株式会社マーズフラッグ

MARS FLAG Corporation.

セキュリティ対策実施項目 Security countermeasure implementation items.

最終更新 (Last update) 2019/08/23

1 サーバ本体に関するセキュリティ対策 Security measures concerning the server body.

No	対策分類	実施項目	Classification of measures	Action Item
1-1	サーバ設置について	サーバおよびルータは、情報セキュリティ担当者以外の第三者による物理的なアクセスを制限するため、執務室から隔離されたサーバルームに設置する。	About server installation	To ensure that servers and routers can not be accessed physically except by information security officers, they should be installed in a server room isolated from the office.
		サーバルームは常時施錠する。		The server room must be locked.
		サーバルームへの入退室記録を行う。 記録する内容は以下とする。 1. 入退室日時 2. 入退室者名（委託先など社外の者の場合、社名を含む） 3. 入退室の目的		Record entry and exit from the server room. The contents to be recorded are as follows: 1. Date and time of entry and exit 2. Name of entry / exit person (In the case of a person outside the company such as a consignee, include company name) 3. Purpose of entry / exit
1-2	サーバの構成について	サーバおよびネットワークの構成管理を行う。 構成を変更した場合は、必ずアップデートを実施する。	About server configuration	Manage server and network configuration. If you change the configuration, be sure to update it.
1-3	サーバへのアクセス	外部記録媒体を利用する場合には、ウイルスやワーム等の感染防止のため、利用する直前にフォーマットを実施する。	Access to server	When using external recording media, format it in advance to prevent infection of viruses, worms and so on.
1-4	監視	サービス停止許容時間を考慮し、必要に応じて24時間365日のサーバの死活監視、リソース(CPU、メモリ等)の、運用監視の仕組みを施す。	Monitoring	Take into consideration the service suspension allowance time, if necessary, to monitor the life-and-death of the server 24 hours a day, 365 days, to provide a mechanism of operation monitoring of resources (CPU, memory, etc.).
1-5	冗長化	障害時を考慮したストレージやサーバの冗長化、サービス停止許容時間を考慮したバックアップ構成を必要に応じて施す。	Redundancy	Considering the time of failure, taking into consideration service allowable time such as making storage and servers redundant, apply backup configuration as necessary.
1-6	入退管理	オンプレミスの場合、サーバ設置場所には認証による入退管理システムを設け、入退を許可したユーザのみが入れる仕組みを施す。 IaaS等クラウドの場合、情報セキュリティ責任者が許可したアカウントのみが操作を行える仕組みを施す。	Entry and exit management	In the case of on-premises, establish an entry and exit management system by authentication at the server installation location, and implement a mechanism that lets enter only users allowed to. In the case of cloud services such as IaaS, it is necessary to implement a mechanism by which only the account permitted by the information security officer can operate.
		オンプレミスの場合、サーバ設置場所への入退管理ログを取得する仕組みを施す。 IaaS等クラウドの場合、操作ログを取得する仕組みを施す。		In the case of on-premises, implement a mechanism to acquire entry and exit management logs to the server installation location. In the case of IaaS etc. cloud services, apply a mechanism to acquire the operation log.
		入退管理ログや操作ログは、必要に応じて監査できる仕組みを施す。		Apply a mechanism that allows confirmation of entry and exit management logs and operation logs as necessary.
		年1回以上、入退管理システムに登録されているユーザおよび、IaaS操作アカウントの棚卸しを実施する。		At least once a year, carry out the inventory of the users registered in the entry and exit management system and the IaaS operation accounts.
1-7	監視	オンプレミスの場合、サーバ設置場所あるいは出入口に監視カメラを設置、監視する。	Monitoring	In the case of on-premises, install surveillance cameras at the server installation place or entrance and monitor them.

2 プラットフォームに関するセキュリティ対策 Platform security measures.

No	対策分類	実施項目	Classification of measures	Action Item
2-1	サービスやポート	不要なサービスは停止、もしくは削除する。	Service and port	Stop or delete unnecessary services.
		サービスを提供していないネットワークポートへの接続要求には、応答を返さない仕組みを施す。		Apply a mechanism that does not return a response to a connection request to a network port that does not provide a service.
		年1回以上、サーバの脆弱性診断を実施する。 構成に変更があった場合は、脆弱性診断を必要に応じて実施する。		At the very least, implement vulnerability assessment of servers once a year. When there is a change in the configuration, vulnerability diagnosis should be carried out as necessary.
2-2	サーバを管理(操作)するアカウントの管理	システムアカウントの初期パスワードは使用しない。 構築時のみ使用するアカウントなど、使用していない不要アカウントの削除を徹底する。	Server administering (operative) accounts management	Do not use the system account default password. Be sure to delete unnecessary accounts, such as accounts used only at configuration time.
		サーバへ物理的に接続する際は、離席時にスクリーンロックをかける。また、操作終了時には必ずログアウトを行う。 サーバへリモート接続する際は、一定時間操作していない時にスクリーンロックをかける。また、操作終了時には必ずログアウトを行う。		When you are physically connected to the server, lock the screen when you leave the office and be sure to logout at the end of the operation. When remotely connecting to the server, lock the screen when not operating for a certain period of time. Be sure to log out at the end of the operation.
		サーバのシェル操作アカウントには特権を付与せず、特権を要する操作を行う場合は必ずsudoを用いて操作を行う。		Do not give special privileges to accounts for the server operations, always use sudo to perform operations requiring special privileges.
		管理権限を有するアカウントは、申請のあった利用者にのみ発行する。 申請にあたってはシステムごとにルールを作成し、証跡を残すようにする。ルールの策定はサイト運営部署内にて決定する。 また、外部委託する場合は、セキュリティ対策を考慮した運用ルールであることが確認できれば、委託先業者の運用ルールに任せる。 申請書には以下を明記する。 - 利用システム - 申請日時 - 対象者名（委託先業者の場合は業者名も明記する） - 権限付与の目的 - 権限の適用期間(○年○月○日～○年○月○日) - 情報セキュリティ責任者または、サイト管理者の署名		Account with administrative authority should be issued only to the user who applied for it. Regarding the application, create rules for each system and leave trace. Formulation of rules is decided within the site operation department. Also, in the case of outsourcing, if it can be confirmed that it is a contractor observing security measures, it is left to the operation rules of the contractor. State the following in the application form. - System used - Application date and time - Person name (In the case of a contractor, also specify the name of it) - Purpose of authorization - Period of authorization (○ year ○ month ○ day ～ ○ year, month · day ○ day) - Signature of information security officer or site administrator
		年1回以上、アカウントの棚卸しを実施する。		Perform inventory of accounts at least once a year.
		アカウントに設定するパスワードは「大文字英字」「小文字英字」「10進数基数」「英数字以外の記号」のうち、3つ以上の要素を含む8文字以上に設定する。		The password for the account is to be set to 8 or more characters including three or more elements among "upper case letters", "lower case letters", "decimal numbers", "non-alphameric characters".
		認証を一定回数失敗した場合は、一時的に当該接続元からの通信を制限し、管理者による制限解除を実施する仕組みを施す。		When authentication fails for a certain number of times, temporarily restrict communication from the connection source, and implement a system for cancelling the restriction by the administrator.
		サーバをリモートから操作する際は、パスワード認証以外の認証方法（公開鍵認証方式）を利用する。		When operating the server remotely, use an authentication method (public key authentication method) other than password one.
2-3	サーバへのアクセス制御	アカウントの役割に応じて、必要な権限を付与し、適切なアクセスコントロールを実施する。 サーバをリモートから操作する際は、端末のIPアドレス等により操作可能な端末を制限する。	Controlling Access to the Server	Grant necessary authority according to the role of account and implement appropriate access control. When operating the server remotely, terminals that can be operated are limited by the IP address of the terminal or the like.
		定期的にアクセス制御ログを確認できる仕組みを施す。		Apply a mechanism to check the access control log regularly.
		年1回以上、アクセス制御の見直しを実施する。		Review the access control at least once a year.
2-4	監査機能	NTPサーバから正確な時刻を同期する。	Audit function	Synchronize the correct time from the NTP server.
		OS、各種ソフトウェアのログイン成功、失敗のログ、イベント／システムログを取得する。		Retrive OS, various software login success and failure logs, event/system logs.
		5W1H「いつ、（When）、どこで（Where）、誰が（Who）、何を（What）、なぜ（Why）、どのように（How）」を含むログを出力する。		5W1H To output a log containing "when, where, who, who, what, why, how."
		一定期間のログをサーバ上に保存する仕組みを施す。		Apply a mechanism to save logs over a certain period on the server.
		サーバ上に保存されたログは定期的に外部ストレージへ複製し、保管する。		Logs saved on the server should be periodically duplicated to external storage and stored.
		脆弱性のあるソフトウェアの使用やサーバ管理状況を定期的に確認する。		Periodically check the use of vulnerable software and server management status.
2-5	各種ソフトウェア	既知の脆弱性や不具合に対策の施されたパッチを適用する。 パッチ適用に動作確認が必要な場合は、動作確認終了後、即時に適用する。 パッチ適用が不可能な場合には代替案を適用する。	Various software	Apply patches for known vulnerabilities or defects. If an operation check is required for the patch, apply the patch immediately after the end of operation check. If a patch application is impossible, apply alternative solutions.
2-7	DNS	ドメイン名およびDNSレコードの登録状況を把握した上で、登録状況に不整合がある場合はドメイン登録情報を更新する。	DNS	After grasping the registration status of the domain name and the DNS record, update the domain registration information if the registration status is inconsistent.
2-8	バックアップ	システム構築時のイメージバックアップを用意する。 構成に変更が生じた場合など、必要に応じてイメージバックアップの更新を行なう。 バックアップを取得する際は、以下を考慮する。 - 適切な世代管理 - 分散保管、遠隔地保管等の保管方法	Backup	Prepare image backup during system configuration and building. Update image backups as necessary, such as when configuration changes occur. When acquiring a backup, consider the following. - Appropriate generation management - Storage method for distributed storage, remote storage etc.
2-9	性能設計	過負荷の状況において、システム上の期待する応答時間内にHTTPレスポンスが返るよう性能設計を行なう。	Performance design	Adopt performance design so that HTTP response is returned within the expected response time on the system even under a heavy load condition.

2-10	アクセス制御	アクセス制御ログは、「警告」「注意」「情報」などのレベルを設定し、必要に応じて確認できるようにする。	Access control	Concernig access control log, set levels such as "warning", "attention", "information", etc. so that it can be checked as necessary.
2-11	監査機能	SIEM(セキュリティ情報イベント管理)が可能な、ログの一元管理をする仕組みを施す。	Audit function	We provide a mechanism for centralized log management that enables SIEM (security information event management).
		収集したログは、必要に応じて確認できるようにする。		Make it possible to check the collected logs when necessary.
2-12	暗号化	ネットワーク上にパスワード等の重要情報が平文で流れるプロトコルは利用しない。	Encryption	Do not use protocols where important information such as passwords flows in plaintext on the network.

3 Webアプリケーション（全般）に関するセキュリティ対策 Security measures for web applications (general).

No	対策分類	実施項目	Classification of measures	Action Item
3-1	サーバを管理(操作)するアカウントの管理	管理者には、管理権限を有するアカウントと一般権限を有するアカウントを発行し、利用者には、一般権限を有するアカウントを発行する。 管理者においては、管理業務以外は一般権限を有するアカウントで操作を行うようにする。 同一のアカウントを複数の利用者で共用する事は禁止する。	Server administering (operative) accounts management	Issue to the administrator an account with administrative privileges and one with general privileges, and issue to the user an account with general privileges. The administrator operate with an account having general authority for tasks other than the administrative ones. Sharing the same account among multiple users is prohibited.
		原則としてアカウントの共用は禁止とするが、当該利用者に使用を認められ、かつ情報セキュリティ責任者の承認を得た場合に限り、アカウントの共用を許可する。 アカウントの共用にあたっては利用簿を作成して管理する。また、外部委託する場合は、セキュリティ対策を考慮した運用ルールであることが確認できれば、委託先業者の運用ルールに任せる。 利用簿には以下を明記する。 - 利用システム - 申請日時 - 対象者名（委託先業者の場合は業者名も明記する） - 利用するアカウント - アカウントの共用目的 - 利用期間(○年○月○日～○年○月○日) - 情報セキュリティ責任者の署名	Sharing the same account among multiple users is prohibited in principle, but it is permitted only for determined personnel or approved ones by the information security officer. When sharing accounts, manage them using a register. Also, in the case of outsourcing, if it can be confirmed that it is a contractor observing security measures, it is left to the operation rules of the contractor. Write the following in the use register. - System used - Application date and time - Person name (In the case of a contractor, also specify the name of it) - Account to use - Account sharing purpose - Period of use (○ year ○ month ○ day ～ ○ year · month month ○ day) - Signature of information security officer
		管理権限を有するアカウントは、申請のあった利用者にのみ発行するようにする。 申請にあたってはシステムごとにルールを作成し、証跡を残すようにする。ルールの策定はサイト運営部署内にて決定する。 また、外部委託する場合は、セキュリティ対策を考慮した運用ルールであることが確認できれば、委託先業者の運用ルールに任せる。 申請書には以下を明記する。 - 利用システム - 申請日時 - 対象者名（委託先業者の場合は業者名も明記する） - 権限付与の目的 - 権限の適用期間(○年○月○日～○年○月○日) - 情報セキュリティ責任者または、サイト管理者の署名	Accounts with administrative authority should be issued only to the user who applied for it. In applying, we create rules for each system and leave trail. Formulation of rules is decided within the site operation department. Also, in the case of outsourcing, if it can be confirmed that it is a contractor observing security measures, it is left to the operation rules of the contractor. State the following in the application form. - System used - Application date and time - Person name (In the case of a contractor, also specify the name of it) - Purpose of authorization - Period of authorization (○ year ○ month ○ day ～ ○ year, month · day ○ day) - Signature of information security officer or site administrator
		年1回以上、アカウントの棚卸しを行う。		Perform inventory of accounts at least once a year.
		アカウントに設定するパスワードは「大文字英字」「小文字英字」「10進数基数」「英数字以外の記号」のうち、3つ以上の要素を含む8文字以上に設定する。		The password for the account is to be set to 8 or more characters including three or more elements among "upper case letters", "lower case letters", "decimal numbers", "non-alphameric characters".
		パスワード認証で一定回数失敗した場合は、当該アカウントを一時的に使用不可にし、管理者による使用不可解除を実施する仕組みを施す。		If the password fails for a certain number of times, temporarily disable the account, and implement a mechanism such as unlocking the unusability by the administrator.
		サーバをリモートから操作する際は、パスワード認証以外の認証方法（公開鍵認証方式）を利用する。		When operating the server remotely, use an authentication method (public key authentication method) other than password authentication.
3-2	アクセス制御	アカウントの役割に応じて、必要な権限を付与し、適切なアクセスコントロールを実施する。 サーバをリモートから操作する際は、端末のIPアドレス等により操作可能な端末を制限する。	Access control	Grant necessary authority according to the role of account and implement appropriate access control. When operating the server remotely, terminals that can be operated are limited by the IP address of the terminal or the like.
		定期的にアクセス制御ログを確認できる仕組みを施す。		Apply a mechanism to check the access control log regularly.
		年1回以上、アクセス制御の見直しを実施する。		We review the access control at least once a year.
3-3	監査	アプリケーションのアクセスログを取得する。	Audit	Acquire the access log of the application.
3-4	検査	アプリケーション開発時に脆弱性診断を実施し、リリース以降は、アプリケーションに対する脆弱性診断を年1回以上実施する。 アプリケーションを修正した場合は、必要に応じて脆弱性診断を実施する。	Inspection	We conduct vulnerability diagnosis at application development and conduct vulnerability diagnosis for applications at least once a year. We also conduct vulnerability diagnosis when necessary, such as when making modifications to the application.
3-5	バックアップ	アプリケーションおよびサービスに不具合が生じた際の復旧に必要なデータのバックアップを行う。 また、復旧手順を定義する。 バックアップを取得する際は、以下を考慮する。 - 適切な世代管理 - 分散保管、遠隔地保管等の保管方法	Backup	Back up data necessary for recovery in case of malfunction of applications and services. Also define the recovery procedure. When acquiring a backup, consider the following. - Appropriate generation management - Storage method for distributed storage, remote storage etc.
3-6	改ざん対策	本番環境へのプログラム登録、抹消等は、必要な手順を定め管理する。	Tampering countermeasures	Estabilish and manage necessary procedures for program registration, deletion, etc. in the production environment.
		開発中または修正中のプログラムファイルと本番プログラムファイルは、分離して管理する。		Separate the management of program files under development or modification from the production ones.
		Webサイトの本番環境には、実行可能なWebアプリケーションのモジュールだけを保持する。		In the production environment of the Web site, only modules of executable Web applications are held.
3-7	サーバ上でWebアプリケーションを管理(操作)するアカウント管理	アカウントのログイン、ログアウトを監視し、特定のアカウントに対する大量のログイン失敗など、不正なアクセスを検知し、アラートを上げる仕組みを施す。	Server web applications administering (operative) accounts management	Perform a mechanism raising alerts, to monitor logins and logouts of accounts, to detect illegal accesses such as a large number of login failures to a specific account.
3-8	アクセス制御	アクセス制御ログや監査ログは、「警告」「注意」「情報」などのレベルを設定し、必要に応じて確認できるようにする。	Access control	Set access control log and audit log levels such as "warning", "attention", "information", etc. so that they can be checked as necessary.

4 Webアプリケーション（設計・プログラミング）に関するセキュリティ対策 Security measures concerning web application (design and programming).

No	対策分類	実施項目	Classification of measures	Action Item
4-1	クロスサイトスクリプティング対策	サニタイジング処理（入力データから、HTMLタグやSQL文を他の文字列に置き換え無害化する。以下同じ。)はHTML生成時に行う。	Cross site scripting countermeasures	The sanitizing process (replacing HTML tags and SQL statements with other character strings from input data, rendering it harmless, the same applies below) is done at the time of HTML generation.
		パラメータをHTMLの通常テキスト内に埋め込む場合は、サニタイジング処理を行う。		When parameters are embedded in normal HTML text, sanitizing process is performed.
		パラメータをHTMLのタグ属性値内に埋め込む場合は、サニタイジング処理を行い、タグ属性の値をダブルクォートまたはシングルクォートでくくる。		When embedding parameters in the HTML tag attribute value, sanitize them and enclose the value in double or single quotes the tag attribute value.
		パラメータをHTMLのURL属性値内に埋め込む場合は、URLが適切な文字で構成されているか(予期しない文字が含まれていないか)チェック後、サニタイジング処理を行い、タグ属性の値をダブルクォートまたはシングルクォートでくくる。 可能であれば、決められた値以外は入力できないようにする。		When embedding parameters in the HTML URL attribute value, after checking whether the URL is composed of appropriate characters (whether unexpected characters are included) or not, sanitize and enclose the tag attribute value in double or single quotes. If possible, make sure that you can not enter anything other than the specified value.
		データベースおよびファイルから読み込んだデータはサニタイジング処理を行う。		Sanitize the data read from database and file.
		相対パスを用いてURLを出力する場合は、スキーマ省略を考慮する。		When outputting URL using relative path, consider schema omission.
		パラメータをHTMLのイベントハンドラ属性値内に埋め込まない。		Do not embed parameters in HTML event handler attribute value.
		パラメータをHTMLのスクリプトエレメント内に埋め込まない。		Do not embed parameters in HTML script element.
		パラメータをHTMLのコメント内に埋め込まない。		Do not embed parameters in HTML comments.
		パラメータをHTMLのスタイルシート指定部分に埋め込まない。		Do not embed parameters in HTML style sheet specification part.
		利用者に対し、HTMLタグやJavaScriptを含む文字列の入力は許可しない。		Do not allow users to enter strings including HTML tags and JavaScript.
		URLを出力するときは、「http：//」や「https：//」で始まるURLのみを許可するようにする。		When outputting the URL, only URLs beginning with "http: //" or "https: //" are permitted.
		<script>…</script>要素の内容を動的に生成しないようにする。		Do not dynamically generate the content of <script> ... </ script> element.
		スタイルシートを外部サイトから取り込めるようにしない。		Do not allow style sheets to be imported from external sites.
		HTMLテキストの入力を許可する場合は、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。（HTMLテキストに対し、許可する要素を「ホワイトリスト方式」で抽出する。）		When inputting of HTML text is permitted, a parse tree is created from the input HTML text, and only the necessary elements, not including the script, are extracted. (For the HTML text, extract the permitted elements with "whitelist method".)
		HTTPレスポンスヘッダのContent-Typeフィールドに文字コード(charset)の指定を行なう。なおContent-Typeフィールドはコンテンツのファイルタイプと一致するものを返す。		Specify the character code (charset) in the Content-Type field of the HTTP response header. The Content-Type field shall return the one matching the file type of the content.
		レスポンスヘッダには、X-Content-Type-Options:nosniffを添付する。		Attach X-Content-Type-Options:nosniff to the response header.

		Cookie 情報の漏えい対策として、発行する Cookie に HttpOnly 属性を加え、TRACE メソッドを無効化する。		As a countermeasure against leakage of cookie information, add HttpOnly attribute to issuing cookie and invalidate TRACE method.
		クロスサイトスクリプティングに有効なブラウザの機能を設定するレスポンスヘッダを返す。（「X-XSS-Protection」や「Content Security Policy」等） （設定値例） - X-XSS-Protection: 1; mode=block ：XSSフィルタ機能がオンになり、XSS攻撃を検知し、実行させない。 - X-XSS-Protection: 0 ：XSSフィルタを無効にする。 - Content-Security-Policy: reflected-xss allow ：XSS攻撃のフィルタリングを無効にする。 - Content-Security-Policy: reflected-xss filter ：XSS攻撃のフィルタリングを選択式にする。 - Content-Security-Policy: reflected-xss block ：XSS攻撃のフィルタリングを有効にする。 上記レスポンスヘッダに対応しているかどうかはブラウザによって異なるため、対象となるWebサイトの推奨利用環境に合わせたヘッダを使用する。		Return a response header that enables the browser protection against cross site scripting ("X-XSS-Protection ", "Content Security Policy" etc). (Setting example) - X-XSS-Protection: 1; mode=block : The XSS filter function is turned on, it detects an XSS attack and does not execute it. - X-XSS-Protection: 0 : Disable XSS filter. - Content - Security - Policy: reflected - xss allow : Disable filtering of XSS attacks. - Content - Security - Policy: reflected - xss filter : Select filtering of XSS attacks selectively. - Content-Security-Policy: reflected-xss block : Enable filtering of XSS attacks. As it depends on the browser level of support of the above header, use a header that matches the recommended environment of the target Web site.
4-2	パラメータ改ざん対策	入力値チェックをサーバ側で行う。	Parameter tampering countermeasures	Perform input value check on the server side.
		Webフォームのテキスト入力項目から渡されるパラメータの入力値チェックを行う。		Perform input value check of parameters passed from the text input controls of the web form.
		Webフォームの選択項目(ラジオボタン・チェックボックス・選択肢リストなど)で渡されるパラメータの入力値チェックを行う。		Check input values of parameters passed in selected controls of the web form (radio button, check box, option list, etc.).
		hiddenフィールドで渡されるパラメータの入力値チェックを行う。		Check the input value of the parameter passed in the hidden field.
		クエリ文字列で渡されるパラメータの入力値チェックを行う。		Perform input value check of parameters passed in query string.
		HTTPリクエストヘッダの入力値チェックを行う。		Check input value of HTTP request header.
4-3	Cookieの改ざん	入力値チェックをサーバ側で行う。	Cookies tampering	Perform input value check on the server side.
		Cookieに格納されているパラメータの入力値チェックを行う。		Check input values of parameters stored in Cookie.
		Cookieに直接ユーザIDなどを入れる場合には、暗号化する。		When entering a user ID etc directly in Cookie, encrypt it.
4-4	e-mailスプーフ	外部からのパラメータをメールヘッダの内容に指定しない。	E-mail spoofing	Do not specify external parameters as contents of email header.
		外部からのパラメータをメールヘッダに指定する場合は、改行文字など危険な文字を排除する。		To specify external parameters in the email header, eliminate dangerous characters such as line feed characters.
4-5	SQLインジェクション対策	SQL文の組み立てにバインド機構を使用する。 バインド機構が利用できない場合は、SQL文の組み立てに用いるパラメータに対し、エスケープ処理を行う。	SQL injection countermeasures	Use bind mechanism to construct SQL statement. If the bind mechanism can not be used, escape processing is performed on the parameters used for assembling the SQL statement.
		SQL文の組み立てに用いるパラメータに対し、入力値チェックを行う。		Perform input value check for parameters used for assembling SQL statements.
		Webアプリケーションに渡されるパラメータにSQL文を直接指定しない。		Do not directly specify the SQL statement in the parameter passed to the Web application.
		エラーメッセージをそのままブラウザに表示しない。		Do not display the error message as it is in the browser.
4-6	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対策	外部からのパラメータにWebサーバ内のファイル名を直接指定できる実装を行わない。 上記ができない場合、ファイルを開く際は固定ディレクトリを指定し、かつファイル名にディレクトリが含まれないようにする。	Unchecked path name parameter and directory traversal countermeasures	Do not implement implementation that can directly specify the file name in the web server as external parameters. If the above can not be done, specify a fixed directory when opening the file, and make sure that the directory name is not included in the file name.
		ファイル名を指定するパラメータでは入力値チェックを行い、あらかじめ決められたファイル名のみ受け付けるようにするか、英数字のみ受け付けるようにする。		For parameters that specify file names, check input values, accept only predetermined file names, or accept only alphanumeric characters.
4-7	アップロードファイルによる脆弱性	外部からファイルをアップロードする場合は、Webサーバのドキュメントルートディレクトリ以外に格納するようにする。	Upload file vulnerability	When uploading files from the outside, store it in a directory other than the document root directory of the web server.
4-8	httpヘッダ・インジェクション対策	ヘッダの出力を直接行わず、Web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。 ヘッダ出力用APIが改行コードを適切に処理できない場合は、改行を許可しないよう、開発者自身で適切な処理を実施する。	Http Header Injection countermeasures	Do not directly output the header, use the API for header output prepared for the execution environment and language of the Web application. When the header outputting API can not properly process the line feed code, the developer properly performs processing so as not to permit line feed.
		外部からの入力の全てについて、改行コードを削除する。		Delete the line feed code for all external input.
4-9	OSコマンドインジェクション対策	シェルを起動できる言語機能の利用を避ける。 例えばPerlでファイルを開く場合、open関数の代わりにsysopen関数を使用する。	OS Command Injection countereasures	Avoid using language features that can invoke the shell. For example, when opening a file in Perl, use the sysopen function instead of the open function.
		危険な関数を使用する場合は、危険な関数に渡すパラメータの入力値チェックを行い、埋め込むデータをシングルクォートでくくる。 また入力値チェックはあらかじめ決められたファイル名のみ受け付けるようにするか、英数字のみ受け付けるようにする。		When using a dangerous function, check the input value of the parameter passed in, and enclose with single quotes the data to be embedded. Also, check the input value so that is accepted only the predetermined file name or only alphanumeric characters.
		シェルを起動できる言語機能を利用する場合は、そのパラメータを構成する全ての変数に対してクライアントチェックを行い、あらかじめ許可された処理のみが実行されるようにする。		When using a language that can invoke the shell, make a client check on all variables constituting the parameter so that are executed only the processes permitted in advance.
		クライアントから渡されたパラメータを危険な関数に渡さない。		Do not pass parameters passed from client to dangerous functions.
		PerlではTaintモードを使用する。		Use Taint mode in Perl.
4-10	eval-インジェクション対策	悪意のある入力値を拒否するため、ホワイトリスト方式で入力値チェックを行う。	Eval injection countermeasure	To reject malicious input values, check the input value in the whitelist manner.
4-11	強制ブラウズ対策	認証後にしか表示されてはならないページを認証前に表示させない。	Forced browsing countermeasures	Make sure that pages that should only be displayed after authentication are not displayed before authentication.
		認証後にアクセス権のないページをファイル名の推測などによって表示されないようにする。		Prevent pages without access right after authentication from being displayed due to inference of file name or the like.
4-12	バッファオーバーフロー対策	直接メモリにアクセスできない言語で記述する。（言語の例：PHP、Perl、Java等）	Buffer overflow countermeasure	Use languages that can not directly access the memory. (Examples of languages: PHP, Perl, Java etc)
		直接メモリにアクセスできる言語で記述する場合は、アクセスできる言語で記述する部分を最小限にする。（言語の例：C、C+、アセンブラ等）		When writing in a language that can access direct memory, minimize the part to be written in that one. (Examples of languages: C, C+, assembler, etc.)
		脆弱性が修正されたバージョンのライブラリを使用する。		Use vulnerability-patched versions of libraries.
4-13	セッションハイジャック対策	セッション管理に利用するセッションIDはクエリ文字列でのやり取りを行わない。	Session hijacking countermeasures	Do not exchange in the query string the session ID used for session management.
		セッションIDを推測困難なものにするために、セッションIDにはログインID、メールアドレスなど他人が知りうる情報を利用しない。		In order to make the session ID difficult to guess, we do not use information that other people can know such as login ID, email address as session ID.
		セッション変数は値を格納するたびに、セッションIDを変更する。		Each time a session variable stores a value, it changes the session ID.
		セッションIDはランダムな値を利用し、固定値にしない。		The session ID uses a random value, not a fixed value.
		セッションIDは推測されないよう、十分に長い桁数にする（10数桁以上）。		The session ID is set to a sufficiently long number of digits (10 or more digits) so as not to be guessed.
		セッションIDをURLパラメータに格納しない。		Do not store the session ID in the URL parameter.
		セッション管理ではセッションIDのみではなく、クライアントのIPアドレスでも管理を行う。		In session management, it manages not only the session ID but also the IP address of the client.
		ログイン成功後に新しくセッションを開始するようにする。 もしくは、ログイン成功後に、既存のセッションIDとは別に秘密情報を発行し、ページの遷移時にその値を確認する。		Make sure to start a new session after successful login. Alternatively, after successful login, confidential information is issued separately from the existing session ID, and the value is confirmed at the time of page transition.
		セッション管理を行なう必要のあるページでは暗号化通信(https)を利用する。		For pages that require session management, encrypted communication (https) is used.
		暗号化通信(https)で利用するCookieにはSecure属性を加える。		Add Secure attribute to cookie used for encrypted communication (https).
		セッションIDをCookieにセットする場合、有効期限の設定に注意する。		When setting the session ID in the cookie, pay attention to the expiration date setting.
		セッションの有効期限を設定し、有効期限を過ぎたものはサーバ側で無効にする。		Set the expiration date of the session and invalidate it on the server side after the expiration date.
		ユーザがパスワードを指定回数以上連続して間違えた場合はそのユーザアカウントをロックし、使用できないようにする。		If the user mistakes the password consecutively more than the specified number of times, lock the user account and make it unusable.
		ユーザがログイン後、画面上で一定時間操作を行わない場合は自動的にログアウトする設定を施す。		Set automatic logout for the logged-in user, in case of a certain period of inactivity on the screen.
4-14	CSRF（クロスサイト・リクエスト・ フォージェリー）	以下の3つの対策のうちいずれかを行う。 1. 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。 2. 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、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。 3. Refererが送られてきた場合は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ようにする。 Refererが送られてこない場合はエラーとし、処理を実行しない。	CSRF (cross site request forgery)	Adopt one of the following three countermeasures. 1. Access by POST method the page executing a process. Generate automatically the previous page inserting secret information in hidden parameters, and excecute the process in the executing page only in case of right values. 2. Request again the password input on the page immediately before executing the processing, and on the executing page execute the process only when the entered password is correct. 3. When Referer is sent, confirm whether it is the correct link source, and execute the process only when it is correct. If Referer is not sent, it is an error, and the process is not executed.
4-15	アクセス制御や認可制御の欠如	アクセス制御機能による防御措置が必要なWebサイトには、パスワードによる秘密情報の入力を必要とする認証機能を設ける。	Lack of access control and authorization control	A Web site that requires defensive measures by the access control function is provided with an authentication function that requires input of confidential information by password.
		認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人に成りすましてアクセスできないようにする。		In addition to the authentication, implement authorization control to prevent access from logged-in users who are pretending to be others.
4-16	フィッシング詐欺の助長	フレームを利用する場合、子フレームのURLを外部パラメータから生成しないように実装する。	Phishing scams	When using an iframe, do not to generate the URL of the child frame from external parameters.
		利用者がログイン後に移動するページのリダイレクト機能を動的に実装するWebサイトについて、リダイレクト先のURLとして使用されるパラメータの値には、自身のドメインのみを許可するようにする。		For a Web site that dynamically implements the redirect function of the page that the user moves after logging in, allow only the domain of its own as the value of the parameter used as the URL of the redirect destination.
		重要情報（お客様の個人情報や、各社における機密レベルの情報等）を入力・表示するページはEV SSL証明書を取得し、サイトの運営者を証明する。		A page that inputs and displays important information (customer's personal information, confidential level information etc. at each company) acquires the EV SSL certificate and certifies the operator of the site.

4-17	GETメソッドによる情報漏えい対策	GETメソッドでユーザ名やパスワードなどの重要な情報を送信しない。	Measures against information leakage by GET method	We do not send important information such as user name and password with GET method.
4-18	アプリケーションへのパラメータタイプ	サーバ側で保持している情報を以降のページでも使用するためにクエリ文字列またはhiddenフィールドに格納しない。	Parameter type to application	The information held on the server side is not stored in the query character string or hidden field so that it can be used on subsequent pages.
		アクセス権に関する情報をクエリ文字列またはhiddenフィールドに格納しない。		Information on access rights is not stored in the query string or hidden field.
4-19	HTML内コメントによる情報漏えい対策	HTML内コメントに重要なデータやその保存先、ファイル名を記載しない。	Measures against information leakage by comments in HTML	Do not write important data, its storage destination and file name in HTML comments.
		HTML内コメントに非公開ページの保存先やファイル名を記載しない。		Do not include the save destination and file name of the private page in HTML comments.
		HTML内コメントにファイルの絶対パスを記載しない。		Do not write the absolute path of the file in HTML comments.
		HTML内コメントにその他内部ロジックを推測されるような情報を記載しない。		Do not write internal logic or inferring information in HTML comments.
4-20	Cookieの利用	Cookieの有効期限は必要最低限とする。	Using cookies	Cookie expiration date shall be the minimum necessary.
		Cookieのアクセス可能ドメイン、パスは必要最低限とする。		The cookie's accessible domain and path are minimum necessary.
		暗号化通信でやり取りを行なうCookieについてはSecureフラグを設定する。		For the cookie that exchanges by encrypted communication, the Secure flag is set.
		Cookieには個人情報、重要情報は格納しないこととし、格納する必要がある場合には必ず暗号化して格納する。		Personal information and important information are not stored in Cookie, and when it needs to be stored, it is always encrypted and stored.
4-21	認証による個人情報漏えい対策	正しい認証情報でのみ、ログインできる。	Measures against personal information leakage by authentication	System can be looged in with right sets of authentication data only.
		クエリ文字列には、POSTメソッドを使い、ユーザID、パスワードを入れない。		For the query string, use POST method, do not include user ID and password.
		ユーザID、パスワードなどの認証情報をデータを入力させる時はSSL/TLSの暗号通信を使用する。 （TLS1.0～1.2を使用する。ただし、TLS使用時は安全な暗号アルゴリズムを使用する。） （安全な暗号アルゴリズム例） - 鍵交換 ： DH 、 ECDH 等 - 署名 ： RSA 、DSA 、 ECDSA 等 詳細は「SSL/TLS暗号設定ガイドライン（P33,34）」等を参照する。（ただし、ハッシュ関数の暗号アルゴリズムには、SHA-1は使用しない。） また、通信経路上での暗号グレード変更による盗聴を防ぐため、サーバやOSの設定ファイルに、以下の設定値を追記する。 - DHE_EXPORT suite の無効化（Logjam脆弱性対策となる）		Use SSL/TLS encrypted communication when entering authentication information such as user ID, password, etc. (Use TLS 1.0 to 1.2, but use secure encryption algorithm when using TLS about.) (Secure encryption algorithm example) - Key exchange: DH, ECDH, etc. - Signature: RSA, DSA, ECDSA, etc. For details, refer to "SSL/TLS cryptographic setting guidelines (P 33, 34)" and others. (However, SHA-1 should not be used for the encryption algorithm of the hash function.) Also, in order to prevent eavesdropping due to cryptographic grade change on the communication route, add the following setting values to the server and OS setting file. - Invalidation of DHE_EXPORT suite (It is a measure against Logjam vulnerability)
		認証エラー時にエラー内容によってエラーメッセージを変えて表示しない。		When an authentication error occurs, change the error message according to the error content and do not display it.
		パスワードの変更時に現在のパスワードを表示しない。		Do not display the current password when changing the password.
		パスワードの変更時に現在のパスワードを再入力させる。		Make the current password reenter when changing the password.
		パスワードをサーバ内で保管する場合は、平文ではなく、ソルト付きハッシュ値の形で保管する。（ソルトとは、パスワードとともに用いられる乱数や任意の文字列のこと） - ソルトはユーザ毎に異なるものを使用してパスワードと組み合わせた文字列をハッシュ化する。 - ハッシュから平文を得るためのアルゴリズムであるレインボーテーブルから防御するため、ソルトの文字数は20文字以上を推奨する。		When storing passwords in the server, they are stored in the form of salt-attached hash values, not plain text (Salt is a random number or arbitrary character string used with a password). - Hash the string combined with the password using different salt for each user. - To protect against the rainbow table, which is an algorithm for obtaining plaintext from hash, it is recommended that the number of characters of salt be 20 or more.
		機密情報を扱うフォームのオートコンプリート機能を無効化し、画面のキャッシュも無効化する。		Disable autocomplete function of confidential information form and disable screen cache.
4-22	個人情報表示時の対策	個人情報など重要な情報を表示する場合SSL/TLSの暗号通信を使用する。（TLS1.0～1.2を使用する。ただし、TLS使用時は安全な暗号アルゴリズムを使用する。） （安全な暗号アルゴリズム例） - 鍵交換 ： DH 、 ECDH 等 - 署名 ： RSA 、DSA 、 ECDSA 等 詳細は「SSL/TLS暗号設定ガイドライン（P33,34）」等を参照。（ただし、ハッシュ関数の暗号アルゴリズムには、SHA-1は使用しない。） また、通信経路上での暗号グレード変更による盗聴を防ぐため、サーバやOSの設定ファイルに、以下の設定値を追記する。 - DHE_EXPORT suite の無効化（Logjam脆弱性対策となる。）	Measures to be taken when displaying personal information	"When displaying important information such as personal information, use SSL/TLS encrypted communication (Use TLS 1.0 - 1.2, but use secure encryption algorithm when using TLS.) (Secure encryption algorithm example) - Key exchange: DH, ECDH, etc. - Signature: RSA, DSA, ECDSA, etc. For details, refer to "SSL/TLS cryptographic setting guidelines (P 33, 34)" and others. (However, SHA-1 should not be used for the encryption algorithm of the hash function.) Also, in order to prevent eavesdropping due to cryptographic grade change on the communication route, add the following setting values to the server and OS setting file. - Disable DHE_EXPORT suite (It will be a measure against Logjam vulnerability.)
		画像ファイルも含め、個人情報など重要な情報の表示には認証などアクセス制限を設ける。		To display important information such as personal information, including image files, set access restrictions such as authentication.
		クレジットカードの番号などは全桁表示させない。		Do not display credit card numbers etc in all digits.
		重要度が高い情報の表示については再度パスワードの入力を求める。		For display of information with high importance, ask for password again.
		パスワードの再入力時にセッションIDを二重化する。		Duplicate session ID when re-entering password.
		関連サーバへアクセスするIDには最低限のアクセス権のみを付加する。		Only the minimum access right is granted to the ID for accessing the related server.
		利用者ログイン等、特に重要な認証においては、二要素認証を使用する。		Two-factor authentication is used in a particularly important authentication such as user log-in.
		利用者ログイン時、前回の最終ログアウト日時を表示する。		When the user logs in, the last logout date and time of the last time is displayed.
4-23	未公開ファイルによる情報漏えい	外部からのアクセスを想定していないファイルを公開ディレクトリに置かない。	Information disclosure due to unpublished files	Do not place files that are not supposed to be accessed from the outside in the public directory.
		Webアプリケーションにおいて一時ファイル作成が必要な場合、公開ディレクトリには一時ファイルを作成しない。		When creating a temporary file in the Web application, do not create a temporary file in the public directory.
4-24	情報保存の対策	収集した情報を公開ディレクトリに置かない。	Measures to save information	Do not put the collected information in the public directory.
		機密性の高い情報は暗号化して保存する。		Encrypt and store confidential information.
		保存した情報ファイルのアクセス権は最低限のものに限定する。		The access right to the saved information file is limited to the minimum.
		Webアプリケーションが保持するオブジェクト、スレッド、接続、ページ、パスワード情報等の機密性の高い情報をキャッシュに不必要に格納しない。		Do not unnecessarily store highly confidential information such as objects, threads, connections, pages, password information etc. held by the web application in the cache.
		不要な機密データは保有せずにすぐに破棄する。		Discard unnecessary confidential data immediately without holding it.
4-25	ユーザインターフェース（サイトの使い勝手）による対策	ブラウザのアドレスバー、ステータスバーを隠さない。	Measures by user interface (usability of site)	Do not hide the address bar and status bar of the browser.
4-26	クリックジャッキング対策	HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限する。 （設定値例） - X-Frame-Options：DENY ：すべてのWebページにおいてフレーム内の表示を禁止 - X-Frame-Options：SAMEORIGIN ：同一ドメイン内のWebページのみフレーム内の表示を許可 - X-Frame-Options：ALLOW-FROM ：指定したドメインのWebページのみフレーム内の表示を許可 （注意事項） 他Webページに自サイトを読み込ませている場合はこの対策がとれないことに注意する。	Measures against click jacking	The X-Frame-Options header field is included in the HTTP response header, in order to restrict access from frame and iframe elements containing sites of other domains. (Setting example) - X-Frame-Options: DENY ：Display within frame is prohibited on all Web pages - X-Frame-Options: SAMEORIGIN ：Only Web pages of the same domain are permitted to be displayed in the frame - X-Frame-Options: ALLOW-FROM ：Only Web pages of the specified domain are permitted to be displayed in the frame (Notes) Please be aware that these measures can not be taken if other web pages are loading the site.
		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、実効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。		Input the password again on the page immediately before the one executing the process, and on the effective page, execute the process only when the password entered again is correct.
4-27	競合状態の脆弱性	2つのスレッドが同時にリソースを使用して処理を行なうプログラムの場合、ロック機能を使用し、処理が停止させない。	Race condition vulnerability	In the case of a program in which two threads simultaneously use resources to perform processing, the lock function is used so as not to stop processing.
4-28	ソースコードレビュー	プログラムを作成・改修した際に、開発者とは別の担当者により、ソースコードレビューを行なう。（既知の脆弱性対策が行えているか、設計では予定されていない機能が組み入れられていないか） （ソースコードレビューの実施方法） 担当者がソースコードをチェックする方法や、静的検査ツールを使う方法等を用いる。	Source code review	When creating/improving the program, the source code review is performed by another person who is different from the developer (whether known vulnerability countermeasures can be performed or not planned functions are not incorporated in the design) (How to carry out source code review) The person in charge checks the source code or it is used a static inspection tool and similars.

5 通信に関するセキュリティ対策 Security measures for communication.

No	対策分類	実施項目	Classification of measures	Action Item
5-1	FW（ファイアウォール）の設置	FWを設置し、必要な通信だけを許可する等、適切なフィルタリングの仕組みを施す。	Installation of FW (firewall)	Install a FW, apply appropriate filtering mechanism such as allowing only needed communication.
		FWの通信ログを一定期間保存し、定期的にログの確認をする。 また、必要に応じて設定変更する。		Save the communication log of FW for a certain period and periodically check the log. Also, change the setting as necessary.
5-2	IDS/IPSの設置	IDS/IPS等を設置し、FWでは防げなかった不正なアクセスを検知、もしくは防止する仕組みを施す。	Installation of IDS/IPS	Install IDS/IPS etc., and apply a mechanism to detect or prevent unauthorized access which can not be prevented by the FW.
		IDS/IPSの通信ログを一定期間保存し、定期的にログの確認をする。 また、必要に応じて設定変更する。		Save the IDS / IPS communication log for a certain period and periodically check the log. Also, change the setting as necessary.
5-3	暗号化	必要に応じて、クライアントサーバ間、又は、サーバ間における通信を暗号化する仕組みを施す。 同様にリモートでアクセスする際も通信を暗号化する仕組みを施す。 （通信の暗号化例） - IP-VPNの利用とIP secによる暗号化 - SSLによる通信の利用	Encryption	Provide a mechanism to encrypt communication between client servers or between servers as necessary. Likewise, when accessing remotely, use a mechanism for encrypting communication. (Encryption example of communication) - Use of IP-VPN and encryption by IP sec - Use of communication by SSL

5-4	管理	ネットワーク構成図を入手し、ネットワークの構成を把握する。 また、ネットワーク構成図の変更管理を実施する。	Management	Obtain the network configuration diagram and grasp the configuration of the network. Also, manage changes of the network configuration diagram.
		ネットワーク機器のログを管理する。		Manage logs of network devices.
		ネットワーク機器類のアカウント管理等に関しては、2-2項目「プラットフォーム」と同様の対応を施す。		Regarding account management etc. of network equipments, take the same measures as in paragraph 2-2 of "platform" chapter.
5-5	バックアップ	ネットワーク機器の設定情報を必要に応じて、バックアップする。	Backup	Back up the network device's configuration information as needed.
		1台のネットワーク機器が使用不可になった場合、2台目に切り替える仕組みを施すなど、通信を停止させない仕組みを施す。		Provide a mechanism to switch to a second network device, when one network device becomes unusable, so that communication is not stopped.
		ネットワークの設定情報をバックアップしたデータは、ネットワーク機器設置場所とは別拠点に保管する。		Data that backed up the network configuration information is stored in a different location from the network device installation location.
5-6	監査機能	各種ネットワーク機器のログを収集するサーバを設ける。	Audit function	Provide a server to collect logs of various network devices.
		SIEM(セキュリティ情報イベント管理)が可能な、ログ一元管理の仕組みを施す。		We provide a log unified management system that enables SIEM (security information event management).
		監査ログにセキュリティレベルを設定し、レベルに応じて通知する仕組みを施す。		Set a security level in the audit log and provide a mechanism to notify according to the level.

6 社内支給端末に関するセキュリティ対策 Security measures concerning in-house terminals.

No	対策分類	実施項目	Classification of measures	Action Item
6-1	社内支給端末を管理(操作)するアカウント管理	管理部のアカウントと、利用者アカウントは必ず別に付与する。	Account management to manage (manipulate) company-supplied terminals	The account of the management section and the user account are necessarily given separately.
		管理部のアカウントと、利用者のアカウントはデフォルト設定ではなく、変更する。構築時に使用したアカウントなど不要なアカウントは必ず削除する。		Change the default settings of the of the administration department account and the user one. Be sure to delete unnecessary accounts such as accounts used during configuration.
		管理者権限ID、ユーザIDの共有アカウントを作成することは原則禁止する。		In principle, it is prohibited to create shared administrator account ID and shared user ID.
		同一のアカウントを複数の利用者で共用する事は原則禁止だが、当該利用者に使用を認められ、かつ情報セキュリティ責任者の承認を得た場合のみ、アカウントの共用を許可する。 アカウントの共用にあたっては利用簿を作成して管理する。また、外部委託する場合は、セキュリティ対策を考慮した運用ルールであることが確認できれば、委託先業者の運用ルールに任せる。 利用簿には以下を明記する。 - 利用システム - 申請日時 - 対象者名（委託先業者の場合は業者名も明記する） - 利用するアカウント - アカウントの共用目的 - 利用期間(○年○月○日～○年○月○日) - 情報セキュリティ責任者の署名		Sharing the same account among multiple users is prohibited in principle, but it is permitted only for determined personnel or approved ones by the information security officer. When sharing accounts, manage them using a register. Also, in the case of outsourcing, if it can be confirmed that it is a contractor observing security measures, it is left to the operation rules of the contractor. Write the following in the use register. - System used - Application date and time - Person name (In the case of a contractor, also specify the name of it) - Account to use - Account sharing purpose - Period of use (○ year ○ month ○ day ～ ○ year · month month ○ day) - Signature of information security officer
6-2	社内ネットワークへ接続する機器の管理	支給もしくは、情報セキュリティ責任者に利用を許可された端末以外を社内ネットワークに接続することを禁止する。	Management of equipment connected to internal network	Prohibit connecting to the internal network with devices other than the provided ones or the ones allowed by the information security officer.
6-3	ソフトウェア脆弱性対応	最新のソフトウェアパッチを適用する。 パッチ適用で動作確認が必要な場合は、動作確認終了後、即時に適用する。	Software vulnerability response	Apply the latest software patch. If an operation check is required for the patch, apply the patch immediately after the end of operation check.
6-4	ウイルス対策	情報セキュリティ責任者が認定したウイルス対策ソフトを導入する。	Antivirus	Install antivirus software certified by information security officers.
		ウイルス対策ソフトのパターンファイルは、最新のファイルを適用する。		Apply the latest virus pattern file to antivirus software.
6-5	バックアップ	必要に応じてシステム構築時のイメージバックアップなど、システム障害時のリカバリCDを用意する。	Backup	If necessary prepare a recovery CD from system failure such as an image backup at the time of system configuration.
6-6	暗号化	ノートPCを使用する場合はストレージを暗号化する。	Encryption	When using a laptop PC encrypt storage.

7 インシデント対応時のセキュリティ対策 Security measures when handling incidents.

No	対策分類	実施項目	Classification of measures	Action Item
7-1	インシデント発生時の連絡	インシデント発生時は、当社が定める連絡方法に従う。	Contact when incidents occurred	When an incident occurs, follow the contact method specified by our company.
7-2	復旧作業	インシデント発生に備え、システムごとにシステム障害時の復旧手順をあらかじめ整備する。	Recovery work	To prepare for incident occurrence, prepare in advance, for each system, recovery procedures in case of system failure.
		システムごとに、システム障害時の復旧手順に従って、システム復旧を実施する。		For each system, perform the system restoration according to the recovery procedure at the time of system failure.
7-3	再発防止策の実施	インシデント発生に備え、システムごとに応急対応をあらかじめ整備する。	Implementation of measures to prevent recurrence	To prepare for incident occurrence, prepare in advance, for each system, emergency responses.
		再発防止対策が確定するまでは、システムごとに定められた応急対応にて、インシデント再発を防止する。		Apply temporaly measures to prevent recurrence of incident until the permanent measures are specified and applied.
		インシデントの再発を防ぐために、その原因を特定し、再発防止策確定後は速やかに対策を実施する。		In order to prevent recurrence of incidents, identify the cause and promptly implement countermeasures after establishment of recurrence prevention measures.