Vol.2018-CSEC-83 No.2
2018/12/13

欺瞞ネットワークの効率的な配置の評価

杉生雅樹[†1]　辻秀典[†1]　橋本正樹[†1]

概要：サイバーセキュリティの分野では日々新たな脅威が生まれている。これに対抗するために、業態を問わず様々な組織がファイアウォールをはじめ、IPS/IDS やスパムフィルターなど様々な対策を行っているが、攻撃が巧妙化・多様化しており、強固な対策を施しても侵入を完全に防ぐことが困難になってきている。そのため近年では、侵入されることを前提にしたセキュリティ対策が注目されてきており、欺瞞技術を用いた防御手法もそのうちの一つである。しかし欺瞞技術には効率的に適用する評価が十分にされていない。本研究では、最も効率のよい欺瞞ネットワークの適用箇所を評価する。そのために既存の欺瞞技術を調査しわかった評価方法について報告をする。

キーワード：サイバーセキュリティ，ネットワークセキュリティ，欺瞞，ネットワーク

Evaluation of efficient placement of deception networks

Masaki SUGI[†1]　Hidenori TSUJI[†1]
Masaki HASHIMOTO[†1]

Abstract: A new threat is born every day in the field of cyber security. In order to counter this, various organizations are conducting various countermeasures including firewalls, IPS / IDS, spam filter, etc. regardless of the business type, however attacks are becoming more sophisticated and diversified, strong measures are taken It is getting harder to completely prevent intrusion. For that reason, in recent years, security measures on the premise of intrusion have been drawing attention, and one of defense methods using fraud technology is one of them. However, evaluation to apply efficiently to deception technology is not sufficient. In this research, we evaluate where the most efficient fraud network is applied. For that purpose, I will investigate the existing deception technique and report on the evaluation method that I understood.

Keywords: Cyber Security, Network Security, Deception, Network

1. はじめに

近年サイバーセキュリティの分野では、欺瞞・偽装技術が注目を集めている。ガードナーが毎年発表しているセキュリティトップ・テクノロジ[1]では、2016 年、2017 年、2018 年と 3 連続で「偽装技術 (Deception)」がトップ 10 入りしている。また、欺瞞を用いたセキュリティ製品なども近年徐々に広まっている。

以降本稿では、第 2 章で欺瞞技術の概要と動向について説明し、続く第 3 章で関連研究、第 4 章では本研究の先行研究について述べる。次に第 5 章では本研究の提案をし、第 6 章で評価方法についてのべる、最後に第 7 章で本稿をまとめる。

2. 欺瞞技術の概要と動向

2.1 近年のサイバー攻撃対策

近年のサイバー攻撃は著しく悪質化している。かつてのサイバー攻撃は自分のスキルを誇示したい等を動機とする愉快犯が多く、基本的には個人の犯行であったが、現在ではハクティビズム等集団による犯罪となり国際問題にまで発展することもある。また、攻撃対象についても、従来からの不特定多数に対する攻撃に加えて、標的型攻撃と呼ばれる、特定組織や個人を狙った情報窃取を行う攻撃が年々増加傾向にある。例えば、図 1 は警察庁が 2017 年に発表した標的型攻撃の被害件数である[2]。平成 25 年に一時減少したものの、そこからまた増加を続けている。一方で、対抗手段に目を向けると、従来セキュリティ対策として重要視されていたのは入り口対策であったが、巧妙化、多様化する攻撃を完全に防ぐことは益々困難になってきている。

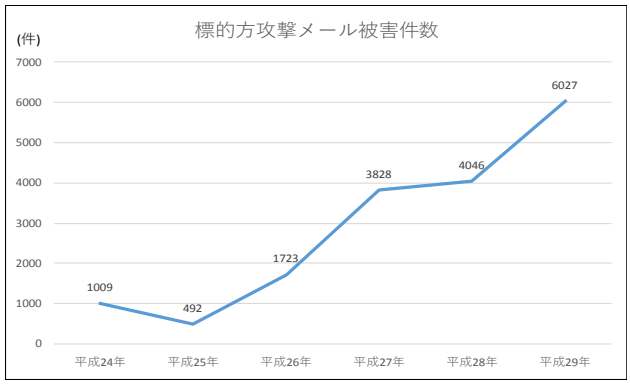

図 1 標的型攻撃被害件数

様々な組織が入り口対策を実施した後に注目されたのが出

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

口対策である。出口対策とは、内部から外部へ出て行く通信を監視することで組織にとって重要な情報の漏洩や、マルウェアが外部と通信をすることを防ぐ対策である。

しかし、出口対策を実施しても、設定不備等により意図しない外部への通信を見逃したり、暗号化したものに対しては効果を発揮できない等の問題がある。そのため、侵入されることを前提にした防御手法を確保する必要があり、特に近年では、侵入前提の防御手法として欺瞞・偽装技術が注目を集めている

2.2 欺瞞の定義と効果

欺瞞とはだますことである。古来より欺瞞技術はスポーツ、軍事、ギャンブルなど多数の分野で大きな威力を発揮してきた。Frank J らの研究[3]では欺瞞を表現するためにCyber-D&D(Denial&Deception)行列が提案されている。これは以下の 4 つに相当する欺瞞を効率的に考案するためのフレームワークである。

- 真実の暴露
- 虚偽の暴露
- 真実の隠蔽
- 虚偽の隠蔽

上記の分類わけを IT セキュリティ技術の一例にしたものを表 1 に示す。

表 1 Cyber-D&D 行列フレームワーク
Table 1 Cyber-D&D Matrix framework.

	暴露	隠蔽
真実	本物の N/W の暴露	システムリソースのアクセス拒否
虚偽	架空システムの暴露	ハニーポットの擬態情報隠蔽

また Pingree らの研究[4]では、コンピュータセキュリティにおける欺瞞について、「攻撃者をミスリードさせ、それによって攻撃者にコンピュータセキュリティ防御を援護する特定の行動をとらせるために計画された行動」と定義している。また、欺瞞技術の目的として、以下の 4 つをあげている。

- 攻撃者の認識を妨害または、挫折させる
- 攻撃者の自動化ツールを妨害する
- 攻撃者の活動を遅延させる
- 攻撃の進行を妨害する

また、Mohammed Almeshekah らの研究[5]では欺瞞技術を用いることにより以下の効果を期待できるものとしている 。

- 攻撃者を混乱、妨害、遅延させる
- おとりによる侵入を検知する
- 敵が得る情報の価値を落とす

欺瞞技術によってだますことが出来ない場合でも、攻撃者が得た情報の審議の確認を強制させることでリソースを浪費させ、少なくとも攻撃者の攻撃コストを増大させることが出来る。

3. 関連研究

本章では欺瞞技術を用いた検知や攻撃者をおびき寄せるシステムに類似しているハニーポットとハニーネット、欺瞞技術を使用したサイバー防御手法について取り上げ、その既存研究について述べる。

小泉らの研究 [6]では、既に存在している行動制限型ハニーポットの改良方法について提案をしている。ハニーポットと気付かれ難く、設置・運用をより効率的に行うためにラッパー方式によるコマンド制御を行う。特殊 OS の偽装（ダミーOS） や偽の対話インターフェース(ダミープロンプト)、コマンドに対する偽の返答(ダミーメッセージ)などを対象に改良をしている。

Sindhu S Pandya の研究[7]では　ハニーネットの簡単かつ効率よく構築する方法について提案している。また、ハニーネットを用いることで侵入への検知、攻撃手法、アプローチなどの得られる情報について述べている。

上記のようにハニーポット、ハニーネットは欺瞞技術として浸透しつつあるが基本的に専用機器を用意し大規模な運用を想定しており、その分コストも高くなる。また、実際に脆弱性を持っているため、攻撃を受けるリスクを内包している。さらにハニーポット情報収集のため攻撃者をだまし続ける必要があり、検知されてしまった場合は攻撃者に回避され、もしくは最悪の場合は利用されてしまう。上記をまとめたものを表 2 に記す。

表 2 ハニーポットのリスク
Table 2 risk of hany pot.

#	種類	リスク
1	コスト	専用リソースかつ高コスト
2	脆弱性	本物
3	リスク	のっとられる可能性があり高リスク
4	運用難易度	だまし続ける必要があり困難

また Mohammed Almeshekah らの研究[5]では Eric M. Hutchins らの研究[8]と MITRE Corp らの研究[9]で攻撃者の行動を細分化しパターンわけした Cyber Kill Chain に対して有効な欺瞞技術を述べている。これをに示す。

表 3　Cyber Kill Chain における各攻撃段階と欺瞞技術
Table 3　Each attack stage and deception technique in Cyber Kill Chain.

#	段階	欺瞞技術
1	偵察	ポート偽装
		偽サイト
2	武器化	Sticky ハニーポット
3	配送	メールの偽装返信
4	攻撃	脆弱性検査への偽装応答
5	インストール	
6	遠隔操作	ハニーポット
7	目的実行	ハニーアカウント
		ハニーファイル
		ハニートークン
		エンドレスファイル
		Fake key

4. 先行研究

本章では、山田らの研究[10]、Yuill[11]らの研究や Ben らの研究[12]を本研究の先行研究として特に取り上げ、詳細に説明する。

4.1 欺瞞用いた能動的サイバー攻撃防御手法の提案と実装

4.1.1 先行研究の目的と意義

山田らの研究の目的は、標的型攻撃に対して、標的となった際の攻撃を失敗させ、また標的となることを回避するための欺瞞手法の基礎を確立することである。そして、攻撃通信を遮断しアラートを発することを基本とした従来の受動的な防御戦術に、欺瞞を用いた能動的な防御戦術を組み込むことで、防御戦術の幅を広げることを目的としている。この目的を達成するために、山田らは、攻撃者に対して偽の情報を送り、攻撃者の判断を誤らせることにより攻撃者のコストを増大させることを提案した。

4.1.2 実験内容と評価

山田らの研究では、以下に説明する 4 つの偽装を実装し、その評価を行なっている。

(1) **ポート偽装**
nmap[13]における最も一般的なポートスキャンとして SYN スキャンと呼ばれるスキャンが存在する。SYN スキャンに対して任意のポートに偽装するプログラムを実装した。

(2) **OS 偽装**
OS を判定するための OS スキャンパケットを送付し、各 OS 固有の OS スキャンパケットに対する返信パケットを評価することにより、端末の OS を判定する機能に対して任意の OS に偽装するプログラムを実装した。

(3) **サービスバージョン偽装**
オープンポートのサービスバージョンスキャン機能に対して任意のサービスバージョン偽装するプログラムを実装した。

(4) **サービス応答偽装**
HTTP リクエストを行い、返信された WEB ページを表示する機能に対して任意の HTTP レスポンスを偽装するプログラムを実装した。これにより HTTP サービスを実行していないにもかかわらず、偽の WEB ページを WEB ブラウザに表示させる。

山田らの研究では、上記 4 つの実装に対して、防御側が欺瞞技術を用いて偽装可能かという観点から評価を行なった。その結果を表 4 に示す。

表 4　偽装技術の実装結果
Table 3　Result of deception.

#	偽装技術	結果
1	ポートスキャン	可能
2	OS 偽装	任意 OS に偽装可能
3	サービスバージョン偽装	可能
4	サービス応答偽装	可能

4.1.3 課題

山田らの研究では欺瞞を用いることで 4 つの応答の偽装を実装し評価を行った。提案手法を欺瞞技術適用モデルに沿って計画、実装、運用することで標的型攻撃の攻撃者からコストを上昇させるための効果があることを示した。しかし下記のような課題があると山田らは述べている。

- 欺瞞のシナリオを増やし防御側の戦術を増やす必要がある
- WindowsXP とそのサービスの偽装のみの実装しかできていない
- FW 機能が実装できていないため、制約が生じている。
- 研究の効果を定量的に評価していない。定量的に評価するために、判定する尺度に関しての検討が必要
- 検知を行うシステムの構築ができていない

4.2 ハニーファイル

4.2.1 先行研究の目的

Yuill らの研究と Ben らの研究では、ハニーファイルの有効な設置な場所とハニーファイルが悪意のあるアクセスを検出するのに有効であるか評価を行った。

4.2.2 実験内容と評価

Yuill らの研究では、ハニーファイルシステムを構築し、ハニーネットに設置をした。そして学生グループに対してシステムに侵入するようなテストを実施した。結果としてはハニーファイルの最も効果的な配置は、ファイルシステ

ムのルートディレクトリの近くであることを発見した。

また、Ben らの研究では、どのような欺瞞文書が攻撃者にとって魅力的かつ、目立つかを評価した。評価方法としては、学生グループに財務書類を Ben が用意したロックされていないシステムから入手するテストを実施した。このシステムには財務書類に紛れて欺瞞文書もシステムに配置した。結果としては全ての学生は開始してから 10 分以内に検知され、欺瞞の使用がシステムへの悪意のあるアクセスを検出するのに非常に効率的であることが示された。

4.2.3 課題

Yuill らの研究と Ben らの研究では、欺瞞が他の防御方法を補完し、効果的な防御方法であることを示すことが出来たが、以下のような課題がある。

- 防御するシステムに対しての欺瞞を手動、もしくは自動的に設置するための最適な方法の評価
- 欺瞞要素を引き起こさずに実行される攻撃(誤検知により攻撃と判断されない率)
- 配置方法を変えた場合の攻撃ではないものに対して、攻撃と判断してしまう誤検知率
- 欺瞞が更新されない場合、時間経過とともに検出が劣化してしまう評価
- 欺瞞と他のセキュリティと統合できるかの評価

5. 提案

5.1 研究の目的と意義

本研究では、先行研究の諸課題を解決しながら、欺瞞システムをさらに効率的に使用することで、1 台の端末が完全にのっとられ、システムに侵入された後、攻撃者が重要情報へたどり着く前に重要情報を守ることを目的とする。

これを達成するために最も欺瞞技術が有効になるネットワークを調査し、そこに対して欺瞞技術を適用することで以下の効果が発揮されるか評価をする。

- 隔離されたネットワークへおびき寄せ、重要情報があるネットワークへ侵入させない。
- 攻撃者が隔離されたネットワークへ侵入し、調査をしている間に重要情報をネットワークから隔離することで重要情報を守る。
- 攻撃ツールを欺くことで攻撃を不発にする。

5.2 提案手法

本稿ではまず通常の図 2 のようなネットワークを構築し、最も攻撃者がアクセスするネットワーク、もしくは攻撃者から見て魅力的なサーバの場所を評価する。

- セグメントは大まかに内部セグメント(イントラ見立て、管理セグメント、外部セグメント(DMZ 見立て)、端末接続セグメントの 4 つからなる。
- IP アドレスのレンジは各セグメントに複数用意する。

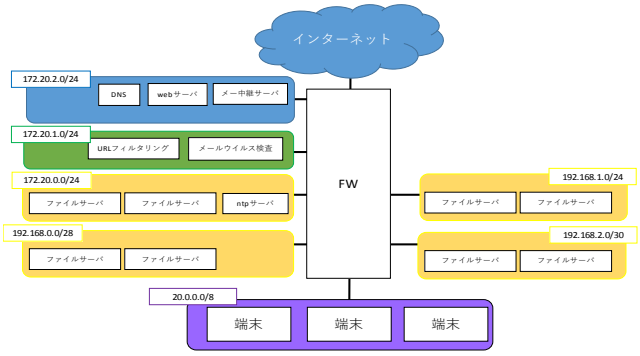

図 2 実験環境

上記の最も効率のよいネットワークに対して以下の 3 の欺瞞技術を用いることで攻撃者の攻撃コスト増加および重要情報の防御を行う。本研究で提案する手法は以下の 3 つである。

- ネットワークの閉じ込めと迷路化
- 認証情報の欺瞞
- 検知

5.2.1 ネットワークの閉じ込めと迷路化

攻撃者が侵入後、権限昇格を行い他端末やネットワークに対してログインを行う。この際に端末に同ネットワーク、閉じ込めるネットワークに欺瞞情報を持たせることで、攻撃者を閉じ込めるネットワークへ誘導する。図 3 のように A のネットワークから B のネットワークへは通信可能であるが、B のネットワークから A のネットワークへは通信不可能である。これにより、一度 B のネットワークへアクセスしてしまうと A のネットワークへは移動できなくなってしまう。

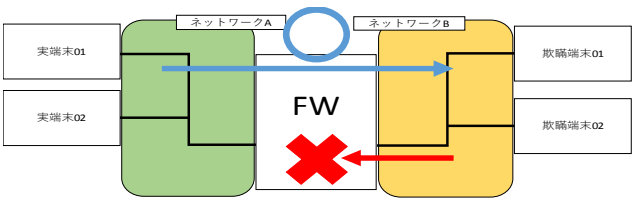

図 3 ネットワークの閉じ込め

閉じ込めたネットワーク内にさらに端末を設置することでネットワークの迷路化を実装する。これにより、攻撃者が閉じ込めるネットワークにいる時間を長くし、検知してからの対策時間を持たせることが出来ると考えている。

5.2.2 認証情報の欺瞞

図 4 のように偽の認証情報を端末に所持させる。攻撃者が権限昇格、横展開をしようとする際に偽の認証情報を参照する。これにより下記の効果が期待できる。

- 偽の端末の認証情報を参照することで本物ではなく、偽の端末へログインをしてしまう。
- 本物の認証情報を見つけるのに時間がかかってしまう。
- 端末の情報が怪しいと感じ、攻撃、調査を中断する。

図 4 偽の認証情報

5.2.3 検知

図 5 のように欺瞞端末にログインが発生した際にアラートを飛ばす。これにより、欺瞞端末にログインした際、防御側は即座に防御することが可能である。

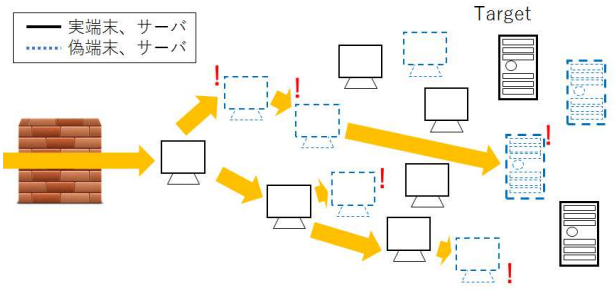

図 5 アラームの検知

6. 評価の方針

欺瞞の評価方法として XIAO らの研究[14]では以下のように示している。すなわち、欺瞞を測定するために最も一般的に使用する評価方法は人間の評価者が欺瞞を判断することである。これに乗っ取り、本研究での目的である攻撃者が重要情報へたどり着く前に重要情報を守ることが可能か評価する方法は以下を実施する。

(1) セキュリティ知識のある者複数人に欺瞞ネットワークが含まれない環境から重要情報を取得するテストを実施する。この際にどのサーバへアクセスするか記録しどのようなネットワークに欺瞞ネットワークを設置するのが最も効率がよいか評価をする。

(2) (1)の実験により最も有効であると判断したネットワークに図 6 のような欺瞞ネットワークを設置し、再度セキュリティ知識のある者複数人に欺瞞ネットワークが含まれるシステムから重要情報を取得するテストを実施する。この際下記が発生した場合、欺瞞システムが有効であると判断する。

- 欺瞞システムによる検知が発生したか
- 閉じ込めたネットワークに入ってしまっていないか。

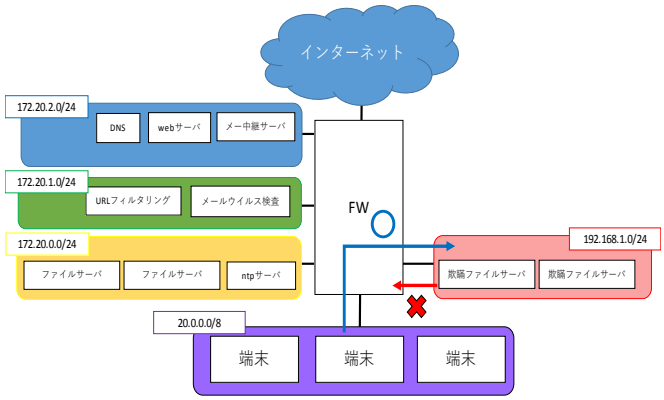

図 6 欺瞞ネットワーク設置後構成

(3) 攻撃者が使用する攻撃ツールやマルウェアを端末上で実行し隔離ネットワークに誘導されるかも検証する。

7. おわりに

第 2 章で欺瞞技術の概要と動向について説明し、続く第 3 章と第 4 章では既存の欺瞞技術について述べた。近年欺瞞技術は大きく注目されていることがわかったが未だ効率のよい評価方法や課題があった。第 5 章、第 6 章では課題を解決するために本研究で行ったことと今後実装していくことについて記載した。

本研究の課題は、実際に評価を実施することと正常通信と攻撃の通信を見分ける方法が挙げられる。本研究の評価を実施した後攻撃者を騙すために構築した欺瞞ネットワークを通常の正しいユーザには適用しない、もしくは騙さないような仕組みなどの対処法についても今後の研究の課題となる。

8. 参考文献

[1] https://www.gartner.com/newsroom/id/3744917
[2] https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf
[3] Frank J. Stech, Kristin E. Heckman, and Blake E. Strom “Integrating Cyber-D&D into Adversary Modeling for Active Cyber Defense”
[4] Pingree,L“Emerging Technology Analysis; Deception

Tecniques and Technologies Create Security Technology Business Opportunities.”, Gartner, Inc(july015).ID:G00278434.
[5] Mohammed Almeshekah Eugene H. Spafford, Mikhail J. Atallah “Improving Security Using Deception” Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, IN 47907-2086
[6] 小泉 芳, 小池 英樹, 安村 通晃 “社団法人 情報処理学会”, 研究報告書 2004-CSEC-27 (11)
[7] Sindhu S Pandya Laxmi Institute of Commerce and Computer Application, Sarigam “Active Defence System for Network Security – Honeypot”
[8] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.Lockheed Martin Corporation, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”
[9] MITRE Corp “Adversarial Tactics,Techniques and Common Knowledge”
[10] 山田 大, "欺瞞用いた能動的サイバー攻撃防御手法の提案と実装" 情報セキュリティ大学院大学特定課題研究, 2016.
[11] Jim Yuill, Dorothy E Denning, and Fred Feer. 2006. Using deception to hide things from hackers: Processes, principles, and techniques. Technical Report. DTIC Document.
[12] Ben Whitham. 2017. Automating the generation of enticing text content for high-interaction honeyfiles. In Proceedings of the 50th Hawaii International Conference on System Sciences.
[13] Nmap Reference Guide,from https://namp.org/book/man.html,July 2017
[14] XIAO HAN, Orange Labs, France,NIZAR KHEIR, Thales, France,DAVIDE BALZAROTTI, Eurecom, France“Deception Techniques in Computer Security: A Research Perspective”