

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

花王では事業・リージョン(または国・地域)別に30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活動を展開しています。

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

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のものとなっています。社会基盤のITに障がい起きた場合、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となります。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仕組みや体制

の構築とその維持になります。

また近年、個人情報EUのGDPRや各国の法律により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。

「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、情報漏えいによる企業信頼の失墜は大きなリスクです。

「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。

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。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。

貢献するSDGs



情報セキュリティ 102-43, 404-2

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」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。2021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/

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、

- ①TS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

を行なっています。2021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、改善活動を実施しています。

海外では各ISCが啓発や自己点検の実施計画を作成・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／エンゲージメント

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2021年には、花王から委託先のロジスティクス会社(アジア5社、欧米6社)に対しセキュリティに関する質問状を送付し、得た回答に対して必要な場合は改善要求を実施し、改善を求めました。

国内の個人情報

業務委託先179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、委託先の監督を行ないました。

ウェブサイトの脆弱性診断

国内外のグループ会社が運営する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ました。脆弱性が存在した場合はソフトの更新で対応しました。欧米サロン系ブランドを中心に改善が図られました。

情報セキュリティ 102-20

体制

情報セキュリティの管理体制

日本のISCは内部統制委員会の傘下の委員会として、経営目標達成のために、機密情報・個人情報等の情報資産(ハードウェア、ソフトウェア、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なっています。

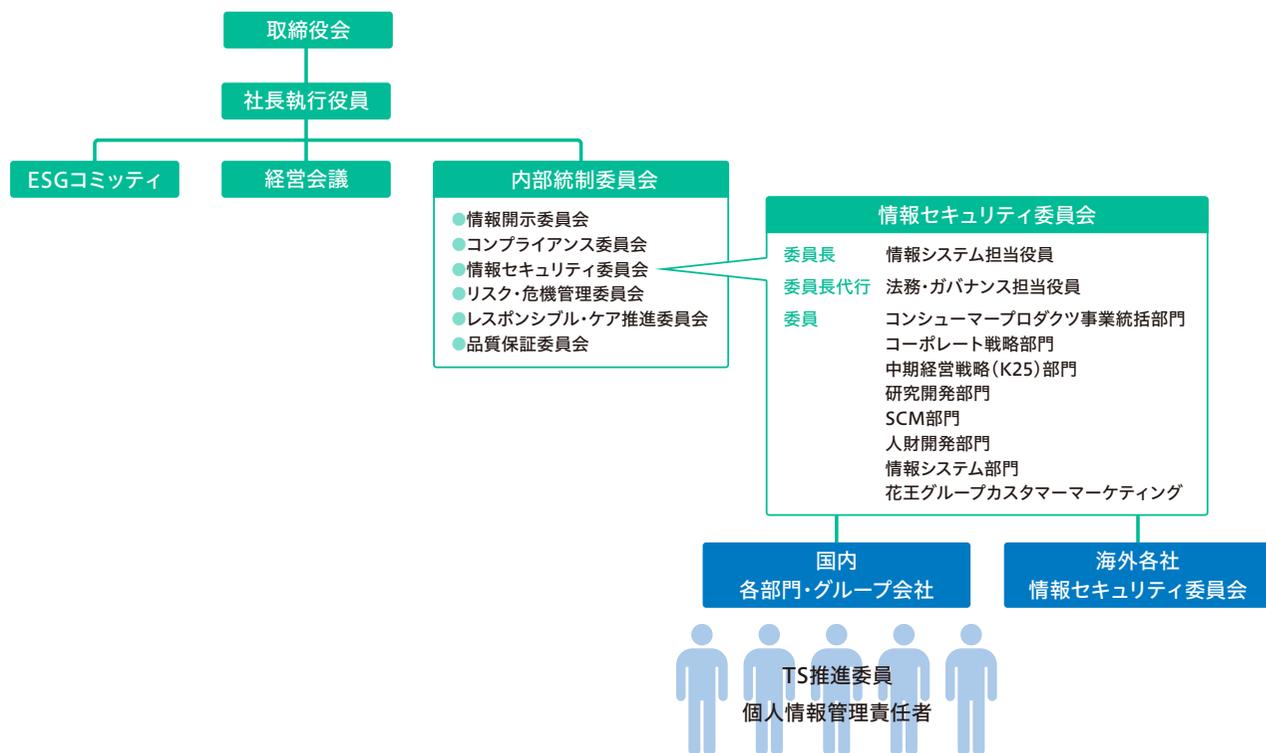
日本では、ISC委員長と委員長代行に執行役員を配置し、人財開発、情報システム、マーケティング、研究開発、知的財産、生産技術、法務・ガバナンス等の多様な部門から委員と事務局を選出し、多様な観点で方針の決定やルールの整備、管理体制の整備、啓発活動の実施を推進しています。

ISCは内部統制委員会に活動報告しており、内部統制委員会が四半期ごとに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。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ヘレポートの提出を義務づけています。

情報セキュリティの管理体制



※2021年12月現在

情報セキュリティ 102-20

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 コンシューマープロダクツ	1	花王(株)
	2	花王(台湾)
	3	花王プロフェッショナル・サロン・サービスズ(台湾)
	4	花王(香港)
	5	花王プロフェッショナル・サロン・サービスズ(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)
ケミカル	12	花王コンシューマープロダクツ(アメリカ)
	13	花王ベナングループ
	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？ ・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 102-20

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 ・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・レスポンス・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			・報告 ・対応策・公表・再発防止策等承認
ISC (CSIRT)			・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			・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			・注意喚起・公表、被害届、情報共有

フロー詳細: 検知 → 即時 → 把握 (第一報当日) → 対応 (翌日以降)

情報セキュリティ

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

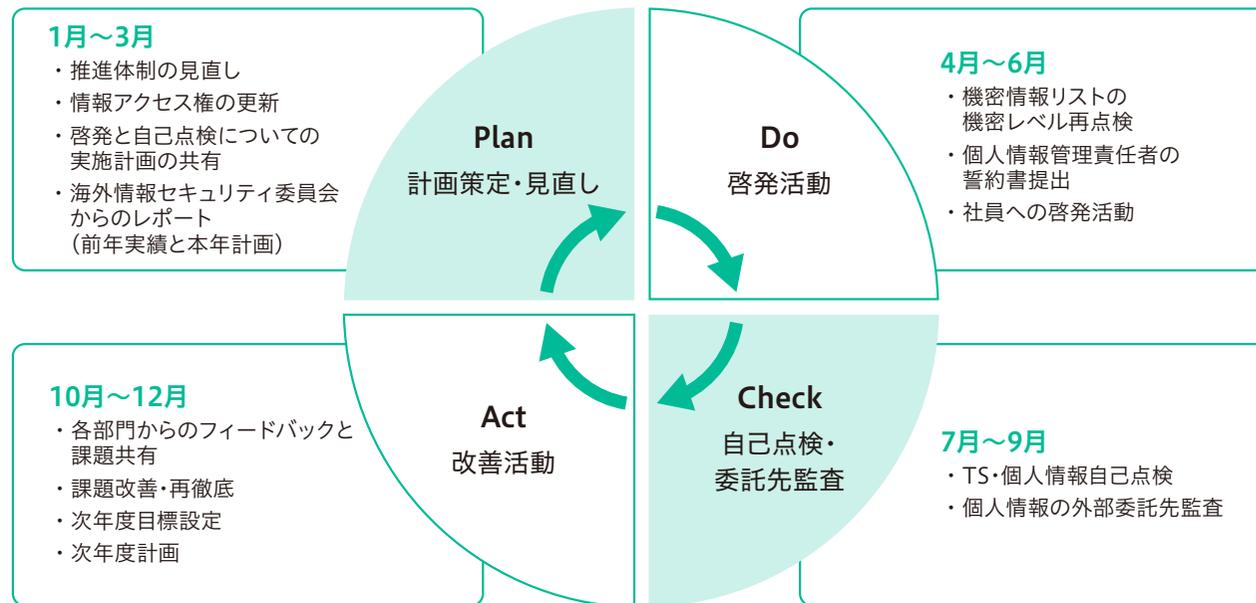
事業インパクト

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、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。

社会インパクト

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

2021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208名、個人情報管理責任者192名の見直し
- ・機密情報リストの見直し
- 日本の109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108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123部門・部署・関係会社でTS自己点検実施
- 日本の97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
- 179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
- ・課題改善・再徹底・次年度目標設定

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。

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、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、海外の地域、会社グループ、個社と規模は異なりますが、海外に29のISCを設置しました。海外のISCから年1回3月に活動のレポートが提出されます。

情報セキュリティ

具体的な取り組み

第1四半期：計画策定・見直し

日本のISC 活動目標策定

2021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 ISC 活動

- ・3月、日本へのレポート提出(PDCA サイクルの活動等)
- ・サードパーティロジスティクスのセキュリティ評価

②サイバー保険加入

- ・2021年4月1日加入。カバー範囲は花王グループ全体。
- ・補償内容：危機管理対応費用、第三者賠償責任費用、海外各国における当局対応費用、自社の経済的被害、事業中断にかかる費用

③各国の個人情報保護法対応の確認(GDPR/CCPA等)

- ・GDPR：2018年のCookie 対応方法の変更
- ・改正個人情報保護法施行対応として個人情報管理強化

④セキュリティ対策の強化

- ・セキュリティ戦略ロードマップ作成
- ・セキュリティ戦略ロードマップに沿った対策実施

⑤PDCA サイクルによる活動

- ・啓発資料・自主パトロール設問の見直し
- ・啓発活動(各部門)実施
- ・自主パトロール・個人情報委託先監査の実施
- ・TS・個人情報保護推進会議開催(11月15日)

第2四半期：啓発活動

各部門・関係会社で啓発活動実施

国内では社内ポータルサイトに規程や一般的なセキュリティの啓発資料が準備されています。また、前年11月に実施したTS・個人情報保護推進会議で使用した啓発用動画やTS・個人情報事故、自主パトロールフィードバックの資料を利用して各部門で啓発活動を実施しています。

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。2021年は8月2日から9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。

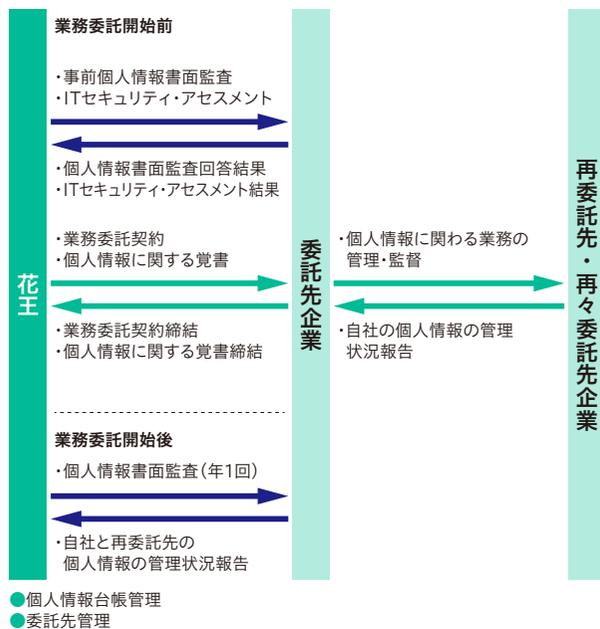
個人情報委託先監査

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することが、委託契約の締結の条件となります。

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。2021年は179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、個人情報取り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。

情報セキュリティ 404-2

個人情報に関わる業務の委託と委託先監査



第4四半期:改善活動

「第28回TS・個人情報保護推進会議」を開催

2021年11月15日に「第28回TS・個人情報保護推進会議」を開催しました。リアル会議とオンライン会議の併用での開催となり、321名の参加となりました。昨年に引き続き、情報処理推進機構(IPA)が作成している啓発動画を視聴した上で、花王の状況を解説するという形で啓発を実施しました。

続いて、2021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。

改善目標は、「啓発活動の着実な実施」と「機密情報の紙(書類)での持出原則禁止」、「個人情報専用サーバ利用時の誓約書の毎年の取り直し」を設定しました。「個人情報専用サーバ利用時の誓約書の毎年の取り直し」は個人情報の取り扱いの注意喚起の意味もあり、徹底するためにMicrosoftのFormsを使うことを検討しています。