情報セキュリティ 102-11,102-12,102-15,103-1,103-2,103-3,404-2

花王のアプローチ

花王グループでは情報セキュリティポリシーのもと、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ェア・ソフトウェア・各種データファイル等の情報資産の保護を目的とした情報セキュリティの強化を図っています。社内ルールの制定や内部管理の徹底と遵守に向け、PDCAサイクルによる保護推進活動を実施しています。

社会的課題と花王が提供する価値

認識している社会的課題

各企業はITを活用して事業や業務を効率的に進めるとともに、データ活用によりビジネスの革新・改革を進めています。これにより、業種を超えた新たな成長分野の創出や多様な人材の確保が進んでいます。

一方近年、サイバー攻撃により事業活動の一時的中断や情報漏洩による業績の悪化のリスクが高まっており、サイバーセキュリティ対策が社会的課題となっています。

花王が提供する価値

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企業に共有することにより、業界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。

「2030年のありたい姿」の実現に関わるリスク

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、情報漏洩による企業信頼の失墜は大きなリスクの一つです。

「2030年のありたい姿」の実現に関わる機会

サイバーセキュリティ対策やTS・個人情報といったデータ管理を強固にすることで、新たなデータ活用の実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。

貢献するSDGs

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」を制定して、サイバーセキュリティ対策や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。

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、新入社員の配属時期や異動による転入者が発生したタイミングで開催され、各部門での実施を基本としています。そのため、TS推進委員や個人情報管理責任者に対して外部講師による講演や最新動向の周知を行なっています。また、各部門での教育のための啓発資料をTS推進委員や個人情報管理責任者に提供しています。全社員向けには社内ポータルサイトによる注意喚起や啓発も行なっています。

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なっています。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、改善活動を推進しています。

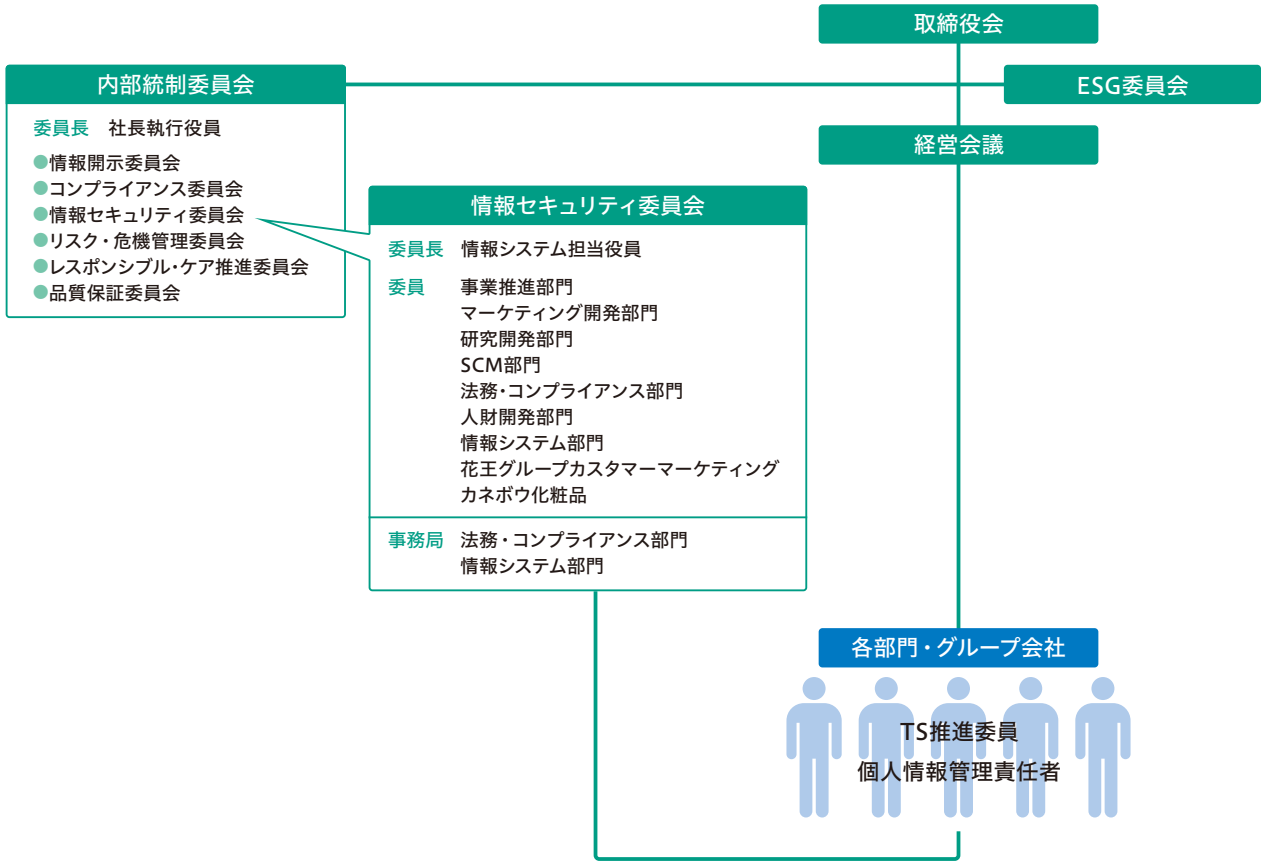
情報セキュリティ 103-2,103-3 花王のアプローチ

体制

花王では、情報セキュリティ委員会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、知的財産、生産技術、法務・コンプライア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。

情報セキュリティ委員会は、四半期に一度、内部統制委員会に活動報告しており、内部統制委員会が取締役会へ傘下の委員会の活動報告をまとめて行ないます。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あわせて報告されます。グローバルでの推進体制は、日本の情報セキュリティ委員会の傘下に各国の情報セキュリティ委員会を配置する形で、GDPR対応を行なった欧州・米州と、すでに情報セキュリティ部会という対応組織のある中国を中心に2019年度に展開していきます。

情報セキュリティの管理体制



※2018年12月現在

情報セキュリティ 103-1,103-2,103-3 花王のアプローチ

中長期目標と実績

中長期目標

・サイバーセキュリティ対策を含めたTS・個人情報およびハードウェア・ソフトウェア・各種データファイル等の情報資産の保護
・情報漏洩事故等、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

中長期目標を達成することにより期待できること

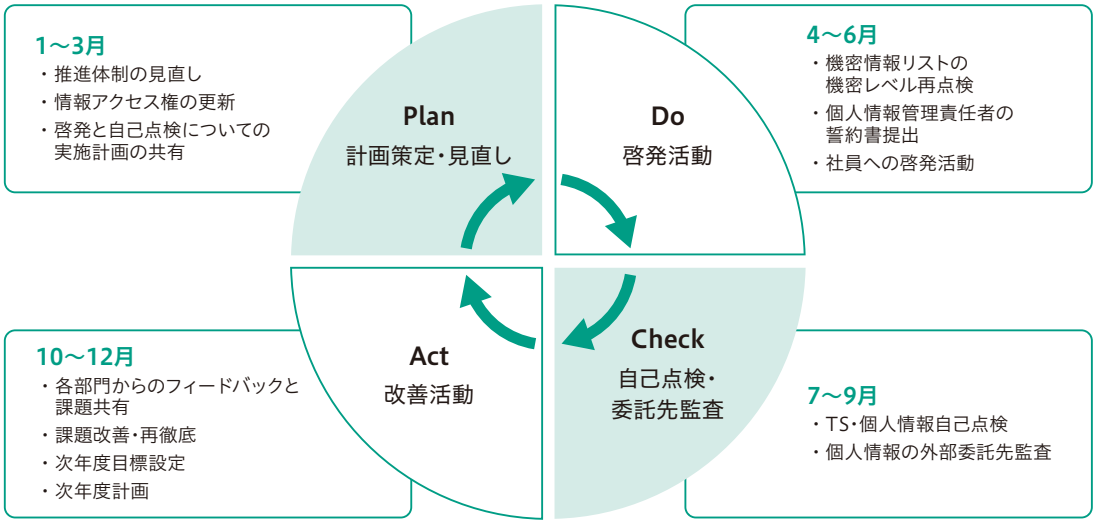
コスト低減あるいは収益拡大

サイバーセキュリティ対策により、TS・個人情報の漏洩・流出を防ぐことができれば、漏洩・流出が発生した場合の対応コストを低減できます。また、TS・個人情報の漏洩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。

社会に及ぼす効果

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。

情報セキュリティ活動のPDCA



情報セキュリティ 103-1,103-2,103-3

花王のアプローチ

2018年の実績

実績

TS・個人情報保護推進活動をPDCAサイクルで実施しました。

第1四半期：計画策定・見直し

- TS・個人情報保護推進体制見直し
- 標的型メール訓練実施
- GDPR対応を監査役会で報告

第2四半期：啓発活動

- 日本の99部門・部署・関係会社でTSの啓発活動を実施
- 日本の77部門・部署・関係会社で個人情報の啓発活動を実施
- 個人情報漏洩時対応訓練実施
- EU向けウェブサイトのGDPR対応実施
- GDPR対応を経営会議で報告
- 中国サイバーセキュリティ法対応状況確認
- 経済産業省の「サイバーセキュリティ経営ガイドラインV2.0」対応

第3四半期：自己点検・委託先監査

- 日本の109部門・部署・関係会社でTSの自己点検を実施
- 日本の88部門・部署・関係会社で個人情報の自己点検を実施
- 182社に対して個人情報委託先書面監査を実施

第4四半期：改善活動

- 2018年11月15日に全体会議（遠隔地はWeb会議で中継）の「第25回TS・個人情報保護推進会議」を開催し、2018年のTS・個人情報に関する事故報告および自己点検のフィードバックと改善目標の設定を行ないました。
- 海外セキュリティアセスメントの実施：アジア10社、米州3社、欧州3社

実績に対する考察

TS・個人情報の保護推進活動は、毎年、継続的に行なう必要があります。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従業員が花王グループの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、このTS・個人情報保護推進活動をグローバルに拡大していくことも必要と考え、検討を始めています。

ステークホルダーとの協働

化学製品製造業者等により構成される業界団体である一般社団法人日本化学工業協会の「情報セキュリティ対応部会」に参加することで、日本の化学業界での情報セキュリティの向上に貢献しています。

また、独立行政法人情報処理推進機構（IPA）が主催する「サイバー情報共有イニシアティブ（J-CSIP）」と、警察庁が主催する「サイバーインテリジェンス情報共有ネットワーク」の2つのサイバー攻撃に対する情報共有ネットワークに加えて、2017年からJPCERT コーディネーションセンターが提供する「早期警戒情報」にも参加しました。これらの情報共有ネットワークからソフトウェアの脆弱性情報やサイバー攻撃の情報を入手するだけではなく、花王が受けたサイバー攻撃の情報を開示・共有することで、日本のサイバーセキュリティ対策に貢献しています。

2018年6月には、花王のキャンペーンを騙り、消費者の個人情報を盗みだそうとする事件が発生しました。これに対しては、ウェブサイトやTwitter・Facebookの公式アカウントで注意喚起を行ない、消費者の皆さまと一緒に被害の防止に取り組みました。

情報セキュリティ 103-1,103-2,103-3

具体的な取り組み

具体的な取り組み

第1四半期：計画策定・見直し

TS・個人情報保護推進体制見直し

組織変更や人事異動による役割変更に伴って、TS推進委員46人、個人情報管理責任者35人、情報セキュリティ委員会委員1人の体制の見直しを実施しました。組織変更や人事異動があっても、花王グループのTS・個人情報保護推進活動が途切れることのないように、次の担当に確実に引き継ぎをしています。

標的型メール訓練実施

2018年2月に日本花王グループの19,746人を対象に4回目の標的型メール訓練を実施し、添付ファイル開封率が13.7%で昨年と比較して改善しました。

しかし、従業員一人一人 がサイバーセキュリティの意識を持って不審なメールを見抜き、不用意に添付ファイルを開封しないよう、今後も継続的な注意喚起が必要です。

標的型メール訓練での開封率

	2015年	2016年	2017年	2018年
開封率	21.3%	31.5%	18.5%	13.7%

第2四半期：啓発活動

個人情報漏洩時対応訓練の実施

2018年4月にPart1：インシデント対応訓練、Part2：記者会見訓練の2部構成で、個人情報漏洩時対応訓練を実施しました。

インシデント対応訓練では、サイバー攻撃により花王のサーバがマルウェアに感染し、その結果、個人情報が漏洩したという想定で、緊急対策会議を複数回開催し、発覚した事実の共有とその対応策の検討・実施を行ないました。記者会見訓練では、2名の執行役員が想定登壇し、記者役のコンサルタントから厳しい質問をしていただきました。この訓練を通して抽出した課題の一つはコールセンターの委託先の確保やキャパシティプランニングです。個人情報の漏洩を公表するためには問い合わせ窓口の設置が必要になりますが、問い合わせ窓口を社内のリソースで対応できない場合を想定して、最短でコールセンターを立ち上げられ、かつコールセンターの人員を最大限増員できる委託先をあらかじめ選定する必要性が明らかになりました。

個人情報漏洩時対応訓練の記者会見訓練より

経済産業省の「サイバーセキュリティ経営ガイドラインV2.0」対応

2017年11月に改訂された「サイバーセキュリティ経営ガイドラインV2.0」では、経営者が認識すべき3原則と経営者が最高情報セキュリティ責任者（CISO）等に指示すべき10の重要事項が定義されています。後者はアメリカ国立標準技術研究所（NIST）のセキュリティフレームワークに関連が示されています。花王は、NISTのセキュリティフレームワークで自社グループの現状を把握・課題を抽出し、改善を図っています。

情報セキュリティ 103-1,103-2,103-3

具体的な取り組み

第3四半期：自己点検・委託先監査

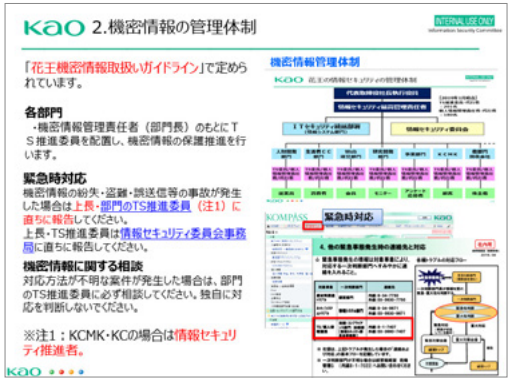
TS・個人情報保護の自己点検

TS自己点検は、啓発活動の実施、部門マニュアルの整備、TS表示の実施、機密情報の管理について徹底を図るため、毎年状況を確認しています。2018年は7月9日から8月10日に実施しました。

個人情報自己点検も同様に、啓発活動の実施、個人情報の保有、個人情報に関する業務の委託の有無、個人情報の管理について、TS自己点検と同時期に実施しました。2018年11月15日の全体会議「TS・個人情報保護推進会議」で自己点検のフィードバックを行ない、改善目標を設定しています。

TSの改善目標は、「機密情報をやむを得ず持ち出す場合は紙媒体ではなく、会社が貸与したPCやスマートフォンで持ち出す」と設定しました。ID・パスワードでロックされている会社貸与PCやPINコードでロックされている会社貸与スマートフォンであれば、盗難・紛失事故があっても、直ちに情報漏洩につながらないためです。

個人情報の改善目標は、「個人情報をセキュリティ機能で守られた個人情報専用サーバで保管する」と設定しました。個人情報専用サーバで保管すると、ファイル単位でアクセス制御が行なえるため、ファイルが漏洩してもアクセス権のある者しか開くことができないので情報が守られます。



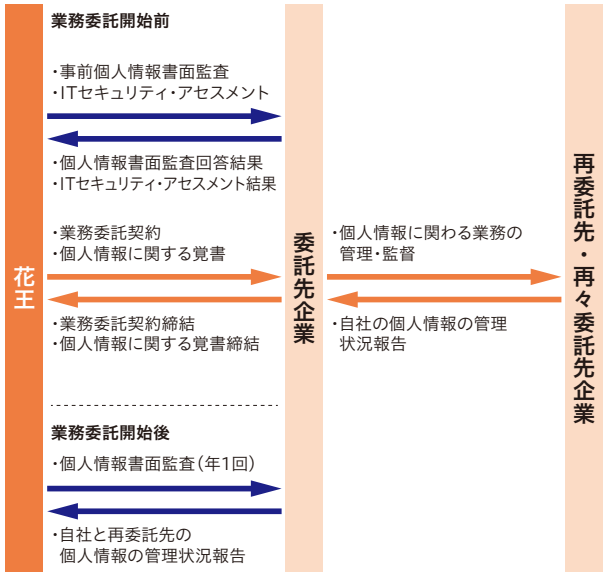
情報セキュリティ啓発資料より

個人情報委託先監査

花王は個人情報に関する業務を委託する場合、委託先が個人情報を安全に扱えるか事前の監査を行なっています。Webキャンペーンのようなシステムを委託先が提供する場合は、ITセキュリティ・アセスメントも行なっています。この委託先の個人情報事前監査とITセキュリティ・アセスメントに合格しないと、委託契約の締結は行ないません。

また、花王は毎年継続的に個人情報委託先監査を行なうことで個人情報の委託先の管理・監督をしています。2018年は182社に対して個人情報委託先監査を実施し、個人情報の管理状況、委託先の個人情報保護の体制を確認しました。個人情報を委託先に保管している場合は、件数を確認し、個人情報取扱い台帳システムに登録しているデータ件数と整合性をチェックしています。

個人情報に関わる業務の委託と委託先監査



●個人情報台帳管理
●委託先管理

情報セキュリティ 102-12,103-1,103-2,103-3

具体的な取り組み

第4四半期：改善活動

「第25回TS・個人情報保護推進会議」を開催

2018年11月15日に「第25回TS・個人情報保護推進会議」を開催しました。外部の講師による講演テーマは、「サイバーセキュリティは事業継続課題」で、ここ数年、機密情報や個人情報の漏洩の原因として大きな脅威になっているサイバー攻撃について、多くの事例を紹介していただきました。続いて、2018年のTS・個人情報に関する事故の総括、TS・個人情報自己点検のフィードバックを行ない、改善目標を設定しました。

TS・個人情報保護推進会議
本社会場に113人、各事業場へは中継で174人が参加

GDPRへの対応

EUの一般データ保護規則（GDPR: General Data Protection Regulation）が2018年5月25日に施行されました。GDPRは個人データの処理と移転に関する法律で、厳しい規制と罰則が特徴となっています。

主な対応

- EU域外への個人データ移転の適法化：標準契約条項（SCC）締結
- 個人の権利行使の尊重：「Privacy Policy更新」「cookie取得の同意取得」
- データ保護責任者（DPO）の設置
- データ保護影響評価（DPIAs）の実施と処理の記述（RoPA）の作成
- 安全管理措置（DPA：Data Processing Agreementの締結）
- 権利侵害時の公開義務

中国サイバーセキュリティ法対応

2017年6月に施行した中国サイバーセキュリティ法では、中国国内で収集した重要データについては中国国内保存が義務付けられています。個人情報はここでいう重要データにあたります。個人情報を越境移転する場合は、個人情報提供者に「データ国外持ち出しの目的、範囲、種類および受領者の所在国または地域」を示し、同意が必要です。

また、個人情報を越境移転する場合は、政府機関によるセキュリティ審査を受ける必要があります。花王グループでは、化粧品の顧客情報システムが個人情報を日本のサーバで処理します。そこで、法的要件を満たすために、化粧品顧客システムでは、中国部分を分離し、中国国内でデータを保存するように対応しています。

海外セキュリティアセスメント

海外セキュリティアセスメントは、花王グループの海外各社に以下の158項目をチェックし、セキュリティ対策の弱い部分を把握して改善を行なうために実施します。

主なチェック項目

- セキュリティポリシーと標準
- ユーザー認証
- システム・オペレーション＆コントロール
- IT資産管理
- 物理環境のコントロール
- マルウェアからの保護
- インシデント管理
- コンプライアンス
- ディザスタリカバリ取り扱い

2018年はこの海外セキュリティアセスメントをアジア10社、米州3社、欧州3社に実施し、海外各社のサイバーセキュリティの向上を図っています。