運用規定

バージョン: 1.0

改訂日: 2024年4月1日

出力日: 2026年3月5日

目次

1. 組織的対策

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員

1. 情報セキュリティのための組織

役職名	役割・責任	担当
情報セキュリティ責任者	情報セキュリティに関する方針の決定および全体の最終責任を負う	**代表取締役**
情報セキュリティ部門責任者	各業務における情報セキュリティ対策の運用管理および実施責任を負う	**CTO**
システム管理者	情報システムに対する技術的セキュリティ対策の設計・導入・運用	**CTO（兼務）**
インシデント対応責任者	インシデント発生時の影響評価、対応方針の決定および対応の指揮	**CTO**
個人情報保護管理者	個人情報保護法および関連法令の遵守責任	**代表取締役**
個人情報苦情・相談窓口	個人情報に関する苦情・相談の一次対応および社内連携	**営業部責任者**
サポート部責任者	カスタマーサポート業務の管理およびサポート情報の保護責任	**サポート部責任者**
教育責任者	情報セキュリティ教育の企画・実施・記録管理	**管理部責任者（または代表取締役）**
情報セキュリティ共有者	情報セキュリティに関する適時の情報共有	**管理部担当者**
監査・点検責任者	情報セキュリティ関連規程および運用状況の点検・評価	**管理部責任者（または代表取締役）**

重大な情報セキュリティインシデントにおいて、経営判断または対外的対応を要する場合は、情報セキュリティ責任者である代表取締役が最終的な意思決定を行う。

当社では、インシデント発生時に迅速な技術的判断と初動対応が重要であると考えており、システム全体を把握しているCTOをインシデント対応責任者としています。なお、経営判断を要する場合は代表取締役が最終判断を行う体制としています。

2. 情報セキュリティ取組みの監査・点検

監査・点検責任者は、情報セキュリティ関連規程の実施状況について、年1回（8月）点検を行い、監査・点検結果を情報セキュリティ責任者に報告する。内部監査およびマネジメントレビュー（経営確認）は同日に実施し、議事録1本にまとめることができる。なお、内部監査部分については、独立性を確保するため、運用当事者以外の者が担当する。

情報セキュリティ責任者は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

- 情報セキュリティ関連規程が有効に実施されていない場合は、その原因の特定と改善
- 情報セキュリティ関連規程に定められたルールが、対策として不十分または有効でない場合は、情報セキュリティ関連規程の改訂
- 情報セキュリティ関連規程に定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は、情報セキュリティ関連規程の改訂

3. 情報セキュリティに関する情報共有

情報セキュリティ共有者は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時（必要に応じて）入手し、社内で共有する。共有の証跡は、Slack等の社内コミュニケーションツールへの投稿記録をもって代替する。

機密性2以上の情報資産については、管理部責任者の許可を得ること。

専門機関

独立行政法人情報処理推進機構（略称：IPA）

- 情報セキュリティ
- ここからセキュリティ

JVN（Japan Vulnerability Notes）

- JVN

一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）

- JPCERT/CC

個人情報保護委員会

- 個人情報保護委員会

2. 人的対策

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全従業員（取締役、社員、派遣社員、パート・アルバイトを含む）

1. 雇用条件

従業員を雇用する際には秘密保持契約を締結する。

2. 従業員の責務

従業員は、以下を遵守する。

- 従業員は、当社が営業秘密として管理する情報及びその複製物の一切を許可されていない組織、人に提供してはならない。
- 従業員は、当社の情報セキュリティ方針及び関連規程を遵守する。違反時の懲戒については、就業規則に準じる。

  注記: 当社が営業秘密として管理する情報とは、「3 情報資産管理 1.1 情報資産の特定と機密性の評価」および「12. 情報資産の定義と管理ルール」に示す機密性評価値が1以上のものをいう

3. 雇用の終了

- 従業員は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から当社が交付を受けた資料又はそれらの複製物の一切を退職時に返還する。
- 従業員は、在職中に知り得た当社の営業秘密又は業務遂行上知り得た技術的機密を利用して、競合的あるいは競業的行為を行ってはならない。

4. 情報セキュリティ教育

教育責任者は、全従業員を対象として、情報セキュリティに関する教育を実施する。

教育内容には、以下を含むものとする。

- 情報セキュリティ関連規程の説明（入社時および年1回）
- 個人情報の取り扱いに関する留意事項
- 新たな脅威や注意喚起が必要な事項（適時、管理部より共有）

教育の実施記録については、専用の受講台帳を作成せず、以下をもって証跡とする。

- カレンダー招待および参加者記録
- 研修資料のURL
- Slack等での「理解しました」等のリアクションまたは返信

5. 人材育成

教育責任者は、情報セキュリティに関する知識向上のため、必要に応じて外部セミナーの受講や公開情報の活用を行う。

なお、業務上必要と判断した場合には、情報セキュリティに関する資格取得を推奨する。

6. BYOD（私物端末の業務利用）

当社は、情報セキュリティ責任者の承認を得た場合に限り、私物端末（BYOD）の業務利用を認める。

BYODを利用する従業員は、以下を遵守しなければならない。

- 端末には画面ロックおよび適切な認証を設定すること
- 業務情報は、当社が指定するクラウドサービス上でのみ取り扱い、私物端末のローカルストレージには保存しないこと
- 端末の紛失、盗難、マルウェア感染等が疑われる場合は、速やかにインシデント対応責任者へ報告すること
- 退職またはBYOD利用終了時には、当社業務に関連する情報を速やかに削除すること

3. 情報資産管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全社・全従業員

1. 情報資産の管理

1.1 情報資産の特定と機密性の評価

当社事業に必要で価値がある情報および個人情報（以下「情報資産」という）を特定し、「12. 情報資産の定義と管理ルール」に基づき分類・管理する。 情報資産の機密性は、以下の基準に従って評価する。

機密性レベル	基準
機密性3：極秘	法令により安全管理が義務付けられている情報、営業秘密として管理されている情報、漏えいにより取引先または顧客に重大な影響を与える情報
機密性2：社外秘	漏えいにより事業に影響を与える情報
機密性1：公開	漏えいしても事業にほとんど影響がない情報

1.2 情報資産の分類の表示

情報資産の機密性は、以下の方法で表示する。

- 電子データ：保存先の名称またはアクセス権限設定により識別する
- 書類：管理方法または文書への機密性表示により識別する

表示が困難な場合は、保管場所や管理方法により機密性を識別する。

1.3 情報資産の管理責任者

情報資産の管理責任者は、当該情報資産を主に利用する部門の責任者とする。

1.4 情報資産の利用者

情報資産の利用者は、「12. 情報資産の定義と管理ルール」に定められた利用者範囲に従うものとする。

2. 情報資産の社外持ち出し

情報資産を社外に持ち出す場合は、以下を遵守する。

- 機密性2以上の情報資産については、管理責任者の許可を得ること
- 機密性3の情報資産については、情報セキュリティ責任者の許可を得ること
- 電子データは、当社が指定するクラウドサービスを利用して取り扱うこと
- **業務情報を私物端末のローカルストレージへ恒久的に保存することは禁止する**
- **Slack 等の業務上利用を認めたクラウドサービスにより、アプリケーションの仕様上、一時的に端末へ保存されるデータについてはこの限りではない**
- **USBメモリ等の可搬型電子媒体の利用は、情報セキュリティ責任者の許可がある場合を除き禁止する**

2.1 業務上必要な一時的なローカル保存

業務上やむを得ず情報資産を端末のローカルストレージに一時的に保存する場合（例：CSVファイルのアップロード作業、データ加工作業等）は、以下の条件をすべて満たすこと。

条件	内容
目的の限定	クラウドサービスへのアップロードまたはデータ加工等、明確な業務目的がある場合に限る
保存期間	作業完了後、速やかに（原則として当日中に）ローカルから削除すること
端末要件	ディスク暗号化が有効な端末を使用すること
保存場所	ダウンロードフォルダ等、管理しやすい場所に保存し、作業後の削除漏れを防止すること
機密性3の情報	機密性3（極秘）の情報資産を一時保存する場合は、事前に情報セキュリティ責任者の許可を得ること

上記の条件を満たす一時的な保存は、「恒久的な保存」には該当しない。

3. 媒体の処分

3.1 媒体の廃棄

機密性2以上の情報資産を含む媒体を廃棄する場合は、復元できない方法で処分する。

- 書類：細断または溶解処理
- 電子媒体：完全消去または物理破壊

※ OS標準機能による削除や簡易フォーマットは不可とする。

3.2 媒体の再利用

機密性2以上の情報資産を保存していた電子媒体を再利用する場合は、完全消去を行う。

4. バックアップ

4.1 バックアップの取得

システム管理者は、業務上重要なデータについて、定期的にバックアップを取得する。 バックアップは、当社が利用するクラウドサービスまたは当社管理下の環境に保存する。

4.2 バックアップデータの取り扱い

バックアップデータは、適切なアクセス制御の下で管理し、不要となった場合は「3. 媒体の処分」に従い処理する。

4.3 クラウドサービスを利用したバックアップ

クラウドサービスを利用する場合は、情報セキュリティ責任者の承認を得た上で導入する。

4. アクセス制御及び認証

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	情報資産の利用者および情報処理施設

1. アクセス制御方針

社外秘または極秘の情報資産を扱う情報システムおよびクラウドサービスに対するアクセス制御は、以下の方針に基づいて運用する。

- 「12. 情報資産の定義と管理ルール」に定める利用者範囲および業務内容に基づき、必要最低限のアクセス権を付与する
- 不要となったアクセス権は、速やかに削除または無効化する
- 業務上必要な場合を除き、特権的な権限の付与は行わない

2. 利用者の認証

社外秘または極秘の情報資産を扱う情報システムおよびクラウドサービスは、以下の方針に基づいて利用者認証を行う。

- 利用者1名につき1つのアカウントを発行する
- アカウントの共有および複数人による共用を禁止する

3. 利用者アカウントの登録

利用者認証に用いるアカウントは、情報セキュリティ責任者の承認を得た上で登録する。

4. 利用者アカウントの管理

利用者認証に用いるアカウントが不要となった場合、システム管理者は、当該事実を確認後、速やかにアカウントの削除または無効化を行う。

5. パスワードおよび認証情報の管理

利用者認証に用いるパスワードおよび認証情報は、以下を遵守する。

- 推測されにくい十分な強度のものを設定する
- 他者に知られないよう適切に管理する

- サービス側で認証ポリシーが提供されている場合は、それに従う

6. 従業員以外の者に対するアカウント発行

当社従業員以外の者に情報システムまたはクラウドサービスのアカウントを発行する場合は、情報セキュリティ責任者の承認を得た上で、機密保持に関する合意を行う。

7. 端末に関する認証および制御

私物端末（BYOD）を含む端末から情報システムまたはクラウドサービスへアクセスする場合は、以下を遵守する。

- 利用者認証を必須とする
- 端末自体の識別による認証（MACアドレス認証等）は原則として用いない

8. アクセス制御対象情報システムおよび認証方法

8.1 対象情報システム

情報システム・サービス	アクセス制御方法
Microsoft Entra ID	アカウント管理の中心。Google WorkspaceおよびAWS SSOと連携
Google Workspace	Entra IDと連携したsptr.jpドメインのGoogle認証
AWS	Entra IDと連携したAWS SSOによるシングルサインオン
Slack	Google Workspaceアカウントによる認証（SSO）
GitHub	Google Workspaceアカウントによる認証（SSO）
GCP（gryffindor等）	sptr.jp Google認証
業務用SaaS	サービス提供者のユーザー認証

8.2 利用者認証方法

情報システム・サービス	利用者認証方法
Microsoft Entra ID	IDおよびパスワードによる認証
Google Workspace	Entra IDからのアカウント同期による認証
AWS	AWS SSO（Entra ID連携）によるシングルサインオン
Slack・GitHub	Google Workspaceアカウントによるシングルサインオン
GCP	sptr.jpドメインのGoogle認証
業務用SaaS	IDおよびパスワード等による認証

制定日: 2024年4月1日
改訂日: 2024年4月1日

5. 物理的対策

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	全事業所

1. セキュリティ領域の設定

当社が利用する事業所内について、情報資産の重要度に応じて以下のとおりセキュリティ領域を設定する。

レベル1領域（来訪者エリア）

対象エリア: 受付、応接スペース、会議室等、来訪者が立ち入る可能性のあるエリア

項目	内容
利用者	従業員および来訪者
施錠	業務時間外は施錠
設置可能情報機器	プロジェクター、ホワイトボード等
制限事項	社外秘または極秘の情報資産を放置しない
部外者管理	従業員の許可を得て入室
来客用名札	必要に応じて着用
火災対策	消火器設置

レベル2領域（執務エリア）

対象エリア: 執務室等、従業員が主に利用するエリア

項目	内容
利用者	従業員
施錠	最終退室者による施錠
設置可能情報機器	パソコン、複合機、電話機、ネットワーク機器
制限事項	情報機器・情報資産の無断操作および無断持出し禁止
部外者管理	従業員の許可およびエスコートが必要
管理記録	必要に応じて実施
火災対策	消火器設置

※ 当社ではサーバールーム等のレベル3領域は設けない。

2. 関連設備の管理

情報機器および関連設備については、以下を遵守する。

- 業務用機器は従業員の管理下で利用する
- 不要となった機器は速やかに撤去または適切に保管する

3. 来訪者エリアにおける注意事項

レベル1領域（来訪者エリア）では、以下を遵守する。

- 複合機・プリンタに原稿や印刷物を放置しない
- ホワイトボードは利用後に消去する
- 業務上必要がない撮影・録音を禁止する
- 来訪者を確認し、不審な場合は従業員が対応する

4. 搬入物の受け渡し

郵便物および宅配便の受け渡しは、以下の方法で行う。

- 郵便物および宅配便は、従業員が受領し、必要に応じて担当者へ引き渡す

6. IT機器利用

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	業務で利用する情報機器

---

1. 適用区分

本規程における IT機器利用の取扱いは、以下の区分に応じて適用する。

- **一般職**：開発業務に従事しない従業員
- **開発者**：ソフトウェア開発、システム運用等に従事する従業員

---

2. ソフトウェアの利用

2.1 一般職

一般職は、業務上必要なソフトウェアおよび当社が承認したクラウドサービスのみを利用する。 新たにソフトウェアまたはサービスを利用する場合は、システム管理者の承認を得る。

以下に該当するソフトウェアの利用を禁止する。

- 不特定多数のコンピュータ間でファイルを共有するソフトウェア
- 正規ライセンスを取得していないソフトウェア
- 信頼性が確認できない提供元のソフトウェア

2.2 開発者

開発者は、業務遂行に必要な開発ツール、ライブラリ、クラウドサービスを利用できるものとする。 ただし、以下を遵守する。

- 業務目的に限定して利用すること
- 正規ライセンスが必要なものについては、適切に取得されていること
- 不審な提供元のソフトウェアを利用しないこと

---

3. ソフトウェアのアップデート

従業員は、業務で利用する OS、ソフトウェアおよびサービスについて、可能な限り最新の状態で利用する。

---

4. マルウェア対策

従業員は、業務で利用する情報機器において、OSまたは利用するサービスが提供する標準的なセキュリティ対策機能を有効にする。

---

5. IT機器の利用

5.1 一般職

一般職は、以下を遵守する。

- 端末にログイン認証を設定する
- 離席時には端末をロックする
- 業務に不要な設定変更を行わない

5.2 開発者

開発者は、以下を遵守する。

- 端末にログイン認証を設定する
- 離席時には端末をロックする
- 業務に影響を与えない範囲で端末設定を行うことができる

---

6. クリアデスク・クリアスクリーン

6.1 一般職

一般職は、社外秘または極秘の情報資産を含む書類や機器を、利用時以外に机上へ放置しない。

6.2 開発者

開発者は、社外秘または極秘の情報資産を第三者が閲覧できない状態を維持する。

---

7. インターネットおよびオンラインサービスの利用

7.1 一般職

一般職は、業務目的でインターネットおよびオンラインサービスを利用する場合、以下を遵守する。

- 公序良俗に反するサイトへのアクセスを行わない
- 不審なサイトへのアクセスや情報入力を行わない

- 当社が承認したサービスのみを利用する

7.2 開発者

開発者は、業務遂行上必要な範囲でインターネットおよびオンラインサービスを利用できるものとする。 ただし、以下を遵守する。

- 業務に関係のない目的での利用を行わない
- 社外秘または極秘の情報資産は、当社が指定したクラウドサービスでのみ取り扱う

---

8. SNSの利用

従業員は、SNS等において当社の業務に関わる情報を公開してはならない。

7. IT基盤運用管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	クラウドサービスおよびそれに付随する管理対象

1. 管理体制

システム管理者は、IT基盤の運用にあたり、情報セキュリティ対策を考慮してクラウドサービスを選定する。 IT基盤に関する重要な情報セキュリティ対策および仕様については、情報セキュリティ責任者の承認を得る。

2. IT基盤の情報セキュリティ対策

2.1 IT基盤の構成方針

当社のIT基盤は、**クラウドサービスのみで構成するものとし、サーバー等のオンプレミスIT基盤は利用しない。** 業務に必要なIT基盤機能は、クラウドサービスまたはクラウドサービス上で提供される機能を利用して実現する。

なお、業務に付随して利用する**プリンタ、ルーター、アクセスポイント等の周辺機器**については、本項の対象外とする。

2.2 認証情報および設定の管理

IT基盤で利用する管理用アカウントおよび設定は、システム管理者が管理する。 初期設定のままの認証情報は使用せず、適切な設定を行う。

2.3 ネットワークおよび通信

IT基盤における通信は、クラウドサービス提供者が提供する標準的なセキュリティ機能を利用する。

3. IT基盤の運用

システム管理者は、IT基盤の運用にあたり、以下を実施する。

- 管理用アカウントおよび権限の適切な管理
- 不要となったアカウント、設定、サービスの削除または無効化

4. クラウドサービスの導入

IT基盤の一部として新たにクラウドサービスを導入する場合は、システム管理者が当該サービスの情報セキュリティ対策を確認したうえで選定する。 新規導入にあたっては、システム管理者の承認を得る。

5. 脅威および攻撃に関する情報の収集

システム管理者は、クラウドサービス提供者や公的機関等が公開する脅威および攻撃に関する情報を収集し、必要に応じて関係者に共有する。

6. サービスの廃止

IT基盤として利用していたクラウドサービスを廃止する場合は、当該サービス上の業務データおよび認証情報が残存しないよう、適切な措置を講じる。

8. システム開発及び保守

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	当社が独自に開発・運用する情報システム

1. 新規システム開発および改修

当社が独自に情報システムの新規開発または改修を行う場合は、以下の事項を考慮して実施する。

- 対象業務の範囲の整理
- 利用するクラウドサービスおよびソフトウェアの選定
- 情報セキュリティ要件の整理
- 運用および保守を考慮した構成の検討
- バックアップおよび障害発生時の対応方針の検討

2. 脆弱性への対処

情報システムの設計および開発においては、利用するソフトウェア、ライブラリ等に関する脆弱性を識別し、必要な対策を講じる。

脆弱性への対処は、Dependabot、Renovate 等の自動化された仕組みによる更新を基本とし、当該更新の適用および影響確認は、システム管理者またはこれと同等の役割を担う者が行う。

3. 開発環境と運用環境の分離

情報システムの開発および改修は、運用環境とは分離された環境で実施する。

新規開発または改修を行った情報システムについては、システム管理者またはこれと同等の役割を担う者が、必要な情報セキュリティ対策が講じられていることを確認した上で、運用環境へ反映するものとする。

4. 情報システムの保守

情報システムの保守は、原則として当社内で実施する。

当社が利用するソフトウェア、ライブラリ、クラウドサービス等について、既知の脆弱性やサポート終了に関する情報を把握し、必要に応じて対応を行う。

5. 業務委託者の関与

情報システムの開発または保守に業務委託者が関与する場合は、以下を遵守する。

- 秘密保持契約を締結すること
- 当社が指定する開発環境およびクラウドサービスを利用すること
- 必要最小限の権限のみを付与すること
- 不要となったアカウントおよび権限は速やかに削除または無効化すること

6. 情報システムの変更管理

情報システムの仕様、構成または設定に変更を加える場合は、以下を考慮して実施する。

- 変更内容および影響範囲の把握
- 必要に応じたセキュリティ要件の見直し
- 変更後の動作確認

変更内容は、必要に応じて関連する記録に反映する。

9. 委託管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2025.01.15
適用範囲	情報資産を取り扱う業務の委託

1. 委託先の評価

「12. 情報資産の定義と管理ルール」において機密性が1以上の情報資産を取り扱う業務を外部に委託する場合は、委託先の情報セキュリティ対策について、事前に確認を行う。

評価にあたっては、以下の事項を参考とする。

- 情報セキュリティまたは個人情報保護に関する方針を有していること
- 情報資産の取扱いに関する基本的な管理体制を有していること
- 委託業務の内容に応じた情報セキュリティ対策が講じられていること
- AIサービスを利用する委託先の場合、入力データの学習利用に関する利用規約を確認していること

2. 委託先の選定

委託先の選定は、前項の確認結果に基づき行い、情報セキュリティ責任者の承認を得る。

3. 委託契約の締結

委託業務を行うにあたり、委託先との契約書または覚書等に、以下の事項を明記する。

- 当社の社外秘または極秘の情報資産および個人情報に関する守秘義務
- 再委託に関する取扱い
- 事故発生時の報告および責任分担
- 委託業務終了時の情報資産および個人情報の返却、廃棄または消去

4. 委託先の管理

委託開始後は、委託先との連絡および業務内容の確認を通じて、情報セキュリティ上の問題がないことを確認する。

委託先における情報セキュリティ対策に重大な不備が認められた場合は、必要な是正措置を求める。

なお、委託先のセキュリティ対策状況の確認は、公開情報（SOC2/ISO認証、プライバシーポリシー、DPA等）、契約条項、および実運用における連絡により代替し、個別のセキュリティ対策確認チェックリストは作成しない。契

約内容の確認および管理はクラウド契約管理サービス（Money Forward クラウド契約）を用いて実施する。

5. 再委託

委託先が当社から受託した業務を第三者に再委託する場合は、事前に当社へ報告し、情報セキュリティ責任者の承認を得るものとする。

再委託にあたっては、委託先と同等の情報セキュリティ管理が行われることを求める。

10. 情報セキュリティインシデント対応及び事業継続管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	情報資産および当社が保有・管理する個人データに関わる情報セキュリティインシデント

1. 対応体制

情報セキュリティインシデントが発生、または発生のおそれがある場合には、以下の体制で対応する。

役割	担当
最終責任者	代表取締役
インシデント対応責任者	情報セキュリティ責任者またはこれと同等の役割を担う者
初動対応者	発見者、またはシステム管理・運用に関与する者

※少人数体制を前提とし、同一人物が複数の役割を兼務することを妨げない。

2. インシデントの影響レベルと対応区分

インシデントの影響範囲に応じ、以下のレベルに区分して対応する。

レベル	内容	主な対応責任者
レベル3	顧客・取引先・社会に影響が及ぶ可能性がある事象 個人情報の漏えい・不正利用が発生または強く疑われる場合	代表取締役
レベル2	事業継続やサービス提供に影響が及ぶ事象	インシデント対応責任者
レベル1	社内業務に限定した影響が生じる事象	インシデント対応責任者
レベル0	直ちに被害はないが、将来的なインシデントにつながるおそれがある事象	システム管理・運用担当者

3. 連絡および報告

レベル1以上のインシデントが発生した場合、発見者は速やかにインシデント対応責任者へ報告する。 必要に応じて、代表取締役へエスカレーションを行う。

※連絡手段は、社内で通常使用しているチャットツール、電子メール、電話等、即時性の高い手段を用いる。

4. インシデント対応の基本方針

インシデント対応にあたっては、以下を基本方針とする。

- 被害拡大の防止を最優先とする
- 事実関係の把握と記録を行う
- 必要に応じて影響範囲・原因・再発防止策を整理する
- 外部への報告・公表は、代表取締役の判断のもとで行う

---

5. インシデント種別と初動対応

5.1 情報漏えい・流出・不正利用

例：

- 個人情報や社外秘情報の外部流出
- クラウドサービス設定不備による公開
- 不正アクセスによる情報取得

初動対応

- 関係するアカウント・アクセス権の一時停止
- 流出範囲・影響範囲の確認
- インシデント対応責任者への即時報告

5.2 改ざん・消失・サービス停止

例：

- データの意図しない削除・改変
- クラウドサービス障害による業務停止

初動対応

- サービス状況・障害範囲の確認
- バックアップからの復旧検討
- 利用者への影響がある場合は社内共有

5.3 マルウェア・不正プログラム感染

例：

- ランサムウェア
- 不正なブラウザ拡張・スクリプト

初動対応

- 該当端末・アカウントの利用停止
- ネットワーク・クラウドアクセスの遮断
- 利用中サービスへの影響確認

---

6. 外部機関への報告・相談

インシデントの内容に応じて、以下への報告・相談を検討する。

- 独立行政法人 情報処理推進機構（IPA）
- 個人情報保護委員会

報告の要否およびタイミングは、法令および事案の重大性を踏まえ、代表取締役が判断する。

---

7. 事業継続管理（BCPの考え方）

当社は、クラウドサービスを前提とした事業運営を行っているため、以下を基本方針とする。

- 重要システムはクラウドサービスの冗長性・バックアップ機能を活用する
- 単一人物・単一環境に依存しない運用を心がける
- 重大インシデント発生時は、復旧よりも安全確保と影響最小化を優先する

---

8. インシデント管理方法

情報セキュリティインシデントは、YouTrack にチケットとして登録し、対応状況および対応履歴を管理する。

---

9. 事後対応および再発防止

インシデント収束後、必要に応じて以下を実施する。

- 原因および対応内容の整理
- 再発防止策の検討・実施
- 社内ルールや運用の見直し

※過度な文書化や形式的な報告を目的とせず、実効性のある改善を重視する。

補足（この規程の位置づけ）

本規程は、**迅速な初動対応と実運用での判断を妨げないこと** を目的とする。 緊急時には、本規程の記載に拘泥せず、被害拡大防止を最優先に行動する。

11. テレワークにおける対策

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2024.04.01
適用範囲	テレワーク勤務者

1. テレワーク共通ルール

1.1 テレワークで利用する情報システム

テレワークを実施する際には、当社が業務利用を認めたクラウドサービスおよび情報システムを利用する。新たな情報システムまたはサービスを業務で利用する場合は、システム管理者の承認を得る。

1.2 テレワークで利用する機器

テレワークで業務を行う際には、以下の情報機器を利用することができる。

情報機器	利用条件
パソコン	社有機器または私有機器（BYOD）
スマートフォン・タブレット	社有機器または私有機器（BYOD）
USBメモリ・外付けHDD	原則利用禁止（情報セキュリティ責任者の許可がある場合を除く）

1.3 テレワーク時のシステム利用方針

テレワークにおける業務は、原則としてクラウドサービスを直接利用する方式とする。業務情報を端末のローカルストレージに恒久的に保存することは禁止する。

業務上やむを得ず一時的にローカルストレージに保存する場合は、「3. 情報資産管理」の「2.1 業務上必要な一時的なローカル保存」に定める条件に従うこと。

2. 情報機器のセキュリティ

2.1 共通事項

テレワークで業務に利用する情報機器について、以下を遵守する。

- 端末にはログイン時の認証（パスワード、生体認証等）を設定する
- OSおよび主要ソフトウェアは可能な限り最新の状態を維持する
- 不審なソフトウェアやアプリケーションをインストールしない

2.2 私有機器（BYOD）を利用する場合

私有機器を業務に利用する場合は、以下を遵守する。

- 端末は本人のみが利用する
- 脱獄・root化等の不正な改造を行わない
- 業務情報は当社が指定するクラウドサービス上でのみ取り扱う

3. ネットワーク利用時の注意

テレワーク時のネットワーク利用にあたっては、以下を遵守する。

- 自宅等のネットワークでは、第三者が容易に接続できない設定とする
- 公衆Wi-Fi利用時は、業務上重要な情報の入力や表示に注意する

4. 勤務中のルール

4.1 端末操作

- 離席時には端末をロックする
- 他者（家族を含む）に業務用端末やアカウントを操作させない

4.2 クラウドサービス・SNSの利用

- 業務データの保存・共有は、当社が認めたクラウドサービスのみを利用する
- 当社の業務や顧客に関する情報をSNS等に公開しない

4.3 外出時の注意

- 必要な情報以外は持ち出さない
- 端末や書類は常に管理可能な状態を保つ

5. データおよび書類の取扱い

5.1 電子データ

- 業務データはクラウドサービス上で管理する
- 不要となったデータは速やかに削除する

5.2 書類・物理媒体

- 秘密情報または個人情報を含む書類は、第三者が閲覧できないよう管理する
- 不要となった書類は、復元できない方法で廃棄する

6. インシデント発生時の対応

テレワーク中に情報セキュリティインシデントまたはそのおそれがある事象を発見した場合は、速やかにインシデント対応責任者またはシステム管理者へ報告する。

12. 情報資産の定義と管理ルール

作成者: 情報セキュリティ委員会

1. 目的

本規程は、当社が保有・管理する情報資産の定義、分類基準、および管理ルールを定めることにより、情報資産の適切な保護を確実にすることを目的とする。

当社では、個別の情報資産を台帳形式で管理するのではなく、情報資産の定義と管理ルールを明確にすることで、クラウド/SaaS環境における実効性のある情報セキュリティ管理を実現する。

2. 情報資産の定義

2.1 情報資産とは

当社事業に必要で価値がある情報および個人情報を「情報資産」と定義する。情報資産には以下が含まれる。

資産種別	具体例
電子データ	データベース、ファイル、ソースコード、設計書等
紙文書	契約書原本、設計図、報告書等
電子媒体	USBメモリ、CD/DVD、外付けHDD等
情報機器	サーバー、パソコン、スマートフォン等
ソフトウェア	アプリケーション、OS等
クラウドサービス上のデータ	SaaS、IaaS、PaaS上に保存されるデータ

2.2 情報資産の所在

当社の情報資産は、主に以下の場所に保管される。

保管場所の種類	具体例
クラウドストレージ	Google Workspace 共有ドライブ
クラウドデータベース	Cloud SQL、Amazon RDS
SaaSサービス	GitHub、Zoho CRM、Money Forward、Slack等
物理的保管場所	バックオフィス金庫（契約書原本等）

3. 機密性レベルの定義

情報資産の機密性は、以下の3段階で分類する。

レベル	分類	定義	具体例
3	極秘	法律で安全管理が義務付けられている情報、守秘義務の対象、限定提供データ、営業秘密、または漏えいにより取引先・顧客に重大な影響を与える情報	顧客情報、従業員情報、ソースコード、契約書
2	社外秘	漏えいにより事業に大きな影響を与える情報	財務諸表、社内規程、営業先情報
1	公開	漏えいしても事業にほとんど影響がない情報	会社案内、公開Webサイトの情報

4. 管理ルール

4.1 機密性レベル別の管理ルール

管理項目	極秘（3）	社外秘（2）	公開（1）
アクセス権限	業務上必要な従業員のみ	関係部門の従業員	全従業員
社外持ち出し	情報セキュリティ責任者の許可必須	管理責任者の許可必須	制限なし
保管場所	当社指定のクラウドサービスまたは施錠管理	当社指定のクラウドサービス	制限なし
廃棄方法	復元不可能な方法で処分	復元不可能な方法で処分	通常廃棄可
暗号化	必須（保存時・転送時）	推奨	不要

4.2 アクセス制御の原則

情報資産へのアクセスは、以下の原則に基づいて管理する。

- 最小権限の原則：業務上必要な最低限の権限のみを付与する
- Need-to-know：知る必要がある者のみがアクセスできる
- 職務分離：相反する権限は分離する
- デフォルト拒否：明示的に許可されない限りアクセスを拒否する

4.3 利用者範囲の決定

情報資産の利用者範囲は、以下の基準に基づいて決定する。

情報の種類	利用者範囲
顧客情報・個人情報	業務上必要な従業員のみ
人事・給与情報	バックオフィス担当者
財務情報	バックオフィス担当者、経営層
ソースコード	開発チーム
営業情報	営業チーム、経営層
社内規程	全従業員

5. 管理責任

5.1 情報セキュリティ責任者

- 本規程の策定・改訂
- 機密性レベルの最終判断
- 極秘情報の社外持ち出し承認

5.2 各部門責任者

- 所管する情報資産の管理
- 利用者範囲の設定・見直し
- 社外秘情報の社外持ち出し承認

5.3 システム管理者

- クラウドサービスの権限設定
- アクセスログの管理
- 技術的セキュリティ対策の実施

6. 情報資産の識別方法

6.1 電子データの識別

電子データの機密性は、以下の方法で識別する。

- クラウドサービスの共有ドライブ名・フォルダ構成による識別
- ファイル名またはメタデータによる識別
- アクセス権限設定による識別

6.2 紙文書の識別

紙文書の機密性は、以下の方法で識別する。

- 文書への機密性表示（極秘、社外秘等）
- 保管場所による識別（施錠キャビネット、金庫等）

7. 見直し

本規程は、年1回、または以下の事象が発生した場合に見直す。

- 新たな種類の情報資産の取り扱い開始
- 大規模なシステム構成変更
- 情報セキュリティインシデントの発生
- 法令・規制の変更

承認

役職	氏名	承認日	署名
情報セキュリティ責任者	代表取締役	2024.04.01	

13. SaaS導入・シャドーIT管理

作成者: 情報セキュリティ委員会

項目	内容
改訂日	2025.01.15
適用範囲	全社・全従業員

1. 目的

本ガイドラインは、業務で利用するSaaS等のクラウドサービスの導入フローを定め、シャドーITを防止することを目的とする。

2. シャドーITの禁止

当社では、情報セキュリティ責任者の承認を得ていないクラウドサービス（シャドーIT）の業務利用を禁止する。

シャドーITとは、組織が把握・承認していない情報システムやサービスを、従業員が独自に業務で利用することをいう。

3. 新規SaaSの導入

新規にSaaSを業務で利用する場合は、情報セキュリティ責任者に確認する。

情報セキュリティ責任者は、公開されているセキュリティ情報（第三者認証、プライバシーポリシー、利用規約等）を確認し、利用の可否を判断する。個別のセキュリティ対策確認チェックリストは作成しない。

情報セキュリティ責任者が把握しているSaaSが、業務利用を認められたサービスとなる。

4. SaaSの利用

情報セキュリティ責任者が把握しているSaaSについては、各従業員が業務上必要な範囲で利用することができる。

5. AIサービスの利用

5.1 AIサービスへの入力禁止データ

以下のいずれかに該当するAIサービス以外を利用する場合、下記のデータを入力してはならない。

- 学習へのデータ利用をオプトアウトした企業契約のAIサービス
- 当社側でホスティングしているAIサービス

分類	具体例
個人情報	氏名、住所、電話番号、メールアドレス、生徒情報、顧客情報等
認証情報・シークレット	パスワード、APIキー、アクセストークン、秘密鍵、接続文字列等
機密性2以上の情報資産	社外秘または極秘に分類される業務情報

5.2 AIサービス導入時の確認事項

AIサービスを新規に導入する場合は、情報セキュリティ責任者が以下の事項を確認する。

- 利用規約における入力データの学習利用に関する条項
- 学習へのデータ利用をオプトアウトする方法の有無
- データの保存・処理に関するセキュリティ対策

6. SaaSの見直し

業務で利用しているSaaSについては、以下の場合に見直しを行う。

- サービス提供者において重大なセキュリティインシデントが発生した場合
- サービスの仕様に重大な変更があった場合
- 利用継続の必要性がなくなった場合

形式的な定期レビューは実施しない。問題がなければ利用を継続し、上記の事象が発生した場合に再評価を行う。

関連文書

- 7. IT基盤運用管理
- 9. 委託管理
- 11. テレワークにおける対策

14. 情報セキュリティリスクアセスメント

作成者: 情報セキュリティ委員会

1. 目的

本書は、「12. 情報資産の定義と管理ルール」に基づき、当社が保有・管理する主要な情報資産に関する情報セキュリティリスクを識別・評価し、適切なリスク対応方針を定めることを目的とする。

本リスクアセスメントは、組織規模および実運用を踏まえて実施し、過度な形式主義に陥らず、実効性を重視する。

1.5 実施手順

1.5.1 実施の契機・頻度

本リスクアセスメントは、以下の契機で実施する。

契機	頻度	備考
定期実施	年1回（8月のマネジメントレビュー前）	内部監査と同時期に実施
臨時実施	随時	下記の事象発生時

臨時実施の契機：

- 新たな重要情報資産の追加
- 大規模なシステム構成変更（クラウドサービスの追加・変更、ネットワーク構成の変更等）
- 情報セキュリティインシデントの発生
- 法令・規制要件の重大な変更
- 事業環境の大幅な変化

1.5.2 役割と責任

役割	担当者	責任
実施責任者	情報セキュリティ責任者（代表取締役）	アセスメント全体の統括、最終承認
実施担当者	情報セキュリティ委員会	アセスメントの実施、報告書作成
資産オーナー	各情報資産の管理責任者	資産情報の提供、脅威・脆弱性の確認

1.5.3 入力情報

リスクアセスメントの実施にあたり、以下の情報を収集・参照する。

- 情報資産台帳（「12. 情報資産の定義と管理ルール」に基づく）
- ネットワーク構成図
- システム構成情報（クラウドサービス一覧、SaaS利用状況）
- 委託先一覧
- 過去のインシデント記録
- 前回のリスクアセスメント結果
- 外部脅威情報（IPAセキュリティ情報、クラウドベンダーのセキュリティ情報等）

1.5.4 実施ステップ

リスクアセスメントは以下のステップで実施する。

ステップ1：対象資産の選定

- 情報資産台帳から、機密性レベル1以上の資産を抽出
- 事業影響の観点から重要度が高い資産を選定
- 新規追加・変更のあった資産を確認

ステップ2：脅威・脆弱性の洗い出し

- 各資産に対する想定脅威を識別（不正アクセス、情報漏えい、改ざん、可用性喪失等）
- 脅威を実現しうる脆弱性を識別（技術的脆弱性、人的脆弱性、物理的脆弱性）
- 過去のインシデント、外部脅威情報を参考に更新

ステップ3：影響度・発生可能性の評価

- 「3. リスク評価基準」に基づき、各リスクの影響度（1〜3）を評価
- 同基準に基づき、発生可能性（1〜3）を評価
- 評価根拠を記録

ステップ4：リスク値算出と判定

- リスク値 ＝ 影響度 × 発生可能性 を算出
- リスクレベル判定基準に基づき、高（6〜9）/中（3〜4）/低（1〜2）を判定

ステップ5：リスク対応方針の決定

- 各リスクに対し、以下のいずれかの対応方針を決定
  - **低減**：管理策を適用してリスクを許容可能なレベルまで低減
  - **受容**：リスクが許容範囲内であり、追加対策を行わない
  - **回避**：リスク源となる活動を中止または変更
  - **移転**：保険加入や外部委託によりリスクを移転
- 「高」判定のリスクは原則として低減または回避を選択

ステップ6：結果の承認とリスク対応計画

- 実施担当者がアセスメント結果を報告書として取りまとめ

- 情報セキュリティ責任者が結果を確認・承認
- 追加の管理策が必要な場合は、リスク対応計画を起票し、実施期限・担当者を明確化

1.5.5 変更管理

評価方法（基準、スコアリング方法等）を変更する場合は、以下を遵守する。

- 変更理由を文書化し、情報セキュリティ責任者の承認を得る
- 変更前後の評価結果の比較可能性を確保するため、変更内容と影響を記録
- 変更履歴を本文書の改訂履歴として管理

1.5.6 成果物

本リスクアセスメントの成果物は以下のとおり。

成果物	内容	保管場所
リスクアセスメント報告書	本文書（「4. リスクアセスメント結果」以降）	ISMS文書管理システム
リスク対応計画	追加管理策が必要な場合に作成	YouTrack（チケット管理）

2. 対象範囲

以下の情報資産のうち、機密性および事業影響の観点から重要度が高いものを対象とする。

- IA-001：顧客基本情報（Cloud SQL / Amazon RDS）
- IA-001-2：顧客管理資料（Google Workspace 共有ドライブ）
- IA-002：従業員情報
- IA-004：ソースコード（GitHub）
- IA-007：営業情報（Zoho CRM）
- IA-008：契約書原本（Money Forward / 紙原本）
- IA-009：カスタマーサポート情報（Zendesk）
- IA-010：分析データ（BigQuery）

3. リスク評価基準

3.1 影響度（Impact）

レベル	定義
3	法令違反、個人情報漏えい、取引先・顧客への重大な影響が発生する
2	事業運営に支障が生じる、信用低下が発生する
1	社内業務への限定的な影響にとどまる

3.2 発生可能性（Likelihood）

レベル	定義
3	過去事例や構成上、発生の可能性が高い
2	一定の条件下で発生する可能性がある
1	発生可能性は低い

3.3 リスクレベル

リスクレベル ＝ 影響度 × 発生可能性

リスク値	判定
6〜9	高（要対応）
3〜4	中（管理策により低減）
1〜2	低（受容）

4. リスクアセスメント結果

資産ID	情報資産	想定脅威	脆弱性	影響度	発生可能性	リスク値	判定	主な管理策	対応方針
IA-001	顧客基本情報（Cloud SQL / Amazon RDS）	不正アクセス、設定不備による情報漏えい	権限設定ミス、認証情報の不適切管理	3	2	6	高	DBはインターネット非公開、アプリ経由アクセス、権限管理、監査ログ	低減
IA-001-2	顧客管理資料（Google Workspace 共有ドライブ）	誤共有、内部不正、操作ミス	人為的ミス、共有設定の誤り	3	2	6	高	共有ドライブ権限管理、管理者限定、定期的な権限確認	低減
IA-002	従業員情報	内部不正、情報漏えい	人的要因、誤操作	3	1	3	中	アクセス権限定、バックオフィス管理、退職時アカウント無効化	低減
IA-004	ソースコード（GitHub）	不正アクセス、情報漏えい	権限過多、認証情報漏えい	3	2	6	高	組織管理、リポジトリ権限管理、SSO、監査ログ	低減
IA-007	営業情報（Zoho CRM）	不正閲覧、情報漏えい	権限設定ミス	2	2	4	中	営業部のみアクセス可能、ロール・権限管理、退職者アカウント無効化	低減
IA-008	契約書原本（Money Forward / 紙）	情報漏えい、紛失	人為的ミス、物理的管理不備	3	1	3	中	電子契約の権限管理、金庫管理	低減
IA-009	カスタマーサポート情報	不正アクセス、顧客情報漏えい	権限設定ミス、認証情報の不適	3	2	6	高	サポート部のみアクセス可能、ロール・権限管理、SSO連携、	低減

資産ID	情報資産	想定脅威	脆弱性	影響度	発生可能性	リスク値	判定	主な管理策	対応方針
	（Zendesk）		切管理					監査ログ、退職者アカウント無効化	
IA-010	分析データ（BigQuery）	不正アクセス、データ漏えい、クエリ結果の不正取得	IAM権限設定ミス、データセットアクセス制御不備	3	2	6	高	IAMによる権限管理、データセット権限設定、監査ログ、VPC Service Controls	低減

5. リスク対応の総括

本アセスメントにおいて「高」と判定されたリスクについては、いずれも既存の技術的・組織的管理策により低減可能であり、現行の運用を継続する。

追加の重大なリスク対応措置は不要と判断するが、以下については継続的に確認を行う。

- クラウドサービスの権限設定
- 退職者・役割変更時のアカウント管理
- 共有ドライブおよびSaaSの利用状況

6. 見直し

本リスクアセスメントは、年1回、または以下の事象が発生した場合に見直す。

- 新たな重要情報資産の追加
- 大規模なシステム構成変更
- 情報セキュリティインシデントの発生

承認

役職	氏名	承認日	署名
情報セキュリティ責任者	代表取締役	2024.04.01	

情報セキュリティ基本方針

作成者: 情報セキュリティ委員会

1. 目的

本方針は、当組織における情報資産の機密性、完全性、可用性を維持し、適切な情報セキュリティ管理を実現することを目的とする。

2. 適用範囲

本方針は、当組織のすべての役員、従業員、契約社員、派遣社員、および当組織の情報資産を取り扱うすべての者に適用される。

3. 基本方針

3.1 情報資産の保護

当組織は、保有するすべての情報資産を適切に分類し、その重要度に応じた管理策を講じる。

3.2 法令遵守

当組織は、情報セキュリティに関連する法令、規制、契約上の義務を遵守する。

主な関連法令：

- 個人情報保護法
- 不正アクセス禁止法
- 電子署名法
- サイバーセキュリティ基本法

3.3 継続的改善

当組織は、情報セキュリティマネジメントシステムを継続的に改善し、セキュリティレベルの向上に努める。

3.4 教育・訓練

当組織は、すべての従業員に対して、情報セキュリティに関する適切な教育・訓練を実施する。

教育内容：

- 情報セキュリティの基礎知識
- 組織の情報セキュリティポリシー

- セキュリティインシデントの報告手順
- ソーシャルエンジニアリング対策

3.5 インシデント対応

当組織は、情報セキュリティインシデントが発生した場合、迅速かつ適切に対応する体制を整備する。

4. 責任

4.1 情報セキュリティ管理責任者

情報セキュリティ管理責任者は、本方針の実施および維持に責任を負う。

4.2 部門責任者

各部門の責任者は、所管する情報資産の適切な管理に責任を負う。

4.3 従業員

すべての従業員は、本方針を遵守し、情報セキュリティの維持に協力する義務を負う。

5. 見直し

本方針は、少なくとも年1回見直しを行い、必要に応じて改訂する。

🚀ヒント

方針の見直しは、内部監査の結果、セキュリティインシデントの発生、法令の改正などを考慮して実施します。

6. 罰則

本方針に違反した場合、就業規則に基づき、懲戒処分の対象となる場合がある。

制定日: 2024年1月15日
承認者: 代表取締役

ISMS学習フォーム

作成者: 情報セキュリティ委員会

1. 概要

本フォームは、従業員の情報セキュリティに関する理解度を確認するためのものである。ISMSの基本的な知識について選択式の問題に回答し、学習の証跡として記録する。

2. 実施要領

項目	内容
対象者	全従業員
実施頻度	年1回（入社時および定期実施）
形式	Google Forms（選択式・自動採点）
所要時間	約5分

3. フォームの内容

以下のトピックについて、選択式で出題される。

- ISMSの基本概念（情報セキュリティの3要素）
- 組織体制（情報セキュリティ責任者）
- 情報資産の分類と管理
- インシデント対応の基本
- テレワーク時の情報取扱い

4. 回答データの管理

項目	内容
保存先	Google Sheets（Google Workspace 共有ドライブ内）
アクセス権限	情報セキュリティ委員会および管理責任者
保存期間	最低3年間
機密性レベル	レベル2（社外秘）

5. フォーム定義の管理

フォームの問題内容はYAML形式で本リポジトリ内（`forms/definitions/`）で管理されている。変更はPRレビューを経て反映される。

6. 関連規程

- 2. 人的対策 - 情報セキュリティ教育
- 12. 情報資産の定義と管理ルール - 情報資産の管理

制定日: 2026年2月25日

ネットワーク構成図

作成者: 情報セキュリティ委員会

1. 概要

本文書は、当組織のネットワーク構成および外部サービスへの接続状況を示すものである。

1.1 用語定義

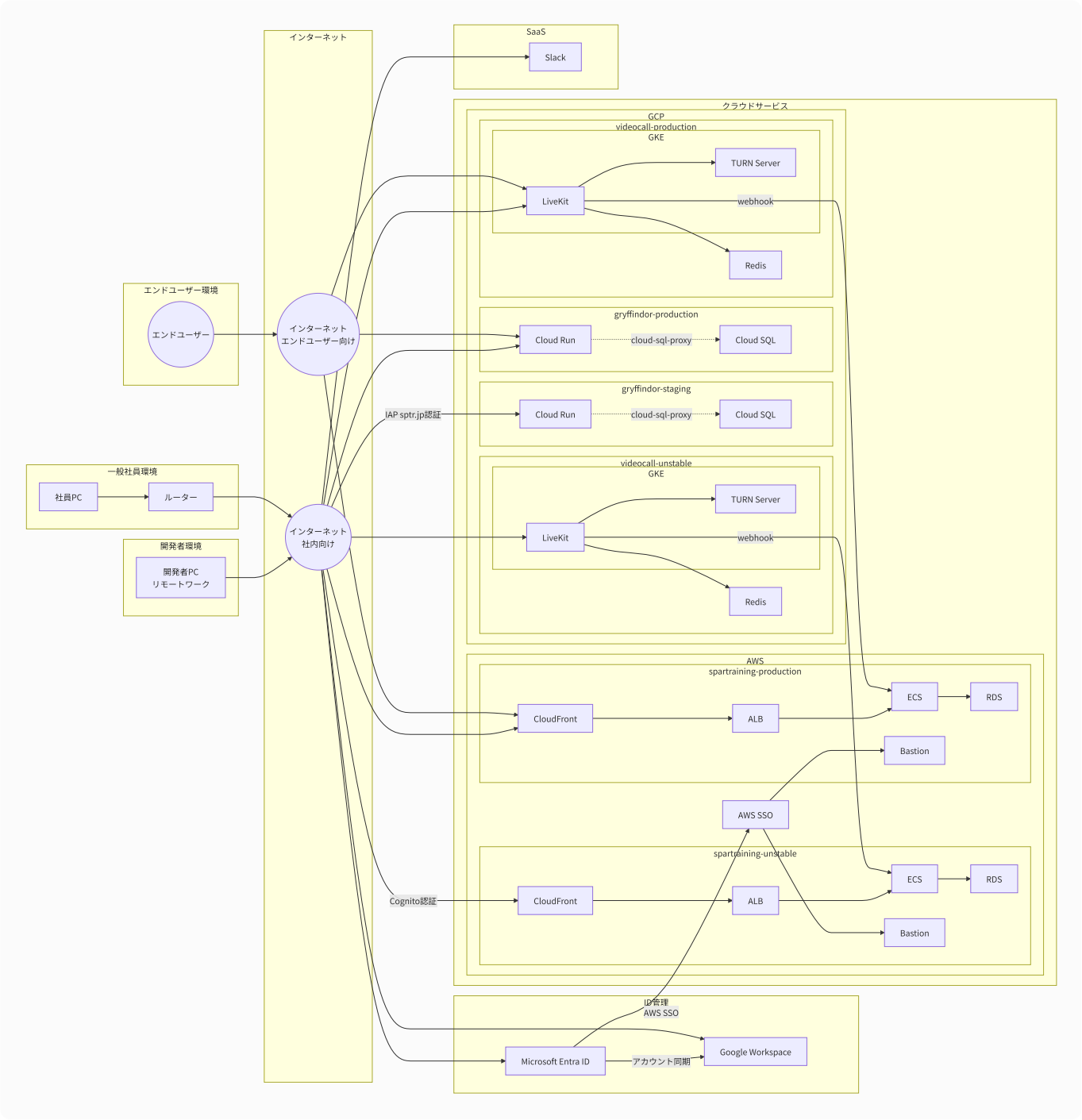
用語	説明
spartraining	スパトレオンライン英会話アプリケーション
gryffindor	スパトレAI英会話アプリケーション
videocall	スパトレビデオ通話基盤（LiveKit）

1.2 エンドユーザーのアクセス

エンドユーザーはproduction環境にのみ接続する。unstable/staging環境は開発・テスト用途であり、エンドユーザーからのアクセスは想定していない。

2. ネットワーク構成図

注記: 図中のインターネット（社内向け/エンドユーザー向け）は、技術的には同一のインターネットである。図ではアクセスの流れをわかりやすくするために2つに分けて表現している。



3. 構成要素

3.1 開発者環境

構成要素	説明
開発者PC	開発者が業務に使用する端末。全員リモートワーク

3.2 一般社員環境

構成要素	説明
社員PC	一般社員が業務に使用する端末

構成要素	説明
ルーター	社内ネットワークとインターネットを接続

3.3 ID管理

サービス	説明
Microsoft Entra ID	アカウント管理の中心。Google WorkspaceおよびAWS SSOと連携
Google Workspace	Entra IDと連携し、sptr.jpドメインのGoogle認証を提供
AWS SSO	Entra IDと連携し、AWSリソースへのシングルサインオンを提供

3.4 spartraining（AWS）

spartrainingはunstable環境とproduction環境の2環境があり、ネットワーク的に完全に分離されている。

環境	構成	認証
unstable	CloudFront → ALB → ECS → RDS	Cognito認証あり
production	CloudFront → ALB → ECS → RDS	-

各環境の特徴は以下の通り。

構成要素	説明
CloudFront	CDNおよびエッジロケーション
ALB	Application Load Balancer
ECS	コンテナ実行環境
RDS	データベース。インターネットからの直接アクセス不可
Bastion	踏み台サーバー。AWS SSO経由のSSHでアクセス。ポートは閉じており、インターネットには面していない

3.5 gryffindor（GCP）

gryffindorはstaging環境とproduction環境の2環境があり、完全に別プロジェクトとしてネットワーク的に分離されている。

環境	構成	認証
staging	Cloud Run → Cloud SQL	sptr.jp Google認証
production	Cloud Run → Cloud SQL	なし（直インターネット）

構成要素	説明
Cloud Run	サーバーレスコンテナ実行環境
Cloud SQL	データベース。cloud-sql-proxy経由でのみアクセス可能。インターネットには面していない

3.6 videocall（GCP）

videocallはスパトレのビデオ通話基盤であり、LiveKitを使用している。GCPのpromising-lampプロジェクトでGKE上に構築されている。unstable環境とproduction環境の2環境があり、それぞれ別クラスタとしてネットワーク的に分離されている。

環境	構成	説明
unstable	GKE → LiveKit → Redis	開発・テスト環境
production	GKE → LiveKit → Redis	本番環境

構成要素	説明
GKE	Google Kubernetes Engine。LiveKitをホスト
LiveKit	WebRTCベースのビデオ通話サーバー
Redis	LiveKitの状態管理用
TURN Server	NAT越えのためのTURNサーバー（turn.rtc.sptr.jp）

spartrainingとの連携として、production環境からspartraining productionへwebhookで通知を送信している。

3.7 SaaS

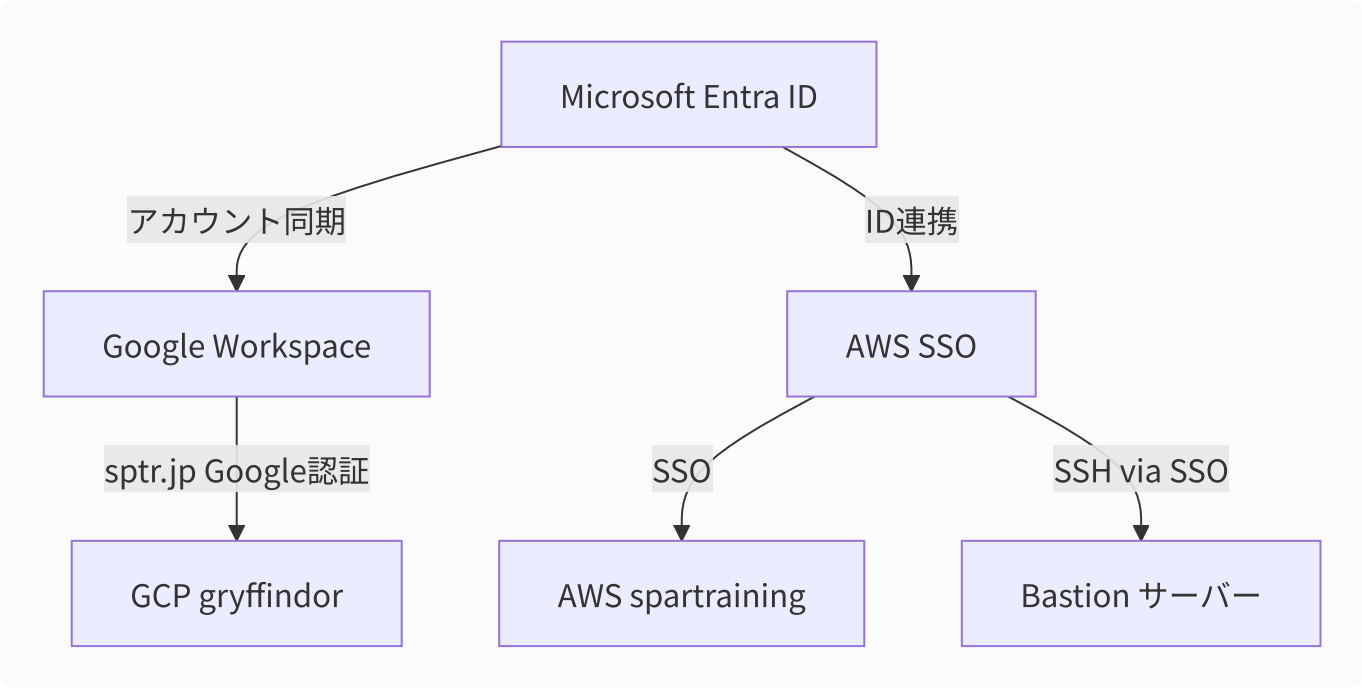
サービス	用途
Slack	コミュニケーション

4. 認証方式

各サービスへのアクセスには以下の認証方式を採用している。

認証方式	対象	説明
sptr.jp Google認証	GCP（gryffindor staging）	sptr.jpドメインのGoogle Workspaceアカウントによる認証
AWS SSO	AWS（spartraining）	Entra IDと連携したAWS SSOによるシングルサインオン
Cognito認証	spartraining unstable	unstable環境へのアクセス認証
なし	gryffindor production	直インターネットアクセス

4.1 ID連携の流れ



5. 開発者のクラウドアクセス

開発者は全員リモートワークで業務を行っており、以下の方法でクラウドリソースにアクセスする。

5.1 GCPへのアクセス

gryffindorのstaging環境へはsptr.jpドメインのGoogle Workspaceアカウントを使用してGoogle認証を行う。production環境は認証なしで直接インターネットからアクセス可能である。

5.2 AWSへのアクセス

Microsoft Entra IDと連携したAWS SSOを使用してアクセスする。spartrainingのunstable/production環境へのアクセスはAWS SSOによって制御される。

5.3 Bastionサーバーへのアクセス

spartrainingの各環境（unstable/production）にはBastionサーバーが1台ずつ設置されている。開発者はAWS SSO経由のSSHでBastionサーバーにアクセスできる。ただし、Bastionサーバーのポートはインターネットに対して閉じられており、実質的にインターネットには面していない。

6. 一般社員のクラウドアクセス

一般社員は社内ネットワーク経由でインターネットに接続し、以下のproduction環境にアクセスする。

6.1 spartraining（AWS）へのアクセス

社員PC → ルーター → インターネット → CloudFront → ALB → ECS → RDS の経路でspartraining production環境にアクセスする。

6.2 gryffindor（GCP）へのアクセス

社員PC → ルーター → インターネット → Cloud Run → Cloud SQL の経路でgryffindor production環境にアクセスする。

7. セキュリティ対策

各サービスにおいて認証を必須化し、Microsoft Entra IDによる一元的なアカウント管理を行っている。GCPへはGoogle Workspaceを経由したシングルサインオン、AWSへはAWS SSOを経由したシングルサインオンを活用している。VPN接続は使用せず、各サービスの認証機能により保護を実施している。

データベース（RDS、Cloud SQL）はインターネットから直接アクセスできない構成となっており、Cloud SQLはcloud-sql-proxy経由でのみアクセス可能である。

制定日: 2024年1月15日
改訂日: 2025年1月22日

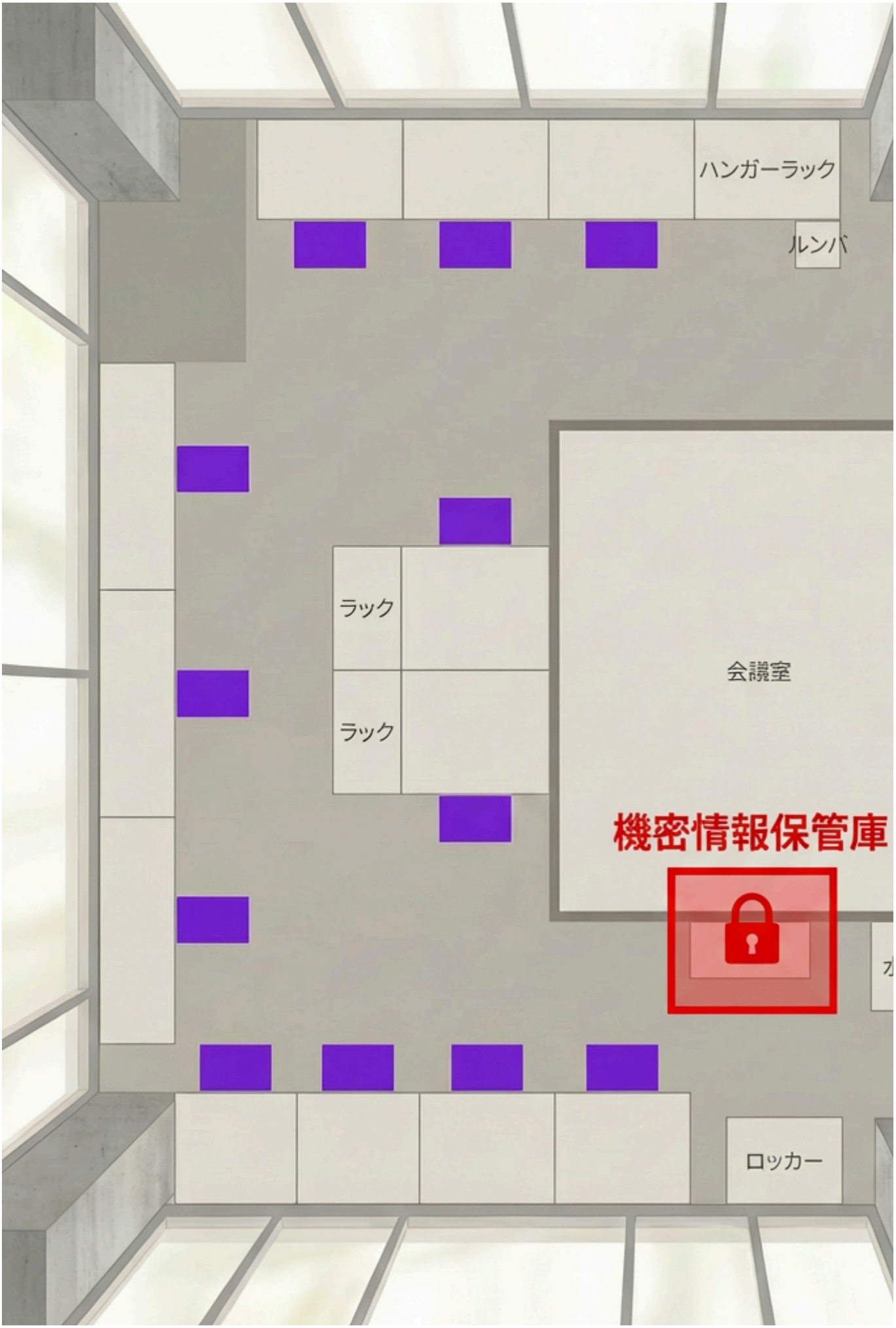
オフィスレイアウト図

作成者: 情報セキュリティ委員会

1. 概要

本文書は、当組織の事業所におけるセキュリティ領域の設定およびレイアウトを示すものである。セキュリティ領域の詳細な管理基準については「5. 物理的対策」を参照すること。

2. オフィスレイアウト図


ハンガーラック
ルンバ
ラック
ラック
会議室
機密情報保管庫
ロッカー

3. セキュリティ領域

当事業所は、情報資産の重要度に応じて以下のセキュリティ領域を設定している。

3.1 レベル1領域（来訪者エリア）

項目	内容
対象エリア	エレベーターホール、非常口付近
利用者	従業員および来訪者
アクセス制御	エレベーターは1Fでカードキーによりロック

3.2 レベル2領域（執務エリア）

項目	内容
対象エリア	執務室出入口の内側（執務スペース、会議室、ラック設置エリア等）
利用者	従業員
アクセス制御	出入口からの入室管理、最終退室者による施錠

4. 主要設備

4.1 執務エリア内設備

設備	説明
会議室	中央に配置。社内打合せおよび来訪者との会議に使用
ラック	サーバー・ネットワーク機器等を収納
施錠ラック	重要機器・媒体を施錠保管
ロッカー	従業員の私物保管用

4.2 その他設備

設備	説明
出入口	執務室への主要な出入口。レベル2領域の境界
非常口	緊急時の避難用。鍵付き
エレベーター	1Fでカードキー利用によりロック

5. 入退室管理

5.1 通常時

執務室への入室は出入口から行い、従業員のみがアクセス可能である。来訪者が執務エリアに入室する場合は、従業員の許可およびエスコートが必要となる。

5.2 緊急時

非常口は鍵付きであり、緊急時のみ使用する。火災等の緊急時には非常口から避難することができる。

制定日: 2025年1月23日