
TOP SECRET

MISSION 3

経営者は事前に何を
備えればよいのか？





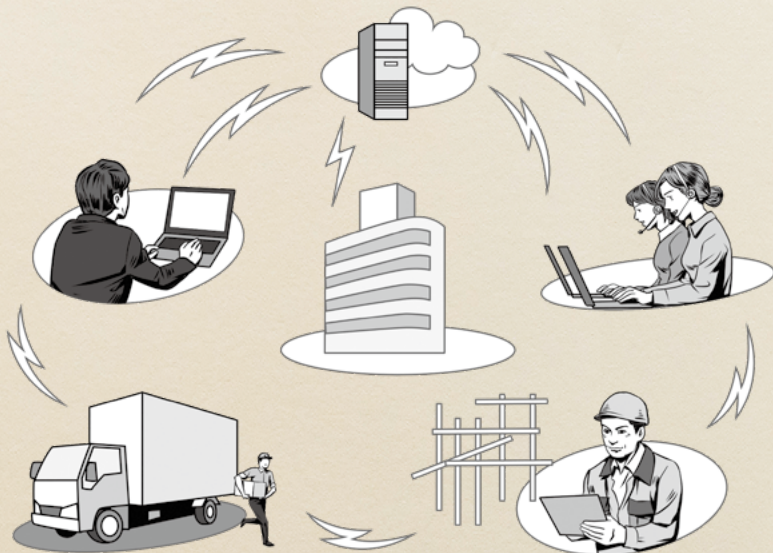
サイバーセキュリティ対策は、事業継続を脅かすリスクの1つ

サイバーセキュリティ対策が 経営に与える重大な影響



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。



POINT
2

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て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。

POINT
3

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ものです。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っ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ことも考えられます。



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



経営者などに問われる法的責任

ITを利活用する際には、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。



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。

POINT
3

海外の法律への対応も必要

サイバーセキュリティへの注目は世界中で高まっており、関連法案が世界各国・地域で施行されています。近年はWebなどで個人情報比較的容易に収集でき、海外との直接取引も容易です。事業展開の中でこうした活動を行っている場合には、諸外国の法律に抵触しないように注意が必要です。

(例)・欧州連合 (EU) : EU 一般データ保護規則

(General Data Protection Regulation : GDPR)

・中華人民共和国 : 中国サイバーセキュリティ法 (CS法)

・アメリカ合衆国 : 「NIST SP800-171」

(米国政府の調達品に関するセキュリティガイドライン)

POINT
4

サイバーセキュリティ対策の情報開示

5G、IoTやAIをはじめとしたICT利活用が社会・経済のあらゆる場面に浸透しつつある中、有効なサイバーセキュリティ対策を講じることは企業の経営課題となっています。加えて、企業の社会的責任を果たし、ステークホルダーからの信頼を得るためには、それらの情報を適切に開示することも重要な視点となっています。



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

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。

人的対策

- ・セキュリティポリシー
- ・各種社内規定、マニュアル
- ・社員の教育・訓練
- ・アクセス管理

組織的（管理的）対策

- ・管理組織の設置・運用
- ・情報資産の分類・持ち出し管理
- ・サイバー攻撃対応マニュアルの作成
- ・事業継続管理

物理的対策

- ・コンピューターや通信装置の保護
- ・重要情報の一元管理／入退室管理
- ・アクセスできる区域の制限
- ・クリアデスク／クリアスクリーン

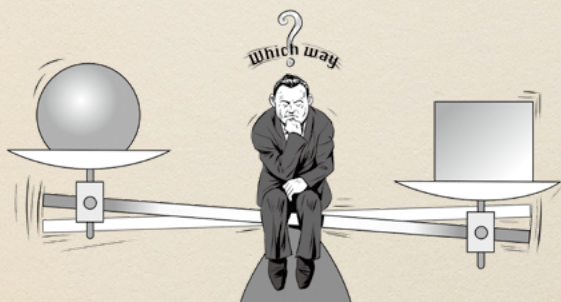
技術的対策

- ・本人認証・アクセス制御／権限管理
- ・ウイルス対策
- ・脆弱性対策
- ・暗号技術／認証技術の利用
- ・ファイアウォールやコンテンツフィルター

POINT
2

セキュリティ対策の投資効果を考える

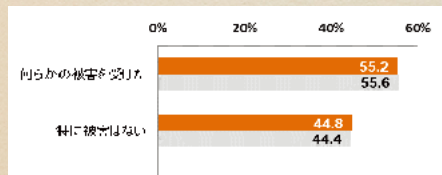
あなたの会社のインターネット接続と業務システムが1週間停止した場合のビジネスへの影響度を考えたことがありますか？ 当然その間はメールもやり取りできないため、営業機会はなくなります。また、この時代にメールも送受信できないということで取引先との信頼関係もなくなります。それらの損失を数字に置き換えたものがセキュリティ対策の投資効果です。



コラム セキュリティ対策は経営上の「投資」と位置付ける！

IDC Japanが2020年1月に実施した国内企業878社の情報セキュリティ対策の実態調査結果によると、2020年度の情報セキュリティ投資見込みについて38%の企業が2019年度を上回ると回答しています。総務省「通信利用動向調査（令和元年）」において

情報通信ネットワークの利用の際に発生した過去1年間のセキュリティ状況の被害



引用：総務省「通信利用動向調査（令和元年）」より

ても55.2%の企業が「何らかの被害を受けた」と回答。対策には相応のコストが必要なものの、近年は中小企業を含むサプライチェーンを狙った攻撃も増えています。こうした観点も鑑み、やむを得ない「経費」でなく、ITを利活用した積極的な経営への「投資」と位置付けることが重要です。



自社のIT活用・セキュリティ対策状況を自己診断する

ITの活用診断



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、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

中小企業基盤整備機構：IT経営簡易診断
情報処理推進機構：DX推進指標



IT活用診断のカギは費用対効果

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（参考「ITガバナンス」P99参照）。

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



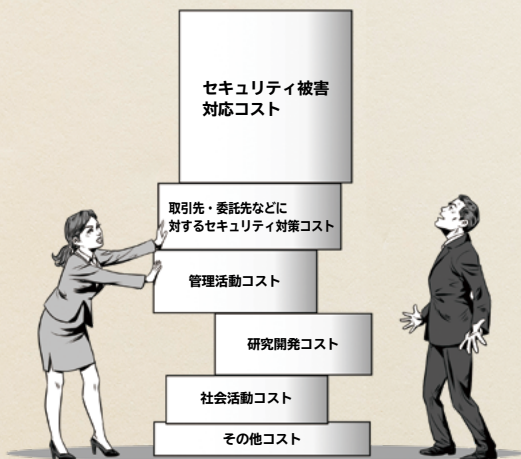
自社のIT活用・セキュリティ対策状況を自己診断する

サイバーセキュリティ 投資診断



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、P94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。

コラム 「ITガバナンス」と6つの原則

IT活用は今や企業戦略の中で不可欠となっています。この観点から経営層には組織価値を高め、ITシステム戦略の策定や運用に必要となる組織能力である「ITガバナンス」が求められています。その成功には、経営層が次の6原則を実践することが肝要とされています。以下、要約して紹介します。

1. **責任**：役割に責任を負う人は、その遂行権限を持つ
2. **戦略**：情報システム戦略は現在と将来を考慮して、そのニーズを満たす必要がある
3. **取得**：情報システムの導入は短期・長期の両面で効果・リスク・資源のバランスを考慮した意思決定に基づく必要がある
4. **パフォーマンス**：情報システムは現在および将来のニーズを満たす必要がある
5. **適合**：情報システムは関連する全ての法律および規制に適合する必要がある
6. **人間行動**：情報システムのパフォーマンス維持に関わる人間行動を尊重する必要がある

参考：経済産業省「システム管理基準」

https://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kanri_h30.pdf



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



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。



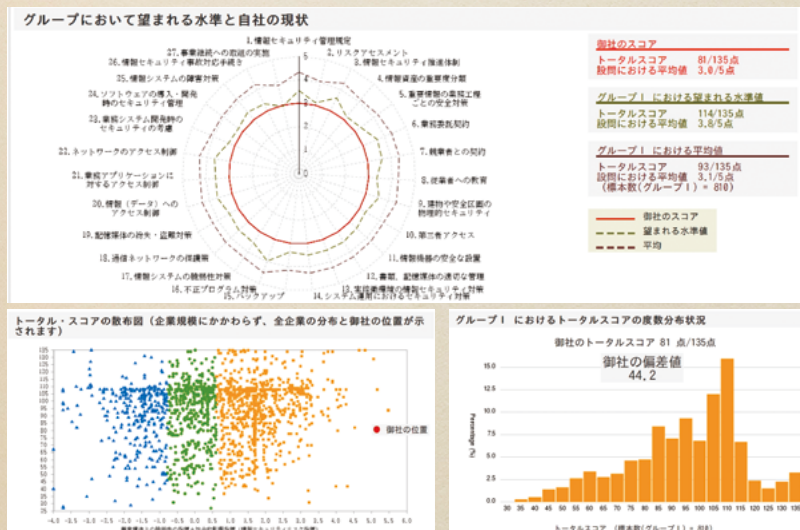
POINT
2

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わからない
 - ・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
- こうした要望に応じて、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。



「情報セキュリティ対策ベンチマーク」(IPA) より転載（一部加工）



ビジネスを継続するためには(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



守りのIT投資と攻めのIT投資

守りのIT投資という言葉を知っていますか。

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

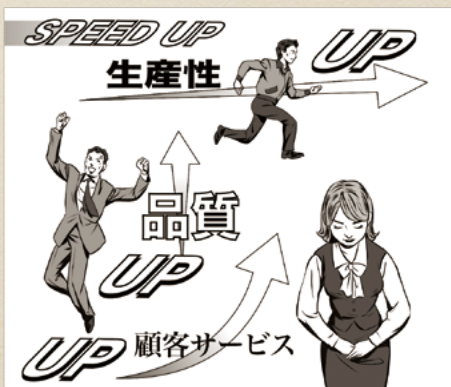
経営者のみなさんが重視している経営課題の1つは、業務効率化やコスト削減です。

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は(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。

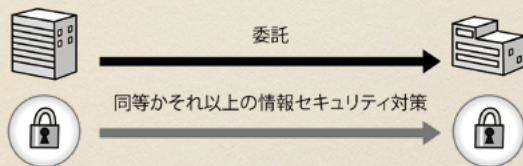


原則2

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は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しても、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は(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ない

サイバーセキュリティ経営の重要10項目

経済産業省と情報処理推進機構 (IPA) がまとめた「サイバーセキュリティ経営ガイドライン Ver 2.0」を基に、経営者が情報セキュリティ全般を統括する「最高情報セキュリティ責任者 (CISO)」に指示すべき重要10項目をまとめました。

重要10項目とは

経営者がリーダーシップをとったセキュリティ対策の推進

サイバーセキュリティリスクの管理体制構築	1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
	2	サイバーセキュリティリスク管理体制の構築
	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の特定と対策の実装	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
	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
	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
インシデント発生に備えた体制構築	7	インシデント発生時の緊急対応体制の整備
	8	インシデントによる被害に備えた復旧体制の整備
サプライチェーンセキュリティ対策の推進	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
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	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

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POINT
1

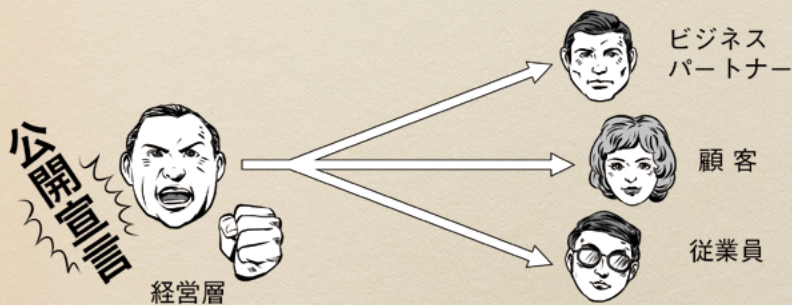
指示すべきことはこれだ

- サイバーセキュリティリスクを経営リスクの1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

POINT
2

やるべきことはこれだ

- 組織全体の対応方針を組織の内外に宣言できるよう、セキュリティポリシーを策定
- セキュリティポリシーを従業員へ周知徹底
- セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示す



サイバーセキュリティリスク管理体制の構築

POINT 1

指示すべきことはこれだ

- ・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

POINT 2

やるべきことはこれだ

- ・CISOは、責任範囲を明確にしたサイバーセキュリティリスク管理体制を構築
- ・取締役、監査役はサイバーセキュリティリスク管理体制を監査
- ・セキュリティ・バイ・デザインの観点を踏まえて体制を構築
- ・経営者のリーダーシップの下で体制を構築



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

POINT
1

指示すべきことはこれだ

- ・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

POINT
2

やるべきことはこれだ

- ・サイバーセキュリティ対策に必要な費用の確保
- ・セキュリティ対策に必要な人材の確保
- ・セキュリティ人材育成、キャリアパスを設計検討
- ・外部の組織が提供するセキュリティ研修等の活用を検討
- ・各部門においてもセキュリティを意識した業務遂行ができるようにする



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

POINT 1

指示すべきことはこれだ

- ・ 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策定させる
- ・ 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

POINT 2

やるべきことはこれだ

- ・ 経営戦略の観点から守るべき情報を特定し把握
- ・ 守るべき情報に対して、発生しうるサイバーセキュリティリスクを把握
- ・ 把握したリスクに対して、実施するサイバーセキュリティ対策を検討（リスクの低減策、回避策、移転策）
- ・ 実施できない場合は、残留リスクとしての識別も
- ・ 法令上の取り扱いも考慮したリスクの特定と緊急時の情報の保護が行えるような対策も検討
- ・ 製品・サービス等においても、セキュリティ・バイ・デザインの観点を踏まえて、対策を考慮



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POINT
1

指示すべきことはこれだ

- 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

POINT
2

やるべきことはこれだ

- 重要業務を行う端末、ネットワーク、システムまたはサービス（クラウドサービスを含む）には、多層防御を実施
- アクセスログや通信ログ等からサイバー攻撃を監視・検知する仕組みを構築
- 従業員に対する教育を行い、適切な対応が行えるよう日頃から備える
- 製品・サービス等においても、セキュリティバイデザインの観点を踏まえて、企画・設計段階からサイバーセキュリティ対策を考慮



サイバーセキュリティ対策におけるPDCAサイクルの実施

POINT 1

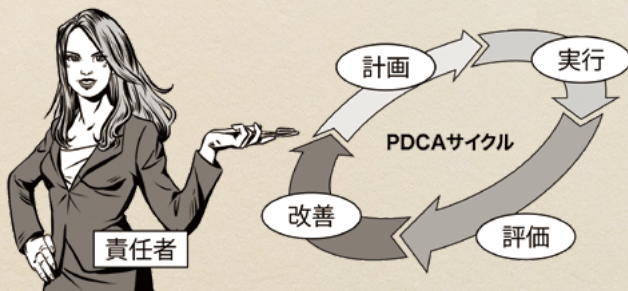
指示すべきことはこれだ

- ・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

POINT 2

やるべきことはこれだ

- ・サイバーセキュリティリスクに継続して対応可能な体制（プロセス）を整備する（PDCAの実施体制の整備）
- ・サイバーセキュリティリスク管理に関するKPIを定め、組織内の経営リスクに関する委員会においてその状況を経営者に報告する
- ・新たなサイバーセキュリティリスクの発見等により、追加的に対応が必要な場合には、速やかに対処方針を修正する
- ・サイバーセキュリティ対策の状況について、情報セキュリティ報告書、CSR報告書等への記載を通じて開示を検討する



指示7

インシデント発生時の
緊急対応体制の整備POINT
1

指示すべきことはこれだ

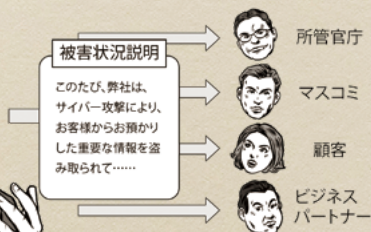
- ・ 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT等）を整備させる
- ・ 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明できる体制を整備させる

POINT
2

やるべきことはこれだ

- ・ 緊急時において、以下を実施できるような対応体制を構築する
- ・ サイバー攻撃による被害を受けた場合、速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築する
- ・ インシデント収束後の再発防止策の策定、所管省庁等への報告手順も含めて演習を行う
- ・ 緊急連絡網として社外を含む情報開示の通知先一覧を整備し、対応に従事するメンバーに共有しておく
- ・ 緊急時に組織内各部署が速やかに協力できるよう予め取り決めをしておく
- ・ 関係法令を確認し、法的義務が履行されるよう手続きを確認しておく

インシデントに関する被害状況、他社への影響等について経営者に報告する



インシデントによる被害に備えた復旧体制の整備

POINT 1

指示すべきことはこれだ

- ・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、復旧対応体制の整備をさせる
- ・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
- ・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

POINT 2

やるべきことはこれだ

- ・業務停止等に至った場合に、以下を実施できるような復旧体制を構築する
- ・サイバー攻撃により業務停止に至った場合、関係機関との連携や復旧作業を実施できるよう指示する。また、対応担当者には復旧手順に従った演習を実施させる
- ・演習内容や組織の関係者の役割を踏まえて検討することが望ましい
- ・重要な業務をいつまでに復旧すべきかの目標について、組織全体として整合をとる（例えばBCPで定めている目標との整合等）



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

POINT 1

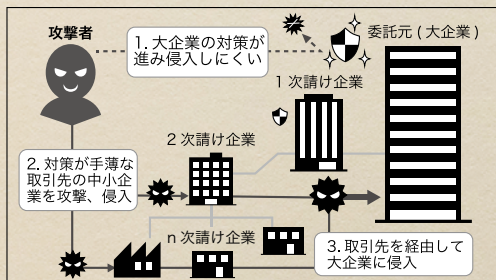
指示すべきことはこれだ

- ・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委託先等を含めた運用をさせる
- ・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

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のビジネスパートナーやシステム管理の委託先等のサイバーセキュリティ対策の内容を明確にした上で契約を交わす
- ・個人情報や技術情報等の重要な情報を委託先に預ける場合は、情報の安全性の確保が可能であるかどうかを定期的に確認する
- ・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委託先等がSECURITY_ACTIONを実施していることを確認する
- ・緊急時に備え、委託先がサイバー保険に加入していることが望ましい



出典：日経コンピュータ 2018年9月27日号より、一部を
改変して作成

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

POINT 1

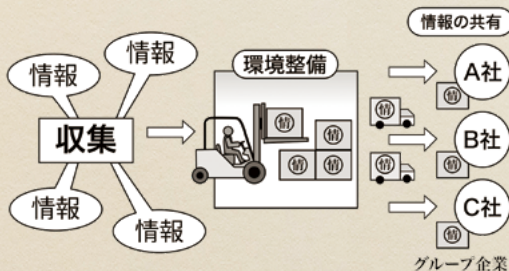
指示すべきことはこれだ

- ・ 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、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行わせる
- ・ 入手した情報を有効活用するための環境整備をさせる

POINT 2

やるべきことはこれだ

- ・ 情報共有を通じたサイバー攻撃の防御につなげていくため、情報を入手するのみならず、積極的に情報を提供する
- ・ IPAやJPCERT/CC等による脆弱性情報などの注意喚起情報を、自社のサイバーセキュリティ対策に生かす
- ・ CSIRT間における情報共有や、日本シーサート協議会等のコミュニティ活動への参加による情報収集
- ・ IPAに対し、告示（コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準）に基づいてウイルス情報や不正アクセス情報の届出をする
- ・ JPCERT/CCにインシデントに関する情報提供を行い、必要に応じて調整を依頼する



◆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/CC)	<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
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おわびするとともに、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



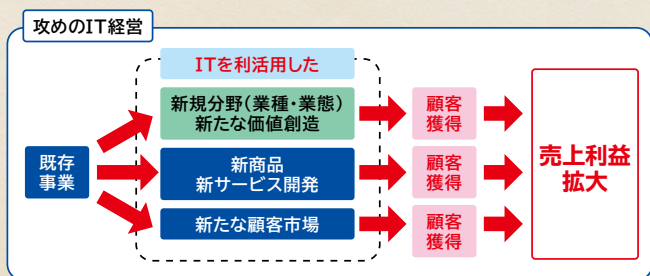
ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

次世代技術を活用した ビジネス展開



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。柔軟かつ大企業に先駆けてIT関連の次世代技術や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ります。デジタル情報やIT技術の進展を受け入れ、それを活用して顧客サービスの強化を図る企業に今大きなビジネスチャンスが訪れています。



「攻めのIT経営中小企業百選」(経済産業省)より



各種の支援策も充実

感染症対策や働き方改革の必要性が高まる中、テレワーク等の実現のためにデジタルツールに関心があっても、導入・定着に至らない中小企業に向けた支援も充実しています。その1つが「中小企業デジタル化応援隊事業」(2020年9月開始)。全国の中小企業とIT専門家をマッチングし、デジタル化・IT化を促進しています。

コラム DX推進はビジネス飛躍のチャンス

これから目指す社会は、「超スマート社会」いわゆる「Society5.0」

政府は、サイバー空間（仮想空間）とフィジカル空間（現実空間）を連携し、すべての物、情報、人を1つにつなぐ「サイバー・フィジカル・システム」（CPS）によって量と質の全体最適を図る社会像として「Society5.0」を提唱し、その考えが「デジタル社会の実現に向けた改革の基本方針」（2020年12月閣議決定）の背景となっています。IoTやビッグデータ、ロボット、AI、5Gなどの技術革新（いわゆる第4次産業革命）により、Society5.0は現実になりつつあります。

DXは、新たな技術を活用したビジネスの変革

新しいITおよびデジタル情報を活用して、ビジネスを変革させるのが「デジタルトランスフォーメーション（DX）」です。DXにより新時代に対応した新たなサービスを創造し、ビジネスを飛躍させることができます。

DX推進のためには、セキュリティも強化

一方、どんなに良いサービスを展開しても、セキュリティ侵害があつては事業が継続できません。ITシステム運用継続計画（IT-BCP）を明確にして、サービス設計の段階から十分なセキュリティ対策を考慮することが重要です。

中小企業のビジネスの拡大・発展に向けて

そのためには、ビジネス、デジタルのスキルとともに、セキュリティ対策のスキルを併せ持った人材が必要です。DXに対応した新たなビジネスの拡大・発展のためには、経営者は、業務や組織、企業風土の変革を含めて、明確なビジョンを持ち、「攻めのIT投資」を牽引する強いリーダーシップが求められます。



引用：内閣府「Society5.0」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)

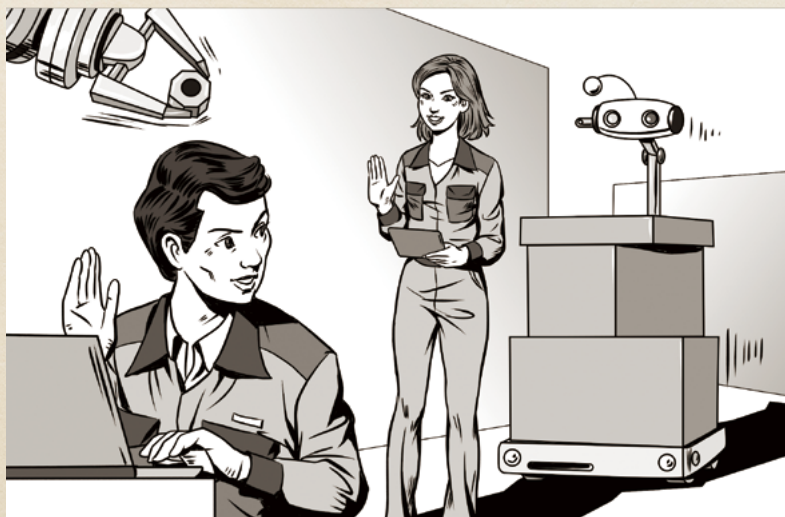
IoT、ビッグデータ、 AI、ロボットの活用



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、効果的に行うことが始まっています。IoT (Internet of Things/モノのインターネット)*、ビッグデータ*、AI (Artificial Intelligence/人工知能)*、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P122を、AIはP124を参照

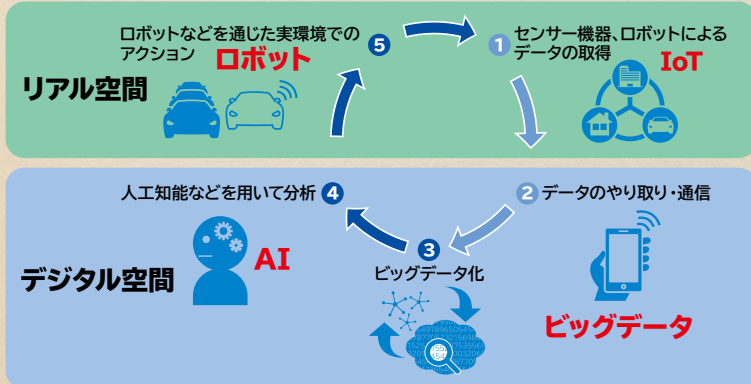


コラム IoT、ビッグデータ、AI、 ロボットはつながっている

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



出典：「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

「5G」に代表される次世代通信技術などによってIoTデバイスは急速に普及し、2024年には10兆円を超える国内市場となる予測もあります。さらに政府が目指す「Society5.0」実現に向けた動きも追い風となり、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は、例えば医療・介護、物流、製造業、交通、農業などさまざまな分野での活用が期待でき、大きなビジネスチャンスになるのです。



コラム 中堅・中小企業のIoT活用事例

製造業（東京都墨田区）社員数：50名
各種装置・機械の設計開発等

3DCADをクラウド環境で離れたところから利用可能に

事例ポイント

専門ソフトウェアの導入によって一般的なノートPCで、社内のハイスペックPCを高性能のままにリモート操作可能とした。客先や工場内など遠隔地のどこからでも社内の3DCADソフトをシームレスに利用して設計データの確認や修正が実現できる環境を構築した。

概要

- ・当該企業は板金加工を中心とした金属加工による部品製造や機械装置設計開発業務に従事。設計開発では3DCAD等のソフトウェアを利用。一般的なオフィスソフトを動作させるPCスペックでは足りずハイスペックな環境が必要であり、場所も設計者の机に限定されている
- ・設計に関して客先での打ち合わせや工場内確認を行う場合、3DCADのデータ参照が必要であり、設計者の机以外の場所で利用することができない。3DCADデータをプリントアウトした紙媒体を多く用いていた。修正や改編の度に紙とCADを行き来しなければならず膨大な手間が発生していた。修正ミスが起こる可能性も高い状況にあった

効果・メリット

客先や工場内など遠隔地のどこからでも社内の3DCADソフトを利用して設計データの確認や修正を迅速に反映。情報セキュリティ面から見ても、データそのものや紙媒体を持ち運ぶ必要がなくなり、情報漏えいのリスクを最小限に抑えた形で外部での設計対応が可能に。

「中堅・中小製造業のIoT活用事例一覧」（ロボット革命・産業IoTイニシアティブ協議会）より抜粋・要約して作成



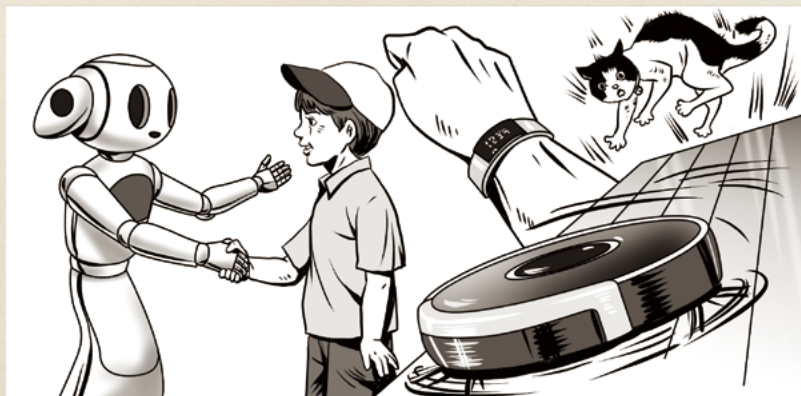
ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

人工知能(AI)が果たす 役割と効果

POINT
1

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)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。例えば、大手調査機関では、日本においては2035年にAIによる労働生産性がベースラインで34%向上するという分析も行われています。



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。

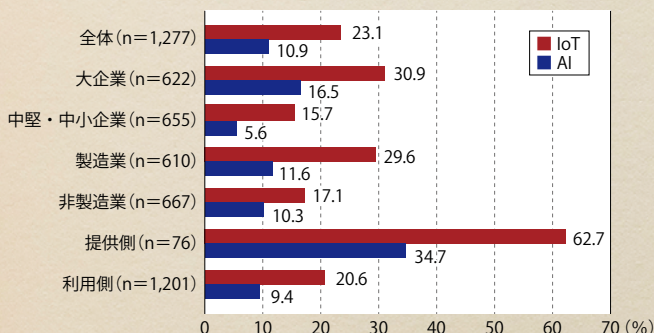
- ・既存業務の人材不足の解消
- ・不足している労働力の補完・省力化
- ・既存の業務効率・生産性の向上（省力化）
- ・新しい価値を持った業務の創出

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

国内のAIとIoT活用状況



出典：財務省「最先端技術（IoT、AI等）の活用状況」（平成30年11月）を参考に作成



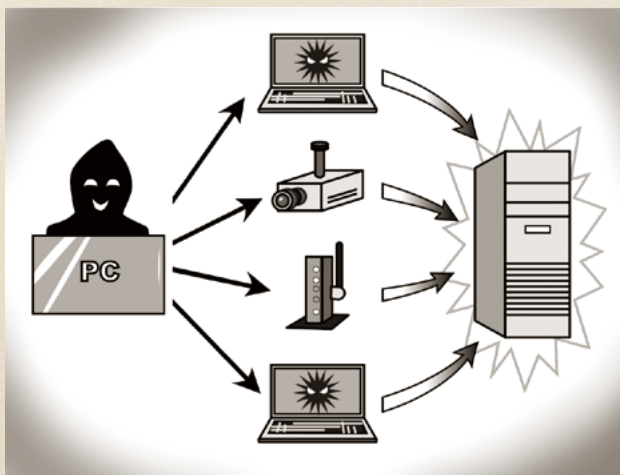
ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

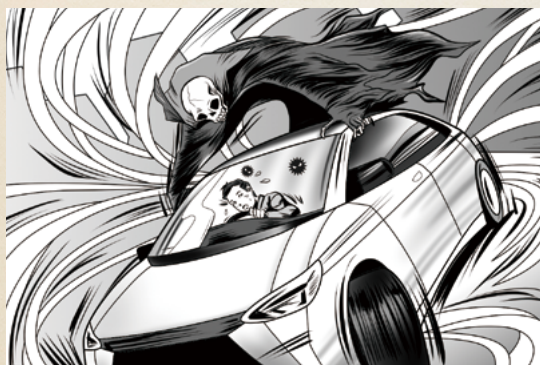
IoTを活用する際のサイバーセキュリティ上の留意点



IoTへの脅威

次世代通信技術である5Gの進歩などを背景に、これから飛躍的に活用場面の増加が予想される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。また、5Gが社会浸透していく中では、これまで以上にさまざまなリスクが生まれ、脅威の在り方もさらに多様化・複雑化することが予想されます。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P128参照)





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の（攻めのIT投資とサイバーセキュリティ対策）

IoTを活用するための 基本ルール

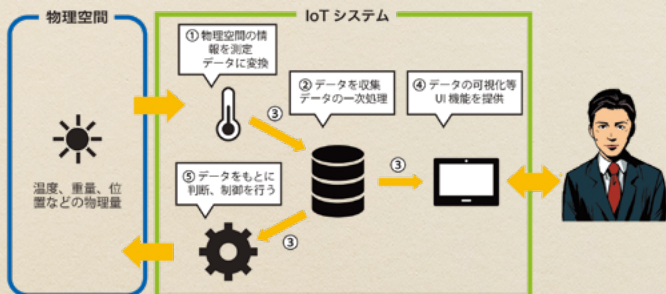
POINT
1

IoTのセキュリティは製造サービス提供側とサービス利用者側の双方の意識が大切

製造業を中心にIoTを利活用する動きが加速しています。

IoT機器はインターネットに接続しているネットワーク機器の一種。そのためパソコンと同様にサイバー攻撃のリスクがありますが、セキュリティ面がなござりにされているものもあります。それらを利用するとサイバー攻撃によってシステムが使えなくなる、あるいは第三者への攻撃の踏み台となるかもしれません。

IoTのセキュリティは、製造サービス提供側とサービス利用者側の双方が注意を払わなくてはならないのです。



出典：JPCERT/CC「IoTセキュリティチェックリスト利用説明書」（2019年6月）より作成

POINT
2

IoT機器やシステム、サービスの提供にあたっての指針

■ 指針1 IoTの性質を考慮した基本方針を定める

IoT機器が原因で情報流出や社会インフラの停止などが起こった場合は、IoT機器やシステム、サービスの提供側の経営責任が問われることもあります。リスクを認識し、内部不正やミスに備えることが必要です。

■ 指針2 IoTのリスクを認識する

他の機器とつながることで、影響が広範囲になるリスクを想定することが大切です。不正操作や、廃棄機器からの情報漏えいリスクも考慮します。

■ 指針3 守るべきものを守る設計を考える

つながる相手や状況に応じてつなぎ方を判断できる設計を検討しましょう。安全安心を実現するために設計が妥当かどうかの評価も必要です。

■ 指針4 ネットワーク上での対策を考える

セキュアなゲートウェイを利用するなど、ネットワーク構成やセキュリティ機能の検討を行いましょう。初期設定もセキュリティに留意し、利用者にも注意喚起を行います。

■ 指針5 安全安心な状態を維持し、情報発信・共有を行う

出荷・リリース後も安全安心な状態を維持できるようソフトウェアをアップデートする手段を確保します。脆弱性について情報発信し、セキュリティに関する重要事項はユーザーへあらかじめ説明しましょう。

参考：IoT推進コンソーシアム「IoTセキュリティガイドラインver1.0」（平成28年7月）より



IoT機器の一般利用者のためのルール

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。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」「不要なサービスや機能は有効化しない」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、不正利用されるおそれがあります。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。

参考：「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

POINT
4

Society5.0とIoT

Society5.0が目指す社会では、IoTによってPCやスマートフォンだけでなく家電製品や車、建物などあらゆるモノがサイバー（仮想）空間とフィジカル（現実）空間で融合されます。このため、IoT機器へのサイバー攻撃が成功すると、フィジカル空間にも影響を与える可能性が高まります。

例えば、IoT製品などに感染するウイルス「Mirai」によりWebサイトが大規模なサイバー攻撃を受けました。さらに重要インフラや生産設備への攻撃による大規模な被害も発生しています。

IoT製品をはじめ、インターネット接続される多様な機器に適切なセキュリティ対策が行われず、インターネット上に晒されアクセス可能な状態にある製品を監視し被害を防止するために、「NOTICE（National Operation Towards IoT Clean Environment）」が行われています（P47参照）。これはサイバー攻撃に悪用されるおそれのあるIoT機器の調査および当該機器の利用者への注意喚起を行うもので、総務省、国立研究開発法人情報通信研究機構（NICT）および一般社団法人ICT-ISACが主体となって実施されています。



出典：内閣府「IoT社会に対応したサイバー・フィジカル・セキュリティ『サイバー・フィジカル・セキュリティ対策基盤』の研究開発」より作成

MEMO