サプライヤー情報セキュリティガイドライン

２０２６年２月

株式会社イノアックコーポレーション

はじめに

本ガイドラインは、株式会社イノアックコーポレーションおよびその関連会社（以下「当グループ」）が、サプライヤーの皆様（以下「サプライヤー」）に対して要請する情報セキュリティ対策を定めたものです。

当グループは、機密情報の適切な管理を徹底することにより、安定した事業継続を確保し、当グループ、サプライヤーの皆様、ならびに社会全体の持続的な発展を目指します。

当グループの情報セキュリティへの取り組みに対する、皆さまのこれまでのご協力に感謝申し上げますとともに、サプライヤーの皆様には、本ガイドラインの趣旨についてより一層のご理解とご協力を賜りますよう、お願い申し上げます。

株式会社イノアックコーポレーション
情報セキュリティ委員会

第１条　目的

本ガイドラインは、当グループとサプライヤーが、サプライチェーン全体における情報セキュリティリスクを適切に管理・低減することを目的として、遵守すべき共通的な考え方および基本事項を定めるものである。

なお、本ガイドラインは、経済産業省等が推進するサプライチェーンセキュリティ強化の考え方を踏まえ、取引内容やリスクに応じて段階的に適用されることを前提とする。

第２条　適用範囲

１、本ガイドラインは、当グループの事業に関連して、サプライヤーが所有、管理、または処理するすべての情報資産に適用されるものとする。

２、当グループの事業に関与するすべてのサプライヤーは、本ガイドラインの趣旨を理解し、その内容を遵守しなければならない。

３、本ガイドラインに基づく具体的な要求水準および適用範囲については、取引内容、取り扱う情報の機密性、システム接続の有無、事業継続への影響度等を考慮し、当グループが準拠する自工会／部工会・サイバーセキュリティガイドライン（2.3版　2025年9月1日）、ならびに経済産業省等が推進するサプライチェーンセキュリティの考え方を基準として、当グループが定めるものとする。なお、サプライヤー評価制度の改定、自工会チェックシートのバージョンアップその他関連する外部ガイドライン等の変更に伴い、本ガイドラインに基づく要求内容および運用方針は、将来変更されることがある。

４、このガイドライン実施日において、すべてのサプライヤーは、当グループが別途指定する日までに、自工会チェックシートにおけるLV1の項目への対応を行う。ただし、当グループが定める重要度判定の結果に基づき、必要と判断した場合には、LV2までの対応を行う。

第３条　情報資産

本方針における情報資産とは、当グループの事業に関するすべての情報、ならびにその情報を支えるシステム、デバイス、ネットワーク、アカウントおよび物理的資産を指す。

これには、電子的形式、紙媒体、物理的媒体およびクラウド環境に保存または提供される情報が含まれる。情報資産は、適切な管理および保護が求められる重要な資産であり、サプライヤーはその安全性の確保に必要な措置を講じなければならない。

第４条　機密区分

情報資産は、漏えい、改ざん、または利用不能となった場合に当グループの事業、取引先、または社会に及ぼす影響の大きさを考慮し、機密区分を設定しなければならない。

機密区分は、情報の機密性、完全性および可用性の観点から定めるものとする。

また、当グループから提供した情報で、あらかじめ機密区分が設定されているものについては、当該区分に準拠した区分を設定しなければならない。

サプライヤーは、設定した当該機密区分に応じて、情報資産を適切に取り扱わなければならない。

第５条　経営の責任

経営層の関与のもと、組織的かつ継続的に情報セキュリティの改善および向上に取り組まなければならない。

第６条　体制

情報セキュリティの維持および改善に向けて、必要な施策を組織的に推進しなければならない。

当該責任者は、その責任範囲において情報セキュリティ施策の検討および実施を担い、適切な管理が行われる体制を定めなければならない。

その体制として、情報セキュリティ責任者として、組織内において十分な権限および意思決定能力を有する者（取締役会等によって指名されたものが望ましい）を任命しなければならない。

また、当該責任者が情報セキュリティ施策を実施し、組織全体に対して指揮監督を行うために必要な業務分掌を確保する。

第７条　教育

すべての従業員が、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにするため、定期的な情報セキュリティ教育及び啓蒙活動を実施しなければならない。

第８条　事故発生時の対応

１、連絡体制の整備

サプライヤーは、情報セキュリティ上の事故またはサイバーインシデント（以下「インシデント」という。）の報告を受け付ける社内外の連絡窓口を明確にし、必要な連絡体制を整備しなければならない。

２、社内連絡ルートの確立

インシデント発生時に迅速な対応が行えるよう、情報セキュリティ体制内における連絡ルートをあらかじめ定めておかなければならない。

３、外部機関との連携

インシデント対応において必要となる外部機関（法執行機関、専門機関等）の連絡先については、あらかじめ整理し、備えておくとともに、定期的に内容を確認し、最新状態を維持しなければならない。

４、インシデント発生時の通知

サプライヤーがインシデントを検知または把握した場合には、速やかに（目安：24～48時間以内）当グループの取引担当者へ連絡し、状況の共有を行わなければならない。特に、当グループの機密性の高い情報が関与するおそれがある場合には、一層迅速な連絡および対応を行わなければならない。

５、調査および協力

インシデント対応に関して、原因究明や影響範囲の確認のため、必要に応じて調査を実施しなければならない。

また、当グループから要請があった場合には、事故の概要、影響範囲、暫定対策および再発防止策等について、合理的な範囲で調査への協力や必要な情報提供を行わなければならない。

６、再発防止

インシデントが発生した場合には、再発防止策を当グループとの協議のもと策定し、速やかに実施しなければならない。

第９条　委託先管理

1、当グループ極秘情報の再委託に関する基本事項

再委託先への極秘情報の提供については、当グループの事前の書面による了解を得ることなく行ってはならない。

2、再委託先における管理状況の確認

再委託先に極秘情報を提供するにあたっては、本ガイドラインと同等レベルの情報セキュリティ管理を求めるものとする。

また、再委託先がさらに第三者へ再委託する場合についても、同様の管理が確保されるよう確実に履行させなければならない。

第１０条　情報セキュリティに関する調査に基づいた是正依頼への対応

当グループは、情報セキュリティの確保および継続的な改善のため、必要に応じてサプライヤーに対し情報セキュリティに関する調査（以下「監査」という。）を実施する。

監査の有無、頻度、範囲および方法については、当該サプライヤーのリスク特性（情報の機密性、取扱量、再委託の有無、過去の不適合状況等）を踏まえ、合理的に判断するものとする。当グループは必要に応じて事前通知の下、現地監査、リモート確認、書面提出等の方法を適宜組み合わせ、効率的かつ実効性のある方法により監査を実施することができる。

サプライヤーは、監査に対し、必要な資料の提出、担当者への説明、現場確認等に誠実に協力しなければならない。
監査の結果、改善が必要と判断される事項が確認された場合、当グループは是正対応を要請することがある。サプライヤーは、当該要請があった場合、可能な限り速やかに対応しなければならない。特に、当グループの機密性の高い情報の保護に直接影響を及ぼす事項が確認された場合には、重大な不適合として、原則14日以内に実施計画を当グループに共有し、速やかに実行しなければならない。なお是正が完了するまでの期間、定期的に当グループに対策状況を共有しなければならない。
指摘事項があった場合には、（１）是正策の検討・作成、（２）是正策および実施計画の当グループへの報告、（３）当グループの承認を得たうえで、対応実施を行わなければならない。
是正対応の進捗状況および対応内容については、適切に報告しなければならない。また、当グループは、是正の有効性を確認・評価するため、必要に応じてフォローアップ調査（再確認）を実施することができ、サプライヤーはこれに協力しなければならない。
なお、改善が合理的期間内に実施されず、当グループの事業継続や情報保護に支障が懸念される場合、当グループは、取引の方法や範囲の見直し、当該情報の取扱いの停止、その他必要な措置を講じることができる。

以上