中国サイバー作戦エコシステム

特別調査報告

2020 年 日本防衛ネットワーク侵害

NSA は何を見たのか - 「確認できない」領域と Trusted Infrastructure の盲点

MISSION-001〜003 を再接続するための独立実証調査

調査基準日：2026 年 9 月 10 日
公開情報調査 / TLP:CLEAR
ネット探検ラボ

Executive Summary

本調査の出発点は、2023 年 8 月 7 日の Washington Post 報道である。同紙は、2020 年秋に米国家安全保障局（NSA）が、中国人民解放軍（PLA）系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たと報じた。攻撃者は「deep, persistent access」を確立し、防衛計画、能力、軍事上の弱点評価など広範な情報を狙っていたとされる。事態を重大視した NSA 長官兼 USCYBERCOM 司令官 Paul M. Nakasone 大将と当時の国家安全保障副補佐官 Matthew Pottinger が訪日し、防衛相、さらに首相へ警告したと報じられている。[S1]

本件の核心は、侵害の有無だけではない。Washington Post によれば、2021 年初頭にも中国側アクセスが残存し、2021 年秋には米側が侵害の深刻さを補強する新情報を得た。米側は Cyber Command の hunt forward team 派遣を提案したが、日本側は外国軍を自国ネットワークへ入れることに慎重で、国内企業が調査し、NSA/CYBERCOM 合同チームが結果をレビューする折衷案となった。[S1]

さらに重要なのは、2021 年 11 月に訪日した Anne Neuberger 米国家安全保障副補佐官（サイバー担当）が、情報源・手法を守るため「米情報機関がどうやって中国側侵害を知ったのか」を日本側へ明示できなかったと報じられている点である。これは公開情報上、NSA の検知経路を特定できないことを意味する。同時に、被害組織内部のログだけではなく、別の観測面から侵害を把握した可能性を研究対象にする合理的根拠となる。ただし SIGINT、国外 C2 監視、同盟側テレメトリ等のどれであったかは公開資料では確認できない。[S1]

日本政府の公式回答は、Washington Post 報道を明確に否定したものではない。2023 年 8 月 8 日の防衛大臣会見では「防衛省が保有する秘密情報が漏洩したとの事実は確認していない」と回答する一方、個別具体的なサイバー攻撃や対応は、対応能力を明らかにするため回答できないとした。[S2] したがって「秘密情報漏洩を確認していない」と「侵害がなかった」は論理的に同義ではない。

ここで BlackTech、UNC3886、Fire Ant の技術が研究上の比較対象となる。BlackTech は日米政府が、ルーターファームウェアを検知されずに改変し、通常ログを迂回する SSH バックドアや EEM による出力操作を用い、日本・米国本社へピボットする能力を公表している。[S7][S8] UNC3886 は TACACS+認証基盤で資格情報を取得し、認証・監査層そのものを侵害した。[S9] Fire Ant は 2025〜2026 年にハイパーバイザー、Cisco IOS XR、TACACS、Linux 管理ホストへ活動面を広げ、ログ停止・選択的抑制、管理出力操作、GRE トンネル、認証情報・通信収集など、組織が「証拠」として依存する Trusted Infrastructure を攻撃面へ変える手法を示した。[S10][S11]

本調査は、これら後年の手法が 2020 年の日本防衛ネットワーク侵害で使われたとは認定しない。新たな研究価値は別にある。すなわち、攻撃者がネットワーク、仮想化、認証、ログ生成・転送といった観測基盤を掌握した場合、「被害側で確認できない」こと自体が侵害不存在の強い反証にならない可能性を、実際の後年事例が実証していることである。

したがって今後の中心命題は「2020 年の犯人は Fire Ant だったか」ではなく、「NSA には見えたと報じられ、日本側が公には確認できないとした侵害において、どの観測面が失われ、どの外部観測面が機能した可能性があるのか」である。これは MISSION-001 の歴史、MISSION-002 の実行エコシステム、MISSION-003 の Trusted Infrastructure 研究を再接続する中核課題となる。

主要判定

命題	判定	根拠・留保
NSA が 2020 年秋に日本防衛ネットワーク侵害を発見した	強い報道証拠	Washington Post が日米の現・元当局者約 12 人を取材。ただし米政府の事件別公式確認文書ではない。
攻撃主体が PLA 系だった	強い報道上の帰属	Washington Post は Chinese military / PLA cyberspies と記述。公開された技術 IOC や部隊番号はない。
Nakasone 大将と Pottinger が訪日して警告	強い報道証拠	Washington Post。訪日の事件別公式記録は今回の公開検索では確認できず。
2021 年初頭にもアクセスが残存	強い報道証拠	Washington Post。技術的残存形態は非公開。
日本政府が侵害自体を否定した	支持されない	防衛相は秘密情報漏洩を確認していないと

		述べ、個別攻撃の回答を拒否。
NSA の具体的検知手段が公開されている	否定	Washington Post は sources and methods 保護のため米側が説明できなかったと報道。
2020 年侵害で Fire Ant/UNC3886 手法が使われた	未確認	時間・技術・IOC を接続する公開証拠なし。
Trusted Infrastructure 侵害は『確認不能』を生み得る	技術的に強く支持	BlackTech、UNC3886、Fire Ant の公開技術報告が、ログ・認証・管理面の侵害を実証。

1. 調査目的と仮説

従来型の調査は「既知 APT 名 - IOC - 被害組織」を並べる方向へ流れやすい。しかし本件では、侵害の観測主体が NSA であり、被害国側の公的説明が「漏洩は確認していない」に留まる。この非対称性そのものを調査対象とする。

検証仮説

- H1 公表抑制仮説：日本側は侵害を相当程度把握していたが、機密・対外関係・防御能力秘匿のため公開しなかった。
- H2 可視性不足仮説：日本側の監視・フォレンジック能力では侵害の全体像を十分に再構成できなかった。
- H3 観測基盤侵害仮説：攻撃者がルーター、認証、仮想化、ログ等を侵害し、被害側の観測を妨害・欺瞞した。
- H4 外部観測仮説：NSA は日本側ネットワーク内部とは異なる観測面から侵害を把握した。
- H5 複合仮説：H1〜H4 の複数が同時に成立した。

現段階では H1〜H5 のいずれも単独で確定できない。特に H4 について、NSA が SIGINT で本件を発見したと断定する資料はない。NSA の任務が foreign SIGINT を含むことは公式資料で確認できるが、一般的能力から個別事件の収集手段を逆算してはならない。[S6]

2. 2020〜2021 年事案の再構成

時期	米側・報道上の出来事	証拠区分
2020 年秋	NSA が中国軍系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たと Washington Post が報道。	主要報道 [S1]
2020 年秋〜冬	Nakasone NSA 長官兼 USCYBERCOM 司令官と Pottinger 国家安全保障副補佐官が訪日し、防衛相、首相へ警告したと報道。	主要報道 [S1]
政権移行期	米側が次期国家安全保障補佐官 Jake Sullivan へ本件を引き継いだと報道。	主要報道 [S1]
2021 年初頭	米サイバー・防衛当局が、中国側アクセスが依然として残っていると認識したと報道。	主要報道 [S1]
2021 年	CYBERCOM が hunt forward team を提案。日本側の慎重姿勢を受け、国内企業調査＋NSA/CYBERCOM レビューの折衷案と報道。	主要報道 [S1]
2021-08-09	中山防衛副大臣が USCYBERCOM を訪問し、Nakasone と戦略的サイバー課題・日米協力を協議。	日米公式 [S4][S5]
2021 年秋	米側が侵害の深刻さを補強する新情報と、日本側対処の進展不足を把握したと報道。	主要報道 [S1]
2021 年 11 月	Neuberger 米国家安全保障副補佐官が訪日。米側が知った方法は sources and methods 保護のため明示できなかったと報道。	主要報道 [S1]
2023-08-07	Washington Post が一連の事案を公表。	主要報道 [S1]
2023-08-08	浜田防衛相：秘密情報漏洩は確認していない。個別具体的攻撃・対応は回答しない。	日本政府一次 [S2]

注目すべきは、2021 年 8 月の中山防衛副大臣による USCYBERCOM 訪問自体は日米双方の公式サイトで確認できるが、その公式説明は一般的な戦略課題・協力であり、2020 年侵害との関係を明示していないことである。[S4][S5] したがって時系列上の近接は確認できても、事件対応の一環だったとは断定しない。

3. NSA は『何を見た』のか

3.1 公開情報で分かる観測結果

- 侵害対象は日本の classified defense networks / most sensitive computer systems と報じられた。[S1]
- アクセスは deep, persistent と表現され、単発侵入ではなく持続的アクセスだったとされる。[S1]
- 狙われた情報として plans, capabilities, assessments of military shortcomings が挙げられる。[S1]
- 2021 年初頭にも中国側がネットワーク内に残っていたとされる。[S1]
- 2021 年秋、米側が侵害の深刻さを補強する fresh information を得たとされる。[S1]

3.2 公開情報で分からないもの

- NSA が最初に検知したセンサー、収集拠点、通信経路。
- マルウェア名、ハッシュ、C2、ドメイン、IP、証明書、プロトコル。
- 侵入口、ゼロデイの有無、資格情報窃取の有無。
- 侵害された具体的ネットワーク名称、装置、ベンダー、拠点。
- PLA の具体的部隊番号、人物、契約企業。
- 『狙った』情報と『実際に窃取された』情報の区別。
- 2021 年秋の fresh information の内容。

3.3 検知経路についての重要な制約

Washington Post は、Neuberger が日本側へ米情報機関の把握方法を明示できなかった理由を、sensitive sources and methods の保護と説明している。[S1] この記述は本調査にとって極めて重要である。公開資料から検知経路を特定できないことは『調査不足』ではなく、情報源保護が明示された構造的な情報空白である。

同記事は、Neuberger が米国側が日本のネットワーク内にいたわけではないことを遠回しに伝えようとしたとも報じる。[S1] これが正確なら、少なくとも日本側内部への直接的な米軍アクセスだけが唯一の観測源だった、という単純な説明には疑問が生じる。しかし、そこから直ちに SIGINT や特定の国外センサーを断定することはできない。

4. 日本政府回答のみ方

2023 年 8 月 8 日の防衛相会見では、第一に『サイバー攻撃により、防衛省が保有する秘密情報が漏洩したとの事実は確認しておりません』と回答した。第二に、記者がハッキング自体の有無を問い直した際、防衛相は『個別具体的なサイバー攻撃やその対応』は対応能力等を明らかにするため回答できないとした。[S2]

したがって、公的記録から導ける最小限の結論は次の通りである。

- 日本政府は Washington Post の侵害報道を公式に認定していない。
- 同時に、侵害そのものを明確に否定してもいない。
- 政府が明示的に否定したのは『秘密情報漏洩を確認した』という状態である。
- 『漏洩を確認できない』は、『侵害が存在しない』とも『漏洩がなかった』とも同義ではない。

ここを言葉の強さで誇張してはならない。一方で、確認不能と不存在を同一視することも技術的に危険である。後述する Trusted Infrastructure 侵害は、その理由を具体的に示す。

5. もう一つの 2020 年 - 外交公電システム報道

2024 年 2 月、日本の外交公電システムが中国側サイバー攻撃を受けたとの報道について、上川外相は報道を承知しているとしつつ、情報セキュリティ事案の性質上、回答を差し控えた。さらに、情報セキュリティは米国等との情報共有・連携強化の基盤だと述べた。[S3]

二次報道では、米側が 2020 年夏に日本へ警告したとされるが、外務省の公式会見は侵害の具体的内容や米側警告を確認していない。[S3] よって、防衛ネットワーク事案と外交公電事案を同一キャンペーンと扱うことはできない。しかし『2020 年前後に、米側が日本政府の高機密ネットワークに関する中国系侵害を先に把握・警告したとの報道が複数存在する』ことは、独立して追跡すべき研究線である。

6. なぜ Fire Ant が重要になるのか

Fire Ant を 2020 年事案の帰属候補として持ち込むのではない。比較対象にする理由は、2025〜2026 年の実インシデント調査が『被害組織が観測に使う基盤そのものを攻撃者が掌握する』技術を具体的に示したからである。

6.1 Fire Ant 2025 - ハイパーバイザー下の盲点

Sygnia は 2025 年、Fire Ant が VMware ESXi/vCenter とネットワーク機器を標的とし、従来型 endpoint security の可視性の外側で活動したと報告した。ESXi では vmsyslogd を停止し、ローカルログとリモート転送の双方を止め、監査証跡を発生源で断つ行為が確認された。また、未登録 VM、VMCI、メモリスナップショットからの資格情報抽出、信頼された経路を使ったセグメント越えなどが報告された。[S10]

6.2 Fire Ant 2026 - Trusted Infrastructure へ

2026 年の Sygnia 報告では、Fire Ant は Cisco IOS XR ルーター、TACACS 認証基盤、Linux 管理ホストを侵害対象へ拡大した。Sygnia は、ルーターを通信・資格情報の収集点として利用し、GRE トンネル、専用 IOS XR ツール、TacTap 等を使って高価値環境への経路を探索したと報告する。[S11]

特に研究上重要なのは、Sygnia が『ground truth の再構成』を防御側課題として明示し、memory、disk、network telemetry、authentication records、configuration state を相互照合する必要性を挙げていることである。[S12] これは、単一ログや管理画面を真実の基準にできない状況を意味する。

7. Fire Ant だけではない - に存在した測欺瞞

7.1 BlackTech

2023 年の日米共同注意喚起は、PRC-linked BlackTech がルーターファームウェアを『without detection』で改変し、海外子会社から日本・米国本社へ trusted relationship を利用してピボットする能力を公表した。[S7][S8] 改変 IOS は通常のロギングを迂回する SSH バックドアを含み、EEM 等を用いた出力・証拠隠蔽も記載される。[S13]

BlackTech は Fire Ant より前から、ネットワーク機器自体を永続化・横展開・証拠隠蔽の基盤に変える発想が中国関連作戦で実在していたことを示す。これは 2020 年事案の技術的説明ではないが、『管理装置が観測者ではなく攻撃面になる』という研究仮説の歴史的裏付けとなる。

7.2 UNC3886

Google Cloud/Mandiant は UNC3886 が TACACS+サーバーを侵害し、LOOKOVER で認証パケットを復号・保存し、さらに正規 tac_plus バイナリを資格情報記録機能付きの悪性版へ置換した事例を報告した。[S9] TACACS+はネットワーク装置の認証・認可・accounting を担うため、ここが侵害されれば、攻撃者はアクセス権だけでなく監査の信頼性にも影響を与え得る。

この点は 2020 年日本事案の研究に直結する。『ログが残っていない』『不正管理操作が確認できない』という観測結果は、ログ生成・認証・管理基盤が健全であることを前提にして初めて強い意味を持つ。

8. 2020 年事案との接続 - 何が言えて、何が言えないか

比較項目	2020 年日本事案	後年の実証事例	評価
持続的アクセス	deep, persistent access と報道	Fire Ant/UNC3886/BlackTech で長期永続化	概念的整合。技術接続は未確認
ネットワーク機器	対象装置非公開	BlackTech/Fire Ant でルーター侵害	比較価値あり。2020 使用証拠なし
認証基盤	非公開	UNC3886/Fire Ant で TACACS 侵害	重要仮説。2020 証拠なし
ログ・証拠操作	非公開	BlackTech/Fire Ant でログ回避・抑制・出力操作	『確認不能』研究に高い関連

外部観測	NSA が発見と報道	具体的センサー非公開	最大の情報空白
中国帰属	PLA 系と報道	BlackTech PRC-linked、UNC3886/Fire Ant China-nexus	同一主体とは扱えない

ここから導ける新しい価値は、帰属の飛躍ではなく『観測モデル』の変更である。従来は被害端末、サーバー、SIEM、EDR 等の証拠を中心に侵害を判断する。しかし Trusted Infrastructure が侵害された場合、ログ生成、ログ転送、認証、ルーティング、仮想化、管理画面の一部が敵対者の制御下に入る。その場合、内部観測だけで侵害不存在を証明することは難しくなる。

9. 測モデル - NSA と日本側の非対称性

本調査では、観測面を次の五層に分ける。

観測面	例	侵害時の問題
Endpoint	EDR、OS ログ、プロセス	ハイパーバイザー/管理層からの操作は見落とし得る
Infrastructure	ルーター、VPN、FW、load balancer	設定・ログ・通信経路そのものが操作され得る
Identity/AAA	TACACS+、RADIUS、AD、SSH 鍵	認証・認可・accounting の証拠価値が低下
Management/Virtualization	vCenter、ESXi、jump host	ゲスト OS 外からの操作、セグメント越え、隠れ VM
External Intelligence	国外通信観測、脅威インフラ、同盟情報等	被害組織内部とは独立した観測。個別 NSA 手法は非公開

仮に上位四層の一部が侵害・欺瞞され、第五層の外部情報機関が攻撃者側から活動を観測した場合、『被害国では確認できないが、同盟国は高確度で侵害を把握する』という非対称は技術的に成立し得る。ただし、これを 2020 年事案の事実認定としてではなく、後年の実証事例から成立可能性が示されたモデルとして扱う。

10. 究上の反件

独自仮説は、反証可能でなければ価値がない。今後、以下の資料が公開されれば仮説を更新する。

- 2020 年侵害の IOC、マルウェア、C2、侵入口、装置種別が公開され、通常 endpoint 中心の侵害だったと判明する。
- 日本側の詳細フォレンジック報告が公開され、内部監視で侵害を把握・除去していたことが確認される。
- NSA/CYBERCOM の機密解除資料により、検知が日本側提供テレメトリだけに依存していたことが確認される。
- PLA 部隊・企業・人物・マルウェアの具体的帰属が公開され、BlackTech/UNC3886/Fire Ant 等との技術的非連続性が明確になる。
- 逆に、ネットワーク機器・AAA・仮想化・ログ抑制を示す 2020〜2021 年の証拠が公開されれば、観測基盤侵害仮説は大幅に強化される。

11. 今後の優先調査

優先度	調査線	具体項目
P0	米側の事件情報	NSA/CYBERCOM/NSC/DoD 関係者の証言、回顧録、議会資料、機密解除文書、FOIA 公開文書。特に 2020 秋、2021 初頭、2021 秋の fresh information。
P0	Nakasone/Pottinger 訪日	訪日日程、面会者、当時の防衛相・首相、NSC 記録、米大使館・NSC 関連公開記録。
P0	Neuberger 2021 年 11 月訪日	訪日記録、会談相手、技術協議、sources and methods に関する後年発言。

P1	日本側ネットワーク構造	2020 年前後の防衛省・自衛隊ネットワーク、認証、SOC、ログ集中、境界機器、調達・更新の公開情報。機密推測は避ける。
P1	2020 以前の中国系 network-device tradecraft	BlackTech、APT40、関連する router firmware/edge device/AAA/LOTL の時系列を 2015〜2021 へ遡る。
P1	外交公電事案	2020 年夏の米側警告報道を一次・準一次資料で再検証し、防衛ネットワーク事案との共通点・相違点を整理。
P2	日米サイバー協力の制度変化	2020〜2023 年の人員・予算・Cyber Defense Command、risk analysis、共同演習、情報共有制度の変化を侵害後の対応として時系列化。

12. 暫定結論 -『確認できない』を研究対象にする

2020 年日本防衛ネットワーク侵害について、公開情報だけで技術的な攻撃経路を再現することは現時点ではできない。Washington Post が報じた NSA の発見、PLA 系帰属、Nakasone/Pottinger 訪日、2021 年までの残存アクセスは重大だが、IOC や侵入経路は公開されていない。[S1]

一方、日本政府の公式記録は、秘密情報漏洩を確認していないことを述べる一方、個別攻撃の有無・対応は明らかにしない。[S2] この状態から『侵害なし』を導くことはできない。

Fire Ant、UNC3886、BlackTech の後年の技術報告は、ネットワーク機器、認証基盤、仮想化基盤、ログ生成・転送が攻撃対象となり、被害側の可視性そのものが損なわれ得ることを実証している。[S7][S9][S10][S11] ここに本研究の新しい価値がある。

次に問うべきは『既知の APT 名のどれだったか』だけではない。NSA が侵害を把握できた観測面と、日本側が公には確認できないとした観測面の差を解明し、その差の中に Trusted Infrastructure の盲点が存在した可能性を、反証可能な形で検証することである。

この研究線は、MISSION-001 の対日 APT 史、MISSION-002 の国家機関-企業-技術者エコシステム、MISSION-003 の Trusted Infrastructure を一つの問題へ収束させる。すなわち、攻撃者が『情報を盗む主体』から『情報が通り、認証され、記録され、監視される基盤そのものを操作する主体』へ進化したとき、日本の防御側は何をもって「確認」と呼べるのか、という問題である。

付録 A - 証拠強度と注意事項

記号	種別	扱い
G1	政府一次資料	その政府が公表した事実・評価として最優先。ただし公表していない事項まで推定しない。
R1	主要報道・複数当局者取材	重要な準一次情報。匿名情報源であるため政府公式確認とは区別。
V1	原著セキュリティ調査	観測した技術事実に強い。国家帰属はベンダー評価として区別。
I	分析推論	複数事実から導く研究仮説。事実と明示的に分離。
U	未確認	公開情報で立証不能。

付録 B - 主要情報源

ID	発行元	資料	URL	区分
S1	Washington Post	Ellen Nakashima, “China hacked Japan’s sensitive defense networks, officials say,” 7 Aug 2023 (updated 8 Aug).	https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/	R1
S2	防衛省	防衛大臣記者会見 令和 5 年 8 月 8 日。	https://www.mod.go.jp/j/press/kisha/2023/0808a.html	G1
S3	外務省	上川外務大臣会見記録 - 中国によるサイバー攻撃（2024 年 2 月）。	https://www.mofa.go.jp/mofaj/press/kaiken/kaikenit_000001_00010.html	G1
S4	USCYBERCOM	Japanese State Minister of Defense Nakayama visits U.S. Cyber Command, 11 Aug 2021.	https://www.cybercom.mil/Media/News/Article/2727713/japanese-state-minister-of-defense-nakayama-visits-us-cyber-command/	G1
S5	防衛省	State Minister Nakayama's Visit to the U.S., Aug 2021.	https://www.mod.go.jp/en/article/2021/08/6513820c0f3f622a23f7a3de9ed288b60f05088b.html	G1
S6	NSA	NSA mission / Nakasone legacy description including foreign signals	https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/	G1

		intelligence mission.	Article/3625189/senate-votes-to-confirm-lt-gen-timothy-haugh-to-lead-cybercom-and-nsacss/	
S7	NSA	U.S. and Japanese Agencies Issue Advisory about China Linked Actors - BlackTech, 27 Sep 2023.	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/	G1
S8	警察庁	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, 27 Sep 2023.	https://www.npa.go.jp/bureau/cyber/koho/caution/caution20230927.html	G1
S9	Google Cloud / Mandiant	Cloaked and Covert: Uncovering UNC3886 Espionage Operations, 2024.	https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations	V1
S10	Sygnia	Fire Ant: A Deep-Dive into Hypervisor-Level Espionage, 24 Jul 2025.	https://www.sygnia.co/blog/fire-ant-a-deep-dive-into-hypervisor-level-espionage/	V1
S11	Sygnia	Fire Ant Evolves: From Hypervisors to Trusted Infrastructure, 27 Aug 2026.	https://www.sygnia.co/blog/fire-ant-evolves-from-hypervisors-to-trusted-infrastructure/	V1
S12	Sygnia	Fire Ant Evolves webinar description - reconstruct ground truth guidance, Sep 2026.	https://www.sygnia.co/webinars/fire-ant-evolves-from-hypervisors-to-trusted-infrastructure-webinar/	V1
S13	IC3 / Joint CSA	People's Republic of China-Linked Cyber Actors Hide in Router Firmware, Sep 2023.	https://www.ic3.gov/CSA/2023/230927.pdf	G1
S14	USCYBERCOM	Posture Statement of Gen. Paul M. Nakasone - China Outcomes Group and NSA/CYBERCOM linkage, 2022.	https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-	G1

			command-before-the/	

付録 C - 本報告の研究上の位置づけ

本報告は MISSION-001〜003 の再要約ではなく、三報で残った空白を埋めるための独立調査である。次回の統合版「中国サイバー作戦エコシステム - 日本を標的とするサイバー作戦の構造と現在地」は、本報告の結果を中核に据えて再構築する。

重要：本報告は、2020 年侵害を Fire Ant、UNC3886、BlackTech へ帰属していない。また、NSA の具体的な収集手段を推定事実として記載していない。後年の実証事例は『観測基盤が侵害されれば確認能力そのものが損なわれる』という技術的可能性を検証する比較材料として使用した。