■CCDS IoT機器セキュリティ要件_2023年版（CCDS-GR01-2023）_ANNEX1_海外セキュリティガイドライン・標準への対応

分類	ID	セキュリティ要件		NIST IR8425[※1]との対応		ETSI EN 303 645[※2]との対応		EUサイバーレジリエンス法案[※3]との対応		
		（サブセットのID、セキュリティ要件）		対応する要求項目	CCDS要件では非対応とした内容	対応する要求項目	CCDS要件では非対応とした内容	対応する要求項目		CCDS要件では非対応とした内容
1）IoT機器の機能要件	1-1	アクセス制御及び認証		#1 Asset Identification	#1「IoT製品のすべてのコンポーネントのインベントリを作成することができる」についてはCCDS要件では非対応。	5.1 No universal default passwords	5.1-3「認証メカニズムにベストプラクティスの暗号を使用する」については、CCDS要件では非対応。	1-(3)-(a)	be delivered with a secure by default configuration, including the possibility to reset the product to its original state;	デフォルトパスワードやPSK以外の初期値については要件を定めていない
				#2 Product Configuration		5.4 Securely store sensitive security parameters				
				#4 Interface Access Control		5.5 Communicate securely		1-(3)-(b)	ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	
						5.9 Make systems resilient to outages				
		1-1-1	TCP/UDPポートの無効化			5.6 Minimize exposed attack surfaces		1-(3)-(h)	be designed, developed and produced to limit attack surfaces, including external interfaces;	
		1-1-2	認証情報の変更	#2 Product Configuration #4 Interface Access Control		5.1 No universal default passwords 5.4 Securely store sensitive security parameters		–	–	
	1-2	データ保護		#3 Data Protection		5.4 Securely store sensitive security parameters		1-(3)-(c)	protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;	
						5.5 Communicate securely	5.5-3「暗号プリミティブを更新可能とする」については、CCDS要件では非対応。			
						5.8 Ensure that personal data is secure				
		1-2-1	データ消去			5.11 Make it easy for users to delete user data		–	–	
	1-3	ソフトウェア更新		#5 Software Update	＃5「（ソフトウェア）更新の自動適用」についてはCCDS要件では非対応。	5.3 Keep software updated	下記については、CCDS要件では非対応。 ・5.3-4「ソフトウェアの更新は、自動的なメカニズムを使用する」 ・5.3-5「初期化後、定期的にセキュリティアップデートが利用可能かどうかを確認する」 ・5.3-15「ソフトウェアの更新ができない制約のある機器については、製品の分離とハードウェアの交換が可能であること」 ・5-3-16「 IoT 機器のモデル名称は、機器上のラベルまたは物理的なインターフェースを介して、明確に認識できる」	1-(3)-(i)	be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	
								1-(3)-(k)	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.	要件が漠然としており、完全な対応整理は困難（CCDSの要件では更新ソフトウェアの改ざん防止のため、真正性の検証を要件としている）
						5.4 Securely store sensitive security parameters				
						5.7 Ensure software integrity	5.7-1「セキュアブートメカニズムを使用してそのソフトウェアを検証する必要がある」については、CCDS要件では非対応。			
	1-4	特にインシデントが多く影響度が大きい要件								
		1-4-1	Wi-Fiの認証方式	#4 Interface Access Control	#2「共有されるデータが、指定されたフォーマットとコンテンツの定義に合致していることを検証する」についてはCCDS要件では非対応。	5.5 Communicate securely		1-(3)-(a)	be delivered with a secure by default configuration, including the possibility to reset the product to its original state;	デフォルトパスワードやPSK以外の初期値については要件を定めていない
		1-4-2	Bluetoothの対策			5.6 Minimize exposed attack surfaces	下記については、CCDS要件では非対応 ・5.6-4「デバッグインタフェースが物理的にアクセス可能な場合は、ソフトウェアで無効化する」 ・5.6-8「コードは、サービス／デバイスの動作に必要な機能に限定する」 ・5.6-9「製造者は、機器に配備されるソフトウェアについて、安全な開発プロセスに従うべきである	1-(3)-(b)	ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	
		1-4-3	USBのアクセス制御							
		1-4-4	インジェクション対策			5.13 Validate input data	5.13-1「ユーザーインターフェースを介して入力されたデータ、アプリケーションプログラミングインターフェース（API）を介して転送されたデータ、またはサービスや機器内のネットワーク間で転送されたデータを検証する必要がある」については、CCDS要件では非対応。	1-(2)	Products with digital elements shall be delivered without any known exploitable vulnerabilities;	CCDSの要件では、統計的に重大な影響が想定される脆弱性を対象としており、全ての既知の脆弱性への対応までは求めてない

分類	ID	セキュリティ要件	NIST IR8425[※1]との対応		ETSI EN 303 645[※2]との対応		EUサイバーレジリエンス法案[※3]との対応		
		（サブセットのID、セキュリティ要件）	対応する要求項目	CCDS要件では非対応とした内容	対応する要求項目	CCDS要件では非対応とした内容	対応する要求項目		CCDS要件では非対応とした内容
2）IoT機器の運用における要件	2-1	連絡窓口・セキュリティサポート体制	#8 Information and Query Reception		5.2 Implement a means to manage reports of vulnerabilities		2-(2)	in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;	
							2-(7)	provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;	
					5.3 Keep software updated		2-(8)	ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	
	2-2	製品に関する文書管理	#7 Documentation				1-(1)	Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;	「生産」工程に対するセキュリティは対象としていない
							2-(1)	identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;	ソフトウェア部品表について「機械で読み取り可能な形式」までは指定しない。
	2-3	利用者への情報提供	#9 Information Dissemination	#9「外部機関（脆弱性追跡期間、認定者と認証者等）への報告」については、CCDS要件では非対応。	5.2 Implement a means to manage reports of vulnerabilities		2-(4)	once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;	
					5.3 Keep software updated				
			#10 Product Education and Awareness		5.11 Make it easy for users to delete user data		2-(5)	put in place and enforce a policy on coordinated vulnerability disclosure;	
					5-12 Make installation and maintenance of devices easy				
3）IoT機器の監査に関する要件	3-1	ログの記録	#6 Cybersecurity State Awareness		5.2 Implement a means to manage reports of vulnerabilities		1-(3)-(j)	provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;	
					5.7 Ensure software integrity				
		3-1-1 時間管理機能							

分類	ID	セキュリティ要件	NIST IR8425[*1]との対応		ETSI EN 303 645[*2]との対応		EUサイバーレジリエンス法案[*3]との対応	
		（サブセットのID、セキュリティ要件）	対応する要求項目	CCDS要件では非対応とした内容	対応する要求項目	CCDS要件では非対応とした内容	対応する要求項目	CCDS要件では非対応とした内容
CCDS要件では該当なし	–	–	–	–	5.9 Make systems resilient to outages	下記については、CCDS要件では非対応 ・5.9-1「データネットワークや電力が停止する可能性を考慮し、レジリエンスを組み込む必要がある」 ・5.9-2「ネットワークアクセスが失われた場合でも動作とローカル機能を維持し、電力損失が回復した場合に正常に回復する必要がある」	1-(3)-(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;	
					6 Data protection provisions for consumer IoT	Provision6-1～6-4の各項目について、CCDSでは非対応。 ※但し、個人情報の保護については、2-3 データ保護にて実装例を掲載	1-(3)-(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');	
					–	–	1-(3)-(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;	
					–	–	1-(3)-(g) minimise their own negative impact on the availability of services provided by other devices or networks;	
					–	–	2-(3) apply effective and regular tests and reviews of the security of the product with digital elements;	
					–	–	2-(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	

*1 NIST IR 8425 "Profile of the IoT Core Baseline for Consumer IoT Products"

*2 ETSI EN 303 645　"Cyber Security for Consumer Internet of Things: Baseline Requirements"

*3 "ANNEXES to the PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL"