CMMC レベル１（プラクティス）

No	CMMC 和訳	CMMC 原文	Level
1	AC.1.001【アクセス制御 (AC)】 システムへのアクセスは、権限のあるユーザー、あるいは権限のあるユーザーの代理として動作するプロセスまたは（その他のシステムを含む）装置に限定する。	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	1
2	AC.1.002 システムへのアクセスは、権限のあるユーザーが実行を許可されている各種のトランザクションおよび機能に限定する。	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	1
3	AC.1.003 外部システムへの接続および使用を検証（verify）し、管理/制限する。	Verify and control/limit connections to and use of external information systems.	1
4	AC.1.004 公衆アクセス可能なシステム上に掲載または処理された情報を管理する。	Control information posted or processed on publicly accessible information systems.	1
5	IA.1.076【識別と認証 (IA)】 システムのユーザー、あるいはユーザーの代理として動作するプロセスまたは装置を特定する。	Identify information system users, processes acting on behalf of users, or devices.	1
6	IA.1.077 組織のシステムへのアクセスを許可する前提条件として、それらのユーザー、プロセスまたは装置のアイデンティティーを認証（または検証）する。	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	1
7	MP.1.118【記憶媒体の保護 (MP)】 廃棄または再利用する前に、CUIを含むシステムの記憶媒体をサニタライズまたは破壊する。	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	1
8	PE.1.131【物理的保護 (PE)】 組織のシステム、装置、およびそれぞれの運用環境への物理的アクセスを、権限のある人に限定する。	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	1
9	PE.1.132 訪問者をエスコートし、その活動を監視する。	Escort visitors and monitor visitor activity.	1
10	PE.1.133 物理的アクセスの監査ログを保持する。	Maintain audit logs of physical access.	1
11	PE.1.134 物理的アクセス装置を管理・監督する。	Control and manage physical access devices.	1
12	SC.1.175【システムと通信の保護 (SC)】 組織の通信（すなわち、組織のシステムによって送受信される情報）を、システムの外部境界および主要な内部境界において監視・管理・保護する。	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	1
13	SC.1.176 内部ネットワークから物理的・論理的に分離された、公開（Publicly）アクセス可能なシステムコンポーネント用のサブネットワークを実装する。	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	1
14	SI.1.210【システムと情報の完全性 (SI)】 情報およびシステムの欠陥をタイムリーに特定し、報告し、修正する。	Identify, report, and correct information and information system flaws in a timely manner.	1
15	SI.1.211 組織のシステム内における適切な場所で、悪意のあるコードからの保護機能を提供する。	Provide protection from malicious code at appropriate locations within organizational information systems.	1
16	SI.1.212 悪意のコード保護メカニズムについて、その新リリースを入手できるようになった時に、それを更新する。	Update malicious code protection mechanisms when new releases are available.	1
17	SI.1.213 組織のシステムの定期的スキャンを実行すると共に、外部ソースからのファイルのリアルタイムスキャンを、ファイルがダウンロードされ、開かれ、実行される都度実行する。	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	1