新型コロナウイルス（COVID-19）

リモートワーク環境の安全性は十分ですか？

世界中がCOVID-19パンデミックと対峙する中で、多くの企業は新たな働き方への迅速な対応を余儀なくされています。世界中の人々は、広範囲にわたる制約条件のもとで、在宅勤務（Working from Home）および緊急時の事業継続拠点から業務を遂行するという課題に取り組んでいます。この混乱に対応するため、多くの企業がリモートアクセスソリューション、リモートコラボレーションツール、クラウドサービス等の機能を活用しています。また、いくつかの企業は、社員が個人所有の端末を使用することを許可しており、長期間にわたる自宅ネットワークの使用が可能になっています。

反社会的勢力等の一部の組織化された犯罪グループは、COVID-19によって引き起こされた恐怖と不確実性の種を利用する機会を狙っています。そして、リモートワークの勤務条件に関連するコントロール（リスク低減を目的とする統制活動）の欠陥を利用して、多種多様な方法で個人および企業を標的にしています。

KPMGは、10のリスク領域における主要なコントロール項目を整理しました。

リモート接続の安全性

リモートアクセスポリシーの認識	リモートアクセスに関連するユーザーガイドラインとセキュリティのベストプラクティスを定義していますか？
特権アカウント管理	特定のビジネスロールに基づき、ユーザーにリモートアクセス権限を割り当てていますか？
安全で暗号化されたアクセス	リモートアクセスシステムでは、最高水準のセキュリティプロトコル（※）を構成していますか？ ※ポイントツーポイントトンネリングプロトコル（PPTP）、レイヤー2トランスポートプロトコル（L2TP）
ネットワークトラフィックのフィルタリング	特定のプロトコルとポート番号に基づいてネットワークトラフィックを制限できていますか？
2要素認証	リモートアクセスを許可しているシステムでは、最低でも2要素認証を有効にしていますか？ 注：多要素認証（Multi-Factor Authentication）システムを使用すると、セキュリティが向上します。
脆弱性管理	脆弱性およびパッチを定期的にチェックする脆弱性管理プロセスは存在しますか？また、リモートアクセスを利用する社員のデバイスでは、ファイアウォール保護が有効になっていますか？

セキュリティ監視	リモートユーザーの監査ログ、管理ログ、トランザクションログの厳密な監視を設定していますか？
スプリットトンネリング	企業VPNを介して接続されているリモートユーザーのスプリットトンネリングを無効にしていますか？
VPN帯域幅の評価	多数のVPN接続を処理するために必要な、十分なVPN帯域幅を確認するための事前ストレスチェックを実行していますか？
リモートアクセスにおける境界セキュリティ	内部ネットワークから分離された境界デバイスにおいて、リモート接続を強制終了していますか？

リモートコラボレーションツールの安全性

ガバナンス管理	コラボレーションツールの使用（ファイル保管のポリシー、メッセージの削除、コンテンツの取得など）に対する適切なガバナンス管理方法を定義していますか？
ツールへのアクセス	ブラウザベースの攻撃を防ぐために、ブラウザではなくシッククライアント（※）を介してコラボレーションツールへのアクセスを提供していますか？ ※シッククライアント（Thick Client）：アプリケーションソフトやデータなどを、物理PCに備えた状態で利用する形態を指す。シンクライアント（Thin Client）の逆の意味。
VPNによるアクセス	社用VPNを介してのみ、コラボレーションツールへのアクセスを有効にしていますか？ VPNへのアクセスの際、多要素認証（Multi-Factor Authentication）を必須としていますか？
汎用URLの利用	ブラウザベースでのアクセスの際、組織内リンクについては、組織内部の詳細を明らかにする可能性がある名前（companyname.app.comなど）ではなく、一般的な名前で構成されていますか？
自動プレビューの無効化	ネットワーク経由での機器のIP漏洩を回避するために、コラボレーションツールのリンクを介して共有された画像の自動プレビュー機能を無効にしていますか？
ハイパーリンクの無効化	フィッシング攻撃を減らすために、インスタントメッセージを介してハイパーリンクを無効にするポリシーを適用していますか？
アイデンティティおよびモビリティ管理	インストール済みアプリケーションの整合性チェックとともに、適切なIDおよびモビリティ管理制御（SAML認証、SSO、エンタープライズモビリティ管理など）を備えたコラボレーションツールを設定していますか？
データセキュリティ	内部および外部でのドキュメント共有の制限、DLP（Data Loss Prevention：情報漏洩防止）を使用した管理されていないデバイスへのアクセスのブロックなど、コラボレーションツールで適切なデータセキュリティ管理を有効にしていますか？
ログ取得およびモニタリング	ファイルのダウンロード・アップロード、不正アクセスの試みなどに関するインシデントと調査を管理するために、各コラボレーションツールのログ取得およびモニタリングのコントロール（リスク低減に向けた統制）を設定していますか？
トレーニングの実施およびセキュリティ意識の向上	コラボレーションツールの使用および関連するセキュリティの考慮事項について、社員向けのトレーニングを実施していますか？（例：グループのミーティングに招待することができるメンバーの特定）

モバイル端末に対するセキュリティ設定の適切さ

MDMソリューション	モバイルデバイス管理（MDM）ソリューションを使用して、企業のデータにアクセスできる個人用および社用デバイスを管理していますか？
ユーザー認証	企業のデータにアクセスできるデバイスに画面ロックパスワード／PINなどの強力なユーザー認証を設定していますか？
重要なユーザー設定	自動入力の無効化、自動デバイスロックアウトの有効化、信頼できるアプリストアからのみアプリケーションのインストールを許可するなどの重要なセキュリティ設定を実行していますか？
盗難防止対策	BYOD（Bring Your Own Device：私有デバイスの業務活用）および社用デバイスでの安全なリモートワイプなど、盗難対策を実施していますか？
ストレージ暗号化	デバイスが盗難された場合、デバイスに保存されている企業のデータにアクセスできないようにするため、モバイル端末のストレージメディアの暗号化を実施していますか？
マルウェア対策	マルウェアから保護するために、BYODおよび企業所有のデバイスにマルウェア対策ソリューションを導入していますか？
セキュリティ更新	最新のセキュリティパッチを適用してモバイル端末を最新の状態に保つように、すべての社員へ通知していますか？また、無線（Over The Air）配布機能を設定して、セキュリティおよびその他のソフトウェアアップデートをリモートでプッシュ配付していますか？
旧バージョンOSの利用制限	旧バージョンのiOSおよびAndroidオペレーティングシステムが、企業リソースへのアクセスを許可されていないことを確認していますか？
ルート権限（管理者権限）を有効化されたデバイスの制限	MDMでポリシーを構成し、ジェイルブレイクされたデバイスやルート化されたデバイスをチェックして、企業リソースへのアクセスが許可されていないことを確認していますか？
ネットワーク・USB接続等のセキュリティ	外部デバイスへの接続（Wi-Fi、Wi-Fi Direct、Bluetooth、Hot Spot、USB、USB OTGなど）が制限され、適切に保護されていることを確認していますか？
データのバックアップ	モバイルデバイスに保存されている重要なデータは、定期的にバックアップされていますか？

PCに対するセキュリティ設定の適切さ

最小権限の原則	職務分掌に基づいて、管理者権限アカウントの利用を数名の社員のみに制限していますか？
強力なアカウントポリシー	すべての社用PCにおいて、強力なパスワードポリシーに基づき、パスワードを設定していますか？（例：複雑なパスワード、8～12文字の最小桁数、最短および最長の有効期間など）。
パスワード保護されたスクリーンセーバー	すべての社用PCにおいて、パスワードで保護されたスクリーンセーバーを適用していますか？
VPNによるリモートアクセス	会社指定のVPN接続を必須としたうえで、社用アプリケーションへのアクセスを設定していますか？
エンドポイント向けのセキュリティソリューション	すべての社用PCにおいて、エンドポイント向けのセキュリティソリューションを導入していますか？ 例：会社が提供するすべてのラップトップのウイルス対策およびDLP（Data Loss Prevention：データ損失防止）

リムーバブルメディアの制限	会社のデータ重複を防ぐために、USBデバイスなどのリムーバブルデバイスの使用を制限していますか？
ハードディスクの暗号化	暗号化ソリューション（ビットロッカーなど）を使用して会社が提供するすべてのラップトップにハードディスク暗号化を適用し、OS起動時のセキュリティ対策として利用していますか？
定期的なバックアップ	企業のITポリシーでは、オンラインのデータバックアップソリューションを介して、すべての社用PCにおいて定期的なバックアップを実施していますか？
ウェブカメラからの保護	社員のプライバシーがトロイの木馬による意図しないビデオキャプチャから保護されるように、会社が提供するすべてのラップトップにWebカムカバーを提供していますか？
ワイヤーロックによる施錠	会社の機材とデータを物理的に保護するために、すべての社用PCにワイヤーロックを提供していますか？

クラウド上のワークロード（独立した業務単位）の安全性

IAM（アイデンティティおよびアクセス管理）：認証	多要素認証を使用してクラウドワークロードを保護していますか？
IAM（アイデンティティおよびアクセス管理）：ユーザーアクセス制御	承認されたユーザーのみが、クラウドデータおよびアプリケーションにアクセス可能なアクセス制御を実装していますか？
IAM（アイデンティティおよびアクセス管理）：特権アクセス	特権アクセスを保護するための追加のコントロールを実装していますか？ 例：条件付きアクセス制御、ジャストインタイム
IAM（アイデンティティおよびアクセス管理）：悪意のある動作の識別	セキュリティ侵害されたアカウントおよびインサイダーの脅威を検出して、悪意のあるデータの漏洩を回避できていますか？
情報保護：データ分類	許可されたデータのみがクラウドワークロードに入ることを確認するためのデータ分類および処理ポリシーがありますか？
情報保護：DLP（データ損失防止）	データ分類スキーマに基づいて、データを漏洩から保護するためにクラウド上のDLP（データ損失防止）ソリューションを実装していますか？
情報保護：暗号化	クラウド上のデータ暗号化を使用してデータが盗まれた場合でもデータへの不正アクセスを防止していますか？
ネットワークセキュリティ：境界	適切な境界セキュリティ制御を実装していますか？ 例：DDOS保護、WAF、ファイアウォール
ネットワークセキュリティ：分離	クラウドワークロード間で許容されるトラフィックのみを確保するために、適切なネットワーク分離グループ化を実装していますか？
ネットワークセキュリティ：セキュアなプロトコル	クラウドワークロードにアクセスする際に、ネットワーク層（TLSなど）およびアプリケーション層（IPSEC、SSH、SSLなど）において安全な通信プロトコルを使用していますか？
ATP（高度な脅威保護）	既知の技術による検出と行動分析の両方で、疑わしいユーザーとデバイスのアクティビティを特定するためにATP（高度な脅威保護）の制御を設定していますか？

リスクが高いプロセスに対するリモート監督の方法

センシティブな運用業務の計画	センシティブな操作をリモートで管理するための手順を文書化していますか？ 例：現金管理、ローン処理、電信送金、コールセンター業務
クリティカルなシステムへのアクセス	承認されたビジネスユーザーおよび管理者のみが、照合、顧客対応などのビジネスプロセスを実行するためのリモートアクセス権を持っていることを確認していますか？
メーカーとチェッカー	監視の仕組みを定義して、メーカーとチェッカーの制御がリモートの作業条件で効果的に動作していることを確認していますか？
特権アクセス管理	特権アクセス管理（Privileged Access Management）ソリューションを使用して、管理者特権を持つユーザーのリモートアクティビティを制御していますか？
人員不足への対応	相当数の欠勤が発生した場合、メーカーとチェッカーのコントロールをどのように確保していますか？
変更承認のワークフロー	リモートでの本番環境および重要なプロセスへの不正な変更を防ぐために定義された変更承認ワークフローは存在していますか？
システム利用不可時の対応	主系システムが利用できない場合に社員が従うべき代替プロセスを確立したうえで、社員に伝達していますか？
データ漏洩防止	リスクの高いプロセスをリモートで実施しているユーザーによるデータ漏洩からデータを保護するために、DLP（データ損失防止）のソリューションを導入していますか？
不正監視	不正を検出して阻止するために不正監視システムを使用していますか？
セキュリティ監視	サイバーセキュリティ警告のリアルタイム分析およびサイバーセキュリティインシデントの管理を目的に、サイバーセキュリティ監視システムを導入していますか？

サプライヤーの混乱が危機管理計画に与える影響度合い

地理的な制約	継続性の取組みに影響を与える可能性のある地域の混乱を予測するために、サプライチェーン全体を把握していますか？
サプライヤーの継続性	危機管理計画は、継続性の取組みにおいてどのように活用できるか、主要ベンダーおよびサプライヤーと話し合いましたか？
サプライヤーの連絡先	主要ベンダーおよびサプライヤーと、緊急時に使用できる連絡窓口と連絡方法を整備していますか？
サプライヤーのリモートワーク能力	リモートワーカーをサポートする主要ベンダーとサプライヤーの能力（オンラインのコラボレーションツール、ビデオ会議、クラウドベースのソリューションなど）を評価していますか？
緊急時を想定した契約条項	既存の契約、主要ベンダーおよびサプライヤーとの関係により、緊急の場合に備えて、追加のキャパシティとサポートを要求できていますか？
代替ベンダーおよびサプライヤー	状況の変化により主要ベンダーおよびサプライヤーが混乱した場合、どのように運用を管理していますか？また、ベンダーやサプライヤーの多様化について検討していますか？
追加の機器のニーズ	リモートの労働条件をサポートするために必要となる追加の機器を調達するための要件には、どのように対処しますか？
主要機器の予備	リモートの労働条件をサポートするために必要となる可能性のある主要機器の予備はありますか？ 例：追加のPC、携帯電話
ベンダーとサプライヤーの依存関係	独自のリソースの使用など、依存関係を減らすために実行できる手順はありますか？
短期および長期計画	サプライチェーンの混乱に対処するための短期的な計画（短期間の正常性の回復）と、長期的な計画（長期的なパンデミック状況）がありますか？

職場環境におけるウイルス感染（COVID-19等）に対する保護策

感染予防の計画	COVID-19等のパンデミックに対処するために、包括的な感染予防の計画を整備して、社員に伝えていますか？
意識向上	職場内に、適切な衛生管理のガイドラインに関するポスター等を掲示していますか？
人員の安全	COVID-19等の感染拡大を最小限に抑えるために、社員に在宅勤務を勧めていますか？また、症状が出た場合は早急に医師に相談するように伝えていますか？
熱探知カメラ	職場への訪問に対して、熱探知カメラ、マスク着用等の感染防止対策を実施していますか？
職場での体温モニタリング	オフィス内の社員の体温を測定するために、ハンドヘルド温度計等を設置していますか？
執務エリアおよび各種表面の清掃・消毒	執務エリア、飲食スペース、トイレ、およびドアノブ、カウンター、照明スイッチ、エレベーターボタンなどの頻繁に手で触れる表面については、定期的な清掃・消毒を実施していますか？
換気・空調	換気、空気浄化、および空調（HVAC）設備は、職場内で適切に機能していますか？
衛生用品	社員に対して、手指の消毒アルコール、ティッシュペーパー、マスク、手袋などの適切な衛生用品を提供していますか？

職場の清掃	社員が使用するデスクおよびコンピュータは、定期的な清掃・消毒を実施していますか？
廃棄物処理	廃棄物は、衛生的な方法で適時処分されていますか？

リモートワークの条件に関する関係者（クライアント、社員等）への効果的なコミュニケーションの実施

リモートワークのポリシー	現状のリモートワーク実施条件を踏まえた、情報セキュリティポリシーの変更を関係者へ伝えていますか？
コミュニケーション計画	サイバーセキュリティインシデントに関連する内部および外部の通信を管理する目的で、明確なコミュニケーション計画を整備しましたか？また、セキュリティ違反が発生した場合に関連する連絡先情報を社員／顧客に提供していますか？
通信のインフラ	リモートワーク実施時の状況をサポートするために、公式の通信チャネルを設置していますか？
危機管理チーム	中核的な職責を持つ上級リーダー等で構成される危機管理チームは存在していますか？
フェイクニュース	COVID-19に関連するニュースまたは情報を、回覧または処理する前にどのように確認していますか？
フィッシング攻撃	COVID-19に対する恐れを利用した最新のフィッシングメールについて、社員向けにリフレッシャー・セッション（最新動向の把握を目的とした研修および意識付け等）を実施していますか？
詐欺行為	詐欺グループが政府職員等を装い、電話を介してまたは直接訪問する形で個人データを求めてくる可能性がある、という意識を社員が持てるような取組みを実施していますか？
リモートワークでの安全対策	リモートワークにおけるベストプラクティスについてリフレッシャー・セッションを実施していますか？ 例：公共Wi-Fiを使用しない、放置された機器を物理的に保護する、個人の仕事で社用PCを使用しない
データの取扱い	リモートワーク実施時のデータの取扱い方法について、社員に明確なガイダンスを提供していますか？
顧客向けの情報提供	安全なインターネット慣行や最新のCOVID-19関連のサイバー脅威について、顧客とコミュニケーションを取っていますか？

サイバーおよび情報セキュリティインシデントへの対応計画の整備

COVID-19による新たな脅威	セキュリティオペレーションセンター（SOC）は、最新のサイバー脅威を継続的に監視していますか？ 例：グローバルに登録されているCOVID-19に関連する新しい600以上のドメイン
インシデント対応計画	インシデント対応計画を更新して、在宅勤務などにより蔓延している最新のサイバー攻撃に対応していますか？また、同計画の有効性についてテストを実施しましたか？ 例：標的型フィッシングメール、ランサムウェア、VPNデバイスへのDDOS
インシデント対応ガバナンス	パンデミックを考慮して、サイバーセキュリティインシデントを管理するための適切なガバナンスメカニズムを整備していますか？
代替SOCの配置	現状のパンデミックを考慮したうえで、代替SOCを探す必要性を検討していますか？ 例：主要なMSSP（Managed Security Service Provider）リソースの損失、MSSPからの十分なネットワーク帯域幅の不足
インシデント報告のチャネル	在宅勤務中に特定できるサイバーおよび情報セキュリティインシデントを報告する際、適切な報告チャネルを社員は知っていますか？
PCおよびモバイル端末のインシデント対応	SOCの監視およびインシデント対応計画は、エンドユーザーの機器を対象範囲に含めていますか？（例：PC、モバイル端末）
クラウドサービスのインシデント対応	SOCの監視およびインシデント対応計画は、クラウドのワークロードを対象範囲に含めていますか？
リモートコラボレーションツールのインシデント対応	SOCの監視およびインシデント対応計画は、リモートコラボレーションツールに対応していますか？
サイバーセキュリティ調査	在宅勤務中にエンドユーザーの機器からサイバーセキュリティインシデントのデータを特定、収集、保存するための手順を整備していますか？
インシデントからの復旧	ビジネス要件と照らし合わせて、影響を受けるサービスの適切な復旧方法を整備していますか？
インシデント発生後のレビュー	同種インシデントの再発を防ぐために、インシデント発生後のレビューを実行したうえで、学んだ教訓を文書化していますか？

Contacts

KPMGコンサルティング株式会社

03-3548-5111
kc@jp.kpmg.com

home.kpmg/jp/socialmedia

本冊子は、KPMGインターナショナルが2020年4月に発行した「COVID-19 How secure are your remote working arrangements?」を翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

Designed by KPMG Lower Gulf Creative team.
Publication number:
2756 Publication
date: April 2020