TrendAI™ Research

# 産業インフラを標的とする犯罪経済の全体像


**Mayra Rosario Fuentes**
シニア脅威リサーチャー
TrendAI™ Research

**Stephen Hilt**
プリンシパル脅威リサーチャー
TrendAI™ Research

**Numaan Huq**
シニア脅威リサーチャー
TrendAI™ Research

# 目次

# はじめに

本リサーチペーパーは、2024年1月から2026年半ばにかけて、サイバー犯罪フォーラムやインスタントメッセージのチャネルで確認された、産業・エネルギー・製造（IE&M）分野のアンダーグラウンド経済を明らかにするものです。犯罪市場が言語、地域、業界を越えて形成され、専門化し、変化していく過程を追跡してきた50本以上のリサーチペーパーからなる、サイバー犯罪アンダーグラウンドシリーズの最新作に当たります。[1]

水道・エネルギー分野で外部に露出し、脆弱な状態にある産業インフラを調査した過去のリサーチ[2]は、本リサーチの土台の一つとなりました。この調査でTrendAI™は、Shodanを使ってインターネットに公開されたHMI（ヒューマン・マシン・インターフェース）を特定し、認証のないシステムが公開インターネット上に放置されている状況を確認しました。「The SCADA That Didn't Cry Wolf」[3]では、12基の水処理プラント用ハニーポットからなるハニーネットを構築し、そのうち7基に対する74件の攻撃を記録しました。攻撃の15%は、実在のプラントであれば壊滅的な障害につながる深刻度に達していました。いずれのプロジェクトも、「誰が産業システムを狙い、侵入後に何をするのか」という問いを異なる角度から追究したものです。

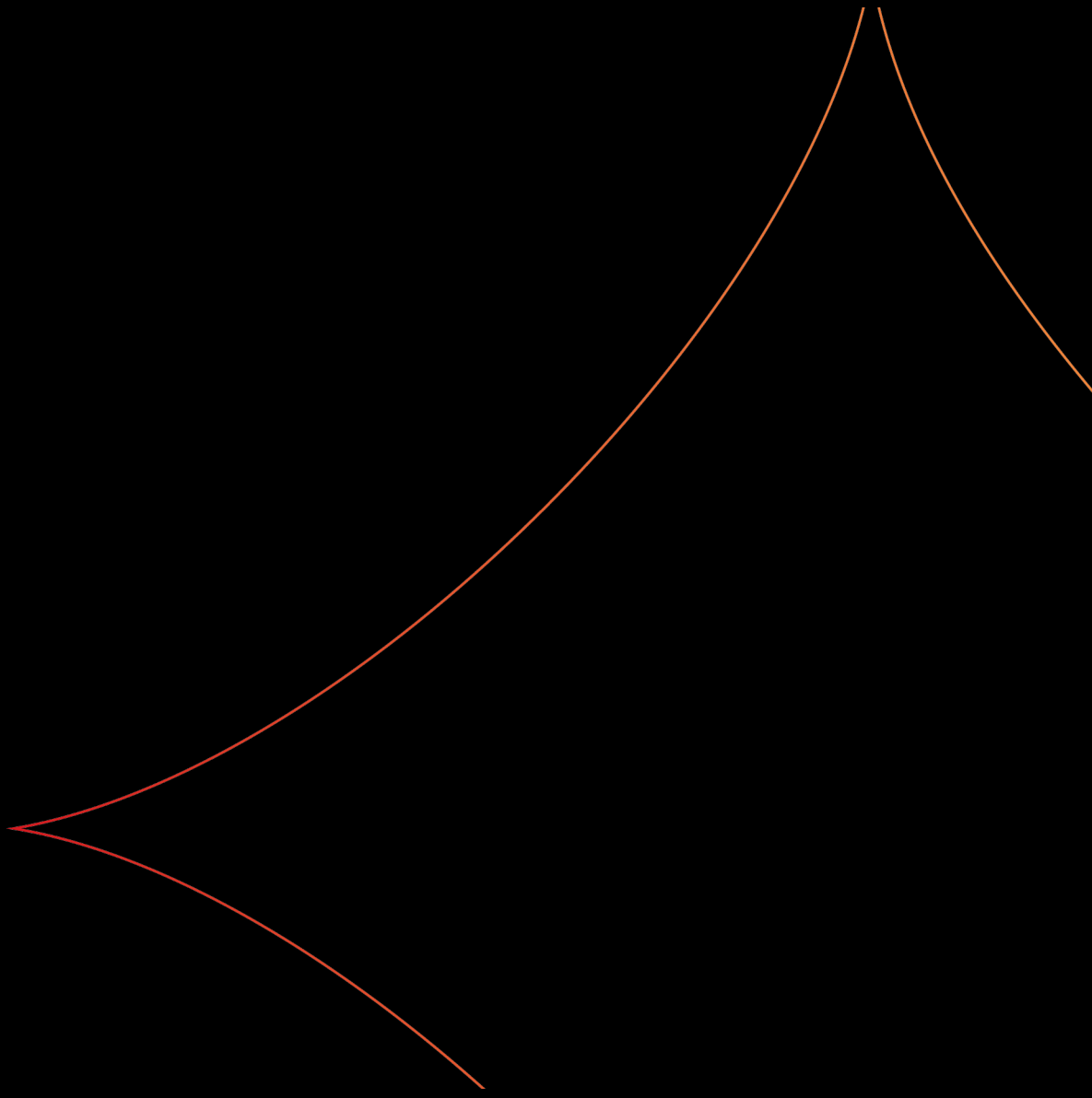
2019年、TrendAI™は問いをさらに絞り込みました。産業分野の標的をインターネットに公開して待つと、何が起きるのでしょうか。その答えを得るため、実在感のある工場ハニーポットを配備しました。[4] 実際の産業制御システム（ICS）用ハードウェア、プログラマブルロジックコントローラ（PLC）、稼働するHMIに加え、小規模な産業用試作企業に見えるWebサイトも用意しました。数週間のうちに、ランサムウェア、リモートアクセス型トロイの木馬（RAT）、暗号資産マイナーが侵入しました。攻撃者は、実在する工場を探すのと同じように、ShodanやVNC（Virtual Network Computing）のスキャンを通じてハニーポットを見つけました。

それから7年が経過し、TrendAI™ Researchはアンダーグラウンドの状況がさらに変化していることを確認しました。IE&M分野を狙う犯罪経済は、もはや場当たり的なスキャンにとどまりません。独自のサプライチェーン、価格体系、知識共有基盤を備えた、分業型の市場へと成熟しています。具体的には、BreachForumsでタイの製造業者の生産システムが25米ドルで販売される一方、ドイツの再生可能エネルギー企業の内部データベースは12 BTC（約74万8,000米ドル）で出品されています。また、ロシア語圏のフォーラムでは、アクセスブローカーが「工場のOT/SCADA（制御技術／監視制御・データ収集）へのアクセス」を、自動車販売で本革シートを強調するかのように、プレミアム機能として宣伝しています。こうした価値の高いアクセスを購入するのは、ランサムウェアのアフィリエイト、データブローカーに加え、国家の利益との関連が疑われるハクティビストです。後者の割合は拡大しつつあります。

本リサーチでは、視点をもう一度変えました。標的を設置して誰が現れるかを待つのではなく、産業分野へのアクセス、知識、攻撃の主張が行き交うフォーラム、マーケットプレイス、インスタントメッセージのチャネルを調査しました。そこから、供給側を起点にこの経済の全体像を描き出しました。

# IE&M分野のアンダーグラウンド・エコシステムの仕組み

調査の結果、IE&M分野のアンダーグラウンドは、カード情報や窃取された認証情報を扱うフォーラムのような専用市場ではないことが分かりました。産業関連のコンテンツは、一部の主要な英語・ロシア語フォーラムにおいて、データベースのダンプとアクセス・アズ・ア・サービス（AaaS）の出品情報の間に位置する、薄い専門領域として存在しています。



活動は次の4つに分かれます。

- **知識共有**：SANS InstituteのICS410海賊版教材やSCADAハッキングのチュートリアルが、初心者にとってのスキル障壁を下げています。
- **アクセス・アズ・ア・サービス**：ブローカーが、VPN（仮想プライベートネットワーク）やRDP（リモートデスクトッププロトコル）を足がかりにした、製造プラント、公益事業、エネルギー企業へのアクセスを販売しています。
- **ハクティビズム**：ロシアやイランとの関連が疑われる地政学的動機を持つグループが、プロパガンダの生成、さらには実際の業務妨害を目的としてOTへの侵入を主張しています。
- **ランサムウェア主導のリーク掲載**：アフィリエイトが、同じアクセスを暗号化と恐喝に利用し、支払いに応じなかった組織をリークサイトに掲載して収益化しています。

## 攻撃者の役割とコミュニケーション

IE&M分野のアンダーグラウンドは単一の市場ではなく、次の主要機能からなる分業体制です。

- 初期アクセスブローカーは、多くの場合、窃取されたリモートアクセス用の認証情報から足がかりを確保し、英語・ロシア語フォーラムで転売します。
- データブローカーは、外部に持ち出された文書やデータベースを販売用にまとめます。
- ランサムウェアのアフィリエイトは、同じアクセスを暗号化と恐喝に利用し、支払いに応じなかった組織をリークサイトに掲載して収益化します。
- 金銭ではなくイデオロギーを動機とするハクティビスト集団は、プロパガンダを生成するためにOTへの侵入を主張します。
- 教材の転売者やチュートリアルの作成者は、フォーラムやインスタントメッセージのチャネルで、専門的なICSセキュリティ教材の海賊版やSCADAハッキングのチュートリアルを流通させ、学習・教育の層を支えています。これにより、産業環境を狙う初心者にとっての知識面の障壁が下がります。

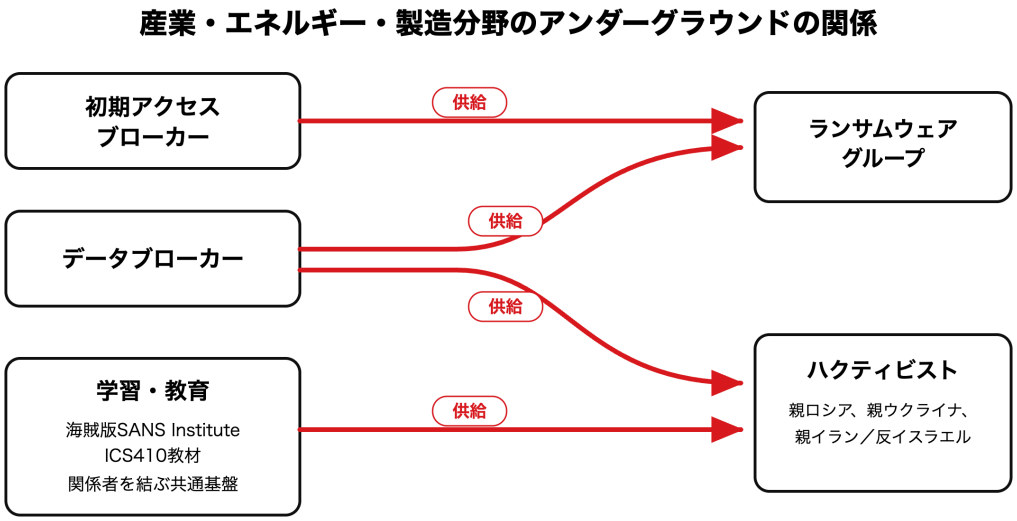



図1：IE&M分野のアンダーグラウンド・エコシステムを構成する関係者と役割

こうした関係者をつなぐコミュニケーションは、2つの層に分かれます。フォーラムの層では、価格や評価の仕組みとともに、アクセス、データ、知識が取引・蓄積されます。市場と資料庫の両方の役割を果たし、長文の販売スレッド、アクセス仲介、チュートリアルなどを収容しています。xss.isやverified.mnといったロシア語圏のニュース・転売サイトは、オペレーションに関する情報を選別し、収益化しています。

一方、インスタントメッセージの層は、ニュースや攻撃の主張をリアルタイムで伝える通信網として機能します。投稿にはタイムスタンプ、ハッシュタグ、スクリーンショットが付随します。CVE（Common Vulnerabilities and Exposures）の勧告、新たな侵害、攻撃の成果を誇示する投稿などが、数時間のうちに提携チャネルへ配信・転載される場でもあります。この層はTelegram上に構築されています。チャネルは標準で公開され、容易に複製でき、情報収集を行うアグリゲーターも自由に登録できます。


図2：IE&M分野のアンダーグラウンドにおける2つのコミュニケーション層

この層の主な活動形態は次のとおりです。

- CVEやサイバー脅威インテリジェンス（CTI）のRSSボット、ICSマルウェアの速報を配信・拡散する。

- GhostSecやZ-Pentestに見られるように、攻撃を主張し、その情報を複数のチャネルへ転載する。

Telegram上では、価格表や長期的な商品一覧はほとんど見られず、フォーラムのような構造化された出品情報もありません。「産業オペレーション」を扱う最大規模の2つのチャネルも、取引や脅威ではなく、無害な自動化について議論していました。一つは、Modbusの読み取り状態やエラーを通知するイタリアのSCADA監視ボット「Intacloud」です。もう一つは、1時間ごとのメガワット時（MWh）、SCADAのPmax、送電網周波数を報告するベトナムの電力系統運用ボット「Báo cáo Sản lượng – TTĐĐ」です。

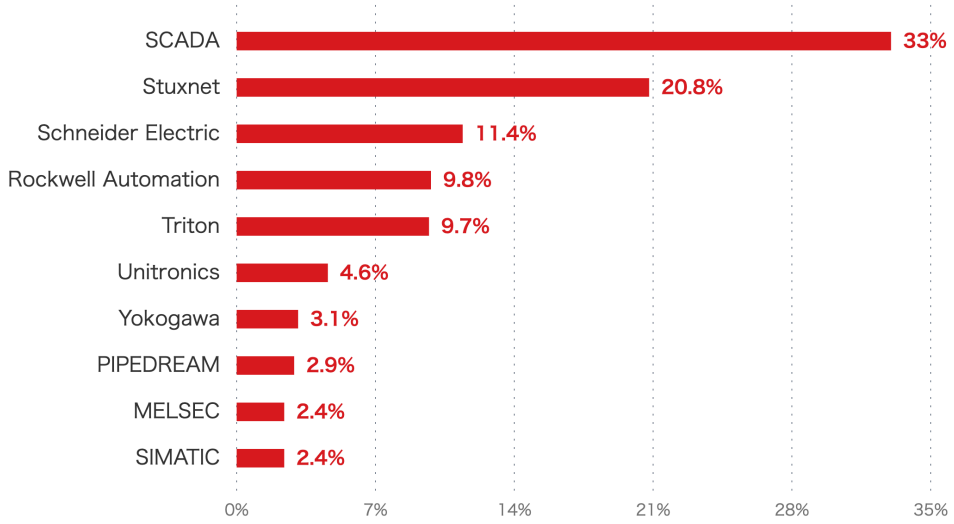



図3：本リサーチでTrendAI™ Researchが監視したTelegramチャネルの主要なICS関連トピック。端数処理のため、合計は100%になりません。

## IE&M分野のアンダーグラウンドで注目される業界

IE&M分野に関するアンダーグラウンドの議論では、製造業が67.9%を占め、突出しています。広大で不均一な環境に多様な接続機器が存在するため、製造業には最も広いアタックサーフェスがあります。情報技術（IT）、制御技術（OT）、IoT（モノのインターネット）機器が混在し、それぞれが外部に露出した侵入口を増やしています。また、製造企業はダウンタイムに対する許容度が極めて低く、ランサムウェアグループにとって最も魅力的な標的です。生産ラインが止まれば損失が急速に膨らむため、短期間で支払いに応じる可能性があります。同じ傾向は、議論の中で標的として取り上げられる機会が増えていたエネルギー分野にも見られます。この分野では、旧式のOTやICSが使われ続け、ITとOTが十分に分離されていないフラットな構成も少なくありません。サイバーセキュリティの成熟度も低い場合、侵入しやすいアタックサーフェスが生じます。

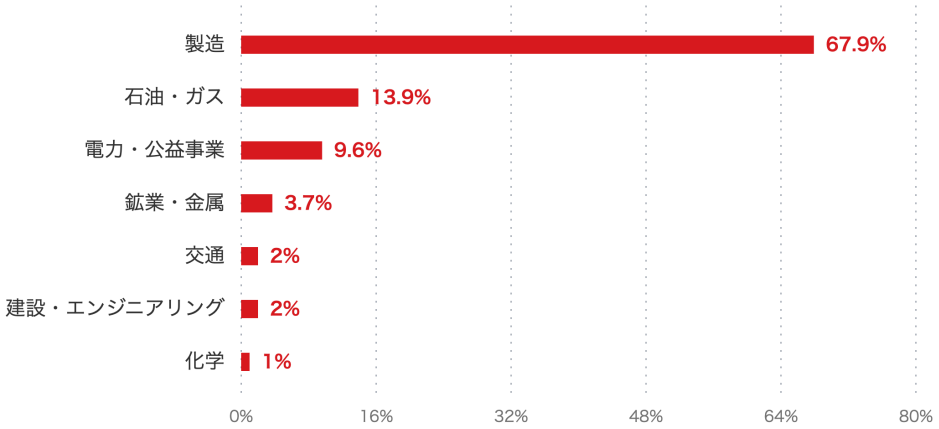



図4：IE&M分野のアンダーグラウンド・フォーラム投稿で標的となった業界の分布。端数処理のため、合計は100%になりません。

## IE&M分野のアンダーグラウンドで使われる言語

フォーラム投稿の83.4%は英語で、ロシア語が14.0%で続きました。トルコ語は1.7%で、その他の言語はいずれも1%未満でした。約18%のスレッドでは2言語以上が併用され、ロシア語による販売活動はxss.isとexploit.inに集中していました。

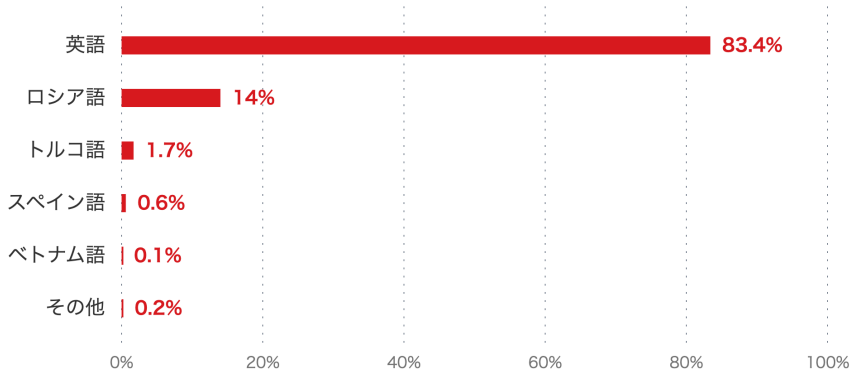



図5：IE&M分野のアンダーグラウンド・フォーラム投稿で使われる主要言語

# サイバー犯罪アンダーグラウンド全体から見たIE&M分野

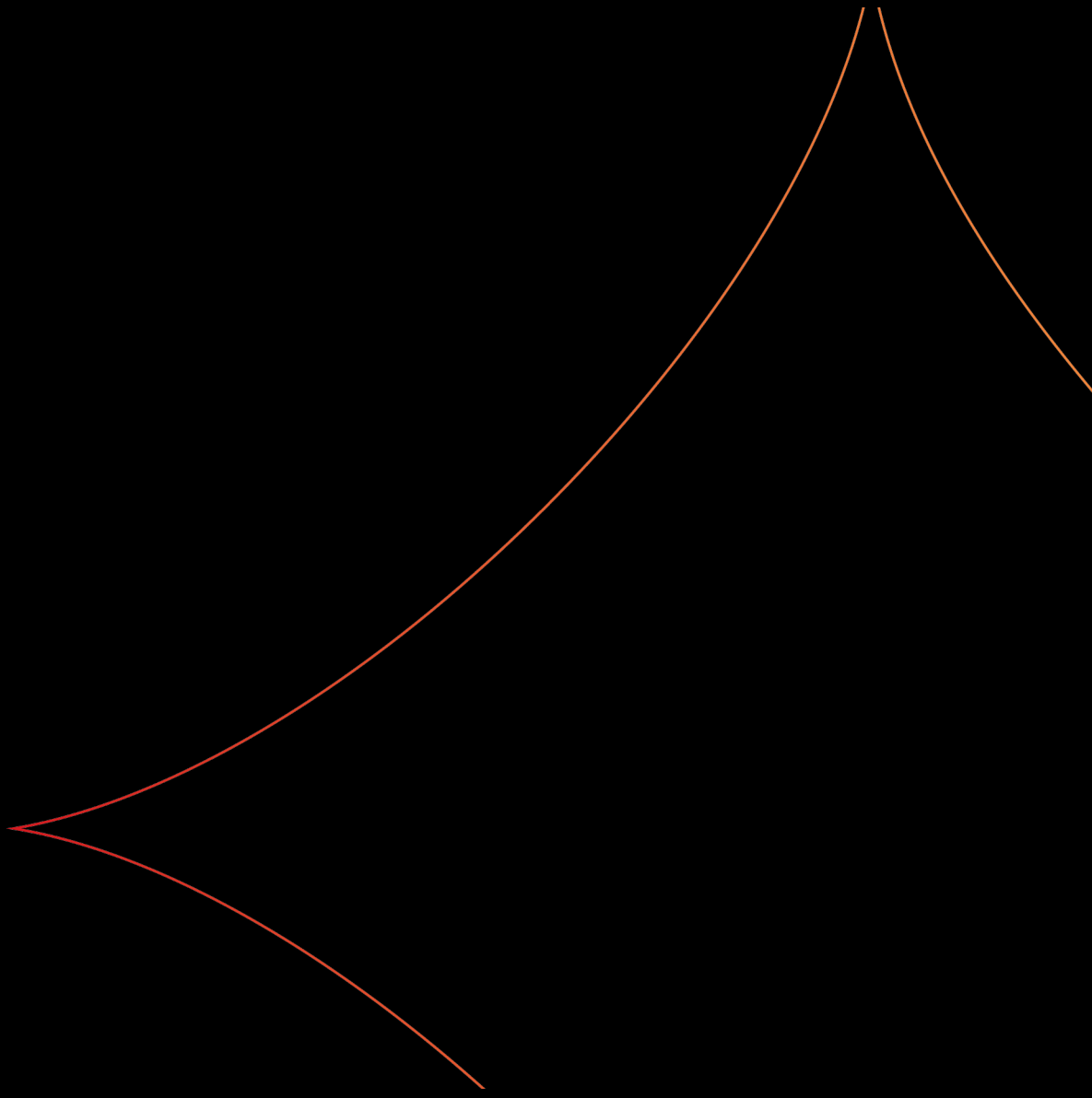
この経済の仕組みは、より広範なサイバー犯罪経済とよく似ています。同じフォーラム（xss.is、exploit.in、BreachForums系サイト）、同じアクセスブローカーの手口、同じエスクローと評価の仕組みに依存しています。

異なるのは、標的とイデオロギーの重なりです。IE&M分野の活動では、銀行詐欺や医療分野のアンダーグラウンドと比べ、ハクティビストによる地政学的動機の活動が占める割合がはるかに大きくなっています。

# アクセス・アズ・ア・サービス

調査と監視を通じて、取引がよく知られた英語・ロシア語フォーラムに集中していることが分かりました。ロシア語圏のxss.isとexploit.inが、アクセス出品情報の大半を占めています。これらは市場の中でも信頼性と取引額が比較的高く、審査を通過したブローカーが企業環境やOTに隣接する環境へのアクセスを競売にかけています。英語圏のDarkForumsや、再開を繰り返すBreachForums系サイトでは、より取引量が多く、低価格のアクセスやデータ漏洩を材料とした恐喝が扱われます。

ただし、フォーラムの販売広告は犯罪者による自己申告であり、詐欺や同じアクセスの重複販売が含まれる場合があります。価格は成約価格ではなく希望価格です。また、地域と業界の分布はブローカーが開示した情報に基づくため、大規模な英語圏の被害組織に偏っています。



# ブローカーの侵入手口

ブローカーは、脆弱な認証情報、使い回された認証情報、窃取された認証情報で保護された、インターネット公開のVPNとRDPを悪用して侵入しています。侵入口となるのは、Fortinet、Citrix、Cisco、Palo Alto Networks、SonicWallなどの脆弱な境界アプライアンスであることが少なくありません。

主要な傾向は、ゼロデイ脆弱性の悪用ではなく、正規のリモートアクセス基盤とアイデンティティの悪用です。

表1は、アクセスに関係するレコードのうち、各侵入経路に言及した割合を示しています。一つの出品情報で複数の経路に言及している場合があります。

| アクセス経路／侵入口 | 割合 | 備考 |
|---|---|---|
| **VPN、リモートアクセスゲートウェイ** | 20.9% | 最も多く言及された経路。<br>特定のエッジ機器名を併記する例が多い |
| **RDP<br>（リモートデスクトップ）** | 13.1% | ブローカーの定番商品。<br>「ドメインユーザ／管理者」として<br>販売される例が多い |
| **窃取された認証情報／ログイン情報** | 12.5% | 使い回し、フィッシング、購入によって<br>入手した企業の認証情報 |
| **ドメイン管理者権限** | 11.0% | 単なる接続ではなく、アイデンティティ／<br>Active Directory（AD）の制御権を販売 |
| **ローカル管理者権限** | 8.0% | 足がかり段階のアクセスで、比較的低価格 |
| **Fortinet／FortiGate** | 7.6% | 名指しされたエッジ機器。<br>VPN／ファイアウォールを悪用 |
| **SCADA／ICS／HMI／PLC** | 6.6% | OTへの到達性をプレミアム機能として宣伝 |
| **RedLine、Lummaなどのスティーラーログ** | 6.2% | アクセスの供給源となる認証情報を提供 |
| **Citrix** | 2.9% | リモートアクセス／仮想化ゲートウェイへの侵害 |
| **SSH** | 2.6% | Linux、ネットワーク機器、<br>アプライアンスへのアクセス |
| **Cisco** | 2.3% | エッジ／VPN機器を標的化 |
| **Exchange／OWA** | 2.2% | メールサーバへの足がかりと認証情報の収集 |
| **Palo Alto Networks／GlobalProtect** | 1.9% | VPNゲートウェイの悪用 |
| **SonicWall** | 1.2% | 中小企業で多用される<br>エッジアプライアンスを標的化 |
| **VMware／ESXi／vCenter** | 1.0% | ランサムウェアにとって価値の高い<br>仮想化レイヤへのアクセス |

表1：各アクセス経路に言及した関連レコードの割合

# 標的となる業界

IE&M分野へのアクセス市場の中心に位置するのは製造業です。アタックサーフェスが広く、IT/OTネットワークへの依存度が高い一方で、インターネット公開基盤へのパッチ適用状況にばらつきがあることと整合します。生産停止による損失が大きいため、ランサムウェアによる収益化にもつながりやすい分野です。

石油・ガスを含むエネルギー・公益事業分野は、出品件数こそ少ないものの、より高値が付き、慎重に取り扱われます。これは、規制上の機微さと、特定の買い手が見出す戦略的価値の両方を反映しています。

鉱業や建設業は、ブローカーが偶然足がかりを得た場合に出品される、機会便乗型の標的として全体像を補っています。

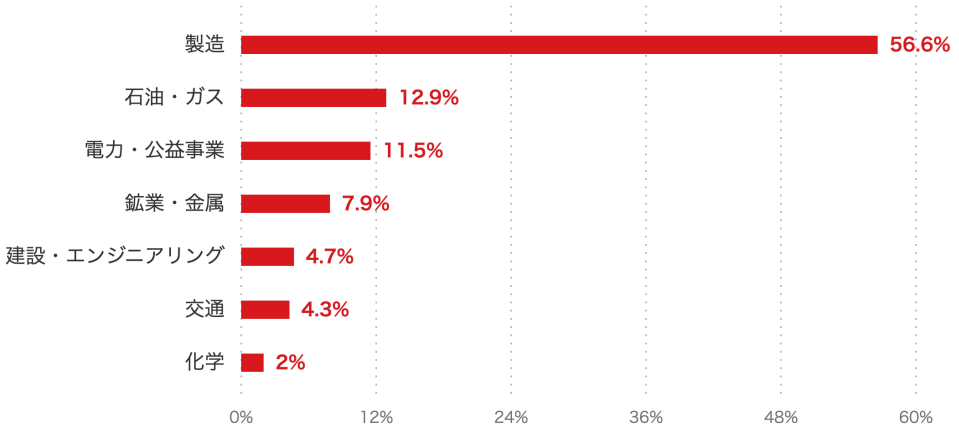



図6：アクセス・アズ・ア・サービスのフォーラムで標的となった業界の分布。端数処理のため、合計は100%になりません。

多くの出品情報は業界を一つに特定せず、産業制御環境への露出を一般的な表現で宣伝しています。「SCADA」「PLC」「HMI」「Modbus」「DNP3」「PROFINET」といった用語が、セールスポイントとして繰り返し登場します。「Siemens」「Schneider Electric」「Mitsubishi Electric」「Allen-Bradley」などのベンダ名も同様です。ただし、こうした情報の多くは稼働中の制御システムへのアクセスではありません。偵察情報、Shodanの検索クエリ集のような外部公開機器の列挙、エクスプロイトやCVEに関する議論、トレーニング教材などです。それでも、買い手が産業分野の標的を発見して攻撃に転用する手間を減らし、どの技術にプレミアム価値があるかを販売者に伝える役割を果たしています。

DarkForumsに投稿され、exploit.inにも転載されたある事例では、包装システムを専門とするイタリアの産業自動化企業から外部に持ち出された17.8 GBのデータが販売されていました。実際のプロジェクトに関する電気回路図や実地試験報告書に加え、EtherCATとPROFINETを使用するSiemens S7-1500およびAllen-Bradley GuardLogixコントローラのPLC図面も含まれていました。このデータセットは、2025年6月に即決価格650米ドルで出品されました。

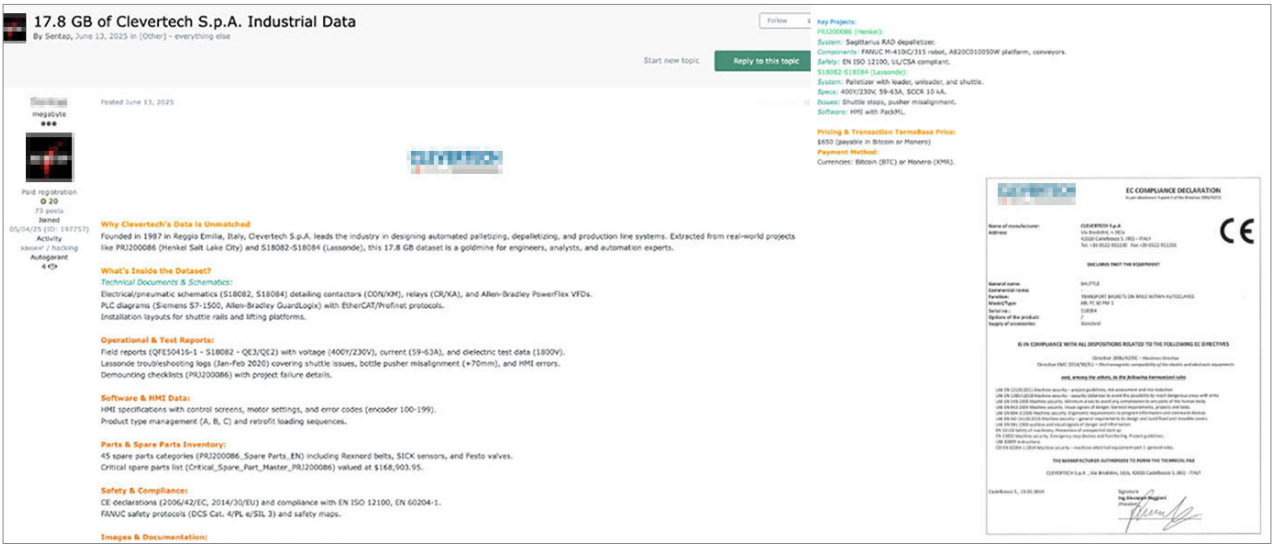



図7：イタリアの産業自動化企業から持ち出されたデータを650米ドルで販売するフォーラム投稿のスクリーンショット

石油・ガスは比較的小規模ながら価値の高い分野であり、IE&M分野のアンダーグラウンドで継続的に狙われています。パイプライン事業者や精製事業者は、物理的安全性と供給継続性が脅かされるため、特に影響を受けやすい標的です。この分野は地政学的にも重要であることから、アクセスはランサムウェアグループ以外の幅広い買い手を引き付けます。

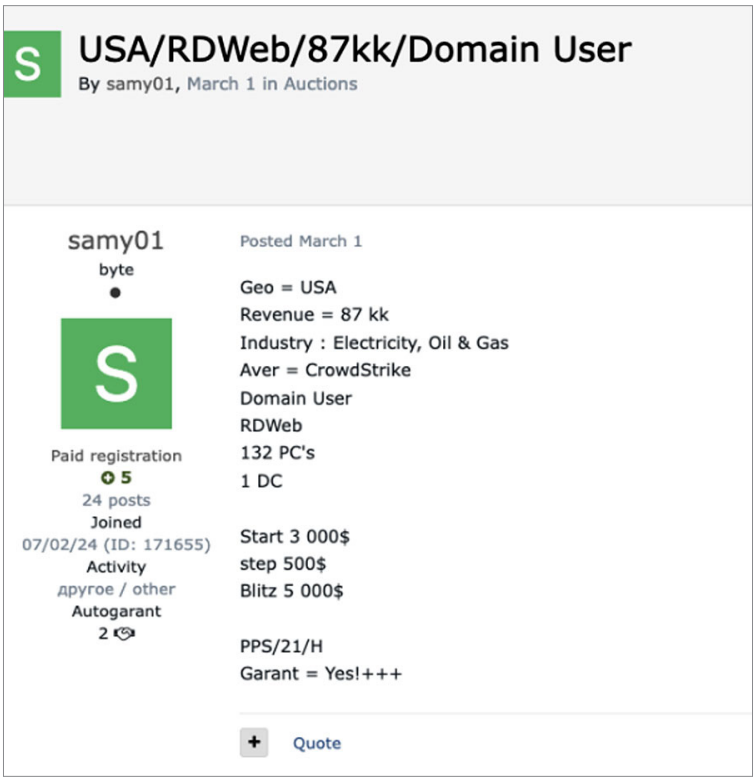



図8：石油・ガス企業へのアクセスを販売するフォーラム投稿のスクリーンショット。入札開始価格は3,000米ドル


図9：地図情報やSCADAシステム情報を含む請負企業のデータを4万米ドルで販売するフォーラム投稿のスクリーンショット

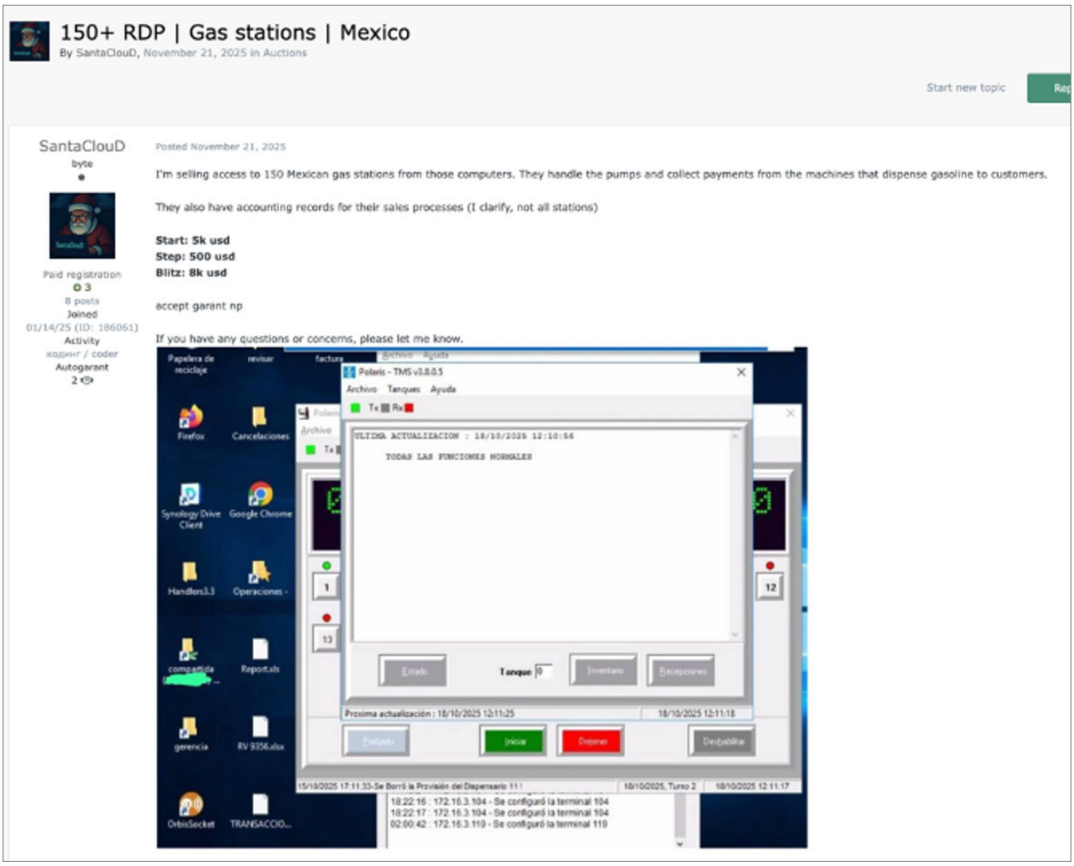



図10：メキシコのガソリンスタンドへのRDPアクセスを販売するフォーラム投稿のスクリーンショット

exploit.inでは、年間売上高1億3,010万米ドル、ドメイン参加PC約400台を持つアルゼンチンのエネルギー・公益事業企業に対する、VPNおよびRDPのドメインユーザアクセスも競売にかけられていました。2025年2月に開始価格800米ドル、即決価格1,200米ドルで出品されたものです。

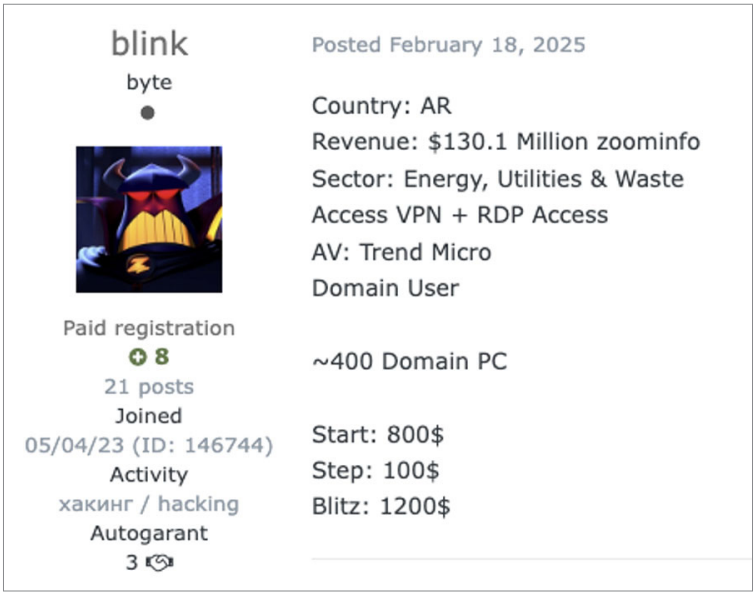



図11：アルゼンチンのエネルギー・公益事業企業に対するVPNおよびRDPのドメインユーザアクセスを販売するフォーラム投稿のスクリーンショット

鉱業・金属分野へのアクセスは取引量が少なく、体系的に開拓されるというより、機会便乗的に扱われています。出品される場合は資源経済への依存度が高い地域に集中し、製錬や鉱石処理など、製造業や冶金処理に関する表現と組み合わせて宣伝されることが少なくありません。

## 標的の地域分布

被害組織の地域は米国に大きく集中し、アクセス関連レコードへの登場数は他国を大幅に上回りました。この集中はランサムウェアの経済性と整合します。米国のIE&M組織は、売上高が大きく、ダウンタイムへの許容度が低いうえ、サイバー保険に裏付けられた支払い能力を持っています。この組み合わせにより、そのアクセスには最も高い転売価値が生まれます。

米国以外の出品情報は、欧州、中南米、中東、アジア太平洋地域に広がっています。

米国、EUの主要国、オーストラリアを一つにまとめるなど、複数国を対象とした出品情報もあります。これは、ブローカーが単一の被害組織を狙うのではなく、機会便乗的に集めたアクセスをまとめて販売していることを示しています。

イスラエルのように地政学的に機微な地域が上位に入っていることから、IE&M分野へのアクセスに対する関心の一部は、金銭目的だけではないと考えられます。

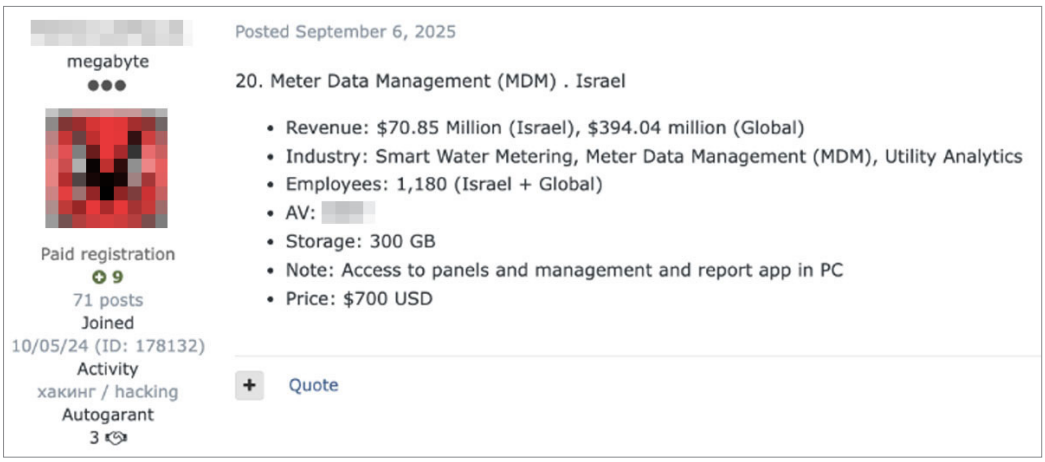



図12：イスラエルの水道メーター管理システムへのアクセスを販売するフォーラム投稿のスクリーンショット

## アクセスの価格と経済性

AaaSの出品価格は市場の低価格帯と高価格帯に集中し、中間価格帯の出品は少なくなっています。最大の区分は10万米ドル超で、全出品の36.1%を占めます。

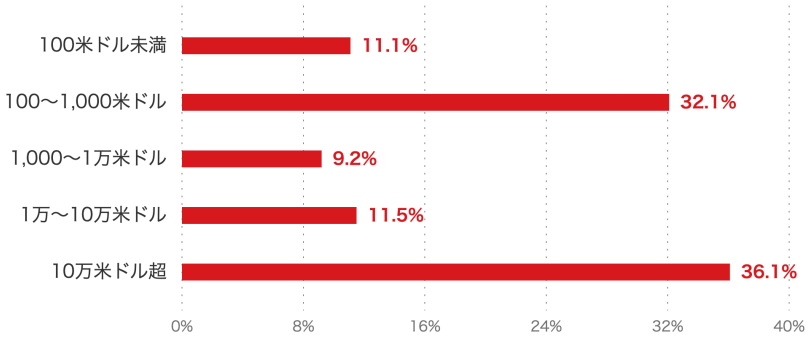



図13：AaaS出品の価格帯分布（米ドル）

BreachForumsでは、パキスタンのNational Transmission & Dispatch Company（NTDC）とWater and Power Development Authority（WAPDA）を完全に制御できるアクセスが、2025年1月に3 BTC（約18万7,000米ドル）で宣伝されていました。出品内容には、SCADAシステム、従業員の人事情報システム（HRIS）データ、ピーク時間帯の電力供給を操作できる権限が含まれていました。

exploit.inでは、ドイツの再生可能エネルギー企業Enerparc AGの内部データベースが、2026年1月に12 BTC（約74万8,000米ドル）で出品されていました。

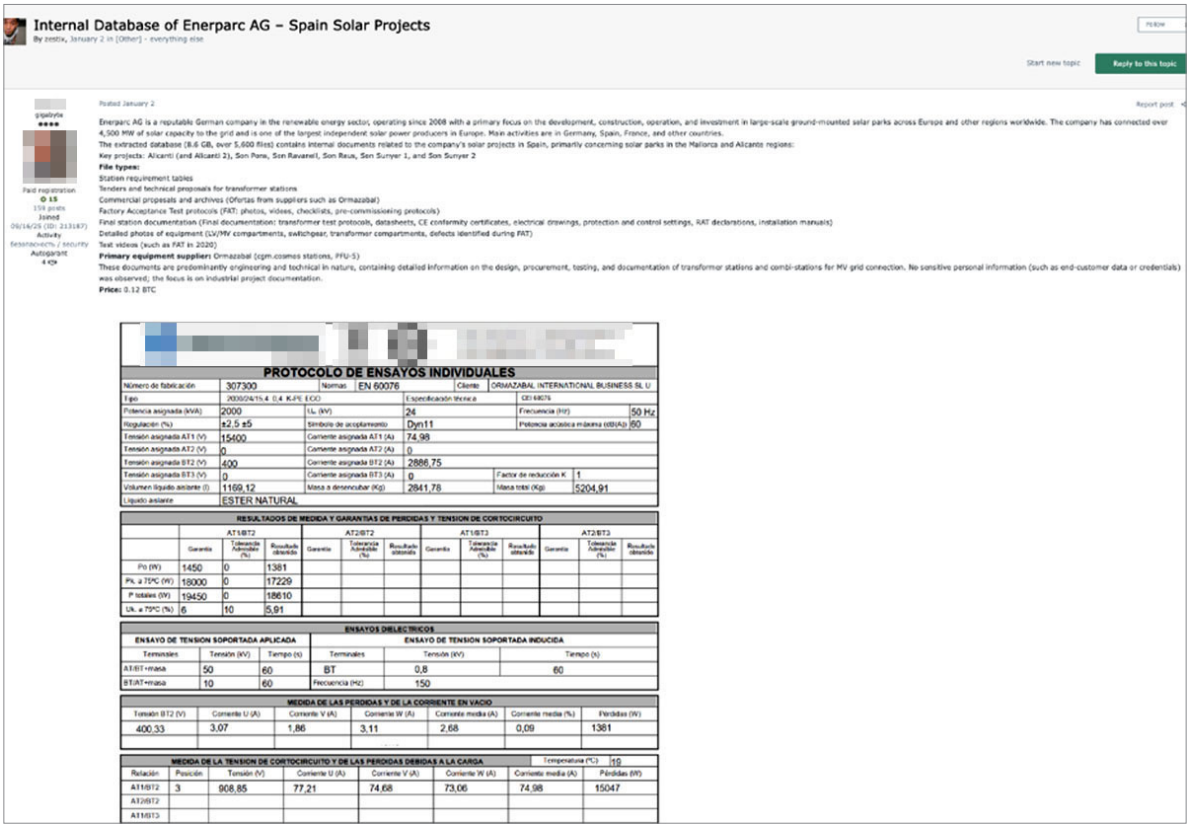



図14：ドイツの再生可能エネルギー企業の内部データベースを12 BTCで販売するフォーラム投稿のスクリーンショット

低価格帯の出品の一部は、DarkForumsやBreachForums系サイトで確認されました。例えばBreachForumsでは、タイの産業用鋳造・製造企業が運用する生産・受注管理システムの完全な管理者アクセスが、2025年3月に25米ドルで販売されていました。販売者は、この異例の安さを「信じられない」価格だと強調していました。

exploit.inでは、年間売上高2,500万米ドル超の韓国の産業機械企業に対する、企業メールと人事システムへのアクセスが出品されていました。管理者、CEO、マネージャのアカウントが含まれ、2025年2月時点の価格は850米ドルでした。

AaaSの出品には競売形式も多く、「Start/Step/Blitz」または同じ意味の「Starting bid/Increment/Buy now」という定型表現が使われます。

exploit.inでは、年間売上高20億米ドルの米国製造企業を対象に、ドメイン認証情報を含まないVPN認証情報へのアクセスが競売にかけられていました。2025年8月に開始価格2,000米ドル、即決価格1万米ドルで出品されたものです。

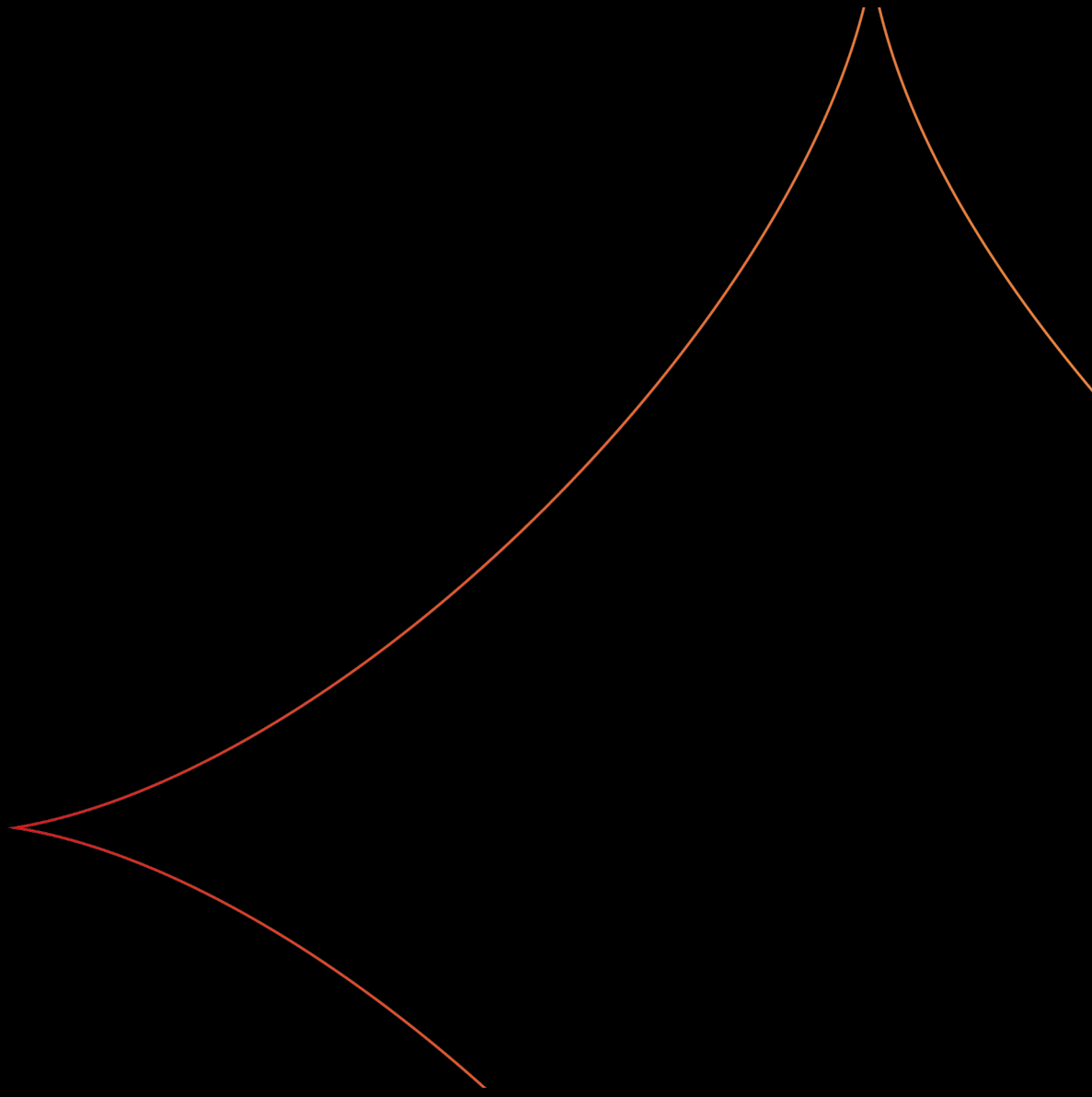

図15：米国製造企業のVPN認証情報へのアクセスを販売するフォーラム投稿のスクリーンショット

BTC建ての出品や、競売または非公開交渉の意図を示すために1米ドルを仮の価格として設定する出品もあります。開始価格を1,000米ドルとする競売が多く、この価格帯が32.1%を占める一因となっています。

少数ながら、数十万米ドルから、名目上はさらに高額な価格を提示する出品もあります。これらは成約価格ではなく、機微なデータを大量に含む商品に対して販売者が希望する、実現性の低い価格と考えるのが妥当です。

# ランサムウェア

本セクションでは、恐喝型リークサイト「Ransomware.live」が公開した、2024年1月から2026年6月までのランサムウェア被害組織データを使用しています。リークサイトへの掲載は、特に身代金を支払わなかった組織や、データを公開された組織が名指しされた事例を表します。この数字から、IE&M分野に対するランサムウェアの圧力を把握できます。



2024年1月から2026年6月にかけて、産業・エネルギー分野の組織は3,178件のリークサイト掲載に登場しました。その77.8%を製造業が占めます。産業インフラ分野（電力・公益事業、石油・ガス、上下水道）の割合は比較的小さいものの、被害の影響は深刻です。

IE&M分野のリークサイト掲載被害者数は、2024年の974件から2025年の1,437件へ約48%増加しました。2026年は上半期だけで767件に達し、年間では2025年と同等か、それを上回るペースです。攻撃はAkira、Qilin、Playを筆頭とする少数のランサムウェア・アズ・ア・サービス（RaaS）グループに集中し、地域別では米国と西欧が大半を占めます。

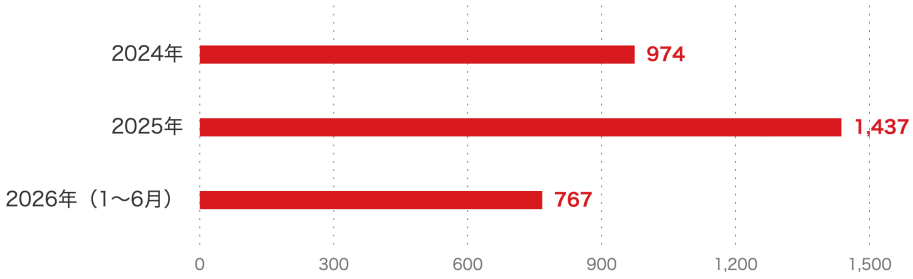



図16：年別に公表された被害組織数。2026年は1月から6月まで。

## ランサムウェア被害データで最も目立つ製造業

公表された被害組織の77.8%を製造業が占め、電力・公益事業が大きく離れた2位ながら無視できない割合で続きます。その他の産業分野は、いずれも大幅に少なくなっています。

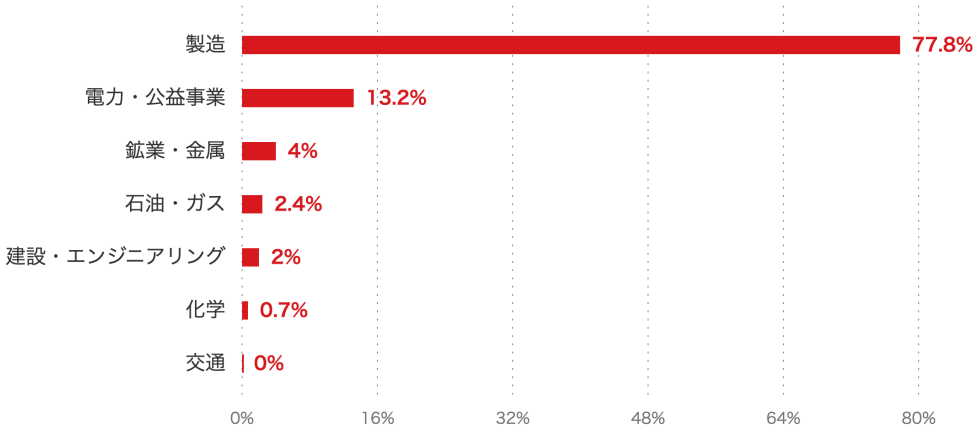



図17：2024年1月から2026年6月までに公表された対象業界別の被害組織。端数処理のため、合計は100%になりません。

製造業は、身代金支払いに至る割合に比べ、ランサムウェアのリークサイトへの掲載が突出して多くなっています。調査からは、次の複数の要因が確認されました。

- 中堅規模の製造業者の多くはバックアップから復旧でき、身代金を支払う代わりにダウンタイムを受け入れています。
- 窃取されるデータは規制対象の個人データではなく、業務データであることが多いため、恐喝の材料としての効力が下がります。
- 利益率が低く、多額の身代金を支払うと経済的に見合いません。

その結果、製造業は攻撃件数も漏洩件数も多い一方、支払いには比較的応じない分野となっています。このため攻撃者は、暗号化による収益だけを狙うのではなく、攻撃件数を積み上げ、データ販売でも収益化する方向へ進んでいます。

## 少数のRaaSグループが被害の大半を占める

IE&M分野の被害の大半は、少数のRaaSグループによるものです。この分野で最も活発なAkira、Qilin、Playは、それぞれ372件、338件、238件の被害組織を公表しました。この3グループだけで、対象範囲内の被害組織全体の約30%を占めます。

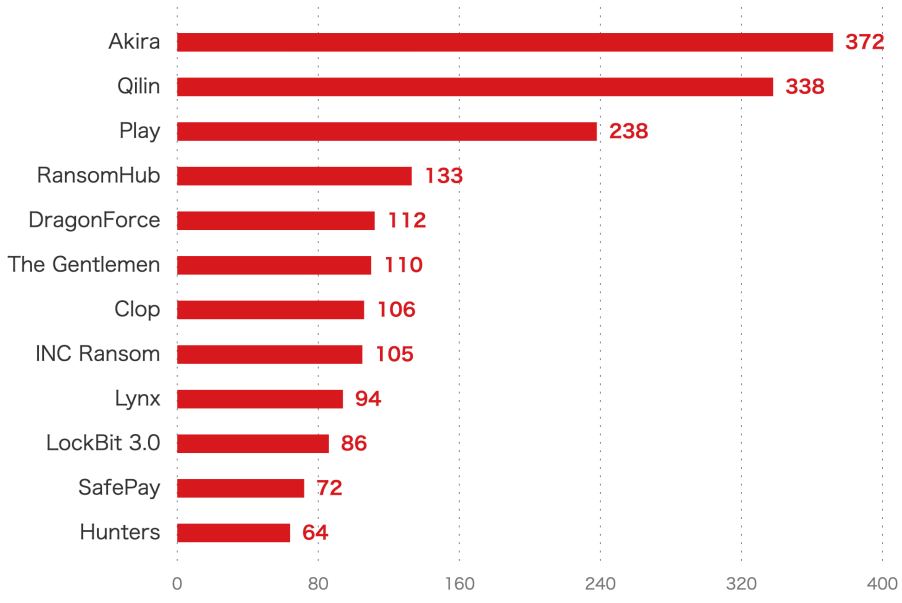



図18：対象範囲内の被害組織数が多い上位12のランサムウェアグループ

被害組織は米国に大きく集中し、ドイツ、カナダ、イタリアが続きます。

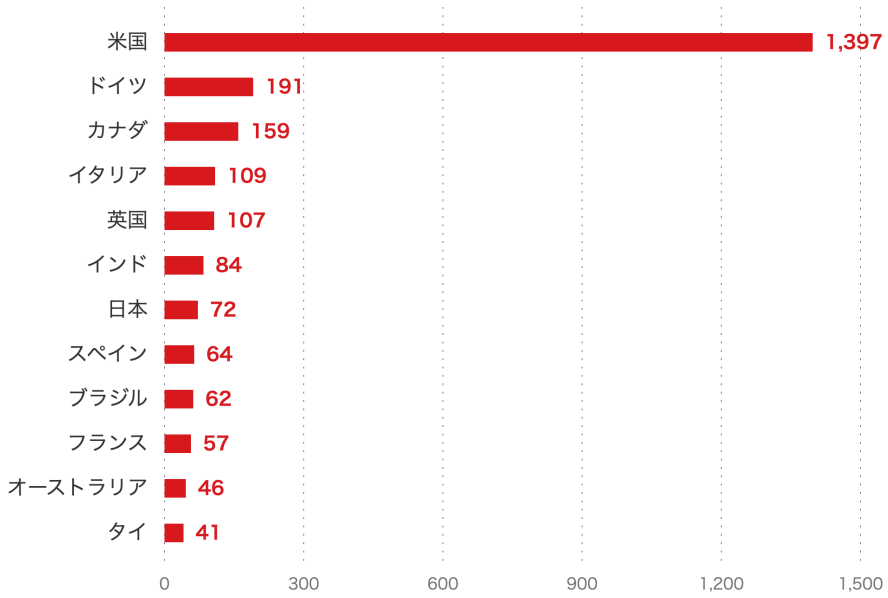
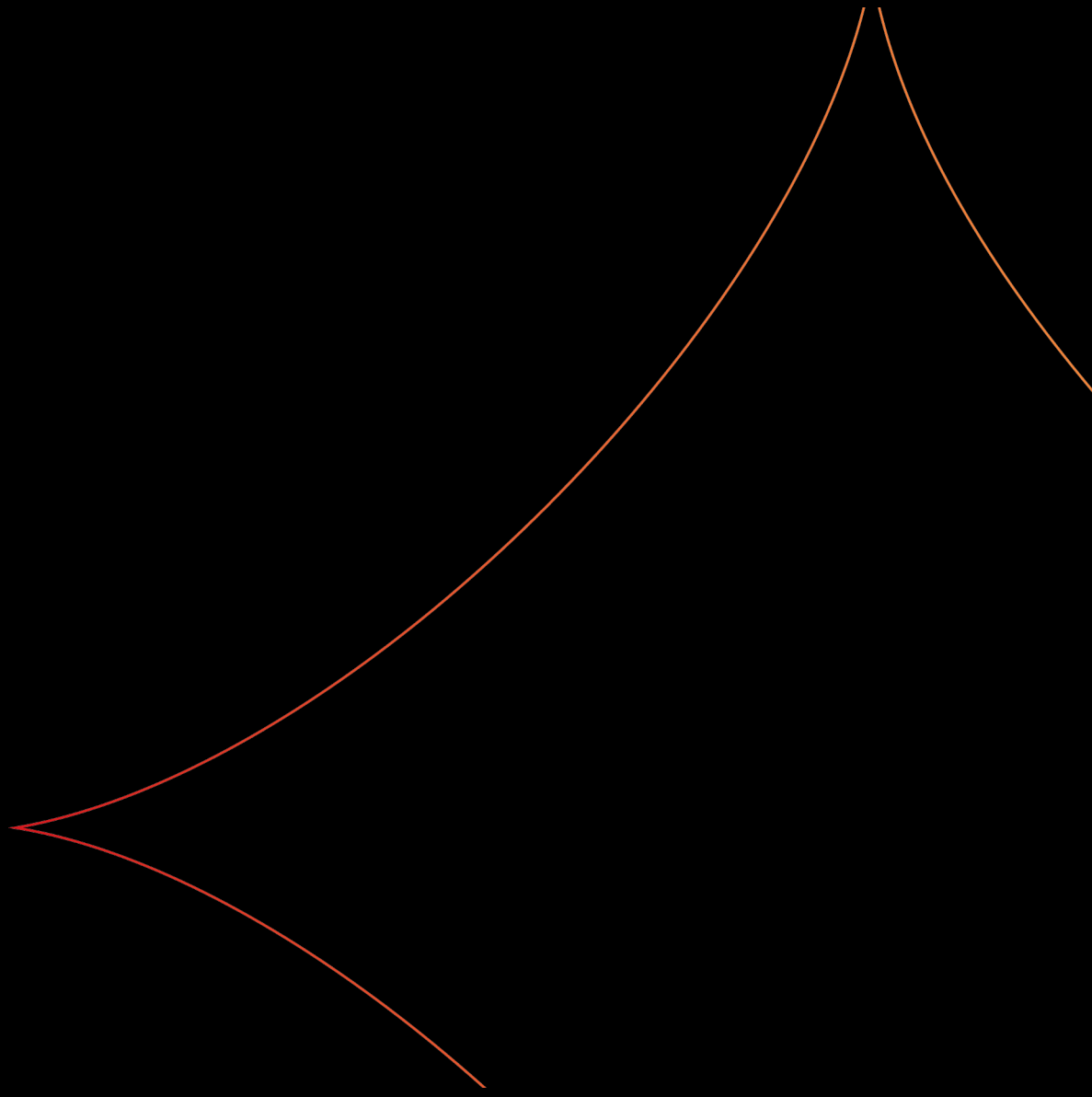



図19：被害公表件数が多い上位12か国

# 知識共有

アンダーグラウンドのフォーラムでは、専門的なICSセキュリティ研修教材がホストされ、転売されています。SANS Instituteの「ICS410: ICS/SCADA Security Essentials」は海賊版コースパックとして222回登場し、SCADA、PLC、産業用プロトコルについて愛好家が質問と回答を交わすスレッドも併存しています。

インスタントメッセージの層では、ペルシャ語やアラビア語のチャネルが、Stuxnetなどの実在するICS攻撃、各種プロトコル、Siemens製PLCを題材とするSCADAハッキングのカリキュラムを構築しています。



### 海賊版ICS研修教材を扱うアンダーグラウンド経済

| 621 | 330 | 293 | 222 |
|---|---|---|---|
| 教育関連の投稿 | SANSへの言及 | ICS410への言及 | 最大のスレッド「[FREE] SANS ICS410」 |

**最も多く共有された教材パック**

| | |
|---|---|
| ハッキング・セキュリティ教材パック | 62 |
| ハッキング・セキュリティ電子書籍パック | 13 |
| ハッキング・セキュリティ電子書籍 Top 100 | 10 |

図20：専門的なICSセキュリティ教材を転売するアンダーグラウンド・フォーラムの監視で確認された主な数字

## ICS410とは

ICS410は、SANS Instituteが提供する産業制御システムの基礎コースであり、GICSP（Global Industrial Cyber Security Professional）認定資格を取得するための必須前提コースです。Purdue Enterprise Reference Architecture（PERA）に加え、PLCやHMIがSCADAおよび分散制御システム（DCS）とどのように接続されるかを扱います。また、Modbus、DNP3、EtherNet/IP、PROFINETなど、制御トラフィックを伝送するOTプロトコルも学習対象です。

SANSのコース教材には、各コースに付属する印刷・デジタル教材、演習環境、仮想マシン（VM）イメージが含まれます。いずれも独自の著作物であり、著作権で保護され、受講料を支払った受講者だけにライセンスされます。2026年6月時点で、ICS410の受講料は9,230米ドルです。[5]

TrendAI™ Researchは、Cracked.toで繰り返し掲載された「SANS and Offensive Security Courses」という転売スレッドを確認しました。再投稿されたバンドルには、SANS 401や408と並んで「SANS 410 - ICS & SCADA Security Essentials.tar.gz」が掲載されています。このスレッドは2024年1月から2025年11月まで活動していました。


図21：ICS410を含むSANSコースの無料ダウンロードリンクを共有する返信が30ページに及ぶ、Cracked.toの「SANS and Offensive Security Courses」スレッド

こうした教材がサイバー犯罪者を引き付けるのは、防御側のカリキュラムが攻撃者の実戦マニュアルも兼ねているためです。エンジニアがプラントを守るために使うコンテンツは、そのまま産業ネットワークの構成図にもなります。狙うべきプロトコル、IT/OTの弱点、安全システムや制御システムが操作された場合の挙動まで示されています。コース教材がなければ、サイバー犯罪者がこうした知識を身に付けるには長い時間と高いコストが必要です。

IranHackのペルシャ語スレッド「Evil PLC (Scada Hacking)」では、PLCを基盤とするSCADAシステムが解説されています。このスレッドには、システムを「発見し、侵入する」方法を教える書籍へのファイル共有リンクがあります。図22に示す書籍には、「産業制御システムはSCADAと呼ばれます。SCADAアーキテクチャでは、必ずPLCが使用されます。本書では、こうしたシステムを発見し、侵入する方法を解説します」という意味の説明が記載されています。


図22：PLCを発見して侵入する方法を解説する、ペルシャ語スレッドに投稿された書籍のスクリーンショット

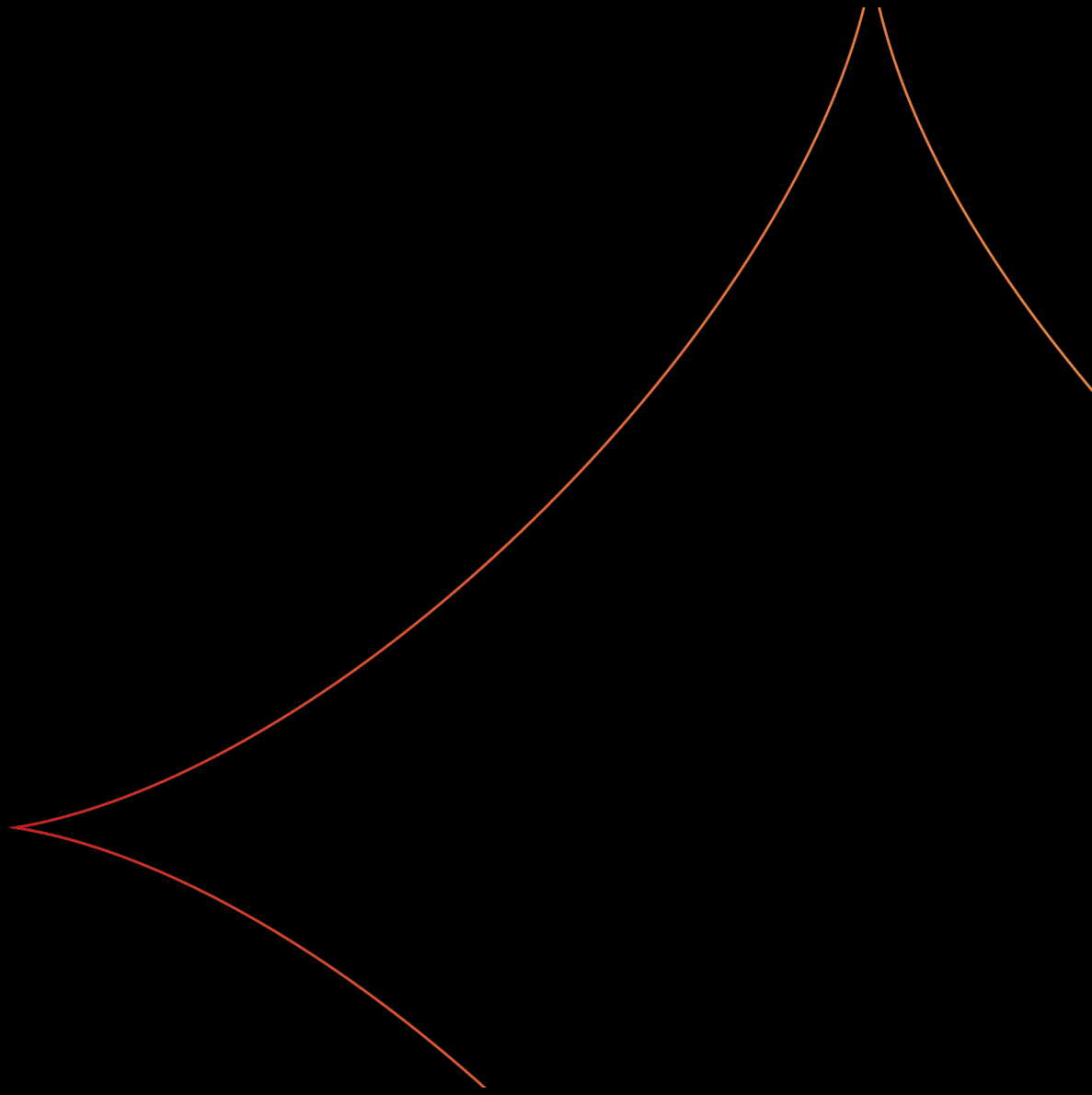
単純な経済的動機もあります。ICS410を正規に受講するには9,000米ドル以上かかるため、海賊版の教材、漏洩した演習ファイル、教材の無料再共有には実質的な転売価値があります。こうした投稿がフォーラムに現れると、安定して数百件の返信を集めます。

# ハクティビズム

2024年から2026年にかけて、ハクティビストはIE&M分野において、目立つ脅威となっていきました。電力網、水道事業、石油・ガス事業、製造プラントへの侵入を主張する事例が増加しています。

本セクションは、これらのハクティビストグループが運営するTelegramチャネルの監視結果に基づきます。チャネルでは、オペレーションの発表、侵害を証明するとされるデータの公開、ツールの共有が行われています。なお、ここで取り上げる主張は各チャネルから直接収集したものであり、必ずしも検証されたものではありません。

主要な攻撃者に焦点を当て、特に2026年1月から7月までの動向を詳しく見ていきます。この時期は、イラン、イスラエル、米国の対立が激化し、インフラを狙う活動が最も急増しました。



全体を通じて、次の2点に注意が必要です。

- これらの攻撃者は技術力よりも執拗さと機会便乗に頼り、インターネット上に露出した、保護の弱い制御システムを悪用しています。

- 公に主張する影響の大きさは、検証された能力を常に上回ります。確認済みのOTへの標的化を、データ層への侵入や演出されたプロパガンダと区別することが、分析上の最大の課題です。

# IE&M分野を標的とするハクティビストグループ（2024〜2026年）

## Handala

調査対象期間のうち、ハクティビストによるIE&M分野の標的化が最も激しかったのは2026年上半期でした。2月下旬にイラン、イスラエル、米国の対立が激化すると、親イランの攻撃者が前面に出ました。中でも象徴的だったのが、米国最大級の民間水道事業者California Water Serviceに対する2026年6月の侵害です。Handalaは、イランのSirikにある貯水池への米国の攻撃に対する直接の報復だと位置付けました。侵害の証拠として約5 GBのデータを公開し、自治体の水道供給を妨害できたものの、実行しなかったと主張しています。

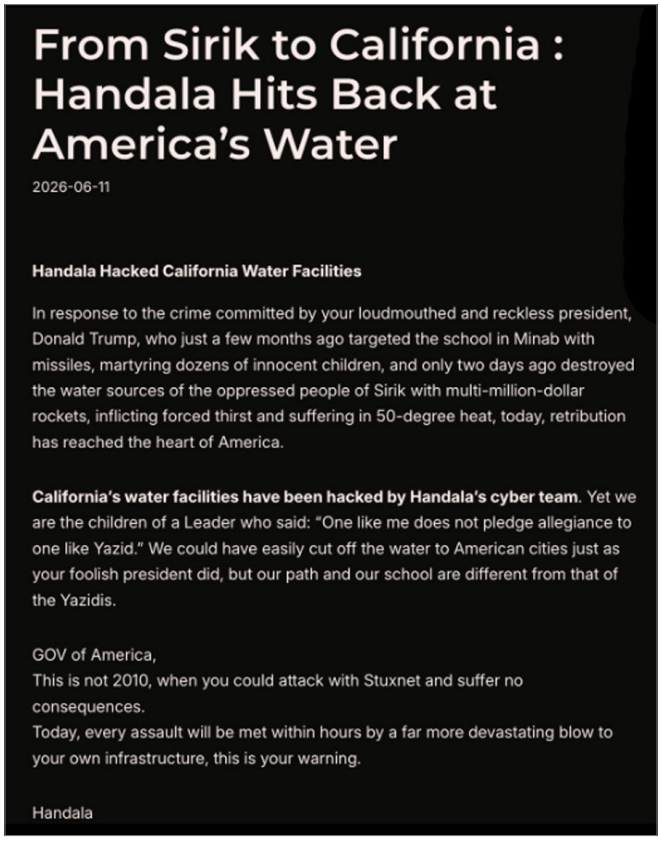



図23：California Water Serviceへの侵害を主張するHandalaのWebサイト

## CyberAv3ngers

CyberAv3ngersは、イスラム革命防衛隊（IRGC）のCyber-Electronic Commandとのつながりを持ち、イランとの関連が疑われる脅威グループです。2020年から活動し、水道や産業制御システムを中心とする産業インフラを標的としてきました。

2026年には、米国の公益事業でPLCを積極的に悪用しました。2026年7月26日から27日にかけて、組織的なサイバー攻撃によってミネソタ州の30を超える地域で上下水道事業の運用が妨害されました。これは、同グループによる攻撃の激化と関連付けられた最新の事例です。[6]

## Hunt3r Kill3rs

Hunt3r Kill3rsは、親イラングループの中でも、実際の作戦能力という点で特に深刻な存在です。イデオロギー的な性格と犯罪的な性格を併せ持ち、米国、イタリア、イスラエルとその同盟国を標的としてきました。

原子力関連施設を含むエネルギー資産やPLC機器へのアクセスを主張しており、OTに到達できる可能性のある攻撃者の一つです。Handalaが比較的小規模なIT侵入を大きな政治的メッセージへ変換するのに対し、Hunt3r Kill3rsは制御システムそのものを探っています。

## NoName057(16)

NoName057(16)は2022年から活動し、Z-Pentestを含む後発のグループ群の基盤となった親ロシアの攻撃者です。分散型の集団として、ウクライナ、北大西洋条約機構（NATO）、EUを標的に活動し、エネルギー、水道、交通システムに対する大規模な妨害キャンペーンで評価を築きました。キャンペーンには、参加者を広く募るクラウドソーシング型のモデルが使われています。

同グループのTelegramチャネルでは、直近数か月にIE&M分野を標的としたDDoSiaプロジェクト関連の主張が確認されました。DDoSiaは、参加者を募って分散的に運営するDDoS（分散型サービス拒否）プラットフォームです。

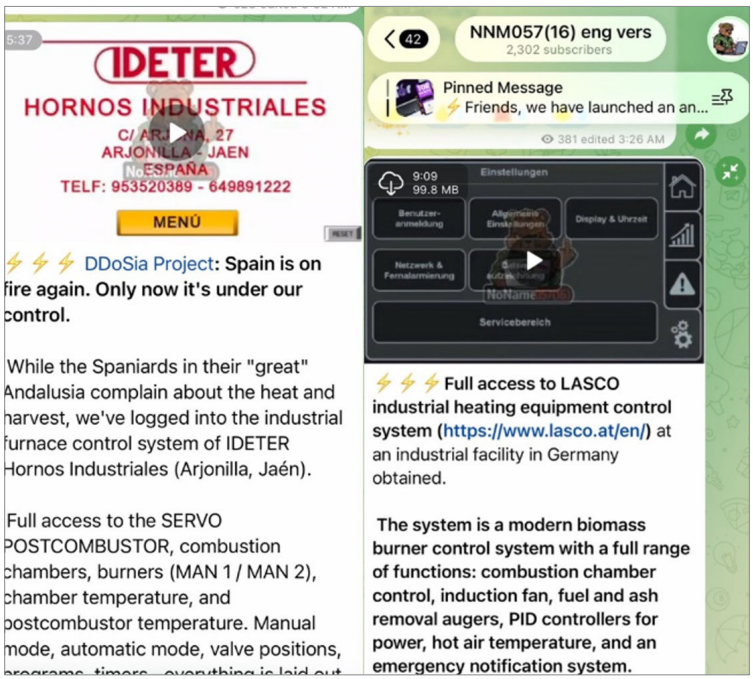



図24：2026年7月にTelegramへ投稿された、2社の産業企業への侵入を主張するスクリーンショット

## Z-Pentest

Z-Pentestは、親ロシアのハクティビストによるOT標的化を代表する存在です。2024年9月に登場し、NoName057(16)やCyberArmyofRussia_Reborn（CARR）から人員を引き継ぎ、本リサーチの対象期間においてOTに特化した最も活発な攻撃者となりました。

欧州、NATO加盟国、米国、台湾のエネルギー、水道、石油・ガス、製造業を対象に、侵入を主張する投稿を継続的に公開しました。Telegramチャネルでは、侵害の証拠とする画面録画や制御パネルの画像を通じてオペレーションを公表しています。

最近では「OPSpain」などのオペレーションにも参加しました。OPSpainは主にNoName057(16)が主導する政治目的のサイバーキャンペーンです。ウクライナに対するスペインの政治・軍事支援への報復として、スペインのデジタルインフラを標的にしています。図25のTelegram投稿には、次のような内容が記載されています。

> 西側諸国は、当然の報いを受け続けている。 😜
>
> スペインの政治家はウクライナへの武器供与に従順に賛成し、ブリュッセルにこびへつらっている。その間に、われわれは彼らの快適な住宅へ入り込み、暖房、給湯、生活環境を支えるシステムを掌握する。
>
> この動画に映っているのは、スペインの個人住宅に設置された暖房・ホームオートメーション用の完全な制御システムだ。
>
> われわれは、このインフラ全体への完全なアクセスを得ている。

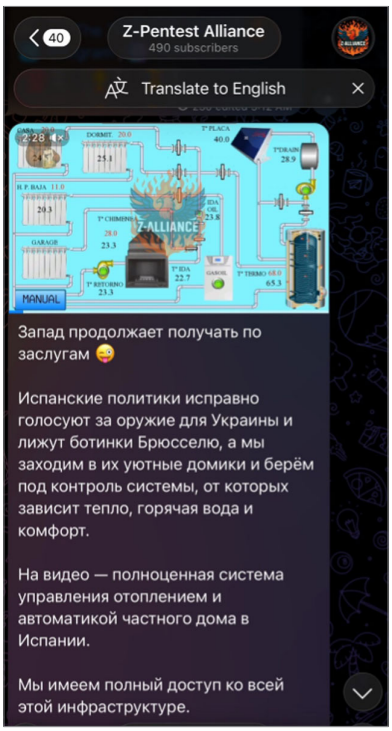



図25：2026年7月13日のOPSpainの一環として、スペインの暖房・ホームオートメーション制御システム全体を映したTelegramチャネルの動画のスクリーンショット

## Sector 16

Z-Pentestから直接派生したSector 16は、2025年1月に登場しました。親グループの手法を引き継ぎ、米国と欧州のエネルギー、電力、製造業を標的にしました。人員、ツール、標的選定の方法はグループ間で公然と継承され、その継続性の背後には国家による支援が存在する可能性があります。

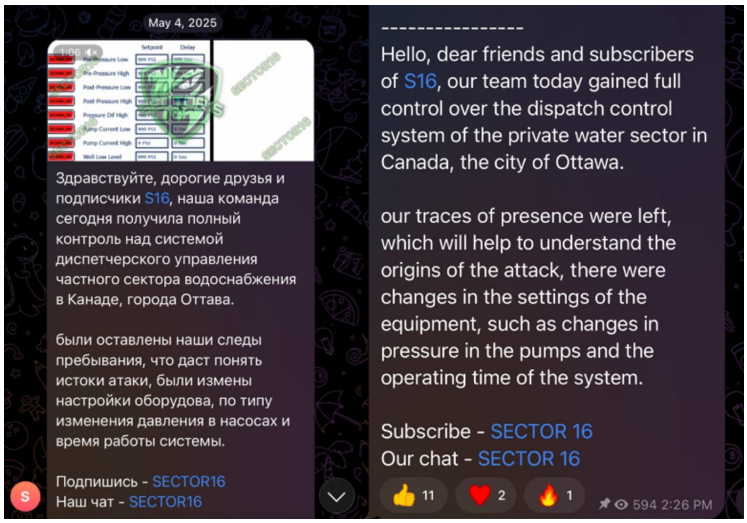



図26：2025年5月4日、オタワの水処理プラントへのアクセスを主張したSector 16のTelegram投稿のスクリーンショット

## Dark Engine

2025年に登場したDark Engine（別名Infrastructure Destruction Squad）は、外部に露出したインターフェースを狙う手法を、EU、アジア、中南米の製造、化学、エネルギー、水道資産に対して使用しました。

2026年5月以降、同グループは「BankGhost Builder」というMaaS（Malware as a Service）型のバンキングトロイの木馬を提供しています。このマルウェアを使うと、攻撃者はセッションの乗っ取り、認証情報の窃取、二要素認証（2FA）の回避、フィッシングキャンペーンの実行が可能になります。アクセスはTelegramチャネルで販売されることが多く、最低価格は200米ドルでした。

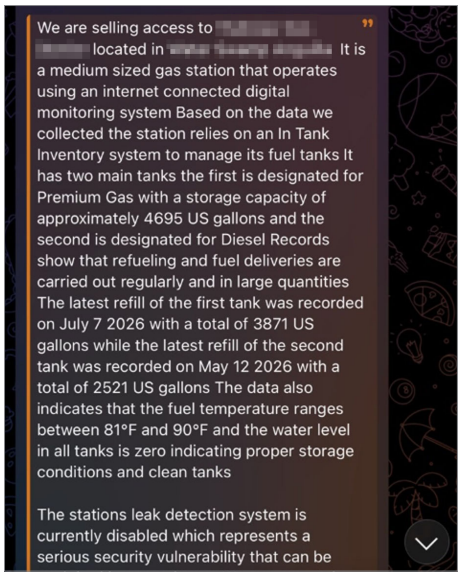



図27：2026年7月14日、アンギラの高速道路沿いのガソリンスタンドへのアクセスを200米ドルで販売するTelegram投稿のスクリーンショット

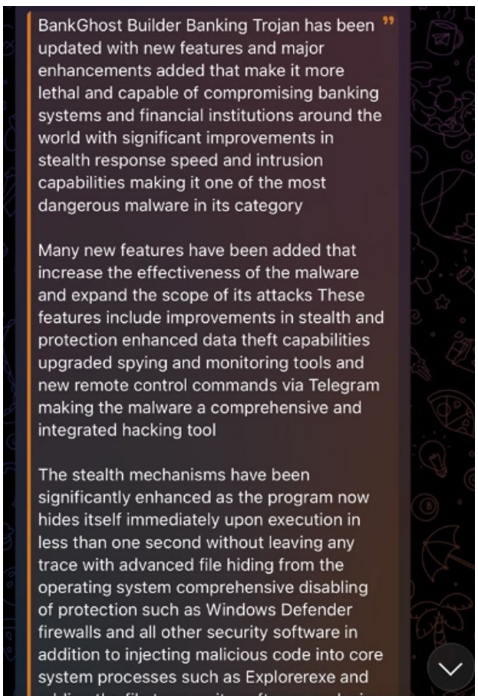



図28：2026年7月14日、バンキングトロイの木馬「BankGhost Builder」の更新を告知するTelegram投稿のスクリーンショット

## TwoNet

2025年1月から活動するTwoNetは、ウクライナ、EU、独立国家共同体（CIS）諸国のエネルギー施設と水処理施設を重点的に狙いました。水処理を特に重視していることから、公益事業の業務システムだけでなく、プロセス制御層まで標的にしていると主張する攻撃者の一つに数えられます。

## CyberTroops

2024年9月から活動するCyberTroopsは、スペインとEU全域の風力・太陽光発電を含むエネルギー・電力関連の標的に注力しました。従来型の送電網や水道インフラを主に狙う他のグループとは異なり、再生可能エネルギー発電資産への集中が特徴です。

## Blackjack

親ロシア、親イランのいずれのグループ群とも異なるBlackjackは、調査期間中にハクティビストによるOTオペレーションが到達した上限を示す存在です。

Blackjackはウクライナを支援する目的で2024年4月に登場し、モスクワの自治体OTシステムに投入されたFuxnetマルウェアとの関連が指摘されています。単にアクセスを主張するだけでなく、制御環境を実際に妨害したことが確認された、数少ないハクティビスト事例の一つです。規模の面では例外的ですが、より数の多い「アクセスと主張」を中心とするオペレーションの能力を測る基準となります。

表2と表3は、攻撃者グループと対象業界を地政学的な陣営別にまとめたものです。

| グループ | 活動開始 | 主な地域 | OT／ICS | 主な業界 | 帰属・性格 |
|---|---|---|---|---|---|
| **親ロシア** | | | | | |
| Z-Pentest | 2024年9月 | 欧州、NATO、米国、台湾 | あり | エネルギー、水道、石油・ガス、製造 | 国家との関連が疑われる |
| NoName057(16) | 2022年 | ウクライナ、NATO、EU | あり | エネルギー、水道、交通 | 親ロシアの集団 |
| Dark Engine | 2025年 | EU、アジア、中南米 | あり | 製造、化学、エネルギー、水道 | ハクティビスト |
| Sector 16 | 2025年1月 | 米国、ドイツ、イタリア、ポーランド | あり | エネルギー、電力、製造 | 国家支援の可能性 |
| TwoNet | 2025年1月 | ウクライナ、EU、旧CIS諸国 | あり | エネルギー、水処理 | ハクティビスト |
| CyberTroops | 2024年9月 | スペイン、EU | あり | エネルギー（風力、太陽光）、電力 | ハクティビスト |
| **親ウクライナ** | | | | | |
| Blackjack | 2024年4月 | ロシア（モスクワ） | あり | 自治体OT（Fuxnetワイパー） | ハクティビスト（自称） |

| グループ | 活動開始 | 主な地域 | OT／ICS | 主な業界 | 帰属・性格 |
|---|---|---|---|---|---|
| **親イラン／反イスラエル** | | | | | |
| Hunt3r Kill3rs | 2024年 | 米国、イタリア、イスラエルと同盟国 | あり | エネルギー（原子力を含む）、PLC | ハクティビスト／犯罪者 |
| Handala | 2023年12月 | イスラエル、米国、湾岸諸国 | あり | エネルギー、製造（データ層） | イラン情報安全保障省（MOIS）のフロント組織 |

表2：本リサーチで観測された、2024年から2026年にかけてIE&M分野を標的としたハクティビストグループの概要。地政学的な陣営別に分類しています。OT／ICS欄の「あり」は、ICS／SCADAへの標的化が確認または主張されていることを示します。

| グループ | エネルギー | 水道 | 石油・ガス | 製造 | 交通 | 化学 |
|---|---|---|---|---|---|---|
| **親ロシア** | | | | | | |
| Z-Pentest | X | X | X | X | X | · |
| NoName057(16) | X | X | · | · | X | · |
| Dark Engine | X | X | · | X | · | X |
| Sector 16 | X | · | · | X | · | · |
| TwoNet | X | X | · | · | · | · |
| CyberTroops | X | · | · | · | · | · |
| **親ウクライナ** | | | | | | |
| Blackjack | · | X | · | · | · | · |
| **親イラン／反イスラエル** | | | | | | |
| Hunt3r Kill3rs | X | · | X | X | · | · |
| Handala | X | · | · | X | · | · |

表3：本リサーチで観測されたハクティビストグループによる業界別の標的化

表3の「X」は、OT／ICSまたはSCADAへの標的化が確認または主張されていることを示します。「·」は、確認した情報源では該当する活動が報告されていないことを示します。

Z-Pentest、NoName057(16)、CARR、Sector 16は、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）、連邦捜査局（FBI）、国家安全保障局（NSA）が2025年12月に発行した共同勧告AA25-343Aで名指しされました。[7] この勧告は、これらを産業インフラのOTシステムを特に活発に標的としている親ロシアのグループと位置付けています。外部に露出したVNC接続を悪用し、水道、エネルギー、食料・農業分野の制御機器へ到達していました。

注目すべきは、こうしたスキルの低い攻撃者が現実世界への影響を実際にもたらしていた点です。APT（Advanced Persistent Threat）ほどの技術的な深さはないものの、その攻撃は水道、エネルギー、食料・農業システムにわたり、物理的被害を含むさまざまな影響を残しました。

## GhostSec

GhostSecは、ハクティビストを取り巻く状況の中でも異例の位置を占めるため、別に取り上げます。その変遷は一直線ではなく、一巡して元に戻るような経路をたどりました。

同グループは2015年、Anonymousから派生した集団として登場しました。Charlie Hebdo襲撃事件後、ジハード主義者のプロパガンダや人員募集基盤を狙った「#OpISIS」など、イデオロギーを動機とする対テロキャンペーンで評価を築きました。

しかし2022年後半から、GhostSecは金銭目的のサイバー犯罪へ明確に軸足を移しました。2023年10月に「GhostLocker」というRaaSプラットフォームを開始し、2024年初頭にはGolangベースの「GhostLocker 2.0」へ更新しました。アフィリエイトがキャンペーンと支払いを追跡できる、包括的な管理パネルを備えていました。2024年5月15日、同グループはランサムウェアからの撤退と、彼らが「純粋なハクティビズム」と呼ぶ活動への復帰を発表しました。政治活動を継続するのに十分な資金を確保したため、GhostLockerのソースコードとRaaSの運営を譲渡すると説明しています。

GhostSecにとってランサムウェアは、イデオロギーを捨てた結果ではなく、その活動に資金を供給する手段でした。サイバー犯罪を最終目的ではなく、ハクティビストの活動を支える収益源として利用したのです。

現在、GhostSecはTelegramでハクティビスト活動を発表する一方、サイバー犯罪フォーラム「breached.st」にも投稿しています。

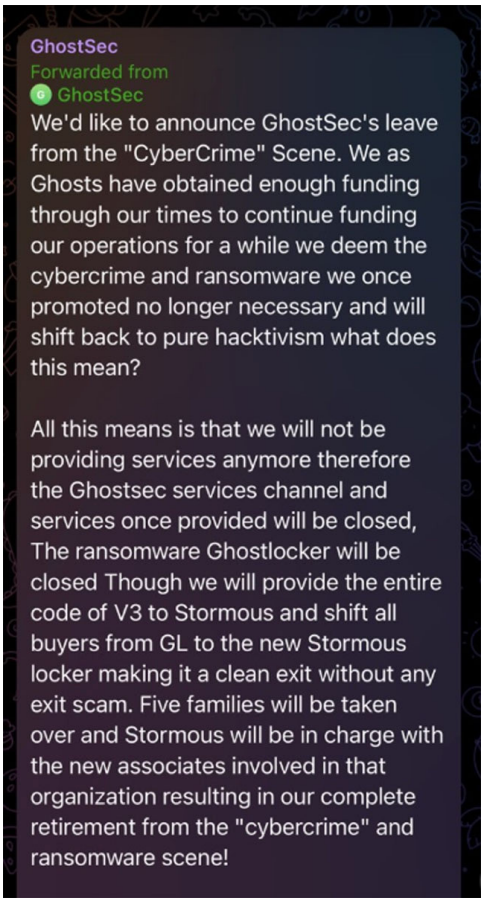



図29：2024年5月15日、GhostSecのRaaS終了を告知するTelegram投稿のスクリーンショット

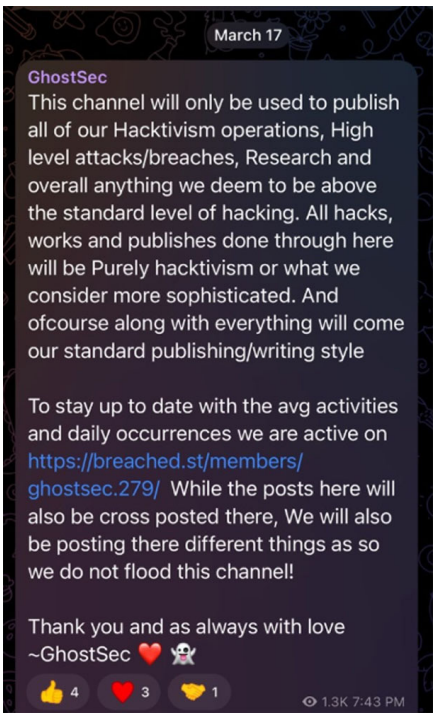



図30：2026年5月22日から活動内容をbreached.stフォーラムに投稿すると告知するTelegramメッセージのスクリーンショット

## 地政学的な陣営

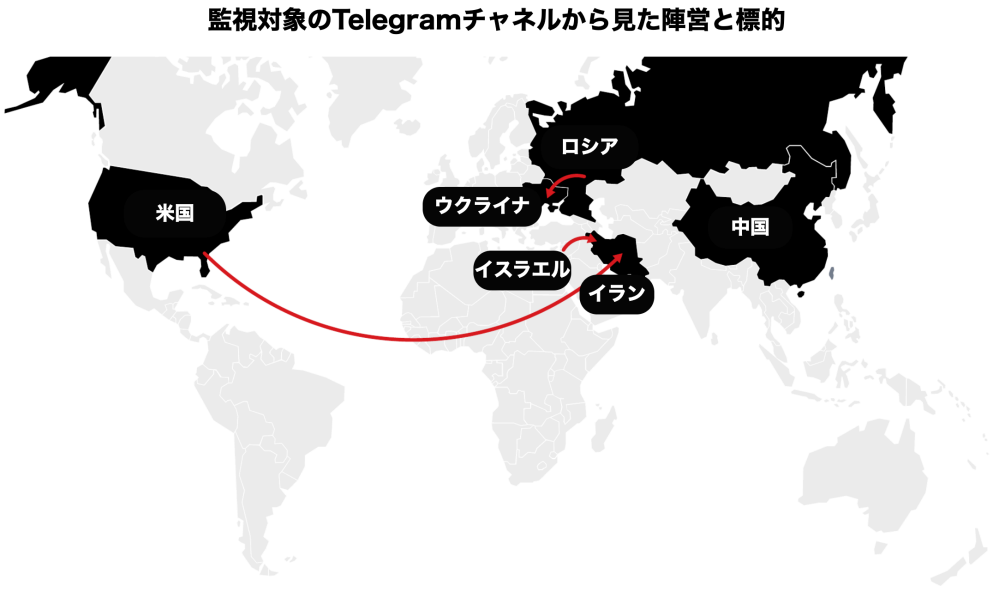



図31：ICSを標的とするハクティビズムの地政学的構造

図31は、本リサーチで監視したTelegramチャネルから、ICSを標的とするハクティビズムの地政学的構造を整理したものです。地図上の矢印は、活動が集中する2つの主要な対立軸を示しています。

一つ目の、より大きな対立軸は、イランから米国を経てイスラエルへとつながります。この軸に沿った活動の大半を3つのグループが担っています。Handalaは、BLEnergyのバッテリーエネルギー貯蔵システムへの攻撃を主張しました。

二つ目の軸はロシアとウクライナの間にあり、NoName057(16)などの親ロシア集団が中心です。活動は、西側諸国の公益事業インフラを狙うDDoSキャンペーンや、PLCを改ざんしたという主張に集中しています。GhostSecは両方の軸にまたがり、ハクティビストとしての動機とランサムウェア活動を併せ持つ存在です。

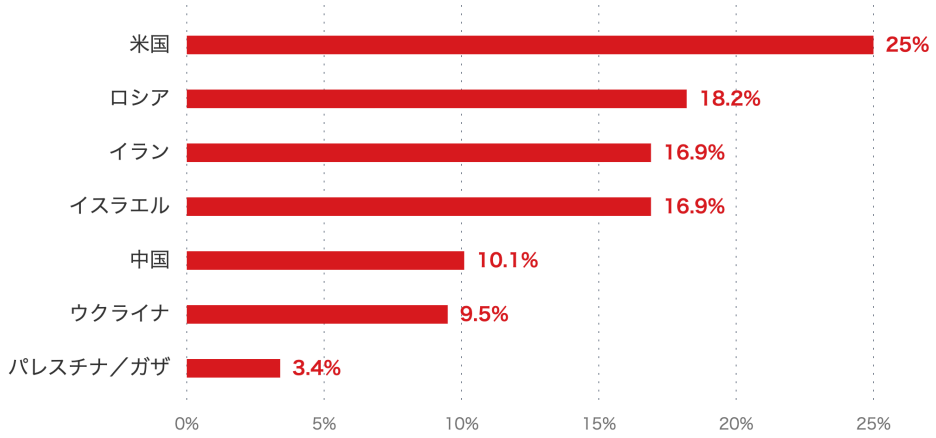



図32：本リサーチで監視したTelegramチャネルにおける国・地域別の言及割合

図32は、国・地域への言及割合を順位付けしたものです。米国が25.0%で首位となり、ロシアが18.2%、イランとイスラエルが同率の16.9%で続きます。中国は10.1%、ウクライナは9.5%、パレスチナ／ガザは3.4%でした。

## GasPotとCISAのイラン関連勧告

2015年、TrendAI™ Researchは、Veeder-Root Guardian ASTタンク監視システムを模したハニーポット「GasPot」を構築しました。[8] 7か国に配備してから6か月以内に、攻撃者がATG（Automatic Tank Gauge：自動タンクゲージ）システムを活発にスキャンし、接続し、改ざんしていることが確認されました。

ハニーポットで記録された活動は、本リサーチで先に説明したハクティビストと、イランとの関連が疑われる脅威のパターンにそのまま重なります。ヨルダンに設置したGasPotでは、タンク名が「H4CK3D by IDC-TEAM」に変更されました。これは、イランのDark Coders Teamが使う署名です。同グループは、Webサイトの改ざんやハクティビズムで知られる親イランの攻撃者です。一方、米国ワシントンD.C.周辺に設置したGasPotは、Low-Orbit Ion Cannon（LOIC）ツールを使った2日間のDDoS攻撃を受けました。GETリクエストのペイロードには、Syrian Electronic Army（SEA）を指す「SEAcannnGO」という文字列が含まれていました。[9]

これは、イランやシリアの利益との関連が疑われるハクティビストグループが、Webサイトだけでなく産業インフラも探っていたことを示す最初期の兆候の一つです。

ハニーポットへの全攻撃の44%は米国で発生し、攻撃元はイラン、シリア、ルーマニア、メキシコ、中国にまで及びました。

この結果はBlack Hatで発表され[10]、詳細はTrendAI™のリサーチペーパーにまとめられています。[11]

その後の10年間に起きたことは、IE&M分野のアンダーグラウンドで現在確認されているものと同じ激化の過程を示しています。機会便乗型の攻撃者が組織的なオペレーションへ移行し、ハクティビストのツールは国家支援型の能力へと成熟しました。

2023年11月、CISAはUnitronics製PLCを狙ったキャンペーンを、イランのIRGC傘下で活動するCyberAv3ngersによるものと判断しました。[12] 米国財務省は2024年2月、IRGC関係者6人を制裁対象に指定しました。[13] 2026年4月には、6機関による共同勧告AA26-097Aが、CyberAv3ngersによる「IOCONTROL」の開発を確認しました。これは、燃料管理システムを含むLinuxベースのIoT・OT機器上で動作する、ICS専用のマルウェアプラットフォームです。[14]

2026年5月、CNNは米国の複数州のガソリンスタンドで、イランによるATGシステムへの侵害が確認されたと報じました。[15] 同年6月、CISAは7つの連邦機関と共同でファクトシートを発行し、活発化する脅威からATGシステムを保護するよう事業者に呼びかけました。[16] 7月には、連邦政府機関が米国の産業インフラを標的とするPLCの悪用について警告しました。[17] この勧告では、攻撃者が運用画面を操作し、担当者が画面上の異常を目視で検知できない状態にしていたことも指摘されています。

2015年にIDC-TEAMがハニーポットのタンク名を改ざんしてから、2026年にIRGCとのつながりを持つ攻撃者が実在する燃料システムへ専用マルウェアを展開するまでの変遷は、IE&M分野のアンダーグラウンド全体で確認される傾向と一致します。ハクティビズムと国家支援型オペレーションの境界は曖昧です。現在はスキルの低い攻撃者の関心を集めるだけの標的でも、将来は組織的なキャンペーンの対象になり得ます。2026年6月時点で、1,562台のATGシステムがインターネットに公開されたままであり、その84%は米国内の一般的な商用インターネットサービスプロバイダ（ISP）回線に接続されています。

# 結論

IE&M分野のアンダーグラウンドは将来のリスクではなく、現在すでに稼働している経済です。アクセスブローカーは、窃取された認証情報や銀行データの取引に使われるのと同じフォーラム上で、同じエスクローの仕組みを使い、工場、公益事業、エネルギー企業への足がかりを販売しています。ランサムウェアグループはこうした足がかりを利用し、2年半で3,178件の被害組織を公表しました。その数は今も増加を続けています。ロシアやイランとの関連が疑われるハクティビストは、同じインフラをイデオロギー上の目的で標的としています。CISA、FBI、NSAは共同勧告AA25-343Aで、この領域ではスキルの低い攻撃者さえ物理的被害を引き起こしていると確認しました。[18] 正規価格が9,000米ドル以上のSANSコースを含むICS研修教材の海賊版が、アクセスを販売するのと同じフォーラムで無料流通し、すべての攻撃者にとっての参入障壁を下げています。

TrendAI™ Researchが調査してきた他のアンダーグラウンドとIE&M分野との違いは、同じ標的群に金銭的動機と地政学的意図が集中していることです。これに対し、医療分野のアンダーグラウンド[19]は、ほぼ全面的に金銭取引を目的としています。IE&M分野では、金銭目的のブローカーやランサムウェアグループと、SCADAのスクリーンショットをプロパガンダとしてTelegramに投稿するイデオロギー目的の攻撃者が、同じフォーラムで活動しています。同じ侵入経路、同じ海賊版教材を共有し、場合によっては人員も重複しています。

防御側への示唆は明快ですが、実行は容易ではありません。アクセスブローカーの侵入口は、ゼロデイ脆弱性ではなく、脆弱な認証情報や窃取された認証情報で保護されたVPNゲートウェイとRDPです。したがって、フィッシング耐性のある多要素認証（MFA）、エッジアプライアンスへの迅速なパッチ適用、ITとOTの確実な分離を実施すれば、産業分野へのアクセスが商品として持つ価値の大半を失わせることができます。

より難しいのは、こうした対策に継続的な投資が必要なことです。産業環境では従来、セキュリティ衛生より生産稼働時間が優先されてきました。多くのレガシーシステムは、そもそもネットワーク分離を前提として設計されていません。

TrendAI™ Researchは今後も、この経済の変化を追跡します。縮小ではなく拡大を示す兆候が確認されています。ランサムウェアの被害組織数は増加し、ハクティビストによるOT標的化は、対象範囲と地域の両面で拡大しています。さらに、研修教材が広く流通するほど、必要なスキルの水準も下がり続けます。

製造、エネルギー、水道システムを支えるインフラを運用する組織は、これをすでに存在する現在進行形の脅威として捉える必要があります。

# 推奨事項

- すべてのVPN、RDP、Citrix、リモートアクセスポータルにフィッシング耐性のあるMFAを必須とし、単要素認証と旧式の認証方式を廃止します。観測された最大の侵入経路であるVPNは、窃取された認証情報だけではアクセスできなくなれば、その大部分が無力化されます。

- インターネットに公開されたエッジアプライアンス（Fortinet、Citrix、Cisco、Palo Alto Networks、SonicWall）を「Tier 0」資産として扱います。緊急対応レベルの頻度でパッチを適用し、サポート終了機器を棚卸しして廃止します。

- 階層型管理、LAPS（Local Administrator Password Solution）、認証情報の適切な管理、特権認証の積極的な監視によって、アイデンティティとActive Directoryを強化します。ブローカーが実際に販売しているのは、ドメイン管理者権限やユーザアクセスだからです。

- ITとOTを分離し、SCADA、PLC、HMIネットワークへ直接到達できるフラットな経路を排除します。すべてのリモートアクセスを、強化されたDMZ（非武装地帯）のジャンプサーバ経由に限定し、監視下で保守アクセスを仲介します。境界をまたぐ通常の管理者操作のベースラインを整備し、可視性の欠如を解消します。

- ローカル環境の管理権限が及ばない改ざん不能なSIEM（セキュリティ情報イベント管理）へログを集約し、12か月を超えて保持します。

- 認証情報のサプライチェーンを監視します。スティーラーログや認証情報の露出を通知するフィードを購読し、露出したアカウントが武器化される前に強制リセットします。

- エンジニアと共同でOT専用のインシデント対応計画を策定し、年1回演習します。販売可能なIT上の足がかりが、制御不能な生産・安全上の事故へ発展しないよう、ランサムウェアと恐喝のシナリオを訓練します。

- 出品件数ではなく、被害の大きさに基づいて防御投資の優先順位を決めます。公益事業、発電、石油・ガス、水道は、観測されるアクセス件数が比較的少なくても、より手厚い保護が必要です。

## TrendAI Vision One™プラットフォームとの対応

- **TrendAI Vision One™ Agentic SIEM**は、ヒストリアン、HMI、SCADA、ネットワーク、アイデンティティから得られるIT・OTログをAIネイティブなプラットフォームへ集約し、ローカル環境の管理権限が及ばない改ざん不能な領域で12か月を超えて保持します。振る舞いのベースラインからの逸脱を検出するため、静的なしきい値ベースのルールでは捉えにくいラテラルムーブメントや、エンジニアリングワークステーション上の異常な操作を発見できます。

- **TrendAI Vision One™ XDR for Networks**は、インライン（TrendAI™ TippingPoint™）とアウトオブバンド（TrendAI™ Deep Discovery™ Inspector）のテレメトリをIT・OTセグメント全体で関連付け、一つの検知像にまとめます。エージェントを実行できないOT機器にソフトウェアを導入することなく、IT/OT境界を横断する多段階の攻撃チェーンを可視化します。

- **TrendAI Vision One™ Network Sensor**は、DMZのジャンプポイントとOTゾーン内部でトラフィックを受動的に取得します。管理されていない資産を棚卸しし、境界をまたぐ通常の管理・保守操作のベースラインを整備します。制御システムの通信を妨げることなく、可視性の欠如を解消できます。

- **TrendAI Vision One™ Cyber Risk Exposure Management（CREM）**は、インターネットに公開されたエッジアプライアンス、アイデンティティ、OT資産を発見してリスクを評価し、インターネット上の露出から生産システムまでの攻撃経路を可視化します。単純なCVE件数ではなく、影響の大きさと悪用可能性に基づいて修復の優先順位を付けます。

- **TrendAI™ TippingPoint™**は、TrendAI™ Zero Day Initiative™（ZDI）の調査に基づく仮想パッチを使い、境界およびIT/OT境界で既知のエクスプロイトをインラインで遮断します。この仮想パッチは、ベンダ自身のパッチより90〜120日早く提供されることがあります。通常の頻度ではパッチを適用できないエッジアプライアンスやレガシーOTシステムを補う制御策です。

- **TrendAI™ Deep Discovery™ Inspector**は、IT/OT境界および制御ゾーン内部の東西トラフィックを監視し、100を超えるプロトコルにわたってコマンド＆コントロール（C&C）活動、ラテラルムーブメント、OTを標的とするマルウェアを検出します。すでにIT上の足がかりを得たブローカーや侵入者がSCADAやPLCシステムへ移動する前に検知できるよう設計されています。

# 参考文献


1. Trend Micro Research（2025年7月1日）Trend Micro「The Trend Micro Underground Series」（英語）。2026年8月10日参照。

2. Stephen Hiltほか（2018年）Trend Micro「Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries」（英語）。2026年8月10日参照。

3. Kyle Wilhoit（2013年）Trend Micro「The SCADA That Didn't Cry Wolf: Who's Really Attacking Your ICS Equipment? (Part 2)」（英語）。2026年8月10日参照。

4. Stephen Hiltほか（2020年）Trend Micro「Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats」（英語）。2026年8月10日参照。

5. Justin Searle（発行年不明）SANS Institute「ICS410: ICS/SCADA Security Essentials」（英語）。2026年8月10日参照。

6. Connor Jones（2026年7月29日）The Register「Iran-linked CyberAv3ngers suspected in attacks on Minnesota water systems」（英語）。2026年8月10日参照。

7. CISA、FBI、NSA（2025年12月9日）米国サイバーセキュリティ・インフラセキュリティ庁（CISA）「Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure (AA25-343A)」（英語）。2026年8月10日参照。

8. Kyle Wilhoit、Stephen Hilt（2015年）GitHub「GasPot」（英語）。2026年8月10日参照。

9. Adam Greenberg（2015年8月6日）SC Media「Black Hat 2015: Honeypots Gather Data on Gas Pump Monitoring System Attacks」（英語）。2026年8月10日参照。

10. Kyle Wilhoit、Stephen Hilt（2015年8月5日）Black Hat「The Little Pump Gauge That Could: Attacks Against Gas Pump Monitoring Systems」（英語）。2026年8月10日参照。

11. Kyle Wilhoit、Stephen Hilt（2015年）Trend Micro「The GasPot Experiment: Unexamined Perils in Using Gas-Tank-Monitoring Systems」（英語）。2026年8月10日参照。

12. FBIほか（2023年12月1日）米国サイバーセキュリティ・インフラセキュリティ庁（CISA）「IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (AA23-335A)」（英語）。2026年8月10日参照。

13. 米国財務省（2024年2月2日）「Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure」（英語）。2026年8月10日参照。

14. FBIほか（2026年4月7日）米国サイバーセキュリティ・インフラセキュリティ庁（CISA）「Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure (AA26-097A)」（英語）。2026年8月10日参照。

15. Sean Lyngaas（2026年5月15日）CNN Politics「Hackers have breached tank readers at gas stations; officials suspect Iran is responsible」（英語）。2026年8月10日参照。

16. CISAほか（2026年6月2日）米国サイバーセキュリティ・インフラセキュリティ庁（CISA）「CISA and Partners Urge Hardening Automatic Tank Gauge Systems」（英語）。2026年8月10日参照。

17. Jamal Bethea（2026年7月23日）Trend Micro「米国の産業インフラを狙う継続中のPLC悪用攻撃について連邦機関が警告」。2026年8月10日参照。

18. FBI、CISA、NSA（2025年12月9日）米国サイバーセキュリティ・インフラセキュリティ庁（CISA）「Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure (AA25-343A)」（英語）。2026年8月10日参照。

19. Stephen Hilt、Numaan Huq、Mayra Rosario Fuentes（2026年6月4日）TrendAI™「アンダーグラウンドで取引される医療データエコノミー」。2026年8月10日参照。

このようなインサイトをもっと見る

**TrendAI™ Deep Research**

TrendAI™

TrendAI™は、AIセキュリティを世界規模でリードするTrend Microのエンタープライズ事業部門です。組織全体にわたるAIの可視性と統合セキュリティを提供し、信頼に基づくイノベーションを後押しするとともに、リスクの解消を支援します。

185か国の大手企業や政府機関から信頼を得ているTrendAI™は、アイデンティティ、インフラ、データに至る組織全体を保護します。

AI Fearlessly.

trendaisecurity.comで詳細を見る