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）

ドキュメントを参照: 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）.html

改訂履歴

【2020 年 4 月 9 日】担当割記載
【2020 年 3 月 17 日】Sec01-01-02 を分離
【2020 年 1 月 28 日】Sec010-08-7 から分離
（2019 年 7 月 25 日）（「中小企業向けサイバーセキュリティ対策の極意」で 改訂もしくは追記すべき内容の調査と原稿作成）

リンク

html 版
ドキュメントを参照: 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）.html
MindManager 版（Download）
ドキュメントを参照: 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）.mmap
【旧版】xmind⇒html 版
ドキュメントを参照: 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）.html
Docx 版（Download）
ドキュメントを参照: 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）.docx

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 2019（2019 年 5 月 23 日）
（2018 年度報告・2019 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
参照: 「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

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
参照: 「中小企業の情報セキュリティ対策ガイドライン第 3 版」のリスク分析の位置付けの変更

IPA・NISC 等のガイドラインの改訂対応

サイバーセキュリティ脅威の最新トレンド対応

IT の最新トレンド対応
参照: IT 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

＜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

改訂箇所

フローティングトピック

はじめに

＜冒頭の説明の見直し＞

改訂箇所：「はじめに」(p.8～9)を改訂

「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ふまえるとともに、 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や、 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等についても言及。

【Mission01】知っておきたいサイバー攻撃の知識

＜統計データのアップデート＞

改訂箇所：「はじめに」,Mission1-13(p.8～9,42～43)を改訂

１． １節「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」で 参照している統計データをアップデート。それに伴い説明文も修正。

なりすまし EC サイトの被害と回避策の記述の充実

改訂箇所：Mission1-12　(P.41)のあとに追加

事業者サイド

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【2018 年 5 月 IPA】

ドキュメントを参照: 000066952.pdf

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】

利用者サイド

ビジネスメール詐欺の被害と回避策の記述の充実

改訂箇所：Mission1-12　(P.41)のあとに追加

【Mission02】すぐやろうサイバー攻撃アクション

【Mission03】経営者は事前に何を備えればよいのか

「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

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】

ドキュメントを参照: 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】.html

改訂箇所：Mission3-10 (p.98～109)を改訂

ガイドライン改訂前の主な課題

昨今のサイバー攻撃の巧妙化により入口出口対策などの事前対策だけでは対処が困難。

米国のサイバーセキュリティフレームワークでも事前対策だけでなく、事後（検知、対応、復旧）対策を要求。

一方で従来のガイドラインは CSIRT の構築などの「対応」に関する項目はあるものの、 「検知」や「復旧」に関する内容が弱く、国際的な状況を踏まえるとガイドラインとの整合性が不十分。

ポイント（経産省発表）

ドキュメントを参照: 20180309_Hiroshi_itou.pdf

重要 10 項目の整理

新規に 2 項目（(5)対策実施と(8)復旧）追加するとともに、既存の項目を再整理。

重要１０項目の並びについても、３原則、及び作業の時系列を意識して再整理。

(7)の参考資料として付録 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」を新規に追加。

事後対策の強化 ～検知・復旧対策の実施～

重要項目 指示 5 として「攻撃の検知」に関する、「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」を追加

重要項目 指示 8 として「復旧」に関する、「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」を追加

サプライチェーン対策の強化

重要項目 指示 9 の「サプライチェーンのビジネスパートナーや委託先等を含めたサイバーセキュリティ対策の実施及び状況把握」において、 委託先におけるリスクマネーの確保や委託先の組織としての活用の把握（ISMS や SECURITY ACTION） 等の留意点を追記

セキュリティ要件を満たさない事業者、製品、サービスはグローバルサプライチェーン、国内サプライチェーンからはじき出されるおそれ

事後対策の強化 ～インシデント発生時の対応～

インシデント発生時に組織として調査しておくべき事項をまとめた付録 C を追加

＜情報共有活動における情報提供の記載を強調＞

重要 10 項目の（10）において、従来は「情報の入手とその有効活用」となっていた部分を「情報の提供、 及び入手とその有効活用」に修正。

「中小企業の情報セキュリティ対策ガイドライン第 3 版」のリスク分析の位置付けの変更

改訂箇所：Mission3-17～20, Information6-6　(P.124～131,180～183)を改訂

4 IT の最新トレンド対応

デジタル・トランスフォーメーション(DX)時代に、「ビジネスを発展させるために」（攻めの IT 投資）に活用すべき IT と 活用におけるサイバーセキュリティ対策（Society5.0 時代のサイバーセキュリティ対策）

改訂箇所：Mission3-11,コラム(p.110～131)を改訂、必要に応じて追加

5 Society5.0 時代に必要なセキュリティ対策

ディープラーニング、ロボット、ビッグデータ、IoT、クラウドサービス等の技術の活用の必要性と、活用におけるセキュリティ対策の記述の充実

IoT 関連セキュリティ対応

【担当：早出】

NIST SP.800-82R2　Guide to Industrial Control Systems (ICS) Security　【再掲】

IoT セキュリティ　標準／ガイドライン　ハンドブック　2017 年度版【2018 年 5 月 8 日 JNSA】

コンシューマ向け IoT セキュリティガイド【2016 年 8 月 1 日 JNSA】

IoT（ICS）サイバーセキュリティ対策ガイド編

1.フィジカルセキュリティスコープ

2.IoT リスクアセスメント

3.IoT サイバーセキュリティ攻撃のシナリオ

4.セキュリティ対策/ベストプラクティス

5.セキュリティギャップ分析

6.IoT セキュリティインシデント事例

7.IoT セキュリティ基準と参考資料

8.IoT セキュリティのプレイヤー

9.（参考情報）

BCP とサイバーセキュリティ

クラウドサービス

各種クラウドサービス

クラウドセキュリティ

クラウドサービス利用のための情報セキュリティマネジメントガイドライン 2013 年度版【METI】

クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）2018 年 7 月【総務省】

5 G セキュリティ対応

【担当：早出】

BYOD セキュリティ対応

Mobile Device Security Corporate-Owned Personally-Enabled (COPE)【NIST SPECIAL PUBLICATION 1800-21】対応

【担当：早出】

API セキュリティ

ブロックチェーンにおけるセキュリティ

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

ID と認証セキュリティ

【担当：中山】

利便性とセキュリティの両立へ向けた新たな動向

FIDO(Fast Identity Onlinbe)

パスワードに代わる認証手段として、指紋や顔画面などを活用した生体認証や、 認証結果を完全にやりとりできる「FIDO」の普及が期待されている

モバイル認証（GSMA Mobile Connect）

携帯電話を Web サービス全般の汎用的な認証手段として利用するための「Mobile Connect」が注目されている

認証セキュリティと NIST SP 800-63 の改定

「パスワードは定期変更すべき」「パスワードは複数の」文字種で混成すべき」などの、 従来は常識とされてきた対策についても、実効性や技術の進展に合わせた見直しが図られてる

5 攻めの IT 投資対応

改訂箇所：Mission3-11,コラム(p.110～131)に追加

5 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

AI が従業員の能力を補い、人間が気づかない部分をコンピュータがアシストすることが可能になりつつある

【担当：中山】

Society5.0, Connected Industry, DX, CPS 対応

○第 4 次産業革命

※DX レポート（IT システム 2025 年の崖の克服）

※科学技術イノベーション統合戦略（内閣府）

※Society5.0

※Connected Industry

※AI 白書 2019

IoT、ビッグデータ、機械学習、クラウドサービス等の活用におけるサイバーセキュリティ対策

5 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

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

従来型サイバーセキュリティ対策の限界

機械学習への期待

マルウェア検知への応用

ネットワーク異常検知への応用

ソースコードレビューへの応用

セキュリティ監視の運用支援への応用

機械学習を活用する上で押さえるべきポイント

誤検知の可能性が避けられない

判定結果の分析が困難である
全てに万能な機械学習アルゴリズムは存在しない
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

【担当：早出】
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）（2019 年 4 月 METI）対応
Society5.0, Connected Industries の実現に向けて、産業界に求められるセキュリティ対策の全体像
サプライチェーン全体での対策（中小企業向け）
対応計画（BCP 対応）
想定されるリスクと対策の整理
サプライチェーンを構成する企業のフィジカル空間での繋がり
フィジカル空間とサイバー空間の繋がり
サイバー空間とサイバー空間の繋がり
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
NIST SP 800-171 の要求事項と「サイバー・フィジカル・セキュリティ対策フレームワーク」との対応表
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

4 守りの IT 投資対応
「業務の効率化、サービスの維持のために」（守りの IT 投資）に活用すべき IT と活用におけるサイバーセキュリティ対策

改訂箇所：Mission3-8(p.94～95)を改訂

5 生産性向上のための「デジタル・ワークプレイス」

改訂箇所：Mission3-11,コラム(p.110～131)に追加
デジタル化時代のデバイスやテクノロジーを駆使して、働くプロセスや場所・コミュニケーション、コラボレーションのあり方を 新たに組み立てようとする考え方

6 生産性向上のための「デジタル・ワークプレイス」の導入におけるサイバーセキュリティ対策

6 従業員エクスペリエンスを向上（働き方改革等）するシステムの導入におけるサイバーセキュリティ対策
テレワークソリューション

【担当：伊藤⇒中山】
従業員にとって、いつでもどこでも柔軟な働き方ができるインフラやアプリケーションが一貫して提供されることで、 仕事をする上での利便性やユーザビリティが向上する
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
システム方式
リモートデスクトップ
仮想デスクトップ
クラウド型アプリ
会社 PC 持ち帰り
端末デバイス
リッチクライアント
シンクライアント
タブレット型 PC

スマートフォン
携帯電話
セキュリティ
本人認証
端末認証
端末管理
暗号化通信
ストレージ暗号化
テレワークセキュリティガイドライン（第 4 版）【2018 年 4 月総務省】
私用端末のビジネス利用
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
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）

【担当：伊藤⇒石井（茂）】

改訂箇所：Mission4-1(p.134～144)を改訂
事前だけでなく事後の「緊急時対応」も含めた一連の対応として、フェーズごとの対策
特定
防御
検知
対応
復旧

【Mission04】もしもマニュアル

【担当：石井（茂）】

【Mission05】やってみよう！サイバー攻撃シミュレーション

【担当：？】

【Information】インフォメーション

「サイバーセキュリティ経営ガイドライン」Ver2.0 付録 A サイバーセキュリティ経営チェックシートの内容の反映

改訂箇所：Information6-7(p.183 以降)として追加
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されている
「中小企業の情報セキュリティ対策ガイドライン第 3 版」のリスク分析の位置付けの変更

改訂箇所：Mission3-17～20, Information6-6　(P.124～131,180～183)を改訂
＜NIST のサイバーセキュリティフレーワークとの対応関係の提示＞

改訂箇所：Information6-7(p.183 以降)として追加
付録 A の各チェック項目について、NIST のサイバーセキュリティフレームワークと対応する項目を提示。
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）

改訂箇所：Information6-8(p.183 以降)として追加
※システム管理者としての基本技術の解説（安全・安心ハンドブック（NISC）参照）

改訂箇所：Information6-8(p.183 以降)として追加

※クレジットカード　PCI/DSS（Payment Card Industry Data Security Standard）

※ブロックチェーン技術の応用

※Wifi セキュリティ

※ランサムウェア

法律違反の可能性への対応方法の解説

【担当：小林】

改訂箇所：Information6-4(p.172～173)の改訂

GDPR 対応

個人情報保護法改正への対応

制度・施策

改訂箇所：Information6-7(p.185～)に追加

情報セキュリティサービス審査登録制度及びシステム監査基準（2018 年改訂）【METI/IPA】

ドキュメントを参照: touroku.html

- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタルフォレンジックサービス
- セキュリティ監視・運用サービス

中小企業のサイバーセキュリティ対策支援体制のモデル構築（サイバーセキュリティお助け隊）（2019 年～）【METI/IPA】

ドキュメントを参照: 20190517002.html

- 2019 年度
  - 宮城県・岩手県・福島県
  - 新潟県
  - 長野県・群馬県・栃木県・茨城県
  - 神奈川県
  - 石川県
  - 愛知県
  - 大阪府・京都府・兵庫県
  - 広島県

【参考】サイバーインシデント緊急対応企業一覧【JNSA】

ドキュメントを参照: emergency_response

- インシデント緊急対応費用

4 関連法規の改訂対応

【担当：小林】

改訂箇所：Information6-4(p.172～173)の改訂

セキュリティ事象に関連する法規の内容要約、事象毎に適用の可能性のある法律名、条文を整理する

ガイドブックの Mission1-1～13 を例に適用が想定される法律名、条文を例示

6 サイバーセキュリティ基本法

不正アクセス禁止法

6 個人情報保護法

個人情報保護に関するガイドライン，特定個人情報の適正な取扱いに関するガイドライン，マイナンバー法施行令 （行政手続における特定の個人を識別するための番号の利用等に関する法律施行令）
GDPR 対応も

6 刑法
不正指令電磁的記録に関する罪（ウイルス作成罪）, 電子計算機使用詐欺罪, 電子計算機損壊等業務妨害罪, 電磁的記録不正作出及び供用罪, 支払用カード電磁的記録不正作出等罪, 詐欺罪

6 その他のセキュリティ関連法規
電子署名及び認証業務等に関する法律, プロバイダ責任制限法, 特定電子メール法

6 知財関連
著作権法, 産業財産権法, 不正競争防止法,

6 労働関連・取引関連法規
労働基準法, 労働者派遣法, 男女雇用機会均等法, 公益通報者保護法, 労働安全衛生法, 下請法, インターネットを利用した取引, 特定商取引法, 電子消費者契約法

6 その他の法律・ガイドライン・技術者倫理
IT 基本法，e-文書法（電磁的記録），電子帳簿保存法，コンプライアンス，情報倫理・技術者倫理

GDPR 対応
GDPR（General Data Protection Regulation：一般データ保護規則）に対応した個人情報情報保護策について記述

4 関係機関、参考文献等リスト

【担当：専門員全員】
主な情報セキュリティベンダー
IT 及びセキュリティ関連用語解説
セキュリティお役立ちリンク
主な参考文献
用語解説インデックス

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）
ドキュメントを参照: https://bluemoon55.github.io/Sharing_Knowledge/MindManager/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）.html

リンク

html 版
ドキュメントを参照: 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）.html
MindManager 版（Download）
ドキュメントを参照: 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
【旧版】xmind⇒html 版
ドキュメントを参照: 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）.html
Docx 版（Download）
ドキュメントを参照: 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）.docx