wework

セキュリティ ホワイトペーパー

2023年5月

もくじ

はじめに

ホワイトペーパーの対象範囲

本セキュリティホワイトペーパーは、特に注釈などがない限り、WeWork Japan合同会社に関する事項のみを取り扱っています。

WeWorkとは

2010年に米・ニューヨークで創業したWeWork は、世界39か国・150都市以上・800拠点以上、国内約40拠点でフレキシブルオフィスを展開しています。WeWork Japanは、2018年2月に国内初となる拠点を東京で開設。創造性や生産性が高まる空間デザインを用いたワークスペースにおいて、月単位での契約、1名から数百名規模の拡大・縮小や、国内30拠点以上の横断的な利用が可能なプロダクトや、柔軟なオフィスソリューションを提供しています。

WeWorkのミッション

つながりは楽しさに。 つながりは自信に。

ここにいること。それがあなたを成長させる。
場を貸してるだけではない、空間であなたを迎えている。
あなたの可能性に、わたしたちもコネクトする。
つながりは、変化と創造を先進的に誘なうでしょう。
WeWork で変化することは、私たちの未来を創造すること。

企業と人、人と人をつなげる空間を提供するプロパティテックの企業として入居者様と共に成長を続けるために、入居企業・利用者が快適に過ごせるよう、以下をお約束します。

・デザイン性のある空間スペース
・人と出会うためのコミュニティスペース
・安定的なインフラ環境の提供
・利便性と柔軟性を兼ね備えた環境整備

そして、「利便性と柔軟性を兼ね備えた環境整備」の一環として、セキュリティ対策も充実させております。

わたしたちのセキュリティに関する考え方

WeWork Japan入居者に安心安全な環境を提供する

日本の社会インフラとしての通信環境を提供するソフトバンクの関連会社として、WeWork Japanには「安定した環境を提供する」という価値観が踏襲されています。フレキシブルオフィスを提供するプロパティテック企業である私たちは、利用する皆様に安心・安全な環境を提供し続けます。その中でも特に「高いセキュリティのもとで、安心・安全に事業を行っていただく」ことは、最重要事項として位置付けています。

サイバー攻撃などによって突発的に事業が停止するようなリスクを排除し、安心して業務に集中いただける環境を提供し続けることは、WeWork Japanを選んでいただくための大きな価値の一つです。

また、入居企業様の先にいる取引企業様に「WeWork Japanに入っているんだからセキュリティ面は安全だね」と認識いただける環境を提供することは、WeWork Japanが入居企業さまのビジネスに直接貢献できる価値の大きな一つとして今後も取り組みを続けていくことをお約束いたします。

セキュリティポリシー

WeWork Japanはセキュリティに関する取り組みを情報管理規定として文書化しています。情報管理の基本的な指針と、それを実現するための個人情報保護のための規定、拠点の設備などの規定によりお客様への安心・安全な情報を提供を目指しています。

また、入居者様、ご利用者様、取引関係者様、従業員・派遣社員・出向社員・採用応募者等、その他のあらゆる個人の皆様（以下併せて「お客様」といいます。）の個人情報の重要性に配慮し、お客様の個人情報を適切に保護することで、お客様の信頼を維持するよう努めています。

当社は、以下の各定めに基づき（但し、グローバルプライバシーポリシーについては、日本国の法令・規制により一部制限される場合がございます。また、グローバルプライバシーポリシーの中の「ユーザー」という記載は「お客様」と読み替えるものといたします。グローバルプライバシーポリシーと本ページに記載する内容に異なる部分がある場合には、本ページの記載が優先されます。）、お客様の個人情報を、細心の注意をもって管理してまいります。

グローバルプライバシーポリシー

個人情報保護方針

海外に所在する企業への個人データの移転

わたしたちのセキュリティに関する考え方

wework

情報セキュリティ基準

お客様のために必要な取り組みとして、WeWork JapanはCIS IG2の基準をクリアしたセキュリティ対策を講じています。

CIS IG2は、米国のセキュリティ非営利団体であるCenter for Internet Security® (CIS®) 主導の下、セキュリティの具体的な対策とその対策レベルが規定され、グローバル含め多くの企業で採用されているガイドラインです。

IGはImplementation Groupの略で、取扱っている情報の重要度、企業規模、サイバーセキュリティ体制などを考慮した企業の状況に応じてCISでは「IG1」「IG2」「IG3」の３グループに分かれています。WeWorkは、重要度の高い情報も取り扱っており、サイバーセキュリティに取り組む体制が一部整っている中規模組織として「IG2」を指針としています。

外部の監査機関の監査を通じて、以下の18カテゴリをチェックしています。

１８のコントロール					
01	組織と資産のインベントリと管理	07	継続的な脆弱性管理	13	ネットワークの監査と防御
02	ソフトウェア資産のインベントリと管理	08	監査ログ管理	14	セキュリティ意識向上スキルのトレーニング
03	データ保護	09	電子メールとWebブラウザの保護	15	サービスプロバイダーの管理
04	組織の資産とソフトウェアの安全な構成	10	マルウェアの防御	16	アプリケーションソフトウェアのセキュリティ
05	アカウント管理	11	データ復旧	17	インシデントレスポンスと管理
06	アクセス制御管理	12	ネットワークインフラストラクチャー管理	18	ペネトレーションテスト

どのようなリスクがあるか現状を把握した上で、リスクの大きさや優先順位を設定し、短期的な対策として行う「暫定施策」と今後長期的な安全を担保するための「恒久施策」を行いセキュリティの向上を計っております。施策はWeWork Japan社内での情報管理を主に行うもの、入居者の安心安全のために行う２つの側面より施策を実施しております。

出典：CIS　https://www.cisecurity.org/controls/implementation-groups/ig2

わたしたちのセキュリティに関する考え方

ISO27001の取得

ISO27001とは、組織内の情報を安全にまもり活用活用するための情報セキュリティマネジメントシステム（ISMS）に関するISOの規格です。ISO27001を通じて、WeWorkは運営する拠点において、情報を取り扱う手順やルールを明確にして、役割や責任を明確にすることを審査機関の認証を通じて実現しています。

WeWork Japanでは、ISO27001を７つの拠点で取得しており、同様の管理をすべての拠点に適用しています。

SOC 2 Type 2

SOC2とは「Service Organization Control Type 2」の略称であり、米国公認会計士協会（AICPA）が定めたサイバーセキュリティのフレームワークの1つです。 主に顧客データをクラウドサービスに保存して処理するサービスなどを提供する会社に適用するフレームワークになっています。

Type 2 はSOC2の評価対象期間を示しており、Type 1が1日だけを対象としているのに対して、統制された運用がきちんと行われているのかを、半年以上のある一定の期間について証跡を提示することになります。

WeWorkは各種運用システムを開発・運用するWeWorkの米国においてSOC 2 Type2報告書を取得しており、WeWork Japanもその手順やルールのもとで運営を行なっています。

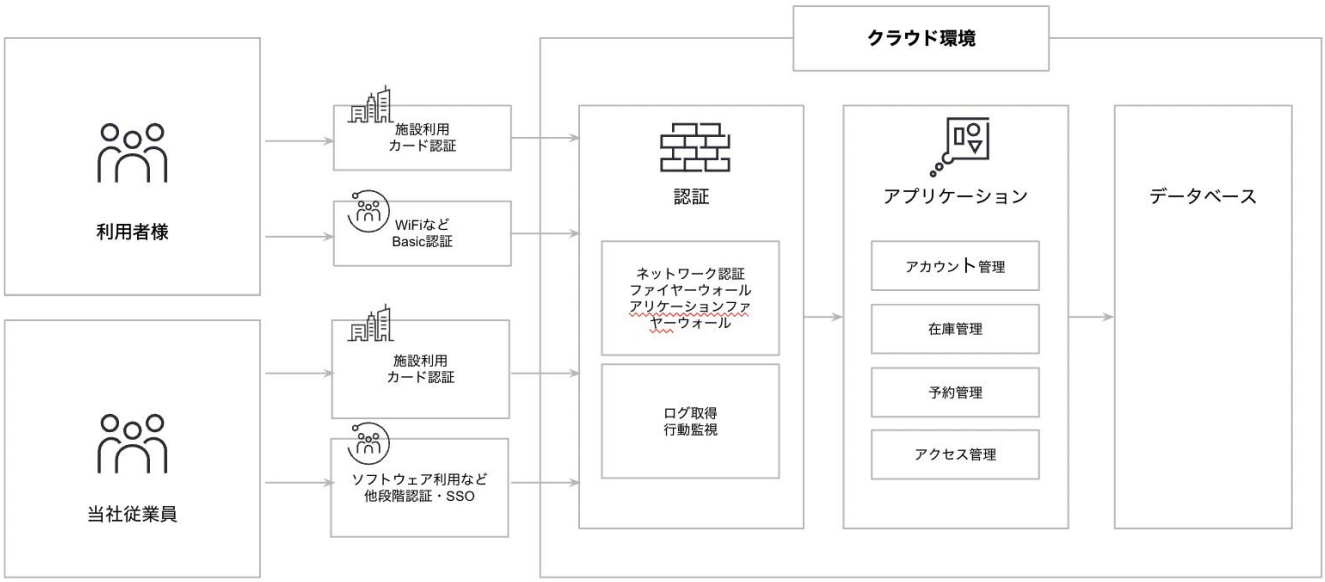
参照情報

ISO27001について
SOC 2 Type 2について
認証WeWorkの認証について

WeWorkのセキュリティ方針と施策

セキュリティ施策

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。



セキュリティ施策の概要

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報告書の取得	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	外部からの侵入防止
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

TO BE UPDATED

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ることが基本となりますが、グローバルで求められる水準を満たすだけでも相当なレベルに達することが可能となります。ただし、日本国内にある当社の事情に合わせなければ、過不足の多い対策となってしまうため、調整が必要です。一定程度は米国基準のままで進める必要がある中で、どこまで受容すべきかは日本の状況に合わせて判断すること。日本に合わせた対策を行う場合は、内容によっては米国本社とのすり合わせが求められます。

ソフトバンク株式会社

WeWork Japanはソフトバンク株式会社の関連企業であり、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

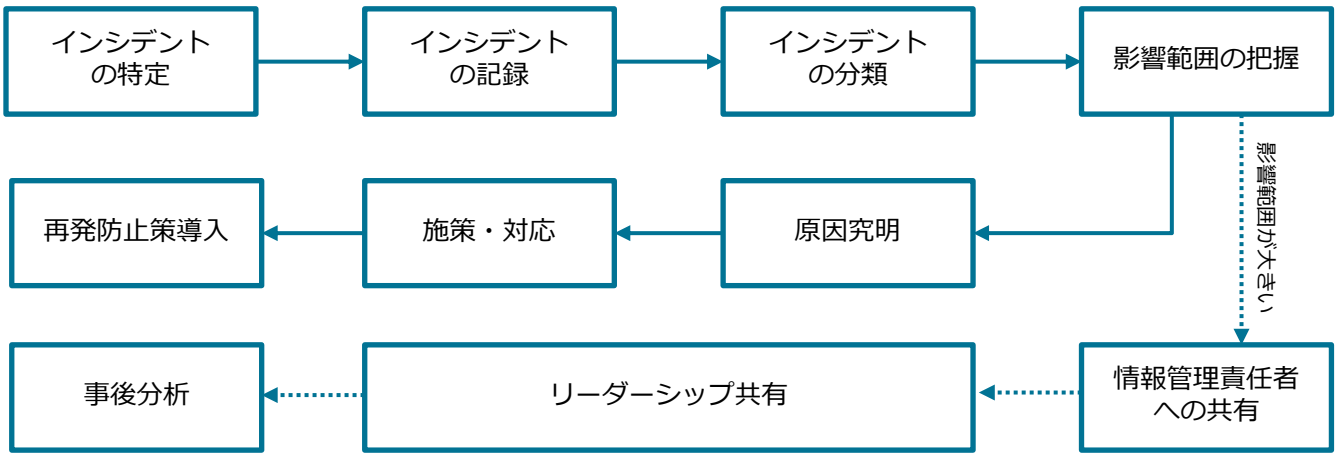
中堅・中小企業専業のセキュリティ支援会社である株式会社CISOが保有する「CISOセキュリティ診断」を活用。この診断プログラムは、セキュリティリスクを７つのカテゴリに分類し、中堅・中小企業にとって重要なセキュリティ施策を「外部からのサイバーセキュリティ対策」「内部情報漏洩などの情報セキュリティ対策」「BCPや物理的なセキュリティ対策」「組織ならびに人的なセキュリティ対策」の４つの観点でリスク判定。結果を数値でスコアリングし、具体的な取り組み施策までをわかりやすく提示するものです。

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、年に2回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

サイバー保険（準備中）

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