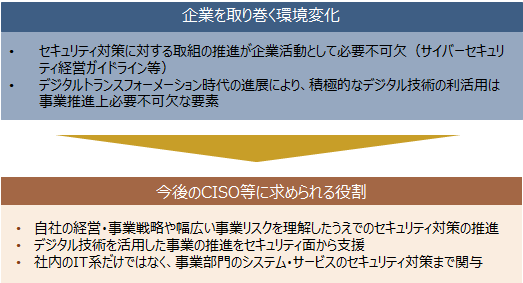
Sec01-02-55\_各種ガイドブックの内容要約\_一般企業向け【SK3】

ドキュメントを参照: [Sec01-02-50\_サイバーセキュリティ関連\_各種ガイドブックの内容要約.mmap](file:///D:\Cloud_Storage\OneDrive%20-%20ＮＰO知的資源イニシアティブ（ＩＲＩ）\git_repository_Duo\Sharing_Knowledge3\MindManager3\Sec01-02-50_サイバーセキュリティ関連_各種ガイドブックの内容要約.mmap)

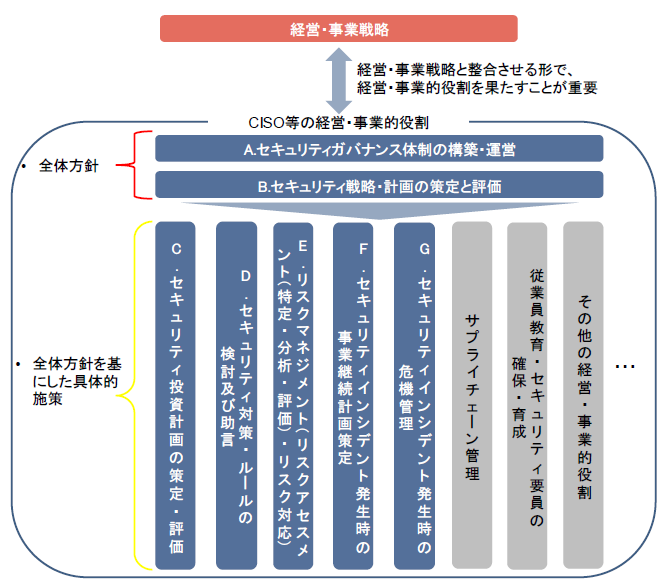
1. 一般企業向け
2. サイバーセキュリティ経営ガイドライン 実践のためのプラクティス集第2版【2020年6月3日IPA】

ドキュメントを参照: <https://www.ipa.go.jp/files/000072309.pdf>

1. CISO等セキュリティ推進者の経営・事業に関する役割調査【2018年6月28日IPA】
   1. 概要
      1. 「サイバーセキュリティ経営ガイドライン」（経済産業省とIPAが共同策定）(\*1)には、 経営者が認識すべき3原則が掲げられています。 その中で、 経営層はサイバーセキュリティリスクを認識し、 リーダーシップをとって対策を進めることが必要とあります。
      2. 一方、 「サイバーセキュリティ人材育成プログラム」（サイバーセキュリティ戦略本部）(\*2)では、 経営層自らがサイバーセキュリティ対策を企画・立案し、 実務者層を動かすことは困難であるとしています。 そのため同プログラムは、 経営層を補佐し、 経営戦略とサイバーセキュリティに関する業務課題を理解したうえで、 様々な役割を持った実務者層を指揮する「橋渡し人材」が必要であるとしています。
      3. 「CISO等セキュリティ推進者の経営・事業に関する役割調査」では、 CISO(\*3)およびその補佐役となる橋渡し人材等のセキュリティ推進者が担う役割、 とくにセキュリティへの取組みが経営と事業に貢献するようマネジメントする役割（以下、 経営・事業に関する役割）について、 その実態や期待されている内容を調査するため、 文献調査・有識者へのインタビュー調査・アンケート調査を行っています。
      4. 調査結果に基づいて、 CISO等セキュリティ推進者の経営・事業に関する役割7つについて整理し、 各役割の目的や役割を遂行する際のポイント等をまとめたプラクティスを、 調査報告書の別冊として作成しました。
   2. －別冊－CISO等セキュリティ推進者の経営・事業に関する役割プラクティス【2018年6月28日IPA】
      1. CISO等セキュリティ推進者の経営・事業に関する役割7つについて整理し、 各役割の目的や役割を遂行する際のポイント等をまとめたプラクティス
      2. 1. はじめに
         1. 1.1 目的
            1. 経営層によるセキュリティ対策の主体的取組の推進には、 経営層の示す経営方針に基づくセキュリティ対策を実践し、 実務課題を踏まえた経営戦略を提示し、 企業内の総合調整や実務者層をまとめリードできる人材が必要である
            2. CISO等には技術的な役割だけではなく、 自社の経営方針・事業戦略とセキュリティ対策の整合等、 経営・事業的貢献の観点からセキュリティ対策を推進する「経営・事業的役割」が今後求められると考えられる。
            3. さらに、 昨今、 デジタルトランスフォーメーションと呼ばれるように、 企業においても、 社内システムのみならず、 事業部門の情報システムや、 工場等で利用される制御システムにおいても、 デジタル技術活用を進めることで新たな事業価値を生み出すべく取組が進展しつつある。
            4. そのため、 より広範囲な業種・業態において積極的なデジタル技術の活用が事業推進上必要不可欠な要素となりつつある。
            5. 一方で、 過剰なセキュリティ対策は、 利便性や業務効率化を下げる場合もあり、 スピードを持って事業を促進するためには、 CISO等が事業を深く理解しつつ、 適切なリスク評価を行うことで事業とセキュリティのバランスを取り、 セキュリティの面から事業推進を支援する役割の重要性が増している。
            6. 図 1-1 今後のCISO等に求められる役割

サブトピック  


* + - * 1. ITサービス業や金融業等、 従来からITが事業の根幹であるような業種と、 製造業や卸売業・小売業等、 今後デジタル技術の活用が本格化する業種とでは、 CISO等が担う経営・事業的役割も異なると想定される。
      1. 1.2 経営・事業的役割の全体像
         1. 図 1-2 CISO等の経営・事業的役割の全体像

サブトピック  


* + - * 1. CISO等の経営・事業的役割は、 企業の経営・事業戦略と整合する形でセキュリティ対策が実施されるように、 遂行することが望ましい。
        2. CISOは3つの防衛線（Three lines of defense）1のセカンドラインのトップ

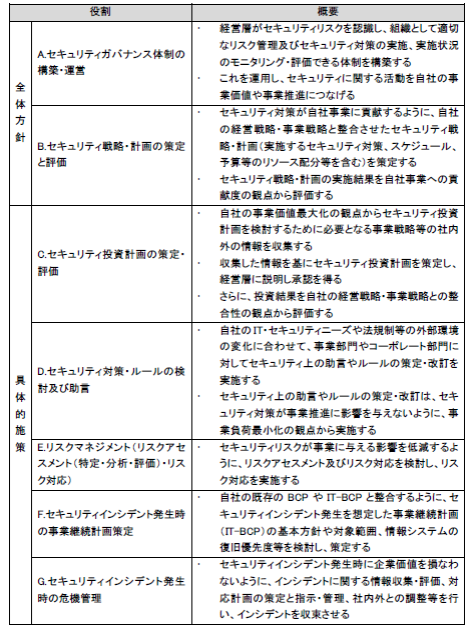
業務執行部門が業務においてリスクの特定及び管理を行う第1の防衛線

業務執行部門のリスク管理の状況を業務執行部門から独立したリスク管理部門等がモニタリングする第2の防衛線

防衛線の有効性を合理的に保証する内部監査部門を第3の防衛線

としたリスク管理の仕組みのこと。

* + - * 1. CISO等は自社の社内ITシステムだけではなく、 事業部門が保有・提供しているITシステム・ITサービスのセキュリティ対策にまで関与していくことが望ましい。
        2. 特に重要と考えられる役割としてA~Gの7つの役割を選定した。 選定した役割の概要は表 1-1の通りで、 2章～8章では選定した役割について役割の目的や作業プロセス等の詳細を説明する。
        3. 表 1-1 本書で対象とする経営・事業的役割の概要

サブトピック  


全体方針

A.セキュリティガバナンス体制の構築・運営

 経営層がセキュリティリスクを認識し、 組織として適切なリスク管理及びセキュリティ対策の実施、 実施状況のモニタリング・評価できる体制を構築する

 これを運用し、 セキュリティに関する活動を自社の事業価値や事業推進につなげる

B.セキュリティ戦略・計画の策定と評価

 セキュリティ対策が自社事業に貢献するように、 自社の経営戦略・事業戦略と整合させたセキュリティ戦略・計画（実施するセキュリティ対策、 スケジュール、 予算等のリソース配分等を含む）を策定する

 セキュリティ戦略・計画の実施結果を自社事業への貢献度の観点から評価する

具体的施策

C.セキュリティ投資計画の策定・評価

 自社の事業価値最大化の観点からセキュリティ投資計画を検討するために必要となる事業戦略等の社内外の情報を収集する

 収集した情報を基にセキュリティ投資計画を策定し、 経営層に説明し承認を得る

 さらに、 投資結果を自社の経営戦略・事業戦略との整合性の観点から評価する

D.セキュリティ対策・ルールの検討及び助言

 自社のIT・セキュリティニーズや法規制等の外部環境の変化に合わせて、 事業部門やコーポレート部門に対してセキュリティ上の助言やルールの策定・改訂を実施する

 セキュリティ上の助言やルールの策定・改訂は、 セキュリティ対策が事業推進に影響を与えないように、 事業負荷最小化の観点から実施する

E.リスクマネジメント（リスクアセスメント（特定・分析・評価）・リスク対応）

 セキュリティリスクが事業に与える影響を低減するように、 リスクアセスメント及びリスク対応を検討し、 リスク対応を実施する

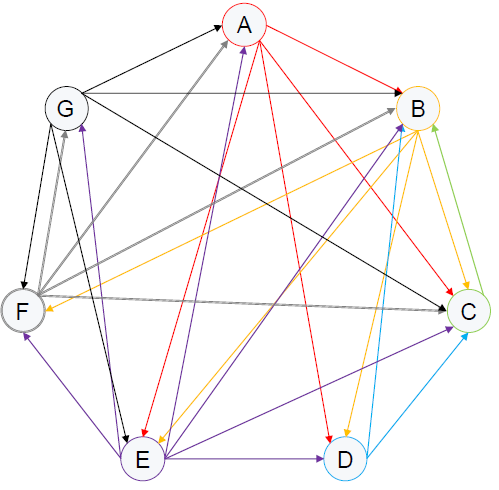
F.セキュリティインシデント発生時の事業継続計画策定

 自社の既存のBCPやIT-BCPと整合するように、 セキュリティインシデント発生を想定した事業継続計画（IT-BCP）の基本方針や対象範囲、 情報システムの復旧優先度等を検討し、 策定する

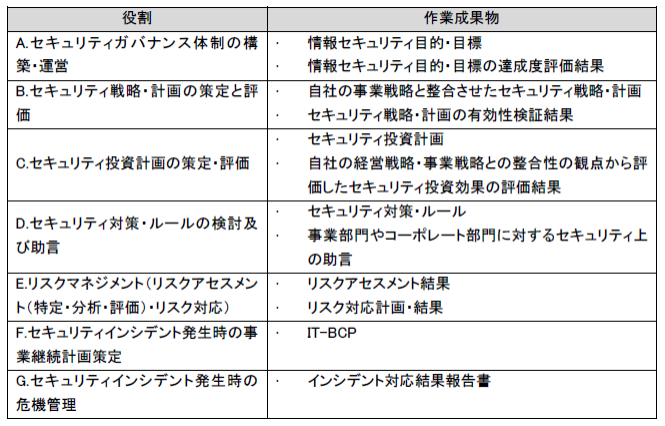
G.セキュリティインシデント発生時の危機管理

 セキュリティインシデント発生時に企業価値を損なわないように、 インシデントに関する情報収集・評価、 対応計画の策定と指示・管理、 社内外との調整等を行い、 インシデントを収束させる

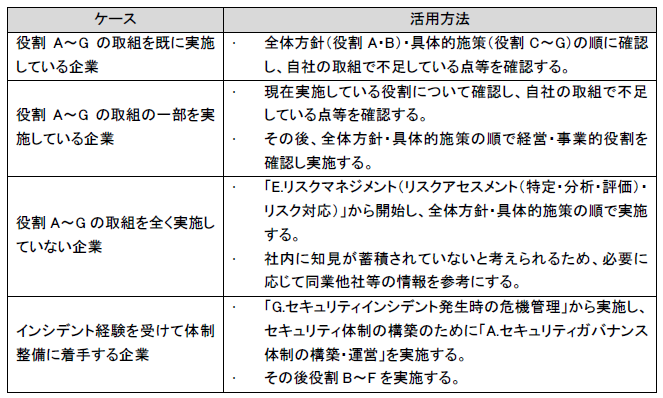
* + - * 1. サブトピック 7
      1. 1.3 経営・事業的役割間の関係と本書の活用方法
         1. 図 1-3において、 各役割から伸びる矢印は、 その役割の作業成果物（アウトプット）が、 矢印の先の役割の作業を進めるためのインプットとなることを示している
         2. 図 1-3 役割間のインプット・アウトプット関係

サブトピック  


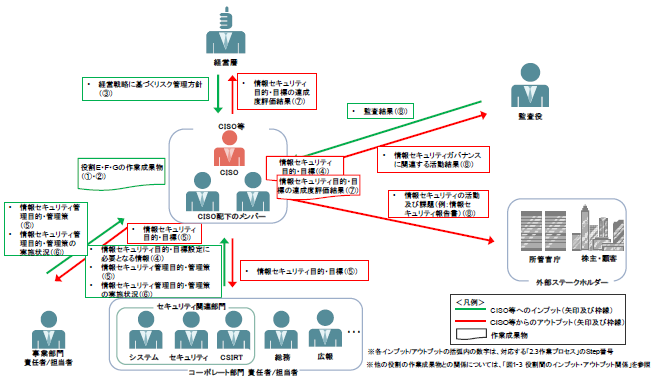
* + - * 1. 表 1-2 各役割の作業成果物

サブトピック  


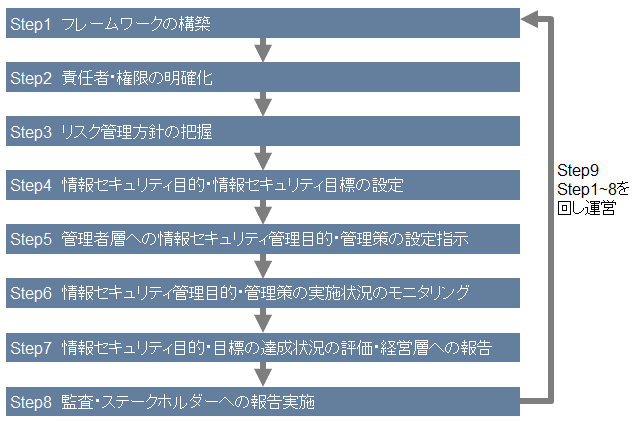
* + - * 1. 表 1-3 ケース別本書の活用方法

サブトピック  


* + 1. 2. セキュリティガバナンス体制の構築・運営（A）
       1. 2.1 目的・狙い
          1. 本役割は経営層がセキュリティリスクを認識し、 組織として適切なリスク管理とセキュリティ対策が実施するための体制を構築・運用し、 自社の事業価値や事業推進に貢献することを目的としている。
          2. 図 2-1 「セキュリティガバナンス体制の構築・運営」の全体像

サブトピック  


* + - 1. 2.2 役割の作業内容
         1. ・経営者による方針決定等の機能を有するセキュリティガバナンスのフレームワークの構築
         2. ・経営層が示すリスク管理方針に基づいた情報セキュリティ目的・情報セキュリティ目標の設定
         3. ・情報セキュリティ目的・情報セキュリティ目標の達成状況を評価し経営層に報告
         4. ・外部監査や外部ステークホルダーへの報告実施
      2. 2.3 作業プロセス
         1. 図 2-2 「セキュリティガバナンス体制の構築･運営」の作業プロセス

サブトピック  


* + - * 1. Step1 フレームワークの構築

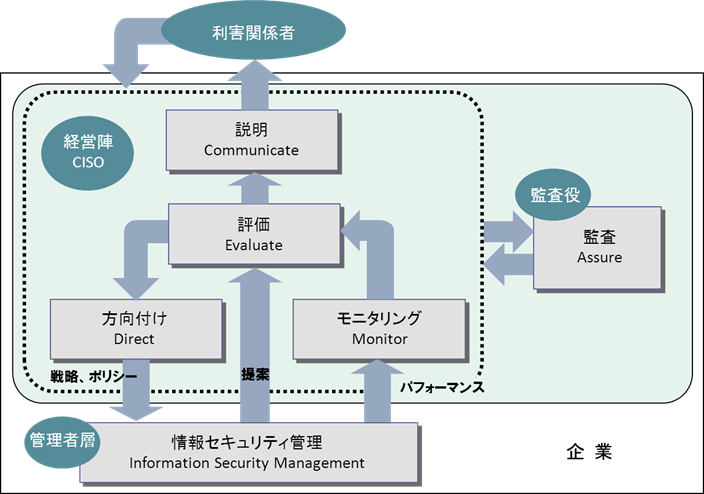
・経営者による方針決定

・組織内の状況をモニタリングする仕組み

・利害関係者に対する開示

・利害関係者による評価の仕組み

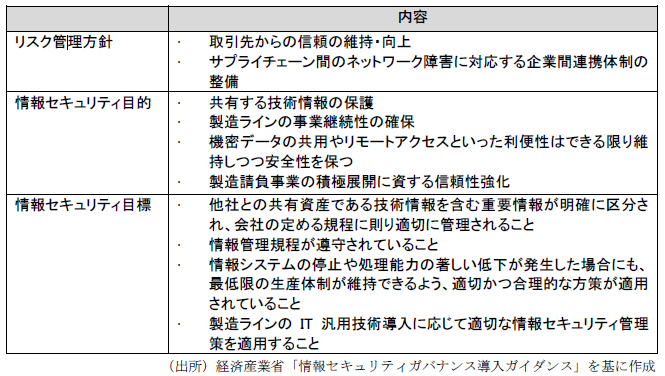
図 2-3 情報セキュリティガバナンスのフレームワーク

サブトピック  


（出所）経済産業省「情報セキュリティガバナンス導入ガイダンス」を基にISO/IEC 27014:2013 の内容を一部反映

* + - * 1. Step2 責任者・権限の明確化
        2. Step3 リスク管理方針の把握
        3. Step4 情報セキュリティ目的・情報セキュリティ目標の設定

表 2-1 情報セキュリティ目的・情報セキュリティ目標の例

サブトピック  


* + - * 1. Step5 管理者層への情報セキュリティ管理目的・管理策の設定指示

Step4で設定した情報セキュリティ目的・目標を事業部門・コーポレート部門の管理者層に伝える。 さらに、 管理者層に対し情報セキュリティ目的・目標を実現するための情報セキュリティ管理目的・管理策の設定を指示する。

情報セキュリティ管理目的・管理策の設定にあたり、 事業部門等セキュリティ人材等が不足していると考えられる組織に対しては、 CISO等が必要に応じて支援することが望ましい。

* + - * 1. Step6 情報セキュリティ管理目的・管理策の実施状況のモニタリング
        2. Step7 情報セキュリティ目的・目標の達成状況の評価・経営層への報告
        3. Step8 監査・ステークホルダーへの報告実施

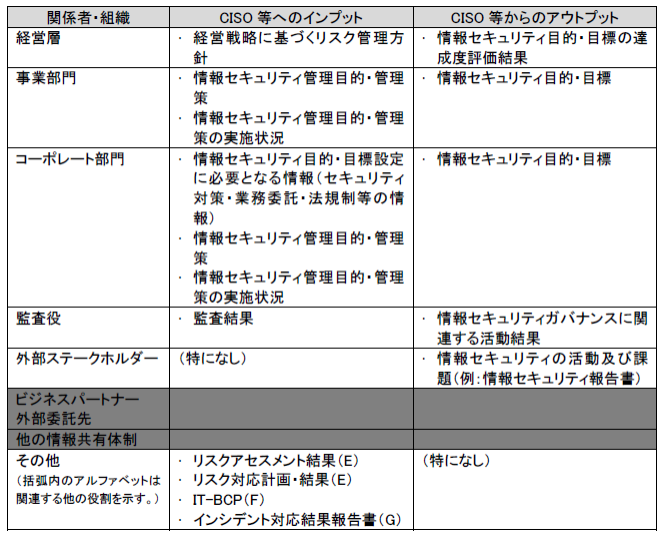
セキュリティガバナンスに関わる活動に関して監査を依頼し、 監査結果を基に見直しを実施する。

また、 外部ステークホルダーに対して、 自社のセキュリティに対する取組について報告を実施する

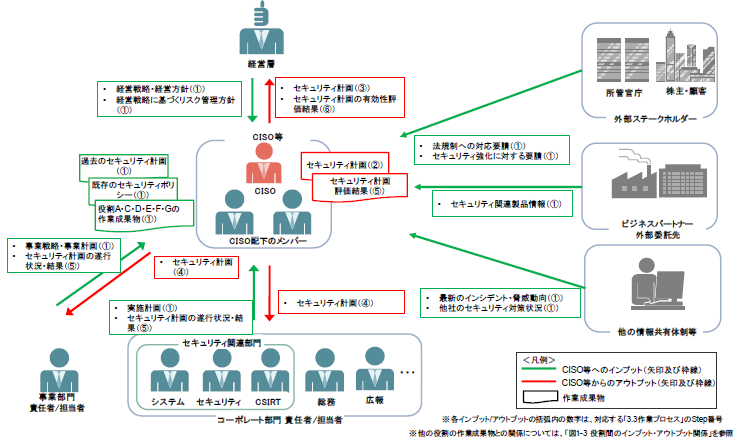
* + - * 1. Step9 情報セキュリティガバナンス体制の運営

Step1～8の取組を回し、 情報セキュリティガバナンス体制を運営する。

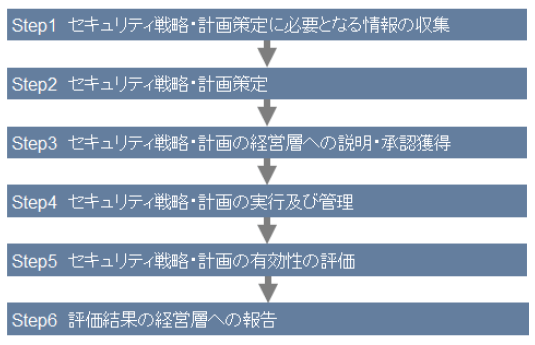
* + - 1. 2.4 作業に必要な情報
         1. 表 2-2 「セキュリティガバナンス体制の構築・運営」に必要となる情報

サブトピック  


* + - 1. 2.5 作業の目標成果
         1. ・情報セキュリティ目的・目標
         2. ・情報セキュリティ目的・目標の達成度評価結果
      2. 2.6 作業で協同・連携する社内外の関係者と協同・連携の内容
         1. ・情報セキュリティ目的・情報セキュリティ目標達成のための、 事業部門・コーポレート部門に対する連携・支援
         2. ・外部ステークホルダーに対する自社のセキュリティ対策に関する情報開示
    1. 3. セキュリティ戦略・計画の策定と評価（B）
       1. 3.1 目的・狙い
          1. 本役割は、 自社の経営戦略・事業戦略と整合したセキュリティ戦略・計画（実施するセキュリティ対策や実施スケジュール、 予算等のリソース配分等）を策定し、 自社の事業価値や事業推進につなげることを目的としている。
          2. 本役割で策定するセキュリティ戦略・計画は企業のセキュリティ対策に関する全体方針であり、 このセキュリティ戦略・計画を基に、 4 章以降の役割の具体的な施策が実施される。
          3. 図 3-1 「セキュリティ戦略・計画の策定と評価」の全体像

サブトピック  


* + - 1. 3.2 役割の作業内容
         1. ・自社の経営戦略・事業戦略と整合させたセキュリティ戦略・計画の策定
         2. ・セキュリティ戦略・計画の実施結果の評価
      2. 3.3 作業プロセス
         1. 図 3-2 「セキュリティ戦略・計画の策定と評価」の作業プロセス

サブトピック  


* + - * 1. Step1 セキュリティ戦略・計画策定に必要となる情報の収集

・経営戦略・経営方針

・事業戦略・事業計画

・自社に影響を与える法規制

・最新のインシデント・脅威動向

・情報セキュリティ目的・目標（A）

・セキュリティ投資計画（C）

・セキュリティ対策・ルール（D）

・リスクアセスメント結果（E）

・IT-BCP（F）

・インシデント対応結果報告書（G）

* + - * 1. Step2 セキュリティ戦略・計画策定

Step1で収集した情報を基に、 セキュリティ戦略・計画を策定する。 セキュリティ戦略・計画には、 実施するセキュリティ対策や実施スケジュール、 予算等のリソース配分等が含まれる

* + - * 1. Step3 セキュリティ戦略・計画の経営層への説明・承認獲得

Step2で策定したセキュリティ戦略・計画を経営層に対して説明し、 承認を得る。 経営層から承認が得られなかった場合は、 Step2に戻り必要な修正を実施する。

* + - * 1. Step4 セキュリティ戦略・計画の実行及び管理

Step3で承認されたセキュリティ戦略・計画を実行する。 事業部門・コーポレート部門が実行するセキュリティ戦略・計画に関しては、 CISO等が実行状況をモニタリングし管理するとともに、 必要に応じて支援する

* + - * 1. Step5 セキュリティ戦略・計画の有効性の評価

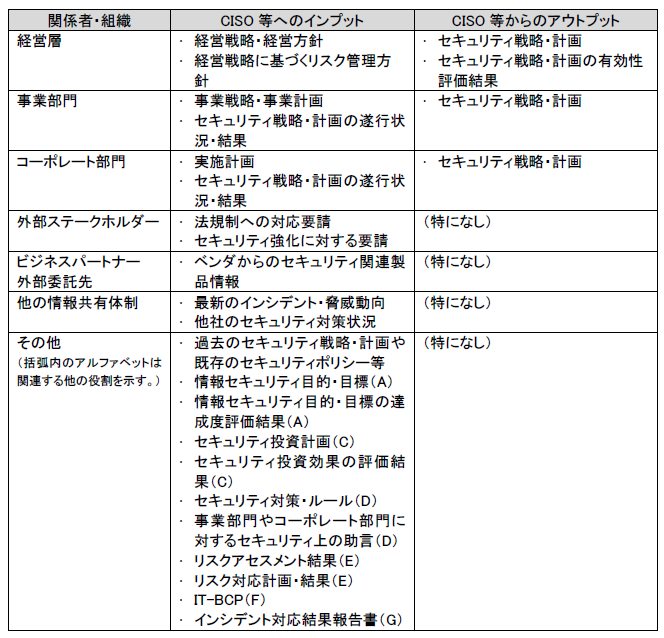
事業部門・コーポレート部門のセキュリティ戦略・計画の実行状況・結果を把握し、 セキュリティ戦略・計画の有効性を評価する。 セキュリティ戦略・計画の有効性を評価する際は、 自社の経営戦略・事業戦略との整合性や自社の事業価値への貢献等の観点から実施することが望ましい。

評価結果は次年度以降のセキュリティ戦略・計画を策定する際に活用する。

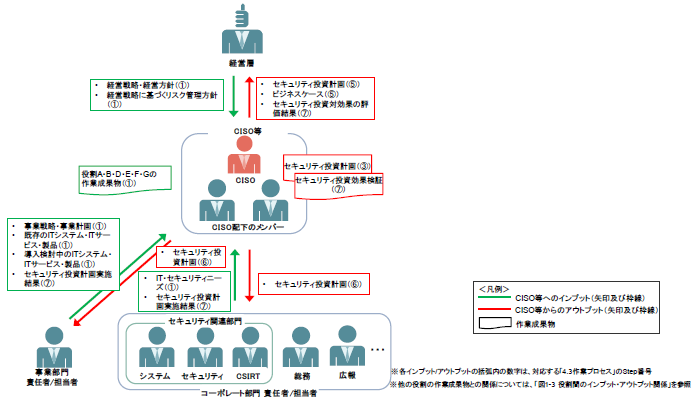
* + - * 1. Step6 評価結果の経営層への報告

Step5の評価結果を経営層へ報告する。

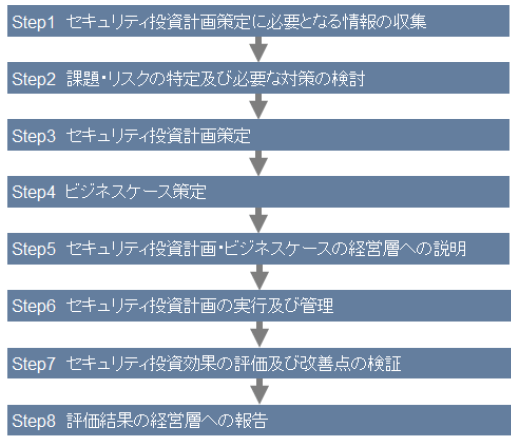
* + - 1. 3.4 作業に必要な情報
         1. 表 3-1 「セキュリティ戦略・計画の策定と評価」に必要となる情報

サブトピック  


* + - 1. 3.5 作業の目標成果
         1. ・自社の事業戦略と整合させたセキュリティ戦略・計画
         2. ・セキュリティ戦略・計画の有効性検証結果
      2. 3.6 作業で協同・連携する社内外の関係者と協同・連携の内容
         1. ・社内外の関係者からのセキュリティ戦略・計画策定に必要となる情報の収集
         2. ・事業部門・コーポレート部門と連携したセキュリティ戦略・計画の実行
    1. 4. セキュリティ投資計画の策定・評価（C）
       1. 4.1 目的・狙い
          1. 本役割は、 「セキュリティ戦略・計画の策定・評価」の役割で策定されたセキュリティ戦略・計画を基に、 必要となるセキュリティ対策を検討し、 対策実施に必要なセキュリティ投資計画を策定するものである。 策定するセキュリティ投資計画には、 新規のITサービス・ITシステムの導入だけではなく、 既存のITサービス・ITシステムの継続利用等の判断も含まれる。
          2. 本役割の遂行にあたっては、 セキュリティ投資が自社の企業価値の最大化につながるようにセキュリティ投資計画を策定し、 自社の経営戦略・事業戦略との整合性の観点から投資の有効性を評価することが望ましい。
          3. 図 4-1 「セキュリティ投資計画の策定・評価」の全体像

サブトピック  


* + - 1. 4.2 役割の作業内容
         1. ・自社の企業価値最大化につながるセキュリティ投資計画の策定
         2. ・セキュリティ投資計画の有効性を示すビジネスケース5の策定
         3. ・セキュリティ投資計画・ビジネスケースの経営層への説明・承認獲得
         4. ・セキュリティ投資計画の実行及び投資効果の検証
      2. 4.3 作業プロセス
         1. 図 4-2 「セキュリティ投資計画の策定・評価」の作業プロセス

サブトピック  


* + - * 1. Step1 セキュリティ投資計画策定に必要となる情報の収集

・経営戦略・経営方針

・事業戦略・事業計画

・既存または導入検討中のITシステム・ITサービス・製品

・情報セキュリティ目的・目標（A）

・セキュリティ戦略・計画（B）

・セキュリティ対策・ルール（D）

・リスクアセスメント結果（E）

・IT-BCP（F）

・インシデント対応結果報告書（G） 等

* + - * 1. Step2 課題・リスクの特定及び必要な対策の検討

Step1で収集した情報を元に、 自社のセキュリティ上の課題やリスクを特定し、 必要な対策を検討する。

* + - * 1. Step3 セキュリティ投資計画策定

Step2で検討した対策を導入するために必要となるセキュリティ投資計画を策定する。

セキュリティ投資計画の策定にあたっては、 自社の事業価値最大化につながるよう、 経営戦略・事業戦略と整合させるように策定することが望ましい。

* + - * 1. Step4 ビジネスケース策定

・セキュリティ投資の目的・必要性

・必要なリソース

・実施スケジュール

・期待される投資効果 等

* + - * 1. Step5 セキュリティ投資計画・ビジネスケースの経営層への説明

Step3・Step4で策定したセキュリティ投資計画・ビジネスケースを経営層に説明し、 承認を得る。 経営層からの承認が得られなかった場合、 Step3に戻り必要な修正を行う。

* + - * 1. Step6 セキュリティ投資計画の実行及び管理

経営層から承認を得たセキュリティ投資計画を実行する。 事業部門やコーポレート部門が実行するセキュリティ投資計画については、 その進捗状況等をCISO等が管理する。

* + - * 1. Step7 セキュリティ投資効果の評価及び改善点の検証

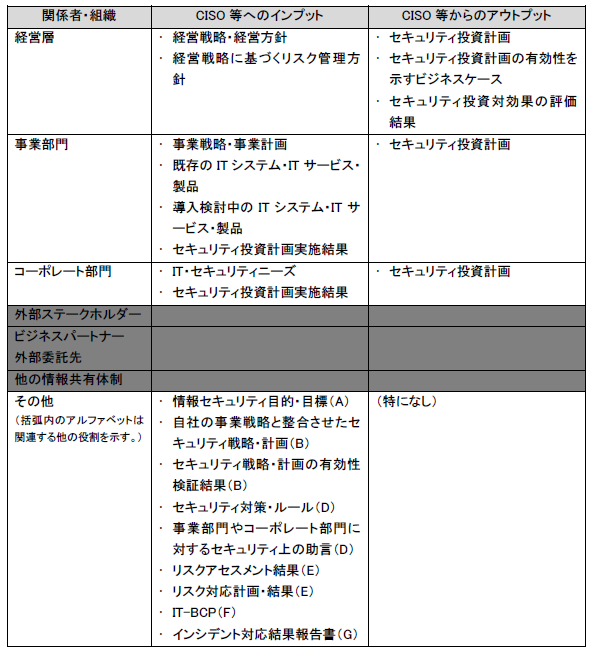
セキュリティ投資計画の実行結果を基に、 セキュリティ投資の投資効果・改善点を検証する。

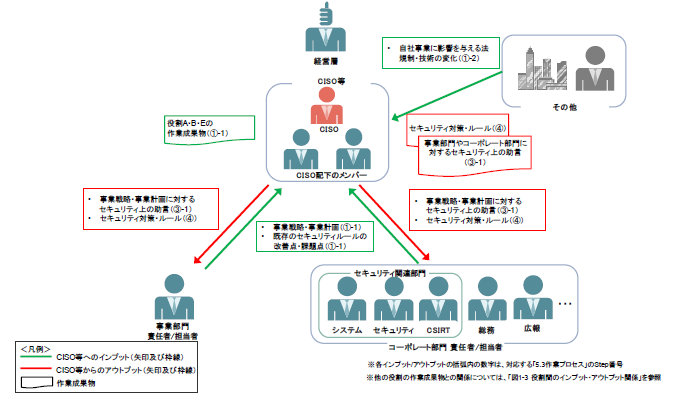
投資効果の検証の際には、 自社の経営戦略・事業戦略との整合性や、 自社事業推進にどの程度貢献したか等の観点から実施することが望ましい。

セキュリティ投資効果の検証結果に関しては、 次年度以降のセキュリティ戦略・計画の策定やセキュリティ投資計画の策定に活用する。

* + - * 1. Step8 評価結果の経営層への報告

Step7で実施したセキュリティ投資効果の検証結果を経営層に報告する。

* + - 1. 4.4 作業に必要な情報
         1. サブトピック  
            
      2. 4.5 作業の目標成果
         1. ・セキュリティ投資計画（導入する製品・サービスや投資金額、 実施時期、 投資効果等を含む）
         2. ・自社の経営戦略・事業戦略との整合性の観点から評価したセキュリティ投資効果の評価結果
      3. 4.6 作業で協同・連携する社内外の関係者と協同・連携の内容
         1. ・自社の経営戦略・事業戦略等の把握・セキュリティ上の課題の検討に必要となる情報の提供・意見交換
         2. ・事業部門やコーポレート部門に対するセキュリティ投資計画の実行支援及び進捗状況の管理
    1. 5. セキュリティ対策・ルールの検討及び助言（D）
       1. 5.1 目的・狙い
          1. 事業部門やコーポレート部門の社内部門の新規の事業展開や新たなITシステム・ITサービスの利用等の内部環境の変化や、 法規制や新規技術の登場等の外部環境の変化に合わせて、 CISO等にはセキュリティ上の助言や新たなルールの策定、 既存ルールの改訂等の対応が求められる。
          2. 本役割では社内外の環境変化に合わせて、 CISO等がセキュリティ上の助言やルールの策定・改定を行うものである。 本役割を遂行する際には、 セキュリティ対策が事業推進に影響を与えないよう、 事業負荷を最小にする観点から検討することが望ましい。 また、 CISO等の役割が事業の推進を成功に導くようにセキュリティ対策・ルールを整備することであることに留意する必要がある。
          3. 図 5-1 「セキュリティ対策・ルールの検討及び助言」の全体像

サブトピック  


* + - 1. 5.2 役割の作業内容
         1. ・事業部門・コーポレート部門等からの内部情報の収集及び法規制や技術動向等の外部情報の収集
         2. ・収集した情報を基にした、 自社のIT利活用ニーズの把握及びセキュリティ上の課題の検討
         3. ・検討した課題を基にした、 事業部門・コーポレート部門に対するセキュリティ上の助言
         4. ・検討した課題を基にした、 既存のルールの改訂または新規ルールの策定及び見直し

実施するタイミングとしては以下のものが考えられる。

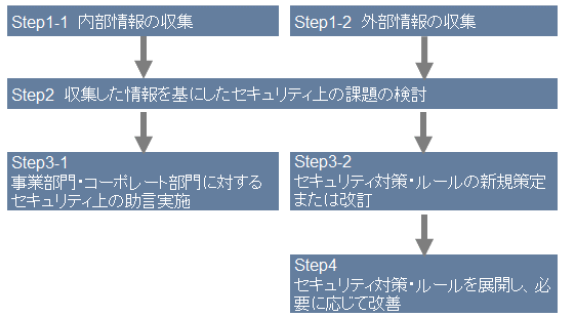
・年度計画検討時

・新規事業検討時

・新規のITサービス導入検討時

・自社に影響を与える法規制や新規技術の登場時

* + - 1. 5.3 作業プロセス
         1. 図 5-2 「セキュリティ対策・ルールの検討及び助言」の作業プロセス

サブトピック  


* + - * 1. Step1-1 内部情報の収集

事業部門及びコーポレート部門に対して、 事業計画（ITシステム・ITサービスを利用した新規事業や新規のITシステム・ITサービスの検討・導入等）や既存のセキュリティルール等に関する改善要望等の情報を収集する。

内部情報の収集にあたっては、 他の役割の成果物である以下のものもインプットとなる。

・情報セキュリティ目的・目標（A）

・自社の事業戦略と整合させたセキュリティ戦略・計画（B）

・リスクアセスメント結果（E）

・リスク対応計画・結果（E）

* + - * 1. Step1-2 外部情報の収集

自社事業に影響を与える法規制の変化や新規技術の動向等について、 定期的に情報を収集する。

* + - * 1. Step2 収集した情報を基にしたセキュリティ上の課題の検討

Step1-1及びStep1-2で収集した情報を基に自社のIT利活用ニーズ等を把握し、 セキュリティ上の課題がないか検討する。

* + - * 1. Step3-1 事業部門・コーポレート部門に対するセキュリティ上の助言の実施

Step2で検討した課題を基に、 事業部門・コーポレート部門に対して、 事業推進・業務運営に必要となるセキュリティ対策の実施等、 セキュリティ上の助言を行う。

助言はセキュリティ対策が事業推進・業務運営の妨げにならないよう、 事業部門・コーポレート部門の負荷を最小にする観点から検討することが望ましい。

* + - * 1. Step3-2 セキュリティ対策・ルールの新規策定または改訂

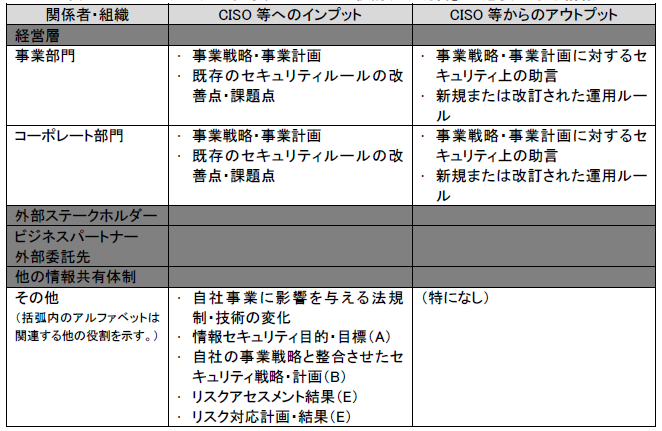
Step2で検討した課題を基に、 セキュリティに関するルールの新規策定または既存のルールの改訂を行う。

ルールの策定・改訂の際は、 セキュリティに関するルールが事業推進・業務運営の妨げにならないよう、 事業部門・コーポレート部門の負荷を最小にする観点から検討することが望ましい。

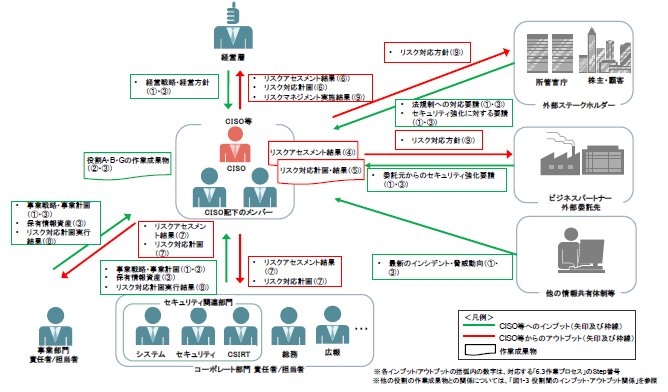
* + - * 1. Step4 セキュリティ対策・ルールを展開し、 必要に応じて改善

策定・改訂したセキュリティに関するルールを社内に展開する。 また、 必要に応じて改善する。

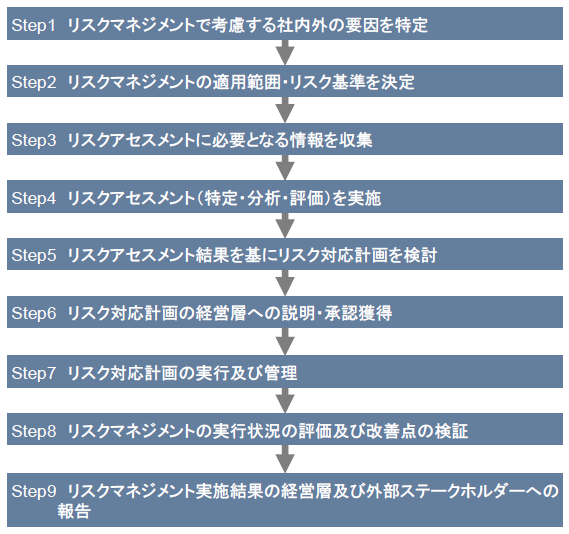
* + - 1. 5.4 作業に必要な情報
         1. 表 5-1 「セキュリティ対策・ルールの検討及び助言」に必要となる情報

サブトピック  


* + - 1. 5.5 作業の目標成果
         1. ・社内外の環境変化に対応した事業部門及びコーポレート部門に対するセキュリティ上の助言
         2. ・社内外の環境変化に対応したセキュリティ対策・ルール
      2. 5.6 作業で協同・連携する社内外の関係者と協同・連携の内容
         1. ・自社のIT利活用ニーズの把握・セキュリティ上の課題の検討に必要となる情報提供・意見交換
         2. ・事業部門のセキュリティ対策の実施等に関して、 コーポレート部門（主にセキュリティ関連部門）と連携した支援
    1. 6. リスクマネジメント（リスクアセスメント（特定・分析・評価）・リスク対応）（E）
       1. 6.1 目的・狙い
          1. セキュリティ対策はセキュリティに関わるリスクに対応することである。
          2. しかし、 対策にかけられる組織のリソースには限りがあることから、 リスクを明確にし、 対応の優先順位をつけ、 最適な対策を選択する必要がある。
          3. また、 組織が抱えるリスクは組織の状況により異なり、 保有する情報資産や脅威の変化に伴い変化していくことから、 セキュリティリスクに対しては、 いったん評価・対応して終わりではなく、 適切に管理していかなければならない。
          4. さらに、 リスクの評価基準は企業としての判断であることから、 経営・事業的な観点でリスクを評価し対応を検討していくことが必要である。
          5. 本役割は、 自社のセキュリティ関連のリスクへの対応方針を定め、 リスクが事業に与える影響を低減することを目的としている。 図
          6. 図 6-1 「リスクマネジメント」の全体像

サブトピック  


* + - 1. 6.2 役割の作業内容
         1. セキュリティに関わるリスクアセスメント（特定・分析・評価）を行う。
         2. リスクアセスメント結果に基づき、 リスク対応計画の策定を行う。
         3. リスク対応計画に基づいた、 実行及び管理を行う。
      2. 6.3 作業プロセス
         1. 図 6-2 「リスクマネジメント」の作業プロセス

サブトピック  


* + - * 1. Step1 リスクマネジメントで考慮する社内外の要因を特定

組織の目的を明確にし、 リスクマネジメントにおいて考慮するのが望ましい社内外の要因を特定する。

外部環境とは、 政治や経済、 法規制、 金融，技術等の社会動向全般、 競争環境等市場の動向、 ステークホルダーの状況等であり

内部環境とは、 組織体制、 方針・戦略、 組織文化、 情報システム、 ステークホルダーの状況等である。

* + - * 1. Step2 リスクマネジメントの適用範囲・リスク基準を決定

リスクマネジメントを適用する範囲と、 リスクを評価するために使用する基準を定める。 評価基準は、 組織の目的やリソース等の状況、 及び法律や規制の要求事項等によって検討される。

評価基準は、 例えば事象の起こりやすさ、 影響の種類や特徴、 リスクレベル、 複数のリスクの考慮等である。

* + - * 1. Step3 リスクアセスメントに必要となる情報を収集

リスクアセスメント（特定・分析・評価）を行うために必要な情報を収集する

* + - * 1. Step4 リスクアセスメント（特定・分析・評価）を実施

リスク特定では、 リスク源やその事象が発生しうる原因・結果を特定し、 リスクの一覧を作成する。

リスク分析では，リスク評価や対応計画の策定に必要な情報を整理する。 分析の際には、 リスク源、 原因と結果、 起こりやすさ等を考慮する。

リスク評価では、 リスク分析結果に基づき、 対応が必要なリスクや実施の優先順位に関して意思決定を行う。

* + - * 1. Step5 リスクアセスメント結果を基にリスク対応計画を検討

リスクアセスメントの結果、 明確になったリスクに対して、 対応方法及び実施時期を明確にし、 リスク対応計画として定める。

リスクの対応方針には

「リスクの低減」

「リスクの保有」

「リスクの回避」

「リスクの移転」

* + - * 1. Step6 リスク対応計画の経営層への説明・承認獲得

Step5で策定したリスク対応計画を経営層に対して説明し、 承認を得る。 経営層から承認が得られなかった場合は、 Step5に戻り必要な修正を実施する。

* + - * 1. Step7 リスク対応計画の実行及び管理

経営層から承認を得たリスク対応計画を実行する。 事業部門やコーポレート部門が実行するリスク対応計画については、 その進捗状況等をCISO等が管理する。

* + - * 1. Step8 リスクマネジメントの実行状況の評価及び改善点の検証

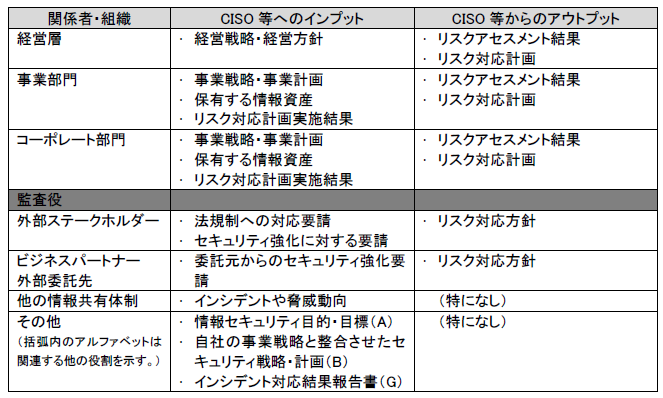
リスク対応計画の実行結果を基に、 リスク対応の効果・改善点を検証する。

リスク対応計画の改善点に関しては、 次年度以降のリスク対応計画の策定に活用する。

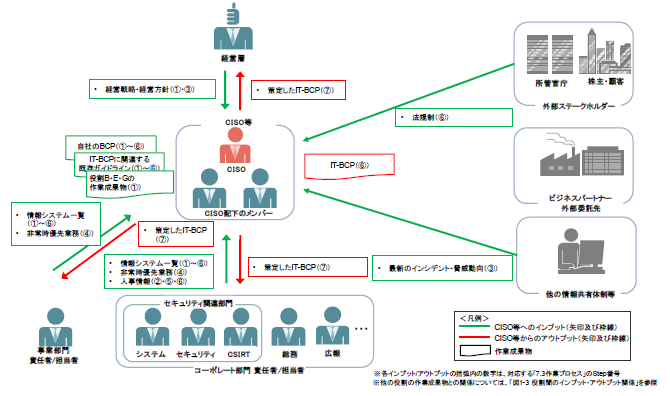
* + - * 1. Step9 リスクマネジメント実施結果の経営層及び外部ステークホルダーへの報告

Step8で実施されたリスクマネジメントの実施結果を経営層に対して説明し、 承認を得る。 外部ステークホルダーに対する報告により、 リスクマネジメントに関わる説明責任を果たす

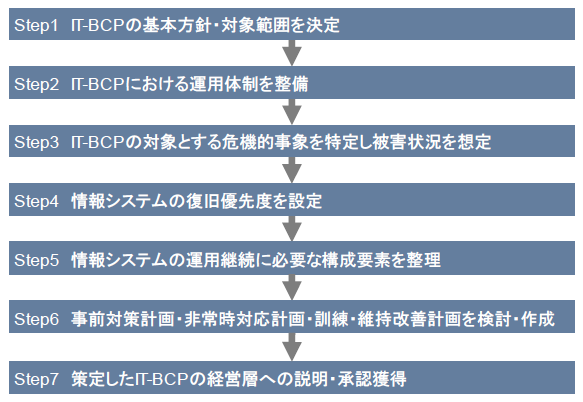
* + - 1. 6.4 作業に必要な情報
         1. 表 6-1 「リスクマネジメント」に必要となる情報

サブトピック  


* + - 1. 6.5 作業の目標成果
         1. リスクアセスメント結果
         2. リスク対応計画・結果
      2. 6.6 作業で協同・連携する社内外の関係者と協同・連携の内容
         1. ・事業部門における事業リスクと、 セキュリティ部門のセキュリティリスク、 コーポレート部門における企業リスクを踏まえ、 リスクアセスメントを実施する。
         2. ・事業部門、 セキュリティ部門、 コーポレート部門がそれぞれ実施可能なリスク対応計画を策定する。
         3. ・リスクアセスメント結果を経営層に説明する。
    1. 7. セキュリティインシデント発生時の事業継続計画策定（F）
       1. 7.1 目的・狙い
          1. セキュリティインシデントは、 場合によってその企業の事業そのものの継続自体を脅かすこともある。
          2. しかし、 地震等の自然災害と異なり、 セキュリティインシデントは原因や影響がすぐに特定できないことから、 ITサービスにインシデントが発生しても事業継続のためにITサービスを維持するのか、 被害拡大防止や原因究明のためにITサービス停止するのかの意思決定を企業として行う必要がある。
          3. また、 仮にITサービスを停止したとしても、 企業価値を損なわないために、 事業継続できるよう行動計画を定めておくことが必要である。
          4. 本役割は、 サイバー攻撃等のセキュリティインシデント発生を想定したIT-BCPを策定することを目的としている。
          5. なお、 本役割では、 セキュリティインシデントを考慮した事業継続に関わる行動計画・ルール等を便宜的に「セキュリティインシデント発生時のIT-BCP」と呼ぶ
          6. 何らかの特定の計画をドキュメントとして策定することが目的ではなく、 企業が既に有するBCPやIT-BCPと整合性の取れた形でセキュリティインシデント発生時に事業継続の観点を含んだ計画・ルール等を定めることを目的とするものである。
          7. 図 7-1 「セキュリティインシデント発生時の事業継続計画策定」の全体像

サブトピック  


* + - 1. 7.2 役割の作業内容
         1. ・事業継続との関係を考慮した上で、 インシデントを想定したIT-BCPを策定する。
         2. ・インシデント発生時の対応を円滑に行うために、 社内外にIT-BCPを説明し、 承認を得る。
      2. 7.3 作業プロセス
         1. 図 7-2 「セキュリティインシデント発生時の事業継続計画策定」の作業プロセス

サブトピック  


* + - * 1. Step1 IT-BCPの基本方針・対象範囲を決定

セキュリティインシデント発生時の事業継続計画策定にあたり、 基本方針や対象範囲（対象となる事象、 システムの範囲等）を定める。

* + - * 1. Step2 IT-BCPにおける運用体制を整備

セキュリティインシデント発生時の事業継続計画策定の対象範囲を踏まえ、 関係する組織（情報システム部、 事業部門、 コーポレート部門等）との間で検討・運用体制を整備する。

* + - * 1. Step3 IT-BCPの対象とする危機的事象を特定し被害状況を想定

危機的事象における状況を明らかにし、 対象とするシステムの早期復旧や稼働継続を阻害する要因である被害状況を想定する。

* + - * 1. Step4 情報システムの復旧優先度を設定

被害発生時に優先して復旧する業務を設定し、 目標とする復旧時間を確認した上で、 復旧優先度を定める。

* + - * 1. Step5 情報システムの運用継続に必要な構成要素を整理

業務の復旧に必要なシステムを洗い出し、 そのシステムの復旧に必要な構成要素を分析する。 さらに、 システムの復旧優先度に従い、 対策目標を設定する。

必要な情報の収集にあたっては、 事業部門の協力を得る必要があり、 対策目標を定める際も、 事業部門の体制を考慮の上、 実現可能な計画を立案する必要があることから、 事業部門との良好なコミュニケーションを図ることが重要である。

* + - * 1. Step6 事前対策計画・非常時対応計画・訓練・維持改善計画を検討・作成

危機的事象の発生時にシステムに生じる被害想定に対するシステムの脆弱性に関して、 その脆弱性を解消する対策を検討し、 事前対策計画として策定する。

システムの復旧活動に必要な対応体制を整備し、 発生から復旧までの対応を示した対応フローや手順書を非常時対応計画として策定する。

担当者の理解力や対応力を高めるために、 訓練計画を策定する。

事前対策計画、 非常時対応計画、 訓練計画をそれぞれ定期的に見直し、 事業継続計画の実効性を継続的に維持するために、 維持改善計画を策定する。

* + - * 1. Step7 策定したIT-BCPの経営層への説明・承認獲得

Step6で策定したIT-BCPを経営層に対して説明し、 承認を得る。 経営層から承認が得られなかった場合は、 Step6に戻り必要な修正を実施する。

* + - 1. 7.4 作業に必要な情報
         1. 表 7-1 「セキュリティインシデント発生時の事業継続計画策定」に必要となる情報

サブトピック  

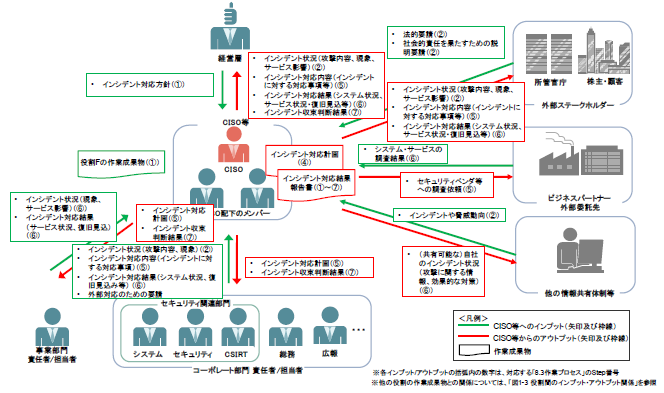

* + - 1. 7.5 作業の目標成果
         1. IT-BCP
      2. 7.6 作業で協同・連携する社内外の関係者と協同・連携の内容
         1. ・事業部門における事業継続要求と、 セキュリティ部門のセキュリティ対応可能な内容、 コーポレート部門における広報等の必要な対応内容を踏まえ、 実効的なIT-BCPを作成する。
         2. ・経営層、 事業部門、 コーポレート部門に対して、 IT-BCPを説明し、 承認を得る。
    1. 8. セキュリティインシデント発生時の危機管理（G）
       1. 8.1 目的・狙い
          1. セキュリティインシデント6により、 個人情報や機微情報が流出したり、 インフラ供給や重要なサービスの停止により社会に影響を与えたりした場合、 経営者は社会から経営責任が問われる可能性がある。
          2. しかし、 サイバー攻撃は避けられないリスクである以上

非常時に迅速な対応が可能となるよう事前に対応計画や体制を整備すること

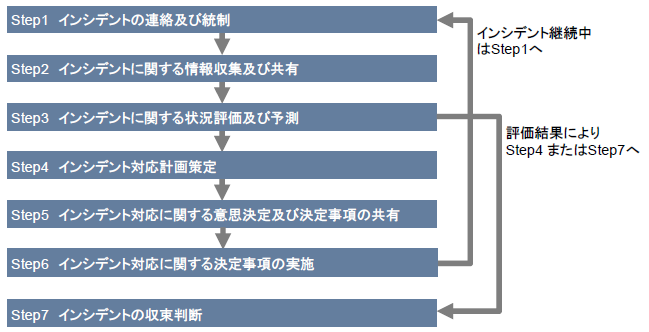
またインシデント発生後の通知先や開示が必要な項目に関して説明できるよう準備しておくこと

そして万が一インシデントによる被害が発生しても、 対応計画に則り、 適切に状況判断しながら、 対処していくこと

* + - * 1. が、 企業価値を損なわないために必要である。
        2. 本役割は、 経営層がセキュリティインシデントの発生時、 企業価値を損なわないための機能を確実に維持することを目的としている。
        3. 図 8-1 「セキュリティインシデント発生時の危機管理」の全体像

サブトピック  


* + - 1. 8.2 役割の作業内容
         1. ・インシデントに関する情報収集・評価を行い、 対応計画の策定と指示・管理を行う。
         2. ・社内外との調整等を行い、 インシデントを収束させる。
      2. 8.3 作業プロセス
         1. 図 8-2 「セキュリティインシデント発生時の危機管理」の作業プロセス

サブトピック  


* + - * 1. Step1 インシデントの連絡及び統制

インシデントの状況を認識し、 経営層からのインシデント対応方針に基づき、 危機対応のための体制を構築する。

* + - * 1. Step2 インシデントに関する情報収集及び共有

インシデントに関する情報を社内外から収集し、 経営層及びインシデント対応を行う各部門に共有する。

* + - * 1. Step3 インシデントに関する状況評価及び予測

収集されたインシデントに関する情報に基づき、 インシデントや事業に関する状況を評価すると共に、 今後のインシデントの変化や事業の状況、 それに伴う事業に対する影響について予測を行う。

インシデントが収束したと判断した場合、 Step7に進む。

* + - * 1. Step4 インシデント対応計画策定

Step3におけるインシデントに関する状況評価及び予測に基づき、 インシデント対応計画を策定する。

インシデント対応計画については、 各事業部門の責任者も策定する。 内容の整合性等については、 危機時に全社的に組織される危機管理委員会等の統率組織等において調整を行う等が考えられる。

* + - * 1. Step5 インシデント対応に関する意思決定及び決定事項の共有

Step4で策定したインシデント対応計画に基づき、 セキュリティ関連部門を含むコーポレート部門や事業部門に対して、 各部門の所掌範囲に応じたインシデント対応計画についての指示を行う。

なお、 事業部門に対する指示は、 事業部門の責任者経由である場合と、 事業部門に直接である場合がある。

* + - * 1. Step6 インシデント対応に関する決定事項の実施

インシデント対応に関する対応事項を実施する。 対応事項を指示した場合は、 その対応状況について把握を行う。

対応状況については、 （1）経営層／CISO等の指示があった場合、 （2）状況の変化があった場合、 （3）（状況の変化がなくとも）一定時間が経過した場合、 等、 適時のタイミングで把握し、 Step1に進む。

* + - * 1. Step7 インシデントの収束判断

Step3のインシデントに関する状況評価結果により、 インシデントが収束したと判断する。

なお収束判断としては

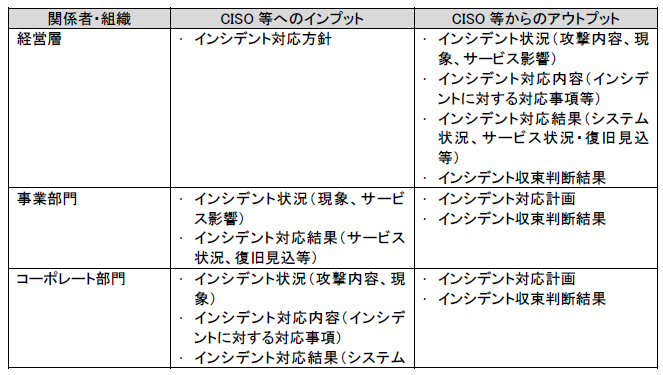
(1)インシデントに対する応急措置が終了した場合

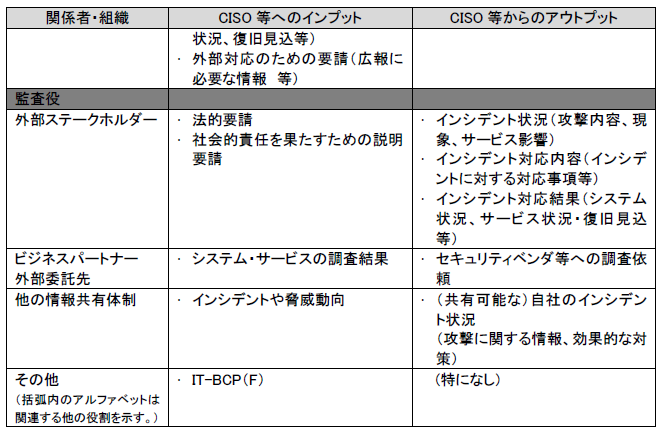
(2)インシデントの原因調査・復旧対応が終了した場合

(3)正式な事故報告書の作成・影響を受けた顧客へのフォロー・再発防止策の検討等事後対応が終了した場合

等が想定される。

* + - 1. 8.4 作業に必要な情報
         1. 表 8-1 「セキュリティインシデント発生時の危機管理」に必要となる情報

サブトピック  


サブトピック  


* + - 1. 8.5 作業の目標成果
         1. ・インシデント対応結果報告書（社内向け）
      2. 8.6 作業で協同・連携する社内外の関係者と協同・連携の内容
         1. ・経営層に対して、 インシデント状況やインシデント対応内容・結果、 サービスの状況等についての適時の報告
         2. ・企業価値を損なわないための、 外部ステークホルダーに対する自社のインシデント状況、 サービスへの影響等に関する情報開示
         3. ・他の情報共有機関等とのインシデントや脅威動向に関する情報共有
    1. 9. 付録： CISO等の経営・事業に関する役割のストーリー
       1. 1. 準大手産業機器メーカーA社： セキュリティガバナンス体制の構築・運営(A)
       2. 2． 中堅アパレルメーカーＸ社： セキュリティ投資計画の策定(C)

1. 情報セキュリティ 10大脅威2018【2018年3月IPA】
   1. 個人
      1. 第1位　インターネットバンキングやクレジットカード情報の不正利用
         1. ウイルス感染やフィッシング詐欺により、 インターネットバンキングの認証情報やクレジットカード情報が攻撃者に窃取され、 不正送金や不正利用が行われている。 2017年は、 インターネットバンキングの被害額は減少傾向だが、 新たに仮想通貨取引所の利用者を狙った攻撃が確認されている。
      2. 第2位　ランサムウェアによる被害
         1. ランサムウェアとは、 PCやスマートフォンにあるファイルの暗号化や画面のロックを行い、 復旧させることと引き換えに金銭を要求する手口に使われるウイルスである。 2017年は、 OSの脆弱性を悪用し、 感染した端末が接続しているネットワークを経路として感染を拡大させるタイプも登場している。 また、 感染した端末だけではなく、 その端末からアクセスできる共有サーバーや外付けHDDに保存されているファイルも暗号化されてしまう。
      3. 第3位　ネット上の誹謗・中傷
         1. コミュニティサイト（ブログ、 SNS、 掲示板等）上で、 個人や組織に対して誹謗・中傷や犯罪予告をする書き込みが行われている。 コミュニティサイトへの書き込みは、 匿名性や手軽さから安易に投稿してしまう傾向にある。 また、 SNSを使った犯罪は社会的な問題となっており、 2017年は殺人事件まで発展した事例もあった。
      4. 第4位　スマートフォンやスマートフォンアプリを狙った攻撃の可能性
         1. 不正アプリを利用者がインストールしてしまうことで、 スマートフォン内の重要な情報を窃取されたり、 不正に操作される被害が確認されている。 また、 データの暗号化等を行うランサムウェアに加えて、 2017年は個人情報を公開すると脅すランサムウェアも確認されている。 さらに、 これらの不正アプリは公式マーケットにも紛れ込んでおり、 公式マーケットであってもインストール前にアプリの信頼性について確認する等の警戒が必要である。
      5. 第5位　ウェブサービスへの不正ログイン
         1. ウェブサービスに不正ログインされ、 金銭的な被害や個人情報が窃取される等の被害が確認されている。 2017年に確認されたウェブサービスへの不正ログインの多くがパスワードリスト攻撃により行われている。 インターネットには多数のウェブサービスが存在しており、 ウェブサービスの利用者がパスワードの使いまわしや推測されやすいパスワードを使用している場合に、 不正ログインが行われてしまう。
      6. 第6位　ウェブサービスからの個人情報の窃取
         1. 2017年も引き続き、 ウェブサービスの脆弱性が悪用され、 ウェブサービス内に登録されている個人情報やクレジットカード情報を窃取される事件が多発している。 それらの情報を窃取されると、 攻撃者により個人情報を悪用して不審なメールを送信されたり、 クレジットカードを不正利用される可能性がある。
      7. 第7位　情報モラル欠如に伴う犯罪の低年齢化
         1. 2017年も未成年者がIT犯罪の加害者として逮捕、 補導される事件が確認されている。 IT犯罪に悪用できるツールや知識がインターネットを通じて誰でも入手・利用できるようになったことで、 情報モラルの欠如した未成年者が、 IT犯罪に手を染めやすくなっている。 また、 未成年者のPCやスマートフォンの所持も当たり前となってきており、 教員や親の監視が行き届きにくい。
      8. 第8位　ワンクリック請求等の不当請求
         1. PCやスマートフォンを利用中にアダルトサイトや出会い系サイト等にアクセスすることで金銭を不当に請求されるワンクリック請求の被害が依然として発生している。 1度のクリックによる請求だけでなく、 複数回のクリックをさせることで、 請求の正当性を主張して不当請求されてしまう事例も確認されている。
      9. 第9位　IoT 機器の不適切な管理
         1. 昨今、 IoT機器の利用が進んでいるが、 利用者はIoT機器がネットワークに接続されている機器であることを意識せずに利用してしまい、 適切な管理が行われていない。 そのような管理されていないIoT機器が攻撃者に狙われ、 分散型サービス妨害（DDoS）攻撃等に悪用されてしまう被害が確認されている。
      10. 第10位　偽警告
          1. PCやスマートフォンでウェブサイトを閲覧中に、 突然「ウイルスに感染している」等の偽警告を表示し、 利用者の不安を煽り、 偽警告の指示に従わせ、 個人情報等を窃取される被害が発生している。 偽警告は本物の警告と誤認されるように巧妙な細工が施されており、 被害者は信じて指示に従ってしまう。
   2. 組織
      1. 第1位　標的型攻撃による情報流出
         1. 企業や民間団体や官公庁等、 特定の組織を狙う、 標的型攻撃による攻撃が引き続き発生している。 メールの添付ファイルやウェブサイトを利用してPCにウイルスを感染させられると、 別のPCに感染を拡大され、 最終的に個人情報や業務上の重要情報が窃取される。
      2. 第2位　ランサムウェアによる被害
         1. ランサムウェアとは、 PC やスマートフォンにあるファイルの暗号化や画面のロックを行い、 復旧させることと引き換えに金銭を要求する手口に使われるウイルスである。 2017年は、 OSの脆弱性を悪用し、 感染した端末が接続しているネットワークを経路として感染を拡大させるタイプも登場している。 また、 感染した端末だけではなく、 その端末からアクセスできる共有サーバーや外付けHDDに保存されているファイルも暗号化されてしまう。 組織内のファイルが広範囲で暗号化された場合、 事業継続にも支障が出る可能性がある。
      3. 第3位　ビジネスメール詐欺
         1. 「ビジネスメール詐欺」（Business E-mail Compromise：BEC）は巧妙に細工したメールのやりとりにより、 企業の担当者を騙し、 攻撃者の用意した口座へ送金させる詐欺の手口である。 詐欺行為の準備としてウイルス等を悪用し、 企業内の従業員の情報が窃取されることもある。 これまでは主に海外の組織が被害に遭ってきたが、 2016年以降、 海外取引をしている国内企業でも被害が確認されている。
      4. 第4位　脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加
         1. 脆弱性対策情報の公開は、 脆弱性の脅威や対策情報を広く呼び掛けられるメリットがある。 一方、 その情報を攻撃者に悪用され、 対策前のシステムを狙う攻撃が行われている。 また、 近年では脆弱性情報の公開後、 その脆弱性を悪用した攻撃が本格化するまでの時間が短くなっている傾向がある。
      5. 第5位　セキュリティ人材の不足
         1. セキュリティ上の脅威は今後さらに増大するだけでなく、 新たな脅威も発生し続けていくことが予想される。 これらの脅威に対応するためにはセキュリティの知識、 技術を有するセキュリティ人材が欠かせないが、 圧倒的に不足しており、 問題視されている。 セキュリティ人材が手薄の組織では、 十分なセキュリティ対策、 対応をとることが難しく、 脅威の増大に伴い実被害につながることも考えられる。
      6. 第6位　ウェブサービスからの個人情報の窃取
         1. 2017年も引き続き、 ウェブサービスの脆弱性が悪用され、 ウェブサービス内に登録されている個人情報やクレジットカード情報等の重要な情報を窃取される被害が発生している。 それらの情報を窃取されると、 攻撃者により顧客や利用者の個人情報を悪用して不審なメールを送信されたり、 クレジットカードを不正利用される可能性がある。
      7. 第7位　IoT 機器の脆弱性の顕在化
         1. 2016年に引き続き、 IoT機器の脆弱性を悪用しウイルスに感染させることで、 インターネット上のサービスやサーバに対して、 大規模な分散型サービス妨害（DDoS）攻撃が行われる等の被害が確認されている。 また、 国内で発売されているIoT製品において脆弱性が発見されており、 機器を乗っ取られる、 または撮影機能等を悪用して個人情報を窃取されるといった危険性があることが公表されている。
      8. 第8位　内部不正による情報漏えい
         1. 組織内部の従業員や元従業員により、 私怨や金銭目的等の個人的な利益享受のため組織の情報が不正に持ち出されている。 また、 組織の情報持ち出しのルールを守らずに不正に情報を持ち出し、 さらにその情報を紛失し、 情報漏えいにつながることもある。 内部不正が発覚した場合、 組織は、 原因追求等の対応に追われ、 また社会的信用の失墜等にもつながる。
      9. 第9位　サービス妨害攻撃によるサービスの停止
         1. ウイルスに感染し、 ボットネット化した機器からDDoS（分散型サービス妨害）攻撃が行われ、 ウェブサイトやDNSサーバーが高負荷状態となり、 利用者がアクセスできなくなる被害が確認されている。 2017年は公式のアプリストアに公開されたスマートフォンアプリがボットネット化し、 DDoS攻撃が行われている。
      10. 第10位　犯罪のビジネス化（アンダーグラウンドサービス）
          1. 犯罪に使用するためのサービスやツールがアンダーグラウンド市場で取り引きされ、 これらを悪用した攻撃が行われている。 攻撃に対する専門知識に詳しくない者でもサービスやツールを利用することで、 容易に攻撃を行えるため、 サービスやツールが公開されると被害が広がるおそれがある。
2. 監査人の警鐘 ‐ 2018年 情報セキュリティ十大トレンド【2018年1月5日JASA】

ドキュメントを参照: [security\_trend\_top10.html](http://www.jasa.jp/seminar/security_trend_top10.html)

* 1. 多様化・巧妙化するランサムウェアの被害拡大
  2. 最新の対策もすり抜ける標的型攻撃による甚大な被害の発生
  3. セキュリティ機能が乏しいIoT製品への攻撃による社会的混乱
  4. クラウドなど集中管理による社会的規模の被害発生
  5. 考慮不足の働き方改革に起因する事故の発生
  6. 日本語ビジネスメール詐欺被害の拡大
  7. ガバナンス欠如のIT投資による重大インシデントの発生
  8. 成長しないマネジメントシステムによる組織活力の低下
  9. 形だけCSIRT/名ばかりセキュリティ人材による弊害の発生
  10. GDPR違反の摘発

1. 2017年セキュリティ10大ニュース【2017年12月So-net】

ドキュメントを参照: [newstopics\_201712.html](http://www.so-net.ne.jp/security/news/newstopics_201712.html?SmRcid=mlc_ml_security_topics)

* 1. 架空請求急増――実在企業かたるメール、 SMSが大量に出回る
  2. フィッシング多発――LINE、 グーグル、 アップル、 アマゾン、 マイクロソフト
  3. マルウェアメール頻発――添付の文書ファイルやメール内リンクで感染
  4. ランサムウェア騒動――Windows Updateとバックアップで対策
  5. 不正ログイン多発――「PW使い回し」狙うリスト攻撃でポイント不正利用
  6. 不正アクセス多発――脆弱性攻撃で大量の個人情報、 クレカ情報流出
  7. アマゾン「マーケットプレイス」で通販詐欺大量発生――返金後も残る不安
  8. ネット接続機器の問題が次々明らかに――脆弱性が放置される機器も多数
  9. マルウェア感染――文書ファイル、 スクリプトファイルが主流に
  10. Windows Vista、 Office 2007サポート終了――パッチ提供の緊急事態も
  11. 参考URL
      1. <注1：架空請求>
         1. ・実在企業名で「有料動画の未納料金が発生している」と脅すSMS詐欺に注意
         2. http://security-t.blog.so-net.ne.jp/2017-03-02

ドキュメントを参照: [2017-03-02](http://security-t.blog.so-net.ne.jp/2017-03-02)

* + - 1. ・架空請求で高齢男性が被害5270万円――メールだけでなくハガキにも注意
      2. http://security-t.blog.so-net.ne.jp/2017-04-27-1

ドキュメントを参照: [2017-04-27-1](http://security-t.blog.so-net.ne.jp/2017-04-27-1)

* + - 1. ・架空請求SMSのバラマキが連日発生、 被害相談でヒットする詐欺サイトにも注意
      2. http://security-t.blog.so-net.ne.jp/2017-05-29

ドキュメントを参照: [2017-05-29](http://security-t.blog.so-net.ne.jp/2017-05-29)

* + - 1. ・「コンビニ払い」の架空請求に注意――仮想通貨購入口座に入金させる新手口
      2. http://security-t.blog.so-net.ne.jp/2017-07-03

ドキュメントを参照: [2017-07-03](http://security-t.blog.so-net.ne.jp/2017-07-03)

* + - 1. ・「心当たりのないメール・SMSには反応しないで」国民生活センターが呼びかけ
      2. http://security-t.blog.so-net.ne.jp/2017-07-07-2

ドキュメントを参照: [2017-07-07-2](http://security-t.blog.so-net.ne.jp/2017-07-07-2)

* + - 1. ・「架空請求詐欺」件数が1.7倍に。 今年上半期の特殊詐欺（警察庁）
      2. http://security-t.blog.so-net.ne.jp/2017-08-16

ドキュメントを参照: [2017-08-16](http://security-t.blog.so-net.ne.jp/2017-08-16)

* + - 1. ・架空請求の被害急増――はがき、 メール、 SMSで届く未払い料金の請求に注意
      2. http://security-t.blog.so-net.ne.jp/2017-11-21

ドキュメントを参照: [2017-11-21](http://security-t.blog.so-net.ne.jp/2017-11-21)

* + - 1. ・SMSを用いて有料動画サイトの未払料金などの名目で金銭を支払わせようとする「株式会社DMM.comをかたる事業者」に関する注意喚起［PDF］（消費者庁）
      2. http://www.caa.go.jp/policies/policy/consumer\_policy/information/pdf/170228adjustments\_1.pdf

ドキュメントを参照: [170228adjustments\_1.pdf](http://www.caa.go.jp/policies/policy/consumer_policy/information/pdf/170228adjustments_1.pdf)

* + - 1. ・SMSを用いて有料動画の未納料金の名目で金銭を支払わせようとする「アマゾンジャパン合同会社等をかたる架空請求」に関する注意喚起［PDF］（消費者庁）
      2. http://www.caa.go.jp/policies/policy/consumer\_policy/information/pdf/consumer\_policy\_information\_171114\_0001.pdf

ドキュメントを参照: [consumer\_policy\_information\_171114\_0001.pdf](http://www.caa.go.jp/policies/policy/consumer_policy/information/pdf/consumer_policy_information_171114_0001.pdf)

* + 1. <注2：フィッシング>
       1. ・2016年12月の国内フィッシング事情
       2. http://security-t.blog.so-net.ne.jp/2017-01-27

ドキュメントを参照: [2017-01-27](http://security-t.blog.so-net.ne.jp/2017-01-27)

* + - 1. ・2017年1月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-02-06

ドキュメントを参照: [2017-02-06](http://security-t.blog.so-net.ne.jp/2017-02-06)

* + - 1. ・2017年2月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-03-06

ドキュメントを参照: [2017-03-06](http://security-t.blog.so-net.ne.jp/2017-03-06)

* + - 1. ・2017年3月、 4月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-05-09-3

ドキュメントを参照: [2017-05-09-3](http://security-t.blog.so-net.ne.jp/2017-05-09-3)

* + - 1. ・2017年5月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-06-08-1

ドキュメントを参照: [2017-06-08-1](http://security-t.blog.so-net.ne.jp/2017-06-08-1)

* + - 1. ・2017年6月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-07-05

ドキュメントを参照: [2017-07-05](http://security-t.blog.so-net.ne.jp/2017-07-05)

* + - 1. ・2017年7月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-08-07

ドキュメントを参照: [2017-08-07](http://security-t.blog.so-net.ne.jp/2017-08-07)

* + - 1. ・2017年8月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-09-11-1

ドキュメントを参照: [2017-09-11-1](http://security-t.blog.so-net.ne.jp/2017-09-11-1)

* + - 1. ・2017年9月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-10-06-2

ドキュメントを参照: [2017-10-06-2](http://security-t.blog.so-net.ne.jp/2017-10-06-2)

* + - 1. ・2017年10月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-11-24

ドキュメントを参照: [2017-11-24](http://security-t.blog.so-net.ne.jp/2017-11-24)

* + - 1. ・2017年11月の国内フィッシング事情
      2. http://security-t.blog.so-net.ne.jp/2017-12-21

ドキュメントを参照: [2017-12-21](http://security-t.blog.so-net.ne.jp/2017-12-21)

* + 1. <注3：マルウェアメール>
       1. ・さまざまな件名でマルウェア（ウイルス）付き日本語メール拡散中
       2. http://security-t.blog.so-net.ne.jp/2017-01-23

ドキュメントを参照: [2017-01-23](http://security-t.blog.so-net.ne.jp/2017-01-23)

* + - 1. ・さまざまな件名で届く「バンキングマルウェア」メール――感染しないチェック法
      2. http://security-t.blog.so-net.ne.jp/2017-05-26

ドキュメントを参照: [2017-05-26](http://security-t.blog.so-net.ne.jp/2017-05-26)

* + - 1. ・請求書を装うマルウェアメールに注意、 Excelマクロでマルウェア感染
      2. http://security-t.blog.so-net.ne.jp/2017-06-05

ドキュメントを参照: [2017-06-05](http://security-t.blog.so-net.ne.jp/2017-06-05)

* + - 1. ・Excelファイルの添付メールに注意、 マルウェア感染のおそれ
      2. http://security-t.blog.so-net.ne.jp/2017-07-20

ドキュメントを参照: [2017-07-20](http://security-t.blog.so-net.ne.jp/2017-07-20)

* + - 1. ・日本郵便など騙るマルウェアメールに注意――添付ファイルで不正送金ウイルス感染
      2. http://security-t.blog.so-net.ne.jp/2017-07-27-2

ドキュメントを参照: [2017-07-27-2](http://security-t.blog.so-net.ne.jp/2017-07-27-2)

* + - 1. ・請求書メールに注意、 添付ファイルでマルウェア感染
      2. http://security-t.blog.so-net.ne.jp/2017-09-01

ドキュメントを参照: [2017-09-01](http://security-t.blog.so-net.ne.jp/2017-09-01)

* + - 1. ・実在企業装うDL型マルウェアメール相次ぐ――リンク先クリックで感染のおそれ
      2. http://security-t.blog.so-net.ne.jp/2017-09-29

ドキュメントを参照: [2017-09-29](http://security-t.blog.so-net.ne.jp/2017-09-29)

* + - 1. ・「詳しくはこちら」クリックに注意――自然な日本語のマルウェアメールが続々
      2. http://security-t.blog.so-net.ne.jp/2017-10-12-1

ドキュメントを参照: [2017-10-12-1](http://security-t.blog.so-net.ne.jp/2017-10-12-1)

* + - 1. ・クレカの請求案内装うマルウェアメールに注意――明細確認で感染のおそれ
      2. http://security-t.blog.so-net.ne.jp/2017-10-24

ドキュメントを参照: [2017-10-24](http://security-t.blog.so-net.ne.jp/2017-10-24)

* + - 1. ・実在企業装うマルウェアメールに注意、 リンクのクリックで感染のおそれ
      2. http://security-t.blog.so-net.ne.jp/2017-11-08

ドキュメントを参照: [2017-11-08](http://security-t.blog.so-net.ne.jp/2017-11-08)

* + - 1. ・実在企業装うマルウェアメール頻発――ダウンロード型、 添付型それぞれの手口
      2. http://security-t.blog.so-net.ne.jp/2017-11-28

ドキュメントを参照: [2017-11-28](http://security-t.blog.so-net.ne.jp/2017-11-28)

* + - 1. ・インターネットバンキングマルウェアに感染させるウイルス付メールに注意（JC3）
      2. https://www.jc3.or.jp/topics/virusmail.html

ドキュメントを参照: [virusmail.html](https://www.jc3.or.jp/topics/virusmail.html)

* + 1. <注4：ランサムウェア>
       1. ・ランサムウェアの被害拡大、 今すぐWindows Updateとバックアップを（IPA）
       2. http://security-t.blog.so-net.ne.jp/2017-05-19-1
       3. ・さまざまな件名で届く「バンキングマルウェア」メール――感染しないチェック法
       4. http://security-t.blog.so-net.ne.jp/2017-05-26
       5. ・猛威ふるうランサムウェア、 国内上陸前に対策を
       6. http://security-t.blog.so-net.ne.jp/2017-06-29
       7. ・請求書メールに注意、 添付ファイルでマルウェア感染
       8. http://security-t.blog.so-net.ne.jp/2017-09-01
       9. ・文書ファイル悪用感染に新手口――誤操作でPC内ファイル暗号化のおそれ
       10. http://security-t.blog.so-net.ne.jp/2017-11-06
    2. <注5：不正ログイン>
       1. ・「リスト型攻撃」相次ぐ――同じID・パスワードの使いまわしに注意
       2. http://security-t.blog.so-net.ne.jp/2017-10-06
    3. <注6：不正アクセス>
       1. ・不正アクセス相次ぐ～通販サイトで情報漏えい、 便乗フィッシングに注意
       2. http://security-t.blog.so-net.ne.jp/2017-01-06
       3. ・情報流出事故相次ぐ――都税と住宅金融機構のクレカ支払いサイト、 ジェトロ、 法政大
       4. http://security-t.blog.so-net.ne.jp/2017-03-14-2
       5. ・不正アクセスで情報流出　日本郵便、 沖縄電力、 2社のオンラインショップ
       6. http://security-t.blog.so-net.ne.jp/2017-03-17-1
       7. ・サーバーソフトの欠陥でクレカ情報など流出――不正使用630万円
       8. http://security-t.blog.so-net.ne.jp/2017-04-27-2
       9. ・サーバーソフトの欠陥による個人情報流出、 国交省や総務省のサイトでも
       10. http://security-t.blog.so-net.ne.jp/2017-06-13
    4. <注7：通販詐欺>
       1. ・大手通販サイトで「注文した商品が届かない」トラブル続出
       2. http://security-t.blog.so-net.ne.jp/2017-04-28
    5. <注8：機器の脆弱性>
       1. ・Androidなど「Bluetooth搭載端末」数十億台に影響する脆弱性が明らかに
       2. http://security-t.blog.so-net.ne.jp/2017-09-14
       3. ・ルーターやネットワークカメラに脆弱性――危険な状態で使っていないかチェックを
       4. http://security-t.blog.so-net.ne.jp/2017-09-15
       5. ・多数の無線LAN機器に影響する脆弱性が明らかに――通信が盗聴されるおそれ
       6. http://security-t.blog.so-net.ne.jp/2017-10-20
       7. ・ドコモのモバイルルーター「Wi-Fi STATION L-02F」に脆弱性、 早急に更新を
       8. http://security-t.blog.so-net.ne.jp/2017-11-07-1
       9. ・バッファローの有線ルータに脆弱性、 最新のファームウェアに更新を
       10. http://security-t.blog.so-net.ne.jp/2017-12-05-1
       11. ・BlueBorne：様々な Bluetooth 実装に複数の脆弱性(jvn)
       12. https://jvn.jp/vu/JVNVU95513538/index.html
       13. ・KRACK：Wi-Fi Protected Access II (WPA2) ハンドシェイクにおいて Nonceおよびセッション鍵が再利用される問題（jvn）
       14. https://jvn.jp/vu/JVNVU90609033/index.html
    6. <注9：マルウェア感染>
       1. ・さまざまな件名でマルウェア（ウイルス）付き日本語メール拡散中
       2. http://security-t.blog.so-net.ne.jp/2017-01-23
       3. ・Word文書送り付けるゼロデイ攻撃が発生中、 Officeに影響する脆弱性発覚
       4. http://security-t.blog.so-net.ne.jp/2017-04-11-2
       5. ・さまざまな件名で届く「バンキングマルウェア」メール――感染しないチェック法
       6. http://security-t.blog.so-net.ne.jp/2017-05-26
       7. ・請求書を装うマルウェアメールに注意、 Excelマクロでマルウェア感染
       8. http://security-t.blog.so-net.ne.jp/2017-06-05
       9. ・Excelファイルの添付メールに注意、 マルウェア感染のおそれ
       10. http://security-t.blog.so-net.ne.jp/2017-07-20
       11. ・日本郵便など騙るマルウェアメールに注意――添付ファイルで不正送金ウイルス感染
       12. http://security-t.blog.so-net.ne.jp/2017-07-27-2
       13. ・うっかり操作でマルウェア感染、 IPAが文書ファイルの新たな悪用手口を解説
       14. http://security-t.blog.so-net.ne.jp/2017-08-02
       15. ・請求書メールに注意、 添付ファイルでマルウェア感染
       16. http://security-t.blog.so-net.ne.jp/2017-09-01
       17. ・実在企業装うDL型マルウェアメール相次ぐ――リンク先クリックで感染のおそれ
       18. http://security-t.blog.so-net.ne.jp/2017-09-29
       19. ・「詳しくはこちら」クリックに注意――自然な日本語のマルウェアメールが続々
       20. http://security-t.blog.so-net.ne.jp/2017-10-12-1
       21. ・クレカの請求案内装うマルウェアメールに注意――明細確認で感染のおそれ
       22. http://security-t.blog.so-net.ne.jp/2017-10-24
       23. ・文書ファイル悪用感染に新手口――誤操作でPC内ファイル暗号化のおそれ
       24. http://security-t.blog.so-net.ne.jp/2017-11-06
       25. ・実在企業装うマルウェアメールに注意、 リンクのクリックで感染のおそれ
       26. http://security-t.blog.so-net.ne.jp/2017-11-08
       27. ・実在企業装うマルウェアメール頻発――ダウンロード型、 添付型それぞれの手口
       28. http://security-t.blog.so-net.ne.jp/2017-11-28
       29. ・危険な「添付ファイル」――感染を防ぐ基本設定、 誤開封後の対処法
       30. http://www.so-net.ne.jp/security/news/newstopics\_201708.html
    7. <注10：サポート終了>
       1. ・（サポート終了）Vistaは4月11日、 Office 2007は10月10日――対策必須
       2. http://security-t.blog.so-net.ne.jp/2017-02-13
       3. ・MS、 4月度のセキュリティパッチを公開　Vistaのパッチはこれが最後
       4. http://security-t.blog.so-net.ne.jp/2017-04-12-1
       5. ・マイクロソフト、 6月度の月例セキュリティパッチを公開――XPやVista用のパッチも
       6. http://security-t.blog.so-net.ne.jp/2017-06-14-1
       7. ・マイクロソフト、 月例セキュリティパッチを公開。 「Office 2007」サポート終了
       8. http://security-t.blog.so-net.ne.jp/2017-10-12
       9. ・実在企業装うマルウェアメール頻発――ダウンロード型、 添付型それぞれの手口
       10. http://security-t.blog.so-net.ne.jp/2017-11-28
       11. ・2017年6月のセキュリティ更新プログラム（月例）（マイクロソフト）
       12. https://blogs.technet.microsoft.com/jpsecurity/2017/06/14/201706-security-bulletin/

ドキュメントを参照: [201706-security-bulletin](https://blogs.technet.microsoft.com/jpsecurity/2017/06/14/201706-security-bulletin/)

1.  サイバーセキュリティ経営ガイドライン Ver 2.0【2017年11月16日METI】

ドキュメントを参照: [20171116003-1.pdf](http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf)

* 1. サイバーセキュリティ経営ガイドライン・概要
     1. I．サイバーセキュリティは経営問題
        1. 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
        2. 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。
     2. II．経営者が認識すべき３原則
        1. (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. (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. (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
     3. III．サイバーセキュリティ経営の重要１０項目
        1. 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
        2. 指示２：サイバーセキュリティリスク管理体制の構築
        3. 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
        4. 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
        5. 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
        6. 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
        7. 指示７：インシデント発生時の緊急対応体制の整備
        8. 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
        9. 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
        10. 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
  2. １．はじめに
     1. 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
        1. 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。
        2. 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。
           1. 中小企業の情報セキュリティ対策ガイドライン(IPA)

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - * 1. 企業経営のためのサイバーセキュリティの考え方（NISC）

ドキュメントを参照: [keiei.pdf](http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf)

* + 1. １．２．本ガイドラインの構成と活用方法
       1. 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。
       2. 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。
       3. 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。
       4. 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。
          1. 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
          2. 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
          3. 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
          4. 付録D 重要１０項目とISO/IEC27001、 27002の関係性
          5. 付録E 本ガイドラインで使用している用語の定義
       5. 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。
          1. 組織における内部不正防止ガイドライン（IPA）

ドキュメントを参照: [000044615.pdf](https://www.ipa.go.jp/files/000044615.pdf)

* + - 1. 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。
  1. ２．経営者が認識すべき３原則
     1. （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
        1. 【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】
        2.  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。
        3.  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。
        4.  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。
     2. （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
        1. 【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.  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。
        3.  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。
     3. （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
        1. 【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】
        2.  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。
        3.  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。
  2. ３．サイバーセキュリティ経営の重要１０項目
     1. 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。
     2. ３．１．サイバーセキュリティリスクの管理体制構築
        1. 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
           1. 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。
           2. 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。

* + - 1. 指示２ サイバーセキュリティリスク管理体制の構築
         1. 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。
         2. 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。
         3. 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。

* + - 1. 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
         1. 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。
         2. 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。

* + 1. ３．２．サイバーセキュリティリスクの特定と対策の実装
       1. 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
          1. 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。
          2. 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。
          3. 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

* + - 1. 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
         1. 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。
         2. 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。

* + - 1. 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
         1. 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。
         2. 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。
         3. 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。
         4. 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。

* + 1. ３．３．インシデント発生に備えた体制構築 3
       1. 指示７ インシデント発生時の緊急対応体制の整備
          1. 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。
          2. 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。
          3. 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。
          4. 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。

* + - 1. 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
         1. 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。
         2. 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。
         3. 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。
         4. 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。

* + 1. ３．４．サプライチェーンセキュリティ対策の推進
       1. 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
          1. 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。
          2. 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。
          3. 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

ドキュメントを参照: [security-action](https://www.ipa.go.jp/security/security-action/)

* + - * 1. 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。

* + 1. 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
       1. 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. 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。
          2. 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。
          3. 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。

* 1. 付録Ａ サイバーセキュリティ経営チェックシート
     1. ※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
     2. ※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）
     3. Framework for Improving Critical Infrastructure Cybersecurity(NIST)

ドキュメントを参照: [cybersecurity-framework-021214.pdf](https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf)

* + 1. ＜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管理体制構築）
          1. 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

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: 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

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

* + - * 1. 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)

* + - * 1. 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

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

(－)

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）

PR.AT-2: 権限を持つユーザ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-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

* + - 1. （サイバーセキュリティリスクの特定と対策の実装）
         1. 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)

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)

* + - * 1. 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

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

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

* + - * 1. 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

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

(－)

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

(－)

* + - 1. （インシデント発生に備えた体制構築）
         1. 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

* + - * 1. 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)

定期的に復旧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

* + 1. ＜サプライチェーンセキュリティ対策の推進＞
       1. 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
          1. 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

* + - * 1. 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

* + - * 1. 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

(－)

* + 1. ＜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＞
       1. 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. 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

* + - * 1. 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

* 1. 付録Ｂ サイバーセキュリティ対策に関する参考情報
     1. 重要１０項目全般に関連する参考情報
        1. 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）

ドキュメントを参照: [csmgl-kaisetsusho.html](https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html)

* + - * 1. （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。 ）
      1. 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）

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - * 1. (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。 )
      1. ISO/IEC 27002:2013（ISO/IEC）
         1. （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。 ）
      2. Framework for Improving Critical Infrastructure Cybersecurity [Version 1.0]（NIST）【2014 年2 月12 日】

ドキュメントを参照: [cybersecurity-framework-021214.pdf](https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf)

* + - * 1. 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。 ）
        2. 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】

ドキュメントを参照: [000038957.pdf](https://www.ipa.go.jp/files/000038957.pdf)

* + - 1. SP800-53 [Rev.4]（NIST）

ドキュメントを参照: [NIST.SP.800-53r4.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

* + - * 1. （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。 ）
      1. SP800-171 [Rev.1]（NIST）

ドキュメントを参照: [NIST.SP.800-171r1.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf)

* + - * 1. （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。 ）
    1. 指示３に関連する参考情報
       1. 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）

ドキュメントを参照: [000039528.pdf](https://www.ipa.go.jp/files/000039528.pdf)

* + - * 1. （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。 ）
      1. 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）

ドキュメントを参照: [000047872.pdf](https://www.ipa.go.jp/files/000047872.pdf)

* + - * 1. （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。 ）
    1. 指示４に関連する参考情報
       1. 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）

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - * 1. （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。 ）
    1. 指示５に関連する参考情報
       1. 「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）

ドキュメントを参照: [000046236.pdf](https://www.ipa.go.jp/files/000046236.pdf)

* + - * 1. （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。 ）
      1. 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）

ドキュメントを参照: [apt-loganalysis.html](https://www.jpcert.or.jp/research/apt-loganalysis.html)

* + - * 1. （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。 ）
      1. 組織における内部不正防止ガイドライン[第4版]（IPA）

ドキュメントを参照: [000057060.pdf](https://www.ipa.go.jp/files/000057060.pdf)

* + - * 1. （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。 ）
      1. 秘密情報の保護ハンドブック[平成28年2月]（経済産業省）

ドキュメントを参照: [trade-secret.htm](http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.htm)

* + - * 1. （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。 ）
    1. 指示６に関連する参考情報
       1. 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）

ドキュメントを参照: [isms.html](https://isms.jp/isms.html)

* + - * 1. （情報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ISO/IEC27001に基づいて第三者認証を行う制度。 ）
      1. 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）

ドキュメントを参照: [csms.html](https://isms.jp/csms.html)

* + - * 1. （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。 ）
      1. 情報セキュリティ管理基準（経済産業省）

ドキュメントを参照: [index.html](http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html)

* + - * 1. （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。 ）
      1. 情報セキュリティ対策ベンチマーク（IPA）

ドキュメントを参照: [benchmark](http://www.ipa.go.jp/security/benchmark/)

* + - * 1. （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。 ）
      1. 安全なウェブサイトの作り方[第7版]（IPA）

ドキュメントを参照: [websecurity.html](https://www.ipa.go.jp/security/vuln/websecurity.html)

* + - * 1. （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。 ）
      1. JVN（IPA、 JPCERT/CC）

ドキュメントを参照: [jvn.jp](https://jvn.jp/)

* + - * 1. （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。 ）
    1. 指示７に関連する参考情報
       1. CSIRT構築マテリアル（JPCERT/CC）

ドキュメントを参照: [csirt\_material](https://www.jpcert.or.jp/csirt_material/)

* + - * 1. （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。 ）
      1. CSIRT構築に役立つ参考資料（日本シーサート協議会）

ドキュメントを参照: [build-wg-document.html](http://www.nca.gr.jp/activity/build-wg-document.html)

* + - * 1. （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。 ）
    1. 指示８に関連する参考情報
       1. 事業継続ガイドライン[平成25年8月改定]（内閣府）

ドキュメントを参照: [guideline03.pdf](http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03.pdf)

* + - * 1. （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。 ）
    1. 指示９に関連する参考情報
       1. 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）

ドキュメントを参照: [140313shitaukeGL3.pdf](http://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf)

* + - * 1. （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。 ）
      1. SECURITY ACTION セキュリティ対策自己宣言（IPA）

ドキュメントを参照: [security-action](https://www.ipa.go.jp/security/security-action/)

* + - * 1. （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。 ）
    1. 指示１０に関連する参考情報
       1. 届出・相談・情報提供（不正アクセスやウイルス等に関する届出）（IPA）

ドキュメントを参照: [todoke-top-j.html](https://www.ipa.go.jp/security/outline/todoke-top-j.html)

* + - * 1. （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。 ）
      1. 標的型サイバー攻撃特別相談窓口（IPA）

ドキュメントを参照: [tokubetsu](https://www.ipa.go.jp/security/tokubetsu/)

* + - * 1. （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。 ）
      1. サイバー情報共有イニシアティブ（J-CSIP）（IPA）

ドキュメントを参照: [J-CSIP](https://www.ipa.go.jp/security/J-CSIP/)

* + - * 1. （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。 ）
      1. @police（警察庁）

ドキュメントを参照: [cyberpolice](https://www.npa.go.jp/cyberpolice/)

* + - * 1. （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。 ）
  1. 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

ドキュメントを参照: [20171116003-2.xlsx](http://www.meti.go.jp/press/2017/11/20171116003/20171116003-2.xlsx)

* + 1. 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）
    2. 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
    3. 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
    4. 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
    5. 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
    6. 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
  1. 付録Ｄ 国際規格ISO/IEC27001及び27002との関係
  2. 付録Ｅ 用語の定義
     1. （1） インシデント
        1. 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. （2） 監査
        1. 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. （3） サイバー攻撃
        1. 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。
     4. （4） サイバーセキュリティ
        1. 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不具合が生じないようにすること。
     5. （5） サイバーセキュリティリスク
        1. 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. （6） 残留リスク
        1. 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. （7） 情報セキュリティ報告書
        1. 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。
        2. （参考： 経済産業省の「情報セキュリティ報告書モデル」：

ドキュメントを参照: [2007\_JohoSecurityReportModelRevised.pdf）](http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf）)

* + 1. （8） ステークホルダー
       1. 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。
    2. （9） セキュリティポリシー
       1. 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。
    3. （10）多層防御
       1. 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。
       2. 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。
    4. （11）ビジネスパートナー
       1. 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。
    5. （12）マルウェア
       1. 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。
    6. （13）リスク
       1. 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。
    7. （14）リスク対応（回避、 低減、 移転、 保有）
       1. 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。
       2. ① リスク回避
          1. 「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。
       3. ② リスク低減
          1. 「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。
       4. ③ リスク移転
          1. 「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。
       5. ④ リスク保有
          1. 「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。
    8. （15）リスク評価
       1. 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。
    9. （16）リスク分析
       1. 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。
    10. （17）ログ
        1. 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。
    11. （18）BCP（Business Continuity Plan）
        1. 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。
    12. （19）CISO（Chief Information Security Officer）
        1. 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。
    13. （20）CSIRT（Computer Security Incident Response Team）
        1. インシデントの発生に対応するための体制のこと。
    14. （20）PDCA
        1. 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。
        2. 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。
        3. 2.Do：目標と計画をもとに、 実際の業務を行う。
        4. 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。
        5. 4.Act：評価結果をもとに、 業務の改善を行う。

1. 情報セキュリティ白書2017【2017年7月IPA】

ドキュメントを参照: [2017.html](https://www.ipa.go.jp/security/publications/hakusyo/2017.html)

* 1. 序章 2016年度の情報セキュリティの概況
  2. 第1章 情報セキュリティインシデント・脆弱性の現状と対策
     1. 1.1 2016年度に観測されたインシデント状況
     2. 1.2 情報セキュリティインシデント別の状況と事例
     3. 1.3 攻撃・手口の動向と対策
     4. 1.4 情報システムの脆弱性の動向
     5. 1.5 情報セキュリティ対策の状況
  3. 第2章 情報セキュリティを支える基盤の動向
     1. 2.1 日本の情報セキュリティ政策の状況
     2. 2.2 情報セキュリティ関連法の整備状況
     3. 2.3 国別・地域別の情報セキュリティ政策の状況
     4. 2.4 情報セキュリティ人材の現状と育成
     5. 2.5 情報セキュリティマネジメント
     6. 2.6 国際標準化活動
     7. 2.7 評価認証制度
     8. 2.8 情報セキュリティの普及啓発活動
     9. 2.9 情報セキュリティ産業の規模と成長の動向
     10. 2.10 その他の情報セキュリティの状況
  4. 第3章 個別テーマ
     1. 3.1 制御システムの情報セキュリティ
     2. 3.2 IoTの情報セキュリティ
     3. 3.3 スマートデバイスの情報セキュリティ
     4. 3.4 金融の情報セキュリティ
     5. 3.5 オリンピックに向けた情報セキュリティ対策
  5. 付録 情報セキュリティ10大脅威2017・資料・ツール
     1. 情報セキュリティ10大脅威2017
     2. 資料A 2016年のコンピュータウイルス届出状況
     3. 資料B 2016年のコンピュータ不正アクセス届出状況
     4. 資料C ソフトウェア等の脆弱性関連情報に関する届出状況
     5. ツール 各ツールの紹介

1. 匿名加工情報の事例集（JIPDEC認定個人情報保護団体対象事業者向け）【PDF】【2017年7月JIPDEC】

ドキュメントを参照: [AOP\_006.pdf](https://www.jipdec.or.jp/protection_org/u71kba00000001hh-att/AOP_006.pdf)

1. 改正個人情報保護法（2017年5月改正施行）対応

ドキュメントを参照: [news005.html](http://www.atmarkit.co.jp/ait/articles/1704/24/news005.html)

* 1. 背景
     1. 攻撃を検知するためだけのIT投資とは、 いわば 守りの投資 であり、 企業に利益を生み出すものではありません
     2. そのため、 経営者に投資の目的を納得させるのが難しい場合もあるでしょう
     3. 事実としてサイバー攻撃への対処は経営課題であり、 そのための投資は企業にとって不可欠
     4. なぜなら、 それによって企業のイノベーションに弊害が及ぶからです
  2. 「全体最適」の視点でバランスの取れたセキュリティ対策を
     1. サイバー攻撃の脅威を無視することは、 新しい事業を生み出す先進的なアイデアとエネルギーを奪ってしまうことを意味する
     2. マルウェアの侵入には入口対策とエンドポイント対策で対処し、 外部との通信路の確立やサーバとの不正通信は出口対策や内部対策で防ぐといった具合
     3. さらに、 もしこれらが突破されてしまった場合にはログを取得／保全して説明責任を果たせるように するなど、 システム全体でバランスの取れた設計を考えることが何よりも重要
  3. 統合的にデザインすることがセキュリティの強化につながる
     1. セキュリティの強化を意識しすぎるあまり、 業務運用にまで悪影響を及ぼしては本末転倒だ。 業務上、 必要な経路は開きつつ、 適切に監視を行うことが肝要
     2. システムを設計する際やイノベーションを起こすためのプラットフォームを構築する際、 セキュリティは全体最適の視点で設計する
     3. 業務全体のデザインとセキュリティのデザインを合わせて統合的にデザイン
     4. こうすることでセキュリティ施策の価値が一層高まり、 セキュリティのための投資ではなくイノベーションのための投資として説明し、 経営者から必要な投資を得やすくなるのです
  4. 改正個人情報保護法のポイント
     1. 個人情報の定義が変更され、 従来の個人情報に加えて個人識別符号の定義（免許証番号、 マイナンバー、 生体情報など）が追加
     2. 人種や病歴、 犯罪歴といった要配慮個人情報が新設
     3. 改正個人情報保護法にどう対応すべきかを解説したガイドラインは2016年11月30日に公開

ドキュメントを参照: [preparation](http://www.ppc.go.jp/personal/preparation/)

* + - 1. ポイントは「組織的安全管理措置」に記載された「取扱状況の把握及び安全管理措置の見直し」
      2. これは監査できちんとチェックし、 経営者に報告して改善を図っているかを問うもの
      3. もし現状の安全管理措置が十分でない場合でも、 きちんと監査が行われていれば対応レベルは向上していくはず
      4. 今後は、 個人情報に関して何かインシデントが起きた際には、 報告命令や業務改善命令、 緊急命令などの大きな権限を持つ個人情報保護委員会から何らかの指導を受けるといった事態も起こり得るため
  1. 匿名加工情報でデータの利活用が容易に
     1. 匿名加工を施して本人を再識別できないようにした情報ならば、 本人の同意なしで他社に提供できるようになる
  2. クレジットカード番号など民間付与の番号も個人情報に海外移転にも規制
     1. 個人情報の定義が明確化され、 氏名、 住所、 電話番号などの一般的な個人情報に加えて、 マスターと突合して個人が特定できる情報も個人情報として取り扱われることとなった。
     2. 例えば、 民間企業が扱うクレジットカード番号、 口座番号、 企業固有の顧客番号、 社員番号、 会社のメールアドレスなども対象となる。
     3. また、 個人識別符号が新たに定義され、 パスポート番号、 運転免許証番号、 健康保険者番号、 マイナンバーなどの公文書に振られた番号、 さらにはDNA配列、 指紋、 静脈、 虹彩といった身体の一部および歩行時の姿勢や動作など人の動きを表したものも対象となり、 これらに対して格別の安全管理措置が求められる
     4. 技術的安全管理対策の観点では、 暗号化について新たな指針が提示された。
     5. 2017年2月16日に個人情報保護委員会が告示「個人データの漏えい等の事案が発生した場合等の対応について」を公表。 この中では、 個人情報を高度に暗号化した場合は秘匿性が高まるため、 万一漏えいした際にも、 国（および本人）への報告義務は許容されるなどの指針が示されている。
  3. 2018年には「EUデータ保護規則」が施行
     1. 「忘れられる権利」や、 自分の個人情報を持つ企業に対して他社への移転を要求する「データポータビリティ」が追加されるなど、 いくつかの規制強化が図られている。
     2. EUデータ保護規則では、 これに対応した仕組みを初めから設計（バイデザイン）して業務に組み込む（バイデフォルト）ことを求めており、 自社で監査して何か問題があれば報告すべしとされている。 これは企業の情報セキュリティ施策にも大きくかかわる方針であり、 今後、 各社のIT部門が特に留意すべき点だと言えよう。
  4. データを中心に据えた「多層防御」で機密情報を守る
     1. システム側で対応すべき事項として「暗号化」と「ログの収集と監査／検知」、 そして「アクセス制御」
     2. バイデザイン／バイデフォルトでシステムおよびデータベースにセキュリティを組み込んでいくアプローチ
  5. 「暗号化、 アクセス制御が不十分」─アセスメントで見えた日本企業の課題
     1. 1つ目の視点はデータの暗号化と伏字化、
     2. 2つ目は職務分掌、
     3. 3つ目はデータの漏えい検知と証跡管理
  6. 「個人情報の保護に関する法律」（2005年4月施行,2017年5月改正施行）

1. 「企業における営業秘密管理に関する実態調査」報告書について【2017年3月17日IPA】

ドキュメントを参照: [ts\_kanri](https://www.ipa.go.jp/security/fy28/reports/ts_kanri/)

* 1. 調査報告書（PDF：1.7MB）

ドキュメントを参照: [000057774.pdf](https://www.ipa.go.jp/files/000057774.pdf)

* 1. 概要説明資料（PDF：1.42MB）

ドキュメントを参照: [000057775.pdf](https://www.ipa.go.jp/files/000057775.pdf)

* 1. 調査報告書-資料編（アンケート調査結果）（PDF：1.75MB）

ドキュメントを参照: [000057776.pdf](https://www.ipa.go.jp/files/000057776.pdf)

* 1. 調査報告書-資料編（判例調査結果）（PDF：867KB）

ドキュメントを参照: [000057777.pdf](https://www.ipa.go.jp/files/000057777.pdf)

1. 組織における内部不正防止ガイドライン（日本語版） 第4版ガイドライン【2017年1月31日IPA】

ドキュメントを参照: [insider](https://www.ipa.go.jp/security/fy24/reports/insider/)

* 1. 1.背景
  2. 2.概要
     1. 2-1.内部不正防止の基本原則
     2. 2-2.本ガイドラインの構成と活用方法
     3. 2-3.内部不正対策の体制構築の重要性
     4. 2-4.内部不正対策の体制
        1. 2-4-1.最高責任者
        2. 2-4-2.総括責任者
        3. 2-4-3.総括責任者の任命について
        4. 2-4-4.各部門／担当者の参画及び協力体制
  3. 3. 用語の定義と関連する法律
     1. 3-1.用語
     2. 3-2.関連する法律
  4. 4. 内部不正を防ぐための管理のあり方
     1. 4-1.基本方針（経営者の責任、 ガバナンス）
     2. 4-2.資産管理（秘密指定、 アクセス権指定、 アクセス管理等）
        1. 4-2-1.秘密指定
        2. 4-2-2.アクセス権指定
     3. 4-3.物理的管理
     4. 4-4.技術・運用管理
     5. 4-5.証拠確保
     6. 4-6.人的管理
     7. 4-7.コンプライアンス
     8. 4-8.職場環境
     9. 4-9.事後対策
     10. 4-10.組織の管理
  5. 付録Ⅰ：内部不正事例集
  6. 付録Ⅱ：内部不正チェックシート
  7. 付録Ⅲ：Q&A 集
  8. 付録Ⅳ：他ガイドライン等との関係
  9. 付録Ⅴ：基本方針の記述例
  10. 付録Ⅵ：内部不正防止の基本5原則と25分類
  11. 付録Ⅶ：対策の分類

1.  【てびき】情報管理も企業力～秘密情報の保護と活用～【2016年12月5日METI】

ドキュメントを参照: [trade-secret.html](http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html)

* 1. 秘密情報の保護ハンドブックの手引き
  2. １．こんなこと、 あるある!? 秘密情報にまつわるトラブル
     1. 大口の取引先から図面を見せてほしいと言われて提示したら・・・
     2. プロジェクトの開発リーダーだった従業員が退職を申し出てきたが、 転職先は競合他社で・・・
     3. 自社開発の技術にもかかわらず、 他社から「盗まれた!」と言われた。
     4. コラム：トラブルに巻き込まれないよう、 社内の秘密情報をうまく把握し、 活用させて企業力を高めていきましょう！
  3. ２．対策は身近なところから！企業を守るための漏えい対策３ステップ
     1. 保有する情報を洗い出します
     2. 秘密とする情報を決めましょう
     3. 情報に合わせた対策の選択と決定をしましょう
        1. 物理的・技術的な防御
           1. １．秘密情報に近寄りにくくするための対策

接近の制御

* + - * 1. ２．秘密情報の持ち出しを困難に「するための対策

持出し困難化

* + - 1. 心理的な抑止
         1. ３．漏えいが見つかりやすい環境づくりのための対策

視認性の確保

* + - * 1. ４．秘密情報だと思わなかった！という事態を招かないための対策

秘密情報に対する認識向上

* + - 1. 働きやすい環境の整備
         1. ５．社員のやる気を高め、 秘密情報を持ち出そうという考えを起こさせないための対策

信頼関係の維持・向上等

* 1. ３．実際にあった！？事例と対策とそのポイント
     1. 従業員向けの対策
     2. 従業員・退職者向けの対策
     3. 取引先向けの対策
     4. 外部者向けの対策
     5. 自社技術で商品をつくったのに、 他社の技術を使ったと言われた
     6. コラム：備えあれば憂いなし！自社の立場を守るためにできること
     7. コラム：他社の秘密情報を意図せず侵害しないために
     8. 転職者を受け入れて新製品を開発したら、 秘密情報の侵害だと訴えられた
  2. ４．万が一秘密情報が漏えいしてしまったら・・・
     1. 情報漏えいには兆候があります！
     2. 漏えいの疑いがあったらできるだけ早く適切な対応を取りましょう
     3. 被害回復のためにも日頃からの備えが大切です
     4. 情報漏えいしたら早めの相談を！
        1. 独立行政法人工業所有権情報・研修館（INPIT）
           1. 営業秘密・知財戦略ポータルサイト

ドキュメントを参照: [tradesecret](http://www.inpit.go.jp/katsuyo/tradesecret/)

* + - * 1. 相談窓口：03-3581-1101 ex.3844
        2. 全国47都道府県の知財総合支援窓口

ドキュメントを参照: [chizai-portal.jp](http://chizai-portal.jp/)

ナビダイヤル:0570-082100

* + - 1. 情報処理推進機構(IPA)
      2. 全国都道府県警察　営業秘密侵害事犯窓口
         1. 警視庁生活経済課

1.  企業経営のためのサイバーセキュリティの考え方の策定について【2016年8月2日NISC】

ドキュメントを参照: [09shiryou07.pdf](http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf)

* 1. http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf

ドキュメントを参照: [09shiryou07.pdf](http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf)

* 1. サイバーセキュリティ戦略本部

ドキュメントを参照: [index.html](http://www.nisc.go.jp/conference/cs/index.html)

* + 1. http://www.nisc.go.jp/conference/cs/index.html

ドキュメントを参照: [index.html](http://www.nisc.go.jp/conference/cs/index.html)

* 1. 経営層に期待される 認識 や経営戦略を企画する人材層に向けた実装のためのツールを示す
  2. 基本方針
     1. ーサイバーセキュリティは、 より積極的な経営への「投資」へー
     2. サイバーセキュリティをやむを得ない「費用」でなく、 積極的な経営への「投資」と位置づけ、 企業としての「挑戦」と、 それに付随する「責任」として取り組むことが期待される
  3. I.基本的考え方
     1. 二つの基本的認識
        1. ＜①挑戦＞
           1. 新しい製品やサービスを創造するための戦略の一環として考えていく
           2. サブトピック
        2. ＜②責任＞
           1. サイバーセキュリティに取り組むことは社会的な要求・要請であり、 自社のみならず社会全体の発展にも寄与する
     2. 三つの留意事項
        1. ＜①情報発信による社会的評価の向上＞
           1. 「セキュリティ品質」を高め、 品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。
           2. そのような取組に係る姿勢や方針を情報発信することが重要。
        2. ＜②リスクの一項目としてのサイバーセキュリティ＞
           1. 提供する機能やサービスを全うする（機能保証）という観点から、 リスクの一項目としてのサイバーセキュリティの視点も踏まえ、 リスクを分析し、 総合的に判断。
           2. 経営層のリーダーシップが必要。
        3. ＜③サプライチェーン全体でのサイバーセキュリティの確保＞
           1. サプライチェーンの一部の対策が不十分な場合でも、 自社の重要情報が流出するおそれあり。
           2. 一企業のみでの対策には限界があるため、 関係者間での情報共有活動への参加等が必要。
  4. II.企業の視点別の取組
     1. ITの利活用やサイバーセキュリティへの取組において、 各企業の事業規模のみならず、 その認識の違いなどを踏まえて取り組んでいく必要がある
     2. ITの利活用を事業戦略上に位置づけ、 サイバーセキュリティを強く意識し、 積極的に競争力強化に活用しようとしている企業
        1. （積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）
        2. 【経営者に期待される認識】
           1. 積極的なITの利活用を推進する中で、 製品やサービスの「セキュリティ品質」を一層高め、 自社のブランド価値の向上につなげるべく、 システムの基盤におけるセキュリティの向上、 情報・データの保護、 製品等の安全品質向上に取り組む。
           2. 様々な関係者との協働が重要であるため、 情報提供に主体的に取り組む。
           3. 決して現存する標準や取り組みなどに満足することなく、 実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、 変革していく存在となることが期待される。
        3. 【実装に向けたツール】
           1. IoTセキュリティに関するガイドライン（「IoTセキュリティのための一般的枠組」等）
           2. 自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信
     3. IT・セキュリティをビジネスの基盤として捉えている企業
        1. （IT・サイバーセキュリティの重要性は理解しているものの、 積極的な事業戦略に組み込むところまでは位置づけていない企業）
        2. 【経営者に期待される認識】
           1. 経営者のリーダーシップによって、 社会的責任としてのサイバーセキュリティ対策に取り組む。
           2. サプライチェーンやビジネスパートナー、 委託先を含めた対策を行う。
           3. 平時・緊急時のいずれにおいても、 情報開示などの適切なコミュニケーションを行う。
        3. 【実装に向けたツール】
           1. サイバーセキュリティ経営ガイドライン
           2. 企業等がセキュリティ対策に取り組む上での保険等のリスク管理手法の活用
           3. サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信
     4.  自らセキュリティ対策を行う上で、 事業上のリソースの制約が大きい企業
        1. （主に中小企業等でセキュリティの専門組織を保持することが困難な企業）
        2. 【経営者に期待される認識】
           1. サプライチェーンを通じて中小企業等の役割はますます重要となる中、 消費者や取引先との信頼関係醸成の観点から経営者自らサイバーセキュリティ対策に関心を持ち、 取り組む。
           2. 外部の能力や知見を活用しつつ、 効率的に進める方策を検討する。
        3. 【実装に向けたツール】
           1. 効率的なセキュリティ対策のためのサービスの利用（中小企業向けクラウドサービス等）
           2.  サイバーセキュリティに関する相談窓口やセミナー、 地域の相談員等の活用

1.  企業（組織）における最低限の情報セキュリティ対策のしおり+1【2015年8月21日 2017年6月30日IPA】【第5版】

ドキュメントを参照: [01\_guidebook.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf)

* 1. 参照
     1. 中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】

ドキュメントを参照: [000055520.pdf](http://www.ipa.go.jp/files/000055520.pdf)

* + 1. 中小企業の情報セキュリティ対策ガイドライン https://www.ipa.go.jp/security/keihatsu/sme/guideline/

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

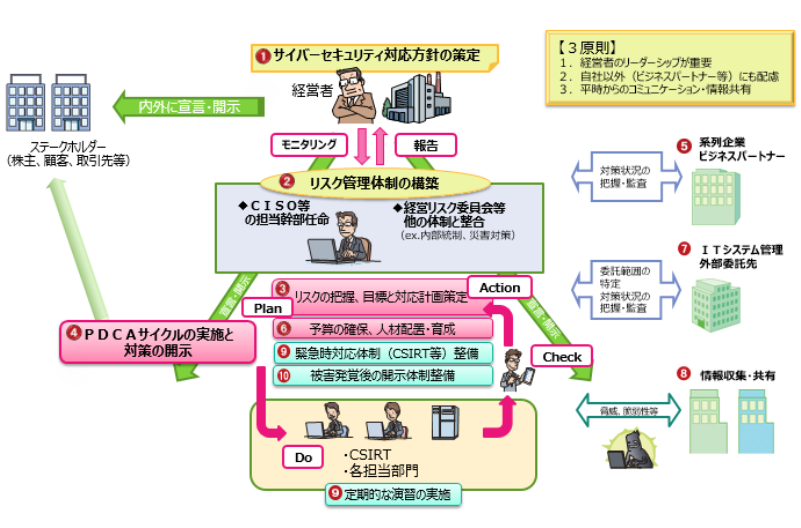
* + 1. 情報セキュリティ対策ベンチマーク https://www.ipa.go.jp/security/benchmark/

ドキュメントを参照: [benchmark](https://www.ipa.go.jp/security/benchmark/)

* 1. 構成
     1. 5分でできる！情報セキュリティ自社診断（付録2）は、 25の設問に答えるだけで自社のセキュリティレベルを把握することができる自社診断シートと、 その解説パンフレットに加え、 情報セキュリティ対策を従業員に会社のルールとして周知する時に活用できる情報セキュリティハンドブックのな形で構成しています。
     2. 組織として最初に取り組むべき情報セキュリティ対策の自社診断シート　基本的対策、 従業員としての対策、 組織としての対策、 全25項目
  2. Part1 基本的対策
     1. №1 パソコン等の脆弱性対策
        1. 1.Windows Update※1 を行うなどのように、 常にOS やソフトウェアを安全な状態にしていますか？
     2. №2 パソコン等のウイルス対策
        1. 2.パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル※2 を自動更新するなどのように、 パソコンをウイルスから守るための対策を行っていますか？
     3. №3 パソコン等のパスワード管理
        1. 3,パスワードは自分の名前、 電話番号、 誕生日など推測されやすいものを避けて複数のウェブサイトで使いまわしをしないなどのように、 強固なパスワードを設定していますか？
     4. №4 重要情報へのアクセス(権)管理
        1. 4.ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、 重要情報に対する適切なアクセス制限を行っていますか？
     5. №5 脅威情報等の情報共有
        1. 5.利用中のウェブサービス※3 や製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
  3. Part2 従業員としての対策
     1. №6 標的型攻撃メール対策等
        1. 6.受信した不審な電子メールの添付ファイルを安易に開いたり本文中のリンクを安易に参照したりしないようにするなど、 電子メールを介したウイルス感染に気をつけていますか？
     2. №7 電子メールの誤送信防止
        1. 7.電子メールを送る前に目視にて送信アドレスを確認するなどのように、 宛先の送信ミスを防ぐ仕組みを徹底していますか？
     3. №8 電子メールでの重要情報漏えい対策
        1. 8.重要情報をメールで送る時は重要情報を添付ファイルに書いてパスワード保護するなどのように、 重要情報の保護をしていますか？
     4. №9 無線LANのセキュリティ対策
        1. 9.無線LAN を利用する時は強固な暗号化を必ず利用するなどのように、 無線LAN を安全に使うための対策をしていますか？
     5. №10 インターネットを介したトラブル防止
        1. 10.業務端末でのウェブサイトの閲覧やSNS への書き込みに関するルールを決めておくなどのように、 インターネットを介したトラブルへの対策をしていますか？
     6. №11 重要情報のバックアップ等の保全対策
        1. 11.重要情報のバックアップを定期的に行うなどのように、 故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？
     7. №12 重要情報の事務所等での管理
        1. 12.重要情報を机の上に放置せず書庫に保管し施錠するなどのように、 重要情報の紛失や漏えいを防止していますか？
     8. №13 重要情報の持ち出し等の管理
        1. 13.重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、 盗難や紛失の対策をしていますか？
     9. №14 パソコン等の第三者利用制限
        1. 14.離席時にコンピュータのロック機能を利用するなどのように、 他人に使われないようにしていますか？
     10. №15 事務所等への不正侵入対策
         1. 15.事務所で見知らぬ人を見かけたら声をかけるなどのように、 無許可の人の立ち入りがないようにしていますか？
     11. №16 事務所等での重要機器の管理
         1. 16.退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、 盗難防止対策をしていますか？
     12. №17 事務所等での入退出管理
         1. 17.最終退出者は事務所を施錠し退出の記録（日時、 退出者）を残すなどのように、 事務所の施錠を管理していますか？
     13. №18 不要になった重要情報の廃棄管理
         1. 18.重要情報を廃棄する場合は、 書類は細断したり、 データは消去ツールを使ったりするなどのように、 重要情報が読めなくなるような処分をしていますか？
  4.  　　Part3 組織としての対策【要確認】
     1. №19 守秘義務等の従業員への徹底
        1. 19.採用の際に守秘義務や罰則規定があることを知らせるなどのように、 従業員に秘密を守らせていますか？
     2. №20 従業員へのセキュリティ意識付け
        1. 20.情報管理の大切さなどを定期的に説明するなどのように、 従業員に意識付けを行っていますか？
     3. №21 BYOD対応のセキュリティ対策
        1. 21.社内外での個人所有のパソコンやスマートフォンの業務利用を許可制にするなどのように、 業務で個人所有端末の利用の可否を明確にしていますか？
     4. №22 取引先とのセキュリティ協議
        1. 22.契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、 取引先に秘密を守ることを求めていますか？
     5. №23 外部サービスのセキュリティ対策
        1. 23.クラウドサービスなど外部サービスを利用する時は利用規約やセキュリティ対策を確認するなどのように、 サービスの安全・信頼性を把握して選定していますか？
     6. №24 BCPを踏まえたセキュリティ事故対策
        1. 24.秘密情報の漏えいや紛失、 盗難があった場合の対応手順書を作成するなどのように、 事故が発生した場合に備えた準備をしていますか？
     7. №25 セキュリティルールの策定と運用
        1. 25.情報セキュリティ対策（上記1～24 など）を会社のルールにするなどのように、 情報セキュリティ対策の内容を明確にしていますか？
  5. さらなる情報セキュリティ対策の検討するには
     1. 「5 分でできる！情報セキュリティ自社診断」の次のステップとして、 ガイドラインを活用したポリシーの策定やベンチマークでの自己診断を実施してみよう。

1.  サイバーセキュリティ経営ガイドライン解説書Ver.1.0【2016年12月IPA】

ドキュメントを参照: [csmgl-kaisetsusho.html](https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html)

* 1. 0. はじめに
     1. 本解説書の想定読者
     2. 本解説書の構成
     3. サイバーセキュリティ経営の原則
     4. 経営者が決定すべき事項
     5. 経営者が責務を果たしているかどうかの問い
     6. 解説の記述方法
  2. 1．サイバーセキュリティ対応方針の策定
     1. セキュリティポリシーの策定
        1. セキュリティポリシーの主な検討項目
     2. セキュリティポリシーの周知
        1. 組織内への周知の重要性
        2. 組織外への公開の重要性
        3. セキュリティポリシー群の種類
        4. セキュリティポリシーの公開
        5. 企業例示について
        6. 企業例示「セキュリティポリシーの策定」
  3. 2．リスク管理体制の構築
     1. サイバーセキュリティリスク管理体制
        1. サイバーセキュリティリスク管理体制の構築方法
        2. サイバーセキュリティリスク管理体制の構築の必要性と経営者の責任
     2. CISO 等に求められること
        1. CISO 等の役割
     3. 既存のリスク管理体制との関係
        1. 既存の管理体制との整合
        2. 既存のリスク管理体制との関係性の明確化
        3. 企業例示「管理体制の構築検討」
  4. 3．リスクの把握、 目標と対応計画策定
     1. 資産の特定
        1. 守るべき資産の特定
        2. 法令等による要求事項の明確化
        3. 情報のライフサイクルに着目した資産のリスト化
        4. ネットワーク上の守るべき資産の特定
     2. サイバー攻撃の脅威を識別
     3. リスクの把握
        1. 適切なリスク分析の重要性
        2. リスク分析手法の種類について
        3. 事業継続を踏まえたビジネスインパクト分析
     4. リスク対応計画の策定
        1. リスク対応方法の検討
        2. リスクに応じた対策の目標と対応計画の策定
        3. 企業例示「リスク対応の検討」
  5. 4．PDCAサイクルの実施と対策の開示
     1. 環境変化に応じたフレームワーク（PDCA）の構築
        1. フレームワーク（PDCA）の構築
        2. フレームワーク（PDCA）のサイクル
        3. 計画見直し方法の検討
     2. 対策状況の把握
        1. 対策状況の把握方法
        2. 経営者への報告内容
        3. KPI の設定・モニタリング
        4. 経営層による評価
        5. 内部監査と外部監査
     3. 対策状況の開示
        1. 企業例示「PDCA の検討」
  6. 5．系列企業・ビジネスパートナーの対策実施及び状況把握
     1. 系列企業・ビジネスパートナーを含めた対策の実施
        1. ビジネスパートナー等との対策実施・連携の検討
     2. ビジネスパートナーの対策状況の把握
        1. ビジネスパートナーの対策状況を把握する方法
        2. より効果的に対策状況を確認する方法
        3. 企業例示「関係者の対応状況把握
  7. 6．予算確保・人材配置及び育成
     1. 必要な対策費用の確保
        1. 対策費用の承認を得るためのポイント
        2. 経営者が判断できる材料とは
     2. 必要な人材の確保・育成
        1. 必要な人材と育成
        2. セキュリティ担当者の育成
        3. 一般従業員の研修
        4. 積極的な外部リソースの活用
        5. 企業例示「資源の確保」
  8. 7．ITシステム管理の外部委託
     1. 自組織による対応と外部委託による対応
        1. 外部委託する範囲を選択するポイント
     2. 委託先のサイバーセキュリティの確保
        1. 委託先への依頼方法
        2. 連携体制の整備・構築
        3. 外部委託先としてクラウドサービス事業者を選定する際のポイント
        4. 企業例示「IT システム管理の外部委託先への対応」
  9. 8．情報収集と情報共有
     1. 情報収集と自社での有効活用
        1. 情報収集の重要性
        2. 情報を常に最新の状態に保つ
        3. 収集した情報を活用するための環境整備
     2. 情報共有・情報提供
        1. 情報共有・提供の重要性
        2. 社会全体での対策向上
        3. 企業例示「情報収集及び情報共有の検討」
  10. 9．緊急時対応体制の整備と演習の実施
      1. CSIRT の構築
         1. CSIRT の構築方法
         2. CSIRT の設計で検討すべき事項
         3. 危機管理に求められる機能
      2. 緊急連絡先・初動対応マニュアルの整備
         1. 緊急時の初動対応フローの整備（マニュアルの策定）
         2. 報告体制・エスカレーション基準
         3. 社外を含めた緊急連絡先
         4. 初動対応事項・復旧事項
         5. 事後対応事項
      3. 定期的・実践的な演習の実施
         1. 初動対応マニュアルの有効性の検証
         2. 社内組織（部門）間のコミュニケーション、 共同作業の有効性の検証
         3. CSIRT 要員のスキル・量の十分性の確認
         4. セキュリティ技術対策の効率性・十分性の確認
         5. 訓練・演習の考え方
         6. 定期的な訓練実施
         7. 企業例示「緊急時の対策検討」
  11. 10．被害発覚後の必要な情報の把握、 開示体制の整備
      1. 被害発覚後の情報収集体制および開示すべき項目の整備
         1. 開示・報告すべき情報の把握
         2. 通知先のリスト化と通知用のフォーマット作成
         3. 通知に必要な情報の整理と周知
         4. 組織の内外への開示・報告内容、 タイミング
         5. 開示・報告先について留意すべき点
      2. 組織内外へ経営者が説明できる体制の整備
         1. 経営者への報告ルートや報告ルールの整備
         2. 企業例示「被害発覚時の準備」
  12. 付録1：ガイドラインの3原則と重要10項目の概要図
  13. 付録2：参照情報
  14. 付録3：サイバーセキュリティ経営チェックシートの実施の目安と確認事項
  15. 別添 ：サイバーセキュリティ対策に関連する被害事例
  16. ＜付録1ガイドラインの3原則と重要10項目の概要図＞
      1. サブトピック  
         

1. サイバーセキュリティ経営ガイドライン解説書Ver.1.0別添：被害事例集【2016年12月IPA】

ドキュメントを参照: [000056149.xlsx](https://www.ipa.go.jp/files/000056149.xlsx)

1.  企業経営のためのサイバーセキュリティの考え方の策定について【2016年8月2日NISC】
2. 情報セキュリティポリシーサンプル改版（1.0版）【2016年3月29日JNSA】

ドキュメントを参照: [policy](http://www.jnsa.org/result/2016/policy/)

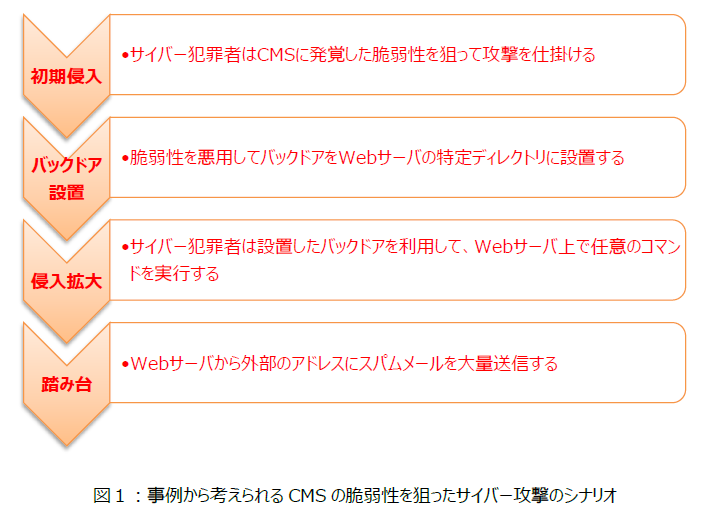
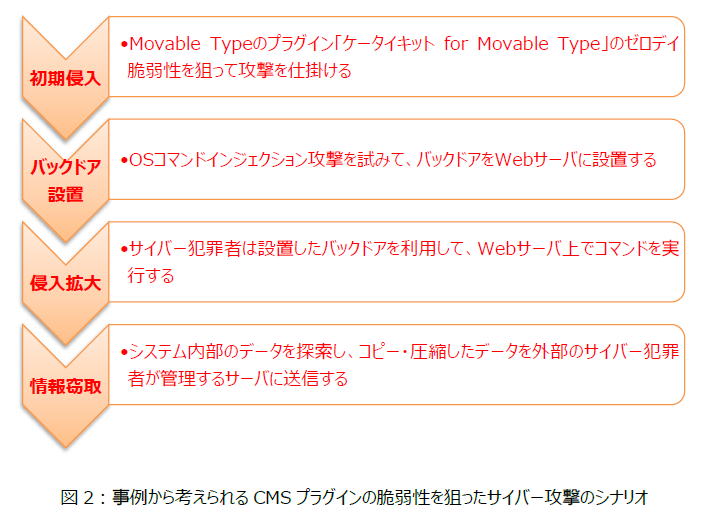
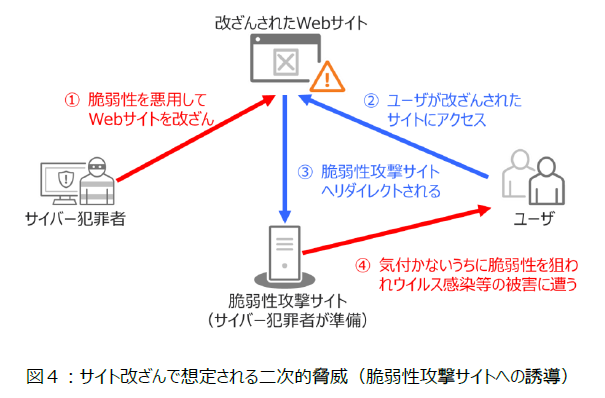
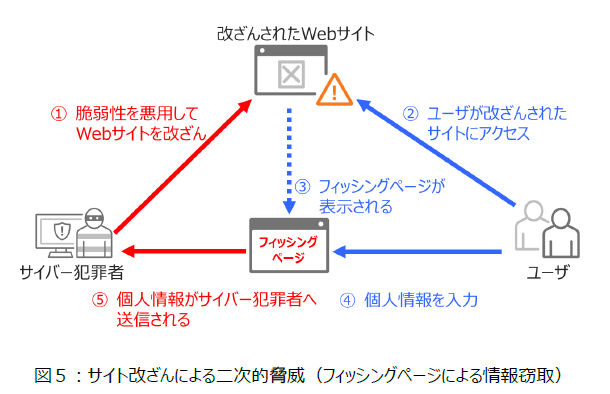
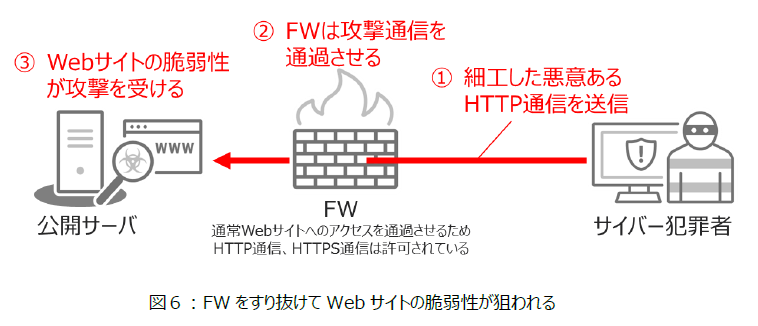
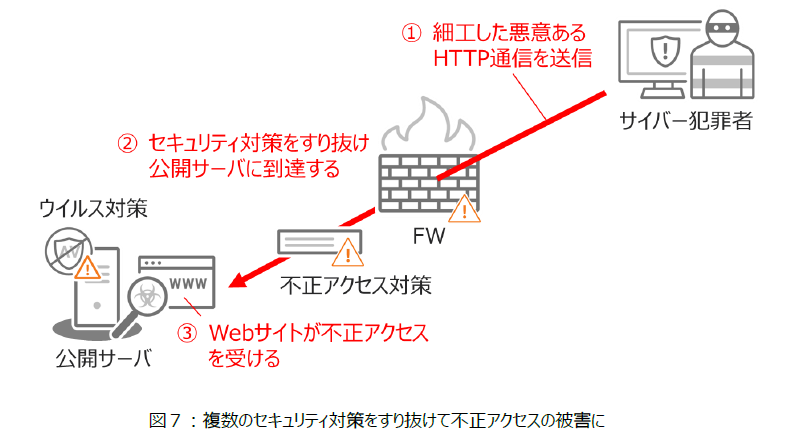
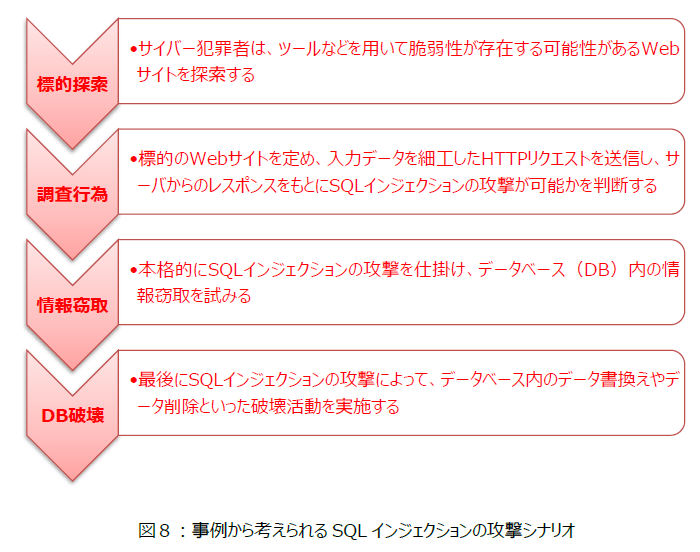
1. すぐ役立つ！法人で行うべきインシデント初動対応 ~「不審な通信」その時どうする~【2016年11月1日トレンドマイクロ】

ドキュメントを参照: [20161031014833.html](http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20161031014833.html)

* 1. 1 はじめに インシデント対応の実情
  2. 2 「インシデント発生」を把握し対応開始を判断する
     1. 2.1 インシデントの発生に気づくために
     2. 2.2 インシデント対応を判断するために
     3. 2.3 まとめ インシデントの把握と対応判断のポイント
  3. 3 「不審な通信」、 その時に行うべきインシデント対応
     1. 3.1 インシデント対応の考え方
     2. 3.2 「影響範囲の確認」のために必要な対応
     3. 3.3 「脅威の封じ込め/根絶」のために必要な対応
     4. 3.4 被疑端末への対応
     5. 3.5 まとめ 具体的なインシデント対応のポイント
  4. 4 「適切な対応」を迅速に行うために
     1. 4.1 インシデント発生を把握し対応開始を判断するための事前準備
     2. 4.2 インシデント対応を適切かつ迅速に行うための事前準備
  5. 5 まとめ

1. 2016年インシデント事例から学ぶ「Webサイトのセキュリティ対策」【トレンドマイクロ】

ドキュメントを参照: [select.asp](https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=233)

* 1. はじめに . 3
  2. 攻撃パターン①：コンテンツ管理システムまたはそのプラグインの脆弱性が狙われた . 3
     1. 事例①：地域情報サイトが攻撃を受け、 約60 万件のスパムメールを送信 3
        1. サブトピック  
           
     2. 事例②：大手放送局等がCMS プラグインの脆弱性を狙われ、 大量の個人情報が漏えい . 4
        1. サブトピック  
           
     3. インシデント事例から学ぶべきポイント 5
  3. 攻撃パターン②：不正サイトに誘導するコードやフィッシングページが設置された 6
     1. 事例①：サイトの一部が改ざん、 ユーザを不正サイトへ誘導 6
        1. サブトピック  
           
     2. 事例②：不正アクセスを受け、 自社のWeb サイトがフィッシングページを表示 . 7
        1. サブトピック  
           
     3. インシデント事例から学ぶべきポイント 8
  4. 攻撃パターン③：ベーシックな対策だけのサイトへの攻撃 9
     1. 事例①：ファイアウォール導入や脆弱性診断を実施していた企業が、 Web サイトからの情報漏えい被害に 9
        1. サブトピック  
           
     2. 事例②：不正アクセス対策をすり抜ける攻撃により顧客情報の一部が漏えい . 10
        1. サブトピック  
           
     3. インシデント事例から学ぶべきポイント 10
  5. 攻撃パターン④：Web アプリケーションの脆弱性を狙ったインジェクション攻撃 . 11
     1. 事例①：SQL インジェクションの攻撃によって、 個人情報の一部が漏えい . 11
        1. サブトピック  
           
     2. 事例②：Web アプリケーションの脆弱性を悪用したバックドアの設置 . 12
        1. サブトピック  
           
     3. インシデント事例から学ぶべきポイント 13
  6. 2016 年インシデント事例から学ぶべきポイントとサーバ対策 . 14
  7. トレンドマイクロ製品による総合サーバセキュリティ対策 15

1. スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書【2015年 5月21日NISC】

ドキュメントを参照: [02shiryou0305.pdf](http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf)

* 1. 1．総則
     1. 1.1 本書の目的・位置付け
     2. 1.2 本書が対象とする者
     3. 1.3 本書の使い方
     4. 1.4 用語の定義
  2. 2．スマートフォン等の特性と業務利用におけるリスク
     1. 2.1 スマートフォン等の特性
     2. 2.2 スマートフォン等の特性及び業務利用における脅威
        1. 表２－１ スマートフォン等の業務利用における脅威と対策の例
  3. 3．スマートフォン等の業務利用の形態
     1. 3.1 端末の配備
     2. 3.2 利用する場所
     3. 3.3 私物端末の利用
     4. 3.4 情報システムの利用形態
  4. 4．目的及び適用範囲の明確化
     1. 4.1 目的の明確化
     2. 4.2 対象とする業務
     3. 4.3 利用者
  5. 5．業務・サービスの利用要件の策定
     1. 5.1 端末やOSの種類
     2. 5.2 端末機能・サービスの要件
        1. 表５－１ 端末機能・サービスの利用要件及び利用制限の例
     3. 5.3 業務用アプリの導入
     4. 5.4 通信ネットワークの要件
     5. 5.5 情報セキュリティ対策要件
        1. (1) ソフトウェアの脆弱性対策
        2. (2) 不正プログラム対策
        3. (3) のぞき見防止対策
        4. (4) 盗難・紛失対策
        5. (5) ログ管理機能
        6. (6) 端末管理ツール（MDM：Mobile Device Management）の導入
        7. 表５－２ MDMの主な機能
           1. 端末ロックの遠隔制御

端末個体ごとに、 遠隔制御でロック、 アンロックを実施

* + - * 1. リモートデータワイプ

端末内全データ削除、 個別データ/特定フォルダ削除、 業務領域のみ削除 等

* + - * 1. 暗号化

外部メモリ出力時のデータ暗号化/復号、 個別データの暗号化/復号

* + - * 1. 端末機能制御

カメラ、 スクリーンショット、 近距離無線通信、 外部メモリ出力等の機能制限

* + - * 1. 端末状態監視

端末状態の取得（OS、 アプリ、 改造の有無、 起動中アプリ 等）

死活監視、 ログ収集、 位置情報取得、 アラートメールの送信、 管理者向け統計処理

* + - * 1. ポリシー設定及び実行

パスワードポリシー設定、 MDMポリシー（リモートデータワイプの条件、 機能制限 等）設定

メーラーや無線LAN接続、 証明書等の端末構成の設定変更 等

* + - * 1. 資産管理

端末所有者の属性管理や端末個体情報(機種、 電話番号 等）の管理 等

* + - * 1. アプリ配信及び削除

業務用アプリの配信と自動インストール、 遠隔削除

* + - * 1. アプリ利用制限

非公認アプリのインストール制限や強制終了、 アプリのアクセス許可制御

外部媒体経由のアプリインストール制御 等

* + - * 1. MDMサーバ接続

SSL・VPNによる通信路暗号化、 GCM等によるエージェント・MDMサーバ間通信路の維持 等

* + - * 1. フィルタリング機能

ウェブフィルタ、 メールフィルタ等の設定情報管理やアクセスログの収集

* + - * 1. 不正プログラム対策ソフトウェアの管理
        2. 不正プログラム対策ソフトウェアのバージョンやパターンファイルの管理、 最新版への更新、 スキャンログの収集、 スキャン実行の要求 等
        3. バックアップ

端末データのバックアップやリスア

* + 1. 5.6 私物端末の業務利用に際して留意すべき事項
       1. 表５－３ 私物端末の業務利用する際に留意すべき事項と要件策定例
          1. 業務情報と私的な情報の混在の回避

 端末内の私的な情報と業務情報を混在させないよう、 これらを明確に分けるための仕組みを導入する

 業務用アプリ導入又は端末に業務情報を保存させない仕組みを導入する

* + - * 1. 家族や友人への貸与の禁止

 私的な利用においても家族や友人が利用することを禁止することを合意した者のみに私物端末の利用を認める

外出先等での端末の盗難・紛失

 業務利用する際の利用場所を限定する

 私的利用時を含めて端末ロックやデータワイプ機能の設定を必須し、 対策の実施について合意した者のみに私物端末の利用を認める

* + - * 1. 利用するネットワークの制限

 私的な利用時であっても安全性の確認できないサイトや通信ネットワークへの接続を禁止するなどの利用手順を策定し、 合意した者のみに私物端末の利用を認める

* + - * 1. ソフトウェア更新や不正プログラム対策の実施

 ソフトウェア更新や不正プログラム対策ソフトウェアの実行を義務付け、 合意したのみに私物端末の利用を認める（OSの更新により業務用アプリが正常動作しなくなる可能性について留意が必要）

* + - * 1. 業務用アプリのインストール

 業務用アプリのインストール可能な端末を所有していて、 かつインストールに合意した者のみに私物端末の利用を認める

* + - * 1. 点検内容の明確化

 業務用アプリ、 MDMやMAMにより点検を自動化する

 あらかじめ点検内容を明確化し、 合意した者のみに私物端末の利用を認める

* 1. 6．実施手順の整備
     1. 6.1 責任者の設置と運用管理体制の整備
     2. 6.2 利用手順の整備
        1. 表６－１ 利用者が遵守すべき端末の利用手順に関する注意事項の例
           1. 利用の原則

行政事務の遂行以外の目的で端末を利用しないこと

不要不急な業務においては極力利用しないこと

不要な情報は端末に残留させず、 速やかに消去すること

他の手段が無い場合に限り利用すること

* + - * 1. 利用手順の遵守

利用手順を遵守すること

定められた手順以外の方法で業務を行わないこと

手順外の処理を行う必要が生じた場合は、 事前に責任者の許可又は承認を得ること

利用を終了した場合は、 速やかに手続すること

利用中にインシデント等が発生した場合は、 手順に従って管理者等へ速やかに連絡し、 必要な措置を講ずること

* + - * 1. 端末管理の徹底

盗難・紛失が起こらないように、 日常的に端末の管理を厳重に行うこと

家族や知人、 第三者が端末操作や画面をのぞき見する行為に注意すること

* + - * 1. 禁止事項

管理責任者の許可なく、 端末の設定を変更しないこと

安全性が確認できないアプリケーションや利用が禁止されているソフトウェアをインストールしないこと

許可された通信回線以外に接続しないこと

PCに接続しないこと（充電等の場合であってもNG）

端末は家族や知人、 第三者に端末を貸与しないこと

* + 1. 6.3 運用管理手順の整備

1. なりすましECサイト対策マニュアル【2015年3月一般社団法人セーファーインターネット協会】

ドキュメントを参照: [narisumashi\_manual.pdf](https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf)

* 1. 1. はじめに
     1. EC サイト運営者の方向け
  2. 2. なりすましEC サイトとは
     1. 実在するサイトの外観（屋号、 商標、 サイト意匠・構成、 使用している画像等）を模倣することにより、 あたかも当該サイトである又は当該サイトと関係のあるサイトであるかのように消費者を誤認させ、 商品代金をだましとったり、 模倣品、 海賊版その他購入しようとした品と全く別個の物を送りつけるサイト
  3. 3. なりすましEC サイトの特徴
     1. 日本語が不自然
     2. 振込先が個人名（外国人の場合が多い）
     3. 支払い方法が銀行振込のみとなっている
     4. 問い合せ先のメールアドレスがフリーメールアドレス
     5. 「特定商取引に関する表示」が曖昧（店舗名・住所・電話番号・メール の表示が欠けている）
     6. 価格が極端に安い
     7. フォームの崩れやリンク切れなど、 Web サイトの作り方に粗雑な点が見られる
     8. 有名ブランド名＋激安 などの表示がある
  4. 4. 被害実態（アンケート結果）
     1. 4.1. 被害実態
     2. 4.2. 対策状況
  5. 5. 当事者たちの責任関係
  6. 6. 対処法、 予防法
     1. 6.1. 対処法
        1. 6.1.1. 問い合わせ対応
           1. 問い合わせ対応文－なりすましEC サイト対策協議会

ドキュメントを参照: [template002.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template002.docx)

* + - 1. 6.1.2. 削除要請
         1. 削除依頼文－なりすましEC サイト対策協議会

ドキュメントを参照: [template003.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template003.docx)

* + - 1. 6.1.3. 都道府県警察サイバー犯罪相談窓口への連絡
         1. 都道府県警察本部のサイバー犯罪相談窓口等一覧

ドキュメントを参照: [soudan.htm](http://www.npa.go.jp/cyber/soudan.htm)

* + 1. 6.2. 予防法
       1. 6.2.1. 注意喚起
          1. サイト掲示用注意喚起文－なりすましEC サイト対策協議会

ドキュメントを参照: [template001.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template001.docx)

* + - 1. 6.2.2. 被害に遭っているかの確認
         1. 自身が運営するEC サイトの店舗名を検索サイトで検索し、 自身が運営する以外のドメインでEC サイトが存在するかをチェックする
         2. 自身が運営するEC サイトの店舗名やサービス名等を検索サイトのアラートサービスに登録し、 自身が運営する以外のドメインでEC サイトが存在するかをチェックする
         3. 自身が運営するEC サイトで掲載している画像を検索サイトで画像検索し、 同じ画像を掲載しているEC サイトが存在するかをチェックする
         4. 自身が運営するEC サイトに掲載している文章を検索サイトで検索し、 文章を盗用したEC サイトが存在するかをチェックする
      2. 6.2.3. 商標権の取得等
      3. 6.2.4. 電子証明書（SSL サーバ証明書）
         1. シマンテック 技術者でなくても分かる 電子証明書とPKI 入門

ドキュメントを参照: [page.jsp](http://www.symantec.com/ja/jp/page.jsp?id=pki-basics)

* + - * 1. GMO グローバルサインSSL とは？

ドキュメントを参照: [knowledge](https://jp.globalsign.com/service/ssl/knowledge/)

* + - 1. 6.2.5. ウェブサイトや運営者情報の登録
         1. 公益社団法人日本通信販売協会 オンラインマーク制度

ドキュメントを参照: [ost](http://www.jadma.org/ost/)

* + - * 1. 株式会社TradeSafe TradeSafe トラストマーク

ドキュメントを参照: [www.tradesafe.co.jp](http://www.tradesafe.co.jp/)

* + - * 1. JIPDEC(一般財団法人日本情報経済社会推進協会) ROBINS シール

ドキュメントを参照: [robinsseal](http://robins-cbr.jipdec.or.jp/usecase/robinsseal/)

* + - 1. 6.2.6. その他
         1. シマンテック セキュアメール ID

ドキュメントを参照: [secure-mail-id](http://www.symantec.com/ja/jp/secure-mail-id/)

* + - * 1. GMO グローバルサイン S/MIME とは

ドキュメントを参照: [smime](https://jp.globalsign.com/service/clientcert/knowledge/smime/)

* + - * 1. JIPDEC(一般財団法人日本情報経済社会推進協会) S/MIME とは

ドキュメントを参照: [smime](http://jcan.jipdec.or.jp/smime/)

* + - * 1. dkim.jp dkim とは

ドキュメントを参照: [about-dkim](http://www.dkim.jp/dkim-jp/about-dkim/)

* + - * 1. JIPDEC(一般財団法人日本情報経済社会推進協会) 安心マーク

ドキュメントを参照: [anshinmark](http://robins-cbr.jipdec.or.jp/usecase/anshinmark/)

* 1. 7. おわりに
  2. 8. 関係関連団体・政府機関紹介

1. Sec01-02-10 ウェブサイト開設等における運営形態の選定方法に関する手引き

ドキュメントを参照: [Sec01-02-10](https://bluemoon55.github.io/Sharing_Knowledge/Cyber_Security/Deliverables/mind2html/Sec01-02-10)

* 1. 改版履歴
     1. 2018年12月25日　独立文書化
     2. 【2018年5月IPA】
  2. はじめに （Executive Summary
  3. 対象読者と活用範囲
     1. ウェブサイトの運営者を主な対象読者としている。 ウェブサイトの運営にあたっては、 経営者、 企画者、 開発者、 運用管理者等がそれぞれの立場で関与することになる。
     2. 自組織でウェブサイトを構築する際に組織の内情や実施可能なセキュリティ対策、 セキュリティインシデント発生時の対応可能範囲等をもとに運営形態を選定する他、 ウェブサイトの構築を外部委託するケースでは、 運営形態に応じて必要となるセキュリティ対策項目の選定と発注要件の決定に活用して頂くことも想定している。
  4. ウェブサイト運営のライフサイクル
     1. 1.企画
     2. 2.設計
     3. 3.実装/構築
     4. 4.テスト
     5. 5.運用/利用
     6. 6.廃棄
  5. ウェブサイト運営形態の選定の重要性
  6. 各章節の想定読者
     1. 経営者：ウェブサイトの運営方針や、 組織としてのセキュリティの全体的な方針を決定する者を指す。
     2. ウェブサイト企画者：ウェブサイトで提供するコンテンツや、 サービス,具体的なセキュリティ方針を企画・決定する立場の者を指す。
     3. ウェブサイト開発者：ウェブサーバの構築や、 ウェブアプリケーションの開発、 方針に従ったセキュリティ対策の実装に携わる者を指す。
     4. ウェブサイト管理者：構築されたウェブサイトを保守・運用管理する立場の者を指す。
  7. 1. ウェブサイトの運営形態について
     1. 表1-1 運営形態の分類と説明
        1. モール
        2. ASP SaaS 型クラウドサービス
        3. PaaS 型クラウドサービス レンタルサーバ
        4. IaaS 型クラウドサービス
        5. ハウジング
        6. オンプレミス
     2. 1.1. 様々な運営形態が登場した背景
     3. 1.2. 各運営形態の特徴
        1. 運営形態を検討、 選定する上で、 選定を判断する観点や指標
           1. ①機能：計画しているウェブサイトの機能を満たせるか、 機能の自由度はどれだけあるか
           2. ②期間：開設までに要する期間（工数）、 サービスインの計画との整合性
           3. ③調達：運営するために調達が必要となる物理環境、 機材、 ソフトウェア等
           4. ④体制：開設、 運営していくのに必要となる人的資源、 体制
           5. ⑤費用：開設での一次費用、 運用における経年費用、 トータル費用等
           6. ⑥セキュリティ：安全な運用を維持するために対応すべきセキュリティ対策
        2. 表1-2-1 運営形態毎の選定項目の比較
           1. ①ウェブサイトの機能の自由度
           2. ②ウェブサイト開設までの日数
           3. ③ウェブサイト開設のため調達が必要な物品数
           4. ④ウェブサイト開設・運営に必要な人的資源
           5. ⑤-1ウェブサイト開設に必要な費用
           6. ⑤-2ウェブサイトの維持・運営に必要な費用
           7. ⑥検討が必要なセキュリティ対策項目
        3. 1.2.1 モール、 ASP、 SaaS 型クラウドサービスの特徴
           1. 表1-2-2 モール、 ASP、 SaaS でのメリットとデメリット
        4. 1.2.2 PaaS 型クラウドサービス、 レンタルサーバ、 IaaS 型クラウドサービスの特徴
           1. 表1-2-3 PaaS、 レンタルサーバ、 IaaS でのメリットとデメリット
        5. 1.2.3 ハウジング、 オンプレミスの特徴
           1. 表1-2-4 ハウジング、 オンプレミスでのメリットとデメリット
        6. 1.2.4 業種による利用傾向
           1. ウェブサイトで公開されている各運営形態の情報27を参照すると、
           2. ASP やモールの運営形態を選ぶ場合は、

ウェブサイト運営サービスに付加される別のサービスを利用できることが選定の理由として挙げられていた。 サーバの構築や運営の技術を持たない個人商店や中小企業等の利用が多くみられ、 そういった企業がEC サイトを出店する際に、 サポートサービスのEC サイト経営の相談サービス等が提供されていることを選定の基準にしているとのコメントが見られた。

* + - * 1. レンタルサーバやクラウドの場合は、

ASP やモールと異なり独自のドメインを取得するサービスが提供されており、 企業紹介のウェブサイトを導入する際に利用されているようである。 選定の理由として挙げられているのは導入するサービスや使用するソフトウェアを自由に選択できる点である28。 機材管理の工数が必要ないこと、 サービスの提供開始までに要する時間が短いこと、 特にクラウドの場合は処理性能等のスケーラビリティが確保されていることがある。

* 1. 2. 各運営形態の選定に向けたアプローチ
     1. 2.1. 運営形態の選定のアプローチについて
        1. 図2-1-1 実現したい目的を優先した観点における選定フロー
        2. 図2-1-2 運用・維持を優先した観点における選定フロー
           1. 判断基準

1.システム構築体制

2.アプリ開発体制

3.運用保守体制

4.セキュリティ対策維持管理体制

* + 1. 2.2. 運営形態毎の自由度
       1. 図 2-2-1 ASP やレンタルサーバでのウェブサイト運営
       2. 図 2-2-2 オンプレミスのウェブサイト運営
    2. 2.3. 運営形態毎に調達が必要となる機材
       1. 表 2-3-1 運営形態毎に調達が必要な機材
       2. サーバ室
       3. 電源管理
       4. ネットワーク回線
       5. サーバ、 OS
       6. ミドルウェア
       7. ウェブアプリケーション
       8. コンテンツ
    3. 2.4. 運営形態毎に発生する費用項目
       1. 表2-4-1 運営形態毎に必要となる費用
       2. サーバ室の整備費用
       3. ネットワーク回線の敷設費用
       4. ネットワーク機器の購入費用
       5. サーバの購入費用
       6. ウェブアプリケーションの開発費用・購入費用
       7. ウェブサーバの構築費用
       8. ウェブサイトの運用管理費用
       9. サービス利用費用、 課金
    4. 2.5. 運営形態毎の責任範囲
       1. 表2-5-1 運営形態毎の責任範囲
       2. サービスの停止
       3. データの破壊・消去
       4. 情報漏洩
       5. 改ざん
    5. 【コラム】 「契約の免責事項
       1. メンテナンスまたは不慮の事故等により、 サービス停止等によるサービス利用者の逸失利益や損害について、 提供者は一切の責任を負わないものとする
       2. 不測の事故等により、 サービス利用者のサーバ上に蓄積されているデータが喪失、 流失、 損壊等が発生した場合、 提供者は一切の責任を負わないものとする
    6. 2.6. 各運営形態で検討が必要なセキュリティ対策
       1. 表2-6-1 運営形態毎に検討すべきセキュリティ対策
       2. セキュリティ対策項目
          1. システムセキュリティ対策

技術的対策

物理

・サーバ室

・入退管理

ネットワーク

・FW　・IDS/IPS

・WAF ・VPN

・ウイルス対策製品

・サンドボックス型製品

・DDoS対策

アプリケーション

・改ざん検知

・認証　・アクセス制御

・データ保護

運用管理的対策

セキュリティパッチ

・パッチ適用

・仮想パッチ適用

監視

・ログ収集、 分析

インシデント対応

・バックアップ

・切り分け　　・抜線

人的対策

要員教育

・ポリシー教育

・技術教育

* + - * 1. 業務セキュリティ対策

社員教育

・リテラシー教育

ユーザ・顧客管理

・ポリシー教育

・情報取扱い規則

コンテンツ管理

・コンテンツ更新ルール

* + 1. 【コラム】 「既知の脆弱性が存在するウェブサイトに関する届出」
  1. 3. セキュリティ対策要件および強化のポイント
     1. 各セキュリティ対策が、 どのような要件を満たすべきか、 どの程度の強度レベルを必要とするか、 等については、 構築するウェブサイトにおいて実現する機能やサービスや事業モデルによって、 大きく異なってくる。
     2. 3.1. 実現する機能、 サービスに対する考慮のポイント
        1. 3.1.1 企業等の組織が公開するウェブサイトでのポイント
           1. 改ざんされることで、 サイト利用者が不利益を被る場合が考えられる。 また、 偽の情報を掲載されてしまったことで、 サイト運営者の信用失墜が発生する。
           2. ウェブサイト改ざんの被害は、 運営組織の大小や掲載されている情報の内容によらず、 事業継続の大きな障害となりうる。 このことから、 「我社のウェブサイトには漏洩して問題がある情報はない」というケースにおいても、 簡単に安心することはできない。
           3. 改ざん被害にあわないためには、 ウェブサイトで使用しているソフトウェアを常に最新の状態に保つことが、 第一の対策となる。
           4. モールやASP の運営形態

ソフトウェアのアップデートはサービス提供者が実施する対策

サービス提供者を選定する段階で、 外部機関によるペネトレーションテストを定期的に実施していたり、 ウェブサイト改ざん検知の機能を提供していたりするサービス提供者を選択することが重要

例えば、 「外部の●●社の脆弱性診断を毎年実施し、 脆弱性が検出されないことを確認している」といった、 明確な対策状況の回答が得られることが望ましい。

* + - 1. 3.1.2 EC サイトでのポイント
         1. EC サイト等では決済機能を提供するため、 ウェブサイト上でクレジットカード情報や、 口座情報等の取り扱いが必要である。 万が一、 EC サイトで不正アクセスや情報漏洩等が発生した場合、 サイト利用者のみならず、 関係している組織に対しても、 重大な被害が発生する。
         2. ASP やモール、 SaaS 型クラウドサービスを利用して運営する場合

決済機能を含む様々なプログラムはサービス提供者によって実装されるものである。 そのため、 サイト運営者による攻撃を検知するためのプログラムの実装や、 脆弱性の修正等の管理をすることができない

サービス提供者を選択する時点で、 外部からの攻撃を検知・遮断するための監視システムを導入しているか、 業界団体や政府機関が定めるセキュリティ基準に準拠した対策を行っているかについて調査する必要がある。

日本国内のサービス提供者であればPCI DSSへの準拠について確認が必須である38

PCI DSS は、 国際クレジットカード国際カードブランド5 社が共同で設立したPCI SecurityStandards Council によって運用、 管理されている基準であり、 日本国内ではクレジットカード情報を自社内で取り扱う企業に対して、 2018 年3 月までにPCI DSS へ準拠することが義務となっている。

* + - * 1. レンタルサーバやPaaS・IaaS 型のクラウドサービス、 ハウジング、 オンプレミスの運営形態の場合

決済機能はサイト運営者が何らかの形で導入する必要がある。 たとえば、 自組織で決済機能を開発する方法や、 クレジットカード会社が提供するサービスを利用するといった方法が考えられる。

ウェブサイトに独自に決済機能を開発する場合、 自組織内で機微な情報を取り扱う必要が発生する。

これによりPCI DSS 準拠へのセキュリティ対策・維持の負荷が増大するため、 外部の決済代行会社に決済機能を委託することで、 サイト運営者の負担を軽減することも一考である。

サイト運営者は悪意ある第三者がサイト利用者になりすまして商品の購入や、 他者の決 済情報を盗み取ることができないようにすることも必要である。

正規の利用者になりすまして情報を盗み取る場合、 正規のサイト利用者と攻撃者を識別することが困難である。

なりすましの被害を受ける原因

1. 簡単で短いパスワードを設定していた

2. 個人情報から類推しやすいパスワードを設定していた

3. 他のウェブサービスで同じパスワードを設定していた

なりすましを防ぐためには、 3.2 節で説明するサイト運営者側の対策だけでなく、 サイト利用者に対して簡単なパスワードの禁止やパスワードの使いまわしをしないこと等の啓発が必要である。

* + - 1. 3.1.3 SNS サイトや掲示板サイト等でのポイント
         1. 悪意ある書き込みや改ざんには十分留意する必要がある。
         2. 例えば、 クロスサイト・スクリプティングの脆弱性の場合

攻撃者がスクリプトを含む内容を投稿することで偽の情報を表示されてしまう。 このような被害を防ぐために、 投稿される内容にスクリプトが含まれていれば、 ウェブサイト上にそのまま出力しないよう特定の記号はエンコードして表示する必要がある。

* + - * 1. クロスサイト・リクエスト・フォージェリの脆弱性がある場合

サイト利用者が意図しない操作を実行させられてしまう可能性が存在し、 結果的に登録情報の書き換えや、 意図しない内容を投稿させられてしまうといった被害につながる。

これを防ぐために、 登録情報の変更等の重要な処理の際にはパスワードの再入力を求めることや、 外部のウェブサイトから転送された通信であるか調査する機能を実装する等の対策が必要である。

* + - * 1. この他の攻撃

他者のセッションを乗っ取り、 他人になりすまして記事を投稿する等がある。 その対策としては、 攻撃者によるセッションID の推測や、 被害者に任意のセッションID を使用させない（セッションID の固定をさせない）ウェブアプリケーションの設計にすることが必要である。

* + - 1. 3.1.4 画像投稿サイト等のファイルアップロードサイトでのポイント
         1. 違法なファイルをアップロードされる以外にも、 実行形式のファイルをアップロードされてしまうことにより、 アップロードサイトのサーバ上で不正なファイルを実行されてしまう可能性がある。
         2. このようなことが可能な場合、 スクリプトを含むファイルをアップロードし、 外部からそのファイルを参照することで、 任意のスクリプトをサーバ上で実行されてしまう被害が考えられる。
         3. スクリプトを実行されることで、 ウェブサイトの改ざんや、 サーバの設定の改ざんにつながる可能性がある。
         4. また、 ウイルスを含むファイルをアップロードされた場合、 サーバにウイルスが感染し、 外部から不正な命令を受け付けるようにされてしまう可能性もある。
         5. このようなリスクを回避するために、 アップロード可能なファイル形式を制限するだけでなく、 アップロードされたサーバ上でファイルのウイルスチェックを行う等の対策を講じることが必要である。
         6. また、 特定のユーザ以外にアクセスを許可しないファイルが、 誰でもURL を直接指定することで閲覧できてしまうといった、 アクセス制限不備の問題が考えられる。
         7. このような脆弱性がある場合、 アップロードされたファイルが不特定多数のサイト利用者から参照可能になってしまう。
         8. この場合、 個人を特定できてしまう情報を含むファイルが、 URL を直接指定するだけで参照できるといった被害が発生する。
         9. このような被害を防止するために、 ファイルのアクセス制限を適切に設定することが求められる。
    1. 3.2. セキュリティ強化のポイント
       1. 技術的な対策の観点
          1. (1) ネットワーク攻撃、 不正アクセス対策

・外部からの攻撃が発生しているかの把握（攻撃の検知等）

サブトピック

・外部からの攻撃からの防御（攻撃の遮断等）

サブトピック

* + - * 1. (2) DDoS攻撃対策

・攻撃通信をネットワークに入れないためにどうするか

* + - * 1. (3) なりすまし対策

・パスワードの管理体制の強化

・使用する接続方式、 認証方式の強化

サイト利用者に普及・啓発すべき対策について以下で解説する。

長く複雑なパスワードを設定するようにサイト利用者に要求すれば

・パスワードを使いまわす可能性の増加

・利便性の低下によるサイト利用者の減少

その一つの答えとして、 次に解説する二要素認証や二段階認証が存在する。

* + - * 1. (4) 重要情報の保護対策

・データベースをインターネット公開領域(いわゆるDMZ45)に配置しない

・重要情報の暗号化

・情報を変更、 参照する際の再認証

重要情報の暗号化について

ウェブサイトに登録した情報を変更、 参照する際の再認証の必要性について

* + - * 1. (5) 事業継続対策

サーバ等の機材故障やインターネット上から攻撃を受けた場合にウェブサイトの停止期間を最小化するためには、 事業継続計画（Business continuity planning）を検討する必要がある。

事業継続を目的とした対策には以下の２点等が存在

・予備システムを設置する

・バックアップを定期的に取得する

・予備システムを設置する

インターネットからの攻撃が行われ、 サーバが破壊されてしまった場合、 データやサービスの復旧には長期間の作業が必要となる。 このような場合に、 破壊されたサーバと同一の構成の予備システムがあれば、 ウェブサイト復旧までの時間を大幅に削減することが可能である。

注意すべき点として、 予備システムを有効に活用するためには、 主となるサーバと可能な限り同じデータを持ち、 同一のソフトウェアバージョンに揃える必要がある。

また、 予備システムが主となるサーバとは別の拠点に設置されていれば、 大規模な地域災害時への対策にも繋がる。

前述の予備システムを設置できない場合は、 次に説明するバックアップの取得が重要になる。

・バックアップを定期的に取得する

インターネット上から攻撃を受け、 ウェブサーバが破壊された際に、 ウェブサーバや重要情報のバックアップを取得していればバックアップデータを元にウェブサイトを速やかに復旧することができる。

多くの場合、 バックアップを取得するために専用のソフトウェアを購入する必要はなく、 OS の機能としてバックアップを取得することができる。

しかし、 バックアップデータを取得していても、 ウェブサーバ上に保管していれば、 ウェブサーバが攻撃を受けた際に同時にバックアップデータも破壊されてしまう可能性がある。

また、 バックアップデータを盗まれることで、 攻撃者が偽サイトを作成することを可能にしてしまうことも考えられる。 サーバ上に保管していない場合でも、 ネットワークに接続された端末に保管されていれば、 ウイルスがネットワークに侵入した際にバックアップデータが破壊・窃取を受ける可能性がある。

以上の理由から、 バックアップデータは外付けハードディスク等に保存し、 ネットワークから切り離して保管しておくことが望ましい。

* + - 1. その他の対策の観点
         1. (1) ログの収集、 分析
         2. (2) 各種基準への準拠

近年では、 ウェブサイトへの攻撃による被害に対応した保険商品等が提供されている。 しかし、 このような保険に加入する場合は、 保険企業やセキュリティ関連組織等が定める基準に準拠したウェブサイト運用が行われていることが条件となっている場合が多い。

また、 ウェブサイトの性質やウェブサイト上で取り扱う情報によっては、 所轄官庁が取り扱いの基準を定めている場合がある。

国内であれば、 経済産業省やNISC46、 海外であればNIST47等の公的機関がセキュリティ要件について様々なガイドラインや基準を定めている。

サービス提供者を選択する際に注意すべき点として、 以下の２点を挙げる。

・関係する団体が定める必須のセキュリティ基準を満たしているか

EC サイト等の決済機能を有するウェブサイトであれば、 使用する決済機能を提供する企業や、 業界団体が定めるセキュリティ基準基準を満たしているかについて確認が必要である。

代表例として、 PCI DSS がある。 3.1.2 項でも解説した通り、 国内でクレジットカードの決済機能を導入する場合は、 PCI DSS に準拠することが求められる。

この他に、 サイト運営者が所属する業界や団体が定めるセキュリティ基準がないか確認し、 その基準を満たしているサービス提供者を選択すべきである。

・必須ではないが、 自発的にセキュリティ基準に則った対策を実施しているか

サービス提供者が自発的に何らかの基準に従ったセキュリティ対策を実施しているか、 という観点で選択を行うべきである。

サービス提供者が自発的に何らかの基準に従ったセキュリティ対策を実施しているか

一例をあげると、 モールやASP のサービス提供者を選択する場合であれば、 総務省が定めた「ASP・SaaS における 情報セキュリティ対策ガイドライン」に準拠しているか、 といった観点で確認することが考えられる。

これは、 ASP やSaaS のサービス提供者に対し、 実施すべきセキュリティ対策について解説した資料である。

着目すべき基準については、 ウェブサイトのサービス内容や運営形態によっても変わるため、 サイト運営者自身で調査することが必要である。

* + - * 1. (3) セキュリティ専門事業者の活用

情報セキュリティを専門としない組織が独自に脆弱性診断や脆弱性対策を行うことは困難と考えられる。 そのため、 脆弱性の検査を行う情報セキュリティ専門の企業による診断を受けることが望ましい。

レンタルサーバ等では、 サーバの構築をサイト運営者自身で行う必要がある。

また、 サイト運営者によっては、 使用するウェブアプリケーションを独自に開発する場合もあり、 サーバや独自開発のウェブアプリケーションに脆弱性を作りこんでいないか、 十分に検査する必要がある。

しかしながら、 サイト運営者自身で脆弱性の検査を十分に行うことは困難であると考えられる。

特にハウジングやオンプレミスによる運営形態では、 サーバだけでなくネットワーク機器等にも脆弱性がないか調査する必要がある。

このような場合には、 脆弱性の検査を専門としたセキュリティ企業に、 サーバやウェブアプリケーションの脆弱性検査の委託を検討する必要がある。 セキュリティ専門企業については、 経済産業省が「情報セキュリティ監査企業台帳」を公開している。

* + - * 1. (4) サービス終了時の情報の破棄

サーバの機器故障やウェブアプリケーションの老朽化、 事業方針の変更等により、 ウェブサイトの運用の終了や、 次期システムへ移行する時期が訪れる。

このような際に適切にデータの破棄が行われていない場合、 ハードウェアを取得した第三者によって重要情報が盗み取られる被害が想定される。 このような被害を防ぐため、 重要情報や情報記録媒体の破棄について対応を検討しておく必要がある。

モールやASP、 レンタルサーバ等ではウェブサイトのプログラムのみならず、 サイト利用

者の個人情報についても、 サービス提供者の管理するサーバ上で管理される。 そのため、 ウェブサイトの運営を終了し、 ASP 等の利用契約を解除する際、 データの破棄・消去をサービス提供者がどのように取り扱いしているかについて、 サービス提供者の選択時に確認する必要がある。

例えば、 使用していたサーバのハードディスクの破壊について証明書を発行する、 米国国防総省が定めるDoD 5220.22-M に従ったデータの消去を保証しているといった観点がある。

各組織がハードウェアを管理するオンプレミス等の運営形態の場合は、 前述の規格に沿って組織内でデータの削除やハードディスクの破壊を実施、 または専門業者に依頼しての実施を検討する必要がある。

* 1. おわりに
     1. ウェブサイトで提供したいサービスや運営形態の手軽さだけでなく、 日々の運営でセキュリティを維持し続けることができるかといった点についても目を向けて頂き、 安全なウェブサイトの運営が可能な運営形態を選定するようにしてほしい。
  2. 補足資料
     1. 【補足1】ウェブサイト構築・運営の委託について
        1. 中小企業をはじめとして、 ウェブサイトの構築や運営を外部企業に委託する場合が数多く存在している。 ASP やモールの運営形態が目的と合致せず、 自組織内でウェブサイトを作成する技術がない場合は正しい選択である。
        2. しかしながら、 外部企業にウェブサイトの構築を委託した際、 契約内容にウェブサイトの脆弱性検査や運用開始後に脆弱性が見つかった場合の対応が盛り込まれておらず、 脆弱性を抱えたままコンテンツの更新だけが行われているウェブサイトが存在しており、 IPA に対して届出が行われている。
        3. このようなウェブサイトを運営するサイト運営者に脆弱性の連絡を行った際、 組織内で修正できないためウェブサイトを構築した企業に依頼する場合がある。
        4. しかし、 修正のための追加費用が発生してしまうことが原因で対応が行われないという事態が発生している。
        5. ウェブサイトに存在する脆弱性への対応は組織毎に判断すべき内容であるが、 重大な問題を抱えたまま運営し、 個人情報の流出等が発生する場合もあるため、 可能な限り脆弱性は解消することが望ましい。
        6. 前述したような事例となることを避けるために、 ウェブサイト構築・運営を委託する際には、 契約する際の項目に脆弱性の検査や脆弱性が見つかった場合の対応を明確に記載することが望ましいといえる。
     2. 【補足2】ログの取得について
        1. ログイン履歴
        2. アクセスログ
        3. 通信ログ
        4. ログを取得する際は以下の点に注意する
           1. ①意図しないログが残っていないか調査する
           2. ②取得場所以外の場所にログを保存する
     3. 【補足3】バックアップの取得間隔について
        1. 実際にバックアップの取得期間をどのように設定するべきかについては、 ウェブサイトの運用計画を定める段階で、 ウェブサイトの目的や更新頻度等からどれぐらいの期間のデータの喪失を許容できるかといった観点で定めることが必要である。
  3. 【付録A】ウェブサイト構築・運営に関する参考資料
     1. 「ウェブサイト構築のライフサイクル」の各フェーズで参考となる資料を一覧にまとめた表である。
     2. 1.企画
        1. 1 情報セキュリティ10 大脅威 2018
           1. https://www.ipa.go.jp/security/vuln/10threats2018.html

ドキュメントを参照: [10threats2017.html](https://www.ipa.go.jp/security/vuln/10threats2017.html)

* + - * 1. IPA
      1. 2 情報セキュリティ白書
         1. https://www.ipa.go.jp/security/publications/hakusyo/2017.html

ドキュメントを参照: [2017.html](https://www.ipa.go.jp/security/publications/hakusyo/2017.html)

* + - * 1. IPA
      1. 3 中小企業の情報セキュリティ対策ガイドライン
         1. https://www.ipa.go.jp/security/keihatsu/sme/guideline/

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - * 1. IPA
      1. 4　中小企業のためのクラウドサービス安全利用の手引き
         1. https://www.ipa.go.jp/security/cloud/tebiki\_guide.html

ドキュメントを参照: [tebiki\_guide.html](https://www.ipa.go.jp/security/cloud/tebiki_guide.html)

* + - * 1. IPA
      1. 5 ウェブサイト構築事業者のための脆弱性対応ガイド
         1. https://www.ipa.go.jp/security/fy20/reports/vuln\_handling/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/fy20/reports/vuln_handling/index.html)

* + - * 1. IPA
      1. 6 セキュリティ担当者のための脆弱性対応ガイド
         1. https://www.ipa.go.jp/security/fy22/reports/vuln\_handling/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/fy22/reports/vuln_handling/index.html)

* + - * 1. IPA
      1. 7 ソフトウエア管理ガイドライン
         1. http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanriguide.htm

ドキュメントを参照: [softkanriguide.htm](http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanriguide.htm)

* + - * 1. 経済産業省
      1. 8 効果的なサイバー防御のためのCIS クリティカルセキュリティコントロール
         1. https://sans-japan.jp/resources/CriticalSecurityControls.html

ドキュメントを参照: [CriticalSecurityControls.html](https://sans-japan.jp/resources/CriticalSecurityControls.html)

* + - * 1. Center For Internet Security
      1. 9 事業継続計画策定ガイドライン
         1. http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents\_000039.html

ドキュメントを参照: [seccontents\_000039.html](http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000039.html)

* + - * 1. 経済産業省
      1. 10 経営者が知っておくべきセキュリティリスクと対応について
         1. https://www.jpcert.or.jp/research/aptrisk.html

ドキュメントを参照: [aptrisk.html](https://www.jpcert.or.jp/research/aptrisk.html)

* + - * 1. Delta Risk Limited Liability Company
      1. 11 システム開発ライフサイクルにおけるセキュリティの考慮事項
         1. https://www.ipa.go.jp/security/publications/nist/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/publications/nist/index.html)

* + - * 1. 米国国立標準技術研究所
      1. 12 データベースセキュリティガイドライン
         1. http://www.db-security.org/report/guideline\_seika.html

ドキュメントを参照: [guideline\_seika.html](http://www.db-security.org/report/guideline_seika.html)

* + - * 1. データベース・セキュリティ・コンソーシアム
      1. 13 DB 内部不正対策ガイドライン
         1. http://www.db-security.org/report/ag\_seika.html
         2. データベース・セキュリティ・コンソーシアム
      2. 14 Payment Card Industry（PCI）データセキュリティ基準 (PCI DSS)
         1. https://ja.pcisecuritystandards.org/minisite/env2/

ドキュメントを参照: [env2](https://ja.pcisecuritystandards.org/minisite/env2/)

* + - * 1. PCI Security Standards Council
      1. 15 連邦政府の情報および情報システムに対するセキュリティ分類規格
         1. https://www.ipa.go.jp/security/publications/nist/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/publications/nist/index.html)

* + - * 1. 米国国立標準技術研究所
      1. 16 政府機関の情報セキュリティ対策のための統一基準（平成28 年度版）
         1. https://www.nisc.go.jp/active/general/kijun28.html

ドキュメントを参照: [kijun28.html](https://www.nisc.go.jp/active/general/kijun28.html)

* + - * 1. 内閣サイバーセキュリティセンター
    1. 2.設計
       1. 17 ウェブサイト改ざんの脅威と対策
          1. https://www.ipa.go.jp/security/technicalwatch/20140829.html

ドキュメントを参照: [20140829.html](https://www.ipa.go.jp/security/technicalwatch/20140829.html)

* + - * 1. IPA
      1. 18 Web Application Firewall 読本
         1. https://www.ipa.go.jp/security/vuln/waf.html

ドキュメントを参照: [waf.html](https://www.ipa.go.jp/security/vuln/waf.html)

* + - * 1. IPA
      1. 19 安全なウェブサイトの作り方
         1. https://www.ipa.go.jp/security/vuln/websecurity.html

ドキュメントを参照: [websecurity.html](https://www.ipa.go.jp/security/vuln/websecurity.html)

* + - * 1. IPA
      1. 20 攻撃者に狙われる設計・運用上の弱点についてのレポート
         1. https://www.ipa.go.jp/security/technicalwatch/20140328.html
         2. IPA
      2. 21 インシデント対応マニュアルの作成について
         1. https://www.jpcert.or.jp/csirt\_material/build\_phase.html

ドキュメントを参照: [build\_phase.html](https://www.jpcert.or.jp/csirt_material/build_phase.html)

* + - * 1. JPCERT/CC
      1. 22 情報資産の重み-対策レベル対応表
         1. http://www.db-security.org/report.html

ドキュメントを参照: [report.html](http://www.db-security.org/report.html)

* + - * 1. データベース・セキュリティ・コンソーシアム
      1. 23 DB セキュリティガイドライン-他フレームワーク対応表
         1. http://www.db-security.org/report.html

ドキュメントを参照: [report.html](http://www.db-security.org/report.html)

* + - * 1. データベース・セキュリティ・コンソーシアム
      1. 24 ITシステムのためのリスクマネジメントガイド
         1. https://www.ipa.go.jp/security/publications/nist/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/publications/nist/index.html)

* + - * 1. 米国国立標準技術研究所
      1. 25 連邦情報システムのためのセキュリティ計画作成ガイド 改訂第1 版
         1. https://www.ipa.go.jp/security/publications/nist/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/publications/nist/index.html)

* + - * 1. 米国国立標準技術研究所
    1. 3.実装/構築
       1. 26 安全なウェブサイトの作り方
          1. https://www.ipa.go.jp/security/vuln/websecurity.html

ドキュメントを参照: [websecurity.html](https://www.ipa.go.jp/security/vuln/websecurity.html)

* + - * 1. IPA
      1. 27 ウェブサイト改ざんの脅威と対策
         1. https://www.ipa.go.jp/security/technicalwatch/20140829.html

ドキュメントを参照: [20140829.html](https://www.ipa.go.jp/security/technicalwatch/20140829.html)

* + - * 1. IPA
      1. 28 攻撃者に狙われる設計・運用上の弱点についてのレポート
         1. https://www.ipa.go.jp/security/technicalwatch/20140328.html

ドキュメントを参照: [20140328.html](https://www.ipa.go.jp/security/technicalwatch/20140328.html)

* + - * 1. IPA
      1. 29 IPA セキュア・プログラミング講座
         1. https://www.ipa.go.jp/security/awareness/vendor/programming/

ドキュメントを参照: [programming](https://www.ipa.go.jp/security/awareness/vendor/programming/)

* + - * 1. IPA
      1. 30 ウェブサイトにおける脆弱性検査手法の紹介（ソースコード検査編）
         1. https://www.ipa.go.jp/security/technicalwatch/20140306.html

ドキュメントを参照: [20140306.html](https://www.ipa.go.jp/security/technicalwatch/20140306.html)

* + - * 1. IPA
      1. 31 CERT C コーディングスタンダード
         1. https://www.jpcert.or.jp/sc-rules/

ドキュメントを参照: [sc-rules](https://www.jpcert.or.jp/sc-rules/)

* + - * 1. JPCERT/CC
      1. 32 連邦政府情報システムのためのセキュリティ管理策アセスメントガイド
         1. https://www.ipa.go.jp/security/publications/nist/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/publications/nist/index.html)

* + - * 1. 米国国立標準技術研究所
    1. 4.テスト
       1. 33 安全なウェブサイトの作り方
          1. https://www.ipa.go.jp/security/vuln/websecurity.html

ドキュメントを参照: [websecurity.html](https://www.ipa.go.jp/security/vuln/websecurity.html)

* + - * 1. IPA
      1. 34 ウェブサイトにおける脆弱性検査手法(ウェブアプリケーション検査編)
         1. https://www.ipa.go.jp/security/technicalwatch/20160928-2.html

ドキュメントを参照: [20160928-2.html](https://www.ipa.go.jp/security/technicalwatch/20160928-2.html)

* + - * 1. IPA
      1. 35 システム監査企業台帳
         1. http://www.meti.go.jp/policy/netsecurity/sys-kansa/

ドキュメントを参照: [sys-kansa](http://www.meti.go.jp/policy/netsecurity/sys-kansa/)

* + - * 1. 経済産業省
      1. 36 情報セキュリティ監査企業台帳
         1. http://www.meti.go.jp/policy/netsecurity/is-kansa/
         2. 経済産業省
    1. 5.運用/利用
       1. 37 ウェブサイト運営者のための脆弱性対応ガイド
          1. https://www.ipa.go.jp/security/fy19/reports/vuln\_handling/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/fy19/reports/vuln_handling/index.html)

* + - * 1. IPA
      1. 38 インシデントハンドリングマニュアル
         1. http://www.jpcert.or.jp/csirt\_material/operation\_phase.html

ドキュメントを参照: [operation\_phase.html](http://www.jpcert.or.jp/csirt_material/operation_phase.html)

* + - * 1. JPCERT/CC
      1. 39 CSIRT ガイド
         1. http://www.jpcert.or.jp/csirt\_material/operation\_phase.html

ドキュメントを参照: [operation\_phase.html](http://www.jpcert.or.jp/csirt_material/operation_phase.html)

* + - * 1. JPCERT/CC
  1. 【付録B】複数の観点による運営形態の選定 アプローチ
     1. 図B-1 ウェブサイト構築時の観点に基づくフローチャート
     2. 図B-2 ウェブサイト運用時の観点に基づくフローチャート
     3. 図B-3 セキュリティインシデント発生時の観点から見たフローチャート
     4. 図B-4 セキュリティインシデント対応体制構築の観点から見たフローチャート

1. 情報セキュリティ読本　四訂版- IT時代の危機管理入門 -【2014年11月4日IPA】

ドキュメントを参照: [ppt.html](https://www.ipa.go.jp/security/publications/dokuhon/ppt.html)

* 1. 第4章　組織の一員としての情報セキュリティ対策
  2. 1.      1. 組織のセキュリティ対策
     1. 計画（Plan） - 体制の整備とポリシーの策定
     2. 実行（Do） - 導入と運用
     3. 点検（Check） - 監視と評価
     4. 処置（Act） - 見直しと改善
     5. 1.1.     1） 計画（Plan）- 体制の整備とポリシーの策定
        1. 組織内の体制を確立する
        2. セキュリティポリシーを策定する
        3. 対策事項の立案と手順書の整備
        4. 1.1.1.      組織内の体制を確立する
           1. 情報セキュリティを推進するための体制を組織内に作ることが出発点
           2. 実施担当者と、 その役割、 権限、 責任を定める
           3. 望ましい体制

経営陣が中心となって取り組む

全社横断的な体制

トップダウンの管理体制

* + - 1. 1.1.2.      セキュリティポリシーの策定
         1. セキュリティポリシーとは

組織として一貫したセキュリティ対策を行うために、 組織のセキュリティ方針と対策の基準を示したもの

* + - * 1. セキュリティポリシーの階層

基本方針

対策基準

対策実施手順

* + - * 1. 策定前の準備

情報資産の「何を守るのか」を決定する

「どのようなリスクがあるのか」を分析する

* + - * 1. 責任者と担当者を明確にする

組織体の長＝情報セキュリティの最高責任者

* + - 1. 1.1.3.      対策事項の立案と手順書の整備
         1. 対策基準とは

情報資産を脅威から守る方法を具体的に定めたもの

* + - * 1. 実施手順とは

対策基準を実際の行動に移す際の手順書（マニュアルのようなもの）

最初に設定する内容とその手順

定期的に実施する対策の手順

インシデント発生時の対策と手順

* + 1. 1.2.     2） 実行（Do）- 導入と運用
       1. 導入フェーズ
       2. 運用フェーズ
       3. 1.2.1.      導入フェーズ
          1. 構築と設定

ウイルス対策ソフトやファイアウォールなどのセキュリティ装置の導入、 暗号機能の導入

OS、 アプリケーションのセキュリティ設定

* + - * 1. 設定における注意点

デフォルト設定は使用しない

不要なサービスの停止

* + - * 1. 脆弱性の解消

最新の修正プログラムを適用

* + - * 1. レベルに応じたアクセス制御

組織のメンバーごとにアクセスレベルを設定

アクセスできる範囲と操作権限を制限する

* + - 1. 1.2.2.      運用フェーズ
         1. セキュリティポリシーの周知徹底とセキュリティ教育

役割と責任、 セキュリティ対策上のルールを周知

被害に遭わないために脅威と対策を教える

* + - * 1. 脆弱性対策

定期的な情報収集とパッチの適用

* + - * 1. 異動/退職社員のフォロー

退職者のアカウントは確実に削除（セキュリティホールになりうる）

* + 1. 1.3.     3） 点検（Check） - 監視と評価 -
       1. 監視と評価
       2. セキュリティ事故への対処
       3. 1.3.1.      監視と評価
          1. ネットワークを監視し、 異常や不正アクセスを検出する

通信、 不正アクセスの監視

異常検知、 不正アクセス検知、 脆弱性検査

* + - * 1. ポリシーが守られているか自己または第三者による評価を行う

自己点検（チェックリストなどにより実施）

情報セキュリティ対策ベンチマークでの自己診断

情報セキュリティ監査

* + - 1. 1.3.2.      セキュリティ事故への対処
         1. セキュリティポリシーに則ったインシデント対応
         2. 特に注意すべき点

被害状況を調査し、 二次災害を防ぐ

原因を特定し、 再発防止策を徹底する

実施した対応の記録、 各種届出（必要な場合）

対応窓口を設置し、 正確な情報を提供する

サブトピック

* + 1. 1.4.     4） 処置（Act） - 見直しと改善
       1. セキュリティポリシーを見直し、 改善点を検討する
       2. セキュリティマネジメントサイクルの実施にともない、 情報セキュリティ対策を高めることが重要
  1. 2.      2. 従業員としての心得
     1. 規則を知り、 遵守する
     2. 情報セキュリティ上の脅威と対策を知る
     3. 「自分だけは 」、 「これぐらいなら 」は通用しない
        1. 必ず上司に報告・相談する
     4. 特に、 情報漏えいに気を付ける
  2. 3.      3. 気を付けたい情報漏えい
     1. 情報漏えいの経路と原因
     2. 情報漏えいを防止するための管理対策のポイント
     3. 企業や組織の一員としての情報セキュリティ心得
     4. 3.1.     情報漏えいの経路と原因
        1. 情報漏えいの経路
           1. PC本体、 スマートフォン、 タブレット端末、
           2. 外部記憶媒体（USBメモリなど）、
           3. 紙媒体、 P2Pファイル交換ソフト
        2. 情報漏えいの原因
           1. 管理ミス、 誤操作、 紛失・置忘れが約8割
        3. 人為的なミスを防ぐことが重要
     5. 3.2.     情報漏えいを防止するための管理対策のポイント
        1. P2Pファイル交換ソフトは使用しない
        2. 私物パソコン等を業務で使用しない（持ち込ませない）
        3. 個人情報や機密情報を外部に持ち出さない（記憶媒体にコピーしない）
        4. 社用のノートパソコンを持ち出す場合は、 ルールを決めて厳密に管理する
     6. 3.3.     企業や組織の一員としての情報セキュリティ心得
        1. 企業や組織の情報や機器を、 許可なく持ち出さない
        2. 私物のノートパソコンやプログラムなどを、 許可なく、 企業や組織に持ち込まない
        3. 企業や組織の情報や機器を未対策のまま放置しない
        4. 企業や組織の情報や機器を未対策のまま廃棄しない
        5. 個人に割り当てられた権限を他の人に貸与または譲渡しない
        6. 業務上知り得た情報を公言しない
        7. 情報漏えいを起こした場合は速やかに報告する
  3. 4.      4. 終わりのないプロセス
     1. 一度、 導入・設定すればそれで終わり、 というものではない。
     2. 運用、 見直し、 フィードバックを繰り返すプロセスが必要。
     3. 技術面だけでなく、 管理面も強化する
     4. 技術的対策と管理的対策はクルマの両輪の関係
  4. 5.      情報セキュリティにおけるさまざまな対策
     1. 参考） IPAセキュリティセンター「情報セキュリティマネジメントについて」
     2. http://www.ipa.go.jp/security/manager/protect/management.html
     3. 参考）読者層別：情報セキュリティ対策実践情報：
     4. http://www.ipa.go.jp/security/awareness/awareness.html

1. 米国の「20の重要なセキュリティ対策」及びオーストラリアの「35の標的型サイバー侵入に対する軽減戦略」【2010年】

ドキュメントを参照: [27.6keigennsennryakuhp.pdf](https://ssl.bsk-z.or.jp/kakusyu/pdf/27.6keigennsennryakuhp.pdf)

* 1. サブトピック 1

1. コンピュータセキュリティインシデント対応ガイド（NIST SP 800-61）【2008年3月NIST】

ドキュメントを参照: [000025341.pdf](https://www.ipa.go.jp/files/000025341.pdf)

* 1. NIST（米国立標準技術研究所）が体系化した英文で80ページほどの文書。 セキュリティ対策を次の4つのフェーズに分けて考えている。
  2. （1）準備：やられないよう備える
  3. （2）検知・分析：やられてもすぐに察知できる
  4. （3）根絶・復旧・封じ込め：やられた場合の被害を小さくし、 すぐビジネスを復旧させる
  5. （4）事件発生後の対応：再発防止と最後の水際の対策を考える

1. JIPDEC経営読本「情報管理はマネーです」【2017年JIPDEC】

ドキュメントを参照: [jipdec\_keieidokuhon\_a4.pdf](https://www.jipdec.or.jp/library/u71kba00000072hw-att/jipdec_keieidokuhon_a4.pdf)

1. IPAテクニカルウォッチ「ランサムウェアの脅威と対策」【2017年1月IPA】

ドキュメントを参照: [000057314.pdf](https://www.ipa.go.jp/files/000057314.pdf)

1. IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」【2017年1月IPA】

ドキュメントを参照: [000043331.pdf](https://www.ipa.go.jp/files/000043331.pdf)

1. 情報漏えい発生時の対応ポイント集(第3版) 【2012年10月IPA】

ドキュメントを参照: [rouei\_taiou.pdf](http://www.ipa.go.jp/security/awareness/johorouei/rouei_taiou.pdf)

1. 「高度サイバー攻撃対処のためのリスク評価等のガイドライン 付属書」 【2016年10月NISC】

ドキュメントを参照: [riskguide-appendix.pdf](https://www.nisc.go.jp/active/general/pdf/riskguide-appendix.pdf)

1. 『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】

ドキュメントを参照: [000046236.pdf](https://www.ipa.go.jp/files/000046236.pdf)

1. モバイルセキュリティ関連
   1. Sec01-02-60\_各種ガイドブックの内容要約(働き方改革関連)へ移動

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-60.html>

* 1. ●MDM導入・運用検討ガイド【経済産業省】

ドキュメントを参照: [MDMGuideV1.pdf](https://www.jssec.org/dl/MDMGuideV1.pdf)

* 1. ●情報セキュリティ対策の基本 スマートフォン編 - IPA【IPA】

ドキュメントを参照: [000059213.pdf](https://www.ipa.go.jp/files/000059213.pdf)

* 1. ●スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン【経済産業省】

ドキュメントを参照: [seccontents\_000142.html](https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000142.html)

* 1. ●私物端末の業務利用におけるセキュリティ要件の考え方【内閣官房】

ドキュメントを参照: [byod.pdf](https://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/byod.pdf)

* 1. ●情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン【厚生労働省】

ドキュメントを参照: [3003011.pdf](https://www.mhlw.go.jp/file/06-Seisakujouhou-11200000-Roudoukijunkyoku/3003011.pdf)

* + 1. ガイドラインの主なポイント
       1. ○ テレワークのメリット
          1. テレワークは労働者が所属する事業場での勤務に比べて、働く時間や場所を柔軟に活用することが可能

労働者にとってのメリット

・通勤時間の短縮

・業務の効率化･時間外労働の削減

・育児や介護と仕事の両立の一助に

・仕事と生活の調和を図ることが可能 等

使用者にとってのメリット

・業務効率化による生産性の向上

・育児･介護等による労働者の離職の防止

・遠隔地の優秀な人材の確保

・オフィスコストの削減 等

* + - 1. ○ テレワークの問題や課題
         1. 問題や課題

・労働時間の管理が難しい

・仕事と仕事以外の切り分けが難しい

・長時間労働になりやすい 等

* + - * 1. ↓テレワークにおける適切な労務管理の実施は、テレワークの普及の前提 となる重要な要素
      1. ○ 労働基準関係法令の適用
         1. テレワークを行う労働者にも、労働基準法、最低賃金法、労働安全衛生法、労働者災害補償保険法等の労働基準関係法令が適用される
         2. 業務を行う場所に応じたテレワークの特徴

① 在宅勤務

通勤の必要がないため、時 間を有効に活用することが 可能となり、仕事と家庭生 活との両立に繋がる

② サテライトオフィス勤務

自宅近くや通勤途中の場所など に設けられたサテライトオフィ スを利用することで、通勤時間 を短縮しつつ、作業環境の整っ た場所での就労が可能

③ モバイル勤務

労働者が自由に働く場所を選 択できる、外勤における移動 時間を利用できる等、業務の 効率化を図ることが可能

* + 1. ガイドラインの概要
       1. １趣旨
       2. ２労働基準関係法令の適用及び留意点等
          1. （１）労働基準関係法令の適用
          2. （２）労働基準法の適用に関する留意点
          3. （３）長時間労働対策について

・テレワークについては、労働者が使用者と離れた場所で勤務をするため、長時間労働を招くおそれがあることも指摘されており、使用者は、長時間労働による健康障害防止を図ることが求められる

① メール送付の抑制

役職者等から時間外、休日又は深夜におけるメールを送付することの自粛を命ずる

② システムへのアクセス制限

外部のパソコン等から深夜・休日はアクセスできないよう設定すること

③テレワークを行う際の時間外・休日・深夜労働の原則禁止等

業務の効率化やワークライフバランスの実現の観点から、時間外・休日・深夜労働を原則禁止とすること又は使用者等による許可制とすること

④長時間労働等を行う労働者への注意喚起

長時間労働が生じるおそれのある労働者や、休日・深夜労働が生じた労働者に対して、労働時間の記録や、労務管理システムを活用して注意喚起を行うこと

* + - * 1. （４）労働安全衛生法の適用及び留意点
        2. （５）労働災害の補償に関する留意点
      1. ３テレワークを適切に導入及び実施するに当たっての注意点
         1. （１）労使双方の共通の認識
         2. （２）業務の円滑な遂行
         3. （３）業績評価等の取扱い
         4. （４）通信費、情報通信機器等のテレワークに要する費用負担の取扱い
         5. （５）社内教育等の取扱い
      2. ４ テレワークを行う労働者の自律
         1. ・労働者においても、勤務する時間帯や自らの健康に十分に注意を払いつつ、作業能率を勘案して自律的に業務を遂行することが求められる
  1. ●テレワークではじめる働き方改革－テレワークの導入・運用ガイドブック－【厚生労働省】

ドキュメントを参照: [01\_01.pdf](https://work-holiday.mhlw.go.jp/material/pdf/category7/01_01.pdf)

* + 1. 目次
       1. はじめに
          1. テレワークは、『ICT（情報通信技術）を活用し、時間や場所を有効に活用できる柔軟な働き方』です。
          2. 近年、スマートフォン、タブレット端末等の情報通信機器が発達するとともに、通信サービスについても、ブロードバンドサービスが普及し、運用コストやセキュリティ確保の課題も解決されつつあり、テレワークを取巻く環境は、飛躍的に変化しています。
          3. 企業にとってのメリット

• 人材の確保・育成

• 業務プロセスの革新

• 事業運営コストの削減

• 非常時の事業継続性（BCP）の確保

•企業内外の連携強化による事業競争力の向上

• 人材の離職抑制・就労継続支援

• 企業ブランド・企業イメージの向上

* + - * 1. 従業員にとってのメリット

• ワーク・ライフ・バランスの向上

• 生産性の向上

• 自律・自己管理的な働き方

• 職場との連携強化

•仕事全体の満足度向上と労働意欲の向上

* + - * 1. ［本書が想定している読者］

■経営者

直面する経営課題（生産性向上、グローバル化の推進、オフィスコストの削減、優秀な人材の採用・流出防止、BCP（事業継続性）の確保等）の解決に向け、テレワークがどのように役立つかを理解し、自社の施策として導入・普及拡大を検討するために

■テレワークの推進担当者（経営企画担当、人事・総務担当、情報システム担当など）

テレワークの導入、普及拡大に当たり、実務的な知識やノウハウを習得し、実践につなげるために

* + - 1. Ⅰ　基礎編
         1. 1.テレワークとは

在宅勤務（終日在宅勤務）

●従業員のワーク・ライフ・バランスを実現する上で効果的です。

●育児・介護期の従業員がキャリアの継続を図ることができます。また、障がいなどにより通勤が困難な従業員の就労継続にも効果的です。

●静かな環境を整えやすいため、集中して業務を行うことができます。

モバイルワーク

●営業職など、所属オフィス外での業務が多い職種にとって特に有用です。

●移動時間を有効活用できる、顧客先で迅速に対応できるなどのメリットがあります。

サテライトオフィス勤務 （施設利用型勤務）

●顧客先に近い施設の利用

顧客先に近い施設を利用することで、迅速な顧客対応、帰社などのための移動時間の削減により、業務を効率化できます。

●従業員の自宅に近い施設の利用

従業員の自宅に近い施設を利用することで、所属するオフィスまで通勤することが困難な人材を活用できます。

●遊休施設や空き家などの活用

遊休施設や空き家などを活用することで、オフィスコストを抑えることができます。

オフィススペースの契約形態

専用型

自社・自社グループ専用として利用され、従業員が営業活動で移動中、あるいは出張中である場合などに立ち寄って就業できるオフィススペースです。事業所とは別にスペースを設置する方法と、各地の事業所内にテレワーク専用のスペースを設ける「スポットオフィス」が存在します。

共用型

複数の企業がシェアして利用するオフィススペースです。最近では、「シェアオフィス」や「コワーキングスペース」ともいい、企業や、フリーランス、起業家が一定の契約のもとにスペースを活用して仕事をしたり、情報交換やイベント開催を行ってビジネスを行うオフィスもあります。

* + - * 1. 2.我が国のテレワークを取り巻く現状
        2. 3.テレワークの効果

企業（経営者・推進担当者）の感じる効果

優秀な人材の確保や雇用継続につながった

資料の電子化や業務改善の機会となった

通勤費やオフィス維持費などを削減できた

非常時でも事業を継続でき、早期復旧もしやすかった

顧客との連携強化、従業員の連携強化になった

離職率が改善し、従業員の定着率向上が図れた

企業のブランドやイメージを向上させることができた

従業員（テレワーク実施者）の感じる効果

家族と過ごす時間や趣味の時間が増えた

集中力が増して、仕事の効率が良くなった

自律的に仕事を進めることができる能力が強化された

職場と密に連携を図るようになり、これまで以上に信頼感が強くなった

仕事の満足度が上がり、仕事に対する意欲が増した

1　企業にとっての効果

【コラム】業務の見える化

業務の「見える化」とは、成果だけでなく、業務の進捗状況を表やグラフ等にすることで、作業者や上司・同僚がその業務の進み具合を適宜確認できるようにすることです。

例えば、スケジュール共有ツールなどでその日に進める業務の内容を周知する、又は作成する資料を誰でも閲覧可能な共有ファイルに格納することで資料の作成状況を共有するなどの方法があります。

業務の「見える化」をすると、作業者は自身以外の従業員と業務の分担がしやすくなるほか、上司が業務の進み具合を管理しやすくなるメリットがあります。

また、業務に対する評価について、成果のみではなく、どのように業務を進めたかのプロセスも評価対象にすることができます。このプロセス評価は、作業者が業務に取り組んだ労力全体の評価を受けられることから、作業に当たった従業員の仕事に対するモチベーションが向上しやすくなったり、業務の無駄や不手際をチェックすることで次回以降の業務の進め方が改善したりする効果があります。

【コラム】キャリアの継続を可能にするテレワーク利用

A社では、従業員のほとんどが出社せず、終日在宅勤務を行っています。中には、配偶者の転勤に合わせて、所属するオフィスから遠く離れた場所に転居した、高い専門性を持つ技術者もいます。

従業員には、業務遂行が十分に可能なシステムが提供され、顧客との会議や従業員同士の打ち合わせには、Web 会議システムを活用しています。

一方、従業員間の対面でのコミュニケーションも大切にしており、2 か月に 1回は全従業員が本社に集合し、顔を合わせて会議と食事をする会を設けるなどの工夫をしています。

2　従業員にとっての効果

ⅰ. ワーク・ライフ・バランスの向上

•通勤時の身体的負担を軽減し、自由に使える時間が増加することで、ワーク・ライフ・バランスを向上させることができる

•生産性の向上によってプライベートの時間をきちんと確保でき、仕事と生活のメリハリがついた

ⅱ. 生産性・創造性の向上

•一人で作業するための空間をつくることで、自分自身の担当業務に集中して取り組むことができるため、生産性・創造性が向上する

ⅲ. 自律・自己管理的な働き方

•目標を定めて業務進捗や業績管理を自律的に行う必要性があるため、セルフマネジメント力が養われる

•ワーク・ライフ・バランスの実現に向けて、仕事と生活との切り分けやバランスをより一層意識するようになり、仕事にメリハリをつけるようになる

ⅳ. 職場との連携強化

•意識的にコミュニケーションを図ろうとする結果、今まで以上にコミュニケーションの回数が増え、上司・同僚との信頼感が高まる

•ツールを介したコミュニケーションがやり取りの気軽さを生み、コミュニケーションの回数が増える

•業務を「見える化」することで、上司と部下が業務の連携を図りやすくなり、信頼関係が向上する

ⅴ.仕事全体の満足度向上・就業意欲の向上

•柔軟な働き方ができるため、ワーク・ライフ・バランスを実現でき、仕事に対する満足度が向上する

•働きたいという意欲を持ちながらも十分な労働時間を確保できなかった人材にとって、テレワークが労働時間の確保に役立ち、より仕事への意欲がより向上する

* + - 1. Ⅱ　実践編
         1. 第1章　モデル類型とは

1.「テレワークモデル実証事業」の効果

2.モデル類型における①テレワーク形態、②職種、③企業規模

3.モデル類型の選択

4.各モデル類型におけるICTシステム・ツール

■図表Ⅱ-1-5　ICTシステム・ツールの選択における基本的なメニュー

■図表Ⅱ-1-6　各モデル類型におけるICTシステム・ツールの選択（一覧）

■図表Ⅱ-1-7　各モデル類型におけるICTシステム・ツールの説明

※各モデル類型におけるICTシステム・ツールの説明

* + - * 1. 第２章　テレワーク導入の手順・推進体制

1.テレワーク導入のイメージ

2.導入のプロセス

※各モデル類型におけるICTシステム・ツールの説明

3.推進体制の構築

* + - * 1. 第３章　テレワーク実施のための全体方針の決定

1.導入目的の明確化

2.基本方針の策定

3.社内の合意形成のポイント

* + - * 1. 第４章　テレワークのためのルールづくり

1.テレワーク実施範囲の検討

図表Ⅱ-4-2　企業がテレワークで実施している業務

2.労務管理

3.導入のための教育・研修

* + - 1. 第５章　テレワークのためのICT環境づくり
         1. 図表Ⅱ-5-1 テレワークができるICT環境
         2. 1.ICT環境導入のための手順

導入手順（例）

❶現在のICT環境の確認

❷テレワーク環境の方式選択・各種ツールの選択

❸導入に必要な期間の確認

❹導入中の業務の停滞箇所・要調整の確認

❺導入期間の全社周知（システムの利用に関する従業員向け研修）

❻システム導入～システムの実際の稼動

* + - * 1. 2.テレワーク環境の選択

（1） 利用端末の確認

❶リッチクライアント（ファットクライアント）型PC

❷ シンクライアント型PC

1）リッチクライアントを専用システムでシンクライアント化する方法

2）シンクライアント専用PCを利用する方法

3）リモートデスクトップ接続クライアントを利用する方法

❸ タブレット型PC・スマートフォン

（2） ネットワーク

（3） サーバ

* + - * 1. 3.テレワーク環境におけるシステム方式の選択

（１）リモートデスクトップ方式

セキュリティ

作業は遠隔操作で実施する。そのため、全ての作業がオフィスの端末で行っている状態と同じで、手元の端末にデータは残らない。また、保存したファイルはオフィスにある端末上に保存される。情報漏えいが起きにくいメリットがある。

（２）仮想デスクトップ方式

（３）クラウド型アプリ方式

（４）会社PC の持ち帰り方式

* + - * 1. 4.労務管理ツール
        2. 5.コミュニケーションツール

❶ 会議システム

❷Eメール・チャット（インスタントメッセンジャー）

❸ 情報共有ツール

1） データ共有ツール

2） グループウェア

* + - 1. 第６章　安全なテレワークのためのセキュリティ対策
         1. 図表Ⅱ-6-1　テレワークに必要なセキュリティの考え方
         2. 1.ルールによるセキュリティ対策

（1）セキュリティガイドラインの策定

●基本方針：セキュリティ全体の根幹

●対策基準：基本方針をもとに実施すべきことや守るべきことを規定したもの

●実施手順：対策基準の事項を具体的に実行するための手順を示したもの

（2）セキュリティルール・情報管理ルールの策定

●自宅における作業環境、PC の保管及び管理方法

●自宅における休憩中の PC の取扱い 〔ロックだけでいいのか、保管して鍵をかけるのか〕

●モバイルワークにおけるPCの管理方法 〔体から離さない、ストラップをつける、のぞき見防止フィルターをつける〕

●オフィスから持ち出す PCの管理 〔暗号化、BIOSパスワードなどを義務付け〕

●オフィス以外での情報管理 〔紙情報の管理、共用スペースでの情報管理〕

（3）ガイドラインとルールの遵守・浸透

* + - * 1. 2.技術的なセキュリティ対策

（1） アクセスの管理・制限

本人認証

端末認証

（２）暗号による管理

ハードディスク（HDD）暗号化

セキュアコンテナ

携帯電話等にセキュアコンテナ（暗号化された企業用の業務データエリア）を作成するソフト及びサービス

情報漏えい対策付きの USB メモリ

（３）運用のセキュリティ

電子データの原本保存

ウイルス対策ソフト

（４）ネットワークのセキュリティ

より安全な回線の選択

サーバ証明書

【コラム】モバイルワークにおけるセキュリティ対策の注意点等（例）

モバイルワーク時のルール（例）

①オフィス外を移動するときは、必ずPCを鞄に入れて常時携帯する

②PCのローカルエリアにファイルを保存しない

③ハードディスクを暗号化する

④社外環境で印刷出力しない

⑤インターネット接続は会社支給のモバイルルータからのみ可とする

⑥社内環境へは暗号化通信を利用して接続する

⑦のぞき見防止フィルターを必ず装着する

⑧PCを持ち帰る時は、上長にメールで報告する

⑨Web会議等の音声が発せられるときは、周囲に聞かれないよう注意する

危険性と対策について

【コラム】セキュリティ保護と業務効率向上とのジレンマ

* + - * 1. 3.物理的なセキュリティ対策
      1. 第7章　テレワーク推進のための評価と改善
         1. 1.評価の仕方
         2. 2.改善の仕方
      2. テレワークの活用でよくあるQ&A
      3. テレワークお役立ちリンク集
    1. システム方式
       1. リモートデスクトップ
       2. 仮想デスクトップ
       3. クラウド型アプリ
       4. 会社ＰＣ持ち帰り
    2. 端末デバイス
       1. リッチクライアント
       2. シンクライアント
       3. タブレット型PC
       4. スマートフォン
       5. 携帯電話
    3. セキュリティ
       1. 本人認証
       2. 端末認証
       3. 端末管理
       4. 暗号化通信
       5. ストレージ暗号化
  1. ●テレワークセキュリティガイドライン第４版【総務省】

ドキュメントを参照: [000545372.pdf](https://www.soumu.go.jp/main_content/000545372.pdf)

* + 1. はじめに
       1. テレワークとは？
          1. 在宅勤務
          2. モバイル
          3. サテライトオフィス
    2. 1. テレワークにおける情報セキュリティ対策の考え方
       1. （ア） 「ルール」「人」「技術」のバランスがとれた対策の実施
          1. 図 1 テレワークにおける脅威と脆弱性について
          2. 図 2 情報セキュリティ対策におけるバランスの考え方
          3. 【コラム】 中小企業の情報セキュリティ対策を支援する取組
       2. （イ） テレワークの方法に応じた対策の考え方
          1. 表1 テレワークの６種類のパターン

リモートデスクトップ方式

仮想デスクトップ方式

クラウド型アプリ方式

セキュアブラウザ方式

アプリケーションラッピング方式

会社ＰＣの持ち帰り方式

* + - * 1. 図3 リモートデスクトップ方式
        2. 図4 仮想デスクトップ方式
        3. 図5 クラウド型アプリ方式
        4. 図6 セキュアブラウザ方式
        5. 図7 アプリケーションラッピング方式
        6. 図8 会社PC の持ち帰り方式
        7. （自社にふさわしいテレワークの方式の検討）
        8. （クラウドサービスの利用について）
        9. 図9 クラウドサービスへの移行
      1. （ウ） 経営者、 システム管理者及びテレワーク勤務者それぞれの立場
         1. ＜システム管理者＞
         2. ＜テレワーク勤務者＞
    1. 2. テレワークセキュリティ対策のポイント
       1. （ア） 経営者が実施すべき対策
          1. （情報セキュリティ保全対策の大枠）

経営者は、 テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、 その内容に応じて見直しを行う。

社内で扱う情報について、 その重要度に応じたレベル分けを行った上で、 テレワークでの利用可否と利用可の場合の取扱方法を定める。

テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、 定期的に教育・啓発活動を実施させる。

情報セキュリティ事故の発生に備えて、 迅速な対応がとれるように連絡体制を整えるとともに、 事故時の対応についての訓練を実施させる。

テレワークにおける情報セキュリティ対策に適切な理解を示した上で、 必要な人材・資源に必要な予算を割り当てる。

* + - 1. （イ） システム管理者が実施すべき対策
         1. （情報セキュリティ保全対策の大枠）

システム全体を管理する重要な立場であることを自覚し、 情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。

情報のレベル分けに応じて、 電子データに対するアクセス制御、 暗号化の要否や印刷可否などの設定を行う。

テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、 定期的に教育・啓発活動を実施する。

情報セキュリティ事故の発生に備えて、 迅速な対応がとれるように連絡体制を確認するとともに、 事故時の対応についての訓練を実施する。

* + - * 1. （悪意のソフトウェアに対する対策）

フィルタリング等を用いて、 テレワーク勤務者が危険なサイトにアクセスしないように設定する。

テレワーク勤務者がテレワーク端末にアプリケーションをインストールする際は申請させ、 情報セキュリティ上の問題がないことを確認した上で認める。

貸与用のテレワーク端末にウイルス対策ソフトをインストールし、 最新の定義ファイルが適用されているようにする。

貸与用のテレワーク端末のＯＳ及びソフトウェアについて、 アップデートを行い最新の状態に保つ。

私用端末をテレワークに利用させる際は、 その端末に必要な情報セキュリティ対策が施されていることを確認させた上で認める。

ランサムウェアの感染に備え、 重要な電子データのバックアップを社内システムから切り離した状態で保存する。

金融機関や物流業者からの事務連絡を装うなどの不審なメールが迷惑メールとして分類されるよう設定する。

* + - * 1. （端末の紛失・盗難に対する対策）

台帳等を整備し、 貸与するテレワーク端末の所在や利用者等を管理する。

* + - * 1. （重要情報の盗聴に対する対策）

テレワーク端末において無線LAN の脆弱性対策が適切に講じられるようにする。

* + - * 1. （不正侵入・踏み台に対する対策）

社外から社内システムへアクセスするための利用者認証について、 技術的基準を明確に定め、 適正に管理・運用する。

テレワーク勤務者がインターネット経由で社内システムにアクセスする際のアクセス方法を定める。 また、 社内システムとインターネットの境界線にはファイアウォールやルータ等を設置し、 アクセス状況を監視するとともに、 不必要なアクセスを遮断する。

社内システムへのアクセス用のパスワードとして、 強度の低いものを用いることができないように設定する。

* + - * 1. （外部サービスの利用に対する対策）

メッセージングアプリケーションを含むＳＮＳに関する従業員向けの利用ルールやガイドラインを整備し、 その中でテレワーク時の利用上の留意事項を明示する。

ファイル共有サービス等のパブリッククラウドサービスの利用ルールを整備し、 情報漏えいにつながる恐れのある利用方法を禁止する。

* + - 1. （ウ） テレワーク勤務者が実施すべき対策
         1. （情報セキュリティ保全対策の大枠）

テレワーク作業中は、 利用する情報資産の管理責任を自らが負うことを自覚し、 情報セキュリティポリシーが定める技術的・物理的及び人的対策基準に沿った業務を行い、 定期的に実施状況を自己点検する。

テレワークで扱う情報について、 定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。

定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組むことで、 情報セキュリティに対する認識を高めることに務める。

情報セキュリティ事故の発生に備えて、 直ちに定められた担当者に連絡できるよう連絡体制を確認するとともに、 事故時に備えた訓練に参加する。

* + - * 1. （悪意のソフトウェアに対する対策）

マルウェア感染を防ぐため、 ＯＳやブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにはアクセスしない。

アプリケーションをインストールする際は、 システム管理者にその旨を申請し、 許可を受けたアプリケーションのみをインストールする。

（私用端末利用の場合）テレワークで利用する端末にインストールするアプリケーションは、 安全性に十分留意して選択する。

作業開始前に、 テレワーク端末にウイルス対策ソフトがインストールされ、 最新の定義ファイルが適用されていることを確認する。

作業開始前に、 テレワーク端末のＯＳ及びソフトウェアについて、 アップデートが適用され最新の状態であることを確認する。

テレワークにはルールに定められた情報セキュリティ対策が適用されているものを使用し、 スマートフォン、 タブレット等に関しては不正な改造（脱獄、 root 化等）を施さない。

テレワーク作業中にマルウェアに感染した場合、 その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、 電子メールの添付ファイルの開封やリンク先のクリックに一層の注意を払う。

* + - * 1. （端末の紛失・盗難に対する対策）

オフィス外に情報資産を持ち出すとき、 その原本を安全な場所に保存しておく。

機密性が求められる電子データを極力管理する必要が無いように業務の方法を工夫する。 やむを得ない場合は必ず暗号化して保存するとともに、 端末や電子データの入った記録媒体（ＵＳＢメモリ等）等の盗難に留意する。

* + - * 1. （重要情報の盗聴に対する対策）

機密性が求められる電子データを送信する際には必ず暗号化する。

無線LAN 利用に伴うリスクを理解し、 テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する。

第三者と共有する環境で作業を行う場合、 端末の画面にプライバシーフィルターを装着したり、 作業場所を選ぶ等により、 画面の覗き見防止に努める。

* + - * 1. （不正侵入・踏み台に対する対策）

社外から社内システムにアクセスするための利用者認証情報（パスワード、 ＩＣカード等）を適正に管理する。

インターネット経由で社内システムにアクセスする際、 システム管理者が指定したアクセス方法のみを用いる。

テレワークで使用するパスワードは、 使い回しを避け、 一定以上の長さで他人に推測されにくいものを用いるように心がける。

* + - * 1. （外部サービスの利用に対する対策）

メッセージングアプリケーションを含むＳＮＳをテレワークで利用する場合、 社内で定められたＳＮＳ利用ルールやガイドラインに従って利用するようにする。

テレワークでファイル共有サービス等のパブリッククラウドサービスを利用する場合、 社内ルールで認められた範囲で利用する。

* + 1. 3. テレワークセキュリティ対策の解説
       1. （ア） 情報セキュリティ保全対策の大枠
          1. １

経営者1

経営者は、 テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、 その内容に応じて見直しを行う。

管理者1

システム全体を管理する重要な立場であることを自覚し、 情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。

勤務者1

テレワーク作業中は、 利用する情報資産の管理責任を自らが負うことを自覚し、 情報セキュリティポリシーが定める技術的・物理的及び人的対策基準に沿った業務を行い、 定期的に実施状況を自己点検する。

＜経営者＞基本対策事項

図10 情報セキュリティポリシーの構成

＜経営者＞推奨対策事項

図 11 情報セキュリティに関するＰＤＣＡサイクル

* + - * 1. ２

経営者2

社内で扱う情報について、 その重要度に応じたレベル分けを行った上で、 テレワークでの利用可否と利用可の場合の取扱方法を定める。

管理者2

情報のレベル分けに応じて、 電子データに対するアクセス制御、 暗号化の要否や印刷可否などの設定を行う。

勤務者2

テレワークで扱う情報について、 定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。

＜経営者・システム管理者＞基本対策事項

＜経営者・システム管理者＞推奨対策事項

図 12 情報のレベル分け

テレワーク トラブル事例 と 対策 〈１〉～情報のレベル分けに関するトラブル事例～

【コラム】 紙媒体での情報の持ち出し

* + - * 1. ３

経営者3

テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、 定期的に教育・啓発活動を実施させる。

管理者3

テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、 定期的に教育・啓発活動を実施する。

勤務者3

定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組むことで、 情報セキュリティに対する認識を高めることに務める。

＜経営者・システム管理者＞基本対策事項

＜テレワーク勤務者＞基本対策事項

図13 情報セキュリティ教育

図14 イントラネットやポスターによる啓発

＜経営者・システム管理者＞推奨対策事項

* + - * 1. ４

経営者4

情報セキュリティ事故の発生に備えて、 迅速な対応がとれるように連絡体制を整えるとともに、 事故時の対応についての訓練を実施させる。

管理者4

情報セキュリティ事故の発生に備えて、 迅速な対応がとれるように連絡体制を確認するとともに、 事故時の対応についての訓練を実施する。

勤務者4

情報セキュリティ事故の発生に備えて、 直ちに定められた担当者に連絡できるよう連絡体制を確認するとともに、 事故時に備えた訓練に参加する。

＜経営者・システム管理者・テレワーク勤務者＞基本対策事項

＜経営者・システム管理者・テレワーク勤務者＞推奨対策事項

* + - * 1. ５

経営者5

テレワークにおける情報セキュリティ対策に適切な理解を示した上で、 必要な人材・資源に必要な予算を割り当てる。

＜経営者＞基本対策事項

* + - 1. （イ） マルウェアに対する対策
         1. ５

管理者5

フィルタリング等を用いて、 テレワーク勤務者が危険なサイトにアクセスしないように設定する。

勤務者5

マルウェア感染を防ぐため、 ＯＳやブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにはアクセスしない。

＜テレワーク勤務者＞基本対策事項

＜システム管理者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈２〉～マルウェア感染に関するトラブル事例～

* + - * 1. ６

管理者6

テレワーク勤務者がテレワーク端末にアプリケーションをインストールする際は申請させ、 情報セキュリティ上の問題がないことを確認した上で認める。

勤務者6

アプリケーションをインストールする際は、 システム管理者にその旨を申請し、 許可を受けたアプリケーションのみをインストールする。

（私用端末利用の場合）テレワークで利用する端末にインストールするアプリケーションは、 安全性に十分留意して選択する。

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈３〉～ウイルス対策ソフトに関するトラブル事例～

* + - * 1. ７

管理者7

貸与用のテレワーク端末にウイルス対策ソフトをインストールし、 最新の定義ファイルが適用されているようにする。

勤務者7

作業開始前に、 テレワーク端末にウイルス対策ソフトがインストールされ、 最新の定義ファイルが適用されていることを確認する。

＜システム管理者＞基本対策事項

＜テレワーク勤務者＞基本対策事項

テレワーク トラブル事例 と 対策 〈４〉～アプリケーション利用に関するトラブル事例～

【コラム】 次世代ウイルス対策ソフト

* + - * 1. ８

管理者8

貸与用のテレワーク端末のＯＳ及びソフトウェアについて、 アップデートを行い最新の状態に保つ。

勤務者8

作業開始前に、 テレワーク端末のＯＳ及びソフトウェアについて、 アップデートが適用され最新の状態であることを確認する。

＜システム管理者＞基本対策事項

＜テレワーク勤務者＞基本対策事項

テレワーク トラブル事例 と 対策 〈５〉～アップデートに関するトラブル事例～

* + - * 1. ９

管理者9

私用端末をテレワークに利用させる際は、 その端末に必要な情報セキュリティ対策が施されていることを確認させた上で認める。

勤務者9

テレワークにはルールに定められた情報セキュリティ対策が適用されているものを使用し、 スマートフォン、 タブレット等に関しては不正な改造（脱獄、 root 化等）を施さない。

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

* + - * 1. 10

管理者10

ランサムウェアの感染に備え、 重要な電子データのバックアップを社内システムから切り離した状態で保存する。

＜システム管理者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈６〉～ランサムウェアに関するトラブル事例～

* + - * 1. 11

管理者11

金融機関や物流業者からの事務連絡を装うなどの不審なメールが迷惑メールとして分類されるよう設定する。

勤務者10

テレワーク作業中にマルウェアに感染した場合、 その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、 電子メールの添付ファイルの開封やリンク先のクリックに一層の注意を払う。

＜テレワーク勤務者＞基本対策事項

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

【コラム】 社内SNS の利用

テレワーク トラブル事例 と 対策 〈７〉～不審メールに関するトラブル事例～

* + - 1. （ウ） 端末の紛失・盗難に対する対策
         1. 11

勤務者11

オフィス外に情報資産を持ち出すとき、 その原本を安全な場所に保存しておく。

【対象】パターン⑥（会社PC の持ち帰り方式）

＜テレワーク勤務者＞推奨対策事項

* + - * 1. 12

管理者12

台帳等を整備し、 貸与するテレワーク端末の所在や利用者等を管理する。

勤務者12

機密性が求められる電子データを極力管理する必要が無いように業務の方法を工夫する。 やむを得ない場合は必ず暗号化して保存するとともに、 端末や電子データの入った記録媒体（ＵＳＢメモリ等）等の盗難に留意する。

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈８〉～端末の紛失に関するトラブル事例～

* + - 1. （エ） 重要情報の盗聴に対する対策
         1. 13

勤務者13

機密性が求められる電子データを送信する際には必ず暗号化する。

＜テレワーク勤務者＞基本対策事項

テレワーク トラブル事例 と 対策 〈９〉～公衆無線LAN 利用に関するトラブル事例～

* + - * 1. 13

管理者13

テレワーク端末において無線LAN の脆弱性対策が適切に講じられるようにする。

勤務者14

無線LAN 利用に伴うリスクを理解し、 テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する。

＜テレワーク勤務者＞基本対策事項

＜テレワーク勤務者＞推奨対策事項

図16 無線LAN 利用上のリスク

* + - * 1. 15

勤務者15

第三者と共有する環境で作業を行う場合、 端末の画面にプライバシーフィルターを装着したり、 作業場所を選ぶ等により、 画面の覗き見防止に努める。

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈１０〉～画面の覗き見に関するトラブル事例～

* + - 1. （オ） 不正アクセスに対する対策
         1. 16

管理者14

社外から社内システムへアクセスするための利用者認証について、 技術的基準を明確に定め、 適正に管理・運用する。

勤務者16

社外から社内システムにアクセスするための利用者認証情報（パスワード、 ＩＣカード等）を適正に管理する。

【対象】パターン①（リモートデスクトップ方式）、 パターン②（仮想デスクトップ方式）、 パターン⑤（アプリケーションラッピング方式）、 パターン⑥（会社PC の持ち帰り方式）

＜システム管理者＞基本対策事項

＜テレワーク勤務者＞推奨対策事項

* + - * 1. 17

管理者15

テレワーク勤務者がインターネット経由で社内システムにアクセスする際のアクセス方法を定める。 また、 社内システムとインターネットの境界線にはファイアウォールやルータ等を設置し、 アクセス状況を監視するとともに、 不必要なアクセスを遮断する。

勤務者17

インターネット経由で社内システムにアクセスする際、 システム管理者が指定したアクセス方法のみを用いる。

＜システム管理者＞基本対策事項

図17 ファイアウォールの設置

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈１１〉～「踏み台」に関するトラブル事例～

* + - * 1. 18

管理者16

社内システムへのアクセス用のパスワードとして、 強度の低いものを用いることができないように設定する。

勤務者18

テレワークで使用するパスワードは、 使い回しを避け、 一定以上の長さで他人に推測されにくいものを用いるように心がける。

＜システム管理者＞基本対策事項

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

図 18 アカウントのパスワード管理

【コラム】 パスワードの管理方法

テレワーク トラブル事例 と 対策 〈１２〉～パスワード管理に関するトラブル事例～

【コラム】 ID・パスワードをブラウザに記憶させても大丈夫？

* + - 1. （カ） 外部サービスの利用に対する対策
         1. 19

管理者17

メッセージングアプリケーションを含むＳＮＳに関する従業員向けの利用ルールやガイドラインを整備し、 その中でテレワーク時の利用上の留意事項を明示する。

勤務者19

メッセージングアプリケーションを含むＳＮＳをテレワークで利用する場合、 社内で定められたＳＮＳ利用ルールやガイドラインに従って利用するようにする。

＜システム管理者・テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈１３〉～SNS 利用に関するトラブル事例～

* + - * 1. 20

管理者18

ファイル共有サービス等のパブリッククラウドサービスの利用ルールを整備し、 情報漏えいにつながる恐れのある利用方法を禁止する。

勤務者20

テレワークでファイル共有サービス等のパブリッククラウドサービスを利用する場合、 社内ルールで認められた範囲で利用する。

＜システム管理者＞基本対策事項

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈１４〉～パブリッククラウド利用に関するトラブル事例～

* + 1. 用語集
    2. 参考リンク集
       1. テレワークではじめる働き方改革 テレワークの導入・運用ガイドブック（厚生労働省）
          1. http://work-holiday.mhlw.go.jp/material/pdf/category7/01\_01.pdf
          2. 厚生労働省と総務省による3 年間の実証事業を通じて得られた知識、 ノウハウをもとに、 テレワークによる効果、 テレワークを導入した場合の労務管理の仕方や労務管理ツールの利用方法、 セキュリティを確保したICT システム・ツールの選択方法等やその手順を紹介しています。
       2. サイバーセキュリティ経営ガイドライン（経済産業省）
          1. http://www.meti.go.jp/policy/netsecurity/mng\_guide.html

ドキュメントを参照: [mng\_guide.html](http://www.meti.go.jp/policy/netsecurity/mng_guide.html)

* + - * 1. 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のある「3 原則」、 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担当幹部（CISO 等）に指示すべき「重要10 項目」をまとめたものです。
      1. 中小企業の情報セキュリティ対策ガイドライン（独立行政法人情報処理推進機構）
         1. https://www.ipa.go.jp/security/keihatsu/sme/guideline/

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - * 1. 中小企業にとって重要な情報を漏えいや改ざん、 喪失などの脅威から保護することを目的とする情報セキュリティ対策の考え方や実践方法について説明するもので、 本編2 部構成と、 「5 分でできる！情報セキュリティ自社診断シート」を含む7 種類の付録で構成されています。
      1. SECURITY ACTION（独立行政法人情報処理推進機構）
         1. https://www.ipa.go.jp/security/security-action/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/security-action/index.html)

* + - * 1. 上述の「中小企業の情報セキュリティガイドライン」の付録に示されている情報セキュリティ対策に取り組むことを自己宣言することで、 「SECURITY ACTION」ロゴマークを自社の名刺、 封筒、 会社案内、 ウェブサイト等に表示させることができ、 自社の取組を対外的にアピールすることができます。
      1. 情報セキュリティ理解度チェック（NPO 日本ネットワークセキュリティ協会）
         1. http://slb.jnsa.org/eslb/

ドキュメントを参照: [eslb](http://slb.jnsa.org/eslb/)

* + - * 1. 自社の従業員における情報セキュリティの理解度がどの程度かを把握する仕組みを提供しています。 チェックの対象は「電子メールに関する知識」「インターネットの利用法」「ウイルスに関する知識」「パスワードの管理」などテレワークでも有用な知識を幅広く扱っています。
        2. 基本的な機能の利用は無料ですが、 機能強化した有料版もあります。
      1. 経営と IT 化相談窓口（NPO IT コーディネータ協会）
         1. https://www.itc.or.jp/management/diagnosis/

ドキュメントを参照: [diagnosis](https://www.itc.or.jp/management/diagnosis/)

* + - * 1. 中小企業が抱える経営課題の解決支援のため、 中小企業支援に関する専門知識や豊富な実績を有する人材として資格認定されたIT コーディネータを紹介する窓口です。
      1. 情報処理安全確保支援士制度（独立行政法人情報処理推進機構）
         1. https://www.ipa.go.jp/siensi/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/siensi/index.html)

* + - * 1. サイバーセキュリティに関する専門的な知識・技能を有する人材である情報処理安全確保支援士の登録制度が平成29 年度に開始されました。 上記ウェブサイトにて登録された情報処理安全確保支援士の得意分野や連絡先等の情報を参照することができます。
  1. ●導入事例　大分県庁　【Soliton】

ドキュメントを参照: [pref-oita.html](https://www.soliton.co.jp/case_study/pref-oita.html)

* 1. NISTガイドライン
     1. Mobile Device Security: Cloud and Hybrid Builds
        1. Executive Summary

ドキュメントを参照: [mds-nist-sp1800-4a-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4a-draft.pdf)

* + - 1. Approach, Architecture, and Security Characteristics

ドキュメントを参照: [mds-nist-sp1800-4b-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4b-draft.pdf)

* + - 1. How-To Guide

ドキュメントを参照: [mds-nist-sp1800-4c-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4c-draft.pdf)