# 情報セキュリティ報告書
# 2025

GREE

# CONTENTS



## 編集方針

### 報告書発行の目的

グリーグループは「インターネットを通じて、世界をより良くする。」をミッションに掲げ、革新的なインターネットサービスの開発およびその事業展開に注力しています。また、お客さまに安心して当社グループのサービスを楽しんでいただくためには、お客さまからお預かりした情報を含む情報資産全般を適切に保護することが重要であると考えています。

この認識に基づき、当社グループは「情報セキュリティ方針」を定め、情報セキュリティマネジメント体制を整備するとともに、人・技術・物理の各側面から情報セキュリティ活動を推進するなど、ステークホルダーの皆さまからの信頼の獲得・向上に取り組んでいます。

本報告書は、こうした取り組みを体系的に整理し、可能な限り詳細に説明するものです。本報告書を通じて、当社グループに対するご理解を深めていただければ幸いです。

**●報告対象期間**

2024年（2024年1月～12月）

ただし、一部報告は上記以外の期間を含んでいます。

**●報告対象組織**

グリーホールディングス株式会社およびグループ会社を対象に、事業において取り扱う設計・技術情報、サービス提供に係るお客さまおよびお取引先情報など、各種重要情報の保護に関する取り組みを中心に記載しています。

**●報告書の発行責任部署（連絡先）**


**グリーホールディングス株式会社**

**ビジネス・テクノロジー本部 セキュリティ部**

〒106-0032 東京都港区六本木6-11-1

六本木ヒルズゲートタワー

TEL 03-5770-9307

# 情報セキュリティ統括管理責任者メッセージ

## グリーグループは、拡大するセキュリティリスクへの迅速な対策を通じて、お客さまが安心・安全にサービスをご利用いただけるよう努めています

情報セキュリティ統括管理責任者

藤本 真樹

グリーグループのサービスは、ゲーム・アニメ事業、メタバース事業、DX事業など多岐にわたります。2024年は、事業・サービスの機能強化や経営の効率化など、ユーザーの皆さまに新たな感動と体験を提供するため、積極的に取り組んだ1年となりました。

近年、生成AIをはじめとした新たなクラウドサービスの急速な発展が社会に大きな変革をもたらし、当社グループにおいても新たな価値創造の原動力として期待されています。しかし、その一方で、サイバー攻撃、特にランサムウェアやネットワーク脆弱性を狙った攻撃はますます巧妙化しており、企業の情報セキュリティ対策には、これまで以上に高度な対応が求められています。

こうした状況のなか、当社グループでは、生成AIとクラウドサービスの利用におけるガバナンス強化、ランサムウェア対策の徹底、個人情報保護の強化、リモートアクセスの安全性確保、そして従業員のセキュリティ意識向上といった多岐にわたる施策を推進してまいりました。特に、従業員向けのセキュリティ教育には力を入れており、動画教材の充実や偽広告攻撃への対策などの啓発活動を通じて、全従業員のセキュリティ意識向上を図っています。

当社グループが提供するサービスを安心してご利用いただくために、ここに2024年度の情報セキュリティ活動についてご報告いたします。

# 情報セキュリティガバナンス

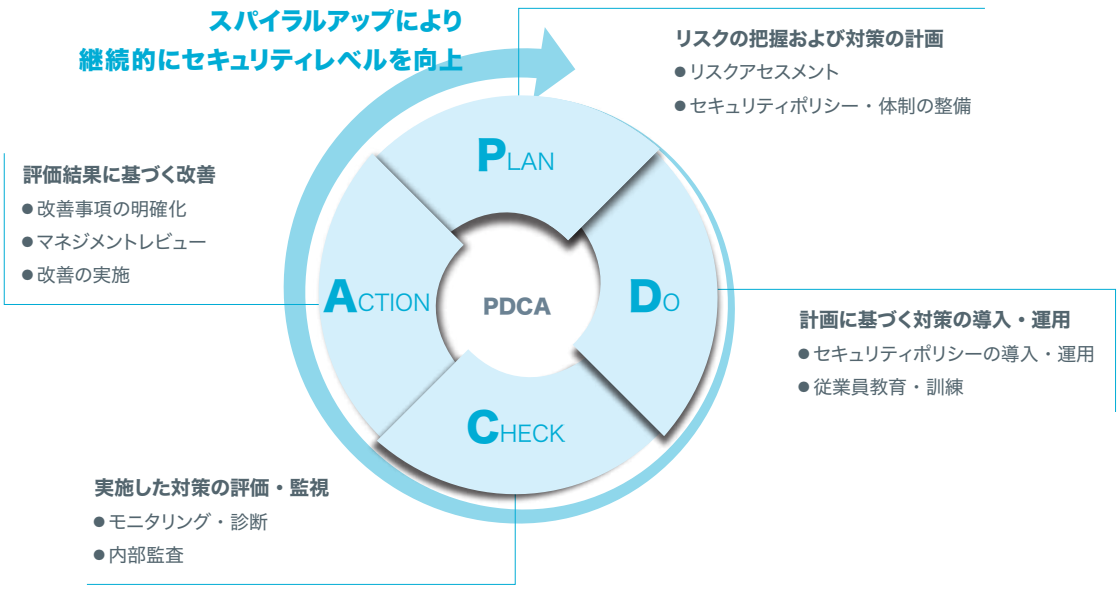
企業の経営資源は、長らく「ヒト」「モノ」「カネ」とされてきました。しかし、現在では第4の経営資源として「情報」が重視され、情報資産の効率的・効果的な活用が企業経営の重要な基盤の一つとなっています。
当社グループでは、情報資産を適切に取り扱いながら、革新的なサービスを継続的に提供できるよう、情報セキュリティ対策を経営上の重要課題として認識し、情報セキュリティマネジメントを推進しています。

## 情報セキュリティ方針

当社グループでは、お客さまからお預かりした情報を含む各種情報資産を適切に保護し、安心してサービスをご利用いただくことが重要であると考えています。
この考えに基づき、「情報セキュリティ方針」を策定・公表するとともに、関連規程および情報セキュリティマネジメント体制を整備し、継続的な改善に努めています。

## 情報セキュリティマネジメント

当社グループは、情報セキュリティマネジメントを体系的かつ着実に実施するための手法としてPDCA（継続的改善活動）を推進し、セキュリティレベルの維持・向上に取り組んでいます。PDCAによって絶えず見直しと改善を行い、環境の変化や新たな脅威に対応しています。



# 情報セキュリティ方針

## 情報セキュリティ管理体制の強化

情報セキュリティを推進するため、代表取締役およびその諮問機関である情報セキュリティ委員会を中心とした体制により、情報セキュリティに関する施策および事案を審議の上、決定・施行します。これにより、グループ横断的に情報セキュリティ管理状況の把握、必要な対策を迅速に対応できる体制を維持・強化していきます。

## 情報セキュリティ対策の実施

情報資産に対する不正アクセス、漏えい、改ざん、紛失、破壊、利用妨害などの情報セキュリティが侵害される事象が生じないように、事前にリスクアセスメントを適切に実施し、発生を防止できるよう十分かつ適切な対策を講じます。

## 情報セキュリティリテラシーの向上

役員および従業員に情報資産を保護することの重要性および情報セキュリティに対する役割と責任についての認識を向上させるために、定期的に情報セキュリティに関する教育を実施します。

## 情報セキュリティに関する関係法令の遵守

情報セキュリティに関連する法令や規則などに準拠した情報資産の管理および運用に関する内部規程類を整備し、役員および従業員への周知徹底を行います。

## 外部委託先管理の徹底

外部委託を行う際には、必要なセキュリティレベルを確保するために、セキュリティ面からも適格性を十分に審査し、外部委託先からの情報漏えいの防止に努めます。

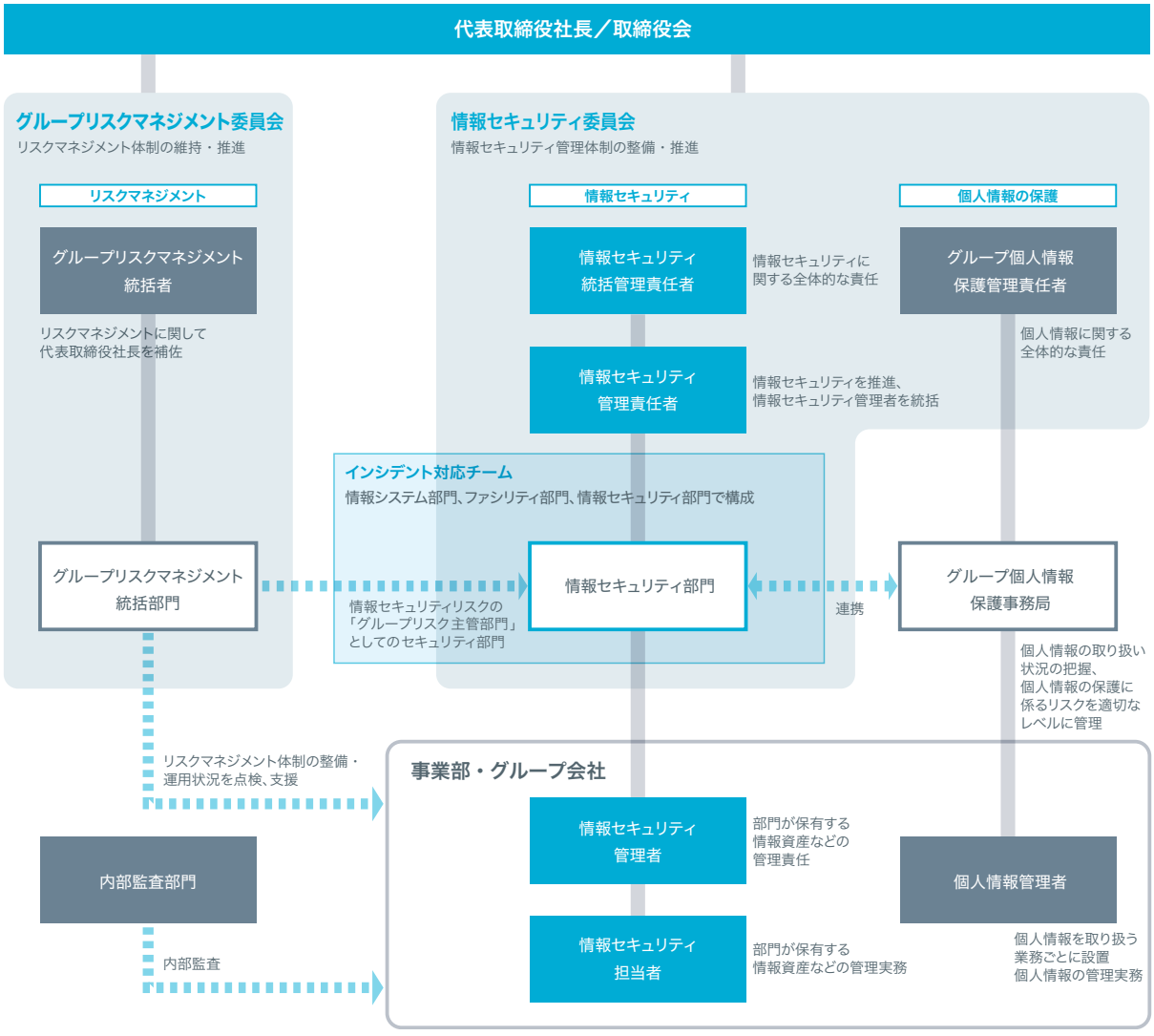
## モニタリング体制の整備・充実

情報セキュリティが徹底されていることを検証するために、自己点検を定期的に実施します。また、採用した管理策および実施した改善の適切性・有効性の評価およびリスクアセスメントの結果を定期的に確認し、これらを基にマネジメントシステムならびに本方針の見直しを行います。

## 情報セキュリティマネジメント体制

当社グループでは、迅速かつ網羅的に情報セキュリティ対策の有効性を確認し、適切に改善を実施していくため、「グループ全体」と「グループ各社」の2段階の情報セキュリティマネジメント体制を整備しています。
また、情報セキュリティに関わる各組織・責任者は、リスクマネジメントを統括するグループリスクマネジメント委員会および個人情報の管理を統括する組織とも連携し、情報セキュリティマネジメント体制の強化を図っています。

### 情報セキュリティマネジメント体制と関連組織



## グループ全体の情報セキュリティマネジメント体制

「情報セキュリティ委員会」のもとに、「情報セキュリティ統括管理責任者」および「情報セキュリティ管理責任者」を設置し、当社グループ全体の情報セキュリティマネジメントを統括しています。

### 情報セキュリティ委員会

情報セキュリティ委員会は、グリーホールディングス株式会社（以下、「グリーホールディングス」）の代表取締役社長を委員長とし、情報セキュリティ部門を事務局とする委員会です。委員は、コーポレート部門および開発部門の統括責任者、その他委員長が指名したメンバーで構成しています。また、オブザーバーとして内部監査室長が参加しています。
委員会は四半期ごとに開催しています。取締役会で決定した経営基本方針に基づき、グループ各社へのセキュリティ担当者の配置やインシデント対応チームの整備など、情報セキュリティマネジメントの推進に関する重要な事項について、代表取締役社長の諮問を受けて審議・答申しています。

### 情報セキュリティ統括管理責任者

情報セキュリティ統括管理責任者は、グリーホールディングスの代表取締役社長が任命し、最高技術責任者が担っています。当社グループの情報セキュリティ対策に関する責任と権限を有しており、情報セキュリティ施策の導入・改善について遅延などの問題がある場合は、代表取締役社長に対して当該組織責任者への是正指示を提言しています。

### 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、情報セキュリティ統括管理責任者が任命し、情報セキュリティ部門長が担っています。当社グループにおける情報セキュリティ対策を推進する責任と権限を有しており、各情報セキュリティ管理者をとりまとめています。

### 情報セキュリティ管理者

情報セキュリティ管理者は、情報セキュリティ統括管理責任者が任命し、各事業本部の本部長が担っています。当社グループが保有する情報資産および関連資産を適切に管理する責務を負っています。

## リスクマネジメント体制

当社グループでは、主要なリスクごとにグループリスク主管部門を設置し、各部門・グループ会社をサポートすることで、適切なリスクマネジメントを推進しています。情報セキュリティリスクについては、情報セキュリティ部門がグループリスク主管部門の役割を担い、「グループリスクマネジメント統括部門」との連携のもとリスクの低減に努めています。

### グループリスクマネジメント委員会

グループリスクマネジメント委員会は、リスクマネジメント体制を維持・推進し、情報セキュリティ委員会が所管しないリスクに関して審議・答申を行います。

### グループリスクマネジメント統括者

グループリスクマネジメント統括者は、グリーホールディングスの代表取締役社長が任命し、コーポレート本部長が担っています。リスクマネジメント体制の維持・改善に関する業務全般を統括し、グループリスクマネジメント統括者補佐およびグループリスクマネジメント統括部門からの報告を受け、必要な指示を行っています。

### グループリスクマネジメント統括部門

リスクマネジメントが実効性をもって運用されるよう、グループリスクマネジメント統括部門を設置しています。各グループリスク主管部門が所管するリスクについてリスクマネジメントの運用状況および各部門・グループ会社におけるリスクマネジメントの整備・運用状況を点検し、その結果をグループリスクマネジメント委員会に報告しています。

### グループリスク主管部門

リスク種別に応じて、リスクマネジメント施策を推進する主管部門を設置しています。リスク種別は、法令・規制違反、社内規程違反、企業倫理違反、契約違反、サービス品質不良、情報漏えいなどに分けられます。各部門・グループ会社におけるリスク管理を専門的な見地からサポートし、組織横断で適用されるルール・手順などの整備・運用を主導しています。

## 個人情報マネジメント体制

個人情報については、「法令遵守およびプライバシー保護」と「情報資産保護」の2つの観点から安全管理措置を講じています。法令遵守およびプライバシー保護に関してはグループ個人情報保護事務局が、情報資産保護に関しては情報セキュリティ部門がそれぞれ管理・監督しています。
一方で、法令遵守、情報資産の保護の双方を考慮する必要がある場合も多いため、グループ個人情報保護事務局と情報セキュリティ部門が連携し、対策の検討および情報の共有を積極的に実施しています。

### グループ個人情報保護管理責任者

グループ個人情報保護管理責任者は、グリーホールディングスの代表取締役社長が任命し、個人情報を安全に保存する義務および許諾を得た個人情報の利用に関して、最終的な利用可否の確認と承認を行う権限と責任を有しています。グループ個人情報保護管理責任者は、当社グループの個人情報保護に関する内部規程の整備、安全対策の実施、教育訓練などを推進するための個人情報保護マネジメントシステムを策定し、それらの周知徹底を図っています。

### 個人情報管理者

個人情報を取り扱うアプリケーション、サービスおよびキャンペーンごとに、その業務に関わる個人情報保護に責任を持つ個人情報管理者を任命しています。個人情報管理者は、グループ個人情報保護事務局の指示に従い、担当業務において適切に個人情報が取り扱われるよう措置を講じ、個人情報を安全に管理しています。

### グループ個人情報保護事務局

グループ個人情報保護事務局は、当社グループにおける個人情報の取り扱い状況を把握し、個人情報およびプライバシーの保護に関するリスクを適切なレベルに管理するための実務を担っています。

## インシデント対応体制

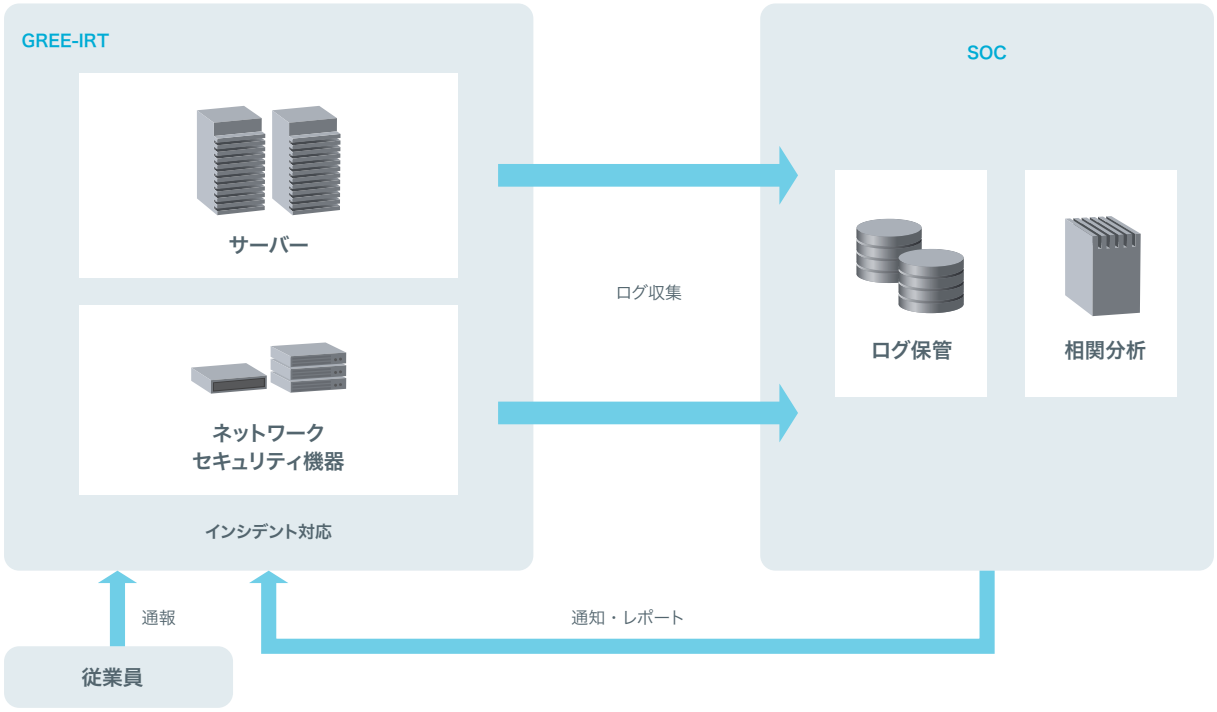
情報セキュリティに関わるインシデントの対応組織として、情報セキュリティ委員会のもとに「インシデント対応チーム（GREE-IRT*1）」を設置しています。同チームはSOC*2（Security Operation Center）からの通知等により、インシデントの発生状況を把握・分析し、他の情報セキュリティ関連組織と連携しながら解決に向け対応します。

また、具体的な行動の指針として「インシデント対応ガイドライン」を整備しています。このガイドラインは、インシデント対応の基本的な方針、体制、ルールを規定するもので、インシデント対応訓練においても活用しており、訓練で得た学びを反映させることで対応の改善を行っています。

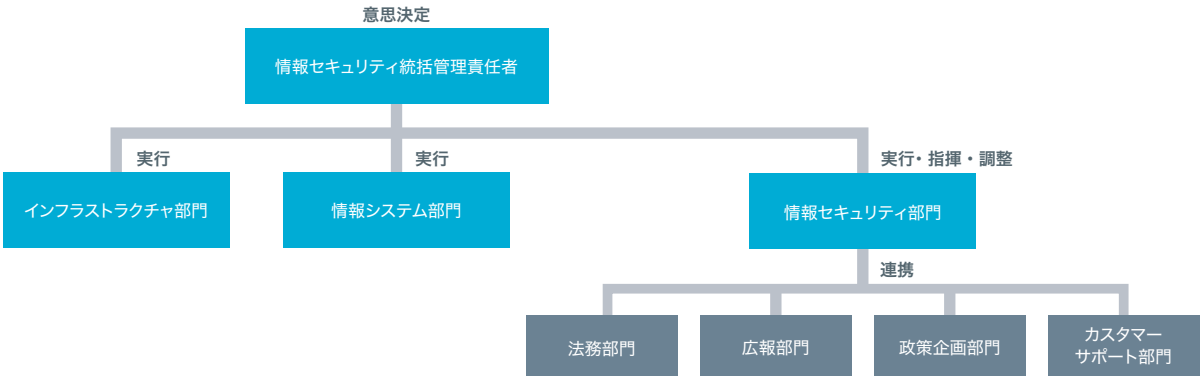
*1 IRT　：Incident Response Teamの略。GREE-IRTでは、情報セキュリティ統括管理責任者、情報セキュリティ部門、インフラストラクチャ部門、情報システム部門を基本チームとし、インシデントの内容に応じて必要な部門が参加

*2 SOC：24時間365日ネットワークを監視し、分析・予防・報告を行う

### インシデント監視体制



## インシデント対応体制




## インシデント対応 役割分担

| 担当 | 機能 | 役割 |
|---|---|---|
| 情報セキュリティ統括管理責任者 | 意思決定 | • 意思決定 |
| 情報セキュリティ部門 | 実行<br>指揮<br>調整 | • 情報セキュリティ統括管理責任者の意思決定支援、軽微な意思決定<br>• インシデント対応の全体管理<br>• 対応方針の検討<br>• 他部門への対応依頼<br>• 専門的な調査<br>• 端末に関する現場でのインシデント対応<br>• 法務部門、広報部門、カスタマーサポート部門への連絡 |
| 情報システム部門 | 実行 | • オフィス環境におけるインシデント対応<br>• 端末に関するリモートでのインシデント対応 |
| インフラストラクチャ部門 | 実行 | • 商用環境におけるインシデント対応 |
| 法務部門 | 対応 | • 法的処置が必要な場合の対応 |
| 広報部門 | 報告 | • 社外への公表 |
| 政策企画部門 | 報告 | • 関連省庁への報告 |
| カスタマーサポート部門 | 対応 | • お客さまからのお問い合わせ対応 |

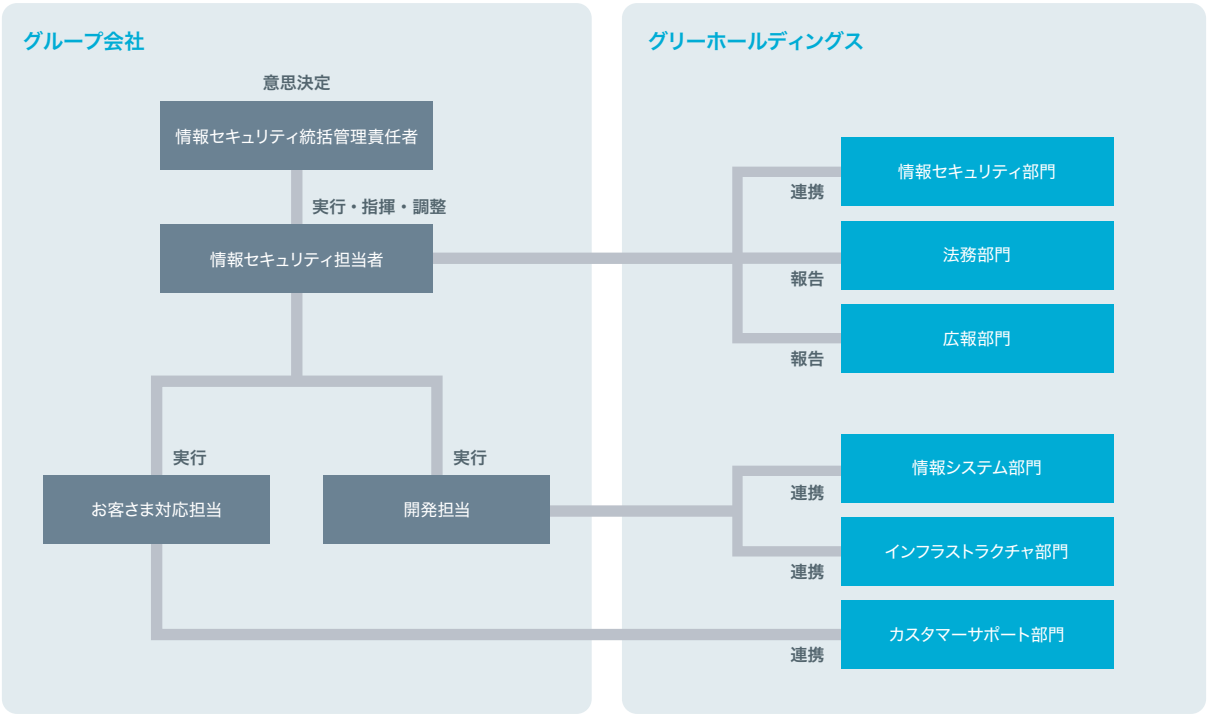
## グループ各社の情報セキュリティマネジメント体制

グループ全体で情報セキュリティ対策を推進するため、各グループ会社に情報セキュリティ管理者および情報セキュリティ担当者を設置しています。
グリーホールディングスの情報セキュリティ部門は、グループ会社の情報セキュリティ担当者を訪問し、環境の変化や課題事項に関するヒアリング、オフィスの物理セキュリティの確認、セキュリティアセスメントで検出された課題の改善状況の確認などを行い、連携の強化を図っています。
各情報セキュリティ担当者は、自身が属するグループ会社と情報セキュリティ部門をつなぐ窓口となるほか、以下の役割を担い、確実に情報セキュリティ施策が実行されるよう推進しています。

**<情報セキュリティ担当者の主な役割>**

- 情報セキュリティ部門から指示のあった対策の徹底
  （全体ミーティングでの周知・パトロールなど）
- セキュリティアセスメントで検出された課題のフォローアップ
- 情報セキュリティ関連の規程類を制定・改定する際の情報セキュリティ部門との連携
- インシデント発生時における情報セキュリティ部門との連携
- 情報セキュリティ教育の推進

**グループ会社 インシデント対応体制**



## グループ会社 インシデント対応 役割分担

| 担当 | 機能 | 役割 |
|---|---|---|
| 情報セキュリティ統括管理責任者 | 意思決定 | ● 意思決定 |
| 情報セキュリティ担当者 | 実行<br>指揮<br>調整 | ● 情報セキュリティ統括管理責任者の意思決定支援、軽微な意思決定<br>● インシデント対応の全体管理<br>● 対応方針の検討<br>● 他部門への対応依頼<br>● 専門的な調査<br>● 端末に関する現場でのインシデント対応<br>● 端末に関するリモートでのインシデント対応<br>● グリーホールディングス関連部門への連絡<br>● 関連省庁への報告、社外への公表<br>● 法的処置が必要な場合の対応 |
| お客さま対応担当 | 実行 | ● お客さまからのお問い合わせ対応 |
| 開発担当 | 実行 | ● インシデント対応 |
| グリー | 支援 | ● グループ会社のインシデント対応支援 |

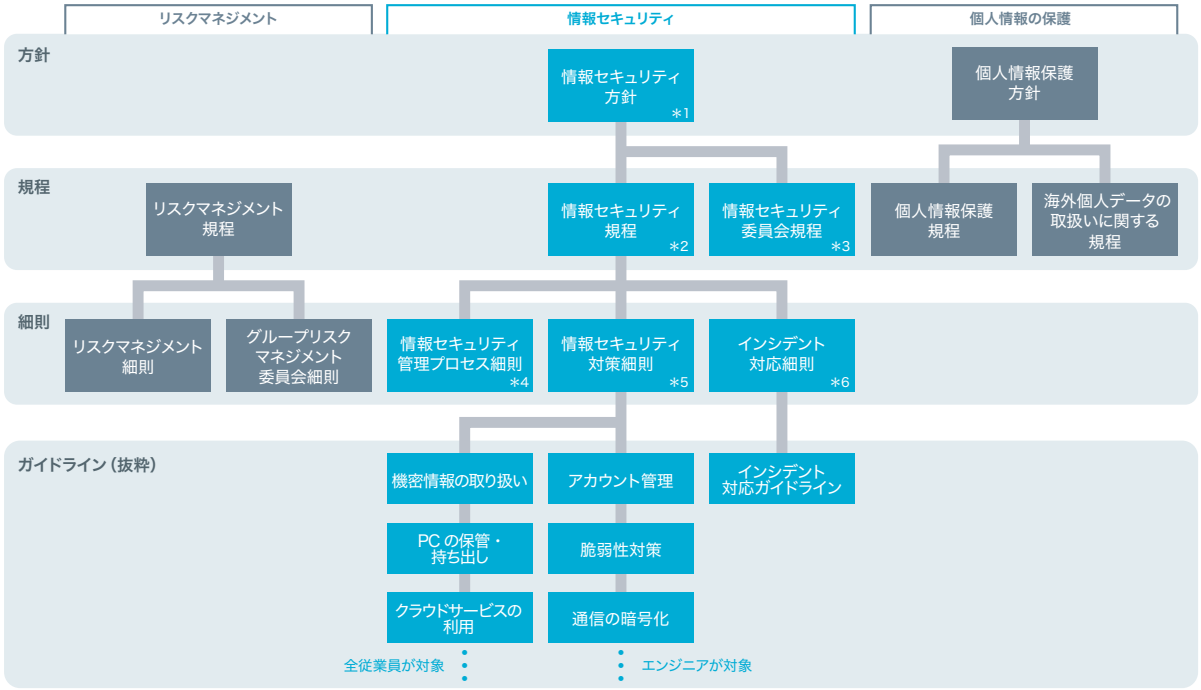
## 情報セキュリティに関するルール

当社グループは、規程および細則に情報セキュリティに関する基本的なルールを定め、ガイドラインに具体的な管理方法を定めています。ガイドラインは、情報資産の取り扱いやリモートアクセスなどに関わる全従業員向けガイドラインと、アプリケーション開発やインフラストラクチャ構築に携わるエンジニア向けガイドラインがあります。いずれも、各種教育や社内ポータルでの掲示を通じて、従業員へ周知徹底しています。

**ガイドライン（一部抜粋）**

| カテゴリー | | ガイドライン名 |
|---|---|---|
| 全従業員対象 | 情報資産の取り扱い | • 情報資産の機密性区分と保管<br>• エリアのセキュリティレベル<br>• ラベリング・文書管理 |
| | PC・セキュリティカードの管理 | • PCの保管・持ち出し<br>• PCの管理者権限の利用<br>• ストレージデバイスの利用<br>• セキュリティカードの管理 |
| | サービス・ネットワークの利用 | • クラウドサービス<br>• 利用を制限するアプリケーション・Webサービス<br>• チャットツール<br>• 情報共有ツール<br>• メールマガジンなど一斉メール配信<br>• サービス利用者から個人情報を取得するフォーム<br>• パスワードの設定<br>• リモートアクセス・遠隔操作ツール |
| | 社外パートナー・ゲスト | • 業務委託を利用する際の注意事項<br>• 社外パートナーのシステム利用<br>• 社外パートナーとの情報共有<br>• ゲストが執務室に入室する際の注意事項 |
| エンジニア対象 | インフラ | • ネットワーク全般<br>• 商用環境へのアクセス方法<br>• アカウント管理（識別・認証・認可）<br>• SSH向け秘密鍵・公開鍵管理<br>• IPアドレス・Portアクセス制限<br>• インフラ構成・変更管理<br>• 特定の正社員のみアクセス許可させるサーバー<br>• ログの保存<br>• SSL/TLSサーバー証明書・秘密鍵<br>• ソフトウェアのインストール・更新 |
| | アプリケーション開発 | • 考慮すべき脆弱性対策<br>• サポートツールの管理<br>• 開発で使用するツール・サービスの管理<br>• クローズド・チャット機能の利用 |

### 情報セキュリティに関するルール体系




＊1：情報セキュリティ対策の方針や行動指針　＊2：情報セキュリティを維持・管理するための組織体制や管理策の概要　＊3：情報セキュリティ委員会の運営について定める
＊4：情報セキュリティ管理プロセスの確立および継続的な運用を実施するに際して必要な事項を定めたルール　＊5：「情報セキュリティ規程」で定めた各規程をより具体化したルール
＊6：インシデント発生時の対応に関するルール

## クラウドサービス利用に関する情報セキュリティ対策

業務効率を高めるため、当社グループにおいてもクラウドサービスの利用が増加しています。当社グループでは、クラウドサービスを利用する際のリスクを軽減するために、利用者が遵守すべき事項をガイドラインとしてまとめています。

原則として、以下の利用条件をすべて満たすサービスは利用を許可していますが、条件を満たさない場合や個人情報など機密性が高い情報を取り扱う場合は、情報セキュリティ部門への届出や利用相談、チェックリストを用いたセキュリティ対策の確認を必要としています。

また、2021年からCASB（Cloud Access Security Broker）のクラウドサービス安全性評価機能を用いて、第三者認証の取得状況やGDPR（General Data Protection Regulation）への対応状況なども詳細に把握し、客観的な基準に基づいたクラウドサービスの安全性評価も行っています。

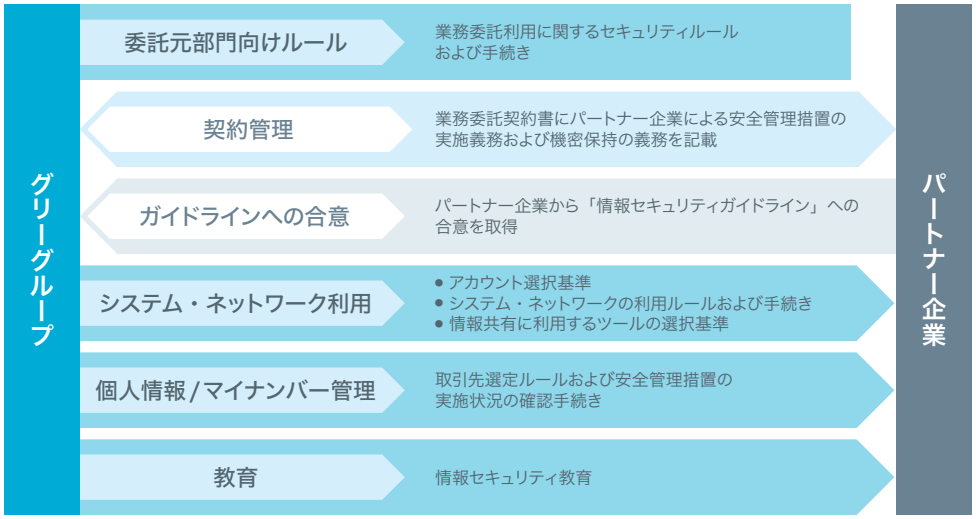
**<クラウドサービスの利用条件>**

- 情報セキュリティに関する認証（ISMS、プライバシーマーク、TRUSTe、PCIDSSなど）を取得していること
- 過去に事故が発生していない、もしくは発生後に改善されていること
- 利用規約に利用者の秘密保護が記載されていること
- 問い合わせ窓口などのサポートが提供されていること
- 監査ログ（サービス内での操作やイベントの履歴を記録したデータ）の取得が可能であること
- 利用する部門にサービス管理責任者を設置すること

## パートナー企業と連携した情報セキュリティ対策

当社グループの事業活動はパートナー企業（業務の委託先）が提供するサービスに支えられています。パートナー企業が当社グループの重要な情報を取り扱うこともあるため、情報セキュリティの観点でもパートナー企業と信頼関係を築き、緊密に連携して情報を保護することが必要です。当社グループでは、業務委託利用に関する情報セキュリティルールを整備し、施策を推進しています。

**パートナー企業と連携した情報セキュリティ対策**



### 業務委託利用に関する情報セキュリティルールの整備

業務委託を利用する際の情報セキュリティ上の注意事項や手続きをルールとして定めています。委託元となる部門は、ルールを理解し、手続きが完了してから業務委託の利用が可能となります。

**<主な内容>**

- 業務委託利用に関して情報セキュリティ対策を必要とする背景
- 業務委託先および再委託先のアカウントの選択、端末の利用、ネットワークの利用、勤務場所などのルール
- 契約管理、ガイドラインへの合意依頼、個人情報に関する手続き

### 契約管理

パートナー企業での安全管理措置の実施義務および秘密保持義務を含む契約を締結しています。
なかでも個人情報を取り扱う業務を委託する場合は、委託元となる部門とグループ個人情報保護事務局が連携し、個人情報管理条項を含む契約を締結しています。

### 「グリーグループ情報セキュリティガイドライン」の遵守

安全に作業いただくことを目的に、パートナー企業に遵守いただきたい情報セキュリティ事項を「グリーグループ情報セキュリティガイドライン」として定めています。パートナー企業に対しては、取引契約を締結する際に同ガイドラインをご確認いただき、記載事項を遵守する誓約書の提出を求めることとしています。

**<主な内容>**

- 勤務場所の安全性確保
- 利用ネットワーク
- 利用可能端末
- 端末の管理
- 情報共有方法
- インシデント発生時の対応

### システムの適切な利用

パートナー企業に付与するアカウントは、開発業務を目的とするタイプと情報共有に限定したタイプを用意しています。委託元となる部門は、委託する業務内容に基づき適切なアカウントを選択することで、システムの利用と情報へのアクセスを必要最低限にすることができます。また、各アカウントの利用について、利用可能な端末、ネットワーク、場所などを指定し、不適切な利用による情報漏えいなどのリスクを低減しています。

### パートナー企業オフィスからのネットワークおよびシステム利用の管理

パートナー企業が、パートナー企業のオフィスから当社グループのネットワークやシステムを利用する場合は、情報セキュリティ部門の承認が必要となります。
その際、利用目的が適切であること、アクセス元のIPアドレスがパートナー企業専有であり他社と共有していないこと、セキュリティ管理体制が十分であることなどを確認しています。また、利用者や利用期間について記録するとともに定期的に確認し、利用する必要がなくなり次第、アクセス権を削除しています。

### 安全な情報共有ツールの利用

パートナー企業とのファイル共有は情報セキュリティ対策が施されたツールを指定しています。PPAP*は誤送信による情報漏えいリスクを高めるだけでなく、ウイルス検知が困難であることから、危険性が高い共有方法として禁止しています。従業員に啓発を行い、パートナー企業にも説明を通じてご理解いただいています。

＊PPAP：メールでパスワード付きのzipファイルを送った後に、別メールでパスワードを送るファイル共有方法。「パスワード（Password）付きzip」「パスワード（Password）送信」「暗号（Angou）化」「プロトコル（Protocol）」の頭文字をとった言葉

### 個人情報/マイナンバーを取り扱う場合の安全性確認

個人情報またはマイナンバーを扱う業務を委託する場合は、委託開始前、および委託開始後は年次で、下記のいずれかの方法で安全性を確認しています。

- プライバシーマーク認定やISMS認証の取得、もしくはSOC2への準拠を確認
- グループ個人情報保護事務局が依頼する「安全管理措置チェック」
- 委託元組織による監査の実施および情報セキュリティ部門のレビュー

## 生成AIサービスの活用と安全な利用

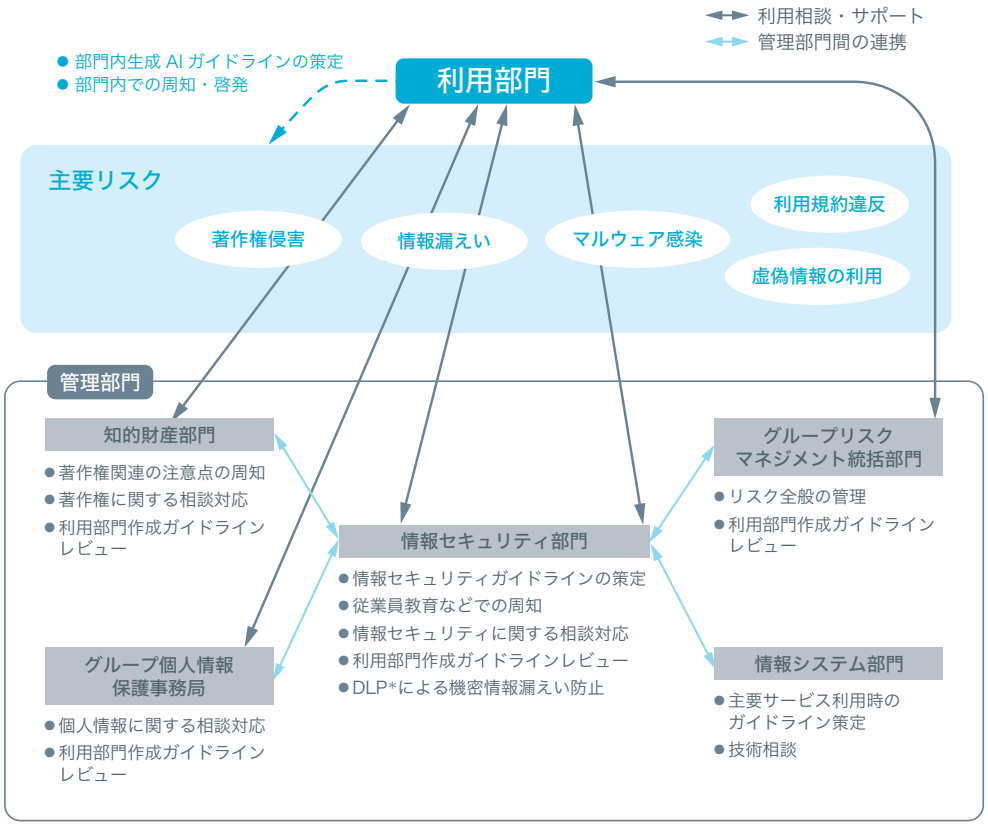
生成AIが急速に普及し、さまざまな組織で試行的導入が始まっています。当社グループでも、業務の効率化やアイデアの創出などの効果を期待し、積極的かつ適切に利用することが重要だと考えています。

生成AIは「学習」する特性上、入力するデータの内容や出力される生成物の利用方法によっては、著作権侵害、情報漏えいなどの問題が発生するおそれもあります。

そこで当社グループでは、情報セキュリティ部門、情報システム部門、知的財産部門、グループリスクマネジメント統括部門、グループ個人情報保護事務局が管理部門となり、生成AIを利用する組織と連携し、安全な利用を進める体制を構築しています。

情報セキュリティの観点では対策の一つとして、業務利用する際の注意事項および手続きをガイドラインとして策定しています。このガイドラインを含め、今後の技術の進展などに合わせて対策をアップデートしていきます。

### 生成AI利用に関するリスクと管理体制




＊ DLP：Data Loss Prevention の略。機密情報や重要データを自動的に特定し、データを常に監視・保護する機能

# 生成 AI 利用に関する情報セキュリティガイドライン（抜粋）

## ガイドラインの目的

情報漏えいなどのセキュリティリスクを回避するために、生成 AI を利用する際のセキュリティルールおよび手続きを定める

## 対象とする生成 AI

人間による指示（文章・画像・音声・動画他）を解釈し、学習データを元に新たなコンテンツ（文章・画像・音声・動画他）を生成するシステム、もしくは、それらのシステムをバックエンドに持つシステム

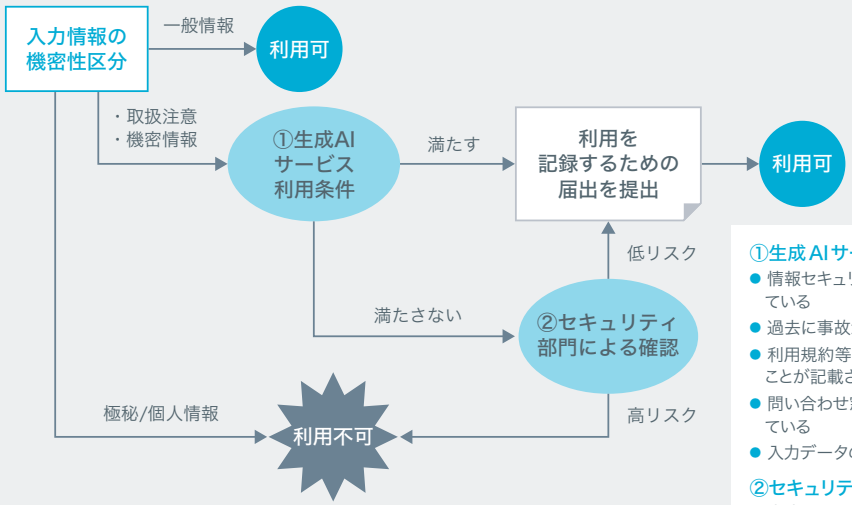
## 遵守事項

- 入力を禁止する情報
- コード生成に使用する場合の責任範囲、社内コード管理
- 自社サービスに組み込む場合の API キーや管理画面のアカウントの管理

## 情報セキュリティ以外のリスクおよびルール・手続きの案内

- 著作権侵害
- 誤情報の利用
- 個人情報の不適切な利用
- 利用規約違反

## 利用可否判断および手続きフロー




**①生成 AI サービス利用条件の例**

- 情報セキュリティに関する認証を取得している
- 過去に事故が報じられていない
- 利用規約等に利用者の秘密を保護することが記載されている
- 問い合わせ窓口等のサポートが提供されている
- 入力データの保護を確保できる

**②セキュリティ部門による確認内容**

- 生成 AI サービスの安全性を調査
- 用途、入力情報、利用人数などの利用環境を把握

# 個人情報保護の対策

当社グループは、個人情報の重要性を認識し、その保護の徹底が社会的責務であると考え、当社グループの各サービスをご利用のお客様及びお取引先から取得した個人情報を、個人情報の保護に関する法律等に則り適切に取り扱い、保護するよう努めています。

## 個人情報保護マネジメントシステム

グループ個人情報保護事務局が下記の対策を実施することで、個人情報の取り扱い状況を把握し、個人情報の保護に係るリスクを適切なレベルに管理しています。

### 主な個人情報保護対策

| | |
|---|---|
| 個人情報保護研修 | 当社グループの従業員を対象に、個人情報の取り扱いに関する理解を深めるため、定期的に研修を実施しています。 |
| 自己点検 | 個人情報の内容と量に基づくリスクに応じて、情報を管理する各部門に個人情報の取得から削除に至るまでの管理状況の自己点検を求めています。自己点検の結果に基づき、必要に応じて各部門に対し改善を求めることで管理体制の維持・向上を図っています。 |
| 管理台帳の棚卸 | 各部門が管理する個人情報の取り扱い状況を把握するために、定期的に情報管理台帳の棚卸を行っています。 |
| 委託先管理 | 個人情報取り扱い業務の委託先が、適切な水準の個人情報管理体制を維持しているかを定期的に確認しています。 |

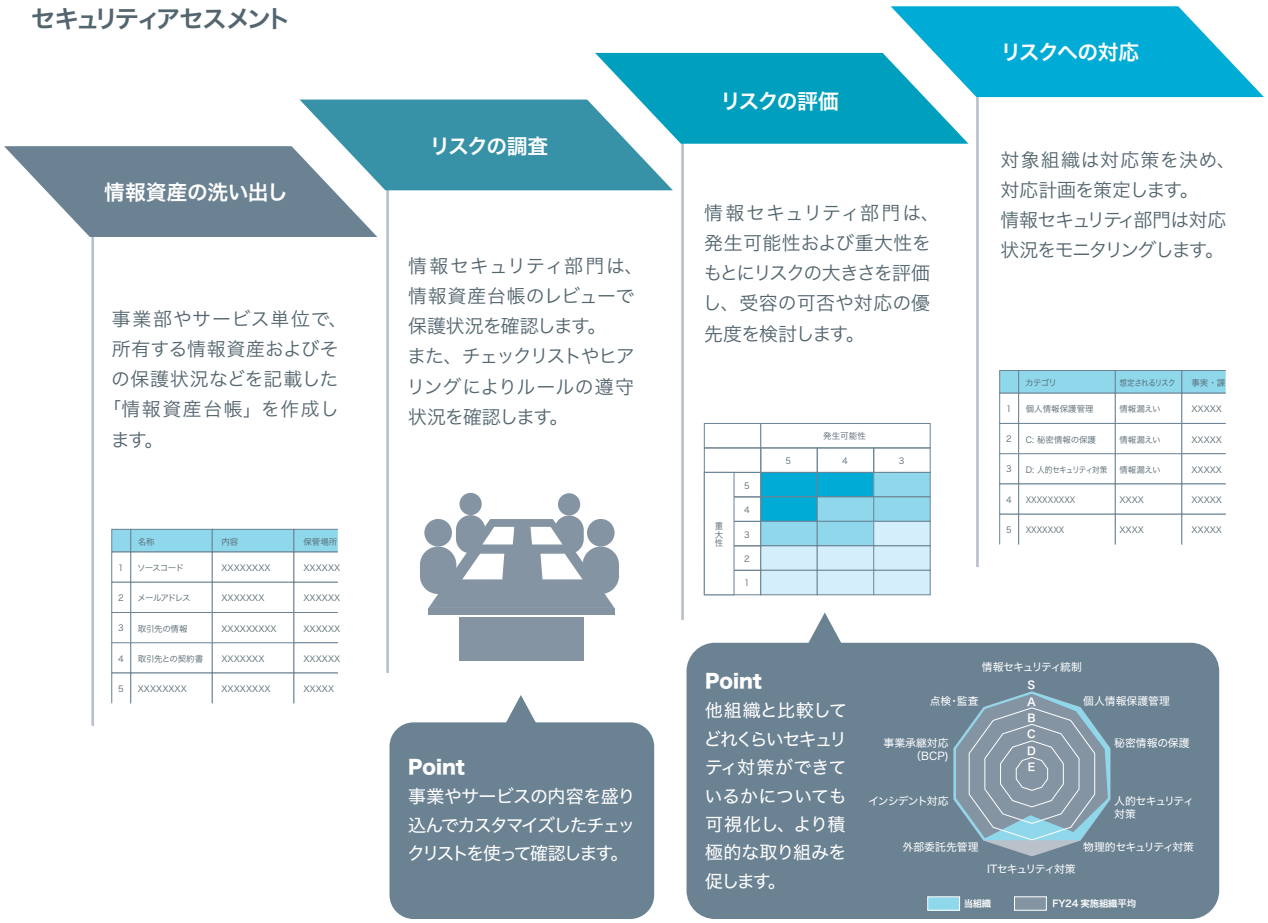
全従業員を対象とした定期研修の資料

### 海外におけるプライバシー保護への対応

当社グループでは、海外のプライバシー関連法令に適切に対応するために「海外個人データの取扱いに関する規程」を定めています。また、海外のお客様にサービスを提供する場合は、法務部門およびグループ個人情報保護事務局にて法令調査や対応事項の設計を行い、法令を遵守できるよう各部門をサポートしています。

## セキュリティアセスメント

当社グループでは、定期的に情報資産におけるリスクの存在を調査し、そのインパクトを評価して対応策を決定するセキュリティアセスメントを実施しています。
セキュリティアセスメントは、情報セキュリティ部門が中心となり、主に①情報資産が適切に保護されているか（情報資産台帳による）、②情報資産を保護するための管理策が適切に実施されているか（チェックリストやヒアリングによる）の2点を確認しています。
情報セキュリティ部門は、検出したリスクを対象組織に報告するとともに、リスク低減に向けた改善策を提案しています。それを受け、対象組織は、情報セキュリティ部門と連携し、当該リスクへの対応方針（軽減、回避、受容など）を決定してリスク管理計画を策定し、計画に沿ったリスク管理策を実施しています。情報セキュリティ部門ではそのリスク管理策の実施状況をモニタリングして、情報資産の管理の強化を図っています。



## ガイドラインに基づく情報セキュリティ対策確認

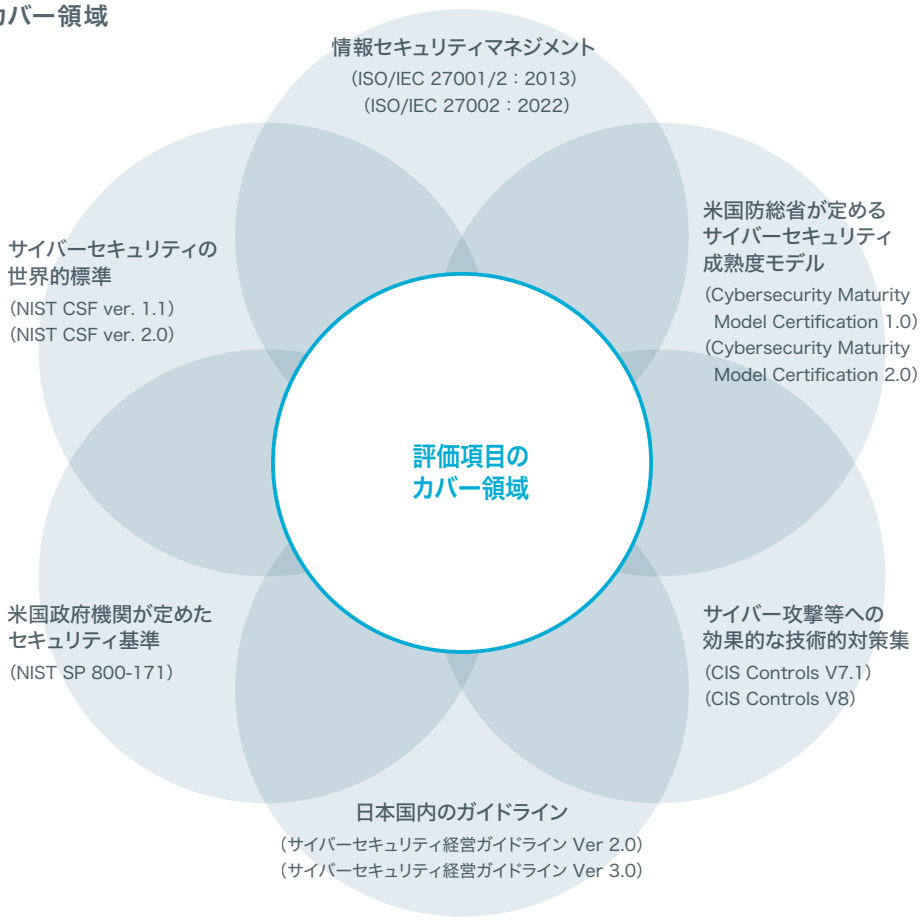
情報セキュリティの対策状況を確認するプラットフォームサービスを用いて、ISMS、NIST*1、CIS*2などの主要な公的情報セキュリティガイドラインで定められたベストプラクティスをベースに、実施状況をスコア化しています。他社のスコアと比較することで、当社の対策レベルを客観的かつ俯瞰的に評価しています。

また、ベストプラクティスと差異がある対策を課題とし、リスクの重要度（リスクスコア）が高いものから優先的に対策の改善を進めています。この取り組みによって、短期的な課題解決だけでなく、リスク状況の変化を常に把握し、将来を見据えた情報セキュリティ戦略を講じることが可能となっています。

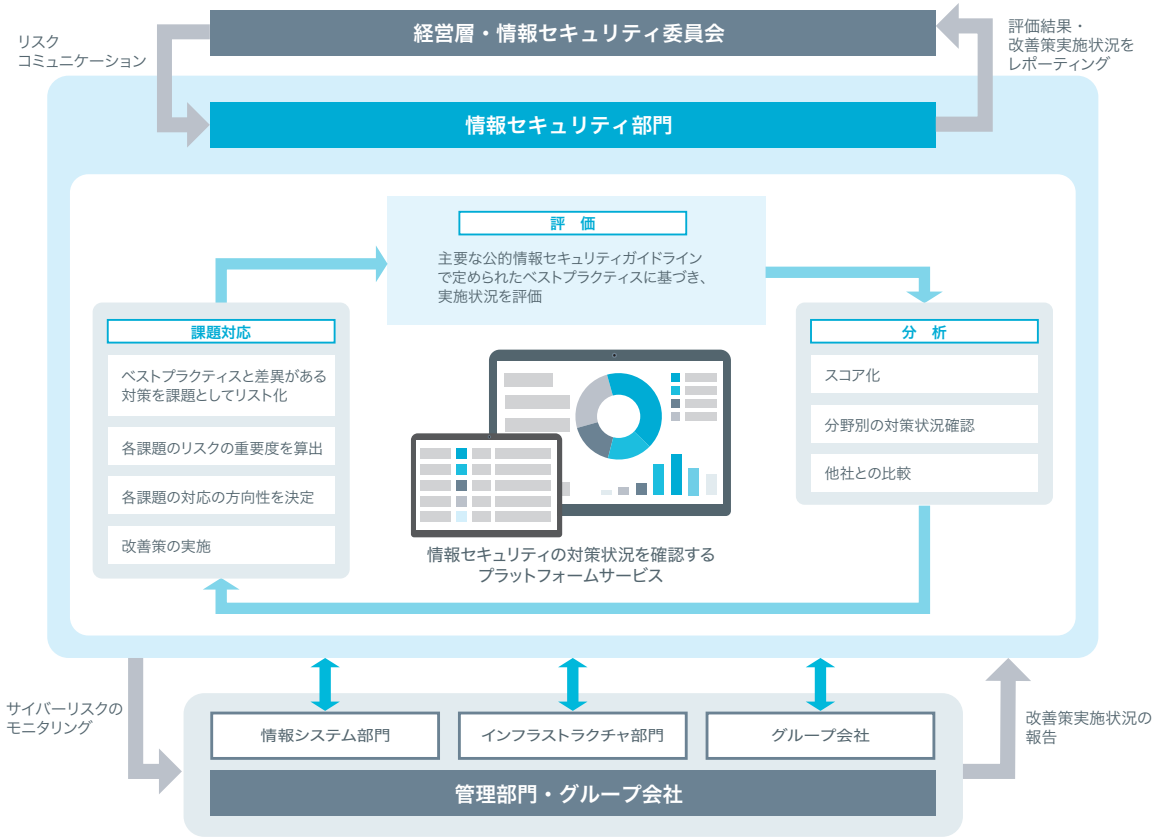
＊1 NIST：National Institute of Standards and Technologyの略称であり、科学技術の標準について研究を行うアメリカ合衆国の連邦政府機関

＊2 CIS ：Center for Internet Securityの略称であり、インターネットセキュリティの標準化について研究を行うアメリカ合衆国の非営利団体

**評価項目のカバー領域**



## 評価およびリスクコミュニケーションのフロー




## ガイドラインに基づくセキュリティ対策

### NRIセキュアテクノロジーズ(株)「Secure SketCH(PREMIUMプラン)」を用いた評価結果

#### 総合評価

S　A　B　C　D

高レベル

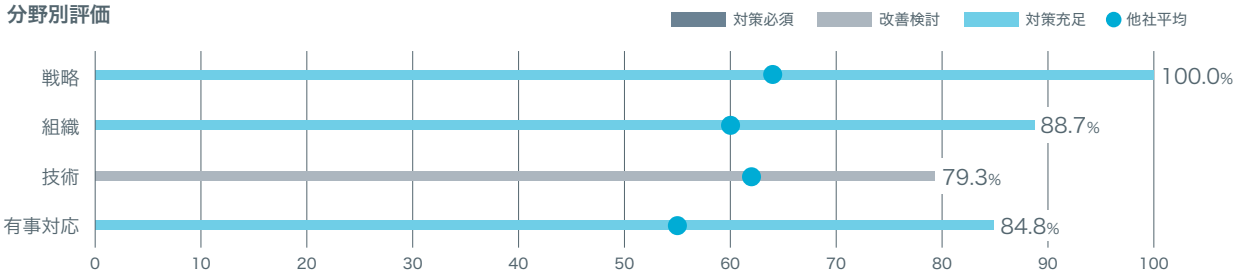
高レベルのセキュリティ対策を実施できています。
高度化する脅威に対応するため、
継続的に対策の高度化を図りましょう。

#### 得点(2024年11月時点)

| 当社グループ | 他社平均 | 他社平均(絞り込み)* |
|---|---|---|
| 843 / 1,000 | 618 / 1,000 | 633 / 1,000 |

＊他社平均(絞り込み):情報処理業界に所属する会社の平均値

#### 分野別評価




本報告書への掲載にあたり、Secure SketCHの評価結果の表記の一部(社名、分野別評価など)に編集を加えています。

## 課題（ベストプラクティスとギャップがある対策）の対応状況（2024年11月時点）

| リスクスコア | 未実施 | 実施中 | 対応見送り | 完了 | 計 |
|---|---|---|---|---|---|
| 高 | 0 | 0 | 0 | 0 | 0 |
| 中 | 7 | 0 | 17 | 2 | 26 |
| 低 | 0 | 1 | 5 | 4 | 10 |
| 計 | 7 | 1 | 22 | 6 | 36 |

## （参考）リスクスコア算出基準

### 発生可能性

| 発生可能性スコア | 発生する可能性 |
|---|---|
| 1 | 皆無 |
| 2 | 現実的ではない |
| 3 | 起こり得る |
| 4 | いつ起きてもおかしくない |
| 5 | 今起ころうとしている |

×

### 影響度

| 発生した時の影響スコア | タイプ① ミッション（サービスへの影響度） | タイプ② 目的（組織目標への影響度） | タイプ③（安全性の確保への影響度） |
|---|---|---|---|
| 1 | 安全にいつも利用できる | 営業利益・信頼性に損害なし | 情報が安全に保護されている |
| 2 | 遅延するが支障がない | 営業利益または信頼性に損害を与える（回復までにかかる時間は半年未満） | 取り扱い注意情報が漏えいする、もしくは不正アクセスされる |
| 3 | 時々利用できない | 営業利益または信頼性に損害を与える（回復までにかかる時間は半年以上） | 機密情報が漏えいする、もしくは不正アクセスされる |
| 4 | 継続的に利用できない | 営業利益または信頼性に損害を与える（回復までにかかる時間は1年以上） | 20,000件未満の個人情報が漏えいする、もしくは不正アクセスされる |
| 5 | 利用できる見込みがない | ビジネスの継続危機 | 機密情報や20,000件以上の個人情報が漏えいする、もしくは不正アクセスされる |

| | | 発生した時の影響スコア* | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 発生可能性スコア | 5 | 5 | 10 | 15 | 20 | 25 |
| | 4 | 4 | 8 | 12 | 16 | 20 |
| | 3 | 3 | 6 | 9 | 12 | 15 |
| | 2 | 2 | 4 | 6 | 8 | 10 |
| | 1 | 1 | 2 | 3 | 4 | 5 |

■ Critical ■ High ■ Medium

*タイプ①～③のうち、一番大きいスコアを採用

CIS RAM(Center for Internet Security® Risk Assessment Method)に基づき策定

# 情報セキュリティ対策

日々、複雑化・高度化が進むサイバー攻撃など、増大する情報セキュリティの脅威に対応するため、当社グループでは、「人」「技術」「物理」の3つの側面から、情報セキュリティ対策を推進しています。

## 人的情報セキュリティ対策

インシデント防止を目的に、従業員の知識習得とスキル向上を目指した教育・訓練および啓発活動を継続的に実施しています。

### 情報セキュリティ教育

従業員が情報セキュリティ対策のルールや、インシデント発生時の通報・初動対応の手順について正しく認識し行動できるよう、集合研修や動画教材を取り入れたオンライン研修を実施しています。各研修の実施後にテストを行い、理解度の低い項目は教材へ反映することで、理解度の向上を図っています。

パソコン紛失による情報漏えい防止対策を啓発する動画教材

また、受講状況をトラッキングして未受講の従業員に向けてリマインドし、受講の徹底に取り組んでいます。課題や受講率を含めた研修の結果を情報セキュリティ委員会に報告しています。

#### 主な教育コンテンツ

| 対象 | 実施内容 |
|---|---|
| 全従業員 | 情報セキュリティ対策の必要性や基本的な情報セキュリティルールの説明、<br>社外の主なインシデント事例の周知、<br>リモートアクセスの利用に関するルールや注意事項の説明 |
| 新入社員<br>（新卒・キャリア採用） | 情報セキュリティ対策の必要性や基本的な情報セキュリティルールの説明 |
| グループ会社や特定の業務に関わる従業員 | 業務・要望を配慮したコンテンツ（営業担当者向け研修、開発担当者向け研修） |

#### eラーニングの受講状況（全従業員向け年次教育、2024年11月末時点）

$$85.9\% \left[ \frac{\text{eラーニング受講完了者}}{\text{全従業員}^{*}} \times 100 \right]$$

*任意受講の従業員も母数に含まれています

## 標的型攻撃メール訓練

IPA（情報処理推進機構）が発表している組織に対する情報セキュリティ10大脅威[*1]では、標的型攻撃メールを含む、メールを利用した脅威が常に上位を占めています。
当社グループでは、教育により標的型攻撃メールの特徴を学び、不審なメールが届いてもメールや添付されたファイルを開封したり、リンクをクリックしたりしないよう従業員への意識付けを行っています。また、標的型攻撃メールを疑似体験する訓練を行い、メールの開封率や通報率[*2]を算出することで、標的型攻撃メール対策の理解度を確認しています。訓練の結果は情報セキュリティ委員会へ報告し、教材に組み込むことで、標的型攻撃メールへの対策のさらなる強化に努めています。

＊1 組織に対する情報セキュリティ10大脅威：IPA（情報処理推進機構）発行「情報セキュリティ白書2024」P16
＊2 通報率：「従業員からの通報件数÷訓練メール送付数×100」で算出

## レッドチーム演習

実環境でレッドチーム（攻撃側）とブルーチーム（防御側、情報セキュリティ部門）に分かれて実施するペネトレーションテスト*を行い、情報セキュリティ対策の実効性を検証する演習です。
検出された課題については、関係部門に伝達し連携して解決策を講じています。また、情報セキュリティ部門としても、より強固な対策、早期対応ができるように体制・手順などを見直しています。ペネトレーションテストを繰り返すことで、サイバー攻撃に関する知識と対応熟練度の向上に取り組んでいます。

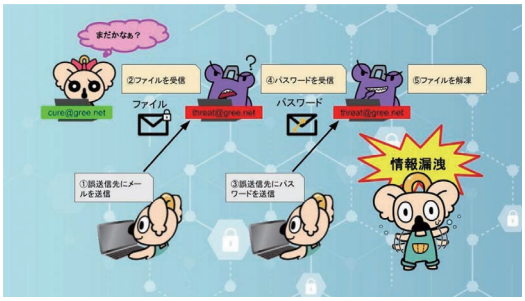
＊ペネトレーションテスト：攻撃者視点を取り入れて実施する情報セキュリティの専門家によるテスト手法

## インシデント対応訓練

インシデントが発生した際に、情報セキュリティ部門と関係部門がスムーズに連携して対応できるよう訓練しています。
この訓練では、情報セキュリティ部門が作成したインシデントのシナリオを使用し、被害を最小限に抑えながら、収束に導くためのシミュレーションを行っています。具体的には、情報セキュリティ部門および関係部門の担当者が、各自の役割を認識し、インシデント対応ガイドラインに基づいて対応できているかを確認しています。また、実施後に参加者からのフィードバックに基づき、インシデント対応チーム（GREE-IRT）の体制の見直し、マニュアルの整備といった改善につなげています。

### 情報セキュリティコラム

社内ポータルに情報セキュリティコラム「防衛本能」を掲載しています。従業員の意識向上を目的とした記事に加え、情報セキュリティ部門の活動の紹介や、情報セキュリティに関するさまざまな話題を提供し、関心を高めるとともに、情報セキュリティ部門へ気軽に相談できる雰囲気づくりを進めています。



コラム「防衛本能」イメージ

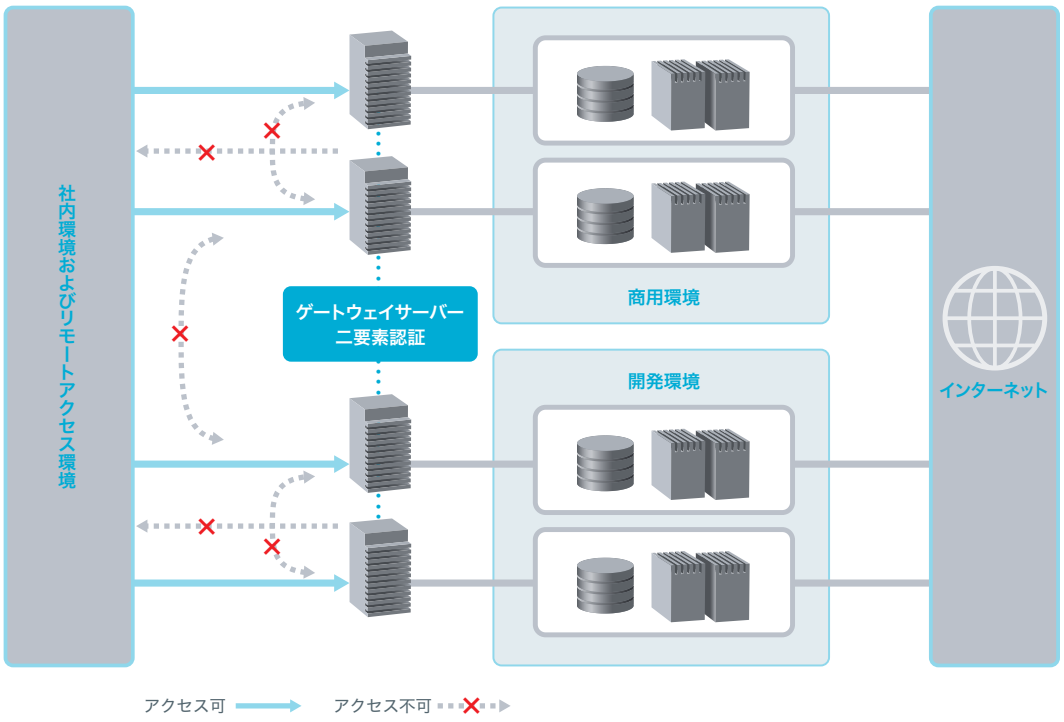
## 技術的情報セキュリティ対策

最新の技術やシステムを取り入れながら、さまざまな技術的対策を講じることで、情報セキュリティに対するリスクの軽減に取り組んでいます。

### 商用環境・開発環境へのアクセス制限

商用環境および開発環境へのアクセスには、ゲートウェイサーバーを経由することとし、不要な通信を阻止することでセキュリティを確保しています。ゲートウェイサーバーへのログインは二要素認証を導入しています。また、商用環境から社内環境および開発環境へのアクセスは原則として許可していません。

**商用環境および開発環境**



## 各サービスのネットワークセグメント管理

商用環境についてはサービスごとに専有の論理ネットワークセグメントを割り当て、ネットワーク間での通信を禁じています。また、アクセス権管理を徹底し、各サービスのネットワークへアクセスできるアカウントを限定しています。

## リモートアクセスの情報セキュリティ対策

オフィス外で勤務することによる情報セキュリティインシデントの発生を防止するために、ゼロトラストセキュリティモデル*を想定し、以下の対策を実施しています。

＊ゼロトラストセキュリティモデル：2010年にForrest Research社のJohn Kindervag氏によって提唱された「全てのアクセスを信頼しない」を前提に対策を行うセキュリティの考え方

**＜主なリモートアクセス対策＞**

- システムの重要度に応じた認証設定など技術面での対策を強化
- IDベースのリスク管理を導入。各IDの特性や権限、行動パターンのほか、専門家が分析した脅威インテリジェンス*などをもとにリスクを判定し、リスクレベルが高いと判断した場合はパスワード変更などの対応を実施
- リモートアクセスの利用者が遵守する事項を定めたガイドラインを策定
- PCを遠隔操作するアプリケーション、サービスを利用するための基準、ルール、手続きを明確化
- PCをオフィスから持ち出す際に上長に申請し承認を得る手続きを実施
- 利用者および利用を承認する管理者の責任を明確化するとともに、責任を認識させるための誓約への合意を要請
- 全従業員を対象とした教育を実施

＊脅威インテリジェンス：サイバー攻撃に関する情報を収集・分析し、それを元にした予測や対策を行うプロセスやデータ

## シャドーIT対策

情報漏えいなどのリスクを削減するため、シャドーIT対策に取り組んでいます。
ストレージサービスを含むクラウドサービスについて、利用を認めていないサービスの利用を検知し、利用者に対してクラウドサービス利用ガイドラインの遵守を促しています。

## アカウント管理

社内環境および開発環境にアクセスできるアカウントは、ディレクトリサービスで人事情報と連携させているため、退職した従業員、休職・長期休暇している従業員のアカウントは即時に無効となり、各環境へのアクセスは不可となります。また、商用環境にアクセスできるアカウントは、各サービスでアクセス権限を管理し、定期的に権限の削除漏れがないかを確認しています。
システムの維持・管理のために発行される特権アカウントについては、システムに与える影響や外部からの攻撃、内部不正に利用されるリスクを踏まえ、特に重要なアカウントと認識し、特権アカウントの定義、アカウント付与を含めた管理方法、ログの取得ルールなどをガイドラインに定めています。

## エンドポイント対策

エンドポイントに対しては、以下の対策を実施しています。

**<主なエンドポイント対策>**

- OSなどのセキュリティパッチをIT資産管理システムから定期的に配信
  ―定期間パッチが適用されないPCには強制的に適用
- 定期的にセキュリティパッチの適用率を集計
- ドメイン参加やMDM（Mobile Device Management）によるポリシーの一括適用
- 各Windows PCのローカル管理者パスワードをユニークなものに自動で変更
- HDD・SSDを暗号化
- EDR（Endpoint Detection and Response）製品を導入し、ウイルス対策の実施およびプロセスの挙動などを監視・検知
- 定期的にエンドポイントに導入したセキュリティ製品のインストール状況や脅威の検知状況を分析

## 電子メール対策

スパムメールフィルターを導入しています。また、添付ファイルはアンチウイルス機能を利用して疑わしいファイルはブロックしています。

## クラウドストレージ対策

情報の保管およびデータの共有には、情報セキュリティ部門が安全性を確認したストレージサービスを利用しています。さらに、情報漏えい対策として、利用者がアクセス権を適切に設定するようルールを設け、周知しています。また、CASB（Cloud Access Security Broker）を導入し、アクセス権が適切に設定されているかを確認しています。

## ネットワーク境界対策・社内LAN情報セキュリティ対策

インターネットと社内LANの境界対策、および社内LANの情報セキュリティ対策として以下を実施しています。

**<主なネットワーク境界・社内LAN対策>**

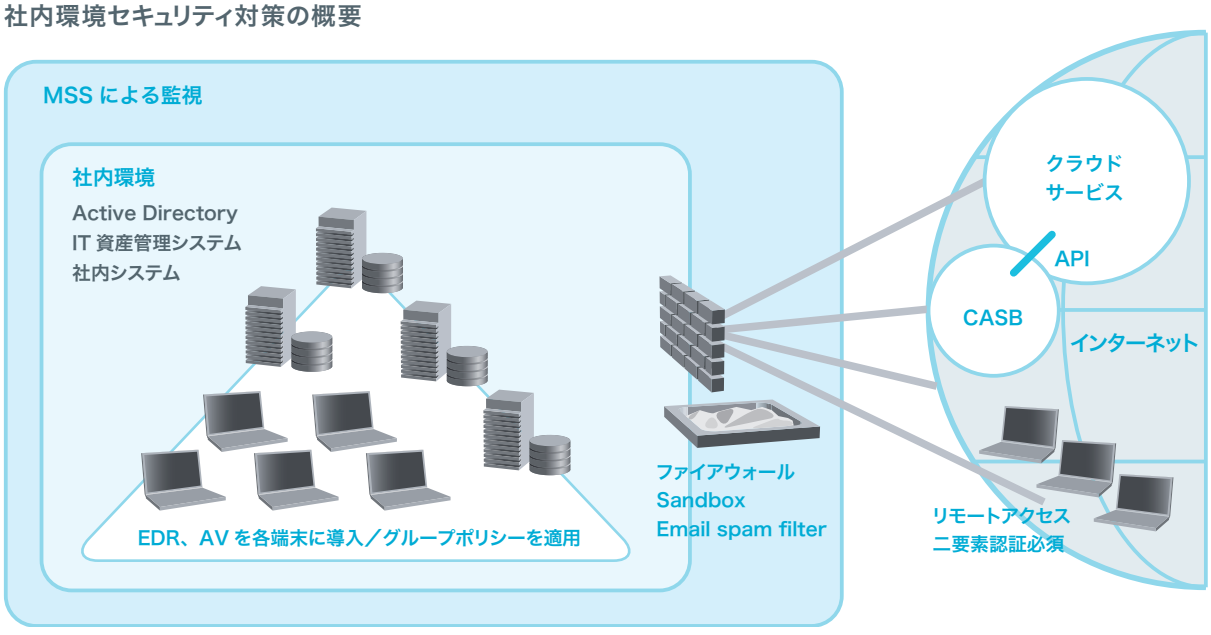
- ファイアウォールを設置し、境界防御を実施
- Webからダウンロードしたファイルは Sandboxを利用して挙動解析を行い、疑わしいファイルをブロック
- 社内LANへのアクセスは802.1x認証*を必要とし、開発用・ゲスト用LANは、用途やデバイスに応じて接続可能なシステムなどを適切に管理

＊802.1x 認証：有線LANや無線LANにおけるユーザ認証の規格

## セキュリティログ監視

MSS（Managed Security Services）を導入し、各種セキュリティログの監視、相関分析を実施しています。MSSから発報されたアラートに対しては、情報セキュリティ部門で対応しています。

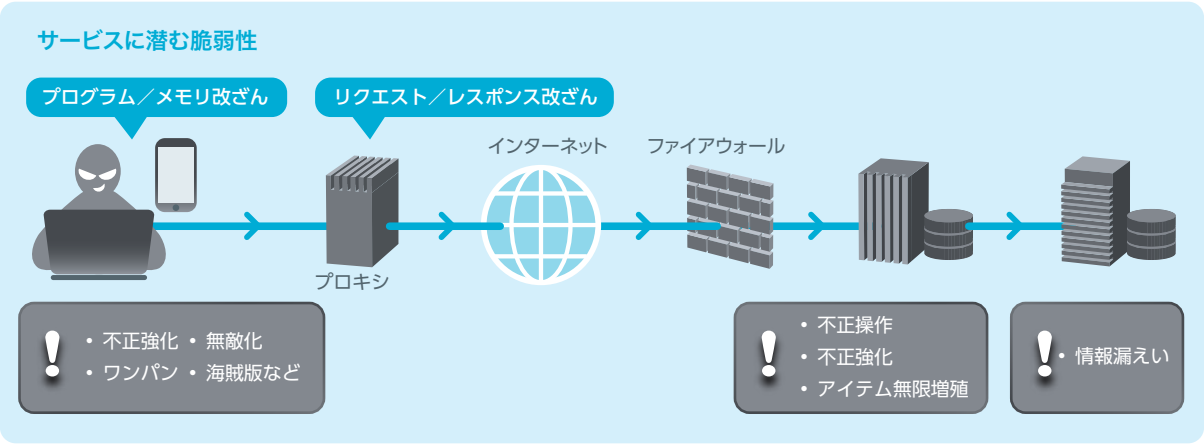
**社内環境セキュリティ対策の概要**



## 脆弱性診断

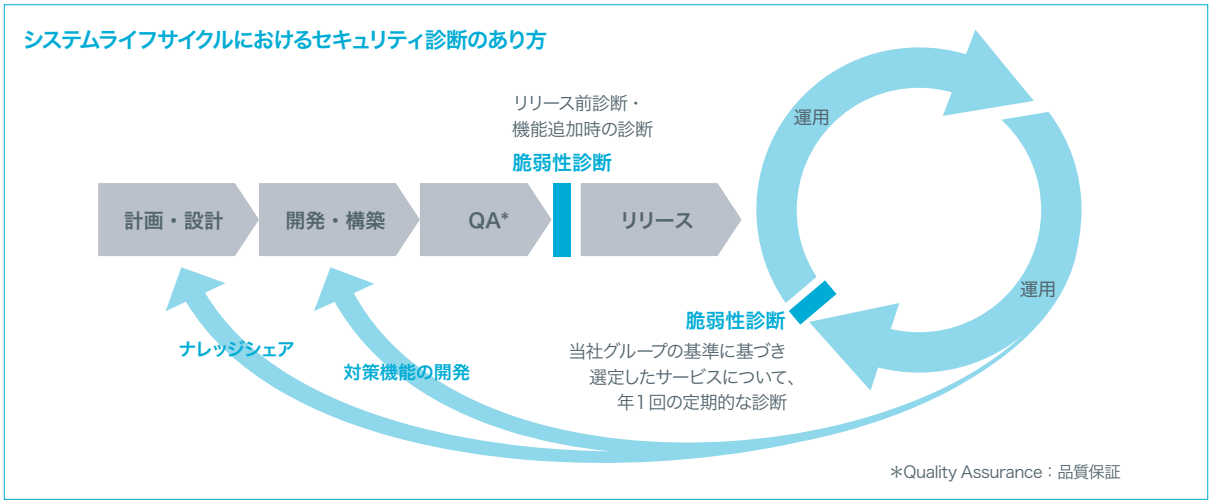
当社グループでは、お客さまが安全かつ安心して利用できるサービスを提供するため、ゲームやアプリケーションのリリース前後に「脆弱性診断」を実施しています。
サービスの脆弱性を利用してゲームデータやプログラムを改ざんし、ゲームを有利に進めることは「チート行為」と呼ばれています。このチート行為によってユーザー間で不公平が生まれないようにするため、サービスの「機密性」「完全性」「可用性」に対する脆弱性診断は重要です。
当社グループでは、情報セキュリティ部門に脆弱性診断を行う専門チームを設置し、ツールを用いた診断とソースコード診断、検知した脆弱性への対処方法の検討・提案、対処結果の確認を実施しています。脆弱性診断チームのメンバーは、日々技術力の向上に努め、診断で得た知見に基づくチート対策を整理して開発部門に提供しているほか、診断結果の報告や脆弱性対策をテーマにした意見交換も実施しています。

### 1. 概要：サービスに潜む脆弱性を発見し、被害に遭うリスクを低減

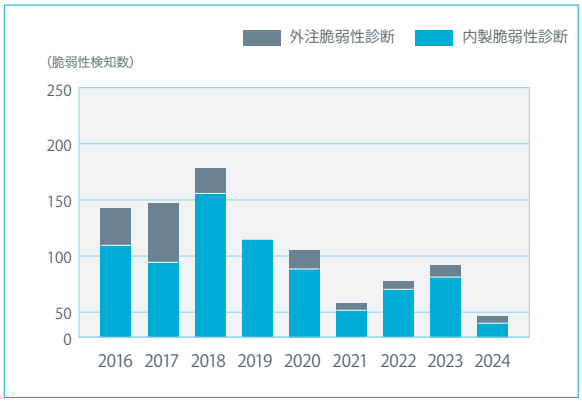



| | | |
|---|---|---|
| 活動の歴史 | 2012年 | • 脆弱性をついた不正が横行（探検ドリランドのカード複製やリアル・マネー・トレードなど）<br>• アプリケーションセキュリティチームを発足 |
| | 2013年 | • 外部の会社を利用した外注脆弱性診断を開始 |
| | 2015年～現在 | • セキュリティ診断チームを新設し、内製と外注の診断を統合管理する体制へ。<br>リリース後の定期的な診断、新規サービスの診断を継続して実施 |

## 2. 診断のライフサイクル

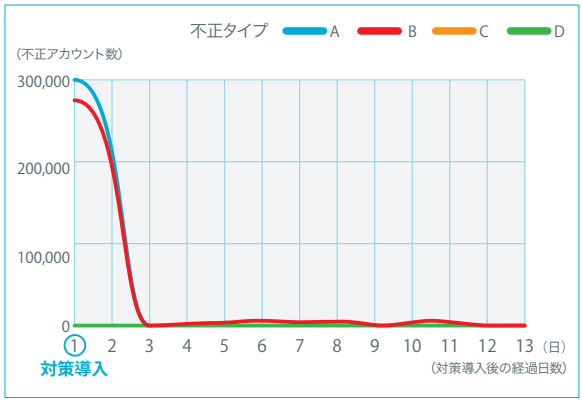



## 3. 診断実績




内製化に注力することで、対応を迅速化するとともに、開発部門へ詳細な対策を展開

## 4. 診断からの波及




### ＜脆弱性診断に基づくチート行為対策の実施例＞

- 海賊版ゲームの解析結果をもとにチート行為対策を立案。50万件の不正アカウントを廃止
- チート対策機能を内製で開発し、サービス部門に提供。一般的な対策を使用せず、独自開発の機能を組み込むことで、チート行為による解析がより困難となるよう機能を強化

## 脆弱性情報の収集

システムやアプリケーションの脆弱性を検出し、迅速に対応するために、有識者による情報収集および社内構築の情報集約機能を活用し、脆弱性情報やセキュリティニュースなどの情報を収集しています。また、緊急度の高い脆弱性情報に関しては、コミュニケーションツールを利用して社内に展開し、対処を促しています。

# 物理的情報セキュリティ対策

情報資産の管理・保管施設および情報処理施設を保護するために、さまざまな物理的対策を実施しています。

## 物理エリアのレベル分け

従業員が入退場するエリアについて、安全性のレベルに応じた管理を行っています。さらに、それぞれのエリアで取り扱い可能な情報の種類や保管方法の条件を定めています。

**エリアのレベル分け**


| レベル | エリア名 | エリアの説明 | 情報の取り扱いルール | 該当エリアの例 |
|---|---|---|---|---|
| 2 | 制限エリア | 従業員のなかでも特定の者のみがアクセス可能 | ほとんどの情報の取り扱いが可能です。ただし、極秘情報や機密情報は掲示してはいけません | サーバー室、金庫、外部倉庫 |
| 1 | 一般エリア | 従業員のみがアクセス可能 | 極秘情報や機密情報の掲示および保存は行ってはいけません。その他、取り扱いの多くに条件があります | 執務室、リフレッシュルーム |
| 0.5 | 共用エリア | 従業員に加え、入居しているビルへ入館できる者がアクセス可能 | 原則、極秘情報、機密情報、取扱注意の掲示および保存は不可です | 来客スペース、セミナールーム |
| 0 | 公開エリア | すべての者が自由にアクセス可能 | 原則、極秘情報、機密情報、取扱注意の掲示および保存は不可です | 自宅、通勤経路、お取引先、飲食店 |

## 入室管理

執務室への入室にはセキュリティカードによる認証が必要です。一部オフィスでは、ビルの出入口にセキュリティゲートを設置し、許可された従業員のみ入退場できるようにしています。
また、サーバールームなど重要な情報を扱うエリアでは、権限を絞り込んだセキュリティカードや監視カメラによってセキュリティを強化しています。

## クリアデスク・クリアスクリーン

離席する場合は、情報関連資産の施錠保管、およびPCの画面ロックまたはログオフを行い、認可されていない者によるアクセスや情報の消失などを防止しています。

## 機密文書などの廃棄

機密情報が含まれるデータおよびライセンスが供与されたソフトウェアは、データ消去や記憶媒体の物理破壊などによって確実に消去しています。また、機密情報の記載がある書類は、機密処理サービス会社を利用して廃棄しています。

# 情報セキュリティに関するコミュニケーション

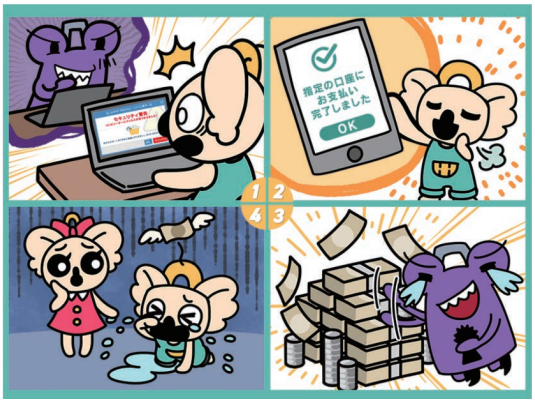
## 他社セキュリティ担当者との情報交換会

BtoCビジネスを主とした企業の情報セキュリティ担当者が参加する情報交換会に、当社グループの情報セキュリティ部門メンバーが参画しています。
参加したメンバーは、当社グループの情報セキュリティ施策についての発表やワーキンググループの企画などを通して、業界全体の情報セキュリティ向上に意欲的に取り組んでいます。

## インターネット利用者に向けた啓発コンテンツの提供

インターネットを利用する上での情報セキュリティリスクや利用者ができる対策を、楽しみながら学べるコンテンツを当社グループのコーポレートサイトで公開しています。オリジナルキャラクターによる4コマ漫画で、パスワードの安全な管理や、偽広告による詐欺被害から身を守る方法などを解説しています。

**偽警告による詐欺（架空請求）**




啓発マンガ「リティと仲間たちと学ぼう」

## 技術カンファレンスでの講演

当社グループは2020年から、さまざまなサービスを開発・運営するなかで得られた技術的な知見や、これから取り組んでいくチャレンジを社内外に紹介する「GREE Tech Conference」を毎年開催しています。2024年10月に開催したカンファレンスでは、情報セキュリティ部門のメンバーもスピーカーとして登壇し、セキュリティインシデント対応の体制構築や運用についてプレゼンテーションしました。


GREE Tech Conference 2024

グリーホールディングス株式会社
(GREE Holdings, Inc.)
https://hd.gree.net/