情報セキュリティ基本方針

三井住友建設株式会社および三井住友建設グループ各社（以下、両者を総称して当社グループ各社といいます。）は、高度情報通信社会を構成する一員として情報セキュリティ[注1)]の重要性を正しく認識し、事業活動における情報の適切な取り扱いに努めます。このため情報セキュリティマネジメントシステム（ISMS）を構築し、継続的に改善します。これにより、個人情報を含む情報資産の保護を確実なものとすると同時に、当社グループ各社の情報セキュリティに対する社会の信頼に応えます。

１．目的及び適用範囲

当社グループ各社の全従業者[注2)]が事業活動における情報セキュリティの重要性を正しく認識し、適切に行動することを目的とし、当社グループ各社のすべての事業活動をその対象とします。

２．経営陣の役割

当社グループ各社の経営陣は、情報セキュリティの水準を適切に保つため、本方針に基づく施策の実施に必要な経営資源を提供します。また、ISMS を運営する組織・体制を構築し、責任と権限を明確にします。

３．情報セキュリティに関するリスクの管理

当社グループ各社は、情報セキュリティに関するリスクアセスメント[注3)]の体系的な手順と評価基準を定めると共に、リスクアセスメントに基づく管理策を定め、実施します。

４．情報セキュリティ活動

１）法令および契約の遵守

当社グループ各社の全従業者は、法令、規制及び契約上の要求事項を確実に遵守します。

２）情報セキュリティ教育

当社グループ各社の全従業者に対して、ISMS 教育及び個人情報保護に関するコンプライアンス教育[注4)]を実施します。

３）安全管理措置

当社グループ各社は、個人情報を含む情報資産を重要度に応じて情報の漏えい、盗難、改ざんおよび破壊などの脅威から保護するための措置を講じるとともに、情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入します。

４）事業継続管理

当社グループ各社は、情報セキュリティインシデント[注5)]の発生またはその予兆があった場合、すみやかに報告し、適正に対応する仕組みを構築します。当社はそのための専門チームとしてCSIRT[注6)]を設置します。

当社グループ各社は、情報セキュリティインシデントに対する事業継続管理の仕組みを構築します。

５．個人情報の取り扱い

当社グループ各社は、事業活動において取り扱う個人情報を、個人情報保護法および当社グループ各社が定める社内規則等に従って、適切に取り扱います。ただし、日本国外の当社拠点およ

び当社グループ各社においては、当項は適用除外とし、各国の個人情報保護に係る法令および各国で整備した個人情報保護規則（社内規則）に従って、個人情報を適切に取り扱います。

１）個人情報の取得について

適法かつ公正な手段によって、個人情報を取得します。

２）個人情報の利用について

個人情報を取得の際に示した利用目的の範囲内かつ業務の遂行上必要な限りにおいて、利用します。また、当社グループ各社は、違法若しくは不当な行為を助長し、または誘発するおそれがある方法により個人情報を利用しません。

個人情報を第三者との間で共同利用し、または個人情報の取り扱いを第三者に委託する場合には、当該第三者につき厳正な審査を行った上で、適正な取扱いと確実な保護を実現するため、適切に監督します。

３）個人情報の第三者提供について

法令に定める場合を除き、事前に本人の同意を得ることなく、個人情報を第三者に提供しません。

４）個人情報の管理について

個人情報の正確性および安全性を確保するため、情報セキュリティ対策をはじめとする安全管理対策を実施し、個人情報への不正アクセス、紛失、破壊、改ざん、漏えい等の防止に努めます。万一当社グループ各社の取り扱う個人データについてこれらの事態が生じたときは、法令の定めに従い、個人情報保護委員会への報告や本人への通知等の適切な対応をとります。

５）個人情報の開示・訂正・利用停止・消去について

本人が自己の個人情報について、開示・訂正・利用停止・消去等を求める権利を有していることを確認し、これらの要求がある場合には、法令や慣行等に照らして適切に対応します。なお、当社グループ各社の個人情報の取り扱いに関するご意見、ご質問は、専用の窓口までご連絡下さいますようお願い申し上げます。

６．文書化及び維持

当社グループ各社は、ISMS を構築し、文書化し、実施し、かつ、システムの有効性の継続的改善を含めて維持します。

７．違反に対する処置

当社グループ各社は、従業者が本方針及び本方針に基づく規定に違反した場合は、該当する規定に基づき処分の対象とします。

2007 年 1 月 1 日　制定
2022 年 4 月 1 日　改訂
2025 年 4 月 1 日　改訂

注１）情報セキュリティ：情報の機密性、完全性及び可用性を維持すること。

機密性：認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。

完全性：資産の正確さ及び完全さを保護する特性。

可用性：認可されたエンティティが要求したときに，アクセス及び使用が可能である特性

注２）全従業者：①取締役、執行役員、役員待遇、顧問、社員、嘱託、出向受入者、派遣社員、パート・アルバイト等、当社の規則を遵守する義務のあるもの、②外注・業務委託先社員の内、一定期間継続して当社が管理する事業所内で作業を行うもの

注３）リスクアセスメント：リスク分析からリスク評価までのすべてのプロセス。

リスク分析：リスク因子を特定し、リスクを算定するためのプロセス。

リスク評価:リスクの重大さを決定するために、算定されたリスクを与えられたリスク規準と比較するプロセス。

注４）個人情報保護コンプライアンス教育：個人情報保護に関する本方針に基づく教育。

注５）情報セキュリティインシデント：望ましくない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの

注６）CSIRT「Computer Security Incident Response Team」の略語で、コンピュータに関する情報セキュリティインシデントを対応するチームを指し、インシデントが発生したときに、被害を最小化して速やかに復旧につなげることを目的に活動する。