SHISEIDO

Information Security Report 2026

情報セキュリティ報告書2026

CEOメッセージ

資生堂グループは、企業使命「BEAUTY INNOVATIONS FOR A BETTER WORLD（美の力でよりよい世界を）」の実現を目指し、生活者の皆さまから最も信頼されるビューティー企業であり続けます。

資生堂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。

資生堂は1872年の創業以来、「美」をテーマにさまざまな領域でグローバルにビジネスを展開しています。

近年では、生成AIをはじめとする先進的なデジタル技術の急速な発展により、ビジネスや働き方、顧客との関係性が大きく変化しています。急速に進むデジタル化において、当社グループではeコマースの積極的な展開に加え、会員サービス「Beauty Key」では2022年の提供開始以降、300万名を超える会員を獲得し、アプリを通じた統合的な顧客体験を実現しています。

さらに、当社の皮膚科学研究とAI技術を融合した「Beauty DNA Program」では、DNA検査に基づく肌の分析と、食事、睡眠、運動などのライフスタイルを含めた総合的なアドバイスを提供することで、より深いレベルでの美容サポートを実現しています。また、当社社内の働き方についても、生成AI技術の導入により、業務の効率化や意思決定の迅速化、創造的な価値創出を支援する環境が整いつつあります。

このように急速にデジタル化が進展するなか、情報セキュリティは単なるシステムの問題ではなく、事業を支える経営課題であると認識しており、当社グループでは2026年においても、情報セキュリティの強化を最重要課題の一つとして位置付けています。特に昨今、日系グローバル企業を標的とした巧妙なランサムウェア攻撃が激化し、事業継続に対する脅威はかつてないほど深刻になっています。これに対し、当社グループではゼロトラストに基づく強固な防御体制の構築を迅速に進めています。また、生成AIについては、安全な利活用を前提としたセキュリティ担保に注力しています。

当社グループでは、2030年に目指すビジョンを「ひととの繋がりの中で新しい美を探求・創造・共有し、一人ひとりの人生を豊かにする」と定めています。この実現に向けては、顧客接点の進化とビジネスの成長スピードを支える最新のIT・デジタル技術を活用したグローバル共通基盤の導入と、そこから取得できるさまざまなデータのさらなる利活用が重要です。

もちろんシステムもデータも安心・安全な環境で保護されていることがその前提であり、すべての基礎となる情報セキュリティの強化を通じ、生活者の皆さま、お得意先さま、お取引先さまに今まで以上に信頼いただけるビューティー企業であり続けるよう引き続き全力で取り組んでいく所存です。

本報告書では、資生堂グループの情報セキュリティに関する最新の取り組みを紹介しておりますので、ぜひご一読いただけますと幸いです。

株式会社資生堂
取締役 代表執行役
チーフオフィサー 社長CEO
藤原 憲太郎

情報セキュリティ担当役員メッセージ

最も信頼されるビューティー企業として認知され、商品・サービスを常に安心してご利用いただけるよう資生堂グループ一丸となって情報セキュリティ対策を推進しています。

本報告書冒頭に掲載した資生堂の社長CEOであり、資生堂グループ全体の情報セキュリティの総責任者である藤原のメッセージにもあるように、当社グループでは情報セキュリティの強化を重要な経営課題として日々取り組んでいます。

昨今、生成AIや自律的に動作するAIエージェントの登場により、テクノロジーは劇的な進化を遂げています。当社グループでは、これらをビジネス成長の強力なエンジンとして積極的に活用していく方針です。一方で、テクノロジーの進化はサイバー攻撃の巧妙化も招いており、特に日系グローバル企業を標的としたランサムウェア攻撃の激化は、私たちの事業継続における最大の懸念事項の一つとなっています。

このような環境下において、当社グループでは、セキュリティ関連の最新テクノロジーについて積極的に情報収集するとともに、それらを駆使した自律的かつ高度なセキュリティ基盤の構築に注力しています。

第一に、従来の境界型防御から脱却し、グローバル全拠点で「ゼロトラスト」の概念に基づいたソリューションの構築を加速させています。これにより、拠点やデバイスを問わず、常に安全なアクセス環境を確保し、ランサムウェアをはじめとする外部脅威からグループの資産を強固に守り抜きます。

第二に、生成AIやエージェントの安全な利活用です。革新的なテクノロジーをいち早く取り入れる際、その利便性を損なうことなくセキュリティを担保することが不可欠です。当社グループでは、人間だけでなくAIエージェントなどの「ノンヒューマン」も含めたすべてのアカウントに対し、セキュリティの高いID・アクセス管理を徹底する枠組みの構築を推進しています。これにより、人・モノ・AIが混在する複雑な環境においても、一貫したセキュリティレベルの維持を実現していきます。

また、技術的な対策のみならず、これらを扱う「人」の意識向上も継続します。強固なセキュリティガバナンスを構築するとともに、全世界の従業員を対象とした定期的な研修や、各地域のリーダー層への情報共有を通じて、グループ全体のセキュリティ文化を醸成しています。

情報セキュリティ対策に「完成」はありません。私たちは、進化し続ける脅威に対して常に先手を打ち、最新のテクノロジーを盾として、お客さまの大切なデータと私たちのビジネスを守り続けていきます。

資生堂グループの事業活動をご信頼いただき、また商品・サービスを安心して継続的にご利用いただけるよう、グループ一丸となって取り組んでまいります。本報告書が、当社グループの進化する情報セキュリティの取り組みをご理解いただく一助となれば幸いです。

株式会社資生堂
チーフオフィサー
チーフインフォメーションテクノロジーオフィサー
樋田 真

Contents

発行にあたって

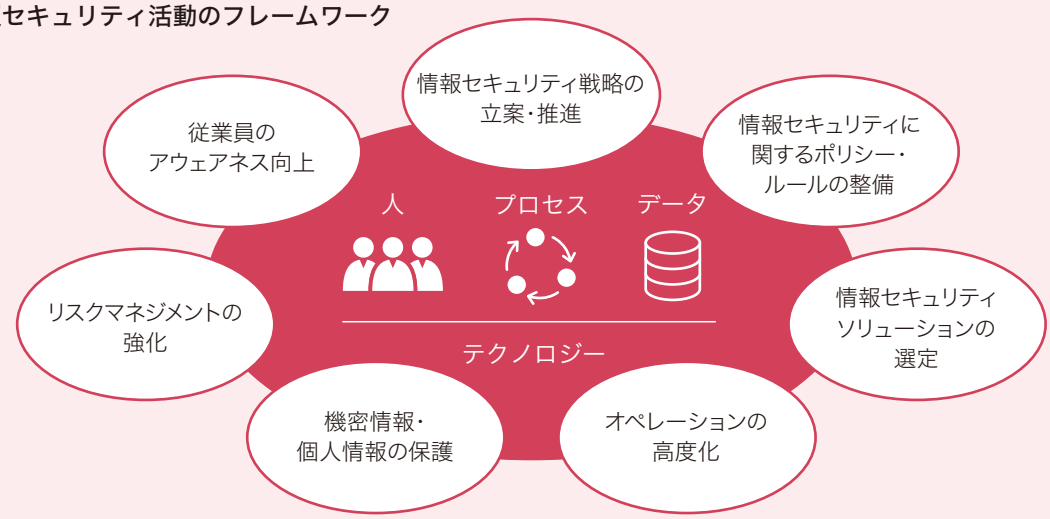
資生堂グループは、お客さまの「美」につながる多様な技術・知見に最新のデジタル技術を掛け合わせ、新たな価値の創造に挑戦し続けています。同時に、こうした取り組みの基盤となる情報システムと情報セキュリティの高度化に取り組んできました。本報告書は、ステークホルダーの皆さまに対する情報開示の一環として、情報セキュリティ活動にフォーカスを当てて発行するものです。当社グループにおける情報セキュリティ活動のフレームワークをベースに、経済産業省が発行している「情報セキュリティ報告書モデル」を参照し報告項目を設定。すべてのステークホルダーの皆さまにご理解いただけるよう、各項目についてわかりやすい文章記述とビジュアル表現に努めました。

■報告対象期間
2026年6月時点

■報告対象組織
株式会社資生堂およびグループ会社
個々の施策などで上記原則と異なる場合は対象を記載

■資生堂Webサイト 情報セキュリティ管理
https://corp.shiseido.com/jp/sustainability/compliance/security.html

情報セキュリティ活動のフレームワーク

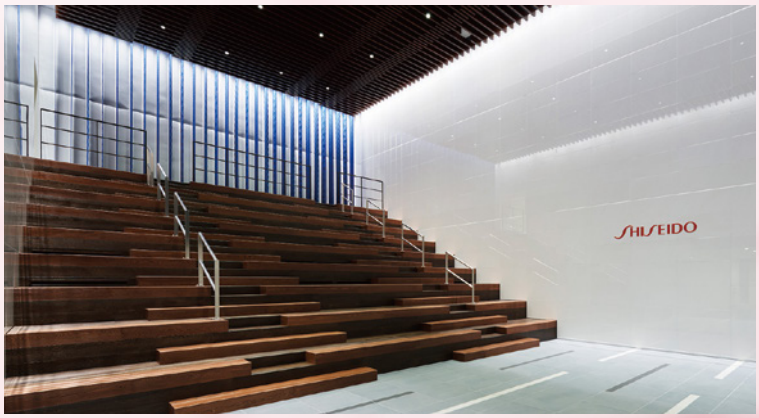


情報
セキュリティ
ガバナンス

情報セキュリティに関する方針

お客さま、取引先、従業員などの個人情報を守ることは、企業の重要な責任の一つです。また、企業としての競争力を向上させていくためには、研究開発や営業・マーケティングなどに関わる機密情報の適切な管理が不可欠です。資生堂グループは、こうした認識に基づき、全従業員を対象とした「資生堂グループ　情報セキュリティポリシー」を定め、グループ全体で一貫した方針のもと、各種情報資産の管理・運用に努めています。

サイバー脅威の動向は、国際情勢や法制度の変化、テクノロジーの進化などを背景に常に変化しています。さらに近年では、在宅ワークの増加など従業員の働き方も大きく変わっています。このような社内外の環境変化に伴うセキュリティリスクにも対応できるよう、情報セキュリティポリシーの継続的な見直しを行っています。



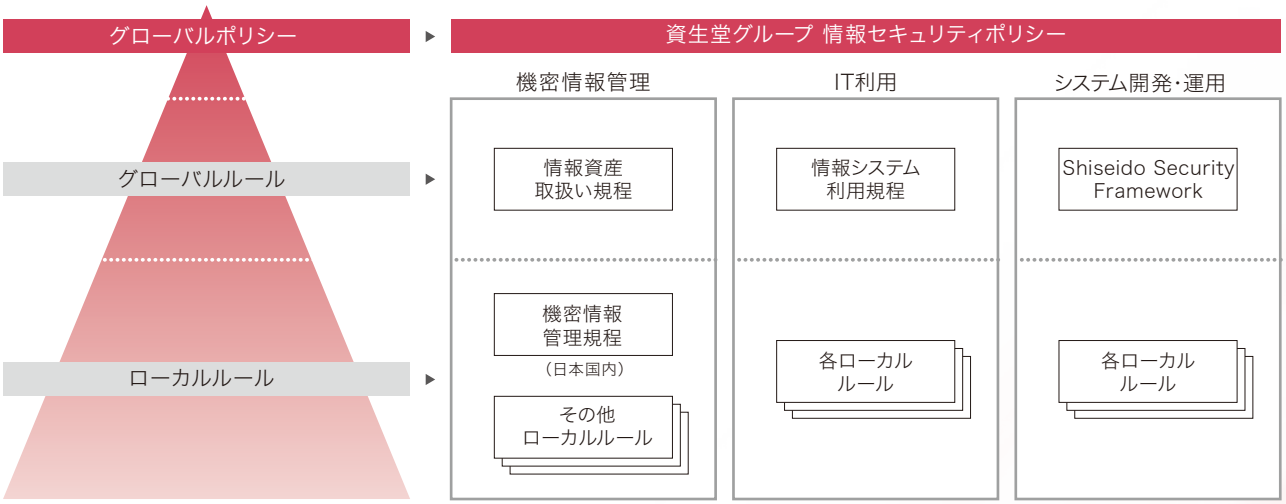
ポリシー・ルール体系

資生堂グループでは、「資生堂グループ　情報セキュリティポリシー」のもと、機密情報管理、IT利用、システム開発・運用などの管理項目ごとにグループ共通の諸規程を整備。これらを「グローバルルール」として海外の事業所も含めて遵守しています。

一方で、情報セキュリティにおいては、各国・地域固有の法制度や商習慣、システム環境に対応する必要もあります。そのため、各海外地域本社やグループ会社で「ローカルルール」を定め、それぞれの国や地域の実情に即した管理を推進しています。

情報セキュリティに関するポリシー・ルールの整備にあたっては、リスクマネジメントの国際規格ISO 31000、情報セキュリティ関連の国際認証規格ISO 27001、NIST（米国国立標準技術研究所）のNIST Cybersecurity Framework、Center for Internet Security※のCIS Controls、経済産業省のサイバーセキュリティ経営ガイドラインや確立されたベストプラクティスを参考にしています。

※NSA（米国国家安全保障局）、DISA（米国国防情報システム局）、NISTなどの政府機関と、企業、学術機関などが協力して、インターネットセキュリティの標準化に取り組む目的で2000年に設立された米国の団体。



マネジメント体制

グループ全体のマネジメント

資生堂グループでは、担当エグゼクティブオフィサーであるチーフインフォメーションテクノロジーオフィサー（CITO）が、情報セキュリティ管理体制の整備に責任を負っています。CITOは、機密情報管理、データ保護、情報システムのセキュリティ対策に関する規程類の整備と運用、それらの安全対策の実施、教育訓練などに責任・権限を有しています。また、その推進および実行は情報セキュリティ部門長が担っています。

なお、情報セキュリティに関する最終的な責任は、代表執行役 社長 CEO（Chief Executive Officer）が負っています。

また、資生堂本社内には「情報セキュリティ部」を設置しています。同部は半期ごとにインシデントの発生状況などをリスクマネジメント部門へ報告しており、重大なインシデントが発生した場合は取締役会へ直接報告するルールとしています。こうしたグループ全体のマネジメント体制強化の取り組みが認められ、2024年10月に一般社団法人日本デジタルトランスフォーメーション推進協会 セキュリティ部会主催の「日本セキュリティ大賞 セキュリティ対策・運用部門」で優秀賞を受賞しました。

参照　https://security-awards.jp/winners.html

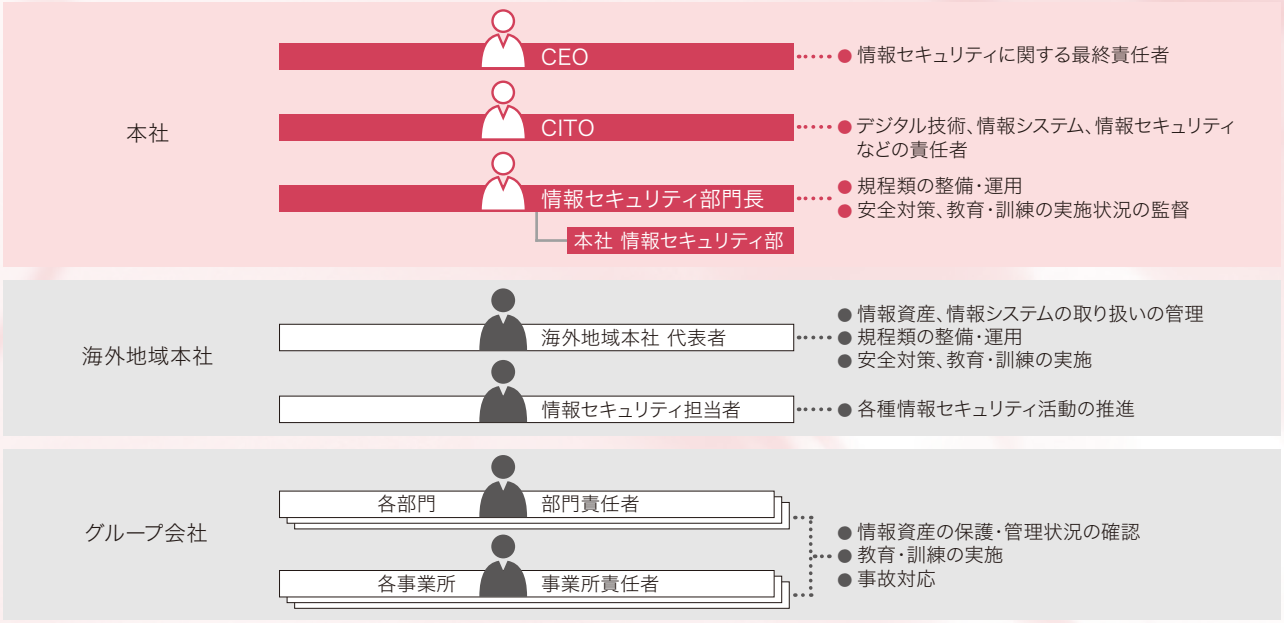
海外地域本社におけるマネジメント

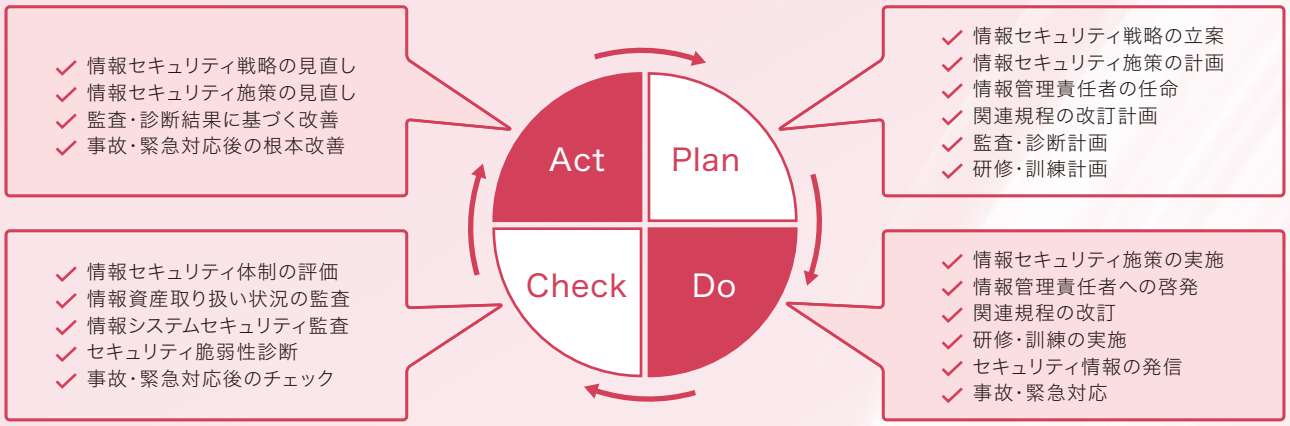
各海外地域本社においては、その代表者が管轄地域内の情報資産と情報システムの取り扱いを管理しています。機密情報管理、情報システム管理、情報セキュリティ対策に関する規程類の整備および運用の徹底、安全対策の実施、教育・訓練などの情報セキュリティ全般に責任を負っています。

また、各海外地域本社には、情報セキュリティ担当者を配置し、資生堂本社と連携して情報セキュリティ活動の継続的な改善に努めています。

グループ会社におけるマネジメント

資生堂グループ各社の各部門・事業所の責任者は、部門・事業所で取り扱う情報資産の保護・管理状況を定期的に確認するとともに、従業員への教育・訓練、取り扱い状況に関する自己点検、および事故発生時の対応などを行っています。





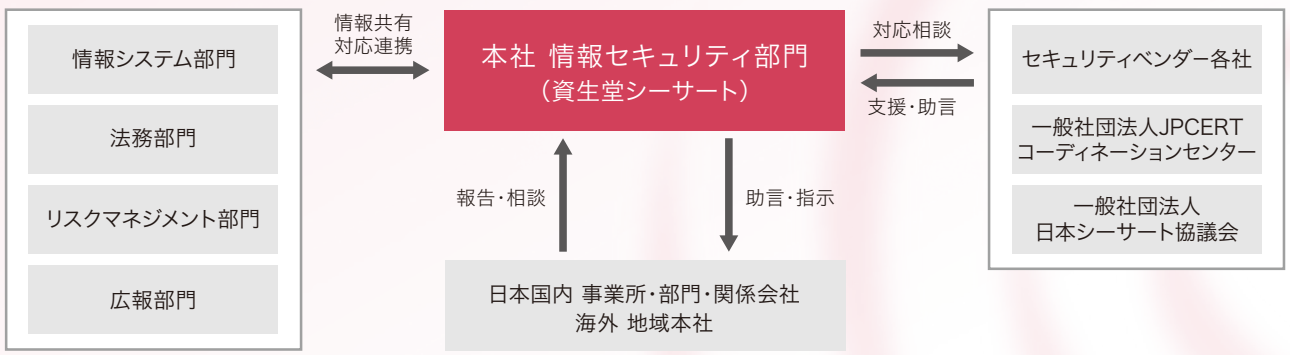
インシデント発生時の体制

情報セキュリティに関わるインシデントなどが発生した際は、情報セキュリティ部が窓口となり、その影響度に応じてリスクマネジメント部門や情報システム部門と連携して対応することとしています。また、海外事業所でのインシデントについては、各海外地域本社の情報セキュリティ担当者やチームが窓口となって、情報セキュリティ部などとともに対応にあたる体制を整備しています。

あわせて、セキュリティインシデントに迅速に対応できるよう、情報セキュリティ部やリスクマネジメント部門、情報システム部門など複数部門のメンバーが所属する資生堂シーサート（Shiseido CSIRT：Shiseido Computer Security Incident Response Team）を整備。インシデント関連情報や脆弱性・攻撃予兆情報を収集・分析し、必要な対策を実行しているほか、外部専門機関の協力を得て全海外地域本社のセキュリティ担当者が参加する「インシデントレスポンス訓練」を実施しています。また、高度な統合型セキュリティソリューションを導入し、インシデントの予防と発生時の影響の最小化を目指しゼロトラスト化を加速させています。

資生堂シーサートは一般社団法人日本シーサート協議会に加盟登録しており、各種ワーキンググループや毎年行われる分野横断的演習などに参加しています。また、そのほかの外部の情報セキュリティ専門機関や、他社の情報セキュリティ部門とも緊密にコミュニケーションをとっています。

このほか、情報セキュリティ部による事故対応訓練を年2回以上実施しており、そこで確認された改善点などを「事故対応マニュアル」に随時反映して対応能力の向上に努めています。



生産拠点での情報セキュリティ体制

生活者の皆さまへ資生堂の商品を安定的にお届けするために、生産拠点のセキュリティ対策も強化しています。この一環として、2020年から国内外の工場で「工場セキュリティアセスメント」を順次実施しています。

日本国内の工場は、2023年度中にすべての拠点においてアセスメントを完了しました。アセスメントが完了した日本国内の工場に関しては、工場のセキュリティを担当するグループと情報セキュリティ部による月次ミーティングを設定し、アセスメント後のセキュリティ対策強化、確実な是正対応を推進しています。また、セキュリティインシデントレスポンス訓練を年1回実施することで、工場内でのセキュリティインシデント発生時の対応体制やプロセスを確認するとともに、対応力の強化を図っています。

サプライチェーンの情報セキュリティ管理

資生堂グループが保有する個人情報や機密情報を取引先が利用する場合や、グループの事業継続や品質確保に大きく関わる業務を取引先に委託する場合は、委託業務の遂行過程で適切な情報セキュリティが確保されるよう管理・監督に努めています。「資生堂グループ　サプライヤー行動基準」には「機密情報・個人情報の保護」を明記しており、各取引先にこの遵守を要請するとともに、重要な情報を取り扱う業務を委託する取引先に対しては情報セキュリティ体制を確認し、必要に応じて安全管理措置の実施を求めています。

従業員のセキュリティアウェアネス

資生堂グループでは、情報セキュリティに対する従業員のアウェアネス向上のためにグローバル共通のeラーニングプラットフォームを導入し、品質が担保されたトレーニングを全海外地域本社で実施しています。あわせて、各国でのトレーニングの実施状況や受講率をリアルタイムで把握できる仕組みも整備しています。

またeラーニングのみならず、新入社員向けのオンサイトでのセキュリティ基礎教育や、毎月実施しているキャリア採用社員向けのオンボーディング研修のなかでも、当社グループの情報セキュリティに関するポリシー・ルールを説明するプログラムを設けています。さらに、情報セキュリティ部のメンバーによる事業部門への「セキュリティ出張講義」も定期的に実施しています。最新の脅威インテリジェンスに基づき、各部門が認識すべき脅威情報について情報セキュリティ部のメンバーが直接レクチャーしています。この出張講義では、インタラクティブなコミュニケーションを通じて従業員のアウェアネスの向上につなげています。

これらに加え、近年ランサムウェア攻撃の激化により業務に深刻な影響を与える事例も増加していることから、2026年に重大インシデントを想定した経営層向けのトレーニングの実施を予定しています。

そのほか、海外地域本社ではオリジナル施策を講じています。Americas地域本社では、標的型メールへの対応訓練を四半期ごとに継続的に実施しており、EMEA地域本社では、生成AIによるディープフェイクを想定した従業員向けの教育施策を実施しています。

情報セキュリティに関する主なeラーニングプログラム

情報セキュリティ基礎研修	全海外地域本社のすべての従業員を対象として年1回実施
脅威動向を踏まえた個別テーマの研修	外部環境や脅威動向を踏まえて随時実施 **実施例** BEC(Business Email Compromise:ビジネスメール詐欺)などを含めたeメールに関するトレーニング

情報セキュリティオペレーション

情報資産の管理

資生堂グループでは情報資産の重要度に応じて、適切な機密レベルを設定することをルールで定めており、「公開情報」「内部情報」「機密情報」「極秘情報」の4段階の機密レベルを設定しています。情報資産を適切に分類し、ラベル付けを行い、必要に応じて暗号化することで、重要な情報資産の漏洩防止に努めています。

また、情報資産へのアクセス権は、それぞれの職務に応じて業務上知る必要がある最小限の範囲で設定することとしています。情報資産の保管期間や廃棄に関しても、ルールを定めています。あわせて、情報資産を外部クラウド環境へアップロードする際のモニタリング体制も強化しています。

モニタリング活動

資生堂グループは、リスクに応じて情報システムや関連する業務プロセスについて評価を実施し、そこで検出された是正事項の改善に努めています。

また、情報システム基盤やアプリケーションに対する脆弱性診断を定期的に実施し、検出された脆弱性の是正対応を図っています。加えて、外部インテリジェンスを活用したモニタリングを常時行っているほか、情報セキュリティに関する施策・体制について外部の専門家による第三者評価も実施しており、そこで指摘された改善・強化事項を情報セキュリティ戦略の立案に反映しています。グローバルすべての地域本社をカバーしたセキュリティモニタリング体制も確立し、日々、モニタリングの精度向上に努めています。

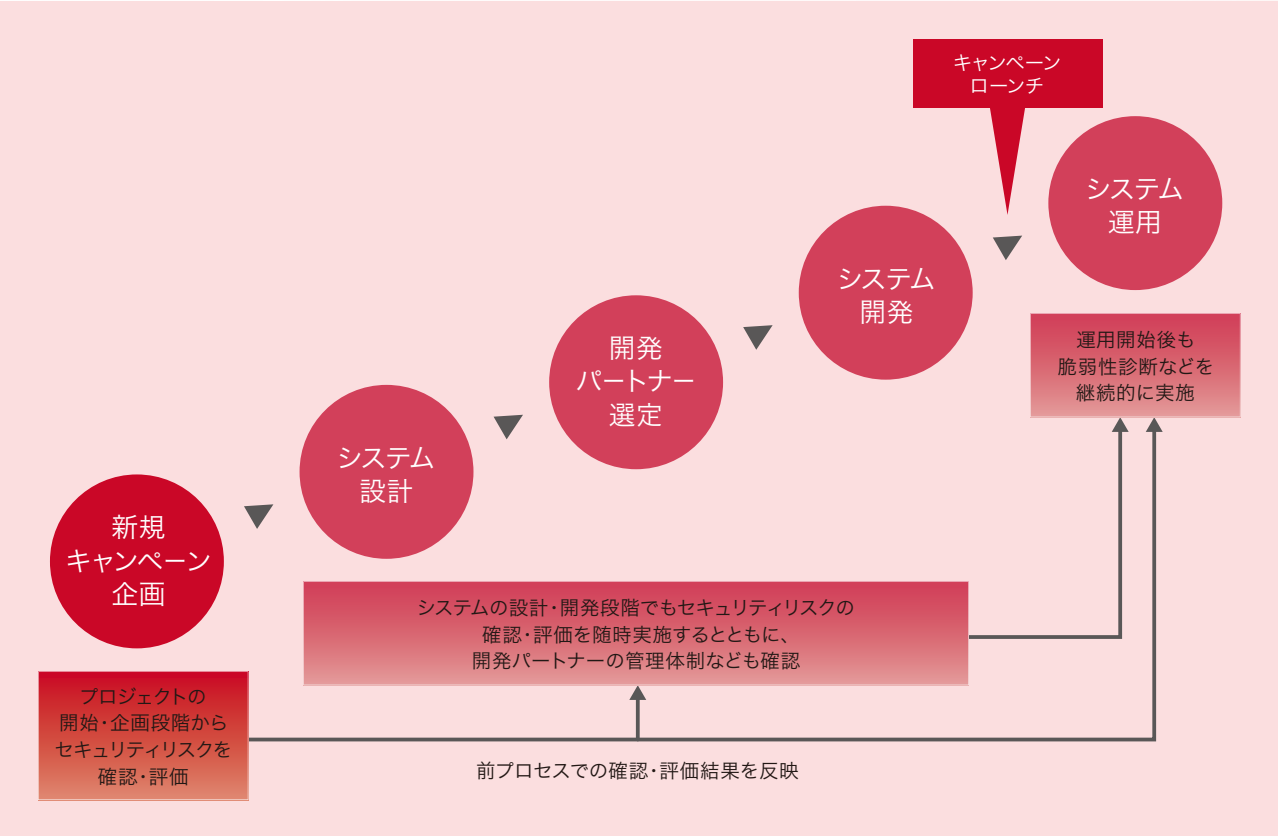
セキュリティ&プライバシーバイデザイン

資生堂では、新規のシステム構築や、当社が標準採用していないクラウドサービスの新規利用、SNSを活用したキャンペーンの実施にあたり、主管部門から情報セキュリティ部へ事前申請を行うプロセスを整備しています。申請後は、情報セキュリティ部の専門メンバーが情報セキュリティの観点からリスクを確認・評価し、リスクが一定水準以下に低減されていると判断した場合に限り、各プロジェクトを進行することとしています。

このように、プロジェクトの企画・開始段階から情報セキュリティ部が参画することで、リスク評価に十分な時間を確保し、手戻りのない安全な取り組みの実現を支援しています。

また、新規システムに限らず、サイバー攻撃による不正アクセスを防止するため、日本地域では既存の通販サイトなどに多要素認証を順次導入しています。

さらに2025年から、生成AIの業務利用に伴う新たなリスクへの対応として、AI活用に関するリスクアセスメントプロセスを整備しました。主要な生成AIツールの利用に際しては、モデル学習の設定をオフにすることを必須条件とするなど、情報漏洩リスクの低減を図っています。また、自律的に動作するAIエージェントの登場をはじめ、急速に発展する生成AIの技術動向に迅速に対応し、常にAIを安全に活用できるよう、2026年から生成AIの利活用に関するより包括的なポリシーおよびガイドラインの制定を進めています。



内部不正対策

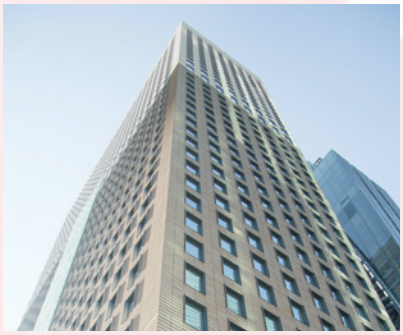
資生堂では、情報セキュリティの強化において、外部からのサイバー攻撃への対策と同様に、内部不正の防止も重要な課題と位置付けています。社内で取り扱う個人情報や機密情報の不正な持ち出しや漏洩を防ぐため、リスクマネジメント部門、人事部門、法務部門、情報システム部門などの関連部門が連携し、組織、人、技術の3つの観点から対策を講じています。

具体的には、就業規則や誓約書の見直しにより、ルール面での抑止力を強化するとともに、全従業員を対象に内部不正に特化した研修を定期的に実施し、意識の向上に取り組んでいます。また、USBなどの外部記憶媒体の利用を技術的に禁止することで、不正な情報持ち出しの防止を図っています。

さらに、メールやUSB、クラウドサービスなどを通じた情報の不正な持ち出しを自動で検知する仕組みを導入し、不正な情報持ち出しが発覚した場合は、関係部門で連携し、迅速かつ適切に対応できる体制を整えています。あわせて、検知だけでなく不正な持ち出し行為を予防するために、情報の持ち出しをブロックする仕組みを2025年に構築し、特定の従業員を対象に運用を開始しています。

情報セキュリティリスク管理

情報セキュリティに関するリスクを適切にマネジメントするには、日々発生する新たな脅威情報や専門的な知見のキャッチアップに加え、幅広い実務経験も求められます。一方で、そのような知見・経験を持つ高度なセキュリティ人材を確保し社内で維持し続けることは、容易ではありません。また、情報セキュリティ投資に対する経営判断においては、外部環境の脅威動向だけでなく、現状の対策実施状況を的確に評価し、リスクレベルを定量的に把握する必要があります。



資生堂グループでは、情報セキュリティに関する重点リスクモニタリング項目を定義し、各項目を個人の「経験」に依存せず一定の「基準」に基づいて毎月評価する独自の仕組みを導入しています。この評価には外部の脅威インテリジェンスも複数取り入れ、より的確かつ多角的に評価する仕組みとしており、リスクレベルの経時的変化と追加対策の必要性をタイムリーに判断できるようにしています。また、外部の有識者によるレビューも行い、評価のさらなる高度化・改善を図っています。

特権アカウント管理

資生堂では、お客さまの個人情報を保管するサーバーを管理するためのアカウント（特権アカウント）の適切な管理を徹底しています。特権アカウントは、システム全体に対して高い権限を持つため、万が一の不正利用が重大な情報漏洩や業務停止につながるリスクを伴います。

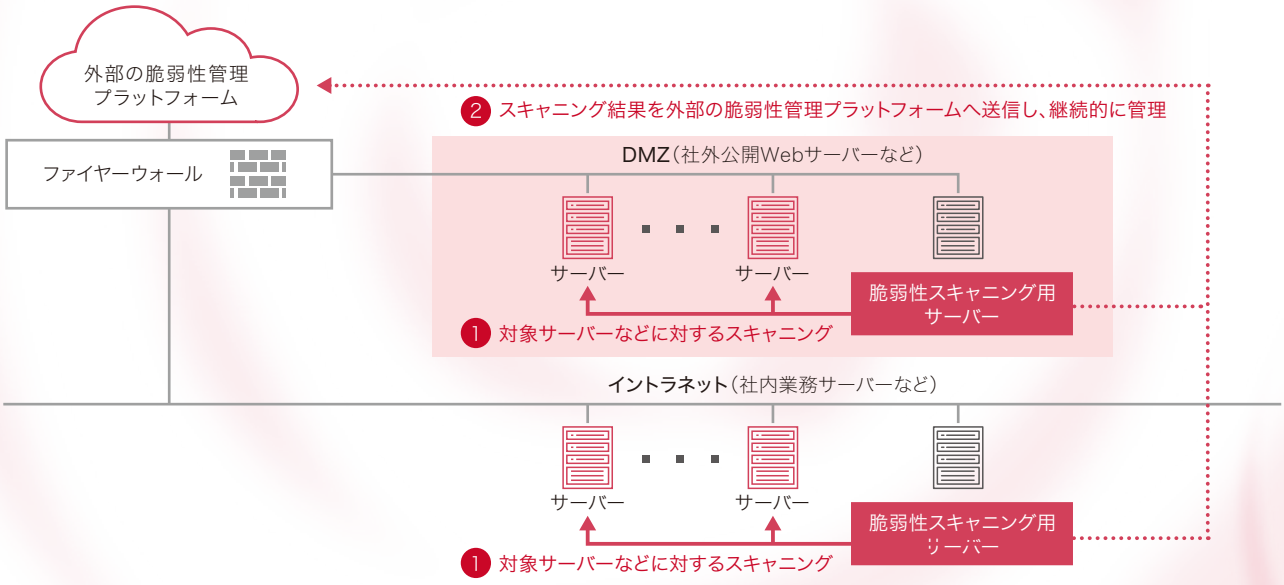
このようなリスクに対応するため、当社では個人情報を保管するサーバーに対して特権アカウントを管理するソリューションを導入し、特権アカウントの利用に関する申請、承認、実行、監査の各プロセスを一元的に管理しています。特に、外部の運用ベンダーがサーバーへアクセスする場合は、必要最小限の権限を一時的に付与し、アクセスの履歴を自動的に取得・保管することで、透明性と追跡性を確保しています。

さらに、特権アカウントの利用状況を定期的にレビューし、不要なアカウントの削除や権限の見直しを実施することで、継続的な情報セキュリティ強化と内部統制の維持を図るとともに、個人情報の保護と信頼性の確保に努めています。

IT基盤の脆弱性管理

IT基盤は、構築時はセキュアだったとしても、時間の経過とともに脆弱性などの問題が確認されることが多く、重大な脆弱性が公表された際には早期に対応する必要があります。しかし、公表される脆弱性の内容は多岐にわたり、その影響もさまざまであることから、すべてに対応することは非現実的です。

そのため資生堂グループでは、脆弱性を優先度付けできるツールを導入し、最も重大な脆弱性から効率的に対応する運用プロセス・ルールを構築しています。対応完了までの時間に関しても、脆弱性の重大度に応じて、「2週間以内」「1カ月以内」など明確な基準を設けて、システム管理者に是正対応を求めています。



Webサイトの脆弱性診断

資生堂は、各ブランド・事業部門において独自のECサイトや情報発信のためのWebサイトを数多く運用しています。

新規サイトをローンチする前には、脆弱性に関するチェックの実施を必須としています。さらに、運用開始後も機能追加や改修、クラウド環境の変化などがあることを鑑みて、脆弱性診断を定期的に実施し、重大な問題が発見された際は、運営部門で迅速に是正対応を行っています。

外部公開資産の管理

インターネットに公開されているサーバーなどの外部公開資産をもれなく把握し、必要なセキュリティ対策を行うことは、悪意のある者から攻撃を受けるリスクを最小化する観点でも非常に重要であると認識しています。

資生堂グループでは、インターネット経由でセキュリティリスクを診断し、セキュリティ態勢をスコアリングできるサービスを導入しています。また、海外地域本社ごと、およびグローバル全体でのセキュリティ態勢の定量的な評価を継続的に行っています。この評価をもとに、情報セキュリティ部が各海外地域本社のセキュリティ担当者と適宜コミュニケーションをとり、着実に是正対応を推進しています。また、同業種の他企業ともスコアを比較評価し、他社との比較において一定水準以上のレベルを維持していることを定期的に確認しています。さらに、新たな外部公開資産を発見するためのツールや運用プロセスも新たに整備し、意図せず外部公開の設定となっている資産などを発見した際は迅速に是正対応することとしています。

資生堂グループの情報セキュリティスコア（2026年6月時点）

「グローバルセキュリティオペレーションセンター」による脅威監視

資生堂では各海外地域本社に情報セキュリティ担当メンバーを配置し、その強化を進めてきましたが、さらなる対策の高度化や標準化を目指して、24時間体制でシステム上の情報セキュリティイベントなどをモニタリングする「資生堂グローバルセキュリティオペレーションセンター」を2023年12月から設置しています。この取り組みでは、外部の情報セキュリティベンダーが提供するマネージドサービスも活用し、全海外地域本社共通ルールのもとにログを収集・分析する基盤を構築しました。

2025年からは当該サービスの拡張を行い、脅威発生時の初動分析や封じ込めに24時間対応できる外部専門チームと連携することで、アラートのモニタリングや検知だけでなく、インシデントの発生についてもグローバルで時間を問わず対応可能な体制を整備しています。

資生堂情報セキュリティ報告書2026 制作チーム
2026年9月

株式会社資生堂 グローバルデジタル本部
グローバル情報セキュリティ部

株式会社資生堂
Shiseido Company, Limited
〒105-8310 東京都港区東新橋 1-6-2
https://corp.shiseido.com/jp/