SHISEIDO

Information Security Report 2024

情報セキュリティ報告書2024

COO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）」のもと、情報セキュリティ対策の強化に取り組んでいます

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。2020年からの新型コロナウイルスによるパンデミックを経た今、資生堂のビジネスや資生堂グループの従業員の働き方は大きな転換期を迎えております。急速に進むデジタル化においては、eコマースの積極的な展開のみに留まらず、YouTube、TikTok、X（旧Twitter）、Instagramなどのソーシャルネットワークを含むさまざまなデジタルプラットフォームを介して、資生堂と生活者の皆さまとの新たな接点が日々生み出されています。さらに、お客さまの情報をOne IDでつなぐ会員サービス「Beauty Key」のローンチ、資生堂が長年培ってきた皮膚科学研究とAI技術を融合した独自の「Beauty DNA Program」など、新たな美容体験の創出も着実に推進しています。また、資生堂社内の働き方に関しても、コロナ前はオフィスへの出社を前提としていましたが、在宅勤務とオフィス出社を組み合わせた多様な働き方へと移行しています。このような急速なデジタル化や新たな生活様式への移行により、必然的に情報セキュリティ対策の重要性もますます高まってきていると認識しています。経済産業省が策定している「サイバーセキュリティ経営ガイドラインVer3.0」なども参照しながら、国内外の経営メンバーと議論し、必要な情報セキュリティ施策についてはタイムリーに実現すべく、鋭意取り組んでおります。

資生堂グループでは、2030年に向けた目標として「PERSONAL BEAUTY WELLNESS COMPANYとして、スキンビューティー領域における世界No.1となる」ことを掲げております。この実現に向け、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・デジタルのグローバル共通基盤の導入、それら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、お取引さまに今まで以上に信頼いただ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ご紹介しておりますので、ぜひご一読を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 社長 COO
藤原 憲太郎

情報セキュリティ担当役員メッセージ

資生堂グループの商品・サービスを常に安心してご利用いただけるよう役員・従業員が一丸となって情報セキュリティ対策を推進しています

本報告書冒頭に記載した資生堂の社長COO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、当社グループは情報セキュリティの強化を重要な経営マターとして日々取り組んでいます。昨今、テクノロジーが著しく進化し、私たちの事業活動に大きなベネフィットをもたらしている一方で、外部からのサイバー攻撃を含めた各種攻撃なども高度化・巧妙化しています。

そのような環境下においても、沢山の生活者の皆さま、お得意先さま、お取引さまよりお預かりしている個人情報や、当社グループの事業上重要な機密データをしっかりと守っていけるよう、人、プロセス、データの3つの観点で多層的な防御を取り入れ、その防御活動を24時間365日しっかりと監視する体制を整えてきました。

人、プロセスにおいては、詳細な社内向け情報セキュリティ報告書を四半期ごとに本社役員および海外地域本社CEOを対象に発行し、活動への意識を高めるとともに、当社グループ内でのベストプラクティスを共有しています。あわせて、全世界の従業員に定期的な情報セキュリティ研修を実施することで、業務の遂行において常に情報セキュリティを意識するよう教育を徹底しています。

また、データにおいては、データを扱うシステムの脆弱性を常に監視しタイムリーに脆弱性を取り除く活動や、外部サービスによる当社の対応状況のベンチマークを実施し、業界内でもトップレベルのベンチマークスコアの獲得を目指しています。

情報セキュリティ対策の強化にゴールはなく、継続的に取り組んで改善していくことが必須という強い認識のもと、毎年本報告書を通じてステークホルダーの皆さまに資生堂グループとしての最新の取り組みをご紹介していきます。当社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ることを願っています。

株式会社資生堂
エグゼクティブオフィサー
チーフインフォメーションテクノロジーオフィサー
高野 篤典

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
原則として2023年度（2023年1月～12月）

■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

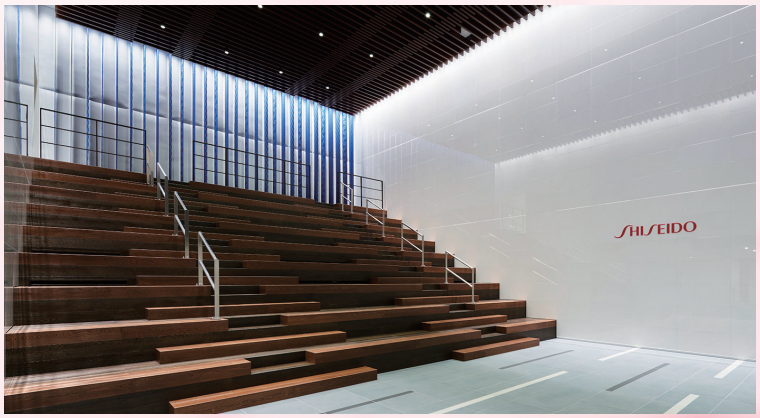
情報セキュリティ活動のフレームワーク

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。



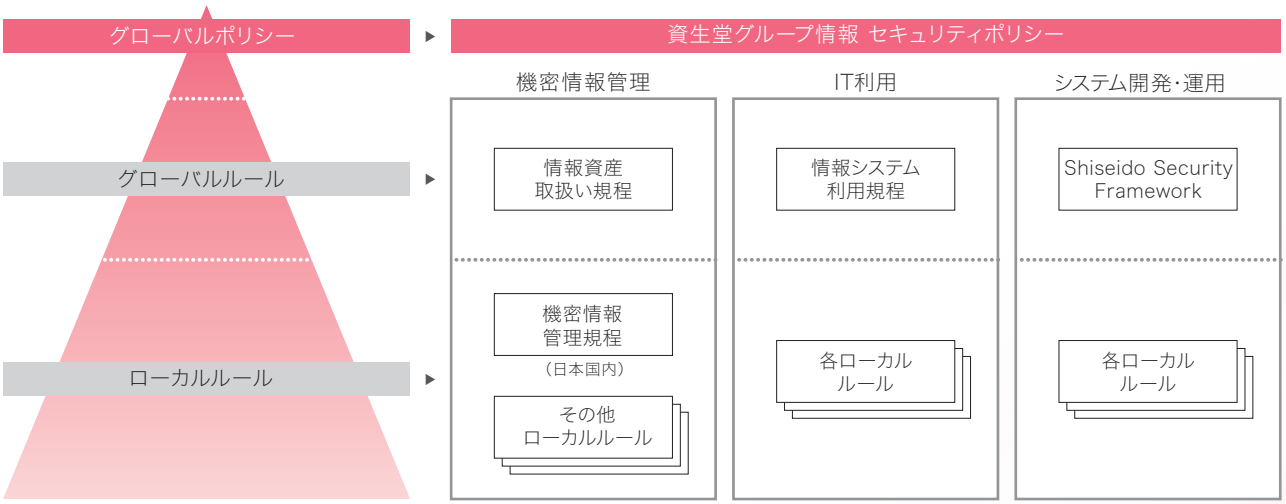
ポリシー・ルール体系

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、代表執行役社長最高執行責任者（COO：Chief Operating 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。

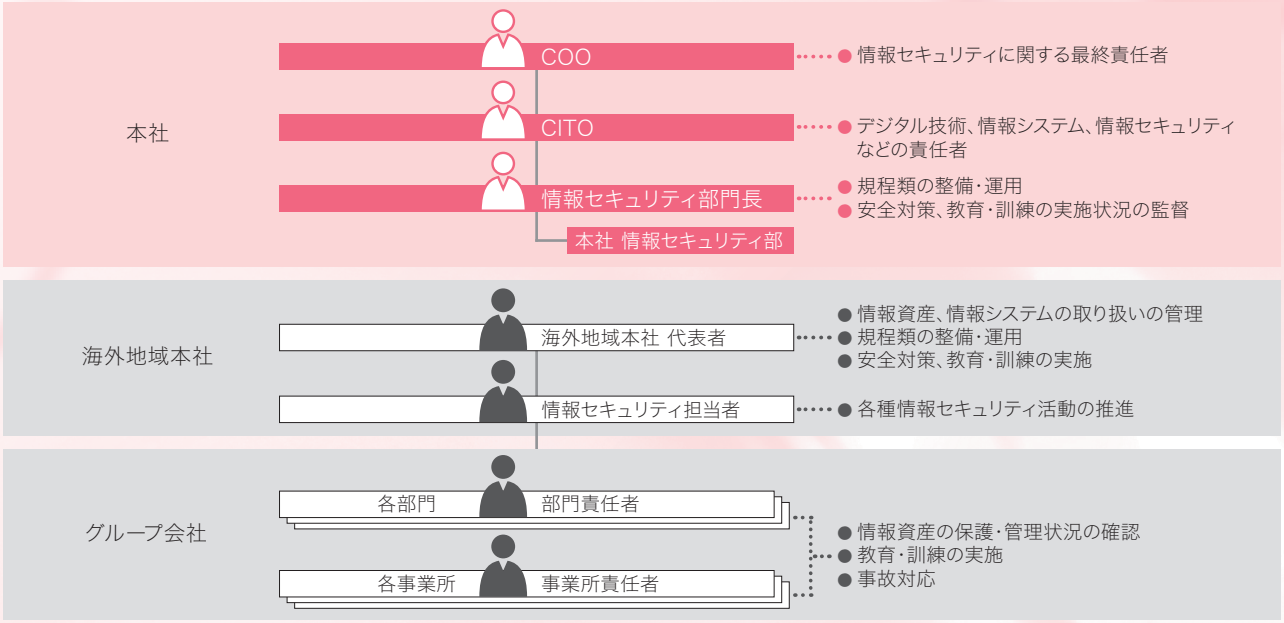
海外地域本社におけるマネジメント

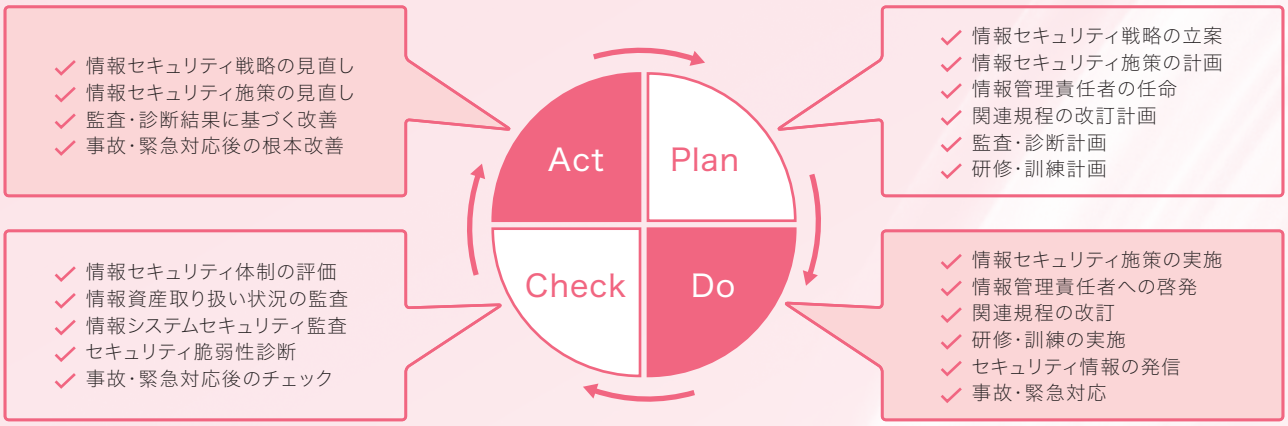
各海外地域本社においては、その代表者が管轄地域内の情報資産と情報システムの取り扱いを管理しています。機密情報管理、情報システム管理、情報セキュリティ対策に関する規程類の整備および運用の徹底、安全対策の実施、教育・訓練などの情報セキュリティ全般に責任を負っています。

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。



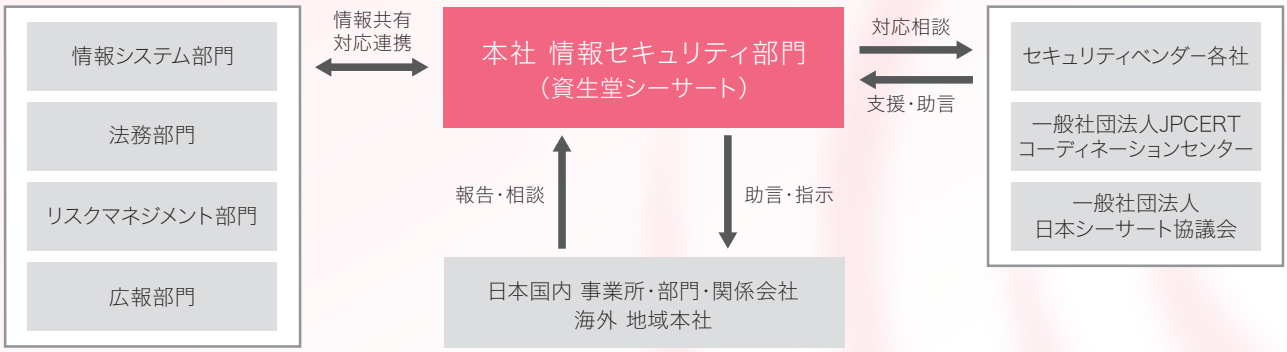


インシデント発生時の体制

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、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。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中でも、当社グループの情報セキュリティに関するルールやポリシー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。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。

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継続的に実施、EMEA地域本社では、ゲーミフィケーションなどを活用した従業員のモチベーションを高める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

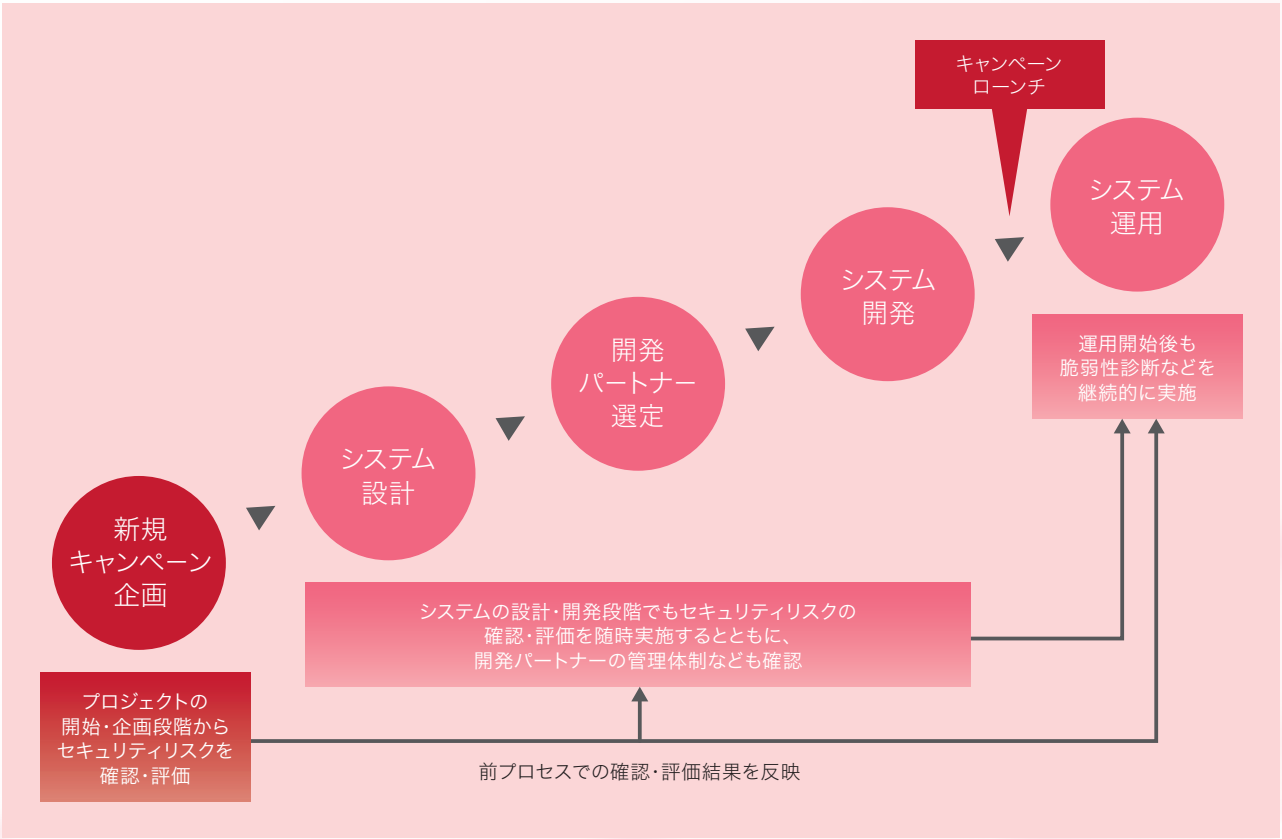
資生堂グループは、リスクに応じて情報システムや関連する業務プロセスについて評価を実施し、そこで検出された是正事項の改善に努めています。

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などを使用した新規キャンペーンの実施にあたり、それらの主管部門から情報セキュリティ部へ事前申請するプロセスを整備しています。申請後に、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でリスクを確認・評価し、一定の水準以下にリスク軽減が図ら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、プロジェクトの開始・企画時から情報セキュリティ部のメンバーが参画し、リスクの確認・評価に時間をかけることで、結果として手戻りなく、安全に新しい取り組みを開始できるようにしています。

また、情報セキュリティ部門内での業務効率化の観点も踏まえ、2022年9月よりワークフローシステムを導入。情報の検索性が向上し、各部門からの問い合わせや相談を一元管理しています。



情報セキュリティリスク管理

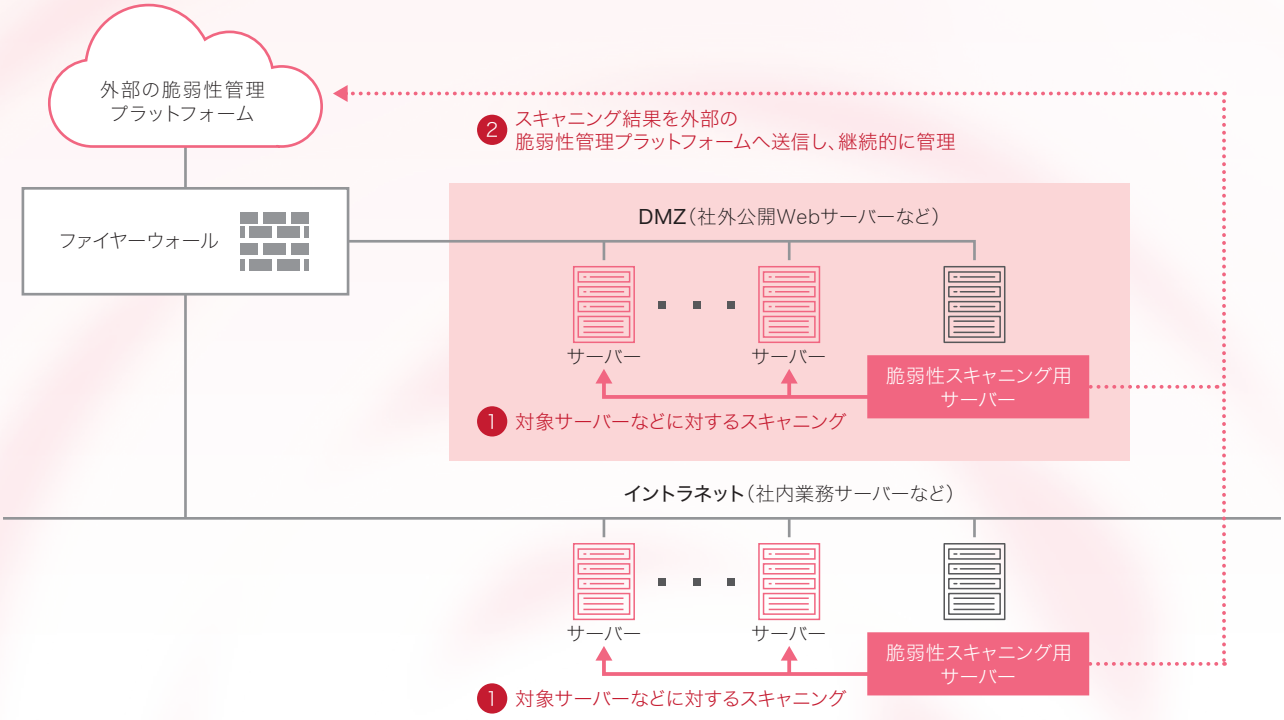
情報セキュリティに関するリスクを適切にマネジメントするには、日々発生する新たな脅威情報や専門的な知見のキャッチアップに加え、幅広い実務経験も求められます。一方で、そのような知見・経験を持つ高度なセキュリティ人材を確保し社内で維持し続けることは、容易ではありません。また、情報セキュリティ投資に対する経営判断においては、外部環境の脅威動向だけでなく、現状の対策実施状況を的確に評価し、リスクレベルを定量的に把握する必要があります。

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。

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。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。

「グローバルセキュリティオペレーションセンター」の構築

資生堂では各海外地域本社にセキュリティ担当メンバーを配置し、情報セキュリティを強化してきましたが、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」の稼働を2023年12月より開始しました。

この取り組みでは、外部の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ながら、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。また、将来的にはセキュリティオペレーションの自動化も視野に、実施するアクションを事前定義したプレイブックの整備も進めています。

資生堂情報セキュリティ報告書2024 制作チーム
2024年7月

株式会社資生堂 情報セキュリティ部
資生堂クリエイティブ株式会社

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/