※未定訳※一部字句修正等を行う可能性があります

国家安全保障と情報への権利に関する国際原則(ツワネ原則)

日本語訳:日本弁護士連合会

※未定訳※一部字句修正等を行う可能性があります

※未定訳※一部字句修正等を行う可能性があります

国家安全保障と
情報への権利に関する
国際原則
(ツワネ原則)

本原則は、70カ国以上の500人を超える専門家との2年以上におよぶ協議を経て、22の団体によって起草され、2013年6月12日に発表された。本原則は、起草の過程で重要な会議が行われた南アフリカ共和国の都市ツワネの名を冠している。

2013年6月12日

※未定訳※一部字句修正等を行う可能性があります

ISBN: 978-1-936133-98-7

Published by
Open Society Foundations
Open Society Justice Initiative
224 West 57th Street
New York, NY 10019 USA
www.opensocietyfoundations.org

Designed by Judit Kovacs | Createch Ltd.
Printed by Createch Ltd. | Hungary

日本語版翻訳　日本弁護士連合会
翻訳協力　森本真由美　内田翔　新津久美子　和田智子　津田秀一　片岡平和　松山晶　鈴木園己
2013 年 11 月

Table of Contents

目 次

Introduction
序

These Principles were developed in order to provide guidance to those engaged in drafting, revising, or implementing laws or provisions relating to the state's authority to withhold information on national security grounds or to punish the disclosure of such information.
本原則は、国家安全保障上の理由により情報の公開を控えたり、そのような情報の暴露を処罰したりする国家の権限に関わる法津又は規定の起草、修正又は施行に携わる人々に指針を提供するために作成された。

They are based on international (including regional) and national law, standards, good practices, and the writings of experts.
本原則は、国際法(世界の一部地域のみを対象とする国際法を含む)及び国内法、各種の基準、優れた実践並びに専門家の論文等に基づいている。

They address national security—rather than all grounds for withholding information. All other public grounds for restricting access should at least meet these standards.
本原則は、国家安全保障上の理由による情報非公開について記述しており、他のあらゆる非公開理由を対象としたものではない。しかし他の理由で情報へのアクセスを制限する場合でも、当局は少なくともこの原則に示された基準を満たさねばならない。

These Principles were drafted by 22 organizations and academic centres (listed in the Annex) in consultation with more than 500 experts from more than 70 countries at 14 meetings held around the world, facilitated by the Open Society Justice Initiative, and in consultation with the four special rapporteurs on freedom of expression and/or media freedom and the special rapporteur on counter-terrorism and human rights:
· Frank LaRue, the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression,
· Ben Emmerson, the UN Special Rapporteur on Counter-Terrorism and Human Rights,
· Pansy Tlakula, the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information,
· Catalina Botero, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, and
· Dunja Mijatovic, the Organization for Security and Co-operation in Europe (OSCE) Representative

on Freedom of the Media.

本原則は、70カ国以上の500人を超える専門家との協議を経て、22の組織及び学術センター(付録にそのﾘｽﾄが記載されている)によって起草された。会議はオープン・ソサエティー・ジャスティス・イニシアティブが進行役を務めて世界各地で 14 回にわたって行われ、表現／ﾒﾃﾞｨｱの自由に関する特別報告者4人及びテロ対策と人権に関する特別報告者1人からも意見を得た。この5人の特別報告者は以下の通り。

- フランク・ラ・ﾘｭ：言論と表現の自由に関する国連特別報告者
- ベン・エマソン：テロ対策と人権に関する国連特別報告者
- パンジー・ﾄｩﾗｸﾗ：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者
- カタリナ・ボテロ：表現の自由に関する米州機構特別報告者
- ﾄﾞｩﾆｬ・ﾐﾔﾄﾋﾞｯﾁ：ﾒﾃﾞｨｱの自由に関する欧州安全保障協力機構(OSCE)代表

Background and Rationale

本原則が起草された背景と理論的根拠

National security and the public's right to know are often viewed as pulling in opposite directions. While there is at times a tension between a government's desire to keep information secret on national security grounds and the public's right to information held by public authorities, a clear-eyed review of recent history suggests that legitimate national security interests are, in practice, best protected when the public is well informed about the state's activities, including those undertaken to protect national security.

国家安全保障と国民の知る権利は、しばしば、対立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情報を秘密にしておきたいと望み、一方で国民には公権力が保有する情報に対する権利がある。この 2 つの事柄の間には、時として緊張関係が存在する。しかしくもりのない目で近年の歴史を振り返ると、正当な国家安全保障上の利益が最大に保護されるのは、実際には、国の安全を守るためになされたものを含めた国家の行為について、国民が十分に知らされている場合だということがわかる。

Access to information, by enabling public scrutiny of state action, not only safeguards against abuse by public officials but also permits the public to play a role in determining the policies of the state and thereby forms a crucial component of genuine national security, democratic participation, and sound policy formulation. In order to protect the full exercise of human rights, in certain circumstances it may be necessary to keep information secret to protect legitimate national security interests.

国家の行為を国民が監視することができ、情報にアクセスすることができるようになれば、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関与できるようになる。つまり情報へのアクセスは、真の国家安全保障、民主的参加、健全な政策決定の極めて重要な構成要素である。そして、人権の行使が完全に保障されるためには、ある一定の状況下では、正当な国家安全保障上の利益を守るために情報を秘密にすることが必要な場合があり得る。

Striking the right balance is made all the more challenging by the fact that courts in many countries demonstrate the least independence and greatest deference to the claims of government when national security is invoked. This deference is reinforced by provisions in the security laws of many countries that trigger exceptions to the right to information as well as to ordinary rules of evidence and rights of the accused upon a minimal showing, or even the mere assertion by the government, of

a national security risk. A government's over-invocation of national security concerns can seriously undermine the main institutional safeguards against government abuse: independence of the courts, the rule of law, legislative oversight, media freedom, and open government.
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、司法が政府の主張に対して極めて従順になり、独立性をほとんど失ってしまうという事実があり、このことが、国家安全保障と国民の知る権利のバランスを正しく保つことをますます困難にしている。国の安全に対するほんのわずかな脅威の提示や、脅威があるという政府の単なる主張があれば、情報への権利や、通常の証拠規則や被告人の権利に例外を設ける治安法を持つ国が多く、そのような法律も政府への追従に拍車をかけている。国の安全が脅かされていると政府が過剰に主張すれば、政府の暴走を防ぐために作られた主なしくみ(裁判所の独立、法の支配、立法府による監視、メディアの自由、開かれた政府)の機能を大幅に損ねてしまうおそれがある。

These Principles respond to the above-described longstanding challenges as well as to the fact that, in recent years, a significant number of states around the world have embarked on adopting or revising classification regimes and related laws. This trend in turn has been sparked by several developments. Perhaps most significant has been the rapid adoption of access to information laws since the fall of the Berlin Wall, with the result that, as of the date that these Principles were issued, more than 5.2 billion people in 95 countries around the world enjoy the right of access to information—at least in law, if not in practice. People in these countries are—often for the first time—grappling with the question of whether and under what circumstances information may be kept secret. Other developments contributing to an increase in proposed secrecy legislation have been government responses to terrorism or the threat of terrorism, and an interest in having secrecy regulated by law in the context of democratic transitions.
本原則は、上述したような積年の難題に応えるものであり、また、近年かなり多くの国が、情報の非公開制度とその関連法を作成・修正し始めているという現実に対応するものである。一方このような政府の動きには、いくつかの理由がある。もっとも大きな理由は、ベルリンの壁の崩壊以降、情報へのアクセスに関する法律の制定が急速に進んできていることだろう。その結果、この原則が発表された時点で、95カ国の52億を超える人々が(実際にはそうでなくても、少なくとも法律上では)情報にアクセスする権利を持っている。こうした国の人々は、情報が秘密にされてよいか、あるいは、どのような状況下なら情報が秘密にされてもよいかという問題に(大抵の場合、初めて)取り組んでいる。他にも、ますます多くの国で秘密保護法が起草されている理由としては、政府によるテロやテロの脅威への対策、そして民主主義への移行過程で、秘密主義を法律で規制することへの関心が高まったことなどがある。

Preamble
前文

The organizations and individuals involved in drafting the present Principles:
この原則の起草に関わった組織及び個人は、

Recalling that access to information held by the state is a right of every person, and therefore that this right should be protected by laws drafted with precision, and with narrowly drawn exceptions, and for oversight of the right by independent courts, parliamentary oversight bodies, and other independent institutions;
国家が保有する情報へのアクセスは全ての人の権利であり、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、また独立した裁判所、国会の監視機関及びその他の独立機関による権利の監視のための法律によって保護されねばならないことを***想起し***、

Recognizing that states can have a legitimate interest in withholding certain information, including on grounds of national security, and emphasizing that striking the appropriate balance between the disclosure and withholding of information is vital to a democratic society and essential for its security, progress, development, and welfare, and the full enjoyment of human rights and fundamental freedoms;
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利益があり得ることを認識し、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り、またその安全、進歩、発展及び福祉並びに人権と基本的自由の完全な享受のために必要不可欠であることを***強調し***、

Affirming that it is imperative, if people are to be able to monitor the conduct of their government and to participate fully in a democratic society, that they have access to information held by public authorities, including information that relates to national security;
人々が政府の行動を監視し、民主主義社会に十全に参加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が絶対必要であると***確信し***、

Noting that these Principles are based on international law and standards relating to the public's right of access to information held by public authorities and other human rights, evolving state

practice (as reflected, ***inter alia***, in judgments of international and national courts and tribunals), the general principles of law recognized by the community of nations, and the writings of experts;
この原則が、当局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・基準、(とりわけ国際及び国内法廷の判決に現れているように)徐々に進化しつつある国家の慣行、国際社会によって認められている法律の一般原則、及び専門家の記述に基づいていることを***明記し***、

Bearing in mind relevant provisions of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples' Rights, the American Convention on Human Rights, the European Convention on Human Rights, and the Council of Europe Convention on Access to Official Documents;
世界人権宣言、市民的及び政治的権利に関する国際規約、人及び人民の権利に関するアフリカ憲章、米州人権条約、欧州人権条約、公文書へのアクセスに関する欧州評議会条約の関連条項に***留意し***、

Further bearing in mind the Declaration of Principles on Freedom of Expression of the Inter-American Commission of Human Rights; the Model Inter-American Law on Access to Information, the Declaration of Principles on Freedom of Expression in Africa, and the Model Law on Access to Information for Africa;
さらに、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に***留意し***、

Recalling the 2004 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and the Inter-American Commission on Human Rights Special Rapporteur on Freedom of Expression; the 2006, 2008, 2009 and 2010 Joint Declarations of those three experts plus the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information; the December 2010 Joint Statement on WikiLeaks of the UN and Inter-American Special Rapporteurs; and the Report on Counter-Terrorism Measures and Human Rights, adopted by the Venice Commission in 2010;
言論・表現の自由に関する国連特別報告者、メディアの自由に関する欧州安全保障協力機構(OSCE)代表、及び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、以上 3 者及び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者による2006年、2008年、2009年、2010年の共同宣言、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を***想起し***、

Further recalling the Johannesburg Principles on National Security, Freedom of Expression and Access to Information adopted by a group of experts convened by Article 19 in 1995, and the Principles of Oversight and Accountability for Security Services in a Constitutional Democracy elaborated in 1997 by the Centre for National Security Studies (CNSS) and the Polish Helsinki Foundation for Human Rights;
さらに、1995年にアーティクル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を***想起し***、

Noting that there are international principles—such as those included in the Model Law on Access to Information in Africa, the UN Guiding Principles on Business and Human Rights ("Ruggie Principles"), the Arms Trade Treaty, the OECD Guidelines for Multinational Enterprises, and the Montreux Document on pertinent international legal obligations and good practices for states related to operations of private military and security companies during armed conflict—that recognize the critical importance of access to information from, or in relation to, business enterprises in certain circumstances; and that some expressly address the need for private military and security companies operating within the national security sector to make certain information public;
一定の状況下で、企業からの、又は企業に関連する情報へのアクセスが決定的に重要であることを認めたものとして、情報へのアクセスに関するアフリカモデル法、ビジネスと人権に関する国連指導原則(ラギー･フレームワーク)、武器貿易条約、経済協力開発機構(OECD)多国籍企業行動指針、武力紛争における民間軍事･警備会社の行動に関する国家の適切な国際法上の義務及びグッドプラクティスに関するモントルー文書などに含まれる国際原則があること、及びそれらの原則の一部は、国家安全保障部門内で運営されている民間軍事･警備会社が特定の情報を公開する必要があることに明確に言及していることを***明記し***、

Noting that these Principles do not address substantive standards for intelligence collection, management of personal data, or intelligence sharing, which are addressed by the "good practices on legal and institutional frameworks for intelligence services and their oversight" issued in 2010 by Martin Scheinin, then the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, at the request of the UN Human Rights Council;

この原則が、国連人権理事会の要請で、2010年、当時テロ撲滅における人権及び基本的自由の促進及び保護に関する国連特別報告者であったマーティン・シェイニンが発表し「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」で言及された、情報収集、個人情報の管理又は情報共有の実際の基準には言及していないことを***明記し***、

Recognizing the importance of effective intelligence sharing among states, as called for by UN Security Council Resolution 1373;
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の重要性を***認識し***、

Further recognizing that barriers to public and independent oversight created in the name of national security increase the risk that illegal, corrupt, and fraudulent conduct may occur and may not be uncovered; and that violations of privacy and other individual rights often occur under the cloak of national security secrecy;
さらに、国家安全保障の名において設けられた公衆への情報公開や独立監視への障害が、違法な、不正な、及び虚偽の行為が発生しそれが暴露されないリスクを高め、プライバシーその他の個人の権利の侵害が国家安全保障上の秘密という覆いの下でしばしば発生することを***認識し***、

Concerned by the costs to national security of over-classification, including the hindering of information-sharing among government agencies and allies, the inability to protect legitimate secrets, the inability to find important information amidst the clutter, repetitive collection of information by multiple agencies, and the overburdening of security managers;
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ことを***懸念し***、

Emphasizing that the Principles focus on the ***public***'s right to information, and that they address the rights to information of detainees, victims of human rights violations, and others with heightened claims to information only to the extent that those rights are closely linked with the public's right to information;
この原則が「公衆の」知る権利に焦点を当てていること、また、公衆の知る権利に密接に結びついている範囲のみにおいて、被拘禁者、人権侵害の犠牲者及びその他の強く情報を求める人々の知る権利に言及していることを***強調し***、

Acknowledging that certain information that should not be withheld on national security grounds may

potentially nonetheless be withheld on various other grounds recognized in international law—including, e.g., international relations, fairness of judicial proceedings, rights of litigants, and personal privacy—subject always to the principle that information may only be withheld where the public interest in maintaining the information's secrecy clearly outweighs the public interest in access to information;
国家安全保障の見地からは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その他の理由で非公開にされる可能性があるが、それは、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と***認識し***、

Desiring to provide practical guidance to governments, legislative and regulatory bodies, public authorities, drafters of legislation, the courts, other oversight bodies, and civil society concerning some of the most challenging issues at the intersection of national security and the right to information, especially those that involve respect for human rights and democratic accountability;
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、その他の監視機関、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・人々に対して実際的な指針を提供することを***希望し***、

Endeavouring to elaborate Principles that are of universal value and applicability;
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***、

Recognizing that states face widely varying challenges in balancing public interests in disclosure and the need for secrecy to protect legitimate national security interests, and that, while the Principles are universal, their application in practice may respond to local realities, including diverse legal systems;
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、その実際の適用は、司法制度の多様性など各地の現実に応じたものであり得ることを***認識し***、

Recommend that appropriate bodies at the national, regional, and international levels undertake steps to disseminate and discuss these Principles, and endorse, adopt, and/or implement them to the extent possible, with a view to achieving progressively the full realization of the right to information as set forth in Principle 1.
原則 1 に定められた知る権利の完全な実現を漸次達成することを目指し、国家、地域、国際レベルの適切な機関がこの原則を流布・議論する措置を取り、承認・採択し、さらにその実行も同時に、ま

たは実行のみを、可能なかぎり行うよう勧告する。

Definitions
語句の定義

In these Principles, unless the context otherwise requires:
この原則においては、文中でとくに指定されない限り、以下のように定義する。

“**Business enterprise within the national security sector**” means a juristic person that carries on or has carried on any trade or business in the national security sector, but only in such capacity; either as a contractor or supplier of services, facilities, personnel, or products including, but not limited to, armaments, equipment, and intelligence. This includes private military and security companies (PMSCs). It does not include juristic persons organized as non-profits or as non-governmental organizations.
「**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(PMSCs)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。

“**Independent**” means institutionally, financially, and operationally free from the influence, guidance, or control of the executive, including all security sector authorities.
「**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。

“**Information**” means any original or copy of documentary material irrespective of its physical characteristics, and any other tangible or intangible material, regardless of the form or medium in which it is held. It includes, but is not limited to, records, correspondence, facts, opinion, advice, memoranda, data, statistics, books, drawings, plans, maps, diagrams, photographs, audio or visual records, documents, emails, logbooks, samples, models, and data held in any electronic form.
「**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。

"**Information of public interest**" refers to information that is of concern or benefit to the public, not merely of individual interest and whose disclosure is "in the interest of the public," for instance, because it is useful for public understanding of government activities.
「**公共の利益となる情報**」とは、公衆に関連のある、又は公衆の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、政府の活動を公衆が理解するために有用であるなどの理由で「公衆のため」であるものを指す。

"**Legitimate national security interest**" refers to an interest the genuine purpose and primary impact of which is to protect national security, consistent with international and national law. (Categories of information whose withholding may be necessary to protect a legitimate national security interest are set forth in Principle 9.) A national security interest is not legitimate if its real purpose or primary impact is to protect an interest unrelated to national security, such as protection of government or officials from embarrassment or exposure of wrongdoing; concealment of information about human rights violations, any other violation of law, or the functioning of public institutions; strengthening or perpetuating a particular political interest, party, or ideology; or suppression of lawful protests.
「**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、正当ではない。

"**National security**" is not defined in these Principles. Principle 2 includes a recommendation that "national security" should be defined precisely in national law, in a manner consistent with the needs of a democratic society.
「**国家安全保障**」という語句は、この原則の中では定義されていない。原則2には、「国家安全保障」は、民主主義社会の必要に応じた形で、国内法で厳密に定義されねばならないという勧告がある。

"Public authorities" include all bodies within the executive, legislative, and judicial branches at all levels of government, constitutional and statutory authorities, including security sector authorities; and non-state bodies that are owned or controlled by government or that serve as agents of the government. "Public authorities" also include private or other entities that perform public functions or services or operate with substantial public funds or benefits, but only in regard to the

performance of those functions, provision of services, or use of public funds or benefits.
「**公権力**」とは、安全保障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、及び政府が所有又は管理する、又は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する、又は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、サービスの提供又は公共基金又は公的給付金の使用に関連する部分のみを指す。

"**Public personnel**" or "**public servant**" refers to current and former public employees, contractors, and sub-contractors of public authorities, including in the security sector. "Public personnel" or "public servant" also include persons employed by non-state bodies that are owned or controlled by the government or that serve as agents of the government; and employees of private or other entities that perform public functions or services or operate with substantial public funds or benefits, but only in regard to the performance of those functions, provision of services, or use of public funds or benefits.
「**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、「公務関係者」又は「公務員」とは、政府が所有又は管理する、又は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、又は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の従業員を指す。ただし、こうした機能の実行、サービスの提供又は公共基金又は公的給付金の使用に関連する部分のみを指す。

"**Sanction,**" when used as a noun, refers to any form of penalty or detriment, including criminal, civil and administrative measures. When used as a verb, "sanction" means to bring into effect such form of penalty or detriment.
「**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。

"**Security sector**" is defined to encompass: (i) security providers, including but not limited to the armed forces, police and other law enforcement bodies, paramilitary forces, and intelligence and security services (both military and civilian); and (ii) all executive bodies, departments, and ministries responsible for the coordination, control, and oversight of security providers.
「**安全保障部門**」の定義には以下が含まれる。 (i) 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。(ii) 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。

Part I: General Principles

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) Everyone has the right to seek, receive, use, and impart information held by or on behalf of public authorities, or to which public authorities are entitled by law to have access.
(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を求め、受け取り、使用し、伝達する権利を有する。

(b) International principles also recognize that business enterprises within the national security sector, including private military and security companies, have the responsibility to disclose information in respect of situations, activities, or conduct that may reasonably be expected to have an impact on the enjoyment of human rights.
(b)国際原則はまた、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は、人権の享受への影響があると合理的に期待される可能性のある状況、活動、行為に関する情報を公開する責任があることを認めている。

(c) Those with an obligation to disclose information, consistent with Principles 1(a) and 1(b), must make information available on request, subject only to limited exceptions prescribed by law and necessary to prevent specific, identifiable harm to legitimate interests, including national security.
(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ず、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) Only public authorities whose specific responsibilities include protecting national security may assert national security as a ground for withholding information.
(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。

(e) Any assertion by a business enterprise of national security to justify withholding information must be explicitly authorized or confirmed by a public authority tasked with protecting national security.
(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。

Note: The government, and only the government, bears ultimate responsibility for national security, and thus only the government may assert that information must not be released if it would harm national security.
注記：政府のみが国家安全保障の究極的な責任をもつ。それゆえに、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。

Public authorities also have an affirmative obligation to publish proactively certain information of public interest.
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) These Principles apply to the exercise of the right of access to information as identified in Principle 1 where the government asserts or confirms that the release of such information could cause harm to national security.
(a)本原則は、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適用する。

(b) Given that national security is one of the weightiest public grounds for restricting information, when public authorities assert other public grounds for restricting access—including international relations, public order, public health and safety, law enforcement, future provision of free and open advice, effective policy formulation, and economic interests of the state—they must at least meet the standards for imposing restrictions on the right of access to information set forth in these Principles as relevant.
(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、アクセス制限の他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、妥当なものとして満たさねばならない。

(c) It is good practice for national security, where used to limit the right to information, to be defined precisely in a country's legal framework in a manner consistent with a democratic society.
(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厳密に定義付けされることは、情報に対する権利を制限してきた国家安全保障にとって望ましいことである。

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

No restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: (1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest; and (2) the law provides for adequate safeguards against abuse, including prompt, full, accessible, and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts.
政府が、その情報の制限が、(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(2)情報制限の妥当性についての独立監視機関による、そして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できない。

(a) ***Prescribed by law***. The law must be accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to understand what information may be withheld, what should be disclosed, and what actions concerning the information are subject to sanction.
(a)「法に基づく」について。 法は、アクセス可能であり、明解であり、綿密且つ正確でなければならない。そうすることで、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、各人が理解できる。

(b) Necessary in a democratic society.
(b)「民主主義社会において必要である」について。

(i) Disclosure of the information must pose a real and identifiable risk of significant harm to a legitimate national security interest.
(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) The risk of harm from disclosure must outweigh the overall public interest in disclosure.
(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公益を上回らなければならない。

(iii) The restriction must comply with the principle of proportionality and must be the least restrictive means available to protect against the harm.

(iii)制限は比例の原則に従わなければならず、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) The restriction must not impair the very essence of the right to information.
(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) ***Protection of a legitimate national security interest***. The narrow categories of information that may be withheld on national security grounds should be set forth clearly in law.
(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るべきである。

Notes: See definition of "legitimate national security interest" in the Definitions section, above. Principle 3(b) is all the more important if national security is not defined clearly in law as recommended in Principle 2.
注記：「語句の定義」に記載されている「正当な国家安全保障上の利益」を見よ。原則3(b)は原則2で推奨されているように、法において国家安全保障が明確に定義されていない場合に一層重要である。

"Public interest" is not defined in these Principles. A list of categories of especially high public interest that should be published proactively and should never be withheld is set forth in Principle 10. A list of categories of wrongdoing that are of high interest to the public, and that public servants should and may disclose without fear of retaliation, is set forth in Principle 37.
「公共の利益」は本原則では定義されていない。積極的に公開されるべきであり、且つ決して非公開であってはならない公益性が特に高い情報カテゴリーのリストは、原則10に明記されている。公衆に関連性が高く、且つ公務員が報復の恐れなしに開示すべき、及び開示可能な不正行為のカテゴリーのリストは原則37に明記されている。

In balancing the risk of harm against the public interest in disclosure, account should be taken of the possibility of mitigating any harm from disclosure, including through means that require the reasonable expenditure of funds. Following is an illustrative list of factors to be considered in deciding whether the public interest in disclosure outweighs the risk of harm:
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。

・*factors favoring disclosure: disclosure could reasonably be expected to (a) promote open discussion of public affairs, (b) enhance the government's accountability, (c) contribute to positive and informed debate on important issues or matters of serious interest, (d) promote effective oversight of expenditure of public funds, (e) reveal the reasons for a government decision, (f) contribute to protection of the environ- ment, (g) reveal threats to public health or safety, or (h) reveal, or help establish accountability for, violations of human rights or international humanitarian law.*

・*情報公開を促す要素:情報公開が(a)公的問題についての開かれた議論を推進し、(b)政府の説明責任を強化し、(c)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し、(d)公的資金の支出についての効率的な監視を推進し、(e)政府の決定の根拠を明らかにし、(f)環境保護に貢献し、(g)公衆衛生又は安全への脅威を明らかにし、あるいは(h)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得る場合。*

・*factors favoring non-disclosure: disclosure would likely pose a real and identifiable risk of harm to a legitimate national security interest;*

・***情報秘匿を促す要素***: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。

・*factors that are irrelevant: disclosure could reasonably be expected to (a) cause embarrassment to, or a loss of confidence in, the government or an official, or (b) weaken a political party or ideology.*

・*無関係な要素:情報公開が(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、あるいは(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。*

The fact that disclosure could cause harm to a country's economy would be relevant in determining whether information should be withheld on that ground, but not on national security grounds.

情報公開が国家経済に損害を与えうる場合は、情報が開示されるかどうかの決定に経済的理由が関係するが、国家安全保障上の理由は関係しない。

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) The burden of demonstrating the legitimacy of any restriction rests with the public authority seeking to withhold information.
(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) The right to information should be interpreted and applied broadly, and any restrictions should be interpreted narrowly.
(b)情報への権利は広義に解釈され且つ適用されるべきであり、いかなる制限も狭義に解釈されるべきである。

(c) In discharging this burden, it is not sufficient for a public authority simply to assert that there is a risk of harm; the authority is under a duty to provide specific, substantive reasons to support its assertions.
(c)この義務を果たすにあたり、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。

> *Note: Any person who seeks access to information should have a fair opportunity to challenge the asserted basis for a risk assessment before an administrative as well as a judicial authority, consistent with Principles 26 and 27.*
> ***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べきである。***

(d) In no case may the mere assertion, such as the issuing of a certificate by a minister or other official to the effect that disclosure would cause harm to national security, be deemed to be conclusive concerning the point for which it is made.
(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) No public authority—including the judiciary, the legislature, oversight institutions, intelligence agencies, the armed forces, police, other security agencies, the offices of the head of state and government, and any component offices of the foregoing— may be exempted from disclosure requirements.

(a)司法、立法、監視機関、情報機関、軍隊、警察やそのほかの安全保障機関、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) Information may not be withheld on national security grounds simply on the basis that it was generated by, or shared with, a foreign state or inter-governmental body, or a particular public authority or unit within an authority.
(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。

Note: Concerning information generated by a foreign state or inter-governmental body, see Principle 9(a)(v).
*注記：他国又は政府間機関によって作成された情報に関しては、原則9 (a) (v)*を参照せよ。

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

All oversight, ombuds, and appeal bodies, including courts and tribunals, should have access to all information, including national security information, regardless of classification level, relevant to their ability to discharge their responsibilities.
裁判所及び法廷を含む全ての監視機関、オンブズマン及び申立機関は、機密のレベルに関わらず、責任を持つ範囲に関連する、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べきである。

Note: This Principle is expanded upon in Principle 32. It does not address disclosure to the public by oversight bodies. Oversight bodies should maintain the secrecy of all information that has been legitimately classified according to these Principles, as set forth in Principle 35.
注記：この原則は原則32において展開される。これは監視機関による公衆への情報公開に言及するものではない。監視機関は、原則35に定められたように、本原則により正当に機密扱いされた全ての情報の機密性を維持するべきである。

Principle 7: Resources
原則 7：資源

States should devote adequate resources and take other necessary steps, such as the issuance of regulations and proper management of archives, to ensure that these Principles are observed in practice.
本原則が実際に順守されることを保証するために、国家は十分な資源を充当し、規則の公布や公文書の適切な維持管理などのその他の必要な措置をとるべきである。

Principle 8: States of Emergency
原則 8:緊急事態

In a time of public emergency which threatens the life of the nation and the existence of which is officially and lawfully proclaimed in accordance with both national and international law, a state may derogate from its obligations regarding the right to seek, receive, and impart information only to the extent strictly required by the exigencies of the situation and only when and for so long as the derogation is consistent with the state's other obligations under international law, and does not involve discrimination of any kind.
国民の生命、及び国内法・国際法に基づき公式に合法的に宣言された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、状況の窮迫が厳密に要求する程度までとし、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とする。

Note: Certain aspects of the right to seek, receive, and impart information and ideas are so fundamental to the enjoyment of non-derogable rights that they should always be fully respected even in times of public emergency. As a non-exhaustive example, some or all of the information in Principle 10 would be of this character.
注記:情報や考えを求め、受け取り、使用し、伝達する権利は、逸脱不可能な権利の享受にとって根本的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尊重されねばならない。すべてを網羅しているわけではないが、原則10のいくつかの又はすべての情報はこの性質を有する。

Part II: Information that May Be Withheld on National Security Grounds, and Information that Should Be Disclosed

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)Public authorities may restrict the public's right of access to information on national security grounds, but only if such restrictions comply with all of the other provisions of these Principles, the information is held by a public authority, and the information falls within one of the following categories:
(a)公権力は国家安全保障を理由に、情報にアクセスする公衆の権利を制限することができるが、そのような制限は、本原則の他のすべての条文に適合しており、その情報が公的機関によって保有されており、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) Information about on-going defense plans, operations, and capabilities for the length of time that the information is of operational utility.
(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

Note: The phrase "for the length of time that the information is of operational utility" is meant to require disclosure of information once the information no longer reveals anything that could be used by enemies to understand the state's readiness, capacity, or plans.
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している。

(ii) Information about the production, capabilities, or use of weapons systems and other military systems, including communications systems.

(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。

Note: Such information includes technological data and inventions, and information about production, capabilities, or use. Information about budget lines concerning weapons and other military systems should be made available to the public. See Principles 10C(3) & 10F. It is good practice for states to maintain and publish a control list of weapons, as encouraged by the Arms Trade Treaty as to conventional weapons. It is also good practice to publish information about weapons, equipment, and troop numbers.
注記：この情報は技術データや発明、及び製造、性能、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線に関する情報は公衆が入手可能でなければならない。原則10C(3)と10F.を参照。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とって優れた実践である。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優れた実践となる。

(iii) Information about specific measures to safeguard the territory of the state, critical infrastructure, or critical national institutions *(**institutions essentielles***) against threats or use of force or sabotage, the effectiveness of which depend upon secrecy;
(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や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。

Note:“Critical infrastructure” refers to strategic resources, assets, and systems, whether physical or virtual, so vital to the state that destruction or incapacity of such resources, assets, or systems would have a debilitating impact on national security.
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、それゆえこれらの資源、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。

(iv) Information pertaining to, or derived from, the operations, sources, and methods of intelligence services, insofar as they concern national security matters; and
(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、及び

(v) Information concerning national security matters that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality; and other diplomatic communications insofar as they concern national security matters.

(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。

Note: It is good practice for such expectations to be recorded in writing.
注記：そのような期待は文書で記録されることが望ましい。

Note: To the extent that particular information concerning terrorism, and counter-terrorism measures, is covered by one of the above categories, the public's right of access to such information may be subject to restrictions on national security grounds in accordance with this and other provisions of the Principles. At the same time, some information concerning terrorism or counterterrorism measures may be of particularly high public interest: see e.g., Principles 10A, 10B, and 10H(1).
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ーで取り上げられる場合、このような情報にアクセスする公衆の権利はこの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。原則10A、10B、10H(1)を参照。

(b) It is good practice for national law to set forth an exclusive list of categories of information that are at least as narrowly drawn as the above categories.
(b)国内法において、少なくとも上記のカテゴリーリストと同程度に範囲を狭めた情報カテゴリーのリストを定めることは優れた実践である。

(c) A state may add a category of information to the above list of categories, but only if the category is specifically identified and narrowly defined and preservation of the information's secrecy is necessary to protect a legitimate national security interest that is set forth in law, as suggested in Principle 2(c). In proposing the category, the state should explain how disclosure of information in the category would harm national security.
(c)国家は、上記のカテゴリーリストに新たなカテゴリー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、そのカテゴリー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。あらたなカテゴリーを提案するに際しては、国家はそのカテゴリー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べきである。

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ー

Some categories of information, including those listed below, are of particularly high public interest given their special significance to the process of democratic oversight and the rule of law. Accordingly, there is a very strong presumption, and in some cases an overriding imperative, that such information should be public and proactively disclosed.
下記に挙げたものを含むいくつかの情報のカテゴリーは、法の支配と民主的監視プロセスにとって特に重要であることを考えると、特に高い公益性を持っている。したがって、その情報は公にされ、積極的に開示されるべきであると強く推定され、場合によってはその公開は最優先の義務となる。

Information in the following categories should enjoy at least a high presumption in favor of disclosure, and may be withheld on national security grounds only in the most exceptional circumstances and in a manner consistent with the other principles, only for a strictly limited period of time, only pursuant to law and only if there is no reasonable means by which to limit the harm that would be associated with disclosure. For certain subcategories of information, specified below as inherently subject to an overriding public interest in disclosure, withholding on grounds of national security can never be justified.
下記のカテゴリーにおける情報は、少なくとも公開が望ましいと強く推定されるべき情報であり、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。すなわち、本原則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ー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. Violations of International Human Rights and Humanitarian Law
A.国際人権法及び人道法上の違反

(1) There is an overriding public interest in disclosure of information regarding gross violations of human rights or serious violations of international humanitarian law, including crimes under international law, and systematic or widespread violations of the rights to personal liberty and security. Such information may not be withheld on national security grounds in any circumstances.
(1)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。

(2) Information regarding other violations of human rights or humanitarian law is subject to a high presumption of disclosure, and in any event may not be withheld on national security grounds in a manner that would prevent accountability for the violations or deprive a victim of access to an effective remedy.
(2)他の人権侵害や人道法違反に関する情報は、公開されることが強く推定されるものであり、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。

(3) When a state is undergoing a process of transitional justice during which the state is especially required to ensure truth, justice, reparation, and guarantees of non-recurrence, there is an overriding public interest in disclosure to society as a whole of information regarding human rights violations committed under the past regime. A successor government should immediately protect and preserve the integrity of, and release without delay, any records that contain such information that were concealed by a prior government.

(3)国家が移行期正義の過程にあり、真実、正義、補償、再発阻止の保証などを確保すること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全体として社会に開示することは最優先の公益性を持つ。後任の政府は、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保護し、保全し、遅滞なく公開するべきである。

Note: See Principle 21(c) regarding the duty to search for or reconstruct information about human rights violations.
注記:人権侵害に関する情報の探索又は再構築の義務については、原則21(c)を参照。

(4) Where the existence of violations is contested or suspected rather than already established, this Principle applies to information that, taken on its own or in conjunction with other information, would shed light on the truth about the alleged violations.
(4)この原則は、人権侵害が立証されている場合よりはその存在について論争があるか疑われている場合において、議論されている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。

(5) This Principle applies to information about violations that have occurred or are occurring, and applies regardless of whether the violations were committed by the state that holds the information or others.
(5)この原則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適用される。

(6) Information regarding violations covered by this Principle includes, without limitation, the following:
(6)この原則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、これに限定されない。

(a) A full description of, and any records showing, the acts or omissions that constitute the violations, as well as the dates and circumstances in which they occurred, and, where applicable, the location of any missing persons or mortal remains.
(a)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、場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。

(b) The identities of all victims, so long as consistent with the privacy and other rights of the victims, their relatives, and witnesses; and aggregate and otherwise anonymous data concerning their number and characteristics that could be relevant in safeguarding human rights.
(b)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。

Note: The names and other personal data of victims, their relatives and witnesses may be withheld from disclosure to the general public to the extent necessary to prevent further harm to them, if the persons concerned or, in the case of deceased persons, their family members, expressly and voluntarily request withholding, or withholding is otherwise manifestly consistent with the person's own wishes or the particular needs of vulnerable groups. Concerning victims of sexual violence, their express consent to disclosure of their names and other personal data should be required. Child victims (under age 18) should not be identified to the general public. This Principle should be interpreted, however, bearing in mind the reality that various governments have, at various times, shielded human rights violations from public view by invoking the right to privacy, including of the very individuals whose rights are being or have been grossly violated, without regard to the true wishes of the affected individuals. These caveats, however, should not preclude publication of aggregate or otherwise anonymous data.
注記:被害者や親族及び証言者の氏名や個人情報は、更なる人権侵害を防ぐ必要がある範囲で、また本人や、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や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、又は受けているまさに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。しかしながらこのことで、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。

(c) The names of the agencies and individuals who perpetrated or were otherwise responsible for the violations, and more generally of any security sector units present at the time of, or otherwise implicated in, the violations, as well as their superiors and commanders, and information concerning the extent of their command and control.
(c)人権侵害を実行した、若しくは責任のある機関と個人の氏名、及びより一般的に、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。

(d) Information on the causes of the violations and the failure to prevent them.
(d)人権侵害の原因及び防止しなかったことに関する情報。

B. Safeguards for the Right to Liberty and Security of Person, the Prevention of Torture and Other Ill-treatment, and the Right to Life
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

Information covered by this Principle includes:
この原則が取り上げる情報は以下のとおり。

(1) Laws and regulations that authorize the deprivation of life of a person by the state, and laws and regulations concerning deprivation of liberty, including those that address the grounds, procedures, transfers, treatment, or conditions of detention of affected persons, including interrogation methods. There is an overriding public interest in disclosure of such laws and regulations.
(1)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には最優先の公益性がある。

Notes: "Laws and regulations," as used throughout Principle 10, include all primary or delegated legislation, statutes, regulations, and ordinances, as well as decrees or executive orders issued by a president, prime minister, minister or other public authority, and judicial orders, that have the force of law. "Laws and regulations" also include any rules or interpretations of law that are regarded as authoritative by executive officials.
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。

Deprivation of liberty includes any form of arrest, detention, imprisonment, or internment.
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。

(2) The location of all places where persons are deprived of their liberty operated by or on behalf of the state as well as the identity of, and charges against, or reasons for the detention of, all persons deprived of their liberty, including during armed conflict.
(2)武力紛争時を含め、国家や国家の代理によって運営され人々の自由が剥奪されたあらゆる場所の所在。及び自由を奪われた人々の身元情報、罪状、拘禁理由。

(3) Information regarding the death in custody of any person, and information regarding any other deprivation of life for which a state is responsible, including the identity of the person or persons killed, the circumstances of their death, and the location of their remains.
(3)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、そうした人々の死亡の状況、遺体の所在を含む)。

Note: In no circumstances may information be withheld on national security grounds that would result in the secret detention of a person, or the establishment and operation of secret places of detention, or secret executions. Nor are there any circumstances in which the fate or whereabouts of anyone deprived of liberty by, or with the authorization, support, or acquiescence of, the state may be concealed from, or otherwise denied to, the person's family members or others with a legitimate interest in the person's welfare.
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。また、いかなる状況であれ、国家によって、又は国家によって権限・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、その人の幸福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。

The names and other personal data of persons who have been deprived of liberty, who have died in custody, or whose deaths have been caused by state agents, may be withheld from disclosure to the general public to the extent necessary to protect the right to privacy if the persons concerned, or their family members in the case of deceased persons, expressly and voluntarily request withholding, and if the withholding is otherwise consistent with human rights. The identities of children who are being deprived of liberty should not be made available to the general public. These caveats, however, should not preclude publication of aggregate or otherwise anonymous data.

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は、当該個人又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. Structures and Powers of Government
C.政府の構造と権力

Information covered by this Principle includes, without limitation, the following:
この原則で取り上げる情報は以下のとおりだが、これに限定されない。

The existence of all military, police, security, and intelligence authorities, and sub- units.
軍隊、警察、安全保障組織や諜報機関及びその下部組織全部の存在。

(1) The laws and regulations applicable to those authorities and their oversight bodies and internal accountability mechanisms, and the names of the officials who head such authorities.
(1)これらの組織や機関、その監視機関、内部説明責任メカニズムに適用され得る法律及び規則。そしてこれらを統轄する当局者の氏名。

(2) Information needed for evaluating and controlling the expenditure of public funds, including the gross overall budgets, major line items, and basic expenditure information for such authorities.
(2)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。

(3) The existence and terms of concluded bilateral and multilateral agreements, and other major international commitments by the state on national security matters.
(3)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. Decisions to Use Military Force or Acquire Weapons of Mass Destruction
D.軍事力行使又は大量破壊兵器の入手の決定

(1) Information covered by this Principle includes information relevant to a decision to commit combat troops or take other military action, including confirmation of the fact of taking such action,

its general size and scope, and an explanation of the rationale for it, as well as any information that demonstrates that a fact stated as part of the public rationale was mistaken.
(1)この原則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、論拠の説明を含む。また、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。

Note: The reference to an action's "general" size and scope recognizes that it should generally be possible to satisfy the high public interest in having access to information relevant to the decision to commit combat troops without revealing all of the details of the operational aspects of the military action in question (see Principle 9).
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(原則9を参照)。

(2) The possession or acquisition of nuclear weapons, or other weapons of mass destruction, by a state, albeit not necessarily details about their manufacture or operational capabilities, is a matter of overriding public interest and should not be kept secret.
(2)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るため秘匿されるべきではない。

Note: This sub-principle should not be read to endorse, in any way, the acquisition of such weapons.
注記:この副原則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と解釈されるべきではない。

E. Surveillance
E.監視

(1) The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.
(1)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、公衆がその情報にアクセスできるべきである。

> *Note: This information includes: (a) the laws governing all forms of surveillance, both covert and overt, including indirect surveillance such as profiling and data-mining, and the types of surveillance measures that may be used; (b) the permissible objectives of surveillance; (c) the threshold of suspicion required to initiate or continue surveillance; (d) limitations on the*

duration of surveillance measures; (e) procedures for authorizing and reviewing the use of such measures; (f) the types of personal data that may be collected and/or processed for national security purposes; and (g) the criteria that apply to the use, retention, deletion, and transfer of these data.

注記:この情報に含まれるものは次のとおり。(a)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 (b)許容できる監視対象 (c)監視を実施又は継続するために必要な疑惑の発端 (d) 監視手段の期間の限度 (e)このような手段の利用の承認・審査手続 (f)国家安全保障上の目的で収集及び/又は加工され得る個人データの種類 (g)こうしたデータの利用、保有、消去、移転に適用する基準

(2) The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance.

(2)公衆は、監視を行う権限を付与された機関についての情報及びそのような監視行為の利用についての統計にアクセスできるべきである。

Note: This information includes the identity of each government entity granted specific authorization to conduct particular surveillance each year; the number of surveillance authorizations granted each year to each such entity; the best information available concerning the number of individuals and the number of communications subject to surveillance each year; and whether any surveillance was conducted without specific authorization and if so, by which government entity.

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ている。

The right of the public to be informed does not necessarily extend to the fact, or operational details, of surveillance conducted pursuant to law and consistent with human rights obligations. Such information may be withheld from the public and those subject to surveillance at least until the period of surveillance has been concluded.

法に従って行われ人権上の義務に矛盾しない監視ならば、必ずしも事実や監視の詳細まで公衆の知る権利に含む必要はない。このような情報は少なくとも監視期間が終了するまでは公表されなくてもよい。

(3) In addition, the public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.
(3)さらに、違法な監視が行われた事実があれば、公衆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限の範囲で情報が公開されるべきである。

(4) These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance.
(4)本原則は情報にアクセスする公衆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。

> *Note: It is good practice for public authorities to be required to notify persons who have been subjected to covert surveillance (providing, at a minimum, information on the type of measure that was used, the dates, and the body responsible for authorizing the surveillance measure) insofar as this can be done without jeopardizing on-going operations or sources and methods.*
> *注記:進行中の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、秘密監視対象となった人に(最低限、利用した監視方法の種類、日付、監視方法の実行に責任のある機関を)通知することを公権力に義務付けるのが望ましい。*

(5)The high presumptions in favor of disclosure recognized by this Principle do not apply in respect of information that relates solely to surveillance of the activities of foreign governments.
(5)この原則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関連する情報には適用されない。

> *Note: Information obtained through covert surveillance, including of the activities of foreign governments, should be subject to disclosure in the circumstances identified in Principle 10A.*
> *注記:他国の行動に対するものを含め、秘密監視行動を通じて得られた情報は原則10Aに示された状況において開示の対象とすべきである。*

F. Financial Information
F.財務情報

Information covered by this Principle includes information sufficient to enable the public to understand security sector finances, as well as the rules that govern security sector finances. Such information should include but is not limited to:

この原則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公衆が理解するために十分な情報が含まれる。このような情報は下記を含むがこれに限定されない。

(1) Departmental and agency budgets with headline items;
(1)主要項目を含めた部門別及び機関別予算

(2) End-of-year financial statements with headline items;
(2)主要項目を含めた年度末財務諸表

(3) Financial management rules and control mechanisms;
(3)財務管理規則と管理システム

(4) Procurement rules; and
(4)資金調達規則 及び

(5) Reports made by supreme audit institutions and other bodies responsible for reviewing financial aspects of the security sector, including summaries of any sections of such reports that are classified.
(5)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章の概要を含む、

G. Accountability Concerning Constitutional and Statutory Violations and Other Abuses of Power
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

This Principle includes information concerning the existence, character, and scale of constitutional or statutory violations and other abuses of power by public authorities or personnel.
この原則は、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. Public Health, Public Safety, or the Environment
H.公衆衛生、市民の安全又は環境

Information covered by this Principle includes:
この原則に取り上げる情報は以下のとおり。

(1) In the event of any imminent or actual threat to public health, public safety, or the environment, all information that could enable the public to understand or take measures to prevent or mitigate

harm arising from that threat, whether the threat is due to natural causes or human activities, including by actions of the state or by actions of private companies.
(1)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か人間活動(国家によるものか民間企業によるものか)かを問わない。

(2) Other information, updated regularly, on natural resource exploitation, pollution and emission inventories, environmental impacts of proposed or existing large public works or resource extractions, and risk assessment and management plans for especially hazardous facilities.
(2)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、そして特に危険な施設のリスク評価と管理計画に関する定期的に更新されるその他の情報。

Part III. A: Rules Regarding Classification and Declassification of Information

第3章. A: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) Whether or not a state has a formal classification process, public authorities are obliged to state reasons for classifying information.

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

> *Note: "Classification" is the process by which records that contain sensitive information are reviewed and given a mark to indicate who may have access and how the record is to be handled. It is good practice to institute a formal system of classification, in order to reduce arbitrariness and excessive withholding.*
>
> *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印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することは優れた実践である。*

(b) The reasons should indicate the narrow category of information, corresponding to one of the categories listed in Principle 9, to which the information belongs, and describe the harm that could result from disclosure, including its level of seriousness and degree of likelihood.

(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) Classification levels, if used, should correspond to the levels and likelihood of harm identified in the justification.

(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た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あるべきである。

(d) When information is classified, (i) a protective marking should be affixed to the record indicating the level, if any, and maximum duration of classification, and (ii) a statement should be included justifying the need to classify at that level and for that period.
(d)情報が機密扱いにされるとき、(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印と、(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すべきである。

Note: Providing a statement justifying each classification decision is encouraged because it makes officials pay attention to the specific harm that would result from disclosure, and because it facilitates the process of declassification and disclosure. Paragraph-by-paragraph marking further facilitates consistency in disclosure of unclassified portions of documents.
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が推奨されるのは、開示した結果起こり得る具体的な損害に公務員の注意を向けるためである。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できる。

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) The public should have the opportunity to comment on the procedures and standards governing classification prior to their becoming effective.
(a)公衆は、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するべきである。

(b) The public should have access to the written procedures and standards governing classification.
(b)公衆は、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を有するべきである。

Principle 13: Authority to Classify
原則 13:機密指定の権限

(a) Only officials specifically authorized or designated, as defined by law, may classify information. If an undesignated official believes that information should be classified, the information may be

deemed classified for a brief and expressly defined period of time until a designated official has reviewed the recommendation for classification.
(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短期間の明確化された期間、機密扱いとみなされ得る。

Note: In the absence of legal provisions controlling the authority to classify, it is good practice to at least specify such delegation authority in a regulation.
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することは優れた実践である。

(b) The identity of the person responsible for a classification decision should be traceable or indicated on the document, unless compelling reasons exist to withhold the identity, so as to ensure accountability.
(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、特定可能であり、書面で示されねばならない。

(c) Those officials designated by law should assign original classification authority to the smallest number of senior subordinates that is administratively efficient.
(c)法に基づき指名されたこれらの公務員は、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べきである。

Note: It is a good practice to publish information about the number of people who have authority to classify, and the number of people who have access to classified information.
注記：機密指定の権限をもつ者の数に関する情報、そして機密情報にアクセスする権限をもつ者の数に関する情報を公開することは良い取り組みである。

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を促進する

Public personnel, including those affiliated with the security sector, who believe that information has been improperly classified may challenge the classification of the information.
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。

Note: Security sector personnel are flagged as deserving of special encouragement to challenge classification given the heightened cultures of secrecy in security agencies, the fact that most countries have not established or designated an independent body to receive complaints from security personnel, and disclosure of security information often results in higher penalties than does disclosure of other information.

注記：安全保障機関には強い秘密主義の風潮があり、またほとんどの国では、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ということを考えれば、安全保障機関の職員は機密指定に異議を唱えるよう特に強く奨励されることが望ましい。

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) Public authorities have a duty to preserve, manage, and maintain information according to international standards. Information may be exempted from preservation, management, and maintenance only according to law.

(a)公権力は、国際基準[1]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) Information should be maintained properly. Filing systems should be consistent, transparent (without revealing legitimately classified information), and comprehensive, so that specific requests for access will locate all relevant information even if the information is not disclosed.

(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整合的で、（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）透明且つ包括的で、アクセスへの具体的な請求があった場合に、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るべきである。

1 These include: International Council on Archives (ICA), ***Principles of Access to Archives:*** (2012); ICA, ***Universal Declaration on Archives*** (2010; endorsed by UNESCO); Council of Europe, ***Recommendation No R(2000)13 on a European policy on access to archives*** (2000); Antonio González Quintana, ICA, ***Archival policies in the protection of human rights:*** an updated and fuller version of the report prepared by UNESCO and the International Council on Archives (1995), concerning the management of the archives of the state security services of former repressive regimes (2009).
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R(2000)13』(2000年)、アントニオ・ゴンザレス・クィンタナ、ICA「人権保護における公文書のポリシー」 かつての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) Each public body should create and make public, and periodically review and update, a detailed and accurate list of the classified records it holds, save for those exceptional documents, if any, whose very existence may legitimately be withheld in accordance with Principle 19.
(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、更新すべきである。ただしその存在自体が、原則19に基づき合法的に秘匿されているような例外的な文書があればそれを除く。

Note: It is good practice to update such lists annually.
注記：これらのﾘｽﾄは1年ごとに更新されることが望ましい。

Principle 16: Time Limits for Period of Classification
原則 16：機密扱いの期間の期限

(a) Information may be withheld on national security grounds for only as long as necessary to protect a legitimate national security interest. Decisions to withhold information should be reviewed periodically in order to ensure that this Principle is met.
(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、本原則の遵守を確保するために、定期的に見直されるべきである。

Note: It is good practice for review to be required by statute at least every five years. Several countries require review after shorter periods.
注記：法令によって、少なくとも5年ごとの見直しを義務付けることが望ましい。より短い期間での見直しを義務付けている国もある。

(b) The classifier should specify the date, conditions, or event on which the classification shall lapse.
(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するべきである。

Note: It is good practice that this time limit, or specification of conditions or event on which classification lapses, is subjected to periodic review.
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、定期的に見直されることが望ましい。

(c) No information may remain classified indefinitely. The presumptive maximum period of classification on national security grounds should be established by law.

(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、法によって定められるべきである。

(d) Information may be withheld beyond the presumptive deadline only in exceptional circumstances, pursuant to a new decision to withhold, made by another decision- maker, and setting an amended deadline.
(d)情報は、例外的な状況においてのみ想定された期限を越えて秘匿され得るが、それは異なる意思決定者によって、期限を修正されて設定され、あらためて秘匿決定がさなれることによる。

Principle 17: Declassification Procedures
原則 17:機密指定解除の手続き

(a) National legislation should identify government responsibility to coordinate, oversee, and implement government declassification activities, including consolidating and regularly updating declassification guidance.
(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すべきである。

(b) Procedures should be put in place to identify classified information of public interest for priority declassification. If information of public interest, including information that falls into categories listed in Principle 10, is classified due to exceptional sensitivity, it should be declassified as rapidly as possible.
(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、適切に定められるべきである。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るべきである。

(c) National legislation should establish procedures for ***en bloc*** (bulk and/or sampling) declassification.
(c)国内法で、総括的な(一括、及び/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するべきである。

(d) National legislation should identify fixed periods for automatic declassification for different categories of classified information. To minimize the burden of declassification, records should be automatically declassified without review wherever possible.

(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で定めるべきである。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べきである。

(e) National legislation should set out an accessible and public procedure for requesting declassification of documents.
(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るべきである。

(f) Declassified documents, including those declassified by courts, tribunals or other oversight, ombuds, or appeal bodies, should be proactively disclosed or otherwise made publicly accessible (for instance, through harmonization with legislation on national archives or access to information or both).
(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するべきである（例えば、国の公文書保管所や情報へのアクセスに関する法律と整合性をとるなど）。

> *Note: This Principle is without prejudice to the proviso regarding other grounds for withholding set forth in preambular paragraph 15.*
> *注記：この原則は、前文パラグラフ15に示される、情報秘匿のための他の理由を考慮するという但し書きを損なわない。*

Note: Additional good practices include the following:
注記：以下は、推奨される追加的な実践である。

- *regular consideration of the use of new technologies in the processes of declassification; and*
- *機密指定解除手続における新たな技術の利用を定期的に検討する。及び、*

- *regular consultation with persons with professional expertise concerning the process for establishing declassification priorities, including both automatic and en bloc declassification.*
- *自動的且つ総括的なものを含め、機密指定解除の優先順位を確立するプロセスに関する専門知識を持つ者との定期的な協議を行う。*

Part III.B: Rules Regarding Handling of Requests for Information

第3章. B: 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

The fact that information has been classified is not decisive in determining how to respond to a request for that information. Rather, the public authority that holds the information should consider the request according to these Principles.

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、本原則に従い、請求について検討するべきである。

Principle 19: Duty to Confirm or Deny

原則19:承認又は否認する義務

(a) Upon receipt of a request for information, a public authority should confirm or deny whether it holds the requested information.

(a)情報請求を受けたときは、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) If a jurisdiction allows for the possibility that, in extraordinary circumstances, the very existence or non-existence of particular information may be classified in accordance with Principle 3, then any refusal to confirm or deny the existence of information in response to a particular request should be based upon a showing that mere confirmation or denial of the existence of the information would pose a risk of harm to a distinct information category designated in a national law or regulation as requiring such exceptional treatment.

(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、国内法又は規定によって示される、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のカテゴリー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) If a public authority denies a request for information, in whole or in part, it should set forth in writing specific reasons for doing so, consistent with Principles 3 and 9, within the period of time specified in law for responding to information requests.
(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及び9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。

Note: See Principle 25 for the requirement that the time in which a response must be given should be set forth in law.
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とする要件については、原則25を参照。

(b) The authority should also provide the requester with sufficient information concerning the official(s) who authorized non-disclosure and the process for doing so, unless to do so would itself disclose classified information, and of avenues for appeal, to allow for an examination of the authority's adherence to the law.
(b)当局はまた、請求者に、そうすることそれ自体が機密情報を開示しない限り、非開示の権限を与えられている公務員及びそのプロセスに関して十分な情報を提供すべきである。また、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すべきである。

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) When a public authority is unable to locate information responsive to a request, and records containing that information should have been maintained, collected, or produced, the authority should make reasonable efforts to recover or reconstruct the missing information for potential disclosure to the requester.

(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、あるいは作ら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。

Note: This Principle applies to information that cannot be located for any reason, for instance because it was never collected, was destroyed, or is untraceable.
注記:その情報がこれまで収集されたことがない、処分されてしまった、追跡不可能であるといったような、どんな理由であろうとも、この原則は、所在が明らかにできない情報に適応される。

(b) A representative of the public authority should be required to indicate under oath and within a reasonable and statutorily specified time all of the procedures undertaken to try to recover or reconstruct the information in such a way that such procedures may be subject to judicial review.
(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行わ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すことを義務付けられるべきである。

Note: When information that is required by law to be maintained cannot be found, the matter should be referred to police or administrative authorities for investigation. The outcome of the investigation should be made public.
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、この件は警察又は行政機関に調査を付託されるべきである。調査の結果は公開されるべきである。

(c) The duty to recover or reconstruct information is particularly strong (i) when the information concerns alleged gross or systematic human rights violations, and/ or (ii) during a transition to a democratic form of government from a government characterized by widespread human rights violations.
(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。すなわち、(i)その情報がな深刻又は組織的な人権侵害の申立に関わる時、及び/又は (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

Exemptions from disclosure apply only to specific information and not to whole documents or other records. Only specific information for which the validity of a restriction has been demonstrated

("exempt information") may be withheld. Where a record contains both exempt and non-exempt information, public authorities have an obligation to sever and disclose the non-exempt information.
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、公権力は、免除されていない情報を切り離して公開する義務がある。

Principle 23: Duty to Identify Information Withheld
原則 23:秘匿された情報を特定する義務

A public authority that holds information that it refuses to release should identify such information with as much specificity as possible. At the least, the authority should disclose the amount of information it refuses to disclose, for instance by estimating the number of pages.
公開することを拒否した情報を保有する公的機関は、そのような情報をできるだけ詳しく特定すべきである。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べきである。

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

Public authorities should provide information in the format preferred by the requester to the extent possible.
公権力は可能な限り、請求者の求める形式で情報を提供すべきである。

> *Note: This includes, for example, the obligation of public authorities to take appropriate measures to provide information to persons with disabilities in accessible formats and technologies in a timely manner and without additional cost, in accordance with the UN Convention on People with Disabilities.*
> *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) Time limits for responding to requests, including on the merits, internal review, decision by an independent body if available, and judicial review should be established by law and should be as short as practicably possible.
(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、法によって制定されなければならず、実行し得る限り短期間でなければならない。

Note: It is considered best practice, in keeping with the requirements set forth in most access to information laws, to prescribe twenty working days or less as the time period in which a substantive response must be given. Where time limits for responding to requests are not set forth in law, the time limit should be no more than 30 days for a standard request. Laws may provide for different time limits in order to take account of different volumes and levels of complexity and sensitivity of documents.
注記:ほとんどの情報アクセス方に定められている要件を踏まえて、実質的な回答が提示されなければならない期限は20営業日以内とするのが最も適切であると考えられる。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日を超えるべきではない。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) Expedited time limits should apply where there is a demonstrated need for the information on an urgent basis, such as where the information is necessary to safeguard the life or liberty of a person.
(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るべきである。

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) A requester has the right to a speedy and low-cost review by an independent authority of a refusal to disclose information, or of matters related to the request.
(a) 請求者は、情報開示の拒否若しくは請求に関する事柄について、独立機関による迅速且つ低費用の審査の権利をもつ。

Note: A refusal may include an implicit or silent refusal. Matters subject to a review by an independent authority include fees, timelines, and format.

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柄には、費用、迅速性、形式も含まれる。

(b) The independent authority should have the competence and resources necessary to ensure an effective review, including full access to all relevant information, even if classified.
(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べきである。

(c) A person should be entitled to obtain independent and effective review of all relevant issues by a competent court or tribunal.
(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べきである。

(d) Where a court makes a ruling that withholding information is warranted, it should make publicly available fact-specific reasons and its legal analysis in writing, except in extraordinary circumstances, and consistent with Principle 3.
(d) 裁判所が情報非開示を承認する判決を出す場合、裁判所は、特殊な状況を除き、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ようにするべきである。

Part IV: Judicial Aspects of National Security and Right to Information

第4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) Invocations of national security may not be relied upon to undermine the fundamental right to a fair trial by a competent, independent, and impartial tribunal established by law.
(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) Where a public authority seeks to withhold information on the ground of national security in any legal proceeding, a court should have the power to examine the information in determining whether the information may be withheld. A court should not ordinarily dismiss a challenge without examining the information.
(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べきである。裁判所は通常、情報を調べることなく、異議申立を退けるべきではない。

Note: In keeping with Principle 4(d), the court should not rely on summaries or affidavits that merely assert a need for secrecy without providing an evidentiary basis for the assertion.
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すべきではない。

(c) The court should ensure that a person seeking access can, to the maximum extent possible, know and challenge the case advanced by the government for withholding the information.
(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べきである。

(d) A court should adjudicate the legality and propriety of a public authority's claim and may compel disclosure or order appropriate relief in the event of partial or full non-disclosure, including the dismissal of charges in criminal proceedings.
(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べきであり、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) The court should independently assess whether the public authority has properly invoked any basis for non-disclosure; the fact of classification should not be conclusive as to the request for non-disclosure of information. Similarly, the court should assess the nature of any harm claimed by the public authority, its likelihood of occurrence, and the public interest in disclosure, in accordance with the standards defined in Principle 3.
(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、独立的に評価するべきである。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だとされてはならない。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) Invocation of national security may not be relied upon to undermine the fundamental right of the public to access judicial processes.
(a)公衆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) Court judgments—setting forth all of a court's orders and including the essential findings, evidence and legal reasoning—should be made public, except where the interest of children under eighteen otherwise requires.
(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、公開されるべきである。

Notes: International law permits no derogation on national security grounds from the obligation to pronounce judgments publicly.
注記:国際法によれば、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。

Records of juvenile court proceedings should not be made public. Records of other judicial proceedings involving children should ordinarily redact the names and other identifying information of children under the age of eighteen.
少年裁判所の裁判手続の記録は公開されるべきではない。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が修正されるべきである。

(c) The public's right of access to justice should include prompt public access to (i) judicial reasoning, (ii) information about the existence and progress of cases, (iii) written arguments submitted to the court, (iv) court hearings and trials, and (v) evidence in court proceedings that forms the basis of a conviction, unless a derogation of this is justified in accordance with these Principles.
(c)公衆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、次に述べるものへ公衆が速やかにアクセスできることを含むべきである。(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。

Note: International law concerning fair trial requirements allows courts to exclude all or part of the public from a hearing for reasons of national security in a democratic society, as well as morals, public order, the interest of the private lives of the parties, or to avoid prejudice to the interests of justice, provided that such restrictions are in all cases necessary and proportionate.
注記:公正な裁判の要件に関する国際法によれば、裁判所は次の様な場合には、部分的又は完全に公衆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) The public should have an opportunity to contest any claim asserted by the public authority that a restriction on public access to judicial processes is strictly necessary on national security grounds.
(d)国家安全保障を理由として、公衆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、公衆は異議を申し立てる機会を有するべきである。

(e) Where a court makes a ruling as to whether a restriction on open access to judicial processes is warranted, it should make publicly available fact-specific reasons and its legal analysis in writing, except in extraordinary circumstances, consistent with Principle 3.
(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ようにすべきである。

Notes: This Principle is not intended to modify a state's existing law regarding preliminary procedures to which the public does not ordinarily have access. It applies only when the court

process would otherwise allow public access and the attempt to deny that access is based on a claim of national security.
注記：本原則は、ある国家における、通常は公衆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を目指しているわけではない。本原則は、それ以外の場合において、裁判所が公衆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のみ、当てはまる。

The public's right of access to court proceedings and materials derives from the significance of access to promoting (i) the actual and perceived fairness and impartiality of judicial proceedings; (ii) the proper and more honest conduct of the parties; and (iii) the enhanced accuracy of public comment.
裁判手続と資料にアクセスする公衆の権利は、以下を促進する上でのアクセスの重要性に由来する。すなわち (i)訴訟手続における実際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一層誠実な行為 (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) The court may not prohibit a defendant from attending his or her trial on national security grounds.
(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) In no case should a conviction or deprivation of liberty be based on evidence that the accused has not had an opportunity to review and refute.
(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、自由を剥奪したりするべきではない。

(c) In the interests of justice, a public authority should disclose to the defendant and the defendant's counsel the charges against a person and any information necessary to ensure a fair trial, regardless of whether the information is classified, consistent with Principles 3-6, 10, 27 and 28, including a consideration of the public interests.
(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ー6、10、27、28に従い、公共の利益を考慮した上で、開示するべきである。

(d) Where the public authority declines to disclose information necessary to ensure a fair trial, the court should stay or dismiss the charges.
(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、裁判所は審理を停止、若しくは起訴を棄却すべきである。

Note: The public authorities should not rely on information to their benefit when claiming secrecy, although they may decide to keep the information secret and suffer the consequences.
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べきではない。

Note: Principles 29 and 30 are included in these Principles concerning public access to information in light of the fact that judicial review, and related disclosures in the context of judicial oversight, are often important means for public disclosure of information.
注記:原則29と30が、公衆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ことが多いためである。

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) All claims of withholding of information by a public authority in a civil case should be reviewed in a manner consistent with Principles 3-6, 10, 27 and 28, including a consideration of the public interests.
(a)民事訴訟における、公権力におる情報非開示の要請は全て、原則3ー6、10、27、28に従い、公共の利益を考慮した上で、精査されるべきである。

(b) Victims of human rights violations have a right to an effective remedy and reparation, including public disclosure of abuses suffered. Public authorities should not withhold information material to their claims in a manner inconsistent with this right.
(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) The public also has the right to information concerning gross human rights violations and serious violations of international humanitarian law.
(c)また公衆は、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の権利も有する。

Part V: Bodies that Oversee the Security Sector

第5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

States should establish, if they have not already done so, independent oversight bodies to oversee security sector entities, including their operations, regulations, policies, finances, and administration. Such oversight bodies should be institutionally, operationally, and financially independent from the institutions they are mandated to oversee.

国家がまだ安全保障部門の組織を監視するための独立監視機関を設置していないならば、これを設置するべきである。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・財政の面で独立しているべきである。

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) Independent oversight bodies should have legally guaranteed access to all information necessary for the fulfillment of their mandates. There should be no restrictions on this access, regardless of the information's level of classification or confidentiality, upon satisfaction of reasonable security access requirements.

(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べきである。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べきではない。

(b) Information to which oversight bodies should have access includes, but is not limited to:

(i) all records, technologies, and systems in the possession of security sector authorities, regardless of form or medium and whether or not they were created by that authority;

(ii) physical locations, objects, and facilities; and

(iii) information held by persons whom overseers deem to be relevant for their oversight

functions.

(b)監視機関がアクセスできる情報には以下のものが含まれるべきであり、しかもこれに限定されない。

⑴安全保障部門の機関が保有する記録、テクノロジー、システムの全て。その形式と媒体、その機関によって作成されたものであるか否かは問われない。

⑵所在場所、備品、施設･設備。

⑶監視職員が、監視職務に関わりがあると判断した個人が保有している情報。

(c) Any obligation of public personnel to maintain secrecy or confidentiality should not prevent them from providing information to oversight institutions. The provision of such information should not be considered a breach of any law or contract imposing such obligations.

(c)機密性を保持する立場にある公務員が負っているあらゆる義務は、彼らが監視機関へ情報を提供することを妨げるべきではない。このような情報の提供は、守秘義務を定めた法律又は契約の違反とみなされるべきではない。

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) Independent oversight bodies should have adequate legal powers in order to be able to access and interpret any relevant information that they deem necessary to fulfill their mandates.

(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ために十分な法的権限を有するべきである。

(i) At a minimum, these powers should include the right to question current and former members of the executive branch and employees and contractors of public authorities, request and inspect relevant records, and inspect physical locations and facilities.

(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べきである。

(ii) Independent oversight bodies should also be given the powers to subpoena such persons and records and hear testimony under oath or affirmation from persons deemed to possess information that is relevant to the fulfillment of their mandates, with the full cooperation of law enforcement agencies, where required.

(ii)また独立監視機関は、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べきである。

(b) Independent oversight bodies, in handling information and compelling testimony, should take account of, inter alia, relevant privacy laws as well as protections against self-incrimination and other requirements of due process of law.
(b)独立監視機関は、情報を処理する際と証言を強制する際には、自己負罪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、とりわけプライバシーに関する法律を考慮に入れるべきである。

(c) Independent oversight bodies should have access to the necessary financial, technological, and human resources to enable them to identify, access, and analyze information that is relevant to the effective performance of their functions.
(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を有するべきである。

(d) The law should require security sector institutions to afford independent oversight bodies the cooperation they need to access and interpret the information required for the fulfillment of their functions.
(d)法は、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解釈できるように、安全保障部門の組織による協力を義務付けるべきである。

(e) The law should require security sector institutions to make proactive and timely disclosures to independent oversight bodies of specific categories of information that overseers have determined are necessary for the fulfillment of their mandates. Such information should include, but not be limited to, possible violations of the law and human rights standards.
(e)法は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べきである。これらの情報には、法や人権基準の違反の可能性についての情報が含まれ、しかもそれだけに限定されるべきではない。

Principle 34: Transparency of Independent Oversight Bodies
原則 34: 独立監視機関の透明性

A. Applicability of Access to Information Laws
情報へのアクセスに関する法の適用可能性

Laws regulating the fulfillment of the public right to access information held by public authorities should apply to security sector oversight bodies.
公権力の保有する情報へアクセスする公衆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も適用されるべきである。

B. Reporting
B. 報告

(1) Independent oversight bodies should be legally required to produce periodic reports and to make these reports publicly available. These reports should include, at a minimum, information on the oversight body itself, including its mandate, membership, budget, performance, and activities.
(1)独立監視機関は、定期的に報告書を作成し、その報告書を公に入手できるよう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べきである。

> *Note: These reports should also include information about the mandate, structure, budget, and general activities of any security sector institution that does not, itself, make such information publicly available.*
> *注記：報告書には、こういった情報を公に入手できるように自分ではしていない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が含まれるべきである。*

(2) Independent oversight bodies should also provide public versions of their reports relating to thematic and case-specific studies and investigations, and should provide as much information as possible concerning matters of public interest, including in respect of those areas listed in Principle 10.
(2)また独立監視機関は、主題ごと及び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するべきであり、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べきである。

(3) In their public reporting, independent oversight bodies should respect the rights of all individuals concerned, including their right to privacy.
(3)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べきである。

(4) Independent oversight institutions should give the institutions subject to their oversight the opportunity to review, in a timely manner, any reports which are to be made public in order to allow them to raise concerns about the inclusion of material that may be classified. The final decision regarding what should be published should rest with the oversight body itself.

(4)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て、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を与えるべきである。何を発表するべきであるかを最終的に決定するのは監視機関自身である。

C. Outreach and Accessibility
アウトリーチとアクセス可能性

(1) The legal basis for oversight bodies, including their mandates and powers, should be publicly available and easily accessible.
(1)その責務と権限を含む、監視機関の法的根拠は、公に入手可能であり、容易にアクセス可能であるべきである。

(2) Independent oversight bodies should create mechanisms and facilities for people who are illiterate, speak minority languages, or are visually or aurally impaired to access information about their work.
(2)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害がある人たちが、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べきである。

(3) Independent oversight bodies should provide a range of freely available mechanisms through which the public, including persons in geographically remote locations, may be facilitated in making contact with them and, in the case of complaints handling bodies, file complaints or register concerns.
(3)独立監視機関は、遠隔地に住んでいる個人を含む公衆に対し、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するべきである。

(4) Independent oversight bodies should have mechanisms that can effectively preserve the confidentiality of the complaints and the anonymity of the complainant.
(4)独立監視機関は、こういった不服申立の機密性と申立人の匿名性を実際上保持できるための仕組みを有するべきである。

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) The law should require independent oversight bodies to implement all necessary measures to protect information in their possession.

(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べきである。

(b) Legislatures should have the power to decide whether (i) members of legislative oversight committees, and (ii) heads and members of independent, non-legislative oversight bodies should be subject to security vetting prior to their appointment.
(b)立法府は、(1)立法府における監視委員会の成員と、(2)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、決定する権限を有するべきである。

(c) Where security vetting is required, it should be conducted (i) in a timely manner, (ii) in accordance with established principles, (iii) free from political bias or motivation, and (iv) whenever possible, by an institution that is not subject to oversight by the body whose members/staff are being vetted.
(c)人物調査が必要とされた場合、その実施は (i)ふさわしい時機に (ii)確立されている指針に沿って(iii)政治的な先入観や意図から離れて (iv)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、行われるべきである。

(d) Subject to the Principles in Parts VI and VII, members or staff of independent oversight bodies who disclose classified or otherwise confidential material outside of the body's ordinary reporting mechanisms should be subject to appropriate administrative, civil, or criminal proceedings.
(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

The legislature should have the power to disclose any information to the public, including information which the executive branch claims the right to withhold on national security grounds, if it deems it appropriate to do so according to procedures that it should establish.
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、そうすることが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、公衆に開示する権限を有するべきである。

Part VI: Public Interest Disclosures by Public Personnel

第6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

Disclosure by public personnel of information, regardless of its classification, which shows wrongdoing that falls into one of the following categories should be considered to be a "protected disclosure" if it complies with the conditions set forth in Principles 38–40. A protected disclosure may pertain to wrongdoing that has occurred, is occurring, or is likely to occur.

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べきである。保護された開示は、過去の、現在の及び予見される不正行為に適用される。

(a) criminal offenses;
(b) human rights violations;
(c) international humanitarian law violations;
(d) corruption;
(e) dangers to public health and safety;
(f) dangers to the environment;
(g) abuse of public office;
(h) miscarriages of justice;
(i) mismanagement or waste of resources;
(j) retaliation for disclosure of any of the above listed categories of wrongdoing; and
(k) deliberate concealment of any matter falling into one of the above categories.

(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) The law should protect from retaliation, as defined in Principle 41, public personnel who make disclosures of information showing wrongdoing, regardless of whether the information is classified or otherwise confidential, so long as, at the time of the disclosure:
(a)法律は、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するべきである。

(i) the person making the disclosure had reasonable grounds to believe that the information disclosed tends to show wrongdoing that falls within one of the categories set out in Principle 37; and
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おり、且つ、
(ii) the disclosure complies with the conditions set forth in Principles 38-40.
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。

(b) The motivation for a protected disclosure is irrelevant except where the disclosure is proven to be knowingly untrue.
(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) A person making a protected disclosure should not be required to produce supporting evidence or bear the burden of proof in relation to the disclosure.
(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るべきではなく、且つ、情報開示に関する証明責任を課されるべきではない。

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. Internal Disclosures

組織内部における情報開示

The law should require public authorities to establish internal procedures and designate persons to receive protected disclosures.

法は、公権力が保護された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べきである。

B. Disclosures to Independent Oversight Bodies

独立監視機関に対する情報開示

(1) States should also establish or identify independent bodies to receive and investigate protected disclosures. Such bodies should be institutionally and operationally independent from the security sector and other authorities from which disclosures may be made, including the executive branch.

(1)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すべきである。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、組織上及び運営上独立しているべきである。

(2) Public personnel should be authorized to make protected disclosures to independent oversight bodies or to another body competent to investigate the matter without first having to make the disclosure internally.

(2)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べきである。

(3) The law should guarantee that independent oversight bodies have access to all relevant information and afford them the necessary investigatory powers to ensure this access. Such powers should include subpoena powers and the power to require that testimony is given under oath or affirmation.

(3)法律は、独立監視機関に対し、関連するすべて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するべきである。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が含まれるべきである。

C. Obligations of Internal Bodies and Independent Oversight Bodies Receiving Disclosures
情報開示を受理する内部機関及び独立監視機関の義務

If a person makes a protected disclosure, as defined in Principle 37, internally or to an independent oversight body, the body receiving the disclosure should be obliged to:
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べきである。

(1) investigate the alleged wrongdoing and take prompt measures with a view to resolving the matters in a legally-specified period of time, or, after having consulted the person who made the disclosure, to refer it to a body that is authorized and competent to investigate;
(1)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。又は、開示を行った者との協議を経て、調査の権限と適格性を有する機関に案件を付託する。

(2) protect the identity of public personnel who seek to make confidential submissions; anonymous submissions should be considered on their merits;
(2)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、その中身自体を検討されるべきである。

(3) protect the information disclosed and the fact that a disclosure has been made except to the extent that further disclosure of the information is necessary to remedy the wrongdoing; and
(3)開示された情報及び開示されたという事実を保護する。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をはこの限りではない。

(4) notify the person making the disclosure of the progress and completion of an investigation and, as far as possible, the steps taken or recommendations made.
(4)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

The law should protect from retaliation, as defined in Principle 41, disclosures to the public of information concerning wrongdoing as defined in Principle 37, if the disclosure meets the following criteria:
法律は、原則37で定義する不正行為に関する情報の公衆に対する開示を、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べきである。

(a) (1) The person made a disclosure of the same or substantially similar information internally and/or to an independent oversight body and:
(a) (1)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) the body to which the disclosure was made refused or failed to investigate the disclosure effectively, in accordance with applicable international standards; or
(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。又は、

(ii) the person did not receive a reasonable and appropriate outcome within a reasonable and legally-defined period of time.
(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。

OR
又は、

(2) The person reasonably believed that there was a significant risk that making the disclosure internally and/or to an independent oversight body would have resulted in the destruction or concealment of evidence, interference with a witness, or retaliation against the person or a third party;
(2)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あると合理的に信じた場合。

OR
又は、

(3) There was no established internal body or independent oversight body to which a disclosure could have been made;
(3)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。

OR
又は、

(4) The disclosure related to an act or omission that constituted a serious and imminent risk of danger to the life, health, and safety of persons, or to the environment.
(4)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。

AND
及び、

(b) The person making the disclosure only disclosed the amount of information that was reasonably necessary to bring to light the wrongdoing;
(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。

Note: If, in the process of disclosing information showing wrongdoing, a person also discloses documents that are not relevant to showing wrongdoing, the person should nonetheless be protected from retaliation unless the harm from disclosure outweighs any public interest in disclosure.
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べきである。

AND
及び、

(c) The person making the disclosure reasonably believed that the public interest in having the information revealed outweighed any harm to the public interest that would result from disclosure.
(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。

Note: The "reasonably believed" test is a mixed objective-subjective test. The person must actually have held the belief (subjectively), and it must have been reasonable for him or her to have done so (objectively). If contested, the person may need to defend the reasonableness of his or her belief and it is ultimately for an independent court or tribunal to determine whether this test has been satisfied so as to qualify the disclosure for protection.
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. Immunity from Civil and Criminal Liability for Protected Disclosures
A.保護された開示の民事上及び刑事上の責任の免除

A person who has made a disclosure, in accordance with Principles 37-40, should not be subject to:
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べきではない。

(1) Criminal proceedings, including but not limited to prosecution for the disclosure of classified or otherwise confidential information; or
(1)刑事訴訟。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、これらに限定されない。

(2) Civil proceedings related to the disclosure of classified or otherwise confidential information, including but not limited to attempts to claim damages and defamation proceedings.
(2)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、これらに限定されない。

B. Prohibition of Other Forms of Retaliation
B.その他の報復措置の禁止

(1) The law should prohibit retaliation against any person who has made, is suspected to have made, or may make a disclosure in accordance with Principles 37-40.
(1)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べきである。

(2) Prohibited forms of retaliation include, but are not limited to, the following:
(2)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。

(a) Administrative measures or punishments, including but not limited to: letters of reprimand, retaliatory investigations, demotion, transfer, reassignment of duties, failure to promote, termination of employment, actions likely or intended to damage a person's reputation, or suspension or revocation of a security clearance;
(a)行政処分又は罰則。懲戒、報復的な調査、降格、異動、転任、昇進の見送り、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。

(b) Physical or emotional harm or harassment; or
(b)身体的若しくは精神的な危害又はハラスメント。

(c) Threats of any of the above.

(c)これら事項のいずれかの脅迫。

(3) Action taken against individuals other than the person making the disclosure may, in certain circumstances, constitute prohibited retaliation.
(3)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うる。

C. Investigation of Retaliation by an Independent Oversight Body and Judicial Authorities
C.独立監視機関及び司法当局による、報復措置の調査

(1) Any person should have the right to report to an independent oversight body and/or to a judicial authority any measure of retaliation, or the threat of retaliation, in relation to protected disclosures.
(1)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べきである。

(2) Independent oversight bodies should be required to investigate a reported retaliation or threat of retaliation. Such bodies should also have the ability to launch investigations in the absence of a report of retaliation.
(2)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るべきである。

(3) Independent oversight bodies should be given the powers and resources to investigate effectively any claimed retaliation, including the powers to subpoena persons and records and hear testimony under oath or affirmation.
(3)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べきである。

(4) Independent oversight bodies should make every effort to ensure that proceedings concerning asserted retaliation are fair and in accordance with due process standards.
(4)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、あらゆる努力を払うべきである。

(5) Independent oversight bodies should have the authority to require the public authority concerned to take remedial or restorative measures, including but not limited to reinstatement; reassignment; and/or the payment of legal fees, other reasonable costs, back pay and related benefits, travel expenses, and/or compensatory damages.

(5)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べきである。これらの措置には、復職、復任、並びに/若しくは、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、及び/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。

(6) Independent oversight bodies should also have the authority to enjoin a public authority from taking retaliatory measures.
(6)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べきである。

(7) Such bodies should complete their investigation into reported retaliation within a reasonable and legally-defined period of time.
(7)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するべきである。

(8) Such bodies should notify relevant persons of at least the completion of an investigation and, as far as possible, the steps taken or recommendations made;
(8)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するべきである。

(9) Persons may also appeal a determination that actions in response to the disclosure do not constitute retaliation, or the remedial or restorative measures, of the independent oversight body to a judicial authority.
(9)また関係者は、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ないとする独立監視機関の決定について、司法当局に申し立てる権利を有する。

D. Burden of Proof
D. 証明責任

If a public authority takes any action adverse to any person, the authority bears the burden of demonstrating that the action was unrelated to the disclosure.
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. No Waiver of Rights and Remedies
E. 権利及び救済措置の放棄の否定

The rights and remedies provided for under Principles 37–40 may not be waived or limited by any agreement, policy, form or condition of employment, including by any pre-dispute arbitration

agreement. Any attempt to waive or limit these rights and remedies should be considered void.
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べきである。

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

States should encourage public officials to make protected disclosures. In order to facilitate such disclosures, states should require all public authorities to issue guidelines that give effect to Principles 37–42.
国家は、公務関係者が保護された開示を行うよう勧奨するべきである。保護された開示を促進するため、国家は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発布させるべきである。

Note: Such guidelines should provide, at a minimum: (1) advice regarding the rights and/or responsibilities to disclose wrongdoing; (2) the types of information that should or may be disclosed; (3) required procedures for making such disclosures; and (4) protections provided for by law.
注記：該当する指針は、最低限次の事項を規定するべきである。(1)不正行為を開示する権利及び/又は責任に関する助言、(2)開示されるべき又は開示されてよい情報の分類、(3)開示する際に必要な手続き、並びに、(4)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) Whenever public personnel may be subject to criminal or civil proceedings, or administrative sanctions, relating to their having made a disclosure of information not otherwise protected under these Principles, the law should provide a public interest defense if the public interest in disclosure of the information in question outweighs the public interest in non-disclosure.
(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限り、公益的保護を保障するべきである。

Note: This Principle applies to all disclosures of information that are not already protected either

because the information does not fall into one of the categories outlined in Principle 37 or the disclosure contains information that falls into one of the categories outlined in Principle 37 but was not made in accordance with the procedures outlined in Principles 38-40.
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) In deciding whether the public interest in disclosure outweighs the public interest in non-disclosure, prosecutorial and judicial authorities should consider:
(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するべきである。

(i) whether the extent of the disclosure was reasonably necessary to disclose the information of public interest;
(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) the extent and risk of harm to the public interest caused by the disclosure;
(ii)当該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) whether the person had reasonable grounds to believe that the disclosure would be in the public interest;
(iii)開示を行う者が、当該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たか否か。

(iv) whether the person attempted to make a protected disclosure through internal procedures and/or to an independent oversight body, and/or to the public, in compliance with the procedures outlined in Principles 38-40; and
(iv)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、及び/又は独立監視機関に対して、及び/又は公衆に対して、保護された開示を試みたかどうか。

(v) the existence of exigent circumstances justifying the disclosure.
(v)情報開示を正当化する急迫した状況の有無。

Note: Any law providing criminal penalties for the unauthorized disclosure of information should be consistent with Principle 46(b).This Principle is not intended to limit any freedom of expression rights already available to public personnel or any of the protections granted under Principles 37-42 or 46.
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自由、又は原則37から原

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。

Part VII: Limits on Measures to Sanction or Restrain the Disclosure of Information to the Public

第7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：情報取り扱い公務員が誠実に行った合理的な情報暴露に対する制裁からの保護

Persons with responsibility for responding to requests for information from the public should not be sanctioned for releasing information that they reasonably and in good faith believed could be disclosed pursuant to law.

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、法に従って開示しうると考えた情報を流出させたことによって制裁を受けるべきではない。

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) Public personnel should be subject to penalties for wilfully destroying or tampering with information with the intent to deny the public access to it.

(a)公務関係者は、市民を情報へアクセスをさせない意図をもって、故意に情報を廃棄したり改ざんした場合には、処罰されるべきである。

(b) If a court or independent body has ordered information to be disclosed, and the information is not disclosed within a reasonable time, the official and/or public authority responsible for the non-disclosure should be subject to appropriate sanctions, unless an appeal is filed in accordance with procedures set forth in law.

(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に、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/又は当該公的機関は、相応の処罰を受けるべきである。

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) The public disclosure by public personnel of information, even if not protected by Part VI, should not be subject to criminal penalties, although it may be subject to administrative sanctions, such as loss of security clearance or even job termination.

(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、刑事処罰の対象とされるべきではない。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) If the law nevertheless imposes criminal penalties for the unauthorized disclosure of information to the public or to persons with the intent that the information will be made public the following conditions should apply:

(b)それにもかかわらず、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べきである：

(i) Criminal penalties should apply only to the disclosure of narrow categories of information that are clearly set forth in law;

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

Note: If national law provides for categories of information the disclosure of which could be subject to criminal penalties they should be similar to the following in terms of specificity and impact on national security: technological data about nuclear weapons; intelligence sources, codes and methods; diplomatic codes; identities of covert agents; and intellectual property in which the government has an ownership interest and knowledge of which could harm national security.

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) The disclosure should pose a real and identifiable risk of causing significant harm;
(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) Any criminal penalty, as set forth in law and as applied, should be proportional to the harm caused; and
(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;そして

(iv) The person should be able to raise the public interest defence, as outlined in Principle 43.
(iv)当該公務員は、情報を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で概要を示したように、求めることができるべきである。

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) A person who is not a public servant may not be sanctioned for the receipt, possession, or disclosure to the public of classified information.
(a)公務員以外の者は、機密情報の受領、保有又は公衆への暴露に関して、制裁を受けない。

(b) A person who is not a public servant may not be subject to charges for conspiracy or other crimes based on the fact of having sought and obtained the information.
(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べきではない。

Note: This Principle intends to prevent the criminal prosecution for the acquisition or reproduction of the information. However, this Principle is not intended to preclude the prosecution of a person for other crimes, such as burglary or blackmail, committed in the course of seeking or obtaining the information.
注記:この原則は、情報の入手又は複写に対する刑事訴追を防止することを目的にしている。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。

Note: Third party disclosures operate as an important corrective for pervasive over-classification.

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

No person who is not a public servant should be compelled to reveal a confidential source or unpublished materials in an investigation concerning unauthorized disclosure of information to the press or public.
公務員でない者は、公式の許可を得ずにメディア又は公衆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べきではない。

Note: This Principle refers only to investigations concerning unauthorized disclosure of information, not to other crimes.
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) Prior restraints against publication in the interest of protecting national security should be prohibited.
(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、禁止されるべきである。

Note: Prior restraints are orders by judicial or other state bodies banning the publication of specific material already in the possession of a person who is not a public servant.
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ある。

(b) If information has been made generally available to the public, by whatever means, whether or not lawful, any effort to try to stop further publication of the information in the form in which it already is in the public domain is presumptively invalid.
(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市民が知ることが可能になっている場合に、その情報がすでに市民社会に存在する形態での、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がないと推定される。

Note: "Generally available" is understood to mean that the information has been sufficiently

widely disseminated that there are no practical measures that could be taken that would keep the information secret.

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と理解される。

Part VIII: Concluding principle

第8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

Nothing in these Principles should be interpreted as restricting or limiting any right to information recognized under international, regional or national law or standards, or any provisions of national or international law that would provide greater protection for disclosures of information by public personnel or others.

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・基準、若しくは国内法又は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・制限するものと解釈されるべきではない。

Annex A: Partner Organizations

付録 A:パートナー機関

The following 22 organizations contributed substantially to the drafting of the Principles, and are committed to working to disseminate, publicize, and help implement them. After the name of each organization is the city, if any, in which it is headquartered and the country or region in which it works. Organizations that undertake substantial work in three or more regions are listed as "global."

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、及び施行の支援にも力を尽くす意思を持っている[2]。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);
  アフリカ情報の自由センター(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 Expresion e Informacion (Americas)
  表現の自由と情報のための地域連合 (南北アメリカ)
- 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/南北アメリカ)

---

2 In addition, Aidan Wills and Benjamin Buckland, of the Geneva Centre for Democratic Control of the Armed Forces (DCAF) but not affiliated with any of the partner organizations, also made especially significant contributions to Part V. on Oversight Bodies and Part VI. on Public Interest Disclosures, as well as to the Principles as a whole.
上記のパートナー機関に所属していないが、軍隊の民主的統制のためのジュネーブセンターのエイダン・ウィルスとベンジャミン・バックランドのことも付言しなくてはならない。2人は、この原則全体についても貢献したが、5章の監視機関の部分と6章の公益的開示の部分に特別に顕著な貢献を果たした。

・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）、

・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）。

“The Principles are a major contribution to the right of access to information and the right to truth concerning human rights violations, and I believe they should be adopted by the Human Rights Council. All states should reflect these Principles in their interpretations of national security law.”

***Frank La Rue**, United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression*

「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。」

― ***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

“My office welcomes the Tshwane Principles as the appropriate balance to ensure state capacity to protect security and the protection of individual freedoms.”

***Catalina Botero**, OAS Special Rapporteur on Freedom of Expression and Access to Information*

「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 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***

“These Global Principles could not have come at a more opportune time.”

***Pansy Tlakula**, Special Rapporteur on Freedom of Expression and Access to Information in Africa*

「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 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***

“The Assembly supports the Global Principles and calls on the competent authorities of all member States of the Council of Europe to take them into account in modernising their legislation and practice concerning access to information.”

Resolution of the Parliamentary Assembly of the Council of Europe, October 2, 2013

「欧州評議会議員会議は、このグローバル原則を支持し、欧州評議会の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***