経済産業省

資料３－３

サイバーセキュリティ経営ガイドライン の取り組みについて

経済産業省 商務情報政策局

サイバーセキュリティ課

サイバーセキュリティ対策における経営者の役割

- 企業戦略として、どの程度ITに対する投資やセキュリティ投資を行うかは経営判断。
- 場合によっては経営者責任を問われる恐れ。

経営判断が必要

- 企業戦略として、どの程度IT投資を行うか（生産性向上、ビジネス拡大）
- その中で、事業継続性の確保やサイバー攻撃に対する防衛力の向上のために、どの程度セキュリティ投資を行うか（企業価値向上）

経営者のリスク対応の是非、経営者責任について社会から問われる恐れ

例えば、以下のような時に問われる恐れがある

- サイバー攻撃により個人情報や秘密情報が漏洩した場合
- インフラの供給停止など、社会に損害を与えてしまった場合

サイバーセキュリティ経営ガイドライン（平成27年12月28日公開、平成28年12月8日改訂）

- 経済産業省と（独）情報処理推進機構（IPA）にて策定。
- 経営者のリーダーシップによってサイバーセキュリティ対策を推進するため、**経営者が認識すべき3原則**と、**経営者がセキュリティの担当幹部（CISO等)に指示すべき重要10項目**を提示。

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

リーダーシップの表明・体制構築

（１）組織全体での対策方針の策定
（２）方針を実装するための体制の構築

PDCAの策定

（３）リスクを洗い出し、計画の策定
（４）PDCAの実施、及び状況報告
（５）ビジネスパートナーを含めたPDCAの実施

攻撃を防ぐ事前対策

（６）予算・人材などリソースの確保
（７）ITシステムの委託先対策も確認
（８）情報収集・共有活動に参加

事後対応の準備

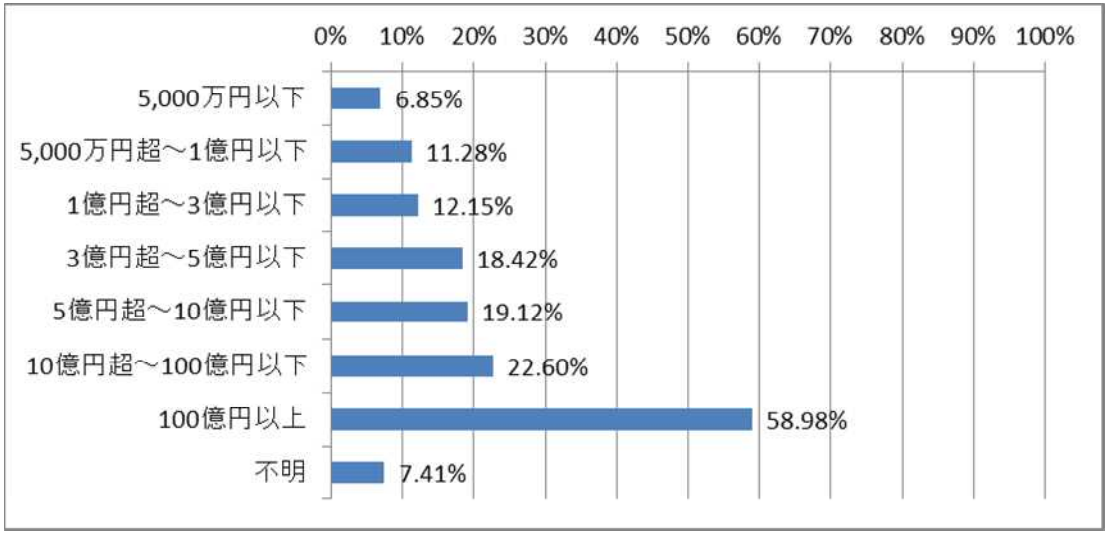
（９）CSIRT整備や訓練の実施
（10）被害発覚後に備えた事前準備

（参考）企業における経営ガイドラインの活用状況

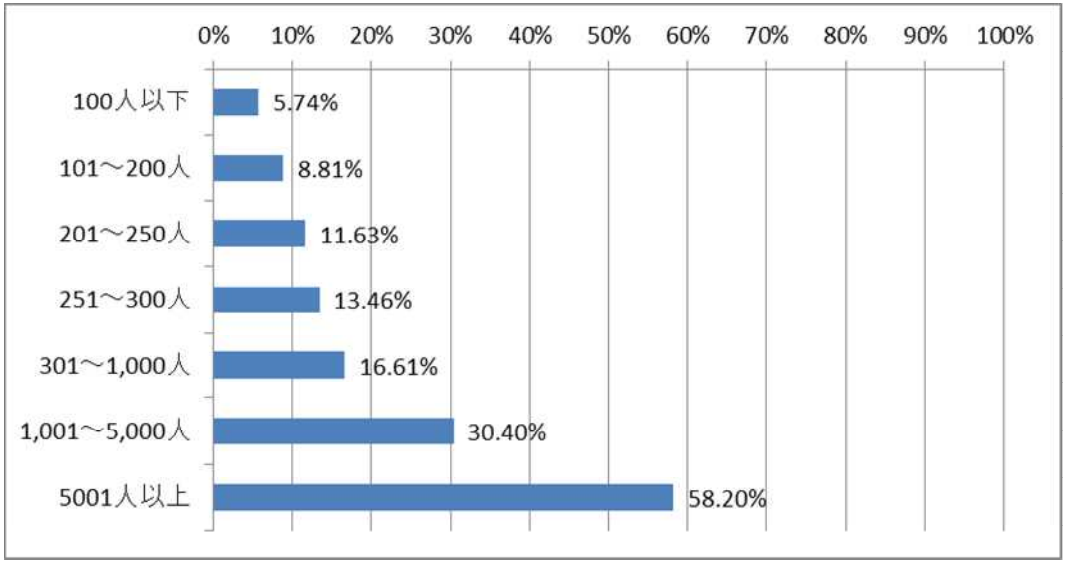
- 企業規模が大きくなるにつれて経営ガイドラインの実施率が高くなっている。
- 特に資本金100億円以上、従業員数5,001人以上の企業においては60%近くが当該ガイドラインを活用している。

経営ガイドラインの参照状況（全体）

経営ガイドラインの参照状況（資本金別）



経営ガイドラインの参照状況（従業員数別）



(*)平成28年度我が国におけるデータ駆動型社会に係る基盤整備（情報処理実態調査の分析及び調査設計等事業）調査報告書（経済産業省）のデータを元に作成
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H28_report.pdf

パブコメ開始時点

重要１０項目の整理（改訂案のポイント①）

- 新規に２項目（(5)対策実施と(8)復旧）追加するとともに、既存の項目を再整理した。
- 重要１０項目の並びについても、３原則、及び作業の時系列を意識して再整理した。

1.リーダーシップの表明と体制の構築	
(1)	セキュリティポリシーの策定
(2)	サイバーセキュリティリスク管理体制の構築
2.サイバーセキュリティリスク管理の枠組み決定	
(3)	リスクの把握、対策目標と計画の策定
(4)	PDCAの実施と対策の開示
(5)	サプライチェーンセキュリティ対策の実施
3.サイバー攻撃を防ぐための事前対策	
(6)	セキュリティ対策のための資源確保
(7)	ITシステム管理の委託範囲の特定
(8)	情報共有活動への参加
4.サイバー攻撃を受けた場合に備えた準備	
(9)	緊急時の対応体制の整備
(10)	被害発覚後の準備

＜経営者がリーダーシップをとった対策の推進＞	
セキュリティマネジメント体制の構築	
(1)	セキュリティポリシーの策定
(2)	サイバーセキュリティリスク管理体制の構築
(3)	セキュリティ対策のための資源確保
セキュリティリスクの特定と対策の実装	
(4)	リスクの把握、対策目標と計画の策定
(5)	リスク対応策（防御・検知・分析）の実施
(6)	PDCAの実施と対策の開示
サイバー攻撃を受けた場合に備えた体制構築	
(7)	緊急時の対応体制の整備
(8)	復旧体制の整備
＜サプライチェーンセキュリティ対策の推進＞	
(9)	サプライチェーンセキュリティ対策の実施
＜関係者とのコミュニケーションの推進＞	
(10)	情報共有活動への参加

新規追加項目　類似項目をマージ

サイバーセキュリティフレームワーク（CSF）との対応関係の整理（改訂案のポイント②）

- 経営ガイドライン付録Ａにて、チェック項目とCSFの対応関係を提示
  （過去に経営ガイドラインを参照している企業から、経営ガイドラインとCSFの対応関係を明示してほしいとの要望があったため）

サイバーセキュリティ経営ガイドラインVer2.0(Draft)より一部抜粋

(1)　サイバーセキュリティリスクの認識、組織全体での対応の策定

□　経営者がサイバーセキュリティリスクを経営リスクの１つとして認識している	(ー)
□　経営者が、組織全体としてのサイバーセキュリティリスクを考慮した対応方針（セキュリティポリシー）を策定し、宣言している	(ID.GV-1)
□　法律や業界のガイドライン等の要求事項を把握している	(ID-GV-3) (DE.DP-2)

サイバーセキュリティ経営ガイドラインのチェック項目

CSFの要求事項

パブコメ開始時点

インシデント発生時に調査すべき事項を追加（改訂案のポイント③）

- インシデント発生時に、企業が調査しておくべき事項を参考情報（付録C）として追加

項番	名称		説明
1	インシデントの分類		ウイルス感染、不正アクセス、（D）DoS攻撃のいずれかを記載。
2	事業分類		日本標準産業分類の中分類を記載。 複数の分類にまたがる場合は、最も売上げが高い業種で分類。 http://www.soumu.go.jp/toukei_toukatsu/index/seido/sangyo/02toukatsu01_03000044.html
3	事業者名（会社名）		事業者名を記入。委託先の場合、委託元の事業者名を記載。 発生した時点と現時点での事業者の名称が異なる場合、（　）に現時点の名称を記載。
4	責任者（担当者）		本件に関する責任者および担当者の所属部署、氏名を記載。
5	連絡先		項番4の責任者および担当者に連絡が可能な電話番号を記載。　また、連絡が可能な曜日および時間帯も併記すること。

インシデントが発生した際に調査すべき事項

インシデントの状況を記載する欄

中小企業の情報セキュリティ対策ガイドライン（平成28年11月15日公開）

- 中小企業向けのガイドラインをIPAにて公開。
- これまでセキュリティ対策を実施していなかった企業向けの対策や、ある程度対策の進んでいる企業向けの対策の提示など、企業のレベルに合わせてステップアップできるような構成としている。

ガイドライン本体

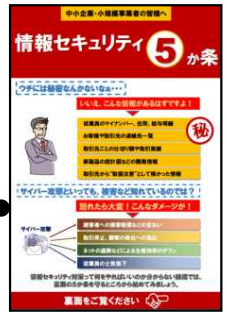
経営者向けの解説

サイバーセキュリティ経営ガイドラインの内容を中小企業向けに整理し、**経営者が認識すべき３原則と実施すべき重要７項目**を解説

管理者向けの解説

管理者が具体的にセキュリティ対策を実施していくための方法を、**企業のレベルに合わせて段階的にステップアップできる**ような構成で解説

Step1 まず始める



最低限実施すべき
セキュリティ対策の5箇条

Step2 現状を知り改善する

簡易的な
セキュリティ対策の25項目

Step3 本格的に取り組む

セキュリティポリシーを策定し、
組織的な対策の取り組み

Step4 改善を続ける

第三者認証(ISMS)の取得を
目指した取り組み

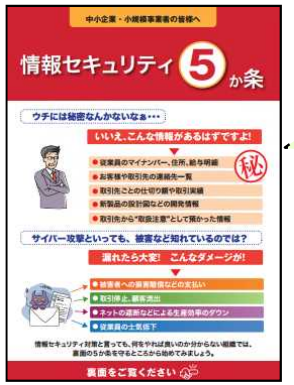
（参考）セキュリティ対策自己宣言「SECURITY ACTION」

- 中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度をIPAにて開始(*)。
- 二つ星を宣言した企業には、サイバー保険の保険料を割り引く制度も損保会社（損保ジャパン）より提供。

★ 一つ星

SECURITY ACTION ★
セキュリティ対策自己宣言

情報セキュリティ5か条に取り組む企業



① OS・ソフトウェアの最新化
（パッチ適用、バージョンアップ）
② ウイルス対策ソフトの導入
③ 強固なパスワード設定
④ データ等は必要最低限の人のみに共有
⑤ 攻撃の手口の把握

★★ 二つ星

SECURITY ACTION ★★
セキュリティ対策自己宣言

情報セキュリティ自社診断により自社の状況を把握し、セキュリティポリシーを策定する企業

25の診断項目により
自社の対策状況を把握

セキュリティポリシー
策定のためのひな形も提供

(*) https://www.ipa.go.jp/security/security-action/