

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

TOP SECRET

MISSION 3

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対策は、事業継続を脅かすリスクの1つ サイバーセキュリティ対策が 経営に与える重大な影響

POINT
1

ビジネスの継続のためにはITの活用は 不可欠

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、生産工程などの運用コストの削減・効率化のために、ITは大きな柱として活用されています。より一層の業務効率の改善や生産力向上を目指して、モバイル端末の活用や外部クラウドサービスの活用も進んでいます。





ITの活用にはサイバー攻撃などへの備えが必要

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、サイバー攻撃など）で事業資産や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ります。

サイバー攻撃は事前のセキュリティ対策によって、防御が可能です。



サイバーセキュリティ対策は経営者が自ら実行

サイバーセキュリティリスクは経営に重大な影響を及ぼす可能性がある一方で、投資効果が見えにくいことから、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップを発揮することが必要不可欠です。



サイバー攻撃を受けると 企業が被る不利益

金銭の損失

顧客の個人情報や取引先などから預かつた機密情報を万一漏えいした場合は、多大な損害賠償が発生します。また、インターネットバンキングの不正送金などで直接的な損失を被る企業も増えています。



顧客の喪失

サイバー攻撃を受けた企業は管理責任を問われ、社会的評価は低下し、顧客離れなど大きなダメージを受けることになります。風評被害がいつまでも続き、イメージが回復せず事業の存続が困難になる場合もあります。

業務の喪失

サイバー攻撃を受けると、被害の拡大を防止するため、システムを停止する措置が必要です。その間はメールすら使えなくなり、営業機会を喪失するとともに、社内の業務も停滞してしまいます。



従業員への影響

内部不正が容易に行えるような職場環境は、従業員のモラルを低下させます。また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされるとも考えられます。



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

経営者に問われる責任

POINT
1

経営者などに問われる法的責任

ITを利活用することは、顧客の個人情報を収集・活用する、他社への差別化として技術情報を活用するなど、さまざまな重要情報を取り扱います。そのため、企業とその経営者には高い責任が求められます。

企業が個人情報などを適切に管理していなかった場合、経営者や役員、担当者は刑事罰やその他の責任を問われることになります。場合によっては、経営者が個人として損害賠償責任を負うこともあります。



POINT
2

関係者や社会に対する責任

情報漏えいを引き起こした企業の経営者には、法的責任だけでなく、その情報の提供者や顧客に対して損害賠償や謝罪などが求められます。

また、会社を代表して、社会に対して情報漏えいの原因や再発防止策を明らかにする義務があります。

さらに、営業機会の喪失・売上高の減少・企業のイメージダウン・取引先との信頼関係の喪失などを引き起こすことにより、事業に大きなダメージを与え、経営者としての経営責任を果たすことができなくなります。



情報管理が不適切な場合に問われる法律

個人情報保護法

民法第709条（不法行為による損害賠償）

建設業法

マイナンバー法

不正競争防止法

金融商品取引法

詳細な罰則規定などはP184参照

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info



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



サイバーセキュリティ対策にかかる 費用の項目

サイバー攻撃に対するセキュリティ対策には、次のような項目があります。これらの項目を実現するためには、当然費用が発生します。





セキュリティ対策の投資効果を考える

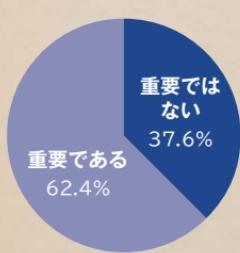
あなたの会社のインターネット接続と業務システムが1週間停止した場合のビジネスへの影響度を考えたことがありますか？

当然その間はメールもやり取りできないため、営業機会はなくなります。また、この時代にメールも送受信できないということで取引先との信頼関係もなくなります。

それらの損失を数字に置き換えたものがセキュリティ対策の投資効果です。



コラム IT投資が重要でないと考える会社はまだ4割近く



中小企業庁が実施した「中小企業の成長と投資行動に関するアンケート調査」によると、IT投資を重要ではないと考えている中小企業がまだ37.6%もあります。

※ ここでは、「最重要である」、「重要である」の回答項を「重要である」とし、「あまり重要ではない」、「重要ではない」の回答項目を「重要ではない」として集計しています。（「中小企業白書2016」より）



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

POINT
1

自社のIT活用状況を診断する

IT化において中小企業が注意したいのは、「IT化の範囲を一気に広げ過ぎない」という点です。中小企業が短期間であらゆる業務にITを導入しようとすると、コストの増大だけでなく、スケジュールが煩雑になり結果的に中途半端なクオリティーのシステムになるリスクがあります。下記の診断ツールが利用できます。

IT活用診断ツール

経済産業省：攻めのIT活用指針

全国商工会連合会：簡易事業診断（IT活用編）

POINT
2

IT活用診断の力は費用対効果

IT導入の目的は、既存ビジネスの効率化や新ビジネス展開などであり、IT化のための投資が、それによって得られる利益を上回っている場合は、投資を削減すべきです。

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

【理想的】

【分類1】 ITの利活用を事業戦略上に位置付け、サイバーセキュリティを強く意識し、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企業

**【もっと積極的】**

【分類2】 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付けていない企業

**【無駄な投資】**

【分類3】 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ていない企業

**【危険】**

【分類4】 サイバー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できていないにもかかわらず、ITの利活用を進めている企業

【分類5】 サイバーセキュリティの必要性を理解していない企業や、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

【対象外】

【分類6】 ITを利用していない企業



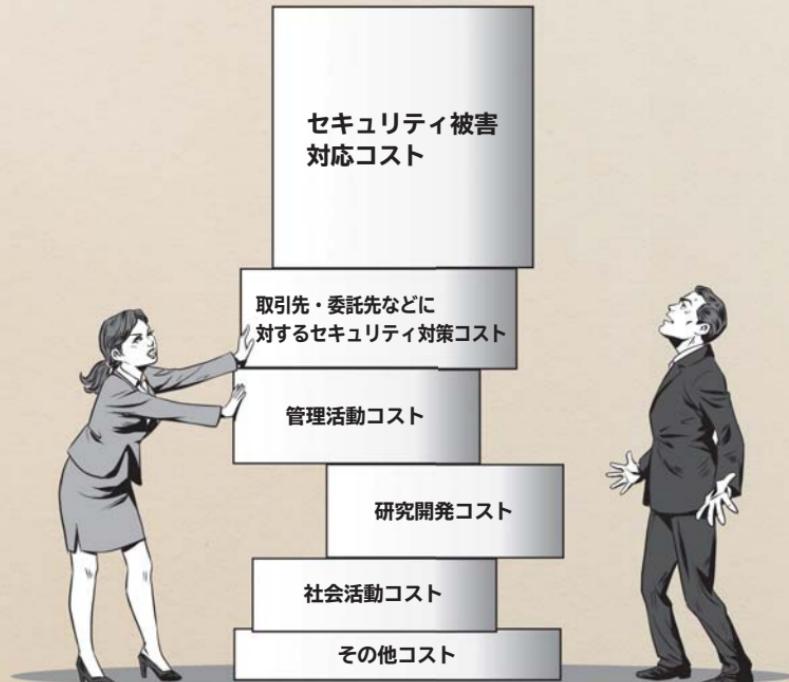
自社のIT活用・セキュリティ対策状況を自己診断する

サイバーセキュリティ 投資診断

POINT
1

サイバーセキュリティ投資（コスト）とは

サイバーセキュリティの投資（コスト）としては、P86に示した対策費用以外にも、さまざまなコストがあります。





サイバーセキュリティ対策はどこまでやればよいのか

これで万全というサイバーセキュリティはありません。特に、技術的対策にどれだけ投資してもリスクは残ります。管理的対策や人的対策を優先する方が効果的です。想定被害額を上回るセキュリティ対策費を費やすことは現実的ではありません。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す。

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
--------------------------------------	---	------------------

問題は残ったリスク（残留リスク）によって発生した被害の想定被害額が、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りますので、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じるか、支出可能な対策費を捻出する必要があります。

セキュリティ侵害発生時に支出可能な対策費	>	残留リスクによる想定被害額
-----------------------------	---	----------------------

残留リスクをどこまで許容できるかは、まさに経営者の判断です。



自社の IT 活用・セキュリティ対策状況を自己診断する

情報セキュリティ 対策診断

POINT
1

情報セキュリティ対策を診断する

企業（組織）はセキュリティ上の脅威に取り囲まれています。

- ・個人、顧客、企業（組織）情報を脅威から守る。
- ・会社内の設備を脅威から守る。

情報セキュリティ対策は常に新たな脅威に対応する必要があり、継続的に自社の対策状況を診断する必要があります。



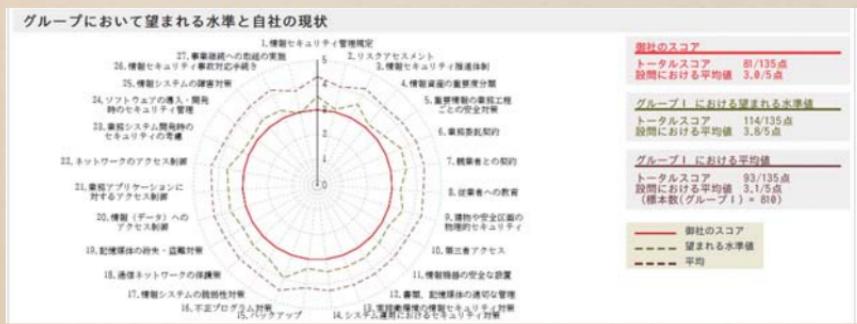
POINT 2

やってみよう！ 情報セキュリティ対策診断

- ・わが社のセキュリティ対策は大丈夫か？
- ・セキュリティ対策予算を増額したいが、どこにどう使ったらいいのか分からぬ。
- ・まだ取り組んでいないセキュリティ対策を考えたい。
- ・自社の情報セキュリティ対策状況はどこが弱点で、どこが強いのか知りたい。こうした要望に応えて、情報処理推進機構（IPA）では、「情報セキュリティ対策ベンチマーク」を提供しています。

情報セキュリティ対策ベンチマークは、設問に答えるだけで、自社のセキュリティレベルを他社との比較で診断することのできるシステムです。

散布図、レーダーチャート、スコア（点数）などの診断結果が自動的に表示されます。



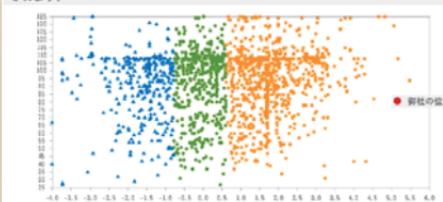
御社のスコア
トータルスコア 81/135点
設問における平均値 3.0/5点

グループ1における望まれる水準
トータルスコア 114/135点
設問における平均値 3.8/5点

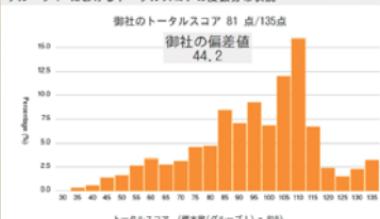
グループ1における平均値
トータルスコア 93/135点
設問における平均値 3.1/5点
(標本数(グループ1) × 80)

御社のスコア
--- 望まれる水準
— 平均

トータル・スコアの散布図（企業規模にかかわらず、全企業の分布と御社の位置が示されます）



グループ1におけるトータルスコアの度数分布状況



「情報セキュリティ対策ベンチマーク（企業・組織のためのセキュリティ対策自己診断ツール Ver.4.x）」（情報処理推進機構セキュリティセンター）より転載（一部加工）



(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)

業務の効率化、 サービスの維持のために

POINT
1

守りのIT投資と攻めのIT投資

守りのIT投資という言葉を聞いたことがありますか。

従来、IT活用は業務効率化やコスト削減を目的として、定型業務の自動化に集中していました。近年、売り上げ増加を目指したIT投資を「攻めのIT投資」と呼ぶようになり、従来のIT投資を「守りのIT投資」と呼んでいます。



POINT
2

業務の効率化にITを活用

経営者の皆さんが重視している経営課題の一つは、業務効率化やコスト削減です。

改善活動による業務効率化という手法は以前から展開されています。IT活用は、受発注業務や経理業務など、定型・繰り返しが多い業務プロセスを自動化、簡便化することに適しています。

POINT
3

生産性の向上やサービス向上のためにITを活用

ITを活用すれば、コスト削減だけでなく、業務のスピードアップ、品質向上、ミス低減など、生産性の向上にもつながります。また、生産状況の見える化などを通して、工程管理や生産管理など生産性を大幅に向上することも可能です。また、顧客サービスのスピードアップなどを通して、サービス力の向上にもつながります。





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)
**経営者が認識すべき
サイバーセキュリティ経営3原則**

原則 1

**サイバーセキュリティ対策は経営者の
リーダーシップで進める**

サイバー攻撃のリスクをどの程度容認するのか、セキュリティ投資をどこまでやるのか、経営者が決めなければサイバーセキュリティ対策はスタートしません。

従業員は安心して業務に集中できる環境を求めますが、利便性が低下し、面倒な作業を伴う対策には積極的に取り組めないこともあります。経営者が自らリーダーシップを発揮しなければ、サイバーセキュリティ対策は進みません。

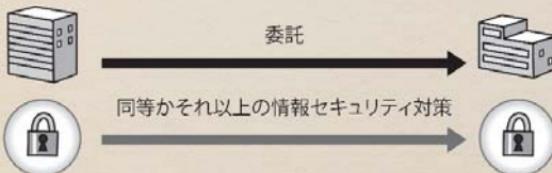


原則2

委託先のサイバーセキュリティ対策を把握する

子会社で情報漏えいが発生した場合はもちろんのこと、外部委託先に提供した情報がサイバー攻撃により流出してしまうことも経営にとって大きなリスク要因です。

自社のみならず、系列企業やサプライチェーンのビジネスパートナー、委託先などのサイバーセキュリティ対策に関する、必要に応じてサイバーセキュリティ対策の報告を求め、不十分な場合は対処を要請します。



原則3

関係者とのサイバーセキュリティに関するコミュニケーションはどんなときにも怠らない

顧客、取引先、委託先、代理店、利用者、株主などからの信頼を高めるには、普段からサイバーセキュリティ対策についての情報開示に努め、関係者との適切なコミュニケーションを図ることが必要です。





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)
経営者がやらなければならぬ
サイバーセキュリティ経営の重要10項目

重要10項目とは

リーダーシップ の表明と体制の 構築	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
	2	サイバーセキュリティ管理体制の構築
リスク管理の枠 組み決定	3	リスクの把握と対応計画の策定
	4	PDCAサイクルの実施と対策状況の開示
	5	系列企業・ビジネスパートナーの対策実施および状況把握
	6	予算確保・人材配置および育成
	7	ITシステム管理の外部委託
攻撃を防ぐため の事前の対策	8	情報収集と情報共有
	9	緊急時対応体制の整備とトレーニングの実施
	10	被害発覚後の必要な情報の把握、開示体制の整備

重要項目
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

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

POINT
1

なぜ重要なか？

経営者がサイバー攻撃を経営リスクとして対処することを宣言することにより、全ての従業員にサイバーセキュリティ対策の重要性を周知させることができます。経営者のサイバーセキュリティ対策宣言は、顧客、取引先、株主などの信頼性を高め、ブランド価値向上につながります。

POINT
2

やるべきことはこれだ！

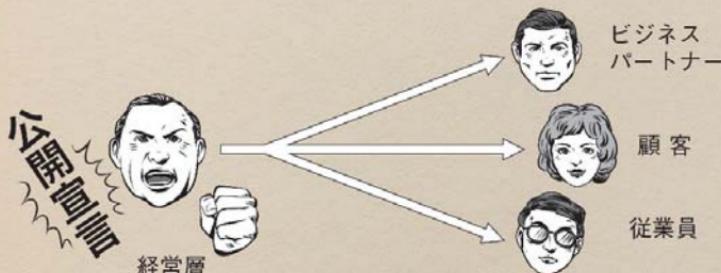
1. セキュリティポリシーを作成する。

セキュリティポリシーの作成には、情報処理推進機構（IPA）から、自社の事情に応じた内容に書き換えて作成することができるサンプルが提供されています。

2. セキュリティポリシーを、顧客、取引先、株主などに宣言する。

情報セキュリティポリシー作成手順 P128

情報セキュリティポリシーサンプルを使った作成手順P180~183



重要項目
2

サイバーセキュリティ管理体制の構築

POINT
1

なぜ重要なか？

仮にサイバー攻撃を受け、事業の継続性に支障が生じるようなシステム停止の判断が必要な局面で、サイバーセキュリティ管理体制を構築していない場合、経営者の判断を仰ぐしかいため、迅速に適切な対応ができない上に、責任の所在が不明確になります。

POINT
2

やるべきことはこれだ！

- 組織内に経営者レベルの権限を持った責任者を任命する。
- 責任者を中心としたサイバーセキュリティ管理体制を構築する。
- サイバーセキュリティ管理体制において各関係者の責任を明確にする。



重要項目
3

リスクの把握と対応計画の策定

POINT
1

なぜ重要なか？

企業の守るべき資産（個人情報や重要技術など）を把握していないと、直面するリスクを的確に把握できません。過度なリスク対策は、日常的なITの利活用を妨げ、事業活動に支障をきたす恐れがあります。また、企業として容認できない残留リスクが残る場合、想定外の損失を被る恐れがあります。

POINT
2

やるべきことはこれだ！

1. 企業の守るべき資産（個人情報や重要技術など）を決める。
2. サイバー攻撃の手口や脅威、被害状況を把握する。
3. サイバーセキュリティリスクが事業に及ぼす影響を想定し、リスクを把握する。
4. サイバーセキュリティリスクの影響の度合いに応じてリスク対策の目標や計画を策定する。また、許容できるリスクとして対策を講じないと判断したものを見落とさず、それを「**残留リスク**」とする。



INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

重要項目
4

PDCAサイクルの実施と対策状況の開示

POINT
1

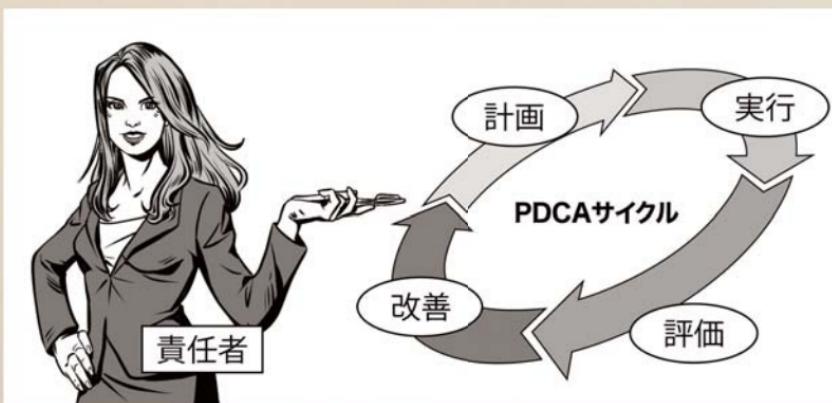
なぜ重要なか？

PDCAサイクルを実施しないと、環境の変化に合わせて、絶えずサイバーセキュリティ対策の見直しと改善を進めることができません。適切なセキュリティ対策の状況開示が行われなかった場合、ステークホルダーの不安感や不信感を引き起こすことになり、企業価値が損なわれる恐れがあります。

POINT
2

やるべきことはこれだ！

1. サイバー攻撃のリスクに対応したPDCAを実施できる体制を整備する。
2. 常に自社のサイバーセキュリティ対策の状況を把握し、必要に応じて経営者が改善のための指示をする。
3. セキュリティ上の新たなリスクがあった場合は、必要な情報を適切に開示する。



重要項目
5

系列企業・ビジネスパートナーの 対策実施および状況把握

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

POINT
1

なぜ重要なか？

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ります。その結果、他社の二次被害の誘因となる恐れや、加害者になる恐れもあります。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ることにより事業継続に支障が生じます。

POINT
2

やるべきことはこれだ！

系列企業やサプライチェーンといった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について、内容を契約書、報告書などで確認し状況を把握します。



重要項目
6

予算確保・人材配置および育成

POINT
1

なぜ重要なか？

適切な予算が確保できていない場合、会社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、信頼できる外部専門会社への委託が困難となる恐れがあります。

POINT
2

やるべきことはこれだ！

1. サイバーセキュリティ対策を実施するために必要な予算を確保する。
2. 必要となる人材の確保や、継続的な社員教育を実施する。



重要項目
7

ITシステム管理の外部委託

POINT
1

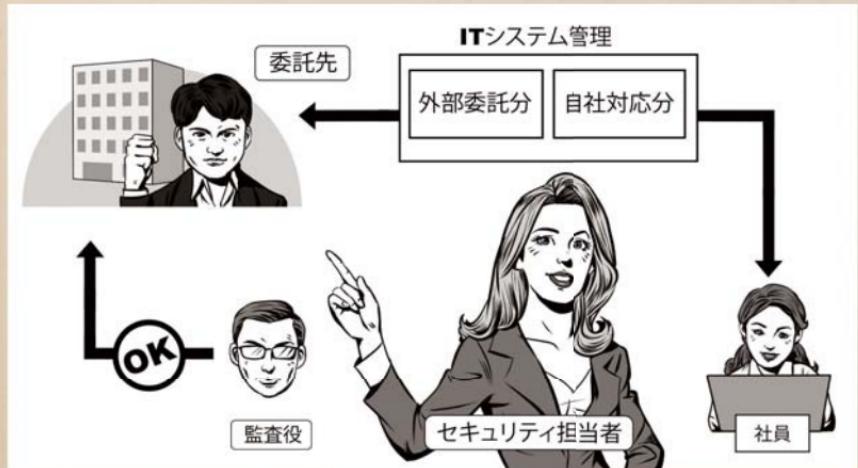
なぜ重要なか？

ITシステムなどの運用について、自社に技術的な能力が欠ける場合はシステム管理を十分に行えず、システムの脆弱性を突いた攻撃を受ける恐れが高まります。

POINT
2

やるべきことはこれだ！

1. 自社で実施すべき対策を把握する。
2. 自社で対策できるリソースがない場合は必要に応じて外部への業務委託を検討する。
3. 外部委託先のセキュリティレベルについて、安全が確保できるように定期的に確認する。



重要項目
8

情報収集と情報共有

POINT
1

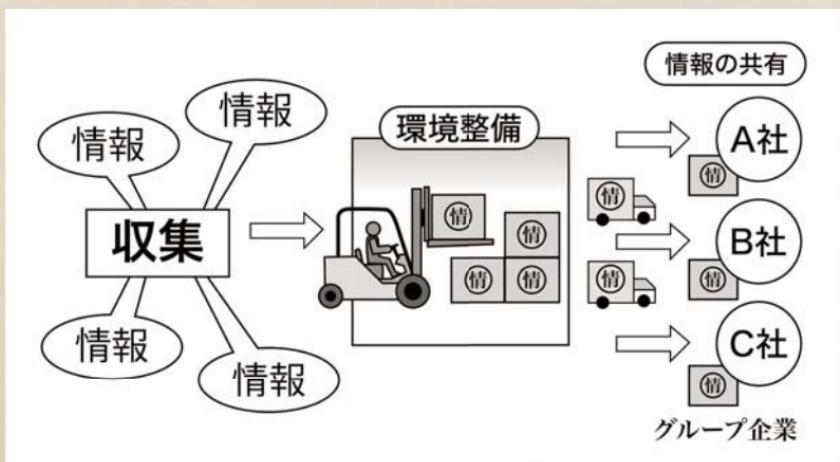
なぜ重要なか？

サイバー攻撃の手法や脅威などを効率的に収集するだけでなく、自社で発見した脆弱性情報や自社に対する攻撃に関する情報を公的機関に提供したり、関連会社などの企業内グループで共有したりすることで、同様の被害が社会全体に広がることを未然に防止できます。

POINT
2

やるべきことはこれだ！

1. 情報処理推進機構（IPA）やJPCERT コーディネーションセンターなどの情報を収集して活用する。
2. 情報を収集するだけでなく、自社の情報も積極的に提供する。
(P165参照)



重要項目
9

緊急時対応体制の整備とトレーニングの実施

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

POINT
1

なぜ重要なか？

緊急時の対応体制（社内の専門部署、緊急連絡先や初動対応マニュアル）が整備されていないと、速やかな原因特定、応急処置を取ることができません。サイバー攻撃を受けた場合は、平時とは異なる状況での判断を求められますので、さまざまなケースを想定した訓練や演習を繰り返し実施する必要があります。

POINT
2

やるべきことはこれだ！

1. 緊急連絡先や初動対応マニュアルなどを整備して対応体制をつくっておく。
2. 緊急時の対応手順の確認やトレーニングを定期的に実施する。



重要項目
10

被害発覚後の必要な情報の把握、 開示体制の整備

POINT
1

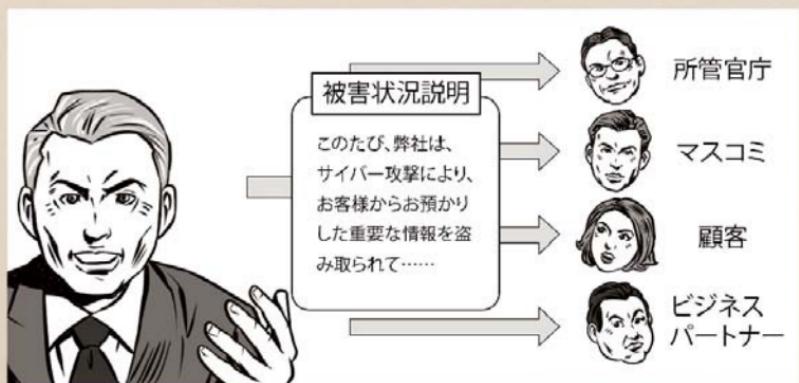
なぜ重要なか？

被害発覚後の対応で重要なことは、被害の拡大防止や二次被害の回避です。速やかに通知や注意喚起が行われない場合、顧客や取引先などへ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可能性があります。場合によっては法的責任を負うことになります。組織内情報管理の責任者である経営者が感染被害を発表しないと、ステークホルダーに対し、組織としての責任を果たしたことにはなりません。

POINT
2

やるべきことはこれだ！

1. サイバー攻撃の被害があった場合に備え、通知・報告するべき機関や関係先、またその内容を整理してマニュアル化しておく。
2. サイバー攻撃の被害について、経営者が顧客や取引先に報告・公表できるように準備しておく。



◆開示・報告先における注意点

開示・報告先	開示・報告時の留意点
所管官庁	<ul style="list-style-type: none"> 事前に先方の窓口を確認し、誰が報告するか決めておく。
サイバーセキュリティ関係機関 (IPA、JPCERT コーディネーションセンター)	<ul style="list-style-type: none"> サイバー攻撃の内容、実施していた対策、被害の概要などを報告する。 同種の攻撃手法による二次被害を避けるため、至急報告する。 (P165以降を参照)
報道機関／マスメディア	<ul style="list-style-type: none"> 窓口を一本化し、対外的な情報に不整合が起こらないようにする。 世評の影響も踏まえて、法務部門、広報部門などと連携し、適切な公表時期を慎重に判断する。 SNSなどのソーシャルメディアにより、社会的にどのように受け止められているか動向を確認する。 被害の状況に応じて、経営者が記者会見を行うことを想定し、公表する内容を検討する。
顧客	<ul style="list-style-type: none"> 被害者に至急その事実を通知しあわびするとともに、個人情報（顧客情報）漏えいの場合は、詐欺や迷惑行為などの被害に遭わないように注意喚起する。 被害者に連絡する方法（メーリングリストで一斉送信など）を確認・整備しておく。
ビジネスパートナー／同業者	<ul style="list-style-type: none"> 対処に必要な情報を速やかに関係者と共有する（外部委託先や、提携しているクレジットカード会社など）。 同業種を狙った一斉攻撃の可能性があるため、攻撃手法などを同業者間で共有する。



ビジネスを発展させるための（攻めのIT投資とサイバーセキュリティ対策）

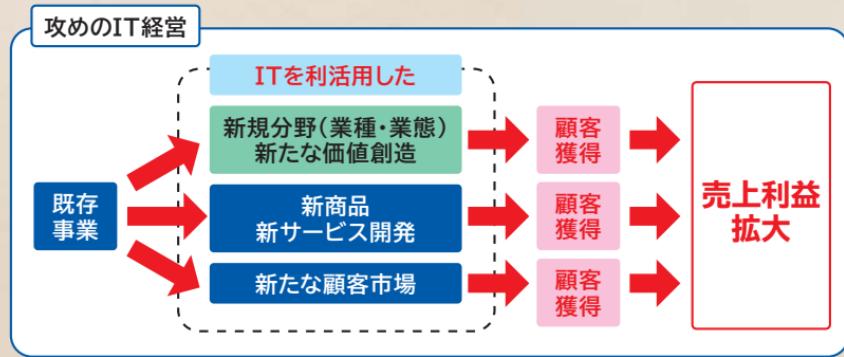
次世代技術を活用した ビジネス展開

POINT
1

攻めのIT投資とは？

ITを活用して製品・サービス開発に取り組み、ビジネスモデルを変革することや新たな価値を創出することが「攻めのIT経営」です。

積極的かつ柔軟にIT技術を受け入れて「攻めのIT経営」で事業を発展させ、より一層顧客サービスの強化を図るために攻めのIT投資が必要です。



「攻めのIT経営中小企業百選」（経済産業省）より

コラム 「攻めのIT経営中小企業百選」

経済産業省では、平成26年度から新たに、「攻めのIT経営中小企業百選」として、これまで100社の中の中小企業を選定しています。



攻めのIT経営中小企業百選

◆東京の企業の例（2016年選定）

株式会社旭フーズ (卸売業)	商品在庫情報の見える化で競争力強化
芝園開発株式会社 (サービス業)	IT活用による駐輪場管理ノウハウで、自治体向けビジネスを拡大
ジー・オー・ピー株式会社 (サービス業)	仮設機材使用量の山積み表自動作成で、提案型営業の強化と業績拡大
株式会社ダンクソフト (情報通信業)	サテライトオフィス構築支援事業で、働き方改革を提案
株式会社築地太田 (卸売業)	Tsukiji OFM Systemを活用し、海外輸出も積極拡大
プラスエンジニアリング株式会社 (製造業)	年間15,000種類の多品種少量・特殊形状部品加工を一元管理する自社開発業務システム
株式会社星製作所 (製造業)	デジタル経営戦略とWeb自動見積もりによる営業力強化
株式会社美萩工芸 (製造業)	営業支援システムなどの活用で大幅な効率化を図る
株式会社ユウトハンズ (印刷業・情報通信業)	文書管理システムの自社導入実績を元に、印刷業から新事業へ進出



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）

IoT、ビッグデータ、AI、ロボットの活用

POINT
1

業務・サービスの効率性を追求

あらゆる機器がインターネットに接続することで、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データを瞬時に分析できます。その結果を踏まえて業務やサービスを効率的、効果的に行なうことが始まっています。IoT※、ビッグデータ※、AI※、ロボットの活用は、人手不足に対応した省力化や、自動化のための投資という面でも期待されています。

※ IoT、ビッグデータはP114を、AIはP116を参照



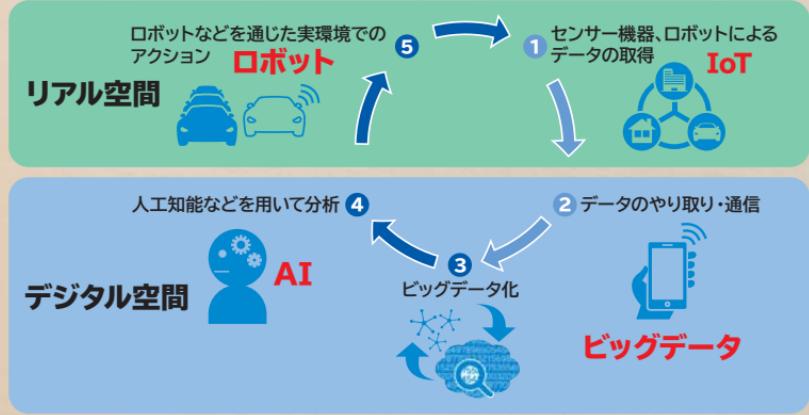
コラム IoT、ビッグデータ、AI、ロボットはつながっている

IoT、ビッグデータ、人工知能（AI）、ロボットなどの技術革新によって社会のあらゆる活動、情報がデータ化され、ネットワークによってつながることが可能な時代になりました。これらを組み合わせた機器やサービスが普及するとともに利活用を実現する事例が増えています。リアルタイムに分析を行い、新たなサービスや製品を生み出すことが可能になると、データそのものが創造の源泉になります。

商品やサービスの提供は個々のニーズに合わせてカスタマイズされ、個々のニーズとの効率的なマッチングが可能になります。AIやロボットはますます人間の役割をサポートし、部分的に代替するようになります。こうした状況にどう対応するかは、事業者にとっても重要なテーマです。

商品・サービスの開発や生産、さらには流通、アフターサービスなど、事業活動に上手に取り込むことができれば、将来の成長の大きな助けになります。

急速な技術革新により、大量データの取得、分析、実行の循環が可能に



「IoT、AI、ロボットに関する経済産業省の施策について」（経済産業省）より



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）

IoTが果たす役割と効果



IoTは中小企業にとって大きなビジネスチャンス

2020年にはIoT機器が530億台に達すると予測されています。ビジネスシーンにおいては、IoTがもたらすビッグデータ（蓄積された膨大なデータ）が新たな価値を見いだす資源として注目されています。中小企業にとっても、IoTが大きなビジネスチャンスになるのです。



コラム ものづくり企業 IoT活用事例

製造業（東京都青梅市）社員数：160名
自動車用金属加工部品、医療向け部品製造

スマートフォンを活用した「見える化システム」を自社開発。
自社の現場発ノウハウを、日本の中小製造業の発展に役立ててもらうために、システムの外販を決定

事例ポイント

社内のエンジニアが「欲しいもの」「必要なもの」をシステム化し、スマートフォンなどを活用して、リアルタイムで「経営と現場の見える化」を実現

概要

- ・出退勤、生産指示、在庫管理、工程不良管理、生産実績管理、品質管理、状況分析などをリアルタイムで棚卸しできる仕組み。経営と現場に「気付き」をもたらすために、独自のシステムを開発
- ・生産管理を中心としたWeb版の統合管理システムに、スマートフォンなどを活用した機械の稼働データを取得するための情報収集装置を組み合わせて「経営と現場の見える化」を実現
- ・IoTを利用した統合情報管理システムを中小製造業でも手が届く価格帯で実現することを目指し、IT関連企業と連携して、外販に向けた取り組みを開始

効果・メリット

現場に行かなければ分からなかった現在の作業状況を、遠隔からリアルタイムで管理可能。また作業者が入力したデータや、機械の稼働データに基づいた経営改善にも活用可能



スマートフォンを活用した
情報収集装置

「中小ものづくり企業IoT等活用事例集」（経済産業省 関東経済産業局 2017年）より抜粋・要約、写真転載（関東経済産業局 地域経済部 情報政策課）



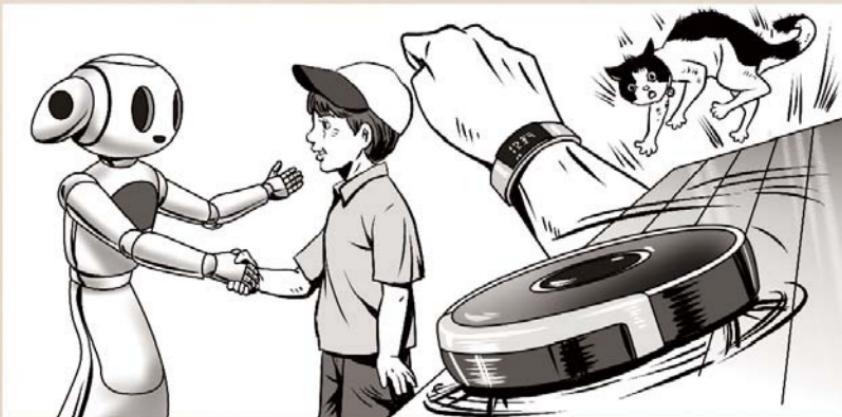
ビジネスを発展させるために（攻めのIT投資とサイバーセキュリティ対策）

人工知能(AI)が果たす役割と効果



急速に進化するAIを活用しよう

インターネットの検索エンジン、スマートフォンの音声検索アプリや音声入力機能、掃除ロボットなどの家電製品、さらに人型ロボットにも人工知能（AI：Artificial Intelligence）が搭載されています。身近となったAIを企業経営に活用することによって、経営上のさまざまな課題を解決するのみならず、新しい価値をも生み出します。



コラム 新しい価値を持った業務の創出

AIを含むICTの進化は雇用と働き方にも影響を及ぼします。

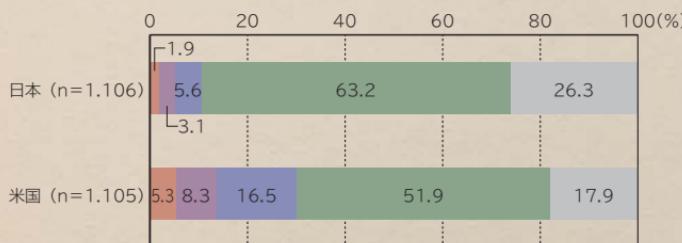
- 既存業務の人材不足の解消
- 不足している労働力の補完・省力化
- 既存の業務効率・生産性の向上（省力化）
- 新しい価値を持った業務の創出

などが期待されています。

<AIの進化で予想されること>

- 労働力不足や過酷労働などの緩和
- 農業・漁業の自動化による人手不足問題の緩和
- 犯罪の発生予知、事故の未然防止
- 個々人の必要に応じたきめ細かいサービスの提供
- 医療データの活用などによる課題解決
- 職人の知識、ノウハウの体系化による維持と伝承

最近のAI導入状況



- 既に導入されており、活用（利用）したことがある
- 既に導入されているが、これまでに一度も利用（活用）したことはない
- 現在は導入されていないが、今後、導入される計画がある（計画中・検討中）
- 現在導入されていないし、今後も導入される計画はない
- わからない

総務省「ICTの進化が雇用と働き方に及ぼす影響に関する調査研究」（平成28年）より作成



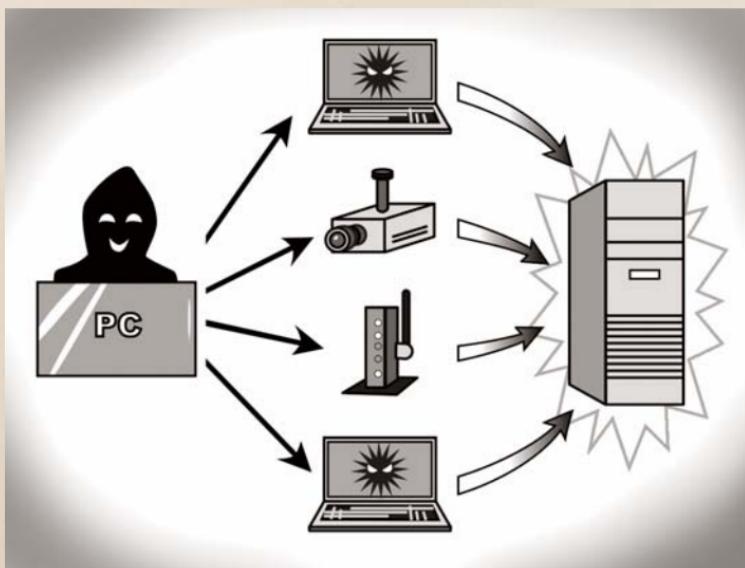
ビジネスを発展させるために（攻めのIT投資とサイバーセキュリティ対策）

IoTを活用する際のサイバーセキュリティ上の留意点

POINT
1

IoTへの脅威

これから飛躍的な増加が予想されるIoT機器ですが、一方でセキュリティ対策が十分とはいえないのが現状です。そのため、IoT機器をターゲットとしたサイバー攻撃が増大することも懸念されています。利用する際には、それを前提とした対策が欠かせません。（対策はP120参照）



インターネットから自動車の脆弱性を突かれ、ハンドルやエンジンなどが遠隔操作される



ホテルの部屋に設置してある通信機器・設備が不正に遠隔操作される



ペースメーカーや植え込み型除細動器が不正操作される





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）

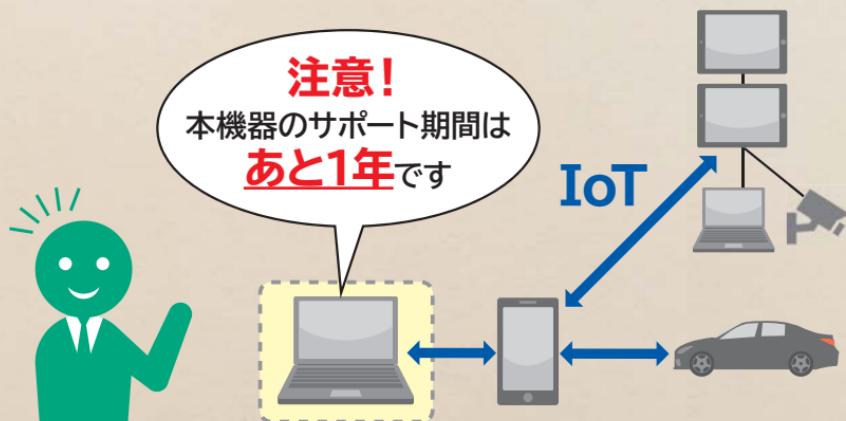
IoTを活用する一般利用者のための基本ルール

POINT
1

リスクの大半は簡単な注意で回避可能

IoT機器もパソコンなどと同様、サイバーセキュリティ対策を怠ってはいけません。インターネットを経由して遠隔操作され会社の重要情報が漏えいする、機器が悪用されて犯罪に巻き込まれるなど、サイバー脅威にさらされる危険性をはらんでいるからです。

こうした脅威から会社を守るために、基本的なルールを確認しましょう。



ルール
1

問い合わせ窓口やサポートのない機器やサービスの購入・利用を控える

機器やサービスの問い合わせ窓口やサポートがない場合は、不都合が生じたとしても、適切に対処することが困難になりますので、サービスの購入・利用は控えましょう。

ルール
2

初期設定に気を付ける

機器を初めて使用する際には、IDやパスワードの設定を適切に行います。パスワードの設定では、「機器購入時のパスワードを必ず変更する」「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回さない」などに気を付けましょう。また、取扱説明書などの手順に従って、自分でアップデートを実施しましょう。

ルール
3

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まま放置すると、不正利用される恐れがあります。使用しなくなったWebカメラやルーターなどをそのまま放置せず、電源プラグを抜きましょう。

ルール
4

使用しなくなった機器は必ずデータを消す

情報が他の人に漏れることのないよう、機器廃棄・下取りなどのときは、事前にデータを削除しましょう。

「IoTセキュリティガイドライン」（総務省 経済産業省 平成28年7月）より

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

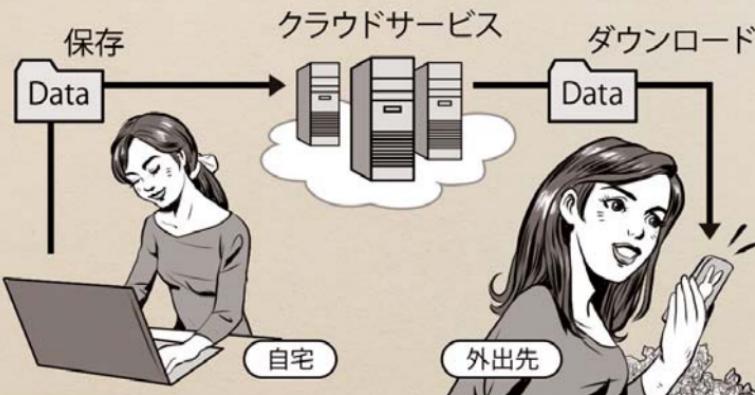
コラム クラウドサービスの活用

クラウドサービスとは

クラウドサービスは、従来は利用者が手元のパソコンなどにインストールして利用していたデータやソフトウェアを、事業者がネットワーク経由でサービスとして提供するものです。インターネットに接続できる環境であればすぐに導入できます。

<メリット>

- ・自社サーバーや情報処理ソフトウェアを保有する必要がなく、初期コストを抑えられる。
- ・常に最新のサービスを利用できる。
- ・メンテナンスする必要がなく運用コストが安い。
- ・サービスの利用範囲を必要に応じて変更できる。
- ・導入や維持について社内担当者の負担が軽減される。
- ・出張先や自宅からも利用できる。



クラウドサービス利用時の留意点

クラウドサービスでも、ネットワークを介して攻撃を受ける可能性や人為的な操作ミス、意図的な情報漏えいなど、情報セキュリティ面でのリスクは、自社でサーバーを保有する場合と同じようにあります。

自社の情報資源をクラウド事業者に委ねる以上は、十分なセキュリティ対策を備えたクラウドサービスを選んで利用することが重要です。

<デメリット>

- ・障害などによりデータが消失する可能性がある。
- ・サイバー攻撃に対するセキュリティ対策のレベルは事業者に委ねられている。
- ・アカウント情報が第三者の手に渡ってしまった場合、簡単に情報漏えいしてしまう。
- ・基本的にパッケージ化されたシステムが提供されるため、自由にカスタマイズしにくい。





セキュリティホールを減らす網羅的・体系的対策の策定方法
**新・5分でできる
自社診断シート**

ACTION
1

すぐに活用しよう!

「中小企業の情報セキュリティ対策ガイドライン」(情報処理推進機構<IPA>)には<新・5分でできる！情報セキュリティ自社診断>があります。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、その解説が付いています。

●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/index.html>
よりダウンロードできます。

<新・5分でできる！情報セキュリティ自社診断>の構成

Part 1 基本的対策

OSやソフトウェアのアップデート、ウイルス対策ソフト、パスワード、アクセス制限などの基本的対策についての設問

Part 2 従業員としての対策

メールの受送信や重要情報の取り扱い、パソコン対策などについて、全ての従業員が注意しなければならないことについての設問

Part 3 組織としての対策

情報セキュリティ対策について、従業員に対する意識付けやルール、事故が発生した場合など会社が行う対策についての設問

<新・5分でできる自社診断シート> (部分抜粋)

説明項目	No	診断内容	チェック				自社影響 アドバイス 対応している手 法
			実施して いる	実施して していない	実施して していない	わからない	
Part 1 基本的な対策	1	Windows Update月1を行なうなどのように、常にOSやソフトウェアを安全な状態にしていますか？	4	2	0	0	PCのOSや各種サ ービスの自動更新 を行なっています
	2	パソコンにウイルス対策ソフトを入れてウイルス定義ファイル毎月2回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なっていますか？	4	2	0	0	PCのウイルス 対策を行なっています
	3	個人情報漏洩しないなどないように、個人情報を扱う際は必ず個人情報を保護して取り扱っていますか？	4	2	0	0	個人情報を保護す るために個人情報 保護法を遵守して います
	4	ネットワーク接続の場合はドライバ、ログの有効期限を超過しないなどに設定されていますか？	4	2	0	0	ネットワーク接 続のドライバを最 新版に更新してい ます
	5	利用中のウイルスバスターもまた、マイクロソフトのセキュリティ（定期的）確認で内部構成 するなどのように、既存の脅威に対するセキュリティ内包有りを定期的に確認していますか？	4	2	0	0	定期的にセキュリ ティを確認してい ます
Part 2 従業員としての 対策	6	貴組織で不正アクセス等による漏洩（アダルトサイト等）を本気で心配し、日々今後の行動を参考に準備したり ないようにしているなど、メールを開いた時に迷惑感に気が付いていますか？	4	2	0	0	組織がセキュリ ティを重視する方 向でメールを開いた 時に迷惑感を抱いて います
	7	電子メール送受信には必ず添付附件アドバイスを確認するなどのように、危険な連絡先を防ぐ ために組織で徹底しているですか？	4	2	0	0	PCのメールアド バイスを確認して います
	8	蜜語情報をメモで保管する蜜語情報を添付ファイルで書いてパスワード保護するなどのように、蜜語情報を保護して いますか？	4	2	0	0	蜜語情報をメモで 保管する蜜語情報を 添付ファイルで書いて パスワード保護する ようにしています
	9	組織(AN)を操作する時は画面暗闇化を必ず利用するなどのように、画面暗闇化を止められた場合の対策をしていますか？	4	2	0	0	組織(AN)を操作す る時は画面暗闇化 を必ず利用しています
	10	廃棄箱などでウイルスサイトの既読やSMSへの書き込みを隠す規則を決めた方でなくとも、インクジェットまたはトナーカートリッジの廃棄をしていますか？	4	2	0	0	廃棄箱などでウイ ルスサイトの既読 やSMSへの書き込み を隠す規則を決め ています
	11	蜜語情報を（ワープラント）を定期的に行なうなどのように、蜜語や鍵操作などを複数して蜜語帳が 消失しないよう管理しているですか？	4	2	0	0	蜜語情報を（ワープ ラント）を定期的 に行なうようにして います
	12	蜜語情報をどのようにして保管せずに保存し削除するなどのように、蜜語情報を紛失や漏洩を防止す る対策をしていますか？	4	2	0	0	PCの蜜語情報を 定期的に削除して います
	13	蜜語情報を外に持ち出すことはせず（パスワード記録や暗号化して身動きできないなどのように、当機や 端末の消滅を防いでいますか？	4	2	0	0	PCの蜜語情報を 外に持ち出さない ようにしています
	14	蜜語情報をコンピュータのロック機能を利用して保護するなどのように、他人に使われないようにしていますか？	4	2	0	0	蜜語情報をコンピ ュータのロック能 力を保護しています
	15	廃棄箱で荷物らしきを見かけたら再をかけるなどにより、偽許印の入り立ちがないようにしていますか？	4	2	0	0	廃棄箱で荷物らしき を見かけたら再をか けるなどにより、偽許 印の入り立ちがないよ うにしています
	16	銀行ATMでの取扱い方法を記憶し出し方に付けておきましょうか？どうより、盗難防止 の仕組みを理解していますか？	4	2	0	0	銀行ATMでの取 扱い方法を記憶し 出し方に付けてお きましょうか？どう より、盗難防止の仕 組みを理解してい ます

〈解説パンフレット〉

新機能	
(Part 1) 基本的対戦	
初心者～上級者向けの対戦モード。AIとの対戦や、他のプレイヤーとの対戦などを楽しむことができます。	
対戦モード～ No.1 対戦モード	対戦モード～ No.2 パーティモード
DDoSアタックモード 対戦モードの拡張版です。	複数台のパソコンに接続可能な MyJVN/一ジャンケンチャッカ
DDoSアタックモードは、DDoS攻撃をシミュレートするモードで、それを通じてハッキング技術を学ぶことができます。また、DDoSアタックモードでは、DDoS攻撃の仕組みを理解するための説明文が表示されます。	DDoSアタックモードでは、DDoS攻撃の仕組みを理解するための説明文が表示されます。
対戦モード～ No.3 対戦モード	対戦モード～ No.4 パーティモード
Windows の脆弱性 対戦モードの拡張版です。	複数台のパソコンに接続可能な MyJVN/一ジャンケンチャッカ
Windows の脆弱性モードは、Windows の脆弱性を確認するモードです。アドバイス機能を用いて、脆弱性を確認する手順を教えてくれます。	Windows の脆弱性モードでは、Windows の脆弱性を確認する手順を教えてくれます。
対戦モード～ No.5 対戦モード	対戦モード～ No.6 パーティモード
ウムツバキワード 対戦モードの拡張版です。	複数台のパソコンに接続可能な MyJVN/一ジャンケンチャッカ
ウムツバキワードモードは、暗号化技術を学ぶモードです。アドバイス機能を用いて、ウムツバキワードを確認する手順を教えてくれます。	ウムツバキワードモードでは、ウムツバキワードを確認する手順を教えてくれます。
対戦モード～ No.7 対戦モード	対戦モード～ No.8 パーティモード
セキュリティ 対戦モードの拡張版です。	複数台のパソコンに接続可能な MyJVN/一ジャンケンチャッカ
セキュリティモードは、セキュリティに関する知識を確認するモードです。アドバイス機能を用いて、セキュリティに関する知識を確認する手順を教えてくれます。	セキュリティモードでは、セキュリティに関する知識を確認する手順を教えてくれます。
対戦モード～ No.9 対戦モード	対戦モード～ No.10 パーティモード
大失敗回復モード 対戦モードの拡張版です。	複数台のパソコンに接続可能な MyJVN/一ジャンケンチャッカ
大失敗回復モードは、失敗したときに何をすべきかを確認するモードです。アドバイス機能を用いて、失敗したときに何をすべきかを教えてくれます。	大失敗回復モードでは、失敗したときに何をすべきかを教えてくれます。
対戦モード～ No.11 対戦モード	対戦モード～ No.12 パーティモード
DDoSアタックモード 対戦モードの拡張版です。	複数台のパソコンに接続可能な MyJVN/一ジャンケンチャッカ
DDoSアタックモードは、DDoS攻撃をシミュレートするモードで、それを通じてハッキング技術を学ぶことができます。また、DDoSアタックモードでは、DDoS攻撃の仕組みを理解するための説明文が表示されます。	DDoSアタックモードでは、DDoS攻撃の仕組みを理解するための説明文が表示されます。



セキュリティホールを減らす網羅的・体系的対策の策定方法

情報セキュリティハンドブック ひな形（従業員向け）

ACTION
1

すぐに活用しよう！

「情報セキュリティハンドブック（ひな形）」を使えば、従業員に自社のセキュリティルールを確認してもらうためのハンドブックが簡単に作成できます。赤い文字色で記載例があらかじめ記載されています。自社のルールに合わせて赤字を中心に修正し、また必要に応じて項目を加筆して効率よく使うことができます。

●情報セキュリティハンドブック（ひな形）

<https://www.ipa.go.jp/files/000055529.pptx>よりダウンロードできます。



<内容構成>

- 全社基本ルール
- 仕事中のルール
- 全社共通のルール
- 従業員のみなさんへ

＜情報セキュリティハンドブックひな形（従業員向け）＞（部分抜粋）

Vol.12

情報セキュリティ ハンドブック (ひな形)

「ハンドブックの使い方」

本ハンドブック(ひな形)は、従業員に配付し
会社のセキュリティルールを理解してもらいた
めのものです。うかがてできる「情報セキュリ
ティ白書診断」に連携しています。赤字で記載し
た箇所は教訓にあります。会社のルール
にあわせて赤字を用心に修正し、また必要に足
る箇所を加筆して、ご利用ください。

2-1 仕事中のルール

電子メールの利用

*メールアドレスは「T」のように記入し、宛先のアドレス欄に記載していくのが一般的です。

(Microsoft Outlook標準機能)

- ▶ フィルト→オフィス→個人用設定完了→通常受信項目にある「発信者から署名に追加する」チェック外す→「OK」
- ▶ 通常トレイ(スイートボックス)をクリックして受信側がからめてのサムネイルで通常受信をクリックする。

*相手が外勤などで不在時にメールを送る場合は、宛先(TO)に自分自身のIDを入れ、BCCで相手の名前をアド入力を実行する。

*重要な情報または個人情報を送付する場合は、本文に記入せず、以下の方法で行う。

- ▶ 重要な情報などは個人情報等添付ファイルに記載して、ワードの設定、またはワードドキュメントのワードとして複数あります。
- ▶ パワーポイントがある場合があります。また複数端末で共有する際のパスワードが発行されないことがあります。



1-1 全社基本ルール											
OSとソフトウェアのアップデート											
<p><OSのファームウェア></p> <p>・最新版のOSをインストールする。[Windows]の場合は「Windows Update」。 ■最新版が入手できるマートの店舗の以下で簡単に手軽に更新可能。</p> <ul style="list-style-type: none"> ▶ ハードウェア販売店の「Windows Update」専用端末にて対応する。 ▶ パソコンの販売店「Windows Update専用端末」にて対応する。 <p>・ファームウェアは必ずバージョンを確認し、常にデータの最新化を実現する。</p> <p>■ドライバのファームウェア。</p> <p>■Microsoft Officeは定期的更新設定を設定する。</p> <p>■Adobe Flash Player, Adobe Readerは自動更新設定を設定する。</p>											
 <p>最新版スマートフォン連携機能を実現。スマートフォンのQRコードを読み取ることで、最新版のファームウェアを自動的にダウンロードする事で、お使いの端末を常に最新版へアップグレードできます。</p>											
ウイルス対策ソフトの導入											
<p>●定期的に利用する機器に以下のウイルス対策ソフトを導入し、実行ファイルを定期的に更新する。 持出用ノートPCもこの規程に適用。実行ファイルの更新を確認する。</p> <ul style="list-style-type: none"> ▶ オンラインのウイルス対策ソフト(アントウイルス)を導入する。(各機器) ▶ タイプ別導入: 000001の機器は専用版にて定期的に更新する。出荷日(初期) 											
パスワードの管理											
<p>#ログインやファイル暗号化に使うパスワードは、以下によって設定・使用する。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">※小・中</th><th style="text-align: center;">× 高士</th></tr> </thead> <tbody> <tr> <td style="text-align: center;">1文字以上上で連続する2文字以上</td><td style="text-align: center;">必ず 曜日+誕生日を組み合わせる</td></tr> <tr> <td style="text-align: center;">アルファベットと数字と大小文字と記号(8)</td><td style="text-align: center;">同じ文字・数字を組み合わせしない</td></tr> <tr> <td style="text-align: center;">[T]Xなどの記号を使わない</td><td style="text-align: center;">同じ文字・数字を組み合わせない</td></tr> <tr> <td style="text-align: center;">ID+パスワード重複しない</td><td style="text-align: center;">意者に見えなくて、SUSCRIBERIDがない</td></tr> </tbody> </table>		※小・中	× 高士	1文字以上上で連続する2文字以上	必ず 曜日+誕生日を組み合わせる	アルファベットと数字と大小文字と記号(8)	同じ文字・数字を組み合わせしない	[T]Xなどの記号を使わない	同じ文字・数字を組み合わせない	ID+パスワード重複しない	意者に見えなくて、SUSCRIBERIDがない
※小・中	× 高士										
1文字以上上で連続する2文字以上	必ず 曜日+誕生日を組み合わせる										
アルファベットと数字と大小文字と記号(8)	同じ文字・数字を組み合わせしない										
[T]Xなどの記号を使わない	同じ文字・数字を組み合わせない										
ID+パスワード重複しない	意者に見えなくて、SUSCRIBERIDがない										

3-1 全社共通のルール

私有情報機器の利用

*私物の情報機器を業務で利用する場合は以下と操作する。

情報機器の種類	遵守事項
パソコン モニタ等のPC端末 スマートフォン等の携帯電話 機器等を含む	<ul style="list-style-type: none"> ①室内、施設で持ち込むことを禁止する ②使用料金は個人負担 ③個人の機器を公的機器として使うことは禁止する ④ウイルス対策、アバランチソフトは既存部機器にインストールしてから導入し、許可料金を支払う場合がある ⑤複数台の端末一括で登録料金一括で支払う場合は複数台の端末の料金を支払う ⑥個人の機器を公的機器として個人的に新規契約を行う時は契約者本人に責任を負う ⑦料金を支払う場合は、料金を支払った後は個人の機器を公的機器として使うことを止める ⑧はたらくかかわらず運営上必要とする時は運営元のアドレスにて封鎖する旨を記載して提出する
スマートフォン タブレット端末 機器等を含む	<ul style="list-style-type: none"> ①会員登録した機器を登録する ②個人情報、会員登録内容は個人情報を売却せず ③契約登録は、社内に登録しないで登録料金を支払う ④スマートフォン等の機器をタブレット等の機器に変更する場合は、機器登録料金を支払う ⑤機器登録料金を支払った場合は、機器登録料金を支払う ⑥登録料金を支払った場合はタブレット等の機器登録料金を支払う ⑦はたらくかかわらず運営上必要とする時は運営元のアドレスにて封鎖する旨を記載して提出する
iPhone等 Android等の タブレット端末 機器等を含む	<ul style="list-style-type: none"> ①会員登録した機器を登録する ②個人情報、会員登録内容は個人情報を売却せず ③契約登録は、社内に登録しないで登録料金を支払う ④スマートフォン等の機器をタブレット等の機器に変更する場合は、機器登録料金を支払う ⑤機器登録料金を支払った場合はタブレット等の機器登録料金を支払う ⑥登録料金を支払った場合はタブレット等の機器登録料金を支払う ⑦はたらくかかわらず運営上必要とする時は運営元のアドレスにて封鎖する旨を記載して提出する



セキュリティホールを減らす網羅的・体系的対策の策定方法
情報セキュリティポリシーの明文化

**ACTION
1**

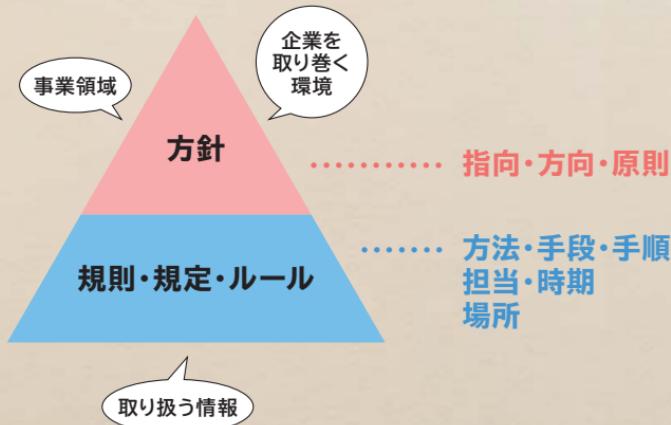
すぐに活用しよう!

情報セキュリティポリシーをゼロからつくり上げるのは、多くの中小企業にとって難しい作業です。

情報処理推進機構（IPA）では、中小企業・小規模事業者向けに、情報セキュリティポリシー作成ツールを提供しています。自社のリスクを分析し、状況に合わせて情報セキュリティポリシーサンプルを編集すれば、自社に合った情報セキュリティポリシーを簡単に作成することができます。

まず、こうしたツールを活用して、自社の情報セキュリティポリシーを策定し、スキルの向上とともに追加変更していきます。

情報セキュリティポリシーサンプルを使った作成手順P180~183



ポリシーの策定には「わが社の情報セキュリティポリシー（付録）」を使い、以下の手順で行います。

手順 1

情報資産管理台帳を作成する

自社で保有している情報を<ツールA リスク分析シート>の「情報資産管理台帳」シートへ記入例に従い書き出し、それぞれの重要度を判定してください。

重要度2 事故が起きると事業に深刻な影響がある
 重要度1 事故が起きると事業に重大な影響がある
 重要度0 事故が起きても事業に影響はない

手順 2

リスク値の算定

<ツールA リスク分析シート>の「脅威の状況」シートで想定される脅威を指定し、「対策状況チェック」シートで自社の対策状況を指定すると情報資産ごとのリスク値が計算されて対策が必要な情報資産が分かれます。

リスク値4～6	大	重点的に対策を実施
リスク値1～3	中	対策を実施
リスク値 0	小	現状維持

手順 3

情報セキュリティ対策を決定

<ツールA リスク分析シート>の「対策状況チェック」シートで自社の対策状況を以下から選択すると、「診断結果」シートに診断結果と自社で策定すべく情報セキュリティポリシーが表示されます。

- | | |
|-----------------|------------------------|
| 1：実施している | …対策を実施済みの場合 |
| 2：一部実施している | …対策を実施しているが、十分でない場合 |
| 3：実施していない／わからない | …対策を実施していないか、関連情報がない場合 |
| 4：自社には該当しない | …当該項目に該当する業務を行っていない場合 |

手順 4

情報セキュリティポリシーを策定

手順3で表示された情報セキュリティポリシーを<ツールB 情報セキュリティポリシーサンプル>の中から選択し、自社の状況に合わせて編集すれば、自社専用の情報セキュリティポリシーが完成します。

なお必要に応じて、さらに項目を追加していただいてもかまいません。

重要度は機密性、完全性、可用性それぞれの観点での評価値から3段階で判定します。

また、被害発生可能性は、情報の内容ごとの脅威の発生頻度×脆弱性への対応状況により3段階で算定し、「リスク値＝重要度×被害発生可能性」でリスク値を診断します（手順2）。これで対策の必要な情報資産が分かれます。

さらに、現段階での対策実施状況により、策定すべき情報セキュリティ対策が表示される仕組みです（手順3）。



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

情報資産管理台帳の作成

ACTION
1

どのような情報資産があるか洗い出して 重要度を判断する

情報セキュリティポリシーの策定に当たっては、組織の事業継続のためにセキュリティを確保すべき情報資産としてどのようなものがあるかをリストアップします。個々の情報の重要度を判断するため、情報資産管理台帳を作成し、自社の情報資産を洗い出します。

<ツールA「リスク分析シート」情報資産管理台帳 記入例>

情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類		
						個人情報	要配慮個人情報	マイナンバー
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	書類			
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	可搬電子媒体			
営業	キャンペーン応募者リスト	20xx年のキャンペーン応募者情報	営業部	営業部	社内サーバー	有		
調達	委託先リスト	外部委託先(直近5年間に実績があるもの)	総務部	総務部	社内サーバー			
調達	発注伝票	発注伝票(過去10年分)	総務部	総務部	社内サーバー			
調達	発注伝票	発注伝票(過去10年分)	総務部	総務部	書類			
技術	製品設計図	現役製品の設計図	開発部	開発部	社内サーバー			
①	②	③	④	⑤	⑥	⑦		
技術	製品設計図	現役製品の設計図	開発部	開発部	書類			



情報資産管理台帳の作成

情報処理推進機構（IPA）では、中小企業・小規模事業者向けに、情報資産管理台帳作成ツールを提供しています。

作成ツールのテンプレートを活用すると効率的に情報資産管理台帳を作成できます。作成ツールでは、情報資産の機密性※や完全性※、可用性※それぞれの評価値を記入し重要度を判定します。

さらに、「脅威の状況」「対策状況チェック」の2枚のシートでリスク値を診断します。

組織的対策や人的対策など11項目について対策状況チェックの診断結果が表示されます。

※ 機密性、完全性、可用性についてはP72参照。

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

info

機密性	完全性	可用性	重要度	保存期限	登録日	現状から想定されるリスク（入力不要・自動表示）			
						脅威の発生頻度（「脅威の状況」シートで設定）	脆弱性（「対策状況チェック」シートで設定）	被害発生可能性	リスク値
0	1	1	1		2016/7/1	2特定の状況で発生する（年に数回程度）	2部分的に脆弱性未対策	1 可能性：低	1 リスク中
0	1	1	1		2016/7/1	2特定の状況で発生する（年に数回程度）	2部分的に脆弱性未対策	1 可能性：低	1 リスク中
2	1	0	2		2016/7/1	3通常の状態で発生する（いつ発生してもおかしくない）	2部分的に脆弱性未対策	2 可能性：中	4 リスク大
0	1	1	1		2016/7/1	3通常の状態で発生する（いつ発生してもおかしくない）	2部分的に脆弱性未対策	2 可能性：中	2 リスク中
1	0	0	1		2016/7/1	3通常の状態で発生する（いつ発生してもおかしくない）	2部分的に脆弱性未対策	2 可能性：中	2 リスク中
1	0	0	1		2016/7/1	2特定の状況で発生する（年に数回程度）	2部分的に脆弱性未対策	1 可能性：低	1 リスク中
2	2	2	2		2016/7/1	3通常の状態で発生する（いつ発生してもおかしくない）	2部分的に脆弱性未対策	2 可能性：中	4 リスク大
⑧ 2	2	2	2	⑨ ⑩	2016/7/1	⑪特定の状況で発生する（年に数回程度）	⑫2部分的に脆弱性未対策	⑬1 可能性：低	⑭2 リスク中

あやしいクイズ

1

サイバーセキュリティ対策について、誤りがあるものは次のうちどれですか。

- ①まずは事業推進のため社内のIT化を一気に行うことを優先し、サイバーセキュリティ対策は収益が上がってから取り組みたい。
- ②サイバー攻撃を受けた際の被害想定額が支出可能な対策費を上回ってしまったので、残留リスクを下げる対策を講じる。
- ③経営者は経営に専念し、サイバーセキュリティ対策は現場の従業員に任せておいた方がよりよい対策ができると思う。
- ④系列企業やビジネスパートナーが対策を実施しているかどうかを確認したり把握したりする必要性は全くない。
- ⑤全従業員を対象に必要な知識を習得してもらうべくセミナーを開催した。
- ⑥攻撃を受けて情報漏えいした可能性が疑われたが、明確な証拠がなかったので、特に何もしなかった。

2

IoTセキュリティガイドラインに定められているIoT機器を使用する際の基本ルールとして、正しいものは次のうちどれですか。

- ①問い合わせ窓口やサポートサービスのない機器の使用は控える。
- ②初期設定のID・パスワードはそのまま使う。
- ③使用しなくなった機器の電源プラグは抜く。
- ④パスワードは誰でも分かりやすいものにする。
- ⑤アップデートを実施する。

答え 1. ①③④⑥ 2. ①③⑤