CallConnect セキュリティチェックシート

クラウド電話システム「CallConnect」を運営する株式会社fonfunでは、IPAの「中小企業の情報セキュリティ対策ガイドライン第3版 付録7 リスク分析シート」に準拠したセキュリティチェックシートを公開しています。

最終更新日：2024年9月30日

対策の種類	項目	実施状況	備考
①組織的対策	経営者の主導で情報セキュリティの方針を示していますか？	○	情報セキュリティ方針を定め、Webページ上で公開しています。 https://www.callconnect.jp/security_policy
	情報セキュリティの方針に基づき、具体的な対策の内容を明確にしていますか？	○	情報セキュリティマニュアルを作成し、社内で共有しています。
	情報セキュリティ対策を実施するための体制を整備していますか？	○	情報セキュリティ事務局を設置、監査をLRM株式会社に依頼し、体制を整備しています。
	情報セキュリティ対策のためのリソース（人材、費用）の割当を行っていますか？	○	情報セキュリティ管理者を育成すると共に、セキュリティ教育や体制整備の予算を計上しています。
②人的対策	秘密情報を扱う全ての者（パートタイマー、アルバイト、派遣社員、顧問、社内に常駐する委託先要員などを含む）に対して、就業規則や契約などを通じて秘密保持義務を課していますか？	○	従業員については、入社時に秘密保持に関する誓約書を作成し、提出を求めています。 顧問については、秘密保持に関する条項を含んだ契約書を作成し、契約締結しています。
	従業員の退職に際しては、退職後の秘密保持義務への合意を求めていますか？	○	退職時には、秘密保持に関する誓約書の作成し、提出を求めています。
	会社の秘密情報や個人情報を扱うときの規則や、関連法令による罰則に関して全従業員に説明していますか？	○	入社時やセキュリティ教育を実施する際に、社内規則について説明を行い、周知を図っています。
③情報資産管理	管理すべき情報資産は、情報資産管理台帳を作成するなど何処にどのようなものがあるか明確にしていますか？	○	情報資産管理台帳を作成し、管理しています。情報資産の取り扱い方法については、情報セキュリティマニュアルにて定めています。
	秘密情報は業務上必要な範囲でのみ利用を認めていますか？	○	情報資産は重要度により分類し、それぞれ必要な範囲での利用を認めています。取り扱い方法は、情報セキュリティマニュアルにて定めています。
	秘密情報の書類に㊙マークを付けたり、データの保存先フォルダを指定するなど識別が可能な状態で扱っていますか？	○	情報資産の重要度により分類し、それぞれ取り扱い方法を定めています。
	秘密情報を社外へ持ち出す時はデータを暗号化したり、パスワード保護をかけたりするなどの盗難・紛失対策を定めていますか？	○	USBメモリを初めとした外部記録媒体へのコピーを禁止するなど、取り扱い規則を定め、HDDの暗号化、パスワード保護を実施しています。
	秘密情報は施錠保管やアクセス制限をして、持ち出しの記録やアクセスログをとるなど取り扱いに関する手順を定めていますか？	○	取り扱い方法を定め、必要最小限の人のみにアクセスを許可、施錠された場所で保管しています。
	重要なデータのバックアップに関する手順を定め、手順が順守されていることを確認していますか？	○	パックアップの手順を定め、パックアップが正しく行われているか定期的に確認しています。
	秘密情報の入ったパソコンや紙を含む記録媒体を処分する場合、ゴミとして処分する前に、データの完全消去用のツールを用いたり、物理的に破壊したりすることで、データを復元できないようにすることを定めていますか？	○	秘密情報が記録された紙、電子データの取り扱い方法を定め、紙はシュレッダーによる破棄の実施を定めています。
④アクセス制御及び認証	業務で利用するすべてのサーバーに対して、アクセス制御の方針を定めていますか？	○	最小権限の原則に基づき、アクセス制御方針を定めています。
	従業員の退職や異動に応じてサーバーのアクセス権限を随時更新し、定期的なレビューを通じてその適切性を検証していますか？	○	退職・移動時には、情報セキュリティ管理者がアクセス権の見直し、削除を実施しています。システム・サービス一覧表を作成し、定期的に不要なアクセス権が残っていないことを検証しています。
	情報を社外のサーバーなどに保存したり、グループウェアやファイル受渡サービスなどを用いたりする場合は、アクセスを許可された人以外が閲覧できないように、適切なアクセス制御を行うことを定めていますか？	○	最小権限の原則に基づき、アクセス制御方針を定めています。
	パスワードの文字数や複雑さなどを設定するＯＳの機能などを有効にし、ユーザーが強固なパスワードを使用するようにしていますか？	○	パスワードの生成ルールを定め、複雑で推測されにくいパスワードを使用しています。パスワード管理には、専用ソフトウェアを利用し、厳重に管理しています。
	業務で利用する暗号化機能及び暗号化に関するアプリケーションについて、その運用方針を明確に定めていますか？	○	暗号化の対象を定め、それぞれの暗号化の方法や鍵管理の方針を定めています。
⑤物理的対策	業務を行う場所に、第三者が許可無く立ち入りできないようにするための対策（物理的に区切る、見知らぬ人には声をかける、など）を講じていますか？	○	物理的セキュリティ境界を定め、入退室管理を実施しています。
	最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？	○	事務所の施錠、退出管理を実施しています。
	重要な情報やIT機器のあるオフィス、部屋及び施設には、許可された者以外は立ち入りできないように管理していますか？	○	物理的セキュリティ境界を定め、執務エリアには情報セキュリティ管理者の許可を得た場合のみ入室可能としています。
	秘密情報を保管および扱う場所への個人所有のパソコン・記録媒体などの持込み・利用を禁止していますか？	○	個人のPC・モバイル端末を利用する場合は、情報セキュリティ管理者の許可が必要と定めています。
⑥IT機器利用	セキュリティ更新を自動的に行うなどにより、常にソフトウェアを安全な状態にすることを定めていますか？	○	OSは常に最新バージョンに更新することをルールとして定めています
	ウイルス対策ソフトウェアが提供されている製品については、用途に応じて導入し、定義ファイルを常に最新の状態にすることを定めていますか？	○	OSの最新バージョンの利用、ウイルス対策ソフトの導入を求め、最新の状態にすることをルールとして定めています。
	業務で利用するIT機器に設定するパスワードに関するルール（他人に推測されにくいものを選ぶ、機器やサービスごとに使い分ける、他人にわからないように管理する、など）を定めていますか？	○	パスワードの生成ルールを定め、複雑で推測されにくいパスワードを使用しています。パスワード管理には、専用ソフトウェアを利用し、厳重に管理しています。
	業務で利用する機器や書類が誰かに勝手に見たり使ったりされないようにルール（離席時にパスワード付きのスクリーンセーバーが動作する、施錠できる場所に保管する、など）を定めていますか？	○	一定時間でのパスワード付きスクリーンセーバーによる自動ロックなどのルールを定め、実施しています。
	業務で利用するIT機器の設定について、不要な機能は無効にする、セキュリティを高める機能を有効にするなどの見直しを行うことを定めていますか？	○	パスワード管理に専用のソフトウェアを利用する、Mac PCの場合は Flie Vault を有効化するなど、対策を行っています。
	社外でIT機器を使って業務を行う場合のルールを定めていますか？	○	機器の外部持出時のルールを定めています。
	個人で所有する機器の業務利用について、禁止するか、利用上のルールを定めていますか？	○	個人のPC・モバイル端末を利用する場合は、情報セキュリティ管理者の許可が必要と定め、機器管理台帳にて機器の管理を実施しています。
	受信した電子メールが不審かどうかを確認することを求めていますか？	○	電子メールの利用ルールを定め、見知らぬ差出人からのメールは決して開かないように求めています。
	電子メールアドレスの漏えい防止のためのBCC利用ルールを定めていますか？	○	電子メールの利用ルールを定め、宛先が外部に流出しないようにしています。
	インターネットバンキングやオンラインショップなどを利用する場合に偽サイトにアクセスしないための対策を定めていますか？	○	OSやブラウザの脆弱性を狙われないように常にOSを最新バージョンに更新するなど対策を実施しています。
⑦IT基盤運用管理	IT機器の棚卸（実機確認）を行うなど、社内に許可なく設置された無線LANなどの機器がないことを確認していますか？	○	機器管理台帳を作成し、定期的に棚卸を実施しています。
	サーバーには十分なディスク容量や処理能力の確保、停電・落雷などからの保護、ハードディスクの冗長化などの障害対策を行っていますか？	○	AWSと Heroku Private Spaces で構築・運用しています。各サーバーの仕様や対策は以下URLの通りとなっており、高い信頼性のあるサービスを利用しています。 https://aws.amazon.com/jp/compliance/data-center/controls/ https://jp.heroku.com/enterprise
	業務で利用するすべてのサーバーに対して、脆弱性及びマルウェアからの保護のための対策を講じていますか？	○	アクセス制御の定期的な見直しを行うと共に、利用サーバーの最新のセキュリティ対策情報を確認しています。
	記憶媒体を内蔵したサーバーなどの機器を処分または再利用する前に、秘密情報やライセンス供与されたソフトウェアを完全消去用のツールを用いたり、物理的に破壊したりすることで、復元できないようにすることを定めていますか？	○	物理的破壊を行うか、外部の廃棄業者に委託するなど、機器の処分ルールを定めています。
	業務で利用するすべてのサーバーやネットワーク機器に対して、必要に応じてイベントログや通信ログの取得及び保存の手順を定めた上で、ログを定期的にレビューしていますか？	○	ログ取得及び監視の対象を定め、改ざん防止のためにアクセス権限を定期的に管理しています。
	重要なITシステムに脆弱性がないか、専用ツールを使った技術的な診断を行うことがありますか？	○	利用サーバーについて脆弱性の有無を定期的に確認しています。
	ファイアウォールなど、外部ネットワークからの影響を防ぐための対策を導入していますか？	○	ファイアウォールを有効化し、外部ネットワークからの予期しない接続を阻止しています。
	業務で利用しているネットワーク機器のパスワードを初期設定のまま使わず、推測できないパスワードに変更して運用していますか？	○	パスワードの生成ルールを定め、複雑で推測されにくいパスワードを使用しています。パスワード管理には、専用ソフトウェアを利用し、厳重に管理しています。
	クラウドサービスなどの社外サーバーを利用する場合は、費用だけでなく、情報セキュリティや信頼性に関する仕様を考慮して選定していますか？	○	外部の委託先システムの利用にあたっては、ISMS認証の取得状況や障害対策について評価を行っています。
	最新の脅威や攻撃についての情報収集を行い、必要に応じて社内で共有していますか？	○	情報セキュリティ支援サービス「Seculio」を利用し、自動的に最新情報を収集しています。必要に応じて社内向けの情報共有ツール上で共有しています。
⑧システム開発及び保守	情報システムの開発を行う場合、開発環境と運用環境とを分離していますか？	○	開発環境、運用環境の分離ルールを定め、誤認して操作しないようにしています。
	セキュリティ上の問題がない情報システムを開発するための手続きを定めていますか？	○	セキュリティ要求事項を検討し、定期的にレビューを行いながら開発することを定めています。
	情報システムの保守を行う場合、既知の脆弱性が存在する状態で情報システムを運用しないようにするための対策を講じていますか？	○	利用サービスにおける脆弱性の有無について最新情報を自動収集するとともに、定期的にセキュリティチェックを実施しています。
⑨委託管理	契約書に秘密保持（守秘義務）、漏洩した場合の賠償責任、再委託の制限についての項目を盛り込むなどのように、委託先が順守すべき事項について具体的に規定していますか？	○	委託先管理ルールを定め、遵守事項について記載しています。
	委託先との秘密情報の受渡手順を定めていますか？	○	秘密情報を含む媒体の輸送方法について定めるとともに、電子メールの利用ルールを定め、運用しています。
	委託先に提供した秘密情報の廃棄または消去の手順を定めていますか？	○	廃棄手順を定め、運用しています。
⑩情報セキュリティインシデント対応ならびに事業継続管理	秘密情報の漏えいや紛失、盗難があった場合の対応手順書を作成するなどのように、事故の発生に備えた準備をしていますか？	○	セキュリティインシデント発生時の対応手順を定めています。
	インシデントの発生に備えた証拠情報の収集手順を定め、運用していますか？	○	利用する各サービスでログを収集しています。
	インシデントの発生で事業が中断してしまったときに再開するための計画を定めていますか？	○	情報セキュリティの観点から復旧対象とそれぞれの要求レベルを定め、復旧手順を整備しています。必要な人員への緊急連絡網を整備するなど、定期的に事業継続試験を実施しています。
⑪個人番号及び特定個人情報の取り扱い	個人番号及び特定個人情報の取り扱いルール（管理担当者の割当て、収集・利用・保管・廃棄の方法）を定めていますか？	○	個人情報保護法に準拠し、個人情報の取り扱い方法について定めています。
	個人番号や特定個人情報に関する漏えいなどの事故に備えた体制を整備していますか？	○	セキュリティインシデント発生時の対応手順を定めています。
	個人番号や特定個人情報の安全管理についてルールや手段を定めていますか？	○	個人情報保護法に準拠し、個人情報の取り扱い方法について定めています。