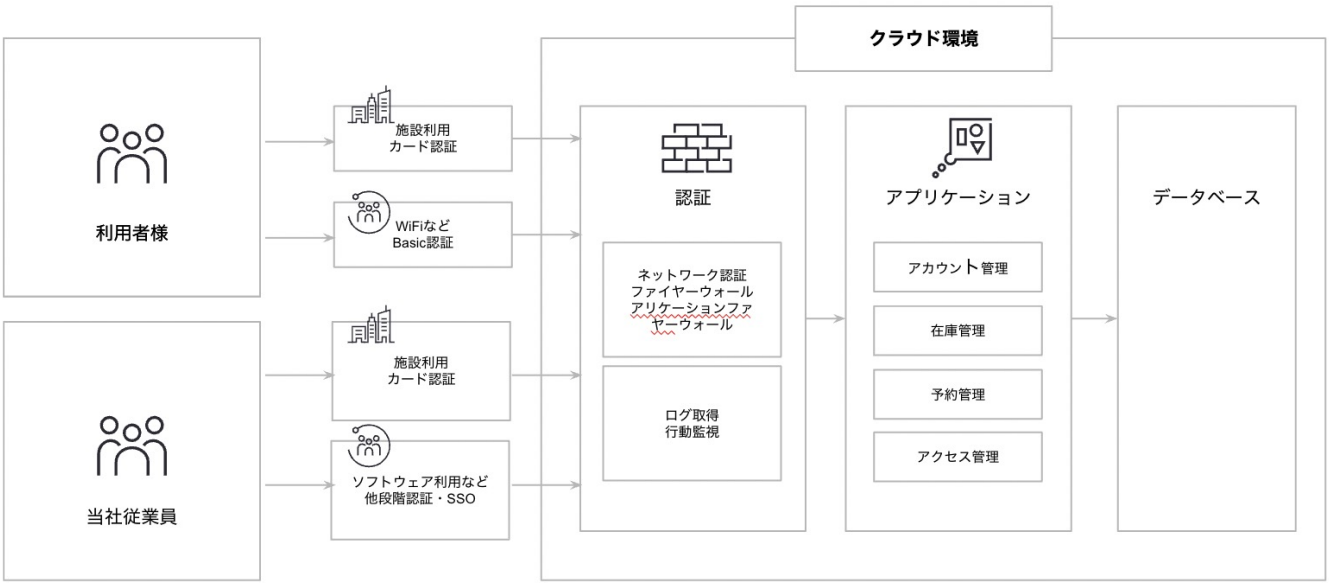
８９８：;<＋ ， － ． ／ ０１７＝＞？@

ＶＷＸＹＺ［ ｌｍ

Wework Japanでは、セキュリティ施策を「体制面」「運用面」「システム面」に分類し、以下のような対策を講じています。



ＶＷＸＹＺ［ ｌｍ（ ｎｏ

組織・体制	運用・管理	システム
セキュリティ対策プロジェクトでの全社的対応の実施	外部委託会社や利用SaaSサービスのセキュリティチェック実施	SSO＋CASB認証によるアクセス管理
情報管理ガイドラインの制定	セキュリティの外部監査（年次実施）	ネットワーク通信環境の冗長化
ISO27001の取得	入社時のセキュリティ教育、年２回のセキュリティ教育	WiFi通信は強力な暗号化プロトコル＋RADIUS認証の採用
日本国個人情報保護法、GDPRに準拠した個人情報管理体制	WEBサイトの脆弱性診断	エンドポイント端末に対するサイバー攻撃者の常時モニタリング
パスワードポリシーの徹底	セキュリティインシデントやシステム障害への対処手順を確立	メールの送受信監視
セキュリティ区画への物理的なアクセス制限	ログ監視・保存	HDD他保管デバイスの暗号化
入室履歴管理の実施	パッチマネジメントによる脆弱性対策	WAFの導入
来訪者に対するインビテーション発行、受付での人的チェック		悪意のあるWEBサイト閲覧制限
入居者の審査		強力なFirewall/IPS/UTM利用
セキュリティカメラ運営（録画映像はネット上での閲覧不可）		DDoS対策の導入

WeWorkのセキュリティ方針と施策

オフィスの入退室管理

WeWork Japanでは利用者および従業員の取り扱う情報に応じて、オフィス内を区画で切り分けて管理しています。

全エリア共通

利用者・従業員が利用可能な範囲を個人単位で管理・制限できるようにし、執務エリアは施錠可能なドアを設置しています。ロックの解除にはセキュリティカードが必要となり、本カードには個人と紐づけられた情報管理により入室のログが管理システムに記録されます。

特定エリア

ネットワーク機器などの設置されたサーバールーム、多くの個人情報を取り扱うエリアは、特定の業務を行うもののみ入室可能としています。

コミュニティエリア

ゲストなどを受け入れる区画として整備されており、WeWork Japan従業員が常駐する時間は制限なく入退室可能としてゲストの登録を行なっています。時間外については他のエリアと同じ入退室制限を行なっています。

エンドポイント管理

WeWork Japanでは、従業員の利用するすべての端末に管理ソフトを導入し一括管理を行なっており、ウィルス対策ソフト、バックアップ、エンドポイント検知・対応の実施およびログの取得により、端末上の操作の記録、プログラムの実行や情報の閲覧など、インシデントが発生した際に原因の究明や対応が行える体制をとっています。

オフィス、自宅など働く場所を選ばないフレキシブルな働き方を推進する上で、端末の紛失や盗難に対応するために個人情報の取扱いを最低限にするとともに、できるだけクラウドでの情報保管することを推進しています。また、万が一の紛失・盗難に際しては、外部から情報を消去できる仕組みを導入しています。

また、USBメモリなどの可搬性の記録媒体については、利用できないように制限をしています。ただし、業務上可搬可能な記録媒体が必要な場合には暗号化が可能な媒体を会社で用意しており、申請をもとに従業員に貸与して利用する措置を講じています。

WeWorkのセキュリティ方針と施策

アカウントの認証

WeWork Japanでは多くの業務をクラウドで行われており、クラウドへの高度なアクセス管理とアカウントの認証を導入しています。従業員に対しては１つのIDを発行し業務に必要なサービスへアクセスをしています。アクセスに際しては、多要素認証を必要とするシングルサインオンおよび認証を一括管理するCASB（Cloud Access Security Broker）を導入しています。

ネットワーク、認証およびアクセスログなどを取得しており、アカウント単位でのログによりだれがいつどこでどのような作業を行ったのか追跡可能な体制としてます。共有アカウントの利用は原則利用不可とするとともに、不要なアカウントは従業員の退職などにあわせて即時に無効化されます。

ログ取得と調査体制

セキュリティの動的な把握およびインシデントの防止・調査のために、端末、ネットワーク、クラウドサービスなどのログを、専用のログ管理システムにおいて常時管理の上、最低でも6ヶ月以上保管しています。

また、監視カメラの情報についても保管の上で、関連する業務に従事する社員のみアクセス可能な区画で管理しています。

ログなどの情報はお客様および社員の個人情報を含む可能性があるため、当該入居者の入退室情報など一部有償でご提供している情報を除いて、外部には提供しておりません。

ネットワークの管理

ネットワークはファイアーウォールでの安全性を確保するとともに、拠点・フロア単位で分割、メンバーの利用するネットワーク、ゲストネットワークを分離などを行うことで影響が限定される仕組みを採用しています。また、ネットワークの脆弱性情報を収集し、収集した情報を元にサービスへの影響を評価し、影響がある場合には速やかに対応します。
WeWorkではネットワークのトラフィックなど運用を監視していますが、そのコンテンツを見ることはありません。メンバーは有償VLANの利用や自社契約でのVPNを活用するなどさらにセキュリティを向上させる手段を講じることが可能です。

WeWorkのリスク管理

WeWorkの社内体制

WeWork Japanではセキュリティ専任部署を設置せずに、全部門が連携することで取り組みを進めることとし、その取りまとめを社長直轄で行っています。セキュリティ対策は、情報システム部門が主導することが多いものですが、当社ではこのように社長直轄のチームを中心にクロスファンクションでの対応を行うことで、情報や対応のサイロ化せずに対応することを目指しています。

パートナーとの連携

常に新しいリスクが発生する情報セキュリティに関しては、アップデートされ続けるセキュリティ情報を理解して対策を行うことが重要ですが、世界でも日本でも、専任のセキュリティ人材の採用は難しく、継続的な教育も困難という状態です。

最新のセキュリティの知見を入れるため、自社内で採用・教育も重要ではあるものの、専門性は外部のパートナーと連携により、より高い安心・安全の提供を目指しています。

WeWork Inc

WeWork Japanは米国のWeWork Incが定めるルールや対策に準じたサービスを提供しております。同時に、日本国内のネットワーク・セキュリティ基準及び法制に対応して、WeWork Incと調整の上で日本において最適なセキュリティを適用しています。

ソフトバンク株式会社

WeWork Japanはソフトバンク株式会社の子会社であり、ソフトバンクのセキュリティ対策や基準およびアセスメントなどを通じて日本においての高いセキュリティ基準と対応を理解し、導入を行なっています。

株式会社CISO

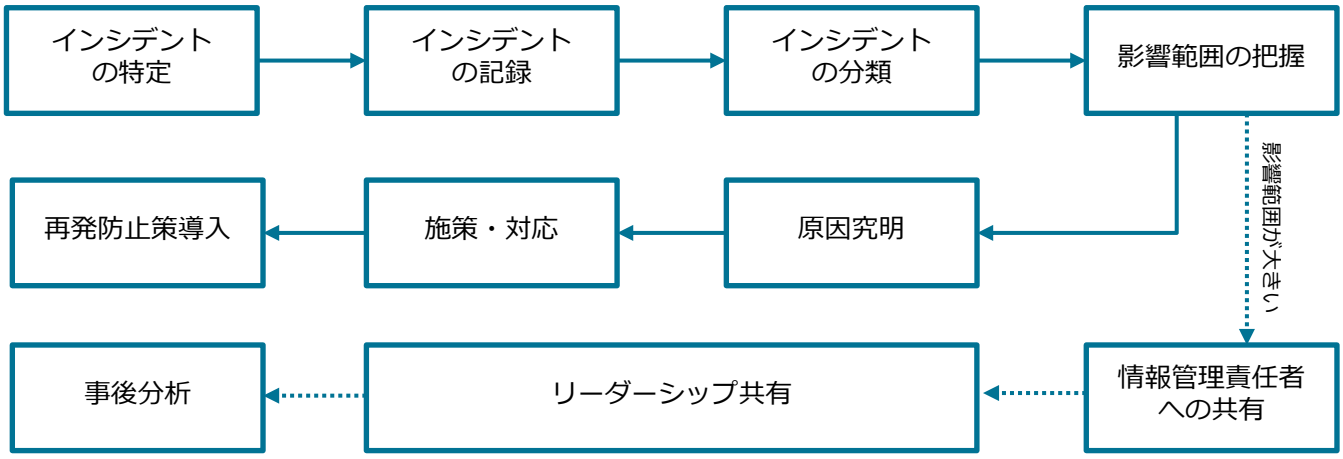
中堅・中小企業専業のセキュリティ支援会社である株式会社CISOが保有する「CISOセキュリティ診断」を活用。この診断プログラムは、セキュリティリスクを７つのカテゴリに分類し、中堅・中小企業にとって重要なセキュリティ施策を「外部からのサイバーセキュリティ対策」「内部情報漏洩などの情報セキュリティ対策」「BCPや物理的なセキュリティ対策」「組織ならびに人的なセキュリティ対策」の４つの観点でリスク判定。結果を数値でスコアリングし、具体的な取り組み施策までをわかりやすく提示するものです。

中堅・中小企業のスタートアップ企業も多数入居するWeWork Japanは、本診断も合わせて活用。スタートアップ企業に求められるセキュリティ対策の重要ポイント（勘所）をWeWork Japan自らが理解した上で、入居企業様にとって必要となるセキュリティ施策を構築しています。

WeWorkのリスク管理

インシデント対応

お客様・WeWork Japanのビジネスへ影響を及ぼすインシデントが発生した場合、早期に発見し、関連する組織が原因の究明と対応を行うこと、同時に、対応する手段を事前に準備しているかがリスクを最小化するために必要となります。そして、再発防止策を実施して同様の問題の発生を防止することが必要です。WeWork Japanはリスクへの対応を規定化するとともに、インシデントをデータベースとして記録し、リーダーシップが共有することで、より効果的なリスク対応を推進しています。



従業員の教育

WeWork Japanでは入社時にリスク、非常事態への対応、情報管理についてのトレーニングを行うとともに、毎年eラーニングにより対処が必要な経緯と背景を含めて学習することで、基礎的な知識と心構え、日々の業務においての遵守事項を身につけることを目指しています。

同時に、近年多発するフィッシングなどの手法に対応するために、シミュレーション型の演習を定期的に実施することで、リスクの理解と対応方法が徹底を推進しています。

さらなる安心・安全に向けて

入居者に安心安全な環境を提供

WeWork Japanの入居者様は、セキュリティ対策が適用されてる旨を外部の取引先企業様などにも提示いただけます。

WeWork Japanとご提供できる基礎部分を構築してきました。この先は入居企業とともに、外部の協力も得ながら一層のセキュリティ対策を進めていく方針です。Weworkは、世の中の変化に合わせて、より快適なスペースを提供するのみならず、セキュリティ体制や運用面でも、柔軟性を持って進化を続けて参ります。

また、入居企業様にとって、これからもより安心・安全にご利用いただくための「セキュリティ運用支援」等のサービス提供を行って参ります。

セキュリティ運用支援サービス（有償）

入退室ログの提供

追加のカードセンサー、監視カメラ

セキュリティ相談窓口

セキュリティ診断、EDRサービスの提供

セキュリティ教育支援

上場に向けたセキュリティ整備の相談

最後に

本書がWework Japanのセキュリティの取り組みについて少しでも理解の一助となれば幸いです。

本資料についてのお問い合わせはWeWork Japanウェブサイトの「お問合せ」までお願いいたします。また、個人情報の管理などは以下をご参照ください。

WeWork Japan ウェブサイト	https://wework.co.jp/
WeWork Japanのご紹介	https://wework.co.jp/brand
個人情報の取扱い	https://wework.co.jp/legal/privacy-policy

wework