サイバー攻撃発生時の経営者報告テンプレート　例

サイバー攻撃の発生時に、第一報・続報・最終報で共通して使う記入様式です。不明な欄は空けずに「確認中」と書き、確度欄で確認済みか推定かに印を付けます。

1. 報告の基本情報

項目	記入欄
報告区分	第一報/第〇報(続報)/最終報
報告日時	〇月〇日〇時〇分時点
事案名・管理番号	
報告先	(例:社長、対策本部長)
報告者(部署・氏名・連絡先)	

2. 経営判断を求める事項

現場の推奨案を必ず添え、承認か変更かを判断できるようにします。

No.	判断事項	現場の推奨案と理由	代替案	判断期限
①	(例:ネットワーク遮断の継続)	(例:継続。理由=感染拡大の防止)	(例:一部業務のみ再開)	
②	(例:顧客・取引先への通知)			
③				

3. 報告項目

No.	報告項目	記入欄	確度
1	事案の概要	検知日時: 検知経緯: 攻撃の種類(例:ランサムウェア):	□確認済み □推定 □確認中
2	業務・システムへの影響	停止・低下中の業務: 影響システム・拠点:	□確認済み □推定 □確認中
3	情報への影響	漏えい・改ざん・暗号化の有無: 情報の項目: 件数:	□確認済み □推定 □確認中
4	顧客・取引先への影響	二次被害のおそれ: 影響する顧客・取引先:	□確認済み □推定 □確認中

No.	報告項目	記入欄	確度
5	原因・侵入経路	判明している範囲:	□確認済み □推定 □確認中
6	実施済みの対応と現状	封じ込め・遮断: 調査: 外部専門家への依頼:	
7	今後の対応方針(現場案)	次回報告までに進める対応: 理由: 必要な資源・支援:	
8	復旧の見通し	目標復旧時間: 現時点の見通し:	□確認済み □推定 □確認中
9	財務・事業への影響見込み	売上・費用への影響: 事業継続上の懸念:	□確認済み □推定 □確認中
10	外部報告・公表の要否と期限	個人情報保護委員会: 警察: 所管省庁: 適時開示: 公表:	
11	再発防止策	(最終報で記入)	
12	次回報告予定	○月○日○時	

本資料は AI を活用して作成した情報を含んでおります。内容の正確性、完全性、最新性については十分に確認しておりますが、その全てを保証するものではありません。本資料の利用により生じたいかなる損害についても、作成者および配布者は責任を負いかねます。ご利用にあたっては、利用者ご自身の判断と責任においてご活用ください。