BABELSTREET

法執行機関のための マネージドアトリビューション 基本ガイド

進化する犯罪情勢

犯罪者はますます高度な技術を駆使して身元や行動を隠蔽するようになっており、州や地方の法執行機関にとり、今まで以上にオンライン捜査が難しくなっています。捜査機関が分析しなければならないデータと、デジタル捜査に対する信頼性との間のギャップ（「リスクと信頼性のギャップ」と呼ばれる）は拡大しており、捜査官やアナリストは業務上のリスクにさらされています。

セキュリティを損なうことなく容疑者を効果的に追跡し、潜入捜査を行い、情報を収集するために、捜査機関にはマネージドアトリビューションが必要です。これは、法執行専門家がデジタルフィンガープリントを管理し、オンラインで安全に捜査を実施するためには不可欠な機能なのです。

現在の犯罪者は地理的な境界に縛られることはなく、インターネットやその他のデジタルツールを駆使し、州境や国境を越えて離れた場所から犯罪を実行するようになりました。サイバー犯罪、オンライン詐欺、違法薬物取引、そして強盗や傷害のような従来の犯罪でさえ、多くの場合、デジタルフットプリントを残しています。こうした状況の変化に呼応して、法執行機関は犯人を効果的に捜査・逮捕するにあたり、新たな戦略に適応し、導入しなければなりません。

これまでの捜査方法は今でも重要です。ただし、巧妙なオンライン犯罪活動に対して無力な部分もあります。IPアドレスはなりすますことができ、オンライン上の身元は捏造することができ、デジタル証跡は簡単に操作または破壊することができます。こうした技術的な制限により捜査が妨げられ、司法手続きを遅滞なく進められず、地域社会が危険にさらされ続けることになります。

マネージドアトリビューションについて

マネージドアトリビューション（管理された属性）は、このような課題に対する解決策を提供します。これは、法執行機関が捜査官のアイデンティティを保護し、業務上のセキュリティを維持しながら、オンライン捜査を隠密かつ効果的に実施することを可能にする一連の手法ならびに技術なのです。捜査官がネットの世界で潜入捜査を行い、情報収集や犯罪活動の追跡を行う際に、正体を明かさず、捜査に支障をきたすことなく行えるようにする、デジタル世界における変装のようなものだと考えてください

マネージドアトリビューションの主な構成要素：

- IPマスキングと位置情報の偽装 — ネットワーク上のアイデンティティを変更することで追跡を防ぎます
- デバイスとブラウザのエミュレーション — 捜査員の行動が、捜査対象となるプラットフォーム上の他の一般的なユーザーと何も変わって見えないことを確実にします
- セキュアなインフラを介したトラフィックのルーティング — 捜査機関のネットワークを悪意のある行為者から隠し、保護します
- 永続的または一時的セッションでのブラウジング — 捜査官は長期的に使用するデジタルペルソナを作成したり、1回限りの追跡不可能なセッションを使用したりすることが可能

マネージドアトリビューションはどのようなときに使われるのか？

マネージドアトリビューションは万能のソリューションではなく、従来の方法では不十分な場合や、捜査官の安全が最優先される場合に戦略的に導入されものです。主な利用シナリオをいくつか紹介します。

覆面捜査 — 潜入捜査官がオンラインで活動する際、マネージドアトリビューションが彼らの真の身元を保護し、暴露することを防ぐことで、安全かつ長期的に捜査活動を続けられるようにします。

犯罪ネットワークへの潜入 — 犯罪活動が計画または実行されている閉鎖的または非公開のオンライングループにアクセスする場合、マネージドアトリビューションによって、捜査官は容疑者を警戒させることなく、グループに紛れ込み、証拠を収集し、不正な活動を追跡することができます。

サイバー犯罪の捜査 — 犯罪者は多くの場合、高度なテクニックを使って居場所や身元を隠します。マネージドアトリビューションにより、捜査官はこうした個人とその悪意のある活動を追跡できます。

捜査官の匿名性を確保 — 潜入捜査以外の役割であっても、捜査官の個人情報がさらされたり、捜査官を狙った嫌がらせなど、増大するリスクに直面しています。マネージドアトリビューションは、捜査官の個人情報を保護し、標的になるのを防ぐのに役立ちます。

複雑なオンライン事件での証拠収集 — マネージドアトリビューションで秘密裏に捜査することで、捜査官は容疑者に気づかれることなく、また捜査を危険にさらすことなく、真正なデジタル証拠を収集することができます。その結果、より強固に裁判を進めることが可能になり、起訴を成功に導けるようになります。

管轄を超えた捜査 — マネージドアトリビューションは、異なる法執行機関間の協力を促進し、司法権の境界を越えて情報を共有し、捜査を調整できます。

マネージドアトリビューションはVPNとどのような点で異なるのか？

「すでに暗号化とプライバシーのためにVPNを使っているのに、マネージドアトリビューションを使う必要性はあるのか？」とお考えの方もいるでしょう。

仮想プライベートネットワーク（VPN）は、主にインターネットトラフィックを暗号化し、安全なサーバーを経由させることで、プライバシーを保護し、盗聴を防ぎ、ユーザー本来のIPアドレスを隠します。VPNは、IPアドレスを変更し、トラフィックを暗号化しますが、オンライン上でのユーザーの存在をコントロールする術はほぼありません。VPNはマスクされた（しかし静的な）アイデンティティを提供することで、匿名性とセキュリティに重点を置いています。

マネージドアトリビューションにより、オンラインでのユーザーは存在を完全にコントロールおよびカスタマイズできます。ユーザーが異なるデジタルペルソナ、場所、行動を設定できるようにして、単なる匿名性以上の保護を実現します。マネージドアトリビューションソリューションは、ブラウザのフィンガープリント、言語設定、タイムゾーン、さらには行動パターンなど、動的にアイデンティティを変更できます。ユーザーの身元を隠すだけでなく、積極的な擬態を可能にすることで、ユーザーは怪しまれることなく特定のオンライン環境に溶け込むことができます。

VPNは一般的なプライバシーとセキュリティ保護には最適ですが、マネージドアトリビューションは高度なデジタルアイデンティティ操作に特化したツールです。匿名性が得たいだけなら、VPNで事足ります。しかし、ユーザーが捜査のために特定の環境に溶け込む必要がある場合、マネージドアトリビューションが不可欠です。

機能	VPN	マネージドアトリビューション
プライバシー保護	✓	✓
IPアドレス変更	✓	✓
暗号化とセキュリティ	✓	✓
地理的制限の回避	✓	✓
ブラウザフィンガープリントの偽装	X	✓
タイムゾーンと言語の変更	X	✓
仮想マシンの隔離	X	✓
マルウェアセーフなファイル分析	X	✓
個人情報不要	X	✓
仮想移動体通信事業者（MVNO）サポート	X	✓
仮想携帯電話番号	X	✓
セッションモードの多様性	X	✓
グローバルエグレスネットワーク	X	✓
アンドロイドOSエミュレーション	X	✓
自動セッションロギング	X	✓
複数ユーザーによる共同作業とチームコントロール	X	✓

マネージドアトリビューションソリューションに求めるべき機能とは？

法執行機関がマネージドアトリビューションソリューションを選定する際には、以下のような主要機能に注目します。

セキュリティと隔離

- 仮想マシンの隔離 ― 各閲覧セッションは、ネットワークやデバイスから完全に隔離された独自のセキュアな仮想マシンで実行されるため、マルウェアなどの脅威が組織のシステムに到達することはありません。
- マルウェアセーフなファイル分析 ― 隔離された環境で不審なファイルを分析し、潜在的なマルウェアやその他のサイバー脅威からインフラを保護します。

個人情報不要 ― アクセスに個人情報（PII、Eメール、電話番号）を必要としないため、中断することなくセッションの完全性を維持しながら、個人情報の暴露リスクを排除することができます。

- カスタマイズ可能で安全なデプロイメント ― 柔軟なログ記録・保存オプションにより、コンプライアンスや運用要件に合わせたプライベートな隔離環境をデプロイできます。

仮想移動体通信事業者 (MVNO) サポート ― セキュリティと運用の柔軟性を強化するために、仮想キャリアを通じてモバイルネットワークとセキュアに通信を行います。

匿名性とアトリビューション管理

- 包括的なアイデンティティ保護 ― IPアドレス、ブラウザのフィンガープリント、その他の識別子を隠すことで完全な匿名性を維持。
- 仮想携帯電話番号 ― 仮想または匿名化された携帯電話番号へのアクセスを提供することで、二要素認証（2FA）と安全な通信を可能にし、プライバシーを確保し、暴露リスクを低減。

運用の柔軟性と効率性

- セッションモードの多様性 ー 運用上のニーズに応じて、オンラインペルソナを長期的に維持するタイプの捜査（永続的ブラウジング）か、一時的なセッション（非永続的ブラウジング）を選択できます。
- グローバルエグレスネットワーク ー 地理的な制約を回避し、無制限の調査と情報収集を可能にするセキュアなエグレスポイントを持つ世界規模のネットワークを活用。
- Android OSエミュレーション ー 外部デバイスやサードパーティツールを必要とせず、モバイル専用プラットフォームや地域アプリにシームレスにアクセス。
- 合理化されたユーザーエクスペリエンス ー 非効率な作業を最小限に抑え、アナリストはツールの利用に悩まされることなく、調査に集中することができる最適化されたワークフロー。
- 拡張OSINTワークフロー統合 — サードパーティ製OSINTツールとデータソースに対応するシームレスな拡張性。

コンプライアンス、監査、コラボレーション

- ミスを防止されたコンプライアンス遵守 ー 内蔵されたセーフガードにより、大きなリスクを伴う環境での誤認のリスクを低減し、コンプライアンスを確保し、よくあるユーザーのミスを防止します。
- 自動セッションロギング ー コンプライアンス、セキュリティ、内部監督のためにセッションを自動的に記録・監査し、運用の透明性を確保します。
- 複数ユーザーによる共同作業とチームコントロール ー ロールベースのアクセス、捜査用ワークスペースの共有、チームの権限管理により、安全なコラボレーションを実現します。

最後に、 マネージドアトリビューションのソリューションベンダーは、ミッションクリティカルな業務における、迅速なオンボーディング、高い可用性、迅速な問題解決を実現するための専任のプロフェッショナルサポートを提供すべきです。

マネージドアトリビューションソリューションの導入

マネージドアトリビューションソリューションの導入は、必ずしも複雑な作業というわけではありません。既存の捜査ツールキットに強力な新ツールが加わったと考えてください。以下のようなステップを検討してみてください。

現在のリスクおよびニーズの評価 — オンライン捜査の実施に伴い、捜査官やインフラがリスクにさらされていないかを判断する。マネージドアトリビューション機能を必要とする捜査部門を特定する。

選択肢を探る — 政府機関の要件に対応し、習得そして使用が容易で、予算内に収まるツールを探す。

導入 — 選択したベンダーと協力して、ソリューションの適切なインストールと設定を確実に行う。そのソリューションが、プライバシー拡張機能や追跡防止ツールにより、安全なブラウジング環境を提供していることを確認する。

デジタル諜報活動技術に関する捜査官の研修 — アトリビューションリスクとベストプラクティスについて捜査官を教育する。疑わしいウェブサイトやフォーラムを安全に閲覧する方法について、定期的に講習を行う。

倫理的かつ合法的な使用に関するポリシーの確立 — 個人の権利とプライバシーを尊重したオンライン捜査のための明確な標準作業手順書（SOP: Standard Operating Procedures）を作成する。法律顧問と協力し、適用される法律とデジタル証拠の取り扱いを確実に遵守する。

マネージドアトリビューションの使用に関するポリシーのサンプルについては付録を参照してください。

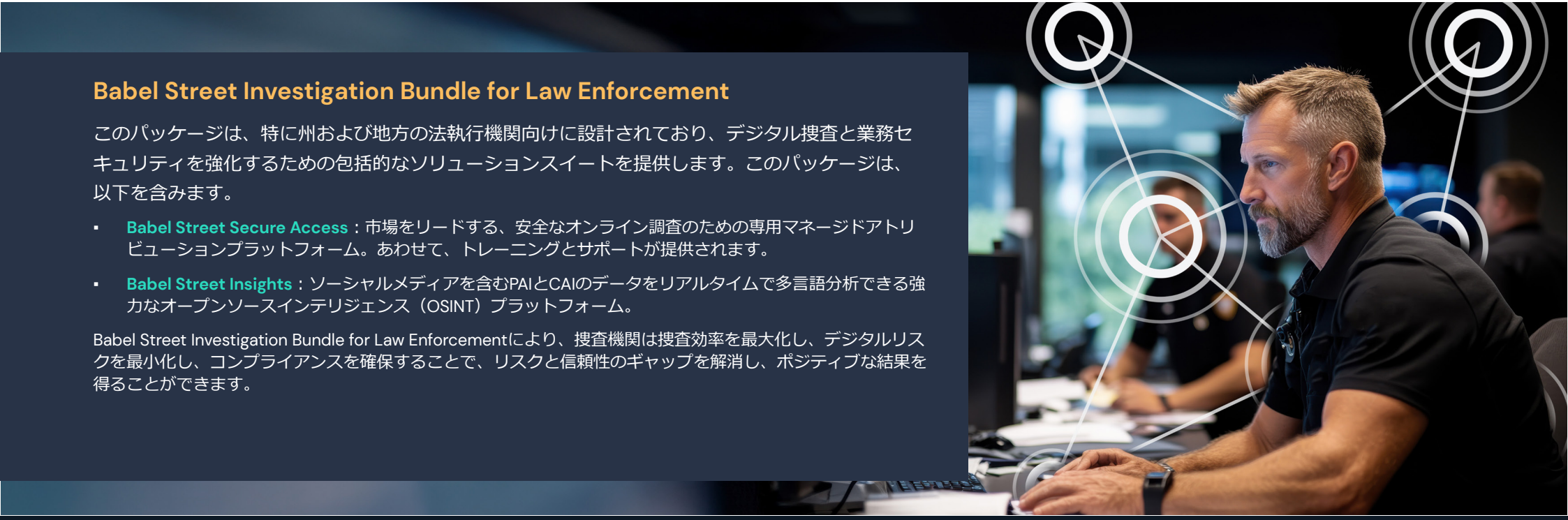
潜入捜査の暴露

人身売買の容疑者についてオンライン捜査を行っていた州警察の部署が、捜査当局に登録されたIPアドレスを使用して犯罪フォーラムに無意識のうちにアクセスしていました。数時間以内に、フォーラムの管理者は訪問者の出所を特定し、サイトをロックダウンして重要な証拠を消し去り、人身売買業者に警告を発しました。マネージドアトリビューションがあれば、部署はその存在を偽装し、発見されることなく監視を続けることができたはずです。

法執行機関におけるマネージドアトリビューションの未来

テクノロジーが進化し続けるにつれて、犯罪者の手口も進化しています。マネージドアトリビューションは、法執行機関が地域社会、家族、アイデンティティを守るために必要なツールを装備する上で、ますます重要な役割を果たすでしょう。

Babel Street Investigation Bundle for Law Enforcementは、マネージドアトリビューションのためのBabel Street Secure Accessと、リアルタイムのデータ分析と捜査インテリジェンスのためのBabel Street Insightsを含み、州および地方の法執行機関に包括的なソリューションスイートを提供します。これらのツールにより、法執行機関の専門家がセキュリティとコンプライアンスを維持しながら、現代の犯罪戦略に対して効果的に対処できるようになります。



Babel Street Investigation Bundle for Law Enforcement

このパッケージは、特に州および地方の法執行機関向けに設計されており、デジタル捜査と業務セキュリティを強化するための包括的なソリューションスイートを提供します。このパッケージは、以下を含みます。

- **Babel Street Secure Access**：市場をリードする、安全なオンライン調査のための専用マネージドアトリビューションプラットフォーム。あわせて、トレーニングとサポートが提供されます。
- **Babel Street Insights**：ソーシャルメディアを含むPAIとCAIのデータをリアルタイムで多言語分析できる強力なオープンソースインテリジェンス（OSINT）プラットフォーム。

Babel Street Investigation Bundle for Law Enforcementにより、捜査機関は捜査効率を最大化し、デジタルリスクを最小化し、コンプライアンスを確保することで、リスクと信頼性のギャップを解消し、ポジティブな結果を得ることができます。

まとめ

デジタル捜査の複雑化に伴い、オンラインセキュリティの確保と業務上の匿名性を積極的に推し進めるアプローチが求められています。州および地方の法執行機関にとって、マネージドアトリビューションは、捜査の完全性を維持し、捜査官を保護し、コンプライアンスの遵守を確保するために不可欠なのです。こうしたソリューションなしには、捜査機関が暴露されたり、捜査が危険にさらされたり、サイバーセキュリティの脅威にさらされたりすることになります。

Babel Street Secure Accessを採用することで、法執行機関の専門家は、より安全かつ効果的で、法的に健全な捜査を行いながら、リスクと信頼性のギャップを埋めることができます。

付録

マネージドアトリビューションの使用に関するサンプルポリシー

ポリシータイトル：マネージドアトリビューションの使用ポリシー

発効日：

レビュー日：

承認者：

目的

本ポリシーは、捜査官の匿名性を保護し、捜査の完全性を維持し、適用される法律の遵守を確保するために、オンライン捜査においてマネージドアトリビューション技術を倫理的かつ合法的に使用するためのガイドラインを定めるものです。

適用範囲

このポリシーは、捜査目的でマネージドアトリビューションツールの使用を許可されたすべての職員に適用されます。

ポリシーガイドライン

- マネージドアトリビューションは、合法的な捜査や情報収集活動にのみ使用されなければいけません。
- 担当者は、使用前にマネージドアトリビューション技術に関するトレーニングを受けてください。
- マネージドアトリビューションの使用はすべて文書化する必要があり、定期的な監査の対象となります。
- マネージドアトリビューションを使用して捜査セッションを開始する前に、捜査官は必要な承認を得なければいけません。
- マネージドアトリビューションツールの使用は、連邦、州、および地方の法律および規制に準拠する必要があります。
- 個人的な利益や不正な目的のためにマネージドアトリビューションを悪用した場合、懲戒処分の対象となります。

説明責任と監督

- 法執行機関は、マネージドアトリビューションツールの使用状況を監視する監督官を指名するものとします。
- ポリシー要件の遵守を確認するために、定期的な監査が実施されます。
- 捜査官は、マネージドアトリビューションを使用した捜査の目的と結果を詳述したレポートを提出する必要があります。
- マネージドアトリビューションの不正使用は調査の対象となり、適切な措置が取られます。

トレーニングとコンプライアンス

- マネージドアトリビューションを使用する職員は全員、初期および継続的なトレーニングを完了する必要があります。
- 本ポリシーが遵守されているかどうか定期的に確認が行われ、ポリシーは必要に応じて更新されます。
- 捜査官は、マネージドアトリビューションに関連する倫理的考慮事項とリスクを理解する必要があります。

Babel Street は、世界で最も高度なアイデンティティ・インテリジェンスとリスク管理を可能にする、信頼、実績のあるテクノロジーパートナーです。 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 およびデータ分析ソリューションを提供します。

Babel Street は、言語を問わず他に類を見ない分析対応データ、能動的なリスク識別、360 度のインサイト、高速自動化、既存システムへのシームレスな統合を提供します。 当社は、政府機関や企業組織が、重要なアイデンティティおよびリスク管理を戦略的な優位性に変換できるように支援します。

詳細については、babelstreet.jp をご覧ください。

BABELSTREET