注意喚起

サプライチェーンにおける サイバーセキュリティ対策の強化 について

２０２２年３月３１日
SC3 攻撃動向分析･対策WG

サイバー攻撃事案のリスクの高まりを踏まえ、政府から2月下旬以降、二度の注意喚起が行われていましたが、その後の状況も踏まえ、3月24日、経済産業省から改めてサイバーセキュリティ対策の強化について注意喚起が公表されました（総務省、警察庁、内閣官房内閣サイバーセキュリティセンター同時発表）。
国内の自動車部品メーカーから被害にあった旨の発表もなされているところ、中小企業、取引先等、サプライチェーン全体で今一度、適切なセキュリティ対策の実施が望まれます。

SC3 攻撃動向分析・対策WGでは、これら注意喚起を受けて実際に企業で実施された取組について、参考となる事例をご紹介します。

1．サイバーセキュリティ対策の強化について（注意喚起）

2．注意喚起を受け企業で実施された取組事例

（政府からの注意喚起）

- 経済産業省「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（2022年2月23日）」
  https://www.meti.go.jp/press/2021/02/20220221003/20220221003.html
- 経済産業省等７省庁「サイバーセキュリティ対策の強化について（2022年3月1日）」
  https://www.meti.go.jp/press/2021/03/20220301007/20220301007.html
- 経済産業省等４省庁「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（2022年3月24日）」
  https://www.meti.go.jp/press/2021/03/20220324008/20220324008.html

【政府発表】 3月1日経済産業省ニュースリリースより
同時発表：金融庁、総務省、厚生労働省、国土交通省、警察庁、内閣官房内閣サイバーセキュリティセンター（NISC）

1．サイバーセキュリティ対策の強化について（注意喚起）

- 昨今の情勢を踏まえると**サイバー攻撃事案の潜在的なリスクは高まっている。**
  （3月1日、国内の自動車部品メーカーから被害にあった旨の発表）
- 経営者のリーダーシップの下、中小企業、取引先等、**サプライチェーン全体で今一度、適切なセキュリティ対策を実施**するようにお願い（国外拠点も同様）。

＜行うべき対策の一例＞

1.リスク低減のための措置	➢ **パスワードが単純でないかの確認**、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、**本人認証を強化**する。 ➢ IoT 機器を含む**情報資産の保有状況を把握**する。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。 ➢ 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**、連絡・相談を迅速に行うこと等について、組織内に周知する。
2.インシデントの早期検知	➢ サーバ等における各種ログを確認する。 ➢ 通信の監視・分析やアクセスコントロールを再点検する。
3.インシデント発生時の適切な対処・回復	➢ データ消失等に備えて、**データのバックアップの実施及び復旧手順を確認**する。 ➢ 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を確認し、対外応答や社内連絡体制等を準備する。

✓ 実際に情報流出等の被害が発生していなかったとしても、**不審な動きを検知した場合**は、早期対処のために**速やかに所管省庁、セキュリティ関係機関に対して連絡、警察にも相談を。**

3月24日の経済産業省によるニュースリリースでは、中小企業においては、自社がサイバー攻撃による被害を受けた場合、その影響が自社にとどまらず、サプライチェーン全体の事業活動に及ぶ可能性があることを踏まえ、**「サイバーセキュリティお助け隊サービス」**の活用など、積極的なサイバーセキュリティ対策に取り組むことを推奨。

2．注意喚起を受け企業で実施された取組事例

- **注意喚起**を契機に、**これまでのセキュリティ対策の徹底**や、**特に注意を要する箇所の点検**を実施する等の取組を実施している企業の事例は以下のとおり。

取組例１　チェックリストを用いて関係企業先の取組状況を緊急確認

「サイバーセキュリティ対策の強化について注意喚起」（日本語、英語）を国内外の全グループ会社に周知、その上で各社の対応状況を確認した。さらには取引先企業300社に、注意喚起項目をアンケートツールでチェックリスト（Yes/No）にして送付、取組状況の緊急確認を実施した。

3月17日に発出した取引先へのレター
「サイバーリスクの高まりを背景とした自己点検の依頼」

セキュリティ対策及びデータ保護に関する点検依頼
「日本の約XXX社を対象とした自己点検の依頼」

経済産業省の通達を参考にしたチェック項目

2．注意喚起を受け企業で実施された取組事例（続き）

- **注意喚起**を契機に、**これまでのセキュリティ対策の徹底**や、**特に注意を要する箇所の点検**を実施する等の取組を実施している企業の事例は以下のとおり。

取組例２　普段から実施している対策の中で特に留意すべきポイントを点検

サイバー攻撃に対して、普段から実施している対策のうち、正面突破※1による攻撃への対処に加えて、人的対応、及びビジネス面の観点で留意すべきポイントを整理し、点検した。

正面突破による攻撃への対処の確認	• サプライチェーンとのネットワーク接続点の安全確認（IPSなどで不正通信の検知・ブロックできるようになっているか、未承認の接続ポイントはないか）。 • ネットワーク出口の機器の脆弱性が残っていないか。認証強度（不特定の第三者の接続を許可している場合には多要素認証）は十分か（リモート接続、VPN接続、クラウド接続を含む）。
人的対応に関する確認	• MS-Officeの文書を開く時、マクロ実行禁止になっているか、手動で自動起動に修正していないか。
ビジネス面の確認	• サプライチェーンの業務が停止した場合の代替手段は用意されているか。

※1 インターネット接続における脆弱性の悪用や認証の突破等による不正アクセス

取組例３　グループ全社への注意喚起とCSIRTによる対応手順を点検・確認

グループ全社へ政府発表「サイバーセキュリティ対策の強化について注意喚起」を受けて注意喚起を複数回実施した。また、セキュリティインシデント発生時のCSIRT対応手順が最新化されていることを確認した。