

インターネット公開資産 観測報告書（2026年9月26日版・第1回）

Sep 26, 2026 ・ @矢又小次郎

1. はじめに

この報告書は、インターネット上で誰でも外から見える状態になっている機器・サーバー（以下「公開資産」）を、外部のインターネット観測サービスのデータを使って調べ、その結果を一般の方にも読める形でまとめたものです。

今回は**第1回目の観測**です。本来この仕組みは「前回と比べて何が増えたか・消えたか・変わったか」を見ることで真価を発揮しますが、第1回には比較対象がありません。そのため本報告書では、変化の評価は行わず、「**現時点で何が見えているか**」という**基準点（ベースライン）の記録**に徹します。第2回以降は、この結果との比較で変化を報告します。

本報告書を読む上で大切な前提が3つあります。

1. **ここに載っていることは「怪しい」という意味ではありません。** 観測システムが機械的なルールで「人が確認すべき候補」を選んだだけで、悪意があると確定したものは一つもありません。
2. **情報の出どころ（観測データの提供元サービス名）は非公開**としています。データは、インターネット全体を定期的に調べている民間の観測サービスから取得した公開情報です。
3. **個別の機器が特定されないよう、IPアドレスの末尾などを伏せてあります**（詳しくは第7章）。

観測日：2026年9月25日（データ収集）／報告書作成：2026年9月26日

2. 要点のまとめ（3分で読める版）

- 今回、58件の公開サービス（53台のサーバー・機器）を記録しました。所在国の内訳はチリ42件、ペルー8件、シンガポール4件、オランダ3件、不明1件で、南米（特にチリ）に偏っています。これは観測の「探し方（検索条件）」をチリ周辺に絞ったためで、世界全体の傾向を示すものではありません。
- 最も目立ったのは、**2台のサーバーがまったく同じ「身分証明書」（TLS証明書）**を使っていた点です。別々の通信事業者のネットワーク上にある2台が同じ証明書を持つのは、同じ人・同じ組織が運用している可能性を示唆します。システムはこの2件を最優先の「即調査」に分類しました。
- 50050番という特定の出入口（ポート）を開けた機器が19件ありました。この番号は、ある有名な攻撃演習用ツールが初期設定で使う番号として知られています。ただし、番号が同じというだけでは何も確定しません。

- ・ 遠隔操作の入口（RDP）をインターネットに直接さらしている機器が20件ありました。これは攻撃されやすい状態であり、機器の持ち主にとってのリスクです（持ち主が加害者という意味ではありません）。
- ・ 自動判定で「人が確認すべき」とされた候補は10件（即調査2件、観察8件）です。現時点で悪意ある活動と確認されたものはありません。
- ・ 第1回のため「変化」はまだ評価できません。次回以降の比較の基準点として本結果を保存します。

3.用語解説（先に読むと本文がわかりやすくなります）

用語	ひとことと言うと	たとえ話
IPアドレス	インターネット上の機器の「住所」。例：203.0.113.10	家の住所
ポート（番号）	1台の機器にある「出入口」の番号。用途ごとに決まった番号が使われることが多い（Webは80番・443番、遠隔操作は3389番など）	建物の「何番窓口」
公開資産	インターネット側から誰でも接続を試せる状態の機器やサービス	通りに面して開いている窓口
スキャン／観測	インターネット上の住所と出入口を片端から確認し、何が応答するかを記録すること。今回は民間の観測サービスが記録済みのデータを参照しており、こちらから相手機器に接続はしていません	町内を歩いて、どの窓口が開いているかを地図に書き込む
ASN（AS番号）	インターネット上のネットワークの「管理者番号」。通信会社やクラウド事業者ごとに割り当てられる	住所の「管轄の不動産会社」
クラウド事業者	サーバーを時間貸しする会社。誰でも借りられるため、同じ事業者の中に無関係な利用者が大勢いる	貸しオフィスビル
TLS証明書	暗号化通信（https）で使うサーバーの「身分証明書」。通常はサーバーや組織ごとに別々のものを使う	印鑑証明

用語	ひとことと言うと	たとえ話
証明書の指紋（ハッシュ値）	証明書を一意に識別する長い英数字。同じ値なら同じ証明書	印影
RDP	Windowsを遠隔から操作するための仕組み（通常3389番）。インターネットに直接さらすと、パスワード総当たり攻撃などの標的になりやすい	家の合鍵を玄関先に置いた状態
C2（コマンド&コントロール）サーバー	攻撃者が乗っ取った機器に指示を送るための司令塔サーバー	犯行グループの指令所
攻撃演習用ツール	企業が自社の防御力を試す「模擬攻撃」に使う市販ツール。正規の用途がある一方、犯罪者に悪用されることも多い	訓練用の模擬弾が本物の犯行に転用される
スコア／Tier	観測システムが機械的なルールで付けた「確認の優先度」の点数と区分。Tier1＝即調査、Tier2＝観察。 危険度や有罪の判定ではありません	健康診断の「要再検査」の印
要調査キュー	スコアの高い順に並べた「人が確認すべき候補」の一覧	再検査の予約リスト
NEW／GONE／MODIFIED	前回と比べて「新たに見えた／見えなくなった／中身が変わった」の区分。第1回は全件がNEW扱いになるため、意味を持つのは第2回以降	前回の地図との書き込みの違い
TP／FP	人が確認した結果、候補が本当に問題あり（TP：真陽性）だったか、問題なし（FP：偽陽性）だったか	再検査で「異常あり」か「異常なし」か

4. 観測の概要

4.1 基本情報

項目	内容
観測回	第1回（比較対象なし）
データ収集日	2026年9月25日
記録件数	58件（サーバー・機器としては53台。1台で複数の出入口を開けているものがあるため）
情報源	民間のインターネット観測サービス1社（名称非公開）
自動判定で選ばれた候補	10件（Tier1 即調査：2件／Tier2 観察：8件）

4.2 国別の内訳

国	件数	割合
チリ	42	72%
ペルー	8	14%
シンガポール	4	7%
オランダ	3	5%
不明	1	2%

※国は「IPアドレスの登録上の所在地」であり、実際に機器を使っている人の国籍や居場所とは限りません。

4.3 出入口（ポート）別の内訳

ポート番号	件数	一般的な用途
3389	20	Windowsの遠隔操作（RDP）
50050	19	標準的な用途は決まっていない番号。攻撃演習用ツールの初期設定として知られる（第5章）
443	7	暗号化されたWebサイト（https）

ポート番号	件数	一般的な用途
80	6	通常のWebサイト（http）
その他（4430／4433／8086／10008／5061／56001）	各1、計6	Web管理画面、IP電話（5061）など様々。個別に確認が必要

この表から、**遠隔操作（3389番）と50050番の2種類だけで全体の約3分の2**を占めていることがわかります。これは観測条件でこれらの番号を重点的に探したためです。

5. 注目点の解説

5.1 【最優先】2台のサーバーが同じ「身分証明書」を共有

何が見えたか：チリの2台のサーバー（200.91.9.x と 216.241.31.x）が、どちらも50050番の出入口で、**完全に同一のTLS証明書**を使っていました。2台は別々の通信事業者のネットワーク（AS7004 と AS18747）に属しています。

なぜ注目するのか：証明書は通常サーバーごとに発行されます。管理者の異なる別々のネットワーク上で同じ証明書が使われている場合、**同じ人物・組織が複数の拠点をまとめて運用している**ことがよくあります。攻撃者が司令塔サーバー（C2）を複数立てる際に、同じ設定を使い回した結果こうなる例も知られています。

ただし：ソフトウェアの初期設定の証明書をそのまま使うと、無関係な機器同士でも同じ証明書になります。また、正規の企業が複数拠点で同じ証明書を使うことも珍しくありません。

「同一人物の運用の可能性がある」という手がかりに過ぎず、悪意の証拠ではありません。システムはこの2件を80点（証明書共有）＋20点（対象国）＝100点、Tier1「即調査」としました。

5.2 50050番の出入口を開けた機器が19件

何が見えたか：50050番を開けた機器が19件あり、ほぼすべてチリでした。うち6件は暗号化通信（https）、13件は通常通信（http）で応答しています。同じ事業者の連番のIPアドレス（4台並び）でまとまって見つかったものが2組ありました。

なぜ注目するのか：50050番は、企業の防御力テストに使われる有名な市販の攻撃演習用ツールが、**操作用サーバーの初期設定として使う番号**として知られています。このツールは犯罪グループ（ランサムウェア集団など）にも広く悪用されてきたため、セキュリティ業界ではこの番号の公開を監視の手がかりにしています。

ただし：ポート番号は誰でも自由に使えます。業務システムや機器メーカーの独自サービスが同じ番号を使っている可能性は十分にあります。特に、**通信会社の同じ区画に連番で並んでいるものは、企業向けの機器が同じ設定で一斉に置かれているだけ、**というケースも考えられ

ます。今回の観測では、これらの機器で「どのソフトが動いているか」は判別できていません（製品名欄は空欄）。

5.3 遠隔操作の入口（RDP）が20件さらされている

何が見えたか：Windowsの遠隔操作機能（3389番）がインターネットに直接公開されている機器が20件、すべてチリで見つかりました。主にチリ国内の複数の通信事業者のネットワーク上にあり、同じ区画に数台ずつ固まっています。

なぜ注目するのか：RDPを直接インターネットにさらすことは、**ランサムウェア被害の代表的な侵入口**の一つとされています。攻撃者は世界中の3389番を自動で探し、パスワードを総当たりで試したり、盗んだパスワードで侵入したりします。

ただし：これらの機器の多くは、一般企業や個人事業者などの「潜在的な被害者側」である可能性が高いと考えられます。攻撃者の拠点という意味ではありません。なお、観測システムの自動判定ではこの20件は「要調査」には選ばれていません（採点ルールがRDP単体の公開には点を付けない設定のため）。

5.4 大手クラウド事業者のネットワーク上の機器

何が見えたか：候補10件のうち8件は、同じ一つのネットワーク（AS136907）上の機器でした。筆者の知識ではこの番号は大手クラウド事業者（Huawei Cloud）のものです（要確認）。所在国はチリ・シンガポール・オランダに分散しています。

なぜ注目するのか：観測システムでは、このネットワークを「重点的に見る対象」に設定しているため、ここで新たに見えた機器には一律35点が付きます。

ただし：クラウドは誰でも借りられる「貸しオフィスビル」です。同じ事業者には属しているからといって、利用者同士は無関係です。**この8件は「事業者が対象リストに入っている」ことだけで点数が付いており、機器そのものに怪しい特徴が見つかったわけではありません。**このため区分は「観察」にとどめています。

そのほか、世界的なWeb配信事業者（Cloudflare）や大手クラウド（Google Cloud）のネットワーク上の機器も含まれています。これらは多数の利用者が共有する設備であり、IPアドレスだけから利用者を特定することはできません。

6. 要調査リストと判定の考え方

6.1 点数の付け方

観測システムは、次のような条件に当てはまるたびに点数を加算し、合計点の高い順に並べます。

条件	加 点	意味
同じ証明書が複数の住所で使われている	80	同一運用者の可能性
重点監視対象のネットワーク上に新しく現れた	35	監視リストに入っている事業者内の新顔
重点監視対象の国に新しく現れた	20	監視対象国の新顔

第1回はすべてが「新しく現れた」扱いになるため、国やネットワークによる加点は**ほぼ全件に機械的に付いています**。次回以降は本当に新しく現れたものだけに付くため、点数の意味がより鮮明になります。

6.2 今回の要調査リスト（10件）

順位	住所：出入口	国	点数	区分	点数の理由
1	200.91.9.x：50050	チリ	100	Tier1 即調査	証明書共有(80)+対象国(20)
2	216.241.31.x：50050	チリ	100	Tier1 即調査	証明書共有(80)+対象国(20)
3	101.44.12.x：443	チリ	55	Tier2 観察	対象ネットワーク(35)+対象国(20)
4	182.160.25.x：50050	チリ	55	Tier2 観察	対象ネットワーク(35)+対象国(20)
5	176.52.142.x：4430	シンガポール	35	Tier2 観察	対象ネットワーク(35)
6	176.52.135.x：8086	オランダ	35	Tier2 観察	対象ネットワーク(35)
7	176.52.140.x：4433	シンガポール	35	Tier2 観察	対象ネットワーク(35)
8	176.52.133.x：56001	オランダ	35	Tier2 観察	対象ネットワーク(35)
9	176.52.142.x：10008	シンガポール	35	Tier2 観察	対象ネットワーク(35)
10	176.52.143.x：5061	シンガポール	35	Tier2 観察	対象ネットワーク(35)

※5位と9位は同じ機器の別の出入口です。3位の機器にはWebサイトの名前（アルゼンチンのドメイン）が付いていましたが、事業者名が推測できるため伏せています。

6.3 人による判定の流れ

リストに載った候補は、担当者が上から順に確認し、次の4つのいずれかに判定します。**現時点ではすべて未判定です**。

- **TP（問題あり）**：悪意ある活動の拠点である裏付けが取れた
- **FP（問題なし）**：正規の業務用サーバーなど、問題ないと判断できた
- **保留**：判断材料が足りず、次回以降の観測を待つ
- **調査中**：追加の確認作業を進めている

判定結果は次回以降の報告書に反映します。

7. この観測の限界と注意事項

- **見えているのは「探したもの」だけです。**今回はチリ周辺と特定の出入口番号に絞って探しました。世界全体やその国全体の状況を表すものではありません。
- **情報源は1社のみです。**観測サービスが記録した時点の情報であり、その後に停止・変更された機器が含まれている可能性があります。第2回以降は複数の情報源を突き合わせて精度を上げる予定です。
- **動いているソフトの名前はほぼ判別できていません。**今回の記録では製品名・バージョン欄がすべて空欄でした。何が動いているかは推測の域を出ません。
- **国やネットワークの情報は登録上のものです。**実際の利用者の所在や国籍を示すものではありません。攻撃者が他国のサーバーを借りたり乗っ取ったりすることはよくあります。
- **この報告書は誰かを告発するものではありません。**掲載した機器の持ち主が攻撃者であると主張するものではなく、多くはむしろ攻撃を受けうる側です。
- **個別の機器の特定を避けるため、IPアドレスの末尾（最後の区切り）を「x」で伏せ、ドメイン名・証明書の指紋の全体は掲載していません。**さらされた遠隔操作の入口の一覧をそのまま公開すると、攻撃者に「狙いやすい標的リスト」を渡すことになるためです。完全なデータは観測者の手元で証跡として保管しています。
- **機器名やネットワーク事業者名についての説明は、筆者の知識に基づく部分を含みます。**正確さを期していますが、公的な確認を経たものではありません。

該当しうる機器の管理者の方へ：遠隔操作（3389番）などをインターネットに直接公開している場合は、VPN経由に限定する、多要素認証を有効にする、不要なら閉じる、といった対策をご検討ください。

8. 付録：全観測一覧（58件・末尾マスク済み）

同じ区画（IPアドレスの最後の区切り以外が同じ）・同じ出入口のものはまとめて件数で表示しています。「raw_tcp」は、応答はあるが通信の種類が判別できなかったものです。

住所（末尾伏せ）	出入口	通信の種類	国	ネットワーク番号	件数
101.44.1.x	80	http	チリ	AS136907	1
101.44.1.x	443	https	チリ	AS136907	1
101.44.12.x	443	https	チリ	AS136907	1
104.18.23.x	443	https	不明	AS13335	1
176.52.133.x	56001	raw_tcp	オランダ	AS136907	1
176.52.135.x	8086	https	オランダ	AS136907	1

住所（末尾伏せ）	出入口	通信の種類	国	ネットワーク番号	件数
176.52.140.x	4433	https	シンガポール	AS136907	1
176.52.142.x	4430	https	シンガポール	AS136907	1
176.52.142.x	10008	https	シンガポール	AS136907	1
176.52.143.x	5061	raw_tcp	シンガポール	AS136907	1
181.78.245.x	50050	http	チリ	不明	1
182.160.25.x	50050	http	チリ	AS136907	1
186.10.110.x	50050	http	チリ	AS27925	1
186.10.46.x	50050	http	チリ	AS27925	1
188.114.97.x	80	http	オランダ	AS13335	1
190.100.131.x	50050	http	チリ	不明	1
190.13.134.x	50050	http	チリ	不明	1
190.98.242.x	50050	http	チリ	AS14259	4（連番）
191.114.97.x	3389	rdp	チリ	AS7418	1
191.116.215.x	3389	rdp	チリ	AS22047	1
191.116.95.x	3389	rdp	チリ	AS22047	1
191.116.98.x	3389	rdp	チリ	AS22047	1
191.119.14.x	3389	rdp	チリ	AS22047	1
191.119.41.x	3389	rdp	チリ	AS22047	1
191.124.123.x	3389	rdp	チリ	AS400619	2
191.124.126.x	3389	rdp	チリ	AS400619	2
191.124.63.x	3389	rdp	チリ	AS400619	1
191.124.7.x	3389	rdp	チリ	AS400619	1
191.124.8.x	3389	rdp	チリ	AS400619	4
191.96.184.x	3389	rdp	チリ	AS270014	4
191.97.49.x	80	http	ペルー	AS18678	1
191.97.49.x	443	https	ペルー	AS18678	1
191.98.128.x	80	http	ペルー	AS27843	1
191.98.137.x	80	http	ペルー	AS27843	1
191.98.137.x	443	https	ペルー	AS27843	1
191.98.142.x	80	http	ペルー	AS27843	1
191.98.142.x	443	https	ペルー	AS27843	1
192.230.90.x	50050	https	チリ	AS19551	4（連番）
200.54.104.x	50050	http	チリ	AS16629	1
200.91.9.x	50050	https	チリ	AS7004	1

住所（末尾伏せ）	出入口	通信の種類	国	ネットワーク番号	件数
201.214.50.x	50050	http	チリ	不明	1
216.241.31.x	50050	https	チリ	AS18747	1
34.176.211.x	50050	http	チリ	AS396982	1
45.71.34.x	443	https	ペルー	AS271860	1
合計					58

補足：AS13335（Web配信事業者）、AS396982（大手クラウド）、AS19551（Webサイト防御サービス事業者と認識、要確認）は多数の利用者が共有する設備です。特にAS19551の連番4件は、防御サービスの中継装置があらゆる出入口に応答している可能性があり、50050番の意味合いは薄いと考えられます。

本報告書は第1回観測の確定記録です。自動判定はあくまで確認の優先順位付けであり、最終的な判断は人が行います。