ネット探検ラボ AI 調査任務

MISSION 002

APT10 Tianjin MSS Huaying Haitai 人物 インフラ 日本標的 調査報告書

公開証拠による完全リンク分析

Project: 中国サイバー作戦エコシステム

調査基準日: 2026 年 9 月 9 日 | 公開情報のみ | 被害組織名は公開確認分に限定

結論の一行要約

公開証拠が最も強く支えるのは「Tianjin State Security Bureau と関連して活動した、Huaying Haitai 所属の請負人を含む APT10 構成員が、長期の技術窃取と MSP 侵害を実行し、日本を直接標的・MSP 経由標的の双方として扱った」という構造である。ただし、APT10 という追跡名の全期間・全サブクラスタを Tianjin MSS へ一括帰属することはできない。

判定語: 〔確認事実〕〔司法当局の主張〕〔政府評価〕〔民間評価〕〔状況証拠〕〔仮説〕〔未確認〕

確度: 高 / 中 / 低（証拠の質・独立性・リンクの直接性を総合）

調査設計・読み方

本報告は、同じ事象を「法的に立証済み」と「捜査機関が起訴状で主張」と「政府の政策・情報評価」と「民間研究者のクラスタリング」に分離する。米国起訴状の事実記載は有罪判決ではなく主張であり、EU 制裁指定は刑事裁判の認定ではない。マルウェア、C2、作業時間、標的選定は帰属を補強するが、それぞれ単独では人物・機関を確定しない。[1][2][5]

ラベル	意味	本報告での使い方
確認事実	公開文書・公開技術データから直接確認可能	文書の存在、記載内容、公開 IOC、公開日等
司法当局の主張	起訴状・指名手配に記載された訴追側の主張	『起訴状は〜と主張』と明記。未決・推定無罪
政府評価	政府・法執行・CERT が公式に示す分析・帰属	情報根拠の非公開部分があり得る
民間評価	原著技術レポートのクラスタリング・帰属	観測範囲と命名体系に依存
状況証拠	WHOIS、アカウント、地理、勤務時間、社会関係等	複数が収束したときのみ補強材
仮説	公開証拠と整合する説明だが未立証	反証可能な形で提示
未確認	一次資料または独立裏付けが不足	人物同定・被害者名は推測しない

出典注は文中の上付き [n] で示し、15 節に URL 付きで列挙した。IOC はすべて歴史的指標であり、現在の悪性・所有・解決先を保証しない。防御用途では現行テレメトリと再検証すること。

目次

1. Executive Summary

最重要判断。Tianjin MSS → Huaying Haitai → Zhu Hua / Zhang Shilong → APT10 → MSP Theft Campaign → 日本、という鎖は、米国の 2018 年起訴状が一つの訴追理論として明示する。起訴状は両名が Huaying Haitai で勤務し、Tianjin State Security Bureau（TSSB）と関連して行動し、APT10 の侵入作戦に従事したと主張する。Zhu は侵入・採用・インフラ登録、Zhang はマルウェア開発・試験・インフラ登録を担ったとされる。これは強い公的帰属だが、有罪判決による確定事実ではない。[1][2][3]

EU は 2020 年、Operation Cloud Hopper への支援・関与を理由に Huaying Haitai、Gao Qiang、Zhang Shilong を制裁対象へ追加した。EU 文書は Gao を C2 インフラ、Zhang を開発・試験したマルウェアで作戦へ結び、会社が資金・技術・物的支援を提供し促進したと記載する。Zhu ではなく Gao を指定した点は、米起訴状と相補的である。[5][6]

日本リンクは二種類ある。第一は、MSP Theft Campaign で侵害された MSP の顧客所在 12 か国に日本が含まれるという司法主張。第二は、2014 年以降の日本の学術・製薬・製造・政府関連を狙った直接攻撃で、ChChes、PlugX、Poison Ivy、RedLeaves、日本語ルアーなどが民間原著と JPCERT/CC により観測された。公開資料は一般に組織カテゴリまでで、固有の被害組織名や、個々の日本攻撃を Zhu/Zhang へ直接割り当てる証拠は示していない。[2][10][11][12][14][15]

2019 年以後の A41APT／Cicada は、複数ベンダーが APT10 へ帰属または関連付けた日本重視の活動である。ただし侵入経路・マルウェアが変化し、JPCERT/CC の会議報告は APT10 と BlackTech の双方との可能性を記す。MirrorFace／Earth Kasha について日本警察庁は『中国の関与が疑われる』と公式評価するが、APT10、Huaying Haitai、Tianjin MSS との同一性は述べない。したがって本報告は後続・関連クラスタとして別枠に置く。[18][19][20][21][22]

Key Judgments

① 2006–2018 の起訴対象コアと Tianjin MSS の結び付き：高（ただし司法主張）／② Huaying Haitai が Cloud Hopper を支援・促進：高（EU 政府評価）／③ 日本が直接・間接の重点標的：高／④ 公開 IOC から Zhu または Zhang を特定の日本被害へ直結：低・未確認／⑤ 2019 年以後の全 APT10 ラベルを同じ Tianjin セルへ帰属：不支持。

リンク	最良の公開根拠	区分	確度
TSSB ↔ Zhu/Zhang/Huaying	米起訴状・FBI 指名手配	司法主張	高
Huaying ↔ Gao/Zhang ↔ Cloud Hopper	EU 制裁規則	政府評価	高
APT10 ↔ MSP Theft Campaign	起訴状、PwC/BAE、ACSC/NCSC	司法主張＋政府/民間評価	高
Cloud Hopper ↔ 日本	起訴状の 12 か国、技術報告の日本標的	司法主張＋民間評価	高
人物 ↔ 特定日本 IOC/被害者	公開資料に直接マッピングなし	未確認	低
MirrorFace/Earth Kasha ↔ historic APT10	ツール・標的の重なりはあるが政府は別名として記載せず	仮説	低〜中

2. APT10 活動史

時期	活動・公開観測	証拠区分	注意点
2006–2008	米起訴状は Technology Theft Campaign 開始を約 2006 年とし、45 超の組織・90 台程度のコンピュータへの不正アクセス等を主張。	司法主張	後年のベンダー命名を遡及適用
2009–2013	FireEye は 2009 年から追跡。Poison Ivy、SOGU 等、航空宇宙・防衛・通信・政府を標的。	民間評価	共有マルウェア単独では不十分
2014–2015	Unit 42 は少なくとも 2014 年から日本組織を標的。起訴状は MSP Theft Campaign を少なくとも 2014 年開始とする。	民間評価＋司法主張	直接攻撃と MSP 経由を分離
2016–2017	日本の学術・製薬・製造、世界の MSP を攻撃。ChChes、RedLeaves、PlugX、QuasarRAT、PowerSploit。PwC/BAE が Cloud Hopper 公表。	民間評価＋JPCERT 観測	Cloud Hopper は作戦名
2018	米英豪日等が APT10 を非難・帰属。Zhu/Zhang 起訴。起訴状は活動が 2018 年まで継続と主張。	司法主張＋政府評価	国家発表は根拠開示量が異なる
2019–2020	A41APT/Cicada が日本企業・海外拠点を標的。VPN 侵害、Ecipekac、SodaMaster、Hartip、ZeroLogon。	民間評価	historic core との同一性は推定
2021–2022	JPCERT/CC・Kaspersky が A41APT を分析。Trend は Earth Tengshe を menuPass/APT10 関連と推測。	民間評価	関連 ≠ 同一
2024–2025	ANEL/LODEINFO を使う Earth Kasha/MirrorFace が日本を攻撃。警察庁/NISC は中国関与疑いと評価。	政府評価＋民間評価	APT10/TSSB の明示帰属なし

活動史の読み方：『APT10』は単一の固定チーム名ではなく、ベンダーが長期間の技術・標的・インフラの重なりを束ねた追跡ラベルである。時間とともに作戦担当、請負人、マルウェア、侵入経路が変わる可能性を前提にする。[14][17]

3. Alias 整理

名称	命名主体/用法	本報告の扱い
APT10	FireEye/Mandiant 等。米司法省も採用	中核の共通呼称
menuPass	FireEye/Unit 42。Poison Ivy パスワード由来と説明	APT10 と強く重なる
Stone Panda	民間ベンダー名。米司法省・MITRE が別名列挙	強い重なり
Red Apollo	PwC 系の呼称。米司法省・MITRE が別名列挙	強い重なり
CVNX	BAE 等。Zhu Hua の別名にも CVNX がある	actor alias と個人 alias の衝突に注意
POTASSIUM	Microsoft 呼称。米司法省・MITRE に列挙	強い重なり
BRONZE RIVERSIDE	Secureworks 呼称、MITRE に関連名	範囲差の可能性
Cicada	Symantec 呼称。2019–20 活動を APT10 と同義運用	後期クラスタ
Operation Cloud Hopper	PwC/BAE の MSP 作戦名	actor alias ではなくキャンペーン
MSP Theft Campaign	米起訴状の法的記述名	Cloud Hopper と大幅重複するが完全同義と断定しない
A41APT	2019–20 のキャンペーン名	Kaspersky は高確度 APT10、JPCERT 会議報告は可能性
Earth Tengshe	Trend の関連グループ	menuPass/APT10『関連』。同一扱いしない
MirrorFace / Earth Kasha	警察庁は相互の別名とする	中国関与疑い。APT10/TSSB 同一性は未確認

MITRE ATT&CK 自身の関連名一覧は有用な索引だが、ベンダーの可視性・定義が異なるため、名称の一致を組織同一性の証拠にしない。[17]

4. 組織・人物関係

主体	公開された役割/関係	区分	評価
中国国家安全部（MSS）	英国等は APT10 が MSS のために行動したと評価。	政府評価	組織レベルは高、内部指揮線は非公開
Tianjin State Security Bureau	MSS 地方機関。米起訴状は被告らが同局と関連して行動と主張。	司法主張	高
Huaying Haitai	天津の企業。米起訴状は Zhu/Zhang の勤務先、EU は Cloud Hopper 支援・促進主体と記載。	司法主張＋政府評価	高
Zhu Hua（朱华）	penetration tester、侵入、インフラ登録、他者採用と起訴状。	司法主張	高
Zhang Shilong（张士龙）	マルウェア開発・試験、インフラ登録。Huaying 勤務。	司法主張＋政府評価	高
Gao Qiang（高强）	EU は C2 インフラを通じ Cloud Hopper へ関与、Huaying 勤務と記載。	政府評価	高
Zheng Yanbin	メール/WHOIS から APT10 インフラ管理者とする匿名 OSINT。	状況証拠	中〜低
Fang Ting / Sun Jie / Feng Tao	企業データベース上の株主・管理者との匿名 OSINT 記載。	未確認	低
Laoying Baichen Instruments	Gao と電話・住所で結ぶ匿名 OSINT。APT10 支援企業との政府認定なし。	状況証拠	低

5. Tianjin MSS–Huaying Haitai 関係

〔司法当局の主張〕米起訴状は、Zhu Hua と Zhang Shilong が天津の Huaying Haitai で働き、MSS の Tianjin State Security Bureau と『in association with』行動したと記す。公開起訴状は、契約書、支払記録、指示書、上司名など指揮統制の生資料を開示していない。従って『TSSB の正式職員』『会社が 100%フロント企業』までを公開証拠だけで確定できない。[1][2]

〔政府評価〕EU 制裁規則は Huaying Haitai が Operation Cloud Hopper に資金・技術・物的支援を提供し、作戦を促進したと記載する。Gao Qiang と Zhang Shilong の勤務先としても結び付ける。これは会社を単なる偶然の雇用主より一段強く作戦支援主体として扱う政府認定である。[5][6]

〔状況証拠〕Intrusion Truth は、Huaying の求人、企業データベース、ドメイン WHOIS、Gao とされるアカウントの移動記録を用い、Huaying 所在地から TSSB 所在地とされる 85 Zhujiang Road への反復移動を主張した。記事は情報提供者と原データの全体を公開しておらず、Uber 領収書だけで指揮関係は立証できない。ただし、その後の米起訴・EU 制裁が会社・人物の一部を独立に公的資料へ載せたため、先行 OSINT の一部は後から補強された。[26][27]

最小限に言えること

Huaying Haitai は、公開政府文書上、Cloud Hopper を支援・促進し、少なくとも Zhang と Gao を雇用した天津企業である。米起訴状上は Zhu も勤務し、Zhu/Zhang は TSSB と関連して行動した。会社の法的地位、契約形態、TSSB 担当官、支払経路は未公開。

6. Zhu Hua / Zhang Shilong

項目	Zhu Hua（朱华）	Zhang Shilong（张士龙）
公開 alias	Afwar / CVNX / Alayos / Godkiller	Baobeilong / Zhang Jianguo / Atreexp
米起訴状の役割	侵入テスト担当。ドメイン/ハッキングインフラ登録、侵入実行、構成員募集	ドメイン/ハッキングインフラ登録、APT10 用マルウェア開発・試験
勤務先	Huaying Haitai（司法主張）	Huaying Haitai（司法主張＋EU 政府評価）
TSSB 関係	TSSB と関連して行動（司法主張）	TSSB と関連して行動（司法主張）
Cloud Hopper	起訴状の MSP Theft Campaign 構成員	起訴状＋EU 制裁で Cloud Hopper 関与
法的状態	2018 年米国で起訴。公開資料上、有罪確定を確認せず	2018 年米国で起訴。EU 制裁対象。公開資料上、有罪確定を確認せず
日本との直接線	MSP 顧客国として日本を含む共同謀議の主張。特定 IOC/被害者との個人直結なし	同左。個別日本攻撃への直接割当なし

Zhang の公開 OSINT。『baobeilong』の GitHub が QuasarRAT と Trochilus を fork し、xiaohong[.]org の過去 WHOIS が Zhang Shilong、atreexp@yahoo.com.cn、天津住所を示したと Intrusion Truth は報告した。この鎖は、起訴状に Baobeilong/Atreexp が Zhang の別名として掲載されたことで重要部分が公的に追認された。しかし GitHub の関心だけでマルウェア作者性は証明されない。[2][25]

Zhu については起訴状が役割を詳述する一方、公開 WHOIS から特定の日本向け C2 へ一対一で接続する資料は本調査では確認できなかった。『Zhu が日本攻撃 X を操作した』という表現は避けるべきである。[2]

7. 日本関連活動年表

年月/期間	日本関連活動	標的カテゴリ	区分・確度
約 2011〜	LAC は menuPass が日本を標的にし始めた時期を約 2011 年とする。	大学、政府関係施設等	民間評価・中
2014〜	Unit 42 は日本の個人・組織を少なくとも 2014 年から標的と評価。	防衛/政策関係を含む組織	民間評価・中〜高
2016 年 6 月	FireEye が日本の大学への攻撃を初期検知し、より広範な日本標的を発見。	大学、製造等	民間観測・高
2016 年 9–11 月	Unit 42 が日本の科学系研究者、製薬、日系製造業の米子会社を標的とする ChChes/PlugX/PIVY 活動を報告。	学術・製薬・製造	民間観測・高
2016 年 10 月〜	JPCERT/CC が日本組織宛の ZIP 添付、実在人物なりすまし、日本のフリーメール、ChChes 感染を確認。	複数の日本組織	CERT 観測・高
2017 年 1 月	『【H 29 科研費】繰越申請について.zip』 →LNK→PowerShell→ChChes。hamiltion.catholicmmb[.]com へ通信。	日本の教育/研究部門	民間技術観測・高
2017 年 2–4 月	RedLeaves 被害を JPCERT/CC が確認。Trochilus 派生、PlugX とのコード/C2 重複を報告。	日本組織（固有名非公開）	CERT 観測＋推定・中〜高
2018 年 12 月	日本政府が中国拠点 APT10 による民間企業・学術機関等への長期かつ広範な攻撃を非難。	民間・学術等	政府評価・高
2019 年 3 月–2021 年 1 月	A41APT。日本企業と海外拠点、SSL-VPN 侵害、Ecipekac/SodaMaster/P8RAT 等。	製造ほか企業・海外拠点	民間評価・中〜高
2019 年 10 月–2020 年 10 月	Symantec Cicada。日本関連企業と 17 地域の子会社、製造・自動車・製薬・MSP 等。	企業・政府を含む複数業種	民間評価・中〜高

年月/期間	日本関連活動	標的カテゴリ	区分・確度
2021 年	Trend は Earth Tengshe を menuPass/APT10 関連と推測し、電子・エネルギー・自動車・防衛関連を標的と報告。	先端産業・防衛	民間評価・中
2024–2025	MirrorFace/Earth Kasha が安全保障・先端技術情報を狙うと警察庁/NISC。	組織・事業者・個人	政府評価・高（中国関与疑い）／APT10 同一性は未確認

公開確認できる日本語ルアー/件名例：『日米拡大抑止協議』『平成 29 年日米安保戦略対話提言(未定稿).exe』『日米関係重要事項一覧表.exe』『安全保障条約変更通知.exe』『【H 29 科研費】繰越申請について.zip』、および英語件名『[UNCLASSIFIED] The impact of Trump’s victory to Japan』。これらは外交・安全保障・研究費・学術手続を利用した社会工学を示す。[12][15]

標的の厳密な範囲。公開根拠が強いのは『日本の大学/科学系研究者、製薬、製造、政府関連/政策関係、MSP、日本企業の海外拠点』というカテゴリである。具体的被害組織名や侵害成否は、原著が伏せている場合は本報告でも推測しない。

8. MSP / Operation Cloud Hopper

Operation Cloud Hopper は、PwC UK と BAE Systems が 2017 年に公表した、MSP とその顧客の信頼関係を悪用する大規模作戦の呼称である。米起訴状の『MSP Theft Campaign』は少なくとも 2014 年開始とされ、MSP 侵害後にマルウェアを置き、認証情報を窃取し、RDP で横展開し、顧客データを暗号化アーカイブ化して複数の侵害済み MSP/顧客システムを経由後に持ち出す流れを主張する。[2][12][13]

1. MSP へ初期侵入。公開報告は複数経路を扱うが、個別事案の初期ベクトルは常に判明していない。[12][13]
2. PlugX、RedLeaves、QuasarRAT 等を正規ファイルに偽装・DLL side-loading で設置。[2][12]
3. 資格情報窃取ツールで管理者認証情報を取得。[2][12]
4. RDP、WMI、PsExec/Impacket 系、管理共有等で MSP と顧客ネットワークを横断。[2][12][17]
5. 関心データを RAR/TAR 等で暗号化・圧縮し、一時保管。[2][12]
6. 他の侵害済み MSP/顧客端末を経由して最終 C2 へ流し、痕跡を削除。[2]

スケール。起訴状は MSP 作戦で約 1,300 の一意な悪性ドメインを登録し、一部アカウントは 2010 年頃から開設されたと主張する。ある MSP と顧客は日本を含む 12 か国に所在した。BAE はインフラが数千ノード規模で相互接続し、観測可能性の限界から総数は不明とした。[2][13]

独立政府裏付け。豪 ACSC は豪州企業が MSP 経由で侵害された事案の TTP が Cloud Hopper と整合すると公表。英国 NCSC は APT10 の MSP 侵害が英国組織への広いアクセスを促進したと評価した。[4][7]

Cloud Hopper ≠ APT10 全体

Cloud Hopper/MSP Theft Campaign は APT10 追跡範囲の重要な一作戦群である。日本への直接スピアフィッシング、Technology Theft Campaign、後期 A41APT をすべて Cloud Hopper と呼ぶのは不正確。

9. Malware / TTP

系統	役割・特徴	日本/作戦との関係	帰属上の注意
Poison Ivy (PIVY)	汎用 RAT、keylogging 等。menuPass パスワード・C2/WHOIS で追跡。	2009–14 中心、日本を含む初期活動	多数 actor が使用
PlugX	モジュール型 RAT。DLL side-loading、443/TCP 等。	日本攻撃と MSP の持続アクセス	中国系多数 actor が使用
EvilGrab	初期侵入・偵察・監視機能。	日本/東南アジア標的	共有性あり
ChChes	HTTP Cookie に暗号化データ、モジュール受信、AES 追加。	2016–17 日本学術・政府関連で強い観測	当時 Unit 42 は比較的固有と評価
RedLeaves	Trochilus 派生、RC4、HTTP/custom、process injection。	2016–17 日本。PlugX とコード/C2 重複	同一 actor は推定
QuasarRAT	オープンソース RAT のカスタム版。	Cloud Hopper、後期 FYAnti payload	公開コード由来
HAYMAKER/SNUGRIDE/BUGJUICE	2016–17 に FireEye が APT10 固有性を評価した新規 backdoor 群。	世界作戦、日本再活性化期	観測範囲依存
ANEL / UPPERCUT	日本中心に使われた backdoor。バージョン更新・難読化。	2017 後半以降、日本標的	後年 Earth Kasha でも再登場、同一 cell 未確認
Ecipekac/DESLoader	多層 fileless loader。SodaMaster/P8RAT/FYAnti を展開。	A41APT、日本企業/海外拠点	Kaspersky 高確度、別研究は可能性評価
LODEINFO	日本の政策・安全保障標的で更新を継続。	2019 以降、日本中心	APT10 umbrella 関連。historic core 直結なし
Hartip / living-off-the-land	Cicada での独自 backdoor、WMI/PowerShell/ZeroLogon。	2019–20 日本関連企業	Symantec 帰属

代表 TTP：スピアフィッシング添付、LNK/Office/二重拡張子、パスワード付き ZIP、PowerShell/PowerSploit、DLL search-order hijacking、プロセス注入、Mimikatz/secretsdump、RDP/WMI/PsExec、ネットワーク探索、正規ツールの改名、RAR/TAR 暗号化、MSP 信頼関係の悪用、DDNS による C2 切替、公開レポート後のインフラ・マルウェア更新。[2][12][14][17]

技術的帰属の重み。比較的強いのは、複数キャンペーンを跨ぐ独自マルウェア実装、複数段のインフラ重複、運用上の癖、標的の連続性、公開後の同時切替が収束する場合。弱いのは、PlugX/PIVY/Quasar/Trochilus、DLL side-loading、PowerShell のような広く共有される要素だけの一致。

10. IOC・インフラ関係

以下は主要リンクを検証するための選抜 IOC であり、完全なブロックリストではない。ドメインは安全のため [.] で無害化した。

種別	IOC（無害化）	観測/関係	出典・区分
C2	js001.3322[.]org → 222.35.137[.]193	Poison Ivy sample b08694…、APT10 旧活動。	FireEye 起点＋匿名 OSINT
C2	weile3322b.3322[.]org → 222.35.137[.]193	同 IP へ 2010–12 解決と OSINT。	状況証拠
送信元 IP	218.67.128[.]26	2010 phishing header、China Unicom 天津。hostname fisherxp-pc と報告。	匿名 OSINT/二次解析
C2	last.p6p6[.]net	PIVY MD5 08A268…、password happyyongzi。	PwC 原著
WHOIS email	wangtongbao1957@gmail[.]com	last.p6p6[.]net 登録と PwC。	民間技術観測
C2	nttdata.otzo[.]com:443	PlugX beacon 例。名称はブランド模倣で被害者認定ではない。	PwC 原著
ChChes C2	area.wthelpdesk[.]com / dick.ccfchrist[.]com / kawasaki.cloud-maste[.]com / kawasaki.unhamj[.]com / sakai.unhamj[.]com	日本向け ChChes。	JPCERT/CC＋Unit 42
ChChes C2	scorpion.poulsenv[.]com / trout.belowto[.]com / zebra.wthelpdesk[.]com / gavin.ccfchrist[.]com	日本向け ChChes。	JPCERT/CC
教育ルアー C2	hamiltion.catholicmmb[.]com	H29 科研費 LNK→PowerShell→ChChes。	PwC＋JPCERT/CC
配布 URL	goo[.]gl/cpT1NW → koala.acsocietyy[.]com/acc/image/20170112001.jpg	画像偽装 PowerShell。	PwC 原著
RedLeaves C2	mailowl.jkub[.]com / windowsupdates.itemdb[.]com / microsoftstores.itemdb[.]com / 67.205.132[.]17 / 144.168.45[.]116	RedLeaves/PlugX 関係を分析。	JPCERT/CC
hash	0B6845FBFA54511F21D93EF90F77C8DE (MD5)	H29_c-26.lnk。	PwC 原著

種別	IOC（無害化）	観測/関係	出典・区分
hash	5262cb9791df50fafcb2fbd5f93226050b51efe400c2924eecba97b7ce437481	RedLeaves SHA-256。	JPCERT/CC
hash	fcccc611730474775ff1cfd4c60481def586f01191348b07d7a143d174a07b0	PlugX SHA-256。	JPCERT/CC

人物・企業に関連して公開されたメール/ドメイン（証拠別）

識別子	公開された接続	証拠区分・限界
atreexp@yahoo.com[.]cn	xiaohong[.]org の 2007 年 WHOIS で Zhang Shilong とされた。atreex[.]cn にも関連。	匿名 OSINT。起訴状が Atreexp を Zhang alias として追認
robin4700@foxmail[.]com	2016 年に xiaohong[.]org WHOIS が変更されたと報告。	匿名 OSINT
baobei@xiaohong[.]org	baobeilong と xiaohong[.]org を結ぶ投稿。	匿名 OSINT
420192@qq[.]com	Gao Qiang とされる Uber 領収書・移動記録。	未公開提供データに依存。状況証拠
zhengyanbin8@gmail[.]com	FireEye PIVY 資料の APT10 関連ドメイン登録者として OSINT が展開。	人物同一性は未確認
zhangduker@gmail[.]com	huayinghaitai[.]com WHOIS と関連ドメイン群。	匿名 OSINT。Zhang Shilong との同一性は未確認
masao_tomikawas@yahoo[.]com	2010 phishing の送信元表示/アカウントとして報告。	日本人被害者・実在人物とは断定不可

WHOIS は転用・虚偽登録・privacy proxy があり得る。ドメイン解決先も共有 hosting や再割当がある。メールアドレス一致は、同一人物性を補強しても、それ自体で政府機関との関係や操作主体を確定しない。

11. Person → Infrastructure → Campaign → Japan リンク分析

リンク鎖	公開証拠	判定
Zhu → 悪性ドメイン/インフラ → APT10 campaigns	起訴状が登録・侵入実行を具体的役割として主張。個別 IOC 名は非開示。	司法主張・高
Zhang → マルウェア/インフラ → APT10 campaigns	起訴状が開発・試験・登録を主張。EU は Cloud Hopper へマルウェアで接続。	司法＋政府・高
Gao → C2 infrastructure → Cloud Hopper	EU 制裁理由が C2 を通じた関与を記載。具体 IOC は公表文に不掲載。	政府評価・高
Zheng → WHOIS/domain 群 → historic APT10	zhengyanbin8 メールと複数ドメイン。匿名 OSINT。	状況証拠・中〜低
Zhang/baobeilong → Trochilus/Quasar 関心 → RedLeaves/Quasar	公開アカウントの fork と起訴 alias の一致。コード関心は開発証明ではない。	状況証拠・中
APT10 infrastructure → ChChes/PlugX/PIVY → 日本	複数原著の C2 重複、imphash、PIVY password、直接観測。	民間評価＋CERT・高
APT10 → MSP → 日本顧客	起訴状が日本を含む 12 か国の顧客データ侵害を主張。	司法主張・高
Zhu/Zhang/Gao → 特定 IOC → 特定日本被害者	公開資料に一対一対応なし。	未確認・低
TSSB → 特定日本攻撃命令	命令文書・担当官・要件・支払記録は非公開。	未確認

最も強い『完全鎖』と、その切れ目

TSSB〔司法主張〕→ Huaying〔司法＋EU 評価〕→ Zhu/Zhang/Gao〔役割記載〕→ APT10/Cloud Hopper〔政府・司法・民間収束〕→ MSP または日本向け malware〔技術観測〕→ 日本の標的カテゴリ〔公的/民間観測〕。切れ目は、① TSSB 内部の具体的指示、②個人と固有 IOC の公開対応、③固有の日本被害組織への最終対応である。

12. Attribution 評価

評価命題	確度	根拠	留保
2006–2018 コア APT10 に中国拠点・天津要素がある	高	起訴状、勤務時間/IP、複数政府評価	情報源の一部非公開
Zhu/Zhang が Huaying で APT10 作戦に従事	高（司法主張）	役割を具体化した米起訴状/FBI	未決で有罪確定ではない

評価命題	確度	根拠	留保
Huaying が Cloud Hopper を支援・促進	高（政府評価）	EU 制裁規則、英政府支持	契約/支払生資料は非公開
TSSB がコア活動に関与	高（政府/司法評価）	米起訴状、英政府等	指揮命令の具体像は不明
日本が重点標的	高	JPCERT、Unit42、PwC、FireEye、政府談話、後期観測	被害者固有名は限定
Cloud Hopper と起訴状 MSP Theft Campaign は同じ活動群	高だが完全同義は留保	時期・手口・標的・公表タイミングが一致	法的境界とベンダー境界が違う
2019–20 A41APT/Cicada は APT10	中〜高（民間評価）	Kaspersky 高確度、Symantec、標的/TTP/ツール連続	JPCERT 会議報告は BlackTech 可能性も
MirrorFace/Earth Kasha は TSSB の historic APT10 セル	低	日本重視、ANEL/LODEINFO 等の系譜	警察庁は APT10/TSSB と明記せず

総合評価。APT10 という追跡名の背後には、少なくとも一時期、国家安全機関の地方局と関連する民間企業所属の技術者・侵入担当、専用/改変マルウェア、借用ツール、DDNS・actor 登録ドメイン・侵害済み端末から成る分散インフラ、直接標的型メールと MSP サプライチェーン侵害を併用する運用モデルがあった。日本は単なる偶発的被害国ではなく、学術・研究、製造、製薬、政府/外交・安全保障関係、MSP と海外拠点を含む持続的な重点であった。[2][4][5][10][12][14][15]

しかし『APT10』は分析上の傘であり、すべての年代・マルウェア・関連クラスタを同一の会社・同一の二人・同一地方局へ還元できない。最も堅牢なのは 2018 年起訴対象のコアと Cloud Hopper までで、後期活動ほど民間クラスタリングへの依存が増える。

13. 反証・矛盾

論点	反証/別解釈	本報告の処理
中国政府の否認	中国外務省は米国等の主張を中傷として否定。	否認を記録。公開技術・司法資料との比較では代替説明の具体証拠は提示されていない
起訴 ≠ 有罪	被告不在のままの起訴は反対尋問・公判検証を経ていない。	全記載を『司法主張』に限定
政府声明の循環参照	同盟国声明が米起訴/共有情報に依存し、完全に独立でない可能性。	独立観測の JPCERT、PwC/BAE、Unit42、FireEye を併記
共有 malware	PIVY、PlugX、Quasar、Trochilus は広く利用可能。	単一サンプルから人物/国家へ帰属しない
共有 hosting/DDNS	同一 IP・DDNS は複数利用者や再割当の可能性。	時間窓、複数ドメイン、登録者、malware config の収束を要求

論点	反証/別解釈	本報告の処理
会社の実態	Huaying に正規のセキュリティ業務があった可能性。	政府文書は作戦支援を認定するが、会社全業務を諜報フロントと断定しない
Gao/Zhu の不一致	米起訴は Zhu/Zhang、EU 制裁は Gao/Zhang。	矛盾ではなく異なる証拠・法的目的の可能性。相補的だが完全名簿ではない
活動空白/再編	Trend は menuPass/APT10 が 2018 年末を最後に見えなくなり関連 Earth Tengshe が 2019 年頃開始とする。	後期を継続性評価にし、同一 cell と断定しない
A41APT の競合帰属	JPCERT 会議報告は APT10 と BlackTech 双方の可能性。	Kaspersky の高確度評価と併記し不確実性を残す
MirrorFace の混同	日本重視・ANEL/LODEINFO だけで historic APT10 と同一視し得る。	警察庁の公式範囲（中国関与疑い）を超えない

別解釈。Huaying は TSSB が必要に応じて業務を委託した複数請負業者の一つで、APT10 は複数チームの重なりだった可能性がある。Zhu/Zhang/Gao が全期間を通じて同一役割だった証拠もない。このモデルは alias の揺れ、ツール共有、2018 年後のクラスタ分裂を説明しやすいが、公開証拠だけでは確定できない。

14. 未解決事項

- Tianjin SSB 側の担当部署・担当官・tasking 文書・契約・支払経路。
- Huaying Haitai の現行法人状態、実質株主、財務、従業員名簿、正規事業と秘密作戦の比率。
- Zhu Hua の具体的オンライン識別子と、個別ドメイン/マルウェア/日本案件への公開マッピング。
- Gao Qiang と fisherxp、Zheng Yanbin、Laoying Baichen の関係を裏付ける一次資料。
- 約 1,300 ドメインの完全リスト、登録アカウント、課金情報、時系列、各キャンペーン割当。
- 日本所在 MSP/顧客の固有名、侵害範囲、窃取情報、通知・復旧の公開可能部分。
- Technology Theft Campaign と日本の直接標的型攻撃の運用者・インフラ共有度。
- 2018 年後の A41APT/Cicada/Earth Tengshe/LODEINFO/Earth Kasha 間の人員・インフラ・コード系譜。
- 中国国内の他地方局・軍・請負会社との役割分担、インフラ再利用の仲介者。
- 起訴後の Zhu/Zhang の所在、司法手続の進展、EU 制裁の更新・解除状況。

15. 重要一次資料・原著資料

[1] U.S. DOJ, ‘Two Chinese Hackers … Charged …’ (2018-12-20) — https://www.justice.gov/usao-sdny/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer

[2] United States v. Zhu Hua and Zhang Shilong, Sealed Indictment, 18 Cr. (S.D.N.Y., 2018) — https://nsarchive.gwu.edu/sites/default/files/documents/5691919/United-States-of-America-v-Zhu-Hua-and-Zhang.pdf

[3] FBI Wanted: APT 10 Group — https://www.fbi.gov/wanted/cyber/apt-10-group

[4] UK NCSC, ‘APT10 continuing to target UK organisations’ (2018) — https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations

[5] Council Implementing Regulation (EU) 2020/1125 — https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1125

[6] UK Government, EU sanctions against malicious cyber actors (2020) — https://www.gov.uk/government/news/foreign-secretary-welcomes-first-eu-sanctions-against-malicious-cyber-actors

[7] Australian Cyber Security Centre, MSP Investigation Report (2018) — https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/msp-investigation-report

[8] 外務省『外交青書 2023』第 3 章（APT10 に関する 2018 年日本政府対応の記録） — https://www.mofa.go.jp/mofaj/gaiko/bluebook/2023/html/chapter3_01_03.html

[9] 防衛省『令和 4 年版防衛白書』サイバー空間における脅威の動向 — https://www.clearing.mod.go.jp/hakusho_data/2022/html/n140302000.html

[10] JPCERT/CC, ChChes – Malware that Communicates … Using Cookie Headers (2017) — https://blogs.jpcert.or.jp/en/2017/02/chches-malware--93d6.html

[11] JPCERT/CC, RedLeaves – Malware Based on Open Source RAT (2017) — https://blogs.jpcert.or.jp/en/2017/04/redleaves---malware-based-on-open-source-rat.html

[12] PwC UK / BAE Systems, Operation Cloud Hopper Technical Annex (2017) — https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-technical-annex-april-2017.pdf

[13] BAE Systems, APT10: Operation Cloud Hopper (2017) — https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html

[14] FireEye/Mandiant, APT10 (MenuPass Group): New Tools, Global Campaign (2017) — https://cloud.google.com/blog/topics/threat-intelligence/apt10-menupass-group

[15] Palo Alto Networks Unit 42, menuPass Returns … Japanese Academics and Organizations (2017) — https://unit42.paloaltonetworks.com/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/

[16] LAC, Cyber attacks targeting Japanese organizations (menuPass) (2017) — https://www.lac.co.jp/english/report/2017/08/30_alert_01.html

[17] MITRE ATT&CK, menuPass (G0045) — https://attack.mitre.org/groups/G0045/

[18] Kaspersky GReAT, APT10 / Ecipekac in A41APT (2021) — https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

[19] JPCERT/CC, JSAC2021 2nd Track – A41APT case (2021) — https://blogs.jpcert.or.jp/en/2021/02/jsac2021report2.html

[20] Symantec/Broadcom, Japan-Linked Organizations Targeted … Cicada (2020) — https://www.security.com/threat-intelligence/cicada-apt10-japan-espionage

[21] 警察庁/NISC『MirrorFace によるサイバー攻撃について（注意喚起）』(2025) — https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html

[22] Trend Micro, 国内標的型攻撃分析レポート 2022 年版 発表 — https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220510-01.html

[23] Intrusion Truth, Who is Mr Zheng? (2018) — 匿名 OSINT — https://intrusiontruth.wordpress.com/2018/07/30/who-is-mr-zheng/

[24] Intrusion Truth, Who is Mr Gao? (2018) — 匿名 OSINT — https://intrusiontruth.wordpress.com/2018/08/02/who-is-mr-gao/

[25] Intrusion Truth, Who is Mr Zhang? (2018) — 匿名 OSINT — https://intrusiontruth.wordpress.com/2018/08/06/who-is-mr-zhang/

[26] Intrusion Truth, Huaying Haitai and Laoying Baichen (2018) — 匿名 OSINT — https://intrusiontruth.wordpress.com/2018/08/09/was-apt10-the-work-of-individuals-a-company-or-the-state/

[27] Intrusion Truth, APT10 was managed by the Tianjin bureau … (2018) — 匿名 OSINT — https://intrusiontruth.wordpress.com/2018/08/15/apt10-was-managed-by-the-tianjin-bureau-of-the-chinese-ministry-of-state-security/

[28] Reuters, China denies economic espionage charges (2018) — 反対見解 — https://www.reuters.com/article/world/china-denies-slanderous-economic-espionage-charges-from-us-allies-idUSKCN1OK08U/

[29] JPCERT/CC JSAC2019 Archive – APT10 ANEL presentation — https://jsac.jpcert.or.jp/archive/2019/index.html

[30] Virus Bulletin, Defeating APT10 compiler-level obfuscations / ANEL (2020) — https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-defeating-apt10-compiler-level-obfuscations/

[31] Kaspersky, Tracking down LODEINFO 2022, Part I — https://securelist.com/apt10-tracking-down-lodeinfo-2022-part-i/107742/

[32] Trend Micro, Earth Kasha's LODEINFO campaign and APT10 umbrella correlation (2024) — https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.html

証拠の優先順位

7. 起訴状・制裁規則・政府/CERT 公式文書（ただし法的性質と未公開根拠を明示）。
8. 原著技術レポート（観測範囲、命名体系、固有/共有ツールを区別）。

9. 匿名 OSINT・報道（一次情報への参照があり、後続公的資料で補強された部分のみ限定利用）。

16. 次 MISSION 候補

候補	目的	優先度
MISSION-003: APT10 1,300 ドメイン復元	起訴状・PwC/BAE・Unit42・passive DNS・証明書・WHOIS から時系列グラフを構築し、人物メールとの公開リンクを検証。	最優先
MISSION-004: 日本標的ルアー・IOC コーパス	2010–2025 の日本語件名、添付名、hash、C2 を原著ごとに正規化し、重複/誤帰属を監査。	高
MISSION-005: Huaying Haitai 企業実態	中国企業登記、変更履歴、訴訟、求人、旧サイト、株主・関連企業を一次記録で検証。	高
MISSION-006: APT10 post-2018 cluster split	A41APT/Cicada/Earth Tengshe/LODEINFO/Earth Kasha のコード・インフラ・標的・時系列を比較。	高
MISSION-007: MSS 請負モデル比較	APT3/Boyusec、APT17、APT40、APT41、APT10 の地方局–企業–個人モデルを同じ証拠基準で比較。	中
MISSION-008: 日本政府一次資料アーカイブ	2018 NISC/MOFA 原文、国会答弁、白書、注意喚起、捜査発表の保存・差分・帰属表現を整理。	中

APT10 エコシステム暫定関係図（文章ベース）

凡例：⇒ 公的資料が明示する関係 / ⇢ 技術・状況証拠による関係 / ? 未確認の切れ目

中国国家安全部（MSS）
⇒〔政府評価〕APT10 は MSS のために行動
⇒ Tianjin State Security Bureau（MSS 地方局）
⇒〔米起訴状の主張〕Huaying Haitai 勤務の Zhu Hua / Zhang Shilong が同局と関連して行動
? tasking 担当官・命令・契約・支払は非公開

Huaying Haitai（天津華盈海泰科技発展有限公司）
⇒〔EU 政府評価〕Operation Cloud Hopper へ資金・技術・物的支援、作戦を促進
⇒ 雇用：Zhang Shilong / Gao Qiang（EU）
⇒ 雇用：Zhu Hua / Zhang Shilong（米起訴状）
⇢ 企業 WHOIS・求人・所在地・移動記録（匿名 OSINT。一部のみ後続公的資料で補強）

人物・役割
Zhu Hua / Afwar / CVNX / Alayos / Godkiller
⇒ 侵入、悪性ドメイン/インフラ登録、他構成員の採用（起訴状の主張）
Zhang Shilong / Baobeilong / Zhang Jianguo / Atreexp
⇒ マルウェア開発・試験、悪性ドメイン/インフラ登録（起訴状・EU）
Gao Qiang
⇒ C2 インフラを通じ Cloud Hopper へ関与（EU）
Zheng Yanbin / fisherxp / その他候補
⇢ メール・WHOIS・SNS・IP・求人（匿名 OSINT）
? 公的な人物同定・雇用・TSSB 関係は未確認

追跡クラスタ / キャンペーン
APT10 ≈ menuPass ≈ Stone Panda ≈ Red Apollo ≈ POTASSIUM ≈ CVNX
├─ Technology Theft Campaign（約 2006–2018、米起訴状）
├─ MSP Theft Campaign（少なくとも 2014–2018、米起訴状）
│ ≈ Operation Cloud Hopper（PwC/BAE の作戦名）
├── 日本直接攻撃（少なくとも 2014–2017 に強い公開観測）
└── 後期関連：A41APT / Cicada / Earth Tengshe / LODEINFO
? historic Tianjin セルと同一の人員・指揮系統は未確認

技術・インフラ
PIVY / PlugX / EvilGrab / ChChes / RedLeaves / QuasarRAT
HAYMAKER / SNUGRIDE / BUGJUICE / ANEL / Ecipekac / SodaMaster / Hartip
DDNS・actor 登録ドメイン・侵害済み端末・MSP 管理経路
⇒ 約 1,300 悪性ドメイン（MSP 作戦、起訴状の主張）
⇒ 資格情報窃取 → RDP/WMI 横展開 → 暗号化 archive → 多段 staging → exfiltration

日本
⇒ 直接標的：大学/科学研究者、学術、製薬、製造、政府・外交・安全保障関連
⇒ 間接標的：侵害 MSP の日本所在顧客、日系企業の海外拠点・子会社
⇒ 日本語ルアー：科研費、日米安保、拡大抑止、政策・会議資料
? 公開 IOC → named person → named Japanese victim の完全な一対一対応は未確認

別系統として保持
  MirrorFace ≈ Earth Kasha
  ⇒〔警察庁/NISC〕2019 年頃以降、日本の安全保障・先端技術情報を狙う、中国関与疑い
    → ANEL/LODEINFO や日本標的という技術・目的上の重なり
    ? APT10 / Huaying / Tianjin MSS と同一との政府明示なし

最終評価

公開証拠が描く APT10 は、『国家機関そのものが全操作を直接実行する』単純モデルではなく、MSS 地方局との関係が司法・政府資料で指摘された天津の民間企業、そこに所属する侵入担当・開発担当・インフラ担当、専用と汎用を混ぜたツール群、DDNS・登録ドメイン・侵害済み MSP から成る多層エコシステムである。MSP を踏み台に顧客へ到達するモデルは、少人数の技術者でも地理・業種を跨ぐ大規模窃取を可能にした。日本は、研究・先端技術・企業情報・外交安全保障という情報需要と整合する、長期かつ反復的な重点標的だった。

同時に、公開証拠の限界も構造の一部である。国家→地方局→会社→人物の大枠は強いが、地方局の具体的 tasking、人物と個々の C2、日本の固有被害者への一対一対応は未公開である。2018 年後のクラスタは技術・標的連続性を示す一方、同じ人員・会社・指揮系統を示さない。よって最も妥当な表現は『APT10 のコア活動の一部は Tianjin MSS 関連の Huaying Haitai 請負エコシステムに帰属する。APT10 ラベル全体は、それを含み得るより広い分析上の傘である』となる。