2-6　国際的な大規模イベントのセキュリティオペレーションに貢献するサイバー攻撃観測技術

2-6　Cyberattack Monitoring Technologies Supporting Security Operations at Large-Scale International Events

笠間 貴弘　久保 正樹
KASAMA Takahiro and KUBO Masaki

国際的なスポーツ大会や国際博覧会のように、数百万人規模の来場者を迎え、世界中から注目を集めるイベントは、しばしばサイバー攻撃の格好の標的となる。攻撃者は、イベントの公式 Web サイトやチケット販売システム、さらには通信のインフラ等を狙い混乱を引き起こすことで社会的な影響を最大化しようとする。このような脅威に備えるためには、個々のシステムに対する適切なセキュリティ対策の実施に加え、広い視点でのサイバー攻撃の動向把握、攻撃や被害に関する情報を関係者間で共有する仕組みの整備などが不可欠である。

NICT サイバーセキュリティ研究室が長年にわたって研究・運用してきた各種のサイバー攻撃観測技術は、インターネット上で日々発生している攻撃活動の実態を捉えることを可能にしてきた。そこで得られたデータや知見は、国際的な大規模イベントのセキュリティ運用においても極めて有用である。本稿では、NICT が開発・運用するサイバー攻撃観測技術と、それらが大阪・関西万博 2025 にどのように貢献しているかについて述べる。

International events such as global sports tournaments and world expos, attracting millions of visitors and worldwide attention, are frequent targets of cyberattacks. Adversaries often aim at official websites, ticketing systems, and critical infrastructure to cause disruption and maximize social impact. Appropriate security measures must be implemented to counter such threats, and comprehensive monitoring of cyberattack trends and practical frameworks for threat and incident information sharing are essential. The Cybersecurity Laboratory of the National Institute of Information and Communications Technology (NICT) has been developing and operating cyberattack monitoring systems that capture various types of malicious activities on the internet. The data and insights obtained through these efforts are highly valuable for security operations at large-scale international events. This paper introduces NICT's cyberattack monitoring systems and their contribution to Expo 2025 Osaka, Kansai, Japan.

1　まえがき

オリンピックや万博のような国家的イベントは、その国際的な注目度の高さからサイバー攻撃の標的となる傾向が強い。たとえば、2021 年に開催された東京オリンピック・パラリンピックでは、大会期間中に通信を遮断したセキュリティイベントが累計で約 4 億 5 千万回にも及んだことが報告されている [1]。これは攻撃の規模がきわめて大きく、組織的かつ持続的に行われていた可能性を示している。このような大規模イベントのセキュリティを確保するためには、多面的な取組が必要である。具体的には、事前のリスクアセスメント（リスクを評価する作業）、事案発生時の迅速かつ的確な対処のための体制整備、インシデント対応訓練、予防・検知に関する情報の収集と発信、さらに関係者間での情報共有を促進するためのプラットフォームの整備・運用などである。

NICT サイバーセキュリティ研究室では、長年にわたりインターネット上で発生する多種多様なサイバー攻撃を観測･分析し、対策技術を研究開発してきた。そして得られたデータや分析結果は、国際的イベントのセキュリティオペレーションに実際に活用されている。東京オリンピック・パラリンピックでは情報セキュリティ関係機関としてインシデント対応に貢献し、現在

は大阪･関西万博 2025 に向けても同様の協力を行っている。

2 無差別型攻撃観測システム NICTER

NICTER（ニクター）は、未使用のグローバル IP アドレス宛に届く通信を観測する「ダークネット観測」という技術を用いたサイバー攻撃観測システムである。この仕組みによって、インターネット上で無差別に行われるサイバー攻撃を効率的に観測できる。サイバーセキュリティ研究室では 2005 年より継続して NICTER の研究開発を進めており、これまでに Conficker [2] や WannaCry [3] といった Windows を狙うマルウェア、2016 年の Mirai [4]、その後の IoT 機器に感染する多様なマルウェアまで、数々の脅威動向を捉えてきた [5]。観測された通信は可視化エンジンによってリアルタイムに表示され、解析者が直感的に状況を理解できるようになっている（図 1）。さらに AI 技術を活用した分析や、他の脅威情報との突合により、今この瞬間のサイバー攻撃の実態を明らかにすることが可能である。

NICTER で得られたデータや知見は NICTERWEB [6] や NICTER 観測レポートとして一般公開されているほか、定点観測友の会（SIGMON）[7] や ICT-ISAC [8] の DoS 攻撃即応 -WG の活動を通じた情報共有にも活用されている。また、サイバーセキュリティ協議会への第二類構成員としての参画や東京オリンピック・パラリンピックへの情報セキュリティ関係機関としての貢献といった実績にもつながっている。

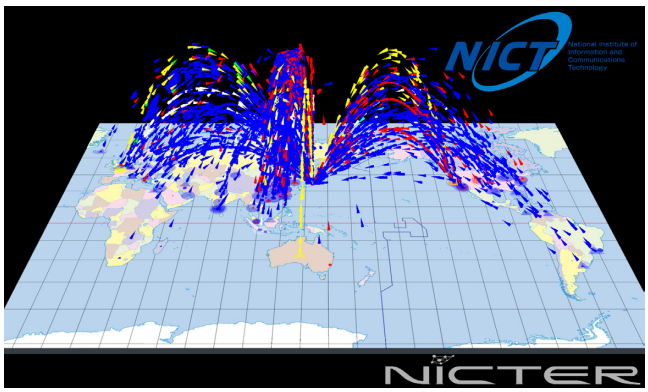

図 1　NICTER のサイバー攻撃可視化エンジン

図 2　DAEDALUS のアラート可視化エンジン

3 対サイバー攻撃アラートシステム DAEDALUS

DAEDALUS（ダイダロス）は NICTER の大規模なダークネット観測網を活用したサイバー攻撃アラートシステムである。一般的に多くの組織では、ファイアウォール（FW）や侵入検知システム（IDS）を用いた「境界防御」によって外部からの攻撃を防いでいる。これに対し、DAEDALUS は組織内部から外部に向けて発信される異常な通信をダークネットで捉える点に特徴がある。これにより、マルウェア感染端末の存在や、DoS 攻撃（サービス妨害攻撃）の発生を早期に検知し、リアルタイムでアラートを送信できる。

DAEDALUS のアラート送信方法は図 3 に示すように大きく 3 種類ある。ケース 1 とケース 2 では、組織内のマルウェア感染端末が自組織内もしくはインターネット上に感染を広げようとした際に、その通信を検知してアラートを送信する。ケース 3 では、組織が外部に公開している Web サーバ等が DoS 攻撃の一種である Syn フラッディング攻撃を受けた際に、送信元 IP アドレスが詐称された攻撃通信への応答を検知してアラートを送信する。このシステムは、大規模イベントにおいてイベントネットワーク内にマルウェア感染が発生した場合や、公式 Web サイト等が攻撃を受けた場合の早期検知に有効である。

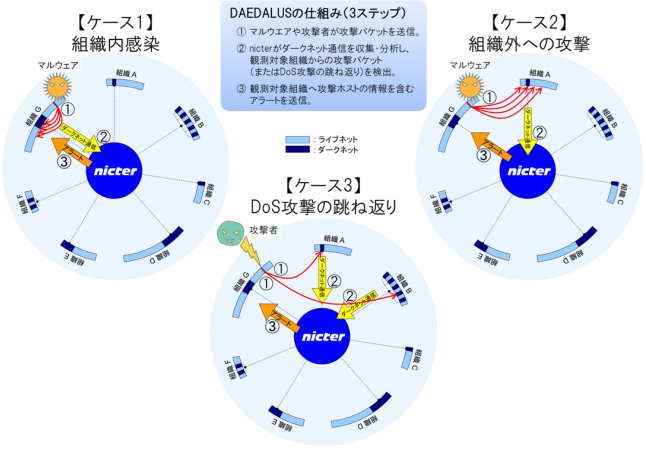

図 3　DAEDALUS のアラート送信パターン

4 DRDoS 攻撃観測システム AmpPot

DoS 攻撃の中でも大きな脅威となっているのが DRDoS 攻撃（分散反射型サービス妨害攻撃）である。DRDoS 攻撃では、DNS や NTP といった（リクエストと比較して）応答が大きくなる特定のサービスを悪用し、インターネット上に存在する当該サービスに応答する多数の機器（リフレクタ）に対して、攻撃対象の IP アドレスに詐称したリクエストを送ることで、増幅された大量の応答を攻撃対象に集中させる。この DRDoS 攻撃を観測するため、サイバーセキュリティ研究室は横浜国立大学 吉岡研究室と連携し DRDoS 攻撃観測システム AmpPot（アンプポット）を開発・運用している [9]。

AmpPot は DRDoS 攻撃に悪用されるリフレクタとして振る舞うハニーポットの一種であり、攻撃者にリフレクタとして認識されることで実際の攻撃リクエストを受信し、標的となった IP アドレスを早期に特定する。さらに、実際の攻撃時には攻撃対象への通信量の制限を行うなどの攻撃への加担を最小限に押さえる仕組みを備えている。DRDoS 攻撃は通信量が膨大になり得るため、その発生を早期に検知することは大規模なサイバー攻撃対策において重要である。

5 Beyond 5G ready ショーケースでの動態展示とセキュリティ監視への貢献

大阪・関西万博 2025 の開催にあたって、サイバーセキュリティ研究室では大きく二つの活動を実施した。第一に、総務省が主催する「Beyond 5G ready ショーケース」において、NICTER 及び DAEDALUS の観測状況をリアルタイムに可視化する動態展示を行った（図 4）。来場者は、日常生活では意識することの少ないサイバー攻撃の実態を目にすることができ、サイバーセキュリティの重要性に対する理解や関心を深める機会となった。

第二に、大阪・関西万博 2025 のセキュリティオペレーションへの貢献である。内閣官房国家サイバー統括室が中心となって運営するサイバーセキュリティ対処調整センターと協力し、上述した NICTER や DAEDALUS、AmpPot を用いた攻撃観測とアラート提供を継続的に実施している。これらの取組に関する詳細については公開できないが、日本開催の大規模イベントのサイバーセキュリティ確保に国の研究機関が開発した技術が実際に活用されていることは大きな意義を持つ。サイバーセキュリティ分野は海外技術に依存する部分が大きく、国内のサイバーセキュリティ技術自給率の低さが課題である [10]。その中で、NICT においては引き続きサイバーセキュリティ技術の研究開発を継続し、日本発のサイバーセキュリティ技術の創出と社会展開に寄与していく。

図 4　Beyond 5G ready ショーケースの展示

【参考文献】

1 内閣サイバーセキュリティセンター，“東京大会におけるサイバーセキュリティ対策と今後の取組方針，” https://www.nisc.go.jp/pdf/policy/2020/Tokyo2020houkoku.pdf, Jan. 2022.
2 “Conficker,” https://ja.wikipedia.org/wiki/Conficker
3 “WannaCry,” https://ja.wikipedia.org/wiki/WannaCry
4 “Mirai,” https://en.wikipedia.org/wiki/Mirai_(malware)
5 笠間 貴弘，森 好樹，遠藤 由紀子，久保 正樹，“ダークネット観測システム NICTER の持続的進化と IoT マルウェアの隆盛，” 情報通信研究機構研究報告，vol.70，no.2，2024.
6 “NICTERWEB,” https://www.nicter.jp/
7 JPCERT/CC，“定点観測友の会という名のコミュニティー活動について，” https://blogs.jpcert.or.jp/ja/2021/09/sigmon72.html
8 “ICT-ISAC JAPAN,” https://www.ict-isac.jp/
9 牧田 大佑，吉岡 克成，“DRDoS 攻撃を観測するハニーポット技術の研究開発，” 情報通信研究機構研究報告，vol.62，vo.2，2016.
10 サイバーセキュリティ戦略本部 研究開発戦略専門員会，“サイバーセキュリティ研究・技術開発取組方針，” https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai12/kenkyu_torikumi.pdf

笠間 貴弘（かさま たかひろ）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
室長
博士（工学）
サイバーセキュリティ
【受賞歴】
2025 年　第 70 回 前島密賞
2024 年　第 40 回 電子通信普及財団賞（テレコム学際研究賞）
2019 年　NDSS2019 Distinguished Paper Award

久保 正樹（くぼ まさき）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
上席研究技術員
サイバーセキュリティ