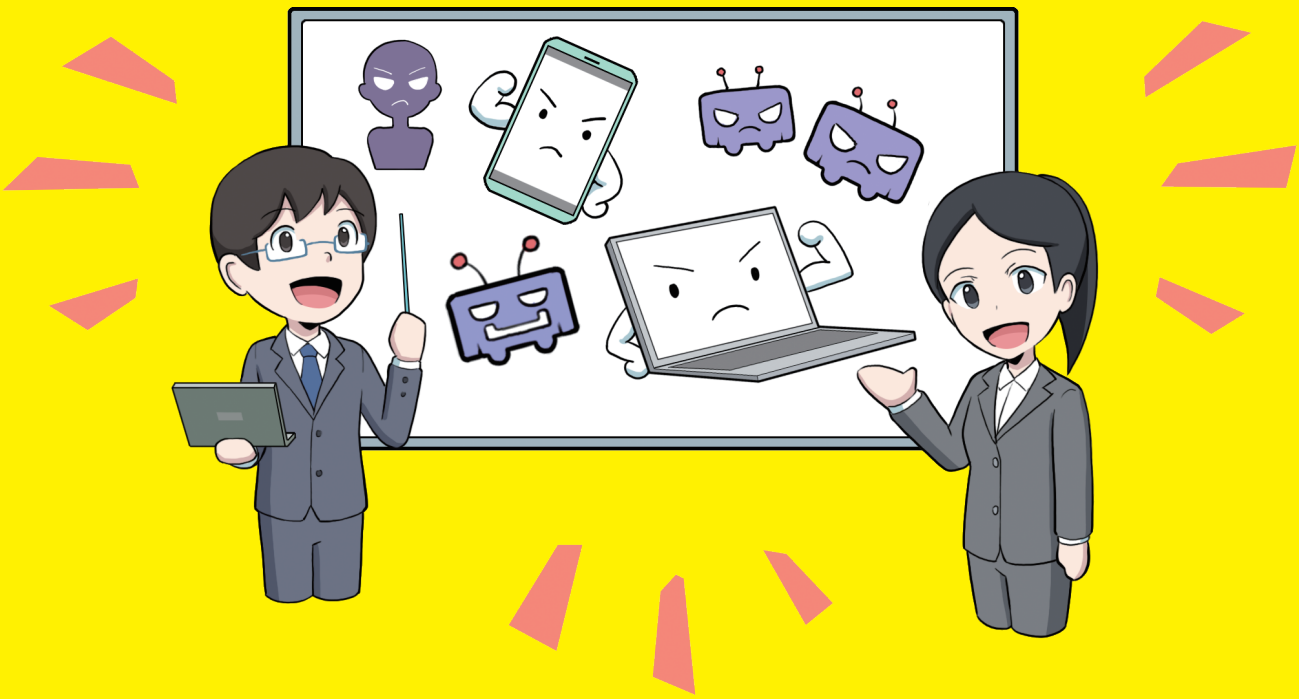
インターネットの

安全・安心ハンドブック

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

リーフレット（中小企業等向け）



知る・守る・続ける

サイバーセキュリティ普及啓発

Ver 5.10

はじめに

本リーフレットの目的

NISCは、国のサイバーセキュリティ施策の推進を行っています。政府の対策を話し合う「サイバーセキュリティ戦略本部」の事務局を担っています。また、各機関へ助言や情報提供を行っています。

近年、中小企業等ではITの利活用が進む一方で、サイバー攻撃手法の巧妙化、悪質化などにより事業に悪影響を及ぼすリスクが高まってきています。サイバー攻撃などによりシステムがダウンしたり、情報流出が発生した場合は、事業活動の停止、取引先からの信頼低下等、甚大な損害が発生することがあります。

そこで、NISCではサイバーセキュリティの基本を学び、企業を守るための対策を理解できるよう、本リーフレットを作成しました。本リーフレットの知識を活用し、サイバー攻撃に対応するための体制を整備しましょう。

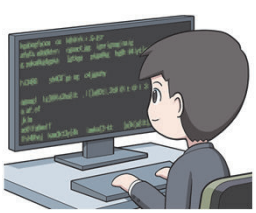
各ページに「インターネット安全・安心ハンドブックVer5.10」における記載箇所や、各省庁・各機関の参考となる取組を載せています。ぜひ確認し、より理解を深めてください。

本リーフレットの対象者

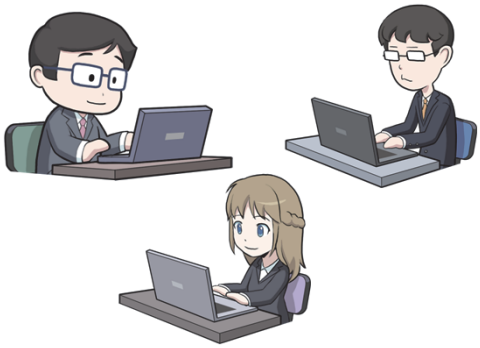
中小企業・小規模事業者　等

経営層、情報管理者、従業員　　等

経営層



情報管理者



従業員

社内の体制等の整備

まずは社内の現状を知り、必要な制度、体制の整備、従業員に学習の機会の提供や訓練を行いましょう。

1 自社の情報資産の状況を確認

- 自社の情報資産を把握し、それぞれの資産の重要度やリスクに応じたセキュリティ対策を講じましょう。

2 必要な体制や規程等の文書の整備

- サイバーセキュリティ対策は、まずは費用の確保と体制整備から行いましょう。
- 方針策定とルール整備を行うことで、社員に対して情報セキュリティに取り組む動機づけと推進を行いましょう。
- セキュリティ事故発生時に別の災害が起きても対応できるように、自社で可能な対応を明確にしておきましょう。

3 従業員に必要な学習の機会の提供と訓練

- 全社員に学習の機会の提供および訓練を実施し、最新のサイバー攻撃手口を共有して攻撃が来ることに備えましょう。
- 第三者認証・認定取得は難易度が高いですが、企業の信頼性向上と社員教育につながる貴重な機会となります。

4 万が一の時の対応の整理と訓練

- サイバー攻撃や災害から事業を守るため、BCPを策定し、訓練をしましょう。

社内の体制等の整備

1 自社の情報資産の状況を確認

自社のビジネスにおける損失や信頼の失墜等のリスクや、情報流出による法的責任に直面するリスクを避けるために、自社の情報資産の状況を確認しましょう。

□	自社の情報資産を把握することで、それぞれの資産の重要度やリスクに応じたセキュリティ対策を講じましょう。

No.	項目	確認事項	チェック
1	情報資産の把握	どのような情報（顧客情報、技術情報等）を保有しているか把握していますか？	□
2		重要な情報がどこに保存されているか（サーバ、PC、ネットワーク機器等）を台帳管理していますか？	□
3		新しい機器やソフトウェアの導入、廃棄時に管理台帳を更新していますか？	□
4	ハードウェア管理	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定していますか？	□
5		退職者や使用していないアカウント等、不要なアカウントを削除していますか？	□
6		ハードウェアの保守・サポート情報を確認できますか？	□
7	ソフトウェア管理	OSやアプリケーションの名称とバージョンを把握していますか？	□
8		インストールされているソフトウェアのライセンス形態を把握していますか？	□
9		バックグラウンドで動作しているソフトウェアおよびサービスは業務上必要なものだけにしていますか？	□
10	運用管理	情報資産管理のためのリソース（人材、費用）の割当を行っていますか？	□
11		定期的に情報資産管理の方法の見直しを行っていますか？	□
12		インシデント発生時に事業を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を把握していますか？	□

- **☑が6個以下** ：情報資産管理が不十分です。早急に現状把握と対策を実施する必要があります。
- **☑が7～9個** ：部分的に実施できていますが、不足している項目があります。早急に対策を検討しましょう。
- **☑が10個以上**：基本的な情報資産管理は実施できています。さらなる詳細化を検討しましょう。

ハンドブック記載箇所
付録04 IPAが取り組むさまざまな中小企業向けセキュリティ対策支援

参考資料

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/guide/sme/about.html

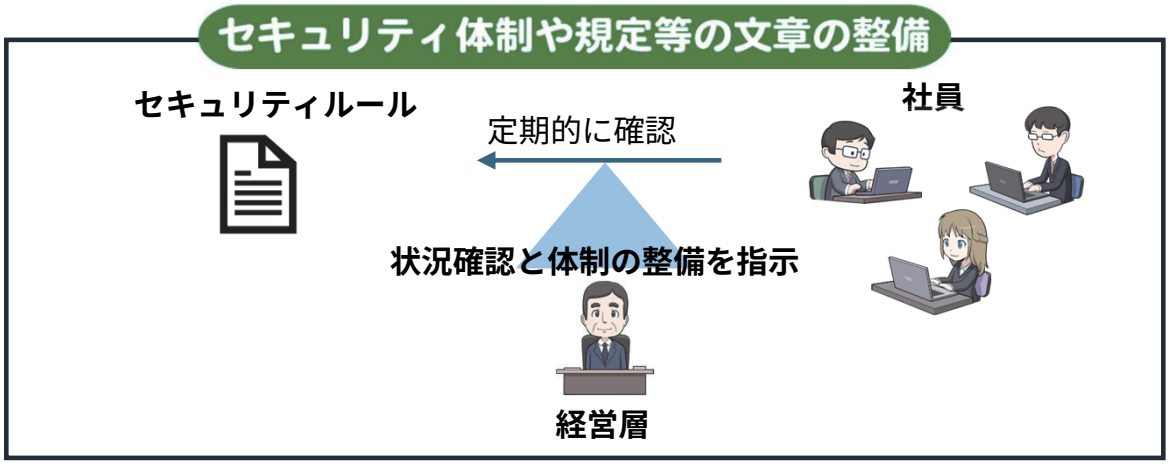
2

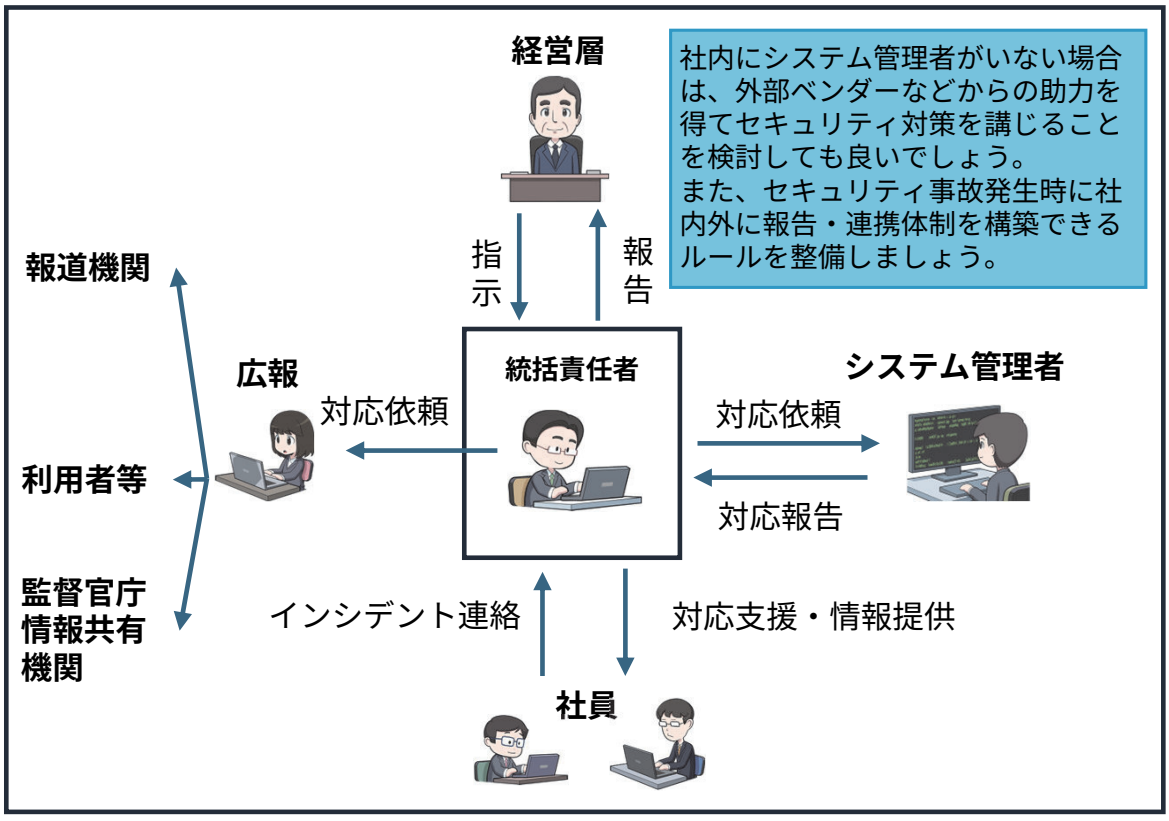
社内の体制等の整備

必要な体制や規程等の文書の整備

セキュリティ事故発生時に被害の拡大を防ぐために、迅速に対応ができるセキュリティ対策の体制や規程等の文書の整備を行いましょう。

□	経営層は、セキュリティ対策の費用の確保と体制整備の指示を行い、社員はセキュリティルールの定期的な確認を行いましょう。
□	セキュリティ体制に基づいて、対策方針を具体的に実施するためのセキュリティのルールを整備しましょう。
□	セキュリティ事故発生時に重要なデータへのアクセス権限が一人に集中しないよう、権限の分散を図り、不可能な範囲は外部の助力を得るなどして複数人が対応できる体制を構築しましょう。





ハンドブック記載箇所
第６章２　災害時やサイバー攻撃時に会社を守るために事業継続計画(BCP)を作ろう

参考資料
経済産業省　サイバーセキュリティ経営ガイドライン
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

3

社内の体制等の整備

従業員に必要な学習の機会の提供と訓練

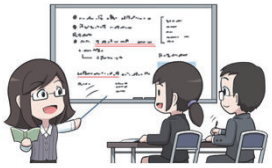
従業員に学習の機会の提供や訓練を行い、社内のセキュリティ意識を高め、サイバー攻撃やインシデントに対応できるようにしましょう。

□	セキュリティ対策に関する基本的な学習の機会を提供し、セキュリティに対する意識を高めましょう。
□	セキュリティ対応に関する最近のサイバー攻撃に関する手口を共有し、セキュリティに対する意識を高めましょう。
□	第三者認証・認定は、対外的にも企業の信頼性を向上させるほか、従業員のサイバーセキュリティ対策能力の向上につながる貴重な機会にもなります。

セキュリティ対策に関する学習の機会の提供例

eラーニング

業務に携わるすべての人にセキュリティ対策の重要性やサイバー攻撃の脅威とリスクを周知しましょう。



集合研修

情報セキュリティインシデントに直面した際の対処方法を、演習・ワークショップ形式で提供しましょう。

標的型メール訓練

実際に不審なメールにどのように対処するのか、現場の対応力・実行力を確認しましょう。

第三者認証・認定の例

ISO/IEC 27001（情報セキュリティマネジメントシステム）

Pマーク

AICPA SOC1/SOC2

ハンドブック記載箇所
第６章７　企業が気を付けたいサイバー攻撃の具体例を知ろう

参考資料

IPA　講習能力養成セミナー
https://www.ipa.go.jp/security/seminar/sme/seminar.html

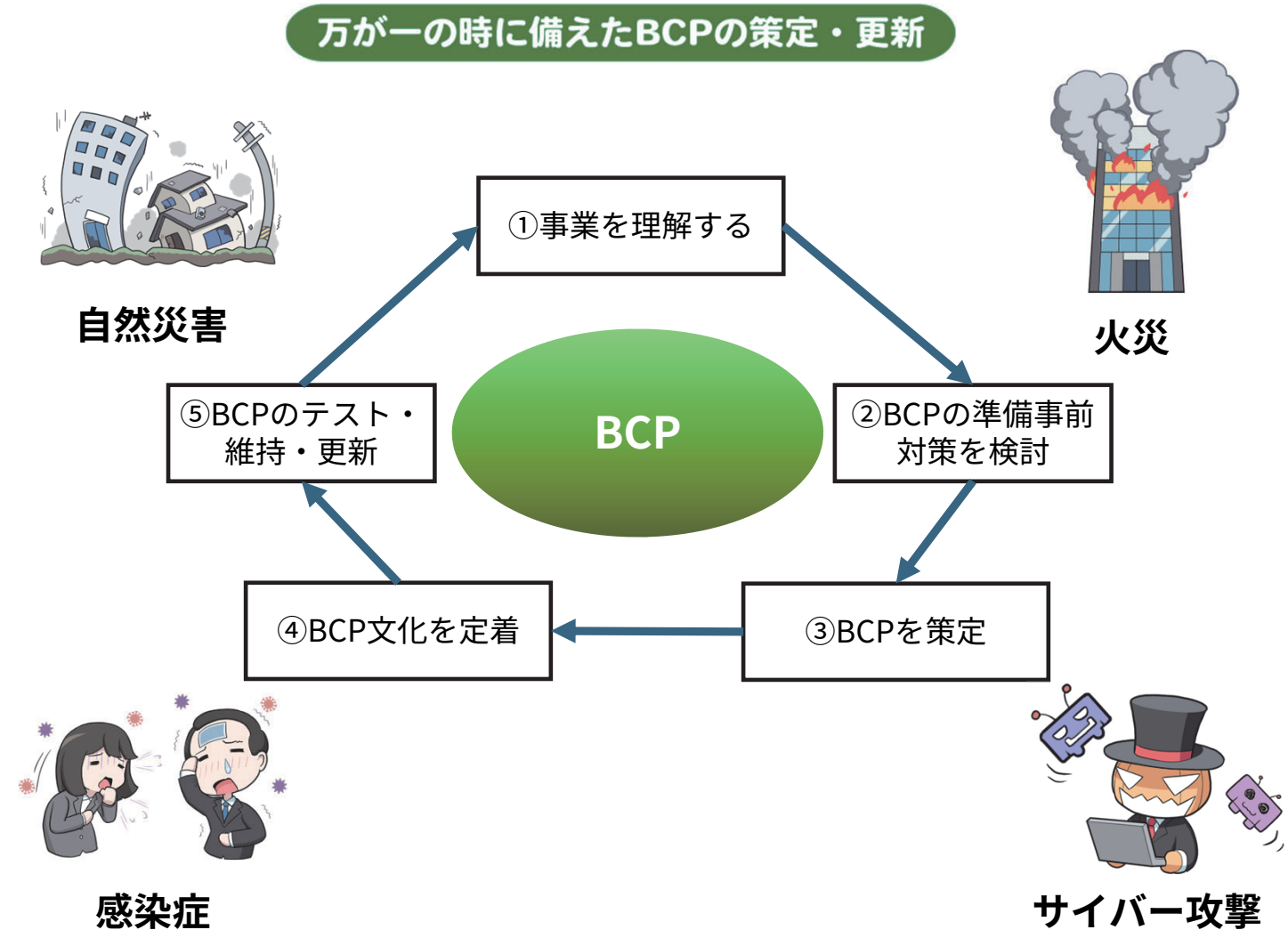
4

社内の体制等の整備

万が一の時の対応の整理と訓練

サイバー攻撃や災害等から事業を守るため、対応方法の整理と訓練をしましょう。

□	サイバー攻撃や災害時にどのように事業継続を行うか、人・モノ・金等の面から事業継続計画(BCP) を考えておきましょう。
□	サイバー攻撃や災害時に、連絡・報告先等を確認するほか、日常的に情報収集できる体制づくりも行いましょう。
□	トラブルに対処する手順書は、物理的な災害による被害（建物や機材の棄損）やサイバー攻撃による被害への対処だけでなく、感染症等人的な損害への対処手順も定めましょう。



ハンドブック記載箇所
第１章8.2　ランサムウェアや天災にも対応できるバックアップ体制
第６章２　災害時やサイバー攻撃時に会社を守るために事業継続計画(BCP)を作ろう

参考資料
中小企業庁　中小企業BCP策定運用指針ウェブサイト
https://www.chusho.meti.go.jp/bcp/index.html

IT機器やネットワークの安全な利用

サイバーセキュリティ上、危うい状況に陥らないために、攻撃者の実態や手口を知るとともに、自社のセキュリティ環境が脅威に対応ができているかを確認し、必要に応じて追加で対処することが重要です。

1 サイバー攻撃の実態や手口を知ろう

- 巧妙化するサイバー攻撃の手口を知り、セキュリティ対策を講じましょう。
- 特に標的型攻撃、脆弱性を突いた攻撃等の脅威に対し、システムの対応と関係者への周知を徹底しましょう。

2 利用する機器を最新の状態にする

- IT機器の脆弱性を突く攻撃に注意しましょう。
- OS・ソフトウェアを常に最新にアップデートし、ウイルス対策ソフトで安全を確認しましょう。

3 ネットワークを安全な状態で使う

- 情報資産を守るため、ネットワークセキュリティを強化しましょう。
- IT機器のセキュリティ対策、VPNの活用、通信の暗号化等で情報漏えいを防ぎましょう。

4 データを漏らさない対策

- なりすまし対策で情報漏えいを防ぎましょう。
- 強力なパスワード設定や多要素認証の活用等で、不正アクセスを阻止しましょう。
- 内部不正対策として、アクセス権限の適切な設定、USB等の機器接続管理、大容量媒体管理等を徹底し、情報資産を守りましょう。

1

IT機器やネットワークの安全な利用

サイバー攻撃の実態や手口を知ろう

サイバー攻撃の実態や手口を知ることで、インシデント発生時の対応を整理しましょう。

□	巧妙化・高度化するサイバー攻撃について、どのような形で狙われるのか、最新の手口や実態を把握しましょう。
□	サイバー攻撃を想定したシステムの対応や関係者への周知を行いましょう。
□	ネットワーク機器等の脆弱性を狙ったランサムウェア攻撃、標的型攻撃によってマルウェアに感染させる手法、フィッシング詐欺による情報漏えい等には注意しましょう。

ランサムウェア攻撃

ファイルを暗号化し、復号と引き換えに身代金を要求するサイバー攻撃。

標的型攻撃

特定の企業や組織をターゲットにし、メールやWebサイトからウイルス・マルウェアを感染させる。

フィッシング詐欺

偽のメールやウェブサイトを使って、本物そっくりになりすまし個人情報やクレジットカード情報等の重要な情報を盗み取る。

DDoS攻撃

複数のコンピュータを利用してサーバに負荷のかかる攻撃を行う。

ハンドブック記載箇所
第６章７　企業が気を付けたいサイバー攻撃の具体例を知ろう

参考資料

IPA　情報セキュリティ10大脅威 2025
https://www.ipa.go.jp/security/10threats/10threats2025.html

2

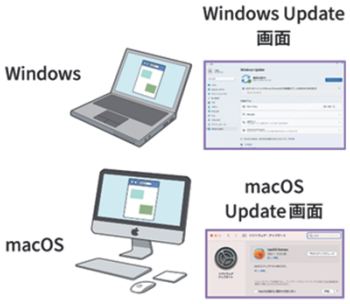
IT機器やネットワークの安全な利用

利用する機器を最新の状態にする

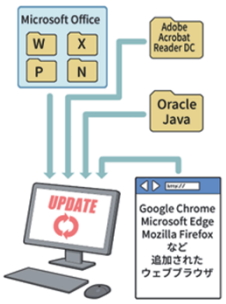
IT機器の脆弱性を突かれた攻撃を受けないように、使用する機器は常に最新の状態にしましょう。

□	サイバー攻撃は、PCの機器の作動に必要なソフトウェア等の脆弱性を突かれることが多いため、業務で利用するPCのソフトウェアは常に最新の状態にしましょう。
□	機器が正常に動作しているか確認しましょう。挙動がおかしい場合は、ウイルス対策ソフトで、怪しいソフトウェアが混入していないか可能な限り確認できる状態にしておきましょう。
□	ネットワーク機器をはじめとする、IT機器（プリンタやネットワークカメラなど）も常に最新の状態にしておきましょう。
□	バックグラウンドで動作するソフトウェアおよびサービスは業務上必要なものだけにしましょう。
□	IT 機器の初期パスワードは、必ず購入時のものから変更しておきましょう。なぜなら同じ機種の初期パスワードが全て同じだった場合などに、不正アクセスされ乗っ取られる可能性があるためです。 また、ファームウェアも常に最新になるように頻繁に更新しましょう。

OSと基本ソフトの更新



重要ソフトも更新



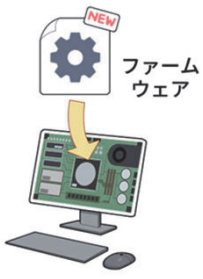
無線LANアクセスルータ

ネットワーク対応プリンタ

ネットワークカメラ

セキュリティソフトも更新

本体のファームウェアも更新



ネットにつながるIT機器（ルータやIoT機器）も初期パスワードの変更やファームウェア更新をしておくこと

ハンドブック記載箇所
第１章２　①OSやソフトウェアは常に最新の状態にしておこう

参考資料

IPA　IT製品の調達におけるセキュリティ要件リスト活用ガイドブック
https://www.ipa.go.jp/security/it-product/guidebook.html

3

IT機器やネットワークの安全な利用

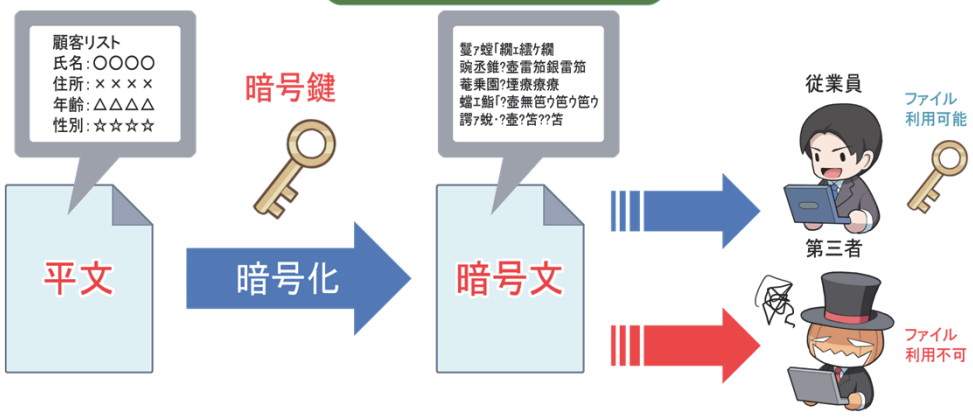
ネットワークを安全な状態で使う

ネットワークの利用を通じたサイバー攻撃や盗聴リスクを防ぐため、ネットワークを安全な状態で使いましょう。

□	サイバー攻撃はネットワークを通じて攻撃してくることが多いため、利用するネットワークはネットワーク機器に関する安全対策のほか、重要な情報の通信にはVPN等を用いる等、ネットワークの暗号化対策も行いましょう。
□	公衆無線LANを使用する場合は、VPNを使った通信内容の暗号化等を行うことにより盗聴リスクに備えましょう。
□	近年、VPN機器の脆弱性を悪用されたサイバー攻撃が発生しています。VPNのファームウェアに脆弱性がないか定期的に確認し、パスワードは推測されにくいできる限り長いものにしましょう。
□	インターネットを通じてデータを提供する場合には、できるだけ暗号化を施す等、第三者が解読できない形で送付しましょう。

VPNによる通信のイメージ

暗号化のイメージ



ハンドブック記載箇所
第５章2.10　まとめて暗号化するVPN
第５章コラム.1　暗号化の超簡単説明

参考資料

IPA　TLS暗号設定ガイドライン 安全なウェブサイトのために（暗号設定対策編）
https://www.ipa.go.jp/security/crypto/guideline/ssl_crypt_config.html

IT機器やネットワークの安全な利用

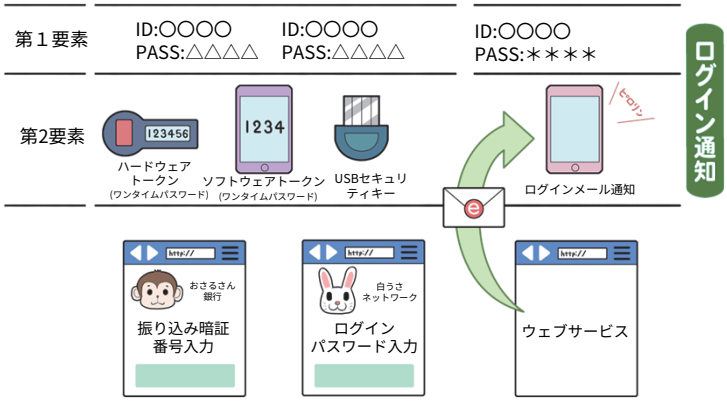
4 第三者へのデータ流出を防ぐ

なりすましによるデータ流出や内部からのデータの持ち出し防ぐために、多要素認証や大容量媒体の管理を行いましょう。

□	社内からのデータ流出については、標的型メール等のなりすまし対策が重要です。攻撃者になりすまされ侵入を許すことで、利用者が管理する情報が意のままに見えてしまうため、不審なメールを発見したら、メールヘッダ、本文、URLを注意深く確認しましょう。
□	なりすまし対策として、パスワードは適切なものを用いるほか、可能であれば、パスワードが万が一漏えいしても第三者からのログインをブロックできる多要素認証を用いたサービスやシステムを利用しましょう。
□	内部不正防止の原則として、不正を犯すことについて機会を与えないこと、動機を与えないこと、正当化させないことが必要です。
□	社員が不正にデータを持ち出すことに対する対策も必要です。アクセス権限の適切な設定、USB等の機器の接続管理や大容量媒体の管理等を行いましょう。

関係者になりすました攻撃者は心の隙を突いて騙す

多要素認証やログイン通知でセキュリティを向上



ハンドブック記載箇所
第1章4.1　可能な限り多要素や生体認証を使う
第５章1.6　二段階認証と二要素認証と多要素認証の安全性
第6章6.3　問題が起きると事業継続に影響を及ぼす

参考資料

IPA　情報漏えいを防ぐためのモバイルデバイス等設定マニュアル
https://www.ipa.go.jp/archive/security/crypto/dev_setting.html

習得テスト

● Q1. 社内の情報資産を適切に管理するにあたって、情報セキュリティの観点から実施すべきこととして適切なものをすべて選んでください。

a. どのような情報資産があるかの特定
b. 現状の情報セキュリティ対策の状況の確認
c. 脅威や脆弱性の状況や動向の把握
d. 発生する可能性があるリスク・損害の想定と特定

● Q2.ランサムウェアが起こす被害として適切なものはどれでしょうか？

a. PCの強制的なロックや、ファイルの暗号化等を行い、復元することと引き換えに身代金を要求する
b. 感染したパソコンの内部情報を勝手に外部に送信する
c. ユーザのキーボード操作をそのまま外部に送信する
d. 攻撃者からの指令で、他のコンピュータへの攻撃等の有害な動作を行う

● Q3. あなたは、メールを使った業務を行っています。受信したメールの内容に対する最初の行動として不適切なものをすべて選んでください。

a. 添付ファイルをクリックする
b. URLリンクをクリックする
c. 銀行口座にお金を振り込む
d. 差出人のメールアドレスに返信をする。

差出人：support@*****.com
件名：【至急】請求書の送付
添付ファイル：請求書.exe

〇〇様
〇〇サポートの藤田です。
弊社の銀行口座が変更になりましたので、
請求書を再送いたします。
http://******.org/

◆パスワードに関する〇×クイズ

- パスワードは、すべてのサービスで同じものを使用してもよい。（　）
- パスワードは、推測されにくく、できる限り長いものが良い。（　）
- パスワードは、他人に教える必要がある場合もある。（　）
- パスワードの入力欄が「●●●」のように隠されていれば、盗み見られることはない。（　）

習得テスト：解答

● Q1. 答え　すべて正しい
解説：適切な対策を実現するためには、まずは自らの情報資産状況や対策の状況、最新の脅威や脆弱性、それによって発生する可能性があるリスク等を正しく認識することが必要となります。自らの状況の正確な把握を通じて、適切な対策を実現していくことが重要です。

参考資料
IPA　中小企業の情報セキュリティ対策ガイドライン第3.1版
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

● Q2. 答え　**a**. PCの強制的なロックや、ファイルの暗号化等を行い、復元することと引き換えに身代金を要求するパスワードを定期的に変更する。
解説：ランサムウェアは、PCの強制的なロックやファイル暗号化等を行い、復元と引き換えに身代金を要求します。ただし、身代金を払ったからといって必ずしも復元してもらえるとは限りません。

参考動画
IPA　今、そこにある脅威 組織を狙うランサムウェア攻撃
https://www.youtube.com/watch?v=TWqJ5P8oaUM

● Q3. 答え　すべて不適切
解説：怪しいメールが届いたら慌てずに以下の観点を確認し、メールを開かずに破棄するか、社内の情報システム担当者などの相談窓口・通報先に連絡しましょう。
差出人アドレス：@以降のドメインが正規のものか、偽のドメインに注意しましょう。
本文：不自然な文章や心当たりのない内容ではないか確認しましょう。
添付ファイル/URL：開くとマルウェア感染の危険あり！少しでも不審なら、メールを開かないようにしましょう。

参考動画
そのメール本当に信用してもいいんですか？ 標的型サイバー攻撃メールの手口と対策
https://www.youtube.com/watch?v=5K9U0-ASQM8

◆ パスワードに関する〇×クイズ
➢ パスワードは、すべてのサービスで同じものを使用してもよい。（×）
解説：一つのサービスでパスワードが漏えいすると他のサービスも不正アクセスの危険に晒されます。
➢ パスワードは、推測されにくい、できる限り長いものが良い。（〇）
解説：単純なパスワードは簡単に推測され、不正アクセスのリスクが高まります。強度を高めるためには、記号を追加しましょう。
➢ パスワードは、他人に教える必要がある場合もある。（×）
解説：いかなる理由でも、パスワードを他人に教えてはいけません。
➢ パスワードの入力欄が「●●●」のように隠されていれば、盗み見られることはない。（×）
解説：入力している文字や指の動きを直接見られるリスクは残ります。

参考動画
IPA　華麗なる情報セキュリティ対策 #3「パスワードの適切な設定と管理」
https://www.youtube.com/watch?v=LuwXd6NqU64

相談窓口と支援サービス

サイバー攻撃に気付いたり、 あるいは第三者からの連絡で気付いた場合は、まずは社内の情報管理者に相談の上、必要に応じて各種窓口に相談しましょう。

気付いた場合は機器の電源を落とさないままネットから切断し、なるべくわかる範囲で事象を記録しておきましょう。

各種連絡窓口のウェブサイト等	QRコード
企業や組織がインシデント発生に関する相談や、標的型サイバー攻撃に関する相談、その他の情報セキュリティに関する一般的な相談がしたい場合には・・・ IPA「サイバーセキュリティ相談窓口（企業組織向け）」 メールでの問い合わせ:cs-support@ipa.go.jp	https://www.ipa.go.jp/security/support/soudan.html
ランサムウェア被害や不正アクセス等による情報漏えい被害等に遭った場合には・・・ 都道府県警察「サイバー事案に関する相談窓口」 よくある相談事例と対応方法のほか、オンラインの相談窓口も設置されています。 被害届は最寄りの警察署等に連絡をお願いします。 なお、緊急性を要する場合には、110番通報しましょう。	https://www.npa.go.jp/bureau/cyber/soudan.html
要配慮個人情報が含まれる個人データの漏えい等した場合には・・・ 個人情報保護委員会「漏えい等の対応とお役立ち資料」	https://www.ppc.go.jp/personalinfo/legal/leakAction/

サイバーセキュリティお助け隊サービス（IPA）	QRコード
サイバーセキュリティに何をしてよいかわからない、セキュリティにコストをかけられないといった悩みを抱える中小企業のために、国が認定したサービスです。「見守り」「駆け付け」「相談」など中小企業に不可欠なサービスをワンパッケージで安価に提供しています。	https://www.ipa.go.jp/security/otasuketai-pr/

インターネットの安心・安全ハンドブック　Ver5.10
リーフレット（中小企業等向け）

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

制作・著作　　内閣官房　内閣サイバーセキュリティセンター

内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity