情報セキュリティ

マテリアリティ設定の背景

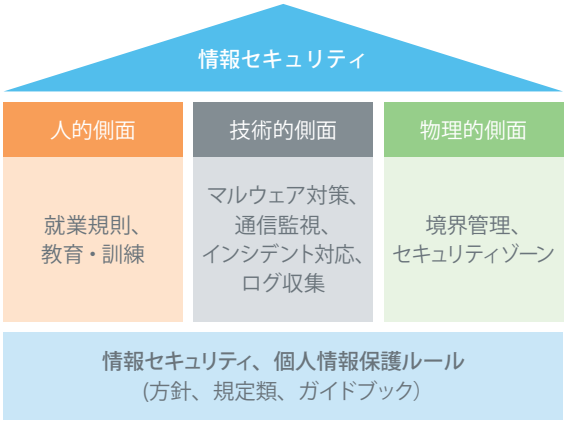
近年、企業の保有する情報をターゲットとした内部不正による情報漏えいやサイバーアタックによる企業活動停止など情報セキュリティのリスクが高まっています。

ステークホルダーの皆様に安心していただくために、ムラタの競争力の源泉となる技術情報や経営情報などの企業機密、取り扱う個人情報、取引先・お客様やパートナーからご提供いただいた情報など、ムラタの保有する情報を守ることが大切だと考え、当マテリアリティを設定しました。

目指す姿

日常的に情報セキュリティリスクマネジメントのPDCAを機能させることでリスクを最小限に抑え、その結果、重大な影響が生じ得ると判断される事案の発生がない状態を目指します。

ムラタでは2007年度からリスク管理委員会の下部組織として情報セキュリティ分科会を設置し、国際標準（ISO27001）をベースに昨今のリスク動向や国内外の関連ガイドラインを取り入れた情報セキュリティマネジメントを実施しています。具体的には「情報セキュリティ基本方針」、「情報セキュリティ管理規定」、「個人情報保護方針」を制定し、情報セキュリティ施策の整備と運用を人的・技術的・物理的の三側面から行っています。そして、新たなリスクや残存するリスクに対しては当分科会で検討し、施策立案とその実施を行っています。さらに組織内外での監査や診断により、その浸透とレベルアップも図っています。



人的側面

就業規則や従業員との誓約書に情報セキュリティに関するルールを記載するとともに国内外の役員・従業員が情報セキュリティについて理解し情報を正しく取り扱えるよう、ルールを分かりやすく解説した「情報セキュリティガイドブック」を、日本語、英語、中国語の3か国語で作成し配付しています。

また、全従業員を対象に情報セキュリティ意識を高める年次教育、フィッシングメール訓練、階層別社内研修、在宅勤務時のセキュリティ教育などを実施しています。（2021年度グローバル教育実施率※＝96% ※教育実施率＝教育実施拠点数÷全拠点数）

技術的側面

ムラタの企業機密や個人情報の漏えい、サイバーアタックによる企業活動の停止などを抑止するため、マルウェア対策、ハードウェア資産管理、ファイアウォールの構築、インターネット通信のチェックやID管理とシステムへのアクセスコントロール、現状の情報システムに対する脆弱性の診断とその対応などの対策を強化しています。

また、グローバルで各種ログを収集・監視し、セキュリティ事故になり得るインシデントへの対応体制も構築しています。特に企業活動の根幹をなす生産現場でのセキュリティ強化にも取り組んでおり、安定・安全な生産体制を維持するため、日々変化するサイバー攻撃やリスクへの対応・対策を進めています。

物理的側面

国内外の事業所・関係会社において、敷地境界では無断侵入を防ぐため、人や車両の入出門管理を常時行っています。敷地内では、機密管理レベルに合わせたセキュリティゾーンを設定し、機密性の高いゾーンにはIDカードなどによるアクセスコントロールを行うなど、社内外からの不正侵入を多重に防いでいます。また、継続的な物理セキュリティレベルの向上のため、人流制限と牽制対策に加えて、早期発見と証拠蓄積対策の視点でも運営状況を定期的に診断・監査し、事故や事故になり得るインシデントへの対応を他事業所・関係会社に水平展開する体制構築を進めています。