Sec01-01-02\_「中小企業向けサイバーセキュリティ対策の極意」 【電子書籍（Web版）】での発信情報【目次案】

# 改訂履歴

## 【2020年8月25日】Sec01-01-03と整合

## 【2020年8月14日】0.3版「本文」を別ファイル化

## 【2020年8月14日】0.2版提出

## 【2020年8月3日】0.1版提出

## 【2020年7月21日】全体調整

## 【2020年7月9日】全体調整

## 【2020年7月3日】

## 【2020年6月23日16:00版】修正すべき項目の再構成

## 【2020年6月19日】検討メモ反映

## 【2020年6月15日】最新動向関連加筆

## 【2020年6月12日】全体目次項目調整結果

## 【2020年6月11日19:00版】全体目次項目を精査中

## 【2020年6月9日】全体目次項目再構成

## 【2020年6月4日】全体構成見直し、リナンバリング、目次候補洗い出し、ポータルでの公開内容加筆

## 【2020年6月2日】目次内容再構成

## 【2020年5月28・29日】Sec01-01-01の内容をマージし、記載のポイントとなる事項を追記【未完】

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-01.html>;

## 【2020年5月25日】ビジネスを発展させるために（攻めのIT投資とサイバーセキュリティ対策）への追加項目の検討

## 【2020年4月29日】目次構成再整理

## 【2020年3月25日】サイバーセキュリティ経営ガイドライン実践状況ツールを追加

## 【2020年3月17日】Sec01-01-01\_「中小企業向けサイバーセキュリティ対策の極意」の改訂 （追補資料の作成） から分離

# リンク

## html版

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02.html>;

## MindManager版（Download）

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02_「中小企業向けサイバーセキュリティ対策の極意」の改訂案（素材）.mmap>;

## EXCEL版（Download）

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02.xlsx>;

## Docx版（Download）

[Page not found &middot; GitHub Pages](https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02.docx);

# 凡例

## 目次掲載項目

## 冊子体及び冊子体ベースWebページ

## 既存項目（見出し・項番等の軽微な修正は含む）

## 追加項目（大きな修正を含む）

## 担当

## 改訂箇所

## 参考資料

# 情報収集・整理業務と本資料の位置づけ

## Webポータルサイト内「サイバーセキュリティ対策情報の書庫」「ナレッジデータベース」「アーカイブ」を公開

### 専門員が収集した情報を体系的に整理し、ナレッジデータベースとして公開する

## Webポータルサイト内で、電子書籍版「中小企業向けサイバーセキュリティ対策の極意」、その他普及啓発資料を公開

### 「サイバーセキュリティ対策情報の書庫」から、普及啓発の目的・媒体に応じて情報を選別・編集し提供内容の材料を提示する

## 冊子体版「中小企業向けサイバーセキュリティ対策の極意」を印刷発行

### 本資料は、電子書籍版「中小企業向けサイバーセキュリティ対策の極意」の内容をイラスト化、コピーリライトする形で、読みやすい読本を提示する

* + - * 1～2年の間に大きく変動しない内容
      * 数年先の社会の動向（市場動向）、IT関連の技術動向を想定する
      * 中小企業の経営者向けとしての狙い
        + 現時点においてはITリテラシーがあまり高くなくても、今後はITの活用が重要性を理解し、 そのためにセキュリティ対策もしっかり行う必要があると認識できるように

## ポータルサイトでの情報発信の想定

### 中小企業の経営者向け必要最小限の情報提供

* + - * 「極意」（Webでの都度更新版）
        + html版
        + EPUB版
        + PDF版
      * 極意（冊子体としての固定版）
        + 冊子体の紹介
        + 冊子体イメージPDF

### 中小企業向けのサイバーセキュリティ対策 に関する体系的な情報発信⇒2021年度に充実

* + - * 中小企業が事業を継続・発展させるためのIT化において、認識すべきサイバーセキュリティ関連の情報へ、 的確にナビゲートするための情報提供
        + 体系的・網羅的に情報を整理。相談者、相談対応者が共に参照しあえる情報
        + 【参考】

※専門員が日々蓄積した知識から抜粋

Sec01-08-5【成果物】専門員業務ハンドブック【目次】

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-08-5.html>;

* + - * + ※IPA「ここからセキュリティ」の一般向け、中小企業向けのリンク先を含む

### 【参考】

* + - * ※ポータルサイトでのページ構成案
      * Sec01-08-2 専門員の所掌業務及び調査分析項目

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-08-2.html>;

# 改訂理由

## 国のサイバーセキュリティ関連法規、施策対応

### サイバーセキュリティ基本法の改正（2019年4月1日施行）対応

### サイバーセキュリティ戦略2018(2018年7月)

* + - * 今後3年間の基本的な計画として策定

### サイバーセキュリティ2020（2020年7月）

* + - * （2019年度報告・2020年度計画）

## 「サイバーセキュリティ経営ガイドライン2.0対応

## 中小企業の情報セキュリティ対策ガイドライン第3版対応

## IPA・NISC等のガイドラインの改訂対応

## ITの最新トレンド対応

### 積極的にITを活用しないとビジネスの継続が困難になる。ITを活用するためにはセキュリティ対策が必須

## サイバーセキュリティ脅威の最新トレンド対応

## 制度・施策の改訂対応

## 関連法規の改正対応

## 新しい生活様式への移行対応

## テレワークの継続化

## ＜全般＞

### 経営者、CISOを対象読者としていることから、冗長な表現を見直し、全体の記載を簡素化。

### 改訂箇所：改訂部分は同時に表現も見直す

# 目次ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー

## 【Mission0】 はじめに

### ケーススタディー１：なぜ、こんな小さな会社が狙われたの？

### ケーススタディー２：ある日突然、銀行口座の預金残高が消えた！

* + - * 人員不足〜以下囲みコラムの平成２７年度―平成XX年度の最新に更新⇒数字のみ修正

### ケーススタディー３：取引先企業への踏み台にされた

* + - * サプライチェーン紹介のページへのリンク

### ケーススタディー４：EMOTET、ランサムウェアの被害にあった？

### ケーススタディー5：BEC攻撃事例⇒海外の取引先からのメール

* + - * 海外からのメールを事例に

### ケーススタディーX：サプライチェーンセキュリティの必要性が高まっていること

### ケーススタディーX：セキュリティ対策を怠ると他社に迷惑をかけることもあるケーススタディーX：

### ケーススタディー6：昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について」

* + - * 【2020年6月12日METI】等を参考に。

### ケーススタディー7：サイバーセキュリティ保険に入っていれば

### ツイッター被害 乗っ取り、詐欺悪用相次ぐ

### サイバー被害 通知義務化 個人情報漏洩の全員に　企業の対応不可避

### 改訂箇所

* + - * 「サイバーセキュリティ経営ガイドライン・概要＞の説明を全体的に修正。
      * IoTやAIの活用といった最近の情勢を踏まえる

## 【はじめに】

### 改訂の趣旨を記述

## 【この冊子の使い方】

## 【目次】

## 【Mission1】　知っておきたいサイバー攻撃の知識

### 1-1：標的型攻撃による情報流出

### 1-2：ランサムウェアを使った詐欺・恐喝

* + - * 【囲みコラム】「No More Ransam」　の紹介

### 1-3：Webサービスからの個人情報窃取

* + - * 【囲みコラム】割賦販売法の改定とクレジットカードのセキュリティ

### 1-4：集中アクセスによるサービス停止

* + - * 【囲みコラム】内容更新

### 1-5：内部不正による情報漏えいと業務停止

* + - * 2016年の損害額を最新に

### 1-6：Webサイトの改ざん

### 1-7：インターネットバンキングの不正送金

* + - * 【囲みコラム】不正送金を阻止するには

### 1-8：悪意のあるスマホアプリ

* + - * グラフ最新化
      * 【囲みコラム】スマートフォン決済不正アプリ

### 1-9：巧妙・悪質化するワンクリック詐欺

### 1-10：Webサービスへの不正ログイン

* + - * 【囲みコラム】不正ログインを…多要素認証の取り込み（NIST800-63-3対応）

### 1-11：公開された脆弱性対策情報の悪用

### 1-12：IoT機器を踏み台にした攻撃

* + - * 【囲みコラム】対策はこれだ…NICT　「NOTICE」の実証事例の結果を追加
      * 【囲みコラム】IoTとデータ利活用の全体像【総務省】

<https://www.soumu.go.jp/ict_skill/pdf/ict_skill_1_1.pdf>;

### 1-13：中小企業におけるサイバー攻撃被害の例

### 1-14：なりすましECサイトの被害と回避策

* + - * 事業者サイド
      * 利用者サイド

### 1-15：ビジネスメール詐欺の被害と回避策

### 【削除】おさらいクイズ

## 【Mission2】　すぐやろう！対サイバー攻撃アクション

### 改訂のポイント

* + - * EPUB、Web版は、情報セキュリティ10大脅威レベルでリライトするか？

### 2-1：サイバー攻撃に対して何ができるか

### 2-2：OSとソフトウェアのアップデート

* + - * OSサポート状況の注記更新

### 2-3：ウイルス対策ソフト・機器の導入

### 2-4：定期的なバックアップ

* + - * OneDrive等クラウドストレージの利用

### 2-5：パスワードの管理

* + - * 【囲みコラム】電子的認証に関するガイドライン（NIST800-63-3対応）

### 2-6：アクセス管理

### 2-7：紛失や盗難による情報漏えい対策

* + - * 【囲みコラム】Wifi利用者向け簡易マニュアル【総務省】

### 2-8：持ち込み機器対策

* + - * テレワーク等での持ち出し・持ち込み機器対策

### 2-9：電子メールの安全利用

### 2-10：標的型攻撃メールへの対応

* + - * 事例は新規に

### 2-11：迷惑メール発信への対応

### 2-12：安全なWebサイト利用

* + - * 【囲みコラム】詐欺サイトはこれ…内容更新する（NISC,IPAの資料参照）

### 2-13：閲覧制限

* + - * 【囲みコラム】中小企業の規制は…事例を更新再調査

### 2-14：重要情報の洗い出し

### 2-15：重要情報の保管

### 【削除】おさらいクイズ

## 【Mission03-A】経営者は事前に何を備えればよいのか【守りの対策】

### サイバーセキュリティ対策は、事業継続を脅かすリスクの１つ。

* + - * 3-1：サイバーセキュリティ対策が経営に与える重大な影響
      * 3-2：サイバー攻撃を受けると企業が被る不利益
      * 3-3：経営者に問われる責任
        + 【削除】【囲みコラム】情報管理が不適切な場合に問われる法律
      * 【Web版コラム】組織の姿勢3分類(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】より)

<https://www.nisc.go.jp/conference/cs/jinzai/wg/index.html>;

### 投資効果（費用対効果）を認識する

* + - * 3-4：投資効果（費用対効果）を認識する
        + 【囲みコラム】数値の見直し

### 【自社の対策状況把握】自社のIT活用・セキュリティ対策状況を自己診断する

* + - * 3-5：ITの活用診断
        + DX推進指標　自己診断結果分析レポート（IPA）の「背景」を参照
      * 3-6：サイバーセキュリティ投資診断
      * 3-7：情報セキュリティ対策診断

### ビジネスを継続するために（守りのIT投資とサイバーセキュリティ対策）

* + - * 3-8：業務の効率化、サービス維持のために
      * 【コラム】テレワークの導入・運用ガイドブック
        + 【コラム】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】
        + 【コラム】テレワークセキュリティガイドライン（第4版）【総務省】
      * 【Web版コラム】
        + 【Web版コラム】生産性向上のための「デジタル・ワークプレイス」
        + 【Web版コラム】電子印鑑の活用
        + 【Web版コラム】私用端末のビジネス利用(BYOD)
      * 3-9：経営者が意識すべきサイバーセキュリティ経営3原則
        + 【参考】経営者が認識すべき「3原則 【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】
      * 3-10：経営者がやらなければならないサイバーセキュリティ経営の重要10項目
        + 経営者からCISOへの10項目の指示

「サイバーセキュリティ経営ガイドライン」Ver2.0の重要10項目の分類及び内容の改訂に伴う記述の加筆訂正

【参考】Sec01-04-1サイバーセキュリティ経営ガイドライン新旧対応関係【2017年12月6日】

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-04-1.html>;

* + - * 【Web版コラム】
        + 【Web版コラム】サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版
        + 【Web版コラム】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

<https://www.ipa.go.jp/files/000072309.pdf>;

## 【Mission03-B】経営者は事前に何を備えればよいのか【攻めの対策】

### ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

* + - * 【持続的発展のため】組織の発展を目指した戦略的なIT活用とサイバーセキュリティ対策
      * 3-11：次世代技術を活用したビジネス展開
        + 【要旨】DX時代→中小も対応しないと→対応するには新たなセキュリティ対策も
        + すでにデジタルトランスフォーメーション(デジタル変革)は始まっている
        + 「攻めのIT経営中小企業百選」事例⇒ IPAのDXへの取組を取り込む （６月１０日付　「DX推進に向けた文書を公開」参照）
      * 【Web版コラム】攻めの姿勢の企業向け
        + 【Web版コラム】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
        + 【Web版コラム】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【NISC】

<http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf>;

* + - * + 【Web版コラム】IT活用の必然性
        + 【Web版コラム】ITを活用したサービスを継続するためには、 情報セキュリティ対策は必須
        + 【Web版コラム】次世代サービス、 技術の利用に当たってのサイバーセキュリティ対策
        + 【Web版コラム】サイバーセキュリティ分野で機械学習が活用される背景と期待
      * 【コラム】DXレポート（ITシステム2025年の崖の克服
        + 【参考】DAX21\_デジタルトランスフォーメーション（DX）

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX21.html>;

* + - * 【Web版コラム】攻めのIT投資対応、Society5.0時代に必要なセキュリティ対策
        + 【Web版コラム】IoT関連セキュリティ対応
        + 【Web版コラム】クラウドサービスとセキュリティ
        + 【Web版コラム】５Gセキュリティ対応
        + 【Web版コラム】BYODセキュリティ対応
        + 【Web版コラム】APIセキュリティ
        + 【Web版コラム】ブロックチェーンにおけるセキュリティ
        + 【Web版コラム】インターネットアクセスにおけるセキュリティの新技術
        + 【Web版コラム】IDと認証セキュリティ
        + 【Web版コラム】AIが人間をアシストする「インテリジェント・ワークプレイス」の活用におけるサイバーセキュリティ対策
      * 3-12～14：活用すべき次世代技術要素と活用の留意点
        + 【要旨】Society5.0とは？インダストリー4.0とは？ クラウドコンピューティング, IoT, ビッグデータ, AI,ロボット,5G等の新たなIT活用が、中小企業においても必要
        + 3-12：IoT、ビッグデータ、AI、ロボットの活用
        + 3-13：IoTが果たす役割と効果
        + 3-14：人工知能（AI）が果たす役割と効果
        + 【コラム】クラウドサービスのメリットは？
        + 【コラム】クラウドサービス導入の留意点
        + 【コラム】クラウドサービスの活用
      * 3-15～16：次世代技術の活用に当たってのサイバーセキュリティの留意点
        + 3-15：IoTを活用する際のサイバーセキュリティ上の留意点
        + 3-16：IoTを活用する一般利用者のための基本ルール

【要旨】IoT, ビッグデータ, AI, ロボット等の新たなIT活用におけるサイバーセキュリティ対策

【コラム】IoT活用企業におけるプライバシー保護に関する考慮事項とは | PwC Japanグループ

【コラム】サイバー・フィジカル・セキュリティ対策フレームワーク対応

【コラム】サプライチェーン全体での対策（中小企業向け）

【コラム】NIST SP800-171 「連邦政府外のシステムと組織における管理された非格付け情報の保護」 改訂Revishon2対応

【コラム】NIST SP800-53 「連邦政府情報システムおよび連邦組織のための セキュリティ管理策とプライバシー管理策」改訂Rev4.0対応

### 【削除】おさらいクイズ

## 【Mission4】　もしもマニュアル

### 【はじめに】サイバーセキュリティ経営ガイドラインVer.2.0の重要10項目とリンクした表現に

### 4-1：緊急事態応用マニュアルの作成

### 4-2：基本事項の決定

### 4-3：漏えい・流出発生時の対応

### 4-4：改ざん・消失・破壊・サービス停止発生時の対応

### 4-5：ウイルス感染時の初期対応

### 4-6：届け出および相談

### 4-7：大規模災害などによる事業中断と事業継続管理

* + - * 事業継続計画（BCP）の一環としてのサイバーセキュリティ対策（明文化）

### 【削除】ワークショップ

## 【Mission5】　やってみよう！サイバー攻撃対策シミュレーション

### 5-1：サイバー攻撃前夜

### 5-2：攻撃発生その瞬間

### 5-3：サイバー攻撃直後

### 5-4：潜入拡大

### 5-5：顧客への被害拡大 取引先への被害拡大

### 5-6：サイバー攻撃の発覚

### 5-7：原因が判明 ウイルス感染が原因

### 5-8：再発防止策の作成

### 5-9：復旧回復

### 5-10：EMOTET、ランサムウェア対策

## 【Information7】　インフォメーション

### 6-1：もしかしてサイバー攻撃？ここに連絡を！

* + - * 警視庁、IPA、東京都？、、？

### 6-2：やられる前に、しっかり予防を！

* + - * 「相談・届出先クイックリスト」から抜粋

<https://bluemoon55.github.io/Presentation_Doc/Cyber/相談・届出先クイックリスト（張り紙用）.pdf>;

### 6-4⇒削除：情報セキュリティ用語解説

### 6-3：セキュリティお役立ちリンク

* + - * 主な文献のリストアップと複数文献を典拠とした内容の要約を纏める

### 【Web版コラム】

* + - * 【Web版コラム】セキュリティお役立ちリンク【詳細版】
      * 【Web版コラム】サイバーセキュリティ経営チェックシート
      * 【Web版コラム】IoT機器調査及び利用者への注意喚起プロジェクト（NOTICE対応）
      * 【Web版コラム】システム管理者としての基本技術の解説
      * 【Web版コラム】経営者向けサイバーセキュリティ経営のための啓発資料

### 6-4：中小企業の情報セキュリティ対策ガイドライン【第3版】

* + - * 6-4：はじめに、経営者編、実践編
        + 「中小企業の情報セキュリティ対策ガイドライン第3版」の位置づけ、全体、活用方法、構成目次と要約を引用。IPAのページへリンク
      * 6-4：情報セキュリティ5か条
      * 6-4：情報セキュリティ基本方針サンプル
      * 6-4：新・5分でできる自社診断シート
      * 6-4：情報セキュリティハンドブックひな形（従業員向け）
      * 6-4：情報セキュリティ関連規程（ポリシー）の明文化
      * 6-4：リスク分析シート
        + 6-4：情報資産管理台帳の作成
      * 6-5：中小企業のためのクラウドサービス安全利用の手引き

### 6-6：IT人材育成・人材確保

* + - * iコンピテンシ・ディクショナリ(iCD)
      * 情報処理技術者試験制度

### 6-7：情報管理が不適切などの場合の処罰など（4ページ程度）

* + - * 制度・施策
      * 関係法令：法律違反の可能性への対応方法の解説

## 【付録】

### 付-2：主な参考文献（2ページ程度）

* + - * 典拠となる文献情報の更新

### 付-3：用語解説インデックス（4ページ程度）

* + - * 新しい用語の解説及び本文へのリンク

# 本編ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー

## Sec01-01-03\_「中小企業向けサイバーセキュリティ対策の極意」【本文案】

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-01-03.html>;