令和４年３月１日

サイバーセキュリティ対策の強化について（注意喚起）

サイバー攻撃事案については、先日、国内の自動車部品メーカーが被害にあった旨を発表するなど、昨今の情勢を踏まえるとその発生リスクは高まっていると考えられます。組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、関係機関や取引先などサプライチェーン全体を俯瞰し、発生するリスクをコントロールしていただくとともに、国外拠点についても、国内の重要システム等へのサイバー攻撃への足掛かりになることがありますので、具体的な支援・指示によりサイバーセキュリティ対策を実施するようお願いいたします。

不審な動きを検知した場合は、下記岩手県警察担当者までご連絡をお願いいたします。

記

１　リスク低減のための措置

(1)　本人認証の強化
- パスワードが単純ではないか
- アクセス権限に問題はないか
- 多要素認証を利用しているか
- 不要なアカウントはないか

(2)　IoT機器を含む情報資産の保有状況の把握とプログラムの更新

特にVPN装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

(3)　不審メール対策の周知
- メールの添付ファイルを不用意に開かない
- URLを不用意にクリックしない
- 不審メールを受信した場合は、迅速に連絡・相談を行う

２　インシデントの早期検知

(1)　各種ログの確認

(2)　通信の監視及び分析

(3)　アクセス権の点検

３　インシデント発生時の適切な対処と回復

(1)　データが消失した場合や第三者により暗号化された場合等に備えて、データのバックアップを実施するほか、復旧手順を確認する。

(2)　インシデント発生時に備えて、インシデントを認知した際の対処手順、各種連絡先等を確認し、担当者や社内連絡体制を準備する。

岩手県警察本部警備部公安課
サイバー攻撃対策係
019-653-0110（代表）