

データセンター・クラウド安全認証制度の全貌 と知財業務への構造的波及：経済安全保障法 制の新展開に関する調査報告

Gemini 4 Argon

制度創設の政策背景と三層構造の規律メカニズム

2026年10月19日、日本政府がデータセンター（DC）およびクラウドサービスの安全性を審査・認証する新たな制度を創設する方針を固めたことが日本経済新聞の一面で報じられた¹。総務省と経済産業省の共管により2027年度以降の導入を目指すこの制度は、国内に立地するデータセンター事業者および国内にサーバーを保有してクラウドサービスを提供する事業者を直接の対象とし、金融や医療をはじめとする機微な重要情報を扱う企業に対して国が認証したサービスの利用を促す枠組みである¹。報道において「中国やロシアなどの影響下にある企業を事実上排除する仕組み」と位置づけられた本制度は、単なるITインフラのセキュリティ基準の引き上げにとどまらず、日本の経済安全保障法制が「ハードウェア・特定重要物資のサプライチェーン防護」から「民間保有データおよび情報処理基盤の主権的統制」へと決定的に舵を切ったことを意味している¹。

この政策転換は突如として浮上したのではなく、2025年秋以降に内閣官房の「経済安全保障法制に関する有識者会議」を中心として緻密に積み上げられてきた法改正プロセスの帰結である¹。高市早苗首相から小野田紀美経済安全保障担当大臣に対して経済安全保障推進法の改正に向けた検討指示が下されたことを皮切りに、2025年12月4日には同有識者会議において「データセキュリティ制度の検討について」と題する討議資料が提示され、国内データ防護の方向性が具体化し始めた¹。続いて2026年1月16日の「提言 骨子（データセキュリティ）」および同年1月30日の「経済安全保障の更なる推進に向けた提言」において、基幹インフラ役務の安定的提供に必要なデータおよび個人に関する機微なデータ（安全保障上重要な民間保有データ）の防護と、我が国の外部から行われる行為からデータセンターおよびクラウド上の大量のデータを防護するための措置の検討が正式に盛り込まれた¹。

2026年3月19日に閣議決定され同年6月10日に成立した改正経済安全保障推進法においては、包括的なデータセンター規制までは盛り込まれなかったものの、附則に施行後3年をめどとした見直し条項が設けられ、国会答弁でも「今回改正とは別に検討継続」と明言されるなど、政府にとって残された最重要の立法課題となっていた¹。その後、2026年7月21日に閣議決定された「経済財政運営と改革の基本方針2026（骨太の方針）」において「安全保障上重要な個人機微データの防護に関する法案の早期提出を目指すとともに、データセンター・クラウドの安全性等を確保するために必要な措置を講ずる」と明記された⁴。そして報道直前の2026年10月16日に開催された第18回経済安全保障法制に関する有識者会議において、資料3「データセキュリティの検討状況」および西村あさひ法律事務所の桜田雄紀弁護士による提出資料「主要国の個人機微データ保護法制と経済安全保障をめぐり国際的潮流」が公表され、制度の骨格が事実上確定するに至ったのである⁸。政府は2027年1月召集の通常国会に関連法改正案を提出し、法整備を先行させたうえで、早くとも2027年度後半以降にDC・クラウドの安全認証制度を実運用に移すスケジュールを描いている¹。

時期	政策・立法上の主要マイルストーン	決定・公表された中核的事項
2025年11月～12月	経済安全保障法制に関する有識者会議での議論開始・資料「データセキュリティ制度の検討について」(12月4日)	民間保有データの安全保障上の保護責任と国内DC・クラウドの実態把握の必要性を提示 ⁴
2026年1月16日・30日	「提言骨子(データセキュリティ)」および「経済安全保障の更なる推進に向けた提言」公表	安全保障上重要な民間保有データ(個人機微データ等)とDC・クラウド上の大量データ防護措置の検討を明記 ¹
2026年3月19日・6月10日	経済安全保障推進法改正案の閣議決定(3月)および成立(6月)	附則に見直し条項を設定し、データセキュリティおよびDC規律は別枠で継続検討することを確立 ¹
2026年7月21日	「経済財政運営と改革の基本方針2026」閣議決定	安全保障上重要な個人機微データ防護法案の早期提出とDC・クラウドの安全性確保措置を閣議決定 ⁴
2026年10月16日	第18回 経済安全保障法制に関する有識者会議(資料3・資料4公表)	ゲノム・医療・金融情報の大量取扱事業者への届出審査制、情報システム契約・データ提供への規律案を提示 ⁴
2026年10月19日	日本経済新聞による安全認証制度創設方針の報道	総務省・経産省によるDC・クラウド4項目認証と事前届出・中止命令を組み合わせた中国・ロシア系排除の枠組み報道 ¹
2027年1月(予定)	通常国会への関連法改正案提出	重要な個人情報を扱う企業の事前届出制度および国による中止命令・勧告権限の法定化 ¹
2027年度後半以降(想定)	データセンター・クラウド安全	国内立地DCおよび国内サー

	認証制度の導入・運用開始	バー保有クラウド事業者に対する審査・認証の開始 ¹
--	--------------	--------------------------------------

本制度の法制的・構造的な最大の特徴は、データを保有・利用する側への行為規制と、データを預かるインフラ側への安全認証を「三層構造」として立体的に組み合わせた点にある¹。

三層構造の規律設計により特定国を名指しせず懸念国系インフラを事実上排除する



第1層(データを持つ側への規律)では、安全保障上のリスクが高い個人に関する機微なデータ(まずは防護の優先度が特に高いゲノムデータ、医療情報、金融情報)を大量に取り扱う事業者に対し、外部への情報流出を生じさせ得る行為である「データの処理・保存を行う情報システム等の契約(クラウドやオンプレミスの導入・維持管理委託)」および「データや生体試料の提供(売買、解析委託等)」にあたって国への事前届出を義務付け、国が個別にリスクを審査・監督する¹。

第2層(データを預かる側への規律)では、総務省と経済産業省が国内立地のDC事業者および国内にサーバーを置くクラウド事業者を審査し、安全性を認証する¹。ここで審査される項目は、既存の国際標準(ISO/IEC 27001等の情報セキュリティ認証)が担保する「リスク管理体制(情報流出・滅失を防ぐ管理の仕組み)」にとどまらない¹。国独自の経済安全保障上の審査項目として、「事業者情報(どのような企業で、誰が株主・経営者・実質的支配者なのか)」、「設備の供給者情報(サーバーやネットワーク機器、ルーター等をどこから調達しているかというハードウェア供給網)」、そして「懸念国の影響有無(外国政府、とりわけ中国やロシア等の懸念国の影響下にないか)」の計4項目が設定される¹。

そして第3層(是正手段)として、第1層の事前届出審査や監督を通じてデータの保管・処理に安全保障上のリスクがあると判断された場合、国が事業者に対して契約やデータ保管の中止命令や勧告を発出できる法的権限を担保する¹。

ここで極めて巧妙な制度設計となっているのが、第1層と第2層を法律上の「義務」ではなく「推奨(認証事業者との契約の推奨)」で繋いでいる点である¹。日本政府は国際社会において「信頼性のある自由なデータ流通(DFFT: Data Free Flow with Trust)」を主導してきた経緯があり、国内のデータ保管先を国が強制的に選別したり特定国を名指しして排除したりする規定を設ければ、データの囲い込み(データ・ローカライゼーション)やWTO協定等の国際通商ルール違反との批判を招きかねない¹。そこで、表面上は「特定国を名指ししない」「民間企業による自由なデータ流通や経済活動を必要以上に制限しない」という原則を維持しつつ、重要データを扱う企業に事前届出と中止命令の網(第1層・第3層)をかけたうえで「国が安全認証したDC・クラウド(第2層)を使えば届出審査上のリスクが回避される」というインセンティブ構造を作出しているのである¹。この「特定国を名指しせず、厳格なサプライチェーン・支配関係基準を満たした事業者のみを認証し、結果として中国・ロシア系が残らない」という手法は、経済産業省が先行導入したIoT製品のセキュリティラベリング制度「JC-STAR」や、エネルギー分野におけるパワーコンディショナー(PCS)・蓄電池からの中国製品の実質的排除と完全に同一の政策テンプレートを踏襲したものである¹。

国家安全保障上の脅威認識と国際法制の比較分析

なぜ今、政府は「個人情報保護法」という既存の法体系が存在するにもかかわらず、経済安全保障法制の枠組みで個人の機微データとDC・クラウドを直接規律しようとしているのか。その本質的な理由は、保護法益の決定的な違いにある¹。個人情報保護法があくまで「個人の権利利益の保護」を目的としているのに対し、新制度は「国家及び国民の安全を害する外部からの影響力行使(インフルエンス・オペレーション)や諜報活動の阻止」を目的としている¹。

内閣官房の有識者会議資料(2026年10月16日第18回会議・資料3)が明確に指摘するとおり、諸外国の諜報機関において、大量の個人データを広範にサーチエンジンやAIにかけて特定の標的(政府高官、自衛隊・防衛産業の関係者、先端技術を持つ企業や研究機関のエンジニア等)の弱みを抽出・加工する工作は既に常態化している¹。具体的には、標的やその家族の重篤な病歴・精神疾患(医療情報)、住宅ローンやクレジットカード債務による経済的困窮(金融情報)、さらには日常の行動パターン(位置情報)や生体認証情報・ゲノムデータが外国情報機関の手に渡れば、それらを材

料とした脅迫（ブラックメール）や金銭的懐柔によって、国家機密や企業の最重要営業秘密・未公開技術情報を奪取することが可能となる¹。

実際に有識者会議資料では、機微な個人データがスパイ工作に悪用された具体的事案と我が国における技術流出事案が明確に関連付けられている⁴。例えば海外事例としては、住宅ローンやクレジットカード債務で困窮していた元米国CIA職員が中国情報機関員の接触を受け、報酬と引き換えにCIA職員情報や工作計画の機密を提供した事案（2018年、米スパイ活動法違反）や、重病で特別なケアを要する子を抱え住宅ローン等でも困窮していたイタリア海軍大佐がロシア駐在武官の接触を受け、NATOおよびイタリアの機密文書を提供した事案（2021年、伊刑法等違反）が挙げられている⁴。そして日本国内においても、大手通信会社の元職員が在日ロシア連邦通商代表部員と共謀して第5世代移動通信システム（5G）に関する営業秘密を提供した事案（2020年、不正競争防止法違反で有罪）に続き、直近の2026年にも工作機械関連会社の元従業員が在日ロシア連邦通商代表部員と共謀し、報酬と引き換えに同社の新商品のアイデア等の営業秘密を提供して検挙される事案（2026年、不正競争防止法違反）が発生している⁴。

さらに注目すべきは、2024年に成立した「重要経済安保情報の保護及び活用に関する法律（セキュリティ・クリアランス法）」第12条第2項との構造的リンクである⁴。同法に基づく適性評価調査の項目には、第5号「精神疾患に関する事項」および第7号「信用状態その他経済的な状況に関する事項」が明記されている⁴。すなわち、国家がセキュリティ・クリアランス制度によって「機密を漏らすおそれがない人物か」を審査する際に重視する「医療・精神状態」や「金融・信用状態」のデータそのものが、民間のクラウドやデータセンターから外国情報機関に筒抜けになっていれば、クリアランス制度の前提自体が根底から崩壊するのである¹。

同時に、インフラ面で中国やロシアの影響下にある事業者が警戒される背景には、単なる外部からのサイバー攻撃（ハッキング）リスクだけでなく、「外国法制による強制的な情報アクセス」と「正規の業務委託・保守運用ルートを通じた情報採取」という構造的リスクが存在する¹。中国では2017年施行の「国家情報法」により、中国国内のあらゆる組織および個人に対して国家の情報活動への協力義務が課されており、たとえ民間企業間で厳格な秘密保持契約（NDA）を締結していたとしても、あるいは顧客が開示を拒否したとしても、事業者が中国政府からの法的要求に対抗することはできない³。ロシアにおいても連邦保安庁（FSB）への協力義務規定が存在し、戦時下や有事にはその圧力とサービス停止リスクが極度に高まる³。

加えて、物理的なサーバーが日本国内のデータセンターに設置されていたとしても、ハードウェアの保守や障害対応、管理ソフトウェアの運用、暗号鍵の管理、あるいはシステム開発の再委託先が国外（懸念国）に存在し、そこから管理者権限（特権ID）によるリモートアクセスが可能な状態になっていれば、データは「正規のルート」を通じて海外から完全に閲覧・収奪可能な状態に置かれる¹。米国CISA等が2025年9月に更新した共同注意喚起「AA25-239A」では、中国政府支援の攻撃者がルーターを改変して長期的なアクセスを維持し、信頼済み接続を足掛かりに通信・政府・重要ネットワークへ侵入する手口が報告されており、また米国国立標準技術研究所（NIST）が2026年7月に公表した『SP 1326』では、ICT調達先のデューデリジェンスに「外国の所有・支配・影響（FOCI: Foreign Ownership, Control, or Influence）」の評価が正式に組み込まれている³。英国国家サイバーセキュリティセンター（NCSC）の「Cloud Security Principles」が「データの物理的保存場所が国内であること」と「外国の法制度や管理者権限から隔離されていること」は同義ではないと警告している点も、今回の日本の審査項目（事業者情報、設備の供給者、懸念国の影響有無）にそのまま反映されている

¹。

こうしたデータ安全保障の規律強化は世界的な潮流であるが、各国の法制アプローチには明確な差異が存在する¹。

主要国のデータ安保規律比較と大量機微データ規制の数量閾値ベンチマーク

● 主要4種のデータセンター・機微データ規律モデル比較

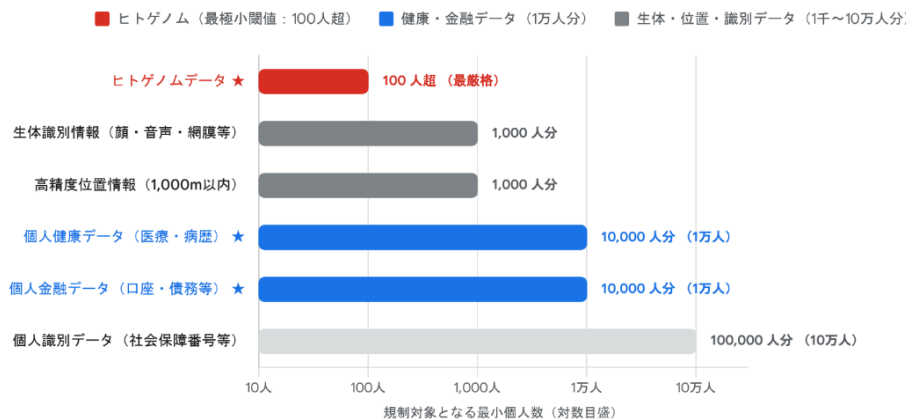
出所：内閣官房有識者会議資料等より作成

2027年以降導入へ 日本 (新法整備案) 届出 + DC認証 + 推奨 (3層型) 対象：重要機微データ保有者 & 国内DC・クラウド事業者 特色：特定国を名指しせず「懸念国の影響 (FOCI)」 「設備供給網」を審査。是正命令・推奨により事実上中国系を排除。 DFFT獨立型・行政指導連携	米国 (DOJ 2025最終規則) 直接的取引禁止・除外命令 対象：懸念国（中露等）への大量機微個人データの移転・アクセス 特色：ゲノム100人～識別10万人の厳格な数量閾値を設定。民事・刑事罰を伴う包括的移転禁止型。 PADFAA / 大統領令14117
欧州連合 (EU) NIS2指令 + データ法 (Data Act) 対象：重要インフラ事業者・サプライチェーン・クラウド 特色：サプライチェーンリスクと報告を義務化。米CLOUD Actによる域外差押えを警戒しデータ主権を強化。 包括セキュリティ・主権防衛型	韓国 (現行制度) データセンター安全性認証制度 対象：国内主要データセンター事業者（クラウド別途検討） 特色：施設・サプライチェーンの安全基準を国が審査認証。日本のDC認証制度の精造的モデル。 DC先行認証モデル

● 米国DOJ規則（2025年発効）における機微データ規制数量閾値（米国人分）

★ = 日本の初期優先対象領域

日本の「大量機微データ取扱事業者」基準の主要参照モデル（対数目盛：100人～10万人）



① 第18回経済安保法制有識者会議（2026年10月）における制度設計の重要視点

① 初期優先3領域の指定

情報機微度と安全保障上の実被害リスクを重視し、まずは「ゲノム」「医療・健康」「金融」から先行指定。特にゲノムは100人規模で集団特性が特定されうるため厳格化。

② 機微度に応じた数量閾値

一律規制によるスタートアップ負担や研究停滞を回避するため、米国型を参考に「一定規模以上を取り扱う事業者」へ限定。機微度に応じた段階的閾値が検討されている。

③ 委託・越境保管の事前棚卸し

外部ハッキングだけでなく、海外衛生検査所へのゲノム解析委託や、海外拠点からのアクセス管理が規律対象。知財・法務部門によるサプライチェーン総点検が急務。

上段は日・米・欧・韓のデータセンター・機微データ規律の比較。日本は韓国のDC認証モデルに米国型の「懸念国の影響 (FOCI)」審査を統合し、届出制と推奨で運用する独自形態をとる。下段は日本の「大量取扱事業者」基準の参照点となる米国司法省 (DOJ) 規則 (2025年発効) の規制対象閾値。ヒトゲノムデータはわずか100人超で規制対象となり、生体認証・位置情報 (1,000人)、健康・金融データ (1万人) と機微度に応じた段階設計がなされている。

Data sources: 内閣官房「第18回 経済安全保障法制に関する有識者会議 資料3 (データセキュリティ制度の検討)」, 西村あさひ法律事務所 桜田弁護士提出資料 (主要国の個人機微データ保護法制), 日本経済新聞報道・解説 (データセンター・クラウド安全認証)

米国では、司法省(DOJ)の最終規則(DSP等)が2025年1月に公表され、同年4月8日に一部発効、10月に全面発効している¹。米国のアプローチは、データの種類ごとに明確な人数閾値(ヒトゲノムデータは100人超、生体識別情報および1,000メートル以内の位置情報は1,000人分、個人健康データおよび個人金融データは1万人分、社会保障番号等の個人識別データは10万人分)を設定し、懸念国(中国・ロシア等)の主体がこれらにアクセスし得る取引を直接禁止・制限する強力なハードローである¹。これに対し欧州連合(EU)は、NIS2指令やデータ法(Data Act)によって非個人データを含む保護網を敷く一方、警戒の対象を中国のみならず「米国のCLOUD Act(クラウド法)」にも向けている¹。CLOUD Actの下では、米国系のクラウド事業者が米国外(日本や欧州)のサーバーに保管しているデータであっても、米国当局が開示命令を発出できるため、欧州では米国系巨大クラウド(ハイパースケーラー)への過度な依存自体がデータ主権(データ・ソブリンティ)上の重大なリスクとして認識されている¹。また、豪州は重要インフラ安全保障法(SOCI法)による包括的義務を課しており、韓国はデータセンター事業者を対象にサプライチェーン対策を含む認証制度を運用し、さらにクラウドやDC関連設備への新規則案を検討している¹。

日本の新制度は、韓国の「DC事業者を対象とした認証制度」という器に、米国流の「懸念国の影響(FOCI)の排除」と「機微個人データの大量取扱事業者に対する届出審査」を融合させたハイブリッド型の設計と評価できる¹。しかし、ここには看過できない構造的ジレンマが内包されている¹。日本の安全認証制度では、中国系やロシア系の事業者が事実上排除される一方、「同盟国の企業であれば安全保障上問題ない」という政治的・実務的判断から、AWS(Amazon Web Services)、Microsoft Azure、Google Cloudという米国系クラウド3強はほぼ確実に安全認証を取得するとみられている¹。その結果、金融・医療・先端研究機関の重要データが米国系3強へと一層集中し、日本の「デジタル赤字」と米国製インフラへの構造的依存が固定化するのみならず、前述した米国CLOUD Actに基づく域外適用リスク(米国の国益や捜査・通商政策に基づくデータ開示要求リスク)が温存されることになる¹。この点は、後述する企業の知的財産・営業秘密管理において極めて重大な実務上の死角となる¹。

知的財産業務への構造的波及と法務・実務上の論点

今回のデータセンター・クラウド安全認証制度および個人機微データの事前届出・審査制度は、一見すると金融機関や医療機関の個人情報管理部門・IT部門の問題のように映るかもしれない¹。しかし、法制的構造と有識者会議の議論を精緻に解剖すると、本制度は企業の知的財産部門、研究開発(R&D)部門、および特許事務所の業務に対して、4つの決定的な経路を通じて直接かつ甚大な波及効果をもたらすことが明らかになる¹。

新データ安保・クラウド認証制度が知財業務の4大領域に及ぼす構造的リスクと実務対応

📌 新制度の3層ガバナンス構造（2027年度以降 導入方針）

総務省・経済産業省／内閣官房有識者会議

第1層：データ保持企業
ゲノム・医療・金融等の機微データを扱う企業への事前届出制

第2層：DC・クラウド事業者
安全性審査・認証（設備供給網・懸念国の影響有無・FOCI）

第3層：国による是正権限
保管リスク時の中止勧告・命令権限／特定国事実上排除

1 【研究開発・知財創出】ゲノム・バイオ・医療・金融AIデータ

経安法改正・データセキュリティ制度

● 規律トリガー
個人機微データ（ゲノム100人超、生体認証1,000人分、医療・金融1万人分等）の外部処理・保存契約および生体試料解析委託に対する国への事前届出義務。

● 知財法務・実務リスク
海外受託先（CRO）や未認証クラウド利用による中止命令リスク。日中の第一国出願義務の二重抵触（経済安保推進法第78条 vs 中国専利法第19条保管審査）による罰則および出願却下。

● 知財部門の実務対応
生体試料・R&Dデータ保管先の国認証クラウド基盤への集約。国際共同研究における「発明完成地」の厳密判定と、特許庁への外国出願事前確認申請（法第79条）の標準化。

2 【営業秘密・ノウハウ保護】クラウド秘密管理性と対中ガバナンス

不誠法第2条6項／2025年3月改訂 管理指針

● 規律トリガー
懸念国法制（中国国家情報法等）による情報提供協力義務による公権力的アクセスリスクの公的認定。外国の所有・支配・影響（FOCI）デューデリジェンスの要求。

● 知財法務・実務リスク
秘密管理性の否認リスク。外国政府による不可抗力的アクセスが想定される環境での保管は「秘密管理性」の欠如と判断される恐れ。対中NDAの現地効力限界と限定提供データ遁洩。

● 知財部門の実務対応
未認証・懸念国系クラウドからの機微データ即時退避。共同研究・開発委託契約へ「国認証クラウド利用条件」を必須取引条件化。退職時の対象特定型NDA誓約書の再設計。

3 【特許非公開・クリアランス】特定区域要件と技術者情報防護

推進法第66条・重要経済安保情報法第12条

● 規律トリガー
保全対象発明情報の適正管理措置（特定区域要件・クラウド同等管理基準）。重要経済安保情報の適性評価（精神疾患、信用状態、経済状況調査）の本格適用。

● 知財法務・実務リスク
クラウドを特定区域とする際の契約・管理不備による適正管理義務違反（指定取消・刑事罰）。先端研究者・知財担当者の個人機微情報流出による抱き込み・営業秘密窃取リスク。

● 知財部門の実務対応
認証済み国内クラウドの「特定区域」事前指定。管理変更に伴う追加費用の「損失補償請求（類型4）」算定準備。適性評価対象技術者の機微プロフィールの社内隔離管理。

4 【知財SaaS・パテントテック】サプライチェーンと暗号鍵統制

ISMAP・米国CLOUD Act・BYOK

● 規律トリガー
国内立地DCおよび国内サーバーを持つクラウド（IaaS/PaaS）を対象とする国の安全審査・認証制度。設備の供給者情報・保守運用体制の審査。

● 知財法務・実務リスク
基盤認証の「非継承」問題。AWS/Azure等が認証されても知財SaaS（検索・AI明細書作成・期限管理）自体の安全性は担保されない。海外オフショア保守や米国CLOUD Act開示リスク。

● 知財部門の実務対応
知財SaaSベンダーの再委託先・海外運用アクセス監査。自社管理鍵（BYOK/HSM：FIPS 140-2 Level 3準拠）による未公開特許・技術原稿の透過的暗号化統制の必須化。

新制度が知財ライフサイクル全体に及ぼす波及経路の全体像。①創薬・医療・金融AIにおけるデータ・生体試料の解析委託規制と第一国出願義務の交錯、②2025年3月改訂「営業秘密管理指針」におけるクラウド秘密管理性の再定義と対中NDA限界、③特許出願非公開制度の「特定区域」要件と損失補償算定、④知財SaaSにおける基盤認証の非継承問題と米国CLOUD Act対策（BYOK）の4層で実務見直しが迫られる。

Data sources: 経済安保・クラウド認証制度解説、セキュリティ対策Lab、内閣官房（第18回データセキュリティ検討資料）、内閣官房（特許出願非公開制度資料）、特許出願非公開制度実務解説、浅村特許事務所、直法法律事務所、TMI総合法律事務所、パテント・リザルト、日立ソリューションズ

1. 創薬・バイオ・医療AI・フィンテックにおける研究開発データ規制と発明完成地の交錯

第1の、そして最も直接的な影響は、バイオテクノロジー、創薬、医療機器・ヘルスケアAI、およびフィンテック領域における「発明創出プロセス(R&D)」そのものへの法的規律である⁴。2026年10月16日の第18回有識者会議資料3が明示したとおり、新法制が第1弾の規律対象とする「ゲノムデータ・医療情報・金融情報」について、規制対象となる行為は単なるサーバー保管にとどまらず、「データの処理・保存を行う情報システム等の契約」および「データや生体試料の提供(売買、委託等)」、とりわけ「ゲノムデータの解析依頼」や「バイオバンク等によるデータ提供」を直撃する設計となっている¹。これまで日本の製薬企業、バイオベンチャー、大学・研究機関、あるいは医療機関においては、コストや解析スピードの観点から、国内で採取した生体試料やゲノムデータのシーケンシング・バイオインフォマティクス解析を中国系等の海外受託解析機関(CRO)に委託したり、海外拠点からアクセス可能なクラウド環境上でAI創薬モデルの学習・解析を行ったりする実務が広く存在していた¹。しかし新制度の下では、これら大量のゲノム・医療データを扱う事業者が情報システム契約や外部への解析委託を行う際には国への「事前届出」が必要となり、委託先やクラウド基盤に懸念国の影響(FOCI)や漏えいリスクがあると判断されれば、国から契約やデータ保管の中止命令・勧告が下されることになる¹。

知財実務の観点からこれが意味するのは、AI創薬における学習用データセットの構築、疾患バイオマーカーの探索、新規ターゲット分子の同定、あるいは医療診断アルゴリズムや金融与信AIモデルの開発において、「どのクラウド上でデータを処理し、どの事業者に解析を委託したか」が、研究開発プロジェクトの法的継続性を左右する決定要因になるということである⁴。未認証のクラウドや懸念国影響下の解析事業者に依存したR&Dパイプラインは、開発途上で国の中止命令によりデータ利用が凍結され、特許出願に至る前の段階で研究自体が頓挫するリスクを抱えることになる¹。

さらに深刻なのが、各国の「第一国出願義務(秘密審査制度)」との管轄権衝突リスクである¹⁹。日本の経済安全保障推進法に基づく「特許出願非公開制度(2024年5月1日施行)」第78条では、日本国内で完成した発明であって特定技術分野(25分野)に属するものについて、原則としてまず日本国特許庁に出願しなければならない「第一国出願義務(外国出願の禁止)」が課されており、違反には刑事罰および国内出願却下の制裁が伴う¹⁹。同制度の基本指針(第4章第5節)において、「日本国内でした発明」か否かは、複数国にまたがって研究開発が行われた場合、「発明の完成地がどこであるか」によって判断されると規定されている¹⁹。一方、中国専利法第19条は、中国国内で完成させた発明・実用新案を外国へ出願する場合、事前に国務院専利行政部門(CNIPA)の「秘密審査(秘密審査)」を受けなければならないと規定している²⁰。また、中国は「データ三法(サイバーセキュリティ法、データ安全法、個人情報保護法)」によって中国国内で生成・処理されたデータの越境移転を厳格に制限している⁹。

もし日本企業が、日本国内の被験者から得たゲノムデータや医療データ、あるいは先端技術データの解析を中国系のクラウドや中国の解析拠点に委託し、その解析結果(AIモデルのパラメータや候補化合物の特定)をもって発明が完成したと評価された場合、深刻な法域衝突が生じる⁴。中国当局からは「中国国内で完成した発明(専利法第19条)および中国の重要データ」として中国での事前秘密審査とデータ持ち出し制限を主張される一方、日本政府からは新データセキュリティ法制に基づく「事前届出違反・中止命令」の対象となるばかりか、特定技術分野に該当すれば日本の特許出願非公開制度(推進法第78条)との間で「発明の完成地」をめぐる二重規制(コンフリクト・オブ・ローズ)に陥るのである⁴。したがって知財部門は、R&D部門に対してデータの保存・解析基盤を国内の安全認

証済みDC・クラウドに完全に閉じ込め、発明の完成地を紛れもなく日本国内に固定することを強く指導しなければならない¹。

2. 不正競争防止法上の「秘密管理性」水準の変容と2025年改訂営業秘密管理指針の再解釈

第2の波及経路は、未公開の発明、製造ノウハウ、設計図、顧客データなどを保護する不正競争防止法(不競法)上の「営業秘密(同法第2条第6項)」および「限定提供データ」の管理実務である¹⁸。営業秘密として法的保護(差止請求、損害賠償、および10年以下の拘禁刑・法人最大10億円以下の罰金という刑事罰)を受けるためには、秘密管理性、有用性、非公知性の三要件を満たす必要があり、とりわけ企業自身の管理努力が問われる「秘密管理性」が訴訟・刑事告訴における最大の争点となる¹⁸。

経済産業省は2025年3月、テレワークの常態化やクラウドストレージの利用拡大、生成AIの社内活用といった社会情勢の変化と最新判例を踏まえ、「営業秘密管理指針」を2019年以来6年ぶりに大規模改訂した¹⁸。この2025年改訂指針においては、民事と刑事の判断基準が統一されるとともに、外部のクラウドサービスを利用して営業秘密を保管・管理する場合であっても、階層制限に基づくアクセス制御や、クラウド事業者が提供するセキュリティ機能(ゼロトラストアーキテクチャ、デバイス認証、ログ監視等)、および利用規約上の守秘義務条項が整備されていれば、秘密管理性は失われず、むしろ秘密管理性を支える要素として評価されることが明確化された¹⁸。

しかし、2027年度以降に「国によるDC・クラウドの安全認証制度」が導入されることで、この「クラウド利用における秘密管理性」および「善管注意義務」の実務的解釈は新たな段階へと引き上げられることになる¹。なぜなら、今回の認証制度創設の背景として、政府自身が「懸念国の影響下にあるクラウドやデータセンターでは、中国の国家情報法等による強制的な情報アクセスや、海外からの保守運用ルートを通じた情報流出を秘密保持契約(NDA)や利用規約だけでは防げない」という事実を公的に認定したからである¹。

この状況下において、もし企業が国の安全認証を取得していない(特に懸念国の資本・支配関係や機器調達リスクを抱える)クラウドサービス上に重要な技術上の営業秘密や限定提供データを保管し、そこから技術流出が発生した場合、「利用規約に守秘義務条項がありID・パスワードを設定していたから秘密管理性は満たしていた」という主張は、少なくとも取引先や株主に対する法的責任(善管注意義務・取締役の監視義務)の場面では通用しなくなるリスクが極めて高い¹。さらに実務上より切実なのは、サプライチェーン全体における取引条件の変化である¹。既に金融庁が2026年4月にサードパーティ・サイバーセキュリティリスク管理の調査報告書を公表し、監督指針で再委託先や連携先へのデータ転送の把握を求めているように、今後は金融機関、医療機関、防衛・基幹インフラ企業、さらには大手メーカーとの共同研究開発契約(Joint R&D Agreement)や秘密保持契約(NDA)、技術ライセンス契約において、「営業秘密および共同研究データを保管・処理するクラウドは、国の安全認証を取得した事業者のサービスに限る(中国系等の未認証クラウドの利用禁止)」という条項が標準的な取引条件(デファクト・スタンダード)として組み込まれることになる¹。

また、先述した2020年の大手通信会社5G営業秘密漏えい事件や2026年の工作機械関連会社営業秘密漏えい事件(いずれも在日ロシア通商代表部員との共謀による不競法違反事件)が示すように、重要技術を持つ企業の従業員が外国情報機関に抱き込まれる端緒には、従業員個人の経済的困窮(金融情報)や健康・家庭問題(医療情報)の把握が存在する¹。すなわち、企業の知財部門にとって「自社の発明者・重要技術者の人事・健康・給与口座等の個人機微データが認証済みの安全なクラウドで守られているか」は、単なる労務管理の問題ではなく、従業員の弱みにつけ込んだ

ヒューミント(人的諜報)による営業秘密流出を未然に防ぐ防諜(カウンター・インテリジェンス)の第一線として位置づけ直される必要がある¹。

3. 特許出願非公開制度における「特定区域」要件と重要経済安保情報(セキュリティ・クリアランス)との連動

第3の波及経路は、経済安全保障推進法に基づく「特許出願非公開制度」および「重要経済安保情報保護活用法(セキュリティ・クリアランス制度)」における厳格な情報保全義務との連動である¹。

2024年5月から運用が開始された特許出願非公開制度において、特定技術分野(25分野)に属する出願が内閣府による第二次審査(保全審査)を経て「保全指定」を受けた場合、指定特許出願人および発明共有事業者には、保全対象発明情報の漏えいを防ぐための厳格な「適正管理措置」が義務付けられる¹⁶。万が一、指定特許出願人が適正管理措置を十分に講じていなかったことにより第三者が保全対象発明の内容を実施または開示した場合、特許出願が却下される(推進法第73条第6項、第74条第2項)という致命的なペナルティが課される²²。

内閣府の有識者会議資料(『特許出願の非公開に関する制度における適正管理措置について』)によれば、保全対象発明情報を取り扱う「特定区域」は原則として指定特許出願人または発明共有事業者が管理する場所を定める必要があるが、「クラウド事業者のサーバに電磁的記録を保管する場合のように、契約先事業者が管理する場所を特定区域として定めることも否定はされない」とされている¹⁶。ただしその条件として、クラウド事業者に保全対象発明の内容を知得させない形で業務委託を行うこと、情報保全上の要求事項を契約により明示すること、そして指定特許出願人自身が管理する場合と「同等の管理」が担保されることが厳格に求められている¹⁶。また、重要経済安保情報保護活用法においても、機密情報は原則として国内サーバーのみに保存し、クラウドを利用する場合は契約・設定でリージョンを日本に固定し、どの情報がどの国のサーバーに保存されるかを台帳管理して契約と技術の二重統制を行うことが求められる²⁷。

これまで知財実務の現場では、「民間企業が保全対象発明の電子データをクラウドに置く場合、どのクラウド事業者であれば内閣府が求める『特定区域』としての同等管理要件を満たすのか」という明確な公的基準が存在しなかった(政府調達向けのISMAPはあくまで行政機関向けの評価制度であるため¹)。しかし、2027年度以降に総務省・経済産業省による「民間向けのDC・クラウド安全認証制度」が稼働すれば、この安全認証を取得していることが、特許出願非公開制度におけるクラウド上の「特定区域」として認められるための事実上の必須要件(セーフハーバー基準)として機能することは確実である¹。

さらに、特許出願非公開制度における「損失補償(推進法第80条)」の実務にも直結する²¹。保全指定を受けた出願人に対する国の補償対象には、実施不許可等に伴う逸失利益、特許権留保に伴う逸失実施許諾料相当額、保全指定により目的を果たせなくなった費用に加え、第4の類型として「適正管理措置等により追加的に要した費用」が含まれている²¹。したがって、自社の特許出願が保全指定を受ける可能性のある先端技術企業(防衛、宇宙状況把握[SSA]、量子、半導体、AI、バイオ等)の知財部門は、平時から利用しているクラウド基盤が国の安全認証を取得できるか否かを確認し、もし保全指定に伴って認証済みクラウドへのデータ移行や専用暗号化環境の構築が必要となる場合には、その追加コストを適正管理措置に伴う追加費用の補償請求として客観的に算定・立証できるよう、契約および費用明細を区分管理しておく必要がある²¹。

4. 知財SaaS・パテントテックのサプライチェーンリスクと「IaaS認証の非継承問題」

第4の、そしてすべての企業の知財部門および特許事務所に日常業務レベルで影響するのが、「知財管理システム・パテントテック(知財SaaS)のサプライチェーン問題」である³。現代の知財業務は、期限・年金管理システム、先行技術調査・パテントマップ分析ツール、AI明細書ドラフティング支援ツール、AI機械翻訳、発明届出ポータルなど、多様なクラウド型SaaSに全面的に依存している³⁰。これらを入力・処理するデータは、まさに出願前の未公開発明(新規性喪失前の技術情報)や自社の研究開発戦略そのものである¹⁸。

ここで知財担当者が最も陥りやすい重大な誤解が、「利用している知財SaaSがAWSやMicrosoft Azure、Google Cloudといった大手クラウド(IaaS/PaaS)上で動いており、それらの大手クラウドが国の安全認証を取得すれば、その上で動く知財SaaSも自動的に安全(認証済み)になる」という錯覚である³。既存の政府向けクラウド評価制度であるISMAPの公式FAQが明確に否定しているとおり、「認証済みのIaaS・PaaS上で構築したという理由だけでは、その上で提供するSaaS自体を登録済みとみなすことはできない」のであり、この原則は2027年度からの新安全認証制度でも全く同様に妥当する³。なぜなら、たとえ基盤となるサーバー(AWS東京リージョンやAzure東日本リージョン等)が国内に立地し国の安全認証を取得していたとしても、その上で知財SaaSを開発・運用するベンダー自身が、システム保守やデータベース管理、あるいはAIモデルのファインチューニング業務を海外(特に中国等の懸念国)のオフショア開発拠点や再委託先に委託していれば、保守用の管理者権限(特権アカウント)を通じて未公開の発明データが海外から完全に閲覧・抽出可能となるからである¹。実際、今回の認証制度創設の契機となった過去の事案でも、外部からのハッキングではなく「業務委託という正規のルート」でデータが海外から見える状態になっていた点が問題視された¹。

知財業界では近年、株式会社パテント・リザルトのようにサービス提供側(自社SaaS)とクラウド利用側(AWS、Azure、Google Cloudのカスタマ管理)の双方でISO/IEC 27017等の情報セキュリティ認証を取得する先進的な動きや、NGB株式会社のようにMicrosoft Azure PortalとAzure Arcを用いてISMS準拠のインフラ可視化・監査体制を強化する取り組みが進んでいる¹²。しかし、新制度が導入される2027年度以降は、従来のISMS(ISO/IEC 27001/27017)の確認にとどまらず、知財SaaSベンダーに対して3つの観点から踏み込んだ監査・確認を行うことが知財部門の責務となる¹。

第一に、基盤およびベンダー自身の資本・サプライチェーン透明性(FOCI確認)の検証である¹。知財SaaSが利用するIaaS/PaaS・データセンター、バックアップ先、ログ・監視サービスが国の安全認証対象(国内サーバー・認証済み基盤)であることはもちろん、SaaSベンダー自身の株主・支配関係およびシステム開発・保守の再委託先に懸念国の影響がないかを確認しなければならない¹。第二に、国外からの運用・保守アクセスと管理者権限の隔離である³。障害対応やメンテナンスを含む一切の運用保守業務が日本国内(または安全保障上の問題がない法域)に限定されており、国外からの特権アクセスが技術的・契約的に遮断されているかを精査する必要がある³。第三に、米国CLOUD Actリスクを見据えた暗号鍵の自社統制(BYOK / HYOK)の実装である¹。前述のとおり、AWS、Azure、Google Cloudの米国系3強は日本の安全認証を取得する見通しであるが、米国企業である以上、米国のCLOUD Act(クラウド法)による米当局からのデータ開示要求リスクは法的に消滅しない¹。特に防衛・デュアルユース技術、先端半導体、量子、重要インフラ等の極めて機微な未公開発明情報を米国系クラウド(またはその上のSaaS)に保管する場合には、クラウド事業者側で暗号鍵を管理させるのではなく、Microsoft Azure Key Vault(FIPS 140-2 Level 3準拠のHSM)等の仕組みを活用したBYOK(Bring Your Own Key: 顧客管理鍵)やHYOK(Hold Your Own Key)を導入し、万が一クラウド事業者が外国政府から開示命令を受けたとしても、復号鍵を持たないため暗号文のままとなり技術内容を知得できない技術的統制(これは特許出願非公開制度における「クラウド事業者」に発明内

容を知得させない措置」にも合致する)を講じるべきである¹。
また、DC・クラウド事業者が認証取得のために中国製の安価なサーバーや通信機器・ルーターを排除し、審査・監査対応コストや国内DC増強投資、さらにはAI普及に伴う電力コストを価格に転嫁することで、クラウド利用料および知財SaaSのライセンス費用が中長期的に上昇するコストプッシュ圧力も予算策定上見込んでおく必要がある¹。

知財部門が講ずべき戦略的対応と実務ロードマップ

2027年1月召集の通常国会への法案提出、および2027年度後半以降の安全認証制度の稼働を見据え、企業の知的財産部門、法務・情報セキュリティ部門、ならびに特許事務所は、法案の細目が確定するのを漫然と待つのではなく、直ちに「自社のデータと知財インフラの地図」を描き始める必要がある¹。データセンターやクラウド、知財管理システムは一度大量のデータを預けると移行(マイグレーション)に多大な時間とコストを要するため、早期の棚卸しと調達基準の改定が不可欠である¹。まず第1フェーズ(2026年10月～12月の即時着手期)においては、知財・R&Dデータの棚卸しとマッピングを完遂する必要がある¹。具体的には、自社R&Dで扱うゲノム・医療・金融・生体・位置情報等の機微データと生体試料の総量および保存・処理クラウドを洗い出すとともに、海外CROや外部研究機関へのデータ解析委託契約を総点検し、経済安全保障推進法第78条および中国専利法第19条の観点から「発明完成地」の法的リスクを評価する¹。あわせて、営業秘密および特許出願非公開制度の対象となり得る特定技術分野(25分野)データの保管場所とアクセス権限を特定しなければならない¹⁶。

続く第2フェーズ(2027年1月～2027年春の法案提出期)では、知財SaaSおよび外部委託先のデューデリジェンスを実行する¹。利用中の知財管理システム、特許検索データベース、AI明細書作成・翻訳SaaS、および外部特許事務所が利用するクラウド基盤を調査し、各ベンダーに対してIaaS/PaaSの所在地、資本・支配関係(FOCI)、再委託先一覧、国外からの保守運用アクセスの有無に関する質問票を送付して監査を行う¹。同時に、機微な未公開発明データを扱うクラウド環境においてリージョン国内固定とBYOK(顧客管理鍵)の導入を実装する¹⁶。

第3フェーズ(2027年夏～2027年度後半の法成立・施行準備期)においては、契約ひな形の改定と社内規程のアップデートを推進する¹。共同研究開発契約、NDA、技術導入・委託契約のひな形に「国の安全認証を取得したDC・クラウドの利用義務」および「懸念国への再委託・データ移転禁止条項」を追加し、2025年3月改訂「営業秘密管理指針」に準拠した社内営業秘密管理規程にも保管先クラウドの要件として国の安全認証取得を明文化する¹。さらに、重要経済安保情報保護活用法第12条の適性評価対象者を含む重要技術者・発明者の個人機微データ保護体制を人事・情報システム部門と連携して強化する¹。

そして第4フェーズ(2027年度後半以降の制度本格稼働期)では、事前届出対応、クラウド移行、および補償請求体制を確立する¹。大量機微データを扱うR&Dプロジェクトにおける国への事前届出手続を法務・知財・R&Dの共同窓口で定型化し、安全認証を取得しないクラウド・SaaSからの計画的データ移行を完遂する¹。また、特許出願非公開制度の保全指定を受けた場合のクラウド「特定区域」指定手続と、適正管理措置に伴う追加クラウド費用の損失補償(類型4)算定エビデンスを整備する¹⁶。これら4つのフェーズにおける管理指標と法的根拠の対応関係を以下の表に整理する。

フェーズ・時期	対象領域	重点管理対象・実務	参照すべき法的根
---------	------	-----------	----------

		到達目標	拠・ガイドライン
第1フェーズ: 即時着手(2026年10月～12月)	知財・R&Dデータの棚卸しとマッピング	ゲノム・医療・金融等の機微データ・生体試料の保管解析先特定と発明完成地リスクの排除 ¹	第18回有識者会議資料3(2026年10月)、経済安保推進法第66条・第78条、中国専利法第19条 ⁴
第2フェーズ: 法案提出期(2027年1月～2027年春)	知財SaaS・外部委託先のデューデリジェンス	知財SaaS・特許事務所の基盤所在地・FOCI・海外保守アクセスの監査とBYOK暗号化統制 ¹	NIST SP 1326(2026年7月)、英国NCSC原則、ISMAP公式FAQ(SaaS非継承原則) ³
第3フェーズ: 法成立～施行準備(2027年夏～2027年度後半)	契約ひな形改定と社内規程のアップデート	共同研究契約・NDA・社内営業秘密規程への認証クラウド指定条項導入と発明者個人情報の防護 ¹	経済産業省「営業秘密管理指針」(2025年3月改訂)、重要経済安保情報保護活用法第12条、金融庁報告書(2026年4月) ³
第4フェーズ: 制度本格稼働期(2027年度後半以降)	事前届出対応・クラウド移行・補償請求体制の確立	事前届出手続の定型化、未認証基盤からの完全移行、保全指定時の特定区域指定と補償算定 ¹	2027年改正経済安全保障推進法、総務省・経産省DC・クラウド安全認証基準、特許出願非公開制度内閣府令 ¹

結論として、総務省・経済産業省によるデータセンター・クラウドの安全認証制度と、内閣官房が主導する個人機微データの事前届出・審査法制は、データの「器(インフラ)」と「中身(機微データ・技術情報)」の両面から懸念国の影響力を排除する経済安全保障上の強力な防壁である¹。知的財産部門にとっては、第一にバイオ・医療・金融AI等のデータ駆動型R&Dにおける解析委託やクラウド利用が直接の届出・中止命令対象となること、第二に不競法上の営業秘密管理や特許出願非公開制度の「特定区域」管理において認証済みクラウドの利用が事実上の規範となること、そして第三に基盤(IaaS)の認証が知財SaaSの安全性を自動保証しないという構造的死角(オフショア保守と米国CLOUD Actリスク)を直視し、契約・技術・ガバナンスの三位一体で知財サプライチェーンを再構築することが強く求められる¹。

引用文献

1. 国がデータセンターとクラウドに「安全認証」へ 中国系締め出しで、
<https://note.com/hirokimiyano/n/nf106195bc922>

2. データセンター・クラウドに安全認証制度 中国系を事実上排除,
<https://news.radiko.jp/article/station/QRR/140388/>
3. 政府、データセンター・クラウドに安全認証制度を創設へ,
<https://rocket-boys.co.jp/security-measures-lab/japan-data-center-cloud-security-certification-china-russia/>
4. データセキュリティ制度の検討について,
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r8_dai18/shiryo3.pdf
5. データセンターは経済安全保障インフラになるのか | yo4shi80 - note,
<https://note.com/yo4shi80/n/n03a2d6e62a46>
6. 中国系クラウドは使えなくなる？2027年度の安全認証制度,
<https://www.echo-station.com/cloud-datacenter-security-certification-2027/>
7. データセンター安全認証で「中国系排除」、国のクラウド名簿103件,
<https://note.com/metis999/n/n70eb670fa25b>
8. データセキュリティの検討状況 | 経済安全保障法制に関する有識者,
<https://pppt.jp/councils/documents/cas-keizai-anzen-hosyohousei-4index/20261016/shiryo3>
9. 主要国の個人機微データ保護法制と経済安全保障をめぐる国際的,
<https://pppt.jp/councils/documents/cas-keizai-anzen-hosyohousei-4index/20261016/shiryo4>
10. 機微個人データ「輸出管理」立法について(20261017追記) - note,
<https://note.com/techlawyer/n/n93c946a5eacc>
11. 経済安全保障法制に関する有識者会議(第18回) - 内閣府,
https://www.cao.go.jp/minister/2609_k_onoda/photo/2026_005.html
12. ISO/IEC 27017の取得要件と2026年改訂動向 - 株式会社一創,
<https://www.issoh.co.jp/column/details/12664/>
13. 第2回推進法改正に関する検討会合 議事のポイント,
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r7_dai13/shiryo10.pdf
14. JC-STARとは？IoT機器を選ぶ際のセキュリティの目安,
https://www.pct.co.jp/technical_note20261008
15. データ主権とは？経済安全保障の観点から分かりやすく解説,
<https://www.softbank.jp/business/content/blog/202509/what-is-data-sovereignty>
16. 特許出願の非公開制度に関する内閣府令(案)と適正管理措置,
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai9/siryou8.pdf
17. BYOKとは？仕組み・メリット・HSMの役割などを解説,
<https://www.hitachi-solutions.co.jp/security/sp/column/cloud/byok.html>
18. 【営業秘密管理・侵害における企業法務実務ガイド】2025年改訂,
<https://nao-lawoffice.jp/venture-startup/intellectual-property-right/eigyo-himitsu-kanri-shingai-jitsumu.php>
19. 日本 特許出願非公開制度(第一次審査 外国出願の禁止),
<https://www.asamura.jp/blog/2024/04/17/patent-application-closed-system-first-examination-prohibition-of-foreign-applications/>
20. 【中国】【実案】【審決シリーズ】1 秘密審査義務違反で無効と,
<https://www.tmi.gr.jp/eyes/blog/2022/13793.html>
21. 特許出願非公開制度の「非公開(防衛)運用」,
<https://yorozuipsc.com/uploads/1/3/2/5/132566344/27498f218450060a399c.pdf>

22. 日本版秘密特許制度(特許出願非公開)の概要 | ブログ | Our Eyes,
<https://www.tmi.gr.jp/eyes/blog/2022/13747.html>
23. 営業秘密のツボ 2025年8月20日 第110号 | 情報セキュリティ - IPA,
<https://www.ipa.go.jp/security/economics/mailmag/20250820.html>
24. 営業秘密・ノウハウの保護 | 不正競争防止法による企業の対策,
<https://ace-law.or.jp/komonbengoshi/jp/ip-trade-secret/>
25. 営業秘密管理指針が大幅改訂！テレワーク・AI時代の企業を知るべき,
<https://nexpert-law.com/column/business/column-8764/>
26. 営業秘密管理指針 - 経済産業省,
<https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf>
27. 【第6回】重要経済安保情報保護活用法の運用に関するガイドライン,
<https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/economic-security/economic-security12.html>
28. 宇宙状況把握(SSA)とは？観測データの知的財産・情報セキュリティ,
<https://asahigodo.jp/legal-issue/%E5%AE%87%E5%AE%99%E7%8A%B6%E6%B3%81%E6%8A%8A%E6%8F%A1ssa%E3%81%A8%E3%81%AF%EF%BC%9F%E8%A6%B3%E6%B8%AC%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E7%9F%A5%E7%9A%84%E8%B2%A1%E7%94%A3%E3%83%BB%E6%83%85/>
29. 法務担当が知っておくべき適格性評価の実務 - KYCコンサルティング,
<https://www.kycc.co.jp/column/20260126/>
30. クラウドセキュリティの国際規格「ISO/IEC 27017」認証を取得,
<https://www.patentresult.co.jp/news/2026/post-21783.html>
31. NGB株式会社 知的財産分野のリーディングカンパニーが挑む,
<https://www.microsoft.com/ja-jp/area/biz/smb/cases-ngbcorporation>