英国におけるＣＣＴＶ等の取扱い及び
オランダにおけるマネー・ロンダリング対策

～海外調査報告～

内閣委員会調査室　　寺西（てらにし）　香澄（かすみ）

１．調査の経緯

近年、世界各地で大規模・無差別テロが相次いでいる。平成 20 年は我が国において北海道洞爺湖サミットを始めとするＧ８関連会合が開催されることから、テロへの警戒警備は喫緊の重要課題である。

また、国内の治安に目を向けると、平成 19 年中の刑法犯認知件数が 190 万 8,836 件と 10 年ぶりに 200 万件を下回ったほか、内閣府が実施した「社会意識に関する世論調査」（平成 20 年２月調査）において、「悪い方向に向かっている分野」として「治安」を挙げた者の割合が 31.6%（前年は 35.6%）と改善傾向にあるものの、市民生活に大きな不安と脅威を与える事件が相次ぐなど、依然として厳しい情勢にある[1]。

我が国のテロ対策及び安全で安心な社会の実現に向けた治安再生への取組は、国民から強い関心が示されているテーマである。また、テロ対策等において、本人識別の確率が高いとされるバイオメトリクス認証（生体認証）技術が導入されつつあるが[2]、取得されたバイオメトリクスデータ（生体情報）の取扱いや管理の在り方についても関心が寄せられているところである。

諸外国におけるテロ対策及び治安対策等の中には、各国の置かれた状況や経験を踏まえた取組が含まれており、我が国の今後の施策実施に当たり示唆を与えるものと思われる。

今般、海外短期派遣研修の機会を得たことから、平成 20 年１月６日から 20 日までの間、テロ対策及び治安対策等につき特徴ある取組を実施している英国及びオランダを訪問し、以下の事項につき調査を行った。

【英国】公共交通機関のテロ対策（運輸省）
　　ＣＣＴＶ（監視カメラ）の映像等の取扱い（情報コミッショナー事務局（ＩＣＯ））
【オランダ】薬物犯罪対策（法務省）
　　危機管理・災害救助政策及びオランダの治安情勢（内務省）
　　マネー・ロンダリング対策（警察庁）

---

[1] 第 169 回国会における泉国家公安委員会委員長所信表明（第 169 回国会参議院内閣委員会会議録第１号２頁（平 20．３．18））

[2] 君塚宏「出入国管理と空港におけるバイオメトリクスの利活用」『電子情報通信学会誌』90 巻 12 号（平 19.12）1031～1036 頁、浦賀毅「バイオメトリクス認証技術について」『警察学論集』61 巻４号（平 20．４）103～107 頁

ＥＵにおける重大犯罪に関する情報共有の在り方（欧州警察機構（Europol））
ロッテルダム港における港湾セキュリティ対策（在オランダ日本国大使館よりブリーフィング）

本稿では、このうち、英国におけるＣＣＴＶ（監視カメラ）の映像等の取扱い及びオランダにおけるマネー・ロンダリング対策について、調査の概要を報告することとしたい。

２．英国における調査　－ＣＣＴＶ（監視カメラ）の映像等の取扱い－

（１）調査の背景

ＣＣＴＶ（Closed-circuit Television，監視カメラ）は英国全土で設置台数が420万台にのぼると推定されている[3]。ＣＣＴＶのほとんどは犯罪防止目的で設置されており、地方自治体又は警察が町の中心部に取り付けているほか、商店が自主的に設置する場合もある。

英国では、警察が捜査活動におけるＣＣＴＶの有効性を評価しているほか、一般市民も、犯罪防止に有効な手段であるとしてＣＣＴＶ設置を容認している。本稿では報告を割愛するが、運輸省への訪問・調査の際にも、地下鉄やバスといった公共交通機関へのＣＣＴＶ設置について、一部に批判の声があるものの、一般的にはプライバシーの問題よりも治安・安全の確保の観点が重視されており[4]、ＣＣＴＶ利用を支持する傾向にあることや、2005年のロンドン地下鉄爆破テロの際にもＣＣＴＶの役割・効果とその重要性が再認識された旨の説明があった。

また、バイオメトリクスデータやＤＮＡ型データの利用も、テロ対策及び捜査活動における有効な手段と認識されており、出入国管理システムへの活用やＤＮＡ型データベースの構築等が進められている。

今般の調査では、その性質上、慎重な取扱いが求められるべきＣＣＴＶの映像、バイオメトリクスデータ及びＤＮＡ型データを活用する前提として、どのような規制が行われているか、また、プライバシー保護の観点といかに調整を図っているかにつき、データ保護等に関する独立の監督機関である情報コミッショナー事務局（Information Commissioner's Office，以下「ＩＣＯ」という。）のデータ保護部門のJonathan Turner氏及びKatherine Price氏より説明を聴取し、質疑応答を行った。

（２）ＩＣＯの位置付け

ア　ＩＣＯの概要

ＩＣＯは、情報公開及びデータ保護の推進を目的とする政府から独立した監督機関

---

[3] ＩＣＯ，“A Report on the Surveillance Society”，September 2006，p.19.
<http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf>

[4] 英国では、犯罪発生率の高さが課題とされており、英国（イングランド及びウェールズに限る。）における主要な犯罪（内務省が警察から報告を受けた犯罪）の発生率（人口10万人当たりの認知件数の比率）は、11,241件（2003年度）、10,628件（2004年度）、10,405件（2005年度）と推移している。なお、統計の取り方等の相違もあり、正確な相互比較は困難ではあるが、参考までに我が国の主要な犯罪の発生率を示すと、2,185件（2003年）、2,006件（2004年）、1,776件（2005年）となっている（「犯罪白書」（平成19年版）39頁）。

であり、情報自由法（Freedom of Information Act 2000）及びデータ保護法（Data Protection Act 1998）等に定められた情報コミッショナー（Information Commissioner）の権限行使をサポートすることによって、法執行の中心的な役割を果たしている。

スタッフは情報公開部門、データ保護部門合わせて約270人おり、本部のほか、一部はスコットランド、ウェールズ、北アイルランドにおいて勤務している。

情報公開部門については政府から補助金が交付されている（2006/2007年度は555万ポンド（約11億円））が、データ保護部門は、個人データを取り扱う者（データ管理者）として登録した企業、政府（省庁ごと）、地方自治体等から支払われる手数料収入（１団体当たり年間35ポンド（約7,000円）。2006/2007年度は総計約1,000万ポンド（約20億円））に基づき運営されている。

イ　データ保護法の概要と情報コミッショナーの任務

データ保護法は、自己に関するデータについてのアクセス権等の一定の権利を与えるとともに、データ管理者に対し、同法に規定するデータ保護８原則[5]の遵守や情報コミッショナーへの登録等を義務付けている。なお、同法では、センシティブな個人データとして人種、政治的信条、宗教的信条、健康状態等に関するデータを挙げている。

情報コミッショナーは、同法に基づき、(a)同法の遵守状況を判断するために必要な情報をデータ管理者に要求する権限、(b)違法行為を行ったデータ管理者に対して適切な措置を講ずることやデータ処理の停止を要求する権限を付与されているほか、議会への活動報告が義務付けられている。

（３）ＩＣＯデータ保護部門の主要業務

ＩＣＯのデータ保護部門は、情報コミッショナーの権限行使をサポートするため、以下の業務を行っている。

ア　助言・勧告

市民からの個人データの取扱いに関する問い合わせへの対応のほか、苦情が寄せられた場合に当該企業等（データ管理者）を審査し、データ保護が行われているか査定する。データ保護法に抵触するおそれがある場合には、警告又は助言を行う。問い合わせへの対応スタッフが約20～50人、ケースワーカー及び助言スタッフが35～40人いる。

2006/2007年度には書面による問い合わせ・苦情が23,988件寄せられたほか、電話による問い合わせが別途年間約10万件寄せられている。

イ　監査・規制

データ管理者が、自らのデータ取扱い状況についての評価を要求してきた場合には、担当者を派遣し、監査をすることができる。データ保護法違反行為があれば通告を行

---

[5] (1)公正かつ合法的な処理、(2)特定された目的による保持、(3)目的に沿った処理、(4)正確性、最新性の確保、(5)必要な期間内での保持、(6)個人の権利を踏まえた処理、(7)安全性の確保、(8)適切な措置なき第三国への移転の禁止

い、それに従わない場合は法的手段（裁判）に訴えることとなる。20～25人のスタッフが担当している。

ウ　広報・啓発

データ保護に関する法制度や、法制度を遵守する上でのメリット・デメリット等を記載したガイダンス資料の作成等により、広報・啓発を行っている。約20人のスタッフが担当している。

（4）ＣＣＴＶ映像の取扱い

ＣＣＴＶについては一般的に国民の支持が得られているものの、画像の「質」や、犯罪防止以外の目的（スピード違反、バスレーンにおける乗用車通行、違法駐車、渋滞税課金等主に交通関係の摘発）での設置については議論がある。なお、防犯用に自宅にＣＣＴＶを設置するといった個人的使用については、データ保護法の対象ではない。

ア　運用基準の策定

ＣＣＴＶのみを対象とした法律はなく、データ保護法の対象の１つとして取り扱われている。ＩＣＯは、データ保護法に基づき、ＣＣＴＶの運用基準（code of practice）を策定している。運用基準には、需要に匹敵する割合でのＣＣＴＶ設置、目的にふさわしい鮮明な映像の撮影、ＣＣＴＶ設置を事前に周知する必要性、映像の保存期間・閲覧対象者の限定などを盛り込んでいる。

運用基準の策定手続としては、ＩＣＯの原案につき３か月の調査期間（consultation period）を設け、関係者等に意見を求めた後、さらに一般国民の意見を求めた上で確定させることとしている。

ＩＣＯは、欧州データ保護デーに当たる2008年１月28日に、当該運用基準の改定版を公表した[6]。改定版は、一般国民からの意見を踏まえて、より明確な表記を目指したほか、最近散見される「音声録音機能付きＣＣＴＶ」に対するガイドラインを新たに盛り込んだ。音声録音については原則禁止とし、特定の（例外的な）場合のみに認めることとしており、例えば、警察が容疑者を逮捕・尋問する場合には許容されるが、タクシーの乗客の会話を録音するため車内に設置することは認められない。

運用基準策定で問題となる点は、映像の保存期間についてである。映像の保存期間は、かつて１か月分をビデオテープに録画していた経緯もあり31日間とされているが、警察はより長期の保存を望んでいる。ＩＣＯとしては、期間を定めず、「目的に応じて弾力的に対応」するよう助言を行ったところである。例えば、パブでのけんかについては短期間の保存で足りるが、銀行ＡＴＭを利用した詐欺事件等については長期間の保存を要する場合も考えられるからである。

イ　内務省が取りまとめた全国ＣＣＴＶ戦略（National CCTV Strategy）に対する見解

内務省は、ＣＣＴＶの「画質」に問題があるため、警察がＣＣＴＶを有効に活用で

---

[6] ＩＣＯ, “CCTV code of practice Revised edition 2008”
<http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf>

きていないとして、ＣＣＴＶの登録制度を設ける方針である[7]。ＩＣＯとしては、警察がすべてのＣＣＴＶを管理することは国民監視につながるおそれがあるため、登録を義務付ける必要はないと考えている。

（５）バイオメトリクスデータの取扱い

バイオメトリクスデータも、データ保護法の対象の１つとして取り扱われている。欧州の一部の国（例えば、東欧地域、フランス、イタリア等）では、公的認可を受けた組織のみにバイオメトリクスデータの取扱いを認めているところがあるが、英国ではバイオメトリクスデータをセンシティブなデータとは考えず、他のデータと同様に取り扱うこととしている。

バイオメトリクスデータの利用は、官民ともに関心が高まっている分野である。一般国民はバイオメトリクスにそれほど抵抗を感じていないようである。ただし、国境での不法移民対策や犯罪防止のためにバイオメトリクスデータを利用することは受入れの余地があるが、職場や学校での利用については議論が起こる可能性がある。

英国は世界に先駆けてバイオメトリクスを導入した国である。警察は、ＩＤＥＮＴ１（アイデントワン）と呼ばれるバイオメトリクスデータベースに700万人分（容疑者のみならず関係者のものも含む。）の指紋データを登録しているほか、犯罪現場から採取した身元不明の指紋データ150万件を保存している。

また、警察には指紋データのほか、テロ対策に関連して取得された指紋データが約50万件あるが、これについては当該データベースへのアクセス権限を有する人間が限定されている。移民や政治亡命者の指紋データベースも別途存在し、警察からは、これらのデータベースの情報共有を求める声も出ている。情報共有は、安全な情報の取扱いが行われている限り有効であると言えるが、一般的にすべてのデータの共有は認められていない。

バイオメトリクスデータとしては主に指紋が利用されているが、近年「顔画像」（facial image）の利用が注目されており、10年後にはこれが重要な役割を担うと考えられている。

欧州では、バイオメトリクスデータをめぐるさまざまな動きが見られる。ＥＵでは、亡命希望者の指紋データベース（ＥＵＲＯＤＡＣ）が設けられているほか、一部の諸国では、警察機関の間における指紋データやＤＮＡ型データの交換・共有を可能とする協定も締結されている。

最近、小学校図書館における「指紋自動認識システム」利用が問題となった。指紋の利用自体について一般的に抵抗感はないものの、この事例においては、保護者にほとんど周知されないまま導入した点や周知期間自体も３日間のみだった点等で不適切であるとの声が保護者から上がっている。ＩＣＯでは、小学校の場合、児童が理解できないまま指紋データを採られる可能性があることから、保護者への通知を前提とした上での導入は許容される旨を助言した。

---

[7] Home Office, “NATIONAL CCTV STRATEGY”, October 2007, P.20.
<http://www.crimereduction.homeoffice.gov.uk/cctv/cctv048.pdf>

（６）ＤＮＡ型データの取扱い

ＤＮＡ型データも、データ保護法の対象の１つとして取り扱われている。

ＤＮＡ型については全国データベースを構築することにつき論議が高まっている。イングランド及びウェールズでは、一定の犯罪に関して逮捕されたときのみ採取が認められており、約470万人分のＤＮＡ型データ（うち30%は同一人物のものとされる）が登録されている。この対象をすべての犯罪に拡大すべきとする意見もある一方、微罪にまで拡大することへの弊害を懸念する意見もある。また、逮捕されたが不起訴処分となった場合においてもＤＮＡ型データは永久に保存されることとなっているため、不起訴となった者のＤＮＡ型データは削除すべきとの意見もある（一部の警察では削除の対応をしているところもある）。なお、スコットランドでは裁判を受けて有罪となった者のＤＮＡ型データのみを保持できることとされている。

ＤＮＡ型データの取扱いに関し、不起訴処分となった者がＤＮＡ型データの削除を求めて裁判を提起したところ、最高裁判所は、「ＤＮＡ型データの保持はプライバシーと無関係」として政府の対応を支持する判決を下した。原告はこれを不服として欧州人権裁判所（European Court of Human Rights）に提訴しており、本年中に判決が出る見通しである。ＩＣＯは、欧州人権裁判所が「人権侵害である」との判決を下すものと予想している。

政府は、ＤＮＡ型データの取扱いに関する新たな法案につき議会を通過させたいとしているが、欧州人権裁判所の裁判結果を見た上で今後の動きが決まってくることが見込まれる。法案の詳細は不明だが、逮捕・拘留時のＤＮＡ型データの取扱いにつき法律上の理由付けを明確にしているものと思われる。

ＤＮＡ型データについては、以下の事項が懸念すべき点として挙げられる。

１点目は、ＤＮＡ型データが警察のデータとリンクされていることである。ＤＮＡ型データベースに名前があれば一般の人と比較して容疑者として疑われる可能性が高まる。これに関連して、ある裁判官が、黒人少年からのＤＮＡサンプル採取の割合が大きい現状を差別的ととらえ、すべての国民のＤＮＡ型をデータベースに登録すべきと発言し大きな議論を呼んだ。これについては国民のみならずＩＣＯも強く反対した。

２点目は、ＤＮＡ型データのみならずＤＮＡサンプルも長期間保持されることである。将来的にサンプルから人種や健康状態を読み取ることができる可能性があり、よりセンシティブなデータとなりうることが懸念されている。

３点目は、先に言及したイングランド及びウェールズについての問題だが、自発的にＤＮＡサンプルを提供した者や犯罪被害者のＤＮＡ型データも永久にデータ削除ができないことである。

政府は全国データベースの構築を目指しており、徐々にサンプル量も増加が見込まれるが、同時に登録ミスのリスクも高まることをＩＣＯは懸念している。裁判においてＤＮＡ型データが証拠として提出された場合、陪審員はＤＮＡ型データを「科学的な根拠があり間違いはない」と重視する傾向にあるため、ミスがあった場合には取り返しのつかない事態を招くおそれがある。

（7）ＩＣＯの今後の課題

ア　データ保護法への理解促進

データ保護法は大変複雑なルールであり、法の内容についての理解が進んでいない。情報コミッショナー自身も「内容面、手続面ともより実用的なものとして市民に分かりやすくすべき」との意見である。データ保護法は市民の権利を守ることを主眼としており、ＩＣＯはこの点を踏まえて検討を進めていく方針である。

イ　監査権限の強化

ＩＣＯはデータ管理者の要求があった場合のみ監査を行うことができるのであって、強制力はない。ただし、2007年秋に、歳入関税庁による約2,500万人分の個人データ紛失が明らかになったこと等もあり、最近ではデータ管理者の要求がない場合にもＩＣＯが監査に入ることを期待する声が強まっている。

監査を実施したとしても、問題の全体像が見えてこないことが現在の課題である。ＩＣＯとしては、監査権限の強化がなされるのであれば、この点はクリアされるのではないかと考えている。

ウ　プライバシー影響評価の必要性

プライバシー影響評価（Privacy Impact Assessment）とは、例えば、事業を行う際に収集される顧客データ等の個人データの量やプライバシーへの影響等を事前に評価するプロセスであり、米国やカナダで導入されている。英国のみならずＥＵにおいてもいまだ導入されていないプロセスであるが、ＩＣＯとしては、そのコンセプトを理解して導入計画を立ち上げることが重要と考えている。

３．オランダにおける調査　－マネー・ロンダリング対策－

（1）調査の背景

第166回国会において内閣委員会で審議され、成立した「犯罪による収益の移転防止に関する法律」には、犯罪収益に関係する疑いのある取引に関する情報を集約・整理・分析して捜査機関等に提供する業務を担うＦＩＵ（Financial Intelligence Unit:資金情報機関）を金融庁から国家公安委員会に移管すること及び当該「疑わしい取引」に関する情報の届出が義務付けられる事業者を拡大することが規定されている。

法案の立案過程において、弁護士等に対する情報届出の義務付けが検討されたが、弁護士が直接警察に依頼者の情報を届け出る仕組みの是非が弁護士自治や守秘義務の観点から議論を呼び、最終的に法案には盛り込まれないこととなった[8]。

オランダのＦＩＵは従来法務省に置かれていたが、2006年に、ＦＩＵ機能と捜査機能を融合すべく、警察庁に新たな組織を設置した。この組織改編に当たり、我が国と同様の議論があった可能性があることから、今般の調査では、オランダＦＩＵの概要、新組織を警察庁に設置した経緯、弁護士を始めとする職業専門家による「疑わしい取引」の通報義務

---

[8] 「犯罪による収益の移転防止に関する法律案」の提出経緯や概要については、倉田保雄「マネー・ロンダリング及びテロ資金対策を強化～犯罪収益移転防止法案～」『立法と調査』265号（平19.３）３～８頁、江口寛章「犯罪収益移転防止法策定の経緯と概要」『警察学論集』60巻７号（平19.７）28～78頁を参照。

の取扱い等につき、Jolanda van de Streek氏（ＦＩＵ所長）、L.M. Peek氏、Peter Speekenbrink氏及びC.P.W. Kok氏より説明を聴取し、質疑応答を行った。

（2）マネー・ロンダリング犯罪について

オランダでは、1994年にあらゆる犯罪行為から得られた収益のマネー・ロンダリングが違法化されたが、2001年12月には、当該収益の起源となる犯罪の立証に係る検察官の負担を軽減するため、刑法にマネー・ロンダリング行為自体を犯罪とする規定が盛り込まれ、検察官は(a)当該金銭が犯罪から得られたものであること、(b)マネー・ロンダリングをしようとする者が犯罪から得られた金銭であると知っていた又は当然知るべきであったことのみを証明すれば足りることとされた。

2004年及び2005年に最高裁判所は、この点につき、当該金銭が具体的にどの犯罪から得られたものかを証明する必要はなく、一般的に犯罪から得られたものであると証明すればよい、と判示している。

（3）オランダＦＩＵ（FIU-Netherlands）の設置

オランダは2006年１月１日から、ＦＩＵを行政的側面と警察の側面を併せ持つ多元的な組織とした。

2006 年以前は、(a)オランダのＦＩＵとして、事業者が一定の指標に基づき「通常でない取引」であると判断した通報の受付・分析を行うＭＯＴ（the Office for the Disclosure of Unusual Transactions：法務省所管）と、(b) 「通常でない取引」のうち、ＭＯＴによる分析の結果、マネー・ロンダリングやその他の犯罪収益に関わっていることが「疑わしい取引」であると判断された情報の提供先である警察部門（ＢＬＯＭ，specialized investigative police unit：内務省所管）の連携・協力により、マネー・ロンダリング対策が講じられてきたが、法務大臣が外部に委託した評価報告書において、(a)と(b)の機能の融合によりマネー・ロンダリングの捜査がさらに効果的となるとの勧告がなされ、ＦＩＵの在り方を検討することとなった。

新たなＦＩＵは警察庁に置かれたが、通報者の過半を占める金融機関が直接警察とコンタクトをとることへの抵抗感等に配慮して、(a)の機能を引き継ぐ行政部門を法務省が引き続きサポートすることとし、情報管理の面等で警察からの一定の独立性を確保することとした（後述）。

（4）オランダＦＩＵの概要

オランダＦＩＵは、(a)行政部門（旧ＭＯＴ）、(b)警察部門（旧ＢＬＯＭ）、(c)サポート部門で構成される。これら３部門は緊密に協力しており、部門横断的にプロジェクトを開始することはできる。なお、部門横断的な人事異動は行われず、それぞれの部門に特化して業務に当たることとなっている。

スタッフ数は56人で、３部門にそれぞれ16～18人が配属されている。スタッフの中には、財務省管轄である税法違反捜査部門からの出向者２人が含まれているが、彼らにはＦＩＵ

の保有情報を漏えいしないよう、特別の守秘義務が課せられている。その他、データベース・システムの高度化のためＩＣＴの専門家を臨時に雇用している。

2007年のＦＩＵ予算は288万ユーロ（約４億6,000万円）である。

（５）「通常でない取引」の通報の取扱い

「通常でない取引」の通報受理及び情報管理は法務省の管轄の下、ＦＩＵ所長の責任において行われている。

「通常でない取引」に関する通報は行政部門に対して行われ、当該通報は特別な法律上の根拠に基づき設置されたデータベースに保存される。なお、通報データの保存期間は５年である。通報データはデータベースに登録されると自動的に他の通報との関連性等がチェックされることとなっており、これらのチェックや調査・分析を経て、最終的にＦＩＵ所長の権限で当該「通常でない取引」が「疑わしい取引」であると結論付けられたときに、当該取引の情報が諜報機関、警察、検察に通告される。

近年の「通常でない取引」の通報受理数及びそのうち「疑わしい取引」と判断された取引数は、以下のとおりである。

年	「通常でない取引」の通報数（件）	うち「疑わしい取引」と判断されたもの（件）	「疑わしい取引」の割合
1999	45,079	10,803	23.96 %
2002	137,339	24,741	18.01 %
2005	181,623	38,481	21.19 %

ア　「通常でない取引」情報の管理

行政部門は「通常でない取引」の調査に当たり、警察等の持つ情報にアクセスすることができるが、警察部門や検察庁等その他の機関が行政部門の情報にアクセスすることは原則としてできず、厳密な条件の下でのみ許可される。

イ　「疑わしい取引」の判断

「疑わしい取引」の判断は、行政部門による「通常でない取引」の調査・分析に伴うもののみならず、以下の場合も含まれる。

(a)警察部門が独自の調査・分析で「疑わしい取引」と判断したもの

(b)外国ＦＩＵからの通報があったもの

(c)検察庁の捜査で「疑わしい取引」と判断されたもの

(d)ＦＩＵ所長が「公共の利益を確保するため通報が必要」と判断したもの（職権的通報）

（６）通報者の義務

「通常でない取引」の通報義務が課せられているのは、銀行、両替所、証券会社、カジノ、生命保険会社、クレジットカード会社、信託会社、金融会社、商品取引業者、公証人、弁護士、不動産会社（仲介業者を含む）、会計士、ビジネスコンサルタント、法律顧問、税

務顧問等である。

通報者は、当該取引から２週間以内に通報しなければならない。また、当該取引についての情報を顧客から直接聞き出すことは禁止されている。通報者は通報したとの事実をもって刑法、民法による訴追を受けることはないと保障されている。通報者が銀行等の金融機関のスタッフの場合、通報は個人名ではなく金融機関名で行う（ただし、公証人や弁護士等は個人名で通報する）。

通報者は、「通常でない取引」の通報時に、通報が主観的判断に基づくものか、又は客観的指標（例えば、一定の金額以上の取引であること等）に基づくものかを明らかにしなければならない。

通報義務の履行を確保するため、以下の機関が監視を行っている。

(a)オランダ中央銀行（金融機関の監視）

(b)投資会社の監視機関

(c)金融取引監視事務所（公証人事務所、弁護士事務所等も対象）

(d)税務署（不動産会社等も対象）

故意に通告を行わなかった者には、１万1,250ユーロ（約180万円）の罰金又は２年以下の懲役が、過失の場合は1,250ユーロ（約20万円）の罰金又は６月以下の懲役が科せられる。

最近は、通報を行わなかった者にまず通報履行を勧告し、履行までの間は課徴金の支払いを命ずることができることとし、それでも履行しない場合に罰則を科すこととしている。この措置にも従わない場合は検察庁が起訴し、最終的に業務の認可取消しもあり得る。

（７）弁護士の通報義務

オランダにおいても、公証人や弁護士による通報義務の在り方について議論があった。

オランダでは、「通常でない取引」の通報を行政部門で受理することにより、情報管理の面等で警察から一定の距離を置くこととしているほか、弁護士については弁護士協会に置かれるコンサルタントに通報についての相談ができる体制が整えられている。ただし、義務履行の監視機関（上記の(c)金融取引監視事務所）も置かれており、最終的には弁護士個人の判断で通報する義務を負うこととなる。

しかし、公証人や弁護士については、その職務の特殊性にかんがみ、通報義務違反に対して罰則を科すのではなく、弁護士協会等の内部規則に基づく懲戒処分が行われることが多い。

（８）国際協力

オランダはＦＡＴＦ（Financial Action Task Force on Money Laundering：金融活動作業部会。マネー・ロンダリング対策において国際的協調を推進する政府間会合）のメンバー国であり、また、各国ＦＩＵの情報交換の場であるエグモント・グループにも参加している。

エグモント・グループにはいくつかのワーキンググループがあるが、オランダはすべてのグループに参加している。例えば、訓練関係のワーキンググループでは、事件処理や情

報処理のテクニック等につき情報交換を行うことで参加国間の知識・経験を共有しているほか、ＦＩＵ調査官の訓練プログラムの作成を行っている。

また、二国間での協力関係の構築も進めており、スウェーデンのＦＩＵとは麻薬取引関係で協定を締結すべく準備をしているところである。

そのほか、情報収集・分析の過程で海外のＦＩＵと直接コンタクトをとることもある。情報を国際的に共有することは非常に重要と考えており、国ごとに運用やシステムの相違はあるものの、今後もグローバルな視点で実効的なマネー・ロンダリング対策を講じていく方針である。

４．むすびに代えて

現在、我が国における防犯カメラの運用は、主に地方公共団体が制定した条例、要綱、指針等に基づき行われているが、全国規模での法的規制や、独立機関による利害調整・紛争解決を期待する意見もある[9]。バイオメトリクスデータ及びＤＮＡ型データの取扱いについても、プライバシーの観点から更なる検討が必要との指摘が見られる[10]。

また、マネー・ロンダリング対策に関しては、本年３月に、平成15（2003）年に再改訂されたＦＡＴＦ勧告に係る我が国の実施状況につき相互審査[11]が行われたところであり、弁護士等に対する疑わしい取引の届出義務の取扱いについての評価結果が注目される。

今般の調査が、今後の犯罪対策等に関する国会論議に資するものとなれば幸いである。

最後に、今般の調査に御協力いただいた訪問先を始め関係各位に感謝を申し上げる。

【参考文献】

財団法人自治体国際化協会「英国の情報開示と保護－情報自由法とデータ保護法を中心として－」『CLAIR REPORT』283号（平18.６.15）
＜http://www.clair.or.jp/j/forum/c_report/pdf/283.pdf＞
Information Commissioner's Office, “Annual Report 2006/07”, July 2007.
U.S. Department of State, “International Narcotics Control Strategy Report, Volume II: Money Laundering and Financial Crimes, Country Reports, The Netherlands”, March 2008. ＜http://www.state.gov/p/inl/rls/nrcrpt/2008/vol2/html/100809.htm＞

---

[9] 岡本美紀「街頭防犯カメラシステムの導入をめぐる諸問題－我が国と英米における現状の比較検討－」『法学新報』112巻１・２号（平17.７）628～629頁、甲斐素直「監視カメラと人権」『日本法学』72巻１号（平18.６）21頁

[10] 瀬戸洋一「価値あるバイオメトリックシステムを構築・運用するための提言」『電子情報通信学会誌』90巻12号（平19.12）1028～1029頁、日本弁護士連合会「警察庁ＤＮＡ 型データベース・システムに関する意見書」（平19.12.21）＜http://www.nichibenren.or.jp/ja/opinion/report/data/071221_000.pdf＞

[11] ＦＡＴＦは、各メンバー国・地域に対し、順次、その他のメンバー国により構成される審査団を派遣して、審査対象国におけるマネー・ロンダリング対策及びテロ資金対策の法制、監督・取締体制、マネー・ロンダリング犯罪の検挙状況など様々な観点から、ＦＡＴＦ勧告の遵守状況を相互に審査している。