NIST SP 800-171 Rev.2 レベル1とレベル2の違い

米国国立標準技術研究所（NIST）発行の特別出版物（SP: Special Publication）800-171は、非連邦政府組織およびシステムにおける管理された非機密情報（CUI: Controlled Unclassified Information）の保護のための枠組みを提供しています。特に、米国戦争省（Department of War、DoW）や一般調達局（GSA）などの連邦政府機関と取引のある契約企業・下請企業にとって、これは重要な枠組みとなります。

サイバーセキュリティ成熟度モデル認証（CMMC）は、米国政府のサイバーセキュリティ強化の方針に合わせて、NIST 800-171 の要件を統合し拡張した認証制度です。ここで規定されるセキュリティレベル（レベル1とレベル2）は、サイバーセキュリティの成熟度と保護の度合いの違いを示しています。

レベル1（以前は「基礎（Foundational）」、現在では「レベル1」と呼ばれています）

NIST 800-171のレベル1は、連邦契約情報（FCI: Federal Contract Information）の基本的な保護要件に重点を置いています。このレベルには、主に連邦調達規則（FAR: Federal Acquisition Regulation）52.204-21に基づく15項目のセキュリティ要件が含まれます。

レベル1の主な特徴：

- 基本的なサイバーハイジーン（衛生管理）を重視。
- 一般公開を意図しない連邦契約情報（FCI）の保護が目的。
- 組織に対し、15項目のセキュリティ要件の実施と運用を義務付け（2024年までは17項目の要件）。
- サプライヤー・パフォーマンス・リスク・システム（SPRS）上で、コンプライアンス（要件への適合）に関する企業の上層部による確認を伴う自己適合宣言を行えば、それ以外の正式な評価は不要。
- 自己評価および確認は 年1回実施。
- FCIを取り扱う組織が対象。

レベル2（以前は「上級（Advanced）」、現在は「レベル2」と呼ばれています）

レベル2は、管理された非機密情報（CUI）の保護に対応しており、NIST SP 800-171で規定されている110項目すべてのセキュリティ要件と詳細にわたり一致しています。

レベル2の主な特徴：

- NIST 800-171 Rev.2 の110項目すべてのセキュリティ要件の実装を義務付け。
- 文書化、ポリシー策定、プロセスの制度化を重視。
- CUIデータを保存・処理・送信する組織が対象。
- 通常は、CMMC フレームワークに基づいた正式な評価または認証が必要。
- レベル1よりも高度なサイバーセキュリティ成熟度の達成。
- 第三者機関による評価は3年ごと、自己評価および確認は年1回実施。

TransVision Co., Ltd.
cmmc@transvision.co.jp

レベル1とレベル2の違い

項目別比較：レベル1／レベル2

	レベル 1	レベル 2
主な対象	連邦契約情報（FCI）	管理された非機密情報（CUI）
セキュリティ要件の項目数	NIST 800-171の15項目の要件	NIST 800-171の110項目の要件
評価頻度	年1回	3年ごと
評価要件	自己評価	第三者機関または政府機関による評価
対象情報	FCI	CUIおよびFCI
文書	SSP（システムセキュリティ計画）は必須ではない（推奨）	SSP（システムセキュリティ計画）は必須

最後に

NIST SP 800-171のレベル1とレベル2は、契約企業が取り扱う情報の機密性に応じて段階的に厳格化されるサイバーセキュリティ対策を示しています。組織は、自社における情報の管理環境や遵守すべき義務を評価し、特に今後の米国戦争省（DoW）や連邦政府によるサイバーセキュリティ規制の変化を踏まえて、どのレベルに適合すべきかを見極める必要があります。

トランスビジョンでは、CMMC準拠に向けたソフトウェア、ハードウェア、ドキュメントパッケージを提供し、認証取得に必要な時間やリソースの削減を支援しています。

CMMC準拠に向けた取り組みを始め、DoWのサプライチェーンへの参入をご検討の際は、ぜひ当社の cmmc@transvision.co.jp までお問い合わせください。

TransVision Co., Ltd.
cmmc@transvision.co.jp