

# Babel Street OSINTソリューション 活用による中国のグローバル戦略調査

中華人民共和国（中国）は、[世界覇権という中国の夢](#)を実現するため、太平洋の近隣諸国に対しては一連の軍事作戦に乗り出し、米国に対しては偽情報キャンペーンを展開してきました。また中国は、敵対関係にある国々のサプライチェーンへの参入を介して知的財産を盗もうとしています。

中国の政治的、経済的、軍事的な動きをより正確に予測し、それに応じて計画を立て、対応するために、米国国防総省をはじめとするインテリジェンス（情報機関）コミュニティは、オープンソースインテリジェンス（OSINT）ソリューションを必要としています。OSINTとは、インテリジェンス（諜報活動）における特定の優先事項、要件、またはギャップに対処するために、一般に公開されている情報（PAI: Publicly Available Information）や市販されている情報（CAI: Commercially Available Information）からインサイトを得る手法です。

## Babel Street製品

このユースケースで取り上げられているBabel Street製品の詳細については、以下をご覧ください。

- [Babel Street Insights](#)
- [Babel Street Insights Synthesis](#)
- [Babel Street Secure Access](#)
- [Babel Street Raw Collections](#)
- [Babel Street Refined Information](#)

以下のシナリオは、諜報員やアナリストはじめ、インテリジェンスに関わる様々な人々がBabel StreetエコシステムのOSINTソリューションを活用して中国のグローバル戦略を調査する方法を示しています。

## シナリオ 1：サビナ礁を巡る緊張状態に関するインサイトの深化

南沙諸島は、大小の島や100以上の岩礁からなる南シナ海の群島ですが、それらの所有権を巡り争いが繰り広げられています。サビナ礁は、この南沙諸島の一部です。中国、フィリピン、マレーシア、台湾、ベトナム、それらのいずれもが領有権を主張しています<sup>1</sup>。サビナ礁は、漁場、石油鉱床、天然ガス鉱床などの資源の近くに位置しており、戦略的な重要性を持っています。

礁の支配権を巡って、フィリピンは最近、海軍の駐留を強化し、礁湖内に沿岸警備船を停泊させたと報じられています。中国はこれを、フィリピンによる意図的な「長期的駐留」（long-term presence）であると見ており、中国政府はこの駐留が自国の領土主権を侵害していると考えています<sup>2</sup>。

重要なインテリジェンス要件の裏付けとして、サビナ礁についての調査を進めようとしているアナリストは、Babel Street Insightsから始めることができます。Insightsのユーザーフレンドリーなブーリアン検索を使うことによって、アナリストは「Xianbin Reef」（サビナ礁の中国名）や「military」（軍事）、「China」（中国）、「Philippines」（フィリピン）、「sign sovereignty」（主権）といった用語について、膨大な数の文書を調べることができます（図1参照）。そして、Insightsから得られた文書を読むことによって、アナリストは検索条件に加えることができる新たなキーワードを見つけることができ、検索された結果に対してさらに絞り込みをかけることができます。そのようなキーワードとして、「Declaration on the Conduct of Parties in the South China Sea」（南シナ海における締約国の行動に関する宣言）、「Chinese maritime militia」（中国の海上民兵）、「Chinese coast guard」（中国の沿岸警備隊）などが考えられます。

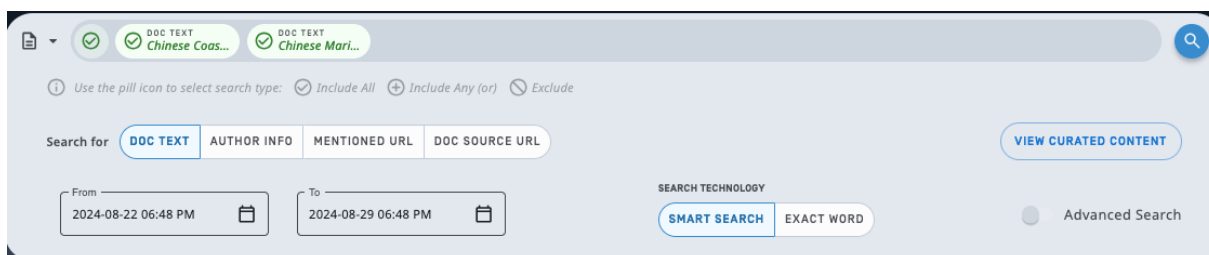


図1：ブーリアン検索を容易に実行できるInsightsのユーザーフレンドリーなインターフェース

このような調査によって、アナリストはサビナ礁を取り巻く複数のストーリーが展開していることを知ることになります。中国とフィリピンは、この状況をまったく異なる視点からとらえています。中国共産党（共産党）によって専門分野の報道が厳しく管理されている国においては、アナリストはInsightsの検索対象範囲を中国メディアに限定することによって、サビナ礁侵攻に対する中国の見解を見出すことができます。翻って、フィリピンのメディアのみを検索することで、アナリストは、フィリピンのジャーナリストが支持している見解を知ることができます。

昨今、ソーシャルメディアは、従来のメディア同様に重要な情報源となっています。サビナ礁の状況に関するフィリピン国民の見解を知りたいければ、アナリストはBabel Street Insightsを使って、人気のソーシャルメディアプラットフォーム上のサビナ礁関連の投稿を検索することができます。

しかしながら、中国のソーシャルメディアプラットフォームからインサイトを引き出す場合には、一層の困難が伴います。同国の「グレートファイアウォール」（インターネットトラフィックを検閲・監視する包括的な技術システム）によって、海外ユーザーからのアクセスが禁止されているからです。Babel Street Insightsのマネージド・アトリビュション機能を利用することで、アナリストはグレートファイアウォールを突破し、WeChat（中国ではWeixinとして知られている）、Weibo、Douyinなどの中国発のプラットフォームにアクセスすることができるようになります。中国はこれらのサイトに投稿される反政府感情を監視・検閲しており、アナリストにとって、これらの情報から中国国民の真意の判断を困難にしています。一方で、中国は工作員を雇ってこれらのサイトに共産党の主張を支持する内容を大量に投稿させているため、中国のソーシャルメディアプラットフォーム上の情報を分析することによって、アナリストは、中国政府が国民に伝えようとしているものについて、深い理解を得ることができます。

中国とフィリピンのソーシャルメディアの両方を調べる中で、アナリストは重要な特定のアカウントの存在に気づくことがあります。その発見をさらに深く掘り下げるため、それらの特定の発信者に絞って検索することができます。Babel Street Insightsを使えば、あるユーザーを、さまざまなソーシャルメディアプラットフォームに点在するスクリーンネームやその投稿と結びつけることができます。また、複数のスクリーンネームを現実世界の人物に結びつけ、その人物の連絡先情報を見つけることができるかもしれません。

諜報員やアナリストは、さらなるインサイトを得るために、Babel Street Synthesisを利用することができます。例えば、あるソーシャルメディア上でサビナ礁に関連する論争を行なっているアカウント同士の関係性を示すネットワークグラフを作成したい場合、中国のサイトで「先賓礁」（「サビナ礁」の中国語での呼び方）というキーワードを指定するだけで済みます。Synthesisは、このキーワードを使用しているユーザー間の関係性とキーワードに対する関連性を計り出し、最も影響力を持つ者を正確に特定します。このようなインフルエンサーの特定を通じて、Babel Street Synthesisはアナリストに対して、これらのユーザーをより深く調査するきっかけを与えてくれます。例えば、そのユーザーのオンラインプロフィール、アクティビティ、さらには関係者にまで調査を広げることができるかもしれません。サビナ礁を取り巻く状況の調査においては、アナリストが中国のシンパや中国の主張を積極的に推進している工作員を特定するのに、こうした機能が役立ちます。

どんな、インテリジェンス・サーチも一度だけで完了するタスクではありえません。むしろ、アナリストや諜報員は情報の継続的な更新を必要としています。Babel Streetの継続的検索機能は、ユーザーが検索条件を指定して保存した後、アクティブにその検索を使用しているかどうかに関わらず、検索処理を定期実行し、情報の更新と変更を追跡し、この情報を自動的に追加します。アナリストが検索結果の要約された展望を必要とする場合には、Insights AI Betaを使って関連する検索結果を要約することもできます。（図2を参照）この機能は、特に調査の更新時に役立ちます。アナリストは、前回の調査以降にサビナ礁周辺で発生した騒乱の報告を、Insights AI Betaにまとめてもらうことができます。

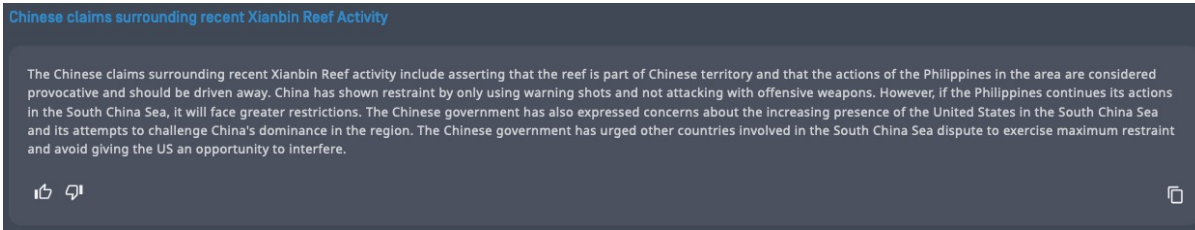


図2：検索結果を元にした、Insights AI Betaによる要約

## シナリオ 2：偽情報の検出と対策

中国はしばしば、敵対国の市民の間に不和と不安をまき散らすために、事実と異なる情報や機密情報を発信することがあります。例えば、中国の工作員はソーシャルメディアを使って、2023年の壊滅的なマウイ島の山火事は、米国の新型気象兵器の実験によって引き起こされたと主張しました<sup>3</sup>。これらの投稿の多くには、AIを使って生成された写真が添付されていました。最近では、日本の横須賀海軍基地に停泊しているニミッツ級空母ロナルド・レーガンの極めて機密性の高い鳥瞰図がソーシャルメディアに投稿されました<sup>4</sup>。こうした写真の公開によって引き起こされた安全保障上の懸念が、空母に駐留する人々やその友人や家族を動揺させたことは間違いありません。

偽情報は、分裂や動揺を招くような話題を中心に発生する傾向があります。そのため、中国発の偽情報を探すアナリストは、自然災害、新たな関税、軍事衝突、その他さまざまな出来事を検索することからInsightsでの調査を始めることができます。アナリストは、伝統的メディアやソーシャルメディアを検索して得られた、このテーマに関する中国の報道を、確認された事実やアナリスト自身の諜報経験の両方と比較することによって、特定の問題について中国が何を考えているかを徐々に理解できるようになります。

次に、OSINTにおいて、疑いようがない事実を探求するにあたって、インテリジェンスの経験が、どのようにそれを補完することができるかを見ていきます。

マウイ島の山火事は6,700エーカー近くが8日間で焼失し、2,200棟以上の建物を破壊し、102人が亡くなりました<sup>5</sup>。Insightsでこの出来事を調査したアナリストは、損壊した電力インフラからの火花が火元になったことを当初から知っていたわけではありません。（原因が報告されたのは、大火から約2か月後の10月になってからでした<sup>6</sup>。）しかし、アナリスト自身の経験、訓練、そして常識に鑑みて、米国の気象兵器が山火事を引き起こした可能性はないと確信していました。米国は現在、気象兵器を使用していません。そして歴史的に見ても、国防総省は、兵器のテストにあたって、アメリカの砂漠の広大な無人の土地を選んできた事実があり、U.S. News & World Report誌が選ぶ世界のトップ<sup>6</sup>に輝く避暑地である、この人口の多い島を実験場所として選ぶようなことは到底考えられません<sup>7</sup>。災害に関するいくつかの投稿には明らかに偽情報が含まれていました。

Babel Streetを使って、マウイ島や類似の状況をめぐる虚偽のシナリオを検証することで、アナリストは偽情報の発信源を突き止め、中国が真実でない主張を広めることで何を達成しようとしているのかを徐々に突き止めます。そのために、中国のソーシャルメディアサイトにアクセスする必要があります。アナリストは、「気象兵器」に言及したソーシャルメディアの投稿から、Insightsの人物検索機能を使って投稿者のオンライン上の活動やペルソナについて詳しく調べ、そうした人物像を現実の身元と結びつけることができます。

アナリストは、このプロセスをSynthesisで継続し、投稿の中で「気象兵器」に言及している人々のネットワークを特定できます。さらに、Synthesisにより、これらのソーシャルネットワークの中で最も影響力を持つインフルエンサーを特定することができます。最終的に、アナリストはこのネットワークのメンバーによる投稿を監視し、その内容に偽情報やその他のレッドフラッグとなるテーマが含まれていないかどうかを調べることができます。

同じようなテクニックを使って、アナリストは中国がどのように意図的に言葉を悪用して自国のストーリーを強化しているのかを研究することができます。中国共産党が75周年を迎える前夜、中国の最高指導者である習近平は「一つの中国政策」へのコミットメントを改めて表明し、「中国の夢」の一環として台湾の「統一」<sup>8</sup>を達成することを誓



いました。ここで、「統一」という言葉を使うことによって、現代中国が台湾に対して何らかの権利があることが仄めかされています。しかし、実際にはいかなる権利も存在しません。両国には、十七世紀にさかのぼる帝国主義と併合の複雑な歴史があります。しかし、国共内戦後の1949年に中国共産党によって設立された現在の中国政府が台湾を統治したことは一度もありません。（「併合」や「占領」といった、より適切な表現ではなく）「統一」といった言葉を使うのは、権威主義政権が意図的に認識を形成しようとする取り組みの表れであり、中国の市民やさらに広範な世界社会を中国が囑望する方向に向かわせようとするものなのです。中国が人心掌握に成功すれば、中国の軍事侵攻は受け入れられやすくなります。

### シナリオ 3：サプライチェーンの保護による知的財産窃盗の防止

米国では、大統領令、国家安全保障戦略、国防戦略、数多くの立法措置が、サプライチェーンの保護の重要性を証明しています。中国に端を発するサプライチェーンの脅威には、重要資源を巡る競争とその資源の搾取、さらにサイバー攻撃が含まれます。

米国向け、あるいは米国内で事業を行う企業の外国人所有権、支配権、影響力が不明瞭になってきており、ますます重要な懸念事項となっています。世界支配を目指す中国の取り組みには最先端技術の利用が含まれ、下院外交委員会<sup>9</sup>から主流メディアまで、さまざまな情報源が、中国は技術的な知的財産を創造するのではなく、盗用することが多いと報じています。イリノイ州の半導体メーカーは、中国の顧客によって自社製品のリバースエンジニアリングが行われたことを発見しました<sup>10</sup>。また、テキサス州の化学メーカーでは、自社独自の技術が中国の顧客によって使用されていることがわかりました<sup>11</sup>。アメリカ合衆国政府は技術的な知的財産の盗難に対して脆弱性を持ち、人工知能、衛星開発、宇宙探査、原子力エネルギー、造船、航空分野で活動しているアメリカ企業も同様です。

米国内のサプライチェーンに中国系企業を密かに参入させるこの方法は、中国が知的財産の窃盗を行うメカニズムのひとつになっています。一見無害に見える中国企業も、実は中国政府や軍とつながりがあるかもしれず、盗まれた情報は、中国の軍事作戦を強化するために使われるかもしれないのです<sup>12</sup>。

アメリカ合衆国政府とそのベンダーは、サプライヤーおよびその最終的な実質的所有者を監視リストと照合すべきであることは明白です。しかし、政府レベルの照合だけでは必ずしも十分ではありません。サプライチェーンを多層にわたって可視化するには、ベンダーの徹底的な審査が必要です。A社が「問題なし」と判定された場合であっても、A社のサプライヤーであるB社はどうでしょうか。そして、B社のサプライヤーであるC社は？政府機関やベンダーは、制裁対象または「リスクが示された」事業体と密接な関係のあるサプライヤーと、知らずに取引している可能性があります。

Babel Street Dataは、アナリストや情報担当者がベンダーを吟味し、サプライチェーンを保護するのに役立ちます。アナリストはBabel Street Dataを利用して、自社やベンダーのサプライチェーンに関する特有の疑問に答えるデータ収集戦略を立てることができます。これによって、リスク懸念のある組織の独自の監視リストを作成できます。このリストは、最終的な実質的所有者の名前の羅列以上の価値を持っています。リスク懸念のある企業が特定された上で、アナリストはBabel Street InsightsとSynthesisを使用してこれらの企業をさらに深く調査し、サプライチェーンにおけるその企業の存在が米国にリスクをもたらすかどうかを判断することができます。

紛争海域での軍事侵攻、巧妙な誤情報・偽情報キャンペーン、サプライチェーン支配の試みはすべて、中国が拡張主義的な「中国の夢」を追求する目的から生じています。これらの行動は、国際規範への挑戦であるのみならず、米国の国家安全保障と確立された世界秩序の安定を脅かすものです。したがって、こうした活動を検知し、理解し、対抗する能力は、かつてないほど不可欠なものとなっています。Babel Streetは、その高度なソリューションによって、実行に結びつく意思決定に必要な、活動の監視、新たな脅威の特定、虚偽や偏ったシナリオの解明、隠れたつながりの発見など、様々な側面でアナリストを支援します。

## 文末脚注

1. CIA, "Explore All Countries — Spratly Islands," The World Factbook, September 2024, <https://www.cia.gov/the-world-factbook/countries/spratly-islands/>

2. Babel Street Insights, 2024

3. Sanger, David E. and Myers, Steven Lee, "China Sows Disinformation About Hawaii Fires Using New Techniques," The New York Times, September 2023, <https://www.nytimes.com/2023/09/11/us/politics/china-disinformation-ai.html>

4. Wilson, Alex and Kusumoto, Hana, "Navy probes apparent drone footage of USS Ronald Reagan posted on social media," Stars and Stripes, May 2024, <https://www.stripes.com/branches/navy/2024-05-10/drone-footage-ronald-reagan-yokosuka-13813098.html>

5. World Vision, "Maui wildfires: Facts, FAQs, and how to help," accessed November 2024, <https://www.worldvision.org/disaster-relief-news-stories/maui-wildfires-facts-faqs-how-to-help#:~:text=The%20deadliest%20U.S.%20wildfire%20in,according%20to%20Maui%20County%20officials>

6. Alfonseca, Kiara and Sarnoff, Leah, "Broken power lines caused deadly Maui wildfire, new report shows," ABC News, October 2024, <https://abcnews.go.com/US/broken-power-lines-caused-deadly-maui-wildfires-new-story?id=114423744#:~:text=%22The%20cause%20of%20the%20fire,had%20been%20two%20separate%20fires>

7. Von Tersch, Elizabeth, "World's Best Places to Visit," U.S. News & World Report, August 2024, <https://travel.usnews.com/rankings/worlds-best-vacations/>

8. Gan, Nectar, "Xi vows 'reunification' with Taiwan on eve of Communist China's 75th birthday," CNN, October 2024, <https://www.cnn.com/2024/10/01/china/china-xi-reunification-taiwan-national-day-intl-hnk/index.html>

9. House Foreign Affairs Committee, "Egregious Cases of Chinese Theft of American Intellectual Property," accessed October 2024, <https://foreignaffairs.house.gov/wp-content/uploads/2020/02/Egregious-Cases-of-Chinese-Theft-of-American-Intellectual-Property.pdf>

10. Ibid

11. Ibid

12. Department of Defense, "DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021," October 2022, <https://www.defense.gov/News/Releases/Release/article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/>

### 免責事項：

この文書に記載されているすべての名称、企業、事象は架空のものです。実在の人物（生死を問わない）、場所、会社、製品と同一とみなすことは意図されておらず、そのように推測されるべきでもありません。



Babel Streetは、信頼あるテクノロジーパートナーとして、世界最先端のアイデンティティインテリジェンスとリスク対策を実現します。Babel Street Insightsプラットフォームは、リスクと信頼のギャップを埋める高度なAIとデータ分析ソリューションを提供します。

Babel Streetは、言語を問わずにすぐに分析に使える最高レベルのデータを提供し、プロアクティブなリスク特定、多面的なインサイトの取得、高速自動処理、既存システムとのシームレスな連携を実現します。政府機関や企業が、身元の特特定やリスクに関するハイリスクな業務を戦略的優位性に転換できるよう支援します。

詳しくは、[babelstreet.jp](https://babelstreet.jp) をご覧ください。