INSITE: 攻撃観測網とOSINT/HUMINTの融合による サイバーセキュリティ情報収集・分析・対策機構

吉岡 克成[3,4,a)]　金子 翔威[1]　青山 航大[2]　九鬼 琉[1]　インミンパパ[3]　佐々木 貴之[3]　田辺 瑠偉[3]

概要：本稿では, 従来からのサイバー攻撃観測や広域スキャンといった直接的なサイバーセキュリティ情報収集手段に加えて, 攻撃の背景となるサイバー攻撃ビジネスや資金の流れ, それらに係る多様な攻撃者の活動を観測するためにオープンソースインテリジェンス (OSINT), ヒューマンインテリジェンス (HUMINT) の収集能力を強化し, これらの融合により, サイバー攻撃のエコシステムや背景を把握し, 対策の効果を向上させる, 新しいサイバーセキュリティ情報収集・分析・対策機構 INSITE (INtegrated Security Intelligence for Tactical Execution) を提案し，その先行事例を示す.

キーワード：サイバーセキュリティ情報収集, 分析, 対策

INSITE: Cybersecurity Framework Integrating Attack Observation with OSINT/HUMINT

Katsunari Yoshioka[3,4,a)]　Shoi Kaneko[1]　Koudai Aoyama[2]　Ryu Kuki[1]　Yin Minn Pa Pa[3]
Takayuki Sasaki[3]　Rui Tanabe[3]

Abstract: We propose a new cybersecurity mechanism called INtegrated Security Intelligence for Tactical Execution (INSITE). In addition to traditional cyber attack observation, INSITE enhances open-source intelligence (OSINT) and human intelligence (HUMINT). By integrating these capabilities, it aims to better understand the ecosystem and backgrounds of cyber attacks, thereby improving the effectiveness of countermeasures. We also present preliminary cases of this approach.

Keywords: cybersecurity, information collection, analysis, countermeasures

1. はじめに

増大するサイバー脅威に対して, これらを観測・分析し, 有効な対策を導出する研究活動が重要となっている. 我々は, ハニーポット等を用いた受動的な観測と, 広域スキャン等による能動的な観測を融合してインターネット上のサイバーセキュリティ情報を収集し, 攻撃の実態を把握することで効果的な対策を導出・実行するというコンセプト [1] に基づき研究開発を実施してきた [2], [3], [4], [5], [6]. しかし, 昨今の多様化, 高度化, 複雑化する脅威に対して従来からの観測網に基づく情報収集だけでは，その実態を正確に把握し効果的な対策を導出することは難しくなっている. 例えば, IoT ボットネットの攻撃を観測し [2], 収集したボット検体を解析することで C&C サーバ等の攻撃インフラを分析したり [4], ボットに感染した利用者に注意喚起を行うことが出来るが [5], [6], これらは対処療法的対策であ

[1] 横浜国立大学理工学部
College of Engineering Science, 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
Faculty of Environment and Information Sciences, Yokohama National University
[a)] yoshioka@ynu.ac.jp

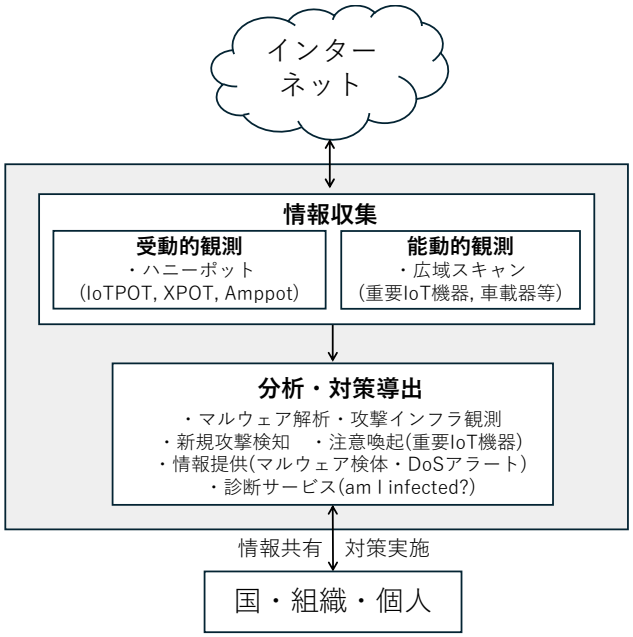

図 1　横浜国大における従来の情報収集・分析・対策機構

り, 脅威の源泉への根本的対策ではない. そこで本稿では, 従来からのサイバー攻撃観測や広域スキャンといった直接的なサイバーセキュリティ情報収集手段に加えて, 攻撃の背景となるサイバー攻撃ビジネスや資金の流れ, それらに係る多様な攻撃者の活動を観測するためにオープンソースインテリジェンス (OSINT), ヒューマンインテリジェンス (HUMINT) の収集能力を強化し, これらの融合により, サイバー攻撃のエコシステムや背景を把握し, 対策の効果を向上させる, 新しいサイバーセキュリティ情報収集・分析・対策機構 **INSITE (INtegrated Security Intelligence for Tactical Execution)** を提案する. 当該機構では, 外部のインテリジェンスを積極的に活用し, 自らの情報収集機能により得られた情報と比較, 突合することで, 情報の信ぴょう性を見積もり, 効果的な対策導出につなげる. 本稿では，まず従来のサイバーセキュリティ情報収集・分析・観測機構とその課題に触れ，次に新しい機構 INSITE の全体像と構成要素である情報収集，分析，対策の機能強化について説明する．さらに，この機構の概念に基づき先行的に着手した情報収集・分析・対策導出事例を示す.

2. 従来の情報収集・分析・対策機構

我々は, ハニーポット等を用いた受動的な観測と, 広域スキャン等による能動的な観測を融合してインターネット上のサイバーセキュリティ情報を収集し, 攻撃の実態を把握することで効果的な対策を導出・実行する，サイバーセキュリティ情報収集・分析・対策機構 [1](図 1) に基づき様々な研究開発を実施してきた. 以下ではその概要を説明し，従来の機構の課題を示す.

情報収集: インターネットから届く攻撃を待ち受ける性質をもつ**受動的観測**として IoT 機器への攻撃を観測する 2 種類のハニーポット IoTPOT[2], X-POT[7]，リフレクション型のサービス妨害攻撃を観測するハニーポット Amppot[8] を定常運用すると共に，脅威の変遷に応じて様々な攻撃の観測に特化したハニーポットを構築・運用してきた．一方，インターネット上の機器やシステムに能動的にアクセスし，情報を収集する**能動的観測**として，広域スキャンシステムを構築し，重要施設に設置された遠隔監視制御機器や車載器の広域スキャンによる探索等を実施してきた [3], [9].

分析・対策実施: ハニーポットで観測した攻撃がどの脆弱性を狙うものであるかを判別し，新規性の高い攻撃を検出する技術 [10] を運用し，実際にゼロデイ攻撃を検知し CVE を取得している [11]．ハニーポットにより収集したマルウェア検体を動的解析し，C&C サーバを推定すると共に，ボットの通信を模擬する疑似マルウェアスクリプトを動作させ，継続的な攻撃インフラ観測を行ってきた [12], [13]．IoTPOT 等の観測結果は，累計 40 か国 250 以上の組織に提供を行い [14]，Amppot の観測結果に基づく DoS 攻撃アラートを ICT-ISAC を通じて国内の主要 ISP に，Shadowserver foundation を通じて，130 の National CERT と 6000 以上のネットワークオペレータに提供している [15]．重要施設に設置された機器については総務省の 3 度の調査 [16] に協力し，これまで重要施設に設置されていると推測される機器を累計で 1,000 件以上発見し，そのセキュリティ対策に貢献している [3]．加えて，一般家庭の IoT 機器のセキュリティ状態を診断し，必要な対策を示すセキュリティ診断サービス am I infected?[17] を運用し，これまでに 11 万人以上に利用されている.

従来の機構の課題: 受動的観測と能動的観測により収集されるサイバーセキュリティ情報はサイバー攻撃やマルウェア，または，サイバー攻撃の対象となる機器のセキュリティ状態などサイバー攻撃に直接的に関わる情報であり，これらは攻撃を検知，遮断するための防御手段の導出や感染・脆弱状態である機器への対策を行う上で有益である．一方，これらのサイバー攻撃の源泉である攻撃者の動機や目的，攻撃者間の関係等を把握することは難しい．そのため，従来の機構では既に確認された脅威への対処療法的な対策に留まり，根本的対策につながりにくいという課題があった．さらに従来の機構では外部の情報・インテリジェンスを十分活用できておらず，昨今の多様化する脅威に対して効率的な情報収集・分析が行えていなかった．次章で説明する新機構ではこれらの課題を解決する構想を示す.

3. 新たなサイバーセキュリティ情報収集・分析・対策機構 INSITE

本章では従来の情報収集・分析・対策機構の課題を解決する新たな機構である INSITE (INtegrated Security Intelligence for Tactical Execution) を説明する.

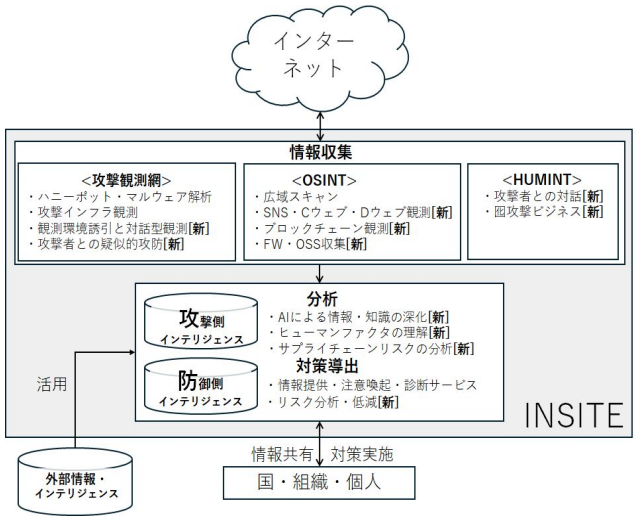

図 2 サイバーセキュリティ情報収集・分析・対策機構 INSITE

3.1 概要

INSITE の全体図を図 2 に示す．なお，図において [新] と記載がある項目は INSITE において新たに研究開発に取り組む技術であり，その概要は次節以降で説明する．INSITE では，サイバーセキュリティ情報を次の 3 つの方法で収集する．具体的には，サイバー攻撃や攻撃に係る対象を直接的に観測するハニーポットや攻撃インフラ観測などの**攻撃観測網**，広域スキャンや Web クローリングによりオープンにアクセス可能な情報源から有益な情報を収集するオープンソースインテリジェンス **(OSINT)**，攻撃者や被害者などからサイバー攻撃に関する様々な情報を収集するヒューマンインテリジェンス **(HUMINT)** を連携させることで情報収集能力を強化する．

収集された情報を分析し，意思決定と対策実行に資する知見，すなわち「インテリジェンス」に深化させる．INSITE では，特に攻撃者の攻撃手法，攻撃インフラ，動機，ビジネスモデル，攻撃組織など，攻撃者に係る**攻撃側インテリジェンス**，サイバー攻撃の対象となる組織や個人に係る**防御側インテリジェンス**と位置づけ，特に AI を活用し，それぞれの獲得を目指す．攻撃側インテリジェンスにより「敵を知り」，防御側インテリジェンスにより「己を知る」ことで状況を適切に把握し効果的な対策を導出する．さらに技術的要素に加えてこれらの効果に大きな影響を与える**ヒューマンファクタの理解**に注力する．また自らの情報収集機能に頼るだけでなく，**外部からの情報・インテリジェンス**を積極的に活用し，比較・検討により情報の信ぴょう性を評価し，分析を深化することで対策の効果を向上させる．以下では各構成要素について概説する．

3.2 情報収集

攻撃観測網: 従来のハニーポットやマルウェア解析，攻撃インフラ監視に加えて，OSINT や HUMINT と連携し，観測環境へ攻撃者を誘引すると共に，観測時に防御行動や欺瞞技術を試行し，より効果的に攻撃を観測する技術として**観測環境への攻撃者の誘因と対話型観測**に新たに取り組む．この技術では，従来までのハニーポットの概念を拡張し，攻撃者の興味を引く脆弱機器の情報やアクセス権限情報を囮として攻撃者コミュニティに流布し，積極的に観測環境に誘引することで効果的な攻撃観測を目指す．さらに，組織内ネットワークに侵入後の攻撃者の横展開等の活動を観測するために NICT のサイバー攻撃誘引基盤 STARDUST[18] を活用し，誘引した攻撃者へのディセプション技術の効果検証等を行う．加えて，IoT 機器等の踏み台 (Operational Relay Box) 化によるサイバー攻撃への悪用を能動的に防ぐ手段を検討するため，感染状態の機器における**攻撃者との疑似的攻防**を行う環境を構築する [19], [20].

OSINT: 従来からの広域スキャンによる IoT 機器等の探索に加えて，**SNS やダークウェブ，クリアウェブにおける攻撃者の活動観測**に取り組む．サイバー攻撃ビジネスやハクティビストの情報発信，ビジネスコミュニケーションが Telegram, Discord などの SNS やダークウエーブのランサムウェアグループサイト，リークデータや攻撃ツール、攻撃サービスのマーケットに拡大している．また，GitHub 等のクリアウェブサイトにおいて脆弱性を攻撃する PoC コードや攻撃ツールが公開されていることから，これらの情報を収集し，攻撃側インテリジェンスを強化する [10], [21], [22], [23]．加えて，サイバー攻撃ビジネスに利用される仮想通貨の流動を把握するために**ブロックチェーンの観測** [24], [25]，防御側インテリジェンスを高度化するために **OSS や IoT 機器のファームウェアの収集**を行い，それらが有する脆弱性の分析を行う [26].

HUMINT: ハニーポットにアクセスする攻撃者のプロファイリング [27] を行うと共にこれらの**攻撃者や SNS・フォーラム参加者との対話**を行い，サイバー攻撃ビジネスに関する慣習や動向を調査する手法を検討する．特に前述の攻撃者の誘因に関係して，組織ネットワークへのアクセス権を販売するブローカの振る舞いを調査し，これを模擬することで観測環境への攻撃者の誘因を行う**囮の攻撃ビジネス**による調査を検討する．

3.3 分析と対策導出

収集情報の AI による分析と深化に注力し，情報収集活動により得られる多様な情報を対策などの意思決定に資する情報であるインテリジェンスに深化させる．具体的には，サイバー攻撃の進化を AI によって推測し，先回りした対策を行う方法を検討しており，マルウェア生成 [28]，多様化 [29]，耐解析機能 [30] に関して AI によるサイバー攻撃の高度化の可能性を検証し，これらのマルウェアに対抗する解析技術の高度化を検討している．また，広域スキャンで発見した機器や施設の自動識別 [31] や，SNS 等で収集される膨大な情報の中からサイバー攻撃関連情報を抽出する

作業 [21] や隠語の理解 [32] など，従来，人手で行っていた様々な知的作業の自動化を進めている．

ヒューマンファクタの理解に基づくインテリジェンスの獲得を目指すことで，利用者のセキュリティリスクの理解や適切な使用を促進する．具体的には，機器メーカによるセキュリティリスクの説明の現状を把握し [33]，セキュリティ診断サービスである am I infected?[17] における具体的な対策手順の提示により注意喚起の効果を高める方法を検討中である [34]．**サプライチェーンリスクの分析**を，OSINT により収集したファームウェアや OSS における脆弱性 [26] や不正機能 [35] の伝搬，発生源を分析することで行い，機器等の製造工程におけるセキュリティ対策や迅速な脆弱性対策を行うための方法を検討する．

本機構の最終的な目標として，多様な情報源から獲得した攻撃側インテリジェンスと防御側インテリジェンスに基づき，組織や個人へのセキュリティリスクを総合的に評価し，これを低減する対策を示すための**リスク分析・低減**を目的とした技術に取り組む．

3.4 新たに獲得が期待されるインテリジェンス

INSITE で獲得が期待されるインテリジェンスについて表 1 にまとめ，新たな情報収集・分析技術がインテリジェンス獲得にどのように貢献し得るかを説明する．

攻撃手法・攻撃タイミング・攻撃インフラ: サイバー攻撃に直接的に関わるこれらの知見はハニーポットやマルウェア解析，攻撃インフラ監視など従来の攻撃観測網で獲得が可能であるが，新たに取り組む観測環境誘引と対話型観測，攻撃者との疑似的攻防，SNS 観測等の OSINT によって，攻撃対象情報の流通，攻撃予告情報を把握することで，攻撃の早期検知や未然対策につながる可能性がある．さらに，AI により攻撃の高度化を事前検証することで，まだ見ぬ未知の攻撃手法の知見が得られる可能性がある [29]．

動機・プロフィール・ビジネスモデル・攻撃者組織: これらの攻撃の背景に係る情報は従来の攻撃観測網や広域スキャンでは把握が難しかったが，SNS やダークウェブ，ブロックチェーン観測といった OSINT や攻撃者との対話や囮攻撃ビジネス等の HUMINT により，攻撃者の主張や攻撃ビジネスの実態，攻撃者間のやり取りを把握し，攻撃の背景理解につながる可能性がある．

攻撃対象・攻撃原因: 攻撃対象やその原因の一部はハニーポットや広域スキャンなど従来からの攻撃観測網や OSINT で把握することができるが，SNS やダークウェブ観測等の OSINT 拡張，HUMINT による攻撃者との対話や囮攻撃ビジネスにより，攻撃対象情報の流通，攻撃予告情報，攻撃対象への攻撃者コミュニティの興味の度合を把握し，攻撃対象やその原因となる脆弱性をより正確に把握できる可能性がある．さらに，機器のファームウェアや OSS 脆弱性をいち早く把握することで最新の攻撃の対象となり得る機器やシステム，組織を特定し，注意喚起を実施できる．

攻撃被害・対応: 攻撃被害やその対応については従来の攻撃観測網や OSINT では十分に把握が難しかったが，SNS 観測やリークデータマーケットの観測により，既に攻撃を受けた組織や個人の状態や，対応状況について把握できる可能性がある．特に漏洩した ID とパスワードのリスト (コンボリスト) などの認証情報は次なる攻撃に直接的につながる可能性があり，攻撃リスクの高まりを把握することで早期対策につながる．さらに、ランサムウエアグループサイトの監視による, 被害者とのチャット, 被害者リストの変更状況分析から攻撃被害, 対応を予測できる [22].

上記のように，INSITE により獲得されるインテリジェンスは従来の対策実施の幅を広げ，その効果を増大させることが期待される．次章では，INSITE の枠組みに基づく先行的な情報収集・分析・対策導出事例について説明する．

4. 先行的取り組み

本章では，INSITE の枠組みに基づき先行的に実施したサイバーセキュリティ情報収集・分析事例を説明する．

4.1 事例 1: 国内の太陽光発電監視機器への攻撃の分析

2024 年 5 月 1 日，国内の太陽光発電施設の遠隔監視機器がサイバー攻撃を受け，インターネットバンキングの不正送金に悪用されていたことが報道された [36]．我々が観測する 500 超の Telegram チャンネルにおいて当該機器に関する書き込みを調査したところ，攻撃者グループ「軍火庫」(「武器庫」の意) のチャンネルにおいて，2023 年 8 月頃に当該機器の 2 種類の脆弱性 CVE-2022-29303, CVE-2023-23333 に関する書き込みが多数発見された．また，同時期の同グループの投稿において福島原子力発電所の処理水の海洋放出に反対し，日本を攻撃せよという旨の書き込みがあり，それと共に当該機器を広域スキャンシステムで探索するための検索クエリや脆弱性を狙った攻撃を行うための PoC コードなどの具体的な攻撃手法が共有されていた (図 3)．さらに CVE-2023-23333 に関する書き込みでは，日本国内の多数の企業名からなる数 GB から数十 GB のファイル一覧の画像が共有されており，これはこれらの企業に攻撃を行うことにより取得した漏洩データである可能性があるが，これ以上の情報は確認できなかった．さらに別のチャンネルにおいても当該機器の別の脆弱性である CVE-2022-31373 への言及と当該脆弱性の PoC コードへのリンクが発見された．Telegram への投稿の調査によって得られた CVE の情報に基づき GitHub や Exploit-DB 上の公開情報を調査したところ，CVE-2022-29303，CVE-2022-31373，CVE-2023-23333 の PoC コードはそれぞれ 2022 年 5 月 17 日 (NVD での掲載の 5 日後), 2022 年 6 月 22 日 (NVD 掲載の翌日), 2023 年 2 月 6 日 (NVD 掲載当日) に公開されていた．

表 1　獲得が期待されるインテリジェンス

内容	説明	INSITE での主な情報源
攻撃側インテリジェンス		
攻撃手法	サイバー攻撃の戦術，技術，手順．攻撃手法，ツール，マルウェア等	攻撃観測網，OSINT
攻撃タイミング	過去の攻撃時期や履歴，今後，攻撃が発生する可能性がある時期等	攻撃観測網, OSINT
攻撃インフラ	攻撃者が使用するサーバ情報 (アドレス，ドメイン等)，第三者サービス	攻撃観測網, OSINT
動機	経済的利益, 政治的・社会的目的，復讐など攻撃の目的や理由等	OSINT, HUMINT
プロフィール	SNS ID やフォーラムの ID など	OSINT, HUMINT
ビジネスモデル	漏洩情報販売, ボットネットレンタル等，収益化に係る情報	OSINT, HUMINT
攻撃者組織	国家背景組織，ハクティビスト，犯罪組織等，攻撃者組織の情報	OSINT, HUMINT
防御側インテリジェンス		
攻撃対象	(潜在的な) 攻撃対象の個人，組織，システム，アドレス・アカウント等	攻撃観測網, OSINT, HUMINT
攻撃原因	脆弱性，設定ミス，サプライチェーンリスク，内部不正など攻撃の要因	攻撃観測網, OSINT
攻撃被害	活動停止，身代金支払い，漏洩情報流通, 評判低下等の被害	OSINT
対応	攻撃者との交渉，被害の公開状況，脆弱性対策など，攻撃発生後の対応	OSINT

図 3　太陽光発電監視装置の攻撃手法を共有する Telegram 上の投稿

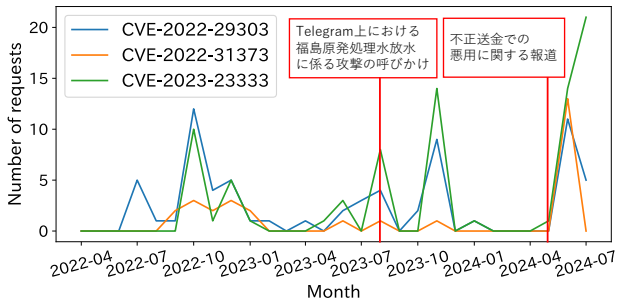

図 4　太陽光発電監視装置の脆弱性を狙う攻撃観測件数の推移

なお，攻撃手法を共有する投稿においては攻撃対象となる機器を広域スキャンシステムで探索するための検索クエリも示されているが，その際広域スキャンシステムとして，世界的に有名な Shodan や Censys ではなく攻撃者グループが活動する国の企業が提供するサービスを利用していた．当該サービスに掲載されている当該機器の件数を調査したところ Shodan や Censys における掲載機器数の約 10 倍もの件数が掲載されていたことから，当該サービスが日本国内の機器探索において優位性を持つ可能性があるが，詳しい検証は今後実施する．

次に，上述の OSINT 調査から得られた攻撃者の活動と，攻撃観測網によって得られた実際の攻撃動向との関連性について示す．図 4 は，我々が運用しているハニーポットである X-POT[7] において観測された，CVE-2022-29303, CVE-2022-31373, CVE-2023-23333 を狙う攻撃リクエスト数の推移を示している．これらの脆弱性を狙った攻撃はそれぞれ 2022 年 7 月 12 日，2022 年 9 月 5 日，2022 年 10 月 10 日に初めて観測されている．特に CVE-2022-29303, CVE-2023-23333 を狙った攻撃は Telegram 上で書き込みがあった 2023 年 8 月頃に増加しており，観測された攻撃リクエスト内の特徴が攻撃者グループ「軍火庫」が Telegram において共有した攻撃の手法と類似していることが確認できた．さらに当該機器の不正送金への悪用に関する報道があった 2024 年 5 月以降にも攻撃観測件数が増加しており，これについても関連が疑われる．

事例まとめ: 本事例では，報道を起点に国内の機器を狙う攻撃に関する調査を行い，当該機器の脆弱性が報道の少なくとも約 2 年前から攻撃対象となっており，2023 年 8 月の福島原発の処理水海洋放出に関連して攻撃が増加した後も断続的に続いていたことが確認された．報道にあった不正送金とそれ以前の攻撃とが同一の攻撃グループによって行われたという明確な関連性は確認できなかったが，攻撃が断続的に続く状況が事前に認識できていれば，不正送金等への悪用を未然に防げた可能性がある．また，広域スキャンシステムと連携することで当該脆弱性を有する機器の公開状況や対策状況などを調査し，更なる対策に繋げることができる可能性がある．このように，ハニーポットによる観測だけでは把握が難しい攻撃主体や背景，その目的の一部を OSINT と関連づけることで攻撃の全体像を推測することができ，対策につながる知見が得られた．

4.2　事例 2：IoT ボットネットと攻撃サービスの紐づけ

ハニーポットで収集した IoT マルウェア検体を動的解析することで，攻撃者が管理する C&C サーバやマルウェアダウンロードサーバを特定できる．我々は文献 [4] において 2016 年から 2021 年の間に収集した IoT マルウェア 64,260

検体の動的解析により 4,736 個の C&C サーバ IP アドレス, 35,494 個のマルウェアダウンロードサーバを特定し，この分布や生存期間を分析している．また，疑似ボットスクリプトによりこれらの C&C サーバにアクセスし，攻撃命令を継続的に収集することで，当該ボットネットの攻撃頻度，攻撃対象，攻撃通信の特徴等を調査している [13]．本節では，これらに加えて OSINT との連携により，ボットネットの活動の背景にあるサイバー攻撃ビジネスを調査した先行事例を説明する．

攻撃者はボットネットを管理するために C&C サーバやマルウェアダウンロードサーバを運用しているが，同一サーバ上で自身のサイバー攻撃ビジネスに係る Web コンテンツや SNS アカウント情報を掲載することがある．図 5 の Web コンテンツは，いずれもある特定の IoT ボットネットの C&C サーバ上で発見されたものであり，Booter や Stresser と呼ばれる DoS 攻撃サービスにつながるドメインや Telegram アカウント情報が掲載されている．実際に攻撃サービスのサイトにアクセスすると図 6 のように 600 から 5000 ルーブルの価格帯で攻撃サービスが販売されていた．攻撃手法の説明もあり，レイヤー 3/4/7 の各サービス妨害攻撃が実行可能であると記載されていた．このサイトはロシア語を基本言語としているが，日本語を含め 8 言語をサポートしていた．さらにこのサービスと関係する 3 つの Telegram のチャネルが記載されており，そのうちの 1 つでは過去に攻撃を行った対象の IP アドレスと攻撃の種別が掲載されていた．別のチャネルでは，当該サービスのカスタマーレビューが掲載されており，サイバー攻撃がビジネス化されていることを象徴している (図 8)．また，実行中の攻撃をリアルタイムでグラフ表示している例もあった (図 7)．DoS 攻撃対策で有名なものを含む 10 種類以上のクラウドサービスを対象としており，攻撃の効果を示すデモンストレーションの狙いがあると予想される．

事例まとめ: 本事例では, ハニーポットで収集した IoT ボットネットの活動背景である DDoS 攻撃サービスを調査した．単にボット検体を収集し攻撃インフラを観測するだけではわからない攻撃ビジネスの背景を知ることで攻撃者の動機，収益化の構造，攻撃者のプロフィールや関連する組織に関する情報が得られた．また，ビジネス促進のためか過去の攻撃履歴や現在実施中の攻撃に関する情報を掲載している事例もあることから，これらの情報を継続的に収集し，他の情報源との関連づけを行うことで，攻撃グループの活動実態や，テイクダウン・無害化といった対策に資するインテリジェンスが獲得できると期待される．

4.3 事例 3: 漏洩データ販売者との対話の試行

2024 年 5 月，4,000 人以上が参加する漏洩データ販売用の Telegram チャネルにおいて日本の銀行の漏洩情報ファイルの販売広告が掲載された．広告と共に公開された情報

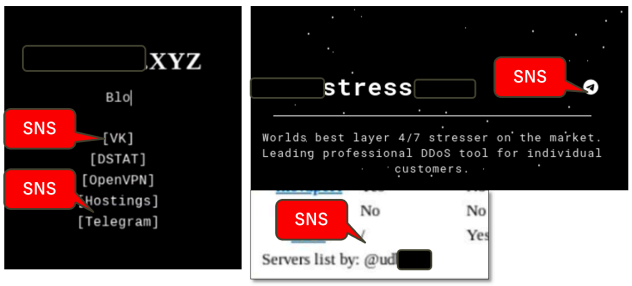

図 5 Web コンテンツに攻撃者の SNS 情報が含まれている例

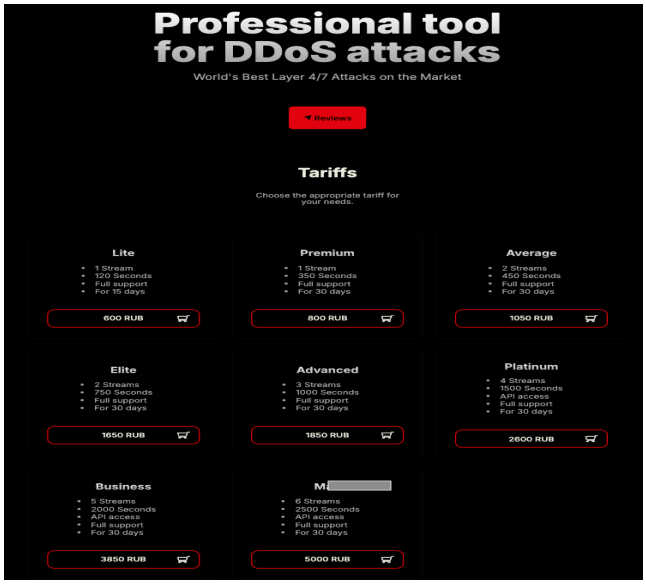

図 6 DoS 攻撃サービスサイト

図 7 実行中の DoS 攻撃のリアルタイムグラフ

には漏洩ファイルに含まれるレコード数やレコードの属性情報として顧客の住所や連絡先等が含まれることが記載されていた．当該チャンネルの個別連絡用アカウントに対して，2024 年 6 月に調査用アカウントからコンタクトし販売者と Telegram 上で試験的に会話を行った．販売者とのやりとりでは，リークデータの総数は 90 万件以上あり，データには個人を証明する情報 (パスポートなど) が 1 万 6 千件，金融機関へのローン申請者の情報が 2 万件，ローン申請フォームが 1 万 6 千件含まれること，約 2 万 5 千件のサンプルデータを 150 ドルで販売すること, 支払いは USTD で受けることなどの説明があった．また，この漏洩データ

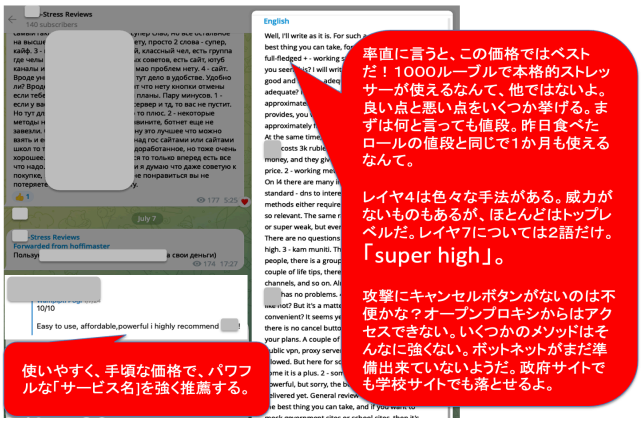

図 8 DoS 攻撃のレビュー

の他に 3 つの日本の大手銀行からの漏洩情報も販売可能であり，そのうち一つの銀行からの情報漏洩は 3 日前であり，もう 1 つの銀行からの情報漏洩は 3 週間前であることの説明があった. さらに，約 1,200 万件の日本人パスポート情報も販売するとの説明があった．2024 年 8 月時点では，上記の漏えいデータ販売の広告は削除されており，既に購入された可能性がある．

事例まとめ: 漏洩データの販売者との会話から多くの情報が得られた一方で，その信ぴょう性を評価する手段がない点は課題である．今後，他の収集情報との突合により信ぴょう性を評価する方法を検討する．また個人情報や機密情報を含む可能性がある漏洩データを実際にやりとりすることがないように細心の注意が必要であることから，本格的な調査の実施の前に研究倫理的および法的な観点で適切な実施方法を検討する必要がある．

5. おわりに

ハニーポット等の攻撃観測技術や広域スキャン等のアタックサーフェイスマネジメント技術に加えて, オープンソースインテリジェンス (OSINT), ヒューマンインテリジェンス (HUMINT) の収集能力を強化し, これらの融合により, サイバー攻撃のエコシステムや背景を把握し, 対策の効果を向上させる, 新しいサイバーセキュリティ情報収集・分析・対策機構 INSITE を提案した．本研究開発構想の全ての項目において法的倫理的な適切性を特に重視し，法令の遵守と研究による恩恵の最大化，被害の最小化を図り，細心の注意と共に計画，実施する．

謝辞 この成果の一部は, 国立研究開発法人新エネルギー・産業技術総合開発機構（ＮＥＤＯ）の委託業務（JPNP22007）の結果得られたものです.

参考文献

[1] 吉岡克成, インミンパパ, 鈴木将吾, 渡邉直紀, 中山颯, 志村俊也, 徐浩源, 四方順司, 松本勉, 中尾康二, 針生剛男, 岩. 八木毅, 秋山満昭, 寺田真敏, 島成佳, 渡部正文, 角丸貴洋, 川北将, 山田正弘, and 井上大介, “能動的観測と受動的観測の融合によるサイバーセキュリティ情報の収集と分析,” in コンピュータセキュリティシンポジウム 2015 論文集, vol. 2015, no. 3, oct 2015, pp. 915–922.

[2] YinMinnPaPa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “Iotpot: Analysing the rise of iot compromises,” in 9th USENIX Workshop on Offensive Technologies (WOOT ’15), 2015.

[3] T. Sasaki, A. Fujita, C. Ganan, M. van Eeten, K. Yoshioka, and T. Matsumoto, “Exposed infrastructures: Discovery, attacks and remediation of insecure ics remote management devices,” in 2022 IEEE Symposium on Security and Privacy (S&P ’22), 2022, pp. 1308–1325.

[4] R. Tanabe, T. Tamai, A. Fujita, R. Isawa, K. Yoshioka, T. Matsumoto, C. Gañán, and M. Van Eeten, “Disposable botnets: examining the anatomy of iot botnet infrastructure,” in Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES ‘20), 2020, pp. 1–10.

[5] C. Orcun, G. Carlos, A. Lisette, K. Takahiro, I. Daisuke, T. Kazuki, T. Ying, Y. Katsunari, and M. van Eeten, “Cleaning up the internet of evil things: Real-world evidence on isp and consumer efforts to remove mirai,” The Network and Distributed System Security Symposium (NDSS ’19), 2019.

[6] 稲澤朋也, 佐々木貴之, 吉岡克成, and 松本勉, “am i infected? iot セキュリティ診断 web サービスを用いたエンドユーザへの注意喚起の実証実験,” in コンピュータセキュリティシンポジウム 2022 論文集, oct 2022, pp. 176–183.

[7] S. Kato, R. Tanabe, K. Yoshioka, and T. Matsumoto, “Adaptive observation of emerging cyber attacks targeting various iot devices.” in IFIP/IEEE International Symposium on Integrated Network Management (IM ’21), 2021, pp. 143–151.

[8] L. Krämer, J. Krupp, D. Makita, T. Nishizoe, T. Koide, K. Yoshioka, and C. Rossow, “Amppot: Monitoring and defending against amplification ddos attacks,” in Research in Attacks, Intrusions, and Defenses (RAID ’15), 2015, pp. 615–636.

[9] T. Ueda, T. Sasaki, K. Yoshioka, and T. Matsumoto, “An internet-wide view of connected cars: Discovery of exposed automotive devices.” in Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES ’22), 2022.

[10] 九鬼琉, 佐々木貴之, インミンパパ, and 吉岡克成, “ハニーポットで観測される新規エクスプロイトの分類手法の提案,” in コンピュータセキュリティシンポジウム 2024, 2024.

[11] “Fxc 製無線 lan ルータにおける os コマンドインジェクションの脆弱性,” CVE-2023-49897, 2023.

[12] 遠藤祐輝, 田辺瑠偉, 吉岡克成, and 松本勉, “ハニーポットとマルウェア動的解析と c&c サーバの監視の融合による iot ボットネット活動分析の高度化,” in ICSS 研究会, no. 12, 2024.

[13] 鮫嶋海地, 遠藤祐輝, 田辺瑠偉, 吉岡克成, 中尾康二, and 松本勉, “Iot ボットの c&c 通信を模したスクリプトによる攻撃インフラの観測,” in ICSS 研究会, vol. 122, 2022.

[14] 横浜国立大学, “Iotpot: Honeypot for revealing iot cyber threats,” https://sec.ynu.codes/iot.

[15] ——, “Amppot: Honeypot for monitoring amplification ddos attacks,” https://sec.ynu.codes/dos.

[16] ICT-ISAC, “脆弱な状態にある重要 iot 機器の令和 5 年度調査及び注意喚起について,” https://www.ict-isac.jp/

news/news20231115.html.
[17] 横浜国立大学, “am i infected? マルウェア感染・脆弱性診断サービス,” https://amii.ynu.codes/.
[18] NICT, “標的型攻撃誘引基盤 stardust,” https://csl.nict.go.jp/team-1.html#nct-team-01-03.
[19] 安井浩基, 田辺瑠偉, 吉岡克成, and 松本勉, “モノの中の戦い：iot 機器への攻撃の長期観測による マルウェアの生存競争の調査,” in コンピュータセキュリティシンポジウム 2023 論文集, oct 2023, pp. 1325–1332.
[20] 池田駿, 安井浩基, 田辺瑠偉, 吉岡克成, and 松本勉, “Iot マルウェアが他の侵入者の活動を妨害する機能の調査,” in ICSS 研究会, vol. 2024, no. 11, 2024, pp. 1–6.
[21] 川口大翔, インミンパパ, 吉岡克成, and 松本勉, “Discord 上のサイバー犯罪に対する chatgpt を利用した情報収集システム,” in 電子情報通信学会 暗号と情報セキュリティシンポジウム, 2024.
[22] 関根悠司, インミンパパ, 吉岡克成, and 松本勉, “Lockbit3.0 ウェブサイトのデータ変遷に基づく攻撃者と被害者の行動の分析,” in ICSS 研究会, 2024.
[23] A. S. B. A. Razak, YinMinnPaPa, K. Yoshioka, and T. Matsumoto, “Unveiling the shadows: Analyzing cryptocurrency address management and fund movement of darknet markets,” in ICSS 研究会, 2024.
[24] T. Sasaki, J. Wang, K. Omote, K. Yoshioka, and T. Matsumoto, “Etherwatch: A framework for detecting suspicious ethereum accounts and their activities,” in IPSJ Journal, 2024.
[25] 鈴木惟央利, インミンパパ, and 吉岡克成, “Ethereum 上の不正な defi トークン対策研究促進のためのデータセット構築,” in ICSS 研究会, 2024.
[26] 木原百々香, 佐々木貴之, and 吉岡克成, “ルータのファームウェアに含まれる oss 脆弱性に関する sca ツールを用いた調査,” in ICSS 研究会, 2024.
[27] T. Sasaki, K. Yoshioka, and T. Matsumoto, “Who are you? osint-based profiling of infrastructure honeypot visitors,” in 11th International Symposium on Digital Forensics and Security (ISDFS ’23), 2023.
[28] YinMinnPaPa, S. Tanizaki, T. Kou, M. van Eeten, K. Yoshioka, and T. Matsumoto, “An attacker’s dream? exploring the capabilities of chatgpt for developing malware,” in Proc. 16th Workshop on Cybersecurity Experimentation and Test (CSET ’23), 2023.
[29] 黄哲偉, インミンパパ, and 吉岡克成, “Chatgpt を用いたソースコードの書き換えがアンチウイルスの検知に与える影響,” in ICSS 研究会, 2024.
[30] 松澤輝, 久保颯汰, インミンパパ, 田辺瑠偉, and 吉岡克成, “Llm を用いて作成した解析回避検体がサンドボックス解析に与える影響の調査,” in コンピュータセキュリティシンポジウム 2024, 2024.
[31] 合屋琴江, 佐々木貴之, and 吉岡克成, “Llm を用いた webui 解析による iot 機器の機種と設置施設の推定,” in コンピュータセキュリティシンポジウム 2024, 2024.
[32] 川口大翔, インミンパパ, and 吉岡克成, “Llm を利用した discord 上のサイバー犯罪関連の隠語の調査,” in コンピュータセキュリティシンポジウム 2024, 2024.
[33] 本多凌大, 櫛引淳之介, 佐々木貴之, and 吉岡克成, “Iot 機器付属のスマートフォンアプリを通じたメーカによるユーザへのセキュリティアドバイスの調査,” in コンピュータセキュリティシンポジウム 2024, 2024.
[34] 竹内謙仁, 九鬼琉, 佐々木貴之, and 吉岡克成, “Llm を用いたユーザマニュアル解析による機器に即した iot セキュリティ対策手順の提示,” in コンピュータセキュリティシンポジウム 2024, 2024.
[35] 上園大智, 櫛引淳之介, 佐々木貴之, and 吉岡克成, “Darkwrt: Iot 機器における不正機能のデータセット作成に向けた事例調査と分類,” in コンピュータセキュリティシンポジウム 2024, 2024.
[36] “太陽光発電にサイバー攻撃 機器 800 台を乗っ取り身元隠し不正送金に悪用,” 産経新聞, 5 2024.