グループセキュリティガイド【別紙2】

現状評価のノウハウ集

―― 議論・ヒアリングから見えてきたこと ――

独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター
中核人材育成プログラム9期生　グループ会社のセキュリティ推進プロジェクト
2026年8月

目次

Chapter 0

はじめに

本資料について

本資料の位置づけ・想定読者・主な情報源

位置づけ

- ICSCoE9期卒業プロジェクト「グループ会社のセキュリティ推進」における成果物「グループセキュリティガイド」の別紙2。
- 成果物内の課題「リスクアセスメントの手法とプロセスの整備」について**解決への打ち手**をまとめる。

⇩

リスクアセスメントのプロセスを検討した結果、その**具体的な手法の前に**、リスクアセスメントの前段階で、**グループ会社の現状評価を行うことが重要と考えた**。

そのため本資料では、**リスク分析手法の解説から入るのではなく、他社事例（Chapter 1）・現状評価の実務（Chapter 2）を先に扱い、リスクアセスメントについては最後（Chapter 3）で今後の発展として位置づける構成**としている。「現状評価のノウハウ集」と題している所以である。

想定読者

親会社セキュリティ担当者

特に、グループセキュリティに携わる方を想定。

主な情報源

- プロジェクトメンバー (複数業界・8社)
- 他社グループへヒアリング (2社)

免責事項

- 本紙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ります。
- 本紙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します。
- 本紙に記載の内容は、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ます。
- 本紙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します。
- 本紙の有効期限は、発行日から2年間とします。

Chapter 1

取り組み事例

取り組み事例ヒアリングの背景

- 企業グループにおけるリスクアセスメントの進め方をプロジェクト内で議論・検討した。

議論の中で…
- グループ会社自身がリスク分析を実施することは難しく、親会社の支援が必要。
- 親会社自身もリスクアセスメントできていない場合がある。
- 業務経験等に基づき整理しているが、あくまで机上の検討内容に留まる。

⇒リスク分析以前に、まず実態を正確に把握する仕組み（現状評価）が必要という課題が浮かび上がった。

- この課題を踏まえ、より具体的で読者の参考となる情報を記載するために、実際に各企業グループの取り組みについてヒアリングを行った。
  ⇒システム単体あるいはグループ会社のアセスメントを実施していた。

事例①	**【システム視点】** • システム導入時に親会社セキュリティ部門が**システム単体のアセスメント**を実施。
事例②	**【マネジメント視点】** • 年次で親会社セキュリティ部門が**グループ会社全体のアセスメント**を実施。

事例①～システム視点～

業種：製造 ／ グループ会社数：約250社 ／ セキュリティ部門人数：26名

実態把握の方法

- 新規情報システム導入、変更時にシステム単位で申請ベースで実施。（申請数：年間100件程度）
- 申請内容だけで不明な場合は、直接ヒアリングも実施。

アセスメントの手法

- 新規システム導入時の申請でシステムの構成など細かくチェックし、システム使用の許可を出している。

親会社の関わり方

- グループ会社に自立してもらいたいという思いはあるが、現状では親会社が積極的に支援している。
- IT環境においては、親会社がグループ共通インフラ（ネットワーク・クラウド等）を提供し、一定のセキュリティレベルを担保することで、各グループ会社でのセキュリティ対策やリスクアセスメントは不要としている。
- 監査部門によるセキュリティ監査も別途年次で実施。

継続化の工夫・課題

■継続化の工夫
- 申請を受けて精査するだけでなく、ヒアリングを実施し、コミュニケーションをとる。
- 資産把握のためにグループ全体で共通基盤を使う方向に進める。

■課題
- OT環境の実態把握は完全にはできていない。
- グループ会社でセキュリティ担当者を立てるのは難しい。

事例②～マネジメント視点～

業種：運輸／ グループ会社数：約50社 ／ セキュリティ統括部門人数：5名

実態把握の方法

- 年次でのITチェックシート提出により、資産・データ・ドメイン等の台帳を各社から収集している。
- 各社担当者のITリテラシー差を踏まえ、現地訪問等で信頼関係を構築しながら実態確認や是正支援を行っている。
- 親会社としては、グループ会社を最も近いサプライチェーンと位置づけ、ITセキュリティを含むアセスメントを進めている。

アセスメントの手法

- あくまでも責任はグループ会社のデータオーナーやシステムオーナーにあることを前提に、セキュリティのアドバイス（支援）を行う。
- 1年かけて全国のグループ会社を行脚し、顔を合わせて会話し、信頼を得る。是正指導だけでなく、グループ会社側に実りのある提案もする。

親会社の関わり方

- 全てのシステムを対象にセキュリティ診断を必須化。あわせて相談窓口となるセキュリティデスクも設置。
- コミュニケーションを重要視し、グループ向けの情報共有会の場を年2～3回設ける。
- 親会社と事業会社を兼務しているが、グループ社へセキュリティ推進する際は親会社の立場で行う。

継続化の工夫・課題

■継続化の工夫
- グループ規程に基づいて支援を行うことで、セキュリティを義務化させる。
- 主要なグループ会社とは定例会を設け、状況把握の鮮度を上げる

■課題
- ルールを策定してもグループ各社の予算確保やリソースの状況により対応計画に差が出る。
- 各社担当者のITリテラシーの差がある。

各事例から見えてきたこと

共通点

- 両社ともp.17に挙げている既存の分析手法を用いたリスクアセスメントは現状未実施。
- 実態把握は親会社主導で実施しており、グループ会社任せにしていない。
- グループ会社側の担当者リソース・スキルに課題を抱えている。

差異

- 評価の焦点が異なる。
  - システム単体（新規導入・変更時の申請ベース）
  - 会社全体（年次チェックシートと現地訪問による包括的な実態把握）
- 実態把握のタイミングが異なる。
  - システム導入・変更というイベント駆動
  - 年次の定期サイクル

示唆

- 手法・規模が異なっても「実態を把握する」ステップは両社共通。
- 事例からも確認された通り、現状評価から始めることが重要。

これを踏まえ、次章では現状評価の具体的な進め方を整理する。

Chapter 2

現状評価について

現状評価の取り組み

現状評価の取り組みとしてどのようなものがあるか、プロジェクト内で整理した。

評価者	親会社セキュリティ部門、または監査部門
評価単位	会社単位
評価観点	企業グループで定める規程やガイドラインに沿っているか
評価項目	既存のフレームワークやガイドラインを参考に親会社が設定
手段	• グループ会社自身が**セルフチェック**して親会社へ報告。 • 親会社セキュリティ部門がグループ会社へ**ヒアリング**。 • 親会社セキュリティ部門または監査部門が、グループ会社へセキュリティに関する実地**監査**を実施。 • 親会社セキュリティ部門で専門グループを組成して、担当するグループ会社へ**専属担当(アドバイザー)が定期訪問。** ※上記は単独での実施に限らず、対象会社の規模や成熟度に応じて複数を組み合わせて段階的に実施することも可能。 ※実施難易度は下の項目ほど高い。
頻度	• セルフチェックやヒアリング、定期訪問…数か月～1年間隔 • 監査…2～3年間隔

評価項目を設定する際の参考資料

まずは「５分でできる！情報セキュリティ自社診断」を参考にして、次のステップとして自工会部工会ガイドラインやSCS評価制度を参照されたい。
なお、Cybersecurity Framework 2.0はセキュリティ対策の実装手順について記載はないが、考え方が整理されたフレームワークであり併せて読むことが望ましい。

資料名	概要 / 特徴（プロジェクト内の口コミ）	リンク※
中小企業の情報セキュリティ対策ガイドライン 第4.0版 付録３　５分でできる！情報セキュリティ自社診断(IPA)	• 中小企業向けに情報セキュリティ対策の基本項目をチェックリスト形式で整理した入門的ガイドライン。 • はじめに参考にするものとしてよくまとまっている。 • これがゴールではなく各項目を自社規程に紐づけて拡張する。	https://www.ipa.go.jp/security/guide/sme/about.html
自工会/部工会・サイバーセキュリティガイドライン v2.3 (jama, 一般社団法人日本自動車工業会)	• 自動車業界のサプライチェーンを対象に、サイバーセキュリティ対策をレベル別に体系化した業界特化型ガイドライン。 • 上記に比べて項目は詳細に。各項目がLv.分けされているためステップアップしやすい。 • 物理セキュリティの項目を考える場合参考になる。	https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html
サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度） ★3・★4要求事項及び評価基準(経産省)	• 経済産業省が策定した、企業のサイバーセキュリティ対策状況を第三者が評価・認定する制度。 • 海外の基準も参考に作成されており網羅性が高い。	https://www.meti.go.jp/policy/netsecurity/scs.html
Cybersecurity Framework 2.0 (NIST)	組織のサイバーセキュリティリスク管理を6つの機能（統治、識別、防御、検知、対応、復旧）で体系化した国際的フレームワーク。	(IPAによる日本語訳版) https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/bego9000000d400.pdf

※2026年6月17日アクセス

Chapter 3

リスクアセスメントについて

リスクアセスメントとは

現状評価によってグループ会社の実態が把握できた後、次のステップとして取り組むべきものがリスクアセスメントである。リスクアセスメントとは、リスクを発見・認識する「リスク特定」、その特質や大きさを測る「リスク分析」、基準と照らし合わせて許容可能かを判断する「リスク評価」からなる一連のプロセス全体を指す。

プロセス	ISO/IEC 27000:2018(JIS Q 27000:2019)における規定
リスクアセスメント（risk assessment）	リスク特定、リスク分析及びリスク評価のプロセス全体
リスク特定（risk identification）	リスクを発見、認識及び記述するプロセス
リスク分析（risk analysis）	リスクの特質を理解し、リスクレベルを決定するプロセス
リスク評価（risk evaluation）	リスク及び／又はその大きさが受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス
リスク対応（risk treatment）	リスクを修正するプロセス

分析手法例

① **ベースラインアプローチ**：既存の標準や基準をもとに、想定する典型的なシステムに対して、予め一定の確保すべきセキュリティレベルを設定し、それを達成するためのセキュリティ対策要件を定め、分析対象となるシステムの対策の適合性等をチェックする。

② **非形式的アプローチ**：組織や担当者の経験や判断によってリスク分析を実施する。

③ **詳細リスク分析**：分析対象のシステム自体に対して、そのシステムもしくはそれにより実現されている事業を、「重要度」（あるいは損なわれた場合の被害レベル）「脅威」「脆弱性」の評価指標の下で、リスク分析を実施する。

④ **組み合わせアプローチ**：複数のアプローチを併用し、作業の効率化、異なった評価視点の活用によって、分析精度の向上と、作業工数増大の回避を図る。

制御システムのセキュリティリスク分析ガイド 第2版(IPA)より
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

リスクアセスメント実施プロセスの整理

親会社とグループ会社の間でリスクアセスメントを実施するプロセスについて整理した。

リスクアセスメントの目的：企業グループ全体のリスクの把握と改善

グループ会社のセキュリティ対策状況の現状評価

①現状評価 ②PDCAサイクル＋仕組みの継続

親会社：方針の策定
- 実施頻度を設計。
  例)初年度に分析と予算確保、次年度に改善。
- リスク分析手法を決定。

親会社またはグループ会社：リスク分析
- リスク分析を実施。
- 改善策を計画、優先順位づけ。

親会社とグループ会社：改善を実施
- グループ会社が改善策を実行。
- 親会社が全体のリスクから新たな施策を検討。

親会社：結果をチェック
- 手法に基づく分析かプロセスを評価。
- 各社の分析結果を集約し全体のリスクを把握。

グループ全体で進めるために…
動機付け：外部第三者評価を踏まえて必要性を訴求。/ SCS評価※等の環境変化を踏まえて推進。
負荷軽減：全社同時ではなくPDCAをずらして実施。 /まずは簡易アセスメントから実施。

※サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）（経済産業省）

既存のリスク分析手法

リスク分析手法について国内の参考資料を取りまとめたため参考にされたい。
手法に正解はなく、手法を準用する、または部分的に採用するなど関係者が納得する手法で実施することが重要である。

資料名	概要 / 想定読者	リンク※
中小企業の情報セキュリティ対策ガイドライン 第4.0版(IPA)	• 第2部4章に**資産ベースの詳細リスク分析**の手法について記載。 • 想定読者：中小企業の経営層、およびIT・セキュリティ担当者	https://www.ipa.go.jp/security/guide/sme/about.html
制御システムのセキュリティリスク分析ガイド 第2版(IPA)	• **資産ベース×脅威ベースの詳細リスク分析**の手法について記載。 • 想定読者：制御システム（OT）の設計・構築・運用に携わる技術者や管理責任者	https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
機能保証のためのリスクアセスメント・ガイドライン(NCO)	• **シナリオベースの詳細リスク分析**の手法について記載。 • 想定読者：重要インフラ事業者や政府機関等の、リスク管理・システム企画担当者	(DLリンク) https://www.cyber.go.jp/files/Risk-assessment.zip
リスクアセスメント実践ラーニングキット～自己学習、研修教材～(NCO)	• 上記の「機能保証のためのリスクアセスメント・ガイドライン」をベースに実施手順を解説している。	https://security-portal.cyber.go.jp/guidance/nco_risk.html

※2026年6月17日アクセス

Chapter 4

まとめ

グループセキュリティ向上のために

- グループ各社の実態を親会社とグループ会社自身が相互に把握することが、セキュリティ対策の実効性を高めるうえで重要である。他社事例においても、現状評価が共通の土台となっていることを確認した。

- まずはグループ会社の現状や実態を、親会社とグループ会社の両者が把握・評価することが重要である。現状評価の取り組みや参考資料をまとめているため、ぜひ活用いただきたい。

- 現状評価によって実態が把握できた先に、リスクアセスメントへと発展させることが望ましい。リスクアセスメントについても、その考え方とプロセスを知見として整理しているため併せて参考にされたい。