別記3

■浜松市ASP・SaaSセキュリティチェックリスト

各チェック項目の充足有無を"回答"欄にご回答ください。また、そのように考える根拠を"回答根拠"欄にご回答ください。

【回答凡例】○：チェック項目を満たす　×：チェック項目を満たさない　△：本市と相談が必要(例：チェック項目は満たさないが、代替策により同水準のセキュリティレベルの確保が必要な場合

事業者名：

システム名：

チェックリスト			事業者回答	
No	分類	チェック項目	回答	回答根拠(対応状況、実現方法 等)
例	○○	○○の対策が実施されていること。	○	当社サービスでは○○の機能を有しており、本機能で○○できることから、本チェック項目を満たすと考える。
（1）セキュリティに関するチェックリスト				
1	人的対策	組織として情報セキュリティポリシーが定められており、全ての従業員等に対して、適切な教育・訓練等を実施することにより、ポリシーの遵守が徹底されていること。		
2	ファシリティ	本サービスで扱うデータは、日本国内のデータセンタでのみ保管されること。		
3	アクセス制御	正当な権限を有する利用者のみがサービスや機能を利用できるように、アクセス制御ができること。		
4	保管データの暗号化	本サービスで扱うデータを保護するために、保管データの暗号化による対策が実施されること。		
5	通信の暗号化	本サービスで扱うデータの通信において、データの盗聴、改ざん等から保護するために、通信の暗号化による対策が実施されること。		
6	証跡管理	情報セキュリティインシデント等発生時にその原因分析等ができるよう、利用者の活動等に係るログが管理されること。		
7	マルウェア対策	マルウェアから保護するために、マルウェアの検出、予防、回復のための対策が実施されること。		
8	脆弱性対策	本サービスに関係する技術的脆弱性に関する情報を速やかに入手するとともに、当該脆弱性に対する対応策が検討・実施されること。		
9	BCP	大規模災害等の緊急時においても情報セキュリティ及び情報セキュリティマネジメント継続のためのルールが組織的に策定されていること。		
10	サービス終了時のデータ消去	本サービスの利用終了から一定期間以内に本市データが完全に消去されること。		
※No11~16は本サービスで個人情報を扱う場合のみご回答ください。				
11	情報資産分類	機密レベルに応じた情報セキュリティポリシーが定められており、個人情報等は機密性の高い情報として、別途情報管理の仕組みが設けられていること。		
12	個人情報保護法等遵守	個人情報保護法及び関連するガイドラインの要求事項に従った個人情報保護管理が実施されること。		

別記3

チェックリスト				事業者回答	
No	分類	チェック項目		回答	回答根拠(対応状況、実現方法 等)
13	重大インシデント	過去3年以内に、個人情報に関する重大なインシデントが発生していないこと。			
14	IPアドレス認証等	ID/パスワードに加え、IPアドレス等他要素によるアクセス制御ができること。			
15	個人情報に関するログ	個人情報の入力・出力に係るシステムログ(操作者、操作日時、操作内容)が管理されること。			
16	セキュリティ監査	定期的に本サービスに関するセキュリティ監査(内部または外部)が実施されていること。			
※No17は本サービスのシステム構成要素として、他事業者のサービスを含む場合のみご回答ください。					
17	サプライチェーン	本サービスのシステム構成要素として、他事業者のクラウドサービス・レンタルサーバ等が含まれている場合も、本サービスのセキュリティインシデント等の発生においては、全面的に貴社にてユーザサポートが実施されること。			
（2）その他要件に関するチェックリスト					
18	データの所有権	本市が本サービスで扱うデータの所有権は本市に帰属すること。			
19	バックアップ	障害が発生した際に、適切にデータ復旧ができるように、本サービスの中で、バックアップができること。			
20	動作環境	本サービス利用に際して、クライアント端末側では標準ブラウザを除くソフトウェアやプライグインのインストール、OSやブラウザ等の設定変更が必要ないこと。			
21	最新OS等への対応	最新バージョンのクライアント端末側OSやブラウザを速やかにサポート対象とすること。			
22	法制度改正対応	既存の法制度の改正対応は、サービスのバージョンアップ等により本サービス提供の範囲内で実施されること。			
23	サービス変更通告	サービス提供者の都合により、サービスの内容を変更する場合は、本市に対して、遅くとも1ヶ月以上前に、その旨と通知すること。			
24	サービス終了通告	サービス提供者の都合により、サービスを終了する場合は、本市に対して、サービス終了の遅くとも6ヶ月以上前に、その旨を通知すること。			
25	サービス終了時のデータ移行	本サービスの利用終了に際して、サービスで保管されているデータを二次利用できるように、汎用的なデータ形式で出力して、本市に引き渡せること。			
（3）【参考】認証取得状況 ※あくまで参考に回答を求めるものであり、下記の認証取得を必須とするものではありません。					
26	認証取得	右記の認証取得状況を回答してください。	ISMAP		－
			Pマーク(プライバシーマーク)		－
			ISO27001		－
			ISO27017		－
			ISO27018		－

■浜松市ASP・SaaSセキュリティチェックリスト【回答例】

各チェック項目の充足有無を"回答"欄にご回答ください。また、そのように考える根拠を"回答根拠"欄にご回答ください。

【回答凡例】○：チェック項目を満たす　×：チェック項目を満たさない　△：本市と相談が必要(例：チェック項目は満たさないが、代替策により同水準のセキュリティレベルの確保が必要な場合

事業者名：○○○○株式会社

システム名：○○○○システム

チェックリスト			事業者回答(回答例)	
No	分類	チェック項目	回答	回答根拠(対応状況、実現方法 等)
例	○○	○○の対策が実施されていること。	○	当社サービスでは○○の機能を有しており、本機能で○○できることから、本チェック項目を満たすと考える。
（1）セキュリティに関するチェックリスト				
1	人的対策	組織として情報セキュリティポリシーが定められており、全ての従業員等に対して、適切な教育・訓練等を実施することにより、ポリシーの遵守が徹底されていること。	○	弊社では「情報セキュリティ基本方針」、「情報セキュリティ対策基準」を定めており、年1回社員に対して、e-Learning研修を受講させているため、本チェック項目を満たすと考える。
2	ファシリティ	本サービスで扱うデータは、日本国内のデータセンタでのみ保管されること。	○	データは東京都に所在するデータセンターに保管されるため、本チェック項目を満たすと考える。
3	アクセス制御	正当な権限を有する利用者のみがサービスや機能を利用できるように、アクセス制御ができること。	○	本サービスでは権限制御の機能を有しており、本機能で本サービス及び機能群単位でのアクセス制御ができることから、本チェック項目を満たすと考える。
4	保管データの暗号化	本サービスで扱うデータを保護するために、保管データの暗号化による対策が実施されること。	○	本サービスは○○社のIaaSサービスを用いて構築していますが、同社から提供される暗号化サービスにより、保管データは全て暗号化されているため、本チェック項目を満たすと考える。
5	通信の暗号化	本サービスで扱うデータの通信において、データの盗聴、改ざん等から保護するために、通信の暗号化による対策が実施されること。	○	端末・サーバ間のデータは、全て暗号化(SSL暗号化)した上で、通信しているため、本チェック項目を満たすと考える。
6	証跡管理	情報セキュリティインシデント等発生時にその原因分析等ができるよう、利用者の活動等に係るログが管理されること。	○	操作ログ(操作者ID、操作内容、操作日時 等)、認証ログ(ログイン操作者ID、エラーの回数 等)等のログを取得・管理していることから、本チェック項目を満たすと考える。
7	マルウェア対策	マルウェアから保護するために、マルウェアの検出、予防、回復のための対策が実施されること。	○	本サービスを構成するサーバではウィルス対策ソフト(○○社製)を導入しており、通信経路上にはWAFも整備している。このため、弊社の考える十分なマルウェア対策を実施していることから、本チェック項目を満たすと考える。

チェックリスト			事業者回答(回答例)	
No	分類	チェック項目	回答	回答根拠(対応状況、実現方法 等)
8	脆弱性対策	本サービスに関係する技術的脆弱性に関する情報を速やかに入手するとともに、当該脆弱性に対する対応策が検討・実施されること。	○	IPAやJPCERTコーディネーションセンター等から発信される脆弱性情報を随時確認して、本サービスに関係する脆弱性情報がある場合には、速やかにセキュリティパッチを適用するなどの対応をしているため、本チェック項目を満たすと考える。
9	BCP	大規模災害等の緊急時においても情報セキュリティ及び情報セキュリティマネジメント継続のためのルールが組織的に策定されていること。	○	弊社では「情報セキュリティ事業継続計画(BCP)」を定めており、年1回社員に対して、e-Learning研修を受講させているため、本チェック項目を満たすと考える。
10	サービス終了時のデータ消去	本サービスの利用終了から一定期間以内に本市データが完全に消去されること。	○	本サービスの利用終了後、3ヶ月後に当該顧客のデータを消去するルールとしているため、本チェック項目を満たすと考える(詳細は利用約款○条参照(https://www.xxxxxx.com))。
※No11~16は本サービスで個人情報を扱う場合のみご回答ください。				
11	情報資産分類	機密レベルに応じた情報セキュリティポリシーが定められており、個人情報等は機密性の高い情報として、別途情報管理の仕組みが設けられていること。	○	弊社では顧客から提供されるデータについて、機密レベルに応じて、3つの分類を設けており、そのうち個人情報を含むデータは最上位の分類と位置付け、技術的対策、物理的対策、人的対策いずれも最も厳格な対策を実施していることから、本チェック項目を満たすと考える。
12	個人情報保護法等遵守	個人情報保護法及び関連するガイドラインの要求事項に従った個人情報保護管理が実施されること。	○	個人情報保護法等に基づき、本サービスのセキュリティ要件を定めていることから、本チェック項目を満たすと考える。
13	重大インシデント	過去3年以内に、個人情報に関する重大なインシデントが発生していないこと。	○	過去3年以内に個人情報の流出・損失等の重大なインシデントは発生していないため、本チェック項目を満たすと考える。

チェックリスト			事業者回答(回答例)	
No	分類	チェック項目	回答	回答根拠(対応状況、実現方法 等)
14	IPアドレス認証等	ID/パスワードに加え、IPアドレス等他要素によるアクセス制御ができること。	△	本サービスでは、管理者権限において、個人情報を参照することができるため、管理者権限のログインにはワンタイムパスワードを用いた多要素認証を行っています。本要件で左記チェックリストのセキュリティ水準を満たすかご相談させてください。
15	個人情報に関するログ	個人情報の入力・出力に係るシステムログ(操作者、操作日時、操作内容)が管理されること。	△	本サービスでは、個人情報個別の入力・出力等の操作ログは取得できませんが、個人情報の入力・出力権限を有する管理者のログインにおける認証ログは取得できます。本要件で左記チェックリストのセキュリティ水準を満たすかご相談させてください。
16	セキュリティ監査	定期的に本サービスに関するセキュリティ監査(内部または外部)が実施されていること。	○	本サービスリリース時に、○○監査事務所のセキュリティ監査を受けるとともに、年1回同事務所の監査を受けており、その際の指摘事項に対して、改善策を講じていることから、本チェック項目を満たすと考える。
※No17は本サービスのシステム構成要素として、他事業者のサービスを含む場合のみご回答ください。				
17	サプライチェーン	本サービスのシステム構成要素として、他事業者のクラウドサービス・レンタルサーバ等が含まれている場合も、本サービスのセキュリティインシデント等の発生においては、全面的に貴社にてユーザサポートが実施されること。	○	本サービスは○○社のIaaSサービスを用いて構築していますが、本IaaSサービスでの障害発生時においても、顧客への各種連絡・サポート等は全て弊社で行うため、本チェック項目を満たすと考える。
（2）その他要件に関するチェックリスト				
18	データの所有権	本市が本サービスで扱うデータの所有権は本市に帰属すること。	○	顧客が登録したデータの所有権は全て顧客に属するルールとしているため、本チェック項目を満たすと考える(詳細は利用約款○条参照(https://www.xxxxxx.com))。
19	バックアップ	障害が発生した際に、適切にデータ復旧ができるように、本サービスの中で、バックアップができること。	○	日次、3世代のデータバックアップを取得しており、障害が発生した場合はそのデータをもとにリストアができるため、本チェック項目を満たすと考える。
20	動作環境	本サービス利用に際して、クライアント端末側では標準ブラウザを除くソフトウェアやプライグインのインストール、OSやブラウザ等の設定変更が必要ないこと。	○	標準的なブラウザ(Microsoft Edge、Google Chrome、Mozilla Firefox)から利用できるため、本チェック項目を満たすと考える。
21	最新OS等への対応	最新バージョンのクライアント端末側OSやブラウザを速やかにサポート対象とすること。	○	最新のOSやブラウザがリリースされる際には、最新版での操作検証・画面検証等を行い、速やかにサポート対象としていることから、本チェック項目を満たすと考える。

チェックリスト				事業者回答(回答例)	
No	分類	チェック項目		回答	回答根拠(対応状況、実現方法 等)
22	法制度改正対応	既存の法制度の改正対応は、サービスのバージョンアップ等により本サービス提供の範囲内で実施されること。		○	最新の法制度に準拠するよう、適宜サービスのバージョンアップをしているため、本チェック項目を満たすと考える。
23	サービス変更通告	サービス提供者の都合により、サービスの内容を変更する場合は、本市に対して、遅くとも1ヶ月以上前に、その旨と通知すること。		○	サービスの内容を変更する場合は、3ヶ月以上前に、顧客の登録メールアドレス宛に通知するルールとしているため、本チェック項目を満たすと考える(詳細は利用約款○条参照(https://www.xxxxxx.com))。
24	サービス終了通告	サービス提供者の都合により、サービスを終了する場合は、本市に対して、サービス終了の遅くとも6ヶ月以上前に、その旨を通知すること。		○	サービスを終了する場合は、6ヶ月以上前に、顧客の登録メールアドレス宛に通知するルールとしているため、本チェック項目を満たすと考える(詳細は利用約款○条参照(https://www.xxxxxx.com))。
25	サービス終了時のデータ移行	本サービスの利用終了に際して、サービスで保管されているデータを二次利用できるように、汎用的なデータ形式で出力して、本市に引き渡せること。		○	本サービスで扱うデータは、常時CSV形式で出力できる機能を備えているため、本機能を用いて、顧客にて利用終了間際にデータ出力することにより、本チェック項目を満たすと考える。
(3)【参考】認証取得状況 ※あくまで参考に回答を求めるものであり、下記の認証取得を必須とするものではありません。					
26	認証取得	右記の認証取得状況を回答してください。	ISMAP		–
			Pマーク(プライバシーマーク)	○	–
			ISO27001		–
			ISO27017		–
			ISO27018		–

■参照ドキュメントの規定

No	分類	参照ドキュメント	規定
1	人的対策	・ISMAP/7.2.2	組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。
		・対策ガイドライン/Ⅱ.4.1.1.	取り扱う各情報資産について管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にした上で管理するとともに、文書化すること。
		・対策ガイドライン/Ⅱ.5.2.1.	全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。
		・対策ガイドライン/Ⅱ.5.2.3.	従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えること
2	サプライチェーン	・対策ガイドライン/Ⅱ.8.1.	クラウドサービスの提供に支障が生じた場合には、その原因がサプライチェーンの事業者に起因するものであったとしても、利用者と直接契約を結ぶ事業者が、その責任において一元的にユーザサポートを実施すること。
3	ファシリティ	・ASP基本要綱/第3条-2	LGWAN-ASP サービスを提供するために用いる外部IDC 等の設置場所は、日本国内に限る。
4	アクセス制御	・ISMAP/9.2.1	アクセス権の割当てを可能にするために、利用者の登録及び登録者削除についての正式なプロセスを実施する。
		・対策ガイドライン/Ⅱ.4.4.2.	事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス及び利用者データへのアクセスを、利用者が制限できるようにアクセス制御を提供すること。
		・対策ガイドライン/Ⅱ.4.4.5.	利用者及びシステム管理者等のアクセスを管理するために、適切な認証方法、特定の場所や装置からの接続を認証する方法等によって、アクセス制御となりすまし対策を行うこと。また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法とパスワードの有効期限を規定に含めること。
		・対策ガイドライン/Ⅲ.1.1.7.	パスワード管理システムは、対話式とすること、また、良質なパスワードとすること。パスワードの文字数等については、情報資産の機密度合いやリスクの大きさを考慮して、具体的なルールについては、組織が自主的に定めること。
5	保管データの暗号化	・ISMAP/10.1.1	情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。
		・対策ガイドライン/Ⅱ.7.1.5.	暗号化機能は、関連する全ての協定、法令及び規制を順守して用いるとともに、利用者が法令及び規制の順守をレビューできるように、事業者は実施している暗号による対応策を記載すること。
6	通信の暗号化	・対策ガイドライン/Ⅳ.3.1.6.	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。
7	証跡管理	・ISMAP/12.4.1	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。
		・対策ガイドライン/Ⅲ.1.1.3.	クラウドサービスの稼働監視、障害監視、パフォーマンス監視及びセキュリティインシデント監視を行うこと。また、クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率を規定すること。稼働停止や異常を検知した場合は、利用者に速報すること。また、結果を評価・総括して、管理責任者に報告すること。
		・ISMAP/12.2.1	マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施する。

8	マルウェア対策	・対策ガイドライン/Ⅲ.1.1.11.	マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。
		・対策ガイドライン/Ⅲ.2.1.1.	クラウドサービスの提供に用いるアプリケーション（データ・プログラム等）についてウイルス等に対する対策を講じること。
9	脆弱性対策	・ISMAP/12.6.1	利用中の情報システムの技術的ぜい弱性に関する情報は、時期を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。
		・対策ガイドライン/Ⅲ.1.1.16.	利用中のシステムの技術的ぜい弱性に関する情報は、時機を失せずに入手すること。また、そのようなぜい弱性に組織がさらされている状況を評価すること。さらに、それらと関連するリスクに対処するために、適切な手段をとること。また、事業者は、提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報を利用者が利用できるようにすること。
10	個人情報管理	・ISMAP/18.1.4	プライバシー及び個人識別情報（PII）の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。
		・対策ガイドライン/Ⅱ.7.1.1.	個人情報(特に要配慮個人情報を含む)、プライバシー情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。また、クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）について、法令、契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理するとともに、利用者から求められたときには提供すること。
11	BCP	・ISMAP/17.1.1	組織は、困難な増強（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。
		・対策ガイドライン/Ⅱ.9.1.1.	組織は、大規模災害等における情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定するとともに、プロセス・手順・対策を確立、文書化し、実施、維持すること。
12	サービス終了	・ISMAP/8.1.5.P	クラウドサービスの事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時期を失せずに返却又は除去する。

ISMAP：ISMAP管理基準（https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028&sys_kb_id=d1f3e275838706102668f3a8beaad354&spa=1）

対策ガイドライン：総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」
（https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nd245620.html）

ASP基本要綱：J-LIS「総合行政ネットワークASP基本要綱」
（https://www.j-lis.go.jp/lgwan/asp/regulation/cms_15763841.html）