

楽天モバイル株式会社 業務委託先における情報管理について

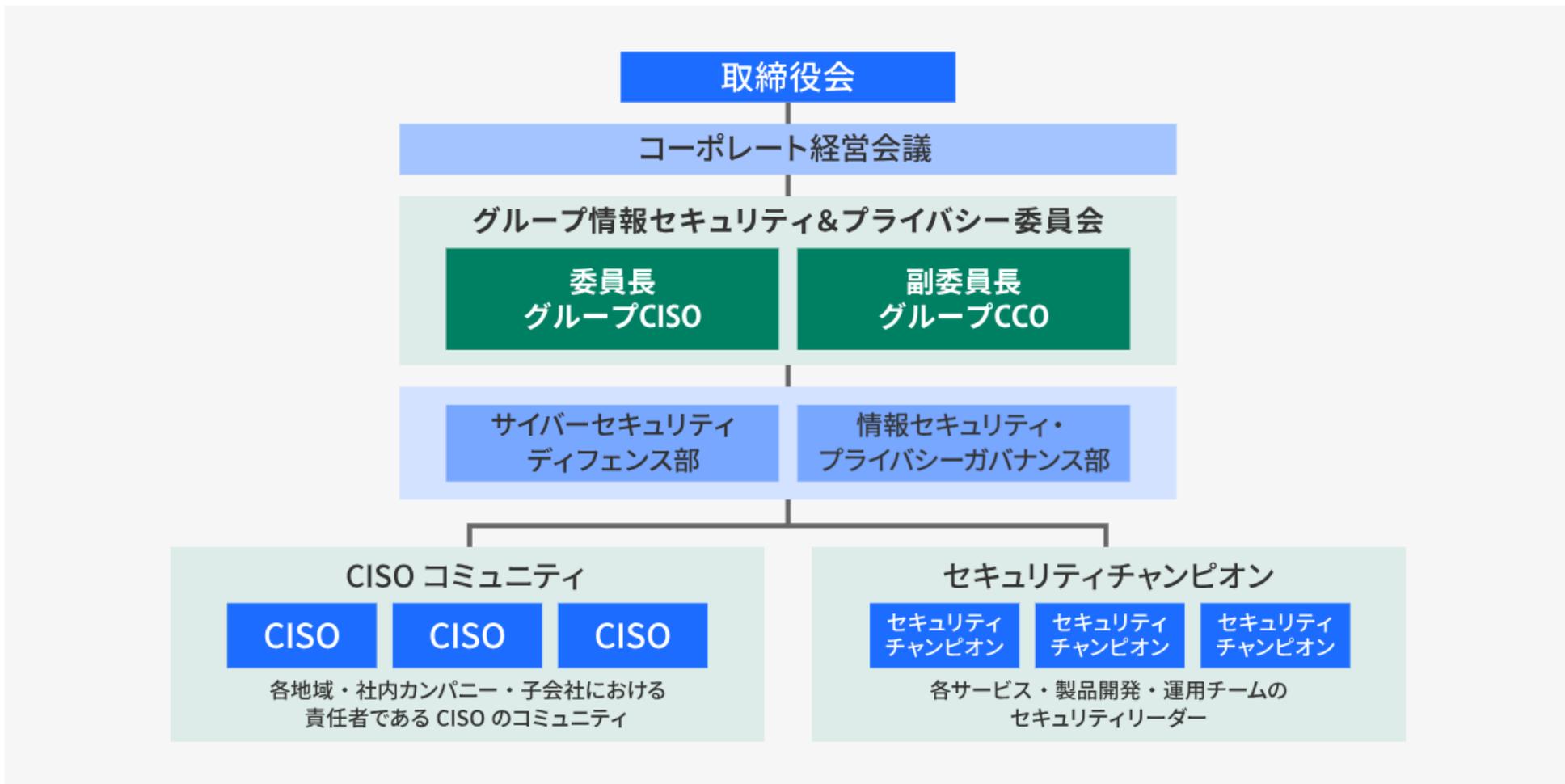
2024年11月25日

楽天モバイル株式会社

楽天グループの情報セキュリティガバナンスについて

楽天グループにおける情報セキュリティガバナンス

楽天グループは、グループ全体の情報セキュリティレベルを担保するため、楽天グループ本社の専任部門によるガバナンス構造を運営している。グループ共通のセキュリティポリシーやソリューションはこの構造を元に導入・適用される。



楽天グループのISMS

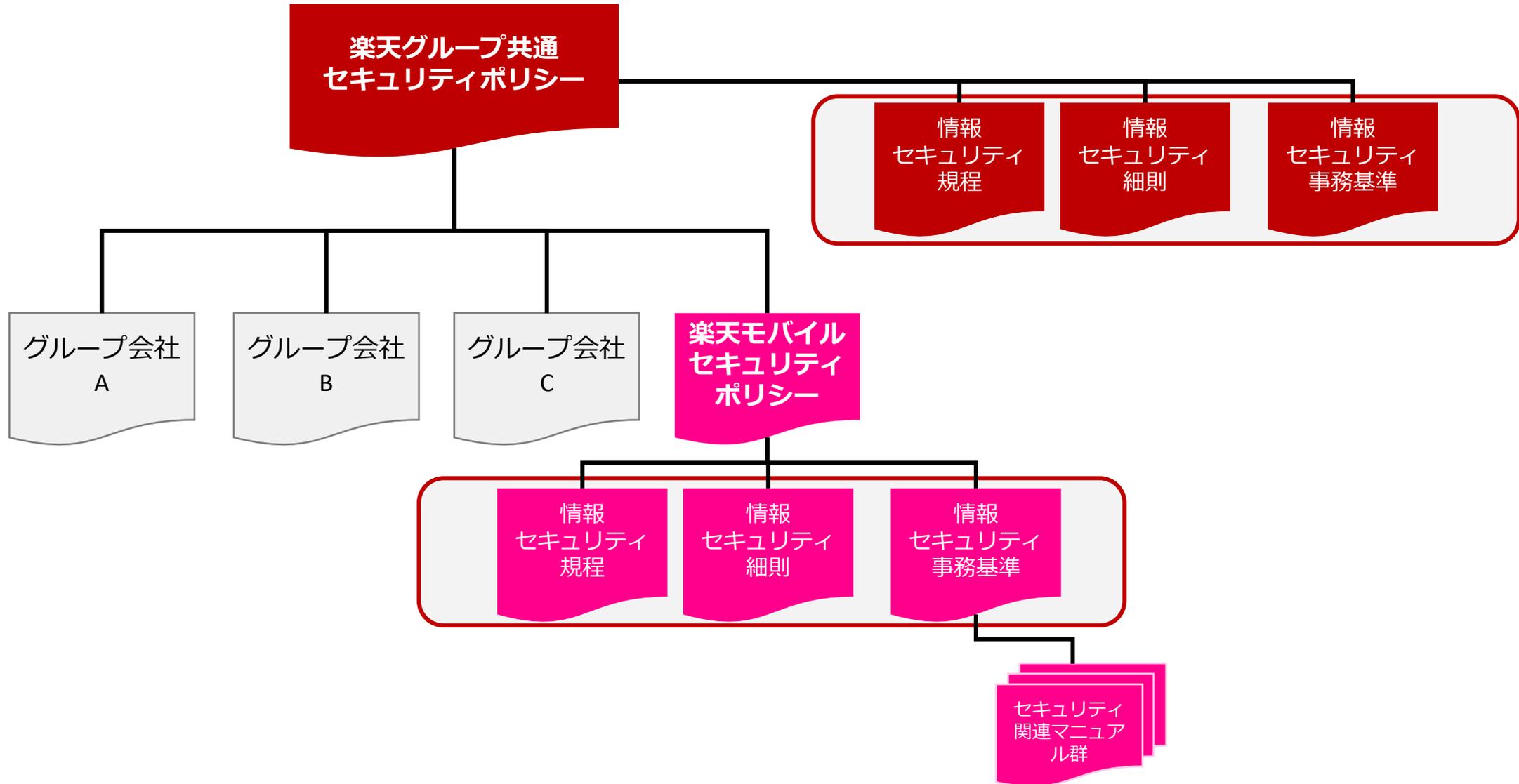
2024年11月時点でグループ内45社が共通の監査を通じてISMS認証を取得している。個人情報に関する安全管理策やオフィスの物理的安全管理策もグループ共通の要件が適用されている。



- 楽天グループ株式会社
- リンクシェア・ジャパン株式会社
- ターゲット株式会社
- 楽天ソシオビジネス株式会社
- 株式会社楽天野球団
- 楽天トラベルサービス株式会社
- 楽天ANAトラベルオンライン株式会社
- 楽天コミュニケーションズ株式会社
- 楽天インサイト株式会社
- 楽天カード株式会社
- 競馬モール株式会社
- 楽天チケット株式会社
- 楽天Edy株式会社
- 楽天モバイル株式会社
- 楽天モバイルエンジニアリング株式会社
- 楽天カスタマーサービス株式会社
- 楽天スクリーム株式会社
- 楽天ペイメント株式会社
- 楽天ウォレット株式会社
- 楽天ヴィッセル神戸株式会社
- 楽天エナジー株式会社
- 楽天カー株式会社
- 株式会社ケイドリームス
- ハンプリード株式会社
- 楽天ビジネスサポート株式会社
- 楽天ドローン株式会社
- 楽天データソリューションズ株式会社
- 楽天モバイルインフラソリューション株式会社
- 楽天ステイ株式会社
- 楽天トータルソリューションズ株式会社
- Rakuten India Enterprise Private Limited
- Rakuten Asia Pte. Ltd
- Rakuten Europe S.à.r.l.
- Rakuten France S.A.S.
- Rakuten TV Europe, S.L.U.
- Rakuten Travel Xchange Pte. Ltd
- Rakuten Symphony INC.
- Rakuten Symphony India Private Limited
- Rakuten Mobile USA LLC
- Rakuten Symphony Singapore Pte. Ltd.
- Rakuten Symphony Deutschland GmbH
- Rakuten Symphony Korea, Inc.
- Rakuten International Commercial Bank Co., Ltd.
- Rakuten Travel Singapore Pte. Ltd
- Rakuten USA, Inc.

楽天グループのセキュリティポリシー

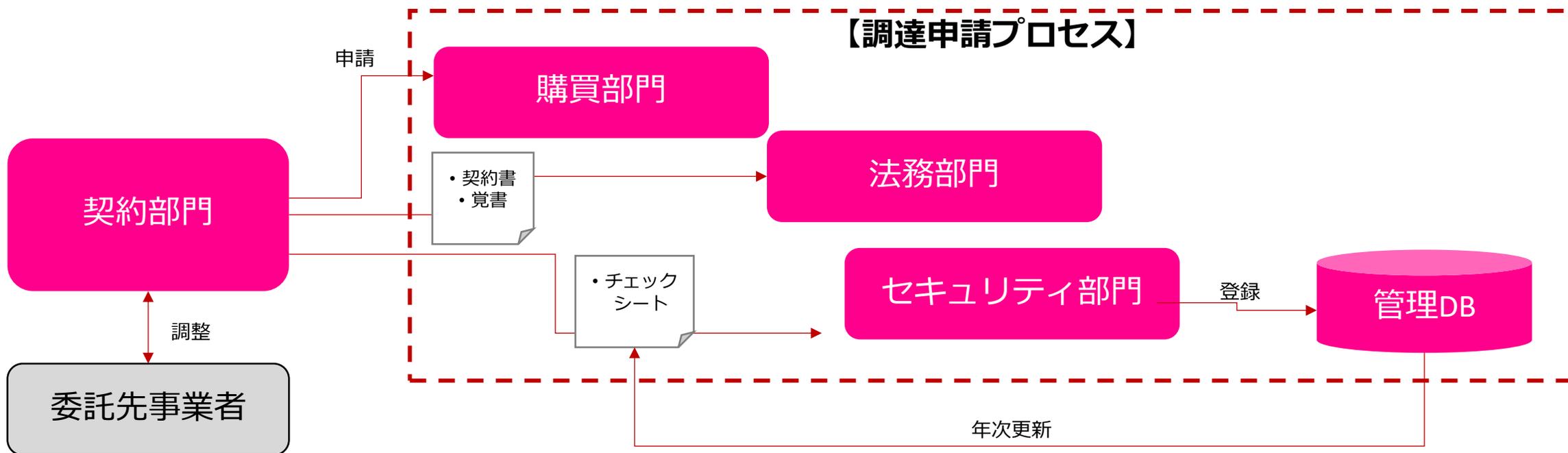
グループ本社のセキュリティ主管部門が策定する上位ポリシーをベースとして、グループ会社にてより詳細なマニュアルを策定。



楽天モバイル株式会社の業務委託先セキュリティ管理について

楽天モバイル株式会社における業務委託先セキュリティ管理の概略

- 法務部門による契約内容レビュー後、情報セキュリティ部門によるセキュリティ審査を実施
- セキュリティ審査は、「**情報セキュリティに係る業務委託先審査申請マニュアル**」に基づいて実施される
- 審査対象は機密情報を取り扱う委託業務およびクラウドサービス
- 委託契約単位（**※委託先事業者単位ではない**）で委託先からチェックシートを取得し、業務内容をレビュー。チェックシートやレビュー内容一式を収容する委託先管理台帳（データベース）を運用。部門長承認をもって契約締結に進む
- 審査内容は契約単位で定期棚卸も実施（年次）



委託先審査の流れ

1. 導入準備

2. 委託審査

3. 委託管理



委託審査は、委託先等へ提供する情報資産や業務環境等に基づいて実施します。

想定に誤りがある場合審査時間の長期化に繋がるため、事前に各要件を整理したうえで準備を進めてください。

詳細は[業務委託先審査申請プロセスマニュアル](#)を参照ください。

審査日数は内容により変動します(関連部署での確認が必要な場合は追加日数を要する場合があります)。

審査完了後も、契約が終了するまでは情報セキュリティレベルが維持されていることを定期的に確認する必要があります。

委託先事業者選定のポイント

マニュアルに以下文言を提示

- 信頼できる企業の選定 ISO27001認証などの情報セキュリティ関連の認証を取得している企業の場合は、セキュリティ面での信頼性が高い企業であることから、審査が比較的スムーズに進行します。一方で、未取得の企業の場合、審査の際に情報セキュリティに関する是正措置が必要になるケースがあり、審査に時間を要する傾向にあります。委託先選定の際には、情報セキュリティ系の認証取得状況を参考に選定することをお勧めします。
- 再委託は、委託元である当社と直接の契約関係にないため委託先以上に監督が難しく、さらに再々委託先にも機密情報を預託される可能性があります。問題発生時の原因究明も困難になりやすいことから、再委託の有無を事前に委託先に確認のうえ、取り扱う情報の重要度を踏まえて判断してください。なお、再委託をする場合、追加の覚書の締結など別途手続きが必要になる場合があります。

クラウドサービスの選定におけるポイント

マニュアルに以下文言を提示。併せてクラウドサービス用チェックシートにて実態を把握する方式。

■ 外部のクラウドサービス等導入時留意事項

- 契約先の提供するサービスレベル（バックアップ、冗長化対策等の可用性・完全性に関する項目）が当社において妥当であること
- 契約先が、情報セキュリティ対策（暗号化、アクセス制限等）に関する事項を明文化した情報セキュリティポリシーを当社に提供すること。また、そのポリシーは当社の情報セキュリティの基準を満たしており、当社がその内容に合意すること
- 契約先は、当社の情報に対する当社の所有権を確認した上で、サービス提供のためにのみ利用し、情報の機密性を維持すること

情報セキュリティチェックシート

委託作業用とクラウド用の2種を運用している。委託作業に携わる事業者がクラウドシステムを利用する場合は両様式への回答が必須となる。

<委託作業型>

- ①全社的な情報セキュリティ体制について（確認項目：20項目）
- ②作業場所・委託業務に関する情報セキュリティについて（確認項目：9項目）
- ③機密レベルの高い情報を取り扱う場合のセキュリティについて（確認項目：14項目）

<クラウドサービス型>

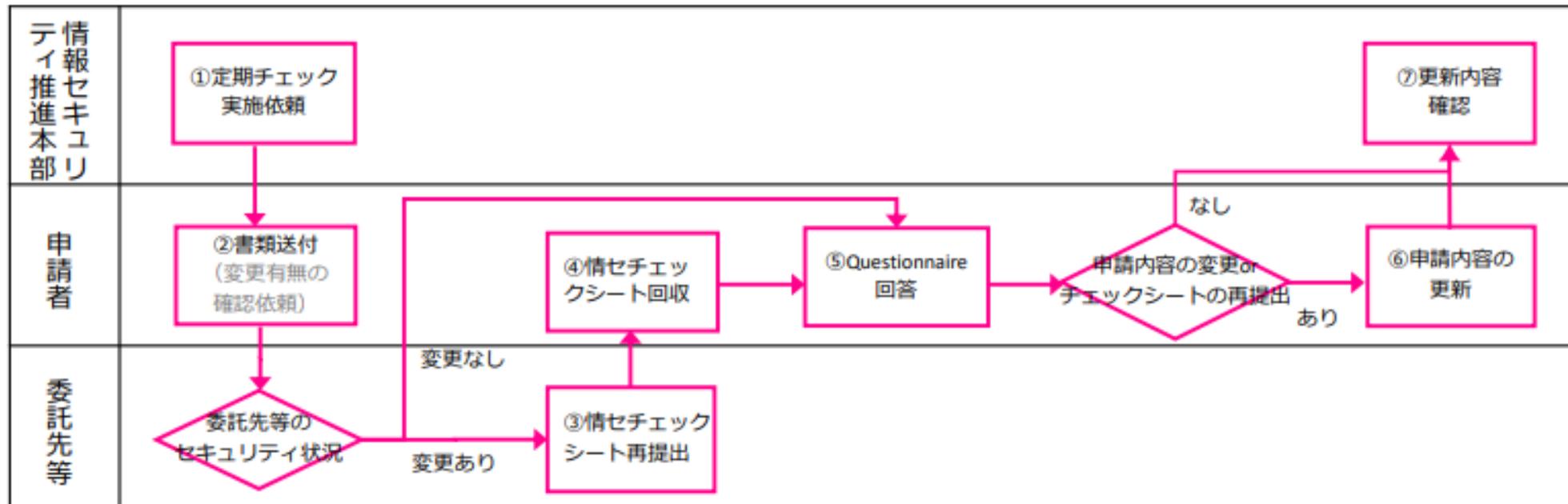
- ①情報セキュリティおよび個人情報保護管理体制（確認項目：9項目）
- ②サードパーティー管理（確認項目：4項目）
- ③アクセス制御（確認項目：6項目）
- ④アプリケーションセキュリティ（確認項目：2項目）
- ⑤運用セキュリティ（確認項目：10項目）
- ⑥データ管理（確認項目：4項目）
- ⑦情報セキュリティインシデント対応（確認項目：3項目）
- ⑧ネットワークセキュリティ（確認項目：4項目）
- ⑨物理セキュリティ（確認項目：8項目）
- ⑩コンプライアンス（確認項目：3項目）

定期チェックの運用

契約中の案件に対し、1年に1回で定期レビューを実施し、情報セキュリティレベルが維持されていることを確認。

<確認の観点>

- 委託先等から提供される報告及び記録をもとに、契約内容のうちSLAの達成状況や情報セキュリティに係る事項が履行されていることを確認
- 契約内容のうち情報セキュリティに係る事項が履行されていないことを確認した場合、委託先等に是正措置を要求する
- 当社の情報資産に関わるセキュリティインシデントが発生した場合、委託先等に被害、原因分析及び是正措置の報告を要求する



委託終了時の対応

委託終了時における情報セキュリティ観点の対応事項についてマニュアルに掲示。

- 委託業務等の発注やクラウドサービスの利用がなくなり、該当案件を終了ステータスとしたい場合は、以下の対応を実施してください
 - ① 委託先等に渡していたConfidential以上の情報の破棄（返却）を依頼し破棄証明書の写しを情報セキュリティ推進本部に提出してください
 - ② 委託先等が当社のサーバ及びシステムを利用している場合は、契約関係の終了に伴い委託先等のアクセス権及びパスワードを直ちに削除又は破棄してください

Rakuten Mobile