相続ドック NEWS RELEASE 2024年8月号

池田税務会計事務所

〒300-0847
茨城県土浦市卸町1-1-1
関鉄つくばビル2F

TEL:029(841)4300　　FAX:029(843)2826

中小企業にも必要？ サイバー攻撃･犯罪への備え

不安定な世界情勢とサイバー攻撃！
ランサムウェアの脅威
警察庁に「サイバー警察局」！

開催中のパリ五輪では、かつてない規模のサイバー攻撃の脅威を専門家が警告しています。最近ではKADOKAWAが受けたサイバー攻撃も話題になりました。実は、中小企業も標的になっており被害も生じています。

五輪とサイバーテロ

●開会式警備に7.5万人！

平時としてはフランス史上最大規模の警備で、最大7万5,000人の警察官と兵士、警備員が常時パリ市内をパトロール。道路や地下鉄駅は閉鎖、4万4,000基の柵が設けられ、セーヌ川や中州に行きたい住民向けには、複雑なQRコードシステムが導入されました。

●東京大会の10倍規模の攻撃？

サイバー攻撃への備えも必要で、パリ五輪はこれまでの五輪以上に悪質なサイバー攻撃のリスクが高まるとのことです。21年の東京大会では計4億5,000万件のサイバー攻撃があったとされますが、パリ大会では東京大会の10倍規模の攻撃が懸念されています。

●五輪がサイバー攻撃の標的に

今や五輪の運営はＩＴに大きく依存するため、格好のサイバー攻撃対象になっています。

＜過去の五輪のサイバー攻撃と対応事例＞

2008年 北京	本番とほぼ同じｼｽﾃﾑでｼﾐｭﾚｰｼｮﾝ、大会24時間前のIPｱﾄﾞﾚｽ総入れ替えの徹底対策を実行。大会期間中は1日1,400万回の攻撃。
2010年 ﾊﾞﾝｸｰﾊﾞｰ	件数は少ないが、**ﾌｨｯｼﾝｸﾞ詐欺**が巧妙化。ﾒｰﾙを通じて誘導し、ﾏﾙｳｪｱに感染させた。
2012年 ﾛﾝﾄﾞﾝ	1億6,500万件、開会式を妨害する照明ｼｽﾃﾑへの攻撃は40分間続くも照明は消えなかった。公式ｻｲﾄへの攻撃は2億2,100万回
2014年 ソチ	毎日最大50件の深刻な攻撃。ｻｲﾊﾞｰ犯罪者が内部潜入して逮捕された。競技場のｽｸﾘｰﾝ改ざん、**ﾗﾝｻﾑｳｪｱ**による脅迫も。
2016年 ﾘｵﾃﾞｼﾞｬﾈｲﾛ	ﾎﾞｯﾄ感染でPC乗っ取られ、組織委員会の暗号化ﾌｧｲﾙが盗まれた。ﾘｵ州知事や市長など要人の個人情報も漏えい。
2018年 平昌	Olympic Destroyerという**標的型ﾏﾙｳｪｱ**が確認された。放送が停止し、公式Webｻｲﾄが閉鎖され、ﾁｹｯﾄｼｽﾃﾑが混乱した。

＜サイバー攻撃とは？＞　ネットワークを通じて行われる攻撃や破壊活動のこと。基幹システムの機能停止や、ウェブサービスのシステムダウン、機密情報や顧客データの盗難などを目的に、マルウェアなどが攻撃に使われる。

＜マルウェアとは？＞　悪質な（malicious）ソフトウェア（software）を略した造語。代表的なものは、プログラムやファイルの一部を書き換えて自己複製する「コンピュータウィルス」、暗号化などによってファイルを利用不能な状態にし、元に戻すことと引き換えに金銭を要求する「ランサムウェア」などがある。

●日本は官民連携で防ぎ切った

東京大会期間中に関係組織や公式サイトなどで検知･遮断したサイバー攻撃はロンドン大会の2倍以上の4億5,000万件でしたが、運営に影響する攻撃は確認されず、組織委員会は「東京大会はサイバー攻撃から守られた」と総括。

＜前例にない規模で攻撃情報共有＞　サイバーセキュリティー対策に、組織委員会や東京都、内閣官房や警察庁などの行政機関の他、重要インフラ事業者、スポンサー企業、競技団体、競技場運営者など350機関が情報共有した。

●世界情勢悪化の影響で！

これまでも五輪のような国際的イベントはサイバー攻撃の標的となってきましたが、世界情勢の悪化を受けて、パリ五輪のリスクがこれまでになく高まったと言われています。

＜ロシア支援の攻撃者が脅威に＞　開催前から、米マイクロソフト社などが「パリ五輪のセキュリティーリスクが高まっている」と警告し、ロシアが支援する攻撃者グループを指摘。ロシア系のハッカーは、過去の五輪でも何度も攻撃を繰り返しているとのこと。

●フランスのウクライナ支援が･･･

ロシア選手はパリ五輪に出場はできますが、母国を代表することはできず、開会式にも参加できません。フランスがウクライナを支援してるという背景もあり、ロシア系の攻撃者グループの主な目的は、パリ五輪の失敗とフランスやIOCの信用失墜だという見方も。

●世界規模のシステム障害の原因は

7月19日、世界各地で大規模なシステム障害が発生。各地の空港で欠航、銀行は送金停止などの大混乱に。これはサイバー攻撃を受けたのではなく、近年被害が増えているランサムウェアなどのサイバー攻撃に備えるセキュリティーソフトの障害が原因という皮肉なものでした。

企業へのサイバー攻撃

●KADOKAWAに激震！

KADOKAWAグループに激震が走ったのは6月8日未明で、子会社のドワンゴが運営する動画配信サイト「ニコニコ動画」やKADOKAWAの公式サイトが利用できない状況に。社内調査の結果、グループのデータセンター内のサーバーが大規模な攻撃を受けたことが判明。

●既刊本の出荷3分の1に減少！

被害は同じデータセンターを使っていた主力の出版や経理部門に波及し、さらに通信制高校「N高等学校」の生徒や、同社と直接取引のあった作家やクリエーターの個人情報も漏洩。

＜サイバー攻撃の影響＞6月27日現在

出版事業	既刊本の出荷部数が平常時の3分の1に減少。新刊は通常通り出荷。
経理機能	人手による作業も含めて7月初旬に復旧のめど。
動画共有	主力のニコニコ動画はサービス停止続く。一部サービスは再開。
情報漏洩	外部の専門家の支援を受けて調査中。クレジットカード情報は社内でデータを保有していないため漏洩はない。

●ハッカー集団の犯行声明あり！

6月27日、KADOKAWAへのランサムウェア（身代金要求型ｳｨﾙｽ）を含むサーバー攻撃を巡り、「BlackSuit」を名乗るハッカー集団がダークウェブ(闇ｻｲﾄ群)に犯行声明を出した。同社の契約書やサービス利用者の情報など1.5テラバイト分のデータのダウンロードを表明。

＜すべてのデータを公開する？＞　犯行声明によると、約1ヵ月前にKADOKAWAのネットワークにアクセスし、ネットワーク全体を暗号化したという。同社経営陣との交渉次第ではすべてのデータを7月1日に公開するとし、身代金要求をほのめかしたが、その後、実際支払いがあったか否かは明らかになっていない。

●劇場型ランサムウェアの脅威！

復旧と引換えに金銭を要求する30年以上前からある手口。近年は暗号化の前にデータを搾取して暴露すると脅したり、被害企業の関係者のデータを公開して関心を高める「劇場型」の手口が増え、犯行が狡猾が化しています。

＜狡猾！第三者も巻き込む最近の手口＞

手口①	企業のシステムに潜入、暗号化し、凍結
手口②	リーク(暴露)サイトに機密情報を暴露
手口③	被害企業のサービスを攻撃し、停止へ
手口④	被害企業に身代金を要求
手口⑤	被害企業の取引先等に攻撃を連絡し脅迫

●全世界で被害が4,800件？

データが盗まれ、攻撃者のサイトでリーク(暴露)される被害は国内外で急増。2023年のリーク件数は全世界で約4,800件、うち国内組織(海外拠点含む)は約140件に上るとか。

＜平均被害額が4億円＞　サイバー対策の英ソフォスが24年1～2月に14ヵ国のＩＴやセキュリティ責任者5,000人に行った調査によると、ランサムウェアの被害を受けた組織では、自社内の半分近い端末が暗号化され使用不能に。被害により発生した復旧費用や逸失利益の総額は平均273万ドル(約4億4,000万円)で、23年調査から1.5倍に急増。

●ランサムウェア首謀者を特定？

被害規模が最大級とされるランサムウェア集団「ロックビット」を巡り、日米欧の捜査当局がロシア人の首謀者を特定。世界中の企業などから脅し取った身代金は5億ドル(約775億円）。

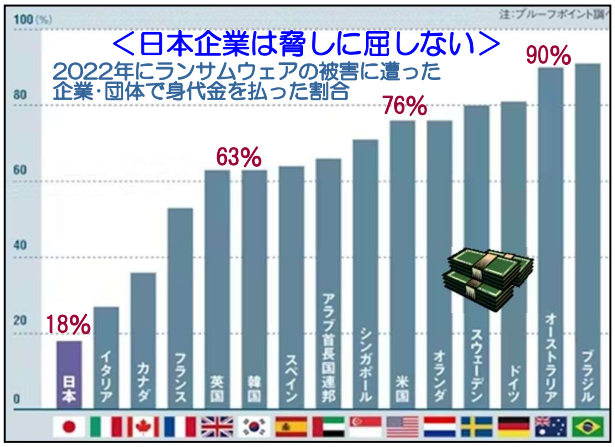
＜報奨金、最高1,000万ドル＞　米司法当局は起訴後、首謀者の身柄拘束ができておらず、逮捕や有罪判決につながる情報に最高1,000万ドル(約15億円）の報奨金を提示している。

●身代金、払わないとどうなる？

KADOKAWAは攻撃を受けてから1ヵ月以上過ぎた今も、完全復旧には至っておらず、全容解明には至っていません。ある調査によると、日本企業では１回目の身代金支払いで復旧できた企業はわずか17%で、それ以外はその後に追加要求されているようです。

●サイバー攻撃に屈しない日本企業

米の情報セキュリティー会社によると、22年に被害に遭った日本企業や団体のうち、身代金の支払いに応じた割合は18%で、他の国を大きく下回っています。



中小企業もサイバー被害

●こんなにあるサイバー攻撃

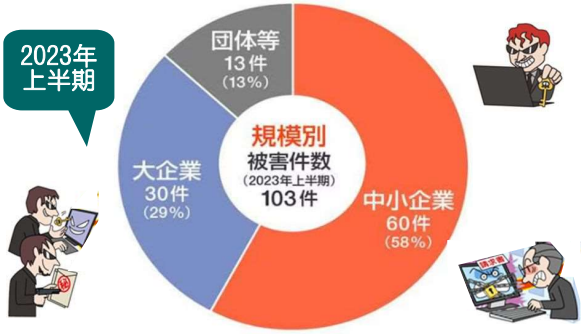
＜短期間でもこれだけニュースに！＞

6/29	KUMON：委託先事業者のﾗﾝｻﾑｳｪｱ被害で会員と指導者の個人情報が漏えい
7/4	愛知県**豊田市**：委託業者のｻｰﾊﾞｰがﾗﾝｻﾑｳｪｱに感染し、延べ42万人分の個人情報が流出
7/5	JAXA：去年のｻｲﾊﾞｰ攻撃での情報漏洩認め謝罪、外部機関との事業情報も流出
7/5	情報処理ｻｰﾋﾞｽの**ｲｾﾄｰ**(京都市)：ﾗﾝｻﾑｳｪｱに感染、自治体や企業などの約150万人分が流失
7/9	**東海信金**ﾋﾞｼﾞﾈｽ(名古屋市)：業務委託先のｻｰﾊﾞｰやPCがﾗﾝｻﾑｳｪｱに感染し顧客氏名が流出
7/10	**東京海上HD**3社：損害査定を委託している会計事務所のｻｰﾊﾞｰがﾗﾝｻﾑｳｪｱに感染と発表
7/10	**富士通**：3月のｻｲﾊﾞｰ攻撃で社内のPCがﾏﾙｳｪｱに感染した件で、情報漏洩の調査結果を発表

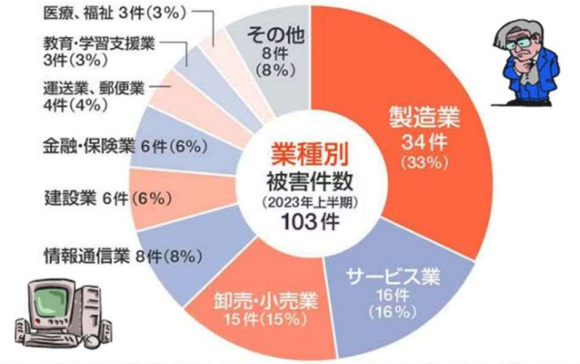
●ランサム被害、6割が中小企業？

2023年上半期に警察庁に報告された「企業・団体等におけるランサムウェア被害」の件数は103件に上り、うち中小企業が約6割を占めていることが分かりました。ＩＰＡ(独立行政法人 情報処理推進機構)によると、「情報セキュリティ10大脅威」ではランサムウェアの被害が3年連続で1位に。

＜ランサムウェア被害の企業・団体等の規模別報告件数＞



＜ランサムウェア被害の企業・団体等の業務別報告件数＞



(注)図中の割合は小数第1位以下を四捨五入している　(出所)「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」(警察庁)を基に東洋経済作成

●調査・復旧に5,000万円以上？

実際にサイバー攻撃を受け、被害が生じてしまうとダメージは大きく、操業停止、金銭損失の他、とりわけ大きなリスクは被害の範囲が取引先にまで及ぶことです。警察庁の調査によれば、復旧に要した時間で最も多かったのは「1週間以上から1ヵ月未満」で、中には「１ヵ月以上」、「復旧費用が5,000万円以上」の回答も。

＜中小企業が狙われる理由＞　中小・零細企業がターゲットになるケースが目立つ。攻撃者集団は攻撃先を絞らず、広域にランサムウェアによる攻撃を仕掛けている他、サプライチェーン(供給網)攻撃の足掛かりとして、セキュリティが脆弱な中小・零細企業が狙われている。

●「サイバー警察局」の誕生！

2022年4月、警察庁はサイバー犯罪対策強化を目的とした新組織「サイバー警察局」と、重大事件の捜査を担う「サイバー特別捜査隊」を発足させました。狙いは、日本企業や病院などでのランサムウェアなどの被害の深刻化と、捜査体制の強化で高まる脅威に対応するため。公式サイトでは、ランサムウェアやフィッシング詐欺の相談・対応事例を発信しています。