製造関係団体　各位

商務情報政策局
令和２年１月31日(金)

昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い

今年に入り、三菱電機、NECが大規模なサイバー攻撃を受けていたことが明らかとなりました。いずれの事案についても、調査し得る限りにおいて、防衛装備品や電力関係などの機微情報が漏洩していないことは、確認済との報告を受けています。他方、不正アクセスにより、企業情報が流出した可能性がある事例が続いており、こうした状況を経済産業省として重く受け止めています。

サイバー攻撃の手法が高度化する中、攻撃を完全に防ぐことが難しいことは承知していますが、深刻な事態を防ぐためにも、各団体におかれては、機微情報を保有する企業に『サイバーセキュリティ経営ガイドライン Ver2.0』など（※）の周知徹底を改めてお願いします。その上で、これらの企業の経営者及びセキュリティ対策に従事する者におかれては、『サイバーセキュリティ経営ガイドライン Ver2.0』などの最新の攻撃手法やそれへの対策を理解の上、十分なセキュリティ対策が実施されていることを、今一度点検してください。

特に防衛・宇宙関連や重要インフラ事業者との取引を行っている企業におかれましては、点検の結果、サイバー攻撃による重要な情報の漏えい等の可能性があったものについては、2月14日までに経済産業省の下記連絡先まで報告をお願いいたします。その上で、機微情報を保有する企業全体でセキュリティ対策を高めていけるよう、攻撃側を利することのないよう検討した上で、適切な場合には、事案の公表をお願いいたします。

サイバー事案に対する社会的関心は非常に高く、これへの対応は、ステークホルダー等とのコミュニケーション等を間違えると会社の経営そのものに深刻な影響を与え得るという意味で経営問題そのものです。したがって、経営者の責任において、より広い視点から、関係機関への報告や対外公表などを含めて、リスクの適切な管理のためのマネジメントの確立とその適切な実施に努めていただきたくお願いします。

※セキュリティ対策時に参照する文書等の例

サイバーセキュリティ経営ガイドライン Ver2.0

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

標的型サイバー攻撃対策（(独)情報処理推進機構）

https://www.ipa.go.jp/security/ta/index.html

（本発表資料のお問合せ先）
商務情報政策局サイバーセキュリティ課長　奥家
担当者：尾﨑、津國、飯山
電話：03-3501-1511(内線　3964)
03-3501-1253(直通)
メール：itsec-public@meti.go.jp