カテゴリ	分類	#	項目	判定	適合状況
	基本セキュリティ要件	3.1.1	システムへのアクセスは、認可されたユーザー、認可されたユーザーに代わって動作するプロセスおよび（その他のシステムを含む）デバイスに限定する。	○	各システムのアクセスは、認可された業務上必要最低限のユーザのみに限定されている。また、RPAによるアクセスについても当該ユーザを代理する範囲に限定している。
		3.1.2	システムへのアクセスは、認可されたユーザーが実行を許可されているタイプのトランザクションおよび機能に限定する。	○	ゲスト、匿名アカウントは作成していない上、運用で作成を禁止している。 共有アカウント（会社の代表メールアカウント）については、代表社員、Secretaryのみアクセスを限定している。 開発用のテストアカウントについては、事前にシステム管理者が許可した場合に限り作成可能としている。 各個人用のWindows環境は、リモートアクセスを許可しているがクライアント側へのデータ転送を拒否している。
	派生セキュリティ要件	3.1.3	承認された認可に従って、CUI のフロー（flow）を管理する。	△	(1) エクスポートが制限されている情報を平文でインターネットに移動できないようにすること →ネットワークは、暗号化しており平文で移動不可としている。 (2) 組織内からのトラフィックであると主張する外部からのトラフィックをブロックすること →外部からのネットワークアクセスは拒否している (3) 内部の web プロキシサーバーからではないインターネットへのリクエストを禁止すること →業務環境は、弊社VDIサーバまたはMDMで管理している端末に限定しており、所定のサーバからのみアクセスのみ許可している (4) データ構造およびコンテンツに基づいて組織間での情報転送 を限定すること。 →組織間の情報転送は、物理的に分離しており限定されている。
		3.1.4	共謀が関与しない場合の有害行為のリスクを減らすため、個人の職務を分離する。	△	(1) ミッション関連の機能とシステムサポート関連の機能を異なる個人や役割に割り当てること →どちらも代表社員が権限を有している (2) 異なる個人がシステムサポートの機能（たとえば、構成管理、品質保証および品質試験、システム管理、プログラミング、おおびネットワークセキュリティなど）を実施すること →代表社員が実施した場合、Secretaryがレビューを行うなど複数人で実施している。 (3) アクセス管理機能を管理するセキュリティ担当者が監査機能の管理も行わ
		3.1.5	特定のセキュリティ機能および特権アカウントを含め、最小特権の原則を採用する。	○	特権アカウントは、必要最低限に付与している。（現在は、代表社員のみ） ローカルアカウントの作成はできないような設定（クライアントの管理権限は代表社員が管理し、利用者は、割り当てられた利用者権限のアカウントのみ利用可能）
		3.1.6	非セキュリティ機能にアクセスする時には、非特権アカウントまたは役割を使用する。	×	管理者権限は、代表社員アカウントと同一であり、非特権アカウントを利用できていない。
		3.1.7	非特権ユーザーが特権機能を実行することを防止し、そのような機能の実行を監査ログに取り込む（capture）。	○	非特権ユーザが特権機能を実行することは防止している。 実施履歴は、OSのログに記録されている。
		3.1.8	ログオン試行失敗回数を限定する。	○	ログオン試行失敗回数を限定し、所定回数誤るとアカウントがロックする。
		3.1.9	適用される CUI のルールに則って、プライバシーおよびセキュリティ通知を提示する。	○	会社貸与スマートフォンについては、会社所有かつ管理されていることを表示している。
		3.1.10	非アクティブ状態が一定時間経過後のデータのアクセスおよび閲覧を防止するために、隠蔽用パターンの表示によるセションロックを使用する。	○	一定時間非アクティブ状態となると画面ロック状態となる設定をしている。 また、システム利用ルールで、離席時は、画面ロックをかけるように制限している。
		3.1.11	規定された条件が成立した場合には、ユーザーセションを（自動的に）終了させる。	○	各個人のWindows環境へのリモートデスクトップのセッションは、クライアント側がスリープ状態になるとセッションが切断される設定となっている。
		3.1.12	リモートアクセスセションを監視し、管理する。	○	リモートアクセス時のアカウント利用状況は、監視でき接続ログを記録している。 VDI環境は、サーバ側でも利用状況をリアルタイムで監視できる。
		3.1.13	リモートアクセスセションの秘匿性を保護するために暗号メカニズムを採用する。	○	リモートアクセスツールにて、セッションは暗号化（暗号化は、4096ビットのRSA秘密/公開鍵交換と256ビットのAESセッションエンコーディングに基づいています。）されている。
		3.1.14	管理されたアクセス制御ポイント経由でリモートアクセスをルーティングする。	○	リモートアクセスは、指定のツールからのみかのうであり、管理外のアクセス制御ポイントからアクセスは不可となっている。 オフィス内のネットワーク環境は、基本外部からのアクセスが不可となっている。
		3.1.15	特権コマンドのリモート実行およびセキュリティ関連情報へのリモートアクセスを認可する。	○	サーバおよびクライアント（モバイルデバイスは除く）は、すべてリモートアクセスが可能
		3.1.16	ワイヤレスアクセスの接続を許可する前に、そうしたアクセスを認可する。	○	ワイヤレスアクセスに接続する際は、パスワードにより制限している。 また、一部の拠点では、デバイスのMacアドレスにより接続を制限している。
		3.1.17	認証および暗号を使用してワイヤレスアクセスを保護する。	○	ワイヤレスアクセスは、パスワード認証（一部、Macアドレス認証も併用）および暗号化している。
		3.1.18	モバイルデバイスの接続を管理する。	○	モバイルデバイスは、あらかじめMDMに登録したデバイスからのみ業務環境にアクセスできる。 個人所有のモバイルデバイスから業務環境にアクセスした場合、自動でMDMに登録され接続を管理することが可能としている。
		3.1.19	モバイルデバイスおよびモバイルコンピューティングプラットフォーム上の CUI を暗号化する。	○	モバイルデバイスは、暗号化をしている。
		3.1.20	外部システムへの接続および使用を検証（verify）し、管理／限定する。	○	Saasの使用は、IDとパスワードにて認証を検証している。 接続可能なIDとパスワードは、管理者が事前に登録し、利用アカウントを限定している。
		3.1.21	外部システム上でのポータブルストレージデバイスの使用を限定する。	○	会社としては、ポータブルデバイスを所有していない。 個人所有のポータブルデバイスは、利用ルールにて使用を禁止している。
		3.1.22	公衆アクセス可能なシステム上に掲載または処理される CUI を管理する。	○	利用ルールで、公衆アクセス可能な場所に情報を掲載していない。 公式Webサイトへの掲載情報は、代表社員がチェックしている。
意識向上及び訓練	基本セキュリティ要件	3.2.1	組織のシステムの管理者（managers）、システムアドミニストレーターおよびユーザーが、組織のシステムのセキュリティに関連する適用ポリシー、規格、および手順ならびに彼らの活動に関連するセキュリティリスクについて認識していることを確実にする。	○	各メンバーに代表社員がセキュリティポリシーを周知している。 社内ポータルサイトにセキュリティポリシー（ルール）に関する内容を掲載して周知している。
		3.2.2	職員が、割り当てられた情報セキュリティ関連の職務と責任を遂行するように訓練されていることを確実にする。	○	各メンバーに業務遂行上関係するセキュリティ事項の教育を教育資料を使用して実施している。

	派生セキュリティ要件	3.2.3	インサイダー脅威の潜在的兆候を認識し、報告するためのセキュリティ意識向上訓練を行う。	○	服務規定により、インサイダー脅威となる事項は禁止および個人で抱え込まないルールとしている。 代表社員より都度、声掛けを行うことで情報交換や意識の向上を図っている。
監査および説明責任	基本セキュリティ要件	3.3.1	非合法的または認可されてないシステム行為に関する監視、分析、調査、報告を可能にするために必要な範囲で、システム監査ログおよび記録を作成し保持する。	○	業務システムへのアクセスは、監視およびログの記録を行っている。
		3.3.2	個々のシステムユーザーの行動が、そのユーザーに対して一意に追跡可能であり、ユーザーが自らの行動に説明責任を負わせられるようにする。	○	電子メール、チャットの履歴は、個人単位で管理しており一意に追跡可能となっている。
	派生セキュリティ要件	3.3.3	ログ取得されたイベントを見直し、更新する。	○	ログイベントは、適宜見直しを行っている。
		3.3.4	監査ログ取得プロセスが失敗した場合にアラートを発する。	×	監査ログ取得プロセス失敗のアラートは、発報できていない。
		3.3.5	非合法的、認可されてない、疑わしい、または異常な行為の兆候を調査し対応するために、監査記録の見直し、分析および報告のプロセスを相互に関連づける。	×	監査記録の見直し、分析の運用はできていない。
		3.3.6	オンデマンドでの分析および報告をサポートするための監査記録の集約および報告書生成機能を提供する。	○	分析をサポートする機能を備えたツールを利用している。
		3.3.7	監査記録にタイムスタンプを生成するために、内部システムクロックを信頼できるタイムソース（時刻提供者）と比較および同期させるシステムケイパビリティを提供する。	△	ログにタイムスタンプは付与されているが、ログによってタイムゾーンが異なっている。
		3.3.8	監査情報および監査ログ取得ツールを、認可されてないアクセス、変更、および削除から保護する。	○	監査ログは、基本削除機能を保有していない。 特権アカウントで削除可能であっても、削除の運用は行っていない。 なお、特権アカウントは、代表社員のみに限定している。
		3.3.9	監査ログ取得機能の管理を特権ユーザーの一部の者に限定する。	○	代表社員のみに限定している。
構成管理	基本セキュリティ要件	3.4.1	個々のシステム開発ライフサイクル全体にわたり、組織が持つシステムの基本構成およびインベントリ（ハードウェア、ソフトウェア、ファームウェアおよび文書を含む）を規定し、維持する。	×	ドキュメント化できていない。
		3.4.2	組織のシステムで採用された情報技術製品のセキュリティ構成設定を規定し、実施する。	×	セキュリティ構成設定をドキュメント化できていない。
	派生セキュリティ要件	3.4.3	組織のシステムに対する変更を追跡、見直し、承認または非承認し、ログ取得する。	×	変更の承認・非承認のプロセスを規定できていない。 また、変更の追跡できない状態となっている。
		3.4.4	変更実施に先立って、セキュリティへのインパクトを分析する。	△	システム管理者による簡易なアセスメントにより、セキュリティインパクトを分析している。
		3.4.5	組織のシステム変更に関する物理的および論理的アクセス制限（restrictions）を明確に定め、文書化し、承認し、実施する。	△	代表社員のみがアクセス可能であることを定めているが、文書化できていない。
		3.4.6	必須なケイパビリティのみを提供するように組織のシステムを構成することにより、 最小機能性の原則を採用する。	○	必要最低限の機能やサービスのみ提供している。提供対象は、随時システム管理者が見直しをしている。
		3.4.7	必須でないプログラム、機能、ポート、プロトコルおよびサービスの使用を制限、無効化または防止する。	△	一部システム管理でのみ使用する機能（コマンドプロンプト、レジストリエディタなど）も利用可能となっている。
		3.4.8	「例外による拒否」（ブラックリスト登録）ポリシーを適用して認可されてないソフトウェアの使用を防止する、あるいは「全拒否、例外による許可」（ホワイトリスト登録）ポリシーを適用して認可されたソフトウェアの実行を許可する。	○	ポリシーを適用してホワイトリスト登録している。
		3.4.9	ユーザーがインストールしたソフトウェアを管理（control）し監視する。	○	ユーザがインストールしたソフトウェアは、専用の管理ツールにて管理、監視している。
識別および認証	基本セキュリティ要件	3.5.1	システムのユーザー、ユーザーに代わって動作するプロセス、およびデバイスを識別する。	○	各アカウントは一意となっており、デバイスも利用者を特定している。 なお、会社の代表アカウントに限り、代表社員およびSecretaryに限り共有しているが、ログイン元のIPアドレスにより利用者を特定できる。
		3.5.2	組織のシステムへのアクセスを許可する前提条件として、ユーザー、プロセス、またはデバイスのアイデンティティを認証（authenticate）（または検証（verify））する。	○	個人のアカウントは、パスワードだけでなく専用のオーセンティケーターアプリで認証することで二段階認証している。
	派生セキュリティ要件	3.5.3	多要素認証を特権アカウントによるローカルおよびネットワークアクセスならびに非特権アカウントによるネットワークアクセスに使用する。	○	特権アカウント、非特権アカウントによるアクセスは、専用のオーセンティケーターアプリで二段階認証をしている。
		3.5.4	特権および非特権アカウントによるネットワークアクセスに、リプレイ耐性のある認証メカニズムを採用する。	○	運用でリプレイに対する対応を行えるプロセスを採用している。
		3.5.5	規定された期間、IDの再利用を防止する。	○	IDなどは、一意になるようにしており、再利用を防止している。
		3.5.6	規定された非アクティブな期間が過ぎた後、ID を無効化する。	○	IDは、随時棚卸しを行い不要なIDは無効にしている。
		3.5.7	新しいパスワードが作成される際には、パスワードの最小限の複雑性と文字の変更を強制する。	○	パスワードポリシーにより、最小限の複雑性と文字の変更を強制している。
		3.5.8	指定された生成回数の間、パスワードの再利用を禁ずる。	×	禁止できていない。
		3.5.9	システムログオン時、常用（permanent）パスワードに即時変更することを条件として一時的パスワードの使用を許可する。	○	一時的なパスワードは、初回ログイン時に強制変更する設定となっている。
		3.5.10	暗号技術で保護されたパスワードのみを保存および伝送する。	○	パスワードは、暗号化されている。
		3.5.11	認証情報のフィードバックを隠す。	○	パスワードは、アスタリスクで表示される。
インシデント対応	基本セキュリティ要件	3.6.1	準備、検知、分析、抑制、復旧およびユーザー対応活動を含め、組織のシステムに運用状態のインシデント対応ケイパビリティを確立する。	△	インシデントの対応訓練は実施できていない。
		3.6.2	インシデントを追跡、文書化し、組織内外の指定された担当者および／または機関に報告する。	×	インシデントの報告プロセスが文書化できていない。
	派生セキュリティ要件	3.6.3	組織のインシデント対応ケイパビリティをテストする。	×	テストが実施できていない。
メンテナンス	基本セキュリティ要件	3.7.1	組織のシステムのメンテナンスを行う。	○	システムは随時メンテナンスしている。
		3.7.2	システムのメンテナンスを実行するために用いられるツール、技法、メカニズム、および職員を管理する。	○	メンテナンスは、代用社員が一手に管理している。
	派生セキュリティ要件	3.7.3	オフサイト（off-site）で行われるメンテナンスのために取り外される装置からすべての CUIがサニタイズ（情報除去）されていることを確実にする。	○	情報は、すべてクラウド上に保管しているため基本ローカルに情報を保存していない。 また、オフサイトでメンテナンスは基本実施していない。
		3.7.4	診断およびテストプログラムが入っている媒体を組織のシステムで使用する前に、悪意のあるコードの有無をチェックする。	○	悪意あるコードをチェックするツールにて常時チェックしている。
		3.7.5	外部ネットワーク接続を介して非ローカルメンテナンスセションを確立する際には多要素認証を要求し、非ローカルメンテナンスの完了時にはその接続を切断する。	○	現状メンテナンス時にセッションを確立していない。
		3.7.6	必要なアクセス認可のないメンテナンス職員のメンテナンス行為を監督（supervise）する。	○	現状、メンテナンスは、システム管理者である代表社員のみ。
媒体保護	基本セキュリティ要件	3.8.1	紙とデジタル双方とも、CUIを含むシステムの媒体を保護する（すなわち、セキュアに保存し物理的に管理する）。	×	紙媒体やデジタル（NAS）は、鍵付きのキャビネットに保管できていない。
		3.8.2	システム媒体上のCUIへのアクセスを、認可されたユーザーに限定する。	×	物理的にアクセスを制限できていない。
		3.8.3	CUIを含むシステムの媒体を廃棄または再利用する前に、サニタイズ（情報除去）または破壊する。	○	システム媒体は、破棄する際は、物理的に破壊している。 再利用する際は、サニタイズしている。
	派生セキュリティ要件	3.8.4	CUIのマーキングと配布制限が必要な媒体にはその旨をマーキングする。	○	現状対象となる媒体なし。
		3.8.5	CUI を含む媒体へのアクセスを管理し、管理区域外での輸送中は、媒体に関する説明責任を維持する。	○	現状対象となる媒体なし。

		3.8.6	代替的な物理的保全措置によって保護されている場合を除き、デジタル媒体上に保存されたCUI の秘匿性を輸送時に保護するため、暗号メカニズムを実装する。	○	デジタル媒体は、暗号化している。
		3.8.7	システムコンポーネント上のリムーバブルメディア（可搬型媒体）の使用を管理する。	×	リムーバブルメディアの使用は管理できていない。
		3.8.8	ポータブルストレージデバイスのオーナーを識別できない時には、そうしたデバイスの使用を禁止する。	○	運用ルールとして、ポータブルストレージデバイスの利用を禁止している。
		3.8.9	保管場所にあるバックアップ CUI の秘匿性を保護する。	○	バックアップデータは暗号化している。
職員のセキュリティ	基本セキュリティ要件	3.9.1	CUI を含む組織のシステムへのアクセス認可に先立って、個人を審査する。	○	システムへのアクセスは、システム管理者が審査している。
		3.9.2	退職や異動などの人事措置中、およびその後において、CUI を含む組織のシステムが保護されていることを確実にする。	○	退職時に貸与していたデバイスはすべて返却させ、アカウントのパスワードを変更することで保護している。
物理的保護	基本セキュリティ要件	3.10.1	組織のシステム、装置、およびそれぞれの運用環境への物理的アクセスを、認可された個人に限定する。	○	サーバ設置場所は、施錠しており鍵は許可された個人のみ貸与している。 サテライトオフィスについてもアクセスするための鍵は、代表社員およびSecretaryに限定している。
		3.10.2	組織のシステムの物理的施設および支援インフラを保護し、監視する。	○	オフィスには、ビデオ監視装置を使用して監視している。 また、鍵の開閉は、ログを記録している。
	派生セキュリティ要件	3.10.3	訪問者をエスコートし、その活動を監視する。	○	訪問者には、メンバーが常時付き添い監視している。
		3.10.4	物理的アクセスの監査ログを保持する。	○	ビデオ監視装置の動体検出機能により、自動録画している。 また、扉の解錠は、アカウントと日時のログを記録している。
		3.10.5	物理的アクセスデバイスを管理（control）および監督（manage）する。	○	鍵とスマートロックシステムを併用して監督している。
		3.10.6	代替作業サイトにおける CUI の保全措置を実施する。	○	リモートワーク時の業務実施ルールを定めている。
リスクアセスメント	基本セキュリティ要件	3.11.1	組織のシステム運用、および CUI に関連する処理、保存、または伝送から生ずる、組織運営（ミッション、機能、イメージ、評判を含む）、組織資産、および個人に対するリスクを定期的にアセスメントする。	×	定期的なアセスメントを実施できていない。
	派生セキュリティ要件	3.11.2	システムおよびアプリケーションの脆弱性スキャンを定期的に、かつ、それらのシステムおよびアプリケーションに影響する新たな脆弱性が特定された場合に実施する。	○	脆弱性スキャンは、常時行っている。 検知された脆弱性の対応を週1回以上行っている。
		3.11.3	リスクアセスメントに従って、脆弱性を取り除く。	○	3.11.2のスキャンにしたがい脆弱性を取り除いている。
セキュリティアセスメント	基本セキュリティ要件	3.12.1	組織のシステムのセキュリティ管理策を定期的にアセスメントし、その管理策の適用が有効かどうかを判断する。	×	定期的にアセスメントできていない。
		3.12.2	組織のシステムの欠陥を修正し、脆弱性を軽減または排除することを意図した実施計画書を作成し、実施する。	×	実施計画書を作成できていない。
		3.12.3	システムのセキュリティ管理策が継続的に有効であることを確実にするため、その管理策を継続的に監視する。	○	システム管理者が継続的に監視している。
		3.12.4	システムの境界、運用環境、セキュリティ要件の実装方法、および他のシステムとの関係または他のシステムへの接続について記述したシステムセキュリティ計画書を作成し、文書化し、定期的に更新する2	×	計画書は作成できていない。
システムおよび通信の保護	基本セキュリティ要件	3.13.1	通信（すなわち、組織のシステムによって送受信される情報）を、組織のシステムの外部境界および主要な内部境界において監視、管理、および保護する。	×	通信内容を監視できるシステムを整備できていない。
		3.13.2	組織のシステム内で効果的な情報セキュリティを促進するような、アーキテクチャー設計、ソフトウェア開発技法、およびシステムエンジニアリングの原則を採用する。	△	層構造の保護を開発している。
		3.13.3	システム管理機能からユーザー機能を分離する。	○	ユーザ機能は、物理的または仮想的に分離できている。
		3.13.4	共有システム資源を経由した、認可されてない情報転送や意図しない情報転送を防止する。	○	共有システム資源は、会社代表アカウントのみであるが、仮想的に利用環境を分離して意図しない情報転送を防止している。
		3.13.5	内部ネットワークから物理的または論理的に分離された、公開（Publicly）アクセス可能なシステムコンポーネント用のサブネットワークを実装する	×	サブネットワークは実装できていない。
		3.13.6	デフォルト設定によりネットワーク通信トラフィックを拒否、また例外によりネットワーク通信トラフィックを許可する（すなわち、全拒否、例外による許可）。	○	ファイアウォールにて、ネットワーク通信トラフィックの許可、拒否を行っている。
		3.13.7	リモートデバイスが、組織のシステムとの非リモート接続を確立することと同時に、外部ネットワーク内にある資源へその他何らかの接続（すなわち、スプリットトンネリング）を介して通信することを防止する。	○	ユーザが構成設定を行えない設定にしている。
		3.13.8	代替的な物理的保全措置によって保護されている場合を除き、伝送中の CUI の認可されてない開示を防止するために、暗号メカニズムを実装する。	○	通信内容はすべて暗号化している。
		3.13.9	通信セション終了時、または規定された非アクティブ時間経過後、そのセションに関連するネットワーク接続を切断する。	○	リモートアクセス時、規定の非アクティブ時間が経過すると画面ロックと同時にセッションを自動的に切断する設定をしている。
		3.13.10	組織のシステムで採用される暗号技術のための暗号鍵を設定し、管理する。	×	要件の規定ができていない。
		3..13.11	CUI の秘匿性保護には、FIPS 認証された暗号技術を採用する。	○	FIPS認証された暗号化技術を採用している。
		3.13.12	共同コンピューティングデバイスのリモートからの活性化を禁止し、そのデバイスに存在するユーザーに対して使用中のデバイスを表示する。	○	共同コンピューティングデバイスはない。
		3.13.13	モバイルコードの使用を管理および監視する。	○	システム管理者がレビューし、都度使用の管理、監視をしている。
		3.13.14	インターネットプロトコルによる音声通信（VoIP）技術の使用を管理および監視する。	○	システム管理者がレビューし、都度使用の管理、監視をしている。
		3.13.15	通信セションの真正性（Authenticity）を保護する。	○	リモートアクセスツールは、ツールの機能により真正性を保護している。
		3.13.16	通信停止中の CUI の秘匿性を保護する。	×	通信停止中の保護はできていない。
システムおよび情報の完全性	基本セキュリティ要件	3.14.1	システムの欠陥をタイムリーに特定し、報告し、修正する。	○	随時特定、修正している。
		3.14.2	組織のシステム内の指定された場所で、悪意のあるコードからの保護機能を提供する。	○	EDRでの保護を実施している。
		3.14.3	システムのセキュリティアラートおよび勧告を監視し、対応措置を講ずる。	○	システムのセキュリティアラートを発報するツールを導入している。
	派生セキュリティ要件	3.14.4	悪意のあるコードからの保護メカニズムが新たにリリースされた場合、更新する。	○	リリースされた場合、自動で更新する設定となっている。
		3.14.5	組織のシステムの定期的スキャンを実行すると共に、外部ソースからのファイルのリアルタイムスキャンを、ファイルがダウンロードされ、開かれ、実行される都度実行する。	○	定期的および都度実行している。
		3.14.6	攻撃および潜在的攻撃の兆候を検知するために、出入する通信トラフィックを含めて組織のシステムを監視する。	×	システム監視ができていない。
		3.14.7	組織のシステムの認可されてない使用を特定（identify）する。	×	システムの使用状況は、監視しているがトラフィックレベルでの監視はできていない、特定もできない。