PACIFIC サイバーセキュリティ研究所レポート Vol.1

観測から見えた“サイバーの空模様”
～ハニーポット観測で読み解く攻撃の実態～

1. はじめに

本レポートでは、インターネット上に構築した攻撃者を誘導するおとりシステムであるハニーポットを活用して観測されたサイバー攻撃について分析し、その傾向と対策をまとめた。観測期間中に外部から受けた攻撃の特徴を明らかにして傾向分析し、今回は特に遠隔操作のための暗号化プロトコルである SSH への攻撃試行に注目し、サイバー攻撃への対策の提言を行う。

2. 構成概要

2.1 ハニーポット概要

ハニーポットとは、攻撃者に対して実際のシステムやサービスであるかのように見せかけることで、不正アクセスやマルウェア活動などのサイバー攻撃を意図的に引き寄せ、観測・記録するためのセキュリティ技術である。実際の業務システムとは切り離された環境で動作するため、被害のリスクを最小限に抑えつつ、攻撃手法や傾向、使用されたツール等の情報を収集することが可能である。これにより、攻撃の傾向を把握したり、新しい手口を早く見つけるのに役立つ。

T-Pot は、そのようなハニーポット技術を統合的に運用可能としたオープンソースのマルチハニーポットプラットフォームである。Cowrie、Dionaea、ConPot など複数のハニーポットを Docker®コンテナとして搭載しており、SSH、SMB、SCADA など多様なプロトコルに対応した擬似サービスを提供する。これにより、幅広い種類のサイバー攻撃を模擬・観測できる環境を実現している。

また、T-Pot には収集データの検索・保存・可視化を行う仕組みが統合されており、収集された攻撃データはリアルタイムで可視化・分析することができる。特に、攻撃の発信元を地図上に表示するアタックマップ（図 1）では世界中からの攻撃元 IP を地図上に可視化し、攻撃の集中度や傾向を直感的に把握することが可能である。

さらに、ダッシュボード（図 2）で、各ハニーポットが収集した詳細なログ情報や、攻撃対象のポート、試行されたクレデンシャル、攻撃の時系列推移などを視覚的に分析することができる。

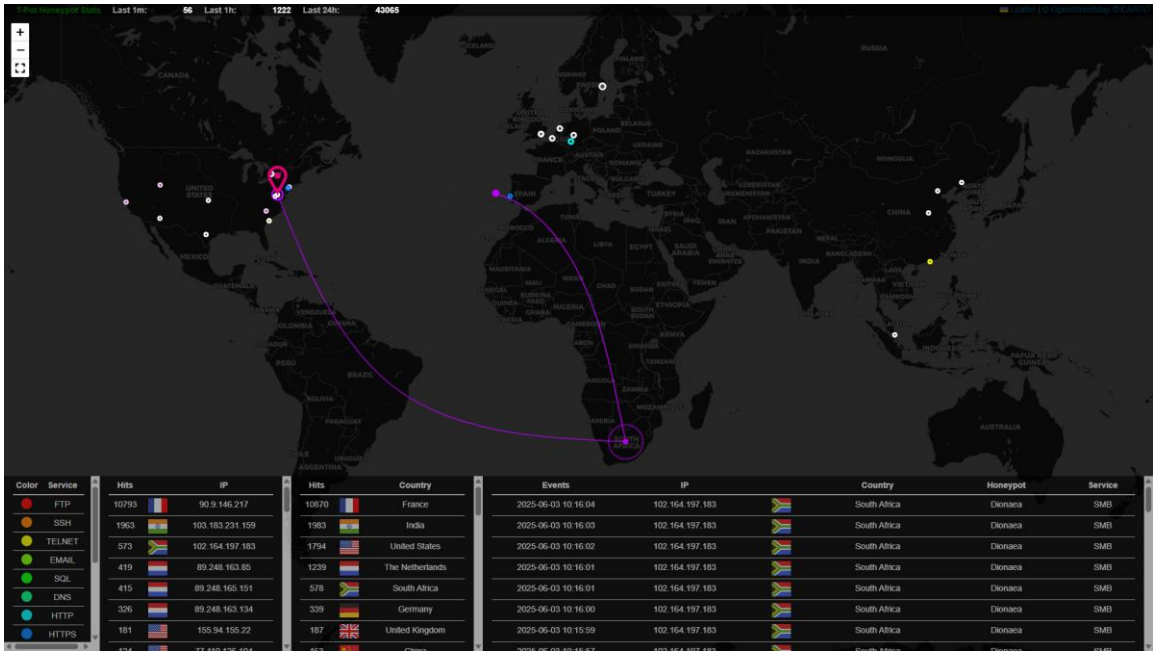

図 1：アタックマップ表示例

図 2：ダッシュボード表示例

2.2 システム構成

本ハニーポット環境は、「T-Pot」と呼ばれる複数のハニーポットを統合したプラットフォームを用いて、AWS 上に以下の構成で構築されている。

クラウド環境：Amazon EC2™（us-east-1 リージョン）
インスタンスタイプ：t3.xlarge（vCPU×4、RAM 16GB）
ストレージ：Amazon EBS™（256GB SSD）
OS ディストリビューション：Ubuntu®
T-Pot バージョン：Hive エディション
ネットワーク構成：

VPC：他用途のインスタンスが存在しない専用 VPC を利用
サブネット：インターネット接続を可能とするパブリックサブネットに設置
セキュリティグループ：
インバウンドルール:

TCP ポート 64295（SSH）：管理者のグローバル IP アドレスからのみ許可
TCP ポート 64297（Web 管理 UI）：管理者の IP からのみ許可
TCP/UDP ポート 0-64000：すべての IPv4（0.0.0.0/0）に対して開放（攻撃観測用）

アウトバウンドルール:

TCP ポート 443（HTTPS）：すべての IPv4（0.0.0.0/0）に対して許可
（T-Pot の同期・アップデート用途）

2.3 配置・運用ポリシー

本ハニーポット環境は、観測対象である攻撃トラフィックを安全かつ効率的に収集・分析するため、適切なネットワーク分離と厳格なアクセス制御を基本方針として構築している。

ネットワーク分離方法：

ハニーポットは、専用の VPC およびパブリックサブネット上にインスタンスを配置している。ネットワークを完全に分離、独立することで、万が一の侵害時にも被害範囲を限定できるようにしている。

アクセス制御方法：

セキュリティグループの設定においては、SSH（64295/TCP）接続を管理者の IP アドレスのみに限定している。また、Web 管理画面および SSH 接続はすべて自身の IP アドレスに制限し、不要なアクセスリスクを排除している。さらに、アウトバウンド通信は HTTPS のみに制限することで、もし攻撃者に使われた場合でも、別の攻撃に悪用されないようにしている（図 3）。

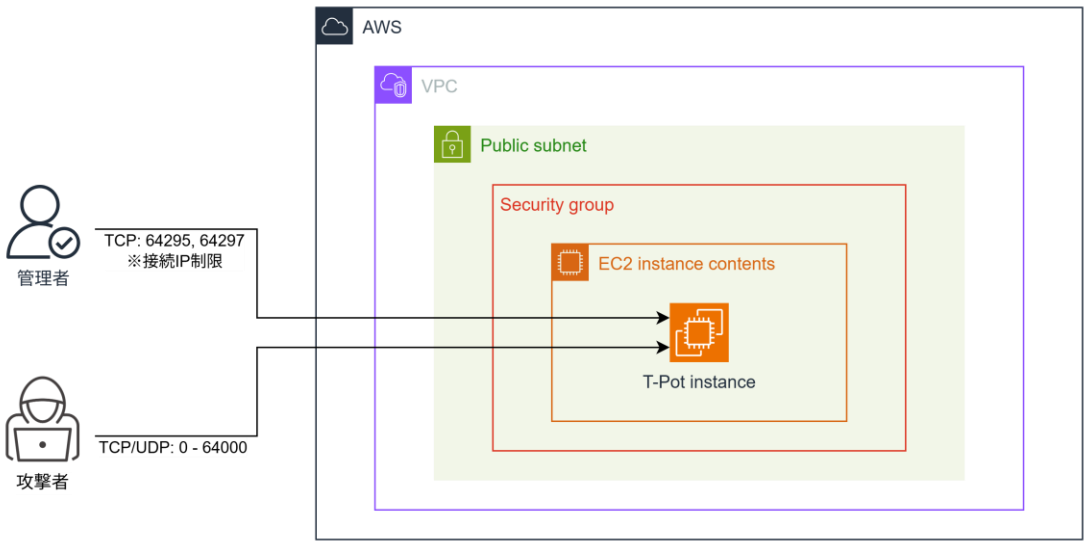

図 3：AWS 上のハニーポット配置構成図

3. 観測された攻撃の概要

T-Pot 環境において稼働する複数のハニーポットに対し、外部から多数の不正アクセス試行が観測された。
以下に、ハニーポット別に観測された主な攻撃内容と傾向をまとめる。

集計期間：2025/6/1～2025/6/7

3.1 総アクセス数と攻撃件数

ハニーポット名	概要	受付サービス	攻撃件数
Honeytrap	任意ポートの接続を検知 稼働サービスの収集	任意ポート(TCP/UDP)	218,475
Dionaea	マルウェア収集	SMB(445), HTTP(80), FTP(21)など	94,595
Ciscoasa	Cisco®機器の脆弱性を模倣	SNMP(161), Telnet(23)など	34,533
Sentrypeer	P2P ボットの通信を検知	P2P 通信(UDP など)	26,522
Cowrie	SSH/Telnet の操作記録	SSH(22), Telnet(23)	16,940
Redishoneypot	Redis の不正操作を記録	Redis(6379)	2,890
Mailoney	メールサーバを模倣	SMTP(25, 587)	1,817
H0neytr4p	Web 攻撃やスキャンを検知	HTTP(80), HTTPS(443)	1,624
Tanner	Elasticsearch 攻撃を検知	Elasticsearch(9200)	1,421
ConPot	SCADA 機器を模倣	Modbus(502)など	946
Adbhoney	ADB の不正操作を記録	ADB(5555)	673
Heralding	認証試行を記録 （RDP/FTP など）	RDP(3389), FTP(21)など	513
Miniprint	プリンタ機器を模倣	LPD(515), JetDirect(9100)	403
ElasticPot	Elasticsearch の模倣	Elasticsearch(9200)	135
Honeyaml	YAML プロトコルを模倣	HTTP ベース(カスタム)	129
合計			401,616

表 1 ハニーポット別攻撃件数

3.2 主な SSH アクセスユーザ名（上位 30 ユーザ）

No	ユーザ名	件数
1	root	576
2	sa	66
3	oracle	52
4	admin	48
5	mssqla	47
6	usera	37
7	user	28
8	es	26
9	test	25
10	git	24
11	pi	23
12	gitlab	22
13	guest	22
14	app	21
15	mysql	21
16	esuser	20
17	www	20
18	ftpuser	19
19	hadoop	19
20	postgres	19
21	flask	18
22	GET / HTTP/1.1	17
23	nginx	17
24	wang	17
25	deploy	16
26	lighthouse	16
27	tomcat	16
28	Accept-Encoding: gzip	15
29	dev	15
30	dolphinscheduler	15

表 2 ユーザ別 SSH アクセス件数

3.3 主な SSH アクセスパスワード（上位 30 パスワード）

No	パスワード	件数
1	123456	235
2	(empty)	89
3	password	57
4	123	54
5	Password	38
6	Admin	35
7	abc123	31
8	User	25
9	Default	19
10	1	18
11	Pass	18
12	pass1234	17
13	12345678	16
14	1234	15
15	Accept: */*	14
16	Raspberry	13
17	111111	12
18	12345	12
19	Ubuntu	12
20	1qaz@WSX	11
21	!QAZ@WSX	10
22	1002	10
23	1qazXSW@	10
24	Hive	10
25	Nginx	10
26	Ubnt	10
27	!Q2w3e4r	9
28	Centos	9
29	Git	9
30	qwe123	9

表 3 パスワード別 SSH アクセス件数

3.4 主な攻撃サービス（上位 5 サービス）

No	サービス名	サービスの説明	ポート番号	攻撃件数
1	SMB	ファイル共有用	445	93,300
2	SIP	VoIP 通話制御	5060	26,504
3	Telnet	平文リモート接続	23	3,539
4	Redis	インメモリデータベース	6379	2,856
5	SSH	暗号化リモート接続	22	1,999

表 4 サービス別攻撃件数

3.5 主な攻撃国（上位 10 国）

No	国	攻撃件数
1	カナダ	129,644
2	アメリカ合衆国	64,353
3	シンガポール	48,575
4	インド	24,950
5	フランス	24,336
6	オランダ	12,535
7	ブラジル	11,933
8	スウェーデン	11,203
9	中国	10,057
10	パキスタン	6,331

表 5 国別攻撃件数

3.6 主な攻撃ネットワーク（上位 10 ASN）

No	AS	ASN	国	攻撃件数
1	16276	OVH SAS	フランス	137,706
2	132203	Tencent Building, Kejizhongyi Avenue	中国	46,968
3	215540	Global Connectivity Solutions Llp	インド	34,270
4	210644	Aeza International Ltd	ロシア	12,919
5	3215	Orange	フランス	11,058
6	10429	TELEFONICA BRASIL S.A	ブラジル	11,051
7	45820	Tata Teleservices ISP AS	インド	10,967
8	202425	IP Volume inc	ルーマニア	10,829
9	9829	National Internet Backbone	インド	7,773
10	14061	DIGITALOCEAN-ASN	アメリカ	6,615

表 6 ネットワーク別攻撃件数

4. 攻撃試行分析から推察される攻撃者の意図とは

本章では、ハニーポットから収集したログを基に、ハニーポット利用傾向、ポート利用傾向、攻撃国の傾向と利用ネットワークの実態について総合的に分析を行った。

4.1 攻撃対象となったハニーポット分析

まずハニーポットのログ解析から、Honeytrap および Dionaea への接続が大多数を占めており、稼働サービスの偵察活動および攻撃対象への感染活動を目的としていることが確認された。また、遠隔操作のための暗号化プロトコルである SSH を模倣するハニーポット Cowrie においては、総当たり方式による認証情報の繰り返し試行が多数観測され、不正ログインを狙った総当たりで全てのパスワードを試行するブルートフォース攻撃の痕跡が顕著であった（表 1）。

認証情報に関するログでは、「root」「sa」「oracle」といった典型的な管理者アカウントへのログイン試行が多数記録され、パスワードに関しても「123456」「abc123」「空白（empty）」等、極めて単純な文字列が多く用いられていることが確認された（表 2, 表 3）。

4.2 攻撃試行の分析

次に攻撃対象ポートに関する分析においては、TCP 445（SMB）への接続要求が顕著に多く観測され、依然としてランサムウェア（Wannacry）の攻撃に使われた SMB の脆弱性（EternalBlue）をはじめとする既知脆弱性が攻撃者に活用され続けている実態が明らかとなった。加えてリモートログイン用プロトコルである TCP 22（SSH）および TCP 23（Telnet）に対して多数の接続要求が観測されており、攻撃者による不正ログインの試行とみられるアクセスの痕跡が確認された（表 4）。

4.3 攻撃国とネットワーク分析

攻撃国分析から、攻撃国は特定の地域や国家に限定されることなく、カナダ、アメリカ、シンガポール、インド、フランスが上位 5 か国を占めている（表 5）。

なお、アメリカ合衆国を除く各国においては、特定の IP アドレスから発せられた一時的かつ集中的な攻撃が主因であるのに対し、アメリカ合衆国からの攻撃は不特定多数の IP アドレスを用いた断続的な攻撃活動が特徴的である。

攻撃者が利用していたネットワークの分布を分析した結果、OVH®（フランス）、Tencent®（中国）、GCS LLP（インド）、Aeza（ロシア）など、グローバルに展開するクラウドおよびホスティング事業者が多数確認された。これにより、正規のプロバイダーが攻撃の中継点として悪用されている実態が明らかとなった（表 6）。

4.4 攻撃手法のまとめ

これまでの分析結果から、観測された攻撃は大きく 5 つの手法に分類される。それぞれの攻撃には明確な目的があり、標的とされるサービスやプロトコルも多岐にわたる。

以下に、観測された攻撃手法の分類と特徴を表形式で整理する（表 7）。

分類	攻撃目的	主な手法	対象サービス・環境
① 無差別スキャン型	脆弱なサービスの発見	全ポートへの接続試行、SIP/Redis スキャン	任意 TCP/UDP, SIP(5060), Redis(6379)等
② SMB 脆弱性型	既知脆弱性の利用による侵入	SMB プロトコルへの接続と脆弱性試行	SMB (445/TCP)
③ SSH ブルートフォース型	不正ログイン／管理者権限の奪取	辞書攻撃・総当たり	SSH (22/TCP)、Telnet (23/TCP)
④ クラウド踏み台活用型	攻撃の匿名化／回避	VPS やクラウドインスタンスを短期使用	全サービス（共通）
⑤ クレデンシャルスタッフィング型	過去漏洩情報の再利用	漏えいした ID とパスワードを使ってログイン	SSH, FTP, RDP など

表 7 攻撃手法まとめ

これらの攻撃手法の多くは、自動化されたツールやボットネットを通じて実行されており、攻撃者の意図としては「侵入可能な環境の効率的なスクリーニング」と「一度の突破による広範な影響の獲得」が見て取れる。また、クラウドインフラの活用により、攻撃元が動的に変化し追跡を困難にしている点は、近年の傾向として注目される。

本分析から、攻撃者は特定のサービスや構成を標的にするというよりも、「設定ミス」や「対応の遅れ」といった脆弱な環境の存在そのものを狙っており、セキュリティ対策の有無によって被害の可否が大きく左右されることが読み取れる。

5. なぜ攻撃者は SSH を狙うのか？

頻度上は第 5 位にとどまった SSH への攻撃試行であるが、リモート管理の中核を担うプロトコルである点から、インフラへの影響度や攻撃成功時の被害規模を鑑みその詳細に注目する。本章では、SSH が攻撃者にとって格好の侵入経路とされる要因について考察する。

5.1 SSH が狙われる技術的背景

まず SSH が攻撃者に狙われる要因として技術的要因を挙げることができる。

SSH は暗号化通信を提供するリモート管理用の標準プロトコルとして広く利用されており、インターネット上には常時多数の SSH サービスが公開されている。これにより、攻撃者にとっては発見しやすく、継続的に標的とされやすい状況が生じている。

さらに、総当たりで全てのパスワードを試行するブルートフォース攻撃、よく使われるパスワードのリスト（辞書）を使って試す辞書攻撃、他サイトから流出した ID とパスワードを使ってログインを試すクレデンシャルスタッフィング攻撃といった手法は高度に自動化されており、汎用ツールを用いて数十万件規模の認証情報を短時間で試行することが可能である。加えて、漏洩した認証情報の流通もこうした攻撃の成功率を押し上げており、SSH は依然として高リスクな攻撃対象と位置づけられている。

5.2 SSH が狙われる運用的背景

前章で技術的要因を述べたが、これに加えて、SSH が狙われるもう一つの重要な要因として運用面の不備が挙げられる。

SSH 自体は本来堅牢なプロトコルであるが、多くのシステムでは、初期設定のまま root ログインが許可され、平易なパスワードが放置されている。特に IoT 機器や小規模クラウド環境では、管理が甘く、脆弱な認証情報が残されたまま運用されがちである。実際に本調査のハニーポットでは、「root」「admin」などに対し「123456」「password」などの試行が多数観測された。

さらに、SSH の公開に対するアクセス制御の不備も散見される。インターネット上に SSH ポートを公開したまま、連続でログインに失敗した相手の通信をブロックする仕組み等の対策を実施していない環境では、攻撃者が低リスクで継続的に認証突破を試みることが可能である。

5.3 SSH 侵害における攻撃者の戦略的動機

SSH に対する攻撃が集中するもう一つの重要な要因として、突破後に得られる管理者権限の価値が極めて高い点が挙げられる。

SSH の認証を突破しシェルアクセスを獲得した攻撃者は、システム設定の改ざんやマルウェアの設置、ログ改ざんなど痕跡隠蔽行為を行うとともに、内部ネットワークへの横展開を実施し、他のシステムや機密情報へのアクセス権を拡大することが可能となる。

このように、多様かつ高度な操作が許容されることから、SSH 認証突破は攻撃者にとって非常に大きな利得となり、攻撃対象としての優先度を高める要因となっている。

6. 脅威に対する技術的対策

SSH に対する攻撃は、その設計上および実装上の構成的な弱点に加え、組織の運用体制や認証管理の甘さを突いたものである。このような脆弱性は、SSH に限らず他のサービスやプロトコルにおいても類似して観測される傾向にある。したがって、対策を検討するにあたっては、SSH 特有の問題に加えて、サイバー攻撃全般に共通する課題への対応を視野に入れる必要がある。本章では、こうした横断的な観点から、有効なセキュリティ対策について技術的な提言を行う。

6.1 初期段階での不要なアクセス遮断

1 点目の対策としては初期段階での不要なアクセス遮断である。

サイバー攻撃の多くは無差別スキャンや自動化された接続試行から始まるため、初動段階で不要なアクセスを遮断することが重要である。具体的には、SSH などの重要サービスに対し、信頼できる接続元だけを許可するホワイトリスト方式で制限するほか、ファイアウォールの通信制御を厳格化し、不要なポートやサービスを閉鎖する構成管理が必要である。ハニーポットでの観測結果からも分かる通り、外部に公開する必要のないポートの開放は、攻撃者による探索の格好の標的となる。

6.2 認証強度の強化と最小権限運用

2 点目の対策は、認証と権限管理の強化である。

SSH 攻撃では、パスワード認証のままでは総当たり攻撃のリスクが高いため、公開鍵認証への移行が基本となる。root による直接ログインは禁止し、一般ユーザ＋sudo の運用で被害拡大を防ぐ。加えて、多要素認証（MFA）を導入すれば、認証情報漏洩を前提とした防御も可能となる。

管理アカウントは必要最小限に絞り、権限も業務に応じた最小限とすることで、内部不正や誤操作のリスクを抑えられる。これらは、侵入リスクの低減と被害最小化に有効な対策である。

6.3 能動的セキュリティ防御の実装

3 点目の対策は、製品導入による能動的な防御手法の実装である。

昨今、サイバー攻撃はますます巧妙かつ複雑になっており、従来の署名ベースのアンチウイルスやファイアウォールのみでは、すべての脅威を検知・防御することは困難である。

この課題への解決策として、ネットワークの異常を AI で検知し、必要に応じて自動で対処する仕組み NDR（Network Detection and Response）の導入が有効である。NDR は、ネットワークトラフィックを常時監視し、機械学習や異常行動分析により不審な通信を検知・可視化するほか、一部製品では遮断や隔離といった自動対処も可能である。これにより、初動から封じ込めまでを想定した多層防御体制を構築できる。

6.4 セキュリティギャップの早期是正

4 点目の対策はセキュリティギャップの早期是正である。

多くのサイバー攻撃では既知の脆弱性や設定ミスといったセキュリティギャップが狙われる。そのようなセキュリティギャップを早期発見し是正するには脆弱性診断の実施が最適である。脆弱性診断の実施によって、人為的に発見が困難な脆弱性や設定ミスを技術的に検知および可視化することで、対応すべき箇所を的確に特定し、優先順位を踏まえた迅速な修正措置を実施できる。結果として、攻撃者の侵入経路を段階的に封鎖し、システム全体のセキュリティ強化に寄与することが期待される。

6.5 セキュリティ対策の整理

ハニーポットの観測結果と技術的対策を以下の表に整理する（表 8）。

分類	攻撃目的	主な手法	有効な技術的対策（主な対応）
① 無差別スキャン型	脆弱なサービスの発見	全ポートへの接続試行、SIP/Redis スキャン	不要ポートの閉鎖（明示的許可制） IP 制限による接続元制御 CSPM によるクラウド設定監査
② SMB 脆弱性型	既知脆弱性の利用による侵入	SMB プロトコルへの接続と脆弱性試行	ポート 445 の遮断（非公開） SMB バージョン制限または無効化 定期的な脆弱性スキャンとパッチ適用
③ SSH ブルートフォース型	不正ログイン／管理者権限の奪取	辞書攻撃・総当たり	パスワードログインの無効化（鍵認証へ） root ログインの禁止 Fail2Ban による遮断 MFA 導入
④ クラウド踏み台活用型	攻撃の匿名化／回避	VPS やクラウドインスタンスを短期使用	ASN/IP 単位での通信制限・ブロック NDR での異常挙動検知＋遮断 定期的な攻撃元 IP リストの更新と封じ込め
⑤ クレデンシャルスタッフィング型	過去漏洩情報の再利用	組合せ試行（ID+パス）	パスワード強度ポリシーの徹底 二要素認証の適用（RDP/FTP 含む） ログ監視と自動ロック機構（ログイン試行回数制限）

表 8 有効な技術的対策まとめ

7. 脅威に対する人的対策

前章では技術的な観点から有効なセキュリティ対策を提言したが、対策を十分に機能させるためには運用的な視点からの対策も不可欠である。そこで本章では、有効なセキュリティ対策について運用的な提言を行う。

7.1 従業員教育

運用的対策の 1 点目は従業員教育である。

情報セキュリティ対策において、人的要因への対応は技術的施策と同様に重要である。特に、推測可能なパスワード設定をはじめとした人的脆弱性は不正ログインの主要な原因であり、技術的防御だけでは十分に対処できない。そのため、複雑性を保ったパスワード管理の重要性、メールの安全な取り扱い、適切な端末管理、さらにサイバー攻撃の最新動向や手口の理解を含めた継続的な教育を通じて、従業員のセキュリティ意識を高め人的脆弱性の低減を図る必要がある。

7.2 セキュリティポリシーの策定と継続的な見直し

2 点目はセキュリティポリシーの策定と継続的な見直しである。

組織全体として一貫したセキュリティ対応を実現するため、基本方針や実施基準を定めた情報セキュリティポリシーの策定と運用が必要不可欠である。ポリシーには、アクセス権限管理、機密情報の分類と取扱い、端末利用、外部媒体持ち込み、クラウドサービス利用、インシデント対応など、業務のあらゆる側面を想定した明文化が不可欠である。

策定後は、全職員への周知徹底を図り、理解度を定期的に確認する仕組みを整備すべきである。また、技術環境や法制度の変化、インシデントの教訓を反映した定期的な見直しを通じて、形骸化を防ぎ、常に最新のリスクに対応可能な体制を維持する必要がある。

7.3 ログ管理と異常検知体制の整備

3 点目はログ管理と異常検知体制の整備である。

サイバー攻撃への対応においては、侵入を防ぐ“入り口対策”に加え、侵入後の不正な通信や情報漏えいをいち早く察知する“出口対策”が不可欠である。その基盤となるのが、各種ログの適切な取得・分析と、それを支える異常検知体制の構築である。具体的には、システムや認証、ネットワーク機器等のログを集中管理し、セキュリティ異常を見つけるツールによる自動分析を行うだけでなく、アラート対応の運用体制の整備が求められる。これにより、侵入の早期発見と被害拡大の防止、さらには事後対応の迅速化が実現可能である。

8.まとめ

本レポートでは、外部からの不正アクセスを誘い出す仕組みであるハニーポットを用いて、実際に行われているサイバー攻撃の傾向を分析した。その結果、古い脆弱性を狙った攻撃や、安易な ID・パスワードでのログインを試みる行為が今も多く見られた。

攻撃は特定の地域に限らず、世界中のさまざまな IP アドレスから仕掛けられていた。中でも OVH や Tencent といったクラウドサービス経由の通信が目立ち、誰でも容易に攻撃に加われる時代であることがうかがえる。さらに、短時間に集中するログイン試行や不自然なポートへの接続も確認され、異常な兆候を早く察知する視点の重要性が浮き彫りとなった。

対策としては、アクセス制御やパスワード管理など基本的なセキュリティ対応の徹底が第一である。さらに、NDR のような異常検知して対応する仕組みや、定期的な脆弱性診断、社員のセキュリティ意識の向上も重要な要素となる。

サイバー攻撃は日々進化しており、「自分たちは大丈夫」と油断せず、平時から備えを重ねていくことが求められる。

9. 連絡先・問い合わせ先

PACIFIC サイバーセキュリティ研究所
Email：seclab@pacific-systems.co.jp
電話番号：048-845-2244