

データセンター・クラウド安全認証制度の動向と知財実務への影響

制度の概要と審査の仕組み

2027
年度
以降

新認証制度の導入検討



総務省・経済産業省

金融・医療などの
重要データを扱う
企業に利用促進



政府は2027年度以降、国内DC・クラウド事業者を対象とした新安全認証制度を検討。資本・支配関係や設備調達先のリスクを審査し、企業の知財管理やAI・SaaS利用基準の再評価が必須に。

知財実務への影響と推奨アクション



知財SaaS・生成AIの選定基準が厳格化



未公開発明などの重要データ管理において、サービスの基盤IaaSや運営主体の支配関係の確認が必須化。



資本関係と調達先の審査による間接的なリスク排除

企業支配構造

設備の調達先

設備の調達先

準拠法



国籍で直接排除せず、
評価を通じて担保

安全性担保

主要国の規制比較と日本案

米国 (FCC/大統領令)



懸念国関連の取引禁止や
事業者・機器の直接排除

EU (NIS2/CADA)



主権保証レベルの段階化と
サプライチェーンリスク評価

韓国 (情報通信網法)



DC事業者に対する情報保護
管理体系 (ISMS) 認証
の義務付け



日本案：民間向けの任意認証として設計、事前認証を通じた間接的な評価

知財部門が短期的（～6ヶ月）に取り組むべき4つの実務



1. 利用ツール台帳の作成



2. 未公開発明の入力ルール制定



3. ベンダー調査票改定



4. 海外拠点との共有経路棚卸しを実施