

【別紙5】セキュリティ要件

記載内容
<p>AT-1-1 通信経路の分離 ・不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。</p>
<p>AT-1-2 不正通信の遮断 ・通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルやアプリケーションの通信を通信回線上にて遮断する機能を備えること。</p>
<p>AT-1-3 通信のなりすまし防止 ・情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えること。 また、電子メールのなりすましの防止策を講ずること。その際、DMARCによる対策は必須とし、送信側の対策はSPF及びDKIMのいずれか又は両方により実施し、受信側の対策はSPF及びDKIMの両方により実施すること。</p>
<p>AT-1-4 サービス不能化の防止 ・サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。</p>
<p>AT-2-1 不正プログラムの感染防止 ・不正プログラム(ウイルス、ワーム、ボット等)による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染や感染拡大を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。</p>
<p>AU-1-2 ログの保護 ・ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護(消失及び破壊や改ざん等の脅威の軽減)のための措置を含む設計とすること。</p>
<p>AU-1-3 時刻の正確性確保 ・情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。</p>
<p>AU-2-1 侵入検知 ・不正行為に迅速に対処するため、農林水産省内外で送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。</p>
<p>AU-2-2 サービス不能化の検知 ・サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。</p>
<p>AC-2-2 アクセス権管理 ・情報システムの利用範囲を利用者の職務や信用情報に応じて制限するため、情報システムのアクセス権を職務や信用情報に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。</p>
<p>AC-2-3 管理者権限の保護 ・特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。</p>
<p>PR-1-1 通信経路上の盗聴防止 ・通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズム及び鍵長については、「電子政府推奨暗号リスト」を参照し決定すること。</p>
<p>PR-1-2 保存情報の機密性確保 ・情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、外部との接続のある情報システムにおいて保護すべき情報を利用者が直接アクセス可能な機器に保存しないこと。</p>
<p>PR-1-3 保存情報の完全性確保 ・情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。</p>
<p>DA-1-1 システムの構成管理 ・情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成(ハードウェア、ソフトウェア及びサービス構成に関する詳細情報)が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。</p>
<p>SC-2-1 調達する機器等に不正プログラム等が組み込まれることへの対策 ・機器等の製造工程において、農林水産省が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。</p>
<p>UP-1-1 情報セキュリティ水準低下の防止 ・情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。</p>
<p>UP-2-1 プライバシー保護 ・情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。</p>
<p>AT-3-1 構築時の脆弱性対策 ・情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。</p>
<p>PH-1-2 侵入の物理的対策 ・物理的手段によるセキュリティ侵害に対抗するため、情報システムの構成装置(重要情報を扱う装置)については、外部からの侵入対策が講じられた場所に設置すること。</p>
<p>AT-3-2 運用時の脆弱性対策 ・運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。</p>

SC-1-1 委託先において不正プログラム等が組み込まれることへの対策
・情報システムの構築において、農林水産省が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類(例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図)を提出すること。本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、農林水産省が情報セキュリティ監査の実施を必要と判断した場合は、受託者は情報セキュリティ監査を受け入れること。
また、役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して、情報セキュリティを確保すること。

農林水産省ドメイン(maff.go.jp)のサブドメインについては、農林水産省のドメイン管理ルールに従い命名等を行うこととし、農林水産省の指示に従うこと。

【別紙6】資料閲覧申請書

農林水産省大臣官房デジタル戦略グループ
デジタル政策推進チーム 宛

資料閲覧申請書

「令和7年度農林水産省次期オンライン申請システムの導入業務」に係る資料閲覧を申請します。

申込日： 令和 年 月 日

1 会社名：

2 住所：

3 部署名・担当者名：

4 電話番号：

5 E-mail アドレス：

6 閲覧日時：第1候補日 令和 年 月 日 時 分～ 時 分
第2候補日 令和 年 月 日 時 分～ 時 分
第3候補日 令和 年 月 日 時 分～ 時 分

7 閲覧者氏名：

：
：
：
：

【別紙7】機密保持誓約書

農林水産省大臣官房デジタル戦略グループ
デジタル政策推進チーム 宛

機密保持誓約書

「令和7年度農林水産省次期オンライン申請システムの導入業務」に係る資料閲覧に当たり、下記の事項を遵守することを誓約します。

記

- 1 農林水産省の情報セキュリティに関する規程等を遵守し、農林水産省が開示した情報（公知の情報を除く。）を本調達の目的以外に使用、又は第三者に開示、若しくは漏洩することのないよう、必要な措置を講じます。
- 2 閲覧資料については、複製及び撮影を行いません。
- 3 本業務に係る調達の期間中及び終了後に関わらず、守秘義務を負います。
- 4 上記1～3に反して、情報の開示、漏えい若しくは使用した場合、法的な責任を負うものであることを確認し、これにより農林水産省が被った一切の損害を賠償します。また、その際には秘密保持に関する農林水産省の監査を受けることとし、誠実に対応します。

令和 年 月 日

住 所

会 社 名

代表者名

【別紙8】質問書

事業者名：

日付： 令和 年 月 日

No.	資料名	頁	仕様書の該当記載内容	分類 (意見/質問)	意見/質問内容
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

【別紙9】証明書別添資料

仕様書 該当箇所	仕様書 記載内容	回答欄
<p>9 入札参加資格に関する事項 (1) 競争参加資格</p>	<p>ア 予算決算及び会計令第70条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であつて、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。 イ 公告日において令和7・8・9年度全省庁統一資格の「役務の提供等」の「A」、「B」、「C」等級に格付けされ、競争参加資格を有する者であること。</p>	
<p>9 入札参加資格に関する事項 (2) 公的な資格や認証等の取得</p>	<p>ア 応札者は、品質マネジメントシステムに係る以下のいずれかの条件を満たすこと。 (ア) 品質マネジメントシステムの規格である「JIS Q 9001」又は「ISO9001」（登録活動範囲が情報処理に関するものであること。）の認定を、業務を遂行する組織が有しており、認証が有効であること。 (イ) 上記と同等の品質管理手順及び体制が明確化された品質マネジメントシステムを有している事業者であること（管理体制、品質マネジメントシステム運営規程、品質管理手順規定等を提示すること。）。 イ 応札者は、情報セキュリティに係る以下のいずれかの条件を満たすこと。 (ア) 情報セキュリティ実施基準である「JIS Q 27001」、「ISO/IEC27001」又は「ISMS」の認証を有しており、認証が有効であること。 (イ) 一般財団法人日本情報経済社会推進協会のプライバシーマーク制度の認定を受けているか、又は同等の個人情報保護のマネジメントシステムを確立していること。 (ウ) 個人情報扱うシステムのセキュリティ体制が適切であることを第三者機関に認定された事業者であること。</p>	
<p>9 入札参加資格に関する事項 (3) 受注実績等</p>	<p>ア 応札者は、過去5年以内に、申請者5,000人以上のオンライン申請システム導入における工程管理、もしくは導入支援の業務実績を有すること。 イ IaaS/PaaSを活用する場合、応札者は以下の1)又は2)のいずれかの条件を満たすこと。 1) 提案予定のクラウドサービスプロバイダーから代理店の認定を受け、かつ登録（AWSの場合AWS Solution Provider Program (SPP) の登録、Azureの場合Licensing Solution Partner (LSP)の登録）を受けていること。加えて、本案件の関係者が、日本国内のクラウドサービスプロバイダーから日本語で契約や技術に関するサポートを受けられる商流であること。 2) 国内企業のディストリビュータ経由で提案予定のクラウドサービスプロバイダーのクラウドサービスの再販が可能であること。 ウ IaaS/PaaSを活用する場合、応札者は、本システムで導入予定（又は提案予定）のパブリッククラウドへの移行又は構築を行った実績を過去3年以内に有すること。</p>	

<p>9 入札参加資格に関する事項 (4) 複数事業者による共同入札</p>	<p>ア 複数の事業者が共同入札する場合、その中から全体の意思決定、運営管理等に責任を持つ共同入札の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。 イ 共同入札を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の契約不適合責任についても協定の内容に含めること。 ウ 共同入札を構成する全ての事業者は、本入札への単独提案又は他の共同入札への参加を行っていないこと。 エ 共同事業者の代表者は、情報セキュリティに係る要件について満たすこと。</p>	
<p>9 入札参加資格に関する事項 (5) 入札制限</p>	<p>「令和7年度農林水産省次期オンライン申請システムの導入及びeMAFFからの移行に係るコンサルティング業務」の受注事業者（再委託先等を含む。）及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」（昭和38年11月27日大蔵省令第59号）第8条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者は、入札には参加できない。 本業務を直接担当する農林水産省ITテクニカルアドバイザー（旧農林水産省CIO補佐官に相当）、農林水産省全体管理組織（PMO）支援スタッフ及び農林水産省最高情報セキュリティアドバイザーが、その現に属する事業者及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」（昭和38年大蔵省令第59号）第8条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先等緊密な利害関係を有する事業者は、本書に係る業務に関して入札に参加できないものとする。</p>	

別紙 情報セキュリティの確保に関する共通基本仕様

該当箇所	記載内容	回答欄
IIの1	<p>応札者は、応札者の資本関係・役員等の情報、本業務の実施場所、本業務の従事者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属・専門性（保有資格、研修受講実績等）・実績（業務実績、経験年数等）及び国籍に関する情報を記載した資料を提出すること。 なお、本業務に従事する全ての要員に関する情報を記載することが困難な場合は、本業務に従事する主要な要員に関する情報を記載するとともに、本業務に従事する部門等における従事者に関する情報（〇〇国籍の者が△名（又は□%）等）を記載すること。また、この場合であっても、担当部署からの要求に応じて、可能な限り要員に関する情報を提供すること。</p>	
IIの2	<p>応札者は、本業務を実施する部署、体制等の情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。） （1）ISO/IEC27001等の国際規格とそれに基づく認証の証明書等 （2）プライバシーマーク又はそれと同等の認証の証明書等 （3）独立行政法人情報処理推進機構（IPA）が公開する「情報セキュリティ対策ベンチマーク」を利用した自己評価を行い、その評価結果において、全項目に係る平均値が4に達し、かつ各評価項目の成熟度が2以上であることが確認できる確認書</p>	

Ⅲの1	<p>1 受託者は、本業務の実施に当たって、以下の措置を講ずること。なお、応札者は、以下の措置を講ずることを証明する資料を提出すること。</p> <p>(1) 本業務上知り得た情報（公知の情報を除く。）については、契約期間中はもとより契約終了後においても、第三者に開示し、又は本業務以外の目的で利用しないこと。</p> <p>(2) 本業務に従事した要員が異動、退職等をした後においても有効な守秘義務契約を締結すること。</p> <p>(3) 本業務に係る情報を適切に取り扱うことが可能となるよう、情報セキュリティ対策の実施内容及び管理体制を整備すること。なお、本業務実施中及び実施後において検証が可能となるよう、必要なログの取得や作業履歴の記録</p>	
Ⅳの1	<p>1 受託者は、本業務において情報システムに関する業務を行う場合には、以下の措置を講ずること。なお、応札者は、以下の措置を講ずることを証明する資料を提出すること。</p> <p>(1) 本業務の各工程において、農林水産省の意図しない情報システムに関する変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図、第三者機関による品質保証体制を証明する書類等を提出すること。）。</p> <p>(2) 本業務において、農林水産省の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入</p>	
Ⅴの6	<p>6 業務委託サービスの提供に当たり、業務委託サービスの提供者若しくはその従業員、再委託先又はその他の者によって、農林水産省の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図、第三者機関による品質保証体制を証明する書類等を提出すること）。</p>	
Ⅴの7	<p>7 業務委託サービスの提供者の資本関係、役員等の情報、業務委託サービスの提供が行われる施設等の場所、業務委託サービス提供に従事する者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属、専門性（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報を記載した資料を提出すること。</p>	
Ⅴの8	<p>8 業務委託サービスの提供者の情報セキュリティ水準を証明する、Ⅱの2で掲げる証明書等または同等以上の国際規格等の証明書の写しを提出すること。</p>	

VIの1 (5)	<p>(5) クラウドサービス提供者の資本関係、役員等の情報、クラウドサービス提供に従事する者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）のうち農林水産省の情報又は農林水産省が利用するクラウドサービスの環境に影響を及ぼす可能性のある者の所属、専門性（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報を記載した資料を提出すること。</p>	
VIの1 (6)	<p>(6) ペネトレーションテストや脆弱（ぜい）弱性診断等の第三者による検査の実施状況と受入に関する情報が開示されていること。</p>	
VIの1 (8)	<p>(8) ISMAPクラウドサービスリスト等に登録されていないクラウドサービスの場合は、ISMAPの管理基準に従い、ガバナンス基準及びマネジメント基準における全ての基準、管理策基準における統制目標（3桁の番号で表現される項目）及び末尾にBが付された詳細管理策（4桁の番号で表現される項目）を原則として全て満たしていることを証明する資料を提出し、農林水産省の承認を得ること。</p>	
VIIIの1	<p>受託者は、本業務において、農林水産省にサーバ装置、端末、通信回線装置、複合機、特定用途機器、外部電磁的記録媒体、ソフトウェア等（以下「機器等」という。）を納品、賃貸借等をする場合には、以下の措置を講ずること。</p> <p>1 納入する機器等の製造工程において、農林水産省が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。</p>	
VIIIの6	<p>6 ISO/IEC 15408に基づく認証を取得している機器等を採用することが望ましい。なお、当該認証を取得している場合は、証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）</p>	

【別紙10】AWS/Azure設定確認リスト

凡例：○：責任者、△：サポート

【PaaS/IaaS】基本的な設定すべきセキュリティ対策（AWS/Azure）	担当		役割分担に関する補足
	MAFFクラウド管理者(PMO)	PJMO	
IDおよびアクセス管理			
組織が許可したアカウントの管理		○	
管理者アカウントに対する多要素認証の利用	△	○	多要素認証を設定していない限りあらゆるAWS/Azureリソースの操作が出来ないように設定
管理者アカウントに紐づく最新の連絡先の登録と定期的な見直し	△	○	年度末に実施
必要最低限の管理者権限の割当て	△	○	AWS：Configを利用して実施 Azure：Azure Policyを利用して実施
グループを利用した権限の設定		○	
管理者アカウントに関する復旧手段の確保		○	
すべてのアカウントへのパスワードポリシーの適用	△	○	AWS：Configを利用して実施 Azure：Azure Policyを利用して実施
アクセスキー、サービスアカウントキー等の適切な管理		○	
管理者アカウントと日常的に使用するアカウントの分離		○	ユーザーの払い出しはPJMO管理
アカウント・権限・認証情報の定期的な見直し		○	年度末に実施
AWSにおいて考慮すべき設定			
AWS サポートセンターへのアクセス設定		○	
IAMに保存されているサーバ証明書の管理		○	
IAM Access analyzerの有効化		○	
Azureにおいて考慮すべき設定			
Microsoft Azure サポートセンターへのアクセス設定		○	
Azure App Serviceに保存されているサーバ証明書の管理		○	
ログの記録と監視			
ログの有効化及び取得	△	○	MAFFクラウド管理者側で有効化の為の手順を作成し、PJMOに配布
ログの一元管理	△	○	
ログの保護	△	○	管理者アカウントで保管
ログの監視/通知の設定	△	○	AWS：アクセスログなどは管理者アカウント側でGuardDutyを用いて対応。 Azure：アクセスログなどは管理アカウント側でMicrosoft Defender for Cloudを用いて対応。 そのほかのログについてはPJMOに一任。
ネットワーク			
ロードバランサの接続設定		○	
仮想マシン			
最新のOSパッチの適用確認		○	
不正プログラム対策ソフトウェアの導入		○	
攻撃対象となるネットワークポートへのアクセス制限		○	
ストレージ			
匿名/公開アクセスの禁止	△	○	不適切設定を有効化し、管理者アカウントで監視
ストレージアクセスの通信設定	△	○	不適切設定を有効化し、管理者アカウントで監視
AWSにおいて考慮すべき設定			
Amazon RDSの暗号化	△	○	不適切設定を有効化し、管理者アカウントで監視
MFA Deleteの有効化	△	○	不適切設定を有効化し、管理者アカウントで監視
Amazon EBSの暗号化	△	○	不適切設定を有効化し、管理者アカウントで監視
Azureにおいて考慮すべき設定			
Azure Databaseの暗号化	△	○	不適切設定を有効化し、管理者アカウントで監視
MFA Deleteの有効化	△	○	不適切設定を有効化し、管理者アカウントで監視
Azure Disk Storageの暗号化	△	○	不適切設定を有効化し、管理者アカウントで監視

項目		見出し	要件		備考	必須可否
1	認証・認可	ユーザー認証	1.1.1	特定のユーザーや管理者のみに表示・実行を許可すべき画面や機能、APIでは、ユーザー認証を実施すること	特定のユーザーや管理者のみにアクセスを許可したいWebシステムでは、ユーザー認証を行う必要があります。また、ユーザー認証が成功した後はアクセス権限を確認する必要があります。そのため、認証済みユーザーのみがアクセス可能な箇所を明示しておくことが望ましいでしょう。リスクベース認証や二要素認証など認証をより強固にする仕組みもあります。不特定多数がアクセスする必要がない場合には、IPアドレスなどによるアクセス制限も効果があります。OpenIDなどIdP(ID Provider)を利用する場合には信頼できるプロバイダであるかを確認する必要があります。IdPを使った認証・認可を行う場合も他の認証・認可に関する要件を満たすものを利用することが望ましいです。	必須
			1.1.2	上記画面や機能に含まれる画像やファイルなどの個別のコンテンツ（非公開にすべきデータは直接URLで指定できる公開ディレクトリに配置しない）では、ユーザー認証を実施すること		必須
			1.1.3	多要素認証を実施すること	多要素認証（Multi Factor Authentication: MFA）とは、例えばパスワードによる認証に加え、TOTP（Time-Based One-Time Password：時間ベースのワンタイムパスワード）やデジタル証明書など二つ以上の要素を利用した認証方式です。手法については NIST Special Publication 800-63Bなどを参照してください。	推奨
	1.2	ユーザーの再認証	1.2.1	個人情報や機微情報を表示するページに遷移する際には、再認証を実施すること	ユーザー認証はセッションにおいて最初の一度だけ実施するのではなく、重要な情報や機能へアクセスする際には再認証を行うことが望ましいでしょう。	推奨
			1.2.2	パスワード変更や決済処理などの重要な機能を実行する際には、再認証を実施すること		推奨
	1.3	パスワード	1.3.1	ユーザー自身が設定するパスワード文字列は最低8文字以上であること	認証を必要とするWebシステムの多くは、パスワードを本人確認の手段として認証処理を行います。そのためパスワードを盗聴や盗難などから守ることが重要になります。	必須
			1.3.2	登録可能なパスワード文字列の最大文字数は64文字以上であること	パスワードを処理する関数の中には最大文字数が少ないものもあるので注意する必要があります。	必須
			1.3.3	パスワード文字列として使用可能な文字種は制限しないこと	任意の大小英字、数字、記号、空白、Unicode文字など任意の文字が利用可能である必要があります。	必須
			1.3.4	パスワード文字列の入力フォームはinput type="password"で指定すること	基本的にinputタグのtype属性には「password」を指定しますが、パスワードを一時的に表示する可視化機能を実装する場合にはこの限りではありません。	必須
			1.3.5	ユーザーが入力したパスワード文字列を次画面以降で表示しないこと（hiddenフィールドなどのHTMLソース内やメールも含む）		必須

項目	見出し	要件	備考	必須可否
		1.3.6 パスワードを保存する際には、平文で保存せず、Webアプリケーションフレームワークなどが提供するハッシュ化とsaltを使用して保存する関数を使用すること	関数が存在しない場合にはパスワードは「パスワード文字列+salt（ユーザー毎に異なるランダムな文字列）」をハッシュ化したものとsaltのみを保存する必要があります。（saltは20文字以上であることが望ましい）パスワード文字列のハッシュ化をさらに安全にする手法としてストレッチングがあります。	必須
		1.3.7 ユーザー自身がパスワードを変更できる機能を用意すること		必須
		1.3.8 パスワードはユーザー自身に設定させること システムが仮パスワードを発行する場合はランダムな文字列を設定し、安全な経路でユーザーに通知すること		推奨
		1.3.9 パスワードの入力欄でペースト機能を禁止しないこと	長いパスワードをユーザーが利用出来るようにするためにペースト機能を禁止しないようにする必要があります。	推奨
		1.3.10 パスワード強度チェッカーを実装すること	使用する文字種や文字数を確認し、ユーザー自身にパスワードの強度を示せるようにします。またユーザーIDと同じ文字列や漏洩したパスワードなどのリストとの突合を行う必要があります。手法については NIST Special Publication 800-63Bなどを参照してください。	推奨
1.4	アカウントロック機能について	1.4.1 認証時に無効なパスワードで10回試行があった場合、最低30分間はユーザーがロックアウトされた状態にすること	パスワードに対する総当たり攻撃や辞書攻撃などから守るためには、試行速度を遅らせるアカウントロック機能の実装が有効な手段になります。アカウントロックの試行回数、ロックアウト時間については、サービスの内容に応じて調整することが必要になります。	必須
		1.4.2 ロックアウトは自動解除を基本とし、手動での解除は管理者のみ実施可能とすること		推奨
1.5	パスワードリセット機能について	1.5.1 パスワードリセットを実行する際にはユーザー本人しか受け取れない連絡先（あらかじめ登録しているメールアドレス、電話番号など）にワンタイムトークンを含むURLなどの再設定方法を通知すること	連絡先については、事前に受け取り確認をしておくことでより安全性を高めることができます。 使用されたワンタイムトークンは破棄し、有効期限を12時間以内とし必要最低限に設定してください。	必須
		1.5.2 パスワードはユーザー自身に再設定させること		必須
1.6	アクセス制御について	1.6.1 Web ページや機能、データをアクセス制御（認可制御）する際には認証情報・状態を元に権限があるかどうかを判別すること	認証により何らかの制限を行う場合には、利用しようとしている情報や機能へのアクセス（読み込み・書き込み・実行など）権限を確認することでアクセス制御を行うことが必要になります。 画像やファイルなどのコンテンツ、APIなどの機能に対しても、全て個別にアクセス権限を設定、確認する必要があります。 これらはアクセス権限の一覧表に基づいて行います。 CDNなどを利用してコンテンツを配置するなどアクセス制御を行うことが困難な場合、予測が困難なURLを利用することでアクセスされにくくする方法もあります。	必須

項目	見出し		要件	備考	必須可否
			1.6.2 公開ディレクトリには公開を前提としたファイルのみ配置すること	公開ディレクトリに配置したファイルは、URLを直接指定することでアクセスされる可能性があります。そのため、機微情報や設定ファイルなどの公開する必要がないファイルは、公開ディレクトリ以外に配置する必要があります。	必須
	1.7	アカウントの無効化機能について	1.7.1 管理者がアカウントの有効・無効を設定できること	不正にアカウントを利用されていた場合に、アカウントを無効化することで被害を軽減することができます。	推奨
2	セッション管理	2.1 セッションの破棄について	2.1.1 認証済みのセッションが一定時間以上アイドル状態にあるときはセッションタイムアウトとし、サーバー側のセッションを破棄しログアウトすること	認証を必要とするWebシステムの多くは、認証状態の管理にセッションIDを使ったセッション管理を行います。認証済みの状態にあるセッションを不正に利用されないためには、使われなくなったセッションを破棄する必要があります。セッションタイムアウトの時間については、サービスの内容やユーザー利便性に応じて設定することが必要になります。また、NIST Special Publication 800-63Bなどを参照してください。	必須
			2.1.2 ログアウト機能を用意し、ログアウト実行時にはサーバー側のセッションを破棄すること	ログアウト機能の実行後にその成否をユーザーが確認できることが望ましい。	必須
	2.2	セッションIDについて	2.2.1 Webアプリケーションフレームワークなどが提供するセッション管理機能を使用すること	セッションIDを用いて認証状態を管理する場合、セッションIDの盗聴や推測、攻撃者が指定したセッションIDを使用させられる攻撃などから守る必要があります。また、セッションIDは原則としてcookieにのみ格納すべきです。	必須
			2.2.2 セッションIDは認証成功後に発行すること 認証前にセッションIDを発行する場合は、認証成功直後に新たなセッションIDを発行すること		必須
			2.2.3 ログイン前に機微情報をセッションに格納する時点でセッションIDを発行または再生成すること		必須
			2.2.4 認証済みユーザーの特定はセッションに格納した情報を元に行うこと		必須
	2.3	CSRF（クロスサイトリクエストフォージェリー）対策の実施について	2.3.1 ユーザーにとって重要な処理を行う箇所では、ユーザー本人の意図したリクエストであることを確認できるようにすること	正規ユーザー以外の意図により操作されては困る処理を行う箇所では、フォーム生成の際に他者が推測困難なランダムな値（トークン）をhiddenフィールドやcookie以外のヘッダーフィールド（X-CSRF-TOKENなど）に埋め込み、リクエストをPOSTメソッドで送信します。フォームデータを処理する際にトークンが正しいことを確認することで、正規ユーザーの意図したリクエストであることを確認することができます。また、別の方法としてパスワード再入力による再認証を求める方法もあります。cookieのSameSite属性を適切に使うことによって、CSRFのリスクを低減する効果があります。SameSite属性は一部の状況においては効果がないこともあるため、トークンによる確認が推奨されます。	必須
3	入力処理	3.1 パラメーターについて	3.1.1 URLにユーザーIDやパスワードなどの機微情報を格納しないこと	URLは、リファラー情報などにより外部に漏えいする可能性があります。そのためURLには秘密にすべき情報は格納しないようにする必要があります。	必須

項目	見出し	要件	備考	必須可否			
		3.1.2	パラメーター（クエリストリング、エンティティボディ、cookieなどクライアントから受け渡される値）にパス名を含めないこと	ファイル操作を行う機能などにおいて、URL パラメーターやフォームで指定した値でパス名を指定できるようにした場合、想定していないファイルにアクセスされてしまうなどの不正な操作を実行されてしまう可能性があります。	必須		
		3.1.3	パラメーター要件に基づいて、入力値の文字種や文字列長の検証を行うこと	各パラメーターは、機能要件に基づいて文字種・文字列長・形式を定義する必要があります。入力値に想定している文字種や文字列長以外の値の入力を許してしまう場合、不正な操作を実行されてしまう可能性があります。サーバー側でパラメーターを受け取る場合、クライアント側での入力値検証の有無に関わらず、入力値の検証はサーバー側で実施する必要があります。	必須		
	3.2	ファイルアップロードについて	3.2.1	入力値としてファイルを受け付ける場合には、拡張子やファイルフォーマットなどの検証を行うこと	ファイルのアップロード機能を利用した不正な実行を防ぐ必要があります。画像ファイルを扱う場合には、ヘッダー領域を不正に加工したファイルにも注意が必要です。	必須	
			3.2.2	アップロード可能なファイルサイズを制限すること	圧縮ファイルを展開する場合には、解凍後のファイルサイズや、ファイルパスやシンボリックリンクを含む場合のファイルの上書きにも注意が必要です。	必須	
	3.3	XMLを使用する際の処理について	3.3.1	XMLを読み込む際は、外部参照を無効にすること	手法についてはXML External Entity Prevention Cheat Sheetなどを参照してください。 https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html	必須	
	3.4	デシリアライズについて	3.4.1	信頼できないデータ供給元からのシリアライズされたオブジェクトを受け入れないこと	デシリアライズする場合は、シリアライズしたオブジェクトにデジタル署名などを付与し、信頼できる供給元が発行したデータであるかを検証してください。	必須	
	3.5	外部リソースへのリクエスト送信について	3.5.1	他システムに接続や通信を行う場合は、外部からの入力によって接続先を動的に決定しないこと	外部から不正なURLやIPアドレスなどが挿入されると、SSRF(Server-Side Request Forgery)の脆弱性になる可能性があります。外部からの入力によって接続先を指定せざるを得ない場合は、ホワイトリストを基に入力値の検証を実施するとともに、アプリケーションレイヤーだけではなくネットワークレイヤーでのアクセス制御も併用する必要があります。	推奨	
4	出力処理	4.1	HTMLを生成する際の処理について	4.1.1	HTMLとして特殊な意味を持つ文字（<>'&）を文字参照によりエスケープすること	外部からの入力により不正なHTMLタグなどが挿入されてしまう可能性があります。「<」→「<」や「&」→「&」、「"」→「"」のようにエスケープを行う必要があります。スクリプトによりクライアント側でHTMLを生成する場合も、同等の処理が必要です。実装の際にはこれらを自動的に実行するフレームワークやライブラリを使用することが望ましいでしょう。また、その他にもスクリプトの埋め込みの原因となるものを作らないようにする必要があります。 XMLを生成する場合も同様にエスケープが必要です。	必須
			4.1.2	外部から入力したURLを出力するときは「http://」または「https://」で始まるもののみを許可すること		必須	

項目	見出し	要件	備考	必須可否
		4.1.3 <script>...</script>要素の内容やイベントハンドラ（onmouseover="" など）を動的に生成しないようにすること	<script>...</script>要素の内容やイベントハンドラは原則として動的に生成しないようにすべきですが、jQueryなどのAjaxライブラリを使用する際はその限りではありません。ライブラリについては、アップデート状況などを調べて信頼できるものを選択するようにしましょう。	必須
		4.1.4 任意のスタイルシートを外部サイトから取り込めないようにすること		必須
		4.1.5 HTMLタグの属性値を「"」で囲うこと	HTMLタグ中のname="value"で記される値(value)にユーザーの入力値を使う場合、「"」で囲わない場合、不正な属性値を追加されてしまう可能性があります。	必須
		4.1.6 CSSを動的に生成しないこと	外部からの入力により不正なCSSが挿入されると、ブラウザに表示される画面が変更されたり、スクリプトが埋め込まれる可能性があります。	必須
4.2	JSONを生成する際の処理について	4.2.1 文字列連結でJSON文字列を生成せず、適切なライブラリを用いてオブジェクトをJSONに変換すること	適切なライブラリがない場合は、JSONとして特殊な意味を持つ文字（"¥, : { } []）をUnicodeエスケープする必要があります。	必須
4.3	HTTPレスポンスヘッダーについて	4.3.1 HTTPレスポンスヘッダーのContent-Typeを適切に指定すること	一部のブラウザではコンテンツの文字コードやメディアタイプを誤認識させることで不正な操作が行える可能性があります。これを防ぐためには、HTTPレスポンスヘッダーを「Content-Type: text/html; charset=utf-8」のように、コンテンツの内容に応じたメディアタイプと文字コードを指定する必要があります。	必須
		4.3.2 HTTPレスポンスヘッダーフィールドの生成時に改行コードが入らないようにすること	HTTPヘッダーフィールドの生成時にユーザーが指定した値を挿入できる場合、改行コードを入力することで不正なHTTPヘッダーやコンテンツを挿入されてしまう可能性があります。これを防ぐためには、HTTPヘッダーフィールドを生成する専用のライブラリなどを使うようにすることが望ましいでしょう。	必須
4.4	その他の出力処理について	4.4.1 SQL文を組み立てる際に静的プレースホルダを使用すること	SQL文の組み立て時に不正なSQL文を挿入されることで、SQLインジェクションを実行されてしまう可能性があります。これを防ぐためにはSQL文を動的に生成せず、プレースホルダを使用してSQL文を組み立てる必要があります。 静的プレースホルダとは、JIS/ISOの規格で「準備された文(Prepared Statement)」と規定されているものです。	必須
		4.4.2 プログラム上でOSコマンドやアプリケーションなどのコマンド、シェル、eval()などによるコマンドの実行を呼び出して使用しないこと	コマンド実行時にユーザーが指定した値を挿入できる場合、外部から任意のコマンドを実行されてしまう可能性があります。コマンドを呼び出して使用しないことが望ましいでしょう。	必須
		4.4.3 リダイレクタを使用する場合には特定のURLのみに遷移できるようにすること	リダイレクタのパラメーターに任意のURLを指定できる場合（オープンリダイレクタ）、攻撃者が指定した悪意のあるURLなどに遷移させられる可能性があります。	必須
		4.4.4 メールヘッダーフィールドの生成時に改行コードが入らないようにすること	メールの送信処理にユーザーが指定した値を挿入できる場合、不正なコマンドなどを挿入されてしまう可能性があります。これを防ぐためには、不正な改行コードを使用できないメール送信専用のライブラリなどを使うようにすることが望ましいでしょう。	必須

項目	見出し		要件	備考	必須可否
			4.4.5 サーバ側のテンプレートエンジンを使用する際に、テンプレートの変更や作成に外部から受け渡される値を使用しないこと	サーバ側のテンプレートエンジンを使用してテンプレートを組み立てる際に不正なテンプレートの構文を挿入されることで、任意のコードを実行される可能性があります。 外部から渡される値をテンプレートの組み立てに使用せず、レンダリングを行う際のデータとして使用する必要があります。 また、レンダリング時にはクロスサイトスクリプティングの脆弱性が存在しないか確認してください。	必須
5	HTTPS	5.1 HTTPSについて	5.1.1 Webサイトを全てHTTPSで保護すること	適切にHTTPSを使うことで通信の盗聴・改ざん・なりすましから情報を守ることができます。次のような重要な情報を扱う画面や機能ではHTTPSで通信を行う必要があります。 ・入力フォームのある画面 ・入力フォームデータの送信先 ・重要情報が記載されている画面 ・セッションIDを送受信する画面 HTTPSの画面内で読み込む画像やスクリプトなどのコンテンツについてもHTTPSで保護する必要があります。	必須
			5.1.2 サーバ証明書はアクセス時に警告が出ないものを使用すること	HTTPSで提供されているWebサイトにアクセスした場合、Webブラウザから何らかの警告がでるとことは、適切にHTTPSが運用されておらず盗聴・改ざん・なりすましから守られていません。適切なサーバ証明書を使用する必要があります。	必須
			5.1.3 TLS1.2以上のみを使用すること	SSL2.0/3.0、TLS1.0/1.1には脆弱性があるため、無効化する必要があります。使用する暗号スイートは、7.2.1を参照してください。	必須
			5.1.4 レスポンスヘッダーにStrict-Transport-Securityを指定すること	Hypertext Strict Transport Security(HSTS)を指定すると、ブラウザがHTTPSでアクセスするよう強制できます。	必須
6	cookie	6.1 cookieの属性について	6.1.1 Secure属性を付けること	Secure属性を付けることで、http://でのアクセスの際にはcookieを送出しないようにできます。特に認証状態に紐付けられたセッションIDを格納する場合には、Secure属性を付けることが必要です。	必須
			6.1.2 HttpOnly属性を付けること	HttpOnly属性を付けることで、クライアント側のスクリプトからcookieへのアクセスを制限することができます。	必須
			6.1.3 Domain属性を指定しないこと	セッションフィクセーションなどの攻撃に悪用されることがあるため、Domain属性は特に必要がない限り指定しないことが望ましいでしょう。	推奨
7	その他	7.1 エラーメッセージについて	7.1.1 エラーメッセージに詳細な内容を表示しないこと	ミドルウェアやデータベースのシステムが出力するエラーには、攻撃のヒントになる情報が含まれているため、エラーメッセージの詳細な内容はエラーログなどに出力するべきです。	必須

項目	見出し	要件	備考	必須可否
7.2	暗号アルゴリズムについて	7.2.1 ハッシュ関数、暗号アルゴリズムは『電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）』に記載のものを使用すること	広く使われているハッシュ関数、疑似乱数生成系、暗号アルゴリズムの中には安全でないものもあります。安全なものを使用するためには、『電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）』や『TLS暗号設定ガイドライン』に記載されたものを使用する必要があります。	必須
7.3	乱数について	7.3.1 鍵や秘密情報などに使用する乱数的性質を持つ値を必要とする場合には、暗号学的な強度を持った疑似乱数生成系を使用すること	鍵や秘密情報に予測可能な乱数を用いると、過去に生成した乱数値から生成する乱数値が予測される可能性があるため、ハッシュ関数などを用いて生成された暗号学的な強度を持った疑似乱数生成系を使用する必要があります。	必須
7.4	基盤ソフトウェアについて	7.4.1 基盤ソフトウェアはアプリケーションの稼働年限以上のものを選定すること	脆弱性が発見された場合、修正プログラムを適用しないと悪用される可能性があります。そのため、言語やミドルウェア、ソフトウェアの部品などの基盤ソフトウェアは稼働期間またはサポート期間がアプリケーションの稼働期間以上のものを利用する必要があります。もしアプリケーションの稼働期間中に基盤ソフトウェアの保守期間が終了した場合、危険な脆弱性が残されたままになる可能性があります。	必須
		7.4.2 既知の脆弱性のないOSやミドルウェア、ライブラリやフレームワーク、パッケージなどのコンポーネントを使用すること	利用コンポーネントにOSSが含まれる場合は、SCA（ソフトウェアコンポジション解析）ツールを導入し、依存関係を包括的かつ正確に把握して対策が行えることが望ましいでしょう。	必須
7.5	ログの記録について	7.5.1 重要な処理が行われたらログを記録すること	ログは、情報漏えいや不正アクセスなどが発生した際の検知や調査に役立つ可能性があります。認証やアカウント情報の変更などの重要な処理が実行された場合には、その処理の内容やクライアントのIPアドレスなどをログとして記録することが望ましいでしょう。ログに機微情報が含まれる場合にはログ自体の取り扱いにも注意が必要になります。	必須
7.6	ユーザーへの通知について	7.6.1 重要な処理が行われたらユーザーに通知すること	重要な処理（パスワードの変更など、ユーザーにとって重要で取り消しが困難な処理）が行われたことをユーザーに通知することによって異常を早期に発見できる可能性があります。	推奨
7.7	Access-Control-Allow-Originヘッダーについて	7.7.1 Access-Control-Allow-Originヘッダーを指定する場合は、動的に生成せず固定値を使用すること	クロスオリジンでXMLHttpRequest (XHR)を使う場合のみこのヘッダーが必要です。不要な場合は指定する必要はありませんし、指定する場合も特定のオリジンのみを指定する事が望ましいです。	必須
7.8	クリックジャッキング対策について	7.8.1 レスポンスヘッダーにX-Frame-OptionsとContent-Security-Policyヘッダーのframe-ancestors ディレクティブを指定すること	クリックジャッキング攻撃に悪用されることがあるため、X-Frame-OptionsヘッダーフィールドにDENYまたはSAMEORIGINを指定する必要があります。 Content-Security-Policyヘッダーフィールドに frame-ancestors 'none' または 'self' を指定する必要があります。 X-Frame-Options ヘッダーは主要ブラウザでサポートされていますが標準化されていません。CSP レベル 2 仕様で frame-ancestors ディレクティブが策定され、X-Frame-Options は非推奨とされました。	必須

項目	見出し		要件		備考	必須可否	
	7.9	キャッシュ制御について	7.9.1	個人情報や機微情報を表示するページがキャッシュされないよう Cache-Control: no-store を指定すること	個人情報や機密情報が含まれたページはCDNやロードバランサー、ブラウザなどのキャッシュに残ってしまうことで、権限のないユーザーが閲覧してしまう可能性があるためキャッシュ制御を適切に行う必要があります。	必須	
	7.10	ブラウザのセキュリティ設定について	7.10.1	ユーザーに対して、ブラウザのセキュリティ設定の変更をさせるような指示をしないこと	ユーザーのWebブラウザのセキュリティ設定などを変更した場合や、認証局の証明書をインストールさせる操作は、他のサイトにも影響します。	必須	
	7.11	ブラウザのセキュリティ警告について	7.11.1	ユーザーに対して、ブラウザの出すセキュリティ警告を無視させるような指示をしないこと	ブラウザの出す警告を通常利用においても無視させるよう指示をしていると、悪意のあるサイトで同様の指示をされた場合もそのような操作をしてしまう可能性が高まります。	必須	
	7.12	WebSocketについて	7.12.1	Originヘッダーの値が正しいリクエスト送信元であることが確認できた場合にのみ処理を実施すること	WebSocketにはSOP (Same Origin Policy) という仕組みが存在しないため、Cross-Site WebSocket Hijacking(CSWSH)対策のためにOriginヘッダーを確認する必要があります。	必須	
	7.13	HTMLについて	7.13.1	html開始タグの前に<!DOCTYPE html>を宣言すること	DOCTYPEで文書タイプをHTMLと明示的に宣言することでCSSなど別フォーマットとして解釈されることを防ぎます。	必須	
7.13.2			CSSファイルやJavaScriptファイルをlinkタグで指定する場合は、絶対パスを使用すること	linkタグを使用してCSSファイルやJavaScriptファイルを相対パス指定した場合にRPO (Relative Path Overwrite) が起きる可能性があります。	必須		
8	提出物	8.1	提出物について	8.1.1	サイトマップを用意すること	認証や再認証、CSRF対策が必要な箇所、アクセス制御が必要なデータを明確にするためには、Webサイト全体の構成を把握し、扱うデータを把握する必要があります。そのためには上記の資料を用意することが望ましいでしょう。	必須
				8.1.2	画面遷移図を用意すること		必須
				8.1.3	アクセス権限一覧表を用意すること	誰にどの機能の利用を許可するかとめた一覧表を作成することが望ましいでしょう。	必須
				8.1.4	コンポーネント一覧を用意すること	依存しているライブラリやフレームワーク、パッケージなどのコンポーネントに脆弱性が存在する場合がありますので、依存しているコンポーネントを把握しておく必要があります。	推奨
				8.1.5	上記のセキュリティ要件についてテストした結果報告書を用意すること	自社で脆弱性診断を実施する場合には「脆弱性診断スキルマッププロジェクト」が公開している「Webアプリケーション脆弱性診断ガイドライン」などを参照してください。	推奨