



セキュリティホワイトペーパー

2026年10月1日更新

wework

エグゼクティブサマリー

WeWork Japanでは、お客様が安心してワークプレイスをご利用いただけるよう、ISO/IEC 27001に基づく情報セキュリティマネジメントの考え方を踏まえ、以下のような多層的なセキュリティ管理に取り組んでいます。

物理的セキュリティ（施設・入室・来訪者管理）

入室記録、来訪者記録、監視カメラ、専用オフィス・共用エリアの管理等により、拠点の安全性確保に努めています。

技術的セキュリティ（Wi-Fi・ネットワーク・ITオプション）

Wi-Fi、有線LAN、通信暗号化、端末間通信の制限等により、共用環境におけるリスク低減を図っています。

組織的・人的セキュリティ（体制・ルール・運用管理）

セキュリティ管理体制、従業者教育、委託先管理、ログ管理、インシデント対応、内部点検・監査および是正処置を通じて、継続的な改善に取り組んでいます。

個人情報保護・データ保護

個人情報、入室情報、設備の利用履歴、監視カメラ映像等を、関係法令、社内規程および公表方針に基づき適切に取り扱います。

お客様との責任分界

WeWork Japanが提供・管理する範囲と、お客様に管理いただく範囲を明確にし、双方が協力して安全な利用環境を維持することを重視しています。

本書に関する共通注記

本ホワイトペーパーに記載するセキュリティ対策、サービス内容、オプション対応、記録・ログ・映像等の提供可否は、拠点、ビル仕様、契約プラン、利用エリア、設備状況、個別条件および法令・契約上の制約により異なる場合があります。

また、入室記録、来訪者記録、監視カメラ映像、ログ、ネットワーク構成、内部運用手順、監査資料その他の情報には、個人情報またはセキュリティ上保護すべき情報が含まれる場合があります。そのため、これらの確認または提供については、利用目的、必要性、対象範囲、契約条件、法令、個人情報保護、第三者の権利保護およびセキュリティ上の必要性を踏まえ、公開可能な範囲で個別に判断します。

特定のセキュリティ要件をお持ちの場合は、契約前または利用開始前に、対象拠点ごとの提供条件をご確認ください。

目次

エグゼクティブサマリー.....	2
本書に関する共通注記.....	3
1. セキュリティに対する基本的な考え方.....	7
1.1 WeWork Japanが考えるセキュリティ.....	7
1.2 対象とするセキュリティ領域.....	8
1.3 公開範囲と非公開情報の考え方.....	8
1.4 継続的改善.....	9
2. 物理的セキュリティ.....	9
2.1 物理的セキュリティの基本的な考え方.....	9
2.2 入退室管理.....	10
2.3 来訪者・作業者の管理.....	10
2.4 情報資産を取り扱うエリアの管理.....	10
2.5 監視カメラ・防犯対策.....	11
2.6 書類・端末・記録媒体の物理的管理.....	11
2.7 専用オフィス・共用エリアにおける情報管理.....	12
2.8 物理的セキュリティに関する拠点差分.....	12
3. 技術的セキュリティ.....	12
3.1 技術的セキュリティの基本的な考え方.....	12
3.2 標準インターネット接続サービス.....	13
3.3 WeWork Wi-Fiのセキュリティ.....	14
3.4 ゲスト向けネットワーク.....	14
3.5 有線LAN接続.....	15
3.6 ネットワーク分離と専用ネットワーク.....	15
3.7 お客様独自ネットワークへの対応.....	16
3.8 持込機器およびアクセスポイントに関する考え方.....	16
3.9 ITクローゼットにおける機器管理.....	17
4. 組織的・人的セキュリティ.....	17
4.1 組織的・人的セキュリティの基本的な考え方.....	18

4.2 セキュリティ管理体制.....	18
4.3 情報資産の把握とリスク評価.....	19
4.4 情報資産の分類と取扱い.....	19
4.5 守秘義務と機密情報の管理.....	19
4.6 従業者への周知・教育.....	20
4.7 委託先・業務委託従事者の管理.....	20
4.8 アカウント・権限の運用管理.....	21
4.9 ログの取得・管理.....	21
4.10 インシデント対応体制.....	22
4.11 内部点検・監査および是正処置.....	22
4.12 継続的な改善.....	23
5. 個人情報保護・データ保護.....	23
5.1 個人情報保護の基本的な考え方.....	23
6. お客様との責任分界.....	24
6.1 責任分界の基本的な考え方.....	24
6.2 WeWork Japanが管理・運営上関与する主な範囲.....	24
6.3 お客様に管理いただく主な範囲.....	25
6.4 共同で対応する範囲.....	26
6.5 領域別の責任分界.....	26
6.6 拠点・契約条件による差分.....	28
6.7 安全な利用環境を維持するためのお願い.....	28
7. 認証・第三者評価・参照フレームワーク.....	29
7.1 ISO/IEC 27001認証の取得状況と適用範囲.....	29
7.2 第三者評価・外部監査.....	30
7.3 参照するセキュリティフレームワーク.....	30
7.4 NIST Cybersecurity Frameworkの活用.....	30
7.5 CIS Controls等の実践的管理策の参照.....	31
8. お問い合わせ・追加開示について.....	31
8.1 セキュリティに関するお問い合わせ.....	31

8.2 セキュリティチェックシート等への対応.....	31
8.3 追加開示の考え方.....	32
8.4 本ホワイトペーパーの位置づけ.....	32
8.5 更新と継続的な見直し.....	33
8.6 関連情報.....	33

1. セキュリティに対する基本的な考え方

本ホワイトペーパーでは、WeWork Japanのサービスを契約または利用される法人・団体・個人のお客様を総称して「お客様」と記載します。また、WeWork Japanのワークプレイスを実際に利用される登録利用者を、当社サービス上の呼称に合わせて「メンバー様」と記載します。メンバー様を訪問される方およびイベントへの参加者は「ゲスト様」または「来訪者」と記載します。

「作業員」とは、清掃、警備、設備保守、点検、修理、工事、配送、ネットワーク機器の設置・保守その他の作業を目的として、WeWork Japanの拠点、執務エリア、設備管理エリア、ITクローゼットその他の管理対象エリアに立ち入る当社従業員以外の外部関係者を指します。

また、本ホワイトペーパーでは、WeWork Japanが提供するオフィススペース、共用エリア、会議室、通信環境、共用設備、施設運営等を含む利用環境を総称して「ワークプレイス」または「ワークプレイス環境」と記載します。また、複数の企業・利用者が柔軟に利用するオフィスサービスの形態を説明する場合には、「フレキシブルオフィス」と記載します。

1.1 WeWork Japanが考えるセキュリティ

WeWork Japanは、フレキシブルオフィスを提供する企業として、利用者の皆様に安心・安全な環境を提供し続けることを重視しています。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」を、サービス品質の重要な要素として位置付けています。

また、日本の社会インフラとして通信環境を提供するソフトバンクの関連会社として、「安定した環境を提供する」という価値観を踏まえ、ワークプレイス環境の安全性、安定性および継続的な改善に取り組んでいます。

1.2 対象とするセキュリティ領域

本ホワイトペーパーでは、WeWork Japanが提供するワークプレイスに関わるセキュリティ領域として、以下を対象とします。

- 拠点への入退室管理、来訪者管理、監視カメラ、専有区画などに関する物理的セキュリティ
- ネットワーク、アカウント管理、ログ管理、端末管理、脆弱性対応などに関する技術的セキュリティ
- セキュリティ方針、管理体制、従業員教育、委託先管理、監査、インシデント対応などに関する組織的・人的セキュリティ
- 個人情報、来訪者情報、入室情報、映像情報などの取扱いに関する個人情報保護・データ保護
- WeWork Japanが提供・管理する範囲と、お客様に管理いただく範囲を明確にする責任分界

これらの領域を体系的に整理することで、WeWork Japanのセキュリティに対する考え方と、具体的な取り組みの全体像を示します。

1.3 公開範囲と非公開情報の考え方

本ホワイトペーパーでは、お客様に安心してサービスをご利用いただくために必要な情報を、外部公開可能な範囲で説明しています。

一方で、セキュリティ管理の詳細な手順、ネットワーク構成、監視・検知の具体的な条件、ログの詳細仕様、運用上の内部手順などについては、公開することによりセキュリティ上のリスクが高まる可能性がありますので、原則的に開示していません。

WeWork Japanは、透明性と安全性の両立を重視し、お客様がサービス利用にあたって必要な確認を行えるよう、公開可能な情報を適切に提供するとともに、セキュリティ上保護すべき情報を慎重に管理します。

1.4 継続的改善

セキュリティは、一度対策を講じれば完了するものではありません。事業環境、技術環境、脅威の動向、お客様の利用形態は常に変化しており、それに応じて必要な管理策も継続的に見直す必要があります。

WeWork Japanでは、情報セキュリティに関するリスクの把握、管理策の実施状況の確認、従業員への教育・啓発、内部点検・監査、インシデントや不具合への対応、是正処置などを通じて、セキュリティ水準の維持・向上に取り組んでいます。

また、お客様からのご要望、セキュリティチェックの内容、法令・ガイドライン・業界標準の変化、当社事業・サービスの拡大等も踏まえ、必要に応じて運用や文書を見直します。

2. 物理的セキュリティ

2.1 物理的セキュリティの基本的な考え方

WeWork Japanでは、メンバー様が安心してワークプレイスを利用できるよう、拠点における入退室管理、来訪者管理、執務エリアの管理、監視カメラ、防災設備、清掃・衛生管理等を通じて、物理的な安全性の確保に取り組んでいます。

情報資産の保護においては、システム上の対策だけでなく、情報を取り扱う場所、入退室の管理、書類・端末・記録媒体の保管、来訪者の管理等も重要です。拠点の特性や利用エリアに応じた物理的な管理策を講じることで、安心・安全なワークプレイス環境の維持に努めています。

2.2 入退室管理

入退室管理は、利用権限を持つメンバー様、来訪者、WeWorkの従業員、作業者等が、それぞれ許可された範囲で施設を利用するための基本的な管理策です。

WeWork Japanでは、拠点や利用エリアの特性に応じて、ICキーカード、スマートロック、受付対応、ゲスト事前登録システム等を用いた入退室管理を行っています。

ここでいう入退室管理とは、施設や管理対象エリアへの立入りを適切に制御し、許可された方が許可された範囲で利用できるようにするための管理を指します。取得・管理する記録の種類および範囲は、拠点、設備仕様、利用エリアおよびサービス内容により異なる場合があります。

入室記録等の確認または提供については、本書冒頭の「本書に関する共通注意」に記載の考え方にに基づき、必要性および対象範囲を確認したうえで対応します。なお、入室情報等の一部については、契約条件または有償サービスとして提供可能な場合があります。

2.3 来訪者・作業者の管理

WeWork Japanでは、来訪者や作業者が拠点を利用する場合、受付対応やゲスト登録等を通じて、入館・訪問の管理を行います。

来訪者や作業者が執務エリア、設備管理エリアその他の管理対象エリアに立ち入る場合には、訪問目的、作業内容、立入エリア、作業時間等を確認し、必要に応じて入室権限を持つ者による対応、受付での確認、事前申請、立会い等により管理します。

2.4 情報資産を取り扱うエリアの管理

WeWork Japanでは、取り扱う情報の重要度や業務内容に応じて、情報資産を取り扱う場所を適切に選択し、エリアの特性に応じた管理を行っています。

共用エリア、執務エリア、ネットワーク機器等を設置する設備管理エリアでは、それぞれ求められる管理水準が異なります。そのため、入退室管理、利用者管理、設備管理等を組み合わせ、各エリアの特性に応じた安全管理に努めています。

また、機密性の高い情報を取り扱う場合には、情報の性質や業務内容に応じて、会議室、バックオフィス等の適切な場所を利用することを従業員に周知しています。あわせて、お客様およびメンバー様に対しても、共用エリアや会議室等の利用場所に応じて、画面表示、会話内容、書類・端末の取扱い等に配慮していただくようお願いしております。

2.5 監視カメラ・防犯対策

WeWork Japanでは、共用エリア等に監視カメラを設置し、防犯、事故・トラブル発生時の確認、利用者保護、施設管理等の目的で運用しています。

監視カメラ映像は、セキュリティ管理上必要な範囲で取り扱い、閲覧・確認できる者を限定します。映像の取扱いについては、個人情報保護・データ保護の観点からも適切に管理します。

2.6 書類・端末・記録媒体の物理的管理

WeWork Japanでは、情報資産の盗難、紛失、覗き見、誤廃棄等を防止するため、書類、端末、記録媒体の物理的な管理を重視しています。

機密性のある書類、記録媒体、携帯可能なデバイス等については、利用目的や情報の重要度に応じて、放置防止、施錠保管、適切な廃棄等の管理を行います。また、離席時や退勤時には、書類や端末が第三者の目に触れたり、持ち出されたりしないよう、従業員への周知・啓発を行っています。

2.7 専用オフィス・共用エリアにおける情報管理

WeWorkのワークプレイスは、専用オフィス、会議室、共用エリア、ラウンジ等を組み合わせたフレキシブルな利用形態を特徴としています。

WeWork Japanは、施設・設備・入退室管理等の管理策を提供するとともに、メンバー様にも利用場所に応じた情報管理をお願いしています。

特に、共用エリアや会議室で機密情報を取り扱う場合には、周囲からの覗き見や会話の聞き取りに配慮し、必要に応じて専用オフィス、会議室等のより適切な場所を利用することが望まれます。

2.8 物理的セキュリティに関する拠点差分

物理的セキュリティ対策は、拠点、ビル仕様、契約プラン、利用エリア、専有区画の有無等により異なる場合があります。

入退室管理、スマートロック、監視カメラ、営業時間外の警備、ITクローゼット、サーバー機器設置、追加セキュリティ要件等について特定の要件をお持ちの場合は、契約前または利用開始前に、対象拠点における設備仕様、運用条件、追加対応の可否をご確認ください。

3. 技術的セキュリティ

3.1 技術的セキュリティの基本的な考え方

WeWork Japanでは、メンバー様が安定した通信環境を利用できるよう、標準インターネット接続サービスおよび各種ITオプションを提供しています。

フレキシブルオフィスでは、複数の企業・利用者が同一拠点内でサービスを利用するため、ネットワーク環境には、利便性、安定性、分離性、安全性のバランスが求められます。

WeWork Japanは、標準的なインターネット接続環境を提供するとともに、お客様の利用形態やセキュリティ要件に応じて、専用VLAN、専用Wi-Fi、専用グローバルIP、機器ホスティング等の選択肢を用意しています。

3.2 標準インターネット接続サービス

WeWork Japanでは、メンバー様が追加費用なく利用できる標準インターネット接続サービスを提供しています。標準サービスには、主に以下の接続方式が含まれます。

- メンバー様向け無線LAN接続サービス
- ゲスト様向け無線LAN接続サービス
- プライベートオフィス内で利用可能な有線LAN接続サービス
- 一部会議室等で利用可能な有線LAN接続サービス

標準インターネット接続サービスは、複数の企業・団体および利用者が同一拠点内で利用する共用型の通信環境です。WeWork Japanでは、認証、暗号化、端末間通信の制限、共用環境に起因するリスクの低減を図っています。

ただし、お客様固有のセキュリティ要件、通信制御、監視、閉域接続、固定IP、専用セグメント等が必要な場合には、専用ネットワーク、専用VLAN、専用Wi-Fi等の個別構成をご検討ください。

なお、標準ネットワークはインターネット接続環境を提供するものであり、お客様の社内ネットワーク、業務システム、クラウドサービス等への接続内容をWeWork Japanが管理または閲覧するものではありません。お客様の社内システムや業務デー

タへのアクセスについては、必要に応じてVPN、ゼロトラストアクセス、端末認証、多要素認証等、お客様側の管理策をご利用ください。

3.3 WeWork Wi-Fiのセキュリティ

WeWork Wi-Fiは、メンバー様が館内で利用できる標準の無線LAN接続サービスです。

WeWork Wi-Fiでは、利用者ごとの認証、通信の暗号化、端末間通信の制限等※により、共用環境に起因するリスクの低減を図っています。

これにより、同一無線LAN上に接続する他の利用者端末との不要な通信を抑制し、共用環境における端末間通信に起因するリスクの低減を図っています。

なお、共用ネットワークである性質上、お客様の端末、アカウント、業務データ、自社システムへの接続手段については、お客様自身で適切に管理いただく必要があります。

認証方式、暗号化方式、対応規格等は、拠点設備、提供サービス、端末互換性および運用条件により変更される場合があります。詳細な設定情報は、セキュリティ上の理由により公開資料では開示していません。

※端末間通信の制限等によりPeer to Peerの通信を要求するサービスは利用できません。

3.4 ゲスト向けネットワーク

WeWork Japanでは、メンバー様を訪問されるゲスト様向けの無線LAN接続サービスを提供しています。

ゲスト向けネットワークは、メンバー様向けネットワークとは用途を分けて提供されます。ゲスト様は、所定の認証手続きを経てネットワークを利用します。

ゲスト向けネットワークは、来訪者の利便性を確保しつつ、メンバー様の業務利用環境と区別して提供されるものです。

お客様は、自社の来訪者に対して、利用目的、機密情報の取扱い、会議中の情報管理等について必要な案内を行うことが望まれます。

3.5 有線LAN接続

WeWork Japanでは、プライベートオフィス内や一部会議室等において、有線LAN接続を利用できる環境を提供しています。

プライベートオフィス内の有線LANは、PC、プリンター、その他業務機器の接続に利用される場合があります。また、会議室等の有線LANは、Web会議など通信の安定性が求められる用途に利用される場合があります。

標準の有線LANは、WeWork Japanが提供する標準ネットワークの一部として提供されます。お客様が他の利用者と分離されたネットワーク環境を希望する場合には、専用VLAN等の個別オプションの利用を検討ください。

3.6 ネットワーク分離と専用ネットワーク

WeWork Japanでは、お客様のセキュリティ要件に応じて、標準ネットワークとは区別された個別のネットワーク構成を提供できる場合があります。

たとえば、専用ネットワーク、専用Wi-Fi、固定IP等のオプションを組みあわせることで、お客様の利用形態に応じた構成を検討することが可能です。

これらの提供可否、提供範囲、仕様、費用、導入条件は、拠点、フロア、契約プラン、ビル仕様、ネットワーク設備等により異なる場合があります。利用を希望される場合は、契約前または導入前に対象拠点ごとの提供可否および運用条件をご確認ください。

3.7 お客様独自ネットワークへの対応

お客様の業務要件により、自社ルータ、自社回線、自社ネットワーク機器等を用いた独自ネットワーク構成が必要となる場合があります。

WeWork Japanでは、一定の条件のもとで、お客様が用意するネットワーク機器の持ち込みについて、対象拠点における設置可否、設置場所、配線、電源、ITクローゼットの利用可否、作業手続等を確認します。

ただし、これらは標準サービスとして一律に提供されるものではなく、拠点、契約プラン、ITクローゼットの空き状況、ビル側の制約、工事可否、運用条件等により対応可否が異なります。

また、お客様が用意する機器、通信回線、システム等については、お客様自身の責任において設定、運用、監視、保守、セキュリティ管理を行っていただく必要があります。

3.8 持込機器およびアクセスポイントに関する考え方

WeWork Japanでは、館内の無線品質および通信環境の安定性を確保するため、お客様によるWi-Fiアクセスポイント、Wi-Fiルータ、モバイルルータその他Wi-Fi通信を提供または中継する機器の持ち込みおよび利用は、原則として制限しています。

お客様が個別にWi-Fiアクセスポイント、Wi-Fiルータ、モバイルルータを設定した場合、WeWork Japanが提供するWi-Fi設備との電波干渉が発生し、館内の通信品質や他の利用者の利用環境に影響を及ぼす可能性があります。

そのため、Wi-Fiネットワークの利用にあたっては、原則としてWeWork Japanが提供する標準無線LANサービスまたは個別に承認されたネットワーク構成をご利用いただく必要があります。

なお、本項における制限の対象は、主にWi-Fi通信を提供または中継する機器および機能を想定しており、赤外線通信、Bluetooth通信、携帯電話回線としての4G/5G通信そのものを対象とするものではありません。ただし、4G/5G回線を利用してWi-Fi接続を提供するモバイルルータについては、Wi-Fi電波を発するため、原則として制限対象となります。

3.9 ITクローゼットにおける機器管理

WeWork Japanでは、一部拠点において、ITクローゼットにお客様機器を収容できる場合があります。

対象区画への入室や作業が必要な場合には、所定の手続きに従い、WeWork Japanの担当者を通じて対応します。お客様またはお客様が手配する作業業者が作業を行う場合には、事前申請、作業内容の確認、立会い、退出確認等が必要となる場合があります。

なお、利用可否、設置可能な範囲、電源、作業可能時間、工事可否その他の条件は、拠点およびビル仕様により異なります。お客様機器の設置、電源、保守、交換、監視、バックアップ、障害対応等については、お客様自身の責任範囲となります。

4. 組織的・人的セキュリティ

本章では、セキュリティ方針、管理体制、従業者教育、委託先管理に加え、アカウント・権限管理、ログ管理、インシデント対応など、技術的な仕組みを適切に運用するための組織的な管理プロセスについて説明します。

4.1 組織的・人的セキュリティの基本的な考え方

WeWork Japanでは、情報セキュリティを、技術的な対策だけでなく、経営、組織、従業員、業務プロセス、委託先管理、インシデント対応を含む総合的な取り組みとして位置付けています。

セキュリティ対策を継続的に機能させるためには、システムや設備の整備に加え、それを運用する体制、従業員一人ひとりの理解、日常業務における適切な判断と行動が不可欠です。

そのため、セキュリティ管理体制の整備、情報資産の適切な管理、従業員への周知・教育、委託先との連携、インシデント対応体制の維持を通じて、安心・安全なサービス提供に努めています。

4.2 セキュリティ管理体制

WeWork Japanでは、情報セキュリティを経営上重要なテーマとして位置付け、情報セキュリティに関する方針、リスク管理、管理策の運用、インシデント対応、改善活動を推進する体制を整備しています。

情報セキュリティに関する事項は、関係部門が連携し、情報システム、法務、施設運営、営業、カスタマーサポート等の観点を踏まえて管理します。また、各部門が保有・利用する情報資産については、業務内容や情報の重要度に応じて管理責任を明確にし、必要な確認・改善を行います。

重大なセキュリティ上の課題やインシデントが発生した場合には、経営層を含む関係者へ報告し、影響範囲、原因、緊急度等を確認したうえで、対応方針、是正処置、再発防止策等を検討・実施します。

4.3 情報資産の把握とリスク評価

WeWork Japanでは、業務上取り扱う情報資産を把握し、その重要度、利用目的に応じて、保管場所、アクセス権限、保存期間、取扱方法等を管理します。

情報資産には、紙媒体の文書、電子データ、業務システム、ネットワーク、記録媒体、入室記録、来訪者記録、監視カメラ映像、契約情報、顧客情報、個人情報等が含まれます。

これらの情報資産について、機密性、完全性、可用性の観点からリスクを評価し、リスクの大きさ、影響範囲、発生可能性、業務上の必要性等を踏まえて、必要な管理策を検討・実施します。また、事業環境、サービス内容、システム構成、法令・ガイドライン、脅威動向等に変更があった場合には、必要に応じてリスク評価および管理策を見直します。

4.4 情報資産の分類と取扱い

WeWork Japanでは、情報資産の重要度や機密性に応じて、適切な分類と取扱いを行います。

経営上重要な情報、顧客情報、個人情報、契約情報、技術情報、業務上限定的に共有すべき情報等については、必要な範囲に限って閲覧・利用できるよう管理します。

情報資産を作成、取得、編集、複製、送信、保存、廃棄する際には、情報の分類、利用目的、開示範囲、保存期間、取扱方法等を確認し、分類に応じた管理を行います。また、重要な情報を送信または共有する場合には、アクセス制御、暗号化、送付先確認等、情報の性質に応じた保護措置を講じます。

4.5 守秘義務と機密情報の管理

WeWork Japanでは、従業者が業務上知り得た機密情報を、業務目的以外に使用せず、第三者へ不適切に開示しないよう管理しています。

機密情報を外部の関係者と共有する必要がある場合には、共有する相手方、目的、情報の範囲を確認し、必要に応じて秘密保持に関する取り決めを行います。

また、退職、異動、契約終了等により業務を離れる場合には、貸与物、アカウント、アクセス権限、保有情報等を確認し、不要なアクセスや情報の持ち出しが残らないよう管理します。

4.6 従業員への周知・教育

WeWork Japanでは、従業員が情報セキュリティ上の役割と責任を理解し、日常業務において適切な判断と行動を取れるよう、周知・教育を行っています。

教育・啓発の対象には、情報の分類と取扱い、個人情報保護、アカウント管理、パスワード管理、フィッシング対策、端末利用、情報の送受信、インシデント報告等が含まれます。

また、事業環境、脅威動向、業務プロセス、法令・ガイドライン等の変化に応じて、必要な内容を見直し、従業員のセキュリティ意識と実践力の向上に努めています。

4.7 委託先・業務委託従事者の管理

WeWork Japanでは、業務委託先や業務委託従事者が当社の情報資産、施設、設備またはサービス提供に関わる場合、業務内容、取扱う情報の重要度、立入可能なエリア、システムへのアクセス有無等を踏まえ、必要なセキュリティ要件を確認します。

委託先との契約や業務開始時には、責任範囲、情報の取扱い、秘密保持、再委託、アクセス権限、事故発生時の連絡、貸与物の管理、契約終了時の返却・削除等について、業務内容およびリスクに応じて必要な条件を明確にします。

また、委託業務の内容やリスクに応じて、委託先の管理状況を確認し、改善が必要と判断した場合には是正または改善を求めます。

清掃、警備、設備保守、ビル管理等の業務に従事する外部関係者についても、業務内容、作業場所、作業時間、情報資産への接触可能性等を踏まえ、契約、入退室管理、作業管理、必要に応じた立会い等により管理します。

4.8 アカウント・権限の運用管理

WeWork Japanでは、業務システムや情報資産へのアクセスについて、業務上必要な範囲に限定して権限を付与します。

アカウントや権限の付与、変更、削除は、利用目的や担当業務に応じて管理します。異動、退職、契約終了等によりアクセスが不要となった場合には、速やかに権限の見直しや削除を行います。

また、アカウントの共有は原則として行わず、やむを得ず共有が必要な場合には、利用目的、利用者、管理責任を明確にしたうえで、必要な管理を行います。アクセス権限については、業務上の必要性やリスクに応じて確認し、不要または過剰な権限が残らないよう管理します。

4.9 ログの取得・管理

WeWork Japanでは、情報システムの利用状況を把握し、不正アクセス、不適切な操作、インシデント発生時の調査等に役立てるため、業務上およびセキュリティ管理上必要な範囲でログを取得・管理します。

取得するログの対象、保存期間、閲覧権限および提供可否は、利用目的、法令、契約、社内規程およびセキュリティ上の必要性を踏まえて定め、閲覧できる者を業務上必要な範囲に限定します。

なお、ログの確認または提供については、本書冒頭の「本書に関する共通注記」に記載の考え方にに基づき、必要性及び対象範囲を確認したうえで対応します。

4.10 インシデント対応体制

WeWork Japanでは、情報漏えい、紛失、不正アクセス、マルウェア感染、システム障害、不正利用その他のセキュリティ上の懸念が発生した場合に備え、インシデント対応体制を整備しています。

インシデントまたはその疑いを検知した場合には、関係者へ速やかに共有し、影響範囲の確認、原因調査、初動対応、被害拡大防止、復旧、再発防止策の検討を行います。重大な影響が想定される場合には、経営層を含む関係者へ報告し、必要な判断と対応を行います。

WeWork Japanが提供する施設、ネットワーク、入退室管理、個人情報管理等に関連して、お客様に重大な影響を及ぼす可能性のあるセキュリティインシデントを確認した場合には、契約条件、法令、個人情報保護、調査の進捗および二次被害防止の観点で踏まえ、判明している範囲で速やかにお客様へ通知します。

通知では、可能な範囲で、事象の概要、確認時点で想定される影響範囲、暫定対応、追加確認事項、お客様側で確認いただきたい事項、今後の対応方針等をお知らせします。

4.11 内部点検・監査および是正処置

WeWork Japanでは、情報セキュリティ管理の実効性を確認するため、情報資産の管理状況、アクセス権限、委託先管理、教育実施状況、インシデント対応、ログ管理、個人情報保護、その他の管理策の運用状況について、定期的に内部点検・監査を行います。

内部点検・監査、インシデント対応、委託先確認、お客様からの要請等を通じて課題が確認された場合には、原因を確認し、必要な是正処置または改善策を検討・実施し

ます。また、実施した対応については有効性を確認し、再発防止および管理策の改善につなげます。

4.12 継続的な改善

WeWork Japanでは、事業環境、脅威動向、法令・ガイドライン、お客様からの要請、インシデントや監査結果等を踏まえて、セキュリティ管理を継続的に見直します。

情報セキュリティ方針、リスクアセスメント、管理策、教育内容、委託先管理、アクセス管理、インシデント対応、ログ管理、個人情報保護等について、必要に応じて改善を行います。

5. 個人情報保護・データ保護

5.1 個人情報保護の基本的な考え方

WeWork Japanでは、お客様、メンバー様、来訪者様、取引関係者様、従業員、採用応募者その他の個人の皆様に関する情報を、重要な情報資産として適切に取り扱います。

WeWork Japanが提供するワークプレイス環境においては、契約情報、利用者情報、来訪者情報、入室情報、会議室等の予約・利用情報、問い合わせ情報、映像情報など、サービスの提供、安全な環境の維持、セキュリティ管理、法令遵守のために必要な個人情報を取り扱う場合があります。

WeWork Japanは、これらの個人情報について、関係法令、社内規程、個人情報保護方針および「個人情報のお取り扱いについて」に基づき、適切な取得、利用、保管、管理、提供および廃棄に努めます。

詳細につきましては、公表しております「個人情報のお取り扱いについて」をご参照ください。

6. お客様との責任分界

6.1 責任分界の基本的な考え方

WeWork Japanは、お客様およびメンバー様が安心して事業活動を行えるよう、ワークスペース、共用設備、ビル管理、オフィスセキュリティ、清掃・衛生管理等を含むワークプレイス環境を提供しています。

一方で、WeWorkのワークプレイスは、多様な企業・利用者が共用するフレキシブルオフィスであるため、セキュリティの維持には、WeWork Japanによる管理だけでなく、お客様自身による適切な利用者管理、端末管理、情報管理も不可欠です。

そのため、WeWork Japanが提供・管理する範囲と、お客様に管理いただく範囲を明確にし、双方が協力して安全な利用環境を維持することを基本的な考え方としています。

6.2 WeWork Japanが管理・運営上関与する主な範囲

WeWork Japanは、提供するワークプレイス環境に関して、当社が管理・運営する範囲、およびビル所有者、ビル管理会社その他の関係者と連携して対応する範囲において、主に以下の事項に関与します。

- 共用エリア、専用オフィス、会議室等のワークスペースの提供・運営
- ICキーカード、スマートロック等による標準的な入退室管理
- ゲスト事前登録システム、受付対応等による来訪者管理
- WeWork Japanの運営範囲における監視カメラの設置・運用
- WeWork Japanの運営範囲における設備、備品等の管理

- ビル設備、警備、防災等に関する関係者との連携・調整
- 共用エリア、専用オフィスにおける清掃・衛生管理に関する手配・運営管理
- 高速インターネット、プリンター、廃棄ボックス等の共用設備・備品の提供・保守
- 拠点運営に関する問い合わせ対応および日常的な運営支援

これらの管理策および運営上の対応は、WeWork Japanが提供する標準的なサービスおよびセキュリティ管理の一部です。ただし、具体的な提供内容およびWeWork Japanの関与範囲は、拠点、契約プラン、ビル仕様、利用条件により異なる場合があります。

6.3 お客様に管理いただく主な範囲

お客様には、自社の利用者、自社情報、自社端末、自社システム、自社データに関するセキュリティを管理いただく必要があります。

主に以下の事項は、お客様の管理範囲となります。

- 自社利用者の追加、変更、削除、退職・異動時の権限見直し
- ICキーカード、アプリ、アカウント等の適切な管理
- 自社端末、スマートフォン、記録媒体、ネットワーク機器等の管理
- 自社システム、自社クラウドサービス、自社データへのアクセス管理
- 自社システムへの接続手段、端末認証、暗号化、マルウェア対策、パッチ適用等の端末・システム対策
- 専用オフィス内の書類、端末、機密情報、個人情報、什器・備品等の管理
- 来訪者の招待、訪問目的の確認、訪問中の行動管理
- 共用プリンター、廃棄ボックス、会議室、電話ブース等を利用する際の情報管理

WeWork Japanがワークプレイス環境および標準サービスを提供する場合であっても、お客様の業務に関する情報、端末、アカウント、システム、データについては、お客様自身で適切に管理いただく必要があります。

6.4 共同で対応する範囲

施設・設備、提供サービス、お客様環境の双方に関係する事項については、WeWork Japanとお客様が協力して対応します。

共同で対応する主な範囲には、以下が含まれます。

- 不審者、不正入室、盗難、紛失、設備異常等が発生した場合の状況確認
- 入室記録、来訪者記録、監視カメラ映像等の確認が必要となる場合の調査対応
- セキュリティインシデント発生時の影響範囲確認および再発防止策の検討
- 専有区画、専用ネットワーク、サーバー機器設置等に関する個別要件の確認
- お客様のセキュリティチェック、監査、調達審査等への対応

なお、記録や映像、技術情報、運用情報その他の非公開情報の確認または提供にあたっては、本書冒頭の「本書に関する共通注記」に記載の考え方にに基づき、公開可能な範囲で対応します。

6.5 領域別の責任分界

以下は、WeWork Japanが提供するワークプレイス環境における主なセキュリティ管理領域について、WeWork Japanとお客様の役割を整理したものです。

領域	WeWork Japanの主な範囲	お客様の主な範囲
ワークスペース	共用エリア、専用オフィス、会議室等の提供・運営	利用者による適切な利用、自社情報・物品の管理
入退室管理	ICキーカード等による入退室管理の仕組みの提供	利用者登録、権限管理、カード等の適切な管理

領域	WeWork Japanの主な範囲	お客様の主な範囲
来訪者管理	ゲスト登録、受付対応等の仕組みの提供	来訪者の招待、訪問目的確認、訪問中の管理
監視カメラ	共用エリア等における監視カメラの設置・運用	自社区画内の情報管理、来訪者・従業員への周知
専用オフィス	専用オフィス、スマートロック等の提供	区画内の施錠、書類・端末・機密情報の管理
ネットワーク	標準ネットワーク環境の提供	自社端末、自社アカウント、自社システムへの接続手段
共用設備	プリンター、廃棄ボックス、備品等の提供・保守	印刷物、廃棄書類、記録媒体等の取り忘れ防止
清掃・衛生	共用部・専有部の清掃、消毒、メンテナンス	自社物品、機密書類、私物等の整理・管理
インシデント対応全般	施設・提供サービスに関する確認・初動対応	自社端末、自社データ、自社業務に関する調査・対応
不審者・不正入館	入室記録確認、現地対応、必要な連絡	自社利用者・来訪者の確認
専用オフィスの盗難	施設側記録の確認、可能な範囲で調査協力	自社資産の特定、警察・保険対応
顧客端末のマルウェア感染	標準ネットワーク影響の確認	端末調査、封じ込め、復旧
ネットワーク障害	提供サービス範囲の確認・復旧対応	自社機器・VPN・クラウド側の確認
個人情報保護	WeWork Japanが取得・管理する個人情報の保護	お客様が取得・保有する個人情報の保護

なお、専用ネットワーク、固定IP、ルーター等の機器設置、site-to-site VPNその他の個別ネットワーク要件については、拠点、契約プラン、ネットワーク仕様等により対応可否が異なるため、事前確認が必要です。

6.6 拠点・契約条件による差分

WeWork Japanが提供するサービスおよびセキュリティ対策は、拠点、ビル仕様、契約プラン、利用エリア、専有区画の有無、オプションサービスの利用有無等により異なる場合があります。

専用オフィス、フロア専有、スマートロック、ITクローゼット利用、追加の入退室管理、専用ネットワーク、個別設備要件等について、特定のセキュリティ要件をお持ちの場合は、契約前または利用開始前に、対象拠点における提供内容、設備仕様、運用条件、追加対応の可否をご確認ください。

6.7 安全な利用環境を維持するためのお願い

WeWork Japanは、ワークプレイスを安心してご利用いただくため、物理的・技術的・組織的なセキュリティ対策を講じています。

一方で、共用環境におけるセキュリティは、すべてのメンバー様の適切な利用によって成り立ちます。お客様には、自社利用者に対して、ICキーカードやアカウントの適切な管理、離席時のPCロック、機密書類の放置防止、来訪者管理、共用設備利用時の情報管理、不審事象発見時の速やかな連絡等について周知いただくことをお願いいたします。

WeWork Japanは、お客様との適切な役割分担と協力を通じて、安心・安全なワークプレイス環境の維持に努めてまいります。

参考：WeWork Japanが提供する主なサービス

ワークスペース・ミーティングスペース、共用設備・備品、ビル管理・オフィスセキュリティ、コミュニティチーム、清掃・消毒・衛生管理等の詳細は、各拠点・契約プランにより異なります。最新の提供内容は、営業担当または公式資料をご確認ください。

7. 認証・第三者評価・参照フレームワーク

7.1 ISO/IEC 27001認証の取得状況と適用範囲

WeWork Japanは、ISO/IEC 27001に基づく情報セキュリティマネジメントシステム（ISMS）を整備・運用し、本社および新宿拠点を対象としてISO/IEC 27001認証を取得しています。

認証取得状況は以下のとおりです。

項目	内容
認証規格	JIS Q 27001:2023（ISO/IEC 27001:2022）
登録組織	WWJ株式会社
認証登録番号	IR0234
登録範囲	シェアオフィスの運営管理
関連事業所	本社、リンクスクエア新宿
認証機関	アイエムジェー審査登録センター株式会社

ISO/IEC 27001認証の対象範囲は、認証登録情報に記載された登録組織、登録範囲および関連事業所に限られます。認証範囲に含まれないその他の拠点についても、認証範囲で整備・運用している情報セキュリティマネジメントの考え方を踏まえ、拠点特

性、ビル仕様、提供サービスおよび運用条件に応じたセキュリティ管理に取り組んでいます。

7.2 第三者評価・外部監査

WeWork Japanでは、情報セキュリティ管理の妥当性および有効性を確認するため、必要に応じて外部機関による審査・監査・評価を受けています。

外部の視点を取り入れることで、社内の自己点検だけでは把握しにくい課題を確認し、管理策の改善、運用の見直し、是正処置につなげています。

なお、外部監査の詳細な結果、監査手続、個別の指摘事項、内部資料等については、セキュリティ上および契約上の理由により、公開範囲を限定する場合があります。

7.3 参照するセキュリティフレームワーク

WeWork Japanでは、ISO/IEC 27001を中心としつつ、必要に応じて国内外のセキュリティフレームワーク、ガイドライン、業界標準等を参照し、管理策の検討や改善に活用しています。

参照するフレームワークは、単に形式的に準拠を示すためではなく、リスクの把握、管理策の整理、改善項目の優先順位付け、社内外への説明性向上のために活用します。

7.4 NIST Cybersecurity Frameworkの活用

WeWork Japanでは、サイバーセキュリティリスクを体系的に整理するため、必要に応じてNIST Cybersecurity Framework等の考え方を活用します。

NIST Cybersecurity Framework 2.0は、Govern、Identify、Protect、Detect、Respond、Recoverの機能を通じて、組織がサイバーセキュリティリスクを管理するための枠組みを示しています。

WeWork Japanでは、これらの考え方を、セキュリティガバナンス、リスク把握、防御、検知、対応、復旧の観点整理に活用し、セキュリティ対策の全体像を継続的に確認します。

7.5 CIS Controls等の実践的管理策の参照

CIS Controls等の実践的な管理策集については、技術的・運用的な管理策を検討する際の参考情報として参照する場合があります。

ただし、CIS Controlsへの準拠または網羅的な適用を本ホワイトペーパーで表明するものではありません。WeWork Japanでは、ISO/IEC 27001を中心とした情報セキュリティマネジメントの枠組みの中で、必要に応じて複数のフレームワークや管理策を参照し、自社の事業特性、リスク、サービス提供形態に応じたセキュリティ管理を行います。

8. お問い合わせ・追加開示について

8.1 セキュリティに関するお問い合わせ

WeWork Japanのセキュリティに関するご質問は、WeWork Japan公式サイトのお問い合わせフォーム、または担当営業・担当窓口までお問い合わせください。

お問い合わせ内容に応じて、担当部門と連携のうえ、公開可能な範囲で回答いたします。なお、拠点、契約プラン、利用条件、個別のセキュリティ要件により、提供可能な情報や対応内容が異なる場合があります。

8.2 セキュリティチェックシート等への対応

お客様の調達審査、情報システム部門による確認、法務・監査部門による確認等において、セキュリティチェックシートや個別質問への回答が必要となる場合があります。

WeWork Japanでは、サービスの利用検討または契約に必要な範囲で、セキュリティチェックシートや個別質問への回答に対応します。回答にあたっては、公開済み資料、本ホワイトペーパー、契約条件、対象拠点、利用予定サービス、開示情報の機微性等を踏まえ、回答可能な範囲および回答方法を確認します。

なお、詳細なネットワーク構成、内部運用手順、監視・検知条件、ログ仕様、委託先情報、監査結果その他の非公開情報については、公開資料としては開示せず、必要に応じて契約、秘密保持、法令、個人情報保護およびセキュリティ上の必要性を踏まえて、個別に開示可否を判断します。

8.3 追加開示の考え方

WeWork Japanは、お客様が安心してサービスを利用できるよう、セキュリティに関する情報を適切に提供することを重視しています。

一方で、セキュリティ管理の詳細情報には、公開することで当社またはお客様の安全性に影響を及ぼす可能性がある情報が含まれる場合があります。そのため、追加資料、詳細情報、証跡類の開示については、契約、秘密保持、法令、個人情報保護、セキュリティ上の必要性等を踏まえて、適切な範囲で対応します。

開示可能な情報の例としては、認証取得状況、管理体制の概要、物理的セキュリティの概要、ネットワークサービスの概要、責任分界に関する説明、個人情報保護に関する公表情報等があります。

8.4 本ホワイトペーパーの位置づけ

本ホワイトペーパーは、WeWork Japanのセキュリティに関する考え方および主な取り組みを、お客様に理解いただくことを目的とした公開資料です。

本書は、個別契約、サービス仕様書、利用規約、個人情報のお取扱い、その他の契約文書または公表文書に優先するものではありません。サービス内容、提供条件、料

金、対応可否等については、個別契約、対象拠点、契約プラン、利用条件等により異なる場合があります。

また、本書に記載する内容は、作成時点の情報に基づくものであり、法令、技術環境、脅威動向、サービス仕様、運用体制等の変更により、予告なく見直される場合があります。

8.5 更新と継続的な見直し

WeWork Japanでは、本ホワイトペーパーについて、セキュリティ管理の見直し、サービス仕様の変更、法令・ガイドラインの変更、お客様からのご要望、監査・点検の結果等を踏まえ、必要に応じて内容を更新します。

最新版の有無や記載内容に関するご質問がある場合は、WeWork Japan公式サイトのお問い合わせフォーム、または担当営業・担当窓口までお問い合わせください。

8.6 関連情報

個人情報の取扱いについては、WeWork Japanが公表する「個人情報のお取扱いについて」をご確認ください。

また、WeWork Japanのサービス内容、拠点情報、契約プラン、セキュリティに関する個別確認については、公式サイトまたは担当窓口よりご確認ください。

本ホワイトペーパーが、WeWork Japanのセキュリティに関する考え方および主な取り組みをご理解いただく一助となれば幸いです。WeWork Japanは、今後もお客様と協力しながら、安心・安全なワークプレイス環境の維持・向上に努めてまいります。