

金融機関等コンピュータシステムの安全対策基準 第8版追補改訂

ジャパンメディアシステム株式会社

LiveOn ASPサービスにおける対応状況

2018年5月25日

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況	
設備基準（コンピュータセンター）	建物	環境	設 1	各種災害、障害が発生しやすい地域を避けること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。</p> <p>この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。</p> <p>LiveOnサーバを設置しているデータセンターは、震度7以上の耐震性を持ち、ガソリンスタンドや工場など危険な建物から離れた場所に建てられています。</p>
		周囲	設 2	立地環境の変化に伴う災害および障害の発生の可能性を調査し、防止対策を講ずること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。</p> <p>この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。</p> <p>LiveOnサーバを設置しているデータセンターは、外部からは分からない構造になっています。</p> <p>物理的なセキュリティ対策としては、有人受付、24時間365日監視カメラ稼働、ICカード入館、写真付き身分証明書提示など厳重な管理を行っています。</p>
	設 3		敷地には通路を確保すること		
	設 4		隣接物との間隔を十分にとること		
	設 5		塀または柵および侵入防止装置を設けること		
	設 6		看板等を外部に出さないこと		
	設 7		建物には避雷設備を設置すること		
	設 8		建物にはコンピュータシステム関連業務専用、または建物内においてコンピュータシステム関連業務専用の独立区画とすること		
	設 9		敷地内の通信回線・電力線は、切断・延焼の防止措置を講ずること		

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
	構造	設 10	耐火建造物であること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「物理的および環境的セキュリティ」(ISO27001:2013、附属書 A.11) が規定されています。 LiveOnサーバを設置しているデータセンターは、環境的なリスクに対する物理的な保護を備えています。
		設 11	構造の安全性を有すること	
		設 12	外壁、屋根等は十分な防水性能を有すること	
		設 13	外壁等に強度を持たせること	
	開口部	設 14	窓には防火措置を講ずること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「物理的および環境的セキュリティ」(ISO27001:2013、附属書 A.11) が規定されています。 LiveOnサーバを設置しているデータセンターのセキュリティ対策としては、有人受付、24時間365日監視カメラ稼働、ICカード入館、写真付き身分証明書提示、出入口の十分な強度の確保など厳重な管理を行っています。
		設 15	防犯措置を講ずること	
		設 16	常時利用する出入口は1カ所とし、出入管理設備、防犯設備を設置すること	
		設 17	非常口を設けること	
		設 18	防水措置を講ずること	
		設 19	出入口の扉は、十分な強度を持たせるとともに、錠を付けること	
	内装等	設 20	不燃材料および防災性能を有するものを使用すること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「物理的および環境的セキュリティ」(ISO27001:2013、附属書 A.11) が規定されています。 LiveOnサーバを設置しているデータセンターは、防火性能を有する内装を利用しており、落下防止対策も実施しています。
設 21		地震による内装等の落下・損壊の防止措置を講ずること		

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況	
	コンピュータ室・データ保管室	位置	設 22	災害を受けるおそれの少ない位置に設置すること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。 LiveOnサーバを設置しているデータセンターは、外部からは分からない構造になっています。 コンピュータ室は防火区画であり、災害や侵入の可能性の低い位置に設置しています。
			設 23	外部から容易に入れない位置に設置すること	
			設 24	室名等の表示は付さないこと	
			設 25	必要空間を確保すること	
			設 26	専用の独立した室とすること	
	開口部	設 27	常時利用する出入口は1カ所とし、前室を設けること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。 LiveOnサーバを設置しているデータセンターは、外部から分からない構造になっています。 物理的なセキュリティ対策としては、有人受付、24時間365日監視カメラ稼働、ICカード入館、出入口の十分な強度の確保など厳重な管理を行っています。	
		設 28	出入口の扉は、十分な強度を持たせるとともに、錠を付けること		
		設 29	窓に防火、防水、破損防止措置を講じ、外部から室内の機器等が見えない措置を講ずること		
		設 30	非常口、避難器具、誘導灯等を設置すること		
	構造・内装等	設 31	独立した防火区画とすること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。 LiveOnサーバを設置しているデータセンターは、環境的なリスクに対する物理的な保護を備えています。また、落下防止対策も実施しています。	
		設 32	漏水防止対策を講ずること		
		設 33	静電気の防止措置を講ずること		
		設 34	内装等には不燃材料および防災性能を有するものを使用すること		
		設 35	地震による内装等の落下・損壊の防止措置を講ずること		
		設 36	フリーアクセス床は地震時に損壊しない構造とすること		

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況		
	設備	設 37	自動火災報知設備を設置すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「物理的および環境的セキュリティ」(ISO27001:2013、附属書 A.11) が規定されています。</p> <p>LiveOnサーバを設置しているデータセンターは、環境及びセキュリティに関するリスクに対する物理的な保護を備えています。 これには、火気の検知と抑制、空気の状態を最適なレベルに調整する空調、物理的なセキュリティ制御などが含まれます。</p>		
		設 38	非常時の連絡装置を設置すること			
		設 39	消火設備を設置すること			
		設 40	ケーブルの難燃化、延焼防止措置を講ずること			
		設 41	排煙設備を設置すること			
		設 42	非常用照明設備、携帯用照明器具を設置すること			
		設 43	水使用設備を設置しないこと			
		設 44	地震感知器を設置すること			
		設 45	出入口には出入管理設備、防犯設備を設置すること			
		設 46	温湿度自動記録装置または温湿度警報装置を設置すること			
		設 47	ネズミの害を防止する措置を講ずること			
		コンピュータ 機器、什器、 備品	設 48		什器・備品は不燃性とすること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「物理的および環境的セキュリティ」(ISO27001:2013、附属書 A.11) が規定されています。</p> <p>LiveOnサーバを設置しているデータセンターは、地震を含む局地的な環境リスクに対する警報と物理的な保護を備えています。</p>
			設 49		静電気防止措置を講ずること	
			設 50		耐震措置を講ずること	
	設 51		運搬車等に固定装置を取り付けること			

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況	
	電源室・空調 機械室	設 52	災害を受けるおそれの少ない位置に設置すること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。</p> <p>LiveOnサーバを設置しているデータセンターは、環境リスクに対する物理的な保護を備えています。 これには、火気の検知と抑制、空気のコンディションを最適なレベルに調整する空調、完全に冗長化された電源システムが含まれます。 物理的なセキュリティ対策としては、有人受付、24時間365日監視カメラ稼働、ICカード入館などの制限を行っています。</p>	
設 53	保守点検に必要な空間を確保すること	設 54	専用の独立した室とすること		
設 55	無窓とし、錠を付けた扉を設置すること	設 56	耐火構造とすること		
設 57	自動火災報知設備を設置すること	設 58	ガス系消火設備を設置すること		
設 59	空調設備の漏水防止措置を講ずること	設 60	ケーブル、ダクトからの延焼防止措置を講ずること		
	電源設備	設 61	電源設備の容量には余裕を持たせること		<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。</p>
設 62	電源は複数回線で引き込むこと	設 63	良質な電力を供給する設備を設置すること		
設 64	自家発電設備、蓄電池設備を設置すること	設 65	電源設備には避雷設備を設置すること		
設 66	電源設備には耐震措置を講ずること				

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況
			設 67	分電盤からコンピュータ機器への電源の引込みは専用とすること	<p>施設内の重要かつ不可欠な箇所における電力障害に際しては、無停電電源装置（UPS）がバックアップ電力を供給します。</p> <p>また、LiveOnサーバを設置しているデータセンターは、施設全体へのバックアップ電力を供給する発電機を備えています。</p>
			設 68	負荷変動の激しい機器との共用を避けること	
			設 69	コンピュータシステムのアースは適切に施工すること	
			設 70	過電流、漏電により各機器に障害を及ぼさないよう措置を講ずること	
			設 71	防災、防犯設備用の予備電源を設置すること	
	空調設備		設 72	空調設備の能力には余裕を持たせること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。</p> <p>この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。</p> <p>LiveOnサーバを設置しているデータセンターは、環境的なリスクに対する物理的な保護を備えています。</p> <p>サーバの過熱を予防し、サービスの中断の可能性を下げるためにサーバやその他のハードウェアを一定の温度に保つには、空調が必要です。</p> <p>LiveOnサーバを設置しているデータセンターは、空気のコンディションを最適なレベルに保つよう調整されています。</p> <p>作業員とシステムが温度と湿度を適切なレベルになるよう監視及び制御を実施しています。</p>
			設 73	空調設備は安定的に空気調和できる措置を講ずること	
			設 74	空調設備はコンピュータ室専用とすること	
			設 75	空調設備の予備を設置すること	
			設 76	空調設備には自動制御装置、異常警報装置を設置すること	
			設 77	空調設備には侵入、破壊防止対策を講ずること	
			設 78	空調設備には耐震措置を講ずること	
			設 79	空調設備の断熱材料、給排気口は不燃材料とすること	

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況
	監視制御設備		設 80	監視制御設備を設置すること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。
			設 81	中央管理室を設置すること	物理的なセキュリティ対策としては、有人受付、24時間365日監視カメラ稼働、ICカード入館など厳重な管理を行っています。
	回線関連設備		設 82	回線関連設備には錠をつけること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。 物理的なセキュリティ対策としては、有人受付、24時間365日監視カメラ稼働、ICカード入館など厳重な管理を行っています。 これには、ネットワークケーブルの適切な保護も含まれています。
			設 83	回線関連設備の設置場所の表示は付さないこと	
			設 83-1	回線は、専用の配線スペースに設けること	
	設備基準（本部・営業店等）	建物	周囲	設 84	敷地内の通信回線・電力線の切断・延焼の防止措置を講ずること
構造			設 85	耐火建築物であること	対象外
			設 86	構造の安全性を有すること	対象外
			設 87	外壁、屋根等は十分な防水性能を有すること	対象外
			設 88	外壁等の強度を確保すること	対象外
開口部			設 89	窓には防火措置を講ずること	対象外
			設 90	窓・扉には防犯措置を講ずること	対象外
			設 91	出入口の扉は十分な強度を持たせるとともに、錠を付けること	対象外
			設 92	通用口には、入室者の識別設備を設置すること	対象外

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
		設 93	出入口には防水措置を講ずること	対象外
	内装等	設 94	天井および壁は、遮熱、吸音機能を持たせること	対象外
		設 95	地震による内装等の落下・損壊の防止措置を講ずること	対象外
		設 96	床表面は、塵埃や静電気が発生しにくい材質のものとする	対象外
		設 97	端末機器への回線等は、切断のおそれのない措置を講ずること	対象外
		設 98	端末機器に接続している回線、電源ケーブル等への漏水防止対策を講ずること	対象外
		設備	設 99	自動火災報知設備および消火器を設置すること
	設 100		設備等の耐震措置を講ずること	対象外
	設 101		耐火金庫を設置すること	対象外
	設 102		避雷設備を設置すること	対象外
	設 103		防犯措置を講ずること	対象外
	回線関連設備	設 104	回線関連設備の設置場所の表示は付さないこと	対象外
		設 105	回線関連設備には錠を付けること	対象外
		設 106	回線関連設備から各端末機器までの配線を二重化すること	対象外
	電源設備	設 107	電源ケーブルは、端末機器等に支障を来さないよう布設すること	対象外

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況		
		設 108	防災、防犯設備用の予備電源を設置すること	対象外		
		設 109	自家発電設備等を設置すること	対象外		
		空調設備	設 110	空調設備を設置すること	対象外	
		自動機器室	設 111	通話装置を設置すること	対象外	
			設 112	非常通報装置を設置すること	対象外	
			設 113	防犯措置を講ずること	対象外	
			設 114	照明設備および非常用照明設備を設置すること	対象外	
			設 115	扉は、一部を素通しにすること	対象外	
			設 116	自動機器の現金の装填と保守のための必要な空間を確保すること	対象外	
			設 117	自動運行設備を設置すること	対象外	
			端末機器	設 118	端末機器には耐震措置を講ずること	対象外
				設 119	機器のアースを確実に取ること	対象外
		設 120		漏水および塵埃等に対する保護措置をとること	対象外	
		サーバー設置場所	位置	設 121	災害を受けるおそれの少ない位置に設置すること	対象外
				設 122	外部から容易に入れない位置とすること	対象外
				設 123	室名等の表示は付さないこと	対象外

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況	
	構造・内装等		設 124	専用の区画とすること	対象外	
			設 125	防火区画に設置すること	対象外	
			設 126	漏水防止対策を講ずること	対象外	
			設 127	フリーアクセス床は地震に備えて耐震措置を講ずること	対象外	
		設備		設 128	消防設備を有すること	対象外
				設 129	地震感知器を設置すること	対象外
				設 130	サーバーを設置した室の出入口には出入管理設備、防犯設備を設置すること	対象外
				設 131	温湿度自動記録装置または温湿度警報装置を設置すること	対象外
			設 132	空調設備を設置すること	対象外	
			設 133	ネズミの害を防止する措置を講ずること	対象外	
	インストアブランチ		設 134	電源コンセントの抜け防止対策を講ずること	対象外	
			設 135	他の区画からの侵入防止措置を講ずること	対象外	
			設 136	使用するストアの設備状況に応じて、適切な補強策を講ずること	対象外	
	設備基準（流通・小売店舗との連携チャネル）	コンビニATM		設 137	防犯措置を講ずること	対象外

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
運用基準	管理体制の確立	運 1	セキュリティ管理方法を具体的に定めた文書を整備すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「情報セキュリティのための方針群」(ISO27001:2013、附属書A.5)と「情報セキュリティのための組織」(ISO27001:2013、附属書A.6)が規定されています。</p> <p>セキュリティポリシーを制定するとともに、社内の管理体制や責任分担を明確化したうえで、管理手順の整備を行っています。</p>
		運 2	セキュリティ管理方法を具体的に定めた文書の評価と改訂を行うこと	
		運 3	セキュリティ管理体制を整備すること	
		運 4	システム管理体制を整備すること	
		運 5	データ管理体制を整備すること	
		運 6	ネットワーク管理体制を整備すること	
	組織の整備	運 7	防災組織を整備すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「冗長性」(ISO27001:2013、附属書A.17.2)が規定されています。</p> <p>防災、防犯及び業務運営の組織体制を整備するとともに、役割分担、規則及び手順等を明確化することにより、サービス運営の安全を確保しています。</p>
		運 8	防犯組織を整備すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「人的資源のセキュリティ」(ISO27001:2013、附属書A.7)が規定されています。</p>
		運 9	業務規定を整備すること	<p>防災、防犯及び業務運営の組織体制を整備するとともに、役割分担、規則及び手順等を明確化することにより、サービス運営の安全を確保しています。</p>

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
	各種規定の整備	運 10	各種規定を整備すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「情報セキュリティのための方針群」(ISO27001:2013、附属書A.5)と「情報セキュリティのための組織」(ISO27001:2013、附属書A.6)と「運用の手順および責任」(ISO27001:2013、附属書A.12.1)が規定されています。</p> <p>ISO27001で要求される業界団体やリスク/コンプライアンス組織、地方当局や規制当局とのコンタクトを行っています。</p>
	セキュリティ遵守状況の確認	運 10-1	セキュリティ遵守状況を確認すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO27001:2013、附属書A.7.2.2)が規定されています。</p> <p>全関係社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も年1回実施するセキュリティ教育を継続的に受けています。</p>
入退管理	入退館(室)管理	運 11	資格付与および鍵の管理を行うこと	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「物理的および環境的セキュリティ」(ISO27001:2013、附属書A.11)が規定されています。</p> <p>LiveOnサーバを設置しているデータセンターは、カスタム設計された電子アクセスカード、警報、金属探知機、生体認証などの安全保護対策を施した多層セキュリティモデルによって物理的なセキュリティを確保しています。</p> <p>また、24時間365日稼働の監視カメラが設置され、侵入者を検知、追跡しています。</p>
		運 12	入退館管理を行うこと	
		運 13	入退室管理を行うこと	
運用管理	マニュアルの整備	運 14	通常時マニュアルを整備すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「操作手順書」(ISO27001:2013、附属書A.12.1.1)が規定されています。</p> <p>ISO27001の要求に従ってISMSを運用しています。</p> <p>文書・マニュアルは全て管理し、バックアップ対象のシステムに保存しています。</p>

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
		運 15	障害時・災害時マニュアルを整備すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「記録の保護」(ISO27001:2013、附属書A.12.1.1)と「事業継続マネジメントにおける情報セキュリティの側面」(ISO27001:2013、附属書A.17)が規定されています。</p> <p>システム復旧を円滑に進めるための作業手順書を作成しています。</p> <p>文書・マニュアルは全て管理し、バックアップ対象のシステムに保存しています。</p>
	アクセス権限の管理	運 16	各種資源、システムへのアクセス権限を明確にすること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「アクセス制御」(ISO27001:2013、附属書A.9)が規定されています。</p> <p>データのプライバシーとセキュリティを確保するため、それぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。</p> <p>実際には同じ物理サーバーに保存されている場合も同様です。</p>
運 17		パスワードが他人に知られないための措置を講じておくこと	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「アクセス制御」(ISO27001:2013、附属書A.9)が規定されています。</p>	
運 18		各種資源、システムへのアクセス権限の付与、見直し手続きを明確化すること	<p>システムへのアクセス権限付与ルールや手順を明確化するとともに、定期的に権限の見直しを行うとともに、パスワードの秘匿性確保の措置を講じています。</p>	
運 19		オペレータの資格確認を行うこと	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「アクセス制御」(ISO27001:2013、附属書A.9)が規定されています。</p> <p>オペレーションの実施体制、手順、ルールを明確化することにより、安全な運用を確保しています。</p>	
運 20	オペレーションの依頼・承認手続きを明確にすること			
運 21	オペレーション実行体制を明確にすること			
運 22	オペレーションの記録、確認を行うこと			
運 23	クライアントサーバー・システムにおける作業の管理を行うこと			

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
	入力管理	運 24	データの入力管理を行うこと	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「システムの取得、開発および保守」(ISO27001:2013、附属書A.14) が規定されています。</p> <p>送受信側いずれかで入力データのチェックを実施しています。</p>
	データファイル管理	運 25	授受・管理方法を定めること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「システムの取得、開発および保守」(ISO27001:2013、附属書A.14) が規定されています。</p>
運 26		修正管理方法を明確にすること	データファイルの管理手順は明確化されており、適切に管理されています。	
運 27		バックアップを確保すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「冗長性」(ISO27001:2013、附属書A.17.2) と「バックアップ」(ISO27001:2013、附属書A.12.3) が規定されています。</p> <p>データファイルはバックアップされており、適切に保管されています。</p>	
	プログラムファイル管理	運 28	管理方法を明確にすること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「システムの取得、開発および保守」(ISO27001:2013、附属書A.14) が規定されています。</p> <p>プログラムファイルの管理手順は明確化されおり、適切に管理されています。</p>
		運 29	バックアップを確保すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「冗長性」(ISO27001:2013、附属書A.17.2) と「バックアップ」(ISO27001:2013、附属書A.12.3) が規定されています。</p> <p>プログラムファイルはバックアップされており、適切に保管されています。</p>

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
	コンピュータウイルス対策	運 30	コンピュータウイルス対策を講ずること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「マルウェアからの保護」(ISO27001:2013、附属書A.12.2)が規定されています。</p> <p>プログラムおよびアンチウイルス/悪意のあるソフトウェアを管理するための手順は、ISO27001規格に準拠しています。</p>
	ネットワーク設定情報管理	運 31	設定情報の管理を行うこと	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「運用の手順および責任」(ISO27001:2013、附属書A.12.1)と「ネットワークセキュリティ管理」(ISO27001:2013、附属書A.13.1)が規定されています。</p> <p>ネットワーク設定情報の管理手続きを定めるとともに、バックアップ取得を行っています。</p>
		運 32	設定情報のバックアップを確保すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「冗長性」(ISO27001:2013、附属書A.17.2)と「バックアップ」(ISO27001:2013、附属書A.12.3)が規定されています。</p> <p>ネットワーク設定情報の管理手続きを定めるとともに、バックアップ取得を行っています。</p>
	ドキュメント管理	運 33	保管管理方法を明確にすること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「記録の保護」(ISO27001:2013、附属書A.12.1.1)が規定されています。</p> <p>アプリケーションのドキュメントの管理については、利用者側の責任となります。 弊社所管部分のドキュメントについては、所定の手続きにより管理され、バックアップ取得を実施しています。</p>

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
		運 34	バックアップを確保すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「冗長性」(ISO27001:2013、附属書A.17.2)と「バックアップ」(ISO27001:2013、附属書A.12.3)が規定されています。</p> <p>アプリケーションのドキュメントの管理については、利用者側の責任となります。 弊社所管部分のドキュメントについては、所定の手続きにより管理され、バックアップ取得を実施しています。</p>
	帳票管理	運 35	未使用重要帳票の管理方法を明確にすること	対象外
		運 36	重要な印字済帳票の取扱方法を明確にすること	対象外
	出力管理	運 37	出力情報の作成、取扱いについて、不正防止および機密保護対策を講ずること	出力情報は、都度記録される仕組みとなっています。
	取引の管理	運 38	各取引の操作権限を明確にすること	対象外
		運 39	オペレータカードの管理を行うこと	対象外
		運 40	取引の操作内容を記録・検証すること	対象外
		運 41	顧客からの届出の受付体制を整備し、事故口座の管理を行うこと	対象外
		運 42	機器および媒体の盗難、破損等に伴い、利用者が被る可能性がある損失および責任を明示すること	対象外

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
	暗号鍵の管理	運 43	暗号鍵の利用において運用管理方法を明確にすること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「暗号」(ISO27001:2013、附属書A.10) が規定されています。 LiveOnで使用している暗号鍵の管理手順・方法については、ISO27001規格に準拠して、社内の管理体制を明確化しています。
	厳正な本人確認の実施	運 44	本人確認を行うこと	対象外
		運 44-1	CD・ATM等の機械式預貯金取引における正当な権限者の取引を確保すること	対象外
	CD・ATM等および無人店舗の管理	運 45	運用管理方法を明確にし、かつ不正払戻防止の措置を講ずること	対象外
		運 46	監視体制を明確にすること	対象外
		運 47	防犯体制を明確にすること	対象外
		運 48	障害時・災害時の対応方法を明確にすること	対象外
		運 49	関係マニュアルの整備を行うこと	対象外
	渉外端末の管理	運 50	運用管理方法を明確にすること	弊社所有端末については、管理台帳にて管理しております。
	カード管理	運 51	カードの管理方法を明確にすること	対象外
		運 51-1	顧客に対して犯罪に関する注意喚起を行うこと	対象外
		運 52	指定された口座のカード取引監視方法を明確にすること	対象外

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
	顧客データ保護	運 53	顧客データの保護策を講ずること	対象外
		運 53-1	生体認証における生体認証情報の安全管理措置を講ずること	対象外
	資源管理	運 54	能力および使用状況の確認を行うこと	<p>LiveOnは、ISMS（ISO27001）認証を受けています。</p> <p>この基準では、「容量・能力の管理」（ISO27001：2013、附属書A.12.1.3）が規定されています。</p> <p>負荷状況を監視するとともに、サービスの利用状況により機器の増強等を検討しています。</p>
	外部接続管理	運 55	接続契約内容を明確にすること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。</p> <p>この基準では、「通信のセキュリティ」（ISO27001：2013、附属書A.13）と「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」（ISO27001：2013、附属書A.14.1.2）が規定されています。</p> <p>外部との接続の安全管理のため、ファイアウォールを設置しています。</p>
		運 56	外部接続における運用管理方法を明確にすること	
	機器の管理	運 57	管理方法を明確にすること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。</p> <p>この基準では、「装置」（ISO27001：2013、附属書A.11.2）が規定されています。</p> <p>各機器へのアクセスは、所定の権限を付与された者に限定しています。</p> <p>従業員が使用する機器については、管理台帳にて管理しています。</p>
		運 58	ネットワーク関連機器の保護措置を講ずること	
		運 59	保守方法を明確にすること	
	運行監視	運 60	監視体制を整備すること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。</p> <p>この基準では、「ロギングおよびモニタリング」（ISO27001：2013、附属書A.12.4）が規定されています。</p> <p>死活監視を実施しており、障害発生時に対応できる体制を整えています。</p>

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
	コンピュータ室・データ保管室の管理	運 61	入室後の作業を管理すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「物理的および環境的セキュリティ」(ISO27001:2013、附属書A.11) が規定されています。</p> <p>物理的アクセスは、入退室や各境界で厳密に管理されています。 作業実施は所定の承認を受けて実施し、記録を残すほか監視カメラによる牽制を図っています。</p>
	障害時・災害時対応策	運 62	関係者への連絡手順を明確にすること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「冗長性」(ISO27001:2013、附属書A.17.2) と「バックアップ」(ISO27001:2013、附属書A.12.3) が規定されています。</p> <p>障害発生時に対応できる体制を整えており、担当を分離させて早期解決を図れるようにしています。</p>
運 63		障害時・災害時復旧手順を明確にすること		
運 64		障害の原因を調査・分析すること		
	コンティンジェンシープランの策定	運 65	コンティンジェンシープランを策定すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「情報セキュリティ継続」(ISO27001:2013、附属書A.17.1) が規定されています。</p> <p>ビジネス継続のポリシーやプランは、ISO27001規格に準拠する形で定義されています。</p>
システム開発・変更	ハードウェア・ソフトウェア管理	運 66	ハードウェア、ソフトウェアの管理を行うこと	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「資産に対する責任」(ISO27001:2013、附属書A.8.1) と「媒体の処分」(ISO27001:2013、附属書A.8.3.2) と「装置のセキュリティを保った処分または再利用」(ISO27001:2013、附属書A.11.2.7) と「運用ソフトウェアの管理」(ISO27001:2013、附属書A.12.5) が規定されています。</p> <p>ISO27001規格に準じ、ハードウェア資産及びソフトウェア資産については、管理台帳を作成して管理しています。</p>

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
	システム開発・変更管理	運 67	開発・変更手順を明確にすること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「開発環境、試験環境および運用環境の分離」(ISO27001:2013、附属書A.12.1.4)と「開発およびサポートプロセスにおけるセキュリティ」(ISO27001:2013、附属書A.14.2)が規定されています。</p> <p>開発・変更に関する管理手順を明確化しています。</p> <p>本番環境とは別のテスト環境を用意し、事前に十分な検証を行ったうえで、本番への移行を実施しています。</p>
		運 68	テスト環境を整備すること	
		運 69	本番への移行手順を明確にすること	
	ドキュメント管理	運 70	作成手順を定めること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「情報セキュリティのための方針群」(ISO27001:2013、附属書A.5)と「情報セキュリティのための組織」(ISO27001:2013、附属書A.6)と「運用の手順および責任」(ISO27001:2013、附属書A.12.1)が規定されています。</p> <p>アプリケーション開発に係るドキュメントについては、各バージョン毎に保管し管理しています。</p>
		運 71	保管管理方法を明確にすること	
	パッケージの導入	運 72	評価体制を整備すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「システムの取得、開発および保守」(ISO27001:2013、附属書A.14)が規定されています。</p> <p>オープンソースソフトウェアを利用する場合は、レビューやリスク評価により安全性を確認した上で使用するようになっています。</p>
		運 73	運用・管理体制を明確にすること	
	システムの廃棄	運 74	廃棄計画・手順を策定すること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「媒体の処分」(ISO27001:2013、附属書A.8.3.2)と「装置のセキュリティを保った処分または再利用」(ISO27001:2013、附属書A.11.2.7)が規定されています。</p> <p>リソース見通しに基づく廃棄計画を策定しています。</p>
		運 75	情報漏洩防止対策を講ずること	

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況	
	各種設備管理	保守管理	運 76	管理方法を明確にすること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「物理的および環境的セキュリティ」（ISO27001：2013、附属書A.11）が規定されています。</p> <p>設備の管理体制、管理基準および手順を明確化するとともに、定期的な点検と結果レビューを実施しています。</p>
			運 77	保守方法を明確にすること	
		資源管理	運 78	能力および使用状況の確認を行うこと	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「容量・能力の管理」（ISO27001：2013、附属書A.12.1.3）が規定されています。</p> <p>設備の管理体制、管理基準および手順を明確化するとともに、定期的な点検と結果レビューを実施しています。 各設備に応じた管理基準を定め、余裕度を設けて監視しています。</p>
		監視	運 79	監視体制を整備すること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「ロギングおよびモニタリング」（ISO27001：2013、附属書A.12.4）が規定されています。</p> <p>各設備を自動監視し、異常検知時はアラートメールに基づき対処しています。</p>
	教育・訓練	教育・訓練	運 80	セキュリティ教育を行うこと	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO27001：2013、附属書A.7.2.2）が規定されています。</p> <p>全関係社員は、入社時研修に組み込まれたセキュリティ研修に加え、在籍期間中も年1回実施するセキュリティ教育を継続的に受けています。 また、障害時時の復旧オペレーション等も定期的に訓練しています。</p>
			運 81	要員に対するスキルアップ教育を行うこと	
			運 82	オペレーション習熟のための教育および訓練を行うこと	
運 83			障害時・災害時に備えた教育・訓練を行うこと		
運 84			防災・防犯訓練を行うこと		

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況
	要員管理	要員管理	運 85	要員の人事管理を適切に行うこと	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「人的資源のセキュリティ」(ISO27001:2013、附属書A.7) が規定されています。
			運 86	要員の健康管理を行うこと	担当の職務記述に基づくパフォーマンス評価を行うとともに、健康診断受診を義務付けています。
	外部委託管理	外部委託に関する計画	運 87	システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲を明確にすること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「供給者関係」(ISO27001:2013、附属書A.15) が規定されています。 LiveOnに関する業務の外部委託は、一切行っていません。
			運 87-1	外部委託先の選定手続きを明確にすること	
			運 88	安全対策に関する項目を盛り込んだ委託契約を締結すること	
	外部委託業務管理	外部委託業務管理	運 89	外部委託先の要員にルールを遵守させ、その遵守状況を管理、検証すること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO27001:2013、附属書A.7.2.2) が規定されています。 LiveOnに関する業務の外部委託は、一切行っていません。。
			運 90	外部委託における業務組織の整備と業務の管理、検証を行うこと	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「供給者関係」(ISO27001:2013、附属書A.15) が規定されています。 LiveOnに関する業務の外部委託は、一切行っていません。
			運 90-1	金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと	対象外

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況
	システム監査	システム監査	運 91	システム監査体制を整備すること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「情報システムの監査に対する考慮事項」(ISO27001:2013、附属書 A.12.7) が規定されています。 毎年、内部監査を行っており、ISO27001の外部監査も受けています。
	インストアブランチ		運 92	出店先の選定基準を明確にすること	対象外
	コンビニATM		運 93	出店先の選定基準を明確にすること	対象外
			運 94	現金装填等メンテナンス時の防犯対策を講じること	対象外
			運 95	障害時・災害時対応手順を明確にすること	対象外
			運 96	ネットワーク関連機器、伝送データの安全対策を講ずること	対象外
			運 97	所轄の警察および警備会社等関係者との連絡体制を確立すること	対象外
			運 98	顧客に対して犯罪に関する注意喚起を行うこと	対象外
	デビットカード	デビットカード・サービスの安全性確保	運 99	デビットカード・サービスにおける安全対策を講ずること	対象外
			運 100	口座番号、暗証番号等の安全性を確保すること	対象外
		顧客保護	運 101	デビットカード利用時の顧客保護の措置を講ずること	対象外
		顧客への注意喚起	運 102	デビットカード利用上の留意事項を顧客に注意喚起すること	対象外

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況
オープンネットワークを利用した金融サービス	インターネット、モバイル	運 103	不正使用を防止すること	対象外
		運 104	不正使用を早期発見すること	対象外
		運 105	安全対策に関する情報開示をすること	対象外
		運 105-1	顧客対応方法を明確にすること	対象外
		運 106	インターネットやモバイル等を用いた金融サービスの運用管理方法を明確化すること	対象外
	電子メール	運 107	電子メールの運用方針を明確にすること	対象外
クラウドサービスの利用		運 108	クラウドサービスの利用を行う場合は、事前に利用目的や範囲等を明確にするとともに、事業者選定の手続きを明確にすること	対象外
		運 109	クラウド事業者と安全対策に関する項目を盛り込んだ契約を締結すること	対象外
		運 110	クラウドサービス利用にあたって、データ漏洩防止策を講ずること	対象外
		運 111	クラウド契約終了時のデータ漏洩防止策を講ずること	対象外
		運 112	クラウド事業者に対する立入監査・モニタリング態勢を整備すること	対象外

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況
	サイバー攻撃 対応態勢の整備		運 113	サイバー攻撃対応態勢を整備すること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「マルウェアからの保護」（ISO27001：2013、附属書A.12.2）が規定されています。</p> <p>LiveOnは、セキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。</p>
技術基準（システム信頼性向上対策）	ハードウェアの信頼性向上対策	ハードウェアの障害予防策	技 1	予防保守を実施すること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「装置の保守」（ISO27001：2013、附属書A.11.2.4）が規定されています。</p> <p>機器の不具合を継続的にモニタリングし、問題が見つかった場合にはアラートメールが担当者へ送信されます。また、定期的な保守を実施しています。</p>
		ハードウェアの予備	技 2	本体装置の予備を設けること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「冗長性」（ISO27001：2013、附属書A.17.2）が規定されています。</p> <p>各サーバに関して、冗長化構成を取っており、万が一故障等で運用が困難になった場合には、スタンバイ機に切り替えてサービスを継続運用できるようにしています。</p>
	技 3		周辺装置の予備を設けること		
	技 4		通信系装置の予備を設けること		
	技 5		回線の予備を設けること		
	技 6	端末系装置の予備を設けること			
ソフトウェアの信頼性向上対策	開発時の品質向上対策	技 7	システム開発計画は中長期計画との整合性を確認するとともに、承認を得ること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「システムの取得、開発および保守」（ISO27001：2013、附属書A.14）が規定されています。</p>	
		技 8	必要となるセキュリティ機能を取り込むこと		
		技 9	設計段階でのソフトウェアの品質を確保すること		

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況
			技 10	プログラム作成段階での品質を確保すること	LiveOnは、変更の管理に体系的なアプローチを採用し、顧客に影響を与えるサービスの変更は徹底的な検証・試験・承認及び情報提供がなされるようになっています。
			技 11	テスト段階でのソフトウェアの品質を確保すること	
			技 12	プログラムの配布を考慮したソフトウェアの信頼性を確保すること	
			技 13	パッケージ導入にあたり、ソフトウェアの品質を確保すること	
	メンテナンス時の品質向上対策		技 14	定型的変更作業時の正確性を確保すること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「変更管理」(ISO27001:2013、附属書A.12.1.2)と「システムの取得、開発および保守」(ISO27001:2013、附属書A.14.2)が規定されています。
			技 15	機能の変更、追加作業時の品質を確保すること	LiveOnは、重要なサービスの変更に対する自己監査により、品質のモニタリング、高い基準の維持、変更管理プロセスの継続的な改善を行っています。
	運用時の信頼性向上対策	運用時の信頼性向上対策	技 16	オペレーションの自動化、簡略化を図ること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「システムの取得、開発および保守」(ISO27001:2013、附属書A.14)が規定されています。 重要なコマンドの投入にあたっては相互確認を実施するとともに、サーバの負荷状況を監視しています。
			技 17	オペレーションのチェック機能を充実すること	
			技 18	負荷状態の監視制御機能を充実すること	
			技 19	CD・ATM等の遠隔制御機能を設けること	対象外

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況
	障害の早期発見・早期回復	障害の早期発見	技 20	システム運用状況の監視機能を設けること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「ロギングおよびモニタリング」（ISO27001：2013、附属書A.12.4）が規定されています。
			技 21	障害の検出および障害箇所の切り分け機能を設けること	各種ツールを利用した監視を実施するとともに、異常イベントの記録機能により障害箇所の切り分けを実施しています。
	障害の早期回復		技 22	障害時の縮退・再構成機能を設けること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「ロギングおよびモニタリング」（ISO27001：2013、附属書A.12.4）が規定されています。 冗長化構成を取り、障害時にサービスに影響を及ぼさないような対策は取っています。 また、ディザスタリカバリ対策も実施しており、サービスを継続運用できる態勢を取っています。
			技 23	取引制限機能を設けること	対象外
			技 24	リカバリ機能を設けること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「冗長性」（ISO27001：2013、附属書A.17.2）が規定されています。 データベースに関して、日次バックアップを取得しています。
	災害時対策	バックアップサイト	技 25	バックアップサイトを保有すること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「冗長性」（ISO27001：2013、附属書A.17.2）が規定されています。 遠隔地にバックアップサイトを保有しています。

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況	
技術基準（安全性侵害対策）	データ保護	漏洩防止	技 26	暗証番号・パスワード等は他人に知られないための対策を講ずること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「アクセス制御」（ISO27001：2013、附属書A.9）が規定されています。 パスワードルールの規制機能はないが、非表示・非印字の対策を取っています。
			技 27	相手端末確認機能を設けること	対象外
			技 28	蓄積データの漏洩防止策を講ずること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「暗号」（ISO27001：2013、附属書A.10）が規定されています。
			技 29	伝送データの漏洩防止策を講ずること	データベースの暗号化を実施しています。 また、伝送経路や伝送データの暗号化も実施しています。
	破壊・改ざん防止	技 30	ファイルに対する排他制御機能を設けること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「システムの取得、開発および保守」（ISO27001：2013、附属書A.14）が規定されています。	
		技 31	ファイルに対するアクセス制御機能を設けること	自身のデータに関する制御と所有権を保持し、不良データの検出機能を実装することが可能です。	
		技 32	不良データ検出機能を充実すること		
	検知策	技 33	伝送データの改ざん検知策を講ずること	LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「ロギングおよびモニタリング」（ISO27001：2013、附属書A.12.4）が規定されています。	
		技 34	ファイル突合機能を設けること	データ管理ポリシーは、ISO27001規格に準拠しています。	

基準大項目	中項目	項番	小項目	LiveOn ASPサービスの対策実施状況	
	不正使用防止	予防策（アクセス権限確認）	技 35	本人確認機能を設けること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「アクセス制御」（ISO27001：2013、附属書A.9）が規定されています。</p> <p>ID/パスワードによる認証機能を実施しています。 また、アクセス権限を管理し、ログの記録も実施しています。</p>
			技 35-1	生体認証の特性を考慮し、必要な安全対策を検討すること	対象外
			技 36	IDの不正使用防止機能を設けること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「アクセス制御」（ISO27001：2013、附属書A.9）が規定されています。</p> <p>ログイン試行に試みたログを監視し、アクセスを試みた形跡が発生した場合にアラートメールを担当者に送信して検知しています。</p>
			技 37	アクセス履歴を管理すること	<p>LiveOnは、ISMS（ISO27001）認証を受けています。 この基準では、「アクセス制御」（ISO27001：2013、附属書A.9）が規定されています。</p> <p>利用者の会議システム利用状況履歴（保管期間：1年間）を保管しています。 また、管理者側のサーバ等へのアクセス履歴も残しています。</p>
	予防策（利用範囲の制限）	技 38	取引制限機能を設けること	対象外	
		技 39	事故時の取引禁止機能を設けること	対象外	
	予防策（不正・偽造防止対策）	技 40	カードの偽造防止対策のための技術的措置を講ずること	対象外	
		技 41	電子的価値の保護機能、または不正検知の仕組みを設けること	対象外	

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況
			技 42	電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「暗号」(ISO27001:2013、附属書A.10) が規定されています。 LiveOnで使用している暗号鍵の管理手順・方法については、ISO27001規格に準拠して、社内の管理体制を明確化しています。
			技 42-1	電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること	対象外
	外部ネットワークからのアクセス制限		技 43	外部ネットワークからの不正侵入防止機能を設けること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「ネットワークおよびネットワークサービスへのアクセス」(ISO27001:2013、附属書A.9.1.2) と「ネットワークセキュリティ管理」(ISO27001:2013、附属書A.13.1) が規定されています。
			技 44	外部ネットワークからアクセス可能な接続機器は必要最小限にすること	ファイアウォールを設置して、不要なポートを遮断しています。
	検知策		技 45	不正アクセスの監視機能を設けること	LiveOnは、ISMS (ISO27001) 認証を受けています。 この基準では、「ネットワークおよびネットワークサービスへのアクセス」(ISO27001:2013、附属書A.9.1.2) と「ネットワーク管理策」(ISO27001:2013、附属書A.13.1.1) が規定されています。 常時アクセスログを監視し、アクセスを試みた形跡が発生した場合、アラートメールを担当者に送信しています。
			技 46	異常な取引状況を把握するための機能を設けること	対象外
			技 47	異例取引の監視機能を設けること	対象外

基準大項目	中項目		項番	小項目	LiveOn ASPサービスの対策実施状況
		対応策	技 48	不正アクセスの発生に備えて対応策、復旧策を講じておくこと	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「ネットワークおよびネットワークサービスへのアクセス」(ISO27001 : 2013、附属書A.9.1.2) と「ネットワーク管理策」(ISO27001 : 2013、附属書A.13.1.1) が規定されています。</p> <p>アクセスログを取得し、不正アクセスが疑われる場合の対応策及び復旧策を整備しています。</p>
不正プログラム防止	防御策	技 49	コンピュータウイルス等不正プログラムへの防御対策を講ずること	<p>LiveOnは、ISMS (ISO27001) 認証を受けています。</p> <p>この基準では、「マルウェアからの保護」(ISO27001 : 2013、附属書A.12.2) が規定されています。</p> <p>ウイルス対策ソフトを導入するとともに、復旧手段を整備しています。</p>	
	検知策	技 50	コンピュータウイルス等不正プログラムの検知対策を講ずること		
	復旧策	技 51	コンピュータウイルス等不正プログラムによる被害時対策を講ずること		