6校

ランサムウエア攻撃

教訓から学ぶセキュリティー対策

新型コロナ禍を契機としたテレワークの普及やデジタル技術を活用したビジネスモデルの変革を目指すDX（デジタルトランスフォーメーション）が加速する中、さまざまな手口によるサイバー攻撃のリスクも高まっている。特に最大の脅威となっているのがデータを暗号化し、と引き換えに身代金を要求する「ランサムウエア」であり、県内企業においても被害が相次いでいる。今回の特集では、25年8月にランサムウエアによる被害を受けた紙・文具・事務機の総合商社㈱レイメイ藤井（本社・福岡市博多区古門戸町、本店・熊本市西区上熊本1丁目、藤井章生社長）の実例をもとに、サイバー被害の教訓から学ぶセキュリティー対策を取材した。

（編集部・甲木昌宏）

特に「ランサムウエア」は最大の脅威となっている（写真はイメージ）

「何が起きたのか、頭が真っ白だった」

坂下 正治
常務取締役管理本部長

「事件が起きた直後は、正直何が起きたのか、どのように対処すべきかまったく分からず、頭が真っ白の状態だった」。

レイメイ藤井の管理部門を統括する坂下正治常務取締役管理本部長は、サイバー被害を受けた直後の心境をこう話し、早期復旧の見通しも立たない深刻な状況にサイバー攻撃の恐ろしさを実感したという。

25年8月9日土曜日。本社を襲ったサイバー攻撃は、お盆休みを挟む夏季休暇の初日に起きた。休日のマニュアル通り、当日朝、IT統括部の社員がリモートワークでサーバーを確認したところ、その一部が停止していることが判明。すぐに同部の社員数名が出社し、サーバーの管理委託先のベンダーに連絡を取りながら調査と当該サーバーの保全を実施した。調査の結果、11時20分にランサムウエア攻撃による被害を確認。12時過ぎに連絡を受けた坂下常務は全役員に携帯メールで連絡し、出社後、即座に対策本部を立ち上げた。

保険が一筋の光明に

サイバー被害が判明した後、まず行ったのが社内のあらゆるネットワークの遮断だ。「とにかく、どのような形で侵入され、ウイルスがどこに潜んでいるか分からず、被害拡大を防ぐためにすべてのケーブルを抜いた」と坂下常務。次に保険会社へ連絡し、初動についてのアドバイスをもらった。同社は約2年前にサイバーリスク保険に加入。この保険が同社にとって「一筋の光明」となったという。

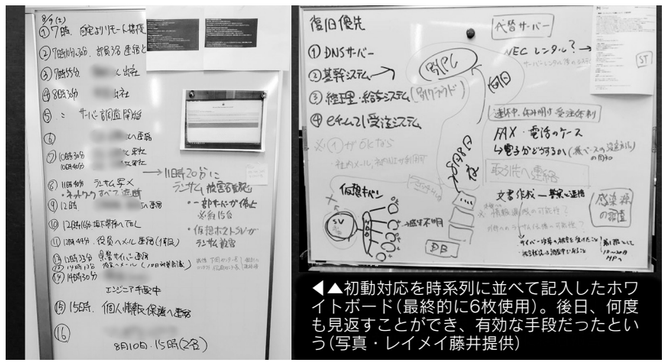
近年、損保各社のサイバーリスク保険は「インシデント初動対応支援サービス」が付帯されており、被害発生直後の対処についてのアドバイスや専門機関の紹介までサポートしてくれる。同社もその指示に従い、12時30分に福岡県警察本部サイバー犯罪対策課へ被害を報告。夕刻には事情確認のために担当警察官が来社し、被害届もその場で受理された。また、情報漏えいの有無に関係なく、個人情報保護委員会への報告も必要とのアドバイスを受け、被害にかかる速報を報告した。

初動の大切さ痛感

翌8月10日には、社長以下全役員、本部長、各拠点の支店長を集め、1回目の対策本部会議を開催。社内のネットワークがつながらない中、各個人のライン電話をつなぎ、情報共有や問題点の把握などに努めた。（対策本部会議は最初の1週間で6回開催、最終的に計9回開き、その後は取締役会で定期的に経過報告）

これと並行し、同日から外部調査機関に委託して被害を受けたサーバーに保存されたデジタルデータを証拠として分析・保全するフォレンジック調査を開始。一方、社内のパソコン画面には「スイッチは入れるな」と手書きした注意書を貼り、2次被害を防ぐための手立てを徹底した。坂下常務は「オフィスのすべてのパソコンにずらりと貼紙がされた光景はある種異様だった」と振り返る。

休日明けの8月12日。出社した社員にサイバー被害の経過を報告し、情

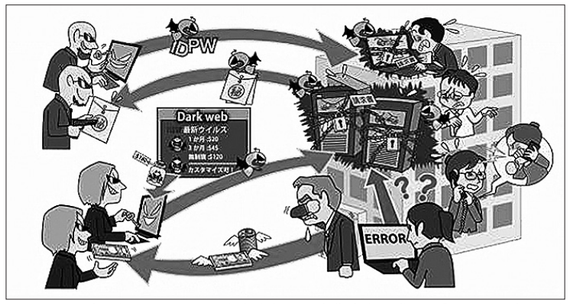


◀▲初動対応を時系列に並べて記入したホワイトボード（最終的に6枚使用）。後日、何度も見返すことができ、有効な手段だったという（写真・レイメイ藤井提供）

▲脅威を増すサイバー犯罪。攻撃者はネットワークの脆弱性を突き、攻撃を仕掛けてくる。

▲福岡本社のサイバー被害で受発注業務などに影響が出た㈱レイメイ藤井熊本本店（熊本市西区上熊本1丁目）

報を共有。一方で、取引先に迷惑が掛からないよう、通常通り営業業務を継続した。しかし、受発注業務を一括管理する基幹システムがダウンしているため、顧客との商談は電話やＦＡＸによる受発注に切り替え、伝票も手書きで対応。社内の通達手段は全店ＦＡＸを使うなど、まさにアナログ時代に戻った感じで業務を継続したという。



▲データの暗号化や画面ロックなどを行い、身代金を要求する「ランサムウエア」のイメージ（出典：IPA独立行政法人情報処理推進機構）

「お盆休みが重なったため、社内体制や顧客対応に関してはある程度の準備ができたのは不幸中の幸いだった。今回のサイバー被害でまず教訓になったのは、初動対応の大切さであり、『もしもの備え』をいかに準備しておくか、その『意識』を持っておくことが重要だと痛感した」と坂下常務は話す。

サーバーに脅迫文

同社を襲った「ランサムウエア」とは、コンピューターやサーバーに侵入し、データやシステムを使用不能にした上で、その解除と引き換えに金銭を要求する不正プログラムである。主な手口は重要なファイルを暗号化したり、システムへのアクセスを遮断することで、業務継続を不可能にする。

また、新たな手口としてネットワーク内のデータを暗号化する前に窃取しておき、「身代金を支払わなければ、このデータを公開する」という「二重恐喝」も確認されている。被害を受けた同社のサーバーにも、「12時間以内に添付のメールアドレスに連絡をすれば、暗号解除の鍵を渡すので安心しろ」という脅迫文が残されていた。

同社は当然、この脅迫に屈して攻撃者に連絡することはなかった。坂下常務は「警察からは独断で連絡しないでくださいと指導を受けたことが、今も強く記憶に残っていると話す。

VPNの脆弱性

最近の傾向として、ランサムウエアの感染経路は、ネットワーク機器を経由した侵入が最も多いという。攻撃者はＶＰＮ（仮想専用線と呼ばれ、拠点間を仮想の専用線で結び、安全に情報をやり取りするための仕組み）機器やルーター、ファイアウォールなどのシステムの脆弱（ぜいじゃく）性や強度の弱い認証情報を狙い、ネットワークに侵入。特にリモートワークの普及でＶＰＮ機器の利用が増加した結果、ＩＤやパスワードなどの認証情報の脆弱性を狙った攻撃が急増している。

なお、データ復旧の専門家によると、暗号化されたデータを元の状態に戻すことはほぼ不可能という。


▲「秘密鍵」がかかったランサムウエアの復旧はほぼ不可能という（写真はイメージ）

サーバーが暗号化 情報漏洩なし

8月18日。フォレンジック解析結果（速報）の報告を踏まえ、同社はホームページで「当社サーバーにおける第三者からの不正アクセスの発生について」と題した第一報を公表。これまでの経緯、現在の状況、今後の対応などを真摯に発信し、被害影響の最小化に努めた。

それから外部専門機関による侵入経路および攻撃活動の最終調査結果が報告されたが9月2日だった。これを受け、9月10日付で被害報告の第二報を公表した。

それによると、攻撃者は社外からネットワーク経由で1台のコンピューターに接続し、そのコンピューターをリモートで操作して不正アクセスを行い、複数の社内サーバーに接続。最終的にサーバー室設置の大半がランサムウエア攻撃によってファイルを暗号化され、サーバー内に脅迫文を残した。

また、漏えいした可能性がある情報については、9月9日現在、同社サーバーから漏えいした可能性がある情報の公開は確認されておらず、解析対象となったサーバーやコンピューターからも外部への明確な情報漏えいの痕跡はなかったと報告している。

PC・メール運用の4項目徹底 侵入前提で被害最小化対策も

今回のサイバー被害のケースでは、被害確認からフォレンジック解析結果の最終報告まで約3週間を要した。（8月9日発生、9月2日に最終報告）。

同社は、この調査結果を待つ間、安全性を確認した上で、段階的なネットワークの復旧と再開を進めた。それと同時に、社内ネットワークの利用にあたり、パソコン（ＰＣ）・メール運用の4つの取り決めを徹底した。

まず第一が、ＰＣ起動時のウイルスチェックの第三者確認だ。特に今回侵入したウイルスの拡張子が各自のＰＣに残っていないかの確認を全社員に義務付け、そのチェック状況を各課長が必ず確認することまで求めた。二つ目が、各自のＰＣに組み込んでいるセキュリティーソフトのアップデートの徹底であり、これも各課長が必ず確認するようにした。三つ目は、運用面でこれまで脆弱性を指摘されていたパスワードを一斉変更。四つ目は、外部への添付ファイルメールの取り扱いを強度の高い最新ツールに変更した。

こうした対策の一方、坂下常務は「今回の被害を教訓に学んだことは、会社としてサイバー攻撃に対する考え方や見方を変えること」と話す。

「セキュリティーが破られないよう守りを強化することは大切だが、攻撃者はさまざまな手口で侵入してくる。今後は侵入されることを前提とした対策も必要であり、サイバー攻撃を受けてもいかに被害を最小にとどめるかを考えることが重要になる」と強調。その対策として、社員の継続的なセキュリティー教育に加え、サイバー攻撃の防御だけでなく、侵入を前提とした防御策を強化する考えだ。

具体的には、ＰＣやサーバーなどのエンドポイントを常時監視し、侵入したマルウェアや不正アクセスの検知・対処を行う「ＥＤＲ」の導入、専門家チームが企業のＩＴ環境を監視し、サイバー攻撃の脅威を迅速に検知、分析、対応するアウトソーシングサービス「ＭＤＲ」の採用、「バックアップの３-２-１ルール」（データは3つコピーし、2つは異なる保存方法、1つはオフラインで保存など）の徹底などを予定しているという。

被害相当額は億円を上回る

9月10日だった。その間も、システム担当部署では被害を受けた基幹システムの復旧作業を各メーカーと一緒に進めた。しかし、被害を受け壊れたシステムを再度構築するには相当の期間がかかる。現在もその作業は続き、最終的に元の状態に復旧するのは今年2月頃になる見込みだ。

さらに、一連の対応に要した経費（被害額）も経営を直撃する大きな課題となった。同社はサイバー攻撃によるネットワーク機能の停止で事業継続に大きな影響が発生し、営業利益ベースで数千万円の利益損失を見込む。これに加え、「サーバーなどの再調達・再構築費用」、「サイバー専門家によるフォレンジック調査費用」、「復旧作業に伴う社員の時間外賃金の増加分」、「携帯テザリングによる通信量の増加分」、「弁護士相談費用」などの経費が必要となり、被害相当額は億円を上回るという。

同社はこうしたリスク

マネジメントの一環として、約2年前にサイバーリスク保険に加入していた。先述の通り、この保険の存在が比較的短期間で収束できた原動力になったと言える。

坂下常務は「初動対応や報告関係機関への連絡、サイバー専門家の紹介、原因調査、今後取るべき対策についてもアドバイスをいただいた」と感謝し、「『もしもの備え』という位置づけでは、保険の活用は極めて有効だった」と話す。

なお、サイバー専門家による報告書は後日、法的な争いになった場合にも有効な証拠書類となる。この調査費用は保険の補償額に含まれ、被害相当額の半分以上は保険の補償でカバーできる見込みという。

▲対策にはパソコンやメールの運用法など「セキュリティポリシー」の策定が急務

「被害体験をお客さまに還元」

同社は1月、社内に「セキュリティシステム推進室」を立ち上げ、サイバー脅威に対する強固なセキュリティー対策を進めている。加えて、新たに導入するセキュリティーソフトを営業担当者が取引先に自信をもって紹介できるよう、販売体制の確立と社内研修に力を入れている。

坂下常務は「当社はお客さまのオフィスのDX化を推進している。サイバー攻撃の被害を受けた会社がこのような話をしても信ぴょう性に欠けるとお叱りを受けるかもしれないが、当社の社員全員が今回の被害を体験している。この体験は何事にも代えがたいものであり、経験しているがゆえに、お客さまに寄り添った対応ができると思っている。この経験を還元する意味でも、遠慮なく当社担当者にお声がけをいただき、サイバーセキュリティー対策の実践に生かしていただきたい」と結んだ。

企業に求められるリスクマネジメント

外部に「移転する」考え方が重要

近年、サイバー攻撃が頻発化し、その対策は優先順位が高い経営課題として取り組まなければならない時代に入った。

それは自社のネットワークが不通になり、事業継続が脅かされるだけでなく、個人情報の流出など顧客や取引先などに被害が波及し、加害者となる可能性もあるからだ。経営者は深刻な被害につながりかねないサイバー攻撃への防御策だけでなく、被害を受けた場合の損害を最小限にとどめるリスクマネジメントが求められている。


東村 智司
理事・熊本支店長

東京海上日動火災保険㈱の東村智司理事・熊本支店長は「攻撃者が狙うのは大企業だけではなく、その企業と取引があり、セキュリティー対策が脆弱な中小企業も対象となる。そして、中小企業のセキュリティーを突破し、メールなどを経由して大企業のシステムに侵入する〝踏み台攻撃〟と言われるものも多く発生している。実際にランサムウエア被害の60％以上は中小企業で発生しており、『自社に狙われるデータはない』、『今まで大丈夫だった』という考え方は排除し、サイバーリスク対策を経営課題と位置付けて取り組んでいく必要がある」と警鐘を鳴らし、「サイバー攻撃に遭った場合、適切な初動をとらなければ被害が拡大し、自社の事業中断期間が長引くとともに、事業再開後も信用低下による売り上げや取引先の減少など、将来に渡って影響が残る」と指摘する。

保険でリスク移転

一方で、サイバー攻撃は日々進化するリスクであり、どれだけ対策にコストをかけてもある一定の段階でリスク減少効果が頭打ちとなり、サイバーリスクを完全に0（ゼロ）にすることはできないと言われている。

東村支店長は「経営への影響が大きい場合、そのリスクを『保有』し続けるのではなく、リスクを『低減』させる取り組みをした上で、残留リスクは『保険を活用して外部に移転する』という考え方が有効とされている。当社におけるサイバーリスク対策では、『移転』としてのサイバーリスク保険の提案、『低減』としてはサイバーリスク対策を盛り込んだBCP（事業継続計画）策定支援、最新のサイバー情報やテキスト、簡易リスク診断などのサービスを提供しているポータルサイト『TOKIO CYBER PORT』を通した従業員教育支援などに取り組んでいる」と説明する。

さらに、同社は事前対策を強化したい企業向けに、サイバーセキュリティー専門事業者である㈱CISO（本社・東京都港区）と提携し、セキュリティー対策代行支援のビジネスマッチングサービスを開始。これによりサイバーリスクついて、事前の予防・防御と発生後の対処を一貫して対応できる体制を充実させた。

第三者への賠償責任負うケースも

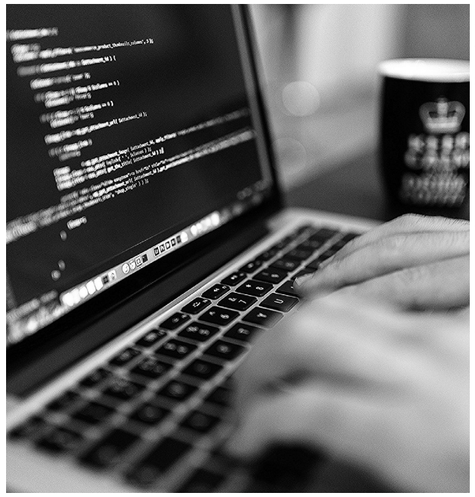
では、サイバー攻撃を受けた場合、どのような対応が求められ、どれくらいの損害費用負担が発生するのだろうか。

サイバー攻撃への初動対応および事後対応を、実際に発生した事例を基に時系列で追うと左記の①～⑤に区分される。いずれのプロセスにおいても多額のコストが発生する可能性があり、取引先のデータや個人情報の流出で経済損失を与えた場合、顧客対応、訴訟対応に加え、加害者となり第三者への損害賠償まで負わなければならないケースもあることを忘れてはならない。

このように初動対応、原因・被害調査、取引先対応、復旧、再発防止の各ステップにおける対応は多岐にわたる。ちなみに、セキュリティー事故やサイバー犯罪の対象となったコンピューターに残されたデータを収集し、原因や痕跡などを調査分析する手段をデジタルフォレンジック調査というが、これには法的証拠となるデータの保全も含まれる。通常は専門技術を持ったセキュリティーベンダーの手で行われ、この費用だけでもパソコン一台あたり100～200万円近くかかると言われている。

サイバー攻撃を受けた場合の初動対応から事後対応の流れ

① 検　　知：検知内容の精査
② 初動対応：影響調査、影響箇所・範囲の特定など
③ 対　　応：ログ収集、証拠保全、原因・被害調査（デジタルフォレンジック調査）、バックアップ復元
④ 事態収束：見舞金支払い、広報対応、弁護士費用、カスタマー対策室設置
⑤ 再発防止計画：各種施策の計画策定など


▲原因や痕跡などを調査するデジタルフォレンジックはパソコン1台あたり100～200万円かかるという

工場の営業停止で損害額7千万円

左の資料は東京海上日動火災保険がまとめた想定事故事例だが、ケース①「年間売上高100億円、従業員400人の製造業」の場合、工場の生産ラインを管理するシステムがランサムウエアに感染し、調査・復旧に時間がかかり、2週間営業が停止した。この事例で発生した主な損害額は、①パソコン・サーバーのデジタルフォレンジック調査・復旧に550万円、②広報対応に関するコンサルティング100万円、③営業停止に伴う喪失利益の発生7000万円、合計7650万円の損害額が発生すると見込んでいる。

●ケース①「年間売上高100億円、従業員400人の製造業」

会社概要
年間売上高:100億円
従業員:400人

事故内容
工場の生産ラインを管理するシステムがランサムウエアに感染。調査・復旧に時間がかかり、2週間営業が停止した。

想定される対応と損害額
- パソコン・サーバーのデジタルフォレンジック調査・復旧:550万円
- 広報対応に関するコンサルティング:100万円
- 営業停止に伴う喪失利益の発生:7000万円

合計 7650万円

対応の流れ
ランサムウエア感染発覚 → 初動対応 感染拡大防止 → 顧客への連絡・広報対応 / 調査・復旧 → 再発防止 → 生産再開

●ケース②「売上高2億円、従業員10人の小売業」

会社概要
年間売上高:2億円
従業員:10人
売上高の80%がECサイト経由の販売

事故内容
ECサイトへの不正アクセスで顧客情報(※)1000件が流出。調査・復旧に時間がかかり、20日間ECサイトを閉鎖した。
(※住所・氏名・電話番号・クレジットカード番号・セキュリティコード・有効期限)

想定される対応と損害額
- サーバーのデジタルフォレンジック調査・復旧費用:500万円
- 顧客対応にかかる弁護士相談:150万円
- 顧客への情報漏えいにかかる通知:10万円
- 顧客への見舞金支払い:100万円
- 営業停止に伴う喪失利益の発生:800万円

合計 1560万円

対応の流れ(例)
顧客情報流出発覚 → 初動対応 被害状況確認 → ECサイト閉鎖 → 公表、顧客への連絡・対応 / 調査・復旧 → 再発防止 → ECサイト再開

出典:東京海上日動火災保険「サイバーリスク対策」資料

ケース②「売上高2億円、従業員10人の小売業」の場合、ECサイトへの不正アクセスで顧客情報1000件が流出し、調査・復旧に時間がかかり、20日間ECサイトを閉鎖した。この事例では、①サーバーのデジタルフォレンジック調査・復旧費用500万円、②顧客対応にかかる弁護士相談150万円、③顧客への情報漏えいにかかる通知10万円、④顧客への見舞金支払い100万円、⑤営業停止に伴う喪失利益の発生800万円で、合計1560万円の被害が発生すると想定している。

中小企業こそ保険を

東村支店長は「中小、中堅企業いずれの場合でも、事故そのものの被害だけでなく、事業再開後も納品遅延による信用低下やウェブサイトの販売数低下など、将来にわたり売り上げに影響が残る可能性があるのがサイバー被害の特徴」と説明。「事故発生時の初動対応費用や損害賠償費用の捻出が困難な中小企業こそ、保険によるリスク移転が重要となる」と繰り返し強調する。

初動対応から発動

サイバーリスク保険は、主に「賠償責任に関する補償」と「サイバーセキュリティー事故対応費用に関する補償」の2つに分けて補償を提供している場合が多い。

東村支店長は「サイバー攻撃があったと判断・確定するためには各種調査が必要であり、費用が発生する。当社のサイバーリスク保険では『サイバー攻撃のおそれ』を『セキュリティー事故』とし、初動対応から保険が発動する仕組みとしている。これによりサイバー攻撃に遭った事業者に迅速な初動対応・原因調査をしていただくことが可能となり、被害拡大の防止にもつながっている。また、この他にもオプションでサイバー被害による利益損失(喪失利益・収益減少防止費用)と営業継続費用を補償することができる」と説明する。

さらに、多くの損害保険会社では、付帯サービスとして「インシデント初動対応支援サービス」を提供している点も大きな特徴だ。前述のレイメイ藤井の初動対応でも触れたが、この付帯サービスが「一筋の光明」となったという。


▶熊本支店が入る東京海上日動火災保険㈱熊本ビル(熊本市中央区水道町)

東京海上日動火災保険の場合、経験豊富な担当者や専門家が24時間365日体制で問い合わせに対応し、緊急時の初動から保険金請求や再発防止策まで支援する「緊急時ホットラインサービス」を提供。この他にも企業のネットワークの脆弱性と攻撃者の標的となる人的リスクを指標化する「ベンチマークレポートサービス」や、外部モニタリングによりセキュリティー上の課題を発見した場合、メールでアラート通知する「サイバーリスク・モニタリングサービス」を保険契約者にサービスとして提供しているという。

熊本支店の契約件数は20%増

東村支店長は「熊本支店では、これまで熊本県警と連携したセミナーや自治体および商工団体と連携したBCP策定支援セミナーの開催などを通して、地域の事業者にサイバーリスク対策の重要性を伝え続けるとともに、代理店と連携してサイバーリスク保険の提案・販売に取り組んできた。昨年は国内大手企業でもサイバー被害が発生し、事業継続に甚大な影響が生じたことは記憶に新しいと思う。年末年始に多くの県内企業の経営者と面談する機会があったが、多くの方がサイバーリスク対策についての話をされ、関心の高まりを感じている。実際、相談件数も増え、熊本支店の契約件数は全国平均を上回り、前年比20%増となっている。保険料は業種や売上規模などにより異なり、必要となる補償も企業によって違う。まずは近くの保険代理店へ問い合わせて欲しい」と話した。

▲今や対岸の火事ではないセキュリティーリスク。第三者への損害賠償を負うケースもあり、経営者はリスクを識別し、適切の管理および対策を講じることが求められている(写真はイメージ)