交渉不成立や条件悪化も含む複数シナリオで復旧計画を準備しておく必要がある。

6.5 支払い件数と獲得身代金 (推定)

6.4 節で示した支払い判定を前提に、一次データから推測できる支払い件数および獲得した身代金を分析する。

獲得身代金の推定はオンチェーンではなくチャット上の金額言及に基づく。支払い完了と推定できるケース (定義 B) について、支払い完了表現直近の金額言及を採用し、BTC 表記は取引当日の終値で USD に換算した。

推定合計は約 33 万 USD であるが、これはチャット上で観測可能な金額から算出した参考推定であり、XMR での支払いやパネル外交渉による過小推定と、支払い判定・金額対応付けの誤りによる過大推定の双方があり得ることに留意が必要である。金額抽出・採用ルールの詳細は付録 C を参照されたい。

図 II-6-11 は支払い完了と推定できた被害組織について、最終要求額をアフィリエイト別に合算した推定獲得身代金を示したものである。

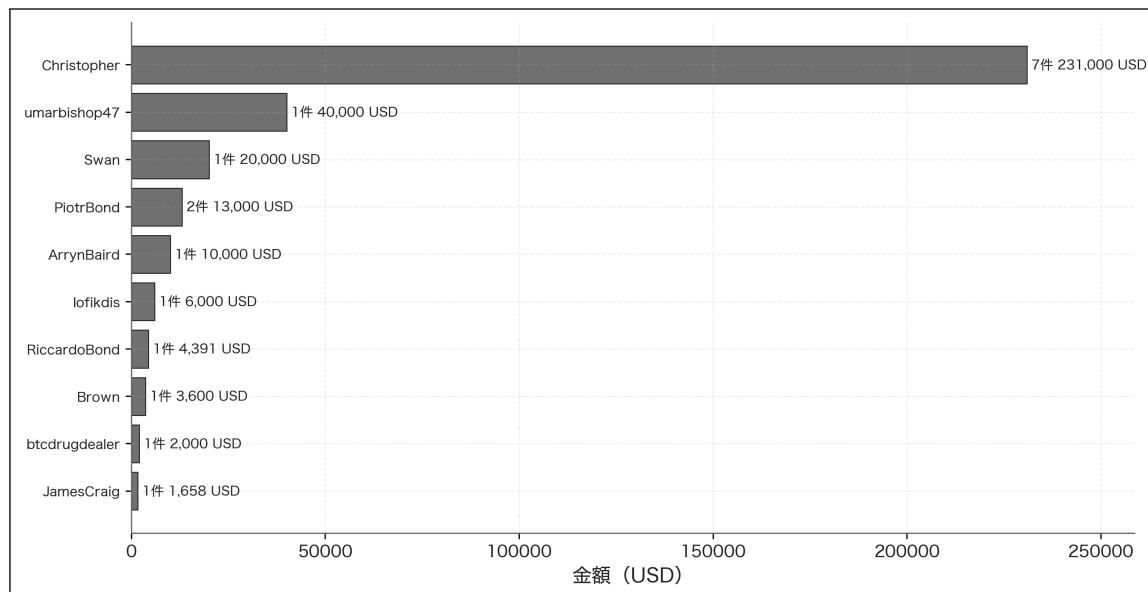


図 II-6-11: アフィリエイト別の獲得身代金額

支払いを実施した組織は 7 件 (DB フラグ基準)~17 件 (チャット推定基準) と推定される。復旧可否と情報漏えいリスクは別の判断軸であり、バックアップから復旧可能でもデータ公開回避のために支払いを選択したケースも存在した。

支払い判定ごとの帰結をリークサイト掲載の観点で整理する (判定基準は付録 A の表 A-1 を参照されたい)。

表 II-6-2: 支払い判定 (推定) × リークサイト掲載

支払い判定	リークサイト掲載	件数	補足 (典型)
支払い推定 (チャット)	掲載	0	支払い組織 (定義 B) のうち、掲載に至った組織は 0 件
支払い推定 (チャット)	未掲載	17	支払い組織 (定義 B)
支払い未確認	掲載	24	突合ヒット (うち 2025 年 12 月以降に LockBit 5.0 に掲載=15)
支払い未確認	未掲載	86	未掲載 103 件 (127 件から掲載 24 件を除外) から支払い推定 17 件を除外

支払いが確認できない組織でもリークサイトに掲載されなかったケースがある。

一部の被害組織情報は、2025 年 12 月以降に出現した LockBit 5.0 のリークサイトに掲載された。掲載の理由は本データからは特定できない。

全 127 組織に対する支払い率は DB フラグ基準で 6%、チャット推定基準で 13%にとどまり、支払い組織がリークサイトに掲載されたケースは見られなかった。ただし、支払いが掲載を抑止したかは一次データからは断定できない。支払いの有無にかかわらず情報漏えい対応を別途準備しておくことが重要である。

なお、支払い率についてもデータ終端による打ち切りの影響を確認したところ、追跡期間の閾値を変えてもいずれも 13~15%の範囲であった (詳細は付録 A 参照)。

6.6 Monero オプションの提示

Bitcoin 以外の選択肢も提示されていた。図 II-6-12 に示すチャット例では、同一の要求に対し「11 万 USD 相当の Bitcoin、または 9 万 USD 相当の Monero」という 2 つの価格が提示されており、Monero での支払いは約 18% 低い価格であった。XMR は一般にトランザクションの追跡が困難とされており、攻撃者が追跡困難な決済手段へ誘導する意図で提示した可能性がある。ただし、実際に XMR で決済されたかどうかは一次データからは特定できない。

※チャット記録をもとにイメージ化したもの

Moneroオプション提示のチャット記録



59X67

原文

you misunderstood.110 000 US Dollars in Bitcoin or 90 000 US Dollars in Monero

日本語訳

誤解しています。11万米ドル相当のビットコイン、または9万米ドル相当のモノネロです。

2025-01-17 20:20

原文

unfortunately we can't offer you decryptor for single institution. decryptor is for entire topack system. we can't guarantee you are not giving it away for lower price you should probably contact <masked:VictimName> and demand resolution with us.

日本語訳

残念ながら、単一の機関向けに復号化ツールを提供することはできません。復号化ツールは<masked:VictimName>全体のシステム向けです。あなたがそれを低価格で他者に渡さないことを保証できません。<masked:VictimName>に連絡し、私たちとの解決を要求する必要があります。

2025-01-17 20:20

原文

that is low price in comparison to network size and data stolen

日本語訳

ネットワーク規模と盗まれたデータ量に比べれば、それは低価格です。

2025-01-17 20:21

原文

if you have any more questions please let us know

日本語訳

他に質問があれば知らせてください。

2025-01-17 20:21

図 II-6-12: Monero オプション提示のチャット例（原文抜粋）

6.7 本章のまとめ

本章では、身代金の要求から支払いに至る金銭フェーズを定量的に分析した。主要な知見を以下に示す。

1. 大量の BTC アドレスプール

59,975 件のアドレスが事前登録され、割り当て済みは 159 件 (0.3%未満) にとどまる。プール外のアドレスがチャットに出現するケースもあり、アフィリエイトに一定の裁量があったと見られる。

2. 要求額の水準

中央値は約 50,000 USD、75 パーセンタイルは約 115,000 USD であった。90 パーセンタイルは約 400,000 USD に達するなど、高額側に長い裾を持つ分布であった。

3. 売上と要求額の非比例性

攻撃者が入力した推定売上 (builds.revenue) と要求額に単純な比例関係は見られなかった。

4. 減額の常態化と裁量のばらつき

減額交渉は一般的に行われており、平均減額率は約 37%、最大で約 84%の減額に至った例もある。減額率の上限は明確に設定されておらず、アフィリエイトの裁量に委ねられていたと見られる。

5. 支払いは全体の 6%(DB フラグ基準)～13%(チャット推定基準)

DB フラグ基準で 7 件、チャット推定基準で 17 件であり、全 127 組織に対する支払い率は低い。なお、支払いの有無だけでは掲載の有無を決定できない。

6. Monero オプションの提示

XMR 支払いで約 18%低い価格が提示された例があり、追跡困難な手段への誘導が試みられていた。

「支払えば復旧・非公開が保証される」という単純な前提は成り立たない。あらゆるケースを想定した上で、意思決定の承認経路・判断基準・復旧手順などを策定しておくことが不可欠である。

7. 復号フェーズ：支払い後のプロセス

本章では、身代金の支払い後に何が起きるかを、チャット記録から追跡する。復号ツールの提供までの時間、復号の成否、および復号プロセスで生じたトラブルを順に整理し、支払い後にツールが提供されても復旧が保証されない実態を具体的な事例とともに示す。

本章では chats を用いて、身代金支払い後のやり取りを追跡する。分析単位は原則 client_id (スレッド)、時刻は UTC である。支払い判定は第 6 章の定義 B に従い、チャット上で支払い完了と推定できるケースを対象とする。攻撃者側が復号ツール (またはそれに準ずるファイル) を送付した痕跡があるものを「提供あり」と判定する。支払い時刻・成否はチャット上の申告に基づくため、オンチェーン確定時刻や実復旧状況とは一致しない場合がある。

7.1 支払いから復号ツール提供までの時間

Lite パネルの構造的な特徴として、復号ツールの生成権限が boss に集中している点が挙げられる。boss が不在の場合、ツール提供が大幅に遅れるケースもあった。

チャットから支払いが推定できる 17 件のうち、復号ツールの受領を拒否した組織を除く 16 件について、ツール提供までの時間を算出した。支払い日時は被害組織側が支払い完了を申告した日時、ツール提供日時は攻撃者側が復号ツールと見られるファイルを送信した日時を採用している。平均は約 6 時間で、最大 34 時間のタイムラグがあった。

図 II-7-1 は支払い完了 (被害組織の申告) からツール送付 (攻撃者の送付) までの時間差を被害組織単位で集計し、分布を示したものである。支払い時刻はチャット上の申告であり、オンチェーン確定時刻ではない。

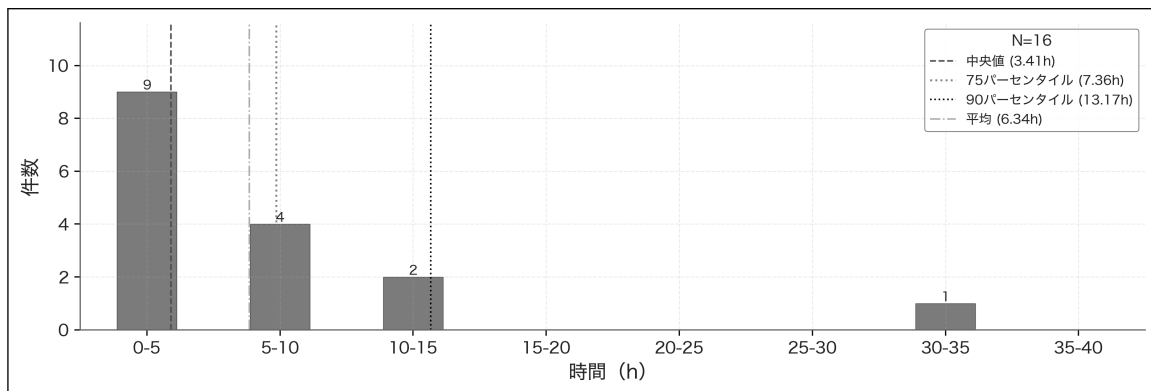


図 II-7-1: 支払いから復号ツール提供までの時間分布

図 II-7-1 が示す通り多くのケースで 24 時間以内に提供が確認できるが、boss 不在による例外も存在する。復号ツールだけでなく、テスト復号においても boss の不在が原因で大きな遅延が発生したケースがあった。図 II-7-2～6 にその例を示す。図 II-7-7 は、boss 依存体制における通常時の対応所要時間の目安を示すチャット例である。

※チャット記録をもとにイメージ化したもの
(1/5)

boss不在による対応遅延のチャット例 1

原文
how to test ?
日本語訳
どうやってテストしますか？
2025-03-10 07:00

Victim

Christopher

原文
File share <URL:Masked>
日本語訳
ファイル共有サービス：<URL:Masked>
2025-03-10 07:09

原文
upload zip archive here
日本語訳
ここにzipアーカイブをアップロードしてください
2025-03-10 07:09

中略

Christopher

原文
you need to wait, tech support is not online now
日本語訳
待つ必要があります、技術サポートは今オンラインではありません
2025-03-10 09:39

原文
When is the tech support online ?
日本語訳
テクニカルサポートはいつオンラインですか？
2025-03-11 03:19

Victim

Christopher

原文
Hello
日本語訳
こんにちは。
2025-03-11 12:23

原文
boss is not there, sometimes he may not answer right away, we are all waiting for him, only the boss has access to the decryptor
日本語訳
上司が不在で、すぐに返答できないことがあります。私たちは皆、上司を待っています。復号ツールにアクセスできるのは上司だけです。
2025-03-11 12:25

原文
I think today he will be here and will make a decryptor for everyone
日本語訳
今日、彼が来て皆のための復号ツールを作ります。
2025-03-11 12:26

図 II-7-2: boss 不在による対応遅延のチャット例 1 (1/5、原文抜粋)

77

boss不在による対応遅延のチャット例 1

原文
I can't do anything
日本語訳
私には何もできません。

2025-03-11 12:27

原文
Got it
日本語訳
了解しました

2025-03-11 12:31

Victim

原文
Hi, just checking in—haven't seen any updates from your team yet. Is there any update on the test decryption? Let me know when we can expect the results. Thanks.
日本語訳
確認です。まだあなたのチームから更新がありません。テスト復号の進捗はありますか？いつ結果を期待できるか教えてください。ありがとうございます。

2025-03-12 02:11

Christopher

原文
Hello
日本語訳
こんにちは

2025-03-12 12:04

原文
strange, but our boss is silent for 3 days, without him there will be no decryptor test and full decryptor
日本語訳
奇妙ですが、ボスが3日間沈黙しています。彼がいないと復号ツールのテストも本番の復号ツールも進みません。

2025-03-12 12:06

中略

原文
We are still willing to proceed with the payment for the full decryption, but we need to resolve the test issue first. Is there any alternative solution to confirm the decryption process?
日本語訳
完全復号の支払いを進める意思はありますが、まずテストの問題を解決する必要があります。復号プロセスを確認するための代替手段はありますか？

2025-03-12 13:23

Victim

Christopher

原文
No, I just wrote that, tech support is the boss, he doesn't have tech support because he doesn't trust to nobody the private keys from the decryptor
日本語訳
いいえ、そう書いただけです。技術サポートとは上司のことです。復号ツールの秘密鍵は誰も信用していないので、彼には専任のサポートはいません。

2025-03-12 13:25

図 II-7-3: boss 不在による対応遅延のチャット例 1 (2/5、原文抜粋)

boss不在による対応遅延のチャット例 1

原文

I understand, but it's the boss's fault, maybe he rides around in his Lamborghini with whores)))) or maybe he's running from the FBI)))

日本語訳

わかっていますが、それはボスのせいです。ランボルギーニで娼婦を乗せて走り回っているのかもしれませんが、FBI から逃げているのかもしれませんが。

2025-03-12 13:27

原文

No problem with the decryptor, the only problem is that the boss hasn't answered anyone for 3 days.

日本語訳

復号化ツール自体には問題ありません。唯一の問題は、ボスが3日間誰にも返答していないことです。

2025-03-12 13:28

原文

we are not scammers, we do our job honestly and I am writing to you honestly

日本語訳

私たちは詐欺師ではありません。誠実に仕事をしており、正直にお伝えしています。

2025-03-12 13:30

原文

never had a boss take so long to respond, I don't know why.

日本語訳

これほど返答に時間がかかるボスは初めてです。理由が分かりません。

2025-03-12 13:36

原文

You can also write to our boss

日本語訳

私たちのボスに連絡してもかまいません

2025-03-12 13:38

原文

you get your bitcoin ready because the boss is coming and he will quickly do the decryptor test

日本語訳

ボスが来てすぐに復号ツールのテストをするので、ビットコインの準備をしておいてください

2025-03-12 13:41

原文

you can save time

日本語訳

時間を節約できます

2025-03-12 13:42

原文

We are fully prepared, but we need the test decryption result first. Let us know when the test is completed, and we will proceed accordingly. Thank you.

日本語訳

準備は整っていますが、まずテスト復号の結果が必要です。テストが完了したらお知らせください。そのうえで進めます。ありがとうございます。

2025-03-12 13:51



Victim

中略

図 II-7-4: boss 不在による対応遅延のチャット例 1 (3/5、原文抜粋)

boss不在による対応遅延のチャット例 1

**Christopher**

原文
sorry, never happened before but the boss is still not online,i don't know, maybe something happened to him, without it lockbit don't work

日本語訳
すみません、こんなことは今までありませんでしたが、ボスがまだオンラインではありません。理由はわかりません。何かあったのかもしれない。ボスがいないと LockBit は機能しません。

2025-03-13 10:19

原文
Has there ever been a backup solution in situations like this?

日本語訳
このような状況でバックアップの解決策が取られたことはありますか？

2025-03-13 10:56

**Victim**

**Christopher**

原文
only the boss has a decryptor, without him no one will have any deals.

日本語訳
復号ツールを持っているのはボスだけです。彼なしでは誰とも取引は成立しません。

2025-03-13 13:36

原文
he will come and explain why this happened, just have to wait, without it we lose money

日本語訳
彼が来て、なぜこうなったかを説明します。少し待つしかありません。そうでないと私たちは損をします。

2025-03-13 13:39

原文
there's a lot of teams here, and I'm not alone. Everyone is waiting for him, there are serious teams working with millions and they also won't do anything without a boss

日本語訳
こちらには多くのチームがいて、私だけではありません。皆が彼を待っています。何百万単位で動く本気のチームもあり、ボスなしでは誰も動きません。

2025-03-13 13:41

原文
but don't worry, he'll be online and we can keep going.

日本語訳
心配いりません。彼はオンラインになりますので、続けられます。

2025-03-13 14:23

原文
I see, so without the boss, what happens to your role?Are you also affected by this situation?

日本語訳
なるほど、ボスがいない場合、あなたの役割はどうなりますか？この状況の影響をあなたも受けていますか？

2025-03-13 14:51

**Victim**

**Christopher**

原文
Lockbit is an affiliate program that provides us with a tool for work, in darknet there are other options with an affiliate program

日本語訳
Lockbitは私たちに作業用ツールを提供するアフィリエイトプログラムです。ダークネットには他にもアフィリエイトプログラムの選択肢があります。

2025-03-13 15:03

図 II-7-5: boss 不在による対応遅延のチャット例 1 (4/5、原文抜粋)

boss不在による対応遅延のチャット例 1

原文

if lockbit stops working it will be world news but that won't happen

日本語訳

もしLockBitが動作を停止したら世界的なニュースになりますが、そんなことは起きません。

2025-03-13 15:05

原文

they can't catch him, it's impossible. FBI offers 10 million for Lockbit's identity

日本語訳

彼らは彼を捕まえられません。不可能です。FBIはLockbitの身元に1000万ドルを提示しています。

2025-03-13 15:06

原文

we've been working with him for 5 years and we've never had a situation like this, he's always been online. Let's wait and hope that everything is fine

日本語訳

私たちは彼と5年間一緒に働いていますが、このような状況は今まで一度もありませんでした。彼はいつもオンラインでした。待って、すべてがうまくいくことを願いましょう

2025-03-13 15:08

原文

you're not the only client I'm talking to right now, we're all just waiting for him.

日本語訳

今話しているのはあなただけではありません。私たちは皆、彼を待っているところです。

2025-03-13 15:09

原文

I'm not worried about your money, I'm worried that something bad will happen to the boss

日本語訳

私はあなたのお金のことを心配しているのではなく、ボスに何か悪いことが起こるのではないかと心配しています

2025-03-13 15:10

原文

I understand that this is a difficult situation for everyone, especially since the boss has never gone offline like this before. You must be under a lot of pressure handling so many people waiting for answers.

日本語訳

皆にとって難しい状況だと理解しています。特に、これまでボスがこのようなオフラインになったことはありませんでしたから。多くの人が回答を待つ中、あなたも大きなプレッシャーの中にはいるはずです。

2025-03-13 15:21



Victim



Christopher

原文

ok thx, let's just wait for him, he will come at any moment

日本語訳

ありがとう。彼を待ちましょう。すぐに来るはずです。

2025-03-13 15:29

原文

boss here

日本語訳

ボスがここにいます。

2025-03-14 08:14

図 II-7-6: boss 不在による対応遅延のチャット例 1 (5/5、原文抜粋)

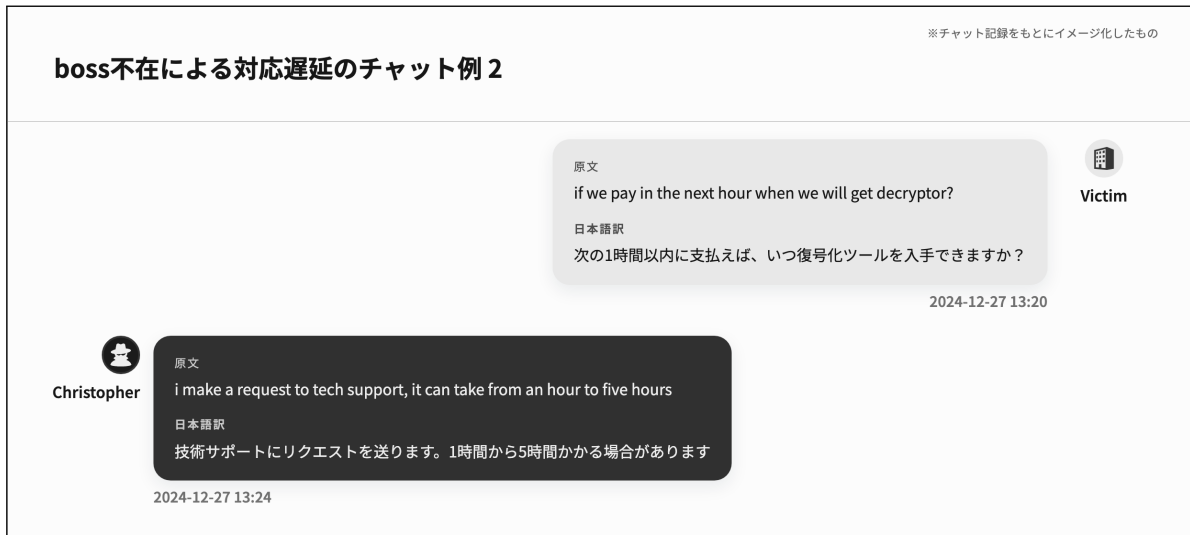


図 II-7-7: boss 依存体制における対応所要時間の目安（原文抜粋）

復号ツールの生成権限は boss に集中しており、その在席状況によって提供が数時間から数日遅延する構造的リスクがある。仮に身代金を支払ったとしても、ツールを入手するまでに待ち時間が生じることを念頭におく必要がある。

7.2 復号結果の分類

チャットを分析した結果、復号ツールが提供されたケースは合計 19 件あった。内訳は、身代金を支払った組織への提供が 16 件（支払い完了 17 件のうち、ツール受領を拒否した 1 件を除く）、および旧 CIS 地域の組織への無償提供が 3 件である。

これら 19 件の復号結果は、成功 2 件、部分成功 2 件、失敗 6 件、不明 9 件であった。成功・部分成功・失敗のいずれかに判定できたのは 10 件で、残る 9 件はチャット上で最終的な結果を確認できなかった。

全 19 件のうち、成功と部分成功を合わせた復旧確認数は 4 件（約 21%）である。ただし、この数値の解釈には 2 つの留保が必要である。第一に、9 件の結果が不明であるため、21% はあくまで確認できた復旧成功の下限であり、結果が判明した 10 件に限れば成功・部分成功は 4 件（40%）となる。第二に、19 件には旧 CIS 地域への無償提供 3 件が含まれるため、21% を「支払い後の復旧率」としてそのまま解釈することもできない。なお、不明としたケースの中にも、復号ツールが正常に動作せずサポートを求めているものが複数含まれており、結果不明を復旧成功とみなすことはできない。以上から、復号ツールを受領しても、必ずしも復旧に至るとは限らない実態が明らかになった。

復号結果「不明」9 件のうち、ツール提供から 70 日以上を経てもチャット上で結果が確認できていないケースが大半であり、これは観測期間の不足よりも被害組織側から結果の報告がなかったことが主因と考えられる。ただし 2 件はツール提供からデータ終端（2025-04-29）までが 10 日・26 日と短く、結果が確認される前にデータが打ち切られた可能性が残る。

表 II-7-1 は復号ツール提供後のやり取りが確認できたケースについて、チャット内の発言内容から復号結果を分類したものである。分類はいずれも被害組織側の発言に基づく。成功は全ファイルの復号が確認できたケース、部分成功は一部ファイルのみ復号できたケース、失敗は復号できなかったケースを指す。対応途中で会話が途切れている、または結果への言及がないケースは不明とした。

表 II-7-1：復号結果の分類

区分	提供形態	成功	部分成功	失敗	不明
ケース数 (支払い提供)	支払い	2	2	3	9
ケース数 (無償提供)	無償	0	0	3	0

なお、本分析は 19 件という限られたケース数に基づいており、不確実性が大きい点に留意が必要である。復号失敗 6 件についても、復号ツール自体の不具合だけでなく、手順の誤りやアフィリエイトの技術的な操作ミス、対象ファイルの破損など複数の要因が考えられ、必ずしもツールの不具合のみを示すものではない。

7.3 復号プロセス中の問題事例

チャットには、復号トラブルに関するやり取りが複数記録されていた。前述の通り、支払い後も復号ツールが機能しなかったケースや、データは返却されたものの重要データが含まれておらず実質的に失敗と見られる事例も見られた。復号失敗の申し立てに対しては、再起動を依頼したり、アンチウイルスソフトとの競合を指摘したりする応答が返されていた。図 II-7-8～11 にその例を示す。

重要データが復号できなかったケースのチャット記録

原文

Hello, we decrypted the files on the virtual machine, but there are still a lot of files that have not been decrypted, please take a look at what the problem is, thank you

日本語訳

仮想マシン上のファイルは復号できましたが、まだ多くのファイルが復号されていません。問題が何か確認してください。ありがとうございます。

2025-03-27 01:17

原文

There are still more than 50,000 files that have not been decrypted, and there is no problem of customers modifying the files, because the files are stored in different folders, you look at the files I sent you, and see how to solve this problem

日本語訳

まだ5万以上のファイルが復号されていません。ファイルは別々のフォルダーに保存されているため、顧客がファイルを改変した問題はありません。送ったファイルを確認して、この問題をどう解決するか教えてください。

2025-03-27 08:27



lofikdis

原文

You need to close all file access processes to ensure that no process accesses these file resources.

日本語訳

いかなるプロセスもこれらのファイルリソースにアクセスしないよう、すべてのファイルアクセスプロセスを停止する必要があります。

2025-03-27 08:31

原文

At the same time, the highest permissions must be used to run. Guaranteed access permissions.

日本語訳

同時に、実行には最高権限を用いる必要があります。アクセス許可は保証されます。

2025-03-27 08:32

原文

All antiviruses have been shut down, processes have been shut down, file permissions have been changed, and they still can't be decrypted.

日本語訳

すべてのアンチウイルスを停止し、プロセスも停止し、ファイル権限も変更しましたが、それでも復号できません。

2025-03-27 08:35

原文

In the same folder, some data can be decrypted, and some data cannot be decrypted, which should have nothing to do with permission restrictions.

日本語訳

同じフォルダ内で、復号できるデータと復号できないデータがあります。権限制限とは無関係と思われます。

2025-03-27 08:37

中略



lofikdis

原文

boss not reply,i wlii give u 100GB files

日本語訳

ボスが返信しません。あなたに100GBのファイルを渡します。

2025-04-02 05:26

図 II-7-8: 重要データが復号できなかったチャット例 (1/2、原文抜粋)

※チャット記録をもとにイメージ化したもの
(2/2)

重要データが復号できなかったケースのチャット記録

原文
<URL:Masked>
日本語訳
<URL:Masked>

2025-04-02 06:46

原文
<Password:Masked>
日本語訳
<Password:Masked>

2025-04-02 06:46

原文
The boss is very busy and often responds to messages for 3-5 days. You can use the original file. I consulted the team and we deployed multiple encryption programs in this client that caused the inability to recover by 1 decryption. The boss is being resolved. Always believe that what our team promises will definitely do, after receiving the ransom.
日本語訳
ボスはとても忙しく、返信まで3〜5日かかることがよくあります。元のファイルを使ってください。チームに確認したところ、このクライアントには複数の暗号化プログラムを展開しており、1つの復号では復旧できない状況でした。ボスが対応中です。私たちのチームが約束したことは、身代金の受領後に必ず実行することを信じてください。

2025-04-02 06:50

原文
We are honest.
日本語訳
私たちは誠実です。

2025-04-02 06:53

原文
Big brother, I downloaded the 100G data you gave, and there is no information we need, and the file we need is an ibd file in the <URL:Masked> directory
日本語訳
兄貴、あなたがくれた100Gのデータをダウンロードしましたが、私たちが必要とする情報はありません。必要なファイルは<URL:Masked>ディレクトリのibdファイルです

2025-04-03 01:11

Victim

図 II-7-9: 重要データが復号できなかったチャット例（2/2、原文抜粋）

85

ロシア地域への誤攻撃と無償提供のチャット例



図 II-7-10: 旧 CIS 地域への誤攻撃と無償提供のチャット例（1/2、原文抜粋）

ロシア地域への誤攻撃と無償提供のチャット例

原文

у вас только виндовс? или есхи тоже есть?

日本語訳

あなたはウィンドウズだけですか？それともESXiもありますか？

2025-02-19 01:27

原文

провел собственное расследование, оказывается адверта взломали, сменили пароль в его учетке, и потом залочили вас, возможно это спец операция ФБР по уничтожению моей репутации или подстава от конкурентов

日本語訳

独自に調査したところ、アフィリエイトの野郎がハッキングされ、アカウントのパスワードが変更され、その後あなた方がロックされたことが判明しました。これはFBIによる私の評判を破壊するための特殊作戦か、競合他社によるでっち上げの可能性があります。

2025-02-19 05:36

原文

вы смогли расшифровать файлы или нет?

日本語訳

ファイルを復号できましたか、それともできませんでしたか？

2025-02-19 05:37

原文

нет не смогли, антивирь ругается.... и даже после отключения нет

日本語訳

いいえ、できませんでした。アンチウイルスが警告します……無効化後でも無理です。

2025-02-19 20:01

king457533579

原文

можете дать мне исполняемый файл локера, которым вас залочили?

日本語訳

あなたをロックしたロッカーの実行ファイルを私に提供してもらえますか？

2025-02-20 00:44

原文

если сможете найти скиньте его мне, может быть антивирус перехватил или хакеры оставили где то

日本語訳

もし見つけられたら私に送ってください。たぶんアンチウイルスが検知したか、ハッカーがどこかに残したのかもしれない。

2025-02-20 00:44

原文

возможно те кто меня подставили изменили хекс эдитором ключ в локере специально чтобы файлы ломались без возможности расшифровки и я не смог помочь вам

日本語訳

おそらく私を陥れた者がロッカーの鍵をHEXエディタで改変し、意図的に復号不可能な破損を起こさせたため、私はあなたを助けられませんでした

2025-02-20 00:45

原文

те файлы что вы мне дали в начале на тестовую дешифровку я тоже не смог расшифровать

日本語訳

あなたが最初にテスト用の復号としてくれたあのファイルも、私には復号できませんでした。

2025-02-20 00:58

Victim

図 II-7-11: 旧 CIS 地域への誤攻撃と無償提供のチャット例（2/2、原文抜粋）

復旧計画では、攻撃者から復号ツールが提供されない場合や、提供されても正常に機能しない場合を想定し、重要データの復旧優先順位やバックアップからの復旧手順を事前に整理しておくことが望ましい。

87

7.4 本章のまとめ

本章では、身代金支払い後の復号プロセスをチャット記録から追跡した。主要な知見を以下に示す。

ツール提供までのタイムラグ：支払い完了から復号ツール提供まで平均約 6 時間、最大 34 時間を要した。復号ツールの生成権限が boss に集中しているため、boss 不在時には大幅な遅延が生じる構造的リスクがある。

復号成功は少数派：ツール提供が確認できた 19 件のうち、成功 2 件、部分成功 2 件、失敗 6 件、不明 9 件であった。支払いが復旧を保証しない実態が示された。

サポートの質のばらつき：復号失敗に対する攻撃者の対応は定型的な指示 (再起動、アンチウイルス無効化等) にとどまり、根本解決に至らないケースが複数あった。

支払い判断にあたっては、ツール入手後も復旧に失敗するリスクを織り込み、バックアップからの復旧を並行して準備する事業継続計画 (BCP) を整備しておくことが求められる。

8. 公開フェーズ：リークサイトへの掲載

本章では、Lite パネルの記録 (主に clients・builds) と外部リークサイトの掲載データを突合し、被害組織の情報公開に至る経過を分析する。掲載までのタイムライン、支払い状況と掲載の関係、Lite パネルとリークサイトの地域・業種分布の差異を順に検証する。

突合キーは正規化ドメイン等のユニークドメインを基本とし、採用単位は本文で明記する。時刻は日付単位で扱い、起点はチャット開始日に統一する (攻撃実行日ではない)。「支払い未確認」は Lite パネル上で支払い記録が見当たらない状態を指し、不払いと断定しない。表記揺れ・別パネル由来・外部データ欠損により、突合できない場合や誤突合が生じる可能性がある。

8.1 掲載までのタイムライン

Lite パネルの記録と外部リークサイトの掲載データを突合し、チャット開始日を起点とした掲載までの日数分布を示す。攻撃実行日は一次データからは確定困難であるため、正確な日時記録が存在するチャット開始日を起点に統一した。

LockBit 3.0 のリークサイトには掲載されなかったものの、2025 年 12 月に出現した LockBit 5.0 のリークサイトに掲載されたケースが 15 件存在した。両者の掲載時期は大きく離れており、本レポートではそれぞれの新規掲載タイミングを示した。

突合の過程ではリークサイト掲載日がチャット開始日より前となるケースもあり、パネルへの登録運用が厳格に管理されていなかった可能性がある。こうした時系列が整合しない 4 件はタイムライン分析 (図 II-8-1・8-2) の対象から除外している。

図 II-8-1 は chats のチャット開始日と外部リークサイト掲載日を正規化ドメイン単位で突合し、掲載までの日数分布を示したものである (LockBit 3.0)。X 軸の起点はチャット開始日であり、攻撃実行日ではない。

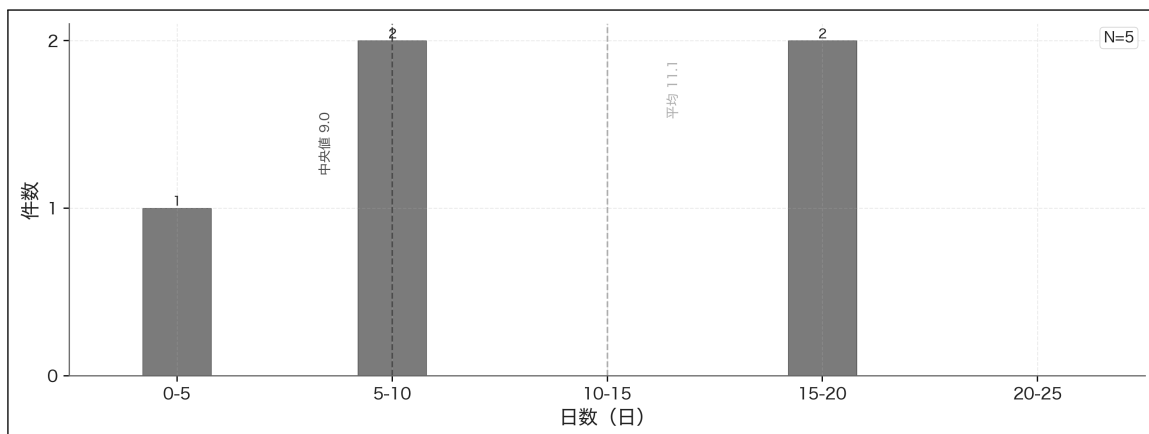


図 II-8-1: チャット開始からリークサイト掲載までの日数分布 (LockBit 3.0)

図 II-8-2 は同様の集計を LockBit 5.0 の掲載データについて示したものである。LockBit 3.0 と 5.0 で掲載タイミングが大きく異なるため、別系列として扱う。

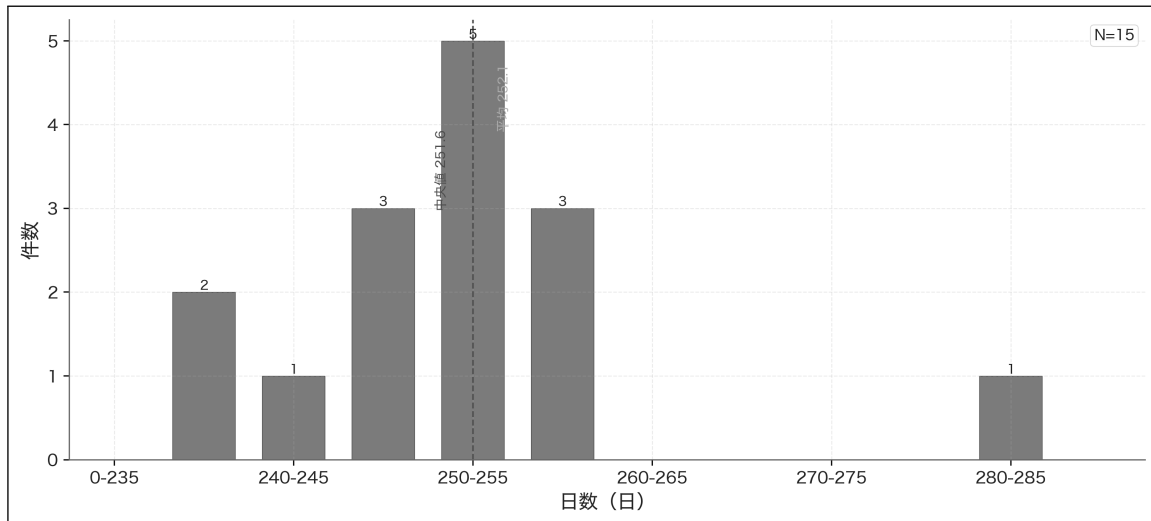


図 II-8-2: チャット開始からリークサイト掲載までの日数分布 (LockBit 5.0)

一度被害に遭えば、リークサイト掲載のリスクを長期にわたり抱えることになる。支払いの有無にかかわらず掲載されないケースも存在するが、その要因は一次データからは断定できない。インシデント対応が終了した後も掲載される可能性が残ることを前提に、長期的な公開リスクを織り込んだ対応計画を整備しておくことが求められる。

8.2 掲載された組織と掲載されなかった組織

チャット記録から支払いが認められなかった被害組織でも、リークサイトに未掲載の組織がある。図 II-8-3 は Lite パネルの記録と外部リークサイト掲載データを正規化ドメイン単位で突合し、支払い未確認の総数 110 件について、掲載・未掲載の割合を示したものである。

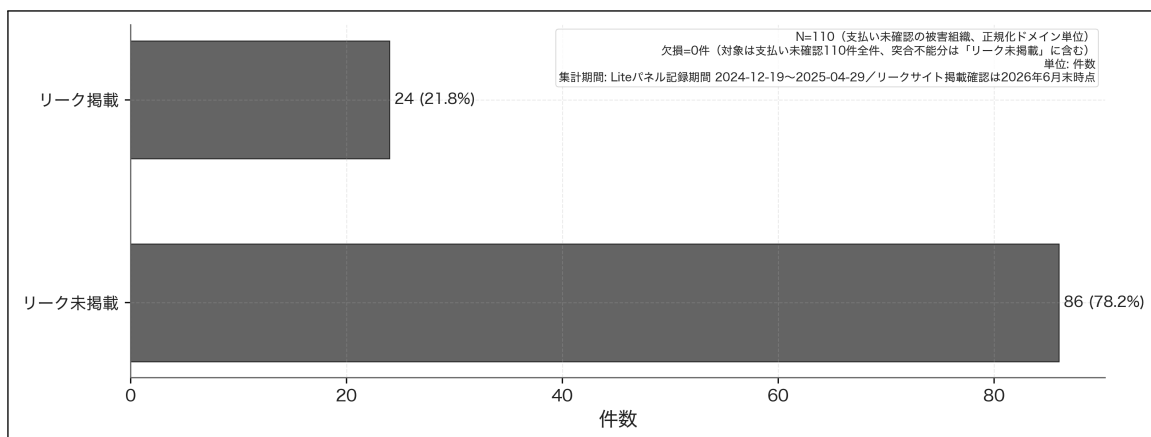


図 II-8-3: 被害組織の支払い・掲載状況の内訳

支払い推定群 (17 件) では掲載を確認した例が 0 件、支払い未確認群 (110 件) では 24 件 (約 22%) であった。支払い推定群で掲載事例が一件も確認されなかったが、支払い判定の誤分類、アフィリエイトによる対応差、案件の選択性、リークサイト突合の漏れなどの要因もあり得るため、この観測だけで支払いが掲載を抑止したと断定することはできない。掲載されなかった要因は一次データからは確定できず、今後も永久的に掲載されないとの断定もできない。情報漏えい対応は掲載の有無にかかわらず準備しておくことが望ましい。

8.3 Lite パネルとリークサイト上に現れる被害組織に関する傾向の差異

LockBit のリークサイト掲載情報では、北米・欧州を拠点とする組織の被害が目立ち、国別ではアメリカが最多である。一方、Lite パネルに記録された被害組織では、国籍が判明した組織の中では中国が最多であった(127 件中 15 件)。ただし、Lite パネルでは国籍不明の組織が 127 件中 37 件(約 29%)と最も多く、実際の地域分布にはなお不確実性が残る。

図 II-8-4・5 は Lite パネル (n = 127) とリークサイト (n = 2,757; 2022 年 1 月～2026 年 7 月、過去掲載を除外) の国別・業種別分布を可視化したものである。母数が大きく異なるため傾向把握にとどめる。

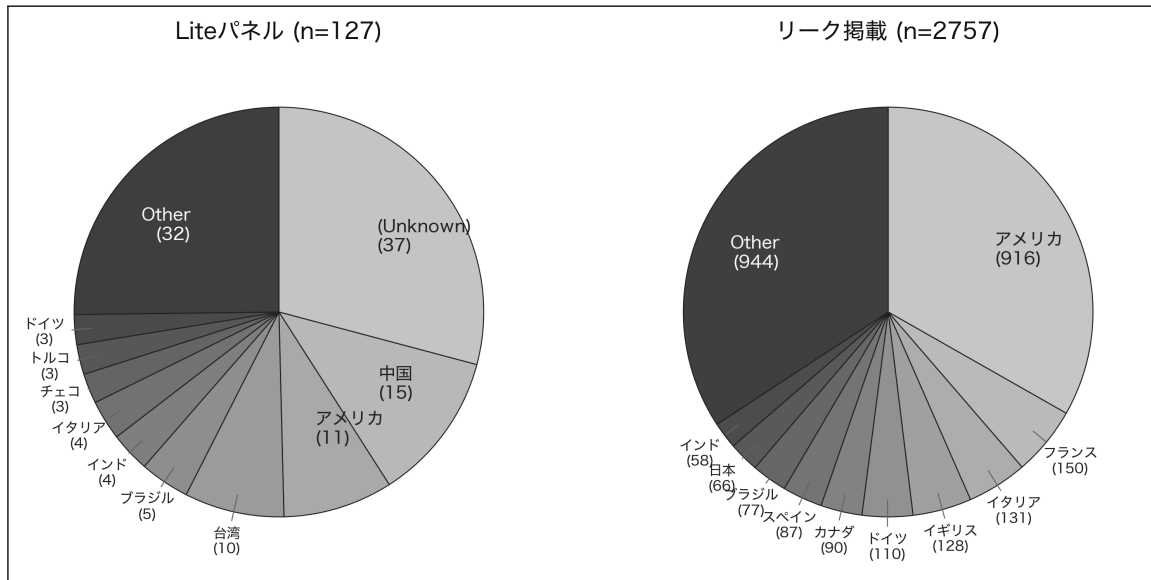


図 II-8-4: 被害組織の国別分布 (Lite パネル vs リークサイト)

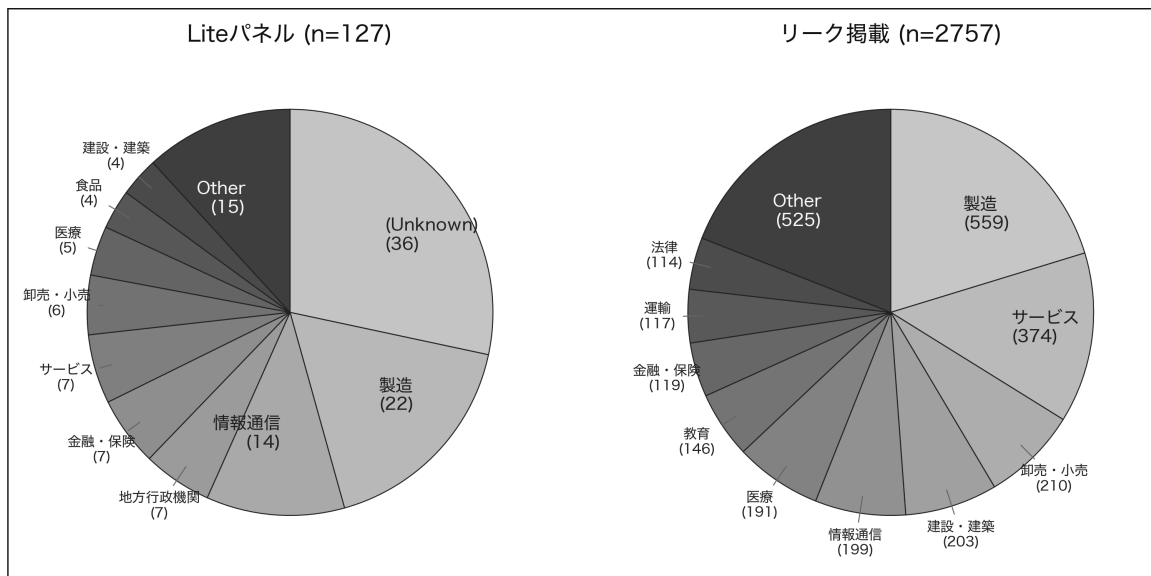


図 II-8-5: 被害組織の業種別分布 (Lite パネル vs リークサイト)

この差異は、今回流出した Lite パネルの記録が LockBit 全体の被害組織像を代表していないことを示しており、本レポートで確認できた被害の範囲は限定的である可能性を示唆する。

8.4 本章のまとめ

本章では、Lite パネルの記録と外部リークサイトの掲載データを突合し、情報公開フェーズの実態を分析した。主要な知見を以下に示す。

1. 掲載タイミングの予測困難性

チャット開始から掲載までの日数はケースごとに幅があり、LockBit 5.0 側で掲載を確認した 15 件では、チャット開始から掲載まで最長約 281 日 (約 9 か月) を要した。

2. 支払いの有無だけでは掲載の有無を決定できない

支払いが確認できた 17 組織のうち、リークサイトに掲載されたケースは 0 件であった。一方、支払いが確認できない 110 組織のうち掲載は 24 件 (約 22%) にとどまり、支払いが確認できないことが即座に掲載に直結するわけではない。

3. 地域・業種分布の乖離

Lite パネルでは国籍が判明した組織の中で中国が最多であったのに対し (ただし全体の約 3 割は国籍不明)、リークサイトではアメリカが最多を占める。リークサイト掲載データは被害の一部に過ぎず、それだけで攻撃傾向を判断することはできない。

公開リスクは支払い判断とは別軸でも評価し、対応方針をあらかじめ策定しておくことで、有事の際に取引先や関係者への対応を迅速に実行できる。

9. 運用上の特徴：管理パネルの運営実態

本章では、パスワード管理の不備、復号ツール生成権限の boss への集中、外部からの不正アクセス試行の痕跡、データベース設計の変遷を順に検証し、管理パネルの運用データから攻撃者側インフラの運営実態を整理する。

攻撃者の基盤も決して堅牢とは言えず、運用・管理上の弱点が存在する。こうした弱点を放置することの危うさは、攻撃者側と防御側のいずれにも共通する。Operation Cronos による基盤掌握について、LockBit 運営者は、侵害されたサーバーで PHP 8.1.2 が稼働していたことから、CVE-2023-3824 が悪用された可能性が高いと推測している。

ただし、同運営者は、PHP のゼロデイ脆弱性など、別の脆弱性が悪用された可能性にも言及している。これは LockBit 側による未検証の主張であり、法執行機関の公表資料では具体的な侵入手法は明らかにされていない。このため、本レポートでは、CVE-2023-3824 を確認された侵入経路としては扱わない。

なお、こうした攻撃者側インフラの実態は、法執行機関その他の権限を有する主体による能動的サイバー防御の観点から多くの活用可能性を有する。Lite パネルに含まれる暗号資産アドレスの監視による資金追跡、チャットログからの C2 サーバーの特定とインフラの監視・無力化、ビルド構成の分析に基づく攻撃手法の予測と防御態勢の先行構築、アフィリエイトの行動パターン分析による予兆検知など、攻撃者基盤の弱点把握から将来の攻撃抑止に至る各段階での活用が想定される。

分析には `users`・`builds`・`system_invalid_requests`・`migrations`・`socket_messages`・`chats` 等の運用データを用いる。

9.1 パスワード・パスフレーズ管理の実態

管理パネルにはアフィリエイトのログインパスワードが平文で保存されていた。これはパネル基盤自体の管理不備である。加えて、`builds` テーブルに記録されたパスフレーズ (ランサムウェアの実行時に入力求められる文字列と見られる) には、同一の値を複数ビルドで使い回している実態が確認できた。使い回しのパターンが把握できれば、解析者がランサムウェア検体を分析する際にパスフレーズを推測する手がかりとなり得る。

ログインパスワードの強度要件

`system_invalid_requests` テーブルのエラーメッセージからは、パネル側にパスワード要件が設定されていたことが読み取れる。要件は大文字・小文字・数字各 1 文字以上を含む 10～40 文字であり、エラーメッセージには以下の文言が記録されている。

Password isn't secure enough. It must have at least 1 uppercase character, 1 lowercase character, 1 number and be 10 or more symbols long, 40 symbols max.

この要件を満たさないパスワード設定が 56 件試行されており、システム側で拒否されていた。要件自体は設定されていたものの、要件を満たさないパスワードを設定しようとするアフィリエイトが一定数存在していた。

図 II-9-1 は `users.password` を対象にパスワード長の分布と頻出パターンを集計したものである。

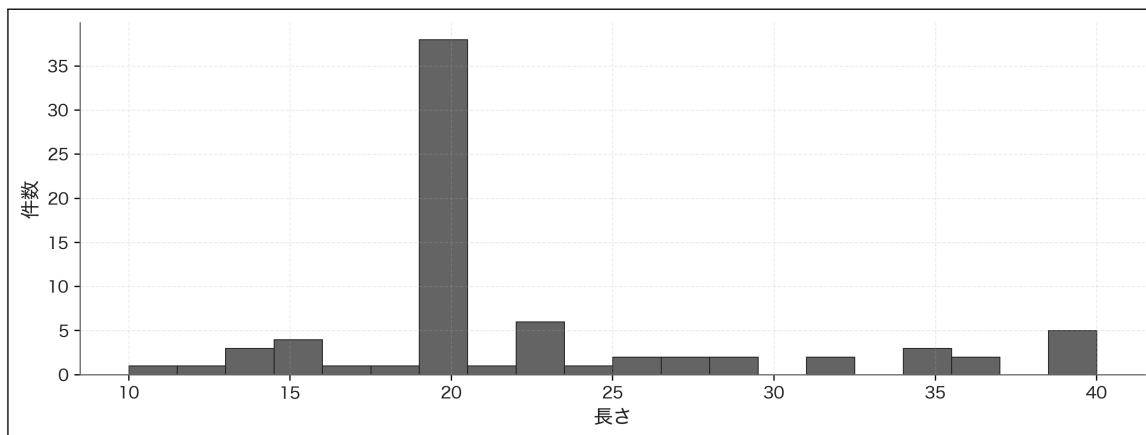


図 II-9-1: アフィリエイトのパスワード長分布

パスフレーズ使い回しの実態

パスフレーズはランサムウェア本体の起動時に入力求められる文字列とみられ、多くが同一のパスフレーズを複数ビルドで使い回していた。使い回されているパスフレーズには単純なものが多く、攻撃者が流れ作業に近い形でビルドを実行していたと見られる。

図 II-9-2 は builds に含まれるパスフレーズについて、同一値の出現回数を集計し使い回し分布を示したものである。

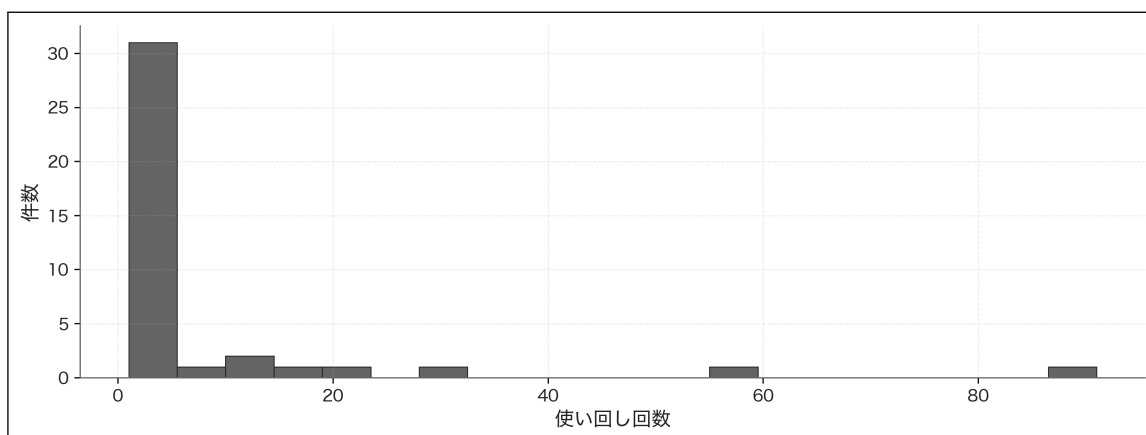


図 II-9-2: パスフレーズの使い回し分布と頻出パターン

図 II-9-3 は頻出パスフレーズの上位パターンを示したものである。

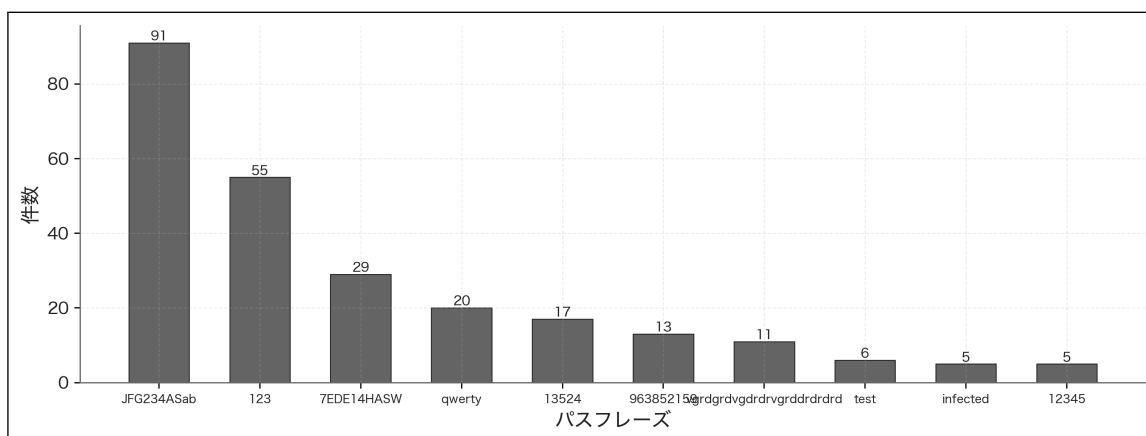


図 II-9-3: パスフレーズの頻出パターン

9.2 管理者依存の運営体制

Lite パネルの運営には、boss を中心としたトップダウン型の体制が見られる。アフィリエイトは復号ツールの生成権限を持たず、boss の対応状況によっては提供が遅延し得るやり取りも見られた他、身代金額についても boss のみが決定権を持つようにも見受けられた。

図 II-9-4～6 にその例を示す。

※チャット記録をもとにイメージ化したもの

管理者依存体制に関するチャット例 1

**Christopher**

原文

don't worry, send a decryptor from tech support, it's unique for each company, there is a version for esxi and win

日本語訳

心配いりません。テクニカルサポートから復号ツールを送ります。各社ごとに固有で、ESXi版とWindows版があります。

2025-02-10 13:37

原文

Okay, because I'm worried that the technical staff might not be available. Is he working today?

日本語訳

わかりました。技術スタッフが不在かもしれないのが心配です。今日は勤務していますか？

2025-02-10 13:47

**Victim**

**Christopher**

原文

so you understand, only one person has access to the decryptor, and that's the boss)

日本語訳

ご理解のとおり、復号ツールにアクセスできるのは一人だけで、その人物はボスです。

2025-02-10 13:53

図 II-9-4: 管理者依存体制に関するチャット例 1（原文抜粋）

※チャット記録をもとにイメージ化したもの

管理者依存体制に関するチャット例 2

原文

Thanks, bro. I appreciate it. Please send it to me as soon as possible.

日本語訳

ありがとう、兄弟。感謝します。できるだけ早く送ってください

2025-02-16 10:10

**Victim**

**Christopher**

原文

we'll wait for him together.

日本語訳

一緒に彼を待ちましょう。

2025-02-16 10:11

原文

I can't do anything here, our boss is working on the update and is very busy now, we'll have to wait and see how he will be

日本語訳

ここでは何もできません。ボスがアップデート作業中で今はとても忙しいので、どうなるか様子を見るしかありません。

2025-02-16 10:12

図 II-9-5: 管理者依存体制に関するチャット例 2（原文抜粋）

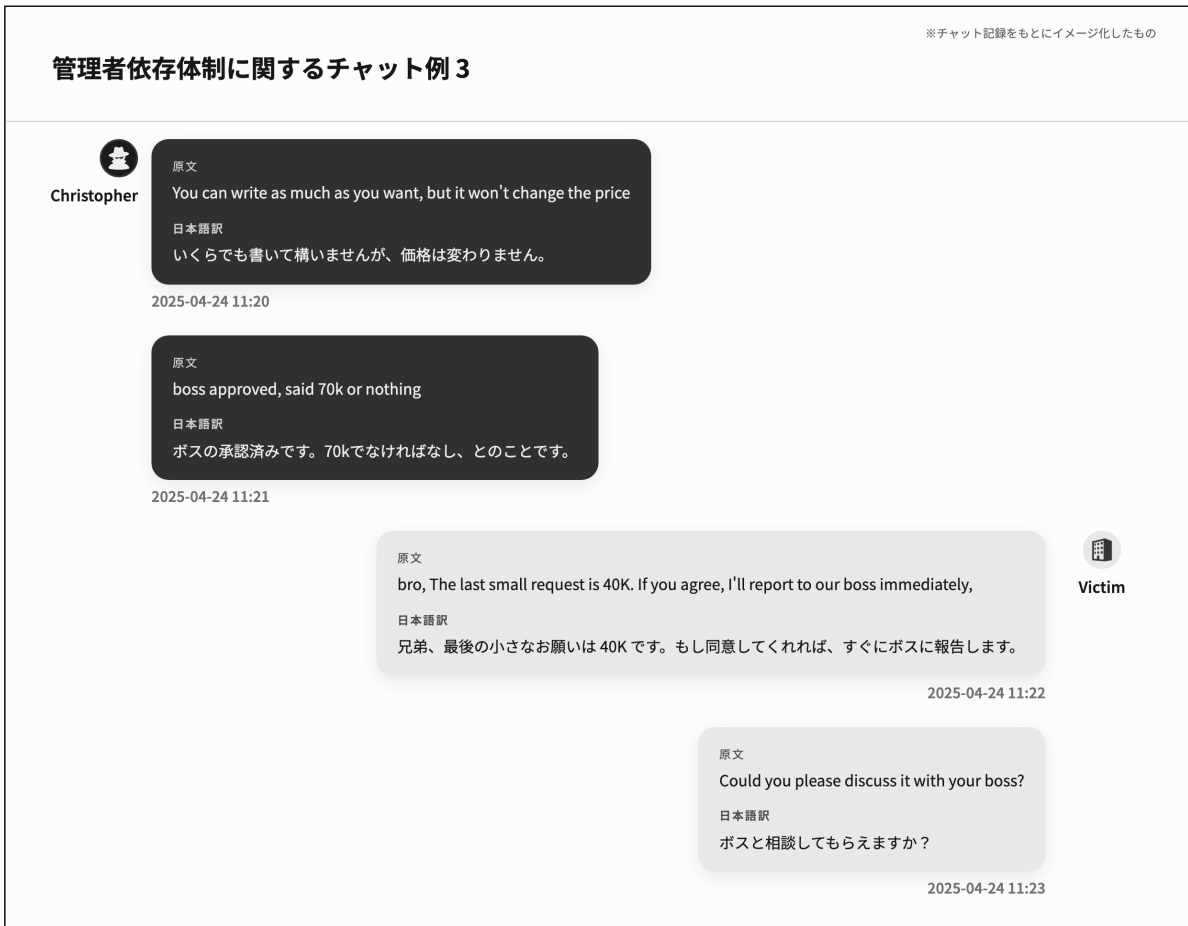


図 II-9-6: 管理者依存体制に関するチャット例 3 (原文抜粋)

復号ツールの生成権限が boss に集中する体制では、支払い後であっても対応に遅延が生じ得る。復旧計画は攻撃者のサポートに依存せずに進めることが望ましい。

9.3 パネルへの操作エラーと不正アクセス試行

system_invalid_requests テーブルには、パネル操作時に発生したエラーや不正なリクエストが記録されている。総件数は 3,245 件であり、その内訳を分析することで、パネルの運用実態と外部からの攻撃試行の両面が読み取れる。

図 II-9-7 は system_invalid_requests.message を対象にエラーメッセージ別の件数を集計したものである (マスキング後の全 6 区分)。

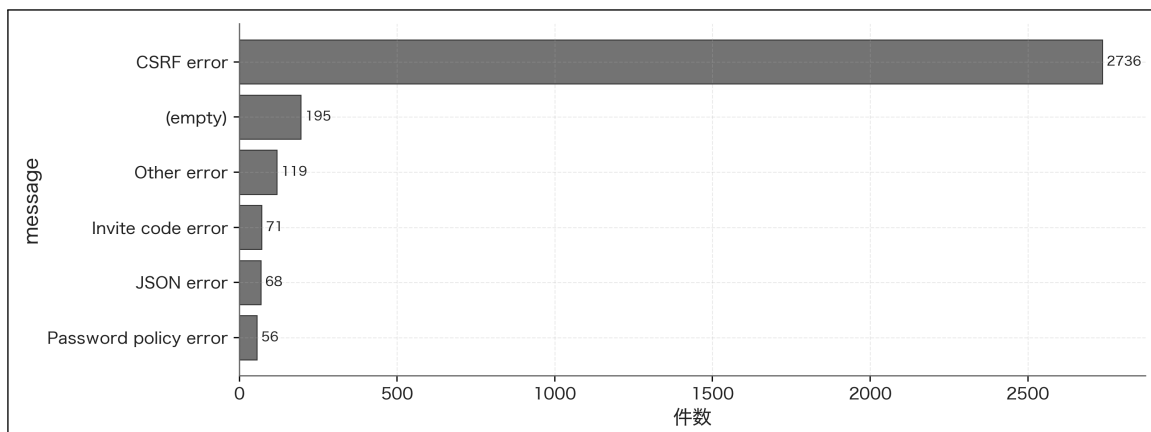


図 II-9-7: エラーメッセージ別件数 (全 6 区分)

エラーメッセージ別の件数を見ると、CSRF トークン不一致が全体の 84%を占める。CSRF トークン不一致 (2,736 件) はブラウザの戻る操作、タブ複製、セッション切れ等による正規ユーザーの操作ミスと外部からの不正アクセス試行の両方が含まれる可能性がある。件数の多さはパネルに対して継続的にリクエストが発生していたことを示すが、件数のみから主体や利用者数は推定できない。招待コード関連のエラー (71 件) は無効または期限切れの招待コードによる登録試行を示し、ブルートフォース試行も考えられる。パスワード強度不足 (56 件) はアフィリエイト自身が要件を満たさないパスワードを設定しようとした記録である。

外部からの攻撃試行の痕跡

リクエストパスの分析から、パネル自体が外部からの攻撃を受けていた形跡が読み取れた。表 II-9-1 はセキュリティ上注目すべきリクエストパスを示したものである。

表 II-9-1：セキュリティ上注目すべきリクエストパス

リクエストパス	件数	想定される探索・攻撃パターン (推定)
/reg?code[]=%27+r+1=1--s	5	デコードすると ' r 1=1-- s となり、SQL インジェクションでよく使われる 1=1 条件とコメントアウト (--) の組み合わせを含む。code[] の書き方から、配列パラメータの処理差分も併せて確認している可能性がある
/reg?code[]=	2	code[](角括弧内に空白) を空値で送信。サーバー側で配列として扱われるか、空白がどう正規化されるかを確認する意図と見られる
/reg?XMR'"	3	クォート ('"') を付与してエラーや入力の反射を誘発する探索。XMR は暗号通貨 Monero の略称だが、自動スキャナによる文字列の可能性もあり断定できない
/?s=index/index/index	3	MVC 系フレームワークで頻出するルーティングパターンの探索。特定のフレームワークに限らず、汎用スキャンとして出現する
/?wicket:interface=:0:userPanel...	4	Apache Wicket 固有の URL パターン。Wicket アプリが動作しているかの確認
/%2561%2573%2573%2565%2574%2573/	2	二重 URL エンコードで assets を難読化したパス。WAF やフィルタが二重エンコードを正しく検出するかを確認する意図と見られる
/reg?code=0	3	code に 0 を指定。同系列の空値や配列風パラメータと併せて、入力検証の処理を確認する一連の試行と見られる

特に /reg?code... のような入力はデコードすると ' r 1=1-- s となり、SQL インジェクションの探索でよく使われる ' or 1=1-- に類似したパターンを含むため、インジェクション系の探索入力である可能性がある。ただし外部からの探索に加え、正規ユーザーの操作ミスも含まれる可能性があることに留意が必要である。

リクエスト経路の分布

図 II-9-8 は system_invalid_requests.path を対象にリクエストパス別の件数を集計したものである (上位 10 件)。正規操作の誤作動と外部からの機械的アクセスが混在し得る。

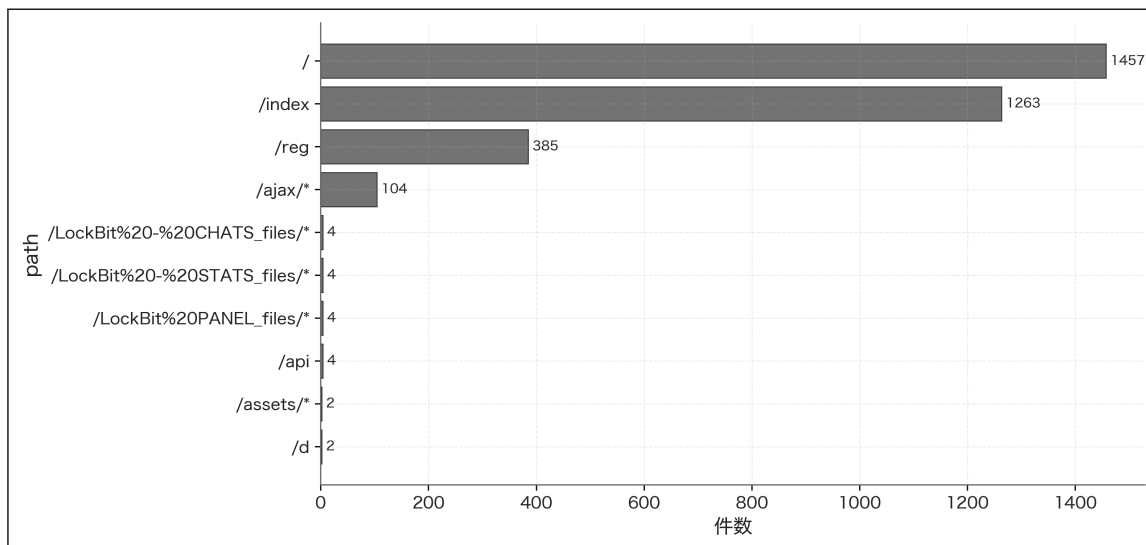


図 II-9-8: リクエストパス別件数 (上位 10 件)

パス分布では攻撃的な文字列だけでなく / や /index のようなトップページ系も上位を占めた。正規操作の誤作動と外部からの機械的なアクセスが混在している可能性を示す。

バックエンド構造の露出

エラーログの file フィールドにはバックエンドのファイルパスが記録されており、パネルの内部構造を推定できる。表 II-9-2 はバックエンド構成を示したものである。

表 II-9-2: バックエンド構成 (system_invalid_requests.file より)

ファイルパス	件数	役割 (推定)
/home/www/backend/functions.php	2,742	共通関数 (CSRF 検証含む)
/home/www/backend/backend/routes/reg.php	240	登録処理
/home/www/backend/core/Api.php	68	API 基盤
/home/www/backend/core/models/User.php	67	ユーザーモデル
/home/www/backend/backend/routes/ajax/builder.php	54	ビルダー機能
/home/www/backend/backend/web/router.php	34	ルーティング
/home/www/backend/backend/routes/ajax/settings.php	16	設定機能

このディレクトリ構成から、PHP アプリケーション本体が /home/www/backend/ 配下に置かれ、機能ごとに整理されていたことが読み取れる。routes/ は URL ごとに処理を振り分けるエンドポイント、models/ はデータベースとの読み書きを担当し、core/ は共通処理をまとめた層と見られる。画面・入力の受け口とデータ処理を分離する一般的な設計パターンに近い構成である。

攻撃者のパネル自体が外部からの探索・攻撃試行を受けていた痕跡があり、攻撃者側もまた、攻撃対象となり得ることが示された。

9.4 データベース設計の特徴

本節では migrations テーブルと socket_messages テーブルを中心に、パネルの開発経緯と運用状況を整理する。なお、データベースのダンプ上は外部キー制約が確認できず、参照整合性が DB 層で強制されていたかは不明である。

スキーマ変更の推移

migrations テーブルには、データベースの構造変更の履歴が 34 件記録されている。1 件の記録が 1 回の構造変更に対応し、それぞれに変更内容を示す名前が付けられている。記録期間は 2022 年 4 月 7 日から 2024 年 12 月 18 日までである。図 II-9-9 は migrations.created_at を対象に月別のスキーマ変更件数を集計したものである。

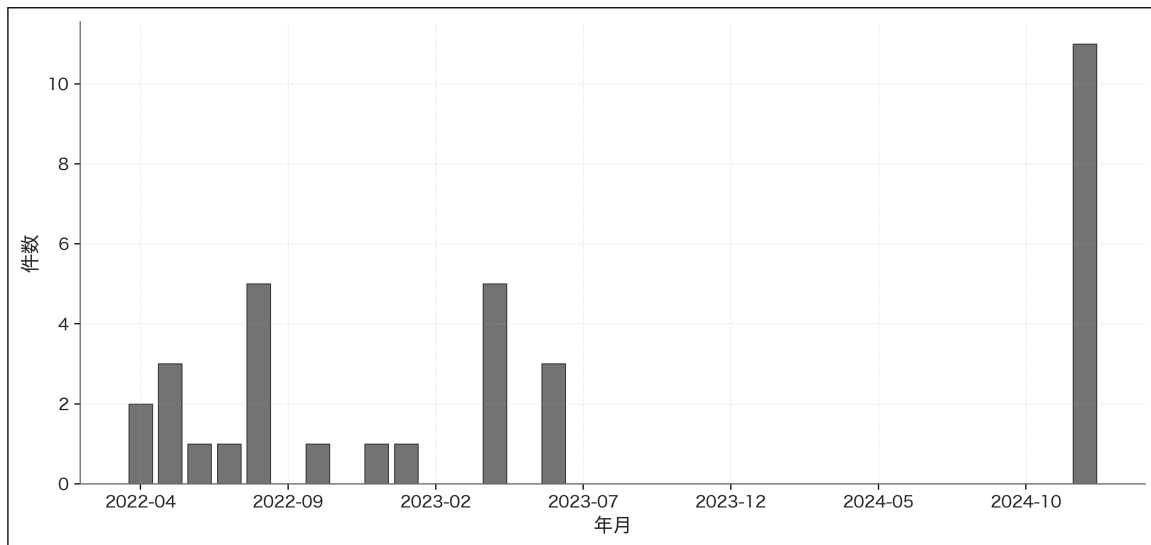


図 II-9-9: 月別スキーマ変更数

月別の推移を見ると、2022 年 4 月～2023 年半ばにかけて計 23 件の変更が記録されている。特に初期の 2022 年 4 月～8 月に 12 件(全体の約 35%)が集中しており、パネルの基本構造はこの時期に整備されたと見られる。その後、約 1 年半の空白期間を経て、2024 年 12 月に 11 件が集中した。この時期は Lite パネルの本格稼働(2024 年 12 月 18 日～)の直前にあたり、稼働に向けた準備と見られる。

図 II-9-10 はマイグレーション名のキーワードに基づき機能カテゴリ別に分類した件数を示したものである。

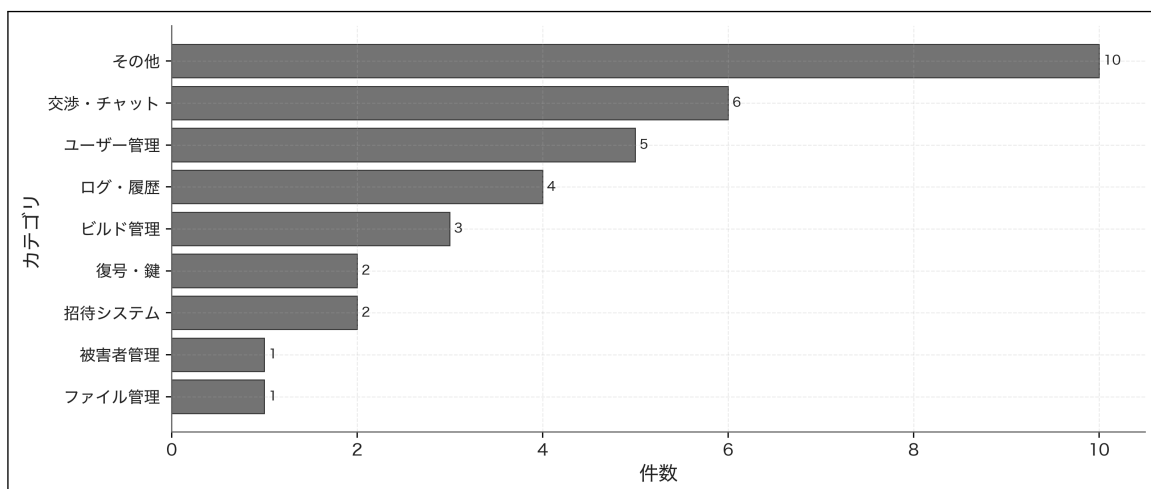


図 II-9-10: スキーマ変更のカテゴリ別件数

カテゴリ別分布では「交渉・チャット」(6 件)と「ユーザー管理」(5 件)が上位を占め、全体の約 3 分の 1 に達する。スキーマ変更の回数は開発工数を直接示す指標ではないが、この 2 領域で構造変更が相対的に多

く発生していたことが読み取れる。

操作ログの分析

socket_messages テーブルには、WebSocket 経由の操作ログが記録されている。残存するログは約 1 週間分 (2025 年 4 月 22 日～29 日) のみであり、それ以前のログはローテーションされていた可能性がある。図 II-9-11 は socket_messages.operation_type を対象に操作タイプ別の件数を集計したものである。

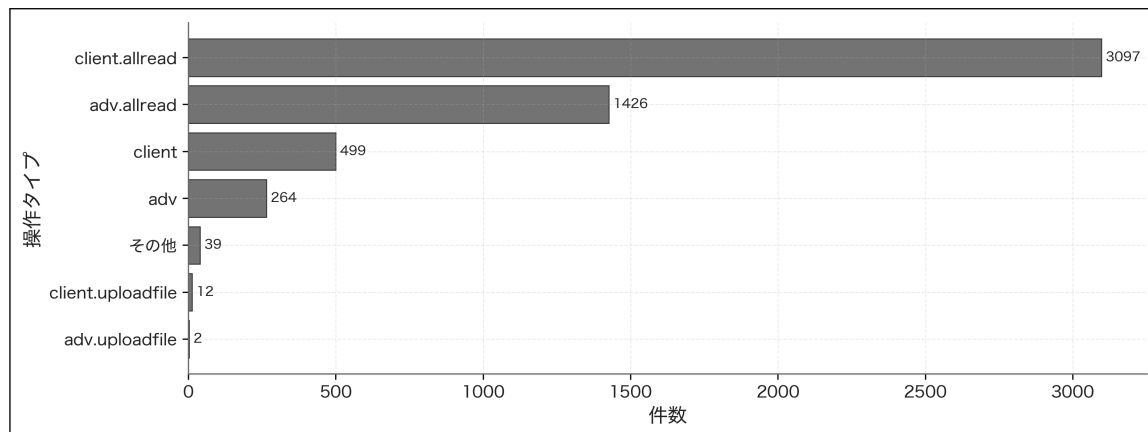


図 II-9-11: 操作タイプ別件数

図 II-9-12 は操作タイプ別の日別件数の推移を示したものである。

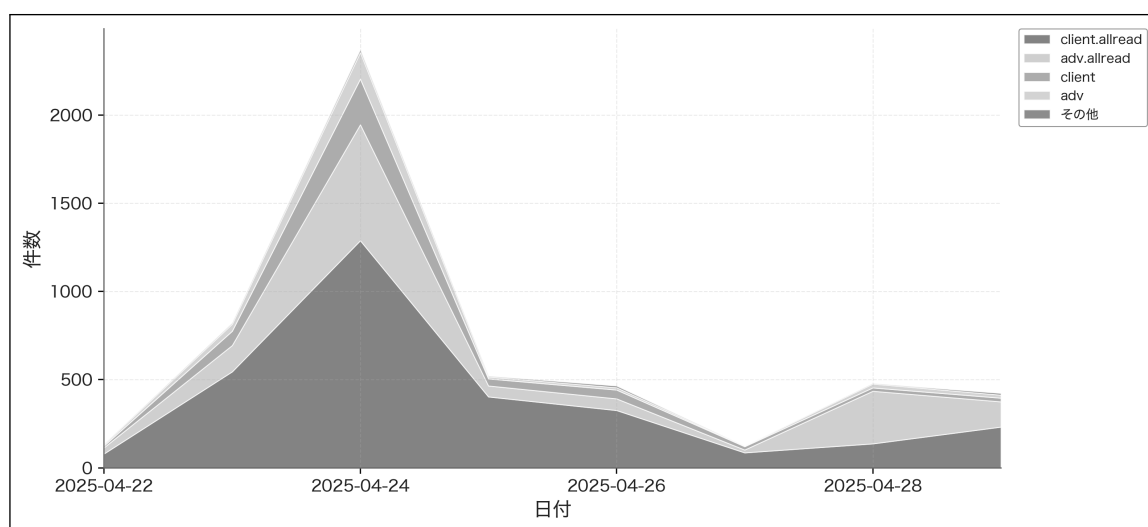


図 II-9-12: 操作タイプ別の時系列推移

操作タイプの内訳を見ると、allread (既読関連と推測される操作) が全体の約 85%を占める (図 II-9-11)。次いで「client」で始まる操作が「adv」で始まる操作の約 2 倍を占めた。client・adv はパネル内の操作対象を示すと見られるが、それぞれが被害組織情報・アフィリエイト情報のどちらに対応するかは断定できない。なお、操作名は socket_messages.request_data の JSON から {type}. {action} の形式で抽出した。人手による操作か自動処理かもこのログからは区別できない。

2025 年 4 月 24 日には 2,370 件の操作ログが記録され、観測期間 (4 月 22 日～29 日) の日次中央値 472 件の約 5.0 倍に達した (図 II-9-12)。なお、流出が確認されたのは 2025 年 5 月 7 日であるが、この増加との関連は本データの範囲では判断できない。

9.5 本章のまとめ

本章では、管理パネルの運用データから攻撃者側インフラの運営実態を分析した。主要な知見を以下に示す。

1. パスワードの平文保存と使い回し

アフィリエイトのパスワードは平文で保存されていた。パスワードポリシー (大文字・小文字・数字を含む 10~40 文字) は存在したが、ビルド用パスフレーズでは単純な文字列の使い回しが常態化していた。

2. boss 依存の運営体制

復号ツールの生成権限が boss に集中しており、不在時にはツール提供やテスト復号が遅延する属人化した体制であった。

3. 外部からの攻撃試行

エラーログには CSRF トークン不一致 (2,736 件) に加え、SQL インジェクションやフレームワーク探索と見られるリクエストが記録されていた。攻撃者のインフラ自体が外部からの探索対象になっていた可能性がある。

4. スキーマ変更時期の偏り

スキーマ変更は 2022 年に集中し、その後約 1 年半の空白を経て 2024 年 12 月の本格稼働直前にまとめて実施されていた。交渉・チャット機能とユーザー管理で構造変更の回数が相対的に多かった (件数は開発工数の直接的な指標ではない点に留意)。なお、ダンプ上は外部キー制約が確認できず、参照整合性が DB 層で強制されていたかは不明である。

攻撃者側インフラにも基本的な管理不備や属人化が存在しており、高度に統制された組織運営が行われていたわけではない。

10. チャットに記録された侵入経路・対策に関する言及

本章では、交渉チャットに記録された侵入経路や対策に関する攻撃者の言及を整理する。

弱いパスワード、VPN 製品の脆弱性、フィッシングなど初期侵入の要因と、AD 分離やバックアップ設計など侵入後の対策に関する助言が見られた。攻撃者の自己申告には牽制や誤誘導が含まれる可能性があり、あくまでチャット内容から読み取れる傾向として扱う。

10.1 初期侵入 (侵入の起点) に関する言及

チャット上で侵入要因として挙げられているのは、脆弱なパスワードや VPN 製品の脆弱性 (Fortinet 製品等) など、従来から指摘されている要因である。これに関連して、攻撃者が被害組織に対し最新アップデートの適用を推奨する趣旨の助言を行う例も見られた (助言の意図や真偽は一次データだけでは判断できない)。図 II-10-1～4 にその例を示す。



図 II-10-1: 弱いパスワードを侵入起点として伝えるチャット例 1 (原文抜粋)



図 II-10-2: 弱いパスワードを侵入起点として伝えるチャット例 2（原文抜粋）



図 II-10-3: 弱いパスワードを侵入起点として伝えるチャット例 3（原文抜粋）

※チャット記録をもとにイメージ化したもの

VPN製品の脆弱性に関するチャット記録

原文

- we will receive a deletion protocol- the assurance that Lockbit (including its affiliates) will not attack <MaskedVictimName> a second time- <MaskedVictimName> will not be published on their blog- we will receive information on how they got into the IT system

日本語訳

- 削除プロトコルを受け取る- Lockbit（その関連会社を含む）が<MaskedVictimName>を二度目に攻撃しないという保証- <MaskedVictimName>は彼らのブログに公開されない- ITシステムにどのように侵入したかの情報を受け取る



Victim

2025-04-16 09:55

原文

hello , did you received the btc ?

日本語訳

こんにちは、BTCを受け取りましたか？



Victim

2025-04-16 13:32

原文

Yes, wait for the answer to your request. We will prepare everything and send it to you shortly

日本語訳

はい、ご依頼への回答をお待ちください。すべて準備して間もなくお送りします



Swan

2025-04-16 13:33

原文

thank you very much

日本語訳

本当にありがとうございます。



Victim

2025-04-16 13:38

原文

1. <Masked:URL>2-3. We guarantee that we will not blog you or attack you again.4. We got into your network through a vulnerability in your FortiVPN.We recommend that you keep up to date with the updates of the products you use.

日本語訳

1.<Masked:URL>2-3. 私たちはあなたのデータを公開したり再攻撃したりしないことを保証します。4. FortiVPN の脆弱性を通じてあなたのネットワークに侵入しました。使用している製品の更新を常に最新に保つことをお勧めします。



Swan

2025-04-16 19:16

図 II-10-4: VPN 製品の脆弱性に関するチャット例（原文抜粋）

このほか、フィッシングを侵入の起点として伝えるケースも見られた。被害組織側が侵入経路を問う中で、内通者の存在を疑うケースも見られた。図 II-10-5～7 にその例を示す。

※チャット記録をもとにイメージ化したもの

フィッシングを侵入起点として伝えるチャット例 1

原文
Could you help me a bit, may I ask the details of how you got access to our network? Did you exploit our public web app server or phish our users?
日本語訳
少し助けていただけますか。どのように私たちのネットワークへアクセスしたのか詳細を伺ってもよいでしょうか。公開Webアプリのサーバーを悪用しましたか。それともユーザーをフィッシングしましたか。

Victim

2025-02-28 11:10

Christopher

原文
is fine, 20k confirm
日本語訳
大丈夫です。2万で確定します。

2025-02-28 11:11

原文
remove the admin from the domain who controls infostructure, no matter what antivirus you install, the domain will always be vulnerable
日本語訳
インフラを管理しているドメインの管理者を外してください。どんなアンチウイルスをインストールしても、ドメインは常に脆弱なままです。

2025-02-28 11:13

原文
got to you through phishing, but I don't remember the first host
日本語訳
フィッシングであなたの所へ到達しましたが、最初のホストは覚えていません。

2025-02-28 11:16

原文
and you had very easy passwords
日本語訳
そしてあなたは非常に簡単なパスワードを使っていました

2025-02-28 11:17

図 II-10-5: フィッシングを侵入起点として伝えるチャット例 1 (原文抜粋)

※チャット記録をもとにイメージ化したもの

フィッシングを侵入起点として伝えるチャット例 2

Christopher

原文
we got to you through phishing, captured the domain, and then the admin host <Masked:UserName>
日本語訳
フィッシングで貴社に侵入し、ドメインを制圧し、その後管理ホストの<Masked:UserName>を取得しました。

2025-04-24 14:55

図 II-10-6: フィッシングを侵入起点として伝えるチャット例 2 (原文抜粋)

105



図 II-10-7: フィッシングを侵入起点として伝えるチャット例 3 (原文抜粋)

弱いパスワード・VPN 製品の脆弱性・フィッシングは従来から指摘されている侵入経路であり、攻撃者の言及からも依然として有効であることが読み取れる。パスワード管理・VPN 製品の脆弱性対応・フィッシング対策を優先し、初期侵入対策と侵入後の横展開対策を併せて整備しておくことが望ましい。

10.2 侵入後活動 (横展開) と対策に関する言及

攻撃者が侵入後の活動 (横展開) に触れる中で、RMM ツール (AnyDesk 等) の悪用を示唆する発言も見られた。これは初期侵入の起点というより、侵入後フェーズの被害拡大要因として整理できる。RMM ツールの悪用により、攻撃者は管理者権限でのコマンド実行や横展開が可能となる。図 II-10-8 にその例を示す。

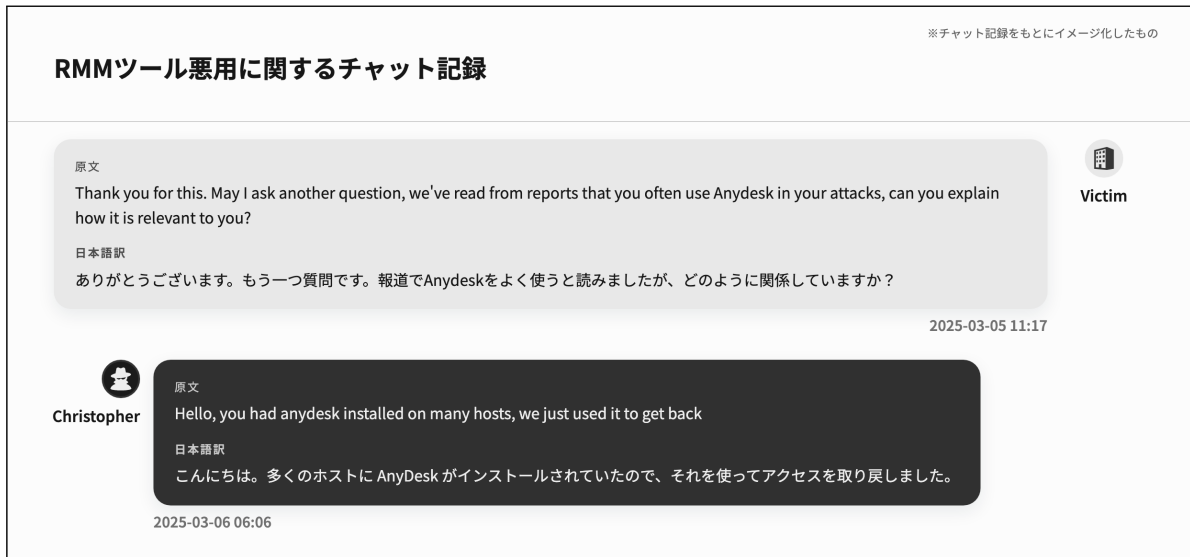


図 II-10-8: RMM ツール悪用に関するチャット例（原文抜粋）

攻撃者がチャット上で示した内容として、RMM を使用して内部ネットワークの偵察やバックアップシステムの無効化を実施した可能性が示唆されている。

また、攻撃者が被害組織に対し、AD 環境においてバックアップや NAS などの重要データを AD ドメイン (認証境界) から切り離すよう助言する場面も複数見られた。「ドメイン内でバックアップを管理しない」「管理者ホストをドメインから分離する」といった指摘が含まれる。バックアップや管理者ホストを AD 認証境界の外に配置することは、ランサムウェアによる復旧阻害への対策の基本方針とされている。図 II-10-9～10 にその例を示す。

バックアップ分離に関する助言のチャット例 1


Victim

原文
So our vulnerability is simply that the password was too weak?

日本語訳
つまり、当社の脆弱性は単にパスワードが弱すぎたということですか？

2025-02-16 10:27

Christopher



原文
host admin needs to be removed from the domain

日本語訳
ホスト管理者をドメインから外す必要があります

2025-02-16 10:28

Christopher



原文
and close the ports at the admin

日本語訳
管理側でポートを閉じてください。

2025-02-16 10:28


Victim

原文
Got it!! T H X !

日本語訳
了解!! サンキュー！

2025-02-16 10:30

Christopher



原文
<Masked:IP>

日本語訳
<Masked:IP>

2025-02-16 10:31

Christopher



原文
backups do not show in the domain

日本語訳
バックアップはドメイン上から見えないようにしてください

2025-02-16 10:32

Christopher



原文
and nas

日本語訳
NASも同様に

2025-02-16 10:33

Christopher



原文
domain is not a secure infostructure

日本語訳
ドメインは安全なインフラストラクチャではありません

2025-02-16 10:33


Victim

原文
Got it, we'll take this as a lesson learned. Thanks for the assistance.

日本語訳
理解しました。今回の件を教訓にします。ご支援ありがとうございました。

2025-02-16 10:34

図 II-10-9: バックアップ分離に関する助言のチャット例 1（原文抜粋）

バックアップ分離に関する助言のチャット例 2

**Christopher**

原文
remove the admin from the domain and make passwords better

日本語訳
ドメインから管理者を外し、パスワードをより強固にしてください。

2025-02-18 11:36

原文
and this will not happen again

日本語訳
そして、これが再発することはありません

2025-02-18 11:36

原文
thx

日本語訳
ありがとう

2025-02-18 11:37

**Victim**

**Christopher**

原文
one nas is not enough for backups it is very unreliable

日本語訳
バックアップに NAS 1台では不十分で、非常に信頼性が低いです

2025-02-18 11:39

原文
what is your good Suggestion

日本語訳
あなたの良い提案は何ですか

2025-02-18 11:40

**Victim**

**Christopher**

原文
at least hyper backup for nas to nas

日本語訳
少なくとも NAS 同士の Hyper Backup

2025-02-18 11:40

原文
2 nas backup we do not go to it from the domain

日本語訳
2台のNASバックアップは、ドメインからはアクセスしていません

2025-02-18 11:41

原文
if you don't want to spend a lot of money on security

日本語訳
セキュリティに多くのお金を使いたくないなら

2025-02-18 11:42

原文
everything in the domain is not safe

日本語訳
ドメイン内のすべてが安全ではありません。

2025-02-18 11:43

図 II-10-10: バックアップ分離に関する助言のチャット例 2 (原文抜粋)

さらに、全 Windows アカウントにおけるパスワードの複雑化、全サーバーへのアンチウイルス導入、ネッ

トワーク活動の嚴重な監視、アンチウイルス未導入端末でのサードパーティ製ソフト実行禁止などを推奨する発言も見られた。図 II-10-11 にその例を示す。

※チャット記録をもとにイメージ化したもの

セキュリティ助言に関するチャット例



umarbishop47

原文

Some tips to improve the security of your servers: First of all, to improve security, you need to change all Windows account passwords without exception. You need to change them to long and complex passwords. Secondly, you need to install antivirus software on all servers without exception (Kaspersky, Sophos, Bitdefender or other reliable antivirus software). You also need to more carefully monitor activity on the corporate network, look for unnecessary activity on the network (track traffic) and not run third-party software on machines without antivirus software.

日本語訳

サーバーのセキュリティを改善するためのヒントです。まず、例外なくすべてのWindowsアカウントのパスワードを長く複雑なものに変更してください。次に、例外なくすべてのサーバーにアンチウイルスを導入してください（Kaspersky、Sophos、Bitdefenderなど信頼できる製品）。さらに、社内ネットワークの活動をより注意深く監視し、不審なトラフィックを探し、アンチウイルスのない端末でサードパーティソフトを実行しないでください。

2025-02-04 13:17

図 II-10-11: セキュリティ助言に関するチャット例（原文抜粋）

こうした助言を「レポート」として提示し、交渉材料として支払い条件や金額に影響させようとする例も見られた。図 II-10-12 にその例を示す。

レポート提供と価格交渉のチャット例


lofikdis

原文
this price is 8,000 USDT

日本語訳
この価格は8,000 USDTです。

2025-03-26 04:19

原文
if u pay it completed within 72 hours,u can get discount

日本語訳
72時間以内に全額支払えば割引が受けられます。

2025-03-26 04:26

原文
only 6,000 USDT

日本語訳
6,000 USDTだけです。

2025-03-26 04:26

原文
We will never cheat our customers. Promise will definitely do it.

日本語訳
私たちは決して顧客をだましたりしません。約束は必ず守ります。

2025-03-26 04:26

原文
Are you able to help locate the system vulnerability, so they can protect themselves from further attacks

日本語訳
システムの脆弱性の特定を手伝えますか。そうすれば、さらなる攻撃から身を守れます。


Victim

2025-03-26 04:32


lofikdis

原文
If you want to buy intrusion paths and protection suggestions. A USDT of 10,000 must be paid.

日本語訳
侵入経路と防御の提案を購入したい場合は、1万USDTの支払いが必要です。

2025-03-26 04:33

原文
We will provide textual intrusion paths and defense advice for you.

日本語訳
侵入経路のテキストと防御の助言を提供します。

2025-03-26 04:34

図 II-10-12: レポート提供と価格交渉のチャット例（原文抜粋）

認証境界の分離、バックアップ設計、監視体制、RMM ツール統制は侵入後フェーズの被害拡大に直結し得る。バックアップや NAS が AD ドメインから適切に分離されているか、RMM ツールの利用実態を把握し許可制・監視を含む統制が取られているかを確認しておくことが望ましい。

10.3 本章のまとめ

本章では、交渉チャットに記録された侵入経路と対策に関する攻撃者の言及を整理した。主要な知見を以下に示す。

1. 初期侵入の要因

弱いパスワード、VPN 製品の脆弱性 (Fortinet 等)、フィッシングが侵入起点として言及されていた。いずれも従来から指摘されている要因である。

2. 侵入後の横展開とバックアップ破壊

RMM ツール (AnyDesk 等) の悪用が示唆されたほか、バックアップや NAS を AD ドメイン (認証境界) から切り離すよう助言する場面が複数あった。

3. 助言の交渉利用

セキュリティ対策の助言を「レポート」として提示し、交渉材料として支払い条件や金額に影響させようとする例も見られた。

これらの言及は攻撃者の自己申告であり、牽制や誤誘導が含まれる可能性がある。ただし、言及された対策 (パスワード強化・VPN 脆弱性管理・AD 分離・RMM 統制・バックアップ設計) は防御側にとっても基本的な施策であり、自組織の実装状況を点検する契機として活用されたい。

付録 A 分析の前提と制約

データの範囲

本レポートの一次データは、2025 年 5 月に流出した LockBit Lite パネルの運用データベースに限定される。主要アフィリエイトが使用するメインパネルのデータは含まない。

以下の情報は一次データからは確定できないため、本レポートでは断定していない。

- ・ 攻撃の実行日時 (ビルド日とは別)
- ・ Lite パネル以外で行われたオフライン交渉の内容
- ・ LockBit 全体の収益規模および攻撃総数
- ・ 被害組織の実被害規模・影響度

支払いや復号に至るケースのカウントは判断基準により一致しない場合がある。本レポートではその幅を許容する方針を取っている。

リークサイト掲載状況の確認は 2026 年 7 月末時点で実施した。実際のダンプ・掲載時期との間に時間差があるため、掲載の有無に関する数値はこの時点での観測値として解釈する。

また、system_invalid_requests や socket_messages 等の運用ログには誤操作・自動処理・第三者の探索が混在し得るため、単一指標から主体や意図を断定しない。

身代金要求額の集計 (6.2 節) では、精査対象 127 ドメインのうち 1 件を除外している。当該案件は被害組織欄がマルウェア研究サイトとなっており、チャット内容も「いくら払うか」という質問に対して 1 億 USD と答えるのみの短いやり取りであり、身代金要求の実態を反映していないと判断した。

集計定義

各セクションの数値は以下の定義に基づいて算出されている。

- ・ **被害組織数**：chats に記録のある client_id 208 件を正規化ドメインで名寄せし、example/test 系 5 件を除外した 127 組織。
- ・ **支払い定義 A**：clients.paid_commission > 0 に基づく支払い。本レポートでは 7 件。
- ・ **支払い定義 B**：チャット内容から支払いの可能性が高いと判断されるケースを含む定義。支払い定義 A の 7 件に 10 件を加えた合計 17 件。
- ・ **復号ツール受領**：支払い確認 (支払い定義 B) と旧 CIS 地域と見られる組織への無償提供などを合わせた 19 件。これら 19 件全ての復号成功が確認されたわけではない。
- ・ **リークサイト掲載**：LockBit のリークサイト上に被害組織の情報が掲載されたことを指す。
- ・ **BTC アドレス割り当て件数**：btc_addresses テーブルのうち target_id ≠ 0 の行数。本レポートでは 159 件。
- ・ **攻撃実行者の母数**：clients.advid 基準 (被害組織レコードを持つユーザー) と builds.userid 基準 (ビルド実行者) では対象が異なる。各章で採用した基準はその都度明記する。

判定基準一覧 (支払い・復号・リークサイト掲載)

支払い判定ごとの帰結をリークサイト掲載の観点で整理するにあたり、各軸の判定基準を以下に示す。

表 A-1：判定軸ごとの判定基準 (観測条件)

判定軸	判定基準	注意点
支払い判定 (定義 A)	clients.paid_commission > 0	DB フラグに依存し、チャット外決済は捕捉できない
支払い判定 (定義 B)	チャット本文の支払い完了表現＋文脈確認	推定を含むため過大/過小評価の余地がある
復号結果	チャット上の記述に基づき「成功／部分成功／失敗／不明」に分類	チャット未記載は「不明」として扱う
リークサイト掲載	観測時点 (2026 年 7 月末) のリークサイト掲載有無	未掲載は「将来も非掲載」を保証しない

データ終端による打ち切り (右側打ち切り) の影響

本レポートの Lite パネル由来データは 2025-04-29 で記録が終了している。この終端に近い時期に交渉を開始した被害組織は、その後の展開 (支払い、交渉再開、復号ツール提供、復号結果、チャットの継続等) を十分観測できていない可能性がある。これにより、チャット記録期間・支払い率などの指標が実態より下方または不明方向に偏る (右側打ち切り) リスクがある。

交渉開始からデータ終端までの追跡期間で母数を絞り、閾値を変えたときの推定値の変化を確認した (感度分析)。

表 A-2：チャット記録期間 (被害組織単位) の追跡期間別 75 パーセンタイル

追跡期間の閾値	母数	75 パーセンタイル
フィルタなし	127 件	約 397 時間
14 日以上	107 件	約 499 時間
30 日以上	90 件	約 633 時間
60 日以上	61 件	約 637 時間
90 日以上 (参考値、母数が少なく不安定)	34 件	約 1,342 時間

閾値を強めるほど 75 パーセンタイルが一貫して長くなっており、第 II 部第 5 章第 3 節で示したチャット記録期間 (特に 75 パーセンタイル) は打ち切りにより下方に偏っている可能性があり、実際のチャット記録期間はこれより長いと考えられる。

表 A-3：支払い率 (定義 B) の追跡期間別推定値

追跡期間の閾値	母数	支払い件数	支払い率
フィルタなし	127 件	17 件	13.4%
14 日以上	107 件	16 件	15.0%
30 日以上	90 件	12 件	13.3%
60 日以上	61 件	9 件	14.8%
90 日以上	34 件	5 件	14.7%

支払い率は閾値を変えてもいずれも 13～15% の範囲であり、第 II 部第 6 章第 5 節で示した支払い率 6% (DB フラグ基準)～13% (チャット推定基準) は、打ち切りによって大きく下方に偏っているとは言えない。

24 時間以内離脱率についても同様の確認を行ったが、追跡期間が短い被害組織ほど離脱率が低い傾向がみられ (打ち切りが離脱率を上げる方向には働いていない)、打ち切りによる系統的な偏りは見られなかった。

付録 B データセット概要(テーブル別レコード数など)

【第 II 部共通】章別分析定義サマリ (完全表)

章によって分析対象・分析粒度・支払い判定等の扱いが異なるため、読者が迷いやすいポイントを表に整理する。章をまたぐ比較や「件数／割合」の読み取りを行う場合は、本表の前提に従うこと。

表 B-1：章別分析定義サマリ

項目	第 1 章	第 2 章	第 3～7 章	第 8 章	第 9～10 章
被害組織の識別単位	月別掲載件数 (グループ全体)	正規化ドメイン (組織単位)	正規化ドメイン (組織単位)	正規化ドメイン (組織単位)	正規化ドメイン (組織単位)
対象データ源	リークサイト掲載情報 (CIG 集計)	Lite パネル由来 DB ダンプ	Lite パネル由来 DB ダンプ	Lite パネル由来 DB ダンプ + リークサイト掲載データ	Lite パネル由来 DB ダンプ
分析粒度	月単位	テーブル/レコード単位	章により異なる (本文で明記)	組織単位 (突合ベース)	章により異なる (本文で明記)
支払い判定	該当なし	paid_commission フラグおよびチャットログ	paid_commission フラグおよびチャットログ	paid_commission フラグおよびチャットログ	該当なし
複数ドメインの扱い	掲載件数ベースのため該当なし	ドメイン単位で計上 (組織数は過大集計の可能性)	ドメイン単位で計上 (組織数は過大集計の可能性)	ドメイン単位で計上 (組織数は過大集計の可能性)	ドメイン単位で計上 (組織数は過大集計の可能性)
欠損・曖昧データ	全体傾向から除外	レコード件数に含めつつ組織母数から除外	章ごとの算出条件に従う	突合不能は未掲載と同義ではない	章ごとの算出条件に従う

各章の数値は分析単位が異なるため、章をまたいで比較する際はその違いを考慮すること。割合 (%) は原則として四捨五入した整数 % で表記するが、感度分析・結合一致率・図中の内訳等、精度の確認が特に重要な箇所では小数第 1 位まで表記する場合がある。

主要テーブル件数一覧 (期間付き)

表 B-2：主要テーブルのレコード数と期間 (UTC)

テーブル名	レコード数	期間 (UTC)	備考
chats	4,423 件	2024-12-19 ～ 2025-04-29	交渉メッセージ総数
clients	246 件	2024-12-19 ～ 2025-04-29	パネル登録 ID 数 (テスト・重複を含む)
builds	1,183 件	2024-12-18 ～ 2025-04-28	ビルドレコード数
builds_configurations	1,183 件	2024-12-18 ～ 2025-04-28	builds と 1 対 1 対応

テーブル名	レコード数	期間 (UTC)	備考
invites	3,693 件	2024-12-18 ~ 2025-04-29	招待トークン発行数
users	75 件	2022-01-31 ~ 2025-04-22	アフィリエイト数。最古 の 2 件は管理者アカウ ント (2022 年作成)
files	1,015 件	2024-12-18 ~ 2025-04-28	管理ファイル数
visits	2,398 件	2024-12-19 ~ 2025-04-29	アクセスログ
socket_messages	5,339 件	2025-04-22 ~ 2025-04-29	最終週のみ記録
system_invalid_req uests	3,245 件	2024-12-18 ~ 2025-04-29	不正リクエスト
btc_addresses	59,975 件	(日付なし)	事前生成アドレス
news	5 件	2024-12-18 ~ 2025-03-30	お知らせ記事
migrations	34 件	2022-04-07 ~ 2024-12-18	開発履歴 (2 年半)

付録 C 金額抽出・採用ルール

金額抽出の概要

本レポートにおける身代金要求額・合意額等の金額データは、chats テーブルに記録されたチャット本文から抽出したものである。

対応通貨と抽出パターン

金額抽出は以下の 3 通貨を対象とし、それぞれ「通貨記号 + 数値」と「数値 + 通貨記号」の両方向パターンで検出する。

USD(米ドル)

- ・パターン 1: usd / us\$ / \$ + 数値 (例: \$50,000、USD 100000)
- ・パターン 2: 数値 + usd / us\$ / dollars (例: 50000 USD、100,000 dollars)

BTC(ビットコイン)

- ・パターン 1: btc / BTC + 数値 (例: BTC 0.5、BTC 1.2)
- ・パターン 2: 数値 + btc / BTC (例: 0.5 BTC)

XMR(モネロ)

- ・パターン 1: xmr + 数値 (例: XMR 10)
- ・パターン 2: 数値 + xmr (例: 10 XMR)

BTC → USD 換算ルール

BTC 建ての金額は、当該チャットメッセージの日付における BTC/USD 終値に基づき USD に換算した推定値を使用している。XMR については公開チェーンで同等の追跡検証が困難であるため、金額分析の主軸には含めていない。

金額の表示上の丸め

図表・本文で USD 額を表示する際は、可読性のため最も近い 1 USD に四捨五入し、3 桁区切りで表記する。これは表示上の処理であり、集計および計算には丸め前の値を用いる。

金額の採用ルール

同一被害組織 (正規化ドメイン単位) で複数の金額が確認された場合、以下のルールに従い代表値を決定する。金額の採用対象は攻撃者側が提示したメッセージに限定し、被害組織側の発言に含まれる金額は採用しない (被害組織側の希望額を採用すると要求水準を過小評価するため)。

- ・ **初回要求額**：各スレッド上で記録されている「初回の身代金要求額」を採用
- ・ **最終要求額 (合意額)**：各スレッド上で記録されている「最終的な要求額」を採用
- ・ **減額率**：初回要求額に対する最終要求額の減少割合として算出 (支払い成立を前提としない指標)
- ・ **推定獲得身代金**：支払い完了と推定できるケース (定義 B) について、支払い完了表現の直近に出現する金額言及を採用

同一組織内で追加の最大値・最小値集約は行わない。

図表における階級表記

図表中の範囲ラベルは、原則として左端を含み、右端を含まない階級を表す。例えば 10-20% は「10%以上 20%未満」、10k-50k は「10,000 USD 以上 50,000 USD 未満」を意味する。10%未満 や <10k は下限側の階級、90%以上 や $\geq 1M$ は上限側の階級を表す。

判定時に参照した情報

チャット内の交渉フェーズや決着状況の判定は、特定語の機械的な検知ではなく、スレッド全体の文脈を読んだうえで行っている。主に以下の情報を参照した。

- ・ **初回要求額**：攻撃者がスレッド内で最初に提示した金額を採用する。
- ・ **最終要求額**：攻撃者がスレッド内で最後に提示した金額を採用する。
- ・ **支払い完了判定**：被害組織側の支払い済みを示す発言、送金確認を求めるやり取り、暗号資産アドレスの提示、その後のツール提供有無など、前後の文脈を総合して判定する。
- ・ **支払い日時**：被害組織側が支払い完了を示した発言時刻を採用する。
- ・ **復号ツール提供判定**：チャット上のファイル共有を示す情報、ファイル名の記録、送付メッセージの内容を参照して判定する。
- ・ **復号ツール提供日時**：復号ツールの送付日時を採用する。
- ・ **キーワード表現**：paid、payment sent、txid、transaction id、tx hash、decryptor、decryption tool などの表現は、上記判定時の補助情報として参照した。

制約と注意事項

- ・ チャット外で行われたオフライン交渉や別媒体 (電話・メール) での合意額は含まれない
- ・ XMR による支払いやパネル外での決済による過小推定と、支払い判定・金額対応付けの誤りによる過大推定の双方があり得るため、推定獲得身代金は参考値として扱う
- ・ 金額のカンマ区切り (例：100,000) は数値として読み取っている
- ・ sent のような汎用的な表現は、ファイル送信等の文脈でも出現し得るため、単独では支払い完了の根拠とせず前後の文脈を確認している

付録D 参考文献

本レポートは、CIG が流出データを分析して独自に観測した事実を中心に構成しているが、法執行機関による摘発の経緯や LockBit 自身の活動再開表明等、一部の背景説明については公開されている外部の一次情報を参考にしている。該当箇所の参考資料を以下に示す。

- CISA・FBI 等共同勧告「Understanding Ransomware Threat Actors: LockBit」(<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a>)
- Europol：Operation Cronos(第 1～3 段階)に関する公表資料(<https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>)
- 英国国家犯罪局 (NCA)：2024 年 2 月の LockBit 基盤掌握に関する公表資料(<https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos>)
- 米司法省：Dmitry Khoroshev 氏に対する 2024 年 5 月の起訴公表資料(<https://www.justice.gov/archives/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware>)
- Check Point Research：2025 年 9 月の「LockBit 5.0」を掲げた活動再開表明に関する分析記事「LockBit 5.0: Ransomware Gang Returns in Force」(<https://blog.checkpoint.com/research/lockbit-returns-and-it-already-has-victims/>)
- ReliaQuest：2025 年 9 月の DragonForce・Qilin・LockBit によるランサムウェア「カルテル」結成に関する分析レポート「Ransomware and Cyber Extortion in Q3 2025」(<https://reliaquest.com/blog/threat-spotlight-ransomware-and-cyber-extortion-in-q3-2025/>)

