ネット探検ラボ AI 調査任務 MISSION 003

中国サイバー作戦エコシステム 現在進行する対日 Trusted Infrastructure 攻撃の実証調査

公開情報から証明できる範囲と証明できない範囲

項目	内容
調査基準日	2026 年 9 月 9 日
基本対象期間	2021 年 1 月 1 日から 2026 年 9 月 9 日
対象	通信 政府 防衛 重要インフラ クラウド ネットワーク 認証 仮想化 その他の Trusted Infrastructure
成果物区分	調査報告書 編集可能原稿
共有区分	TLP CLEAR

主要結論

日本への直接的な Trusted Infrastructure 侵害は、BlackTech の海外拠点から日本本社へのルーターピボットと、LapDogs による日本国内 SOHO 機器の侵害について公開資料で確認できる。ただし、Salt Typhoon、Volt Typhoon、Fire Ant、UNC3886 について、日本国内の通信バックボーン、重要インフラ、認証基盤が当該アクターに侵害されたと断定できる公開証拠は確認できなかった。

Executive Summary

本調査は、中国国家との関係を政府機関または有力なセキュリティ機関から評価されたアクターが、2021 年以降に日本の Trusted Infrastructure を侵害しているかを検証した。世界での活動、日本の共同署名、日本国内の侵害、アクター帰属を別々の命題として評価した。

結論は限定付きで肯定である。公開情報で最も強い対日証拠は BlackTech である。日米合同アドバイザリは、BlackTech が日本企業の海外子会社を侵害し、支店ルーターと信頼関係を悪用して日本本社へピボットし、Cisco IOS ファームウェアの改変、SSH バックドア、EEM による CLI 出力操作とフォレンジック妨害を行ったと記録する。これは Level 2 を直接満たし、対象が日本本社である点で Level 1 に接続する。もっとも、公開文書は被害企業名、個別侵害日、国内機器の台数を明らかにしていない。[1, 2]

日本国内の機器侵害を数量で示す最も明瞭な資料は、SecurityScorecard の LapDogs 報告である。報告は、2024 年 11 月 26 日に日本の 123 台超の機器が感染し、観測した Buffalo AirStation 107 台はいずれも日本所在で大半が東京にあったとする。また、日本の自治体サービス部署、IT・ネットワーク企業、建設・不動産企業の ORB 被害を匿名で列挙する。侵害の地理的接続は強いが、中国帰属は単一社の「中程度確度の China-nexus」評価であり、国家機関または特定 APT との接続は未確認である。[15]

Volt Typhoon について、JPCERT/CC は日本組織も狙う Operation Blotless を 2023 年から把握し、Volt Typhoon と多くの共通点があるとした。ただし、Volt Typhoon だけの活動か、同じ戦術を使う別アクターを含むかは精査できていないと明記した。したがって、日本組織への類似作戦は確認事実だが、日本国内の Volt Typhoon 侵害とは断定できない。米政府の「危機・紛争時の破壊的攻撃に備えた米重要インフラへの事前侵入」という評価も、日本国内の被害事実へ転用できない。[3, 4, 5]

Salt Typhoon について、日本の NCO・警察庁が 2025 年の国際共同アドバイザリに参加したことは確認できる。同文書は通信バックボーン、PE・CE ルーター、GRE・IPsec、トラフィックミラーリング、TACACS+・RADIUS、パケットキャプチャ、設定変更、ログ削除を詳述し、活動の一部が Salt Typhoon、OPERATOR PANDA、RedMike、UNC5807、GhostEmperor と重なるとする。しかし作成機関は商用追跡名を 1 対 1 対応させず、一般的な APT 活動として記述している。日本の共同署名は Level 4 であり、日本国内の通信事業者侵害の証拠ではない。[7, 8, 9]

Fire Ant は 2026 年まで活動し、Cisco IOS XR、TACACS、Linux 管理ホスト、PCAP、GRE、ログ抑制、CLI 出力改変を組み合わせた。UNC3886 と強い行動上の重複があるが、Sygnia は同一主体と確定していない。Fire Ant と UNC3886 の原著報告には Japan の記載がなく、日本との直接接続は未確認である。[12, 13, 14]

米国が先に日本の侵害を把握して通知した事例として、2020 年の防衛ネットワーク侵害と外務省公電システム侵害が報道されている。Washington Post は NSA が侵害を発見し、NSA 長官らが日本側へ通報したと報じた。日本

政府は個別攻撃への回答を避け、秘密情報の漏えいは確認していないとした。このため「具体的な通報が報道された」は確認できるが、「日米両政府が侵害と通報を公式確認した」とは評価できない。[21, 22, 23]

最終設問への短答

問	判定	要旨
1	確認できる	BlackTech、MirrorFace などの対日活動は 2021 年以降も政府資料で扱われる。Trusted Infrastructure に限定すると BlackTech と LapDogs が主要証拠。
2	限定的に確認	BlackTech の支店ルーターと信頼関係、LapDogs の国内 SOHO 機器。国内通信バックボーンや電力等の実名被害は未確認。
3	存在する	ルーターと SOHO 機器は確認。Operation Blotless では SSL VPN 等の外部アプライアンス経由が示される。日本国内 TACACS+・RADIUS 侵害は未確認。
4	手口は確認	海外子会社から日本本社へのピボットは日米政府文書が明記。被害企業名と個別時系列は非公表。
5	未確認	日本は Salt Typhoon 関連文書の共同作成国だが、国内通信事業者の侵害確認は公表されていない。
6	直接接続は未確認	Operation Blotless は類似活動であり、Volt Typhoon 単独帰属も重要インフラ被害も確定していない。
7	未確認	Fire Ant・UNC3886 原著報告に日本の記載なし。TTP 重複だけでは接続できない。
8	報道例あり 公式確証不足	2020 年防衛・外交ネットワーク事案で米国通知が報道されたが、政府は侵害と通知の詳細を確認していない。
9	共通性あり	外部公開機器の悪用、正規認証情報、信頼関係、ルーターでの収集、ログ妨害、ORB、

問	判定	要旨
		Living off the Land。
10	共通指揮は立証不能	作戦思想、技術市場、請負企業、共有 ORB が共通性を生む。共通指揮系統の証拠ではない。
11	部分的に強く確認	Salt 関連 3 社と PLA・MSS、i-Soon と MPS・MSS、Integrity Tech と Flax Typhoon は政府・司法資料で接続。全アクター共通の階層は未確認。
12	管理面が最優先	EOL 機器、OOB 管理、ファームウェア整合性、AAA 秘密情報、PCAP・トンネル・設定変更、外部ログ、子会社接続を重点監視。

1 調査方法

調査対象期間は 2021 年 1 月 1 日から 2026 年 9 月 9 日とした。2020 年以前の資料は、BlackTech の前史、MISSION 001・002 との連続性、米国から日本への通報事案を理解するために限って参照した。

検索は日本、米国、英国、豪州、カナダ、ニュージーランドの政府・捜査・情報機関資料を優先し、次に JPCERT/CC、Mandiant、Microsoft、Cisco Talos、Sygnia、SecurityScorecard 等の原著技術資料を確認した。報道は非公開事実の所在を示す場合に用い、政府側の反応を併記した。

評価単位は、アクター名ではなく主張である。同じ報告の中でも、侵害の存在、被害地域、技術、国家帰属、企業や人物との接続を分解した。商用追跡名はベンダーごとに観測範囲が異なるため、名称一致を同一主体の証拠にしなかった。

日本との接続レベル

Level	定義	本調査での扱い
1	日本国内で実侵害を確認	最重要。被害主体名が匿名でも、国内機器・組織の侵害が原資料に明記されれば該当。
2	海外拠点から日本本社へ侵入	BlackTech 型。信頼関係と支店機器の悪用を含む。
3	国内 IP 機器 インフラが標的または攻撃基盤	ORB や侵害済み SOHO 機器を含む。アクター帰属は別評価。
4	日本政府が共同文書に参加	状況証拠。国内被害の確認ではない。
5	潜在的対象との分析	参考。対日攻撃確認とはしない。

検索上の限界

- 被害企業名、正確な侵害日、国内 IP、機器設定は多くの政府文書で匿名化されている。
- 日本政府が保有する非公開の被害報告や同盟国情報は評価できない。
- 侵害済みルーターや VPS の IP は再割当てされる。IOC は過去の観測であり、現在の悪性を意味しない。
- 2026 年 8 月以降の資料は公開後間もなく、独立検証が限定される。

2 証拠評価基準

分類	意味
確認事実	一次資料または複数の独立資料から直接確認できる技術・公表行為。
政府評価	政府、警察、情報機関による公式評価。観測事実と分ける。
司法上の主張	起訴状、令状宣誓供述書、制裁理由。判決・有罪認定ではない。
民間セキュリティ企業評価	インシデント対応または脅威分析に基づく評価。確度表現を維持する。
状況証拠	技術、時間帯、言語、被害選定、インフラの相関。
仮説	複数証拠から合理的だが確定できない推論。
未確認	探索した公開情報では直接証拠を確認できない。

帰属確度

確度	基準
A 非常に強い	政府・司法資料が国家機関、企業、人物まで具体的に接続。
B 強い	複数政府機関が国家支援または国家関連として公式評価。
C 中程度	複数の有力セキュリティ企業が中国系と評価。
D 弱い	単一社または技術・状況証拠による China nexus。
E 未確定	中国帰属を裏付ける十分な証拠なし。

3 対日活動タイムライン

時期	活動	公開情報で確認できる事項	日本 Level	帰属
2021 年以降	MirrorFace	警察庁は 2019 年頃から現在まで日本国内の組織・事業者・個人を狙うキャンペーンと評価。Trusted Infrastructure 型とは限らない。	Level 1	政府評価 B
2023 年 5 月	Volt Typhoon	米国・グアム等の重要インフラ活動が公表。日本被害の記載なし。	Level 5	政府評価 B
2023 年から	Operation Blotless	JPCERT/CC が日本組織も狙う類似活動を把握。Volt Typhoon 単独帰属は未確定。	Level 1	アクター帰属 E
2023 年 9 月	BlackTech	日米政府が海外子会社から日本本社へのルーターピボットと改変ファームウェアを公表。	Level 2	政府評価 B
2023 年 9 月から	LapDogs	日本を含む SOHO 機器に ShortLeash を配備し ORB 化。	Level 3	民間評価 D
2024 年 11 月 26 日	LapDogs	日本のみを対象としたと分析される一括感染。123 台超。	Level 3	民間評価 D
2025 年 1 月	Salt Typhoon	米財務省が Sichuan Juxinhe を Salt Typhoon へ直接接続。日本被害の記載なし。	日本接続なし	政府 制裁 A
2025 年 5 月	Volt Salt	政府会議資料は国内重要インフラ企業で未発見と記載。別の国会参考人は類似攻撃があると述べ、評価主体が異なる。	反証	限定資料
2025 年 6 月	LapDogs	日本の自治体サービス、IT・	Level 1 3	民間評価 D

時期	活動	公開情報で確認できる事項	日本 Level	帰属
		ネットワーク、建設・不動産の匿名被害を原著が公表。		
2025 年 8 月	Salt 関連活動	日本 NCO・NPA を含む多国間文書が通信・ルーター侵害 TTP と中国企業 3 社を公表。国内被害とは記載せず。	Level 4	政府評価 A B
2026 年 4 月	中国系 Covert Networks	日本 NCO 参加文書が SOHO・IoT・ルーターの共有中継網を警告。国内被害とは記載せず。	Level 4	政府評価
2026 年 8 月	Fire Ant	Sygnia が 2026 年までの Trusted Infrastructure 侵害を公表。日本の記載なし。	日本接続なし	民間評価 C

4 アクター別分析

4 1 BlackTech

日米合同アドバイザリは BlackTech を PRC linked actors とし、日本企業と米国企業の海外子会社を侵害後、信頼された支店ルーターを経由して日本・米国の本社へ移動すると記録する。日本本社は primary targets と明記される。日本の警察庁・NISC も、日本を含む政府、産業、技術、メディア、エレクトロニクス、通信分野への情報窃取を確認している。[1, 2]

ルーター侵害では、正規の古い IOS を起動してメモリ上で署名検証を迂回し、改変ブートローダーと改変ファームウェアを導入する。内蔵 SSH バックドアは特別なユーザー名とトリガーパケットで有効化され、ACL とコマンド・エラーログを迂回する。EEM ポリシーは show コマンド出力から特定行を除外し、copy、rename、move を拒否してフォレンジック取得を妨げる。[2]

2021 年以降の継続性は、2023 年に日米政府が観測に基づく共同文書を発行し、BlackTech がツールを継続更新していると述べたことから支持される。ただし、公開文書は個別侵害の実施年を示さない。したがって「2023 年時点で脅威が継続し、対日作戦手口が政府から公表された」は確認できるが、「特定の日本企業が 2021 年以降に新規侵害された日付」は未確認である。

論点	判定	根拠
日本企業 日本組織	確認	日本企業の海外子会社と日本本社を対象として明記。被害名は匿名。
海外子会社から日本本社	確認	支店ルーターと trusted relationship を悪用。
Cisco IOS ファームウェア	確認	旧正規イメージ、メモリホットパッチ、未署名ブートローダー・ファームウェア。
SSH バックドア	確認	特別ユーザー名、magic packet、ログと ACL の迂回。
EEM CLI 妨害	確認	出力行除外、copy rename move 阻止。
中国政府との関係	政府評価	PRC linked。特定の MSS PLA 部局、企業、人物は公表されず。
帰属確度	B	日米政府の共同評価。具体的指揮系統がないため A にはしない。

4 2 Salt Typhoon 関連活動

2025 年国際共同文書の対象活動は、2021 年以降、通信、ISP、政府、運輸、宿泊、軍事インフラを狙い、バックボーン、PE、CE ルーターと信頼接続を中心に侵害した。文書は活動の一部が Salt Typhoon、OPERATOR PANDA、RedMike、UNC5807、GhostEmperor と重なるとするが、商用名と政府側観測が 1 対 1 対応しないと明記する。したがって、これらを同一アクターの別名一覧として統合してはならない。[7]

初期侵入では Ivanti、PAN OS、Cisco IOS XE 等の既知脆弱性を悪用し、ゼロデイの観測はない。侵害後は ACL、SSH 鍵・アカウント、HTTP 管理ポート、SNMP、Tcl、Guest Shell、GRE・IPsec・静的経路を操作する。SPAN、RSPAN、ERSPAN と組込み PCAP を利用し、TACACS+・RADIUS 通信、加入者データ、通信内容・メタデータ、設定、MPLS 情報を収集する。ログ消去、転送停止、設定復元による痕跡抑制も記録される。[7]

中国企業との接続は強い。共同文書は Sichuan Juxinhe、Beijing Huanyu Tianqiong、Sichuan Zhixin Ruijie が PLA と MSS の複数部局へサイバー製品・サービスを提供すると評価する。米財務省は Sichuan Juxinhe が Salt Typhoon に直接関与したとして制裁した。ただし、三社すべてを Salt Typhoon という単一組織の構成員とみなすことや、各商用追跡名の全活動を同じ指揮系統へ帰属させることは文書の範囲を超える。[7, 8, 10]

日本との接続は共同作成国であることに留まる。NCO・警察庁は文書が日本のサイバーセキュリティ確保に有用として参加したが、日本の通信事業者、ISP、バックボーンが侵害されたとは公表していない。2025 年 5 月の政府会議資料は Volt Typhoon と Salt Typhoon が国内重要インフラ企業で現時点まで見つかっていないと記載しており、少なくとも同日時点の公表情報に不利な証拠である。[9, 11]

追跡名	本調査の扱い
Salt Typhoon	米財務省が Sichuan Juxinhe との直接関与を評価。2025 年共同文書の活動と部分重複。
OPERATOR PANDA	共同文書と部分重複。Salt Typhoon との完全同一性は不採用。
RedMike	Recorded Future の活動クラスター。共同文書と部分重複。
UNC5807	Mandiant 追跡名。共同文書と部分重複。
GhostEmperor	Demodex 等で知られるクラスター。TTP や観測範囲の重複を同一主体の証拠にしない。

4 3 Volt Typhoon

米政府は Volt Typhoon を PRC state sponsored actor とし、米国の通信、エネルギー、運輸、水道等へ長期アクセスを維持し、重大な危機または紛争時の破壊的・妨害的攻撃に備えて事前配置していると評価した。DOJ は Cisco・Netgear の EOL SOHO ルーター数百台からなる KV Botnet を無害化し、同ボットネットが米国その他の標的への活動の出所秘匿に使われたと説明した。[4, 5]

グアムとインド太平洋の標的選定は、日本の安全保障に重大な含意を持つ。しかし作戦環境上の関連は、日本国内の侵害事実ではない。日本政府が 2024 年の Five Eyes 中心の Volt Typhoon 共同文書の作成国でないこと、日本の被害組織名が米側資料にないことも区別する必要がある。

JPCERT/CC の Operation Blotless は、日本組織も狙う同様の活動として最重要である。外部公開アプライアンス、SSL VPN、NTDS 窃取、Web shell、正規ツール、ログ不足という特徴があり、JPCERT/CC 対応事例を含む。しかし同機関は Volt Typhoon のみか別アクターを含むか精査できないと明記した。よって本調査は「Volt Typhoon 類似の対日事前侵入型活動」を確認し、「Volt Typhoon による日本重要インフラ侵害」は未確認とする。[3]

論点	判定
日本国内の標的	Operation Blotless として日本組織を確認。ただし Volt Typhoon 帰属は未確定。
通信 電力 水道 港湾 運輸	米国等では政府評価。日本国内の該当セクター被害は公開確認なし。
SOHO Router ORB	KV Botnet は確認。日本所在ノードの公表確認なし。
Credential Abuse	NTDS や有効アカウントの窃取・再利用。
Pre positioning	米政府評価は強いが、対象は米重要インフラ中心。日本への外挿は禁止。
帰属確度	Volt Typhoon は B。Operation Blotless のアクター帰属は E。

4 4 UNC3886 と Fire Ant

Mandiant は UNC3886 を suspected China nexus espionage actor とし、2021 年末以降、VMware ESXi・vCenter、FortiOS、TACACS+、Linux、ネットワーク機器を侵害したと報告する。ゼロデイや既知脆弱性、VMCI

バックドア、REPTILE・MEDUSA 系 rootkit、LOOKOVER、改変 tac_plus を組み合わせる。LOOKOVER は TACACS+を復号し、取得記録を 0xEF で XOR して保存した。[12]

Sygnia の Fire Ant は 2025 年に ESXi・vCenter 侵害として公表され、2026 年には Cisco IOS XR、TACACS、Linux 管理ホストへ拡張した。GRE トンネルが running config や commit history に現れない、syslog 配信を選択抑制する、show 出力からトンネル関連行を除外する、ルーター上で PCAP を作成して FTP 送信する、といった「証拠層」への攻撃が確認された。TacTap は tac_plus へ共有ライブラリを注入し、受理済み TACACS セッションを捕捉した。[13, 14]

Fire Ant と UNC3886 は、VMCI、TACACS、Medusa、SSH、router、0xEF XOR などで強く重複する。一方、ファイル名、パス、実装、起動マーカーには差がある。Sygnia の表現も strong overlap であり、同一主体の断定ではない。本調査は Fire Ant を UNC3886 like activity として比較し、同一アクターとは認定しない。

日本との直接接続は確認できなかった。Sygnia の 2025 年・2026 年原著、Mandiant の UNC3886 原著のいずれにも Japan または Japanese の被害記載がない。日本で類似 TTP が見つかった場合も、ルーター、TACACS、Linux rootkit という一般化可能な手法だけでは帰属できない。

活動	日本接続	帰属	評価
UNC3886	未確認	C	複数の Mandiant 調査に基づく suspected China nexus。政府による特定部局接続なし。
Fire Ant	未確認	C	Sygnia の China nexus 評価。UNC3886 との強い重複は同一性を意味しない。

4 5 その他の Trusted Infrastructure 活動

LapDogs は本調査で BlackTech に次ぐ重要な対日事例である。ShortLeash は Linux 系 SOHO 機器に常駐し、偽の Nginx 応答、LAPD を装う自己署名 TLS 証明書、root 権限、systemd 永続化を用いて ORB を構成する。日本の機器侵害、匿名組織、台数が公表されており、日本 Level 1 および 3 を満たす。[15]

ただし SecurityScorecard 自身が、ORB は複数アクターに共有され得る、UAT 5918 が運営者か利用者か確認できない、他アクターの利用も確認できないと述べる。したがって、LapDogs ノードの日本所在は侵害事実を示す一方、Salt Typhoon、Volt Typhoon、APT40 等への帰属を示さない。

APT40 は MSS 関連と各国政府が評価し、公開直後の脆弱性を素早く悪用し、EOL・未修正 SOHO 機器を最終ホップとして使う。日本は 2024 年共同アドバイザリに参加したが、掲載事例は豪州組織の侵害であり、日本被害の証拠ではない。[16, 17]

Flax Typhoon と Integrity Technology Group は、SOHO ルーター、IP カメラ、DVR、NAS 等 20 万台超の世界規模ボットネットを司法当局が公表した。2026 年の共同文書は、同社が Raptor Train を管理し、単一 Covert Network が複数アクターに利用され得ることを警告する。公開資料は日本ノードの存在を具体的に示していないため、日本接続は Level 4 以下に留める。[18, 19]

MirrorFace は 2021 年以降も対日中国関連作戦が継続することを示す強い補助証拠であるが、主要侵入経路はスピアフィッシングや正規機能悪用であり、本 MISSION の Trusted Infrastructure 侵害とは分ける。[24]

5 日本との接続

活動	Level	証拠主体	日本接続の内容	確度
BlackTech	2 かつ 1 へ接続	日米政府共同文書	海外子会社の支店ルーターから日本本社へピボット。対象名は匿名。	高
Operation Blotless	1	JPCERT/CC	日本組織を狙う類似活動。アクターと重要インフラ区分は未確定。	中
LapDogs	1 3	SecurityScorecard	日本の 123 台超の一括感染、Buffalo 107 台、匿名の自治体・IT 等。	侵害 高 帰属 低
Salt 関連活動	4	政府共同文書	日本は共同作成国。国内通信事業者被害の記載なし。	低
Volt Typhoon	5	米政府資料	インド太平洋・グアムの含意。国内被害へ外挿不可。	低
Fire Ant UNC3886	接続なし	原著資料	Japan 記載なし。	なし
APT40	4	国際共同文書	日本署名。事例は豪州。	低
MirrorFace	1	警察庁 NISC	日本国内組織を継続標的。Trusted Infrastructure 型とは限らない。	高

米国から日本への通知

Washington Post は、NSA が 2020 年秋に中国軍ハッカーによる日本の機密防衛ネットワーク侵害を発見し、Paul Nakasone NSA 長官兼 USCYBERCOM 司令官と Matthew Pottinger 大統領副補佐官が東京で防衛相と首相へ説明したと報じた。報道によればアクセスは 2021 年初めにも継続した。[21]

防衛相は 2023 年 8 月 8 日、日米が平素から緊密にやり取りしていると述べつつ、秘密情報漏えいを確認していないと回答した。侵害の有無については、個別攻撃と対応能力が明らかになるため回答できないとした。これは報道を否定したものではないが、肯定したものでもない。[22]

2024 年 2 月には、外務省の外交公電システムが 2020 年に中国から侵害され、米政府が日本へ警告したとの報道が出た。官房長官は個別の事実関係への回答を避け、秘密情報漏えいは確認していないとした。この事案も公開された政府一次資料で侵害主体、経路、通知文書を確認できない。

以上から、米国側が先に把握して日本へ通知した具体例は複数報道されている。しかし、日米政府が通知日、侵害範囲、アクター、被害を公式文書で確認した公開例は見つからなかった。MISSION 003 の基本期間外に始まる事案だが、報道上は 2021 年まで継続したため前史として扱う。

6 Trusted Infrastructure 侵害技術

局面	共通技術	主な活動	防御上の意味
Initial Access	公開機器の既知脆弱性 EOL 機器 Valid Accounts	BlackTech Salt APT40 Operation Blotless LapDogs	境界機器の露出とログ不足が初期侵入の検証を困難にする。
Persistence	改変ファームウェア SSH 鍵 アカウント Web shell systemd VMCI	BlackTech Salt Volt UNC3886 Fire Ant LapDogs	OS 再導入だけでは router hypervisor 管理層の永続化が残る。
Credential Access	TACACS+ RADIUS NTDS SSH credential capture packet capture	Salt Volt UNC3886 Fire Ant	認証基盤自体が侵害されると監査証跡と認証情報を同時に失う。
Discovery Lateral	routing table VRF BGP MPLS SNMP VPN SMB RDP SSH	BlackTech Salt Fire Ant Volt	信頼接続と管理経路が組織境界を越える移動路になる。
Collection	PCAP traffic mirroring subscriber metadata config email auth traffic	Salt Fire Ant BlackTech	ネットワーク装置は広い可視性を持つ収集点。
Defense Evasion	log deletion suppression CLI manipulation rootkit LOTL	全主要活動	ネットワーク装置の表示とログを単独の真実源にできない。
C2 Infrastructure	compromised routers SOHO ORB VPS GRE IPsec proxy	BlackTech Salt Volt LapDogs APT40	出口 IP は被害者機器でありアクター同一性の証拠にならない。

技術的相関の評価

BlackTech と Fire Ant は CLI・ログを欺く点、Salt 関連活動と Fire Ant は IOS XR、PCAP、TACACS、GRE を扱う点、Volt Typhoon と Operation Blotless は正規ツールと認証情報を重視する点で似る。しかし、これらの機能はネットワーク制御面を侵害した攻撃者にとって合理的な選択であり、同一主体を証明しない。

より説明力があるのは、作戦思想と供給市場の共有である。中国系アクターは、公開機器への N day 悪用、侵害済み機器を出口にする Covert Network、正規管理機能の悪用、認証とログの掌握を組み合わせる。複数企業が PLA、MSS、MPS へサービスを供給する公開資料は、この分業モデルと整合する。

7 IOC とインフラ分析

以下は検知・調査の起点であり、即時ブロックまたは帰属判定の根拠ではない。IP は再割当て、VPS、侵害済み第三者機器であり得る。Salt 関連文書自身も観測時期が 2021 年 8 月から 2025 年 6 月で、現在使用されていない可能性を明記する。[7]

活動	種別	例	意味と留意点
Salt 関連	IPv4	1.222.84[.]29 103.169.91[.]231 167.88.173[.]252	過去の関連 IP。現時点の悪性・所有者・アクター同一性を保証しない。
Salt 関連	IPv6	2001:41d0:700:65dc:f656:929f	共同文書掲載。表記をデファング。
Salt 関連	SHA256	f2bbba1ea0f34b262f158ff31e00d39d89bbc471d04e8fca60a034cabe18e4f4	cmd1 SFTP client。PCAP 取得機能あり。
LapDogs	TLS	CN=ROOT O=LAPD ST=California C=US L=LA OU=Police department	自己署名証明書の subject issuer。順序差あり。
LapDogs	JARM	3fd3fd16d3fd3fd22c3fd3fd3fd3fdf20014c17cd0943e6d9e2fb9cd59862b	悪性サービス探索用。誤検知検証が必要。
LapDogs	Domain	northumbra[.]com study.northumbra[.]com	C2 関連。現在状態を別途確認。
LapDogs	SHA256	9b954bfc2949d07eb41446225592eaa65ed3954cd2b93a13c574bb89147a4465	ShortLeash Linux variant。
Fire Ant	Path	/var/log/.tacplus.acct /var/run/acpid.lock	TacTap credential artifact と UNIX socket。

活動	種別	例	意味と留意点
Fire Ant	SHA1	be6b27f429324a4af05a310d8ec9635e37c68a94	IOS XR implant /usr/bin/acpid。
Fire Ant	SHA1	955cd45a2f6f226a2fdf44b329af1c8dde90cb38	TacTap injected library /lib/libseconfd.so。
BlackTech	構成痕跡	旧正規 IOS 改変 bootloader 改変 firmware 隠された EEM	ハッシュより実行状態、boot chain、running config との差分を重視。

ASN VPS Provider 証明書の扱い

公開資料から個々の IP の現在 ASN やホスティング事業者を固定的に記載すると、調査基準日以降の再割当てで誤解を生む。本報告は原資料が明示する VPS、侵害済みルーター、ORB、証明書、マルウェアハッシュを優先し、現在の WHOIS 結果をアクター帰属に使用しない。

8 MITRE ATTACK マッピング

ID	Technique	活動	手順
T1190	Exploit Public Facing Application	Salt APT40 Operation Blotless LapDogs	境界機器や管理 UI の既知脆弱性。
T1078	Valid Accounts	Volt Salt BlackTech Fire Ant	取得した管理・サービス資格情報の利用。
T1199	Trusted Relationship	BlackTech Salt Fire Ant	子会社・provider customer・管理接続を横断。
T1542.004	Pre OS Boot ROMMONkit	BlackTech	改変ブートローダーによる永続化。
T1601.001	Modify System Image	BlackTech	改変 IOS イメージ。
T1601.002	Downgrade System Image	BlackTech	古い正規ファームウェアを利用。
T1556.004	Network Device Authentication	BlackTech	SSH バックドアと特別ユーザー。
T1205	Traffic Signaling	BlackTech Fire Ant UNC3886	magic packet port knocking。
T1562.003	Impair Command History Logging	BlackTech	コマンドログ迂回。

ID	Technique	活動	手順
T1562.006	Indicator Blocking	BlackTech Fire Ant	CLI 表示から特定行を除外。
T1021.004	SSH	BlackTech Salt Fire Ant UNC3886	ネットワーク装置 Linux 管理ホストへのアクセス。
T1090.002	External Proxy	BlackTech	侵害支店ルーターを proxy 化。
T1090.003	Multi hop Proxy	Volt Flax LapDogs Covert Networks	複数の侵害済み機器を経由。
T1584.008	Compromise Infrastructure Network Devices	Volt APT40 LapDogs Flax	SOHO router 等を ORB 化。
T1098.004	SSH Authorized Keys	Salt	装置の SSH 鍵追加。
T1059.008	Network Device CLI	BlackTech Salt Fire Ant	CLI で構成・永続化・妨害。
T1572	Protocol Tunneling	Salt Fire Ant	GRE IPsec reverse tunnel。
T1040	Network Sniffing	Salt Fire Ant UNC3886	PCAP TACACS RADIUS traffic capture。
T1003.003	NTDS	Volt Operation Blotless	AD データベース窃取。
T1505.003	Web Shell	APT40 Operation Blotless	公開サーバー・アプライアンスで永続化。

ATTACK は観測手順の整理に用いる。技術 ID の一致は、同じソフトウェア機能や攻撃目的から生じるため、アクター同一性や共通指揮の証拠にしない。

9 中国サイバー作戦エコシステム構造

公開資料が支持する構造は、単一の国家機関から全アクターへ直線的に命令が流れるモデルではない。少なくとも、情報要求を持つ国家機関、製品・侵入・インフラを供給する民間企業、技術者、攻撃基盤、商用名で追跡される活動クラスターが重なり合う市場型・請負型の構造が確認できる。

層	公開資料で確認できる接続	証拠区分
PLA MSS	Sichuan Juxinhe Beijing Huanyu Tianqiong Sichuan Zhixin Ruijie からサイバー製品・サービスを受ける。	多国間政府評価
MPS MSS	i Soon へ標的を依頼し、盗取データを購入。i Soon は MPS 職員を訓練。	司法上の主張
中国民間企業	Integrity Technology Group が Raptor Train を開発・管理し、FBI は Flax Typhoon 活動との関係を評価。	司法 政府評価
技術者 チーム	i Soon の CEO COO penetration team infrastructure support sales R and D 等の役割が起訴状に記載。	司法上の主張
攻撃インフラ	VPS 侵害済み router SOHO IoT Covert Network が複数作戦に供給される。	政府 民間評価
APT 活動	商用追跡名は観測範囲であり、法人・部署・人物と 1 対 1 ではない。	分析上の制約

重点 3 社

企業	確認できる関係	確度と限界
Sichuan Juxinhe Network Technology	米財務省が Salt Typhoon への直接関与を理由に制裁。多国間文書は PLA MSS への提供を評価。	A。ただし Salt Typhoon 全活動の唯一運営者とは書かれていない。
Beijing Huanyu Tianqiong Information Technology	多国間文書が 2021 年以降の活動と接続し、PLA MSS への製品・サービス提供を評価。	A に近い政府評価。特定商用名との 1 対 1 接続は未公表。

企業	確認できる関係	確度と限界
Sichuan Zhixin Ruijie Network Technology	同上。	A に近い政府評価。個々の侵入案件・人物との対応は未公表。

i Soon が示す MPS MSS 市場

2025 年の米司法省起訴は、i Soon が MSS と MPS から依頼を受けるだけでなく、自主的に侵害して盗取データを少なくとも 43 の MSS・MPS 局へ販売し、メールボックス 1 件につき約 1 万から 7 万 5 千ドルを請求し、MPS 職員へ侵入方法を訓練したと主張する。これは MISSION 002 の APT10 型階層に加え、複数顧客へ能力とデータを販売する市場型の関係を示す。起訴上の主張であり、有罪判決ではない。[20]

共通指揮系統の検証

BlackTech、Salt 関連、Volt Typhoon、UNC3886、Fire Ant、LapDogs の全てを同じ指揮系統へ接続する公開証拠はない。最も支持される代替説明は、国家機関の需要、複数請負企業、共有または再利用される Covert Network、共通製品、技術者移動、合理的に収斂するネットワーク侵害手法が、TTP の類似を生むというものである。

10 MISSION 001 002 との連続性

MISSION 001 は 2020 年以前に公表された対日 APT 活動を広く整理し、後年の帰属を当時既知の事実として扱わない原則を置いた。MISSION 003 でも同じ原則を維持し、2023 年の BlackTech 政府評価を過去の全活動へ自動的に遡及させない。

MISSION 002 は APT10 について、MSS、Tianjin State Security Bureau、Huaying Haitai、Zhu Hua・Zhang Shilong・Gao Qiang、Cloud Hopper、日本関連活動の具体的な連鎖を政府・司法資料で検証した。MISSION 003 で同程度の人物・地方機関まで到達できるのは、i Soon 等の別事例と Salt 関連企業の一部であり、BlackTech、Volt Typhoon、UNC3886、Fire Ant では到達できない。

連続性の核心は、海外拠点、管理事業者、クラウド、ルーター、認証基盤という信頼境界を利用して本来の標的へ到達する作戦設計である。APT10 の MSP 経由侵入と BlackTech の海外子会社ルーター、Fire Ant の target behind the target は構造的に似る。ただし類似は共通主体を意味しない。

11 反証と代替仮説

反証仮説	評価
日本への攻撃は確認されていない	全面的には反証。BlackTech と LapDogs の直接接続がある。ただし Salt Volt Fire Ant の国内被害は未確認。
日本政府が共同文書に参加しただけ	Salt APT40 Covert Networks には該当。共同署名を Level 1 へ格上げしない。
Fire Ant と日本の接続はない	公開情報の範囲で支持。原著に Japan 記載なし。
TTP 類似は一般手法	強く支持。router CLI PCAP SSH log suppression はネットワーク制御面侵害で合理的に収斂。
中国国家帰属は民間評価のみ	Fire Ant UNC3886 LapDogs には概ね該当。BlackTech Salt Volt APT40 には政府評価あり。
別 APT を誤統合	Salt 関連名、Fire Ant UNC3886、Volt Operation Blotless で高リスク。原資料の留保を維持。
同一 IOC は共有第三者インフラ	支持。2026 年共同文書は単一 Covert Network を複数アクターが使い得ると明記。
報道が政府資料以上を断定	2020 年防衛・外務省侵害通知が該当。政府は詳細を公式確認していない。

相反する公開記述

2025 年 3 月の衆議院内閣委員会で大澤淳参考人は、Volt Typhoon や Salt Typhoon に似た準備攻撃が日本の政府機関・重要インフラへ行われていると述べた。一方、2025 年 5 月 12 日付の政府会議資料は両者が国内重要インフラ企業で見つかっていないと記載する。前者は参考人の意見陳述で政府認定ではなく、後者も会議配布資料の記載である。対象範囲、把握時点、帰属閾値が異なる可能性があり、どちらも匿名の個別事案を立証しない。[11, 26]

12 未解決事項

- BlackTech の個別日本被害企業、侵害日、国内ルーターの型番・台数。
- 2023 年共同文書の観測事例が 2021 年以降の新規侵害か、過去事例を含むか。
- Operation Blotless の被害セクターと、Volt Typhoon 以外の混在アクター。

- Salt 関連活動について日本の通信事業者、ISP、PE CE router、TACACS RADIUS 侵害が非公開で存在するか。
- LapDogs 日本ノードのうち、単なる ORB 被害と内部ネットワークへの二次侵入の割合。
- Fire Ant と UNC3886 の組織的関係、共通開発者、共有ツール供給元。
- 米国から日本への 2020 年通知の公式記録、通知先、侵害範囲、改善措置。
- 重点 3 社の法人役員、技術者、個別 PLA MSS 部局、各商用クラスターとの対応。
- 公開 IOC の現在の所有・用途・失効状態。

13 日本への安全保障上の含意

日本にとって最も重要な観点は、Trusted Infrastructure が単なる侵入口ではなく、横展開、収集、永続化、証拠改変を同時に可能にする作戦基盤であることだ。侵害後も業務が通常どおり動くため、可用性監視だけでは検知できない。

台湾有事やインド太平洋危機の想定では、米軍支援、通信、港湾、輸送、電力、クラウド、データセンターの相互依存が標的価値を高める。しかし、地政学的合理性だけで日本国内の侵害を認定してはならない。防御は潜在リスクに基づいて先行し、公開評価は証拠閾値を維持する必要がある。

14 技術的防御優先事項

優先度	領域	実施事項
最優先	資産と EOL	router firewall VPN hypervisor NMS AAA を台帳化し、外部公開面、所有者、保守期限、firmware hash、設定基準を結び付ける。
最優先	OOB 管理	管理プレーンを業務ネットワークと分離し、専用管理端末、MFA、個人別アカウント、送信元 allow list を使う。
最優先	信頼関係	海外子会社、MSP、provider customer、cloud interconnect ごとに到達性を最小化し、支店 router 侵害を前提に再設計する。
最優先	ログ独立性	network device TACACS RADIUS hypervisor のログを外部へリアルタイム転送し、改ざん防止保存と時刻同期を行う。
高	構成と実行状態	running config、startup config、commit

優先度	領域	実施事項
		history、routing VRF tunnel、実際の socket process memory を相互照合する。
高	PCAP mirror tunnel	Embedded Packet Capture、SPAN RSPAN ERSPAN、GRE IPsec、static route、非標準 SSH HTTP port の生成を即時検知する。
高	AAA 防御	TACACS RADIUS の共有秘密を強化・定期回転し、可能な保護方式を採用。AAA server 自体の EDR、integrity、process injection を監視する。
高	資格情報リセット	edge device 侵害時は装置だけでなく、装置を通過・保存した domain admin、service、SSH、SNMP、API 秘密情報を失効させる。
高	firmware boot	secure boot、署名済み image、ROMMON・bootloader 整合性、vendor 既知 gold image との差分、downgrade を監視する。
中	ORB 対策	静的 deny list だけに頼らず、consumer broadband、SOHO TLS certificate、JARM、NetFlow、地域・時刻・端末属性を組み合わせる。
中	フォレンジック	封じ込め前に volatile data、process、socket、memory、on box files、config、AAA、upstream flow を取得し、単一ログを信用しない。

15 結論

中心命題は部分的に立証された。中国国家関連と政府評価された BlackTech が、日本企業の海外拠点とルーターの信頼関係を悪用して日本本社へ侵入し、Cisco IOS ファームウェア、SSH、EEM を使って永続化と証拠隠蔽を行

うことは、日米政府の共同資料で確認できる。さらに、China nexus の帰属確度は低いものの、LapDogs が日本国内の多数の SOHO 機器と匿名組織を実際に侵害したことは原著テレメトリで確認できる。

一方、Salt Typhoon 型の日本通信バックボーン侵害、Volt Typhoon による日本重要インフラへの事前侵入、Fire Ant または UNC3886 による日本の Cisco IOS XR・TACACS・Linux 管理基盤侵害は、公開情報から確認できなかった。日本の共同署名、グアムとの地政学的接続、TTP の一致は代替にならない。

公開情報が示す中国サイバー作戦エコシステムは、国家機関、地方部局、民間企業、技術者、Covert Network、活動クラスターの多層構造である。Salt 関連 3 社と PLA・MSS、i Soon と MPS・MSS、Integrity Technology Group と Flax Typhoon の接続は強い。しかし、主要アクターすべてを単一指揮系統に束ねる証拠はない。共通 TTP は、能力・作戦思想・供給市場・共有インフラの重なりとして理解するのが最も証拠に忠実である。

16 出典一覧

[1] 中国を背景とするサイバー攻撃グループ BlackTech によるサイバー攻撃について. 警察庁 内閣サイバーセキュリティセンター. 2023 年 9 月 27 日. 該当箇所: pp 1 2 日本を含む標的 海外子会社 本社 ルーターファームウェア. https://www.npa.go.jp/bureau/cyber/pdf/20230927press.pdf

[2] People’s Republic of China Linked Cyber Actors Hide in Router Firmware. NSA FBI CISA NPA NISC. 2023 年 9 月. 該当箇所: pp 1 6 pivot firmware SSH EEM MITRE. https://media.defense.gov/2023/Sep/27/2003309107/-1/-1/0/CSA_BLACKTECH_HIDE_IN_ROUTERS_TLP-CLEAR.PDF

[3] Operation Blotless 攻撃キャンペーンに関する注意喚起. JPCERT CC. 2024 年 6 月 25 日. 該当箇所: 概要 攻撃概要 推奨調査 日本組織 Volt との関係留保. https://www.jpcert.or.jp/at/2024/at240013.html

[4] PRC State Sponsored Actors Compromise and Maintain Persistent Access to U S Critical Infrastructure AA24 038A. CISA NSA FBI and partners. 2024 年 2 月 7 日. 該当箇所: Executive Summary pre positioning and sectors. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[5] U S Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure. U S Department of Justice. 2024 年 1 月 31 日 更新 2025 年 2 月 6 日. 該当箇所: paras 55 75 KV Botnet routers notification. https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

[6] Volt Typhoon targets US critical infrastructure with living off the land techniques. Microsoft Threat Intelligence. 2023 年 5 月 24 日. 該当箇所: targeting Guam critical infrastructure LOLBins ORB. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[7] Countering Chinese State Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System. NSA CISA FBI DC3 and international partners. 2025 年 9 月 Version 1 1. 該当箇所: pp 1 38 actors companies routers AAA PCAP GRE IPsec IOC ATTACK. https://www.fbi.gov/file-repository/cyber-alerts/countering-chinese-state-sponsored-actors-compromise-of-networks-worldwide-to-feed-global-espionage-system-082725.pdf

[8] NSA and Others Provide Guidance to Counter China State Sponsored Actors Targeting Critical Infrastructure Organizations. NSA. 2025 年 8 月 27 日. 該当箇所: companies and MSS PLA links co sealing agencies. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/

[9] ソルトタイフーンに関する国際アドバイザリーへの共同署名について. 警察庁 国家サイバー統括室. 2025 年 8 月 27 日. 該当箇所: 日本の共同署名と国内向け位置づけ. https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250827.html

[10] Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise. U S Department of the Treasury. 2025 年 1 月 17 日. 該当箇所: Sichuan Juxinhe direct involvement Salt Typhoon. https://home.treasury.gov/news/press-releases/jy2792

[11] 資料 8. サイバーセキュリティ戦略本部関連会議資料. 2025 年 5 月 12 日. 該当箇所: Volt Typhoon Salt Typhoon の国内重要インフラ企業での発見状況に関する記載. https://www.cyber.go.jp/pdf/council/cs/dai43/43shiryou8.pdf

[12] Cloaked and Covert Uncovering UNC3886 Espionage Operations. Mandiant Google Cloud. 2024 年 6 月 18 日. 該当箇所: UNC3886 China nexus ESXi FortiOS TACACS LOOKOVER tac plus VMCI. https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations

[13] Fire Ant Evolves From Hypervisors to Trusted Infrastructure. Sygnia. 2026 年 8 月 27 日. 該当箇所: IOS XR GRE PCAP TacTap log and CLI manipulation IOC. https://www.sygnia.co/blog/fire-ant-evolves-from-hypervisors-to-trusted-infrastructure/

[14] Fire Ant A Deep Dive into Hypervisor Level Espionage. Sygnia. 2025 年 6 月. 該当箇所: ESXi vCenter CVE persistence evasion. https://www.sygnia.co/blog/fire-ant-a-deep-dive-into-hypervisor-level-espionage/

[15] LapDogs The New ORB in Town. SecurityScorecard STRIKE. 2025 年 6 月. 該当箇所: pp 2 25 Japan victimology 123 devices Buffalo 107 attribution IOC. https://securityscorecard.com/wp-content/uploads/2025/06/LapDogs-STRIKE-Report-June-2025.pdf

[16] APT40 Advisory PRC MSS Tradecraft in Action. ASD ACSC and international partners. 2024 年 7 月 9 日. 該当箇所: SOHO routers compromised infrastructure Australian case studies. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/apt40-advisory-prc-mss-tradecraft-in-action

[17] 国際アドバイザリー APT40 Advisory PRC MSS tradecraft in action への署名. NISC NPA. 2024 年 7 月 9 日. 該当箇所: 日本の共同署名. https://www.cyber.go.jp/news/list

[18] Court Authorized Operation Disrupts Worldwide Botnet Used by PRC State Sponsored Hackers. U S Department of Justice. 2024 年 9 月 18 日. 該当箇所: Integrity Technology Group Flax Typhoon 200000 devices. https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

[19] Defending against China nexus covert networks of compromised devices. NCSC UK and international partners including Japan NCO. 2026 年 4 月 23 日. 該当箇所: pp 3 10 shared covert networks Integrity Tech ATTACK. https://media.defense.gov/2026/Apr/22/2003916747/-1/-1/0/NCSC-ADVISORY-DEFENDING-AGAINST-CHINA-NEXUS-COVERT-NETWORKS-OF-COMPROMISED-DEVICES.PDF

[20] Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns. U S Department of Justice. 2025 年 3 月 5 日. 該当箇所: i Soon MSS MPS customers training and sale of stolen data. https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global

[21] China hacked Japan's sensitive defense networks officials say. The Washington Post. 2023 年 8 月 7 日. 該当箇所: NSA discovery and notification reported from unnamed current and former officials. https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/

[22] 防衛大臣記者会見. 防衛省. 2023 年 8 月 8 日. 該当箇所: 質疑応答 秘密漏えい未確認 個別攻撃への回答留保. https://www.mod.go.jp/j/press/kisha/2023/0808a.html

[23] Pentagon confident on sharing intelligence with Japan despite China hacking report. Reuters. 2023 年 8 月 8 日. 該当箇所: 報道内容と日米政府の反応. https://www.reuters.com/technology/japan-says-cannot-confirm-leakage-after-report-says-china-hacked-defence-2023-08-08/

[24] MirrorFace によるサイバー攻撃について. 警察庁 内閣サイバーセキュリティセンター. 2025 年 1 月 8 日. 該当箇所: 2019 年頃から現在までの日本国内キャンペーンと中国関与評価. https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html

[25] China Nexus Espionage ORB Networks. Mandiant Google Cloud. 2024 年 5 月 22 日. 該当箇所: ORB lifecycle shared infrastructure IOC extinction. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks

[26] 第 217 回国会 衆議院内閣委員会 第 9 号. 衆議院. 2025 年 3 月 28 日. 該当箇所: 大澤淳参考人の意見陳述 類似準備攻撃に関する発言. https://www.shugiin.go.jp/internet/itdb_kaigiroku.nsf/html/kaigiroku/000221720250328009.htm

[27] CISA NSA FBI and Japan Release Advisory Warning of BlackTech PRC Linked Cyber Activity. CISA. 2023 年 9 月 27 日. 該当箇所: authoring agencies observation statement. https://www.cisa.gov/news-events/news/cisa-nsa-fbi-and-japan-release-advisory-warning-blacktech-prc-linked-cyber-activity

[28] U S and Japanese Agencies Issue Advisory about China Linked Actors Hiding in Router Firmware. NSA. 2023 年 9 月 27 日. 該当箇所: 政府共同公表 BlackTech sectors and capability. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/article/3539209/us-and-japanese-agencies-issue-advisory-about-china-linked-actors-hiding-in-rou/

内部参照資料

MISSION 001 中国サイバー作戦エコシステム 調査報告 2020 年以前に公表された対日 APT 活動の基礎調査。

MISSION 002 APT10 ecosystem research report MSS Tianjin State Security Bureau Huaying Haitai 人物 Operation Cloud Hopper 日本関連活動の検証。