# 情報セキュリティ

## 基本的な考え方

考え方 方針

TOPPANグループは、グローバルな社会課題を解決するリーディングカンパニーを目指し、事業に必要な情報やシステムを適切かつ安全に管理することが経営上の重要課題であることを認識し、TOPPANグループを挙げて情報セキュリティ管理およびサイバーセキュリティ対策に取り組んでいます。

IoTの高度化やデジタル化の急速な進展を背景に、サイバー攻撃の脅威が高まっており、機密情報や個人情報を含む情報資産の漏えいだけでなく、事業そのものの継続までが脅かされるようになっています。

こうした中で、DXの利活用を通じて企業価値を創造し、お客さまや社会の信頼に応えるため、TOPPANグループは「TOPPANグループ情報セキュリティ方針」や「個人情報保護方針」を掲げ、グループ一丸となり、技術面・運用面での対応を徹底しています。全国に展開するセキュリティエリアでの個人情報取り扱いの徹底やサイバー攻撃に対するツールや仕組みの導入を積極的に進めています。

TOPPANグループ情報セキュリティ基本方針 >

https://www.holdings.toppan.com/ja/about-us/our-corporate-approach/security-information.html

個人情報保護方針 >

https://www.holdings.toppan.com/ja/privacy.html

### TOPPANグループ情報セキュリティ基本方針

私たちTOPPANグループは、情報コミュニケーション産業として、事業に必要な情報の管理が、お客さまの信頼に応え、TOPPANグループの永続的な発展を図るために、経営上の重要課題であることを認識し、TOPPANグループを挙げて情報セキュリティ管理に取り組みます。

1. 私たちは、法と社会秩序を遵守のうえ、社内の規程類に則り、当社の事業に必要な情報を適切に管理します。
2. 私たちは、情報を収集するにあたっては、正当な目的および方法をもってこれを行います。
3. 私たちは、お客さまより預託を受けた情報について、お客さまの信頼に応えるべく、安全に情報を管理します。
4. 私たちは、私たちの取り扱う情報資産について、不正なアクセスまたは滅失、毀損、改ざん、漏えい等の危険を深く認識し、必要かつ合理的な安全対策を講ずるとともに、問題が発生した場合は、適切かつ速やかに対処し是正します。
5. 私たちは、情報セキュリティマネジメントシステムを構築、運用、維持し、さらに継続的に改善を図ります。

制定日　平成13年4月1日
最終改定日　令和元年6月27日

凸版印刷株式会社
代表取締役社長　麿 秀晴

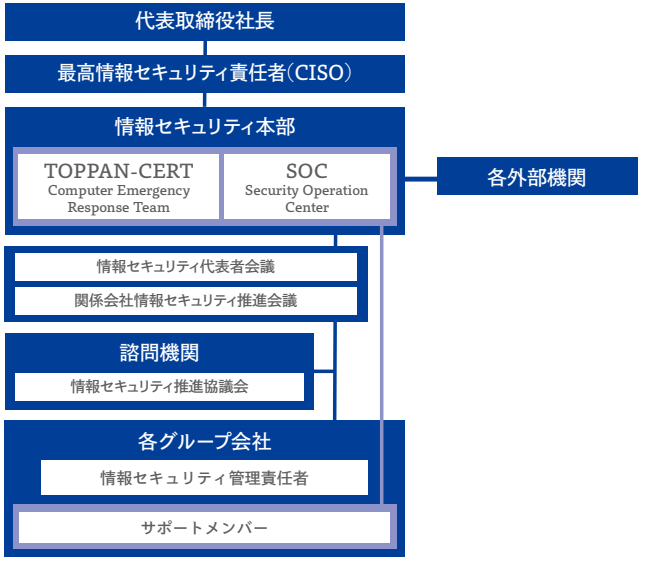
## 推進体制

推進体制

TOPPANグループでは、情報セキュリティ本部を設置し、ガバナンスならびに技術的に対応するとともに、組織横断的なサイバー対応の専門チームを設けて、グループ会社を統括し、外部機関とも連携を図りながら情報セキュリティ管理を推進しています。また、情報セキュリティ本部担当役員を最高情報セキュリティ責任者(CISO)として任命しています。

グループ会社には情報セキュリティ管理責任者を置き、情報セキュリティ本部による統制のもとで各組織のセキュリティ管理を推進しています。

### 情報セキュリティの組織管理体制



# 情報セキュリティ管理体制

推進体制

## 情報セキュリティマネジメント

最高情報セキュリティ責任者のもと、情報セキュリティ本部が、情報セキュリティに関する全体計画の策定、規程の整備・見直しなどを行い、グループ会社との定期的な会議体を設けて、情報セキュリティに関する方針や施策の共有を図っています。

また、グループ会社に対しては、定期的な監査を実施し、マネジメントの状況確認と是正改善を行っています。

さらに、これらの活動については、最高情報セキュリティ責任者に定期的な報告を行うとともに、万一、インシデントが発生した場合にも、最高情報セキュリティ責任者に適宜報告を行い、迅速にインシデントに対応する体制となっています。

## リモートワークへの対応

リモートワークに対応した情報セキュリティルールの見直し、およびコミュニケーションツールの利用基準を策定し、事務所外での業務を安全に遂行するための環境を整備しています。また、リモートワーク中の不審メール受信やウイルス感染時も、迅速に通報を行うことのできる仕組みを導入しています。

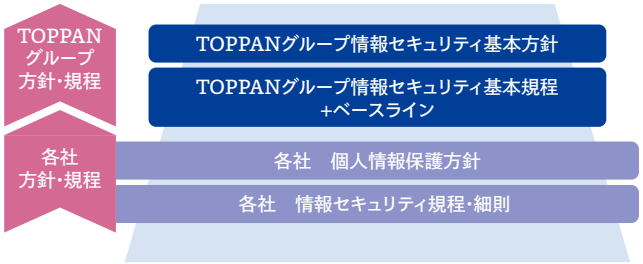
情報セキュリティ管理に関しても、内部監査などの各種監査業務にリモート形式を取り入れて実施しています。

## セキュリティガバナンス強化のための対応

TOPPANグループのガバナンスを支える規程体系は、ISO/IEC27000をベースにJIS Q 15000に準拠したものとしています。

また、近年のサイバーセキュリティ、データ利活用、IoT、グローバル化といった要求に対応し、海外も含めたTOPPANグループ全体としてのガバナンス強化を目的として、TOPPANグループ情報セキュリティ基本規程ベースラインによるセキュリティ水準の評価を毎年実施するとともに、改善計画の策定とその実施状況をモニタリングすることで、TOPPANグループ各社におけるセキュリティ水準の向上を図っています。

### 情報セキュリティ規程体系




# 各種法規制・規範への対応

活動実績・データ

日本の個人情報や機密情報保護関連の法規制のみならず、TOPPANグループが展開している各国における、プライバシーや機密関連法規制への対応を実施しています。

## 改正個人情報保護法への対応

2022年4月の改正個人情報保護法への対応として、情報セキュリティ規程などの個人情報関係ルールの改定を行いました。また、個人情報保護委員会から開示されたガイドラインに従って、仮名加工情報および個人関連情報への対応、越境移転がある場合の本人への通知、インシデント発生時における報告対応を行っています。

## 個人情報とプライバシー保護に関する各国法規制への対応

高まりつつある個人情報保護とプライバシー意識の高揚に応じて、プライバシー保護に関する法規制が制定されていますが、TOPPANグループが展開する各国や地域における当該法規制に関する、情報収拾や調査を通じて、法規制への適切な対応を実施しています。

## プライバシーマークおよびISMSへの対応

情報セキュリティにかかわる認証として、プライバシーマークおよびISMS(情報セキュリティマネジメントシステム)を取得しています。

個人情報などお客さまの重要な情報を安全に取り扱うため、ルールの制定、環境の構築、要員の教育に取り組んでいます。

## マイナンバー制度への対応

従業員のマイナンバー取り扱い業務、およびお客さまによる顧客のマイナンバー収集を代行する業務などに対応するため、セキュリティエリアの基準に、個人情報保護委員会「特定個人情報の適正な取り扱いに関するガイドライン」に基づく安全管理措置を追加しました。

他の情報取り扱いと分離するため、独立したマイナンバー取り扱いルームを設け、専門チームによる認定監査を実施しています。

# 個人情報・機密情報保護の徹底

活動実績・データ

## セキュリティエリアの設置

TOPPANグループでは、個人情報(マイナンバー含む)の取り扱い、金銭的価値を有する証券印刷物の生産や取り扱い、その他機密指定案件の取り扱い業務は、入退室制限、独立したネットワーク環境など、内部不正や外部からの不正アクセス防止などの対策が施されたセキュリティエリアで行っています。

その結果、2022年度の情報の不正な持ち出しなどの事故は0件であり、今後も事故0件を継続することを目標としています。

**セキュリティエリアのある拠点とその数**
**(2023年3月31日現在)**


※ 個人情報を取り扱うセキュリティエリアの数

## セキュリティエリアの安全管理策

個人情報取り扱い業務および機密情報取り扱い業務については、セキュリティエリアの運用管理ルールに則った現場での日常的なチェックと、定期的な内部監査によって、セキュリティレベルの維持向上を図っています。

＜内部監査での運用管理のチェック＞

専門の監査員により、セキュリティエリアの設置・管理・運用の状況を定期的に監査し、結果を評価認定することで、運用管理レベルの維持と強化を図っています。

＜入退室管理＞

セキュリティエリアには、許可された人間のみが入退室可能な技術的対応(本人認証、共連れ防止策等)を施しています。

また、画像、映像、音声などを記録・通信する装置(カメラ、携帯電話、スマートフォン等)の持ち込みは禁止し、エリアの外に私物入れロッカー等を設置しています。

＜エリア内管理＞

セキュリティエリア内では、監視カメラを死角ができないように設置し、不正なデータ持ち出しに対するモニタリングが可能な対応をしています。

＜端末管理＞

また、セキュリティエリアで使用される端末には、原則として外部記憶媒体の接続を禁止するとともに、IDとパスワードに加えてその他要素も加えた二要素認証を適用したログインを行っています。

また、ログ管理システムに操作ログを収集・保管し解析することによって、不正が疑われる場合には監視センターより責任者へ連絡して確認を取る運用を行っています。


監視カメラ


入退管理

## サプライチェーンに対するセキュリティ管理

TOPPANグループでは、個人情報や機密情報の取り扱いを含む一部の業務をグループ会社や協力会社に委託したり、他社のクラウドサービスを活用したりして業務を行うことがあります。

その場合、これらの委託先が当社のセキュリティ基準を満たしていることを確実にするため、委託する業務内容や情報の種類に応じて、適切なセキュリティ対応を実施している外部委託先を認定する制度の導入やクラウドサービスの安全性確認を行い、サプライチェーンリスクの低減を図っています。

## 社内業務における情報資産の取り扱い対応

TOPPANグループでは、社内業務で取り扱う情報資産の機密性に応じて区分をつけ、情報資産の区分に応じた、保管、持ち出し、開示等に関するルールを規定し安全な情報資産の取り扱い対応を実施しています。

# サイバー攻撃に対する対策

活動実績・データ

サイバー攻撃は特に重大なリスクであると認識しており、セキュリティリスクの低減に向け様々な対応策を実施しています。

### PC内での不審な挙動を検知するためのツール（EDR:Endpoint Detection and Response）によるPC・サーバーへの対策

2019年度より導入を開始したEDRの展開を進め、社内の事務端末をはじめ、製造現場の端末やMac、サーバーへのEDR導入を完了しました。また、ネットワークログなどを組み合わせ、高度なウイルスを早期に検出・対処する体制を継続的に強化しています。

### クラウド利用リスクの低減のための可視化・統制サービスCASB（Cloud Access Security Broker）の活用

クラウドサービスの利用が進み、クラウド上で重要な情報を扱うことが増えてきたことを背景に、クラウドサービスをより安全に活用するためCASBサービスを2020年度より利用しています。クラウドサービスごとのリスクの把握やクラウドサービスのリスクの高い利用の検知と制限、安全な利用に活用しています。

### 脅威インテリジェンスとOSINT（Open Source INTellignce）の活用

TOPPANグループに対するサイバー攻撃の兆候や外部から見つけられる可能性のある脆弱性を早期に発見するため、脅威インテリジェンスや第三者評価の活用とOSINTの活動を継続しています。攻撃を受ける前に発見された問題に対処することで、サイバー攻撃リスクの低減を図っています。

2022年度からは個人情報・機密情報の委託先にも対象を広げ、サプライチェーンのセキュリティ強化にも努めています。

### Webサイトの脆弱性診断対応強化

Webサイトの脆弱性を狙ったサイバー攻撃の対策として、これまで脆弱性診断の運用を行ってきましたが、日々発生する新たな脆弱性に対応するために、定期的かつ自動的にネットワーク診断を行う脆弱性監視の運用や外部サービスによる脆弱性の検出を行っています。これにより、自社サービスの安全性向上に加え、より安全なサービスのお客さまへの提供につなげています。

2022年度は開発部門だけでなく営業・販促部門にも脆弱性対策に関する教育を実施し、企画・設計段階からのセキュリティの確保につなげています。

### 情報セキュリティにおける重大インシデント対応ガイドラインの制定

サイバー攻撃の脅威は世界的規模に拡大し、その悪質さ、巧妙さが想定外なだけでなく、瞬時にして甚大な被害に拡大することから、従来の事故対応の手法では対応し得ないものとなっています。

TOPPANグループでは、サイバー攻撃等による重大インシデントに対応するためのベースとなる「考え方」、「態勢」、「対応フロー」をガイドラインとしてまとめ、想定外の事象が発生し得るとの前提に立った対応力強化を図っています。

### 電子メール攻撃への対策

マルウェア「Emotet」や、取引先を装い金銭や特定情報をだまし取るビジネスメール詐欺などの電子メールを悪用した脅威に対し、AI分析や機械学習を活用して電子メールを検疫するサービスを2022年度に導入し、運用を開始しました。これにより、標的型攻撃による金銭や情報搾取、ウイルス感染のリスクを低減しています。2023年度以降、同様の対策を他のグループ会社にも展開を進め、TOPPANグループのメール攻撃耐性強化を図ります。

### サイバー対応専門チームの対応力強化

2022年12月にTOPPANグループにおける組織横断的なサイバー対応の専門チームである、TOPPAN-CERTは内閣サイバーセキュリティセンター（NISC）と日本シーサート協議会（NCA）が主催する連携分野横断的演習などに参加し、実際にサイバー攻撃を受けた場面を想定し、CERTメンバーが中心となって対応を行い、演習後には振り返りを実施することで対応手順や課題を検証することで、サイバー攻撃を受けた際の対応手順の改善に役立てています。

### サイバーセキュリティ状況の共有

社内外のサイバーセキュリティ環境の状況の理解を深めるため、情報セキュリティ関係者向けに四半期ごとのサイバーセキュリティ情報共有会を実施しています。

# 第三者認証の取得

活動実績・データ

ISMS認証取得「ISO/IEC27001」とプライバシーマーク付与認定(JIS Q 15001:2017)などを凸版印刷株式会社およびグループ会社で取得しています。(2023年6月30日現在)

## ISMS認証取得(ISO/IEC 27001)(情報セキュリティマネジメントシステム)

| | |
|---|---|
| 凸版印刷(株) 情報コミュニケーション事業本部、DI本部 ビジネスプラットフォーム部、DXデザイン事業部 インテグレーションビジネスセンター テクニカル本部、(株)トッパンコミュニケーションプロダクツ、(株)トッパングラフィックコミュニケーションズ、ティージーエス(株)、(株)TBネクストコミュニケーションズ | IC06J0151 |
| TOPPANエッジ(株)(トッパングループ関西ビジネスセンター) | JQA-IM0137 |
| (株)トッパンインフォメディア | JUSE-IR-404 |
| 凸版印刷(株)(朝霞工場、滋賀工場)、(株)トッパンエレクトロニクスプロダクツ(朝霞工場、滋賀工場)半導体フォトマスク、(株)トッパン・テクニカル・デザインセンター半導体製品の設計・開発および製造委託・管理 | IS 530416 |
| (株)ONE COMPATH | IS 533218 |
| 凸版印刷(株)西日本事業本部 情報セキュリティ管理部九州中四国チームおよびISMS推進委員会 | I308 |
| (株)トッパングラフィックコミュニケーションズ(関西制作本部) | IC13J0361 |
| 凸版印刷(株)東日本事業本部 | IS 606897 |
| (株)トッパンコミュニケーションプロダクツ 滝野工場、凸版印刷(株)関西事業部 関西技術部 情報系滝野生産技術T | IC14J0376 |
| 凸版印刷(株)中部事業部 セキュアBPO事業T、(株)トッパングラフィックコミュニケーションズ(中部制作部)、(株)トッパンコミュニケーションプロダクツ名古屋工場 | IC17J0444 |
| その他非公開:1事業者 | |

## ISMS認証取得(ISO/IEC27017)(クラウドセキュリティマネジメント)

| | |
|---|---|
| 凸版印刷(株) DXデザイン事業部 ICT開発センター開発一部3チーム | SC22J0025 |

## プライバシーマーク付与認定(JIS Q 15001:2017)

| | |
|---|---|
| 凸版印刷(株) | 10190891 |
| (株)トッパンコミュニケーションプロダクツ | 24000216 |
| (株)トッパングラフィックコミュニケーションズ | 10190298 |
| トッパンエディトリアルコミュニケーションズ(株) | 24000308 |
| 凸版物流(株) | 10450006 |
| (株)トッパントラベルサービス | 10450093 |
| TOPPANエッジ(株) | 10190934 |
| トッパン・フォームズ・セントラルプロダクツ(株) | 24000366 |
| トッパン・フォームズ東海(株) | 24000204 |
| トッパン・フォームズ関西(株) | 24000101 |
| トッパン・フォームズ西日本(株) | 18860028 |
| TOPPANエッジITソリューション(株) | 10820089 |
| TOPPANエッジ・サービス(株) | 10450002 |
| 北海道トッパン・フォームズ(株) | 10190307 |
| (株)トスコ | 11820447 |
| (株)ジェイエスキューブ | 10860018 |
| 図書印刷(株) | 24000032 |
| 東京書籍(株) | 10190966 |
| (株)リーブルテック | 10190035 |
| 東京物流企画(株) | 10860071 |
| (株)学習調査エデュフロント | 10861827 |
| (株)フレーベル館 | 24000369 |
| (株)BookLive | 28000007 |
| 東京都チャレンジドプラストッパン(株) | 24000419 |
| (株)ONE COMPATH | 24000445 |
| (株)トッパン・コスモ | 24000449 |
| UNIWORX | 21004696 |
| 桐原書店 | 24000459 |
| (株)TBネクストコミュニケーションズ | 24000464 |

# 情報セキュリティ教育

教育・啓発

TOPPANグループでは、情報セキュリティ管理体制の強化＝人財の強化、であるという認識のもと、様々な視点からの教育や自己点検を実施しております。

## 全従業員向け教育の実施

TOPPANグループでは、年1回、全従業員のセキュリティレベル向上のために定期教育を実施しています。

2022年度は、「～変化する“今”を生きるために～サイバーをはじめとする情報セキュリティの脅威に、グループ一丸で対抗を」をテーマに、サイバー攻撃への備え、日常業務におけるセキュリティ上の留意点、改正個人情報保護法施行への対応にのみならず、各事業(本)部固有のリスクも加味した幅広い視点からの教育を実施しました。

## 工場技術者に対するセキュリティ教育の実施

TOPPANグループでは、2021年度より「技術防人養成所」と銘打った教育を開始しました。これは、工場の技術員に対し、製造設備の導入企画から廃棄までの過程における、必要なセキュリティの要件を教育することで、製造現場におけるセキュリティが強化された製造DXを実現する取り組みです。

2022年度は20名が「技術防人養成所」を修了しています。

## 経営層向けサイバーセキュリティ演習の実施

TOPPANグループにおける経営層、上位管理職層におけるサイバーインシデントに対する危機対応、リスク管理の能力向上のため、サイバー攻撃による重大インシデント発生を想定したサイバーセキュリティ演習を年2回実施しています。

また、演習終了後にはその結果を評価することで、サイバーインシデント対応上の課題を把握し、改善を実施しています。

## 全社自己点検の実施

TOPPANグループでは、情報セキュリティ管理の実態について、従業員一人ひとりが把握し、その気付きからもセキュリティ意識の向上を図るために、全社的な自己点検にも取り組んでいます。

この結果については、部門ごとに提供することで職場単位での改善対応を自ら行動できるようにしています。

2022年度は、リモートワークに慣れた従業員が、秘密情報を含む媒体や書類の適切な取り扱いを認識するための設問を追加し、常に最新の勤務環境に応じた意識が涵養できるよう考慮しています。

## 新たなセキュリティトレーニング環境

2022年度より、セキュリティトレーニング環境としてTSAT(TOPPAN Security Awareness Training)を構築しました。

この環境を活用することで、訓練→評価→教育のトレーニングプロセスを繰り返し実施することが容易になり、これまで以上に効率的なTOPPANグループのヒト強化によるサイバー攻撃耐性強化を実現可能としました。

## ウイルスメール対応訓練の実施

不審なメールは開封せず、開封してしまったとしても速やかに通報できるよう、TOPPANグループのメールアドレス利用者全員(約25,000名)に、通報先のショートカットやアイコンを設定した上で、通報を経験してもらう訓練を年2回実施しています。2022年度はウイルスメール対応訓練の対象を従来の子会社、関連会社に加え、海外子会社(合計 約50,000名)に広げました。

訓練では、訓練メールのリンクをクリックしても訓練対象者には訓練と気付かせないWebページを表示させることで、より本物のメール攻撃に近い難易度の高い内容で実施しました。

## サイバーセキュリティ人材育成会社「Armoris」によるトレーニングの継続的な実施

TOPPANグループは企業・公共機関を対象に、サイバーセキュリティ人材育成プログラムおよび組織のセキュリティ向上サービスを提供する「Armoris」を設立し、実戦的な人材育成プログラム「DOJO」および「DOJO Lite」「DOJO Shot」「 DOJO CORE 」などを継続して展開しています。

個々人の技量進度に合ったプログラムに加えて、長期間継続的にトレーニングを行える「DOJO」、最新のテーマに沿った事例やケーススタディが学べる「DOJO Lite」、「DOJO Shot」、インシデント対応を実際に体験する実戦的な「DOJO CORE」を展開することにより、TOPPAN自らはもちろん、日本における個人と組織のセキュリティ能力向上を目指しています。

「DOJO」サービスイメージ