簡易版BCPシート（サイバー）

1.インシデント対応にあたっての重要ポイント

インシデント対応とは情報セキュリティインシデントが発生した際に、通報を受け、状況を踏まえ対処方針を決定し、問題解決を行い、インシデントを収束させるプロセスである。

1 **組織全体で対処**
見えない攻撃者との攻防となるため、刻々と変化する状況下でインシデント収束するためには組織全体で対処しなければならない。

2 **初動は迅速に対応**
対外的には二次被害が出る前に先手を打つことが要求されるため、充分な情報が揃っていない状況で判断し、スピード感を持った対応が求められる。

3 **さまざまな対応を同時並行で推進**
情報システムの復旧、原因調査、取引先対応や顧客対応を同時並行で進めなければならない。自組織内で全て対応することが困難な場合はセキュリティベンダーなど外部専門家に支援依頼する。

2.対応体制

意思決定者	社長	事業継続是非を含むインシデント対応方針や対策承認など、組織全体の情報セキュリティ対策を決定する。
初動対応担当	ITシステム担当者（スミキーナ）	主に情報システムに関する指揮をとる。
対外対応担当	総務担当者	主に顧客、取引先、警察など社外組織との応対の指揮をとる。

想定被害１

Emotet（マルウェア）感染

従業員Aが利用するパソコン1台にて取引先を騙る不審なメールを受信し、添付ファイルをクリックした。直後から社内にAを騙る不審なメールが多数送信されるとともに、取引先にも同様の不審メールが複数送信されている。社内ではさらに2名の従業員が不審なメールの添付ファイルをクリックしてしまったと報告があった。

想定被害２

コーポレートサービス紹介サイト（公開ホームページ）改ざん

自組織の公開ホームページのトップページにある新着情報の表示箇所に突然外国語の見慣れない文章とURLが多数書き込まれていると、顧客からの連絡があり気付いた。さらに公開ホームページ管理者である従業員Aおよび保守委託業者Bが管理ページにアクセスを試みたが、パスワードが変更されているのかログインできない状態となっている。また、同サイトは利用者専用ページにアクセスするためのお客様メールアドレスとログイン用のパスワード情報を保持している。

4.対応手順

（1）初動

①検知・連絡（目安：確認直後～24時間以内）

想定被害 1	意思決定者	初動対応担当から被害状況連絡を受け、インシデント対応体制の発令
	初動対応担当	・被害パソコンの特定（いつ添付ファイルをクリックしたのか） ・被害証跡の確保（不審通信成功ログファイルの保存、ウィルス検知ログファイルの保存、表示画面のキャプチャなど） ・状況を整理し意思決定者へ報告
	対外対応担当	緊急時ホットラインに連絡
想定被害 2	意思決定者	初動対応担当から被害状況連絡を受け、インシデント対応体制の発令
	初動対応担当	・被害事実の目視確認（問合せ内容通りの事象あり） ・被害証跡の確保（改ざんされた画面のキャプチャ、不正に変更されているコンテンツデータの保存など） ・状況を整理し意思決定者へ報告
	対外対応担当	緊急時ホットラインに連絡

1 初動

②被害の極小化（目安：確認直後～24時間以内）

1 初動	想定被害 1	意思決定者	
		初動対応担当	・被害パソコンの隔離（対象のサーバー・PC・Webシステムをネットワークから切り離す。証拠保全のためPCの電源は切らない。） ・被害メールアカウントのパスワード変更 ・全パソコンのアンチウィルス検査 ・Emocheckのダウンロードと試行（Emocheckとは、一般公開されている公的機関推奨のEmotet専用の感染チェックツール） ・全パソコンのEmocheck実施 ・全従業員に当該不審メールの文面共有と注意喚起
		対外対応担当	取引先に状況報告とお詫び速報
	想定被害 2	意思決定者	被害サイトの停止判断
		初動対応担当	・ホスティング業者に連絡し被害サイトの停止を依頼（ホスティング業者：Webコンテンツを掲載するサーバーを貸し出しているサービス提供者で、通信事業者やインターネットサービスプロバイダーが多い） ・ホスティング業者に管理者パスワードの再発行を依頼 ・お詫び用サイト準備と立ち上げ（被害サイトは調査、復旧のため停止しているため、攻撃されていない別のWebサイトを流用もしくは臨時開設したり、SNS活用等でお詫びする）
		対外対応担当	・お詫びサイトコンテンツの準備（被害を認識し組織的に対応着手していること、およびサービスの一時停止をお詫びする文書を作成する） ・利用者・取引先への状況報告とお詫び速報

③関係者との連携（目安：確認直後～72時間以内）

1 初動	想定被害 1		社内調査チームとの連携（セキュリティベンダー、システムベンダーなど外部委託先関係者も含めてインシデント対応方針の確認）
		意思決定者	【a.被害範囲確認】 ・アンチウィルス検査とEmocheck実施状況把握と未実施フォロー ・不審ファイル開封パソコンの特定（利用者からの報告とアンチウィルスシステムログを突き合わせ、どのくらいの期間感染していたのか） ・不審メール送信範囲の特定 ・情報漏えい可能性情報の一次整理（被害パソコンに保存していたメールの本文内容について個人情報、取引先機密情報有無と対象を調査） 【b.詳細調査実施判断】 ・セキュリティベンダーへの調査委託判断（取引先から調査結果の提出を求められることも考慮する） 【c.事業継続判断】 ・メール利用継続判断 【d.復旧判断】 ・調査用の保全パソコンの決定 ・保全パソコン以外の被害パソコンをクリーンインストール指示（アンチウィルスシステムおよびアンチウィルスベンダーからの対処方法実施だけでは確実に被害パソコン内の脅威をすべて取り除けたと言い切れないため、パソコンのハードディスクドライブ(HDD)を工場出荷時に戻し、アプリケーションなどを全て再インストールする）
		初動対応担当	
		対外対応担当	社外との連携（以下を対応） ・個人情報保護委員会への報告（個人情報保護法改正により、企業の情報漏えいインシデントは報告義務化されている） ・JPCERTコーディネーションセンター(JPCERT/CC)への報告（JPCERT/CCは日本を代表するCSIRTであり、国内のコンピュータセキュリティ情報を収集し、情報発信する機関） ・保険代理店への事故報告

1 初動	想定被害２	意思決定者	社内調査チームとの連携（セキュリティベンダー、システムベンダーなど外部委託先関係者も含めてインシデント対応方針の確認） 【a.被害範囲確認】 ・不正アクセスした攻撃者のアクセス権限で閲覧出来た情報の範囲を特定 ・情報漏えい可能性情報の一次整理（個人情報、取引先機密情報有無と対象を調査） ・不審メールのバラマキなど追加被害の確認 【b.詳細調査実施判断】 ・セキュリティベンダーへの調査委託判断（取引先から調査結果の提出を求められることも考慮する） 【c.事業継続判断】 ・代替サイト立ち上げ要否および時期の見極め 【d.復旧判断】 ・復旧（もしくは暫定復旧）に必要なセキュリティ対策の検討と見積り指示
		初動対応担当	
		対外対応担当	社外との連携（以下を対応） ・個人情報保護委員会への報告（個人情報保護法改正により、企業の情報漏えいインシデントは報告義務化されている） ・JPCERTコーディネーションセンター(JPCERT/CC)への報告（JPCERT/CCは日本を代表するCSIRTであり、国内のコンピュータセキュリティ情報を収集し、情報発信する機関） ・保険代理店への事故報告

（2）調査・公表

①調査（目安：1週間～3か月）

意思決定者	セキュリティベンダーへの調査発注を決裁
初動対応担当	・セキュリティベンダーへの調査発注内容と費用を報告 ・セキュリティベンダーへ調査のため提供する被害機器・パソコンやデータファイルの発送 ・調査後のセキュリティベンダー作成報告書を受領し、ベンダー報告会に出席（セキュリティベンダーが作成する調査報告書は裁判で調査証明書として活用される等、基本的に専門用語を用いた技術文書になっているため、報告会で調査員から補足説明を受ける場を設けることが多い） ・意思決定者へ調査結果を報告
対外対応担当	セキュリティベンダーとの契約および保険金支払い可否を損害保険会社担当に確認

2 調査・公表

②報告・情報公開（目安：1週間～3か月）

意思決定者	・連絡、お詫び対象と対応方針を承認 ・外部委託発注を決裁
初動対応担当	
対外対応担当	以下実施 【a.対外報告準備】 ・報告、お詫び対象と対応方針の決定（個人情報など機密情報が流出した場合は損害賠償対応方針も決定する） ・報告、お詫び文書の作成 ・想定問答集の準備 ・問合せ、クレーム対応体制の準備（コールセンター、お客様問合せ窓口および対応フローの準備） ・訴訟対応の準備（弁護士への事前連携） 【b.顧客、取引先、親会社への報告】 ・報告（二次被害の可能性があるため、出来る限り広範囲に実施） 【c.情報が流出した可能性がある被害者への報告、お詫び】 ・報告（抜け漏れないように実施） ・ホームページ等で公表（個別連絡手段が取れない場合） ・問合せ、クレーム対応 ・弁護士への相談

（3）事後対応

①復旧（目安：インシデント対応方針決定後～）

想定被害１	意思決定者	
	初動対応担当	・セキュリティベンダーへ提供した被害パソコンをクリーンインストール ・意思決定者への復旧報告
	対外対応担当	
想定被害２	意思決定者	
	初動対応担当	・被害サイトのコンテンツデータを被害前のバックアップデータからリストア（このまま再公開すると再度攻撃被害を受けてしまうため注意） ・Web脆弱性診断の実施 ・診断結果に応じたセキュリティ対策の実施 ・意思決定者への復旧報告
	対外対応担当	

②再発防止（目安：調査完了後～3か月）

意思決定者	再発防止計画の承認
初動対応担当	・被害および原因を受けて必要なセキュリティ対策の検討 ・再発防止計画の作成
対外対応担当	

③事後対応（目安：確認直後～3か月）

意思決定者	インシデントクローズ宣言（意思決定者がタスクの完了、残存リスクの受容を承認し、対応チームを解散する）
初動対応担当	
対外対応担当	・最終報告書の作成 ・顧客、取引先、親会社、被害者へ最終報告（調査結果、再発防止策を明記）

５.社外連絡先一覧

	電話番号	ベンダー/代理店名
セキュリティベンダー[*1]		
システム運用ベンダー[*2]		
保険契約の保険代理店等[*3]		

*1 セキュリティベンダーとは
主にウィルス対策ソフトウェアをはじめとするセキュリティ対策ソフトウェアや関連サービスを開発・提供している事業者のこと。

*2 システム運用ベンダーとは
導入されているシステムが問題なく稼働するように日々の運用管理を実施する事業者のこと。

*3 サイバーリスク保険証券記載の連絡先を入力する。

公的機関

	連絡先	補足
都道府県警本部 サイバー犯罪相談窓口[*1]		窓口等一覧：https://www.npa.go.jp/bureau/cyber/soudan.html
監督省庁[*2]		窓口等一覧：https://www.ppc.go.jp/files/pdf/180717_kengeninin_list_detail.pdf
JPCERTコーディネーションセンター[*3]へのインシデント報告	―	Webフォーム・電子メール・Faxで報告可能。 対応できる内容・連絡先：https://www.jpcert.or.jp/form/
IPA　情報セキュリティ 安心相談窓口[*4]	03-5978-7509	電話・電子メール・Fax等でご相談が可能。 詳細：https://www.ipa.go.jp/security/anshin/index.html

*1 窓口等一覧ページから自社の都道府県の窓口を確認し、連絡先に入力する。

*2 個人データの漏えい等事案が発生した場合に報告する。自社の業種等の報告先の監督省庁を確認し、連絡先を入力する。

*3 JPCERTコーディネーションセンター（JPCERT/CC）とは
コンピューターセキュリティインシデントについて、日本国内に関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行う、特定の政府機関や企業からは独立した中立の組織。

*4 IPA　情報セキュリティ安心相談窓口とは
IPA（独立行政法人情報処理推進機構）が国民に向けて開設している、ウイルスおよび不正アクセスに関する技術的なご相談を受け付ける窓口。

東京海上日動　サイバーリスク保険等の加入者専用サービス

	電話番号	補足
緊急時 ホットラインサービス	0120-269-318 （24時間365日対応）	東京海上日動のサイバーリスク総合支援サービス インシデント発生時の初動対応から再発防止に至るまで専門的なアドバイスや「調査支援」「緊急時広報支援」「コールセンター設置支援」「弁護士相談」等の専門事業者を紹介するもの

親会社CSIRT[*1]、委託先、取引先各社等

社名	連絡先	担当部署・担当者

*1 CSIRT：Computer Security Incident Response Teamの略。組織のサイバーインシデントに対処するため、情報収集や対応方針の策定、インシデント発生時の原因解析、再発防止などを行う体制のこと。