2012 年 12 月 26 日

独立行政法人情報処理推進機構(IPA)

# セキュリティインシデントの積極的な検知:ハニーポットの利活用

本概要は、欧州ネットワーク情報セキュリティ庁(ENISA:European Network Information Security Agency)が発行する、"Proactive Detection of Security Incidents- Honeypots"の抄訳となります。報告書は多くのハニーポットツールについて記載していますが、本概要では主に SCADA 向けツールの概要を「1.SCADA ハニーポット」に示しています。SCADA 向け以外のハニーポットツールについては、ENISA が CERT での利活用を推奨するツールを「2.CERT で利活用できるハニーポット」に纏めています。内容の詳細につきましては、原文をご参照ください。
(※本文中のリンク先は全て英文となります)

URL:

http://www.enisa.europa.eu/activities/cert/support/proactive-detection-of-security-incidents-II-honeypots

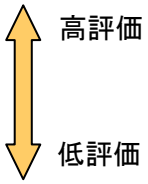
複雑で巧妙なサイバー攻撃が増加する中、組織のインシデント対応チーム(CERT)には少しでも早く脅威を認識することが求められている。ハニーポットはそのために有益なツールとなる(※ハニーポットは、サイバー攻撃者による攻撃手法や、マルウェアの振る舞いなどを調査・研究するため、わざと侵入し易いよう設定された機器やシステム環境)。本報告書では、CERT が利活用できる既存のハニーポットツールがないか、オープンソースの 30 のツールについて実用性に焦点をあてて調査・分析を行い、有効性や導入の障壁を探った。

各ハニーポットツールの評価項目は以下の通り。(評価基準の詳細は、原文参照のこと)

- Detection Scope:検知できる攻撃の範囲は、1 つのサービス/アプリケーション/プロトコルのみ(Specialized)か、複数(Multi-function)か
- Accuracy of Emulation:サービス/アプリケーション/プロトコル等の動作をどれだけ正確にエミュレートできているか、どれだけハニーポットだと見破りにくいか
- Quality of Collected Data:メタデータの種類や量、分析のし易さなど
- Scalability and Performance:拡張性、同時に処理出来るセッション数、スループット
- Reliability:フリーズや異常終了等しない、正常動作の持続時間、人によるモニタリングの必要性、過負荷時の反応など
- Extensibility:機能の拡張性(API の整備、ソースコード改変の難易度)
- Ease of Use and Setting Up:使い易さ(ユーザインターフェースやドキュメントの有無やレベル、インストールの容易さなど)
- Embeddability:ハニーポット機能の他システムへの統合性
- Support:開発者やユーザコミュニティによるサポートの有無やレベル
- Cost:導入費用感
- Usefulness for CERT:CERT にとって導入することが有益か

各項目の評価レベルは、以下。上に行くほど評価が高く、下に行くほど低くなっている。

| Detection scope | | Rating | | Cost | | Usefulness for CERT | |
|---|---|---|---|---|---|---|---|
| MULTI | Multi-function | ★★★★ | Excellent | $ | Low |  | Essential |
| | | ★★★ | Good | $$ | Medium |  | Useful |
| SPEC | Specialised | ★★ | Fair | $$$ | High |  | Not useful |
| | | ★ | Poor | | | | |




但し、最終的な「CERT にとって導入することが有益か」どうかの評価は、あくまで“CERT にとって”であり、ツール自体の評価と異なる場合もある。

## 1. SCADA ハニーポット

本調査では、SCADA 向けのハニーポットについても、2 件調査を行っている。

### (1) SCADA HoneyNet Project (http://sourceforge.net/projects/scadahoneynet/)

SCADA HoneyNet Project は、SCADA、DCS、PLC など制御システムネットワークの様々なアーキテクチャをエミュレートする低対話型(low-interaction)ハニーポットの構築を目的としており、本物のシステムによく似せた、基本的な機器で構成されたハニーポットとなっている。

SCADA HoneyNet Project の評価結果は以下の通り。

| DETECTION SCOPE | ACCURACY OF EMULATION | QUALITY OF COLLECTED DATA | SCALABILITY AND PERFORMANCE | RELIABILITY | EXTENSIBILITY | EASE OF USE AND SETTING UP | EMBEDDABILITY | SUPPORT | COST | USEFULNESS FOR CERT |
|---|---|---|---|---|---|---|---|---|---|---|
| MULTI | ★★ | ★ | ★★★ | ★★★ | ★★ | ★★ | ★★★ | ★ | $ |  |

エミュレートできるコマンドが少ないこと、役に立つメタデータが取得できないこと、サポートがない(2005 年以降開発が止まっており、ユーザコミュニティも活動していない)ことなどから、評価が低い項目がある。利点としては、CPU やメモリを多く使用しないために軽く、パフォーマンスが高い。また、信頼性も高く、他システムとの統合性も良い。

しかし、ICSでよく使うサービスをインターネット上で模して役に立つかは疑問であり、このようなハニーポットは、やはり本物の制御システムネットワークに仕掛けるのが最も効果的と思われる。とは言え、Modbus[1]をエミュレートできるハニーポットツールは少なく、将来インターネット上に仕掛けられた制御システムのハニーポットがより一般的になった場合のため、または実験として、既存の監視ツールに統合してみるのも一案である。

[1] 【IPA 補足】Modbus プロトコル http://www.modbus.org/

（2）SCADA Honeynet （http://www.digitalbond.com/tools/scada-honeynet/）

SCADA Honeynet は 2 つの仮想マシンから構成されており、1 つはハニーポットとしてセットアップされたサーバで、デジタルボンド社で改良を加えた低対話型ハニーポットツールの Honeyd、SCADA 環境をエミュレートするよう設定された FTP サーバと HTTP サーバ、Modbus エミュレータがセットされている。

もう 1 つは Honeywall をインストールしたサーバで、ハニーポットへのトラフィックを監視するのに使う。また、実際の制御システムを高対話型（high-interaction）ハニーポットとして使う場合向けに、Snort IDS の機能が拡張され、Modbus、DNP3、ICCP 検知用のルールが追加されている。

SCADA Honeynet の評価は以下の通り。


サービスのエミュレーションが非常に限定的であること、役立つメタデータの取得が行えないこと、honeyd 以外、サービスをエミュレートするツールは 1 つの IP アドレスしか使えないため全体の拡張性がないこと、他のシステムとの統合性がないこと、サポートがないことなどから、評価が低い項目もある、Modbus エミュレータのインストールはドキュメントも無く困難だが、他はドキュメントも充実しており、時間も掛からない。

デジタルボンド社によれば、開発期間中（18 ヶ月間）インターネット上に仕掛けておいたが、制御システムに対する攻撃は 1 件も検知されなかったという。このようなハニーポットは、本物の制御システムネットワークに仕掛けるのが最も効果的であり、インターネット上、または通常のイントラネットに仕掛けるのは意味がないと思われる。

なお、Snort IDS 用のルールは、ハニーポットツールとは別にダウンロードし、検知能力向上のために監視システムに適用することが可能。

## 2. CERT で利活用できるハニーポット

本調査の結果、CERT での利活用に推奨されるハニーポットツールを以下に挙げる。

（1） 低対話型サーバ型ハニーポット

- Dionaea：最も推奨されるハニーポットツール。FTP、WINS、TFTP、MS Windows RPC、SMB、HTTPS、MSSQL、MySQL、VoIP など幅広くサポートし、動作のエミュレーションレベルも高い
- Glastopf：最も推奨されるハニーポットツールの一つ。特にウェブ攻撃（HTTP）に強い
- Kippo：SSH に対するサポートをより強化したいのであれば、これが良い
- Honeyd：古いながらも、幅広く基本をカバーしていて良い

（2） 高対話型サーバ型ハニーポット

この区分のハニーポットツールは、非常に古いか（例：Sebek）、まだ成熟していない（例：Qebek）ものしかない。

- HiHAT：運用に若干努力を要するが、この区分では、恐らくは現時点で基も使えるハニーポットツール。ウェブ攻撃重視であり、更新も 2007 年以降停滞中
- Argos：手間を掛けるリソースがあるなら、更新活動も活発で、将来性は最も高い。高対話型クライアント型ハニーポットツールのベースでもある

（3） クライアント型ハニーポット

- Thug：低対話型。技術進化への対応が迅速。怪しいリンクの検証に有効。ウェブサイトのスキャンや守るべきサイトの監視には不向き（そうしたサイトは複雑過ぎてハニーポットがクラッシュする可能性あり）
- Capture-HPC NG：高対話型。怪しいリンクの検証のほか、ウェブサイトのスキャンや守るべきサイトの監視にも有効。初期にチューニングの努力を要する
- Honey-Spider Network 2.0：フレームワーク。複数のクライアント型ハニーポットの供用を可能にし、各ソリューションの利点を活用し、欠点のカバーが可能

## 3. CERT でハニーポットが利活用されていない理由の考察と勧告

攻撃の検知や分析におけるハニーポットの有効性は認知されていても、2011 年に ENISA が行ったアンケート調査によれば、ハニーポットを使用していると回答した CERT は非常に少ない。以下に考えられる理由を幾つか挙げる。

1. オープンソースのハニーポットツールの多くは、研究者の趣味や、学生の研究プロジェクトとして開発されたもので、プロジェクトの継続性や開発者によるサポートが乏しく、普及に必要な成熟度に達していない
2. オープンソースのハニーポットツールの多くは、使用するのも、収集したデータの意味を理解するのも困難
3. 収集データを分析し、結果をどう理解すべきか教えてくれる支援ツールが不足している
4. 収集データの標準化がされていない（分析の自動化やツールの開発などが進まない）
5. 高対話型ハニーポットは、一般的に維持・運用が難しい（多大なリソースを必要とする）
6. ハニーポットは実システム上で発生するトラフィック（production-level traffic）は監視しないため、実システムで発生する「正常なトラフィック」が分からず、実システムへの攻撃の検知やブロックはできない。このため、必須のソリューションとは見なされていない
7. クライアント型ハニーポットは特に使用するのが非常に難しい。扱うサービスが複雑で変化が激しく、誤検知が起き易い
8. ハニーポットと同じことを他のツール等で実現しており、ハニーポットを使用しているという認識がない
9. 必須のソリューションと見なされていないためか、セキュリティベンダは商用ハニーポットツールの提供に消極的。従って商用ハニーポットが殆ど存在しない
10. ハニーポットは攻撃に関するデータの収集に非常に有効だが、必ずしもネットワークを守る直接のソリューションを得るためではなく、より深い知識を入手し、その知識をソリューションの開発や提供に

活かすのに利用される。従って、研究機関やウィルス対策ベンダなど特定分野に特化したセキュリティベンダなど、一部の組織による利活用が進んでいる（理論的には、CERT もそうした組織の 1 つであるべきであり、脅威に対してより高い意識と知識を持ち、インシデントの積極的な検知にハニーポットを利活用すべき）

11. オープンソースのハニーポットツールの多くは、古過ぎて現在のシステムでは使えない
12. 多くの国家 CERT／政府 CERT は、管轄するネットワークに対する直接的な制御権を持っていない（ハニーポットを導入できない）
13. 社会的にも検討が進んでいない、ハニーポットの利用に伴う法的および倫理的懸念

CERT でハニーポットの利活用な進まない理由は様々考えられるが、ハニーポットは攻撃に対するデータを収集し、より深い知識を得るのに有効な手段である。また、実システム上で発生するトラフィックを監視しないため、プライバシーに関する懸念は低いと思われる。CERT におけるハニーポットの利用を進めるとともに、欧州レベルでも、グローバルレベルでも、CERT はハニーポットの開発にも積極的に取り組むべきである。

## 4. 将来的なハニーポットの研究分野

今後、ハニーポットの研究を進める上で、取り上げるべき分野を以下に示す。

- 現状のハニーポットによる検知の中心となっているドライブ・バイ・ダウンロード攻撃以外の攻撃への対応
- 動的ハニーポットの検討
- 新しいプラットフォームへの対応
  - モバイル
  - IPv6
  - ネットワーク機器およびルータ向けマルウェア
  - ICS／SCADA
  - 仮想化プラットフォーム
  - ソーシャルネットワーク
  - 医療機器のファームウェア
- 収集データの分析（データが示す意味の解析）

以上