遠隔制御監視システムを模したハニーポットへのアクセス者の挙動の分析

熊谷 拓洋[1,a)]　佐々木 貴之[1]　藤田 彬[2,3]　吉岡 克成[3,4]　松本 勉[3,4]

概要：近年の IoT 機器の普及に伴い，産業分野でも IoT 機器の導入が進められているが，それらへのサイバー攻撃のリスクも増大している．過去には，産業用 IoT 機器を含む遠隔制御監視システムが脆弱な状態で管理・運用されているインフラ施設が存在していることが報告されている．そこで我々は，セキュリティに不備のあるインフラ施設や工場の遠隔制御監視システムへの攻撃の実態を知るため，遠隔制御監視システムを模したハニーポットを，遠隔制御に用いる機器を用いて構築し，運用を行っている．約 2 年間の観測により，遠隔制御監視システムの管理 WebUI に記載された施設に関する情報の量によってアクセス者の挙動が変わることや，杜撰な管理がなされている遠隔制御監視システムの存在を知る手段の一つとしてハッカーフォーラムがあることがわかった．また，管理 WebUI に記載されている認証情報を用いて Telnet にログインしシステム内部を探索する攻撃者や，PLC を発見するためのツールを用いて効率的にアクセスを行うスキャンシステムの存在が確認された．

キーワード：ハニーポット，インフラ施設，遠隔制御監視システム

Analysis of the Behavior of Visitors to Honeypots Imitating a Remote Monitoring and Control System

Takuhiro Kumagai[1,a)]　Takayuki Sasaki[1]　Akira Fujita[2,3]　Katsunari Yoshioka[3,4]
Tsutomu Matsumoto[3,4]

Abstract: With the spread of the Internet of Things (IoT), IoT devices have been leveraged in industrial fields. It has been reported that there are important facilities using insecure remote monitoring and control systems. To observe attacks on such systems, we have constructed and operated honeypots that imitate the remote control and monitoring systems using real devices. Our observations of several years show that the behavior of a visitor changes depending on the amount of information regarding the facilities exhibited in the WebUI of the system. Moreover, we identify that a hacker forum is one of the sources to find the insecure systems. We also observed human-operated multi-stage attacks, in which attackers first access the WebUI, obtain the credential for remote maintenance service, then login to the system using the credentials for further activities. Furthermore, we identify a highly distributed scanning system that conducts well-coordinated Internet-wide scanning while staying under the radar.

Keywords: Honeypot, Infrastructure, Remote Monitoring and Control System

[1] 横浜国立大学大学院環境情報学府
Yokohama National University Graduate School of Environment and Information Sciences
[2] 情報通信研究機構
National Institute of Information and Communications Technology
[3] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University
[4] 横浜国立大学大学院環境情報研究院
Yokohama National University Graduate School of Environment and Information Sciences
[a)] kumagai-takuhiro-hv@ynu.jp

1. はじめに

近年，IoT の普及が急速に進んでおり，様々な場面において IoT 機器が使用されるようになってきている．特に，産業分野における IoT 機器の利用は大きく増加しており，今後もさらなる増加が見込まれている [1]．しかし，産業分野へ IoT 機器が普及する一方では，それらへのサイバー攻撃へのリスクも増大していると言える．過去の総務省の調査によると，セキュリティ関係の設定の不備で，産業用 IoT 機器の管理 Web インターフェース（WebUI）が誰でも閲覧可能な状態で運用されているインフラ施設が存在していることが報告されている [2]．そのようなインフラ施設は典型的に，PLC（Programmable Logic Controller）や SCADA（Supervisory Control and Data Acquisition），DCS（Distributed Control System）などによって構成される産業用制御システム (Industrial Control System, ICS) によって運用され，遠隔制御監視システムによってインターネットを通じた遠隔操作が可能となる．しかし，そのような脆弱な管理がなされている遠隔制御監視システムに対してどのようなアクセスや攻撃が発生するかを詳細に分析した研究は我々の知る限りでは行われていない．

そこで我々は，脆弱な管理下にあるインフラ施設の遠隔制御監視システムを模したハニーポットを提案，運用し，アクセス者の観測と挙動の分析を行ってきた [3]．このハニーポットでは，インフラ施設や工場の遠隔制御監視に実際に使用される PLC やデータロガーを用い，管理 WebUI から水道，電力などの制御パラメータを監視している状況を模擬しており，制御パラメータを操作したり，監視制御機能自体を稼働・停止させることができるようになっている．また，管理 WebUI 上に記載されている認証情報を用いて別の管理チャネルである Telnet を用いたシステムへのアクセスが可能となっており，内部情報の閲覧や操作が可能となっている．

本研究では，自動化されたアクセスよりも，インフラ施設の重要性を理解した上で行われる人の手によるアクセスに着目し，それらの挙動の分析を行う．そのため，本ハニーポットでは大量のアクセスからフルブラウザアクセスと思われるものを抽出するための工夫が施されている．

本論文のコントリビューションは，約 2 年間のハニーポットの運用によって得られた次の 4 つの観測結果である．まず，管理 WebUI に記載されている施設名や機器画像などの情報の量によってアクセス者の挙動に変化が生じ，情報量が多いほど深く探索を行う傾向があることがわかった．次に，このような杜撰な管理がなされている遠隔制御監視システムを知る手段の一つとして海外のハッカーフォーラムがあることがわかり，フォーラムに投稿されたある一つのスレッドによって，人の手によって行われたと思われるアクセスが大幅に増加したことが確認された．3 つ目に，管理 WebUI に記載されている認証情報を用いて Telnet にアクセスしシステム内部を実際に探索する攻撃者が観測された．最後に，ハニーポット内の PLC に対する通信の分析から，機器を見つけるためのスキャンを海外のクラウドサービスから非常に効率化されて行われていることが確認された．

以降では，2 章で関連研究について述べ，3 章では本研究に用いたハニーポットの構成について述べる．4 章ではハニーポットの分析結果とそれに対する考察を述べ，最後に，5 章ではまとめと今後の課題について述べる．

2. 関連研究

IoT や ICS のセキュリティに関する調査は世界で幅広く行われている．論文 [4] では 5 つの産業用プロトコルを対象に IPv4 空間をスキャンし，インターネット上に公開されている ICS についての調査を行っている．論文 [5] では国内の IoT 機器に対してスキャンを行い，様々な IoT 機器が外部からアクセス可能になっていることや，重要施設の遠隔制御監視システムが誰でも閲覧可能な状態で公開されていたことを報告している．また，インターネット上に公開されているネットワーク機器を探索し，ポートの開放状況や機器の脆弱性などを提供するサービスが存在する．代表例として，Censys[6]，Shodan[7]，Zoomeye[8] などが挙げられ，これらは Web や API を通じて誰でもサービスを利用することができるが，悪用防止のため，無料の範囲内では機能に制限がかけられていることが多い．

IoT や ICS に着目したハニーポットは数多く提唱されている．論文 [9] では，様々な CPU アーキテクチャで動作する IoT 機器を模擬するハニーポットを構築し Telnet による攻撃の分析を行っている．SCADA HoneyNet Project[12] は SCADA などの産業用ネットワークをシミュレートするハニーポットの構築を Honeyd[13] 上で行うことを目的としている． Conpot[10] は ICS を模した低対話型のオープンソースハニーポットである．論文 [11] は，Conpot をベースとしており ICS 基盤全体を模擬することによって攻撃者をより惹きつけることのできるハニーポットを提唱している．

また，攻撃者の人間的な側面に着目した ICS ハニーポットの研究も行われている．論文 [14] では，ICS のネットワーク内にハニーポット（CamouflageNet）を設置し，スキャンを受けた際に自らの設定を変更させることにより，攻撃にかかるリソースを増大させる方法を提案している．論文 [15] では，侵入後のシステムの特性が攻撃者にどのような影響を与えるかを検証しており，ハニーポットの場所，侵入の難易度，ファイルの数などを変えることによる攻撃者の行動の変化を分析している．論文 [16] では，RATs（Remote Access Trojans）の一つである DarkComet が動

作するハニーポットを設置し，DarkComet のオペレータの行動を理解することに焦点をおいた調査を行っている．論文 [3] では，インフラ施設の遠隔制御監視システムを模したハニーポットを提案し，アクセスの特徴を主成分分析をすることによって，「調査性」「探究性」「攻撃性」という 3 軸でアクセス者の特徴をある程度説明し得ることを示している．

本研究は ICS のハニーポットを対象としているが，特に人間の手による攻撃に着目しており，施設名や設置場所を記載したりすることによって攻撃者の興味を惹いたり，遠隔制御監視システムに侵入した際の攻撃者の挙動の分析を行うことができる．

3. 遠隔制御監視システムを模したハニーポット

3.1 概要

遠隔制御監視システムとは，電力施設や治水施設といった重要インフラや工場などを遠隔で制御するためのシステムであり，典型的にはセンサやアクチュエータに接続して制御を行う PLC などの制御機器と，それらの稼働状況を外部から監視・記録し必要な制御を行うデータロガーなどの監視制御機器によって構成される．管理者は，データロガーを通じて遠隔からシステムの稼働状況を確認し運用を行う．一般的には閉域網で利用され，外部からの接続は行えないようになっているが，実態としてルータのポートフォワーディング設定により，外部ネットワークからデータロガーにアクセスできるように運用されている場合がある．本研究では，ネットワークを誤って設定してしまい，外部に公開されてしまった遠隔制御監視システムを模擬するハニーポットを構築し，それに対するアクセスを分析する．

我々が構築を行ったハニーポットでは，内閣サイバーセキュリティセンターが重要インフラとして指定した「情報通信」,「金融」,「航空」,「空港」,「鉄道」,「電力」,「ガス」,「政府・行政サービス」,「医療」,「水道」,「物流」,「化学」,「クレジット」,「石油」の 14 分野の施設をそれぞれ 2 施設ずつと，重要インフラではないものの人々の日常生活において重要な役割を持つ 2 施設，合計 30 施設の電力と水道の管理を行っている状況を模擬している．

本研究においては人間の手によるアクセスに着目しているため，コンピュータによって自動化されたアクセスを対象とするハニーポットとは重視する点が大きく異なり，人間の興味を刺激したり，対話，追跡を行う機能やコンテンツが必要となる．次節に，攻撃者の誘引，対話，追跡を行うために実装した要素について説明する．

3.2 システム構成

本研究で用いたハニーポットの構成を図 1 に示す．この

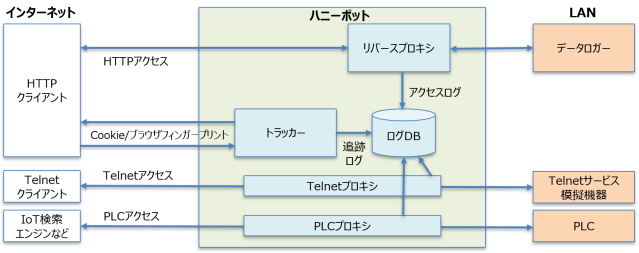

図 1 ハニーポットの構成

Fig. 1 Architecture of honeypot

ハニーポットでは，以下の 3 つの機能が備わっている．

- **誘引**：検索エンジンなどを経由してくる訪問者を惹きつけるため実機の PLC を使用し，プロキシを通じてスキャンに応答する．また，リバースプロキシを用いて割り当てられた IP ごとに管理 WebUI のコンテンツを生成する．
- **対話**：データロガーの管理 WebUI を通じて施設の制御項目が操作可能であり，攻撃者の操作に応じて変化するシミュレータが設置されている．また，Telnet へのアクセスに対応している．
- **追跡**：Cookie とブラウザフィンガープリントを用いて攻撃者を追跡する．

以降では，各構成要素について説明する．

データロガー

データロガーでは管理 WebUI（80/tcp）が動作しており，HTTP 通信は上流のマシンのリバースプロキシによってデータロガーへ転送される．管理 WebUI 上では，インフラ施設の水道や電力を監視している状況を模擬しており，実運用されているシステムを参考に施設名/現在時刻の表示，制御項目（ON/OFF ボタン，リセットボタン，設定値変更フォーム），そしてイベントの表示を実装した．

リバースプロキシ

本研究に用いるハニーポットには複数のグローバル IP アドレスが割り当てられており，アクセス先によって管理 WebUI の表示コンテンツを変更するためリバースプロキシを実装した．これにより，データロガーの実機を多数用意することなく，ハニーポットに割り当てた複数の IP アドレスでそれぞれ異なる管理 WebUI が表示され，複数の施設を模擬することが可能となる．

トラッカー

管理 WebUI に対して長期間にわたる複数回のアクセスを行った際に，動的アドレス割当などでアクセス元の IP アドレスが変わる可能性がある．本研究においては，ハニーポット側で Cookie とブラウザフィンガープリントを発行することによりアクセス者の追跡を行う．

Telnet サービス模擬機器

管理 WebUI よりも自由度が高い操作が可能な Telnet によるアクセスを観測するため，Telnet サービスを模擬する機器をハニーポット内部に設置した．更に高度な攻撃を行いたい人や，当該システムに興味を惹きつけられた人は，Telnet にもアクセスすると想定される．当該システムにおいては，Telnet サービス模擬用機器として Raspberry Pi を用いた．データロガー同様，Telnet のポート（23/tcp）への通信は上流マシンの Telnet プロキシによって Telnet サービス模擬機器へ転送される．Telnet の認証情報は管理 WebUI 上に記載されており，管理 WebUI を閲覧しなければ推測が困難なものとなっている．Telnet にログインすると，内部ネットワーク内の機器の IP アドレスを記載したテキストファイルが配置されており，さらなる内部探索を行うための情報を得ることができる．

PLC

実運用される ICS を模擬し，インフラ施設に興味を持つアクセス者を誘引するための工夫として，実機の PLC を内部ネットワークに配置した．PLC では，PLC 固有のポートに加えて BACnet や Modbus が動作しており，それらのサービスへの通信はプロキシによって上流マシンから転送される．PLC の存在については，Telnet による内部探索を行うことによって確認することができる．

3.3 WebUI のコンテンツの特徴

3.3.1 管理 WebUI の情報量を変化させたハニーポットの設置

管理 WebUI には施設名やデータロガーの機器画像が掲載されているが，それらの情報がアクセス者の興味にどれだけの影響を与えるかを検証するため，掲載する情報量が異なる 4 種類の管理 WebUI を用意した．すべての情報が掲載されているものを「フルバージョン」，フルバージョンから施設名を取り除いたものを「施設名なし」，施設名なしからさらに機器画像を取り除いたものを「施設名・機器画像なし」，認証画面しか表示されていないものを「認証画面のみ」とする．それぞれの管理 WebUI のスクリーンショットを図 **2** に示す．

3.3.2 認証ダイアログの表示タイミング

実運用されるシステムにおいてはトップページに認証が設けられていることが多く，アクセス者の多くは認証画面を見て諦めてしまうため，アクセス者の分析を行うためのハニーポットにおいてそのような設定は不向きである．そこで，本研究のハニーポットではアクセス事例を増やすためにトップページには認証を設けず，制御項目の変更の際には認証ダイアログが出るよう設定した．なお，実システムにおいても，利便性向上のため，このような方法で認証が設定されている場合がある．認証ダイアログには，どのような文字列を入れても認証が通るよう設定がなされている．

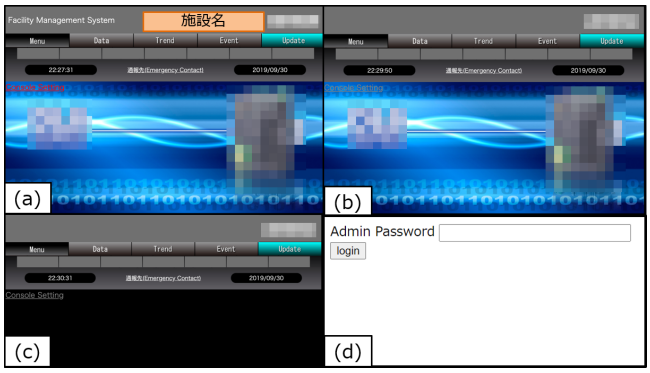

図 2　4 種類の管理 WebUI (a) フルバージョン，(b) 施設名なし，(c) 施設名・機器画像なし，(d) 認証画面のみ

Fig. 2　4 types of WebUI. (a)Full version, (b)No facility name, (c)No facility name & device image, (d)Authentication only.

3.3.3 通知先メールアドレスの表示

このハニーポットへのアクセス者には善意を持った人 (セキュリティ研究者など) と悪意を持った人がいることが想定されるが，善意のアクセス者が通報などの目的で連絡先情報を閲覧する可能性を考慮し，クリックするとメーラーが開かれるリンクを設置した．

4. ハニーポットのアクセス分析と考察

前章で述べたハニーポットを実ネットワーク上で運用し，アクセスの観測と分析を行った．観測期間を以下の表 **1** に示す．なお，(a)〜(d) はそれぞれ，(a) フルバージョン，(b) 施設名なし，(c) 施設名・機器画像なし，(d) 認証画面のみ，を表す．

表 1　ハニーポット観測期間

Table 1　Observation period of honeypot.

ハニーポット	観測期間
(a) No.1 - No.30	2018/08/31 - 2020/02/29
(b) No.31 - No.40	2019/09/10 - 2020/02/29
(c) No.41 - No.50	2019/09/10 - 2020/02/29
(d) No.51 - No.60	2019/09/10 - 2020/02/29

4.1 管理 WebUI への手動アクセスの抽出

ハニーポットの管理 WebUI に関しては，人間の手によって行われた手動によるアクセスを分析の対象とする．今回の分析においては，手動によるアクセスはフルブラウザによって行われるものと考え，以下の特徴を使用した．

- Cookie が有効である
- Javascript が有効である
- favicon.ico に対して GET リクエストを行っている

上記の条件に当てはまるアクセスを抽出した後，Cookie とブラウザフィンガープリントを利用してアクセス者の同定を行う．即ち，別の IP アドレスを用いてアクセスしていたとしても，Cookie やブラウザフィンガープリントが同一であった場合は，同一のホストによるアクセスであるとカウントする．抽出の結果として，フルバージョンのハニーポットに関しては表 1 の観測期間において 233 のユニークホストが手動アクセスと判定された．

4.2 管理 WebUI の情報量によるアクセス者の挙動の分析

前章で述べた 4 種類の異なる管理 WebUI を持つハニーポット 60IP について，以下の 4 つの観点でアクセス者の分析を行った．

- 期間中にアクセスを行ったホストの数
- ハニーポット 1IP 当たりの 1 日のアクセス者数
- 平均コマンド数
- 平均滞在時間

観測結果から上記パラメータを算出し，**表 2** にまとめた．

表 2 管理 WebUI の情報量によるアクセス者の行動の違い
Table 2 Differences in behavior of visitors depending on the amount of information in WebUI

	ホスト数	ハニーポット 1IP 当たりの 1 日のアクセス者数	平均コマンド数（リンククリック数/ホスト数）	平均滞在時間 (秒)
(a)	233	0.043	5.00	445
(b)	69	0.039	4.03	230
(c)	94	0.055	3.43	167
(d)	4	0.015	N/A	5.4

表 2 から，2 つの事が読み取れる．第一に，管理 WebUI に掲載されている情報の量が多いほど，アクセス者のコマンド数や滞在時間が長くなる傾向があることである．つまり，管理 WebUI のコンテンツはアクセス者の興味を引いているものと思われる．第二に，管理 WebUI の情報量はハニーポットへのアクセス者数に大きな影響を与えていないことであるが，その理由として，管理 WebUI にどの程度の情報量が含まれているかは，実際にアクセスしてみないとわからないことが挙げられる．

4.3 海外フォーラムへの掲載による影響の分析

2019 年 12 月 9 日，管理 WebUI 上に掲載されている連絡先情報を通じて，設置中のハニーポット No.3 に関する情報が海外のハッカーフォーラムに投稿されているとの通報をセキュリティベンダから受け取った．その後，匿名の個人から，加えて JPCERT からの通報を受け取った．**表 3** に，ハニーポット No.3 に関するタイムラインを掲示する．

海外フォーラム掲載による影響を調べるため，ハニーポット No.3 のアクセス数の推移を調べた．ハニーポット No.3 の日ごとの新規ホスト数の推移を表したグラフを**図 3** に示す．

表 3 ハニーポット No.3 に関するタイムライン
Table 3 Timeline for Honeypot No.3.

日付	事象
2018/08/31	ハニーポット設置
2019/01/09	個人ブログにハニーポット No.3 に関する情報が掲載される
2019/12/08	海外フォーラムにハニーポット No.3 に関するスレッドが立つ
2019/12/09	セキュリティベンダからの通報
2019/12/10	匿名からの通報
2019/12/17	JPCERT からの通報

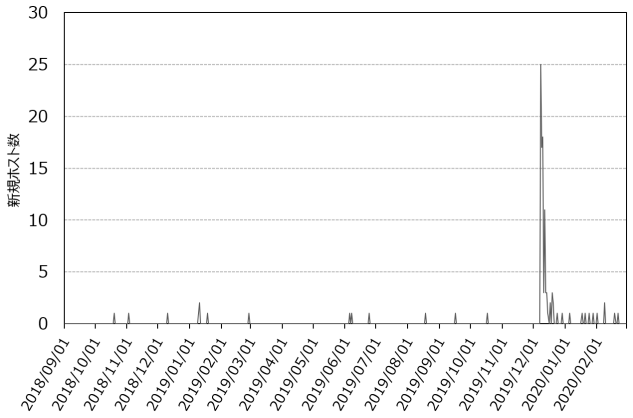

図 3 ハニーポット No.3 の日ごとの新規ホスト数の推移
Fig. 3 Transition of number of new hosts in No.3 honeypot.

2019 年 1 月 9 日に個人ブログにハニーポット No.3 に関する情報が掲載された後，翌日の 2019 年 1 月 10 日には新規ホストが 2 件観測された．また，2019 年 12 月 8 日に海外のハッカーフォーラムにハニーポット No.3 に関するスレッドが立った後はアクセス数が跳ね上がり，数日間非常に多い新規ホスト数を記録した．管理 WebUI の制御項目変更時の認証ダイアログは，ハッカーフォーラムに掲載以前は一度も開かれたことがなかったが，2019 年 12 月 8 日に 7 回，2019 年 12 月 9 日に 2 回，2019 年 12 月 10 日に 1 回開かれ，8 日の 7 回のうち 2 回は認証ダイアログに「`admin`」「`password`」といったパスワードを入力して認証の突破を試みる動きが見られた．操作がなされたのは，機器が保持するイベントのカウンターをリセットするためのボタンであり，監視制御の ON/OFF ボタンや，設定値の変更ボタンを操作するするような動きは見られなかった．

また，ハッカーフォーラム掲載後にハニーポット No.3 の Telnet の認証を突破しているホストは 2 件確認されたが，内 1 件は管理 WebUI を経由せず直接ログインに成功している．認証を突破したホストの一方は，「`sudo -s`」のコマンドを入力して root 権限を取ろうとする動きが見ら

れたが認証に失敗し，その後切断したため，そのホストがどのような操作を行おうとしていたのかを確認することはできなかった．もう一方のホストも同様に root 権限を取ろうとし，その後システム内部を探索したりユーザファイルにアクセスする動きが見られた．

以上の観測結果より，ハッカーフォーラムに掲載されると多くのアクセス者が流入することが分かったが，管理 WebUI 上では制御項目を大きく変更するような行為は見られず，慎重に管理 WebUI の探索を行うアクセス者が大半を占めた．また，Telnet にログインしてきたアクセス者はいずれも root 権限の獲得を行おうとしていたが，この行動は他の Telnet ログイン者にも見られたものであり，ハッカーフォーラムを経由したと思われるアクセス者が特段攻撃的であるかどうかの判断はできない．

4.4 Telnet へのアクセスの分析

表 1 の期間中のフルバージョンのハニーポットにおいて，管理 WebUI へ手動アクセスを行ったと判定されたのは 233 ホストであったが，そのうち認証の可否に関わらず Telnet のポートに対してアクセスを行ったのは 54 ホストであった．更にそのうち，Telnet の認証を試行したのが 19 ホストであるが，内 13 ホストが認証に成功してる．しかし，Telnet へのログインに成功している IP アドレスは 18 件確認されているため，管理 WebUI を見たアクセス者が別の IP アドレスを用いて Telnet にアクセスしたか，もしくは Telnet の ID とパスワードが何処かに流出した可能性がある．**図 4** は，Telnet ログインに成功したホストがセッション内に打ち込んだコマンド数をプロットしたグラフであり，同じ形状で且つ同じ色の点は同一のホストを表している．なお，初めて Telnet ログインに成功したホストが現れたのが 2019 年 3 月 23 日で，それより以前にログインに成功したホストは存在しない．

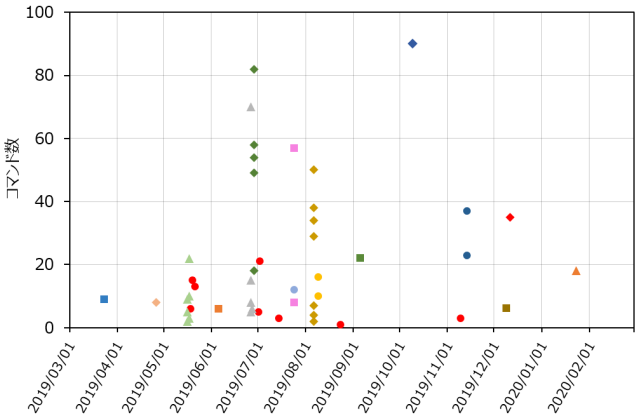

図 4　Telnet ログインに成功したホストのコマンド数

Fig. 4　The number of commands on a host that have successfully logged in to Telnet.

コマンド数の分布から，アクセス者の行動パターンが 2 種類に分けられることがわかる．1 つ目は，短期間に複数回アクセスを行うパターンである．このようなホストは，同一日に集中してアクセスする場合が多くなっており，複数回アクセスを行うホストの大半がこのパターンに当てはまった．2 つ目は，長期間に渡って複数回アクセスを行うパターンである．今回の観測期間においては殆ど見られなかったパターンであるが，2019 年 5 月中旬から 2019 年 11 月までの長期間に渡ってアクセスを行っているホストが 1 件だけ確認された．前者のパターンは後者に比べて，1 セッション内で打ち込むコマンドの数が多い傾向が見られた．

これら Telnet にログインを行ってきたホストは，大きく分けて次のような挙動が見られた．

- ユーザーファイルへのアクセス
- システムの探索
- 設定変更/アプリのインストール
- ファイル持ち出し
- 外部アクセス
- 内部ネットワーク探索

ログインしたホストの大半は，ホームディレクトリに配置されている機器リストのテキストファイルを開いており，中には記載されているローカル IP アドレスを用いて内部ネットワークを更に深く探索を行うホストも存在した．また少数ではあるが，curl や wget などを用いて外部コンテンツを取り込もうとする動きも見られた．

さらに，興味深いコマンドを入力してきたホストも存在した．入力コマンドの例を**図 5** に示す．

```
(1) nmap -p 1-1023 --reason [内部ネットワークの IP アドレス]
(2) nc [グローバル IP アドレス] 7414 -e /bin/bash
    python -c import socket,subprocess,os;
    s=socket.socket[以下略]
(3) netstat -na | grep ESTA
    netstat -na | grep LIST
```

図 5　Telnet ログイン後の入力コマンド例

Fig. 5　Example of commands entered after logging in to Telnet

(1) の訪問者は nmap で単純にサービスを検索するだけではなく，判定の理由を表示させる reason オプションを使いこなしている．また，(2) の訪問者には，nc や python で外部に接続するバックドアを設置する試みがみられた．(3) の訪問者は，TCP や UDP の接続状態を調べるコマンドである netstat の結果に，ESTABLISHED や LISTEN などのような状態を示す単語が入っていることを知っており，Linux 系の知識があると考えられる．

4.5 PLC へのアクセスの分析

PLC はプロキシを通じて絶えず外部からの通信を受け取っている．今回ハニーポットに組み込んだ PLC には固有のポートが存在するが，そのポートに対する通信は機器

に関連しないものが大半を占めている．しかし，その PLC の固有のポートに，ある特有のペイロードを送信すると，PLC が機器情報を含む応答を返すため，その性質を利用して特定の機種の PLC をインターネット上から発見することができる．実際に，その性質を利用したディスカバリツールがインターネット上に誰でも利用可能な状態で公開されており，ハニーポットに対する通信を分析すると，ディスカバリツールによるものと思われるパケットが日々多く観測されている．**図 6** に，当該システム内の PLC に対してディスカバリツールによる通信を送ってきた合計のホスト数が多かった上位 10 個の AS について月ごとのユニークホスト数の推移を示した． なお，アクセス者の AS 情報は GeoIP2 ISP Database[17] を用いて調べた．

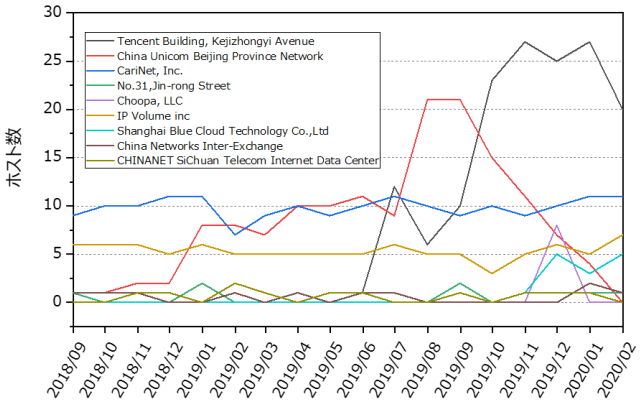

図 6 PLC のディスカバリツールを用いたホスト数上位の AS の月ごとのユニークホスト数

Fig. 6 Number of unique hosts per month for the top AS in terms of number of hosts using PLC's discovery tool.

上位の AS を見ると，「Tencent Building, Kejizhongyi Avenue」が 2019 年 7 月頃から大きく数を伸ばしていることが伺える．しかし，他の上位の AS と比較するとディスカバリツールのパケットは少なく抑えられている．また，これらの「Tencent Building, Kejizhongyi Avenue」からのホストについて，アクセス先のハニーポットをプロットしたグラフを**図 7** に示す．

図 7 において，黒色の点は一度のみアクセスしたホストを表しており，黒色以外は複数回アクセスしたホスト (同色は同一ホスト) を表している．当該 AS からのアクセスは，図が示すとおりどれか一つのハニーポットに対して集中してアクセスを行っているわけではなく，すべてのハニーポットに対して満遍なく行われていることがわかる．また，同一のホストが別日に同じハニーポットに対してアクセスを行っていないことがわかる．

以上のことから，これらのホストからの通信は高度に分散されたスキャンシステムによるものではないかと考えられる．これらのホストは Tencent のクラウドサービスから

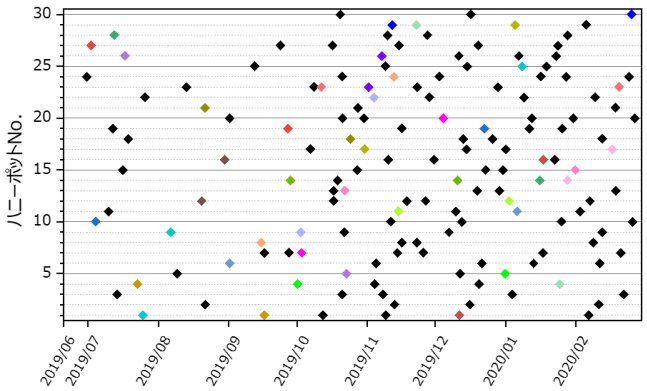

図 7 Tencent のホストからのディスカバリツールによるアクセス先

Fig. 7 Destination of the discovery tool from the Tencent hosts.

アクセスを行っているためアクセス元の国情報が様々であり，一つのアクセス先に対して最小限の通信を行っているため，スキャンの実態が非常に掴みづらいものとなっている．

5. まとめと今後の課題

遠隔制御監視システムを模したハニーポットを設置し，アクセス者の挙動の分析を行った．情報量の異なる 4 種類の管理 WebUI のアクセス状況の分析を行った結果，施設名や機器画像など管理 WebUI 上に掲載されている情報が多いほどアクセス者がより興味を持って探索を行うことが確認された．また，管理 WebUI を経由して Telnet にログインし，高度なコマンドを駆使することによって内部ネットワークを深く探索するアクセス者が観測された．さらに，管理 WebUI に掲載した連絡先を通じた通報によって得られた情報から，このような脆弱な管理下にあるシステムを知る方法の一つとして，ハッカーフォーラムがあることがわかった．当該ハニーポットに設置されている PLC に対しては，ディスカバリツールを用いて効率良くスキャンを行う同一 AS のホストが複数確認され，高度に分散されたスキャンシステムの存在が示唆された．

本研究における課題点はいくつか存在する． 1 つ目は，手動アクセスの抽出が完全なものではない点である．本研究においては，手動アクセスの条件として先に挙げた 3 つを使用しているが，例えばアクセス時に Cookie や Javascript を無効化していた場合は手動アクセスではないと判定される．このような誤った判定を無くすためにも，手動アクセスの判定手法を更に精密なものにしていく必要がある．2 つ目は，アクセス者のアクセス経路を把握しきれていない点である．Shodan，Censys，Zoomeye などの検索エンジンによるハニーポットへの影響については検証を実施しておらず，管理 WebUI がそれらの検索エンジンに登録された後にどの程度アクセスが増えるのか，または ICS ポート

の開閉状況によって管理 WebUI へのアクセスに影響ができるかなどの検証を今後の課題としたい．

謝辞 本研究成果の一部は，国立研究開発法人情報通信研究機構 (NICT) の委託研究「サイバー攻撃ハイブリッド分析技術に向けたセキュリティ情報自動分析基盤技術の研究開発」の支援により得られた．

参考文献

[1] 総務省，”総務省｜令和元年版 情報通信白書｜ IoT デバイスの急速な普及.” https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd112120.html (2020.08.11).

[2] 総務省，”重要インフラ等で利用される IoT 機器の調査.” https://www.soumu.go.jp/main_content/000561906.pdf (2020.08.11).

[3] 加藤里奈, 佐々木貴之, 藤田彬, 吉岡克成, 松本勉, ”インフラ施設の遠隔監視制御システムを模したハニーポットの提案.” 2019 年暗号と情報セキュリティシンポジウム (SCIS), 2019.

[4] Ariana Mirian, Zane Ma, David Adrian, MatthewTischer, Thasphon Chuenchujit, Tim Yardley, Robin Berthier, Joshua Mason, Zakir Durumeric,J Alex Halderman, et al. ”An internet-wide view of ics devices.” 2016 14th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2016.

[5] 森博志, 鉄穎, 小山大良, 藤田彬, 吉岡克成, 松本勉, ”能動的観測と受動的観測による iot 機器のセキュリティ状況の把握.” 情報処理学会研究報告研究報告 (CSEC), Vol. 2017, No.27, pp.1–6, 2017.

[6] ”Censys” : https://censys.io/

[7] ”Shodan” : https://www.shodan.io/

[8] ”Zoomeye” : https://www.zoomeye.org/

[9] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, ”IoTPOT: Analysing the Rise of IoT Compromises.” 9th USENIX Workshop on Offensive Technologies (WOOT 15), 2015.

[10] ”Conpot” : http://conpot.org/

[11] Dimitrios Pliatsios, Panagiotis Sarigiannidis, Thanasis Liatifis, Konstantinos Rompolos, Ilias Siniosoglou, ”A Novel and Interactive Industrial Control System Honeypot for Critical Smart Grid Infrastructure.” 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019.

[12] ”SCADA HoneyNet Project” : http://scadahoneynet.sourceforge.net/

[13] ”Honeyd” : http://www.honeyd.org/

[14] Hidemasa Naruoka, Masafumi Matsuta, Wataru Machii, Tomomi Aoyama, Masahito Koike, Ichiro Koshijima, Yoshihiro Hashimoto, ”ICS Honeypot System (CamouflageNet) based on attacker’s human factors.” 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, 2015.

[15] Barron Timothy, Nick Nikiforakis, ”Picky attackers: Quantifying the role of system properties on intruder behavior.” Proceedings of the 33rd Annual Computer Security Applications Conference, 2017.

[16] Brown Farinholt, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharmdasani, Haikuo Yin, Stevens Le Blondk, Damon McCoy, Kirill Levchenko, ”To catch a ratter: Monitoring the behavior of amateur darkcomet rat operators in the wild.” 2017 IEEE symposium on Security and Privacy (SP), 2017.

[17] ”GeoIP2 ISP Database” : https://www.maxmind.com/en/geoip2-isp-database