経済産業省

資料７－４

経済産業省におけるサイバーセキュリティ施策の取組状況について

令和５年６月２日

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の改訂概要（全体）

- 本ガイドラインについて、**経営者の責務としてサイバーセキュリティに関する残留リスクを低減すること**等を明記するとともに、**サプライチェーンの多様化・複雑化等の情勢の変化やサイバー・フィジカル空間の融合に対応した対策の必要性**を踏まえた改訂を実施。

＜現行のガイドライン構成＞

１．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**関係者との適切なコミュニケーション**が必要

２．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の対策及び状況把握
関係者とのコミュニケーション	**指示10** 情報共有活動への参加

＜改訂の概要＞

●取引関係にとどまらず、国内外のサプライチェーンでつながる関係者へのセキュリティ対策への目配り、総合的なセキュリティ対策の重要性や社外のみならず、社内関係者とも積極的にコミュニケーションをとることの必要性を記載

●セキュリティ業務従事者のみならず、全ての従業員において、必要かつ十分なセキュリティ対策を実現できるスキル向上の取組の必要性を記載

●サイバーセキュリティリスクの識別やリスクの変化に対応した見直しやクラウド等最新技術とその留意点などを記載

●事業継続の観点から、制御系も含めた業務の復旧プロセスと整合性のとれた復旧計画・体制の整備やサプライチェーンも含めた実践的な演習の実施等について記載

●サプライチェーンリスクへの対応に関しての役割・責任の明確化、対策導入支援などサプライチェーン全体での方策の実行性を高めることについて記載

サイバーセキュリティ経営ガイドライン Ver3.0の改訂概要①

- 企業において、サイバーセキュリティリスクを組織の経営リスクの一環として認識し、サイバーセキュリティを包含するエンタープライズリスクマネージメントを実践していくことが必要。そのため、経営者の責務として、**サイバーセキュリティ対策の実施を通じたサイバーセキュリティに関する残留リスクを低減させること**を明記
- 経営者が認識すべき３原則については、**国内外のサプライチェーンでつながる関係者へのセキュリティ対策への目配り、総合的なセキュリティ対策の重要性**や社内・社外含めた**関係者との積極的にコミュニケーションをとることの必要性**を強調

■　概要・はじめに

- サイバーセキュリティ対策は「投資」（将来の事業活動・成長に必須な費用）と位置付けることが重要。企業活動におけるコストや損失を減らすために必要不可欠な投資
- サイバーセキュリティリスクを把握・評価した上で、対策の実施を通じてサイバーセキュリティに関する自社が許容可能とする水準まで低減することは、企業として果たすべき社会的責任であり、その実践は経営者としての責務
- 経営者は、サイバーセキュリティ体制が適切でなかった場合に、善管注意義務違反などの会社法・民法等の規定する法的責任やステークホルダーへの説明責任を負う可能性がある。

■　経営者が認識すべき３原則

(1) 経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要

(2) サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要

(3) 平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

サイバーセキュリティ経営ガイドライン Ver3.0の改訂概要②

- 経営者が指示すべき10の重要事項については、**デジタル環境の活用等の情勢の変化やサイバー・フィジカル空間の融合に対応した対策の必要性**を踏まえた改訂を実施

■ 経営者が指示すべき１０の重要事項

リスク管理体制の構築

（指示１）**サイバーセキュリティリスクの認識、組織全体での対応方針の策定**
※経営リスクとして認識、組織全体の対応方針、公表

（指示２）**サイバーセキュリティリスク管理体制の構築**
※役割と責任の明確化、組織内のリスク管理体制とも整合

（指示３）**サイバーセキュリティ対策のための資源（予算、人材等）確保**
※外部ベンダーや自社のセキュリティ人材、プラス・セキュリティ

リスクの特定と対策の実装

（指示４）**サイバーセキュリティリスクの把握とリスク対応に関する計画の策定**
※事業に用いるデジタル環境、サービス及び情報の特定、サイバー攻撃の脅威・影響度合を踏まえた対応計画

（指示５）**サイバーセキュリティリスクに効果的に対応する仕組みの構築**
※防御、監視・検知、分析、対応

（指示６）**PDCAサイクルによるサイバーセキュリティ対策の継続的改善**
※サイバーセキュリティリスクの特徴、最新の脅威への対応

インシデントに備えた体制構築

（指示７）**インシデント発生時の緊急対応体制の整備**
※CSIRT、PSIRT等（初動対応、再発防止）、情報開示、演習（制御系含む）

（指示８）**インシデントによる被害に備えた事業継続・復旧体制の整備**
※復旧目標、手順、体制、制御系含めたBCPとの連携、サプライチェーン含めた実践的な演習

サプライチェーンセキュリティ

（指示９）**ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策**
※監査の実施など対策状況の把握、対策の導入支援や共同実施、緊急時の協力

関係者とのコミュニケーション

（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**
※情報共有を行う関係の構築、被害の報告・公表への備え（IPA・JPCERT/CC、ISAC、CSIRT間の連携など）

サイバーセキュリティ経営ガイドライン Ver3.0の改訂

https://www.meti.go.jp/press/2022/03/20230324002/20230324002.html

経済産業省
Ministry of Economy, Trade and Industry

申請・お問合せ | English | サイトマップ | 本文へ | 文字サイズ変更 小 中 大 | アクセシビリティ閲覧支援ツール

ニュースリリース | 会見・動静・談話 | 審議会・研究会 | 統計 | 政策について | 経済産業省について

ホーム ▶ ニュースリリース ▶ ニュースリリースアーカイブ ▶ 2022年度3月一覧 ▶ 「サイバーセキュリティ経営ガイドライン」を改訂しました

印刷

「サイバーセキュリティ経営ガイドライン」を改訂しました

2023年3月24日

▶ 安全・安心

経済産業省では、サイバー攻撃の多様化・巧妙化に伴い、サイバーセキュリティ対策における企業等の経営者のさらなるリーダーシップの発揮などが求められていること等を踏まえ、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある事項等をまとめた「サイバーセキュリティ経営ガイドライン」を改訂しました。

1. 背景・趣旨

経済産業省では、独立行政法人情報処理推進機構（IPA）とともに、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある事項及び経営者が情報セキュリティ対策を実施する上での責任者となるCISO（Chief Information Security Officer：最高情報セキュリティ責任者）等に指示すべき事項をまとめたサイバーセキュリティ経営ガイドラインを策定し、その普及を行ってまいりました。

昨今、サイバー攻撃は多様化・巧妙化しており、また、サプライチェーンを介したサイバーセキュリティ関連被害の拡大を踏まえた、サプライチェーン全体を通じた対策の推進の必要性が高まっているなど、各企業等においては、組織幹部が自らの果たすべき役割を認識した上で、リーダーシップを発揮し、更なる対策の強化や適切に対応することなどが求められております。

こうした現状等を踏まえ、有識者や関係者を交えた研究会を開催し、そこでの検討を踏まえ、サイバーセキュリティ経営ガイドラインの改訂を行いました。

2. 改訂のポイント

「サイバーセキュリティ経営ガイドライン」を改訂しました （METI/経済産業省）
https://www.meti.go.jp/press/2022/03/20230324002/20230324002.html