情報セキュリティ基本方針

近年の情報化の進展に伴い、企業における諸活動は様々な情報システムを活用して展開されるようになりました。
情報の存在が紙を中心にしたものから大きく変貌し、あらゆる形態で保存、伝達され、それが全ての業務に使用されるようになった今日において、これらの情報を様々な脅威から適切に保護するための情報セキュリティ対策が必須となってきました。

当社の技術及び経営情報、さらに広く取引先あるいはグループ会社の重要な情報を厳格に保護すること、及び企業活動やサプライチェーンを維持し、環境・保安・品質を担保することは、企業の持続的発展を保つとともに、社会的責任でもあります。また、当社の事業活動にかかわる様々な取引先や業界団体、行政からの要求事項についても真摯に対応していく必要があります。
情報セキュリティ対策は、情報システムに対する技術的な面だけでは到底成し得ず、利用者一人一人が日々行う業務において、その重要性を認識し、情報セキュリティに関するルールを守っていかなければなりません。

情報セキュリティを確保するためには、情報機器のネットワーク接続、アクセス管理を適切に行い、コンピュータウイルス等への対策を実施することで、内外からの様々な脅威に対応することが不可欠です。また情報を社外に持ち出すときには、持ち出す情報を必要最小限にするとともに、各種記録媒体、パーソナルコンピュータ（以下「ＰＣ」という）、携帯電話等のデバイスを注意して取り扱わなければなりません。さらに電子メールによる情報送信やＰＣなどの修理・廃棄のための外部持ち出しにも細心の注意が必要です。

この基本方針の効果的な実施を確実にするため、下記を東ソーグループ　サイバーセキュリティポリシーとして定め、それに基づき「情報セキュリティ管理指針」を定め、周知徹底を図ります。

東ソーグループ　サイバーセキュリティポリシー

1. ウイルス対策ソフトの適用義務
   ・安定的に更新される「企業向けウイルス対策ソフト」の導入を徹底し、コンピュータウイルスなどによる業務停止や、ウイルス対策ソフトの老朽化による防御不能状態が無いように対策を講じること
   ・未適用デバイスは、社内ネットワークへの接続を禁じること

2. 未承認デバイスの接続禁止
   ・意図しないウイルス感染や情報漏えいを防ぐうえでも、承認が得られていないＵＳＢメモリやＰＣ等は、社内環境への接続を禁じること
   ・生産機能を有する会社においては、制御装置へＵＳＢメモリ等を接続する際には事前確認を行うこと

3. サイバーインシデント発生時の連絡義務
   ・ウイルス感染被害・情報漏えいなどが生じた場合は、速やかに東ソーＩＴ統括部及び事業責任部門へ通知すること
   ・ＩＴ統括部は解決に向けた支援を行うと共に、セキュリティ業者手配/斡旋や官公庁・警察等への届け出を行うこと

制　　定：２００７年１２月　１日
一部改訂：２０２３年１１月　１日
一部改訂：２０２４年　５月１３日
一部改訂：２０２５年　５月　１日

サイバーセキュリティ委員長