AmpPot を活用した DRDoS 攻撃対応早期化の取り組み

蒲谷　武正[†1]　千賀　渉[†1]　村上　洸介[†2]　牧田　大佑[†3†4]
吉岡　克成[†3]　中尾　康二[†1†4]

概要: 本稿においては,「国際連携によるサイバー攻撃の予知技術の研究開発」プロジェクトにおいて開発した, DRDoS（Distributed Reflection Denial-of-Service）攻撃を早期検知する AmpPot から得られるアラート情報を活用した，サイバー攻撃早期対応の取り組みについて述べる．AmpPot から得られる早期警戒情報を運用者へリアルタイムで提供する事で, ネットワーク障害時の早期原因把握に資すると共に, DoS 攻撃への対応早期化において有効であることを示す.

キーワード：AmpPot，DRDoS 攻撃，攻撃対応早期化

Quick response activity against DRDoS attacks utilizing AmpPot

Takemasa Kamatani[†1]　Wataru Senga[†1]　Kosuke Murakami[†2]　Daisuke Makita[†3†4]
Katsunari Yoshioka[†3]　Koji Nakao[†1†4]

Abstract: We report on the results of a quick response activity against cyber-attacks utilizing DRDoS (Distributed Reflection Denial-of-Service) early detection system named AmpPot that was developed by PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange) project. We show that real-time early alert information gained from AmpPot is useful to identify the cause of failure of network equipment at an early stage and is also useful to shorten a response time against DRDoS attacks.

Keywords: AmpPot, DRDoS attack, Quick response

1. はじめに

近年，インターネット上の様々なサービスを踏み台として悪用する DRDoS 攻撃（Distributed Reflection DoS attack）が大きな脅威となっており，インターネットサービスプロバイダ（ISP）の運用担当者の負荷が高まっている．ISP が通信事業用設備を維持しサービスを安定的に提供するためには，障害発生等の原因となる攻撃を把握し早期対応することが重要である.

昨年度 3 月に終了した総務省による「国際連携によるサイバー攻撃予知・即応プロジェクト（PRACTICE [a]プロジェクト）では，研究開発の成果の一つとして AmpPot[1]と呼ばれる DRDoS 攻撃を早期検知するためのシステムを開発し，国内 ISP において攻撃対応早期化の取り組みを行ってきた.

†1 KDDI 株式会社, 〒102-8460 東京都千代田区飯田橋 3 丁目 10 番 10 号 ガーデンエアタワー．KDDI CORPORATION, Garden Air Tower, 3-10-10, Iidabashi, Chiyoda-ku, Tokyo 102-8460, Japan.
†2 株式会社 KDDI 研究所，〒356-8502 埼玉県ふじみ野市大原 2 丁目 1 番 15 号. KDDI R&D Laboratories, Inc., 2-1-15 Ohara, Fujimino, Saitama, 356-8502 Japan.
†3 国立大学法人横浜国立大学，〒240-8501 神奈川県横浜市保土ケ谷区常盤台 79−1．Yokohama National University, 79-1, Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa 240-8501, Japan.
†4 国立研究開発法人 情報通信研究機構，〒184-8795 東京都小金井市貫井北町 4-2-1．National Institute of Information and Communications Technology, 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan.
a) 総務省プロジェクト「国際連携によるサイバー攻撃予知・即応プロジェクト」の英文表記“Proactive Response Against Cyber-attacks Through International Collaborative Exchange”の頭文字による略称.

本稿では，平成 27 年度に実施された PRACTICE プロジェクトにおける通信事業者における AmpPot のアラート情報を活用した DRDoS 攻撃対応早期化の取り組みについて報告する.

本論文の構成は次のとおりである．2 章で本研究の目的について述べ，3 章で AmpPot のアラート情報を活用した早期警戒情報配信システムについて説明し，4 章で ISP 基幹ネットワークのデータを用いた検証結果について述べる．5 章で考察について述べ，最後に今後の課題を述べる.

2. 目的

DRDoS 攻撃の背景として，設定不備等によって DRDoS 攻撃の踏み台と成り得るオープンリゾルバや NTP，SSDP 等のサービスがインターネット上に多数存在していること，さらには, Web 経由で指定宛先に DRDoS 攻撃を含む DDoS 攻撃を実施する Booter（Stresser）サービスの増加により，今後も当該攻撃によるインターネットユーザ，及び，通信事業者の被害は増加していくことが考えられる.

ISP においては DDoS 攻撃 等の大量通信発生時に，設備の被害を緩和するため，重要設備の常時監視を行うと共にその原因となる大量通信に対する規制等を実施している．ISP が DDoS 攻撃に対して早期対応を行うためには，障害発生の原因となる攻撃内容を早期把握すると共に，対処に向けて事前に準備を行う事が重要である.

本稿においては，通信事業者の運用者が AmpPot から得られるアラート情報を活用する事による，DRDoS 攻撃起因の障害発生の原因特定や対応早期化における有効性について検証を行った．

3. AmpPot のアラート情報を活用した早期警戒情報配信システム

本章では，AmpPot から提供されるアラート情報を運用者へ配信する早期警戒情報配信システムについて述べる．

3.1 攻撃対処における AmpPot の活用

AmpPot は DRDoS 攻撃の踏み台となるオープンリゾルバ等の一部として設置・運用されており，いわゆる囮サービスとして実際に発生する通信内容を観測し，その傾向や特徴を明らかにする事を目的として開発された[2]．本稿においては，AmpPot で観測された DRDoS 攻撃情報を活用し，運用者が攻撃対処を行うための仕組みを特定 ISP の攻撃対処事例を踏まえ構築した．

早期警戒情報配信システムにおいては，DRDoS 攻撃情報をアラートメール形式で提供する．運用者は通常の障害復旧対応時に参照する設備監視アラート情報に加え，AmpPot から得られる早期警戒情報を参照することにより，攻撃対象設備や攻撃通信の種類，影響範囲の確認を行った後，トラヒック規制等の実施を行う．早期警戒情報配信システムを使った攻撃対処の流れについて図 1 に示す．

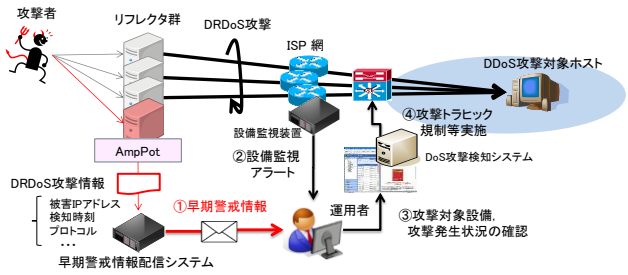

図 1　AmpPot を活用した攻撃対処の流れ

3.2 早期警戒情報配信システムの概要

早期警戒情報配信システムは，図 2 に示すとおり DRDoS 攻撃を検知しアラートを送信する AmpPot 群と解析・情報配信用サーバ，及び，AmpPot から提供を受けたアラート情報を集約しメール配信するアラートメール配信システムから構成されており，AmpPot は情報提供元の研究機関内等に設置されている．

AmpPot が攻撃を検知すると攻撃対象 IP アドレス，AS 番号，攻撃開始時刻，プロトコル（攻撃種類），FQDN（DNSAmp 攻撃の場合のみ）を含む観測情報がアラートメール配信システムへリアルタイムで送信される．アラート情報は複数の AmpPot から Fluentd [3] over VPN により ISP 等が用意したアラートメール配信システムへ提供される．

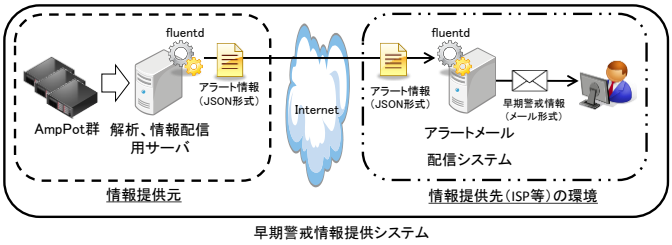

図 2　早期警戒情報提供システムの概要

3.3 AmpPot から提供されるアラート情報

本稿において活用した AmpPot は，囮となる複数種類のサービスが稼働するハニーポット群から構成されており，早期警戒情報配信システムに対しては 6 種類（DNS, NTP, CHARGEN, QOTD, SSDP, SNMP）の DRDoS 攻撃に関する情報が提供される．

AmpPot においては，同一 IP アドレスから 60 秒以上の間隔をあけずに 100 パケット（閾値）以上のパケットを受信した場合，その一連の通信を該当 IP アドレスに対する攻撃と判断している．また，AmpPot で観測された各被害 IP アドレスに対する攻撃開始と攻撃終了の情報をリアルタイムで提供する事を目的とし，情報提供元に設置された n 台の AmpPot 1, AmpPot 2 … AmpPot n から以下 2 種類のアラート情報が提供される． ”AmpPot アラート 1”と”AmpPot アラート 2”は，各被害 IP アドレスに対する一連の通信の開始と終了のタイミングで各解析・情報配信用サーバから提供される．

AmpPot アラート 1：1 分を 1 区間と定義し，1 区間内に各 AmpPot に到達するパケットの集計を行い，被害 IP アドレスに対する観測パケット数が閾値を超えた時刻を攻撃開始時刻と定義し，攻撃開始時刻を含む区間の観測結果が提供される．

AmpPot アラート 2：1 分を 1 区間と定義し，1 区間内に各 AmpPot に到達するパケットの集計を行い，連続した区間において同一 IP アドレスから 60 秒間以上パケットの観測がなかった場合に該当 IP アドレスに対する攻撃が終了したと判断し，最後に到達したパケットの到着時刻を攻撃終了時刻と定義する．本アラートにおいては，攻撃開始から攻撃終了までの全ての区間の観測結果が提供される．

“AmpPot アラート 1” ，及び，“AmpPot アラート 2”は JSON フォーマットにより定義され，表 1 に示す情報が各 AmpPot から提供される．

表 1　AmpPot により提供されるアラート情報

No.	項目名	形式	内容説明
1	detecttime	文字列	AmpPotにおいて攻撃対象 IP アドレスからのパケットが閾値を超えた時刻
2	target	文字列	攻撃対象 IP アドレス
3	service	文字列	攻撃を観測したサービス（DNS, NTP, CHARGEN, QOTD, SSDP, SNMP の 6 種類）
4	country	文字列	「2」の国情報
5	avepps	浮動小数点	平均の PPS
6	elapsedtime	整数値	継続時間（秒）
7	as	文字列	「2」の AS 情報
8	stoptime	文字列	攻撃観測を終了した時刻
9	alerttime	文字列	アラートを送信した時刻
10	starttime	文字列	攻撃観測を開始した時刻
11	query	文字列	クエリの回数（service が”DNS”の場合のみ）
12	sensorid	文字列	AmpPot の ID
13	maxpps	浮動小数点	最大の PPS
14	totalpacket	整数値	総攻撃パケット数

3.4 AmpPot 群から提供されるアラート情報の集約

AmpPot から提供されるアラート情報は，複数台の AmpPot から任意のタイミングで送信されること，さらには, 観測された全ての被害 IP アドレスに関する観測情報を含んでいることから，情報提供先となる ISP 等においてこのアラート情報を活用するためには，アラート情報の集約が必要となる．

本研究においては，情報提供先に設置するアラートメール配信システムにおいてアラート情報を ISP の自網宛の情報のみに絞ると共に，同時刻に複数の AmpPot から配信されるアラート情報を被害 IP アドレス毎に一連の攻撃情報として集約して運用者へ通知する仕組みを実装した．

アラート集約において, AmpPot から提供される”AmpPot アラート 1”，及び，“AmpPot アラート 2”を活用し，各被害 IP アドレスに対する攻撃開始時刻, 攻撃終了時刻を特定する. 被害 IP アドレスに対して最も攻撃を早く検知した AmpPot から提供される” AmpPot アラート 1”を攻撃開始アラート，また，一連の通信において最後に到達する攻撃パケットを観測した AmpPot から提供される” AmpPot アラート 2”を攻撃終了アラートとして判定し，それぞれの情報を攻撃開始アラートメール・攻撃終了メール情報として ISP の運用者へ提供する．アラート情報の集約については図 3 に示すとおりとなっている．

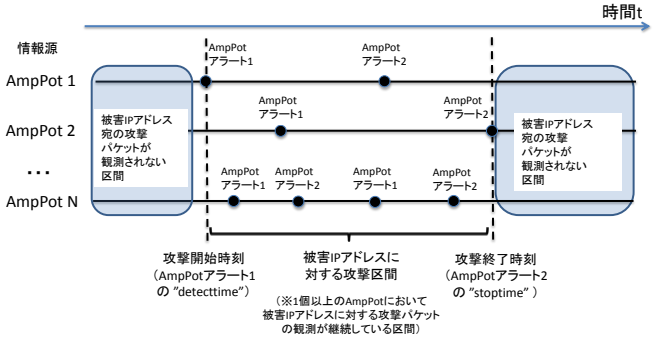

図 3　アラート情報の集約

1 個以上の AmpPot において被害 IP アドレスに対する攻撃パケットの観測が継続している区間が一連の攻撃区間と定義され, 図 3 の例においては, AmpPot1 から提供される” AmpPot アラート 1”の情報から攻撃開始時刻を，AmpPot2 から提供される” AmpPot アラート 2”から攻撃終了時刻の情報を取得している．

4. AmpPot アラート情報を活用した DRDoS 攻撃早期対応の検証

本章では，提案手法の有効性を示すために行った検証内容及びその結果について述べる．

4.1 早期警戒情報を活用した障害復旧対応

ISP においては,「電気通信事業者における大量等への対処と通信の秘密に関するガイドライン」[4] に基づき, 様々な監視機器から取得されるアラート情報を参照して大量通信発生時の被害対象, 影響範囲等を把握すると共に，対応要否や対処方法の判断を行い, 通信規制等を実施している．

本研究において使用する AmpPot は，DRDoS 攻撃の踏み台となる複数のサービスを囮として運用しており，一般に公開しているサービスでは無い[5]ことから，AmpPot において観測される通信はインターネット上に公開されているサーバ等の探索を目的とするスキャンや DRDoS 攻撃等不正活動に関係する可能性が高い．本取り組みにおいては，AmpPot で観測したパケットを分析して得られる統計値において DRDoS 攻撃の傾向や特徴が強く反映されていることを踏まえ，障害発生設備に対する DRDoS 攻撃発生の有無や攻撃規模を確認するための情報として AmpPot から得られる早期警戒情報を通信規制等実施時に有効活用する事を考えた．

ISP の多くにおいて大量通信発生時には，専用の DDoS

攻撃対策のサービスにより提供される異常検知，代理応答等の機能を使って対処，あるいは，ネットワーク上の通信の制御技術（ルータによるアクセス制御や経路による攻撃通信トラヒックの吸い込み 等)を使って対処するケースが多いが，本稿においては攻撃通信トラヒックの吸い込み方式[6]により運用を行うケースを前提として，AmpPot により提供されるアラート情報を活用した障害復旧対応の早期化について検証を行った．

4.2 早期警戒情報を活用するための攻撃対処フロー

早期警戒情報を活用するための攻撃対処フローを図 4 に示す．従来の攻撃対処フローにおいては，運用者は監視機器による障害検知結果通知をトリガーとして対応を開始するが，本研究においては運用者が障害に関連する早期警戒情報を攻撃開始アラートメール・攻撃終了アラートメールとして障害検知結果通知と並行して取得する事により，障害発生時の原因特定や通信規制等の対処に必要な情報を適切なタイミングで取得し，対応の早期化を図った．

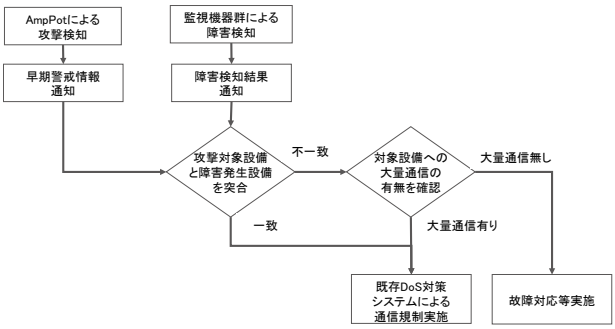

図 4　早期警戒情報を活用した攻撃対処フロー

ISP 運用者は，図 4 の「攻撃対象設備と障害発生設備を突合」の記載箇所において，障害発生設備が DRDoS 攻撃の被害 IP アドレスを収容しているかどうか，攻撃検知時刻と障害発生時刻が一致しているかどうか，さらには，被害 IP アドレスに到達する総トラヒック量について確認し，障害発生設備に対する DRDoS 攻撃の発生が確認できた場合に既存 DoS 対策システムによる通信規制等を実施する．攻撃開始・終了アラートメールの配信内容を図 5 に示す．

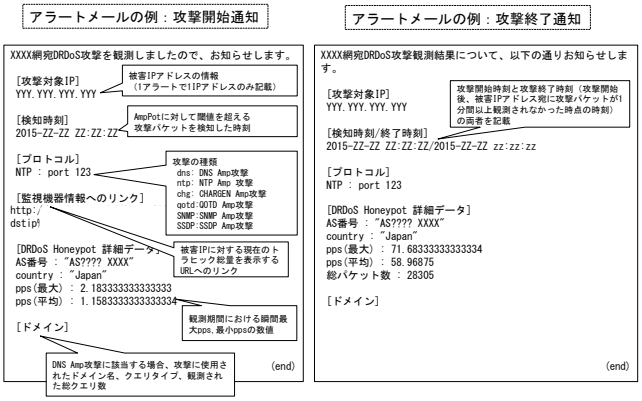

図 5　攻撃開始・終了アラートメール

運用者が使用する情報は，アラートメール本文，あるいは，アラートメール本文に記載された監視機器が提供するポータルへの URL リンク情報を参照する事により即時に得られるため，早期警戒情報を適切なタイミングで運用者へ提供する事により，運用者の判断を支援すると共に，通信規制実施等の対処に要する時間を短縮することが期待される．

4.3 早期警戒情報配信のタイミングについての検証

本稿においては，ISP の運用者が障害発生をトリガーとして攻撃対処を実施する事を踏まえ，障害発生時刻と早期警戒情報送付時刻の差を比較し，早期警戒情報の運用者への通知のタイミングについて評価を行った．

2015 年 4 月 1 日から 2016 年 2 月 26 日までの 11 か月間を対象として検証を実施した結果，AmpPot は期間内に 30 件の障害対応を要する攻撃を検知した．比較結果については図 6 に示すとおりとなっている．

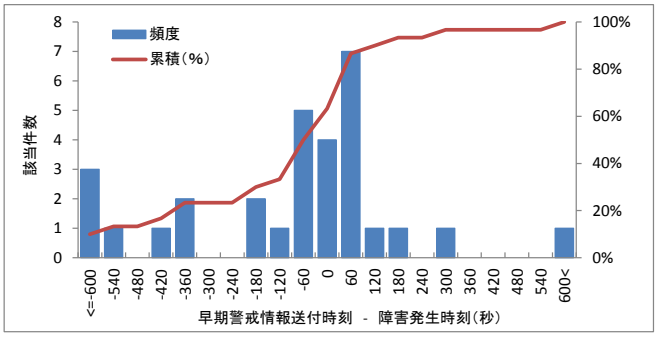

図 6　早期警戒情報送付時刻と障害発生時刻の比較

この 30 件の攻撃に関して ISP における障害発生時刻と早期警戒情報送信時刻の比較を行ったところ，19 件については障害発生の前に運用者に対して通知を行った．その他 11 件のうち，9 件については障害対応時に通知を行っており，残りの 2 件については障害対応後の通知となった．障害対応後に通知された早期警戒情報 2 件のうち 1 件については，被害 IP アドレスに対して同時刻に実施された 2 種類の DRDoS 攻撃（NTP・DNS） のうち 1 種類の攻撃トラヒック（DNS）のみを検知しており，なおかつ，初期段階の攻撃トラヒックを検知できていなかった．これについては，次節で詳細に述べる．別の 1 件については，AmpPot において障害発生の 109 秒前に攻撃を検知していたものの，情報提供元の解析・情報配信用サーバの処理遅延に伴い運用者への通知も遅れた．

本システムにおいて検知した障害対応を要する攻撃事象に関して，30 件中 28 件については運用者の障害対応実施前に攻撃対象の設備を特定するための情報として提供されており，適切なタイミングで情報提供が行われている事を確認した．

4.4 早期警戒情報による攻撃傾向の把握

障害発生の原因となった攻撃通信の傾向を正しく通知できていたかどうかについて検証するため，AmpPot が検知し早期警戒情報として運用者へ通知された攻撃種類の情報と障害発生の原因となった攻撃通信のプロトコル分布についての比較を行った．大量通信におけるプロトコル分布については，既存の監視機器により取得可能なプロトコル別の総トラヒック量 （総パケット数）の情報を使用した．

2015 年 4 月 1 日から 2016 年 2 月 26 日までの 11 か月間において早期警戒情報配信システムが検知した 30 件の障害対応を要する攻撃について確認したところ，29 件については全て「AmpPot で検知した攻撃トラヒックのプロトコル」と「障害発生の原因となった大量通信において最もトラヒック量(パケット数)が多かった通信のプロトコル」が合致しており，障害の原因となった攻撃通信の傾向を正しく捉えることができていた．

その一方，1 件の障害においては図 7 に示すとおり，AmpPot が検知した DRDoS 攻撃のプロトコルが DNS であったのに対し，障害発生時に被害 IP アドレスに対して発生したトラヒック量が最も多かったプロトコルが NTP であり，両者が一致していなかった．図 7 のケースにおいては，NTP リフレクション攻撃の検知ができていなかったことにより，AmpPot の検知が障害発生後となった．

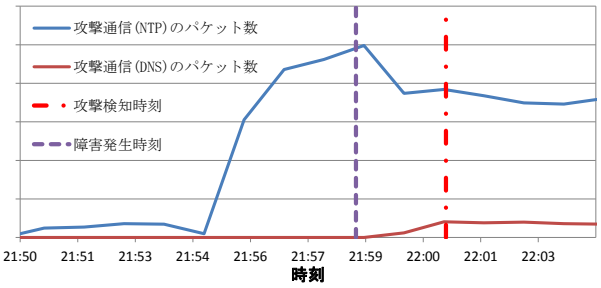

図 7　AmpPot が検知した攻撃種類と障害発生の原因となった通信のプロトコルが一致しないケース

4.5 アラートを活用した攻撃対応早期化についての検証結果

早期警戒情報活用による対応時間短縮の効果を検するため，早期警戒情報配信時の DRDoS 攻撃対応に要した時間と早期警戒情報非配信時の DRDoS 攻撃対応に要した時間を比較した．DRDoS 攻撃対応に要した時間は，障害発生から通信規制を実施するまでに要した時間と定義しており，「早期警戒情報配信時の DRDoS 攻撃対応に要した時間」，及び，「早期警戒情報非配信時の DRDoS 攻撃対応に要した時間」のいずれも 2015 年 4 月 1 日から 2016 年 2 月 26 日までの 11 か月間の期間を対象として得られた全ての数値を平均した値とした．検証の結果は表 2 に示すとおりとなった．

表 2　早期警戒情報の有無、通知のタイミングと攻撃対処に要した時間の関係

早期警戒情報の有無、通知のタイミング		攻撃対処に要した時間（秒）
早期警戒情報を通知した場合	障害発生前に早期警戒情報を通知	82
	障害発生後に早期警戒情報を通知	142
早期警戒情報を通知できなかった場合		167

運用者への早期警戒情報の通知の有無，通知のタイミングを踏まえ DRDoS 攻撃起因の障害対応時の攻撃対処に要した時間を比較した結果，表 2 に示すとおり障害発生前に早期警戒情報を通知できたケースにおいて最も攻撃対処に要した時間が短く 82 秒であった．これは早期警戒情報を全く通知せずに攻撃対処を行った場合の攻撃対処に要した時間と比較するとおよそ 85 秒の時間短縮となった．一方，障害発生後に早期警戒情報が通知されたケースにおいても攻撃対処に要した時間が，早期警戒情報が全く通知されなかったケースと比較して 25 秒短縮されており，実際に攻撃対処の際に早期警戒情報を参照し，判断を行う事により対応が早まったことが考えられる．

5. 考察

評価結果に示すとおり，DRDoS 攻撃起因の障害発生時に 30 件の早期警戒情報が送付され，そのうちの 19 件については障害発生前の情報提供となっており，平均すると障害発生の 411 秒前に早期警戒情報が運用者へ通知された．運用者は，障害発生前に攻撃対象 IP アドレスを収容する設備の情報を元に攻撃対処へ備えることにより，障害発生時の原因把握，対処方法の決定を効果的に実施することが可能となり，攻撃対応の早期化につながったと考えられる．また，その他の 9 件については障害発生後に運用者へ通知されたものであったが，障害対応中に障害発生設備に対する DRDoS 攻撃の有無の情報が運用者へ提供されたことにより，対処方法の決定等が早まったと考えられる．

本システムにより DRDoS 攻撃により発生した障害について，その攻撃の対象と種類，規模について運用者に対し障害発生原因の把握に資するタイミングで情報提供可能であることが示された．また，提案手法により攻撃通信トラヒックの吸い込み方式と併用した早期警戒情報の活用により，「4.5　アラートを活用した攻撃対応早期化についての検証結果」に示したとおり，DRDoS 攻撃起因の障害発生時の復旧対応に要する時間が短縮されたことを確認した．

6. 今後の課題

AmpPot のアラート情報を活用した DRDoS 攻撃対応の取り組みにより障害発生前，あるいは，障害対応時に障害発生設備への DRDoS 攻撃の有無，攻撃開始時刻，攻撃種類，及び，攻撃規模等の情報を運用者へ通知することにより，障害発生時の原因特定に資することを確認した．

その一方で，早期警戒情報の通知が運用者の対応後になったケースについては，DRDoS 攻撃の近年の傾向において複数種類の DRDoS 攻撃が同時に実施される場合が多いことや，攻撃者が攻撃過程でリフレクタ群の組み合わせを変更している可能性がある[1]ことから，AmpPot の観測範囲を広げることにより攻撃検知の早期化を図っていく必要がある．また，DRDoS 攻撃発生時に対処が必要な設備障害へ発展するか否かについては攻撃の規模のみならず攻撃対象設備のキャパシティにも依存するため，本アラート情報の活用においては，設備監視アラートやアセット情報等と併用する事で早期警戒情報の確度を高めることが期待される．

AmpPot のアラート情報を使った早期警戒アラート配信の仕組みについては，2015 年 12 月にテレコム・アイザックジャパン （Telecom-ISAC Japan） [b] へ移管済み[7]であり，Telecom-ISAC Japan 会員の国内 ISP の一部に対してアラート配信を開始している． 一方，本システムの海外展開については PRACTICE プロジェクトにおいて大枠の合意をしているものの，今後関係者間での多くの具体的な調整や作業が必要となる．PRACTICE プロジェクトで得られた知見や技術的成果，また，海外連携先との協力関係は今後も何らかの形で引き継いでいき，サイバー攻撃のリスク低減に役立つことを期待したい．

謝辞 本研究は，総務省による研究開発委託「国際連携によるサイバー攻撃の予知技術の研究開発」により行われた．

参考文献

[1] Lukas Kramer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow, "AmpPot: Monitoring and Defending Amplification DDoS Attacks," Proc. Research in Attacks, Intrusions, and Defenses (RAID15), Lecture Notes in Computer Science, Vol. 9404, pp. 615-636, 2015.

[2] 筒見 拓也, 野々垣 嘉晃, 田辺 瑠偉, 牧田 大佑, 吉岡 克成, 松本 勉, "複数種類のハニーポットによる DR-DoS 攻撃の観測," IPSJ SIG Notes 2014-CSEC-65(16), 1-6, 2014.

[3] “Build Your Unified Logging Layer”, <http://fluentd.org> 2016 年 8 月 1 日閲覧.

[4] 一般社団法人日本インターネットプロバイダー協会(2015) 「電気通信事業者におけるサイバー攻撃への対処と通信の秘密に関するガイドライン － 第 4 版 -」 <https://www.jaipa.or.jp/other/mtcs/guideline_v4.pdf > 2016 年 8 月 1 日閲覧.

[5] 牧田大佑，吉岡克成，松本勉, "DNS ハニーポットによる DNS アンプ攻撃の観測," IPSJ Journal No. 55, Vol. 9, pp. 2021 - 2033, 2014.

[6] Urakawa, J., Sawaya, Y., Yamada, A., Kubota, A., Makita, D., Yoshioka, K., Matsumoto, T.: An Early Scale Estimation of DRDoS Attack Monitoring Honeypot Traffic. In: Proceedings of the 32nd Symposium on Cryptography and Information Security, 2015.

[7] 千賀渉，蒲谷武正，村上洸介，中尾康二，“PRACTICE ―国際連携によるサイバー攻撃の予知・即応プロジェクト―”, 2016 年電子情報通信学会総合大会, 2016.

b) 一般財団法人日本データ通信協会 テレコム ・アイザック 推進会議 (2016 年 3 月 9 日に Telecom-ISAC Japan の活動は，発展的に一般社団法人 ICT-ISAC へ継承された．)