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

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。

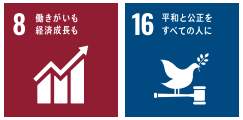
「2030年のありたい姿」の実現に関わるリスク

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(管理者編)(ユーザー編)」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。

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」にて公表しており、お問い合わせ・苦情の受付についても「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。

➡花王グループ会社の個人情報保護指針
www.kao.com/jp/corporate/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
www.kao.com/jp/corporate/privacy/privacy-contact/

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TSや個人情報の保護に関わる情報セキュリティについての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。

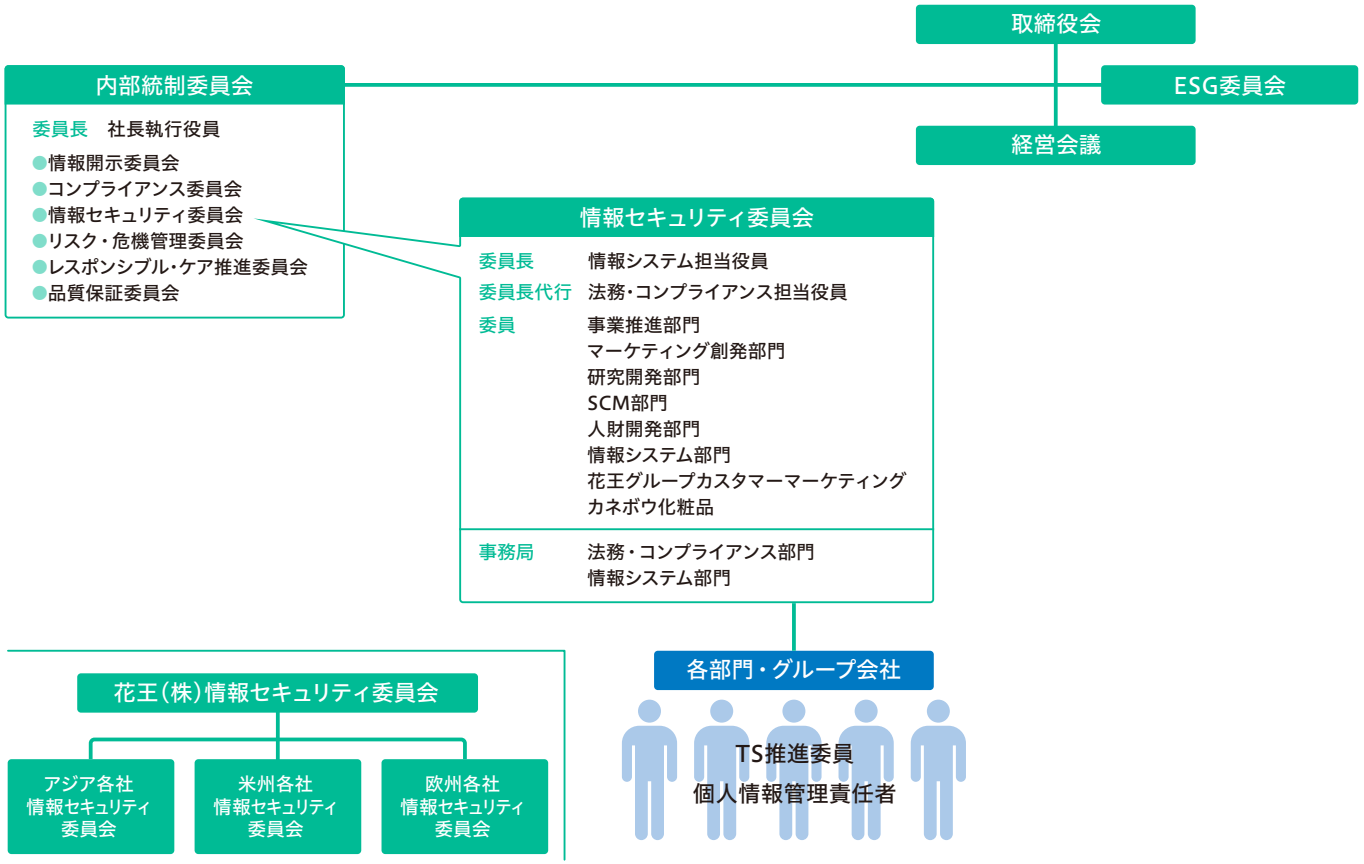
情報セキュリティ 102-20,103-2

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、研究開発、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体制整備を推進しました。

情報セキュリティの管理体制



※2019年12月現在

情報セキュリティ 103-2,103-3

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

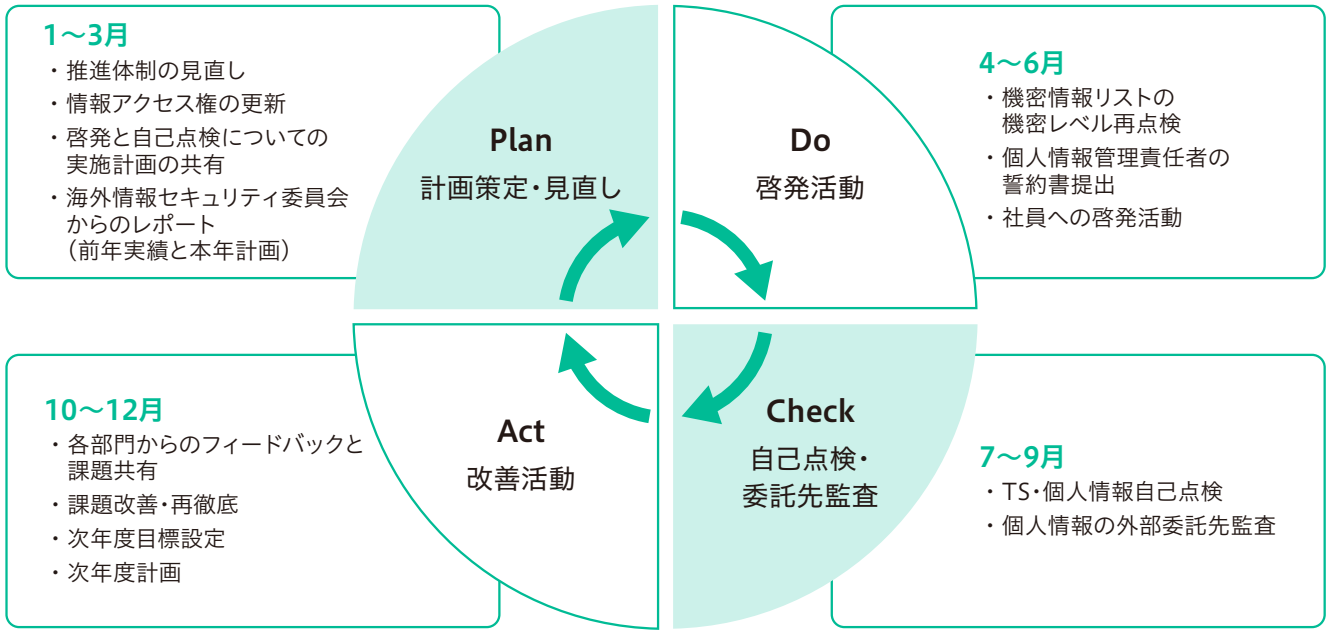
事業インパクト

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。

社会的インパクト

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 103-2,103-3

2019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
- 実施計画策定
- 啓発資料改定（ITセキュリティガイドライン（ユーザー編）対応）

第2四半期：啓発活動

- 日本の120部門・部署・関係会社でTSの啓発活動を実施
- 日本の93部門・部署・関係会社で個人情報の啓発活動を実施
- グローバルでの推進体制の経営会議で承認
- 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」対応継続

第3四半期：自己点検・委託先監査

- 日本の130部門・部署・関係会社でTSの自己点検を実施
- 日本の101部門・部署・関係会社で個人情報の自己点検を実施
- 195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

- 2019年11月14日に全体会議（遠隔地はウェブ会議で中継）の「第26回TS・個人情報保護推進会議」を開催し、情報セキュリティに関わる最近のインシデントをもとに従業者の意識と行動の向上を促すとともに、昨年提示した改善目標についてのリマインド、ならびに2019年のTSと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。
- 米国カリフォルニア州消費者保護法への対応状況確認
- GDPR対応の運用状況確認

日本花王グループにおいて、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、個人情報の保護について、これまでに、法律に基づいて罰金を科せられたことや指導・勧告を受けたことはありません。

2019年に「個人情報に関するお問い合わせ・苦情受付窓口」に寄せられた内容は、会員登録情報の変更方法に関するものが3件でした。

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するための体制整備を進めています。

情報セキュリティ 103-2

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56人、個人情報管理責任者50人、情報セキュリティ委員会2人、同委員会事務局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、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。

第2四半期：啓発活動

社内規程の再整備

サイバー攻撃への対応強化のため、2019年6月に社内規程「ITセキュリティガイドライン」を「ITセキュリティガイドライン（管理者編）」に改定し、新たに「ITセキュリティガイドライン（ユーザー編）」を制定しました。管理者編は、ITシステム管理の視点で改定しており、ユーザー利用視点は方針に留めています。一方、ユーザー編は、ユーザー利用視点のオペレーションレベルと「情報機器利用の手引き」を統合してルール化し、啓発資料も改訂し、サイバー攻撃へのユーザーの意識向上を図っています。

ガイドライン一覧と一例

情報セキュリティ 103-2

ビジネスメール詐欺や標的型攻撃メールに関する注意喚起

2019年3月以降に花王に対するビジネスメール詐欺や標的型メールによる攻撃が複数回確認されました。被害防止のため、技術的対策として、受信メールのフィルタリング強化とウェブサイトの無害化を実施しています。また、ビジネスメール詐欺や標的型攻撃メールでは、花王内部に実在する者を差出人として記したメールが大半を占めるため、花王外から発信されたメールの標題の先頭に[External]を表示することにして、悪意ある外部の者によるなりすましを防ぐための対策を行ないました。

一方、人的対策として、ビジネスメール詐欺については、日本語および英語のイントラネットの掲示板にて、花王の国内外の従業者への注意喚起を行なっています。また、標的型攻撃メールについても、攻撃対象と思われる社員に対して注意喚起を行なっています。

注意喚起メール

各社社長にも注意喚起メールを送信し、英語ポータルサイトでも啓発

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、抽出された課題のうち2018年に対応できなかったものについては継続して改善を図っています。

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

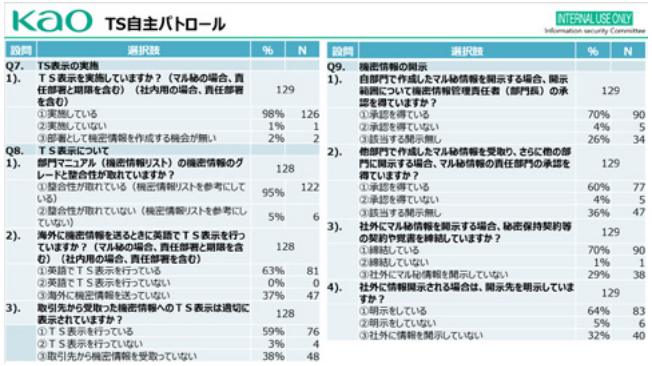
TS自己点検では、啓発活動の実施、部門マニュアルの整備、TS表示の実施、機密情報の管理について徹底を図るため、毎年状況を確認しています。2019年は7月22日から8月23日に実施しました。

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。2019年11月14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、「機密情報を紙で持ち出さない」と設定しました。情報の持ち出しには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からのクラウド利用を促し、PCやスマートフォンの盗難・紛失事故があっても直ちに情報漏洩につながらない方策を進めています。

個人情報の改善目標は、「個人情報データは個人情報専用サーバに保管」と設定しました。個人情報専用サーバで保管すると、データが暗号化されるとともに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 103-2,404-2



kao TS自主パトロール

INTERNAL USE ONLY
Information security Committee

設問	選択肢	%	N
Q7.	TS表示の実施		
1).	TS表示を実施していますか？（マル秘の場合、責任部署と期限を含む）（社内用の場合、責任部署を含む）		129
	①実施している	98%	126
	②実施していない	1%	1
	③部署として機密情報を作成する機会が無い	2%	2
Q8.	TS表示について		
1).	部門マニュアル（機密情報リスト）の機密情報のグレードと整合性が取れていますか？		128
	①整合性が取れている（機密情報リストを参考にしている）	95%	122
	②整合性が取れていない（機密情報リストを参考にしていない）	5%	6
2).	海外に機密情報を送るときに英語でTS表示を行っていますか？（マル秘の場合、責任部署と期限を含む）（社内用の場合、責任部署を含む）		128
	①英語でTS表示を行っている	63%	81
	②英語でTS表示を行っていない	0%	0
	③海外に機密情報を送っていない	37%	47
3).	取引先から受取った機密情報へのTS表示は適切に表示されていますか？		128
	①TS表示を行っている	59%	76
	②TS表示を行っていない	3%	4
	③取引先から機密情報を受取っていない	38%	48

設問	選択肢	%	N
Q9.	機密情報の開示		
1).	自部門で作成したマル秘情報を開示する場合、開示範囲について機密情報管理責任者（部門長）の承認を得ていますか？		129
	①承認を得ている	70%	90
	②承認を得ていない	4%	5
	③該当する開示無し	26%	34
2).	他部門で作成したマル秘情報を受取り、さらに他の部門に開示する場合、マル秘情報の責任部門の承認を得ていますか？		129
	①承認を得ている	60%	77
	②承認を得ていない	4%	5
	③該当する開示無し	36%	47
3).	社外にマル秘情報を開示する場合、秘密保持契約等の契約や覚書を締結していますか？		129
	①締結している	70%	90
	②締結していない	1%	1
	③社外にマル秘情報を開示していない	29%	38
4).	社外に情報開示される場合は、開示先を明示していますか？		129
	①明示をしている	64%	83
	②明示をしていない	5%	6
	③社外に情報を開示していない	32%	40

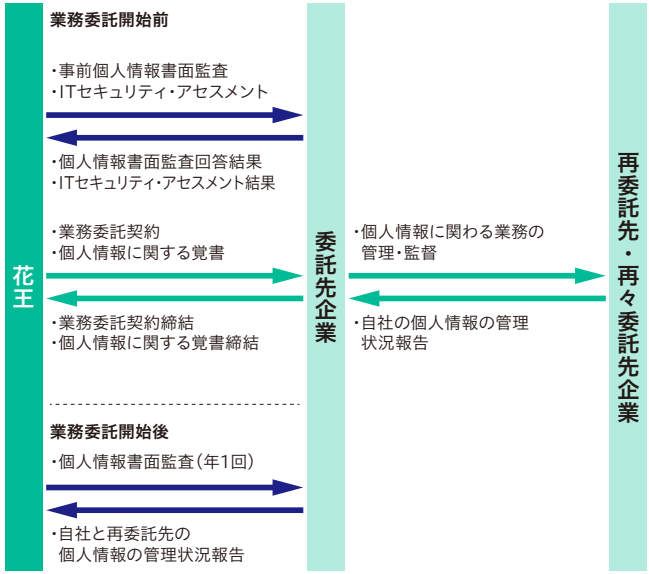
TS自己点検チェックリスト

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。ウェブ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。2019年は195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

第4四半期：改善活動

「第26回TS・個人情報保護推進会議」を開催

2019年11月14日に「第26回TS・個人情報保護推進会議」を開催しました。社内講師による講演テーマは、「サイバーセキュリティセミナー～標的型メール攻撃を防ぐ主役は“みなさん”です！～」で、機密情報や個人情報の漏洩などの原因の一つになっている標的型攻撃メールに加えてビジネスメール詐欺およびランサムウェアなど、花王の個々の従業者を狙う悪意ある者の手口を紹介し、それらへの対応のための適切な行動の徹底の浸透を図りました。続いて、2019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110人、各事業場へは中継で169人が参加

情報セキュリティ 103-2,102-43

GDPR施行後の運用状況確認

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。規則施行後の運用状況を、EU内の花王グループ会社に確認を行ないました。

組織とルールの整備や必要な契約締結など、個人情報取り扱いにおける安全管理措置については、規則にて求められる内容に対応しています。また、GDPRにて新たに定められ個人情報に関する本人からの要求への対応と監督機関への事故報告については、適切に実施できています。

課題としては、EU内の各社が作成した数百件の個人情報の処理活動記録（Record of Processing Activity）の継続的な定期確認の実施とそのプロセス改善と認識しており、そのために管理ツールの導入を検討しています。

海外各社へ情報セキュリティ委員会を展開

サイバー攻撃対応や情報資産保護の花王グループ海外各社における強化のために、情報セキュリティ委員会を海外に展開します。これによって、TSや個人情報の保護推進など情報セキュリティの活動を海外各社の従業員レベルまで広げ、情報セキュリティに関する重大な事象について花王（株）へのレポーティングラインを確立しました。

花王における必要な規程改定は2019年5月に承認され、花王グループ海外各社にて、2020年からの活動開始を目標に規程の制定と体制の整備を進めています。

公開ウェブサイトのセキュリティの確認

インターネット上に公開されているウェブサイトでは適切なセキュリティの措置ができていないと、そのウェブサイトが悪意ある者によって乗っ取られ、サイバー攻撃の踏み台などに悪用されることがあります。

国内の花王グループ会社では、新規に作成するウェブサイトについて、脆弱性などのセキュリティの問題がないことの確認を行なっています。また、国内の花王グループ会社がインターネット上にすでに公開しているウェブサイトが被害に遭わないように、現状を把握してそれぞれのセキュリティの状況の確認を行ない、問題が見つかった場合には必要な対応を実施しています。

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/CC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エ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。

経済産業省が開催した「産業サイバーセキュリティ対策説明会」にも参加し、急増が予想されるサイバー攻撃に備えて、日本政府の方針に従って業界をあげて対策に取り組みます。