セキュリティ要件チェックシート

No	チェック項目	項目の説明	要件	補足事項
1	アクセス制御 （利用者の認証機能）	本システムの利用者IDの認証方式および多要素認証の有無 多要素認証の例）　生体認証（指紋など)、OTP(ワンタイムパスワード）、SMS(ショートメッセージ、メール)認証、クライアント証明書 など	ID/パスワードによる認証方式	半角大文字、小文字、数字からなる8文字以上
2	アクセス制御 （管理者の認証機能）	本システムの管理者IDの認証方式および多要素認証の有無 多要素認証の例）　生体認証（指紋など)、OTP(ワンタイムパスワード）、SMS(ショートメッセージ、メール)認証、クライアント証明書 など	ID/パスワードによる認証方式	半角大文字、小文字、数字からなる8文字以上
3	データベース （暗号化対策）	データベースの暗号化対策関する有無および対象について	全データベースを対象に実施	
4	データベース （バックアップ）	データのバックアップ取得の方法について ・頻度 ・何世代分 ・保管方法	・頻度：日次 ・世代管理：全データベースを対象に過去7日分 ・保管方法：AWS S3に保管	
5	ネットワーク通信 （アクセス元IP制限）	アクセス元のIPアドレスによる限定の有無について	管理画面はクライアント証明書によるアクセス制限を実施済み	
6	ネットワーク通信 （暗号化）	通信経路の暗号化の有無および実現内容について	TLS1.2以上によるHTTPS（SSL）通信を利用	
7	ネットワーク通信 （不正アクセス対策）	外部からの不正アクセスを防止するための機能について 機能例）　DDoS(大量アクセス)防止機能、WAF、IDS/IPS、UTM	DDoS(大量アクセス)防止機能については、AWSの機能により実施・検知されています。 IDS/IPSについては現状実装されていません。 以下ヘッダー項目設定 ・Strict-Transport-Securityヘッダー ・Content-Type-Optionsヘッダー ・X-Frame-Optionsヘッダー：DENY ・X-XSS-Protectionヘッダー ・Content-Security-Policyヘッダー	
9	プログラムの改ざん検知	実行プログラムの改ざん検知について	本システムはAWS ECSにてコンテナ上で動作しており、こちらは本来読み書き可能となりますが、読み取り専用として設定を行っているためプログラムの改竄は発生しない想定です	
8	マルウェア対策	実行プログラムのマルウェア対策について	本システムはAWS ECSにてコンテナ上で動作しており、読み取り専用としているためマルウェア対策についてはホストマシンであるAWS側の責任範囲となります	
10	監査ログ （利用者証跡）	サービス利用の証跡(ログ)をどのレベルまで取得することができるか	補足事項にあるログ項目を実装済	・ログの種類：HTTPSリクエストメソッド、IPアドレス、SHOPID、USERID ・保管期間：保管期間１年
11	脆弱性診断	本システムを構成するサーバやネットワーク機器、アプリケーションへの、システムのリリースや機能追加/更新時に脆弱性診断を実施について	・実施タイミング： 23年5月末の追加開発含めたリリース完了後、6月に実施 その後は、追加リリース時に脆弱性診断を実施する予定	※年次の定期実施については要検討
12	脆弱性対策	セキュリティパッチの適用やバージョンアップの実施について	OSのセキュリティパッチは随時適用しています。 ミドルウェアについてはシステムへの影響を考慮して適用の判断を行っています。	