Vol.2014-DPS-158 No.39
Vol.2014-CSEC-64 No.39
2014/3/7

産業制御システムに対するサイバー攻撃の調査

水沼暁[†1]　　佐藤直[†1]

近年，主に重要インフラ業界で扱われる制御システムを標的としたサイバー攻撃によるインシデントが増加している．制御システムを情報系システムに接続することにより利便性向上およびコスト削減を実現しているが，制御システムと情報系システムそれぞれの脆弱性を考慮する必要がある．海外では，制御システムに対するインシデント報告件数は年々増加傾向にある．しかし，日本における報告件数及び事例の公開状況は海外と比較しても極端に少数であり，国内の制御システムインシデント状況が不透明である．そのため，制御システム事業者にサイバー攻撃の脅威が伝わらず，危機感が希薄になりがちである．しかし実際の攻撃者は，常に制御システムの脆弱性を狙っていると考えられる．そこで本研究では，SCADA HoneyNet Project のソースコードを用いて，制御システムを偽装したハニーポットを構築し，インターネットに公開することで第三者からのアクセス状況を調査した．その結果，80 番および 1433 番のポートに対するアクセスが異常に多いことが判明した．

Survey on the cyber-attacks to industrial control systems

AKIRA MIZUNUMA[†1]　NAOSHI SATO[†1]

Recently the incidents due to the cyber-attack targeting for the control systems of critical infrastructure have increased. The improved convenience and cost reduction can be achieved by connecting the control systems to information system. But vulnerability of these control system and information system must be considered. The number of incident reports tend to increase overseas. However, the number of incident report in japan is much less than overseas. Crisis consciousness does not increase for the cyber-attack because its risk is not informed. But attackers are believed to target the vulnerability of control system constantly. This study constructed a honeypot which emulates the SCADA system using the source code of “SCADA HoneyNet Project”. And it investigated the illegal access from attackers. As a result, it found the access rate to specific port 80 and 1433 is a significantly high.

1. はじめに

2010 年に発生した，イランの核燃料施設を操業停止させたマルウェア「Stuxnet」を発端に，主に機器を制御する目的で構築された制御システムを標的としたサイバー攻撃が増加しており，報道されることが珍しくなくなってきている．その背景には，制御システムと情報系システムの連携の一般化がある．もともと制御システムはプラントや工場内に限定されたネットワーク構成を採られていることが多く，外部とのやり取りがないため，独自の OS や通信プロトコルを採用する独立志向のシステムとして運用されてきた．そのため，インターネット上を賑わしているマルウェア等の脅威とは無縁と考えられていた．しかし，時代とともに通信インフラの整備が進み，制御システムを遠隔で監視・操作することを可能とする SCADA システムの採用が広がってきた[1]．SCADA システムにより，システム構築の際に汎用機器や通信プロトコルの採用及び人員などのコスト削減を実現している．しかし，汎用的な技術を導入したことにより，今まで無縁と考えていたインターネット上の脅威にも対応する必要が発生している．実際に「Stuxnet」のインシデントでは，USB メモリを介した感染経路をとっていると報道されており，制御システムを扱う事業者や現場社員のセキュリティ意識が，現在のネットワーク上の脅威に追いついていないと考えられる．そういった事態を問題視し，米国では制御システムを専門としている CERT である ICS-CERT を立ち上げており，インシデントの対応や情報展開を積極的に行っている．その報告の中では，制御システムを取り扱う業界のうち，2013 年は特にエネルギー業界に対する攻撃が多かったと報告している．原因のひとつに，システムで扱う機器に脆弱性が発見されたことがある．そして，とりわけ攻撃の対象が重要インフラ業界を狙ったものが多く，被害が甚大となり易く，多数の組織で注意喚起がされている．日本国内の団体では，独立行政法人情報処理推進機構（以下 IPA）が今後注目すべき脅威のひとつに重要インフラを挙げており，制御システムへのサイバー攻撃を懸念している[2]．また，内閣官房情報セキュリティセンター（以下 NISC）では，IT 障害が国民生活や社会活動計画に重大な影響を及ぼし得る重要インフラ分野として 10 の分野に分けていたものを，2014 年には 13 分野に

†1 情報セキュリティ大学院大学
Institute of Information Security

Vol.2014-DPS-158 No.39
Vol.2014-CSEC-64 No.39
2014/3/7

増やすことを検討している[3]．その他，制御システムセキュリティを見直す動きが活発化しており，国内外を問わず，様々な企業および団体でインシデント情報の報告・共有やセキュリティ勉強会が設けられている．

2. 制御システムの現状

2.1 制御システムインシデント

米国 ICS-CERT が重要インフラ事業者への標的型サイバー攻撃のインシデント報告を集計した結果，2009 年には 9 件だった報告が，2010 年には 41 件，2011 年には 198 件と年々数倍の増加傾向にある[4]．また，2012 年から 2013 年にかけては，半年間で既に 200 件を超過している[5]．その中でも割合が多い分野はエネルギー業界となっており，攻撃内容は SQL インジェクション，スピアフィッシング攻撃が大半を占めている．その他の国々でも重要インフラを狙ったサイバー攻撃は数年前から発生しており，2008 年にはポーランドの鉄道システムに侵入し，脱線事故を引き起こしている．この事件では実際にけが人を出しており，犯人は 14 歳の少年だったことが世間を驚かせた[6]．

このように，海外において制御システムを狙ったサイバー攻撃は実際に人命にも関わる被害が発生しており，制御システムのセキュリティを高める活動が活発になってきている．一方，日本国内でも JPCERT/CC が 2013 年より制御システムに関するインシデントの報告受付を開始している．しかし，2013 年の報告件数は 5 件のみで，海外の実情と比較しても，極端に低い数値となっている．その背景には，情報を発信することによる風評被害や，マルウェア感染した機器を故障と判断して完結してしまうことが背景にあることが考えられる．また，それに伴い国内の制御システムインシデント事例が公表されないことによって，制御システムを扱う現場に危機意識が定着しないという問題も含んでいると考えられる．

2.2 制御システムセキュリティの研究活動の現状

制御システムセキュリティの意識向上のために，経済産業省では「制御システムセキュリティ検討タスクフォース」を 2011 年に立ち上げ，テストベッド構築や制御機器認証評価体制の整備，人材育成・普及啓発等を目的として活動している．タスクフォース発足後，制御システムに関連する複数の国内企業の協力により，2012 年 3 月に「技術研究組合制御システムセキュリティセンター（CSSC）」が発足し制御システムのセキュリティ向上技術の研究開発を主な活動として行っている．CSSC では，2013 年 5 月に宮城県多賀城市にテストベッドが構築され，演習を通して，サイバー攻撃の演習・人材育成を実施している．

このように，制御システムに関する研究は既に開始しているが，国内で実際に制御システムに対する攻撃・アクセスがどういった状況になっているかといったことは，現在のところ明らかになっていない．日本 CSIRT 協議会や JPCERT/CC においても制御システムセキュリティの問題を指摘してはいるが，実際の攻撃調査等を公表してはいない．そこで，国内において制御システムをインターネット上に公開した場合，どのようなアクセスがあるのか，アクセス状況を調査することとした．今回の調査では，制御システム用ハニーポットを構築することとした．

3. ハニーポットを用いた調査

3.1 ハニーポットの有用性

マルウェアや不正アクセスなどのサイバー攻撃を調査するには，攻撃情報の収集が必要である．収集する際に有用なツールとして「ハニーポット」がある．ハニーポットはサイバー攻撃手法や，マルウェアの振る舞いなどを調査・研究するために，意図的に脆弱性を残した設定で構築された「おとり」の機器やシステム環境であり，新たな脅威を検出する上でも必要なものとなる．ハニーポットは攻撃を収集するために誤り無く攻撃を検知できることが望ましい．また，攻撃コード，マルウェア，攻撃元ホストの情報など，攻撃に関連する様々な情報を収集することを目的としている．そのためには，ハニーポット自身が攻撃者にハニーポットだと識別されないよう，実システムに近い高偽装性が求められる．もし攻撃者に攻撃対象ホストがハニーポットだと気付かれた場合，攻撃が中止され，情報が収集できずに終わる場合がある．また，ハニーポットを実装している端末自体が乗っ取られ，攻撃者となってしまうリスクも考慮する必要がある．ハニーポットで収集した情報を元に，セキュリティ脅威への対策サイクルのイメージを図 1 に示す．

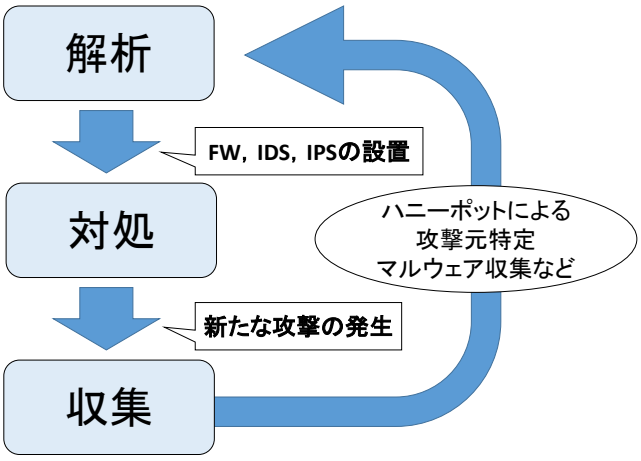

図 1　セキュリティ脅威への対策サイクル

3.2 ハニーポットの分類

攻撃者に攻撃対象ホストがハニーポットだと気付かれな

いためには，実システムのようにサービスを対話させることが必要となる．そのサービスの運用方法により，ハニーポットは高対話型と低対話型に分類される．

- 高対話型ハニーポット

高対話型ハニーポットは，脆弱性を残した実際の OS・アプリケーションを実装した機器を運用するハニーポットである．ハニーポットとしてエミュレートする必要が無く，実際のシステムを運用している状態と変わらないため，ハニーポットであると気付かれにくく，高い攻撃情報収集性を実現する．脅威に関する有用な情報を得易いが，実際のシステムを運用するので，攻撃者に制御を奪われる危険性が非常に高くなる．

- 低対話型ハニーポット

低対話型ハニーポットは，アプリケーションとして実装され，様々なサービスをエミュレートするハニーポットである．アプリケーションは比較的シンプルな設計となっているため，パフォーマンスと拡張性が比較的高い．攻撃者は，エミュレートされた Telnet や FTP などのサービスと対話することになる．サービスにログインしても，実際のオペレーティングシステムは存在しないため，攻撃者にとって有用な情報は得られず，攻撃対象ホストがハニーポットであると判断され易い．一般的に脆弱性の再現性が低く，攻撃検知性能や偽装性能も高対話型と比較すると低くなる．

3.3 SCADA システム用ハニーポット

欧州ネットワーク情報セキュリティ庁（ENISA : European Network and Information Security Agency）では，数十種類のハニーポットツールについて評価した結果を 2012 年に公開している．その調査対象のうち，制御システムにおいて用いられている SCADA システムを偽装するハニーポットツールについて次の 2 件を評価している[7].

- SCADA HoneyNet Project

SCADA HoneyNet Project は，制御システムネットワークのアーキテクチャをエミュレートするハニーポット構築を目的として，オープンソースのハニーポットツールである「HoneyD」上で SCADA システムを偽装している．ハニーポット構築の際に，動作が軽く，信頼性が高いことが利点として挙げられているが，エミュレート可能なコマンドが少ないことが欠点として報告されている．

- SCADA Honeynet(Digitalbond)

SCADA Honeynet(Digitalbond)は，制御システムセキュリティを扱うデジタルボンド社が改良した HoneyD を用いて，SCADA ハニーポットを構築する．また，別の端末にて，ハニーポットへのトラフィック監視を目的とする Honeywall を実装して運用する．

ただし，上記ハニーポット共に，参考情報が少なく，サポートがないので，SCADA 環境を偽装する低対話型ハニーポットの開発・研究が整備されていない．

3.4 先行研究

各種ハニーポットを用いた性能評価や攻撃情報収集などの研究は国内外を問わず実施されているが，制御システムを偽装したハニーポットを運用した結果はこれまで公表されてこなかった．しかし，トレンドマイクロ社が公開した調査資料では，制御システムを偽装したハニーポットを世界 8 カ国に設置して観測した結果が報告されており，設置箇所のひとつに日本が含まれている[8].

2013 年 4 月に公開された調査報告では，高対話型ハニーポットを採用し，Web サーバ，ポート 502（Modbus : 制御システムでよく使用される通信プロトコル），FTP，HTTP のサービスをエミュレートしている．また，別途 HMI の機能に見せかけたピュアプロダクションハニーポットと呼ばれる物理サーバ及び PLC（Programmable Logic Controller）装置を用いて，制御システムハニーネットワークを米国内に構築して調査している．その結果，ハニーポット公開から 18 時間後には攻撃を確認し，攻撃元の内訳では，中国（33.3%），米国（17.9%），ラオス（10.3%）の順で多い結果となっていた[9].

2013 年 8 月には同組織より調査レポートの第 2 弾が公開されており，国を跨いだ，より大規模なハニーネットワークを公開し，深刻度の分類や攻撃元の調査結果を公開している．

3.5 SCADA ハニーポットによる調査

本研究では，コスト面および安全面を考慮し，制御システムを偽装した低対話型ハニーポットを構築し，インターネット上に公開することで，外部からのアクセス状況を調査することとした．また，以下の理由により，SCADA HoneyNet Project において公開されているソースコードを用いて，制御システムを偽装する HoneyD ハニーポットを構築することとした．

- 今回事前調査したハニーポットのうち，構築手順が比較的明確である．
- 端末一台で構築可能である．
- エミュレートするサービスの拡張設定が容易である．

HoneyD は，ネットワーク上にバーチャルホストを作るためのデーモンとして動作するバーチャルハニーポットであり，オープンソースとして提供されている．このバーチャルホストは，任意のサービスを運用するよう設定し，特定の OS を偽装することが可能である．また，HoneyD はネットワーク上の未使用の IP アドレスを監視し，スキャンと侵入を検出するために用いられる[10].

3.6 実験概要および想定

今回の研究で構築したシステム構成図を図 2 に示す．本研究では，HoneyD を用いて 1 台のホストをエミュレート

Vol.2014-DPS-158 No.39
Vol.2014-CSEC-64 No.39
2014/3/7

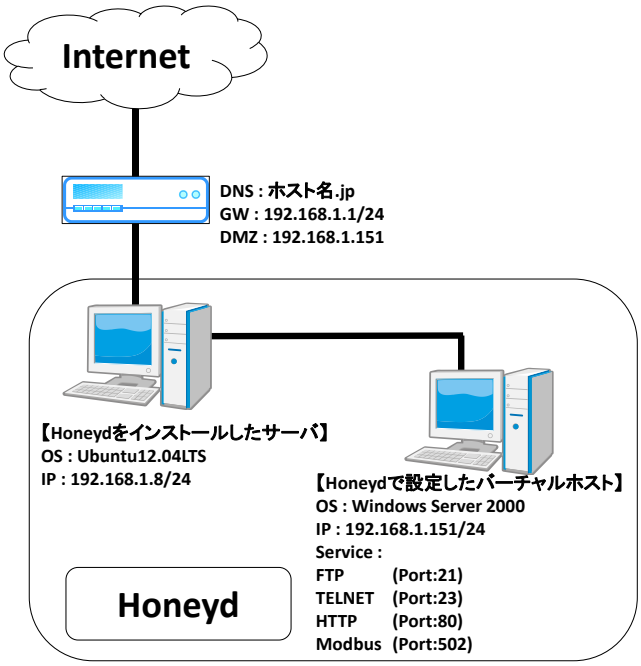

図 2 構築したハニーポットシステムの構成

した．SCADA HoneyNet Project において公開されているソースコードは Python で記述されている．また，ソースコードは 4 種類作成されており，それぞれ FTP/port21，Telnet/port23，HTTP/port80，Modbus/port502 のサービスを HoneyD 上で実現する．それぞれ，アクセス者に対し，実際にサービスが稼動しているよう対話することが可能である．HoneyD を実行した際，NMAP によりそれぞれのポートがオープンであることを確認している．

また，本研究を実施する際に DNS 登録を実施し，HoneyD サーバ上では 1 台のホストをエミュレートし，外部からのアクセスログを取得する．HoneyD 上で作成した仮想ホスト上に流れてくるトラフィックは，HoneyD のログとして出力される．

SCADA HoneyNet Project において公開されているオープンソースは，以下の 4 ファイルである．

- honeyd-ftpd.py
- honeyd-telnet.py
- honeyd-modbus.py
- honeyd-html.py

hoenyd-html.py はソースコード内に THML が記述されており，HoneyD を起動することにより簡易的な制御システム監視ページがブラウザ上からアクセス可能となる．デフォルト設定では，「PLC Web Page」というタイトルのページが表示され，PLC に関する数値設定などを扱うよう見せかける設計となっている．また，サービスポートの情報を記載しているページへの遷移も可能であり，対象ポートのサービスが稼動しているよう見せかけている．（図 3）

また，本研究で用いた設定ファイルを図 4 に示す．HoneyD 起動の際，この Config ファイルを指定する必要がある．今回使用した Config ファイルでは Windows 2000 Server を仮想バーチャルマシンとして構築している．また，TCP および UDP に対する振る舞いは Reset（TCP や UDP ポートが閉じている状態をエミュレートする）とし，ICMP に応対するよう設定している．

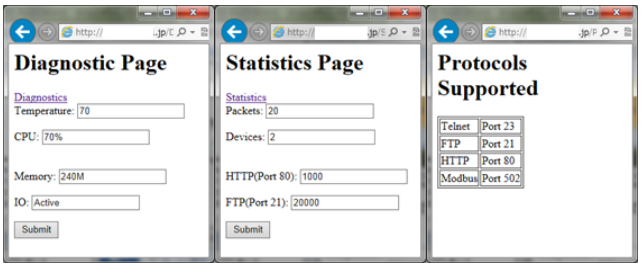

図 3 honeyd-html.py による SCADA Web ページ

```
1  create template↓
2  set template ethernet "3com"↓
3  set template personality "Microsoft Windows 2000 Server SP2" ↓
4  set template default tcp action reset↓
5  set template default udp action reset↓
6  set template default icmp action open↓
7  ↓
8  add template tcp port 21 "python /usr/share/honeyd/plc/honeyd-ftpd.py"↓
9  add template tcp port 23 "python /usr/share/honeyd/plc/honeyd-telnet.py"↓
10 add template tcp port 502 "python /usr/share/honeyd/plc/honeyd-modbus.py"↓
11 add template tcp port 80 "python /usr/share/honeyd/plc/honeyd-html.py"↓
12 add template tcp port 20000 open↓
13 add template tcp port 22 open↓
14 ↓
15 set template uptime 1728650↓
16 bind 192.168.1.151 template↓
17 [EOF]
```

図 4 HoneyD の Config ファイル

本研究で構築した制御システム用ハニーポット（以下，SCADA ハニーポット）をインターネット上に公開することで，Modbus/port502 に対するスキャンの動きを観測することが出来れば，制御システムに対する調査活動が行われていることを証明できると考えられる．その際，攻撃者は SCADA ハニーポットで実現した偽装 HTML のページで Modbus プロトコルが提供されていることを確認してから，スキャン活動に移ると考えられる．

4. ハニーポットによる調査

今回の実験は，2014 年 1 月 1 日 0:00 から 1 月 31 日 23:59 までの 1 ヶ月間，実験用ネットワークに設置したハニーポットに対するアクセスログを解析した．

4.1 ハニーポットへのアクセス数

ハニーポットに対するアクセス数を日別に集計したものを表 1 および図 5 に示す．

表 1 SCADA ハニーポットに対するアクセス数（1 月）

日	アクセス数	日	アクセス数	日	アクセス数
1	290	11	186	22	213
2	343	12	119	23	103
3	24573	13	157	24	5447
4	221	14	116	25	982
5	348	15	26551	26	372
6	154	16	942	27	379
7	148	17	95	28	125
8	126	18	123	29	144
9	156	19	169	30	151674
10	151	20	136	31	208
		21	143	計	214894

SCADA ハニーポット設置初日にはアクセスは約 300 件に達し,その翌々日には 2 万件を越える結果を出している．これにより，SCADA ハニーポットは設置後数日以内に何らかのスキャンが行われたと考えられる．その後も，アクセス数は 300 件程に収まっているが，定期的に数万件を越えるアクセスが観測されている．1 月 30 日に至っては，15 万件という異常なアクセス数を観測している．これら大量アクセスは, それぞれ一意の IP アドレスからアクセスしてきている．3 日のアクセスは，主にポート 1433/tcp を狙っており，15 日および 30 日のアクセスはポート 80/tcp を狙ってきている．

1 月 15 日のアクセスにおいて，その日の総アクセス数（26551 件）のうち約 99%（26384 件）が一意の IP アドレスから SCADA ハニーポットのポート 80 番に対するアクセスであった．また，1 月 30 日の大量アクセスも，別の IP アドレス元ではあるが，ポート 80 番に対して 151397 件のアクセスがあった．また，1 月 24 日のアクセスも同様にポート 80 番へのアクセスがその日の 98%を占めていた．

1 月 3 日のアクセスは，ポート 1433 番に対するアクセスが 99%を占めていた．ポート 1433 番は Microsoft のデータベース・ソフトウェアである MSSQL で使用されるポートであり，データベース管理用アカウントへの侵入を狙った攻撃方法が報告されている．1433 番ポートに関するサービスの脆弱性を利用したワーム感染の試みがあるとして，JPCERT/CC から以前より注意喚起がされており，本事象もそのひとつだと考えられる．

これらの大量アクセスは，攻撃者によるポートスキャンであるのか，またはマルウェアによる自動的なアクセスか区別することが難しい．また，制御システムで用いられる Modbus や DNP3 のポートに対するアクセスは検知できなかった．そのため，今回の大量アクセスの背景に，制御システムとしてスキャンを仕掛けてきたかどうかという判断は難しい．

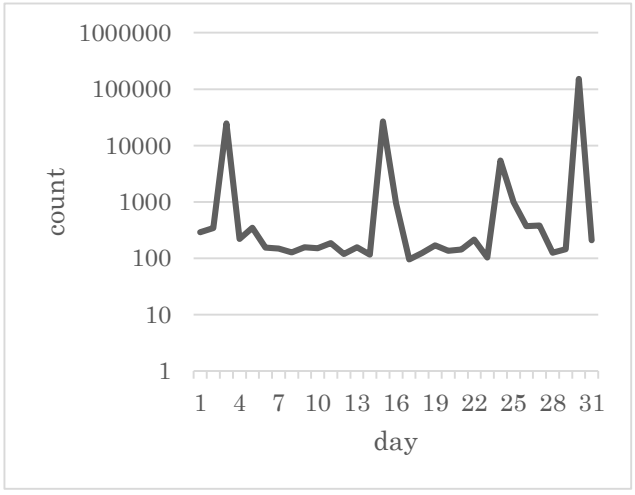

図 5　SCADA ハニーポットに対するアクセス数

表 2　ポート別アクセス数

ポート番号	アクセス数	ポート番号	アクセス数	ポート番号	アクセス数
80	185785	135	36	8799	28
1433	24712	8088	36	9797	26
22	1396	3128	34	9999	26
445	387	8081	34	10029	25
3389	358	81	33	5631	25
8080	237	9000	32	25	20
49494	196	8090	31	139	15
23	186	8888	30	1080	14
5900	172	0	29	21	14
5901	119	10001	29	4028	12
443	77	808	29	27017	10
4899	64	10011	28	110	9
1998	55	10012	28	2083	8
32764	53	10019	28	8009	8
21320	44	10033	28	53	7
3306	40	8001	28	その他	273
ALL	214894				

4.2 ポート別アクセス数

SCADA ハニーポットに対するアクセスをポート別に表したものを表 2 に示す．**4.1** でも述べたポート 80 番および 1433 番が多数の割合を占めている. そのほか, ポート 22 番（SSH）や 445 番（ファイル共有プリンタ）に対するアクセスも検知された．しかし，制御用サービスとして今回導入しているポート 502 番（Modbus）に対するアクセスは検知しなかった．その他，ポート 20000 番（DNP3）に対するアクセスも検知していない．これらより，本調査における SCADA ハニーポットに対するアクセスは，制御システムを対象としているアクセスとは言い難い．

4.3 ハニーポットに対する国別アクセス割合

ハニーポットに対して, アクセス元 IP からアクセス元の国を割り出し，集計したものを図 6 に示す．この際，一意の IP アドレスから複数のアクセスが存在しても，1 つとしてカウントしている．集計した結果，中国からのアクセスが 28%と最も多く，次に米国が 17%と続いている．台湾や

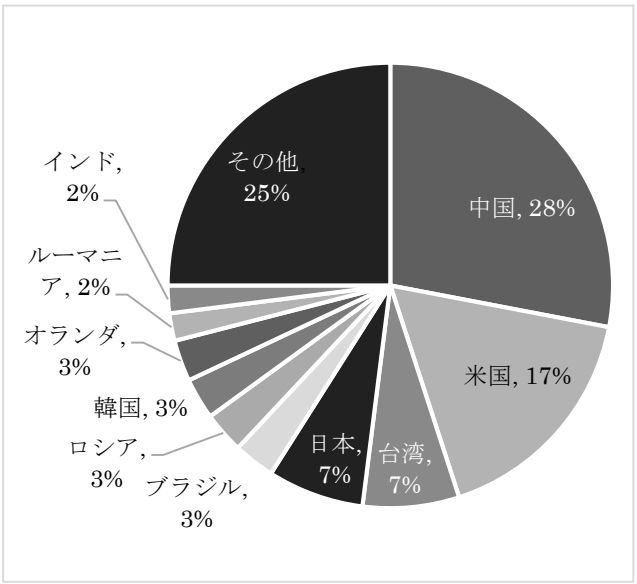

図 6　国別アクセスの割合

日本，などからも割合としては多く，5 割近くがアジアからのアクセスとなっている．しかし，これはひとつの IP アドレスから複数のアクセスが観測してもひとつとして分析しているため，アクセス数で集計し直すと，30 日の大量アクセスは,ルーマニアが 8 割以上であったことがわかった．

4.4 考察

今回の調査の結果，ftp，telnet，http に対するアクセスは検知したものの，Modbus に対するアクセスは検知しなかった．原因のひとつに，ハニーポットの設置期間が短期であることが考えられる．また，ハニーポットの情報を検索エンジンに登録するなど，情報の開示をしなかったことも原因と考えられる.3.4 のトレンドマイクロ社による調査報告書では，構築したハニーネットを検索エンジンへ登録するなどの種まき行為により，攻撃を検知し易い環境を構築していた．これにより，公開後からまもなく攻撃を検知していることから,如何にハニーポットの疑いを持たせずに，システムの情報を外部に公開するかが，制御システムへの攻撃・アクセス情報を収集するのに必要なことだと考えられる．また，今回のハニーポットでは ftp および telnet に対するアクセスを検知したが，使用できるコマンドが少ないため，攻撃者にとってはアクセス先がハニーポットであると判断し易いのではないかと考えられる．その状況を作らないためにも，より実際に存在しているシステム構成および設定ファイルのチューニングが必要となる．今回使用した HoneyD の拡張性は高く，設定により数千の端末を仮想適に作り出すことも可能となっており，プラントのような大規模な制御システムを模することも可能である.しかし，SCADA HoneyNet Project において公開されているソースコードは 2005 年以降開発が進んでいないこともあり，設定がデフォルトの状態でハニーポットを運用しても，即座にハニーポットと見抜かれてしまうと考えられる．ソースコード内に含まれている作者コメントにも，各人がそれぞれの SCADA 用設定をしてもらいたいため，最低限の設定しか記述していないと記載されている．ソースコード自体にもバグが存在しており，ログ監視の妨げとなった．コミュニティが機能していないこともあり，そういった問題点は各自解決する必要がある．

SCADA Honeynet(Digitalbond)による調査でも，ハニーポット公開後 18 ヶ月間攻撃を検知することは出来なかったとあり，制御システムをはっきりと狙った攻撃の収集手法がまだ困難であることも考えられる．しかし，今回の実験でも，脆弱性のある Windows サーバを実際に公開していた場合，継続的なスキャンなどの結果，マルウェアに感染していた恐れもある．また，検索エンジンに登録していなくとも，SCADA ハニーポットで展開された Web ページへのアクセス記録があるとおり，攻撃意思の有無に関係なく，常にスキャン活動を実行し，脆弱性のある箇所を調査しているマルウェア若しくは人物がいることを想定していなければならない．

5. まとめ

本調査では，まず制御システム業界におけるセキュリティの現状を調査した．そして，日本における制御システムのアクセス状況に関する研究が公表されていないことから，自身で制御システムを模したハニーポットを用いてアクセス状況を調査した．ハニーポットを構築する際，SCADA HoneyNet Project から提供されている HoneyD 用のオープンソースを用いることにより，簡易的な SCADA ハニーポットを構築した．そして 1 ヶ月間のアクセス状況を解析することにより，SCADA システムで用いる特有のポートに対する不正アクセスは見受けられなかったが，http や SQL で用いられるポートに対する大量アクセスを検知することが出来た．

今後は，より多くの攻撃情報を収集するため，実際の制御システムを模するハニーポットを構築すると共に，制御システムコミュニティや検索エンジンに登録して，露出を高める．このように制御システムハニーポットを構築することにより，制御システムを狙った有用な攻撃情報を収集可能であると考えられる．

参考文献

[1] Eric D.Knapp, INDUSTRIAL NETWORK SECURITY, james Broad, pp7-8, Syngress, USA, 2011
[2] 独立行政法人 情報処理推進機構（IPA）, 2013 年版 10 大脅威, 2013-03
[3] 内閣官房情報セキュリティセンター（NISC）, 重要インフラの情報セキュリティ対策に係る第 3 次行動計画（案）,2014-01-24
[4] Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）, ICS-CERT Incident Response Summary (2009-2011) pp2-5, 2012-09-05
[5] Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）, ICS-CERT Monitor Apr-Jun2013 pp2, 2013
[6] The Register, Polish teen derails tram after hacking train network, http://www.theregister.co.uk/2008/01/11/tram_hack/, 2008-01-11
[7] European Network and information Security Agency（ENISA）, Proactive Detection of Security Incidents pp101-105, 2012-11
[8] TREND MICRO, 産業制御システムへのサイバー攻撃実態調査レポート 第 2 弾, 2013-08
[9] TREND MICRO, 産業制御システムへのサイバー攻撃実態調査レポート, 2013-08
[10] Lance Spitzner, 小池英樹（訳）, 電気通信大学小池研究室セキュリティ研究グループ（訳）, Honeypots ハニーポット, 慶應義塾大学出版会, 2004-07