Vol.2022-CSEC-99 No.19
Vol.2022-SPT-49 No.19
Vol.2022-EIP-98 No.19
2022/12/23

相互協力による継続的観測システムを用いた C2 サーバの稼働状況の調査

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：相互協力による継続的観測システムは，公的機関が提供する不正接続先情報を対象に，C2 サーバの状態変化への対処及び観測の運用効率化，そして脅威の把握を目的としたシステムである．通知受領以降における C2 サーバの稼働状況は，これまで調査されることのなかったものである．本研究では，C2 サーバのサイバー攻撃活動ならびに再活性化の把握のため，受領組織間の相互協力を想定した複数観測点での観測を実施している．本稿では，継続的観測システムを用いた公的機関から提供された C2 サーバの稼働状況として，C2 サーバの応答推移を 8 つのタイプに分類すると共に，分類結果に基づき，変化点で確認した事象について調査した結果を報告する．

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

Survey on Activities of C2 Servers with the Mutual Cooperation Continuous Monitoring System

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

Abstract: The Mutual Cooperation Continuous Monitoring System targets C2 server information provided by public agencies for the efficiency of the handling of activity changes on C2 servers and monitoring, and to improve awareness on their threats. The situations of C2 servers after the receipt of notification has never been investigated before. In this study, to use for cyberattacks of C2 servers and notice the reactivation of them, we have been conducting the monitoring with multiple monitor agents, assuming the mutual collaboration among notified organizations. In this paper, we report the situations of C2 servers using the continuous monitoring system. The result shows that the activity progress patterns of C2 servers provided by public agencies can be classified into eight types, and we analyze the events that occur at the change points based on the classification results.

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った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し，指令を出すための Command and Control サーバ(以下，C2 サーバ)が用いられる．攻撃者は C2 サーバを短期間のみ稼働させ使い捨てる場合や，長期的な利用のためドメインの変更や攻撃活動に合わせた停止と再開を繰り返す場合がある[1]．C2 サーバに関する不正接続先情報(以降，不正接続先情報)の活用については，2015 年に開始した米国土安全保障省による Automated Indicator Sharing(AIS)をはじめとする官民協調型の脅威情報共有として推進されている[2]．国内においても JPCERT/CC[3]や IPA[4]などが脅威情報共有のハブ組織として活動しており，不正接続先情報を関連組織に通知している．

その一方で，不正接続先情報として通知された C2 サーバの稼働状況の把握は受領組織がそれぞれ独自に取り組んでおり，組織間の連携のための基盤は整備されていないのが現状である．通知受領後における C2 サーバの稼働状況は，稼働中はサイバー攻撃活動，活動停止時は再活性化の把握のため，継続的に観測することが望ましい．

本研究では，公的機関が提供する不正接続先情報を対象に，活動状況把握のため，相互協力による継続的観測システム(以下，継続的観測システム)を運用している[5][6]．継続的観測システムでは受領組織間での相互協力を想定し，複数観測点での継続的観測を実施している．

本稿では，公的機関から提供された不正接続先情報(2020 年 10 月～2022 年 5 月，計 82 件)を対象に，継続的観測システムを用いた観測結果(2021 年 12 月～2022 年 7 月)について報告する．

2. 関連研究

関連研究では，不正接続先情報への対処という点で，SOC(Security Operation Center)や CSIRT(Computer Security Incident Response Team)などのセキュリティチームにおける脅威把握，不正接続先に関する情報収集についてまとめる．

†1 東京電機大学
Tokyo Denki University
2 (株)日立製作所
Hitachi Ltd.

Vol.2022-CSEC-99 No.19
Vol.2022-SPT-49 No.19
Vol.2022-EIP-98 No.19
2022/12/23

2.1 脅威把握のための情報収集

脅威把握のための情報収集としては，攻撃検知時の対応判断への活用と，インシデントの事前・事後対応への活用の 2 つの視点がある．

(1) 攻撃検知のための情報収集

攻撃検知に関する情報収集の目的は，主に検知精度の向上とアラート調査の 2 つがある．文献[7]では，複数の IDS 運用による広域監視の課題として各監視地点のログ形式の不一致やログの過剰出力などを挙げ，送信元/宛先ポート・IP アドレス・国名コードや各イベントの出現回数を用いた長期的なイベント傾向と短期的なイベント傾向の変化度から検知精度を向上させている．出力されたアラートに対しては，対応可否判断が必要であることから，文献[8]では，対応判断のための OSINT 調査において 6 名のセキュリティ有識者のブラウジングデータを収集し，全員に共通する判断基準として検知ファイル名・通信先のレピュテーションや攻撃対象となっている脆弱性情報があることを報告している．文献[9]では，CDN やパブリッククラウドといった外部サービスの利用により攻撃の全体像の把握や攻撃元 IP アドレスの調査といった情報収集に時間が掛かる課題を挙げ，攻撃検知・影響分析・対応までの時間短縮の一案として SOC のインハウス化を挙げている．

(2) インシデント対応のための情報収集

インシデントの事前対応となる平時の情報収集では，攻撃の特徴や流行，手法の変化といった情報が重要である．文献[10][11]では，過去から現在までの攻撃の変化や不正接続先・不正ファイルなどの利用状況など，経緯も含めた情報を共有する仕組みを提案している．インシデントの事後対応となる有事の情報収集では，被害極小化のための情報が重要である．文献[12]では，当該インシデントへの対応ベストプラクティス情報や関連不正接続先情報など，緊急対応時に即効性のある情報を共有する仕組みを提案している．

2.2 不正接続先に関する情報収集

不正接続先の情報収集に関しては，インディケータの関連情報から不正接続先である C2 サーバを特定する間接的な方法と，ネットワーク上の不審な振る舞いから特定する直接的な手法がある．

(3) インディケータの関連情報を用いた特定

文献[13]では，VirusTotal から調査対象のサブドメインや IP アドレスを取得して不正ドメインを特定する手法，文献[14]では，WHOIS をはじめとする攻撃者に察知されにくい情報から C2 サーバを特定する手法を提案している．

(4) ネットワーク上の不審な振る舞いを用いた特定

文献[15]では，攻撃の実施時刻前後で不正ドメインの DNS 登録状況の振る舞いにパターンがあることを報告している．文献[16]では，マルウェアの動的解析による不正通信を分析し，TCP 通信や通信内容の文字列，URL，DNS リクエストの 4 点から特定のマルウェアファミリーに関連する C2 サーバの特徴を報告している．

3. C2 サーバの稼働状況の調査

本章では，公的機関から提供された不正接続先情報(2020 年 10 月～2022 年 5 月，計 82 件)を対象に，継続的観測システムを用いて取得した応答記録から，C2 サーバの稼働状況について報告する．

3.1 相互協力による継続的観測システム

継続的観測システムは，公的機関が提供する不正接続先情報の C2 サーバに対し，ping と HTTP リクエストを送信し，そのレスポンスを記録・共有することで稼働状況を把握する．また，相互協力体制により複数観測点での継続的観測を行い，各不正接続先情報に付与される脅威情報識別番号を使用した稼働状況の可視化機能により，関連組織との迅速な共有を可能にする．継続的観測システムの概要を図 1 に示す．

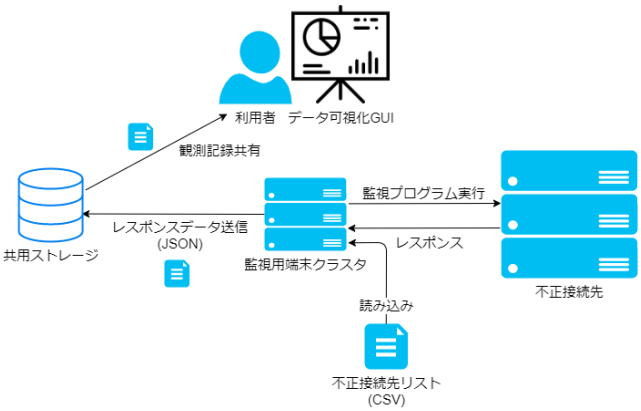

図 1：相互協力による継続的観測システム

3.2 調査概要

本調査は，2020 年 10 月から 2022 年 5 月にかけて公的機関から提供された不正接続先情報を対象に，継続的観測システムを用いて観測(2021 年 12 月～2022 年 7 月)した結果に基づく．

(1) 観測対象

公的機関から提供された不正接続先情報は，脅威情報識別番号(本稿では A～Q に置き換え)が計 17 件付与されており，計 82 件の C2 サーバを含む．また，不正接続先情報のうち，一連のサイバー攻撃に関する情報については，提供された情報に基づき脅威グループとしてグルーピングした(表 1).

(2) 観測点

相互協力による継続的観測システムの観測点は，2 組織で運用しており，クラウド環境 12 ヵ所，国内に設置したオンプレミス環境 2 ヵ所，計 14 カ所である(表 2).

Vol.2022-CSEC-99 No.19
Vol.2022-SPT-49 No.19
Vol.2022-EIP-98 No.19
2022/12/23

表 1：観測対象及び観測期間

#	脅威グループ	C2 ｻｰﾊﾞ件数	通知年月	観測期間
A	ｸﾞﾙｰﾌﾟ AB	12	2020/10	2021/12～2022/07
B		8	2020/10	2021/12～2022/07
C	ｸﾞﾙｰﾌﾟ CD	8	2020/10	2021/12～2022/07
D		6	2020/10	2021/12～2022/07
E	ｸﾞﾙｰﾌﾟ EFGH	2	2020/12	2021/12～2022/07
F		2	2021/01	2021/12～2022/07
G		1	2021/02	2021/12～2022/07
H		1	2021/03	2021/12～2022/07
I	未分類	1	2021/06	2021/12～2022/07
J	未分類	12	2021/08	2021/12～2022/07
K	ｸﾞﾙｰﾌﾟ KO	2	2021/09	2021/12～2022/07
L	未分類	1	2021/10	2021/12～2022/07
M	未分類	3	2022/03	2022/05～2022/07
N	未分類	7	2022/03	2022/05～2022/07
O	ｸﾞﾙｰﾌﾟ KO	3	2022/03	2022/05～2022/07
P	未分類	10	2022/04	2022/07
Q	未分類	3	2022/05	2022/07

表 2：観測点一覧

#	設置地域	ﾌﾟﾗｯﾄﾌｫｰﾑ
1	米国西部(カリフォルニア)	AWS
2	米国東部(バージニア北部)	AWS
3	欧州(フランクフルト)	AWS
4	欧州(ロンドン)	AWS
5	欧州(ミラノ)	AWS
6	中東(バーレーン)	AWS
7	南米(サンパウロ)	AWS
8	アジアパシフィック(香港)	AWS
9	アジアパシフィック(ムンバイ)	AWS
10	アジアパシフィック(シンガポール)	AWS
11	アジアパシフィック(シドニー)	AWS
12	アジアパシフィック(東京)	AWS
13	日本 A	オンプレミス
14	日本 B	オンプレミス

(3) 調査内容

本調査では，公的機関から提供された不正接続先情報を対象に，継続的観測システムを用いて観測した結果を，次の 3 つの視点からまとめる．

- 時間軸から見た C2 サーバの稼働状況
- 複数観測点から見た C2 サーバの稼働状況
- 脅威情報識別番号ならびに脅威グループから見た C2 サーバの稼働状況

4. 調査結果

4.1 時間軸から見た稼働状況

時間軸から見た C2 サーバの稼働状況では，HTTP 応答，ping 応答の推移を示す．

4.1.1 HTTP 応答から見た稼動状況

HTTP 応答から見た稼動状況の一例として，観測点#14 における脅威情報識別番号 A～Q を対象とした C2 サーバの HTTP ステータスコードの応答推移を図 2 に示す．なお，脅威情報識別番号の不正接続先情報として C2 サーバが複数報告されている場合には，うち 1 つのみを記載し，グラフ縦軸には，応答なしを 0，応答ありを 1XX，2XX，3XX，4XX，5XX としてステータスコードをプロットした．

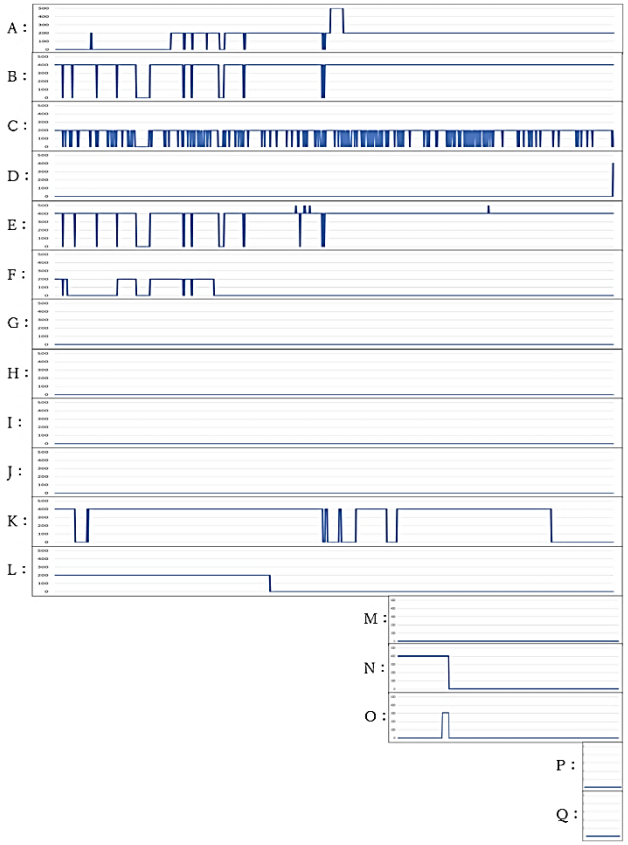

図 2：観測点#14 における HTTP の応答推移

図 2 **エラー! 参照元が見つかりません。**に示す通り，C2 サーバの HTTP ステータスコードの応答推移は C2 サーバ毎に異なる．そこで，本節では，HTTP ステータスコードの応答推移を概観するために，応答推移を大分類として 3 種，小分類として 8 種のタイプに分類した．分類結果を表 3 に示す．

表 3：HTTP 応答推移のタイプ分類

大分類	小分類	概要
応答なし	タイプ 1	応答しない
1 種類のステータスコードを応答	タイプ 2	2XX を継続的に応答
	タイプ 3	3XX を継続的に応答
	タイプ 4	4XX を継続的に応答
	タイプ 5	5XX を継続的に応答
複数のステータスコードを応答	タイプ 6	ある時点から継続的に応答する内容が変化
	タイプ 7	各観測点で継続的に応答する内容が異なる
	タイプ 8	複数の応答内容を短周期で行き来する

応答推移のタイプの概要は，次の通りである．なお，応答推移のタイプ分類は，観測期間全体の特徴を元に目視で

Vol.2022-CSEC-99 No.19
Vol.2022-SPT-49 No.19
Vol.2022-EIP-98 No.19
2022/12/23

分類した．例えば，図 4 の場合，各観測点の応答推移グラフで部分的に値が 0(応答なし)になっているが，観測期間全体で 4XX を継続していることから，タイプ 4 と分類した．図 5 の場合，図中の破線時点で応答推移が変化したことが特徴であり，タイプ 6 に分類した．

(1) 応答なし

観測期間内で応答しない状態が継続的に続いている場合で，この応答推移をタイプ 1 とした．図 3 にタイプ 1 に分類した C2 サーバの応答推移の例を示す．

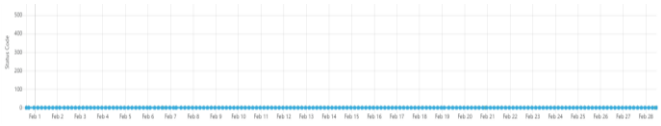

図 3：タイプ 1 の応答推移の例(観測点 1 カ所)

(2) 1 種類のステータスコードを応答

観測期間内で 1 種類の HTTP ステータスコードを継続して応答する場合である．この応答推移では，ステータスコードの 1 桁目が持つ意味ごとに 4 種類(2XX，3XX，4XX，5XX)に分類できるため，それぞれタイプ 2～5 とした．図 4 に，タイプ 4 に分類した C2 サーバの観測点 3 カ所の応答推移の例を示す．

図 4：タイプ 4 の応答推移の例(観測点 3 カ所)

(3) 複数のステータスコードを応答

ある時点から継続的に応答する内容が変化する応答推移をタイプ 6 とした．タイプ 6 に分類した図 5 の場合，観測点 3 カ所すべてにおいて，図中の破線時点で継続的に応答する内容が変化している．

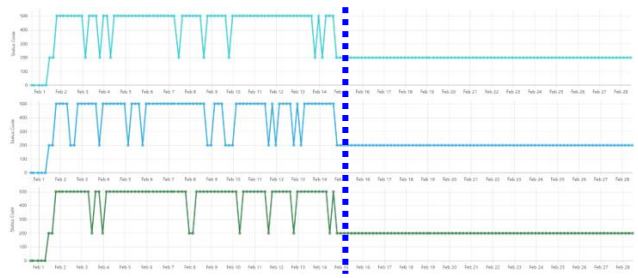

図 5：タイプ 6 の応答推移の例(観測点 3 カ所)

観測点によって応答推移が異なる場合をタイプ 7 とした．タイプ 7 に分類した図 6 の場合，上段の観測点はタイプ 4，下段の観測点はタイプ 1 の応答推移である．

図 6：タイプ 7 の応答推移の例(観測点 2 カ所)

観測点によって応答推移が異なり，さらに，複数の応答推移の変動が多数見受けられる場合をタイプ 8 とした．タイプ 8 に分類した図 7 の場合，観測点 6 カ所の応答推移が異なり，さらに，応答のないタイプ 1 と 2XX を応答するタイプ 2 を繰り返している．なお，本調査で観測したタイプ 8 の場合，応答推移に周期性は見られなかった．

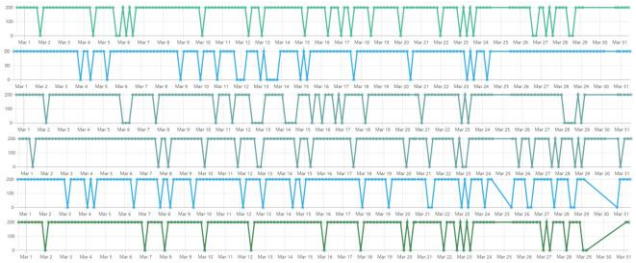

図 7：タイプ 8 の応答推移の例(観測点 6 カ所)

計 82 件の C2 サーバの応答推移をタイプ分類した結果を表 4 に示す．なお，C2 サーバによっては，複数の応答推移タイプが混在している場合もあることから，該当するタイプをすべて 1 件としてカウントしている．

表 4：C2 サーバの応答推移タイプ別件数

応答推移タイプ	C2 サーバ件数
タイプ 1	50
タイプ 2	3
タイプ 3	0
タイプ 4	10
タイプ 5	1
タイプ 6	17
タイプ 7	3
タイプ 8	2

4.1.2 ping 応答から見た稼動状況

ping 応答から見た稼動状況については，C2 サーバの HTTP ステータスコードの応答変化と異なる時期に ping の応答変化が発生した場合を対象に調査した結果を示す．

ping の応答変化において，損失率の増減を変化点とした場合，HTTP 応答のないタイプ 1，ある時点から継続的に応答する内容が変化するタイプ 6 で最も変化点件数を観測し

Vol.2022-CSEC-99 No.19
Vol.2022-SPT-49 No.19
Vol.2022-EIP-98 No.19
2022/12/23

ている．表 5 に HTTP ステータスコードの応答変化と異なる時期に ping の応答変化が発生した件数を示す．

表 5：ping/HTTP 応答変化が異なる時期に発生した件数

ping の応答変化	C2 サーバ件数		HTTP の応答変化と時期が異なる件数
損失率：100→0%	タイプ 1	6	6
	タイプ 4	1	
	タイプ 6	4	
	タイプ 7	1	
	タイプ 1/8	1	1
損失率：0→100%	タイプ 1	8	8
	タイプ 4	1	
	タイプ 6	6	1
	タイプ 6/7	1	1
	タイプ 7	1	
	タイプ 8	1	1

このうち, [ping 応答なし→あり, HTTP 応答なし→あり], [HTTP 応答あり→なし, ping 応答あり→なし]の場合について，観測した状況を表 6，表 7 に示す．表 6 の C2 サーバは，応答推移タイプ 1 と 8 に該当し，[ping 応答なし→あり]の 5 日後に[HTTP 応答なし→あり]の変化が見られた事例である．表 7 の C2 サーバは，応答推移タイプ 6 と 7 に該当し, [HTTP 応答あり→なし]から 1 ヵ月以上経過してから[ping 応答あり→なし]の変化が見られた事例である．いずれも，ping というネットワークレベルの稼働状況と，HTTP というアプリケーションレベルの稼働状況には，ズレが発生する事例があることを確認した．

表 6：ping 応答なし→あり，HTTP 応答なし→あり

応答推移タイプ	ping の変化時期 応答なし→あり	HTTP の変化時期 応答なし→あり
タイプ 1-1/8-1	2022 年 1 月 14 日	2022 年 1 月 19 日

表 7：HTTP 応答あり→なし，ping 応答あり→なし

応答推移タイプ	ping の変化時期 応答あり→なし	HTTP の変化時期 応答あり→なし
タイプ 6-1	2022 年 7 月 2 日	2022 年 5 月 31 日
タイプ 6-2/7-1	2022 年 5 月 4 日	2022 年 3 月 23 日
タイプ 8-1	2022 年 5 月 16 日	変化なし

4.2 複数観測点から見た稼働状況

複数観測点から見た C2 サーバの稼働状況では, HTTP ステータスコードの応答変化点で観測されたリダイレクトと，クローキングと推定される事例について報告する．

(1) リダイレクト

ある時点から継続的に応答する内容が変化するタイプ 6 を対象に，計 17 件の C2 サーバの応答変化の概況をまとめた(表 8)．表 8 において A-1 の枝番は，脅威情報識別番号 A に属する C2 サーバのひとつであることを示す．

計 17 件のうち，3 件の C2 サーバにおいてリダイレクト設定されていることを確認した．表 9 に，VirusTotal において，リダイレクト先を不正と判定した件数を示す．ただし，表 9 に示す通り，不正と判定した件数は低く，全て正規サイトであった．

リダイレクトの具体的な事象として, C2 サーバ B-2 については，アクセス先が別サイト(リファラ：Referrer)から到達した際，リファラ情報を削除するサービスであるデリファラ(De-Referrer)を介してオーストラリアのサービスサイトにリダイレクトされていた(図 8)．

表 8：タイプ 6 に分類した C2 サーバの応答変化の概況

C2 ｻｰﾊﾞ	変化日付	変化前	変化後
A-1	2021/12/26	応答なし	200
	2021/12/27	200	応答なし
	2022/2/1	応答なし	200/500 を交互に応答
	2022/2/15	200/500 を交互に応答	200
	2022/4/3	200	500
	2022/4/7	500	200
A-2	2021/12/29	404(8 観測点)	応答なし(8 観測点)
	2022/3/23	404(6 観測点)	応答なし(6 観測点)
A-3	2022/1/2	200	400
	2022/5/4	400	200
B-1	2022/3/11	応答なし	400
B-2	2022/1/19	応答なし	200
	2022/1/23	200	応答なし
B-3	2022/2/22	応答なし	200
	2022/3/22	200	応答なし
D-1	2022/7/15	応答なし	400
F-1	2021/12/13	200	応答なし
	2022/1/6	応答なし	200
	2022/2/18	200	応答なし
K-1	2022/2/28	応答なし	200(7 観測点)/ 404(7 観測点)
	2022/3/3	404(7 観測点)	応答なし
	2022/6/23	200(7 観測点)	応答なし
K-2	2022/3/10	200	応答なし
L-1	2022/3/31	応答なし	応答なし/ 400 を交互に応答
	2022/4/27	応答なし/400 を交互に応答	400
	2022/6/22	400	応答なし
N-1	2022/5/25	400	応答なし
N-2	2022/5/25	400	応答なし
N-3	2022/5/25	400	応答なし
O-1	2022/5/25	400	応答なし
O-2	2022/5/25	400	応答なし
O-3	2022/5/23	応答なし	307
	2022/5/25	307	応答なし

表 9：VirusTotal におけるリダイレクト先の評価

C2 サーバ	不正と判定した件数
A-1	0
B-2	1
B-3	0

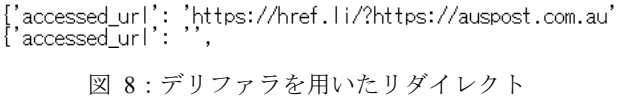

図 8：デリファラを用いたリダイレクト

(2) クローキング

観測点によって応答推移が異なるタイプ 7 を対象に，観

Vol.2022-CSEC-99 No.19
Vol.2022-SPT-49 No.19
Vol.2022-EIP-98 No.19
2022/12/23

測できた応答推移の事象を表 10 にまとめた．観測点によって応答推移が異なることが，C2 サーバの不正な活動に直結するものではないが，3 件の C2 サーバにおいてクローキングと推定される活動を確認した．

表 10：クローキングと推定される事例

C2 サーバ	応答推移の概要
A-2	全観測点で 404 を応答し，その後，観測点 8 カ所，観測点 6 カ所が段階的に応答停止
C-1	観測点 1 カ所のみ 403 を応答し，他の観測点 13 カ所は応答なし
K-1	応答なしの状態から，観測点 7 カ所が 200，残り観測点 7 カ所が 404 を応答するように変化

4.3 脅威情報識別番号ならびに脅威グループから見た稼働状況

脅威情報識別番号ならびに脅威グループから見た C2 サーバの稼働状況については，脅威情報識別番号ならびに脅威グループあたりの月別平均 HTTP レスポンス数で示す(図 9, 図 10). なお，月別平均 HTTP レスポンス数については，脅威情報識別番号ならびに脅威グループ毎に，すべての C2 サーバの応答有無を積算し，さらに属する C2 サーバ数と複数ある観測点からの応答差異を加味することで均等化している．いずれの場合も，観測期間においては大きな変動はなかった．

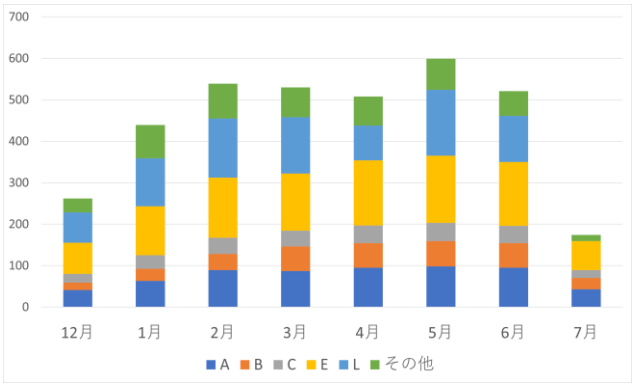

図 9：脅威情報識別番号あたりの
月別平均 HTTP レスポンス数

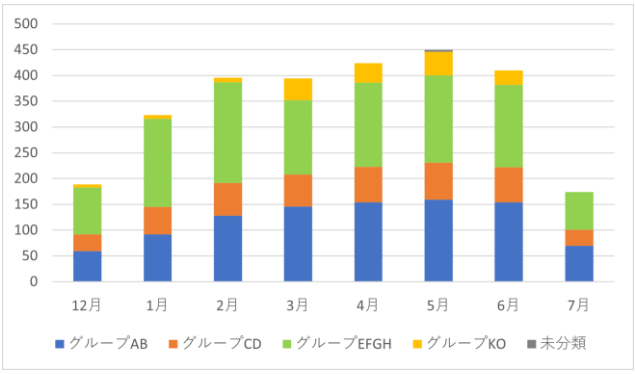

図 10：脅威グループあたりの
月別平均 HTTP レスポンス数

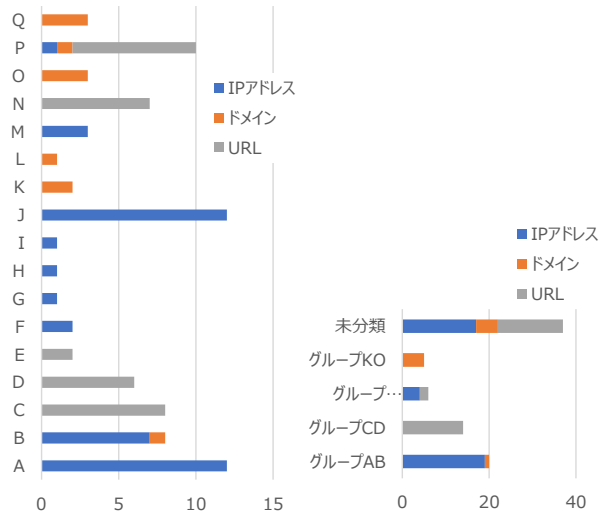

図 11：脅威情報識別番号ならびに脅威グループ毎に
登録されているインディケータ種別件数

4.4 考察

今回の調査結果に基づき，C2 サーバの稼働状況を把握するためのポイントを，時間軸，複数観測点，脅威情報識別番号ならびに脅威グループの 3 つの視点から考察する．

(1) 時間軸の視点

時間軸の視点で C2 サーバの活動状況を把握する際には，HTTP ステータスコードを元に C2 サーバの応答推移を分類し，そのタイプ毎に，次に示す点に着目すると良い．なお，1 種類のステータスコードを応答するタイプ 2～5 の場合には，ステータスコードと ping 損失率共にほぼ変化が見られなかったことから，HTTP レスポンスのボディに着目する必要がある．ただし，HTTP レスポンスのボディを対象とした調査は，今回の調査でカバーできなかったことから，今後の課題である．

- 応答しない状態が継続的に続くタイプ 1 の場合には，ネットワークレベルでの変化を示す ping 損失率
- 複数のステータスコードを応答するタイプ 6~8 の場合には，ステータスコードの変化

(2) 複数観測点の視点

複数観測点の視点では，図 12 のように，観測点の応答記録の欠落が発生した場合にもカバーができるため，月別平均 HTTP レスポンス数のように，脅威情報識別番号ならびに脅威グループ毎に C2 サーバの稼働率のような定量化をする際に有効である．さらに，今回の観測結果から，各観測点の応答を比較することにより C2 サーバのクローキングに関する活動を把握できる可能性があることを示した．

Vol.2022-CSEC-99 No.19
Vol.2022-SPT-49 No.19
Vol.2022-EIP-98 No.19
2022/12/23

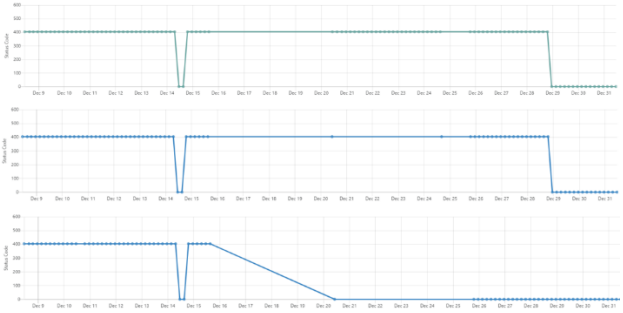

図 12：HTTP レスポンス欠落の例(観測点 3 カ所)

(3) 脅威情報識別番号ならびに脅威グループの視点

脅威情報識別番号ならびに脅威グループの視点では，登録されているインディケータ種別件数(図 12)との関係性を確認してみたが，インディケータ種別やその件数による影響は見受けられないことから，時間軸の視点で変化点を捉えつつ，DNS による名前解決有無，WHOIS に登録されている情報精査，HTTP レスポンスのボディの精査が必要になると考えている．

5. おわりに

本稿では，公的機関が提供する不正接続先情報について，これまで不明だった通知受領以降の稼働状況を報告した．

時間軸の視点では，ping 損失率や HTTP ステータスコードなど, C2 サーバの応答推移に合わせて変化点を捉えたほか, C2 サーバの稼働状況把握のひとつとしてリダイレクトの実例を示した．

複数観測点の視点では，応答記録の欠落が発生した場合にもカバーができるため，応答記録を使った定量化や，C2 サーバの稼働状況のひとつとしてクローキングと推定される実例を示した．

今後の課題は，1 種類のステータスコードを応答するタイプ 2～5 の場合についての追加調査，C2 サーバの不正活動有無の特定，不正接続先情報に付与される脅威情報識別番号を使用した稼働状況の可視化機能による関連組織との迅速な共有の実施などである．

参考文献

[1] ZDNet:カスペルスキー，日本を狙うサイバー攻撃を報告-米国政府の対応にも見解，入手先〈https://japan.zdnet.com/article/35111882/〉(参照 2022-11-14).
[2] CISA: Automated Indicator Sharing，入手先〈https://www.cisa.gov/ais〉(参照 2022-11-14).
[3] JPCERT コーディネーションセンター，入手先〈https://www.jpcert.or.jp〉(参照 2022-11-14).
[4] 独立行政法人情報処理推進機構，入手先〈https://www.ipa.go.jp/〉(参照 2022-11-14).
[5] 堀井大雄ほか：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，コンピュータセキュリティシンポジウム論文集 (2021).
[6] 堀井大雄ほか：C2 サーバを対象とした脅威持続把握のための公開情報の再考，研究報告セキュリティ心理学とトラスト (SPT)，Vol.2022-SPT-48，No.17，pp.1-7 (2022).
[7] 竹森敬祐ほか：Security Operation Center のための IDS ログ分析支援システム，電子情報通信学会論文誌 A，Vol.J87-A，No.6，pp.816-825 (2004).
[8] 鐘本楊ほか：セキュリティオペレーションの効率化に向けた SOC アナリストの共通行動抽出，コンピュータセキュリティシンポジウム論文集，pp.645-652 (2020).
[9] 福本佳成ほか：Security Operation Center 構築とセキュリティ監視運用の取り組み，デジタルプラクティス，Vol.9，No.3，pp.609-619 (2018).
[10] 羽田大樹ほか：CSIRT のための Web ブラックリストの分類の提案，情報処理学会論文誌，Vol.59，No.9，pp.1596-1609 (2018).
[11] 平井達哉ほか：企業における CSIRT の活動とそれを支援する情報共有システム，デジタルプラクティス，Vol.9，No.3，pp.627-642 (2018).
[12] 平井達哉ほか：重要インフラ事業者向けサイバー攻撃関連情報共有システムの提案，コンピュータセキュリティシンポジウム論文集，pp.878-884 (2016).
[13] 田辺瑠偉ほか：統合型マルウェア検査サービス Virus Total を用いた 悪性ドメイン検知手法，情報処理学会論文誌，Vol.59，No.9，pp.1610-1623 (2018).
[14] 久山真宏ほか：攻撃者に察知されにくい情報を用いた C&C サーバの 検知手法の提案と評価，情報処理学会論文誌，Vol.58，No.9，pp.1410-1418 (2017).
[15] S. Hao. et al.: Monitoring the Initial DNS Behavior of Malicious Domains, Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference (IMC '11), Association for Computing Machinery (2011).
[16] G. Bastos. et al.: Identifying and Characterizing Bashlite and Mirai C&C Servers, 2019 IEEE Symposium on Computers and Communications (ISCC), IEEE (2019).