部局における情報セキュリティ向上の取組とその実践的検討

太田 憲治 [1)], 安倍 渉 [1)], 伊藤 勝哲 [1)], 大場 正志 [1)], 河内 英智 [1)],
小森 和樹 [1)], 千葉 淳 [1)],前田 桂史 [1)], 桑野 龍 [1)]

1) 東北大学 事業支援機構 総合技術部

Initiatives for Enhancing Information Security in University Departments and Their Practical Examination

Kenji Ota [1)], Wataru Abe [1)], Katusaki Ito [1)] Masashi Ohba [1)], Hidetomo Kawauchi [1)],
Kazuki Komori [1)], Atsushi Chiba [1)], Keiji Maeda [1)], Ryu Kuwano [1)]

1) Division of Engineering and Technical Staff, Tohoku University.

概要

大学部局ネットワークにおける情報セキュリティ強化の取組として,ライブネットとダークネットの分析を組み合わせた脅威インテリジェンス活用を実施した.2025 年 1 月から 4 月の分析により,以下の知見を得た.第一に,Mirai 系通信を含む恒常的な IoT 機器探索行為が継続的に観測された.第二に,ダークネットと実環境の双方に出現する共通攻撃元 IP が定量的に把握され,運用上注視すべきリスク源の存在が明らかとなった.第三に,SSL-VPN を標的とした短期集中型の認証攻撃が確認され,事前の探索行為と連動する攻撃の実態が明らかとなった.さらに,本取組は多様な専門性を有する職員が部局横断的に連携し,定例会合において議論を行うとともに,実際の環境やツールを用いた観測データの解析・分析を通じて技術的知見を共有する活動を継続的に実施している.かかる体制を構築することにより,技術の習得および知識・経験の継承が促進され,ひいては部局間の技術力向上に寄与している.

1 はじめに

近年,大学を取り巻くサイバー空間の脅威は急速に多様化・高度化しており,研究・教育活動を支える情報インフラの保護は喫緊の課題となっている.各部局の情報ネットワーク技術担当者は,限られた人員と予算の中で構築・運用・保守を担い,東北大学 CSIRT と連携しながら情報資産の防御に努めている.しかし,システム運用の負荷や人材の確保・育成には依然として大きな困難が存在する.

このような状況を踏まえ,本研究では部局情報ネットワークにおける新たな情報セキュリティの取り組みとして,ダークネット観測情報を活用した脅威インテリジェンス分析と,その技術能力向上を目的とした活動について報告する.特に,ライブネットおよびダークネットにおけるトラフィックを継続的に分析することで,通常の運用では把握が難しい「見えない脅威」の可視化を実現し,その成果を部局間のセキュリティ技術向上へと還元している.

本取り組みの特徴は,多様な専門性を有する職員が連携し,部局横断的な体制を構築している点にある.構成メンバーは各自の専門知識を活かしながら,日常業務内での自己研鑽や定例会合において議論を行うとともに,実際の環境やツールを用いた観測データの解析・分析を通じて技術的知見を共有する活動を通じて高度な技術の習得と継承を進めており,主配置部局にとどまらない全学的な技術支援にも積極的に関与している.

こうした活動は,部局ネットワーク管理における理想的なサイバーセキュリティ体制の実現に寄与すると期待される.本発表では,ライブネットとダークネットの分析を組み合わせた脅威インテリジェンス活用から得られた知見と課題に加え,今後の展望について包括的に整理・考察する.

2 背景・経緯

近年,国際社会におけるサイバー空間の脅威は急速に拡大・多様化している.国家間の緊張や地政学的リスクを背景に,サイバー攻撃は重要インフラや教育研究機関を標的とする事例も増加している.また,ランサムウェアやボットネットによる大規模攻撃,IoT 機器を悪用した無差別スキャンなど,攻撃の手法も高度化しつつあり,研究・教育活動を支える部局の情報インフラにとって深刻な脅

威となっている.

こうした社会的・国際的背景を踏まえると,部局のセキュリティ対策は従来型の境界防御やログ監視に依存するだけでは限界がある.攻撃の兆候を早期に捉え,未知の脅威を可視化するためには,新たなアプローチの導入が不可欠である.

日常的に運用されているライブネットの分析および解析では,正規の通信と攻撃を目的とした不審な通信が混在しており,どのパケットに注目すべきかを判断するのは容易ではない.膨大なトラフィックの中から攻撃の兆候を抽出するには高度な解析技術と労力を要する.

一方で,ダークネットとは,実際には利用されていない IP アドレス空間のことであり,通常であれば通信が届くことはない.しかし現実には,マルウェア感染機器や攻撃者によるスキャン活動の結果として,この空間にも多数のパケットが送られてくる.したがって,ダークネットを観測することで「誰にも届くはずのない通信＝攻撃や不正活動の兆候」を効率的に収集することができる.この特徴により,「ダークネット観測データ」の活用が,サイバー攻撃の大局的な動向を把握するための手段として以前より注目されている.

ライブネットへ届くパケットとダークネットへ届くパケットとの両方を観測することで,それぞれの特徴を補完的に活用できる.すなわち,ライブネットからは実際の業務環境における攻撃の影響や挙動を把握し,ダークネットからは大規模かつ無差別型の攻撃の全体像を効率的に抽出することが可能である.両者を組み合わせることで,単独では見えにくい攻撃の兆候を明らかにすることで,部局の情報セキュリティの向上に資するものと考えられる.

3　課題

ライブネットとダークネットの観測データを併用することで,従来は把握が難しかった攻撃の兆候を捉える可能性が広がる.しかし,これらの取り組みを実効的なセキュリティ強化へと結びつけるためには,以下のような課題が存在する.

(1) 技術的課題

ダークネット観測基盤を構築し,観測品質を維持したまま安定的に運用するための技術が求められる.また,観測データは膨大であるため,有用な情報を効率的に抽出する手法の確立も重要である.特に,解析技術や検知手法の改善に加えて,保存期間と検索性能を両立させるストレージおよびインデックス設計も技術的課題として挙げられる.

(2) 運用・人材的課題

部局のネットワーク担当者は限られた人員と予算の中で運用を担っており,観測基盤の維持や分析を日常業務と並行して行うことは負担が大きい.さらに,専門性を持つ人材の確保や育成が容易ではなく,技術継承の仕組みも十分に整備されていない.そのため,属人的な運用に陥るリスクや,知識・経験の断絶が課題として挙げられる.

(3) 組織的課題

部局ごとの取り組みだけでは知見が分散し,セキュリティ水準にばらつきが生じやすい.得られた知見を全学的に共有・活用することが難しい点も課題である.したがって,CSIRT との役割分担と連絡・判断フローを明確化するとともに,観測結果や知見を学内全体で共有できる協力体制や仕組みを整備することが求められる.

4　課題解決の取り組み

これらの課題を解決するために,技術的側面と人材的側面の両面から取組を進めてきた.以下に,その具体的な施策を示す.

技術的な取組としては,情報通信研究機構との共同研究により,同機構が開発したサイバー攻撃観測・分析システム NICTER[1] および対サイバー攻撃アラートシステム DAEDALUS[2] の提供を受け,過大な負担を伴うことなくダークネット観測に必要な基盤を導入した.さらに,この基盤と連携させてライブネットとダークネットを統合的に扱う解析・分析環境を構築し,観測 IP アドレス宛に到達するパケットを継続的に収集・分析することで,安定した観測環境を実現している.

加えて,ライブネットワークとダークネット双方のトラフィックを比較・分析することにより,実際の業務環境における攻撃の挙動と,無差別に行われる大規模攻撃の全体像を相互に補完的に把握できる.両者を組み合わせることで,単独の観測では捉えにくい「見えない脅威」を浮かび上がらせ,より精緻な脅威分析へとつなげている.

人材的課題に対応するため,毎月の定例会合を開催し,実際の環境やツールを用いた観測データの解析・分析を通じて多角的な視点からの議論を行い,高度な技術の習得と技術的知見の共有を継続的に実施している.これにより,技術の習得と知識・経験の継承が進み,最終的には部局間の技術

力向上にも寄与している.このように,多様な専門性を有する職員が協働することにより,属人的な対応に依存しない持続可能なセキュリティ体制を構築した.

5　得られた知見

2025 年 1 月から 4 月にかけて実施したダークネットとライブネットの観測データの比較分析により,攻撃活動の様相についていくつかの特徴的な傾向が明らかになった.

まず,ダークネット観測の結果からは,攻撃活動の大局観が得られた.観測パケット全体のうち平均して全体の約 50%は調査系パケットで,インターネット上の広範なスキャン活動が恒常的に行われている実態が確認された.非調査系パケットに限ると平均 9.46%が Mirai 系通信であった.(図 1)

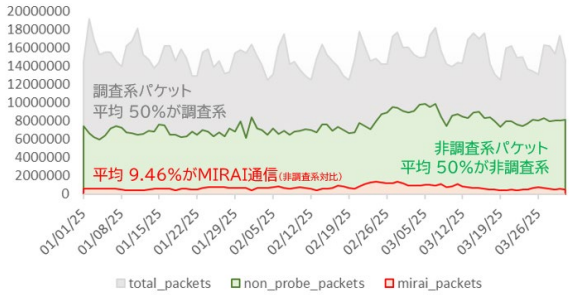


図 1) 観測パケットにおける調査系・非調査系・Mirai 通信の推移（2025 年 1 月～3 月）

観測結果をさらに精査すると,Telnet（23 番）や HTTP（80 番）,SSH（22 番）といった汎用的なサービスポートに加えて,9999 番,8888 番,7000 番,8000 番,9000 番といった高位の非標準ポートに対するアクセスが継続的に確認された.これらのポートは,家庭用ルータや DVR（防犯カメラ録画装置）,IP カメラ,ストリーミング関連機器などの IoT 機器が管理や通信に利用する例が多いとされており,不正操作を介したボットネット形成に向けた探索行為が継続している可能性が示唆される.

また、時間帯別に通信量を解析した結果,変動は小さく,通信量・傾向のいずれにおいても顕著な日内周期性は確認されなかった.このことから,攻撃活動は時間帯に依存せず常時発生していることが明らかとなった.(図 2)

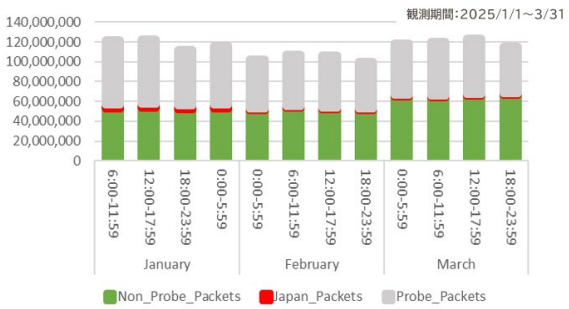


図 2) 時間帯別にみた観測パケットの種別別推移（2025 年 1 月～3 月）

次に,ライブネットとの比較から,ダークネットと実環境の双方に共通して出現する攻撃元 IP の存在が定量的に把握された.ダークネット側ユニーク IP に占める共通 IP の割合は平均 23.66%,ライブネット側ユニーク IP に占める共通 IP の割合は平均 38.45%であり,1 日あたりの共通ユニーク IP 数は平均 23,347 件に達した.すなわち,両環境に重複して現れる攻撃元が相当数存在する.

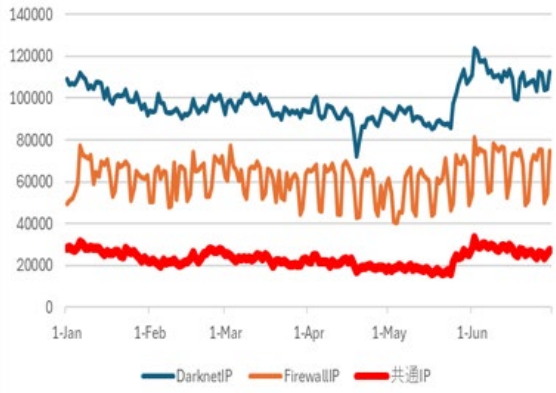


図 3) Darknet 観測 IP 数,ライブネット観測 IP 数,および共通 IP の時系列比較（2025 年 1 月～6 月）

加えて,ライブネット側のユニーク IP のうちファイアウォール装置で「許可トラフィック」に含まれ,かつダークネットでも観測された送信元 IP（以下,許可共通 IP）が占める割合は平均 0.66%であり,実運用上の監視・対策において注視すべき水準と考えられる.

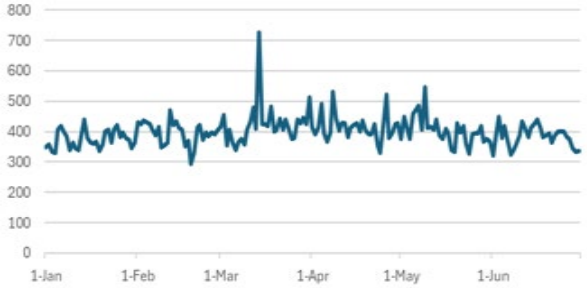
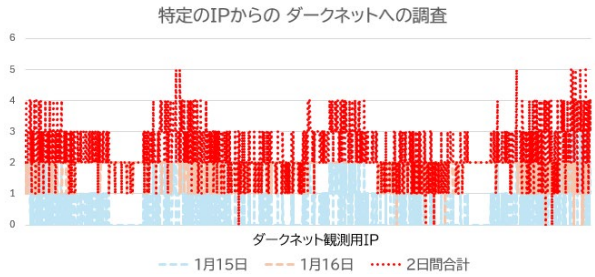


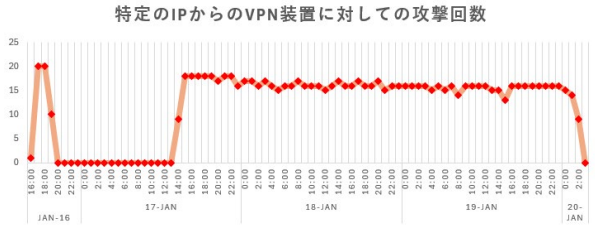
図 4) 許可通信における IP 数の時系列推移（2025 年 1 月～6 月）

さらに,近年脆弱性が頻繁に指摘されている SSL-VPN に着目した分析からも興味深い所見が得られた.SSL-VPN 装置の総ログ 1,721,287 件のうち,ダークネット由来と判定された通信は 42 か国・1400IP に分布しており,28,326 件（1.65%）であった.割合自体は限定的であるものの,詳細な精査の結果,Mirai 関連フラグに一致する通信が 2IP 確認され,いずれもユーザ名を投入したログイン試行を伴っていた.

このうち日本発の送信元 IP は 1 件のみであったが、当該 IP についてはダークネット側での調査行為の後、一定時間を経て実環境側への攻撃試行が観測され、調査から攻撃へと至る手順を示唆する時系列が確認された。調査は 2025 年 1 月 15 日～16 日の二日間に集中して行われ、ダークネット観測 IP のほぼ全てに対して調査パケットが送信されていた（図 5）。攻撃の発生は 2025 年 1 月 16 日～20 日に集中しており、観測後は急速に沈静化した（図 6）。さらに、認証試行に用いられたユーザ名は極めて多様であり、少なくとも 435 種類の ID パターンが確認された。



5) 特定 IP によるダークネット宛通信の比較
（1 月 15 日-16 日および 2 日間合計）



6) 特定 IP から VPN 装置への攻撃回数の時系列推移
（2025 年 1 月 16 日～20 日）

以上の結果は,（i）ダークネット観測により広域かつ常時的なスキャン・ボット探索の実態を把握できること,（ii）ダークネットとライブネットの照合によって実環境に影響し得る攻撃元を特定・優先化できること,（iii）SSL-VPN のような周辺境界サービスに対する短期集中型の認証攻撃が存在し,事前の探索行為と連動している可能性があること,を示唆している.これらの知見は,検知ルールの最適化,アラートの優先度付け,境界サービスの強化（多要素認証やレート制御,地理的ブロック等）といった実務的対策の設計に資する基礎情報となる.

6 まとめ・今後の展望

ライブネットとダークネットの分析データを組み合わせることで,従来の境界防御やログ監視では把握が困難であった攻撃傾向や脅威の兆候を明らかにした.特に,商用ルータや各種サービス用ポートを標的とした継続的な攻撃,IoT 機器に関連する高位ポートへのアクセス,さらには SSL-VPN に対する短期集中型の認証攻撃など,大学部局の情報インフラに直接的な影響を及ぼし得る具体的な攻撃の実態が確認された.これらの結果は,ダークネット観測が潜在的な脅威の可視化に有効であることを裏付けるものである.

一方で,膨大な観測データを効率的かつ精緻に分析し,実効的なセキュリティ強化へと結びつけるためには,さらなる技術的・組織的工夫が必要である.今後は,機械学習や異常検知技術を応用し,攻撃の兆候を自動的に抽出・予測することで,早期警戒システムとして機能させることが期待される.また,分析結果を侵入防御やアクセス制御へフィードバックし,事後対応から事前対応への転換を進めることで,実環境におけるセキュリティ対策を強化できる.

さらに,こうした取り組みを持続的に発展させるためには,部局横断的な協働体制の維持・強化や人材育成の仕組みづくりが不可欠である.多様な専門性を有する職員が連携し,知見を全学的に共有することにより,持続可能な情報セキュリティ基盤を構築できる.

以上の知見と展望は,部局における情報セキュリティ体制の高度化に資するとともに,教育研究機関における今後のセキュリティ対策の指針となることが期待される.

謝辞

本研究のリアルタイム型ダークネット観測基盤システムの導入・運用にあたり、情報通信研究機構の牛込龍太郎研究技術員には技術的なご支援をいただきました。また、ダークネット観測における分析手法については、同機構の遠藤由

紀子主任研究技術員にご協力をいただきました。さらに、東北大学 CSIRT の折内新司特任教授には、本施策の導入および運営に関してご支援をいただきました。ここに記して、関係各位に深く感謝申し上げます。

参考文献

[1] NICTERWEB. https://www.nicter.jp.
[2] DAEDALUS. https://www.nict.go.jp/out-promotion/other/case-studies/itenweb/DAEDALUS.html
[3] NICTER Blog. https://blog.nicter.jp/.
[4] NICTER 観測レポート. https://www.nicter.jp/report