LINE WORKS

VER. 1.0

Security White Paper

セキュリティ
ホワイトペーパー

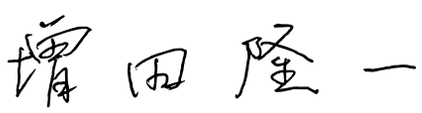
はじめに

「LINE WORKS(ラインワークス)」は、ビジネス版 LINE として、業務におけるコミュニケーションの課題を解決するツールです。LINE のような使い勝手で導入したその日から誰でもすぐに使え、チャットだけではなくカレンダーやタスクなど仕事に役立つ機能が盛り込まれています。

そして業務でご利用になるツールだからこそ、お客様に LINE WORKS のセキュリティや個人情報保護の方針や対策についてご理解の上、より安心・安全にご利用いただきたいと考えています。
クラウドサービスの安全性は提供ベンダーとお客様で作り上げていくものです。インフラ回りを中心とした弊社の取り組みに加え、アプリの設定やデータの管理などに対するお客様の適切な運用によって、より強固なセキュリティとなっていきます。

本ホワイトペーパーは、LINE WORKS をこれから導入されたい方だけではなく、すでにお使いの方に対してもお役に立てる情報を紹介しています。導入前から導入後までの各フェーズにおいての LINE WORKS のセキュリティおよび個人情報保護に関して網羅的に記載していますので、ぜひ本資料をご活用ください。

LINE WORKS 株式会社 代表取締役社長



目次

LINE WORKS セキュリティホワイトペーパーの構成と用語

LINE WORKS セキュリティホワイトペーパーの構成

本ホワイトペーパーでは、LINE WORKS サービスにおける情報セキュリティと個人情報保護に関する取り組みに関する解説と、LINE WORKS サービスを利用者がセキュアに利用するために必要な設計、設定、管理に関する情報の提供を行います。

LINE WORKS セキュリティホワイトペーパーを読む前に
1 章 : LINE WORKS とは 2 章 : 情報セキュリティと個人情報保護の基礎知識
LINE WORKS のセキュリティ
3 章 : LINE WORKS の情報セキュリティと個人情報保護を実現する取り組み 4 章 : LINE WORKS サービスにおける「責任共有モデル」
LINE WORKS 利用者のためのセキュリティ情報
5 章 : LINE WORKS サービスをセキュアに利用するための設計と設定 6 章 : LINE WORKS サービスをセキュアに運用するための管理機能
附録 : LINE WORKS に関するリンク集など

LINE WORKS セキュリティホワイトペーパーの全体像

1 章 : LINE WORKS とは？

LINE WORKS サービスとは何か？ LINE とはどう違うのか について解説します。

2 章 : 情報セキュリティと個人情報保護の基礎知識

情報セキュリティと個人情報保護に関して一般論をもとに基礎知識について解説します。

LINE WORKS のセキュリティ

3 章と 4 章では、LINE WORKS サービスの情報セキュリティや個人情報保護への取り組みに興味がある方に対して、LINE WORKS 株式会社としての取り組みと、LINE WORKS サービスにおける「責任共有モデル」について解説します。

3 章 : LINE WORKS の情報セキュリティと個人情報保護を実現する取り組み

LINE WORKS 株式会社における情報セキュリティおよび個人情報の保護のための取り組みについて解説します。

4 章 : LINE WORKS サービスにおける「責任共有モデル」

SaaS サービスに対するセキュリティ上の脅威の概要と、その脅威に適切に対応するために必要な「責任共有モデル」について、LINE WORKS を例に解説します。

LINE WORKS 利用者のためのセキュリティ情報

5 章と 6 章では、LINE WORKS サービスの導入企業や組織の担当者 (導入担当者、管理者) に対して、LINE WORKS サービスをセキュアに利用するために必要な情報を提供します。

5 章 : LINE WORKS サービスをセキュアに利用するための設計と設定

LINE WORKS サービスをセキュアに利用するために必要な設計および設定について解説します。導入担当者は、これらの設計や設定を行った後、管理者に対して LINE WORKS サービスを引き継ぎます。(導入担当者が管理者を兼ねる場合もあります。)

6 章 : LINE WORKS サービスをセキュアに運用するための管理機能

LINE WORKS サービスをセキュアに運用するために必要な管理機能について解説します。管理者は、導入担当者から引き継いだ LINE WORKS サービスについて、これらの管理機能を活用して日々の運用管理を行います。

LINE WORKS セキュリティホワイトペーパーにおける用語

ここでは、本ホワイトペーパーにおける基本的な用語を紹介します。

LINE WORKS

ビジネス用コミュニケーションツールの LINE WORKS サービスのことを指します。

LINE WORKS 株式会社

LINE WORKS サービスを提供する LINE WORKS 株式会社を指します。

テナント

LINE WORKS サービスの契約毎に割り当てられるサービス上の論理的な空間です。LINE WORKS を全社で 1 つ契約している場合は全社で一つのテナントを利用します。部署毎に契約している場合は、部署毎に別々のテナントを利用します。LINE WORKS サービスでは、共有リンクや社外を含むグループなどの機能を利用する場合を除いて、他のテナントのデータにアクセスすることはできません。

メンバー

LINE WORKS サービスの利用者です。メンバーは、モバイル版アプリ、PC 版アプリ、Web ブラウザなどを利用して LINE WORKS サービスにアクセスします。

管理者

LINE WORKS サービス上のメンバーや機能を管理する権限を持つ特殊なメンバーです。管理者は、管理者画面を利用して、LINE WORKS サービスの設定や管理を行います。LINE WORKS サービスのテナントを開設したメンバーは自動的に「最高管理者」となり、他のメンバーを「副管理者」や「運用担当者」などに指定することで管理業務の一部を委任することができます。

1章 LINE WORKS とは

1.1. LINE WORKS の概要や特徴

「LINE WORKS(ラインワークス)」は、トーク・カレンダー・掲示板・ビデオ会議など、仕事に便利なグループウェア機能が 1 つのアプリにそなわった「ビジネス版 LINE」とも言えるビジネスコミュニケーションツールです。

LINE WORKS には、以下の特徴があります。

なじみのある使いやすいチャット

LINE WORKS の「トーク」機能では、「LINE」の使いやすさをそのままに、豊富な仕事用スタンプで気持ちを伝えあうことができます。誰でもすぐ使えるチャットによって、社内のコミュニケーションが活性化していきます。

どこでも社内コミュニケーション

LINE WORKS は、スマートデバイスでの利用を中心に設計されており、デスクワークが少ない「現場」ではたらく社員や、出張先や外出先でのコミュニケーションがスムーズになるほか、情報共有の円滑化や、PC 利用がメインのバックオフィスの業務効率化など、ビジネスを一層加速させていきます。

LINE とつながる唯一のチャットサービス

LINE WORKS は、LINE ユーザーとトークがつながる唯一のビジネスチャットです。お客様やお取引先とのコミュニケーションも LINE WORKS ひとつで完結します。

音声・ビデオ通話の幅が広がる

LINE WORKS では、アカウントを持っていない人でも音声・ビデオ通話ミーティングにゲスト参加することができます。

仕事で活用できる充実したグループウェア機能

LINE WORKS は、ビジネスですぐ使える以下のグループウェア機能を提供しています。

掲示板

社内への情報の周知や、社内メンバーと情報を共有するための掲示板です。用途に合わせた掲示板を作成し、社内コミュニケーションを活性化に役立てることができます。

カレンダー

自分の予定を管理するだけでなく、他のメンバーと予定を共有して管理できるカレンダーです。他のメンバーの予定も一目で把握できるため、会議などの予定を簡単に調整できます。

タスク

自分のタスクはもちろん、トークルームの他のメンバーと業務リストを共有したり管理するための機能です。期限と担当者を指定できるので、重要な業務を忘れずに、効率的に管理することができます。

アンケート

メンバーの意見を集計するための機能です。社内イベントの出欠確認や満足度調査など、様々なアンケートを簡単に作成することができます。

アドレス帳

組織図と連絡先を一目で確認できる業務用アドレス帳です。社内メンバー、顧客 / 取引先など、業務に必要な連絡先を一箇所で管理することができます。

メール

便利な機能と迷惑メールブロックをはじめとする強固なセキュリティで安心して使えるメールサービスです。会社のメールアドレスを使用することで、信頼度を高めることができます。

Drive (共有フォルダ)

社内の業務文書を保管し、共有するためのクラウドストレージです。PC だけでなくスマホでもファイルを確認して、仕事を続けることができます。

セキュリティを重視した管理機能

LINE WORKS は、企業様のセキュリティポリシーに合わせてきめ細やかな設定が可能です。退職者が発生した場合に、シンプルかつ確実な退職処理を行い、万が一の端末紛失でも遠隔でデバイスのデータ削除やデバイス初期化を行うことができます。

LINE WORKS は、日本の法令はもちろん国際規格を遵守し、国際認証を取得した高いレベルのセキュリティシステムでサービスを管理・提供しています。

1.2. LINE と LINE WORKS の違い

1.2.1.「LINE」と「LINE WORKS」: 運営会社の違い

「LINE」と「LINE WORKS」では、運営会社が異なります。

「LINE」の運営会社

「LINE」は、LINE ヤフー株式会社が運営しています。LINE ヤフー株式会社は、東証プライムの上場企業です。

「LINE WORKS」の運営会社

「LINE WORKS」は、2016 年 1 月にワークスモバイルジャパン株式会社により提供を開始しました。2024 年 1

月にワークスモバイルジャパン株式会社は、社名を LINE WORKS 株式会社に変更しました。LINE WORKS 株式会社は、NAVER Cloud Corporation(韓国：以下、NCC) を親会社に持つ日本法人です。

1.2.2.「LINE」と「LINE WORKS」: サービスの違い

「LINE」と「LINE WORKS」では、それぞれのサービスを活用する場面が異なります。

「LINE」のサービスの特徴

「LINE」は、友だちや家族と、トーク (チャット) · 音声通話 · ビデオ通話などを楽しむことができる無料のコミュニケーションアプリです。

「LINE WORKS」のサービスの特徴

「LINE WORKS」は、トーク · カレンダー · 掲示板 · ビデオ会議など、仕事に便利なグループウェア機能を備えた、ビジネス版 LINE とも言えるコミュニケーションアプリです。社内のコミュニケーションを活性化するための機能だけではなく、「LINE WORKS」上で扱う情報や個人情報を保護するための機能も充実しています。
このように、「LINE WORKS」は、主にビジネスを加速しつつ、大事なビジネスデータの保護も実現するツールであると言えます。

1.2.3. LINE WORKS の開発・運用体制について

LINE WORKSにおける開発および保守をLINE WORKS株式会社による管理、統制の下、NCCに委託しています。なお、LINE WORKS の一部の機能（Drive エクスプローラーおよび PC 版 LINE WORKS のアプリ）については、NCC を通じて NAVER VIETNAM にてその開発を行っています。
ただし、保存データはすべて日本のデータセンターに保管され、日本の法令に従って管理および処理されます。また、開発委託を行ったすべてのプログラムは、リリース前に当社によるソースコードレベルのセキュリティチェックを実施し、当社の承認後、NCC によってサービス運用環境に配布されています。
また、LINE WORKSにおけるインフラの運用業務をNCCにて行っています。LINE WORKSの提供とバックアップデータの保管は、当社の管理、統制の下で日本国内のデータセンターにて行われ、すべての通信経路は暗号化により安全に管理されています。詳細はプライバシーセンターの**「ユーザーデータ取扱い」**をご参照ください。

1.3. LINE WORKS 株式会社のミッション・ビジョン・バリューと沿革

1.3.1. LINE WORKS 株式会社のミッション・ビジョン・バリュー

1.3.1.1. LINE WORKS 株式会社のミッション

「仕事、楽しい」を広げる 47 都道府県ではたらくすべての人に

私たちはお客様に、仕事／はたらくというシーンのコミュニケーションにおいて、特に店舗や現場や地方のような、IT が活用しにくい企業・職場・地域の人にとって、仕事でも使える（仕事用なのに使いやすい）+ 誰でも使える

（IT スキルを問わない）サービスを提供し続けます。

1.3.1.2. LINE WORKS 株式会社のビジョン

はたらく仲間がつながる世界、その開拓者になる

お客様の社内はもちろん、お客様の顧客・取引先・協働者がつながり、距離が縮まり、仲間として、ひとつのチームとして成長する、そんな世界を多くの人に体験してほしい、と私たちは考えています。そのために、私たちは、お客様、パートナー、開発者、地域コミュニティともチームとなって、お互いが成長・発展していけるよう、すべてのはたらく人がつながる世界を創る開拓者となります。

1.3.1.3. LINE WORKS 株式会社のバリュー

リアカチ

お客様に本当の価値を提供しよう

多面的・長期的・根本的に考える。持続的成長＞短期的成果。

ハタカチ

自ら旗を立て、チームで勝ちにいこう

リーダーシップとフォロワーシップ。応援する。リスペクト。

チャレカチ

チャレンジこそ価値、勝ちにつなげよう

成功のためには早くチャレンジしよう。失敗から学ぶことが成功につながる。

1.3.2. LINE WORKS 株式会社の沿革

LINE WORKS 株式会社は、「楽しいビジネスコミュケーションをはたらくすべての人に」という創業の志を今も大事にして「LINE WORKS」を提供し続けています。

2015.06

ワークスモバイルジャパン株式会社 設立

2016.01

アプリケーション「Works Mobile」提供開始

2017.02

アプリケーション名を「LINE WORKS」に変更

2018.11
LINE WORKS フリープラン 提供開始

2021.10
西日本営業所 開設

2022.07
福岡営業所 開設

2023.04
LINE 社 AI 事業「LINE CLOVA」を統合

2024.01
社名を「LINE WORKS 株式会社」に変更

LINE WORKS 株式会社は、ユーザーに最良の IT サービスを提供するために日々、改善を続けています。私たちは単にサービスを作るだけにとどまらず、働き方の改革を通じて、顧客の業務革新をリードするパートナーになろうと考えています。

LINE WORKS 株式会社の詳細については、LINE WORKS 公式サイトの**「会社紹介」**をご参照ください。

2 章 情報セキュリティと個人情報保護の基礎知識

2.1. 本章の概要

本章では、SaaS サービスに興味がある全ての方を想定読者として、情報セキュリティと個人情報保護の基礎知識について解説します。

2.2. 情報セキュリティ

2.2.1. 情報セキュリティとは

情報セキュリティとは、保有する情報資産を脅威から保護することを言います。ここで「情報資産」とは、保有するあらゆる情報のことを言います。そして、情報資産には、情報そのものだけでなく、その情報を保管する記録媒体 (紙、デバイスなど)、情報を加工・処理する装置などを含みます。企業や組織における情報資産は競争力の源泉であり、その企業や組織の存続に不可欠な要素であると言えます。
情報セキュリティにおいては、情報資産を以下の 3 つの脅威から保護する必要があります。

情報の機密性 (Confidentiality) に対する脅威

認可された人やプログラムだけが情報にアクセスできることを「機密性」と言います。情報の機密性への脅威の例として、機密情報 (パスワードや知的財産) の盗難、スパイウェアの侵入、その結果としての情報の漏えいや不正利用などがあります。

情報の完全性 (Integrity) に対する脅威

保有する情報が正確であり、不正に改ざんされたりせずに完全である状態を保持することを「完全性」と言います。情報の完全性への脅威の例として、不正アクセスや悪意のあるソフトウェアによる情報の改ざんや破壊などがあります。

情報の可用性 (Availability) に対する脅威

必要なときに情報にアクセスできることを「可用性」と言います。情報の可用性への脅威の例として、情報機器が設置されているデータセンターの物理的な破壊、サイバー攻撃によるサービスの停止、ランサムウェアの不正な暗号化による情報へのアクセス不能などがあります。

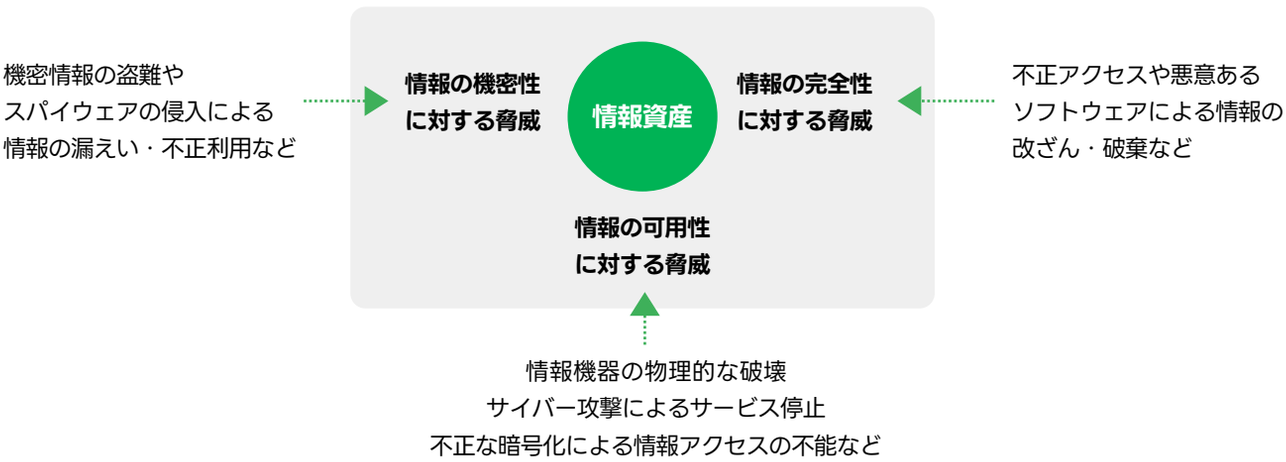


図 . 情報資産の 3 つの脅威 (機密性、完全性、可用性)

これらの脅威への対策を適切に行うためには、保有する情報資産の特性に合わせて、セキュリティ体制の構築と保護策の実施をする必要があります。

2.2.2. 情報セキュリティマネジメント

企業や組織が、その保有する情報資産を適切に管理し、保護するためには、その企業や組織全体で情報セキュリティのための体系的な取り組みを行う必要があります。

企業や組織の情報セキュリティマネジメントにおいては、主に以下の活動を行います。

- 情報セキュリティ関連法令の遵守
- 情報セキュリティ方針の策定・実施
- 情報セキュリティ教育の実施

2.2.2.1. 情報セキュリティ関連法令の遵守

日本国内においてインターネットサービスを提供している事業者は、電気通信事業法の定めるところにより、サービスを円滑に提供し、その利用者の利益を守り、公共の福祉を増進することが求められます。

2.2.2.2. 情報セキュリティポリシーの策定・実施

企業や組織が直面する情報セキュリティ上の脅威から情報資産を保護するために、その基本方針として「情報セキュリティポリシー」を定めます。情報セキュリティポリシーでは、その企業や組織が持つ情報資産の特性に合わせて、情報セキュリティに対する基本的な考え方、情報セキュリティを確保するための指針、体制、基準、ルールなどを策定します。

2.2.2.3. 情報セキュリティ教育の実施

企業や組織の情報資産を安全に管理し、保護するためには、その役員・従業員が、情報セキュリティに関する正しい知識とスキルを身に付け、組織全体でセキュリティ文化を醸成していく必要があります。更に、今日のビジネス環境において、日々出現する新たな攻撃手法や脆弱性に対応するためには、定期的なトレーニングや e ラーニングの活用により、古い知識とスキルを更新していくことも重要となります。

2.3. 個人情報の保護

2.3.1. プライバシーと個人情報

「プライバシー」とは、個人の私事や秘密およびこれらを自分でコントロールする権利のことを言います。プライバシーは、当初は「一人でいさせてもらう権利」(身体のプライバシー) として理論付けられましたが、情報化社会の進展とともに「自己の個人情報をコントロールする権利」(情報のプライバシー) として認知されてきています。インターネットによる高度な情報社会において、他者による不当な侵害から個人情報を保護することは、個人の尊厳と自由を守るために非常に重要であると言えます。

情報のプライバシーにおける「個人情報」とは、生存する個人に関する情報で、特定の個人を識別できるもののことを言います。例えば、姓名だけで個人を特定できればその「姓名」が、住所と姓だけで個人を特定できれば「住所と姓」の組合せが個人情報となります。また、顧客 ID や社員番号など、その見た目だけでは個人を特定できなくても、顧客台帳や従業員名簿を参照すればどの個人か識別できるものも、個人情報に該当します。

個人情報の対象である個人や、個人情報を保有する企業や組織は、個人情報を以下の 3 つの脅威から保護する必要があります。

個人情報を不正に収集される脅威

企業や組織への攻撃や不注意による顧客データの漏えい、個人への攻撃や不注意によるログイン情報の流出などにより、個人情報が悪意のある第三者に不正に収集されてしまう場合があります。

個人情報を不正に使用される脅威

不正に収集された個人情報が使用され、個人の財産や名誉などを毀損されてしまう場合があります。個人情報を不正に使用された個人は、経済的な損失や社会的信用の損失、もしくはその両方について損害を被る可能性があります。

個人情報を不正に公開される脅威

不正に収集された個人情報が公開され、個人の名誉などを毀損されてしまう場合があります。個人情報を不正に公開された個人は、その社会的信用について大きな損害を被る可能性があります。

個人情報を保護するためには、不正に個人情報を収集されないことが何よりも重要となります。自らの個人情報を保護したい個人は、強固なパスワードの使用、多要素認証の利用、不審なメールやリンクを開封しない、公共 Wi-Fi を使用するときには HTTPS もしくは VPN を利用する、などの行動が求められ、顧客の個人情報を保有する企業や組織は、保有する個人情報の特性に合わせて個人情報保護体制の構築と保護策の実施をすることが求められます。

個人情報の保護は、個人情報保護法などの法令によって企業や組織に義務付けられているだけでなく、その顧客や社員からの信頼を得るために不可欠な要素であると言えます。

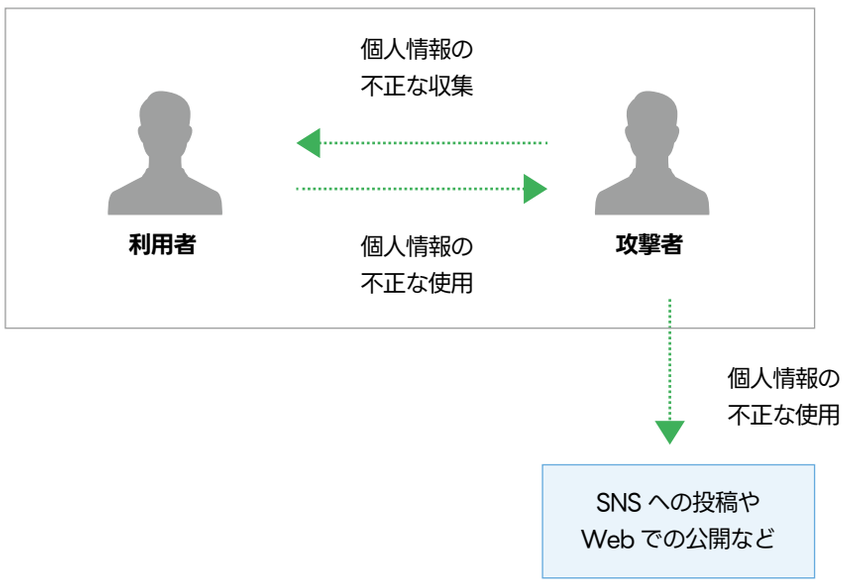


図 . 個人情報への 3 つの脅威 (収集、使用、公開)

2.3.2. 個人情報マネジメント

企業や組織が、個人情報を適切に管理し、保護するためには、その企業や組織全体で個人情報マネジメントのための体系的な取り組みを行う必要があります。

企業や組織の個人情報マネジメントにおいては、主に以下の活動を行います。

- 個人情報関連法令の遵守
- 個人情報保護方針の策定・実施
- 個人情報保護教育の実施

2.3.2.1. 個人情報関連法令の遵守

個人情報を取り扱う全ての企業や組織は、個人情報保護法や関連する法令の定めるところにより、個人の権利や利益を守ることが求められます。

2.3.2.2. 個人情報保護方針の策定・実施

企業や組織が直面する個人情報上の脅威から個人情報を保護するために、その基本方針として「個人情報保護方針」を定めます。個人情報保護方針では、その企業や組織が持つ個人情報の特性に合わせて、個人情報保護に対する基本的な考え方、個人情報を保護するための指針、体制、基準、ルールなどを策定します。

2.3.2.3. 個人情報保護教育の実施

企業や組織の個人情報を安全に管理し、保護するためには、その役員・従業員が、個人情報保護に関する正しい知識とスキルを身に付け、組織全体で個人情報保護文化を醸成していく必要があります。

3 章 LINE WORKS の情報セキュリティと個人情報保護を実現する取り組み

3.1. 本章の概要

本章では、情報システム担当者や情報セキュリティ監査担当者など SaaS サービスの情報セキュリティや個人情報保護への取り組みに興味がある方を想定読者として、LINE WORKS 株式会社における情報セキュリティおよび個人情報の保護のための取り組みについて解説します。

3.2. LINE WORKS 株式会社における情報セキュリティマネジメント

3.2.1. 情報セキュリティ関連法令の遵守

LINE WORKS 株式会社は、サービスの提供に関わる全ての活動において電気通信事業法を遵守し、以下の定めおよび取り組みを行っています。

1. 電気通信事業法に定められた通信の秘密保護のために、「LINE WORKS サービス利用規約」第 18 条に、以下の定めを明記し、厳密に遂行しています。
   当社は、電気通信事業法 (昭和 59 年法律第 86 号) 第 4 条に基づき、お客様及びユーザーの通信の秘密を守ります。
   当社は、お客様及びユーザーの同意がある場合、又は次の各号の場合を除き、保存データ等の通信の秘密に係る情報にアクセスできないものとします。

   1. 本サービスの安全な運営のため
   2. 本サービスの運営上の問題を事前に防止し又は事後に解決するため
   3. お客様の要請があり、当社がこれに対応するため。ただし、お客様が購入、利用又は設定しなかったことによるデータ消失等を補完するための要請に対応することを保証するものではありません。
   4. 刑事訴訟法 (昭和 23 年法律第 131 号) 又は犯罪捜査のための通信傍受に関する法律 (平成 11 年法律第 137 号) その他の法令の定めに基づく強制力のある処分又は裁判所の命令が行われた場合
   5. 他人の生命、身体、財産又は名誉、プライバシーの保護のために必要があると当社が判断した場合

   LINE WORKS サービスの利用規約の詳細については、「LINE WORKS サービス利用規約」をご参照ください。

2. 電気通信事業法に定められた外部送信規律に基づいて、利用者の情報収集および外部送信について公表しています。詳細については、「外部送信される情報の取り扱いについて」をご参照ください。

3.2.2. LINE WORKS 株式会社における情報セキュリティポリシーの策定・実施

LINE WORKS 株式会社の情報セキュリティポリシー

LINE WORKS 株式会社は、下記を情報セキュリティポリシーとして定めています。

- 会社は会社の情報資産に対する機密性、完全性、可用性を保障します。
- 会社は利用者の個人情報、プライバシー保護を最優先価値に置いてサービスを安定的に提供します。
- 会社は、情報セキュリティの活動を通して、会社のビジネスが新たな価値を創出できるよう支援します。
- 会社は創出された情報保護価値が会社内で限定されず、利用者、株主、ビジネスパートナーなど多様な利害関係者に共有されることができるよう、情報保護に対する社会的責任を尽くします。

LINE WORKS 株式会社の情報セキュリティの原則

LINE WORKS 株式会社では、以下の情報セキュリティの原則を策定し、遂行します。

- 業務遂行において、利用者の個人情報取り扱い、端末の管理、侵害事故発生時の迅速な対応など、セキュリティ要求事項を正しく理解し、実践します。
- 利用者の個人情報が安全に保護されことができるよう、関連法令や会社の基準を遵守して、処理する個人情報が紛失、盗難、漏えい、改ざん及び誤・濫用されないように注意深く管理します。
- 外部への業務委託においては、発注から契約終了まで各段階別のセキュリティ要求事項を正しく理解し、実践します。
- サービス運営において、公開サービス、社内システム及びサービス管理システムのサステイニングステップを含め、運営業務におけるセキュリティ要求事項を遵守します。
- インフラ運営において、サーバー、ネットワーク、DB などがセキュリティホールを利用した流出、誤・濫用、損傷、破壊など一連の不法行為、事故から安全に管理されなければなりません。
- 情報保護責任者は、会社およびサービスの情報資産に対する機密性、完全性、可用性を保障するために必要なポリシー、指針などを策定、検討、施行し、正しく施行されているか周期的に点検します。

LINE WORKS 株式会社の情報セキュリティ指針およびガイドライン

LINE WORKS 株式会社では、情報セキュリティポリシーを実現するために、社内において情報セキュリティ指針および指針を実現するための具体的な手順であるガイドラインを定めています。例として以下のような情報セキュリティガイドラインを策定し、運用しています。

情報セキュリティリスクマネジメントガイドライン

LINE WORKS 株式会社における情報セキュリティリスクの識別・分析・評価を行うために必要な用語の定義、原則などについて定めています。LINE WORKS 株式会社の全ての役職員は、このガイドラインに従って会社の対外的な活動および社内のプロセスを遂行しています。

サービス企画設計セキュリティガイドライン

LINE WORKS 株式会社が提供するサービスで取り扱う情報のセキュリティを確保するために、サービス企画および設計を行う際に必要な観点や基準を定めています。例えば、認証の迂回防止、適切なアクセス範囲、サービス管理システムへの要求などを明示しています。LINE WORKS 株式会社において、サービスの企画や設計に携わる全ての役職員は、このガイドラインに従ってサービスの企画や設計のプロセスを遂行しています。

サービス開発セキュリティガイドライン

LINE WORKS 株式会社が提供するサービスで取り扱う情報のセキュリティを確保するために、サービス開発において共通となる観点や基準を定めています。例えば、ソースコードのセキュリティレベルやアクセス制御、開発環境やプロダクトの管理などについて明示しています。また、ウェブアプリケーションやモバイルアプリケーションそれぞれの特色に対応したセキュリティ策を明示しています。LINE WORKS 株式会社において、サービスの開発に携わる全ての役職員は、このガイドラインに従ってサービスの開発プロセスを遂行しています。

3.2.3. LINE WORKS 株式会社における情報セキュリティ教育の実施

LINE WORKS 株式会社では、全ての役員・従業員に対して年 2 回以上定期的に情報セキュリティに関する教育を実施し、セキュリティへの意識と知識水準の維持を行なっています。

3.3. LINE WORKS 株式会社における個人情報マネジメント

3.3.1. 個人情報関連法令の遵守

LINE WORKS 株式会社は、サービスを利用者をはじめとした関係者全ての方々の個人情報の保護を最優先事項の一つとして位置づけ、サービスの提供に関わる全ての活動において個人情報保護法を遵守し、以下の定めおよび取り組みを行っています。

1. LINE WORKS 株式会社は、個人情報保護に対するすべての責任と義務を果たし、併せてサービスの利用者のプライバシー保護にも積極的に対応するため、LINE WORKS 株式会社における個人情報の取り扱いについて「LINE WORKS プライバシーポリシー」を定めて公開しています。個人情報を本人から直接取得する場合は、その個人情報の利用目的を明示いたします。
2. LINE WORKS 株式会社のサービス提供において個人情報を取り扱う場合は、取得する個人情報の範囲と利用目的を特定し、その目的の達成に必要な範囲に限定して個人情報を取り扱います。LINE WORKS 株式会社のサービス提供において取得する個人情報の範囲、その利用目的については、「LINE WORKS プライバシーポリシー」の「2. 取得するご関係者情報及び取得方法」「3. ご関係者の情報の利用目的」をご参照ください。
3. LINE WORKS 株式会社は、取得した個人情報を安全に管理するために、社内において個人情報保護指針およびガイドラインを定め、LINE WORKS 株式会社の従業員および業務委託先に対して適切な教育および監督をしています。
4. LINE WORKS 株式会社は、プライバシーポリシーに掲げる場合を除き、正当な権限がある方からの事前の同意を得ずに、個人情報を第三者に提供いたしません。詳細については、LINE WORKS プライバシーセンターの「個人情報の第三者提供」をご参照ください。
5. LINE WORKS 株式会社のサービス提供において取得した個人情報の開示請求等に対するお問い合わせについて、厳正なルールに従って対応いたします。詳細については、LINE WORKS プライバシーセンターの「保有個人情報の開示請求について」をご参照ください。
6. LINE WORKS 株式会社は、サービス利用者からの個人情報の取扱いに関するご連絡を、適切かつ迅速に処理いたします。LINE WORKS 株式会社のプライバシーポリシーに関するご意見、ご質問、苦情、LINE WORKS 株式会社による個人情報取り扱いに関するお問い合わせ、個人情報保護法等に関する対応、その他ご不明な点がある

場合は、LINE WORKS 株式会社のプライバシー窓口 (privacy_wm@line-works.com) までお問い合わせください。

なお、LINE WORKS サービスのご利用者 (メンバー) の個人情報 (氏名、電話番号、メールアドレスなど) については、ご利用企業の LINE WORKS サービス管理者に管理責任があります。
メンバーの登録情報が事実と異なる場合、管理者画面で情報修正、削除の操作を行うことができます。管理者権限を持たないメンバーの方は、管理者へのご相談をお願いいたします。

3.3.2. LINE WORKS 株式会社における個人情報保護方針の策定・実施

LINE WORKS 株式会社の個人情報保護方針

LINE WORKS 株式会社では、以下の個人情報保護の方針を策定し、実施しています。

プライバシーの原則

LINE WORKS 株式会社では、サービス利用者の個人情報とプライバシー保護のために、以下の 4 つの「プライバシーの原則」を公開し、実践しています。

1. 個人情報保護に関する法令と国際基準の遵守
2. ユーザーによる自己情報コントロール権の尊重
3. 個人情報の必要最小限の収集と管理責任
4. プライバシーの保護の最優先

詳細については、LINE WORKS プライバシーセンターの**「プライバシーの原則」**をご参照ください。

Privacy by Design

LINE WORKS 株式会社は、サービスの提供において「Privacy by Design」という考え方を採用し、積極的に推進しています。「Privacy by Design」とは、サービスや機能のライフサイクル全体にわたって個人情報の保護に取り組むことを言います。「Privacy by Design」の取り組みにより、サービスや機能の企画や設計の段階において個人情報の保護の検討が行われ、開発から運用においても利用者の観点からの個人情報保護が重要視されます。

LINE WORKS 株式会社は、サービスや機能の企画から運用保守までのライフサイクルにおいて、プライバシー影響評価 (PIA: Privacy Impact Assessment) を行い、個人情報に対して一貫した保護を行った上でサービスの提供をしています。

Privacy by Design の詳細については、LINE WORKS プライバシーセンターの**「Privacy by Design」**をご参照ください。

プライバシー影響評価 (PIA) の詳細については、「3 章 LINE WORKS の情報セキュリティと個人情報保護を実現する取り組み」の「LINE WORKS のプロセス : セキュアなサービスライフサイクル」をご参照ください。

LINE WORKS プライバシーポリシー

LINE WORKS 株式会社では、個人情報保護に対するすべての責任と義務を果たし、個人情報を提供される方々 (以下「ご関係者」といいます。) の個人情報保護に積極的に対応するため、「プライバシーの原則」に基づいて「LINE WORKS プライバシーポリシー」を制定し、実践しています。

「LINE WORKS プライバシーポリシー」では、主に以下について規定しています。

- ポリシーの適用範囲
- 取得する個人情報及び取得方法
- 個人情報の利用目的
- 個人情報の第三者提供、委託、共同利用など
- 個人情報に対する安全対策
- 個人情報提供者の権利

詳細については、LINE WORKS プライバシーセンターの**「LINE WORKS プライバシーポリシー」**をご参照ください。

LINE WORKS 株式会社の個人情報保護規程

LINE WORKS 株式会社では、「プライバシーの原則」、「Privacy by Design」、「LINE WORKS プライバシーポリシー」の 3 つの個人情報保護方針を実現するために、社内において個人情報保護規程を定めています。個人情報保護規程は、個人情報保護を実現するための指針および指針を実現するための具体的な手順であるガイドラインで構成されています。

LINE WORKS 株式会社社内で行われる業務は、個人情報保護規程を根拠にその業務ルールが整備されており、個人情報関連法令や情報セキュリティマネジメントシステム (ISMS) に準拠して遂行されています。LINE WORKS 株式会社は、個人情報の保護を最優先で業務に取り組んでおり、例として以下のような個人情報保護策を実施しています。

暗号化による個人情報の保護

LINE WORKS 株式会社の業務およびサービスにおいて、個人情報をコンピューティングリソースに保存もしくは情報通信ネットワーク上で伝送する場合は、暗号化により保護します。暗号化方式およびアルゴリズムについては、その用途に最も適したリスクの低いものを指定しています。

外部への業務委託における個人情報の保護

LINE WORKS 株式会社の業務を外部へ委託する場合に個人情報を取扱うときは、個人情報の保護について社内と同一水準の遵守事項を委託契約で定め、委託前および委託契約期間中において継続的に個人情報への影響評価および点検を実施します。

外部サービス利用における個人情報の保護

LINE WORKS 株式会社の業務やサービスにおいて外部のサービスを利用する場合に個人情報を取扱うときは、

外部サービスの利用目的および安全性に応じて、利用前および利用期間中において継続的に個人情報への影響評価および点検を実施します。

3.3.3. LINE WORKS 株式会社における個人情報保護教育の実施

LINE WORKS 株式会社では、全ての役員・従業員に対して年 2 回以上定期的に個人情報保護に関する教育を実施し、セキュリティへの意識と知識水準の維持を行なっています。

3.4. 情報セキュリティと個人情報の保護を実現するプロセス・組織・第三者認証

企業や組織において、適切に情報セキュリティと個人情報を保護するためには、その企業や組織の全体で取り組みを行い、情報セキュリティと個人情報を尊重する文化を醸成していく必要があります。
LINE WORKS 株式会社では、「プロセス」「組織」「第三者認証」の 3 つの仕組みにより、情報セキュリティと個人情報の保護の確立を行っています。

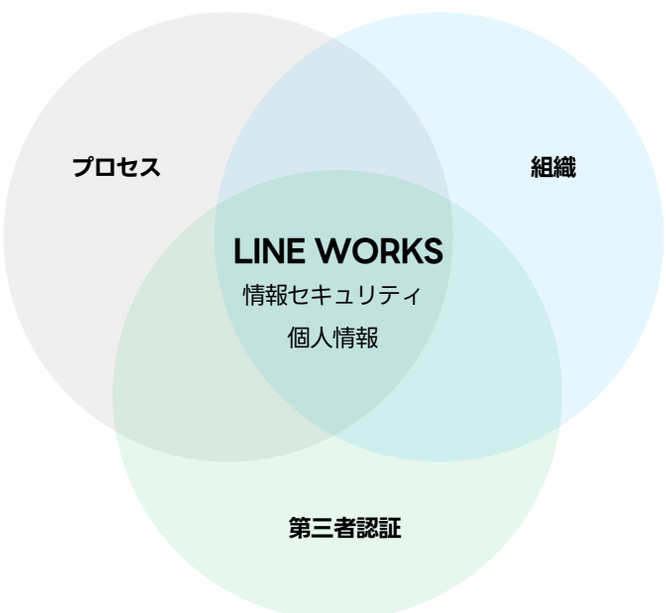


図 . 情報セキュリティと個人情報の保護を実現するプロセス・組織・第三者認証

3.4.1. LINE WORKS のプロセス : セキュアなサービスライフサイクル

SaaS サービスは、コンセプトや主要な機能などの企画・設計から始まり、開発や品質保証などの工程を経て、リリースにより利用者が実際に使えるようになります。そして、利用者が 365 日 24 時間安心してサービスを使えるようにするために不可欠な「サービス運用」の活動を行います。このような一連の流れを SaaS の「ライフサイクル」と言います。利用者が SaaS サービスを安心して利用できるようにするために、そのライフサイクル全体において、情報セキュリティと個人情報の保護を行う必要があります。
LINE WORKS 株式会社では、以下の 5 つのフェイズにおいて、情報セキュリティと個人情報の保護を最優先にしてサー

ビスの開発・運用を行っています。

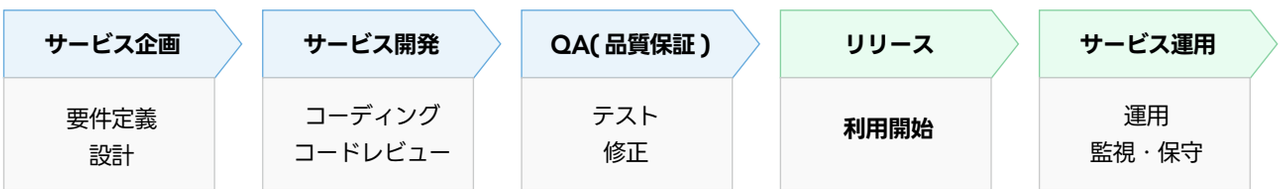


図 . LINE WORKS サービスライフサイクル

サービス企画

サービス利用者の課題を特定し、それらに対するソリューションとして、サービスの機能、ユーザーインタフェース、セキュリティ、パフォーマンスなどの要件を定義します。セキュリティの観点から、ソリューションに対する脅威のモデリング、その脅威に対するリスク評価、セキュリティ要件の特定·文書化を行った上で、セキュアなアーキテクチャの設計を行います。

サービス開発

サービス企画で定義された要件に従って、サービスの機能、ユーザーインタフェース、セキュリティ、パフォーマンスなどの実現に必要な実装を行います。セキュリティを重視したコーディング基準とベストプラクティスを遵守して実装を行い、定期的なレビューや自動化されたセキュリティスキャン、開発者による脆弱性スキャンやペネトレーションテストなどを実施します。

QA (品質保証)

サービス開発により実装されたサービスの機能、ユーザーインタフェース、セキュリティ、パフォーマンスなどの品質の評価を行います。設計上のセキュリティ要件にどの程度満たしているかを評価し、品質評価組織による品質テスト、脆弱性スキャンやペネトレーションテストなどを行います。QA により問題が発見された場合は、開発組織による修正を行い、再度品質評価を実施します。

リリース

品質評価を満たしたサービスの機能、ユーザーインタフェース、セキュリティ、パフォーマンスなどを、利用者が利用可能な状態にします。セキュリティの観点から､確立されたリリースプロセスに従ってセキュアにデプロイ (配置) を行います。デプロイ後に、適切なアクセス制御により利用者が新しい実装を利用できる状態にし、リリースノートにより新機能に関する情報を提供します。

サービス運用

サービスの利用者に提供されているサービスの機能、ユーザーインタフェース、セキュリティ、パフォーマンスなどの実装について、運用、監視および保守を行います。セキュリティの観点から、サービスの監視を継続的に行い、不審な活動やセキュリティ違反の兆候を検出した場合は、迅速に対応を行います。定期的なセキュリティレビュー

を実施し、新たなセキュリティ脅威に対応するために必要な改善を継続的に行います。

LINE WORKS 株式会社は、提供するサービスのライフサイクルにおいて、以下のセキュリティ活動を積極的に行っています。

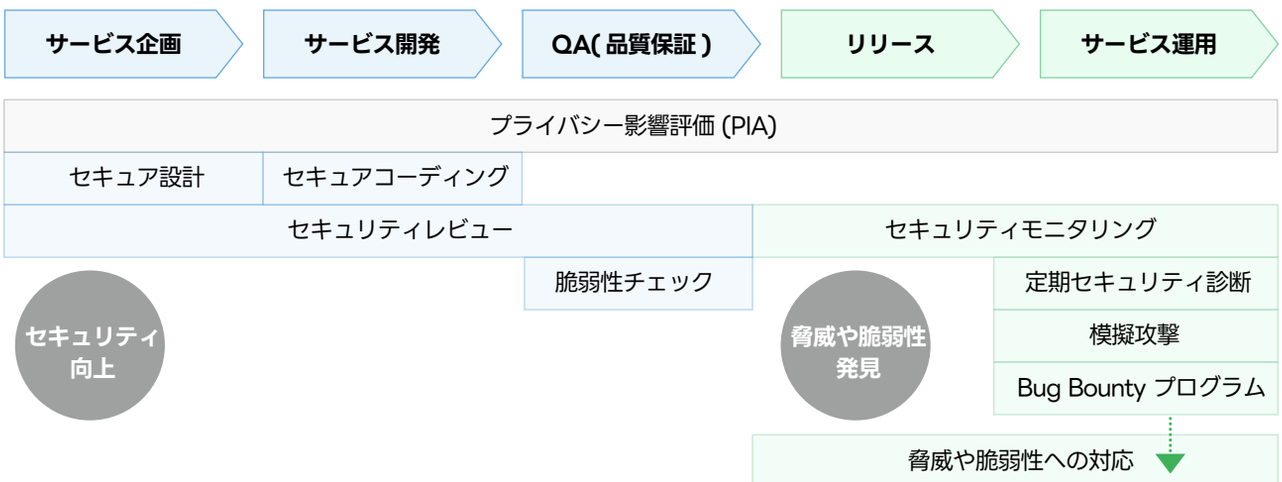


図 . LINE WORKS サービスのライフサイクルにおけるセキュリティ活動

プライバシー影響評価 (PIA)

LINE WORKS 株式会社では、サービスのライフサイクル全ての活動において、新たに個人情報などを取り扱う場合は、プライバシー影響評価 (PIA) を行っています。プライバシー影響評価とは、個人情報などのプライバシー情報を業務で取り扱う場合に、利用者の立場に立って事前にリスクを分析・評価する考え方のことを言います。プライバシー影響評価によって洗い出された潜在的なリスクに対して、適切な保護策を策定し、そのリスクの低減や回避などの制御を行います。

LINE WORKS 株式会社では、社内の PIMS(Privacy Information Management System) を通じてサービスにおけるプライバシー情報の取扱いについて問い合わせを登録することで、セキュリティ専門部署の担当者が関連法規および社内規定に基づき必要な保護措置を回答および支援する体制を敷いています。また、法令や社内のガイドラインの遵守状況を点検し、不十分な点がある場合は補完するよう措置を講じています。

セキュリティ向上のための活動

セキュア設計

LINE WORKS 株式会社では、サービスの企画において、情報セキュリティや個人情報保護を設計の柱とする考え方により、セキュアな設計を行っています。

脅威モデリング

サービスに対する脅威をモデリングし、潜在的な脅威とそれらに対する防御策を特定します。

リスク評価

サービスに対する脅威と防御策から、潜在的なセキュリティリスクを特定し、リスク評価を行います。

セキュリティ要件の定義

リスク評価の結果を受けて、データ保護、アクセス制御、暗号化などのセキュリティ要件を特定し、文書化します。

セキュアなアーキテクチャの設計

サービスについてセキュアなアーキテクチャを設計します。セキュアなアーキテクチャにおいては、適切なデータ分離、最小限の権限原則、安全な通信チャネルの確保などが行われます。

セキュアコーディング

LINE WORKS 株式会社では、サービスの開発において、安全なソースコードが使用されるように、セキュリティの重視したコーディング基準とベストプラクティスを遵守し、セキュアなコーディングを行っています。

自動スキャン

ソース管理システムに登録された開発中のソースコードに対して、常にツールによるスキャンを実施し、修正が必要なコードに関しては自動的に通知を行い、修正を行います。

コードレビュー

安全なコードを実現するために、セキュリティに関する高度な知見を有する専門家による定期的なレビューを実施します。

セキュリティテスト

開発プロセスにおいて、開発者による脆弱性スキャンやペネトレーションテストなどのセキュリティテストを実施します。

セキュリティレビュー

LINE WORKS 株式会社では、新たなサービスや機能を追加するときに、その企画、開発、QA(品質保証) において、情報セキュリティや個人情報保護観点によるレビューを行っています。

サービス企画に対するレビュー

サービス企画段階において、主に設計書あるいは企画文書に基づいてセキュリティレビューを行い、保護措置が必要な部分について指摘および措置を行います。

サービス開発に対するレビュー

サービス開発段階において、ソースコードの静的分析を行い、API 設計や使用する暗号化方法などのセキュリ

ティ技術について指摘および措置を行います。

セキュリティ要件への適合評価

QA(品質保証) において、開発された実装が設計上のセキュリティ要件にどの程度満たしているかを評価します。実装がセキュリティ要件を満たしていない場合、サービス開発への差し戻しを行います。

品質テストによる評価

QA(品質保証) において、開発された実装に対して品質評価組織による品質テスト、コードスキャンなどのセキュリティテストを実施します。セキュリティテストにより問題が発見された場合、開発組織による修正を行い、セキュリティテストによる評価を再度実施します。

脆弱性チェック

LINE WORKS 株式会社では、リリースする全てのサービスおよび機能について、QA(品質保証) において、脆弱性チェックを行っています。

脆弱性テストによる評価

QA(品質保証) において、リリースを予定している実装に対してセキュリティ専門家による脆弱性チェックを実施します。脆弱性テストにより問題が発見された場合、開発組織による修正を行い、QA による品質評価を再度実施します。

セキュアなデプロイメント・リリース

QA(品質保証) において、脆弱性チェックに合格したコードは、確立されたデプロイプロセスを経て、セキュアにリリースされます。サービスの利用者は、安心して新サービスや新機能を利用することができます。

脅威や脆弱性発見のための活動

セキュリティモニタリング

LINE WORKS 株式会社では、リリースおよびサービス運用において、不正アクセスやセキュリティ侵害の試みを検知するために、セキュリティ専門スタッフによる 24 時間 365 日体制で監視を行います。

定期セキュリティ診断

LINE WORKS 株式会社では、日々進化するセキュリティ脅威からサービスと利用者を保護するため、サービス運用において定期的にセキュリティ診断を実施しています。

網羅的な脆弱性診断

不正な侵入につながる脆弱性が存在しないか確認するために、サービス全体に対して網羅的に診断を行います。

継続的なセキュリティ改善

新たな脅威や脆弱性の出現に迅速に対応できるように、セキュリティ体制およびセキュリティプロセスを継続的に改善します。

模擬攻撃

LINE WORKS 株式会社では、サービスのセキュリティ強度を確認するために、サービス運用において定期的に模擬攻撃 (ペネトレーションテスト) を行っています。

現実的な攻撃シナリオ

セキュリティ侵害のためによく用いられる技術や手法を駆使した現実的な攻撃シナリオを用いて、サービス環境に対して模擬攻撃を行います。

実際の攻撃耐性の確認

悪意のある第三者の視点で、実際にサービスに侵入することができるかを具体的に検証することで、攻撃された場合のサービスのセキュリティ耐性を確認します。

Bug Bounty プログラム

Bug Bounty は世界中のホワイトハッカーの協力により、LINE WORKS サービスの脆弱性を早期に発見し、ホワイトハッカーへ報酬を支払うプログラムです。外部の第三者による、多角的・網羅的な脆弱性検知により、早期の脆弱性対応を行い、サービスの安全性を向上させることを目的とします。

Bug Bounty プログラムの詳細は LINE WORKS プライバシーセンターの「Bug Bounty」をご参照ください。

脅威や脆弱性への対応

LINE WORKS 株式会社では、リリースおよびサービス運用において発見や報告された脅威や脆弱性に関する情報は専門部署に集約されます。集約された情報は専門スタッフにより分析され、その結果をもとに対策が実施されます。

コンピュータセキュリティインシデントチーム (CERT)

検知した不正アクセスやセキュリティ侵害の試みに対して、社内 CERT を通じてリアルタイムで対応します。外部機関などから脆弱性に関する情報提供を受けた場合は、その情報の内容を分析し、必要な保護措置を行います。

インシデント対応計画

インシデント対応計画を策定し、セキュリティインシデントの発生時に迅速に対応します。

3.4.2. LINE WORKS の組織 : 情報セキュリティ・個人情報保護体制の確立

企業や組織の活動において保有する情報資産や個人情報を適切に保護するために、その企業や組織が直面する脅威やリ

スクに応じて、情報セキュリティ・個人情報保護のための体制を整備する必要があります。LINE WORKS 株式会社では、LINE WORKS のサービスにおける情報セキュリティおよび個人情報保護の実現のために、高度な専門能力を有する責任者や組織を設置して対応しています。

最高情報セキュリティ責任者（CISO) / 最高個人情報責任者 (CPO)

LINE WORKS 株式会社では、CISO および CPO を任命し、LINE WORKS サービスの提供における情報セキュリティと個人情報の保護に対する責任と権限を明確にしています。

最高情報セキュリティ責任者（CISO: Chief Information Security Officer）

企業や組織全体の情報セキュリティ方針を策定し、実施および教育に対して責任を負います。CISO は情報セキュリティに関する専門知識を有し、経営層とセキュリティ実務を担う組織の橋渡しをするとともに、情報セキュリティマネジメントに必要な全ての活動を行います。

最高個人情報責任者 (CPO: Chief Privacy Officer)

企業や組織の個人情報の保護について方針を策定し、実施および教育に対して責任を負います。CPO は個人情報の保護に関する専門知識を有し、個人情報マネジメントに必要な全ての活動を行います。

リスク管理委員会

LINE WORKS 株式会社では、情報セキュリティと個人情報保護の方針を評価・決定する組織として、経営陣を含む「リスク管理委員会」を設置しています。

LINE WORKS の「リスク管理委員会」は、LINE WORKS のサービス開発、運営に関するモニタリング、セキュリティ事故の予防を行っています。万が一、セキュリティ事故が発生した場合は、迅速な対応を行います。

LINE WORKS プライバシー＆セキュリティチーム

LINE WORKS 株式会社では、情報セキュリティと個人情報保護の方針や施策を迅速に実施するための組織として、「LINE WORKS プライバシー＆セキュリティチーム」を設置しています。

「LINE WORKS プライバシー＆セキュリティチーム」は、CPO/CISO を筆頭に、政策や法務等に関する専門家と、プライバシー保護やセキュリティに関する経験値が高い専門スタッフで構成され、決定された施策等の実施のほか、それぞれの分野におけるトレンドの把握や調査を通じて潜在的な問題の把握や改善の提案を実施しています。また、社内各部署が個人情報を扱う場合の暗号化について、技術・運用の両面から支援および点検を行い、外部委託および外部サービス利用について、事前および委託・利用期間中において継続的に個人情報への影響評価および点検を行います。

「LINE WORKS プライバシー＆セキュリティチーム」は、LINE WORKS 株式会社の情報セキュリティおよび個人情報の保護に対する取り組みについて、透明性を持って情報提供を行うために「LINE WORKS Privacy Center」を公開しています。「LINE WORKS Privacy Center」では、LINE WORKS のプライバシーポリシー、情報セキュリティシステム、透明性レポート、個人情報の取り扱いなど、情報セキュリティや個人情報の保護に関する様々な情報を提供しています。

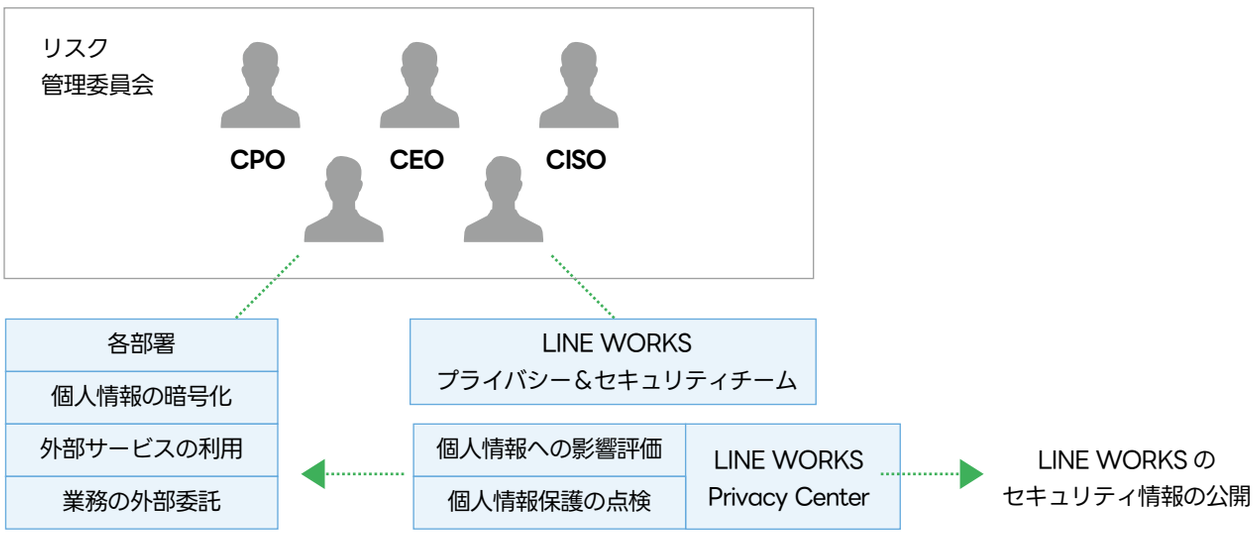


図 . LINE WORKS 株式会社の情報セキュリティ・個人情報保護体制

LINE WORKS 株式会社の情報セキュリティおよび個人情報保護の体制については、LINE WORKS プライバシーセンターの**「セキュリティ体制」**をご参照ください。

3.4.3. LINE WORKS への第三者認証 : 国際標準・公的標準への準拠と認証取得

企業や組織独自のやり方で情報セキュリティマネジメントや個人情報マネジメントを行おうとしても、情報資産や個人情報を適切に保護することは容易ではありません。多くの企業や組織が高い品質、高いレベルで情報セキュリティマネジメントや個人情報マネジメントを実践できるようにするために、以下のような国際的な標準や公的な標準が規格化されています。

ISO/IEC 27001 、27017 、27018 、27701

国際標準化機構 (ISO) と国際電気標準会議 (IEC) が共同で定めた、情報セキュリティマネジメントに関する国際標準です。

- ISO/IEC 27001 は、組織が自社で保護すべき情報資産を洗い出し、その情報資産について、機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability) をそれぞれ維持して改善していくことができる体制を構築することを目的とした標準規格です。

ISO/IEC 27017、ISO/IEC 27018、ISO/IEC 27701 は、ISO/IEC 27001 のアドオンとして位置づけられた標準規格です。

- ISO/IEC 27017 は、クラウドサービスに特化した情報セキュリティのための標準規格です。
- ISO/IEC 27018 は、パブリッククラウドにおける個人情報の保護にフォーカスした標準規格です。
- ISO/IEC 27701 は、取得した個人情報の管理と保護にフォーカスした標準規格です。

LINE WORKS 株式会社は、2016 年に外部監査機関を通じて、LINE WORKS サービスに関する運営、開発過程を対象に、ISO/IEC 27001、27017、2018 の認証報告書を取得し、毎年更新しています。また、2023 年に外部審査機関を通じて ISO/IEC 27701 の認証報告書を取得しています。

SOC 2, SOC 3

米国公認会計士協会 (AICPA) が制定した、サービス運営組織の総合的な内部統制について一定の基準を満たしていることを評価する制度です。

LINE WORKS 株式会社は、2015 年から毎年、LINE WORKS サービスにおける情報セキュリティや個人情報の保護に関する内部統制を対象に、外部監査機関の監査を受け、SOC 2(Service Organization Control Type 2) および SOC 3(Service Organization Control Type 3) の報告書を取得しています。

ISMAP

政府が求めるセキュリティ要求を満たすクラウドサービスを予め評価・登録する制度で、内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省により運営されています。

LINE WORKS 株式会社は、LINE WORKS サービスについて ISMAP 水準のセキュリティを確保することを目的として、LINE WORKS 株式会社に対する要求事項および LINE WORKS サービスにおける情報セキュリティ管理・運用の基準について自主的な予備調査への取り組みを完了しています。本審査対応については、継続検討中です。

このように、LINE WORKS 株式会社は、情報セキュリティや個人情報保護に関連する国際標準・公的標準への準拠および認証の取得を積極的に行っています。

詳細については、LINE WORKS プライバシーセンターの**「認証 / 監査 / 評価」**をご参照ください。

4 章 LINE WORKS サービスにおける「責任共有モデル」

4.1. 本章の概要

本章では、SaaS サービスのセキュリティに興味がある方を想定読者として、SaaS サービスに対するセキュリティ上の脅威の概要と、その脅威に適切に対応するために必要な「責任共有モデル」について、LINE WORKS を例に解説します。

4.2. サービス利用者とサービス提供者による「責任共有モデル」

クラウドサービスの普及および高度化に伴い、クラウドサービスに対する攻撃などの脅威も高度化してきています。このような状況において、クラウドサービスの情報セキュリティを高めるためには、クラウドサービスの提供者と利用者が協力して、クラウドサービスに対する責任を共有する必要があります。このような「責任を共有する」という考え方を「責任共有モデル」と言います。

> 総務省は、2022 年 10 月に**「クラウドサービス利用・提供における適切な設定のためのガイドライン」**を公表しています。このガイドラインでは、「クラウドサービスの事業者 (提供者) と利用者の責任範囲・内容は、クラウドサービスの内容や利用条件・環境ごとに異なる」とした上で、以下の 3 つの責任共有モデルを例示しています。
>
> - SaaS(Software as a Service) に関する責任共有モデル
> - PaaS(Platform as a Service) に関する責任共有モデル
> - aaS(Infrastructure as a Service) に関する責任共有モデル

4.3. LINE WORKS セキュリティ責任共有モデル

LINE WORKS では、総務省が例示する「SaaS に関する責任共有モデル」に準拠し、LINE WORKS のアカウントを有するお客様と、LINE WORKS の間で情報セキュリティ責任を共有する「LINE WORKS セキュリティ責任共有モデル」を採用しています。

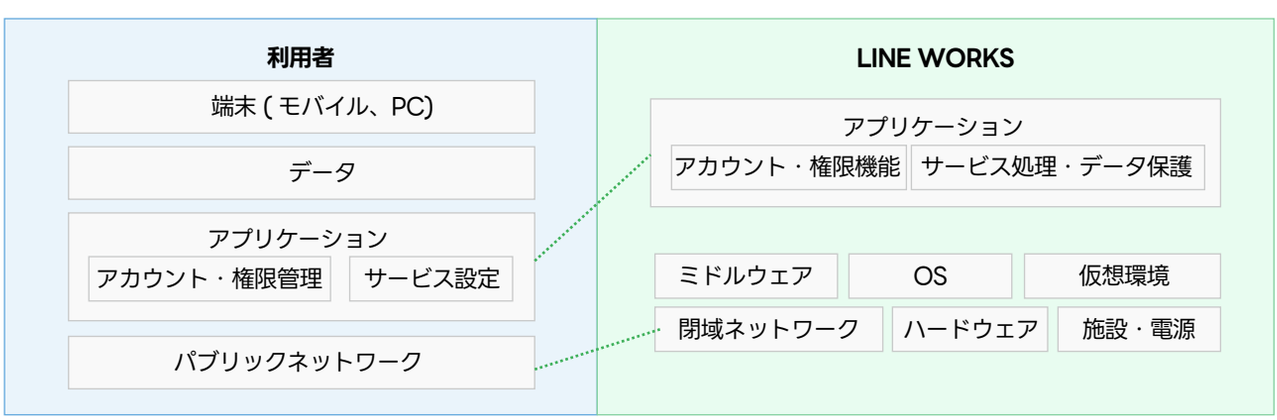


図 . LINE WORKS の責任共有モデル (レイヤー別 : SaaS)

LINE WORKS セキュリティ責任共有モデルにおいて、LINE WORKS 株式会社は、以下の管理や保護などを適切に行う責任を負うものとします。

- アプリケーション

  アカウント・権限を保護するために必要な機能の提供、運用管理

  サービス処理やサービスデータに対する脅威からの情報セキュリティ保護
- SaaS サービス基盤

  ミドルウェアの適切な設定、運用管理

  OS の適切な設定、運用管理

  仮想環境の適切な設定、運用管理

  ハードウェアの適切な運用管理

  内部ネットワークの適切な運用管理

  施設・電源の適切な運用管理

LINE WORKS セキュリティ責任共有モデルにおいて、LINE WORKS の利用者は、以下の管理や保護を適切に行う責任を負うものとします。

- アプリケーション

  LINE WORKS 上のアカウント・権限の適切な管理

  LINE WORKS サービスに関する設定の適切な管理
- データ

  LINE WORKS サービスで利用するデータの適切な管理
- 端末 (モバイル、PC)

  LINE WORKS サービスに接続する端末 (モバイルや PC) の適切な管理
- パブリックネットワーク

  パブリックネットワークからの LINE WORKS へのアクセス経路の適切な管理

LINE WORKS は、利用者の責任を遂行するために必要なサービス上の機能やドキュメントを積極的に提供します。

4.4. 脅威から見る「LINE WORKS セキュリティ責任共有モデル」

インターネット上で提供されている SaaS サービスは、常に以下のような脅威に直面しています。

SaaS サービス利用者

- 利用者に対する脅威

SaaS サービス利用者と提供者の通信

- 通信に対する脅威

SaaS サービス提供者

- アカウント・権限に対する脅威
- サービス処理に対する脅威
- サービスデータに対する脅威
- データセンターや拠点に対する脅威

これらの脅威に効果的かつ継続的に対応していくためには、その脅威の特性ごとに SaaS サービスの利用者および提供者の双方でセキュリティに対する責任を共有し、適切に分担していく必要があります。
LINE WORKS は、これら 6 種類の脅威全てに対して、サービス提供者として分担すべき責任を果たすために必要かつ十分な保護策を実施しています。

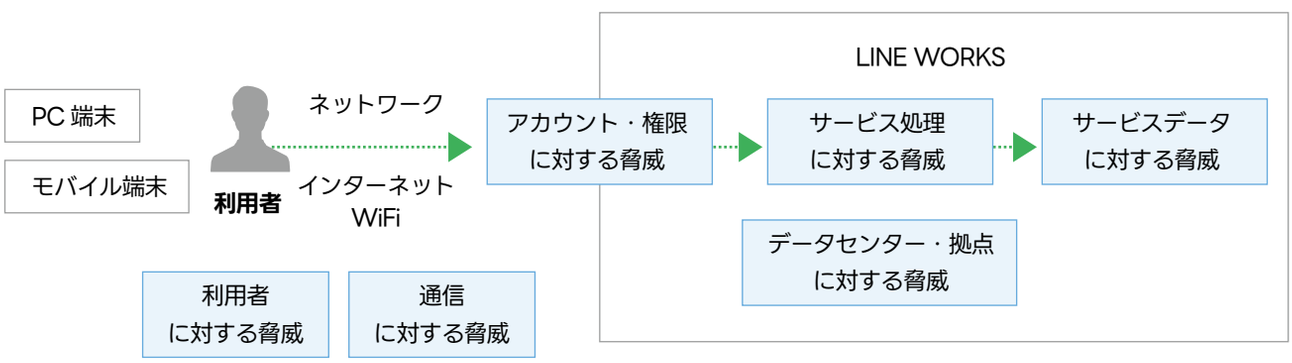


図 . SaaS に対する 6 種類の脅威 (LINE WORKS の場合)

また、LINE WORKS 利用者が分担すべき責任を果たしていただくために、以下の 3 つの脅威に対応するための機能を LINE WORKS 上で提供しています。

- 利用者に対する脅威
- 通信に対する脅威
- アカウント・権限に対する脅威

「LINE WORKS セキュリティ責任共有モデル」においては、脅威に対して適切に対応していくために、以下のように、LINE WORKS 利用者と LINE WORKS でセキュリティ責任を分担いたします。

	LINE WORKS 利用者の責任	LINE WORKS の責任
利用者に対する脅威	セキュリティ機能の活用による情報資産や個人情報の保護	保護策の実施によるセキュリティの確保
通信に対する脅威	セキュリティ機能の活用による情報資産や個人情報の保護	保護策の実施によるセキュリティの確保
アカウント・権限に対する脅威	セキュリティ機能の活用による情報資産や個人情報の保護	保護策の実施によるセキュリティの確保
サービス処理に対する脅威	(LINE WORKS が認める正常な操作の範囲で責任なし)	保護策の実施によるセキュリティの確保
サービスデータに対する脅威	(LINE WORKS が認める正常な操作の範囲で責任なし)	保護策の実施によるセキュリティの確保
データセンターや拠点に対する脅威	(LINE WORKS が認める正常な操作の範囲で責任なし)	保護策の実施によるセキュリティの確保

LINE WORKS 利用者の責任におけるセキュリティ

LINE WORKS セキュリティ責任共有モデルにおいて、LINE WORKS の利用者は、脅威から情報資産や個人情報を保護するために、以下の管理を適切に行う責任を負います。

- 利用者に対する脅威

  LINE WORKS サービスに接続する端末 (モバイルや PC) の適切な管理

  LINE WORKS サービスで利用するデータの適切な管理

  LINE WORKS サービスに関する設定の適切な管理
- 通信に対する脅威

  パブリックネットワークからの LINE WORKS へのアクセス経路の適切な管理
- アカウント・権限に対する脅威

  LINE WORKS サービス上のアカウント・権限の適切な管理

LINE WORKS は、利用者が脅威から情報資産や個人情報を保護するために必要なサービス上の機能やドキュメントを提供します。

LINE WORKS の責任におけるセキュリティ

LINE WORKS セキュリティ責任共有モデルにおいて、LINE WORKS は、以下の脅威からサービスのセキュリティを確保する責任を分担します。

- アカウント・権限に対する脅威

  アカウント・権限を保護するために必要な機能の提供、運用管理
- サービス処理やサービスデータに対する脅威

  ミドルウェアの適切な設定、運用管理

  OS の適切な設定、運用管理
- データセンター・拠点に対する脅威

  仮想環境の適切な設定、運用管理

  ハードウェアの適切な運用管理

  内部ネットワークの適切な運用管理

  施設・電源の適切な運用管理

4.4.1. 利用者に対する脅威

4.4.1.1. 脅威の概要

インターネット上のサービスの利用において、その利用者に対して以下のような脅威が存在します。

端末への脅威

スマホなどのモバイル端末、インターネットに接続している PC 端末などは、常に悪意のある攻撃者からの脅威に直面しています。安全が確保されていない端末に対して、コンピューターウィルスやスパイウェアなどのマルウェア (悪意

のあるソフトウェア) が侵入し、端末が保有する情報が漏えいしたり、端末が乗っ取られて SaaS サービスに不正アクセスされる事例が後を絶ちません。近年はランサムウェア (身代金を要求する悪質なマルウェア) による端末やデータの不正な暗号化により金銭が要求されるケースが目立って増えてきています。
脅威から端末を守るためには、端末の OS やアプリケーションを常に最新に保ち、信頼できないアプリケーションをインストールしないなど、端末の安全を確保することが重要です。

共有情報への脅威

社内や SaaS サービスで共有している社外秘の情報が、意図せずに公開されたり、盗まれることによって情報が漏えいする脅威が存在します。共有情報の漏えいの多くが、管理者の設定ミス、もしくは、ユーザー自身が SaaS の共有機能を利用してインターネット上に公開することによって発生しています。
脅威から共有情報を守るためには、共有機能の設定を正しく行ない、ユーザー自身が適切に情報を取り扱うように周知していくことが重要です。

利用者への脅威

利用者が、フィッシングメールなど大手企業や公的機関を詐称したメールやメッセージに騙され、ログイン情報やクレジットカード情報などの重要な個人情報を詐取される脅威が存在します。近年は、詐取された個人情報により脅迫され、犯罪の幇助を強いられるケースも発生してきています。
脅威から利用者を守るためには、信頼できないサイトへの接続を控え、個人情報の入力を求められたときは、その入力先が正当なサイトであることを必ず確認することが重要です。

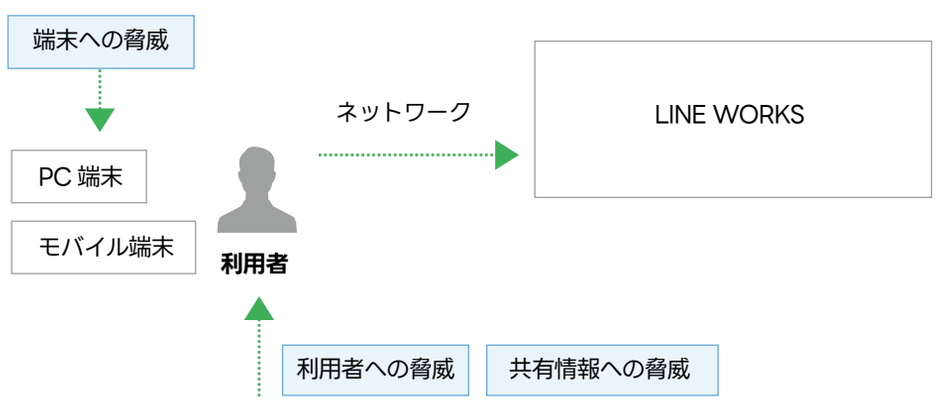


図 . 利用者に対する脅威

4.4.1.2. 利用者によるセキュリティ確保

LINE WORKS の管理者および利用者 (メンバー) は、LINE WORKS の機能を活用して、LINE WORKS の利用者への脅威から情報資産や個人情報を保護します。

端末への脅威への対応

LINE WORKS のサービスを利用する端末に対する脅威から情報資産や個人情報を保護するために、LINE WORKS の以下の機能を活用します。

セキュリティ：モバイル管理

LINE WORKS では、LINE WORKS のサービスを利用するモバイル端末を脅威から保護するために、システム設定で以下の設定をすることができます。

LINE WORKS モバイル版アプリの機能制限

データの保持・閲覧期間

モバイル版アプリから各サービス内のデータを閲覧できる期間を指定します。設定した期間を過ぎたファイルは自動的に削除されます。

画像 / テキスト情報のコピー

モバイル版アプリ内の画像 / テキストの、クリップボードへのコピーを禁止することができます。(メール作成 / 投稿など直接入力する範囲と OS からデフォルトで提供するビュアーでは制限されません。)

モバイルデバイス管理 (MDM)

LINE WORKS が提供する LINE WORKS MDM をご利用いただくと、管理者は遠隔でデバイスにインストールされた LINE WORKS モバイル版アプリのデータ削除やデバイスの初期化をすることができます。
MDM を利用することで、モバイル端末の盗難や紛失時に、その悪用や情報漏えいを防止することが可能になります。

共有情報への脅威への対応

LINE WORKS 上の共有情報に対する脅威から情報資産や個人情報を保護するために、LINE WORKS の以下の機能を活用します。

セキュリティ：ファイル管理

LINE WORKS では、LINE WORKS 上の共有ファイルを脅威から保護するために、システム設定で以下の設定をすることができます。

ファイル形式での制限

LINE WORKS のファイル共有に利用できるサービスやファイル形式を指定することができます。これにより、不正なファイルの持ち込みや攻撃を防止することが可能になります。

モバイル版アプリにおけるファイル利用の制限

モバイル版アプリで、ファイルをダウンロードやアップロードできないようにすることができます。また、モバイル版アプリで表示する画像や動画、文書上にウォーターマーク (操作しているメンバーを特定するための文字列) を重ねて表示することもできます。これにより、モバイル版アプリ利用者のファイルの持ち出しによる外部への情報漏えいや、不正なファイルの持ち込みや攻撃を防止することが可能になります。

外部ユーザーとのトークルームでファイル送信・添付

LINE ユーザーや外部の LINE WORKS ユーザーとのトークルームにおけるファイルの送信を許可もしくは禁止を選択することができます。社外のユーザーとのトークによる利便性と、社内情報の社外への流出リスクを考慮して検討します。

ファイルのダウンロードログ

LINE WORKS のファイル共有を利用して、メンバーがファイルをダウンロード・閲覧した記録を保存・確認することができます。ファイル共有による情報漏えいのリスクが高い場合は、メンバーのファイルダウンロード・閲覧履歴を追跡するために有効にします。

サービス：トーク

LINE WORKS では、LINE WORKS におけるトークの内容を脅威から保護するために、システム設定で以下の設定をすることができます。

外部ユーザーとのトーク

外部ユーザーとのトークの利用を特定のメンバーに限定することができます。社外のユーザーとのトークによる利便性と、社内情報の社外への流出リスクを考慮して検討します。

トークのモニタリング

トークを使用して不適切なやり取りが行われていないかについて、ポリシーを設定して監視することができます。トークによる情報漏えいのリスクが高い場合は、モニタリングの設定を行い、継続的に監視をします。

サービス：Drive

LINE WORKS では、LINE WORKS の Drive に保存されているファイルを脅威から保護するために、システム設定で以下の設定をすることができます。

共有ドライブ

共有ドライブは社内 (同ドメイン) のメンバーが共同で利用できるドライブです。全社や部署別、プロジェクト別の共有ドライブとそのフォルダ構成を検討し、役割別に必要となるアクセス権限を検討します。

リンクのアクセス権限

共有ドライブ、マイドライブ、トークルームフォルダそれぞれについて、共有リンクによるアクセス権限を付与する対象を指定することができます。リンクは、そのリンク先のファイルに対する直接のアクセス権となり、リンクの設定によっては外部への共有も可能となります。リンクの利便性と、社内情報の社外への流出リスクを考慮して検討します。

Drive のモニタリング

Drive を使用して不適切なデータのアップロードやダウンロードが行われていないかについて、ポリシーを設定して監視することができます。Drive による情報漏えいのリスクが高い場合は、モニタリングの設定を行い、継続的に監視をします。

監査

LINE WORKS の「監査」機能を利用することで、メンバーの利用履歴を検索することができます。モニタリングのポリシーに該当する操作があった場合や、不正利用などが疑われる場合は、監査ログを調査して、いつ、誰が、どのような操作をしたのかを追跡します。

LINE WORKS の監査ログには保存期限があるため、お客様の情報セキュリティポリシーに従って監査ログの保存ポリシーを策定し、保存ポリシーの範囲内で必要最低限のダウンロードおよび管理を行います。監査ログには通信の秘密に関わる情報が含まれるため、ダウンロード後は厳重な管理および慎重な取り扱いが必要となります。

重要
LINE WORKS サービスの管理者は、監査・モニタリングサービスの利用に伴い、メンバーのデータ (トーク内容など) にアクセスする場合は、法令および「LINE WORKS サービス利用規約」の定めに従い、メンバーの有効な同意を必ず得るものとします。

なお、メンバーからの同意の有無に関わらず、メンバーのデータにアクセスしたことにより管理者とメンバーとの間で生じたトラブルについては、LINE WORKS 株式会社は責任を負いかねますのでご留意ください。

利用者への脅威への対応

インターネット上のサービスの利用者への脅威から情報資産や個人情報を保護する上で、技術的な対応は大きなウエイトを占めますが、情報資産や個人情報を保護するための行動や意識を欠かすことはできません。

そのためには、組織のトップからのセキュリティに対する明確なコミットメント、セキュリティポリシーの確立、社員への教育とトレーニングにより、組織全体でセキュリティを重視する文化を築き上げる必要があります。セキュリティ文化を根付かせることは一朝一夕にできることではありません。組織全体のコミットメントと継続的な取り組みにより、組織としてビジネスと従業員を守る文化が醸成されていきます。

4.4.1.3. LINE WORKS による保護策

LINE WORKS は、「LINE WORKS セキュリティ責任共有モデル」に基づき、LINE WORKS の利用者を脅威から保護するために必要な機能を利用者に提供するとともに、以下のような保護策を実施します。

アップデート通知機能による最新バージョン情報の提供

LINE WORKS は、モバイル版アプリ、PC 版アプリおよびブラウザ版について常に機能の改善を行っており、セキュリティ上の不備などがあった場合には迅速に対応しています。ブラウザ版は常に最新バージョンをご利用いただけます

が、モバイル版アプリおよび PC 版アプリについては、利用者によるアップデートが必要となります。

LINE WORKS は、利用者に対する脅威への対応として、モバイル版アプリおよび PC 版アプリについても常に最新バージョンを使用することを推奨しています。最新バージョンがリリースされた場合、モバイル版アプリおよび PC 版アプリによりアップデート通知を行います。

LINE WORKS アプリの強制アップデート

LINE WORKS は、モバイル版および PC 版アプリのセキュリティを確保するため、古いバージョンのアプリについて強制アップデートを行い、安全な最新バージョンをご利用いただくための措置を行っています。

不正利用ユーザー対策

外部の LINE WORKS のユーザーから不適切なメッセージなどが送られてきた場合、不正な利用者として LINE WORKS に通報することができます。通報があった場合、LINE WORKS は、通報内容を確認し、調査および対応を行います。

詳細については、LINE WORKS ヘルプセンターの**「外部ユーザーの通報」**をご参照ください。

4.4.2. 通信に対する脅威

4.4.2.1. 脅威の概要

SaaS サービスの利用において、その利用者とサービスとの間の通信に対して以下のような脅威が存在します。

海外などからの不正なアクセスによる脅威

インターネットの性質上、パブリックなネットワーク上にあるリソースには、世界中からアクセスすることができます。SaaS サービス上に保有している情報資産や個人情報が、海外などからの不正アクセスにより漏えいする可能性があります。

海外などからの不正なアクセスによる脅威から情報資産や個人情報を守るためには、アクセス元の国 / 地域や IP アドレスによるアクセス制限を行うことが有効です。

盗聴による脅威

インターネットの性質上、その通信は多くの公開ネットワークを経由してやりとりされます。そのため、暗号化されていない状態で通信が行われると、その経路上では誰でもその内容を知ることができてしまいます。

盗聴の脅威から通信を守るためには、送受信するデータや通信自体を暗号化することが有効です。最新のアルゴリズムで暗号化されたデータや通信は、たとえ盗聴されてもその内容を知られる可能性は極めて低くなります。

偽サイトへの誘導による情報漏えいの脅威

通信を暗号化していてもその通信先が偽サイトの場合、その通信は通信先で暗号が復号化されて平文になるため、通信の中身は漏えいしてしまいます。信頼できないネットワークを利用した場合、利用者が気付きにくい形で、DNS 情報の書き換えによる偽サイトへの誘導や、不正なサイト証明書によって HTTPS 通信の実質的な無効化が行われ、通信の中身が漏えいする可能性があります。

偽サイトによる情報漏えいの脅威から通信を守るためには、まず、信頼できないネットワークを利用せず、偽サイトに誘導されるリスクを抑制することが重要です。その上で、データを暗号化して更に通信を暗号化して送信することが有効です。これにより、仮に通信の中身が漏えいしてもデータ自体は暗号化されているため、情報の漏えいを回避することができます。

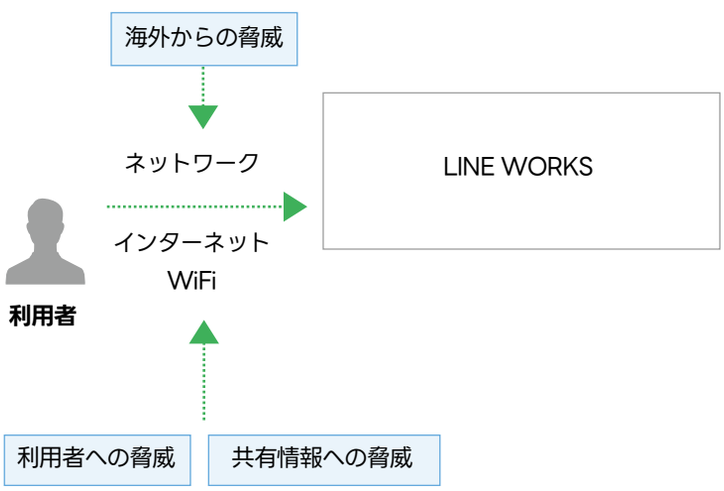


図 . 通信に対する脅威

4.4.2.2. 利用者によるセキュリティ確保

LINE WORKS の管理者は、LINE WORKS の機能を活用して、インターネット上の通信に対する脅威から LINE WORKS 上に保有する情報資産や個人情報を保護します。

海外などからの不正なアクセスによる脅威への対応

LINE WORKS 上に保有する情報資産や個人情報を、海外などから不正なアクセスによる脅威から保護するために、LINE WORKS の以下の機能を活用します。

ネットワーク管理

メンバーが LINE WORKS を利用する際に使用するアクセス元の IP アドレスや国 / 地域を指定することができます。これより、指定された IP アドレスもしくは国 / 地域以外からのアクセスが遮断されます。

偽サイトへの誘導による情報漏えいの脅威への対応

まず、信頼できないネットワークをビジネスにおいては使用しないことが重要です。その上で、偽サイトに誘導されない、もし誘導されても安易に重要な情報を入力しないことが重要です。

4.4.2.3. LINE WORKS による保護策

LINE WORKS は、「LINE WORKS セキュリティ責任共有モデル」に基づき、LINE WORKS の利用者の通信を脅威から保護するために必要な保護策を実施します。

盗聴による脅威

LINE WORKS は、サービス通信の盗聴を防止するために、以下の保護策を行っています。

利用者との通信の暗号化

利用者と LINE WORKS との間の通信について、HTTPS による保護を行っています。これにより、利用者と LINE WORKS との間の通信が暗号化され、盗聴の脅威を回避することができます。

4.4.3. アカウント・権限に対する脅威

4.4.3.1. 脅威の概要

インターネット上のサービスやシステムの利用において、利用者のアカウントや権限に対して以下のような脅威が存在します。

アカウントに対する脅威

企業や組織の情報資産や保有する個人情報を狙って、悪意のある攻撃者がサービスやシステムにアクセスできるアカウントを乗っ取るために多様な攻撃を行なっています。企業やサービスからの公式の連絡を装ったメールやメッセージを使って、ユーザー名やパスワードなどのアカウント情報を盗み出すフィッシング攻撃や、サービスやシステムに対して数千回以上のログインを試行しつづけるパスワード攻撃などによりアカウント情報を奪われる事例が後を絶ちません。特定の企業や組織を狙った「標的型攻撃」もありますが、インターネット全体に対して無作為に攻撃をしていく中で発見した「セキュリティ強度が弱いところから情報資産や個人情報を効率良く奪っていく」というやり方の方が圧倒的に多いのが現実です。

アカウントを脅威から守るためには、「自分たちが狙われることは無い」とは決して考えず、パスワードの強度を高くする、連続してログインに失敗時にアカウントを凍結する、多要素認証を活用するなどのポリシーを決めて実行することが重要です。

権限に対する脅威

インターネット上の攻撃者は、何らかの方法で入手したアカウントの情報を悪用してサービスやシステムにアクセスし、情報資産や個人情報を閲覧したり、改ざんや破壊をしたり、外部に持ち出そうとします。このときに、使われたアカウントに強い権限が付与されていた場合は、そこに保管されている全ての情報資産と個人情報について閲覧、改ざん、破壊、持ち出しなどの侵害を行うことが可能となってしまいます。

万が一、アカウントの乗っ取りが発生した場合でも、情報資産や個人情報への侵害による被害を最低限に抑えるためには、各アカウントは必要な権限に絞り、強い権限によるリスクを下げることが重要です。
また、権限を個人に対して付与するのではなく、役割別に権限の組合せ (テンプレート) を定義し、各個人にはその役

割に応じた権限テンプレートを適用することが極めて有効です。このようなアクセス権限の管理方法を「ロールベースのアクセス管理」と言います。

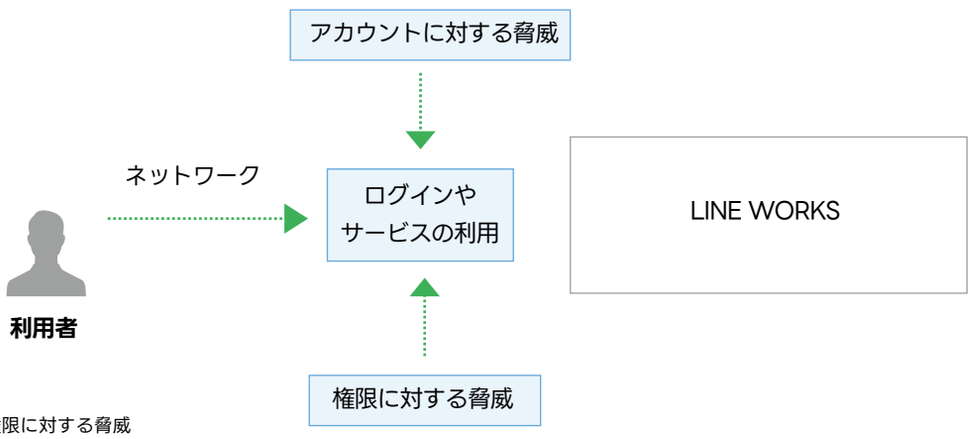


図 . アカウント・権限に対する脅威

4.4.3.2. 利用者によるセキュリティ確保

LINE WORKS の管理者およびメンバー (LINE WORKS の利用者のことを言います。) は、LINE WORKS の機能を活用して、LINE WORKS のアカウント・権限に対する脅威から情報資産や個人情報を保護する必要があります。

アカウントに対する脅威への対応

LINE WORKS のアカウントに対する脅威からメンバーを保護するために、LINE WORKS の以下の機能を活用します。

メンバー : メンバーの招待

LINE WORKS では、不正なメンバーの追加を防ぐために、LINE WORKS を利用するメンバーの招待について、システム設定で以下を指定することができます。

メンバーの招待方法

- すべてのメンバーが他のメンバーを招待することを認める。
- メンバーの招待を管理者のみに認める。

招待されたメンバーのサービス利用開始時期

- 招待と同時に利用可能にする。
- 管理者が承認してから利用可能にする。

メンバーの所属する組織の規模やセキュリティポリシーに応じて、設定を選択します。

セキュリティ : アカウント管理

LINE WORKS では、メンバーのログイン情報を保護するために、パスワードやログインに関するポリシーなどについて、

システム設定で以下を指定することができます。

パスワードポリシー

メンバーが使用するパスワードの形式 (文字種)、長さ、有効期限、パスワードの再使用禁止などについて指定できます。

ログインポリシー

LINE WORKS のログインポリシーでは、2 段階認証を使用することができます。2 段階認証を利用した場合、メンバーは LINE WORKS にログイン後、SMS やメール、生体認証による認証を行います。これにより SMS やメールにアクセスできない第三者による不正アクセスを防止することができます。

LINE WORKS のログインポリシーにより、操作が一定時間の無い場合に自動的にログアウトさせることができます。自動ログアウトは、モバイル版アプリとブラウザ版アプリで個別に指定します。

ログイン方法

ログイン時の使用できる認証方法 (携帯番号、LINE アカウント、モバイル端末の生体認証など) を指定することができます。

シングルサインオン (SSO)

LINE WORKS は、メンバーが一度の認証で複数のアプリケーションやサービスにアクセスできる技術である「シングルサインオン (SSO)」に対応しています。

SSO によりアカウントやパスワードを一元管理することで、退職に伴うアカウントの削除、異動に伴う権限の変更などを、利用しているサービスやシステムごとに行う必要がなくなります。これにより、退職者のアカウントの削除漏れや、異動後のメンバーに不適切な権限が残ることによる情報漏えいのリスクを低減させることができます。

LINE WORKS における SSO 利用については、LINE WORKS Developers「SSO の概要」をご参照ください。

権限に対する脅威への対応

LINE WORKS の管理者およびメンバーは、権限に対する脅威からメンバーを保護するために、LINE WORKS の以下の機能を活用します。

メンバー : 役職 / 職級 / 利用権限タイプ

LINE WORKS では、「利用権限タイプ」を設定することで「ロールベースのアクセス管理」を行うことができます。LINE WORKS 上でのメンバーの役割に応じて「利用権限タイプ」を作成し、各メンバー個人に「利用権限タイプ」を割り当てることで、権限の適切な付与を実現します。これにより、メンバーのログイン情報を不正に利用された場合の被害を最小限に抑えます。

セキュリティ：サービス利用設定

LINE WORKS では、「権限テンプレート」により、利用できるサービスの権限や機能の組み合わせを定義することができます。権限テンプレートを「利用権限タイプ」と紐付けることで、その「利用権限タイプ」が指定されているメンバーは、サービスや機能にアクセスする権限を得ることができます。(権限テンプレートを特定の個人と紐付けることもできます。)

セキュリティ：管理者権限

LINE WORKS では、サービスの管理のために、「最高管理者」「副管理者」「運用担当者」の 3 種類の管理者権限を用意しています。管理者権限は、LINE WORKS の利用において非常に強力であるため、その管理を委任するときに、必要最低限の権限のみを付与した独自にカスタムした「管理者権限」を作成することができます。独自にカスタムした管理者権限の利用により、管理者のログイン情報を不正に利用された場合の被害を最小限に抑えます。情報資産や個人情報を適切に保護するためには、管理者が意図しない操作をメンバーが行わないように、メンバーの権限を適切に設計し、管理する必要があります。

4.4.3.3. LINE WORKS による保護策

LINE WORKS は、「LINE WORKS セキュリティ責任共有モデル」に基づき、アカウント・権限を脅威から保護するために必要な機能を、利用者に提供します。

4.4.4. サービス処理に対する脅威

4.4.4.1. 脅威の概要

インターネット上のサービスには、そのサービスにおける処理に対して、以下のような脅威が存在します。

機能不備による脅威

インターネット上で稼動しているコンピュータープログラムにおいて、何らかの不備が発生することは避けられません。適切なソースコード管理により、多くの不備はその公開前に解消されますが、技術の進展とともに、以前は正常なものとされていたものが現状とは合致しなくなったり、新たな視点からそれが不備であるとされたりすることで、公開中のプログラムに不備がある状態になる場合があります。

モバイル端末や PC、あらゆるサービス、あらゆるアプリケーションの提供者は、このような不備を防止するために、プログラムコードの定期的な自動チェックと、不備を発見したときには迅速な修正を行っています。

サービスやアプリケーションの利用者が、プログラムの機能不備による脅威を避けるために、その利用環境 (モバイル端末、PC) の OS、利用しているアプリケーションについて、常に最新のものを使う必要があります。

脆弱性への攻撃による脅威

プログラムの機能に不備があり、それが情報セキュリティや個人情報に関わるものである場合は、そのプログラムには「脆

弱性がある」という状態になります。インターネット上のサービスの多くは、常に脆弱性を狙ったセキュリティ攻撃の脅威に直面しています。既に広く知られている脆弱性を利用する「エクスプロイト攻撃」では、最新版ではない OS やソフトウェアを利用している環境に対して攻撃を行い、残されたままになっている脆弱性を利用して不正アクセスを行います。攻撃者が独自に発見した脆弱性や、まだ一般には公開されていない脆弱性を利用する「ゼロデイ攻撃」では、修正パッチによる対応や脆弱性情報が公開される前に脆弱性を利用して不正アクセスを行います。

脆弱性への攻撃による脅威から情報資産や個人情報を守るためには、常に OS やソフトウェアを最新に保ち、少しでも脆弱性を減らしていくことが重要です。ゼロデイ攻撃に対しては、セキュリティ専門組織を社内に設置し、外部のセキュリティ専門組織の支援を得ることで攻撃リスクの低減を行います。

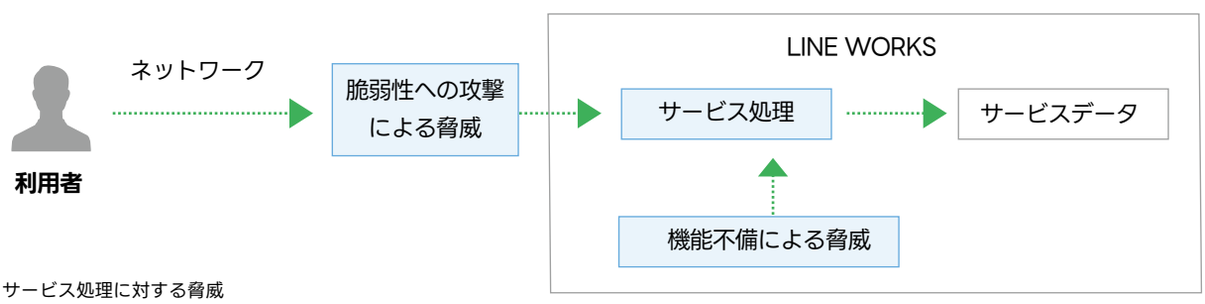


図 . サービス処理に対する脅威

4.4.4.2. LINE WORKS による保護策

LINE WORKS は、「LINE WORKS セキュリティ責任共有モデル」に基づき、LINE WORKS サービス上の処理を脅威から保護するために必要な保護策を実施します。

機能不備による脅威の発生防止

LINE WORKS は、機能不備による脅威の発生を防止するために、以下の保護策を行っています。

最新バージョンの提供

LINE WORKS が提供するサービスについて常に機能の改善を行っており、機能やセキュリティ上の不備などがあった場合には迅速に対応しています。

脆弱性を狙う攻撃による脅威への対応

LINE WORKS は、脆弱性を狙う攻撃による脅威に対応するために、以下の保護策を行っています。

IDS による不正なアクセスの検知・防御

不正侵入検知システム (IDS) により、脆弱性を狙った不正なアクセスを検知・防御する体制を敷いています。

24 時間サイバー脅威モニタリング

不正侵入などの外部からの攻撃に対して、24 時間 365 日体制で監視しています。攻撃を検知した場合は、セキュリティの専門スタッフが迅速に対応を行います。

定期的な脆弱性チェック

LINE WORKS のサービスは、リリース前に QA(品質保証) による綿密なセキュリティチェックが行われますが、サービスの安全を常に保つために、セキュリティ専門家による脆弱性チェックを定期的に実施します。

脆弱性発見時に迅速な対応を実施

LINE WORKS で利用しているプロダクトに脆弱性が発見された場合、定期リリースを待たずに直ちに可能な対応 (緊急修正パッチの適用など) を行います。

定期的な模擬攻撃による点検

サービスのセキュリティ強度を確認するために、現実的な攻撃シナリオを用いて、定期的に模擬攻撃を行います。悪意のある第三者の視点で、実際にサービスに侵入することができるかを具体的に検証することで、サービスのセキュリティ耐性を確認します。

4.4.5. サービスデータに対する脅威

4.4.5.1. 脅威の概要

SaaS サービスには、そのサービスが保有するデータに対して、以下のような脅威が存在します。

他の利用者のデータへの想定外のアクセス

複数の利用者が利用するシステムにおいて、データへのアクセス設計や設定が適切に行われていない場合、利用者の保有する情報資産や個人情報に、他の利用者からアクセスできてしまう可能性があります。
システム提供者は、このようなアクセスの発生を防ぐために、サービスデータの構造や配置について深く注意を払い、設計・開発から運用の全ての活動を行うことが求められています。

サービスデータへの不正なアクセス

サービスやシステムの内部で利用している「公開すべきではないデータ」に対して、攻撃者は経済的な利益や技術的な興味から攻撃を行っています。例えば、サービスやシステムの管理情報や、管理者のアカウント情報などが流出した場合、結果として、そのサービスやシステムに保管されている情報資産や個人情報の漏えいや、改ざん・破壊が行われる可能性があります。
攻撃者からサービス内部のデータを守るためには、これらの情報を暗号化し、セキュリティ強度の高い区域で保管することが重要です。

サービスデータの改ざん・破壊による事業への損失

サービスやシステムの内部で利用しているデータが改ざんや破壊された企業や組織は、その事業の継続が困難になった

り、社会的な信用を失ったりする恐れがあります。
データを改ざんや破壊の被害から復旧させるためには、適切にバックアップを取得し、データの復旧を確実に行うことができる体制を整備することが重要です。

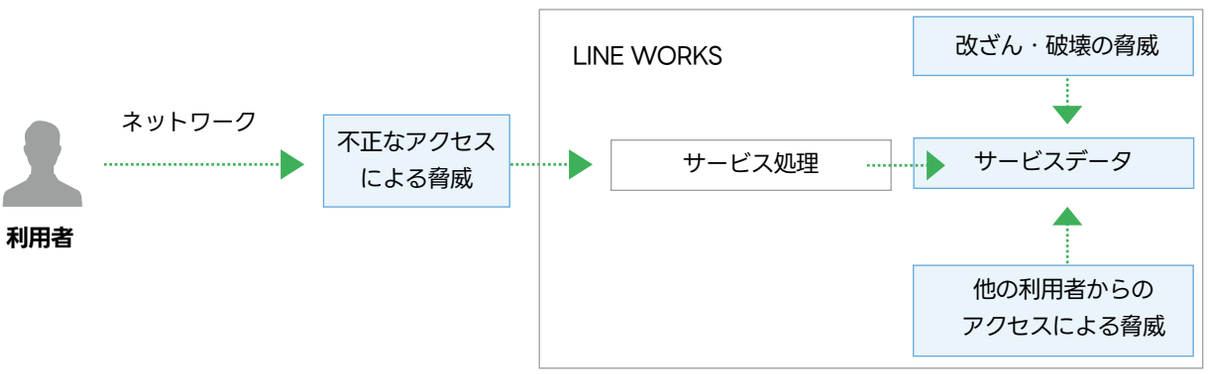


図 . サービスデータに対する脅威

4.4.5.2. LINE WORKS による保護策

LINE WORKS は、「LINE WORKS セキュリティ責任共有モデル」に基づき、LINE WORKS のサービス上のデータを脅威から保護するために必要な保護策を実施します。

他の利用者のデータへの想定外アクセスの防止

LINE WORKS は、サービス内において他の企業や組織との間で想定していないデータアクセスが発生することを防止するために、以下の保護策を行っています。

論理的なデータの分離

LINE WORKS の契約単位でテナントという論理的に独立した空間を割り当てており、テナントを超えてデータにアクセスができない制約があります。この制約により、他のテナントのユーザーが、テナントを超えて自社の情報資産や個人情報にアクセスしたり、情報の漏えいや改ざんなどが行われたりすることを防止しています。

サービスデータへの不正アクセスの防止

LINE WORKS は、サービス内部のデータへの不正アクセスを防止するために、以下の保護策を行っています。

データ保存場所の防御

LINE WORKS のデータは国内のデータセンターに保存されています。サービスで保有するデータの重要度およびリスクに応じて、そのデータ保存場所に対してネットワーク的にも物理的にも強度の高いセキュリティ施策を実施しています。

データの暗号化

サービスで保有するデータは、その対象と用途に応じて暗号化することを義務付けています。暗証番号やパスワー

ドのように復号を行わないデータについてはハッシュアルゴリズムを使用します。サービスでの利用時に復号を行うデータについては対称鍵アルゴリズムを使用した上で鍵を厳重に保管します。これらの暗号化されたデータは、外部からはもちろん、内部においても直接読み取りをすることはできません。

データ改ざん・破壊の検知

セキュリティ監視システムにより 365 日 24 時間体制で監視をしており、データの改ざんや破壊の試みをリアルタイムで検知し、迅速にブロックできる体制を敷いています。

サービスデータの改ざん、破壊による被害の抑制

LINE WORKS は、サービスデータへの不正なアクセスや改ざん、破壊の防止に万全を期していますが、万が一サービスデータで改ざん、破壊が発生した場合は、直ちに復旧するために以下の保護策を行っています。

サービスデータのバックアップ

サービス内部のデータについて、その重要度に合わせてバックアップの取得周期や取得範囲、保存方法についてルールを定めて運用しています。バックアップによる復旧を迅速に行うための手順および体制を整備し、定期的な復旧演習を実施しています。

4.4.6. データセンターや拠点に対する脅威

4.4.6.1. 脅威の概要

インターネットサービスには、そのサービスが稼動しているデータセンターや業務を行う拠点に対して、以下のような脅威が存在します。

自然災害や深刻な事故

企業や組織が持つ情報資産や個人情報は、データセンターや企業の拠点などに保管されていますが、地震による破壊や洪水による水没などの自然災害や、建物の火災や破壊などの深刻な事故により失われる可能性があります。
SaaS サービスの提供者は、このような自然災害によるサービスの停止を防止するために、災害復旧計画 (DR: Disaster Recovery) の策定とその実施体制を敷いています。

不正侵入

攻撃者が、データセンターや企業の拠点の内部に侵入し、そこに保管されている情報資産や個人情報に対して攻撃 (取得、改ざん、破壊など) が行われる可能性があります。侵入はセキュリティカードや鍵の盗難や複製、施設の監視カメラの死角などを利用した無許可での立ち入りによって行われるだけでなく、人の心理を利用して、取引業者や関係者を装って行われる場合もあります。
不正侵入の脅威から情報資産や個人情報を守るためには、データセンターや企業の拠点について、適切に入退館管理をし、建物内部において扱う情報資産や個人情報のレベルに応じて、部屋の割り当てと、入室許可の対象者を制限することが重要です。

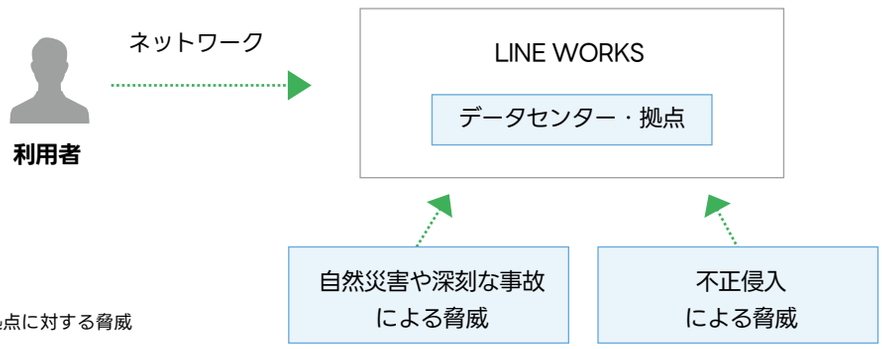


図 . データセンター・拠点に対する脅威

4.4.6.2. LINE WORKS による保護策

LINE WORKS のデータは国内のデータセンターに保存されています。「LINE WORKS セキュリティ責任共有モデル」に基づき、データセンターや拠点への脅威に対する保護策を実施します。

自然災害や深刻な事故への備え

LINE WORKS は、自然災害や深刻な事故が発生した場合においても、LINE WORKS サービスを持続して提供できるために、以下の取り組みを行っています。

データセンターの多重化

LINE WORKS は、利用するデータセンターや業務を行う拠点を多重化しており、自然災害や深刻な事故の発生により単一のデータセンターや拠点が被災した場合でも、サービスの提供を持続できる体制を敷いています。

DR システム構築

LINE WORKS は、サービス提供について災害復旧 (DR: Disaster Recovery) システムを構築しており、自然災害や深刻な事故の発生により緊急事態が発生した場合においても、その影響を最小限に抑制してサービスを継続できる体制を敷いています。

不正侵入の防止

LINE WORKS は、データセンターや拠点への不正侵入を防止するために、以下の保護策を行っています。

データセンター・拠点の保護

データセンター・拠点への不正アクセスを防止するため、全てのセキュリティ区域において入退室セキュリティシステムおよび映像セキュリティシステムによる保護を行います。セキュリティ区域は保安レベルに応じて物理的に分離し、高レベルのセキュリティ区域においては、非認可者の出入りを完全に遮断するとともに、認可者についても二重認証による厳密な入室管理を行います。

データセンターについてはその所在地を非公開とし、あらかじめ許可されたスタッフのみが所在地にアクセスおよび入館できる体制を敷いています。

データセンター・拠点の 24 時間監視

データセンター・拠点に設置した映像セキュリティシステムの映像は、管制センターにおいて 365 日 24 時間体制で監視および対応を行います。

データセンターの入退館管理および定期的な監査

データセンターへの入退館については、その記録を長期保管し、適切な入館が行われていることを定期的に点検します。

5 章 LINE WORKS サービスをセキュアに利用するための設計と設定

5.1. 本章の概要

本章では、LINE WORKS サービスをセキュアに利用するために必要な設計および設定について解説します。
LINE WORKS の導入担当者は、LINE WORKS を安全に活用するために、以下の 3 つの領域について設計を行い、設計に従って LINE WORKS の設定を実施します。

アカウント・権限に関する設計・設定
アカウント・権限への脅威に対応するために必要な設計・設定を行います。

通信に関する設計・設定
通信への脅威に対応するために必要な設計・設定を行います。

サービス利用に関する設計・設定
利用者のサービス利用における脅威に対応するために必要な設計・設定を行います。

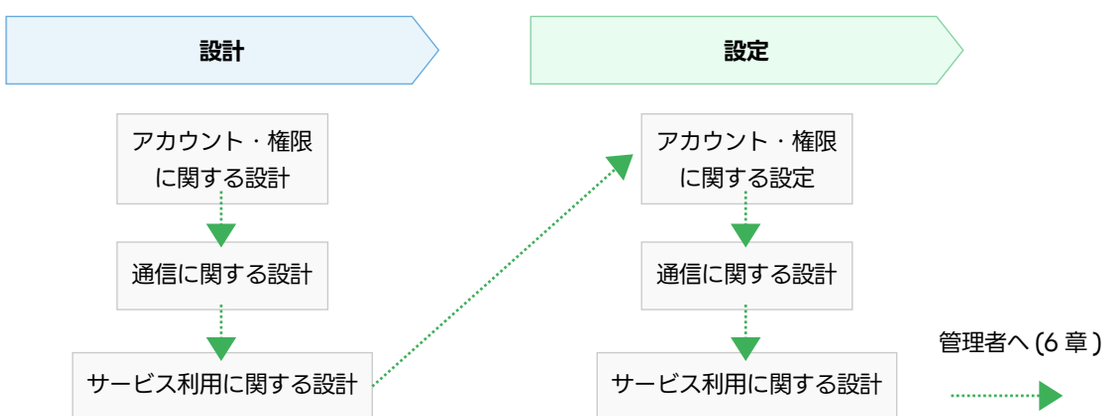


図 . 5 章の概要

注釈
LINE WORKS の設定は、社内の有識者や専門部署などによる設計レビュー後に行うことを推奨します。

導入完了後、導入担当者は管理者に対して LINE WORKS サービスの管理を引き継ぎます。(導入担当者が管理者を兼ねる場合もあります。)

5.2. 管理者画面へのアクセス

LINE WORKS の設定は**管理者画面**で行います。LINE WORKS のテナント開設時に管理者画面にアクセスすることができるのは、テナントを開設した最高管理者のみです。

注釈

LINE WORKS の契約単位で割り当てられる論理的な空間を「テナント」と言います。

最高管理者は、他のメンバーに副管理者の権限を付与することで、導入作業を委任することができます。他のメンバーに管理者権限を付与することができるのは最高管理者のみです。

5.3. アカウント・権限に関する設計・設定

アカウント・権限への脅威に対応するために、メンバー、セキュリティの設計・設定を行います。

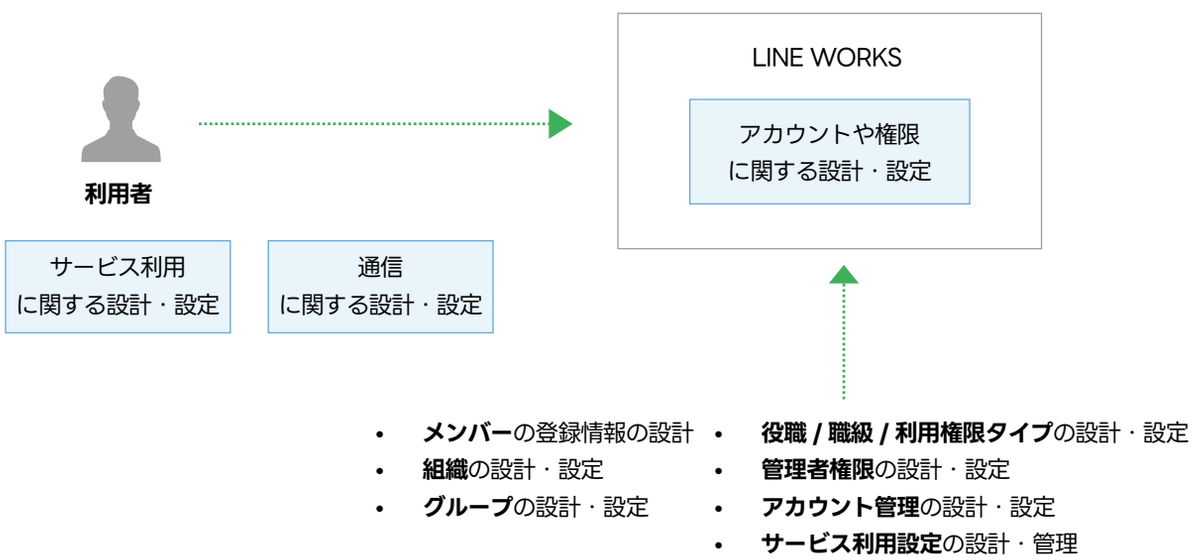


図 . アカウント・権限に関する設計・設定

5.3.1. メンバー : 登録情報の設計

LINE WORKS を利用するメンバーの個人情報を保護するために、LINE WORKS に登録するメンバー情報の設計を行います。

5.3.1.1. メンバーの登録情報

LINE WORKS では、メンバーについて以下の情報を登録することができます。

氏名

- 姓 / 名 (必須)
- ニックネーム

所属情報

- ID
- 利用権限タイプ
- 職級
- 組織
- 役職
- 電話番号
- 携帯番号
- 個人メールアドレス

その他

- 使用言語
- 勤務先
- 担当業務
- SNS
- 生年月日
- 入社日
- 社員番号
- 関係者連絡先

5.3.1.2. メンバーの登録情報の設計

メンバー情報の各項目について、以下のポリシーを検討します。

- 管理者が登録すべき事項
- メンバーが登録すべき事項
- 初期パスワードの受け渡し方法
- 利用開始日の決定ルール

メンバー情報に登録できる情報には、生年月日や社員番号など、メンバーのプライバシーに関連する情報があります。お客様の業務方針および社内ルールに従い、メンバー情報に登録すべき情報の検討が必要です。検討の結果、メンバーの個人情報を登録することになった場合、その管理責任はお客様の管理者が負うことになります。

注釈

LINE WORKS 株式会社は個人情報委託先ではありません。

5.3.1.3. メンバーの登録

メンバーの登録は、管理者画面の「メンバー」>「メンバー」から行います。メンバーの登録の詳細は、管理者画面利用ガイドの**「メンバーの追加」**の「メンバーを個別追加する」をご参照ください。

5.3.2. メンバー : メンバーの招待

LINE WORKS への不正なメンバーの追加を防ぐために、新規に利用するメンバーの招待に関する設計・設定を行います。

5.3.2.1. メンバーの招待の機能

LINE WORKS では、利用するメンバーの招待について以下を指定します。

リンク /QR コードによる招待

- リンク /QR コードによる招待を許可する。
- リンク /QR コードによる招待を許可しない。

招待を許可した場合、招待された人が自分でメンバー登録を行うことができます。招待を許可しない場合、全てのメンバーは管理者が登録を行います。
招待を許可した場合は、更に以下の設定を指定することができます。

メンバーの招待方法

- すべてのメンバーが他のメンバーを招待することを認める。
- メンバーの招待を管理者のみに認める。

自動承認 (招待されたメンバーのサービス利用開始時期)

- 有効 (招待と同時に利用可能にする。)
- 無効 (管理者が承認してから利用可能にする。)

メンバーの招待方法で、「メンバーの招待を管理者のみに認める」を選択した場合、管理者画面の「メンバーの招待」画面へのアクセス権を持つメンバーのみがリンク /QR コードによる招待をすることができます。

自動承認を有効にすると、現在の承認待ちメンバーおよび今後招待されるメンバーはすべてサービスを利用可能となり、メンバー数としてカウントされます。有償プランの場合は利用料金、またはライセンス数の対象となりますのでご注意ください。

5.3.2.2. メンバーの招待の設計

誰でもメンバーを招待できると、不正なメンバーの追加が容易になるリスクがあります。お客様のセキュリティポリシーに従い、また LINE WORKS のメンバー規模に応じて決定します。

5.3.2.3. メンバーの招待の設定

設定は、管理者画面の「メンバー」>「メンバーの招待」から行います。設定の詳細については、管理者画面利用ガイドの**「メンバーの招待」**をご参照ください。

5.3.3. メンバー：組織の設計

LINE WORKS を利用する企業などの内部組織が保有する情報資産や業務上の秘密情報などを保護するために、コミュニケーションの範囲となる「組織」の設計を行います。

注釈　組織が存在しない小規模な団体や、組織や社内外を横断してメンバーが集まるプロジェクトについては「グループ」を利用します。

5.3.3.1. 組織の機能

LINE WORKS では「組織」を作成することで、企業内部の各組織専用のトークルームを利用することができるようになります。各組織のトークルームでは、LINE WORKS のグループウェア機能である「ノート」「予定」「タスク」「フォルダ」を活用して、組織のメンバー間で情報共有をすることもできます。
組織を作成する場合、以下の情報を登録します。

組織の基本情報

- 組織名 (必須)
- 説明
- ID (必須)

トークルーム機能

- トーク (トークを無効にした場合、以下のグループウェア機能は使用できません。)
- ノート
- 予定
- タスク
- フォルダ

高度な設定

組織長にトークルーム機能の権限を付与

有効にした場合、組織長が LINE WORKS のグループウェア機能 (トーク / ノート / 予定 / タスク / フォルダ) の利用の有無を設定できます。
また、組織長は以下の管理をすることができます。

- 組織ノートのコメント設定
- 組織ノートのカテゴリー管理
- フォルダの使用容量確認

- フォルダのゴミ箱容量確認
- トークファイルの自動保存設定
- リンク共有の利用設定

メンバー全員にサービス通知へのお知らせを送信

有効にした場合、組織の設定変更を行った時などに、メンバー全員にサービス通知で通知されます。

組織公開

有効にした場合、組織一覧、組織検索、サジェストに組織が表示されます。

5.3.3.2. 組織の設計

企業や組織において、営業部や経理部などの複数の組織が存在する場合、LINE WORKS 内に自社組織にあわせた組織を作成し、メンバーを所属させて運用します。トークルームの範囲が広い方がコミュニケーションの範囲が拡がる一方で、本来共有すべきではないメンバーに対する情報共有が行われ、それが情報漏えいに繋がる危険性もあります。重要なことは、適切な範囲で適切なコミュニケーションを行うことです。「組織」の設計においては、お客様の現実の組織において望ましいチームコミュニケーションを LINE WORKS 上でどう実現するか、という視点が重要です。

「組織長にトークルーム機能の権限を付与」については、LINE WORKS のグループウェア機能の使用の有無について各組織の組織長の裁量に委ね、組織内部での運用を委任する場合は有効にします。

「組織公開」については、外部のユーザー (LINE ユーザー / 外部の LINE WORKS のユーザー) との交流が多い場合に、組織構造について外部に知られたくない場合は無効にすることを検討します。

5.3.3.3. 組織の設定

設定は、管理者画面の「メンバー」>「組織」から行います。設定の詳細については、管理者画面利用ガイドの**「組織の追加」**をご参照ください。

5.3.4. メンバー：グループの設計

組織が存在しない小規模な団体や、組織や社内外を横断してメンバーが集まるプロジェクトについては、LINE WORKS の「グループ」を利用してコミュニケーションを行います。

5.3.4.1. グループの機能

LINE WORKS では「グループ」を作成することで、グループ専用のトークルームを利用することができるようになります。

グループには以下の 2 つのタイプがあります。

- (内部) グループ : 社内のメンバーのみで構成されたグループです。
- 外部ユーザーとのグループ: 外部の LINE WORKS ユーザーと協業するための非公開グループです。(LINE ユー

ザーを含めることはできません。)

各グループのトークルームでは、LINE WORKS のグループウェア機能である「ノート」「予定」「タスク」「フォルダ」を活用して、グループのメンバー間で情報共有をすることもできます。
グループを作成する場合、以下の情報を登録します。

グループの基本情報

- グループ名 (必須)
- 説明

トークルーム機能

- トーク (トークを無効にした場合、以下のグループウェア機能は使用できません。)
- ノート
- 予定
- タスク
- フォルダ

高度な設定

グループマスターにトークルーム機能の権限を付与

有効にした場合、グループマスターが LINE WORKS のグループウェア機能 (トーク / ノート / 予定 / タスク / フォルダ) の利用の有無を設定できます。
また、グループマスターは以下の管理をすることができます。

- グループノートのコメント設定
- グループノートのカテゴリー管理
- フォルダの使用容量確認
- フォルダのゴミ箱容量確認
- トークファイルの自動保存設定
- リンク共有の利用設定

メンバー全員にサービス通知へのお知らせを送信

有効にした場合、グループの設定変更を行った時などに、メンバー全員にサービス通知で通知されます。

グループ公開

有効にした場合、グループ一覧、グループ検索、サジェストにグループが表示されます。

5.3.4.2. グループの設計

企業などにおいて、組織が存在しない小規模な団体や、組織や社内外を横断してメンバーが集まるプロジェクトについ

ては、LINE WORKS 内に柔軟にグループを作成し、メンバーを所属させて運用します。トークルームの範囲が広い方がコミュニケーションの範囲が拡がる一方で、本来共有すべきではないメンバーに対する情報共有が行われ、それが情報漏えいに繋がる危険性がることは、組織もグループも変わりません。重要なことは、適切な範囲で適切なコミュニケーションを行うことです。「グループ」の設計においては、お客様の内部組織とは異なるコミュニケーション、あるいは横串組織のコミュニケーションやお客様の顧客とのコミュニケーションを LINE WORKS 上でどう実現するか、という視点が重要です。

「グループマスターにトークルーム機能の権限を付与」については、LINE WORKS のグループウェア機能の使用の有無について各グループのグループマスターの裁量に委ね、グループ内部での運用を委任する場合は有効にします。

5.3.4.3. グループの設定

設定は、管理者画面の「メンバー」>「グループ」から行います。設定の詳細については、管理者画面利用ガイドの**「グループを作成」**をご参照ください。

5.3.5. メンバー：役職 / 職級 / 利用権限タイプ

LINE WORKS では「利用権限タイプ」を活用することで「ロールベースのアクセス管理」を行うことができます。ロールベースのアクセス管理とは、役割に応じて権限の組合せを設計し、各個人にはそれぞれの役割に応じた権限の組合せを付与するアクセス管理の方法です。

5.3.5.1. 利用権限タイプの機能

LINE WORKS では、「権限テンプレート」により、メンバーが利用できるサービスの権限や機能の組み合わせを定義することができます。この「権限テンプレート」を、メンバー個人に直接割り当てることもできますが、メンバーの役割ごとに定義した「利用権限タイプ」を活用することで、同一の役割のメンバーに対して同じ権限を付与することが容易になります。また、メンバーの役割が変わったときでも、メンバーに割り当てる「利用権限タイプ」を切り替えることで適切な権限への変更をすることができます。

5.3.5.2. 利用権限タイプの設計

LINE WORKS の利用において、LINE WORKS 上に保有している情報資産や個人情報を保護するためには、各メンバーの雇用形態、職位、所属する部署やプロジェクトにおける役割などにより、LINE WORKS 上で利用するサービスや必要な権限のパターンを洗い出します。洗い出したパターン毎に「利用権限タイプ」を作成し、それぞれの「利用権限タイプ」に必要な「権限テンプレート」を作成します。

権限テンプレートの詳細については、本章の「セキュリティ：サービス利用設定」をご参照ください。

5.3.5.3. 利用権限タイプの設定

設定は、管理者画面の「メンバー」>「役職 / 職級 / 利用権限」>「利用権限タイプ」から行います。設定の詳細については、管理者画面利用ガイドの**「役職、職級、利用権限タイプの管理」**の「利用権限タイプ」をご参照ください。

5.3.6. セキュリティ：管理者権限

LINE WORKS の全ての機能を操作できる管理者画面を適切に保護するために、「管理者権限」に関する設計・設定を行います。

5.3.6.1. 管理者権限の機能

LINE WORKS テナントの開設時に、あらかじめ「最高管理者」「副管理者」「運用担当者」の 3 種類の管理者権限が用意されています。

最高管理者

管理者画面の全メニューにアクセスできます。LINE WORKS アカウントを開設したメンバーは最高管理者になります。最高管理者は 1 人しか設定できません。他のメンバーに管理者権限を委任することができます。

副管理者

「LINE WORKS の解約」メニュー以外の全てのメニューにアクセスできます。副管理者は複数のメンバーを指定することができます。

運用担当者

基本設定 / メンバー / サービス / アプリのメニューにアクセスできます。運用担当者は複数のメンバーを指定することができます。

既存の管理者権限設定がご利用の実情に合わない場合は、独自の管理者権限を作成することができます。

注釈

「セキュリティ」メニューの「管理者権限」サブメニューは、最高管理者・副管理者のみアクセス可能です。(独自に作成した管理者権限でアクセスすることはできません。)

5.3.6.2. 管理者権限の設計

管理者権限は、LINE WORKS の利用において非常に強力であるため、セキュリティの観点から、どのような権限をどのメンバーに付与するのかを慎重に検討する必要があります。

LINE WORKS では、管理者権限について次の 3 ステップでの設計を推奨しています。

Step1: LINE WORKS 提供の管理者での運用の検討

LINE WORKS では、あらかじめ用意している「最高管理者」「副管理者」「運用担当者」の 3 種類の管理者権限での運用を推奨しています。この 3 種類の管理者権限により管理目的を達成できる場合は Step2 に進みます。達成が難しい場合は Step3 に進みます。

Step2: 各管理者の選定

「最高管理者」「副管理者」「運用担当者」それぞれの管理者権限をどのメンバーに付与するかを決定します。

Step3: 管理者権限のカスタマイズと各管理者の選定

「最高管理者」「副管理者」「運用担当者」の 3 種類の管理者権限で管理目的を十分に達成できない場合、どのように管理者権限をカスタマイズし、それぞれの管理者権限をどのメンバーに付与するかを決定します。

管理者権限のカスタマイズにおいては、以下のセキュリティの観点で設計を行います。

「基本設定」へのアクセス権限

管理者画面の「基本設定」メニューの「会社情報」サブメニューにアクセス権限がある場合、ワークスグループ名を変更することができます。

有償プランをご契約の場合、ワークスグループ名として独自のドメイン名をご利用いただくことができます。ワークスグループ名 (ドメイン名) を変更した場合、全メンバーが全サービスからログアウトされ、再ログインは変更後のワークグループ名でのみ可能となります。また、24 時間は再変更ができません。LINE WORKS 利用上の影響が非常に大きい操作ができる権限であるため、慎重に付与する必要があります。

「メンバー」へのアクセス権限

管理者画面の「メンバー」の各メニューにアクセス権限がある場合、個別のメンバーの登録、管理、削除をすることができます。非常に強い権限であるため、慎重に付与する必要があります。

「メンバーの招待」サブメニューにアクセス権限がある場合、メンバーの招待に関する制限を変更することができます。管理者が意図しない変更が行われた場合、不適切なメンバーの招待・自動登録が行われてしまうおそれがあります。

「サービス」へのアクセス権限

管理者画面の「サービス」の各メニューにアクセス権限がある場合、そのサービスについて管理者と同等の操作を行うことができます。その権限を付与する場合は、その用途や目的を精査し、慎重に検討する必要があります。以下のサービスの管理権限は、情報セキュリティやプライバシーに影響のある設定変更が可能なため、特に慎重に付与する必要があります。

- トーク
- アドレス帳

「セキュリティ」へのアクセス権限

管理者画面の「セキュリティ」の各メニューにアクセス権限がある場合、LINE WORKS の各セキュリティ機能について管理者と同等の操作を行うことができます。その権限を付与する場合は、その用途や目的を精査し、慎重に検討する必要があります。以下のセキュリティ機能の管理権限は、情報セキュリティやプライバシーに影響の大きい設定変更が可能なため、特に慎重に付与する必要があります。

- アカウント管理

- モバイル管理
- ネットワーク管理
- ファイル管理
- サービス利用設定
- 外部ユーザーとのトーク権限

「監査」へのアクセス権限

管理者画面の「監査」の各メニューにアクセス権限がある場合、LINE WORKS の各サービスの利用履歴について管理者と同等のアクセスを行うことができます。以下の監査機能の権限は、情報セキュリティやプライバシーに影響のある情報へのアクセスや持ち出しが可能となるため、特に慎重に付与する必要があります。

- トーク
- ログダウンロード

「モニタリング」へのアクセス権限

管理者画面の「モニタリング」の各メニューにアクセス権限がある場合、LINE WORKS の各モニタリング機能について管理者と同等の操作を行うことができます。モニタリング機能への権限を有する場合、悪意ある操作を行う前に通知を変更・削除することで、その発覚を遅延させることが可能となるため、モニタリングに関する権限を付与するときは、その用途や目的を精査し、慎重に検討する必要があります。

5.3.6.3. 管理者権限の設定

設計に従って、管理者権限の設定を行います。

設定は、管理者画面の「セキュリティ」>「管理者権限」から行います。設定の詳細については、管理者画面利用ガイドの**「管理者権限の管理」**をご参照ください。

5.3.7. セキュリティ：アカウント管理

メンバーのアカウントを安全に保護するために、「アカウント管理」に関する設計・設計を行います。

5.3.7.1. アカウント管理の機能

LINE WORKS のアカウント管理では、以下の機能について管理することができます。

- パスワードポリシー
- ログインポリシー
- ログイン方法

パスワードポリシーの機能

LINE WORKS のパスワードポリシーでは、以下のポリシーを指定することができます。

パスワードの形式

「半角英数字」もしくは「半角英数字と特殊文字」の使用を必須とします。

パスワードの長さ
最小 (8～20) 文字数を指定します。(最大は 20 文字で固定)

パスワードの有効期限
なし /30 日 /60 日 /90 日 /180 日 /360 日から選択します。

パスワードの再使用禁止
なし /1～5 世代から選択します。

ログイン失敗時のアカウント一時停止
連続してログインに失敗した場合に、アカウントを一時停止することができます。アカウントが一時停止となるまでのログイン連続失敗回数について、3～10 回のうちから選択します。一時停止したアカウントを再度使用するには管理者による一時停止解除が必要となります。

ログインポリシーの機能
LINE WORKS のログインでは、以下のポリシーを指定することができます。

2 段階認証 (2-step verification)
ログイン時に、LINE WORKS ID とパスワードによる認証に加え、登録済みの携帯番号または個人メールアドレスに送信された認証番号での認証を行います。
「すべてのメンバーに必須とする」か「メンバーが個別に選択する」のどちらかを選択します。
信頼済みのモバイル端末に対して 2 段階認証をスキップする設定をすることもできます。
2 段階認証は、外部のクライアント (IMAP、SMTP、POP3 など) を介したログインには適用されません。

PC 版アプリ /Drive エクスプローラーのログイン維持
各メンバーが PC 版アプリ /Drive エクスプローラーの「環境設定」にある「基本設定」または「ログイン設定」から、自動ログイン機能を設定することを許可することができます。

無操作によるログアウト設定
一定時間メンバーによる操作がない場合に、サービスから自動的にログアウトするよう設定できます。

PC ウェブブラウザ / モバイルブラウザ
制限なし /30 分 /1 時間 /2 時間 /4 時間 /6 時間 /12 時間 /24 時間 /7 日 /14 日 /30 日から選択します。

モバイル版アプリ

30 日 /180 日 /1 年から選択します。

ログアウト後にサービスを利用するためには、再ログインが必要となります。

ログイン方法の機能

LINE WORKS のログインでは、LINE WORKS ID とパスワードの組み合わせ以外に、以下の認証方法を利用することができます。

携帯番号でログイン

LINE WORKS ID の代わりに携帯番号を入力して 1 回限りのログイン認証番号を受け取り、ログインします。

LINE でログイン

各メンバーが自身の個人 LINE アカウントを LINE WORKS へのログイン方法として利用します。

モバイル端末の画面ロック解除でログイン (FIDO 認証)

モバイル端末を信頼できるモバイル端末として登録し、モバイル端末の生体認証や画面ロック解除を使ってログインします。PC からのログインにも使用することができ、より安全なログインをすることができます。

5.3.7.2. アカウント管理の設計

パスワードポリシーの設計

パスワードポリシーについては、以下の観点で設計を行います。

パスワードの形式、長さ、有効期限、再利用禁止

メンバーのパスワードの強度を確保するため、お客様のパスワードポリシーに適した設計を行います。

ログイン失敗時のアカウント一時停止

不正ログインを防ぐために、メンバーアカウントが一時停止となるためのログイン連続失敗回数を決定します。回数が少ないほど保護強度は高くなりますが、一時停止解除の頻度が高くなるため、管理者の業務負担が重くなる可能性があります。

ログインポリシーの設計

ログインポリシーについては、以下の観点で設計を行います。

2 段階認証 (2-step verification)

不正ログインを防止するために、お客様のセキュリティポリシーに従い、2 段階認証の使用レベル (必須 / 選択) を決定します。

信頼済みのモバイル端末では 2 段階認証をスキップ

ログインの簡略化のための機能であるため、セキュリティ強度とのバランスを考慮して、有効化 / 無効化を決定します。

PC 版アプリ /Drive エクスプローラーのログイン維持

ログインの簡略化のための機能であるため、セキュリティ強度とのバランスを考慮して、有効化 / 無効化を決定します。

無操作によるログアウト設定

画面ロックをせず離席するような状況において自動ログアウトすることにより、のぞき見や不正アクセスを防止することができるため、ソーシャルエンジニアリング対策が必要かどうかにより設定値を決定します。

ログイン方法の設計

ログイン方法については、以下の観点で設計を行います。

携帯番号でログイン

社用携帯電話の利用状況や、お客様のセキュリティポリシーにおける個人所有携帯電話の業務利用の可否に基づいて、携帯番号によるログインの可否を決定します。

LINE でログイン

お客様のセキュリティポリシーにおける個人 LINE アカウントの業務利用の可否に基づいて、LINE によるログインの可否を決定します。

モバイル端末の画面ロック解除でログイン (FIDO 認証)

モバイル端末の生体認証をログインに使用することで、セキュリティ強度は向上します。社用モバイル端末の利用状況や、お客様のセキュリティポリシーにおける個人所有モバイル端末の業務利用の可否、メンバーの IT リテラシーに応じて、モバイル端末の画面ロック解除によるログインの可否を決定します。

5.3.7.3. アカウント管理の設定

設計に従って、アカウント管理の設定を行います。

設定は、管理者画面の「セキュリティ」>「アカウント管理」から行います。設定の詳細については、管理者画面利用ガイドの**「アカウント管理」**をご参照ください。

5.3.8. セキュリティ : サービス利用設定

メンバーや利用権限タイプによって利用できる LINE WORKS の機能を制限するために、「サービス利用設定」に関する設計・設定を行います。

LINE WORKS の各サービスの利用可否は、権限テンプレートを利用して設定します。

5.3.8.1. 権限テンプレートの機能

LINE WORKS の権限テンプレートでは、LINE WORKS に対する権限について、以下の設定を行うことができます。

利用サービスの設定

権限テンプレートが適用されるメンバーによる各サービスへのアクセスの可否を設定します。

掲示板

- モバイルアプリによるアクセスの可否
- ブラウザによるアクセスの可否
- モバイル版アプリからファイルのダウンロードの制限

トーク

- モバイルアプリによるアクセスの可否

  注釈

  モバイルアプリによるサービス利用が有効な場合、モバイルアプリからトークへのアクセスを拒否することはできません。
- ブラウザによるアクセスの可否
- PC アプリによるアクセスの可否
- モバイル版アプリからファイルのダウンロードの制限

カレンダー

- モバイルアプリによるアクセスの可否
- ブラウザによるアクセスの可否
- モバイル版アプリからファイルのダウンロードの制限

アドレス帳

- モバイル版アプリからファイルのダウンロードの制限

Drive

- モバイルアプリによるアクセスの可否
- ブラウザによるアクセスの可否
- PC アプリによるアクセスの可否
- モバイル版アプリからファイルのダウンロードの制限 (トークルームのフォルダ)

タスク

- モバイルアプリによるアクセスの可否
- ブラウザによるアクセスの可否

アンケート

- モバイルアプリ / ブラウザ /PC アプリによるアクセスの可否 (一括設定)
- モバイル版アプリからファイルのダウンロードの制限

利用権限タイプ

権限テンプレートが適用される利用権限タイプを指定します。一つの利用権限タイプには、一つの権限テンプレートのみ割り当てることができます。

メンバー

権限テンプレートが適用されるメンバーを個別に指定します。

5.3.8.2. 権限テンプレートの設計

権限テンプレートについては、以下の観点で設計を行います。

独自の権限テンプレートの検討

初期状態では、すべてのメンバーに「基本設定」(全てのサービス利用を許可) の権限テンプレートが適用されます。基本設定を異なる権限設定が必要な場合は、新規に権限テンプレートを作成します。

利用サービスの設定

情報漏えいなどのリスクを低減させるために、お客様のセキュリティポリシーに従って、各メンバーの雇用形態、職位、所属する部署やプロジェクトなどに応じて権限テンプレートを設計します。

例えば、アルバイト用の権限テンプレートでは、会社の機密ファイルがアップロードされる共有ドライブを使用できないようにし、モバイル版アプリでのサービス利用は認めずパソコンだけでアクセスできるようにするなどの設計を行います。これにより、アルバイトのメンバーが LINE WORKS の認められた機能をオフィス内だけで利用できるようにすることができます。

利用権限タイプ

職位や職種が同一の複数のメンバーに対して共通の権限を付与する場合は、そのメンバーに同一の利用権限タイプを設定し、権限テンプレートをその利用権限タイプに付与するように設計します。

メンバー

個別のメンバーに特定の権限を付与する場合は、そのメンバーに権限テンプレートを直接付与するように設計します。

5.3.8.3. 権限テンプレートの設定

設計に従って、権限テンプレートの設定を行います。

設定は、管理者画面の「セキュリティ」>「サービス利用設定」から行います。設定の詳細については、管理者画面利

用ガイドの「サービス利用設定」をご参照ください。

5.4. 通信に関する設計・設定

通信への脅威に対応するために、ネットワークの設計・設定を行います。

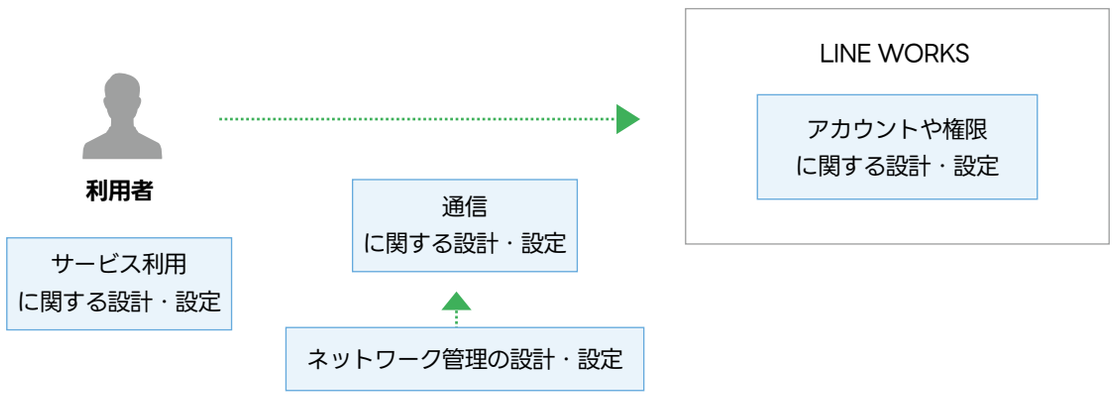


図 . 通信に関する設計・設定

5.4.1. セキュリティ：ネットワーク管理

LINE WORKS 上の情報を安全に保護するために、「ネットワーク管理」に関する設計・設定を行います。LINE WORKS のネットワーク管理では、アクセス IP 制限について管理することができます。

5.4.1.1. アクセス IP 制限の機能

LINE WORKS では、メンバーのアクセス元の IP アドレスや国を制限することができます。

指定した IP アドレスからのみアクセスを許可

指定した IP アドレスからのみアクセスを許可する場合、ブラウザ版、PC 版アプリ、Drive エクスプローラーによるアクセスは、指定した IP アドレスからのみアクセスすることができます。ただし、モバイルアプリによるアクセスについては、その特性上、IP アドレス制限の対象とはなりません。また、「例外管理」にメンバーを登録することで、そのメンバーはすべての IP アドレスからサービスにアクセスすることができるようになります。

許可した国からのみアクセスを許可

すべての IP アドレスからのアクセスを許可する場合において、サービスの利用を許可する国を指定することで、それ以外の国からのアクセスを制限することができます。アクセスを許可した国以外からログインする場合には、携帯番号または個人メールアドレスによる本人確認の認証が必要となります。

	サービス利用国制限	アクセス IP 制限
ブラウザ版	○	○
モバイル版アプリ	○	×

PC 版アプリ	○	○
Drive エクスプローラー	○	○

最高管理者によるアクセスについては、アクセス IP 制限の設定に関係なく、すべての IP アドレスからサービスにアクセスすることができます。

5.4.1.2. アクセス IP 制限の設計

アクセス IP 制限については、以下の選択肢を検討して設計します。

指定した IP からのみアクセスを許可

LINE WORKS に保有する情報資産や個人情報を保護するために、使用環境を特定の場所に制限している場合や、公共の場での PC 利用を禁止している場合は、使用環境の IP アドレスをリストアップして管理します。

すべての IP からのアクセスを許可

インターネット上のどこからでもアクセスできるようにする場合は、すべての IP からのアクセスを許可します。

LINE WORKS は日本国内での利用を前提としてサービスを提供しており、海外からの利用についてはベストエフォートでの提供となっています。海外からのご利用の予定が無い場合は「サービス利用国制限」を有効にし、「サービス利用国制限の例外管理リスト」に「日本」およびメンバーが訪問する可能性がある国を登録することを推奨いたします。これにより、許可した国以外の海外からの不正アクセスなどの攻撃を遮断することができます。

5.4.1.3. アクセス IP 制限の設定

設計に従って、アクセス IP 制限の設定を行います。

設定は、管理者画面の「セキュリティ」>「ネットワーク管理」から行います。設定の詳細については、管理者画面利用ガイドの**「ネットワーク管理」**をご参照ください。

5.5. サービス利用に関する設計・設定

利用者のサービス利用における脅威に対応するために、セキュリティ、サービスの設計・設定を行います。

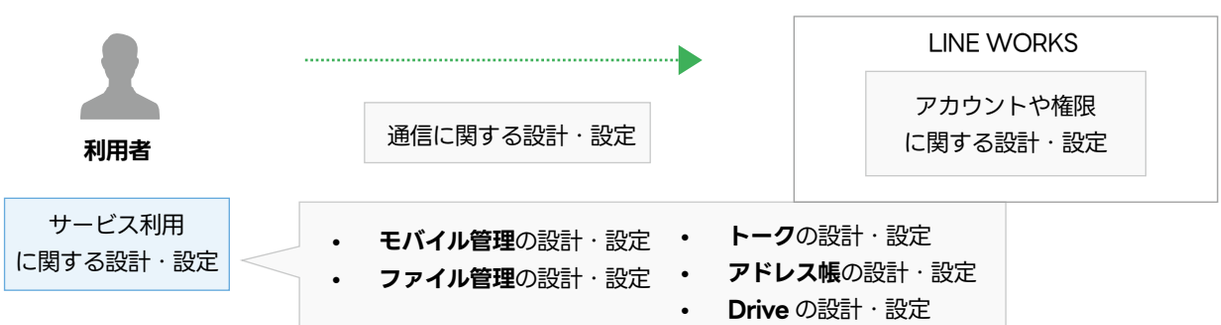


図 . サービス利用に関する設計・設定

5.5.1. セキュリティ：モバイル管理

メンバーが利用するモバイル版アプリのセキュリティを確保するために、「モバイル管理」に関する設計・設定を行います。

5.5.1.1. モバイル管理の機能

LINE WORKS の「モバイル管理」では、以下の機能について管理することができます。

- LINE WORKS モバイル版アプリの機能制限
- モバイルデバイス管理 (MDM)

モバイル版アプリ機能制限の機能

LINE WORKS モバイル版アプリでは、以下の機能制限を行うことができます。これらの機能制限により、モバイル端末の紛失時でも不正ログインによる情報漏えいなどを抑制することが可能となります。

データの保持・閲覧期間

モバイル版アプリから各サービス内のデータを閲覧できる期間を指定できます。設定した期間を過ぎたファイルは自動的に削除されます。

「制限なし / 直近 3 日以内のデータのみ閲覧可能 / 直近 7 日以内のデータのみ閲覧可能 / 直近 30 日以内のデータのみ閲覧可能」から選択します。

画像 / テキスト情報のコピー

モバイル版アプリ内の画像 / テキストの、クリップボードへのコピーを禁止することができます。禁止した場合でも、メール作成 / 投稿など、モバイル版アプリ内で直接入力する範囲と OS からデフォルトで提供するビュアーでは制限されません。

モバイルデバイス管理 (MDM) の機能

デバイスの紛失や盗難に備えるために、LINE WORKS においてモバイルデバイス管理 (MDM) を利用することができます。

モバイルデバイス管理 (MDM)

LINE WORKS が提供する LINE WORKS MDM をご利用いただくと、管理者は遠隔でデバイスにインストールされた LINE WORKS モバイル版アプリのデータを削除したり、デバイスを初期化したりすることができます。
LINE WORKS MDM を利用するには、事前にメンバーが MDM の利用に必要なファイルを iOS または Android 端末にインストールする必要があります。

LINE WORKS は、サードパーティの MDM 製品とも連携が可能です。

5.5.1.2. モバイル管理の設計

機能制限の設計

モバイル端末からの情報流出を防ぐために、お客様のセキュリティポリシーに従って、データの保持・閲覧期間の制限、画像 / テキスト情報のコピーの制限の設計をします。

モバイル端末の紛失や盗難を考慮し、MDM の導入の可否を決定します。MDM を導入する場合は、LINE WORKS MDM を採用するのか、サードパーティの MDM 製品を選定するのかを決定します。

注釈

LINE WORKS MDM 以外の MDM 製品については LINE WORKS サポートの対象外となります。サードパーティの MDM 製品に関するご質問は、製造元へお問い合わせください

5.5.1.3. モバイル管理の設定

設計に従って、モバイル管理の設定を行います。

設定は、管理者画面の「セキュリティ」>「モバイル管理」から行います。設定の詳細については、管理者画面利用ガイドの**「モバイル管理」**をご参照ください。

5.5.2. セキュリティ：ファイル管理

LINE WORKS サービスにおけるファイルの利用を適切に保護するために、「ファイル管理」に関する設計・設定を行います。

5.5.2.1. ファイル管理の機能

LINE WORKS の「ファイル管理」では、以下の機能について管理することができます。

- モバイル版アプリにおけるファイル利用制限
- ファイル形式での制限
- 外部ユーザーとのトークルームでファイル送信・添付
- ファイルのダウンロードログ

モバイル版アプリにおけるファイル利用制限の機能

LINE WORKS では、モバイル版アプリにおけるファイル利用について、以下の制限をすることができます。

モバイル版アプリからのファイルダウンロードを制限

モバイル版アプリでファイルをダウンロードできないように、サービス別に設定できます。文書ビューアでのファイル閲覧は可能です。

モバイル版アプリからのファイルアップロードを制限

モバイル版アプリからファイルをアップロード (送信 / 添付を含む) できないように設定できます。

ウォーターマーク

モバイル版アプリで表示する画像 / 動画 / 文書上に、ウォーターマーク (操作しているメンバーを特定するための文字列) を重ねて表示します。

ファイル形式での制限の機能

LINE WORKS では、拡張子を指定して LINE WORKS サービス上でのファイル送受信を制限することができます。

制限するサービス

掲示板 / トーク / カレンダー (トークルームの予定)/ アドレス帳 /Drive (トークルームのフォルダ)/ タスク (トークルームのタスク)/ アンケートについて、ファイル送受信を制限することができます。
「制限するサービス」で Drive を選択していない場合でも、Drive と連携しているサービスのいずれかにファイル制限が適用されている場合は、Drive からのファイル添付や Drive へのファイル保存などが制限されます。

ファイル形式の制限によるサービスへの影響については、管理者画面利用ガイドの「ファイル管理」の「ファイル形式で制限する」をご参照ください。

制限する拡張子

LINE WORKS サービス上でファイル送受信を制限するファイルの拡張子を指定できます。制限するファイル形式の拡張子は、200 件まで指定することができます。

外部ユーザーとのトークルームにおけるファイル送信・添付の機能

LINE WORKS では、外部ユーザーとのトークルームにおけるファイル送信可否について、以下の制限をすることができます。

LINE ユーザーとのトークルーム

LINE ユーザーとのトークルームにおけるファイル送信の可否を選択します。

外部 LINE WORKS ユーザーとのトークルーム

外部 LINE WORKS ユーザーとのトークルームにおけるファイル送信可否を選択します。

ファイルのダウンロードログの機能

LINE WORKS では、メンバーがファイルをダウンロード・閲覧した記録を保存・確認することができます。

監査でファイルのダウンロードログを保存

メンバーがファイルをダウンロード・閲覧した記録の保存を有効化できます。各メンバーによるファイルのダウンロード・閲覧履歴は、管理者画面「監査」内にある「ファイル」から参照することができます。

5.5.2.2. ファイル管理の設計

モバイル版アプリにおけるファイル利用制限の設計

モバイル版アプリへの制限については、以下の観点で設計を行います。

モバイル版アプリからのファイルダウンロードを制限

モバイル端末からの情報の流出や持ち出しのリスクを軽減させるために、お客様のセキュリティポリシーに従って、ファイルダウンロードの制限を設計します。

モバイル版アプリからのファイルアップロードを制限

モバイル端末からの不正なファイルのアップロードや悪性のファイルの持ち込みリスクを軽減させるために、お客様のセキュリティポリシーに従って、ファイルアップロードの制限を設計します。

ウォーターマーク

モバイル版アプリで表示する画像や動画、文書の流出を抑止するために、スクリーンショット機能を使用して撮影した画面に操作を行ったメンバーの情報を表示するかどうかを決定します。

ファイル形式での制限の設計

ファイル形式での制限については、以下の観点で設計を行います。

制限するサービス

お客様の想定される利用環境から、不正なファイルが LINE WORKS に保存されるリスクを検討し、ファイルの送受信を制限するサービスを決定します。

制限する拡張子

LINE WORKS サービスでファイルを使用する場合、自動的にマルウェアのチェックが行われます。しかし、日々新たに現れるマルウェア / ウィルスによる被害を防止し、意図しない形式のファイルのやり取りを抑制するためには、LINE WORKS 上で利用するファイル形式を制限することが非常に有用です。お客様のセキュリティポリシーに従って、送受信を制限するファイルの拡張子をリストアップします。

外部ユーザーとのトークルームにおけるファイル送信・添付の設計

外部ユーザーとのトークルームにおけるファイル送信・添付については、社外のユーザーとのトークによる社内情報の社外への流出リスクを軽減するために、お客様のセキュリティポリシーに従って、トークルームにおけるファイルの送信・添付の可否を決定します。

この許可は、管理者画面の「サービス」>「トーク」>「外部ユーザーとのトーク」の「LINE 連携」および「外部 LINE WORKS 連携」の「ファイル送信・添付」の設定で変更することもできます。

ファイルのダウンロードログの設計

ファイルのダウンロードログ機能は、デフォルトで無効となっています。メンバーがファイルをダウンロード・閲覧履歴を追跡するため、お客様のセキュリティポリシーに従って、ログ保存の可否を決定します。

5.5.2.3. ファイル管理の設定

設計に従って、ファイル管理の設定を行います。

設定は、管理者画面の「セキュリティ > ファイル管理」から行います。設定の詳細については、管理者画面利用ガイドの**「ファイル管理」**をご参照ください。

5.5.3. サービス：トーク

LINE WORKS のトークの設計と設定を行います。

5.5.3.1. トークの機能

LINE WORKS の「トーク」については、以下の機能を管理することができます。

- トークの一般機能
- 外部ユーザーとのトーク
- トークのモニタリング

トークの一般機能

LINE WORKS のトークでは、以下の設定をすることができます。

トーク / ファイル管理

トーク保存 / 検索期間

トークを確認および検索できる期間を指定します。1 か月 /3 か月 /6 か月 /1 年 /2 年 /3 年のいずれかを指定します。設定した期間を過ぎたトークは削除され、確認および検索ができません。

写真 / ファイルの保存期間

トークで送受信されるファイルや写真を閲覧またはダウンロードできる期間を指定します。7 日 /15 日 /30 日 /3 か月 /6 か月 /1 年 /2 年 /3 年のいずれかを指定します。「トークの保存 / 検索期間」で設定した期間を超えて利用することはできません。

添付ファイル 1 個あたりの上限

トークで送信するファイルの 1 件あたりのサイズ上限を指定します。

1MB/5MB/10MB/20MB/50MB/100MB/500MB/1GB/2GB のいずれかを指定します。設定サイズ以上のファイルは送信できません。

ノート

添付できるファイル１個あたりの容量

ノートに添付できるファイル１個あたりのサイズ上限を指定します。

10MB/20MB/50MB/100MB/500MB/1GB/2GB のいずれかを指定します。

ゴミ箱の保管期間

ノートの投稿をゴミ箱に移動してから完全削除されるまでの期間を指定します。自動削除しない /30 日後にゴミ箱から完全削除 /60 日後にゴミ箱から完全削除 /90 日後にゴミ箱から完全削除、のいずれかを指定します。

外部ユーザーとのトークの機能

LINE WORKS のトークを利用することで、LINE もしくは外部の LINE WORKS のユーザーとコミュニケーションを行うことができます。これらの外部ユーザーとのトーク利用について、以下の設定をすることができます。

連携設定

外部ユーザーとのトークを利用するかどうかを指定します。

連携機能の利用権限

外部ユーザーとのトークの利用を許可する場合に、すべてのメンバーに許可するのか、特定のメンバーのみに許可するのかを指定します。特定のメンバーに対して許可する場合は、新規登録メンバーに対してトーク利用の権限を自動的に付与することもできます。

ファイル送信・添付

外部ユーザーとのトークの利用を許可する場合に、トークルームにおける外部ユーザーとのファイル送信を利用するかどうかを指定します。

あいさつメッセージを自動送信

LINE ユーザーとのトークの利用を許可している場合、メンバーを友だち追加した LINE ユーザーに対して、自動的にあいさつメッセージを送信するように指定することができます。(外部の LINE WORKS ユーザーに対して設定することはできません。)

トークのモニタリング機能

LINE WORKS のトークにおけるセキュリティ事故を検知するために、トークに対するモニタリングのポリシーとレポートに関する設定をすることができます。

ポリシー管理

LINE WORKS のトークでは、送信されたトークを対象にポリシーを作成し、ポリシーに定義された条件に該当するトークをモニタリングすることができます。トークのモニタリングポリシーでは、「条件」と「通知」を指定します。

条件設定

トークを送信する際にモニタリングするポリシーの条件を指定します。複数の条件を指定した場合、指定した条件すべてに該当しなければ、通知は行われません。(AND 条件で動作します。)

トークのモニタリングポリシーでは、以下の条件を指定することができます。

モニタリング対象

- メンバーへの送信：社内向けに送信されるトークを対象にします。
- 外部への送信：社外向けに送信されるトークを対象にします。

送信者

モニタリングするトークの送信メンバーを指定することができます。メールアドレスは最大 50 個まで入力することができ、メーリングリストは入力できません。

受信者

モニタリングするトークの受信メンバーを指定することができます。メールアドレスは最大 50 個まで入力することができ、メーリングリストは入力できません。送信者と受信者が同じ場合、モニタリングされません。

コンテンツフィルタリング / 添付ファイル

コンテンツフィルタリング / 添付ファイルのいずれかをモニタリング条件として指定することができます。

注釈

複数のコンテンツを指定した場合、すべてのコンテンツに該当しなければ、通知は行なわれません。(AND 条件で動作します。)

コンテンツフィルタリングを指定した場合、トークの内容に指定したメッセージ内容もしくは添付ファイル名が含まれていると通知が行なわれます。
添付ファイルを指定した場合、トークにファイルが添付されていると通知が行なわれます。

Bot のトーク

ポリシーの条件に、Bot が送信するトークを含めるかどうかを指定します。

通知設定

ポリシーの条件が満たされた場合に実行される通知について指定します。

検知周期

ポリシーに設定した条件を満たしたときに、メールとトークとで通知します。通知周期は 1 時間 /6 時間のい

ずれかを選択します。

メールで通知

ポリシーに設定した条件を満たしたときに、メールで通知するかどうかを指定します。通知する場合、メールで通知を受信する管理者のメールアドレスを指定します。最大 5 個までのメールアドレスを登録することができます。

トークで通知

ポリシーに設定した条件を満たしたときに、トークで通知するかどうかを指定します。通知する場合、トークで通知を受信する管理者のメールアドレスを指定します。最大 5 個までのメールアドレスを登録することができます。

モニタリング

LINE WORKS では、トークのモニタリングポリシーで検知された内容を、指定したメールアドレスに自動送信することができます。

レポート周期

レポートを受信する周期を選択します。レポート周期は、毎日、毎週から選択できます。

受信メールアドレス

レポートの送信先となるメールアドレスを指定します。

重要

LINE WORKS サービスの管理者は、監査サービスの利用に伴い、メンバーのデータ (トーク内容など) にアクセスする場合は、法令および「LINE WORKS サービス利用規約」の定めに従い、メンバーの有効な同意を必ず得るものとします。なお、メンバーからの同意の有無に関わらず、メンバーのデータにアクセスしたことにより管理者とメンバーとの間で生じたトラブルについては、LINE WORKS 株式会社は責任を負いかねますのでご留意ください。

5.5.3.2. トークの設計

トークの一般機能の設計

トークについては、以下の観点で設計を行います。

トーク / ファイル管理

トークやトークに添付された写真やファイルは、保存期間が長い方が利便性が高くなりますが、情報漏えいのリスクも高くなります。お客様のセキュリティポリシーに従い、トークの保存 / 検索期間や、トークに添付された写真やファイルの保存期間を決定します。

ノート

ノートのゴミ箱は、保管期間が長い方が削除したノートを復元できる可能性が高いため、利便性が高くなりますが、情報漏えいのリスクも高くなります。お客様のセキュリティポリシーに従い、ノートのゴミ箱の保管期間を決定します。

外部ユーザーとのトークの設計

外部ユーザーとのトーク利用においては、以下の観点で設計を行います。

連携機能の利用権限

社外への情報流出リスクを軽減させるためには、不要なメンバーに対しては外部ユーザーとのトーク利用の権限を付与しないことが効果的です。どのような組織、役職、職級のメンバーに対して外部ユーザーとの連携する権限を付与するかについて、お客様のセキュリティポリシーに従って決定します。

新規メンバーに連携権限を自動付与

LINE WORKSに新規に登録されたメンバーに対して、連携権限を自動的に付与すべきか決定します。外部ユーザーとのトーク利用をメンバー全員に対して許可する場合は有効にします。許可されたメンバーのみに許可する場合は無効にします。

ファイル送信・添付

外部ユーザーとのトークルームにおけるファイルの送受信を許可するかどうかについて決定します。ファイル送受信の利便性と、LINE WORKS 上で取り扱う情報が漏えいした場合のリスクを評価し、お客様のセキュリティポリシーに従って決定します。

この許可は、管理者画面の「セキュリティ」>「ファイル管理」の「外部ユーザーとのトークルームでファイル送信・添付」の設定で変更することもできます。

あいさつメッセージを自動送信

メンバーを友だち追加した LINE ユーザーに対して送信する定型文を決定します。

自社の LINE WORKS メンバーと連携する LINE ユーザーに対して、事前に自社のプライバシーポリシーなどを案内する必要がある場合、その概要や参照先の URL などを最大 500 文字の範囲で記述します。

トークのモニタリングの設計

トークのポリシーについては、以下の観点で設計を行います。

条件設定

モニタリング対象

以下のいずれか、もしくは両方をモニタリング対象とすることができます。

- メンバーへの送信 : 同じ LINE WORKS(社内) 向けに送信されるトークをモニタリングの対象にします。
- 外部への送信 : LINE や外部の LINE WORKS に向けて送信されるトークをモニタリングの対象にします。

送信者、受信者

モニタリングの対象となる送信者や受信者をメールアドレスで指定することができます。それぞれ登録できるメールアドレスは最大 50 個です。メーリングリストは登録できません。

送信者と受信者の設定が同じ場合、モニタリングされません。

コンテンツフィルタリング、添付ファイル

特定のキーワードが含まれたトークをモニタリングする場合は、キーワードを指定してコンテンツフィルタリングを条件としたポリシーを作成します。

注釈

トークのコンテンツフィルタリングによる条件は、スペースを入力した場合、複数のキーワードによる AND 検索となります。「空白」や「記号（例として半角アンダーバー”_”など)」が含まれている文字列を指定している場合、設定した条件以外の結果も検知される場合があります。コンテンツフィルタリングに指定した文字列だけを完全一致で検知したい場合、「空白」や「記号」を含めないことを推奨します。

ファイルが添付されたトークをモニタリングする場合は、添付ファイルを条件としたポリシーを作成します。コンテンツフィルタリングと添付ファイルは、同時に条件として指定することはできません。

Bot のトーク

Bot が送信するトークをモニタリングでどう扱うかを指定します。

- Bot のトークを除く : Bot のトークをモニタリングの対象外とします。
- Bot のトークを含む : すべてのトークをモニタリングの対象とします。
- Bot のトークのみ選択 : Bot トークのみをモニタリングの対象とします。

通知設定

トークや添付ファイルについてモニタリングをしていることを利用者に認知してもらいたい場合は、メンバーへの通知を有効にします。一方で、通知することにより、どこまでモニタリングしているのかが判明することで、むしろセキュリティリスクが向上する可能性がある場合は、メンバーへの通知を無効にします。

トークのモニタリングについては、以下の観点で設計を行います。

レポート周期

トークポリシーレポートを受信する周期を指定します。毎日もしくは毎週から選択します。

受信メールアドレス

トークポリシーレポートを受信するメールアドレスを指定します。登録できるメールアドレスは最大 5 つです。

5.5.3.3. トークの設定

トークの設定

設計に従って、トークの設定を行います。

トークの設定は、管理者画面の「サービス」>「トーク」>「一般」から行います。設定の詳細については、管理者画面利用ガイドの**「トークの一般設定」**をご参照ください。

外部ユーザーとのトークの設定

設計に従って、外部ユーザーとのトークの設定を行います。

外部ユーザーとのトークの設定は、管理者画面の「サービス」>「トーク」>「外部ユーザーとのトーク」から行います。設定の詳細については、管理者画面利用ガイドの**「外部ユーザーとのトーク設定」**をご参照ください。

トークのモニタリングの設定

設計に従って、トークのモニタリングの設定を行います。

トークのモニタリングの設定は、管理者画面の「モニタリング」>「トーク」から行います。設定の詳細については、管理者画面利用ガイドの「モニタリング」の**「トーク」**をご参照ください。

5.5.4. アドレス帳

顧客 / 取引先に登録する外部との連絡先の会社タグ、MY タグ、公開範囲、ごみ箱の保管期間について設計します。

5.5.4.1. アドレス帳の機能

LINE WORKS の「アドレス帳」については、以下の機能を管理することができます。

- アドレス帳の一般機能
- 顧客 / 取引先の管理

アドレス帳の一般機能

LINE WORKS のアドレス帳では、以下の設定をすることができます。

顧客 / 取引先

アドレス帳に登録する顧客 / 取引先について、会社タグ、マイタグ、公開範囲、ごみ箱の保管期間を設定します。

全社共用タグの作成権限

全社共用タグの管理を誰に認めるか指定します。

- 管理者のみ作成可
- メンバーが自由に作成可

マイタグの利用を許可

有効にした場合、メンバーはアドレス帳上に個人で使うタグを作成し利用することができます。

連絡先の公開範囲の既定値

連絡先の追加時に公開範囲の既定値として表示されるメンバーの範囲を指定します。

- すべてのメンバー
- 特定のメンバー

ゴミ箱での保管期間

削除された連絡先をゴミ箱に保管する期間を設定することができます。

- 自動削除をしない /30 日後 /60 日後 /90 日後から選択します。

設定された保管期間を経過すると完全に削除されます。

グループ

アドレス帳からグループの作成を認めるかどうかについて設定します。

グループ作成権限

グループの作成を誰に認めるか指定します。

- 管理者のみ作成可
- メンバーが自由に作成可

「メンバーが自由に作成可」を選択すると、すべてのメンバーがアドレス帳から自由にグループを作成できます。

この設定は社内メンバーのみが参加するグループに適用されます。外部ユーザーとのトーク権限を持つメンバーは、外部ユーザーを含むグループを作成できます。

社内メンバー

アドレス帳に社内メンバーの個人情報を掲載するかどうかについて設定します。

個人メールアドレスの公開

組織図やアドレス帳における個人メールアドレスの表示の有無について指定します。

携帯番号の公開

組織図やアドレス帳における携帯番号の表示の有無について指定します。

兼務 / 休職の公開

組織図における兼務 / 休職のメンバー数の表示の有無について指定します。

入社日の公開

組織図やアドレス帳における入社日の表示の有無について指定します。

誕生日の公開

組織図やアドレス帳における誕生日の表示の有無について指定します。

顧客 / 取引先の管理

顧客 / 取引先は、会社のメンバーと共有・管理する連絡先をまとめておくアドレス帳です。登録された顧客 / 取引先の情報は、全社からアクセス可能になります。

LINE WORKS の業務での利用開始後、管理者は顧客 / 取引先の検索やマスターの変更、公開範囲の変更、削除などの管理を行います。

5.5.4.2. アドレス帳の設計

アドレス帳に登録する情報について、以下のポリシーを検討します。

- 全社共用タグ / マイタグの利用
- 連絡先の公開範囲の既定値
- ゴミ箱での保管期間
- アドレス帳からのグループ作成
- 社内メンバーの個人情報の掲載
- 顧客 / 取引先のマスター (主管理者) の指定ルール
- 顧客 / 取引先の削除ルール

社内メンバーの個人情報の掲載については、メンバーの個人情報の安全な管理という観点から、社内のセキュリティポリシーやプライバシーポリシーに従い決定します。
顧客 / 取引先のマスター (主管理者) の指定ルールについては、主担当者や主管部署のリーダーを指定する、などのルール決めが必要となります。
顧客 / 取引先の削除ルールについては、取引や契約の終了、一定期間取引が無い場合など、削除するための条件を決めておきます。

5.5.4.3. アドレス帳の設定

設計に従って、アドレス帳の設定を行います。

アドレス帳の設定は、管理者画面の「サービス」>「アドレス帳」>「一般」から行います。設定の詳細については、管理者画面利用ガイドの「アドレス帳の一般設定」をご参照ください。

5.5.5. サービス : Drive

Drive サービスの設計と設定を行います。

5.5.5.1. Drive の機能

LINE WORKS の「Drive」については、以下の機能を管理することができます。

- Drive の一般機能
- Drive のモニタリング

Drive の一般機能

Drive では、以下の設定をすることができます。

リンク共有機能

ファイルを共有する際に、メールへの添付やトークによる直接送信の代わりに、共有ドライブやマイドライブ、トークルームフォルダなどに保存したファイルに対してアクセス可能な URL を生成し、共有することができます。

リンク共有機能

Drive のリンク共有機能を利用するかどうかを指定します。

リンクの有効期限

リンク共有を許可した場合、アクセスできる有効期限を設定できます。制限なし / 最大 7 日 / 最大 30 日 / 最大 90 日 / 最大 180 日のいずれかを指定します。期限が終了したリンクは期限終了ページに移動し、以降利用ができません。

リンクのアクセス権限

共有ドライブ、マイドライブ、トークルームフォルダそれぞれについて、共有リンクによるアクセス権限を付与する対象を以下から一つもしくは複数指定します。

- 自社社員のみ
- リンクを知っている全員、パスワードを知っている人のみ
- ワンタイムパスワード認証でアクセス可能

ゴミ箱の保管期間

ゴミ箱の保管期間は、フォルダのゴミ箱にあるファイルを自動的に削除する時期を設定する機能です。この設定は

共有ドライブ、マイドライブ、トークルームフォルダのすべてに適用されます。

ゴミ箱の保管期間

フォルダのゴミ箱の自動削除期間を指定します。自動削除をしない /5 日後にゴミ箱から完全削除 /15 日後にゴミ箱から完全削除 /30 日後にゴミ箱から完全削除 /50 日後にゴミ箱から完全削除のいずれかを指定します。

ファイルのバージョン履歴

ファイルのバージョン履歴は、Drive 内の各ファイルを更新する度に履歴を保存する機能です。指定された拡張子のファイルは、バージョン履歴から過去の状態に復元することができます。

バージョン履歴の保存期間

ファイルを上書きする前の状態を保存する期間を指定します。削除しない /1 ヶ月 /3 ヶ月 /6 ヶ月 /12 ヶ月のいずれかを指定します。

ファイルのタイプ

バージョン履歴を利用するファイルの拡張子を指定します。

共有ドライブ

共有ドライブは社内 (同ドメイン) のメンバーが共同で利用できるドライブです。社内全体で共有する資料やコンテンツを保存し、効率的にファイルを共有することができます。

共有ドライブを作成するためには、以下の項目を指定します。

名前

共有ドライブの名前を指定します。

説明

共有ドライブの説明を指定します。

グループマスター

共有ドライブの説明を指定します。

共有範囲

共有ドライブの共有範囲を、すべてのメンバーにするのか、特定のメンバーのみにするのかを指定します。特定の利用権限タイプに対して共有ドライブへのアクセスを制限することもできます。

リンク共有の使用

共有ドライブにおいて、共有リンクを使用するかどうかを指定します。

Drive のモニタリング機能

LINE WORKS の Drive におけるセキュリティ事故を検知するために、Drive に対するモニタリングのポリシーとレポートに関する設定をすることができます。

ポリシー管理

LINE WORKS の Drive では、Drive 上での操作 (ダウンロード、アップロード、リンク共有) を対象にポリシーを作成し、ポリシーに定義された条件に該当する操作をモニタリングすることができます。Drive のモニタリングポリシーでは、「条件」「適用期間」「通知」を指定します。

条件設定

Drive を操作する際にモニタリングするポリシーの条件を指定します。
複数の条件を指定した場合、指定した条件すべてに該当しなければ、通知は行われません。(AND 条件で動作します。)

Drive のモニタリングポリシーでは、以下の条件を指定することができます。

基準 (必須)

コンテンツフィルタリング

いずれの操作をモニタリング対象とする場合でも指定することができます。ファイル名 + 内容 / ファイル名 / 内容 / 拡張子のいずれかを選択し、検知するキーワードを指定します。キーワードは、1 つのみ指定することができます。特殊文字が含まれると、フィルタリング結果に影響を与える場合があります。

- リンク共有の場合、ファイルまたはフォルダ単体のリンクを共有するときに検知されます。
- フォルダへのリンク共有の場合、フォルダ内のファイルはコンテンツフィルタリングの対象外となります。

ファイル容量

ダウンロード / リンク共有の操作をモニタリング対象とする場合に指定することができます。

- ダウンロードの場合、1 日にダウンロードしたファイルの容量が設定値以上の場合に検知します。
- リンク共有の場合、リンク共有の作成時にファイル / フォルダの容量が設定値以上の場合に検知します。

ファイル数

ダウンロードの操作をモニタリング対象とする場合に指定することができます。1 日にダウンロードしたファイルの数が設定値以上の場合に検知します。

メンバー指定

モニタリングする対象のメンバーまたは組織名を指定することができます。指定されたメンバーが、条件に該当する操作を実施した場合に検知します。

適用期間の設定

ポリシーを適用する期間を設定します。

期間

開始日と終了日を指定します。終了日として「期限なし」を指定することもできます。

タイムゾーン

タイムゾーンを指定します。

通知設定

ポリシーの条件が満たされた場合に実行される通知について指定します。

メンバーに通知

ポリシーに該当する操作を行ったメンバーに対して通知するかどうかを指定します。通知する場合、通知する内容 (メッセージ) を指定することができます。通知方法として「メール」「トーク」の一方もしくは両方を指定します。

管理者に通知

ポリシーに該当する状況が発生した場合に、管理者に対して通知するかどうかを指定します。通知する場合、最大 5 個までのメールアドレスを登録することができます。通知方法として「メール」「トーク」の一方もしくは両方を指定します。

モニタリング

LINE WORKS では、Drive のモニタリングポリシーで検知された内容を、指定したメールアドレスに自動送信することができます。

レポート周期

レポートを受信する周期を選択します。レポート周期は、毎日、毎週から選択できます。

受信メールアドレス

レポートの送信先となるメールアドレスを指定します。

5.5.5.2. Drive の設計

Drive の一般機能の設計

Drive については、以下の観点で設計を行います。

リンク共有機能、リンクのアクセス権限

リンクは、そのリンク先のファイルに対する直接のアクセス権となり、リンクの設定によっては外部への共有も可能となります。リンク共有時の情報セキュリティリスクを軽減させるため、お客様のセキュリティポリシーに従って、リンク共有機能の利用の可否、リンクの有効期限、リンクのアクセス権限について決定します。

ゴミ箱の保管期間

メンバーからデータが消えた等の問い合わせがあった場合、監査機能での調査に加え、ゴミ箱に保存されているデータから確認・復元できる場合があります。一方で、ゴミ箱内にあるデータも Drive の容量を使用する上、リスクの高い情報が長期間保持される可能性もあります。お客様のセキュリティポリシーに従って、ゴミ箱の保管期間を決定します。

共有ドライブ

全社および部署別 / プロジェクト別の共有ドライブとそのフォルダ構成を検討し、お客様のセキュリティポリシーに従って、必要となるアクセス権限を決定します。

Drive のモニタリングの設計

Drive のポリシーについては、以下の観点で設計を行います。

条件設定

ファイル数によるモニタリング

ファイル数の多いダウンロードは情報漏えいの可能性があります。この観点においてはファイル数を条件としたポリシーを作成します。

コンテンツフィルタリングによるモニタリング

特定の機密情報が含まれたファイルのダウンロード、アップロード、リンク共有をモニタリングする場合は、ファイル名あるいはファイルに含まれたキーワードを条件としたポリシーを作成します。Drive のコンテンツフィルタリングによる条件は、1 つのポリシーにつきキーワードを 1 つだけ指定することができます。

通知設定

ダウンロードやアップロードについてモニタリングをしていることを利用者に認知してもらいたい場合は、メンバーへの通知を有効にします。一方で、通知することにより、どこまでモニタリングしているのかが判明することで、むしろセキュリティリスクが向上する可能性がある場合は、メンバーへの通知を無効にします。

Drive のモニタリングについては、以下の観点で設計を行います。

レポート周期

Drive ポリシーレポートを受信する周期を指定します。毎日もしくは毎週から選択します。

受信メールアドレス

Drive ポリシーレポートを受信するメールアドレスを指定します。登録できるメールアドレスは最大 5 つです。

5.5.5.3. Drive の設定

Drive の設定

設計に従って、Drive の設定を行います。

Drive の設定は、管理者画面の「サービス」>「Drive」>「一般」から行います。設定の詳細については、管理者画面利用ガイドの「Drive の一般設定」をご参照ください。

Drive のモニタリングの設定

設計に従って、Drive のモニタリングの設定を行います。

Drive のモニタリングの設定は、管理者画面の「モニタリング」>「Drive」から行います。設定の詳細については、管理者画面利用ガイドの「モニタリング」の「Drive」をご参照ください。

6 章 LINE WORKS サービスをセキュアに運用するための管理機能

6.1. 本章の概要

本章では、LINE WORKS サービスをセキュアに運用するために必要な管理機能について解説します。
LINE WORKS サービスの管理者は、導入担当者から引き継いだ LINE WORKS サービスについて、これらの管理機能を活用して、以下の 5 つの領域について管理を行います。

1. アカウント・権限に関する管理

アカウント・権限への脅威に対応するために必要な管理を行います。

2. 通信路に関する管理

通信への脅威に対応するために必要な管理を行います。

3. ユーザーの利用に関する管理

ユーザーへの脅威に対応するために必要な管理を行います。

4. トラブルシューティング

サービスの利用においてトラブルが発生した場合に、冷静かつ迅速に対応を行います。

5. サービス契約の更新

サービス契約の更新について、必要な手続きを行います。

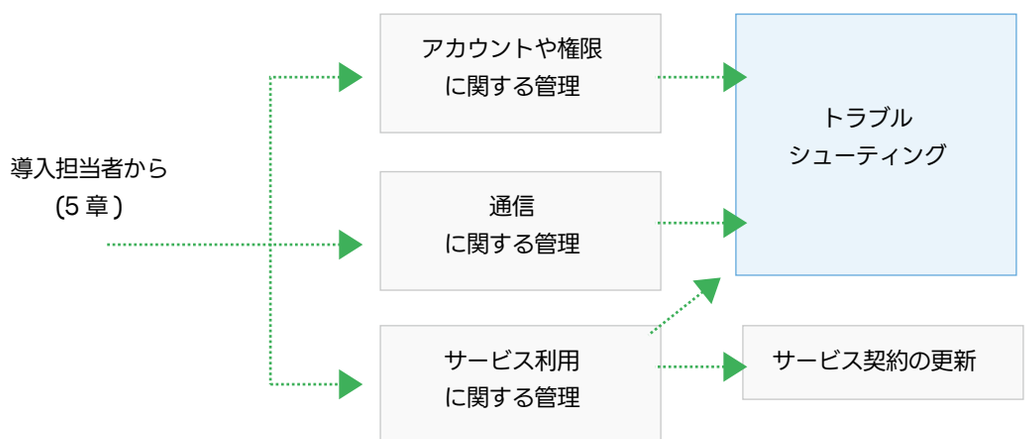


図 . 6 章の概要

注釈 | 定期的に、社内の有識者や専門部署などによる管理業務に対するレビューを実施することを推奨します。

6.2. 管理者画面へのアクセス

LINE WORKS サービスの管理は**管理者画面**で行います。LINE WORKS のテナント開設時に管理者画面にアクセスすることができるのは、テナントを開設した最高管理者のみです。

注釈
LINE WORKS の契約単位で割り当てられる論理的な空間を「テナント」と言います。

最高管理者は、他のメンバーに管理者権限を付与することで、LINE WORKS サービスの管理作業の全てもしくは一部を委任することができます。他のメンバーに管理者権限を付与することができるのは最高管理者のみです。

6.3. アカウント・権限に関する管理

アカウント・権限に関する脅威に対してメンバー、セキュリティの管理を行います。

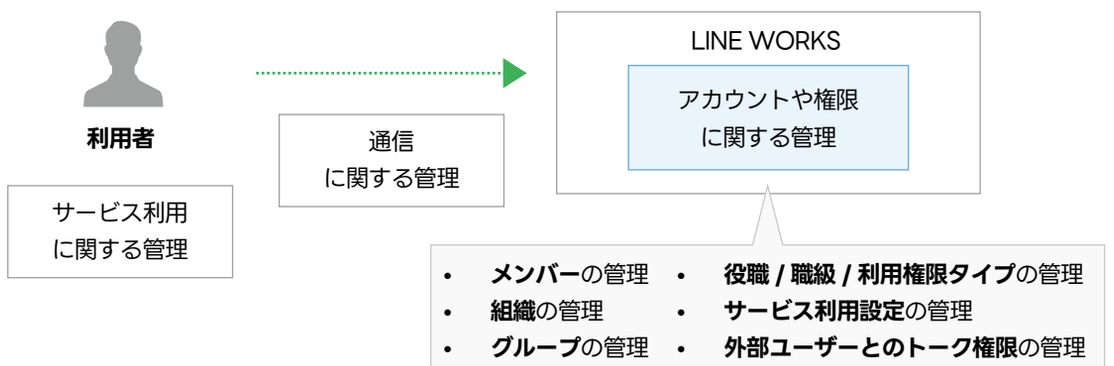


図 . アカウント・権限に関する管理

6.3.1. メンバー : メンバー

6.3.1.1. メンバーの管理機能

管理者は、メンバーの管理のために、以下の機能を利用することができます。

メンバーリスト

メンバーの追加や削除、組織変更などの管理を行うことができます。

ミニプロフィール

メンバーの顔写真や基本情報が表示され、メンバーリストでは確認できないメンバーの情報を確認することができます。

メンバーの検索

メンバーの登録情報に対して検索を行うことができます。

メンバー情報の管理

メンバーに関する各種情報について確認や変更を行うことができます。

各機能の詳細については、以下をご参照ください。

メンバーリスト :
https://guide.worksmobile.com/jp/admin/admin-guide/manage-members/members/member-list/

ミニプロフィール :
https://guide.worksmobile.com/jp/admin/admin-guide/manage-members/members/mini-profile/

メンバーの検索 :
https://guide.worksmobile.com/jp/admin/admin-guide/manage-members/members/search-members/

メンバー情報の管理 :
https://guide.worksmobile.com/jp/admin/admin-guide/manage-members/members/members-information/

6.3.1.2. メンバーの管理

LINE WORKS のメンバー管理では、以下の作業を行います。

- メンバーの追加
- メンバーの情報修正
- メンバーの所属変更
- メンバーの休職設定
- メンバーの削除

メンバーの追加

LINE WORKS をはじめる時や、途中からメンバーが加わった場合に、管理者は LINE WORKS にメンバーを追加します。

メンバー情報のうち、以下の項目については個人情報となるため、取り扱いに注意が必要となります。

- 姓
- 名
- 電話番号 (個人名義の電話の場合)
- 携帯電話番号 (個人名義の携帯電話の場合)
- 個人メールアドレス
- 生年月日

パスワードについては、管理者が作成する場合と、自動作成もしくはメンバーが作成する場合を選択することができます。

- パスワードを管理者が作成する場合、同じパスワードや強度の低いパスワードを作成すると、セキュリティ強度が低下するため注意が必要となります。
- パスワードを自動作成する場合や、メンバーが作成する場合、パスワードの通知先となるメールアドレスの入力に誤りが無いよう注意が必要となります。

LINE WORKS の利用において情報流出リスクを軽減させるためには、不要な情報にアクセスできないようにメンバーを管理する必要があります。また、サービスを利用しないメンバーを作成しないことも有効です。
メンバーの追加の詳細については、管理者画面利用ガイドの**「メンバーの追加」**をご参照ください。
パスワード作成の詳細については、管理者画面利用ガイドの**「パスワードの作成」**をご参照ください。

メンバーの情報修正

管理者は、LINE WORKS のメンバーの以下の情報を修正することができます。

- メンバー情報
- メンバー ID
- パスワード
- 利用開始の日付

メンバー ID の変更

メンバー ID を変更すると、メンバーは 5 分以内にすべてのサービスからログアウトされ、利用中の外部トーク連携用トーク ID、QR コード、招待用リンクも変更されます。メンバーが LINE WORKS のサービスを使用するためには、新しいメンバー ID でログインする必要があります。

パスワードの変更

管理者は、メンバーのパスワードについて、強制的に変更したり、メンバーに変更を要請したりすることができます。
パスワードの強制変更を行った場合、メンバーは 5 分以内にすべての LINE WORKS サービスからログアウトされます。
メンバーが LINE WORKS のサービスを使用するためには、変更後のパスワードで再度ログインする必要があります。
パスワードの変更を要請した場合、メンバーにトークでパスワードの変更を要請する案内が送信されます。メンバーは案内トークのリンクからパスワードを変更するか、次回ログイン時にパスワードを変更する必要があります。
パスワードを変更すると、最大 5 分以内にすべての LINE WORKS サービスからログアウトされます。

以下の場合は、情報を保護するために直ちにパスワードの変更を行う必要があります。

- メンバーがパスワードを忘れた・紛失した場合
- メンバーが乗っ取られた場合
- 本人ではないユーザーがアクセスした場合
- パスワードの漏えいが疑われる場合

メンバー情報の修正の詳細については、管理者画面利用ガイドの**「メンバー情報の修正」**をご参照ください。

メンバーの所属変更

人事異動などにより、所属組織に変更がある場合、管理者は LINE WORKS のメンバーの所属を変更します。
メンバーの所属を変更する場合、変更後のメンバーの権限が業務上の役割に応じた適切な状態になっているかチェックする必要があります。

メンバーの所属変更の詳細については、管理者画面利用ガイドの**「所属組織の管理」**をご参照ください。

メンバーの休職設定

LINE WORKS のメンバーが休職した場合、管理者は休職設定を行います。
休職設定を行うことで、そのメンバーのプロフィールと組織図に休職情報が表示されます。また、休職期間を設定することで、期間終了後に休職表示を自動的に解除することができます。メンバーに一時停止設定を行うことで、休職中に LINE WORKS のサービスにログインできないようにすることもできます。

メンバーの休職設定の詳細については、ヘルプセンターの**「休職者が出たときは何をすればいいですか？」**をご参照ください。

メンバーの削除

人事異動や退職などの理由により、メンバーが LINE WORKS のサービスを業務で使用しなくなった場合、管理者はそのメンバーを削除します。
LINE WORKS サービスの利用において情報流出リスクを軽減させるためには、退職者や異動者が不要な情報にアクセスできないようにメンバーを管理する必要があります。

メンバーの削除の詳細については、管理者画面利用ガイドの**「メンバーの削除」**をご参照ください。

6.3.2. メンバー：組織

6.3.2.1. 組織の管理機能

管理者は、組織の管理のために、以下の機能を利用することができます。

組織リスト

組織の追加や修正、移動、削除などの管理を行うことができます。

組織情報

組織名や説明、トークルーム機能の利用状況、所属するメンバーの一覧などが表示され、組織リストでは確認できない組織の情報を確認することができます。組織の修正や削除、組織長の変更を行うことができます。

組織の検索

組織名、組織 ID、組織のメンバーを条件に検索を行うことができます。

6.3.2.2. 組織の管理

LINE WORKS の組織管理では、以下の作業を行います。

- 組織の追加
- 組織の修正
- 組織の移動
- 組織の削除
- 組織データの復元

組織の追加

LINE WORKS をはじめる時や、途中から組織が設立された場合に、管理者は LINE WORKS に組織を追加します。

組織の追加の詳細については、管理者画面利用ガイドの**「組織の追加」**をご参照ください。

組織の修正

管理者は、LINE WORKS の組織の以下の情報を修正することができます。

- 組織名
- 組織の説明
- 組織 ID
- トークルームやグループウェア各機能の有効化 / 無効化
- 高度な設定
- 組織長

組織の修正の詳細については、管理者画面利用ガイドの**「組織の修正」**をご参照ください。

組織の移動

組織変更などにより、組織の構成や階層に変更がある場合、管理者は LINE WORKS の組織の移動を行います。

組織の構成や階層を変更する場合、変更後の組織の構成や階層が実際のコミュケーションの範囲と合致しているかチェックする必要があります。想定外のメンバーが組織に含まれている場合、トークルームでの会話や情報に不正にアクセスされるリスクが発生します。

組織の移動の詳細については、管理者画面利用ガイドの**「組織の移動」**をご参照ください。

組織の削除

廃止など理由により、組織が存在しなくなった場合、管理者はその組織を削除します。

組織に所属するメンバーがいる組織を削除することはできません。組織の削除前に所属するメンバーを移動させるか、組織から削除します。削除する組織の下位に組織がある場合は、下位組織も削除されます。

組織の削除の詳細については、管理者画面利用ガイドの「組織の削除」をご参照ください。

組織データの復元

組織を削除してから 30 日以内のトーク、ノート、予定、フォルダのデータは復元することができます。

組織データの復元の詳細については、管理者画面利用ガイドの「組織データの復元」をご参照ください。

6.3.3. メンバー：グループ

6.3.3.1. グループの管理機能

管理者は、グループの管理のために、以下の機能を利用することができます。

グループリスト

グループの追加や修正、削除などの管理を行うことができます。

グループ情報

グループ名や説明、グループマスター、トークルーム機能の利用状況、所属するメンバーの一覧などが表示され、グループリストでは確認できないグループの情報を確認することができます。グループの修正や削除、グループマスターの変更を行うことができます。

グループの検索

グループ名、グループタイプ、グループのメンバーを条件に検索を行うことができます。

6.3.3.2. グループの管理

LINE WORKS のグループ管理では、以下の作業を行います。

- グループの追加
- グループの修正
- グループの削除
- グループの検索
- グループデータの復元

グループの追加

社内外のプロジェクトや社内サークルなど、社内外を横断してコミュニケーションをはじめる場合に、管理者は LINE WORKS にグループを追加します。

グループには以下の 2 つのタイプがあります。

- (内部) グループ : 社内のメンバーのみで構成されたグループです。
- 外部ユーザーとのグループ: 外部の LINE WORKS メンバーと協業するための非公開グループです。(LINE ユーザーを含めることはできません。)

グループの追加の詳細については、管理者画面利用ガイドの「グループを作成」をご参照ください。

グループの修正

管理者は、LINE WORKS のグループの以下の情報を修正することができます。

- グループ名
- グループの説明
- グループマスター
- グループメンバー
- トークルームやグループウェア各機能の有効化 / 無効化
- 高度な設定

グループの修正の詳細については、管理者画面利用ガイドの「グループの修正」をご参照ください。

グループの削除

プロジェクトの完了や社内サークルの廃止など理由により、グループが不要になった場合、管理者はそのグループを削除します。

グループを削除すると、トークルームやグループウェアのすべてのデータが削除されます。復元することはできません。

外部グループを削除した場合は、グループを利用中のすべての会社から削除されます。

グループの削除の詳細については、管理者画面利用ガイドの「グループの削除」をご参照ください。

グループデータの復元

グループを削除してから 30 日以内のトーク、ノート、予定、フォルダのデータは復元することができます。

グループデータの復元の詳細については、管理者画面利用ガイドの「削除したグループデータの復元」をご参照ください。

6.3.4. メンバー : 役職 / 職級 / 利用権限タイプ

6.3.4.1. 役職 / 職級 / 利用権限タイプの管理機能

管理者は、メンバーの管理のために、以下の機能を利用することができます。

役職

メンバーに付与できる職務上の責任の単位です。

職級

メンバーに付与できる職務上のレベルです。

利用権限タイプ

メンバーに付与できるサービス利用権限のタイプです。

役職、職級、利用権限タイプの詳細については、管理者画面利用ガイド**「役職、職級、利用権限タイプの管理」**をご参照ください。

6.3.4.2. 役職 / 職級 / 利用権限タイプの管理

LINE WORKS の役職 / 職級 / 利用権限タイプの管理では、以下の作業を行います。

- 役職の使用の有無。役職の追加、変更、削除。
- 職級の使用の有無。職級の追加、変更、削除。
- 利用権限タイプの使用の有無。利用権限タイプの追加、変更、削除。

「利用権限タイプ」と「権限テンプレート」

利用権限タイプを利用することで「ロールベースのアクセス管理」を行うことができます。「ロールベースのアクセス管理」では、個々のメンバーに個別に権限を付与するのではなく、メンバーの役割に応じて「利用権限タイプ」を作成し、各メンバーに「利用権限タイプ」を割り当てます。利用できるサービスや機能の組み合わせを定義した「権限テンプレート」を、「利用権限タイプ」に紐付けることで、各メンバーが利用できる権限が決定します。
役割の変更があった場合は、権限テンプレートを変更することで、同じ「利用権限タイプ」のメンバー全員の権限を変えることができます。個々のメンバーでの権限変更と比べて変更漏れが発生しにくいため、不必要なサービスへのアクセスを防止することに繋がります。

6.3.5. セキュリティ : サービス利用設定

6.3.5.1. サービス利用設定の管理機能

管理者は「ロールベースのアクセス管理」を行うために、以下の機能を利用することができます。

- 権限テンプレートの作成
- 権限テンプレートの利用権限タイプやメンバーへの割り当て

「ロールベースのアクセス管理」については、本章の「メンバー : 役職 / 職級 / 利用権限タイプ」をご参照ください。

6.3.5.2. サービス利用設定の管理

LINE WORKS のサービス利用設定の管理では、以下の作業を行います。

権限テンプレートの作成

利用できるサービスや機能の組み合わせを定義した「権限テンプレート」を作成します。

利用権限タイプ

権限テンプレートと紐付ける「利用権限タイプ」を指定します。指定された「利用権限タイプ」を付与されているメンバーは、権限テンプレートで定義された権限の範囲で LINE WORKS のサービスや機能を利用することができます。

権限テンプレートが変更された場合、「利用権限タイプ」を付与されているメンバー全員の権限が変更されます。

メンバー

権限テンプレートを直接紐付けるメンバーの指定をします。

サービス利用設定の詳細については、管理者画面利用ガイドの**「サービス利用設定」**をご参照ください。

6.3.6. セキュリティ：外部ユーザーとのトーク権限

6.3.6.1. 外部ユーザーとのトーク権限の管理機能

管理者は、外部ユーザーとのトーク権限の管理のために、以下の機能を利用することができます。

- LINE 連携の利用を許可するメンバーの追加、削除
- 外部の LINE WORKS 連携の利用を許可するメンバーの追加、削除

6.3.6.2. 外部ユーザーとのトーク権限の管理

LINE WORKS の外部ユーザーとのトーク権限の管理では、以下の作業を行います。

LINE

LINE 連携の利用を許可するメンバーの追加、削除を行います。

「サービス」>「トーク」>「外部ユーザーとのトーク」>「LINE 連携」で「連携機能の利用権限」がすべてのメンバーに許可されている場合や、「新規メンバーに連携権限を自動付与」が有効な場合は、自動的にメンバーが追加されます。

外部 LINE WORKS

外部の LINE WORKS 連携の利用を許可するメンバーの追加、削除を行います。

「サービス」>「トーク」>「外部ユーザーとのトーク」>「外部 LINE WORKS 連携」で「連携機能の利用権限」がすべてのメンバーに許可されている場合や、「新規メンバーに連携権限を自動付与」が有効な場合は、自動的にメンバーが追加されます。

外部ユーザーとのトーク権限の詳細については、管理者画面利用ガイドの**「外部ユーザーとのトーク権限」**をご参照ください。

6.4. 通信に関する管理

通信への脅威に対応するために、ネットワークの管理を行います。

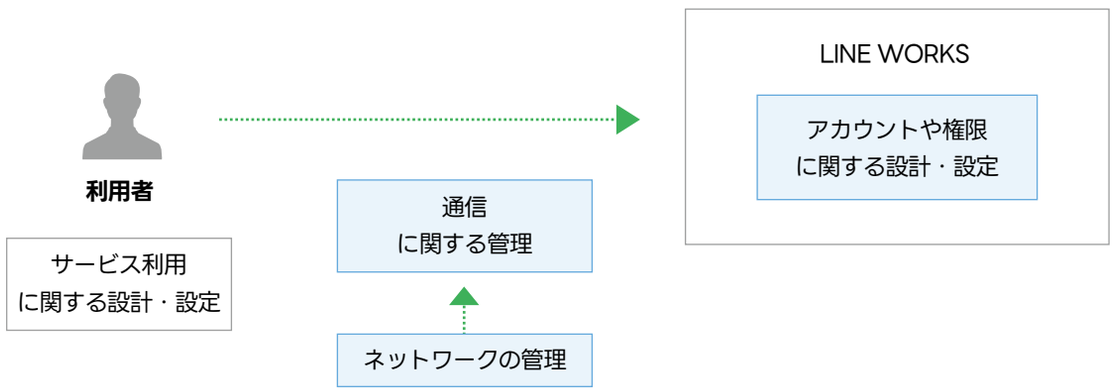


図 . 通信に関する管理

6.4.1. セキュリティ：ネットワーク管理

6.4.1.1. アクセス IP 制限の管理機能

管理者は、アクセス IP 制限の管理のために、以下の機能を利用することができます。

- アクセス IP の追加、削除
- サービス利用国の追加、削除

6.4.1.2. アクセス IP 制限の管理

LINE WORKS のアクセス IP 制限の管理では、以下の作業を行います。

すべての IP アドレスからアクセスを許可する場合

サービスを利用する国を制限することができます。この制限を有効にしている場合、制限の例外となる国を追加・削除することができます。

指定した IP アドレスからのみアクセスを許可する場合

アクセスを許可する IP アドレスもしくは IP アドレスレンジを追加・削除することができます。

ネットワーク管理の詳細については、管理者画面利用ガイドの**「ネットワーク管理」**をご参照ください。

6.5. サービス利用に関する管理

利用者のサービス利用における脅威に対応するために、セキュリティ、端末、サービスの管理を行います。

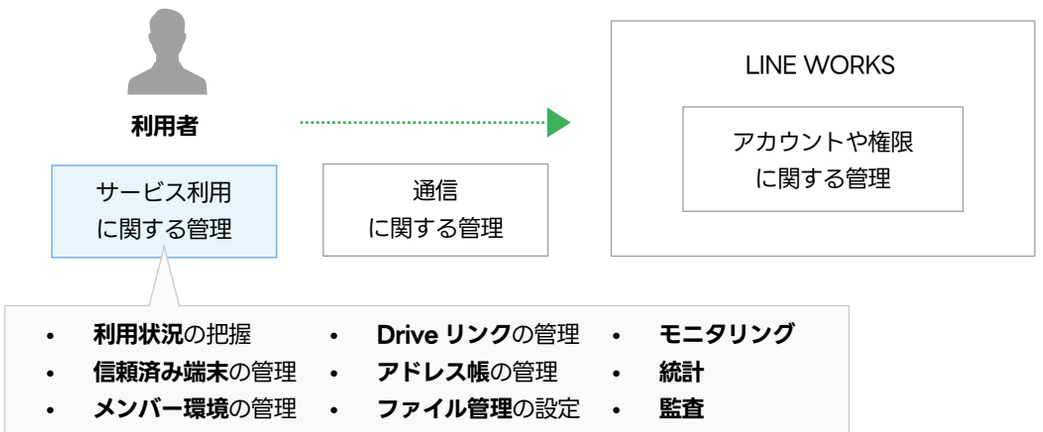


図 . サービス利用に関する管理

6.5.1. セキュリティ : 利用状況

6.5.1.1. 利用状況の管理機能

管理者は、利用状況の管理のために、以下の機能を利用することができます。

LINE WORKS では、アプリ (PC 版 / モバイル版) でサービスにアクセスした端末の情報を確認することができます。

また、古いバージョンのアプリを利用しているメンバーにアップデート通知を送信することができます。

LINE WORKS では、以下の端末情報の確認やダウンロードをすることができます。

デバイス

デバイスのモデル名です。

Vendor ID

デバイスの固有 ID です。デバイスを初期化すると変更されます。LINE WORKS アプリを削除して再インストールしても変更されません。

ユーザー

デバイスを使用しているメンバーの名前と ID です。

OS

デバイスの OS とバージョンです。

インストール済みアプリ

デバイスにインストールされた LINE WORKS アプリの種類とバージョンです。

最終アクセス

該当するデバイスが、最後に LINE WORKS にアクセスした時間です。

6.5.1.2. 利用状況の管理

LINE WORKS を正常かつ安全に利用いただくためには、LINE WORKS ご利用中のメンバー全員が最新バージョンの OS、アプリをお使いいただくことが重要です。また、メンバーの利用バージョンを統一することにより、バージョン間の互換性を考慮する必要がなくなり、社内でのトラブルシューティングの際にバージョン情報の確認が不要となるメリットがあります。
定期的に利用状況を確認し、メンバー全員が最新のバージョンを使用していることを確認することをお勧めいたします。

LINE WORKS の利用状況の管理では、以下の作業を行います。

モバイル

利用者のモバイル版アプリについて以下の情報を確認します。

- デバイス
- OS
- インストール済みアプリ
- ユーザー
- 最終アクセス

インストール済みのアプリが最新版で無い場合、インストール済みアプリ欄に「アップデートが必要」と表示されます。表示されているメンバーを選択し、「アップデート案内」ボタンをクリックすることで、メンバーのモバイル版アプリに対して、アップデート通知を送信することができます。

PC

利用者の PC 版アプリについて以下の情報を確認します。

- デバイス
- OS
- インストール済みアプリ
- ユーザー
- 最終アクセス

インストール済みのアプリが最新版で無い場合、インストール済みアプリ欄に「アップデートが必要」と表示されます。表示されているメンバーを選択し、「アップデート案内」ボタンをクリックすることで、メンバーの PC 版

アプリに対して、アップデート通知を送信することができます。

利用状況の確認については、管理者画面利用ガイドの「利用状況」をご参照ください。

6.5.2. セキュリティ：信頼済み端末管理

6.5.2.1. 信頼済み端末の管理機能

「セキュリティ」>「アカウント管理」で「携帯電話の画面ロック解除でログイン (FIDO 認証)」を許可している場合、FIDO 生体認証を使用してログインすると、そのモバイル端末情報が「信頼済み端末」として LINE WORKS に登録され、以降はモバイル版アプリへのログイン時に 2 段階認証をスキップすることができます。

管理者は、信頼済み端末の管理のために、以下の機能を利用することができます。

- 信頼済み端末の確認・削除

6.5.2.2. 信頼済み端末の管理

LINE WORKS の信頼済み端末の管理では、以下の作業を行います。

信頼済み端末の確認

LINE WORKS に登録されている信頼済み端末について以下の情報を確認します。

- 端末名
- OS
- メンバー
- 認証日時
- 直近の認証

信頼済み端末の削除

端末を選択し、「信頼済み端末から削除」ボタンをクリックすることで、信頼済み端末を削除することができます。

削除された信頼済み端末では、次回のモバイル版アプリへのログイン時に 2 段階認証を要求されます。

信頼済み端末の詳細については、管理者画面利用ガイドの「信頼済み端末」をご参照ください。

6.5.3. メンバー環境の管理

6.5.3.1. LINE WORKS サービスのご利用環境

LINE WORKS では、LINE WORKS サービスの利用における正常動作を確認し、お客様をサポートできる利用環境 (ブラウザ版 /PC 版 / モバイル版) を公開し、随時アップデートをしています。お客様のご利用環境において LINE WORKS サービスが正常に動作し、お客様の情報を安全に保つためには、お客様のメンバーのご利用環境が最新のシステム要件に該当しているかどうかを定期的にご確認いただく必要があります。

LINE WORKS は、お客様のご利用環境に応じてサポートご提供の可否を判断いたします。

システム要件を満たす環境

LINE WORKS サービスの利用における正常動作を確認し、お問い合わせ窓口等でもサービスでの正常動作を前提としてサポートができる利用環境です。

ベストエフォート対応の環境

サービス利用における正常動作は保証しておらず、お問い合わせ窓口等でもシステム要件を満たさない環境に起因する可能性がある場合は、サポートが難しく修正等の提供は約束しない環境です。

サポート対象外の環境

「システム要件」「ベストエフォート対応」に記載するシステムおよび端末以外でのサービス利用環境です。このような環境については、LINE WORKS における動作確認を行なっておらず、すべての窓口におけるサポートの対象外となります。

また、運営上の都合により必要に応じてサービスへのアクセスを遮断する場合があります。

LINE WORKS のご利用環境に関する詳細については、設定利用ガイドの**「システム要件」**をご参照ください。

6.5.3.2. LINE WORKS アプリのバージョン

モバイル用および PC 用の LINE WORKS アプリは、最新版から二つ前のメジャーアップデートバージョンまでご利用いただけます。

注釈

メジャーアップデートとは、バージョン番号の小数点第一位が変わるアップデートを指します。小数点第二位が変わるマイナーアップデートでは、サービスを利用できるバージョンおよび必須アップデート対象のバージョンは変わりません。

2 バージョン前のメジャーアップデートバージョンに満たないバージョンは必須アップデートの対象となり、サービス利用のためにはアップデートが必要となります。LINE WORKS アプリを継続的にご利用いただくために、お客様のメンバーのアプリのバージョンを定期的にご確認いただく必要があります。

注釈

最新版のアプリのインストールには、「システム要件」記載の OS バージョンであることが必要となります。

LINE WORKS アプリのバージョンの詳細については、設定利用ガイドの**「システム要件」**の「アプリ利用時のご注意」をご参照ください。

LINE WORKS アプリのアップデート情報については、LINE WORKS 公式サイトの**「アップデート情報」**をご参照ください。

6.5.3.3. メンバー環境の管理

管理者は、メンバー環境の管理のために、「メンバー」>「メンバー」で一覧表示される各メンバーの「メンバー情報」において以下の機能を利用することができます。

デバイス

メンバーの信頼済み端末と、モバイル版アプリと Drive エクスプローラーを使用したデバイスについて、以下の情報を確認することができます。

- デバイス
- OS
- インストール済みアプリ
- 最終アクセス

古いバージョンのアプリを利用している場合は、メンバーのアプリにアップデート通知を送信できます。
MDM(遠隔デバイス管理) を有効にしている場合は、モバイル版アプリ内のデータを削除したり、初期化したりすることができます。削除したデータを復元することはできません。
デバイスの確認については、管理者画面利用ガイドの**「メンバー情報の管理」**の「デバイス」をご参照ください。

アクセス状況

メンバーが直近 90 日間に LINE WORKS へのアクセスに利用した端末について、以下の情報を確認することができます。

- アクセス時間
- アクセス環境
- 位置 (IP アドレス)

管理者は、それぞれの端末について、強制ログアウトを行うことができます。外部からの不正アクセスなどがあった場合に実行します。
アクセス状況の確認については、管理者画面利用ガイドの**「メンバー情報の管理」**の「アクセス状況」をご参照ください。

6.5.3.4. モバイル端末の買い替え対応

お客様が MDM を導入されている場合に、メンバーがご利用中のモバイル端末を買い替えたり交換したりしたときは、LINE WORKS を引き続きご利用いただくために、新しいモバイル端末に LINE WORKS MDM のプロファイルの導入を行う必要があります。

注釈

メンバーがモバイル版アプリ下部のメニュー「ホーム」の「設定」にある「モバイルデバイス管理」から、プロファイルのインストールをする必要があります。

LINE WORKS MDM プロファイル導入の詳細については、設定利用ガイドの「モバイルデバイス管理」の「モバイルデバイス管理を利用する」をご参照ください。

6.5.4. セキュリティ : Drive リンク管理

6.5.4.1. Drive リンクの管理機能

管理者は、Drive リンクの管理のために、以下の機能を利用することができます。

- 共有リンクの確認・削除

6.5.4.2. Drive リンクの管理

LINE WORKS の Drive リンクの管理では、以下の作業を行います。

共有リンクの確認

共有リンクについて以下の情報を一覧で確認することができます。

- ファイル / フォルダ名
- 作成者
- 作成日
- リンクの権限

各共有リンクの「情報」をクリックすることで、リンクの詳細情報を確認することができます。

- リンク作成者
- リンクの有効期限
- リンク

ファイル / フォルダ情報

- 名前
- タイプ
- サイズ
- パス
- アップロード日
- 修正日

リンクのアクセス情報

- ユーザー
- ファイル / フォルダ名
- アクセス
- 日時

共有リンクの削除

共有リンク一覧の「管理」もしくは、リンクの詳細の「リンク」から、共有リンクを削除することができます。

Drive リンク管理の詳細については、管理者画面利用ガイドの「Drive リンク管理」をご参照ください。

6.5.5. サービス：アドレス帳

6.5.5.1. アドレス帳の管理機能

管理者は、アドレス帳の顧客 / 取引先の管理のために、以下の機能を利用することができます。

- 顧客 / 取引先の確認・削除

6.5.5.2. アドレス帳の管理

LINE WORKS のアドレス帳の管理では、以下の作業を行います。

顧客 / 取引先の確認

顧客 / 取引先について以下の情報を一覧で確認することができます。

- 名前
- 会社・所属
- 連絡マスター
- 公開範囲

各顧客 / 取引先をクリックすることで、連絡先情報 (連絡先の一部の情報) を確認することができます。

- 名前
- メールアドレス
- 連絡マスター
- 公開範囲

顧客 / 取引先の削除

顧客 / 取引先一覧もしくは、個別の連絡先情報から、顧客 / 取引先を削除することができます。

アドレス帳の顧客 / 取引先の管理の詳細については、管理者画面利用ガイドの「顧客 / 取引先の管理」をご参照ください。

6.5.6. セキュリティ：ファイル管理

6.5.6.1. ファイルの管理機能

管理者は、ファイルの管理のために、以下の機能を利用することができます。

- 制限するファイル形式の追加・削除

6.5.6.2. ファイルの管理

LINE WORKS のファイルの管理では、以下の作業を行います。

ファイル形式での制限

LINE WORKS サービス上でのファイル送受信を制限するファイル形式 (拡張子) の追加・削除を行います。指定された形式のファイルは、LINE WORKS 上にアップロードしたり共有したりすることができません。

ファイル管理の詳細については、管理者画面利用ガイドの**「ファイル管理 」**をご参照ください。

6.5.7. モニタリング

LINE WORKS に設定されたポリシーによる通知を受信した場合、その検知内容を確認し、必要な対応を行います。

6.5.7.1. 通知の受信

通知をメールで受信した場合は「ポリシー名」のリンクを、トークで受信した場合は「監査ポリシー表示」をクリックすると、管理者画面のモニタリングポリシー表示画面に遷移し、どのようなポリシーに対する事象を検知したのかを把握することができます。

ポリシーにより検知された内容の確認については、管理者画面利用ガイドの**「トーク」**の「トークのモニタリング」をご参照ください。

6.5.7.2. 管理者画面での確認

管理者画面のモニタリング画面では、各ポリシの使用状態、検知数などを一覧で確認することができます。

ポリシーによる検知が発生した場合、検知数のリンクをクリックすることで、検知履歴にアクセスすることができます。検知履歴画面では、実際に検知された詳細を確認することができます。

6.5.7.3. メンバーの一時停止

必要がある場合は、ポリシー通知の対象となったメンバーの一時停止を行います。
メンバーの一時停止を行うことで、そのメンバーは LINE WORKS のサービスを利用できなくなります。ポリシーが検知した事象の解決後、一時停止を解除することで、メンバーは再び LINE WORKS の利用が可能となります。

メンバーの一時停止の詳細については、管理者画面利用ガイドの**「メンバー情報の管理 」**の「一時停止」をご参照ください。

6.5.8. 統計

管理者は、統計情報の確認のために、以下の統計を利用することができます。

- アカウント
- アクティブメンバー
- インストール状況
- 共有ストレージ
- 掲示板

- トーク
- メール
- カレンダー
- Drive (トークルームフォルダ)
- アドレス帳
- アンケート
- タスク

統計の詳細については、管理者画面利用ガイドの「統計」をご参照ください。

6.5.9. 監査

管理者は、監査のために、以下の機能を利用することができます。

- メンバーの利用履歴の検索・確認
- 監査ログのダウンロード

メンバーの利用履歴の検索・確認

LINE WORKS の監査機能を利用して、LINE WORKS の利用履歴を確認することができます。LINE WORKS の利用において問題が発生した場合、監査情報から問題発生時点の状況を確認します。

LINE WORKS の監査機能では、以下の利用履歴を確認することができます。

管理者画面

管理者画面で実行されたすべてのタスクの履歴と操作したメンバーを確認することができます。

掲示板

掲示板サービスにてメンバーが作業した履歴を確認することができます。

トーク

トークについて送信、受信、削除の履歴を確認することができます

メール

メールについて送信、受信、削除の履歴を確認することができます。(メールの監査機能は、アドバンストプランでのみ利用できます。)

カレンダー

カレンダーのメンバーがカレンダーおよび予定を登録、修正、削除した履歴を確認します。

アドレス帳

メンバーがアドレス帳情報を登録や、閲覧、修正した履歴を確認します。

Drive(トークルームフォルダ)

Drive、トークルームフォルダでファイルのアップロード、更新、共有などの履歴を確認することができます。

タスク

タスクの作成、修正、完了、進行中に変更、削除の主な作業履歴を確認することができます。

アンケート

アンケートの作成、編集、削除などの履歴を確認することができます。

通話

アプリ (v3.0 以降) を使用したメンバーの通話履歴を確認することができます。

画面共有

画面共有における参加者と利用履歴を確認することができます。

トークルームノート

トークルームノートにおける投稿、編集、削除などの履歴を確認することができます。

テンプレート

テンプレートの作成、編集、削除などの履歴を確認することができます。

Bot API

Bot API を呼び出したログを検索することができます。

Developer Console

Developer Console で実行されたすべてのタスク履歴と操作したメンバーを確認することができます。

ログイン

LINE WORKS サービスにログインした記録を確認することができます。

ファイル

LINE WORKS でファイルをダウンロード・閲覧した記録を確認することができます。

監査の詳細については、管理者画面利用ガイドの「監査」をご参照ください。

重要

LINE WORKS サービスの管理者は、監査サービスの利用に伴い、メンバーのデータ (トーク内容など) にアクセスする場合は、法令および「LINE WORKS サービス利用規約」の定めに従い、メンバーの有効な同意を必ず得るものとします。なお、メンバーからの同意の有無に関わらず、メンバーのデータにアクセスしたことにより管理者とメンバーとの間で生じたトラブルについては、LINE WORKS 株式会社は責任を負いかねますのでご留意ください。

6.5.9.1. 監査の機能

監査ログのダウンロード

LINE WORKS の監査機能における監査情報の保管期限とダウンロードの可否については、プランに応じて以下のようになります。

	保管期限	ダウンロード
有償プラン	180 日	可能
フリープラン	2 週間	不可

有償プランをご契約のお客様は、180 日経過までに監査情報をダウンロードいただくことで、180 日以上前の状況を確認することが可能となります。

6.5.9.2. 監査作業の実施

LINE WORKS の監査では、以下の作業を行います。

メンバーの利用履歴の検索・確認

管理者画面や各サービスについて、監査ログからメンバーの利用履歴を検索・確認します。検索条件として、期間のほか、検索画面ごとに詳細な条件を設定することができます。

監査ログのダウンロード

管理者画面や各サービスについて、監査ログをダウンロードします。

監査ログファイルのダウンロードは、各画面の「ダウンロード」ボタンをクリックすることにより開始します。ログファイルの準備が完了すると「監査」>「ログダウンロード」からダウンロードが可能となります。

6.6. トラブルシューティング

LINE WORKS サービスにおいてトラブルが発生した場合は、冷静かつ迅速に対応することが重要となります。

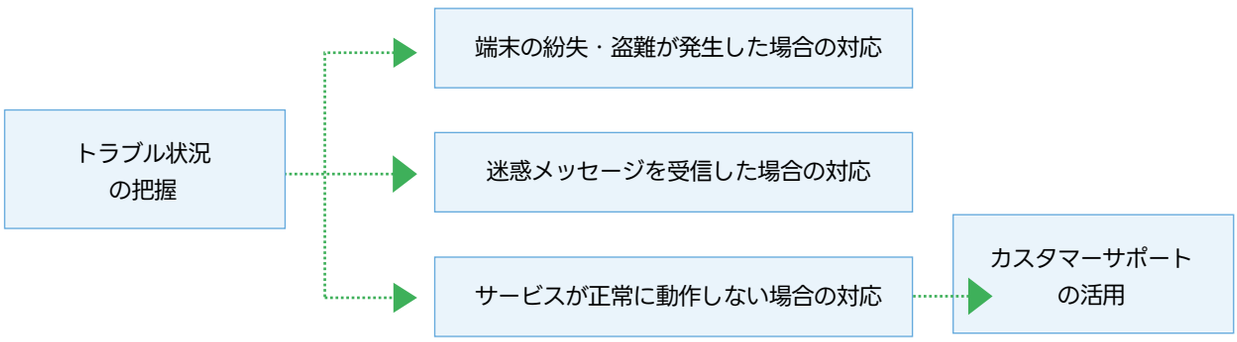


図 . トラブルシューティング

6.6.1. トラブル状況の把握

まず、トラブル事象の発生状況を把握します。問題の発生状況を正確に把握することにより、早期解決が可能となります。

トラブル事象発生状況を把握するためには、5W1H を把握することが有用です。

いつ (When)

いつトラブル事象が発生したのか、可能な限り正確な時刻を把握します。

どこで (Where)

どこでトラブル事象が発生したのか、可能な限り正確な場所や操作対象などを把握します。

誰が (Who)

誰がトラブル事象に遭遇したのか、可能な限り正確な氏名や連絡先、人数などを把握します。

何を (What)

何をしようとしてトラブル事象が発生したのか、可能な限り正確な動作や操作などを把握します。

どのようになった (How)

どのようなトラブル事象が発生したのか、可能な限り正確な事象や影響などを把握します。

なぜ (Why)

なぜトラブル事象が発生したのか、発生原因を把握するための材料となる情報を可能な範囲で把握します。実際の発生原因は、トラブルシューティングの過程で明確にしていきます。

6.6.2. 端末の紛失・盗難が発生した場合の対応

LINE WORKS を利用している端末 (PC/ モバイル) の紛失や盗難が発生した場合、迅速にその端末から LINE WORKS へのアクセスを遮断する必要があります。

6.6.2.1. アプリの利用停止

端末の紛失や盗難があった場合、個別のメンバー情報画面で「アプリの利用停止」を設定することにより、そのメンバーのアプリ (PC 版 / モバイル版) の利用を停止することができます。

アプリの停止をした場合でも、そのメンバーは引き続き、ブラウザから LINE WORKS にアクセスして利用することができます。

6.6.2.2. パスワード変更と強制ログアウト

ブラウザ利用をしている端末について紛失・盗難が発生した場合、該当メンバーのパスワードを変更し、強制ログアウトをさせることで、その端末から再度アクセスできないようにすることができます。

管理者画面の「メンバー」メニューの「メンバー」サブメニューから、メンバー一覧にアクセスし、該当するメンバーのメンバー情報について、以下の変更を行います。

パスワードの強制変更

「セキュリティ設定」の「パスワード」の「変更」ボタンをクリックします。ポップアップ画面の「強制変更」タブから、メンバーのパスワードを変更します。

強制ログアウト

「アクセス状況」の「管理」ボタンをクリックします。紛失・盗難対象からのアクセスについて「ログアウト」ボタンをクリックします。

パスワードの強制変更については、管理者画面利用ガイドの**「メンバー情報の修正」**の「パスワードを強制変更する」をご参照ください。

強制ログアウトについては、管理者画面利用ガイドの**「メンバー情報の管理」**の「アクセス状況」をご参照ください。

6.6.2.3. モバイルデバイス管理 (MDM) によるモバイル端末の管理

モバイルデバイス管理 (MDM) を利用している場合は、モバイル端末の LINE WORKS へのアクセスを管理することができます。

LINE WORKS MDM をご利用の場合、管理者は遠隔でモバイル端末にインストールされた LINE WORKS モバイル版アプリのデータを削除したり、モバイル端末を初期化したりすることができます。

LINE WORKS MDM による遠隔操作の詳細については、設定利用ガイドの**「モバイルデバイス管理」**の「遠隔でデバイスを管理する」をご参照ください。

6.6.3. 迷惑メッセージを受信した場合の対応

外部の LINE WORKS のユーザーから不適切なメッセージが届いた場合、そのトーク内容、トークルーム、トーク相手を LINE WORKS に通報することができます。通報の事実は相手に知らされません。

LINE WORKS は通報された内容を調査し、利用規約に違反する行為が確認された場合は、相応の対応を行います。なお、

調査結果はお知らせできません。ご了承ください。

外部ユーザーに関する通報の詳細については、LINE WORKS ヘルプセンターの**「外部ユーザーの通報」**をご参照ください。

6.6.4. サービスが正常に動作しない場合の対応

LINE WORKS にログインできない、特定のサービス (トーク、ドライブなど) に接続できない、主要機能が動作しない (トーク招待、メッセージ送信など)、著しい速度低下など、サービスが正常に動作しない場合、サービス側の障害なのか、ご利用環境に依存するトラブルなのか、切り分けを行います。

一般的に、以下のステップで切り分けを行っていきます。

1. トラブル事象の範囲の確認

まず、トラブル事象の発生範囲を確認します。トラブル事象の発生範囲を把握することで、事象発生時の操作を確認するためのヒアリングを行う対象が明確になります。
次に、トラブル事象による影響範囲を確認します。トラブル事象による影響範囲が広く、影響が大きい場合は、迅速な対応が求められます。一方で、トラブル事象による影響範囲やその影響が限定的な場合は、あわてず冷静に状況を見極めることも重要となります。

2. トラブル事象の再現性の確認

トラブル事象について、同じ操作を行った場合の再現性について確認します。操作状況が明確であれば、再現性の確認が容易となります。操作状況が不明瞭の場合、再現性の確認や、サポートによる支援が困難となってしまいます。どんな操作を行ったのかという履歴は、管理者画面の「監査」から確認することができます。
同じ操作をしてもトラブルが再現しない場合、障害が解消しているか、もしくは偶発性の高い事象である可能性が高いため、トラブル自体は解消している可能性があります。再現する場合は、環境に依存した障害が起きているか、LINE WORKS においてトラブルが発生している可能性があります。

3. サービス状態の確認

LINE WORKS では常に安定したサービス運用に努めていますが、万が一各機能が正常に動作しない等が起こった場合には、LINE WORKS Service Status でサービス状態をご確認ください。**LINE WORKS Service Status** では、LINE WORKS の各サービスについて、現在のサービス状態と、過去 3 ヶ月間のサービス状態について確認することができます。

4. サポート窓口のご利用

お客様のご契約形態に応じて適切なお問い合わせ窓口をご利用ください。
LINE WORKS の窓口については、ヘルプセンターの**「LINE WORKS に関する問い合せ窓口を知りたいです」**をご参照ください。

5. コミュニティのご利用

LINE WORKS は、LINE WORKS サービスの利用者同士のコミュニケーションの場として、以下の 2 つのコミュニティサービスを提供しています。

LINE WORKS コミュニティ : https://community.worksmobile.com/jp/

LINE WORKS についての質問や活用方法を共有するスペースです。

LINE WORKS Developer コミュニティ : https://forum.worksmobile.com/jp/

LINE WORKS Developers に関して、他の開発者と意見交換や情報共有ができる交流スペースです。

コミュニティでは LINE WORKS の利用者間で様々な意見交換が行われており、障害状況に関する情報が得られる可能性があります。コミュニティにおける情報について、LINE WORKS は何らの保証をいたしません。あらかじめご了承ください。

6.6.5. LINE WORKS カスタマーサポートの活用

LINE WORKS では、製品の設定方法、操作手順がわからない場合や、製品の動作に関するトラブルなど困りごとがある際のご支援を行うためのカスタマーサポートをご提供しています。LINE WORKS カスタマーサポートをご活用いただくことで、トラブル事象への迅速な対応が可能となります。

カスタマーサポートのご提供内容は以下の通りです。

対象者	問い合わせ方法	受付時間
フリープラン開設後 30 日未満の管理者	電話	平日 9:00 ～ 18:00 （土日・祝日・年末年始を除く）
有償プランご契約中の管理者	電話もしくは Web フォーム	Web フォーム : 24 時間 電話 : 平日 9:00 ～ 18:00

お問い合わせから 24 時間以内に、カスタマーサポートから一次回答をいたします。(ただし、土日祝日・年末年始期間など休業期間を除きます。)

なお、LINE WORKS API に関する問い合わせはカスタマーサポートの対象外となります。

LINE WORKS のサポートプランの詳細については、LINE WORKS「サポートプラン」をご参照ください。

6.7. サービス契約の更新

6.7.1. 更新手続き

サービスの更新方法は LINE WORKS の購入先により異なる場合があります。不明な場合は購入先にご確認下さい。

6.7.2. 解約する場合の留意点

LINE WORKS サービスを解約する場合、解約後にお客様が保有する情報資産や個人情報の保護レベルが低下することを回避するために、以下の点について留意していただく必要があります。

セキュリティ担当部署への連絡・相談

サービスを解約する旨をセキュリティ担当部署に事前に連絡します。これにより、LINE WORKS サービスの解約に伴う情報セキュリティや個人情報の保護のためのポリシーや体制などの変更について社内のセキュリティ専門家の支援が得られるようにします。

バックアップすべきデータの選定

解約前にサービスに保存されている重要なデータを確実にバックアップします。重要なデータを失うリスクを避けるため、解約プロセスの早い時期にバックアップを確保しておくことが重要です。

LINE WORKS サービスの解約においても、事前に必要なデータをバックアップしてから解約手続きを行うことをお勧めします。

データの移行先の選定

バックアップ後は、そのデータの安全な移行先を選定します。データの互換性とセキュリティを確保するために、適切な移行先を選定する必要があります。データの移行は慎重に行い、移行先においても正しくデータを使用できるように確認する必要があります。

アクセス権の確認と削除

サービスの解約にあたり、そのサービスへのすべてのアクセス権を確認し、必要に応じて削除します。

LINE WORKS サービスは、最高管理者を除く全てのメンバーを削除するまで解約することができません。解約手続きを開始する前に、全てのメンバーの削除を最高管理者が行ってください。

メンバーの削除の詳細については、管理者画面利用ガイドの**「メンバーの削除」**をご参照ください。

サービスの解約確認

サービス提供者との契約を正式に終了し、契約書や利用規約に従って、必要な手続きを完了させます。

LINE WORKS サービスは、ブラウザ版でのみ解約手続きを行うことができます。LINE WORKS サービス上のお客様のデータは、解約日から 7 日後に完全に削除され、復旧は不可能となります。

LINE WORKS サービスの解約の詳細については、管理者画面利用ガイドの**「LINE WORKS の解約」**をご参照ください。

情報管理台帳の更新

サービスの解約に伴い、情報管理台帳を更新する必要があります。

LINE WORKS サービスの解約がお客様のデータ保護に関するポリシー、アクセス制御のポリシーなどのセキュリティポリシーに影響する場合は、その更新も行う必要があります。

利用者への通知と教育

最後に、サービスの解約とそれに伴う変更点について、利用者に通知し、必要に応じてサポートを行います。

LINE WORKS サービスの解約がシャドー IT の利用に繋がらないように、セキュリティ文化を維持していくことが重要です。

附録

附録 A: LINE WORKS に関する情報

A.1. LINE WORKS に関するリンク集

導入ご検討の方やご利用中の方向けの資料

LINE WORKS では、導入や活用をご支援するために多様なコンテンツや資料をご提供しています。

LINE WORKS とは : https://guide.worksmobile.com/jp/start/what-is-line-works/
LINE WORKS の簡単な紹介を動画とともにご覧いただくことができます。

導入検討用資料 : https://line-works.com/ebook/
LINE WORKS に関する様々な情報をご提供します。

初期設定ガイド : https://line-works.com/ebook/video-for-beginner/
LINE WORKS の始め方 (初期設定) を解説します。

活用支援ガイド : https://line-works.com/step-up/
LINE WORKS の基本的な使い方や業務課題に合わせた活用方法をお届けします。

資料 (さわってわかった LINE WORKS): https://line-works.com/ebook/tieup/
LINE WORKS サービス関連の様々な資料をダウンロードしていただくことができます。

LINE WORKS ヘルプセンター : https://guide.worksmobile.com/jp/
LINE WORKS に関する疑問やお悩みを解決するために豊富な情報をご提供します。

管理者向けの資料

LINE WORKS の管理者の方向けに、詳細なドキュメントをご提供します。

管理者画面利用ガイド : https://guide.worksmobile.com/jp/admin/admin-guide/
LINE WORKS の管理者が利用する「管理者画面」の利用法や活用法を解説します。

セキュリティ担当者やセキュリティ監査担当者向けの資料

LINE WORKS のセキュリティについて詳細を知りたい方向けに、専門的なドキュメントをご提供しています。

LINE WORKS プライバシーセンター : https://line-works.com/privacycenter/
LINE WORKS のプライバシーポリシーやセキュリティシステムなど、情報セキュリティや個人情報保護に対する LINE WORKS の取り組みに関する情報を公開しています。LINE WORKS が取得している認証の証明書や報告書をダウンロードしていただくことができます。LINE WORKS の管理者であれば、ISO 27000 に準拠した LINE WORKS の管理策 (チェックリスト) をダウンロードすることが可能です。

セキュリティシステムガイド : https://line-works.com/ebook/security-system-guide/

LINE WORKS のコミュニティ

LINE WORKS では、利用者や開発者の方向けにコミュニケーションを行う場を提供します。

LINE WORKS コミュニティ : https://community.worksmobile.com/jp/
LINE WORKS についての質問や活用方法を共有するスペースです。

LINE WORKS Developer コミュニティ : https://forum.worksmobile.com/jp/
LINE WORKS Developers に関して、他の開発者と意見交換や情報共有ができる交流スペースです。

A.2. LINE WORKS のプライバシー窓口

個人情報開示のご請求

LINE WORKS サービスで表示されるメンバー情報 (氏名、電話番号、メールアドレスなど) については、ユーザー企業の LINE WORKS サービスの管理者に管理責任があり、管理者画面で情報修正、削除の操作を行うことができます。管理者権限を持たないメンバーの方は、管理者へのご相談をお願いいたします。管理者からの保有個人情報の開示請求に関するお問い合わせは、LINE WORKS サービスへログインの上、お問い合わせください。
個人情報開示請求の詳細については、LINE WORKS プライバシーセンターの「個人情報の開示請求など」をご参照ください。

個人情報の第三者提供に関するお問い合わせ

LINE WORKS は、プライバシーポリシーに掲げる場合を除き、ユーザーのご関係者又はご関係者に代わり正当な権限がある者より事前の同意を得ないで、個人情報を第三者に提供いたしません。
管理者からの保有個人情報の第三者提供に関するお問い合わせは、LINE WORKS サービスへログインの上、お問い合わせください。
個人情報の第三者提供の詳細については、LINE WORKS プライバシーセンターの「個人情報の第三者提供」をご参照ください。

プライバシーポリシーに関するお問い合わせ

LINE WORKS は、ユーザーの大切な個人情報やプライバシーの保護を最優先としてサービスを運用しています。LINE WORKS のプライベートポリシーの詳細については、「LINE WORKS Pvivacy Center」をご参照ください。
プライバシーポリシーに関するご意見、ご質問、苦情や当社による個人情報取り扱いに関するお問い合わせ、個人情報保護法等に関する対応、その他ご不明な点がある場合は、LINE WORKS のプライバシー窓口までお問い合わせください。
LINE WORKS のプライバシー窓口 : privacy_wm@line-works.com

附録 B: 情報セキュリティや個人情報の保護に関する情報

法令やガイドライン

政府は、企業におけるクラウド活用を推進するとともに、情報セキュリティや個人情報を保護するために、各種の法令やガイドラインを公開しています。

国民のためのサイバーセキュリティサイト :
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/intro/intro.html

クラウドサービス提供における情報セキュリティ対策ガイドライン (第 3 版 : 2021 年 9 月):
https://www.soumu.go.jp/main_content/000771515.pdf

クラウドサービス利用・提供における適切な設定のためのガイドライン (2022 年 10 月):
https://www.soumu.go.jp/main_content/000843318.pdf

政府情報システムのためのセキュリティ評価制度 (ISMAP): https://www.ismap.go.jp/csm

国際標準・公的標準

国際標準化団体や民間団体などが、情報セキュリティや個人情報の保護に関する標準を定め、一定の水準を満たしている企業や組織に認証証明書や報告書を発行しています。

ISO/IEC 27001: https://www.bsigroup.com/ja-JP/ISO27001/
情報セキュリティマネジメントに関する国際標準規格です。
アドオン規格として、以下のような標準規格があります。

- ISO/IEC 27017: https://www.bsigroup.com/ja-JP/ISO27017/
- ISO/IEC 27018: https://www.bsigroup.com/ja-JP/ISO27018/
- ISO/IEC 27701: https://www.bsigroup.com/ja-JP/iso-27701-privacy-information-management/

SOC2: https://www2.deloitte.com/jp/ja/pages/risk/solutions/or/soc2.html
サービス運営組織の総合的な内部統制について一定の基準を満たしていることを評価する国際評価制度です。

APEC 越境プライバシールールシステム (CBPR): https://www.jipdec.or.jp/project/cbpr.html

APEC 域内で越境する個人情報の保護に関する国際認証制度です。

附録 C: ソリューション選定のヒント

C.1. 附録 C の概要

附録 C では、課題解決のためのソリューション (製品など) の選定者を想定読者として、ソリューションの選定において必要な活動について、SaaS サービスを採用するケースを例に解説します。

注釈 | SaaS サービス以外を選択する場合であっても、選定の基本的な流れは同様となります。

SaaS サービスのセキュリティライフサイクルにおいて、選定者は、ソリューションの選定を行い、選定したソリューションを導入担当者に引き継ぎます。ビジネスや業務において発生している課題を認識·分析する「課題分析」を行った結果、その課題の解決に貢献するソリューションの選定を行う場合があります。

注釈 | ソリューションを導入せずに課題を解決できる場合もあるため、必ずしも課題解決にソリューションの導入が必要というわけではありません。

選定者は、このソリューションの選定のための活動を行い、社内承認を得て、ソリューションの導入を決定します。ソリューションが商用ソフトウェアや SaaS サービスの場合は、その利用に関する契約の締結を行います。

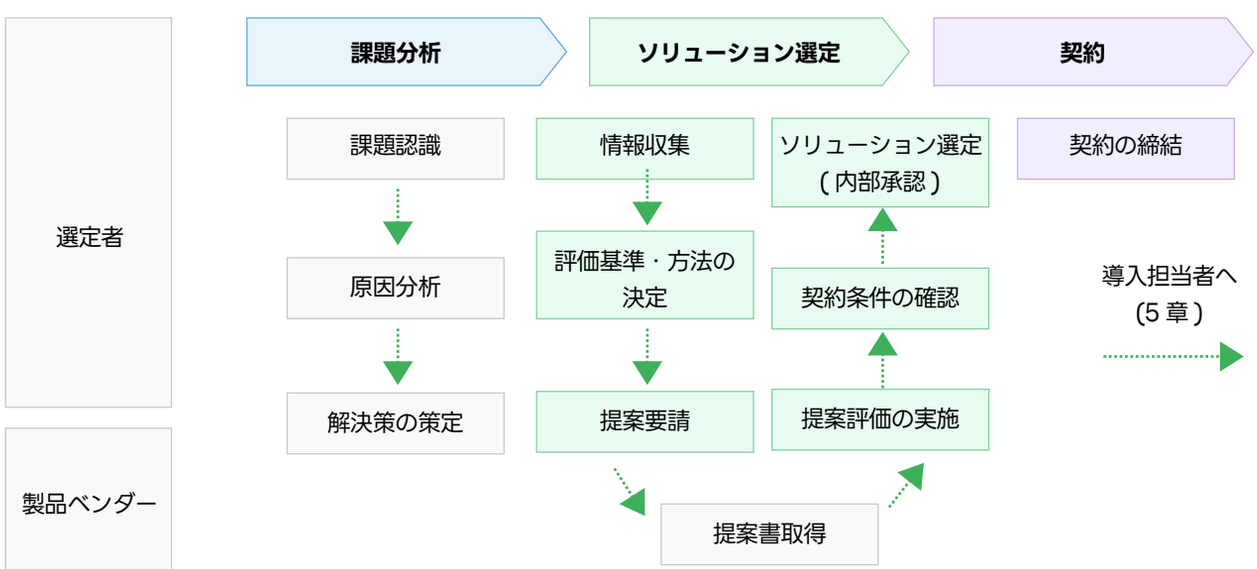


図 ソリューション選定の概要

C.2. 課題分析

ビジネスや業務において課題が発生した場合、以下の流れで課題を分析していきます。

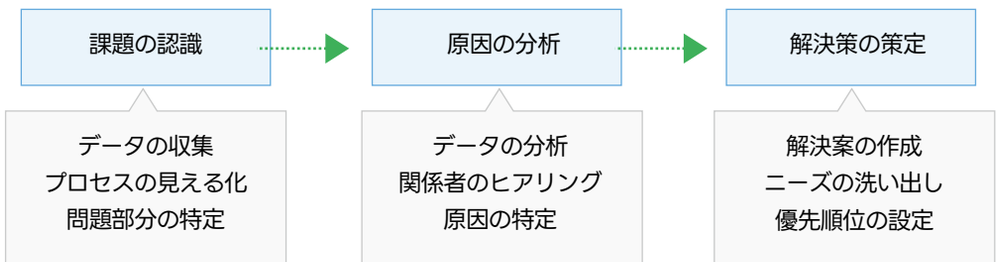


図 . 課題分析の流れ

C.2.1. 課題認識

まず、課題がどんなものであるのか、現状を認識できるように、以下の作業を行います。

1. データの収集

現在のビジネスプロセスや業務プロセスに関するデータを収集します。これにより、現在発生している課題について客観的に議論をすることが可能になります。

2. プロセスの見える化

現在のビジネスプロセスや業務プロセスを視覚化します。フローチャートやプロセス図を作成し、各プロセスで行われていることや、そのプロセスで扱われるデータを明確にします。

3. 問題部分の特定

現在のビジネスプロセスや業務プロセスの中で、非効率やボトルネックになっている部分、ミスや誤りが発生しやすい部分を特定します。

C.2.2. 原因分析

次に、課題認識の結果に対して、以下の原因分析を行います。

1. データの分析

収集したデータを分析し、そのパターンや傾向を基に、課題が発生する根本原因を特定します。

2. 関係者のヒアリング

課題となっているビジネスプロセスや業務プロセスに関わる関係者にヒアリングやアンケートを行い、現場の観点から見た問題点や原因に関する情報を収集します。

3. 原因の特定

データやヒアリングから得られた情報から、各種の分析手法 (QC 七つ道具など) を活用して、根本原因を特定します。

C.2.3. 解決策の策定

最後に、解決策の策定を行います。

1. 解決案の作成

実行可能な解決案を複数作成します。ブレインストーミングなどのディスカッション手法を活用ことは、実行可能な解決案を作成する上で有効です。

2. ニーズの洗い出し

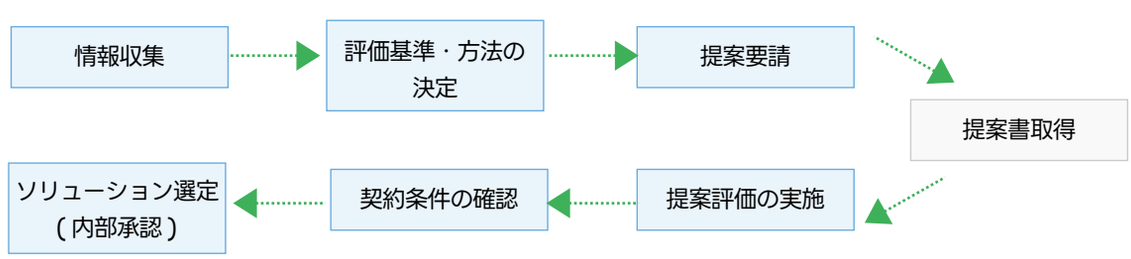
課題が発生しているビジネスプロセスや業務プロセスに関与する人達 (内部関係者、外部関係者などのステークホルダー) から意見を求め、どのような問題をどのように解決すべきかを洗い出します。

3. 優先順位の設定

洗い出されたニーズに対して、優先順位を付けて、最終的な解決策を策定します。全てのニーズを満たすソリューションを見つけることは困難なため、最も重要なニーズを優先して解決策を決定します。

C.3. ソリューション選定

策定した解決策をベースに、その解決策を実現するためのソリューションを選定します。ソリューション選定は、一般的に以下の流れで行います。



C.3.1. 情報収集

策定した解決策に基づき、選択し得るソリューションについて情報を収集します。

1. 利用可能なソリューションのリスト作成

キーワード検索などにより、課題を解決するために選択し得るソリューションの手法や製品のリストを作成します。

2. 各ソリューションの調査

リストに掲載された各ソリューションについて、その概要、主な機能、活用事例などを調査します。

3. トライアル

課題の解決に有効と考えられるソリューションについて、可能であれば一定期間のトライアルを行います。

4. 既存業務やシステムとの相性の確認

トライアルの結果から、既存の業務やシステムに対するインパクトや、親和性を確認します。大きな変化を与えるソリューションは、副作用も大きい場合があるため細心の注意が必要となる場合があります。ソリューションと業務の相性を調べるためには、各ソリューションのユーザ活用事例などが参考になります。

5. 技術評価と価格評価の計画

トライアルの結果から、今回の課題解決における技術評価と価格評価の計画を立案します。
技術評価の計画においては、情報収集しているソリューションのために自社で準備可能な技術水準を決定しておきます。たとえ、すばらしいソリューションであっても、自社の技術水準で手に負えないものは、継続して利用することができません。自社の技術水準を超えるソリューションの導入は、セキュリティ上のリスクになる可能性も高くなります。

6. ソリューション提供元企業の調査

ソリューションとして製品を選定した場合、そのソリューションを長期にわたって利用できるためには、その提供元企業の事業継続性が重要です。取得可能な範囲で、ソリューション提供元企業の情報を収集します。

C.3.2. 評価基準・方法の決定

ソリューションの情報収集を行った後、選定を行う上での評価基準と、評価方法を決定します。
ソリューションの評価においては、「機能」「セキュリティ」「コスト」の 3 つの観点で評価します。ここでは、「機能」「セキュリティ」の 2 つの観点における評価基準と評価方法について解説します。

C.3.2.1 機能に関する評価基準の決定

まず、ソリューションが機能上の要件を満たしているかどうかの基準を決定します。

1. 要求機能のリスト化

解決策において定めたニーズと、情報収集によって得られた各ソリューションの仕様をもとに、評価対象となる機能のリストを作成します。

2. 要求機能に対する優先順位付け

作成した要求機能リストの各機能に対して、優先順位を明記します。

3. 非機能要件の明記

評価対象のソリューションに SaaS などのサービス製品が含まれる場合は、機能以外の要件 (非機能要件) についても評価基準に明記する必要があります。

非機能要件の例として、以下のようなものがあります。

- サービスを利用できる時間や場所などの制約
- 処理速度やレスポンスなどのパフォーマンス
- サービスの可用性
- サービス提供事業者のサポートの体制や質

C.3.2.2 セキュリティに関する評価基準の決定

次に、ソリューションがセキュリティ上の要件を満たしているかどうかの基準を決定します。

1. ソリューションが提供するセキュリティ機能のリスト化

情報収集によって得られた各ソリューションの仕様をもとに、ソリューションが提供するセキュリティ機能のリストを作成します。

セキュリティ機能の例として、以下のようなものがあります。

認証・アクセス制御機能

ユーザー認証の強化機能 (多要素認証など)、アクセス権限の管理機能など

データ暗号化機能

暗号化対象となるデータの種類、データの暗号化方法など

ネットワーク保護機能

ファイアウォール、侵入検知システムなど

データ漏えい防止機能

機密情報の漏えいを防ぐための情報ポリシー機能など

インシデント検知・対応機能

セキュリティ侵害の発生を検知する機能や、対応を支援するための機能など

2. セキュリティ機能に対する優先順位付け

解決策が想定する利用場面を前提として、セキュリティ機能リストの各機能に対して、優先順位を明記します。

3. プライバシーポリシーに対する要件の明記

評価対象のソリューションに SaaS などのサービス製品が含まれる場合は、サービスが提示するプライバシーポリ

シーに関する評価項目を評価基準に明記する必要があります。

4. 個人情報委託に関する評価基準の明記

評価対象のソリューションに対して、個人情報を委託する必要がある場合、セキュリティ要求事項、委託先評価、委託契約の検討、委託フローの整備した上で、個人情報委託先に関する評価項目を評価基準に明記する必要があります。

社内にセキュリティ専門部署が存在する場合や、社外のセキュリティ専門組織の支援を得られる場合は、セキュリティに関する評価基準の決定について、支援を依頼することを推奨します。

C.3.2.3 機能に関する評価方法の決定

機能に関する評価基準を決定した後、その評価方法を決定します。

1. 評価基準によるスコアリング

機能に関する評価は、基本的に、評価基準に定めた事項に対する優先順位によるスコアリングにより行います。

2. ユーザー体験テストによる評価の実施

評価基準だけでは見落されがちな、ユーザーが直接的に得る、以下のような体験による評価を補助的に行います。

- ユーザーインターフェースの使いやすさ
- 他のソリューションとの連携
- カスタマイズ性、など

3. トライアルにおける評価の実施

情報収集段階のトライアルでは確認できなかった機能について、トライアル期間中にあらためて検証をし、その結果により評価を行います。

C.3.2.4 セキュリティに関する評価方法の決定

セキュリティに関する評価基準を決定した後、その評価方法を決定します。

1. 評価基準によるスコアリング

セキュリティに関する評価も、基本的には、評価基準に定めた事項に対する優先順位によるスコアリングにより行います。

2. 実環境におけるセキュリティ評価

評価基準では評価しにくい、実環境での以下のようなセキュリティ評価を補助的に行います。

- セキュリティの専門家による脆弱性評価やコードレビュー
- ペネトレーションテストや脆弱性スキャン

社内にセキュリティ専門部署が存在する場合や、社外のセキュリティ専門組織の支援を得られる場合は、セキュリティに関する評価方法の決定についても、支援を依頼することを推奨します。

C.3.3. 提案要請

決定した機能評価およびセキュリティ評価の基準・方法を基に、解決策を実現するために必要な事項を記述した提案要請書 (RFP: Request for Proposal) を作成し、ソリューション提供元企業もしくはそのパートナーに対して、提案要請を行います。

C.3.4. 提案評価の実施

ソリューション提供元企業もしくはそのパートナーから提案書を受領した後、予め定めた機能評価およびセキュリティ評価の基準・方法に従い、提案に対する評価を行います。

C.3.4.1 機能評価の実施

機能評価の基準・方法に従い、提案に対する機能評価を実施します。

1. 機能評価基準によるスコアリング
2. 補助的な機能評価
   - ユーザー体験テスト
   - トライアルにおける評価
3. 機能に対する総合的な評価

C.3.4.2 セキュリティ評価の実施

セキュリティ評価の基準・方法に従い、提案に対するセキュリティ評価を実施します。

1. セキュリティ評価基準によるスコアリング
2. 補助的なセキュリティ評価
   - 実環境におけるセキュリティ評価 (インストール型ソフトウェアの場合のみ)
3. セキュリティに対する総合的な評価

C.3.5. 契約条件の確認

提案評価の結果、商用のソリューションを採用することが内定した場合、以下を実施します。

1. 利用規約の確認

ソリューション提供元企業との権利義務関係を確認するため、ソリューションの利用規約を確認します。必要に応じて、社内の法務部門などと連携し、リーガルチェックなどを行います。

2. 利用プランの決定

ソリューションがサービスの場合は、利用サービスのプランから、初期導入規模に見合うプランを選択します。

3. 見積書の取得

プランの決定後、ソリューション提供元企業またはそのパートナーから見積書を取得します。また、必要に応じて、社内の会計部門などと連携し、支払い方法の決定を行います。

C.3.6. ソリューション選定 (内部承認)

ソリューションの評価結果、契約条件をもとに稟議書を作成し、ソリューションの選定について社内承認を得ます。
社内承認の取得後、以下を実施します。

1. 契約担当者の指定

社内の調達規程に基づき、ソリューションの契約担当者を指定します。契約担当者は、ソリューション提供元企業もしくはそのパートナーとの間での契約締結を行います。

2. ソリューション管理者の指定

社内の規程に基づき、ソリューションの管理者を指定します。ソリューションの管理者には、一般的に以下の指定が必要になります。

導入担当者

ソリューションの導入作業を担当します。インストール型ソフトウェアの場合はインストールや初期設定を行います。SaaS 型サービスの場合は、初期設定を行います。管理者が兼任することもあります。

管理者

導入完了後、日常的な定常運用やトラブル対応などの非定常運用を担当します。契約更新時に、更新評価および更新手続きもしくは解約手続きを行います。

導入担当者は導入時に、管理者は運用期間中に、ソリューションの管理業務を行うための管理者権限が必要となります。

3. セキュリティ責任者の指定

社内のセキュリティ保護規程に基づき、ソリューションのセキュリティ責任者を指定します。ソリューションのセキュリティ責任者は、ソリューションに関するセキュリティ方針を決定し、ソリューションのセキュリティ運用を継続的にモニタリング·評価する役割を担います。会社全体のセキュリティ責任者がソリューションのセキュリティ責任者になることもあります。
セキュリティ責任者は、ソリューションを情報資産として管理します。ソリューションの稼動開始時に、情報管理台帳にソリューション情報を登録します。

C.4. 契約

契約担当者が、ソリューション提供元企業またはそのパートナーとの間で契約を締結することで、契約上の利用開始期日から正式にソリューションのユーザーとなります。これにより、導入担当者は、ソリューションの導入作業を開始す

ることが可能となります。