セキュリティ対策

事例集

セキュリティ対策事例一覧

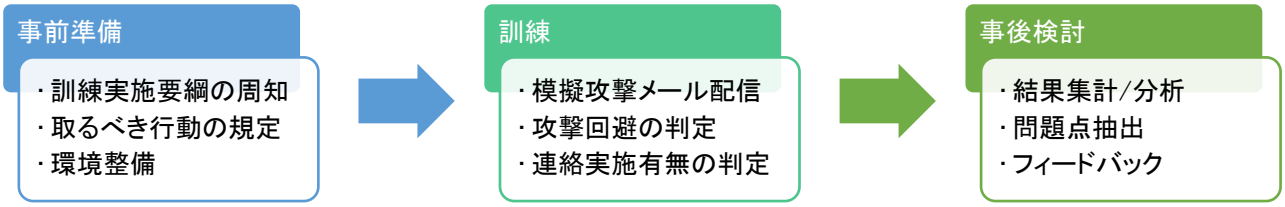
No.	事例	対応するガイドライン
1	標的型メール攻撃の対策訓練	1.4.1 サイバーセキュリティ経営 4.3 インシデント対応
2	マルウェア対策製品導入不可端末へのセキュリティ対策	3.3.1 マルウェア対策ソフトウェア
3	取引先と連携したセキュリティ	1.4.1 サイバーセキュリティ経営

事例 No.1　　標的型メール攻撃の対策訓練

A 社では、標的型メール攻撃への対策として、標的型メール攻撃を模擬したメールを全従業員に送付し、正しく対処できるかどうかの訓練を実施している。

この種の訓練では、主に、攻撃を受けた本人が攻撃を回避できるか（例えば、偽装された添付ファイルを開くことがないか）を判定するものである。しかし、攻撃回避を判定するのみでは、訓練の効果が限定的となってしまう。

訓練においては、事前準備や事後検討も重要になる。事前準備としては、標的型メール攻撃を受けた際の取るべき行動を規定するとともに、取るべき行動を行いやすいように環境を整えることが重要となる。また、訓練後には、訓練の結果を集計・分析して問題点の抽出し、フィードバックを行う必要がある。



実施内容

・標的型メール攻撃を受けた（疑わしいメールを受信した）場合や、攻撃を回避できなかった（ファイルを開いた）場合の取るべき行動を規定し、周知、教育した。

・セキュリティインシデント発生時に慌てぬよう、業務ポータルサイト等の社員が普段接する箇所に、連絡方法・連絡先を掲載した。

・標的型メール攻撃の模擬訓練において、攻撃回避の判定の他、連絡を正しく行うことまで含めて訓練を実施した。

・標的型メール攻撃の模擬訓練の結果を集計し、回避率が低い傾向の分析を行い、フィードバックを図った。

効果

・訓練を重ねるにつれ、標的型メール攻撃の回避率が向上する傾向が見られた。実際の標的型メール攻撃を受けたとしても、実被害が発生する可能性は低減されると考えられる。

・模擬訓練で、特定の職位のグループに回避率が低い傾向が見られた事があった。その理由を分析後、フィードバックすることにより効果的な訓練効果を得られた。

事例 No.2 マルウェア対策製品導入不可端末へのセキュリティ対策

B 社では、工場へのセキュリティ対策を推進していたが、オフライン端末やパフォーマンスへの懸念からマルウェア対策ソフトがインストールできない端末への対策を苦慮していた。

オフラインであっても USB メモリなどを経由しマルウェア感染することが有るが、オフラインのため定義ファイルなどの更新ができず対策がとれていなかった。オフライン端末の中にはサポート期限切れの OS を使用し続けている状況にもあった。

また、ネットワークへ接続はしているが、生産活動への影響が懸念される端末に対してもマルウェア対策製品導入ができないといった悩みもあり工場へのセキュリティ対策推進の課題となっていた。

そこで B 社はオフライン端末やマルウェア対策製品の導入が難しい端末へのセキュリティ対策として USB 型マルウェアチェック・駆除ツールを利用しセキュリティ対策を実施した。

実施内容

- オフライン端末やマルウェア対策製品導入不可端末を外部から検索する USB 型マルウェアチェック・駆除ツールを導入した。
- USB 型マルウェアチェック・駆除ツールによる検索を定期的に実施するよう運用ガイドラインを整備した。

効果

- オフライン端末やマルウェア対策製品導入不可端末であってもセキュリティ対策を実施することができるようになり、B 社の工場全体へのセキュリティ対策を適用することができるようになった。

事例 No.3　取引先と連携したセキュリティ

C 社では、取引先と一体となったセキュリティ対策の浸透や是正を推進し、サプライチェーン全体のセキュリティレベルの向上をはかっている。

取引先のセキュリティ対策状況により、セキュリティレベルを分類し、適切なレベルの取引先へ委託する仕組みを取り入れている。

取引先に求める対策は、大きく分類すると①契約管理、②再委託管理、③作業従事者の管理、④情報の管理、⑤技術対策の導入、⑥セキュリティ実装、⑦点検の実施 の 7 項である。

① 契約管理

自社(委託元)と取引先の間で、秘密保持義務などを含む会社間の基本契約を締結する。

② 再委託管理

取引先は、委託元から書面による事前承諾を得ない限り、第三者に再委託してはならない旨、基本契約で定める。また、再委託先確認書の提出を義務化して、プロジェクト毎の体制を明確化する。

③ 作業従事者の管理

自社から委託された業務に従事する作業者が守るべき対策について、自社に対し誓約してもらうことで対策実施を徹底する。

④ 情報の管理

業務で取り扱う秘密情報の管理について秘密指定の指針を定め、秘密表示、持ち出し管理、廃棄・返還の管理を定め、実施を徹底する。

⑤ 技術対策の導入

技術対策を必須の対策（可搬型電子機器や外部記憶媒体の全体暗号化など）と、推奨の対策（情報漏えい防止システムなど）の導入を依頼する。

⑥ セキュリティ実装

顧客向けの製品・システム・サービスの開発・運用について実施要領を定め、セキュリティを考慮した開発・運用の実施を依頼する。

⑦ 点検の実施

要求水準を定義した基準書に基づき、取引先の対策実施状況を点検し、適宜改善を指導する。また、サイバーセキュリティの情勢を踏まえ基準書をインシデント発生の備えたものへ改訂を行い、さらに取引先と連携した活動を強化する。

[出典] https://jpn.nec.com/sustainability/ja/pdf/isr2023j.pdf