

イ
ベ
ン
ト
①



今回のサイバー攻撃に関して、攻撃者から公開を示唆する脅迫メールが届く

対応を議論してください

補足

既にプレスリリース等の対
外発表を実施していた場
合には対応不要(+20点)
バックオフィスが指揮する

求める行動

脅迫メールの
対応方針を決める

振り返りポイント

届いた脅迫メールに対し、
「無視して破棄する」等の対
応方針について組織的な結
論を出すことができたか？

加減点

- ・イベント前に対応完了：+20点
- ・合意に至った：+10点
- ・合意に至らなかった：-10点

イベント
②



今回の事象について、経営層が説明を求めてきた。

対応を議論してください

補足

既に経営層への説明を実施していた場合には対応不要(+20点)

CSIRTが指揮する

求める行動

経営層に共有する
内容を議論する

振り返りポイント

今回のサイバー攻撃に対し、
「概要」「事業への影響」「見
通し」等について関係者と共
有範囲を合意できたか？

加減点

- ・イベント前に対応完了：+20点
- ・合意に至った：+10点
- ・合意に至らなかった：-10点

イ
ベ
ン
ト
③



外部機関(監督官庁など)
から説明を求められる。

対応を議論してください

補足

既に監督官庁への報告を
実施していた場合には対
応不要(+20点)
バックオフィスが指揮する

求める行動

監督官庁へ情報連携する
内容を議論する

振り返りポイント

「概要」「事業への影響」「見
通し」等について関係者と共
有範囲を合意できたか。

また、経営層に相談すること
は議論できたか。

加減点

- ・イベント前に対応完了：+20点
- ・合意に至った：+10点
- ・経営層に共有した：+10点
- ・合意に至らなかった：-20点

イベント
④



震度4の地震が発生した

対応を議論してください

補足

CSIRTが指揮する

求める行動

地震の影響調査の
優先度を議論する

振り返りポイント

地震の影響調査との優先度
を議論することができたか。

加点・減点

- ・合意に至った：＋１０点
- ・合意に至らなかった：－１０点

イ
ベ
ン
ト
⑤



コールセンターにサイバー
攻撃に関する問い合わせ
があった。

対応を議論してください

補足

一般コールセンター業務
はバックオフィスが担当し
ている

バックオフィスが指揮する

求める行動

対応方針の結論を出す

振り返りポイント

その場で対応を行わず、現在の情報を整理したうえで、対応方針の結論を出したか。特に公表すること、公表しないことについて関係者と議論できたか。

加点・減点

- ・合意に至った：+10点
- ・経営層に共有した：+10点
- ・合意に至らなかった：-20点

イ
ベ
ン
ト
⑥



マスコミからサイバー攻撃
に関する問い合わせが
あった。

対応を議論してください

補足

マスコミ対応はバックオ
フィスが担当している

バックオフィスが指揮する

求める行動

対応方針の結論を出す

振り返りポイント

その場で対応を行わず、現在の情報を整理したうえで、対応方針の結論を出したか。特に公表すること、公表しないことについて関係者と議論できたか。

加点・減点

- ・合意に至った：+10点
- ・経営層に共有した：+10点
- ・合意に至らなかった：-20点

イベント
⑦



お客さま向けホームページ
が閲覧できなくなった

対応を議論してください

補足

ホームページはIT部門が
担当している(問い合わせ
はまだない)。

バックオフィスが指揮する

求める行動

対応方針の結論を出す

振り返りポイント

現状のサイバーインシデント
対応とホームページ復旧の
関連性・優先度を議論でき
たか。

お客さまへの案内として
SNS活用等を検討できたか。

加点・減点

- ・対応の優先度を決定：＋１０点
- ・SNS案内の実施を決定：＋１０点
- ・合意に至らなかった：－２０点

イベント
⑧



材料調達先がサイバー攻撃を受け、材料入荷しないと連絡が入った

対応を議論してください

補足

材料の調達はバックオフィスが担当している
バックオフィスが指揮する。

求める行動

状況から因果関係を疑う

振り返りポイント

工場に今回の事象について
情報連携できたか。

自社と調達先のサイバー被害の因果関係を疑うことが
できたか。

加点・減点

- ・因果関係を疑えた：+20点
- ・放置してしまった：-10点

イベント
⑨



SNSで自社がサイバー攻撃を受けているのではないか、と炎上している

対応を議論してください

補足

**会社の公式SNSの管理は
バックオフィスが実施
バックオフィスが指揮する**

求める行動

対応方針の結論を出す

振り返りポイント

プレスによる発信も含めて、一般顧客向けの対応について対応方針を議論することができたか。

加点・減点

- ・合意に至った：＋１０点
- ・合意に至らなかった：－１０点

イ
ベ
ン
ト
⑩



工場のメンテナンス会社
から作業端末がウイルス
感染していた報告がきた

対応を議論してください

補足

メンテナンス会社への発
注は現場担当が実施
現場担当が指揮する

求める行動

対応を議論し、本シナリオ
との因果関係を疑う

振り返りポイント

自社との因果関係を疑い、
詳細を確認したか。

メンテナンス時のウイルス
チェック方法に問題が無かつ
たか確認できたか。

加減点

- ・因果関係を疑う：＋１０点
- ・チェック方法を確認する：＋１０点
- ・放置してしまった：－１０点

イベント
②



工場の端末がランサムウェアに感染し、身代金要求画面が表示された

対応を議論してください

補足

感染した端末は現場担当者の業務用端末
CSIRTが指揮する

求める行動

対応方針の結論を出す

振り返りポイント

ランサムウェア感染による身代金要求に関する対応を組織として判断することができたか。

支払いをすることの法的問題を議論できたか。

加点・減点

- ・組織として意思決定した：＋１０点
- ・法的問題を議論した：＋１０点
- ・対応を議論せず放置：－１０点