九州大学学術情報リポジトリ
Kyushu University Institutional Repository

ダイナミック・セキュリティと刑務所インテリジェンスに関するハンドブック（２・完）

九州刑事政策研究会（訳）

大谷，彬矩
日本学術振興会 ： 特別研究員(PD)

相澤，育郎
立正大学法学部 ： 助教

https://doi.org/10.15017/4485652

出版情報：法政研究. 88 (1), pp.84-47, 2021-07-27. Hosei Gakkai (Institute for Law and Politics) Kyushu University
バージョン：
権利関係：

ダイナミック・セキュリティと刑務所インテリジェンスに関するハンドブック（２・完）

九州刑事政策研究会（訳）

目次

翻訳者によるはしがき

本資料は、国際連合の機関の一つである国連薬物犯罪事務所（United Nations Office on Drugs and Crime, UNODC）が、2015年に公表した「ダイナミック・セキュリティと刑務所インテリジェンスに関するハンドブック[(i)]」（以下、「ハンドブック」と記す）を訳出したものである。本号では、ハンドブックの第３章および第４章を翻訳し、巻末の付録は割愛した。

ハンドブックの翻訳は英語版を基本とし、さらに正確を期すため、これまで日本で公にされてきた、国際条約・国連準則および欧州評議会による勧告の翻訳も可能な限り参照している。第３章を大谷彬矩が、第４章を相澤育郎が翻訳した。なお、本文で〔 〕を付している箇所は、読者の理解を助ける意図から、翻訳者が補充したものである。

ハンドブックでは、国際条約・国連準則や欧州評議会による勧告の他、多くの文献が引用されている。それらについて、すでに翻訳が公表されているものについては割愛し[(ii)]、公表されていないものについては訳出した。ただし、ハンドブックが公

（ｉ） UNODC, Handbook on Dynamic Security and Prison Intelligence, 2015.
（ii） 本号で翻訳した範囲のうち、ハンドブックで引用された文献の翻訳が掲載されているものと

表されたのは2015年であるため、その時点での文献に依拠している。

（大谷彬矩）

第３章　刑務所インテリジェンス：定義、ガヴァナンス、組織

刑務所インテリジェンスの重要性

インテリジェンスの機能は、どの組織にとっても重要な構成要素である。法執行機関、軍隊および商業ビジネスにおいて、インテリジェンスと分析は、意思決定過程において幹部職員によって用いられてきた。インテリジェンスは、不明確性を減少させ、適切な分野に資源を集中させることに役立つ[16]。

拘禁は、継続的な犯罪行為の抑止には必ずしもならない。受刑者の中には、刑務所にいる間に犯罪活動を継続する者もいる。このことは、不法なビジネスを運用したり、他の受刑者を急進化しようと試みたり、刑務所内でギャングに関連する活動を継続するといった形で現れる。彼らは、テロリスト活動への指示や、薬物組織および凶悪犯罪集団の運営を含む、刑務所の外の犯罪活動を維持しようと努める。

国際的な潮流は、犯罪ネットワークが刑務所内で存在し続けていることも示している。犯罪者は、刑務所にいる間に接触し、場合によっては、その犯罪性を、刑務所システムを超えて拡張する。受刑者の中には、逃走を企て、刑務所の規律秩序を害することを目的とした活動を行う者もいる。他の受刑者は、職員を買収または籠絡し、刑務所内に不正物品を持ち込ませることを試みる。

刑事執行機関がそれらの活動を特定することを保証するために、すべての刑務所は、安全な環境で、保安関連情報を収集し、評価することを可能にする構造化され

して、吉田敏雄「欧州刑事施設規則（１）（２）―2006年１月11日の欧州会議閣僚委員会勧告２号―」北海学園大学学園論集135号（2008年）95-114頁、136号（2008年）117-137頁。

(16)　例えば、警察活動に関するインテリジェンスの重要性の議論について、*UNODC Toolkit on Police Information and Intelligence Systems*を参照。

た刑務所インテリジェンスシステムを導入するべきであり、それは保安とインテリジェンスの目的を達成するために、国内法と調和している必要がある。すべての刑務所職員は、保安情報を積極的に収集し、保安部局に情報を提供する責任を有する。このことは、ダイナミック・セキュリティの鍵となる一面であり、質の高い情報を得るつもりならば職員が積極的に従事することと、受刑者とプロフェッショナルな関係性を維持することを必要とする。

刑務所インテリジェンスシステムは、〔すでに〕長年にわたって存在している。確かに、多くの法域で形式化されたのは最近のことに過ぎないが、インテリジェンス活動の基礎的な（および直観的な）アプローチの多くは共通している。例えば、刑務所職員は常に、刑務所内で起こっていることについての手がかりを関連づける共通の脅威を特定することや、特定の受刑者の癖を覚えることに努め、または内部の情報を提供する受刑者と特別な関係を作ることを行っている。このことは、常に純粋に刑務所での好ましい業務と考えられている。

効果的な刑務所インテリジェンスの利益

- 逃走、暴動および騒憂の予防への寄与
- 犯罪活動および刑務所規則違反の特定と予防
- 外部社会での犯罪活動の特定と予防
- 職員の買収と密輸の発見
- 組織犯罪および／またはテロリスト集団と、刑務所制度内でのそれらの活動の特定と、それらのグループにおいて、犯罪活動を主導し、組織する個人の性質の把握
- 様々な組織犯罪グループの影響と刑務所制度における相互関係、刑務所制度の外での影響の評価
- 刑務所制度における傷つきやすさの認識
- 刑務所制度における急進化と過激主義の認識
- 傷つきやすい受刑者および彼らを傷つける者を認識することにより、傷つきやすい受刑者の保護

- 事案の予防と管理における情報に基づいた意思決定の支援

刑務所情報およびインテリジェンスの利用は、過去50年以上にわたって洗練されてきた。かつて、刑務所保安チームの構成員によって管理されるインデックスカードの照合作業に基づいていた刑務所情報システムは発展した。いくつかの法域では、情報技術は、専用の進歩的なソフトウェアと訓練を受けた刑務所職員であるアナリストのスキルを用いる刑務所保安部局に導入された。情報の利用も、より洗練された。インテリジェンスの技術と方法論は、規律秩序に対する脅威を特定し、または進行している活動もしくはハイリスクの受刑者を識別するために発展してきた。多くの法域では、刑務所を基盤とするインテリジェンスシステムは、法執行機関の作業を支援する技術と方法論を再生産している。

定義

インテリジェンスには多くの定義があるが、もっとも良い定義は以下のものである。

利用可能なすべての関連情報の客観的な収集、評価、照合、付加価値分析から得られる予測的で、正確で、関連性のある、時宜を得た仮説。

情報＋分析＝インテリジェンス

この点に関して、刑事司法におけるインテリジェンスも次のように定義できる。

> 将来の活動を予測するために、過去および現在の活動の分析から得られ、脅威的な犯罪集団または犯罪活動の影響を阻止し、または最小化するためにとり得る代替的な行動の実行を提案する成果（またはサービス）。

この定義は、刑事司法におけるインテリジェンスについて、将来の行動を予測する過去および現在の情報の分析という観点から説明している。そのような情報は、

調査主体にとって役に立つ。手がかりを提供し、情報のギャップを明確にすることで調査の質を高める潜在能力を有しているからである。

あらゆる調査手続が努めていることは、チャンスの要素を減らすことである。未来を読む「魔法」のような能力と混同されてはならない。

刑務所内でのインテリジェンスは、以下のように定義され得る。

> 刑務所インテリジェンスの機能は、戦略的かつ操作的に運用される計画された矯正によって、活動に従事させることを計画している組織、または事故が生じる前に刑務所の規律秩序、安全および保安に対する脅威になり得る活動を行うことを計画している受刑者、訪問者、職員および組織を特定することである。

刑務所インテリジェンスは、規律秩序、安全および保安に対する脅威と犯罪活動の両方を特定するために、特定の個人（例えば、受刑者、刑務所の訪問者、刑務所当局によって雇われた職員）と個人が集まった集団（例えば、刑務所のギャング）を注視する。

目的は、管理者が適切な決断を行うことができるように、情報を分析し、不明確性を減じることによって、行動として現れる前に脅威を特定することである。このような事象は、受刑者の逃亡の可能性を示すものであり、その場合、受刑者はより警備が厳重な施設に移送され、分類が変更され、リスクを管理するための追加措置が講じられる。他の例は、面会者による受刑者への薬物の違法売買であり、受刑者は面会禁止（外部交通の制限）の措置が講じられるか、面会者は面会に先立って徹底して検査を受けるべきである。警察と効果的な情報共有を行うとき、警察が面会に先立って面会者を検査し、薬物を所持していれば拘禁をすることが可能である。

刑務所インテリジェンスは、事案の最中や事案後の支援にも利用することができ、インテリジェンスに携わる職員と調査主体との間で最も大きな接点が生まれる

場である。例えば、戦略的なインテリジェンスは、刑務所内での暴動または重大な暴行のような事象に対する迅速な対応を必要とする。事象の種類によって、インテリジェンスは様々な形をとる。例えば、人質事件の場合は、インテリジェンスは以下のことを含む。

(a) 事案インテリジェンス―介入が必要かどうかを確定するための事案についてのあらゆる情報。人質事件の「拠点」(事案の発生場所)、事案の種類、事案に関するすべての情報を含む。

(b) 戦略的な情報―戦略的なチーム（例えば、人質対応グループ）や交渉担当者が選択肢や戦略を計画するために必要な、事案に関連するあらゆる情報。

(c) 人物（または伝記）情報―人質をとった人間、人質、負傷者などの人物に関わるあらゆる情報。この情報は、事案に対応する指揮官が情報に基づいて戦略や選択肢に関する決断を行うことができるように、人格の類型に関するプロファイルを発展させることに用いられる。

インテリジェンスに関連する用語の間の差異に関する適切な理解は、どのように接するかを正しく認識するために重要である（下記の用語と定義を参照)。

良好なインテリジェンスは、リスクに基づく意思決定にも活用することができる。例えば、インテリジェンスは、区分、仮釈放レポート、一時的釈放および最終的な釈放に関する決定のために、行動の証拠を提供することができる。

インテリジェンスに関する共通の用語と定義

情報〔Information〕　生の形式でのデータおよび知識。

インテリジェンス〔Intelligence〕　関連情報の収集、分析、処理から得られる価値を付加された成果で、意思決定者が目標の設定から政策立案まで、より良い情報に基づいた決定を行えるようにするもの。刑務所では、特に、施設の保

安、安全および規律秩序に対する潜在的な脅威に関連した意思決定が問題となる。

刑務所インテリジェンス〔Prison intelligence〕　刑務所職員または法執行官によって利用され得る付加価値を伴う情報。

戦術的インテリジェンス〔Tactical intelligence〕　職員が直接活動を現地の状況に合わせて適用することを支援する。処理されたインテリジェンスは、特定の地域的なリスクに対処するためのリソースの展開を可能にする。

運用インテリジェンス〔Operational intelligence〕　現場管理者〔line manager〕が、運用環境の中で最大の効率を実現するために活動を計画し、リソースを展開することを支援する。

戦略的インテリジェンス〔Strategic intelligence〕　新たに変化する脅威や機会についての洞察を提供することで、政策立案を支援する。これにより、政策立案者は長期的な組織目標を達成するための幅広い戦略を立てることができる。

受動的インテリジェンス〔Passive intelligence〕　収集することを意図せずに定期的に収集された情報

事前対策インテリジェンス〔Proactive intelligence〕　職員が収集することを意図して、計画的に収集された受刑者または状況についての特定の情報

（情報またはインテリジェンスの）分析〔Analysis〕　あるものをその構成要素に分解または分離すること。それらの部分の特定。その背後にある一般原則を発見するためにソースまでさかのぼること。この手続の表または報告書。インテリジェンスの分析とは、簡単に言えば、情報を収集・利用し、評価してインテリジェンスに変換し、情報に基づく意思決定をサポートする成果を作るインテリジェンスを分析することである。効果的に実施されるとき、分析は事実を超える。情報の良し悪し、今まで知らなかったこと、状況を理解するために必要なこと、さらに詳しい情報を得るためにはどこを探せばいいか、状況についての理解を刑務所の同僚や外部の法執行機関にどのように伝えればよいか、を刑務所職員に伝えることができる。

評価〔Evaluation〕　データがインテリジェンスに変換される手段であり、情

報のソースや信頼性によってその文脈に関する情報を検討する、構造化されたプロセスを含む。
インテリジェンス成果物〔Intelligence products〕　情報レポート、情報の請求に応えるためのインテリジェンス・サマリー、ブリーフィング（口頭および文書）、リスクアセスメント、プロファイル（受刑者、刑務所訪問者、グループ、所在）、インテリジェンスアラート、組織図を含む。

インテリジェンスの指針と組織

拘禁中の受刑者について、インテリジェンスの収集の目的は、国が受刑者を「スパイ」したり、基本的人権を侵害したりするためではなく、受刑者が拘禁中に継続して犯罪を行わないようにするためである。刑務所インテリジェンスを発展させることによって、刑務所当局は、職員、受刑者自身、究極的には広くコミュニティのために、拘禁環境をできる限り安全で危険のないものにしようと努めている。

世界中の刑務所当局がインテリジェンスの収集に従事する程度は、非常に様々である。多くの刑務所は、保安部局を有するが、事前の、かつ制度的なインテリジェンスの収集に常に従事しているわけではない。しかし、決断力と機知に富んだ多くの受刑者を統制し、社会の人々やお互いに対するリスクを最小化するために、刑務所の管理者は質の高いインテリジェンスを必要とする。

国家レベルでは、適切な安全策とともに、刑務所情報およびインテリジェンスの管理、収集および利用に関する明確な指針がなければならない。それらは、関連するガイドラインとマニュアルによって支えられる。刑務所インテリジェンスを発展させ、効果的にするために、インテリジェンスの収集が安全な刑務所を運用する不可欠な部分であることが受け入れられなければならない。

国家の刑務所当局は、刑務所間、刑務所と外部の法執行機関との間で、刑務所情報およびインテリジェンスを管理し、受け渡しをするために統合されたシステムを発展させる責任を有するべきである。それは、刑務所インテリジェンスおよび

情報のための国家または中央調整機関の創設に関わる。データの取扱いおよび統合（データの安全性を高めることを含む）のための技術的インフラの改善に責任を持つべきである。加えて、職員が刑務所情報およびインテリジェンスを活用できる技術的設備を整えるべきである（鍵となる刑務所データベースの創設および発展とそれへのアクセスに対するサポートを含む）。

ほとんどすべての刑務所は、いくつかの種類の情報のソースと照合された情報ファイルを有している一方で、それらをどのように結合するかに関する構造化された同一の指針を有している必要がある。どんな統合された刑務所情報およびインテリジェンスの枠組みも、刑務所インテリジェンスの枠組みの効果的な運用に不可欠である。

刑務所インテリジェンスに関する共通の基準は以下の事項をカバーしていなければならない：

- 情報およびインテリジェンスの収集、評価および分析
- 情報およびインテリジェンスの記録およびロギング
- 事前に記録され、ロギングされた情報を分析、利用するためにそれらの情報に当たること
- インテリジェンスの安全性の基準
- レポートおよびブリーフィング

インテリジェンスの収集は、刑務所当局のマネジメントの構造の中に組み込まれていなければならない。優れた取組みは、すべての刑務所でのインテリジェンスの収集を調整するために、刑務所当局の本部を拠点とするユニットを持つことと、それぞれの刑務所で専門の刑務所インテリジェンス・ユニット（PIUs）を創設することである。PIUは、地域のインテリジェンスを管理することに責任を有する一人の刑務所インテリジェンス・オフィサー、またはチームから構成される。PIUは、刑務所保安チームの一部であり、刑務所保安管理者に説明責任を負うべきである。このPIUは、インテリジェンスの評価、照合、普及に責任を負わなければならない。

優れた取組みは、優先事項を設定し、その活動が適法で比例性を満たしていることを保証することによって、PIUの活動を監督する刑務所インテリジェンス管理委員会（PIMB）を設立することである。

刑務所インテリジェンス・ユニットは以下の事項を提供する：

- 様々なインテリジェンスの成果（例えば、保安を脅かすグループ、個々の高リスク犯罪者、不法取引、重大な刑務所事故などに関する）の供給を介した、戦術的、運用的、戦略的なインテリジェンスに関わる事柄の助言
- 事故のない環境を達成することに貢献する他の受刑者へのサポート
- 買収のない職場環境を達成するための、関連する適時の情報
- 特定のターゲットに向けた活動を行うための関連情報を持つ主要なセキュリティエリア
- インテリジェンスに関連するテーマについて、すべての職員を対象とする研修
- 刑務所当局および他の法執行機関へのインテリジェンスの成果の提供と調査援助

刑務所情報およびインテリジェンス（特に職員の買収に関して）のセンシティブな性質のために、そのエリアで働くために選抜された者は、他の刑務所の役割におけるよりも、誠実さにおいて、より高い水準の資格を必要とする。インテリジェンス・ユニットにおける職員の業務は、時折、職員のバックグラウンドを調査し、彼らが引き起こし得るリスクを評価する高度な保安審査の対象とされる。

刑務所インテリジェンスの専門家職員のプロフェッショナルな展開は（特に分析スタッフの技術とインテリジェンスの管理者に関して）、刑務所職員の研修施設にとって鍵となる役割である。PIUの職員のみが研修を受けるのではなく、すべての刑務所職員が研修を受け、インテリジェンス収集手続への寄与において、その責任が周知されなければならない。

効果的な刑務所インテリジェンスの体制を構築することが実効性のある仕組みで

あることは疑いないが、長期的には、優れたインテリジェンスにより、限られたリソースを最も必要とされる場所に集中させることができる。

刑務所インテリジェンス機能にとって不可欠な要求

- *人びと*：職員は最も効果的な場所で採用され、選抜され、配置されなければならない。
- *組織*：刑務所インテリジェンス・ユニット（PIU）は、発展され、優先事項と計画を柔軟に変更できなければならない。
- *供給*：PIUには、最先端の技術、インフラ、設備が適切に投入されなければならない。
- *研修*：用意される研修プログラムは、選抜された職員をPIUと刑務所の両方で訓練するために、PIUの中になければならない。
- *機器*：これは、スキャナー、デジタルカメラ、コミュニケーション機器、携帯電話リーダーなど、PIUの機能のための機器の購入に直接的に関わる。
- *教義*：これは、PIU運用のための指針となる原則であり、手続きを運用する基準、PIU内外の定められた指揮系統を含む。

効果的な安全策を組み込むこと

刑務所の情報やインテリジェンスは、刑務所の職員が保有できる情報の種類、保有目的、取り扱い方法を規定する法律によって大きく制限されることがある。

刑務所のシステムを含む政府のデータベースの内容を第三者が知ることを完全に妨げる法律があるかもしれないし、反対にかなりのアクセスを可能にする情報自由法があるかもしれない。しかし、情報の管理に対する文化的な選好や、業務上の理由（例えば、対象者が疑われていることを誰かに知らせたくない）などにより、その情報に特に関与している人以外には広められない情報が常にある程度存在する。

刑務所の情報およびインテリジェンスの中には、センシティブなものもあり、また、それを収集するために侵入的な技術が使用されることもあるため、設置された監視機構やセキュリティ対策が特に重要となる場合がある。これらは通常、法律ま

たは実務および手続の規則に含まれている。例えば、欧州刑事施設規則24条を参照。

【欧州刑事施設規則24条２項・３項（割愛）。国連被拘禁者処遇最低基準規則（ネルソン・マンデラ・ルールズ）の、法的助言者および刑務所査察官などの特定の人物との私的で完全な秘密交通権に関する61条１項および84条１項も参照】

モニタリングは、特定の外部交通の形態によってもたらされる脅威に比例したものでなければならず、外部交通を制限する間接的な方法として用いてはならない。

欧州人権裁判所は、受刑者の信書の発受を無差別かつ日常的にチェックすることは、欧州人権条約８条14項に違反するとしている。
Jankauskas v. Lithuania [2005], European Court of Human Rights, 59304/00.

どの国にも、センシティブな、または秘匿性が高いと考えられる「機密情報」と呼ばれる重要な情報がある。これは通常、「機密」や「秘密」などのラベルを付けて「保護的に表示」される。これらの見出しに分類された情報は、特別な取り扱い制限が設定され、適切なレベルの許可を受けた人にのみアクセスが許される。

特別な取り扱いの制限は、誰が機密情報を見ることができるかだけでなく、どのような条件で見ることができるか、どのような媒体に保存することができるか、どのように送信することができるか、どのように破棄しなければならないかについても定義することができる。

多機関によるアプローチ

刑務所インテリジェンスは、より広範な法執行機関のインテリジェンスシステムの一部であるべきだということを忘れてはならない。交換される情報の量と質、そして請求に対する回答の速さが、協力のレベルを示している。刑務所インテリジェンスは、刑務所の外での法執行活動に不可欠な場合がある。同様に、外部の法執行機関からのインテリジェンスは、刑務所内で何が起こっているかを理解する上で非

常に重要となる。近年、他の法執行機関による刑務所発のインテリジェンスの使用に関して、いくつかの重要な進展があった。

刑務所とインテリジェンス・ユニットは独立して存在しているわけではない。犯罪者は通常、警察による捜査と裁判所による裁判を経て初めて刑務所に収容される。犯罪者が刑務所に入った時点で、警察、司法、ソーシャルサービス、その他の機関がその者について、すでに保有している豊富な情報がある。この時点で、刑務所のインテリジェンス・ユニットが、犯罪者に関するすべての利用可能なインテリジェンスを収集し、その者に関する犯罪者プロファイルを作成することが不可欠である。これを効果的に行うためには、刑務所のインテリジェンス・ユニットと警察の担当者との間に良好な協力関係があることが不可欠である。ほとんどの警察機関には、受刑者関連のインテリジェンスを収集・処理するインテリジェンス部門がある。

刑務所と警察のインテリジェンス・ユニットの関係は、しばしば無視されたり、軽視されたりするものの、それは、国家が受刑者を管理し、拘禁中や出所後に社会復帰させようとするならば、不可欠なものである。この基本的な関係は、各組織内に単一の連絡先を設け、警察官を刑務所ユニットに、または刑務官を警察ユニットに配置することで、確立・維持することができる。先進的な構造では、一部の警察組織は、刑務所のインテリジェンス・ユニットの活動を反映し、強化し、支援するために、専用の共同インテリジェンス・ユニットを維持している。共同インテリジェンス・ユニットの詳細については、後述の章を参照のこと。

刑務所当局の目的は、受刑者を社会復帰させることであるべきである。社会サービスと保護観察サービスは、このプロセスに不可欠であり、特に受刑者の地域社会への釈放を管理する際には、インテリジェンス・ユニットと良好な協働関係を築く必要がある。

他の法執行機関による刑務所発のインテリジェンスの利用

- 適時かつ実用的な刑務所インテリジェンスは、重大な犯罪や組織的な犯罪、特

にそれが国境を越えた性質のものである場合、その防止、削減、捜査に大きな影響を与える。(「適時」とは、適切な時期に提供されることを意味し、「実用的」とは、その詳細と信頼性が行動を起こすことを支援することを意味する)。

- 刑務所インテリジェンスは、あらゆる形態の犯罪の防止、削減、発見において、リソースの方向付けと優先順位の設定に重要な役割を果たす。
- 刑務所インテリジェンスは、しばしば「情報化された警察活動」と呼ばれる効果的な警察活動モデルに貢献することができる。このモデルでは、情報は戦略的な方向性を示すのに不可欠であり、地域警察や日常的なパトロールを含むあらゆる形態の戦術的な警察活動に職員を配置する際の中心となる。

優れた取組みは、情報およびインテリジェンスを交換するための合意された取り決めを文書（例えば、覚書、プロトコル、合意書など）に記載することである。保有する情報およびインテリジェンスが断片的で重複してしまう危険性がある。強力な情報交換のメカニズムは、このような事態を軽減するのに役立つ。

電話の傍受や盗聴器など、技術的な監視を行うための設備は、国家の保安機関に集中していることがある。このような場合には、リソースを共有するために機関間の良好な協力関係が重要である。

刑務所に常駐する警察インテリジェンス・オフィサー

いくつかの法域では、警察（国、連邦、地方）が刑務所に多数の警察官を配置している。これらの警察官は、刑務所インテリジェンスの収集を管理する責任がある。警察官は、所属する刑務所に関連するすべての警察活動の唯一の窓口となり、インテリジェンスや証拠に関連して法執行機関から受けた要請を調査する。これらの警察官はまた、刑務所の保安部局と連絡を取り、アドバイスを受けたり、許可を手配したり、受刑者関連情報へのアクセスを容易にしたりする。

刑務所に常駐する警察連絡オフィサーは以下の事項を提供する：

- 受刑者の刑執行計画、移送、釈放情報

- 提携関係、緊張関係、継続的な活動、将来的な意図など、現在および今後の組織犯罪ネットワークおよび個人に関する最新情報
- 対象者のプロファイル作成をサポートするためのインテリジェンス収集
- 刑務所内での任務報告ミーティングの後方支援および計画支援
- 刑務所インテリジェンスの成果の利用に関する指導
- 受刑者を裁判所や他の刑務所に移送する際の、表向きおよび裏向きの戦術的アドバイスとサポート
- 暴力的過激派の受刑者、保護された証人、逃亡のリスクが高い受刑者、多機関による公的保護の手配が必要な受刑者など、特別な重要性を有する受刑者グループに関する情報へのアクセス

秘密裏に行われる監視

秘密裏に行われる監視は、情報収集のための特に侵入的な方法である。秘密裏に行われる監視措置の使用には、受刑者のプライバシーの権利と、重大な犯罪性を調査する必要性とのバランスを慎重に考慮する必要がある。

秘密裏に行われる監視

当局が住民を強制的にコントロールする社会では、これらの技術の使用は無差別に行われる可能性がある。他のシステムでは、犯罪が重大であること、技術の使用が事件に不可欠であること、重要な証拠がより侵入的でない方法では確保できないことなど、濫用に対するいくつかの厳しい保護措置が必要となる。司法または独立機関による監視が一般的であり、国際人権法でも要求されている。

UNODC—Policing: Crime Investigation, Criminal Justice Assessment Toolkit, 2006, p. 13.

秘密裏の監視に関する規定は、受刑者の権利を十分に考慮したものでなければならない。秘密裏の監視の許容性とこれらの措置の限界については、国際的な人権団体や裁判所で様々な決定がなされている。濫用に対するいくつかの厳しい保護措置が必要である。司法または独立機関による承認と監視が一般的であり、国際人権法

の下で要求されている。

事例―イギリス

2000年に施行されたRIPA（Regulation of Investigatory Powers Act）は、刑務所に秘密裏の監視を行う権限を与えるものである。この法律と関連する施行規則は、秘密裏の監視の使用と刑務所内での適用のための枠組みを提供している。

- すべての刑務所は、犯罪や重大犯罪の防止・発見、混乱の防止、または公共の安全のために必要かつ適切な場合、秘密裏の監視の使用を要求することができる。
- すべての刑務所では、秘密裏の監視が法律に基づいて行われることを保証するために、訓練を受けたスタッフが重要な役割を担っている。
- 刑務所内のインテリジェンス収集システムには、秘密裏に行われる監視の使用が不可欠である。
- 秘密裏の監視は、刑務所内のコントロールを維持し、管理者が情報に基づいた決定を下すのに役立つ。
- 刑務所全体でRIPAを遵守し、これを毎年、監視委員会（OSC）が確認する。

受刑者の単独室を秘密裏に監視すること（侵入型監視）は、適切な司法機関または行政機関によって許可されなければならない。単独室内での人質事件に対応するためであれば、監視は刑務所当局の管理者によって承認されるべきである。公共の場での秘密裏の監視（指示された監視）は、刑務所当局のレベルで許可されるべきである。警察や他の調査機関による刑務所内での秘密裏の監視の計画的な使用は、運用を開始する前に、まず刑務所当局によって検討されなければならない。すべての秘密裏の監視は、すべて文書で記録されなければならない。

刑務所環境で展開される秘密裏の監視技術

- 電話の録音
- 郵便物／メールの検閲
- 聴取機器の使用

- 追跡機器の使用
- 専門の監視チームの利用
- 写真による監視の活用
- ビデオ監視の活用
- 手紙、パッケージ、小包の秘密裏の検査
- 位置情報追跡機器の使用

視聴覚による監視は、受刑者の弁護士との面会の秘密や職業上の秘密、あるいは検診時のプライバシーの権利を侵害するために用いられてはならない。ビデオ監視、特にビデオ録画には、映像の保存やアクセスを含めた保護措置を講じるべきである。

視聴覚による監視の使用は、汚職や不正操作を防止・発見するためのスタッフの監視にも拡張することができる。適切な安全策とコントロールが常に導入されるべきである。

受刑者である情報提供者の利用

情報収集のために情報提供者や人的情報源を利用することは古くから行われている。情報提供者は、刑務所の管理者が他の方法では得られない情報を提供することができるが、刑務所内での情報提供者の利用は、情報提供者にとって特に危険であり、また虐待を受ける可能性もある。情報提供者には様々な動機がある。彼らは、報酬（金銭や早期釈放）を求める受刑者である場合もあれば、反対派を追放しようとする常習犯罪者である場合もある。情報は、個人的な利益（刑務所での特別な仕事、追加の特権、一時的な釈放、早期釈放）のための交渉材料として提供されることもあれば、現金と交換されることもある。すべての受刑者が良い情報提供者になるわけではなく、その動機が疑わしい場合もある。

情報提供者の扱いは秘匿されることを要し、特権や金銭を受け取ることもあるため、悪用される可能性が非常に高い。一般的には、情報提供者から提供された情報の信頼性と出所を慎重に評価し、可能であれば裏付けを取って、その正確性と妥当

性を「評価」する必要がある。刑務所の情報提供者が情報を提供するたびに、職員はその動機を質問し、情報を記録するべきである。受刑者である情報提供者の信頼性を評価するための一連のガイドラインは、良好な管理を促進するのに役立つ。同時に、刑務所当局は、情報提供者に配慮する義務があり、報復から保護しなければならないことも認識しなければならない。

受刑者である情報提供者を利用するときに求められる安全策

- どのように管理されるべきか
- 情報提供者との対話および報告のルール
- 安全な場所に保管された機密ファイルへの情報の記録（名前の代わりにコードナンバーを割り当てる、ディレクターのオフィスの金庫に保管するなど）
- 情報提供者の個人情報は、情報提供者に対応する者のみが知ることができるようにすること（情報提供者の取り扱いを監督する責任を持つ上級職員を任命するなど）
- 情報提供者の利用に関する特別なトレーニングの提供
- 情報提供者を管理することを許可された刑務所職員を指定すること
- 情報提供者への報奨制度と手続

人的情報源から収集したすべての情報は、現行の国内法に基づいて認可され、持ち出されるべきである。すべての情報源には取扱担当者が存在し、取扱担当者は管理者に報告する必要がある。管理者はシステム管理者に報告し、システム管理者はすべての情報源が登録されていることを確認する必要がある。

鍵となる原則

- インテリジェンスは、刑務所の保安とより広いコミュニティに対するリスクの予防と発見のための活動に役立つ。
- 戦略的インテリジェンスおよび運用インテリジェンスを適切に開発、評価、発信する。
- インテリジェンス評価は、地域の安全上の優先事項や目的を特定し、リスク

管理に役立てる。
- 職員は、保安、プロフェッショナル、個人的な基準が求められていることを認識する。
- 保安インテリジェンスは買収の防止に寄与する。
- 現場で入手した、あるいは他の施設や機関から受け取った情報は、記録、保存、アクセス、および合法的に処理され、すべての者にとって公平な取扱いが保障される。
- 外部交通差し止めの結果として得られたインテリジェンスは、合法的かつ適切に共有される。
- 保安記録は、受け取り／保有刑務所の必要に応じて作成、更新される。
- 保安情報やインテリジェンスは、安全かつ合法的に、そして適時に受け入れ先の刑務所に転送される。
- 外部交通の差し止めと、入手した資料を保持し、普及させることは適法である。
- 保安上のインテリジェンスを目的とした受刑者の郵便物の差し止めや電話の傍受は許可されており、それがもたらす脅威に比例している。
- 指示された、侵入的な秘密裏の監視は、常に許可を要し、管理され、記録される。
- 秘密裏の人的情報源（情報提供者）の利用は、許可を要し、安全に管理され、記録される。
- 情報提供者や監視によって得られた情報は、特定の利害関係者と安全に共有される。

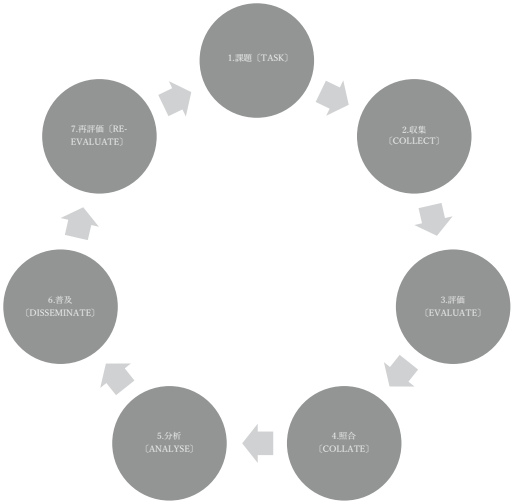
第４章　刑務所インテリジェンス：サイクル、手続、構成要素

インテリジェンスとは、情報に「何か」が加えられたものである。この「何か」とは、インテリジェンス手続〔process〕である。インテリジェンス手続は、偶然の要素を減少させる。それは未来を予言する「魔法」のような力と混同するべきではなく、単なる助言に過ぎない。それは情報を解釈して意味を与えるということである。もっとも単純に言えば、インテリジェンスとは、処理された情報〔processed

information〕と言うことができるかもしれない。刑務所や法執行の文脈では、インテリジェンスとは処理、つまり取得、利用および保護された情報と言うことができる。それは刑務所の規律秩序と保安に対する脅威を予防／排除するために、犯罪捜査もしくは懲罰調査、または職員による介入を、決定し、支援するものである。

忘れてはならないのは、インテリジェンス手続の一部として分析された情報を扱う際、その証明責任と、多くの法域の刑事裁判で要求される立証責任は異なるということである。インテリジェンスを扱う者が留意しなければならないのは、さらなる事実によって決定的な証明がなされない限り、あるいはそれまでは、インテリジェンス手続によって到達した結論は、その作成者の側の仮定であるということである。

インテリジェンス手続は、一連の機能によって構成されており、これらの機能を総合することで、生の情報を検証し、それに広範な意味を与える。この一連の機能とは、課題設定、収集、評価、照合、分析、普及および再評価である。こうした一連の機能は、インテリジェンス・サイクルとも呼ばれ、これによって生の情報が、政策決定に利用可能で有用なインテリジェンスへと変換される。



インテリジェンス・サイクル

課題設定（方針設定としても知られる）

インテリジェンス・サイクルの最初の段階では、課題設定と方向づけが行われる。インテリジェンス分析は、分析成果の消費者、つまりこの場合は刑務所当局のニーズに応じて行われる。したがって分析作業は、サイクルのこの段階でイニシアチブをとる刑務所管理者による課題設定を通じて、方向づけが行われる。そうとは言え、パートナーシップという原則からは、分析成果への要求が消費者と提供者によって明確に定義、了解されるように、両者が協働することに対する責任の共有が求められる。

その結果、課題設定（方針設定）には、刑務所当局の情報ニーズの定式化と優先順位の決定、人員とリソースの特定と組織化、収集プランの策定、そして多様な刑務所運営者とインテリジェンス職員への業務の割り当てを行うことが含まれる。刑務所当局は、その全ての施設において、情報収集のための包括的な課題設定と調整手続を有しなければならない。同様に、保安やインテリジェンスに関わる事項を所

掌する上級職員が任命されなければならない。この職員は、各刑務所のインテリジェンス管理委員会の長と、警察および保護観察所の代表者を含む、小委員会を創設する必要がある。この小委員会は、部局全体と個々の刑務所に対する保安およびインテリジェンスの戦略的な優先順位に承認を与える。

同様に刑務所当局は、受刑者および刑務所に接触を図った全ての人が、保安に関連する情報および懸念事項について報告する「任務〔tasked〕」を負うことを明確にしなければならない。

保安部局が必要とする情報

ほとんどの刑務所システムは類似の必要性を有しており、職員に以下の事項に関連するインテリジェンスを収集する権限を与えることになる。

- 逃走計画
- 組織的なギャング関連活動
- 麻薬取引
- 職員または他の受刑者に対する計画的な攻撃
- 携帯電話およびインターネットを用いた不正な連絡
- 急進化および暴力的過激派の活動
- ぜい弱な受刑者に対するいじめ
- 刑務所の安全と保安、秩序ならびに管理へのリスク

加えて、刑務所の中には、個別の特殊な必要性を有する施設があることもある。いくつかの国では、性犯罪者は分離された刑務所または区画に収容されており、刑務所にいる間、不正な連絡を使って犯罪を継続することのないよう、性犯罪者に注意する必要があるかもしれない。テロリストの受刑者が多くいる施設では、必然的に急進化や過激派的なふるまいに大きな注意を払うことになるだろう。

保安とインテリジェンスの優先順位が設定されると、保安とインテリジェンス小委員会は、刑務所インテリジェンス・ユニット／共同インテリジェンス・ユニット

および職員にそのことを通知する。その結果、全員が目的を明確にし、合法的かつ相応の権限を持つようになる。

収集

インテリジェンス手続とは、結局は情報収集と同義である。情報収集とは、指示的かつ集中的な情報の取得であり、公然または秘密裏の手段を使ってあらゆる可能なリソースから行われる。そこには、刑務所のデータベース、裁判資料、ならびに職員、受刑者および第三者（例えば、法執行機関）からの情報、保安部門、調査官および護送部門など他の刑務所部門、カメラの映像、検査の結果、メディアおよびソーシャル・ネットワークならびにインテリジェンス部門が合法的にアクセス可能な他の情報源が含まれうる。

情報収集における刑務所職員の重要性

刑務所という環境は、主要な対象が収監されているので、ある意味では基本的なインテリジェンスの収集に適している。刑務所という文脈の中では、情報収集は何よりもまず刑務所の職員を通じて行われる。刑務所職員は、受刑者と日常的に接触し、事故〔incidents〕の際に一番に対処する者であるから、刑務所インテリジェンスにとってもっとも重要な（そしてしばしばもっとも活用されていない）情報源である。職員は受刑者から何か言われることや、何かを見つけること、何かを聞いたり読んだりすることがあるかもしれない。刑務所インテリジェンスという考え方が発達すればするほど、こうした職員から提供される情報とインテリジェンスの量は増大する。第２章で論じたように、ダイナミック・セキュリティの主要な利点の一つは、刑務所の職員が日常的活動の中で、受刑者から情報を集めることができるという点にある。すべての刑務所職員は、警戒と注意を怠らず、その指揮系統を通じて、またはインテリジェンス担当者に、情報を報告しなければならない。それにより、継続的なインテリジェンス・サイクルの中で、情報を検討することが可能となる。

情報収集における刑務所職員の役割

刑務所職員は、常に警戒を怠らず、異常な事態を報告し、そして受刑者との間に尊敬と信頼に裏打ちされたプロフェッショナルな仕事上の関係を築くことを通じて情報を収集する。例えば、

- 会話を立ち聞きする
- 受刑者がしていることを見る
- 受刑者が誰と話しているのか、つまり人間関係のパターンを観察する
- ふるまいやよくする行動のパターンに注意する
- 異常な行動または問題行動の予兆を特定する
- 物理的な変化に留意する（視線上に障害物を置くことで、見通しが悪くなる）
- 電話および手紙を監視する
- 検査中の保有している物品や衣服の観察
- 普通ではない要求または事故

情報を収集した職員は、インテリジェンス・システムに追加するため、関連の保安情報報告書、または代わりの文書を提出しなければならず、保安チームのメンバーによって、情報源の評価が行われる。

外部の法執行機関、政府機関、非政府組織（例えば、慈善援助団体）または受刑者の家族もしくは友人から情報が提供される可能性もある。潜在的な情報源は、ほぼ無限にある。利用可能な情報源は、実務家の一般的および局所的な知識と、時間をかけて築き上げられ、維持されてきたつながりにかかっている。

刑務所環境での収集の領域

刑務所という環境では、受刑者に関する情報収集には主要な 4 つ領域がある。すなわち、名籍データ、面会者データ、連絡データおよび保安行動データである。

*名籍データ－*有罪判決を言い渡される、または刑務所に戻されるまでに、たいていの場合その人物は、すでに警察および司法手続を経験している。これは基本的な

生物学的データと背景のチェックがすでに済んでいることを意味するだろう。そこには、受刑者の写真、指紋、DNA、誕生日、パスポートまたは身分証、傷痕およびタトゥー、現住所、家族の氏名、関係者の氏名、ギャングまたは集団への加入、ならびに電話およびＥメールによる接触の詳細などが含まれることがありうる。刑務所システムに受刑者が編入されると直ちに、その者の個人名籍ファイルが開設され、そこには上記のデータが可能な限り多く含まれなければならない[(17)]。保安上のリスクまたは行動に関する情報またはインテリジェンスを記録することができる追加の保安ファイルが、各受刑者について存在していることは、優れた取り組みである。これは紙媒体または電子システムであるかどうかに関わらず、別のファイルまたはフォルダーに保管されなければならない。

面会者データ－ほとんどの受刑者は、家族、友人および関係者からの面会を受けるだろう。面会者の中には、刑務所の規律秩序や保安の潜在的な脅威となる者もいる。なぜなら、面会者によって、禁制品の持ち込み、受刑者の逃走や証人への脅迫の援助、証拠の隠滅あるいは別のやり方による裁判の進行阻害が行われうるからである。そうであるので、面会者は受刑者との面会が認められる前に、注意深く管理され、審査される必要がある。法域のインフラが許せば、すべての面会者に受刑者との関係を記載した申込書の提出を要求し、そして面会が許可される前に、面会者が身分証明書の原本と確認済みの住所を提示することは、優れた取り組みである。各面会の日時も記録されなければならない。

連絡データ－刑務所の規律秩序を維持し、受刑者による犯罪や拘禁からの逃走を防ぐためには、受刑者間の内部的な連絡と同様に、受刑者と刑務所外の接触者との間の外部的な連絡も監視することが不可欠である。かつては受刑者の連絡の主たる方法は固定電話または手紙であり、それらの監視は刑務所当局にとって比較的容易であった。しかしながら、携帯電話の利用が急速に拡大し、その多くがインターネットに接続可能となって以来、世界中の刑事施設が、受刑者による家族との連絡、

(17)　受刑者が刑務所に到着した際に収集すべき情報の詳細な説明については、*UNODC Handbook on Prisoner File Management* (2008)を参照のこと。

また場合によっては犯罪関係者との連絡を統制するために努力してきた。携帯電話（および他の不正物品）が施設に密かに持ち込まれることを防ぐために、受刑者、面会者および刑務所職員に対する厳格な検査体制をとることによって、刑務所はようやく受刑者の連絡を管理し始めたところである。リソースと技術が許すところであれば、携帯電話「ブロッカー」の使用または携帯電話サービス・プロバイダーの協力により、刑務所内で使われる不正な携帯電話の切断が検討されるべきである。そのような措置がとられない限り、刑務所の中から携帯電話を使って、証人への脅迫、違法薬物取引、さらには殺人といった犯罪行為を試みる受刑者がいることを示す証拠は多数ある。また携帯電話は、逃走、暴動および人質行為の計画にも使われうる。不正な携帯電話が押収された場合には、通話への適切な対処と分析が捜査官を支援し、犯罪を防ぐかもしれない。第１章（21頁〔前号200頁－訳者注〕）では、外部交通と監視の問題、そして安全策についてより詳細な議論が行われている。

保安行動データ－前線にいる刑務所の各職員は、保安に影響を与える可能性のある受刑者の行動をすべて観察し、報告するよう訓練されていなければならない。任務中、刑務所職員はギャング集団とそのヒエラルキーを特定する立場に置かれるだろう。職員は、どの受刑者が日常的に武器もしくは薬物、または他の不正物品を所持しているのかを知ることになる。もっとも重要なことに、職員は規則から外れた個人または集団の行動を識別できるようになる。こうした行動は保安インテリジェンス報告書（62頁以下の保安情報報告書のセクション〔本号「保安情報報告書」－訳者注〕およびより詳細は付録１〔未翻訳－訳者注〕を参照）または同様の様式で報告されなければならない。それにより、情報を公式に記録、査定および共有することができる。

情報収集計画の立案

刑務所インテリジェンス部門が新たな問題または特定の受刑者もしくは受刑者集団について追加の情報を要する事態も生じるであろう。情報収集は、時間を要する手続である。情報の収集に費やされる時間の総量は、収集手続が始まる前の入念な計画立案によって、最小化し、そして効果的に管理することができる。情報収集手

続のための計画を立てることによって、探索する情報のタイプと分量に対して、組織的かつ最終的な焦点、境界および限界が与えられる。また計画では、コストとリスクに関する情報が提供され、そして潜在的な情報源と収集された情報の使途の概略が示される。

情報収集計画の利益

- 焦点が絞られた情報収集の方法論が提示される
- 収集する情報の総量が定義される
- 無関係の情報収集に費やされる時間が最小化される
- 情報源となるべき場所と人の概略が示される
- 情報収集の責任者が任命される

情報収集計画は訓練された手続であり、これがインテリジェンス成果物〔product〕の発展に必要な情報を得るために、適切な情報源が用いられることを保証にする。計画は、何が要求される情報であり、それを得る責任があるのは誰かを明確に特定することによって、整理され、焦点が絞られた調査を容易にすることができる。

調査の方法

インテリジェンス実務家が利用できる潜在的な調査の方法〔avenues of inquiry〕は、ほぼ無限にある。調査の中には、政策指針によって規制されたものもあれば、長年にわたって築き上げられ、維持されてきたネットワークに依存することになるものもある。利用可能な情報源は、個々のインテリジェンス実務家の個人的な創意工夫に依るところが大きい。

調査の方法は、必要とされる情報を見極め、それを最短の時間で、どこから、どうやって得るのかを把握するための技術に過ぎない。この知識と能力は調査を単純化し、刑務所における犯罪または他の事故を防ぐ手助けとなることができる。これは科学ではなく、インテリジェンス実務家の個人的な知識と人生経験に単純に依拠

する。

調査の方法の幅は、取り組まれている調査の性質に大きく依存することになる。調査の性質は（a）公然の調査と（b）秘密裏の調査に分けられる（違いは、被疑者または被調査者が保安部局の関心に気づいているかどうかを、調査者が配慮するか否かにある）。刑務所環境における秘密裏の監視の問題については、第３章において論じられた。

保安情報報告書

情報が適切に記録されれば、それは極めて価値のあるものとなり得る。情報は正確に記録されていなければ、それが忘れ去られ、誤用され、あるいは誇張されることで、利益以上の害を生み出す可能性がある。この場合の優れた取り組みは、刑務所職員が収集された情報を提出できる標準化された様式があることである。これは保安情報報告書または単に情報報告書と呼ばれることもある。

報告書には、第三者が将来利用するかもしれない情報が含まれるので、不十分な表現や不完全な情報によって未来の読者が誤った結論を導くことができないように、その作成には十分な配慮がなされなければならない。正確性を担保する最善の手段は、どの情報が、どこで、いつ、そしてどのような状況で得られたのかについて、詳細に記述しておくことである。報告書を作成する職員も、結論へと至るステップを収録しなければならない。

情報源の機密保持に対しても、十分な配慮がなされなければならい。たいていの場合、良き情報源は極めてまれである。守秘義務に背くことは、さらなる情報の提供を情報源から拒否される結果になり得るし、最悪の場合、情報源を将来的な危害のリスクにさらすことにもなりかねない。情報を評価するためには、保安部局は情報源の身元を知っていなければならないが、情報を提供した受刑者の身元を知る必要のない職員に明かすことのないように、十分な注意が払われなければならない（公開の情報源である場合はこの限りではない。受刑者情報の利用については54頁

のセクション〔本号「受刑者情報の利用」－訳者注〕）を参照のこと。

情報報告書の内容に基づいて行動する責任は、通常は作成者以外の人物にかかってくることになるので、報告書は提出や配布の前に、可能な限り完成した状態となっていることが重要である。保安情報報告書は、その名が示唆するように、情報の源であり、したがってインテリジェンス手続の起点となるものである。

とりわけ刑務所という環境では、インテリジェンス実務家は、部門〔units〕および部局〔departments〕またはそのいずれかの最前線にいるメンバーによる情報報告書の提出を、あらゆる機会を使って促すべきである。

あらゆる情報は、調査またはインテリジェンスへの利用可能性を有している。保安部局がさまざまな情報というパズルのピースをつなぎ合わせて初めて、その意味が理解可能となり、現実の価値が知られるようになる。各自が普通ではない、あるいは規格外と感じたことは提示されなければならず、保安部局がそれを記録し、価値があるのかを判断することになるだろう。

何らかの情報源からハード・コピーの形で提出された情報は、保安情報報告書に転記されなければならない。保安情報報告書とすべての文書には、保安区分が指定されなければならない。刑務所当局の管轄から外れる文書を受け取った場合、可能な限り迅速に、当該文書は適切な機関に転送されなければならない。

推奨されている保安情報報告書のフォーマットおよび保安情報報告書を補完するガイドラインは付録１〔未翻訳－訳者注〕に収録されている。

効果的な情報収集の試金石〔key tests〕

- 刑務所職員は、日常のルーティンとして、インテリジェンス・ログを（紙または電子媒体によって）提出できるか？
- 職員は、それをすることを推奨されているか？

- 刑務所職員による情報およびインテリジェンスの提供に関する、何らかの達成尺度〔performance measure〕があるか？
- 情報とインテリジェンスの記録に関する共通の国家基準があるか？
- 共通のフォーマットと専門用語が使用されているか？
- 刑務所の情報およびインテリジェンスを収集し、展開するために配置された専門的な刑務所職員のネットワークがあるか？もしそうであれば、どのくらいあるか？その業務の説明はどのようにされているか？それはどのように運営されているか？
- 刑務所内で事故が起きた後に、どのような教訓が得られたかについて、職員は公式に事情を聴取〔debriefed〕されているか？その情報は、情報またはインテリジェンスとして伝達されているか？それはどのように、誰に対して行われているか？

評価

評価には、情報源の信頼性および情報の質を査定することが含まれる。すべての情報は、情報源の信頼性と情報の正確性を評価するための検証を受けなければならない。情報の受領の際に、特別な訓練を受けた刑務所職員のメンバーが、その評価を行わなければならない。提供後に情報を監督し、品質を保証する適切な手続がなければならない。今後の評価を改善させたければ、情報を集めた職員のメンバーと評価者に対するフィードバックは重要である。

提供されたすべての情報またはインテリジェンスは、*(a)* これまでの情報源に対する信頼性の歴史と、*(b)* 情報源がその提供する情報を直接的に知っている程度（例えば、情報源が直接得た情報なのか、あるいは本人が他の誰かから聞いたことなのか？）、に基づいて評価されることによって、優れた取り組みは発展してきた。

情報の評価のために使用されているシステムにはさまざまなものがあるが、本質的にはその発想は同じである。つまり、情報源の信頼性の見積もりと、現に提供さ

れた情報の正確性の見積もりを提供することである。

海軍本部コード〔Admiralty Code〕として知られる国際的に用いられる公式は、こうした査定に対して、英語と数字を組み合わせた評価を与えるために設計されている。このコードの構成要素は、高い蓋然性〔high probability〕からほぼ誤り〔probable inaccuracy〕までの間で測定する段階的なスケールを表している。アセスメントをすることが状況的に不可能な場合には、追加のコードが含まれる。各構成要素は慎重にかつ互いに独立して検討されなければならない。

海軍本部コード	
A．完全に信頼できる 〔Completely reliable〕	1．裏づけのある報告 〔Report confirmed〕
B．通常は信頼できる 〔Usually reliable〕	2．ほぼ真実の報告 〔Probably true report〕
C．いくらか信頼できる 〔Fairly reliable〕	3．真実の可能性がある報告 〔Possibly true report〕
D．通常は信頼できない 〔Not Usually reliable〕	4．真実か疑わしい報告 〔Doubtful true report〕
E．信頼できない〔Unreliable〕	5．ありえない報告 〔Improbable report〕
F．信頼性は不明 〔Reliability unknown〕	6．真実か判断できない 〔Truth cannot be judged〕

情報源の信頼性 − 情報源の性格の検証は、提供された情報に設定される信頼性のレベルを査定するために、以下の事項を考慮して行われる。

- 近接性 − 情報源が情報の対象に対してどのくらい近いのか。すなわち、情報源は知ることのできる立場にあったのか？
- 知覚の限界 − 聴覚、視覚、発見および分類において、人間および機械的な観察者は、双方ともに限界を有している。
- 疲労 − 疲れているとき、個々人はさまざまな反応をする。それはアルコールや薬物の摂取の結果かもしれない。情報源が身体的または精神的な消耗により、

疲労、ストレスまたは苦痛を感じていることもありうる。

- バイアス－バイアスがない情報源は、普通というより例外である。個々人は、以前の体験、考え方、利己心、願望および能力によって、バイアスのかかった態度をとるかもしれない。バイアスは意識的であることもあれば、無意識の場合もあるかもしれない。
- 知識と経験－情報源が当該情報に関連する専門的な知識または経験を有している場合、その特定の文脈において、その人物は信頼できると見なされる。
- 過去の実績－その情報源が過去に情報を提供したことがある場合、それはどの程度正確だったのか？もし正確でない、あるいは間違っていた場合、どのような状況だったのか？

情報の正確性―最初の判断では、その情報が事実と称されているのか、意見またはうわさと称されているのかどうかを特定しなければならない。

情報の完全性―情報報告書の内容は、可能な限り、作成者がそれを編集したままの状態でなければならない。しかしながら、時間が経つにつれて、あいまいさや意図しない結論を取り除くために、そして秘匿された情報源を特定したり、他の方法で調査を妨げるような情報を排除するために、文章の一部を書き換える必要が出てくることもありうる。

この評価に関連して、配布の許可範囲を制限するために、「取り扱い〔handling〕」または「普及〔dissemination〕」コードが加えられることがありうる。これは情報またはインテリジェンスを、権限のない者による開示から保護することを意図している。

照合

評価に続いて、紙または電子媒体で受領されたすべての記録とログは、分析に備えて、照合、ファイル化、相互参照および整理されなければならない。照合は、収集されたデータを、検索と分析が可能なフォーマットに編集することを意味する。

照合では、内容を数値化するために情報を検証し、類似の情報を論理的なグループに仕分けし、それによって生の情報を分析者や調査者が利用可能なフォーマットに落とし込むことが必要とされる。調査対象となっている活動の具体的な属性に関わらず、通常そこには、人物、場所、物および出来事に関連する情報が格納されることになる。

照合でのグループ化

- 人物－特定可能な者とそうでない者の両方で、お互いの関係性を含む。
- 場所－刑務所、庭、居室、工場等における特定の場所。
- 物－電話番号、薬物、刃物、逃走装置、手製の武器、刑務所で作られたアルコール等。
- 出来事－生じた、生じている、または生じるかもしれない出来事で、そこには特定の日付と他の出来事（例えば、これ以降とそれ以前）との関係から暗示される人物が含まれる。
- 行動－具体的な、申し立てられた、推測される活動、または活動の種類。

分析

分析とは、情報の意味と本質的な特徴を解明するための注意深い検証を意味している。インテリジェンス手続において分析は鍵の一つとなる。分析とは、利用可能な情報の意味と本質的な特徴についての掘り下げた検証と説明することができる。分析は情報のギャップ、長所と短所を際立たせ、進むべき道を示してくれる。

分析には、２つの基本的な類型がある。戦略的分析〔strategic analysis〕は、より高い「ヘリコプター的」かつ長期的な視点を有しており、また戦術的分析〔tactical analysis〕は、即時的な運用上の問題に焦点を当てている。戦略的情報とインテリジェンスは、傾向と発生する脅威を検討する。戦術的情報とインテリジェンスは、今ある状況または現在の運用に目を向けており、それはしばしばリアル・タイムである。

分析では、文脈の中で情報を検討し、その意味することについて結論を導き、今

ある知識とのギャップを際立たせ、次に起きそうなことを示し、そして可能な将来の行動を推奨する。この作業は、一般的な調査の途中に、分析者が異常、傾向または関連性に気づくことによって引き起こされるかもしれないが、より一般的には、上級管理者が疑問を投げかけたり、あるいは特定の照会事項を伝えることによって開始されるであろう。

分析の成果は、業務を委託した人物の要求に基づいて、多様なフォーマットで提供されうる。それらは（薬物取引といった）複雑な戦略的事項に関する掘り下げた報告書の形から、特定の事項（逃走企図、携帯電話を使用する受刑者）についての短い口頭説明の形までありうる。

良き刑務所インテリジェンスの成果とは、説得的、簡潔かつアクセス可能であり、強固なエビデンスに裏づけられた明確かつあいまいさのない勧告が付されているものである。情報のフローや情報源が薄弱な場合、分析成果も弱いものとなるだろう。

情報とは、すべてのピースが情報の断片から成るジグソー・パズルになぞらえることができる。正しくそれらをつなぎ合わせれば絵が現れるが、絵が完成するためには、すべてのピースが正しい位置に収まらなければならない。どんなささいな１ピースであったとしても、それがなければ絵にはなりえない。情報についても同じである。つまり、断片のつなぎ合わせが、インテリジェンス収集の手続なのである。

インテリジェンスが高く格付けされた場合、インテリジェンスに基づいて、手続の変更、ある区域の物理的な変更、追加のスタッフの配置、または特定の物に対して注意をするようにスタッフに伝えるといった行動となり得る。

分析の重要な側面に、仮説立案〔hypothesis development〕がある。仮説立案という用語は、簡単に言えば、ある情報の収集が意味していることについて、選択す

べき理論を提案することを指している。通常であれば、同じデータ一式から、複数の仮説を立てることができる。仮説の要素とは、次のようなものである。

仮説の要素

- 誰が－鍵となる複数の人ないし個人
- 何を－犯罪行為
- どのように－実行の手段
- どこで－地理的な位置
- なぜ－動機
- いつ－過去、現在または未来

普及

普及の段階とは、分析結果がクライアント、つまり刑務所管理者へ配布されることを意味する。普及の手続は、以下のような多様な形態をとることができる。

- 構造化された正式な報告書
- 配布資料を用いた、構造化された正式な口頭報告
- 週刊の広報形式による要旨
- インテリジェンスおよび調査チームに対するその場での概要説明

インテリジェンス手続の最初のサイクルは、普及の段階で完結する。

概要版インテリジェンス

概要版インテリジェンス〔intelligence briefs〕は、分析によって判明した結果を提供する。成果物は簡潔であり、そして特定の問題または傾向に関係する結論のみを示さなければならない。インテリジェンス実務家は、自分たちの分析を批判的に評価し、最終的な成果物が、管理者が情報に基づいた決定をするための重要なインテリジェンスを明確に表明するよう努めなければならない。

概要版インテリジェンス

概要版インテリジェンスは、タイムリーな業務遂行を可能にするために、問題の要旨を提供するものである。それは今ある成果物のアップデートを伝えるために用いることもできる。概要版インテリジェンスは、包括的な評価よりも問題の要約を提供することで業務量を減らし、新たな問題をより効率的かつタイムリーに報告することを助ける。

概要版インテリジェンスは、刑務所管理者による最初の要求に基づいていなければならない。例えば、刑務所長が刑務所での薬物乱用の水準に関するレポートを求めているのであれば、概要版インテリジェンスはその題材に焦点をあてなければならない。作成者は、刑務所管理者が知りたいことを明確に理解しなければならず、さらに管理者がその成果によってやろうとしていることをある程度理解しなければならない。（クライアントによる委託が最初にない）自己発信の成果物の場合は、当該成果物の使われ方の可能性に配慮すべきである。インテリジェンス実務家は、クライアントの認識を通して、特定の状況のどの側面が興味を与え、または利益をもたらすのかを予測しなければならない。

知っておかないといけないのは、実際の概要版は、必ずしもその作成に投入された時間と労力を表さないということである。報告書の中に納められている２～３頁のインテリジェンスが、数日、数週間または（場合によっては）数ヶ月の仕事の結果でありうるということを、クライアントに納得させることは難しい。分析者は、努力の総量と文書の長さを一致させるようとする罠に陥らないようにすべきである。

インテリジェンス成果物を作成するための重要なポイントは、刑務所管理者の関心のある問題に答えることである。このような関心事項は、インテリジェンス・サイクルの「課題定義〔task definition〕」の段階で設定されることが理想である。仮にその段階で関心事項が設定されなかったとしても、インテリジェンス実務家は、何らかのかたちでクライアントの関心を理解していなければならない。概要版インテリジェンスの中では、刑務所当局の利益のため、すべてのことが「だから何？〔so

what?〕」という疑問に答えることを重視しなければならない。

付録２〔未翻訳―訳者注〕は概要版インテリジェンスのひな型と補足ガイドラインである。

インテリジェンスの共有

インテリジェンスは、どこまで共有されるか決定する必要がある。保安部局で保管され続ける場合もあれば、刑務所長または刑務所当局本部に付託される場合もある。時には、インテリジェンスが他の法執行機関に関連があり、有用となることもあるだろう。インテリジェンス成果物には、適切な取り扱いコードが明確に付けられていなければならない。刑務所インテリジェンスは、受刑者には決して共有されてはならない。

ほとんどの場合、インテリジェンス報告書は、保安責任者または刑務所長に伝達され、何か行動をするのか、するのであれば何をするのかが決定されることになる。同様に保安責任者や刑務所長は、インテリジェンスについて「知る必要のある」人物を決定する。

インテリジェンス取り扱いコードの例

- 作成された国の法執行機関内での普及を許可する
- 他の国内機関への普及を許可する
- 国際的な法執行機関への普及を許可する
- 作成した機関のみで普及を許可する
- 普及を許可するが、受領機関は定められた条件を守る必要がある

インテリジェンスに基づいて行動する

可能性として次のような行動がありうる。

- 何もしない
- 何もしないが、問題に関する情報を引き続き集めるように職員に指示を与える

（戦略的または運用上の目的の一部として）

- １人ないし複数の受刑者を移動させる
- 受刑者または建物を検査する
- 面会者または職員を検査する
- 戦略的な問題であれば、地方または国の部局に知らせる
- 地域の法執行機関に知らせる（策定されたプロトコルに従って）

再評価

再評価は、インテリジェンス・サイクルの各段階を改善することができる方法を特定するために行われる、サイクル全体の継続的な点検を意味する。再評価は、単にサイクルの最後で行われるのでなく、その手続全体を通じて行われることで、もっとも価値のあるものとなる。しばしば再評価によって、サイクル全体のやり直しが必要となることもあるだろう。

【付記】本稿は、JSPS科研費（19H01422、19K13536、20J00787）の助成を受けたものである。