情報セキュリティ報告書

2023

GREE

CONTENTS

編集方針

報告書発行の目的

グリーは「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
2022年（2022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）

グリー株式会社
開発本部 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

パンデミック、国際情勢の変化などの外部環境に迅速に対応し情報セキュリティ活動を柔軟に変化させながら、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

当社グループの情報セキュリティ報告書をご覧いただきましてありがとうございます。

当社グループにとっての2022年は、大型ゲームのリリースや、メタバース事業のコンテンツ拡充など、全世界の皆さまにグループのサービスをより楽しんでいただけるよう、これまで以上に邁進した1年でした。また社会の動向に目を向けると、新型コロナウィルス感染症が当初より落ち着きを見せはじめた一方で、国際情勢の変化に伴い不安定な経済環境となった1年でもありました。

このような変化のなか、当社グループがお客さまに安定してサービスを提供するためには、事業活動を支える情報セキュリティをより堅牢・強固なものとすることが必要だと考えています。それは、情報セキュリティ部門を含む関係部門が環境変化に即した施策を迅速に実行するとともに、個々の従業員がセキュリティ意識を高く持ち、日々の業務のなかで実践していくという、グループ一丸となった活動によって達成することができます。

当社グループのインターネットサービスをご利用いただいている全世界の皆さまの安心につながるよう、ここに2022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

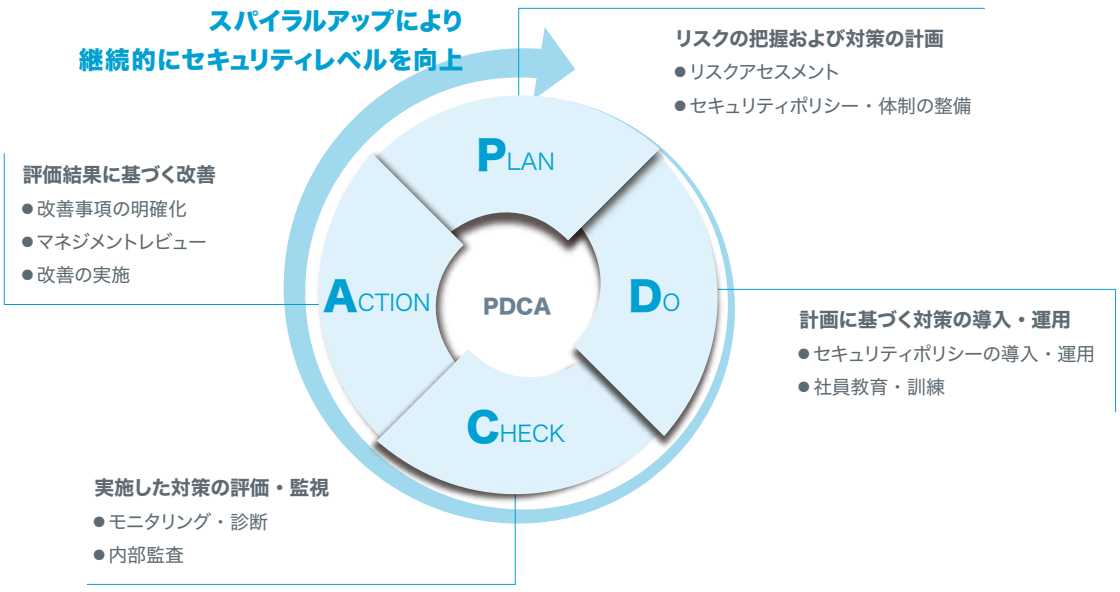
企業の経営資源は、長らく「ヒト」「モノ」「カネ」とされてきました。しかし、現在では第4の経営資源として「情報」が重視され、情報資産の効率的・効果的な活用が企業経営の重要な基盤の一つとなっています。
当社グループでは、情報資産を革新的なサービスの提供に活かしていけるよう、情報セキュリティ対策を経営課題として改めて認識し、情報セキュリティマネジメントを推進しています。

情報セキュリティ方針

グリーでは、お客さまからお預かりした情報を含む情報資産を適切に保護し、お客さまに安心して当社のサービスを楽しんで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、当社は「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、全社レベルの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。

情報セキュリティ目的の策定

役員および従業員の本方針および情報セキュリティに関する諸施策に対する意識向上ならびに継続的改善に資する目標として、「情報セキュリティ目的」を設定し、その達成に向けて取り組んでいきます。

情報セキュリティ目的の達成を阻害する事象への対応

当社事務所または社内システムへの不正な侵入または情報資産の漏えい、改ざん、紛失、破壊、利用妨害などの情報セキュリティ目的の達成を阻害する事象が生じないように、事前にこれらの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。

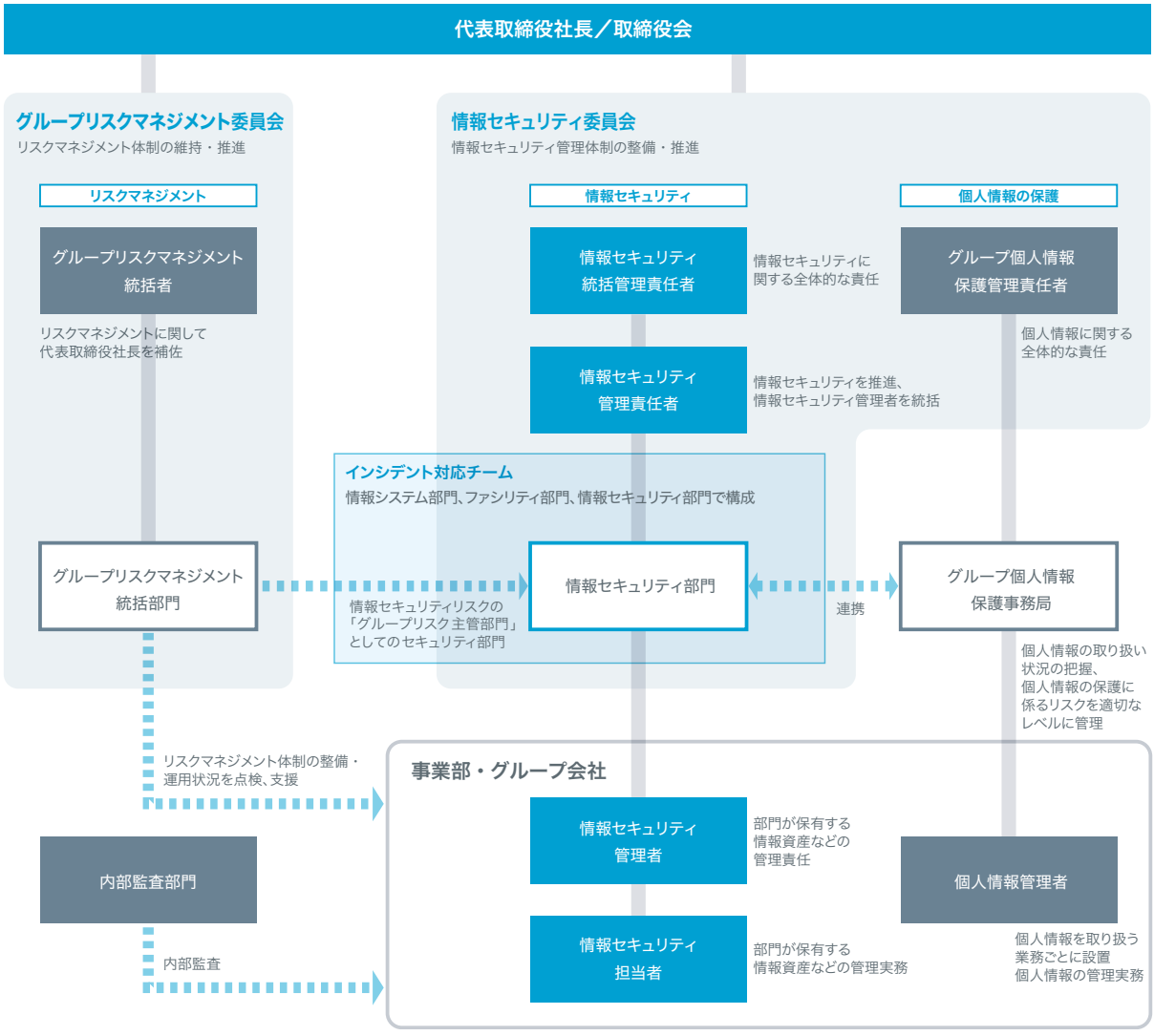
モニタリング体制の整備・充実

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、マネジメントレビューとして、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、改善を適切に実施していくため、「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、開発本部長、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、開発本部長が担い、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います。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、各事業本部の本部長が担い、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の維持・推進、およびリスクマネジメント関連各委員会・会議*が所管しないリスクについて検討・審議しています。

＊情報セキュリティ委員会と、ユーザーの利用環境がより適切・快適になるよう調査・検討する利用環境向上委員会

■ 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には、コーポレート本部長を任命しています。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のリスクマネジメントの運用状況などを点検するとともに、必要に応じて各部門・グループ会社におけるリスクマネジメントの整備・運用状況も直接点検したうえで、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

情報セキュリティ、不適切なサービスの設計仕様および表現、ユーザーによる不適切行為、システムの誤動作などのリスクごとに、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。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。

個人情報管理

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法務部門内にある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、情報資産の双方の保護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個人情報の利用に関して許諾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

法務部門内に設置している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情報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事務を担っています。

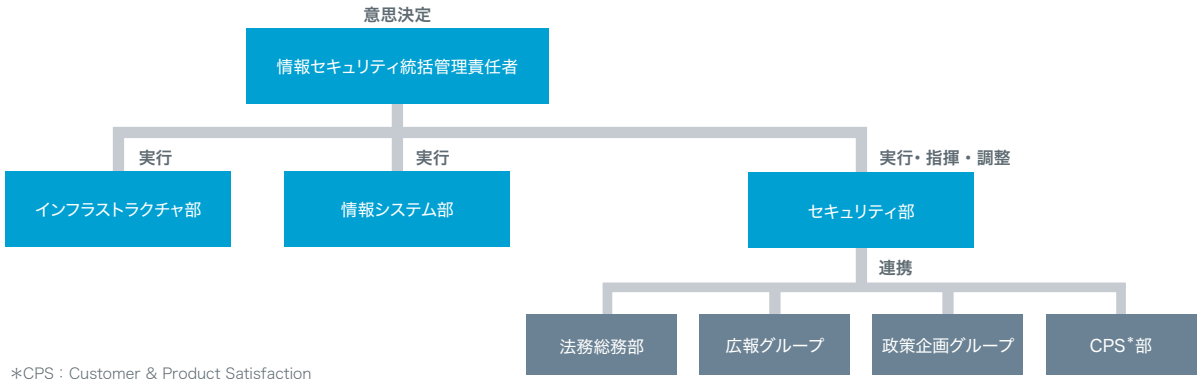
インシデント対応体制

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*）」を設置しています。同チームは、インシデントが発生した際の通知を受ける窓口となり、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、2016年12月に発生したインシデントとその対応を踏まえ、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。

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

インシデント対応体制



＊CPS：Customer & Product Satisfaction

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
セキュリティ部	実行 指揮 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 • インシデント対応の全体管理 • 対応方針の検討 • 他部門への対応依頼 • 専門的な調査 • 端末に関する現場でのインシデント対応 • 法務総務、広報、CPSなど関連部門への連絡
情報システム部	実行	• オフィス環境におけるインシデント対応 • 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	実行	• 商用環境におけるインシデント対応
法務総務部	対応	• 法的処置が必要な場合の対応
広報グループ	報告	• 社外への公表
政策企画グループ	報告	• 関連省庁への報告
CPS部	対応	• お客さまからのお問い合わせ対応

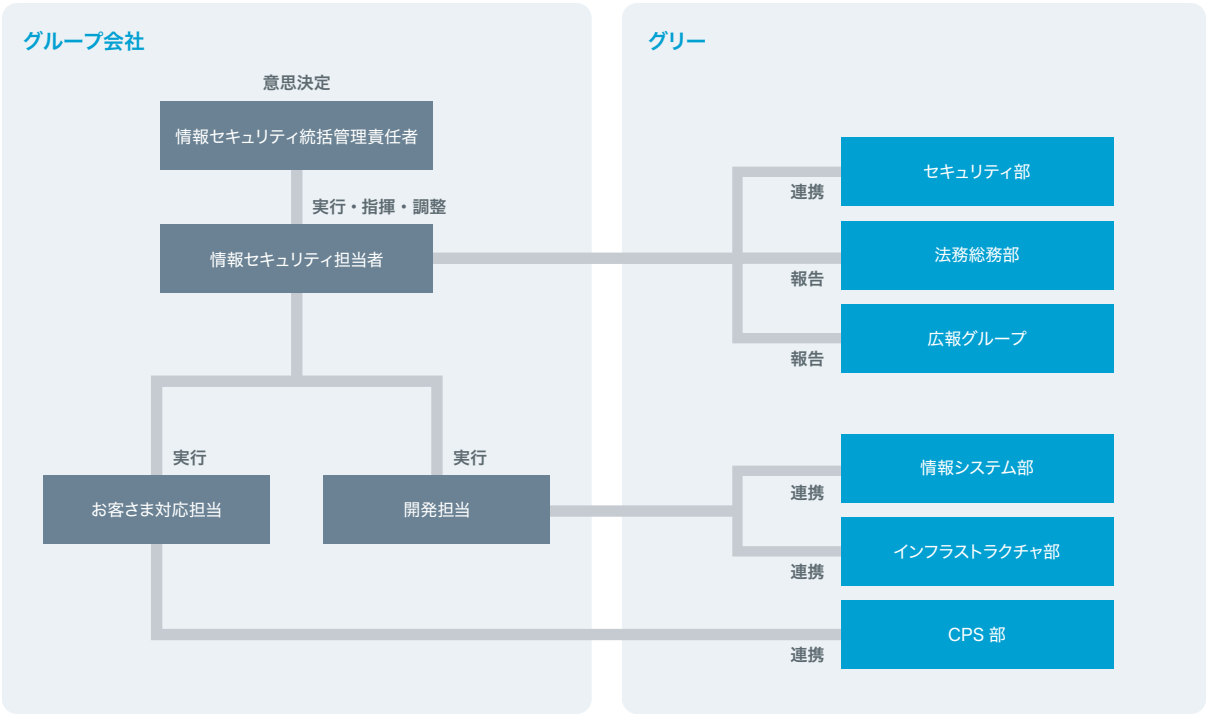
グループ各社の情報セキュリティマネジメント体制

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半期ごとに訪問し、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、情報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を行うなど、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、情報セキュリティ施策の確実な実行を推進しています。

＜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した対策の徹底
  （全体ミーティングやチャットでの周知・見回りなど）
- 情報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 指揮 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 • インシデント対応の全体管理 • 対応方針の検討 • 他部門への対応依頼 • 専門的な調査 • 端末に関する現場でのインシデント対応 • 端末に関するリモートでのインシデント対応 • グリー関連部門への連絡 • 関連省庁への報告、社外への公表 • 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、情報セキュリティに関する規程および細則を定めています。
また、規程・細則に基づき、実際の業務の進め方やノウハウに焦点を当てたガイドラインを作成しています。
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や、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を対象とした商用ガイドラインなどを整備しています。このほか、内部監査と個人情報保護に関するルールを定めた規程類も整備しています。
当社グループでは、教育や社内ポータルでの掲示などを通じて、従業員へこれらの規程類の周知徹底を図っています。

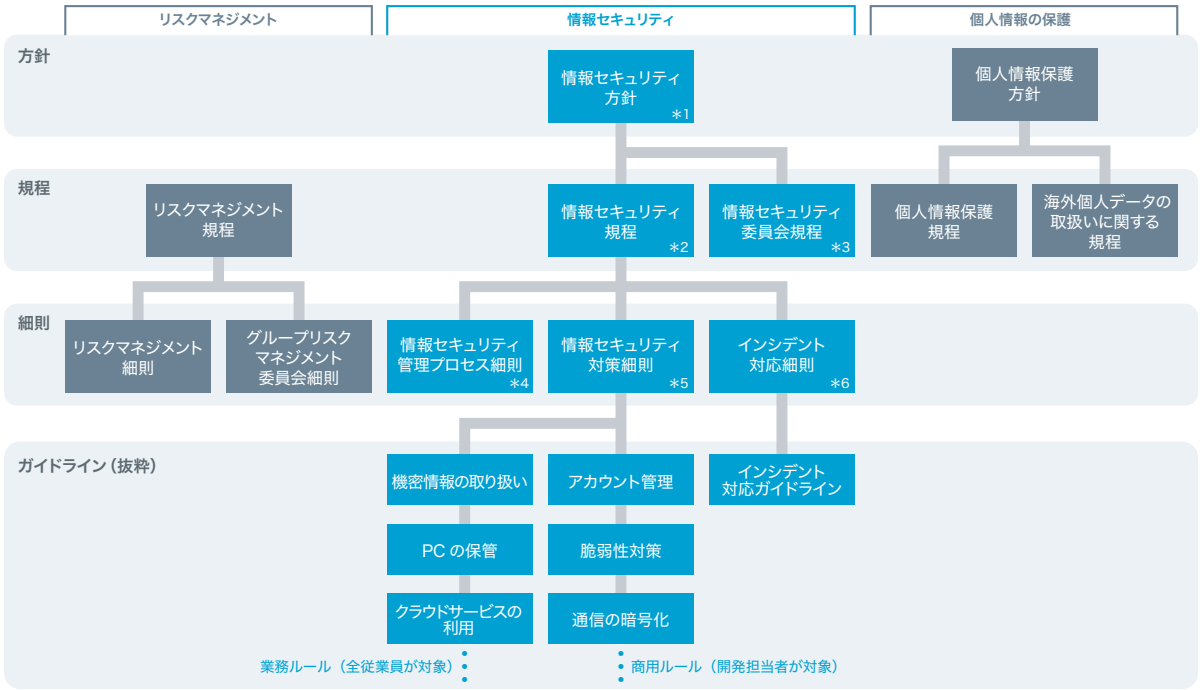
ガイドライン（一部抜粋）

カテゴリー		ガイドライン名
全従業員向け	情報資産の取り扱い	• 情報資産の機密性区分と保管ルール • 機密性に応じた情報の取り扱いエリア • 管理共用部における情報漏えい対策 • 情報の持ち運び方法 • ラベリング・文書管理 • ストレージサービスを利用した情報共有 • パスワード運用ルール
	PC・セキュリティカードの管理	• PCの保管・持ち出し • PCの管理者権限の利用 • USBメモリなどストレージデバイスの利用 • セキュリティカードの管理
	ネットワーク	• PCの無線LANアクセスポイントとしての利用
	業務委託・パートナー・ゲスト	• 業務委託業者利用におけるセキュリティ確認 • 社外パートナー向けコラボレーションツールのIP接続制限 • 社外パートナーとの情報共有 • ゲストが執務室に入室する際の注意事項
	社内サービス	• チャットツールでグループを作成する際の注意事項
	社外サービス	• クラウドサービスの利用におけるセキュリティ確認 • アプリケーション・Webサービスの利用制限
	メールの一斉配信	• メールマガジンなどお客さまへの一斉メール配信
	個人情報の取得	• サービス利用者から個人情報を取得するフォームの設定

ガイドライン（一部抜粋）

カテゴリー		ガイドライン名
エンジニア向け	インフラ	• ネットワーク全般 • 商用環境へのアクセス方法 • アカウント管理（識別・認証・認可） • SSH向け秘密鍵・公開鍵管理 • IPアドレス・Portアクセス制限 • インフラ構成・変更管理 • 特定の正社員のみアクセス許可させるサーバー • ログの保存 • SSL/TLSサーバー証明書・秘密鍵 • 利用するソフトウェア
	アプリケーション開発	• 考慮すべき脆弱性対策 • サポートツール • 開発で使用するツール・サービス • 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EU一般データ保護規則（GDPR）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、Pマーク、TRUSTe、PCIDSSなど）を取得していること
- 過去に事故が報じられていないこと
- 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

外部委託先管理

業務委託にあたっては、お取引先の技術力とともに、情報セキュリティ水準がグリーの定める水準に達していることが、非常に重要であると考えています。

そのため、機密情報や個人情報を取り扱う業務を委託する際には、必要な情報セキュリティ水準を満たしているかを審査し、管理・監督しています。

お取引先との連携

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="4">アクセスする情報</th></tr>
<tr><th>限定的（特定プロダクトの情報など）</th><th>社内情報全般</th><th>個人情報</th><th>マイナンバー</th></tr>
<tr><td rowspan="3">勤務場所</td><td>グリーやグループ会社のオフィス</td><td colspan="4">• 通常どおり契約や入社の手続きを行い、セキュリティ研修や誓約書の案内があった場合は、それに従う</td></tr>
<tr><td rowspan="2">お取引先のオフィス</td><td colspan="4">• グリーやグループ会社のツールには委託した業務内容に必要な範囲でアクセス権を付与する
• アクセスはオフィスから行う</td></tr>
<tr><td>—</td><td colspan="3">追加対策事項の例（アクセスする情報によって異なる）
• ISMSやPマークなど認証の取得の有無
• チェックリストを用いた安全管理措置の実施状況確認
• 個人情報の委託手続き</td></tr>
<tr><td>それ以外</td><td>• アクセスするグリーやグループ会社のツールは必要なものだけに制限する
• 社外からお取引先への接続手段はお取引先の責任で用意する</td><td colspan="3">—
（取り扱いは控えること）</td></tr>
</table>

■ お取引先の選定

お取引先がアクセスする情報の機密性およびその業務エリアに応じて、セキュリティ管理体制の確認事項をガイドラインとして定め、評価したうえで選定しています。

■ 情報漏えい防止条項への合意

秘密保持義務を盛り込んだ契約を締結したうえで、取り引きを開始します。
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盛り込んだ契約を締結しています。

■ 社内ネットワークおよび社内システム利用時の手続き

お取引先がグリー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アドレスがお取引先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、必要な見直しを行っています。

■ 点検

カスタマーサポート、品質管理などお客さまの個人情報を取り扱う部門では、委託先の監督の一環として定期的に委託先監査を実施し、情報セキュリティ部門で監査結果を確認しています。

2022年に強化した情報セキュリティガバナンス

情報セキュリティガバナンスは、整備して終わりということはありません。
定期的に見直し、状況に応じて強化しています。2022年は主に下記に取り組みました。

■ パスワード運用ルールの強化

各種サービスを利用するうえでパスワードの設定は必須です。しかし、パスワード自体が単純なものであれば、設定したとしても安全性は低く、不正ログインや情報漏えいなどのリスクが高まるため、より複雑なパスワードとなるよう、設定に求める要件を変更しました。

■ 特権アカウント管理のガイドラインを整備

特権アカウントは、システムの維持・管理のために発行され、システムに大きな影響を与えるアカウントです。特権アカウントが外部からの攻撃や内部不正に利用されるリスクを踏まえ、従業員の理解および管理を徹底することを目的に、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ました。

■ PPAPの廃止

以前よりお取引先とのファイル共有方法としてPPAP*は非推奨としていましたが、改めて危険性が高い共有方法として禁止しました。社内告知やブログなどで従業員に啓発を行い、お取引先にも説明を通じてご理解いただき、安全な方法への切り替えを進めています。

＊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。

情報セキュリティアセスメント

情報セキュリティに関わるリスクのなかには事業へ多大な損害を与えるものも存在します。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「情報セキュリティアセスメント」を実施しています。

情報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遵守されているか（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、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。

情報セキュリティアセスメント

情報資産の洗い出し

事業部やサービス単位で、所有する情報資産およびその保護状況などを記載した「情報資産台帳」を作成します。

	名称	内容	保管場所
1	ソースコード	XXXXXXXX	XXXXXX
2	メールアドレス	XXXXXXX	XXXXXX
3	取引先の情報	XXXXXXXXX	XXXXXX
4	取引先との契約書	XXXXXXX	XXXXXX
5	XXXXXXXX	XXXXXXXX	XXXXX

リスクの調査

情報セキュリティ部門は、情報資産台帳のレビューで保護状況を確認します。
また、チェックリストやヒアリングによりルールの遵守状況を確認します。

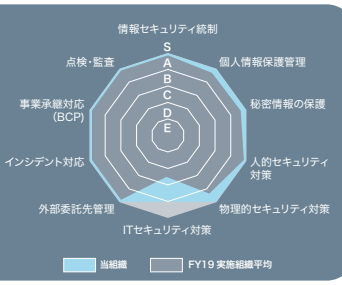
Point
事業やサービスの内容を盛り込んでカスタマイズしたチェックリストを使って確認します。

リスクの評価

情報セキュリティ部門は、発生可能性および重大性をもとにリスクの大きさを評価し、受容の可否や対応の優先度を検討します。

重大性 \ 発生可能性	5	4	3
5			
4			
3			
2			
1			

Point
他組織と比較してどれくらいセキュリティ対策ができているかについても、対象部門に伝え刺激を与えています。



リスクへの対応

対象組織は対応策を決め、対応計画を策定します。
情報セキュリティ部門は対応状況をモニタリングします。

	カテゴリ	想定されるリスク	事実・課
1	個人情報保護管理	情報漏洩	XXXXX
2	C: 秘密情報の保護	情報漏洩	XXXXX
3	D: 人的セキュリティ対策	情報漏洩	XXXXX
4	XXXXXXXXX	XXXX	XXXXX
5	XXXXXXX	XXXX	XXXXX

ガイドラインに基づく情報セキュリティ対策確認

2020年に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導入しました。このサービスを用いて、ISMS、NIST、CIS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、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2021年から、ベストプラクティスとギャップ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強化を進めています。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つねに把握し、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。

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

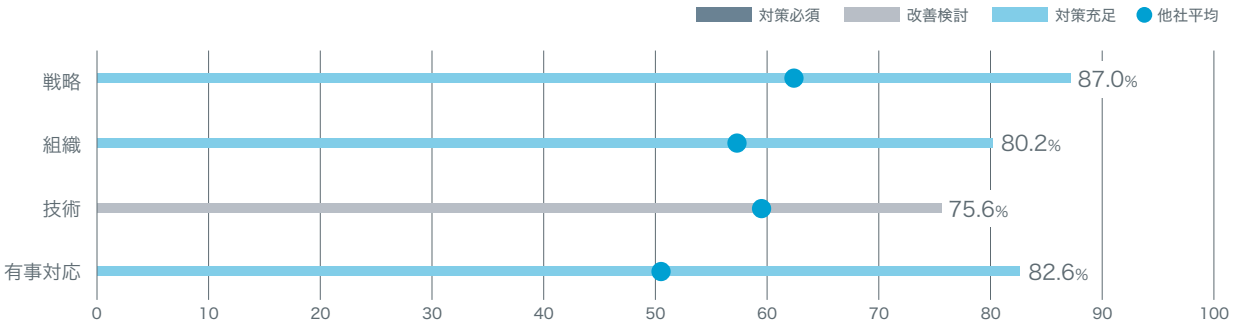
高レベルのセキュリティ対策を実施できています。
高度化する脅威に対応するため、
継続的に対策の高度化を図りましょう。

得点（2022年11月時点）

グリー	他社平均	他社平均（絞り込み）*
785（2021年 785）	597（2021年 591）	631（2021年 603）
1,000	1,000	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（2022年11月現在）

リスクスコア	未実施 (OPEN)	実施中 (IN PROGRESS)	対応見送り (PEND)	完了 (CLOSE)	計
高	0	0	0	0	0
中	8	1	16	1	26
低	2	1	7	0	10
計	10	2	23	1	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洩する、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）	機密情報が漏洩する、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洩する、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洩する、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（高） ■ high（中） ■ medium（低）

＊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

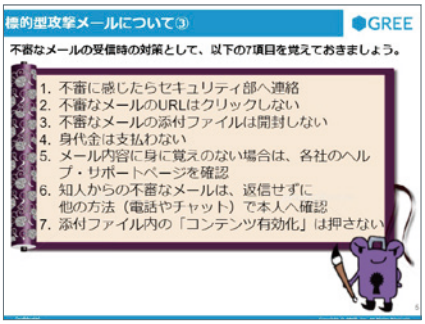
日々、複雑化・高度化が進むサイバー攻撃など、増大する情報セキュリティの脅威に対応するため、当社グループでは、「人」「技術」「物理」の3つの側面から、情報セキュリティ対策を推進しています。

人的情報セキュリティ対策

従業員の知識・スキル不足によるインシデントを減らすため、継続的に教育・訓練などを実施し、従業員の知識・技能の習得と維持・向上、啓発に取り組んでいます。

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eラーニングを実施しています。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。
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。



全従業員対象の定期研修

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、 社外の主なインシデント事例の周知、 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 （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（全社員向け年次教育、2022年11月末時点）

$$90\% \quad \left[\frac{\text{eラーニング受講完了者}}{\text{全社員}} \times 100 \right]$$

標的型攻撃メール訓練

2016年12月に標的型攻撃メールによるインシデントが発生しました。また、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大脅威では、メールを起因とする脅威が常に上位を占めています。このような状況を踏まえ、標的型攻撃メールに対する知識の向上や通報の徹底を目的とした訓練を実施しています。

当社グループでは、この訓練を通じてインシデントの通報率*の向上と早期対応につなげています。最近の標的型攻撃メールは明確な特徴が少なく、添付ファイルの実行やメールに記載されたURLのクリックを避けるのは困難であることから、被害が拡大する前に早期に検知することが重要です。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。

＊通報率＝従業員からの通報件数÷総発生件数×100

レッドチーム演習

実環境での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ための演習です。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、ブルーチーム（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。レッドチーム（攻撃側）とブルーチーム（防御側）に分かれて実施する

インシデント対応マニュアルの見直し

リモートアクセスなどの働き方の変化を踏まえて、インシデント対応マニュアルの見直しに取り組んでいます。過去、実際に発生したインシデントへの対応を振り返るとともに、他社事例やインシデント対応訓練の結果を参考にして、PCの回収方法の確認や、証拠保全の方法などを見直しています。

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、実施後に情報セキュリティ部門と関係部門の担当者間の連携に対する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）などの体制の見直し、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

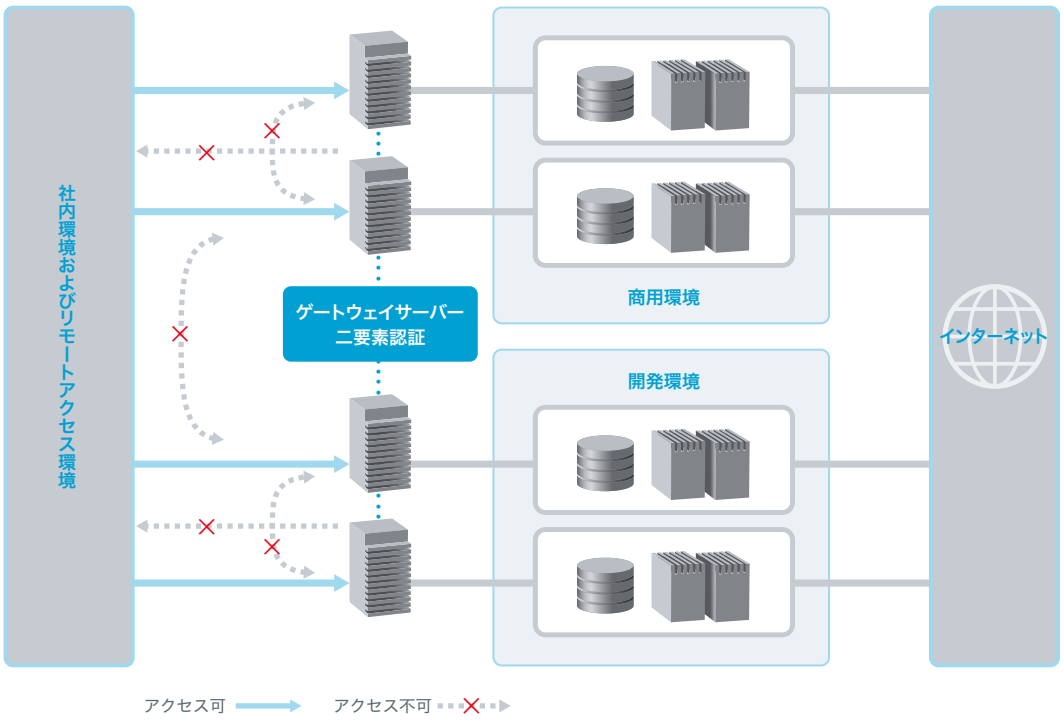
技術的情報セキュリティ対策

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



各プロダクトのネットワークセグメント管理

商用環境についてはプロダクト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、各プロダクト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

以前からリモートアクセスを導入していましたが、働き方改革の推進にともない利用が拡大しています。この状況を踏まえ、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。

＜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
- 利用者が遵守する事項を定めたガイドラインを策定
- 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
- IDベースのリスク管理を導入。通常とは異なる場所からのサインインや、専門家が分析した脅威インテリジェンスをもとにリスクを判定し、リスクレベルが高いIDはパスワード変更などの対応を実施

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、会社未承認の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、各プロダクトでアクセス権限を管理しています。定期的な確認と見直しなどを実施し、アクセス権限の削除漏れがないようにしています。

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。また、2016年12月のインシデントを教訓として対策を強化しています。

＜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
  ー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
  未適用PCの所有者に対しセキュリティパッチを適用
- ドメイン参加やMDM（Mobile Device Management）を利用した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、ウィ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ィ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。

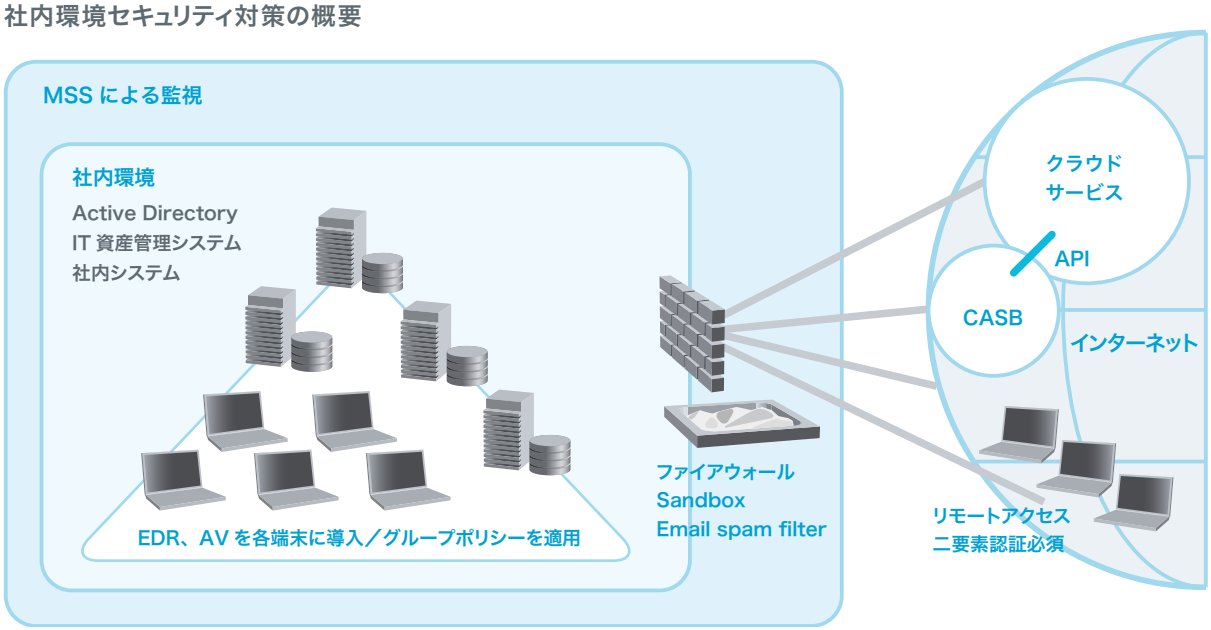
＜主なネットワーク境界・社内LAN対策＞

- 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、疑わしいファイルはブロック
- 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

セキュリティログ監視

マネージドセキュリティサービス（MSS）を導入し、各種セキュリティログの監視、相関分析を委託しています。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



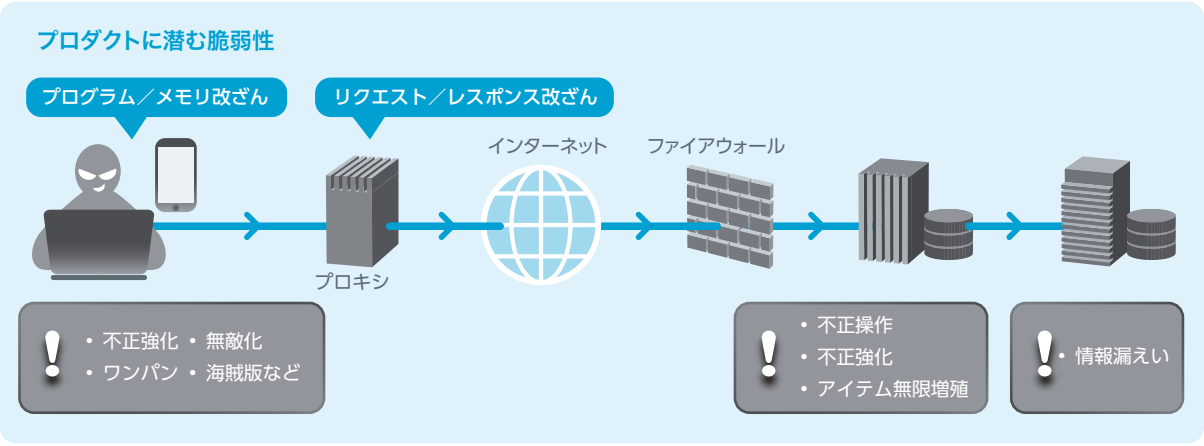
脆弱性診断

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。

残念ながら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、楽をしてゲームを有利に進めたり一人勝ちしたりするようなユーザーが存在します。このような不正を行うことは「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。

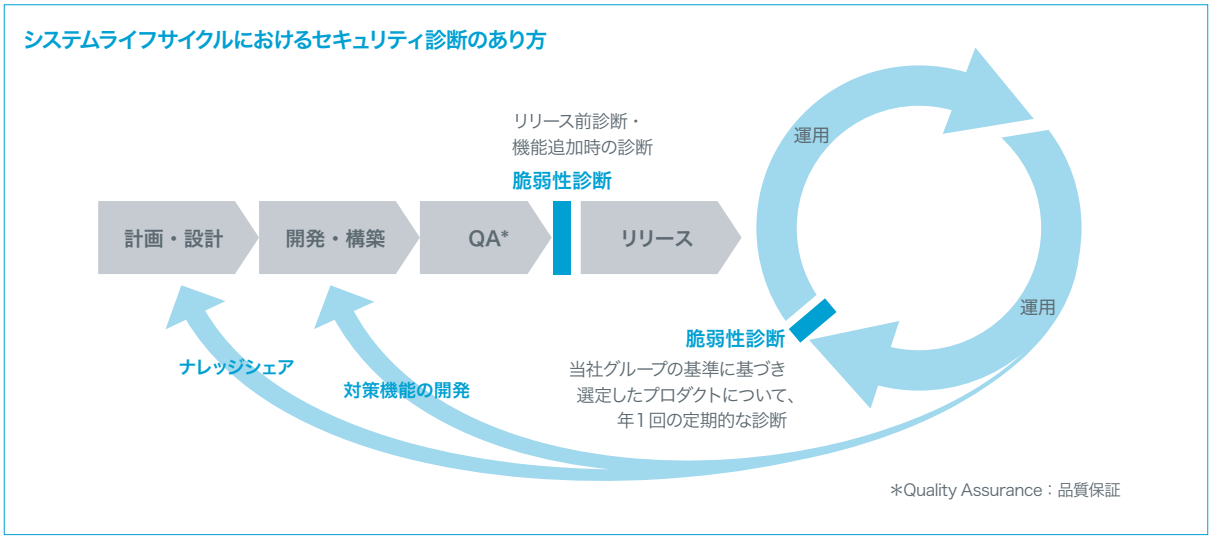
当社グループでは、情報セキュリティ部門に脆弱性診断を行う専門チームを設置し、ツールを用いた診断およびソースコード診断、検知した脆弱性への対処方法の検討・提案、対処結果の確認を実施しています。脆弱性診断チームのメンバーは、勉強会や社外の診断会社によるレクチャーを積極的に活用して、技術力の向上に努めています。また、診断で得た知見に基づくチート対策を整理して開発部門に提供しているほか、診断結果の報告会や脆弱性対策をテーマにした意見交換会も開催しています。

1. 概要：プロダクトに潜む脆弱性を発見し、被害に遭うリスクを低減

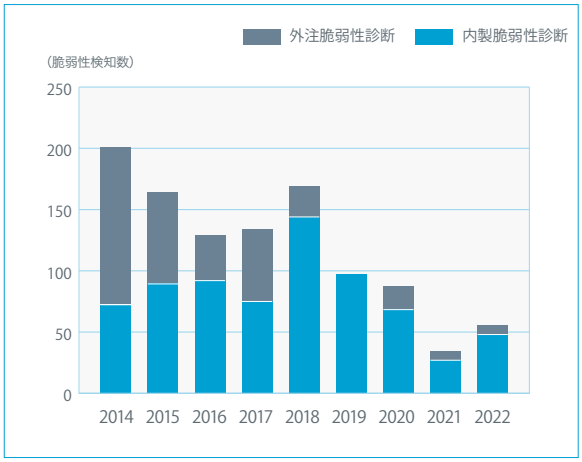


活動の歴史	2012年	• 脆弱性をついた不正が横行（探検ドリランドのカード複製やリアル・マネー・トレードなど） • アプリケーションセキュリティチームを発足
	2013年	• 外部の会社を利用した外注脆弱性診断を開始
	2015年～現在	• セキュリティ診断チームを新設し、内製と外注の診断を統合管理する体制へ。 リリース後の定期的な診断、新規プロダクトの診断を継続して実施

2. 診断のライフサイクル

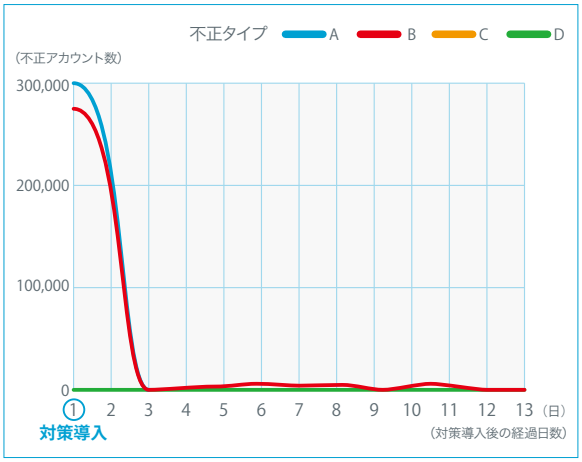


3. 診断実績



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主なチート行為対策>

- 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、プロダクト部門に提供。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、チーターによる解析がより困難となるよう機能を強化

OSINTを活用したセキュリティ検証

OSINT*で取得した情報を利用して疑似攻撃を行い、攻撃者が公開情報を悪用してシステムへの侵入が可能か、情報漏えいが発生するかなどを検証しています。

この取り組みにより、組織を取り巻く脅威を把握し、セキュリティ施策を強化しています。

＊OSINT (Open Source Intelligence)：一般に公開され利用可能な情報をもとに、機密情報などを収集、解析する手段・手法

<検証内容の例>

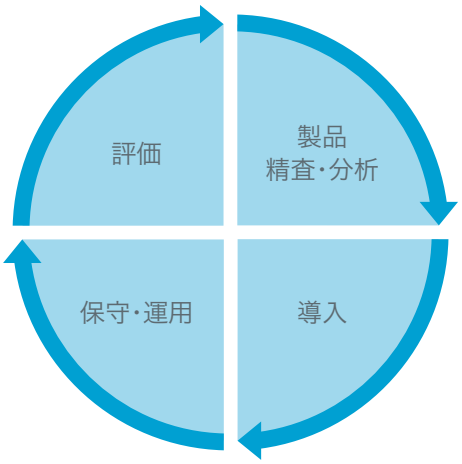
- 収集したメールアドレスに対するフィッシング
- ドメイン／IPアドレス／公開サービスなど外部リソースの分析
- GitHub、開発環境などから意図せず公開された情報の有無
- 漏えいした認証情報を用いたSaaSへの侵入

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。

ベンダーマネジメント

2020年4月から情報セキュリティ部門に「ベンダーマネジメントチーム」を設け、情報セキュリティ関連サービスの調達・開発・運用・保守について、提案書や見積書などを多角的に精査・分析・評価する取り組みを始めました。情報セキュリティ関連サービスを一元的に管理することで、最適なリソースやサービスを導入しつつ、ガバナンスの強化を進めています。



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確保しています。

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、機密情報の記録された媒体は、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

B to Cビジネスを主とした企業の情報セキュリティ担当者を対象として四半期ごとに開催される情報交換会に情報セキュリティ部門のメンバーが参加しています。
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、業界の情報セキュリティの前進に意欲的に取り組んでいます。

共同イベントでの啓発活動

2022年6月9日（サイバー防災の日*）に開催された啓発イベント「サイバー防災」に参画しました。「サイバー防災」は、インターネット事業や通信事業を展開する企業11社が参画し、インターネット利用者に情報セキュリティへの意識を高めていただくことを目的としています。参画する各社は共同でWebサイトを開設し、クイズをはじめ、楽しみながら学べるコンテンツを提供しています。
今回、当社はパスワードの安全な管理方法を啓発する活動を担当し、オリジナルキャラクターによる4コマ漫画とバーチャルYouTuber「KMNZ（ケモノズ）」による動画を用意しました。

＊サイバー防災の日：LINE（株）およびヤフー（株）が制定し、外出時に家の鍵をかけるように、インターネット上でも防犯意識を持つ（鍵をロックする）必要があることを啓発する日

「サイバー防災」のWebサイト

啓発マンガ「リティと仲間たちと学ぼう」

「KMNZ」による動画
REALITY（株）とIPプロダクションのFicty（株）が共同プロデュースする「KMNZ」は、“けもみみの国”からやってきた犬耳のリタと猫耳のリズからなるガールズデュオで、スマートフォン向けメタバース「REALITY」やYouTubeなどで2018年6月より活動しています。

オンライン学習サービスでの情報セキュリティ講義

（株）Schooが運営するオンライン学習サービス「Schoo」にて、情報セキュリティ部門のメンバーが、「情報セキュリティに対するリーダーとしての意識のあり方」「情報セキュリティの推進施策」「リモートワークにおける情報セキュリティ対策」の3テーマで講師を務めました。

Schoo講義より「情報セキュリティ ― 管理職編」

グリー株式会社

開発本部 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