２０２５年２月２８日

「明治安田サイバーセキュリティ経営宣言」の公表について

明治安田生命保険相互会社（執行役社長　永島 英器）は、「明治安田サイバーセキュリティ経営宣言」を２０２５年３月１日付で制定いたしますので、お知らせします。「明治安田サイバーセキュリティ経営宣言」の全文は別紙をご参照ください。

○「明治安田サイバーセキュリティ経営宣言」制定の考え方

近年、デジタル技術の活用が進展し、生成ＡＩをはじめとする新たなテクノロジーの社会実装が進むなかで、当社を取り巻くビジネス環境は日々変化しています。サイバーセキュリティの分野においても、デジタル技術などを悪用した高度なサイバー攻撃の脅威が、これまで以上に高まり、大きな社会問題となっています。

当社では、サイバー攻撃の脅威に対するセキュリティ対策が、経営戦略として優先されるべき重要な要素であると認識しており、経営主導のもと、セキュリティ対策の高度化を能動的に推進し、組織的・技術的な対応態勢を不断かつ機動的に見直してまいります。

本宣言のもと、経営主導によるサイバーセキュリティ対策の高度化をいっそう推進し、サプライチェーン全体、ひいては社会全体のサイバーセキュリティ強化に貢献するとともに、お客さま・取引先等への信頼性向上を図ってまいります。

以　上

【ご照会先】
広報部　広報グループ　TEL 03-3283-8054

明治安田生命保険相互会社　〒100-0005 東京都千代田区丸の内2-1-1

MY Mutual Way2030

別 紙

明治安田サイバーセキュリティ経営宣言

明治安田生命保険相互会社は、サイバーセキュリティ対策を経営戦略上の重要な要素であると認識し、「明治安田サイバーセキュリティ経営宣言」（以下「本宣言」）を策定しました。本宣言のもと、深刻化・巧妙化するサイバー脅威に対し、経営主導によるサイバーセキュリティ対策の強化をいっそう推進してまいります。

１．経営課題としての認識

経営者自らが最新情勢への理解を深めることを怠らず、ＤＸを進めるうえで必須となるサイバーセキュリティを投資と位置づけて積極的な経営に取り組みます。経営者自らがデジタル化に伴うリスクと向き合い、サプライチェーン全体を俯瞰したサイバーセキュリティの強化を経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組みます。

具体的には、サイバー攻撃に対するサイバーセキュリティ対策を経営戦略上の重要な要素と位置づけ、経営レベルで定期的に議論・演習・確認を行ない、適切なリソースを配分し、経営主導で継続的にセキュリティ対策を推進します。

２．経営計画の策定と意思表明

特定・防御だけでなく、検知・対応・復旧も重視したうえで、経営計画やインシデントからの早期回復に向けたＢＣＰ（事業継続計画）の策定を行ないます。経営者が率先して社内外のステークホルダーに意思表明を行なうとともに、認識するリスクとそれに応じた取組みを各種報告書に記載するなど開示に努めます。

具体的には、経営主導の態勢強化のため、グループリスク管理責任者（CRO：Chief Risk Officer）配下にMY-SIRT（マイ・サート：MEIJIYASUDA Computer Security Incident Response Team）を設置しています。MY-SIRTでは、サイバーインシデント発生に備えた態勢の整備、24時間365日でのセキュリティ監視、定期的な演習・訓練を通じたインシデント対応能力の強化、コンティンジェンシープランの整備を実施します。また、ディスクロージャー誌等を通じてセキュリティ強化の取組みについて開示します。

３.社内外体制の構築・対策の実施

予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じます。経営・企画管理・技術者・従業員の各層における人材育成や教育を行ないます。サイバーセキュリティ対策のガイドライン・フレームワークの活用や、政府によるサイバーセキュリティ対策支援活動との連携等を通じて、取引先や委託先、海外

も含めたサプライチェーン対策に努めます。

具体的には、全従業員および各層別のセキュリティ教育・訓練を通じて全社的なサイバーセキュリティの意識向上とカルチャー醸成に努めます。また、サイバーセキュリティに係る専門組織ではキャリア採用を行ない、多様なバックグラウンドと専門知識を持つプロフェッショナル人材とともに先進技術を活用したセキュリティ対策を実施します。加えて、委託先におけるセキュリティ対策状況のモニタリング等を通じ、サプライチェーン対策に努めます。

４．対策を講じた製品・システムやサービスの社会への普及

システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努めます。

具体的には、お客さま向けサービスを安心・安全にご利用いただくために、技術の進展にともなう認証強化を図るなど、お客さまにおいてご利用可能なセキュリティ対策を充実させるとともに、不正なログインのモニタリングを実施します。また、新たなサービスの提供前には国際規格に基づくセキュリティ評価を実施するとともに、セキュリティ対策の実効性を継続的に検証します。

５．安心・安全なエコシステムの構築への貢献

関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図ります。各種情報を踏まえた対策に関して注意喚起することによって、サプライチェーン全体、ひいては社会全体のサイバーセキュリティ強化に貢献します。

具体的には、金融庁、内閣サイバーセキュリティセンター、情報処理推進機構等の公的機関に対して適時適切な連携を行なうとともに、金融ＩＳＡＣ、金融情報システムセンター、生命保険協会等の業界団体と脅威情報や脆弱性情報などの情報共有を積極的に行なうことで、社会全体のサイバーセキュリティ強化に努めます。

日進月歩で深刻化・巧妙化するサイバー攻撃の最新動向を注視し、都度対策を見直し、最新技術に基づいた対応を推進します。