付録

見えないアタックサーフェス：データセンター周辺で露出する数千台の産業用制御システム

付録A

調査方法の概要

データ収集

米国内1,063か所のデータセンターのGPS座標から半径1km以内を対象に、Shodan APIでICSプロトコルを検索

BACnet | 47808　Modbus | 502　Fox/Niagara | 1911　EtherNet/IP | 44818

S7 | 102　DNP3 | 20000　OPC-UA | 4840

フィルタリング工程

1. **ベースライン判定** — 有効なIP 10文字以上 米国内のみ
2. **Tier 1 ASNブラックリスト** — クラウド／VPS／調査機関のASNを強制除外
3. **プロトコル検証** — ポート固有のフィンガープリントを照合
4. **複数ポートによるハニーポット検出** — ICSポート6個以下／IP
5. **信頼度スコアリング** — 0〜10点

主要なスコアリング要素

Shodanのtag:ics	+4.0点
有効なプロトコル応答	+3.0点
HVAC／データセンター関連用語	+1.0〜+4.0点
既知ベンダーのキーワード	+1.0〜+2.0点
法人向けISP	+0.5〜+1.0点

責任ある情報開示

全体を通じて一部を匿名化しました。例示したIPアドレスは伏せ、個別施設の名称は一般化しています。Shodanによる受動的スキャンの範囲を超えるエクスプロイトや能動的な調査は行っていません。

安全上および倫理上の理由から、デバイスのポートを直接調査していません。

本リサーチの主な目的は、特定の組織を標的とすることではなく、業界全体にかかわる問題への体系的な認識を高めることです。

付録B

Shodanデータのフィルタリング

本節では、最初に取得した73,847件のレコードをどのように絞り込み、実在する運用技術（OT）をそれ以外のデータから識別したのか、その方法を詳しく説明します。

レイヤ1：ASNの強制除外

最初に適用した最も厳しいフィルタは、自律システム番号（ASN）のブラックリストです。物理インフラを制御する実在のICSデバイスが、クラウドプラットフォームやVPSホスティングで稼働することは、ほとんどありません。データセンターの冷却システムを管理するビルディングオートメーションコントローラがAmazon Web Services（AWS）やDigitalOcean上に置かれることはなく、通常はサーバ室や機械室から、地域の法人向けISPまたは企業ネットワークに接続されています。

段階的な除外方式を実装しました。

Tier 1（強制除外 - ハニーポット確率90%超）： ほかに正当性を示す要素があっても、該当するASNはスコアリング前にすべて除外しました。AWS上のデバイスがBACnetへ完全に応答し、Shodanの「tag:ics」が付与されていても除外対象です。

- **主要クラウドプラットフォーム：** Amazon AWS、Microsoft Azure、Google Cloud、Oracle Cloud、Alibaba Cloud、Cloudflare
- **VPS／ホスティング事業者：** DigitalOcean、Contabo、OVH、Hetzner、Linode、Vultr、Scaleway、Leaseweb、M247、およびそのほか15社以上
- **既知の調査／ハニーポットネットワーク：** Shadowserver Foundation、GreyNoise Intelligence、AlphaStrike Labs。いずれも攻撃者の行動を調査するため、意図的にハニーポットを運用している組織です

結果：2,143台を除外。 このフィルタだけで、スコアリング開始前に明らかな誤検出を取り除けました。冷却設備を管理する実在のBACnetコントローラが、月額5米ドルのVPSインスタンスで稼働することはありません。

Tier 2（強い疑い - ハニーポット確率60〜90%）： 強制除外はしていませんが、該当するASNには大きな減点（-2.0〜-3.0点）を適用しました。低価格ホスティング事業者（Psychz Networks、QuadraNet）、海外のVPSサービス、複数用途のコロケーション施設などが含まれます。有効なプロトコル応答、Shodanのtag:ics、HVAC関連バナーなど、正規デバイスであることを強く示す要素が確認できれば、こうしたネットワーク上のデバイスも高信頼度に分類される可能性があります。

Tier 3（要検証 - 正規の可能性はあるが確認が必要）： Comcast Business、Cox Business、AT&T Business、Spectrum Businessなどの法人向けISPには、中立またはわずかな加点（+0.5〜+1.0点）を適用しました。施設では、企業向け専用回線ではなく地域の法人向けISPをBAS接続に使う場合が多いため、こうしたネットワークには正規のデータセンター向けビルディングオートメーションシステムが存在します。

レイヤ2：プロトコル検証

ICSの各ポートには、想定されるプロトコルフィンガープリントがあります。ポート47808から応答があっても、BACnetが稼働しているとは限りません。そのポート番号を偶然使用しているHTTPサーバ、SSHサービス、VPNエンドポイントの可能性もあります。

BACnet（ポート47808）では検証が必須： 応答内にvendor_idフィールド、device_instance番号、またはBACnetオブジェクトタイプ（analog-input、analog-output、binary-value）が含まれているかを確認します。「vendor_id: 15」（Johnson Controls）や「vendor_id: 95」（Tridium）に加えて、「Zone Temperature」や「Supply Fan Status」といったオブジェクト名がバナーに含まれていれば、実在するデバイスと判断できます。

DNP3（ポート20000）の検証が最も困難でした。 ポート20000はVPNコンセントレータ、ネットワーク管理インターフェース、その他の非ICSサービスでも広く使われるため、誤検出率は約90%に達します。そこで、次の厳格な検証を実施しました。

- TLSハンドシェイク（応答内の\x15\x03または\x16\x03バイト列）を検出して除外
- Telnet／ルータのプロンプト（「Welcome to CLI」「Password:」「Login:」「Username:」）を除外
- VPNポータル（GlobalProtect、Cisco AnyConnect、Palo Alto）を除外
- 実際のDNP3プロトコルを示す情報（「outstation」「master station」）と、裏付けとなるShodanタグの両方を必須化

結果：DNP3の誤検出は543台から4台へ減少（99.3%減）。 当初はデータセンター周辺に数百台のSCADAシステムがあるように見えましたが、その大半はVPNコンセントレータとネットワーク機器でした。残った4台のDNP3デバイスには、正規のSCADAに見られる特徴が確認されました。

レイヤ3：最も確実な基準 - Shodanのtag:ics

正規のICSデバイスを示す最も信頼性の高い要素は、Shodan独自のtag:ics分類です。Shodanがこのタグを付与した場合、スキャナがプロトコルレベルのハンドシェイクを正常に完了し、そのデバイスが実際の産業用制御プロトコルを使用していると検証したことを意味します。単なるポート照合ではありません。各プロトコルを理解するエンジニアが管理するICS専用スキャンモジュールによって、詳細なプロトコル検証が行われています。

信頼度スコアリングでは、tag:icsに+4.0点を付与しました。これは単一要素として最大の加点です。「bacnet」や「modbus」などプロトコル固有のタグと組み合わさる場合は、基本の+4.0点に加算せず、置き換える形で合計+5.0点としました。この要素だけで、結果が「中信頼度」から「高信頼度」へ自動的に引き上げられる場合があります。クラウドホスティングなど、判定を覆す別の警告要素がない限り、ShodanがICSと判定した結果を信頼しています。

レイヤ4：複数ポートによるハニーポット検出

ハニーポットは、攻撃者や調査担当者を引きつけるように設計されています。接触機会を最大化するため、一般に1つのIPで多数のサービスを公開します。一方、実在のICSデバイスが稼働させるのは、その固有の機能に必要なサービスだけです。ICSプロトコルのスキャン結果をもとに、各IPアドレスが公開しているポートの総数を分析しました。

- **公開ICSポートが1〜3個：** 専用デバイスとして現実的。HTTP管理インターフェースを備えたBACnetコントローラなど（+1.0点）
- **公開ポートが4〜6個：** 複数の管理インターフェースを備えた実在のデバイスである可能性あり（加点・減点なし）
- **公開ICSポートが6個超：** 強い疑い。実在のデバイスがこれほど多くのプロトコルを使用することはまれ（-2.0〜-4.0点）
- **公開ポートが10個超：** ほぼ確実にハニーポット（完全に除外）

考え方は単純です。実在のBACnet HVACコントローラが、Modbus、S7、DNP3、EtherNet/IP、OPC-UAを同時に実行することはありません。1台のノートPCでWindows、macOS、Linux、FreeBSD、Solarisを同時に動かしているようなものです。技術的には可能でも、現実には考えにくい構成です。6種類を超えるICSプロトコルが確認されたデバイスは、ハニーポットとして判定しました。公開ICSポートが5個を超えるホストは17台あり、いずれもハニーポットの特徴を示していました。

レイヤ5：信頼度スコアリングアルゴリズム

強制フィルタを通過したデバイスには、複数の要素を組み合わせた包括的なスコアリングを実施しました。各デバイスは中立となる5.0点から開始し、さまざまな要素に基づいて加点または減点します。

要素	スコアへの影響	根拠
法人向けISP	+0.5〜+1.0	Verizon Business、AT&T Business、Cox Business
住宅向けISP	-1.0	実際のデータセンターインフラが家庭用回線に接続されることはない
有効なプロトコル応答	+3.0	想定ポートで正しいプロトコルが応答
ポート上の誤ったプロトコル	-3.0	BACnetポート上のHTTP、Foxポート上のSSH
Shodanのtag:ics	+4.0	最も確実な基準 - Shodanが検証したICSデバイス
tag:ics + プロトコルタグ	+5.0	二重検証
HVAC／BASキーワード	+1.0〜+2.0	「AHU」「chiller」「cooling tower」「VAV」
データセンター関連キーワード	+2.0〜+4.0	「data center」「UPS」「CRAC」「PDU」
既知ベンダーを示す文字列	+1.0〜+2.0	Tridium、Delta Controls、Carrier、Trane

表1. 複数要素によるスコアリング方式

最終分類のしきい値：

- **7.0以上：高信頼度** - 主要分析に採用（6,300台）
- **5.0〜6.9：中信頼度** - 手動確認を推奨（791台）
- **3.0〜4.9：低信頼度** - 誤検出の可能性が高い（100台）
- **3.0未満：除外** - ほぼ確実にハニーポットまたは設定不備

フィルタリング結果：73,847件から6,300件へ

フィルタ段階	レコード数	残存率
Shodanの未処理レコード	73,847	100%
重複排除とベースライン判定後	14,510	19.6%
Tier 1 ASNブラックリスト適用後	12,367	16.7%
プロトコル検証後	7,191	9.7%
高信頼度（7.0以上）	6,300	8.5%

表2. フィルタリング結果