システム導入に係るセキュリティ要件一覧表

No	大項目	中項目	内容
千代田区情報セキュリティポリシー【対策基準】第4.0版に遵守しているかの対策項目			
1	ID管理について	IDの共有禁止	①IDの共有の禁止 利用者1人につき1IDを作成して利用する運用とし、管理者と利用者は明確に分けて運用すること。 (システム的に1人１IDを付与出来ない場合は、ID利用帳簿を作成し、運用管理を行うこと。) ID共有禁止の理由：いつ、どこで、誰がログイン・ログアウトして、データをどうしたのか(更新・削除等)、 後からログで追跡出来るようにするため。
2		認証による個人を特定	②認証による個人を特定 個人を特定できるような認証の仕組みにすること。
3		IDの発行管理	③IDの発行管理 IDの発行/廃止、管理者ID/利用者IDを管理簿等で管理すること。 定期的に不要になったアカウントがないかの確認、不要となったアカウントを速やかに削除又は無効化等を行うこと。
4	パスワード設定管理について	パスワードの設定	①パスワードは英字(大文字、小文字)、数字、記号4種類から3種類以上を組み合わせて、 12桁以上の長さで設定すること。
5		パスワードの変更	②パスワードは定期的(90日に1回等)に変更すること。
6	アクセス権の管理について	アクセス権の設定について	①管理者と利用者で権限を分けて設定し、取り扱う情報や業務に応じてアクセスできる人を制御すること。 ●管理者権限(administrator、root)：システムの管理者。 システムの設定変更や全ての情報を閲覧・照会・編集・削除が可能。 ●一般ユーザー権限(標準ユーザー、一般ユーザー)：システムの設定変更が出来ない。 システムの変更が必要ない範囲で利用可能。
7		アクセス権の見直し	②人事異動、担当者の変更があった際には、速やかにアクセス権の見直しを行い、適切に管理すること。
8	ソフトウェア保守について	ソフトウェア保守契約の締結	①ソフトウェア保守契約を締結すること。 保守契約を締結しない場合は、事業を継続できる体制を整えること。 【例】 ・ソフトウェア保守契約を締結する。 ・保守契約を締結していないが、ソフトウェア(OSやアプリ)に障害が発生した場合、 事業者が対応していただける体制になっている。
9		脆弱性の対応	②脆弱性対応等の対策(OSや機器のファームウェア等のセキュリティパッチやアップデートの配布、適用)について、 仕組みや手順を整えること。
10		体制	③システム障害等が発生した場合に備えて、事業者と速やかに連携が出来るように 連絡体制図や連絡フロー図等の体制を整えること。
11	ハードウェア保守について	ハードウェアの保守契約の締結	①ハードウェア保守契約を締結すること。 保守契約を締結しない場合は、事業を継続できる体制を整えること。 【例】 ・ハードウェア保守契約を締結している。 ・ハードウェア保守契約を締結していないが、メーカー保証が1年付いており、 保証が切れた場合その都度、有償で修理対応する。その間予備機にて事業を継続する。 ・オンサイト保守5年パックに入っている。
12		体制	②ハードウェア故障等が発生した場合に備えて、事業者と速やかに連携が出来るように 連絡体制図や連絡フロー図等の体制を整えること。
13	【管理区域(マシン室等)のセキュリティ】 設置機器の管理・対策について	サーバの設置場所	【サーバ・ネットワーク機器を利用する場合】 ①サーバ・ネットワーク機器の設置場所について、区へ報告すること。 ※クラウドの場合はリージョンまで. ※政府情報システムの為のセキュリティ評価制度(ISMAP)に登録されたクラウドサービスを利用する場合は、 ISMAPクラウドサービスリストに登録されている「登録番号」と「クラウドサービスの名称」が必要
14		物理的セキュリティ対策	②設置場所のセキュリティ対策について、区へ報告すること。
15	端末の管理・対策について	物理的セキュリティ対策	①システムで利用する端末(デスクトップPC、ノートPC、モバイル端末)について、 セキュリティワイヤ等で机に固定、もしくは使用時以外は施錠可能なキャビネットで施錠管理を行うこと。
16			②端末の盗難、情報漏洩対策として、BIOSパスワード、ハードディスクパスワードを併用し設定すること。 対策されていない場合は、盗難防止の為、上記対策を行う必要がある。
17		外部記録媒体への書き出し制御	③セキュリティツールを用いて、端末から外部記録媒体へのデータ書き出しの制御を行うこと。
18		情報持ち出し時の暗号化	④外部記録媒体やメールにてデータの持ち出す(データ連携)場合は、データの暗号化を実施すること。
19	バックアップの取得管理について	バックアップの取得頻度	①サーバの冗長化とは別にシステムバックアップとデータバックアップを定期的に取得すること。 取得頻度と何世代保管しているかを区に報告すること。

20	バックアップの取得管理について	バックアップからの復旧体制	②取得したバックアップからシステムやデータの復旧ができる体制を整備すること。 また具体的な復旧手順書や復旧までの対応フロー図等を用意すること。
21		災害対策用のバックアップ(遠隔地)	③取得したバックアップにおいて、災害等によるデータの同時消失を防止する為、 サーバの設置場所(データの保管場所)とは別の場所に保管すること。
22	システム運用監視について	監視システム・サービスの導入	①ネットワークやサーバ等の状況がわかるような監視システムまたはサービスを導入すること。
23		障害発生の検知・通知	②システムに停止等の障害が発生した場合、障害を検知し管理者に通知されるような仕組みとすること。
24	ネットワーク分離/機器認証について	管理用端末等の機器認証	システムに接続する機器(端末)を限定もしくは認証して接続する仕組みとすること。
25	不正プログラム対策について	不正プログラム対策ソフトの導入	①端末、サーバ等に不正プログラム対策の為のソフトウェアを導入すること。
26		パターンファイルの更新	②不正プログラム対策のソフトウェア及びパターンファイルが常に最新の状態に保たれるようにすること。
27	ログの取得管理について	ログの取得	①「いつ、どこで、だれが、何を、どうしたのか」をログ取得すること。 システムの利用状況の把握や障害調査等、情報セキュリティ確保に必要なログ(操作、認証、イベント等)を取得すること。
28		ログの点検・分析する体制	②取得したログ情報の調査、確認が行える体制を組むこと。
29		ログの保存期間	③取得した各種ログについて2年以上保存すること。
30	インターネットアクセスの制限について	ネットワーク機器の設定・ソフトの導入	インターネットへの無制限なアクセスを防止するため、URLフィルタリング等により適切にアクセスの制限を実施すること。
千代田区Webサイト構築【対策基準】第2.1版に遵守しているのかの確認事項 構築事業者様確認用			
31	サーバ基本設定	不要なサービスの停止	Webサイトの運営に必要のないサービスを停止すること
32		外部公開が不要なポートの遮断	外部に公開する必要のないポートは遮断すること
33		システム情報の非表示	サーバが外部に出力する情報に、利用しているOSやミドルウェアのバージョン等の情報が外部に出力されないように隠蔽すること。
34		公開不要なファイルの確認	① 公開を想定していないファイルを公開用のディレクトリに保管しないこと。 ② ディレクトリ構造が画面表示されないようにすること。
35		管理用インタフェースの制限	運用保守のための管理用画面等のインタフェースは原則としてインターネットに公開しないこと。 やむを得ず公開する場合は、アクセス元IPアドレスによるフィルタリング等のアクセス制限を行うこと。また、通信内容の暗号化を行うこと。
36	認証	認証の実施	特定のユーザのみに表示・実行を許可すべき画面や機能には、認証を必要とすること。 管理者用画面には認証を必要とすること。
37		不要アカウントの削除	運用開始前に、検証用アカウント等不要なアカウントを削除すること。
38		パスワード規則	①パスワード文字列は少なくとも大小英字と数字の両方を含み、最低8文字以上であること。 ②画面にパスワード文字列を表示しないこと。
39		認証時におけるメッセージ	認証画面において、ユーザIDとパスワードのどちらが間違っているか推測できるようなメッセージを表示しないこと。 （例：「パスワードが間違っています」というメッセージにはせず、「ユーザIDもしくはパスワードが違います」というようなメッセージにすること。）
40		パスワードの保存	パスワードをサーバ内で保管する際は、平文ではなくソルト付きハッシュ値の形で保管すること。
41		アカウントロック 【機密性または完全性の重要度が「高」の場合】	認証時に無効なパスワードで一定回数の試行があった場合、一定時間はアカウントがロックアウトされた状態にすること。 対策例 10回認証に失敗した場合、30分間アカウントがロックアウトされた状態になる。
42	セッション管理	セッションIDの生成	① 自前でセッション管理の仕組みを構築せずに、ミドルウェアやフレームワーク等が提供するセッション管理の仕組みを利用すること。 ② セッションIDを推測が困難なものにすること。
43		セッションIDの扱い	セッションIDをURLパラメータに格納せずに、Cookieに格納するか、POSTメソッドのhiddenパラメータに格納して受渡しをすること。
44		Cookieの設定	HTTPS通信で利用するCookieにはsecure属性を設定すること。
45		CSRF（クロスサイト・リクエスト・フォージェリ）	登録・変更・削除等の処理が実行される箇所において、CSRFの脆弱性への対策を施すこと。 対策例） ・処理を実行するページをPOSTメソッドでアクセスするようにし、その「hiddenパラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。 ・処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。 ・Refererが正しいリンク元かを確認し、正しい場合のみ処理を実行する。
46		セッションIDの破棄	① 認証済みのセッションが一定時間（例：60分）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、サーバ側でセッションを破棄しログアウトすること。 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側でセッションを破棄すること。

47	セキュリティ実装	SQLインジェクション	① SQLインジェクションの脆弱性への対策を施すこと。 ② ミドルウェアやフレームワークが出力するSQL文等を含むエラーメッセージをそのままブラウザに表示しないこと。
48		OSコマンド・インジェクション	OSコマンド・インジェクションの脆弱性への対策を施すこと。 対策例） ・シェルを起動できる言語機能の利用を避ける。 ・シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。
49		パス名パラメータの未チェック/ディレクトリ・トラバーサル	① ディレクトリ・トラバーサルの脆弱性への対策を施すこと。 ② 原則として、外部からのパラメータにファイル名を直接指定しないようにし、ファイル名を指定する必要がある場合には想定外のファイル名であるかどうかのチェックを行うこと。
50		クロスサイト・スクリプティング	クロスサイト・スクリプティングの脆弱性への対策を施すこと。 対策例） ・ウェブページに出力する全ての要素に対して、エスケープ処理を施す。 ・URLを出力するときは、「http://」や「https://」で始まるURLのみを許可する。 ・<script>…</script>要素の内容を動的に生成しない。 ・スタイルシートを任意のサイトから取り込めるようにしない。 ・入力されたHTMLテキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。
51		HTTPヘッダ・インジェクション	HTTPヘッダ・インジェクションの脆弱性への対策を施すこと。 対策例） ・ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用APIを使用する。 ・改行コードを適切に処理するヘッダ出力用APIを利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。
52		メールヘッダ・インジェクション	メール送信処理が行われる箇所において、メールヘッダ・インジェクションの脆弱性への対策を施すこと。 対策例） ・メールヘッダを固定値にして、外部からの入力はすべてメール本文に出力する。 ・メールヘッダを固定値にできない場合、ウェブアプリケーションの実行環境や言語に用意されているメール送信用APIを使用する。 ・HTMLで宛先を指定しない。
53		クリックジャッキング	クリックジャッキングの脆弱性への対策として、HTTPレスポンスヘッダにX-Frame-Optionsヘッダを出力すること。
54		その他	① URLパラメータにユーザIDやパスワード等の情報を格納しないこと。 ② 入力値の文字種や文字列長の検証を行うこと。 ③ ミドルウェアやフレームワークが出力する詳細なエラー内容をブラウザに表示しないこと。 ④ 重要な処理（例：認証の失敗、アカウント情報の変更）が行われた際にログを記録すること。
55	通信の暗号化	HTTPSの使用	Webサイトの全てのページにおいて、HTTPSを使用すること。
56		SSLサーバ証明書	SSLサーバ証明書はWebサイトへのアクセス時に警告（発行者、発行先、有効期間等の不備によるもの）が出ないものを使用すること。
57		SSL/TLSのバージョン	TLS1.2以上を使用し、SSL2.0／3.0、TLS1.1を無効にすること。
58	その他 【機密性、完全性または可用性の重要度が「高」の場合】	マルウェア対策	外部からコマンド実行やファイル転送が可能なプロトコル（例：HTTP、HTTPS、FTP、SSH等）を使用しているサーバについて、マルウェア対策ソフトを導入すること。 導入後は、定期的（例：1日1回）にマルウェア定義ファイルを更新すること。
59		不正アクセス検知・防御	サーバへの不正アクセスを検知するため、IPS/IDSを導入すること。導入後は、攻撃パターン情報（シグネチャ）を適宜更新（フォールスポジティブが発生した際のシグネチャの見直し、最新のシグネチャの適用等）すること。
60		WAF	重大な脆弱性への暫定対処を可能とするために、WAFを導入すること。
61		重要情報の暗号化	重要な情報（個人情報等）をサーバ等に保存する場合には、情報の重要度に応じて暗号化を実施すること。
62	運用構成管理	使用しているOS、ソフトウェアの	脆弱性への対応を迅速に行うことができるよう、サーバで使用しているOSやソフトウェアの情報を管理すること。使用しているOSやソフトウェアのサポート期限を把握し、サポートが終了する前にアップデートできるよう計画をたてること。
63		脆弱性情報の取得	使用しているOSやソフトウェアの開発元等から提供される脆弱性情報や、JPCERT/CCやIPA等から提供される注意喚起情報を継続的に入手し、ソフトウェアの更新や問題の回避を検討すること。
64	管理用アカウントの管理	アカウント共用の禁止	管理者用アカウントは複数人で共有せずに、個人毎に割り当てること。なお、やむを得ず複数人で共用する場合には、当該アカウントを使用した者が特定できるように運用すること アカウント共有禁止の理由：「いつ、どこで、誰がログイン・ログアウトして、データをどうしたのか(更新・削除等)、後からログで追跡出来るようにする為です。」 （例：対象サーバにアクセスするための端末のアカウントを個人毎に割り当てる等）。
65		不要アカウントの定期的な確認	管理者アカウントのうち、不要となったアカウントは速やかに削除又は無効化すること。また、定期的に不要となったアカウントがないか確認すること。
66	ログの監視	取得すべきログの明確化と収集	①サーバ・ネットワーク監視及びセキュリティの確保に必要なログを収集すること ②ログ調査、確認が行えるように2年以上保存すること。 ※②については、千代田区情報セキュリティポリシー【対策基準】から抜粋。 対策例 システムの操作ログ、認証ログ、イベントログを取得し2年以上、保管している。
67		認証ログの確認	認証があるWebサイトについて、パスワードリスト攻撃等を検知するため、認証ログ（認証エラー発生件数の急激な増加、特定IPアドレスからの大量アクセス等）を定期的に確認すること。監視システムのアラームによる確認でも可とする。

68	対策状況の報告	-	セキュリティの対策状況について、以下のタイミングにて区へ報告すること。 (1) 新規構築時 ・本稼動前に実施した脆弱性診断の結果および対策結果 (2) 運用時 以下の事項について最低年1回、及び区からの求めがあった場合に報告すること。 ・使用しているOS、ソフトウェアの一覧およびバージョン（最新バージョンでない場合には、その旨および最新バージョンを使用していない理由を報告すること。） ・管理用アカウントについて、No66,No67「管理用アカウントの管理」の項目を確認した結果 ・監視しているログの確認結果
69	ドメインの管理について	ドメインの取得	ドメインを取得する場合は、そのドメインの管理方法を明確にすること
70		ドメイン変更の必要性の検討	ドメインの変更については、利用を停止するドメインが悪用される危険性が高いことから、必要性について慎重に検討を行うこと。（ドメイン変更の必要がない場合、変更を行わないこと。）
71		ドメインの利用停止、変更につ	一度作成したWebサイトのドメインについては、極力変更しないこと。 ・万が一、Webサイトのドメインの変更や利用停止を行う場合、使用しなくなるドメインについては、二次利用もしくは不正に取得される恐れがあるため、契約を続けて保管すること。 ・ドメインの利用停止を行う場合は、ドメインを利用停止する旨を関連する案内ページを用いて案内を行うこと。※1 ・ドメインの変更を行う場合は、新ドメインへのサービス移行を行った上で、新ドメインの案内ページの表示を行うこと。※1 また、旧ドメイン運用停止後一定期間は、検索エンジン、お気に入り等から旧ドメインへのアクセスを考慮して対策を講じること。 ※1.提示内容例 ・現行ドメインの運用停止期間 ・現行ドメインの運用停止後は当該ドメインからの情報提供は行わない ・運用停止するドメインで提供している情報の新ドメインでの掲示先 ・運用停止するドメインをなりすまし防止の為一定期間所有を行う旨の記載
72	外部サービスの利用	事業者の信頼性	サービスを提供する事業者は信頼できる事業者であること。 ・日本国内の事業者によるサービスであること。 ・日本の法律が適用できること。 ・個人情報の取扱いに関する規定があること。 ・守秘義務に関する規定があること。 ・情報セキュリティに関する基本方針・規定等が整備されていること。 ・事業継続に関する基本方針・規定等が整備されていること。
73		サービスの信頼性	サービスの稼働率などのサービスレベルが示されていること。 ・サービスの稼働率の目標値が規定されていること。 ・プライバシーマーク（JIS Q 15001）等、ISMS（JIS Q 27001）等の認証を取得していること。 ・サービスが停止しない仕組み（冗長化、負荷分散等）を設けていること。 ・SLAが契約書に添付されていること。 ・日本国内にデータセンターがあること。
74		セキュリティ対策	サービスにおけるセキュリティ対策が具体的に公開されていること。 ・死活監視を実施していること。 ・マルウェア対策を実施していること。 ・セキュリティパッチ管理が一定の間隔で実施されること。 ・データの暗号化措置への対応があること。 ・ファイアウォール等の不正アクセスを防止する措置があること。 ・不正なサーバ侵入に対する検知等の仕組みがあること。 ・ネットワークの暗号化措置への対応があること。
75		管理用インタフェースのセキュリ	管理者用インタフェースに対する認証やアクセス制限が適切にされていること。 ・IPアドレスによるアクセス制限、ワンタイムパスワード等
76		基盤環境のセキュリティ対策	サービス側に基盤環境の管理責任がある場合に、必要なポート、サービスのみを有効とする等の対応が可能であること。また、使用しているOS、ミドルウェアの設定変更やバージョンアップが可能であること。
77		サポート	サービスの利用や設定等について問い合わせを受け付ける窓口が用意されていること。
78	評価	脆弱性診断	Webサイトの新規構築時には、本稼動前に脆弱性診断を実施し、その結果に基づいて対策を実施すること。
情報資産の廃棄			
79	データ消去	機密性に応じた機器の廃棄等	情報資産を保存した電子記録媒体は「情報を復元できないように処置（物理的破壊）した上で廃棄（破砕・溶解・破壊・圧縮等）」し廃棄証明書の提出を受けなければならない。ただしクラウドサービスが第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を確認し判断する。 廃棄証明書には以下の内容を含むものとする。 ・ データ消去を行ったパソコン及び記録媒体の情報 ・ 消去作業の情報として、消去実行事業者名、処置前の電磁的記録媒体の写真、実施日時、処置方法、処置後の電磁的記録媒体の写真、媒体領域/区画に関する情報を含む処置作業の結果、及び残留するリスク等の特記事項等