

お客さまへの価値提供プロセスにおける 情報セキュリティ品質の向上

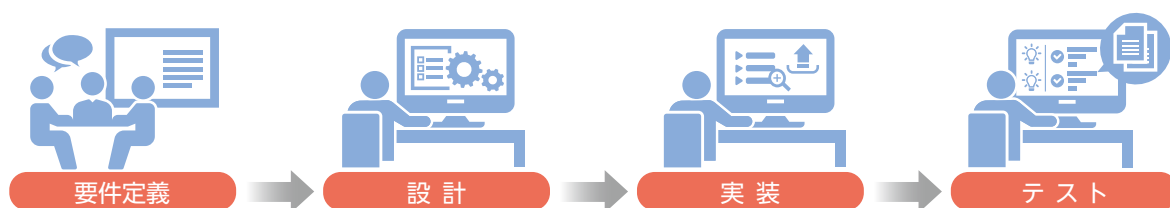
営業や保守サービス、ソフトウェア開発などの業務プロセスにISMSを中心としたマネジメントシステムを組み込むことによって、情報セキュリティ品質の向上に取り組んでいます。

▶お客さまに安心安全を提供する開発プロセス

キヤノンITソリューションズでは、金融、製造、流通・サービス、社会公共、公益分野における業種別ソリューションをはじめ、SIサービス、クロスインダストリーソリューション、パッケージ開発など、広範なサービスを通じてお客さまが抱える課題を解決しています。システムの受託開発にあたっては、お客さまからの「信頼」と「安心・安全」にお応えするために、品質管理とともに情報セキュ

リティへの配慮が不可欠です。

具体的には、「開発環境のセキュリティ」として、体制整備・開発場所の入退室管理・情報資産の適切な取り扱いなどの対策を行うほか、下記のように、「システム開発のセキュリティ」として、各開発プロセスにおけるリスクに応じた情報セキュリティ対策を行っています。



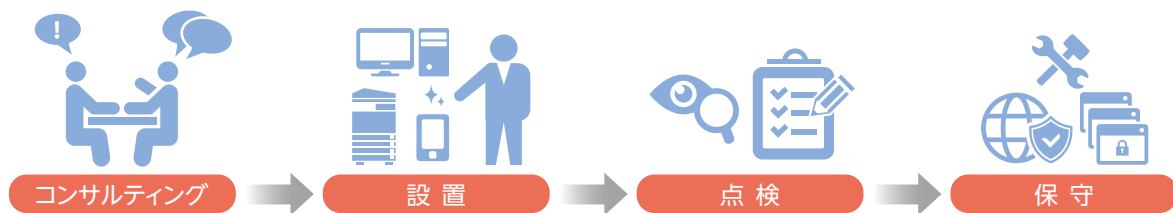
開発プロセスにおけるリスクと情報セキュリティ対策事例

	リスク	対 策
要件定義	- セキュリティ要件の認識誤り - セキュリティ要件の不足	開発要件定義にあたっては、十分な知識を持った要員をアサインしてセキュリティ要件を定義し、レビューを行っています。
設計	- セキュリティ要件との齟齬 - セキュリティ設計のミス	設計段階においては、セキュリティ要件の定義に基づき、具体的なセキュリティ機能を明確化するためのセキュリティ設計を行っています。セキュリティ設計は、十分なレビューを行い、必要に応じて実現性についての検証も行います。
実装	- コーディングミス - システムの不十分な構成管理	- 実装段階における脆弱性の混入を防ぐため、セキュアプログラミングを行っています。なお、最新のセキュリティ技術については、常に関係者間でノウハウやナレッジを蓄積、共有化しています。 - また、システムの構成要素の識別と管理を確実にし、仕様変更や脆弱性が確認された場合の修正を迅速に行えるよう構成管理に万全を期しています。
テスト	検証と妥当性確認の漏れ	- システムの開発工程でセキュリティの検証と妥当性確認のために、レビューやさまざまなテストを行っています。 - 脆弱性検出ツールなどを用いて十分なテストを実施しています。

▶ お客さまに安心安全を提供する保守サービスの実践

キヤノンシステムアンドサポート（以下、キヤノン S&S）は、全国約 170 の拠点で、営業・サービス・サポートが一体となってコンサルティングから保守サービスまで一貫してお客さまの支援を展開しています。

キヤノン S&S は、ISMS およびプライバシーマークの認証に加えて ISO9001 を取得しており、それらに準拠した手順を踏まえ、お客さまに安心して複合機やプリンター、ネットワーク機器をご利用いただくための保守サービスを提供しています。



保守サービスプロセスにおけるリスクと情報セキュリティ対策事例

	リスク	対 策
外出前（社内）	サービス工具（パソコン・USB メモリー）の紛失・ウイルス感染	- サービス工具（パソコン・USB メモリー）は、施錠保管しています。 - 外出前に最新のセキュリティパッチを適用し、ウイルスチェックを実施しています。 - USB メモリーは日々の持ち出し・返却を記録し、管理しています。
修理受付（移動中）	修理受付用の携帯電話（スマートフォン）の紛失による情報漏えい	- 自動ロック機能、リモートロック機能、リモートワイプ機能、暗号化機能、パスコードロック機能、セキュリティ監視機能を実装しています。 - 携帯電話はネックストラップを使用して、落下・紛失を防止しています。
	パソコンの紛失による情報漏えい	社外利用のパソコンはハードディスクパスワード、ログインパスワードに加えてハードディスク暗号化ソフトで保護しています。
点検・保守（お客さま先）	お客さまデータの漏えい ネットワーク接続時のウイルス流布	- 紙詰り処理などで取り除いた用紙には機密情報が含まれる可能性があるため、その処理をお客さまに確認しています。 - お客さまのデータをお預かりする際は、お客さまに管理方法や作業内容を説明し、了承をいただいています。 - 代替機は、不要なデータが登録されていない状態で貸出し、返却の際にはお客さま情報を消去しています。 - お客さまのネットワークへ外部のパソコンを接続することを禁止しています。 - 作業上やむを得ず当社パソコンを接続する際には、お客さまにそのセキュリティ対策や作業内容を説明した後、書面にて了承をいただいております。
帰社後（社内）	セキュリティ意識・知識の欠如	サービスメンテナンス時に必要なセキュリティ対策に関する教育を適宜実施しています。
	お客さまよりお預かりしたデータの目的外利用・誤廃棄・漏えい	- お客さまからデータをお預かりする際は、データの利用目的や返却方法などを「確認書」にてチェックし、その内容に従って取り扱います。 - なお、お預かりしたデータは施錠できる環境で保管するなど適切に管理しています。

▶ お客さまに安心安全を提供する IT 保守サービス

キヤノンS&S カスタマーサポートセンターは、IT保守をご契約いただいたお客さまの機器に何らかのトラブルがあった際、電話およびリモート操作での復旧支援や必要に応じて現地技術者の訪問手配などを行う、IT機器の障害対応窓口です。

品質推進担当を中心に、リモートツール※の利用におけるリスクの洗い出しと情報セキュリティ対策を実践し、お客さまが安心してパソコンやネットワーク機器をご利用いただけるようサポートします。



リモートツールの利用におけるリスクと情報セキュリティ対策事例

	リスク	対 策
リモート接続	●作業担当者の経験不足によるリスク	●6か月以上の電話対応業務経験および技術研修の受講完了を必須としています。 ●リモートツールによる接続権限の付与条件として、実機を使つてのトラブルシューティングと接続アセスメントを行い、合格者にのみリモート接続の権限を付与しています。
	●お客さまの意図しない接続による情報漏えい	●リモートツールの利用画面上の同意ボタンより、お客さまのご了承をいただき、接続しています。
	●安全性の低いパスワードによる第三者の利用	●リモート接続時には、大文字小文字の英文字および数字を組み合わせた複雑なパスワードを使用し、かつ3か月に一回パスワードを変更してセキュリティを高めています。
リモート作業	●盗聴による情報漏えい	●リモートツールは、盗聴・解読が極めて困難な、暗号化技術を採用しています。すべてのデータ通信を暗号化し、高いセキュリティにより情報漏えいの防止を行っています。
	●技術難易度の高い作業による、パソコンの破損やデータを消失するリスク	●リモート作業の内容を5段階のレベルに分け、難易度に応じて上級対応者へのエスカレーション、または現地担当者への訪問対応依頼を行います。
リモート作業後	●接続解除忘れによる情報漏えい	●作業中はお客さまのパソコンの壁紙を黒くして、接続を解除すると通常の壁紙に戻る設定とし、接続中が切断されたかを明確にしています。またお客さまに接続が切れたことを確認いただいた上で、通話を終了しています。

※リモートツールとは、インターネット経由でお客さまのパソコン画面を共有する仕組みです。
この仕組みを利用することで、担当スタッフが遠隔でお客さまのパソコンを操作することが可能となります。

▶ お客さまに安心安全を提供する修理プロセスの追求

キヤノン MJ では、キヤノンホームページにてパーソナル向け製品の引取修理サービスを提供しています。セキュリティ対策を施したサイトから、お客さまご自身で家にいながらいつでも修理をお申し込みいただくことが可能です。

また、銀座・大阪のサービスセンターおよび品川キヤノンプラザ S 修理メンテナンス受付コーナーでは、対面にてパーソナル向け製品の修理・メンテナンスのご相談やお申し込みを承っています。

各受付窓口や修理センターでは、お客さまの大切な製品と個人情報をお預かりしている重要性を認識し、情報セキュリティ対策

と教育に取り組み、安心して快適に製品をお使いいただけるアフターサポート体制を整えています。



サービスセンターでの
対面受付



ホームページでの
申込受付

修理サービスプロセスにおけるリスクと情報セキュリティ対策事例

	リスク	対 策
受付	●修理受付時のお預かり品（修理品・付属品）の取り違え ●お客さまの個人情報の紛失・漏えい	●窓口で修理受付時にお預かりする機器と付属品、保証書などをお客さまと一緒に確認し、管理用バーコード付きのタグを付けて、専用システムで管理しています。 ●お申し込み時にご提供いただいた個人情報は、強固なセキュリティで保護された当社基幹システム内で管理しています。
	●修理費用のお見積もりをお知らせする際のファクス／eメールの誤送信	●ファクス／eメールはお申し込み時に登録いただいた宛先へシステムから自動送信を行い、誤送信を防止しています。
修理作業	●お預かりした可搬メディアへのコンピューターウイルス感染	●可搬メディアをお預かりした場合は、検疫用パソコンで最新の定義ファイルを用いたウイルスチェックを実施します。 ●修理関連業務用パソコンのすべてにウイルス対策ソフトを導入し、最新の定義ファイルとセキュリティパッチを適用しています。
	●お預かり品の盗難・紛失	●修理センター内の各工程において、管理用バーコードを用い、専用システムに登録されている情報と現品の照合を行っています。 ●修理中に付属品を紛失しないために、作業工程ごとに付属品チェックシートと現品の多重チェックを行っています。 ●盗難・紛失防止として、終業後は施錠環境にて保管しています。
	●修理センターにおける情報セキュリティ事故の発生	●修理センターでは、個人情報の管理・運用手順の指導や教育と、定期的に管理状態の監査を実施しています。
配送	●個人情報に記載された伝票やお預かり品の誤送付	●梱包前に、宅配伝票・修理完成伝票に記載されている機種名と現品が一致していることを確認した上で、修理完成伝票とお預かり品それぞれの管理用バーコードで照合しています。
窓口返却	●お預かり品の誤返却	●お客さまご持参のお預かり書と修理完成伝票に記載されている内容（修理番号、機種・機番、お客さま名、付属品）の声出し確認を行っています。 ●お預かり書・修理完成伝票・お預かり品、それぞれの管理用バーコードを照合し一致していることを確認して返却しています。

NVS導入時におけるセキュリティケア(キヤノンS&S)

NVS(ネットワークビジュアルソリューション)※は、設置した場所の様子をパソコンやスマートフォンなどで、24時間リアルタイムで送信映像を確認することができる監視カメラシステムです。インターネットにつながる製品の性質上、サイバー攻撃を受けるリスクが存在します。そこで、システムそのものへのセキュリティ対策のほか、キヤノンS&SではNVS導入時に次の取り組みを行っています。

● 管理者パスワードの変更

管理者パスワードは、お客さまにて必ず初期設定から変更していただくこと、安全のために定期的に更新していただくようお願いしています。

● プライベートIPアドレスによる運用を推奨

インターネット接続時は、プライベートIPアドレスでの運用をご提案し、さらにファイアーウォールが設定された環境でのご利用をお勧めしています。

さらにキヤノンS&Sでは、お客さまにNVSの販売とともにUTM(統合脅威管理)ソリューションを同時に提案することで、お客さまにとって容易かつ適正なコストでのセキュリティ対策を実現しています。

※ NVS(ネットワークビジュアルソリューション) = 監視カメラシステム全体のことで、ネットワークカメラとネットワーク録画装置、ネットワーク録画ソフト、アナログカメラ、アナログ録画装置、周辺機器および工事・保守で構成されます。

電子化レポートで、作業報告のペーパーレス化を実現(キヤノンS&S)

キヤノンS&Sでは、タブレットスタイルの2in1パソコンを活用した作業報告書※の電子化を2018年8月より開始し、お客さまに見やすく、わかりやすい作業報告を実施しています。

従来は、作業終了後に手書きの帳票もしくは複合機から出力した帳票にお客さまのご署名をいただいていたが、現在はタブレット画面上でご説明し電子署名をいただいています。作業報告書の電子化により、見やすく、わかりやすい作業報告とペーパーレス化を実現しています。

また、作業報告書をご入用のお客さまには電子ファイルでお送りすることもできるため、お客さまご自身のパソコン画面上で報告書の内容をご確認いただけます。紙面で保管・管理する必要もなくなり、お客さま満足の向上に貢献しています。

※ 作業報告書とは、複合機、パソコン・サーバーなどの設置・点検・修理などを実施した際に、作業内容を記し、お客さまからご署名をいただく報告書です。



電子化レポートで「見やすい」「わかりやすい」作業報告を実施