つなごう。驚きを。幸せを。
docomo Business

NTTドコモビジネスの社員が語る

“ランサムウェア対策、生成AIで変わる攻撃と今取るべき対策とは“

エバンジェリスト
城　征司

昨今、企業に対するランサムウェア攻撃の被害事例が相次いで報じられており、対策について頭を悩まされている企業も多いのではないでしょうか。最新のランサムウェア攻撃の実態と、それを防御するためには企業はどのような対策をとっていくべきなのか、そしてこれから先のサイバーセキュリティ対策について、NTTドコモビジネスのセキュリティ分野のエバンジェリストである城さんにインタビューを行いました。

NTTドコモビジネス株式会社
エバンジェリスト
城　征司

NTTドコモビジネス入社20年。
一貫してサイバーセキュリティ分野に携わり、大企業のお客さまへ、ソリューションの提案や導入、またそのセキュリティのお悩みを解決するためのコンサルティングといった業務に従事している。

頻発するランサムウェアの被害 いったい“今”何が起きているのか

インタビュアー：最近、大企業におけるランサムウェア被害が頻繁しています。今何が起きているのでしょうか。その背景やランサムウェア被害の特長を教えてください。

城：2025年の秋に大きなランサムウェアのインシデントが起き、社会全体にランサムウェアに関する認知が広がったと思います。気づかれたと思いますが、ランサムウェア攻撃の被害は、攻撃を受けた企業だけにとどまらず、社会経済全体に影響を与えるということが特長です。
昨今、1つの企業だけでビジネスをするのは難しく、製品を売る会社、製品の部品を作る会社、部品や製品を配送する物流サービスの会社と、さまざまな企業が連携しているため、ある企業でランサムウェア被害がでるとサプライチェーン全体に影響が及ぶのです。
　実際にインシデントが起きた事例では、あるランサムウェア被害を受けた会社の子会社の物流サービスを利用していた関係で、一見すると全く関係がないと思われていた企業のネットストアの受発注システムが停止する、という影響が出ました。ニュースを見て驚いた方もいたかと思いますが、被害を受けると影響範囲そして損失額が甚大になるのです。

さらに、攻撃者側の観点から、特長が2つあります。まず1つ目は二重脅迫という攻撃手段です。二重とは何かというと、ランサムウェアはデータを暗号化し、もとに戻す鍵が欲しければお金を払ってくださいというものなのですが、それだけではなく、もしお金を払わないとこのデータを一般に公開するぞと脅します。暗号化したデータは戻らないし、お金を払わないと世の中に個人情報や特許情報などの機密情報が公開されてしまう。こういった二重の観点で攻撃する手法です。2つ目の特長は、ランサムウェア攻撃の入り口の8割以上が、近年社会に広まってきたリモートアクセスの仕組み、認証の不備や脆弱性が原因となり、攻撃者がそこから内部に侵入しているということです。このリモートアクセスの仕組みの管理方法が良くない企業が非常に多いため、リモートアクセスの脆弱性は、まず最初に対応しないといけない領域だと考えています。

ランサムウェア対策の1つである EDRは対策として十分なのか

インタビュアー：ランサムウェア対策の1つとしてEDRによる対策があると思いますが、EDRをいれておけば、まずは十分なのでしょうか？

城：EDRを入れたら十分かというよりは、EDRを適切に入れられていない環境が多い方がまず問題だと思っています。例えば、PCにはEDRを入れました、しかしサーバーには入れてませんという環境がかなり多いです。最近あった大きなランサムウェア被害のケースでもそうでしたし、ランサムウェア被害ではないですが、数年前に弊社が受けたサイバー攻撃もEDRを導入できていなかったサーバーに対する検知が遅れ、被害が大きくなったという経緯があります。

また、せっかくEDRを入れても、入れっぱなしではダメで、監視が大切です。監視体制は人間がやることになるので、例えば平日の昼間だけにしますという会社もあります。そうなると、休日や夜間は監視していないことになり、当然攻撃者は監視されていないところに忍び込むため、その間の攻撃に気づけなかったというような事例もあります。

EDRを入れた後、そしてしっかり運用していくことがとても重要です。仮にしっかり入れたとしても、EDRの検知を回避したり、EDRを無効化するような高度な攻撃方法もあります。そのためEDRは大事だけれども、実際には複数の対策を積み重ねて、相互に補完するような形で組み合わせて入れるということがとても重要になってくるのです。

バックアップを取得していれば ランサムウェア対策は大丈夫なのか

インタビュアー：バックアップを取得していれば、ランサムウェアの被害にあっても、復元できて大丈夫なのではと思いますが、いかがでしょうか。

城：ランサムウェア被害を受けた企業のうち、実は約90%の企業はきちんとバックアップを取っていたのですが、そのうち90%の企業のうちの約85%は、実はそのバックアップからすべてのデータをきちんと復旧できなかったのです。ただバックアップを取るだけではうまくいかなかったということですね。

では、それはなぜかというと、いろいろな要因は考えられますが、まず1つは、バックアップのデータ自体がランサムウェアに暗号化されてしまうということです。せっかくバックアップをとって置いていても、バックアップまで丸ごと攻撃されたら何の意味もないのです。そのため、バックアップを取るときは隣に置いておけば良いというわけではなく、攻撃者の攻撃が届かないようなネットワークが隔離されたような場所に置くというような対策が必要になります。加えて、復旧する前に、そのデータ自体がすでにランサムウェアに感染していないかチェックしておかないと、復旧した瞬間にまた暗号化されてしまうというように、繰り返してしまうので、ランサムウェアの感染チェック機能というのも必要になってきます。

2つめは、仮に正しくバックアップを取れていたとしても、復旧するのが難しいということです。企業のデータはさまざまなシステムが多種多様にありますので、昨日のバックアップと1週間前に取ったバックアップ、これを両方同時に復旧したら、もしかしたら生産データや受発注データなど、整合が取れなくなってしまうかもしれないのです。そのため、事前のバックアップの設計や、データがきちんと復旧できるかという訓練がすごく大事で、これができないとバックアップを取得していても上手く復元できなかったという悲しい結果につながってしまうのです。

正しい対策を講じるには攻撃者の視点を理解することも重要

インタビュアー：サイバー攻撃をより深く理解するためには、攻撃者を知ることも重要かと思います。攻撃者はどのような観点で企業を狙っているのか、教えていただけますか。

城：はい。わかりました。まずは、攻撃者も AI 活用によるDXが進んでいるということが挙げられますね。そのため、これまでは時間をかけて自分の頭を動かしたり、手を動かしたりしてやってきたことが、AIを使って一気に省力化できるのです。そのため、広範囲でしつこい攻撃というのも、今までよりも簡単にできるようになってしまいます。

また、これまではあと攻撃者が外国人の場合、日本語は理解しにくかったのですね。ただ、生成AIのおかげで、日本語という言語の壁がすごく低くなりました。攻撃者にとっては日本の情報を入手しやすくなったり、日本に合わせた攻撃を仕込みやすくなったということが考えられます。必ずしもランサムウェアだけを指さないのですが、フィッシングメールの攻撃も以前は、日本語が明らかに不自然でしたが、今は自然な日本語になっています。こういった観点で今後、日本に対するランサムウェア攻撃、サイバーセキュリティに関する攻撃が増えてくる可能性があると思っています。

インタビュアー：では、防御する側はどのように対策を講じるべきでしょうか。

城：相手はAIを使って攻撃を進化させているのに、我々防御する側が一生懸命に手動で対応するというのは、無理なのです。そのため、防御する側も、AIを活用したセキュリティ対策を整えていくというトレンドになっています。

例えば、攻撃を見つけるための装置があるのですが、これが記録をログとして残してくれます。このログを今までは人が手動で分析していましたが、最近はAIが自動で分析をしてくれます。また、何かリスクが発見された際に、現場のエンジニアのリーダー向けのレポートもあれば、あるいは技術に必ずしも詳しいとは限らない経営層向けのレポートを作る必要があるかもしれません。それを今まで人が書いていたのですが、これをAIで書くようになるとかですね。

あるいは、セキュリティ対策にとって脆弱性をきちんと管理することは重要になりますが、結構大変なので、この脆弱性を管理するところもAIに任せてしまうというのもあります。

また、攻撃を受けた後に、今度は同じ攻撃を受けないように穴を塞ぎたいわけなのですが、その穴を塞ぐような設定変更をする、こういったところを今まではセキュリティを担当する部署として、CSIRTやSOCと呼ばれる部署があったのですが、こうしたセキュリティ部門や、あとはシステムを管理する情報システム部門などの関係部署でさまざまなAIを導入して、AIが活躍するようになってくるかなと思います。 そうなるともう、AI対AIの時代になってくるというふうに考えております。

これからのサイバーセキュリティ対策トレンドをよみ将来的な脅威を考える

インタビュアー：今後のセキュリティ対策はどのようになっていくと思いますか。

城：その観点でいうと、４点注意していきたいところがあります。

城：1つは先ほども申し上げたサプライチェーン。1社セキュリティの対応が弱いところがあったら、まずそこから侵入します。サプライチェーン全体がネットワークでつながっているようなことがあれば、そこを起点に攻撃者はどんどん中に入っていきます。そのため、自社のセキュリティ対策だけをやれば良いわけではなくて、特に大企業のお客さまの場合、サプライチェーン全体のセキュリティ対策が重要になってきます。

関連して、2026年からセキュリティ対策の企業の評価制度が始まる予定です。自社のセキュリティ対策を５段階で評価するような仕組みになっていて、セキュリティ対策をしっかりしたい企業から見ると、対策レベルの低い会社とは取引をしないという選択肢も出てきます。 そうなると、今後、セキュリティ対策というのはただのコストではなくて、ビジネスに参加するための必須ライセンスになってくる、そういう時代が来るのではないかと思っています。

2つ目は、OTとIoTですね。今まで工場の中だけで動いていた機械がインターネットにつながるようになり、工場で取得したデータをインターネット上のクラウドサービスで分析して、また生産プロセスの改善につなげるといったDXがこれからさらに進んでいきます。このOT/IoTのセキュリティ対策が非常に課題になっています。例えば工場の機械はできるだけ止めずにビジネスが継続できるのが理想です。この工場の生産装置が止まってしまうと、ビジネスに多大な影響を与えてしまうので、OT/IoT機器は、一旦入れたら5年とか10年そのままというケースがあります。その間に脆弱性が出ても、修正するためのファイルを適用することが、PCに比べると判断が難しい場合が多いです。結果的にそこが隙になってしまうというのが、OT/IoTの難しさだと思います。

続いて 3つ目はAI です。攻撃をAIで効率化する、守る側も防御をAIで効率化する、その観点でここまでAIについて話しました。我々はセキュリティに限らず、いろいろな企業で今、AIあるいは AIエージェントの利用が進んでいると思います。 将来的には、何百何千のAIエージェントが同時に動いたり消えたり発生したり、あるいはそのうち、社員と同じように、判断して行動して、会議にも出席するデジタルワーカーと言うのですが、こういったものが出てくる社会になっていくと言われています。すると、攻撃者はこのAIを狙った攻撃をしかけます。AIを攻撃してくるAIをAIで守るみたいな話になるのですが…、実はそのAIが攻撃対象になった場合、防御方法が、人間向けのセキュリティ対策とはまた少し変わってくるのです。いざAIが何百何千と社内に導入された時に守る方法が分かっていないと攻撃者から見ると格好の隙になります。そのため、実は今、AIの利活用を進めていくのと同時に、AIを守るためのセキュリティを並行して考えていくことが非常に重要です。

最後4つ目は、少し先の世界の話かと思いますが、OT/IoT と AI を組み合わせたフィジカルAIです。フィジカルAIは、現実世界にある工場の生産装置のようなロボットを操作するAIのことを言います。工場で荷物を運搬したり、製品の検品とか組立を行うロボットがAIで高度化していきます。あとは自動運転の車ですね。 自動運転の車のAIが周囲の映像を見て、道路状況、混雑具合、歩行者などの周辺状況を見て、ハンドル操作やブレーキ操作を自動で行うといったことがあります。例えば、道を走っている自動運転車が一斉に攻撃を受けたら大混乱が起きると思いますし、ただビジネスが止まるというよりは、もう人間の生命に大きく関わるような事態にもなりかねません。その点でいうと、OT/IoTに対するセキュリティ、そしてAIに対するセキュリティというのを今しっかりやりながら、数年先に来るフィジカルAIに対するセキュリティといった観点も考慮して、セキュリティ対策を考えていく必要がある時代が来ていると言えます。

お問い合わせ

NTTドコモビジネス株式会社

サイト **https://www.ntt.com/business/services/crx-solution.html**