資料３－４

経済産業省

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４年１２月２２日

経済産業省

サイバーセキュリティ経営ガイドラインの改訂の概要

- サイバー攻撃の多様化やサプライチェーンの複雑化により、**サプライチェーン全体を通じたサイバーセキュリティ対策の必要性が高まっており、経営者が自らリーダーシップを発揮して更なる対策の強化や適切な対応が必要**。
- このような実情等を踏まえ、経営者が認識すべき原則及びCISO等に指示すべき事項を記載した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**を踏まえた改訂を予定。

＜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

＜改訂案の概要＞

●取引関係にとどまらず、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

サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて（概要）

令和４年10月28日
経 済 産 業 省
公 正 取 引 委 員 会

【背 景】

■ 昨今、サイバーセキュリティ対策が不十分な**中小企業がサイバー攻撃に狙われ、サプライチェーン全体に問題が波及**する事態が発生。

■ 令和４年４月、「原油価格・物価高騰等に関する関係閣僚会議」（内閣総理大臣、内閣官房長官、関係大臣、公正取引委員会委員長が出席）において、**コロナ禍における「原油価格・物価高騰等総合緊急対策」**を決定。

「サイバーインシデントによってサプライチェーンが分断され、物資やサービスの安定供給に支障が生じることのないよう、**中小企業等におけるサイバーセキュリティ対策を支援**するとともに、**取引先への対策の支援・要請に係る関係法令の適用関係について整理**を行う。」

【内 容】

■ 発注者側となる事業者は、以下を参考に、サプライチェーンの保護に向けて、取引先のサイバーセキュリティ対策の強化を促しつつ、サプライチェーン全体での付加価値の向上に取り組み、取引先とのパートナーシップの構築を目指していただきたい。

①サイバーセキュリティ対策に関する支援策

■ **サイバーセキュリティお助け隊サービス**（中小企業に対するサイバー攻撃への対処として不可欠なサービスをワンパッケージで提供）の利用促進

■ **セキュリティアクション**（中小企業がセキュリティ対策に取り組むことを宣言）の推進

■ **中小企業の情報セキュリティ対策ガイドライン**（中小企業を対象に、情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき方針、対策を実践する際の手順や手法をまとめたもの）の活用

■ **パートナーシップ構築宣言**（発注側企業が取引先との間でパートナーシップを構築することを宣言）の中で、取引先にサイバーセキュリティ対策の助言・支援を行うことを取組例として記載

②サイバーセキュリティ対策の要請に係る独占禁止法・下請法の考え方

■ サイバーセキュリティ対策の必要性が高まる中、**サプライチェーン全体のセキュリティ対策強化は重要**な取組。**サイバーセキュリティ対策を要請すること自体が直ちに問題となるものではない**。

■ ただし、要請の方法や内容によっては、問題となることもあるため、そのようなケースを例示。

＜問題となるケースの例＞

① 取引上の地位が優越している事業者が、サイバーセキュリティ対策の実施によって取引の相手方に生じるコスト上昇分を考慮することなく、一方的に著しく低い対価を定める場合

② 取引上の地位が優越している事業者が、新たなセキュリティサービスを利用する必要がないにもかかわらず、自己の指定する事業者が提供するより高価なセキュリティサービスの利用を要請し、当該事業者から利用させる場合

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

ガイドラインの背景・目的

- 工場のIoT化によるネットワーク接続機会の増加に伴いサイバー攻撃リスクが増加。また、ネットワークの接続に乏しい工場であっても不正侵入者等による攻撃の可能性あり。
- 意図的な攻撃の場合もあれば、たまたま攻撃される場合もある。

→**いかなる工場でもサイバー攻撃のリスクあり**。

- 本ガイドは業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを示した「手引き」。

→**各業界・業種が自ら工場のセキュリティ対策を立案・実行**することで、**工場のセキュリティの底上げを図ることが目的**。

想定する読者の方

- ITシステム部門
- 生産関係部門（生産技術部門、生産管理部門、工作部門等）
- 戦略マネジメント部門（経営企画等）
- 監査部門
- 機器システム提供ベンダ、機器メーカ
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。

対策に取り組む効果

- **工場のBC／SQDC※の価値がサイバー攻撃により毀損されることを防止**。
- セキュリティが担保されることでIoT化や自動化が進み、多くの工場から新たな付加価値が生み出されていくことを期待。

※ 安全確保(S：Safety)、
事業／生産継続(BC：Business Continuity)
品質確保(Q：Quality)
納期遵守・遅延防止(D：Delivery)
コスト低減(C：Cost)

セキュリティ対策企画・導入の進め方

ステップ 1

内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2** 業務の整理
- **ステップ1-3** 業務の重要度の設定
- **ステップ1-4** 保護対象の整理
- **ステップ1-5** 保護対象の重要度の設定
- **ステップ1-6** ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7** ゾーンと、セキュリティ脅威の影響の整理

ステップ 2

セキュリティ対策の立案

- **ステップ2-1** セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策
① ネットワークにおけるセキュリティ対策
② 機器におけるセキュリティ対策
③ 業務プログラム・利用サービスにおけるセキュリティ対策

(2)物理面での対策
① 建屋にかかわる対策
② 電源／電気設備にかかわる対策
③ 環境(空調など)にかかわる対策
④ 水道設備にかかわる対策
⑤ 機器にかかわる対策
⑥ 物理アクセス制御にかかわる対策

ステップ 3

セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策

(1)ライフサイクルでの対策
① 運用・管理面のセキュリティ対策
A) サイバー攻撃の早期認識と対処
（OODAプロセス）
B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C) 情報共有

②維持・改善面のセキュリティ対策
・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
・組織・人材のスキル向上（教育、模擬訓練等

(2) サプライチェーン対策
・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す