2022.03.24

サイバーセキュリティニュース ＜2021 No.003＞

昨今のランサムウェアについて

【要旨】
■ 昨今の国際情勢等から、サイバー攻撃を受けるリスクは一層高まっている。
■ ランサムウェア攻撃が拡大、猛威を振るっており、その影響は実害を受けていないサプライチェーン上の広範囲までおよび、甚大となるおそれがある。
■ 企業グループ、そしてサプライチェーンも含めて、サイバー攻撃を完全に防ぐことはできないという認識のもと、防御を中心とした対策（事前対策）だけでなく、攻撃を受けた際の対策（事後対策）を進めることが必要である。

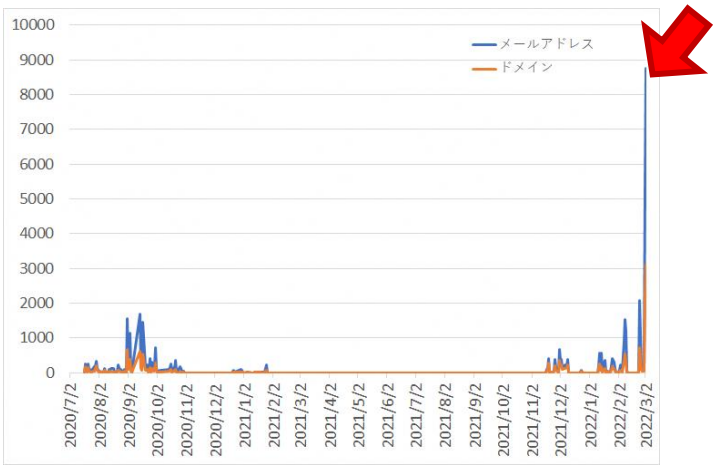
1．昨今の情勢をうけたサイバー攻撃の激化

2022 年 2 月 24 日、ロシアがウクライナへの侵攻を開始した。この侵攻においては、現実空間における当事者両国間の争いのみならず、サイバー空間において数多くの関係者を巻き込んだ争いが繰り広げられていることは着目すべき点といえる。

既に米欧日各国により、ロシア金融機関への国際決済網からの排除や資産凍結、同国への輸出禁止など各種の経済制裁が実施され、また、企業単位でも同国における事業活動の停止の発表が相次いでいる。

そうした中、ロシア語圏に活動拠点を置くといわれる、あるランサムウェア犯罪グループは「ロシアやロシア語圏の重要なインフラ、平和な市民の生活と安全が脅かされる場合、全力で報復する」との声明を発表した。独自の経済制裁的な行動をした企業・組織だけでなく、経済制裁を実施している国に属する企業に対しても「報復や見せしめ」としてサイバー攻撃のターゲットとなる可能性が高まっている。

また、昨今の情勢との関連性は不明ではあるものの、前述の犯罪者グループとの関与が疑われるマルウェア「Emotet」（エモテット）の感染が拡大していることも着目すべき点である。JPCERT/CC（ジェーピーサート/シーシー）は 3 月 3 日に「マルウェア Emotet の感染再拡大に関する注意喚起[1]」として「2022 年 3 月に入り、Emotet に感染しメール送信に悪用される可能性のある.jp メールアドレス数が 2020 年の感染ピーク時の約 5 倍以上に急増している」と発表している。



【図 1】Emotet に感染しメール送信に悪用される可能性のある.jp メールアドレス数の新規観測の推移
（出典：JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」）

[1] JPCERT/CC「マルウェア Emotet の感染再拡大に関する注意喚起」https://www.jpcert.or.jp/at/2022/at220006.html

Emotet は、2021 年 1 月に Europol（ユーロポール。欧州刑事警察機構）が、欧米 8 カ国の法執行機関・司法当局の協力により、攻撃基盤を停止させたことで、攻撃の停止あるいは被害は大幅に減少していたが、同年 11 月から活動再開が確認され、前述のとおり、2022 年 3 月は活動が急激に拡大し、被害も拡大しているところである。

Emotet は、メールアドレス、メール内容などの情報の窃取を図るほか、組織内ネットワーク内への拡散、他のマルウェア、例えばランサムウェアを呼び込み、被害を拡大させるおそれがある。

本稿では、昨今のサイバー攻撃・犯罪において多大な影響を及ぼしているランサムウェアの特徴と対策のポイントについて解説する。

２．昨今のランサムウェアの特徴

ランサムウェアとは、身代金を意味する「Ransom」と「Software（あるいは Malware）」を組み合わせた造語である。攻撃先の PC やサーバ内にあるデータを暗号化し、データの復号（回復）と引換に身代金を要求するマルウェアとして、ここ数年の間で大きな脅威となっている。以下に昨今のランサムウェア攻撃の特徴を解説する。

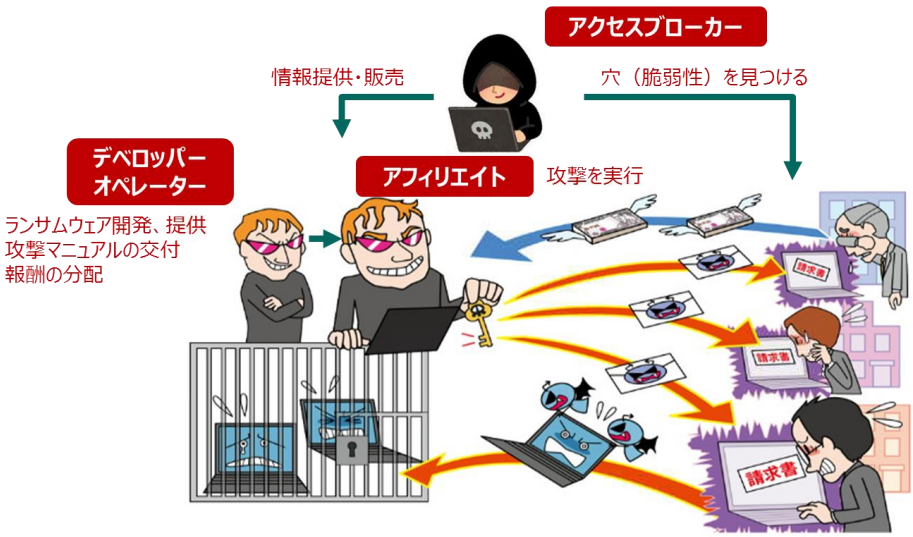
（１）分業化、エコシステム化

ランサムウェアによる被害が大幅に増えている背景のひとつに、攻撃の高度化・分業化やエコシステム化が挙げられる。

攻撃者グループの役割は、

・ランサムウェアの開発や提供をする者（デベロッパー、オペレーター）
・ターゲット企業の穴（脆弱性）を見つけて、情報提供・販売をする者（アクセスブローカー）
・攻撃を実行する者（アフィリエイト）

といったように分業化され、ダークウェブ（一般的なウェブブラウザでは閲覧することができない、匿名性の高いネットワーク上に構築されたサイト群）等において、それぞれの役割の募集や情報交換がされている。このような分業化に基づくビジネスモデルは「RaaS（ラース。Ransomware as a Service）」といわれ、振り込め詐欺に代表される特殊詐欺集団と同じような組織形態が確立されており、ランサムウェアを開発するノウハウのない者でも攻撃することが可能になっている。

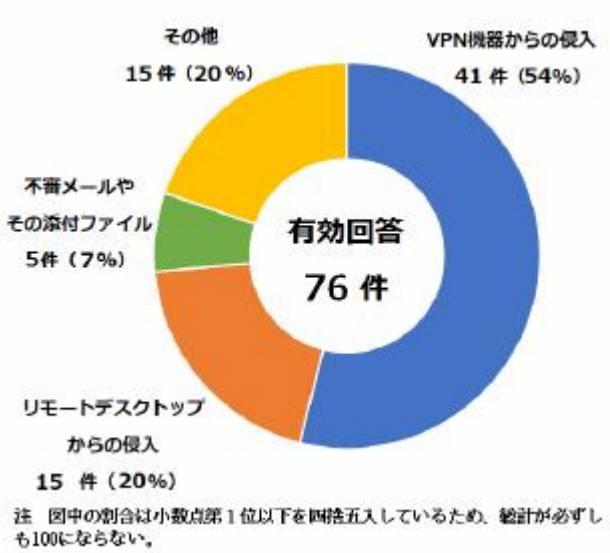


【図２】RaaS（Ransomware as a Service）
（出典：IPA「情報セキュリティ10大脅威」をもとに弊社が加工）

（２）感染経路

警察庁が 2022 年 2 月 10 日に公表した「令和３年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」によると、ランサムウェアの感染経路としては、ＶＰＮ機器（セキュリティを確保した通信を行うための機器）の脆弱性やリモートデスクトップ（遠隔操作のための機能）等から組織内部のネットワークに侵入しランサムウェアに感染させる手口が被害の多くを占めていることがわかる。

コロナ禍において、テレワークの導入等により外部から内部ネットワークへの接続が急増し、セキュリティ対策の一環としてＶＰＮ機器やリモートデスクトップを導入する企業等が増加していること、そしてこれらの機器・サービスの導入に携わる一部のベンダのアフターフォローがないこともあいまって、脆弱性を放置している組織が多いことがその要因として挙げられる。



【図３】ランサムウェアの感染経路

（出典：警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」）

近年着目される攻撃手法としては、比較的セキュリティ対策が手薄な取引先を経由したり、利用しているソフトウェア等の製品に不正プログラムを紛れ込ませたりしてターゲット企業への攻撃成功を試みる、いわゆる「サプライチェーン攻撃」が、世間一般でいわれるところである。

例えば、2021 年 7 月に発生した、アメリカ IT 企業が開発する IT 管理製品の脆弱性を狙ったランサムウェア攻撃では、マネージドサービスプロバイダと呼ばれる運用サービス事業者を経由して同製品を利用する 1,000 社を超えるユーザー企業に被害が発生した。クラウドサービスの活用を前提としたバックオフィス機能のアウトソース化が進むなかで、サイバー攻撃によるサプライチェーンリスクの影響の大きさを証明した事案となった。

サイバー攻撃は金銭を目的としたケースがその大多数を占める。攻撃者にとってみれば、いかに身代金の支払いを引き出すことができる企業をターゲットにするかがポイントとなるが、例えば、大企業との取引を行っている企業などは、その取引先に対する影響度の大きさから狙われやすいといえる。国内においては、2022 年 2 月 28 日に、サプライヤー（部品仕入先）に対するサイバー攻撃を原因として、自動車メーカー国内全工場の操業を停止する事態が発生した。この事例では、自動車メーカーへの攻撃を図った可能性は否定できないものの、金銭目的として行われた攻撃であると仮定するならば、そのターゲットとなる企業が狙われるべくして狙われたといえる

事例であった。いずれにせよ、被害の拡大を防ぐべく原因や感染経路の調査のために操業を停止せざるを得なかったことも含め、サイバー攻撃によるサプライチェーンリスクの影響の大きさを改めて証明した事案といえよう。

（３）四重の脅迫

ランサムウェアによる攻撃は高度化の一途を辿っている。その攻撃は、単純にランサムウェアに感染させるだけではないということである。

まず、挙げられるのは「二重の脅迫」といわれる手法である。攻撃者はあらかじめ機密情報などの重要な情報を窃取し、攻撃者がダークウェブで管理する「リークサイト」上で盗み出した情報の一部を公開し「身代金を払わないのなら、盗んだ機密情報をリークサイトに暴露する」といった脅迫をしてくるケースがある。

さらに「身代金を払わないのなら、DDoS 攻撃（あらかじめ乗っ取った複数の機器を経由しサービスを停止させる攻撃）を仕掛ける」といったもの、攻撃をした企業の取引先や顧客に対して「重要情報をさらされたくなければ、ランサムウェア攻撃をした企業に身代金を払わせろ。または、自ら身代金を払え」といったもの、いわば三重、四重の脅迫を仕掛けてくる。

一方、世の中に多く「流通」しているものは、これらの最大「四重の脅迫」型ではなく、ランサムウェア感染のみのバラマキ型の事象、または「リークサイト」への公開を伴わない事象も多いことにも留意しておきたい。

３．ランサムウェアに関する規制

（１）身代金の支払いについての規制

身代金の支払いは、ランサムウェアの攻撃者グループの増加、その活動の拡大に直結する、犯罪助長に繋がる行為であることは明白といえよう。このような状況下において、各国において身代金の支払いについての規制の動きがある。

その代表例として挙げられるのは米財務省の OFAC（オファック。外国資産管理局）および FinCEN（フィンセン。金融犯罪捜査網）による勧告である。この勧告では「サイバー保険会社、インシデント対応に携わる企業など、被害者に代わってサイバーの攻撃者へのランサムウェア支払いを促進する企業は、将来のランサムウェア支払い要求を助長するだけでなく、OFAC 規制に違反する危険性がある」として、身代金の支払いが OFAC 規制（米国指定の国・地域などについて、取引禁止や資産凍結などの経済制裁措置）に該当することを、2020 年 10 月に表明している（2021 年 9 月にも追加勧告あり）。

米国のその他の機関や米国以外の国においても同様の動きがあり、英 NCSC（ナショナルサイバーセキュリティセンター）、豪政府、仏 ANSSI（国家情報システムセキュリティ庁）などから身代金支払を推奨しない旨が表明されている。また、我が国でも経済産業省が 2020 年 12 月に公表した「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」において「ランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである」と記載しているところである。

（２）サイバー保険による身代金の補償

我が国のサイバー保険では、身代金は補償対象としていない。一方、諸外国のサイバー保険においては身代金を補償対象としていることがある。しかしながら、このような補償は犯罪助長に繋がるものであり、これに対しても制限、規制などの動きがある。

まず、2021 年 5 月に仏 AXA 社は、司法当局等がランサムウェアの壊滅的な世界的流行について懸念を表明したことを受けて、サイバー保険の引受けを停止すると発表している。また、2021 年 6 月に英 RUSI（英国王立防衛安全保障研究所）が「政府と規制当局は保険会社に対し、身代金

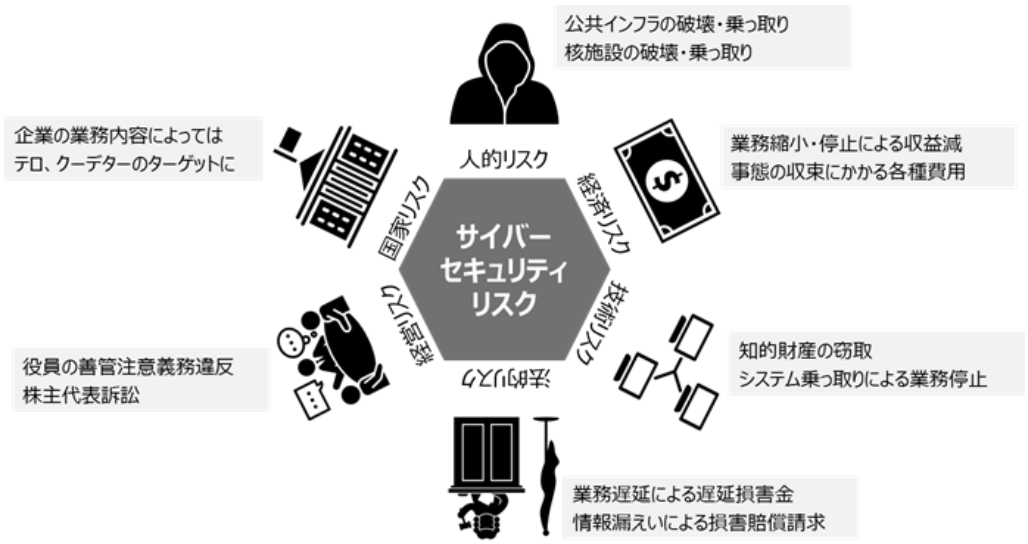
を支払う前に保険契約者が法執行機関に通知する契約上の義務を設けるよう迅速に働きかける必要がある」とするレポートを公表したり、2021 年 10 月に豪政府が公表した「ランサムウェアアクションプラン」においては「サイバー犯罪者は、ランサムウェア攻撃の準備のために盗んだデータを分析し、保険金額と同じ身代金の支払いを要求することがよくあります」として、サイバー保険と身代金要求の関係性を示している。

海外メディアにおいては、ランサムウェア犯罪グループのメンバーへのインタビューを行ったとする記事が存在する。同記事では犯罪グループのメンバーによる「サイバー保険の加入者リストを入手するために保険会社を狙っている」といった旨のコメントがあり、サイバー保険における身代金の補償対象化はランサムウェアのエコシステムの一端を担ってしまうことの顕れともいえる。単純な話ではないものの、サイバー保険では身代金を補償しないこと、それがランサムウェア被害を防ぐための一つの手立てであるといえよう。

4．対策のポイント

我が国においては、2 月 23 日に経済産業省から「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」と注意喚起が発表されたが、2 月 28 日には、部品仕入先によるサイバー攻撃被害を原因とした国内自動車メーカー全工場の操業停止が発生した。これを受けて 3 月 1 日には、経済産業省、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の 7 省庁が合同で改めて注意喚起を発表した。

この注意喚起では「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（中略）、対策の強化に努める」ことが求められている。企業を取り巻くリスクの中でも、とりわけサイバーセキュリティリスクは多くのリスクと接点がある。サイバー攻撃にあった結果、情報の窃取・改ざんなどデータへの被害・影響だけでなく、施設やインフラの物理的破壊・乗っ取りも起こりうる。その影響は自社にとどまらず取引先やユーザーにまで広がることもあり、事態の収束対応に不手際があった場合には、取引先やユーザーから業務遅延や情報漏えいによる損害賠償請求を受けたり、役員の善管注意義務違反を申し立てる株主代表訴訟が提起されるなど、経営の責任が問われる事態に発展することを、昨今の情勢を契機に理解を深めていただきたい。



【図４】サイバーセキュリティリスクと他のリスクとの関連性

ICT（情報通信技術）の普及および進展により、現実空間における企業間でのつながりのほかに、サイバー空間におけるデータのつながりや、現実空間とサイバー空間におけるデータのつながりにおいてもセキュリティを担保する必要がある。こうした状況では、当事者の多様化がリスクの増大につながるとともに、インシデント発生時の各当事者の責任範囲が不明確になり、対応が混乱することも懸念される。対策は自組織だけでなく関係するサプライチェーン上の取引先にも求めることで、各当事者の責任範囲を明確にしつつ、対策に不備があれば改善の指示を出す必要がある。

サイバー攻撃を完全に防ぐことは不可能であるという認識の下「組織体制整備」「リスクの特定」「防御」「検知」「対応・復旧」に沿った対策を進めることが必要だが、とりわけ、インシデント発生を模した訓練を実施することで、対応手順の有効性と合理性、各部門の役割と選任した責任者の適切性、経営層への報告基準と報告ルートの適切性、経営層の判断基準と対応指示の適切性などを検証し、必要に応じて見直しを実施することを強く推奨する。訓練を繰り返し実施し、各自が行うべき対応を疑似体験することで、対応力を身に付けることができ、訓練実施により洗い出された課題を解決・改善することで、実効性のある組織体制へのスパイラルアップが期待できる。

本稿が取引先や委託先も含めたサプライチェーンにおけるサイバーセキュリティガバナンスの強化の一助となれば幸いである。

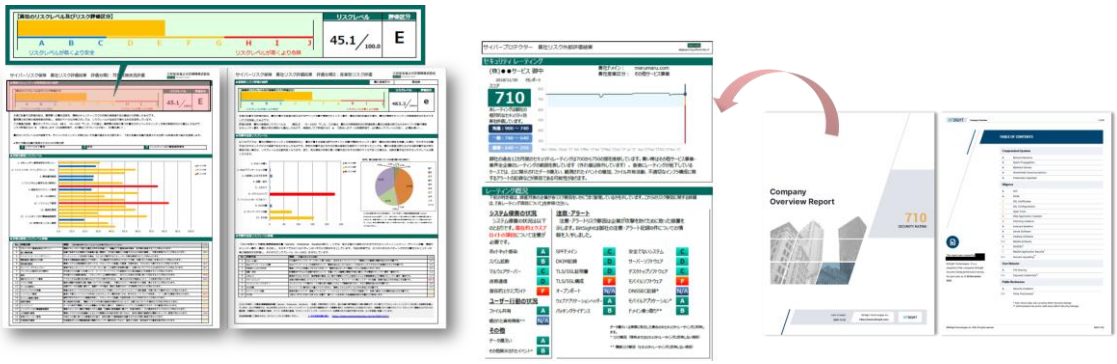
ＭＳ＆ＡＤインターリスク総研株式会社
新領域開発部 サイバーリスク室　室長
岡田　智之

新領域開発部 サイバーリスク室　マネジャー
神山　太朗

ＭＳ＆ＡＤインシュアランスグループでは、ベライゾン社とビットサイト社が有するサイバーセキュリティに関する最先端の知見を活用し、複雑化・高度化するサイバーリスクを多面的かつ精緻に評価するサービスを実施しています。

自組織における現状の情報管理体制の評価・見直しからサプライチェーン上の取引先や委託先の「システム感染」「不具合情報」まで表会をすることも可能、実効性のあるサプライチェーンサイバーセキュリティ管理体制の構築・整備と定着をご支援します。

【ベライゾン社「内部評価」とビットサイト社「外部評価」イメージ】



また、サイバー攻撃・情報漏えい発生等の危機シナリオに基づく模擬記者会見などのトレーニングを実施しており、トレーニングを通じた緊急時の対応能力の向上だけでなく、策定したルールの実効性検証・当該ルールの周知、既存対策の見直し効果など、様々なメリットを享受できるよう支援します。

ＭＳ＆ＡＤインターリスク総研株式会社は、MS&AD インシュアランスグループに属する、リスクマネジメントについての調査研究及びコンサルティングに関する専門会社です。
情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱
新領域開発部 サイバーリスク室
東京都千代田区神田淡路町2-105
TEL.03-5296-8918
http://www.irric.co.jp/