経営層向け

事例で学ぶサイバーリスクマネジメント
～経営トップがすべきこと　実践編～

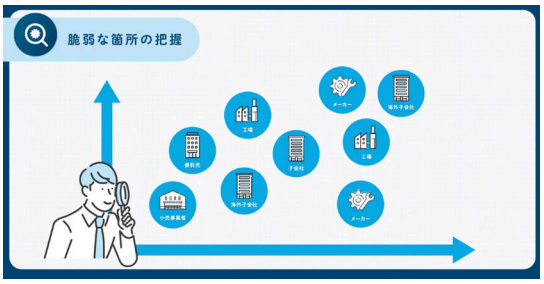
①自社だけでなく「事業」を守る：強靭なサプライチェーンの構築

近年、企業とそのサプライチェーンを狙ったサイバー攻撃の事例が増加しています。被害を防ぐためには、自社のみの対策ではなく、サプライチェーン全体でのセキュリティ向上に取り組むことが必要です。

自社のセキュリティ対策を万全にしたとしても、ネットワークで接続された委託先や子会社など、対策できていない部分から侵入される恐れがあります。サプライチェーン全体を俯瞰し、事業全体を守るための３つのポイントを紹介し、それぞれについて経営層が取るべきアクションを解説します。

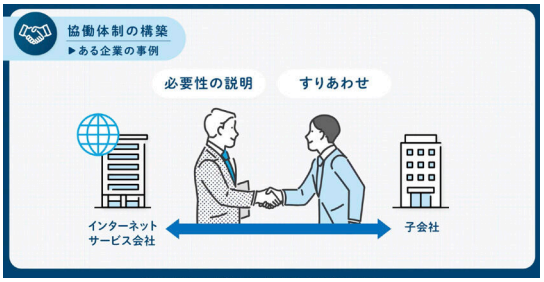
ポイント1 脆弱な箇所の把握

巨大化したサプライチェーン上の脆弱な箇所を効率的に把握するには、どうしたらよいのかの一例をご紹介します。ある企業では、事業の関連性（事業運営における関連度と機密性の高さ）とリスクの大きさ（サイバーセキュリティの対策状況や対応実績）から、自社の事業と関連性の高い企業を選び、優先度を付けて、順番に脆弱性評価をすることができました。
このように経営層の役割として、脆弱な箇所を効率的に把握するために、自社に最適なリスク評価の方法を検討し、それを整備することが挙げられます。



ポイント2 協働体制の構築

多くの場合、企業は人員や資金などのリソースが不足していることでセキュリティ対策に取り組むことができない、対策そのものに後ろ向きであるなどの事情を抱えています。経営層は、子会社や委託先の経営層と意見交換を行い、各社の事情を理解した上で、それに応じたサポートを行いましょう。一例として、公的なIT導入補助金を紹介する、特定のサイバーリスクへの対応を契約時の対応条項として盛り込むなどです。



ポイント3 緊急時への事前の備え

緊急時への事前の備えとして、子会社や委託先に対して、サポート整備や定期的なトレーニングを実施することが重要です。
ある大手製造業では、子会社や委託先の従業員に対して専用の問合せ窓口を設立したり、インシデント対応の合同訓練を実施するなどのサポートをすることでサプライチェーン全体の習熟度を向上させました。
その結果、あるサプライヤーがランサムウェアに感染した際も、被害の拡大防止策を迅速に行い、影響を局所化することができました。

より詳しい内容を動画で確認するには、QRコードまたは下記URLからアクセス
https://security-portal.nisc.go.jp/guidance/executives2/index.html

内閣サイバーセキュリティセンター(NISC)