

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【案】

<https://bluemoon55.jp/>

改訂履歴

- 【2020年5月28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】
- 【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

<https://bluemoon55.jp/>

リンク

html版

<https://bluemoon55.jp/>

MindManager版（Download）

<https://bluemoon55.jp/>

旧版

xmind⇒html版

<https://bluemoon55.jp/>

Docx版（Download）

<https://bluemoon55.jp/>

情報収集・整理作業と本資料の位置づけ

- 専門員が収集した情報を体系的に整理し、知識庫として「専門員ハンドブック」を作成・維持する
- 「専門員ハンドブック」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
- 本資料は、ポータルサイトでの体系的な情報発信を想定してまとめ、抜粋・要約する形で、電子書籍、冊子体で提供する内容の材料を提示

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）



4

5

「サイバーセキュリティ経営ガイドライン2.0対応

5

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

5

IPA・NISC等のガイドラインの改訂対応

5

サイバーセキュリティ脅威の最新トレンド対応

5

ITの最新トレンド対応

5

制度・施策の改訂対応

5

関連法規の改正対応

5

<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【改訂案】



Subtopic

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！
- ケーススタディー 3：取引先企業への踏み台にされた
- ケーススタディー 新規



1

2

2

2

2

[MISSION](#) 送信

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

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
- 1-3：Webサービスからの個人情報窃取
- 1-4：集中アクセスによるサービス停止
- 1-5：内部不正による情報漏えいと業務停止
- 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
- 1-8：悪意のあるスマホアプリ
- 1-9：巧妙・悪質化するフィッシング詐欺
- 1-10：Webサービスへの不正ログイン
- 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
- 1-13：中小企業におけるサイバー攻撃被害の例
- <統計データのアップデート>



1

2

2

2

2

2

2

2

2

2

2

2

2

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



5

改訂箇所：Mission1-12 (P.41)のあとに追加



ビジネスメール詐欺の被害と回避策の記述の充実



5

改訂箇所：Mission1-12 (P.41)のあとに追加



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



冊子版は、敢えて改訂する必要があるか要検討

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
- 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
- 2-5：パスワードの管理
- 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



2

2

2

2

2

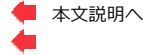
2

2

[MISSION](#) 送信

2-8：持ち込み機器対策	2	
2-9：電子メールの安全利用	2	
2-10：標的型攻撃メールへの対応	2	
2-11：迷惑メール発信への対応	2	
2-12：安全なWebサイト利用	2	
2-13：閲覧制限	2	
2-14：重要情報の洗い出し	2	
2-15：重要情報の保管	2	
【Mission03-A】経営者は事前に何を備えればよいのか【守りの対策】	1	【Mission】送信
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。	2	
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	
3-2：サイバー攻撃を受けると企業が被る不利益	3	
3-3：経営者に問われる責任	3	
参考	3	
【参考】情報セキュリティ対策を怠ることで企業が被る利益【中小企業の情報セキュリティ対策】	4	
【参考】経営者が負う責任【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）】	4	
【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）	3	
投資効果（費用対効果）を認識する	2	
3-4：投資効果（費用対効果）を認識する	3	
【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	2	
3-5：ITの活用診断	3	
3-6：サイバーセキュリティ投資診断	3	
3-7：情報セキュリティ対策診断	3	
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）	2	
3-8：業務の効率化、サービス維持のために	3	
【コラム】クラウドサービスのメリットは？	3	
【コラム】クラウドサービス導入の留意点	3	
【コラム】生産性向上のための「デジタル・ワークプレイス」	3	
【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】	3	
【コラム】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】	3	
【コラム】私用端末のビジネス利用(BYOD)	3	
【コラム】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）	3	
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	3	
【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）】	4	
経営者として取り組むべき「重要7項目の取組」【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）】	4	
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	3	
経営者からCISOへの10項目の指示	4	
※サイバーセキュリティ経営ガイドライン2.0版（新版）対応		
「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	5	
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.com
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



本文説明へ

改訂のポイント（経産省発表）

⇒ 本文説明へ

<https://www.jssec.or.jp/>

重要10項目の整理

事後対策の強化 ～検知・復旧対策の実施～

サプライチェーン対策の強化

事後対策の強化 ～インシデント発生時の対応～

<情報共有活動における情報提供の記載を強調>

【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

4

【Mission03-C⇒Mission6.6】【組織維持のため】網羅的なサイバーセキュリティ管理と実践（予防・予兆・事象発生）

【Mission】送信

セキュリティホールを減らす網羅的・体系的な対策の策定方法

2

3-XX 網羅的・体系的な対策のために

3

※、詳細は、「Mission6-6情報セキュリティポリシーテンプレート」で、中小企業の情報セキュリティ対策ガイドライン第3版を紹介する形で一括提示

【Mission03-B】経営者は事前に何を備えればよいのか【攻めの対策】

1

【Mission】送信

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)

2

【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

4

Society5.0時代に必要なセキュリティ対策

ITの最新トレンド対応

3

攻めのIT投資対応

3

3-12：IoT、ビッグデータ、AI、ロボットの活用

3

3-13：IoTが果たす役割と効果

3

3-14：人工知能（AI）が果たす役割と効果

3

【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

4

※DXレポート（ITシステム2025年の崖の克服）

【コラム】BYODセキュリティ対応

5

【コラム】IDと認証セキュリティ

5

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

3-16：IoTを活用する一般利用者のための基本ルール

3

【コラム】IoT関連セキュリティ対応

5

【コラム】クラウドサービス

5

【コラム】5Gセキュリティ対応

5

【参考】攻めの姿勢の企業向け

5

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

【参考】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】

5

【参考】IT活用の必然性

5

【参考】IT活用のためには、情報セキュリティ対策は必須

5

【参考】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

5

【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	◀	4	
【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	◀	4	
【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Revision2対	◀	4	
【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」	◀	4	
MISSION4 もしもマニュアル		1	【Mission 送信
4-1：緊急事態応用マニュアルの作成	➡	2	
4-2：基本事項の決定	➡	2	
4-3：漏えい・流出発生時の対応	➡	2	
4-4：改ざん・消失・破壊・サービス停止発生時の対応	➡	2	
4-5：ウイルス感染時の初期対応	➡	2	
4-6：届け出および相談	➡	2	
4-7：大規模災害などによる事業中断と事業継続管理	➡	2	
MISSION5 やってみよう！サイバー攻撃対策シミュレーション		1	【MISSIC 送信
5-1：サイバー攻撃前夜	➡	2	
5-2：攻撃発生その瞬間	➡	2	
5-3：サイバー攻撃直後	➡	2	
5-4：潜入拡大	➡	2	
5-5：顧客への被害拡大 取引先への被害拡大	➡	2	
5-6：サイバー攻撃の発覚	➡	2	
5-7：原因が判明 ウイルス感染が原因	➡	2	
5-8：再発防止策の作成	➡	2	
5-9：復旧回復	➡	2	
MISSION6 インフォメーション		1	【MISSIC 送信
6-1：もしかしてサイバー攻撃？ここに連絡を！	➡	2	
6-2：やられる前に、しっかり予防を！	➡	2	
6-3：情報セキュリティ5カ条	➡	2	
6-4：情報セキュリティ用語解説	➡	2	
6-5：セキュリティお役立ちリンク	➡	2	
6-X：中小企業の情報セキュリティ対策ガイドライン【第3版】	◀	2	
6-6：情報セキュリティポリシーサンプル	➡	3	
3-XX 情報セキュリティ5か条	◀	3	
3-XX 情報セキュリティ基本方針	◀	3	
3-17：新・5分でする自社診断シート	➡	3	
3-18：情報セキュリティハンドブックひな形（従業員向け）	➡	3	
3-19：情報セキュリティポリシーの明文化	➡	3	
3-20：情報資産管理台帳の作成	➡	3	
付-1：情報管理が不適切などの場合の処罰など	➡	2	
6-X：関係法令	◀	3	
付録		1	付録 送信
付-2：主な参考文献	➡	2	

本書で引用した文献名一覧		
付-3：用語解説インデックス	➡	2
索引		
以下、本文		
MISSION1 知っておきたいサイバー攻撃の知識		MISSION 受信
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？	➡	2
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！	➡	2
ケーススタディー 3：取引先企業への踏み台にされた	➡	2
ケーススタディー 新規	➡	2
「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。	➡	
なりすましECサイトの被害と回避策の記述の充実	➡	5
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【18年5月IPA】		https://www.ipa.go.jp
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ア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	➡	5
改訂箇所：Mission1-12 (P.41)のあとに追加	➡	
MISSION2 すぐやろう！対サイバー攻撃アクション		MISSION 受信
1-1：標的型攻撃による情報流出	➡	2
1-2：ランサムウェアを使った詐欺・恐喝	➡	2
1-3：Webサービスからの個人情報窃取	➡	2
1-4：集中アクセスによるサービス停止	➡	2
1-5：内部不正による情報漏えいと業務停止	➡	2
1-6：Webサイトの改ざん	➡	2
1-7：インターネットバンキングの不正送金	➡	2
1-8：悪意のあるスマホアプリ	➡	2
1-9：巧妙・悪質化するワンクリック詐欺	➡	2
1-10：Webサービスへの不正ログイン	➡	2
1-11：公開された脆弱性対策情報の悪用	➡	2
1-12：IoT機器を踏み台にした攻撃	➡	2
1-13：中小企業におけるサイバー攻撃被害の例	➡	2
<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。		

【Mission03-A】経営者は事前に何を備えればよいのか【守り】	1	【Mission 受信】
サブタイトル【組織維持のために】経営者、管理者が、自組織の現状として認識すべきこと 管理者が知っておくべきこと（管理者を設置していない場合は経営者が自ら知っておくべきこと）		
総論 サイバーセキュリティの被害に遭った場合、組織の存立が危ぶまれる事態になりえることを自覚する・世の中で起こっているセキュリティ被害を対岸の火事だと思っている経営者、ITは導入しているにも関わらずセキュリティ対策のための費 国は、大企業のみならず、中小企業も、「サイバーセキュリティ経営ガイドライン」を参照することを求めている		
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。 組織の社会的責任の認識	2	
Mission3-1 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	
情報セキュリティ対策は、経営に大きな影響を与えます！ 経営者が法的・道義的責任を問われます！ 組織として対策するために、担当者への指示が必要です！ 中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】 セキュリティ侵害を受ける70～80%が人為的なミス、故意 サイバーセキュリティ対策の中で最もコストがかかるのが技術的対策。しかし全てのリスクに対して技術的対策をすることは困難。悪意があれば技術的な対策はすり抜けられる セキュリティー被害を受けた場合、その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要。 また、システムを入れる際に、セキュリティも同時に入れるなど、ITとセキュリティ対策を一緒にすることも大切である。 更に、経営者を含め、社員全員に対し、セキュリティポリシーやガイドブックを作成したり、併せてITパスポートの試験を受けさせることも大切である。		中小企業の情報セキ
Mission3-2 情報セキュリティ対策を怠ることで企業が被る不利益	3	
(1) 金銭の喪失, (2) 顧客の喪失, (3) 業務の喪失, (4) 従業員への影響 中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】		中小企業の情報セキ
Mission3-3 経営者に問われる責任	3	
(1) 経営者などに問われる法的責任 ・個人情報・他社から預かった秘密情報・自社の秘密情報・株価に影響を与える可能性のある未公開内部情報 (2) 関係者や社会に対する責任 ・営業停止、売上高の減少、企業イメージの低下などで、自社に損害をもたらすだけでなく、取引先に対する信頼関係の喪失、業界やサービス全体のイメージダウン・法令順		中小企業の情報セキ
参考	3	中小企業の情報セキ
【参考】情報セキュリティ対策を怠ることで企業が被る不利益 【中小企業の情報セキュリティ対策ガイドライン案】		https://www.ipa.go.jp
資金の喪失 顧客の喪失 業務の喪失 従業員への影響		
【参考】経営者が負う責任 【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）】		https://www.ipa.go.jp
経営者などに問われる法的責任 個人情報 他社から預かった秘密情報 自社の秘密情報 関係者や社会に対する責任		

営業停止、売上高の減少、企業イメージの低下などで、自社に損害をもたらすだけでなく、取引先に対する信頼関係の喪失、業界やサービス全体のイメージダウン
【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）】
<https://www.ipa.go.jp>

原則1 情報セキュリティ対策は経営者のリーダーシップのもとで進める

経営者は、IT活用を推進する中で、情報セキュリティ上のリスクを認識し、自らリーダーシップを発揮して対策を進めることが必要です

原則2 委託先における情報セキュリティ対策まで考慮する

原則3 情報セキュリティに関する関係者とのコミュニケーションは、どんなときにも怠らない

経営者として取り組むべき「重要7項目の取組」【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）】
<https://www.ipa.go.jp>

取組1 情報セキュリティに関するリスクを認識し組織全体での対応方針を定める

情報セキュリティ対策を組織的に実施する意思を、関係者に明確に示すために、情報セキュリティに関する方針を定め、要求に応じて提示できるようにしておきます。

取組2 情報セキュリティ対策を行うための資源（予約、人材など）を確保する

情報セキュリティ対策を実施するために、必要な予算と人材を確保します。

取組3 情報セキュリティのリスクを把握し、どこまで情報セキュリティ対策を行うのかを定めたくて担当者を実行させる

事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、必要十分な対策を検討させます。

取組4 情報セキュリティ対策に関する定期的な見直しを行う

取組3で定めた情報セキュリティ対策について、定期または随時に見直しして、必要な改善や追加の対策を決めるように担当者に指示します。

取組5 業務委託する場合や外部ITシステムやサービスを利用する場合は、自社で必要と考える対策が担保されるようにする

契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、合意する必要があります。

取組6 情報セキュリティに関する最新動向を収集する

新たな脅威に備えるようにします。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。

取組7 緊急時の社内外の連絡先や被害発生時に行うべき内容について準備しておく

情報セキュリティ対策を実施するとともに、万が一のインシデントに備えて、緊急時の連絡体制を整備します。さらに、その連絡体制がうまく機能するかをチェック

【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)【NIS(3

【レベル1】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

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。小企業・零細企業の多く
小企業・零細企業の多く。家庭も。

(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)

ITを十分に活用していない組織、サイバーセキュリティが自社の問題と認識していない組織

情報リテラシーの向上

個人情報、企業機密、知的財産

預かり情報

インターネットバンキング

最低限のサイバーセキュリティ対策

【レベル2】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

(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)

高リスクの許容

必要以上のサイバーセキュリティ対策のため、業務の効率化、競争力強化を阻害している企業



【守りのIT投資】ITを活用した業務効率化、生産性向上、労働力確保を図っている組織





仮想化技術の適用

運用・保守コストの削減

【守りのセキュリティ対策】網羅的で費用対効果の高い対策の実施

【レベル3】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

(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)		
ITを成長エンジンとして活用【成長戦略より】		
コスト削減から価値創造へ		
中小企業の生産性向上、人材不足の解消の糸口に		
投資		
情報化投資		
革新的投資		
研究開発等		
経済的競争能力投資		
職員の研修・訓練、ブランディング、マーケティング、経営コンサルティングの外部委託		
【攻めのIT投資】新技術、新サービスを戦略的に活用した新ビジネス展開		
【攻めのセキュリティ対策】攻めのセキュリティ対策（未知のリスクを許容）		
クラウドサービス		
IoT		
第4次産業革命		
ビッグデータ		
AI		
ブロックチェーン		
テレワーク、サテライトオフィス		
投資効果（費用対効果）を認識する		2
Mission3-4 投資効果（費用対効果）を認識する		3
セキュリティ対策の投資は、人的対策、管理的対策、物理的対策、それでもカバーできないことを技術的対策		
サイバーセキュリティはやむを得ない「費用」でなく、ITを活用した積極的な経営への「投資」と位置付ける		
【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		2
Mission3-5 ITの活用診断		3
費用対効果		
IT化による想定利益＞IT化投資額（IT導入、運用、セキュリティ対策費）		
IT化の目的は、既存ビジネスの効率化、新ビジネス展開等であり、IT化のための投資が、IT化によって得られる利益を上回っている場合は、IT化投資を削減すべきである		
ITおよびサイバーセキュリティに関する組織の視点6分類		
「企業経営のためのサイバーセキュリティの考え方」を参考に、分類を追加してみたもの		
【参照】「企業経営のためのサイバーセキュリティの考え方」【2016年8月3日NISC】		
【理想的に】ITの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		
（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）		
ITの利活用と情報セキュリティ対策のバランスが取れている企業		
情報のオープン化、外部情報の活用、機密情報の保護をきちんと行い、ITの利活用により新しいサービスを展開		
【もっと積極的に】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		
（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）		
ITを積極的に活用してビジネスの発展を目指すことが必要		
【無駄な投資】過剰なセキュリティ意識により、ITの利活用を著しく制限し、ITの利活用を競争力強化に活用させていない企業		
ITの利活用と情報セキュリティ対策のバランスが取れていなく、費用対効果の悪い企業		

	基本姿勢として、情報は全て機密、IT環境は必要最低限に利用を制限 必要以上のセキュリティ対策により、無駄に費用をかけ、業務効率、サービスの向上を阻害している企業 過剰なセキュリティ意識により、ITの利活用を著しく制限し、競争力強化に活用させない企業 過剰なリスク意識により、インターネットでの情報発信、情報収集や、IT活用による業務効率を向上させる意識のない企業 セキュリティ偏重の判断は、業務の現場の不便をもたらし、柔軟な発想や市場変化に対する機敏性を損なわせる。最悪の場合、ビジネスイノベーションの規格をも潰してしまう。 組織内のITリテラシーの向上が十分でないために、低いレベルの人に合わせたセキュリティ対策のために、意識の高い人の業務の効率化を阻害している リスクを再評価して過度にならない適切なセキュリティ対策の再構築が必要 【危険】情報セキュリティ対策の必要性は理解しているが、必要十分なセキュリティ対策が出来ていないにも関わらず、ITの利活用を進めている企業 ITの利活用と情報セキュリティ対策のバランスが取れていない企業 (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) 業務効率とのバランスが取れているセキュリティ対策を実施しようとしている企業 情報セキュリティポリシーの策定と実践、定期的な監査 創造力、発想力のある人材の育成 ITスキルと知識を持った人材の育成が必要 【危険】情報セキュリティの必要性を理解していない企業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 (主に小企業・零細企業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) まずは、最低限の情報セキュリティ対策を理解し、コストを掛けずに効果の大きいことから実施することが必要 【対象外】ITを利用していない企業 サイバーセキュリティ侵害が起こりえず、対象外だが、業務効率化のためにITの活用を促すか？ 情報セキュリティ対策は必要	
Mission3-6 サイバーセキュリティ対策診断		3
費用対効果		
	セキュリティ侵害による想定被害額（経済的損失、社会的信用）＞セキュリティ対策費 セキュリティ対策費が、セキュリティ侵害による想定被害額を上回っている場合は、対策費を削減すべきである セキュリティ侵害発生時に許容可能対策費＞残留リスクによる想定被害額 重大なセキュリティ侵害が発生した時の想定被害額が、支出可能な対策費を上回っている場合は、事業継続が困難になる。支出可能な対策費に収まるように、残留リスクを下げる対策を講ずるか、支出 ただ、技術的対策はどれだけ投資してもリスクは残る。管理的対策、人的対策を優先するほうが効果的である 残留リスクをどこまで許容できるかは、経営者の判断である	
Mission3-7 情報セキュリティ対策診断		3
物理的なセキュリティ対策も合わせて実施しているか。物理的セキュリティ対策は、直接的にはサイバーセキュリティ対策ではないが、IT関連機器の設定変更など、サイバーセキュリティ侵害のきっかけを作る可能性がある		
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）		2
組織を維持するために経営者、管理者が認識し、実践すべきことは？		
Mission3-8 業務の効率化、サービスの維持のために		3
業務の効率化、サービスの維持のために		
	中小企業にとって、業務の効率化、生産の効率化、人材確保は重要な課題であり、業務、生産工程等の運用コストの削減、効率化のためにITを活用してきた。 より一層、効率化を図っていかなければ、ビジネスは継続できず、モバイル端末の活用、外部クラウドサービスの活用も、効率化に有効な手段の一つとして普及が進んできている しかし、ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、セキュリティ侵害、）が発生して、事業資産（人・業務やサービスの改善のために、インターネットに接続してITを活用する際には、同時に、サイバー攻撃等への備えが必要である ITを活用したサービスの構築・運用に掛かる費用は、経費ではなく先行投資。リスクに見合った情報セキュリティ対策は、サービスの構築・運用の中で実施すべき先行投資であり、緊急事態が発生した後にITを導入する際に、併せてセキュリティ対策をすることにより、コストを削減できる	
【コラム】クラウドサービスのメリットは？		
ITシステムに関する技術に詳しい人材がいない場合は、外部サービスを利用したほうが、コストとセキュリティ対策との両面から有利な場合も多い		

・社内サーバーが不要・IT投資のリスク軽減・常に最新でメンテナンスが不要・導入や維持に関する社内担当者の負担軽減

【コラム】クラウドサービス導入の留意点



できるだけしっかりした会社から提供されているサービスを選ぶために

取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断する

クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定

クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とする

クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める

クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に

【コラム】生産性向上のための「デジタル・ワークプレイス」



【担当：中山】



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

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 6

テレワークソリューション

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

【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】



<https://work-holiday.>

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

【コラム】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】



【コラム】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】

<http://www.nisc.go.jp>

【コラム】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（第4版）



【担当：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

Mission3-9 【経営者が認識すべき】サイバーセキュリティ経営の3原則



3

経営者は、以下の3原則を認識し、対策を進めることが重要である。

サイバーセキュリティ経営ガイドライン Ver 1.1【2016年12月8日METI】

<http://www.meti.go.jp>

中小企業の情報セキュリティ対策ガイドライン（第2版）

- (1) 経営者のリーダーシップが重要。経営者は、IT活用を推進する中で、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
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
また、サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった後、企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。
このため、サイバーセキュリティリスクを多様な経営リスクの中での一つとして適切に位置づけ、その対応方針を組織の内外に明確に示しつつ、経営者自らがリーダーシップを発揮して経営資源を用いて対策を講ずる。
- (2) 自社以外（ビジネスパートナー等）にも配慮。自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要
サプライチェーンのビジネスパートナーやITシステム管理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る。
自社のみならず、サプライチェーンのビジネスパートナーやITシステム管理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) 平時からのコミュニケーション・情報共有。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、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要
事業のサイバーセキュリティリスクへの対応等に係る情報開示により、関係者や取引先の信頼性を高める。
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、関係者や取引先の不信任の高まりを抑え、説明を容易にすることができる。
事業のサイバーセキュリティリスク対応として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。

Mission3-10 【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

3

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

改訂のポイント（経産省発表）



<https://www.jssec.or>

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ナ
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

サイバーセキュリティ経営ガイドライン2.0版（新版）



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

3. 1. サイバーセキュリティリスクの管理体制構築

指示1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定

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

対策を怠った場合のシナリオ

- ・経営者がサイバーセキュリティリスクへの対応を策定し、宣言していないと、サイバーセキュリティ対策などの実行が組織の方針と一貫した
- ・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、：

1.1版

（１）サイバーセキュリティリスクの認識、組織全体での対応の策定

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

情報セキュリティ対策を組織的に実施する意思を、関係者に明確に示すために、情報セキュリティに関する方針を定め、要求に応じて提示できるようにして、事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、必要十分な対策を検討させます。

指示 2 サイバーセキュリティリスク管理体制の構築

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

その際、組織内のその他のリスク管理体制とも整合を取らせる。

対策を怠った場合のシナリオ

- ・サイバーセキュリティリスクの管理体制を整備していない場合、組織としてサイバーセキュリティリスクの把握が出来ない。
- ・組織内におけるその他のリスク管理体制との整合を取らないと、組織全体としてのリスク管理の方針と不整合が生じる恐れがある。

1.1版

（２）サイバーセキュリティリスク管理体制の構築

サイバーセキュリティ対策を行うため、経営者とセキュリティ担当者をつなぐ仲介者としてのCISO等からなる適切なサイバーセキュリティリスクの管理体制の構築、各関係者の責任は明確になっていますか？

また、防犯対策など組織内のその他のリスク管理体制と整合をとらせていますか？

指示 3 サイバーセキュリティ対策のための資源（予算、人材等）確保

サイバーセキュリティ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。

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ー
- ・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。

1.1版

（６）サイバーセキュリティ対策のための資源（予算、人材等）確保

サイバーセキュリティリスクへの対策を実施するための予算確保は出来ていますか？ また、サイバーセキュリティ人材の育成や適切な処遇をさせていますか？

情報セキュリティ対策を実施するために、必要な予算と人材を確保します。

3. 2. サイバーセキュリティリスクの特定と対策の実装

指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を立てる。その際、サイバー保険の活用や守るべき情報について専門ベンダーへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。

対策を怠った場合のシナリオ

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

1.1版

【分割】（３）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標 [【分割】](#) 送信

サイバー攻撃の脅威に対し、経営戦略の観点から、守るべき資産を特定させた上で、社内ネットワークの問題点などのサイバーセキュリティリスクを把握させ、その上で、暗号化やネットワークの分離など複数のサイバーセキュリティ対策を組み合わせた多層防御など、リスクに応じた対策の目標と計画を策定させている。また、サイバー保険の活用や守るべき資産について専門企業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ていますか？

指示 5 サイバーセキュリティリスクに対応するための仕組みの構築

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

対策を怠った場合のシナリオ

- ・サイバーセキュリティリスクに応じた適切な対策が行われていない場合、サイバー攻撃が発生した場合の被害が拡大する可能性がある。
- ・技術的な取組を行っていたとしても、攻撃の検知・分析とそれに基づく対応ができるよう、適切な運用が行われていなければ、サイバー攻撃の

1.1版

【分割】（3）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標 **【分割】** 受信

サイバー攻撃の脅威に対し、経営戦略の観点から、守るべき資産を特定させた上で、社内ネットワークの問題点などのサイバーセキュリティリスクを把握させ、その上で、暗号化やネットワークの分離など複数のサイバーセキュリティ対策を組み合わせた多層防御など、リスクに応じた対策の目標と計画を策定させている。また、サイバー保険の活用や守るべき資産について専門企業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ていますか？

指示 6 サイバーセキュリティ対策におけるPDCAサイクルの実施

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

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

また、ステークホルダーからの信頼性を高めるため、対策状況を開示させる。

対策を怠った場合のシナリオ

- ・PDCA（Plan[計画]、Do[実行]、Check[実施状況の確認・評価]、Act[改善]）を実施する体制が出来ていないと、立てた計画が確実に実行され
- ・最新の脅威への対応ができていない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しなさいと、サイバーセキュリティ
- ・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

1.1版

（4）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示

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として実施するフレームワークを構築させていますか？

その中で、監査（または自己点検）の実施により、定期的に経営者に対策状況を報告させた上で、必要な場合には、改善のための指示をしていますか？

また、ステークホルダーからの信頼性を高めるため、対策状況について、適切な開示をさせていますか？

情報セキュリティ対策について、定期または随時に見直して、必要な改善や追加の対策を決めるように担当者に指示します。

3. 3. インシデント発生に備えた体制構築 3

指示 7 インシデント発生時の緊急対応体制の整備

影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT等）を整備させる。

被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。

また、インシデント発生時の対応について、適宜実践的な演習を実施させる。

対策を怠った場合のシナリオ

- ・緊急時の対応体制を整備していないと、原因特定のための調査作業において、組織の内外の関係者間のコミュニケーションが取れず、速やかな
- ・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。

1.1版

（9）緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施

適切な初動対応により、被害拡大防止を図るため、迅速に影響範囲や損害を特定し、ITシステムを正常化する手順を含む初動対応マニュアル策定や

情報セキュリティ対策を実施するとともに、万が一のインシデントに備えて、緊急時の連絡体制を整備します。さらに、その連絡体制がうまく機能するかを
指示 8 インシデントによる被害に備えた復旧体制の整備

インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制のBCPとの連携等、組織全体として整合のとれた復旧目標計画を定めさせる。

また、業務停止等からの復旧対応について、適宜実践的な演習を実施させる。

対策を怠った場合のシナリオ

- ・重要な業務が適切な時間内に復旧できず、企業経営に致命的な影響を与える恐れがある。
- ・演習を実施していないと、不測の事態が起こった際に、担当者が緊急時に適切に行動することが出来ない。

1.1版

(10) 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

外部に対して迅速な対応を行うため、被害の発覚後の通知先や開示が必要な情報について把握させていますか？ また、情報開示の際、経営者が組織

3. 4. サプライチェーンセキュリティ対策の推進

指示 9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCAについて、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。

中小企業自らがセキュリティ対策に取り組むことを宣言する制度

<https://www.ipa.go.jp>

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
- ・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。

1.1版

(5) 系列企業や、サプライチェーンのビジネスパートナー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

自社のサイバーセキュリティが確保されるためには、系列企業やサプライチェーンのビジネスパートナーを含めてサイバーセキュリティ対策が適切に行われている

(7) ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保

サイバーセキュリティ対策を効率的かつ着実に実施するため、リスクの程度や自組織の技術力などの実態を踏まえ、ITシステムの管理等について、自組織契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、合意する必要があります。

3. 5. ステークホルダーを含めた関係者とのコミュニケーションの推進

指示 10 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加し、積極的な情報提供及び情報入手を
また、入手した情報を有効活用するための環境整備をさせる。

対策を怠った場合のシナリオ

- ・情報共有活動への参加により、解析した攻撃手法などの情報を用いて、他社における同様の被害を未然に防止することができるが、情報共有

1.1版

(8) 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のための環境整備

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の参加と、入手した情報を有効活用す
新たな脅威に備えるようにします。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先など:

【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

2020年3月25日公開

可視化ツールβ版について

<https://www.ipa.go.jp>

サイバーセキュリティの実践状況を企業自身がセルフチェックで可視化するための サイバーセキュリティ経営ガイドラインベースの可視化ツールです。
ツールのダウンロード

<https://www.ipa.go.jp>

【Mission03-C】 【組織維持のため】 網羅的なサイバーセキュリティ管理と実践（予防・予兆・事象発生時） 1 6-6：情報送信 【Mission】 受信

セキュリティホールを減らす網羅的・体系的な対策の策定方法 2

⇒中小企業の情報セキュリティ対策ガイドライン第3版として、一括で提示

セキュリティホールを減らす網羅的・体系的な対策の策定方法 2

3-XX 網羅的・体系的な対策のために 3

※、詳細は、「Mission6-6情報セキュリティポリシーサンプル」 中小企業の情報セキュリティ対策ガイドライン第3版を紹介する形で一括提示

【Mission03-B】 経営者は事前に何を備えればよいのか【攻め】 1 【Mission】 受信

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) 2

【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

【コラム⇒各項目】 ITの最新トレンド対応 3

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-

Society5.0時代に必要なセキュリティ対策 4

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和、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】

5Gセキュリティ対応【担当：早出】

【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 NIST 800-63-3 電子的認証に関するガイドライン 対応 2要素認証 パスワード設定に関する要件の変更、パスフレーズの利用 【参照】世界の電子認証基準が変わる-NIST-SP800-63-3を読み解く		世界の電子認証基準
	FIDO(Fast Identity Onlinebe) 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		
Mission3-11 次世代技術を活用したビジネス展開		3	
Subtopic			
組織を発展させるために経営者、管理者が認識し、実践すべきことは？			
	柔軟にかつ大企業に先駆けて、IT関連の次世代技術、デジタル情報を活用していくことが、中小企業の発展につながる。デジタル情報、IT技術の進展を受入れ、それを活用して顧客サービスの強化を図る ビジネスの拡大・発展のための「攻めのIT投資」は、確立していない世界であり、セキュリティリスクも高くなる。 次世代技術を活用したビジネス展開		
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			
現状認識	今は、IoT、ビッグデータ、ロボット、AI等の技術革新による、第4次産業革命の入り口にいる 【参照】IT人材白書2017【2017年4月IPA】 https://www.ipa.go.jp あらゆるものがインターネットに接続するIoTの広がり、あらゆる情報がビッグデータとして活用され、AI技術により、様々な分野で定型的な業務はもとより、人海戦術では不可能だった業務まで、既存のビジネスや業務に新技術を取り入れるだけでなく、ビジネスモデルを変え、経済活用のみならず、個人の生活や社会構造まで影響が及ぶ デジタルフォーメーション（デジタル変革）とは、あらゆる情報がデジタル化され、IT技術によって、社会や産業、企業、人のあり方や働き方が変わっていくこと 第4次産業革命が進むにつれて、発展するビジネスと縮小するビジネスが明確になっていく 時代環境が大きく変わる時、それにそぐわないビジネスは淘汰されていく 匠の技的な高度な伝統的技能を要する作業や、旧来の延長線で仕組みの高度化、洗練により、生き残れるビジネスもあるが、現状維持のビジネスの多くは、相対的に意義を失う可能性が IoT、ビッグデータ、ロボット、AI等の技術を、クラウドコンピューティングやモバイル環境で活用できるようになったことは、少ない投資で事業を立ち上げることが可能であり、中小企業、ベンチャー		
組織として	時代の潮流を捉えて、組織が社会の変化の中で、時代に適合して発展できる道を探り、ビジョンをはっきり示すことが重要であり、それは経営者の責務 「デジタルトランスフォーメーション」を実現するには、ビジネスとデジタルのスキルを併せ持った人材の育成と獲得をしていく必要がある		
個人として	自らも「デジタルトランスフォーメーション」の流れの中にあることの意識 求められるのは、周囲を巻き込みながら改革を進める能力やビジネスとデジタルを結び付けて 全体をデザインする能力を持った人材になること 目の前の業務だけにとらわれることなく、広く視野を持って進むべき道を探り、学ぶ。勉強会やコミュニティなど、学びの場は周囲にある。自己研さんによって能力を高めれば高めただけ、社会に!		
【コラム】攻めのIT投資対応		3	
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		4	
	【担当：中山】		

	<p>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</p> <p>Society5.0, Connected Industry, DX, CPS対応</p> <p>○第4次産業革命</p> <p>※DXレポート（ITシステム2025年の崖の克服）</p> <p>※科学技術イノベーション統合戦略（内閣府）</p> <p>※Society5.0</p> <p>※Connected Industry</p> <p>※AI白書2019</p> <p>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</p>	
	<p>Mission3-12 IoT、ビッグデータ、AI、ロボットの活用</p> <p>中小企業での活用事例「IoTユースケースマップ」 http://usecase.jmfrri.jp/#/</p> <p>深刻な人手不足に対応した、省力化、自動化のための投資 人が行ってきたことをセンサー化し、センサーからの膨大な情報を機械的に分析することにより、今までできなかった高度な分析と、その結果を踏まえて業務やサービスを効率的、効果的に行える</p>	<p>3</p> <p>http://usecase.jmfrri.jp/#/</p>
	<p>Mission3-13 IoTが果たす役割と効果</p> <p>中小企業にとって、経費削減と人材確保は大きな課題 各種センサーによる自動測定や電子タグ等（RFID）を人やモノに貼り動きの情報を計測し収集することにより、リアルタイムで状況が把握できる その際に、センサーが誤動作したり、誤った情報を発信すると、正確な状況を把握できなくなり、業務やサービスが混乱する IoT、ビッグデータ、AI、ロボットは繋がっている</p> <p>①センサー、機器、ロボットによりデータが取得され、②データのやり取りや通信により③集約されることによりビッグデータ化し、④人工知能等を用いて分析され⑤ロボット等を通じて実環境でのアクションとして IoT、AI、ロボットに関する経済産業省の施策について【2016年2月METI】 https://www.iajapan.jp/</p> <p>IoT、ビッグデータ、AI、ロボットを利用することにより、人が行ってきたことが効率化されるとともに、これらを使いこなすことにより、人の仕事の質を高める能力が付加価値となる</p>	<p>3</p> <p>https://www.iajapan.jp/</p>
	<p>Mission3-14 人工知能（AI）が果たす役割と効果</p> <p>人工知能は、中小企業の既存の業務の人手不足の解消に留まらず、既存の人手で新たな業務を行えるようになることが期待できる。 不足している労働力を補完する。既存の労働力を省力化する。既存の業務効率・生産性を高める。既存の業務の提供する価値（品質や顧客満足度など）を高める。これまでに存在しなかった新しい価値をもった業</p> <p>【参照】平成28年度情報通信白書【総務省】 http://www.soumu.go.jp/</p>	<p>3</p> <p>http://www.soumu.go.jp/</p>
	<p>Mission3-15 IoTを活用する際のサイバーセキュリティ上の留意点</p> <p>IoT装置は、十分なセキュリティ対策がされていないものが多い。特に以前のIoT製品に関しては管理者権限パスワードの変更手順や、ファームウェアのアップデート機能はほとんど実装されていない。 利用者側として、IoT製品は十分なセキュリティ対策がされていないことを前提とした対策が必要 製造者は、IoT製品のファームウェアの自動アップデート機能を実装し、脆弱性に対して速やかに対応する等の「IoT製品ガイドライン」に沿った対応が必要 膨大な情報をビッグデータとして活用に当たっては、「改訂個人情報保護法」の個人情報に該当する可能性の「グレーゾーン」の情報も増える。また、利用の仕方によっては著作権侵害になるケースもある。さらに、情報</p>	<p>3</p> <p>http://www.meti.go.jp/</p>
	<p>Mission3-16 IoTを活用する一般利用者のためのルール</p> <p>問合せ窓口やサポートがない機器やサービスの購入・利用を控える：インターネットに接続する機器やサービスの問合せ窓口やサポートがない場合、何か不都合が生じたとしても、適切に対処すること等が困難になる。f 初期設定に気をつける・機器を初めて使う際には、IDやパスワードの設定を適切に行う。パスワードの設定では、「機器購入時のパスワードのままとしなない」、「他の人とパスワードを共有しない」、「他のパスワードを使い 使用しなくなった機器については電源を切る：使用しなくなった機器や不具合が生じた機器をインターネットに接続した状態のまま放置すると、不正利用される恐れがあることから、使用しなくなった機器は、そのまま放置 機器を手放す時はデータを消す：情報が他の人に漏れることのないよう、機器を捨てる、売るなど機器を手放す時は、事前に情報を削除する。</p> <p>IoTセキュリティガイドラインver1.0【2016年7月5日総務省・経済産業省】 http://www.meti.go.jp/</p>	<p>3</p> <p>http://www.meti.go.jp/</p>
参考	<p>【参考】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</p>	

デジタルトランスフォーメーション

最先端の技術を生かし、コスト削減だけでなく、ビジネスの推進にどう貢献するか

DXの目指すところ

「ITの浸透が、人々の生活をあらゆる面でより良い方向に変化させること」

DX時代には

企業がこれからのビジネスで勝ち残っていくためには、新しい製品、サービス、パートナーシップ、ビジネスモデルなどを創造し、新たな価値を創出し、プラットフォームの構成

「クラウド」「ビッグデータ／アナリティクス」「ソーシャル技術」「モビリティ」

プラットフォームの上にイノベーションアクセラレーター」の技術

イノベーションを後押しするIoT、AIや機械学習などの認知システム、ロボティクス、AR（Augmented Reality、拡張現実）／VR（Virtual Reality、仮想現実）デジタルトランスフォーメーション、インダストリー4.0、ソサエティ5.0、

データを効率的に集積し、それをAIのディープラーニング機能などを活用して認識・加工し、自らの企業活動に生かしていけるかが、企業の成長の可否を決める時代IT化、デジタル化の進展を受入れ、それを活用して顧客との関係性強化を図る企業は、大きなビジネスチャンスを得ることが期待できる。

人工知能（AI）、ディープラーニング、ビッグデータ、IoT、M2M、仮想現実（AR）、3Dプリンタ等を活用した新サービスが、一般化する前に先駆的に取り入れるベンチ

CtoB

多様な消費者ニーズに対応して、きめ細やかで丁寧なモノづくりが企業の持続的発展に不可欠な要素となる【日経1月4日13面 佐藤康博】

競争力強化

新サービス、新技術を活用した生産性の向上

新サービス、新技術を活用した新ビジネス展開

大手企業と中小企業、ベンチャー企業との協業

新サービス、新技術は新ビジネスのチャンスだが、セキュリティ上のリスクも大きい

【参考】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>

基本方針－サイバーセキュリティは、より積極的な経営への「投資」へ

グローバルな競争環境の変化

ITの発展によるビジネスの変革が、消費者向けのビジネスから企業間取引へと拡大

サイバー空間と実空間の融合がさらに進み、チャンスもリスクも一層増大

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

基本的な考え方

二つの基本的認識

<①挑戦> サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、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

<②責任> 全てがつながる社会において、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

三つの留意事項

<①情報発信による社会的評価の向上>

「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。

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リスクの項目としてのサイバーセキュリティ>

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、リスクを分ける経営層のリーダーシップが必要。

<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>

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。

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。

IT活用の必然性

IT活用するためにセキュリティ対策を実施する

セキュリティ対策は目的ではない。

業務の効率化のためにITを活用する。

必要以上のサイバーセキュリティ対策は、業務の効率化を阻害する

単なる効率化だけではビジネスの競争に勝ち残れない

これまで企業のITシステムは、業務、生産工程等を効率化して、経営を安定化させることに重きが置かれてきた。

組織の発展のためにはITの活用が重要

これからはデジタルトランスフォーメーションの時代の時代と言われている。社会の進展に対応したサービスを展開するためにITを活用する

IT化、デジタル化の進展を受入れ、それを活用して顧客との関係性強化を図る企業は、大きなビジネスチャンスを得ることが期待できる。

デジタルトランスフォーメーションに対応することが重要

10分で分かる！近未来予想図202X | nikkei BPnet (日経BPネット) : 日経BPオールジャンルまとめ読みサイト

<http://www.nikkeibp.jp>

デジタルトランスフォーメーション時代には、創造力、技術力を持ったベンチャー企業など、ビジネスチャンスあり

柔軟にかつ大企業に先駆けて、デジタルトランスフォーメーションに対応していくことが、組織の発展につながる。

人海戦術、定型化した作業、精密作業は、匠の技レベルでなければシステム、機械に置き換わっていく。

「つながる工場」「インダストリー4.0」「自動運転」「スマートアグリ」

人工知能 (AI) , ディープラーニング, ビッグデータ, IoT, M2M, 仮想現実 (AR) , 3Dプリンタ等のデジタルを、ITを駆使した新サービスを、一般化する

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

セキュリティ侵害は組織の存続が脅かす

ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、セキュリティ侵害、）

事業を継続できるように

どんな緊急事態が発生しても、事業を継続できるようにする対策を明示しておくことが必要

サービスの向上を図るために

情報資産（保有情報（媒体に依らず）、情報機器、情報システム）に対する情報セキュリティ上のリスクを低減させる

セキュリティ対策は先行投資

ITを活用したサービスの構築・運用に掛かる費用は、経費ではなく先行投資。リスクに見合った情報セキュリティ対策は、サービスの構築・運用の中で実施すべき先

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

人工知能 (AI) , ディープラーニング, ビッグデータ

M2M, 制御システム【情報セキュリティ白書2016】

IoT【情報セキュリティ白書2016】

IoT早期導入者のためのセキュリティガイダンス【CSA】

■IoTセキュリティガイドラインver1.0【2016年7月5日総務省・経済産業省】

<http://www.meti.go.jp>

■安全なIoTシステムの創出【2016年3月1日NISC】

<http://www.nisc.go.jp>

■コンシューマ向けIoTセキュリティガイド【2016年6月24日JNSA】

<http://www.jnsa.org/>

■IoT早期導入者のためのセキュリティガイダンス【2016年2月24日CSA】

<https://www.cloudsec.jp>

クラウドサービス

■クラウドセキュリティガイドライン活用ガイドブック2013年版【METI】

<http://www.meti.go.jp>

■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【2014年4月総務省】

<http://www.soumu.go.jp>

■クラウドセキュリティ関連ISO規格

ISO/IEC27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項（スライド）【JIPDEC】

<https://www.isms.jp/>

ISMSクラウドセキュリティ認証の概要（スライド）【JIPDEC】

<https://www.isms.jp/>

ISO/IEC27017:2015に基づくクラウドセキュリティの構築のポイント（スライド）【JIPDEC】

<https://www.isms.iipr>

スマートデバイス

スマートフォン、タブレット等

■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】

<http://www.nisc.go.jp>

VR, MR, AR

エンターテインメント、自動車業界、広告業界、教育、宇宙産業、

VR/AR技術の将来展望【2016年6月MRI】

<http://www.mri.co.jp/>

VR（Virtual reality:仮想現実）

AR（Augmented reality：拡張現実）

MR（Mixed Reality：混合現実）

SR（Substitutional Reality：代替現実）

ブロックチェーン

仮想通貨

ブロックチェーンの安全性とセキュリティコンセンサス・ベイス（株）

<https://www.boj.or.jp>

3Dプリンタ

危険物製造、著作権侵害

・・・

【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



3

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

【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



3

【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Revision2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

【Mission04】 もしもマニュアル

【担当：石井（茂）】

- 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

1 [MISSION](#) 受信

【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

1 [MISSION](#) 受信

【MISSION6】 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
- 6-4：情報セキュリティ用語解説
もう少し充実させる
- 6-5：セキュリティお役立ちリンク

1 [MISSION](#) 受信

「Sec01-02_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_インテックス」から抜粋
「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
<NISTのサイバーセキュリティフレーム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

<https://bluemoon55.>

<https://bluemoon55.>

※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

6-X：中小企業の情報セキュリティ対策ガイドライン【第3版】



2

6-3：情報セキュリティ5カ条



3

Mission3-XX 情報セキュリティ基本方針



3

Mission3-17 新・5分でできる自社診断シート



3

Subtopic

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

組織においてあまり費用をかけることなく実行することで効果がある情報セキュリティ対策を25項目に絞られてます

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

Subtopic

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）【2017年5月10日IPA】

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/>

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

<http://www.ipa.go.jp/>

<https://www.ipa.go.jp/>

<https://www.ipa.go.jp/>

Part1 基本的対策

No.1 パソコン等の脆弱性対策

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？

No.2 パソコン等のウイルス対策

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？

No.3 パソコン等のパスワード管理

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？

No.4 重要情報へのアクセス(権)管理

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？

No.5 脅威情報等の情報共有

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

Part2 従業員としての対策

No.6 標的型攻撃メール対策等

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？

No.7 電子メールの誤送信防止

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？

No.8 電子メールでの重要情報漏えい対策

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？

No.9 無線LANのセキュリティ対策

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？

No.10 インターネットを介したトラブル防止

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？







No.11 重要情報のバックアップ等の保全対策

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？

No.12 重要情報の事務所等での管理

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？

No.13 重要情報の持ち出し等の管理

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？			
No.14 パソコン等の第三者利用制限			
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？			
No.15 事務所等への不正侵入対策			
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？			
No.16 事務所等での重要機器の管理			
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？			
No.17 事務所等での入退出管理			
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？			
No.18 不要になった重要情報の廃棄管理			
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？			
Part3 組織としての対策【要確認】			
No.19 守秘義務等の従業員への徹底			
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？			
No.20 従業員へのセキュリティ意識付け			
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？			
No.21 BYOD対応のセキュリティ対策			
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？			
No.22 取引先とのセキュリティ協議			
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、取引先に秘密を守らせることを求めていますか？			
No.23 外部サービスのセキュリティ対策			
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？			
No.24 BCPを踏まえたセキュリティ事故対策			
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？			
No.25 セキュリティルールの策定と運用			
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？			
さらなる情報セキュリティ対策の検討するには			
「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。			
Mission3-18 情報セキュリティハンドブックひな形（従業員向け）		3	
従業員向け情報セキュリティハンドブック 【中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】】 【付録2をサンプルとして】			中小企業の情報セキ
6-6：情報セキュリティポリシーサンプル		3	【Mission 受信
Mission3-19 情報セキュリティ関連規程の明文化		3	
Information6-6 情報セキュリティポリシーサンプル			
自社の情報セキュリティポリシー 【中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】】 【付録3 ツールBをサンプルとして】			中小企業の情報セキ
Mission3-XX 情報資産台帳の作成		3	
Mission3-20 リスク分析シート		3	
どんな情報資産があるか			
ビジネスに影響を与える重要度の高い情報資産の洗い出し			
重要度とは？			
機密性、完全性、可用性それぞれの評価値から3段階で判定			

どんな脅威があるか

サイバー攻撃, 情報漏えい, 故意, 過失, 誤謬びゅう, 不正行為, 妨害行為, サービス妨害,
風評, 炎上, SPAM (迷惑メール), ファイル共有ソフト

物理的脅威

(事故, 災害, 故障, 破壊, 盗難, 不正侵入 ほか)

技術的脅威

(不正アクセス, 盗聴, なりすまし, 改ざん, エラー, クラッキング ほか)

人的脅威

(誤操作, 紛失, 破損, 盗み見, 不正利用, ソーシャルエンジニアリング ほか)

どんな情報資産にどんな脆弱性があるか

現状の対策で、重要度の高い情報資産ごとにどんな脆弱性があるか

脆弱性のレベル

バグ, セキュリティホール, 人為的脆弱性

被害発生の可能性は?

対象となる情報資産ごとの【脅威の発生頻度x脆弱性のレベル】を3段階で

情報資産ごとのリスクの大きさは?

リスク値=重要度x被害発生可能性

どんな予防的対策を取るか?

予防的対策を取っても残るリスクは? (情報資産ごとの残留リスク)

リスクは許容範囲か

セキュリティ侵害をどこまで許せるか

予防できなかったセキュリティ侵害が起きた場合

どこまで対策をしてもリスクはゼロにならない。残留リスクによりセキュリティ侵害があった場合、対応策を明確にしておく

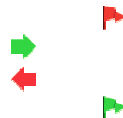
リスク分析シート (情報資産台帳・脅威の状況・脆弱性チェック) 【中小企業の情報セキュリティ対策ガイドライン (第3版) 【2019年12月19日IPA】】

[中小企業の情報セキ](#)

Mission3-XX 中小企業のためのクラウドサービス安全利用の手引き

付-1: 情報管理が不適切ななどの場合の処罰など

制度・施策



3

2

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】

<https://www.meti.go.>

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】

<https://www.meti.go.>

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】			https://www.insa.org
インシデント緊急対応費用			
6-X関係法令：法律違反の可能性への対応方法の解説			3
改訂箇所：Information6-4(p.172～173)の改訂			
関連法規の改訂対応			
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			
サイバーセキュリティ基本法			6
不正アクセス禁止法			
個人情報保護法			6
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）			
刑法			6
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，その他のセキュリティ関連法規			6
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			
知財関連			6
著作権法，産業財産権法，不正競争防止法，労働関連・取引関連法規			6
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			
その他の法律・ガイドライン・技術者倫理			6
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			
付録			1
付-2：主な参考文献			2
本書で引用した文献名一覧			
付-3：用語解説インデックス			2
索引			

[付録](#) 受信

github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02.html

github.io/Sharing_Knowledge3/MindManager3/Sec01-01-01.html

github.io/Sharing_Knowledge3/MindManager3/Sec01-01-02.html

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

github.io/Sharing_Knowledge/Cyber_Security/Deliverables/mind2html/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
[ddot; GitHub Pages](#)

[セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](#)

いても言及。

[g/dl/20180309_Hiroshi_itou.pdf](#)

[/files/000066952.pdf](#)

利用はないとして対策に後ろ向きの経営者、最も重要な情報にアクセスする権限を持ちながら、セキュリティに関しての意識の低い経営者。これらの経営者が最大のセキュリティリスク

[セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](#)

[セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](#)

子・顧客・取引先・従業員

[セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](#)

[セキュリティ/keihatsu/sme/guideline/](#)

[セキュリティ/keihatsu/sme/guideline/](#)

[>/security/keihatsu/sme/guideline/](#)

[>/security/keihatsu/sme/guideline/](#)

。

す。

’するためインシデントを想定した模擬訓練を定期的に行うと理想的です

可能な対策費を捻出する必要がある

もの（情報及び設備）・金）、社会的信用が失われ、早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性がある。

対処する経費として想定してはいけない

評価し判断する

とする

mhlw.go.jp/material/pdf/category7/01_01.pdf

[y/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf](https://conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf)

[p/press/2015/12/20151228002/20151228002-2.pdf](#)

資は必要不可欠かつ経営者としての責務である。

ける必要がある。その際、変化するサイバーセキュリティリスクへの対応や、被害を受けた場合の経験を活かした再発防止も必要である。

また、サイバー攻撃情報（インシデント情報）を共有することにより、同様の攻撃による他社への被害の拡大防止に役立つことを期待できる。

性が不十分。

[g/dl/20180309_Hiroshi_itou.pdf](#)

一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

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。

ものとならない。
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。

おきます。

薬は出来ていますか？

への委託が困難となる恐れがある。

画を策定させる。

不都合が生じる恐れがある。

ていますか？
いますか？

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。

ていますか？
いますか？

しない恐れがある。
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。
: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。

か？

な対処ができない。

組織内のCSIRT構築など対応体制の整備をさせていますか？また、定期的かつ実践的な演習を実施させていますか？

チェックするためインシデントを想定した模擬訓練を定期的に行うと理想的です

整備をさせる。

敵の内外への説明が出来る体制の整備をさせていますか？

委託先等を含めた運用をさせる。

[/security/security-action/](#)

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。

ことが重要。このため、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、系列企業やサプライチェーンのビジネスパートナーを含めた運用をさせていますか？

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ていますか？ また、ITシステム管理を外部委託する場合、当該委託先へのサイバー攻撃等も想定し、当該委託先のサイバーセキュリティの確保をさせていますか？

をさせる。

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。

るための環境整備をさせていますか？

共有します。

[/security/economics/checktool/](#)

[/files/000081169.xlsx](#)

ーセキュリティ対策)

[が変わる：NIST SP800-63-3を読み解く – サポート - トラスト・ログイン byGMO【IBSKUID\(スクイド\)】](#)

いわた見直しが図られてる

る企業に、大きなビジネスチャンスがある。

[/jinzai/jigyou/about.html](#)

、AI技術を適用したサービス、ロボットの適用が始まっている

高い

-企業や個人の活躍のまたとないチャンスである

ードしていく人材になっていく

[jp/#/](#)

に実行される

[org/iot/event/2016/pdf/3_01_sano.pdf](#)

業務を創出する。既存の業務に取組む意欲や満足度を高める。新しい業務に取組む意欲や満足度を高めること。

[p.jp/johotsusintokei/whitepaper/h28.html](#)

をビッグデータとして公開する際に、故意・過失に関わらず、機密性の高い情報を公開してしまう可能性もある

問合せ窓口やサポートがない機器やサービスの購入・利用は行わないようにする。

回さない」等につける。・取扱説明書等の手順に従って、自分でアップデートを実施してみる。

せずに電源を切る。

[p/press/2016/07/20160705002/20160705002.html](#)

ていく必要があるという

想現実)、3Dプリンティングなど

がすぐそこまで来ている【日経1月4日13面 佐藤康博】

ニヤー的企業（イノベーター、アーリーアダプター）

[/active/kihon/pdf/keiei.pdf](#)

とが期待される

考えていく
る

析し、総合的に判断。

co.jp/atcl/tk/DTrans/kmy/

前に先駆的に取り入れることが重要

が発生して、事業資産（人・もの（情報及び設備）・金）、社会的信用が失われ、早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性がある。

行投資であり、緊急事態が発生した後に対処する経費として想定してはいけない

press/2016/07/20160705002/20160705002.html

conference/cs/kenkyu/dai03/pdf/03shiryou05.pdf

[result/iot/](#)

curityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf

press/2013/03/20140314004/20140314004-3.pdf

c.jp/menu_news/s-news/01ryutsu03_02000073.html

dec.or.jp/doc/JIP-ISMS517-10.pdf

dec.or.jp/seminar/cloud/shiryou-1.pdf

dec.or.jp/seminar/cloud/shiryou-2.pdf

[y/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf](http://conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf)

opinion/column/tech/tech_20160520.html

[/announcements/release_2016/data/rel160831b4.pdf](http://announcements/release_2016/data/rel160831b4.pdf)

github.io/Presentation_Doc/Cyber/相談・届出先クイックリスト（張り紙用）.pdf

github.io/Sharing_Knowledge3/MindManager3/Sec01-02.html

[files/000055520.pdf](#)
[/security/keihatsu/sme/guideline/](#)
[/security/benchmark/](#)

「か？

[セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](#)

[セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](#)

[セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](#)

jp/policy/netsecurity/shinsatouroku/touroku.html

jp/press/2019/05/20190517002/20190517002.html

[/emergency_response/](#)

:関する法律施行令)

詐欺罪