制御システムに侵入したマルウェアの活動を検出する技術の開発

A Technique for Detecting Malware Activity in Industrial Control Systems

アズビル セキュリティフライデー株式会社 有元 伯治
Michiharu Arimoto

アズビル セキュリティフライデー株式会社 佐内 大司
Daiji Sanai

キーワード
デコイサーバ，セキュリティ，マルウェア，サイバー攻撃，制御システム

制御システムに対する高度なサイバー攻撃への対策として，マルウェアが制御システムに侵入していることを前提としたシステム構築が必要となっている。制御システムをサイバーセキュリティに考慮し運用していくためには，「気づき」が最も重要なポイントである。「おとり方式」によってマルウェアの活動を検出する方法が，制御システムに「気づき」を与える仕組みとして有効である。「おとり方式」を採用した制御システム向けのデコイサーバを開発したので報告する。

To counter sophisticated cyber-attacks on control systems, it is necessary to give the control system a structure that assumes the intrusion of malware. For cyber security, "noticing" while the control system is operating is the most important point. The "decoy method" is an effective way of enabling the detection of malware activity by the system. Here we report on our newly developed decoy server for control systems.

1. はじめに

2010年6月，イランの原子力プラントが高度なマルウェア（コンピュータウィルス）の攻撃を受け，大きなダメージを受けたことに端を発し，制御システムセキュリティが国家的課題と位置づけられた。2014年11月に成立／施行されたサイバーセキュリティ基本法では，「重要インフラにおける情報セキュリティ確保」が基本施策としてあげられ，2020年東京オリンピックに向けて本格的なサイバーセキュリティへの取組みが始まろうとしている。2014年度に国が設定した重要インフラは，情報通信，金融，航空，鉄道，電力，ガス，政府・行政サービス（地方公共団体を含む），医療，水道，物流，化学，クレジットおよび石油の13分野である。ここにはazbilグループが事業対象としているオートメーションの分野が含まれており，azbilグループにおいても重要インフラや制御システムのセキュリティが重要な課題になっている。

2. 制御システムのセキュリティリスク

制御システムのセキュリティ問題がクローズアップされるようになった背景には，制御システムが情報系と同じオープンシステムを利用し始めたことが大きく関係している。具体的には，今まで専用のハードウェアとして作られていた制御装置が，パソコンや汎用コンピュータ上のソフトウェアとして実装されようになった。そして管理用周辺機器を含めた多くの制御機器がパソコン上のソフトウェアとして提供され，制御システムはパソコンなしには動かないものも多くなってきた。制御装置間を接続する手段も，今までのメーカー独自の専用プロトコルやRS-485などのシリアル通信接続から，イーサネット上のTCP/IPへと変わった。これによって，ベンダー間の接続が容易になり，マルチベンダーの制御システムが手軽に構成できるようになった。さらに，近年では生産情報や工場のエネルギーを見える化するニーズ

の高まりから，制御システムと業務系ネットワークが接続されるケースが増えている。これは主に，業務システム側から工場側のシステムデータをモニターすることに限定されているが，確実に，業務システムと制御システムの接続が進んでいるのである。

このような状況の変化によって，制御システムはマルウェア（コンピュータウイルスなどの悪意のあるプログラム）への感染というセキュリティリスクを負うことになった。想定される主な感染経路は次のようなものがある。

(1) 業務ネットワーク（オフィスネットワーク）に侵入したマルウェアが，モニタリング用のネットワーク経由で制御システムに感染を拡大する。
(2) マルウェアに感染したエンジニアリング用のパソコンを，メンテナンス作業のために制御システムに接続することで，制御システム内にマルウェアが拡散する。
(3) マルウェアに感染したUSBやCD-ROMなどのメディアを，現場作業者が制御システムに接続してしまい，制御システム内にマルウェアが拡散する。

3. マルウェア対策の必要性と難しさ

制御システムは，従来，他のネットワークに接続されていないクローズドシステムであったことから，アンチウィルスソフトウェアの導入は不要と考えられ，積極的には行われてこなかった。しかし，オープン化の流れの中で，もはや「クローズドシステムである」という考え方はできなくなり，制御システムへのアンチウィルスソフトウェアの導入が急務となっている。一方で，情報系システムの実情を見ると，マルウェアは日増しに高度化し，その種類も日に数万単位で増えていて，アンチウィルスソフトウェアによるウィルス対策は既に破綻しはじめている。現在のパソコン用のアンチウィルスソフトウェアの検出率は20％前後まで低下しており，アンチウィルスソフトウェアを導入したところで，マルウェアのほとんどが検出できないのである。実際にイランの原子力プラントを攻撃したStuxnetというマルウェアは，攻撃当時のアンチウィルスソフトウェアでは検出できなかった。アンチウィルスソフトウェアの導入は必須だが，これにより完全にマルウェアの攻撃を防御することはできなくなっているのである。この傾向は，今後さらに進むことは確実で，情報システムと同様に，マルウェアが制御システムに侵入していることを前提としたシステム構築が必要となっている。

4. 制御システムでの本当のセキュリティ課題「気づき」

稼働している制御システムのセキュリティでは，情報系システム向けのセキュリティでは対応が難しい部分がいくつかある。その中の大きな課題として「気づき」がある。

生産現場では，日常的に様々なトラブルや異常が発生している。このトラブルへの対応のために，保全担当者が現場でシステムを監視し，不具合が発生すれば復旧作業を行っている。過去の豊富な経験と知識から，トラブルシュートの手順ができあがっており，現場では日々これに従って作業が行われている。

では，仮に制御システムがマルウェア侵入によりサイバー攻撃を受けた場合を考えてみることにする。その場合，誰かがサイバー攻撃であることを通知してくれる訳ではない。例えば，温度が適正値より上昇してしたままになった場合，現場の保全担当者は，従来のトラブルシュートに則って，機器の交換や調整を行うであろう。サイバー攻撃であることなど全く疑わない。現にStuxnetによるイランの原子力プラントへのサイバー攻撃の際，現場では攻撃によって壊れた遠心分離器の交換作業をひたすら繰り返していた。つまり過去に全く経験したことがないサイバー攻撃については，トラブルシュートがなく，これに気づくことすらできないのである。

もし不具合の原因がサイバー攻撃であった場合，情報セキュリティの専門家が調査を実施しない限り，サイバー攻撃が原因であったことには気づけないのである。これは，今までの現場のトラブルシュートとは別のフローでの対応が必要であり，サイバー攻撃の調査に移行できるトラブルシュートを作らなければならないことを意味している。我々は，制御システムにサイバーセキュリティを考慮し運用していくためには，この「気づき」が最も重要なポイントだと考えている。つまり発生したトラブルの原因が，「サイバー攻撃かもしれない」ことにいち早く気づく仕組みが必要である。そして，その「気づき」の仕組みをどのように提供するかがオートメーションに取り組むazbilグループの課題である。

5. 制御システム特有の制約条件と目指すモデル

トラブルの原因がセキュリティ問題かもしれないと疑う「気づき」を与える仕組みを制御システム向けに開発する場合，そこには情報系とは異なる制御システム特有の課題がある。

(1) 制御システムでは，24時間，365日の連続稼働が行われていることが多く，容易にシステムを停止できない。稼働中のシステムに対してセキュリティ対策を施すことはとても難しく，結果として対策ができない。
(2) 制御システムに対してエンドユーザーがセキュリティ対策を施した場合，制御ベンダーはシステム動作の保証をしない，あるいは対策を施すことさえ禁止されているというケースがある。
(3) 制御システムにセキュリティ対策を加える場合，制御システムの動作に悪影響が出ないことを事前に十分に検証する必要があることから，セキュリティ対策の実施には長い時間が必要になる。

では仮に「気づき」の機能が制御システムに提供できた場合を考えてみる。例えば現場で発生しているトラブルがセキュリティの問題かもしれないと疑った場合を想定してみる。その場合でも，セキュリティ問題の調査は簡単には進めることができない。なぜならば，セキュリティ問題の原因究明には，非常に専門的で高度な知識が必要とされるからである。セキュリティ専門家による調査や分析が必須で，

セキュリティ専門家に調査を依頼しなければならないのである。だからといって，セキュリティ専門家に調査を依頼したとしても，セキュリティ専門家は制御システムの基本的な動作に関する知識すらなく，制御システムに手を加えるような深い調査を実施することはできない。つまり制御システムのセキュリティ問題は，セキュリティ専門家でも調査ができないという現実がある。

このように，制御システムには特有の制約条件があるので，「気づき」を提供するシステムの開発にあたっては，下記の条件を目標として設定した。

(1) 既存の制御システムで利用できること，また，いつでも着脱できること
(2) 制御システムの稼働に影響を与えない技術であること
(3) 未知のマルウェアの活動であってもいち早く検出できること
(4) セキュリティ専門家に原因究明の調査を依頼できる仕組みを提供すること

我々は，様々な視点から検討した結果，「おとり方式」によってマルウェアの活動を検出する方法が，制御システムに「気づき」を与える仕組みとして有効であると判断した。おとり方式とは，制御システム上に，攻撃されやすいデコイサーバ（おとりPC）をあえて用意して，そこへの攻撃を監視し，不審なアクセスを検出するという方式である。マンションを例にして，おとり方式をわかりやすく説明する。

例えば，オートロック付きのマンションがあり，空き巣が何らかの方法でマンション内に侵入してしまったとする。空き巣は，鍵を掛け忘れている部屋を探し出し，中に侵入し，盗みを働こうとするであろう。ここで，一つの部屋を「おとり部屋」として準備する。この部屋には，わざと鍵を掛けずに空き巣が入りやすい環境を用意しておく。

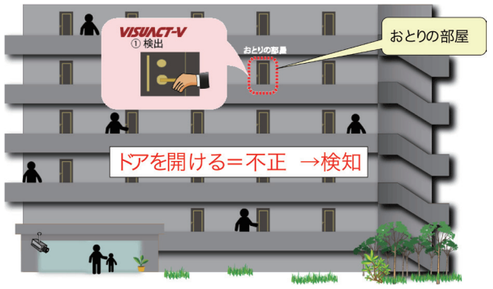

図１　おとり方式　ー 検知のしくみ ー

それを知らない空き巣は，やがてこのおとり部屋にやってきて，ドアノブを回し，鍵が掛かっていないことを知り，ドアを開け中に侵入する。この時，この部屋はおとり部屋であり，ドアノブを回すことすら不審な行為であると判断できる。さらにドアを開け中に入ったとなれば，不審者であると推定できる。つまりドアノブを回す行為やドアを開けて中に入る行為を監視して，アラートを出すという仕掛けを提供するのである。さらに，ホテルのドアのオートロックを玄関ドアに反対向きにつけるというアイデアもある。つまりおとり部屋の玄関ドアは，外からは開くけれども，中からは開かないという仕掛けである。こうすることで，ひとたび中に入った空き巣は，出てくることができなくなり，捕獲できるという仕掛けである。

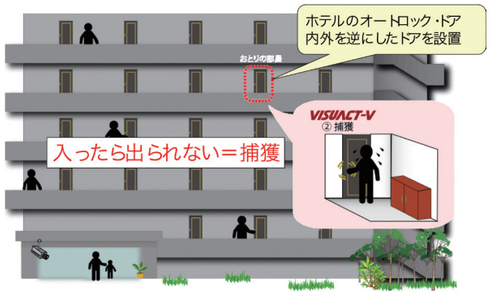

図２　おとり方式　ー 捕獲のしくみ ー

これと同じような原理のデコイサーバを制御システムにも提供しようというのが我々のアイデアである。制御システム内にデコイサーバをあたかも制御システムかのように設置する。このデコイサーバは，本来は誰からもアクセスはないはずである。

もしアクセスがあった場合には，それは制御システムに侵入したマルウェアやハッカーによる不審な活動であると推測できる。制御システムは，管理されたノードだけで構成され，あらかじめ決められたノード間でしか通信が行われないという特性を持っているので，この方法は単純でありながら大きな効果が期待できる。

おとり方式のメリットとしては下記のようなものがある。

- マルウェアの内部探索の段階でいち早くその怪しい活動を検出できる。また，ただちに発信元（感染元）を特定できる。
- 攻撃手法が既知であるかどうかにかかわらず，どのような攻撃パターンでも検出できる。
- おとりとなるデコイサーバを，制御システムへ簡単に設置，着脱できる。
- 設置しておくだけなので，制御システムへの影響がなく，システムを不安定にすることがない。

6. 制御システム用デコイサーバの機能

制御システム用のデコイサーバの主な機能は次の三つである。

(1) 攻撃検知

デコイサーバは，制御システムの機能を持っている必要はないが，制御システムネットワークに接続し，あたかも制御システムを構成するサーバのように見えるようにする。そして，制御システム内に侵入したマルウェアやハッカーからの不正なアクセスを待ち受ける。この時，デコイサーバに

は，ネットワークアクセスを監視し分析する機能を搭載しておく。この監視機能により，マルウェアの活動，つまり不正なアクセスを検出できるようになる。想定されるマルウェアの活動は次のようなものである。

何らかの方法で，制御システム内への侵入に成功したマルウェアは，まず，ネットワークや周辺ノードに対して探索や拡散活動を行う。この探索や拡散活動の段階で，デコイサーバに対して何らかのアクセスが行われる可能性がかなり高い。もともとデコイサーバ自体は，制御システムを構成するサーバではないので，もし外部から何らかのアクセスがあった場合，それを怪しいアクセス，すなわち攻撃であろうと推測できる。本来はどこからもアクセスがないはずのデコイサーバへのアクセスを検知するというスマートな検知手法であり，未知のマルウェアであってもネットワーク上で活動していれば検出できる。

(2) マルウェアへの感染を検知

もし，デコイサーバが制御システムに侵入したマルウェアからの攻撃を受けて，次のステップとしてマルウェアに感染してしまったとする。その場合，そのマルウェアの検体を捕獲したい。マルウェアを捕獲できれば，検体を取り出して制御システムの外で，専門家による詳しい調査を行えるのである。これを実現するために，デコイサーバをある程度マルウェアに感染しやすい状態でネットワークに接続する，つまり高度なセキュリティは施さない状態で稼働させておく。もし，マルウェアに感染した場合は，デコイサーバがその感染を検知し，マルウェアの捕獲機能を動作させる。

デコイサーバがマルウェアに感染したかどうかの検知は，デコイサーバから出ようとする通信の監視によりこれを実現する。マルウェアはデコイサーバへの感染に成功すると，次のステップとしてデコイサーバを拠点にしたネットワーク上の他のコンピュータへの攻撃を開始する。すなわちデコイサーバから制御システムネットワークに向けて，攻撃パケットを出し始める。このデコイサーバから出ようとするネットワークアクセスを検出し，デコイサーバへのマルウェア感染を検知するのである。ただし，デコイサーバがマルウェアに感染し，攻撃の拠点となってしまっては本末転倒である。デコイサーバが攻撃拠点にはならないような機能実装を行うことが必須である。

(3) マルウェアを捕獲

デコイサーバがマルウェアに感染したことを検知した場合，これをトリガーに感染したマルウェアの検体を捕獲する仕組みを提供する必要がある。しかしマルウェアがデコイサーバのどこに潜んでいるのかを見つけるためには，専門家による高度な解析が必要である。これらの高度な解析は，制御システムから切り離して，専門家に依頼できるようにするために，デコイサーバではマルウェアの検体抽出は行わず，感染したデコイサーバのメモリやハードディスクの状態をそのまま保全する機能を持たせる。

7. 制御システム用デコイサーバの実装

制御システム用のデコイサーバを実装する上では，次の課題の解決が必要である。

(1) デコイサーバは，マルウェアに感染させる必要があるが，感染したとしてもデコイサーバが次の攻撃元にならないように，デコイサーバからの攻撃を全て遮断する。

(2) デコイサーバがマルウェアに感染した場合でも，デコイサーバのコントロール自体がマルウェアに乗っ取られないようにする。

(3) マルウェアの検体を確保するために，感染させたPCのメモリおよびハードディスクの状態をまるごと保存する機能を実装する。デコイサーバの構成には仮想PC技術とファイアウォールを採用し，以下の構成で構築することにより実現した。

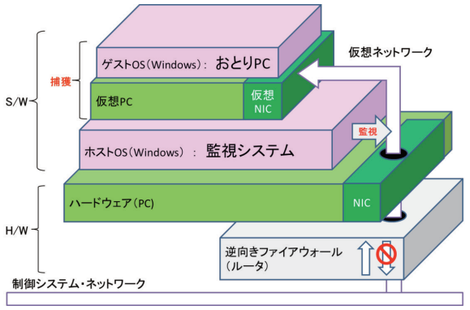

図３　システム構成イメージ

①マルウェアに感染した場合でも，デコイサーバから制御システム側を攻撃できないようにするファイアウォール（逆向き）
②デコイサーバのシステムを稼働する「ハードウェアPC」
③②の上で動作する「ホストOS」上の監視システム
④仮想マシンとして実装された「おとりPC」

デコイサーバ自体がマルウェアに乗っ取られないよう保護するために，
・「おとりPC」を，ホストと独立した「仮想マシンとして実装」する。
・「ホストOS」は通信インターフェイスをもたず，外部から一切通信ができないように保護する。
・「おとりPC」がマルウェアに感染した場合でも，マルウェアが「ホストOS」へのネットワークアクセスができないように，「おとりPC」の仮想NIC（Network Interface Card）を，ネットワークへ直接接続する。

次に，おとりPCが通常のWindowsPCと同じように動作するようにする必要がある。制御システムネットワーク側からのおとりPCへのアクセスは全てを透過し，制御システムネットワーク側からおとりPCへのファイル共有接続などは一切制限しない。

おとりPC自体は，通常のWindowsPCとして動作させることで，マルウェアの攻撃を受け，感染しやすい状態に設定する。感染することを前提に，強度なセキュリティを施さずに稼働する。一方で，おとりPCにマルウェアが侵入，感染した場合，おとりPC上の感染マルウェアが他のコンピュータへ攻撃できないように，おとりPCから送信するパケットは，すべてファイアウォールでブロックする。このことにより，デコイサーバへの攻撃に成功しおとりPCに侵入したマルウェアを，デコイサーバ内から逃さず，閉じ込めることができる。おとりPCは仮想マシンとして実装されており，おとりPCの仮想マシンのイメージをまるごと保存，取り出すことで，おとりPCに感染したマルウェアを安全に捕獲することができる。

マルウェア検出プログラムは，ホストOS上で動作し，おとりPCの通信を監視する。おとりPCへのアクセスパケットや，おとりPCからマルウェアによる送信パケットがあれば，これを検知する。また，マルウェアが多用するファイル共有のプロトコル（SMB: Server Message Block）については，これをリアルタイムで分析し，マルウェアの活動を記録する。さらに，ファイル共有以外のすべての攻撃パケットを記録する。

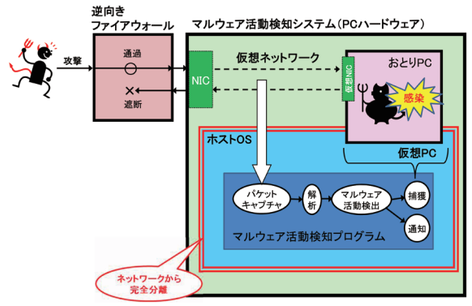

図４　機能構成図

8. 技術的ポイント

おとり方式を採用したデコイサーバの開発において，四つの主要な技術的なポイントがある。

(1) 攻撃されない監視システム
ネットワークインターフェースを持たないホストOS上に，仮想ネットワーク，仮想NIC，仮想マシンを構成し，ネットワークインターフェースを持ったおとりPCを実現した。

(2) マルウェアのリアルタイム検知機能
仮想ネットワーク上の攻撃をリアルタイムでプロトコル分析し，検知する仕組みを開発した。

(3) マルウェア捕獲機能
仮想マシンとして実装されたデコイサーバを，仮想イメージをそのままファイル保存する機能をもつことで，マルウェアの捕獲を実現した。

(4) 感染したデコイサーバからの攻撃遮断
おとりPCがマルウェアに感染したとしても，そこから制御システムを攻撃することができないような逆向きファイアウォールを構成した。

9. おわりに

デコイサーバによるマルウェアの活動検知は，独立行政法人情報処理推進機構（IPA）から2014年9月に発行された『「高度標的型攻撃」対策に向けたシステム設計ガイド』[(1)]でも紹介されている。年々高度化し，検出が難しくなっていくサイバー攻撃への気づきの手法として注目を集めている。

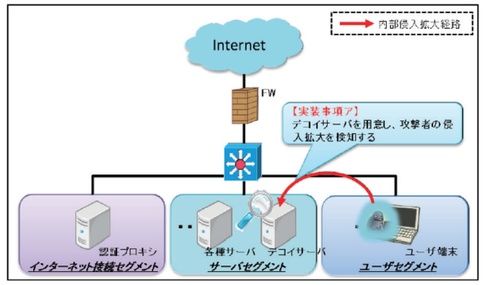

図５　デコイサーバによる監視
（「高度標的型攻撃」対策に向けたシステム設計ガイド，2014 より引用）

企業内部のネットワークセキュリティ問題に取り組んでいるazbilグループのアズビル　セキュリティフライデーでは，このデコイサーバ方式のサイバー攻撃検出にいち早く着目し，おとり方式を採用したマルウェア・センサーVISUACT™-Vを2012年にリリースしている。

VISUACT-Vは，デコイサーバの他にもファイアウォール，侵入検知システム，サンドボックス，そしてVISUACTを利用したSMBプロトコルのリアルタイム解析といった，複数のセキュリティ技術の組合わせで構成されている。サイバー攻撃が，ますます高度化していく中で，企業の内部ネットワークの監視／リアルタイム解析，およびデコイサーバによるマルウェアやハッカーの不正な活動のいち早い検知は，制御システムに限らず，情報セキュリティの次のソリューションとして注目されている。

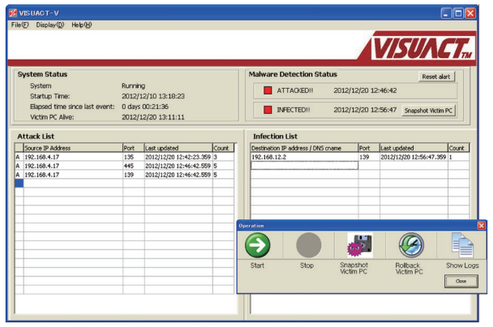

図６．　VISUACT-V 画面イメージ

＜参考文献＞
(1) 独立行政法人情報処理推進機構 技術本部 セキュリティセンター:「高度標的型攻撃」対策に向けたシステム設計ガイド, 2014

＜著者所属＞
有元　伯治　アズビル セキュリティフライデー株式会社 開発部
佐内　大司　アズビル セキュリティフライデー株式会社 代表取締役社長