情報セキュリティ

花王では国・地域・事業・会社で30の情報セキュリティ委員会を設置しています。この情報セキュリティ委員会がサイバーセキュリティ対策・機密情報・個人情報及びハードウエア・ソフトウエア・各種データファイル等の情報資産の保護を目的とした活動を展開しています。

社会的課題

独立行政法人情報処理推進機構が発行している「情報セキュリティ白書2023」では、以下のように述べられています。

『企業・団体におけるランサムウェア被害が増え続けた。攻撃の手口では、窃取したデータを暴露する「二重の脅迫」に加え、被害組織へのDDoS攻撃や、被害の事実を被害組織の顧客や利害関係者に連絡する等の脅迫手法も確認されている。』

『2022年2月の自動車部品会社へのランサムウェア攻撃では、部品供給先である自動車工場の稼働が1日停止した。同年10月の大阪市の医療センターへのランサムウェア攻撃では、VPNでつながる給食提供業者から侵入され、サーバーを介して医療センターの電子カルテシステムに障害が及んだ。』

日本の例を挙げましたが海外でも同様の状況で、企業や組織に対するサイバー攻撃により機密情報や個人情報の漏えい、ランサムウェアによる生産活動や事業活動の停止といった被害が多数発生しています。そのため、サイバー攻撃を防ぐためのセキュリティ対策を社会的課題として認識しています。

また、近年では、EUのGDPR(一般データ保護規則)や各国の法律により個人情報の保護が強化されています。花王は、こうした各国の個人情報保護の強化に対応することも社会的課題として認識しています。

方針

花王は、サイバー攻撃を受けないためのセキュリティ対策の実施、サイバー攻撃を受けても被害を最小限に押さえ込めるしくみや体制の構築とその維持をめざしています。

花王では情報セキュリティ委員会(Information Security Committee: ISC)が中心となり、リスク危機管理委員会と連携しながらインシデント対応体制を構築し、有事に備えています。技術的な対策は情報システム部門が主導でリスクアセスメントを実施し、セキュリティ対策の戦略ロードマップを作成、これに沿って対策を実施しています。

国内では、
・情報セキュリティポリシー
・機密情報取扱いガイドライン
・個人情報取扱いガイドライン
・ITセキュリティガイドライン(管理者編)
・ITセキュリティガイドライン(ユーザー編)
・Web・アプリセキュリティガイドライン

海外では、
・Information security policy
・Global Trade Secret Regulation
・IT security guidelines(準備中)

等の規程を制定して、サイバーセキュリティ対策や機密情報(トレードシークレット:TS)・個人情報の管理を徹底しています。これらは、法令や各省庁・委員会のガイドラインに準拠するだけでなく、花王としての管理体制・管理方法の方針を明確にしています。

個人情報の定義や個人情報の取り扱いに関する事業者の義務は、各国の法律ごとに内容が異なります。それらの法律の制定や改定の内容を把握し、花王グループが取るべき必要な対応を実施し、各国の法律を遵守しています。

個人情報の取り扱いの方針や問い合わせ窓口については、海外を含めた各社のウェブサイトで「個人情報保護方針」を公表しています。

Web
花王グループ会社の個人情報保護指針
日本語版
https://www.kao.com/jp/privacy/
英語版
https://www.kao.com/global/en/privacy/
EMEA向け(GDPR準拠)
https://www.kao.com/emea/en/privacy/

花王グループ会社の保有する個人情報に関するお問い合わせ・苦情受付窓口
日本語版
https://www.kao.com/jp/privacy/privacy-contact/
EU向け(GDPR準拠)
https://privacyportal-eu.onetrust.com/webform/4d856428-3bc6-45cd-82ac-13948107e0b3/5d905f69-ba05-479c-849a-4178fd4cb6e7

戦略

リスクと機会

リスク

サイバー攻撃による生産活動・販売活動・マーケティン

情報セキュリティ GRI 2-28

グ活動・研究開発活動の長期間の停止や、TS・個人情報といった情報の漏えいによる企業の信頼の失墜は大きなリスクです。

機会

サイバーセキュリティ対策やTS・個人情報といった情報資産管理を強固にすることで、新たなデータ活用・新たなビジネスの実現やICTを活用した多様な働き方を可能とします。

戦略

セキュリティ対策の緊急度と予算を考慮した上で、セキュリティ戦略ロードマップに沿ってサイバーセキュリティ対策を実施しています。2023年には、メールの添付ファイルやリンクの無害化、なりすましメールの対策、アカウントの乗っ取りの防止対策、PCやサーバーにおける不審な挙動を検知して迅速な対応を実施するセキュリティソフト(Endpoint Detection and Response)を導入しました。

また、24時間365日、ネットワークやサーバー、PCを監視し、サイバー攻撃やウイルス感染等を検知し、即時対応を行うSecurity Operation Center(SOC)をグローバルに展開しています。2023年8月にはPPAP禁止のため、パスワード付きzipファイルが添付されたメールの送受信を拒否しました。こうした取り組みと併せて、社員へのセキュリティ教育も実施しています。

社会的インパクト

花王は情報共有ネットワークを通じて、自社が経験したサイバー攻撃を共有することで、業界や日本企業全体のセキュリティ対策の向上に貢献しています。

そのため、

- 独立行政法人情報処理推進機構(IPA)の「サイバー情報共有イニシアティブ(J-CSIP)」
- 警察庁の「サイバーインテリジェンス情報共有ネットワーク」
- JPCERTコーディネーションセンターの「早期警戒情報」

に参加しています。また、業界団体である日本化学工業協会の情報セキュリティ対応部会に参加し、各企業との情報交換にも取り組んでいます。

また、サプライチェーン全体に対してサイバーセキュリティ対策を実施することで、業界全体・日本企業全体のサイバーセキュリティの向上の一端を担っています。

貢献するSDGs

事業インパクト

サイバーセキュリティ対策によりサイバー攻撃の被害による事業中断やTS・個人情報の漏えい・流出を防ぐことができれば、企業としての信頼を損なうことを防ぐことができると同時に、被害が発生した場合の損害賠償や原因究明・対策実施等にかかる対応コストを低減できます。またサイバー攻撃によるインシデントへの対応やTS・個人情報漏えい時の対応が確立されていれば、被害を最小限に抑えることができます。

花王グループがサイバー攻撃に対する強固なセキュリティ対策を実施できれば、セキュリティ対策に対する信頼性も高くなり、新たなデータ活用・新たなビジネスの実現やICTを活用した多様な働き方の実現が容易になります。

ガバナンス

体制

情報セキュリティの管理体制

情報セキュリティに関する最上位規程の「情報セキュリティポリシー」では、「情報セキュリティの対策立案及び維持管理を行うために、代表取締役社長執行役員の指名による情報セキュリティ最高責任者(CISO)を任命し、これらの指揮・監督を行わせる」となっています。CISOは執行役員で、ISCの委員長を務め、ISCは経営目標達成のために、機密情報・個人情報等の情報資産(ハードウエア、ソフトウエア、各種データファイル等を含む)の保護を推進する委員会で、花王グループ全体

情報セキュリティ

のサイバー攻撃対策や各国の個人情報保護法への対応を行っています。

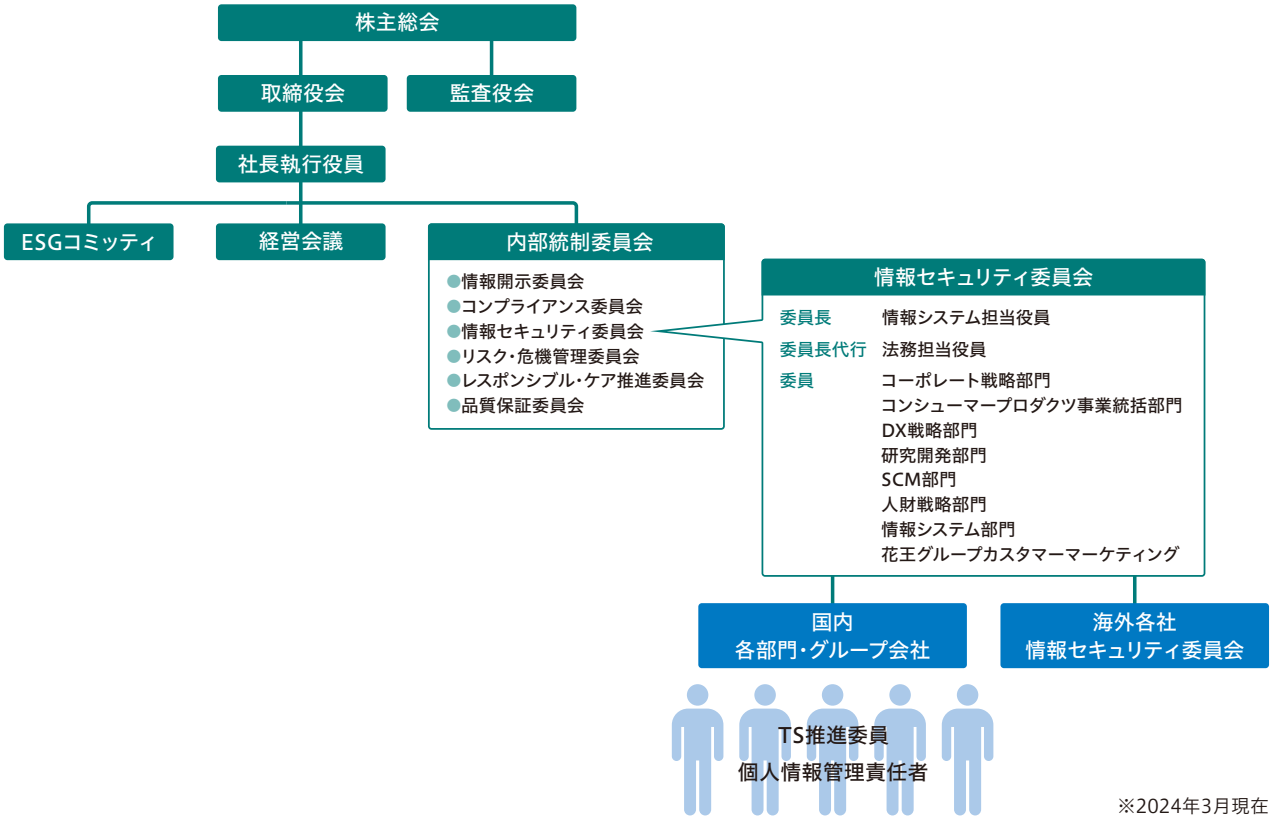
日本では、ISC委員長と委員長代行に執行役員を配置し、人財戦略、情報システム、マーケティング、研究開発、知的財産、生産技術、法務等の多様な部門から委員と事務局を選出し、多様な観点で方針の決定やルールの整備、管理体制の整備、啓発活動の実施を推進しています。

ISCは内部統制委員会を通じて、四半期ごとに取締役会へ報告を行います。報告は、本年度の活動目標とその進捗及び実績評価で、第4四半期には翌年の活動目標も併せて報告されます。ただし、緊急対応の必要な案件については、リスク・危機管理委員会と連携して、直ちに経営にレポートされます。

海外では、各社の経営会議メンバーがISCを構成し、日本のISCの傘下に海外の各ISCを配置するかたちになっています。活動は日本と同様に四半期単位のPDCAサイクルによる活動で、3月には日本のISCへレポートの提出を義務づけています。

P25 Our ESG Vision and Strategy > ガバナンス

情報セキュリティの管理体制



※2024年3月現在

日本のISCへのレポートフォーマット

No.	項目	内容
1	自己啓発活動	全員を対象に行うこと。啓発内容や対象者を記述する。
2	自己点検	自己点検内容や回答者を記述する。回答者は以下のどのパターンか？ ・社員を部門ごとにサンプリングして回答者を選定 ・マネジャーが部門の状況を把握して回答 ・その他
3	改善目標設定・実施	自己点検の結果、成績の悪い項目を改善目標に設定し、改善計画を記述する。
4	事故発生件数	機密情報の盗難・紛失・誤送信による漏えいや情報機器の盗難・紛失の件数を種類ごとに記述する。 詳細は事故報告書に記述する。
5	個人情報に関する情報	個人情報の保有件数、個人情報に対するクレーム件数、個人情報の削除要求件数を記述する。
6	その他	TS・個人情報、サイバー攻撃に関する報告があれば記述する。

情報セキュリティ

情報セキュリティ委員会(ISC)設置状況

部門	番号	会社・リージョン
本部	1	花王(株)
コンシューマープロダクツ	2	花王(台湾)
	3	花王プロフェッショナル・サロン・サービシーズ(台湾)
	4	花王(香港)
	5	花王プロフェッショナル・サロン・サービシーズ(香港)
	6	花王タイ・花王コンシューマープロダクツ
	7	花王(インドネシア)
	8	花王(シンガポール)
	9	花王(マレーシア)
	10	花王(ベトナム)
	11	花王コンシューマープロダクツ(EMEA)
	12	花王コンシューマープロダクツ(アメリカ)
ケミカル	13	花王ペナングループ
	14	ピリピナス花王
	15	花王インドネシア化学
	16	花王コーポレーション(スペイン)
	17	ドイツ花王化学
	18	キミ花王
	19	花王チミグラフ
	20	花王ケミカルズ アメリカズ
	21	花王コリンズ
中国	22	花王中国グループ
カネボウ	23	カネボウコスメティックスヨーロッパ
	24	カネボウコスメティックスドイツ
	25	カネボウコスメティックスイタリア
	26	カネボウコスメティックス台湾
	27	カネボウコスメティックスタイ
	28	カネボウコスメティックスマレーシア
	29	カネボウコスメティックス韓国
	30	カネボウコスメティックスロシア

花王のインシデント対応のメンバーと役割

名称	メンバー	役割・タスク等
経営幹部	・代表取締役　・監査役	・重大なインシデントの把握 ・対応策、公表、再発防止策の判断・承認
リスク・危機管理委員会	・委員長　・事務局	・サーバー攻撃/個人情報保護対応チームからエスカレーション
緊急対策会議CSIRT Computer Security Incident Response Team	・ISC委員長　・ISC委員　・ISC事務局 ・危機管理　・RC推進部　・企業PR戦略部 ・社員サービス部　・MKプラットフォーム部 ・生活者CC　・主管部門	・インシデントの把握と対応 ・即時対応:ネットワーク遮断、サーバ停止、アカウント停止等の判断 ・経営幹部への報告: 即時対応策、再発防止策の検討・報告・実施、ステークホルダー、外部関係機関への開示の判断
SOC Security Operation Center	・情報システム部門:ネットワーク、サーバー、セキュリティサービス ・企業PR戦略部:マスコミ対応、ニュースリリース作成 ・危機管理・RC推進部:SNS監視 ・カスタマーサクセス部:会員・キャンペーンサイト管理 ・生活者CC:外部からの通報管理 ・ISC事務局:警察庁、IPA、JPCERT/CCからの通報管理	・各種の監視を行い、異常値を検出。異常値が検出された場合、CSIRTへ報告、原因調査、技術的対応実施 ・外部からの通報を受け、事実確認を行いCSIRTへ報告
ステークホルダー/ 外部関係機関	・取引先　・社員　・生活者　・マスコミ ・監督機関　・警察　・IPA ・JPCERT/CC　・情報共有ネットワーク	・ステークホルダーへの情報開示、監督機関への報告 ・警察、IPA、JPCERT/CCへの援助要請 ・情報共有ネットワークへの情報提供

※ 危機管理・RC推進部:危機管理・レスポンシブルケア推進部、生活者CC:生活者コミュニケーションセンター、
MKプラットフォーム部:マーケティングプラットフォーム部

花王のインシデント対応フロー

	検知	把握	対応
経営幹部・監査役 リスク・危機管理委員会		第一報当日	・報告 ・対応策・公表・再発防止策等承認 翌日以降
ISC (CSIRT)	即時	・事実把握 ・緊急度判断 ・緊急対策会議 ・幹部報告準備 ・外部に支援要請 当日	・対応策・注意喚起・公表・再発防止策・問い合わせ対応等検討・準備
SOC	・モニタリング ・社員から通報 ・外部から通報 ・SNS書込み	・継続分析 ・原因調査	・対応策・注意喚起・公表・再発防止策・問い合わせ対応実施
ステークホルダー 外部関係機関セキュリティ会社		・警察、IPA、JPCERT/CCに支援要請 ・契約先と連携	・注意喚起・公表、被害届、情報共有

情報セキュリティ

インシデント対応体制

サイバー攻撃や情報漏えい等のインシデントが発生した場合に備えて、インシデント対応の体制を整備し、被害を最小限に抑える備えをしています。実際にインシデントが発生した時に備え、机上での訓練を年に複数回実施しています。

教育と浸透

社内教育は、TSや個人情報の基礎知識の周知徹底を目的に各部門での実施を基本としています。そのため日本国内では毎年11月に、各部門のTS推進委員や個人情報管理責任者を集めて全体会議を開催しています。会議内容は、以下の4点となります。

①TSや個人情報、情報セキュリティについての講演や啓発
②花王のTSや個人情報に関する事故件数、傾向の分析とフィードバック
③改善目標の設定
④TS・個人情報保護推進、情報セキュリティについてのトピックス

2023年は、会議室とウェブ会議で266名のTS推進委員・個人情報管理責任者が参加しました(会議録画の視聴者は134名)。全社員向けには社内ポータルサイトによる啓発資料の掲載やタイムリーな注意喚起も行っています。さらに、社内教育の浸透度を測るために、自己点検によるチェックも行っています。自己点検によるチェックでは課題を抽出し、改善目標を設定、改善活動を実施しています。

海外では各国のISCが啓発や自己点検の実施計画を作成・実施し、3月に日本にレポートを提出しています。

ステークホルダーとの協働

サイバーセキュリティ

サプライチェーン全体のセキュリティ対策のため、業務委託先やサプライヤーと協働して、以下のセキュリティ評価を実施しています。

・2020年:3rd Party Logistics(アジア:17拠点、Americas/EMEA:20拠点)に対してセキュリティ評価実施
・2022年:包材サプライヤー107社、原材料サプライヤー86社にセキュリティ評価実施(リスクの高いサプライヤーに対しては、購買部門が対策を協議)
・2023年:製造委託先9社にセキュリティ・チェック評価実施

国内の個人情報委託先の書面監査

業務委託先200社に対して、書面監査を実施し、個人情報の管理体制・ルール・安全管理措置を確認し、委託先の監督を行いました。

Webアプリセキュリティガイドライン

システム開発の委託先に花王のセキュリティ要件を示し、その要件を満たすように設計・開発することを求めるために「Webアプリセキュリティガイドライン」を制定・施行しました。

この中には、システム担当者、開発担当者、運用担当者のセキュリティに関わる社内手続きや考慮点も示されています。

リスク管理

日本のPDCAサイクルによるTS・個人情報保護推進活動は以下のとおりです。

Plan:計画策定・見直し

・推進体制の見直し、情報アクセス権の更新を実施
・機密情報リストの見直しを実施
・啓発と自己点検についての実施計画の共有
・海外のISCからのレポート(前年実績と本年計画)

Do:啓発活動

・機密情報リストの機密レベル再点検を実施
・個人情報管理責任者の誓約書提出
・社員への啓発活動を実施

Check:自己点検・委託先監査

・TS・個人情報自己点検を実施
・個人情報の外部委託先監査を実施

情報セキュリティ

Act：改善活動

・TS・個人情報事故の総括を実施
・TS・個人情報自己点検のフィードバックを実施
・改善目標の設定

リスクの把握

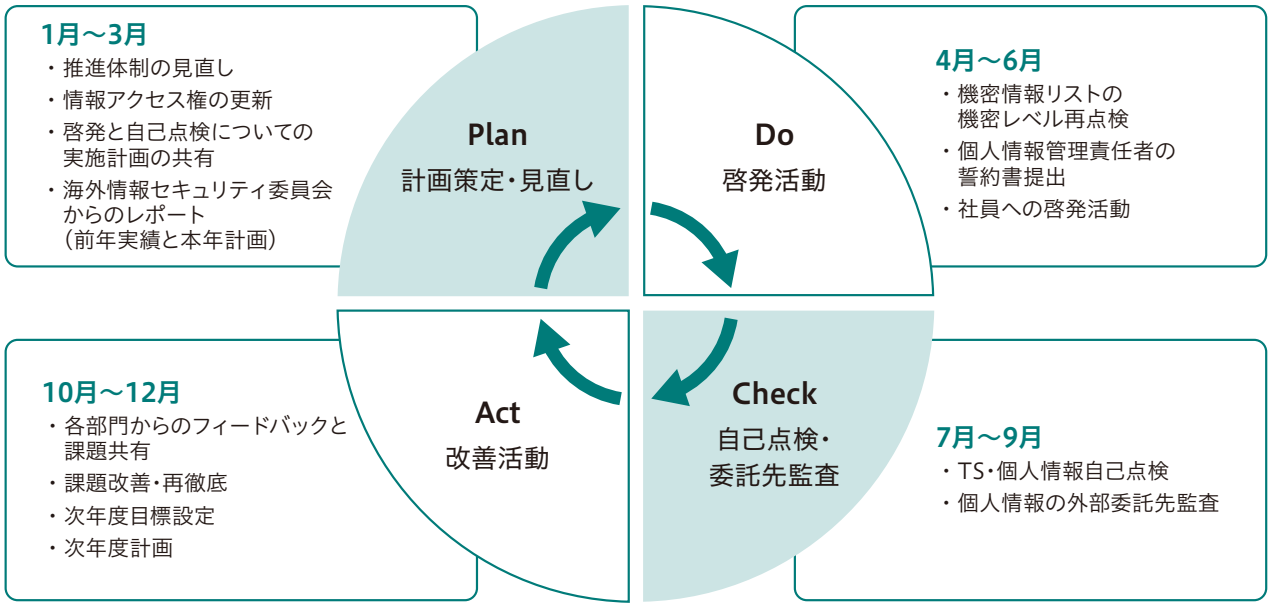
・機密情報、個人情報、セキュリティが規程どおり管理・運用されているかという点については、自己点検でのセルフチェックにより把握しています。
・個人情報を扱う業務のリスク把握については、2023年7月に稼働した新個人情報管理システムでリスクスコアにより把握する予定です。

リスクの軽減

・セルフチェックにより把握されたリスクについては、全体会議でのフィードバックや改善目標に設定することでリスクの軽減を図っています。

P40 Our ESG Vision and Strategy > リスク管理

情報セキュリティ活動のPDCA



指標と目標

中長期目標と2023年実績

中長期目標

・サイバーセキュリティ対策を含めたTS・個人情報及びハードウエア・ソフトウエア・各種データファイル等の情報資産の保護
・情報漏えい事故等、緊急事態発生時の事実確認、緊急対応の実施、再発防止策策定と実施

2023年実績

花王において、TS・個人情報保護を含めた情報セキュリティに関して重大な事故の発生はありませんでした。また、「問い合わせ窓口」に寄せられた個人情報に関する苦情はありませんでした。海外ではEUで個人情報の削除要求が25件あり、速やかに対応しました。

Plan：計画策定・見直し

・TS推進委員316名、個人情報管理責任者296名の見直し
・日本の125部門・部署・関係会社で機密情報リストの見直し
・海外28のISCからのレポート受領（カネボウコスメティックスロシアが活動休止中）

Do：啓発活動

・個人情報に関する誓約書提出2,391名

情報セキュリティ

・日本の139部門・部署・関係会社で啓発活動実施

Check：自己点検・委託先監査

・日本の146部門・部署・関係会社でTS自己点検実施
・日本の116部門・部署・関係会社で個人情報自己点検実施
・200社に対して個人情報の委託先監査を実施

Act：改善活動

花王において、TS・個人情報保護を含めた情報セキュリティに関して重大な事故の発生はありませんでした。
・2023年11月22日に全体会議を開き、会議室とウェブ会議で266名のTS推進委員・個人情報管理責任者が参加しました（会議録画の視聴者は134名）。
・2023年のTS・個人情報の事故件数は10月末時点で104件です。そのうち67件が紛失で、ほとんどが会社貸与携帯電話の紛失事故でした。会社貸与携帯電話や会社貸与PCは暗号化されていて、本体を紛失しても情報漏えい事故にはなりません。

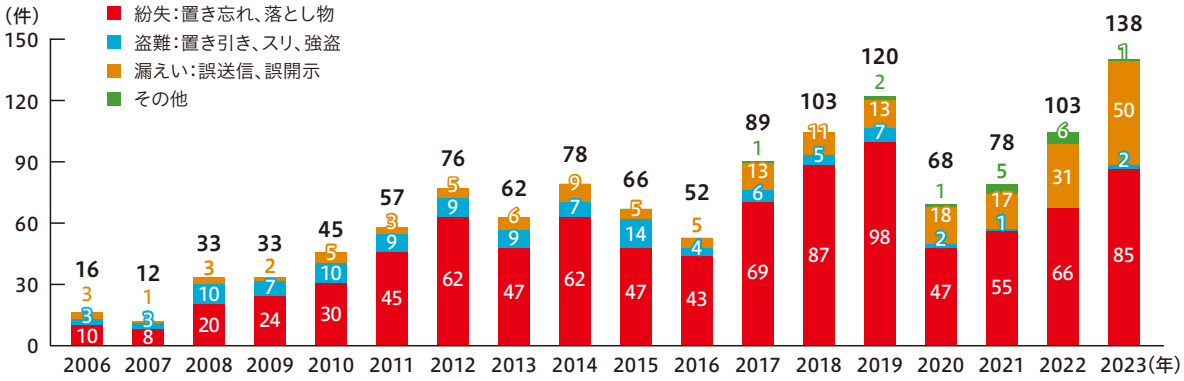
2023年実績に対する考察

TS・個人情報の保護を十分に理解している人でも、数年経つと知識が曖昧になり、事故を起こすリスクが高まるため、TS・個人情報の保護推進活動は、毎年、継続的に行う必要があります。新入社員やキャリア採用の方を含めた全社員が花王のTS・個人情報の保護ルールを理解し、実践することが大切です。

また、TS・個人情報保護推進活動を花王グループ全体で推進するために、海外の地域、会社グループ、個社の単位で海外に29のISCを設置しています。海外のISCが毎年3月に活動レポートを提出することで活動内容を確認しています。

国内花王グループ事故発生件数推移

・2023年は前年を大きく上回る
・PC・スマートフォンの紛失が2022年34件から72件に倍増



※KCMK、CMK、KCグループは2008年度から

情報セキュリティ

主な取り組み

情報セキュリティ委員会（ISC）の活動目標

2023年のISC活動目標を以下のように策定し実施しました。

①セキュリティ対策の強化

・セキュリティの強化のためセキュリティ戦略ロードマップに沿ってセキュリティ対策を強化
・メールセキュリティ、ウェブセキュリティ、アカウントセキュリティ、エンドポイントセキュリティの強化を実施
・PPAP禁止の実施

パスワード付きzipファイルはメール添付するとウイルスチェックが行えないため、パスワード付きzipファイルを添付したメールの送受信を拒否する設定を8月に行いました。

②サイバー保険更新

・サイバー保険の補償範囲
- 危機管理対応費用
- 第三者賠償責任
- 海外各国における当局対応費用
- 自社の経済的被害（含むデータ等の損害）
- 事業中断にかかる費用

③サプライヤーのセキュリティ対策のヒヤリング

2023年7月に製造委託先9社のセキュリティ・チェックを検討しましたが、2022年のサプライヤーのセキュリティ・チェックですでに実施済みということを確認しました。

④海外29情報セキュリティ委員会の活動状況把握

・カネボウコスメティックスロシア：活動休止中
・啓発活動の実施：28件
・自己点検の実施：26件
・目標設定の実施：26件
・インシデント発生あり：6社22件
・個人情報に対する削除要求25件（対応済み）
・EUのCookie削除要求：84件
・個人情報に対する苦情：0件

⑤国内個人情報保管理の強化

7月に個人情報の新管理システムが稼働しました。これにより、「どのような個人情報がどれだけあるか？」「どのシステムで処理され、どのように活用されているか？」「個人情報取扱のリスクはどこにあるか？」を把握します。

⑥情報セキュリティのPDCAサイクル

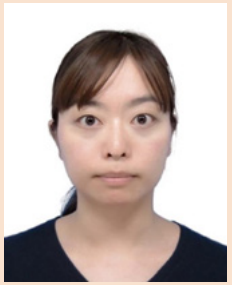
1. 機密情報リスト・啓発資料・自主パトロール設問の見直し
2. 啓発活動（各部門）実施
3. 自主パトロール・個人情報委託先監査の実施
4. 11月TS・個人情報保護推進会議の開催

・動画による啓発活動と花王の対策の解説
・国内のTS・個人情報事故報告
・自主パトロール総括
・改善目標設定
・個人情報を扱う誓約書の対象範囲変更の説明

情報セキュリティ

社員の声

DXを支えるグローバルセキュアインフラ環境の実現



雨宮 史歩
花王株式会社
情報システム部門
ESM部

情報システム部門のセキュリティ担当として、海外拠点含む花王グループ全体のセキュリティ戦略の立案、ソリューション導入、監視、インシデント対応等を実施しています。特に2023年は、セキュリティの礎となる認証基盤のグローバル展開が完了し、海外やテレワーク環境など場所を問わず、いつでも社員が安心してITを活用していくための環境が整いました。

サイバー攻撃は日々高度化・多様化しているため、今後も日本国内だけではなく海外IT担当とも連携し、「会社と社員」を守るしくみづくりに取り組んでいきます。

社員の声

グローバル全体のセキュリティ強化を推進

中治 干城
花王株式会社
法務部門
法務部

情報セキュリティ委員会の事務局運営と個人情報保護施策の推進を行っています。

情報セキュリティ委員会では8月を除く毎月、新規施策等について多様な観点での議論や方針の決定、ルールの整備、社内管理体制の整備、外部委託先の定期監査とりまとめ、啓発活動の実施を推進しています。特に啓発活動では、花王グループ社員への隅々に渡る啓発・教育活動を行い、質疑応答等のやりとりの中で社員一人ひとりの意識がより高まっていることを実感しています。また、海外各社の情報セキュリティ委員会とも緊密にやりとりし、グローバル全体でセキュリティ強化推進を行っています。時代の変化により対応するべき施策は年々増えていきますが、社員一丸となって対応を進めていきます。