

国際市民裁判所・第一号法廷・国家情報管理国際原則法

—目次—

序文

前文

語句の定義

第1章 一般的諸原則

第2章 国家安全保障を理由に秘匿され得る情報と開示されるべき情報

第3章 情報の機密指定及び機密解除に関する規則

第4章 情報請求の扱いについての規則

第5章 国家安全保障と情報への権利の司法的側面

第6章 安全保障部門を監視する機関

第7章 公務関係者による公益的開示

第8章 公衆への情報暴露に対する制裁又は制約行為の制限

第9章 結びの原則

付記<パートナー機関>

—序文—

今日の国際間における情報管理は複雑化の一途を辿っています。個々の国家においても、経済的、文化的、宗教的な要素に関連しながら、独自の情報管理が運用されています。国家と同盟国だけの利益が優先される世界とは、冷静にみつめれば、戦争や覇権を前提とした時代錯誤の情報管理と言えます。国や市民間の格差が是正されること無く、旧態依然とした国益の論理だけが、情報の制御を独り占めにしています。人類の平和共存への願いを遠回りさせるだけの今日の状況は、一刻も早く淘汰されなければなりません。限られた人類の生存への時間を、これ以上無駄にすることは出来ないのです。

特定秘密保護法や国家安全情報局を制定する中で、平然と無視されて来た「市民の知る権利」を取り戻さなければ、これからの民主主義そのものが歪められて行くのは必定と言えます。市民裁判所の意義は、これらの現状を共通認識として、地球上のすべての市民同士が連帯し、政治の在り方を根底から変革して行く所にあります。第一号法廷においては、まず国家管理における情報統制を解除し、国の行政機関や大統領府による情報の占有を監視し、異議を申立て、真の民主主義を実現する為に機能する事を目的とします。

アフリカのツワネにて 70ヶ国・500人に及ぶ人々の2年にもわたる協議の結果発信された「ツワネ原則」を原点として、国際市民裁判所の原則法として成案したものが、今回の「国家情報管理国際原則法」です。この様な法律が何時までも必要とされる社会は決して我々人類が望んできた道ではありません。将来、この様な法律が不必要となる国際社会こそ、我々市民が真に求めるものだということを宣言しておかなければなりません。<NGO市民プラットフォームジャパン>

—前文—

本法は、国家安全保障上の理由により、情報の公開を拒んだり、同種の情報の公益通報者を処罰したりする、国家の権限に関わる法律として制定されたものである。情報非公開についての遵守を規定し、一定の制限を設けて情報へのアクセスを制限しようとする場合でも、この原則に示された基準に従わねばならない。

国家安全保障と国民の知る権利は、しばしば相対するものとみなされる。政府は国家安全保障上の理由から時として情報を秘密にしようとするが、国民には公的機関が保有する情報に対して知る権利が存在する。過去の人類が記してきた歴史を振り返る時、実際には、国家の安全を守る行為について、国民が十分に知らされている場合に限ってそれは有効であった事実を我々は知らなければならない。

施政者の行為を国民が監視できれば、政治家や国家公務員の職権乱用を防ぐだけでなく、人々が国の方針決定にも参加できるようになる。機密とされる情報へのアクセスは、国家安全保障だけでなく、国民の政治への民主的参加を可能とし、政策決定の極めて重要な構成要素となる。人権の行使が保障される為には、ある一定の状況下で国家安全保障上の理由で情報を秘密にする必要も在り得るであろう。しかし、この場合は事前に国民の承認を得る必要があり、その為の監視機関として市民参加の機構を常設しなければならない。

多くの国において、ひとたび国家安全保障が持ち出されると、司法が行政府の主張に対して極めて従順となり、司法の独立性を殆ど失ってしまうという状況が垣間見える。それ故に国家安全保障と国民の知る権利との平等性が歪められてしまっている。国家の安全に対するほんの些細な脅威の報告や、脅威があるという行政府の僅かな主張があれば、情報を知る権利や、通常の証拠能力や被告人の権利に対してさえ例外を設けている国も少なくない。国家の安全への脅威があると行政府が過剰に主張すれば、行政府の暴走を防ぐために作られた機構そのもの(司法の独立、法の規範、立法府による監視、メディアの自由、国民の自由な発言)を損ねてしまうおそれさえある。

国家が保有する情報へのアクセスは全ての人民の権利であり、従ってこの権利は例外規定の少ない厳密に定められた法律によって規定されなければならない。また独立した裁判所、国の監視機関及びその他の独立機関による監視のための権利を、法律によって厳正に保護されなければならない。国家安全保障の見地を含め、国家が特定の情報を秘匿することによる正当な理由があるかどうかを認識し、情報の公開と非公開の間に適切な基準を設けることが民主主義社会にとって極めて重要である。又、安全、進歩、発展、福祉並びに基本的人権の完全な享受のためには必要不可欠なことでなければならない。人々が政府の行動を監視し、民主主義社会に正当に機能することを可能にしようとするならば、国家安全保障に関連する情報を含め、公権力が保有する情報へのアクセスする権利が絶対的に必要であると認識しなければならない。

この法案は、政府が保有する情報に人々がアクセスする権利及びその他の人権に関する国際法及び基準を厳密に精査し決定されたものである。

・過度の機密指定は、政府関連機関や同盟国の間での情報共有を妨げ、正当な秘密の保護を不可能にし、多くの不要な情報の中から重要な情報をみつけることを不可能にし、複数の機関が情報を重ねて収集することになり、安全保障担当者に過重な負担をかけるなど国家安全保障にとって損失となる場合もある事に留意しなければならない。

・国家安全保障の見地から非公開にすべきでない特定の情報が、それにもかかわらず、例えば国際関係、司法手続の公平性、訴訟人の権利、個人のプライバシーなど、国際法に認められた様々な理由で非公開にされる可能性があるが、その情報の秘密性を維持することによる公共の利益が、情報にアクセスすることによる利益よりも明らかに大きい場合に限られるという原則による。

・政府機関、立法機関、監督機関、その他の公的機関、法律起草者、裁判所、及び「国家安全保障と知る権利」の間にある最も難解な問題に関わる市民団体、とりわけ人権と民主的説明責任の尊重に携わる機関や人々に対して、実際的な指針を提供することを希望し、普遍的な価値と汎用性を持つ原則を作り上げるよう努めた。

・公開することによる公共の利益と、正当な国家安全保障上の利益保護のために秘密にする必要性のバランスを取るに当たっては、広く様々な困難に各国が直面すること、また、原則が普遍的である一方で、その実際の運用は、司法制度の多様性など各地の現実に応じたものでもありうる。

< 準拠 > 「米州人権委員会の表現の自由に関する原則宣言」、「情報へのアクセスに関する米州モデル法」、「アフリカにおける表現の自由に関する原則宣言」、「情報へのアクセスに関するアフリカモデル法」、「言論・表現の自由に関する国連特別報告書」、「メディアの自由に関する欧州安全保障協力機構(OSCE)」、「表現の自由に関する米州人権委員会特別報告者の2004年共同宣言」、「表現の自由と情報へのアクセスに関する人及び人民の権利に関するアフリカ委員会特別報告書」、「国連及び米州特別報告者のウィキリークスに関する2010年12月の共同声明」、「2010年にヴェニス委員会で採択されたテロ対策及び人権に関する報告書」、「1995年・アーティクル19が招集した専門家グループによって採択された国家安全保障」、「表現の自由及び情報へのアクセスに関するヨハネスブルグ原則」、「国家安全保障研究センター(CNSS)及びポーランド・ヘルシンキ人権財団によって1997年に作成された立憲民主主義における安全保障サービスの監視と説明責任原則」、「国連安全保障理事会決議第1373号によって要求された国家間の効果的な情報共有」「情報局とその監視のための法的制度的枠組みに関するグッドプラクティス」

<Definitions>

— 語 句 の 定 義 —

— 本法においては、文中でとくに指定されない限り、以下のように定義する —

<国家安全保障部門内の企業>とは、何らかの取引や事業を国家安全保障部門の中で行っている、又は行ってきた法人を指す。ただし、サービス設備、人員又は商品(例えば軍需品、器材、情報などであるが、これに限定されるものではない)を提供する請負業者又は供給会社のみを指す。これには、民間軍事会社及び民間警備会社も含まれる。しかし非営利又は非政府組織として設立された法人は含まれない。

<独立した>とは、組織上、財政上、及び運営上、全ての安全保障部門を含む行政当局からの影響、指導、管理を受けないという意味である。

<情報>とは、物理的特性に関わらず全ての記録資料の原本又は複写、及び全ての有形無形の資料を指し、それが保有されている形式や媒体を問わない。この中には、記録、通信、事実、意見、勧告、覚書、データ、統計、書籍、描画、計画、地図、図表、写真、視聴覚記録、記録文書、電子メール、日誌、標本、模型、及びあらゆる電子形式で保有されたデータが含まれるが、これらに限定されるものではない。

ORIGINAL

<公共の利益となる情報>とは、すべての市民に関連のある、あるいは役に立つ情報のことであり、単に個人的な利益のある情報のことではない。そしてその情報が公開されることが、例えば、政府の活動を市民が理解するために有用であるなどの理由で「市民のため」であるものを指す。

<正当な国家安全保障上の利益>とは、その利益の真の目的と主たる効果が、国際法・国内法に沿って国家の安全を守ることにある場合を指す。(その隠匿が正当な国家安全保障上の利益を保護するために必要である可能性がある情報のカテゴリーは原則 9 に定める) 国家安全保障上の利益は、その本来の目的と主たる効果が国家安全保障に関係のない利益を守るため、例えば政府や官僚を恥辱又は悪事の暴露から守るため、人権侵害、その他のあらゆる法律違反若しくは公共機関の機能に関する情報の隠ぺいのため、特定の政治的利益、党派又はイデオロギーの強化又は維持のため、若しくは合法的な抗議行動の抑圧のためなどであった場合正当とは見做されない。

<国家安全保障>とは、民主主義社会の必要に応じた形で、個々の国家の国内法で厳密に定義されているが、本法においては、国家間における平和共存を実現する為の安全保障を意味し、対外的な脅威から国民を守護する目的で制定されているものをいう。ただし、一国の利益のみを追求する為の法は、この概念からは除去される。

<公権力>とは、安全部門当局を含む政府当局及び憲法・法律によって設置された当局の全階層における行政、立法、司法部局の内部にある全ての機関、政府が所有又は管理するところの政府の代理を務める非国家機関を指す。また「公権力」には、公共の機能やサービスを実行し、相当額の公共基金や公的給付金によって運営される民間その他の主体が含まれる。ただし、こうした機能の実行やサービスの提供又は公共基金及び公的給付金の、使用に関連する部分のみを指す。

<公務関係者又は公務員>とは、安全保障部門を含め当局の職員、請負業者、下請け業者である者、又は過去にそうであった者を指す。さらに、政府が所有又は管理する機関に所属している者、政府の代理を務める非国家機関に雇用されている者、公共の機能やサービスを実行する者、相当額の公共基金や公的給付金によって運営される民間その他の機関の従業員を指す。

<制裁>とは、名詞として使用される場合、刑事上、民事上及び行政上の措置を含むあらゆる形態の処罰又は不利益を指す。動詞として使用される場合、「制裁を行う」とは、このような形態の処罰又は不利益を与えることを指す。

<安全保障部門>の定義には以下が含まれる。

- (1) 正規軍、警察及びその他の法執行機関、非正規軍、情報局、治安局(軍人・非軍事両方)を含む安全保障の提供者。ただし、これらに限定されるものではない。
- (2) 安全保障の提供者の調整、管理、監視の責任を持つ全ての執行機関、部局、省庁。

。

第 1 章 : 一般的諸原則

Principle 1: Right to Information

原則 1: 情報に対する権利

(a) 何人も、公権力により、あるいは公権力のために保有された情報、又は公権力が法によりアクセスする権利をもつ情報の開示を求め、受け取り、使用し伝達する権利を有する。

(b) 国際原則は、民間軍事会社及び民間警備会社を含む国家安全保障部門内の企業が、人権の享受への影響があると合理的に判断される可能性のある状況、活動、行為等に関する情報を、関連諸機関（独立監視機構、当該国裁判所）に開示する責任があるものと定める。

(c) 原則 1(a)及び 1 (b) に沿って、情報公開の義務を持つ者は、請求された情報を開示しなければならない。例外は、国家安全保障を含めた正当な利益への特定可能な損害を回避するために必要且つ法に定められた場合のみとする。

(d)国家の安全の保護を含む特定の責任をもつ公権力のみが、国家安全保障を理由とした情報非開示を主張し得る。

<注記>：ただし、非開示についての正当な理由の説明責任は当該する公権力にあり、関係する諸機関及び市民の代弁者としての独立監視機構、並びに当該国の裁判所に対し、詳細な事実を明らかにしなければならない。

(e)情報非開示を正当化するために国家安全を主張する民間企業のいかなる主張も、国家安全を保護する目的をもつ公的機関・独立監視機構・裁判所によって厳密に認可あるいは承認されなければならない。

<注記>：政府のみが国家安全保障を損なう場合がある情報の非開示を主張しうる。公権力はまた、公共の利益に関する特定の情報を率先して公開する積極的な義務を有する。

Principle 2: Application of these Principles

原則 2 : 本原則の適用

(a)本法は、**原則 1** で示したように、情報の開示が国家安全保障を損なう可能性があるとして政府が主張又は確認した場合に、その情報にアクセスする権利の行使に対して適用する。

(b)国家安全保障が情報制限の最も重要な公的理由の一つであることを考慮すると、公権力が、たとえば国際関係、公共秩序、公共福祉と安全、法執行、自由で公開された助言の将来的提供、効果的な政策形成、及び国家の経済的利益などの、アクセス制限の公的理由を主張するときは、その理由は、少なくとも本原則に規定されている情報アクセス権へ制限を課すための基準を、妥当なものとして諸機関及び独立監視機構と裁判所へ通知しなければならない。

(c)民主主義社会にふさわしい形で、国の法的枠組みの中で、情報開示・非開示を厳密に定義付けすることは、国家安全保障にとって必定のものである。

Principle 3: Requirements for Restricting the Right to Information on National Security Grounds

原則 3 : 国家安全保障上の理由に基づいた情報に対する権利の制限のための要件

政府が、その情報の制限が、**原則 (1) (a)** 法に基づき、且つ **(b)** 民主主義社会において必要であり **(c)** 国家安全保障上の正当な利益を保護するためであると明示することができない場合、また**原則 (2)** 情報制限の妥当性についての独立監視機関による検証と、裁判所の全面的検討による、速やかで、十全で、アクセス可能で、且つ効果的な調査を含む、職権乱用を十分に阻止するための規定を示すことが

できない場合は、いかなる国家安全保障上の理由に基づく情報への権利制限も適用してはならない。

(a)本法は、情報へのアクセスが可能であり、明解であり、綿密且つ正確でなければならないと定める。どの情報が非公開となり得るか、どの情報が開示されるべきか、そして情報に関するどのような行為が制裁の対象であるかを、何人であっても理解出来なければならない。

(b)民主主義社会において非開示が必須とされる要件

(i)その情報を公開すれば正当な国家安全保障上の利益を重大に害するという現実的且つ特定可能なリスクがなければならない。

(ii)情報を公開することによる損害のリスクが、情報を公開することによる総合的見地からの公益を上回らなければならない。

(iii)制限は比例の原則に従わなければならない、且つ損害から保護するための最も制限の少ない手段でなければならない。

(iv)制限することで情報に対する権利の本質を損なってはならない。

(c)「正当な国家安全保障上の利益の保護」について。国家安全保障上の理由により非開示になりうる情報の厳密な分類は、法により明確に定められなければならない。

<注記>：情報を公開することによる公共の利益と、損害のリスクとのバランスを保つために、たとえば合理的な額の資金の支出を必要とする手段などを講じることにより、開示による損害を軽減させる可能性を考慮すべきである。以下は情報公開の公的利益が損害のリスクを上回るかどうかの決定を行う際に考慮すべき要素の例である。

<情報公開を促す要素>：

(i) 公的問題についての開かれた議論を推進する

(ii) 政府の説明責任を強化する

(iii) 重要な問題に関して情報を与えられた上での建設的な議論を行うことに貢献する

(iv) 公的資金の支出についての効率的な監視を推進する

(v) 政府の決定の根拠を明らかにする

(vi) 持続的な環境保護に貢献する

(vii) 公衆衛生又は安全への脅威を明らかにする

(viii) 人権侵害又は国際人道法違反を暴露し、あるいはその説明責任の確保を補助すると合理的に予測される。

<情報秘匿を促す要素>

(a)情報公開することにより、正当な国家安全保障上の利益を侵害する、現実的で特定可能なリスクがあり得る場合。

<無関係な要素>

(a) 政府あるいは公務員に恥辱を感じさせたり信用を失墜させたりする原因となる。

(b) 政党やイデオロギーを弱体化させると合理的に予測され得る場合。

Principle 4: Burden on Public Authority to Establish Legitimacy of Any Restriction

原則 4 : あらゆる制限の正当性を確立するために公的機関が担うこと

(a) 制限の正当性を示す義務は、情報の非開示を求める公的機関にある。

(b) 情報を知る権利は広義に解釈され且つ適用されなければならない。

(c) 公的機関は単に損害のリスクがあると主張するだけでは不十分である。当該機関は、主張を裏付ける具体的且つ実質的な根拠を示す義務がある。

<注記> : 情報にアクセスを求めるすべての人は、**原則 26 と 27** に基づき、当局が主張するリスク判断の根拠について行政また司法当局に対し異議を申し立てる公平な機会を有する。

(d) 公開が国家安全保障に損害を生じるという旨の大臣又はその他の官僚による文書の発行などの、単なる主張は、いかなる場合も決定的なものとはみなされない。

Principle 5: No Exemption for Any Public Authority

原則 5 : あらゆる公的機関への適用

(a) 司法、立法、監視機関、情報機関、軍隊、警察やその他の安全保障機関、国家元首及び政府首班関連機関、そしてこれら機関を構成するあらゆる機関を含む公的機関は、情報公開の条件を免除され得ない。

(b) 情報は、他国又は政府間機構若しくは特定の公的機関又は公的機関内の部局によって作成されたり、共有したりしていることのみを根拠に、国家安全保障上の理由で秘匿されてはならない。

Principle 6: Access to Information by Oversight Bodies

原則 6 : 監視機関による情報へのアクセス

裁判所及び法廷を含む全ての監視機関、オンブズマン、申立機関等は、機密のレベルに関わらず、責任を持つ範囲に関する国家安全保障を含む、全ての情報へのアクセス権を有する。

Principle 7: Resources

原則 7: 資源

本法が実際に遵守されることを保証するために、国家は十分な人的・財政的・機能的資源を充当し、規則の公布や公文書の適切な維持管理等その他の必要な措置を執らなければならない。

Principle 8: States of Emergency

原則 8: 緊急事態

国民の生命始め、国内法・国際法に基づき公式に宣言された国の存在を脅かす緊急事態の際には、国家は、情報を求め、受け取り、伝達する権利に関する義務を免除され得る。ただし、それは窮迫した状況がすべての市民に理解された時とし、この免除が国際法に基づく他の義務との一貫性がある場合で、しかもいかなる種類の差別も伴わない限りにおいてのみ可能とする。

<注記>：情報や考えを求め、受け取り、使用し、伝達する権利は、その享受に際しては非常に重要な側面を持ち、国の緊急事態においてさえも常に十分に配慮し尊重されねばならない。すべての情報はこの性質を有すると考えなければならない。

第 2 章：国家安全保障を理由に秘匿され得る情報と開示されるべき情報

Principle 9: Information that Legitimately May Be Withheld

原則 9: 合理的に秘匿され得る情報

(a)公権力は国家安全保障を理由に、情報にアクセスする市民の権利を制限することができるが、そのような制限は、本法の他のすべての条文に適合し、その情報が公的機関によって保有され、下記のカテゴリーのいずれかに当てはまる場合に限られる。

(i)その情報が戦略上有効である期間中の、進行中の防衛計画や作戦、状況に関する情報

<注記>：「戦略上有効である期間中」とは、開示されても国家の準備態勢、能力、又は計画を知るために、敵と目される者が利用できる情報が何もない場合、その情報は開示されなければならないということを意味する。

(ii)通信システムを含む兵器システムその他の軍事システムの製造、性能、使用についての情報。

<注記>：この情報は技術データや発明、及び製造、使用に関する情報を含む。兵器や他の軍事システムに関する予算等の情報は国民が入手可能でなければならない。通常兵器について武器貿易協定で推奨されるような兵器の管理リストを維持・公開することは国家に必要とされる実践である。また、兵器や装備、兵士の数に関する情報を公開することも必要である。

(iii)国土や重要インフラ又は重要な国家機関を、脅威または妨害工作、武力の行使から護衛するため

の具体的な手段に関する情報で、機密であることでその効果を発揮するもの。

<注記>：「重要インフラ」とは戦略的資源、資産及び物理的又は仮想的システムを指し、これらの資源、資産及びシステムの破壊又は無効化は国家安全保障を弱体化させる影響があるもののことを指す。

(iv)情報局の活動、情報源、手段に関連又は由来する情報で、国家安全保障の問題に関するもの。

(v)外国や政府間機関からとくに極秘を期待されて提供された国家安全保障の問題に関する情報、及び他の外交上のコミュニケーションで提供された国家安全保障の問題に関する情報。

<注記>：このような情報は文書として記録し保管されなければならない。

<注記>：テロやテロ対策に関わる特定の情報が上記のいずれかのカテゴリで取り上げられる場合、この情報にアクセスする市民の権利は本原則や他の原則に従って国家安全保障の見地から制約を受けることがあり得る。ただし同時に、テロやテロ対策に関わるいくつかの情報にはとくに高い公益性があり得る。本法 10(a)、10(b)、10(h)-(1)、を参照。

(b)国内法において、少なくとも上記のカテゴリリストと同程度に範囲を狭めた情報カテゴリのリストの作成と保存を定めなければならない。

(c)国家は、上記のカテゴリリストに新たなカテゴリを追加することができる。ただし、原則 2(c)で提案されているように、そのカテゴリが具体的に特定され厳密に定義された上で、情報を秘匿することが、法律で定められた正当な国家安全保障を保護するために必要である場合に限られる。あらたなカテゴリを提案するに際しては、国家はそのカテゴリの情報の開示がどのように国家の安全保障を脅かすかについて説明する責を負う。

Principle 10: Categories of Information with a High Presumption or Overriding Interest in Favor of Disclosure

原則 10: 公開することが望ましいと強く推定される情報又は公開による利益が大きい情報のカテゴリ

下記に挙げたものを含むいくつかの情報のカテゴリは、法の支配と民主的監視プロセスにとって特に重要であり、高い公益性を持つ。その情報は公にされ、積極的に開示されるべきであり、場合によってはその情報の公開は最優先の義務となる。

下記のカテゴリにおける情報は、公開が必然とされる情報であり、国家安全保障を根拠に秘匿され得るのは、以下の場合に限られる。

本法の他の条項と矛盾しない形で、最も例外的な状況においてのみ、厳密に限定された期間に限り、法に基づいてのみ、そして開示することによる損害を抑える合理的な手段がない場合である。下記に記された特定のサブカテゴリの情報は本質的に公開による利益が最優先されるものであり、国家安全保障を根拠に非公開とすることは決して正当化され得ない。

(a)国際人権法及び人道法上の違反

(i)深刻な人権侵害や、国際法に基づく犯罪を含む国際人道法の重大な違反、個人の自由と安全に対する権利の組織的又は広範な侵害に関する情報の開示には、優先的な公益性がある。このような情報は、いかなる場合においても国家安全保障を根拠に非公開とされてはならない。

(ii)他の人権侵害や人道法違反に関する情報は公開されるべきものであり、どのような場合でも、人権侵害の説明責任を阻むような形で、又は犠牲者が効果的な救済にアクセスする手段を奪うような形で、国家安全保障を根拠に秘匿することはできない。

(iii)国家が政権移行期過程にあり、真実、正義、補償、再発阻止への担保確保がとくに求められている時、過去の体制下でなされた人権侵害に関する情報を社会に開示することは最優先の公益性を持つ。後続する政府は、前政権が隠ぺいしていたこのような情報を含むあらゆる記録をただちに確保し、保全し、遅滞なく公開しなければならない。

<注記>：人権侵害に関する情報の調査や再構築の義務については、**原則 21(c)**を参照。

(iv)この法律は、人権侵害が立証された、あるいは侵害について疑いがあると思われる場合において、その侵害の真実を明らかにするような情報(単独もしくは他の情報と関連して用いられる)に対して適用される。

(v)この法律はすでに発生した人権侵害及び現在進行中の人権侵害に対して適用され、人権侵害の行為者が情報を保有する国家であれ他の者であれ同様に適用される。

(vi)この法律で取り上げる人権侵害に関する情報は以下のとおりだが、これに限定されるものではない。

①人権侵害を構成する作為又は不作為、及び発生の日付や状況、合によっては行方不明者や遺体の所在を示す完全な記述や記録。

②被害者、親族、証言者のプライバシーその他の権利を侵害しない範囲での全被害者の身元情報、人権を守る上で関連があり得る被害者の数や特徴を示す集計データ又は匿名データ。

<注記>：被害者や親族及び証言者の氏名や個人情報、更なる人権侵害を防ぐ必要がある範囲で、また本人が死亡している場合はその遺族が情報の非公開をはっきりと自発的に要求した場合、又は非公開が本人自身の希望であることが明白な場合、公開することによって不利益を受ける集団にとって非公開であることが特に必要であることが明白な場合には、一般への開示は保留することができる。性暴力の被害者に関しては、氏名や他の個人情報の公開に対する承諾を得ることは必須である。18歳未満の子どもの個人情報は一般へ公開されるべきではない。この原則を解釈する時に念頭に置くべきなのは、様々な政府が様々な時代に、被害者個人の真の希望を顧みず、重大な人権侵害を受けた、又は受けているその個人を含むプライバシーの権利を盾に、人権侵害を国民の目から隠してきたという現実である。しかしこのことで、集計データ又は匿名データの公表を除外すべきではない。

③人権侵害を実行した責任のある機関と個人の氏名、人権侵害の発生当時存在した又は関与した国家安全保障部門の名称、上司や司令官の氏名、そして指揮や監督の範囲に関する情報。

(b)人間の自由と安全に関する権利の保護、拷問及び虐待の防止、生存権の保護

(i)国家による人命剥奪の権限を与える法律や規則、及び自由の剥奪に関する法律や規則（根拠、手続、移送、処遇、取り調べ方法を含めた拘禁状態に関するものを含む）。このような法律や規則を開示することは最優先の公益性がある。

<注記>：原則 10 を通して使用される「法律や規則」という語は議会立法又は委任立法、法令、規則及び条例、また大統領、首相、大臣又は他の公的機関による布告や行政命令、司法命令など、法的拘束力があるすべてのものを含む。また「法律や規則」は行政官によって権限を持つとみなされるあらゆる命令や法解釈をも含む。自由の剥奪には、あらゆる形態の逮捕、拘禁、投獄又は抑留を含む。

(ii)あらゆる人の拘禁中の死亡に関する情報、国家の責任によるその他の人命剥奪に関する情報。（犠牲者の身元情報、人々の死亡の状況、遺体の所在を含む）。

<注記>：いかなる状況であれ、国家安全保障を根拠に、人の秘密拘禁、秘密拘禁場所の設立と運営、秘密処刑につながる情報を秘匿してはならない。又、いかなる状況であれ、国家によって権限・援助・承認を与えられた者によって自由を剥奪された人の行方や所在が、その人の家族や、その人の全人生に正当な関係のある他の人々に対して、隠されたり、通知を拒否されたりしてはならない。自由を剥奪された者、拘禁中に死亡した者、又は国家機関によって死に至らしめられた者の氏名及びその他の個人情報、当該個人、あるいは当人が死亡している場合はその家族が、とくに秘匿を希望する場合、また秘匿することがかえって人権を尊重する場合は、プライバシーの権利の保護の必要な範囲で一般に対して秘匿することができる。自由を剥奪されている子どもの個人情報は一般に対して開示するべきではない。しかしこうした制限は、集計データ又は匿名データの公表を妨げるものではない。

(c)政府の構造と権力

この法律で取り上げる情報組織や機関は以下のとおりだが、これに限定されるものではない。

・軍隊、警察、国家安全保障組織や諜報機関及びその下部組織（民間も含む）のすべて。

(i)これらの組織や機関、その監視機関、内部説明責任に適用され得る法律及び規則。そしてこれら統轄する当局者の氏名。

(ii)総予算額、主要項目、基本的支出情報を含む公的資金の支出を評価・管理するために必要な情報。

(iii)二国間又は多国間で締結された協定の存在と条項、及び国家安全保障事項に基づく当該国による他の主要な国際的関与。

(d)軍事力行使又は大量破壊兵器の入手の決定

(i)この法律で取り上げる情報は、戦闘部隊の派遣又はその他の軍事行動の決定に関連する情報であり、その軍事行動の事実の確認、総合的な規模と範囲、論拠の説明、公式の理由の一部として述べられた事実が誤りであったことを示すあらゆる情報も含む。

<注記>：行動の「総合的な」規模と範囲に言及した理由は、これを開示することにより、問題となっている軍事行動の作戦面のすべての詳細を公表することなく、戦闘部隊の派遣決定に関連する情報にアクセスするという高い公益性を満たすことが一般的にできるからである。

(ii) 国家による核兵器や他の大量破壊兵器の保有や入手は、製造過程や作戦能力について詳細である必要は無いが、重要な公共の利益の問題であり、これを秘匿してはならない。

<注記>：この法文はいかなる意味においても、このような兵器の入手を容認するものではない。

(e) 監視

(i) あらゆる種類の監視に関する全体的な法的枠組みは、監視の認可や対象の選択、得られた資料の使用、共有、保管、破棄のすべての過程と同様、国民がそのすべての情報にアクセスできる。

<注記>：この情報に含まれるものは次のとおり。

- ① プロファイリングやデータ収集などの間接的な監視を含め公開・非公開のあらゆる形態の監視及び利用される監視手段の種類について定める法律
- ② 許容できる監視対象
- ③ 監視を実施又は継続するために必要な疑義の存在
- ④ 監視手段の期間の限度
- ⑤ 手段の利用の承認・審査手続
- ⑥ 国家安全保障上の目的で収集及び加工され得る個人データの種類
- ⑦ データの利用、保有、消去、移転に適用する基準

(ii) 市民は、監視を行う権限を付与された機関についての情報及び監視行為の利用についての統計にアクセスできる。

<注記>：これには、毎年特定の監視行為を行う特定の権限を付与された各政府機関の情報や、各機関に毎年与えられる監視許可の数、毎年監視の対象となる個人の数及び通信の数に関する入手できる最善の情報、明確な権限なしに監視が行われているかどうか、もし行われているとすれば、どの政府機関によるものかといった情報が含まれる。

(iii) 違法な監視が行われた事実があれば、市民はすべてを知らされるべきである。このような監視の対象となった個人のプライバシーの権利を侵害しない最大の範囲で情報は公開される。

(iv) 本法は情報にアクセスする市民の権利に関するものであり、監視対象となった、あるいはなったかもしれないと信じる個人の、その他の実質的且つ手続的権利を損なうものではない。

<注記>：監視行動又は情報源や手段を危機に陥れずに、可能な限りにおいて、ミッションの事実の存在を利用した監視方法の種類、日付、監視方法と実行に責任のある機関を)通知することは公権力の義務である。

(v) この法律の原則的運用で開示が望ましいと強く推定される情報は、他国の活動の監視にのみに関連する情報も適用される。

(f) 財務情報

この法律で取り上げられる情報には、国家安全保障部門の財政及び国家安全保障部門の財政を定めた規定を、市民が理解するための十分な情報が含まれる。この情報は下記を含むがこれに限定されない。

- (i) 主要項目を含めた部門別及び機関別予算
- (ii) 主要項目を含めた年度末財務諸表
- (iii) 財務管理規則と管理システム
- (iv) 資金調達規則
- (v) 最高会計検査機関及びその他の国家安全保障機関の財政面を審査する責任のある機関によって作成された報告書。機密扱いにされた同様の報告書のあらゆる項目の概要を含む。

(g) 憲法・法令違反及びその他の権力乱用に関する説明責任

この法律は、公権力又は公務関係者による憲法・法令違反及びその他の権力乱用の存在、性質、規模に関する情報を含む。

(h) 公衆衛生、市民の安全又及び環境

この法律に取り上げる情報は以下のとおり。

- (i) 公衆衛生、市民の安全又は環境に対する差し迫った実際的な脅威がある場合において、その脅威から生じる損害を理解したり、防止・軽減する手段をとったりすることを可能にするすべての情報。その脅威の原因が自然現象であるか人間活動によるものか(国家によるものか民間企業によるものか)を問わない。
- (ii) 天然資源の搾取、汚染排出物リスト、大規模公共事業又は資源採取の計画又は実施の環境への負荷、そして特に危険な原子力発電施設及び核廃棄施設や核関連物質の運搬等のリスク評価と管理計画に関するその他の情報。

第3章：情報の機密指定及び機密解除に関する規則

Principle 11: Duty to State Reasons for Classifying Information

原則 11：情報を機密指定する理由を述べる義務

(a) 国家が機密指定の公式のプロセスを有しているといわないに関わらず、公権力は、情報を機密指定する理由を述べる義務がある。

<注記>：「機密指定」とは、注意を要する情報が含まれる記録が検討され、その上で誰がアクセスしてよいのか、いかにして記録が扱われるべきか、を指示する旨が与えられるプロセスのことである。恣意性と過剰な情報秘匿を減らすために、情報の機密指定に関する公式のシステムを構築しなければならない。

(b) 機密指定の根拠として、その情報が属する、**原則 9** でリスト化されたカテゴリーのいずれかに対応した、情報の厳密な分類を示すべきであり、また、開示することによって生じうる損害を、その深刻

さの程度、それが起こりうる可能性を含めて、記述しなくてはならない。

(c)機密のレベル設定をする場合は、レベルの決定を正当化する上で想定される損害の程度と、それが起こりうる可能性に釣りあうものでなければならない。

(d)情報が機密扱いにされる時

(i)機密のレベル(設定されている場合)と機密扱いの最長期間を示す保護的な措置が明示されている時。

(ii)そのレベルと期間を定める必要性を正当化する文言を記録に添付されている時。

<注記>：各情報の機密指定の決定理由を述べる文言を添付することの意味は、開示した結果起こり得る具体的な損害について、組織の注意を促すためである。パラグラフごとに印を付けることで、文書中の機密でない部分を開示する際により整合性を保つことが可能となる。

Principle 12: Public Access to Classification Rules

原則 12：機密指定の規則へのパブリック・アクセス

(a)市民は、機密指定を規定する手続きと基準について、それらが効力を発する前に意見を述べる機会を有しなければならない。

(b)市民は、機密指定を定める手続きと基準に関する文書へのアクセスする権利を有する。

Principle 13: Authority to Classify

原則 13：機密指定の権限

(a)法によって定義される、特別に権限が与えられ指名された公務員だけが、情報を機密扱いにすることを申請することができる。指名されていない公務員が、情報が機密扱いにされるべきだと考えた場合、使命された公務員が機密指定の提案を検討するまでの期間、機密扱いとはみなされない。

<注記>：機密指定の権限を定める法規定がない場合、少なくとも委任権限を規則で明確化しなければならない。

(b)機密扱いの決定について責任のある者を特定する情報は、それを秘匿するやむをえない理由が存在しない限り、説明責任を確保するために書面で示されねばならない。

(c)法に基づき指名されたこれらの政治家及び公務員は、一次機密指定権限を、行政上効率的な最少人数の上級職員に割りふる事もできる。

<注記>：機密指定の権限をもつ者の数に関する情報、及び機密情報にアクセスする権限をもつ者の人数及び担当部署並びに氏名に関する情報は公開されなければならない。

Principle 14: Facilitating Internal Challenges to Classification

原則 14：機密指定に対する内部での異議申立の促進

安全保障部門に所属する者を含め、情報が不適切に機密指定されていると考える公務関係者は、情報の機密指定に異議を唱えることができる。

<注記>：安全保障機関には強い秘密主義の風潮があり、又ほとんどの国では、治安職員からの異議申し立てを受理する独立した機関が設置又は指定されておらず、治安関連の情報の暴露は、その他の情報の暴露に比べて厳しい処罰が科されることが多い。安全保障機関の職員が機密指定に異議を唱える独立した機関の設置は絶対事項である。

Principle 15: Duty to Preserve, Manage, and Maintain National Security Information

原則 15：国家安全保障に関する情報を保管し、管理し、維持する義務

(a)公権力は、国際基準に準じて、情報を保管、管理、維持する義務を有する。情報は、法に基づいてのみ、保有、管理、維持の対象から除外される。

(b)情報は適切に維持されるべきである。分類整理のシステムは統合的で、(合法的に機密扱いとなった情報が漏れることがない形で)透明且つ包括的に維持管理されていなければならない。アクセスへの具体的な請求があった場合は、開示されていない情報であってもすべての関連情報の所在が特定できなければならない。

<注記>：これには以下が含まれる：国際公文書協議会(ICA)『公文書へのアクセスの原則』(2012年)、ICA『世界アーカイブ宣言』(2010;ユネスコ承認)、欧州評議会『公文書へのアクセスに関する欧州の政策に関する勧告(2000)13』(2000年)、ICA『人権保護における公文書のポリシー』、「抑圧的な政権における国家安全保障機関の公文書管理(2009年)に関するユネスコと国際公文書協議会作成によるレポートの最新完全版」(1995年)。

(c)各々の公的機関は、保有する機密記録の、詳細で正確なリストを作成し、公開し、定期的に検討し、更新されなければならない。これらのリストは1年ごとに更新される。

Principle 16: Time Limits for Period of Classification

原則 16：機密扱いの期間と期限

(a)情報は国家安全保障上の理由によって秘匿され得るが、正当な国家安全保障上の利益を保護するために必要な限りにおいてのみである。情報を秘匿する決定は、本法の遵守を確保するために、定期的に見直されなければならない。

(b)機密指定を決定する者は、機密扱いが失効する日付、条件、又は出来事について明記しなければならない。

<注記>:機密扱いが失効する期限、又は条件や出来事の詳細は、定期的に見直されなければならない。

(c)無期限に機密扱いにしてもよい情報はない。国家安全保障を理由にした機密扱いの想定される最大期限は、10年とする。見直しはない。

(d)情報は例外的な状況においても、想定された期限を越えて秘匿されてはならない。たとえ異なる意思決定者によっても、その期限を修正されることはできない。

Principle 17: Declassification Procedures

原則17: 機密指定解除の手続き

(a) 機密指定解除の指針を確立し、定期的に更新することを含め、政府が機密指定解除の作業を調整し、監視し、履行する責任を国内法に明記しなければならない。

(b) 公益性をもつ機密指定された情報を優先的に機密指定解除するための手続きは、適切に定めなければならない。原則10のリストのカテゴリーに分類されるような情報を含む、公益性のある情報が、例外的な重要性のために機密扱いにされている場合、それはできる限り迅速に機密解除されなければならない。

(c)国内法で、総括的な（一括、又はサンプリングによる）機密解除のための手続きを制定しなければならない。

(d)それぞれのカテゴリーの機密指定情報について、自動的な機密解除期限を国内法にて定める。機密解除の負担を最小限にするために、可能な場合はいつでも、記録は再検討なしに自動的に機密指定解除される。

(e)文書の機密解除請求について、アクセス可能な公的手続を国内法で定めなければならない。

(f)裁判所、法廷、その他の監督機関、オンブズマン、申立機関によって機密指定が解除されたものも含め、機密指定が解除された文書は積極的に公開するか、さもなければ公的にアクセス可能にしなければ

ればならない。

第4章：情報請求の扱いについての規則

Principle 18: Duty to Consider Request Even If Information Has Been Classified

原則18：情報が機密扱いになっていたとしても、請求を検討する義務

情報が機密扱いになっているという事実は、情報公開の請求にどう対応するかという際に、決定的なことではない。むしろ情報をもつ公的機関は、本法に従い、請求について検討しなければならない。

Principle 19: Duty to Confirm or Deny

原則19：承認又は否認する義務

(a)情報請求を受けた時は、公的機関は、請求されている情報を保有しているかどうかについて、承認又は否認しなければならない。

(b)特別な状況において、特定の情報の存在・不在自体が機密扱いにされている可能性を、司法権が原則3に基づいて認めるとき、特定の請求への回答において、情報の存在を承認又は否認することを拒否する場合には、いかなる場合でも、そのような例外的な措置を必要とするような特定の情報に危害がもたらされるリスクがあることを説明しなければならない。

Principle 20: Duty to State Reasons for Denial in Writing

原則20：拒否の理由を書面で述べる義務

(a)公的機関が、情報の全体あるいは一部に対する請求を拒否する時は、その具体的な理由を、原則3に則り情報請求への対応に関する法律に定められた期間内に、書面で明らかにしなければならない。

<注記>：回答がなされなければならない期限については法に明記されなければならない。要件については、原則25を参照。

(b)当局はまた、請求者に、非開示の権限を与えられている公務員及びその過程に関して十分な情報を提供しなければならない。又、当局の法律遵守について審査するための異議申立方法についても十分な情報を提供しなければならない。

Principle 21: Duty to Recover or Reconstruct Missing Information

原則 21: 遺失した情報を回復又は再構築する義務

- (a) 公的機関が請求者に回答する情報の所在を示すことができず、且つ、その情報を含む記録が、保管され、収集され、あるいは秘密保持が施行されているはずである場合、当該公的機関は請求者に対する将来的開示可能性のために、遺失した情報を回復又は再構築するための合理的な努力をしなければならない。

<注記>：その情報がこれまで収集されたことがない、又は処分されてしまった、あるいは追跡不可能であるといったような、どのような理由があろうとも、この法律は適応される。

- (b) 公的機関の代表者は、その手順が司法の審理の対象となり得るような方法で、情報を回復又は再構築するために定められている手続きのすべてを、誓約の上で、合理的且つ法で定められた時間内に示さなければならない。

<注記>：保管されることが法によって義務付けられている情報が見つからないとき、この件は警察又は司法機関に調査を付託されるべきものである。調査の結果は公開されなければならない。

- (c) 以下の場合、遺失した情報を回復・再構築する義務の程度は特に強い。

(i) その情報が深刻な、又は組織的な人権侵害の申立に関わる時。

(ii) 広範な人権侵害によって特徴づけられる政府から、民主的な形態の政府への移行の期間にある時。

Principle 22: Duty to Disclose Parts of Documents

原則 22: 文書の一部を開示する義務

公開の免除は、特定の情報に対して適用されるのであり、文書全体や、その他の記録の全体に対してではない。制限の妥当性が説明されている特定の情報（「免除情報」）のみが秘匿され得る。ある記録に免除される情報とそうでない情報がともに含まれる場合、免除されていない情報は切り離して公開しなければならない。

Principle 23: Duty to Identify Information Withheld

原則 23: 秘匿された情報を特定する義務

公開することを拒否した情報を保有する公的機関は、その情報をできるだけ詳しく特定しなければならない。少なくとも当該公的機関は、例えばページ数を概算するなどして公開を拒んだ情報の量について公開する義務を持つ。

Principle 24: Duty to Provide Information in Available Formats

原則 24: 入手可能な形式によって情報を提供する義務

公権力は可能な限り、請求者の求める形式で情報を提供しなければならない。

<注記>：このことは、例えば公権力が、障害をもつ人々に対して、アクセスできる形式や技術で、速やかに、費用を上乗せすることなく、国連の障害者権利条約に従って、情報を提供する適切な手段を講じる義務を含む。

Principle 25: Time Limits for Responding to Information Requests

原則 25：情報請求に対する回答の期限

(a) 状況、内部検討、利用可能な場合は独立機関の決定、司法の審理を含め、請求に対する回答期限は、特定時の法によって制定され、実行し得る限り短期間でなければならない。

<注記>：情報アクセス法に定められている要件を踏まえ、実質的な回答が提示されなければならない期限は 20 営業日以内とする。請求に対する回答期限が法に定められていない場合、通常の請求に対する期限は 30 日を超えてはならない。文書の量、複雑さの程度、慎重に取り扱う度合いに応じて、異なる期限を定め得る。

(b) その情報が人の命や自由を守るために必要である場合など、緊急性に基づく情報の必要が立証される場合、期限の短縮が適用され得る。

ORIGINAL

Principle 26: Right to Review of Decision Withholding Information

原則 26：情報の秘匿の決定を審査する権利

(a) 請求者は、情報開示の拒否若しくは請求に関する事例について、独立機関による迅速且つ低費用の審査の権利をもつ。

<注記>：拒否には、黙殺によるものも含まれる。独立機関による審査の対象となる事例には、費用、迅速性、形式も含まれる。

(b) 独立機関は、たとえ秘匿情報であっても、すべての関連情報への十分なアクセスを含む、実効的な審査に必要な資格と資源を有する。

(c) 人は、あらゆる関連問題について、権限のある裁判所や法廷による独立した有効な審査を実施させる資格を有する。

(d) 裁判所が情報非開示を承認する判決を出す場合、特別な状況を除き、**原則 3** に則り、事実に即した根拠及び法的分析を書面で公的に入手できる。

第5章：国家安全保障と情報への権利の司法的側面

Principle 27: General Judicial Oversight Principle

原則27：司法による監視についての一般原則

- 。
- (a)法によって定められた、正当で、独立した、公平な法廷による公正な裁判を受ける基本的な権利は、国家安全保障が持ち出されてもこれに依拠して損なわれてはならない。
- (b)公的機関が国家安全保障を理由に、いずれかの法的手続きに則って、情報の非開示を試みた場合、裁判所にはその情報を調査し、非開示にして良いかどうかを決定する権限が与えられる。裁判所は通常、情報を調べることなく、異議申立を退けることはない。
- <注記>：裁判所は**原則4**を踏まえて、秘匿の必要性のみを主張しながらその主張を支える根拠を述べていない要約書や宣誓供述書に依拠はしない。
- (c)裁判所は、情報の入手を試みる個人が、可能である最大限の範囲で、政府によって提出されたその情報の非開示申請について知り、異議を申し立てられることを保障する。
- (d)裁判所は、公的機関による主張の適法性及び妥当性について裁定を下す。その上で情報を開示するよう強制し、部分的又は全体的な非開示となった場合には、刑事訴訟における訴えの棄却を含む、適切な救済を行うことができる。
- (e)裁判所は、公的機関が情報非開示に対して援用する根拠が適正であるかどうかを独立的に評価する。情報開示請求に関しては、情報が機密扱いであることが決定的な問題と解釈はしない。同様に裁判所は、公的機関が主張する損害の性質と、損害が起こる可能性、そして情報を開示した場合の公共の利益について、**原則3**に従って評価しなければならない。

Principle 28: Public Access to Judicial Processes

原則28：訴訟手続へのパブリック・アクセス

- (a)市民が訴訟手続へアクセスする基本的な権利は、国家安全保障が持ち出されてもこれに依拠して損なわれてはならない。
- (b)判決文は、裁判所による全ての命令を明記し、重要な事実認定と証拠と法的推論を記載し、18歳未満の子どもの利害に関わる場合を除き、公開される。

<注記>：国際法によって、国家安全保障を理由に判決を公に発表する義務を軽減させることは許されない。少年裁判所の裁判手続の記録は公開される事はない。その他の、子どもが関わる訴訟手続の記録は通常、18歳未満の子どもの名前と、身元の特定につながるその他の情報は修正され得る。

(c)市民が司法にアクセスする権利は、この権利の縮小が本原則に従い正当化される場合を除き、次に述べるものへ市民が速やかにアクセスできることを含まなければならない。

(i)裁判における法的推論

(ii)個々の裁判の存在と、その経過に関する情報

(iii)法廷に提出された意見書

(iv)法廷審問と対審

(v)裁判手続の中で有罪判決の根拠となった証拠

<注記>：公正な裁判の要件に関する国際法によって、裁判所は次の様な場合には、部分的又は完全に市民を審判から排除することができる。すなわち、民主主義社会における国家安全保障・倫理・公の秩序・裁判の当事者の私生活における利害を理由とする場合、又は法的公正さが損なわれることを回避する場合である。ただしあらゆる案件において、このような制限が行われる場合には、その必要があり、且つ必要の程度に対応していることが条件である。

(d)国家安全保障を理由として、市民の訴訟手続へのアクセスの制限が絶対に必要だとする、公的機関によって発せられるあらゆる主張に対して、市民は異議を申し立てることができる。

(e)裁判所が、訴訟手続への自由なアクセスの制限を承認するかどうかについて裁定を下す場合、**原則3**に則り、特殊な状況下にある場合を除いて、裁判所は書面により事実(具体的な根拠と法的分析)を公的に入手できる。

<注記>：本法則は、ある国家における、通常は市民がアクセスできない準備手続について規定している現行法の修正も目指している。本法則は、それ以外の場合において、裁判所が市民によるアクセスを許しており、なお且つそのアクセスを却下しようとする試みが国家安全保障を根拠にしている場合には当然該当する。

裁判手続と資料にアクセスする市民の権利は、以下を促進する上でのアクセスの重要性に由来する。

(i)訴訟手続における実務上及び認識上の平等性と公平性

(ii)裁判の当事者による適正且つ誠実な行為

(iii)パブリック・コメントの精度向上

Principle 29: Party Access to Information in Criminal Proceedings

原則 29：刑事訴訟の当事者による情報へのアクセス

(a)裁判所は、被告人が自身の裁判に出廷することを、国家安全保障を理由にして禁止してはならない。

(b)いかなる場合でも、被告人が証拠について精査、反論する機会を持たないまま、有罪判決を下したり、自由を剥奪したりしてはならない。

(c)法的公正さの点から、公的機関は被告人と被告人の弁護人に対し、その個人が問われている容疑と、公正な裁判を確実にを行うために必要なその他の情報を、たとえ機密扱いの情報であっても、**原則 3～6、10、27、28**に従い、公共の利益を考慮した上で、開示しなければならない。

(d)公正な裁判を保証するために必要な情報の開示を公的機関が拒んだ場合、裁判所は審理を中止し、当該機関に対し強制調査を行うことができる。

<注記>：公権力は、情報を秘匿することで起こる不利益を自ら被ると決断してもよいが、情報の秘匿を求める際にその情報を公権力の都合のために援用することはできない。

<注記>：**原則 29 と 30** が、市民による情報へのアクセスに関する本原則の中に含まれているのは、司法による精査と、それと関連して起こる司法の監視を背景とした情報開示とが、情報公開のための重要な手段であるためである。

Principle 30: Party Access to Information in Civil Cases

原則 30：民事訴訟の当事者による情報へのアクセス

(a)民事訴訟における、公権力による情報非開示の要請は全て、**原則 3～6、10、27、28**に従い、公共の利益を考慮した上で、精査される。

(b)人権侵害の被害者は、被った侵害についての情報公開を含む、実効的な救済及び補償を受ける権利を有する。公権力は、この権利に矛盾するような方法で、被害者の主張のために不可欠な情報を秘匿してはならない。

(c)市民は、重大な人権侵害や、国際人道法の重大な違反に関する情報へ、アクセスする権利を有する。

第6章：安全保障部門を監視する機関

Principle 31: Establishment of Independent Oversight Bodies

原則 31：独立監視機関の設置

国家安全情報保護部門の組織を監視するための市民及び市民に基づく団体（NGO、NPO、任意団体、オンブズマンを含む）を中心とした独立の監視機関を必ず設置しなければならない。監視項目には、機

関の活動・規則・指針・財務・管理運営が含まれる。このような監視機関は、監視対象機関からは、組織・運営・財政の面で完全に独立したものでなければならない。

Principle 32: Unrestricted Access to Information Necessary for Fulfillment of Mandate
原則 32 : 任務の遂行のために必要な、情報への無制限のアクセス

(a) 独立監視機関が、その責務を遂行するために必要な全ての情報にアクセスできることは、法によって保証される。情報の機密性のレベルに関わらず、合理的な安全保障上のアクセス条件を満たしていれば、アクセスに制限を設けることは出来ない。

Principle 33: Powers, Resources and Procedures Necessary to Ensure Access to Information
原則 33 : 情報へのアクセスを保証するために必要な権限、資源、手続き

(a) 独立監視機関は、責務を遂行する上で必要とみなされるあらゆる関連情報にアクセスし解釈できるように十分な法的権限を有する。

(i) 上記の権限は少なくとも、現在と過去の行政府の成員と公権力の被雇用者及び契約業者に質問し、関連がある記録を要求・検査し、さらにその物理的な所在場所と施設を視察する権利を含む。

(ii) 独立監視機関は、必要な場合には法執行機関による十分な協力のもと、これらの人物を召喚し記録を取り寄せ、責務を達成する上で必要な情報を保有していると判断された人物に、宣誓の上で証言させる権限を与えられる。

(b) 独立監視機関は、情報を処理する際や証言を求める場合には、証人に対する保護やその他の適正な法の手続きが求める条件とともに、プライバシーに関する規律を十分に考慮に入れる必要がある。

(c) 独立監視機関は、その責務の効率的な実行に関わる情報の特定、アクセス、分析を可能にするために必要な財的・技術的・人的な資源へのアクセスする権利を有する。

(d) 独立監視機関が責務を遂行するために必要な情報にアクセスし、理解を共有できるように、安全保障部門の組織による協力を義務付ける。

(e) 安全保障部門の組織に対し、監視者が責務を達成するために必要と判断した特定の種類の情報を、積極的且つ速やかに、独立監視機関へ開示することを義務付ける。これらの情報には、法や人権に対する違法性の可能性についての情報も含まれるが、それだけに限定はされない。

Principle 34: Transparency of Independent Oversight Bodies

原則 34 : 独立監視機関の透明性

(a) 情報へのアクセスに関する法の適用可能性

公権力の保有する情報へアクセスする市民の権利の行使を規制する法は、安全保障部門の監視機関に対しては適用されない。

(b) 報告

(i) 独立監視機関は、定期的に報告書を作成し、その報告書を公にしなければならない。報告書には、少なくとも、監視機関の責務、人員、予算、実績、そして活動についての情報を含む、監視機関自体についての情報が含まれる。

<注記>：報告書には、安全保障部門の組織の責務、体制、予算、そして全体的な活動についての情報も含まれる。

(ii) 独立監視機関は、主題ごとに具体的な個別事例の分析・調査に関連した公開用の報告書も提出しなければならない。また原則 10 に記載されている種類の情報を含めた、可能な限り多くの、公共の利益に関わる情報を提供することも同様である。

(iii) 独立監視機関は、公開用の報告書の中で、関係のある全ての個人の、プライバシーの権利を含む諸権利を尊重する。

(iv) 独立監視機関は、監視の対象である組織に対し、公開される報告書を速やかに精査し、その中に機密扱いされても良いような資料が含まれていることについて、懸念を提起する機会と権利を有する。何を発表すべきであるかを最終的に決定するのは監視機関に委託される。

(c) 支援活動とアクセス能力

(i) その責務と権限を含む、監視機関の法的原資は、市民にとっては常に入手可能であり、容易にアクセス可能でなければならない。

(ii) 独立監視機関は非識字者や、マイノリティー言語の使用者、又は視力や聴力に障がいがある人たちが、機関の活動に関する情報へアクセスできるための方法と設備を設置する。

(iii) 独立監視機関は、遠隔地に住んでいる個人を含む市民に対し、監視機関と連絡を取ったり、不服を扱う機関へ不服を申し立てたり懸念を表明するために、自由に利用できる各種の方法を提供しなければならない。

(iv) 独立監視機関は、不服申立の機密性と申立人の匿名性を保持できるための仕組みを有する。

Principle 35: Measures to Protect Information Handled by Security Sector Oversight Bodies

原則 35 : 安全保障部門の監視機関が扱う情報を保護するための対策

(a)法は、独立監視機関が、保有している情報を保護するために必要な対策を実行するよう義務付ける。

(b)立法府は、立法府における監視委員会の成員と、独立した、立法府に属さない監視機関の長と成員が、その就任に先だって人物調査を受けるべきであるか、を決定する権限を有する。

(c)人物調査が必要とされた場合、その実施は(1)ふさわしい時機に (2)確立されている指針に沿って (3)政治的な先入観や意図から離れて (4)可能である限りは、人物調査を受ける成員若しくは職員の所属する機関による監視の対象ではない組織によって、行われる。

(d)第 6、7 章中の原則に従い、独立監視機関の成員や職員が、機密扱いその他の秘匿情報を、その機関による報告のための通常の枠組の外で開示した場合、その人物は行政、民事、刑事の、ふさわしい処分を受けなければならない。

Principle 36: Authority of the Legislature to Make Information Public

原則 36 : 立法府が有する、情報公開の権限

立法府は、行政府が国家安全保障を理由に秘匿の権利を主張する情報を含むあらゆる情報を必要と判断した場合には、立法府が制定する手続きに従って、市民に開示する権限を有する。

第7章 : 公務関係者による公益的開示

Principle 37: Categories of Wrongdoing

原則 37 : 不正行為

公務関係者による情報開示は、次に掲げる分類のいずれかに該当する不正行為を示すとき、当該情報の機密指定のいかんに関わらず、**原則 38 から原則 40** までに定める条件を満たす場合において、「保護された開示」であるとみなされる。保護された開示は、過去、現在、及び予見される不正行為に対して適用され得る。

- (a) 刑事犯罪
- (b) 人権侵害
- (c) 国際人道法違反
- (d) 汚職
- (e) 公衆衛生と公共の安全に対する危険
- (f) 環境に対する危険

- (g) 職権濫用
- (h) 誤審
- (i) 資源の不適切な管理又は浪費
- (j) この分類のいずれかに該当する不正行為の開示に対する報復措置
- (k) この 分類のいずれかに該当する事項の意図的な隠蔽

Principle 38: Grounds, Motivation, and Proof for Disclosures of Information Showing Wrongdoing **原則 38 : 不正行為を示す情報開示の理由、動機及び証明**

(a)法は、不正行為を示す情報開示を行う公務関係者を、当該情報が機密又はその他の秘匿情報であるかどうかに関わらず、情報開示の時点で次の条件を満たしている限り、**原則 41** で定める報復措置から保護される。

- (i) 情報開示を行う者が、その情報が**原則 37** で定める分類のいずれかに該当する不正行為を示すことに資すると信ずる合理的な根拠を有している場合。
- (ii) 当該情報の開示が、**原則 38** から**原則 40** までに定める条件を遵守している場合。

(b)保護された開示の動機は、故意に虚偽の開示が行われたと証明される場合を除き、問われない。

(c)保護された開示を行う者は、補足的証拠の提示を要求されず、且つ、情報開示に関する証明責任を課されない。

Principle 39: Procedures for Making and Responding to Protected Disclosures Internally or to Oversight Bodies

原則 39 : 組織内部において又は監視機関に対して行われる保護された開示の手続き及びその対応

(a)組織内部における情報開示

法は、公権力が保護された情報の開示の受理のための内部手続きを確立し、当該情報の受理担当者を指名するよう義務付ける。

(b)独立監視機関に対する情報開示

- (i) 国は、保護された開示を受理及び調査する独立の機関を設置又は指定しなければならない。この機関は、安全保障部門、及びその内部から開示が行われうる 行政府を含むその他の当局からは、組織上及び運営上独立していなければならない。
- (ii) 公務関係者は、最初に組織内部での開示を求められることなく、独立監視機関又は案件の調査権限を有する他の機関に対し、保護された開示を行う権限を付与される。
- (iii) 法律は、独立監視機関に対し、関連するすべての情報へのアクセスを保証し、アクセスの確保に

必要な調査権限を付与しなければならない。この権限には、召喚権限及び宣誓又は確約の下に証言を請求する権限も含まれる。

(c) 情報開示を受理する内部機関及び独立監視機関の義務

原則 37 で定義する保護された開示が組織内部において、又は独立監視機関に対して行われた場合、この開示を受理する機関は、次に掲げる義務を負う。

- (i) 申し立てのあった不正行為を調査し、法律に定められた期間内に案件を解決することを目指して、速やかに措置を講じる。あるいは、開示を行った当事者との協議を経て、調査の権限と適格性を有する機関に案件を付託する。
- (ii) 内密に情報提供を行うことを希望する公務関係者については、その個人が特定されないようにする。匿名通報は、その内容を精査し検討されなければならない。
- (iii) 開示された情報及び開示されたという事実を保護する必要がある。ただし、不正行為を正すためにさらなる情報開示が必要な場合はこの限りではない。
- (iv) 情報開示を行う者に対して、調査の進捗状況及び完了の旨を通知し、且つ可能な限り、講じられた措置又は提言について通知する。

Principle 40: Protection of Public Disclosures

原則 40: 公衆に対する情報開示の保護

本法は**原則 37** で定義する不正行為に関する情報の市民に対する開示を、次に掲げる要件を満たす場合において、**原則 41** で定義する報復措置から保護する。

- (a) 情報開示を行った者が、同一の又は相当に類似する情報を組織内部と独立監視機関のどちらか、あるいはその両方に対して開示しており、且つ、
 - (i) 情報開示を受理した機関が、適用される内部規定に則り、開示された件の調査を拒否した場合又は有効な調査を実施しなかった場合。
 - (ii) 開示を行った者が、合理的且つ法律で定められた期間内に、合理的且つ適切な成果を得なかった場合。
 - (iii) 開示を行った者が、組織内部と独立監視機関のどちらか、あるいはその両方に対する情報開示が、証拠の破壊又は隠蔽、証人に対する妨害、又は開示を行った者本人又は第三者に対する報復措置を招くおそれが相当であると合理的に信じた場合。
 - (iv) 情報開示の対象とし得る既存の内部組織又は独立監視機関が存在していなかった場合。
 - (v) 開示された情報が、人の生命、健康及び安全又は環境を危険にさらす、深刻且つ切迫した危険のある作為又は不作為に関する場合。

(b)開示を行う者が、不正行為を明らかにするために合理的且つ必要な範囲に限定した情報を開示している場合。

<注記>：不正行為を示す情報開示に際して、開示を行う者が不正行為の提示と無関係な資料を開示した場合であっても、その者は、その情報の開示による損害が開示によるいかなる公共の利益にもまさる場合を除いて、報復措置から保護される。

(c)情報開示を行う者が、情報を公開することによる公共の利益が、開示によるいかなる損害にもまさると、合理的に信ずる場合。

<注記>：「合理的に信ずる」との基準は、主観と客観の混合基準である。当該者は、事実その旨を信じており（主観）、そう信ずることはその者にとって合理的でなければならない（客観）。異議を申し立てられた場合、その者は信ずる旨の合理性について弁護する必要に迫られうる。その場合、案件が当該基準を満たし保護された開示と認定されるか否かの判断は、最終的には独立した裁判所又は法廷に委ねられる。

Principle 41: Protection against Retaliation for Making Disclosures of Information Showing Wrongdoing

原則 41：不正行為を示す情報の暴露に対する報復措置からの保護

(a)保護された開示の民事上及び刑事上の責任の免除

原則 37 から原則 40 までに則り情報暴露を行う者は、次に掲げる事項の対象とされる事はない。

(i)刑事訴訟では、機密又はその他の秘匿情報の暴露に対する訴追を含むが、これらに基づいた訴訟からは除外される。

(ii)機密又はその他の秘匿情報の暴露に関する民事訴訟。損害賠償請求及び名誉毀損を申し立てる訴訟を含むが、これらについてもその責任は免除される。

(b)その他の報復措置の禁止

(i)本法は、原則 37 から原則 40 までに則り情報開示を行った、行ったと疑われる、又は行う可能性のある者に対する報復措置を禁止する。

(ii)禁止される報復措置は次の事項を含むが、これらに限定されない。

(iii)行政処分又は罰則。懲戒、報復的な調査、降格、異動、転任、昇進等の見送り、解雇、当事者の評価を貶める目的若しくは可能性のある行為、又は秘密取扱認可の差し止め若しくは取り消しを含むが、これらに限定されない。

(iv)身体的若しくは精神的な危害又はハラスメント。

(v)これら事項のいずれかの脅迫。

(vi)情報開示を行う者以外の者を対象とした行為は、状況の如何により、禁止される報復措置に含まれる。

(c) 独立監視機関及び司法当局による、報復措置の調査

(i) 何人も、保護された開示に関するあらゆる報復措置又はその脅迫について、独立監視機関と司法当局のどちらか、又はその両方に通報する権利を保障される。

(ii) 独立監視機関は、通報された報復措置又はその脅迫について調査しなければならない。当該機関は、報復措置の通報がなくても、調査を開始する権限を付与されている。

(iii) 独立監視機関は、証人の召喚権限及び記録の開示請求権、並びに宣誓又は確約の下に証言を請求する権限を含め、申し立てられたあらゆる報復措置に関して有効な調査を実施するための権限並びに資源が付与される。

(iv) 独立監視機関は、訴えられた報復措置に関する法的手続きが公正且つ法の適性手続きに則って行われることを確実にするため、あらゆる努力を行う。

(v) 独立監視機関は、関係する公的機関に対し、是正措置又は復元的措置を行わせる権限を付与される。これらの措置には、復職、復任、並びに、法的措置の経費、その他の適切な経費、未払いの賃金及び賞与、渡航費、又は損害賠償の支払いが含まれるが、これらに限定されない。

(vi) 独立監視機関は、公的機関に報復措置を禁ずる権限を有する。

(vii) 当該機関は、通報された報復措置に関する調査を合理的且つ法律で定められた期間内に、完了しなければならない。

(viii) 当該機関は、案件の関係者に対して、少なくとも調査の完了を通知し、且つ可能な限り、講じられた措置又は行われた提言を通知しなければならない。

(ix) 関係者は、情報開示に対する行為が報復行為若しくは救済措置又は矯正措置にあたらぬとする独立監視機関の決定について、立法府に申し立てる権利を有する。

(d) 証明責任

公的機関が何人に対してであれ、何らかの不利益をもたらす行為を行った場合、当該公的機関は、その行為が当該情報開示と無関係であると証明する責任を負う。

(e) 権利及び救済措置の放棄の否定

原則 37 から原則 40 までに定めた権利及び是正措置は、いかなる合意、施策、雇用形態又は雇用条件、若しくは紛争仲裁に先んじて行われる合意によっても、放棄又は制限されてはならない。これらの権利及び救済措置を放棄又は制限させるいかなる試みも無効とみなされる。

Principle 42: Encouraging and Facilitating Protected Disclosures

原則 42: 保護された開示の勧奨並びに促進

国家は、保護された開示を促進するため、全ての公権力に対し、原則 37 から原則 40 までに効力を与え

る指針を發布させなければならない。

<注 記>：該当する指針は、最低限次の事項を規定しなければならない。

- (i)不正行為を開示する権利及び 責任に関する助言
- (ii)開示されるべき又は開示されてよい情報の分類
- (iii)開示する際に必要な手続き
- (vi)法律による保護

Principle 43: Public Interest Defence for Public Personnel

原則 43：公務関係者のための公益的保護

(a)公務関係者が、本原則により別段に保護されない情報開示を行ったことにより、刑事訴追若しくは民事訴訟又は行政処分の対象となった場合、法律は、当該開示による公共の利益が非開示による公共の利益にまさると認定される限り、公益的保護を保障しなければならない。

<注記>：この原則は、開示された情報が**原則 37**で規定される分類のいずれにも該当しないために、又は**原則 37**で規定される分類のいずれかに該当する情報が含まれているが**原則 38**から**原則 40**までに規定される手続きに則ることなく開示されたために、保護されていないすべての情報開示にも適用される。

(b) 情報開示による公共の利益が、非開示による公共の利益にまさるか否かの判断において、検察庁及び司法当局は次の事項を検討しなければならない。

- (i)開示の程度が、公益情報の開示のために合理的に必要な程度であるか否か。
- (ii)当該情報開示が引き起こした公共の利益の損害の程度及びその可能性。
- (iii)開示を行う者が、当該情報開示が公共の利益に適うと信じる合理的理由を有しているか否か。
- (vi)開示を行う者が、**原則 38**から**原則 40**で規定される手続きに則り、内部手続を通じて、又は独立監視機関に対して、及び市民に対して、保護された開示を試みたかどうか。
- (v)情報開示を正当化する急迫した状況の有無。

<注記>：無権限の情報開示に対する刑事処罰を規定するあらゆる法律は、**原則 46(b)**と一貫していなくてはならない。この原則は、公務関係者が既に有しているあらゆる表現の**原則 42**及び**原則 46**により保障されるあらゆる保護を制限するものではない。

第8章：公衆への情報暴露に対する制裁又は制約行為の制限

Principle 44: Protection against Penalties for Good Faith, Reasonable Disclosure by Information Officers

原則 44：情報を取り扱う公務員が誠実にを行った合理的な情報暴露に対する制裁からの保護

市民からの情報請求に応じる責任がある者は、合理的且つ誠実に、法に従って開示しようと考えた情報を流出させたことによって制裁を受けることはない。

Principle 45: Penalties for Destruction of, or Refusal to Disclose, Information

原則 45 : 情報の廃棄及び開示拒否に対する処罰

(a)公務関係者は、市民に情報へアクセスをさせないという意図をもって、故意に情報を廃棄したり改ざんした場合には、処罰される。

(b)裁判所や第三者機関によって情報開示命令が出されたとき、当該情報が合理的な期間内に開示されなかった場合、法の定めた手続に従って申立が起こされない限り、その情報非開示の責任者及び当該公的機関は、相応の処罰を受けなければならない。

Principle 46: Limitations on Criminal Penalties for the Disclosure of Information by Public Personnel

原則 46 : 公務関係者による情報暴露に対する刑罰の限度

(a)公務関係者による情報暴露は、第 6 章によって保護されない場合であっても、刑事処罰の対象とはされない。しかし、秘密取扱許可を取り消されたり、免職処分を受けたりといった行政上の制裁を受けることはあり得る。

(b)情報を公にする意図で、公式な許可を得ずに社会や個人に情報を暴露する行為に対して、法律によって刑罰が規定されている場合においては、以下の条件が適用される。

(i) 刑事罰は、法律に明確に定められ、厳密に分類された情報の暴露のみに科される。

<注記> : 開示すれば刑事罰の対象になり得る情報カテゴリーが法律に定められている場合、国家安全保障に与える特殊性と影響力の点で、以下と同程度でなければならない。核兵器に関する技術データ、情報源、暗号、情報収集方法、外交暗号、秘密諜報員の身上情報、政府が所有権を有する知的財産で、それを知られることで国家の安全が害される可能性のあるもの。

(ii) その暴露によって、重大な損害を引き起こす現実的且つ特定可能なリスクがなければならない。

(iii) 法律に規定され、適用される刑事罰は、情報暴露によって引き起こされる損害に相応したものでなくてはならない。

(vi) 当該公務員は、情報を暴露したことによって生じる公共の利益に依拠する保護を、**原則 43** で概要を示したとおり、求めることができる。

Principle 47: Protection against Sanctions for the Possession and Dissemination of Classified Information by Persons Who Are Not Public Personnel

原則 47：公務員以外の者による機密情報の保有及び流布に対する制裁からの保護

(a)公務員以外の者は、機密情報の受領、保有又は市民への暴露に関して、制裁を受けない。

(b)公務員以外の者は、情報を求めたり入手したりしたという事実を理由に、共謀その他の容疑で訴追されることはない。

<注記>：この原則は、情報の入手又は複写等に対する刑事訴追を防止することを目的としている。しかしながら、この原則はその他の犯罪、たとえば情報を探索又は入手する過程での不法侵入や恐喝のような犯罪の免責を目的とするものではない。

<注記>：第三者機関による開示は、過度の機密指定の蔓延を正すという重要な役割を果たす。

Principle 48: Protection of Sources

原則 48：情報源の保護

公務員でない者は、公式の許可を得ずにメディア又は市民に対して行った機密情報暴露容疑の取り調べにおいて、秘密の情報源や公表されていない資料を明かすことを強制されることはない。

<注記>：この原則は、公式の許可を得ずに行った機密情報開示容疑の取り調べにのみ適用され、その他の犯罪には適用されない。

Principle 49: Prior Restraint

原則 49：事前の制限

(a)国家の安全を保護するために公開を事前に制限することは、禁止される。

<注記>：事前の制限とは、司法当局やその他の国家機関によって下される命令で、公務員以外の者がすでに保有する、特定の資料の公表を禁止するものではない。

(b)どのような方法であれ、合法的であるか否かに関わらず、ある情報が「一般的に知ることが可能」と認められている場合、それ以上の公表を阻止しようとするいかなる試みも効力はない。

<注記>：「一般的に知ることが可能」とは、その情報が十分広範に流布されており、その情報を機密にしておく実効的な方法がない事を意味する。

第9章：結びの原則

Principle 50: Relation of these Principles to Other Standards

原則 50：本原則と他の基準との関連

本原則は、公務関係者その他による情報の開示に対し、より強力な保護を定めた国際法、地域法、国内法、もしくは国内法や国際法の条項によって承認された情報へのいかなる権利をも、限定・制限するものではない。最優先法としての位置づけにあることと理解されるべき法である。

Partner Organizations

パートナー機関

以下の 22 の団体が本原則の起草に実質的に寄与し、その普及、広報、及び施行の支援に尽力する意思を明白に持つことを宣言する。

各団体の名称の後には、本部の所在都市（市の記載がないものもある）とその団体が活動する国や地域が記されている。3 地域以上にわたって活動している団体には「グローバル」と記載する。

・ Africa Freedom of Information Centre (Kampala/Africa);

アフリカ情報自由センター（カンパラ/アフリカ）

・ African Policing Civilian Oversight Forum (APCOF) (Cape Town/Africa)

アフリカ警察活動市民監視フォーラム（APCOF）（ケープタウン/アフリカ）

・ Alianza Regional por la Libre Expresione Informacion (Americas)

表現の自由と情報のための地域連合（アメリカ）

・ Amnesty International (London/ global);

アムネスティ・インターナショナル（ロンドン /グローバル）

・ Article 19, the Global Campaign for Free Expression (London/global);

アーティクル 19・自由な表現のためのグローバルキャンペーン（ロンドン /グローバル）

・ Asian Forum for Human Rights and Development (Forum Asia) (Bangkok/Asia);

アジア人権・開発フォーラム（フォーラム・アジア）（バンコク/アジア）

・ Center for National Security Studies (Washington, D.C./Americas);

国家安全保障研究センター（ワシントン DC/アメリカ）

・ Central European University (Budapest/Europe);

中央ヨーロッパ大学（ブダペスト/欧州）

・ Centre for Applied Legal Studies (CALS), Wits University (Johannesburg/South Africa);

ウィッツ大学応用法学研究センター（CALS）（ヨハネスブルグ /南アフリカ）

・ Centre for European Constitutionalization and Security (CECS), University of Copenhagen (Copenhagen/ Europe);

コペンハーゲン大学欧州立憲・安全保障センター（CECS）（コペンハーゲン/欧州）

・ Centre for Human Rights, University of Pretoria (Pretoria/ Africa);

プレトリア大学人権センター（プレトリア /アフリカ）

・ Centre for Law & Democracy (Halifax/ global);

法とデモクラシーセンター（ハリファクス/グローバル）

・ Centre for Peace and Development Initiatives (Islamabad/ Pakistan);

平和と開発イニシアティブセンター（イスラマバード/パキスタン）

・ Centre for Studies on Freedom of Expression and Access to Information (CELE), Palermo
University School of Law (Buenos Aires/ Argentina);

パレルモ大学法学部・表現の自由と情報へのアクセス研究センター（CELE）
（ブエノスアイレス/アルゼンチン）

・ Commonwealth Human Rights Initiative (New Delhi/ Commonwealth);

英連邦人権イニシアティブ（ニューデリー /英連邦）

・ Egyptian Initiative for Personal Rights (Cairo/ Egypt);

エジプト個人の権利イニシアティブ（カイロ/エジプト）、

・ Institute for Defence, Security and Peace Studies (Jakarta/ Indonesia);

防衛・安全保障・平和研究所（ジャカルタ/インドネシア）、

・ Commonwealth Human Rights Initiative (New Delhi/ Commonwealth);

英連邦人権イニシアティブ（ニューデリー /英連邦）

・ Egyptian Initiative for Personal Rights (Cairo/ Egypt);

エジプト個人の権利イニシアティブ（カイロ/エジプト）、

・ Institute for Defence, Security and Peace Studies (Jakarta/ Indonesia);

防衛・安全保障・平和研究所（ジャカルタ/インドネシア）、

・ Institute for Security Studies (Pretoria/ Africa);

安全保障研究所（プレトリア /アフリカ）、

・ International Commission of Jurists (Geneva/ global);

国際法律家委員会（ジュネーブ /グローバル）、

・ National Security Archive (Washington DC/ global);

アメリカ国家安全保障アーカイブ（ワシントン DC/グローバル）、

・ Open Democracy Advice Centre (Cape Town/ Southern Africa); and

オープン・デモクラシー・アドバイス・センター（ケープタウン/南アフリカ）、

・ Open Society Justice Initiative (New York/ global).

オープン・ソサエティー・ジャスティス・イニシアティブ（ニューヨーク/グローバル）。

<記>

「本原則は、情報にアクセスする権利及び人権侵害に関する真実に対する権利に大きく寄与するもので、私は、国連人権理事会によって本原則が採択されるべきだと考える。全ての国が、国家安全保障に関する国内法の解釈に本原則を反映させるべきである。」

ーフランク・ラ・リュ—— 言論と表現の自由の権利に関する国連特別報告者

「当事務所は、安全保障のための国家の能力と個人の自由の保護との間に適切な均衡を保つものとして、

ツワネ原則を歓迎する。」

—カタリナ・ボテロー 表現の自由と情報へのアクセスに関する米州機構(OAS)特別報告者—

「このグローバル原則が起草されたことは、非常に時宜を得ている。」

—パンジー・トゥラクラー アフリカの表現の自由と情報へのアクセスに関する特別報告者—

「欧州評議会議員会議は、このグローバル原則を支持し、欧州評議会全加盟国の当該分野の関係官庁に対して、情報へのアクセスに関する法律の制定と運用を現代化するにあたっては、本原則を考慮に入れることを求める。」

— 欧州評議会議員会議決議 — 2013年10月2日

今回の法案作成に当たって翻訳並びに精査・検証・法文作成にご協力下さいました日本弁護士連合会所属の弁護士の方々、並びに市民活動家の方々やNGOスタッフの皆様に、心より感謝申し上げます。

2014年3月13日 NGO市民プラットフォームジャパン 共同代表 西田博一

ORIGINAL