TOP SECRET

MISSION 4

もしもマニュアル

緊急時対応用マニュアルの作成

サイバー攻撃を受けたときのために、あらかじめ緊急時対応用マニュアルを作成しておきましょう。
作成に当たっては、情報処理推進機構（IPA）が中小企業・小規模事業者向けに提供している「中小企業の情報セキュリティ対策ガイドライン」付録3の作成ツール「情報セキュリティポリシーサンプル」の「11.情報セキュリティインシデント対応ならびに事業継続管理」を活用すれば、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。
緊急時対応用マニュアルは定期的に見直すことも必要です。

マニュアルに記載すべき事項

緊急時対応用マニュアルには次の項目を記載します。

記載すべき項目	記載すべき内容	本書の参照ページ
対応体制	一次対応者、対応責任者、最高責任者を決めます。	136ページ
サイバー攻撃被害の影響範囲と対応者	サイバー攻撃が発生した場合に対応策を決めるため、サイバー攻撃被害の影響範囲のレベルと対応者を決めます。	136ページ

記載すべき項目	記載すべき内容	本書の参照ページ
サイバー攻撃被害の連絡および報告体制	サイバー攻撃が発生した場合の連絡・報告手順を決めます。	137ページ
対応手順	サイバー攻撃被害の内容ごとに、影響範囲のレベルごとの対応手順を決めます。	137ページ
漏えい・流出発生時の対応	社外秘または極秘情報資産の盗難、流出、紛失の場合の対応を決めます。	138ページ
改ざん・消失・破壊・サービス停止発生時の対応	情報資産の意図しない改ざん、消失、破壊や情報資産が必要なときに利用できない場合の対応の対応を決めます。	140ページ
ウイルス感染時の初期対応	悪意のあるソフトウェアに感染した場合の対応の対応を決めます。	143ページ
届け出および相談 ＜届け出・相談先＞	サイバー攻撃被害対応後に届け出または相談する機関を検討しておきます。	145ページ
大規模災害などによる事業中断と事業継続管理	大規模災害などの影響により事業が中断した場合に備えて、対応策を決めておきます。	146ページ
想定されるリスク	事業の中断が想定される大規模災害などを検討します。	146ページ
復旧責任者および関連連絡先	想定する大規模災害等が発生し、事業が中断した際の復旧責任者の役割および関係者連絡先について確認します。	147ページ
事業継続計画	被害対象に応じて復旧から事業再開までの計画を立案します。	147ページ

P136～147に記載例を示します。

基本事項の決定

対応体制を決める

サイバー攻撃を受けたときに会社として対応する体制を決めます。
対応体制として一次対応者、対応責任者、最高責任者を決めます。

最高責任者	代表取締役
対応責任者	サイバー攻撃対応責任者
一次対応者	発見者またはシステム管理者

サイバー攻撃被害の影響範囲と対応者を決める

サイバー攻撃被害の影響範囲のレベルと対応者を決めます。サイバー攻撃被害が発生した場合、被害レベルを判断して対応を決めます。

被害レベル	影響範囲	対応者
3	顧客、取引先、株主などに影響が及ぶとき 個人情報が漏えいしたとき	最高責任者 対応責任者
2	事業に影響が及ぶとき	対応責任者
1	従業員の業務遂行に影響が及ぶとき	一次対応者
0	影響はないが、将来においてサイバー攻撃が発生する可能性がある事象が発見されたとき	一次対応者

ACTION 3 サイバー攻撃被害の連絡および報告体制を決める

サイバー攻撃が発生した場合の連絡・報告手順を決めます。

レベル1以上の被害が発生した場合、発見者は以下の連絡網に従い、対応者に速やかに報告し、指示を仰ぐ。

被害レベル	最終対応者	緊急連絡先
3	最高責任者	携帯電話：090-****-**** メールアドレス：president@*****.co.jp
2	対応責任者	携帯電話：090-****-**** メールアドレス：incident@*****.co.jp
1	一次対応者	携帯電話：090-****-**** メールアドレス：system@*****.co.jp

ACTION 4 対応手順を決める

サイバー攻撃を認知した際、確認事項や連絡系統を一元化し迅速な対応をするための対応手順を決めます。

区分	サイバー攻撃被害の状況
漏えい・流出	社外秘または極秘情報資産の盗難、流出、紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

対応手順1

漏えい・流出発生時の対応

被害レベル3の場合

STEP1	発生の報告	漏えいや流出の事実を発見したり、外部から連絡を受けたりした者は即座に対応責任者および最高責任者に報告します。	発見者、一次対応者
STEP2	原因の特定と二次被害の防止	対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行します。	対応責任者
STEP3	被害者対応の準備	個人情報が流出した場合、漏えい・流出した個人情報の本人（被害者）への対応を準備します。	対応責任者
STEP4	問い合わせ対応の準備	被害者本人や関係先からの問い合わせ対応を準備します。	対応責任者
STEP5	報道発表の準備	対応責任者は影響範囲・被害の大きさによって総務部に報道発表の準備を申請します。	対応責任者

STEP6	被害届の提出	対応責任者はサイバー攻撃などの不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出ます。	対応責任者
STEP7	監督官庁への届け出	対応責任者は個人情報の漏えいの場合には監督官庁に届け出ます。	対応責任者
	対応結果および対策を公表	最高責任者は、社内および影響範囲の全ての組織・人に対応結果および対策を公表します。	最高責任者

ACTION 2 被害レベル2の場合

STEP1	発生の報告	発見者は発見次第、システム管理者に報告します。	発見者
STEP2	漏えい先の調査と報告	システム管理者は漏えい先を調査し、対応責任者に報告します。	システム管理者
STEP3	社内への通知	システム管理者は社内関係者に周知します。	システム管理者

対応手順2

改ざん・消失・破壊・サービス停止発生時の対応

被害レベル3の場合

STEP1	発生の報告	発見者は即座に対応責任者および最高責任者に報告します。	発見者
STEP2	原因の特定と応急措置の実施	システム管理者は原因を特定し、応急処置を実行します。	システム管理者
STEP3	社内周知と担当部署への連絡	対応責任者は社内に周知するとともに総務部情報システム担当に連絡します。	対応責任者
STEP4	復旧措置	電子データの場合はシステム管理者がバックアップによる復旧を実行します。	システム管理者
		機器の場合はシステム管理者が修理、復旧、交換などの手続きを行います。	システム管理者
		書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復します。	情報セキュリティ部門責任者
STEP5	原因対策の実施	システム管理者は原因対策を実施します。	システム管理者
	対応結果および対策を公表	最高責任者は、社内および影響範囲の全ての組織・人に対応結果および対策を公表します。	最高責任者

ACTION 2 被害レベル2の場合

STEP1	発生の報告	発見者はシステム管理者に報告します。	発見者
STEP2	原因の特定と応急措置の実施	システム管理者は原因を特定し、応急処置を実行します。	システム管理者
STEP3	社内周知と担当部署への連絡	対応責任者は社内に周知するとともに総務部情報システム担当に連絡します。	対応責任者
STEP4	復旧措置	電子データの場合はシステム管理者がバックアップによる復旧を実行します。	システム管理者
		機器の場合はシステム管理者が修理、復旧、交換などの手続きを行います。	システム管理者
		書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復します。	情報セキュリティ部門責任者
STEP5	原因対策の実施	システム管理者は原因対策を実施します。	システム管理者

ACTION 3 被害レベル1の場合

STEP1	発生の報告	発見者はシステム管理者に報告します。	発見者
STEP2	原因の特定と応急措置の実施	システム管理者は原因を特定し、応急処置を実行します。	システム管理者

STEP3	復旧措置	電子データの場合はシステム管理者がバックアップによる復旧もしくは再作成・入手を実行します。	システム管理者
		機器の場合はシステム管理者が修理、復旧、交換などの手続きを行います。	システム管理者
		書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復します。	情報セキュリティ部門責任者
STEP4	原因対策の実施	システム管理者は原因対策を実施します。	システム管理者

ACTION 4 被害レベル0の場合

発見者は発見次第、発生可能性のあるサイバー攻撃と想定される被害をシステム管理者に報告します。

MISSION 4-5

対応手順3

ウイルス感染時の初期対応

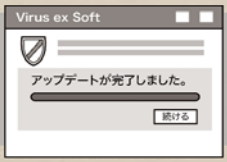
ACTION 1 従業員が対応可能な場合

従業員は、業務に利用しているパソコン、サーバーまたはスマートフォン、タブレット（以下「コンピューター」といいます。）がウイルスに感染した場合には、次の手順を実行します。

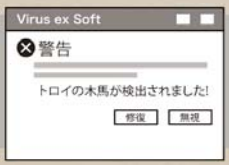
STEP1 ネットワークからコンピューターを切断します。

STEP2 システム管理者に連絡します。

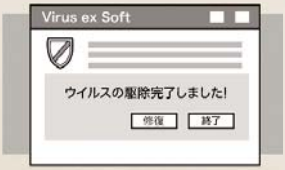
STEP3 ウイルス対策ソフトの定義ファイルを最新版に更新します。



STEP4 ウイルス対策ソフトを実行しウイルス名を確認します。



STEP5 ウイルス対策ソフトで駆除可能な場合は駆除します。



STEP6 駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認します。

STEP7 システム管理者に報告します。

ACTION 2 従業員が対応できない場合

従業員自身で対応できないと判断する場合はシステム管理者に問い合わせます。

・ウイルス対策ソフトで駆除できない。
・システムファイルが破壊・改ざんされている。
・ファイルが改ざん・暗号化・削除されている。

対応手順4

届け出および相談

システム管理者は、サイバー攻撃被害への対応後に以下の機関への届け出または相談を検討します。

＜届け出・相談先＞

独立行政法人 情報処理推進機構セキュリティセンター（IPA/ISEC）

ウイルスの届け出

郵送、FAX、E-mail、Webにて受け付けしています。
届け出の際は、Webサイトにある届出様式を使用してください。
Web：https://www.ipa.go.jp/security/outline/todokede-j.html
FAX：03-5978-7518
E-mail：virus@ipa.go.jp
※郵送先については、Webサイトにてご確認ください。

不正アクセスに関する届け出

FAX、E-mailにて受け付けしています。
届け出の際は、Webサイトにある届出様式を使用してください。
Web：https://www.ipa.go.jp/security/ciadr/index.html
FAX：03-5978-7518
E-mail：crack@ipa.go.jp

相談

情報セキュリティ安心相談窓口
主に電話、E-mailにてご相談を受け付けしています。
電話：03-5978-7509
受付時間：10：00−12：00　13：30−17：00　土日祝日・年末年始を除く
E-mail：anshin@ipa.go.jp
※詳細については、Webサイトをご覧ください。
https://www.ipa.go.jp/security/anshin/index.html

大規模災害などによる事業中断と事業継続管理

会社のITシステムが直面するリスクには、サイバー攻撃などの人為的なリスクのほかに、大規模災害や停電など環境的なリスクもあります。こうしたリスクによって、ITシステムが使えなくなり、長期の事業中断を余儀なくされるケースもあります。企業の経営者は、こうした環境リスクの影響により、会社の事業が中断した場合に備えておく必要があります。

想定されるリスクをリストアップする

ITシステムが重大な被害を受け、事業を中断しなければならないリスクをリストアップします。

- 大型地震の発生に伴う設備の倒壊・損壊（電源設備や空調機など）
- 通信会社の事故による回線の途絶
- 落雷による一部地域の停電

ACTION 2 復旧責任者および関連連絡先

リストアップしたリスクに基づいて被害対象となる設備と復旧の責任者、関係者の連絡先を整理しておきます。

被害対象	復旧責任者	関係者連絡先
電源設備 空調機	総務部長	○○電力△△支店 (株)○○設備
(○○システム) ハードウェア ソフトウェア ネットワーク機器 回線サービス バックアップクラウド サーバー	対応責任者 システム管理者	(株)○○システム開発 (株)△△ネットワーク サービス (株)◇◇マネージド サーバー
顧客	営業部長	営業部取引先リスト参照
従業員人的被害	総務部長	従業員名簿参照

ACTION 3 事業継続計画

対応責任者は、想定する大規模災害などの被害が発生し、事業が中断した際の復旧責任者の役割認識および関係者連絡先について、有効に機能するか検証します。

復旧責任者は、被害対象に応じて復旧から事業再開までの計画を立案します。

ワークショップ 自社でやろう サイバー攻撃への対応リアクション

ある日、JPCERT コーディネーションセンターという団体から次のような連絡を受けました。

「あなたの会社から官公庁に対するサイバー攻撃が行われています。」

担当者から連絡を受けたあなた（経営者）はどうしますか。

1. そんなことはないだろうと考え、そのまま事業を継続する。
2. 事業を継続しながら、原因を探すよう指示する。
3. いったん全てのネットワークを遮断し、原因を探すよう指示する。

正解はもちろん3です。

1は論外です。もしかすると損害賠償を請求されることにもなりかねません。できれば2と考えたいところですが、どの端末が汚染されているのか分からない状況では事業を継続しながらでは不十分です。

ではどのような原因が考えられますか。

1. レンタルサーバーを利用しているWebサーバーが乗っ取られ、他社のネットワークの弱点を探すための不正な動作をしている。
2. 会社内の端末の1つがウイルスに感染して、ウイルスが入ったメールを官公庁や他の企業に送り続けている。
3. 会社内の端末の1つがウイルスに感染して、会社内にある従業員のメールアドレスやマイナンバーなどの個人情報、取引先情報などをひそかに送り続けている。

正解は全てです。

他の会社や官公庁に対するサイバー攻撃の拠点になっているということは、あなたの会社の端末が乗っ取られていて、誰にも分からないように外部からコントロールされているということですから、全ての原因が考えられます。