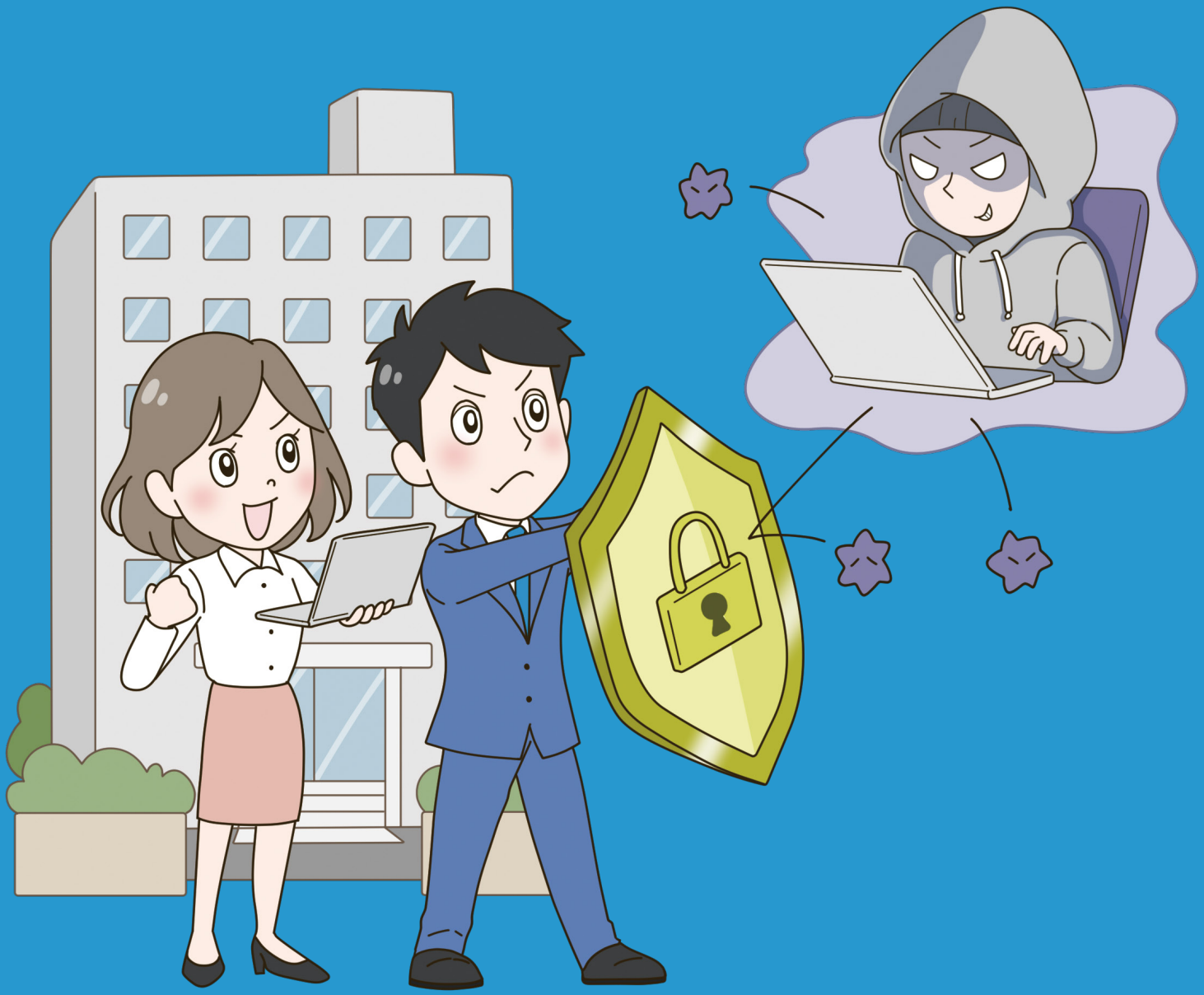
【企業・従業員層向け】講習テキスト

サイバーセキュリティ普及啓発

社内・社外のセキュリティを向上しよう

企業として気を付けたい
サイバーセキュリティ対策



企業として気を付けたい
サイバーセキュリティ対策

サイバー攻撃は、企業の規模や業種に関係なく行われています。
攻撃者は、セキュリティ対策が手薄な企業や、
従業員の不注意をきっかけに侵入を試みます。
そのため、「自社は大丈夫」と過信せず、企業として気を付けたい
サイバーセキュリティ対策を正しく理解することが重要です。

1. 企業活動を脅かすサイバー攻撃
サイバー攻撃は企業全体のリスクです

POINT **サイバー攻撃は企業の事業継続や信用に大きな影響を与える**

サイバー攻撃は
企業全体のリスクです

サイバー攻撃は、情報漏えいや金銭的被害だけでなく、業務が停止したり、社会的信用が低下してしまうなど、企業の事業活動そのものに大きな影響を与えます。

一度被害が発生すると、復旧には多くの時間やコストがかかり、取引先や顧客に影響が及ぶ可能性もあります。

そのため、サイバー攻撃は特定の部署だけの問題ではなく、企業全体で向き合うべき重要なリスクです。

2. 注意したいサイバー攻撃の手口
小さな侵入が大きな被害につながる

POINT **攻撃の手口と被害の広がりを理解し、被害を最小限に抑えましょう**

攻撃者は、企業や従業員が日常的に利用するさまざまな経路を狙って侵入を試みます。

例えば、取引先を装ったメールを送付し、金銭を騙し取ろうとしたり、メールをきっかけに偽のウェブサイトへ誘導し、IDやパスワード等の情報を盗み取ろうとしたり、マルウェアに感染させようとしたりします。

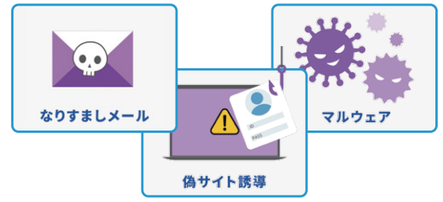
攻撃の手口は年々巧妙化しており、取引先を装った偽のメールに騙されるケースが実際に発生しています。

一見すると、普段やりとりしている相手からの正規の連絡のように見えるため、不審だと気づきにくいことがあります。

マルウェアに感染した機器は攻撃に利用され、社内のシステムへ被害が広がる恐れがあります。

攻撃の手段や被害の広がりを理解するとともに、被害を最小限に抑えるためのバックアップの重要性を認識しておくことも大切です。

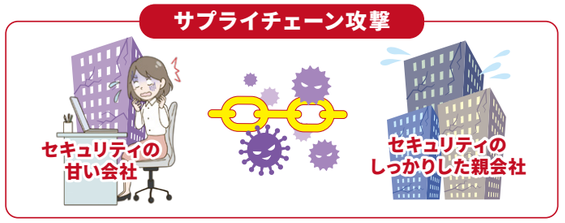
小さな侵入が大きな被害につながる



バックアップ体制を整えよう

3. サプライチェーン攻撃への注意
守るのは自社だけではありません

POINT **「自社は関係ない」と思わず対策を見直しましょう**



「サプライチェーン攻撃」は、企業同士のつながりを悪用した攻撃です。

セキュリティが堅牢な企業を直接狙うのではなく、対策が不十分な企業を足がかりにして、最終的な攻撃対象へ侵入します。

このような攻撃があることを理解し、「まさか自社には関係ない」と過信せず、正しいサイバーセキュリティ対策を行うことが重要です。

4. 基本となるセキュリティ対策
パスワードの管理を見直しましょう

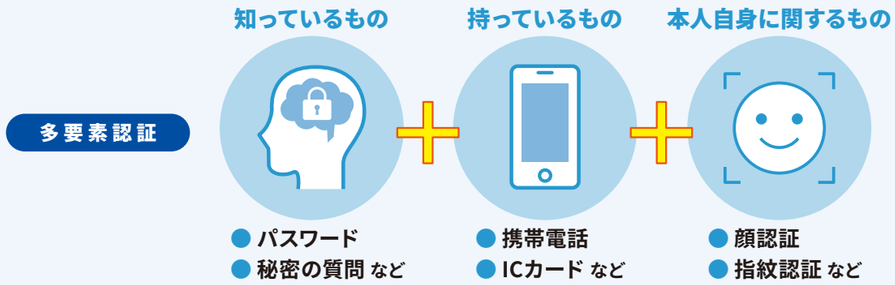
POINT パスワードは、出来るだけ長く設定し、使い回しはしないこと

基本的なセキュリティ対策として、パスワードの管理も重要です。パスワードは、長く推測されにくいものを設定し、複数のサービスやシステムで使い回さないようにしましょう。

また、多要素認証を設定することで、さらに安全性を高めることができます。

身に覚えのないパスワードの再設定リクエストが送られてくるなど、パスワードが流出した可能性がある場合は、速やかにパスワードを変更しましょう。

2つ以上の要素を組み合わせて設定しよう



多要素認証は、パスワードだけでなく、その他の認証方法を組み合わせてロックを厳重にする方法です。機種や利用するサービスによって、さまざまな認証方法がありますが、複数の認証方法を組み合わせることで、安全性は大きく高まりますので、必ず設定するようにしましょう。

- **パスワードの定期変更は基本は必要なし。**
- **ただし、流出の可能性がある場合などは、速やかに変更してください。**

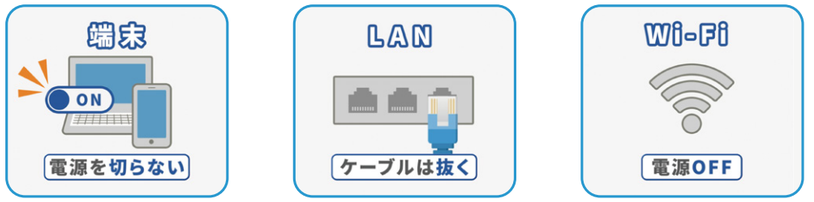
5. 攻撃の兆候を感じたら
異変に気付いたら正しく対応しましょう

POINT 異変に気付いたら証拠を残し組織の手順で対応する

身に覚えのないログイン通知や、不審な操作履歴などに気づいた場合は、サイバー攻撃を受けている可能性があります。その際は、電源を切ったり操作を続けたりせず、まずはネットワークから切断し、画面やログなどの情報をそのまま残すことが重要です。

その後は、自己判断で対応せず、組織で定められた手順に従って、上司や担当部署へ速やかに連絡し、落ち着いて適切な緊急対応を行いましょう。

実被害が判明したら・・・



端末の電源は落とさない
証拠保全のため、
端末の電源は落とさない。

LANケーブルを抜く
通信を遮断し、
マルウェアの拡散と
攻撃者との通信を断つ。

無線LANもオフにする
無線LANは、
本体もアクセスポイントも
オフにする。

上司や担当部署へ速やかに連絡し、落ち着いて対応する

サイバーセキュリティ クイズ

第1問 「サプライチェーン攻撃」の説明として正しいものはどれですか？

1. ターゲットに直接マルウェアを仕掛けること
2. 対策が不十分な関連企業などを足がかりにして、最終的な対象を攻撃すること
3. 特定の個人宛に大量のメールを送り付けること
4. 企業のホームページを開いてF5キーを連打すること

回答記入欄

第2問 パスワードの設定と管理について、「間違っている」ルールはどれですか？

1. 忘れないために、あらゆるサービスで同じパスワードを使うようにする
2. 長く複雑なものを設定する
3. 誕生日や名前など、推測されやすいものは避ける
4. 基本的に定期変更は必要ないが、流出の恐れがある時は速やかに変更する

回答記入欄

第3問 攻撃者が、サイバー攻撃を行う際に使うものは次のうちどれですか？

1. メールの添付ファイル
2. メールのリンク
3. 取引先を装った電話
4. 1～3のすべて

回答記入欄

第4問 「多要素認証」とはどのような仕組みですか？

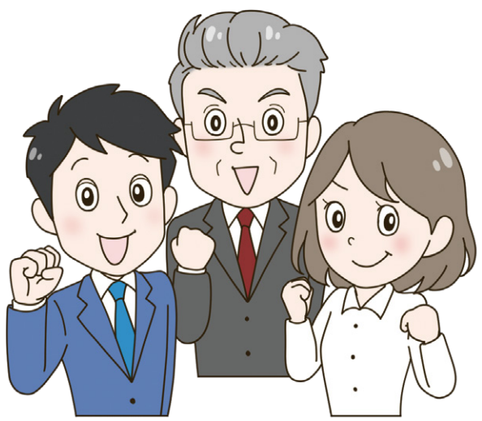
1. 複数の人が一つのパスワードを共有すること
2. 認証を何回も繰り返し行うこと
3. パスワードだけでなく、生体認証、スマートフォンアプリなど複数の認証要素を組み合わせること
4. パスワードを忘れた時に、複数の質問に答えること

回答記入欄

第5問 もしサイバー攻撃を受けていることに気づいたら、最初に行うべき対応はどれですか？

1. 証拠を消すためにすぐに端末の電源を切る
2. 電源は落とさず、すぐにLANケーブルを抜くかWi-Fiをオフにしてインターネットから切断する
3. 画面に警告文と電話番号が表示されるので、電話をかけて指示に従う
4. 誰にも言わずにしばらく様子を見る

回答記入欄



ぜひ、この講習テキストや講習動画を
職場の皆さまで共有して、
サイバーセキュリティへの
関心を高めるきっかけにご活用下さい。

クイズの答え　第1問：②、第2問：①、第3問：④、第4問：③、第5問：②

サイバーセキュリティの基本的な知識を紹介

インターネットの安全・安心ハンドブック

職場での研修や話し合いなど、学習の機会にお役立てください。

国家サイバー統括室（NCO）では、サイバーセキュリティに関する普及啓発活動の一環として、「インターネットの安全・安心ハンドブック」を公開しています。本ハンドブックは、皆さまにサイバーセキュリティに関する基本的な知識を紹介し、誰もが最低限実施しておくべき基本的なサイバーセキュリティ対策を実行してもらうことで、さらに安全・安心にインターネットを利活用してもらうことを目的に制作したものです。

CONTENTS

国家サイバー統括室
National Cybersecurity Office

「インターネットの安全・安心ハンドブック」のダウンロードはこちら ▶

https://security-portal.cyber.go.jp/guidance/handbook.html