

35のリスク項目 (R1 - R35)			
No.	用語	対訳	備考
<b>Policy And Organizational Risks</b>		<b>ポリシーと組織関連のリスク</b>	
R.1	Lock-In	ロックイン	ロックイン: 特定の事業者のサービスに処理を依存する結果、その事業者への依存から離れられなくなること。
R.2	Loss Of Governance	ガバナンスの喪失	
R.3	Compliance Challenges	コンプライアンスの課題	
R.4	Loss Of Business Reputation Due To Co-Tenant Activities	他の共同利用者の行為による信頼の喪失	
R.5	Cloud Service Termination or Failure	クラウドサービスの終了または障害	
R.6	Cloud Provider Acquisition	クラウドプロバイダの買収	
R.7	Supply Chain Failure	サプライチェーンにおける障害	
<b>Technical Risks</b>		<b>技術関連のリスク</b>	
R.8	Resource Exhaustion (Under Or Over Provisioning)	リソースの枯渇(リソース割当の過不足)	
R.9	Isolation Failure	隔離の失敗	
R.10	Cloud Provider Malicious Insider - Abuse Of High Privilege Roles	クラウドプロバイダ従事者の不正 - 特権の悪用	
R.11	Management Interface Compromise (Manipulation, Availability Of Infrastructure)	管理用インタフェースの悪用(操作、インフラストラクチャアクセス)	
R.12	Intercepting Data In Transit	データ転送途上における攻撃	
R.13	Data Leakage On Up/Download, Intra-Cloud	データ漏えい(アップロード時、ダウンロード時、クラウド間転送)	
R.14	Insecure Or Ineffective Deletion Of Data	セキュリティが確保されていない、または不完全なデータ削除	
R.15	Distributed Denial Of Service (Ddos)	DDoS攻撃(分散サービス運用妨害攻撃)	
R.16	Economic Denial Of Service (Edos)	EDoS攻撃(経済的な損失を狙ったサービス運用妨害攻撃)	
R.17	Loss Of Encryption Keys	暗号鍵の喪失	
R.18	Undertaking Malicious Probes Or Scans	不正な探査またはスキャンの実施	
R.19	Compromise Service Engine	サービスエンジンの侵害	
R.20	Conflicts Between Customer Hardening Procedures And Cloud Environment	利用者側の強化手順と、クラウド環境との間に生じる矛盾	
<b>Legal Risks</b>		<b>法的なリスク</b>	
R.21	Subpoena And E-Discovery	証拠提出命令と電子的証拠開示	
R.22	Risk From Changes Of Jurisdiction	司法権の違いから来るリスク	
R.23	Data Protection Risks	データ保護に関するリスク	
R.24	Licensing Risks	ライセンスに関するリスク	
<b>Risks Not Specific To The Cloud</b>		<b>クラウドに特化していないリスク</b>	
R.25	Network Breaks	ネットワークの途絶	
R.26	Network Management (ie, Network Congestion / Mis-Connection / Non-Optimal Use)	ネットワークの管理(ネットワークの混雑、接続ミス、最適でない使用)	
R.27	Modifying Network Traffic	ネットワークトラフィックの改変	
R.28	Privilege Escalation	特権の(勝手な)拡大	
R.29	Social Engineering Attacks (ie, Impersonation)	ソーシャルエンジニアリング攻撃(なりすまし)	
R.30	Loss Or Compromise Of Operational Logs	運用ログの喪失または改ざん	
R.31	Loss Or Compromise Of Security Logs (Manipulation Of Forensic Investigation)	セキュリティログの喪失または改ざん(フォレンジック捜査の操作)	
R.32	Backups Lost, Stolen	バックアップの喪失、盗難	
R.33	Unauthorized Access To Premises (Including Physical Access To Machines And Other Facilities)	構内への無権限アクセス(装置その他の設備への物理的アクセスを含む)	
R.34	Theft Of Computer Equipment	コンピュータ設備の盗難	
R.35	Natural Disasters	自然災害	

53の脆弱性項目(V1 - V53)			
No.	用語	対訳	備考
<b>Vulnerabilities Specific To Cloud</b>		<b>クラウドに特化した脆弱性</b>	
V1	AAA Vulnerabilities	AAAの脆弱性	AAA (authentication, authorisation and accounting) : 認証、認可および課金管理
V2	User Provisioning Vulnerabilities	ユーザプロビジョニングの脆弱性	プロビジョニング:システムリソース等を顧客のニーズに応じて提供するプロセス。システム使用権限をユーザに割り当てることを意味する場合や、そのような割当の変更管理を意味する場合もある。
V3	User De-Provisioning Vulnerabilities	ユーザプロビジョニング削除の脆弱性	
V4	Remote Access To Management Interface	管理用インターフェースへのリモートアクセス	
V5	Hypervisor Vulnerabilities	ハイパーバイザの脆弱性	
V6	Lack Of Resource Isolation	リソース分離の欠如	
V7	Lack Of Reputational Isolation	不信の伝播に対する隔離の欠如	
V8	Communication Encryption Vulnerabilities	通信路暗号の脆弱性	
V9	Lack Of Or Weak Encryption Of Archives And Data In Transit	アーカイブおよび転送中のデータの暗号化の強度不足または未実施	
V10	Impossibility Of Processing Data In Encrypted Form	暗号化状態でのデータ処理が不可能であること	
V11	Poor Key Management Procedures	不適切な鍵管理手順	
V12	Key Generation: Low Entropy For Random Number Generation	乱数生成器への低エントロピーの入力	
V13	Lack Of Standard Technologies And Solutions	技術とソリューションにおける標準の欠如	
V14	No Source Escrow Agreement	ソースコードエスクロー(預託)契約の欠如	
V15	Inaccurate Modelling Of Resource Usage	リソースの使用に関する不正確なモデリング	
V16	No Control On Vulnerability Assessment Process	脆弱性診断プロセスに関する管理の欠如	
V17	Possibility That Internal (Cloud) Network Probing Will Occur	内部(クラウド)ネットワークへの偵察行為が発生する可能性	
V18	Possibility That Co-Residence Checks Will Be Performed	共同利用者からの覗き見の可能性	
V19	Lack Of Forensic Readiness	法的対応体制の不備	
V20	Sensitive Media Sanitization	機密性の高いメディアのサニタイゼーション(記録の抹消)	
V21	Synchronizing Responsibilities Or Contractual Obligations External To Cloud	クラウド外の契約上の義務または責任のクラウドへの適用	
V22	Cross-Cloud Applications Creating Hidden Dependency	クラウドをまたがるアプリケーションに潜在する相互依存性	
V23	SLA Clauses With Conflicting Promises To Different Stakeholders	複数利害関係者間で矛盾するSLA条項	
V24	SLA Clauses Containing Excessive Business Risk	SLA条項に含まれる過剰なビジネスリスク(クラウドプロバイダにとって)	SLA(Service Level Agreement)
V25	Audit Or Certification Not Available To Customers	利用者に監査または認証の証明書が提供されない問題	
V26	Certification Schemes Not Adapted To Cloud Infrastructures	クラウドのインフラに適用できる認証スキームの欠如	
V27	Inadequate Resource Provisioning And Investments In Infrastructure	クラウドのインフラに対する投資またはリソース割当の不足	
V28	No Policies For Resource Capping	リソースの利用上限制限ポリシーの欠如	
V29	Storage Of Data In Multiple Jurisdictions And Lack Of Transparency About This	複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如	
V30	Lack Of Information On Jurisdictions	司法管轄権に関する情報の欠如	
V31	Lack Of Completeness And Transparency In Terms Of Use	利用規約の完全性と透明性の欠如	
<b>Vulnerabilities Not Specific To Cloud</b>		<b>クラウドに特化していない脆弱性</b>	
V32	Lack Of Security Awareness	セキュリティ意識の欠如	
V33	Lack Of Vetting Processes	身元調査プロセスの欠如	
V34	Unclear Roles And Responsibilities	役割と責任の不明確性	
V35	Poor Enforcement Of Role Definitions	役割定義の適用の不備	
V36	Need-To-Know Principle Not Applied	「知る必要性」原則の不適用	
V37	Inadequate Physical Security Procedures	物理的なセキュリティ手順の不備	
V38	Misconfiguration	設定ミス	

V39	System Or OS Vulnerabilities	システムまたはOSの脆弱性	
V40	Untrusted Software	信頼できないソフトウェア	
V41	Lack Of, Or A Poor And Untested, Business Continuity And Disaster Recovery Plan	事業継続計画および災害復旧計画の欠如、不備、テストの未実施	
V42	Lack Of, Or Incomplete Or Inaccurate, Asset Inventory	資産目録の欠如、不備、不正確性	
V43	Lack Of, Or Poor Or Inadequate, Asset Classification	資産分類の欠如、不備、不足	
V44	Unclear Asset Ownership	不明確な資産の管理責任	
V45	Poor Identification Of Project Requirements	プロジェクト要件定義の不足	
V46	Poor Provider Selection	プロバイダの選定不備	
V47	Lack Of Supplier Redundancy	サプライヤの冗長化(SUPPLIER REDUNDANCY)の欠如	
V48	Application Vulnerabilities Or Poor Patch Management	アプリケーションの脆弱性またはパッチ管理の不備	
V49	Resource Consumption Vulnerabilities	リソースの消費に関する脆弱性	
V50	Breach Of NDA By Provider	プロバイダによるNDA違反	NDA(Non-Disclosure Agreement): 秘密保持契約
V51	Liability From Data Loss (Cp)	データ喪失に対する責任(クラウドプロバイダ)	
V52	Lack Of Policy Or Poor Procedures For Logs Collection And Retention	ログの収集および保存に関するポリシーの欠如または手順の不備	
V53	Inadequate Or Misconfigured Filtering Resources	フィルタリングリソースの不備または設定ミス	

**23の資産項目(A1 - A23) (Assets)**

No.	用語	対訳	備考(原文にある説明の訳)
A1	Company Reputation	企業の評判	
A2	Customer Trust	顧客の信頼	苦情申立人が評価し得るもので、誠意が含まれる
A3	Employee Loyalty And Experience	従業員の忠誠心と経験	
A4	Intellectual Property	知的財産	
A5	Personal Sensitive Data	個人の秘密データ	(欧州のデータ保護指令の定義通り)
A6	Personal Data	個人データ	(欧州のデータ保護指令の定義通り)
A7	Personal Data - Critical	個人データ(重要)	欧州のデータ保護指令において個人データの範疇に含まれている全データ、および、組織または企業によって重要と判断または分類されるデータ
A8	HR Data	人材データ	データ保護要件以外に、運用上の見地から関係するデータ
A9	Service Delivery - Real Time Services	サービス提供 - リアルタイムによるサービス	時間が重視されるサービスで、ほぼ100%に近い可用性レベルが必要
A10	Service Delivery	サービス提供	
A11	Access Control / Authentication / Authorization (Root/Admin V Others)	アクセス制御/認証/権限付与 (root/管理者対その他)	
A12	Credentials	クレデンシャル	システムにアクセスする患者および担当者のもの
A13	User Directory (Data)	ユーザディレクトリ(データ)	これが適切に機能しなければ、誰もアクセスできない
A14	Cloud Service Management Interface	クラウドサービスの管理用インターフェース	クラウドを通じて提供されるすべてのサービスを管理する管理用インターフェース(ウェブベースまたはリモートシェル等)
A15	Management Interface APIs	管理用インターフェースAPI	
A16	Network (Connections, etc)	ネットワーク(接続等)	内部および外部クラウドの接続を含む
A17	Physical Hardware	物理的なハードウェア	
A18	Physical Buildings	物理的な建物	
A19	CP Application (Source Code)	クラウドプロバイダアプリケーション(ソースコード)	
A20	Certification	認証	ISO、PCI DSS等
A21	Operational Logs (Customer And Cloud Provider)	運用ログ(クラウド利用者およびクラウドプロバイダ)	これらログは、ビジネスプロセスを維持、最適化するため、および、監査目的で使用
A22	Security Logs	セキュリティログ	セキュリティ違反の証拠やフォレンジック解析時に有効
A23	Backup Or Archive Data	バックアップまたはアーカイブデータ	