日本語版の提供について

「Cloud Control Matrix3.0J」(以下CCMと記述)は、Cloud Security Allianceより提供されている「Cloud Control Matrix3.0」の日本語訳です。
このCCMは、原文をそのまま翻訳した物です。
従って、日本独自の法令や基準に関する記述は含まれておりません。

日本クラウドセキュリティアライアンスに関する情報は、以下のURLより参照可能ですのでご覧ください。
http://cloudsecurityalliance.jp

なお、日本語版の作成にあたって、**BSIジャパン**様に翻訳をご協力いたきました。

監修
二木　真明
山崎　万丈
小川　良一
勝見　勉
有本　真由
諸角　昌宏

2014年4月23日

著作権および資料の取扱いについて

以下の文言が、オリジナルのCCM本体末尾に記載されています。
本資料の取扱いに際しては、下記を遵守してください。

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance					Corporate Governance Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																				
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Application & Interface Security *Application Security* **アプリケーションとインターフェースセキュリティ** *アプリケーションセキュリティ*	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	アプリケーション及びインタフェース（API）は、業界の認める標準（たとえばWebアプリケーションの場合、OWASPなど）に従って、設計、開発及び導入しなければならない。また、これらは該当する法的及び規制上の順守義務に従わなければならない。		X	X	X	X	X		X	X	X	X		S3.10.0 S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.	I.4	G.16.3, I.3		SA-04	AI2.4		Domain 10	6.03.01. (c)	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-14	NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SC-2 NIST SP 800-53 R3 SC-4 NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1) NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1) NIST SP 800-53 R3 SC-10 NIST SP 800-53 R3 SC-11 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-12 (2) NIST SP 800-53 R3 SC-12 (5)	1.2.6	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1	Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11	CIP-007-3 - R5.1	SC-2 SC-3 SC-4 SC-5 SC-6 SC-7 SC-8 SC-9 SC-10 SC-11 SC-12 SC-13 SC-14 SC-17 SC-18 SC-20 SC-21 SC-22 SC-23		6.5
Application & Interface Security *Customer Access Requirements* **アプリケーションとインターフェースセキュリティ**	AIS-02	Prior to granting customers access to data, assets, and information systems, all identified security, contractual, and regulatory requirements for customer access shall be addressed and remediated.	データ、資産、情報システムへの顧客のアクセスを許可する前に、顧客のアクセスに関して特定されたすべてのセキュリティ上、契約上、及び規制上の要求事項が(顧客に)知らされており、満たされていなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.		C.2.1, C.2.3, C.2.4, C.2.6.1, H.1	10 (B) 11 (A+)	SA-01			Domain 10		NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6	1.2.2 1.2.6 6.2.1 6.2.2		A.6.2.1 A.6.2.2 A.11.1.1	Commandment #6 Commandment #7 Commandment #8		CA-1 CA-2 CA-5 CA-6		
Application & Interface Security *Data Integrity* **アプリケーションとインターフェースセキュリティ** *データの完全性*	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	アプリケーションのインタフェース及びデータベースで手動又はシステムによる処理エラー、データ破損、又は誤用が発生しないようにするために、データの入出力のチェックルーチン（マッチングやエディットチェックなど）を実装しなければならない。		X	X	X	X	X		X	X	X	X	X	I3.2.0 I3.3.0 I3.4.0 I3.5.0	(I3.2.0) The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies. (I3.3.0) The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. (I3.4.0) The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies. (I3.5.0) There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.	I.4	G.16.3, I.3		SA-05			Domain 10		NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-3	NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 SI-6 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1) NIST SP 800-53 R3 SI-9 NIST SP 800-53 R3 SI-10 NIST SP 800-53 R3 SI-11	1.2.6	45 CFR 164.312 (c)(1) 45 CFR 164.312 (c)(2) 45 CFR 164.312(e)(2)(i)	A.10.9.2 A.10.9.3 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.6.1 A.15.2.1	Commandment #1 Commandment #9 Commandment #11	CIP-003-3 - R4.2	SI-10 SI-11 SI-2 SI-3 SI-4 SI-6 SI-7 SI-9		6.3.1 6.3.2
Application & Interface Security *Data Security / Integrity* **アプリケーションとインターフェースセキュリティ** *データセキュリティ/完全性*	AIS-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure protection of confidentiality, integrity, and availability of data exchanged between one or more system interfaces, jurisdictions, or external business relationships to prevent improper disclosure, alteration, or destruction. These policies, procedures, processes, and measures shall be in accordance with known legal, statutory and regulatory compliance obligations.	1つ以上のシステムのインタフェース、異なる司法管轄区又は外部の取引関係者間で交換されるデータについての不正な開示、改ざん又は破壊を防ぐため、その機密性、完全性及び可用性を確実に保護するポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。これらのポリシー、手順、プロセス、対策は、既知の法律上及び規制上の遵守義務に沿ったものでなければならない。		X	X	X	X	X	X	X	X	X	X		S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	B.1	G.8.2.0.2, G.8.2.0.3, G.12.1, G.12.4, G.12.9, G.12.10, G.16.2, G.19.2.1, G.19.3.2, G.9.4, G.17.2, G.17.3, G.17.4, G.20.1	6 (B) 26 (A+)	SA-03	DS5.11		Domain 10	6.02. (b) 6.04.03. (a)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-13	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-4 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-8	1.1.0 1.2.2 1.2.6 4.2.3 5.2.1 7.1.2 7.2.1 7.2.2 7.2.3 7.2.4 8.2.1 8.2.2 8.2.3 8.2.5 9.2.1		A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	All		AC-1 AC-4 SC-1 SC-16		2.3 3.4.1 4.1 4.1.1 6.1 6.3.2a 6.5c 8.3 10.5.5 11.5
Audit Assurance & Compliance *Audit Planning* **監査保証とコンプライアンス** *監査計画*	AAC-01	Audit plans, activities, and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	監査計画、監査、並びにデータの複製、アクセス及びデータの区切りの画定を伴う監査実施項目は、業務プロセスの中断のリスクを最小限に抑えるよう設計されなければならない。監査活動は、利害関係者が事前に計画しこれに同意しなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S4.1.0 S4.2.0	(S4.1.0) The entity's system security is periodically reviewed and compared with the defined system security policies. (S4.2.0) There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.		L.1, L.2, L.7, L.9, L.11	58 (B)	CO-01	ME 2.1 ME 2.2 PO 9.5 PO 9.6		Domain 2, 4	6.01. (d)	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-7	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CA-7 (2) NIST SP 800-53 R3 PL-6	10.2.5	45 CFR 164.312(b)	Clause 4.2.3 e) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1	Commandment #1 Commandment #2 Commandment #3		CA-2 CA-7 PL-6		2.1.2.b

CLOUD CONTROLS MATRIX VERSION 3.0

CCMv3

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance						Corporate Governance Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																		
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Audit Assurance & Compliance *Independent Audits* **監査保証とコンプライアンス** *独立した監査*	AAC-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure that the organization addresses any nonconformities of established policies, procedures, and known contractual, statutory, or regulatory compliance obligations.	独立したレビュー及び評価を少なくとも年に1回、又はあらかじめ定められた間隔で実施し、設定された方針、手順、並びに既知の契約上、法令上及び規制上の遵守義務への不適合について、組織が確実に対応できるようにしなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S4.1.0 S4.2.0	(S4.1.0) The entity's system security is periodically reviewed and compared with the defined system security policies. (S4.2.0) There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.		L.2, L.4, L.7, L.9, L.11	58 (B) 59 (B) 61 (C+, A+) 76 (B) 77 (B)	CO-02	DS5.5 ME2.5 ME 3.1 PO 9.6		Domian 2, 4	6.03. (e) 6.07.01. (m) 6.07.01. (n)	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 RA-5	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 RA-5 (1) NIST SP 800-53 R3 RA-5 (2) NIST SP 800-53 R3 RA-5 (3) NIST SP 800-53 R3 RA-5 (6) NIST SP 800-53 R3 RA-5 (9)	1.2.5 1.2.7 4.2.1 8.2.7 10.2.3 10.2.5	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(D)	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8	Commandment #1 Commandment #2 Commandment #3	CIP-003-3 - R1.3 - R4.3 CIP-004-3 R4 - R4.2 CIP-005-3a - R1 - R1.1 - R1.2	CA-1 CA-2 CA-6 RA-5		11.2 11.3 6.6 12.1.2.b
Audit Assurance & Compliance *Information System Regulatory Mapping* **監査保証とコンプライアンス** *情報システムに関する規制の把握*	AAC-03	An inventory of the organization's external legal, statutory, and regulatory compliance obligations associated with (and mapped to) any scope and geographically-relevant presence of data or organizationally-owned or managed (physical or virtual) infrastructure network and systems components shall be maintained and regularly updated as per the business need (e.g., change in impacted-scope and/or a change in any compliance obligation).	データ又は組織が所有若しくは管理する(物理的又は仮想の)インフラストラクチャーネットワーク及びシステムコンポーネントの範囲及び地理的位置に関連する(および対応づけられる)、組織の外部の法令上及び規制上の遵守義務の一覧を維持し、事業上の必要に応じて定期的に更新しなければならない(影響を受ける範囲の変更や遵守義務の変更など)。	X	X	X	X	X	X	X	X	X	X	X	X	S3.1.0 x3.1.0	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair system [availability, processing integrity, confidentiality] commitments and (2) assess the risks associated with the identified threats.		L.1, L.2, L.4, L.7, L.9	76 (B) 77 (B) 78 (B) 83 (B) 84 (B) 85 (B)	CO-05	ME 3.1		Domain 2, 4	6.10. (a) 6.10. (b) 6.10. (c) 6.10. (d) 6.10. (e) 6.10. (f) 6.10. (g) 6.10. (h) 6.10. (i)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SI-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-13 (1) NIST SP 800-53 R3 SC-30 NIST SP 800-53 R3 SI-1	1.2.2 1.2.4 1.2.6 1.2.11 3.2.4 5.2.1		ISO/IEC 27001:2005 Clause 4.2.1 b) 2) Clause 4.2.1 c) 1) Clause 4.2.1 g) Clause 4.2.3 d) 6) Clause 4.3.3 Clause 5.2.1 a - f Clause 7.3 c) 4) A.7.2.1 A.15.1.1 A.15.1.3 A.15.1.4 A.15.1.6	Commandment #1 Commandment #2 Commandment #3		AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-7 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 RA-1 RA-2 SA-1 SA-6 SC-1 SC-13 SI-1		3.1.1 3.1
Business Continuity Management & Operational Resilience *Business Continuity Planning* **事業継続管理と運用** **レジリエンス** *事業継続計画*	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	すべての事業継続計画が、検査、保守及び情報セキュリティの要求事項に関する優先順位の特定について一貫性を持つように、事業継続計画立案及び計画作成のための一貫性のある統一された枠組みを確立し、文書化し、採用しなければならない。事業継続計画の要求事項には、以下が含まれる。 ・関連する依存関係に従った目的及び範囲の定義 ・計画の利用者が理解し利用できるようにすること ・(一人または複数の)指名された責任者(オーナー)が計画のレビュー、更新及び承認に責任を負うこと ・伝達経路、役割及び責任の定義 ・詳細な復旧の手順、手動による回避策及び参考情報 ・計画発動の手順	X	X	X	X	X	X	X	X	X	X	X	X	A3.1.0 A3.3.0 A3.4.0	(A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. (A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies. (A3.4.0) Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.		K.1.2.3. K.1.2.4, K.1.2.5, K.1.2.6, K.1.2.7, K.1.2.11, K.1.2.13, K.1.2.15		RS-03			Domain 7, 8	6.07. (a) 6.07. (b) 6.07. (c)	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-4 (1) NIST SP800-53 R3 CP-6 NIST SP800-53 R3 CP-6 (1) NIST SP800-53 R3 CP-6 (3) NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-7 (1) NIST SP800-53 R3 CP-7 (2) NIST SP800-53 R3 CP-7 (3) NIST SP800-53 R3 CP-7 (5) NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-8 (1) NIST SP800-53 R3 CP-8 (2) NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-9 (1) NIST SP800-53 R3 CP-9 (3) NIST SP800-53 R3 CP-10 NIST SP800-53 R3 CP-10 (2) NIST SP800-53 R3 CP-10 (3) NIST SP800-53 R3 PE-17		45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(B) 45 CFR 164.308 (a)(7)(ii)(C) 45 CFR 164.308 (a)(7)(ii)(E) 45 CFR 164.310 (a)(2)(i) 45 CFR 164.312 (a)(2)(ii)	Clause 5.1 A.6.1.2 A.14.1.3 A.14.1.4	Commandment #1 Commandment #2 Commandment #3		CP-1 CP-2 CP-3 CP-4 CP-6 CP-7 CP-8 CP-9 CP-10 PE-17		12.9.1 12.9.3 12.9.4 12.9.6
Business Continuity Management & Operational Resilience *Business Continuity Testing* **事業継続管理と運用**	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	事業継続計画及びセキュリティインシデント対応計画は、事前に定められた間隔で、又は組織及び環境の重大な変化に合わせて検証されなければならない。インシデント対応計画には、影響を受ける顧客(テナント)、及び重要なサプライチェーン内の事業プロセスの依存関係をになうその他の取引関係先を関与させなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	A3.3	(A3.3) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.		K.1.3, K.1.4.3, K.1.4.6, K.1.4.7, K.1.4.8, K.1.4.9, K.1.4.10, K.1.4.11, K.1.4.12	52 (B) 55 (A+)	RS-04			Domain 7, 8	6.07.01. (b) 6.07.01. (j) 6.07.01. (l)	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-4 (1)		45 CFR 164.308 (a)(7)(ii)(D)	A.14.1.5	Commandment #1 Commandment #2 Commandment #3		CP-2 CP-3 CP-4		12.9.2
Business Continuity Management & Operational Resilience *Datacenter Utilities / Environmental Contitions* **事業継続管理と運用** **レジリエンス** *データセンターのユーティリティ / *	BCR-03	Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications,and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	不正な妨害又は損害から保護することを目的として、あらかじめ定められた間隔でデータセンター設備サービス及び環境状況(水、電力、温度及び湿度管理、通信、インターネット接続など)の安全を確保し、監視し、維持し、有効性が継続していることを確認しなければならない。また、予想される又は予想外の事態に備えて、自動フェールオーバー又はその他の冗長性を持った設計を行わなければならない。	X	X						X	X	X	X		A3.2.0 A3.4.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. (A3.4.0) Procedures exist to protect against unauthorized access to system resource.	F.1	F.1.6, F.1.6.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12	9 (B) 10 (B)	RS-08			Domain 7, 8	6.08. (a) 6.09. (c) 6.09. (f) 6.09. (g)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)			A.9.2.2 A.9.2.3	Commandment #1 Commandment #2 Commandment #3 Commandment #4 Commandment #9 Commandment #11		PE-1 PE-4 PE-13		

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corporate Governance Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Consumer	Tenant / Consumer	Scope Applicability: AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Business Continuity Management & Operational Resilience *Documentation* **事業継続管理と運用 レジリエンス** *文書*	BCR-04	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	情報システムに関する文書（管理者ガイド、ユーザガイド、アーキテクチャー図など）は、権限を持った人が次の事項を確実に実施するために、利用できなければならない。 ・情報システムの設定、設置及び運用 ・システムのセキュリティ機能の有効利用		X	X	X	X	X	X	X	X	X	X			S3.11.0 A.2.1.0	(S3.11.0) Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities. (A.2.1.0) The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.		G.1.1	56 (B) 57 (B)	OP-02	DS 9 DS 13.1			Domain 7, 8		NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-10 NIST SP 800-53 R3 SA-5	NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-9 (1) NIST SP 800-53 R3 CP-9 (3) NIST SP 800-53 R3 CP-10 NIST SP 800-53 R3 CP-10 (2) NIST SP 800-53 R3 CP-10 (3) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1)	1.2.6		Clause 4.3.3 A.10.7.4	Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11	CIP-005-3a - R1.3 CIP-007-3 - R9	CP-9 CP-10 SA-5 SA-10 SA-11		12.1 12.2 12.3 12.4
Business Continuity Management & Operational Resilience *Environmental Risks* **事業継続管理と運用 レジリエンス** *環境リスク*	BCR-05	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	自然災害や故意による攻撃（火災、洪水、静電気あるいは雷、太陽によって誘発される磁気嵐、風、地震、津波、爆発、原子力事故、火山活動、バイオハザード、市民暴動、土砂災害、地殻運動、その他の自然又は人的災害）からの損害を予測し、それらに対する物理的保護を設計し、対応策を適用しなければならない。	X						X	X	X	X	X			A3.1.0 A3.2.0	(A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	F.1	F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8		RS-05			Domain 7, 8	6.07. (d) 6.08. (a) 6.09. (a) 6.09. (b) 6.09. (d)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3) NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	8.2.4	45 CFR 164.308 (a)(7)(i) 45 CFR 164.310(a)(2)(ii)	A.9.1.4 A.9.2.1	Commandment #1 Commandment #2 Commandment #3	CIP-004-3 R3.2	PE-1 PE-13 PE-14 PE-15 PE-18		
Business Continuity Management & Operational Resilience *Equipment Location* **事業継続管理と運用 レジリエンス** *機器の位置*	BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	環境上の脅威、危険、及び権限を持たないアクセスの機会によるリスクを軽減するために、施設を環境上のリスクの高い場所から隔離し、妥当な距離をとった位置にバックアップ施設を備えることでこれを補助しなければならない。	X						X	X	X	X	X			A3.1.0 A3.2.0	(A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	F.1	F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8	53 (A+) 75 (C+, A+)	RS-06			Domain 7, 8	6.07. (d) 6.08. (a) 6.09. (a) 6.09. (b) 6.09. (d)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18		45 CFR 164.310 (c)	A.9.2.1	Commandment #1 Commandment #2 Commandment #3		PE-1 PE-5 PE-14 PE-15 PE-18		9.1.3 9.5 9.6 9.9 9.9.1
Business Continuity Management & Operational Resilience *Equipment Maintenance* **事業継続管理と運用 レジリエンス** *機器のメンテナンス*	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	システムの運用の継続性と保守要員の確保を確実にするため、機器の保守に関する方針及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。	X	X	X	X	X	X	X	X	X	X	X			A3.2.0 A4.1.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. (A4.1.0) The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.		F.2.19	1 (B)	OP-04	A13.3		Domain 7, 8	6.09. (h)	NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-5	NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-2 (1) NIST SP 800-53 R3 MA-3 NIST SP 800-53 R3 MA-3 (1) NIST SP 800-53 R3 MA-3 (2) NIST SP 800-53 R3 MA-3 (3) NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-4 (1) NIST SP 800-53 R3 MA-4 (2) NIST SP 800-53 R3 MA-5 NIST SP 800-53 R3 MA-6	5.2.3 8.2.2 8.2.3 8.2.4 8.2.5 8.2.6 8.2.7	45 CFR 164.310 (a)(2)(iv)	A.9.2.4	Commandment #2 Commandment #5 Commandment #11	CIP-007-3 - R6.1 - R6.2 - R6.3 - R6.4	MA-2 MA-3 MA-4 MA-5 MA-6		
Business Continuity Management & Operational Resilience *Equipment Power Failures* **事業継続管理と運用 レジリエンス** *機器の停電*	BCR-08	Information security measures and redundancies shall be implemented to protect equipment from utility service outages (e.g., power failures and network disruptions).	施設のユーティリティサービスが停止した場合（たとえば、停電、ネットワークの中断など）に機器を保護するために、情報セキュリティ対策及びバックアップ機能を実装しなければならない。	X	X	X					X	X	X	X			A3.2.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	F.1	F.1.6, F.1.6.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12	54 (A+)	RS-07			Domain 7, 8	6.08. (a) 6.09. (e) 6.09. (f)	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14	NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-8 (1) NIST SP800-53 R3 CP-8 (2) NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-9 NIST SP800-53 R3 PE-10 NIST SP800-53 R3 PE-11 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3) NIST SP800-53 R3 PE-14			A.9.2.2 A.9.2.3 A 9.2.4	Commandment #1 Commandment #2 Commandment #3		CP-8 PE-1 PE-9 PE-10 PE-11 PE-12 PE-13 PE-14		
Business Continuity Management & Operational Resilience *Impact Analysis* **事業継続管理と運用 レジリエンス** *影響解析*	BCR-09	There shall be a defined and documented method for determining the impact of any disruption to the organization that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	事業中断が組織に与える影響を判断するための手段を定義し文書化しておかなければならない。これには、以下の事項が含まれる。 • 重要な製品及びサービスの特定 •プロセス、アプリケーション、事業パートナー、サードパーティサービスプロバイダなど、すべての依存関係の特定 •重要な製品及びサービスへの脅威の把握 •予想された又は予想外の事業中断による影響の確認及び時間経過に伴うこれらの影響の変化の確認 • 最大許容停止時間の設定 • 復旧の優先順位の設定 •最大許容停止時間内に重要な製品及びサービスを再開するための目標復旧時間の設定 • 再開に必要な資源の見積もり	X	X	X	X	X	X	X	X	X	X	X	X		A3.1.0 A3.3.0 A3.4.0	(A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. (A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies. (A3.4.0) Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.		K.2		RS-02			Domain 7, 8	6.02. (a) 6.03.03. (c) 6.07. (a) 6.07. (b) 6.07. (c)	NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 RA-3	NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 RA-3		45 CFR 164.308 (a)(7)(ii)(E)	ISO/IEC 27001:2005 A.14.1.2 A 14.1.4	Commandment #1 Commandment #2 Commandment #3	CIP-007-3 - R8 - R8.1 - R8.2 - R8.3	RA-3		

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance						Corporate Governance Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																				
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Business Continuity Management & Operational Resilience *Management Program* **事業継続管理と運用 レジリエンス** *管理プログラム*	BCR-10	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for business resiliency and operational continuity to manage the risks of minor to catastrophic business disruptions. These policies, procedures, processes, and measures must protect the availability of critical business operations and corporate assets in accordance with applicable legal, statutory, or regulatory compliance obligations. A management program shall be established with supporting roles and responsibilities that have been communicated and, if needed, consented and/or contractually agreed to by all affected facilities, personnel, and/or external business relationships.	軽微なリスクから大規模な事業中断に至るまでのリスクを管理することを目的として、事業の回復力と運用の継続性のためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。これらの方針、手順、プロセス、手段では、該当する法的又は規制上の順守義務に従って、重要な業務や企業資産の可用性を保護しなければならない。役割や責任を記載した管理プログラムを作成しなければならない。また、これらは、影響を受けるすべての施設、人員、外部取引関係者に通知され、必要に応じて同意又は契約により合意されていなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	A3.1.0 A3.3.0 A3.4.0	Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies. Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.		K.1.2.9, K.1.2.10, K.3.1	27 (B) 31 (C+, A+)	RS-01	PO 9.1 PO 9.2 DS 4.2		Domain 7, 8	6.07. (a)	NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 CP-2	NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-2 (1) NIST SP 800-53 R3 CP-2 (2)		45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(C)	Clause 4.3.2 A.14.1.1 A.14.1.4	Commandment #1 Commandment #2 Commandment #3		CP-1 CP-2		12.9.1
Business Continuity Management & Operational Resilience *Policy* **事業継続管理と運用 レジリエンス** *ポリシー*	BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	業界によって受け入れられるような標準（ITIL　v4、COBIT　5など）に基づいて事業部門、従業員、顧客を支援する組織のIT機能を適切に計画し、提供し、支援することを目的として、適切なITガバナンス及びサービス管理のためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。さらに、ポリシーと手順では、（必要な）役割と責任を定義し、定期的な従業員訓練によって周知徹底しなければならない。				X	X	X	X	X	X	X	X		S2.3.0	(S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality of data, processing integrity, system security and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.		G.1.1	45 (B)	OP-01	DS13.1		Domain 7, 8	6.03. (c)	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 CM-6 (1) NIST SP 800-53 R3 CM-6 (3) NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-4 (1) NIST SP 800-53 R3 MA-4 (2) NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1) NIST SP 800-53 R3 SA-12	8.2.1		Clause 5.1 A 8.1.1 A.8.2.1 A 8.2.2 A.10.1.1	Commandment #1 Commandment #2 Commandment #3 Commandment #6 Commandment #7		CM-2 CM-3 CM-4 CM-5 CM-6 CM-9 MA-4 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-12		12.1 12.2 12.3 12.4
Business Continuity Management & Operational Resilience *Retention Policy* **事業継続管理と運用 レジリエンス** *保持ポリシー*	BCR-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	重要な資産の保持期間を、それぞれのポリシー及び手順、並びに該当する法的又は規制上の順守義務に従って定義し、これに準拠するためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。バックアップ及び復旧のための手段は、事業継続計画の一部として導入し、有効性の確認のために適宜テストしなければならない。			X	X	X	X	X	X	X	X	X	X	A3.3.0 A3.4.0 I3.20.0 I3.21.0	(A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies. (A3.4.0) Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies. (I3.20.0) Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies. (I3.21.0) Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.		D.2.2.9	36 (B)	DG-04	DS 4.1 DS 4.2 DS 4.5 DS 4.9 DS 11.6		Domain 5	6.03. (h) 6.07.01. (c)	NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-9	NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-2 (1) NIST SP 800-53 R3 CP-2 (2) NIST SP 800-53 R3 CP-6 NIST SP 800-53 R3 CP-6 (1) NIST SP 800-53 R3 CP-6 (3) NIST SP 800-53 R3 CP-7 NIST SP 800-53 R3 CP-7 (1) NIST SP 800-53 R3 CP-7 (2) NIST SP 800-53 R3 CP-7 (3) NIST SP 800-53 R3 CP-7 (5) NIST SP 800-53 R3 CP-8 NIST SP 800-53 R3 CP-8 (1) NIST SP 800-53 R3 CP-8 (2) NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-9 (1) NIST SP 800-53 R3 CP-9 (3)	5.1.0 5.1.1 5.2.2 8.2.6	45 CFR 164.308 (a)(7)(ii)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR 164.308(a)(7)(ii)(D) 45 CFR 164.316(b)(2)(i) (New)	Clause 4.3.3 A.10.5.1 A.10.7.3	Commandment #11	CIP-003-3 - R4.1	CP-2 CP-6 CP-7 CP-8 CP-9 SI-12 AU-11		3.1 3.1.1 3.2 9.9.1 9.5 9.6 10.7
Change Control & Configuration Management *New Development / Acquisition* **変更管理と構成管理** *新規開発および調達*	CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装し、データ、実/仮想アプリケーション、インフラストラクチャーネットワーク及びシステムコンポーネント、ならびに事業用・業務用・データセンター用各施設の新規の開発および調達が、組織の事業責任者もしくはその責にある職務または機能によって、確実に事前承認されているようにしなければならない。	X	X	X	X	X	X	X	X	X	X	X		S3.12.0 S3.10.0 S3.13.0	(S3.12.0) Procedures exist to maintain system components, including configurations consistent with the defined system security policies. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies. (S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	I.2	I.1.1, I.1.2, I.2. 7.2, I.2.8, I.2.9, I.2.10, I.2.13, I.2.14, I.2.15, I.2.18, I.2.22.6, L.5		RM-01	A12 A16.1		None	6.03. (a)	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7)	1.2.6		A.6.1.4 A.6.2.1 A.12.1.1 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.5 A.15.1.3 A.15.1.4	Commandment #1 Commandment #2 Commandment #3		CA-1 CM-1 CM-9 PL-1 PL-2 SA-1 SA-3 SA-4		6.3.2

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corporate Governance Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Tenant / Consumer	Scope Applicability: AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Change Control & Configuration Management *Outsourced Development* **変更管理と構成管理** *開発の外部委託*	CCC-02	The use of an outsourced workforce or external business relationship for designing, developing, testing, and/or deploying the organization's own source code shall require higher levels of assurance of trustworthy applications (e.g., management supervision, established and independently certified adherence of information security baselines, mandated information security training for outsourced workforce, and ongoing security code reviews).	組織が自組織のためのソースコードの設計・開発・試験・実装のために、外部委託先の労働力又は外部の取引先を使用する場合は、信頼度の高いアプリケーションの保証をより高いレベルで要求しなければならない。(例: 管理に対する上位の監督、確立され第三者に証明された情報セキュリティのベースラインへの準拠、外部委託先の労働力に対する情報セキュリティ教育の義務付け、継続的なセキュリティ目的のコードレビュー)		X	X	X	X	X	X	X	X	X	X	X	S3.10.0 S3.13	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability, confidentiality of data, processing integrity, systems security and related security policies. (S3.13) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	C.2 I.1 I.2 I.4	C.2.4, G.4, G6, I.1, I.4.4, I.4.5, I.2.7.2, I.2.8, I.2.9, I.2.15, I.2.18, I.2.22.6, I.2.7.1, I.2.13, I.2.14, I.2.17, I.2.20, I.2.22.2, I.2.22.4, I.2.22.7, I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14, I.3, J.1.2.10, L.7, L.9, L.10	27 (B)	RM-04			None		NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1) NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1) NIST SP 800-53 R3 SA-12			A.6.1.8 A.6.2.1 A.6.2.3 A.10.1.4 A.10.2.1 A.10.2.2 A.10.2.3 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.5.5 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	Commandment #1 Commandment #2 Commandment #3		SA-4 SA-5 SA-8 SA-9 SA-10 SA-11 SA-12 SA-13		3.6.7 6.4.5.2 7.1.3 8.5.1 9.1 9.1.2 9.2b 9.3.1 10.5.2 11.5 12.3.1 12.3.3
Change Control & Configuration Management *Quality Testing* **変更管理と構成管理** *品質検査*	CCC-03	A program for the systematic monitoring and evaluation to ensure that standards of quality and security baselines are being met shall be established for all software developed by the organization. Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established and documented, and tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security. Management shall have a clear oversight capacity in the quality testing process, with the final product being certified as "fit for purpose" (the product should be suitable for the intended purpose) and "right first time" (mistakes should be eliminated) prior to release. It is also necessary to incorporate technical security reviews (i.e., vulnerability assessments and/or penetration testing) to remediate vulnerabilities that pose an unreasonable business risk or risk to customers (tenants) prior to release.	組織が開発するすべてのソフトウェアが、品質及びセキュリティベースラインの基準に適合していることを確実にするために、体系的な監視及び評価のプログラムを確立しなければならない。情報システム、アップグレード、新バージョンの品質評価及び受入れ基準を確立し文書化しなければならない。また、セキュリティを維持するために、開発時及び受入れ前にシステムの試験を実施しなければならない。管理者は、品質試験過程において明確な監視能力を持ち、最終成果物が「目的に合致している」(成果物が意図した目的に適している)こと、また、リリース前に「適正である」(瑕疵が除去されている)ことを証明できなければならない。また、リリース前に不当な事業リスク又は顧客(テナント)へのリスクをもたらす脆弱性を解決するために、技術的なセキュリティレビュー(脆弱性の評価または侵入試験)を取り入れる必要もある。		X	X	X	X	X	X	X	X	X	X		A3.13.0 C3.16.0 I3.14.0 S3.10.0 S3.13	(A3.13.0, C3.16.0, I3.14.0, S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability, confidentiality of data, processing integrity, systems security and related security policies. (S3.13) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.		C.1.7, G.1, G.6, I.1, I.4.5, I.2.18, I.22.1, I.22.3, I.22.6, I.2.23, I.2.22.2, I.2.22.4, I.2.22.7. I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14,I .2.20, I.2.17, I.2.7.1, I.3, J.2.10, L.9		RM-03	PO 8.1		None	6.03.01. (b) 6.03.01. (d)	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1) NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1)	9.1.0 9.1.1 9.2.1 9.2.2		A.6.1.3 A.10.1.1 A.10.1.4 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	Commandment #1 Commandment #2 Commandment #3		CM-1 CM-2 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-13		1.1.1 6.1 6.4
Change Control & Configuration Management *Unauthorized Software Installations* **変更管理と構成管理** *未承認のソフトウェアのインストール*	CCC-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	組織が所有又は管理するユーザのエンドポイントデバイス(支給されたワークステーション、ラップトップ、モバイルデバイスなど)、ITインフラストラクチャーネットワーク及びシステムコンポーネントに承認されていないソフトウェアがインストールされることを防ぐために、方針及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。		X	X	X	X		X	X	X	X	X		A3.6.0 S3.5.0 S3.13.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. (S3.5.0) Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software. (S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	G.1 I.2	G.2.13, G.20.2,G.20.4, G.20.5, G.7, G.7.1, G.12.11, H.2.16, I.2.22.1, I.2.22.3, I.2.22.6, I.2.23		RM-05			None		NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-3	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-5 (1) NIST SP 800-53 R3 CM-5 (5) NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1) NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 CM-8 (1) NIST SP 800-53 R3 CM-8 (3) NIST SP 800-53 R3 CM-8 (5) NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1)	3.2.4 8.2.2		A.10.1.3 A.10.4.1 A.11.5.4 A.11.6.1 A.12.4.1 A.12.5.3	Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #11		CM-1 CM-2 CM-3 CM-5 CM-7 CM-8 CM-9 SA-6 SA-7 SI-1 SI-3 SI-4 SI-7		

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corp Gov Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Change Control & Configuration Management *Production Changes* **変更管理と構成管理** *業務の変更*	CCC-05	Policies and procedures shall be established, and supporting IT governance and service management-related business processes implemented, for managing the risks associated with applying changes to business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, as well as infrastructure network and systems components. Technical measures shall be implemented to provide assurance that, prior to deployment, all changes directly correspond to a registered change request, business-critical or customer (tenant) impacting risk analysis, validation of expected outcome in staged environment, pre-authorization by appropriate management, and notification to, and/or authorization by, the customer (tenant) as per agreement (SLA).	業務上重要な、又は顧客(テナント)に影響する実/仮想アプリケーション及びシステム間インタフェース(API)の設計及び設定、インフラストラクチャーネットワーク及びシステムコンポーネントに変更を適用する際のリスクを管理するために、ポリシー及び手順を確立し、これらを補完するITガバナンス及びサービス管理のための事業業務プロセスを導入しなければならない。導入前に、技術的対策を施すことによって、すべての変更が、登録された変更要求、業務上重要な又は顧客(テナント)に影響するリスクの分析、ステージごとに起こりうる結果の検証、適切な経営陣による事前承認、契約(SLA)に従った顧客(テナント)への通知およびその承認、のすべてを満たすことを保証しなければならない。		X	X	X	X	X	X	X	X	X	X	X	A3.16.0 S3.13.0	(A3.16.0, S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.		I.2.17, I.2.20, I.2.22		RM-02	A16.1 A17.6		None	6.03. (a)	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 PL-5 NIST SP 800-53 R3 SI-2	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CA-7 (2) NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-5 (1) NIST SP 800-53 R3 CM-5 (5) NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 CM-6 (1) NIST SP 800-53 R3 CM-6 (3) NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 PL-5 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-6 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1)	1.2.6	45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.4 A.12.5.1 A.12.5.2	Commandment #1 Commandment #2 Commandment #3 Commandment #11	CIP-003-3 - R6	CA-1 CA-6 CA-7 CM-2 CM-3 CM-5 CM-6 CM-9 PL-2 PL-5 SI-2 SI-6 SI-7		1.1.1 6.3.2 6.4 6.1
Data Security & Information Lifecycle Managment *Classification* **データセキュリティと情報ライフサイクル管理** *分類*	DSI-01	Data and objects containing data shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization, third-party obligation for retention, and prevention of unauthorized disclosure or misuse.	データ及びデータを含むオブジェクトは、データタイプ、データ発生地の司法管轄、データ所在地の司法権、コンテキスト、法規制、契約上の制約、価値、機微性、組織にとっての重要性、第三者のための保存義務、不正な開示や誤用の防止の諸観点に基づいて、機密区分されなければならない。			X	X	X	X	X	X	X	X	X	X	S3.8.0 C3.14.0	(S3.8.0) Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary. (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies.		D.1.3, D.2.2		DG-02	PO 2.3 DS 11.6		Domain 5	6.04.03. (a)	NIST SP 800-53 R3 RA-2	NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 AC-4	1.2.3 1.2.6 4.1.2 8.2.1 8.2.5 8.2.6		A.7.2.1	Commandment #9	CIP-003-3 - R4 - R5	RA-2 AC-4		9.7.1 9.10 12.3
Data Security & Information Lifecycle Management *Data Inventory / Flows* **データセキュリティと情報ライフサイクル管理** *データ保存/フロー*	DSI-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	法律、規制、又はサプライチェーン契約(SLA)の準拠の影響を確認し、データに関連するその他の事業リスクに対処することを目的として、地理的に分散するサービスの実/仮想アプリケーション、インフラストラクチャーネットワーク及びシステムコンポーネント内に(常時又は一次的に)存在し、他の第三者と共有されるデータのデータフローの一覧を作成し、文書化し、維持するための方針及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。プロバイダは、特に顧客データがサービスの一部として利用される場合は、要求に基づいて、顧客(テナント)に遵守義務が及ぼす影響及びリスクを通知しなければならない。																--			Domain 5	6.10. (a) 6.10. (b) 6.10. (c) 6.10. (d) 6.10. (e)		NIST SP 800-53 R3 SC-30								
Data Security & Information Lifecycle Management *eCommerce Transactions* **データセキュリティと情報ライフサイクル管理** *eコマーストランザクション*	DSI-03	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	契約上の問題やデータの破損を防ぐことができるように、公的ネットワークを使って送受信されるe-コマースに関わるデータを適切に分類し、不正行為、許可されていない開示又は変更から保護しなければならない。		X				X		X	X	X	X	X	S3.6 I13.3.a-e I3.4.0	(S3.6) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks. (I13.3.a-e) The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. (I3.4.0) The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing	G.4 G.11 G.16 G.18 I.3 I.4	G.19.1.1, G.19.1.2, G.19.1.3, G.10.8, G.9.11, G.14, G.15.1		IS-28	DS 5.10 5.11		Domain 2		NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-1	NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-10 NIST SP 800-53 R3 AU-10 (5) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1) NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1)	3.2.4 4.2.3 7.1.2 7.2.1 7.2.2 8.2.1 8.2.5	45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	A.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1 A.10.9.2 A.15.1.4	Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11		AC-14 AC-21 AC-22 IA-8 AU-10 SC-4 SC-8 SC-9		2.1.1 4.1 4.1.1 4.2
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy* **データセキュリティと情報ライフサイクル管理**	DSI-04	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	データ及びデータを含むオブジェクトのラベリング、処理取扱い、セキュリティのためのポリシー及び手順を確立しなければならない。データをまとめて格納するオブジェクトには、ラベルを継承して保持する仕組みを実装しなければならない。			X	X	X	X	X	X	X	X	X	X	S3.2.a	*(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.*	G.13	D.2.2		DG-03	PO 2.3 DS 11.6		Domain 5	6.03.05. (b)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-12	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-16 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-3 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1) NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-12	1.1.2 5.1.0 7.1.2 8.1.0 8.2.5 8.2.6		A.7.2.2 A.10.7.1 A.10.7.3 A.10.8.1	Commandment #8 Commandment #9 Commandment #10	CIP-003-3 - R4 - R4.1	AC-16 MP-1 MP-3 PE-16 SI-12 SC-9		9.5 9.6 9.7.1 9.7.2 9.10
Data Security & Information Lifecycle Management *Information Leakage* **データセキュリティと情報ライフサイクル管理** *情報漏えい*	DSI-05	Security mechanisms shall be implemented to prevent data leakage.	データの漏えいを防ぐために、セキュリティ機構を実装しなければならない。			X	X	X	X	X	X	X	X	X		C3.5.0 S3.4.0	(C3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies. (S3.4.0) Procedures exist to protect against unauthorized access to system resources.		I.2.18		DG-07	DS 11.6		Domain 5		NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-3	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-2 (1) NIST SP 800-53 R3 AC-2 (2) NIST SP 800-53 R3 AC-2 (3) NIST SP 800-53 R3 AC-2 (4) NIST SP 800-53 R3 AC-2 (7) NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 AC-3 (3) NIST SP 800-53 R3 AC-4 NIST SP 800-53 R3 AC-6 NIST SP 800-53 R3 AC-6 (1) NIST SP 800-53 R3 AC-6 (2) NIST SP 800-53 R3 AC-11 NIST SP 800-53 R3 AC-11 (1) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SC-28 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1)	7.2.1 8.1.0 8.1.1 8.2.1 8.2.2 8.2.5 8.2.6		A.10.6.2 A.12.5.4	Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8 Commandment #9 Commandment #10 Commandment #11		AC-2 AC-3 AC-4 AC-6 AC-11 AU-13 PE-19 SC-28 SA-8 SI-7		1.2 6.5.5 11.1 11.2 11.3 11.4 A.1

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance					Corp Gov Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																	
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Data Security & Information Lifecycle Management *Non-Production Data* **データセキュリティと情報ライフサイクル管理** *非生産データ*	DSI-06	Production data shall not be replicated or used in non-production environments.	製造データは、非製造環境で複製も使用もしてはならない。				X	X	X		X	X	X	X		C3.5.0 S3.4.0 C3.21.0	(C3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies. (S3.4.0) Procedures exist to protect against unauthorized access to system resources. (C3.21.0) Procedures exist to provide that confidential information is protected during the system development, testing, and change processes in accordance with defined system confidentiality and related security policies.		I.2.18		DG-06			Domain 5	6.03. (d)		1.2.6	45 CFR 164.308(a)(4)(ii)(B)	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	Commandment #9 Commandment #10 Commandment #11	CIP-003-3 - R6	SA-11 CM-04		6.4.3
Data Security & Information Lifecycle Management *Ownership / Stewardship* **データセキュリティと情報ライフサイクル管理** *管理責任 / 受託責任*	DSI-07	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	すべての情報に対して管理責任者が指名されなければならない。管理責任者の責任は、定義され、文書化され、通知されなければならない。			X	X	X	X	X	X	X	X	X		S2.2.0 S2.3.0 S3.8.0	(S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users. (S2.3.0) Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them. (S3.8.0) Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary		C.2.5.1, C.2.5.2, D.1.3, L.7		DG-01	DS5.1 PO 2.3		Domain 5		NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2	6.2.1	45 CFR 164.308 (a)(2)	A.6.1.3 A.7.1.2 A.15.1.4	Commandment #6 Commandment #10	CIP-007-3 - R1.1 - R1.2	CA-2 PM-5 PS-2 RA-2 SA-2		
Data Security & Information Lifecycle Management *Secure Disposal* **データセキュリティと情報ライフサイクル管理** *安全な廃棄*	DSI-08	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	あらゆるストレージメディアからデータを安全に破棄し、完全に消去するためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装することにより、データがいかなるコンピュータフォレンジック手法によっても回復できないようにしなければならない。			X	X	X	X	X	X	X	X	X		C3.5.0 S3.4.0	(C3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies. (S3.4.0) Procedures exist to protect against unauthorized access to system resources.		D.2.2.10, D.2.2.11, D.2.2.14,	37 (B)	DG-05	DS 11.4		Domain 5	6.03. (h)	NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 PE-1	NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 MP-6 (4) NIST SP 800-53 R3 PE-1	5.1.0 5.2.3	45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	A.9.2.6 A.10.7.2	Commandment #11	CIP-007-3 - R7 - R7.1 - R7.2 R7.3	MP-6 PE-1		3.1.1 9.10 9.10.1 9.10.2 3.1
Datacenter Security *Asset Management* **データセンタセキュリティ** *資産管理*	DCS-01	Assets must be classified in terms of business criticality in support of dynamic and distributed physical and virtual computing environments, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly (or in real-time), and assigned ownership supported by defined roles and responsibilities, including those assets used, owned, or managed by customers (tenants).	資産は事業上の重要性の視点から分類しなければならない。事業上の重要性とは、動的及び分散した物理的及び仮想コンピュータ環境、サービスレベルの期待値、運用の継続性の要件を担保することである。すべての現場や地理的場所に位置する業務上不可欠な資産の完全な目録とその使用履歴を維持し、定期的に（又はリアルタイムに）更新し、定義された役割及び責任を持つ管理責任者を割当てなければならない。対象とする資産には、顧客（テナント）が使用、所有、又は管理する資産も含む。													S3.1.0 C3.14.0 S1.2.b-c	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies. (S1.2.b-c) b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction policies. c. Assessing risks on a periodic basis.				FS-08			Domain 8											
Datacenter Security *Controlled Access Points* **データセンタセキュリティ** *コントロールされたアクセスポイント*	DCS-02	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	機微なデータ及び情報システムを保護するために、物理的なセキュリティ境界（フェンス、壁、柵、警備員、ゲート、電子的監視、物理的認証メカニズム、受付デスク、安全パトロールなど）を実装しなければならない。	X							X	X	X	X		A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B)	FS-03	DS 12.2 DS 12.3		Domain 8	6.08. (a) 6.09. (i)	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-8	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-6 (1) NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-7 (1) NIST SP 800-53 R3 PE-8 NIST SP 800-53 R3 PE-18	8.2.3		A.9.1.1 A.9.1.2	Commandment #1 Commandment #2 Commandment #3 Commandment #5	CIP-006-3c R1.2 - R1.3 - R1.4 - R1.6 - R1.6.1 - R2 - R2.2	PE-2 PE-3 PE-6 PE-7 PE-8 PE-18		9.1 9.1.1 9.1.2 9.1.3 9.2

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance						Corporate Governance Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																		
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Consumer / Tenant	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Datacenter Security *Equipment Identification* **データセンタセキュリティ** *アイデンティフィケーション*	DCS-03	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	接続認証の手段として自動的に機器を識別する仕組みを使用しなければならない。接続認証の完全性を確認するために、既知の機器の所在場所に基づいて所在場所を特定する技術を使用することができる。	X	X	X	X	X								S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	D.1	D.1.1, D.1.3		SA-13	DS5.7		Domain 10	6.05. (a)	NIST SP 800-53 R3 IA-4	NIST SP 800-53 R3 IA-3 NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-4 (4)			A.11.4.3	Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #8		IA-3 IA-4		
Datacenter Security *Off-Site Authorization* **データセンタセキュリティ** *オフサイト認証*	DCS-04	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	ハードウェア、ソフトウェア又はデータをサイト外の場所に移動させるには、事前の承認が必要である。	X			X		X	X	X	X	X	X		S3.2.f C3.9.0	(S3.2.f) f. Restriction of access to offline storage, backup data, systems, and media. (C3.9.0) Procedures exist to restrict physical access to the defined system including, but not limited to: facilities, backup media, and other system components such as firewalls, routers, and servers.		F.2.18, F.2.19,		FS-06			Domain 8	6.08. (a) 6.09. (j)	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 AC-17 (1) NIST SP 800-53 R3 AC-17 (2) NIST SP 800-53 R3 AC-17 (3) NIST SP 800-53 R3 AC-17 (4) NIST SP 800-53 R3 AC-17 (5) NIST SP 800-53 R3 AC-17 (7) NIST SP 800-53 R3 AC-17 (8) NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 PE-17		45 CFR 164.310 (c) 45 CFR 164.310 (d)(1) 45 CFR 164.310 (d)(2)(i)	A.9.2.5 A.9.2.6	Commandment #4 Commandment #5 Commandment #11		AC-17 MA-1 PE-1 PE-16 PE-17		9.8 9.9 9.10
Datacenter Security *Off-Site Equipment* **データセンタセキュリティ** *オフサイト機器*	DCS-05	Policies and procedures shall be established, and supporting business processes implemented, for the use and secure disposal of equipment maintained and used outside the organization's premise.	組織の構外で保管され使用される装置の利用と安全な処分のためのポリシー及び手順を確立し、これらを補強するための業務プロセスを実装しなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	D.1	D.1.1, D.2.1. D.2.2,		FS-07			Domain 8	6.05. (a) 6.05. (b) 6.05. (c)	NIST SP 800-53 R3 CM-8	NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 CM-8 (1) NIST SP 800-53 R3 CM-8 (3) NIST SP 800-53 R3 CM-8 (5) NIST SP 800-53 R3 SC-30		45 CFR 164.310 (d)(2)(iii)	A.7.1.1 A.7.1.2	Commandment #6 Commandment #7 Commandment #8		CM-8		9.9.1 12.3.3 12.3.4
Datacenter Security *Policy* **データセンタセキュリティ** *ポリシー*	DCS-06	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.	オフィス、部屋、施設、セキュリティエリア内での安全でセキュリティが確保された労働環境を維持するためのポリシー及び手順を確立し、これらを補強するための業務プロセスを実装しなければならない。	X										X	X	A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	H.6	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.4.2, F1.4.6, F.1.4.7, F.1.7, F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B)	FS-01			Domain 8	6.08. (a) 6.09. (i)	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-4 NIST SP 800-53 R3 PE-5 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-6 (1)	8.2.1 8.2.2 8.2.3	45 CFR 164.310(a)(1) 45 CFR 164.310(a)(2)(ii) 45 CFR 164.310(b) 45 CFR 164.310 (c) (New)	A.9.1.1 A.9.1.2	Commandment #1 Commandment #2 Commandment #3 Commandment #5	CIP-006-3c R1.2 - R1.3 - R1.4 - R2 - R2.2	PE-2 PE-3 PE-4 PE-5 PE-6		9.1
Datacenter Security - *Secure Area Authorization* **データセンタセキュリティ** *セキュアエリア認証*	DCS-07	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	許可された者だけが立入りできるようにするために、物理的な立入り制御の仕組みによってセキュリティエリアへの入退出を制限し監視しなければならない。	X	X	X	X	X	X		X	X	X	X		A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B)	FS-04	DS 12.3		Domain 8	6.08. (a) 6.09. (i)	NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-16	NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-7 (1) NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 PE-18	8.2.3		A.9.1.6	Commandment #1 Commandment #2 Commandment #3 Commandment #5	CIP-006-3c R1.2 - R1.3 - R1.4	PE-7 PE-16 PE-18		
Datacenter Security *Unauthorized Persons Entry* **データセンタセキュリティ** *許可されていない*	DCS-08	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	サービスエリアなどの出入口、及び許可されていない者が施設内に立ち入る可能性のある場所は、データの破壊、改ざん、紛失を避けるために、監視及び管理し、可能であれば、データの保管及び処理施設から離さなければならない。	X	X	X	X				X	X	X	X		A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	G.21	F.2.18		FS-05			Domain 8	6.08. (a) 6.09. (j)	NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 PE-16	NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-2 (1) NIST SP 800-53 R3 PE-16	8.2.5 8.2.6	45 CFR 164.310 (d)(1)	A.9.2.7 A.10.1.2	Commandment #6 Commandment #7		MA-1 MA-2 PE-16		9.8 9.9

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corporate Governance Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Tenant / Consumer	Scope Applicability: AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Datacenter Security *User Access* **データセンタセキュリティ** *ユーザアクセス*	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.	利用者及び支援スタッフによる情報資産及び情報処理機能への物理的アクセスを制限しなければならない。	X							X	X	X	X		A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B) 10 (B)	FS-02	DS 12.3		Domain 8	6.08. (a) 6.09. (i)	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-6 (1) NIST SP 800-53 R3 PE-18	8.2.3		A.9.1.1	Commandment #1 Commandment #2 Commandment #3 Commandment #5	CIP-006-3c R1.2 - R1.3 - R1.4 - R1.6 - R1.6.1 - R2 - R2.2	PE-2 PE-3 PE-6 PE-18		9.1
Encryption & Key Management *Entitlement* **暗号化と鍵管理** *権限付与*	EKM-01	All entitlement decisions shall be derived from the identities of the entities involved. These shall be managed in a corporate identity management system. Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	すべての権限付与の決定は、関与する組織による身分保証によって行われなければならない。これらは、企業のアイデンティティ管理システムで管理されなければならない。 鍵には識別可能な所有者が存在し（つまり鍵とアイデンティティが紐付いていること）、また（組織には）鍵管理ポリシーがなくてはならない。																															
Encryption & Key Management *Key Generation* **暗号化と鍵管理** *鍵作成*	EKM-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	サービスの暗号システムの暗号鍵を管理するためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない（鍵の生成から廃棄、更新に至るライフサイクルの管理、PKI、使用される暗号プロトコルの設計及びアルゴリズム、安全な鍵生成に適したアクセス制御、暗号化データ又はセッションに使用される鍵の隔離を含む交換及び保管など）。プロバイダは、要求に応じて、特に顧客（テナント）データがサービスの一部として利用されたり、顧客（テナント）が管理の実施に対する責任の一部を共有したりしている場合は、顧客（テナント）に暗号システム内の変更を通知しなければならない。		X		X	X	X	X	X	X	X	X		S3.6.0 S3.4	(S3.6.0) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks. (S3.4) Procedures exist to protect against unauthorized access to system resources.		L.6	38 (B) 39 (C+)	IS-19	DS5.8		Domain 2	6.04.04. (a) 6.04.04. (b) 6.04.04. (c) 6.04.04. (d) 6.04.04. (e) 6.04.05. (d) 6.04.05. (e) 6.04.08.02. (b)	NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13	NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-12 (2) NIST SP 800-53 R3 SC-12 (5) NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-13 (1) NIST SP 800-53 R3 SC-17	8.1.1 8.2.1 8.2.5	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312(e)(1)	Clause 4.3.3 A.10.7.3 A.12.3.2 A.15.1.6	Commandment #9 Commandment #10 Commandment #11		SC-12 SC-13 SC-17 SC-28		3.4.1 3.5 3.5.1 3.5.2 3.6 3.6.1 3.6.2 3.6.3 3.6.4 3.6.5 3.6.6 3.6.7 3.6.8
Encryption & Key Management *Sensitive Data Protection* **暗号化と鍵管理** *機微データの保護*	EKM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	該当する法的及び規制上の順守義務に従って、ストレージ（ファイルサーバ、データベース、エンドユーザのワークステーションなど）内の機微なデータ及び送信時（システムインタフェース、公的ネットワーク経由、電子メッセージ通信など）のデータ保護を目的として暗号プロトコルを使用するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。		X	X	X	X	X	X	X	X	X	X		C3.12.0 S3.6.0 S3.4	(C3.12.0, S3.6.0) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks. (S3.4) Procedures exist to protect against unauthorized access to system resources.	G.4 G.15 I.3	G.10.4, G.11.1, G.11.2, G.12.1, G.12.2, G.12.4, G.12.10, G.14.18, G.14.19, G.16.2, G.16.18, G.16.19, G.17.16, G.17.17, G.18.13, G.18.14, G.19.1.1, G.20.14	23 (B) 24 (B) 25 (B)	IS-18	DS5.8 DS5.10 DS5.11		Domain 2	6.04.05. (a) 6.04.05. (c)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-13	NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-18 (1) NIST SP 800-53 R3 AC-18 (2) NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1) NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1) NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-13 (1) NIST SP 800-53 R3 SC-23 NIST SP 800-53 R3 SC-28 NIST SP 800-53 R3 SI-8	8.1.1 8.2.1 8.2.5	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312 (e)(1) 45 CFR 164.312 (e)(2)(ii)	A.10.6.1 A.10.8.3 A.10.8.4 A.10.9.2 A.10.9.3 A.12.3.1 A.15.1.3 A.15.1.4	Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11	CIP-003-3 - R4.2	AC-18 IA-3 IA-7 SC-7 SC-8 SC-9 SC-13 SC-16 SC-23 SI-8		2.1.1 3.4 3.4.1 4.1 4.1.1 4.2
Encryption & Key Management *Storage and Access* **暗号化と鍵管理** *保管とアクセス*	EKM-04	Strong encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	オープンな検証済みの形式かつ標準アルゴリズムである強力な暗号化方式（AES - 256など）を使用しなければならない。鍵は（当該クラウドプロバイダの）クラウド内に保管するのではなく、クラウドの利用者又は信頼できる鍵管理プロバイダが保管しなければならない。鍵の管理と鍵の使用は、異なる責務として分離されなければならない。																			--			Domain 11										
Governance and Risk Management *Baseline Requirements* **ガバナンスとリスク管理** *ベースライン要求*	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.	開発済み又は購入済みで、組織が所有又は管理する実/仮想アプリケーション、インフラストラクチャーシステム及びネットワークコンポーネントのための基準となるセキュリティの要求事項を確立しなければならない。またそれらの要求事項は該当する法的及び規制上の順守義務に準拠していなければならない。標準的な設定から逸脱する場合は、導入、提供、使用の前に、変更管理ポリシー及び手順に従って承認を受けなければならない。セキュリティベースラインの要求事項への準拠は、その頻度がビジネス要求に基づいて確立され承認されない場合、少なくとも年1回は再評価されなければならない。	X	X	X	X	X	X	X	X	X	X	X		S1.1.0 S1.2.0(a-i)	(S1.1.0) The entity's security policies are established and periodically reviewed and approved by a designated individual or group. (S1.2.0(a-i)) The entity's security policies include, but may not be limited to, the following matters:	L.2	L.2, L.5, L.7 L.8, L.9, L.10	12 (B) 14 (B) 13 (B) 15 (B) 16 (C+, A+) 21 (B)	IS-04	AI2.1 AI2.2 AI3.3 DS2.3 DS11.6		Domain 2	6.03.01. (a) 6.03.04. (a) 6.03.04. (b) 6.03.04. (c) 6.03.04. (e) 6.07.01. (o)	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 SA-2 NIST SP 800-53 R3 SA-4	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 SA-2 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SC-30	1.2.6 8.2.1 8.2.7		A.12.1.1 A.15.2.2	Commandment #2 Commandment #4 Commandment #5 Commandment #11		CM-2 SA-2 SA-4		1.1 1.1.1 1.1.2 1.1.3 1.1.4 1.1.5 1.1.6 2.2 2.2.1 2.2.2 2.2.3 2.2.4

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corporate Governance Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Governance and Risk Management *Data Focus Risk Assessments* **ガバナンスとリスク管理** *データフォーカスリスクアセスメント*	GRM-02	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	データガバナンスの要求事項に関連するリスクアセスメントを事前に定められた間隔で実施し、その際に以下の事項を考慮しなければならない。 •機微のデータがどこで保管され、アプリケーション、データベース、サーバ、ネットワークインフラストラクチャー間で送受信されるかの認識 •定められた保持期間及び使用終了時の廃棄に関する要求事項への準拠 •データの分類並びに許可されていない使用、アクセス、紛失、破壊及び改ざんからの保護			X	X	X	X	X	X	X	X	X	X	S3.1.0 C3.14.0 S1.2.b-c	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies. (S1.2.b-c) b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction policies. c. Assessing risks on a periodic		L.4, L.5, L.6, L.7	34 (B)	DG-08	PO 9.1 PO 9.2 PO 9.4 DS 5.7		Domain 5	6.01. (d) 6.04.03. (a)	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SI-12	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SI-12	1.2.4 8.2.1	45 CFR 164.308(a)(1)(ii)(A) 45 CFR 164.308(a)(8)	Clause 4.2.1 c) & g) Clause 4.2.3 d) Clause 4.3.1 & 4.3.3 Clause 7.2 & 7.3 A.7.2 A.15.1.1 A.15.1.3 A.15.1.4	Commandment #1 Commandment #2 Commandment #3 Commandment #6 Commandment #7 Commandment #9 Commandment #10 Commandment #11			CA-3 RA-2 RA-3 MP-8 PM-9 SI-12		12.1 12.1.2
Governance and Risk Management *Management Oversight* **ガバナンスとリスク管理** *管理の監視*	GRM-03	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.	管理者は、自らの責任範囲に関わるセキュリティポリシー、手順及び標準を認識し、順守し続ける責任がある。							X	X	X	X	X	X	S1.2.f S2.3.0	(S1.2.f) f. Assigning responsibility and accountability for system availability, confidentiality, processing integrity and related security. (S2.3.0) Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	E.1	E.4	5 (B) 65 (B)	IS-14	DS5.3 DS5.4 DS5.5		Domain 3, 9		NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7	NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CA-7 (2)	1.1.2 8.2.1		Clause 5.2.2 A.8.2.1 A.8.2.2 A 11.2.4 A.15.2.1	Commandment #6 Commandment #7 Commandment #8			AT-2 AT-3 CA-1 CA-5 CA-6 CA-7 PM-10		12.6.1 12.6.2
Governance and Risk Management *Management Program* *ガバナンスとリスク管理* *管理プログラム*	GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	資産及びデータを紛失、誤用、許可されていないアクセス、開示、改変、破壊から保護するために、管理的、技術的、物理的保護措置を含む情報セキュリティマネジメントプログラム(ISMP)を開発し、文書化し、承認し、実装しなければならない。セキュリティプログラムは、事業の特性に関わる範囲では、少なくても以下の分野を含めなければならない。 ・リスク管理 ・セキュリティポリシー ・情報セキュリティの組織 ・資産管理 ・人的セキュリティ ・物理的及び環境的セキュリティ ・連絡及び運用管理 ・アクセス制御 ・情報システムの取得、開発及び保守	X	X	X	X	X	X	X	X	X	X	X	x1.2.	(x1.2.) The entity's system [availability, processing integrity, confidentiality and related] security policies include, but may not be limited to, the following matters:		A.1, B.1	2 (B) 3 (B) 5 (B)	IS-01	R2 DS5.2 R2 DS5.5		Domain 2				8.2.1	45 CFR 164.308(a)(1)(i) 45 CFR 164.308(a)(1)(ii)(B) 45 CFR 164.316(b)(1)(i) 45 CFR 164.308(a)(3)(i) (New) 45 CFR 164.306(a) (New)	Clause 4.2 Clause 5 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8	Commandment #1 Commandment #2	CIP-001-1a - R1 - R2 CIP-003-3 - R1 - R1.1 - R4 CIP-006-3c R1	PM-1 PM-2 PM-3 PM-4 PM-5 PM-6 PM-7 PM-8 PM-9 PM-10 PM-11		12.1 12.2
Governance and Risk Management *Management Support/Involvement* *ガバナンスとリスク管理* *補強 / 関与*	GRM-05	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	経営陣及び管理職は、文書による明確な指示及びコミットメントを通じて情報セキュリティを担保するための業務指示を発し、指示が実施されたことを確認しなければならない。							X	X	X	X	X		S1.3.0	(S1.3.0) Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned. The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users The security obligations of users and the entity's security commitments to users are communicated to authorized users.		C.1	5 (B)	IS-02	DS5.1		Domain 2		NIST SP 800-53 R3 CM-1	NIST SP 800-53 R3 CM-1	8.2.1	45 CFR 164.316 (b)(2)(ii) 45 CFR 164.316 (b)(2)(iii)	Clause 5 A.6.1.1	Commandment #3 Commandment #6	CIP-003-3 - R1 - R1.1	CM-1 PM-1 PM-11		12.5
Governance and Risk Management *Policy* **ガバナンスとリスク管理** *ポリシー*	GRM-06	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	情報セキュリティのポリシー及び手順を確立し、影響を受けるすべての人員及び外部の取引関係者がいつでもレビューできるよう準備しておかなければならない。情報セキュリティのポリシーは、組織の事業責任者（又はその他のビジネス責任者若しくはビジネス責任部門）によって承認され、事業責任者のための情報セキュリティにおける役割及び責任を明示した戦略的事業計画及び情報セキュリティマネジメントプログラムによって担保されなければならない。							X	X	X	X	X	X	S1.1.0 S1.3.0 S2.3.0	(S1.1.0) The entity's security policies are established and periodically reviewed and approved by a designated individual or group. (S1.3.0) Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned. (S2.3.0) Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.		B.1		IS-03	DS5.2		Domain 2	6.02. (e)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	8.1.0 8.1.1	45 CFR 164.316 (a) 45 CFR 164.316 (b)(1)(i) 45 CFR 164.316 (b)(2)(ii) 45 CFR 164.308(a)(2)	Clause 4.2.1 Clause 5 A.5.1.1 A.8.2.2	Commandment #1 Commandment #2 Commandment #3	CIP-003-3 - R1 - R1.1 - R1.2 - R2 - R2.1 - R2.2 - R2.3	AC-1 AT-1 AU-1 CA-1 CM-1 IA-1 IR-1 MA-1 MP-1 MP-1 PE-1 PL-1 PS-1 SA-1 SC-1 SI-1		12.1 12.2

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance						Corporate Governance Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																		
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Governance and Risk Management *Policy Enforcement* **ガバナンスとリスク管理** *ポリシー強化*	GRM-07	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	セキュリティポリシー及び手順に違反した従業員に対する正式な懲罰あるいは制裁のポリシーを確立しなければならない。違反した場合に講じられる措置を従業員に認識させなければならない。また、ポリシー及び手順で懲戒手続きを規定しなければならない。							X	X	X	X	X	X	S3.9 S2.4.0	(S3.9) Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis. (S2.4.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users.		B.1.5		IS-06	PO 7.7		Domain 2		NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-8	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-8	10.2.4	45 CFR 164.308 (a)(1)(ii)(C)	A.8.2.3	Commandment #6 Commandment #7		PL-4 PS-1 PS-8		
Governance and Risk Management *Policy Impact on Risk Assessments* **ガバナンスとリスク管理** *リスクアセスメントにおけるポリシーインパクト*	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	リスクアセスメントの結果には、その妥当性と有効性を維持するために、セキュリティポリシー、手順、標準及び管理策の更新を含めなければならない。	X	X	X	X	X	X	X	X	X	X	X	X			B.2 G.21 L.2	B.1.1, B.1.2, B.1.6, B.1.7.2, G.2, L.9, L.10		RI-04	PO 9.6		Domian 2, 4	6.03. (a)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1			Clause 4.2.3 Clause 4.2.4 Clause 4.3.1 Clause 5 Clause 7 A.5.1.2 A.10.1.2 A.10.2.3 A.14.1.2 A.15.2.1 A.15.2.2		CIP-009-3 - R2	CP-2 RA-2 RA-3		12.1.3
Governance and Risk Management *Policy Reviews* **ガバナンスとリスク管理** *ポリシーレビュー*	GRM-09	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	情報セキュリティポリシーとセキュリティ戦略との継続的な合致、情報セキュリティポリシーの有効性、正確性、妥当性、及び法的又は規制上の順守義務への適用性を確認するために、組織の事業責任者（又はその他の事業責任者若しくは事業責任部門）は、事前に定められた間隔または組織変更に対応して情報セキュリティポリシーをレビューしなければならない。							X	X	X	X	X	X	S1.1.0	(S1.1.0) The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	B.2	B.1.33. B.1.34,		IS-05	DS 5.2 DS 5.4		Domain 2		NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-5 (2) NIST SP 800-53 R3 IA-5 (3) NIST SP 800-53 R3 IA-5 (6) NIST SP 800-53 R3 IA-5 (7) NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	1.2.1 8.2.7 10.2.3	45 CFR 164.316 (b)(2)(iii) 45 CFE 164.306 €	Clause 4.2.3 f) A.5.1.2	Commandment #1 Commandment #2 Commandment #3	CIP-003-3 - R3.2 - R3.3 - R1.3 R3 - R3.1 - R3.2 - R3.3	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-5 IR-1 MA-1 MP-1 PE-1 PL-1 PM-1 PS-1 RA-1 SA-1 SC-1 SI-1		12.1.3
Governance and Risk Management *Risk Assessments* **ガバナンスとリスク管理** *リスクアセスメント*	GRM-10	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	定性的手法又は定量的手法を使用して、特定されたすべてのリスクの発生可能性及び影響度を判断するために、企業の組織構造に適合した正式なリスクアセスメントを、少なくとも年1回又は事前に定められた間隔で実施しなければならない。固有リスク及び残存リスクに関連する発生可能性及び影響度は、すべてのリスクカテゴリ（たとえば、監査結果、脅威分析及び脆弱性診断、規制の順守など）を考慮し、独立して判断されなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S3.1 x3.1.0 S4.3.0	(S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system [availability, processing integrity, confidenitality] commitments and (2) assess the risks associated with the identified threats. (S4.3.0) Environmental, regulatory, and technological changes are monitored, and their effect on system availability, confidentiality of data, processing integrity, and system security is assessed on a timely basis; policies are updated for that assessment.	I.1 I.4	C.2.1, I.4.1, I.5, G.15.1.3, I.3	46 (B) 74 (B)	RI-02	PO 9.4		Domain 2, 4	6.03. (a) 6.08. (a)	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3	NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SC-30	1.2.4 1.2.5	45 CFR 164.308 (a)(1)(ii)(A)	Clause 4.2.1 c) through g) Clause 4.2.3 d) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.14.1.2 A.15.1.1 A.15.2.1 A.15.2.2		CIP-002-3 - R1.1 - R1.2 CIP-005-3a - R1 - R1.2 CIP-009-3 - R.1.1	PL-5 RA-2 RA-3		12.1.2
Governance and Risk Management *Risk Management Framework* **ガバナンスとリスク管理** *リスク管理フレームワーク*	GRM-11	Organizations shall develop and maintain an enterprise risk management framework to mitigate risk to an acceptable level.	組織は、リスクを受容可能なレベルにまで軽減するために、事業のリスク管理の枠組みを開発し維持しなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S3.1 x3.1.0	(S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system [availability, processing integrity, confidenitality] commitments and (2) assess the risks associated with the identified threats.	L.2	A.1, L.1		RI-01	PO 9.1		Domain 2, 4		NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SA-9 (1) NIST SP 800-53 R3 SC-30 NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 CM-1	1.2.4	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(B)	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.6.1 A.14.1.2 A.15.2.1 A.15.2.2		CIP-009-3 - R4	AC-4 CA-2 CA-6 PM-9 RA-1		12.1.2

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corporate Governance Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Governance and Risk Management *Risk Mitigation / Acceptance* *ガバナンスとリスク管理* *リスク軽減 / 受容*	GRM-12	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval.	リスクを受容可能なレベルにまで軽減しなければならない。リスク基準に基づく受容可能なレベルは、妥当な対策所要時間及び経営陣の承認に基づいて設定され文書化されなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S3.1 x3.1.0	(S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system [availability, processing integrity, confidenitality] commitments and (2) assess the risks associated with the identified threats.	I.4 L.2	I.3, L.9, L.10	43 (C+, A+)	RI-03	PO 9.5		Domain 2, 4		NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 RA-1	NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 RA-1		45 CFR 164.308 (a)(1)(ii)(B)	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 4.3.1 Clause 5.1 f) Clause 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.15.1.1 A.15.2.1 A.15.2.2		CIP-009-3 - R1.2	CA-5 CM-4		
Human Resources *Asset Returns* *人事* *資産返還*		Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	従業員の退職時あるいは外部との取引関係の終了時には、組織が所有するすべての資産を定められた期間内に返却しなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	D.1	E.6.4		IS-27			Domain 2		NIST SP 800-53 R3 PS-4	NIST SP 800-53 R3 PS-4	5.2.3 7.2.2 8.2.1 8.2.6	45 CFR 164.308 (a)(3)(ii)(C)	A.7.1.1 A.7.1.2 A.8.3.2			PS-4		
Human Resources *Background Screening* *人事* *経歴スクリーニング*	HRS-02	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	現地の法律、規制、倫理及び契約上の制約に従って、すべての採用予定者、契約者及び第三者の経歴を確認しなければならない。この確認は、アクセスされるデータの分類、業務の要求事項及び受容可能なリスクに応じて行わなければならない。						X	X	X	X	X	X	X	S3.11.0	(S3.11.0) Procedures exist to help ensure that personnel responsible for the design, development, implementation, and operation of systems affecting confidentiality and security have the qualifications and resources to fulfill their responsibilities.	E.2	E.2	63 (B)	HR-01	PO 7.6		None	6.01. (a)	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-3	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-3	1.2.9		A.8.1.2	Commandment #2 Commandment #3 Commandment #6 Commandment #9	CIP-004-3 - R2.2	PS-2 PS-3		12.7 12.8.3
Human Resources *Employment Agreements* *人事* *雇用契約*	HRS-03	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	雇用契約書には、確立された情報ガバナンス及びセキュリティポリシーの順守に関する規定および条件を取り入れなければならない。また、新規採用された従業員（フルタイム又はパートタイム従業員、臨時従業員など）に企業の施設、資源、資産へのアクセスを許可する前に、雇用契約書に署名させなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S2.2.0	(S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users	C.1	E.3.5	66 (B)	HR-02	DS 2.1		None		NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	1.2.9 8.2.6	45 CFR 164.310(a)(1) 45 CFR 164.308(a)(4)(i)	A.6.1.5 A.8.1.3	Commandment #6 Commandment #7		PL-4 PS-6 PS-7		12.4 12.8.2
Human Resources *Employment Termination* *人事* *雇用の終了*	HRS-04	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	雇用の終了もしくは雇用手続きの変更に関する役割及び責任は、明確に割り当てられ、文書化され、通知されなければならない。							X	X	X	X	X	X	S3.2.d S3.8.e	(S3.2.d) Procedures exist to restrict logical access to the system and information resources maintained in the system including, but not limited to, the following matters: d. The process to make changes and updates to user profiles (S3.8.e) e. Procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own		E.6		HR-03	PO 7.8		None		NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-8	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-8	8.2.2 10.2.5	45 CFR 164.308 (a)(3)(ii)(C)	A.8.3.1	Commandment #6 Commandment #7		PS-4 PS-5		
Human Resources *Industry Knowledge / Benchmarking* *人事* *業界知識 / ベンチマーキング*	HRS-05	Industry security knowledge and benchmarking through networking, specialist security forums, and professional associations shall be maintained.	ネットワーク、専門家によるセキュリティフォーラム、専門団体を通じて、セキュリティに関する業界の知識及びベンチマーキングを維持しなければならない。							X	X	X	X	X	X	S4.3.0	(S4.3.0) Environmental, regulatory, and technological changes are monitored, and their effect on system availability, confidentiality, processing integrity and security is assessed on a timely basis; policies are updated for that assessment.		C.1.8	64 (B)	IS-12			Domain 2		NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 SI-5			A.6.1.7	Commandment #1 Commandment #2 Commandment #3		AT-5 SI-5		
Human Resources *Mobile Device Management* *人事* *モバイルデバイス管理*	HRS-06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。また、より高い保証となる補完統制、実行可能なポリシー及び手順（セキュリティ訓練の義務付け、身元確認の強化、権限付与とアクセス制御、デバイス監視など）の実施が必要な場合もある。	X	X	X	X	X	X	X	X	X	X	X	X	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.		G.11, G12, G.20.13, G.20.14		IS-32	DS5.11 DS5.5		Domain 2		NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-19 NIST SP 800-53 R3 MP-2 NIST SP 800-53 R3 MP-6	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 AC-17 (1) NIST SP 800-53 R3 AC-17 (2) NIST SP 800-53 R3 AC-17 (3) NIST SP 800-53 R3 AC-17 (4) NIST SP 800-53 R3 AC-17 (5) NIST SP 800-53 R3 AC-17 (7) NIST SP 800-53 R3 AC-17 (8) NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-18 (1) NIST SP 800-53 R3 AC-18 (2) NIST SP 800-53 R3 AC-19 NIST SP 800-53 R3 AC-19 (1) NIST SP 800-53 R3 AC-19 (2) NIST SP 800-53 R3 AC-19 (3) NIST SP 800-53 R3 MP-2 NIST SP 800-53 R3 MP-2 (1) NIST SP 800-53 R3 MP-4 NIST SP 800-53 R3 MP-4 (1) NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 MP-6 (4)	1.2.6 3.2.4 8.2.6	45 CFR 164.310 (d)(1)	A.7.2.1 A.10.7.1 A.10.7.2 A.10.8.3 A.11.7.1 A.11.7.2 A.15.1.4	All	CIP-007-3 - R7.1	AC-17 AC-18 AC-19 MP-2 MP-4 MP-6		9.7 9.7.2 9.8 9.9 11.1 12.3

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corporate Governance Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Human Resources *Non-Disclosure Agreements* **人事** *守秘義務契約*	HRS-07	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	データ及び運用の詳細事項を保護するための組織のニーズに合わせて、守秘義務契約もしくは秘密保持契約に関する要求事項を特定し、文書化し、事前に定めた間隔でレビューしなければならない。						X	X	X	X	X	X	X	S4.1.0	(S4.1.0) The entity's system availability, confidentiality, processing integrity and security performance is periodically reviewed and compared with the defined system availability and related security policies.		C.2.5		LG-01			Domain 3		NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1)	1.2.5		ISO/IEC 27001:2005 Annex A.6.1.5	Commandment #6 Commandment #7 Commandment #8 Commandment #9		PL-4 PS-6 SA-9		12.8.2 12.8.3 12.8.4
Human Resources *Roles / Responsibilities* **人事** *ロール / 責任*	HRS-08	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	契約社員、従業員及び外部の利用者が情報資産及びセキュリティに関連している場合、その役割及び責任を文書化しなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S1.2.f	(S1.2.f) f. Assigning responsibility and accountability for system availability, confidentiality, processing integrity and related security.	B.1	B.1.5, D.1.1,D.1.3.3, E.1, F.1.1, H.1.1, K.1.2	5 (B)	IS-13	DS5.1		Domain 2		NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	1.2.9 8.2.1		Clause 5.1 c) A.6.1.2 A.6.1.3 A.8.1.1	Commandment #6 Commandment #7 Commandment #8		AT-3 PL-4 PM-10 PS-1 PS-6 PS-7		
Human Resources *Technology Acceptable Use* **人事** *技術的に受け入れられる使用*	HRS-09	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	組織が所有又は管理するユーザのエンドポイントデバイス（支給されたワークステーション、ラップトップ、モバイルデバイスなど）、IT基盤のネットワーク及びシステムコンポーネントの使用を許可する条件を定義するためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。さらに、必要に応じて、個人のモバイルデバイス及び関連するアプリケーションを使用して企業の資源にアクセスすること（すなわち、BYOD）を許可する条件を定義することも考慮し、適宜取り入れなければならない。					X	X	X	X	X	X	X	X	S1.2 S3.9	(S1.2) The entity's security policies include, but may not be limited to, the following matters: (S3.9) Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.	B.3	B.1.7, D.1.3.3, E.3.2, E.3.5.1, E.3.5.2		IS-26	DS 5.3		Domain 2		NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-8 NIST SP 800-53 R3 AC-20 NIST SP 800-53 R3 PL-4	NIST SP 800-53 R3 AC-8 NIST SP 800-53 R3 AC-20 NIST SP 800-53 R3 AC-20 (1) NIST SP 800-53 R3 AC-20 (2) NIST SP 800-53 R3 PL-4	8.1.0	45 CFR 164.310 (b)	A.7.1.3	Commandment #1 Commandment #2 Commandment #3		AC-8 AC-20 PL-4		12.3.5
Human Resources *Training / Awareness* **人事** *トレーニング / 認識向上*	HRS-10	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	組織のすべての契約社員、外部の利用者、従業員に対してセキュリティ意識向上の訓練プログラムを策定し、必要に応じて義務付けなければならない。組織のデータにアクセスするすべての個人は、組織に関係する職務に関連する組織の手順、プロセス、ポリシーについての定期的に意識の向上および知識の更新を目的とした訓練を受けなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S1.2.k S2.2.0	(S1.2.k) The entity's security policies include, but may not be limited to, the following matters: k. Providing for training and other resources to support its system security policies (S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users.	E.1	E.4	65 (B)	IS-11	PO 7.4		Domain 2	6.01. (c) 6.02. (e)	NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4	NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4	1.2.10 8.2.1	45 CFR 164.308 (a)(5)(i) 45 CFR 164.308 (a)(5)(ii)(A)	Clause 5.2.2 A.8.2.2	Commandment #3 Commandment #6	CIP-004-3 - R1 - R2 - R2.1	AT-1 AT-2 AT-3 AT-4		12.6 12.6.1 12.6.2
Human Resources *User Responsibility* **人事** *ユーザ責任*	HRS-11	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	すべての人員に、以下の事項に対する自身の役割及び責任を認識させなければならない。 •設定されたポリシー、手順、適用される法律上又は規則上の遵守義務に対する認識及びコンプライアンスを維持すること •安全でセキュアな作業環境を維持すること	X	X	X	X	X	X	X	X	X	X	X	X	S2.3.0	(S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality, processing integrity and security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	E.1	E.4	65 (B) 66 (B)	IS-16	PO 4.6		Domain 2		NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 PL-4	NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 PL-4	1.2.10 8.2.1	45 CFR 164.308 (a)(5)(ii)(D)	Clause 5.2.2 A.8.2.2 A.11.3.1 A.11.3.2	Commandment #5 Commandment #6 Commandment #7		AT-2 AT-3 AT-4 PL-4		8.5.7 12.6.1
Human Resources *Workspace* **人事** *ワークスペース*	HRS-12	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	無人の作業場所で、機微な文書が（デスクトップ上などで）閲覧されないようにするため、また、一定時間使用されない場合にユーザのセッションが無効になるようにするために、ポリシー及び手順を確立しなければならない	X					X	X	X	X	X	X	X	S3.3.0 S3.4.0	(S3.3.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. (S3.4.0) Procedures exist to protect against unauthorized access to system resources.	E.1	E.4		IS-17			Domain 2		NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-2	NIST SP 800-53 R3 AC-11 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-2 NIST SP 800-53 R3 MP-2 (1) NIST SP 800-53 R3 MP-3 NIST SP 800-53 R3 MP-4 NIST SP 800-53 R3 MP-4 (1)	8.2.3		Clause 5.2.2 A.8.2.2 A.9.1.5 A.11.3.1 A.11.3.2 A.11.3.3	Commandment #5 Commandment #6 Commandment #7 Commandment #11		AC-11 MP-2 MP-3 MP-4		
Identity & Access Management *Audit Tools Access* **アイデンティティとアクセス管理** *監査ツールアクセス*	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	ログデータが改ざんされたり悪用されたりすることのないように、組織の情報システムとやり取りをする監査ツールへのアクセス及び使用については適切な分類や取扱い制限を行わなければならない	X	X	X	X	X	X		X	X	X	X		S3.2.g	*(S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).*				IS-29	DS 5.7		Domain 2	6.03. (i) 6.03. (j)	NIST SP 800-53 R3 AU-9	NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-9 (2)	8.2.1		A.15.3.2	Commandment #2 Commandment #5 Commandment #11	CIP-003-3 - R5.2	AU-9 AU-11 AU-14		10.5.5
Identity & Access Management *Credential Lifecycle / Provision Management* **アイデンティティとアクセス管理** *資格証明のライフサイクル / プロビジョニング管理*	IAM-02	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO	データや組織が所有又は管理する実/仮想アプリケーションインタフェース、IT基盤のネットワーク及びシステムコンポーネントにアクセスするすべての社内及び顧客（テナント）ユーザの適切な身元確認、権限付与、アクセス管理を確実に行うために、ユーザアクセスのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。これらのポリシー、手順、プロセス及び手段には、以下の事項を含めなければならない。 ・ユーザアカウントの権限付与及び解除を行うための手順並びにその基準となる職責及び責任を職務機能（社内従業員及び臨時従業員の変更、顧客管理によるアクセス、仕入れ先との取引関係、その他の第三者との取引関係など）に基づき最少権限付与原則に沿って定めること ・ビジネスケースを考慮した、より高度の保証及び複数要素認証用秘密情報の配備（たとえば、管理インタフェース、鍵生成の機能、リモートアクセスなどを利用する場合、職務権限分離の確実な実施、緊急アクセスを行う場合、大規模なリソースを必要とするプロビジニングや地理的に分散した配備を行うような場合、重要なシステムへの人員の冗長配置の場合など） ・マルチテナントアーキテクチャにおける、それぞれのサードパーティー（プロバイダや他のテナントなど）ごとの、データ及びセッションに対するアクセスの隔離に関する事項 ・IDの信用性確認、サービス間連携アプリケーション（API）と情報処理の相互運用性（たとえばSSOと認証フェデレーションなどについてのもの）に関する事項 ・インスタンス化から破棄に至るまでのアカウント資格情	X	X	X	X	X	X	X	X	X	X	X		S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	B.1	B.1.8, B.1.21, B.1.28, E.6.2, H.1.1, K.1.4.5,	8 (B) 40 (B) 41 (B) 42 (B) 43 (B) 44 (C+)	IS-07	DS 5.4		Domain 2	6.01. (b) 6.01. (d) 6.02. (e) 6.03. (b) 6.03.04. (b) 6.03.04. (c) 6.03.05. (b) 6.03.05. (d) 6.03.06. (b) 6.04.01. (c) 6.04.01. (f) 6.04.02. (a) 6.04.02. (b) 6.04.02. (c) 6.04.03. (b) 6.04.06. (a) 6.04.08. (a) 6.04.08. (b) 6.04.08. (c) 6.04.08.03. (a) 6.04.08.03. (b)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-7 NIST SP 800-53 R3 AC-14 NIST SP 800-53 R3 IA-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-7 NIST SP 800-53 R3 AC-10 NIST SP 800-53 R3 AC-14 NIST SP 800-53 R3 IA-1	8.1.0	45 CFR 164.308 (a)(3)(i) 45 CFR 164.312 (a)(1) 45 CFR 164.312 (a)(2)(ii) 45 CFR 164.308(a)(4)(ii)(B) 45 CFR 164.308(a)(4)(ii)(c)	A.11.1.1 A.11.2.1 A.11.2.4 A.11.4.1 A.11.5.2 A.11.6.1	Commandment #6 Commandment #7 Commandment #8	CIP-007-3 - R5.1 - R5.1.2	AC-1 IA-1		3.5.1 8.5.1 12.5.4

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance						Corporate Governance Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																		
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
		• Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	・データ及びセッションへのアクセスのための認証、許可、アカウンティング（AAA）ルールに関する事項（たとえば暗号化、強力かつマルチファクターの期限付き非共有の認証シークレットを使用するといった規則） ・データ及びセッションへのアクセスのための認証、許可、アカウンティング（AAA）ルールを、顧客（テナント）自身が管理するための許可範囲及び提供する補助機能に関する事項 ・該当する法律又は規制順守の要求事項への準拠に関する事項																																
Identity & Access Management *Diagnostic / Configuration Ports Access* **アイデンティティとアクセス管理** *診断 / 構成ポートアクセス*	IAM-03	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	診断ポート及び構成ポートへのユーザアクセスはその権限を付与された担当者又はアプリケーションに限定しなければならない。	X				X			X	X	X	X	X	S3.2.g	*(S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).*		H1.1, H1.2, G.9.15		IS-30	DS5.7		Domain 2		NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-5	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1) NIST SP 800-53 R3 MA-3 NIST SP 800-53 R3 MA-3 (1) NIST SP 800-53 R3 MA-3 (2) NIST SP 800-53 R3 MA-3 (3) NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-4 (1) NIST SP 800-53 R3 MA-4 (2) NIST SP 800-53 R3 MA-5			A.10.6.1 A.11.1.1 A.11.4.4 A.11.5.4	Commandment #3 Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8	CIP-007-3 - R2	CM-7 MA-3 MA-4 MA-5		9.1.2
Identity & Access Management *Policies and Procedures* **アイデンティティとアクセス管理** *ポリシーと手続き*	IAM-04	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	ITインフラストラクチャーにアクセスするすべての人に関するID情報を保管し管理し、個人のアクセスレベルを決定するためのポリシー及び手順を確立しなければならない。ユーザのIDに基づいてネットワーク資源へのアクセスを制御するためのポリシーも確立しなければならない。																		--			Domain 12												
Identity & Access Management *Segregation of Duties* **アイデンティティとアクセス管理** *職務の分離*	IAM-05	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	ユーザロールの競合に関連する事業リスクに対処することを目的として規定された職務分離方針に応じてユーザアクセスを制限するために、ユーザアクセスポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。	X	X	X	X	X	X	X	X	X	X	X		S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.		G.2.13. G.3, G.20.1, G.20.2, G.20.5		IS-15	DS 5.4		Domain 2	6.04.01. (d) 6.04.08.02. (a)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-6	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-2 (1) NIST SP 800-53 R3 AC-2 (2) NIST SP 800-53 R3 AC-2 (3) NIST SP 800-53 R3 AC-2 (4) NIST SP 800-53 R3 AC-2 (7) NIST SP 800-53 R3 AC-5 NIST SP 800-53 R3 AC-6 NIST SP 800-53 R3 AC-6 (1) NIST SP 800-53 R3 AC-6 (2) NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-6 (1) NIST SP 800-53 R3 AU-6 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6)	8.2.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308(a)(4)(ii)(A) 45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.3	Commandment #6 Commandment #7 Commandment #8 Commandment #10	CIP-007-3 R5.1.1	AC-1 AC-2 AC-5 AC-6 AU-1 AU-6 SI-1 SI-4		6.4.2
Identity & Access Management *Source Code Access Restriction* **アイデンティティとアクセス管理** *ソースコードアクセス制限*	IAM-06	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	定められたユーザアクセスのポリシー及び手順に基づいて、職務に応じた最小権限付与原則に従い、組織自身が開発したアプリケーション、プログラム、オブジェクトソースコード、その他の知的財産（IP）へのアクセス及び自社開発のソフトウェアの使用を適切に制限しなければならない。			X	X	X	X		X	X	X	X		S3.13.0	(S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.		I.2.7.2, I.2.9, I.2.10, I.2.15		IS-33			Domain 2			NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-5 (1) NIST SP 800-53 R3 CM-5 (5)	1.2.6 6.2.1		Clause 4.3.3 A.12.4.3 A.15.1.3	Commandment #6 Commandment #7 Commandment #9 Commandment #10		CM-5 CM-6		6.4.1 6.4.2
Identity & Access Management *Third Party Access* **アイデンティティとアクセス管理** *第三者アクセス*	IAM-07	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	組織の情報システム及びデータへの第三者のアクセスを必要とする業務プロセスで発生するリスクを特定、評価、優先順位付けした後、権限のない又は不適切なアクセスの発生可能性及び影響度を最小限に抑え、監視し、測定するために、それに対応できるリソースを投入しなければならない。 リスク分析に基づく管理策の手直しは（第三者に）アクセスを提供する前に実装されなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S3.1 x3.1.0	(S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system [availability, processing integrity, confidentiality] commitments and (2) assess the risks associated with the identified threats.	B.1 H.2	B.1.1, B.1.2, D.1.1, E.1, F.1.1, H.1.1, K.1.1, E.6.2, E.6.3		RI-05	DS 2.3		Domain 2, 4	6.02. (a) 6.02. (b) 6.03. (a)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-5 (2) NIST SP 800-53 R3 IA-5 (3) NIST SP 800-53 R3 IA-5 (6) NIST SP 800-53 R3 IA-5 (7) NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1	7.1.1 7.1.2 7.2.1 7.2.2 7.2.3 7.2.4		A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.4			CA-3 MA-4 RA-3		12.8.1 12.8.2 12.8.3 12.8.4

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance					Corp Gov Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																	
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Consumer / Tenant	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Identity & Access Management *Trusted Sources* **アイデンティティとアクセス管理** *信頼された発行元*	IAM-08	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	業務上必要であると明確に指定されたユーザにのみ適用される複製制限及び最小権限のルールに基づいて、本人のみがアクセスできるようにするために、認証に使用されるIDの保管及びアクセスを許可するためのポリシー及び手順を確立しなければならない。													S3.2.0 S4.3.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls). (S4.3.0) Environmental, regulatory, and technological changes are monitored, and their effect on system availability, confidentiality, processing integrity and security is assessed on a timely basis; policies are updated for that assessment.				IS-08 IS-12			Domain 12													
Identity & Access Management *User Access Authorization* **アイデンティティとアクセス管理** *ユーザアクセス権限*	IAM-09	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	データや組織が所有又は管理する実/仮想アプリケーション、基幹システム、ネットワークコンポーネントへのユーザアクセス(従業員、契約社員、顧客(テナント)、事業パートナー、供給者関係など)の提供は、事前に組織の管理者によって、それが、定められたポリシーや手順に従って、許可され、また適切に制限されているかについて承認を受けていなければならない。 プロバイダは、要求に応じて、特に顧客(テナント)のデータがサービスの一部として利用されたり、顧客(テナント)が管理策の実装に対する責任の一部を共有したりしている場合は、このユーザアクセス提供を顧客(テナント)に通知しなければならない。		X	X	X	X	X		X	X	X	X	X	S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).		H.2.4, H.2.5,	35 (B) 40 (B) 41 (B) 42 (B) 44 (C+)	IS-08	DS5.4		Domain 2	6.03.04. (b) 6.03.04. (c) 6.03.05. (d) 6.03.06. (a) 6.03.06. (b) 6.04.01. (a) 6.04.01. (b) 6.04.01. (d) 6.04.01. (e) 6.04.01. (g) 6.04.03. (c) 6.04.08.02. (a)	NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 MA-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-7	NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 AC-3 (3) NIST SP 800-53 R3 AC-5 NIST SP 800-53 R3 AC-6 NIST SP 800-53 R3 AC-6 (1) NIST SP 800-53 R3 AC-6 (2) NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-2 (2) NIST SP 800-53 R3 IA-2 (3) NIST SP 800-53 R3 IA-2 (8) NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-4 (4) NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-5 (2) NIST SP 800-53 R3 IA-5 (3) NIST SP 800-53 R3 IA-5 (6) NIST SP 800-53 R3 IA-5 (7) NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 MA-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SC-30 NIST SP 800-53 R3 SI-9	8.2.2	45 CFR 164.308 (a)(3)(i) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308 (a)(4)(i) 45 CFR 164.308 (a)(4)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C) 45 CFR 164.312 (a)(1)	A.11.2.1 A.11.2.2 A.11.4.1 A.11.4.2 A.11.6.1	Command #6 Command #7 Command #8 Command #9 Command #10	CIP-003-3 - R5.1.1 - R5.3 CIP-004-3 R2.3 CIP-007-3 R5.1 - R5.1.2	AC-3 AC-5 AC-6 IA-2 IA-4 IA-5 IA-8 MA-5 PS-6 SA-7 SI-9		7.1 7.1.1 7.1.2 7.1.3 7.2.1 7.2.2 8.5.1 12.5.4
Identity & Access Management *User Access Reviews* **アイデンティティとアクセス管理** *ユーザアクセスレビュー*	IAM-10	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	ユーザアクセスは、その権限付与の妥当性について、組織の事業責任者、もしくは、責任ある立場の役割または機能をもつ者に対し、組織が職務ごとの最小権限原則に従っていることを表す証拠を提示することにより、定期的に再評価し承認を受けなければならない。 アクセス違反が特定された場合、定められたユーザアクセスのポリシー及び手順に従って改善措置を実施しなければならない。	X	X	X	X	X	X		X	X	X	X	X	S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).		H.2.6, H.2.7, H.2.9,	41 (B)	IS-10	DS5.3 DS5.4		Domain 2		NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-2 (1) NIST SP 800-53 R3 AC-2 (2) NIST SP 800-53 R3 AC-2 (3) NIST SP 800-53 R3 AC-2 (4) NIST SP 800-53 R3 AC-2 (7) NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-6 (1) NIST SP 800-53 R3 AU-6 (3) NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7	8.2.1 8.2.7	45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C)	A.11.2.4	Command #6 Command #7 Command #8 Command #10	CIP-004-3 R2.2.2 CIP-007-3 - R5 - R.1.3	AC-2 AU-6 PM-10 PS-6 PS-7		
Identity & Access Management *User Access Revocation* **アイデンティティとアクセス管理** *ユーザアクセス取り消し*	IAM-11	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	定められたポリシー及び手順に従いユーザのステータスの変更(雇用又はその他の取引関係の終了、職務の変更又は転任など)に基づいて、データや組織が所有又は管理する実/仮想アプリケーション、インフラストラクチャーシステム、ネットワークコンポーネントへのユーザアクセスを適時に取消し又は変更しなければならない。ブロバイダは、要求に応じて、特に顧客(テナント)データがサービスの一部として利用されたり、顧客(テナント)が管理の実施に対する責任の一部を共有したりしている場合は、これらの変更を顧客(テナント)に通知しなければならない。	X	X	X	X	X	X		X	X	X	X		S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	H.2	E.6.2, E.6.3		IS-09	DS 5.4		Domain 2	6.03.04. (b) 6.03.04. (c) 6.03.05. (d) 6.03.06. (a) 6.04.02. (b)	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-2 (1) NIST SP 800-53 R3 AC-2 (2) NIST SP 800-53 R3 AC-2 (3) NIST SP 800-53 R3 AC-2 (4) NIST SP 800-53 R3 AC-2 (7) NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5 NIST SP 800-53 R3 SC-30	8.2.1	45 CFR 164.308(a)(3)(ii)(C)	ISO/IEC 27001:2005 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.2	Command #6 Command #7 Command #8	CIP-004-3 R2.2.3 CIP-007-3 - R5.1.3 -R5.2.1 - R5.2.3	AC-2 PS-4 PS-5		8.5.4 8.5.5
Identity & Access Management *User ID Credentials* **アイデンティティとアクセス管理** *ユーザID認証*	IAM-12	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	適切な本人確認、権限付与、アクセス管理を確実に実施するため、定められたポリシー及び手順に従って、社内又は顧客(テナント)のユーザアカウントの資格情報を以下に示すような視点から、適切に制限しなければならない。 ·IDの信用性確認、サービス間連携アプリケーション(API)と情報処理の相互運用性(SSOと認証フェデレーションの場合など) · 作成から破棄に至るまでのアカウント資格情報のライフサイクル管理 · 実現可能な場合は、アカウントの資格情報及びIDストアの最小化又は再利用 ·業界に広く受け入れられる標準方式や法規制を遵守した認証、許可、アカウンティング(AAA)ルール(強力かつマルチファクターの期限付き非共有の認証秘密情報使用など)		X	X	X	X			X	X	X	X	X	S3.2.b	*(S3.2.b) b. Identification and authentication of users.*	B.1 H.5	E.6.2, E.6.3, H.1.1, H.1.2, H.2, H.3.2, H.4, H.4.1, H.4.5, H.4.8	6 (B)	SA-02	DS5.3 DS5.4		Domain 10	6.03.04. (b) 6.03.04. (c) 6.03.05. (d) 6.04.05. (b)	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-6 NIST SP 800-53 R3 IA-8	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 AC-11 NIST SP 800-53 R3 AC-11 (1) NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-2 (3) NIST SP 800-53 R3 AU-2 (4) NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-2 (2) NIST SP 800-53 R3 IA-2 (3) NIST SP 800-53 R3 IA-2 (8) NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-5 (2) NIST SP 800-53 R3 IA-5 (3) NIST SP 800-53 R3 IA-5 (6) NIST SP 800-53 R3 IA-5 (7) NIST SP 800-53 R3 IA-6 NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 SC-10		45 CFR 164.308(a)(5)(ii)(C) 45 CFR 164.308 (a)(5)(ii)(D) 45 CFR 164.312 (a)(2)(i) 45 CFR 164.312 (a)(2)(iii) 45 CFR 164.312 (d)	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4 A.11.5.5	Command #6 Command #7 Command #8 Command #9	CIP-004-3 R2.2.3 CIP-007-3 - R5.2 - R5.3.1 - R5.3.2 - R5.3.3	AC-1 AC-2 AC-3 AC-11 AU-2 AU-11 IA-1 IA-2 IA-5 IA-6 IA-8 SC-10		8.1 8.2, 8.3 8.4 8.5 10.1, 12.2, 12.3.8

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance					Corporate Governance Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																				
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Identity & Access Management *Utility Programs Access* **アイデンティティとアクセス管理** *ユーティリティプログラムアクセス*	IAM-13	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	システム、オブジェクト、ネットワーク、仮想マシン、アプリケーション制御を無効にする可能性のあるユーティリティプログラムは、使用を制限しなければならない。		X	X	X	X	X		X	X	X	X	X	S3.2.g	(S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).		H.2.16		IS-34	DS5.7		Domain 2		NIST SP 800-53 R3 CM-7	NIST SP 800-53 R3 AC-6 NIST SP 800-53 R3 AC-6 (1) NIST SP 800-53 R3 AC-6 (2) NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1)			A.11.4.1 A 11.4.4 A.11.5.4	Commandment #1 Commandment #5 Commandment #6 Commandment #7	CIP-007-3 - R2.1 - R2.2 - R2.3	AC-5 AC-6 CM-7 SC-3 SC-19		7.1.2
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection* **インフラと仮想化のセキュリティ** *監査ログ / 侵入検出*	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	適用される法令もしくは規則に対する違守義務を果たし、疑わしいネットワークの動作やファイルの不整合について、特定のユーザアクセスに起因することを説明できるようにし、セキュリティ違反の事態が生じた際のフォレンジック調査をサポートするために、監査ログに関する保護、保持、ライフサイクル管理を高いレベルで実現しなければならない。	X	X	X	X	X	X	X	X	X	X	X		S3.7	(S3.7) Procedures exist to identify, report, and act upon system security breaches and other incidents.	G.7 G.8 G.9 J.1 L.2	G.14.7, G.14.8, G.14.9, G.14.10, G.14.11, G.14.12, G.15.5, G.15.7, G.15.8, G.16.8, G.16.9, G.16.10, G.15.9, G.17.5, G.17.7, G.17.8, G.17.6, G.17.9, G.18.2, G.18.3, G.18.5, G.18.6, G.19.2.6, G.19.3.1, G.9.6.2, G.9.6.3, G.9.6.4, G.9.19, H.2.16, H.3.3, J.1, J.2, L.5, L.9, L.10		SA-14	DS5.5 DS5.6 DS9.2		Domain 10	6.03. (i) 6.03. (j) 6.03.03. (a) 6.03.03. (d) 6.03.04. (e) 6.04.07. (a) 6.07.01. (a) 6.07.01. (c)	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-3 NIST SP 800-53 R3 AU-4 NIST SP 800-53 R3 AU-5 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 AU-12 NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-2 (3) NIST SP 800-53 R3 AU-2 (4) NIST SP 800-53 R3 AU-3 NIST SP 800-53 R3 AU-3 (1) NIST SP 800-53 R3 AU-4 NIST SP 800-53 R3 AU-5 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-6 (1) NIST SP 800-53 R3 AU-6 (3) NIST SP 800-53 R3 AU-7 NIST SP 800-53 R3 AU-7 (1) NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 AU-12 NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 SC-18	8.2.1 8.2.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b) 45 CFR 164.308(a)(5)(ii)©	A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4 A.10.10.5 A.11.2.2 A.11.5.4 A.11.6.1 A.13.1.1 A.13.2.3 A.15.2.2 A.15.1.3	Commandment #6 Commandment #7 Commandment #11	CIP-007-3 - R6.5	AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-9 AU-11 AU-12 AU-14 SI-4		10.1 10.2 10.3 10.5 10.6 10.7 11.4 12.5.2 12.9.5
Infrastructure & Virtualization Security *Change Detection* **インフラと仮想化のセキュリティ** *変更検出*	IVS-02	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).	プロバイダは、すべての仮想マシンイメージの完全性を常に確認しなければならない。仮想マシンイメージに対して行われた変更は、その実行状態（待機時、停止時、実行中など）に関係なく、すべて記録し、注意喚起をしなければならない。イメージの変更又は移動とその後のイメージの完全性の確認の結果は、電子的手段（ポータル、アラートなど）によって顧客がすぐ得られるようにしなければならない。																																	
Infrastructure & Virtualization Security *Clock Synchronization* **インフラと仮想化のセキュリティ** *時間同期*	IVS-03	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	活動を時系列に追跡及び再現できるよう、すべての関連する情報処理システムのシステム時刻を同期するために、互いに同一の信頼できる外部の時刻発生源（もしくは時刻サーバ）を使用しなければならない。		X	X		X			X	X	X	X		S3.7	(S3.7) Procedures exist to identify, report, and act upon system security breaches and other incidents.	G.7 G.8	G.13, G.14.8, G.15.5, G.16.8, G.17.6, G.18.3, G.19.2.6, G.19.3.1	20 (B) 28 (B) 30 (B) 35 (B)	SA-12	DS5.7		Domain 10	6.03. (k)	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-8	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-8 NIST SP 800-53 R3 AU-8 (1)			A.10.10.1 A.10.10.6			AU-1 AU-8		10.4
Infrastructure & Virtualization Security *Information System Documentation* **インフラと仮想化のセキュリティ** *情報システム文書*	IVS-04	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	法的及び規制上の順守義務に従って、必要なシステム性能を実現するために、可用性、品質、適切な容量及び資源を計画し、準備し、測定しなければならない。システムの過負荷のリスクを軽減するために、将来必要な容量を予測しなければならない。		X	X	X		X		X	X	X	X	X	A3.2.0 A4.1.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. (A4.1.0) The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.		G.5		OP-03	DS 3		Domain 7, 8	6.03.07. (a) 6.03.07. (b) 6.03.07. (c) 6.03.07. (d)	NIST SP 800-53 R3 SA-4	NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7)	1.2.4		A.10.3.1	Commandment #1 Commandment #2 Commandment #3		SA-4		
Infrastructure & Virtualization Security *Management - Vulnerability Management* **インフラと仮想化のセキュリティ**	IVS-05	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).	実装者は、脆弱性の評価ツール又はサービスが、使用される仮想化技術（仮想化認識など）に確実に対応するようにしなければならない。																	--			Domain 1, 13											

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corp Gov Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Infrastructure & Virtualization Security *Network Security* **インフラと仮想化のセキュリティ** *ネットワークセキュリティ*	IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, reviewed at planned intervals, supported by documented business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure. Network architecture diagrams must clearly identify high-risk environments and data flows that may have legal, statutory, and regulatory compliance impacts. Technical measures shall be implemented to apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and packet black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	ネットワーク環境及び仮想マシンは、信頼できるネットワークと信頼できないネットワーク接続間のトラフィックを制限し監視するよう設計し構成されなければならず、また定期的な見直しを必要とする。その根拠として、すべての許可されるサービス、プロトコル、ポートについては、その許可についてのビジネス上の正当性を文書化しなければならない。また、これには安全でないと考えられるプロトコルについての許可すべき根拠やそれを補うための管理策について記載しなければならない。ネットワーク構成図においては、法規制上のコンプライアンスに影響する可能性のある高リスクの環境やデータの流れを明示しなければならない。技術的対策においては多層防御技術（たとえば、パケットの詳細分析、流量制御、ハニーネットなど）を、（出入り双方向について）異常な通信パターン（たとえばMACアドレス詐称やARPポイズニングのようなもの）や分散サービス妨害（DDoS）攻撃などの検知と速やかな対処のために実装しなければならない。	X	X	X	X	X	X		X	X	X	X	X	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	G.2 G.4 G.15 G.16 G.17 G.18 I.3	G.9.17, G.9.7, G.10, G.9.11, G.14.1, G.15.1, G.9.2, G.9.3, G.9.13		SA-08			Domain 10	6.03.03. (a) 6.03.03. (d) 6.03.04. (d) 6.04.07. (a) 6.07.01. (c)	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-20 (1)	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1) NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18) NIST SP 800-53 R3 SC-20 (1) NIST SP 800-53 R3 SC-21 NIST SP 800-53 R3 SC-22 NIST SP 800-53 R3 SC-30 NIST SP 800-53 R3 SC-32	8.2.5		A.10.6.1 A.10.6.2 A.10.9.1 A.10.10.2 A.11.4.1 A.11.4.5 A.11.4.6 A.11.4.7 A.15.1.4	Commandment #1 Commandment #2 Commandment #3 Commandment #9 Commandment #10 Commandment #11	CIP-004-3 R2.2.4	SC-7		1.1 1.1.2 1.1.3 1.1.5 1.1.6 1.2 1.2.1 2.2.2 2.2.3
Infrastructure & Virtualization Security *OS Hardening and Base Conrols* **インフラと仮想化のセキュリティ** *OS堅牢性と基本管*	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	各オペレーティングシステムは、ビジネスニーズに合致したポート、プロトコル、サービスのみを提供するように強化されねばならず、また、あらかじめ用意された技術的管理策、たとえばウイルス対策やファイル整合性モニタ（ファイルハッシュチェック）のようなものを、OSの基本ビルドまたはテンプレートの一部として持っていなくてはならない																	--			Domain 1, 13												
Infrastructure & Virtualization Security *Production / Non-Production Environments* **インフラと仮想化のセキュリティ**	IVS-08	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.	情報資産への権限のないアクセス又は変更を防ぐために、本番環境とテスト環境を分離しなければならない。	X	X	X	X	X	X		X	X	X	X		S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	B.1	I.2.7.1, I.2.20, I.2.17, I.2.22.2, I.2.22.4, I.2.22.10-14, H.1.1	22 (B)	SA-06	DS5.7		Domain 10	6.03. (d)		NIST SP 800-53 R3 SC-2		1.2.6		A.10.1.4 A.10.3.2 A.11.1.1 A.12.5.1 A.12.5.2 A.12.5.3	Commandment #1 Commandment #10 Commandment #11		SC-2		6.4.1 6.4.2
Infrastructure & Virtualization Security *Segmentation* **インフラと仮想化のセキュリティ** *区分*	IVS-09	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations	組織が所有又は管理する実/仮想マルチテナントアプリケーション、基盤システム、ネットワークコンポーネントは、プロバイダや特定（テナント）ユーザによるアクセスが他の（テナント）ユーザと適切に分離されるよう、以下の事項に基づいて設計し、開発し、導入し、設定しなければならない。 ・定められたポリシー及び手順 ・社内管理の強化と高レベルの保証が必要な重要資産や機微なユーザデータ及びそれらを扱うセッションの隔離 ・法的及び規制上の順守義務への準拠	X	X	X	X	X	X		X	X	X	X	X	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	G.17	G.9.2, G.9.3, G.9.13		SA-09	DS5.10		Domain 10	6.03.03. (b) 6.03.05. (a) 6.03.05. (b) 6.04.01. (a) 6.04.01. (g) 6.04.03. (c) 6.04.08.02. (a) 6.04.08.02. (b) 6.05. (c)	NIST SP 800-53 R3 SC-7	NIST SP 800-53 R3 AC-4 NIST SP 800-53 R3 SC-2 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18)		45 CFR 164.308 (a)(4)(ii)(A)	A.11.4.5 A.11.6.1 A.11.6.2 A.15.1.4	Commandment #1 Commandment #2 Commandment #3 Commandment #9 Commandment #10 Commandment #11	CIP-004-3 R3	AC-4 SC-2 SC-3 SC-7		1.1 1.2 1.2.1 1.3 1.4
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection* **インフラと仮想化のセキュリティ**	IVS-10	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	物理サーバ、アプリケーション又はデータを仮想サーバに移動させる場合には、安全で暗号化された通信回線を使用しなければならない。また、このような移動には、可能な場合、本番用のネットワークから分離された作業用のネットワークを使用しなければならない。																	--			Domain 1, 13												
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening* **インフラと仮想化のセキュリティ**	IVS-11	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	仮想システムをホストするシステムに対するすべてのハイパーバイザー管理機能又は管理コンソールへのアクセスは、最小権限の原則に基づいて担当者が制限され、技術的管理策（二要素認証、監査証跡の取得、IPアドレスのフィルタリング、ファイアウォール、管理コンソールに対するTLSで保護された通信など）によってサポートされなければならない。																	--			Domain 1, 13												
Infrastructure & Virtualization Security *Wireless Security* **インフラと仮想化のセキュリティ** *ワイヤレスセキュリティ*	IVS-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	以下の事項を含め、ワイヤレスネットワーク環境を保護するためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。 ・権限のないトラフィックを制限するために、境界にファイアウォールを導入し設定する ・セキュリティ設定で認証及び送信用の強力な暗号化を有効にする、ベンダのデフォルト設定を変更する（暗号鍵、パスワード、SNMPコミュニティ文字列など） ・ワイヤレスネットワークデバイスへのユーザアクセスを権限のある人に制限する ・権限のない（不正な）ワイヤレスネットワークデバイスの存在を検出し、適宜ネットワークから切断する	X	X	X	X	X	X	X	X	X	X	X	X	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	D.1 B.3 F.1 G.4 G.15 G.17 G.18	E.3.1, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18 G.9.17, G.9.7, G.10, G.9.11, G.14.1,	40 (B) 44 (C+)	SA-10	DS5.5 DS5.7 DS5.8 DS5.10		Domain 10		NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 SC-7	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-18 (1) NIST SP 800-53 R3 AC-18 (2) NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 CM-6 (1) NIST SP 800-53 R3 CM-6 (3) NIST SP 800-53 R3 PE-4 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18)	8.2.5	45 CFR 164.312 (e)(1)(2)(ii) 45 CFR 164.308(a)(5)(ii)(D) 45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(ii)	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.6.1 A.10.6.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7 A.12.3.1 A.12.3.2	Commandment #1 Commandment #2 Commandment #3 Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11	CIP-004-3 R3 CIP-007-3 - R6.1	AC-1 AC-18 CM-6 PE-4 SC-3 SC-7		1.2.3 2.1.1 4.1 4.1.1 11.1 9.1.3

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corporate Governance Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Service Consumer	Supplier / Tenant	Scope Applicability: AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
																				G.15.1, G.9.2, G.9.3, G.9.13																			
Interoperability & Portability *APIs* **相互運用性と移植容易性** *API*	IPY-01	The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.	コンポーネント間の相互運用性を最大限にサポートし、アプリケーションの移行をスムーズにするために、プロバイダは、オープンでその仕様が開示されたAPIを使用しなければならない。																			--			Domain 6											
Interoperability & Portability *Data Request* **相互運用性と移植容易性** *データ要求*	IPY-02	All unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, or .pdf)	構造化されていないすべてのデータを顧客が利用できるようにし、要求に応じて業界標準の形式(.doc、.xls、.pdfなど)で提供しなければならない。																			--			Domain 6											
Interoperability & Portability *Policy & Legal* **相互運用性と移植容易性** *ポリシーと法律*	IPY-03	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage and integrity persistence.	サービス間連携アプリケーション(API)、情報処理の相互運用性、移植性を考慮したアプリケーション開発、情報交換、使用、完全性の維持などに関する顧客(テナント)の要求事項を満たすためのポリシー、手順、相互に合意した条項/条件を確立しなければならない。																			--			Domain 3	6.04.03. (b) 6.04.08. (a) 6.04.08. (b) 6.06. (a) 6.06. (b) 6.06. (c) 6.06. (d) 6.06. (e) 6.06. (f)										
Interoperability & Portability *Standardized Network Protocols* **相互運用性と移植容易性** *標準ネットワークプロトコル*	IPY-04	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	プロバイダは、データのインポート及びエクスポート並びにサービス管理のために、安全な（暗号化、認証済み）標準ネットワークプロトコルを使用し、関連する相互運用性や移植性の標準を詳しく記述した文書を顧客（テナント）に提供しなければならない。																			--			Domain 6											
Interoperability & Portability *Virtualization* **相互運用性と移植容易性** *仮想化*	IPY-05	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	プロバイダは、相互運用性を確保するために、業界で広く認知された仮想化プラットフォーム及び標準仮想ファイル形式(OVFなど)を使用しなければならない。また、使用するハイパーバイザーへの独自の変更や使用しているすべてのアドオンソリューション固有の仮想フック(ハイパーバイザー機能への介入)を文書化し、顧客がレビューできるようにしなければならない。																			--			Domain 6											
Mobile Security *Anti-Malware* **モバイルセキュリティ** *アンチマルウエア*	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	プロバイダの情報セキュリティ意識向上訓練に、モバイルデバイス固有のマルウェア対策意識向上訓練を取り入れなければならない。																			--			None (Mobile Guidance)											
Mobile Security *Application Stores* **モバイルセキュリティ** *アプリケーションストア*	MOS-02	The company shall have a documented and communicated list of approved application stores that have been identified as acceptable for mobile devices accessing or storing company data and/or company systems.	企業は、企業データや企業システムにアクセスしたり、データをそこに格納したりするモバイルデバイスでの使用が許容されることを確認済みのアプリケーションの認定配信サービスのリストを文書化し周知させなければならない。																			--			None (Mobile Guidance)											
Mobile Security *Approved Applications* **モバイルセキュリティ** *承認されたアプリケーション*	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	企業は、承認されていないアプリケーション又は承認されているが事前に確認済みでないアプリケーション配信サービスから入手したアプリケーションのインストールを禁止するポリシーを文書化しておかなければならない。																			--			None (Mobile Guidance)											
Mobile Security *Approved Software for BYOD* **モバイルセキュリティ** *BYODとして承認されたソフトウエア*	MOS-04	The BYOD policy and supporting awareness training shall clearly state the approved applications and application stores that may be used for BYOD usage.	BYODに関するポリシー及びこれを補強する意識向上訓練において、BYODで使用可能な承認済みアプリケーション及びアプリケーション配信サービスを明確に示さなければならない。																			--			None (Mobile Guidance)											
Mobile Security *Awareness and Training* **モバイルセキュリティ** *認知とトレーニング*	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	プロバイダは、モバイルデバイスの定義、及びすべてのモバイルデバイスで許容される使用法及び要求事項を記載したモバイルデバイスのポリシーを文書化しておかなければならない。プロバイダは、プロバイダのセキュリティ意識向上訓練プログラムを通じて、ポリシー及び要求事項を公表し伝達しなければならない。																			--			None (Mobile Guidance)											
Mobile Security *Cloud Based Services* **モバイルセキュリティ** *クラウドベースサービス*	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	企業のモバイルデバイス、又はBYODで使用されるすべてのクラウドベースのサービスは、その使用法と企業の業務データの格納について、事前承認を受けなければならない。																			--			None (Mobile Guidance)											
Mobile Security *Compatibility* **モバイルセキュリティ** *互換性*	MOS-07	The company shall have a documented application validation process to test for device, operating system, and application compatibility issues.	企業は、デバイス、オペレーティングシステム、アプリケーションの互換性の問題に対して検査を行うアプリケーション検証プロセスを文書化しておかなければならない。																			--			None (Mobile Guidance)											

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corporate Governance Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Mobile Security *Device Eligibility* **モバイルセキュリティ** *デバイスの適格性*	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	BYODに関するポリシーでは、BYODの使用を許可するためのデバイスの適格性の要求事項を定義しなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Device Inventory* **モバイルセキュリティ** *デバイスの一覧表*	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD), will be included for each device in the inventory.	企業データを格納しこれにアクセスするのに使用されるすべてのモバイルデバイスの一覧表を保持し、更新しなければならない。一覧表の各デバイスの項目には、デバイスの状態に関するすべての変更(オペレーティングシステム及びパッチレベル、紛失又は使用終了のステータス、デバイスを割当てられた人又は(BYOD)デバイスの使用を承認された人など)を記載しなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Device Management* **モバイルセキュリティ** *データ管理*	MOS-10	The company shall have a centralized, mobile device management solution deployed to all mobile devices permitted to store, transmit, or process company data.	企業は、企業データを格納、送信、処理することを許可されたすべてのモバイルデバイスに対して、一元的なモバイルデバイス管理策を導入しなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Encryption* **モバイルセキュリティ** *暗号化*	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	モバイルデバイスポリシーでは、デバイス全体か、又はすべてのモバイルデバイス上の機微であると特定されたデータに対して暗号化を要求しなければならない。またポリシーは技術的管理策を通じて実施されなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Jailbreaking and Rooting* **モバイルセキュリティ** *ジェイルブレイクとルート化*	MOS-12	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and shall be enforced through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).	モバイルデバイスポリシーでは、モバイルデバイスに組込まれたセキュリティ対策の回避を禁止しなければならない(ジェイルブレイク、ルート化など)。またポリシーは、デバイス上の検出手段及び予防的手段を通じて、あるいは一元的なデバイス管理システム(モバイルデバイス管理など)を通じて、実施されなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Legal* **モバイルセキュリティ** *法律*	MOS-13	The BYOD policy shall include clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required.	BYODポリシーでは、プライバシーの必要保護レベル、訴訟の要件、電子的証拠開示、訴訟ホールド（訴訟等に関連して関係資料・情報を保存すること）等について明確に記述しなければならない。BYODポリシーは、デバイスの全データ消去が必要になった場合の企業データ以外のデータの損失の可能性について明記しなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Lockout Screen* **モバイルセキュリティ** *ロックアウト画面*	MOS-14	BYOD and/or company owned devices shall require an automatic lockout screen, and the requirement shall be enforced through technical controls.	BYODや企業が所有するデバイスには、自動ロック画面が必要である。この要求事項は、技術的管理策を通じて実施されなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Operating Systems* **モバイルセキュリティ** *オペレーティングシステム*	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	企業の変更管理プロセスを通じて、モバイルデバイスのオペレーティングシステム、パッチレベル、アプリケーションに対する変更を管理しなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Passwords* **モバイルセキュリティ** *パスワード*	MOS-16	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	企業のすべてのデバイス又はBYODでの使用が認められたデバイスに対するパスワードポリシーは、文書化し、技術的管理策を通じて実施されなければならない。このポリシーは、パスワードや暗証番号(PIN)の長さの変更、認証の要件の変更を禁じなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Policy* **モバイルセキュリティ** *ポリシー*	MOS-17	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	モバイルデバイスのポリシーでは、BYODのユーザに、データのバックアップの実行を要求し、未承認のアプリケーションストアの使用を禁じ、マルウェア対策ソフトウェアの使用(サポートされている場合)を要求しなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Remote Wipe* **モバイルセキュリティ** *リモート消去*	MOS-18	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	企業のBYODプログラムを通じて使用が許可されたすべてのモバイルデバイス、又は企業が支給したモバイルデバイスでは、企業のIT統括部門によるリモート消去が許可されるか、又は企業が提供するすべてのデータが企業のIT統括部門によって消去されなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Security Patches* **モバイルセキュリティ** *セキュリティパッチ*	MOS-19	Mobile devices connecting to corporate networks or storing and accessing company information validatedshall allow for remote validation to download the latest security patches by company IT personnel. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier.	企業のネットワークに接続し、企業の情報の格納やアクセスを行うモバイルデバイスでは、企業のIT担当者が最新のセキュリティパッチをダウンロードできるよう、リモート検証が許可されなければならない。デバイスメーカー又は通信業者の通常リリースに応じて、すべてのモバイルデバイスに、最新のセキュリティ関連パッチをインストールしなければならない。																		--			None (Mobile Guidance)											
Mobile Security *Users* **モバイルセキュリティ** *ユーザ*	MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	BYODポリシーでは、BYODとして認可されたデバイスが使用又はアクセス可能なシステム及びサーバを明記しなければならない。																		--			None (Mobile Guidance)											

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance						Corporate Governance Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																	
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance* **セキュリティインシデント管理、Eディスカバリ、クラウドフォレンジックス** *契約 / 機関の維持*	SEF-01	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	コンプライアンスに関する司法当局との直接的な連携及び迅速な実施を必要とするフォレンジック調査の準備を整えておくために、該当する規制当局、国家及び地方の司法当局、その他の法管轄当局との連絡窓口を維持し、定期的に更新（影響を受ける適用範囲の変更、遵守義務の変更など）しなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S4.3.0 x4.4.0	(S4.3.0) Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment. (x4.4.0) Environmental, regulatory, and technological changes are monitored, and their impact on system [availability, processing integrity, confidentiality] and security is assessed on a timely basis. System [availability, processing integrity, confidentiality] policies and procedures are updated for such changes as required.		L1		CO-04	ME 3.1		Domain 2, 4		NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-6 (1) NIST SP 800-53 R3 SI-5	1.2.7 10.1.1 10.2.4		A.6.1.6 A.6.1.7	Commandment #1 Commandment #2 Commandment #3	CIP-001-1a R3 - R4	AT-5 IR-6 SI-5		11.1.e 12.5.3 12.9
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management* **セキュリティインシデント管理、Eディスカバリ、クラウドフォレンジックス** *インシデント管理*	SEF-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	定められたITサービスマネジメントのポリシー及び手順に従って、セキュリティ関連の事象を優先順位付けし、適時かつ一貫したインシデント管理を確実に行うために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	IS3.7.0 S3.9.0	(IS3.7.0) Procedures exist to identify, report, and act upon system security breaches and other incidents. (S3.9.0) Procedures exist to provide that issues of noncompliance with system availability, confidentiality of data, processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	J.1	J.1.1, J.1.2	46 (B)	IS-22	DS5.6		Domain 2	6.04.07. (b) 6.07.01. (a) 6.07.01. (d) 6.07.01. (e) 6.07.01. (f) 6.07.01. (g) 6.07.01. (h)	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-3 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-4 (1) NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 IR-8	1.2.4 1.2.7 7.1.2 7.2.2 7.2.4 10.2.1 10.2.4	45 CFR 164.308 (a)(1)(i) 45 CFR 164.308 (a)(6)(i)	Clause 4.3.3 A.13.1.1 A.13.2.1	Commandment #2 Commandment #6 Commandment #8	CIP-007-3 - R6.1 CIP-008-3 - R1	IR-1 IR-2 IR-3 IR-4 IR-5 IR-7 IR-8		12.9 12.9.1 12.9.2 12.9.3 12.9.4 12.9.5 12.9.6
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting* **セキュリティインシデント管理、Eディスカバリ、クラウドフォレンジックス** *インシデントレポーティング*	SEF-03	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	従業員及び外部の取引関係者に自身が負うべき責任を周知しなければならない。また、必要があれば、従業員及び外部の取引関係者は、速やかにすべての情報セキュリティ事象を報告することに同意し、または契約により合意しなければならない。情報セキュリティ事象は、適用される法令上又は規制上の遵守義務に従って速やかに、事前に設定された伝達経路を通じて報告されなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	A2.3.0 C2.3.0 I2.3.0 S2.3.0 S2.4 C3.6.0	(A2.3.0, C2.3.0, I2.3.0, S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality of data, processing integrity and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them. (S2.4) The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users. (C3.6.0) The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system confidentiality and related security policies and that the third party is in compliance with its policies.	J.1 E.1	J.1.1, E.4	5 (B) 46 (B) 48 (A+) 49 (B) 50 (B)	IS-23	DS5.6		Domain 2	6.07.01. (a)	NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-6 (1) NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 SI-5	1.2.7 1.2.10 7.1.2 7.2.2 7.2.4 10.2.4	45 CFR 164.312 (a)(6)(ii) 16 CFR 318.3 (a) 16 CFR 318.5 (a) 45 CFR 160.410 (a)(1)	Clause 4.3.3 Clause 5.2.2 A.6.1.3 A.8.2.1 A.8.2.2 A.13.1.1 A.13.1.2 A.13.2.1	Commandment #2 Commandment #6 Commandment #8	CIP-003-3 - R4.1 CIP-004-3 R3.3	IR-2 IR-6 IR-7 SI-4 SI-5		12.5.2 12.5.3
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation* **セキュリティインシデント管理、Eディスカバリ、クラウドフォレンジックス** *インシデントレスポンスの法的準備*	SEF-04	In the event a follow-up action concerning a person or organization after an information security incident requires legal action, proper forensic procedures, including chain of custody, shall be required for the preservation and presentation of evidence to support potential legal action subject to the relevant jurisdiction. Upon notification, customers (tenants) and/or other external business relationships impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	情報セキュリティインシデントの発生後、従業員又は組織に関連する対処につき法的措置が必要になる場合は、関連する司法管轄において行われる可能性のある今後の法的措置を支援する証拠を保全し提出するために、適切なフォレンジック手続（証拠保全、収集、保管の流れの記録を含む）を履践する必要がある。通知に基づいて、セキュリティ違反の影響を受ける顧客（テナント）や他の外部取引関係者には、法的に認められる範囲で、フォレンジック調査に参加する機会が与えられなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S2.4.0 C3.15.0	(S2.4.0) The process for informing the entity about system availability issues, confidentiality issues, processing integrity issues, security issues and breaches of the system security and for submitting complaints is communicated to authorized users. (C3.15.0) Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	J.1 E.1	J.1.1, J.1.2, E.4		IS-24	DS5.6		Domain 2	6.04.07. (b) 6.07.01. (f) 6.07.01. (h)	NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-8	NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-6 (1) NIST SP 800-53 R3 AU-6 (3) NIST SP 800-53 R3 AU-7 NIST SP 800-53 R3 AU-7 (1) NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-9 (2) NIST SP 800-53 R3 AU-10 NIST SP 800-53 R3 AU-10 (5) NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 IR-8 NIST SP 800-53 R3 MP-5 NIST SP 800-53 R3 MP-5 (2) NIST SP 800-53 R3 MP-5 (4)	1.2.7	45 CFR 164.308 (a)(6)(ii)	Clause 4.3.3 Clause 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3		CIP-004-3 R3.3	AU-6 AU-7 AU-9 AU-11 IR-5 IR-7 IR-8		
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics* **セキュリティインシデント管理、Eディスカバリ、クラウドフォレンジックス** *インシデントレスポンスマトリックス*	SEF-05	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	情報セキュリティインシデントを監視し、その種類や規模、コストを定量化するような機能を導入しなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	S3.9.0 C4.1.0	(S3.9.0) Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis. (C4.1.0) The entity's system security, availability, system integrity, and confidentiality is periodically reviewed and compared with the defined system security, availability, system integrity, and confidentiality policies.		J.1.2	47 (B)	IS-25	DS 4.9		Domain 2	6.07.01. (a) 6.07.01. (i)	NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-8	NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-4 (1) NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-8	1.2.7 1.2.10	45 CFR 164.308 (a)(1)(ii)(D)	A.13.2.2		CIP-008-3 - R1.1	IR-4 IR-5 IR-8		12.9.6

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance						Corporate Governance Relevance	Delivery Model Applicability			Supplier Relationship		Scope Applicability																		
				Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity* **サプライチェーンの管理、透明性、説明責任** *データ品質と完全性*	STA-01	Providers shall inspect, account for, and correct data quality errors and risks inherited from partners within their cloud supply-chain. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	プロバイダは、クラウドサプライチェーン内のパートナーから引き継いだデータ品質の欠陥とリスクを検査し、詳細を明らかにし、修正しなければならない。プロバイダは、サプライチェーン内のすべての人員に対する適切な職務の分割、ロールベースのアクセス、最小権限のアクセスを通じて、データセキュリティリスクを軽減し抑制するための管理策を策定し実装しなければならない。																		--			Domain 2											
Supply Chain Management, Transparency and Accountability *Incident Reporting* **サプライチェーンの管理、透明性、説明責任** *インシデントレポーティング*	STA-02	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).	プロバイダは、電子的手段（ポータルなど）を通じて定期的に、影響を受けるすべての顧客とプロバイダがセキュリティインシデント情報を利用できるようにしなければならない。																		--			Domain 2											
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services* **サプライチェーンの管理、透明性、説明責任** *ネットワーク / インフラストラクチャサービス*	STA-03	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	相互に合意したサービス、容量の予測、ITガバナンス、サービス管理ポリシー及び手順に従って、業務上不可欠な又は顧客（テナント）に影響する実/仮想アプリケーション及びシステム間のインタフェース（API）の設計及び設定、インフラストラクチャーのネットワーク及びシステムコンポーネントを設計し、開発し、展開しなければならない。	X	X	X	X	X	X	X	X	X	X	X	X	C2.2.0	(C2.2.0) The system security, availability, system integrity, and confidentiality and related security obligations of users and the entity's system security, availability, system integrity, and confidentiality and related security commitments to users are communicated to authorized users.	C.2	C.2.6, G.9.9	45 (B) 74 (B)	IS-31	DS5.1 0		Domain 2	6.02. (c) 6.03.07. (a) 6.03.07. (b) 6.03.07. (c) 6.03.07. (d)	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 CP-6 NIST SP 800-53 R3 CP-6 (1) NIST SP 800-53 R3 CP-6 (3) NIST SP 800-53 R3 CP-7 NIST SP 800-53 R3 CP-7 (1) NIST SP 800-53 R3 CP-7 (2) NIST SP 800-53 R3 CP-7 (3) NIST SP 800-53 R3 CP-7 (5) NIST SP 800-53 R3 CP-8 NIST SP 800-53 R3 CP-8 (1) NIST SP 800-53 R3 CP-8 (2) NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1) NIST SP 800-53 R3 SC-30	8.2.2 8.2.5		A.6.2.3 A.10.6.2	Commandment #6 Commandment #7 Commandment #8		SC-20 SC-21 SC-22 SC-23 SC-24		
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments* **サプライチェーンの管理、透明性、説明責任** *プロバイダの内部評価*	STA-04	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	プロバイダは、ポリシー、手順、これらをサポートする対策や基準の適合性及び有効性の内部評価を年1回実施しなければならない。																		--			Domain 2											
Supply Chain Management, Transparency and Accountability *Supply Chain Agreements* **サプライチェーンの管理、透明性、説明責任** *サプライチェーンの合意*	STA-05	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)	プロバイダと顧客（テナント）とのサプライチェーンについての契約書（SLAなど）には、少なくとも、以下のような相互に合意した条項/条件を取り入れなければならない。 ・取引関係及び提供されるサービスの範囲（顧客（テナント）のデータの取得・交換・利用方法、構成テンプレート及び機能、サービス提供及びサポートに必要な人員・基盤ネットワーク・システムコンポーネント、プロバイダ及び顧客（テナント）の役割及び責任、下請け及び外部委託の取引関係、ホストされるサービスの物理的地理的位置、並びに既知の規制上の法令遵守に関する考慮事項など） ・情報セキュリティの要求事項、プロバイダ及び顧客（テナント）の取引関係の継続期間中の主たる連絡窓口、影響を受けるすべての取引関係によるガバナンス、リスクマネジメント、保証、並びに、法律上及び規制上の遵守義務を効果的に実行するために導入される詳細な補助的関連ビジネスプロセス及び技術的対策への言及 ・顧客（テナント）への影響力を持つプロバイダの管理下における変更の通知や事前承認 ・影響を受けるすべての顧客（テナント）その他の取引関係者（影響を受けるアップストリーム及びダウンストリームのサプライチェーン）に、セキュリティインシデント（あるいは、確認された漏えい）を適宜通知すること	X	X	X	X	X	X	X	X	X	X	X	X	S2.2.0 A3.6.0 C3.6.0	(S2.2.0) The availability, confidentiality of data, processing integrity, system security and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users. (A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. (C3.6.0) The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system	C.2	C.2.4, C.2.6, G.4.1, G.16.3	74 (B) 75 (C+, A+) 45 (B) 75 (C+, A+) 79 (B) 4 (C+, A+)	LG-02	DS5.1 1		Domain 3	6.02. (e) 6.10. (h) 6.10. (i)	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 PS-7 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 MP-5 NIST SP 800-53 R3 MP-5 (2) NIST SP 800-53 R3 MP-5 (4) NIST SP 800-53 R3 PS-7 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1)	1.2.5	45 CFR 164.308 (a)(4)(ii)(A) 45 CFR 164.308 (b)(1) 45 CFR 164.308 (b)(2)(i) 45 CFR 164.308 (b)(2)(ii) 45 CFR 164.308 (b)(2)(iii)	A.6.2.3 A10.2.1 A.10.8.2 A.11.4.6 A.11.6.1 A.12.3.1 A.12.5.4	Commandment #1 Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8		CA-3 MP-5 PS-7 SA-6 SA-7 SA-9		2.4 12.8.2

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Network	Compute	Storage	App	Data	Corp Gov Relevance	Delivery Model Applicability: SaaS	PaaS	IaaS	Supplier Relationship: Service Provider	Tenant / Consumer	AICPA TS Map	AICPA Trust Service Criteria (SOC 2SM Report)	BITS Shared Assessments AUP v5.0	BITS Shared Assessments SIG v6.0	BSI Germany	CCM V1.X	COBIT 4.1	CSA Enterprise Architecture / Trust	CSA Guidance V3.0	ENISA IAF	FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	GAPP (Aug 2009)	HIPAA / HITECH Act	ISO/IEC 27001-2005	Jericho Forum	NERC CIP	NIST SP800-53 R3	NZ ISM	PCI DSS v2.0
		• Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	・評価対象の組織に許容できないビジネスリスクが及ぶことなく、契約条項を遵守しているかどうかを評価し独立して検証すること（業界が認める認証、証明用監査報告書、その他の証明形式など） ・取引関係の終了及び影響を受ける顧客（テナント）データの処理 ・アプリケーション開発、情報の交換、使用、完全性維持を目的とする、顧客（テナント）のサービス間のアプリケーション（API）とデータの相互運用性及び可搬性の要求事項															confidentiality and related security policies and that the third party is in compliance with its policies.											45 CFR 164.308 (b)(3) 45 CFR 164.308 (b)(4) 45 CFR 164.312(e)(2)(i) 45 CFR 164.312 (c)(1) 45 CFR 164.312(e)(2)(ii) 45 CFR 164.314 (a)(1)(i) 45 CFR 164.314 (a)(1)(ii)(A) 45 CFR 164.314 (a)(2)(i) 45 CFR 164.314 (a)(2)(i)(A) 45 CFR 164.314 (a)(2)(i)(B) 45 CFR 164.314 (a)(2)(i)(C) 45 CFR 164.314 (a)(2)(i)(D) 45 CFR 164.314 (a)(2)(ii)(A) 45 CFR 164.314 (a)(2)(ii)(A)(1) 45 CFR 164.314 (a)(2)(ii)(A)(2) 45 CFR 164.314 (a)(2)(ii)(B)						
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews* **サプライチェーンの管理、透明性、説明責任** *ガバナンスのレビュー*	STA-06	Providers shall review the risk management and governance processes of their partners to ensure that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	プロバイダは、実施内容が整合性を保持し、パートナーのクラウドサプライチェーンの他のメンバーから引き継いだリスクの主な原因を明らかにするための調整を確実に行うために、パートナーのリスクマネジメント及びガバナンスプロセスをレビューしなければならない。																		--			Domain 2												
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics* **サプライチェーンの管理、透明性、説明責任** *サプライチェーンマトリックス*	STA-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants), with an ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream), and for managing service-level conflicts or inconsistencies resulting from disparate supplier relationships.	サプライチェーン全体（アップストリーム/ダウンストリーム）で条項/条件への不適合を測定し対処できる、プロバイダと顧客（テナント）間の完全、正確かつ妥当な合意書（SLAなど）を維持し、異業種の供給者関係から生じるサービスレベルの競合や不整合を管理するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。																		51 (B)	--		Domain 3	6.02. (c) 6.02. (d) 6.07.01. (k)									
Supply Chain Management, Transparency and Accountability *Third Party Assessment* **サプライチェーンの管理、透明性、説明責任** *第三者の評価*	STA-08	Providers shall assure reasonable information security across their information supply chain by performing a regular review. The review shall include all partners upon which their information supply chain depends.	プロバイダは、定期的なレビューを実施して、情報サプライチェーン全体で妥当な情報セキュリティが維持されることを保証しなければならない。レビューには、情報サプライチェーンに関与するすべてのパートナーを含めなければならない。																		--			Domain 2												
Supply Chain Management, Transparency and Accountability *Third Party Audits* **サプライチェーンの管理、透明性、説明責任** *第三者の監査*	STA-09	Third-party service providers shall demonstrate compliance with information security and confidentiality, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at planned intervals to govern and maintain compliance with the service delivery agreements.	第三者のサービスプロバイダは、第三者契約に含まれる情報セキュリティ及び情報の機密性、サービス定義、供給サービスレベル契約書を順守していることを実証しなければならない。サービス提供の契約書への順守状況を監督し維持するために、第三者の報告書、記録、サービスの監査及びレビューを事前に定められた間隔で実施しなければならない。	X	X	X	X	X	X	X	X	X	X	X		S2.2.0 C2.2.0 C3.6	Note: third party service providers are addressed under either the carve-out method or the inclusive method as it relates to the assessment of controls. (S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users. (C2.2.0) The system confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters: (see sub-criteria on TSPC tab) (C3.6) The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system confidentiality and related security policies and that the third party is in compliance with its policies.	C.2	C.2.4,C.2.6, G.4.1, G.4.2, L.2, L.4, L.7, L.11	60 (B) 62 (C+, A+) 83 (B) 84 (B) 85 (B)	CO-03	ME 2.6 DS 2.1 DS 2.4		Domain 2, 4	6.02. (b) 6.02. (d)	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SC-7	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1) NIST SP 800-53 R3 SA-12 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-7 (1) NIST SP 800-53 R3 SC-7 (2) NIST SP 800-53 R3 SC-7 (3) NIST SP 800-53 R3 SC-7 (4) NIST SP 800-53 R3 SC-7 (5) NIST SP 800-53 R3 SC-7 (7) NIST SP 800-53 R3 SC-7 (8) NIST SP 800-53 R3 SC-7 (12) NIST SP 800-53 R3 SC-7 (13) NIST SP 800-53 R3 SC-7 (18)	1.2.11 4.2.3 7.2.4 10.2.3 10.2.4	45 CFR 164.308(b)(1) 45 CFR 164.308 (b)(4)	A.6.2.3 A.10.2.1 A.10.2.2 A.10.6.2	Commandment #1 Commandment #2 Commandment #3		CA-3 SA-9 SA-12 SC-7		2.4 12.8.2 12.8.3 12.8.4 Appendix A

CLOUD CONTROLS MATRIX VERSION 3.0

Control Domain	CCM V3.0 Control ID	Control Specification	日本語訳	Architectural Relevance: Phys	Architectural Relevance: Network	Architectural Relevance: Compute	Architectural Relevance: Storage	Architectural Relevance: App	Architectural Relevance: Data	Corporate Governance Relevance	Delivery Model Applicability: SaaS	Delivery Model Applicability: PaaS	Delivery Model Applicability: IaaS	Supplier Relationship: Service Provider	Supplier Relationship: Tenant / Consumer	Scope Applicability: AICPA TS Map	Scope Applicability: AICPA Trust Service Criteria (SOC 2SM Report)	Scope Applicability: BITS Shared Assessments AUP v5.0	Scope Applicability: BITS Shared Assessments SIG v6.0	Scope Applicability: BSI Germany	Scope Applicability: CCM V1.X	Scope Applicability: COBIT 4.1	Scope Applicability: CSA Enterprise Architecture / Trust	Scope Applicability: CSA Guidance V3.0	Scope Applicability: ENISA IAF	Scope Applicability: FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--	Scope Applicability: FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--	Scope Applicability: GAPP (Aug 2009)	Scope Applicability: HIPAA / HITECH Act	Scope Applicability: ISO/IEC 27001-2005	Scope Applicability: Jericho Forum	Scope Applicability: NERC CIP	Scope Applicability: NIST SP800-53 R3	Scope Applicability: NZ ISM	Scope Applicability: PCI DSS v2.0
Threat and Vulnerability Management *Anti-Virus / Malicious Software* **脅威と脆弱性の管理** *アンチウイルス / 悪質なソフトウエア*	TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	組織が所有または管理するユーザのエンドポイントデバイス（支給されたワークステーション、ラップトップ、モバイルデバイスなど）やIT基盤のネットワーク及びシステムコンポーネントにおけるマルウェアの実行を防止するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。		X	X	X	X			X	X	X	X	X	S3.5.0	(S3.5.0) Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.		G.7	17 (B)	IS-21	DS5.9		Domain 2	6.03. (f)	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-5 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1) NIST SP 800-53 R3 SI-8	8.2.2	45 CFR 164.308 (a)(5)(ii)(B)	A.10.4.1	Commandment #4 Commandment #5	CIP-007-3 - R4 - R4.1 - R4.2	SA-7 SC-5 SI-3 SI-5 SI-7 SI-8		5.1 5.1.1 5.2
Threat and Vulnerability Management *Vulnerability / Patch Management* **脅威と脆弱性の管理** *脆弱性 / パッチ管理*	TVM-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed (physical and virtual) applications and infrastructure network and system components, applying a risk-based model for prioritizing remediation through change-controlled, vender-supplied patches, configuration changes, or secure software development for the organization's own software. Upon request, provider shall inform customer (tenant) of policies and procedures, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	組織が所有または管理する実/仮想アプリケーション、IT基盤のネットワーク及びシステムコンポーネント内の脆弱性を適宜検出するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。また、組織が所有しているソフトウエアに対する変更管理、ベンダー提供パッチの適用、構成変更、安全なソフトウエアの開発を通じた改善措置を優先順位付けするために、リスクベースのモデルを適用しなければならない。プロバイダは、要求に応じて、特に顧客（テナント）データがサービスの一部として利用されたり、顧客（テナント）が管理の実施に対する責任の一部を共有したりしている場合は、顧客（テナント）にポリシーおよび手順を通知しなければならない。		X	X	X	X		X	X	X	X	X		S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	I.4	G.15.2, I.3	32 (B) 33 (B)	IS-20	AI6.1 AI3.3 DS5.9		Domain 2	6.03.02. (a) 6.03.02. (b) 6.03.05. (c) 6.07.01. (o)	NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 RA-5 (1) NIST SP 800-53 R3 RA-5 (2) NIST SP 800-53 R3 RA-5 (3) NIST SP 800-53 R3 RA-5 (6) NIST SP 800-53 R3 RA-5 (9) NIST SP 800-53 R3 SC-30 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-5	1.2.6 8.2.7	45 CFR 164.308 (a)(1)(i)(ii)(A) 45 CFR 164.308 (a)(1)(i)(ii)(B) 45 CFR 164.308 (a)(5)(i)(ii)(B)	A.12.5.1 A.12.5.2 A.12.6.1	Commandment #4 Commandment #5	CIP-004-3 R4 - 4.1 - 4.2 CIP-005-3a - R1 - R1.1 CIP-007-3 - R3 - R3.1 - R8.4	CM-3 CM-4 CP-10 RA-5 SA-7 SI-1 SI-2 SI-5		2.2 6.1 6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3
Threat and Vulnerbility Management *Mobile Code* **脅威と脆弱性の管理** *モバイルコード*	TVM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	承認されていないモバイルコードが実行されるのを防止するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。ここで、承認されていないモバイルコードとは、組織が所有または管理するユーザのエンドポイントのデバイス（支給されたワークステーション、ラップトップ、モバイルデバイスなど）、IT基盤のネットワーク及びシステムコンポーネント上で、信頼できるネットワークまたは信頼できないネットワークのシステム間で転送され、受信者が明示的にインストールや実行をすることなくローカルシステム上で実行されるソフトウエアのことである。		X	X		X	X		X	X	X	X	X	S3.4.0 S3.10.0	(S3.4.0) Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.		G.20.12, I.2.5		SA-15			Domain 10	6.03. (g)						A.10.4.2 A.12.2.2	Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #11		SC-18		