情報セキュリティ特別約款(ISTC)

以下の情報セキュリティ条項は、MFBMおよび／またはサプライヤーの情報を保全するという共通の目的を達成するため、サプライヤーが満たすべき基準および要件を定めるものである。

I. 情報およびシステムの保全及び適切な管理

MFBMおよびサプライヤーは、両当事者間で共有されるすべての情報について、その機密性、完全性および可用性を確保するため、当該情報を善良なる管理者の注意義務をもって適正に管理し、不正なアクセス、不正な改ざん、破壊または滅失、不正な送信、漏えいもしくは開示、不正または目的外の処理、その他一切の不正使用または不当な利用から保護するものとする。かかる措置は、情報セキュリティに関する最新の技術水準および業界標準に従い、適切に講じられるものとする。

サプライヤーは、自己の管理下にあるシステム、設備、端末およびその他の資産について、MFBMのインフラストラクチャ、情報資産または業務に対し、直接的または間接的にセキュリティ上の脅威を生じさせることのないよう、合理的かつ適切な技術的および組織的な安全管理措置を継続的に講じなければならない。特に、サプライヤーは、業務に使用するすべての関連システムおよびコンピュータ機器が、マルウェア（ランサムウェア等）に感染しないこと、ならびに必要なセキュリティ対策が常に最新の状態で適用され、維持されるよう措置を講じるものとする。

II. インシデント管理

1. インシデントの通知義務

サプライヤーは、自己に発生したインシデントのうち、サプライヤーが保有するMFBMの情報の機密性、完全性または可用性を侵害し、または侵害するおそれのあるものについて、当該インシデントがMFBMの情報に関連する場合、またはMFBMに対して悪影響を及ぼすおそれがある場合には、直ちにMFBMに通知する義務を負うものとする。

かかるインシデントには、データの滅失または不正使用、マルウェアへの感染、特にMFBMの情報に対する不正アクセス（サイバー攻撃等）が含まれるものとし、また、これらのインシデントが発生したことを示唆する状況が発生した場合も含まれるが、これらに限定されない。サプライヤーは、かかるインシデントについては、遅滞なく、MFBMの担当する調達部門の窓口に対して報告しなければならない。

2. 連絡先

サプライヤーは、情報セキュリティに関する責任者を任命し、その責任者は、セキュリティインシデントおよび違反行為をMFBMに報告し、対応策および改善策を監視する責任を負う。

3. インシデント是正措置

サプライヤーは、かかるインシデント、情報セキュリティ侵害、および重大な脆弱性が遅滞なく解決されるようにしなければならない。サプライヤーは、被害軽減ともに、MFBMの情報復旧のために必要なあらゆる措置を講じるものとする。MFBMの要請に応じて、サプライヤーは詳細なインシデント報告書を提出し、セキュリティテストの結果、特定された情報セキュリティリスクおよび情報セキュリティインシデント、ならびにそれに応じて実施された是正措置または実施予定の是正措置を記載しなければならない。

III. スタッフの意識教育

サプライヤーは、MFBMの情報にアクセスする従業員および請負業者に対し、MFBMの情報の許容される使用範囲を含め、MFBMの情報へのアクセスに関するセキュリティ要件およびインシデント管理等の具体的な手順について指導するものとする。

IV. 情報セキュリティ認証

MFBMは、MFBMの情報の種類および保護要件、またはMFBMの事業運営におけるサプライヤーのサービスの重要性に応じて、サプライヤーに対し、取引関係を通じて適切なレベルの情報セキュリティ対策を講じるよう求めることがある。パートナーは、MFBMからの要請があった場合には、パートナーの事業所において確保されているサイバーセキュリティに関する認証レベルについての情報を提供するものとする。当該情報には、TISAX®（アセスメントレベル3）ラベル、ISO 27001、SOC 2等の外部認証、あるいは生産資材供給会社に適用される、かかる外部認証と同等のセキュリティ認証が含まれるものとする。MFBMは、各調達契約の範囲内で、その他全てのサプライヤーに対しても同等の認証情報を要求できるものとする。両当事者は、各証明書および情報セキュリティの適切なレベルに関する変更された要件に従い、対象拠点の初期監査に必要な合理的な期間を合意できる。

V. 監査する権利

MFBMは、MFBMの情報セキュリティ要件との整合性を確認する目的で、事前の通知および相互の合意を条件として、サプライヤーのサイバーセキュリティ対策について評価および監査を実施する権利を有するものとする。当該評価および監査には、認証の有効性ならびにその実装および運用の有効性の確認が含まれるものとするが、これに限定されるものではない。合意済情報セキュリティ要件の実施および維持に対する違反、情報セキュリティインシデントの存在を認識した場合、またはそのような違反を疑う合理的な理由がある場合、MFBMは情報セキュリティ要求事項および合意済追加情報セキュリティ要件の遵守状況を確認（以下「監査」という。）する権利を有する。サプライヤーは、監査に必要な範囲で、必要な情報の提供に協力するものとする。MFBMは、通常の営業時間内に適時に通知した上で、可能かつ合理的な範囲で、業務プロセスを中断することなく、契約者の施設（関連するITシステムを含む）を監査し、合意された技術的および組織的措置が遵守されていることを確認できる。その際、MFBMは、サプライヤーの第三者に対する守秘義務を遵守するものとする。MFBMは、第三者に対して同様に守秘義務を負う外部の有資格会社に監査を実施させる権利を有するものとするが、当該有資格会社は、サプライヤーの競合会社でないことを条件とする。これは、MFBMが有する監査権および情報に関する権利を制限または排除するものではない。