導入事例

内閣サイバーセキュリティセンター

各府省庁等の組織強靭化を推進！ 各府省庁等のCSIRT要員にクラウド型訓練サービス基盤「NetQuest Platform」で情報セキュリティインシデント訓練を実施

NISC 内閣サイバーセキュリティセンター

内閣サイバーセキュリティセンター（NISC）では、毎年行っている各府省庁等のCSIRT要員の情報セキュリティインシデント対処能力評価において、アライドテレシスのクラウド型訓練サービス基盤「NetQuest Platform」を採用した。本基盤を利用して、各府省庁等のCSIRT要員にインシデント対処訓練を一斉実施。従来よりも運用の工数を抑え、多くの組織に対して同一の状況を付与でき、一連のインシデント対処について経験できたとNISC担当者は評価している。

課 題

- メールによる従来型の訓練方式は時間がかかり相応の工数が発生

採用ポイント

- 多くの組織を対象とした一斉訓練が可能
- 採点や評価報告書の作成等の自動化による効率性

効 果

- 多くの組織を対象にした訓練を工数を抑えて実現
- 一連のインシデント対処を経験

各府省庁等のCSIRT要員における セキュリティインシデント対処能力評価

サイバー攻撃がますます複雑・巧妙化する中、複数の政府機関を同時に狙うサイバー攻撃の発生も考えられる状況だ。

セキュリティインシデントを認知し、初動対処、被害拡大防止、早期復旧等に取り組むにあたっては、「CISO（Chief Information Security Officer、最高セキュリティ責任者）等の幹部職員を含む府省庁等の関係者への報告や連絡等を適時・適切に行い、幹部職員の指揮のもと、組織として適切に対処することが重要であると考えています」と、内閣サイバーセキュリティセンター（NISC）政府機関総合対策グループの担当者は語る。

NISCは、日々高度化や巧妙化するサイバー攻撃に対処できるようにするため、サイバーセキュリティ基本法第26条第1項第2号「国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。」を踏まえて、各府省庁等に設置されているCSIRTを対象に行うインシデント発生を模した対処訓練を毎年主催している。毎年訓練テーマを変更し、新しいテーマについても基礎的な内容を設定して足場を固めるようにするだけでなく、技術知識を必要とする内容も設定して難易度にも幅を持たせている。

従来のセキュリティインシデント訓練の課題

従来の訓練は、NISCと各府省庁等のCSIRT間でメールのやり取りを行う形式で、NISCからインシデント状況を付与し、各府省庁等のCSIRTが対処アクションをメールで回答する、という形式を取っていた。

手書きベースのため、やり取りに相応の工数がかかるほか、訓練実施後の報告書の作成や、それを基にしたフィードバックがあり、これも組織数によって相応の工数がかかるものであった。

また、個別組織に対して訓練をするのであれば、当該組織のシステム構成や内部規程等に基づく手順に沿って訓練シナリオや評価をすることができるが、多数の組織を対象に一斉に訓練をする場合、ある程度、一定の仮想組織、システム構成および手順で実施しなければならない。その結果、すべての組織に合致した訓練にはならないことや、当該訓練結果の評価がすべての組織の実際の評価と合致するわけではないことが課題であるという。

各府省庁等で「NetQuest」を使った 演習訓練を実施

アライドテレシスは今回の調達に対し、クラウド型情報インシデント訓練サービス基盤「NetQuest Platform（以下、NetQuest）」を使用した演習を提案。入札の結果アライドテレシスが受注し、NISCとともに各府省庁等に対して演習を実施した。

NetQuestは、従来の集合型インシデント対応演習と異なりクラウド型の訓練サービスだ。会場設営や進行役のファシリテータアサイン、特別な訓練設備、準備作業などが不要で、運営側の工数・コストを削減でき、またNetQuestにログインすれば訓練が実施できるため訓練受講者の工数・コストも削減できる。

NetQuestでは、組織のコミュニケーション・エスカレーションの強化を図り、サイバー攻撃被害に迅速かつ効果的に対応するための意思決定フローの訓練が実施される。この訓練はクラウド上で提供されるため、複数拠点が同時に参加することができ、現実に近いインシデント対処のコミュニケーションを経験することができる。さらに演習の結果はレーダーチャートで評価される。また訓練前後のアンケートを用いた組織の成熟度をチェックすることができる。技術面の問題把握だけでなく、関連部署との連携フローの仕組みが確立されているか等、組織のインシデント対処の指示能力を測る事が可能だ。

そしてもう1つユニークな特長が、このNetQuestがSaaS（Software as a Service）として提供されている点だ。今回の案件ではとくに、NetQuestを利用した訓練により訓練実施体制の人員規模の増大を防ぎ、また採点や評価報告書の作成等の自動化よって効率化を図り、工数やコストを削減することができた。

NetQuestを使ったことによるメリットと今後の展望

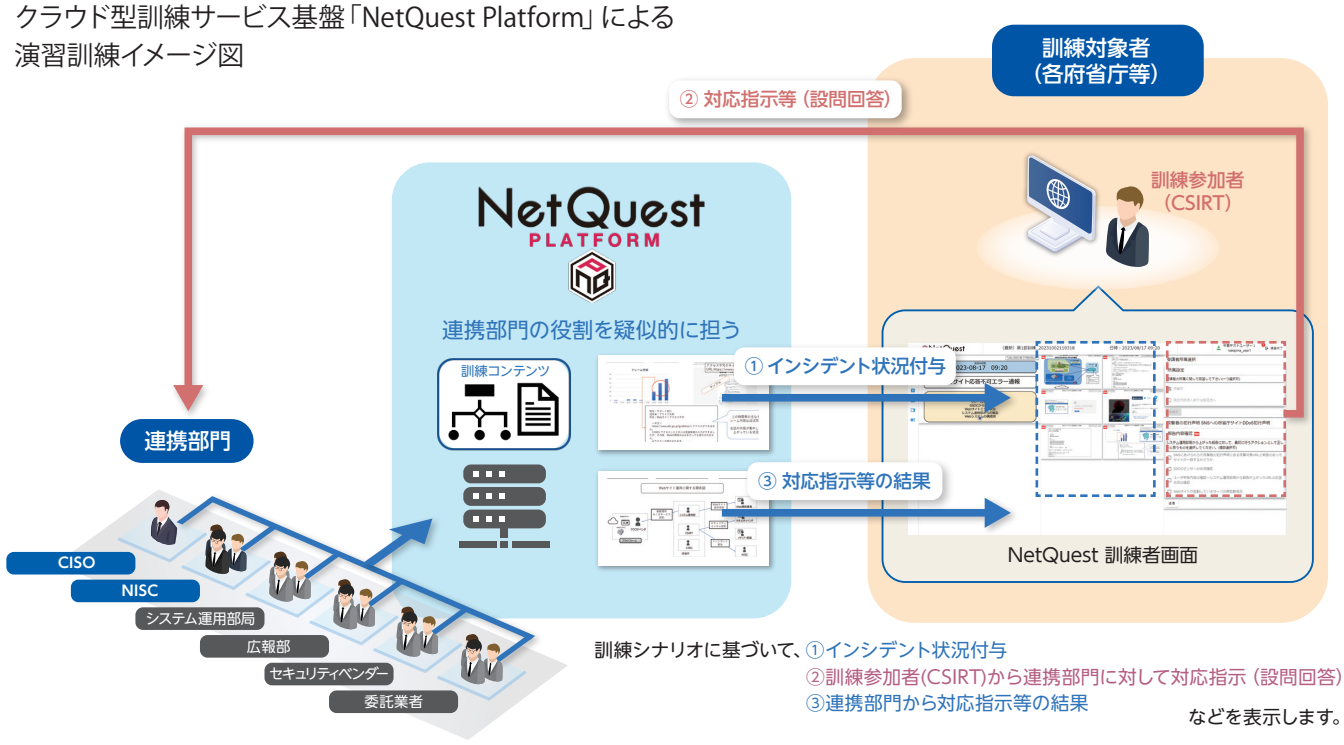
実際にNetQuestを使った演習を実施して、NISCの担当者は、従来と同様に遠隔でインシデント訓練を十分実施できたことを評価し、良かった点として、「多くの組織に対して同一の状況を付与でき、一連のインシデント対処について経験できた点である」と語った。

また、シナリオについても、丁寧な進行で、取り残される者を出さず進められたことを評価している。一部の訓練参加組織において解答を送信したもののサーバー上で登録されていない事態もあったが、アクシデントが生じた原因について速やかに確認し、訓練継続を可能とするための適切な対処を行った。また閲覧用アカウントの追加要望にも速やかに対応したこともあわせ、アライドテレシスの対応を評価している。

従来の訓練と比べると「状況付与とタイムラインが全ての組織で同一であるため、多くの組織を対象に訓練できた点が一番の効果」（NISC担当者）と言い、その反面、選択肢式にしたため実際のインシデント対処における行動とは異なるものとなった点を今後検討すべき反省点として挙げている。

「各訓練参加組織が複数の回答候補の中からどのような理由で回答を絞り込んだか等、回答に至る過程をより深掘りできればよいと思いました。また、一連の訓練を通して認知した課題に対しては、民間企業も含めてどのような対応を取っているか検討し、実態に沿うよう改善していきます」と今後の展望を語った。

クラウド型訓練サービス基盤「NetQuest Platform」による演習訓練イメージ図



訓練シナリオに基づいて、①インシデント状況付与
②訓練参加者(CSIRT)から連携部門に対して対応指示（設問回答）
③連携部門から対応指示等の結果
などを表示します。

お客様プロフィール

■内閣サイバーセキュリティセンター（NISC）

所 在 地 ： 東京都千代田区永田町2-4-12

サイバーセキュリティ基本法に基づき2015年1月、内閣にサイバーセキュリティ戦略本部が設置され、同時に内閣官房に内閣サイバーセキュリティセンターが設置された。サイバーセキュリティ戦略本部の事務局としての役割のほか、行政各部の情報システムに対する不正な活動の監視・分析やサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助、監査等を行うとともに、サイバーセキュリティの確保に関する総合調整役を担う。

https://www.nisc.go.jp/

ネットワーク構築などのご質問やご相談、その他のお問い合わせ

https://www.allied-telesis.co.jp/contact/

アライドテレシス株式会社 〒141-0031 東京都品川区西五反田7-21-11 第2TOCビル https://www.allied-telesis.co.jp/