徹底討論 これからのデータ基盤

ランサムウェア対策に効く2つのアプローチ

コロナ禍に乗じたサイバー攻撃が増えている。特に、ランサムウェアの被害は深刻だ。重要なデータを暗号化されて人質にとられることは、企業にとって悪夢そのものだろう。では、ランサムウェアへの対策は、一般的なセキュリティ対策とは何が違うのだろうか。2020年10月に開催されたWebinarでは、NICTサイバーセキュリティ研究所 井上大介氏ら専門家が、ランサムウェア対策のバックアップに必要な条件を議論した。

コロナ禍で高まるサイバー脅威、ランサムウェアは“標的型”に進化

今回のコロナ禍は、企業のサイバーセキュリティにもさまざまな影響を及ぼしている。たとえば、「マスクが当選しました」といったコロナ禍に便乗したフィッシングメールは急激に増加した。

また在宅勤務が増えたことで、自宅から会社に接続するときに利用するVPNプロトコルの脆弱（ぜいじゃく）性を突いた攻撃も増加している。データを暗号化して身代金を要求する「ランサムウェア」の脅威も引き続き高く、直近ではさらに高度化・巧妙化しているという。

情報通信研究機構（NICT）サイバーセキュリティ研究所 サイバーセキュリティ研究室 室長 井上 大介 氏は、次のように説明する。

「ランサムウェアでは有名なものとして、2017年5月に発生したWannaCry（ワナクライ）が挙げられます。

国立研究開発法人 情報通信研究機構（NICT）
サイバーセキュリティ研究所
サイバーセキュリティ研究室 室長
井上 大介 氏

NICTの観測でも、日本国内で1日に2000ホストが感染する勢いでした。このWannaCryは不特定多数をターゲットとする“ばらまき型”でしたが、最近では特定の企業を狙った“標的型ランサムウェア”が登場しています」（井上氏）

ランサムウェアの怖いところは、要求される身代金だけではない。データが使えなくなるため、事業が止まってしまう。さらに、回復のためのコスト、企業のブランド毀損（きそん）も含めると、そのダメージは計り知れない。

アンケートから見えてくるランサムウェア対策の実態

では、企業はランサムウェアに対してどのような対策をとれば良いのだろうか。

Webinarでは視聴者に対してアンケートで、「近年のランサムウェアの流行は自社のセキュリティ対策にどのような影響を与えたか」について尋ねた。

アンケートの結果は、「専用の対策は実施していないがセキュリティ施策は強化した」が45.6%で１位だった。(図１)

「事実、ランサムウェア専用の対策は難しいのが現状です。ランサムウェア攻撃は、システムに侵入し、感染を拡大し、ストレージを見つけて暗号化……と、複数の攻撃・テクニックで構成されているためです」（井上氏）

セキュリティ対策全般で重要となる考え方といえば、NIST（アメリカ国立標準技術研究所）の「サイバーセキュリティフレームワーク（Cyber Security Framework：CSF)」だ。これは、企業がセキュリティ対策を考える指針となるもので、「識別」「防御」「検知」「対応」「復旧」の５つから構成される。

日本アイ・ビー・エム システム事業本部 ソリューション事業部 ハイブリッドクラウド & AI ストレージセンター IT スペシャリスト 澤田 知子は、次のように述べる。

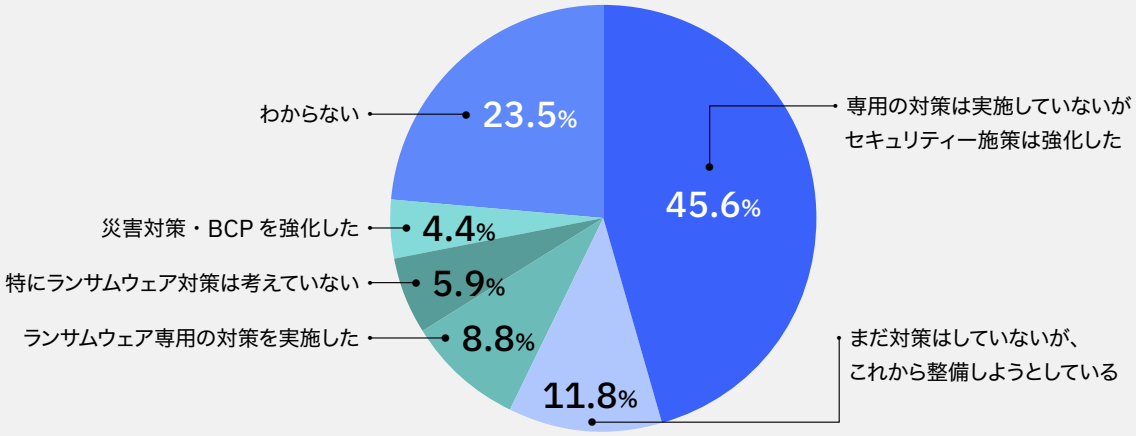
「CSF はもちろんランサムウェア対策としても有効です。

日本アイ・ビー・エム
システム事業本部
ソリューション事業部
ハイブリッドクラウド & AI ストレージセンター
IT スペシャリスト
澤田 知子

ただ、通常のセキュリティ対策では『防御』『検知』『対応』の３つにフォーカスが当たりがちなのに対し、ランサムウェア対策では『検知』と『復旧』も含めたサイバーレジリエンシーという観点で対策を考えることが重要になります」（澤田）

ランサムウェア対策では、災害対策との違いも意識しなくてはならない。災害対策としてデータのバックアップをとっている企業は多いが、澤田は「災害対策のバックアップが、必ずしもランサムウェア対策になっていないケースが少なくありません」と指摘する。

(図1) 近年のランサムウェアの流行が、自社のセキュリティ対策にどのような影響を与えたのか



ランサムウェア対策のバックアップに必要な「エアギャップ」と「イミュータブル」

ランサムウェアは、データを暗号化して身代金を要求する。したがって、災害対策用のバックアップデータがあれば、それを書き戻すことで問題を解決できるのではないか、という考え方もあるだろう。しかし、現実はそれほど簡単ではない。

日本アイ・ビー・エム システム事業本部 ソリューション事業部 ハイブリッドクラウド & AI ストレージセンター IT スペシャリスト 杉浦 勝 は次のように説明する。

「残念ながら、せっかくバックアップしているのに、バックアップ先も暗号化されてしまうケースは少なくありません。

サイバー攻撃はいつ発生したのかが分かりにくいため、攻撃に気づく前にバックアップサイクルが一周すると、バックアップも含めてデータがすべて暗号化されてしまうのです」（杉浦）

Webinar では、ここで再びアンケートを実施し、「ランサムウェアを意識したデータ保護、復旧を実施するにあたっての懸念」を聞いた。最も多い回答は「コスト」（36.8%）、次いで「適切なバックアップの範囲、世代数、頻度が分からない」（21.1%）だった。（図2）

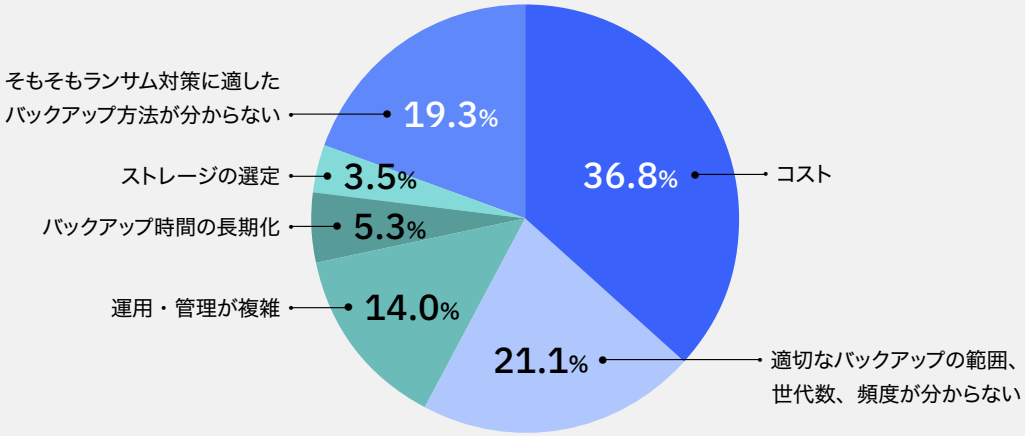
「コスト」がトップになるのは、ある意味当然としても、「適切なバックアップの範囲、世代数、頻度が分からない」が 2 位になったのは、発生時期と影響範囲の特定が難しいサイバー攻撃の特性を反映しているといえそうだ。

日本アイ・ビー・エム
システム事業本部
ソリューション事業部
ハイブリッドクラウド & AI ストレージ
センター
IT スペシャリスト
杉浦 勝

では、ランサムウェア対策のバックアップに必要な条件は何か。杉浦氏は「エアギャップ（Air Gap）」と「イミュータブル（Immutable）」という 2 つのキーワードを挙げる。

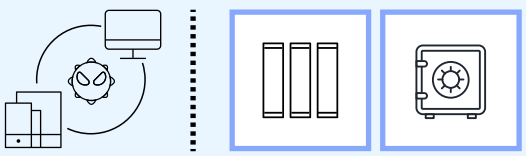
「『エアギャップ』とは、ネットワークにつながっていない物理的に隔離されたエリアにデータを置いてデータを保護する考え方です。一方の『イミュータブル』は “ 改変不能 ” という意味で、いったん書き込んだら改変が不可能な保管先にデータを保存し、保護する考え方です」（杉浦）（図3）

（図2）ランサムウェア対策を意識したデータ保護・復旧を実施する際の懸念



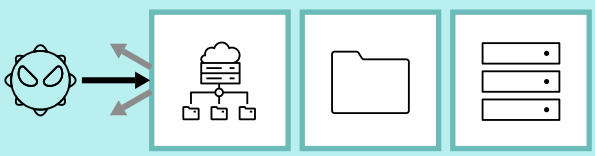
（図3）安全な保管先は「エアギャップ」と「イミュータブル」

エアギャップ（Air Gap）
物理的に隔離されたエリア



・オフラインのテープ
・サーバー・アクセスから完全分離された
隔離エリア（DS8000 セーフガードコピー）

イミュータブル（Immutable Storage）
改変不能（Immutable）な保管先



・Immutable オブジェクト・ストレージ
・Immutable ファイル・システム
・WORM テープ
*WORM：Write Once Read Many

「エアギャップ」や「イミュータブル」の考え方に基づいて開発された製品は、すでに市場に流通している。代表的な例がテープ(LTO)だ。データをテープにバックアップし、オフラインで保管するのは「エアギャップ」の実現に相当する。IBM でも、小規模からエンタープライズレベルまで、さまざまなテープ製品を提供している。

また、テープに関しては、一度、書き込んだら改変できない「WORM（Write Once Read Many)」という「イミュータブル」な性格を持つテープも存在する。テープの最大のメリットは容量当たりの単価が安いことだが、澤田によれば、WORM テープも一般のテープとそれほど変わらない低コストで利用できるということだ。

「イミュータブルなストレージには、WORM テープのほかにも、オブジェクトストレージ、ファイルストレージなどの種類があります。また、イミュータブルなストレージをクラウドで利用するサービスとして『IBM Cloud Object Storage』も提供しています」（澤田）

一方で、近年は「エアギャップ」や「イミュータブル」の仕組みを搭載しているストレージ製品も少なくない。最も多いのが、設定によってコピー先をアクセス不可にしたり改変不能にしたりする機能を備えた製品だ。ただしこれらの製品は、攻撃者によって設定を操作されるリスクがある。また、バックアップできる世代数が少なく、短期間でバックアップサイクルが一周する製品も少なくない。

こうした課題を、IBM のストレージシステム「IBM DS8900F」に搭載された「セーフガード・コピー」という機能は解決する。

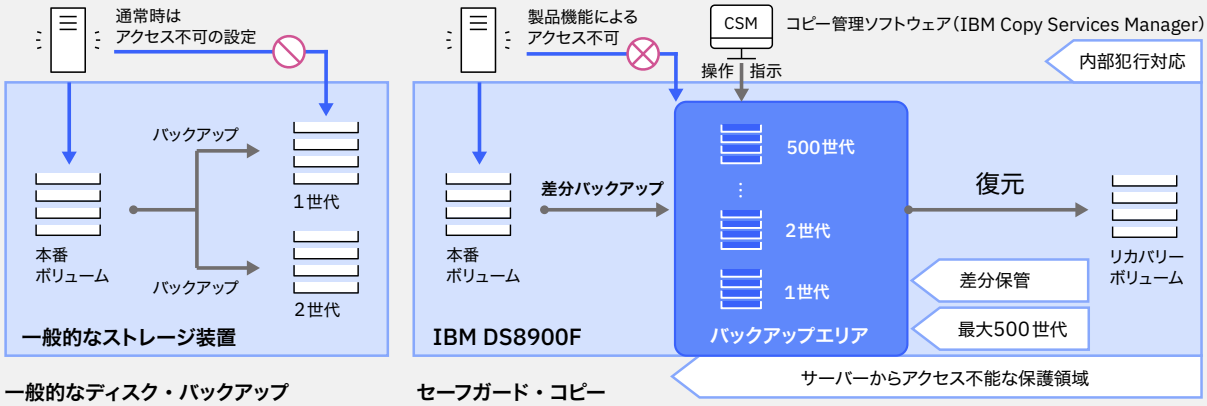
「セーフガード・コピーは、ストレージ筐体（きょうたい)内部にサーバからアクセスできない保護領域を設けて、『エアギャップ』を実現する機能です。さらに、差分のみを保管することで、最大 500 世代のバックアップをとることが可能です」（杉浦）（図4）

また、バックアップソフトである「IBM Spectrum Protect」には、攻撃をいち早く検知する機能が搭載されている。これにより、バックアップサイクルが一周して、正常なデータが失われるリスクを低減できる。

「Spectrum Protect では、差分を確認するために、バックアップ前にデータをスキャンします。そこで、差分データの急激な増加といった異常を検知すると、ユーザーに通知する機能が用意されています。侵入を検知するセキュリティ製品と組み合わせて活用すれば、早期発見に役立ちます」（澤田）

（図4）一般的なストレージのバックアップ機能と IBM DS8900F のセーフガード・コピーの違い

ディスクでのエアギャップ、改変不可対応



一般的なディスク・バックアップ

・設定によるアクセス不可（エアギャップ)、改変不可（Immutable）
・容量、機能的に取得世代が限られる

セーフガード・コピー

・製品機能（エアギャップ）によるアクセス不可、改変不能（Immutable）
・差分による最大 500 世代のバックアップ取得可能
・セキュリティ機能の強化により内部犯行対応可能

物理的な破壊と論理的な破壊の両方に対応した金融機関の事例

セーフガード・コピー機能を搭載したストレージ製品は、すでにランサムウェア対策として導入が進んでいる。杉浦は、金融機関の事例を挙げる。

「ある金融機関は、基幹システムの物理的な障害に備えて、筐体間コピーの仕組みを構築していました。ところが、別の周辺システムがサイバー攻撃を受けて、データの論理破壊のリスクに気づきました。そこで、基幹システムに弊社のストレージ製品を導入し、セーフガード・コピーによる 1 日 1 回のバックアップと 3 日分のデータ保持を行い、論理破壊にも対応できる仕組みを構築したのです」（杉浦）（図5）

ランサムウェア対策としては、この金融機関のように、既存のバックアップの仕組みで対応できるかどうかを再検討することが重要になるだろう。また、サイバー攻撃の最新動向をウオッチすることも大切だ。

「ランサムウェア攻撃は、日々進化しています。最近は、データを暗号化したうえでデータを外部に持ち出し、『身代金を払わないとデータを公開する』と脅迫する新たな手口も登場しています。したがって、今後はデータをいかに攻撃者から見えなくするかも重要になるでしょう」（井上氏）

企業が重要なデータを持っているかぎり、そのデータは間違いなくサイバー攻撃のターゲットになる。それが事業継続に関わる重要なデータであればあるほど、リスクは高まるだろう。一方で、システムへの侵入を 100%防げないのも現実だ。

だからこそ、たとえ侵入を許し、データを暗号化されたとしても、確実に元に戻せる仕組みを持つことが求められる。その実現に、ぜひ IBM のテクノロジー・製品を役立ててもらいたい。

※当掲載内容は、2020年 11月にビジネス＋ IT に掲載されたものの転載です。肩書きや記載された情報は当時のものです。

(図5) セーフガード・コピー事例：金融サービス業の高可用性システム

セーフガード・コピーでデータの論理破壊対策を行った金融機関の例

・ディスク筐体の物理障害に備え、筐体感同期コピーを実施
・データの論理破壊に備え、両サイトでセーフガード・コピー（SGC）を実施

・本番データは約30TB
・セーフガード・コピーによる 1日1回のバックアップを実施、3日分保持

詳細はこちら https://www.ibm.com/jp-ja/it-infrastructure/solutions/security

〒103-8510 東京都中央区日本橋箱崎町 19-21