

KIRIN

キリンホールディングス株式会社
Kirin Holdings Company, Limited

キリンホールディングス株式会社

情報セキュリティ報告

INFORMATION SECURITY REPORT

トップメッセージ

キリングroupでは、お客様・従業員・株主・社会からの長期的な信頼の獲得、そして経営目標の達成や事業の継続性に重大な影響を及ぼす不確実性をリスクと定義しています。ネガティブリスクの低減や顕在化の未然防止を通じたリスクの許容範囲内に収めることをリスクマネジメントにおける基本方針とし、このためのマネジメント体制の構築・整備、コンプライアンスの徹底を進めています。

キリングroupは、KV2027ビジョン「食から医にわたる領域で価値を創造し、世界のCSV先進企業となる」を実現すべく、2022年から開始する中期経営計画では、ポストコロナを見据え、各事業において構造改革を実行するとともに新たな価値創造を進めて成長を加速させてまいります。

これらの取り組みのためには、アナログで進める業務のデジタル化、社内外のワークフローのデジタル化、グループの事業モデル並びに組織風土のデジタル基盤による変革が欠かせず、2022中期経営計画においても従前に続いて戦略的に重要度の高いテーマを掲げて各課題の解決を進めます。

これらの推進に際して、営業機密情報のみならず、個人情報等の重要な情報資産をサイバー攻撃等から確実に保護できる環境を整備し、お客様をはじめステークホルダーの皆さまが安心してキリングroupとお取引いただけるようにすることが不可欠です。従いまして、グループとして情報セキュリティを重要リスクの一つと認識し、「社内ルールの整備・充実と従業員の啓発」といった基本課題に「グループ内のガバナンス強化」と「技術対策の推進」を加えた三つを柱として様々な対策を計画的に進めています。

過去より、キリンググループの情報セキュリティ対策は、営業機密情報をはじめとする情報資産の漏洩や紛失等のリスク低減に力点を置いて、また個人情報保護の高まりとあわせ、情報資産及びこれらを保管・保存する機器や建物の管理に関するルールの制定と定着、並びに漏洩リスク低減のための情報システム基盤の構築を進めてまいりました。

こうした過去のステージを当社「情報セキュリティ1.0」としますと、その後のインターネット上で提供されるサービス、通信ネットワーク及びモバイル機器等の進化と普及にあわせ、また急増する悪意ある攻撃に対する防衛力強化を狙い、「情報セキュリティ2.0」として2021年末までのマイルストーン毎に段階的に成熟度を上げていくロードマップを策定して施策を展開してまいりました。直近で特に傾注していたのは、プライバシーデータ保護ポリシーの制定、情報セキュリティ対策に関するチェック・統制対象のグローバルスコープで拡大、監視・検知、及びインシデント発生時態勢の強化としてのSOC及びCSIRTの設立と充実、リモートワークへの対応、等です。

攻撃者はその脆弱性を狙います。

一か所の対処の不備が全体のリスクを高めることから、個々の施策の浸透・定着の水準も上げていく必要があります、このためにサイバー攻撃や情報資産に関する私たちの理解をより深めていくことが不可欠と考えています。

2022中期経営計画でも、このような認識の下、当グループの情報セキュリティ活動を「ステージ3.0」として取り組みます。

本情報セキュリティ報告書は、キリンググループの取り組みをご紹介しますものです。ぜひご一読いただければ幸いです。

キリンホールディングス株式会社
デジタルICT戦略部長



Table of Content

トップメッセージ	02
情報セキュリティのガバナンス	06
情報セキュリティの体制	08
情報セキュリティのリスク	10
情報セキュリティインシデントへの対応体制	12
プライバシーデータ保護ポリシー	13
エリアでの管理	14
リモートワークでの対応状況について	15
情報セキュリティインシデント	16
マネジメントレビュー	18
情報セキュリティ人財	20

本書はキリングroup全体の
情報セキュリティに関しての報告を経済産業省発行
「情報セキュリティ報告書モデル」を参考に
まとめたものです

「企業を支える」から 「事業をリードする」情報セキュリティ

グループ全体の情報システム機能(ヒト・モノ・カネ)を集約し、IT戦略策定から案件の実行までのITライフサイクル全般に関わり、情報システムのガバナンスを通じたグループ情報戦略を主導しています。

情報セキュリティの規程構成

- 情報セキュリティマネジメントシステムの確立と実施および継続的改善
- 教育の実施
- 事業継続性管理
- 法令および規範並びに契約上の要求事項の遵守

■ 個人情報保護方針

<https://www.kirinbs.co.jp/privacy.html>

※一部グループ会社については、個人情報保護方針を個別に制定しています。

■ ウェブサイト

<https://www.kirinholdings.co.jp/>

■ 対象期間

2021年(1月～12月)の情報セキュリティに関する活動や取組を対象としています。

■ 対象会社

当報告書はグループ全社を対象としていますが、一部の活動や取組については実施していない内容があります。

情報セキュリティの基本方針

情報セキュリティ対策の向上をグループ共通の重点取り組みの一つと捉え、さまざまな対策を講じています。

「社内ルールの整備・充実」や「従業員に対する教育」といった基本となる取り組みに加えて、「グループ内に対するガバナンスの強化」と「技術的対策の推進」を柱とする情報セキュリティ対策レベル向上の取り組みを計画的に進めています。

具体的には、情報セキュリティに関するルールを定め、適切な情報管理を実施しています。

また、内外の環境変化に応じて随時ルールの見直し・追加を行い、常に高いセキュリティレベルを維持しています。

情報セキュリティのガバナンス

キリングroupは情報セキュリティ対策の遵守状況を定期的に確認しています。国内外グループ各社に対して、情報システム分野における機能分担会社であるキリンビジネスシステムが遵守状況をチェックし、是正すべき点を確認した場合は速やかに改善を促しています。

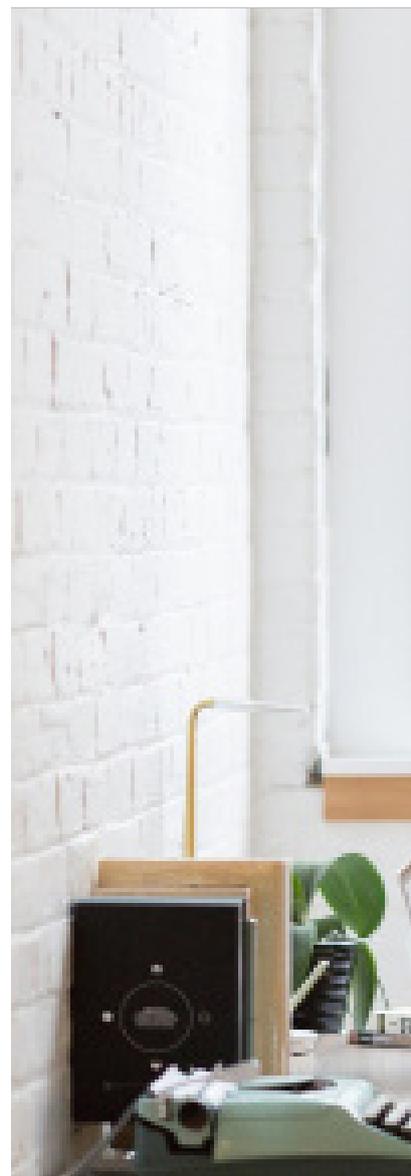
キリングroupの全社を対象に

従来からキリングroup全体の情報セキュリティに関する基本的な考え方、対策、管理方法などを定めた「キリングroup情報セキュリティ規程」を制定しています。情報セキュリティに関する国際標準規格ISO/IEC27001:2013(日本国内ではJISQ27001:2014)に準拠する形で2021年1月に改訂しました。

同時に海外グループ会社向けの「情報セキュリティガイドライン」を制定し、海外グループ各社では、全従業員を対象にしたE-ラーニングなどの研修を定期的実施することにより、従業員の情報管理意識およびスキル向上を図っています。

新たな取り組みとして、個人の認証の強化や入退室の管理の強化に順次取り組んでいます。

このような取り組みにより、キリングgroupにおける情報セキュリティの強化を図っています。



情報セキュリティガイドライン

各従業員には「情報セキュリティ規程」を軸にした各種マニュアルを用意して、各グループ会社の実情に応じた工夫をしています。

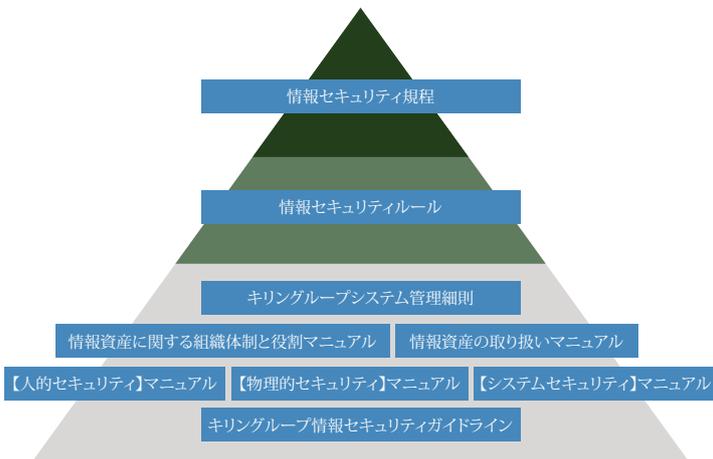
各マニュアルについて

キリングgroupのマニュアルは、各種情報セキュリティに関する規定を踏まえ、キリングgroup事業独自のルールに合わせ、第三者コンサルティング会社によるレビュー、およびEラーニングからの課題をフィードバックし、必要に応じて更新しています。

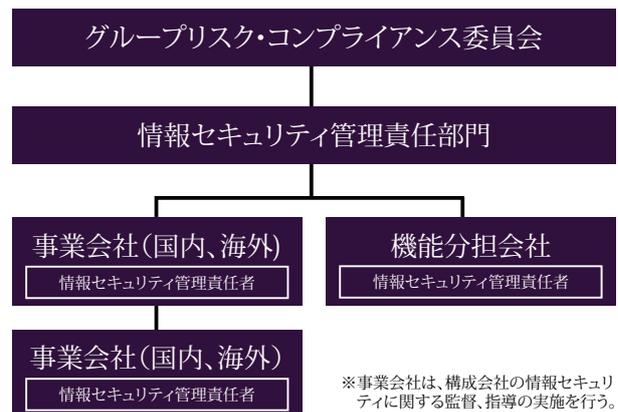
キリングroup事業会社独自のルールを設定し、従業員の意識向上を目指しています



情報セキュリティの規程構成



情報セキュリティ体制図



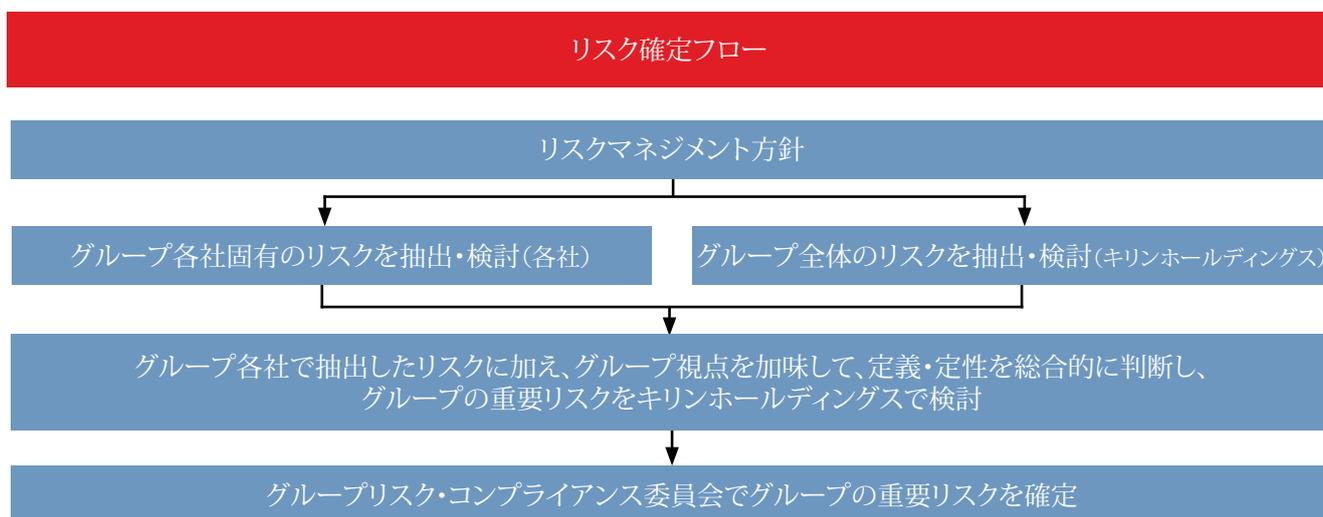
情報セキュリティの体制

キリングroupでは、キリンビジネスシステムを、グループ全体の情報セキュリティ向上の統括・推進部門と位置付け、キリングroupにおける情報セキュリティ向上のために、グループ各社の監督・指導を行っています。

重要リスク確定体制

グループ各社では、キリングroupのリスクマネジメント方針に基づき、定量・定性の両面から事業固有のリスクを抽出・検討しています。

これらリスクをグループリスク・コンプライアンス委員会事務局(キリンホールディングス経営企画部)で集約・精査し、影響度が大きく発生確率が高いリスクやグループ全体に共通するリスクについては、グループリスク・コンプライアンス委員会で審議の上、グループの重要リスクとして確定しています。



主要国内グループ会社

キリンビール株式会社
キリンビバレッジ株式会社
メルシャン株式会社
キリンシティ株式会社
協和キリン株式会社
協和発酵バイオ株式会社
小岩井乳業株式会社
キリンアンドコミュニケーションズ株式会社
キリンエンジニアリング株式会社
キリングroupプロジスティクス株式会社
キリンテクノシステム株式会社
キリンビジネスエキスパート株式会社
キリンビジネスシステム株式会社
キリンエコー株式会社

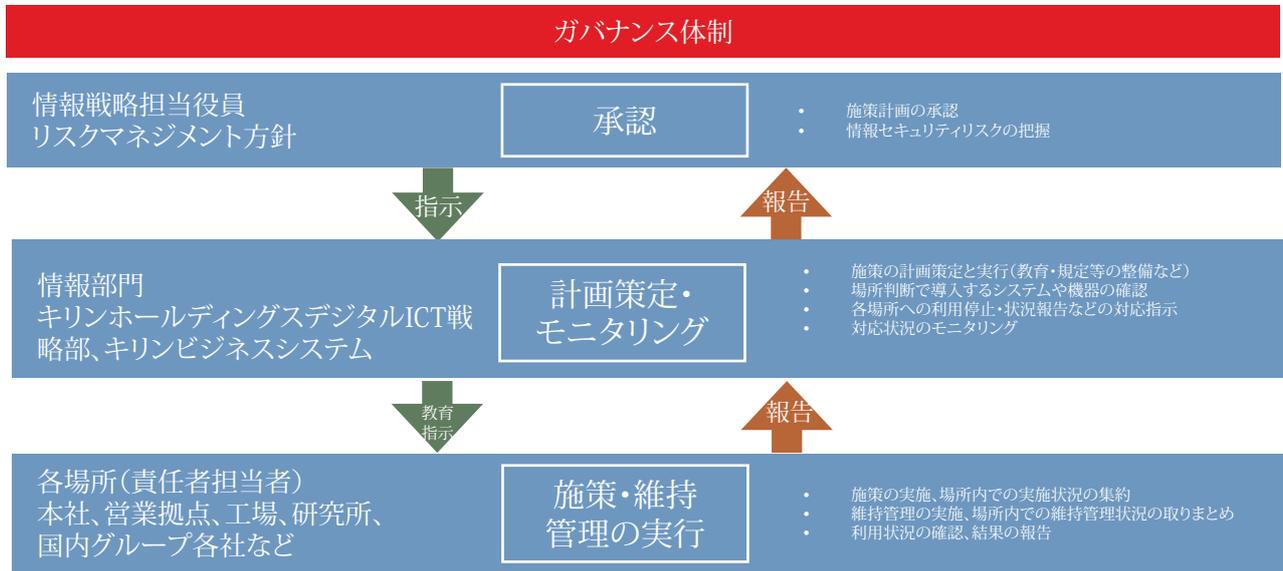
主要国外グループ会社

Lion Pty Ltd (オーストラリア)
Interfood Shareholding Company(ベトナム)
Kirin Holdings Singapore Pte, Limited(シンガポール)
Kirin Europe GmbH(ドイツ)
Coca-Cola Beverages Northeast, Inc.(アメリカ)
Four Roses Distillery, LLC(アメリカ)

各国固有の法律、制度に従いセキュリティ施策を行っています。

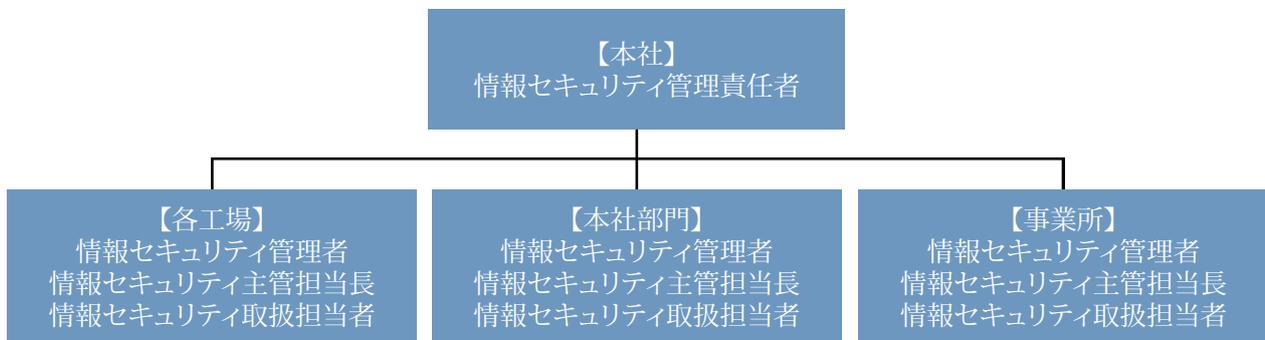
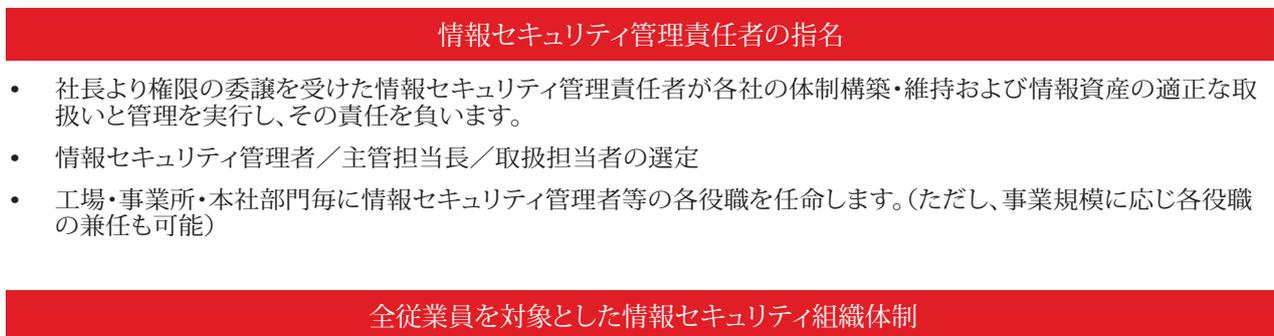
情報セキュリティガバナンス体制

情報セキュリティ対策に関する取組体制を明確化し、情報資産の漏えいのリスクを低減させるとともに、外部からの情報セキュリティに対する脅威に対応し、情報セキュリティ対策の実効性を高めます。



情報セキュリティ推進体制

情報セキュリティ管理責任者を中心に情報セキュリティを推進する。



情報セキュリティのリスク

グループ内のセキュリティ対応体制を整え、人的・物理的・技術的対策を実施することで、ウィルス感染や外部からの不正アクセスといったサイバー攻撃の脅威への対策強化に努めています。

機密性区分に応じた情報管理

- 社内の極めて限られた者だけが知りえる特に重要な情報資産
- 社内の限られた関係者であれば知ることができる情報資産
- 社内の者(状況によりグループ内の限られた会社)であれば誰でも知ることができる情報資産
- 社内外の誰でも知ることができる公開情報

破棄

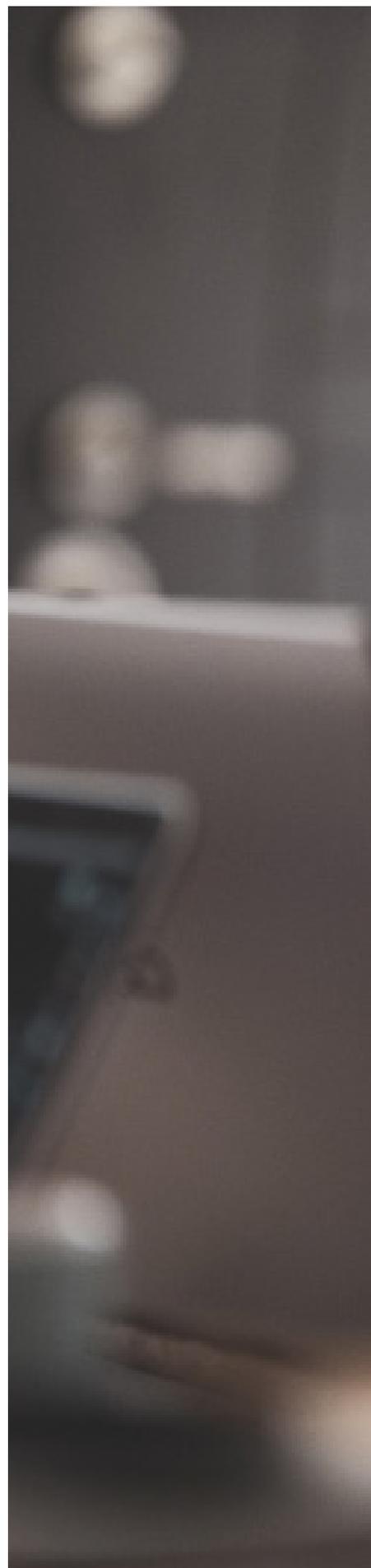
各媒体に合わせ廃棄ルールを設定し管理しています。

廃棄・削除	手段
印刷物[紙]	<ul style="list-style-type: none">• 印刷物[紙]はシュレッダー、溶解処理等により廃棄します。• 溶解処理実施までの管理に注意します。• セキュリティBOX・保存箱等の管理・保管に留意しています。
外部記憶媒体	<ul style="list-style-type: none">• USBメモリ、大容量ディスク等の外部媒体は、物理的に破壊します。
電子データ	<ul style="list-style-type: none">• バックアップを含めて対象となる全ての電子データを削除します。
パソコン	<ul style="list-style-type: none">• 専用データ消去ソフトを利用し、電子データを削除します。

雇用時、退職時および雇用変更時の管理

秘密保持に関して誓約書または雇用契約書に含めています。

- 従業員の退職または解雇時に、その在職中に知り得た重要情報を特定し、秘密保持等の義務の内容を確認させる。
- 在職中に知り得た情報を、競合企業のために提供または開示しない。
- 過去に就業していた企業または組織で知り得た情報を、当該企業または当該組織の承諾無しに、自社内で開示あるいは利用しない。





情報管理の戦略

グループ内のセキュリティ対応体制を整え、人的・物理的・技術的対策を実施することで、ウィルス感染や外部からの不正アクセスといったサイバー攻撃の脅威への対策強化に努めています。

情報セキュリティインシデントへの対応体制

キリングroupでは、深刻化しているサイバー攻撃の脅威に対応するため「KIRIN-CSIRT」を構築し、キリングroupにおける重要リスクの一つである情報セキュリティに取り組んでいます。

KIRIN-CSIRT

グループ内のセキュリティ対応体制を整え、人的・物理的・技術的対策を実施することで、ウィルス感染や外部からの不正アクセスといったサイバー攻撃の脅威への対策強化に努めています。

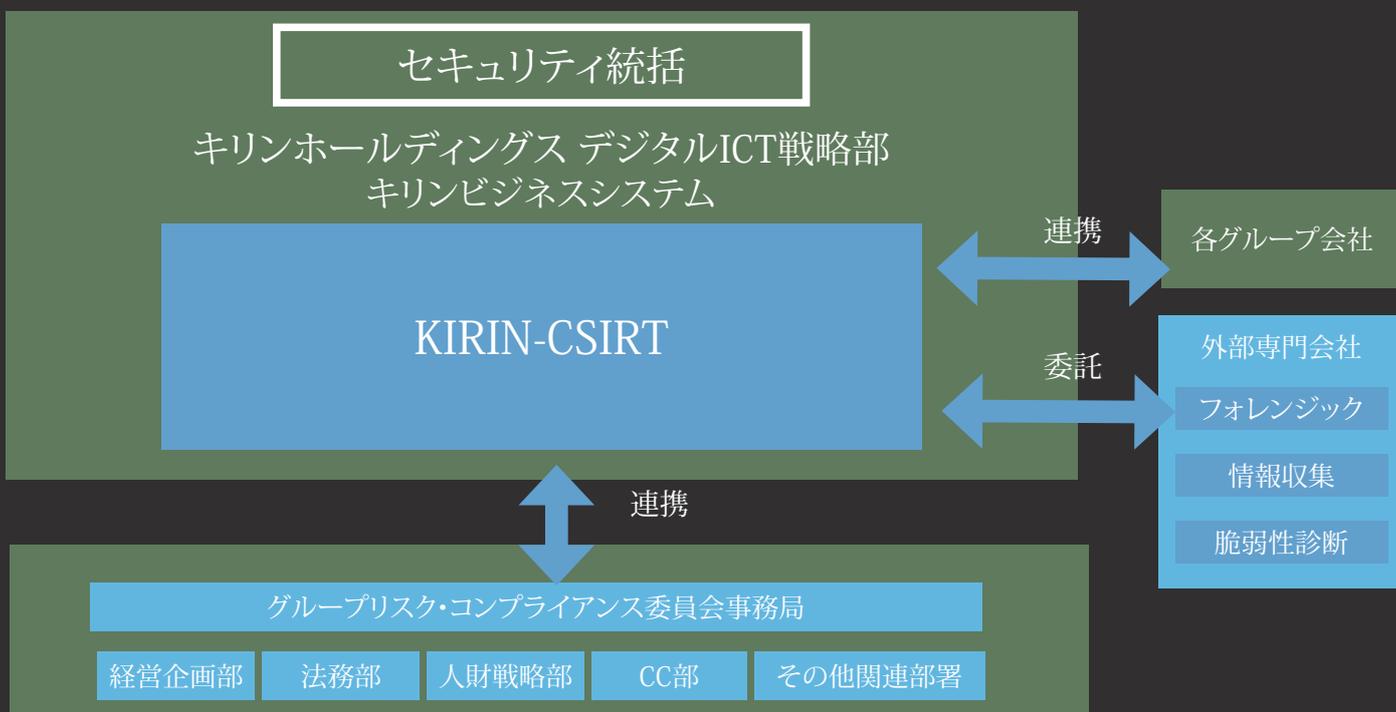
目的

セキュリティインシデント発生時におけるスピーディで組織的な対応をするため、体制を整備しています。

関連部署と連携

CSIRTはキリンホールディングスリスク委員会事務局、IR室、CSV戦略部、法務部、人財戦略部(人事系・総務系共に)、コーポレートコミュニケーション部と連携し、設立しています。

KIRIN-CSIRT体制



CSIRT(Computer Security Incident Response Team)とは？

CSIRTとは、コンピュータやネットワーク(特にインターネット)上で何らかの問題(主にセキュリティ上の問題)が発生した場合にその対応を行う組織の総称。

プライバシーデータ保護ポリシー

キリングroupでは、国連の「ビジネスと人権に関する指導原則」に準拠し、事業活動における人権尊重への取り組みにかかわるすべての文書・規範として位置付けた「キリングroup人権方針」を2018年に策定し実践しています。

人権尊重の実践を進めていく上で「個人情報保護」は重要な取り組みテーマの一つとして捉え、「キリングroup プライバシーデータ保護ポリシー」を新たに策定しました。

キリングroupの全役員および従業員に適用され、個人情報保護への取り組みに関するすべての文書・規範の上位文書としています。

要旨

人権を尊重する経営をより一層推進していく取り組みとして当基本方針に従い実践していきます。

- 経済協力開発機構(OECD)が採択したガイドライン基本8原則の実践

原則	実践
収集制限	個人データを収集する際には、法律にのっとり、また公正な手段によって、個人データの主体(本人)に通知または同意を得て収集します。
データ内容	個人データの内容は、利用の目的に沿ったものであり、かつ正確、完全、最新に保ちます。
目的明確化	個人データを収集する目的を明確にし、データを利用する際は収集したときの目的に合致させます。
利用制限	個人データの主体(本人)の同意がある場合、もしくは法律の規定がある場合を除いては、収集したデータをその目的以外に利用しません。
安全保護	合理的な安全保護の措置によって、紛失や破壊、使用、改ざん、漏えいなどから保護します。
公開	個人データの収集を実施する方針などを公開し、データの存在やその利用目的、管理者等を明確に示します。
個人参加	個人データの主体(本人)が、自分に関するデータの所在やその内容を確認できるとともに、異議を申し立てることを保証します。
責任	個人データの管理者は、これらの諸原則を実施する上での責任を持ちます。

- 社会規範の変化に応じた継続的改善に取り組む実践と従業員教育

継続的な活動	実践
社会規範を踏まえた改善	世の中の意識や動向を踏まえ、道義的な側面も考慮しながら個人データ保護のための仕組みを見直し、改善事項を明確にします。
従業員への教育	個人データ保護のための従業員教育を実施します。

- 改善・進捗状況の定期的な公表

キリングroupの取り組み進捗状況をキリンホールディングスのホームページで開示します。

「キリン流」の個人情報保護方針

- プライバシーデータ保護ポリシーのグローバルスタンダードであるOECD 8原則に加えて、キリングgroupが持つステークホルダーとの信頼を重視する考え方を反映することで、「キリン流」の個人情報保護に関する方針を打ち出しています。
- GDPRを筆頭に世界各国でプライバシー関連法令が続々と誕生している状況を踏まえ、本ポリシーとキリングgroup各社が所在する現地法令を踏まえ、社内規程整備を推進しています。
- 一般消費者の皆様はじめ数多くのステークホルダーの個人情報を預かり事業を展開することに対する説明責任を果たすため、個人情報保護に関する取り組み状況の発信を盛り込んでいます。

個人情報等の重要情報に対し、適切に管理し運用しています。

エリアでの管理

事業所施設内外を重要度に応じてエリアに区分しない場合、グループ各社の施設・設備への物理的な不正侵入を防ぐ取り組みを実施しています。事業所の物理的な環境にも情報セキュリティは大きく左右されることから、制御が難しい場合は、運用ルール等での対応としています。

会話・行動について

「不用意な会話」「覗かれる状況での資料の閲覧」「会議終了後の忘れ物」「外部からの問合せ(なりすましを含む)への対応」などの観点から外部での情報資産に対するルールを策定しています。

持ち出しについて

持出時の不注意により、紛失・盗難に遭う可能性があります。また、配送方法によっては受渡しの確認が取れず、荷出し・荷受け時の紛失の可能性が高い場合があることも考慮に入

リモートワーク時の標語

不安に思った時は、自身で抱え込まずにリーダーやセキュリティチームへご相談ください。



委託先の管理

前提として委託先が情報漏えいなどの事故を発生させた場合は、委託元であるキリングループの責任が問われます。委託先は委託元が行うべき業務を代行しているものであり、委託元であるキリングループは委託先においても事故が発生しないように管理・監督を行う義務があります。

インターネットの利用

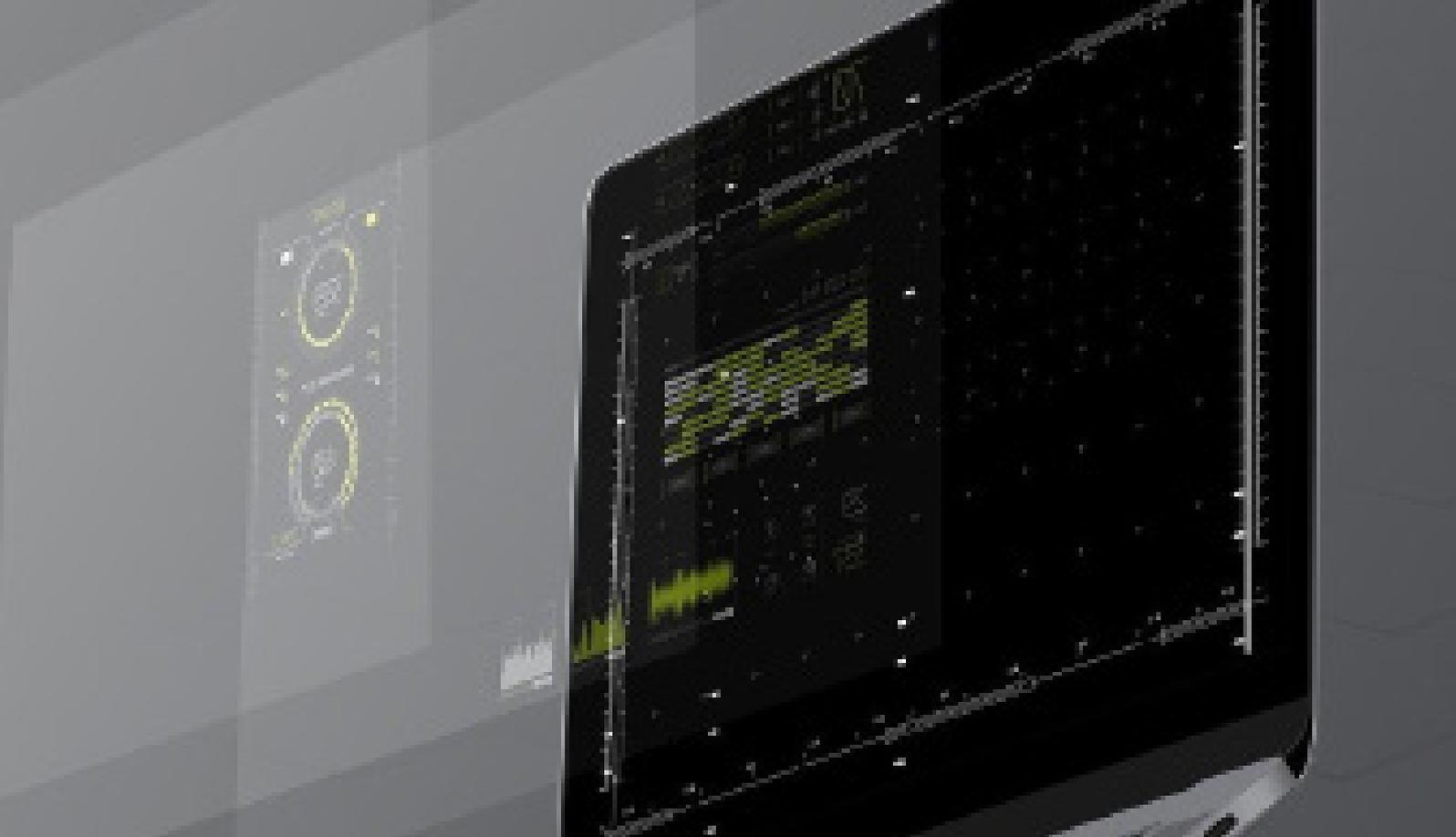
社用情報機器において業務外の目的で使用することを禁止しています。また、セキュリティ機器による通信制御も実装しています。

インターネットの閲覧

インターネットは業務目的以外での使用を禁止しています。Webページからファイルをダウンロードする場合、業務で利用するもののみ限定としています。

SNS利用

個人によるインターネット上の情報発信においては、コンプライアンス・モラルに触れる事項に配慮した内容とすることを義務としています。



情報システムの利用

システム利用者の活動、例外処理および情報セキュリティ事象を記録したログを取得します。

また、将来の調査およびアクセス制御の監視を補うために、一定期間保持します。

スマートデバイスの利用

社内システムへのアクセスやメール等を介した業務情報の保存が可能な場合、適切なセキュリティ機能が施されていないと情報の漏えい等につながるおそれがあります。

会社貸与のスマートデバイスに関して必要となるセキュリティ機能は利用ルールやセキュリティ対策の内容に応じて異なるため、適切な機能を決定し実装します。

リモートワークへの対応状況について

リモートワークは場所や時間に縛られることなく業務ができるため、とても利便性の高い働き方ですが、一方で使い方を誤ると大きな事故を起こしてしまう危険性もあります。

リモートワーク時の従業員への注意

リモートワークにおいてセキュリティの観点から注意すべき事項をチェックリストの形式でまとめて各従業員に情報セキュリティを意識させています。

- ウィルス感染対策
- 紛失・盗難対策
- 盗聴・不正アクセス対策

注意喚起の周知

リモートワーク時の注意もリモートワークの手引きと同時に周知しています。

情報セキュリティインシデント

情報セキュリティ事故または事故に繋がりがねない事象が適切に報告されず対処が行われなかった場合、事故が発生してしまったり、被害がより深刻化してしまうおそれがあります。

セキュリティインシデントまたはその疑いを発見した場合には、速やかに定められた連絡先に連絡するようルールを定めています。

技術的対策

DX(デジタル トランスフォーメーション)を推進するためには、新たな技術・サービスの導入と同時に、それらを正しく効果的に活用するための情報セキュリティ対策も極めて重要です。

深刻化しているサイバー攻撃への対策を強化しており、麒麟ホールディングス、麒麟ビールなどの主要会社において機械学習機能を備えた先進的なセキュリティ対策ツール導入などを講じています。情報セキュリティインシデントは「SOC(セキュリティ オペレーション センター)」で機械的に検知し、「KIRIN-CSIRT」と連携して、影響範囲の特定・最小化、原因分析を進めています。

海外拠点強化

サイバー攻撃などでの経済的な影響を低減するためグローバルで付保を行うなどリスクの移転も含めて対応を行っています。これらにより、一定レベル以下にリスクは低減できていると考えていますが、未知のサイバー脅威などには幅広く情報収集などを行いながら対策を講じています。

- 国内キリングroup各社に導入・蓄積したセキュリティ対策のノウハウを基に、共同利用型のセキュリティサービスを提供しています。
- セキュリティ有識者が存在せず、自社での対策が難しい海外キリングroup会社に対して、本サービスの導入および運用に関する技術的支援を実施しています。
- 国内キリングroup各社に導入している機能との共通化を図ることにより、スケールメリットを活かした低廉なサービス提供を実現しました。

アクティブ・プロアクティブな検知

機密性区分に応じた情報管理

人的もしくは機械的にセキュリティインシデントが発生していることを発見した場合、またはその疑いのある事象を発見した場合には、速やかにセキュリティインシデントの報告窓口へ連絡します。セキュリティインシデントの報告窓口が不明な場合には、セキュリティ管理者に確認し、セキュリティ管理者がモニタリングをします。

対応時の標語

セキュリティインシデントまたはその疑いを発見した場合には、速やかに定められた連絡先に連絡する

従業員端末の個別通信遮断

従業員個人が二次災害を防ぐ

従業員がインターネット通信、メール、もしくは従業員個人が不審を感じた時点で、直感的に通信を遮断し、情報システム担当へ連絡されるシステムを実装しています。

この行動を周知することにより、被疑機器からの二次災害を防ぎ、健全な事業活動を支えています。

インシデント対応方針とフロー

インシデントレベル

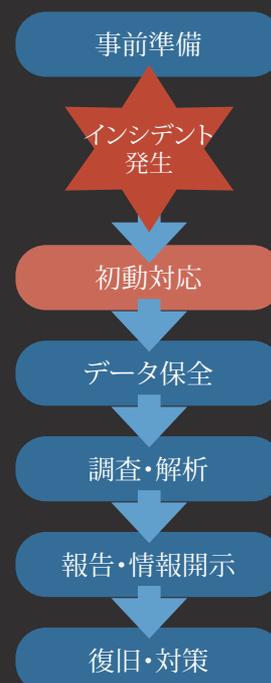
インシデントレベルを影響の大きさに応じ5段階に定義しています。

インシデント対応レベルにより情報セキュリティ管理責任者が停止判断を行います。

関連部署が参加し、意思決定をします。

さらに、状況により担当役員またはグループリスク・コンプライアンス

対応フロー



対応時の基本方針

優先順位

1. 人命(健康と安全)確保
2. 法令遵守
3. お客様の個人情報の漏洩防止、被害の最小化
4. ウイルス感染によってキリンが攻撃用の環境を提供してしまい、結果としてサイバー攻撃に関与・加担することの防止
5. 業務継続

マネージメントレビュー

情報戦略を所管するトップマネージメントへ問題発生時の連絡はもちろんとして、年複数回定期的な報告会を設けています。

この報告はセキュリティ推進に当たり、推進者側の意識の統制と、今なにが起こっているか、何をしようとしているかを、トップマネージメントと推進者の情報交流を行い全員の行動を相互牽制することを目的としています。

個人情報の取り扱いマニュアル

国内外事業会社を対象にキリングroupの情報セキュリティロードマップ、「利用基準・管理基準の整備」に従い継続的に状況を調査しています。

本報告期間では国内外の複数の拠点を対象に調査をしました。

あわせて指摘点のある拠点にはモニタリングを継続しています。

改正個人情報対応

改正個人情報保護法は2022年法改正を踏まえて対応しています。

ICT

グループ全体のDX推進に必要なデジタル時代に即したICT(インフォメーション アンド コミュニケーションテクノロジー)・データ基盤の整備も強力に進めています。

従業員のフルリモート勤務を実現するシステムやネットワークインフラは新型コロナウイルス感染症の拡大以前から整備してきましたが、2020年度にはマーケティングなどのさらなる強化に向けてDXP(デジタル エクスペリエンス プラットフォーム)を構築しました。

また、現在も社内会議のオンライン化、押印の廃止など業務の効率化を進めるとともに、より柔軟なクラウドベースの基幹システム導入を進めています。

これからも、あらゆる領域でDXの取り組みを加速していくために、グループ全体でICT基盤の構築に取り組んでいきます。



情報戦略を所管するトップマネジメントへ
問題発生時の連絡はもちろんとして、年複数
回定期的な報告会を設けています。

情報セキュリティ人財

eラーニングや体験型の研修を実施することによって、従業員が情報セキュリティに関する知識を蓄え行動・実践できるように取り組んでいます。

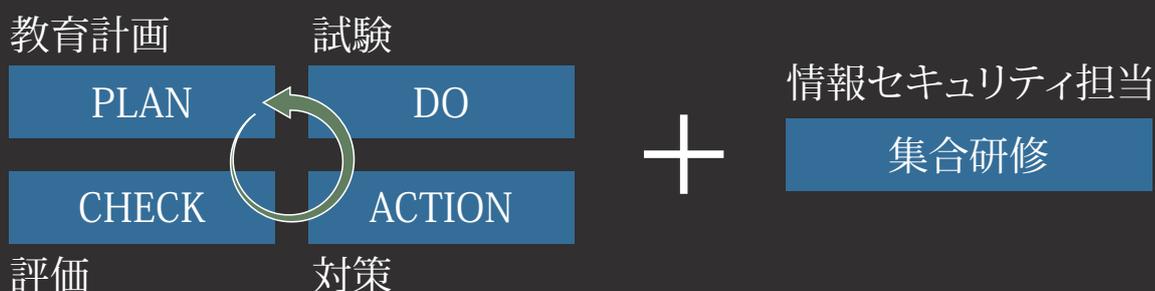
業務に応じた到達点

各業務内容により目指すべき人財像が異なります。業務や職責ごとに設定し到達を目指します。

キリングroup全社が学ぶ

キリングroupでは各種カリキュラムで各会社の情報セキュリティの意識を高めています。キリングオリジナルの教育コンテンツは毎年必要に合わせ更改し、実績から傾向を分析、対策をしています。

情報セキュリティコンテンツの更新

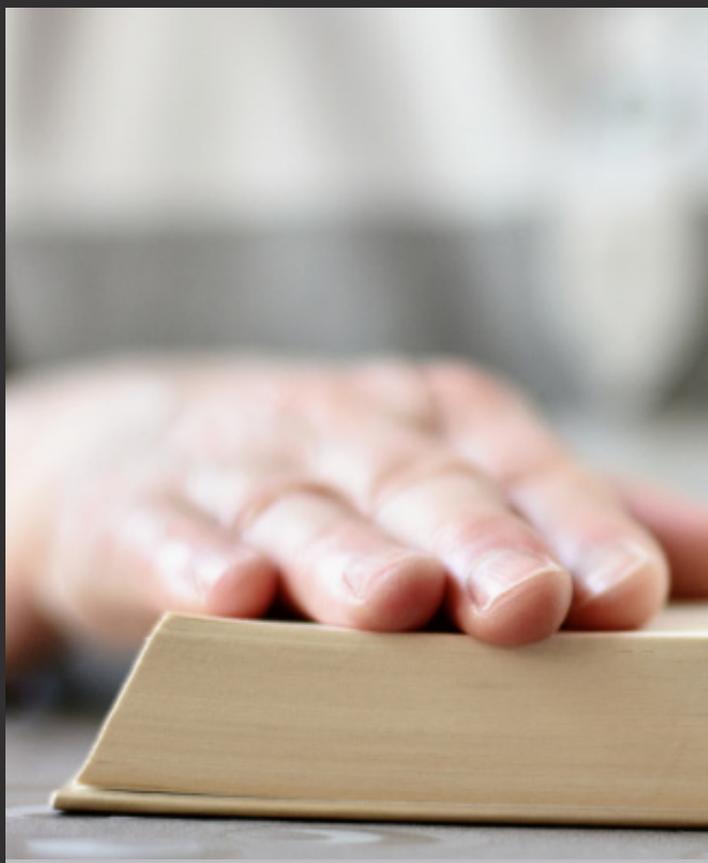


情報セキュリティ人財定義

定義	能力
認知者 複数の段階あり	<ul style="list-style-type: none"> 情報セキュリティの知識を持つ人財。 キリングgroupの情報セキュリティの規程の必要性について知っている。
理解者 セキュリティ習熟者	<ul style="list-style-type: none"> 認知者の知識を持ったうえで行動できる人財。 情報セキュリティの目的、方針、必要な行動を具体的に理解している。 情報セキュリティインシデントの有事の際の窓口として行動できる。 知識を持ち、実務として発揮できる。

人財の知識と行動

人財	知識面		行動面	
	一般知識	キリング固有	本人	本人+他人
認知者	○	○	△	—
理解者	○	○	○	△(担当場所)



約400人の情報セキュリティ担当を対象とした研修を実施

全グループ会社の「情報セキュリティ」を向上させるための方策として、「理解者研修」を実施し約400人の情報セキュリティ人財を育成しました。

育成した情報セキュリティ人財は各場所で全社施策を推進、管理していきます。

理解者研修

キリングroup独自で研修コンテンツを作成、セキュリティ知識を理解しその知識を元に行動・実践出来る人財「理解者」になる以下の力量を持つように身近な違反例を複数使用し研修を実施しました。

- 周りを巻き込み、プロセスを定着させる力
- すぐに自場所で実施可能な行動例
- キリンのマニュアルに対する理解

The image shows three screenshots of training slides for 'グループディスカッション' (Group Discussion). Each slide is titled 'KIST (Info Information Security Training) 第2部：演習パート' and 'KIRIN'. The first two slides focus on 'モノの紛失' (Loss of items) with an incident of losing a bag with documents at a friend's gathering. The risk is '機密情報が社外に流出する恐れ 社用携帯等を使用される恐れ' (Risk of confidential information leaking outside the company and using company mobile devices). The process is 'カバン等は常時持ち歩く 社用携帯等をストップで身に巻ける' (Always carry bags, etc., and wear company mobile devices with a stop). The third slide focuses on 'テレワーク時の注意' (Caution during telework) with an incident of posting new product information on SNS at a cafe. The risk is '機密情報が社外へ流出する恐れ' (Risk of confidential information leaking outside the company). The process is '信頼のあるWi-Fiを利用する 画面をのぞかれないようにする 会話の内容を聞かれないようにする' (Use trusted Wi-Fi, prevent others from seeing the screen, and prevent others from hearing the conversation).

理解者研修の反響

研修にあたり、評価とは別の自由記載のフリーコメントアンケートを用意したところ、参加者の80%の記載がありました。

担当者は前向きに取り込んでおり、情報セキュリティについて興味を強く持っていることが確認できました。



キリングroupの情報セキュリティポータルサイト

情報セキュリティポータルを設置しています。

自己学習、報告・相談・連絡を容易にし、反復学習が可能です。

また、情報セキュリティの文書類の集約や相談、問い合わせ窓口を設置しています。

キリングroupン従業員は、アクセスする事で情報セキュリティが実践できます。



キリングroupの情報セキュリティ人財育成

これまでの人財育成

キリングroupでは情報セキュリティを末端まで張り巡らせるために、各会拠点に対し、情報セキュリティ人財を配置しました。

配置された情報セキュリティの中心となる人財は周りを巻き込み、より強固な情報セキュリティの維持に取り組んでいます。

これからの人財育成

配置された情報セキュリティの中心となる人財がより行動しやすく、ひいては各場所の情報セキュリティ意識と対策を高められるように人財育成も強化していきます。

周囲を巻き込む力を強くし、各拠点の全体の情報セキュリティ意識を底上げしていきます。

情報機能専門会社の情報セキュリティ技術

情報機能専門会社の人財育成

キリングroupの情報機能は、専門の機能会社がグループ各社に最適なITサービスの提供を行っています。

その過程では、業務知識、システム知識、ITスキルに加え、先端技術の探索、活用面でもアライアンスを組んでいる(株)NTTデータの資産を利用して、事業課題の解決、IT部門の人財育成を行っています。

これからの情報機能専門会社

情報機能に対する経営からの高まる期待を受けて、専門の機能会社は次のステージへと向かうために新経営ビジョン、行動指針を見直しました。

新ビジョン「キリン×ITで社会・お客様・働く仲間のごよびを創造する企業になります」を宣言し、活動しています。

“One KIRIN” Values

キリングroupの一員として大切に考える、気持ち

2021年は情報セキュリティ人材へ情報セキュリティリモート教育を本格的にスタートさせた一年でした。この教育では各アンケートで、社内のいろいろな声をいただいています。

現場からの声

維持したいご意見(抜粋)

- セキュリティ担当者として何をすれば良いのか(一人で抱え込む必要はないという点も含め)を整理できた点が非常に良かったです。
- 昨年、異動により担当となったが、このような研修機会を設けていただき、大変ありがたいです。
- システム部門に所属していますが、ユーザー部門の意識は高く、対策も考えていることが聞いてよかったです。改めて情報セキュリティに関して意識付けするいい機会になりました。ありがとうございました。
- (理解者研修の) グループワークが楽しかったです。
- 有難うございました、定期的開催頂けると、スキル維持と実践に役立て易いと感じました。
- 明日から自場所で活用できるものもあり、提案していこうと思います。
- 対策抽出のフレームワークなど、他業務でも参考になる情報を得ることができた。
- グループワークで皆さんのアイデアを聞いたのが良かったです。
- 一般社員にもeラーニングだけではなく、こうした対話の機会が設定できるとよいのかなと思いました。

次回に向けてのご意見(抜粋)

- あまり難しい内容ではないので、もう少し実務的な対応を要求される内容にしても良いのではないかと感じました。
- 実際にインシデントが起きたあとの対応などの内容があってもよいかと思いました。
- 定期的実施するのが良いと思います。
- 担当者が認知しているところから、どう自場所に浸透したらいいのかというところはまさに共通の課題と感じているので、この機会は貴重なものと感じた。
- 簡潔な研修メニューで良かったと思います。研修を続けていくにつれ難易度を上げて良いかと思いました。その方が身に染みるので。ただ今回は非常にとっつきやすかったです。ありがとうございました。
- 見せていただいた資料を使って、例えば協力会社の人と研修したりしたいですが、可能でしょうか？
- 他の事例もワークする機会があれば良いと思いました。



Feedback



社員が気づいた問題点や
反省点、改善のアイデア



注：本報告書に掲載されているサービス名および商品名などは、キリンホールディングスあるいは各社の登録商標または商標です。

キリンホールディングス株式会社(Kirin Holdings Company, Limited)
キリンビジネスシステム株式会社 (KIRIN BUSINESS SYSTEM COMPANY, LIMITED)

〒164-0001

東京都中野区中野四丁目10番2号

中野セントラルパークサウス