グループセキュリティ方針作成の解説書

グループセキュリティガイド【別紙 1】

このページは空白です。

はじめに

本書は、「グループセキュリティガイド」（以下「ガイド」という。）の別紙 1 である。ガイドが企業グループ全体のセキュリティ推進の全体像と提言を示すのに対し、本書はその第一歩であるグループセキュリティ方針の作成方法を、記載項目・記載例・テンプレートの形で具体的に解説するものである。

本書は、社内ルール体系における方針の位置づけ（1 章）、方針の公開・周知の方法（2 章）、方針に記載する項目（3 章）を解説し、付録として方針のテンプレート（内部展開用・外部公開用）を収録している。

本書は、企業グループの中の親会社においてグループセキュリティに関わる業務を行う実務担当層を主な読者として想定しており、適用範囲はガイドに準ずる。

免責事項は以下のとおり。

- 本書は単に情報として提供され、内容は予告なしに変更される場合がある。
- 本書に誤りが無いことの保証や、商品性または特定目的への適合性の黙示的な保証や条件を含め明示的または黙示的な保証や条件は一切無いものとする。
- 本書に記載の内容は、独立行政法人情報処理推進機構（IPA）および産業サイバーセキュリティセンター（ICSCoE）の意見を代表するものではなく、作成者の見解に基づいている。
- 本書の利用によるトラブルに対し、本書作成者ならびに監修者は一切の責任を負わないものとする。
- 本書の有効期限は、発行日から 2 年間とする。

目次

1. 社内ルールの体系構造

本書では、企業における社内の規程類を、方針（ポリシー）、規程、運用手順・ガイドラインの 3 つに分類する。

- **方針（ポリシー）**：組織が目指す方向性や理念といった、上位に位置づけられる文書。抽象性が高く、経営層からのメッセージが込められる文書である。
- **規程**：方針を実現するための具体的なルールを定める文書である。
- **運用手順・ガイドライン**：規程をさらに実務レベルに落とし込んだ参照文書。推奨事項や具体的な作業手順を示し、担当者が迷わず行動するために用いる。

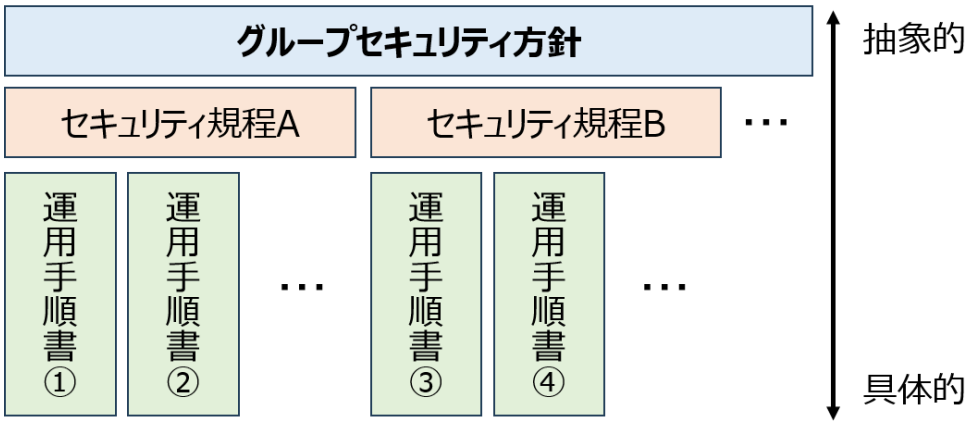

図 1-1：方針、規程、運用手順・ガイドラインの関係図

本書が解説の対象とするのは、このうち最上位に位置づけられる方針、すなわちグループセキュリティ方針である。

なお、グループにおいては、グループセキュリティ方針がこの階層の最上位に位置し、グループ各社（親会社を含むグループ各会社をいう。以下同じ。）は本方針に基づいて自社の規程を整備する（3.3.3 参照）。

1.1 方針と経営方針・経営理念との関係

セキュリティ方針は、単独で存在するルール文書ではない。組織の経営理念・経営方針を上位概念として、それを情報セキュリティの観点から具体化したものと位置づけられる。

たとえば、経営理念として「顧客からの信頼を礎に事業を営む」を掲げる組織であれば、セキュリティ方針はその信頼を技術・組織・人の面から守るための経営の意思表明として機能する。経営方針に「コンプライアンスの徹底」や「リスク管理の強化」が含まれる場合も同様に、セキュリティ方針はその実践的表明となる。

このように方針は経営と直結しているため、経営層が自ら承認・制定することが重要である。グループセキュリティ方針においては、グループ全体の経営理念・グループ経営方針との整合を明示したうえで、グループ各社が準拠すべき原則を定めるという構造を取ることが望ましい。

2. 方針の公開・周知方法

本章では、親会社として策定する「グループセキュリティ方針」について、その公開方法・範囲をどのように設定すべきかを検討する。方針をグループ内に周知する方法についても本章で触れる。

方針を「外部へ Web サイト等で一般公開」するのか（外部公開）、「グループ内（従業員・役員）限定の公開」にとどめるのか（内部展開）は、親会社が負う社会的責任、ステークホルダーへの開示姿勢、およびグループガバナンスの実効性に直結する重要な経営判断となる。本章では、それぞれのパターンのメリット・デメリットを整理し、自社グループに最適な公開方法を選択するための判断軸を解説する。

2.1 公開パターンの比較（メリット・デメリット）

親会社の方針公開における、主な 2 つの公開パターンの特徴、メリット、および想定されるリスクは次のとおりである。

表 2-1 公開パターンの比較

公開パターン	メリット	デメリット
外部公開	■ 社会的信用の向上 株主、取引先、顧客に対して、親会社がグループ全体のセキュリティを主導している姿勢を示し、強い安心感を与えられる。 ■ ESG・ガバナンス開示（IR）への貢献 非財務情報として、セキュリティガバナンスへの取り組みを市場に透明性高くアピールできる。 ■ サプライチェーン上の優位性 顧客や市場からセキュリティ体制の提示を求められた際、公式な方針として即座に証明できる。	■ 情報漏えい・偵察活動への加担リスク 記述が具体的すぎると、グループ全体のセキュリティ体制の弱点や管理対象、採用しているフレームワークを攻撃者に推測される恐れがある。 ■ 形骸化時のレピュテーションリスク 公表している方針と、グループ内の実際の運用実態（またはインシデント発生時の対応）に乖離があった場合、社会的な批判や信頼失墜のリスクが大きくなる。
内部展開	■ 実効性の高い具体的な記述が可能 外部への情報漏えいを気にせず、親会社とグループ会社の責任分担、統括責任者の設置と権限、セキュリティ業務の業務化など、グループ統治に踏み込んだ項目（3.4 参照）を方針に明記できる。	■ 外部への「証明コスト」の増大 取引先、監査機関、株主などから「セキュリティ方針」の提示を求められた際、その都度開示手続きや要約版の個別作成が必要になり、業務負荷が増大する。

公開パターン	メリット	デメリット
内部展開	■ セキュリティリスクの低減 組織の内部構造やグループ統治の内容が外部に露出しないため、攻撃者にヒントを与えない。	■ 社会的アピールの機会損失 セキュリティへの先進的な取り組みが外部から見えにくくなるため、企業ブランディングや市場（IR）におけるプラス評価を得られにくい。

2.2 親会社としての方針選択の軸（判断基準）

親会社として最適な公開方法を経営層や法務部門と合意形成するにあたり、以下の 2 つの判断軸に照らし合わせて検討を行うことを推奨する。

軸①市場（IR）およびステークホルダーからの開示要求の強さ

上場企業として、あるいはグローバル市場において、非財務情報（ESG やコーポレートガバナンス）の一環として、セキュリティへの取り組み姿勢の開示がどれほど強く求められているか。

軸②サプライチェーンにおけるポジションと社会的責任

自社グループがサプライチェーン全体の「頂点」として、顧客や社会に対して模範となるセキュリティ方針を宣言・提示する必要性がどれだけ高いか。

2.3 参考：「ハイブリッド型」の検討

外部公開のメリット（市場へのアピール・信用獲得）と内部展開のメリット（実効性と機密性）を高いレベルで両立させるため、親会社が方針を策定するにあたっては「ハイブリッド型」の採用が有効である。

・外部向け（Web サイト等）

内部展開用と同じ項目を保ちつつ、記述の抽象度を上げ、対外的な宣言の形（当グループは～します）に書き改めたグループセキュリティ方針を公開する。

・内部向け（グループ内限定）

親会社とグループ会社の責任分担、統括責任者の設置と権限、セキュリティ業務の業務分掌への明記といったグループ統治の項目（3.4 の内容）を盛り込んだ「グループセキュリティ方針」を構築し、グループ内の統制に用いる。なお、具体的な体制図や手順は、方針ではなく下位の規程等に定める。

このように、文書の目的と対象に応じて「外部公開用」と「内部展開用」を切り分けるアプローチは、親会社のブランド防衛と確実なガバナンス推進を同時に達成するための現実解となる。

なお、いずれの公開方法を選ぶ場合も、方針がグループ内に定められ、機能していることが出発点となる。3 章の記載例は内部展開を前提とした規範の形で示しており、これをまとめた内部展開用のテンプレートを付録 A に、外部公開用に抽象度を上げた宣言型のテンプレートを付録 B に示している。

3. グループセキュリティ方針へ記載する項目

本章は、グループセキュリティ方針への具体的な記載事項を解説する。本章は、方針の目的（3.1）、対象範囲（3.2）、方針に記載する項目とその説明（3.3）、なぜなぜ分析から導いた項目（3.4）の順で構成される。3.3 で述べる項目は、多くの企業に共通するものであり、グループセキュリティ方針には、原則としてこれらすべてを記載する。3.4 は、本プロジェクトで独自に実施したなぜなぜ分析から導出した項目であり、自社グループの状況に応じて項目を選択する。

本章の並びは、完成する方針の構成にそのまま対応する。すなわち方針は、冒頭に目的および対象範囲を置き、その後に、共通して記載する項目（3.3 の 9 項目）と、自社グループの状況に応じて選択する項目（3.4 の 4 項目）を並べる構成となる。

各項目では、方針に記載する要素のうち、必ず記載するものを「必須」、自社グループの判断で記載するものを「任意」と示している。
また、各項目には、方針にそのまま適用できる記載例を示す。記載例を自社グループの状況に応じて変更する場合は、あわせて示す差し替え注記を参照されたい。

各項目の記載例は、グループ内への展開（2 章で述べた内部展開）を前提とし、グループ内に適用する規範の形（～する）で書いている。これらをまとめた内部展開用のテンプレートを付録 A に、外部公開用のテンプレートを付録 B に示す。公開方法の考え方は 2 章を参照されたい。

グループの統治のあり方（親会社がどこまで統制し、各社にどこまで委ねるか）には類型（集権型・連邦型等）が存在し、これはガイドで説明される。本方針および本章の記載例では、特定の類型を前提とせず、いずれの類型でも通用する形で記載する。

3.1 グループセキュリティ方針の目的

概要

方針の冒頭には、この方針を何のために定めるのかという「目的」を置く。本節では、その目的に何を書くかを解説する。各社のセキュリティ基本方針が自社の情報資産を守ることを目的とするのに対し、グループセキュリティ方針はグループ全体でセキュリティの方向性をそろえることを目的とする。この違いを意識して目的を記述する。

解説

方針の役割（必須）

この方針は、グループ共通の方向性を定める文書である。各社がそれぞれの判断でセキュリティ対策を決めると、グループとしての足並みがそろわない。目的の冒頭で、グループ全体の方向性をそろえることがこの方針の役割であると明確にする。自社グループで特にそろえたい点（対策の水準、用語の統一等）があれば、あわせて書き加える。

グループ全体を適用範囲とする根拠（必須）

グループで共通の方針を持つ根拠は、グループ会社へのサイバー攻撃が親会社・グループ全体に波及するという構造にある。グループ会社は親会社に比べてセキュリティの人員や予算が限られることが多く、それによる対策の不備が攻撃の入口となり、ネットワーク接続や事業関係を通じて親会社をはじめとするグループ全体に被害が及ぶ。つまり一社の対策不足はその会社だけの問題にとどまらず、グループ全体のサイバーリスクとなる。この波及の構造を、自社グループの言葉で具体的に記述する。

特記事項（任意）

自社グループが重視する観点を、目的に加えてもよい。例として、事業の継続を確保すること、顧客や取引先からの信頼を維持すること、グループ各社が共通して満たすべきセキュリティ対策の水準（対策の到達度）を定めることなどである。これらは自社グループの事業特性によって重みが異なるため、必須ではなく任意とする。

記載例

> 本方針は、〇〇グループ（親会社および全グループ会社をいう。以下同じ。）の情報セキュリティを確保するための基本的な方向性を定めるものである。グループを構成するいずれかの会社における対策の不足は、ネットワークや事業上のつながりを通じてグループ全体に影響を及ぼし得る。本方針は、こうしたリスクを低減するため、グループ全体でセキュリティ対策の方向性をそろえ、各社が事業活動において取り扱う情報資産をサイバー攻撃をはじめとする脅威から保護することを目的とする。

差し替え注記

- 特記事項を加える場合
  「また、セキュリティを確保することにより、事業の継続および顧客・取引先からの信頼の維持を図る。」等を目的に追記する。
- セキュリティ対策の水準を定める場合
  「当グループは、グループ各社が共通して満たすべきセキュリティ対策の水準を定め、その確保を図る。」等を目的に追記する。
- 「グループ」「グループ会社」の定義は、3.2 の対象範囲における定義と必ず整合させる。
- 自社の波及経路を具体的に記す場合
  「特に、親会社と各グループ会社を接続するネットワークを通じて……」のように、波及の経路を自社グループの実態に置き換える。

3.2 グループセキュリティ方針の対象範囲

概要

方針が「誰に・何に適用されるか」を、組織・人・情報資産の 3 つの面から定める。適用対象を曖昧にすると、グループ会社が自社は対象外であると解釈する余地が生まれる。これを防ぐため、適用の範囲を明確に記述する。

対象範囲で記載すべき内容の全体像

記載項目	必須/任意	記載例	自社で検討する点
組織の範囲	必須	親会社およびグループ会社	合弁会社・海外現地法人・持分法適用会社を含めるか
対象者	必須	業務上、情報資産に触れる全関係者（雇用形態を問わない）	委託先社員を方針の対象に含めるか
対象とする情報資産	必須	自社グループで取り扱う情報資産を対象とする	守る対象をどの粒度で列挙するか
制御系（OT）の扱い	任意	（OT 保有時）対象に含める	方針の対象とするか

解説

組織の範囲

記載例は「親会社および全てのグループ会社」である。ただしグループには、連結子会社のほかに持分法適用会社、合弁会社、海外現地法人など、親会社の統制の度合いが異なる会社が含まれる。完全子会社には方針をそのまま適用できるが、合弁会社は相手先との契約があるためグループ会社すべてへの一律の適用が難しい場合がある。担当者は、自社グループの会社についてこの観点で棚卸しを行い、一定の基準（議決権比率・事業上の重要度など）のもと対象となる会社を決定し、方針に明記する。

対象者

正社員・役員に限らず、契約社員、派遣社員、さらに業務で情報資産に触れる委託先の社員まで含めるかを決める。グループ会社の業務が外部委託や派遣に依存していることも多く、雇用形態で対象者を決定するのではなく、情報資産にアクセス可能かで対象者を決定した方がよい。

対象とする情報資産

情報資産には、電子データや紙の文書など様々な形のものが含まれ得るが、何を情報資産とするかは各社の事業や取り扱う情報によって異なる。そのため、方針では情報資産を対象とすることを示すにとどめ、具体的な定義および分類は下位の規程に委ねる。

制御系（OT）の扱い

OT はグループ会社固有の重要なリスク源となるため、保有するグループでは対象

に含める。一方、OT 環境を持たないグループでは記述する必要がないため、必須ではなく任意とする。

記載例

> 本方針は、〇〇グループを構成する親会社および全てのグループ会社（以下、これらを総称して「グループ各社」という。）に適用する。また、これらの会社の従業員、役員ならびに雇用形態を問わず業務上、情報資産を取り扱う全ての者（派遣社員、業務委託先の要員等を含む。）に適用する。本方針は、当グループが事業活動において取り扱う情報資産を対象とする。情報資産の具体的な定義および分類は、本方針に基づく規程において定める。対象とするシステムは、情報システム、クラウドサービスおよび制御システム（OT）とする。

差し替え注記

- 適用対象を一部のグループ会社に限定する場合
  「親会社および別表に定めるグループ会社に適用する」とし、対象会社の選定基準（議決権比率・事業上の重要度等）を併記する。
- 対象者を雇用形態で決定する場合
  「従業員および役員に適用する」とし、委託先の要員には委託契約により別途義務づける。
- 制御系（OT）を保有しないグループの場合
  「制御システム（OT）」の記述を削除する。

3.3 項目とその説明（共通項目）

本節では、グループセキュリティ方針に記載する項目のうち、多くの企業に共通するものを解説する。これらは、国内 50 社の公開しているセキュリティ方針・宣言に加え、一部のプロジェクトメンバーの派遣元企業の内部方針を調査し、多くの方針に共通して記載されていたものを抽出したうえで、経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0[i]」の重要 10 項目と照合して整理した。これらの項目はいずれも、グループ全体でセキュリティ対策の方向性をそろえるために必須となる要素であるため、グループの方針には、原則としてこれらすべての項目を記載することを強く推奨する。各項目を、概要・記載すべき理由・記載時の留意点・記載例の順で説明する。

各項目では、方向性を示すにとどめ、具体的な手順・定義・役割分担は、方針の下位の規程に記載する。親会社とグループ会社の間の役割の振り分けはグループ統治の類型によって異なるため、記載例では類型に寄らない書き方としている。なお、記載例の主語は、親会社を含む全社の義務には「グループ各社」、グループとしての仕組みの設置には「当グループ」、グループ会社に限る義務には「グループ会社」を使い分けている。

各項目と経産省ガイドラインの重要 10 項目の対応を表 3-1 に示す。

表 3-1 項目と経産省ガイドライン重要 10 項目の対応関係

項目	経産省 GL 重要 10 項目での言及箇所
法令遵守	指示 1
推進体制	指示 2
規程整備	指示 1
リスクマネジメント	指示 4・5・6
インシデント対応	指示 7・8
教育	指示 3・5
継続的改善	指示 6
委託先・サプライチェーン管理	指示 9
情報資産の把握	指示 4

なお、重要 10 項目のうち指示 10（サイバーセキュリティに関する情報の収集、共有及び開示の促進）に対応する項目は、共通項目には含めていない。プロジェクトメンバーが調査したグループセキュリティ方針では、情報共有・開示に触れていたものは 50 社中 9 社と少数であり、多くの企業が方針に記載する共通項目とは言えないためである。情報共有や開示への取組を方針として示したいグループは、項目として追加するとよい。

3.3.1 法令遵守

経産省 GL 対応：重要 10 項目 指示 1

概要

グループ各社が、セキュリティに関する法令・規制・契約上の要求事項を把握し、これを遵守すること。守るべき法令には、個人情報保護法や不正競争防止法のほか、業種ごとの業法や、取引先との契約で課されるセキュリティ要求が含まれる。

記載すべき理由

グループ会社は事業や所在地ごとに適用される法令が異なり、親会社がすべて把握できないことが多い。各社が対象とすべき法令を理解し遵守する仕組みが必要であり、万が一法令違反が発生した場合、グループ全体の信用とブランドを毀損する。

記載時の留意点

法令そのものを列挙するのではなく、法令を遵守するという姿勢と枠組みを示す。適用される法令は各社の事業・所在地で異なるため、原則として個別の法令名は方針に書かない。

記載例

> グループ各社は、自社に適用される情報セキュリティに関する法令、規制その他の規範を遵守する。

差し替え注記

- 海外拠点を持つグループの場合
  「国内外の法令」とし、各国の法令遵守をグループ会社の責任として明記する。
- グループ全体に共通して適用される業法（金融・医療・電気通信等）がある場合
  該当する業法を具体的に挙げて記載する。

3.3.2 推進体制

経産省 GL 対応：重要 10 項目 指示 2

概要

グループ全体でセキュリティを推進するための体制を整備すること。各社が自社の体制を持つことに加え、親会社にはグループ全体を統括する仕組みを置く。

記載すべき理由

推進体制が定まっていないと、施策を実行する主体と責任の所在があいまいになり、対策が進まない。特にグループでは、各社が個別に体制を持つだけでは不十分で、グループ全体を統括する体制が必要である。統括推進体制がない場合、グループ会社ごとに実施施策や対応がばらつき、横断的な意思決定ができない恐れがある。

記載時の留意点

最初に各社がそれぞれ推進体制（推進責任者・担当部門）を持つという基盤の整備を述べる。次に、グループ全体を統括する責任者と戦略を策定・審議する会議体（委員会等）の設置を加える。なお、この統括の仕組みは本プロジェクトのなぜなぜ分析から導いた項目であり、自社グループの状況に応じて記載する。詳細は 3.4.2 で扱う。

記載例

> グループ各社は、自社におけるセキュリティを推進する体制を整備する。
> あわせて、当グループは、グループ全体のセキュリティを統括する責任者を置き、セキュリティ戦略を策定・審議する会議体を設置する。

3.3.3 規程整備

経産省 GL 対応：重要 10 項目 指示 1

概要

方針に基づき、具体的な遵守事項を定めるセキュリティ規程を整備すること。方針が方向性を示すのに対し、規程は方針を実行可能な具体的ルールに落とす。

記載すべき理由

方針は抽象度が高く、グループ各社が実際に何をすべきか分からず、対策が実施されない。方針をより具体化した規程がないと方針が宣言にとどまり、実効性を持たない。

記載時の留意点

どの規程を誰が整備するかは類型・運用によって変わるため、方針では「本方針に基づき規程を整備する」という形にとどめる。

記載例

> グループ各社は、本方針に基づき、自社のセキュリティに関する規程を整備する。

3.3.4 リスクマネジメント

経産省 GL 対応：重要 10 項目 指示 4・5・6

概要

グループ全体でセキュリティのリスクを把握し、対策の優先順位を決め、継続的に見直すこと。

記載すべき理由

リスクを把握しないまま対策を講じると、本当に守りたい資産に経営資源が適切に配分されず、重大なリスクが放置される可能性がある。各社の事業や事業リスクは異なるが、だからこそ、共通の枠組みで把握しなければ、リスクの大小をグループ横断で比較できず、対策の優先順位を決められない。

記載時の留意点

リスクを把握し、優先順位をつけ、見直すという一連の枠組みを示す。リスクの把握・評価の具体的な手法・手順は下位の規程等で定め、方針では実施することの宣言にとどめる。

記載例

> グループ各社は、自社のセキュリティに関するリスクを把握し、対策の優先順位を定めて継続的に見直す。

3.3.5 インシデント対応

経産省 GL 対応：重要 10 項目 指示 7・8

概要

セキュリティインシデント発生時の対応体制と事業を復旧させる体制を整える。

記載すべき理由

万が一インシデントが発生した場合にも被害を最小限に抑えるためには、事前に対応体制および復旧体制を用意することが重要である。対応および復旧の遅延は、グループ全体へ被害が波及するため、方針で定めるべき項目である。

記載時の留意点

緊急時の対応と事業の復旧の 2 点について記載する。対応手順や連絡体制の詳細は規程に委ね、方針では体制を整備するという宣言にとどめる。

記載例

> グループ各社は、セキュリティインシデントの発生に備え、緊急時の対応および事業の復旧のための体制を整備する。

3.3.6 教育

経産省 GL 対応：重要 10 項目 指示 3・5

概要

グループ各社のすべての従業員・役員が、自らの業務に応じて必要なセキュリティの知識・意識を持つよう、教育を実施する。

記載すべき理由

教育の仕組みがないと、グループ会社ごとにセキュリティの知識・意識に差が生じる。セキュリティの意識が低い会社がサイバー攻撃の起点となり、その影響がグループ全体に波及する恐れがある。

記載時の留意点

すべての従業員・役員の知識・意識の向上を図るという方向性を示す。教育の実施主体や、親会社による支援の有無・程度は類型・運用によって異なるため、方針では教育を実施することの宣言にとどめ、詳細は各社の運用および下位の規程に委ねる。

記載例

> グループ各社は、自社のすべての従業員・役員のセキュリティに関する知識および意識の向上を図るため、教育を継続的に実施する。

3.3.7 継続的改善

経産省 GL 対応：重要 10 項目 指示 6

概要

セキュリティ対策を策定して満足するのではなく、定期的に評価し、変化に応じて見直す仕組みを持つ。

記載すべき理由

脅威は絶えず変化する。対策を見直す仕組みがないと、当初の対策が陳腐化し、新たな攻撃に対応できなくなる。

記載時の留意点

対策を定期的に評価し、変化に応じて見直すという継続の仕組みを示す。評価の方法や頻度の詳細は規程・運用に委ね、方針では継続的に見直すという宣言にとどめる。

記載例

> グループ各社は、自社のセキュリティ対策の実施状況を定期的に評価し、事業環境やリスクの変化に応じて継続的に見直す。

3.3.8 委託先・サプライチェーン管理

経産省 GL 対応：重要 10 項目 指示 9

概要

業務委託先やシステムで連携する取引先に対しても、自社グループと同等のセキュリティ水準を求めるべきである。

記載すべき理由

委託先やシステム連携先といった取引先のセキュリティが十分でないと、取引先を起点にグループが攻撃を受ける。自社・グループ内の対策だけでなく、サプライチェーン経由の侵害も想定する必要がある。

記載時の留意点

委託先や連携先にも自社グループと同等の水準を求める、という方向性を示す。求める水準の具体や契約・監査による担保の方法は規程に委ね、方針では水準を求めるという宣言にとどめる。

記載例

> グループ各社は、業務の委託先およびシステム連携を行う取引先に対し、当グループと同等のセキュリティ水準を求める。

3.3.9 情報資産の把握

経産省 GL 対応：重要 10 項目 指示 4

概要

グループ各社が、守るべき情報資産の所在や保有データを把握し、情報資産の重要度によって分類する。

記載すべき理由

守るべき情報資産を把握していないと、重要な情報資産にセキュリティ対策が行われていない事態が発生する可能性がある。プロジェクトメンバーの派遣元企業においても、グループ会社の情報資産を親会社が把握しきれないという意見が多数上がった。

記載時の留意点

守るべき情報資産を把握し分類するという方向性を示す。何を情報資産とみなすかの定義や分類の基準は規程に委ね、方針では把握し分類するという宣言にとどめる。

記載例

> グループ各社は、自社の守るべき情報資産を把握し、その重要度に応じて分類する。

3.4 なぜなぜ分析から導いた項目（選択項目）

本節では、本プロジェクトが実施したなぜなぜ分析から導いた項目を解説する。3.3 が多くの企業に共通する項目であるのに対して、本節は「グループ会社のセキュリティがなぜ進まないか」を分析した結果、その根本原因（真因）の解決策として方針に書くべきと判断した項目である。これらは、経営方針としてグループセキュリティの推進を決定していることを前提に、その決定を実行に移すために必要な事項を方針上の記述に落とすものにあたる。なお、なぜなぜ分析の過程および真因の一覧はガイドの付録 A および付録 C に示す。

本節に記載の項目は、自社グループの状況に応じて記載を選択する。各項目について、背景にある課題・目指す状態・記載例を示す。本方針では特定のグループ統治の類型を前提とせず、いずれの類型でも通用する形で記載する。

3.4.1 親会社とグループ会社の責任分界の明確化

背景にある課題

親会社とグループ会社の間で、セキュリティに関して親会社が決めること・各社が決めることの責任分界が定められていない。責任分界とは、親会社とグループ会社の間で、親会社が決定・取り組むべき事項と、各社が決定・取り組むべき事項の境界を定めることを意味する。

この課題に紐づく真因は、次のとおりである。

・親会社とグループ会社の間でセキュリティに関する責任分界点が明確に定められていない（P-14）

目指す状態

親会社とグループ会社が、セキュリティに関する責任・役割を分担することを方針で定める。方針では、責任を分担するという原則と、その区分を下位の規程で定めることを宣言するにとどめ、区分の内容そのものは方針には書かない。

親会社が定める範囲とグループ会社に委ねる範囲をどのように区分するかは、類型についての説明（ガイド 5.1.2）で示しているため、これを参考に、自社グループにおける区分を規程で定める。親会社とグループ会社の責任を区分することが、本方針の各項目における役割分担の基礎となる。

記載例

> 当グループは、セキュリティに関する責任を親会社とグループ会社の間で分担する。親会社が定める事項とグループ会社が定める事項の区分は、本方針に基づく規程において定める。

3.4.2 推進体制（統括責任者・戦略を策定する場の設置）

背景にある課題

本項目は、3.3.2「推進体制」で述べた体制の上に位置づけられる。グループ各社が推進体制を持っていても、グループ全体を統括する責任者が不在で、戦略を策定する会議体が定まっていなければ、横断的な意思決定が進まない。

この課題に紐づく真因は、次のとおりである。

・グループセキュリティの推進責任者(グループ CISO 等)が正式に任命されていない（P-13,P-21）

・組織としてセキュリティ戦略を策定する会議体(セキュリティ委員会等)が存在しない（P-23）

目指す状態

グループ全体のセキュリティを統括する責任者（グループ CISO 等）を置き、セキュリティ戦略を策定・実行する権限を付与する。あわせて、戦略を策定・審議する会議体（グループセキュリティ委員会等）を設置する。これにより、3.3.2 の体制（各社が持つ推進体制）が、統括責任者と戦略を策定・審議する場を統合した体制となる。

記載例

> 当グループは、グループ全体のセキュリティを統括する責任者を置き、セキュリティ戦略の策定および実行に必要な権限を付与する。あわせて、グループのセキュリティ戦略を策定・審議する会議体を設置する。

3.4.3 グループセキュリティ戦略の策定・周知

背景にある課題

親会社がグループセキュリティ戦略を作成できていない、またはグループセキュリティ戦略は存在するが、グループ会社に示していない。方針が方向性を示すのに対し、戦略はそれを実現するための道筋（ロードマップ）を示すものである。戦略がなければ、方針を掲げても実現に向けた具体的な歩みが各社任せになる。

この課題に紐づく真因は、次のとおりである。

・親会社がグループセキュリティ戦略を作成・示していない（G-22）

目指す状態

方針を実現するためのグループセキュリティ戦略（ロードマップ）を策定し、グループ会社に周知する。戦略は、3.4.2 で設けるグループセキュリティ戦略を策定・審議する場で策定・審議される。グループ会社への周知の方法は 2 章「方針の公開・周知方法」を参考にされたい。

記載例

> 当グループは、本方針を実現するためのグループセキュリティ戦略を策定し、グループ会社に周知する。

3.4.4 セキュリティ業務の業務分掌への明記と業務量の可視化

背景にある課題

グループ会社で、セキュリティ業務が業務分掌に位置づけられておらず、その結果、必要な工数が確保されていない。業務量を可視化する仕組みもない。このため、セキュリティ業務は担当者の役割として明確にされず、十分な時間を割くことができない。また、セキュリティ業務が属人的になる。

この課題に紐づく真因は、次のとおりである。

・セキュリティ業務を「正式な業務」として工数確保する経営判断がない（G-12）
・セキュリティ業務の可視化・マニュアル化の仕組みがない（G-16）

目指す状態

グループ会社におけるセキュリティ業務を業務分掌に明記し、相応の工数を確保したうえで、業務量を可視化する。

記載例

> グループ各社において、セキュリティに関する業務分掌において明確にし、その遂行に必要な工数を確保し、業務量を可視化する。

おわりに

本書では、グループセキュリティ方針の位置づけから、その公開・周知の方法、そして方針に記載すべき項目までを解説した。3 章の記載例を一つの方針文書の形にまとめたテンプレートを、付録 A（内部展開用）および付録 B（外部公開用）に示す。自社グループの方針を作成する際の参考にされたい。

本書がグループセキュリティを推進するための第一歩である方針制定の一助となれば幸いである。

参考文献

[i] 経済産業省，サイバーセキュリティ経営ガイドライン Ver3.0，
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

付録 A　内部展開用テンプレート

本付録は、3 章の記載例を一つの方針文書の形にまとめた、グループ内に方針を展開するためのテンプレートである。各条の意味・書き方・差し替えは 3 章の対応する項目を参照のこと。

> ※【選択】を付した条（第 12 条〜第 15 条）は、3 章 3.4 の選択項目に対応する。自社グループの状況に応じて採否を決め、採用しない場合は削除する。

○○グループセキュリティ方針

1. 目的

本方針は、○○グループ（親会社および全グループ会社をいう。以下同じ。）の情報セキュリティを確保するための基本的な方向性を定めるものである。グループを構成するいずれかの会社における対策の不足は、ネットワークや事業上のつながりを通じてグループ全体に影響を及ぼし得る。

本方針は、こうしたリスクを低減するため、グループ全体でセキュリティ対策の方向性をそろえ、各社が事業活動において取り扱う情報資産をサイバー攻撃をはじめとする脅威から保護することを目的とする。

2. 適用範囲

本方針は、○○グループを構成する親会社および全てのグループ会社（以下、これらを総称して「グループ各社」という。）に適用する。また、これらの会社の従業員、役員ならびに雇用形態を問わず業務上、情報資産を取り扱う全ての者（派遣社員、業務委託先の要員等を含む。）に適用する。本方針は、当グループが事業活動において取り扱う情報資産を対象とする。情報資産の具体的な定義および分類は、本方針に基づく規程において定める。対象とするシステムは、情報システム、クラウドサービスおよび制御システム（OT）とする。

3. 法令遵守

グループ各社は、自社に適用される情報セキュリティに関する法令、規制その他の規範を遵守する。

4. 推進体制

グループ各社は、自社におけるセキュリティを推進する体制を整備する。

5. 規程整備

グループ各社は、本方針に基づき、自社のセキュリティに関する規程を整備する。

6. リスクマネジメント

グループ各社は、自社のセキュリティに関するリスクを把握し、対策の優先順位を定めて継続的に見直す。

7. インシデント対応

グループ各社は、セキュリティインシデントの発生に備え、緊急時の対応および事業の復旧のための体制を整備する。

8. 教育

グループ各社は、自社のすべての従業員・役員のセキュリティに関する知識および意識の向上を図るため、教育を継続的に実施する。

9. 継続的改善

グループ各社は、自社のセキュリティ対策の実施状況を定期的に評価し、事業環境やリスクの変化に応じて継続的に見直す。

10. 委託先・サプライチェーン管理

グループ各社は、自社の業務の委託先およびシステム連携を行う取引先に対し、当グループと同等のセキュリティ水準を求める。

11. 情報資産の把握

グループ各社は、自社の守るべき情報資産を把握し、その重要度に応じて分類する。

12. 親会社とグループ会社の責任分担【選択】

当グループは、セキュリティに関する責任を親会社とグループ会社の間で分担する。親会社が定める事項とグループ会社が定める事項の区分は、本方針に基づく規程において定める。

13. グループ全体の統括（統括責任者・戦略を策定・審議する場）【選択】

当グループは、グループ全体のセキュリティを統括する責任者を置き、セキュリティ戦略の策定および実行に必要な権限を付与する。あわせて、グループのセキュリティ戦略を策定・審議する場を設ける。

14. グループセキュリティ戦略の策定・周知【選択】

当グループは、本方針を実現するためのグループセキュリティ戦略を策定し、グループ会社に周知する。

15. セキュリティ業務の業務化と可視化【選択】

業務分掌において明確にし、その遂行に必要な工数を確保し、業務量を可視化する。

附則　本方針は、〇年〇月〇日から施行する。

制定日　〇年〇月〇日

〇〇株式会社　代表取締役社長　〇〇 〇〇

付録 B　外部公開用テンプレート

本付録は、方針を外部に公開する場合のテンプレートである。項目は内部展開用（付録 A）と同じ 15 項目を保ちつつ、文体を公開文書の慣例（ですます調）に合わせ、内部統治の具体（責任区分の規程への委任、統括責任者への権限の付与、業務の工数確保・可視化の仕組み等）は記述の具体度を下げている。公開方法の考え方は 2 章を参照のこと。

> ※【選択】を付した条（第 12 条～第 15 条）は、3 章 3.4 の選択項目に対応する。採用している場合に記載し、採用していない場合は削除する。※公開にあたっては、文書名を「グループ情報セキュリティ基本方針」等、対外的な慣例に合わせて変更してもよい。

○○グループセキュリティ方針

1. 目的

本方針は、○○グループ（○○株式会社およびそのグループ会社をいいます。以下「当グループ」といいます。）における情報セキュリティの基本的な方向性を定めるものです。

当グループは、事業活動において取り扱う情報資産を適切に保護し、サイバー攻撃をはじめとする脅威からグループ全体を守ることにより、お客様、お取引先および社会からの信頼に応えます。

2. 適用範囲

本方針は、当グループを構成する全ての会社に適用します。また、従業員および役員のほか、雇用形態を問わず業務上、情報資産を取り扱う全ての者に適用します。

3. 法令遵守

当グループは、情報セキュリティに関する法令、規制その他の規範を遵守します。

4. 推進体制

当グループは、グループ全体のセキュリティを推進するための体制を整備します。

5. 規程整備

当グループは、本方針に基づき、セキュリティに関する社内規程を整備します。

6. リスクマネジメント

当グループは、セキュリティに関するリスクを把握し、対策の優先順位を定めて継続的に見直します。

7. インシデント対応

当グループは、セキュリティインシデントの発生に備え、緊急時の対応および事業の復旧のための体制を整備します。

8. 教育

当グループは、すべての従業員・役員のセキュリティに関する知識および意識の向上を図るため、教育を継続的に実施します。

9. 継続的改善

当グループは、セキュリティ対策の実施状況を定期的に評価し、事業環境やリスクの変化に応じて継続的に見直します。

10. 委託先・サプライチェーン管理

当グループは、業務の委託先およびシステム連携を行う取引先に対し、当グループと同等のセキュリティ水準を求めます。

11. 情報資産の把握

当グループは、守るべき情報資産を把握し、その重要度に応じて分類し、適切に管理します。

12. 親会社とグループ会社の責任分担【選択】

当グループは、セキュリティに関する責任を親会社とグループ会社の間で分担し、グループ一体となってセキュリティの確保に取り組みます。

13. グループ全体の統括（統括責任者・戦略を策定・審議する場）【選択】

当グループは、グループ全体のセキュリティを統括する責任者を置くとともに、グループのセキュリティ戦略を策定・審議する場を設けます。

14. グループセキュリティ戦略の策定・周知【選択】

当グループは、本方針を実現するためのグループセキュリティ戦略を策定し、グループ全体で推進します。

15. セキュリティ業務の業務化と可視化【選択】

当グループは、グループ各社においてセキュリティに関する業務を適切に位置づけ、その遂行に必要な資源を確保します。

制定日　〇年〇月〇日

〇〇株式会社　代表取締役社長　〇〇 〇〇