銀泉リスクマネジメントレポート

サイバー攻撃による
『事故が起きたら、どんな対応が必要になる？』

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。3月には、国内の自動車部品メーカーから被害にあった旨の発表がなされたように、サプライチェーンに迷惑をかけないためにも、サイバーリスク対策は喫緊の課題です。

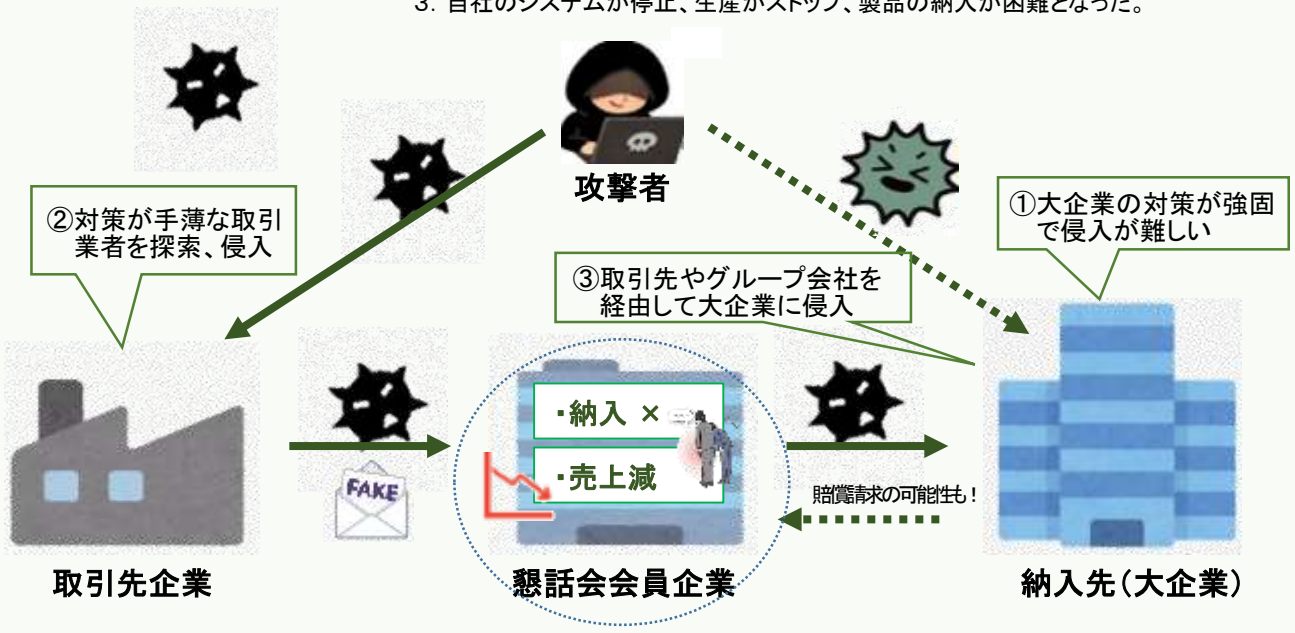
コロナ禍において、不要不急の外出を控えるため、多くの企業でテレワークが推進されるなど、企業のIT環境が大きく変化しています。それに伴い、急速に普及したテレワーク環境、それを利用する人間の隙を突くサイバー攻撃が増加していると考えれらます。まずは、最近の特徴的なサイバー攻撃を上げると次のようになります。

☆特徴的なサイバー攻撃
（1）コロナ禍に便乗したフィッシングメール
（2）テレワーク環境を狙った攻撃
（3）サプライチェーン攻撃
（4）ランサムウェアの多様化
（5）ウィルス対策ソフトを突破する攻撃

政府機関も、サイバー攻撃の脅威に対する認識を深めるとともに、対策の強化に努めていただきますよう注意喚起をしてします。
特に、左図の（3）サプライチェーン攻撃には、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう適切なセキュリティ対策が必要です。

サプライチェーン攻撃事例

1. 取引先企業の社員になりすまし、懇話会会員企業へウイルス感染したメールを送付。
2. 油断した懇話会会員企業の社員がメールを開封し、自社のシステムが感染。
3. 自社のシステムが停止、生産がストップ、製品の納入が困難となった。



サイバー攻撃で、営業が休止または阻害された影響で、 下記の被害想定できます。

賠償リスク
自社のシステムがサイバー攻撃を受けたことが原因で、取引先の業務を阻害し、取引先から損害賠償請求を受けるリスク
*取引先の事業停止による高額な利益損害の賠償請求を受ける可能性もあります。

利益リスク
サイバー攻撃でシステムダウンし、自社の営業が停止して喪失利益が生じるリスク

費用リスク
サイバー攻撃の原因や被害範囲の調査、ウイルス感染したサイトやサーバの閉鎖、ネットワークの遮断のために費用が生じるリスク

裏面で、事故が起きたら、どんな対応が必要か事例でご案内させていただきます。

●サイバー攻撃で情報漏えいを引き起こした際に具体的にどのような対応が発生するのか、企業がリリースする案内文をもとにご案内します。

2022年4月1日

お客様各位

弊社ＥＣサイトへのサイバー攻撃と情報漏えいのご案内

株式会社●●●●

今般弊社のＥＣサイト「×××」においてサイバー攻撃被害あり、1万件の個人情報漏えいのおそれがあることが判明しました。本日、被害の恐れのある方には書面によるご案内を発送いたしました。ご迷惑をおかけし申し訳ございません。

１．経緯
2022年3月15日、クレジットカード会社からの報告で情報漏えいの懸念がある旨が判明し、同サイトを閉鎖し、第三者調査機関による調査を行いました。その結果クレジットカード情報が不正利用された可能性があることが判明しました。

２．対応
同サイトについては既にインターネットから遮断しております。また、今後も不正利用が発生しないか専門機関に対してモニタリングを依頼しております。加えて調査結果をふまえセキュリティ対策強化による再発防止を図っております。

３．お問合せ先
本件に関するお問合せは以下までお願いいたします。
・株式会社●●●●お客様相談窓口
電話番号：0120-00-0000（平日9:00～18:00）

〈費用例〉

PR費用
お客様向けの連絡を行う際、その内容やタイミングなどについて専門業者に相談することが一般的です。（約300万円）

お詫び対応
お客様への案内状送付は不可欠です。
（100円×1万人＝約100万円）

サイト閉鎖費用
サイバー攻撃を受けたサイトやサーバーを閉鎖やネットワークから遮断し被害拡大の防止にも費用がかかります。（約300万円）

フォレンジック費用
詳細な原因や不正利用の有無など被害範囲の徹底調査はその後の事故対応を左右する極めて重要な対応です。サイバー攻撃の種類にもよりますが、PC1台100万円、サーバー1台200万円程度かかります。（約500万円）

お見舞金
不正利用された金額、カード番号が漏えいすると不正利用されていなくともカード会社にてカードの再発行にかかった費用（1枚あたり約1,000円）も請求される場合があります。
（1,000円×1万人＝約1,000万円）

モニタリング費用
不正利用が無いか一定期間のモニタリングが必要となります。（約500万円）

再発防止対策費用
同様の被害に遭わないための再発防止策の導入が不可欠です。（約300万円）

コールセンター費用
問合せ対応は専門業者に委託した場合、複数のオペレーターを確保し、最低でも1～2か月が必要になることが多いです。
（3名×2か月×50万円＝約300万円）

サイバー保険お勧めします

企業様としては、
『フォレンジック業者』や『弁護士』といった専門業者にいつでも依頼できる体制を平時から構築する必要がありますが、その分野に長けた専門業者を把握している企業は一握りです。
そのため、
専門業者の紹介が可能、その対応費用も支出可能でかつ賠償金や自社の喪失利益をカバーできるサイバー保険に加入しておくということは、サイバー攻撃からの早期回復、信頼回復に対する企業の備えとしてまさに打ってつけといえます。

【お問合せ先】
銀泉株式会社　URL　:https://www.ginsen-gr.co.jp
◆東京損害保険推進部
担当：成川／仲野　E-mail: gsinfoins@ginsen-gr.co.jp
〒102-0022　東京都港区海岸1丁目2番20号汐留ビルディング13階・17階
TEL　03－6777-7015

HPでのお問合せはこちらから