中国サイバー作戦エコシステム MISSION-001 調査報告

対象：2020 年より前に確認・報告・公表された、中国または中国系脅威アクターとの関連が指摘される対日 APT 活動

Executive Summary と調査上の判定基準

本調査では、**原則として 2019 年 12 月 31 日までに活動そのものが観測・報告されていた事案**を中核象とした。　2020 年以降の政府表、起訴、共同アドバイザリについては、過去の活動を遡及的にしたり、組織人物政府機との係を明らかにしたりする場合に限って「 後年の補強証拠」として使用した。この区別は重要である。たとえば Tick/BRONZE BUTLER の対日攻は　2017～2019 年までに詳細が公開されていたが、**中国人民解放軍 61419 部隊との係を日本政府が公に評価したのは 2021 年**である。

本調査で最も強く確認できたのは、単一の「中国 APT」が日本を攻してきたという構ではなく、**複数の異なる運用モデルが長期間併存していたこと**である。APT10 については、中国国家安全部（MSS）天津市家安全局と民間企業 Huaying Haitai、個人ハッカーを結ぶ米司法省の起訴内容があり、日本政府も 2018 年に中国を拠点とする APT10 による長期・広範な攻撃を公に非難している。Tick については、日本に極端に特化した侵入活動が先に技術的に確認され、後年になって日本警察・政府が PLA 61419 部隊との関係を「可能性が高い」と評価した。APT41 では、民間研究機が家支援型諜報と金目的犯罪の行運用を指摘し、　2020 年の米司法省文書では中国の民間企業 Chengdu 404 と複数人物が登場する。この三者だけでも、**国家機関直結型、軍部隊との関係が推定される型、民間・犯罪活動と国家目的が混在する型**という異なるモデルが見える。

対日作戦の技術的特徴として特に重要なのが、**日本国内でしか広く使われないソフトウェアに対するゼロデイ／脆弱性悪用**である。JPCERT/CC がインシデント対応を基に整理した VB2019 研究では、三四郎の CVE-2014-0810、一太郎の CVE-2013-5990 および CVE-2014-7247、SKYSEA Client View の CVE-2016-7836 が扱われている。とりわけ Tick は、2016 年 6 月ごろから CVE-2016-7836 を未公開段階で攻に利用し、日本の　IP 範囲を集中的に走査したとされる。これは、日本市場・日本語環境・導入ソフトウェアを事前研究する能力が存在したことを示す強い状況証拠である。

さらに重要なのは、**同じゼロデイが異なるアクターに近接して現れる現象**である。JPCERT/CC は一太郎 CVE-2014-7247 について、Blue Termite とされる攻撃の直後に APT17 系の活動でも測したとしており、同一攻撃者と断定していない。この事実は、脆弱性・exploit・開発者・ブローカー・委託先の共有といった「エコシステム」を調査する上で非常に価値がある一方、**共通 CVE を理由に二つの APT を同一組織とみなすことはできない**。

もう一つの反復パターンは、最終標的そのものではなく**信頼された中間事業者・更新経路・管理基盤を踏み台にすること**である。APT10 の MSP Theft Campaign、APT17 の更新サーバ／DNS 操作、BlackTech と ASUS WebStorage 更新機能、Winnti/APT41 系で観測されたコード署名証明書・ソフトウェア供給網への侵入はいずれもこの方向性を示す。ただし、これらが共通指令系統の存在を意味する証拠は発見できなかった。

本報告では証拠を次のように区別する。

- **確認事実**：インシデント対応、マルウェア解析、起訴資料等から直接確認できる事象
- **政府評価**：日本・米国等の政府機関が公式に示した帰属または評価
- **民間評価**：セキュリティ企業・研究者によるクラスタリング、国家関連評価
- **状況証拠**：言語、勤務時間、標的選、インフラ、コド等から間接的に示唆されるもの
- **仮説**：複資料を組み合わせると明可能だが、直接がないもの

- **未確認**：公開資料では検証できなかったもの

帰属強度については、本調査時点で**A＝政府機関・人物・法人まで具体化、B＝国家／軍との政府評価あり、C＝中国系との民間評価が中心、D＝中国関連状況証拠のみ、E＝中国帰属を確認できず比較対象**とした。これは分析上の暫定尺度であり、法的立証基準ではない。

暫定的な核心アクターは、APT10、Tick/BRONZE BUTLER、BlackTechである。 APT16、APT17、APT12、Tonto Team/CactusPete、APT41/Winntiは重要な周辺クラスタとして追跡価値が高い。Icefogは対日活動が非常に重要だが国家帰属は弱く、Blue Termite/CloudyOmegaはさらに慎重に扱うべきである。

対日APT活動の暫定年表と主要事案

以下の年表では、「公表時点」と「後年の帰属」を混同しないようにした。

時期	活動／アクター	日本側標的・観測	主な技術マルウェア	時／後年の属評価
2009年頃〜	IXESHE／後にAPT12系と整理される活動	Trend Microは2009年から東アジア政府、電子機器、通信などを狙うIXESHEを追跡。後年のAPT12/Etumbot資料では日本も標的地域に含まれる。	IXESHE、侵害済み内部端末をC2化、Dynamic DNS、spearphishing	中国系APT12/Numbered Pandaとの対応付けは存在するが、初期IXESHEの全活動を一組織に帰すのは慎重であるべき。
2011年〜	Icefog	Kasperskyは日本・韓国を主標的とし、日本の衆院への2011年侵入をIcefogの代表的事案の一つとして挙げた。Fuji TV、日本中国経済協も標的一に含む。	Icefog、後にJavafog、spearphishing、短期集中型の手動情報探索	操作者監視IP等から中国・韓国・日本の少なくとも3か国に関係者がいる可能性。Kaspersky自身は「cybermercenary」モデルも提示しており、中国国家機関との直接関係は確認できない。
2011～2013年	Emdivi系／後のCloudyOmega⊠Blue Termiteにつながる活動	JPCERT/CCはEmdiviを2011年頃から測されたマルウェアと整理。2013年以降、日本組織へのspearphishingが活化。	Emdivi、Java exploitなど	日本への攻撃は強い。本調査で中国国家・中国系組織との十分な帰属根拠は得られず。
2013年8～9月	APT17／Deputy Dog	JPCERT/CCの日本向けAPT整理ではOperation DeputyDog、Operation	Agtid、CVE-2013-3893、CVE-2013-3918、後にPlugX、McRAT、Htran	FireEyeはAPT17をChina-based APTと評価。日本政府による個別帰属は今回確

時期	活動／アクター	日本側標的・観測	主な技術マルウェア	当時／後年の帰属評価
		Ephemeral Hydra 系の watering-hole 活動を記載。		認できず。
2013～2014 年	日本固有ソフト脆弱性悪用クラスタ	三四郎 CVE-2014-0810 をゼロデイで悪用、日本政府機関向け「年始挨拶」型 spearphishing。以前から一太郎 CVE-2013-5990 等も使用。	PlugX、C2 103.246.112.123	JPCERT/CC incident handling 由来。特定国家組織への帰属は資料上慎重。
2014～2015 年	CloudyOmega／Blue Termite	2014 年 5 月～2015 年 9 月、多数の日本組織へ spearphishing。健康保険組合を装うルアー、一太郎ゼロデイ等。	Emdivi、CVE-2014-7247、後に Hacking Team 流出 Flash 0-day、Mimikatz/WCE 等	日本特化性は強い。中国帰属は本調査の一次資料から確立せず。
2014～2015 年	APT17	悪性 DNS 操作、正規更新路の改変、標的 IP レンジに限定したマルウェア配送。	Agtid、Derusbi、BLACKCOFFEE、改変 mod_rootme、pam_unix.so	China-based APT。特定 MSS/PLA 部門との公開一次証拠は今回未確認。
2014 年～	APT10／menuPass	Palo Alto Networks は日本を少なくとも 2014 年から標的としていたと評価。日本の研究者・学術機関・組織に、外交・日米関係等を題材とした spearphishing。	Poison Ivy、PlugX、ChChes、後に RedLeaves 等	2018 年、日本政府が中国を拠点とする APT10 を非難。米司法省は MSS 天津市国家安全局との関係を起訴状で具化。
2015 年	APT16	日本・台湾のハイテク、政府サービス、メディア、金融を標的とする campaign。	IRONHALO、ELMER、EPS exploit、CVE-2015-2545、CVE-2015-1701 を含む攻撃チェーン	FireEye/Mandiant は China-based group と整理。日本政府帰属は未確認。
2015～2016 年	Winnti 系	JPCERT/CC の日本 APT 括では、特定業種への侵入、コード署名明書	Winnti 系ツール、盗難コード	後の APT41 との技術的・組織的重複はあるが、Mandiant 自身が

時期	活動／アクター	日本側標的・観測	主な技術マルウェア	当時／後年の帰属評価
		署名証明書の窃取とそれを用いた感染を記録。		「partially coincides」としており、Winnti = APT41 と全称同一視すべきではない。
2015 年	Tick／BRONZE BUTLER	日本向け watering hole、Flash ゼロデイ等。日本語能力の高い攻撃者として追跡。	Daserf、後に xxmm/Datper	Secureworks は PRC 起源の可能性を評価。政府組織特定は当時なし。
2016 年 6 月～2019 年 2 月	Tick／BRONZE BUTLER	SKYSEA Client View の CVE-2016-7836 を未公開段階から悪用。観測されたスキャンは日本向けセンサーに集中。	Wali、NodeRAT、xxmm、Datper、CVE-2016-7836	日本特化の強い技術証拠。2021 年に日本警察・政府が PLA 61419 との関係を高い可能性として評価。
2016～2018 年	APT10／Operation Cloud Hopper 関連	日本組織への spearphishing に加え、MSP を侵害し顧客環境へ展開するキャンペーン。米起訴資料は日本に所在する被害企業を明記。	ChChes、RedLeaves、盗難認証情報、暗号化アーカイブ、MSP 経由 lateral movement	MSS 天津市国家安全局と Huaying Haitai の係を米司法省が起訴で主張。日本政府も APT10 を公に非難。
2017 年	Tick	ネットワク部で MS17-010 系と DoublePulsar を横展開に使用。	Mimikatz、WCE、PsExec、scheduled task、WinRAR、MS17-010/DoublePulsar	JPCERT/CC と Secureworks の TTP が整合。
2017 年	APT10／menuPass	日本の学者・組織向けに日米外交、米大統領選後の政策などを題材としたメール。	ChChes、Poison Ivy、PlugX、偽装・free webmail	Unit 42 がインフラ重複、ツール、Poison Ivy password 等から menuPass に高い確信。
2018 年 1 月～	BlackTech	文部科省を装ったメールが日本組織へ送付され、TSCookie を配送。JPCERT/CC は日本組織を狙う活動を継続観測。	TSCookie、PLEAD	JPCERT/CC による国内観測。中国系評価は当初民間研究中心。
2018 年	APT10	日本語の海洋、外交、北朝鮮関	VBA macro、UPPERCUT 系、	FireEye/Mandiant の追跡。

時期	活動／アクター	日本側標的・観測	主な技術マルウェア	当時／後年の帰属評価
		連文書等をルアーとする更新 TTP。	RedLeaves 等	
2018 年 12 月	APT10 公的帰属	日本政府が中国を拠点とする APT10 の民間企業・学術機関等への長期・広範な攻撃を断固非難。米国は同月、APT10 構成員とされる 2 名を起訴。	—	本ミッション中、最も具体性が高い国家・法人人物リンク。
2018～2019 年	Tonto Team／CactusPete	Kaspersky の 2019 年総括は、同系統が歴史的に日本、韓国、台湾、米国を標的にしていたと記載。	Bisonal 系、spearphishing、Office exploit、Mimikatz 等	Chinese-speaking、後に suspected Chinese state-sponsored と整理されるが、日本での個々の事案の公開粒度は低い。
2019 年	BlackTech	日本で侵入後 TSCookie 種が測。IconDown も日本組織から発見。ESET 報告では ASUS WebStorage 更新機能悪用との係。	TSCookie、PLEAD、IconDown、RC4	日本で継続する侵入活動。
2019 年	APT41／Winnti 重複領域	FireEye が APT41 を正式に「graduated」させ、中国系の国家支援諜報＋金銭目的活動を並行するグループとして公表。過去の Winnti 等と部分的重複。	supply-chain compromise、盗難 code-signing certificate、多数の private malware	日本の Winnti 図測との接続は重要だが、個々の 2015～16 年対日事件をそのまま APT41 へ再するのは未確定。
2019 年 12 月～	LODEINFO	JPCERT/CC は 2019 年 12 月から日本組織に対する新しい spearphishing と LODEINFO を測。	malicious Word、LODEINFO	2019 年末の活動。本 MISSION では 2019 年時点の一次資料から中国系 actor との確実な連結まで到達できず、次回の重要追跡事項。

この年表で特に目立つのは、**2013～2019 年に日本固有ソフト、MSP、ソフトウェア更新、侵害済み Web サイト、認証情報を使った横展開が繰り返し出現すること**である。これは「日本を標的とする中国系 APT」を単にフィッシングメールの集合として追うより、**脆弱性調達、供給網アクセス、C2** 調達、認証情報窃取、コード署名証明書、請負人材まで含めて追跡すべきことを示している。

APT 名・Alias・政府機関・企業・人物の対応

APT 名称はベンダーごとの観測単位であり、法人登記上の組織名ではない。特に Winnti のような名称は、マルウェア、攻撃コミュニティ、複数クラスタの総称として使われる場合があるため、**Alias 表は「同一組織表」ではなく「報告上の対応関係表」**として扱う必要がある。Mandiant も APT41 について BARIUM や Winnti と「部分的に重なる」と表現している。

主名称	公開資料に現れる別名・関連名	対日活動	政府組織とのリンク	本調査の扱い
APT10	Red Apollo、CVNX、Stone Panda、menuPass、POTASSIUM	少なくとも 2014 年以降。学術・組織、MSP 顧客等。	MSS 天津市国家安全局、Huaying Haitai Science and Technology Development Company。米起訴による。	A：最重要。DOJ 自身がこれらの alias を列挙。
menuPass	Palo Alto の追跡名。APT10／Stone Panda との対応	日本の学者・組織	上記 APT10 係	Alias として高い整合。ただしベンダー観測範囲の差は残る。
Tick	BRONZE BUTLER	日本を主要標的。重要インフラ、重工、製造、国際関係等	PLA Unit 61419 との関係が高い可能性との日本政府・警察評価（2021 年）	B：最重要。pre-2020 技術測 + post-2020 政府。
BlackTech	Palmerworm 等。後年の各社・政府資料では複数追跡名あり	2018～19 年、日本で継続観測	2023 年以降、日米等の共同政府表で PRC-linked/state-sponsored actor として扱われる	B/C。pre-2020 段階では具体的な中国政府部署・人物は公開確認できず。
APT16	FireEye の APT16。SVCMONDR 等を別名とするデータベースもあるが、本報告では採用を保留	日本・台湾、ハイテク、政府サービス、メディア、金融	China-based との FireEye/Mandiant 評価	C。国家部署への一次的リンクなし。
APT17	Deputy Dog。Agtid は関連マルウェア／活動識別子であり単純な actor alias とはしない	日本向け watering-hole、更新経路等	FireEye が China-based APT と評価	C。日本政府の個別帰属は未確認。
APT12	IXESHE、Numbered	Etumbot 等で日本を標的とする	中国系との民間評価	C、暫定。初期 IXESHE campaign

主名称	公開資料に現れる別名・関連名	対日活動	政府組織とのリンク	本調査の扱い
	Panda、DynCalc、DNSCALC 等として整理されることがある	活動が報告		と後年 APT12 クラスタの範囲が完全に一致するとは断定しない。
Tonto Team	CactusPete、Karma Panda。Kaspersky 資料には LoneRanger 表記も存在	日本、韓国、台湾、米国を歴史的標的	Chinese-speaking。後年 suspected Chinese state-sponsored との整理	C。日本の個別侵入事例の原資料追跡が不足。
APT41	BARIUM、Winnti、Wicked Panda、Wicked Spider 等と報道・司法文書上の重複	JPCERT が記録した日本 Winnti 活動との連候補	2020 DOJ で Chengdu 404 と中国人被告。FireEye は中国国家支援諜報＋独立した金銭目的活動と評価	A/C だが Japan mapping は暫定。Winnti 全体 = APT41 とはしない。
Icefog	Icefog、Javafog（後続 malware）	日本を主要標的。国会、メディア、日中関係団体等	Kaspersky は操作者が中国・韓国・日本に存在する可能性を示した	D。「中国系国家 APT」とするには弱い。
Blue Termite	CloudyOmega は同一日本向け campaign を別社が追跡した名称	日本に極めて強く特化	今回取得した一次資料で中国国家との関係を確認できず	E。比較対象。日本 APT だから中国 APT である、と逆算してはならない。

具体的な政府機関・企業・人物については、公開一次資料で最も明瞭なのが APT10 である。米司法省は 2018 年 12 月 20 日、**Zhu Hua（朱华、Afwar/CVNX/Alayos/Godkiller）と Zhang Shilong（张士龙、Baobeilong/Zhang Jianguo/Atreexp）**を起訴し、両名が天津の **Huaying Haitai** で勤務し、中国 MSS の **Tianjin State Security Bureau** と関連して活動したと主張した。Zhu は侵入活動と人員募集、Zhang はマルウェア開発・テスト、両者は悪性ドメインやインフラ登録にも関与したとされる。これはあくまで**起訴上の主張であり、有罪判決による認定と同義ではない**。DOJ 自身も被告は有罪が証明されるまで無罪と推定されると明記している。

Tick について、日本政府は 2021 年、**PLA Unit 61419 を背景に持つ可能性が高い**との評価を公表した。警察庁資料は、国内で攻撃用レンタルサーバの不正契約に関する捜査を進め、その過程で背景組織の特定につながったことを記述している。ここは APT10 とは証拠類型が異なり、公開起訴状による人物・法人・指令系統の詳細までは示されていない。したがって本調査では「PLA 61419 との関係を日本政府が高い可能性として評価」とし、「61419 部隊が全 Tick 活動を直接命令した」とは記述しない。

APT41 の後年資料では、**Qian Chuan、Fu Qiang、Jiang Lizhi** が Chengdu 404 Network Technology Company で勤務しながら侵入を行ったと米司法省が主張し、別事件で **Zhang Haoran、Tan Dailin** も起訴されている。FBI は被害対象に日本企業が含まれるとする。ただし DOJ の 2020 年発表そのものも、APT41/Barium/Winnti/Wicked Panda/Wicked Spider を「 security researchers have tracked using these labels」と表現しており、すべての過去 Winnti 活動をこの 5 人へさせる根拠にはならない。

この点は「エコシステム」調査にとって重要である。2025 年に米司法省が i-Soon/Anxun 関係者を起訴した際には、MPS や MSS が民間会社・フリーランサーに侵入を依頼し、盗難データを購入するモデルを明示的に説明した。しかしこれは **APT10、Tick、BlackTech が i-Soon と同じ組織だった証拠ではない**。むしろ、中国のサイバー作戦を分析する際に「国家職員だけ」「政府がすべて直接実施」という二択では不十分で、民間企業、契約者、独立ハッカー、データ仲介を含めたモデルを検討すべきという後年の比較材料である。

マルウェア・脆弱性・TTP・攻撃インフラの関連性

JPCERT/CC の日本向けインシデント資料からは、単に共通マルウェアを見るより、**日本固有ソフトのゼロデイ、供給網、認証情報、インフラ再利用の組合せ**を見る方が有効であることが分かる。特に PlugX、Poison Ivy、Mimikatz、Windows Credential Editor、China Chopper などは複数アクターが使用するため、それ自体は強い帰属証拠ではない。

アクター／campaign	マルウェア・ツール	脆弱性／CVE	侵入・展開方法	代表インフラ／特徴
APT10/menuPass	ChChes、RedLeaves、Anel、EvilGrab、PlugX、Poison Ivy、QuasarRAT	日本向け 2017～18 campaign は主に文書・macro 系で、今回の主要一次資料から固有 CVE を確定せず	spearphishing、悪性 Word/VBA、MSP 侵害、盗難 admin credentials、横展開、暗号化 archive	apple.cmdnetview.com、fbi.sexxxy.biz、kawasaki.unham.com、fukuoka.cloud-maste.com 等、複数世代の関連 domain。Unit42 はインフラ重複や Poison Ivy 設定等をクラスタリング根拠とした。
Tick/BRONZE BUTLER	Daserf、Datper、xxmm/Minzen、Wali、NodeRAT、KVNDM、Gofarer、MSGet、DGet、Mimikatz、WCE、WinRAR	CVE-2016-7836、2017 年に MS17-010/DoublePulsar を横展開に利用	watering hole、asset-management software scan、credential dump、PsExec、scheduled task、RAR exfil	107.189.139.237、180.150.227.72、27.255.84.171 等。侵害済み Web サイトを C2 化し China Chopper も設置。日本サイトの index_old.php 等を利用した例。
日本固有ソフト悪用クラスタ	PlugX 等	CVE-2014-0810（三四郎）、CVE-2013-5990（一太郎）	日本政府組織等へ spearphishing	サンプルが 103.246.112.123 を共有。
Blue Termite/CloudyOmega	Emdivi、credential tools、WinRAR 等	CVE-2014-7247（一太郎）、2015 年 Hacking Team 漏えい後の Flash 0-day 利用	spearphishing、組織内探索、credential dump、archive/exfil	侵害サーバ上に DST Asp 站長檢測 Tools、Anti-shell、Spider PHP shell、X14ob-Sh3ll 等が確認された例。
APT17	Agtid、PlugX、	CVE-2013-3893、	watering hole、	改変 update

アクター／campaign	マルウェア・ツール	脆弱性／CVE	侵入・展開方法	代表インフラ／特徴
	McRAT、Htran、Derusbi、BLACKCOFFEE	CVE-2013-3918。CVE-2014-7247 との近接観測あり	domain-registration hijack、malicious DNS、update/supply-chain hijack、Pass-the-Hash	server、DNAT、標的 IP 制限。Linux 側に backdoored mod_rootme、pam_unix.so。
APT16	IRONHALO downloader、ELMER HTTP backdoor	CVE-2015-2545 を利用した EPS 系 exploit。FireEye 報告では CVE-2015-1701 を組み合わせる chain も記録	spearphishing、weaponized Word documents、日本語／繁体字ルアー	HTTP 型 C2。
BlackTech	TSCookie、PLEAD、IconDown	pre-2020 の主要 JPCERT 資料では特定 CVE より malware/supply chain が中心	MEXT impersonation、侵入後 malware、ASUS WebStorage update abuse との連	IconDown は例として update.panasocin.com/logo.png を取得、256-byte RC4 key で payload を復号。
Icefog	Icefog、Javafog、後年 Poison Ivy/Quarian 等	今回の 2013 一次資料から日本案件固有 CVE を確定せず	spearphishing attachment/link、手動探索、短期「hit-and-run」	70 超の連 domain のうち 13 を Kaspersky が sinkhole。lingdona.com は Javafog 追跡に使用。
Winnti/APT41 ☒連領域	Winnti 系、盗難 certificate で署名した malware、多数の private malware	日本案件固有 CVE は今回未特定	certificate theft、software supply chain、production environment compromise	Mandiant は APT41 の供給網攻撃で system identifier によって追加 payload を特定標的に限定する手法を記録。

日本固有ソフトウェア脆弱性は、今回最も重要な“エコシステム指標”の一つである。 三四郎、一太郎、SKYSEA は、世界規模の無差別攻撃で偶然選ばれるより、国内導入状況を理解した攻撃者が優先的に研究したと考える方が自然である。JPCERT/CC 自身も、攻撃グループが region-specific software を意図的に研究し、ゼロデイを使用していたと結論付けている。

一方、CVE-2014-7247 が Blue Termite 系と APT17 系で短い間隔で利用された点は特に追跡価値がある。考え得る説明には、**共通 exploit 供給者、脆弱性ブローカー、開発者の共有、attack framework の移転、情報交換、あるいは単なる独立取得**がある。しかし現在の公開資料ではどれを採用すべきか決められない。したがって「 APT17 = Blue Termite」あるいは「同じ中国政府部署が両者へ exploit を配布した」という結論は仮説の域を出ない。

現行 MITRE ATT&CK へ正規化すると、主要観測は次のようになる。これは各原著が必ずしも当時 ATT&CK ID を記載していたという意味ではなく、**本調査で観測 TTP を現在の ATT&CK 体系へ対**

応させた分析用マッピングである。ATT&CK 自体は実観測に基づく戦術・技術知識ベースである。

測された　TTP	ATT&CK Technique	主なアクター／事例
添付ファイル型標的メール	T1566.001 Spearphishing Attachment	APT10、APT16、Blue Termite、Icefog、BlackTech
URL 型標的メール	T1566.002 Spearphishing Link	APT10、Icefog、BlackTech
クライアントアプリ脆弱性悪用	T1203 Exploitation for Client Execution	一太郎／三四郎、APT16
Watering hole	T1189 Drive-by Compromise	APT17、Tick
ソフトウェア更新経路の侵害	T1195.002 Compromise Software Supply Chain	APT17、BlackTech、Winnti/APT41
Internet/asset scanning	T1595.002 Vulnerability Scanning	Tick/SKYSEA
Credential dumping	T1003 OS Credential Dumping	Tick、Blue Termite、APT17
Pass-the-Hash	T1550.002 Pass the Hash	APT17 等
Golden Ticket	T1558.001	Tick
Silver Ticket	T1558.002	Tick
SMB/Admin Share 利用	T1021.002 SMB/Windows Admin Shares	Tick、APT10 系 lateral movement
Scheduled Task	T1053.005 Scheduled Task	Tick、Blue Termite
PsExec/service execution	T1569.002 Service Execution	Tick
Windows command 行	T1059.003 Windows Command Shell	APT17、Tick、Blue Termite
RAR 等で収集物を圧縮	T1560.001 Archive via Utility	Tick、APT10、Blue Termite
HTTP/HTTPS C2	T1071.001 Web Protocols	APT10、APT16、Tick、BlackTech
追加ツール取得	T1105 Ingress Tool Transfer	多数
遠隔サービス脆弱性で横展開	T1210 Exploitation of Remote Services	Tick の MS17-010
証拠ファイル削除	T1070.004 File Deletion	Blue Termite 等

特に APT10 と Tick では、侵入後の行動が単純な RAT 設置を超える。APT10 の MSP campaign では管理者認情報をみ、　　MSP から顧客へ横展開し、収集データを暗号化 archive 化した後、別の侵害済みマシンを経由して外へ出す手順が米起訴資料に記載されている。Tick では domain admin 取得、Golden/Silver Ticket、PsExec、scheduled task、RAR 分割暗化、外部サビスへのアップロードなどが観測されている。

Attribution 評価、反証、矛盾、不確実性

本調査で最も重要なのは、「中国との関連」を一種類の証拠として扱わないことである。

アクター	暫定帰属強度	帰属を強める証拠	帰属を弱める／限定する証拠
APT10	A／高	日本政府による 2018 年の中国拠点 APT10 非難。米 DOJ が MSS 天津市国家安全局、Huaying Haitai、Zhu	DOJ 文書は起訴上の主張であり司法上の有罪認定ではない。APT10 というベンダークラスタの 全活動」

アクター	暫定帰属強度	帰属を強める証拠	帰属を弱める／限定する証拠
		Hua、Zhang Shilong を具体化。日本を含む MSP 被害国を明記。	が同じ二名・同一部署によるとまでは起訴内容から言えない。
Tick/BRONZE BUTLER	B／高〜中	日本特化した長期 TTP、PLA 61419 との係を日本政府・警察が後年「可能性が高い」と評価。国内サーバ契約捜査も帰属に寄。	2017 時点の Secureworks 証拠は中国語ツール、PRC ⊠連ハッカーとのリンク、休日パターン等の状況証拠が中心。さらに Secureworks は標的の多様さから複数 tasking team／組織の可能性にも触れている。単一軍部隊だけで全活動を説明できるとは限らない。
BlackTech	B/C／中〜高	JPCERT が日本で長期・継続観測。後年の日米等政府共同資料で PRC-linked actor として扱われる。	pre-2020 公開資料では MSS⊠PLA 等の具体部署、法人、人物を結ぶ一次証拠が見つからない。中国国家スポンサーを 2018 年当時から確定扱いするのは時系列上不適切。
APT41	A/C／中〜高	FireEye が中国国家支援型諜報と金銭目的活動を併行すると高く評価。2020 DOJ が中国人被告と Chengdu 404 を公表し、日本被害も記載。	APT41、Winnti、BARIUM 等は観測範囲が完全一致しない。金銭目的活動が「国家指示外」である可能性を FireEye 自身が認めており、全侵入を国家作戦とみなせない。
APT16	C／中	FireEye/Mandiant が China-based group と評価し、日本を明示的標的に含む。	公開一次資料で中国政府部署、企業、人物との具体的リンクを今回確認できず。
APT17	C／中	FireEye が China-based APT として追跡。JPCERT の対日技術資料と TTP が結び付く。	PlugX、Htran、Derusbi、BLACKCOFFEE 等の技術共通性だけでは国家帰属できない。日本政府の個別帰属を確認できず。
APT12	C／中〜低	IXESHE/Etumbot/Numbered Panda として東アジア、日本と	Campaign 名、malware 名、actor 名が後から統合されて

アクター	暫定帰属強度	帰属を強める証拠	帰属を弱める／限定する証拠
		の関係が継続的に報告される。	おり、2009 年からの全 IXESHE 活動を現在の APT12 と同一視することには不確実性。
Tonto/CactusPete	C／中〜低	Kaspersky が Chinese-speaking actor、日本を歴史的標的と評価。	国家部署との具体的公開リンクが薄い。2012～14 年の日本被害の原事件資料を今回十分回収できず。
Icefog	D／低	中国語・日本語・韓国語能力、インフラ監視から中国・韓国・日本の関係者を示唆。日本は主要標的。	Kaspersky 自身が小規模「cybermercenary」型として分析。中国政府との直接リンクなし。むしろ多国籍・請負型の可能性を残す。
Blue Termite/CloudyOmega	E／中国帰属未確立	日本に対する高度なゼロデイ利用という事実は強い。	今回取得した原資料には、中国国家／中国系 actor とする十分な帰属証拠なし。中国 APT 史に自動的に組み込むべきではない。

帰属を弱める共通要因も整理しておく必要がある。

第一に、**中国語文字列、中国の勤務時間、中国の祝日に活動が下がること、中国所在 IP** は補助的な状況証拠にすぎない。Secureworks はこれらを Tick の中国起源評価に用いているが、こうした特性は遠隔操作、外注、偽装、共有ツールでも再現できる。Tick の後年の政府帰属が重要なのは、この種の状況証拠だけではなく、日本警察による国内インフラ捜査等が加わったためである。

第二に、**共有マルウェア＝共有組織ではない**。PlugX は APT10、APT17、日本固有ソフト悪用活動など複数箇所に現れ、Poison Ivy、Mimikatz、WCE、PsExec、China Chopper も広く利用される。したがって、ツール一致を「同一 APT」や「同じ政府機関」の根拠とするのは危険である。

第三に、**CVE の共有も同一性証拠ではない**。一太郎 CVE-2014-7247 を複数 actor が近接して利用したという JPCERT/CC の測は、むしろ　exploit 供給網や仲介者の存在を調査する契機であり、actor 統合の根拠ではない。

第四に、APT41 は「国家 APT」という単純な分類そのものへの反証例である。FireEye は同一クラスタが国家支援型諜報に用いる非公開 malware を、個人的利益とみられるゲーム企業攻撃などでも使ったと評価している。これは、同じ人員・ツール・インフラが **state tasking と private crime の両方**に使われ得ることを意味する。

第五に、Icefog はさらに異なるモデルを示す。Kaspersky は日本を主要標的とする高度な情報窃取活動を確認しつつ、長期間居座る典型的 APT ではなく、必要情報だけを探して離脱する「hit-and-run」型、小規模な「cybermercenary」型と分析した。したがって、日本を狙い、中国に関係する兆候があるという二点だけから中国国家機関へ帰属するのは不適切である。

現時点で支持できるのは、「中国のサイバー作戦には国家機関、軍、地方情報機関、民間企業、個人ハッカー、兼業的犯罪活動が混在し得る」というモデルであり、「すべての対日中国系 APT を一つの中央指令系統が直接統制している」というモデルではない。 APT10、Tick、APT41 の公開資料を比較するだけでも、組織形態が異なることが分かる。

2020 年以降への連続性とエコシステム上の手掛かり

Tick → PLA 61419 は今回最も重要な遡及リンクである。2016～19 年に JPCERT/CC と Secureworks が観測した日本特化型活動が、2021 年には日本政府によって PLA Unit 61419 を背景に持つ可能性の高い活動として公表された。この時間差は、今後の調査でも「当時の技術クラスタ」と「数年後に公表される人物・組織帰属」を別データとして保存し、後から結合する必要性を示す。

APT10 → MSS 天津市国家安全局＋民間企業モデルは 2018 年時点ですでに具体化していた。DOJ によれば APT10 の活動は少なくとも 2006～2018 年に及び、2014 年ごろから MSP Theft Campaign が展開された。日本を含む 12 か国の MSP または顧客環境が侵害され、攻撃者は MSP の信頼関係を利用して顧客へ進出した。ここには「政府情報機関—民間会社—penetration tester／malware developer—攻撃インフラ」というエコシステム構造が具体的に現れる。

BlackTech では、2018～19 年に JPCERT/CC が TSCookie、PLEAD、IconDown 等を日本で追跡し、2021 年にも JPCERT/CC は国内 BlackTech 活動が 2018 年頃から継続しているとした。さらに後年、日米などの政府機関が BlackTech を中国政府に関連する actor として扱った。従って、BlackTech については「pre-2020 日本 incident → post-2020 国家帰属」の追跡をさらに深掘りする価値が高い。

APT41/Winnti では 2019 年の FireEye 報告と 2020 年の米司法省文書の間に重要な連続性がある。FireEye は 2019 年、APT41 を国家支援型諜報と金銭目的犯罪を並行する中国系 actor と評価し、Winnti/BARIUM と部分的に重なるとした。2020 年 DOJ は中国人被告と Chengdu 404 を明らかにし、日本の企業も被害対象に含まれたとした。これは、2015～16 年の日本 Winnti 図 測について、**どこまでが APT41／Chengdu 404 系に属するのかを再クラスタリングする価値がある**ことを意味するが、現時点では未解決である。

APT40 と Hainan MSS 系も比較対象として重要である。2021 年、日本外務省は APT40 を中国政府を背景に持つ可能性が高いと評価するとともに、別途 Tick と PLA 61419 の関係に言及した。米司法省は APT40 に関連する別事件で、Hainan State Security Department の職員と、フロント企業 Hainan Xiandun Technology Development を利用したとする起訴を公表した。これは MISSION-001 の pre-2020 中核事案そのものではないが、APT10 の Huaying Haitai モデルと並んで、**地方 MSS 機関＋名目的民間技術会社**という組織パターンを比較する材料になる。

さらに 2025 年の i-Soon 事件では、米司法省が MPS図MSS の依頼を受ける民間会社とフリーランサー、APT27 関係者からなる「hacker-for-hire ecosystem」を具体的に描いた。これを 2010 年代の各 APT へ遡及適用することはできないが、APT10、APT41、APT40 などで既に見えていた民間会社利用を比較研究する上で極めて重要である。

これらから、次のような**暫定エコシステム構造**が考えられる。

- **国家需要側**：MSS 地方局、PLA 部隊、MPS 等が情報需要・任務を持つ可能性。APT10 では天津 MSS、Tick では PLA 61419 という具体例がある。
- **実行・請負側**：民間技術会社、個人 penetration tester、malware developer、兼業 criminal actor。Huaying Haitai、Chengdu 404、後年の Hainan Xiandun/i-Soon は組織モデルの比較材料になる。
- **能力供給側**：ゼロデイ、攻撃コード、malware framework、コード署名証明書、web shell、credential tooling。日本では一太郎・三四郎・SKYSEA のゼロデイが特に重要である。
- **アクセス供給側**：侵害済み Web サイト、MSP、更新サーバ、ソフトウェア供給網、盗難 credentials。APT10、APT17、BlackTech、Winnti/APT41 で異なる形で反復する。

ただし、**この四層が一つの統合市場として存在していたこと自体はまだ仮説である**。公開資料から確認できるのは、各事案でその一部が実在したというところまでである。

今回発見できなかった、あるいは原資料まで到達できなかった情報も重要である。

未解決事項	現状
2018 年の日本外務省 APT10 外務報道官談話の当時ページ	外交青書 2020/2021 で発出事実と内容は確認できたが、本調査検索では原ページを安定して取得できなかった。
Tick と PLA 61419 を結ぶ人物・法人の完全な公開チェーン	2021 警察資料で帰属評価と国内捜査は確認したが、APT10 の起訴状ほど詳細な人物・企業グラフは公開資料から構築できなかった。
BlackTech の pre-2020 中国政府部署・人物	未発見。JPCERT の日本 incident corpus は厚いが、スポンサー側の人物・法人情報が薄い。
APT16 の具体的人物・政府部署	未発見。China-based という民間評価まで。
APT17 の日本案件を特定 MSS/PLA 部署へ結ぶ一次資料	未発見。
APT12/Etumbot の 2014 年 Arbor Networks 原著資料	二次・引用資料まで確認したが、今回の検索では元 ASERT PDF を十分再検証できなかった。JPCERT JSAC 資料も当該文献を参照している。
Blue Termite を中国国家 actor とする一次証拠	未発見。現時点では中国 APT 本体に算入すべきでない。
2011 年国会侵入について日本政府が Icefog へ帰属した資料	未発見。Icefog との係は　Kaspersky による民間。
2015～16 年日本 Winnti incident の APT41 個人への再	未解決。Winnti と APT41 の部分重複以上の証拠が必要。
2019 年 12 月開始 LODEINFO の actor connection	JPCERT で活動開始は確認できたが、MISSION-001 では当時の一次資料から中国系 actor 帰属まで確証を得られなかった。
個々の日本被害組織名	JPCERT/CC・各社とも非公開の事案が多く、業種までしか判明しないケースが多数。
共通ゼロデイ供給者	CVE-2014-7247 等の actor 間共有現象は確認できるが、開発者・broker・販売者は未特定。

重要資料一と次の MISSION で追跡すべき未解決事項

以下は MISSION-001 で特に価値が高かった資料である。URL 欄は恒久 URL を確認できたものを直接記載し、それ以外は本回答の引用リンクを原文アクセス先として付した。

資料	発行主体・発行日	URL／原文	重要性
Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns…	U.S. Department of Justice、2018-12-20	https://www.justice.gov/archives/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion	**最重要。** APT10、MSS 天津市国家安全局、Huaying Haitai、Zhu Hua、Zhang Shilong、日本を含む MSP 侵害を一つの司法文書で接続。
Indictment / SDNY	U.S. Attorney's Office	原 PDF	起訴内容を press

資料	発行主体・発行日	URL／原文	重要性
APT10 materials	SDNY、2018-12-20		release より法的に精査する際の原資料。容疑はあくまで allegations である点も重要。
外交青書 2020：サイバー	日本国外務省、2020 年	https://www.mofa.go.jp/mofaj/gaiko/bluebook/2020/html/chapter3_01_03.html	2018 年、日本政府が中国を拠点とする APT10 による長期・広範な攻撃を非難した事実を公式確認。
menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations	Palo Alto Networks Unit 42、2017-02-16	原文	APT10/menuPass が日本を少なくとも 2014 年から狙ったこと、日本語・外交ルアー、ChChes、詳細な C2 係を示す。
menuPass Playbook and Indicators of Compromise	Palo Alto Networks Unit 42、2019-02-04	原文	APT10 alias、長期 TTP、Operation Cloud Hopper、malware⊠IOC の整理に重要。
BRONZE BUTLER Targets Japanese Enterprises	Secureworks、2017-10-12	https://www.secureworks.com/research/bronze-butler-targets-japanese-enterprises	**最重要。** Tick の日本特化標的、SKYSEA 0-day、マルウェア群、credential theft、exfiltration、PRC 起源評価とその根拠を詳細化。
VB2019 paper: APT cases exploiting vulnerabilities in region-specific software	JPCERT/CC researchers ／Virus Bulletin、VB2019 表　　Web 版 2020-05	原文	**MISSION-001 の技術的中核資料。** 三四郎一太郎SKYSEA、APT17、Blue Termite、Tick、APT10、Winnti を同じ日本インシデント文脈で比較。
Malware TSCookie	JPCERT/CC、2018-03	https://blogs.jpcert.or.jp/en/2018/03/malware-tscooki-7aa0.html	BlackTech の日本国内測、　MEXT impersonation、TSCookie を一次に近い形で確認。
Malware Used by BlackTech after Network Intrusion	JPCERT/CC、2019-09	原文	BlackTech が日本で単発ではなく侵入後活動まで継続していたことを示す。
IconDown – Downloader Used by BlackTech	JPCERT/CC、2019-10/11	https://blogs.jpcert.or.jp/en/2019/11/icondown-downloader-used-by-blacktech.html	日本組織での IconDown、C2、RC4、ASUS WebStorage supply-chain との接点。
The Icefog APT: Frequently Asked	Kaspersky GReAT、	https://securelist.com/the-	2011 年以降の日本標的、国会、Fuji TV、

資料	発行主体・発行日	URL／原文	重要性
Questions	2013-09-26	icefog-apt-frequently-asked-questions/57892/	日本中国経済協会、標的業種を記録。同時に国家帰属の弱さも示す。
IT Threat Evolution: Q3 2013	Kaspersky、2013-11-14	https://securelist.com/it-threat-evolution-q3-2013/57885/	Icefog C2、sinkhole、標的情報、操作者所在地推定を補強。
IXESHE: 持続的標的型攻撃調査	Trend Micro、2012-05-30	https://www.trendmicro.com/ja_jp/about/topics/2012/nt-20120530-01.html	2009 年まで遡る東アジア APT 活動、内部 C2 化という特徴を記録。APT12 系の前史調査起点。
The EPS Awakens / The EPS Awakens Part 2	FireEye、2015-12	原著の現行参照先・関連資料	APT16、日本・台湾標的、IRONHALO/ELMER、EPS exploit chain の基礎。
Hiding in Plain Sight: FireEye and Microsoft Expose Obfuscation Tactic…	FireEye、2015-05-14	原文現行ミラー	APT17/Deputy Dog と BLACKCOFFEE の China-based 評価に重要。
APT41: A Dual Espionage and Cyber Crime Operation	FireEye/Mandiant、2019-08-07	https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation	国家支援諜報と私的金銭目的活動の併存、Winnti/BARIUM との部分重複、supply chain モデルを示す。
Seven International Cyber Defendants, Including “APT41” Actors…	U.S. DOJ、2020-09-16	https://www.justice.gov/archives/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer	post-2020 補強資料。Chengdu 404、個人、日本被害を具体化。
中国政府を背景に持つ APT40…等について（外務報道官談話）	日本国外務省、2021-07-19	原文	APT40 だけでなく、Tick と PLA 61419 の日本政府評価を確認する重要な遡及帰属資料。
治安の回顧と展望（令和 3 年版）	警察庁、2021-12	警察庁公開 PDF	国内捜査と Tick/PLA 61419 attribution の係を確認する一次政府資料。
BlackTech joint cybersecurity advisory	米国・日本等政府機関、 2023 年	原文	pre-2020 BlackTech の日本活動を後年の PRC 国家関連評価と接続する資料。
Justice Department	U.S. DOJ、2025-03-05	https://	**エコシステム研究向**

資料	発行主体・発行日	URL／原文	重要性
Charges 12 Chinese Contract Hackers…		www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global	け。MPS/MSS、i-Soon、freelancer、APT27 という hacker-for-hire モデルを公式文書で具体化。ただし MISSION-001 各 actor への直接証拠ではない。

次の MISSION で追跡すべき未解決事項は、優先順位を次のように設定するのが妥当である。

優先度	未解決事項	追跡理由
P0	Tick ↔ PLA Unit 61419 の人物・企業・インフラ・国内サーバ契約の完全なリンクグラフ化	対日特化性が最も高く、日本政府自身が具体的 PLA unit を示している。公開捜査資料、刑事事件、法人WHOIS、サーバ契約記録まで遡る価値が最大。
P0	APT10 ↔ Tianjin State Security Bureau ↔ Huaying Haitai ↔ 日本被害の個別マッピング	国家機関・企業・人物・日本という四要素がすでに公開資料で接続されている。DOJ indictment の全 IOC、登録 domain、人物 alias を日本 incident へ突合すべき。
P0	一太郎／三四郎／SKYSEA ゼロデイの供給元・開発者・共有係	「中国サイバー作戦エコシステム」の核心になり得る。特に CVE-2014-7247 が複数 actor へ短期間で現れた理由を調べる必要がある。
P0	BlackTech の中国政府側組織・人員の同定	日本での pre-2020 incident corpus は豊富だがスポンサー側が空白。2023 年以降の政府情報を逆向きにたどるべき。
P1	2015～16 年 Winnti 日本案件 ↔ APT41/Chengdu 404 の再クラスタリング	code-signing certificate theft、supply chain、人材・インフラを DOJ 2020 資料と照合すると、初期の対日 APT41 活動が具体化する可能性がある。
P1	APT17 と Blue Termite 間の exploit 共有経路	同一 actor 化ではなく、exploit broker／developer／contractor 共有の有無を調査する。
P1	APT12/IXESHE/Etumbot の原著資料回収	2009～14 年という早期層を補完するため重要。Arbor ASERT 原 PDF、FireEye の HIGHTIDE/RIPTIDE 資料、CrowdStrike 資料まで一次へ遡る。
P1	2019 年 12 月 LODEINFO の初期活動と後年 actor attribution の検証	2019−2020 年代への連続性を判定する境界事例。2019 時点の IOC から後年クラスタへ

優先度	未解決事項	追跡理由
		pivot すべき。
P1	APT16⊠APT17⊠Tonto Team の日本被害組織と中国側人員の再調査	現状はベンダーによる China-based 評価止まり。政府機関・請負会社への接続ができれば重要度が大きく上がる。
P2	Icefog の「 中国系 APT」仮説を反証込みで再検討	日本標的としては重要だが、Kaspersky 自身が中国・韓国・日本の関係者および cybermercenary モデルを示している。国家帰属しない可能性も保持すべき。
P2	Blue Termite/CloudyOmega の中国帰属の有無をゼロベースで検証	日本 APT 史では重要だが、現時点で中国国家 actor に分類する根拠が不足。誤ったクラスタ統合を防ぐための反証調査として重要。
P2	APT10、APT40、APT41、i-Soon に見られる“地方情報機関 + 民間技術会社”モデルの比較	Tianjin MSS–Huaying Haitai、Hainan MSS–Hainan Xiandun、Chengdu 404、i-Soon の間に制度的共通性があるかを検証。ただし現時点で同一ネットワークとの証拠はない。

MISSION-001 時点の最重要未解決問題は、「誰が日本を攻撃したか」だけではなく、「誰が日本固有の脆弱性・アクセス・インフラ・人材を供給し、それらが複数の追跡名の間でどのように移動したのか」である。 とりわけ一太郎 CVE-2014-7247 の複数 actor 利用、Tick の SKYSEA CVE-2016-7836 ゼロデイ、APT10 の MSP 侵害、BlackTech/Winnti 系の供給網侵害は、個別 APT の割り究を超えて共通の「 能力供給層」を探索すべきい手掛かりを提供している。一方、それらの共通性から直ちに共通の国家指令系統を推定する証拠は、今回の調査では発見されな