質の高い社会ネットワークの構築

～利便性が高く安定感・信頼のネットワークとセキュリティ～

当社は、社会に必要不可欠なライフラインである通信ネットワークにおいて、最新かつ高品質なサービスを提供し続けることで、いつでも安定的につながる信頼性の高い通信サービスの実現を目指します。

より良いサービスを提供すべく、2020年3月から提供開始している5Gの全国展開を進めるとともに、成層圏通信プラットフォーム「HAPS」に代表される非地上系ネットワーク（Non-Terrestrial Network、以下「NTN」）ソリューションにより、宇宙空間や成層圏から通信ネットワークを提供することで「どこでも、誰でも、つながる」社会の実現を目指します。

災害時の通信インフラ維持では、防災や減災への取り組みと備えを強化し、どのような状況下でも安定した通信サービスを提供できるよう、ライフラインを維持するための取り組みを強化しています。

さらに、サプライチェーンを標的とした攻撃や働き方改革によるリモートワーク環境を標的とした攻撃など、サイバー攻撃のさらなる巧妙化・複雑化を常に注視しながら、最先端技術を積極的に採用します。高度なセキュリティ環境を整備するとともに、24時間365日のセキュリティ監視と即時対応体制のさらなる充実化を図っています。全社員に向けた高いセキュリティ意識を根付かせるための研修を実施し、データの取り扱いについては、プライバシーセンターを設け、ご自身が情報の利用状況を確認・管理できるお客さまのプライバシーを最優先に考えたダッシュボードを提供します。

5Gやネットワークを最先端テクノロジーやさまざまな顧客接点と組み合わせることで、新たな価値を創造し、持続可能な社会づくりと産業の発展に貢献していきます。

社会課題

- 高品質なネットワークの維持運営
- 自然災害によるインフラ寸断の予防、早期復旧
- 高度化するサイバー攻撃への対応

創出価値

(1) 持続的な生活インフラの整備
(2) 防災・減災に貢献する盤石な通信インフラ構築
(3) データセキュリティとプライバシー保護の取り組みの推進

リスクと機会

リスク
- 超高速・大容量、超低遅延、同時多接続の5Gを前提とする新規ビジネスチャンスの喪失
- 通信障害発生、災害復旧の遅れによる対応コスト増、顧客からの信用低下、契約者離反
- 個人情報の不適切な利用、個人情報漏えいによる顧客からの信用低下、契約者離反

機会
- 5Gエリア全国展開に伴う通信の高速・大容量化を反映したARPUの向上による収益拡大
- 自動運転や遠隔医療など5Gを活用した新たな産業やサービスの展開
- 高い通信品質やセキュリティへの信頼性に対する顧客満足度の向上

KPI

(1)
- 5G展開計画
  5G SA（スタンドアローン）エリア拡大：全都道府県主要部スマホSA化（2026年度）
- ネットワーク重大事故発生件数：0件
- 大容量光海底ケーブル：運用開始（2023年度）

(2)
- 東北ルート：商用運用開始（2023年度）
- 災害応急／復旧機材の維持・強化
  移動基地局車／可搬型移動基地局：200台以上維持、移動電源車配備台数80台以上維持
  可搬型衛星アンテナ：200台以上維持、災害復旧に関わる対外機関との連携強化

(3)
- 情報セキュリティ重大事故件数：0件（毎年度）
- プライバシーに関連する重大事故件数：0件（毎年度）
- お客さまによる自身の情報の取り扱い内容理解促進：プライバシーダッシュボード設定機能追加、アプリ・ウェブサイト利用内容の情報取扱公表

主な事業・取り組み

- 5Gエリアの広域展開と品質向上
- 海底ケーブルプロジェクト参画
- ネットワーク広域化による通信の地域格差解消
- ネットワーク事故防止に向けた取り組み推進
- AIによるネットワーク監視運用支援
- 災害時の通信サービス環境の確保（移動基地局、可搬型衛星アンテナ設備、ドローン活用など）
- 災害時の迅速な通信環境復旧に向けた体制整備
- 基幹ネットワーク3ルート化などの災害復旧対策
- 高度セキュリティシステム、ツールによる運用・管理
- 個人情報の保護と適切な利用の促進
- 社員教育の徹底、環境・設備構築

質の高い社会ネットワークの構築

Key Person Interview

専務執行役員 兼 CTO
佃 英幸

5G通信技術の進歩で新たなサービスの実現へ

当社は、「Beyond Carrier」戦略を掲げ、通信事業基盤をより強固にすると同時に、最新テクノロジーを活用して産業のDX（デジタルトランスフォーメーション）化を推進し、社会課題の解決に取り組んでいます。5Gについては、2020年3月から商用サービスを全国で開始し、5Gスタンドアローン方式（SA）の商用サービスを2021年10月から国内で開始しました。これにより、従来では実現が困難だった超高速・大容量、超低遅延、多数同時接続の通信を実現し、2023年3月には、ネットワークスライシングや企業のニーズに合わせてカスタマイズしたネットワークサービスが可能になるプライベート5Gの提供を始めました。

今後は、5G SAの拡大と、多くの産業のニーズに応えられるプライベート5G（専有型／共有型）の展開で、これまでにないさまざまなサービスを実現します。

災害対策と安全・安心な通信環境の実現

当社は、通信インフラを重要なライフラインと考えています。近年、気候変動や環境の変化により、地球規模で大きな自然災害が多発していますが、災害時における通信サービスへの影響を最小限に抑えるべく、係留気球無線中継システムや有線給電ドローン無線中継システム、移動基地局車や移動電源車の配備をはじめ、ネットワークの冗長化や停電対策の導入など多くの取り組みを実施し、安定した通信サービスの提供に努めています。

また、情報セキュリティの強化やお客さまのプライバシー保護にも重点を置いています。情報セキュリティ強化策として、巧妙化するサイバー攻撃に対応する最新のセキュリティシステムを導入しています。お客さまのプライバシー保護として、社員への教育を行う他、プライバシーセンターの導入によるダッシュボードの提供により、お客さまのパーソナルデータが意図しない形で使われないよう、確認・設定の変更ができる仕組みを提供しています。

NTNソリューションを通じたユビキタスネットワークの構築に向けて

当社は、既存のモバイルネットワークと、衛星（低軌道衛星・静止軌道衛星）および成層圏通信プラットフォーム「HAPS（High Altitude Platform Station）」を組み合わせたユビキタスネットワーク（多階層ネットワーク）により、通信ネットワークのカバレッジの拡張と上空のエリア化に取り組んでいます。世界中のあらゆる企業や産業に、デジタル化・自動化による変革が求められる中、通信の形は今後さらなる多様化が進むと想定しています。当社は、パートナー企業と連携しながら、ユビキタスネットワークを実現し、あらゆる場所でさまざまな通信がシームレスにつながる環境をつくり、社会に貢献することを目指します。

次世代社会インフラの提供に向けて

当社は、これまでの通信インフラから、未来社会を実現する次世代社会インフラを提供する企業へと進化していきます。現在は、データセンターが都市部に集中しているため、データ処理およびそれに伴い消費される電力も都市部に集中しています。これに対して、データセンターを各地に分散して構築することでデータ処理および消費電力を全国に分散させ、電力を地産地消でまかなうことで構造的な課題を解決することができると考えています。今後も安定的な通信ネットワークを提供することはもちろんですが、最新テクノロジーによる新たな価値を創造し続けることで、幅広い分野の社会課題解決に貢献していきたいと考えています。

質の高い社会ネットワークの構築

創出価値 ❶

持続的な生活インフラの整備

5Gネットワークを中心とする高度なセキュリティで守られた安全かつ強靭なインフラの維持と、利便性と信頼性の高い通信サービスを提供します。人・モノ・情報をつなぐ基盤として、社会・経済活動を持続的に支え、さらなる進化を目指し、技術開発に挑戦し続けることで、課題解決や新しい価値の提供に貢献していきます。

5Gネットワークの早期展開に向けた取り組み

当社は、5G基地局の整備を加速して進めています。5G技術をフル活用するため、高速・大容量を用いたサービス開発、高信頼低遅延や多数同時接続に関する先行研究など、さまざまな活動・調査研究に取り組んでいます。

5Gのご利用形態

5Gの利用形態には、いわゆる一般的に5Gと呼ばれる「パブリック5G」の他に、個別に5Gのプライベートネットワークを構築する「ローカル5G」やパブリック5Gを部分的に個別占有する「プライベート5G」といった形態があり、さらに「プライベート5G」には、5G環境をパブリック5Gとシェアする形で運用する共有型と、お客さまの敷地で構築運用する専有型の2つの形態があります。

2023年3月29日には、法人向けの5G（第5世代移動通信システム）マネージドサービス「プライベート5G」として、プライベート5G（共有型）のサービス提供を開始しました。「プライベート5G」では、企業や自治体などのさまざまなニーズに合わせて、個別にカスタマイズした5Gネットワークサービスの提供が可能となります。

ローカル5Gとプライベート5G

ローカル5Gは、通信事業者ではない企業や自治体が、一部のエリアまたは建物・敷地内に専用の5Gネットワークを構築する方法で、他のエリアで通信トラブルが起きた場合やネットワークが混雑した場合、パブリック5Gと比べて影響を受けにくい特長があります。

一方、プライベート5Gは、企業・自治体ごとに個別に構築される点はローカル5Gと変わりませんが、ローカル5Gで必要だった無線免許の取得や保守運用の手間を自社で負担せずに、通信事業者である当社が、個別要件に応じたネットワーク環境を企業や自治体の敷地内の基地局に設置し保守運用を担うことで、個々の要件に適した5Gネットワークを構築できるというメリットがあります。

プライベート5Gの提供により、これまで手間やコスト面からローカル5Gの導入を諦めざるを得なかった企業でも5G活用が進むことが予想されます。ニューノーマルな時代においては、遠隔制御や自動化など、現場に行かずに業務を進めるための技術に対するニーズは高まっていき、リモートワークにおいても5Gを活用することで、よりスムーズかつ効率的に業務を進められるようになります。

本格的なデジタル時代を迎え、5GはDXの推進に大きな役割を果たすと考えています。お客さまの業態でどのような形で5Gを活用するかを考慮し、業務の効率化や競争力の向上につなげることで、持続的な社会の発展に貢献していきます。

パブリック5G 通信事業者保有周波数	プライベート5G（共有型） 通信事業者保有周波数	プライベート5G（専有型） 通信事業者保有周波数	ローカル5G ローカル5G周波数
			
通信事業者が5G環境を全国に順次展開	5G環境をパブリック5Gとシェアする形で運用	ソフトバンクがお客さまの敷地で構築運用	企業や自治体が5G環境を個別構築
構築／運用：ソフトバンク 設置場所：全国	構築／運用：ソフトバンク 設置場所：全国	構築／運用：ソフトバンク 設置場所：お客さまの施設内	構築／運用：お客さま 設置場所：お客さまの施設内

➔ 詳しくはこちら

質の高い社会ネットワークの構築

創出価値 ❶ 持続的な生活インフラの整備

安定的につながる通信サービスの提供

当社は、情報通信サービスの根幹である通信ネットワークを安定的に運用するために、全国のネットワークセンターに技術者を常駐させ、携帯電話の無線基地局や伝送路、センター内に設置されている通信設備などのメンテナンスを行っています。通信ネットワークや無線基地局の稼働状況は、ネットワーク・オペレーション・センターにおいて専門の技術者が24時間365日体制で監視しています。

全国のネットワークセンターやネットワーク・オペレーション・センターで実施した業務改善の施策は「メンテナンス・プロ・コンテスト」を毎年開催することで、他部門に水平展開し、オペレーションの信頼性、効率化を目指します。

また「統合マネジメントシステム」「品質マネジメントシステム」「ITサービスマネジメントシステム」などの国際規格を取得し、サービスの品質を維持・向上するための継続的な業務改善と体制を構築しています。

2022年度の電気通信事業法施行規則第57条に該当するネットワーク重大事故の発生は0件でした。

安全な基地局建設に向けて

安全管理の徹底と事故防止活動の継続に向け、全国安全大会を各施工会社と合同で開催しています。2022年は初の試みとして、メタバース会場での開催実施となりました。安全取組施策として、安全パルスサーベイの実施、事故防止検討会・施工会社へのモニタリング、KYサポートブック配布による事例共有などを実施し、また、安全表彰では、長年にわたって無事故を継続しているビジネスパートナー企業に対して、その安定した業務運営と確実な安全管理ノウハウを表彰しました。

引き続き現地の安全パトロール強化や、現場作業員の教育の徹底をはじめ、無事故で一大プロジェクトを完遂させるべく、安全意識向上のためのメッセージを発信し、事故撲滅に向けた安全啓発活動に取り組んでいきます。

全国安全大会のメタバース会場の様子

電波の安全性

電波の安全性に関する情報提供

電波は、携帯電話サービスだけではなく、防災・消防無線などの災害時の非常用無線として、さらには衛星放送やナビゲーションシステム、無線LANやIoTなどさまざまな分野で利用されており、社会生活になくてはならないものとなっています。

基地局や携帯電話からの電波が健康にどのような影響を及ぼすのか不安に思われるお客さまにも、安心して携帯電話やスマートフォンなどをご利用いただけるよう、電波が健康に与える影響について調査し、電波の安全性に関する情報を公表しています。

電波の安全に関するポリシー

基地局および携帯電話などからの電波の強さが、人体に影響を与えないよう「電波防護」のための関係法令が制定されており、当社を含む電波を使用する事業者は、電波法などの関係法令を遵守しています。

電波の安全に関するポリシーや携帯電話などの局所吸収指針の下、サービスを提供しています。

➔ 詳しくはこちら

質の高い社会ネットワークの構築

創出価値 ❶

持続的な生活インフラの整備

海外ネットワーク構築に向けた取り組み

当社が取り組む海底ケーブルプロジェクト「ADC（Asia Direct Cable）」は、全長約9,400kmの光海底ケーブルで、日本、中国、香港、フィリピン、ベトナム、タイ、シンガポールを結び、2023年中の完成・運用開始を目指しています。

ADCは、最新の光波長多重伝送方式を採用することで、140Tbps（テラビット毎秒）以上の設計容量を実現し、5Gをはじめ、IoT、AI、クラウドサービスなど、アジア太平洋地域で急増するインターネットトラフィック需要に対応します。また、ADCの運用によって、アジア太平洋地域のネットワークの冗長性の確保、信頼性の高い通信の実現、回線需要変化への柔軟な対応に貢献します。

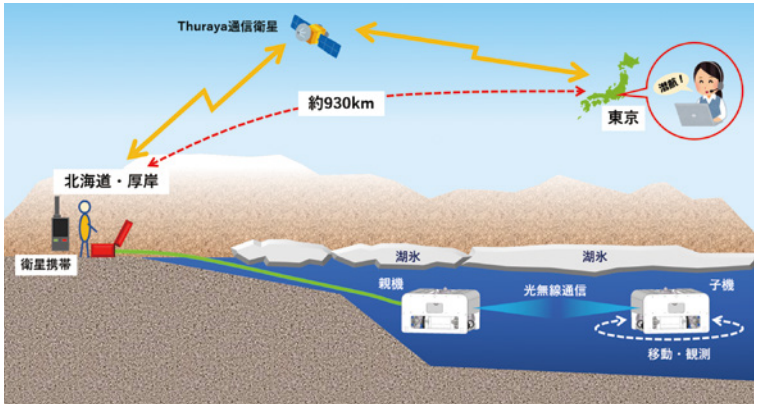
当社では、ADCの建設において、日本の陸揚げ局として千葉県南房総市に所在する「ソフトバンク丸山国際中継所」を提供しています。ソフトバンク丸山国際中継所は、すでに運用開始している太平洋横断光海底ケーブル「JUPITER」など多数の海底ケーブルが接続されており、国際通信のハブとなるデータセンターとして重要な役割を担っています。ADCやJUPITERとの接続および接続拠点の整備により、アジア太平洋地域におけるトラフィック需要に対して継続的かつ安定的なサービスを提供するとともに、日本における国際海底ケーブルの重要なゲートウェイとして貢献していきます。

「ADC」の敷設経路イメージ図

Beyond 5Gによる海の産業革命を目指して

当社と国立大学法人東京海洋大学の後藤 慎平助教らによる研究チームは、北海道厚岸翔洋高等学校の柴田 耕一郎教頭の協力の下、Beyond 5Gによる海の産業革命を目指して、水中ロボットをリアルタイムで遠隔制御する実証実験に世界で初めて※成功しました。

水中では、従来、音響通信が用いられてきましたが、伝搬速度が遅く、情報量も少ないなど、精密な測位やリアルタイム性、セキュリティに多くの課題がありました。これらの課題を解決する手法として、可視光通信技術が注目されていますが、可視光通信にも極めて高い指向性を持つ光を正確に受光しなくてはならないという課題があり、高精度な光トラッキング技術が要求されます。今回の実験では、通信対象をカメラで視認しておおまかにトラッキングできていれば通信が確立可能で、高精度な光トラッキング技術までは必要としないOCC（Optical Camera Communication）技術を活用しました。また、外洋や極域などの海域までカバレッジを拡張するNTNとしてThuraya Telecommunications Companyの通信衛星を利用した無線通信を活用し、地上の電波が届かない厚岸湖の分厚い氷が張った水中の狭隘空間で、2台の水中ロボットを約930km離れた東京都港区の当社本社から、自在に制御することができました。



NTNとOCCによる水中ロボットの制御実験のイメージ図

この技術が実用化されれば、アクセスが困難な地域や海域においても、データ収集や観察、機器の監視、メンテナンスなどのための現地調査の負担が軽減されます。また、OCCや、中・長距離での大容量通信が可能な、高度な光トラッキング技術を活用した水中レーザー光無線通信技術を活用することで、従来の音響通信による測位が困難な極浅海域でも、安定的かつリアルタイムにロボットとの通信が可能であることから、海氷または湖氷下などにおける漁業や調査での活用も見込まれます。さらに、海象・気象の影響を受けにくいことから、これらの水中光無線通信技術による水中灯台などのインフラを構築することで、洋上物流に代わる次世代物流への活用も期待できます。

水中光無線通信技術によって、実用的な水中（海中）無線通信ネットワークの構築が可能になることで、海洋産業の効率化や新産業の創出など大きな経済効果をもたらします。当社と東京海洋大学は、今後、さらに実用的かつ確実な技術にするため、南極海などでの実証実験を通して、まずは極地や島しょ地域などでの実用化に取り組む計画です。そしてBeyond 5Gによる海洋産業革命の実現に向け、通信距離10数mから100m以内の短距離・中距離における1対1および多対多の光無線通信や、通信距離数100mを超える長距離の1対1の水中光無線通信の実現によって、全球的な海中通信網の確立を目指します。

※ 2023年3月3日時点（当社および東京海洋大学調べ）

質の高い社会ネットワークの構築

創出価値 ❶

持続的な生活インフラの整備

NTNソリューションの展開

当社は、世界におけるデジタルデバイドの解消をミッションに掲げており、宇宙空間や成層圏から通信ネットワークを提供するNTNと地上のモバイルネットワークを融合したユビキタスネットワークの構築を目指しています。これにより、世界中のあらゆる場所でさまざまな通信がシームレスにつながる環境を目指します。また、ユビキタスネットワークの構成要素として、「OneWeb」「HAPS」といったNTNソリューションを展開予定です。

高速かつ低遅延な通信を実現する「OneWeb」

「OneWeb」は、静止衛星よりも地球に近い、高度1,200kmにある低軌道衛星による高速大容量衛星通信です。12の極軌道上に衛星を打ち上げており、2時間に1回の速度で地球を周っています。静止衛星よりも地球に近い低軌道に多くの衛星を打ち上げることで、従来の衛星通信と比較して高速かつ低遅延の通信を実現します。

「OneWeb」を提供するOneWeb社と当社は2021年4月、日本での展開に向けた協業に合意し、サービス開始に向けて準備を進めています。2023年の初めに衛星コンステレーションの構築を完了しており、同年末までにグローバルの通信ネットワークが完成する予定です。これを受けて、当社は、日本国内におけるOneWebを活用した衛星通信サービスの提供に向けた準備に入ります。

(注) 本サービスの今後の提供に関しては、検討中のため変更となる場合があります。

無人航空機から直径約200kmエリアにサービスを提供する「HAPS」

成層圏通信プラットフォーム「HAPS」は、高度20kmの成層圏に滞空している無人航空機から、地上に向けて通信サービスを提供します。1機当たり直径約200kmと地上基地局に比べて非常に広範囲なエリアをカバーできるため、島々や山岳部といった人口の少ないエリアに対しても、スポットで電波を提供することができます。また、災害対策では、被災地の上空に機体を飛ばすことで、暫定的に通信エリアの復旧を実現します。

HAPS向け電波伝搬シミュレーターを開発

当社とHAPS事業展開のために設立したHAPSモバイル株式会社は、両社主導の下、2021年10月にHAPS向け「電波伝搬推定法」の国際標準化を達成し、この推定法を実装した電波伝搬シミュレーターを2022年11月に開発しました。これにより、HAPSのサービス展開に向けた電波伝搬解析をより正確かつ効率的に行えるようになります。

この電波伝搬シミュレーターは、当社とHAPSモバイルがITU-Rの国際標準化に貢献したHAPS向け「電波伝搬推定法」の計算方法を実装しており、緯度や経度によって異なる気温や降雨の強度などの気象データ、地形や建物などの地理情報を活用して伝搬損失を解析できるため、世界中のあらゆる地域を対象に正確な電波伝搬解析を行うことができます。

今後両社は、このシミュレーターを活用し、電波伝搬解析およびシステム設計の検討を行っていきます。

次世代リチウム金属電池セルの電池パックを開発、成層圏で動作実証に成功

当社は、2022年10月に次世代リチウム金属電池セルを使用したHAPS向けの電池パックを開発しました。Enpower Japan株式会社と共同開発した次世代リチウム金属電池セルは、重量エネルギー密度439Wh/kgを誇り、またエナックス株式会社の協力の下、拘束機構やヒーター、断熱材などの各部材の軽量化にも成功し、重量エネルギー密度300Wh/kgの電池パックの実現に大きく近づきました。

そして当社とHAPSモバイル株式会社は、2023年1月30日から2月2日にかけて、成層圏での電池パックの充放電サイクル試験を実施し、マイナス約60度前後の極低温の成層圏でも地上の試験と同レベルの正常な動作実証に初めて成功しました。

今後は、実際のHAPSの動力源として大型電池パックの開発を目指すとともに、HAPSに加えて、産業用ドローンなどへの搭載も検討していきます。

成層圏での動作実証

創出価値 ❷

防災・減災に貢献する盤石な通信インフラ構築

災害時において、通信インフラは最も重要なライフラインの一つであり、いかなる状況下でも安定した通信サービスを提供できるよう、災害に強い通信ネットワークの構築を図るとともに、災害発生時の速やかな復旧体制づくりに努めています。AIやICTを活用し、災害情報の迅速な集約・伝達を行い、災害から身を守る防災対策や、災害発生後の被害を少なくする減災対策に取り組みます。

災害対策について

災害協定に基づく体制

大規模災害時の通信確保のために広範な相互協力の下、迅速な復旧活動の実施を目的に、防衛省および海上保安庁と「災害協定」を締結しています。大規模災害の発生時における人命救助活動などに必要な通信手段として、当社は防衛省および海上保安庁へ、衛星携帯電話や携帯電話などの通信機器を提供します。

また、防衛省および海上保安庁は、当社が被災地において通信手段の確保や復旧活動を行うに当たり、物資の輸送や各種施設・設備の使用などに協力します。

有事に備え、各地で陸上自衛隊や海上保安庁と連携した訓練を実施しています。今後も防衛省および海上保安庁ならびに関係機関との円滑な連携を図りながら災害対策に取り組むとともに、通信事業を担う企業としての社会的責任を果たしていきます。

災害時マネジメント体制

防災等業務計画

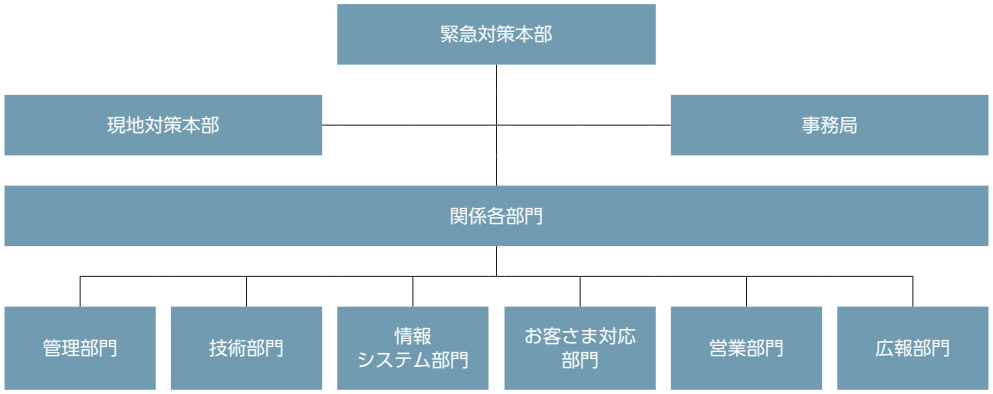
「災害対策基本法」に基づき、国の定める指定公共機関として「防災業務計画」を策定しています。災害予防対応や災害発生時の体制を確立し、災害が発生した際は「防災業務計画」を遵守するとともに、その他の関連機関と連携し対応します。

社内体制の整備

災害発生時に迅速に対応するため、対応マニュアルの作成や周知徹底を行う他、非常時の連絡体制の整備や防災備蓄品を配備しています。

対応マニュアルの徹底	災害などによる設備被災の発生が予想される場合、速やかな復旧により、サービスへの影響を最小限とするための対策（災害対応マニュアルの策定など）を確立しています。
非常時の体制確立と連絡網の整備	災害発生時の通信ネットワーク障害に即応できる体制を確立し、緊急連絡網を整備して万が一に備えています。
災害対策用設備および防災備蓄品の配備	通信網の早期復旧を図るため、復旧資材および予備備品などを確保するとともに、飲料水や食料などの生活必需品も全国の拠点に備蓄しています。また、災害対策用設備（非常用発電機など）を全国各地に配置しています。
緊急対策本部の設置	大規模災害など緊急事態発生時には、担当部門が各事業分野における影響や被害の情報収集・分析を行います。その上で、影響や被害状況に基づき緊急対策本部を設置し、事態の早期復旧などの対策を講じます。

緊急対策本部 体制図



質の高い社会ネットワークの構築

創出価値 ❷ 防災・減災に貢献する盤石な通信インフラ構築

災害対策について

移動電源車の全国配備

災害などによる停電で電源が途絶えた基地局の電源供給などを目的に、全国に移動電源車を配備しています。移動電源車配備台数は80台以上の維持を目標に2023年3月現在、全国に91台配備して継続したサービスを提供できるように努めています。

移動電源車

移動電源車（地域別配備台数）

（2023年3月現在）

北海道	6	近畿	11
東北	9	中国	6
関東	18	四国	7
信越	2	九州	13
北陸	5	沖縄	4
東海	10	計	91台

移動基地局車・可搬型移動基地局の配備

災害などによる基地局の倒壊や停電などで、通信サービスがつながりにくいエリアやご利用になれないエリアを早期に復旧させるため、移動基地局を配備します。移動基地局にはさまざまなタイプがあり、被災エリアの状況に応じた基地局を全国各地に配置し、緊急時に備えています。移動基地局車と可搬型移動基地局を合わせて200台以上の維持を目標に掲げ、被災エリアの復旧に当たります。


移動基地局車

移動基地局車

■ 移動基地局車 小型タイプ

災害などにより伝送路に被害が生じた際、衛星エントランスを用いて臨時の基地局を開設します。小型タイプの機動性を生かして、被災エリアにいち早く駆けつけます。

■ 移動基地局車 中型タイプ

伝送路に被害が生じた際には衛星エントランスを、伝送路が使用できる際は固定の伝送路を用いて、臨時の基地局を開設します。

■ 移動基地局車 大型タイプ

伝送路に被害が生じた際には衛星エントランスを、伝送路が使用できる際は固定の伝送路を用いて、臨時の基地局を開設します。最大通話可能数が最も多いタイプです。全ての車両でSoftBank 4G LTEに対応しています。

移動基地局車（地域別配備台数）

（2023年3月現在）

	小型タイプ	中型タイプ	大型タイプ
北海道	1	4	2
東北	1	4	3
関東	2	13	10
信越	0	3	1
北陸	1	2	2
東海	1	6	6
近畿	1	6	4
中国	1	4	2
四国	1	3	2
九州	1	7	3
沖縄	0	2	1
計	10台	54台	36台

可搬型移動基地局

衛星エントランス対応の可搬型移動基地局を全国に200台配備しています。そのうち100台は車載が可能なタイプです。

可搬型移動基地局

質の高い社会ネットワークの構築

創出価値 ❷ 防災・減災に貢献する盤石な通信インフラ構築

災害対策について

可搬型衛星アンテナの配備

短時間で臨時衛星伝送路の構築が可能な組み立て式の自動捕捉衛星アンテナです。高速化対応の機材も備え付けられており、高速衛星回線を利用することで、光ファイバー回線の代わりとして利用します。現在、全国に計282台配備しています。

可搬型衛星アンテナ

可搬型衛星アンテナ（地域別配備台数）

（2023年3月現在）

北海道	14	近畿	24
東北	16	中国	22
関東	57	四国	26
北陸	10	九州	73
東海	18	沖縄	22
計			282台

マイクロエントランス

電波を遮る障害物などがない双方の基地局にアンテナを取り付け、エントランス無線（ミリ波およびマイクロ波帯の周波数の電波）を使用した電波の送受信を行うことで、光ファイバー回線の代わりとして利用します。

行政や自治体との連携

災害時を想定した防災訓練

当社は、大規模災害発生時に迅速な対応を行うため、自治体や陸上自衛隊、防衛省、海上保安庁と連携した防災訓練を定期的に実施しています。いざというときにスムーズに連携できるよう、自衛隊・海上保安庁との物資積み込み訓練や、自治体の主催する「総合防災訓練」「帰宅困難者対策訓練」など、電力会社など他のライフライン事業者と共に参加し、災害時の連絡体制や連携手段を確認しています。

災害時復旧訓練では、どのようなときでも通信サービスを提供し続けられるよう、シーン・ケース別に復旧方法や手順を確認します。災害による基地局の倒壊や停電、また基地局とネットワークをつなぐための伝送路の断線などで、通信サービスがつながりにくい、またはつながらなくなったサービスエリアを早期に復旧させるため、移動基地局車や可搬型基地局などさまざまな設備を全国各地に配備しています。停電時は非常用バッテリーに切り替え電力を確保し、停電の長期化などで電源が不足した事態に備えて非常用発電機を各地域の保守拠点に配備し、定期的な実地訓練を行っています。

有線給電ドローン無線中継システム

当社は、災害による基地局の倒壊などで通信サービスが不通になった場合、ライフラインの一部である携帯電話サービスを迅速に復旧することを目的に、「有線給電ドローン無線中継システム」を国立大学法人東京工業大学と双葉電子工業株式会社と共同開発し、2022年7月から運用を開始しました。災害時の臨時回線としての利用に備え、まず関東エリアの当社のネットワークセンターに配備し、順次全国の拠点に配備していく予定です。

有線給電ドローン無線中継システムは、無線中継装置と有線給電システムを搭載しています。地上に設置した無線中継装置（親機）と、ドローンに搭載した無線中継装置（子機）で構成されており、親機と子機間の通信はRoF（Radio on Fiber）技術を用いた光ファイバーで行います。親機に接続した基地局無線装置とモバイルネットワークの接続は、基本的に衛星通信経由で行うため、基地局などの地上設備の被災の影響を受けずに、迅速に臨時のサービスエリアを構築できます。また、本システムの通信方式は、LTE（2.1GHz帯）に対応しており、ドローンを地上100mに停留飛行させることで、郊外では半径3km以上、見通しの良いエリアでは半径5km以上のサービスエリアを確保できます。

基地局の建て直し

基地局全体および通信機器の流出など、基地局が被災して使用できなくなった場合でも、当該基地局を利用するお客さまが確認され、地盤・土台の安全性が確保されている場合には、同じ場所に新しい基地局を建て直します。

質の高い社会ネットワークの構築

創出価値 ❷ 防災・減災に貢献する盤石な通信インフラ構築

行政や自治体との連携

自治体への端末貸し出し

被災地域での連絡手段や復興活動、救援活動などに使用するために衛星電話や携帯電話、タブレットなどを全国の拠点に配備し、自治体や公共団体、非営利団体などへ無償で貸し出す体制を整備しています。「令和4年7月14日からの大雨」「令和4年8月3日からの大雨」「令和4年台風第15号」において、携帯電話やWi-Fi機器などを被災地に貸し出し、2023年3月現在で合計101台の端末等の貸し出しを行いました。

➔ 災害対策・復興支援 P. 202～203

避難所での連絡手段の支援

災害時における避難所への支援として、電話連絡用の携帯電話や固定型電話機の他、お手持ちのパソコン・スマートフォンでインターネット回線を使って、安否確認、支援情報を収集するための通信手段であるWi-Fi機器（00000JAPAN）、停電時における充電サービスの設置など、無料で利用可能な設備を提供しています。

災害時の通信確保

災害発生時に、被災地域で安否確認などのために電話回線やインターネット回線、ネットワーク機器などの一部にアクセスが集中し、通常の通話やデータの送受信が行えなくなる状態を「輻輳（ふくそう）」と呼びます。電気事業通信法で定められた110番や119番などの重要通信も、輻輳によりつながりにくくなる場合があります。

このような事態を防ぎ、輻輳の拡大による大規模な通信システムのダウン（通信障害）を回避するために、輻輳の規模に応じて通信サービスを一時的に規制することで、一定の通信サービスを維持・確保します。

また、災害時に携帯電話サービスに影響が発生した場合、速やかに災害対策本部を設置し、全国から人員を招集するとともに、移動基地局車や可搬型基地局、可搬型衛星アンテナ、移動電源車、可搬型発電機などの機材を現地に搬入し、給電作業やエリア確保のための復旧活動を迅速に行います。

今後も気象災害などによる被害の影響を最小限にとどめるべく、防災・減災に貢献する盤石な通信インフラの構築に努めていきます。

災害時の安心を提供するサービス

災害や防災に関する情報の提供や災害が発生した際の情報通知、お客さまのコミュニケーション手段を確保するためのサービスを提供しています。

■ Yahoo! 防災速報

突然の豪雨や地震、避難指示などの情報をプッシュ通知でいち早くお知らせします。現在地に加え国内最大3地域まで設定でき、旅行先や離れた家族の情報もお届けする無料の防災アプリケーションです。

■ 防災手帳

災害発生時の備えとしてだけでなく、日常にも役に立つコラムや防災用品などのコンテンツを提供しています。

■ 緊急速報メール

気象庁が配信する「緊急地震速報」や「津波警報」、国・地方公共団体が配信する「災害・避難情報」などを、対象エリアにいるお客さまにブロードキャスト（同報）配信するサービスです。

■ 災害用伝言板

災害時に音声発信が集中してつながりにくくなった場合に、お客さまよりメッセージをお預かりし、伝えたい相手にメッセージをお届けするサービスです。

■ 緊急通報の位置情報通知

携帯電話から緊急通報（110番、118番、119番）した場合に、緊急通報を行った場所の位置情報を緊急通報受理機関に自動的に通知します。

創出価値 ❸

データセキュリティとプライバシー保護の取り組みの推進

最先端テクノロジーを活用したネットワークの監視・運用と、社員に対するセキュリティ教育を徹底し、通信の秘密および顧客情報の保護の対策に最善を尽くします。情報セキュリティリスクの把握や、お客さまのパーソナルデータなどのプライバシーの保護に率先して取り組むことで、安心・安全な通信環境を利用できる社会の実現に貢献します。

情報セキュリティ・プライバシー保護

方針

当社は、情報漏えいリスクに対し、抜本的かつ高度な対策を講じることにより、常にお客さまをはじめ社会からの信頼を得られるよう「情報セキュリティポリシー」および「パーソナルデータの保護に関する方針」を策定し、順守しています。さまざまな脅威から情報資産を保護し、かつ適正に取り扱うことにより、情報セキュリティの維持に努めます。

情報セキュリティポリシー

■ 情報セキュリティポリシーの運用

1. 情報セキュリティ管理体制の構築

当社が保有する全ての情報資産の保護に努め、情報セキュリティに関する法令その他の規範を順守することにより、社会からの信頼を常に得られるよう、非常にセキュアな情報セキュリティ管理体制を構築していきます。

2.「最高情報セキュリティ責任者」の配置

「最高情報セキュリティ責任者（CISO: Chief Information Security Officer）」を配置するとともに、情報セキュリティ委員会を組織します。これにより全社にわたる情報セキュリティの状況を正確に把握し、必要な対策を迅速に実施できるよう積極的に活動します。

3. 情報セキュリティに関する内部規程の整備

情報セキュリティポリシーに基づいた内部規程を整備し、個人情報だけではなく、情報資産全般の取り扱いについて明確な方針を示すとともに、情報漏えい等に対しては、厳しい態度で臨むことを社内外に周知徹底します。

4. 監査体制の整備・充実

情報セキュリティポリシーおよび規程、ルール等への準拠性に対する内部監査を実施できる体制を整備していきます。また、より客観的な評価を得るために外部監査を継続していくことに努めます。これらの監査を計画的に実施することにより、従業員等がセキュリティポリシーを順守していることを証明します。

5. 情報セキュリティ対策を徹底したシステムの実現

情報資産に対する不正な侵入、漏えい、改ざん、紛失、破壊、利用妨害等が発生しないよう、徹底した対策を反映したシステムを実現していきます。対策としては、高セキュリティエリアでの作業「need to knowの原則」※に基づくアクセス権付与、データベースアクセス権の制限等、データやシステムへのアクセスを徹底的に管理する考え方で臨みます。

※need to knowの原則：「情報は知る必要のある人のみに伝え、知る必要のない人には伝えない」という原則

6. 情報セキュリティリテラシーの向上

従業員等にセキュリティ教育・訓練を徹底し、当社の情報資産に関わる全員が、情報セキュリティリテラシーを持って業務を遂行できるようにします。また、刻々と変わる状況に対応できるよう、教育・訓練を継続して行っていきます。

7. 業務委託先の管理体制強化

業務委託契約を締結する際には、業務委託先としての適格性を十分に審査し、当社と同等以上のセキュリティレベルを維持するよう要請していきます。また、これらのセキュリティレベルが適切に維持されていることを確認し続けていくために、業務委託先を継続的に見直し、契約の強化に努めます。

■ 情報セキュリティポリシーの対象

当ポリシーが対象とする「情報資産」とは、当社の企業活動において入手および知り得た情報ならびに当社が業務上保有する全ての情報とし、この情報資産の取り扱いおよび管理に携わる当社の「役員、社員、派遣社員等」および当社の情報資産を取り扱う「業務委託先およびその従業員」が順守することとします。

質の高い社会ネットワークの構築

創出価値 ❸ データセキュリティとプライバシー保護の取り組みの推進

情報セキュリティ・プライバシー保護

情報セキュリティ体制

当社は、情報セキュリティに関する法令その他の規範を順守し、情報資産の保護やサイバー攻撃を防御するため、情報セキュリティ管理体制を構築しています。従業員が順守すべき「情報セキュリティポリシー」を制定、「最高情報セキュリティ責任者(CISO：Chief Information Security Officer)」を設置するとともに、CISOを委員長とする情報セキュリティ委員会(ISC：Information Security Committee)およびSoftBank Computer Security Incident Response Team (SoftBank CSIRT) を組織し、環境変化、技術革新に適合した対策の見直しや、情報セキュリティ・サイバーセキュリティ対策に有益な情報を共有しています。

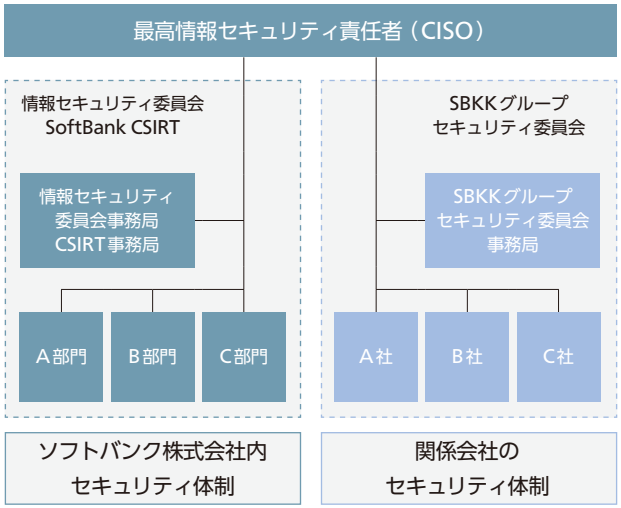
なお、情報セキュリティに起因するシステム障害が発生した場合、システム運用責任者とCISOが協力して状況の把握、対応方法を検討し復旧します。また、重大な状況が発生した場合、社長を緊急対策本部長とする緊急対策本部を設置し対応に当たるとともに、総務省などの監督官庁に対し、法令の定めに応じ速やかに報告します。

情報セキュリティ委員会(ISC)

CISOを委員長として、各部門の情報セキュリティ管理担当者などで構成する情報セキュリティ委員会(ISC)を設け、全社横断的な組織として情報セキュリティ施策の推進・管理に努めています。また、効果的なセキュリティ施策を実行するために、情報セキュリティ委員会事務局(ISC事務局)を設置し、情報セキュリティの施策や計画の迅速な推進・調整を行っています。

■ ISCの役割

・情報セキュリティ活動に有益な情報の共有
・情報セキュリティ活動に関わる全社的な施策・計画の共有
・情報セキュリティに関わる全社的な状況の把握と改善
・情報セキュリティ教育の推進・啓発
・情報セキュリティ施策の各部署間の調整



SoftBank CSIRT

SoftBank CSIRTを組織することにより、セキュリティインシデントの未然防止と、迅速なインシデント対応により被害を極小化しています。SoftBank CSIRTは、当社サービスのセキュリティインシデントに対応する組織です。CISOの下、セキュリティ部門のメンバーおよび各部門の所属長に任命されたメンバーで構成されています。CSIRT事務局を設置し、情報セキュリティ委員会事務局および社内外の関連組織とともに対応しています。

また、インシデントの未然防止として、脆弱性対応(情報収集と分析、対応依頼、対応状況の把握)、セキュリティルールの策定、セキュリティ教育、注意喚起、インシデント発生時の準備・対応として、インシデント発生時対応フローの整備、インシデント対応訓練などを行っています。

関係会社のセキュリティ体制

当社は、関係会社(当社子会社および関連会社)でリスク管理体制を整備し、情報セキュリティ・サイバーセキュリティに関するリスクの低減および、その未然防止を図るとともに、リスクに対する評価・分析および対策・対応を行っています。

CISOを委員長とし、関係会社の情報セキュリティ管理の責任者を構成員とする、SBKKグループセキュリティ委員会を設置し、情報セキュリティに関する脅威やその対策についての情報共有、またセキュリティ教育および訓練の実施、インシデント発生時の対応の連携などを行っています。また、当社グループ各社による適正なセキュリティ管理に必要な体制および順守事項などを定めた「ソフトバンク関係会社セキュリティガイドライン」を策定しています。

質の高い社会ネットワークの構築

創出価値 ❸

データセキュリティとプライバシー保護の取り組みの推進

お客さまの情報を守るために

当社は、安心して利用できるサービスを提供するために、情報漏えいやサイバー攻撃からお客さまを守る対応を行っています。

セキュリティ対策

お客さまの情報をはじめとした各種情報資産を守るために、セキュリティ体制の整備、社内でのサービス開発・導入時のセキュリティチェックやアドバイス、リリース前・運用中のセキュリティ診断を実施しています。サービスや設備を監視するSOC (Security Operation Center) の運営、規定の整備、社内や他組織との連携、米国国立標準技術研究所 (NIST) のCSF (Cybersecurity Framework) や米国CIS (Center for Internet Security) のCIS Controlsを用いた対策内容の見直しや新しい取り組みの検討なども行っています。

徹底した情報管理

当社のファシリティ環境においては、レベル1から5の5段階のセキュリティエリアを設定し、それぞれのレベルに応じて厳格に管理しています。レベル3以上を「高セキュリティエリア」と位置付け、個人情報や通信の秘密など、特に重要な情報はこのエリア内のみで取り扱います。

一例として、高セキュリティエリアに指定されているカスタマーサポートセンターでは、警備員とカード認証による入退室管理をはじめ、禁止携帯品の持ち込み防止など、高セキュリティエリア専用のルールを設定し、徹底したセキュリティ管理を実施しています。

また、取り組みの一環として、情報セキュリティマネジメントシステムの国際規格であるISO 27001の認証を満たした運営を実施しており、毎年2回、プライバシーポリシーの順守状況を含めて情報セキュリティマネジメントが適切に運用されていることを確認するため、ISO 27001に基づく外部監査を受けています。

セキュリティ監視

当社では、お客さまの情報や通信サービスを提供する設備を守るため、SOC (Security Operation Center) にて、セキュリティアナリストが24時間365日、セキュリティ監視を実施しています。

サイバー攻撃対策として、通信サービスを提供する設備へのDoS攻撃※や、設備と接続している機器への侵入に対する監視、業務用パソコンのマルウェア感染や不正なサイトへのアクセス検知、社内システムの脆弱性を突いた攻撃への監視などを行っています。また、社内に対しては、不正な情報持ち出しや機器の操作を抑止しています。

※ DoS攻撃：対象のサイト等へ大量のデータを送り、システムが正常に作動しない状態へ追い込む攻撃

お客さまの利用環境を守る取り組み

ウイルス、スパイウェア、ワンクリック詐欺などの危険からお客さまを守り、お客さまが快適に携帯電話やスマートフォン、インターネットのサービスを利用できるよう、さまざまなセキュリティ対策を提供しています。

■ ウイルス対策

「スマートセキュリティ powered by McAfee®」は、お客さまのスマートフォンをウイルス被害から守ります。インストールしたアプリケーション、メール添付ファイル、microSDメモリカードを通して侵入するウイルスを検出します。

■ ワンクリック詐欺対策

「詐欺ウォール／Internet SagiWall」は、お客さまのインターネット利用時に、ワンクリック詐欺などの危険なサイトを検知します。閲覧するウェブサイトを常に監視して、危険の疑いのあるサイトにアクセスすると警告画面を表示します。

■ セキュリティ保護

「BBセキュリティ」は、お客さまのスマートフォンやパソコンなどのセキュリティ環境を常に最新に維持できる「SoftBank光」「SoftBank Air」をご利用中のお客さま向けのサービスです。

■ データ盗聴・ハッキング対策

「セキュリティチェッカー」は、公衆Wi-Fiなどのネットワーク接続時に、大事なデータや機種を守り、盗聴や通信傍受をはじめとした危険を検知し、お客さまのスマートフォンを保護します。

迷惑メール対策

携帯電話やスマートフォンに突然届く迷惑メールや架空請求メールなどの悪質メールを防ぐため、蓄積されたスパム (迷惑メール) データベースを基にメールの内容を機械的に判断し、スパムと判断されたメールの受信をブロックする迷惑メールフィルターを標準で提供しています。また、受信された迷惑メールを転送するだけで申告が可能な迷惑メールの申告窓口を開設し、当社の契約回線から迷惑メールの送信が確認された場合は、利用停止や契約解除などの厳しい措置を講じます。

質の高い社会ネットワークの構築

創出価値 ❸ データセキュリティとプライバシー保護の取り組みの推進

お客さまの情報を守るために

不正アクセス防止対策

ウイルス感染やメール本文に記載されたURLへアクセスした結果、銀行口座番号、クレジットカード番号、ID・パスワードなどの個人情報が悪意を持った第三者に不正に取得される事案が多発しています。これらの情報を用いて、ご利用料金やご契約内容の確認・変更のお手続きができる会員ページ「My SoftBank」「My Y!mobile」への不正アクセスを防止し、お客さまの個人情報を守るため、セキュリティを強化しています。

■ 暗証番号の設定

「My SoftBank」「My Y!mobile」にログインする際、ご契約時に申込書にご記入いただいた暗証番号を必ず入力する設定へ変更できます。

■ ワンタイムパスワードの発行

ソフトバンクまとめて支払い、ワイモバイルまとめて支払いをご利用の際、お客さまの携帯電話にSMS（メール）で認証番号をお送りします。この番号は、一定時間のみ有効なコードで、契約者本人のみ知ることができます。

■ 不正アクセス対策

「なりすまし」などの不正アクセス対策として「My SoftBank」「My Y!mobile」の一部のメニューを閲覧・利用する際に、SMS・eメールなどで携帯電話の利用状況などを確認する場合があります。

連携して守るサイバーセキュリティ

ライフラインである通信インフラを担う事業者として、また、通信と最先端技術を融合した革新的なサービスの提供を目指す企業として、社外のさまざまな組織・団体と連携し、社会全体のセキュリティ向上に努めています。社外組織との連携は、SoftBank CSIRTが担当しています。

国内外CSIRTとの連携による情報交換

SoftBank CSIRTは、国内外のセキュリティ団体・組織に加盟し、他社のCSIRTと共に共通のセキュリティテーマや課題について議論し、効果的な対応策・解決策を検討しています。

▼ 主な加盟団体・組織

一般社団法人　日本コンピュータセキュリティインシデント対応チーム協議会
（日本シーサート協議会）

FIRST (Forum of Incident Response and Security Teams)

一般社団法人　ICT-ISAC

インシデント発生時の連携と合同演習

複数の組織で同一原因によるインシデントが発生する場合や一つの組織のインシデントが他組織にも影響する場合は、必要に応じて他社CSIRTと連携して対応しています。

また、インシデント発生時に迅速に対応できるよう、定期的に他社CSIRTと合同演習を行い、発生時の対応や組織間の連携を確認しています。

これらの取り組みを通して、インシデントが及ぼす影響を最小限に抑え、被害の低減に努めています。

脆弱性関連情報の受け付け

脆弱性診断を行うなどさまざまな取り組みにより、当社ウェブサイトおよびサービスのセキュリティ向上に努めています。また、社外の技術者が当社ウェブサイトやサービスの脆弱性を発見した場合は、SoftBank CSIRTにて情報提供を受け付け、担当部署や関係者と対応に当たっています。

質の高い社会ネットワークの構築

創出価値 ❸

データセキュリティとプライバシー保護の取り組みの推進

お客さまの情報を守るために

継続的なセキュリティ強化

デジタルデバイスの普及や巧妙化するサイバー攻撃に対し、新しい技術や手法の採用、意識向上のための社員教育、専門家の育成を行うことで継続的なセキュリティ強化に努めています。

人的対策

■ 従業員の教育

日々の業務の中で情報を適切に取り扱えるよう、役員・従業員を対象とした集合研修や定期的なeラーニング教育、各種訓練、セキュリティルールの見直しなどを継続的に行い、情報セキュリティ・サイバーセキュリティに関する意識向上に取り組んでいます。

社内研修では、特に「個人情報保護」「通信の秘密」「内部不正対策」に関する事項を主なテーマとしており、情報セキュリティの知識およびモラルの向上に継続的に取り組んでいます。

また、情報セキュリティに関する資料や啓発動画は、いつでも従業員が閲覧できるよう、社内のイントラネット上に掲載しています。2022年度はグループ会社も対象にした「グループセキュリティ月間」を定め集中的に教育を実施し、グループ全体の意識向上に取り組みました。

■ セキュリティ人材の育成

日々変化するセキュリティ脅威と戦うために、セキュリティ担当者は、脅威情報や対策情報の収集と共有、技術・知識の向上に努めています。また、専門的な知見を強化するためにセキュリティ関連資格の取得を推進しています。

セキュリティ担当者が持つ主な資格

CISSP、公認情報システム監査人（CISA）、公認情報セキュリティマネージャー（CISM）、情報処理安全確保支援士（RISS）、GIAC系資格、CEH、AWS 認定 セキュリティ専門知識等

技術的対策

■ 監視技術

近年、攻撃手法の複雑化によってインシデントの早期検知が困難な状況となる中、検知数は日々、増加傾向にあります。このような状況下でも攻撃の兆候を見逃さないために、当社では検知手法の継続的改善、脅威インテリジェンス（攻撃の検知や遮断に利用可能な情報）を活用した分析と対策の実施、対応業務の自動化などを行うことで、監視品質の向上に努めています。

■ 脅威や攻撃の監視

デジタルデバイスやサーバーなどから集まってくる通信ログデータを監視し、組織内外へ不審な通信やマルウェア感染が発生していないかなど、多方向からの脅威を想定して判断しています。加盟しているセキュリティ団体やセキュリティベンダーと情報共有体制を構築し、他社事例や脆弱性・攻撃情報のリポートから最新動向の把握に努めています。

また、最新の攻撃を検知するための方法として、セキュリティ情報イベント管理（SIEM: Security Information and Event Management）を活用し、さまざまなログの収集、相関分析手法を用いることで、巧妙化・複雑化した攻撃の早期検知を目指しています。

■ 通信ネットワークのセキュリティ監視

通信ネットワークは社会基盤としての期待が大きく、その信頼性・品質は従来と比べ物にならないほど高いものが求められています。通信事業者である当社は、安定した通信ネットワークを提供するために、さまざまな監視を行っています。セキュリティ監視もその一つです。

5Gネットワークでは、単に高速というだけでなく、超低遅延・多数同時接続という特徴を有することから、これまで実現しなかった遠隔操作・自動運転などさまざまな分野への活用が期待されています。そのため、DDoS攻撃※などにより発生する通信量の変化、攻撃者からの5G設備へのアクセスなどに対応するため、さらなる高いレベルのセキュリティ監視体制の構築に努めています。

※ DDoS攻撃：複数の機器から特定の機器に対して、過剰なアクセスやデータを送付する攻撃を一斉に行うサイバー攻撃

5Gネットワークを活用した事例

超低遅延：タイムラグ（遅延）により従来では難しかったロボットの遠隔制御、自動運転、遠隔医療等の実現が期待されています。

多数同時接続：あらゆるモノ、多数のセンサーがネットワークに接続され、産業や社会に変革をもたらすIoTの強力な加速が期待されています。

質の高い社会ネットワークの構築

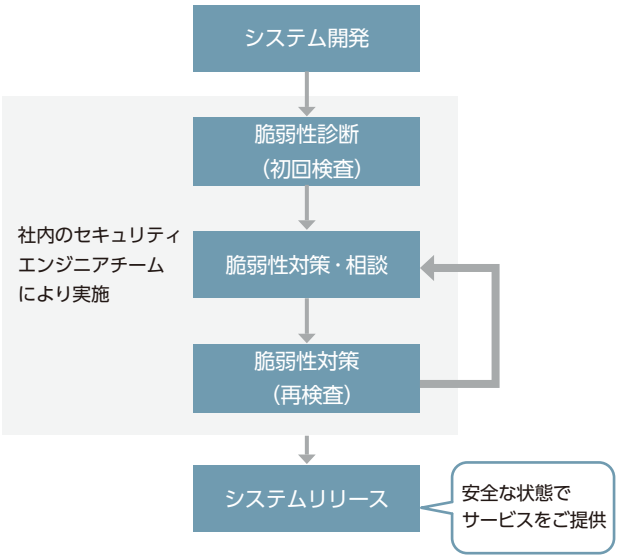
創出価値 ❸ データセキュリティとプライバシー保護の取り組みの推進

お客さまの情報を守るために

■ セキュリティ診断

システムの設定不備や脆弱性を残したままサービスの提供を開始した場合、当社のネットワークやシステムが攻撃を受け、お客さまへ被害が及ぶ危険性があります。当社では、社内のセキュリティエンジニアチームが徹底した脆弱性診断を実施し、検出された脆弱性に対し改善を指示することで、安全なサービス提供に努めています。

リリース後も新しい脆弱性が生まれるため、脆弱性診断と対策フォローを継続的に行うことにより、セキュリティリスクをゼロに近づける活動を行っています。



■ 社内環境の強化

近年、セキュリティ対策の標準になりつつあるMDM (Mobile Device Management) やEDR (Endpoint Detection and Response) など先進的な技術を積極的に採用することで、巧妙化する攻撃に対応しています。また、標的型攻撃メール対策訓練などを独自に実施し、社内のセキュリティ強化に役立てています。

情報セキュリティ事故の状況

2022年度、情報セキュリティ重大事故発生件数は0件でした。今後も研修や情報セキュリティ事故防止に取り組み、情報セキュリティ重大事故発生防止に努めます。

サイバー犯罪被害防止に向けた啓発活動

BBソフトサービス株式会社は、サイバー犯罪被害防止や啓発活動の一環として、インターネット詐欺リポートを毎月発行しています。このリポートは、ネット詐欺専用セキュリティソフト「詐欺ウォール®」で検知・収集した詐欺サイトを集計・分析したもので、さまざまな手口の詐欺サイトについて、発生状況やサイトの特徴、最新の手口、被害防止のポイントなどを取り上げています。

2023年3月の詐欺ウォールによる詐欺サイト検知数は5,778,392件で、2023年2月と比較すると、673,820件増加する結果となりました。

インターネット詐欺リポートを毎月発行することで、巧妙化するサイバー犯罪の被害防止に貢献します。

プライバシー保護の取り組み

プライバシーセンターの開設

当社は、お客さまの「パーソナルデータ」をさまざまなシーンで適切に利用し、皆さまにより便利で快適に暮らしていただくことを目指しています。プライバシーセンターでは、お客さまの情報をどのように取得・利用・保護しているかなど、私たちの取り組みをお客さまにとってより分かりやすい説明で案内しています。また、お客さまご自身が情報の利用状況を確認・管理できるダッシュボードを提供しています。

質の高い社会ネットワークの構築

創出価値 ❸ データセキュリティとプライバシー保護の取り組みの推進

プライバシー保護の取り組み

パーソナルデータ保護のための行動指針

当社は、お客さまからお預かりしたパーソナルデータを、お客さまの生活の質の向上や社会課題の解決のために活用しています。なお、パーソナルデータの取り扱いには細心の注意を払い、適切に保護しています。

①お客さまの意思を最大限に尊重します。

パーソナルデータは、お客さまの大切な情報です。何にどう利用するかをお客さまご自身で設定・管理いただくことでお客さまの意思を尊重し、望まれない形での利用はしません。

②お客さま視点に立ち分かりやすく説明します。

パーソナルデータに対する私たちの考えや利用方法について、分かりやすい言葉やイラストを用いて、お客さまに伝わる説明を心がけます。

③お客さまの大切なデータを厳重に管理します。

多様化するサイバー攻撃などの脅威から24時間365日お客さまのパーソナルデータを保護するため、セキュリティ対策を徹底します。

④パーソナルデータを適切な体制で取り扱います。

法令・世論・お客さまの心情など多様な視点でパーソナルデータを取り扱うために、全社横断の専門組織を構築しています。また、社員への啓発・教育やパートナー企業との連携にも積極的に取り組みます。

⑤パーソナルデータを利用し社会課題の解決に取り組みます。

お客さまのパーソナルデータを利用することで、さまざまな社会課題の解決にも取り組み、誰もが快適に暮らせる豊かな社会の創造を目指します。

パーソナルデータの保護に関する方針

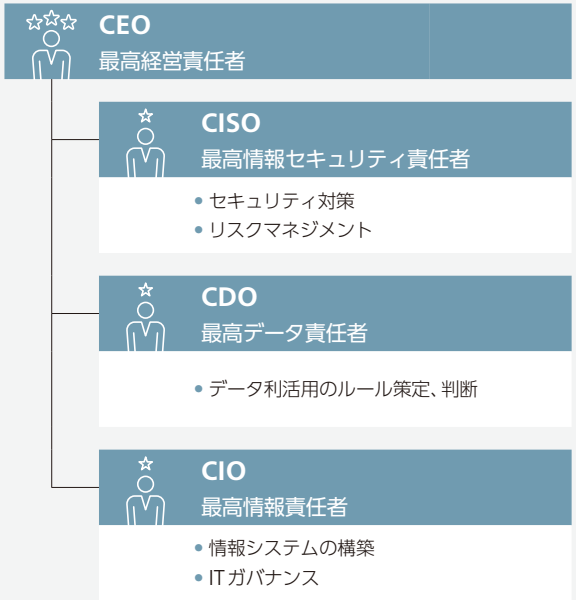
当社は、お客さまをはじめ、さまざまなステークホルダーのパーソナルデータを取り扱っています。お客さま等のパーソナルデータの取り扱いに細心の注意を払うとともに、お客さま等の権利に十分配慮するよう努めています。以下の法令、国が定める指針その他の規範の遵守徹底を図る他、認定個人情報保護団体（日本データ通信協会）に対象事業者として加入し、プライバシーの保護に率先して取り組んでいます。

・個人情報の保護に関する法律（通称：個人情報保護法）
・電気通信事業法（通信の秘密に係る規定）
・電気通信事業における個人情報保護に関するガイドライン
・個人情報保護マネジメントシステム―要求事項
（JIS Q 15001）

パーソナルデータを守る体制

■ 組織

当社は、お客さま等のパーソナルデータを保護するために全社的な体制を構築しています。データ管理、情報セキュリティ、情報システムの三つの観点で、各々責任者を配置し、パーソナルデータを統合的に管理しています。



質の高い社会ネットワークの構築

創出価値 ❸ データセキュリティとプライバシー保護の取り組みの推進

プライバシー保護の取り組み

■ ルール

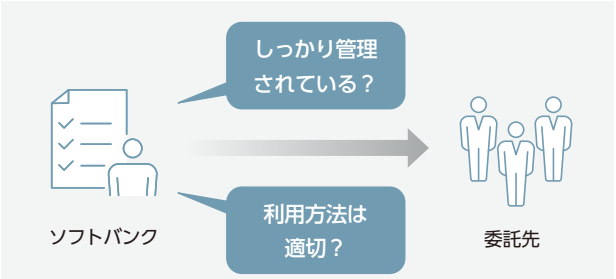
当社は、パーソナルデータの取り扱いに関する内部規程を整備し、明確な方針を示しています。パーソナルデータの漏えい、滅失または毀損（以下「漏えい等」）に対しては、厳しい態度で臨むことを社内に周知徹底するとともに、漏えい等が発生した場合は、就業規則に基づき懲戒処分を含む適切な対応をします。

また、パーソナルデータを適切に取り扱うため、パーソナルデータを取り扱う当社の全社員および派遣社員を対象に、年1回の研修を実施しています。

■ 委託

当社は、各種サービス等の問い合わせ対応業務、設備メンテナンス業務、料金関連業務その他の業務において、パーソナルデータの取り扱いの全部または一部を委託する場合があります。業務委託契約を締結する際は、業務委託の相手としての適格性を十分に審査します。業務委託契約には、安全管理措置、秘密保持、再委託の条件、その他のパーソナルデータの適正な取り扱いに関する事項について定めます。委託期間中においては、定期的な業務状況のモニタリング等を実施することにより、当社の業務委託先を適切に監督しています。

業務の受託に伴って委託元から提供（預託）されたパーソナルデータについては、これを委託元と当社との間で締結する契約の目的の達成に必要な範囲内で利用します。



セキュリティ対策

当社は、パーソナルデータの漏えい等を防止するため、アクセス管理、持ち出し制限、外部からの不正アクセス防止のための措置等、必要かつ適切な安全管理措置を講じています。

セキュリティ対策を実効性のあるものとするため、個人情報保護マネジメントシステムを遵守徹底し、定期的にリスクアセスメントを実施しています。リスクが発見された場合は適切に対応し、モニタリングによりリスクの最小化を図っています。また、パーソナルデータ保護の適切性については、社内で監査できる体制を整備しています。

サイバー攻撃からの防御
通信サービス設備へのDoS攻撃や業務用パソコンのマルウェア感染、不正サイトへのアクセス検知等、多様な対策を行っています。

専門家による常時監視
SOC（Security Operation Center）にて24時間365日、セキュリティを監視する専門の体制を整えています。

不正持ち出しの防止
社員などへの情報アクセス権限の付与は必要最低限とし、業務用パソコンの監視・ログ取得も行っています。

データ保管期間の設定
パーソナルデータは、利用目的の達成に必要な期間（法令で定められた期間を含む）をもとに保管期限を定めています。

質の高い社会ネットワークの構築

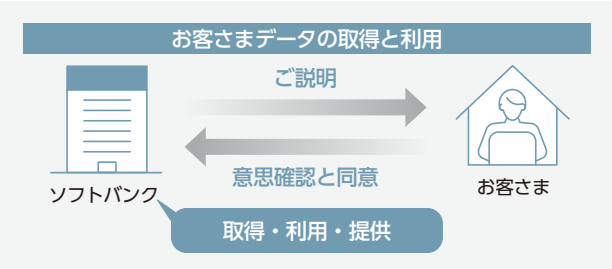
創出価値 ❸ データセキュリティとプライバシー保護の取り組みの推進

プライバシー保護の取り組み

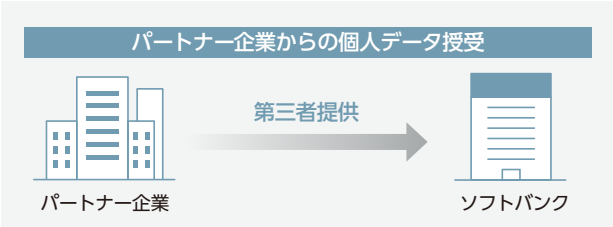
プライバシーの保護とお客さま等への配慮

■ パーソナルデータの適切な取得、利用、提供および公表

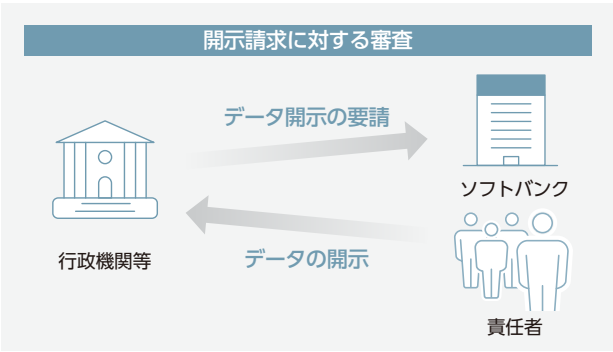
当社は、プライバシーに配慮し、パーソナルデータの取得、利用および提供を制限しています。パーソナルデータの取得に当たっては、利用目的を明確にし、申込書等の書面、ウェブサイト等の画面、口頭等の方法で、適法かつ公正な手段を用います。また、パーソナルデータの利用および提供ならびに公表等に当たっては、事業の内容および規模を考慮した上で、適切に実施しています。特にセンシティブ情報を取り扱う場合は、法令に定めるものを除く他、本人の同意に基づき、業務遂行上必要な範囲に限ります。



また、パーソナルデータは、利用目的の達成に必要な期間保持しています（法令で定められた期間を含む）。当社が第三者から個人データの提供を受ける場合は、法令遵守の上、提供元の個人情報保護の理念を尊重し、別途提供元と当社との間で締結する契約に定める条件に従い、取り扱います。



行政機関から個人情報に関する要求があった際、CDOがその正当性を確認します。個人データを第三者提供する場合は、法令に基づき、ご本人の同意を取得します。



個人データに関連した人権侵害が発生した場合は、速やかに調査を行い、必要な是正措置を講じます。個人データを第三者提供した結果、個人データに関連した人権侵害が発生した場合は、ご本人に対し救済措置を行うための窓口を設置するなど、必要な対応を実施します。

■ 通信情報の取り扱い

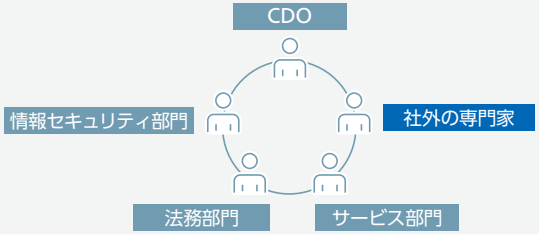
当社は、パーソナルデータの中でも通信の秘密に係る情報については厳格に管理しています。電気通信サービスの提供に必要な場合、お客さま等の同意がある場合、法令に基づく場合、その他の違法性阻却事由がある場合を除いて、通信履歴、通話履歴、発信者情報等の通信の秘密に係る情報を取得、保存、利用および提供することはありません。

通信の秘密に係る情報の取り扱い後は、その情報を速やかに消去しています。

電気通信の加入者情報を業務委託における委託先を含む第三者に提供するに当たっては、通信の秘密の保護に係る電気通信事業法第４条その他の関連規定を遵守します。

■ プライバシー影響評価

当社は、パーソナルデータの利活用に当たっては、社外の専門家を交えた専門チームが法令のみならず、お客さま等のメリットや社会への貢献と、お客さま等への不利益や心情を多面的に評価し、お客さま等に安全・安心を与える内容となるよう確認しています。



質の高い社会ネットワークの構築

創出価値 ❸ データセキュリティとプライバシー保護の取り組みの推進

プライバシー保護の取り組み

報告と今後の取り組み

2022年度、当局等の指導を受けた個人情報の漏えいや目的外利用、苦情等の法令違反などプライバシーに関連する重大事故件数は0件でした。

お客さま等のパーソナルデータを保護するため、今後も継続的な見直し・改善を図ります。

また、当社は「パーソナルデータの保護に関する方針」の内容の全部または一部を改訂することがあります。重要な変更がある場合には、当社ウェブサイト等において、分かりやすい方法でお知らせします。

■「パーソナルデータの保護に関する方針」の対象

「パーソナルデータの保護に関する方針」は当社のお客さまの他、取引先企業の社員や当社の社員等、当社が取得するパーソナルデータの全ての主体を対象とします。

「パーソナルデータの保護に関する方針」は、各項に特別な断りがない限り当社が取得する全てのパーソナルデータに適用されます。

外国にある第三者への提供

当社は、お客さまから同意を得た場合または法令で認められる場合に、お客さまのパーソナルデータを外国にある第三者へ提供（当社業務を委託する場合を含みます）することがあります。第三国に移転する場合は、移転国の個人情報保護制度等を考慮し、国内と同等の基準に適合した場合のみ、パーソナルデータを提供します。

具体的には以下の2カテゴリに分け、安全管理措置を講じています。

1. 国内と同等の個人情報保護制度が整備されている国または地域（欧州連合加盟国など）

提供先事業者については、適格性を十分に審査した上で安全管理措置、秘密保持、再委託の条件、その他の個人データの適正な取り扱いに関する事項を契約において定めています。また定期的に取り扱い状況のモニタリング等を実施することによって、パーソナルデータの取り扱いを適切に監督します。

2. 国内と同等の個人情報保護制度が整備されていない国または地域

上記の地域における取り扱いに加え、当該国でのデータ保管を行わず、閲覧においてもデータが残らない仕組み・セキュリティルームでの運用・入退室の厳格化など、十分なデータの保護が確保される措置を講じます。

なお、パーソナルデータの取り扱いに影響を及ぼすおそれのある制度について、毎年、日本の行政機関などが公表している情報を元に確認しています。

「ソフトバンクAI倫理ポリシー」を策定

当社は、「Beyond Carrier」戦略の下、従来の通信事業者の枠を超え、AIやIoTなどの先端技術を活用し、革新的なサービスの提供やDXの推進に取り組んでいます。

これらの先端技術のうち、AIは近年あらゆる産業での活用が広がり、今後も活用方法の多様化や技術の高度化が進むことが予想されています。

一方で、活用の仕方によっては差別的な評価や選別を導く可能性があるなど、倫理面での配慮や注意が必要な技術であることが指摘されています。

このような背景の下、当社は、AIを適切に活用してお客さまに安全・安心なサービスを提供するため、「ソフトバンクAI倫理ポリシー」を策定しました。

具体的には「人間中心の原則」「公平性の尊重」「透明性と説明責任の追求」「安全性の確保」「プライバシー保護とセキュリティの確保」「AI人材・リテラシーの育成」の六つの項目において指針を定め、この指針にのっとった事業運営やサービス開発などを行っていきます。

また、このポリシーをグループ会社でも適用できる体制を整えており、2023年6月1日時点で56社が適用を決定し、より具体的なルールを定めた社内規程やガイドラインも制定しました。今後もAIガバナンスに精通した有識者から成る外部委員会の設置などグループ内で連携し、継続して体制を強化していきます。

➔ 詳しくはこちら