セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策					推奨レベル				本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
1	情報を他人から守る（機密性保護）	認証	パスワードを利用する	パスワードが推測可能な容易な物になっていると、第三者がシステムに不正アクセスし、情報を漏えいしてしまうおそれがある。	・パスワードを利用しない。	・初期パスワードをすみやかに変更する。 ・定期的（六ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上）を設定する。 ・パスワードは、管理者を含め誰にも教えない。 ・パスワードを書き留めたり、コンピュータ上のファイルに保管したり、メールで送信したりしない。やむを得ず紙片等にパスワードを記載する必要がある場合には、そのパスワードが容易に第三者に見られることがないように保管する。 ・自分のパスワードが他人に漏えいした可能性や疑いがある場合は、パスワードを変更する。	・定期的（三ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上、パスワード世代管理、三種類以上の文字種の使用）を設定する。	・同一利用者が複数のアカウントをもつ場合は、それぞれ異なるパスワードを設定する。また、一つのパスワードから他方が推測しやすいパスワードを設定しない。 ・機密性が高い部署では、生体認証を使用する。			A.11.3.1	・政府機関統一基準適用個別マニュアル群 庁舎内におけるPC利用手順 PCの取扱編 端末利用者パート 2.3 識別コードの日常の取扱い(2), (3)
2			ネットワーク上の機器を識別する	不正な情報機器がネットワークに接続されると、情報が漏えいするおそれがある。	・未登録や不正なコンピュータの接続を検出できない。	・未登録や不正なコンピュータの社内ネットワークへの接続を、検出して警報をあげる。 ・接続コンピュータのログを取得する。	・未登録や不正なコンピュータの社内ネットワークへの接続を、検出し、警告して、接続を防止する。 ・接続コンピュータのログを取得する。	・未登録や不正なコンピュータの社内ネットワークへの接続を検出・警告し、接続を防止する。 ・正常な未登録のコンピュータを、自動的に登録する。			A.11.4.3	
3			利用者が本人であることを証明し承認する	利用者の身分が証明できないと、権限がない利用者が情報を不正に取得して社外へ漏えいさせるおそれがある。	・一台のコンピュータを一つのアカウントで、複数の利用者が使用する。 ・認証ログは取得しない。	・Windowsのアカウント、パスワードを利用して、利用者を識別する。 ・一台のコンピュータを複数の利用者では使用させない。 ・認証ログを取得する。	・一台のコンピュータに対して、一人しか使用させない。 ・特定のカードやログインの二重化などで、本人認証を実施する。 ・認証ログを取得する。	・生体認証（静脈・指紋認証など）を利用して、利用者の本人認証を実施する。 ・二要素認証を実施し、認証強度を上げる。 ・認証ログを取得する。			A.11.5.2	
4			業務ソフトウェアや機器認証で使うパスワードを管理する	パスワードの管理がされていないと、不正な活動や情報漏えいが確認できないおそれがある。	・パスワードを管理しない。	・認証機能を使用して、コンピュータを利用する。	・認証機能を使用して、コンピュータと業務ソフトウェアを利用する。	・生体認証を利用してパスワードを使わない。			A.11.5.3	・政府機関の情報セキュリティ対策のための統一基準（第2版） 4.1.1 主体認証機能(1)
5			業務ソフトウェアの起動時間を監視する	業務ソフトウェアが終了されずに放置されていると、情報が盗まれるおそれがある。	・業務ソフトウェアの未使用時間を監視しない。	・業務ソフトウェアの未使用時間を監視する。 ・一定時間以上利用されないセッションを監視する。	・業務ソフトウェアの未使用時間を監視し、警告する。	・業務ソフトウェアの未使用時間を監視し、警告して、遮断する。			A.11.5.5	
6			情報へのアクセスを管理する	誰もが情報を閲覧できるようになっていると、情報の改ざんや漏えいのおそれがある。	・サーバ上の情報に誰でもアクセスできる。 ・情報を機密レベルに分類しない。 ・情報にアクセスした履歴を取得しない。	・サーバ上の情報にアクセス権をつけて、権限のない利用者は使用できないようにする。 ・情報にアクセスした履歴を取得しない。	・情報を重要度別（（秘）（社外秘）（関係者外秘）など）に分類して、重要度別に利用者やグループ単位でアクセス権をつけて管理する。 ・情報にアクセスした履歴を取得する。 ・印刷物を減らすことにより、管理する対象を減らし、情報漏えいのリスクを減らす。 ・印刷物に対して、誰がいつ印刷したものか、わかるように「すかし」などを挿入する。	・アクセスの履歴を定期的に監査して、情報の持ち出しに問題があれば是正する。			A.11.6.1	
7		暗号化	コンピュータや電子媒体を暗号化する	情報機器が盗難又は紛失されると、情報が漏えいするおそれがある。	・データを暗号化しない。	・社外に持ち出すコンピュータ、電子媒体（USBメモリ、外付けHDD、CD/DVDなど）の中のデータを暗号化する。	・社内のコンピュータ、社外に持ち出すコンピュータ、電子媒体（USBメモリ、外付けHDD、CD/DVDなど）に対して暗号化をする。	・社内のコンピュータ、社外に持ち出すコンピュータ、電子媒体（USBメモリ、外付けHDD、CD/DVDなど）に対して暗号化をする。 ・復号時には認証が毎回必要となる。			A.12.3.1	
8			ネットワークを流れる情報を暗号化する	ネットワーク上のデータが盗聴されると、情報が漏えいするおそれがある。	・社外に送るデータは平文で送信する。 ・Webの通信は暗号化（SSL通信）しない。	・Webの通信を暗号化（SSL通信など）する。	・社外に出る情報を、事前に社内で暗号化して送信する。 ・Webの通信を暗号化（SSL通信など）する。	・コンピュータから発信する情報(メールの添付データなど）を、社内、社外にかかわらず、すべて事前に暗号化して送信する。 ・Webの通信を暗号化（SSL通信など）する。			A.12.3.1	
9			暗号鍵の強度を上げる	暗号の複雑さが低いと、簡単に復号化されて情報が漏えいするおそれがある。	・暗号化しない。	・公に認知されているアルゴリズムで暗号化する。 ・鍵長が64ビット以上の暗号化を使用する（AES 64ビット以上など）。	・公に認知されているアルゴリズムで暗号化する。 ・鍵長が128ビット以上の暗号化を使用する（AES 128ビット以上など）。	---> 前レベルと同様				
10			暗号鍵を管理する	暗号鍵が外部に流出すると、暗号化したデータを復号されて、情報が漏えいするおそれがある。	・暗号化しない。	・暗号鍵を、平文（通常の文字列）のままソフトウェア上で管理する。	・暗号鍵を、暗号化してソフトウェア上で管理する。 ・サーバ上で、暗号鍵の保管場所を誰にでもわかるようにする。	・暗号鍵を暗号化して、独自のパスワード等で保護する。 ・暗号鍵の所在については、システム的に管理者以外は閲覧できなくする。			A.12.3.2	
11		侵入検出（IDS/IPS）	社外ネットワークからの攻撃や不正侵入を防御する	サーバやネットワーク機器に対する侵入行為や攻撃を受けると、データが改ざんされたり、情報が漏えいしたり、システムが停止したりするおそれがある。	・不正アクセスは考慮しない。	・外部からの不正アクセスを検討・考慮する。 ・外部からの攻撃を検出・防御する仕組み（IDSなど）を導入する。	・外部からの不正アクセスを検討・考慮する。 ・外部からの攻撃を検出・防御する仕組み（IDSなど）を導入する。 ・外部からのアクセスログを取得して、定期的にレポートする。	・外部からの不正アクセスを検討・考慮する。 ・外部からの攻撃を検出・防御する仕組み（IDSなど）を導入する。 ・不正アクセス検出した場合、自動的に遮断する仕組みを導入する。 ・外部からのアクセスログを取得して、定期的にレポートする。			A.10.4.1	
12		ウイルス対策	悪意あるプログラムを検出する	コンピュータに誤動作を起こさせる悪意あるプログラム（ウイルスやスパイウェア等）により、システムが利用できなくなる、データが消去される、情報が外部に漏えいしてしまう、などのおそれがある。	・ウイルス対策を実施しない。	・悪意あるプログラム（ウイルス・スパイウェア）が、コンピュータ上のデータに付着していないか、検出する機能を導入する。 ・社内の全コンピュータのウイルス対策状況を把握する仕組みを導入する。 ・悪意あるプログラムを検出した場合、システム管理者に通報する。	・悪意あるプログラム（ウイルス・スパイウェア）が、コンピュータ上のデータに付着していないか、検出して駆除する。 ・システムの変更された部分を自動的に修復できる機能を導入する。 ・社内の全コンピュータのウイルス対策状況を把握する仕組みを導入する。 ・悪意あるプログラムを検出・駆除及びシステムを修復した場合、システム管理者に通報する。	・悪意あるプログラム（ウイルス・スパイウェア）が、コンピュータ上のデータに付着していないか、検出して駆除する。 ・システムの変更された部分を自動的に修復できる機能を導入する。 ・悪意あるプログラムによるネットワーク通信を自動的に遮断する。 ・社内の全コンピュータのウイルス対策状況を把握する仕組みを導入する。 ・悪意あるプログラムを検出・駆除及びシステムを修復した場合、システム管理者に通報する。			A.10.4.1	
13			メールに添付した悪意あるプログラムを検出する	コンピュータに誤動作を起こさせる悪意あるプログラム（ウイルスやスパイウェア等）がメールから侵入すると、システムが利用できなくなる、データが消去される、情報が外部に漏えいしてしまう、などのおそれがある。	・メールのウイルス対策を実施しない。	・悪意あるプログラム（ウイルス）が、メールに添付していないか、検出する。 ・ウイルスを検出した場合、システム管理者に通報する。	・悪意あるプログラム（ウイルス・スパイウェア）が、メールに添付していないか、検出する。 ・メールに添付している悪意あるプログラムを駆除する。 ・ウイルスの可能性があるものを検出する。 ・ウイルスを検出した場合、システム管理者に通報する。	・悪意あるプログラム（ウイルス・スパイウェア）が、メールに添付していないか、検出する。 ・メールに添付している悪意あるプログラムを駆除する。 ・ウイルスの可能性があるものを検出する。 ・ウイルスを検出した場合、システム管理者に通報する。			A.10.4.1	
14			迷惑メールを遮断する	迷惑メールが侵入すると、トラフィック増加、システム負荷の増加、悪意あるプログラムの侵入、悪意あるWebサイトへの転送、などのおそれがある。	・迷惑メールを対策しない。	・迷惑メールの判別をおこない、印をつける。	・迷惑メールの判別をおこない、隔離領域に振り分ける。	・迷惑メールの判別をおこない、悪質な送信元からの受信を拒否する。			A.10.4.1	
15			不要なWebサイト閲覧を管理する	業務に不必要なWebサイト閲覧を許可していると、業務効率の悪化、トラフィック増加、悪意あるプログラムの侵入、外部への情報漏えい、などのおそれがある。	・Webサイトの閲覧に制限をかけない。	・指定されたURLをブロックする。	・指定されたURLをブロックする。 ・提供されるデータベースを使用して、カテゴリ単位でWebサイトをブロックする。	・指定されたURLをブロックする。 ・提供されるデータベースを使用して、カテゴリ単位でWebサイトをブロックする。 ・信頼度の低いWebサイト、危険度が高いWebサイトを、設定したセキュリティレベルでブロックする。			A.10.4.1	・政府機関の情報セキュリティ対策のための統一基準（第2版） 4.2.1 セキュリティホール対策(2), 4.2.2 不正プログラム対策(1)(2)
16			全社のセキュリティ対策製品を集中的に運用管理する	社内のセキュリティ対策製品が管理できていないと、緊急時対応の遅れ、ポリシー漏れ、管理状況の把握が困難、などのおそれがある。	・各製品を個別に運用する。	・利用者のコンピュータに導入されたウイルス対策製品を集中的に管理運用する。 - アップデート状況 - ウイルス検出状況	・社内のすべてのセキュリティ対策製品を集中的に管理運用する。 - アップデート状況 - ウイルス検出状況	・社内のすべてのセキュリティ対策製品を集中的に管理運用する。 - アップデート状況 - ウイルス検出状況 - 自動的なレポート生成機能			A.10.4.1	

セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策					推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
17			Webサイト閲覧時に悪意あるプログラムを検出する	Webサイトから悪意あるプログラムが侵入すると、システムが利用できなくなる、データが消去される、情報が漏えいしてしまう、などのおそれがある。	・Webサイトからの悪意あるプログラムを検出しない。	・Webサイトからのウイルスを検出、自動処理する。 ・処理内容を管理者等に報告する。	・Webサイトからのウイルスを検出、自動処理する。 ・Webサイトからのスパイウェアを検出、自動処理する。 ・処理内容を管理者等に報告する。 ・パターンファイルに対応していない悪意あるプログラムを検出するための機能を導入する。	・Webサイトからのウイルスを検出、自動処理する。 ・Webサイトからのスパイウェアを検出、自動処理する。 ・処理内容を管理者等に報告する。 ・パターンファイルに対応していない悪意あるプログラムを検出するための機能を導入する。 ・利用者グループ毎に異なるポリシー設定する。			A.10.4.1	
18			ブラウザ上で動作する悪意あるプログラムを検出する	ブラウザ上で自動実行されるプログラム（ActiveXスクリプト、Javaアプレット等）が不正に実行されると、ウイルスに感染してしまう、情報が外部に漏えいする、などのおそれがある。	・ブラウザ上ではすべてのプログラムを実行する。	・署名済みのプラグインもしくは管理者の承認済みのスクリプトのみを実行する。	・未署名なActiveXや有効ではないJAVAアプレットの動作を制限する。	・未署名なActiveXや有効ではないJAVAアプレットの動作を制限する。 ・利用者グループ毎に異なるポリシー設定する。			A.10.4.2	
19		ファイアウォール	ネットワークサービスの利用を管理する	ネットワークへのアクセスを適切に制御しないと、社内外から不正なアクセスが発生し情報が漏えいするおそれがある。	・ネットワークサービス利用に関する方針を策定しない。	・ネットワークサービス利用に関する方針を策定する。 ・社外からの通信を遮断する。	・ネットワークサービス利用に関する方針を策定する。 ・社外からの通信は必要なもののみ許可する。 ・社外への通信は必要なもののみに制限する。 ・ネットワークサービス利用に対するログを監視し、必要に応じて警告する。	・ネットワークサービス利用に関する方針を策定する。 ・社外からの通信は必要なもののみ許可する。 ・社外への通信は必要なもののみに制限する。 ・ネットワークサービス利用に対するログを監視し、必要に応じて警告する。 ・必要に応じて、通信を自動的に遮断する。			A.11.4.1	
20			ネットワーク上の装置を識別する	ネットワークを通過・拒否される装置が適切に識別できないと、不正アクセスなどの発生時に対応が長期化するおそれがある。	・各システムに適切なホスト名などを設定しない。 ・DNSやLDAPによりホスト名などを確認できる設定をしない。	・各システムに適切なホスト名などを設定する。 ・DNSやLDAPなどによりホスト名などを容易に確認できる。 ・装置の接続状況をログに残す。	・装置管理のための情報を一箇所に統合する。 ・装置の追加・削除を適切に管理する。 ・装置の接続状況を定期的にレポートする。	・装置の認識がシステムで自動化し管理する。 ・不正な装置接続を自動的に遮断する。			A.11.4.3	
21			遠隔診断用及び環境設定用ポートを保護する	診断・管理用ポートへ不正アクセスを受けると、システムが不正に変更されたり情報が漏えいしたりするおそれがある。	・診断、管理用ポートへ誰でもアクセスできる。	・診断、管理用ポートに適切なアクセス権を設定する。	・診断、管理用ポートに適切なアクセス権を設定する。 ・管理用ネットワークは通常のネットワークとは別に用意し、一般利用者からは物理的・論理的にアクセス不可能にする。	・診断、管理用ポートに適切なアクセス権を設定する。 ・管理用ネットワークは通常のネットワークとは別に用意し、一般利用者からは物理的、論理的にアクセス不可能にする。 ・管理用ネットワークへのアクセスログを監視し、不正なアクセスを警告する。			A.11.4.4	
22			ネットワーク領域を分割する	ネットワークを適切に分割しないと、不正にアクセスされるおそれがある。	・社内ネットワークに社外からアクセスできる。	・社内ネットワークへは社外からのアクセスを禁止する。	・社内ネットワークの一部資源のみ、社外からのアクセスを許可する。	・社外に公開されたネットワーク（DMZ）と社外からはアクセスできない社内ネットワークを完全に分離する。			A.11.4.5	
23			ネットワーク接続を制御する	ネットワークへの接続制御を実施しないと、不正アクセスや情報漏えいが発生するおそれがある。	・誰でもネットワークが自由に使用できる。	・端末毎に接続制限をかける。	・利用者毎にネットワーク使用をコントロールする。 ・アクセス違反に対する適切なモニタリングを実施して、異常時には自動的に警告する。	・利用者毎にネットワーク使用をコントロールする。 ・アクセス違反に対する適切なモニタリングを実施して、異常時には自動的に警告する。 ・不正なネットワーク使用を強制的に切断する。			A.11.4.6	
24			ネットワークルーティングを制御する	内部、外部からの不正なルーティング情報が流入すると、既存のネットワーク情報が不正に変更されたり、情報システムが利用できなくなったりするおそれがある。	・対策しない。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・静的ルーティングなど、固定的なルーティングを制御する。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・管理下以外のネットワーク機器に対して、ルーティング情報のフィルタを実施する。	・ルーティング情報更新に認証情報(パスワードなど)を追加する。			A.11.4.7	
25		VPN装置	ネットワークサービスの利用を管理する	ネットワークの利用が適切に定義されていないと、不正アクセスが行われたり、情報漏えいしたりするおそれがある。	・適切なネットワークサービス利用に関する方針を策定しない。	・外部からのネットワークサービス利用に関する方針を策定する。	・外部からのネットワークサービス利用に関する方針を策定する。 ・利用者に対して定期的に周知、徹底する。	・外部からのネットワークサービス利用に関する方針を策定する。 ・利用者に対して定期的に周知、徹底する。 ・定期的な内部監査を行い、方針の運用状況を確認			A.11.4.1	
26			外部から接続する利用者を認証する	外部利用者を正しく認証できないと、外部からの不正アクセスで、情報漏えいしたり情報システムが停止したりするおそれがある。	・認証なしに誰でもアクセスできる。	・ユーザ名、パスワードによる利用者の認証をする。	・パスワードの複雑化や定期的な強制変更を実施する。 ・定期的なレポートを作成する。	・ワンタイムパスワードや生体認証など、より高度な利用者の認証を併用する。			A.11.4.2	
27			ネットワーク上の装置を識別する	ネットワークを通過・拒否される装置を適切に識別できないと、不正アクセスなどの発生時に対応が長期化するおそれがある。	・すべての装置がネットワークに接続できる。	・ネットワークにアクセスする装置種別(機種名、OS種別、バージョンなど)を判定する機器を導入する。	・ネットワークにアクセスする装置種別(機種名、OSバージョンなど)を判定する機器を導入する。 ・事前に設定した方針に従ってアクセス可否を自動的に制御する。	---> 前レベルと同様			A.11.4.3	
28			通信を暗号化する	通信を暗号化していないと、不正アクセスが行われたり、情報漏えいしたりするおそれがある。	・通信を暗号化しない。	・外部への通信を暗号化する。	---> 前レベルと同様	・より強力な暗号化方式（AES 128ビット以上など）を利用する。			A.11.7.1	
29			在宅勤務で使用するコンピュータを管理する	会社で許可していないコンピュータが在宅勤務で利用されると、情報が漏えいするおそれがある。	・個人所有コンピュータを使用する。	・会社支給のコンピュータで作業する。 ・すべてのデータがサーバ上にあり、コンピュータには一時保管するが、コンピュータにはデータが保存できなくする。 ・ファイルのアクセスログを取得する。	・会社支給のコンピュータで作業をする。 ・すべてのデータがサーバ上にあり、コンピュータには一時保管するが、コンピュータにはデータが保存できなくする。 ・一時保管したデータは、一定時間で自動的に消去する。	・会社支給のコンピュータで作業をする。 ・すべてのデータがサーバ上にあり、コンピュータには保管できない仕組みにする。 ・ファイルのアクセスログを取得する。 ・コンピュータ間の通信データを暗号化する。			A.11.7.2	
30		オペレーティングシステム（OS）	オペレーティングシステム（OS）の利用者を管理する	認可されない利用者がOSを利用できると、権限以上の操作ができることによる情報漏えいのおそれがある。	・利用者によるアクセス権限の変更をしない	・利用者を識別し、利用者毎にアクセス制御可能な機能、およびファイルシステムを区別する。	・利用者毎の情報システムへのアクセスを統合管理する。	・アクセスログを取得して、範囲外のアクセスについては自動的に警告する。			A.11.5	
31			利用者の成りすましを防ぐ	利用者のログオン情報が悪用されると、成りすましにより第三者がログオンしたり、情報漏えいしたりするおそれがある。	・対策しない。	・Secure Attention Sequence (SAS) などの、認証画面を不正なソフトウェアで模倣されない機能を導入する。 ・パスワードなどの認証情報を暗号化して、複合化できない状態で保存する。 ・パスワードの有効期間が切れた場合、アカウントを無効化する。	・過去にログオンしたユーザ名などのログオンに必要な情報の一部または全てを表示しない。 ・一定回数以上のログオン失敗に対して、一定時間のログオンを禁止する(失敗のしきい値：50回、ロックアウト期間：15分) ・辞書攻撃を防ぐために、一定時間内に連続したログオンを制限する。 ・ログオン時間(利用可能時間帯)を経過した場合は利用者を強制的にログオフする。 ・ログオン時間(利用可能時間帯)の有効期間が切れた場合はコンピュータを切断する。	・一定回数以上のログオン失敗が発生した場合に、管理者に通知する。 ・一定回数以上のログオン失敗に対して、一定時間のログオンを禁止する。(失敗のしきい値：15回、ロックアウト期間：15分)			A11.5.1	
32			オペレーティングシステム変更時に業務ソフトウェアの動作を検証する	オペレーティングシステム変更時に業務ソフトウェアを十分に検証しないと、不具合の発生、新たなぜい弱性の発生、問題の長期化、などのおそれがある。	・検証しない。	・オペレーティングシステムに変更があった場合、都度変更を記録する。	・年間サポート計画及び予算には，オペレーティングシステムの変更に必要なレビューやシステム試験を含める。 ・セキュリティ更新などによるオペレーティングシステムへの変更が行われることを前提に、システムの完全性を確認、試験する手順を定める。 ・オペレーティングシステムに対する変更を記録する。 ・変更後に、問題が発生した場合に回復させる手順を定める。	・緊急時に、セキュリティ更新プログラムまたはシステムの設定変更を最短で行うための最低限の手順を定める。			A.12.5.2	
33		無線LAN、リモートアクセスのセキュリティ	外部から接続する利用者を認証する	外部利用者を正しく認証できないと、外部からの不正アクセスで、情報漏えいしたり情報システムが停止したりするおそれがある。	・認証しない。	・内部の情報システムにアクセスする前に、ゲートウェイ等で利用者の認証を実施する。 ・外部からのアクセスは、一箇所のみで受け付ける。	・外部からの認証には、ハードウェアキー及びパスワードを利用する。	・外部からの認証には、ハードウェアキー及びワンタイムパスワードを利用する。 ・外部からの認証には、電子証明書を利用する。			A.11.4.2	
34			モバイルコンピュータの利用を管理する	モバイル中の情報機器が盗難される又は紛失してしまうと、情報が漏えいするおそれがある。	・対策しない。	・モバイルコンピュータは、データの暗号化もしくはハードディスクパスワードを利用する。	---> 前レベルと同様	・モバイルコンピュータは、シンクライアントシステムを導入する。			A.11.7.1	

セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策				推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
35			ネットワークサービスのセキュリティを強化する	拠点間ネットワークが盗聴されると、情報が漏えいするおそれがある。	・対策しない。	・拠点間のネットワークは、VPN等の暗号化もしくはアクセス制御が実施されたネットワークサービスを利用する。	・外部へのアクセスに対してのログをモニタリングして、必要時には自動的に警告する。 ・拠点間のネットワークは、VPN等の暗号化もしくはアクセス制御が実施されたネットワークサービスを利用する。	・外部へのアクセスに対してのログをモニタリングして、必要時に自動的に警告する。 ・危険なWebサイトへのアクセスは自動的に遮断する。 ・拠点間のネットワークは、VPN等の暗号化もしくはアクセス制御が実施されたネットワークサービスを利用する。			A.10.6.2	
36		ログの収集や解析	監査ログを取得する	情報システムの監査ログを適切に記録していないと、発生した不正な活動に気づかないおそれがある。	・監査ログを取得しない。	・情報システムのアクセスログを取得する。 ・アクセスログを、定期的に点検する。 ・アカウントによるログオンイベント（ローカル）を記録する（成功）。 ・アカウントへの管理作業を記録する（成功）。 ・アカウントまたはパスワードのポリシー変更を記録する（成功）。 ・システムに影響のあるイベントを記録する（成功）。	・アカウントによるログオンイベント（ネットワーク、ドメイン、ローカル）を記録する（成功）。	・アカウントによるログオンイベント(ネットワーク、ドメイン、ローカル）を記録する（成功/失敗）。 ・アカウントへの変更(管理作業)を記録する（成功/失敗）。 ・アカウントまたはパスワードのポリシー変更を記録する（成功/失敗）。 ・システムに影響のあるイベントを記録する（成功）。 ・オブジェクト(ファイル等)へのアクセスを記録する（失敗）。			A.10.10.1	
37			システムの使用状況を監視する	情報システムの使用状況を監視していないと、問題が発生した際の原因究明が困難になるおそれがある。	・情報システムを監視しない。	・情報システムへの不正なアクセスを定期的に確認する。	・情報システムが不正アクセスされた際に、自動的に検出し、通知するシステムを導入する。	・システムに重大な影響のあるイベントが発生した場合は、システム管理者に通知する。			A.10.10.2	
38			ログ情報を保護する	ログ情報を保護していないと、内容の改ざんや破棄されるおそれがある。	・ログを保護しない。	・情報システムのログを、オフラインで定期的にバックアップする。 ・情報システムのログにアクセス可能なアカウントを制限する。 ・ログの記録漏れ、上書き等が発生しないよう、十分な記憶容量を確保する。 ・ログが削除された事をログに記録する機能を導入する。	・オペレーティングシステムまたはソフトウェアの機能で、適切なログの保護措置が取られている。 ・ディスク等の容量不足などにより、ログが記録できない場合は、システムを停止する。 ・ログのオフラインでのバックアップは、十分な期間に遡って参照可能とする。	・短いサイクルで、別の情報システムにオンラインでログをコピーまたは移動する。			A.10.10.3	
39			実務管理者及び運用担当者の作業を記録する	一般利用者以上の権限を有する利用者の作業を記録していないと、ポリシーに反する作業に気がつかない、犯罪行為を証明する事ができない、などのおそれがある。	・ログを記録しない。	・実務管理者および運用担当者のログを記録する。	---> 前レベルと同様	・実務管理者及び運用担当者の作業が正当であることを確認するために、作業指示書を作成し保管する。			A.10.10.4	
40			障害発生時の状況を記録する	障害発生状況を記録していないと、障害が発生した際の原因究明が困難になるおそれがある。	・障害発生を記録しない。	・情報システムの障害発生を記録する。	・記録された障害毎に、明確な対応策または運用規則を定める。 ・対応策が決められていない場合の運用規則を定め	・情報システムが障害発生した場合は、システム管理者に通知する。			A.10.10.5	
41		ぜい弱性検査	システムのぜい弱性を管理する	情報システムのぜい弱な箇所を攻撃されると、情報が漏えいするおそれがある。	・ぜい弱性を修復しない。	・全てのソフトウェアに対して、セキュリティパッチの有無を、定期的に自己監査で確認する。	・ぜい弱性検査ツールによる検査を、ツール等で定期的に実施する。	・ぜい弱性検査ツールによる検査を、ツール等定期的に実施し、内部監査を実施する。			A.12.6.1	
42		媒体管理	取り外し可能な媒体を管理する	媒体が正しく運用されていないと、情報が漏えいするおそれがある。	・媒体を管理しない。	・媒体一覧を作成する。 ・媒体の利用記録を作成する。	・媒体の利用可能者を、システム的に制限する。	・媒体に保管した情報の、利用可能者をシステム的に制限する。			A.10.7.1	
43			媒体の配送方法を管理する	配送中の媒体が盗難又は紛失すると、情報が漏えいするおそれがある。	・媒体の配送に関するルールを決めない	・配送中は媒体を手元から離さない。 ・媒体の配送に外部業者を利用する場合は、機密保持や紛失時の損害賠償等について契約書に含める。	・媒体を配送する際は、媒体内データの暗号化もしくはアクセス制御機能つき媒体を利用する。	---> 前レベルと同様			A.10.8.3	
44		メール管理	メール送信のルールを決める	送信したメールが盗聴される、もしくは、メール送信先を間違えることにより、情報が漏えいするおそれがある。	・メール送信のルールを決めない。	・メール送信時は、宛先のメールアドレスを十分に確認するように教育する。	・添付ファイルを暗号化する。 ・メールの送信先を、システム的に制限する。	・メール全体を暗号化する。			A.10.8.4	
45			メール受信のルールを決める	不審なメールを受信してしまうと、悪意あるプログラムに感染する、情報が漏えいする、などのおそれがある。	・メール受信のルールを決めない。	・迷惑メール等を開かないように教育・指導する。	・迷惑メール等を、システム的にフィルタリングする。 ・ログ等で監視する。	---> 前レベルと同様			A.10.8.4	
46		廃棄	コンピュータを安全に廃棄、再利用する	廃棄、再利用したコンピュータに過去のデータが残っていると、情報が漏えいするおそれがある。	・データを消去せずにコンピュータを廃棄する。	・コンピュータの記憶領域について、初期化又はヌル値やランダム値の上書き等、残留データを消去する。 ・物理的に破壊する。	・コンピュータの記憶領域について、初期化又はヌル値やランダム値の上書き等、残留データを消去する。 ・廃棄証明書を履歴として保管する。	---> 前レベルと同様			A.9.2.6	
47			媒体を安全に廃棄、再利用する	廃棄、再利用した媒体に過去のデータが残っていると、情報が漏えいするおそれがある。	・データを消去せずに媒体を廃棄する。 ・紙をそのまま廃棄する。	・媒体の記憶領域について、初期化又はヌル値やランダム値の上書き等、残留データを消去する。 ・紙を廃棄する場合は、シュレッダーを利用する等、紙の復元を困難にする。	・媒体の記憶領域について、初期化又はヌル値やランダム値の上書き等、残留データを消去する。 ・廃棄証明書を履歴として保管する。 ・紙を廃棄する場合は、シュレッダーを利用する等、紙の復元を困難にする。	---> 前レベルと同様			A.10.2.7	
48	情報が事実と等しい（完全性保証）	原本性保証	送受信した情報が同一の内容であることを確認する	送受信した業務メッセージなどの情報が同一の内容であることを確認できないと、改ざんされた情報で業務が混乱するおそれがあ	・送信、受信された業務データの整合性を確認しない。	・送信、受信された業務データを人的手段(電話など）で確認する。	---> 前レベルと同様	・送信、受信された業務データに対して、パリティチェックなどでの整合性チェックをシステム的に実行する。			A.12.2.3	
49		監査	情報システムを監査する	情報システムを定期的に監査しないと、不正な活動が検出できなくて、情報を漏えいするおそれがある。	・内部監査をしない。	・個人的に、定期的な監査を実施する。	・定期的な監視と監視実績に基づいた監査を実施する。 ・監査については、定期的に社内組織に委託する。	・監視計画と監視実績に基づいた、監査を実施する。 ・監査については、定期的に第三者組織に委託する。			A.15.3	
50	システムを稼働し続ける（可用性保証）	冗長化	業務サーバ障害時に短時間で復旧させる	業務を行うためのサーバが停止すると、業務が停止して損失が大きくなる。	・サーバが復旧するまで業務を停止する。	・業務サーバのCPUを二重化する。 ・サーバ停止時にも、業務を数十分～数時間の停止で復旧する。	・業務サーバのCPUを二重化する。 ・サーバ停止時にも、業務を数分～数十分の停止で復旧する。	・業務サーバを二重化する。 ・サーバ停止時にも業務を停止させない。				
51		負荷分散装置の設置	高負荷時を考慮してシステムを設計する	システムや装置が処理できる負荷を超えてしまうと、システムの遅延、停止によって、業務が遅延、停止するおそれがある。	・処理能力を考慮しないでシステムを設計する。	・業務に必要なリソース(ネットワーク負荷）の計画と予測をする。 ・システムを、最大使用量で設計する。 ・高負荷時に、業務が遅延することはあるが、停止することはない設計をする。	・業務に必要なリソース(ネットワーク負荷）の計画と予測をする。 ・システムを、最大使用量よりも余裕を持たせて設計する。 ・高負荷時に、業務が遅延することはあるが、停止することはない設計をする。	・業務に必要なリソース(ネットワーク負荷）の計画と予測をする。 ・システムを、最大使用量よりも余裕を持たせて設計する。 ・高負荷時でも、業務が遅延する（レスポンスが低下する）ことのない設計とする。				
52		容量管理・拡張性	情報システムの処理能力を管理する	情報システムの処理能力が不足すると、情報システムが利用できなくなるおそれがある。	・情報システムの処理能力やディスク容量を監視しない。	・処理能力やディスク容量等について、利用者やデータの伸びに対し、一定期間対応可能な情報システムにする。	・拡張する際に、容易に対応可能な情報システムとする。	・情報システムの稼働能力を監視して、計画的に情報システムの容量の増強をことが容易にできるようなシステムとする。			A.10.3.1	
53		トラフィック監視・制御	ネットワークの運用を管理する	ネットワークの管理方針が整備されていないと、外部からの不正アクセスや情報漏えいのおそれがある。	・社外との境界においてネットワーク管理方針を定義しない。 ・インターネットとの接続箇所に、基本的なアクセスフィルタを実施できる装置(ルータ兼用型など)を設置する。	・社外との境界において適切なネットワーク管理方針を定義する。 ・ファイアウォールやUTM機器を設置して、適切なアクセスポリシーを設定する。	・社外との境界において適切なネットワーク管理方針を定義する。 ・ファイアウォールやUTM機器を設置して、適切なアクセスポリシーを設定する。 ・機器の運用状況を適切にモニタリングする。 ・ぜい弱性などに対するパッチ適用の運用体制を決める。	・社外との境界において適切なネットワーク管理方針を定義する。 ・ファイアウォールやUTM機器を設置して、適切なアクセスポリシーを設定する。 ・機器の運用状況を適切にモニタリングする。 ・ぜい弱性などに対するパッチ適用の運用体制を用意する。 ・運用状況を定期的にレポートする。 ・問題発生時の緊急運用体制を定義する。			A.10.6.1	
54			高負荷時を考慮してネットワークを設計する	ネットワーク障害や大量のデータ転送が発生すると、ネットワークが通常通りに利用できなくなるおそれがある。	・負荷を考慮しないでネットワークを設計する。	・通信会社のネットワークサービスを利用する場合は、帯域保証や稼働率に関する内容を、契約書に含める。	・インターネット接続回線や拠点間ネットワークを多重化する。	・インターネット接続回線や拠点間ネットワークについて、複数の通信会社からサービスを受ける。			A.10.6.2	

セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策					推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
55			ネットワークサービスの利用を管理する	ネットワークサービスへのアクセスを適切に制御しないと、社内外からサービスへの不正なアクセスが発生したり、情報が漏えいしたりするおそれがある。	・ネットワークサービス利用に関する方針を策定しない。	・ネットワークサービス利用に関する方針を策定する。	・ネットワークサービス利用に関する方針を策定する。 ・利用者に対して定期的に周知・徹底する。	・ネットワークサービス利用に関する方針を策定する。 ・利用者に対して定期的に周知・徹底する。 ・定期的な内部監査を行い、方針の運用状況を確認する。			A.11.4.1	
56			外部から接続する利用者を認証する	外部利用者を正しく認証できないと、外部からの不正アクセスで、情報漏えいしたり情報システムが停止したりするおそれがある。	・外部からのアクセスに対して利用者認証、監視、制御を実施しない。	・ユーザ名、パスワードでユーザ認証する。	・パスワードの複雑化や定期的な強制変更を実施する。 ・定期的なレポーティングを実施する。	・ワンタイムパスワードや生体認証などの、より高度なユーザ認証を併用する。			A.11.4.2	
57			ネットワーク上の装置を識別する	ネットワークを通過・拒否される装置が適切に識別できないと、不正アクセスなどの発生時に対応が長期化するおそれがある。	・どんな機器でもネットワークに接続できる。	・ネットワークにアクセスする装置種別(機種名、OS種別、バージョンなど)を判定する機器を導入する。 ・許可されない機器の接続を禁止する。	・外部からアクセスされる装置種別(機種名、OSバージョンなど)を判定する機器を導入する。 ・許可された機器のみ接続する。	・外部からアクセスされる装置種別(機種名、OSバージョンなど)を判定する機器を導入する。 ・ポリシー設定で、許可、不許可を自由にコントロールする。			A.11.4.3	
58			遠隔診断用及び環境設定用ポートを保護する	診断・管理用ポートへのアクセスが適切に管理されていないと、設定情報の不正な改ざん、システムの停止、などが発生するおそれがある。	・専用ポートへ誰でもアクセスできる。	・専用ポートに適切なアクセス権を設定する。	・専用ポートに適切なアクセス権を設定する。 ・マシンルームなどの専用ルームへ設置して、物理的に保護する。	・管理用ネットワークは通常のネットワークとは別に用意し、一般利用者からは物理的、論理的にアクセス不可能にする。			A.11.4.4	
59			ネットワーク領域を分割する	ネットワークを適切に分割しないと、不正にアクセスされるおそれがある。	・ネットワークを全く分割しない。	・ルータとスイッチでネットワークを物理的に分割する。	・プロジェクトもしくは組織単位でネットワークを分割する。 ・L3スイッチでネットワークを論理的に分割する。	・プロジェクトもしくは組織単位でネットワークを分割する。 ・VLANでネットワークを論理的に分割する。			A.11.4.5	
60			ネットワーク接続を制御する	ネットワークへの接続制御を実施しないと、不正アクセスや情報漏えいが発生するおそれがあ	・ネットワーク接続を制御しない。	・各ネットワーク境界で適切にアクセス制御する。	・アクセス違反を適切にモニタリングする。 ・異常時は自動的に警告する。	・アクセス違反を適切にモニタリングする。 ・異常時は自動的に警告する。 ・異常時は自動的に遮断する。			A.11.4.6	
61			ネットワークルーティングを制御する	内部・外部からの不正なルーティング情報が流入すると、既存のネットワーク情報が不正に変更されたり、情報システムが利用できなくなったりするおそれがある。	・制御しない。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・静的ルーティングなど、固定的にルーティングを制御する。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・管理下以外のネットワーク機器からのルーティング情報をフィルタする。	・NATを使用し、外部に対して内部ネットワークを不可視にする。 ・管理下以外のネットワーク機器からのルーティング情報をフィルタする。 ・ルーティング情報更新に認証情報（パスワードなど）を追加する。			A.11.4.7	
62		ソフトウェア監視	オペレーティングシステムを保守する	OSを保守しないと、業務停止、ぜい弱性の発生、情報の漏えい、などのおそれがある。	・OSを保守しない。	・セキュリティ対策などのパッチを本番機に直接適用する。	・本番相当環境で是正保守をテストし、障害がないことを確認し本番機に適用する。	・本番相当環境で是正保守、予防保守をテストし、障害がないことを確認し本番機に適用する。			A10.1.5？	
63			ソフトウェアを保守する	ソフトウェアを保守しないと、業務停止、ぜい弱性の発生、情報の漏えい、などのおそれがある。	・ソフトウェアを保守しない。	・セキュリティ対策などのパッチを本番機に直接適用する。	・本番相当環境で是正保守をテストし、障害がないことを確認し本番機に適用する。	・本番相当環境で是正保守、予防保守をテストし、障害がないことを確認し本番機に適用する。				
64			ソフトウェア修正情報を収集する	ソフトウェア修正のためのパッチ情報が把握されていないと、必要な是正保守が行われているかどうかが検証できず、ぜい弱性等が放置されるおそれがある。	・情報を収集しない。	・不定期に情報収集する。	・是正保守として、パッチ情報（提供元、種別、相互依存性、更新版の有無、仕様への影響等）の更新やベンダからの情報入手のサイクルを、運用ルールとして規定する。	・是正保守および予防保守として、パッチ情報（提供元、種別、相互依存性、更新版の有無、仕様への影響等）の更新やベンダからの情報入手のサイクルを、運用ルールとして規定する。				
65			パッチ適用の間隔を定める	是正保守としてのパッチ適用間隔がルール化されていないと、作業に長時間かかり、システムを長時間停止するおそれがある。	・パッチを適用しない	・パッチ適用に関するルールを設定しない。	・パッチを適用する間隔を是正保守として規定する。	・パッチを適用する間隔を、是正保守または予防保守として規定する。				
66			パッチ適用による障害の、回避策を定める	二次障害（パッチ適用による障害）への対策を規定しておかないと、システムを長時間停止するおそれがある。	・障害発生時に対応を検討する。	---> 前レベルと同様	・二次障害発生時の復旧（ロールバック等）作業をルール化する。	---> 前レベルと同様				
67			パッチ適用の作業時間を定める	パッチ適用の作業時間がルール化されていないと、システムを長時間停止するおそれがある。	・パッチを適用しない。	・パッチ適用に関するルールを設定しない。	・パッチを適用する作業時間を是正保守として規定する。	・パッチを適用する作業時間を、是正保守または予防保守として規定する。				
68			パッチ適用を検証し、管理する	パッチ適用状態を管理しないと、ぜい弱性等の危険が解消されないで残ってしまうおそれがある。	・パッチを適用しない。	・本番機に直接適用する。	・本番相当環境で是正保守をテストし、障害が無いことを確認し本番機に適用する。 ・適用状態を管理、監視する。	・本番相当環境で是正保守、予防保守をテストし、障害が無いことを確認し本番機に適用する。 ・適用状態を管理、監視する。				
69			ソフトウェアの変更を管理する	ソフトウェアのバージョンアップなどによる変更を管理していないと、業務に障害があった場合に原因の切り分けが遅れ、業務を長時間停止するおそれがある。	・ソフトウェアを変更しない。	・常に最新のソフトウェアを使用する。	・ソフトウェアの変更のたびに、影響度を確認し、承認を得て、テスト環境で実施し、ロールバック計画を立てて、本番環境に適用する。	・定期的に、影響度を確認し、承認を得て、テスト環境で実施し、ロールバック計画を立てて、本番環境に適用する。				
70		機器監視	電気設備を監視する	電気設備を監視していないと、停電や電圧異常で、システムやネットワーク機器が不安定になったり停止したりするおそれがある。	・電気設備を監視しない。	・無停電電源装置（UPS）を使用する。	・無停電電源装置（UPS）を使用する。 ・使用するUPSのログ機能などを使用し、システム上、重要なサーバやネットワーク機器の電圧異常を管理する。 ・異常時に管理者に対して通知する。	・無停電電源装置（UPS）を使用する。 ・使用するUPSのログ機能などを使用し、システム上、重要なサーバやネットワーク機器の電圧異常を管理する。 ・異常時に管理者に対して通知する。 ・建物の停電時に、一定時間システムを稼働し続けら			A.9.2.2	
71			空調設備を監視する	空調設備を監視していないと、温度の異常な上昇などで、システムやネットワーク機器が不安定になったり停止したりするおそれ	・空調設備を監視しない。	・システム上、重要なサーバやネットワーク機器を温度管理された部屋に配置する。	・システム上、重要なサーバやネットワーク機器自身の温度を管理する。 ・異常時に管理者に対して通知する。	・システム上、重要なサーバやネットワーク機器自身の温度を管理する。 ・異常時に管理者に対して通知する。 ・異常時に空調を自動的にコントロールする。				
72			通信ケーブルを使用した不正アクセスを防止する	通信ケーブルを使用した不正アクセスがあると、情報が漏えいするおそれがある。	・通信ケーブルを自由に使用できる。	・未使用ポートを使用不可に設定する。	・未使用ポートを使用不可に設定する。 ・ポートのLinkUp/Downを監視する。	・MACアドレス認証や、HUB接続などの複数機器の接続防止策を用意する。 ・ポートセキュリティを実施できる検疫システムを導入			A.9.2.3	
73			通信ケーブルの誤挿入・誤抜去を予防する	通信ケーブルの誤挿入・誤抜去が防げないと、システムが停止する恐れがある。	・通信ケーブルを自由に使用できる。	・ケーブルに適切なラベルを貼り、容易に識別できるようにする。	・ケーブルに適切なラベルを貼り、容易に識別できるようにする。 ・未使用ポートを使用不可に設定する。	・ケーブルに適切なラベルを貼り、容易に識別できるようにする。 ・未使用ポートを使用不可に設定する。 ・ポートのLinkUp/Downを監視する。				
74			監査ログを取得する	ネットワーク、システムからの異常検出ログを見逃すと、不正アクセスの検出が遅れたり、情報が漏えいしたりするおそれがある。	・監査ログを取得しない。	・各システムの監査ログ(アクセスログなど)を集約、確認できるように設定する。	・IDSなどにより、監査ログを解析して警告するシステムを導入する。	・IPSなどにより、監査ログを元に自動的にアクセスを拒否するシステムを導入する。			A.10.10.1	
75			システムの稼働状況を監視する	情報システムの稼働状況を監視していないと、問題が発生した際の原因究明が困難になるおそれがある。	・システムの稼動状況を監視しない。	・情報システムが正確に稼動しているか、手動で確認する。	・情報システムが正確に稼動しているか、自動で監視する。 ・定期的に監視状況をレポートする。	・情報システムが正確に稼動しているか、自動で監視する。 ・情報システムに障害が発生した際、緊急の警告を発する。			A.10.10.2	
76			ログ情報を保護する	ログ情報を保護していないと、ログへの不正アクセスや情報が改ざんされるおそれがある。	・ログ情報に誰でもアクセスできる。	・ログ情報は適切なアカウント、パスワードを持つ利用者のみがアクセスできるように設定する。	・アクセスできる機器を限定する。 ・成りすましなどによるアクセス対策(パスワードの定期的な変更、トークンなどの併用)を実施する。	---> 前レベルと同様			A.10.10.3	

セキュリティ・可用性チェックシート（詳細項目版）

	技術的セキュリティ対策					推奨レベル				本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
77			実務管理者及び運用担当者の作業を記録する	作業ログを適切に記録していないと、誤った作業などに対する事後確認を行うことができないおそ	・作業ログを取得しない。	・作業ログを保存する。	・作業ログを保存する。 ・事前に定めた規定に従い、定期的にレビューする。	---> 前レベルと同様			A.10.10.4	
78			障害発生時の状況を記録する	障害発生状況を記録していないと、障害が発生した際の原因究明が困難になるおそれがある。	・障害ログを取得しない。	・障害ログを含む、各種システムログを個別に取得する。	・システム全体の各種システムログを一元管理する。 ・障害発生時に各種警告を自動的に送る。	・システム全体の各種システムログを一元管理する。 ・障害発生時に各種警告を自動的に送る。 ・障害発生時の対応策を用意する。			A.10.10.5	
79			システム時刻を同期する	各システム時刻を同期させていないと、障害や不正アクセスの解析が煩雑になり、異常が発生した際の対応が長期化するおそ	・各システムの時刻を手動で個別に設定する。	・内部・外部NTPサーバを用意し、各システムをNTPに同期させる。	・複数のNTPサーバを用意する。	・GPSなどを利用した専用装置を設置する。			A.10.10.6	

セキュリティ・可用性チェックシート（詳細項目版）

	物理的セキュリティ対策					推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
80	情報を他人から守る（機密性保護）	セキュリティ区画の定義	業務やプロジェクト単位で作業エリアを区分けする	業務部署やプロジェクトの区画を設定していないと、近隣の部署に情報が漏えいするおそれがある。	・作業エリアを決めない。	・仕切りはないが、業務・プロジェクト単位で島（列）を作る。	・業務・プロジェクト単位に、ついたて等で仕切りを作る。	・業務・プロジェクト単位に部屋を分けて作業する。			A.9.1.1	
81		マシンルームの設置	オフィスや部屋への入退出を管理する	入退出を管理していないと、部外者がオフィスや部屋に入れてしまい、情報を盗まれるおそれがある。	・オフィスや部屋等を施錠しない。	・オフィスや部屋の入退出時を、社員証などのIDで管理する。 ・帰宅時には、オフィスや部屋を鍵で施錠する。	・常時、ICカード又は生体認証等により、部屋の入退室を制限する。 ・守衛や防犯カメラを設置する。 ・部屋の入退室を記録する。	・入室ログのない退室は、許可しない。 ・インターロック（二重扉）を実施する。			A.9.1.3	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設16, 連13
82			内部犯による情報機器の盗難を予防する	情報機器が内部の利用者に盗難されると、情報が漏えいするおそれがある。	・情報機器が自由に持ち出せる。	・コンピュータをワイヤー等で固定する。 ・サーバは、施錠されたサーバラック内に保管する。	・コンピュータをワイヤー等で固定する。 ・サーバは、施錠されたサーバラック内に保管する。 ・サーバ類の設置場所を、施錠された区域内にする。	・情報機器の設置場所を、アクセス制御された区域内にする。 ・情報機器（サーバ）の設置場所を、施錠された区域内にして、入退出の記録をとる。			A.9.2.1	・政府機関統一基準適用個別マニュアル群 庁舎内におけるPC利用手順 PCの取扱編 5.2 端末の設置 ・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設23
83		防犯設備の設置	外部犯による情報機器の盗難を予防する	外部からの侵入者に情報機器が盗難されると、情報が漏えいするおそれがある。	・情報機器の設置場所を監視しない。	・情報機器の設置場所を監視する。 ・外部からの不正な侵入に対して警報を鳴らす。	・情報機器の設置場所を監視する。 ・外部からの不正な侵入に対して警報を鳴らす。	・情報機器の設置場所を監視する。 ・外部からの不正な侵入に対して警報を鳴らし、通報する。			A.9.1.4	
84		マシンルームへの電磁波シールドの設置	情報機器を電磁波から保護する	電磁波からの保護ができていないと、情報データが破壊されるおそれがある。	・電磁波に対するシールド対策をしない。	---> 前レベルと同様	・電磁波に対するシールド対策を、コンピュータやネットワーク機器に施す。	・マシンルームに対して電磁波のシールド対策をする。			A.9.1.4	
85	情報が事実と等しい（完全性保証）	定期的なバックアップ取得	業務データのバックアップを安全な場所に保管する	バックアップを安全な場所に保管しないと、不慮の災害発生時などにシステムを業務可能な状態に復旧できなくなるおそれがある。	・業務データをバックアップしない。	・業務に必要なデータを媒体に、定期的(日次、週次)バックアップを行い、安全な場所に輸送して保管する。	・業務に必要なデータを、遠隔地にリモートで、定期的（日次、週次）にバックアップを行う。	・業務に必要なデータを遠隔地にリモートで、リアルタイムにバックアップする。			A.10.5.1	
86			復旧時間を考慮してバックアップ媒体を選択する	復旧に要する時間を考慮してバックアップ媒体を選択しないと、必要な時間内にシステムを復旧できないおそれがある。	・業務データをバックアップしない。	・バックアップデータを、テープや光ディスクのような運搬可能な媒体に保管する。	・バックアップデータを、ハードディスクに保管する。	---> 前レベルと同様				
87	システムを稼働し続ける（可用性保証）	温度・湿度管理	情報機器の設置場所の環境を適切に保つ	温度や湿度を適切に保たないと、情報システムが正常に動作しなくなるおそれがある。	・空調を設置しない。	・空調を設置する。 ・湿度を40～60%に保つ（静電気対策）。	・空調を設置する。 ・湿度を40～60%に保つ（静電気対策）。 ・結露を発生させない。	・空調を、故障に備えて、冗長化する。			A.9.1.4	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設33
88		耐震、耐火、耐水対策済み施設の利用	情報機器を災害から守る	地震、火災、洪水等の災害への対策を整えておかないと、情報システムが故障し、業務が長期間停止するおそれがある。	・災害を考慮しない。	＜耐震＞ ・情報機器を、落下防止金具もしくはバンド等で固定する。 ・サーバラックを、パネルアンカー等で固定する。 ＜耐火＞ ・自動火災報知設備を設置する。 ・消火設備（消火器、スプリンクラー）を設置する。 ・情報機器を、火災の危険性のない場所（火使用設備が隣室又は直上下階にない場所等）に設置する。 ・室内の火気使用を制限する。 ＜耐水＞ ・情報機器を、浸水の危険性のない場所（2階以上、水使用設備が隣室又は直上階にない場所等）に設置する。	＜耐震＞ ・情報機器を、落下防止金具もしくはバンド等で固定する。 ・サーバラックを、パネルアンカー等で固定する。 ＜耐火＞ ・自動火災報知設備を設置する。 ・消火設備（消火器、スプリンクラー）を設置する。 ・情報機器を、火災の危険性のない場所（火使用設備が隣室又は直上下階にない場所等）に設置する。 ・室内の火気使用を制限する。 ＜耐水＞ ・情報機器を、浸水の危険性のない場所（2階以上、水使用設備が隣室又は直上階にない場所等）に設置する。	＜耐震＞ ・建物を、免震建築物もしくは制振建築物にする。 ・情報機器を、免震床に設置する。 ＜耐火＞ ・消火設備（全域放出型消火ガス）を設置する。 ＜耐水＞ ・漏水を排出する排水溝等を設置する。			A.9.1.4	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設22, 32, 37, 39, 50
89		無停電電源装置、バックアップ電源等の設置	電力を安定供給する	電力を安定供給しないと、停電や電圧異常で、システムやネットワーク機器が不安定になったり停止したりするおそれがある。	・停電対策を実施しない。	・UPSを設置する。 ・建物に、避雷針を設置する。 ・静電気対策として、アースを利用する。	・自家発電装置を設置する。	・電力会社から、電源を複数回線で引き込む。			A.9.2.2	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設62, 64, 65, 69
90		ケーブル敷設経路対策の実施	通信、電源ケーブル配線を保護する	通信、電源ケーブルが切断されてしまうと、情報システムが停止する、長期間利用できなくなるおそれがある。	・通信、電源ケーブルをむき出しにする。	・通信、電源ケーブルは、フリーアクセス床の下を通す。 ・通信、電源ケーブルに、カバーをつける。	---> 前レベルと同様	・通信、電源ケーブルは、専用の配線管を通し、人目につかないように設置する。			A.9.2.3	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版）設97
91		在庫管理	情報資産を管理する	情報資産（情報機器・電子媒体・紙）が管理されていないと、紛失・盗難の検出ができないおそれがある。	・情報資産を管理しない。 ・媒体や紙資産の、保管場所や管理番号がない。	・情報資産を部署単位で管理する。 ・媒体や紙資産については、管理番号は付与せずに、カテゴリ別で保管する。	・情報資産の管理にツールを使う。 ・管理番号を付与して管理する。 ・媒体や紙の資産については、管理番号を付与して、管理台帳等で所在を明確にして、鍵をかける。	・情報資産の管理にツールを使う。 ・管理番号を付与して、定期的に内部監査する。 ・媒体や紙の資産については、管理番号を付与して、管理台帳等で所在を明確にして、鍵をかける。 ・鍵は管理者が管理する。			A.7	
92			情報資産の管理責任を明確にする	情報資産の責任者が明確でないと、資産の管理・保存期限、滅却などが計画的におこなわれず、不要になった資産から情報が漏えいするおそれがある。	・利用者の判断で資産を保存・滅却する。	・資産ごとに管理責任者を決め、管理責任者の判断で資産を保存・滅却する。	・資産ごとに管理責任者・保存期間・滅却期日を決め、定期的に資産を見直す。	・資産ごとに管理責任者・保存期間・滅却期日を決め、資産管理を計画的に実施する。			A.7.1	
93		機器設置スペースの拡張性	機器設置スペースに拡張性を持たせる	機器設置場所に拡張性がないと、情報処理機器をセキュリティが低い場所に設置しなくてはならなくなる。	・設置スペースを拡張しない。	・情報処理機器の設置スペースを確保する時に、現在の業務処理データ量を考慮する。	・将来の業務拡張計画などから、情報処理機器の設置スペースを設計する。	---> 前レベルと同様				

セキュリティ・可用性チェックシート（詳細項目版）

	管理的セキュリティ対策				推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
94	情報を他人から守る（機密性保護）	セキュリティポリシー	セキュリティポリシーを策定する	セキュリティ基本方針を定義しておかないと、一貫したセキュリティ対策がとれず、ぜい弱なシステムになってしまうおそれがある。	・セキュリティポリシーを策定しない。	・現状を把握し、リスク分析の結果をもとに、情報セキュリティ基本方針を策定する。	---> 前レベルと同様	---> 前レベルと同様			A.5.1	
95		利用者管理	情報にアクセスするためのガイドラインを策定する	情報アクセスのためのガイドラインを策定しておかないと、情報を制御する対象や範囲が明確にならない。	・アクセス制御方針を策定しない。	・情報へのアクセス制御方針を文書化する。	・情報へのアクセス制御方針を文書化する。 ・定期的にレビューする。	・情報へのアクセス制御方針を文書化する。 ・定期的にレビューする。 ・アクセス方針に従った業務であることを、監査する。			A.11.1.1	
96			システムの利用者を管理する	情報システムの利用者を管理していないと、部外者がシステムを利用できてしまい、情報が漏えいする可能性がある。	・利用者を登録、管理しない。	・一つのアカウントを複数の利用者で使用しない。 ・利用者の増減や移動に伴い、アカウント及びアクセス権を変更する。	・利用者の増減や移動をシステムで管理し、アカウント及びアクセス権を自動的に変更する。	・利用者の増減や移動をシステムで管理し、アカウント及びアクセス権を自動的に変更する。 ・登録情報として、生体認証を導入する。			A.11.2.1	
97			特権を持つ利用者を管理する	特権を持つ利用者の作業を管理しないと、機密情報を不正に操作されて外部に漏えいされるおそれがある。	・特権ユーザの履歴ログを取得しない。	・特権ユーザを絞り込み、特権ユーザの操作ログを取得する。	・特権ユーザを絞り込み、特権ユーザの操作ログを取得して定期的に監査する。	---> 前レベルと同様			A.11.2.2	
98			利用者のパスワードを管理する	利用者のパスワードを定期的に変更するなどの管理をしていないと、パスワードが流出し、システムに不正アクセスされる、情報が盗まれる、などのおそれがある。	・パスワードを変更しない。	・利用者のパスワードが、定期的に変更されていることをチェックする。	---> 前レベルと同様	・利用者のパスワードが定期的に変更されるシステムを導入する。 ・変更依頼のメッセージをシステムから送る。			A.11.2.3	
99			利用者のアクセス権を管理する	利用者のアクセス権を定期的に見直さないと、プロジェクトや組織の変更にともなって、参照できてはいけないものが継続して見えてしまい、情報が漏えいするおそれがある。	・アクセス権を見直さない。	・アカウント及びアクセス権を、定期的に見直す。	---> 前レベルと同様	・組織やプロジェクトが変更になった場合、ユーザ管理システムと連携して、自動的にアクセス権を変更する。 ・変更になったアクセス権を定期的に監査する。			A.11.2.4	
100			情報処理施設の使用を記録する	情報処理施設が不正に使用されると、情報処理機器へアクセスされて、情報が漏えいするおそれがある。	・情報処理施設への入出や使用を記録しない。	・情報処理施設への入出を記録する。	・情報処理施設の入出記録をシステムで取得する。 ・定期的に監査する。	・情報処理施設の入出記録をシステムで取得する。 ・施設への入館時に、許可されている利用者であるかを自動的にチェックする。 ・定期的に監査を行う。			A.15.1.5	
101			情報を暗号化する	情報の暗号化をルールとして企業内で統一しておかないと、利用者毎に暗号化対象が変わってしまい、重要情報が漏えいするおそれがある。	・暗号化しない。	・個人の判断で、ファイルを暗号化する。	・情報(データ）を強制的に暗号化する。	・すべてのファイルを強制的に暗号化する。			A.15.1.6	
102		入退室管理	作業領域を施錠し監視する	オフィス等の作業領域を施錠、監視しておかないと、部外者が不正に侵入し、情報の漏えいや情報機器の盗難等のおそれがある。	・オフィス等を施錠しない。	・帰宅時には、部屋を鍵で施錠する。	・常時、ICカード又は生体認証等で、部屋の入退室を制限する。 ・防犯カメラを設置する。 ・部屋の入退室を記録する。	・入室ログのない退室は、許可しない。 ・インターロック（二重扉）を実施する。			A.9.1.2	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版） 設16, 運13
103		秘密保持契約	第三者との契約内容を定める	第三者との契約内容をあらかじめ決めておかないと、機密保持契約がないために情報漏えい時の責任追及ができないなど、情報が守られなくなるおそれがあ	・契約内容をあらかじめ規定しない。	・第三者との間で、担当者が機密保持契約を交わす。	・第三者との間で、担当部署間が機密保持契約を交わす。 ・機密保持契約には、情報の入手についてセキュリティを守る条項を明記する。	・第三者との間に、双方の法務部門を通して、会社名義で機密保持契約を交わす。 ・機密保持契約には、情報の入手についてセキュリティを守る条項を明記する。			A.6.2.3	
104		ぜい弱性情報収集と修正プログラム適用	ぜい弱性情報を入手して対策する	OSやアプリケーションのぜい弱性の情報が入手できないと、ぜい弱性がそのまま放置されて、情報が漏えいするおそれがある。	・ぜい弱性情報を収集しない。	・OSやアプリケーションのぜい弱性レポートを定期的に入手して、パッチ適用を計画する。	・OSやアプリケーションのぜい弱性レポートを定期的に入手して、パッチ適用を計画する。 ・本番相当環境で是正保守をテストし、障害がないことを確認し本番機に適用する。	・OSやアプリケーションのぜい弱性レポートを随時入手して、パッチ適用を計画する。 ・本番相当環境で是正保守、予防保守をテストし、障害がないことを確認し本番機に適用する。			A.12.6.1	
105		資産管理	情報資産を管理する	情報資産を正確に管理しておかないと、資産を紛失、盗難しても気付かないおそれがある。	・情報機器の一覧を作成しない。	・情報機器の一覧を作成する。 ・情報機器一覧の棚卸を行う。	・情報資産（情報そのもの）の一覧を作成する。	・情報資産の管理にツールを使い、拾い上げ、管理番号が付与されており、定期的に内部監査などを実施する。 ・媒体や紙の資産については、管理番号を付与して、管理台帳等で所在が明確にして、施錠する。			A.7.1.1	
106			情報資産を分類する	情報資産が重要度に応じて正しく分類されていないと、重要な情報が厳重に管理されず、権限のない利用者に情報が漏えいするおそれがある。	・情報資産の分類基準を作成しない。	・情報資産の分類基準（極秘、秘、社外秘等）を作成する。	・情報資産の分類基準（極秘、秘、社外秘等）を作成する。 ・分類ごとに資産番号を付与する。	・情報資産の分類基準（極秘、秘、社外秘等）を作成する。 ・分類ごとに資産番号を付与する。			A.7.2.1	
107			情報資産を分類に応じて取り扱う	情報資産が分類基準に従って取扱わないと、権限のない利用者に情報が漏えいするおそれがある。	・情報資産を分類基準に従って取扱わない。	・資産ごとに管理責任者を決める。 ・管理責任者の判断で資産を保存・滅却する。	・情報資産に、分類基準に従って分類した結果を明記する。 ・情報資産を、分類基準に従って取扱う。 ・資産ごとに管理責任者、保存期間、滅却期日を決める。	・情報資産に、分類基準に従って分類した結果を明記する。 ・情報資産を、分類基準に従って取扱う。 ・資産ごとに管理責任者、保存期間、滅却期日を決める。			A.7.2.2	
108			机上の情報を保護する	情報が机上に放置や表示された状態になっていると、目視で情報が漏えいするおそれがある。	・机上での情報の取り扱いルールがない。	・帰宅時には、書類を机上に放置しない。 ・一定時間（30分）が経過したら、画面を自動的にスクリーンロックする。	・離席時には、書類を机上に放置しない。 ・離席時には、すみやかに、画面を操作不可能な状態（ログオフ、スクリーンロック等）にする。 ・一定時間（10分）が経過したら、画面を自動的にスクリーンロックする。	・ディスプレイに、盗み見防止のフィルタを装備する。 ・ディスプレイに、電磁波対策のフィルタを装備する。		A.11.3.3	・政府機関統一基準適用個別マニュアル群 庁舎内におけるPC利用手順 PCの取扱編 5.1 端末機能にかかわる検討、5.2 端末の設置(10)
109	情報が事実と等しい（完全性保証）	情報のバックアップ	情報をバックアップする	情報を適切にバックアップしていないと、情報の消失、改ざん等が発生した際に、復旧できなくなってしまうおそれがある。	・バックアップを取得しない。	・バックアップのポリシー（世代管理、バックアップ対象、取得サイクル等）を作成する。 ・ポリシーに従い、情報をバックアップする。 ・リストアが、適切な時間内に可能であることを確認する。	・バックアップ媒体を、同一建物内に保管する。 ・バックアップデータを、暗号化する。	・バックアップ媒体を、遠隔地（60km以上）に保管する。			A.10.5.1	・金融機関等コンピュータシステムの安全対策基準・解説書（第7版） 運27
110		情報システムの正確性	システムを受入れる時に検証する	システムを受け入れる際に十分な検証を実施しないと、運用開始後にシステムの不良に気づくことになり、長期間業務が停止してしまうおそれがある。	・システムをテストしない。	・システムを新たに導入もしくは変更する場合は、本番稼動前にテストする。 ・システム開発者がテストした結果を見て検収する。	・システムを新たに導入もしくは変更する場合は、本番稼動前にテストする。 ・受け入れテストを第三者に委託して、客観的にテストする。	・システムを新たに導入もしくは変更する場合は、本番稼動前にテストする。 ・自社内に受け入れ検査の体制と、受け入れ検査用のデータを用意して、擬似本番環境にて適切な期間検収テストを行う。			A.10.3.2	
111		情報の正確性	入力データの正確さを追求する	入力されたデータが正確でないと、誤りが多い情報になってしまい、業務が停止してしまうおそれ	・入力データをチェックしない。	・入力フィールドには、可能な限り、文字種や桁数等の制限をつける。	・データ入力作業を委託する場合、入力誤り率に関するサービスレベルを契約で取り決める。 ・入力データの妥当性をシステムでチェックする。	---> 前レベルと同様			A.12.2.1	
112	システムを稼働し続ける（可用性保証）	教育と訓練	セキュリティ教育を実施する	セキュリティや情報漏えいに対する基本方針などを利用者が正しく理解していないと、安易に情報を取り扱い外部に漏えいしてしまうおそれがある。	・セキュリティ教育をしない。	・部署単位で、セキュリティ教育を定期的に実施する。	・部署単位で、セキュリティ教育を定期的に実施し、教育受講者を管理する。 ・作業外注者に対してセキュリティ教育を実施する。	・組織のトップから、全社員に対してセキュリティメッセージを通達する。 ・部署単位で、セキュリティ教育を定期的に実施し、教育受講者を管理する。 ・作業外注者に対してセキュリティ教育を実施する。 ・会社組織として、セキュリティ教育推進部署を設置する。			A.8.2.2	
113		運用体制	利用者の活動を管理する	企業内の組織で運用する場合、悪意を持った利用者から情報が漏えいするおそれがある。	・利用者の操作ログを取得しない。	・利用者の操作ログを取得して、定期的に監査する。	---> 前レベルと同様	・複数の責任者で相互に監視する。 ・利用者の操作ログを取得して、定期的に監査する。			A.6.1	
114			外部組織を管理する	運用を第三者組織に委託した場合、委託先から情報が漏えいするおそれがある。	・利用者の操作ログを取得しない。	・利用者の操作ログを取得して、定期的に監査する。	---> 前レベルと同様	・利用者の操作ログを取得して、定期的に監査する。 ・コンピュータの操作画面をモニターする。			A.6.2	

セキュリティ・可用性チェックシート（詳細項目版）

	管理的セキュリティ対策					推奨レベル			本件業務のセキュリティ仕様			
	要素	分類	対策項目	リスクの詳細	レベル1	レベル2	レベル3	レベル4	該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
115		監査	情報システムの運用を監査する	情報システムを定期的に監査していないと、不正な活動を検出できなくて、情報が漏えいしてしまうおそれがある。	・情報システムを監査しない。	・定期的に、個人による監査を実施する。	・監視計画と監視実績に基づいた監査を実施する。 ・監査については、定期的に社内組織に委託する。	・監視計画と監視実績に基づいた監査を実施する。 ・監査については、定期的に第三者組織に委託する。			A.15.3	
116		緊急時対応計画	情報漏えい時の対応を管理する	漏えい事故のレベルによって対応を管理していないと、対応が遅れ被害が大きくなるおそれがある。	・漏えい事故を管理しない。	・漏えい事故を管理する。 ・すべての漏えい事故を同様に扱う。	・漏えい事故を管理する。 ・漏えい事故に対する、レベル判断基準を設定する。 ・漏えい事故のレベルに応じた対応を規定しない。	・漏えい事故に対する、レベル判断基準を設定する。 ・レベルに応じた対応を、組織的な手順として確立する。 ・事故対応の情報、活動が、組織のトップまでスムー			A.13	
117			情報セキュリティ事象を報告する	情報セキュリティに何らかの変化があった場合の報告の仕組みが規定されていないと、対応が遅れて被害が拡大するおそれがある。	・情報セキュリティ事象の報告ルートを規定しない。	・情報セキュリティ事象の報告ルートを規定する。	・情報セキュリティ事象の報告ルート、速やかな報告ルールを規定する。	---> 前レベルと同様			A.13.1.1	
118			セキュリティの弱点を報告する	セキュリティの弱点が発見されても報告する仕組みがないと、報告が遅れ、弱点を攻撃されたり、弱点を利用して情報が漏えいしたりする。	・セキュリティの弱点の報告ルートを規定しない。	・セキュリティの弱点の報告ルートを規定する。	・セキュリティの弱点の報告ルート、速やかな報告ルールを規定する。	---> 前レベルと同様			A.13.1.2	
119			情報の取り扱いを記録する	誰がどのように情報を取り扱ったかを記録していないと、情報漏えい発生時に原因の追及が困難になり、再発を防げないおそれがある。	・情報の取り扱いを記録しない	・情報の取り扱い履歴を、ログに記録する。	・情報の取り扱い履歴を、ログに記録する。 ・利用者の情報の取り扱いを、ログに記録する。 ・情報のログと、利用者のログを利用して、情報の流通経路をトレースするシステムを導入する。	---> 前レベルと同様			A.13.2.3	
120		見直し	情報セキュリティ事故を管理して改善する	情報セキュリティ事故の管理を定期的に見直して改善しないと、同じような事象が発生するおそれがある。	・情報セキュリティ事故を管理しない。	・情報セキュリティ事故を管理する。 ・不定期に事故の改善を実施する。	・情報セキュリティ事故を管理する。 ・定期的に事故の改善を実施する。	・情報セキュリティ事故を管理する。 ・事故発生直後に改善を実施する ・定期的に事故改善を見直す。			A.13.2	

Webアプリケーション セキュリティ・可用性チェックシート（詳細項目版）

	要素	分類	対策項目	リスクの詳細	推奨レベル レベル1	レベル2	レベル3	レベル4	本件業務のセキュリティ仕様 該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
1	情報を他人から守る（機密性保護）	ユーザ認証	パスワードを利用する	パスワードが推測可能な容易なものになっていると、第三者がシステムに不正アクセスし、情報を漏えいしてしまうおそれがある。	・パスワードを設定しない。	・初期パスワードをすみやかに変更する。 ・定期的（六ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上）を設定する。 ・パスワードは、管理者を含め誰にも教えない。 ・パスワードを書き留めたり、コンピュータ上のファイルに保管したり、メールで送信したりしない。やむを得ず紙片等にパスワードを記載する必要がある場合には、そのパスワードが容易に第三者に見られることがないように保管する。 ・自分のパスワードが他人に漏えいした可能性や疑いがある場合は、パスワードを変更する。	・定期的（三ヶ月毎）に、パスワードを変更する。 ・パスワードは、複雑なもの（八桁以上、パスワード世代管理、三種類以上の文字種の使用）を設定する。	・同一利用者が複数のアカウントをもつ場合は、それぞれ異なるパスワードを設定する。 ・一つのパスワードから他方が推測しやすいパスワードを設定しない。 ・生体認証を利用する。			A.11.2.3 A.11.3.1 A.11.5.2 A.11.5.3	・政府機関統一基準適用個別マニュアル群 庁舎内におけるPC利用手順 PCの取扱編 端末利用者パート 2.3 識別コードの日常の取扱い(2), (3)
2			ログインの認証方法をルール化する	認証に関するルールが明確になっていないと、第三者がシステムに不正アクセスし、情報を漏えいしてしまうおそれがある。	・認証に関するルールを定めない。	・認証の再試行可能回数を定める。 ・再試行可能回数を超えて認証が失敗した場合は、二十四時間当該アカウントを停止する。 ・認証情報はセッションまたはCookieに保存する。 ・ログインID/パスワード等の認証情報をCookie上に暗号化せずに保存する。	・認証画面(機能)を使用して、コンピュータとアプリケーションを利用する。 ・一定回数以上ログオンに失敗したアカウントは、ロックアウトさせる。 ・パスワードの定期的な変更を、システム機能により強制させる。 ・パスワードを他人から推測されにくいものにすることを、システム機能により強制させる。 ・パスワードをシステム内に保存する場合は、暗号化する。 ・パスワードをクライアントーサーバ間で通信する場合は、暗号化する。	・認証のログを採取する。 ・ログインID/パスワードはセッション上に保存せず、利用者をシステム側で管理する一意な文字列をセッションに保存する。			A.11.3.2 A.11.4.2 A.11.5.2	Web Application Security Consortium http://www.webappsec.org/
3			ログイン状態の継続をルール化する	ブラウザを閉じた後もアプリケーションに対しての認証状態を継続させる場合、第三者の操作によって情報が漏えいするおそれがある。	・認証状態の継続に関するルールを定めない。	・ブラウザを閉じた後も、期限を定めずシステムに対しての認証状態を継続する。	・ブラウザを閉じた後も、一定期間システムに対しての認証状態を維持する。 ・認証状態の維持は、ユーザの明確な意思によって行われるものとし、その操作方法について明記する。	・個人情報及び、商取引を行うページへのアクセスの際には、たとえ既にログイン状態であったとしても、再度ログインを行うようユーザに要求し、第三者による不正な操作を防止する。			A.11.4.2 A.11.5.5	
4			認証画面を暗号化する	認証画面へアクセスする際に、SSLによる暗号化などを施さないと、通信経路を傍受され、情報漏えいが発生するおそれがある。	・認証画面を暗号化しない。	・認証画面を暗号化する。 ・SSLの鍵の種類については規定を設けない。	・SSLの鍵長は128Bitを使用する。	・SSL証明書は、EV-SSL証明書を使用する。			A.11.5.1	
5		アクセス権限	アクセス権限を策定する	アクセス権限を策定しないと、利用者のアクセス可能範囲が明確とならないため、不正なアクセスを許してしまうおそれがある。	・アクセス権限を定めない。	・利用者と管理者にクライアントを分類する。 ・利用者は、管理者の機能を使用できないものとする。	・管理者の中に権限の階層を設ける。 ・管理者であっても、所定の権限がない場合はアクセスを許可しない。	・各機能へのアクセスログを採取する。			A.11.2.4 A.11.6.1	
6		暗号化	データを暗号化する	データを暗号化しないと、個人を特定できる情報が漏えいした場合、第三者にその情報が知られるおそれがある。	・データを暗号化しない。	・クレジットカード等の情報に限定して暗号化する。 ・暗号化に使用する文字列を暗号化しない。	・個人を特定できる情報を暗号化する。 ・暗号化に使用する文字列を暗号化する。 ・暗号化に使用する文字列は、管理者以外でも容易に知ることができる。	・全てのデータを暗号化する。 ・暗号化に使用する文字列は、管理者以外に知らせない。			A.10.7.3	
7			パスワードを暗号化する	パスワードを暗号化しないと、第三者によってデータの漏えいが起きた場合、パスワードが第三者に知られるおそれがある。	・パスワードを暗号化しない。	・パスワードは、復号可能な方式を使用して暗号化する。	・パスワードは復号できない方式を使用して暗号化し、たとえシステム管理者であってもユーザのパスワードを復号できないようにする。	---> 前レベルと同様			A.10.7.3	
8		セッション・Cookieの運用	セッションを使用したデータ保持の方法を利用する	セッションの運用ルールを定めないと、第三者によってセッション上のデータが漏えいするおそれがある。	・セッションの使用ルールを定めない。	・セッションIDは、開発に使用するアプリケーションが規定するものを使用する。 ・セッションはWebブラウザを閉じるまでの間有効とする。 ・新規にWebブラウザにてアクセスする度にセッションを作成する。 ・セッションIDはURL文字列またはCookieに保存する。	・一定時間以上アクセスがない場合、システム側でセッションを自動的に破棄し、利用者にはセッションが期限切れとなった旨を通知する。 ・認証及び個人情報を操作する処理においては、アクセスのたびにセッションを再作成する。 ・セッションIDはCookieに保存する。	・セッションを使用するすべての処理で、アクセスのたびにセッションを再作成する。 ・セッションIDを格納するCookieは、暗号化通信が行われている環境下でのみ使用する。			A.11.5.5	
9			Cookieを使用したデータ保持の方法を利用する	Cookieの運用ルールを定めないと、第三者による盗聴等の被害を受けるおそれがある。	・Cookieの使用ルールを定めない。	・ログインID/パスワード等の認証情報をCookie上に保存する。 ・Cookieの有効期限は三十日以内とする。 ・Cookieは保有するドメイン全体で使用する。 （例：xxxxx.com）	・システムが認識できる、意味を持たない文字列を認証情報の代替として保存する。 ・認証情報を扱うCookieについては、セッションの有効期限に準じた有効期限を使用する。 ・その他の情報のCookieへの保存は許可しない。 ・Cookieは使用するドメインでのみ使用する。 （例：www.xxxxx.com）	・利用者の嗜好分析・行動解析に使用する、個人を特定することができない情報に限り、Cookie上への保存を許可する。 ・ログイン情報等を取り扱うCookieについては、Cookieを発行したドメインでのみ使用する。			A.11.5.5	
10		アプリケーションの対策	偽Webサイトによるフィッシング詐欺を対策する	Webサイトでむやみにフレームなどを使用すると、コンテンツの詐称によりパスワードの抜き取りやフィッシング詐欺サイトへの誘導の危険性があります。	・Webサイトのデザインについてのルールを定めない。	・フレームを使用しない。 ・IFRAME/レイヤーについては規定しない。	・IFRAME/レイヤーを使用しない。	・管理者機能の、管理者自らの操作によってHTMLを使用したコンテンツを作成する場合に限り、IFRAME/レイヤーの使用を許可する。			A.10.4.1 A.12.2.4	Web Application Security Consortium http://www.webappsec.org/
11			クロス・サイト・トレーシングを対策する	クロス・サイト・トレーシングが使用されると、他のぜい弱性を利用して、第三者が利用者（会員等）や管理者に成りすますおそ	・「TRACE」メソッドを有効にする。	・「TRACE」メソッドを無効にする。	・「TRACE」メソッドを無効にする。 ・攻撃を検出して、ログをとる。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.10.4.1	Web Application Security Consortium http://www.webappsec.org/
12			クロス・サイト・スクリプティング（XSS）を対策する	クロス・サイト・スクリプティング（XSS）が使用されると、パスワードの抜き取りやフィッシング詐欺サイトへの誘導、情報漏えい等のおそれがある。	・利用者が入力した値をそのまま利用する。	・利用者が入力した値は、例外なく無害化処理を施した上で表示する。	・攻撃を検出して、ログをとる。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.10.4.1 A.12.2.4	Web Application Security Consortium http://www.webappsec.org/
13			クロス・サイト・リクエスト・フォージェリを対策する	クロス・サイト・リクエスト・フォージェリを使用されると、第三者によるWebサイトの改ざん等のおそれがある。	・ログイン後の画面を、URL直入力でいつでも表示することができる。	・ログイン後の画面は、URL直入力などによる画面表示を禁止し、正規の画面遷移のみ許可する。	・1アクセス毎に有効な、セッションIDとは異なるIDを利用者に付与しシステム側と照合することで、正規の画面遷移以外を排除する。 ・攻撃を検出して、ログをとる。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.10.4.1 A.12.2.1	Web Application Security Consortium http://www.webappsec.org/
14			パラメータ改ざんを防止する	パラメータ改ざんが発生すると、第三者が利用者（会員等）や管理者に成りすますおそれがある。	・パラメータ改ざんをチェックしない。	・入力フォームの値について改ざんがされていないか、遷移先のページでチェックする。	・外部から入力（入力フォーム、URLパラメータやhidden、Cookie、ヘッダパラメータ等による入力）について改ざんがされていないか、遷移先のページでチェックする。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.10.4.1 A.12.2.1	Web Application Security Consortium http://www.webappsec.org/
15			ネットワークの過負荷と、サーバへの過大な同時アクセスを対策する	バッファオーバフローを使用されると、Webサーバのサービス停止や、Webサーバを乗っ取られるおそれがある。	・サーバ上で使用するアプリケーションのバージョン管理をしない。	・アプリケーションのバージョンを管理し、バージョンアップ計画を作成して、順次最新の状態になるように運用する。	・重要なぜい弱性が報告された場合は、即時バージョンアップ対応を行う。 ・対策バージョンのリリースまでに時間がかかる場合に、ぜい弱性の報告内容から自社アプリケーションに該当の事象があるかを調査し、可能な範囲での対策を講じる。	・重要なぜい弱性が報告された場合は、即時バージョンアップ対応を行う。 ・即時対応が不可能な場合はサービスを停止する。			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
16			サーバへの不正な要求によるサーバ攻撃を対策する	書式文字列攻撃されると、Webサーバのサービス停止や、Webサーバを乗っ取られるおそれがある。	・何も対策を施さない。	・printf等の書式文字列関数のパラメータに、外部から入力したデータを使用する際は、書式文字列攻撃の対策を実施する。	・書式文字列関数を使用しない。 ・攻撃を検出して、ログをとる。	・WAFを導入する。 ・攻撃を検出して、管理者に通知する。				Web Application Security Consortium http://www.webappsec.org/
17		他システム・アプリケーションとの連携	外部プログラムの実行によるぜい弱性を対策する	外部プログラムを不正に実行させると、Webサイトからの情報漏えい、改ざん等のおそれがある。	・Webサーバのユーザ権限を使用する。 ・外部から入力されたデータをチェックしない。	・Webサーバの利用者は既定のユーザを使用する。 ・外部から入力されたデータに、外部プログラムが埋め込まれていないかチェックし排除する。	・Webサーバが実行可能なOSコマンドを制限する。 ・外部から入力されたデータに、外部プログラムが埋め込まれていた場合、ログに履歴を残す。	・基本的にWeb上からOSのコマンドは実行しない。どうしても実行しなければならない場合は、外部から入力されたデータに依存しない方法をとる。 ・WAFを導入する。 ・攻撃を検出して、管理者に通知する。			A.12.2.1	Web Application Security Consortium http://www.webappsec.org/

Webアプリケーション セキュリティ・可用性チェックシート（詳細項目版）

	要素	分類	対策項目	リスクの詳細	推奨レベル レベル1	レベル2	レベル3	レベル4	本件業務のセキュリティ仕様 該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
18			SSI インジェクションを対策する	SSI インジェクション(Server-side Include)を使用されると、パスワードの抜き取りやフィッシング詐欺サイトへの誘導のおそれがある。	・外部から入力されたデータをそのまま使用してSSI箇所を処理する。	・外部から入力（入力フォーム、URLパラメータ、Cookie、ヘッダパラメータ等による入力）されたデータを使用してコードを生成する際は、SSI インジェクション対策を実装する。	---> 前レベルと同様	・SSIは使用しない。			A.10.4.1 A.12.2.1	Web Application Security Consortium http://www.webappsec.org/
19			不正スクリプトの実行を防止する	不正なスクリプトが実行されると、Webサイトからの情報漏えい、改ざん等のおそれがある。	・利用者からアップロードされたファイルの内容を検証しない。	・利用者からアップロードされたスクリプトを実行させない。	・アップロード可能な拡張子を制限する。	・アップロードされたファイルをバイナリレベルで評価し、不正なデータを排除する。			A.10.4.1 A.12.2.1	Web Application Security Consortium http://www.webappsec.org/
20		Webサーバの設定	ディレクトリのファイル一覧表示を防止する	ディレクトリのファイル一覧表示がむやみに許可されていると、攻撃者にWebサイト攻撃のための情報を提供することになるおそれがある。また、セキュリティモラルの低いWebサイトとみなされ、攻撃対象にされるおそれがある。（ディレクトリ・リスティングと同じ[*]）	・ディレクトリ内のファイル一覧表示を許可する。	・ディレクトリ内のファイル一覧表示を許可しない。	・プログラムやHTMLファイルを配置しないディレクトリには、index.html等の名称で、空のファイルを配置する。	---> 前レベルと同様			A.10.7.3 A.12.4	Web Application Security Consortium http://www.webappsec.org/
21			パスの乗り換えを防止する	パスの乗り換えを使用されると、第三者への情報漏えいのおそれがある。	・ドキュメントルートの外に存在するファイルを表示する。	・URLに「..」等の不正な文字列を入力しても削除や置換を行い、不正なパスの切り替えを実施させない。	・既定以上のディレクトリ階層のファイルへのアクセスをアプリケーションの設定で禁止する。	---> 前レベルと同様			A.12.4	Web Application Security Consortium http://www.webappsec.org/
22			Webサーバ上のアプリケーションが特定されるのを防止する	Webサーバ上のアプリケーションが特定されると、種類やバージョン情報から有効な攻撃方法が特定されるおそれがある。	・Webサーバの種類、バージョンを公開する。	---> 前レベルと同様	・Webサーバの種類、バージョンを公開しない。	---> 前レベルと同様			A.10.7.3	Web Application Security Consortium http://www.webappsec.org/
23		アプリケーションのディレクトリ構成	リソースの位置を推測不可能にする	リソースが推測可能になっていると、第三者への情報漏えいのおそれがある。	・推測しやすい名称のファイルやフォルダをドキュメントルート直下に配置する。	・ドキュメントルート直下にAdminのような推測しやすい名称で、管理者用ページを含んだフォルダを配置しない。 ・管理者用ページのパスのように、重要なファイルのパスを含んだ robots.txt を置かない。	・ドキュメントルート直下に、推測しやすい名称のファイルやフォルダを配置しない。 ・robots.txt は配置しない。 ・コンテンツのバックアップとして、.bakや.oldの拡張子でファイルを保存しない。	・ハッカーがよく狙う推測可能なリソース（例：robots.txt)を配置し、アクセスログをとる。				Web Application Security Consortium http://www.webappsec.org/
24		バックアップファイルの取扱い	バックアップファイル等、サーバ上のデータの情報漏えいを防止する	サーバ上のデータが情報漏えいすると、そのシステムを悪用する足掛かりを攻撃者に提供するおそれがある。（「強制ブラウジング」を含む）	・サーバ内にファイルを自由に配置する。	・データベースのダンプファイルやコンテンツのバックアップなど、Webサイトの解析を行う足がかりとなる情報や、個人情報などの重要な情報は、ドキュメントルート下に置かない。	・重要か否かに拘らず、コンテンツ表示に使用しないファイルは一切置かない。 ・コンテンツで参照するデータファイルも外部から直接リンクを張る必要が無い場合は、ドキュメントルート以外に置いて外部から参照させない。	・重要な情報は、一度に多数の情報が閲覧できる一覧表示やCSVファイル出力などは行わない。			A.10.7.3	
25		アプリケーションの欠陥	アプリケーション機能の悪用を防止する	アプリケーション機能が悪用されると、第三者への情報漏えい、改ざん、迷惑メールの踏み台等のおそれがある。	・機能を自由に使用できる。	・Webサイト内検索機能を利用しても、公開を意図しないファイルにはアクセスさせない。 ・ファイルをアップロードする機能を利用しても、内部のファイルを置き換えさせない。 ・Webサイト上のメールの入力フォームを利用しても、迷惑メールを送らせない。	---> 前レベルと同様	・アップロードされたファイルはディレクトリ上に保管せず、所定の検証手続きを済ませた上でデータベース上に保管する。			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
26			瞬間的なアクセス過多などによるサービス提供不能を防止する	サービス拒否(DoS/DDoS)を実行されると、Web サーバが利用者へ提供するサービスを妨害されるおそれがある。	・全てのリクエストを受け付ける。	想定しうる連続したリクエストを受信した場合でも、耐えることができることを確認する。	・DoS対策機能を持ったファイアウォール、ルータ等の導入もしくは、DoS対策専用機器を導入して対策を講じる。 ・アプライアンスの導入が困難な場合は、OSレベルまたはWebサーバの拡張機能を使用して対策を講じる。	・DoS/DDoS攻撃対策を専門業者に委託し導入する。			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
27			自動反復プログラムによる不正行為を防止する	利用者の作業を自動化するプログラムによる入力を制御する仕組みを用意しないと、不当に大量の会員登録を行われる等のおそれがある。	・登録フォームに必要情報を入力後、確認画面を表示した後に登録を完了させる。	・登録時は、直接登録完了を行わず、登録したメールアドレスに登録完了画面のURLを送信し、登録を完了させる。	---> 前レベルと同様	・入力フォームにはCaptchaを使用する。			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
28			プロセスを検証する	プロセス検証が不適切だと、第三者が利用者（会員等）に成りすます等のおそれがある。	・プロセスを確認しない。	・複数の画面を、決められた順番に進めていくプロセスにおいて、順番通りのステップを経てプロセスを進めているかを確認する。	---> 前レベルと同様	---> 前レベルと同様			A.12.2.2	Web Application Security Consortium http://www.webappsec.org/
29		ネットワーク構成	データベースサーバへの攻撃を防止する	データベース（DB）サーバが攻撃されると、DBサーバからの情報漏えい、改ざん等のおそれがある。	・WebサーバとDBサーバを同一サーバに置く。 ・Webアプリケーションからの DBサーバへのアクセスを制限しない。	・WebサーバとDBサーバを同一サーバに置く。 ・Webアプリケーションからの DBサーバへのアクセス権は一般ユーザ権限とする。（管理者権限にしない）	・DBサーバとWebサーバを物理的に別々のサーバに配置する。 ・Webアプリケーションからの DBサーバへのアクセス権は一般ユーザ権限とする。（管理者権限にしない） ・DBサーバはWebサーバ以外からのアクセスが不可能な、ローカルエリア上に配置する。	・機密情報は、DBへの登録内容を全て暗号化し、参照する利用者に応じて復号化して提供する。 ・DBに対して送られたSQL文は全てログとして収集し、DBサーバとは別サーバに保存する。			A.11.4.6	
30			Webサーバの配置場所を検討する	Webサーバが攻撃を受けると、Webサーバの改ざん等のおそれがある。	・Webサーバをそのままインターネット上に公開する。	・Webサーバはファイアウォールを経由して公開する。	・Webサーバは、リバースプロキシや不可分散装置等の一次アクセス受付サーバと、アプリケーション実行用サーバに分割する。 ・一次アクセス受付サーバのみ、外部ネットワークからのリクエストを受け付ける。	・WebサーバはWAFを経由して公開する。			A.11.4.6	
31		情報の交換	業務用情報システムへの不正なアクセスを防止する	業務用情報システムへ不正にアクセスされると、情報の改ざんや漏えいなどのおそれがある。	・認証に関するルールを定めない。	・認証の再試行可能回数を定める。 ・再試行可能回数を超えて認証が失敗した場合は、二十四時間当該アカウントを停止する。 ・認証情報はセッションまたはCookieに保存する。 ・ログインID/パスワード等の認証情報をCookie上に暗号化せずに保存する。	・認証画面(機能)を使用して、コンピュータとアプリケーションを利用する。 ・一定回数以上ログオンに失敗したアカウントは、ロックアウトする。 ・パスワードの定期的な変更を、システム機能により強制する。 ・パスワードを他人から推測されにくいものにすることを、システム機能により強制する。 ・パスワードをシステム内に保存する場合は、暗号化する。 ・パスワードをコンピュータ間で通信する場合は、暗号化する。	・認証のログを採取する。 ・ログインID/パスワードはセッション上に保存せず、利用者をシステム側で管理する一意な文字列をセッションに保存する。			A.10.8.5	
32		電子商取引サービス	取引内容を第三者から保護し、当事者間だけの情報とすることを規定する	コンピュータ間でやりとりされる情報を保護しないと、取引の内容が漏えい、改ざんされるおそれがある。	・データを暗号化しない。	・取引情報を入力する画面はSSLによって暗号化し、入力した取引情報もSSLによって暗号化する。 ・SSL認証は、電子証明書を使ったサーバ認証を行い、利用者はID/パスワードを使用して認証する。 ・取引結果についてはメールにて双方に通知する。	・取引情報を入力する画面データはSSLによって暗号化し、入力した取引情報もSSLによって暗号化する。 ・SSL認証は電子証明書を使ったサーバ認証を行い、利用者はID/パスワードを使用して認証する。 ・取引結果についてはメールにて双方に通知のみを行い、閲覧用のURLから取引結果を確認する。	・利用者のSSL認証はID/パスワードだけではなく、電子証明書を使用して個人認証する。 ・高額取引や原本性を重んじる商取引では、電子署名を使用して電子商取引の内容を保証する。			A.10.9.1	
33			オンラインで取引する	コンピュータ間でやりとりされる情報を保護しないと、取引の内容が漏えい、改ざんされるおそれがある。	・データを暗号化しない。	・取引情報を入力する画面はSSLによって暗号化し、入力した取引情報もSSLによって暗号化する。 ・SSL認証は、電子証明書を使ったサーバ認証を行い、利用者はID/パスワードを使用して認証する。 ・取引結果についてはメールにて双方に通知する。	・取引情報を入力する画面データはSSLによって暗号化し、入力した取引情報もSSLによって暗号化する。 ・SSL認証は電子証明書を使ったサーバ認証を行い、利用者はID/パスワードを使用して認証する。 ・取引結果についてはメールにて双方に通知のみを行い、閲覧用のURLから取引結果を確認する。	・利用者のSSL認証はID/パスワードだけではなく、電子証明書を使用して個人認証する。 ・高額取引や原本性を重んじる商取引では、電子署名を使用して電子商取引の内容を保証する。			A.10.9.2	
34			公開されている情報の改ざんを防止する	価格や情報等、Webサイト上に掲載される情報が改ざんされ、不正に利用される可能性がある。	・情報を確認しない。	・公開前の情報について、内容に誤りがないかを目視で確認する。	・公開された情報に誤りがないことを目視で確認する。	・改ざんを検出するシステムを使用し、情報の改ざんを監視する。 ・改ざんを検出した場合は管理者に連絡する。 ・情報の更新ログを取得する。			A.10.9.3	

Webアプリケーション セキュリティ・可用性チェックシート（詳細項目版）

	要素	分類	対策項目	リスクの詳細	推奨レベル レベル1	レベル2	レベル3	レベル4	本件業務のセキュリティ仕様 該当レベル	対策仕様	JISQ項番	参考文献（JIS Q 27002：2006以外）
35		ログの収集と解析	監査ログを取得する	情報システムの適切な監査ログを記録しないと、発生した不正な活動に気づく事ができないおそれがある。	・ログを取得しない。	・情報システムのアクセスログを取得する。 ・アクセスログを、定期的に点検する。 ・アカウントによるログオンイベント（ローカル）を記録する。(成功) ・アカウントへの変更(管理作業)を記録する。(成功) ・アカウントまたはパスワードのポリシー変更を記録する。(成功) ・システムに影響のあるイベントを記録する。(成功)	・アカウントによるログオンイベント（ネットワーク、ドメイン、ローカル）を記録する。(成功)	・アカウントによるログオンイベント（ネットワーク、ドメイン、ローカル）を記録する。(成功/失敗) ・アカウントへの管理作業を記録する。(成功/失敗) ・アカウントまたはパスワードのポリシー変更を記録する。(成功/失敗) ・システムに影響のあるイベントを記録する。(成功) ・オブジェクト(ファイル等)へのアクセスを記録する 。(失敗) ・特権の使用を記録する。(失敗)			A.10.10.1	
36			ログ情報を保護する	取得したログ情報を保護しないと、内容の改ざんやログが破棄されるおそれがある。	・ログを取得しない。	・情報システムのログのバックアップを、 オフラインで定期的に取得する。 ・情報システムのログにアクセス可能なアカウントを制限する。 ・ログの記録漏れ、上書き等が発生しないよう、十分な記憶容量を確保する ・ログの削除が行われた事をログに記録する。	・オペレーティングシステムまたは、アプリケーションの機能により、適切なログの保護措置をとる。 ・ディスク等の容量不足などにより、ログが記録できない場合は、システムを停止する。 ・ログのオフラインでのバックアップは、十分な期間に遡って参照可能にする。	・ログを短いサイクルで、別の情報システムにオンラインでコピーまたは移動する。			A.10.10.3	
37			障害のログを取得する	障害ログを取得しないと、発生した事象に関して原因究明が困難になるおそれがある。	・ログを取得しない。	・情報システムの障害発生を記録する。	・記録された障害毎に、明確な対応策または運用規則を定める。 ・対応策が決められていない場合の、運用規則を定め	・情報システムで障害が発生した場合は、システム管理者に通知する。			A.10.10.5	
38		Webアプリケーション開発	プログラムに関するコーディング規約を定義する	開発者間で共通したプログラミングに関するコーディング規約がないと、品質と保守性に問題があるシステムになるおそれがある。	・コーディング規約を設けない。 ・単独の担当者でシステムを開発する。	・コーディング規約を定めるが文書化しない。	・コーディング規約を正式に規定し、文書化する。 ・コーディング規約を担当者に周知する。	・プログラムがコーディング規約に準拠しているかを専用のツールを使用してチェックする。				
39			プログラムを作るにあたって守らなければならないセキュリティ方針を策定する	セキュリティ指針を策定していないと、属人的なセキュリティ意識に基づいたプログラミングを行うことになるため、品質とセキュリティ性に問題があるシステムになるおそれがある。	・セキュリティ指針を策定しない。	・セキュリティ指針を策定し、教育を実施する。 ・セキュリティ指針を定期的に見直す。	・社外の作業者に対して、社内と同様の教育を実施する。	・セキュリティ教育の浸透状況を監査する。				
40			プログラム作成後、セキュリティの問題点が無いことをチェックする	セキュリティテストを実施していないと、セキュリティ指針が周知徹底されていた場合でもぜい弱性を含んだシステムになるおそれがある。	・セキュリティテストを実施しない。	・開発者本人による属人的なセキュリティテストを実施する。	・セキュリティテストについての明確な枠組みを作り、テストプロセスに組み込む。	・セキュリティテストは、開発者ではなくテスト専門の担当者が実施する。				
41	情報が事実と等しい（完全性保証）	原本性保証	データがネットワーク上で改ざんされていないことを保障する	データが完全性を保証できないと、メッセージなどの情報が改ざんされて業務を混乱させるおそれがある。	・送信、受信されたデータの整合性を確認しない。	・SSL認証を行い、メッセージを暗号化することで、メッセージの完全性を保証する。 ・SSL認証は電子証明書を使ったサーバ認証を実施し、利用者側はID/パスワードを使用した認証を実施する。	・クライアント側のSSL認証は、ID/パスワードだけではなく、電子証明書を使用した個人認証を実施する。	・電子署名を使用して、送受信メッセージの完全性を保証する。 ・金融、証券など、署名の日時に重要性がある場合は、タイムスタンプつきの電子署名を利用する。			A.12.2.3	
42		監査	情報システムを監査する	情報システムを定期的に監査しないと、不正の検出ができなく、情報漏えいを見逃すおそれがある。	・内部監査を実施しない。	・定期的な個人による監査を実施する。	・監視計画と監視実績に基づいた、監査を実施する。 ・監査については、定期的に社内組織に委託する。	・監視計画と監視実績に基づいた、監査を実施する。 ・監査については、定期的に第三者組織に委託する。			A.15.3	
43	システムを稼働し続ける（可用性保証）	冗長化	サーバを冗長化構成にする	サーバが障害などで停止してしまうと、利用者に提供しているサービスが停止してしまうおそれがある。	・サーバの障害時に、サーバが復旧するまでサービスが停止する。	・Webサーバ及びDBサーバを二重化する。 ・サーバの障害時に、サービスが数十分～数時間の停止後、復旧できるようなシステム構造にする。	・Webサーバ及びDBサーバを二重化する。 ・サーバの障害時に、サービスが数分～数十分の停止後、復旧できるようなシステム構造にする。	・Webサーバ及びDBサーバを二重化する。 ・一部のサーバに障害が発生しても、サービスは停止しないシステム構造とする。				
44			ネットワーク経路を冗長化構成にする	サーバまでのネットワーク経路が遮断されると、利用者に提供しているサービスが停止してしまうおそれがある。	・ネットワーク障害時に、ネットワークが復旧するまでサービスが停止する。	・ネットワーク経路を二重化する。 ・ネットワーク障害時に、サービスが数十分～数時間の停止後、復旧できるようなシステム構造とする。	・ネットワーク経路を二重化する。 ・ネットワーク障害時に、サービスが数分～数十分の停止後、復旧できるようなシステム構造とする。	・ネットワーク経路を二重化する。 ・一部のネットワークに障害が発生しても、サービスは停止しないシステム構造とする。			A.10.6	
45			データを冗長化構成にする	サーバのデータが消失すると、利用者に提供しているサービスが停止するおそれがある。	・データクラッシュ時に、データを復旧するまでサービスが停止する。	・データを二重化する。 ・データクラッシュ時に、サービスが数十分～数時間の停止後、復旧できるようなシステム構造とする。	・データを二重化する。 ・データクラッシュ時に、サービスが数分～数十分の停止後、復旧できるようなシステム構造とする。	・データを二重化する。 ・一部のデータがクラッシュしても、サービスは停止しないようなシステム構造となする。				
46		負荷分散装置の設置	サーバ負荷の設計と分散方式を検討する	サーバが過負荷になると、アプリケーションの停止や、ぜい弱性を原因とする情報漏えいのおそれがある。	・負荷を考慮しない。	・データを二重化する。	・サーバや負荷分散装置を二重化し、耐障害性を高める。	・負荷分散対象サーバを仮想化やクラスタ化し、より大規模な負荷を想定した構成とする。				
47		容量管理・拡張性	サーバの容量や能力を管理する	情報システムの能力が不足すると、情報システムが利用できなくなるおそれがある。	・情報システムの容量監視をしない。	・ディスク容量や処理能力等について、利用者やデータの伸びに対し、一定期間対応可能な情報システムにする。	・情報システムの拡張が、容易なシステムにする。	・情報システムの稼働能力を監視する。 ・情報システムの容量の増強を計画的に実施する。 ・情報システムの容量の増強が容易なシステムにする。			A.10.3.1	
48		保守運用	アプリケーションを保守する	アプリケーションの不具合やぜい弱性を放置しておくと、情報漏えいが発生するおそれがある。	・アプリケーションを保守しない。	・アプリケーションに関する保守や監視を、他業務を兼務する従業員が実施する。	・アプリケーションの保守は専任の情報システム担当者が行う。 ・アプリケーションの監視（特に死活監視）を実施する。 ・アプリケーションに関する不具合やぜい弱性の情報を管理し、計画的に対策する。	・保守作業は事前に保守計画を明らかにし、保守計画に沿った作業のみを実施する。 ・事前に申請のない保守作業は一切禁止する。 ・保守作業の内容は履歴に残す。 ・作業内容の履歴は、管理者であっても変更や削除が不可能な方法で保存する。 ・緊急時の対応について事前に手順を明らかにし、操作手順に沿って作業を実施し、作業履歴は漏れなく保存する。				
49			アプリケーションを更新する	アプリケーションの更新を計画的に実施しないと、ぜい弱性が混入するおそれがある。	・アプリケーションの更新は、動作検証しない。	・アプリケーションの更新は、擬似環境上で問題がないことを確認した上で実施する。	・更新箇所の履歴を管理する。 ・更新にはメンテナンス期間を設け、更新による不具合が本番環境で発生しないことを確認する。	・本番環境上で、メンテナンス期間中に退行テストもあわせて実施する。				
50			アプリケーションのバージョンを管理する	アプリケーションに不具合が発覚した際に、問題の無いバージョンに速やかに退行することが出来ないと、改修が完了するまでの間、アプリケーションの停止またはぜい弱性を抱えたままの運用をしなくてはならないおそれがある	・アプリケーションのバージョンを管理しない。	・アプリケーションのバージョン管理は、旧バージョンのバックアップファイルを残すことでバージョン管理とする。	・アプリケーションのバージョン管理は、バージョン管理ソフトウェアもしくは台帳を使用して管理する。	・アプリケーションの更新を行う際は、関連するプログラム一式を書庫ファイルに整理し、不具合発生時には関連するプログラム一式を速やかに退行できるようにする。				