Sec93_01_サイバーセキュリティ経営ガイドラインVer2.0の内容要約

20171116003-1.pdf

概要

「サイバーセキュリティ経営ガイドラインVer2.0」の内容を要約したもの

「サイバーセキュリティ経営ガイドラインVer2.0」を活用する際の索引として利用することを想定

原本
- 「サイバーセキュリティ経営ガイドラインVer2.0」【2017年11月16日METI】
- https://www.meti.go.jp/policy/netsecurity/mng_guide.html
  - https://www.meti.go.jp/policy/netsecurity/mng_guide.html

改版履歴
- 2022年1月6日 改版
- 2020年7月31日 初版

サイバーセキュリティ経営ガイドライン・概要

I. サイバーセキュリティは経営問題
- セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要
- セキュリティ投資は必要不可欠かつ経営者としての責務である。

II. 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を認識し、リーダーシップによって対策を進めることが必要
- (2) 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
- (3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

III. サイバーセキュリティ経営の重要１０項目
- 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
- 指示２：サイバーセキュリティリスク管理体制の構築
- 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
- 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
- 指示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
- 指示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
- 指示７：インシデント発生時の緊急対応体制の整備
- 指示８：インシデントによる被害に備えた復旧体制の整備
- 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対策及び状況把握
- 指示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

１．はじめに

本ガイドラインのVer1.0、及び1.1は、経済産業省と独立行政法人情報処理推進機構（IPA）の共催である「サイバーセキュリティリスクと企業経営に関する研究会」、Ver2.0は「サイバーセキュリティ経営ガイドライン改訂に関する研究会」においてそれぞれ検討が行われ、とりまとめたものである。

- １．１．サイバーセキュリティ経営ガイドラインの背景と位置づけ
  - また、
    内閣サイバーセキュリティセンター（NISC）では、
    企業の経営層を対象としてグローバルな競争環境の変化の中でサイバーセキュリティをより積極的な経営への「投資」と位置づけ、
    企業の自発的な取組を促進するため、
    サイバーセキュリティの基本的な考え方と企業の視点別の取組方法について、
    考え方を示した文書（「企業経営のためのサイバーセキュリティの考え方」5）を策定している。
    - 中小企業の情報セキュリティ対策ガイドライン(IPA)
      - guideline
    - 企業経営のためのサイバーセキュリティの考え方（NISC）
      - keiei.pdf
- １．２．本ガイドラインの構成と活用方法
  - 巻頭の概要は経営者向け、
    ２章～３章はサイバーセキュリティ対策を実施する上での責任者である担当幹部（CISO等）及びセキュリティ担当者向けである。
  - 経営者においては、 最低限、
    巻頭の概要に目を通した上で、
    ３原則を認識し、
    重要１０項目についてCISO等に指示をすべきである。
  - CISO等は、 経営者の指示に基づき、
    重要１０項目の各解説頁の「対策例」も参考にしつつ、
    セキュリティ対策の取組みを、
    セキュリティ担当者に対してより具体的に指示をし、
    推進することが必要である。
  - また、 本ガイドラインでは、
    重要１０項目の実施にあたって、
    参考となる情報を付録として提示している。
    各付録の内容は以下の通りである。
    - 付録A
      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を実施する上で参考となる資料等
    - 付録C
      インシデント発生時に原因調査等を行う際、
      組織内で整理しておくべき事項
    - 付録D
      重要１０項目とISO/IEC27001、27002の関係性
    - 付録E
      本ガイドラインで使用している用語の定義
  - なお、
    内部犯行による情報漏えい等のリスクへの対処については、 必要に応じ、
    「組織における内部不正防止ガイドライン」（IPA）6を参照することで、
    より効果的な対策が可能となる。
    - 組織における内部不正防止ガイドライン（IPA）
      - 000044615.pdf
  - また、
    サイバーセキュリティ対策にこれから取り組む企業においては「中小企業の情報セキュリティ対策ガイドライン」（IPA）も参考となる。

２．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を認識し、
  リーダーシップによって対策を進めることが必要
  - 【経営者自らがリーダーシップを発揮して適切な経営資源の配分を行う】
  - □
    ビジネス展開や企業内の生産性の向上のためにITサービス等の提供やITを利活用する機会は増加傾向にあり、
    サイバー攻撃が避けられないリスクとなっている現状において、
    経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である。
  - □ また、
    サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった後、
    企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。
  - □ このため、
    サイバーセキュリティリスクを多様な経営リスクの中での一つとして位置づけ、
    サイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）を任命するとともに、
    経営者自らがリーダーシップを発揮して適切な経営資源の配分を行うことが

必要である。

【自社のみならず、
サプライチェーンのビジネスパートナーやシステム管理等の委託先を含めたセキュリティ対策を徹底する】

（２） 自社は勿論のこと、
ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要

□
サプライチェーンのビジネスパートナーやシステム管理等の委託先がサイバー攻撃に対して無防備であった場合、

自社から提供した重要な情報が流出してしまうなどの問題が生じうる。

□ このため、 自社のみならず、
サプライチェーンのビジネスパートナーやシステム管理等の委託先を含めたセキュリティ対策を徹底することが必要である。

【平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行う】

（３）
平時及び緊急時のいずれにおいても、

サイバーセキュリティリスクや対策に係る情報開示など、
関係者との適切なコミュニケーションが必要

□
万一サイバー攻撃による被害が発生した場合、 関係者と、
平時から適切なセキュリティリスクのコミュニケーションができていれば，
関係者の不信感の高まりを抑えることができる。

□ このため、
平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行うことが必要である。

３．サイバーセキュリティ経営の重要１０項目

経営者は、 CISO等に対して、
以下の１０項目を指示し、
着実に実施させるとともに、
実施内容についてCISO等から定期的に報告を受けることが必要である。
自組織での対応が困難な項目については、
外部委託によって実施することも検討する。

３．１．サイバーセキュリティリスクの管理体制構築

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

サイバーセキュリティリスクを経営リスクの一つとして認識し、
組織全体での対応方針（セキュリティポリシー）を策定させる。

対策を怠った場合のシナリオ

・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、
サイバーセキュリティ対策などの実行が組織の方針と一貫したものとならない。

・トップの宣言により、
ステークホルダー（株主、 顧客、
取引先など）の信頼性を高め、
ブランド価値向上につながるが、
宣言がない場合は、
企業におけるサイバーセキュリティへの重要度がステークホルダーに伝わらず信頼性を高める根拠がないこととなる。

指示２
サイバーセキュリティリスク管理体制の構築

サイバーセキュリティ対策を行うため、
サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。

その際、
組織内のその他のリスク管理体制とも整合を取らせる。

対策を怠った場合のシナリオ

・サイバーセキュリティリスクの管理体制を整備していない場合、
組織としてサイバーセキュリティリスクの把握が出来ない。

・組織内におけるその他のリスク管理体制との整合を取らないと、
組織全体としてのリスク管理の方針と不整合が生じる恐れがある。

サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。

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

対策を怠った場合のシナリオ

・適切な予算確保が出来ていない場合、
組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、
信頼できる外部のベンダへの委託が困難となる恐れがある。

・適切な処遇の維持、
改善ができないと、
有能なサイバーセキュリティ人材を自社にとどめておくことができない。

3．2．サイバー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

経営戦略の観点から守るべき情報を特定させた上で、
サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、
リスクに対応するための計画を策定させる。

その際、
サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、
残留リスクを識別させる。

対策を怠った場合のシナリオ

・企業の経営戦略に基づき、
各企業の状況に応じた適切なリスク対応を実施しなければ、
過度な対策により通常の業務遂行に支障をきたすなどの不都合が生じる恐れがある。

・受容できないリスクが残る場合、
想定外の損失を被る恐れがある

指示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

サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる。

対策を怠った場合のシナリオ

・サイバーセキュリティリスクに応じた適切な対策が行われていない場合、

サイバー攻撃が発生した場合の被害が拡大する可能性がある。

・技術的な取組を行っていたとしても、
攻撃の検知・分析とそれに基づく対応ができるよう、
適切な運用が行われていなければ、
サイバー攻撃の状況を正確に把握することができず、
攻撃者に組織内の重要情報を窃取されるなどの、
致命的な被害に発展する恐れがある。

指示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

計画を確実に実施し、
改善していくため、
サイバーセキュリティ対策をPDCAサイクルとして実施させる。

その中で、
定期的に経営者に対策状況を報告させた上で、
問題が生じている場合は改善させる。

また、
ステークホルダーからの信頼性を高めるため、 対策状況を開示させる。

対策を怠った場合のシナリオ

・PDCA（Plan[計画]、 Do[実行]、Check[実施状況の確認・評価]、Act[改善]）を実施する体制が出来ていないと、
立てた計画が確実に実行されない恐れがある。

・最新の脅威への対応ができているかといった視点も踏まえて組織のサイバーセキュリティ対策を定期的に見直さないと、
サイバーセキュリティを巡る環境変化に対応できず、
新たに発生した脅威に対応できない恐れがある。

・適切な開示を行わなかった場合、
社会的責任の観点から、
事業のサイバーセキュリティリスク対応についてステークホルダーの信頼を失うとともに、
インシデント発生時に企業価値が大きく低下する恐れがある。

3．3．インシデント発生に備えた体制構築 3

- 指示7
  インシデント発生時の緊急対応体制の整備
  - 影響範囲や損害の特定、
    被害拡大防止を図るための初動対応、

    再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT等）を整備させる。
  - 被害発覚後の通知先や開示が必要な情報を把握させるとともに、
    情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。
  - また、
    インシデント発生時の対応について、
    適宜実践的な演習を実施させる。
  - 対策を怠った場合のシナリオ
    - ・緊急時の対応体制を整備していないと、
      原因特定のための調査作業において、

      組織の内外の関係者間のコミュニケーションが取れず、
      速やかな対処ができない。
    - ・速やかな情報開示が行われない場合、
      顧客や取引先等にも被害が及ぶ恐れがあり、
      損害賠償請求など責任を問われる場合がある。
    - ・法的な取り決めがあり、
      所管官庁等への報告が義務づけられている場合、
      速やかな通知がないことにより、
      罰則等を受ける場合がある。
    - ・演習を実施していないと、
      不測の事態が起こった際に、
      担当者が緊急時に適切に行動することが出来ない。
- 指示8
  インシデントによる被害に備えた復旧体制の整備
  - インシデントにより業務停止等に至った場合、
    企業経営への影響を考慮していつまでに復旧すべきかを特定し、
    復旧に向けた手順書策定や、
    復旧対応体制の整備をさせる。
  - BCPとの連携等、
    組織全体として整合のとれた復旧目標計画を定めさせる。
  - また、
    業務停止等からの復旧対応について、
    適宜実践的な演習を実施させる。
  - 対策を怠った場合のシナリオ
    - ・重要な業務が適切な時間内に復旧できず、
      企業経営に致命的な影響を与える恐れがある。
    - ・演習を実施していないと、
      不測の事態が起こった際に、
      担当者が緊急時に適切に行動することが出来ない。

3．4．サプライチェーンセキュリティ対策の推進

- 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対策及び状況把握
  - 監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCAについて、 系列企業、
    サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる。
  - システム管理等の委託について、
    自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。
  - 中小企業自らがセキュリティ対策に取り組むことを宣言する制度
    - security-action
  - 対策を怠った場合のシナリオ
    - ・系列企業やサプライチェーンのビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないと、
      これらの企業を踏み台にして自社が攻撃されることもある。 その結果、
      他社の２次被害を誘発し、
      加害者となる恐れもある。 また、
      緊急時の原因特定などの際に、
      これらの企業からの協力を得られないことにより事業継続に支障が生ずる。
    - ・システム管理などの委託業務において、
      自組織で対応する部分と委託する部分の境界が不明確となり、
      対策漏れが生じる恐れがある。

3．5．ステークホルダーを含めた関

係者とのコミュニケーションの推進

指示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

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、
サイバー攻撃に関する情報共有活動へ参加し、
積極的な情報提供及び情報入手を行わせる。

また、
入手した情報を有効活用するための環境整備をさせる。

対策を怠った場合のシナリオ

・情報共有活動への参加により、解析した攻撃手法などの情報を用いて、
他社における同様の被害を未然に防止することができるが、
情報共有ができていないと、
社会全体において常に新たな攻撃として対応することとなり、
企業における対応コストが低減しない。

付録A サイバーセキュリティ経営チェックシート

※本チェックシートは、
基本的な項目を示しており、
企業の状況に応じて追加対策等を行うことも重要である

※以降では、
本チェック項目とNISTが提供するサイバーセキュリティフレームワーク10との対応関係も合わせて提示する（括弧書きはサイバーセキュリティフレームワークのサブカテゴリーの識別子に対応）

Framework for Improving Critical Infrastructure Cybersecurity(NIST)

cybersecurity-framework-021214.pdf

＜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＞

（サイバーセキュリティリスクの管理体制構築）

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　（－）

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:
自組織の情報セキュリティポリシーを定めている。

A.5.1.1
情報セキュリティのための方針群

ID.GV-3:
プライバシーや市民の自由に関する義務を含む、
サイバーセキュリティに関する法規制上の要求事項を理解し、
管理している。

A.18.1
法的及び契約上の要求事項の順守

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

DE.DP-2:
検知活動は必要なすべての要求事項を満たしている。

A.18.1.4
プライバシー及び個人を特定できる情報（PII）の保護

指示2
サイバーセキュリティリスク管理体制の構築

組織の対応方針（セキュリティポリシー）に基づき、
CISO等からなるサイバーセキュリティリスク管理体制を構築している　（－）

サイバーセキュリティリスク管理体制において、
各関係者の役割と責任を明確にしている

ID.GV-2:
情報セキュリティ上の役割と責任について、
内部と外部パートナーとで調整・連携している。

A.6.1.1
情報セキュリティの役割及び責任

A.7.2.1 経営陣の責任

組織内のリスク管理体制とサイバーセキュリティリスク管理体制の関係を明確に規定している

ID.GV-4:
ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している。

(ISO N/A)

必要なサイバーセキュリティ対策を明確にし、
経営会議などで対策の内容に見合った適切な費用かどうかを評価し、
必要な予算を確保している　（－）

PR.AT-2:
権限を持つユーザが役割と責任を理解

A.6.1.1
情報セキュリティの役割及び責任

- 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
  - サイバーセキュリティ対策を実施できる人材を確保し、
    各担当者が自身の役割を理解している
    （組織の内外問わず）
    - している。
      - A.7.2.2
        情報セキュリティの意識向上，
        教育及び訓練
    - PR.AT-3:
      第三者である利害関係者（例：供給業者、 顧客、
      パートナー）が役割と責任を理解している。
      - A.6.1.1
        情報セキュリティの役割及び責任
      - A.7.2.2
        情報セキュリティの意識向上，
        教育及び訓練
    - PR.AT-4:
      上級役員が役割と責任を理解している。
      - A.6.1.1
        情報セキュリティの役割及び責任
      - A.7.2.2
        情報セキュリティの意識向上，
        教育及び訓練
    - PR.AT-5:
      物理セキュリティおよび情報セキュリティの担当者が役割と責任を理解している。
      - A.6.1.1
        情報セキュリティの役割及び責任
      - A.7.2.2
        情報セキュリティの意識向上，
        教育及び訓練
  - 組織内でサイバーセキュリティ人材を育成している
    - PR.AT-1:
      すべてのユーザに情報を周知し、
      トレーニングを実施している。
      - A.7.2.2
        情報セキュリティの意識向上，
        教育及び訓練
  - 組織内のサイバーセキュリティ人材のキャリアパスの設計を検討、
    及び適正な処遇をしている
    - （−）
  - セキュリティ担当者以外も含めた従業員向けセキュリティ研修等を継続的に実施している
    - PR.AT-1:
      すべてのユーザに情報を周知し、
      トレーニングを実施している。
      - A.7.2.2
        情報セキュリティの意識向上，
        教育及び訓練
- （サイバー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
    - 守るべき情報を特定し、
      当該情報の保管場所やビジネス上の価値等に基づいて優先順位付けを行っている
      - ID.AM-1:
        企業内の物理デバイスとシステムの一覧を作成している。
        - A.8.1.1 資産目録
        - A.8.1.2 資産の管理責任
      - ID.AM-2:
        企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。
        - A.8.1.1 資産目録
        - A.8.1.2 資産の管理責任
      - ID.AM-3:
        企業内の通信とデータの流れの図を用意している。
        - A.13.2.1 情報転送の方針及び手順
      - ID.AM-4:
        外部情報システムの一覧を作成している。
        - A.11.2.6
          構外にある装置及び資産のセキュリティ
      - ID.AM-5:
        リソース（例：ハードウェア、
        デバイス、 データ、
        ソフトウェア）を、 分類、 重要度、
        ビジネス上の価値に基づいて優先順位付けしている。
        - A.8.2.1 情報の分類
    - 特定した守るべき情報に対するサイバー攻撃の脅威、 脆弱性を識別し、
      経営戦略を踏まえたサイバーセキュリティリスクとして把握している
      - ID.RA-3: 内外からの脅威を特定し、
        文書化している。
        - (ISO N/A)
      - ID.RA-1: 資産の脆弱性を特定し、
        文書化している。
        - A.12.6.1 技術的脆弱性の管理
        - A.18.2.3 技術的順守のレビュー
      - ID.RM-1:
        リスク管理プロセスが自組織の利害関係者によって確立、 管理され、
        承認されている。
        - (ISO N/A)
    - サイバーセキュリティリスクが事業にいかなる影響があるかを推定している
      - ID.RA-4:
        ビジネスに対する潜在的な影響と、
        その可能性を特定している。
        - (ISO N/A)
      - ID.RA-5: リスクを判断する際に、
        脅威、 脆弱性、 可能性、
        影響を考慮している。
        - A.12.6.1 技術的脆弱性の管理
      - ID.RM-2:
        自組織のリスク許容度を決定し、
        明確にしている。
        - (ISO N/A)
    - サイバーセキュリティリスクの影響の度合いに従って、 リスク低減、
      リスク回避、
      リスク移転のためのリスク対応計画を策定している
      - ID.RA-6:
        リスクに対する対応を定め、
        優先順位付けしている。
        - (ISO N/A)
      - ID.RM-3:
        企業によるリスク許容度の決定が、

- 重要インフラにおける目組織の役割と、
その分野に特化したリスク分析の結果に基づいて行われている。 (ISO N/A)

サイバーセキュリティリスクの影響の度合いに従って対策を取らないと判断したものを残留リスクとして識別している
- ID.RA-6:
リスクに対する対応を定め、
優先順位付けしている。 (ISO N/A)
- ID.RM-3:
企業によるリスク許容度の決定が、
重要インフラにおける自組織の役割と、
その分野に特化したリスク分析の結果に基づいて行われている。 (ISO N/A)

重要業務を行う端末、
ネットワーク、 システム、
またはサービスにおいて、
ネットワークセグメントの分離、
アクセス制御、
暗号化等の多層防御を実施している。
- アクセス制御（PR.AC）：
資産および関連施設へのアクセスを、
承認されたユーザ、 プロセス、
またはデバイスと、
承認された活動およびトランザクションに限定している。
  - A.9 アクセス制御
  - A.11 物理的及び環境的セキュリティ
  - A.13 通信のセキュリティ
- データセキュリティ（PR.DS）：
情報と記録（データ）を情報の機密性、 完全性、
可用性を保護するために定められた自組織のリスク戦略に従って管理している。
  - A.8 資産の管理
  - A.12 運用のセキュリティ
  - A.13 通信のセキュリティ
  - A.14 システムの取得、 開発及び保守

システム等に対して脆弱性診断を実施し、
検出された脆弱性に対処している。
- PR.IP-12:
脆弱性管理計画を作成し、
実施している。
  - A.12.6.1 技術的脆弱性の管理
  - A.18.2.2
情報セキュリティのための方針群及び標準の順守

検知すべきイベント（意図していないアクセスや通信）を特定し、
当該イベントを迅速に検知するためのシステム・手順・体制（ログ収集や分析のための手順書策定）を構築している。
- DE.AE-1:
ネットワーク運用のベースラインと、
ユーザとシステム間の予測されるデータの流れを特定し、 管理している。 (ISO N/A)
- DE.AE-5:
インシデント警告の閾値を定めている。 (ISO N/A)
- DE.DP-3:
検知プロセスをテストしている。 A.14.2.8
システムセキュリティの試験

指示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

意図していないアクセスや通信を検知した場合の対応計画（検知したイベントによる影響、
対応者などの責任分担等）を策定している
- DE.AE-4:
イベントがもたらす影響を特定している。 (ISO N/A)
- DE.DP-1: 説明責任を果たせるよう、
検知に関する役割と責任を明確に定義している
A.6.1.1
情報セキュリティの役割及び責任
- DE.DP-4:
イベント検知情報を適切な関係者に伝達している。 A.6.1.2 職務の分離

サイバー攻撃の動向等を踏まえて、
サイバーセキュリティリスクへの対応内容（検知すべきイベント、
技術的対策の強化等）を適宜見直している
- DE.DP-5:
検知プロセスを継続的に改善している。 A.16.1.6
情報セキュリティインシデントからの学習

従業員に対して、
サイバーセキュリティに関する教育（防御の基本となる対策実施（ソフトウェアの更新の徹底、
マルウェア対策ソフトの導入等）の周知、
標的型攻撃メール訓練など）を実施している。
- PR.AT-1:
すべてのユーザに情報を周知し、
トレーニングを実施している。 A.7.2.2
情報セキュリティの意識向上, 教育及び訓練

- 経営者が定期的に、
サイバーセキュリティ対策状況の報告を受け、 把握している （−）
- サイバーセキュリティにかかる外部監査を実施している （−）

指示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

サイバーセキュリティリスクや脅威を適時見直し、
環境変化に応じた取組体制（PDCA）を整備・維持している
- PR.IP-7:
保護プロセスを継続的に改善している。 (ISO N/A)

- サイバーセキュリティリスクや取組状況を外部に公開している （−）

（インシデント発生に備えた体制構築）

- 指示7 インシデント発生時の緊急対応体制の整備
  - 組織の内外における緊急連絡先・伝達ルートを整備している（緊急連絡先には、 システム運用、Webサイト保守・運用、契約しているセキュリティベンダの連絡先含む）
    - RS.CO-3: 対応計画に従って情報を共有している。
      - A.16.1.2 情報セキュリティ事象の報告
    - RS.CO-4: 対応計画に従って、利害関係者との間で調整を行っている。
      - (ISO N/A)
    - RS.CO-5: サイバーセキュリティに関する状況認識を深めるために、外部利害関係者との間で任意の情報共有を行っている。
      - (ISO N/A)
  - サイバー攻撃の初動対応マニュアルを整備している
    - PR.IP-9: 対応計画（インシデント対応および事業継続）と復旧計画（インシデントからの復旧および災害復旧）を実施し、 管理している。
      - A.16.1.1 責任及び手順
      - A.17.1.1 情報セキュリティ継続の計画
      - A.17.1.2 情報セキュリティ継続の実施
    - 復旧計画（RC.RP）：サイバーセキュリティイベントによる影響を受けたシステムや資産をタイムリ ーに復旧できるよう、復旧プロセスおよび手順を実施し、維持している。
      - A.16.1.5 情報セキュリティインシデントへの対応
  - インシデント対応の専門チーム（CSIRT等）を設置している
    - RS.CO-1: 対応が必要になった時の自身の役割と行動の順番を従業員は認識している。
      - A.6.1.1 情報セキュリティの役割及び責任
      - A.16.1.1 責任及び手順
  - 経営者が責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等を定めている
    - RS.CO-2: 定められた基準に沿って、イベントを報告している。
      - A.6.1.3 関係当局との連絡
      - A.16.1.2 情報セキュリティ事象の報告
  - インシデント対応の課題も踏まえて、 初動対応マニュアルを見直している
    - RC.IM-1: 学んだ教訓を復旧計画に取り入れている。
      - (ISO N/A)
    - RC.IM-2: 復旧戦略を更新している。
      - (ISO N/A)
  - インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っている
    - PR.IP-10: 対応計画と復旧計画をテストしている。
      - A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価
- 指示8 インシデントによる被害に備えた復旧体制の整備
  - 被害が発生した場合に備えた業務の復旧計画を策定している
    - ID.BE-5: 重要サービスの提供を支援する、レジリエンスに関する要求事項を定めている。
      - A.11.1.4 外部及び環境の脅威からの保護
      - A.17.1.1 情報セキュリティ継続の計画
      - A.17.1.2 情報セキュリティ継続の実施
      - A.17.2.1 情報処理施設の可用性
    - PR.IP-9: 対応計画（インシデント対応および事業継続）と復旧計画（インシデントからの復旧および災害復旧）を実施し、 管理している。
      - A.16.1.1 責任及び手順
      - A.17.1.1 情報セキュリティ継続の計画
      - A.17.1.2 情報セキュリティ継続の実施
    - 復旧計画（RC.RP）：サイバーセキュリティイベントによる影響を受けたシステムや資産をタイムリ ーに復旧できるよう、復旧プロセスおよび手順を実施し、維持している。
      - A.16.1.5 情報セキュリティインシデントへの対応
  - 復旧作業の課題を踏まえて、復旧計画を見直している
    - RC.IM-1: 学んだ教訓を復旧計画に取り入れている。
      - (ISO N/A)
    - RC.IM-2: 復旧戦略を更新している。
      - (ISO N/A)
  - 組織の内外における緊急連絡先・伝達ルートを整備している
    - RC.CO-1: 広報活動を管理している。
      - (ISO N/A)
    - RC.CO-2: イベント発生後に評判を回復している。
      - (ISO N/A)
    - RC.CO-3: 復旧活動について内部利害関係者と役員、 そして経営陣に伝達している。
      - (ISO N/A)
  - PR.IP-10: 対応計画と復旧計画をテストしている
    - A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価

定期的に復旧対応訓練や演習を行っている　。

<サプライチェーンセキュリティ対策の推進>

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対策及び状況把握

システム管理などについて、
自組織のスキルや各種機能の重要性等を考慮して、
自組織で対応できる部分と外部に委託する部分を適切に切り分けている

ID.BE-3: 企業のミッション、 目標、活動に関して優先順位を定め、伝達している。
(ISO N/A)

ID.BE-4:重要サービスを提供する上での依存関係と重要な機能を把握している。
ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3

A.11.2.2
サポートユーティリティ（ライフライン事業者）

A.11.2.3
ケーブル配線のセキュリティ

A.12.1.3 容量・能力の管理

委託先が実施すべきサイバーセキュリティ対策について、
契約書等により明確にしている

ID.AM-6:
すべての従業員と第三者である利害関係者（例：供給業者、 顧客、パートナー）に対して、サイバーセキュリティ上の役割と責任を定めている。
A.6.1.1
情報セキュリティの役割及び責任

ID.BE-1:
サプライチェーンにおける企業の役割を特定し、 伝達している
A.15.1.3 ICTサプライチェーン

A.15.2.1
供給者のサービス提供の監視及びレビュー

A.15.2.2
供給者のサービス提供の変更に対する管理

PR.IP-8:
保護技術の有効性について、適切なパートナーとの間で情報を共有している。
A.16.1.6
情報セキュリティインシデントからの学習

系列企業、
サプライチェーンのビジネスパートナーやシステム管理の運用委託先などのサイバーセキュリティ対策状況（監査を含む）の報告を受け、
把握している
(−)

<ステークホルダーを含めた関係者とのコミュニケーションの推進>

指示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

各種団体が提供するサイバーセキュリティに関する注意喚起情報やコミュニティへの参加等を通じて情報共有（情報提供と入手）を行い、
自社の対策に活かしている

ID.RA-2:
情報共有フォーラム／ソースより、脅威と脆弱性に関する情報を入手している。
A.6.1.4 専門組織との連絡

マルウェア情報、
不正アクセス情報、
インシデントがあった場合に、
IPAへの届出や一般社団法人JPCERTコーディネーションセンターへの情報提供、
その他民間企業等が推進している情報共有の仕組みへの情報提供を実施している

ID.RA-2:
情報共有フォーラム／ソースより、脅威と脆弱性に関する情報を入手している。
A.6.1.4 専門組織との連絡

付録Ｂ サイバーセキュリティ対策に関する参考情報

重要１０項目全般に関連する参考情報

サイバーセキュリティ経営ガイドライン解説書[Ver.1.0]（IPA）
csmgl-kaisetsusho.html
（サイバーセキュリティ経営ガイドラインの３原則、
重要１０項目を具体的に実施するための考え方について解説。）

中小企業の情報セキュリティ対策ガイドライン[第2.1版]（IPA）
guideline
(中小企業がセキュリティ対策に取り組む上でのポイントを解説したガイドライン。
最低限対策が求められる「情報セキュリティ5か条」や、
企業のセキュリティ対策状況を診断する「5分でできる！情報セキュリティ自社診断」等の付録も提供。）

ISO/IEC 27002:2013（ISO/IEC）
（情報マネジメントシステムの仕様を定めた国際標準規格であり、
情報セキュリティ管理のベストプラクティスを提供。）

重要インフラに係わる企業向けに実施

すべきセキュリティ対策を「特定」、「防御」、「検知」、「対応」、「復旧」の5つの機能に分類し、さらにそれらの機能を22のカテゴリーで提示した米国のガイドライン。重要インフラ以外の企業でも活用可能。）

Framework for Improving Critical Infrastructure Cybersecurity [Version 1.0]（NIST）【2014 年2月12 日】

cybersecurity-framework-021214.pdf

重要インフラのサイバーセキュリティを向上させるためのフレームワーク【IPA和訳】

000038957.pdf

（連邦政府機関が実施すべきセキュリティ対策を提示した米国のガイドライン。
米国連邦政府向けのクラウドサービスを提供する際に、
本ガイドラインへの準拠が要求される場合がある。）

SP800-53 [Rev.4]（NIST）

NIST.SP.800-53r4.pdf

（連邦政府機関以外の組織及び情報システムに対するCUI11を保護する上で実施すべきセキュリティ対策を提示した米国のガイドライン。
米国連邦政府関係の業務を受託する際に、
本ガイドラインへの準拠が要求される場合がある。）

SP800-171 [Rev.1]（NIST）

NIST.SP.800-171r1.pdf

指示３に関連する参考情報

（サイバー攻撃等を防ぐためにどのような対策が必要で、
その対策を実施するためにはどのような人材が必要なのかを例示し、
人材育成を行うためのヒントをまとめたガイドライン。）

ITのスキル指標を活用した情報セキュリティ人材育成ガイド[2015年5月]（IPA）

000039528.pdf

（セキュリティ上の脅威を取り上げ、

被害を防ぐためにはどのような対策を実施すべきかを例示し、
セキュリティ管理者としての役割を具体的に提示したガイドライン。）

職場の情報セキュリティ管理者のためのスキルアップガイド[2015年9月]（IPA）

000047872.pdf

指示４に関連する参考情報

（本ガイドラインの4章にてリスク分析の手法を解説。また、
リスク分析の実施を支援するリスク分析シートも付録して提示。）

中小企業の情報セキュリティ対策ガイドライン[第2.1版]（IPA）

guideline

指示５に関連する参考情報

（標的型攻撃対策として、
システム内部への侵入を前提とした上で、
侵害拡大防止及び監視強化を目的とした内部対策について解説したガイドライン。）

「高度標的型攻撃」対策に向けたシステム設計ガイド[2014年9月]（IPA）

000046236.pdf

（サイバー攻撃への備えと効果的な対策の観点から、
一般的に利用される機器に攻撃者の活動の痕跡をログとして残すための考え方、
それらのログから痕跡を見つけ出す方法等を記載したガイドライン。）

高度サイバー攻撃への対処におけるログの活用と分析方法[1.0版]（JPCERT/CC）

apt-loganalysis.html

（組織における内部不正を防止するために実施すべき対策として、
10の観点（コンプライアンス、職場環境等）のもと30項目の対策を提示したガイドライン。）

組織における内部不正防止ガイドライン[第4版]（IPA）

000057060.pdf

（秘密情報の漏えいを未然に防止するための対策例を集めて紹介したハンドブック。）

秘密情報の保護ハンドブック[平成28年2月]（経済産業省）

trade-secret.htm

指示６に関連する参考情報

（情報セキュリティマネジメントシス

情報セキュリティマネジメントシステム（ISMS）適合性評価制度（JIPDEC）

テムにおける国際標準規格ISO/IEC27001に基づいて第三者認証を行う制度。）

isms.html

サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度（JIPDEC）

（産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムにおける国際標準規格IEC62443-2に基づいて第三者認証を行う制度。）

csms.html

情報セキュリティ管理基準（経済産業省）

（情報セキュリティマネジメントの構築から具体的な管理策に至るまで包括的な内容を含み、
国際標準規格ISO/IEC27001とも整合を持った基準。）

index.html

情報セキュリティ対策ベンチマーク（IPA）

（Web上で質問に答えることによって、
自社のセキュリティ対策の実施状況を散布図、 レーダーチャート、
スコア等で表示するツール。
自社の対策状況を他社の対策状況と比較することも可能。）

benchmark

安全なウェブサイトの作り方[第7版]（IPA）

（セキュリティを考慮したWebサイトを作成するための技術的な対策を提示したガイドライン。
別冊としてWebサイトに脆弱性が存在していないかを確認するためのテスト項目を提示したウェブ健康診断仕様等も提供。）

websecurity.html

JVN（IPA、 JPCERT/CC）

（日本で使用されているソフトウェア等の脆弱性関連情報とその対策情報を提供する、
脆弱性対策情報ポータルサイト。）

jvn.jp

指示７に関連する参考情報

CSIRT構築マテリアル（JPCERT/CC）

（組織的なインシデント対応を行うためのCSIRTを構築する上で、
「構想フェーズ」、
「構築フェーズ」、
「運用フェーズ」のそれぞれの段階で考慮すべきポイントを解説したガイドライン。）

csirt_material

CSIRT構築に役立つ参考資料（日本シーサート協議会）

（CSIRTの構築に際し、
構築初心者／経営者向け説明時／構築担当者の企画・構築・運用の各段階におけるドキュメント類をまとめた参考資料集。）

build-wg-document.html

指示８に関連する参考情報

事業継続ガイドライン[平成25年8月改定]（内閣府）

（事業継続計画の策定・改善にあたって、 事業継続の必要性を明示し、
実施が必要な事項、
望ましい事項等を提示したガイドライン。）

guideline03.pdf

指示９に関連する参考情報

情報サービス・ソフトウェア産業における下請適正取引等の推進のためのガイドライン[平成29年3月]（経済産業省）

（下請適正取引等の推進を図ることを目的として策定したものであり、
個人情報保護やセキュリティ対策に係る取り組み等の考慮すべき事項を解説したガイドライン。）

140313shitaukeGL3.pdf

SECURITY ACTION
セキュリティ対策自己宣言（IPA）

（中小企業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。）

security-action

指示１０に関連する参考情報

届出・相談・情報提供（不正アクセス

（コンピュータウイルス、
不正アクセス、
脆弱性関連情報等に関する届出を行う際の届出様式、 届出先、
届出状況等を提供するWebサイト。

やウイルス等に関する届出）（IPA）　　）

todoke-top-j.html

（標的型サイバー攻撃を受けた際に、

専門的知見を有する相談員が対応する窓口。）

標的型サイバー攻撃特別相談窓口（IPA）

tokubetsu

（重要インフラで利用される機器の製造業者、 電力業界、 ガス業界、
化学業界、 石油業界、
資源開発業界、 自動車業界、
クレジット業界において情報共有と早期対応を行うための活動。）

サイバー情報共有イニシアティブ（J-CSIP）（IPA）

J-CSIP

（サイバー犯罪・サイバーテロの未然防止及び被害の拡大防止を図るために、
ネットワークセキュリティに関する様々な情報を提供するWebサイト。）

@police（警察庁）

cyberpolice

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

20171116003-2.xlsx

インシデント発生時、
原因調査等を行う際に組織内で整理しておくべき事項を示す。
本資料の内容を参考に原因調査等を行い、
必要な事項については適宜経営者や関係者に報告を行うことが望ましい。
本付録では、
以下の5つの表を提供する。
インシデントの状況に応じて該当する表を利用すること（案件により複数の表を利用することもある。 例えば、
不正アクセスにより情報漏えいが発生した場合は表1、 表2、
表4を利用する）

表1 基本項目
全てのインシデントで共通して調査すべき項目

表2 情報漏えいに係る項目
情報漏えいが発生した際に調査すべき項目

表3 ウイルス感染に係る項目
ウイルス感染が発生した際に調査すべき項目

表4 不正アクセスに係る項目
不正アクセスを受けた際に調査すべき項目

表5 （D）DoSに係る項目
（D）DoS攻撃を受けた際に調査すべき項目

付録D 国際規格ISO/IEC27001及び27002との関係

付録E 用語の定義

（1） インシデント　　サイバーセキュリティ分野において、

サイバーセキュリティリスクが発現・現実化した事象のこと。

（2） 監査　　組織内においてサイバーセキュリティ対策が適切に実施されているかどうかを判定するために、
監査証拠を収集し、
それを客観的に評価するための、
体系的で、 独立し、
文書化したプロセスのこと。
監査は、
内部監査（第一者）または外部監査（第二者・第三者）のいずれでも、
または複合監査（複数の分野の組合せ）でもあり得る。

（3） サイバー攻撃　　コンピュータシステムやネットワークに、
悪意を持った攻撃者が不正に侵入し、

データの窃取・破壊や不正プログラムの実行等を行うこと。

サイバーセキュリティとは、
電子データの漏えい・改ざん等や、
期待されていたITシステムや制御システム等の機能が果たされないといった

（4） サイバーセキュリティ
不具合が生じないようにすること。

（5） サイバーセキュリティリスク
サイバーセキュリティリスクとは、
サイバーセキュリティに関連して不具合が生じ、
それによって企業の経営に何らかの影響が及ぶ可能性のこと。

（6） 残留リスク
リスク対応（回避、 低減、
移転）後に残るリスク。
保有リスクともいう。

（7） 情報セキュリティ報告書
企業の情報管理・情報システム等のセキュリティの取組の中でも社会的関心の高いものについて情報開示することにより、
当該企業の取組が顧客や投資家などのステークホルダーから適正に評価されることを目指すもの。
（参考：
経済産業省の「情報セキュリティ報告書モデル」：
2007_JohoSecurityReportModelRevised.pdf）

（8） ステークホルダー
意思決定もしくは活動に影響を与え、
影響されることがあるまたは影響されると認知している、
あらゆる人または組織。
具体的には、 株主、 債権者、 顧客、
取引先等である。

（9） セキュリティポリシー
企業・組織におけるセキュリティに関する理念である意図と方針を経営者が正式に表明したもの。
セキュリティポリシーに沿って、
組織内セキュリティ対策が規定される
。

（10） 多層防御
物理層、
ネットワーク層からデータ層までの多層防御を導入することで、
１つの機器やソフトウェアに依存する拠点防御対策や、
単一の境界防御層（主としてネットワーク境界）に依存する対策の場合より
、
未知のマルウェアや新たな攻撃手法の登場により容易に突破されるリスクの軽減が期待される。
IPAでは、 多層防御の１例として、
以下四つのポイントを紹介している。
①ソフトウェア感染リスクの低減、
②重要業務を行う端末やネットワークの分離、
③重要情報が保存されているサーバでの制限、 ④事後対応の準備。

（11） ビジネスパートナー
業務の委託先や受託元、
物品・サービスの調達先等の取引関係のある企業のこと。

（12） マルウェア
セキュリティ上の被害を及ぼすウイルス、 スパイウエア、
ボットなどの悪意をもったプログラムを指す総称。
これらのプログラムは、
使用者や管理者の意図に反して（あるいは気づかぬうちに）コンピュータに入り込み悪意ある行為を行う。

（13） リスク
国際規格（ISO/IEC 27000）では、
「諸目的に対する不確かさの影響」と定義されている。
対処の方法には、
大きく分けて「リスク回避」、
「リスク低減」、 「リスク移転」、
「リスク保有」の４つがある。
なお、
さらに詳細化した分類として、 JIS Q 0073リスクマネジメント用語では、
リスク回避、
機会を追及するためのリスクを取るまたは増加させる、 リスク源の除去、
起こりやすさを変更すること、
結果を変えること、 リスク移転、
リスク保有の７分類が定義されている
。
「リスク回避」とは、
脅威発生の要因を停止あるいは全く別の方法に変更することにより、
リスクが発生する可能性を取り去ることである。 例えば、
「インターネットからの不正侵入」という脅威に対し、
外部との接続を断た

- （14）リスク対応（回避、 低減、 移転、 保有）
  - ① リスク回避
    - 外部との接続を断ち、
      Web上での公開を停止してしまうような場合などが該当する。
  - ② リスク低減
    - 「リスク低減」とは、
      脆弱性に対してセキュリティ対策を講じることにより、
      脅威発生の可能性を下げることである。 ノートパソコンの紛失、 盗難、
      情報漏えいなどに備えて保存する情報を暗号化しておく、
      サーバ室に不正侵入できないようにバイオメトリック認証技術を利用した入退室管理を行う、
      従業員に対するセキュリティ教育を実施することなどが該当する。
  - ③ リスク移転
    - 「リスク移転」とは、
      リスクを他社などに移すことである。
      例えば、
      リスクが顕在化したときに備え、
      保険で損失をカバーすることや、
      組織内のITシステムの運用を他社に委託し、
      契約などにより不正侵入やマルウェア感染の被害に対して損害賠償などの形で移転すること等が該当する。
  - ④ リスク保有
    - 「リスク保有」とは、
      ある特定のリスクにより、
      起こり得る損失の負担を受容することである。
- （15）リスク評価
  - リスクの大きさが、
    受容可能かまた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（リスクの重大性を評価するために目安とする条件であり、
    組織の目的並びに外部環境および内部環境に基づいたもの）と比較するプロセスのこと。
- （16）リスク分析
  - リスクの特質を理解し、
    リスクレベル（ある事象の結果とその起こりやすさとの組合せとして表現される、
    リスクの大きさ）を決定するプロセスのこと。
- （17）ログ
  - コンピュータの利用状況やデータの通信記録。
    操作を行った者のIDや操作日付、
    操作内容などが記録される。
    セキュリティ上、
    インシデントの原因追究などに利用する。
- （18）BCP（Business Continuity Plan）
  - 企業が自然災害、 テロ攻撃、
    サイバー攻撃などによる被害が発生した場合において、
    中核となる事業の継続、
    早期復旧を実現するために、
    平時及び緊急時における事業継続のため手段等を取り決めておく計画のこと。
- （19）CISO（Chief Information Security Officer）
  - 経営陣の一員、
    もしくは経営トップからその役を任命された、
    セキュリティ対策を実施する上での責任者のこと。
- （20）CSIRT（Computer Security Incident Response Team）
  - インシデントの発生に対応するための体制のこと。
- （20）PDCA
  - Plan - Do - Check - Act の略。
    品質改善や環境マネジメントでよく知られた手法であり、
    次のステップを繰り返しながら、
    継続的に業務を改善していく手法の 1 つのこと。
  - 1.Plan：問題を整理し、
    目標を立て、
    その目標を達成するための計画を立てる。
  - 2.Do：目標と計画をもとに、
    実際の業務を行う。
  - 3.Check：実施した業務が計画通り行われて、
    当初の目標を達成しているかを確認し、 評価する。
  - 4.Act：評価結果をもとに、
    業務の改善を行う。