アンダーグラウンドフォーラムにおける初期アクセスブローカーの調査：市場動向と活動実態の分析

伊藤 祥梧 * 1,a)　海藤 十和 * 1　青砥 陸[2]　田辺 瑠偉[3]　インミンパパ[3]　吉岡 克成[3,4]

概要：初期アクセスブローカー（Initial Access Broker: IAB）は，企業や組織のネットワークへの不正アクセス手段（VPN，RDP 等）を販売する脅威アクターであり，ランサムウェア攻撃の初期侵入段階において重要な役割を果たしている．近年，IAB のアンダーグラウンドフォーラムにおける活動が活発化しているが，フォーラム内での取引の傾向やその行動特性に関する分析は限られており，その活動の実態は十分に解明されていない．本研究では，CrimeBB データセットから抽出した 10 フォーラム，16 年間（2008 年 2 月-2024 年 5 月）に及ぶ観測データから分類した初期アクセス販売投稿 2,134 件を対象に，IAB の活動を「市場視点」と「アクター視点」の二方向から包括的に分析する．市場視点の分析では，複数のフォーラムに投稿された IAB 投稿を対象として，アクセス種別，価格分布，標的地域・業種の定量分析を実施した．その結果，アクセス販売の平均価格は$15,263 ± 72,274 となり，極めて大きな価格分散を持つ市場特性が確認された．また，最頻出のアクセス種別は RDP（平均$3,540）であった．アクター視点の分析では，各 IAB アカウントについて，投稿内容，他ユーザからの評価，アカウントの活動期間・投稿回数などを分析した結果，932 の IAB アカウントの 66%が単一種別を販売するなど専門化の傾向が見られた．また，97%のアカウントは投稿数が 10 件以下であり，一部のアカウントが大多数の投稿を行い，他ユーザからの反応も集中していた．本研究の知見は，高リスクな IAB の特定や新たな脅威の早期検出に向けた脅威インテリジェンスの基盤となることが期待される．

キーワード：Initial Access Broker(IAB)，アンダーグラウンドフォーラム，活動分析

An Investigation of Initial Access Brokers on Underground Forums: Market Trends and Activity Analysis

Shogo Ito* 1,a)　Towa Kaidou* 1　Riku Aoto[2]　Rui Tanabe[3]　Yin Minn Pa Pa[3]
Katsunari Yoshioka[3,4]

Abstract:
Initial Access Brokers (IABs) are threat actors who sell unauthorized access methods (e.g., VPN, RDP) to corporate and organizational networks, playing a crucial role in the initial intrusion phase of ransomware attacks. While IAB activities in underground forums have increased in recent years, analysis of transaction trends and behavioral characteristics within these forums remains limited, and the actual nature of their activities has not been fully clarified. This study conducts a comprehensive analysis of IAB activities from both a **market perspective** and an **actor perspective**, using 2,134 initial access sales posts classified from observational data spanning 16 years (February 2008 – May 2024) across 10 forums extracted from the CrimeBB dataset. From the market perspective, we performed quantitative analyses of access types, price distributions, target regions, and industries across multiple forums. The results showed that the average price of access sales was $15,263 ± 72,274, confirming market characteristics with extremely high price variance. RDP was the most frequent access type, with an average price of $3,540. From the actor perspective, we analyzed each IAB account in terms of post content, user evaluations, account activity periods, and post frequency. The analysis revealed that 66% of the 932 IAB accounts specialized in selling a single type, indicating a trend toward specialization. Moreover, 97% of accounts had 10 or fewer posts, with a small number of accounts generating the majority of posts and attracting concentrated responses from other users. The findings of this study are expected to provide a foundation for threat intelligence aimed at identifying high-risk IABs and enabling early detection of emerging threats.

Keywords: Initial Access Broker(IAB), Underground Forum, Activity Analysis

1. はじめに

初期アクセスブローカー（Initial Access Broker, 以降では IAB）は，現代のサイバー犯罪エコシステムにおいて中核的役割を担う脅威アクターである．IAB は脆弱性の悪用や認証情報の窃取等により獲得された，標的組織のネットワークへの初期アクセス権をランサムウェアオペレーター等の攻撃者に販売することで利益を得ている．近年，IAB の活動は急速に組織化・専門化が進んでおり，サイバー犯罪のビジネス化を象徴する存在となっている．特にアンダーグラウンドフォーラムにおける活動が活発化しており，初期アクセス市場 (以降では IAB 市場) の動向を理解する上で，これらのアンダーグラウンドフォーラム上での IAB の活動の実態把握は重要である．

これまでに，特定のフォーラムにおける IAB の活動を監視し，観測期間中に多くの投稿を行った IAB の動向や，IAB 市場の概要についてのレポートが公表されている [1], [2], [3], [4], [5]．しかし，これらのレポートは観測対象のフォーラムや期間が限定的であり，IAB 市場全体の動向や IAB の行動特性を体系的に把握するには不十分である．さらに，IAB が販売するアクセスの特徴，活動期間，投稿頻度，市場からの反応といった詳細な行動特性についても十分に解明されていない．

IAB はランサムウェア攻撃における初期侵入の担い手として知られている．Gray ら [6] は Conti 集団の内部チャット分析により RaaS モデルを支える実態を，Van der Horst ら [7] は攻撃経路の不透明化への関与を明らかにし，Marion [8] はランサムウェアエコシステムでの専門化された役割を指摘している．しかし，これらの研究は IAB をランサムウェアエコシステムの一構成要素として扱っており，その活動実態や行動特性を中心的に分析していない．このため，IAB の実態をデータに基づいて体系的に分析した研究は存在しない．

そこで本研究では，IAB の広告活動が集中しているアンダーグラウンドフォーラムを対象とし，投稿内容の定量・定性分析を通じて IAB の行動特性と市場構造を解明する．具体的には，CrimeBB [9] データセットに含まれる 10 フォーラムの投稿データ（2008 年 2 月-2024 年 5 月）を対象として，既存手法 [10] により抽出された初期アクセスの販売を行う投稿（以降では IAB 投稿）2,134 件を定量・定性的に分析する．

本研究の分析は，以下の 2 つの観点から構成される．

- **市場レベル分析**：アクセス種別，価格，標的地域，連絡手段，フォーラムごとの違いなど市場全体の傾向を可視化・統計的に分析する．
- **アクターレベル分析**：投稿をアカウント単位で集約し，取り扱う商品特性，投稿活動の規模・頻度，市場からの反応などをもとに, IAB の行動特性と構造的パターンを明らかにする．

市場レベル分析では，初期アクセスの平均販売価格は $15,263 であったが，中央値は$421 となり，IAB 市場の高い価格変動性が示された．アクセス種別では RDP が最多取引かつ低価格である一方，Web Mail が高価格帯を形成する階層構造が判明した．標的分析では政府・金融機関が主要対象となり，重要インフラほど高価格で取引される傾向が明らかになった．地理的には北米が約 60%を占め，英語圏先進国への集中が確認された．アクターレベル分析では，932 の IAB アカウントを特定し，その行動特性を分析した結果，明確な構造的パターンが判明した．取扱アクセスでは 66%が単一種別に特化し，8 種類以上の多角化を行う IAB は 3.5%に留まる専門化主流の構造が確認された．販売投稿数では 70%超が 1 件のみ，97%が 10 件以下と大多数の IAB が少数回の投稿活動に留まるパターンが確認された．また，他ユーザからの注目度にも大きな格差があり，少数のアカウントに反応が集中する構造が確認された．これらの結果は，IAB 市場の構造的特徴と IAB の活動に関する包括的理解を提供するものである．

本研究の貢献は下記の通りである:

- 10 フォーラム，16 年間の観測データに基づく市場・アクター二層分析による大規模・長期的な IAB 実態分析
- アクセス種別の価格階層，業界・地域別標的特性など，不正アクセス市場の構造的特徴の明確化
- IAB の活動戦略分化，短期散発的活動パターン，外部プラットフォーム連携など，行動実態の解明

2. 用語説明と関連研究

2.1 用語説明

アンダーグラウンドフォーラムは 4 段階からなる階層的な情報構造を持つ．本研究で使用する CrimeBB データセットも以下の構造に基づいて組織化されている．

フォーラム (Forum)：個別のアンダーグラウンドサイト（例：Raidforum，XSS，Cracked 等）．本研究では 10 個のフォーラムを分析対象とする．

ボード (Board)：フォーラム上で管理者によって設定される，テーマごとの区画．一般的な議論や技術解説等のボードに加えて，違法商品の取引に関連するボードも存在する．

スレッド (Thread)：ボード上にユーザが自由に作成することができる，特定の話題に関するディスカッション単位．

---

*第一著者および第二著者は同等に本研究へ寄与した．

1 横浜国立大学/Yokohama National University
2 横浜国立大学大学院環境情報学府/Graduate School of Environment and Information Sciences, Yokohama National University
3 横浜国立大学大学院先端科学高等研究院/Institute of Advanced Sciences, Yokohama National University
4 横浜国立大学大学院環境情報研究院/Graduate School of Environment and Information Sciences, Yokohama National University
a) ito-shogo-yt@ynu.jp

IAB の販売活動では，通常 1 つのアクセス権につき 1 つのスレッドが作成される．評判や返信の分析を行う際は，同一スレッド内の投稿を用いる．

投稿 (Post)：スレッド上の個別のメッセージ．本研究の分析単位であり，IAB による販売広告や購入希望者とのやり取りが含まれる．

また，アクターレベル分析では以下のアカウント単位を用いて，IAB 投稿を 1 件以上行うアカウント（以降では IAB アカウント）を IAB に対応づけて分析を行う．

アカウント (Account)：フォーラム上で各ユーザに一意に割り当てられる識別単位であり，作成した投稿やスレッドが紐づけられる．

2.2 関連研究

ランサムウェアエコシステム研究における IAB の分析：ランサムウェア攻撃のビジネス化に伴い，IAB の存在とその役割に関する学術的関心が高まっている．しかし，既存の学術研究においては，IAB をランサムウェアエコシステムの構成要素として言及するものの，その活動実態を主要な分析対象とした研究は確認できない．Gray ら [6] は，大規模ランサムウェア組織である Conti の内部チャット記録を分析し，IAB が Ransomware as a Service（RaaS）モデルにおいて重要な役割を果たしていることを実証した．この研究により，アクセス権獲得を専門とするチームの存在と，IAB からアフィリエイトへのアクセス販売が組織的攻撃の基盤となっていることが明らかになった．ただし，この分析は単一組織の事例研究に基づいており，IAB の活動の一般的特性については言及されていない．Van der Horst ら [7] は，現代のサイバー犯罪エコシステムの構造変化が既存のアトリビューション手法の有効性を制約していると論じている．特に，IAB という中間業者の存在が攻撃者特定を根本的に困難にしており，従来の理論の再考が必要であると指摘している．しかし，この研究も IAB の活動パターンや市場構造の分析は行っていない．Marion ら [8] は，サイバー犯罪エコシステムの職業化において IAB が初期侵入の専門化アクターとして機能していることを概観している．この研究は，IAB がサイバー犯罪全体の効率化を促進している構造的要因であることを示唆しているが，実証的データに基づく詳細分析は実施されていない．

IAB の実態調査に関する産業レポート：セキュリティベンダーは，実際のアンダーグラウンドフォーラムデータに基づく IAB の活動実態を調査している．Cyberint [1] は 4 フォーラムを 2 年半観測し，主要国・業種の標的動向や組織規模の変化を示した．Cyjax [2] は 2024 年の四半期別市場動向を整理し，標的傾向やアクセス種別統計に加え，最も活発な 10 人の IAB の特徴を分析した．Outpost24 [3] は 2 つのフォーラムから 152 件の販売投稿を収集し，標的組織や購入者側の動向を分析し，実際のランサムウェアグループとの接触事例も報告している．Flare [4] は Exploit フォーラムを 3 ヶ月監視して 72 件のオークション型販売を確認し，IAB が他市場や Telegram からアクセスを調達している可能性を指摘した．Recorded Future [5] は IAB を「ランサムウェア攻撃を可能にする専門的地下産業」と位置づけ，ロシア語圏フォーラムにおけるオークション形式の販売実態を報告した．これらの報告はフォーラムデータに基づく貴重な知見を提供しているが，その制約として，多くが数ヶ月から 2 年程度の短期観測に基づいており，IAB の長期的行動や市場構造の変化を十分に捉えられていない．また，市場全体の統計に焦点が置かれることが多く，個別 IAB の行動特性や戦略差異の分析は限定的である．

本研究の位置付け：本研究は以下の点で既存研究と差別化される．第一に，2008 年 2 月から 2024 年 5 月までの 16 年間にわたる販売投稿 (2,134 件) と投稿者のアカウント (932 件) を分析対象とし，既存研究を大幅に上回る規模での分析を実現する．第二に，分析観点の包括性において，市場全体の傾向分析（市場レベル分析）と個別 IAB の行動特性分析（アクターレベル分析）を組み合わせた二層構造の分析を行う．以上により，本研究は IAB の活動実態と IAB 市場の構造を実証的データに基づいて体系的に明らかにする初の学術的試みである．

3. 分析手法

本研究は，IAB の活動実態を包括的に解明するため，市場レベルとアクターレベルの二層構造分析を採用する．市場レベル分析では IAB 市場全体の傾向を定量的に把握し，アクターレベル分析では個別 IAB の行動特性をプロファイリングする．これらにより，市場構造と個別アクターの戦略的行動の両面から IAB の活動実態を明らかにする．

3.1 データセットと前処理

本研究で用いるデータは，既存の犯罪関連フォーラムデータセットである **CrimeBB** [9] に基づいており，10 個のアンダーグラウンドフォーラムから収集された投稿のうち，論文 [10] で提案した IAB 投稿分類システムを用いて，初期アクセス販売の投稿を抽出したものである．このシステムは，BERT と LLM の 2 層構造により IAB 関連投稿を検出した後，LLM を用いて英語の販売投稿の抽出と構造化を行う．抽出される情報は以下の通りである．

- アクセス種別：アクセスに用いられる手段 (RDP, shell など)
- アクセスレベル： システム内部での権限の強さ（Domain Admin, User など）
- 標的組織： 標的組織の名称，情報 (○○ company, xxx.com など)
- 標的地域：標的組織の場所に関する情報 (Asia, United States など)

表 1 各情報が投稿から抽出された割合

情報名	割合
アクセス種別	100%
アクセスレベル	31.65%
標的組織	30.72%
標的地域	28.60%
標的組織の業種	22.38%
標的組織の収益	5.90%
販売価格	36.25%
連絡手段	53.91%

- 標的組織の業種： 標的組織が属する産業に関する情報 (energy, goverment など)
- 標的組織の収益： 標的組織の収益（規模）に関する情報 ($2M, € 3kk など)
- 販売価格： 広告内に提示されている価格（$2,000, 0.1BTC など）
- 連絡手段： 購入者が販売者に連絡するための手段 (Private Message, Telegram など)

投稿から各情報が抽出されている割合を表 1 に示す．抽出はアクセス種別を基準として実施され，投稿から得られた各アクセス種別（例：RDP）に対し，標的組織と価格を対応付ける形で情報を抽出している．複数のアクセス種別を組み合わせて提供する販売投稿が存在するため，1 つの投稿からアクセス種別ごとに抽出を行った後，価格情報が同一かつ他の情報の文字列一致率が 8 割を超えるものについては併売品として統合する．例えば次の投稿が存在する場合：「*Selling access for XXX. Access includes:RDP, shell $500.*」，その抽出結果は：{ アクセス種別：RDP, 価格：$500, 標的組織：XXX}, { アクセス種別：shell, 価格：$500, 標的組織：XXX} であり，最終的な統合処理は次の通りである：{ アクセス種別：RDP・shell, 価格:$500, 標的組織: XXX}.

また，複数の標的に対するアクセスを一括販売する投稿も存在する．こうした複数アクセス・複数対象の販売については，個別アクセスの価格算出が困難であるため，本研究ではアクセス単位ではなく販売品目単位での分析を行った．各投稿には我々が抽出したこれらの情報に加え，CrimeBB に付随している投稿者，投稿日時，投稿先 (フォーラム，ボード，スレッド) といったメタ情報が存在している．なお，標的組織の収益，及び販売価格については複数の通貨が混在しているため，投稿日時のレートを用いて US ドルに統一している．対象期間は 2008 年 2 月から 2024 年 5 月で，抽出された IAB 投稿は 2,134 件であり，得られた販売品目数は 2,458 件である．

3.2 市場レベル分析手法

IAB 市場の構造と価格形成メカニズムを理解するため，投稿から抽出した情報（アクセス種別，販売価格，標的地域・業種）について，頻度分布と基本統計量（平均値，中央値，標準偏差等）を算出した．分析は以下の 3 つの観点から実施した：(1) IAB 市場に関する基礎統計（英語投稿数，IAB 投稿数，価格分布），(2) アクセス種別に関する分析，(3) 標的情報と価格の相関分析である．価格分析においては，単一アクセス種別のみを対象とした単体販売と複数アクセスを組み合わせたマルチアクセス販売を区別し，各アクセス種別の純粋な市場価値を評価した．

3.3 アクターレベル分析手法

個別 IAB の行動特性を把握するため，アカウント情報と投稿内容に基づく，プロファイリング分析を行った．

この分析を行うためには，個々のアカウントが投稿したものを分別して収集する必要がある．CrimeBB データセットは creator_id を用いることで，アカウント名の変更に対しても追跡が可能となっているが，creator_id が付加されていない（値が-1 となっている）場合が存在するため，creator_id のみを用いて投稿を分別することはできない．そこで，アカウント名の変更にも対応して同一ユーザの投稿を正確に収集するため，以下の手順を用いた．

(1) **初期収集**
投稿には `creator`（投稿時点のアカウント名）と `creator_id`（一意の内部 ID）が付与されている．まず `creator` をキーに投稿を収集し，そこから有効な `creator_id`（-1 以外）を抽出する．

(2) **名前変更の追跡**
同じ `creator_id` に紐づく別名が存在する場合は，その名前でも投稿を検索し直す．例：`creator_id = 42` に属する投稿に「Alice123」と「CyberQueen」が含まれていれば，両方の名前を使って投稿を収集する．

各 IAB アカウントに対する分析対象の指標は，取扱アクセス種別の傾向・多様性，販売価格帯，標的地域・業種の偏り，アカウントの活動期間・投稿頻度，他プラットフォームへの誘導状況，および他ユーザからの評判である．

評判分析では，IAB の投稿に対する返信を収集し，返信数と感情分析ツール VADER [11] による感情極性を用いて市場からの反応を定量化した．対象は初期アクセスの販売投稿が含まれているスレッド内にある全投稿であり，返信対象の特定は，投稿内でのアカウント言及，引用投稿の存在を優先し，これらが不明な場合はスレッド作成者への返信として判定している．

4. 市場動向と活動実態の分析

4.1 IAB 市場に関する分析

IAB 市場の分析結果の統計情報を表 2 に示す．これを見ると，IAB の活動の規模にはフォーラム間で大きな差があることが分かる．特に nulled は 333 アカウント，570 投稿と突出しており，2015 年から 2024 年にわたって継続的に観測されている．一方，blackhatworld は 2008 年から

データが存在するフォーラムであるが，IAB 投稿は相対的に少なく，主用途が異なることを示唆している．さらに，raidforums（2017 – 2022）の閉鎖後には，breached（2022 – 2023）や breachforums（2023 – 2024）が出現し，短期間ながらも多くの IAB による取引が行われていたことが確認できる．一方で, lolzteam や ogusers では IAB 関連の投稿数が少なく，本研究の対象範囲における活動は限定的であった．

価格分析の結果においてもフォーラム間で差異が確認された．breached では, 平均価格$30,585（標準偏差$221,929）に対して中央値$200 と極端な乖離があり，少数の高額投稿が市場全体の平均値を押し上げていることが示された．nulled でも，平均価格$3,170（標準偏差$33,897）に対して中央値$12 であり，大半が低価格取引で占められていた．また，cracked と blackhatworld では平均価格がそれぞれ $156，$294 と低価格帯に集中している一方で，breachforums と xss は平均価格が$4,000 – 5,000 台，中央値$600 – 800 台と，中価格帯を中心とする分布を示していた．以上から，IAB 市場は標準偏差が平均価格を大きく上回る高い価格変動性を特徴とし，大多数の低価格取引と少数の高額取引によって二極化した市場構造を形成していることが明らかとなった．

4.1.1 アクセス種別に関する分析

アクセス種別ごとの取引件数と価格帯を分析した結果を表 3 に示す．ここで「Unknown Type」とは，投稿から抽出されたアクセス種別が「Access」等の明示的でないものだった場合を指す．また,「マルチアクセス」は，複数のアクセス種別が併売されている販売品目を指す．

単体販売では，RDP が 700 件（うち価格情報あり 341 件）と最多の総件数を占めており，中央値が$17.73 と低価格帯に集中していることが確認できる．これに対し，Web Mail は，価格情報のある 54 件のうち中央値$800 と高価格帯を形成している．Shell アクセスでは総件数 209 件，価格情報 61 件で最高価格$2,000,000 という極端な高額取引が確認された．マルチアクセス販売では，635 件中 91 件で価格情報が得られ，中央値が$300 となっている．最高価格 $1,154,104 の高額投稿の存在や平均価格$19,046 は単体アクセスと比較して高水準にあり，複数のアクセス種別の組み合わせによる価値の向上を示している．

4.1.2 標的情報と価格相関分析

標的組織の業界別価格特性と地理的分布について分析を行った．表 4 に業界別の価格統計を示す．業界別分析の結果，政府機関が総件数 126 件と最多であり，そのうち 77 件で価格情報が得られ，中央値$450 と中価格帯に位置していた．さらに，金融業では 120 件中 19 件と価格情報は限定的であるものの，中央値$1,200 と最も高水準を示し，最高 $2,000,000 の極端な高額取引も観測された．また，エネルギー産業も中央値$1,100 と高額水準にあり，これらの政府機関・金融業・エネルギー産業といった公共性・社会基盤性の高い領域では，他業種に比べて価格が高い傾向が確認された．地理的分析では，米国が 113 件と最多であり，カナダ（47 件），オーストラリア（21 件），英国（20 件），ドイツ（17 件）が続いた．特に北米地域（米国・カナダ）が全体の約 60%を占めており，IAB 市場における標的が英語圏先進国に集中していることが明らかとなった．

4.1.3 市場分析結果のまとめ

市場分析で得られた知見を以下にまとめる．

- 市場全体では平均値と中央値の乖離が顕著であり，大多数の低価格取引と少数の高額取引による二極化構造が確認された．この傾向は，標準偏差が平均価格を大きく上回るという高い価格変動性にも表れている．
- アクセス種別の分析では，RDP が取引件数において最多（700 件）を占める一方，価格は低水準（中央値 $17.73）に集中していた．これに対し，Web Mail は取引件数は限定的であるが中央値$800 と高価格帯を形成しており，アクセス種別ごとに明確な価格差が存在することが示された．また，マルチアクセス販売は単体販売と比較して高価格であり，複数のアクセスを組み合わせることによる価格の上昇が確認された．
- 標的組織に関する分析では，政府機関（126 件）および金融業（120 件）が主要な対象となっていた．特に，金融業およびエネルギー産業といった重要インフラ領域は中央値$1,100〜$1,200 の高価格帯を示しており，社会基盤性の高い組織ほど高額で取引される傾向が明らかとなった．さらに，地理的分布の分析では，北米（米国・カナダ）が全体の約 60%を占め，標的が英語圏先進国に集中する傾向が確認された．

4.2 IAB のプロファイリング分析

本章では, IAB についてアクターレベルから分析を行う．前章で市場全体の構造を明らかにしたのに対し, 本章では各 IAB の投稿内容, フォーラム内での評判，活動形態などに基づいて行動や特徴を明らかにすることを目的とする．

4.2.1 取扱アクセス分析

各 IAB アカウントが取り扱っているアクセスの種類数を分析した結果，全体の 66%を占める 622 アカウントが 1 種類のみを扱っており，多くの IAB が単一のアクセス種別に依存する傾向が見られた．一方で，33 アカウントは 8 種類以上のアクセス種別を取り扱っており，多様な手口を展開する IAB の存在も確認された．このことから，IAB には「特定手口への特化」を基本とする大多数と「多角化戦略」を採用する少数という異なる戦略アプローチが存在することが明らかになった．

4.2.2 評判とコミュニティの反応

フォーラム上で他ユーザから受けた返信に基づき，IAB の評判を (1) 販売スレッドに対する返信者数，(2) IAB に

表 2　データセット基礎統計情報

フォーラム名	開始日	終了日	英語投稿数	IAB 投稿数	アカウント数	平均価格 ± SD (USD)	中央値 (USD)
blackhatworld	2008/02	2024/05	11,682,520	276	148	294 ± 794	28
breached	2022/03	2023/03	525,724	198	93	30,585 ± 221,929	200
breachforums	2023/06	2024/02	258,301	372	140	4,937 ± 19,242	600
cracked	2018/12	2022/10	1,844,858	79	21	156 ± 193	106
lolzteam	2016/08	2019/04	2,180,581	9	8	19,372 ± 27,393	19,372
nulled	2015/05	2024/02	4,667,283	570	333	3,170 ± 33,897	12
offensive-community	2013/03	2018/11	147,861	127	15	540 ± 550	450
ogusers	2017/06	2019/03	2,781,838	33	24	63,220 ± 249,823	18
raidforums	2017/03	2022/01	1,065,590	188	59	25,495 ± 158,650	10
xss	2019/04	2023/03	30,158	282	91	4,857 ± 10,265	800
ALL	2008/02	2024/05	25,184,714	2,134	932	15,263 ± 72,274	421

表 3　アクセス種別ごとの販売価格統計（USD）

アクセス種別	総件数	価格あり	最高価格	平均価格	中央値
RDP	700	341	1,000,000	3,540	17.73
Unknown Type	215	82	184,075	8,176	496.28
Shell	209	61	2,000,000	36,401	100
Webshell	103	27	4,000	409	100
Web Mail	72	54	50,000	2,231	800
VPN	45	28	9,000	1,092	500
cpanel	42	26	6,500	649	525
マルチアクセス	635	91	1,154,104	19,046	300

表 4　業界別販売アクセスの価格統計（USD）

業界	総件数	価格あり	最高価格	平均価格	中央値
政府機関	126	77	150,000	4,831	450
金融業	120	19	2,000,000	118,439	1,200
教育機関	38	16	2,000	545	175
医療機関	18	9	327,294	36,627	130
エネルギー産業	14	5	50,000	10,980	1,100
電子産業	6	5	1,600	910	700

対する返信の感情 (ポジティブ/中立/ネガティブの割合) に基づいて分析する．

各アカウントが作成した初期アクセス販売を行うスレッドに対する返信者数を分析した結果（588 アカウント対象），返信者数の分布は大きく偏在していることが判明した．全体の 76.9%（452 アカウント）が平均返信者数 3 名以下であった一方，5 名以上の返信者を集めるアカウントは 12.1%（71 アカウント），10 名以上では 5.1%（30 アカウント）存在しており，コミュニティ内での注目度に大きな格差があることが確認された．

IAB に対する返信の感情を分類した結果，ポジティブが 10,336 件と最も多く，次いで中立が 7,534 件，ネガティブは 1,855 件にとどまった．この結果から，多くの返信が肯定的あるいは中立的であり，否定的な反応は相対的に少数であることが分かる． また，10 件以上の返信を受けた 136 アカウントを対象とした個別分析では，大多数のアカウントがポジティブな返信を多く受けている一方で，ネガティブな返信の割合が高いアカウントも一部存在することが確認された．これにより，IAB 間でコミュニティ内での評価に差異があることが示された．

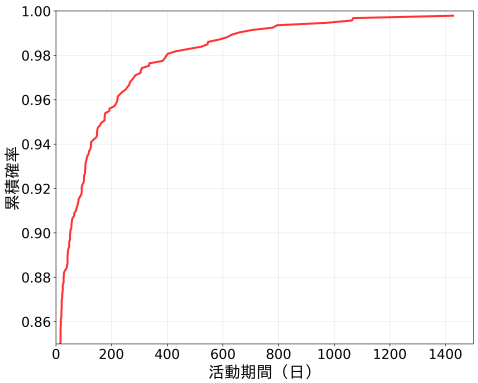

図 1　IAB アカウントの推定活動期間の累積分布 (CDF)

4.2.3　アカウントの活動パターン

IAB アカウントの活動期間を推定し，(1) 最初と最後の IAB 投稿間の時間差（活動期間）と (2) 投稿回数 の 2 つの指標から分析する．

それぞれ IAB アカウントの活動期間，及び販売投稿回数の分布を図 1 と図 2 に CDF 曲線により示す．これらの図は，重要な分布変化が観察される範囲に焦点を当てるため，軸範囲を限定して表示している．活動期間については，約 90%のアカウントが 50 日未満の短期的な運用であることが示され，1 年を超えて活動しているアカウントは 3%未満であることが確認された．販売投稿数については，全体の 7 割を超えるアカウントが 1 件のみの販売投稿を行っており，10 件以下の投稿を行うアカウントが 97%を占めることが明らかになった．

4.2.4　他プラットフォームへの誘導

投稿内で言及されている情報から，各 IAB がどの程度外部サービスに依存しているかを分析する．図 **??**は，各 IAB が言及している private message, reply のような内部サービスを除いた連絡手段の種類数を表している．各アカウントで言及されている連絡手段を調査した結果，46.5%のアカウントが外部の連絡手段（SNS や暗号化通信アプリなど）を利用していることが判明し，IAB 市場の実態がアンダーグラウンドフォーラム上だけに止まっていないことが示唆された．個別の連絡手段としては，Telegram(165

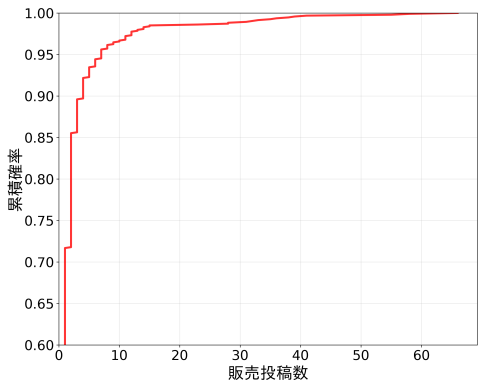

図 2 IAB の販売投稿数の累積分布 (CDF)

件) や Discord(108 件) といった SNS が最も多く言及されていることが明らかとなった．その他には，フォーラムの機能である private message の他，jabber，tox，xmpp のような通信プロトコルを指定するものも多く確認された．

4.2.5 プロファイリング結果のまとめ

プロファイルングで得られた知見を以下にまとめる．

- 活動戦略の分化: 取扱アクセス種別について，全体の 66%が単一種別への特化を示す一方，8 種類以上を扱うアカウントが 3.5%存在し，異なる活動戦略による明確な分化が確認された．
- 短期活動パターン: 活動期間は 89.2%のアカウントが 50 日未満であり，かつ販売投稿数については 70%超のアカウントが 1 件のみとなっており，大多数のアカウントが短期間での少数回活動を行っている．
- コミュニティ内での注目度格差: 返信者数分析において，76.9%が 3 名以下である一方，10 名以上の返信者を集めるアカウントが 3.5%存在し，IAB 間でのコミュニティ内影響力の格差が確認された．
- コミュニティ内評価の多様性: 全体的にはポジティブな反応が過半数を占めるものの，個別アクター分析では評価の著しく低いアカウントも存在し，IAB 間で信頼度に明確な差異が認められる．
- 外部プラットフォームとの連携: 46.5%の IAB が外部連絡手段を利用しており，特に Telegram と Discord が主流となっており，IAB 市場がフォーラム外へも拡張していることが確認された．

5. ケーススタディ

5.1 販売から攻撃実行までの追跡事例

2021 年 8 月 9 日，XSS フォーラムにおいてパキスタンの政府機関へのアクセスが$26,000〜$30,000 という高価格で販売される投稿が確認された．この投稿に対し，8 月 12 日にあるアカウントが”interested. DM me.”と返信し，購入への関心を示した．8 月 14 日，当該政府機関においてシステム停止が発生した．当局は当初，データ移行作業時の技術的不具合が原因であると発表していたが，翌 15 日にはパキスタンの主要メディアがサイバー攻撃によるものとして報道した．同日，アクセスを販売していた IAB は”Sold. Is in news now.”と投稿し，販売したアクセスを利用した攻撃が実際に発生し，それがニュースとして報道されていることを示唆した．

この事例は，投稿された時期と該当組織で報告されたサイバー攻撃インシデントの発生時期に整合性が見られ，実際の攻撃活動と IAB によるアクセス販売の関連性を示唆する貴重な事例となっている．

5.2 日本を標的とした事例

日本を標的とした初期アクセス販売は 7 件確認された．標的組織の詳細が明記されている事例として，年商 10 億ドル規模のグローバル企業の日本支社への VPN・RDP 販売や，実在する企業名を含む複数種別アクセス（管理者権限・データベース・FTP 等）の販売があった (例：”I am selling access to a***s Japan. Access is limited to: Store-front Admin, MySQL, GMO & FTP. Price is set to $400”)．その他には日本企業を標的とした RDP 販売や SMTP 販売等が確認された．7 件という限定的な件数は，日本が IAB にとって主要な標的地域ではない可能性を示唆している．しかし，大手企業への複合的なアクセス販売から一般的な RDP 販売まで，様々なレベルでの攻撃を想定したアクセス提供が確認された．

6. 考察

6.1 IAB 市場の構造と動態

本節では， 4.1 節で得られた IAB 市場の構造とその動態について考察する．価格は二極化しており（中央値 $421，最高 $2,000,000），大きな分散は攻撃者の目的と技術力の多様性を反映した結果だと考えられる．すなわち，低価格帯は低スキル層による雑多な販売，高価格帯は高度な技能・運用能力を備えた重要販売に対応する．地理・業界別には北米が約 60%を占め，政府（$450），金融（$1,200），エネルギー（$1,100）が高価格で，標的価値の評価が価格に反映された．アクセス種別では，RDP が最多（700 件）で低価格，Web Mail は高価格であるなど，販売されるアクセスにより異なる特徴が確認された．また，マルチアクセスは平均 $19,046 と単体アクセスを大きく上回り，複数のアクセス種別を併売することによる価格の上昇が確認できる．総じて，IAB 市場は経済合理性に基づく価格形成を有し，攻撃者は標的価値・アクセス希少性と自らの技術水準を踏まえて最適化しており，市場監視は脅威予測の有効な指標となると考察される．

6.2 IAB の多様性と行動パターン

本節では， 4.2 節で得られたアクターレベルの分析結果について考察し，その特徴と意味について議論する．アク

セス種別の取扱いパターンに見られる階層的構造は，IAB市場における戦略的分業を示している．少数の多角化型アカウント（3.5%）は高度な技術力と複数の侵入手法を保有する組織的脅威アクターの存在が，大多数の専門特化型アカウント（66%）は特定の脆弱性や攻撃手法に依存した個人レベルでの活動が考えられる．

活動期間の分析では，89.2%のアカウントが 50 日未満の短期運用であり，70%超が 1 件のみの投稿という特徴が確認された．この短期・少量投稿パターンは，アカウントの使い捨てによる法執行リスクの回避を目的とした運用戦略を示唆している．さらに，返信者数と感情の分析では，返信を多く集めるアカウントは少数に限られていた．また，評価内容はポジティブが主流で，一部に低評価アカウントも存在していた．これは，フォーラム参加者が IAB の信頼性を実質的に評価・選別していることを示している．加えて，投稿内容の分析では，標的に関する詳細情報が約 3 割の投稿にのみ含まれるなど，多くの投稿で具体的な商品情報が限定的であった．また，46.5%のアカウントが外部連絡手段を言及していることから，これらの投稿は潜在的購入者への初期的な接触を目的としており，具体的な取引交渉や詳細情報の提供は，Telegram や Discord 等の外部プラットフォームで行われている可能性が示唆される．

以上から，本分析結果は，脅威インテリジェンス戦略において，IAB の活動特性（取扱アクセスの多様性，活動パターン，フォーラム内評価）に基づいたリスク評価の有効性を示唆している．特に，多角化型かつ長期活動のアカウントへの重点的な監視や，外部プラットフォームへの誘導パターンの追跡により，効率的な脅威検出が期待される．

6.3 本研究の限界

本研究には，いくつかの限界が存在する．観測対象外のフォーラムで活動する IAB の存在や，投稿以外の取引手段（例：DM 取引，外部プラットフォーム）については本研究では考慮できていない．また，手法とデータセットに関して，今回は投稿から得られた販売品目全体に対して分析を行っており，同一のアクセスに対する複数回の広告や，レンタルサーバーの販売等の IAB の定義に沿わない投稿の存在による統計への影響を考慮できていない．

7. まとめと今後の課題

CrimeBB データセットから抽出した 10 フォーラム・16 年間の IAB 投稿 2,134 件を対象に，IAB の活動を市場視点とアクター視点から包括的に分析し，IAB 市場の構造的特徴と IAB の明確な行動特性を明らかにした．本研究で得られた結果は，IAB の活動実態を解明し，効果的な脅威インテリジェンス戦略構築のための実証的基盤を提供するものである．今後は，投稿データ以外の情報源（例：チャットログ，被害報告，リークデータなど）を統合し，IAB のより包括的なエコシステム分析を目指す．

謝辞　本研究の一部はＮＥＤＯ（国立研究開発法人新エネルギー・産業技術総合開発機構）の委託事業「経済安全保障重要技術育成プログラム／先進的サイバー防御機能・分析能力強化」（JPNP24003）によるものである．

参考文献

[1] Cyberint (a Check Point Company). Initial access brokers report 2025. Technical report, Cyberint / Check Point, 2025. Based on underground forums and dark-web marketplaces analysis over the past two and a half years.

[2] Cyjax Threat Intelligence. Initial access broker market summary q3 2024. Technical report, Cyjax, November 2024. White paper summarizing IAB listings trends in Q3 2024.

[3] KrakenLabs / Outpost24. Demystifying initial access brokers (iabs) and links to ransomware. Technical report, Outpost24 KrakenLabs, 2024. Analyzed 152 corporate access sale offers from underground forums.

[4] Flare Intelligence. Initial access brokers, russian hacking forums, and the underground corporate access economy. Technical report, Flare, August 2023. Based on analysis of hundreds of IAB posts on Russian-language hacking forums.

[5] Recorded Future (Insikt Group). Initial access brokers are key to rise in ransomware attacks. Technical report, Recorded Future, 2022. Also referred to as CTA-2022-0802 report; analyzes chain enabling ransomware via IABs.

[6] Ian W. Gray, Jack Cable, Benjamin Brown, Vlad Cuiujuclu, and Damon McCoy. Money over morals: A business analysis of conti ransomware. In Proceedings of the APWG Symposium on Electronic Crime Research (eCrime), pp. 1–12. IEEE, 2022.

[7] Max van der Horst, Ricky Kho, Olga Gadyatskaya, Michel Mollema, Michel van Eeten, and Yury Zhauniarovich. High stakes, low certainty: Evaluating the efficacy of sanction-based attribution in the ransomware ecosystem. In Proceedings of the 33rd USENIX Security Symposium (USENIX Security '25), 2025. Prepublication version.

[8] Jean-Yves Marion. Ransomware: Extortion is my business. Communications of the ACM, Vol. 68, No. 5, pp. 36–47, 2025.

[9] Sergio Pastrana, Daniel R. Thomas, Alice Hutchings, and Richard Clayton. Crimebb: Enabling cybercrime research on underground forums at scale. In Proceedings of The Web Conference 2018 (WWW '18). International World Wide Web Conferences Steering Committee, 2018. Dataset description paper introducing CrimeBB.

[10] 海藤十和, 伊藤祥梧, 田辺瑠偉, インミンパパ, 吉岡克成. "darkbert と llama 3.3 を用いた初期アクセスブローカーによる投稿の分類と情報抽出". 情報処理学会コンピュータセキュリティシンポジウム（CSS2025）, 2025.

[11] Clayton J Hutto and Eric E Gilbert. Vader: A parsimonious rule-based model for sentiment analysis of social media text. In Proceedings of the 8th International Conference on Weblogs and Social Media (ICWSM-14), pp. 216–225. AAAI, 2014.