

○：規定内容が公開されており、中身が確認できる（有料のもの含む） △：規定内容で一部公開の部分がある ×：規定内容が確認できない									○：内容の大部分が情報に関するもの △：内容の一部が情報に関するもの ×：情報に関する規定なし				○：内容の大部分が研究・開発に関するもの △：内容の一部が研究・開発に関するもの ×：研究・開発に関する規定なし				有り：規定がある場合 無し：規定がない場合		左記が無し」の場合は「-」とする	
連番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究・開発に関する規定の有無	研究開発に関連する情報保全規定の有無	研究開発に関連する情報保全規定の概要	出所					
1	日本	特定秘密の保護に関する法律	法律	2013年	2022年	政府	その他	○	①防衛、②外交、③特定有害活動の防止、④テロリズムの防止に関するものとして法律で別表に列挙する事項に関する情報が対象となっており、その漏えい我が国の安全保障に著しく支障を及ぼすおそれがあるため、特に厳格な取り扱いを要するものを、「特定秘密」として定義し、その指定及び有効期間、保護措置、提供、取り扱い者の制限や適正評価について定めている。	○		△	有り	特定秘密として指定される「防衛に関する事項」の中で、「自衛隊の運用又はこれに関する見知り若しくは計画若しくは研究」、「武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のもの」等に係る情報が示されている	(内閣府) https://www.cas.go.jp/jp/tokuteihimitsu/point.pdf					
2	日本	日米相互防衛援助協定等に伴う秘密保護法	法律	1954年	2022年	政府 (防衛省)	多義的技術	○	日米相互防衛援助協定等に基づき米国政府から供与された装備品等についての構造又は性能その他の事項等、及びこれらの事項に係る文書、図画又は物件で、公になっていないものを「特別防衛秘密」として指定し、機密・極秘・秘の区分がある	○		×	無し	-	(防衛省) https://www.mod.go.jp/igo/compliance/guidance/pdf/kamri04-Himitsuhozen.pdf					
3	日本	自衛隊法	法律	1954年	2023年	政府 (防衛省)	多義的技術	○	自衛隊の任務、自衛隊の部隊の組織及び編成、自衛隊の行動及び機能、隊員の身分取扱い等を定める法律であり、その中で自衛隊員の義務として「秘密を守る義務」を規定しており、漏洩時の罰則がある	△		×	無し	-	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=329AC0000000165_20230526_504AC0000000055&keyword=%E8%7%A%A%E8%A1%9B%E9%9A%8A%E6%8B%95					
4	日本	行政文書の管理に関するガイドライン	ガイドライン	2011年	2022年	政府	その他	○	行政機関による公文書の適切な管理要領について示す書であり、その中で「特定秘密以外の公表をしないこととされている情報が記録された行政文書」のうち秘密保全を要する行政文書を秘密文書として極秘文書、秘文書の区分を指定している	○		×	無し	-	(内閣府) https://www8.cao.go.jp/chosei/koubun/hoursai/kanri-gl.pdf					
5	日本	国家公務員法	法律	1947年	2023年	政府 (内閣府)	その他	○	国家公務員たる職員に適用される人事、給与、評価、懲戒、服務等に関する諸規定を定めている法律であり、国家公務員は職務において、職務上知ることのできた秘密を守る義務（守秘義務）について規定しており、漏洩時の罰則がある	△		×	無し	-	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=322AC00000000120					
6	日本	行政手続における特定の個人を識別するための番号の利用等に関する法律	法律	2013年	2023年	政府	その他	○	いわゆるマイナンバー制度の運用について規定するものであり、その中でマイナンバーをその内容に含む個人情報（特定個人情報）の利用範囲を限定する等、一般の個人情報よりも厳格な保護措置を定めており、正当な理由なく特定個人情報を提供することや、業務で知りえたマイナンバーを不正な利益を図る目的で第三者に提供・漏用した場合等の不正行為に対し、罰則が規定されている	○		×	無し	-	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=425AC00000000027_20230609_505AC0000000048&keyword=%E8%A1%8C%E6%94%BF%E6%89%8B%E7%8B%9A%E3%81%AB%E3%81%8A%E3%81%91%E3%82%8B%E7%89%89%E5%AE%9A%E3%81%AE%E5%80%8B%E4%BA%BA%E3%82%92%E8%A0%8B%E3%85%A5%E3%81%99%E3%82%8B%E3%81%9F%E3%82%81%E3%81%AE%E7%95%AA%E5%8B%95%E3%83%8A%E5%8B%A9%E7%84%A8%E7%AD%89%E3%81%AB%E9%9A%E2%E3%81%99%E3%82%8B%E6%83%95%E5%BE%8B					
7	日本	個人情報の保護に関する法律	法律	2003年	2023年	政府	その他	○	個人の権利利益保護のため、個人情報とそれに関連する個人識別符号、要配慮個人情報、仮名加工情報、匿名加工情報、個人関連情報等について定義し、その取り扱いに必要な事項を定めている	○		△	有り	利用目的（本人の同意を得ない利用範囲での個人情報の取り扱い）、適正な取得（不正な取得、同意を得ない要配慮個人情報の取得）や第三者提供（同意を得ない第三者への個人データ提供）等を制限する条文の中で、学術研究機関等が個人情報の授受を行う場合、学術研究の用に供する目的では個人の権利利益をそこなう場合を除いて例外規定が定められている	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=415AC00000000057					
8	日本	金融分野における個人情報保護に関するガイドライン	ガイドライン	2017年	2023年	政府 (個人情報保護委員会・金融庁)	その他	○	個人情報保護法及びその関係法令を踏まえて金融分野の性質及び個人情報利用方法を鑑み、個人情報保護のための格別の措置が講じられるよう必要な措置を講じ、金融分野事業者が個人情報の適正な取扱いの確保に努めて行う義務を定めている	○		×	無し	個人情報保護法に規定される学術研究を目的とした場合の例外規定等について触れられている	(個人情報保護委員会) https://www.ppc.go.jp/files/pdf/230401_kinyubunya_GL.pdf					
9	日本	医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス	ガイドライン	2017年	2023年	政府 (個人情報保護委員会・厚生労働省)	バイオ	○	個人情報保護法及びその関係法令を踏まえて医療・介護分野の性質及び個人情報利用方法を鑑み、個人情報保護のための格別の措置が講じられるよう必要な措置を講じ、医療・介護関係事業者が個人情報の適正な取扱いの確保に関して行う義務を定めている	○		△	有り	個人情報保護法に規定される学術研究を目的とした場合の例外規定等について触れられている	(個人情報保護委員会) https://www.ppc.go.jp/files/pdf/01_jiryokuaigo_guidance5.pdf					
10	日本	経済産業分野のうち個人通信情報を用いた事業分野における個人情報保護ガイドライン	ガイドライン	2017年	2023年	政府 (個人情報保護委員会・経済産業省)	バイオ	○	ヒトゲノム・遺伝子解析研究の進展に伴う新たな医療・健康サービス産業の活発化を背景として、個人通信情報を用いた事業分野における個人情報の適正な取扱いやサービスの質の確保等、適正な事業の実施のために事業者が遵守すべき事項を示すもの 個人情報保護法における各種用語について、個人情報保護法を用いたサービスにおける定義を示しているほか、個人通信情報取り扱い事業者等の義務について定めている	○		×	無し	-	(個人情報保護委員会) https://www.ppc.go.jp/files/pdf/230401_genetec_data_GL.pdf					
11	日本	電気通信事業者における個人情報保護に関するガイドライン	ガイドライン	2022年	2023年	政府 (個人情報保護委員会・総務省)	サイバー	○	電気通信事業者に対し、個人情報保護法や電気通信事業法に規定される通信の秘密に関する事項その他の個人情報の適正な取扱いについて指導を示すものであり、個人情報取り扱いに係る電気通信事業者の義務、各種電気通信事業者で扱う情報の取り扱いについて規定している	○		△	有り	個人情報保護法に規定される学術研究を目的とした場合の例外規定等について触れられている	(個人情報保護委員会) https://www.ppc.go.jp/files/pdf/230616_telecom_GL.pdf					
12	日本	電気通信事業法	法律	1984年	2023年	政府 (総務省)	サイバー	○	電気通信事業の運営及び電気通信役務の提供に関する必要な事項を定めたものであり、電気通信事業者は取り扱う情報について、通信の秘密を侵してはならないこと、及び通信に関して知りえた他人の秘密を守らなければならない義務が規定されている。令和5年の改正では、Webサイトやアプリケーションの利用者情報を第三者に送信する際の規制対象行為が定められた	△		×	無し	-	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=359AC00000000086_20230616_504AC0000000070&keyword=%E9%9B%BB%E6%80%B7%E9%80%8A%E4%BF%A1%E4%BA%8B%E6%A5%AD%E6%B3%95					
13	日本	JISQ15001:2017	ガイドライン	1999年	2017年	JIS	その他	○	個人情報保護法に定める事業者の義務の遵守、及び個人情報取り扱い事業者が保有している個人情報や個人データについて把握し、個人情報保護のための必要体制・経営資源を確保するとともに、その体制を定期的に見直す個人情報保護マネジメントシステムについて規定した産業標準規格	○		×	無し	-	(JIS) https://webdesk.jsa.or.jp/books/W11M0120					
14	日本	行政機関が保有する情報の公開に関する法律	法律	1999年	2022年	政府	その他	○	行政機関が保有している行政文書を、原則一般の情報の公開請求に応じ公開することを定めた法律であり、不開示情報として以下のような6類型の詳細を定めている。 ・個人に関する情報であって特定の個人を識別することができるもの、公にすることによって個人の権利利益を害するもの ・法人等に関する情報又は事実を窺む個人の当該事業に関する情報 ・公にすることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利を被るおそれがあるもの ・公にすることにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共安全の維持に支障を及ぼすおそれがあるもの ・国の機関、独立行政法人等、地方公共団体及び地方独立行政法人の内部又は相互間における審議、検討又は協議に関する情報 ・国の機関、独立行政法人等、地方公共団体又は地方独立行政法人が行う事務又は事実に関する情報	○		△	有り	行政文書の定義の中で、「政府で定める研究所その他の施設において、政府で定めるところにより、歴史的若しくは文化的な資料又は学術研究用の資料として特別の管理がされているもの」は除くとされている	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=411AC00000000042_20220401_503AC00000000037&keyword=%E6%83%85%E5%A0%B1%E5%85%AC%E9%96%8B%E6%8B%95					
15	日本	独立行政法人の保有する情報の公開に関する法律	法律	2001年	2023年	政府	その他	○	独立行政法人が保有している法人文書を、原則一般の情報の公開請求に応じ公開することを定めた法律であり、不開示情報として以下のような4類型の詳細を定めている ・個人に関する情報であって特定の個人を識別することができるもの、公にすることによって個人の権利利益を害するもの ・法人その他の団体に関する情報又は事実を窺む個人の当該事業に関する情報 ・国の機関、独立行政法人等、地方公共団体及び地方独立行政法人の内部又は相互間における審議、検討又は協議に関する情報であって、公にすることにより、率直な意見の交換若しくは意思決定の中立性が不当に損なわれる等のおそれのあるもの ・国の機関、独立行政法人等、地方公共団体又は地方独立行政法人が行う事務又は事実に関する情報であって、公にすることにより国の安全を害する、犯罪の予防に支障をきたす等のおそれがあるもの	○		△	有り	行政文書の定義の中で、「政府で定める博物館その他の施設において、政府で定めるところにより、歴史的若しくは文化的な資料又は学術研究用の資料として特別の管理がされているもの」は除くとされている また、不開示情報の四の中で、「調査研究に係る事務に関し、その公正かつ客観的な遂行を不当に阻害するおそれのあるもの」が該当している	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=413AC00000000140_20230607_505AC00000000047&keyword=%E6%83%85%E5%A0%B1					
16	日本	サイバーセキュリティ基本法	法律	2014年	2022年	政府	サイバー	○	我が国のサイバーセキュリティに関する施策に関し、基本理念、国及び地方公共団体の責務等、及びサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の実施について根拠を規定している	○		△	有り	国はサイバーセキュリティに関する研究開発を推進することが定められている他、大学その他の教育研究機関は、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体等が実施するサイバーセキュリティに関する施策に協力する義務が定められている	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=426AC10000000104_20220617_504AC0000000068&keyword=%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%A3%E3%83%A8%E3%83%86%E3%82%A3					
17	日本	政府機関等の情報セキュリティ対策のための統一基準	ガイドライン	2005年	2023年	NISC	サイバー	○	政府機関において統一的に必要なとされる情報セキュリティ対策を示すものであり、組織の整備すべき体制・計画、情報セキュリティ関係底層の運用、情報の取り扱い要領、外部委託に関する事項、情報のライフサイクルやセキュリティ要件とうについて規定している。 その中で政府機関で取り扱う情報の重要性に応じた「機密性」、「完全性」、「可用性」の観点からの情報の格付け区分を定義している	○		×	無し	-	(NISC) https://www.nisc.go.jp/pdf/policy/general/kijyun30.pdf					
18	日本	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針	ガイドライン	2015年	2023年	NISC	その他	○	情報通信、金融、航空、空港、鉄道、電力、ガス、医療、水道、物流等の重要インフラ事業者等が作成すべき安全基準等に規定することが望ましい内容を示したものの、 その中で各事業者が取り扱う情報の分類と取り扱いについて、対策する際の参照先として以下が挙げられている。 ・「JIS Q 27002:2014」 8.2.1 ～ 8.2.3 ・「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 3.1.1 ・「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 3.1.1	○		×	無し	-	(NISC) https://www.nisc.go.jp/pdf/policy/infra/shishin5rev.pdf					
19	日本	水道分野における情報セキュリティガイドライン	ガイドライン	2005年	2019年	厚生労働省	サイバー	○	厚生労働省から水道事業者に対し、水道事業で取り扱う情報について、格付け（重要度による分類：A～D）を行うとともに、それに応じた取扱制限の基準、期限を明示するための手順を用意することを求めている。 また電磁的記録については機密性、完全性及び可用性の観点から要機密情報、要保全情報、要安定情報に分類し、画面については機密性の観点から分類することを示している。	○		×	無し	-	(厚生労働省) https://www.city.saitama.jp/002/002/011/012/p015553_d/fil/guide_ver4.pdf					
20	日本	電力制御システムセキュリティガイドライン	ガイドライン	2015年	2019年	一般社団法人 日本電気協会	サイバー	○	電力インフラ事業者による電力制御システム等のサイバーセキュリティ確保を目的として、実施すべきセキュリティ対策について規定している物であり、組織のとりべき体制や電力制御システムのシステム面・運用面のセキュリティ対策を示している	○		×	無し	-	(日本電気協会) https://store.denki.or.jp/products/detail/646					
21	日本	製造・供給に係る制御系システムのセキュリティ対策ガイドライン	ガイドライン	公式サイトに情報なし（業界団体加入者限定）	公式サイトに情報なし（業界団体加入者限定）	業界団体 （一般社団法人日本ガス協会）	サイバー	×	-	-	-	-	-	-	-					
22	日本	鉄道分野における情報セキュリティ確保に係る安全ガイドライン	ガイドライン	2006	2019	政府 (国土交通省)	サイバー	○	鉄道分野における情報セキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめたもの。具体的には、昨今のサイバー攻撃動向や鉄道分野の事業特性に応じた脅威という観点から、構造的攻撃対策、パスワードリスト攻撃対策等を示している。鉄道分野において、国民生活や社会経済活動への影響が大きく事業継続に対する取り組みの対象となる情報システム及び情報資産を対象としている。例えば、重要インフラサービス障害の発生によって列車運行の遅延、運休や列車の安全安定輸送に対する支障などの影響を及ぼす重要システム、及びその中で利用される情報資産が挙げられる。 取り扱う情報の重要度に応じて、機密性、完全性、可用性の観点からの情報の格付け（ランク付け）を行うとともに、作成、入手、利用、保存、提供、複製、送信、消滅等といった情報のライフサイクルの各段階における遵守事項、情報セキュリティ対策を規定する。なお、個人データについては、重要インフラ利用者の安心感への影響に鑑みだ取扱いを規定する。	○		△	有り	情報システムの開発、アプリケーション・コンテンツの開発等を外部委託（調査・研究業務を含む）する場合、委託先選定、委託の実施において必要な対策を講ずる必要があるとしている。	(国土交通省) https://www.mlit.go.jp/common/001283894.pdf					

通番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究開発に関連する情報保全規定の有無	研究開発に関連する情報保全規定の概要	出所
23	日本	航空分野における情報セキュリティ確保に係る安全ガイドライン	ガイドライン	2006	2019	政府 (国土交通省)	サイバー	○	航空分野における情報セキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめたもの。具体的には、昨今のサイバー攻撃動向や航空分野の事業特性に応じた脅威という観点から、標的型攻撃対策、パスワードリスト攻撃対策等を示している。航空分野において、国民生活や社会経済活動への影響が大きく事業継続に対する取り組みの対象となる情報システム及び情報資産を対象としている。例えば、重要インフラサービス障害の発生によって運航の遅延、欠航や航空機の安全運航に対する支障などの影響を及ぼす重要システム及びその中で利用される情報資産が挙げられる。 取り扱う情報の重要度に応じて、機密性、完全性、可用性の観点から情報の格付け（ランク付け）を行うとともに、作成、入手、利用、保存、提供、運搬、送信、消去等といった情報のライフサイクルの各段階における遵守事項、情報セキュリティ対策を規定する。なお、個人データについては、重要インフラ利用者の安心感への影響に鑑みた取扱いを規定する。	○	△	有り	情報システムの開発、アプリケーション・コンテンツの開発等を外部委託（調査・研究業務を含む）する際は、委託先選定、委託の実施において必要な対策を講ずる必要があるとしている。	(国土交通省) https://www.mlit.go.jp/sogoseisaku/jouhouka/sosel_jouhouka9999.html
24	日本	空海分野における情報セキュリティ確保に係る安全ガイドライン	ガイドライン	2006	2019	政府 (国土交通省)	サイバー	○	空海分野における情報セキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめたもの。具体的には、昨今のサイバー攻撃動向や空海分野の事業特性に応じた脅威という観点から、標的型攻撃対策、パスワードリスト攻撃対策等を示している。空海分野において、国民生活や社会経済活動への影響が大きく事業継続に対する取り組みの対象となる情報システム及び情報資産を対象としている。 取り扱う情報の重要度に応じて、機密性、完全性、可用性の観点から情報の格付け（ランク付け）を行うとともに、作成、入手、利用、保存、提供、運搬、送信、消去等といった情報のライフサイクルの各段階における遵守事項、情報セキュリティ対策を規定する。なお、個人データについては、重要インフラ利用者の安心感への影響に鑑みた取扱いを規定する。	○	△	有り	情報システムの開発、アプリケーション・コンテンツの開発等を外部委託（調査・研究業務を含む）する際は、委託先選定、委託の実施において必要な対策を講ずる必要があるとしている。	(国土交通省) https://www.mlit.go.jp/sogoseisaku/jouhouka/sosel_jouhouka9999.html
25	日本	物流分野における情報セキュリティ確保に係る安全ガイドライン	ガイドライン	2006	2019	政府 (国土交通省)	サイバー	○	分野横断的に有効な対策項目及び対策の例示に加え、物流分野における情報セキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめたもの。具体的には、昨今のサイバー攻撃動向や物流分野の事業特性に応じた脅威という観点から、標的型攻撃対策、パスワードリスト攻撃対策等を示している。る大手物流事業者が保有する以下の重要システム、及びその中で中利用される情報資産を対象としている。 取り扱う情報の重要度に応じて、機密性、完全性、可用性の観点から情報の格付け（ランク付け）を行うとともに、作成、入手、利用、保存、提供、運搬、送信、消去等といった情報のライフサイクルの各段階における遵守事項、情報セキュリティ対策を規定する。なお、個人データについては、重要インフラ利用者の安心感への影響に鑑みた取扱いを規定する。	○	△	有り	情報システムの開発、アプリケーション・コンテンツの開発等を外部委託（調査・研究業務を含む）する際は、委託先選定、委託の実施において必要な対策を講ずる必要があるとしている。	(国土交通省) https://www.mlit.go.jp/sogoseisaku/jouhouka/sosel_jouhouka9999.html
26	日本	クレジットカード・セキュリティガイドライン	ガイドライン	2020	2023	政府 (経済産業省)	サイバー	○	クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画がその実施期限である 2020 年 3 月末に終了し、クレジットカード取引の関係事業者が実施すべきセキュリティ対策を「クレジットカード・セキュリティガイドライン」としてとりまとめたもの。「カード情報保護」と「不正利用防止」のため、クレジットカード取引の関係事業者が講ずべきセキュリティ対策を定めるとともに、その対策を有効に機能させるために取組むべき事項を記載している。カード情報は、カード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）及び機密認証データ（カード情報を含む全トラックデータ、CAV2/CVC2/CVV2/CID/いわゆるセキュリティコード、PIN又は PIN プロック）としている。	○	×	無し	-	(経済産業省) https://www.meti.go.jp/press/2022/03/20230315001/20230315001.html
27	日本	医療情報システムの安全管理に関するガイドライン	ガイドライン	2005	2023	政府 (厚生労働省)	サイバー	○	医療情報システムの安全管理や、民間事業者等が行う重篤の保存等における情報通信の技術の利用に関する法律（平成 16 年法律第 149 号。以下「e-文書法」という。）等の法令等への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示すもの。医療機関等において、すべての医療情報システムの導入、運用、利用、保守及び廃棄に関わる者を対象としている。本ガイドラインで対象とする医療情報は、医療に関する患者情報（個人識別情報）を含む情報を想定している。	○	×	無し	-	(厚生労働省) https://www.mhlw.go.jp/stf/shing/0000516275_00006.html
28	日本	地方公共団体における 情報セキュリティポリシーに関する ガイドライン	ガイドライン	2001	2022	政府（総務省）	サイバー	○	各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したもの。本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げるものではないとしている。 情報資産を機密性（1～3）、完全性（1、2）及び可用性（1、2）により分類し、必要に応じて取扱制限を行うものとする	○	×	無し	-	(総務省) https://www.soumu.go.jp/main_content/000805453.pdf
29	日本	ISO/IEC 27002（JIS Q 27002:2014）	ガイドライン	2006年	2014年	ISO/IEC（JIS）	その他	○	国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定した、企業などの組織における情報セキュリティマネジメントシステムの仕様を定めた規格であり日本ではJISが翻訳を行っている その中で組織の行うべき情報機密性の分類体系について4つのレベルの例を示している	○	×	無し	-	(JIS規格) https://kkakurui.com/q/Q27002-2014-01.html
30	日本	中小企業の情報セキュリティ対策ガイドライン	ガイドライン	2016年第2版 (初版発刊時期が公表HPに無し)	2023年	IPA	サイバー	○	中小企業に情報漏えい、改ざん、消失などの脅威から保護するための情報セキュリティ対策の考え方や、段階的に実現するための方法を紹介しており、その中で社内の情報資産ごとの機密性・完全性・可用性の評価値から、重要度を算定し格付けするための表紙を例示している。	○	×	無し	-	(IPA) https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf
31	日本	不正競争防止法	法律	1934年	2023年	経済産業省	その他	○	事業者間の公正な競争と国際約束の適正な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置を規定するものであり、事業者が持つ秘密情報（営業秘密）が不正に持ち出された場合等の法的保護について規定している	△	×	無し	-	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=405AC00000000047
32	日本	組織における内部不正防止ガイドライン	ガイドライン	2013年	2023年	IPA	その他	○	組織内部者の不正による顧客情報や製品情報などの漏えいを防止するため、内部不正防止の重要性や対策の体制、関連する法律などの概要を「基本方針」「資産管理」「技術的管理」「職場環境」「事後対策」等の10の観点のもと、具体的な対策について示している	△	×	無し	-	(IPA) https://www.ipa.go.jp/security/guide/insider.html
33	日本	産業競争力強化法（技術情報管理認証制度）	法律	2013年	2023年	政府 (経済産業省)	その他	○	日本の産業競争力を強化することを目的とした施策策について定めた産業競争力強化法の中で、事業者（企業や研究機関等）の技術情報の管理について、国で示した「守り方」に即して守られているかどうかを、国の認定を受けた機関による認証を受けられる制度（技術情報管理認証制度）が規定されている 技術情報管理認証制度は企業の情報セキュリティ対策を、国の認定を受けた機関が策定した基準に基づいて審査・認証する制度である。企業の「強み」となる情報に絞った管理を認定する制度であるため、対象とする情報の区分や種類は認証範囲によって異なる。企業による「情報の指定」といった取り組みも認証に向けた評価項目となっている 経済産業省の指定する認証機関8機関のうち、5つは対象とする業務範囲に指定はないが、航空宇宙防衛に係るものは防衛基盤整備協会による認証、製造業・中小企業は日本金型工業会、ライド（株）が行う区分となっている	○	△	有り	技術情報管理認証制度の対象は研究機関を含む事業者等であり、認証を受けるための情報管理の進め方が求められている	(経産省) https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/out_line.pdf
34	日本	外国為替及び外国貿易法（安全保障貿易管理制度、対外直接投資審査制度）	法律	1949年	2023年	政府 (経済産業省)	その他	○	外国為替、外国貿易その他の対外取引に対する管理・調整事項を定めた物であり、その中で外国貿易において国際的な平和及び安全の維持を妨げることとなると認められる特定の貨物の輸出や技術の提供を行うおとする者に対し、経済産業省の定める輸出者の遵守すべき基準に基づく許可取得を義務付けている	△	×	無し	-	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=332AC00000000166
35	日本	核燃料物質、核燃料物質及び原子炉の規制に関する法律	法律	1957年	2023年	政府 (経済産業省)	その他	○	特定核燃料物質の防護に関する秘密について、原子力事業者・従業員等に対する守秘義務を規定している。信頼性確認を行った上で秘密を業務上知り得る者を指定するなどの防護措置を講じingことを原子力事業者等に義務付けている守秘義務違反及び防護措置に係る違反命令違反に対する罰則あり	○	△	無し	-	(経産省) https://www.meti.go.jp/policy/innovation_corp/himitsujohe/161012_himitsujohe.pdf
36	日本	国立研究開発法人におけるデータポリシー策定のためのガイドライン	ガイドライン	2018年	-	政府 (内閣府)	その他	○	国立研究開発法人におけるデータポリシー策定の参考として、研究データの管理と利活用についてのポイント、及びデータポリシーで定めるべき項目及び基本的な記述内容を示すもの 位置づけとして、公金が使われた研究開発成果の管理・利活用についての組織としての方針（データポリシー）の策定によって、多様な情報・データが分野間で共有されることによってイノベーション創出に繋がることが強調されている	○	○	有り	ガイドラインの対象は国立研究開発法人における研究成果等のデータ取り扱いであり、（内閣府） https://www8.cao.go.jp/cstp/stsnota/datapolicy/datapolicy.pdf	
37	日本	大学における研究データポリシー策定のためのガイドライン	ガイドライン	2021年	-	大学ICT推進協議会	その他	○	大学におけるデータポリシー策定の参考として、大学で研究データポリシーを策定することの意義、その類型、データポリシーに定めるべき項目と検討の視点、策定のプロセス等について示されている 位置づけとして、近年の国際的なオープンサイエンスの流れと大学内部のコンプライアンスへの対応を求めている	○	○	有り	ガイドラインの対象は大学における研究成果等のデータ取り扱いであり、近年のオープンサイエンスの流れとコンプライアンスへの対応が求められている (大学ICT推進協議会) https://rdm.axes.jp/_media/sites/14/2021/07/urdp-guideline.pdf	
38	日本	大学における秘密情報の保護ハンドブック	ガイドライン	2004年	2016年	政府 (経済産業省)	その他	○	大学が秘密情報を管理する重要性と、大学が扱う情報の中からのように秘密情報を選別して管理するかや、秘密情報管理のルール策定、学内体制のあり方、学生が秘密情報を扱う場合の対策等について説明している	○	○	有り	ハンドブックの内容そのものが大学における活動を対象としているため、研究開発を含むほか、秘密情報管理における研究に参加する学生等の扱い（雇用・秘密保持義務など）に関する留意事項も示している (経済産業省) https://www.meti.go.jp/policy/innovation_corp/himitsujohe/161012_himitsujohe.pdf	
39	日本	防衛省が関与する装備品等の開発及び生産のための基礎の強化に関する法律	法律	2023年	-	政府 (防衛省)	多義的技術	○	防衛産業による装備品等の安定的な製造等を確保するための法律であり、防衛生産・技術基盤の強化を図るべく、事業撤退による供給途絶やサイバー攻撃による企業からの情報漏洩といった、様々なリスクに対応した措置を防衛省がとることができる と定められている その中で「 <u>装備品等契約における秘密の保全措置</u> 」が規定され、防衛省と装備品等に係る契約を締結した事業者が取り扱う必要のある装備品等や自衛隊に関する情報を「 <u>装備品等秘密</u> 」として指定して、当該事業者に保秘義務を課しており、漏洩時の罰則がある	△	×	無し	-	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=505AC00000000054_20240613_0000000000000000
40	日本	防衛産業保全マニュアル（Defense Industrial Security Manual：DISM）	ガイドライン	2023	-	政府 (防衛装備庁)	多義的技術	○	国内の防衛産業に普及するとともに、同盟国・同志国等の政府・防衛産業にも共有し、防衛装備・技術協力を含めた防衛生産・技術基盤の強化を図っていくことを念頭に、防衛産業に適用される秘密情報の保護に係る法令、規則等に基づく防衛産業における情報保護措置を、一元的に整理したもの。特定秘密保護法に基づく「特定秘密」、MDA 秘密保護法に基づく「特別防衛秘密」、そして自衛隊法等により保護されている「秘」の3つの秘密により構成「秘密情報：Classified Information」を対象として、保全方法を定めている	○	△	有り	同盟国から導入した先進装備品の生産・維持整備や共同研究開発、防衛装備品等転等、ますます国際化が進捗するとともに、各国の秘密情報の円滑な共有が必要であり、そのために「国際水準を踏まえた産業保全の強化」に向けた取組を定めている (第4節：国際共同プロジェクトに関する秘密保全)	(防衛装備庁) https://www.mod.go.jp/ata/img/dism/dism2023_jp.pdf
41	日本	装備品等及び役務の調達における情報セキュリティ基準	ガイドライン	確認中	2023	政府 (防衛装備庁)	多義的技術	○	防衛省の保護すべき情報を取り扱うに当たり、事業者のとるべき必要な措置を定めたものの用語の定義や対象とする情報、情報セキュリティ基本方針等の作成、組織のとるべき体制、情報保護の管理要領、物理的なセキュリティ対策、防衛省による監査の実施等について定めている	○	○	有り	研究開発を委託される事業者が具体的にとるべき情報セキュリティ対策が示されている http://www.clearing.mod.go.jp/kunrei_data/_/td/2021/jc20220331_00137_000.pdf	
42	日本	装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領	ガイドライン	確認中	2023	政府 (防衛装備庁)	多義的技術	○	防衛関連企業が保有又は使用する情報システムのセキュリティの確保に関して必要な事項を定めたものの防衛関連企業の保護システム（保護すべき情報と取り扱う情報システム）におけるアクセス制御、識別・認証、通信制御、システム監視、脆弱性のスキャンといった具体的な実施事項について定めている	○	○	有り	研究開発を委託される事業者が具体的にとるべき情報システムのセキュリティ実施事項が示されている (防衛装備庁) http://www.clearing.mod.go.jp/kunrei_data/_/td/2021/jc20220331_00137_001.pdf	
43	日本	政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：ISMAP）	ガイドライン	2020	2023	政府 (ISMAP運営委員)	サイバー	○	政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度。「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本枠組みについて」（令和2年1月30日サイバーセキュリティ戦略本部決定）に基づき、内閣サイバーセキュリティセンター・デジタル庁・総務省、経済産業省が運営している。クラウドサービス登録申請者に対する要求事項、情報セキュリティ管理・運用の基準となる管理事項、監査機関登録申請者に対する要求事項などを規定している。	○	×	無し	-	(ISMAP) https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005&sys_kb_id=027b4440dbdf9506e6cb915f96619f5&spa=1 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028&sys_kb_id=3e49d830c37bed1010a335977a013163&spa=1
44	日本	安全保障貿易に係る機微技術管理ガイダンス（大学・研究機関用）	ガイドライン	2008	2022	政府 (経済産業省)	多義的技術	○	外為法に基づく技術の提供等の管理について、大学・研究機関が実施すべきことを取り纏め、法令遵守のための効果的な体制整備と機微な技術情報の管理水準の向上を促進する目的で経済産業省が策定したものである	○	○	有り	大学・研究機関で安全保障貿易管理上の機微な情報の管理業が示されている (経済産業省) https://www.meti.go.jp/policy/ampo/law_document/tutatu/i07sonota/i07sonota_jishukanr/i03.pdf	
45	日本	研究データリポジトリ整備・運用ガイドライン	ガイドライン	2019	-	政府 (内閣府)	その他	○	データリポジトリの整備・運用を行う国研及び大学等が国際的にも信頼され、研究データの保存・公開を適切に進めることができるよう、その整備・運用の指針を示すもの	○	△	無し	-	(内閣府) https://www8.cao.go.jp/cstp/youusakai/kokusaitopen/guideline.pdf

連番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究開発に関連する情報保全規定の有無	研究開発に関連する情報保全規定の概要	出所
46	日本	衛星リモートセンシング記録の適正な取扱いの確保に関する法律	法律	2016	2022	政府	宇宙	○	日本における衛星リモートセンシング記録の適正な取扱いを確保するため、国の責務を定めるとともに、衛星リモートセンシング装置の使用に係る許可制度を設け、あわせて、衛星リモートセンシング記録保有者の義務、衛星リモートセンシング記録を取り扱う者の認定、内閣総理大臣による監督その他の衛星リモートセンシング記録の取扱いに關し必要な事項を定めるもの	○	○	有り	同法の施行規則では、衛星リモセン情報を取り扱うための組織的・人的・物理的・技術的な管理策について規定されており、研究開発に用いる場合も同様である	(e-GOV 法令検索) https://elaws.e-gov.go.jp/document?lawid=428AC0000000077
47	米国	Executive Order 13526（大統領令13526号）	行政指令	2009	-	政府	その他	○	機密情報の取扱いに關して定めた大統領命令であり、「軍事計画」「外国政府の情報」「諜報活動に関する情報源、方法等」「秘密情報を含む政府の外交活動」「国家安全保障に関する科学、技術、経済的事項」「大量破壊兵器の製造等」等に該当する情報を機密情報として定義し、情報の重要度(漏洩した際の影響度等)に応じて、機密、極秘、秘に区分している。指定された情報の漏洩取得に対して罰則があり、最重刑は死刑である。	○	×	無し	(NATIONAL ARCHIVES) https://www.archives.gov/isoo/policy-documents/cnsl-eo.html	
48	米国	インテリジェンス・アイデンティティ保護法	法律	1982	2005	政府	その他	○	米国の諜報員や情報源の保護を目的とした法律で、諜報員・秘密工員や対外諜報活動に関する情報を故意に開示することを禁止している。	○	×	無し	(Intelligence Identities Protection Act) https://sgp.fas.org/crs/intel/RS21636.pdf (U.S. Senate Select committee on Intelligence) https://www.intelligence.senate.gov/laws/intelligence-identities-protection-act-1982 (CONGRESS.GOV) https://www.congress.gov/bill/97th-congress/house-bill/4	
49	米国	電気通信プライバシー法（ECPA）	法律	1986	2008	政府 (司法省)	サイバー	○	電気通信プライバシー法は、電子通信（有線又は電子システムによって全部又は部分的に送信される、あらゆる性質の記号、信号、文章、画像、音声、データ、又は情報の伝達）に対する政府の監視を禁止した法律である。	○	×	無し	(BIA) https://bja.ojp.gov/program/ki/privacy-civil-liberties/authorities/statutes/1285	
50	米国	イリノイ州生体情報プライバシー保護法（BIPA）	法律	2008	-	州 (イリノイ州)	その他	○	民間企業等による「生体認証情報」（個人を識別するために使用される個人の生体認証識別子に基づく情報）「生体認証識別子」（顔または虹彩のスキャン、指紋、声紋、又は手や顔の形状のスキャン）に関連する情報の収集、使用等を規制するための州法である。	○	×	無し	(Illinois General Assembly) https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57	
51	米国	イリノイ州個人情報保護法	法律	2006	-	州 (イリノイ州)	その他	○	イリノイ州個人情報保護法はイリノイ州民のプライバシーを保護するための州法であり、個人のファーストネーム、又はファーストネームのイニシャル及びラストネームと、社会保険番号や運転免許証の番号等のデータ要素を組み合わせたものであって、氏名若しくはデータ要素が暗号化若しくは編集されていないか、又は暗号化若しくは編集されているものの、セキュリティ侵害により、暗号化解除若しくは編集解除の鍵、若しくはその他の方法により氏名若しくはデータ要素を復元なしに読み取ることができるようになったもの ユーザー名又は電子メールアドレスと、オンラインアカウントへのアクセスを許可するパスワード又はセキュリティ質問と回答の組み合わせであって、ユーザー名、電子メールアドレス、パスワード又はセキュリティ質問と回答のいずれかが暗号化又は編集されていないか、暗号化又は編集されているものの、暗号化解除又は編集解除その他の方法でデータ要素を読み取るための鍵がセキュリティ侵害によって入手されているものを保護すべき個人情報として、それらの情報の収集、処理等に関して要件等を定めている。	○	×	無し	(Illinois General Assembly) https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67	
52	米国	カリフォルニア州消費者プライバシー法（CCPA）	法律	2018	2020	州 (カリフォルニア州)	その他	○	カリフォルニア州消費者プライバシー法は、カリフォルニア州民のプライバシー、消費者の保護を目的とした州法であり、特定の消費者又は世帯を識別し、関連し、叙述し、合理的に関連付けることができ、又は意図的に若しくは間接的に合理的にリンクさせることのできる情報を個人情報として定義して、それらに対する消費者等の権利や、企業の義務について定めている。	○	×	無し	(California LEGISLATIVE INFORMATION) https://leginfo.ca.gov/laces/codes/codes_displayText.xhtml?lawCode=CIV&division=3.8&title=1.81.5.&part=4.8&chapter=&article=	
53	米国	ニューヨーク州ハッキング防止及び電子データセキュリティ改善法（SHIELD法）	法律	2019	-	州 (ニューヨーク州)	サイバー	○	データセキュリティの強化による個人情報の保護を目的とした州法であり、自然人に関する情報であって、氏名、番号、個人的な特徴（personal mark）又はその他の識別子により、その個人を特定することができるものを個人情報として定義し、それらの個人情報の企業に対する要件等を定めている。	△	×	無し	(Office of the New York State Attorney General) https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act	
54	米国	ニューヨーク州金融サービス局サイバーセキュリティ規則（NYDFS サイバーセキュリティ規則）	規則	2017	2023	州 (ニューヨーク州)	サイバー	○	ニューヨーク州の金融サービス企業に対してサイバーセキュリティの要件を定めた規則であり、その中で個人に関する情報で、氏名、個人の特徴（personal mark）又はその他の識別子、ソーシャルセキュリティナンバーや運転免許証番号又は非運転免許身分証明書番号等のいずれか1つ以上との組み合わせにより、当該個人を特定するために使用することができるものの、及び③④⑤又は性別を除く、医療提供者若しくは個人により作成された又は個人から得られた、あらゆる形式又は媒体の、当該個人の家族の構成員の過去、現在若しくは将来の身体的、精神的若しくは行動的な健康又は状態等に関連するあらゆる情報又はデータ（「非公開情報（nonpublic information）」）を個人情報として定義し、それらの取扱い、要件について定めている。	△	×	無し	(CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES) https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf	
55	米国	情報自由法（FOIA）	法律	1966	2016	政府	バイオ	○	情報自由法は、連邦政府の保有している情報にアクセスする権利を定めた連邦法である。その法律の中で不開示情報とが定められており、①人事・医療に関するファイル等、②商業上の秘密等、③大統領命令に基づき、国防又は外交政策のために秘密にしておくことが認められ、かつ、大統領命令に従い、実際に指定が正当に行われているもの等、④捜査や訴訟の手段等を明らかにする法執行記録や情報等、⑤情報秘匿性権が認められる文書や書簡等、⑥行政機関内部の人事規則及び慣行に関すること等、⑦制定法により特に開示が免除されているもの、⑧油井に関する地質学、地球地理学上の情報等については開示をすることができない。	○	×	無し	(U.S. Department of Justice) https://www.justice.gov/oip/freedom-information-act-5-usc-552	
56	米国	医療保険の携行性と責任に関する法律（HIPAA）	法律	1996	2013	政府 (保健福祉省)	バイオ	○	HIPAAは患者の同意や知識なしに機密性の高い患者の健康情報が開示されないように保護するための国家標準の作成を要求する連邦法で、医療における個人情報を「保護されるべき健康情報（Protected Health Information）」健康状態、医療の提供、医療費の支払いに関連する情報で、個人に結びつけることが可能なものとして定義し、対象事業者に対して保護のための要件等を定めている。また、HIPAAで定められた要件を具体化するためにHIPAAプライバシールールが定められている。	○	×	無し	(CDC) https://www.cdc.gov/php/publications/topic/hipaa.html	
57	米国	統一営業秘密法（UTSA）	法律	1979	1985	政府 (商務省)	その他	○	UTSAはの営業秘密法(州法)の雛形として用いられた法律であり、営業秘密に関して「その開示若しくは使用によって経済的価値を得ることのできる他の者により、一般的に知られておらず、かつ適切な手段によっては容易に解明されないことにより、現実の又は潜在的な、独立の経済的価値を生じさせるもの」「その秘密性の維持のために、当該状況のもとにおいて合理的な努力の対象となっている。処方、パターン、編集物、プログラム、装置、方法、技術又はプロセスを含む、情報」を営業秘密として定義し、多くの州(NY州を除く)の営業秘密法(州法)の雛形に使用されている。	○	×	無し	(UNIFORM TRADE SECRETS ACT) https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf 〔経済産業省「営業秘密に関する取組の法制化進展」〕 https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/outreach_r3_europeandunitsd.tates.pdf	
58	米国	連邦営業秘密保護法（DTSA）	法律	2016	-	政府 (商務省)	その他	○	DTSAは、連邦レベルで営業秘密を保護する法律であり、「形式・種類にかかわらず財務、ビジネス、化学、技術、経済、工学に関する情報」で「所有者が情報を秘密にするために合理的方法を取っていて、その情報が経済的恩恵をもたらし、その情報から恩恵を受けられる他者が合法な方法でその情報を知ることができないもの」を営業秘密として定義し、これまで、州法のみで対応されていた営業秘密の権限等が連邦裁判所に訴えられることが可能となった。	○	×	無し	(CONGRESS.GOV) https://congress.gov/114/plaws/pub1153/PLAW-114pub1153.pdf	
59	米国	グラム・リーチ・ブライリー法（GLBA）	法律	1999	2021	政府 (連邦取引委員会)	その他	○	GLBAは、米国の金融機関に対して顧客の個人情報の共有や保護を定めた連邦法であり、金融サービスの提供を通じて顧客から収集されるあらゆる情報を非公開個人情報（Non-Public Personal Information）として定義している。	○	×	無し	(CONGRESS.GOV) https://www.congress.gov/106/plaws/pub102/PLAW-106pub102.pdf	
60	米国	ECRA（Export Control Reform Act：輸出管理改革法）	法律	2018	-	政府 (商務省)	多義的技術	○	国防権限法2019の一部として制定された法律であり、それ以前は米国の軍民両用品（dual use items）の規制のための根拠として機能していた行政規則である輸出管理規則（Export Administration Regulations、EAR）に対して、より確固とした連邦法の根拠法を定めるものである。 具体的には①新規で「新興・基盤的技術（emerging and foundational technologies）」を対象とした輸出規制の構築、②包括的武器輸出禁止国に対する輸出ライセンスの対象範囲および除外基準などの見直し、③商務省のライセンス発行審査における審査要件に、対象技術の輸出が米国の防衛産業基盤に及ぼす影響を追加する等が挙げられる。	×	×	無し	(JTRO資料「脱・嚴格化する米国の輸出管理法令留意点と対策」) https://www.jetro.go.jp/text_images/_Reports/01/e95620416cd2f8a3/20210031.pdf (CONGRESS.COM) https://www.congress.gov/bill/115th-congress/house-bill/5040/text	
61	米国	EAR（Export Administration Regulations：輸出管理規則）	規則	1979	2023	政府 (商務省)	多義的技術	○	EARは米国からの商品や技術の輸出、再輸出を規制する規則であり、軍事用としても非軍事用としても利用可能な「デュアル・ユース品目」と呼ばれる商用製品の輸出に適用される。 EARは商務省産業安全保障局（Bureau of Industry and Security：BIS）が管理・規制の執行を管理している。EAR規制対象品目は、物品（Commodities：炭、建築資材、道路橋梁、自動車部品など）、ソフトウェア（Software）、技術（Technology）をはじめ多岐にわたり、米国からの輸出のみでなく、再輸出の取引にも適用される。 （すべてのEAR規制対象品目の再輸出に、商賣者の輸出許可が必要なわけではなく、許可の必要の有無は、対象製品、輸出国、輸出国における輸入者、輸出处により異なる。）	×	×	無し	(Bureau of Industry and Security) https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear https://www.bis.doc.gov/index.php/federal-register-notices	
62	米国	FIRRM（Foreign Investment Risk Review Modernization Act：外国投資リスク審査近代化法）	法律	2018	2020	政府 (商務省)	その他	○	FIRRMは対米外国投資に係る国家安全保障の懸念に対応するために国防権限法2019の一部として制定された法律であり、従来のはCFIUS（対米外国投資委員会）で定められた審査対象であった外国人による米国の事業の支配をもたらす合併、取得、買収に加えて、基本的には引き続き外国からの対米投資の取扱いを規制しつつも、重要技術の流出や重要インフラへの悪影響などの防止の観点からセンシティブな米国政府施設に近接する不動産取引や、重要技術を持つ米国事業の外国人による「支配」を伴わない投資を審査対象取引に加え、また一部の取引の際にはCFIUSへの事前届け出が義務付けられた。	×	×	無し	(CONGRESS.COM) https://www.congress.gov/bill/115th-congress/house-bill/5841/text (U.S. DEPARTMENT OF THE TREASURY) https://home.treasury.gov/news/press-releases/sm872	
63	米国	安全で信頼できる通信ネットワーク法	法律	2018	-	政府 (連邦通信委員会)	サイバー	○	米国の安全保障上、許容できないリスクをもたらす企業が製造する製品やサービスが米国ネットワークに侵入するのを防ぐことを目的とし、安全保障上許容できないリスクをもたらす企業が製造する製品やサービスについてリストを公表することを義務付け、リストに指定された企業についてはFCCの補助金を使用して、これら企業の通信サービスなどを購入・維持することも禁止される。 （リストに指定された企業：中国のファーウェイ、ZTE、ハイテラ、ハイビジョン、ダーファの5社（2021年）中国のチャイナ・モバイル、チャイナ・テレコム、ロシアのカスベルスキの3社（2022年））	×	×	無し	(CONGRESS.COM) https://www.congress.gov/bill/116th-congress/house-bill/4998	
64	米国	安全機器法	法律	2021	-	政府 (連邦通信委員会)	サイバー	○	米国の安全保障上、許容できないリスクをもたらす機器の認可申請を審査または承認しないことを示した法律であり、安全で信頼できる通信ネットワーク法に基づき、米国の安全保障上、許容できないリスクがあると認定された企業の通信機器・サービスやビデオ監視システムは、FCCにより米国内での使用のための認証を全面的に禁止される。	×	×	無し	(CONGRESS.COM) https://www.congress.gov/bill/117th-congress/house-bill/3919	
66	米国	DoDI 8500.01	ガイドライン	2014	2019	政府 (国防総省)	多義的技術	○	国防総省内部の全ての組織、情報技術、電子形式情報に適用される、リスク管理、運用レジリエンス、統合と相互運用性、サイバースペース防衛、アイデンティティ保証等のサイバーセキュリティポリシーを示す国防総省指令	○	×	無し	(DoDI 8500.01) https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dod/850001_2014.pdf	
67	米国	DoDI 8510.01	ガイドライン	2022	-	政府 (国防総省)	多義的技術	○	国防総省（DoD）の情報システムのリスク管理フレームワーク（RMF）を確立する国防総省指令であり、国防総省情報システムとプラットフォーム情報技術（PIT）を評価および認可するための7つのステップで構成されている	○	×	無し	(DoDI 8510.01) https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dod/851001p.pdf?ver=2019-02-26-101520-300	

連番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究開発に関連する情報保全規定の有無	研究開発に関連する情報保全規定の概要	出所
68	米国	NIST SP800-171	ガイドライン	2015	2020	業界団体 (NIST)	その他	○	連邦政府外のシステムと組織における管理された余格付け情報(CUI)の保護のための継続要件を示したものであり、CUIの処理を遂行する場合には業者はNIST SP800-171に準拠しなければならない。なお2020年に更新版であるNIST SP800-171 Revision 2 が発表されている。	○	△	有り	システム開発に係る規定が定められている	(NIST) https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0 https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
69	米国	ISO/IEC 27002	ガイドライン	2007	2022	業界団体 (ISO/IEC)	その他	○	ISO/IEC27002は、国際標準化機構(ISO)と国際電気標準会議(IEC)が発表した情報セキュリティ、サイバーセキュリティ、プライバシー保護 といった情報セキュリティの実装ガイダンスを含む一般的な情報セキュリティ管理のリファレンス セットを提供する情報セキュリティ標準である。	○	×	無し	-	(ISO) https://www.iso.org/standard/75652.html
70	米国	重要インフラのサイバーセキュリティを改善するためのフレームワーク (Framework for Improving Critical Infrastructure Cybersecurity)	ガイドライン	2014	2018	業界団体 (NIST)	サイバー	○	組織の規模、サイバーセキュリティリスクの程度、サイバーセキュリティの複雑さに関わらず、あらゆる業界、コミュニティの組織がリスクマネジメントの原則とベストプラクティスを適用し、セキュリティとレジリエンスを改善することを目的としたフレームワーク。	○	×	無し	-	(NIST) https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (IPA資料「重要インフラのサイバーセキュリティを改善するためのフレームワーク」) https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-atr/000071204.pdf
71	米国	連邦情報処理基準 (Federal Information Processing Standard：FIPS)	ガイドライン	2004	2023	業界団体 (NIST)	サイバー	○	米国防務政府のコンピューター・システム用にNISTによって発行された標準及び指針。米国防務政府が使用するコンピュータシステムのセキュリティと相互運用性を保証するように設計されている。機密情報を扱う際に政府機関や請負業者が満たさなければならない特定の要件を定義している。 FIPS 出版物は、1996 年の情報技術管理改革法(公法 104 - 106) および1987 年のコンピュータ セキュリティ法(公法 100 - 235)の第 5131 条に基づき、商務長官の承認を経て NIST によって発行される。 FIPS 140-2：機密情報を保護するために使用される暗号化アルゴリズムとモジュールの設計、実装、テストに関するガイドラインを提供 FIPS 186：デジタル署名の生成と検証に使用されるデジタル署名アルゴリズム (DSA) とセキュア ハッシュ アルゴリズム (SHA) について説明されており、これらの暗号化アルゴリズムの実装に関するガイドラインを提供 FIPS 199：セキュリティ 投資の潜在的な影響に基づいて、情報および情報システムのセキュリティ分類を定義 FIPS 201：連邦職員および請負業者が使用する個人認証 (PIV) カードの要件を定義。主体認証情報や ID 情報の保存など、PIV カードの技術仕様 の概要が説明されている。	各FIPSシリーズの内容によるため割愛	各FIPSシリーズの内容によるため割愛	各FIPSシリーズの内容によるため割愛	各FIPSシリーズの内容によるため割愛	(NIST) https://www.nist.gov/itl/publications-0/federal-information-processing-standards-fips (IPA) https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-atr/000025321.pdf
72	米国	Executive Order 13556（大統領令13556号）	行政命令	2010	-	政府	その他	○	法律、規則、及び政府全体のポリシーに従って保護 (safeguarding) または拡散 (dissemination) を制御 (control) する必要がある情報（管理対象非機密情報（CUI：Controlled Unclassified Information））を管理 (managing) するための、オープンで統一的なプログラムを策定するもの。ただし、2009年12月29日の大統領令第13526号又は改正原子力法に基づき機密とされた情報を除く。	○	×	無し	-	(ホワイトハウス) https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information https://www.eva.aviation.jp/wp-content/uploads/2021/02/E013556-CUI-%E5%AFA%E8%A8%B32018-219-Eva%E8%A8%B3.pdf
73	米国	ITAR (International Traffic In Arms Regulations：国際武器取引規則)	規則	1976	2022	政府	多義的技術	○	米国製の武器関連品目・技術の取引を規制する米国の行政規則の一つで、国務省 (DOS) の武器取引管理局 (DDTC) が所管している。 米国防軍品リスト (USML) に記載の製品、技術などの輸出 (Export)、再輸出 (Re-export)、再移転 (Re-transfer) を規制	△	×	無し	-	(Federal Register) https://www.federalregister.gov/documents/2022/03/23/2022-05629/international-traffic-in-arms-regulations-consolidation-and-restructuring-of-purposes-and
74	米国	NIST SP800-171 Revision 2	ガイドライン	2020	-	業界団体 (NIST)	その他	○	米政府機関がセキュリティ対策を講じるためのリポート群「SP800」シリーズの1つで、「CUI」の取り扱いを定めた規定。CUIの秘匿性を保護するための推奨セキュリティ要件を連邦政府機関に提供することを目的としている。	○	△	有り	システム開発に係る規定が定められている	(株式会社エヴァピエーション) https://www.eva.aviation.jp/security/nist-sp-800-171%E5%BC%88rev-2%E5%BC%89%E3%80%E3%82%AE%E3%83%B3%E3%83%AD%E3%83%BC%E3%83%89/
75	米国	32CFR part2002 (Controlled Unclassified Information)	規則	2016	-	政府	その他	○	行政機関の統制された未分類情報(CUI)プログラム(CUIプログラム)について説明し、CUIとして適切な情報を指定、処理、および管理解除するためのポリシーの確立を目的とした規則であり、それらの具体的な実施方法について記載をしている。	○	×	無し	-	(Code of Federal Regulations) https://www.echr.gov/current/title-32/subtitle-B/chapter-XX/part-2002
76	米国	国家安全保障決定指令189 (NSDD-189)	指令	1985	-	政府	その他	○	連邦政府が資金提供する研究開発活動で生成される科学的、技術的、および工学的情報の流れを制御するために、1985年にロナルドレーガン大統領によって確立されたポリシーで基礎研究と機密研究を明確に区別し、基礎研究の成果、情報は可能な限り制限されず公開されるべきであるとしている。	×	×	無し	-	(NSDD-189) https://rip.fas.org/offdocs/nsdd/nsdd-189.htm
77	米国	CHIPSプラス法	法律	2022	-	政府	その他	○	米中の先端技術開発競争の中で、半導体の国内製造強化を目的として成立した法律で、半導体分野に5年間で総額527億ドル（約7兆円）の支援を行うものとなっている。（用途については国内製造強化の他に国家主導の研究開発プログラム資金、コンソーシアム設立基金、人材育成基金等に分けられている） ただし、半導体技術に関する情報流出を防止するため、補助金を受領する企業は中国を全額に置いた初めであるガードレール条項を同意しなければならない。 ガードレール条項には受益者が懸念国(中国、北朝鮮、ロシア、イラン等)で半導体製造関連の実質的な拡張投資を10年間制限する条項（拡張ガードレール）と受益者が懸念ある外国事業体と共同研究またはそれらへの技術ライセンスングを制限する条項（投資ガードレール）がある。※ ガードレール条項については9月25日公示、11月24日から有効となる	△	△	無し	-	(ISU.S.C.4651「CREATING HELPFUL INCENTIVES TO PRODUCE SEMICONDUCTORS FOR AMERICA」) https://www.govinfo.gov/content/pkg/USCODE-2022-title15/pdf/USCODE-2022-title15-chap72A-sec4651.pdf (FEDERAL REGISTER) https://www.federalregister.gov/documents/2023/09/25/2023-20471/preventing-the-improper-use-of-chips-act-funding
78	米国	国際機関法	法律	-	-	政府	その他	○	米国防務議会が年度ごとに国防省に対して特定の事業計画に対する年間予算とその支出を指定することを主な目的とした法律であるが、2018年の国際機関法2019以降については対中国への情報・技術流出への対応に関する規程が多く盛り込まれるようになった。（国際機関法の中でFIRMAやECRAについても規程されている）	△	△	無し	-	(NDA420139) https://www.congress.gov/115/bills/hr/5515/1/USCODE-2022-title15-sec4651.pdf (NDA42023) https://docs.house.gov/billsthisweek/20221205/BILLS-117thesa_SUS.pdf
79	米国	32CFR part117 NISPOM (National Industrial Security Program Operating Manual:国家安全保障産業プログラム運用マニュアル)	ガイドライン	1993	2021	政府	多義的技術	○	米国の国家安全保障に関連する機密情報を取り扱う民間企業に対して統一されたセキュリティ基準を提供し、その情報の保護を安全を確保することを目的として、それまで各政府機関によって独自に設定され、統一性のないセキュリティ基準を統一し、より効果的なセキュリティ対策を実施するための基盤である国家産業安全保障プログラム (NISPM) を確立し、民間企業が国家安全保障に関連する情報を適切に扱うためのガイドラインとして成立した。	○	○	有り	機密に関連する研究開発を行う事業者が具体的に実施すべき事項について定められている	(FEDERAL REGISTER) https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispm
80	米国	NIST SP800-172	ガイドライン	2021	-	業界団体 (NIST)	その他	○	NIST SP800-171の補足として、(1)CUIが非連邦政府システムおよび組織に存在している場合、(2)非連邦政府機関が連邦政府機関に代わって情報を収集または保持していない場合や、政府機関に代わってシステムを使用または運用していない場合、および(3)CUI レジストリに記載されている CUI カテゴリの認可法、規則、または政府全体のポリシーによって規定された CUI を保護するための特定の必要条件がない場合における、CUIの機密性、完全性、および可用性を保護するための一連の拡張セキュリティ要件を連邦政府機関に提供するもの	○	△	有り	システム開発に係る規定が定められている	(NIST SP800-172) https://csrc.nist.gov/pubs/sp/800/172/final (IPA資料) https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-atr/000093059.pdf
81	米国	米国政府が支援する研究開発の国家安全保障戦略に関する国家安全保障大統領覚書33 (NSPM-33)を実施するためのガイダンス	ガイドライン	2022	-	政府 (研究安全保障小委員会 研究環境合同委員会)	その他	○	米国政府が支援する研究開発に対する国家安全保障方針を定めた国家安全保障大統領覚書33 (NSPM-33) の実施に関するガイドラインを定めたもので、情報の開示要件や情報共有等に関する規程について定められている	○	△	有り	研究開発情報の開示等に関する規程が定められている	(GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33)) https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf
82	米国	DoDI 5200.48 (Controlled Unclassified Information)	ガイドライン	2020	-	政府 (国防総省)	その他	○	国防総省内における、CUIの取り扱いに関する方針を定めた内部規則であり、国防総省内におけるCUIに係る各役職の責任、マーキング、管理等の要件、破壊等の要件等について定められている。	○	△	無し	-	(DoDI 5200.48) https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dod/520048a.PDF
83	米国	FAR(Federal Acquisition Regulations：連邦調達規則)	ガイドライン	-	-	政府 (FAR委員会)	その他	○	連邦政府の調達（購入・契約）に関する一連の規則で、連邦政府が商品やサービスを調達する際の手続き、要求事項、および実施方針を定めている。 FAR Part27（特許、データ及び著作権）等が定められている	○	△	有り	研究開発における知財管理に関する規程が定められている	(FAR) https://www.acquisition.gov/browse/index/far
84	米国	DFARS(Defense Federal Acquisition Regulation Supplement：国防調達連規則補足)	ガイドライン	-	-	政府 (国防総省)	その他	○	米国のFARに対する適用と補則を記載した規則であり、国防関連の調達においてFARに加えて適用され、国防総省が契約を結ぶ際の特有の手続きや要件等を定めている。 多くの規則があるが、主には以下のような規則が定められている DFARS 252.227-7038（特許権・権利事項(大企業)による所有権) DFARS 252.204-7000（情報の開示) DFARS 252.204-7008（対象となる防衛情報の保護管理への事項) DFARS 252.204-7012（対象となる防衛情報の保護とサイバーインシデントの報告)	△	△	無し	研究開発における知財管理に関する規程が定められている	(DFARS) https://www.acquisition.gov/dfars
85	米国	DoDM 5200.01 (DoD情報セキュリティプログラム)	ガイドライン	2012	2020	政府 (国防総省)	その他	○	国防総省における情報セキュリティ分類、管理方法等を提供する文書であり、全1～4巻でそれぞれ異なる情報の取り扱いに関する規程が定められている。 1巻：概要、分類、および分類解除について 2巻：情報のマーキングについて 3巻：機密情報の保護について 4巻：CUIについて	○	△	有り	一部研究の情報のについての取り決め事項が記載されている	(DoD Issuances) https://www.esd.whs.mil/directives/issuances/dodm/
86	米国	DoDI5220.31/DoDM 5220.32（国家産業安全保障プログラム） (改正前はDoD 5220.22-Mの表記)	ガイドライン	2018	2021	政府 (国防総省)	その他	○	32CFR part117 NISPOMの規程に基づいて策定されたDoD内の規則であり、DoDと民間企業の機密情報等に関連する共同研究において、機密情報の管理等で実施すべき事項が定められている。	○	○	有り	機密に関連する研究開発を行う事業者が具体的に実施すべき事項について定められている	(DoD Issuances) https://www.esd.whs.mil/directives/issuances/dodm/ https://www.esd.whs.mil/directives/issuances/dodi/
87	米国	DoDI 8582.01（非機密非公開情報を処理するDoD以外の情報システムのセキュリティ）	ガイドライン	2019	-	政府 (国防総省)	その他	○	DoDの内部規則であり、管理された未分類の情報（CUI）を含む、未分類の非公開の国防総省情報を処理、保管、または送信する国防総省以外の情報システムのセキュリティを管理するための方針を確立し、責任を割り当て、指示を与えるものである。	○	△	有り	一部研究の情報のについての取り決め事項が記載されている	(DoD Issuances) https://www.esd.whs.mil/directives/issuances/dodi/
88	米国	18 U.S.C. § 793, 794, 798	法律	-	-	政府	その他	○	18 U.S.C.は刑法・刑事訴訟法について定めたものであり、連邦レベルでの犯罪、刑罰、刑事手続き、司法システム等について規定されている。 その中でも 793、794、798では、機密情報の漏えいに対する罰則について、以下のような行為を行った場合の刑罰等が定められている 国防に関連する場所や情報の不正なアクセス、複製等を行った者は罰金、10年以下の懲役、またはその両方が科される。 機密中という状況下において外国政府・敵等に国防に関連する情報を伝達等した者は、死刑または終身刑に処せられる 米国の安全または利益に対する調査、または外国の利益のために機密情報を不正に伝達、公開、利用する行為や、 敵国 または外国政府の暗号、通信諜報に関連する情報の不正な取り扱いを行った者は罰金、10年以下の懲役、またはその両方が科される	△	×	無し	-	18 U.S.C. § 793, 794, 798 https://www.law.cornell.edu/uscode/text/18/793 https://www.law.cornell.edu/uscode/text/18/794 https://www.law.cornell.edu/uscode/text/18/798
89	米国	DoDI 1035.01（テレワーク・リモートワーク）	ガイドライン	2024	-	政府 (国防総省)	その他	○	DoDの内部規則であり、DoDの職員等がテレワーク・リモートワークを実施するにあたっての方針、責任、手続、実施可能要件等が定められている。	△	×	無し	-	(DoDI 1035.01) https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/103501p.pdf

連番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究開発に関する情報保全規定の有無	研究開発に関する情報保全規定の概要	出所
90	米国	NPD 2810.1F (NASA情報セキュリティポリシー)	ガイドライン	2022	-	NASA	その他	○	NASAにおける機密、非機密情報の保護のための情報セキュリティに関する方針、適用範囲、権限、責任等について定めたものである。	○	×	無し	-	(NPD2810.1F) https://nods3.gsfc.nasa.gov/displayDir.cfm?l=NPD&c=2810&s=1E
91	米国	NPR 2810.1F (情報および情報システムのセキュリティ)	ガイドライン	2022	-	NASA	その他	○	NASAにおける機密、非機密情報の保護のための情報システムに必要な識別機能、プロテクト機能、検出機能、応答機能、リカバリ機能等のセキュリティ機能について定めたものである。	○	×	無し	-	(NPR 2810.1F) https://nods3.gsfc.nasa.gov/displayDir.cfm?l=internal_ID=N_PR_2810_001F_&page_name=Chapter3
92	米国	NPR 2810.7 (管理された非機密情報(CUI))	ガイドライン	2021	-	NASA	その他	○	NASAにおける、CUIの取り扱いに関する方針を定めた内部規則であり、NASAにおけるCUIに係る各役職の責任、マーキング、管理等の要件、廃棄等の要件等について定められている。	○	×	無し	-	(NPR 2810.7) https://nods3.gsfc.nasa.gov/displayDir.cfm?l=NPR&c=2810&s=7
93	米国	NPR8000.4C (エージェンシーのリスク管理手続き要件)	ガイドライン	2022	-	NASA	その他	○	NASAにおけるリスクマネジメントについて定めたものであり、プログラムやプロジェクトにおけるリスク管理要件を規定しているものであり、この規程に基づいて、[NASA Risk Management Handbook] が作成されている。 NASAでは、リスク管理についてRIDI(Risk Informed Decision Making：リスク情報に基づく意思決定)とCRM(Continuous Risk Management：継続的リスク管理)という2つのプロセスを1つ組みに統合しリスク管理を実施している。	△	×	無し	-	(NPR8000.4C) https://nods3.gsfc.nasa.gov/displayDir.cfm?l=NPR&c=8000&s=4C
94	米国	NPR3600.2B (NASAテレワークプログラム)	ガイドライン	2019	-	NASA	その他	○	NASAのテレワークに関して規程したものであり、責任区分、応募資格、トレーニング要件や設備等について必要となる事項が定められている。	△	×	無し	-	(NPR3600.2B) https://nods3.gsfc.nasa.gov/displayDir.cfm?l=NPR&c=3600&s=2B
95	カナダ	情報セキュリティ法 (Security of Information Act)	法律	1985	2019	政府 (公共安全省)	その他	○	安全保障上の機密の漏洩や、違法行為を定めるもの 時に、情報の漏洩、バイ行為、テロリズムへの関与など、国家安全保障に影響を及ぼす可能性のある行為に対して法的な措置を講じるための枠組みを提供している。情報の取扱いに関する規則が含まれており、情報の機密性の確保が重視されている。	○	×	無し	-	(Security of Information Act) https://laws-lois.justice.gc.ca/eng/acts/o-5/
96	カナダ	政府のセキュリティポリシー (Policy on Government Security)	政策文書 (Policy paper)	2019	-	政府 (サイバーセキュリティセンター)	その他	○	カナダ政府のプログラムとサービスの信頼できる提供をサポートし、情報、個人、資産の保護をサポートするために、政府のセキュリティ管理を効果的に管理すること、カナダ政府の安全管理に関してカナダ人、パートナー、監督機関、その他の関係者に保証を提供することを目的としている。 セキュリティレベル (影響レベル: Very High、High、Medium、Low) や機密性区分 (Top Secret、Secret、Confidential)、保護区分 (A〜C) についても示されている	△	×	無し	-	(Policy on Government Security) https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578
97	カナダ	セキュリティマネジメント指令 (Directive on Security Management)	ガイドライン	1995	-	政府 (公共安全省)	その他	○	部門や機関内で効率的、効果的かつ責任あるセキュリティ管理を実現することを目的としたもの。CSO (Chief security officer) に求められる具体的な要件等について示している。	○	×	無し	-	(Directive on Security Management) https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611
98	カナダ	情報開示セキュリティ法 (Security of Canada Information Disclosure Act)	法律	2015	2019年	政府 (公共安全省)	その他	○	安全保障上の観点から、カナダ政府機関における保有情報の開示を促進することを目的とする。 情報の開示を行った機関、開示を受けた機関それぞれが、当該情報の説明や開示者、開示先等に関する記録を保持する義務が定められている。	○	×	無し	-	(Security of Canada Information Disclosure Act) https://laws-lois.justice.gc.ca/eng/acts/S-6.9/
99	カナダ	データ流出脅威に対する防御 (Defending against data exfiltration threats)	ガイドライン	2023	-	政府 (Canadian Centre for Cyber Security)	サイバー	○	既存のデータ流出手法について説明し、そのような脅威の影響を軽減するために展開可能な保護戦略を提案したもののデータ流出の原因となる脅威の攻撃メカニズムを整理した上で、データ流出防止戦略について解説している	○	×	無し	-	(Defending against data exfiltration threats) https://www.cyber.gc.ca/en/guidance/defending-against-data-exfiltration-threats-itsm40110
100	カナダ	図書館公文書館法 (Library and Archives of Canada Act)	法律	2004	2015	政府 (カナダ図書館公文書館)	その他	○	カナダ図書館および公文書館を設立し、著作権法を改正し、それに伴う特定の法律を改正する法律 政府記録 (政府機関の管理下にある記録) の取扱いについて規定している。	△	×	無し	-	(Library and Archives of Canada Act) https://laws-lois.justice.gc.ca/eng/acts/l-1.7/
101	カナダ	個人情報保護及び電子文書法 (Personal Information Protection and Electronic Documents Act)	法律	2000	2019	政府 (プライバシー委員会)	その他	○	テクノロジーによって情報の流通と交換が一般化する時代において、個人情報に関する個人のプライバシーの権利と、企業がその状況に応じて適切に個人情報を収集、使用、開示する必要性を認識する形で、個人情報の収集、使用、開示について規定するルールを確立することを目的としたもの。 商業活動に従事する民間組織及び民間事業者が、個人を特定可能な情報 (個人情報) を扱う際の規定を定めている。	○	△	有り	情報を使用しなければ達成できない経済的または学術的な研究または研究の目的に使用され、情報がその機密性を確保する方法で使用され、同意を得ることが実行不可能であり、組織が情報が使用される前にコミッショナーに使用を通知している場合、組織は、個人の同意なしに個人情報を使用することができる	(Personal Information Protection and Electronic Documents Act) https://laws-lois.justice.gc.ca/eng/acts/p-8.6/
102	カナダ	プライバシー法 (Privacy Act)	法律	1985	2023	政府 (プライバシー委員会)	その他	○	政府機関が保有する個人情報に関して個人のプライバシーを保護し、その情報にアクセスする権利を個人に与えることを目的としたもの 個人情報をあらゆる形式で記録される識別可能な個人に関する情報と定義している 個人情報保護及び電子文書法が民間組織・民間事業者を対象としているのに対して、本法は政府や公共団体が保有する個人情報に関する取扱いについて規定している (詳細はプライバシー規則で規定)。	○	△	無し	-	(Privacy Act) https://laws-lois.justice.gc.ca/eng/ACTS/P-21/index.html
103	カナダ	情報アクセス法 (Access to Information Act)	法律	1985	2023	政府 (プライバシー委員会)	その他	○	開かれた民主主義社会を促進するため、連邦機関の説明責任と透明性を高め、これらの機関の行為に関する公開討論を可能にすることとしたもの 個人情報プライバシー法と同義とする。また政府機関情報としては、政府機関からの出版物 (Publication on government institutions)、広報 (Bulletin) 等について規定されている 政府機関の長は、本法に基づき要求された記録のうち、以下等を含むものの開示を拒否することができる ・企業秘密、またはカナダ政府もしくは政府機関に属し、実質的価値を有するか、もしくは実質的価値を有する可能性が合理的に高い財務、商業、科学もしくは技術情報 ・政府機関の役員又は職員が研究を通じて得た科学的又は技術的な情報であって、その開示により当該役員又は職員が公表の優先権を奪われることが合理的に予想されるもの	○	△	有り	開示請求に対する拒否要件のとして、技術・研究に係る情報の規定あり	(Access to Information Act) https://laws-lois.justice.gc.ca/eng/acts/a-1/
104	カナダ	輸出入許可法 (Export and Import Permits Act)	法律	1985	2021	政府 (グローバル連携省)	多岐的技术	○	物品の輸出入、技術移転、仲介といった貿易に関連する活動を規制するもの。 輸出入の管理リストを作成し、リスト上の物品等の取引を行う場合には、ライセンスの発行を受ける必要がある。 ライセンスを受けた者は、本法の遵守状況を当局が判断するために必要な情報を保存することが義務付けられている。 デュアルユース品目も管理リストに含まれている (General Export Permit No. 41 ― Dual-use Goods and Technology to Certain Destinations)	△	△	無し	-	(Export and Import Permits Act) https://laws-lois.justice.gc.ca/eng/acts/o-19/
105	カナダ	カナダ投資法 (Investment Canada Act)	法律	2021	-	政府	その他	○	海外資本によるカナダ国内への直接投資 (新規事業および既存事業の買収) を規制する法令である。国家の経済成長、雇用機会の奨励および国家安全保障の保護を目的とする。非カナダ市民 (個人、政府、機関) による投資は、イノベーション・科学・経済開発省に通知または審査申請を行う必要がある。当局が必要と認める場合、海外投資がもたらす国家安全保障への影響を審査する。	×	×	無し	-	(Investment Canada Act) https://laws-lois.justice.gc.ca/eng/acts/i-21.8/
106	カナダ	原子力安全管理法 (Nuclear Safety and Control Act)	法律	1997	2017年	政府 (原子力安全委員会)	その他	○	原子力分野を規制するため、原子力委員会の設立、事業者へのライセンス発行、罰則等を規定。 同法44条に基づく一般原子力安全管理規則により、所定の情報の譲渡や開示が規制されている。 (a) 核兵器又は核爆発装置の設計、製造、使用、運用又は保存に必要な核物質(当該核物質の性質を含む)。 (b) 核兵器又は核爆発装置の設計、製造、使用、運用又は保存 (c) 法、またはライセンスに基づいて作成された規則、およびセキュリティに関連する事件に従ってライセンスによって確立されたセキュリティの取り決め、セキュリティ機能、セキュリティシステム、およびセキュリティ手順。 (d) 核セキュリティ規則第1条に定義されるカテゴリ-I、II又はIIIの核物質の輸送の経路又はスケジュール	△	△	無し	-	(Nuclear Safety and Control Act) https://laws-lois.justice.gc.ca/eng/acts/n-28.3/
107	カナダ	テクノロジーとサイバースリスク管理 (Technology and Cyber Risk Management)	ガイダンス	2022	-	政府 (金融機関監督室)	サイバー	○	金融機関向けのガイドライン。 金融機関がテクノロジーやサイバーセキュリティに関するべき事項を定めている。 ガバナンスやシステム管理、データの識別や保護等を体系的に規定。	○	×	無し	-	(Technology and Cyber Risk Management) https://www.asfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management
108	カナダ	ITSAP.00.131	ガイダンス	2020	-	政府 (サイバーセキュリティセンター)	バイオ	○	医療機関向けのガイダンス。 サイバーセキュリティの認識の強化、サイバー攻撃をこな困難にするためのパスワード設定や作業環境の保護等について解説が行われている。	○	×	無し	-	(ITSAP00.131) https://www.cyber.gc.ca/en/guidance/cyber-security-healthcare-organizations-protecting-yourself-against-common-cyber-attacks
109	カナダ	研究パートナーシップのための国家安全保障ガイドライン (National Security Guidelines for Research Partnerships)	ガイドライン	2023	-	政府 (イノベーション・科学経済開発省)	その他	○	外国の干渉、スパイ活動、および望ましくない知識移転から保護することを目的としたガイドライン。研究に対する潜在的な国家安全保障リスクを特定および軽減するために、研究者、研究機関、および政府の資金提供者が一貫したリスクをターゲットとしたデューデリジェンスを実施できるよう、リスクの要素となるものは何か、リスクの特定方法等について記されている。 リスクの要素として機密性の高い研究が挙げられており、デュアルユース技術は機密性が高い研究に該当することが明示されている。 本ガイドラインは、自然科学・工学研究評議会 (NSERC) の補助金へのすべての申請から、民間組織のパートナーを含む連邦研究パートナーシップ資金に適用される。	△	○	有り	本ガイドライン全体が研究開発に関するものであるところ、情報保全を含む本ガイドラインの概要は先の概要欄に記したとおり。	(National Security Guidelines for Research Partnerships) https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships
110	カナダ	Safeguarding Your Research	ガイドライン	-	-	政府 (イノベーション・科学経済開発省)	その他	○	研究パートナーシップのための国家安全保障ガイドラインを踏まえた、リスクを特定するためのチェックリストを記したガイドラインであり、プログラムによっては、本チェックリストを申請書とともに提出する必要がある。 リスクの兆候が確認された場合は、健全なサイバーセキュリティとデータ管理の実践を確保することや、研究成果の利用目的に関する合意を含むリスク軽減計画を記載する必要がある。	△	○	有り	本ガイドライン全体が研究開発に関するものであるところ、情報保全を含む本ガイドラインの概要は先の概要欄に記したとおり。	(Safeguarding Your Research) https://science.gc.ca/site/science/en/safeguarding-your-research
111	カナダ	知的財産行使ガイドライン (Intellectual Property Enforcement Guidelines)	ガイドライン	-	-	政府	その他	○	競争政策と知的財産権の間のインターフェースにどのようにアプローチするか等についての解説が行われている	△	×	無し	-	(Intellectual Property Enforcement Guidelines) https://sed-isde.canada.ca/site/competition-bureau-canada/en/how-we-foster-competition/education-and-outreach/intellectual-property-enforcement-guidelines#sec02
112	EU	E U の全ての機関・団体における情報セキュリティに関する規則案	法律	2022	-	欧州委員会	その他	○	欧州行政で取り扱う情報を保護するため、包括的な情報カテゴリーと、すべての組合機関および団体に対する共通の取扱い規則を確立するとともに、欧州行政全体にわたって一貫した情報セキュリティ文化を促進する欧州連合の機関と団体との間で協力スキームを確立することを目的とした規則案 機密情報やその取り扱いに係る用語の定義、必要な機関・体制の構築、情報取り扱い規則について定めている	○	×	無し	-	(EUR-Lex) https://commission.europa.eu/document/11fa0c3f-f242-4f6b-a7a6-4e714da35432_en

連番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究開発に関連する情報保全規定の有無	研究開発に関連する情報保全規定の概要	出所
113	EU	EU秘密情報を守るための保安規則に関する2015年3月13日付委員会決定	法律	2013	2015	欧州委員会	その他	○	欧州理事会がEU機密情報（EUCI）を必要な作業で取り扱うことができるよう、EUCIを保護するためのセキュリティの基本原則と最低基準を定めている。 EUの機密情報は、開示の影響の重大度によって定義される以下の4つのレベルに分類される。 ・ TRÈS SECRET UE/EU TOP SECRET: 漏洩によりEUまたは1つ以上の加盟国の本質的な利益に非常に重大な害を及ぼす可能性がある情報 ・ SECRET UE/EU SECRET: 漏洩により EUまたは1つ以上の加盟国の本質的な利益を深刻に損なう可能性がある情報 ・ CONFIDENTIEL UE/EU CONFIDENTIAL: 漏洩によりEUまたは1つ以上の加盟国の本質的な利益を損なう可能性がある情報 ・ RESTREINT UE/EU RESTRICTED: 漏洩によりEUまたは1つ以上の加盟国の利益に不利になる可能性がある情報	○	×		無し	(EUR-Lex) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D0444
114	英国	1989年公秘秘密法（Officials Secret Act.1989）	法律	1989	-	政府	その他	○	国家安全保障に関連する国家機密および公式情報の保護を規定する法律。同法律により以下の情報が保全される。 ③防諜とインテリジェンスに関する情報、④防衛に関する情報、⑤国際関係に関する情報及び外国又は国際機関から入手した秘密の情報、⑥犯罪関係情報、⑦通信の傍受に関する情報、⑧防諜、インテリジェンス、防衛又は国際関係についての情報	○	×		無し	(legislation.gov.uk) https://www.legislation.gov.uk/ukpga/1989/6/contents (国立国会図書館) https://dl.ndl.go.jp/view/download/digidepo_8331133_po_0806.pdf?contentNo=1
115	英国	2023年国家安全保障法（National Security Act 2023）	法律	2023	-	政府	その他	○	情報の不正取得・開示、外国諜報機関の支援、禁止区域への無断立ち入り等のスパイ活動を禁止し、国家安全保障上の脅威の排除を規定している法律。対象となる情報として、「保護情報（情報へのアクセスが何らかの方法で制限されているもの）」、「営業秘密」が規定されている。また、禁止区域には英国の防衛目的で使用されている土地が規定されている。防衛目的の定義には、英国軍の武器、装備の発明、開発、生産、運用、保管または処分、およびそれに関連する研究が含まれる。	○	○		有り	禁止区域の定義に、防衛目的（英国軍に関連する研究）が含まれている (legislation.gov.uk) https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted
116	英国	2000年情報自由法（Freedom of Information Act 2000）	法律	2000	2022	政府	その他	○	政府が保有する情報に対する国民の情報開示請求権、適用除外情報等を規定しており、適用除外情報として安全保障、個人情報、研究等の区分がある。 研究プログラムの過程で得られた情報、または研究プログラムから得られた情報は、以下の場合において適用除外となる ・ 公的機関またはその他の者が、研究の報告書（その情報の記述を含むか否かを問わない）を公表することを目的として、そのプログラムが継続されている場合 ・ 公表目前に本法に基づき当該情報を開示することが、研究プログラム、研究プログラムに参加する個人の利益、その情報を保有する当局の利益等を害するおそれがある場合	○	△		有り	(legislation.gov.uk) https://www.legislation.gov.uk/ukpga/2000/36/data.xht?view=snippet&wrap=true
117	英国	2004年環境情報規制（Environmental Information Regulations 2004）	法律	2004	-	政府	その他	○	英国の公的機関が保有する環境情報にアクセスする法的権利を規定している。	○	×		無し	(legislation.gov.uk) https://www.legislation.gov.uk/uksi/2004/3391/made
118	英国	英国一般データ保護規則（UK GDPR）	法律	2021	2022	政府	その他	○	「個人データの処理および英国国外への移転を行うための要件を定めるとともに、処理または移転を行う者が遵守すべき規範・義務を定めた規則。英国の「EU」からの離脱に伴って、EUの一般データ保護規則（GDPR: General Data Protection Regulation）の内容に基づいて、2021年1月1日に施行された。研究目的での個人データの利用に係る処理についても規定されている。	○	△		有り	管理者が個人データの処理を行う場合には、各処理行為について、法的根拠に基づいて処理行為を行うかについて分析を行い、適切な法的根拠を選択する必要がある。研究目的の個人データの処理の場合、「公共の利益」を法的根拠とされることが多いものの、同意等他の法的根拠に基づく場合もある。研究目的の処理との関係では、法的根拠に関するいずれの規定も適用関係が不明確な部分があり、適法なデータ処理に該当するか否かの判断が難しく、研究の促進を阻害している面があったため、DCMSのコンサルテーションにおいて、研究に関連するUK GDPRおよびDPAの法的規定をすべてまとめ、読みやすくする旨の提案（DCMS コンサルテーション・パブリックコメント、科学的研究の定義を法律に盛り込む旨の提案（DCMS コンサルテーション・パブリックコメント）、6条の研究に関する新たな法的根拠を設ける旨の提案（DCMS コンサルテーション・パブリックコメント）、研究目的のための広範な同意を許容する旨の提案（DCMS コンサルテーション・パブリックコメント））を行っている。 (legislation.gov.uk) https://www.legislation.gov.uk/eur/2016/679/contents (JETRO) https://www.jetro.go.jp/ext_images/_Reports/01/b0226c40493434/20220001rev1.pdf
119	英国	2018年データ保護法（Data Protection Act 2018）	法律	2018	2022	政府	その他	○	個人情報全般を保護対象として包括的に規定しており、治安維持、不正防止、移民管理、調査・研究、報道等の区分を目的とする場合のデータ保護を例外規定。 DPA 2018は、免除規定などにより、UK GDPRと並立し、補足する役割を果たしており、DPA 2018には、一時的に個人データの処理に関する規制であるUK GDPR（Part2）、法執行機関のための個別の制度（Part3）、3つの諜報機関のための独立した制度（Part4）という3つの独立したデータ保護制度が含まれている。	○	△		有り	調査・研究を目的とした場合に例外規定がある。 (legislation.gov.uk) https://www.legislation.gov.uk/ukpga/2018/12/enacted/data.xht?view=snippet&wrap=true (JETRO) https://www.jetro.go.jp/biznews/2018/05/da31ef0107682ba0.html
120	英国	2018年ネットワークおよび情報システム規則（The NIS Regulations 2018）	法律	2018	-	政府	サイバー	○	重要なサービスおよびデジタルサービスを提供するためのネットワークおよび情報システムのセキュリティレベル（サイバーおよび物理的回収力の両方）を高めるための法的措置を規定している。	○	×		無し	(GOV.UK) https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
121	英国	2021年電気通信（Telecommunications (Security) Act 2021）	法律	2021	-	政府	サイバー	○	電気通信および電気通信プロバイダーのセキュリティを取り締まる役割に関して、英国通信局であるOfcomの役割を基礎にし、強化するもの	△	×		無し	(legislation.gov.uk) https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted
122	英国	2021年国家安全保障・投資法（National Security and Investment Act 2021：NSI）	法律	2021	2022	政府	その他	○	国家安全保障を脅かす可能性がある、外国企業や投資家による英国企業に対する合併・買収などについて、政府の調査・介入を強化することを目的としたもの。 上記17の指定業種に該当するエンティティとの取引を対象としており、これらの分野に関する取引を行う企業や投資家が対象となる英国企業の株式または議決権を25%以上取得する場合、政府への通知を義務付ける ※17の指定業種：先端素材、先進ロボティクス、人工知能、民生用原子力、通信、コンピュータハードウェア、政府への重要なサプライヤー、暗号認証、データ・インフラストラクチャー、防衛、エネルギー、軍民併用技術、量子技術、衛星・宇宙技術、危機管理に関する重要なサプライヤー、合成生物学、輸送	△	×		無し	(legislation.gov.uk) https://www.legislation.gov.uk/ukpga/2021/25/contents/enacted (西村あさひ法律事務所) https://www.nishimura.com/sites/default/files/images/newsletter_221102_europe.pdf
123	英国	国家安全保障・投資法: 高等教育および研究集約型セクター向けのガイダンス（National Security and Investment Act: guidance for the higher education and research-intensive sectors）	ガイドライン	2021	-	内閣府	その他	○	高等教育機関、その他の研究機関、およびこの分野の投資家が2021年国家安全保障および投資法（NSI法）の範囲を解説したもの。	△	○		有り	研究者向けのガイダンスが記載されている (GOV.UK) https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors
124	英国	2011年防衛および安全保障公約規則（The Defence and Security Public Contracts Regulations 2011：DSPCR）	法律	2011	-	政府	多岐的技術	○	防衛、安全保障関連の公共調達における手続きを定める。契約が機密情報を含む場合、契約当局が要求する保護レベルで機密情報を処理、保存、および送信する能力の証拠を求めることができる。また、契約当局は、機密情報の安全性を確保するために必要な措置及び要件を契約文書に明記する義務が規定されている。当該措置及び要件は、政府のセキュリティクリアランス要件に準拠している必要がある。	○	△		無し	(GOV.UK) https://www.legislation.gov.uk/uksi/2011/1848/contents/made
125	英国	1958年公文書法（Public Records Act 1958）	法律	1958	2023	政府	その他	○	公文書に該当するものが何であるかを等を規定するもの 公文書の保存・保管等に関して規定している。	△	×		無し	(legislation.gov.uk) https://www.legislation.gov.uk/ukpga/Elt2/6-7/51/contents/enacted
126	英国	セキュリティポリシーフレームワーク（Security policy framework）	ガイドライン	2013	2022	内閣府	その他	○	英国政府の資産（人、情報、インフラ）を保護するために必要な基準、ベストプラクティスのガイドライン、アプローチについて解説。政府の業務が効果的、安全かつ確実に機能することを可能にする。セキュリティに対する適切なリスク管理されたアプローチを達成するために必要な成果に焦点を当てている。また、本ガイドラインを運用する上では、データ保護法、情報公開法、公文書法、平等法、重大組織犯罪・警察法など、関連する法的義務と保護を十分に考慮する必要性が提唱されている イギリス政府が扱う全ての情報を対象としており、情報の機密性に応じてOFFICIAL、SECRET、TOP SECRETの3つのレベルが設定されている。また、各レベルに応じて異なるセキュリティの取り決めがあることが示されている。	△	×		無し	(GOV.UK) https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework
127	英国	セキュリティ分類ポリシー（Government Security Classifications Policy：GSCP）	ガイドライン	2013	-	内閣府	その他	○	政府が取り扱う情報情報を、その機密性に応じてOFFICIAL、SECRET、TOP SECRETに区分し、情報区分ごとに必要なベースライン動作を示している。 Top Secret：英国又は同盟国の国家安全保障を直接支え、又は脅かす著しく機密な情報であって、あらゆる脅威からの保護に係る極めて高度な保証を要するもの Secret：非常に機密な情報であって強力な組織犯罪集団や国家主体等の高度な能力を有する脅威からの保護を要するもの Official：侵害された場合に中程度の被害をもたらす可能性しかないが、能力の異なる広範な脅威主体から保護を要する政府が保有する情報の大部分	○	×		無し	(GOV.UK) https://www.gov.uk/government/publications/government-security-classifications
128	英国	政府ベースライン人員セキュリティ基準（Government baseline personnel security standard：BPSS）	ガイドライン	2013	2018	内閣府	その他	○	政府資産にアクセス可能な者（公務員、軍属、臨時職員、政府請負業者）の雇用前審査、国家安全保障に関する審査について解説したガイダンス。	△	×		無し	(GOV.UK) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf
129	英国	英国政府人的安全管理（HMG personnel security controls）	ガイドライン	2013	2022	政府	その他	○	国家安全保障に関する審査方針や審査プロセスの仕組みについてのガイダンス。審査対象者に提供を求める情報について示している。 審査に係る個人データの処理に関してはデータ保護法が適用されることが示されている	△	×		無し	(GOV.UK) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1112598/20221031-HMG-Personnel-Security-Controls-V6.0-October-2022.docx.pdf
130	英国	英国のセキュリティ審査: クリアランスレベル（United Kingdom Security Vetting: clearance levels）	ガイドライン	2020	-	内閣府	その他	○	国家安全保障審査クリアランスレベルのリストと、誰がそれを必要とし、どのようなチェックが完了したかに関するガイドライン。 審査資格として、主に5つのレベル：Accreditation Check (AC)、Counter-Terrorist Check (CTC)、Level 1B、Security Check (SC)、Developed Vetting (DV)について解説されている。	○	×		無し	(GOV.UK) https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels
131	英国	2018年営業秘密規則（The Trade Secrets (Enforcement, etc.) Regulations 2018）	法律	2018	2018	政府	その他	○	営業秘密を以下の1～3のように定義し、保護している。 a. 単体として、又は、その正確な構成や要素の組立てに関して、当該情報と同様の情報を通常扱う業界内の人々の間で一般に知られておらず、又は、そのような人々が容易にアクセスすることができない点において、秘密にされている。 b. 秘密であるために、商業的価値がある。 c. 当該情報を合法的に管理している者により、特定の状況下で合理的と考えられる、情報を秘密に保つための措置が講じられている。	△	△		無し	(legislation.gov.uk) https://www.legislation.gov.uk/uksi/2018/597/made/data.xht?view=snippet&wrap=true (JETRO) https://www.jetro.go.jp/ext_images/_jpnnews/europe/2016/20160527.pdf

連番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究開発に関連する情報保全規定の有無	研究開発に関連する情報保全規定の概要	出所
132	英国	2002年輸出管理法 (Export Control Act 2002)	法律	2002	2020	政府	多義的技術	○	物品の輸出、技術移転、海外における技術運動の提供及び規制貨物の貿易に関連する活動を規制するもの。 なお、国務長官は、次に掲げる活動を禁止又は規制する効果を有する管理命令を発することはできない。 (a)科学研究の通常の過程における情報の伝達 (b)一般に利用可能な情報を公開すること。 (c)公衆が一般に入手可能な情報の伝達。ただし、当該活動を行う自由に対する命令による干渉が必要である場合（必要以上でない場合）を除く	△	△	無し	-	(legislation.gov.uk) https://www.legislation.gov.uk/ukpga/2002/28#:-text=Text%20created%20by%20the%20government%20department.readers%20who%20are%20not%20legally%20qualified.&text=Text%20created%20by%20the%20are%20not%20legally%20qualified.&text=by%20the%20government%20department.readers%20who%20are%20not
133	英国	輸出管理・軍民両用品、ソフトウェアと技術、拷問用品、放射線源 (Export controls: dual-use items, software and technology, goods for torture and radioactive sources)	ガイドライン	2019	2023	ビジネス貿易省	多義的技術	○	輸出管理法に基づき規制されるデュアルユース品目を輸出するためのライセンス取得に関するガイダンス。	×	×	無し	-	(GOV.UK) https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources#dual-use-items-software-and-technology
134	英国	1977年特許法 (Patent Act 1977)	法律	1977	2021	政府	その他	○	発明の特許付与の基準、手続等を規定する法律。国家安全保障や公共の利益を害する恐れがある特許出願について、その公表を禁止・制限することができる。また、当該情報が国家安全保障や公共の利益を害すると判断された場合には、当該特許出願を取り消すことができる。	○	○	有り	研究開発成果の特許を取得する場合で、国家安全保障や公共の利益を害する恐れがある特許出願について、その公表を禁止・制限	(GOV.UK) https://www.legislation.gov.uk/ukpga/1977/37/contents
135	英国	政府における知識資産管理 (Knowledge asset management in government)	ガイドライン	2021	-	政府技術移転局、科学・イノベーション・技術省、財務省、ビジネス・エネルギー産業戦略省	その他	○	政府が保有する知識資産を定義し、その管理や保護等に関するガイダンス	○	○	有り	知識資産を生み出す可能性がある活動の一つとして研究開発が挙げられている	(GOV.UK) https://www.gov.uk/government/publications/knowledge-asset-management-in-government
136	フランス	国防秘密保全に関する府行府一般通達第1300号 (INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE N° 1300 SUR LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE)	通達	2011	2021	政府	その他	○	秘密情報の保護に関する一般原則を規定。防衛、治安、金融・経済産業の保護、科学・文化遺産の保護等の活動全般等に関する情報等を国防秘密として定義。公開された場合の国防への損害の大きさに応じて3段階で情報を区分 (Very Secret Defense, Secret Defense, Confidential Defense)。機密情報や資料を国内外で輸送する際の取扱いについて規定している (ディビジョン4)	○	×	無し	-	(レジフランス) https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000033293465
137	フランス	個人データの保護に関する法律 (La loi Informatique et Libertés)	法律	1978	2018	政府 (CNIL)	その他	○	フランスの個人情報保護に関する法律であり、個人番号若しくは個人に固有な1又は2以上の要素を通じて直接的又は間接的に識別され又は識別することが可能である自然人（データ主体）に関する全ての情報を個人情報の定義としている。なお、2018年にEUの一般データ保護規則(GDPR)を反映して改正され、個人情報に関する個人の権利(データアクセス、修正、消去についての権利等)が強化された。	○	×	無し	-	(France Vie publique) https://www.vie-publique.fr/loi/20787-loi-2018-protection-des-donnees-personnelles-cnll-rsgd (CNIL) https://www.cnil.fr/fr/la-loi-informatique-et-libertes
138	フランス	公衆と行政の関係に関する法典 (Code des relations entre le public et l'administration)	法律	2015	2018	政府 (法務省)	その他	○	フランスの情報公開制度に関する法律として「行政及び公衆間の関係改善のための諸措置ならびに行政・経済・社会制度改善にかかわる諸措置に関する1978年7月17日法律」に代わり2015年に制定されたものである。情報公開に関する規程の中で①政府及び執行にかかわる責任ある機関における普通的情報、②防衛上の秘密、③フランスの外交政策の実施、④国家の安全、治安、人々の安全又は行政機関の情報システムの安全、⑤通関と公債、⑥裁判所の手続又は手続手続の実施（但し、権限ある機関による承認がある場合は除く）、⑦捜査機関によるあらゆる犯罪の捜査及び予防、⑧環境法典L1224-4条を除き、法律によって保護されたその他の秘密が情報公開の適用外である不表示情報として挙げられている。	○	×	無し	-	(レジフランス) https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000031367557 (経産省資料「経産省資料「各国における情報公開制度に関する調査研究」」) https://www.soumu.go.jp/main_content/000628852.pdf
139	フランス	営業秘密の保護に関する法律	法律	2018	-	政府	多義的技術	○	EUが2016年に制定した企業秘密の保護に関する指令を反映する形で制定した法律であり、①それ自体またはその要素の正確な複製及び開示によって重要な事案に加え、新たにAI、半導体等の重要な技術に係る研究開発分野への投資の奨励に資する者が容易にアクセスすることができないものであること、②「秘密であるが故に、実質的、または潜在的な商業価値を有していること、③秘密性を維持するために状況を考慮した上で正当な保有者による合理的な保護措置の対象であることを要件として営業秘密を定義している。	○	×	無し	-	(レジフランス) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037262111/ (EU「企業秘密の保護に関する指令」) https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/trade-secrets_en
140	フランス	フランスへの対内投資に関する命令 2019 年 12 月 31 日第 2019-1590 号 (Décret n° 2019-1590 du 2 décembre 2019 relatif aux investissements é trangers en France)	行政命令	2019	-	政府 (経済・財務省)	その他	○	フランスの外国投資管理を強化するための行政命令であり、既存の審査対象事業だった防衛事業やエネルギー等公共の安全又は国防防衛にとって重要な事業に加え、新たにAI、半導体等の重要な技術に係る研究開発分野への投資の奨励に資する者が容易にアクセスすることができないものであること、②「秘密であるが故に、実質的、または潜在的な商業価値を有していること、③秘密性を維持するために状況を考慮した上で正当な保有者による合理的な保護措置の対象であることを要件として営業秘密の取得についても対内直接投資に係る規制の対象とされた。	×	×	無し	-	(レジフランス) https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039727443 (経産省資料「各国における対内直接投資規制の動向」」) https://www.meti.go.jp/policy/trade_policy/vto/3_dispute_settlement/32_wto_rules_and_compliance_report/322_past_columns/2021/2021-8.pdf
141	フランス	国防機密の分類及び保護の方法に関する政令 (Décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale)	行政命令	2021	-	政府 (経済・財務省)	その他	○	首相による国防機密の分類および保護の機軸に関する政令（デクレ）である。2021年7月1日より作成された国防機密および媒体に関わる認可や契約の取扱い方法を示すもので、国防機密情報の分類を変更することで、より適切な情報保護を目的とする。	×	×	無し	-	(ANSSI) https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-muage-securumcloud/faq-avant-de-se-lancer-dans-la-qualification-securumcloud/
142	フランス	SecNumCloudビザ	認証ラベル	2016	-	国立情報システム・セキュリティ庁 (ANSSI)	その他	○	国立情報システム・セキュリティ庁 (ANSSI) が頒布できるセキュリティ基準を満たすと認めたクラウドサービスプロバイダーにあたる認証ラベル。SecNumCloudビザは、認定したプロバイダーやそれらが処理するデータがEU域外の法律の対象とならなよう、対象企業を本社がEU域内にある企業に限定している。	○	×	無し	-	(SecNumCloudビザ) https://www.ovhcloud.com/en-gb/enterprise/certification-conformity/secnumcloud/
143	フランス	二重用途物品の輸出、移渡、仲介および輸送の管理に関するEU域内体制を確立する 2009年5月5日付理事会規則428/2009 (COUNCIL REGULATION (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items)	EU規則	2009	-	EU	その他	○	EUにおける二重用途（デュアルユース）品目（ソフトウェアや技術を含む）の輸出、移渡、仲介および輸送の管理制御の確立を目的とする。二重用途品目リストに掲載されている物品の輸出は、官電当局の認可を必要とする。リストに不記載であっても、輸出入国や利用等の懸念がある場合は、許可が必要となる。物品の輸送には、電子媒体によるソフトウェアや技術のEU域外の宛先への送達を含む。	×	×	無し	-	(EUR-Lex) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0428
144	フランス	共通輸出規則に関する2015年3月11日付州議会・理事会規則2015/479 (REGULATION (EU) 2015/479 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 2015 on common rules for exports)	EU規則	2015	-	EU	その他	○	EUから第三国向けの輸出に関する共通規則として、加盟国が保護策を導入する場合の手続きを確立する。保護策は、公序良俗、公共政策または公衆、または人権、動物、植物の健康と生命の保護、国交、または産業的および商業的財産の保護を目的とする措置が必要となる場合を対象と、当該規則は、すべての工業製品および農産物に適用される。	×	×	無し	-	(EUR-Lex) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R0479
145	フランス	国防機密の分類及び保護の方法に関する政令 (Décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale)	法律	1978	2024	政府	その他	○	1978年に発行された個人データの処理を規制する法律で、データ保護法として知られている。個人データに対する権利として、情報を得る権利・異議を唱える権利・情報へアクセスする権利・誤ったデータを修正する権利が挙げられている。	○	×	無し	-	(レジフランス) https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165357/LEGISCTA000006165357
146	フランス	フランス刑法 (Code pénal)罰則 (第413条の9～12)	法律	2016	2023	政府	その他	○	2016年に発行された法律で、デジタル社会における様々な側面に関する法的枠組みを提供することを目的としており、「オープンデータアクセス権の強化」「ネット中立性の確保」「デジタル教育の促進」「オープンソースソフトウェアの利用」「デジタルアクセシビリティの向上」について記載されている。	×	×	無し	-	(レジフランス) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202935
147	フランス	国防法典 (Code de la défense)	法律	2004	2024	政府	その他	○	フランスの軍事および防衛に関連するさまざまな法律と規制を体系化し、整理したものである。国防法典のフランス国防法典第2311条の2および第2311条の3において機密情報の分類について以下のように規範している 機密情報およびメディアは2段階の分類に従う 最高機密 (Très Secret) : その開示またはアクセスが国防および安全保障にとって例外的に重大な結果をもたらす情報および媒体に適用される 機密 (Secret) : その開示またはアクセスが国防および安全保障に害を及ぼす可能性が高い情報および媒体に適用される	△	×	無し	-	(レジフランス) https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI0000039445194 https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI0000039445192
148	ドイツ	連邦保安審査に関する機密事項の保護に関する法律 (Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen)	法律	1994	2021	政府 (内務省)	その他	○	行政における、公共の利益のために機密にする必要がある情報を対象とし、同情報を取り扱う者に対するセキュリティクリアランス等を規定。 公共の利益のために機密にする必要のある事実、対象又は情報は、 ①厳秘（権限のない者が知るに至ることで、国又は州の存立又は生命にとり重要な利益 が損なわれる場合）、 ②厳秘（国又は州の保安又は利益に重大な害を生じさせる場合）、 ③秘（国又は州の利益にとって有害となり得る場合）に区分して指定。	○	△	無し	-	(ドイツ政府HP) https://www.gesetze-im-internet.de/s_g/BjNR086700994.html
149	ドイツ	資料の秘密保護のための一般管理規則 (機密事項指定規則) (Allgemeine Verwaltungsvorschrift zum materiellen Geheimenschutz)	規則	2023	-	政府 (内務省)	その他	○	保安審査法に基づき、その実施に関する規則を定めるもの。 機密情報を扱う組織の職務、機密情報の管理、保存、破壊の方法等、機密情報の取扱いに関する規定を掲置。	○	△	無し	-	(ドイツ政府HP) https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_13032023_SlHS40011405.htm
150	ドイツ	刑法典	法律	1871	2022	政府 (司法省)	その他	○	ドイツ刑法。 93条～101条において、国家機密の漏洩に対する罰則を定める。 国家機密の定義として、「ドイツ連邦共和国の対外安全保障に重大な不利益を及ぼす危険を回避するために、限られた範囲の者のみがアクセスすることができ、かつ、外面から秘匿されなければならない事実、物または知識」と定めている。	○	△	無し	-	(ドイツ政府HP) https://www.gesetze-im-internet.de/stgb/BjNR001270871.html
151	ドイツ	連邦データ保護法 (Bundesdatenschutzgesetz)	法律	2017	2021	政府 (データ保護と情報の自由のための連邦委員会)	その他	○	個人情報保護全般に関する規定、情報の域外への移転に関する規定、安全保障分野等での例外規定を掲置。	○	○	有り	研究を目的とした場合の適用除外がある	(ドイツ政府HP) https://www.gesetze-im-internet.de/bds_g/BjNR209710017.html
152	ドイツ	情報自由法	法律	2005	2020	政府 (内務省)	その他	○	行政庁の保有する情報に対する情報開示請求権、行政庁の保有する情報の目録の公表義務、適用除外情報等を規定。	○	△	無し	-	(ドイツ政府HP) https://www.gesetze-im-internet.de/ifg/BjNR2772200005.html
153	ドイツ	営業秘密の保護に関する法律 (Gesetz zum Schutz von Geschäftsgeheimissen (GeschGehG))	法律	2019		政府 (環境・自然保護・原子力安全・消費者保護省)	その他	○	営業秘密を定義し、その違法な取得、使用及び開示に対する保護に関して規定するもの。	○	△	無し	-	(ドイツ政府HP) https://www.gesetze-im-internet.de/geschgehg/BjNR046610019.html
154	ドイツ	外国貿易及び支払法	法律	2013	2022	政府 (経済・気候変動省)	多義的技術	○	外国貿易における取引が制限される分野等を規定するもの	○	△	無し	-	(ドイツ政府HP) https://www.gesetze-im-internet.de/awg_2013/BjNR148210013.html

連番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究開発に関連する情報保全規定の有無	研究開発に関連する情報保全規定の概要	出所
155	ドイツ	BSI法	法律		2009年	政府（情報セキュリティ庁（BSI））	サイバー	○	情報技術安全庁（BSI）における情報技術セキュリティに関する任務を規定するとともに、重要インフラ運用者によるインフラに係る重要部品の使用開始時における事前通知する義務を規定。	○	△	無し	-	（ドイツ政府HP） https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
156	ドイツ	原子力法	法律	1959	2022	政府（環境・自然保護・原子力安全・消費者保護省）	その他	○	原子力施設を設置する者のライセンス取得義務等を定めるもの	△	△	無し	-	（ドイツ政府） https://www.gesetze-im-internet.de/atg/BJNR008140959.html
157	ドイツ	健康データ保護に関するガイドンス	ガイドライン	2018	-	政府（経済・気候変動省）	その他	○	連邦データ保護法を補完する形で、医療業界における個人情報保護に関して包括的に定めるもの	○	○	有り	研究を目的とした場合の適用除外がある	（経済気候変動省） https://www.bmwk.de/Redaktion/EN/Dossier/guidelines-on-the-protection-of-health-data.html
158	ドイツ	銀行法	法律	1961	2023年	政府（金融監督庁）	その他	○	金融機関に関する総括的な法律。 業務上知りえた情報の守秘義務や、マネロやテロファイナンス対策の観点からの情報保全すべし。	○	×	無し	-	（ドイツ政府HP） https://www.gesetze-im-internet.de/kredwvg/BJNR008810961.html
159	オーストラリア	Protective Security Policy Framework(PSPF)	ガイドライン	2018	-	政府	その他	○	PSPFはオーストラリア政府機関が国内外の人々、情報、資産を保護するための政府のセキュリティ保護ポリシーを定めたものである。このフレームワークの中で①個人の安全等、②政府組織の能力、資産、法執行・政策実行能力等、③国の経済、④国のインフラ、⑤国際関係、⑥治安・国防・インテリジェンス活動を機密情報として区分している。	○	×	無し	-	(PSPF) https://www.protectivesecurity.gov.au/publications-library/policy-8-sensitive-and-classified-information#~:text=The%20Australian%20Government%20uses%203%20security%20classification%3A%20PROTECTED,for%20applying%20the%20relevant%20sensitive%20r%20security%20classification.
160	オーストラリア	Export Control Act 2020	法令	2021	-	政府	その他	○	オーストラリア領土からの農産物や食品を含む商品の輸出規制を行うための枠組みである。人間、動物物の生命または健康の保護、あるいは国際的な法を目的として、本法に基づき規制の制定により、所定の商品の輸出を禁止できる。同法に基づいて入手された情報（個人情報を含む）を「保護情報」として、その使用や開示条件を規定している。	○	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2021C00139
161	オーストラリア	Defence Trade Controls Act 2012	法令	2018	-	政府	その他	○	防衛貿易管理法（DTC）は、オーストラリアの国益保護を目的として、防衛輸送物資リスト（DSGL）記載品目、および米露防衛貿易協力条約の対象品目の国外との取引を規制する。規制の対象は、軍事および二重用途の技術、ソフトウェアおよび物品である。これらの品目の取引には、国防大臣の許可が必要で、取引を許可された者は、記録を保持する義務がある。大臣は、法の執行に関わる情報収集を行うことができる。	×	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2012C00231
162	オーストラリア	Defence Export Controls (DEC)	ガイドライン	-	-	政府	その他	○	防衛輸出規制（DEC）は、オーストラリアの国益保護を目的として、軍用・二重用途品の輸出を規制する法律（DTC、米露防衛貿易協力条約、防衛法等）の遵守の増進と監視を行う枠組みである。規制の対象は、軍事および二重用途の技術、ソフトウェアおよび物品である。DECは、防衛輸送物資リスト（DSGL）で指定された物品または技術の輸出、供給、仲介、公開の承認や拒否を行う。	×	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2018A00029
163	オーストラリア	研究開発に関する全般的な概説	ガイドライン	-	-	政府	その他	○	オーストラリア保健医学倫理委員会（NHMRC）が資金提供を行う研究に関わる法規制の概要を説明する。オーストラリア政府が資金提供を行う研究について、政府機関の役割を説明する。	×	○	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2018A00063
164	オーストラリア	Management of Data and Information in Research	ガイドライン	-	-	政府	その他	○	オーストラリア保健医学倫理委員会（NHMRC）が作成した、同国の研究実施規範（Australian Code for the Responsible Conduct of Research）」を導入ガイドラインである。オーストラリアの機関が支援する研究に関わるデータおよび情報の取扱いの明確化を目的とする。	○	○	有り	研究機関の責任の明確化を行う（①研究機関は、データ管理ポリシーを作成し、データの生成から収集、アクセス、使用、分析、開示、保管、保持、廃棄、共有および再利用に至るまで、適切な取り扱いを確保する。②研究者を対象として、組織の管理ポリシーへの理解トレーニングを実施する。③研究実施規範の調査ガイドに基づき、規範の遵守について管理および調査を行う）。④研究者は、ポリシーを順守してデータ管理を行う。研究プロジェクトで使用、またはそこから派生した機密情報のほか、国家安全保障情報や輸出規制の対象となる情報の保護を確保する必要がある。⑤研究データや一次資料の長期保存、および開示対象の決定を行う責任を負う）。	(Standards Australia) https://www.standards.org.au/standards-catalogue/standard-details
165	オーストラリア	Guidelines to counter foreign interference in the Australian university sector	ガイドライン	2019	-	政府	その他	○	オーストラリア政府と同国大学が共同開発した、大学研究活動への外国の干渉に対処するためのガイドラインである。外国からの干渉により主権や国益が損なわれるリスクを評価し、軽減することを目的とする。	×	○	無し	-	https://www.globalipdb.inpiti.go.jp/jpwp/wp-content/uploads/2016/04/3b858fec4f503cbeb715c6a044c28ef6.pdf
166	オーストラリア	Australian Government intellectual property manual	ガイドライン	2018	-	政府	その他	○	オーストラリア政府職員を対象とする政府の知的財産（IP）保護のガイドラインである。Public Governance, Performance and Accountability Act 2013 (PGPA) に基づき、効率的かつ効果的な方法でIPを識別、記録、使用、評価、保護、活用するためのシステムの実装を含むIP管理を目的とする。	×	○	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2020C00023
167	オーストラリア	1988年プライバシー法	法律	1988	2022	政府	その他	○	1988年プライバシー法はオーストラリアの個人情報保護に関する法律で、識別された個人又は合理的に識別可能な個人に関する情報又は意見も個人情報と定義し、連邦公共部門および民間部門における個人情報の収集、使用、保管、開示に関する取扱いについて定めている。	○	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2020A00116
168	オーストラリア	情報自由法	法律	1982	2023	政府	その他	○	1982年情報自由法はオーストラリアの個人又は組織に対してオーストラリア政府が保有している情報へのアクセス要求ができる権利を与える法律である。ただし①国家安全保障、防衛または国防関係に影響を与ええる文書、②内閣文書、③法の執行及び法の完全の保護に関する文書、④制定法の秘密指定が適用される文書、⑤法執行物の対象となる文書、⑥機密入手した資料を含む文書、⑦開示が国会倫理委員または法廷倫理委員となる文書、⑧営業秘密または商業的に価値のある情報を開示する文書、⑨冤罪人名義及び関連書類が挙げられており、また、公益条件付不開示情報として（公共の利益に反しない限り、通常、条件付きで免除された文書へのアクセスを許可する必要がある）で、御達邦と州の関係、⑩審議プロセス、⑪連邦またはノーフォーク島の金銭的利益または財産の利益、⑫機関の特定の運営、⑬個人のプライバシー、⑭ビジネスに関する文書、⑮研究に関する文書、⑯オーストラリア経済に関する文書に該当するものは情報公開の適用外である不開示情報として挙げられている。	○	×	無し	-	(DEFENCE SECURITY PRINCIPLES FRAMEWORK) https://www.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf
169	オーストラリア	重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）	法律	2018	2022	政府（内務省）	その他	○	重要インフラ安全保障法は、国の重要インフラへの外国の関与によってもたらされるオーストラリアの安全保障上のリスクを管理するため法律であり、オーストラリアの重要インフラ分野として通信、データ保存・処理、金融、上下水道、エネルギー、ヘルスケア・医療、高度教育・研究、食品、輸送、宇宙技術、防衛等を挙げている。	○	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2019C00043
170	オーストラリア	外国影響力透明化法(FITSA)（Foreign Influence Transparency Scheme Act 2018）	法律	2018	-	政府	その他	○	FITSAは、外国政府又は外国企業に代わって政治的な活動を行う場合に、依頼者や活動内容等の情報の登録及び開示が義務付けられることとされている。	×	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2018A00063/latest/text
171	オーストラリア	ISO/IEC 27002（AS/NZS ISO/IEC 27002:2006）	規格	2008	-	業界団体（Standards Australia）	その他	○	国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定した、企業などの組織における情報セキュリティマネジメントシステムの仕様を定めた規格で、オーストラリアではStandards Australiaが対応をしている。	○	×	無し	-	(SAI Global) https://www.saiglobal.com/PDFTemp/Previews/OSH/AS/AS20000/27000/27002-2006+A11.pdf
172	オーストラリア	営業秘密の保護（判例法による）	法律	1969	-	政府	その他	○	オーストラリアの法律では営業秘密は単なる機密情報の1つの見なされており、営業秘密の保護に関する法令、規則等はないが、判例法によって営業秘密について①情報が単に包括的な文書で示されているのではなく、具体的に特定されていること、②情報は秘密のものであり、秘密性が維持されていること、③情報をその所有者から受領した際に、情報に対する守秘義務が受領者に課されていること、④情報の不正利用が現実には発生したが、不正利用が不可能な状況にあることと定義されている。	△	×	無し	-	(新聞国等知財情報データベース) https://www.globalipdb.inpiti.go.jp/jpwp/wp-content/uploads/2016/04/3b858fec4f503cbeb715c6a044c28ef6.pdf
173	オーストラリア	外資による取得および買収に関する法律	法律	1975	2021	政府（外国投資審査委員会）	その他	○	買収と買収の規制・監督を目的とした法律であり、投資額の大かにかかわらず、国家安全保障の観点から重要とされる土地や事業に対する外国投資は、オーストラリア政府による審査の対象となるとの視覚あり。	×	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2021C00022
174	オーストラリア	外国関係法（Australia's Foreign Relations (State and Territory Arrangements) Act 2020）	法律	2020	-	政府（外務貿易省）	その他	○	豪の州や準州、及び大学等が外国政府と協定を締結する際の外務大臣への事前通知及び外務大臣からの承認取得を義務付けるもので、州や準州及び大学等と外国政府の取り決めがオーストラリアの外交政策と一致していない場合には取り決めの拒否を行うことができる。	×	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/C2020A00116/asmade
175	オーストラリア	防衛セキュリティ原則の枠組み(DEFENCE SECURITY PRINCIPLES FRAMEWORK)	枠組み	2020	-	政府（国防省）	多義的技術	○	国防省の職員や契約により国防関係の業務に従事する人物たちが取り扱う情報について、OFFICIAL、OFFICIAL：Sensitive、PROTECTED、SECRET、TOPSECRETに分類をし、それらに対するアクセス権限やデータ等の取扱いについて規格している。	○	×	無し	-	(Australian Government DoD) https://www.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf
176	オーストラリア	Freedom of Information Act 1982	法律	1982	2024	政府	その他	○	情報の自由と、連邦政府及びその機関の公式文書へのアクセス権を一般の人々に保証する法律。	○	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/C2004A02562/latest
177	オーストラリア	刑法（第91条）	法律	1995	2019	政府	その他	○	オーストラリアに対してスパイ行為を行った者に対する罰則等を規定、安全保障に対する害を与える原因の有無や外国に渡す行為の有無、また外国の諜報機関への協力等について15年の禁錮から終身刑までの罰則が規程されている。	×	×	無し	-	(Federal Register of Legislation) https://www.legislation.gov.au/Details/C2019C00043
178	インド	National Information Security Policy and Guidelines	ガイドライン	2013	-	政府（内務省）	その他	○	政府および公共部門の組織等の管理下または所有権下にある情報を、そのライフサイクル全体を通じて保護することを目的としたガイドラインで、ガイドラインの行政組織や採用可能なすべての情報については全てTop secret、Secret、Confidential、Restrictedに分類すべきであるとの記載がある。	○	×	無し	-	(NATIONAL INFORMATION SECURITY POLICY AND GUIDELINES) http://64.100.38.63/files/NATIONAL%20INFORMATION%20SECURITY%20POLICY%20AND%20GUIDELINES.pdf
179	インド	The Foreign Trade (Development & Regulations) Amendment Act, 2010	法律	2010	-	政府	その他	○	インドの輸出入を管理する「1992年外国貿易（開発・規制）法」を改正し、規制及び罰則を強化することを目的とした法律。輸出入の定義を商品だけでなく「技術」、「役務」にも拡大し、原子力や大量破壊兵器などの国家安全保障に関わる分野を「特定物品、役務および技術」として輸出の禁止・制限を行うことで貿易管理を行っている。	×	×	無し	-	(THE INFORMATION TECHNOLOGY ACT, 2000) https://www.indiacode.nic.in/bitstream/123456789/13116/1/i_t_act_2000_updated.pdf
180	インド	情報技術法（THE INFORMATION TECHNOLOGY ACT, 2000）	法律	2000	-	政府（電子情報技術省）	その他	○	データ保護とプライバシーを扱う法律であり、自然人に関する情報であって、事業者が保有し、又は保有可能性のある他の情報と合わせて、直接的又は間接的に、当該自然人を識別することができる情報を個人情報として定義している。	○	×	無し	-	(THE INDIAN CONTRACT ACT, 1872) https://www.cag.gov.in/uploads/media/Indian-Contract-Act-1872-20200816140128.pdf
181	インド	インド契約法（THE INDIAN CONTRACT ACT, 1872）	法律	1872	2013	政府（法務省）	その他	○	インドの契約（秘密保持契約、雇用契約、技術的ノウハウ契約）に関連する法律であり、契約などに盛り込まれる秘密保持義務に関して規程している。	○	×	無し	-	(「国開知財制度研究会」報告書) https://www.globalipdb.inpiti.go.jp/jpwp/wp-content/uploads/2018/12/e4747330878a0ca6f11c5f313e4c71.pdf

連番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究開発に関連する情報保全規定の有無	研究開発に関連する情報保全規定の概要	出所
198	韓国	保安業務規定（一部改正）	規定	1964	2021	政府 (国家情報院)	その他	○	「国家情報院法」第4条により国家情報院の職務中にセキュリティ業務遂行に必要な事項を規定することを目的としたもの。 国家情報院法で国家秘密が定義されており、それに基づきセキュリティ業務規定で秘密区分がなされている。そしてセキュリティ業務規定施行規則で秘密分類指針が示されており、中央行政機関は国家情報院から配布される秘密部分分類指針によって各機関の情報を分類することになっている 国家秘密：国家安全に対する重大な不利益を回避するために限られた人へのみ得が許され、範囲又は反団体人に秘密にしておくべき事実、物又は知識	○	×	無し	-	(韓国国家法令情報センター) https://www.law.go.kr/lsinfoP.do?lsSeq=225717&lsId=003649&chClsCd=010202&urlMo-de=lsinfoP&viewCls=lsinfoP&efYd=20210101&vSet=%EA%B3%B4%EC%95%88&ancYnChk=000000
199	韓国	保安業務規定施行規則（一部改正）	規則	1964	2022	政府 (国家情報院)	その他	○	「セキュリティ業務規定」の施行に必要な事項を規定することを目的としたもの。 中央行政機関等の長は、国家情報院長とあらかじめ協議して、セキュリティ業務規定に基づいた各機関のセキュリティ業務施行細則を作成・施行することになっている そのため、1級秘密～III級秘密に分類されている。また、情報上開放上の非公開情報で職務遂行上保護が必要なものを対外秘としている それにより秘密部分分類指針が作成・配布されるが、一般には公開されていない	○	×	無し	-	(韓国国家法令情報センター) https://www.law.go.kr/admRuLL.sinfoP.do?admRuId=51518&efYd=4&admRuNm=%EB%B3%B4%EC%95%88%EC%97%85%EB%AC%B4%EC%A8%B7%9C%EC%A8%B3%B5%EA%B0%9C%EC%A0%95%20%EC%88%B9%9C%ED%96%89%EA%B7%9C%EC%B9%99&linkYn=Y#f117-0
200	韓国	公共機関の情報公開に関する法律（一部改正）	法律	1998	2020	政府 (行政安全部)	その他	○	公共機関が保有・管理する情報に対する国民の公開請求及び公共機関の公開義務に関して必要な事項を定めることにより、国民の知的権利を保障し、国政に対する国民の参加と国政運営の透明性を確保することを目的としたもの 本法における「情報」は、公共機関が職務上作成または取得して管理している文書および電子媒体を含むあらゆる形態の媒体などに記録された事項と定義される。 他の法令で秘密・非公開事項に指定された情報や国家安全保障に関連する情報は本法令の適用外となっている	○	△	有り	非公開対象情報（第9条） 公共機関が保有・管理する情報は公開対象となる。ただし、公開された場合、業務の公正な遂行や研究・開発に支障をきたす恐れをもちたると認められる相当な理由がある情報は公開しなくてもよい	(韓国国家法令情報センター) https://www.law.go.kr/lsLinkProc.do?lsNm=%EA%B3%B5%EA%B3%B5%EA%B8%B0%EA%B4%8C%EC%9D%88%20%EC%A0%95%EB%B3%B4%EA%B3%B5%EA%B0%9C%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%B9%95%EA%A0%4C%ChCdsCd=010202&mode=20#
201	韓国	国家空間情報基本法（一部改正）	法律	2009	2021	政府 (国土交通部)	その他	○	国家空間情報体系の効率的な構築と総合的活用及び管理に関する事項を規定することにより、国土及び資源を合理的に利用して国民経済の発展に資することを目的としたもの。 「地上・地下・水上・水中など、空間上に存在する自然的または人工的なオブジェクトに対する位置情報およびこれに関連する空間的認知および意思決定に必要な情報」として「空間情報」を定義し、その保護を義務付けている（第2章、6章）。 中央行政機関、地方自治体、大統領令に定める民間機関（電気・ガス等エネルギー事業者）が空間情報セキュリティ管理規定を整備し、情報の分類を行い公開範囲を規定している。	○	×	無し	-	(韓国国家法令情報センター) https://www.law.go.kr/lsinfoP.do?lsSeq=230207&lsId=010916&chClsCd=010202&urlMo-de=lsinfoP&viewCls=lsinfoP&efYd=20220317&vSet=%EA%B5%AD%EA%B0%80%EA%B3%B5%EA%B0%84%EC%A0%95%EB%B3%B4%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%B5%EA%B0%84%EC%A0%95%EB%B3%B4
202	韓国	環境空間情報セキュリティ管理規定（一部改正）	規定	2008	2022	政府 (環境部)	その他	○	国家空間情報基本法第35条及び同法施行令により、環境部所管国家空間情報セキュリティ業務の遂行に必要な事項を規定することを目的としたもの。 環境部本部、所属機関及び所属公共機関に適用される 環境部が保有する空間情報（航空写真、衛星画像、地図等）の分類を行い、公開範囲を規定。 空間情報の保護及び管理について規定されている（第3章）	○	△	有り	空間情報の公開及び活用（第13条） 公開制限空間情報を業者又は学術研究等の目的で活用しようとする者は、別紙第3号書式を作成し、空間情報提供担当に提出しなければならない。	(韓国国家法令情報センター) https://www.law.go.kr/admRuLL.sinfoP.do?admRuIdSeq=2100000216899&vSet=%EA%B3%B5%EA%B0%84%EC%A0%95%EB%B3%B4
203	韓国	国土交通部国家空間情報セキュリティ管理規定（一部改正）	規定	2009	2022	政府 (国土交通部)	その他	○	「国家空間情報基本法」第35条、同法施行令第24条及び「国家空間情報保安管理基本指針」により国土交通部所管国家空間情報保安業務遂行に必要な事項を規定することを目的としたもの 「国家空間情報基本法」第35条第4号による国土交通部とその所属機関及び傘下公共機関に適用される。 国土交通部が保有する空間情報（航空写真、衛星画像、地図等）の分類を行い、公開範囲を規定。 空間情報保護対策が規定される（第4章）	○	△	有り	公開制限空間情報の公開要件（第16条） ③公開が制限される空間情報を学術研究、公共福祉及び安全等の目的で活用しようとするときは、あらかじめ管理機関の長の承認を受けなければならない。 ②公開が制限される空間情報に対する公開申請があるときは、次の各号の事項等を検討しなければならない。 1.氏名、住所、生年月日などの身元事項 2.所属機関、団体及び役職 3.使用目的と妥当性 4.活用後管理対策	(韓国国家法令情報センター) https://www.law.go.kr/admRuLL.sinfoP.do?admRuIdSeq=2100000215941&vSet=%EA%B3%B5%EA%B0%84%EC%A0%95%EB%B3%B4
204	韓国	農林畜産食品部国家空間情報セキュリティ管理規定（改正）	規定	2009	2013	政府 (農林畜産食品部)	その他	○	国家空間情報に関する法律第28条及び同法施行令第24条と国家地理情報セキュリティ管理基本指針により農林畜産食品部所管国家空間情報セキュリティ業務の遂行に必要な事項を規定することを目的としたもの。 空間情報を生産・構築・管理・流通及び活用する農林畜産食品部及びその所属機関等に適用される（第2条） 農林畜産食品部が保有する空間情報（航空写真、衛星画像、地図等）の分類を行い、公開範囲を規定。 空間情報の保護及び管理について規定されている（第3章）	○	△	有り	③農林畜産食品部長官及び所属機関の長は、所管公開制限空間情報について学術研究等の目的で公開を要請された場合には、次の各号の事項を確認・検討して提供することができる。 1.氏名、住所、住民登録番号などの身元事項 2.所属機関、団体及び役職 3.使用目的と妥当性 4.活用後管理対策	(韓国国家法令情報センター) https://www.law.go.kr/LSW/admRuLL.sinfoP.do?admRuIdSeq=22000000024883#~:text=%EA%B3%B5%EA%B0%84%EC%A0%95%EB%B3%B4%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%B5%EA%B0%84%EC%A0%95%EB%B3%B4%EC%97%90%20%EA%B4%80%ED%95%9C%20%EB%B2%B5%EA%B0%84%EC%A0%95%EB%B3%B4
205	韓国	農村振興庁空間情報セキュリティ管理規定（一部改正）	規定	2008	2013	政府 (農村振興庁)	その他	○	「国家空間情報に関する法律」第28条と同法施行令第24条及び「国家空間情報保安管理基本指針」により、農村振興庁所管空間情報セキュリティ業務の遂行に必要な事項を規定することを目的としたもの。 空間情報を生産・構築・管理・流通及び活用する農村振興庁及びその所属機関に適用される（第2章） 農村振興庁が保有する空間情報（航空写真、衛星画像、地図等）の分類を行い、公開範囲を規定。 空間情報の保護及び管理について規定されている（第3章）	○	△	有り	③庁長及び所属機関の長は、所管公開制限空間情報について学術研究等の目的で公開を要請された場合には、次の各号の事項を確認・検討し、問題がないと判断されれば、これを提供することができる。 1.氏名、住所、住民登録番号などの身元事項 2.所属機関、団体及び役職 3.使用目的と妥当性 4.活用後管理対策	(韓国国家法令情報センター) https://www.law.go.kr/LSW/admRuLL.sinfoP.do?admRuIdSeq=20000000025757
206	韓国	文化財庁国家空間情報セキュリティ管理規定（改正）	規定	2005	2011	政府 (文化財庁)	その他	○	「国家空間情報に関する法律」第28条及び同法施行令第24条と国家空間情報セキュリティ管理基本指針により文化財庁所管国家空間情報セキュリティ業務の遂行に必要な事項を規定することを目的としたもの 空間情報を生産・構築・管理・流通及び活用する文化財庁及びその所属機関に適用される（第2条） 文化財庁が保有する空間情報（航空写真、衛星画像、地図等）の分類を行い、公開範囲を規定。 空間情報の保護及び管理について規定されている（第3章）	○	△	有り	③庁長及び所属機関の長は、所管公開制限空間情報について学術研究等の目的で公開を要請された場合には、次の各号の事項を確認・検討し、問題がないと判断されれば、これを提供することができる。 1.氏名、住所、住民登録番号などの身元事項 2.所属機関、団体及び役職 3.使用目的と妥当性 4.活用後管理対策	(韓国国家法令情報センター) https://www.law.go.kr/LSW/admRuLL.sinfoP.do?admRuIdSeq=20000000017612
207	韓国	産業通商資源部国家空間情報セキュリティ管理規定（一部改正）	規定	2021	2022	政府 (産業通商資源部)	その他	○	「国家空間情報基本法」第35条と同様の法施行令第24条及び「国家空間情報セキュリティ管理基本指針」により、産業通商資源部所管国家空間情報セキュリティ業務の遂行に必要な事項を規定することを目的としたもの 産業通商資源部が保有する空間情報（航空写真、衛星画像、地図等）の分類を行い、公開範囲を規定することになっている 空間情報を生産・構築・管理・流通及び活用する産業通商資源部とその所属機関、公共機関に対して適用される（第3条） 空間情報保護対策が規定される（第4章）	○	△	有り	公開制限空間情報の公開要件（第19条） ③公開が制限される空間情報を学術研究等の目的で活用しようとする者は、別紙第3号書式を作成して管理機関の長に提出し、予め管理機関の長の承認を受けなければならない。 ②管理機関の長は、公開が制限される空間情報に対する公開申請があるときは、申請者の身元を確認し、使用目的及び妥当性、活用後管理対策等を検討しなければならない。	(韓国国家法令情報センター) https://www.law.go.kr/LSW/admRuLL.sinfoP.do?admRuIdSeq=2100000205901
208	韓国	国立海洋調査員国家空間情報セキュリティ管理指針（一部改正）	指針	2010	2020	政府 (海洋水産部)	海洋	○	「国家空間情報基本法」及び「海洋水産部国家空間情報セキュリティ管理規定」により国立海洋調査員所管国家空間情報のセキュリティ業務遂行に必要な事項を規定することを目的としたもの 海洋水産部が保有する空間情報（航空写真、衛星画像、地図等）の分類を行い、公開範囲を規定。 国立海洋調査員とその所属機関及び業務上国立海洋調査員の指導・監督を受ける業者又は団体に適用される。 海洋空間情報保護対策を規定している（第4章）	○	△	有り	公開制限海洋空間情報の公開要件（第18条） ③公開が制限される海洋空間情報を学術研究、海洋水産政策の確立及び施行、公共福祉及び安全等の目的で活用しようとするときは、あらかじめ本廳、所属機関長の承認を受けなければならない。 ②公開が制限される海洋空間情報を提供しようする場合、次の各号の措置をとらなければならない。 1.要請機関では別紙第3号書式を作成し、文書として要請 2.各部署長は、海洋空間情報提供要請の検討後、セキュリティ担当官にセキュリティレビュー要請 3.セキュリティ担当官は、セキュリティ性検討後、各部署長に結果を通知し、海洋空間情報提供要請事項を記録維持 4.資料提供時には別紙第4号書式の受領確認及び保管要領を厳格執行 5.使用期間満了時要請機関では機関長名義の資料保管要領文書を調査員に通報	(韓国国家法令情報センター) https://www.law.go.kr/admRuLL.sinfoP.do?admRuIdSeq=2100000195397&vSet=
209	韓国	国土地理情報院国家空間情報セキュリティ管理規定（他法改正）	規定	2013	2015	政府 (国土地理情報院)	その他	○	国家空間情報基本法第28条と同様の法施行令（国土交通部令）、国土地理情報院保安業務管理指針（国土地理情報院規程）により、国土地理情報院空間情報保安業務の遂行に必要な事項を規定することを目的としたもの。 国土地理情報院及び業務上国土地理情報院の調整監督を受ける業者又は団体に適用される。 国土地理情報院が保有する空間情報（航空写真、衛星画像、地図等）の分類を行い、公開範囲を規定。 空間情報の保護・管理に関する規定を定めている（第10条）	○	△	有り	国土地理情報院長は、所管公開制限空間情報について学術研究等の目的で公開を要請された場合には、次の各号の事項を確認・検討して提供することができる。 1.氏名、住所、住民登録番号などの身元事項 2.所属機関、団体及び役職 3.使用目的と妥当性 4.活用後管理対策	(韓国国家法令情報センター) https://www.law.go.kr/lsLinkProc.do?lsNm=%EA%B5%AD%EA%B0%80%EC%97%B0%EA%B5%AC%EA%B0%8C%EB%B0%9C%ED%98%81%EC%B8%A0%EB%B2%95%95&chClsCd=010202&mode=20#
210	韓国	国家研究開発革新法（一部改正）	法律	2021	2022	政府 (科学技術情報通信部)	その他	○	国家研究開発事業の推進体制を革新し、自律的で責任ある研究環境を造成することで国家革新力を高め、国民経済の発展と国民の生活の質向上に資することを目的としたもの。 研究開発情報として、以下を定義 イ、国家研究開発事業・研究開発課題など研究開発の遂行に関する情報。 ロ、研究開発機関・研究者など研究開発を行う主体に関する情報。 ハ、研究開発成果の名称・種類・所属機関など研究開発成果に関する情報。 ニ、その他、国家研究開発事業の推進に必要な情報として大統領令で定める情報 上記について、科学技術情報通信部の示す情報処理基準に即した情報の取り扱いが求められる	△	○	有り	- 研究開発情報の処理等（第19条） 科学技術情報通信部長官は、研究開発情報の処理（研究開発情報を収集・生産・管理及び活用すること）に関する基準（「情報処理基準」）を告示しなければならない - 統合情報システム構築及び運営（第20条） 科学技術情報通信部長官は、内閣府国家研究開発事業の推進及び研究開発情報の処理のための国家研究開発事業統合情報システム（「統合情報システム」）を構築して運営することができる - 国家研究開発事業等の保安（第21条） 関係中央行政機関の長及び研究開発機関の長は、所管国家研究開発事業及び研究開発課題に関連して研究開発成果等大統領令で定める重要情報が流出しないよう保安対策を樹立・施行しなければならない	(韓国国家法令情報センター) https://www.law.go.kr/lsLinkProc.do?lsNm=%EA%B5%AD%EA%B0%80%EC%97%B0%EA%B5%AC%EA%B0%8C%EB%B0%9C%ED%98%81%EC%B8%A0%EB%B2%95%95&chClsCd=010202&mode=20#

連番	国	名称	種別	策定年	最終更新	所管	産業領域・技術分野	情報入手容易性*	概要	情報に関する取扱いの規定の有無	研究・開発に関する規定の有無	研究開発に関連する情報保全規定の有無	研究開発に関連する情報保全規定の概要	出所
211	韓国	科学技術情報通信部所管科学技術分野研究開発事業セキュリティ管理指針（一部改正）	指針	2014	2019	政府 (科学技術情報通信部)	その他	○	「科学技術情報通信部所管科学技術分野研究開発事業処理規定」の第40条第4項により、科学技術情報通信部所管研究開発事業の安全管理に必要な事項を定めることにより、先端科学技術及び研究結果の流出を防止することを目的としたもの 科学技術情報通信部所管研究開発事業を遂行する機関及び研究者、処理規定第10条の専門機関及び第11条の研究開発事業団に適用される	△	○	有り	研究機関独自のセキュリティ管理規定 専門機関の長及び研究開発事業を遂行する研究機関の長は、研究開発事業を遂行に関連する主要なセキュリティ資料等の無断流出を防止するため、次の各号の事項を反映し、独自のセキュリティ管理規定を設け、運営しなければならない（第5条） 1. 研究セキュリティ審議会の構成及び運営に関する事項 2. 研究開発事業課題遂行に関連するセキュリティ等級分類及びセキュリティ対策 3. 研究開発事業課題遂行に関する情報資料、研究施設、参加研究員に対するセキュリティ措置 4. 研究内容及び成果物の対外発表時のセキュリティ措置	(韓国国家法令情報センター) https://www.law.go.kr/%ED%96%98%EC%A0%95%EA%B7%9C%EC%B9%99/%EA%B3%BC%ED%95%99%EA%B8%B0%EC%88%A0%EC%A0%95%EB%B3%B4%ED%86%B5%EC%88%A0%EB%B6%B0%EC%B8%BC%EA%B4%B0%EA%B3%BC%ED%95%99%EA%B8%B0%EC%88%A0%EB%B6%B4%EC%95%BC%EC%97%B0%EA%B5%AC%EA%B0%9C%EB%B0%9C%EC%82%AC%EC%97%B5%EB%B3%B4%EC%95%88%EB%B4%B0%EB%A6%AC%EC%A7%B0%EC%B9%A8/
212	韓国	原子力安全法（一部改正）	法律	2011	2022	政府 (原子力保安委員会)	その他	○	原子力の研究・開発・生産・利用等による安全管理に関する事項を規定し、放射線による災害の防止と公共の安全を図ることを目的としたもの 原子力安全委員会は、公共の安全を図るために原子力利用施設に対する建設許可及び運営許可に関する審査結果と原子力安全管理に関する除染結果など大統領令で定める情報を積極的に公開しなければならない。ただし、国家の重大な利益を著しく損なう恐れがある場合、公開しないことができる。 放射線健康影響調査に関連する業務に従事する者又は従事した者は、職務上知った個人情報又は秘密を漏洩したり、職務上目的以外の目的での使用を禁止されている	△	×	無し	-	(韓国国家法令情報センター) https://www.law.go.kr/IsLinkProc.do?lsNm=%EC%B9%B0%EC%B9%90%EC%B9%90%EB%A0%A5%EC%95%86%EC%A0%B4%EB%B2%95&chrClsCd=010202&mode=20#1032
213	韓国	海洋漁業開発基本法（一部改正）	法律	2002	2022	政府 (海洋水産部)	海洋	○	海洋及び水産資源の合理的な管理、保全及び開発並びに水産業の振興のための政府の基本方針及び指針を定めることにより、国民経済の発展及び国民の福祉の向上に寄与することを目的としたもの 海洋開発情報化の推進に関する規定の中で、情報の取扱いについて規定されている 漁業研究機関等の設置、運営及び促進に関する法律の定めるところにより、水産水産資源の合理的な管理、保全、開発及び利用のための研究及び科学技術開発のための研究機関を設置し、及び育成することができる旨の規定あり（第30条）	△	△	無し	-	(韓国国家法令情報センター) https://www.law.go.kr/IsLinkProc.do?lsNm=%ED%95%B4%EC%96%91%EC%B8%98%EC%B2%B0%EB%B0%BC%EC%A0%B4+%EA%B8%B0%EB%B3%B8%EB%B2%95&chrClsCd=010202&mode=20&ancYnChk=0&AJAX
214	韓国	海洋漁業情報の収集、管理及び共同利用に関する規程（一部改正）	規定	2017	2020	政府 (海洋水産部)	海洋	○	海洋漁業開発基本法第32条及び同法施行令第23条の規定により、海洋及び海洋漁業資源の合理的な管理、保全、開発及び利用並びに水産業の振興のための海洋漁業情報の収集、管理及び共同利用に関する事項を定めることを目的としたもの 「海洋漁業情報」とは、海洋及び水産資源の合理的な管理、保全、開発、利用及び促進に関する情報であって、海洋水産大臣が作成し、収集し、又は管理するものと定義される	○	×	無し	-	(韓国国家法令情報センター) https://www.law.go.kr/IsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EC%A0%95%EB%B3%B4+%EA%B4%B0%EB%A6%AC%undefineId
215	韓国	対外貿易法（一部改正）	法律	1987	2022	政府 (産業通商資源部)	多岐的技術	○	対外貿易の振興、公正な取引秩序の確立及び国際収支のバランスと通常の拡大を図ることにより、国民経済の発展に貢献することを目的としたもの 戦略物資の輸出に統制に必要な情報等に関して規定がされている。また、貿易に関する履行のために収集した情報の第三者への提供や漏洩、使途目的以外の利用に関しても規定している	△	△	有り	自律水準貿易取引者 産業通商資源部長官は、企業又は大統領令で定める大学及び研究機関の自律的な戦略物資管理能力を高めるために、戦略物資の有無に対する判定能力、輸入及びエクスポートに対する分析能力など、大統領令で定める機能を備えた貿易取引者を自律水準貿易取引者として指定することができる（第25条）	(韓国国家法令情報センター) https://www.law.go.kr/IsInfP.do?lsSeq=242931&lsId=001467&chrClsCd=010202&urlMoDe=IsInfP&viewCls=IsInfP&etYd=20221211&vSct=%EB%B8%80%EC%99%B8%20%EB%AC%B4%EC%97%AD&ancYnChk=0#0000
216	韓国	不正競争防止および営業秘密保護に関する法律（一部改正）	法律	1962	2021	政府 (特許庁(産業財産保護政策課))	その他	○	不正競争行為と他者の営業秘密の侵害行為を規制するもの。「営業秘密」は「公然と知られておらず、独立した経済的価値を有するものである、相当な努力によって秘密に維持された生産方法、販売方法、その他営業活動に有用な技術上又は経営上の情報」と定義されている	△	×	無し	-	(韓国国家法令情報センター) https://www.law.go.kr/LSW/IsLinkProc.do?lsNm=%EB%B6%B0%EC%A0%95%EA%B2%B0%EC%9F%B3%EB%B0%A4%EC%A7%B0+%EB%B0%B8%EB%B3%B4%ED%88%EB%B8%EC%97%B0+%EA%B4%B0%EB%B2%95%EB%B2%95%EA%B5%A0&chrClsCd=010202&mode=20&ancYnChk=0#
217	韓国	産業技術の流出防止および保護に関する法律（一部改正）	法律	2007	2023	政府 (産業通商資源部)	その他	○	産業技術の不正な流出を防止し、産業技術を保護することにより、国内産業の競争力を強化し、国家の安全保障と国民経済の発展に貢献することを目的としている。 国家機関、地方自治団体、「公共機関の運営に関する法律」第2条による公共機関その他大統領令で定める機関は、国家核心技術に関する情報を公開してはならない。ただし、国家の安全保障及び国民経済の発展に悪影響を与える恐れがない場合には公開することができる（第9条の2）	△	△	有り	国家研究開発事業の事業管理 対象機関の長は、産業技術に関連する国家研究開発事業を遂行する過程で開発成果物が外部に流出しないように必要な対策を樹立・施行しなければならない（第12条） 秘密保持義務 第20条第2項の規定により産業保安技術開発事業者に雇用され、産業保安技術研究開発業務を遂行する者は、その職務上知った秘密を漏洩又は盗用してはならない（第34条）	(韓国国家法令情報センター) https://www.law.go.kr/LSW/IsLinkProc.do?lsNm=%EC%B2%B0%EC%B7%85%EA%B8%B0%EC%B8%A0%EC%9D%98+%EC%9C%A0%EC%B6%9C%EB%B0%A9%EC%A7%B0+%EB%B0%B8%EA%B5%EA%B0%B6%95%ED%A9%B4%EB%B8%EC%97%B0+%EA%B4%B0%EB%B2%95%9C+%EB%B2%95%95%EA%B5%A0&chrClsCd=010202&mode=20&ancYnChk=0#
218	韓国	国家先端戦略産業競争力強化および保護に関する特別措置法（一部改正）	法律	2022	-	政府 (産業通商資源部)	その他	○	経済安全保障の確保および先端産業競争力の強化のため、「先端戦略技術」を指定し、関連産業を育成・保護するもの。「先端戦略技術」は産業通商資源部長官の指定するものであり、先端戦略技術を外国企業などに輸出しようとする場合、または先端技術の侵害者が海外MNC・合弁投資を進めようとする場合、事前承認が必要となる。また、同技術を有する専門人材を特定し、離職・情報漏洩を防止する措置を講ずることになっている 戦略技術関連品目の供給安定化調整に関する資料における情報に対しての保全措置が規定されている（第10条）。また、戦略技術を含む情報を提供された者が情報を提供された目的以外の用途でその情報を使用・開示することを禁止している（第15条）	△	×	無し	-	(JETRO) https://www.jetro.go.jp/biznews/2022/01/352ed41b75e4c8bb.html (韓国政府立法省) https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B5%AD%EA%B0%80%EC%B2%A8%EB%B8%A8%EC%A0%B4%EB%B6%B3%EC%B2%B0%EC%97%B5%EA%B2%B0%EC%9F%B1%EB%A0%A5%EA%B0%B6%95%ED%A9%B4%EB%B8%EC%97%B0+%EA%B4%B0%EB%B2%95%9C+%EB%B2%95%95%EA%B5%A0&chrClsCd=010202&mode=20&ancYnChk=0#
219	韓国	個人情報保護法（改正）	法律	2011	2020	政府	その他	○	個人情報の保護に関する法令。個人情報を「生存する個人に関する情報であって、次のいずれかに該当する情報」として、「匿名、住民登録番号、電話番号を通じて、個人を知ることができる情報」、「その情報だけでは特定の個人を知ることができなくても、他の情報と照準に結合して知ることができる情報」と定義している。	○	△	有り	個人情報処理者は、科学的研究のために情報主体の同意なしに仮名情報を処理可能（第28条の2） 科学的研究のための真なる個人情報処理者間の仮名情報の統合は、保護委員会又は中央行政機関が指定する専門機関が行う（第28条の3）	(JETRO) https://www.jetro.go.jp/biznews/2020/01/004f6ae91037174.html (韓国国家法令情報センター) https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%88%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%98%EB%B2%95
220	韓国	健康医療データ活用ガイドライン	ガイドライン	2022	-	政府 (保健福祉部)	バイオ	○	個人情報保護法に基づく仮名処理・仮名情報の活用について、健康医療データの特性性を踏まえた処理過程全体の手続き及びガバナンス上の安全配慮、倫理的事項を示すもの	○	×	無し	-	(健康福祉部) http://www.mohw.go.kr/upload/viewer/skin/doc.html?fn=1672200758259_20221228131238.pdf&rs=/upload/viewer/result/202307/
221	韓国	医療機関個人情報保護ガイドライン	ガイドライン	2010	2012	政府 (保健福祉部)	バイオ	○	500床以上の医療機関を対象として、個人情報保護およびセキュリティ管理組織、人的資源管理、情報システム運営およびセキュリティ管理、ネットワークおよびログ管理、バックアップおよびストレージメディア管理、ユーザー認証およびアクセス管理、侵害事故の予防および対応など、管理的、技術的、物理的情報保護に関する内容を示している	○	△	有り	医療研究に際して個人情報扱う場合の個人情報保護委員会と院内研究倫理審査委員会との権限関係等について示している	(健康福祉部) http://www.mohw.go.kr/upload/viewer/skin/doc.html?fn=1268699925313_20100316093845.hwp&rs=/upload/viewer/result/202307/
222	韓国	ニューメディアサービス個人情報保護ガイドライン	ガイドライン	2012	-	政府 (行政安全部)	その他	○	スマートフォン、クラウドコンピューティングなどニューメディアを基盤としたサービスをを中心にサービスプロバイダと利用者が設置すべき事項を示している ニューメディアサービス(New Media service)は、クラウドコンピューティングサービス、ソーシャルネットワークサービス、ソーシャルコマースサービス、スマートフォン活用サービスを対象としている サービス提供者の守るべき基本的な個人情報保護措置と、利用者側の個人情報提供時の注意事項などが示されている	○	×	無し	-	(行政安全部) https://www.mois.go.kr/ft/bbs/type910/commonSelectBoardArticle.do?bbsId=BBSMSTR_00000000000&nttid=28727
223	韓国	金融分野個人情報保護ガイドライン（改正）	ガイドライン	2013	2017	政府 (金融監督院)	その他	○	クレジットカード会社による個人情報流出事故の発生を契機とした個人情報保護に対する社会的な要請の増加及び金融系企業に対する個人情報保護のための明確な基準の必要性から、金融機関当事者が実際に参考にできる個人情報(信用)情報処理基準を提示したものである	○	△	有り	統計作成及び学術研究などの目的のために必要な場合で、特定の個人を識別できない形で個人情報を提供する場合は、本来の目的であっても、情報主体の別途同意がなく、個人情報を提供可能	(金融監督院) https://www.fsc.go.kr/pn010106/726127srchCgry=6&curPage=41&srchKey=&rchText=&rchBeginDt=&rchEndDt=
224	韓国	人工知能(AI) 個人情報保護セルフチェックリスト	ガイドライン	2021	-	政府 (個人情報保護委員会)	その他	○	AI技術の適用による新しいサービス導入を背景として、AI技術サービスの開発・運営における個人情報処理の安全性と信頼性の確保を目的としたもの 個人情報保護法上の個人情報処理者となるAI技術開発・運営者を対象として、安全な個人情報の処理、侵害の防止に向けた遵守事項の事前・随時公表事項を示している	○	△	有り	AIによる個人情報の収集にあたって、その目的が科学的研究、統計作成などに当たる場合の同意取得適用除外などに触れられている	(個人情報保護委員会) https://www.picp.go.kr/np/cop/bbs/selectBoardArticle.do?mCode=D010030000
225	韓国	国家知識情報連携及び活用促進に関する法律	法律	2021	-	政府 (科学技術情報通信部)	その他	○	国民が自由かつ便利に国家知識情報を利用できるように国家知識情報の連携及び活用を促進するために必要な事項を定めることにより、国民の知識財産創出及び活用力量を高め、国家競争力の強化に資することを目的としたもの。 国家機関、地方自治団体及び「知識情報化基本法」第2条第16号による公共機関（以下「国家機関等」という。）が、生産・保蔵・管理している科学技術、教育・学術、文化芸術、社会経済、行政等に関する情報のうち、知識の活用情報として国家知識情報委員会の指定を受けた情報を「国家知識情報」として指定し、国家知識情報の効率的な連携及び活用のために統合プラットフォームを構築・運営することが定められている	○	×	無し	-	(韓国国家法令情報センター) https://www.law.go.kr/IsInfP.do?lsSeq=232613&lsId=014089&chrClsCd=010202&urlMoDe=IsInfP&viewCls=IsInfP&etYd=20211209&vSct=%EC%A0%95%EB%B3%B4&ancYnChk=0#0000
226	韓国	秘密記録管理運用基準	ガイドライン	2010	2021	政府 (国家記録院)	その他	○	「公共記録物管理に関する法律」による各級公共機関で生産される秘密記録物原本の管理手続きを規定する基準 秘密記録物管理のための公共機関の責任と役割、秘密業務に対する記録管理基準表の管理、秘密記録物の生産と保護期間、保存期間付、秘密記録物の生産状況通知のための手続き及び方法、秘密記録物を移管するために行わなければならない業務内審等について定めている	○	×	無し	-	(国家記録院) https://www.archives.go.kr/next/common/downloadFile.do?up_filepath=2F6e5781742e646174612F64616e616765722F64F1B9D0B1E2B7CFB9B020B0FC8AC2&706466
227	韓国	秘密記録管理業務指針	ガイドライン	-	2020	政府 (国家記録院)	その他	○	公共機関で生産・保有する秘密記録物を安全かつ効率的に管理するために必要な詳細な業務処理基準と手続きを定めることを目的としたもの 秘密とはセキュリティ業務規定に定められた国家安全保障に害をなす国家秘密のことを指しており、秘密記録物の管理主体やその生産、保管、閲覧等に係る管理基準を定めている	○	×	無し	-	(国家記録院) https://www.archives.go.kr/next/common/downloadFile.do?up_filepath=2F6e5781742e646174612F64616e616765722F64F1B9D0B1E2B7CFB9B020B0FC8AC2&20B0C1F6C4A120B0B3C1A40C672&706466
228	韓国	外国人投資促進法	法律	1998	2023	政府	その他	○	韓国における外国人投資を支援し、外国人投資に便宜を提供して外国人投資の誘致を促進することによって、韓国経済の発展に資することを目的として制定された法律 その目的は、法律に特別に定めのない限り外国人投資家に韓国人と同様の待遇を適用することや租税の減免、地方自治団体の外国人投資誘致活動に対する支援など、外国人投資に対する保護措置を規定しているが、国家の安全および公秩序の維持に支障をもたらす場合など特定の条件における外国人投資に対する制限を規定している	○	△	無し	-	(韓国国家法令情報センター) https://www.law.go.kr/법령/외국인투자촉진법
229	韓国	国家研究開発革新法	法律	2021	2023	政府	その他	○	政府機関の出資する研究開発事業（国家研究開発事業）の根拠法であり、同法及び施行令、施行細則において国家研究開発事業の公費及び管理、必要な機関や環境の整備等、事業運営全般に関する事項を規定している	○	○	有り	同法施行規則の下位規則にある国家研究開発セキュリティ対策では、研究開発事業の中でも機密性の高い「セキュリティ課題」の分類方法と、セキュリティ課題における情報管理について規定している (韓国国家法令情報センター) https://www.law.go.kr/법령/국가연구개발혁신법	