Building a better working world

サイバーインシデント経営層向け訓練サービス

EYストラテジー・アンド・コンサルティング株式会社

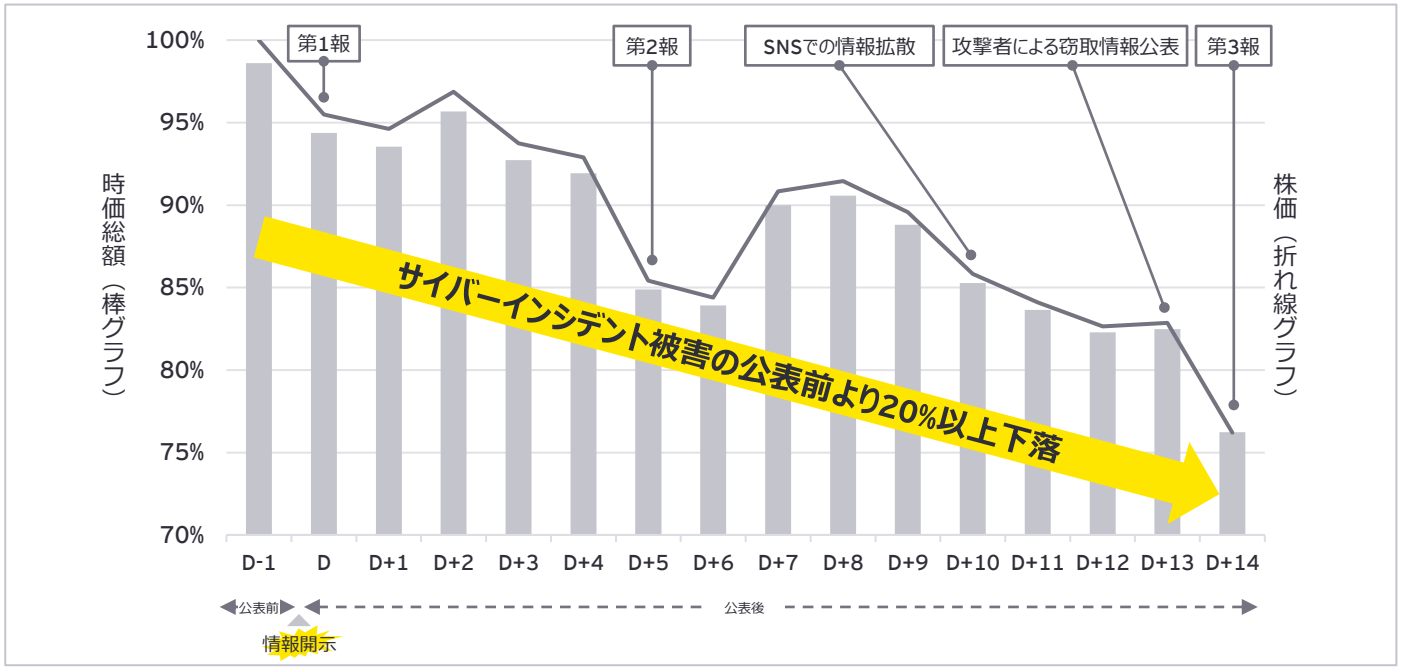
背景

近年、ランサムウェアによる業務停止・情報流出被害が頻発するなど、サイバー攻撃による被害が深刻化しています。

また、各国プライバシー規制等の強化に伴い、個人情報流出（恐れも含む）の発生時に、規制当局への報告も含め、迅速かつ適切に対応できなかった場合、企業の信頼が失墜するだけでなく、高額な制裁金を科される可能性もあります。

実際に起きた事例として、サイバーインシデントが発生し、世間に公表してから2週間で株価は約20%下落し、時価総額においては1,000億円を超える損失となった企業も存在します。

サイバーインシデント被害公表前後におけるX社の株価および時価総額の推移（実在の企業とは異なります）



想定される経営判断ポイント

前述の事例を取ると、公表された発生事象の内容から内部で実際になされたであろう経営判断のポイントを推測すると、各対応のタイミングや各評価結果の妥当性、対応内容の適切さ等、振り返るべきポイントは、公表された限られた情報からでも多岐にわたることが想定されます。

	発生事象の概要（一部フェイクを入れています）	経営判断の妥当性を振り返るべきポイント（想定）
第1報	▸ 不正アクセスを受け複数サービスが利用できないことを公表 ▸ 影響拡大防止およびデータ保全のため、データセンター内のサーバーをシャットダウン	▸ 初動対応のタイミング、内容は適切だったか? ▸ シャットダウンによる業務影響の評価は適切だったか? ▸ 公表のタイミング、内容は適切だったか?
第2報	▸ 障害がランサムウェアを含む大規模サイバー攻撃によるもので、さらに広範囲に影響が及んでいることを公表 ▸ 顧客に対するおわび動画を公開	▸ 原因究明のための調査は適切だったか? ▸ 公表のタイミング、内容は適切だったか? ▸ 関係各所への報告タイミング、内容は適切だったか?
SNSでの情報拡散	▸ SNSで真偽不明のX社に対するネガティブ情報が拡散 ▸ SNSでの拡散内容に対して明確に否定	▸ SNSでの情報拡散に対する危機管理はできていたか? ▸ 情報拡散後のSNSへの対応は適切だったか?
攻撃者による窃取情報公表	▸ 攻撃者により、窃取された情報の一部が公表 ▸ 従業員の個人情報や機密書類等が世間に流出	▸ 攻撃者に対する対応は適切だったか? ▸ 情報漏えい有無の調査は適切に行われていたか?
第3報	▸ 情報漏えいの事実が確認されたことを公表 ▸ 経営層が株を大量に売却したという虚偽情報が拡散	▸ 公表のタイミング、内容は適切だったか? ▸ 虚偽情報への対応は適切だったか?

EYができること

EYはサイバーセキュリティ領域に関する数十年の経験を持つ熟練の専門家を擁しています。EYのサイバーセキュリティ専門家が、「クライアントの業務特性を考慮したリアリティーのあるサイバーインシデントシナリオ作成」、「プロフェッショナルファームとしての高品質なファシリテーション」、「数十年の経験によって培われたサイバーセキュリティ専門家としての納得感のあるフィードバック」を行う、クライアント経営層向けのサイバーインシデント訓練を提供します。

サイバーセキュリティ共同リーダー／EY Japan金融サービス　パートナー

EYストラテジー・アンド・コンサルティング株式会社

小川 真毅 *Masaki Ogawa*

▸ **主な経歴**

外資系IT企業を経て、EYストラテジー・アンド・コンサルティング株式会社に入社。金融機関向けサイバーセキュリティアドバイザリーチームをリード。

前職では執行役員として、コンサルティング、SI、マネージドサービス、インシデントレスポンス、レッドチームなどセキュリティ事業全般を統括。

複数の外資系IT企業や、会計監査系ファームにて、サイバーセキュリティ事業や組織の立ち上げをリード。

キャリアにおいては24年以上、一貫してサイバーセキュリティ分野に従事し、業界団体への参画や、セミナー・イベントでの講演、記事の執筆など多数。

▸ **主な実績**

- グローバルセキュリティガバナンス体制構築
- グローバルセキュリティ監視インフラおよびCSIRT整備
- サイバーフュージョンセンター構築および運営
- 金融機関向けセキュリティソリューション導入（EDR / XDR / FW / IDS / IPS / WAF / SASE / DLP / IAM / SIEM / SOAR / ASM）

▸ **学歴／資格／業界団体参画**

- CISSP / CISA / CISM / CBCI / PMP
- 経営学修士（MBA）
- 日本サイバー犯罪対策センター（JC3）元幹事
- 日本セキュリティ監査協会（JASA）元理事

アプローチ

インシデント訓練の流れとして、シナリオ検討からスタートし、開催準備、訓練実施、事後振り返りを含めて4つのSTEPで進めます。

サイバーインシデント訓練のアプローチ		EYの想定作業内容	
1 シナリオ検討	▸ 開催する訓練の目的を定義し、参加者を選定 ▸ 訓練の目的に則し、近年のサイバー攻撃に類似する事例等を調査し、訓練シナリオを検討	シナリオ検討	▸ 訓練の目的を定義し、昨今のサイバー攻撃事例等を考慮したシナリオ案を検討
2 開催準備	▸ 訓練実施に向けた対象者への参加依頼や、当日のタイムスケジュール等を検討 ▸ 検討したタイムスケジュール、訓練シナリオ等を踏まえたコンテンツ資料を作成	タイムテーブル検討	▸ 訓練時間と参加人数を考慮し、質疑応答、ワークショップ等を含めた訓練実施における当日のタイムテーブルを検討
		参加者への質問事項検討	▸ 訓練において参加者に体験してもらう重要な経営判断が必要となる質問事項を検討
		当日資料作成	▸ 訓練当日に画面投影するコンテンツを作成
		事後アンケート検討	▸ 訓練実施後に参加者に記入を依頼するアンケート内容を検討
3 訓練実施	▸ オンサイト、オフサイト等クライアントのご要望に応じた開催型式にて、数十年の経験を持つEYのサイバーセキュリティ専門家が複数名で訓練を実施	簡易リハーサル	▸ 実際に訓練を実施する会場を下見し、設備や立ち位置等チェックするとともに、当日の流れを関係者で確認
		訓練参加	▸ 事前に準備した資料等を用いて訓練を実施
4 事後振り返り	▸ 開催した訓練に関するアンケートを参加者から取得 ▸ アンケート結果や、訓練実施結果から導出される助言・提言を含めた総括報告書を作成	総括報告書作成	▸ 訓練結果に対して、貴社規定類との整合性や、参加者のアンケート結果を踏まえた専門家として総括となる報告書を作成

EY Japan Forensics フォレンジック・テクノロジーリーダー／サイバー・アシュアランスリーダー

EY新日本有限責任監査法人　プリンシパル

杉山 一郎 *Ichiro Sugiyama*

▸ **主な経歴**

国内大手セキュリティ会社を経て、EY新日本有限責任監査法人に入社、ForensicsのTechnology部門のリーダーとして、サイバーセキュリティやデジタルフォレンジック関連業務（eDiscovery等）に従事。また、サイバー・アシュアランスリーダーとして、会計監査におけるサイバーセキュリティのリスク評価等の支援業務も行う。

日本国内のフォレンジック黎明（れいめい）期からフォレンジック業務に従事し、これまでに「日本の特定産業を標的としたサイバー攻撃」「過労死認定に係る労務状況調査」等、数多くの調査事案に対応した経験を有する。

デジタルフォレンジックの研修プログラムを独自に開発し、法執行機関に提供しており、これまでに法執行機関の調査員延べ1,000人以上の研修に当たる。

NPO法人　デジタル・フォレンジック研究会が発刊する、証拠保全ガイドラインの初版からWGメンバーとして参加するなど、デジタルフォレンジックの啓発活動やenPit-Proなどセキュリティ人材育成の活動にも積極的に関与。

▸ **学歴／資格／業界団体参画**

- GIAC認定資格 4種保有
  - GIAC Certified Forensic Analyst、
  - GIAC Certified Forensic Examiner、
  - GIAC Network Forensic Analyst、
  - GIAC Advanced Smartphone Forensics Certification
- GIAC Advisory Boardメンバー
- デジタル・フォレンジック・プロフェッショナル認定実務者資格（CDFP-P）
- 主な著書：『サイバーセキュリティ対応の企業実務』（2023年、中央経済社）等

作成物イメージ

▸ タイムテーブル

オンサイト、オフサイト等の開催場所や、想定訓練時間等のクライアントのご要望に応じた開催型式に沿って、タイムテーブルをオーダーメードいたします

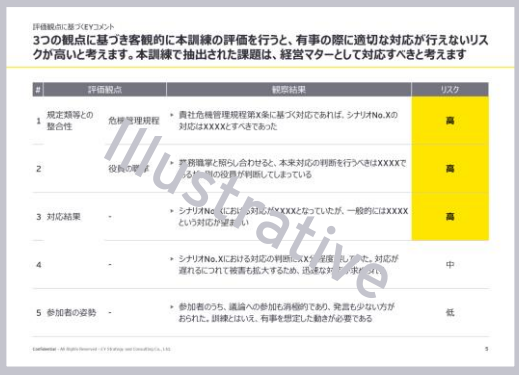
#	時間（目安）	内容	担当		概要
			クライアント	EY	
1	1分	訓練開始のごあいさつ	✓		▸ 司会、進行に関するごあいさつ
2	4分	訓練の意義、昨年度の振り返り	✓		▸ 訓練の意義や目的についてのごあいさつ
3	4分	訓練の進行説明、注意事項		✓	▸ ファシリテーター自己紹介を含め、訓練の進行、注意事項などを説明
4	2分	シナリオA：状況付与1		✓	▸ シナリオAに関するクライアントにおけるサイバーインシデント被害状況の説明および質問
5	20分	経営判断の検討および検討結果の発表1	✓		▸ 質問に対するグループディスカッションを行い、経営判断の結果および判断の経緯を発表
6	3分	ファシリテーターのフィードバック1		✓	▸ 発表内容に対する専門家の視点を交えたフィードバック1
7	2分	シナリオA：状況付与2		✓	▸ シナリオAに関するサイバーインシデント被害状況の変化の説明および質問
8	20分	経営判断の検討および検討結果の発表2	✓		▸ 質問に対するグループディスカッションを行い、経営判断の結果および判断の経緯を発表
9	3分	ファシリテーターのフィードバック2		✓	▸ 発表内容に対する専門家の視点を交えたフィードバックおよびシナリオAの締めの言葉
10	2分	シナリオB：状況付与1		✓	▸ シナリオBに関するクライアントにおけるサイバーインシデント被害状況の説明および質問
11	20分	経営判断の検討および検討結果の発表1	✓		▸ 質問に対するグループディスカッションを行い、経営判断の結果および判断の経緯を発表
12	3分	ファシリテーターのフィードバック1		✓	▸ 発表内容に対する専門家の視点を交えたフィードバック1
13	2分	シナリオA：状況付与2		✓	▸ シナリオBに関するサイバーインシデント被害状況の変化の説明および質問

▸ 経営層向け訓練投影資料

当日のタイムテーブルに沿って実施するシナリオや質問事項等のコンテンツ内容を記載します。さらに、一部音声やアニメーションを設定し、訓練の臨場感を醸成します

▸ 総括報告書

訓練実施において観察されたサイバーインシデント対応における疑似対応結果について、有事のベストプラクティスや貴社規定類との整合性等の観点を用いた評価結果を記載します



問い合わせ先

EYストラテジー・アンド・コンサルティング株式会社

お問い合わせはこちらよりお願いいたします。

ey.com/ja_jp/connect-with-us/consulting