# NSG グループ情報セキュリティに関するポリシー

| 一般事項 | |
|---|---|
| ポリシー表題 | 情報セキュリティに関するグループポリシー |
| 承認者 | CEO |
| 承認日 | 2025 年 12月 23日 |

| | |
|---|---|
| **ポリシーの目的** | 本文書は、NSGグループの情報セキュリティポリシーを定めるものである。本ポリシーは、グループの情報セキュリティに関する包括的なポリシーである。<br>情報セキュリティは、情報及び情報システムを不正なアクセス、使用、開示、中断、変更又は破壊から保護することによって達成されるものである。これは、関連する法律、規制および契約上の義務に従い、グループの資産ならびに顧客、従業員またはグループの代理人ために収集、保管、転送または処理されるすべての情報の機密性、完全性、可用性を提供するために行われる。本ポリシーは、電子的、物理的、無形のあらゆる形態の情報（知識など）に適用される。 |
| **適用範囲** | NSG グループ 情報 セキュリティポリシーは、以下に適用される。<br>・ NSG が経営を管理するグループ内すべての地域およびすべての国の、全NSG グループ会社（合弁会社および関連会社を含む）とその従業員。<br>・ NSG グループの情報システムを直接的または間接的にサポートおよび/または使用する第三者組織、およびその従業員。 |
| **定義** | OT（オペレーショナルテクノロジー）とは、工場や物流業務における機械や設備といった物理的プロセスを制御・監視するために使用されるシステムを指す。<br>ICS（産業用制御システム）とは、OTの一種であり、生産ラインやエネルギーシステムなどの産業プロセスを管理・自動化するために使用される。 |
| | |

| | |
|---|---|
| **ポリシーの詳細** | **情報セキュリティの目的**<br>情報セキュリティの目的は、本ポリシーに従って組織における戦略的なビジネス目標を実施し、かつ想定通りに機能しているかどうかを判断するための助けとなる。<br><br>情報セキュリティの目的は以下の通りである。<br><br>・ビジネスとの整合性 -情報セキュリティは、NSGグループのビジョン、使命、および中期経営計画における戦略的優先事項を支援する。そのため、安全な事業成長、デジタルトランスフォーメーション、サステナビリティ施策を促進し、NSGグループのすべての施策において、設計段階から情報セキュリティ要件を評価・統合するための適切なワークフローを実装する。<br><br>・遵守と義務 -情報セキュリティ、データ保護、データプライバシーに関する適用法令、規制、契約上の要件、および社内基準を遵守する。遵守状況は、各基準で要求されるレビューサイクルに沿って、当該プロセス責任者、コンプライアンス部門、監査部によって評価される。<br><br>・情報セキュリティポリシーと組織 - NSGグループは、NSGグループの情報セキュリティに対する姿勢を支援する全文書が最新かつ適合状態に保たれていることを確認し、これらを情報セキュリティポータル上に公開する。<br><br>・人的資源 - NSGグループは、NSGグループの従業員・代理人に対し、情報セキュリティトレーニングを実施し、トレーニングの進捗率を追跡することで、品質と遵守状況を定期的に監視する。進捗率が設定した最小値に達していない場合、必要に応じてNSGグループの従業員・代理人を追跡し、ガバナンスフォーラムに報告する。<br><br>・IDとアクセス管理 -知的財産、事業運営データ、個人情報を含むNSGグループの情報資産の機密性、完全性、可用性を確保し、無許可のアクセス、開示、変更、破壊から保護する。そのため、正当な関係者が適切なタイミングで、適切な情報源に適切にアクセスできるようにするとともに、プロセスと制御を実装する。 |

・リスクと監査–リスク指向のアプローチにより情報セキュリティを管理し、重要な資産に対するリスクを特定・評価し、それらを軽減するために適切な制御を適用する。NSGグループの全社的リスクマネジメントに従い、顧客、監査部または外部監査人に指摘された情報セキュリティの不適合が定義されたリスク処理および軽減策に基づいて対処されていることを年1回確認する。

・データの分類 – すべての情報資産を、その機密性および事業価値に応じて、特定・分類・ラベル付けするための体系的なプロセスを実装・維持する。これにより、情報ライフサイクル全体を通じて適切な保護措置が適用され、法的、規制上、契約上の要件に沿って機密性、完全性、可用性が確保される。

・事業所セキュリティ –すべての製造および物流拠点がOT/ICS環境を保護し、サプライチェーンのセキュリティを強化し、事業継続を支援するための最低限のベースラインセキュリティ制御を確立し、維持する。

トップマネジメントコミットメント

NSGグループは、高度な情報セキュリティの維持に努め、NSGグループの経営会議で承認を受けた情報セキュリティ体制を確立している。

CDIOは、IT環境全体における規制遵守およびリスク管理を維持するために、遵守すべきデジタル関連ポリシー、スタンダードおよびコントロールを策定する。

CDIOは、既存のデジタル資産・サービスの変更、および新規デジタル資産・サービスの導入を統制し保証するために、規模・所在地・資金源を問わず、リスク、実行可能性、価値およびコストを評価する補完的な変更管理プロセスを実装する。

総コスト（資本的支出および/または収益的支出）が0.1億円を超える大規模なデジタル施策については、すべてのデジタル投資の価値を最大化するために、CDIOがデジタル投資ポートフォリオ（DIP）プロセスの定義および運用に責任を負い、デジタル技術の設計（テクノロジーアーキテクチャ）、選定および実装を統制する。DIPプロセスは、すべてのSBUおよびファンクションに適用され、デジタル投資の価値最大化を図るものである。

**本ポリシーの遵守について**

本ポリシーの遵守は必須である。 NSGグループのすべての従業員または代理人は、個人として本ポリシーを遵守する責任を負い、必要に応じて、更なる明確化のために、NSGグループデジタル部門の指導を受けなければならない。NSGグループデジタル部門が例外として認めた場合を除き、本ポリシーからの逸脱を禁止する。NSG グループデジタル部門は、セキュリティポリシーからの全適用除外事項を登録する。

NSGグループデジタル部門は、グループ全体で本ポリシーを遵守するために、適切な仕組みを確立する責任を負う。 本ポリシーの遵守状況は、検査、監査および/または書面による遵守確認の要請を通じて、監視される場合がある。

ポリシーのレビュー担当者および承認者は、その責任範囲内で本ポリシーの遵守状況を定期的に評価する責任を負う。本ポリシーへの違反が判明した従業員または NSGグループの代理人は、懲戒処分ポリシーに含まれるプロセスに従い、懲戒処分の対象となる場合がある。

**NSGグループの従業員または代理人の責任**

NSGグループの従業員または代理人は、日々の業務が情報セキュリティポリシー、基準、およびプロシージャーに準拠するようにしなければならず、情報セキュリティポリシーが遵守されていることを毎年、確認しなければならない。

**情報セキュリティの継続的な改善**

情報セキュリティポリシーに使用される情報セキュリティ重要文書は、NSGグループのニーズを満たすために、少なくとも年1回、レビューされる。

レビューでは、グループの組織やシステムの変更、関連する法律や規制の変更などを考慮しなければならない。

情報セキュリティポリシー、基準およびプロシージャーの独立したレビューは、少なくとも年1回実施されなければならない。

**セキュリティポリシー**

| | |
|---|---|
| | NSGグループデジタル部門は、情報セキュリティポリシー、基準およびプロシージャーを承認・公開し、NSGグループのすべての従業員、代理人および関連する社外関係者に周知しなければならない。<br><br>**サードパーティーのセキュリティ**<br>NSGグループ又は顧客の情報の収集、取扱い、処理および／または保存するためにアクセスできるサードパーティーに対して、当グループの情報セキュリティ管理プロセスを定義したサードパーティーセキュリティ保証プログラムが実施されていなければならない。サプライヤーによる組織の資産へのアクセスに関連するリスクを軽減するための情報セキュリティ要件は、サプライヤーと合意し、文書化するものとする。<br><br>NSGグループデジタル部門は、契約事業部門に代わって、サードパーティーをサポートしなければならない。 |
| | |
| | |
| | |
| **変更履歴** | • 2023年3月31日　CEOによる承認<br>• 2024年3月17日　CEOによる承認<br>• 2025年12月23日　CEOによる承認 |