


Sec01-11-02_ITおよびサイバーセキュリティに関する組織の視点6分類別を実施すべき対策

この要約資料の概要


概要	ガイドブック内「MISSION 3-5 自社のIT活用・セキュリティ対策状況を自己診断する ITの活用診断」の「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」毎に具体的に実施すべき事項を整理したもの		
原本	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】	https://www.nisc.go.jp/active/kihon/pdf/keiei.pdf	
改版履歴	2022年1月26日 改版		
	2018年1月19日 初版		
ファイル	https://cybersecurity-tokyo.jp/security/docs/Sec01-11-02.pdf		

サイバーセキュリティ対策状況の自己診断

IPAの「5分でできる！自社診断&ポイント学習」の実施 

<https://security-shien.ipa.go.jp/learning/index.html>

【ガイドブック INFORMATION
6-4 中小企業の情報セキュリティ対策
の段階的レベルアップ】

「中小企業の情報セキュリティ対策ガイドライン第3版」内の「5分でできる情報セキュリティ自社診断」 

<https://www.ipa.go.jp/files/000055848.pdf>

診断結果で提示された参考資料をベースに対策を実施する

組織のIT活用状況及びサイバーセキュリティ対策の意識及び実施レベルの確認【6分類】

【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
【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	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の活用により新しいサービスを展開
	(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)
【無駄な投資】過剰なセキュリティ意識により、ITの活用を著しく制限し、ITの活用を競争力強化に活用させていない企業	ITの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、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す、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機会を潰している。
	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も阻害している

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

【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・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

【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

【理想的に】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

対策の基本的な考え方

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

最低限実施すべき対策

自社セキュリティポリシーに従った定期的な監査と監査に基づいた対策の見直し

【ガイドブック MISSION
3-11 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） 次世代技術を活用したビジネス展開】

【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

対策の基本的な考え方

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

最低限実施すべき対策

【ガイドブック MISSION
3-11 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） 次世代技術を活用したビジネス展開】

【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

対策の基本的な考え方

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

最低限実施すべき対策

【ガイドブック MISSION
3-4 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 投資
効果（費用対効果）を認識する】

【ガイドブック MISSION
3-5 自社のIT活用・セキュリティ対策状況を自己診断する ITの活用診断】

【ガイドブック MISSION
3-6 自社のIT活用・セキュリティ対策状況を自己診断する サイバーセキュリティ投資診断】

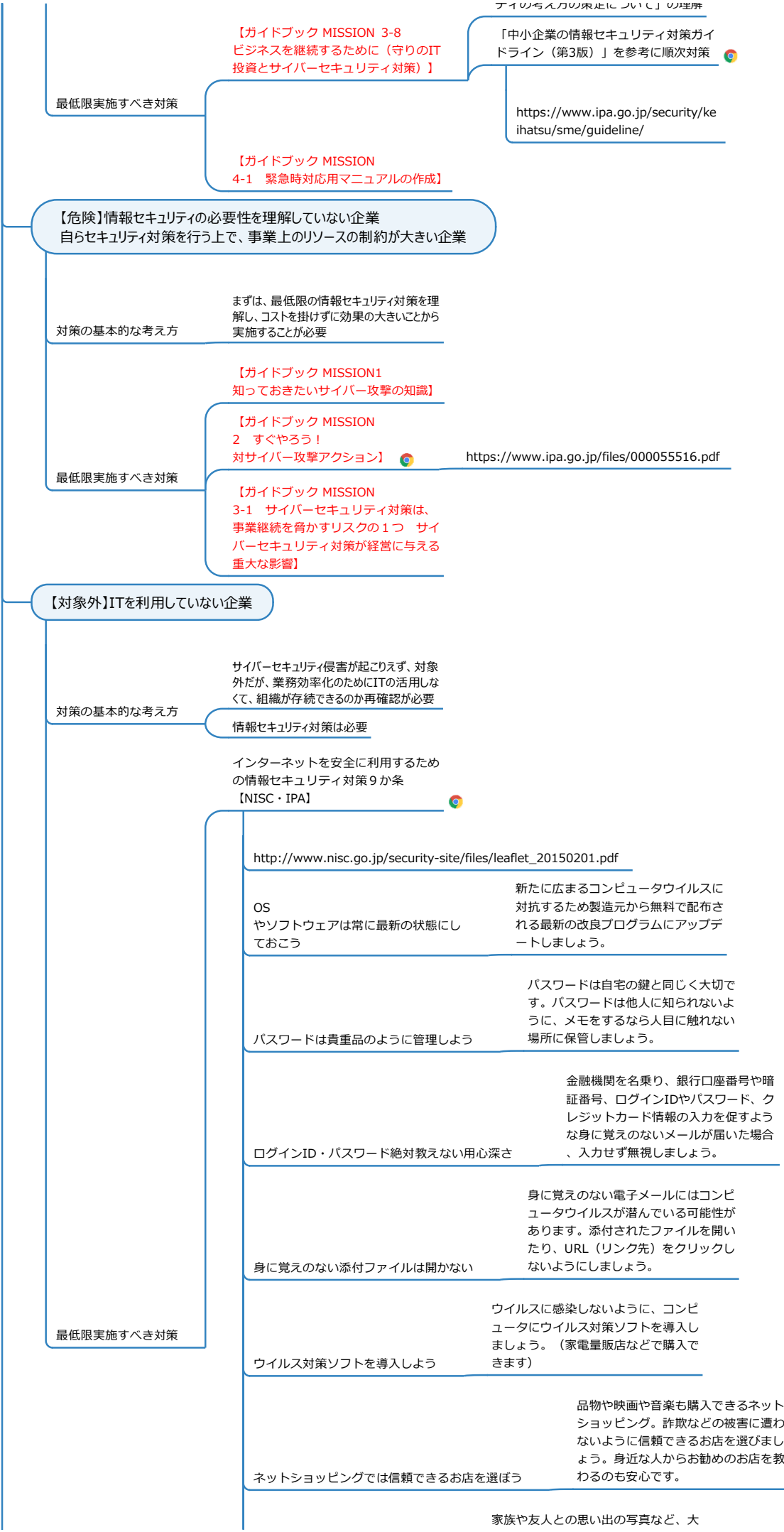
【危険】情報セキュリティ対策の必要性は理解しているが、必要十分なセキュリティ対策が出来ていないにも関わらず、ITの利活用を進めている企業

対策の基本的な考え方

情報セキュリティポリシーの策定と実践、定期的な監査が必要

創造力、発想力のある人材の育成が必要

ITスキルと知識を持った人材の育成が必要





大切な情報は失う前に複製しよう	切な情報がパソコンの故障によって失われることのないよう、別のハードディスクなどに複製して保管しておきましょう。
外出先では紛失・盗難に注意しよう	大切な情報を保存したパソコン、スマートフォンなどを自宅から持ち出すときは機器やファイルにパスワードを設定し、なくしたり盗まれないように注意で持ち歩きましょう。
困ったときはひとりで悩まず まず相談	詐欺や架空請求の電子メールが届く、ウイルスにより開いているウェブページが閉じないなどの被害に遭遇したら、一人で悩まず各種相談窓口に相談しましょう。

【付録】

一般論

自己診断

オンライン 5分でできる！自社診断&ポイント学習  http://www.nisc.go.jp/security-site/files/leaflet_20150201.pdf

パンフレット 5分でできる！情報セキュリティ自社診断シート・パンフレット  http://www.nisc.go.jp/security-site/files/leaflet_20150201.pdf

体系的な対策の検討を待たずとも、今すぐに最低限の事項を実施する

緊急的な対策を実施するに当たっては、診断結果に基づいて提示された資料を参考にする

経営者は、「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」の考え方を認識する 経営者がIT活用の必要性と、ITを活用するためにはセキュリティ対策が必要であることの認識

経営者は、「サイバーセキュリティ経営ガイドライン」に記載された事項を認識する

I. サイバーセキュリティは経営問題

セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要

セキュリティ投資は必要不可欠かつ経営者としての責務である。

II. 経営者が認識すべき3原則

(1)経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

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

(3)平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

III. サイバーセキュリティ経営の重要10項目

指示1：サイバーセキュリティリスクの認識、組織全体での対応方針の策定

指示2：サイバーセキュリティリスク管理体制の構築

指示3：サイバーセキュリティ対策のための資源（予算、人材等）確保

指示4：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

指示5：サイバーセキュリティリスクに対応するための仕組みの構築


指示6：サイバーセキュリティ対策におけるPDCAサイクルの実施

指示7：インシデント発生時の緊急対応体制の整備

指示8：インシデントによる被害に備えた復旧体制の整備

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

指示10：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

情報セキュリティ5か条（全2ページ） 

システム管理者は、「中小企業の情報セキュリティ対策ガイドライン」に記載された事項を具体的に実施する

<https://www.ipa.go.jp/files/000055516.pdf>

5分でできる！情報セキュリティ自社診断パンフレット（全8ページ）

<https://www.ipa.go.jp/files/000055848.pdf>

5分でできる！情報セキュリティ自社診断（全8ページ）

<https://www.ipa.go.jp/files/000055848.pdf>

情報セキュリティハンドブック（ひな形）（全11ページ）

<https://www.ipa.go.jp/files/000055529.pptx>

情報セキュリティ基本方針（サンプル）（全1ページ、35KB）

<https://www.ipa.go.jp/files/000072146.docx>

情報セキュリティ関連規程（サンプル）（全51ページ）

<https://www.ipa.go.jp/files/000055794.docx>

クラウドサービス安全利用の手引き（全8ページ）

<https://www.ipa.go.jp/files/000072150.pdf>

リスク分析シート（全7シート）

<https://www.ipa.go.jp/files/000055518.xlsx>

一般従業員は、「中小企業の情報セキュリティ対策ガイドライン」内の「情報セキュリティハンドブックひな形」に記載された事項を順守する

参考資料

ガイドブック「中小企業向けサイバーセキュリティ対策の極意」

<https://cybersecurity-tokyo.jp/security/guidebook/>

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】

<http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf>

サイバーセキュリティ戦略本部

<http://www.nisc.go.jp/conference/cs/index.html>

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

基本方針

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

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

I.基本的考え方

二つの基本的認識

<①挑戦> 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責任> 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、リスクを分析し、総合的に判断。
- 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。

II. 企業の視点別の取組

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

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）

【経営者に期待される認識】

- 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。
- 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。
- 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。

【実装に向けたツール】

- 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）
- 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

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）

【経営者に期待される認識】

- 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。
- 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。
- 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。

【実装に向けたツール】

- サイバーセキュリティ経営ガイドライン
- 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
- 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

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）

【経営者に期待される認識】

- 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もち、取り組む。
- 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。

【実装に向けたツール】

- 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）
- 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

サイバーセキュリティ経営ガイドラインVer2.0

【2021年4月26日最新版 METI】



https://www.meti.go.jp/policy/netsecurity/mng_guide.html

中小企業の情報セキュリティ対策ガイドライン（第3版）

【2021年3月10日最新版 IPA】



<http://www.ipa.go.jp/files/000055520.pdf>