Securify Scan

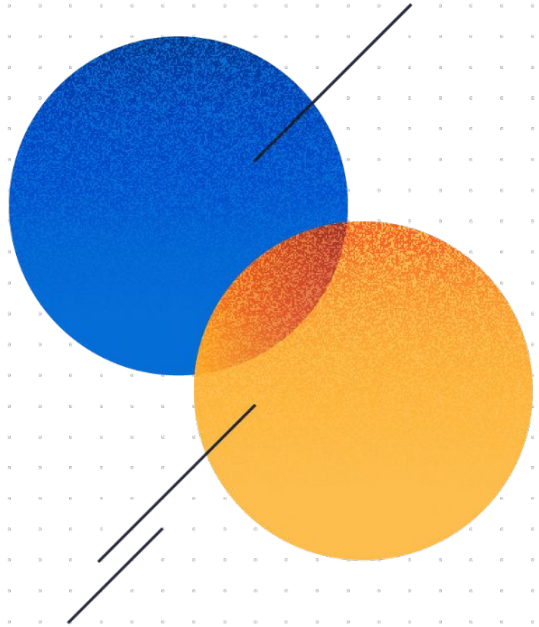
3-SHAKE

あなたのビジネスを守るために！

経営層が抑えておくべき

サイバーセキュリティ経営ガイドライン

目次



01

サイバーセキュリティにおけるガイドラインとは

ガイドラインとは

Securify Scan

「ガイドライン」とは、新たに施行される法律に対応して、各官庁や外郭団体から発表される「法律の内容をより具体化し、何をすればよいかを明確にする指針」です

- サイバーセキュリティ関連の法律では、「 ○○しなければならない」といった条文が多数見られる一方、「具体的に何を、どの程度行えばよいか」について明記されていません
- このため、官庁または外郭団体は、「関係する事業者または個人は、具体的にこのようなアクションを行うべきである」という、**法律に対応する行動指針** を発表します。これがガイドラインです。
- ガイドラインには大きく分けて**「義務」と「努力義務」**の2つが記載されています
  - **「義務」**は、対応必須となる項目のことで、対応しない場合は法律違反となります。
  - **「努力義務」**は、対応が望ましいものの、義務化はされていないため、対応しなかった場合も法律違反となりません
- 以下では、全ての組織の指針となる「サイバーセキュリティ経営ガイドライン」を紹介します

02

サイバーセキュリティにおける ガイドライン紹介

サイバーセキュリティ経営ガイドライン [経済産業省] (1)

Securify Scan

経済産業省が作成する**「サイバーセキュリティ経営ガイドライン」は、企業の経営者が率先してセキュリティ対策を推進する**ことを目的とします。サイバーセキュリティ対策をはじめる組織において、最初に対応すべき内容が網羅されています。

- 当ガイドラインの必要性
  - 適切なセキュリティ投資を行わずに社会に損害を与えた場合、リスク対応の是非、経営責任、法的責任が追求され、ビジネスに影響をもたらす可能性がある
  - セキュリティ投資は、ITの利活用を通じた企業の成長においても重要な要素となる
- 経営者が認識すべき原則
  - **リーダーシップ**: セキュリティ投資・責任者の任命など、適切な経営資源配分の実施
  - **委託先管理**: 自社・ビジネスパートナー・委託先を含めたセキュリティ対策の徹底
  - **コミュニケーション**: 平時からサイバーセキュリティのコミュニケーションを積極的に実施

サイバーセキュリティ経営ガイドライン [経済産業省] (2)

Securify Scan

- ガイドライン付録には、各テーマごとに必要な情報が提供されている （要約版スライドもあり）
  - **付録A: サイバーセキュリティ経営チェックシート** (ガイドライン18-21ページ)
    - 重要10項目が適切に実施されているかどうかを確認するためのチェックシート
  - **付録B: サイバーセキュリティ対策に関する参考情報** (ガイドライン22-26ページ)
    - 重要10項目、指示に関するリンク集
  - **付録C: インシデント発生時に組織内で整理しておくべき事項** (Excel)
    - インシデント発生時の対応フロー、チェックすべき項目リスト
  - **付録D: 国際規格 ISO/IEC27001 及び 27002 との関係** (ガイドライン27ページ)
    - 情報セキュリティマネジメントの国際規格と重要 10項目の対応表
  - **付録E: 用語の定義** (用語集、ガイドライン 28-31ページ)
  - **付録F: サイバーセキュリティ体制構築・人材確保の手引き 第2.0版** (ドキュメント)
    - 組織体制の整備、セキュリティ人材の対応分野マップ、人材確保の方法を解説

サイバーセキュリティ経営ガイドライン: 重要10項目 [1]

Securify Scan

経営者がリーダーシップをとったセキュリティ対策の推進

- **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**
  - 対策を怠った場合
    - 経営者がサイバーセキュリティリスクへの対応を策定し、宣言していないと、対策実行に一貫性を欠く。また、対策の重要度が伝わらず会社の信頼性が向上しない
  - 対策例
    - 経営方針と整合性が取れたセキュリティポリシーを策定する
    - セキュリティポリシーを多くの従業員がアクセスできる場所に掲載し、従業員教育を行い周知徹底する
    - セキュリティポリシーを一般公開し、信頼性を高める

サイバーセキュリティ経営ガイドライン: 重要10項目 [2]

Securify Scan

経営者がリーダーシップをとったセキュリティ対策の推進

- **2.サイバーセキュリティリスク管理体制の構築**
  - 対策を怠った場合
    - 管理体制がない場合は、組織としてセキュリティリスクが把握できない
    - 組織内の他のリスク管理体制と整合を取らないと、組織全体のリスク管理と不整合が生じる恐れがある
  - 対策例
    - CISO等は、サイバーセキュリティリスク体制を構築し、責任範囲を明確にする
    - CISO等は、組織内の経営リスクに関する委員会に参加する
    - 取締役、監査役は管理体制が構築、運用されているかを監査する
    - 企画・設計段階からサイバーセキュリティ対策を考慮した体制を構築する

サイバーセキュリティ経営ガイドライン: 重要10項目 [3]

Securify Scan

経営者がリーダーシップをとったセキュリティ対策の推進

- **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**
  - 対策を怠った場合
    - セキュリティ対策の実施や人材の確保、外部ベンダへの委託が困難になる
    - 有能なセキュリティ人材を自社にとどめておけない
  - 対策例
    - 必要なセキュリティ対策を明確にし、予算を確保する
    - 従業員やセキュリティ担当者向けのセキュリティ研修・教育予算を確保する
    - セキュリティ人材の雇用が困難な場合は、専門ベンダの活用を検討する
    - 社内のセキュリティ人材育成、キャリアパスを設計検討する
    - 自社内で人材育成が難しい場合は、外部の研修を活用する

サイバーセキュリティ経営ガイドライン: 重要10項目 [4]

Securify Scan

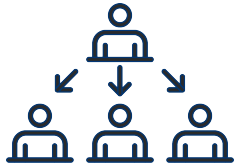
経営者がリーダーシップをとったセキュリティ対策の推進

- **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**
  - 対策を怠った場合
    - 適切なリスク対応を実施しないと、過度の対策で業務に支障を来す恐れがある
    - 受容できないリスクがある場合、想定外の損失を被る恐れがある
  - 対策例
    - 守るべき情報を特定し、それがどのように保存されているか把握する
    - 守るべき情報に対して、発生しうるセキュリティリスクを把握する
    - 把握したリスクに対して、実施するセキュリティ対策を以下の観点で検討する
      - リスク低減策の実施、リスク回避策の実施、リスク移転策の実施
    - リスク発生確率や損害を考慮し、対策不要としたリスクを「残留リスク」と識別する
    - 情報保護におけるセキュリティリスクを把握し、セキュリティ対策を検討する
    - 法令上、安全管理措置義務がある情報は、リスク特定と迅速な情報保護対策を検討する
    - セキュリティバイデザインの観点で、企画・設計段階からセキュリティ対策を考慮する

サイバーセキュリティ経営ガイドライン: 重要10項目 [5]

Securify Scan

経営者がリーダーシップをとったセキュリティ対策の推進



- **5.サイバーセキュリティリスクに対応するための仕組みの構築**
  - 対策を怠った場合
    - 攻撃時の被害拡大・重要情報の窃取など致命的な被害となる可能性がある
  - 対策例
    - 重要業務を行う端末、ネットワーク、システム /サービスは多層防御を実施する
    - 脆弱性診断を実施し、システムなどの脆弱性の検出・対処を行う
    - 重要情報は、暗号化、バックアップ、改ざん検知の仕組みを導入する
    - アクセスログや通信ログからサイバー攻撃を監視・検知する仕組みを構築する
      - 検知すべきイベントを明確にし、発生時は速やかに関係者にアラートを上げるなど対策。スキルを持つ人材がいない場合は、外部監視サービス利用を検討する
    - 従業員に対する教育を行い、適切な対処が行えるよう日頃から備える
      - ソフトウェア更新の徹底、マルウェア対策ソフト導入など低減策の実施、定期的な確認を行う。不審メール受信時は、報告とともに全従業員に注意喚起を行う

サイバーセキュリティ経営ガイドライン: 重要10項目 [6]

Securify Scan

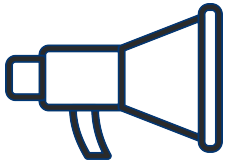
経営者がリーダーシップをとったセキュリティ対策の推進

- **6.サイバーセキュリティ対策における PDCA サイクルの実施**
  - 対策を怠った場合
    - PDCA [計画、実行、確認評価、改善] の実施体制がないと、計画が確実に実施されない恐れがある
  - PDCA の実施体制の整備
    - セキュリティリスク管理に関する KPI を定め、状況を経営者に報告
    - 必要に応じて、セキュリティ診断や監査を受け、問題点を検出し、改善を実施
    - 新たなリスク発見により、追加対応が必要な場合には、 速やかに対処方針を修正
    - セキュリティ対策状況について、セキュリティリスクの性質・度合いに応じて、報告書等を通じて開示を検討

サイバーセキュリティ経営ガイドライン: 重要10項目 [7]

Securify Scan

経営者がリーダーシップをとったセキュリティ対策の推進



- **7.インシデント発生時の緊急対応体制の整備**
  - 緊急時において、以下を実施できるような対応体制を構築
    - 各種ログの保全や感染端末の確保等の証拠保全が行える体制構築、関係機関との連携による調査の実施
    - インシデント収束後の再発防止策の策定、所管省庁等への報告など演習を実施
    - 再発防止策の検討にあたっては、必要に応じて外部の専門家の知見を活用
    - 緊急連絡網、情報開示の通知先一覧を整備し共有
    - 初動対応時の影響を検討、組織内各部署が速やかに協力できるよう取り決める
    - 関係法令を確認し、法的義務が履行されるよう手続きを確認
    - インシデントに関する被害状況、他社への影響等について経営者に報告

サイバーセキュリティ経営ガイドライン: 重要10項目 [8]

Securify Scan

経営者がリーダーシップをとったセキュリティ対策の推進

- **8.インシデントによる被害に備えた復旧体制の整備**
  - 業務停止等に至った場合に、以下を実施できるような復旧体制を構築する
    - 攻撃により業務停止した場合、速やかに復旧するため、関係機関と　の連携や復旧作業実施を指示
      - 加えて、復旧手順に従った演習を実施
    - 業務の復旧目標（重要な業務をいつまでに復旧すべきか）について、組織全体として整合をとる
      - 例: BCPで定めている目標との整合を考慮する

サイバーセキュリティ経営ガイドライン: 重要10項目 [9]

Securify Scan

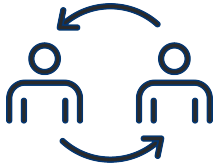
サプライチェーンセキュリティ対策の推進

- **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対策　及び状況把握**
  - 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対策及び状況把握
  - 系列企業・ビジネスパートナー・システム管理の委託先等と、セキュリティ対策の内容を明確にした上で契約
  - 系列企業・ビジネスパートナー・システム管理の委託先等から、セキュリティ対策状況の報告を受け、把握
  - 重要情報を委託先に預ける場合は、委託先の経営状況等も踏まえて、情報の安全性の確保が可能かどうかを定期的に確認
  - 系列企業・ビジネスパートナー・システム管理の委託先等は、SECURITY ACTIONの実施を確認 (ISMS 等の認証取得がより望ましい)
  - 委託先はサイバー保険加入が望ましい

サイバーセキュリティ経営ガイドライン: 重要10項目 [10]

Securify Scan

サプライチェーンセキュリティ対策の推進



- **10.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供**
  - 情報入手するのみならず、積極的に情報を提供
  - 諸機関の注意喚起情報を、自社のサイバーセキュリティ対策に活用
  - CSIRT 間における情報共有、日本シーサート協議会 等の活動参加を通じた情報収集を自社の対策に活用
  - IPA に対し、告示に基づいて マルウェア情報や不正アクセス情報の届出
  - JPCERT コーディネーションセンター にインシデントに関する情報を提供
  - 重要インフラ事業者の場合には、J-CSIPなどの情報共有の仕組みを利用

まとめ

- サイバーセキュリティについては、政府として重要項目として、ガイドラインの整備が進められています。
- ガイドラインの整備は進められている状況ですが、あくまで守る主体は各企業に一任されています。

次ページで紹介する、**スリーシェイクが提供している**「SecurifyScan」を利用することで、
ツールによる脆弱性診断で可視化し、脆弱性の対策を行うことができますので、「重要項目の5.サイバーセキュリティリスクに対応するための仕組みの構築」のアクションの対応の一つとして、ぜひお試しください。

Securify Scan（セキュリファイ スキャン）とは

Securify Scan

Webアプリケーションの
継続的セキュリティを簡単に実現

Securify Scan

Securify Scan（セキュリファイスキャン）は自社のプロダクトに対して、**手軽に、何度でも**脆弱性診断の実施を可能にし、セキュリティレベルを可視化DevSecOpsへの取り組みをサポートします。

▸ **まずは2週間の無料トライアルでお試しいただけます！**

Thank you.