Computer Security Symposium 2021
26 - 29 October 2021

C2 サーバを対象とした相互協力による継続的観測システムの提案

堀井 大雄[†1]* 藤井 翔太[†2] 青木 翔[†2] 佐藤 隆行[†2] 寺田 真敏[†1, †2]

概要：標的型攻撃に使用される C2 サーバの情報は，サイバー攻撃対策における不正接続先情報として共有されている．その一方で，通知後の不正接続先の活動状況の確認は組織毎に独自で実施しており，組織間での相互協力は行われていないのが現状である．本研究では，運用面での効率化及び誤検知低減のため，通知された不正接続先を対象とした相互協力による継続的観測システムを提案する．提案システムでは，複数観測点での観測，並びに脅威情報の識別番号を利用した不正接続先の観測結果の共有を特徴としている．また，提案システムの試行運用として公的機関かは配信された不正接続先を継続観測したところ，半年以上経過しても約 30%の割合で HTTP サーバとして応答する場合があることを確認した．

キーワード：C2 サーバ，継続的観測，サイバー脅威インテリジェンス

Proposal of continuous monitoring system for C2 servers through mutual cooperation

Daiyu Horii[†1] Shota Fujii[†2] Sho Aoki[†2] Takayuki Sato[†2] Masato Terada[†1, †2]

Abstract: The information of C2 servers used in targeted attacks is shared as the information of unauthorized access points in cyberattack countermeasures. On the other hand, each organization independently checks the activity status of the malicious destination after notification, and there is no mutual cooperation among organizations. In this study, we propose a continuous monitoring system for the notified unauthorized access points by mutual cooperation in order to improve operational efficiency and reduce false positives. The proposed system is characterized by multiple monitoring agents and the sharing of the monitoring results of the unauthorized accesses by using the identification number of the threat information. In addition, as a trial operation of the proposed system, we continuously monitored the malicious destinations distributed by public organizations, and confirmed that about 30% of the malicious destinations still respond as HTTP servers even after more than half a year.

Keywords: C2 server, Continuous monitoring, Cyber Threat Intelligence

1. はじめに

2012 年以降，特定の組織や産業を狙う標的型攻撃は継続して発生している．標的型攻撃ではマルウェアに感染した端末を制御するために指令サーバ（以降，C2 サーバ）が用いられる．攻撃者は短期的な利用として使い捨ての形態で C2 サーバを稼働する場合や，長期的に利用し続けるためにドメイン名の変更や攻撃活動に合わせて停止と稼働を繰り返す場合がある．感染した端末を制御する C2 サーバの情報共有については，2015 年に始動した米国土安全保障省による Automated Indicator Sharing（AIS）[1]など，サイバー脅威インテリジェンス（Cyber Threat Intelligence: CTI）を複数の組織で共有し，サイバー脅威への迅速な対応を可能にする官民協調型の基盤の整備が進んでいる．国内においては， JPCERT/CC[2]や IPA[3]などがハブ組織として活動しており，C2 サーバの情報を不正接続先として配信している．

その一方で，配信された不正接続先の稼働把握のための観測については各組織が独自に取り組んでいるのが現状で，連携するための基盤の整備は行われていない．不正接続先の稼働把握については，配信された不正接続先をファイアウォールなどの拒否リストから，いつ削除して良いのか？を考える上で必要になる．このような運用を考えていくと，不正接続先の稼働を確認するという作業が各所で個別に実施されている可能性が高く，不正接続先の観測の観点で効率的でない．また，攻撃者が特定 IP アドレスからの観測や周期性のある観測を発見した場合はアクセスを遮断することが考えられ，観測点が 1 つのみの場合，観測結果の信ぴょう性が低下する恐れがある．更に，観測システムやネットワークに障害が発生した場合の可用性の問題もある．

本研究では，これらの問題に対し，相互協力型の継続的観測システムを提案する．提案システムでは，公的機関から配信された不正接続先を対象に複数観測点で Ping と HTTP による継続的観測を行い，レスポンスを記録・共有する．さらに，公的機関から配信された不正接続先に関する一連の攻撃活動に脅威情報識別番号を付与すると主に，脅威情報識別番号を使った稼動状況の可視化を通して関連

†1 東京電機大学
Tokyo Denki University
†2 株式会社日立製作所
Hitachi, Ltd.

* daiyu-horii@isl.im.dendai.ac.jp

組織との迅速な共有を可能にする．

本稿では，配布された不正接続先情報の観測について課題を示した後，問題解決のための相互協力による継続的な観測を実施する提案システムの概要について述べる．また，提案システムの試行運用を通して収集したレスポンスデータを分析した結果について報告する．

2. 研究背景

2.1 不正接続先の稼動把握に関する課題

標的型攻撃に用いられるマルウェアは C2 サーバと呼ばれる指令サーバと通信する機能を有している．C2 サーバのライフサイクルは多様であり，例えば，短期的な利用として使い捨ての形態で C2 サーバを稼働する場合や，長期的に利用し続けるためにドメイン名の変更や攻撃活動に合わせて停止と稼働を繰り返す場合がある[4]．また，配信情報は不正接続先の IP アドレス，ドメイン名，URL 情報と，マルウェアのファイル名，ハッシュ値，感染手法などに限られており，不正接続先がどのように振る舞うかといった情報は付随していない場合が多く，その稼動把握は各組織が自身で取り組まなければならない．

不正接続先としての C2 サーバへの対策として，配信された不正接続先をファイアウォールなどの拒否リストに登録するという方法がある．しかし，いつ拒否リストから削除して良いのか？を考える上で，配信された不正接続先を継続的に観測し，観測対象の活性度の経過や兆候を観察しつつ拒否リストへの継続追加・削除を判断することが必要となる．

2.2 脅威情報の共有

特定の業界や産業を狙った標的型攻撃において，複数組織に対して同じ手法を用いた攻撃が実施される場合が多く見られる[5]．このため，不正接続先の IP アドレス，ドメイン名，URL 情報や，マルウェアのファイル名，ハッシュ値などの攻撃活動に関する脅威情報を流通させることで，更なる被害を抑えるのに非常に有効である（図 1）．事前措置視点では，入手した情報に基づきサイバー攻撃が行われる前に迅速にサイバー攻撃対策を施すこと，事後措置視点では，サイバー攻撃による侵害有無を特定することなどが考えられる．

攻撃活動に関する脅威情報の流通については，機械可読可な形式で脅威情報を記述することで自動化を進めるために，MITRE が中心となり開発を進めてきた STIX/TAXII をはじめとする脅威情報記述形式及び関連技術がある[6]．また，2015 年には，STIX/TAXII を採用した米国土安全保障省による Automated Indicator Sharing（AIS）[1]が運用されるなど，官民協調型の脅威情報共有基盤の整備が進んでいる．

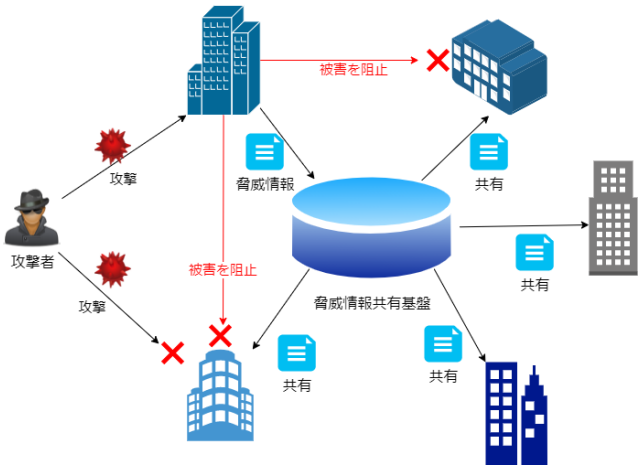

図 1 脅威情報共有による被害拡大の防止

このような取り組みに呼応し，脅威インテリジェンスプラットフォーム（Threat Intelligence Platform: TIP）と呼ばれる，脅威情報の分析と共有によるサービスを提供しているセキュリティベンダも数多く存在する一方，その殆どはデータの分析より収集に焦点を当てていると指摘する研究もある[7]．即ち，データを収集・共有する体制は整備されているものの，実際に脅威情報を活用して有効なサイバー攻撃対策を講じることが出来ているかは，定量的評価が難しいこともあり，不明瞭であることを指摘している．また，配信された脅威情報や上記のサービスを用いた適切なサイバー攻撃対策の成否は各組織の運用次第である側面が大きいと考えられる．

3. 相互協力による継続的観測システム

本章では，提案する C2 サーバを対象とした相互協力による継続的観測システムの構成と機能について述べる．

3.1 提案システムの概要

提案システムは，公的機関などによって配信される不正接続先を対象に相互協力による継続的観測を行い，それらの活動状況の把握及び対処の判断を支援することを目的としている．提案システムを実現するにあたっては，次に示す機能要件を設定した．

(1) 自律した不正接続先観測

提案システムで実施する観測は相互協力が可能である一方，単一障害点や観測点同士の相互依存を避けるため，個々の観測点は単体でも観測が実施可能であること．

(2) 観測記録の共有

相互協力を実現するために，ある観測点において他観測点が記録した観測記録が参照可能であること，すなわち，協力者間でデータを共有する仕組みを持つこと．

(3) 観測記録の可視化

提案システムは，観測記録を参照して不正接続先の稼動状況の把握と対処の判断を支援すること．ここでは，CLI などのテキストでは状況把握は困難であり，判断の

即時性にも欠けるため，支援する手法として不適切であると考え，GUI を用いたグラフを用いて観測記録を可視化することとする．

3.2 提案システムの構成

提案システムの構成を図 2 に示す．提案システムでは，観測用端末クラスタを構成するが，読み込んだ不正接続先リストに従い，個々の観測用端末は自律して動作する（機能要件 1)．次に，個々の観測用端末は，不正接続先に関する観測記録をシステムで共用するストレージに転送し，アクセスが許可されている利用者の間で共有する（機能要件 2)．不正接続先の稼動状況の把握と対処の判断を支援については，可視化用 Web サーバを用い，共用ストレージからダウンロードした観測記録をグラフ化する（機能要件 3)．

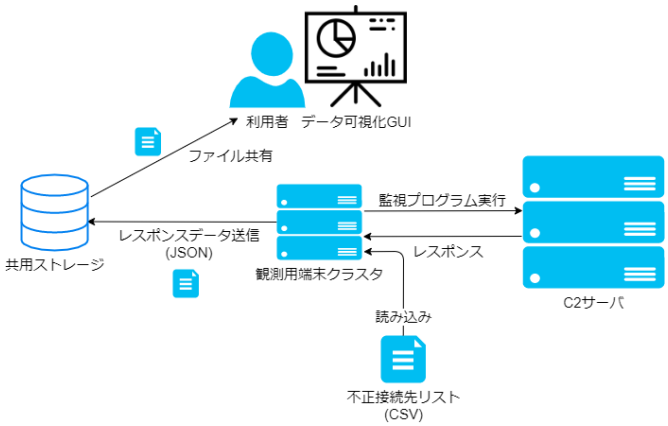

図 2　提案システムの構成

4. 提案システムの実装

本章では，提案システムの実装方式について述べる．

4.1 自律した不正接続先観測

(1) 実行フロー

観測プログラムは不正接続先へ Ping と HTTP GET リクエストを送信し，その応答結果を記録するものであり，同プログラムの実行フローは次の通りである．

ステップ 1：不正接続先情報の取得

不正接続先情報を CSV 形式で記述した不正接続先リストから取得する．同ファイルには攻撃活動に対する脅威情報識別番号，IP アドレス，ドメイン名，URL，ポート番号，報告日を記載する．この際，各不正接続先と脅威情報識別番号を紐付けておくほか，マルウェアハッシュ値，ファイルタイプや概要などの情報がある場合はあわせて記載する．

ステップ 2：Ping の送信

不正接続先情報に基づき，観測対象へ Ping を送信する．この際，ステップ 1 で取得した不正接続先情報として IP アドレス，ドメイン名，URL のいずれか 2 つ以上に記載がある場合，記載があるものから URL，ドメイン名，IP アドレスの順に優先して選択するものとする．Ping は 4 回送信し，パケット損失率，平均 RTT，TTL を記録する．

ステップ 3：HTTP GET の送信

HTTP GET リクエストの送信では，送信先はステップ 2 と同様な方法で選択する．送信の際には，感染端末からのアクセスに近づけるため，HTTP ヘッダの Accept-Encoding, User-Agent を設定する．HTTP レスポンスの記録としては，ステータスコード及び理由フレーズ（例: 200 OK）を記録する．

ステップ 4：観測結果の記録

観測記録の保存形式は，ICT-ISAC Japan[8]が総務省「ソフトウェア脆弱性を狙ったサイバー攻撃の防御に向けた情報共有基盤に関する実証実験」で使用している JSON 形式の STIX 拡張記述仕様に従い，観測日時をファイル名とした JSON ファイルとして保存する（図 3)．


```
{
    "x-ict-isac.jp": {
        "id": "72e17d5f-f9d1-471a-8bd7-011d190f38c7",
        "monitoring": {
            "domain-name": [
                ""
            ],
            "ipv4-addr": [
                "[redacted].142"
            ],
            "ping-ext": {
                "loss": "0%",
                "ttl": 55,
                "rtt": "7.359ms"
            },
            "network-traffic": {
                "src-port": 59238,
                "dst-port": 80
            },
            "http-request-ext": {
                "request-method": "get",
                "request-value": "",
                "request-version": "http/1.1",
                "request-header": {
                    "Accept-Encoding": "gzip,deflate",
                    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
                    "Host": "[redacted].142"
                }
            },
            "http-response-ext": {
                "status_code": 200,
                "reason_phrase": "OK"
            },
            "file": {
                "file-type": "",
                "name": "",
                "hashes": {
                    "md5": "",
                    "sha1": "",
                    "sha256": ""
                }
            },
            "observe-time": "2021-07-01T16:01:20",
            "files": [],
            "input": "[redacted].142"
        },
        "process-time": {
            "system-name": "vcity-monitor",
            "start": "2021-07-01T16:01:15",
            "end": "2021-07-01T16:01:20"
        }
    },
    "submit_time": "2021-07-01T16:01:15"
}
```


図 3　STIX 拡張記述仕様に従った観測記録の例

(2) 周期的実行

提案システムでは，4 つのステップからなる観測プログラムを周期的に実行する．周期は時刻 00:00:00 JST を基準とし，4 時間毎とする．なお，実装では，Linux に搭載されている systemd のサービスとして観測プログラムを観測用端末に定期実行させることにより，これを実現した．

4.2 観測記録の共有

観測記録の共有では，この取り組み自体が試行段階にあり，観測の実データ流通による情報共有の可能性を探るため，観測記録の共有にはクラウドストレージの Box を用いた．実装にあたっては同クラウドサービスが提供する Python 用ライブラリ（SDK）を利用しており，ファイルのアップロード・ダウンロードは Box API を介して行う．共

有フォルダにはアクセス制限が設けてあり，アクセスには Box 側の認証を必要とするため，利用者は Box API が指定する形式の認証用 JSON ファイルを用いてアクセスすることで，観測記録を共有する．

4.3 観測記録の可視化

観測記録の可視化は Web ブラウザ上の GUI で実現し，Web サーバの構築には Python 及び同言語のライブラリとして提供されている軽量 Web フレームワークの Flask を使用した．UI の実装には，デザインテンプレートである Bootstrap 及び JavaScript ライブラリの Chart.js を使用し，グラフを用いたダッシュボード形式を採用した．

可視化ダッシュボードでは，月単位で可視化を行う．利用者は攻撃活動の脅威情報識別番号，年月を選択することで，選択した月の 1 ヵ月分の観測記録を可視化するダッシュボードに遷移する．図 4，図 5 にダッシュボードでの観測記録の可視化を示す．

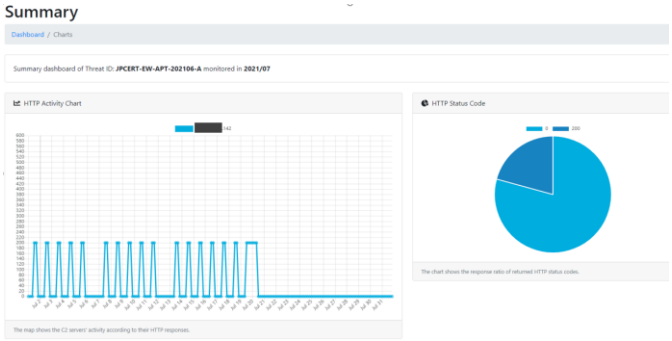

図 4　HTTP レスポンス結果の可視化

図 5　Ping 応答結果の可視化

ダッシュボードでは，1 ヵ月分の観測記録を，折れ線グラフ及び円グラフを使用する．折れ線グラフでは HTTP ステータスコードと Ping の応答率を可視化し，横軸を時間，縦軸はステータスコードとパケット損失率である．また，1 つの脅威情報識別番号に複数の不正接続先が含まれていた場合には，色を変え同じグラフ中にプロットする．円グラフでは，1 ヵ月間に取得した全 HTTP レスポンスの割合を可視化する．

5. 提案システムを用いた観測

本研究では，4 章で実装した提案システムを実際に運用し，2021 年初頭から継続して観測を実施している．本章では，2021 年 1 月から 2021 年 4 月までの 4 ヶ月間及び 2021 年 7 月の 1 ヵ月間に観測した記録を分析した結果を報告する．

5.1 観測記録の概要

観測期間中に提案システムで使用した観測用端末数は，1 台である．

観測対象としては，公的機関から配信された不正接続先を対象としている．なお，5 月から 6 月にかけては，観測記録の保存形式の変更に伴う観測システムの不具合により記録が取れなかったため分析対象外とした．

観測対象とする不正接続先の総数は 47 件で，割り振った脅威情報識別番号は 9 件である．脅威情報識別番号の最も古いものは 2020 年 10 月，最も新しいものは 2021 年 6 月である．

5.2 分析

(1) 脅威情報識別番号で見た応答率の経過

観測期間で得た，各脅威情報識別番号の月別の HTTP レスポンスの応答率（%）及び脅威情報識別番号の登録年月を表 1 に示す．なお，脅威情報識別番号 E~I を監視対象リストに追加したのは 2021 年 6 月であるため，7 月のみの観測記録となっている．

(2) HTTP レスポンス

表 1 の示す通り，全ての脅威情報識別番号において不正接続先の HTTP レスポンス返答率は時間の経過と共に低下する傾向を示しており，これは多くの不正接続先の生存期間は短いという研究調査に概ね則していると思われる[9]．しかしながら，一部の脅威情報識別番号では半年以上経過した 7 月時点においても 3 割以上が HTTP レスポンスを返していることを確認した．最も古い脅威情報識別番号の報告月が 2020 年 10 月であることを考えると，同観測期間中に不正接続先が稼働していた割合は多いと言える．このことから，攻撃者は今後もこれらのドメインや接続先を長期利用する可能性が考えられる．その理由としては，今回対象としている不正接続先が公的機関から配信されたものであり，一定レベル以上の分析がされた情報であるという点と，実際に HTTP GET リクエストを送信した宛先として，比較的変更されやすいドメイン名ではなく IP アドレスが多いという点が挙げられる．

脅威情報識別番号 B や D のように，低い活性度であった活動がある時点で再度活性化することを確認した．両者の HTTP レスポンスと Ping の記録の相関を調べたが（図 6），共に相関がある期間とない期間が存在した．これは Ping が失敗している可能性も考えられるが，ある程度の相関性が確認出来ることから，攻撃者のネットワークに何らかの変更があったと考えられる．

表 1　月別の HTTP レスポンス返答率

脅威情報識別番号	報告年月	観測月				
		2021 年 1 月	2021 年 2 月	2021 年 3 月	2021 年 4 月	2021 年 7 月
A	2020 年 10 月	74.2	49.2	47.0	54.1	36.4
B	2020 年 10 月	5.5	2.2	1.4	11.0	0
C	2020 年 10 月	61.5	36.5	32.9	36.5	38.4
D	2020 年 10 月	47.7	28.9	33.3	38.2	25.6
E	2020 年 12 月	-	-	-	-	100
F	2021 年 1 月	-	-	-	-	40.6
G	2021 年 2 月	-	-	-	-	100
H	2021 年 3 月	-	-	-	-	0
I	2021 年 6 月	-	-	-	-	20.7

図 6　HTTP レスポンスと Ping の相関

(3) HTTP ステータスコード

不正接続先が返答する HTTP ステータスコードのパターンにも違いが見られた. 全ての脅威情報識別番号において，最も多く観測したパターンは継続して同じステータスコードを返答するパターンである．しかし，この場合においてもある短期間にのみ HTTP レスポンスを返答しなくなる場合が見られたが，Ping 損失率と比較すると，殆どの通信先で Ping 損失率が 100%の時に丁度 HTTP レスポンスの返答がなくなっていることを確認した（図 6）．これも，攻撃者のネットワークそのものに変更が加わっているためだと考えられる．

一方で，ステータスコードの変化が多く見られる不正接続先も確認した．ある不正接続先において，1 月から 2 月にかけ継続してステータスコード 200 OK を返答していた URL が 3 月のある時点から 404 Not Found を返答するように変化し，更にその 2 週間ほど後の 4 月には 500 Internal Server Error を返答するよう変化したことを確認した．これは攻撃者の C2 サーバのプログラムに変更が加わった可能性が考えられる．なお，同接続先は 7 月の全期間で HTTP と Ping 共に全く返答しなくなり，活動を停止したと思われる．

ステータスコードが停止から稼働に変化する事例についても観測している（図 7）．この事例では，ある不正接続先は 1 月時点で 404 Not Found を継続的に返答し，月末になると時折 500 Internal Server Error を返答していた．翌月の 2 月には 200 OK を返答するよう変化し，同期間において Ping と連動して小刻みに応答ありとなしを繰り返していた．これは，攻撃活動に合わせてサーバの応答を調整しているためであると考えられる．続く 3 月と 4 月では Ping と HTTP 共に全く応じなくなった．この結果は，404 Not Found や 500 Internal Server Error を返答していた期間は後に攻撃活動を実施するための準備期間であったことを示していると推測されるが，3 月と 4 月において返答がなくなったのは活動が停止したためなのか，あるいは観測用端末が攻撃者によって接続拒否されたためなのかは，本検証では断定に至らなかった．

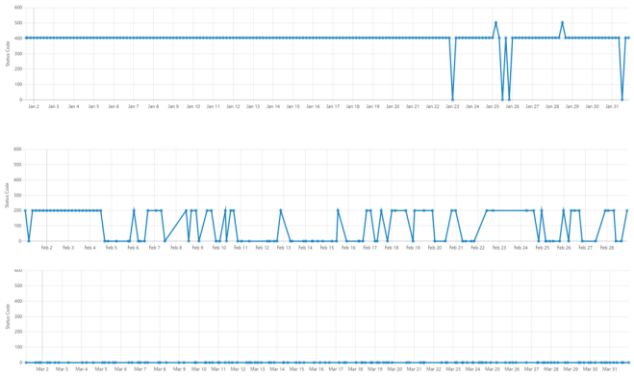

図 7　ステータスコードの変化(上から 1 月，2 月，3 月)

5.3 考察

公的機関から配信された不正接続先を対象に Ping ならびに HTTP レスポンスを継続的に観測した結果，長期に渡って，稼働や停止を繰り返す事例があることを確認した．このことから，提案システムを用いて不正接続先を継続的に観測し，結果を共有することにより，観測対象の活性度の経過や兆候を観察しつつ拒否リストへの継続追加・削除を利用できると考える．また，同様の不正接続先を受信した組織が協力するという提案システムの考え方は，観測に伴う負荷軽減を図るという点で有効である．

ただし, 提案システムは, あくまでも Ping ならびに HTTP レスポンスの観測に留まる．不正接続先がサイバー攻撃において脅威が残存しているかを判断するためには，提案システムが実装している観測項目以外についても観測あるい

は調査が必要である．

5.3.1 提案システムの課題

(1) 複数観測点のサポート

5.2 節で実施した観測の結果より，Ping と HTTP レスポンスの継続的観測及び可視化による不正接続先の稼働状況の把握において，提案システムの有効性を確かめた．他方，観測期間中に提案システムで使用した観測用端末数は，1 台であったことから，観測結果の不明点を明らかにできなかったこともある．この点は，観測用端末を複数とすることにより解決できる可能性がある．

(2) 観測記録の共有

観測記録の共有には，クラウドストレージの Box を使用した．観測記録のダウンロードは，Box が提供するディレクトリ同期機能である Box Sync を用いることもでき利便性向上も可能であるが，クラウドストレージだからこその利点を検討していく必要がある．

(3) 観測対象としての不正接続先情報

観測対象として不正接続先情報としては， IP アドレス，ドメイン名，URL がある．同一の不正接続先であっても，IP アドレス，ドメイン名，URL のいずれで確認するかによって，応答が異なる可能性があり，結果として観測記録の信ぴょう性低下につながる恐れがある．例えば，ドメイン名や URL の記載がある場合には名前解決の結果に得た IP アドレスに対し Ping 送信するなどが考えられるが，一方で，ドメイン名の使用状況の把握として観測を続ける有意性も見いだすことが出来るため，観測対象としての不正接続先情報については引き続き検討していく必要がある．

6. おわりに

本稿では，不正接続先を対象に継続的な観測を実施し，複数観測点での記録を共有することにより攻撃活動の把握を支援する相互協力型の継続的観測システムについて述べた．また，同システムを構成する自律した不正接続先観測，観測記録の共有，観測記録の可視化のそれぞれについて実装方式を示した．

提案システムを用いた観測では，公的機関から配信された不正接続先を対象に Ping ならびに HTTP レスポンスを観測し，同記録を可視化ダッシュボードで分析することによって各攻撃活動に割り振った脅威情報識別番号に属する不正接続先の状態把握を検証した．その結果，公的機関から配信された不正接続先の中には，長期に渡って，稼働や停止を繰り返す事例があることを確認した．

今後は複数観測点による継続的観測など提案システムの課題解決に取り組んでいく．また，観測記録の共有については，観測記録の形式を ICT-ISAC Japan が使用している JSON 形式の STIX 拡張記述仕様である JSON 形式に従っている．このため，クラウドストレージの Box 以外に，STIX ファイルとしてまとめ，STIX を配信するための通信規格である TAXII を利用した共有を実施することで，より汎用性の高いデータ流通の可能性を検証したいと考えている．

謝辞

本研究にあたって，有益な助言を頂いた総務省「ソフトウェア脆弱性を狙ったサイバー攻撃の防御に向けた情報共有基盤に関する実証実験」の関係者各位に深く感謝いたします．

参考文献

[1] CISA: Automated Indicator Sharing，https://www.cisa.gov/ais.（参照 2021-08-14）
[2] JPCERT コーディネーションセンター，https://www.jpcert.or.jp （参照 2021-08-14）
[3] 独立行政法人情報処理推進機構，https://www.ipa.go.jp/ (参照 20201-08-14)
[4] 須藤年章：悪性サイトドメインの長期観測結果に基づくブラッ クリスト利用の有効性に関する一考察，コンピュータセキュリティシンポジウム 2013 論文集（CSS 2013），pp. 376－381.（参照 2021-08-14）
[5] 独立行政法人情報推進機構セキュリティセンター: 特定業界を執拗に狙う攻撃キャンペーンの分析~2015 年秋から 2016 年春に見られた攻撃事例~，サイバーレスキュー隊（J-CRAT） 分析レポート 2015，https://www.ipa.go.jp/files/000053445.pdf （参照 2021-08-14）
[6] OASIS Cyber Threat Intelligence Technical Committee，https://oasis-open.github.io/cti-documentation/.（参照 2021-08-14）
[7] Sauerwein, C., Sillaber, C., Mussman, A., and Breu, R.: Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives, In Proceedings of the 13th International Conference on Wirschaftsinformatik （WI2017），St Gallen, S. pp.837-851.（参照 2021-08-14）
[8] ICT-ISAC, https://www.ict-isac.jp/.（参照 2021-08-14）
[9] Zhao, B., Z., H., Ikham, M., Asghar, H., J., Kaafer, M., A., Chaabane, A., and Thilakarathna, K.: A Decade of Mal-Activity Reporting: A Retrospective Analysis of Internet Malicious Activity Blacklists, In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security （AsiaCCS ‘19），pp.1-13.（参照 2021-08-16）