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(ISC)を設置しています。このISCがサイバーセキュリティ対策・機密情報(トレードシークレット(TS))・個人情報およびハードウエア・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

インフォメーションテクノロジー(IT)の急速な発展と普及に伴い、ITは生活のあらゆる部分に浸透し、いまや社会基盤として必要不可欠なものとなっています。社会基盤のITに障害が起きた場合、電気やガスや水道のライフラインや交通インフラの停止等により、経済活動へ大きな打撃を与えることになります。さらに近年、サイバー攻撃により、企業からの機密情報や個人情報といった情報資産の流出が発生しており、サイバーセキュリティの確保が社会的課題となっています。2014年11月のサイバーセキュリティ基本法の成立により、国をあげてサイバーセキュリティ対策に取り組んでいます。

花王では情報セキュリティ委員会(Information Security Committee: ISC)が中心となってリスク危機管理委員会との連携のもとに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ロードマップに沿って対策を実施しています。花王がめざしているのは、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になります。

また近年、EUのGDPR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。この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。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。それらの個人情報保護法の制定や改定の内容を把握し、花王グループ会社が取るべき必要な対応を実施し、各国の個人情報保護法を遵守しています。

方針

花王は、「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)(ユーザー編)」、「Web・アプリセキュリティガイドライン」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・管理方法を明確にしています。

個人情報の取り扱いについては、「花王グループ会社の個人情報保護指針」で公表しており、お問い合わせ・苦情の受け付けについても「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」で窓口を公表しています。

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://www.kao.com/global/en/EU-Data-Subject-Request/

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・マーケティング活動・研究開発活動の長期間の停止や、機密情報(トレードシークレット:TS)・個人情報といった情報の漏えいによる企業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機密情報(トレードシークレット: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

情報セキュリティ GRI3-3

現やネットワークを介した多様な働き方を可能とします。

戦略

サイバーセキュリティ対策はセキュリティ戦略ロードマップに沿って予算を確保し、実施しています(セキュリティ対策の緊急度と配分できる予算により決定)。

2022年にはメールセキュリティ(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)、アカウントモニタリング(アカウントの乗っ取りの防止対策)、EDR(Endpoint Detection and Response:PCやサーバーにおける不審な挙動を検知し、迅速な対応を実施するソフトウェア)の欧米・日本に導入しました。2023年は第1四半期でEDRのアジア導入を完了予定です。また、24時間365日、ネットワークやサーバや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)のグローバル展開を実施する予定です。併せて従業員へのセキュリティ教育も実施します。

社会的インパクト

花王は、自社が経験したサイバー攻撃について情報共有ネットワークを通じて業界や日本の企業に共有することにより、業界や日本の企業全体のセキュリティ対策の向上に貢献したいと考えています。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/CC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。

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うことになります。

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、機密情報(トレードシークレット:TS)・個人情報の漏えい・流出を防ぐことができれば、漏えい・流出が発生した場合の対応コストを低減できます。また、機密情報(トレードシークレット:TS)・個人情報の漏えい時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。

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および維持管理を行うために、代表取締役社長執行役員(CEO)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。情報セキュリティ最高責任者(CISO)は執行役員で、情報セキュリティ委員会(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、人財開発、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・ガバナンス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および実績評価で、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

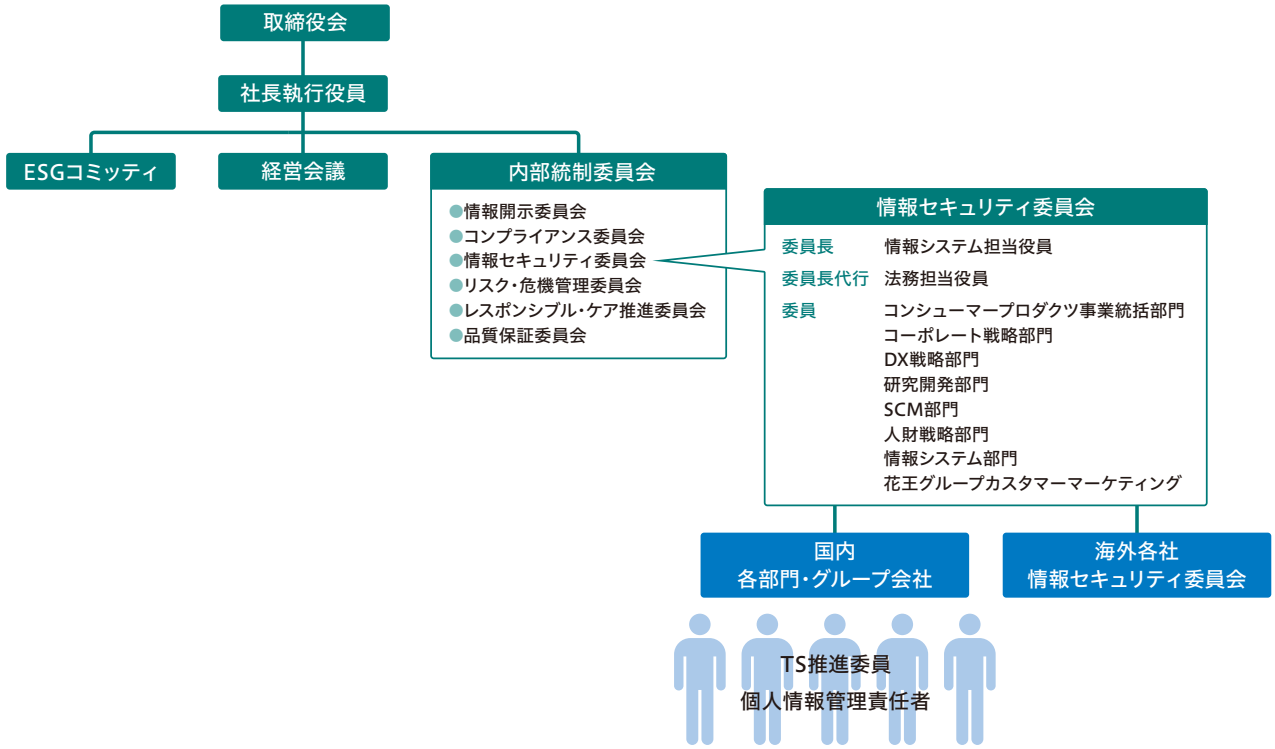
情報セキュリティ GRI3-3

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。

P18 Our ESG Vision and Strategy > ガバナンス

情報セキュリティの管理体制



※2023年1月現在

情報セキュリティ GRI3-3

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
花王グループ	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

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 GRI3-3

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。

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　・消費者　・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・問合せ対応等検討・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・問合せ対応実施
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 GRI3-3, 404-2

教育と浸透

社内教育は、機密情報(トレードシークレット: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き、

①機密情報(トレードシークレット:TS)や個人情報や情報セキュリティについての講演や啓発
②花王の機密情報(トレードシークレット:TS)や個人情報に関する事故件数や傾向の分析やフィードバック
③各部門での教育のための啓発資料提供

を行っています。2022年は11月に実施し、会議室とウェブ会議で321名のTS推進委員・個人情報管理責任者が参加しました。

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を行っています。自己点検によるチェックで課題を抽出し、改善目標を設定、改善活動を実施しています。

海外では各情報セキュリティ委員会(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2022年には、包材サプライヤー107社、原材料プライヤー86社にヒアリングを実施し、評価を行いました。リスクの高いサプライヤーに対しては、購買部門が対策の協議を実施しています。

国内の個人情報委託先の書面監査

業務委託先206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サイクルによる機密情報(トレードシークレット:TS)・個人情報保護推進活動は以下の通りです。

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
・海外情報セキュリティ委員会(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

・機密情報(トレードシークレット: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

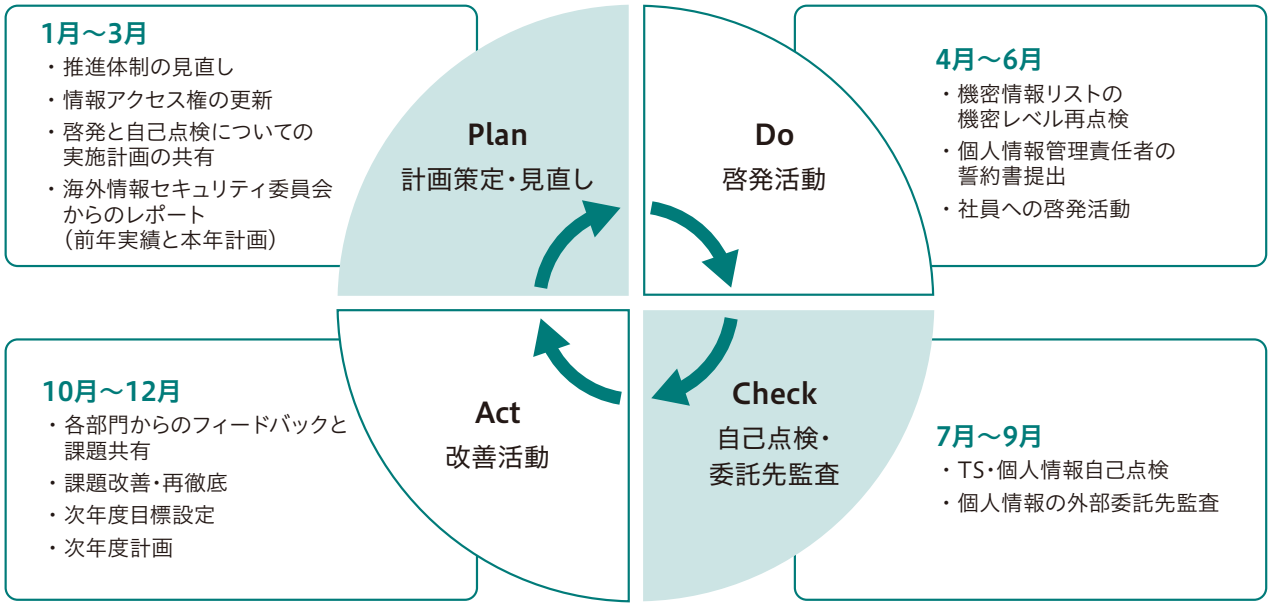
Act:改善活動

・機密情報(トレードシークレット:TS)・個人情報事故の総括を実施
・機密情報(トレードシークレット: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

P33 Our ESG Vision and Strategy > リスク管理

情報セキュリティ

情報セキュリティ活動のPDCA



目標と指標

中長期目標と2022年実績

中長期目標

・サイバーセキュリティ対策を含めた機密情報（トレードシークレット：TS）・個人情報およびハードウエア・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、対応決定、再発防止策策定と実行

2022年実績

花王において、機密情報（トレードシークレット：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。

Plan：計画策定・見直し

・TS推進委員303名、個人情報管理責任者247名の見直し

・日本の144部門・部署・関係会社で機密情報リストの見直し

・海外29ISCからのレポート受領

Do：啓発活動

・個人情報管理責任者の誓約書提出2,090名

・日本の160部門・部署・関係会社で啓発活動実施

情報セキュリティ

Check：自己点検・委託先監査

・日本の166部門・部署・関係会社でTS自己点検実施
　- 日本の124部門・部署・関係会社で個人情報自己点検実施
・179社に対して個人情報の委託先監査を実施

Act：改善活動

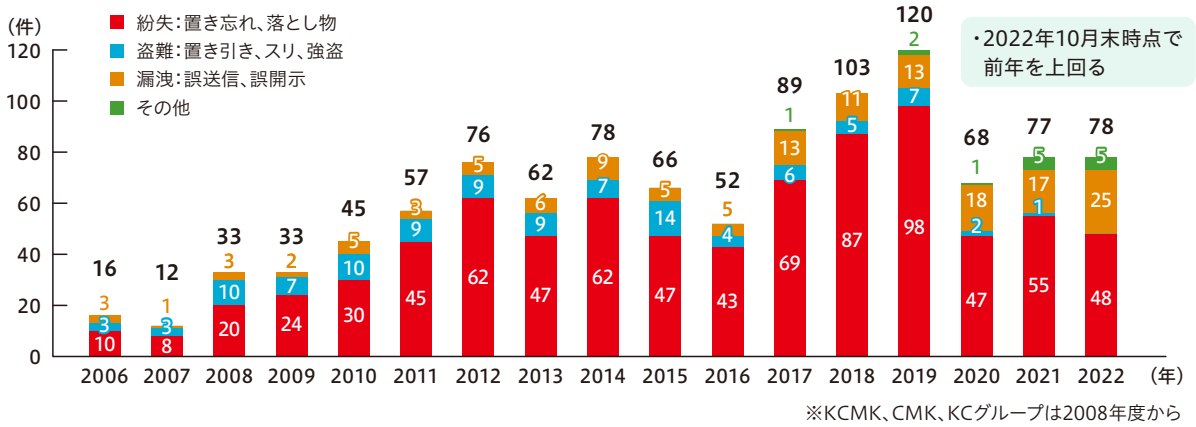
花王において、TS・個人情報保護を含めた情報セキュリティに関して重大な事故の発生はありませんでした。また、「問い合わせ窓口」に寄せられた個人情報に関する苦情はありませんでした。

・2022年11月15日に全体会議を開き、305名が参加しました。
・2022年の機密情報（トレードシークレット：TS）・個人情報の事故件数は10月末時点で78件です。

2022年の機密情報（トレードシークレット：TS）自己点検の結果、改善目標は以下のようになりました。

・部門マニュアル（機密情報リスト）は定期的に見直し、保管期間を明記する。
・自宅での機密情報の管理を徹底し、離席時のPC画面ロックを徹底する。

国内花王グループ事故発生件数推移（2022年10月末まで）



※KCMK、CMK、KCグループは2008年度から

2022年の個人情報自己点検の結果、改善目標は以下のようになりました。

・自部門の取り扱う情報に個人情報が含まれているかを定期的に確認し、個人情報を取得・保管している場合は個人情報取扱い台帳システムに登録する。

2022年実績に対する考察

機密情報（トレードシークレット：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。機密情報（トレードシークレット：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機密情報（トレードシークレット：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、この機密情報（トレードシークレット：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の情報セキュリティ委員会（ISC）を設置しています。海外のISCから年1回3月に活動レポートにより活動内容を確認しています。

情報セキュリティ

主な取り組み

日本の情報セキュリティ委員会(ISC)の活動目標策定

2022年のISC活動目標を以下のように策定し実施しました。

①海外29情報セキュリティ委員会の活動状況

・KC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

②サイバー保険更新

③国内改正個人情報保護法施行対応

・規程改定の説明会の1月に実施
・国内WebサイトのCookie取得の同意取得を4月から実装

④サプライヤーのセキュリティ対策のヒヤリング

・6月に包材サプライヤー107社、原材料サプライヤー86社にヒヤリング実施、リスクを把握、対策を検討

セキュリティ対策の強化

⑤セキュリティ戦略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、Web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

⑥PPAP廃止検討

・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、花王からパスワード付きzipファイルを添付したメールを送信しない、また受け取らないために代替手段の提供や社内規程の改正を検討、2023年6月からの実施を予定。

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

・個人情報専用サーバー利用の誓約書MS Forms化による電子データでの管理実施

③自主パトロール・個人情報委託先監査の実施

④11月TS・個人情報保護推進会議の開催

・動画による啓発活動
・PPAP廃止の説明
・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