サイバーセキュリティ演習・フォローアップヒアリング

サイバーセキュリティ演習・フォローアップヒアリング

サイバーセキュリティ演習結果概要

サイバーセキュリティ演習概要

- 日程：【A群】9月24日、【B群】10月23日、24日
- 時間：10：00～17：00(休憩含)
- 場所：TKPガーデンシティPremium名古屋新幹線口
- 内容：【午前】講習(座学式)、【午後】演習(設問回答式)
- 講師：デロイトトーマツサイバー合同会社　手柴
- 参加社数(全体)：参加63社、不参加113社

(1)設問正答率

インシデントレスポンスに係る設問に関して、各シナリオの正答率は80%前後となった。

(2)演習アンケート結果

全体において「インシデントが発生した場合、適切に対処できる/ある程度対処できる」と回答した割合が85%を超えた。

(3)参加者の声

今後の取り組みや課題認識として、最も挙げられたトピックが「情報セキュリティルール作成(インシデント対応等)」であり、次点で「技術的対策(ADサーバー導入、バックアップの実施等)」であった。

サイバーセキュリティ演習・フォローアップヒアリング

フォローアップヒアリング結果概要

フォローアップヒアリング概要

- 実施時期：10月17日～11月7日
- 対象：演習参加社のうち6社(ランダムに選考し連絡実施)
- ヒアリング実施者：デロイトトーマツサイバー合同会社
- 内容：
  - 現状と課題認識
  - 事業に係る意見・要望等

フォローアップヒアリング結果サマリ

- 現状の課題認識では、情報セキュリティに係るリソース不足、経営層の理解度不足、セキュリティレベルに係るベースラインの必要性等、様々な課題が存在することが分かった。
- 事業に係る意見として、規模や業態の実態に即したサービス提供の必要性が高いことが分かった。

サイバーセキュリティ演習・フォローアップヒアリング

サイバーセキュリティ演習概要

- 9月24日に初回のサイバー演習を実施し、A群企業様にご参加頂きました。
- 10月23、24日にB群企業様、および一部A群企業様向けの演習を実施しました。
- 参加企業数については、下記表の通りです。

グループ	日程	参加企業
A群向け演習	9月24日（火）10:00-17:00	参加：6社、不参加：9社
B群向け演習	10月23日（水）10:00-17:00 10月24日（木）10:00-17:00	参加：57社、不参加：104社 ※A群再調整9社含む

サイバーセキュリティ演習・フォローアップヒアリング

サイバーセキュリティ演習結果 (1)設問正答率

- 午前中にサイバーセキュリティ基礎講習を実施し、午後に架空企業のシステム担当者という設定で3つの攻撃シナリオについて演習を実施しました。
- 攻撃シナリオ毎の参加者全体の平均正答率は以下の通りです。

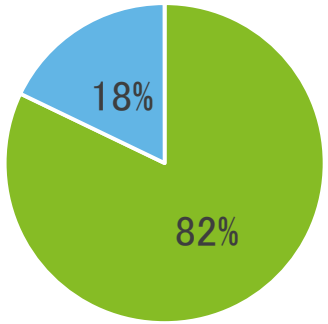
グループ	攻撃シナリオ① 設問数11	攻撃シナリオ② 設問数7	攻撃シナリオ③ 設問数5
A群(n=6)	82%	86%	83%
B群(n=55)	78%	85%	75%
全体平均(n=61)	80%	87%	77%

サイバーセキュリティ演習・フォローアップヒアリング

サイバーセキュリティ演習結果　(2)アンケート結果サマリ(1/3)

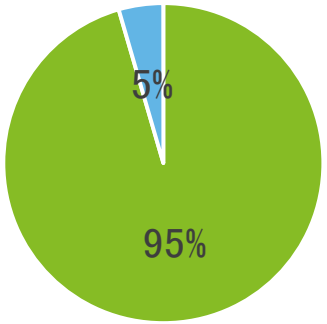
アンケート結果サマリ（n=61）

1 演習の実施時間は適切でしたか？



- 適切だった・ある程度的適切だった
- 適切ではなかった

2 演習の難易度は適切でしたか？



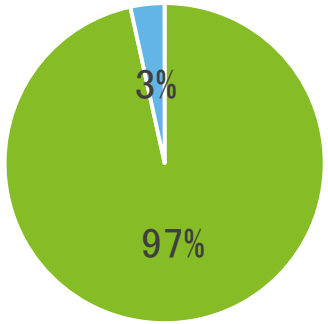
- 適切だった・ある程度適切だった
- 適切ではなかった

サイバーセキュリティ演習・フォローアップヒアリング

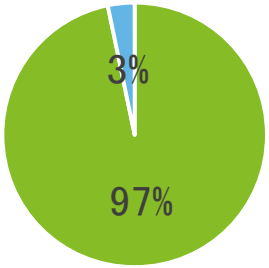
サイバーセキュリティ演習結果　(2)アンケート結果サマリ(2/3)

アンケート結果サマリ（n=61）

3 時間配分や進行は適切でしたか？



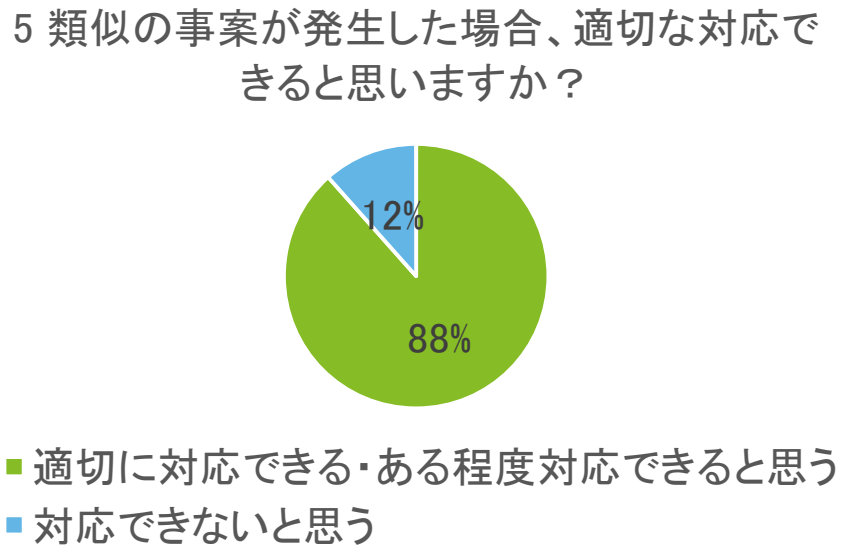
4 インシデント対応時の全体の流れを理解できましたか？



サイバーセキュリティ演習・フォローアップヒアリング

サイバーセキュリティ演習結果 (2)アンケート結果サマリ(3/3)

アンケート結果サマリ（n=61）



サイバーセキュリティ演習・フォローアップヒアリング

サイバーセキュリティ演習結果 (3)参加者の声

参加者の声(一部抜粋)

■ **9月参加者**

- ✓ 冷静な判断を行う必要があると感じた
- ✓ ウィルス等の危険性について、上層部含め、認識不足、整備不足であるため、会社全体で対策をしていかなければいけないと思った
- ✓ 社内での注意喚起、教育が課題と感じた
- ✓ ネットワーク以外の媒体でデータのバックアップを取っておきたいと思った
- ✓ 現在、個人情報の取り扱いについて、誰でも外部に持ち出せる状況になっている点を改善していきたい
- ✓ 専門家、ベンダーとの連携を強化していきたいと思った　等

■ **10月参加者**

- ✓ 現在、アクセス権限の整理があいまいになっているため、再構成しなければならないと感じた
- ✓ 経営者がサイバーセキュリティリスクを軽視しているのでいかに参加させるのかが課題であると思った
- ✓ サイバーインシデントに対する自社の準備ができていないことを痛感した
- ✓ ADサーバ、PCログ収集解析ツールを導入したい
- ✓ 取組体制を見直したいと思う
- ✓ 社内のルール作り、勉強の実施が必要と感じた　等

サイバーセキュリティ演習・フォローアップヒアリング

フォローアップヒアリング結果サマリ(1/3)

■セキュリティ対策の現状と課題認識の傾向(1/2)

大分類	中分類	現状	課題認識
組織/人	現状のセキュリティ体制	• セキュリティ/IT担当者は一人のみまたは少数である。	• セキュリティ/ITの知見を持ったリソースが存在せず、新たに雇用する予算的余裕がない。 • セキュリティ対策の持続可能性が低い。(担当者が高齢化しており、後継者がいない)
	経営層の関与・理解度	• 経営層が予算承認等で関与はするが、セキュリティ/ITに係る理解度は低い。	• 必要な対策について、経営層が判断できない。 • 経営層に対して説明する側の理解度が低いため、訴求力が低い。
ルール/プロセス	セキュリティポリシー/規程の策定状況	• ポリシーは存在するが、文書化された規程は存在しない。	• どの程度の規程を作成する必要があるのか判断できない。 • 規程の展開が行き届かない。 • 規程の運用(改訂)に係るリソースが十分ではない。
	インシデント発生時の対応	• インシデント対応の手順は存在せず、対応が場当たり的になっている。	• 対応手順が定められていない。 • ベンダー相談ができない部分の判断ができない。 • スピーディな対応ができない場合がある。

サイバーセキュリティ演習・フォローアップヒアリング

フォローアップヒアリング結果サマリ(2/3)

■セキュリティ対策の現状と課題認識の傾向(2/2)

大分類	中分類	現状	課題認識
技術	講じている技術的対策	• アンチウイルスソフトは導入されている。 • 従業員のPCログインは管理されていない。	• PC/サーバーのアップデートができない。 • バックアップ媒体が破損したとき、データが消失する可能性がある。 • 社内のネットワークが把握できていない。
	セキュリティ監視状況	• 日常的な監視は行っていない。	• 監視を行えるリソースが存在しない。 • ネットワーク構成を把握できていないため、UTMの導入ができない。

サイバーセキュリティ演習・フォローアップヒアリング

フォローアップヒアリング結果サマリ(3/3)

■実証事業に係る意見・要望等

ロコールセンター/お助け隊に対する意見・要望等

- お助け隊は24時間365日の対応ができ、スピーディ(1時間以内)な対応が可能であれば望ましい。
- お助け隊が安価で利用可能であれば望ましい。
- コールセンターに問い合わせ可能な内容を明確に周知してほしい。
- コールセンター側で個社の状況を把握した方に問い合わせ可能であれば助かる。
- コールセンターにはベンダーに相談できない内容を相談できれば助かる。

ロその他情報セキュリティ全般に係る事項

- 最低限このレベルまで対策を講じるべき、という基準が欲しい。
- 個社の状況を把握したうえで、第三者視点でアドバイスを提供できる外部専門家は助かる。(IPAの支援士派遣サービス)
- 定期的な情報収集の場として、セミナー/ワーキンググループがあれば助かる。