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

花王では事業・リージョン(または国・地域)別に24の情報セキュリティ委員会(ISC)を配置しています。このISCが共通の方針や規程、ガイドラインを制定し、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。

ESGキーワード | サイバーセキュリティ対策 | 機密情報の保護 | 個人情報の保護 | 情報資産の保護 | GDPR対応 | インシデント対応体制 | ウェブサイトの脆弱性診断 | 在宅勤務時のセキュリティ対策

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。

また、コロナ禍で在宅勤務が普及し、在宅勤務時を含めた情報管理やセキュリティの確保が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。

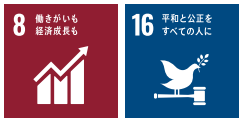
「2030年までに達成したい姿」の実現に関わるリスク

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年までに達成したい姿」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。2020年に個人情報に関するクレームはありませんでした。

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

英語版
www.kao.com/global/en/privacy/

EMEA向け(GDPR準拠)
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
www.kao.com/jp/corporate/privacy/privacy-contact/

EU向け(GDPR準拠)
www.kao.com/global/en/EU-Data-Subject-Request/

情報セキュリティ 102-20,102-43,103-2,404-2

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、各部門のTS推進委員・個人情報管理責任者に対してTS・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い、各部門での教育のための啓発資料を提供しています。

全社員向けには社内ポータルサイトによる啓発資料の掲載やタイムリーな注意喚起も行なっています。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。

海外では各ISCが啓発や自己点検の実施計画を作成し、実施しています。

ステークホルダーとの協働／エンゲージメント

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。

体制

情報セキュリティの管理体制

日本では、情報セキュリティ委員会(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・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。

ISCは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。

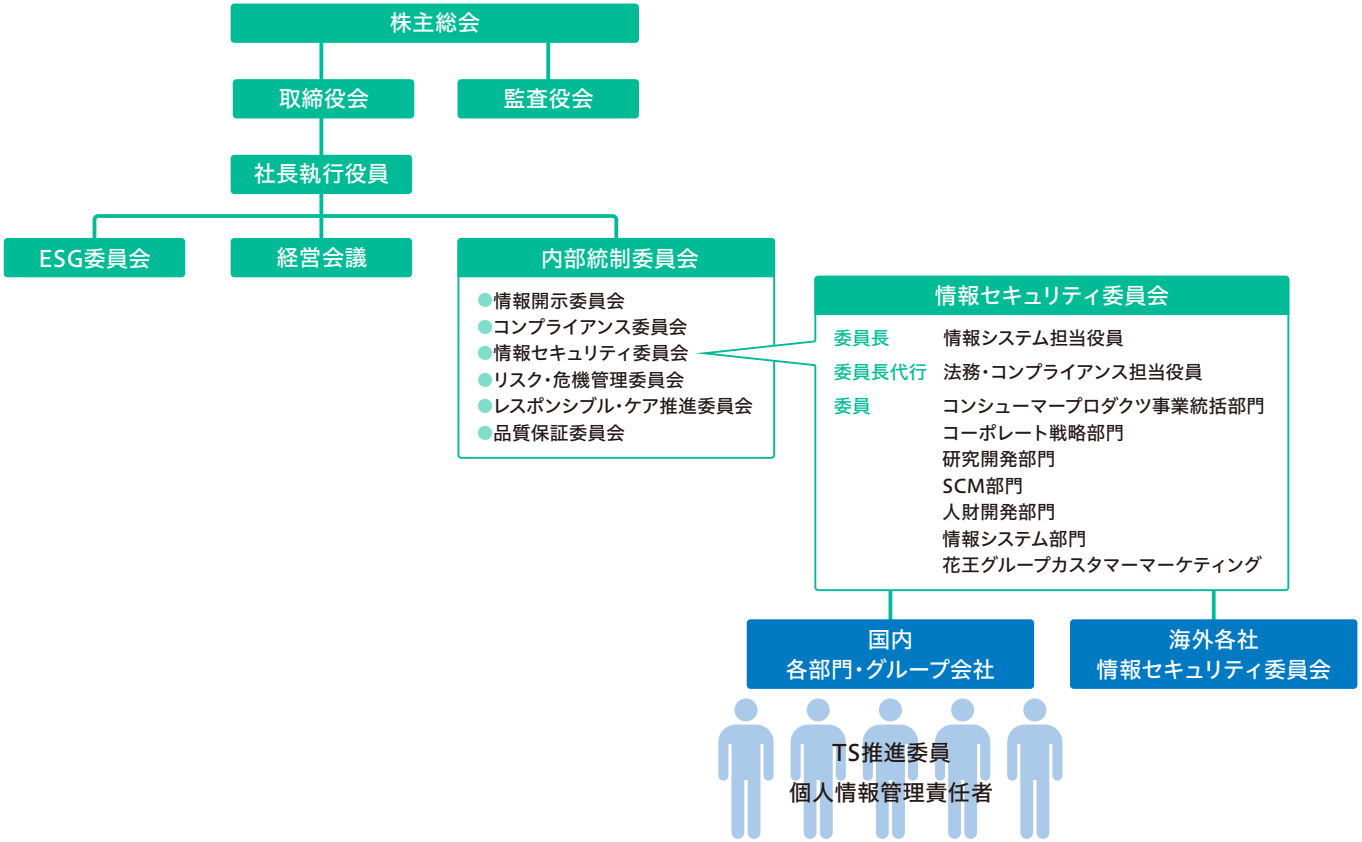
海外では、各社の経営会議メンバーがISCを構成し、日本のISCの傘下に海外の各ISCを配置する形になっています。活動は日本と同様に四半期単位のPDCAサイクルによる活動で、3月には日本のISCへレポートの提出を義務付けています。

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	花王中国グループ
	3	花王(台湾)
	4	花王プロフェッショナル・サロン・サービシーズ(台湾)
	5	花王(香港)
	6	花王プロフェッショナル・サロン・サービシーズ(香港)
	7	花王タイ
	8	花王コンシューマープロダクツ
	9	花王(インドネシア)
	10	花王(シンガポール)
	11	花王(マレーシア)
	12	花王(ベトナム)
	13	花王コンシューマープロダクツ(EMEA)
	14	花王コンシューマープロダクツ(アメリカ)
ケミカル	15	花王ペナングループ
	16	ピリピナス花王
	17	花王インドネシア化学
	18	花王コーポレーション(スペイン)
	19	ドイツ花王化学
	20	キミ花王
	21	花王チミグラフ
	22	花王ケミカルスアメリカス
	23	花王コリンズ
カネボウ	24	台灣カネボウ化粧品
	25	タイカネボウ化粧品
	26	カネボウコスメティックスマレーシア
	27	カネボウコスメティックスコリア
	28	カネボウコスメティックスロシア

情報セキュリティ 102-20,103-2

情報セキュリティの管理体制



※2020年12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	全員を対象に行なうこと。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？ ・従業員を部門ごとにサンプリングして回答者を選定 ・マネージャ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・誤送信による漏洩や情報機器の盗難・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 102-20,103-2

インシデント対応体制

サイバー攻撃や情報漏洩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　・社員サービス部　・広報部 ・生活者CC　・MKプラットフォーム部 ・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 ・広報部：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：警視庁、IPA、JPCERT/CCからの通報管理	・各種の監視を行ない、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、事実確認を行ないCSIRTへ報告
ステークホルダー/ 外部関係機関	・取引先　・従業員　・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
情報セキュリティ委員会 (ISC：Information Security Committee) 緊急対策会議	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	・対応策公表 ・注意喚起公表 ・再発防止策公表 ・問合せ対応等検討準備
SOC (Security Operation Center)	・モニタリング ・従業員から通報 ・外部から通報 ・SNS書込み	・継続分析 ・原因調査	・対応策公表 ・注意喚起公表 ・再発防止策公表 ・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 ・被害届の提出 ・情報共有

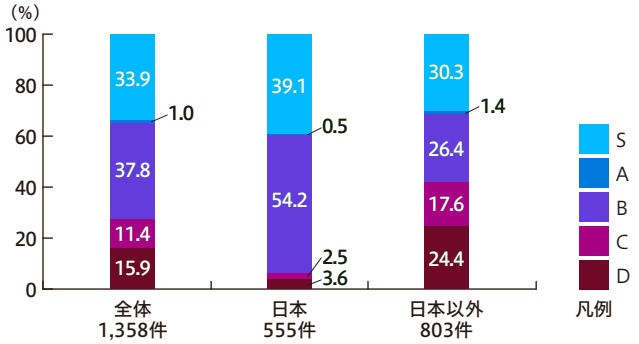
情報セキュリティ 103-3

ウェブサイトの脆弱性診断

花王のウェブサイトの脆弱性診断を行ない、サイバー攻撃に利用されるような未対応な脆弱性が存在しないか確認し、存在した場合はいち早く問題を解決しています。たとえば、サポートを終了したソフトの更新といった対応で解決しています。

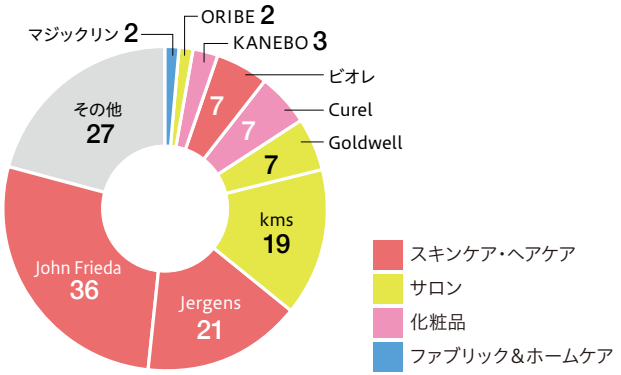
欧米サロン系ブランドを中心に改善傾向が見られます。

ウェブサイトの脆弱性診断（2020年）



レベル	優先度	脆弱性例	想定リスク
S	なし	問題検出なし	
A	参考	サーバ証明書の設定不備	利用者のウェブサイトに対する不信感 ウェブサイトのレピュテーション低下
B	低	不要なポートの開放	攻撃に利用される危険性
		プロダクトバージョン情報の露呈	攻撃の有益な情報として利用
		SSL暗号化設定の不備	利用者の通信を盗聴
C	中	メンテナンスポートの開放	攻撃を受ける可能性の増加
D	高	危険性の高い脆弱性が報告されているプロダクトの利用	プロダクト脆弱性の悪用
		サポート終了したプロダクトの利用	

対応したブランド



対応したドメイン

ドメイン	ランクC/D数	国・地域
ca	6	カナダ
nl	4	オランダ
us	4	アメリカ
org	3	—
kr	3	韓国
cm	3	カメルーン
eu	3	EU
br	2	ブラジル
mobi	2	—
be	2	ベルギー
ch	2	スイス
nz	2	ニュージーランド
dk	2	デンマーク
fi	2	フィンランド
no	2	ノルウェー
se	2	スウェーデン
ie	1	アイルランド

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

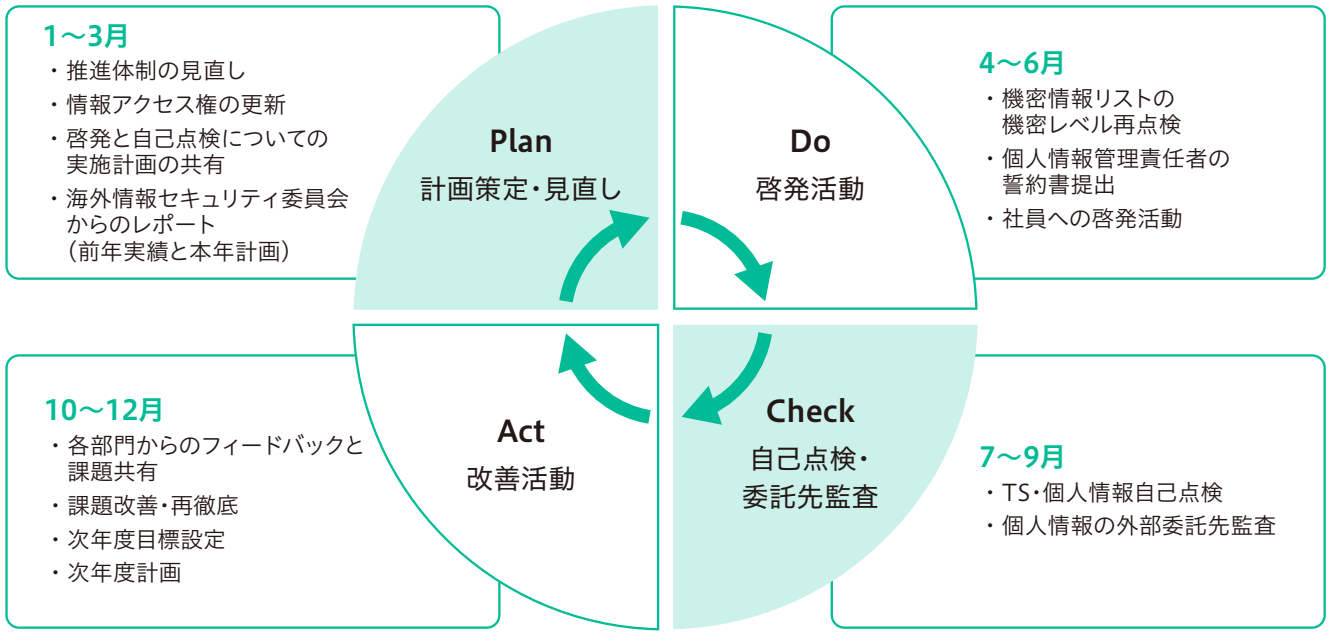
事業インパクト

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

2020年の実績

実績

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
- TS推進委員59名、個人情報管理責任者71名の見直し

・機密情報リストの見直し
- 日本の105部門・部署・関係会社で見直し

・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
・個人情報管理責任者の誓約書提出
・社員への啓発活動
- 日本の113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

・TS・個人情報自己点検
- 3月から在宅勤務が長期化したため、TS自己点検実施前に再度以下の設問を見直し

・在宅勤務で機密情報を保管
・在宅勤務で機密情報の印刷の必要性
- 日本の124部門・部署・関係会社でTS自己点検実施
- 日本の109部門・部署・関係会社で個人情報自己点検実施

・個人情報の外部委託先監査
- 190社に対して個人情報委託先書面監査を実施

Act：改善活動

・各部門へのフィードバックと課題共有
- 在宅勤務や外出自粛・飲食店の営業自粛の効果でTS・個人情報の事故は半減
- 在宅勤務によるメールの誤送信、郵便の誤送付が増加

・課題改善・再徹底・次年度目標設定
- 在宅勤務での機密情報管理の徹底
- メールや郵送時の宛先間違いの防止

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、「問合せ窓口」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。

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行ない、活動のレポートを年1回3月に提出するようにしました。今後、情報開示できるように海外での活動を取りまとめていきます。

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

日本の情報セキュリティ委員会（ISC）活動目標策定

2020年のISC活動目標を以下のように策定し実施しました。

①海外各社へISCの展開
・日本へのレポート提出（PDCAサイクルの活動等）（3月）
→23のISCから提出
・適時の注意喚起発信
→一部のオンライン会議ツールについて注意喚起実施（4月）
②個人情報管理強化
・海外各社に個人情報管理ツールの導入
→8月にEUで本稼働
③各国・地域の個人情報保護法対応の確認（CCPA等）
→海外法対応で新たな活動開始
④インシデント発生時に復旧計画の整備
→4月にインシデント発生時に復旧実施済
⑤PDCAサイクルによるTS・個人情報保護推進活動の実施
→11月TS・個人情報保護推進会議で改善目標設定

第2四半期：啓発活動

オンライン会議ツールの注意喚起

新型コロナウイルス感染症拡大防止対策として、花王では多くの社員が在宅勤務に切り替わりました。それによりオンライン会議ツールの使用機会が増えましたが、一部のオンライン会議ツールにセキュリティ上の問題があることが判明し、情報の漏洩リスクやPCへの不正アクセスの可能性があることから、社員へ使用を禁止する注意喚起を行ないました。後にソフトウエアアップデートでセキュリティリスクが解消された時点で利用禁止を解除しています。

このように、世の中で起こっている事象にも注意を払い、花王のセキュリティを守る活動を行なっています。

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。2020年は7月21日から8月21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。2020年11月16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。

改善目標は、「在宅勤務での機密情報管理の徹底」と「メールや郵送時の宛先間違いの防止」と設定しました。機密情報の取扱いについて日本は「花王機密情報取扱いガイドライン」、海外は「Global Trade Secret Regulation」という規定があり、これに基づいて機密情報を管理しています。

在宅勤務でオフィスの外で勤務する場合でも規程を遵守することが求められます。また、オフィスであれば複数メンバーでチェックすることもできますが、在宅勤務では一人で業務を行なう場面が増加します。そのような場合こそ、単純ミスを防ぐために再確認等の防止策が求められます。

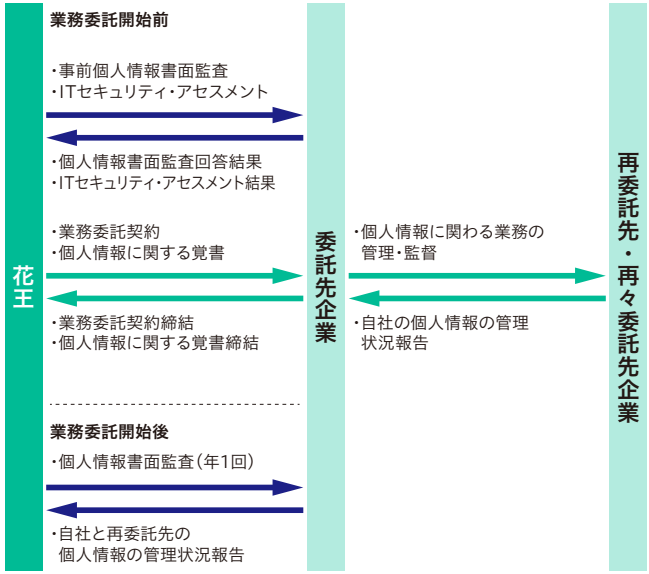
情報セキュリティ 103-2,404-2

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。2020は190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3四半期：アナウンス

在宅勤務における印刷ルールの制定

2020年3月から在宅勤務における印刷ルールについて検討していましたが、5月の緊急事態宣言解除で出社可能となったために社内へのアナウンスを停止していました。しかし、また7月中旬にコロナ感染者が拡大したことで在宅勤務へ再度シフトしたため、8月に在宅勤務での印刷を部門判断で許可するアナウンスを行ないました。これにより、印刷のためだけに出社するような事態を回避し、社員の感染リスクを低減しました。

第4四半期：改善活動

「第27回TS・個人情報保護推進会議」を開催

2020年11月16日に「第27回TS・個人情報保護推進会議」を開催しました。コロナ禍での開催ということで、初めての全面的なオンライン会議での開催となりました。例年は外部の講師を招いて機密情報・個人情報・セキュリティに関する講演を行ない、各部門での啓発活動のトピックスに活用していました。今回は、警視庁やIPAといったセキュリティに関わる組織が作成している啓発動画を各自で鑑賞してもらい、ポイントを確認するという試みで行ないました。続いて、2020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。