地方公共団体における情報システム セキュリティ要求仕様モデルプラン （Web アプリケーション）

第 1.0 版

財団法人地方自治情報センター 自治体セキュリティ支援室

目次

別紙 6 実装状況報告書（サンプル）

別紙 7 契約書への追加条文例

別紙 8 Web アプリケーションセキュリティ要求仕様等検討委員会 委員等一覧

本書について

情報システムは住民向けのサービス基盤として欠かせない存在ですが、情報システムを安全に利用する上で避けては通れない問題があります。それが「脆弱性」に関する問題です。

脆弱性とは情報セキュリティ上の弱点のことであり、脆弱性の問題を放置すると、情報の流出や、ホームページ等コンテンツの改ざん、サービスの停止などの問題を引き起こす可能性があります。一見すると安定して動作しているように見えていても脆弱性が内在することもあり、情報システムの調達・構築・運用にあたってこの対処をあらかじめ決めておくことは安定的な運用に欠かせないことです。

特に近年では Web アプリケーションの脆弱性を狙ったサイバー攻撃の発生が顕著であり、一般のニュースで取り上げられることも珍しくなくなりました。そして、残念ながら一部の地方公共団体（以下「団体」という。）でも、Web アプリケーションの脆弱性によって Web サイトを改ざんされるなどの被害が発生しているところです。

このような状況にかんがみ、地方自治情報センター（以下「当センター」という。）は「地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）」（以下「本書」という。）を作成しました。

本書は、団体において Web アプリケーションを導入するにあたって、システムの脆弱性をなくし、安全に運用するために必要な要求仕様事項を取りまとめた「特記仕様書の例」です。

本書は様々な前提条件における様々な種類の Web アプリケーションを導入する際に必要なすべてのセキュリティ要件を網羅したものではありませんが、各種ソフトウェアの脆弱性対策にフォーカスしたものとなっています。

本書の内容を一部カスタマイズして各団体の「Web アプリケーションセキュリティに関する特記仕様書」を検討、作成いただき、入札仕様書に追加要件として添付することにより、SQL インジェクション、クロスサイト・スクリプティングといった Web アプリケーションの脆弱性や、納品後（運用時）に新たに発見された脆弱性についても計画的に解決するための道筋をつけられるようになることを目的として作成しています。

モデルプランの効用（メリット）は次のとおりです。

- 特記仕様書を添付するだけで一定のセキュリティレベルを要求することができます（あまり詳しい技術知識を持っていなくても利用可能）。
- 脆弱性を作り込まないことを提案事業者（受注事業者）に約束させることができます。
- 発注時（事前）に対策を考えることで、納品後の運用（事後）に備えることができます。

本書を参考に、より多くの団体にセキュアな Web アプリケーションが導入されることを祈念します。

最後に、本書及び解説書の作成に当たってご協力いただきました多くの方々のご支援に感謝申し上げます。

平成 24 年 10 月

（財）地方自治情報センター

自治体セキュリティ支援室

地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）に関するアンケートへのご協力のお願い

本書及びその解説書は今後よりよいものとするために内容を適宜修正していくことも検討しています。また、本書をご活用頂いている団体の事例紹介なども検討しています。

つきましては、本書及び解説書の内容をより充実させるために、ご一読、ご活用いただいた際に感じられたこと等から下記アンケートを記入いただき、当センター担当者まで是非お送りください。よろしくお願いします。

＜Web アプリケーション要求仕様モデルプラン（第 1.0 版）に関するアンケート＞

回答対象者：地方公共団体職員

回答方法　：メール

回答送付先：（財）地方自治情報センター 自治体セキュリティ支援室 担当宛

lasc_info@lasdec.asp.lgwan.jp （LGWAN 接続が必要です）

lasc@lasdec.or.jp （Internet）

回答送付時件名：Web アプリケーション要求仕様モデルプラン（第 1.0 版）に関するアンケート回答

本文（回答）：

設問 1. どのようなシステムに本書を活用しましたか？（複数可・回答必須）

例 1：市の情報システム調達手順書へ参考資料として紹介した。〇件の PJ で利用した。

例 2：〇〇システムの導入検討において RFI で活用した。また RFP でもカスタムして利用した。

設問 2. 本書はシステムのセキュリティ要求仕様検討に役立ちましたか？（１つを選択・回答必須）

1. 非常に役に立った
2. おおむね役に立った
3. 一部役に立つ箇所があった
4. あまり役に立たなかった
5. 全く役に立たなかった

設問 3. 問題となったこと、疑問に思ったことはありますか？（任意）

設問 4. 地方公共団体の各種システムにおける脆弱性を少なくするためには本書の提供以外にどのような支援が必要ですか？（任意）

設問 5. 本書に対するご意見等、その他ありましたらお寄せください。（任意）

アンケートは以上です。ご協力ありがとうございました。

特記仕様書（雛形）の利用に当たって

次ページ以降の特記仕様書（雛形）は、脚注にて、検討の余地がある要件や各団体でアレンジした特記仕様書を作成するにあたっての留意事項、参考資料等へのリンクを付けています。雛形としてご利用の際はこれら脚注を削除してください。脚注を除いた Word 版は下記 URL にて公開しています。

地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）【Word 版・脚注なし】
https://www.lasdec.or.jp/cms/12,28369,84.html

なお、雛形を利用することによって、今まで実施してこなかった・考慮してこなかった作業が増えることから従来に比して提案金額の増額を要求する事業者があることが想定されます。予め考慮の上ご活用ください。

＜雛形のアレンジに当たっての留意事項＞

各団体の名称や期間等の情報を入れるべき箇所については、「*(団体名)*」や、「*(システム名)*」、「*本市(都道府県・区・町・村)*」、「*○月○日*」等、斜体で記載されています。適宜自団体のものに変更してください。

本文中、特定の用語を強調する場合は、「」（括弧）を用いています。また、本文中の特定の章や別紙その他の資料を示す場合、『』（二重かぎ括弧）を用いています。

なお、本書の内容をご理解いただくための補足資料として、解説書を用意しています。本書と併せてご活用いただけますと幸いです。

地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）解説書
https://www.lasdec.or.jp/cms/12,28369,84.html

（特記仕様書（雛形）はここからです）

（団体名）

（システム名）の

Webアプリケーションセキュリティに係る特記仕様書

〇年〇月

（団体名）（所属部課名）

1. 調達に関する基本事項

1.1. 本特記仕様書の目的と運用

本特記仕様書（以下「本書」という。）は、*本市（都道府県・区・町・村）*が導入する　*（システム名）*（以下「本システム」という。）のシステム調達仕様書（以下「仕様書」という。）に加え、本システムに追加で求めるセキュリティ要件、対応指針を記載するものである。受注者は本書に従わなくてはならない。

なお、本書に記載のないセキュリティ要求仕様に関しては仕様書による。契約書及び他の仕様書等の記載が本書と異なる場合は、本書を優先する。

1.2. 本システムのセキュリティ保証期間について

「セキュリティ保証期間」は次のとおりとし、期間中本書で定める対応を求める。

セキュリティ保証期間[1]

〇年〇月〇日　より　〇年〇月〇日

1.3. 提案時の提出物

以下を記載した書類を提出すること。

(1) 遵守状況一覧

本書で定める要求仕様の遵守状況の概要を示したもの。『別紙 3　遵守状況一覧』により提出すること。

(2) セキュリティ実装方針

『3.1. Web アプリケーション脆弱性対応』で示した脆弱性が Web アプリケーションに混入しないように構築するための方針を示したもの。『3.2.セキュリティ実装方針の提出』に従い、提出すること。パッケージ Web アプリケーション等自社開発でない場合はその開発元のものを提出すること。

(3) 重要事項説明書

本書で定める要求仕様の一部について、その履行が困難でかつ次のア、イにある各条件に合致する場合、代替案の提出を認める。代替案を提出する場合は『別紙 4-1 重要事項説明書』を参考として任意の書式にて作成すること。

ア 『2. 選定ソフトウェアに関する保守性・運用性要件』『8. 保守要件』に挙げた要件を満たすことが困難なソフトウェアを選定する場合

当該ソフトウェアについて次の項目を記載し、記載された代替案の内容の履行を保証すること。

- 当該ソフトウェア名称及びメーカー名
- 当該ソフトウェアの使用目的
- 要件を満たすことができない項目名及びその理由
- 満たすことができない要件の代替案及び代替案を採用する場合の費用見積（費用が必要な場合のみ）

[1] セキュリティ保証期間は、システムの稼働予定期間と同じであることが望ましい。（具体的には 5 年間を想定。期間の決定にあたっては解説書も参照されたい。）

イ 『3. Webアプリケーション脆弱性対応』『4. セキュリティ機能』に挙げた要件を満たすことが困難なソフトウェアを選定する場合

明示的に任意項目である旨の指定がある要件項目については、重要事項説明書による代替案を提出してよい。ただし、それ以外の項目は全て必須項目であり、代替案の提出を認めない。

2. 選定ソフトウェアに関する保守性・運用性要件

システムのプラットフォームソフトウェア（OS、ミドルウェア、ソフトウェア部品（ライブラリ等）を指す。）及びWebアプリケーションソフトウェア（パッケージWebアプリケーションを含み、以下「Webアプリケーション」という。）の選定にあたっては次の要件を満たすこと。また、一部要件を満たせない場合の提案方法については要件の記述に従うこと。

(1) 選定するプラットフォームソフトウェア及びWebアプリケーションのメーカーにおけるサポートライフサイクルポリシー[2]において、当該ソフトウェアのメーカーから*本市（都道府県・区・町・村）*に対して、セキュリティ保証期間の全期間中、脆弱性修正パッチ（以下「パッチ」という。）の開発及び提供がされることが確認できること。

(2) 当該ソフトウェアメーカーのサポートライフサイクルポリシーから判断して、セキュリティ保証期間の全期間を満たす形でパッチの開発及び提供がされない可能性があるソフトウェアを提案する場合『1.3. 提案時の提出物 (3) 』に従って資料を作成し、提出すること。

(3) 納品前の適切な時期に、*本市（都道府県・区・町・村）*と別途協議の上、納品時のパッチ適用状態を定める。定めたパッチは全て適用した状態で納品できること。

(4) プラットフォームソフトウェア及びWebアプリケーションは、当該ソフトウェアで新たに発見された脆弱性に関する情報やパッチのリリース情報（以下「パッチ情報」という。）がインターネットに遅滞なく公開されているものを選定すること。

(5) 当該ソフトウェアに係るパッチ情報がインターネットに公開されない場合、パッチ情報を*本市（都道府県・区・町・村）*に提供するための代替手段について『1.3. 提案時の提出物 (3) 』に従って資料を作成し、提出すること。

3. Webアプリケーション脆弱性対応

本システムにおけるWebアプリケーションの脆弱性対応として次の要件を満たすこと。

3.1. Webアプリケーション脆弱性対応

『別紙1 脆弱性リスト』で示す脆弱性が本システムに混入しないようWebアプリケーションを構築すること。

3.2. セキュリティ実装方針の提出

『3.1. Webアプリケーション脆弱性対応』で示した脆弱性がWebアプリケーションに混入しないように構築するための方針を『別紙5 セキュリティ実装方針(サンプル)』を参考として任意の書式で作成し、提出すること。なお、『別紙1 脆弱性リスト』に記載されている項目に関して漏らさず記載すること。

[2] 製品サポートの提供期間および提供内容の基本的な方針をまとめたもの

4. セキュリティ機能[3]

本システムにおけるセキュリティ機能は、次の仕様要件を満たすこと。

4.1. ログイン処理[4]

4.1.1. 利用者認証方式

利用者の認証方式はパスワード認証[5]とする。

4.1.2. アクセス制御機能

(1) 利用者の認証を行い、認証した利用者のみが本システムの「利用者認証を要する機能（画面)」を利用できるようにすること。
(2) 利用者認証を経ていない者は本システムの「利用者認証を要する機能（画面)」を利用できないようにすること。
(3) 「利用者認証を要する機能（画面)」は、セッションが終了した後は利用できないこと。
(4) 「利用者認証を要する機能（画面)」について、『5.3. 最終提出物 (1)』で示す画面遷移図に識別マーク等を使って示し、その通りに (1)、(2) の機能を実装すること。

4.1.3. パスワードに利用できる文字[6]

パスワードに利用する文字は以下を遵守すること。ただし、二要素認証の第 2 要素（ワンタイムパスワードトークンの生成するパスワードなど）はこの限りでない。

(1) パスワードに利用できる文字種は、英字（大文字、小文字を区別)、数字、記号の 3 種とし、それぞれ自由に利用[7]できること。
(2) パスワードに利用する文字数は 8 文字未満を受け付けないようにすること。また、少なくとも 64 文字のパスワードは受け入れられること。

4.1.4. ログインフォームの実装方法

パスワードの入力欄は入力した文字を伏字にする（input 要素において type 属性の値に password を指定（type=”password”）する）こと。又は、伏字にする・しないを選択できる機能を持つこと。

4.1.5. ログイン失敗時のメッセージ出力

パスワード認証に失敗した際に、利用者 ID の間違いか、パスワードの間違いかが区別できるメッセージを表示しないこと。

---

[3] 本書で示す要件は例であり、個別 Web アプリケーション毎に検討しなければならないことがあることを付言する。必要に応じて適宜追加要件等を仕様書に記載すること。また『4.6. 暗号化』等、一部の要件はオプション要件である。オプション要件は脚注に（オプション）と表記する。対象となるデータの重要性を考慮の上、適宜選択すること。
[4] 提案システムにログイン処理がある場合に求める。
[5] 本書ではごく一般的な Web アプリケーションを想定し、パスワード認証をする場合を例示している。他の認証方式の場合は別途検討する必要がある。
[6] 本項で示した内容、具体的な数値は例である。システム上の制約によっては変更が望ましいことがあるため、予め RFI 等により仕様を調査し、発注者が判断、決定すること。
[7] 最低限、英字と数字の両方が使えることを求めるべきである。

4.1.6. アカウントロック機能[8]

パスワードを連続して 10 回間違った場合は、当該アカウントを 30 分間ロックすること[9]。

4.1.7. オフライン攻撃からのパスワード保護

(1) パスワードは平文で保存せず、ソルトつきハッシュの形で保存すること。

(2) ソルトは利用者毎に別々に設定すること。

(3) ソルトは最低 5 文字以上[10]とること。

4.1.8. セッション管理機能

(1) 利用者のセッション管理にはプログラミング言語や Web アプリケーション実行環境の備えるセッション管理機構を用いること。

(2) ログイン状態にある利用者のセッション識別のための情報（セッション ID）は、クッキーを用いて保持すること。

4.1.9. セッションの開始

セッションはログイン処理成功後に開始すること。

4.1.10. セッションの有効期間[11]

セッションの有効期間は 30 分とすること。

4.1.11. セッションの終了

次の場合はセッションを終了し、セッション情報を破棄すること。

(1) 利用者がログアウト機能を呼び出した場合（ログアウトボタンを押す等）

(2) 最後にページが表示された時刻を起点としてセッションの有効期間を超えた（セッションタイムアウト）場合

4.2. 認可処理[12]

4.2.1. 認可処理の要件定義と文書化

認可処理は次のとおり文書化し、権限毎の役割をロールとして作成すること。

(1) 認可処理の必要な機能、情報を識別して、認可処理の必要な画面には、『5.3. 最終提出物　(1)』で示す画面遷移図上に識別マーク等をつけること。

(2) 各ロールと権限を一覧表（権限マトリックス）に整理すること。

---

[8] 本項で示した具体的な数は目安であり、サービスの特性を考慮して発注者が判断、決定すること。また、「管理者の操作により利用者のアカウントロックが解除できること」という要件を追加しても良い（オプション）。

[9] 本書を利用する団体において、上位ポリシーにアカウントロックの規定がある場合は、当該規定も満足するように、ロックに至る試行回数とロック時間を変更すること。

[10] 本項で示した数字（文字数）は例である。

[11] 本項で示した具体的な数値（時間）は例である。

[12] 提案システムに認可処理がある場合に求める。

4.2.2. 認可処理の実装

(1) 各利用者の権限確認には、セッション変数に保存された利用者識別情報（利用者 ID 等）を基準とすること。

(2) 認可を要する情報表示や機能実行をする前に、実行中の利用者が、当該情報の表示や機能を実行するための権限を有していることを画面毎に確認すること。

(3) 認可されなかった場合は、適切なエラー表示をすること。

4.3. アカウント管理[13]

4.3.1. 利用者登録（アカウントの作成）時における登録メールアドレスの確認[14]

(1) 利用者登録時にメールアドレスを登録させること。

(2) 利用者によって登録されたメールアドレスに対してメールを送付し、登録メールアドレスが利用者に利用されているアドレスであることを確認する処理を実装すること。

(3) 登録メールアドレスが利用者に利用されているアドレスであると確認できた後に本システムにおける利用者登録を完了（登録の確定）とし、利用者登録の完了を経てからアカウントを作成すること。

(4) 登録されたメールアドレスに対してメールを送付する際に、利用者が登録したパスワードを記載しないこと。

4.3.2. 利用者 ID の重複防止機能

利用者 ID が重複しないよう、チェック処理を含めること。

4.3.3. 登録メールアドレス変更機能

(1) 利用者が登録したメールアドレスを変更する機能を実装すること。

(2) メールアドレス変更機能の実行前に、パスワードの入力を利用者に求め、正しいパスワードであることを確認すること。

(3) メールアドレス変更機能の実行後は、利用者登録時と同様の処理を経ること。

(4) 変更前のメールアドレス（旧メールアドレス）にも登録メールアドレスが変更された旨の通知をメール送付すること。

4.3.4. パスワード変更機能

(1) 利用者がパスワードを変更する機能を実装すること。

(2) パスワード変更機能の実行前に、現在のパスワードの入力を利用者に求め、正しいパスワードであることを確認すること。

(3) パスワード変更機能の実行後に、登録されているメールアドレスへ、パスワードが変更された旨の通知をメール送付すること[15]。

---

[13] 提案システムにログイン処理がある場合に必要に応じて求める。「利用者のメールアドレス」を登録させることで実現する機能については利用者のメールアドレス登録をしない場合はこれを求めない。

[14] 利用者登録時にメールアドレスを登録する場合に求める。

[15] メールアドレスの登録がある場合に求める。

4.3.5. パスワードリセット機能[16]

利用者がパスワードを失念した場合の対処機能は次の (1)、(2) いずれかの方式とし、(3) または (4) の要件を満たすこと。(利用者確認の手段[17]として、予め登録したメールアドレスに宛てたメールが受信できることを用いる。)

(1) パスワードリセット機能を利用するための URL を登録メールアドレスにメール送付する方式
(2) 仮パスワードを発行し、メールで通知する方式（仮パスワードでログインした場合は、パスワード変更機能のみが利用できるものとする）
(3) （1）の機能の実装に際して、第三者がパスワードリセット機能を使えないように、URL には十分長い乱数による秘密情報（以下「トークン」という。）をつけること。
(4) （2）の機能に対する総当たり攻撃対策を施すこと。

4.3.6. 管理者によるアカウント削除・一時利用停止機能[18]

(1) 管理者による利用者アカウントの削除機能を実装すること。
(2) 管理者による利用者アカウントの一時利用停止機能を実装すること。

4.3.7. 利用者によるアカウント削除機能[19]

(1) 利用者による自身のアカウント削除機能を実装すること。
(2) アカウント削除機能の実行前に、パスワードの入力を利用者に求め、正しいパスワードであることを確認すること。
(3) アカウント削除機能の実行後、登録されていたメールアドレスにアカウントが削除された旨の通知をメール送付すること。[20]

4.4. ログイン状態にある利用者の意図に反した機能実行の防止機能

外部リンク等により本システムの画面（機能）に遷移するだけで、本システムの機能がログイン状態にある利用者の意図に反して実行されることを防止すること。なお、ここで言う「ログイン状態にある利用者の意図に反した機能実行の防止」とは、クロスサイト・リクエスト・フォージェリ（以下「CSRF」という。） 対策及びクリックジャッキング対策を指す。

4.4.1. 該当画面の洗い出し

CSRF 対策及びクリックジャッキング対策を施すべき画面（機能）を洗い出し、『5.3. 最終提出物 (1)』で示す画面遷移図上に識別マーク等を付けること。なお、当該機能のページは POST メソッドで呼び出すようにすること。

16 （オプション）発注者がパスワードリセット機能を求めない場合は、本項目を削除すること。
17 要件として「パスワードを失念した利用者に対し、予め登録してある情報に対する回答を正答することを用いる」を利用者確認の手段として追加しても良い。なお、同要件を追加する際は「予め登録してある情報に対する回答の正誤はシステムからは回答しないこと」としなければならない。
18 （オプション）発注者が管理者によるアカウントの削除・一時停止機能を求めない場合は本項目を削除すること。
19 （オプション）発注者が利用者によるアカウント削除機能を求めない場合は本項目を削除すること。
20 メールアドレスの登録がある場合に求める。

4.4.2. CSRF 対策

対策対象の画面（機能）を実行する前のページにてトークンを生成して埋め込み、処理を実行する際は、その値が正しい場合のみ実行すること。

4.4.3. クリックジャッキング対策

対象画面の 1 つ手前の画面にて、次の (1)、(2) いずれかの HTTP レスポンスヘッダを出力すること。なお、対象画面以外にも出力してよい。

(1) X-FRAME-OPTIONS: DENY

(2) X-FRAME-OPTIONS: SAMEORIGIN

4.5. ログ出力

システム監査、事故調査を目的として次によりログを出力・保管すること。

4.5.1. 出力するログの種類

次のログを出力すること。

(1) Web サーバのアクセスログ

(2) アプリケーションログ

(3) データベースのアクセスログ [21]

(4) エラーログ

4.5.2. 出力しないログの種類

次のログ取得については、構築時、動作テスト時には出力してよいが、本番稼働時までに無効にしておくこと。ただし、システム検証やトラブル対応のために、*本市（都道府県・区・町・村）*の管理者が認めた場合は除く。

(1) デバッグログ

4.5.3. アプリケーションログで取得するイベント

次のイベントをアプリケーションログにて取得すること。なお、次に記載していない他のイベントも取得してもよい。

(1) ログイン（成功・失敗問わず）

(2) ログアウト

(3) アカウントロック

(4) 利用者登録・登録削除

(5) 利用者の登録内容更新

(6) 利用者のパスワード変更

(7) 秘密情報の参照

(8) その他重要な操作 [22]（CSRF対策の対象となる操作は必須）

[21] （オプション）発注者がデータベースのアクセスログを求めない場合は削除すること。

4.5.4. 出力するログの項目[23]

次の情報をログに含めること。なお、これ以外の情報を含めても良い。

(1) アクセス日時（年、月、日、時、分、秒）
(2) アクセス元 IP アドレス（IPv4 又は IPv6）
(3) 利用者 ID
(4) アクセス対象（URL 又はページ番号等）
(5) 操作内容
(6) 操作対象（利用者 ID、文書 ID など）
(7) 実行結果（成功あるいは失敗、処理件数など）

4.5.5. 出力しないログの項目

次の情報はログの項目として取得しないこと。

(1) パスワード

4.5.6. ログからの情報漏えい・改ざん対策

(1) ログが不正に参照・変更・削除されないよう保護すること。
(2) ログから個人情報等の秘密情報が漏えいすることを防ぐため、ログの目的（監査、事故追跡）を損なわない範囲で秘密情報を含めない処理又は秘密情報の一部のみの出力(マスク処理)をすること。

4.5.7. ログの保管

(1) ログの保管年限は 3 年とする。[24]
(2) ログの安全な保管方法（媒体、保管フォーマット、保管場所等）を定めること。

4.6. 暗号化[25]

4.6.1. 利用者と本システム間における Web アプリケーション通信の暗号化

(1) システムで送受信する情報のうち、秘密情報[26]に該当するものを要件定義時に一覧表にまとめること。
(2) 利用者と本システム間で秘密情報を送受信する際に利用する画面（機能）を SSL/TLS の利用対象とし、『5.3. 最終提出物　(1)』で示す画面遷移図上に識別マーク等を付け、そのとおりに実装すること。
(3) サーバ証明書は利用を想定するすべてのブラウザで警告の出ないものを使用し、証明書の発行先名は、運営者の名称とする。地方公共団体組織認証基盤（LGPKI）を用いる場合は、Firefox を利用想定ブラウザから外すこと。
(4) SSL2.0 は使用しない設定にすること。

---

[22] 発注者のシステムごとに検討し、「追跡可能としておく必要がある操作」を洗い出すこと。
[23] アプリケーションのログにおける（2)、(4) はウェブサーバのアクセスログと紐づけられるのであれば不要。
[24] 本項で示した具体的な数値（年限）は例である。
[25] （オプション）発注者が適宜選択し、暗号化を求めない項目は削除すること。
[26] 秘密情報の定義は親文書である仕様書で定義しておくこと。

4.6.2. 内部の通信に関する補足

インターネットを介さない、内部の秘密通信については暗号化ではない方法による通信の秘密確保も可とする。通信の秘密確保方法について提案書に記載すること。

4.6.3. データベースの暗号化

(1) 秘密情報をデータベースに保存する際は暗号化を施すこと。
(2) 暗号化アルゴリズムは電子政府推奨暗号リスト[27]に記載されたアルゴリズムを用いること。
(3) 暗号鍵の管理方法を提案書に記載すること。

4.6.4. ファイルの暗号化

(1) 秘密情報をファイルに保存する際は暗号化を施すこと。
(2) 暗号化アルゴリズムは電子政府推奨暗号リストに記載されたアルゴリズムを用いること。
(3) 暗号鍵の管理方法を提案書に記載すること。

5. テスト（検査）要件

本システムの構築にあたって次のテスト（検査）を行い、報告書を提出すること。

5.1. 開発時中間検査[28]

受注者は、開発途中に*本市（都道府県・区・町・村）*が指定する時期に、以下の中間検査を実施し、報告すること。

仕様　　:『LASDECウェブ健康診断仕様について 平成22年度版[29]』
検査箇所:受注者、*本市（都道府県・区・町・村）*協議の上、抜取検査が可能な箇所を特定する。
提出物　:セキュリティ検査結果報告書、検査ログ（データ）

5.2. 出荷時検査（最終検査）

(1) 受注者は最終検査として脆弱性の有無を調べるセキュリティ検査を実施し、本書の要件を満たしていることを確認すること。
(2) 検査手法（概要）、検査項目、検査箇所、検査箇所ごとの検査結果を記載したセキュリティ検査報告書を任意の書式で作成し、提出すること。
(3) セキュリティ検査ログのデジタルデータをセキュリティ検査報告書に含めて提出すること。検査ログを提出できない合理的な理由があると認めるときは、DVD-R など変更できない媒体に書き込み、セキュリティ保証期間は受注者が厳重に保管するとともに、データのハッシュ値を提出すること。
(4) 納品時における OS、ミドルウェア等ソフトウェアのバージョン及び最新パッチのリリース状況を確認すること。

---

[27] 電子政府推奨暗号リスト http://www.cryptrec.go.jp/list.html
[28] （オプション）発注者が中間検査を求めない場合は本項目を削除すること。
[29] 発注時点で最新のものを利用すること。

5.3. 最終納品物

本書による納品物は次のとおり。

(1) 画面遷移図

次の各項目の識別マーク等をつけた画面遷移図を提出すること。

ア アクセスするためにログイン処理が必要な画面（機能）

イ 認可処理の必要な画面（機能）

ウ 暗号化通信の適用画面（機能）

エ CSRF 対策の実施画面（機能）

オ パッケージソフトウェアを用いる場合、カスタマイズした画面（機能変更した画面）

カ パッケージソフトウェアを用いる場合、新規追加した画面（機能追加した画面）

(2) 権限マトリックス表

『4.2.1. 認可処理の要件定義と文書化』に従い作成された各ロールと権限を一覧にした表を提出すること。

(3) セキュリティ検査報告書

次の資料を提出すること。

ア『5.1.開発時中間検査』に従い作成されたセキュリティ検査報告書[30]

イ『5.2.出荷時検査（最終検査)』に従い作成されたセキュリティ検査報告書

ウ『5.2.出荷時検査（最終検査)』にあるセキュリティ検査時の検査ログデジタルデータ。提出時の媒体等は容量を勘案の上、別途指定する。

エ 納品時のソフトウェアの最新パッチに関する情報が掲載されている URL 又は最新パッチに関する情報を入手する手段を記載した報告書。書式は任意とする。

オ 納品時のソフトウェアに納品時点の最新パッチが適用されていない状態で納品する場合は、当該パッチ未適用時にもたらされる脅威に関する説明及びその回避策を記載した報告書。書式は任意とする。

6. 検収

本システムの Web アプリケーション脆弱性対応は次のとおり検収する。

6.1. 脆弱性検査結果の確認[31]

(1) 本書で定める要求を満たしていることを受注者の提出した検査報告書をもって検査する。

(2) 本書で定める要求を満たしていることを『LASDECウェブ健康診断仕様について 平成 22 年度版[32]』を用いて*本市（都道府県・区・町・村）*が検査する。

(3) 本書で定める要求を満たしていることを*本市（都道府県・区・町・村）*が指定する第三者の実施する脆弱性診断結果をもって検査する。

---

30 （オプション）発注者が中間検査を求めない場合は本項目を削除すること。

31 発注者は（1）～（3）の中から１つ以上を選択すること。なお、これは例である。

32 発注時点で最新のものを利用すること。

6.2. 実装状況報告書の確認

『3.2.セキュリティ実装方針の提出』に示したセキュリティ実装方針に基づき、『別紙 6 実装状況報告書』を検査する。

7. セキュリティ保証期間中の脆弱性対応

本システムにおけるセキュリティ保証期間中の脆弱性対応として、次の事項について誠意をもって行うこと。

7.1. セキュリティ保証期間中の脆弱性対応（パッチの開発・提供）

セキュリティ保証期間中に発見された脆弱性への対処について、以下の場合は追加費用なしで修補（パッチの開発・提供）すること。

(1) 『別紙 1 脆弱性リスト』に含まれる脆弱性で、受注者が対処済みである旨をセキュリティ実装方針によって宣言したもの。
(2) 本書によらず、受注者が追加提案として対処を約束した脆弱性。

なお、修補（パッチの開発・提供）以外の代替案によって脆弱性の影響を回避できる場合は、受注者、*本市（都道府県・区・町・村）*双方協議の上、代替案による対処も可とする。

ただし、次の場合は対応内容及び費用負担について、受注者、*本市（都道府県・区・町・村）*双方協議の上、決定する。

ア 『別紙 1 脆弱性リスト』に含まれない脆弱性が発見されたとき。
イ 受注者が追加提案として対処を約束した脆弱性に含まれない脆弱性が発見されたとき。

8. 保守要件[33]

本システムの保守対応（パッチの適用作業又はバージョンアップ作業）として、次の事項について誠意をもって行うこと。

8.1. 脆弱性対応基本方針

(1) 脆弱性対応作業費用については別途保守契約で定める。セキュリティ保証期間中に脆弱性対応のためのパッチ適用作業やバージョンアップ作業が発生し、費用を要する場合は、その費用を予め運用費用見積に含め、提出すること。
(2) セキュリティ保証期間中に本システムが、『別紙 1 脆弱性リスト』に記載の脆弱性に対応できていないことが判明[34]した場合、これを追加費用なしで修補（パッチの適用作業又はバージョンアップ作業）すること。

[33] 保守を別ベンダー、別契約とする場合には、当該保守契約書に『8. 保守要件』の内容を記載し、本項を削除すること。
[34] システム導入後、脆弱性対応ができていないことが後日判明することがある。次のような場合が考えられる。脆弱性を発見した第三者の通報により判明する場合／LASDEC の脆弱性診断等の実施により判明する場合／実際にセキュリティインシデント（サイバー攻撃被害の顕在化）が発生し、判明する場合

8.2. パッチ適用ポリシー[35]

(1) ソフトウェアのパッチは、パッチリリース後 1 週間以内に適用・非適用の方針を決めること。また最終結論の方針に依らず、その判断理由について報告すること。

(2) パッチ適用を決定した場合、パッチリリース後 2 週間以内に適用作業を完遂すること。また、適用作業終了後は、パッチ適用状況（適用の成功・不成功、動作への影響有無等）を報告すること。

(3) 前項 (1)、(2) を保証できない場合、『1.3. 提案時の提出物　(3)』に従って資料を作成し、提出すること。

以上

[35] 本項で示した内容、具体的な数値（期間）は例である。

別紙１ 脆弱性リスト

本システムに混入しないよう対処を求める脆弱性は次のとおり。なお、各脆弱性の定義は「脆弱性名称の定義に関する参照先」にて確認すること。

「脆弱性名称の定義に関する参照先」の各（1）～（3）で示す参照先記載内容は次のとおり。なお、一部の脆弱性定義は（1）～（3）に該当するものがないため、当該名称解説 URL を記載している。

(1) IPA 『安全なウェブサイトの作り方 改訂第５版(2012 年３月 30 日改訂)』のページと、章番号記載
http://www.ipa.go.jp/security/vuln/websecurity.html
(2) CWE - Common Weakness Enumeration のCWE番号[36]を記載。※同サイトにおける脆弱性名称を一部和訳。
http://cwe.mitre.org/
(3) LASDEC『ウェブ健康診断仕様について（平成 22 年度版・一般公開用)』のページと、識別記号記載
https://www.lasdec.or.jp/cms/12,1284.html#siyou-h22

No	脆弱性名称		脆弱性名称の定義に関する参照先	
1	SQL インジェクション		(1)	P.6 - 1.1
			(2)	CWE-89
			(3)	P.7 - (A)
2	OS コマンド・インジェクション		(1)	P.10 - 1.2
			(2)	CWE-78
			(3)	P.9 - (D)
3	ディレクトリ・トラバーサル脆弱性		(1)	P.13 - 1.3
			(2)	CWE-98
			(3)	P.10 - (G)
4	「ログイン機能」の不備		(①～④に該当するもの)	
	①	推測可能なセッション ID	(1)	P.18 - 4-(ⅰ)
			(2)	CWE-330
			(3)	P.13 - (K) - 2
	②	URL 埋め込みのセッション ID の外部への漏えい	(1)	P.19 - 4-(ⅱ)
			(2)	CWE-522
			(3)	P.13 - (K) - 4, 5
	③	クッキーのセキュア属性不備	(1)	P.19 - 4-(ⅲ)
			(2)	CWE-614
			(3)	P.13 (K) - 3
	④	セッション ID の固定化	(1)	P.19 - 4-(ⅳ)-a、P.20 - 4-(ⅳ)-b
			(2)	CWE-384
			(3)	P.13 (K) - 1

[36] IPA 共通脆弱性タイプ一覧 CWE 概説 http://www.ipa.go.jp/security/vuln/CWE.html

No	脆弱性名称		脆弱性名称の定義に関する参照先	
5	クロスサイト・スクリプティング(XSS)		(1)	P.22 - 1.5
			(2)	CWE-79
			(3)	P.8 - (B)
6	利用者の意図に反した実行の防止機能の不備		(①、②に該当するもの)	
	①	クロスサイト・リクエスト・フォージェリ (CSRF)	(1)	P.29 1-6
			(2)	CWE-352
			(3)	P.8 (C)
	②	クリックジャッキング	(1)	該当なし
			(2)	該当なし
			(3)	該当なし
				＜参考＞ http://en.wikipedia.org/wiki/Clickjacking
7	メールヘッダ・インジェクション脆弱性		(1)	P37 - 1.8
			(2)	CWE-93
			(3)	P.10 - (F)
8	「アクセス制御」と「認可処理」の不備			(次の①、②に該当するもの)
	①	アクセス制御	(1)	P.40 - 9-(ⅰ)
			(2)	CWE-284
			(3)	P.14 - (L)
	②	認可処理	(1)	P.40 - 9-(ⅱ)
			(2)	CWE-264
			(3)	P.14 - (L)
9	HTTP ヘッダ・インジェクション		(1)	P.44 - 1.7
			(2)	CWE-113
			(3)	P.11 - (I)
10	eval インジェクション		(1)	該当なし
			(2)	CWE-95
			(3)	該当なし
11	競合状態の脆弱性		(1)	該当なし
			(2)	CWE-366
			(3)	該当なし
12	意図しないファイル公開		(1)	該当なし
			(2)	CWE-425 、CWE-548
			(3)	P.9 - (E)

No	脆弱性名称	脆弱性名称の定義に関する参照先	
13	アップロードファイルによるサーバ側スクリプト実行	(1)	該当なし
		(2)	CWE-434
		(3)	該当なし
14	秘密情報表示時のキャッシュ不停止	(1)	該当なし
		(2)	CWE-524
		(3)	該当なし
15	オープンリダイレクタ脆弱性(意図しないリダイレクト)	(1)	該当なし
		(2)	CWE-601
		(3)	P11 - (H)
16	クローラへの耐性	(1)	該当なし
		(2)	該当なし
		(3)	P.15 - 2.5

別紙 2（参考）要求仕様チェックシート － 発注者用 －

雛形を利用するにあたって、基本情報の整理と Web アプリケーションの機能・役割により選択する必要がある機能要件やオプション要件についてまとめてあります。各団体で雛形をベースに作成する特記仕様書におけるアレンジが必要な箇所の確認及び意思決定メモにご活用ください。

分類	チェック項目（要件）	モデルプラン関係箇所（章番号）	内容（メモ）	必須要件 or 任意要件	備考
自団体情報	団体名	表紙		―	表紙に団体名を入れてください。文中における団体名は「*本市(都道府県・区・町・村)*」としています。適宜修正（置換）してください。
	所属部課名	表紙		―	表紙に記載してください。
	システム名	表紙 1.1.		―	文中では「本システム」としています。必要に応じて適宜修正（置換）してください。
基本情報	提案を求める範囲	8.	□開発及び保守 □開発のみ	―	□開発及び保守の場合：該当箇所を残す。 □開発のみの場合　　：該当箇所を削除。
	セキュリティ保証期間	1.2.	年　月　から　年　月 まで	―	システムの稼働予定期間と同じであることが望ましいです。なお、解説書ではサービス開始から 5 年間を提案しています。
	システム稼働予定期間	―	年　月　から　年　月 まで	―	セキュリティ保証期間の検討のためのメモです。
アクセス制御・認可	認証処理	4.1. 4.2. 4.3. 4.4.	□要　□不要　□提案を求める		□要　関係箇所を残す □不要　関係箇所を削除 □提案を求める　雛形をアレンジする
	認証方式	4.1.1.	□パスワード　□提案を求める		□パスワード　関係箇所を残す □提案を求める　雛形をアレンジする

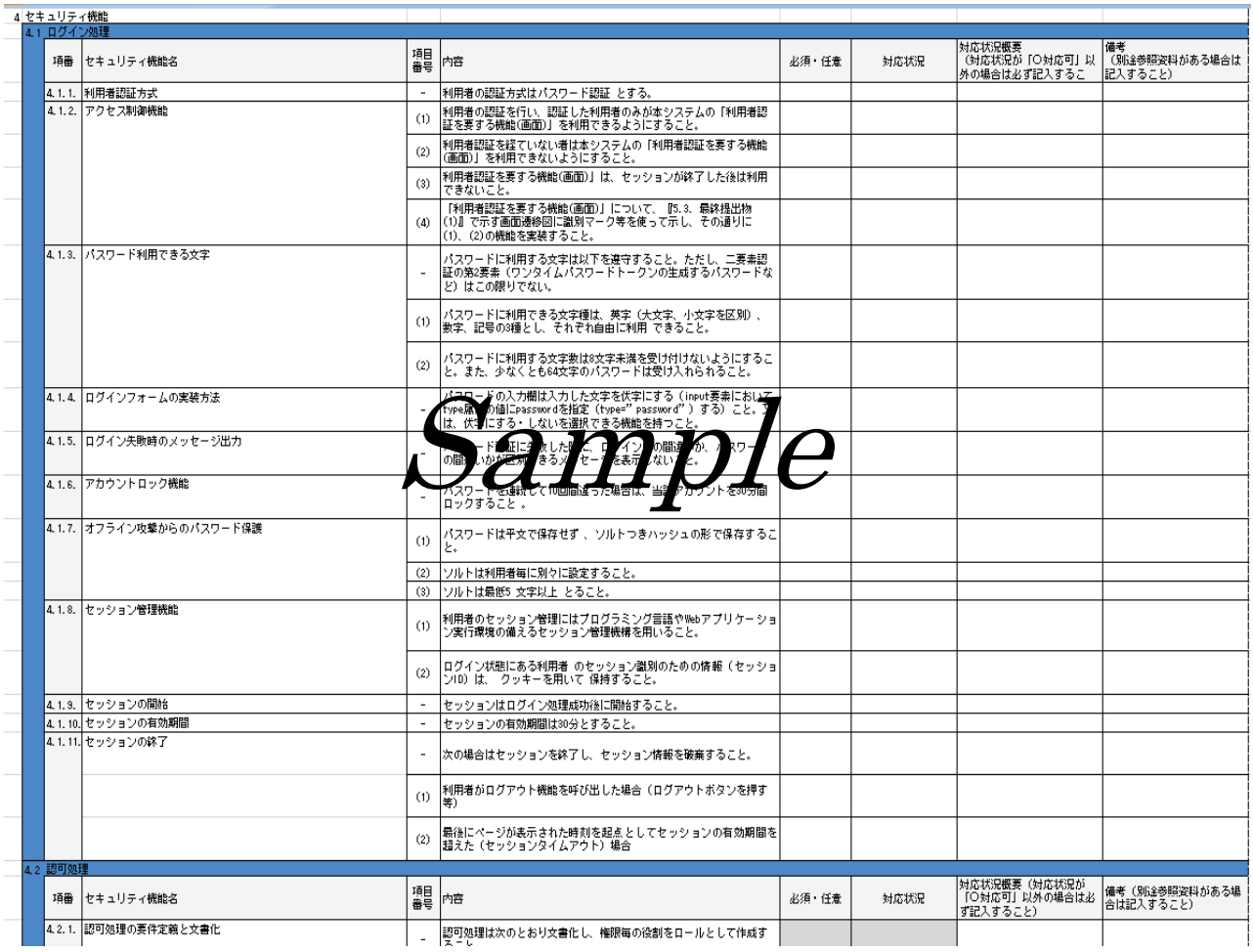
分類	チェック項目（要件）	モデルプラン関係箇所（章番号）	内容（メモ）	必須要件 or 任意要件	備考
アクセス制御・認可（続き）	認可処理	4.2.	□要　□不要　□提案を求める		□要　関係箇所を残す □不要　関係箇所を削除 □提案を求める　雛形をアレンジする
	利用者のメールアドレス登録	4.3.1. 4.3.3.(3)、(4) 4.3.4.(3) 4.3.5. 4.3.7.(3)	□してもらう □してもらわない □提案を求める		□してもらう　関係箇所を残す □してもらわない　関係箇所を削除 □提案を求める　雛形をアレンジする
	パスワードリセット機能（※オプション）	4.3.5.	□要　□不要　□提案を求める		□要　関係箇所を残す □不要　関係箇所を削除 □提案を求める　雛形をアレンジする
	管理者によるアカウント削除・一時利用停止機能（※オプション）	4.3.6.	□要　□不要　□提案を求める		□要　関係箇所を残す □不要　関係箇所を削除 □提案を求める　雛形をアレンジする
ログ	ログの保管期間	4.5.7.(1)	年		本書では3年としていますが、システム特性、ログ量等を加味の上、決定してください。
	データベースログの取得（※オプション）	4.5.1.(3)	□要　□不要　□提案を求める		□要　関係箇所を残す □不要　関係箇所を削除 □提案を求める　雛形をアレンジする
暗号化	利用者とシステム間の通信の暗号化（※オプション）	4.6.1.	□要　□不要　□提案を求める		□要　関係箇所を残す □不要　関係箇所を削除 □提案を求める　雛形をアレンジする

分類	チェック項目（要件）	モデルプラン関係箇所（章番号）	内容（メモ）	必須要件 or 任意要件	備考
暗号化（続き）	内部の通信 （※オプション）	4.6.2.	□ある　□ない　□不明（提案を求める）		□ある　関係箇所を残す □ない　関係箇所を削除 □不明（提案を求める）　雛形をアレンジする
	データベースの暗号化 （※オプション）	4.6.3.	□要　□不要　□提案を求める		□要　関係箇所を残す □不要　関係箇所を削除 □提案を求める　雛形をアレンジする
	ファイルの暗号化 （※オプション）	4.6.4.	□要　□不要　□提案を求める		□要　関係箇所を残す □不要　関係箇所を削除 □提案を求める　雛形をアレンジする
検査	開発時中間検査 （※オプション）	5.1. 5.3.(3)ア	□実施する　□実施しない		□実施する　関係箇所を残す □実施しない　関係箇所を削除
検収	脆弱性検査結果の確認方法 （※１つ以上選択。複数選択も可）	6.1.	□書類審査　□自主検査　□第三者検査		選択した方法のみ記載を残す。
その他（基本要件等）	秘密情報 （個人特定情報）	－		－	「氏名、住所、電話番号、メールアドレス、その他」等。特記仕様書ではなく、仕様書（親文書）に定義しておくことを想定しています。
	秘密情報 （プライバシー情報）	－		－	「図書蔵書検索予約システムにおける貸し出し履歴」等。特記仕様書ではなく、仕様書（親文書）に定義しておくことを想定しています。
	秘密情報 （その他）	－		－	その他の重要な情報等。特記仕様書ではなく、仕様書（親文書）に定義しておくことを想定しています。

分類	チェック項目（要件）	モデルプラン関係箇所（章番号）	内容（メモ）		必須要件 or 任意要件	備考
その他（基本要件等）（続き）	利用者 OS 環境条件	－	パソコン	□Windows □Linux □Mac □その他（ ）	－	特記仕様書ではなく、仕様書（親文書）に定義しておくことを想定しています。
			スマートフォン	□iPhone □Android □その他（ ）		
			フィーチャーフォン	□i モード □Yahoo!ケータイ □EZweb □その他（ ）		
			タブレット	□iPad □Android タブレット □その他（ ）		
	利用者ブラウザ環境条件	4.6.1.(3)	□Internet Explorer（ ） □Firefox（ ） □Google Chrome（ ） □Opera （ ） □Safari （ ） □その他 （ ）		－	ブラウザ名、バージョンを記載します。 特記仕様書ではなく、仕様書（親文書）に定義しておくことを想定しています。
	パッケージ Web アプリケーションのカスタマイズ	5.3.(1)オ、カ	□する □しない □不明（提案を求める）		－	□する 関係箇所を残す □しない 関係箇所を削除 □提案を求める 雛形をアレンジする

別紙 3　遵守状況一覧

別紙 3 遵守状況一覧は、モデルプランの要件を表に転記したものです。Excel シートにて提供しています。
（以下の図は資料の一部イメージです）
次の URL から入手してください。
https://www.lasdec.or.jp/cms/12,28369,84.html



4 セキュリティ機能

4.1 ログイン処理

項番	セキュリティ機能名	項目番号	内容	必須・任意	対応状況	対応状況概要（対応状況が「○対応可」以外の場合は必ず記入すること）	備考（別途参照資料がある場合は記入すること）
4.1.1.	利用者認証方式	-	利用者の認証方式はパスワード認証 とする。				
4.1.2.	アクセス制御機能	(1)	利用者の認証を行い、認証した利用者のみが本システムの「利用者認証を要する機能(画面)」を利用できるようにすること。				
		(2)	利用者認証を経ていない者は本システムの「利用者認証を要する機能(画面)」を利用できないようにすること。				
		(3)	利用者認証を要する機能(画面)」は、セッションが終了した後は利用できないこと。				
		(4)	「利用者認証を要する機能(画面)」について、『5.3. 最終提出物(1)』で示す画面遷移図に識別マーク等を使って示し、その通りに(1)、(2)の機能を実装すること。				
4.1.3.	パスワード利用できる文字	-	パスワードに利用する文字は以下を遵守すること。ただし、二要素認証の第2要素（ワンタイムパスワードトークンの生成するパスワードなど）はこの限りでない。				
		(1)	パスワードに利用できる文字種は、英字（大文字、小文字を区別）、数字、記号の3種とし、それぞれ自由に利用 できること。				
		(2)	パスワードに利用する文字数は8文字未満を受け付けないようにすること。また、少なくとも64文字のパスワードは受け入れられること。				
4.1.4.	ログインフォームの実装方法	-	パスワードの入力欄は入力した文字を伏字にする（input要素においてtype属性の値にpasswordを指定（type=”password”）する）こと。また、伏字にする・しないを選択できる機能を持つこと。				
4.1.5.	ログイン失敗時のメッセージ出力	-	パスワード認証に失敗した際、ログインの間違いか、パスワードの間違いかが判別できるメッセージを表示しないこと。				
4.1.6.	アカウントロック機能	-	パスワードを連続して10回間違えた場合は、当該アカウントを30分間ロックすること 。				
4.1.7.	オフライン攻撃からのパスワード保護	(1)	パスワードは平文で保存せず 、ソルトつきハッシュの形で保存すること。				
		(2)	ソルトは利用者毎に別々に設定すること。				
		(3)	ソルトは最低5 文字以上 とること。				
4.1.8.	セッション管理機能	(1)	利用者のセッション管理にはプログラミング言語やWebアプリケーション実行環境の備えるセッション管理機構を用いること。				
		(2)	ログイン状態にある利用者 のセッション識別のための情報（セッションID）は、 クッキーを用いて 保持すること。				
4.1.9.	セッションの開始	-	セッションはログイン処理成功後に開始すること。				
4.1.10.	セッションの有効期間	-	セッションの有効期間は30分とすること。				
4.1.11.	セッションの終了	-	次の場合はセッションを終了し、セッション情報を破棄すること。				
		(1)	利用者がログアウト機能を呼び出した場合（ログアウトボタンを押す等）				
		(2)	最後にページが表示された時刻を起点としてセッションの有効期間を超えた（セッションタイムアウト）場合				

4.2 認可処理

項番	セキュリティ機能名	項目番号	内容	必須・任意	対応状況	対応状況概要（対応状況が「○対応可」以外の場合は必ず記入すること）	備考（別途参照資料がある場合は記入すること）
4.2.1.	認可処理の要件定義と文書化	-	認可処理は次のとおり文書化し、権限毎の役割をロールとして作成すること。				

別紙 4-1　重要事項説明書[37]　(1/2)

重要事項説明書　　事業者名

No	項目		重要事項の概要	
	仕様書等の記載内容		重要事項	説明書ページ
	仕様書等の名称	記載内容		
○				
○				

[37] 本書は例であり、提出を求める意義、意味を確認した上で、団体、提案者双方がわかり易いものを工夫いただきたい。

別紙 4-1　重要事項説明書　(2/2)

仕様書にある対策と同程度に脅威を削減できる代替案　説明書（No.○）

No	項目		代替案の概要	
	仕様書等の記載内容		代替案	説明書ページ
	仕様書等の名称	記載内容		
○				

代替案の詳細説明

別紙 4-2　重要事項説明書（サンプル[38]）（1/3）

重要事項説明書　　事業者名　○×株式会社

No	項目		重要事項の概要	
	仕様書等の記載内容		重要事項	説明書ページ
	仕様書等の名称	記載内容		
1	○○システムにおける Web アプリケーションセキュリティ特記仕様書	4.1.3 パスワード利用できる文字	特記仕様書において「少なくとも 64 文字のパスワードは受け入れられること」と記載されていますが今回提案するシステムは「32 文字まで」となり、この変更ができません。	P.○
2	同上	8.2. パッチ適用ポリシー	パッチ適用ポリシーに示された対応期間内にパッチ適用できない可能性があります。	P.○

[38] サンプルで示した内容は例であり、本書ではその内容を肯定も否定もしていない。

別紙 4-2　重要事項説明書（サンプル）(2/3)

仕様書にある対策と同程度に脅威を削減できる代替案　説明書（No. 1）

No	項目		代替案の概要	
	仕様書等の記載内容		代替案	説明書ページ
	仕様書等の名称	記載内容		
1	○○システムにおける Web アプリケーションセキュリティ特記仕様書	4.1.3 パスワード利用できる文字	「利用者に安全性の高いパスワードを強制する機能」及び仕様に記載の要件を複合的に実装することによる回避	P.○

代替案の詳細説明

（仕様を満たせない背景概要）

仕様書において「少なくとも 64 文字のパスワードは受け入れられること」と記載されていますが今回提案するシステムは「32 文字まで」となり、この仕様変更ができません。

（理由）

今回構築するシステムの認証機能は××社製 ID 管理システムと連携しています。当該システムの仕様が 32 文字までとなっているためです。

（代替案）

セキュリティ面においては、パスワードの最大文字数の減少によるリスクを、既に特記仕様書でご指定頂いている次の要件①、②に追加で③の実装を提案します。

①パスワードの文字種は「英字（大文字と小文字）＋数字＋記号」を混在させる

②アカウントロック

③パスワード辞書を使った「利用者に安全性の高いパスワード登録を強制する機能」

これらの複合的実装により、文字数不足という仕様による「利用者が安直なパスワード設定をすることによる、利用者におけるブルートフォース攻撃被害」の脅威をある程度緩和、許容できると考えております。（なお、仕様における“文字数 64 文字の受入れ”とは、少ない文字数までしか許容しないシステムによって、より強力なパスワードを登録したい利用者のパスワード登録における選択肢をわざわざ狭めないことを意図していると認識しています。）

（費用に関する補足）

③の追加提案は、××社製 ID 管理システムの基本機能の１つですので、追加費用はかかりません。機能の詳細等は、別紙×を参照ください。

別紙 4-2　重要事項説明書（サンプル）(3/3)

仕様書にある対策と同程度に脅威を削減できる代替案　説明書（No.2）

No	項目		代替案の概要	
	仕様書等の記載内容		代替案	説明書ページ
	仕様書等の名称	記載内容		
2	○○システムにおける Web アプリケーションセキュリティ特記仕様書	8.2. パッチ適用ポリシー	Web アプリケーションファイアウォール（WAF）を用いた防御（脅威の軽減）	P.○

代替案の詳細説明

（本件の背景）

当社で作成した××システムは、社内の検査部門により『別紙 X 社内出荷検査規定-セキュリティ検査概要』のとおりの検査の上、出荷することとしており万全を期す所存です。『別紙１脆弱性リスト』にある全ての脆弱性への対応は、当社がお示ししたセキュリティ実装方針のとおりです。

本件は、万一の場合の軽減策を『8.2. パッチ適用ポリシー』にある 2 週間以内の修補対応（パッチ適用）の代替案として提案するものです。

（代替案が必要な理由）

××システムの修補（パッチ開発）に時間がかかることがあります。これは××という理由からです。そのため、すぐに修補作業（パッチ適用）に取り掛かれない可能性があり、お示しいただいている 2 週間以内適用のポリシーを守れないことが懸念されます。

（代替案について）

社内の検査において脆弱性が発見されなかったものの、万一ですが、第三者による脆弱性診断等により、『別紙 1 脆弱性リスト』に記載の脆弱性が発見された場合において、WAF による防御が可能な場合は、修補（パッチ適用）ではなく、WAF による暫定処置で修補（パッチ適用）の代替ないし修補（パッチ開発及びその適用）までの時間確保手段として利用することを考えています。

なお、WAF の導入についてはシステム導入と同時に行い、貴市と協議の上、運用方針等を調整させていただきます。

（費用等詳細について）

導入予定の WAF の詳細説明及び導入後イメージ、導入、運用に必要な費用等に関しては、『別紙 Y WAF 導入に関して』をご参照ください。

以上

別紙 5 セキュリティ実装方針（サンプル）

○○システムにおけるセキュリティ実装方針について

標記システムに係るセキュリティ実装方針を以下に示します。以下は対策の概要及び当社における開発規約の抜粋です。

1. セキュリティ実装方針

1.1. SQL 呼び出し

（対策概要）

SQL 呼び出し時には、SQL インジェクション対策として以下を行う。

（開発規約抜粋）

必須：以下のすべてを実施すること 1-1-1. プレースホルダを用いて SQL を呼び出す 1-1-2. SQL の動的組み立てをしない 1-1-3. SQL 接続時に文字エンコーディングの指定を行う

1.2. CSRF 対策

（対策概要）

CSRF 対策として、POST メソッドのリクエストにはトークンの受け渡しと確認を行う。なお、本項はクリックジャッキング対策を兼ねる。

（開発規約抜粋）

必須：以下のすべてを実施すること 1-2-1. 秘密情報を入力する画面や、副作用のある画面は POST リクエストとする 1-2-2. POST リクエストのフォームにはトークンを hidden パラメータで埋め込む。トークンにはセッション ID の SHA-1 ハッシュ値を用いる 1-2-3.POST リクエストのフォーム画面では、HTTP レスポンスヘッダとして X-FRAME-OPTIONS: SAMEORIGIN を生成する（クリックジャッキング対策） 1-2-4. POST リクエストを受けるページでは処理に先立ちトークンの値を確認し、トークンが不正な場合はエラーとして直ちに処理を中止する

1.3. メールヘッダ・インジェクション対策

（対策概要）

本システムではメール送信機能を備えないため、本対応は不要です。

～以降各対策について同様に続く。省略～

以上により『別紙 1 脆弱性リスト』で示された脆弱性の対応を実施します。

別紙 6 実装状況報告書（サンプル）

○○システムにおける実装状況報告書

標記システムに係るセキュリティ実装方針に基づく実装状況を以下のとおり報告します。

実装状況 確認結果概要

未実施件数	1 件

1.1 SQL インジェクション対策

項番	開発規約	実施状況
1-1-1	プレースホルダを用いて SQL を呼び出す	○
1-1-2	SQL の動的組み立てをしない	○
1-1-3	SQL 接続時に文字エンコーディングの指定を行う	○

1.2 CSRF 対策

項番	開発規約	実施状況
1-2-1	秘密情報を入力する画面や、副作用のある画面は POST リクエストとする	○
1-2-2	POST リクエストのフォームにはトークンを hidden パラメータで埋め込む。トークンにはセッション ID の SHA-1 ハッシュ値を用いる	○
1-2-3	POST リクエストのフォーム画面では、HTTP レスポンスヘッダとして X-FRAME-OPTIONS: SAMEORIGIN を生成する（クリックジャッキング対策）	○
1-2-4	POST リクエストを受けるページでは処理に先立ちトークンの値を確認し、トークンが不正な場合はエラーとして直ちに処理を中止する	○

～省略～

次のとおり、「別紙 1 脆弱性リスト」に係る脆弱性対応状況を報告します。

「別紙 1 脆弱性リスト」への対応状況	全て対応済み ・ 一部非対応あり（いずれかに○）
非対応項目の具体的内容	最終テスト時の第三者企業による脆弱性検査で脆弱性が 1 件検出されました。○○機能において、X 脆弱性が残存しています。調査したところ、これは△△における××の実装漏れが原因でした。本件の改修には○日かかる見込みです。
回避策の有無	有 ・ 無 （いずれかに○）
2. 回避策の具体的内容	Web アプリケーションファイアウォールを利用して当面これを回避します。回避できることは既に検証済みです。検証結果については別途報告します。なお、□月△日のバージョンアップ時にこれを改修します。

別紙 7 契約書への追加条文例

地方公共団体における情報システムセキュリティ要求仕様・モデルプラン（Web アプリケーション）を採用した際、契約書に盛り込む条文例を以下に示します。

（脆弱性への対応）
第〇条
第◎条に定める検収の後、別紙脆弱性リスト記載事項についての脆弱性（以下、本条において単に「脆弱性」という。）が発見された場合、甲は乙に対して当該脆弱性の修正を請求することができる。ただし、乙がかかる修正責任を負うのは、特記仕様書に定めるセキュリティ保証期間中に甲から請求がなされた場合に限るものとする。

２　前項にかかわらず、脆弱性が軽微であって、その修正に過分の費用を要する場合、乙は前項所定の修正責任を負わないものとする。

別紙8 Webアプリケーションセキュリティ要求仕様等検討委員会 委員等一覧（五十音順）

＜委員＞

飯島　輝泰　埼玉県毛呂山町　子ども課子育て支援係（元情報推進室 係長）※第1回～3回まで
大高　利夫　藤沢市　総務部IT推進課　総務部参事（兼）IT推進課長
木村　修二　NPO関西情報化維新協議会 理事
佐藤　慶浩　日本ヒューレット・パッカード株式会社　個人情報保護対策室　室長
鈴木　正朝　新潟大学　大学院実務法務研究科・法学部　教授（情報法）
高木　浩光　独立行政法人 産業技術総合研究所　セキュアシステム研究部門　主任研究員
高倉　弘喜　名古屋大学　情報基盤センター　情報基盤ネットワーク研究部門　教授
鶴巻　暁　　上條・鶴巻法律事務所　弁護士
徳丸　浩　　HASHコンサルティング株式会社　代表取締役
中山　紀雄　総務省　自治行政局　地域情報政策室　電子自治体推進係　係長
丸山　満彦　デロイト トーマツ リスクサービス株式会社　取締役　執行役員

＜オブザーバー＞

芝原　努　　一般財団法人 関西情報センター　情報化推進グループ　課長
瀧川　将矢　財団法人 地方自治情報センター　主任研究員

＜委員会事務局＞

京セラコミュニケーションシステム株式会社（委員会事務委託先）
財団法人 地方自治情報センター　自治体セキュリティ支援室

地方公共団体における情報システム
セキュリティ要求仕様モデルプラン
（Web アプリケーション）

2012 年 10 月 22 日公開

［技術監修・委員］
独立行政法人 産業技術総合研究所　高木　浩光

［執筆協力・技術アドバイザー・委員］
HASH コンサルティング株式会社　　徳丸　浩

［執筆協力・委員会事務局］
京セラコミュニケーションシステム株式会社
間嶋　英之
小関　直樹
原田　隆正

［編集・委員会事務局］
財団法人 地方自治情報センター
自治体セキュリティ支援室（担当：百瀬、古家）
〒102-8419　東京都千代田区一番町 25 番
（全国町村議員会館内）
TEL. 03-5214-8040
Mail. lasc_info@lasdec.asp.lgwan.jp （LGWAN）
lasc@lasdec.or.jp（Internet）