

DC・クラウド「安全認証」構想と企業の知財・データ防衛

政府は2027年度以降、DC・クラウド事業者を対象とした「安全認証」制度を導入する方針。本制度は、単なるサーバー所在地ではなく、事業者の支配関係や外国政府の影響、暗号鍵管理を含む「実質的なデータ支配権」を評価の核心とする。

政策・認証構想の核心（評価の真髄）



「サーバー所在地」のみの評価



「実質的なデータ支配」の評価へ
所在地だけでなく、親会社・支配関係、外国法域、暗号鍵管理が審査軸となる。

「懸念国の影響・主体リスク」を評価
国籍そのものより特権アクセス、サプライチェーン、法的拘束力が総合評価される。

保護対象は未公開発明・営業秘密・ソースコードも含む
個人データにとどまらず、研究データや製品設計図も重要な防衛対象となる。

企業が着手すべき実務アクション



高機微知財データの可視化と「データマップ」の作成

未公開発明や営業秘密の保存先、CSP、鍵、特権管理者を網羅的に標卸しする。



クラウド契約における「規制変更時の無罰退出権」の確保

認証喪失や規制変更時に違約金なしで移行・データ消去できる条項を組み込む。



所在地に頼らない「暗号鍵主権」の確立とアクセス遮断

顧客管理鍵（BYOK）を採用し、国外管理者からのアクセス権限を技術的に遮断する。