第二回 意見交換会「深刻化するランサムウェア被害とその対策」サマリー

1. 開催趣旨と講義概要

昨今の DX やテレワークの普及により生産性が向上する一方、その裏で巧妙化するサイバー攻撃、特にランサムウェアのリスクが高まっています。本会では、最新の手口と中小企業がとるべき現実的な対策について、講師の梶原氏によるレクチャーと参加企業による意見交換が行われました。

主な講義ポイント

- **攻撃の組織化（RaaS/IAB）：** ランサムウェア攻撃は分業・組織化が進んでおり、攻撃ツールや認証情報が安価に売買され、誰でも攻撃者になれる状況にある。
- **最新の侵入手口：**
    - VPN 機器やリモートデスクトップの脆弱性を突いた侵入が過去の被害の多くを占める。
    - AI を用いた精巧なフィッシングメール、QR コードを用いた「クイッシング」、偽の警告画面を表示する「サポート詐欺」、認証画面を装い不正コマンドを実行させる「ClickFix」など、手口が多様化している。
- **リスクへの 4 つのアプローチ：** 「回避・低減・移転・保有」の観点から対策を考える。特に「発生頻度の低減（脆弱性対策・多要素認証）」と「被害の最小化（バックアップ・初動対応）」が重要。
- **初動の鉄則：** 被害発生時は、ネットワークを切断する一方で、**「電源オフ再起動は絶対してはならない」**。メモリ上のログなど証拠が消失するためである 。

---

2. 意見交換会・質疑応答ハイライト

参加者は主に中小規模の事業者（製造業、システム開発、サービス業等）であり、リソースが限られる中での現実的な対策や、従業員の意識改革に関する悩みが多く寄せられました。

① セキュリティガイドラインと現実のギャップ

IPA（独立行政法人情報処理推進機構）などが示すガイドラインの要求水準が高く、中小企業としてどこまで対応すべきかという切実な悩みに対し、議論が交わされました。

- **製造業 A 氏：**

「正直 IPA さんとか出している中小企業の指針とかって相当レベルの高いことだと思ってるんですよ。あれに満たなくてもまあなんていうか現場というか監査員とか行政も含めて、まあしょうがないよねって言ってもらえるんだろうかっていう。」

- 講師回答：

全てを網羅するのは困難であるため、取引先の重要データなど「ここだけは守る」という資産にメリハリをつけて対策を行うこと、また説明責任を果たせるよう最低限の対策（脆弱性対策、教育、バックアップ）を行うことが現実的であるとの助言がありました。

② クラウド・テレワーク環境の盲点

自社サーバーを持たずクラウドを利用している場合や、自宅のネットワーク環境に関するリスクについての認識共有が行われました。

- **システム開発 A 氏：**

「ローカルといいますか。自分の PC に残さないという運用を基本としているんですが。そういった場合でも、まあ先ほどおっしゃっていたように、その ID、パスワードによって。そういったクラウドに入られたり、データにアクセスされたりといった可能性はあるかと思いまして。」

- 講師回答：

クラウドであっても ID/パスワードが漏洩すれば第三者がアクセス可能となるため、多要素認証やパスワードの使い回し禁止が重要です。また、テレワーク環境においては、**「自宅のパソコンとか自宅のルーターとかの ID、パスワードをまだまだ変えていないというのが国内でも散見されて、そこも入り口になっている」**と指摘がありました。

③ 従業員教育と「自分ごと化」の難しさ

ニュース等で被害を知っていても、従業員個人が脅威を「自分ごと」として捉えるこ

との難しさが課題として挙がりました。

- **システム開発 A 氏：**

「結構ニュースにはなるものの、自分ごととして現実的に受け止められているかっていうのは結構人によって違う。そういった点で何かご知見がありましたらよろしいでしょうか？」

- 講師回答：

動画視聴だけでは実感しにくいため、**「標的型メールの訓練」**を実施し、実際に引っかかる体験を通じて危機感を持たせることが効果的であると推奨されました 。

④ 出張先・移動中のセキュリティ（Wi-Fi・BitLocker）

フリーWi-Fi の危険性や、紛失時の対策についても具体的な質問が出ました。

- **製造業 A 氏：**

「フリーワイファイがそもそも危険だっていう理由って何なんだっけなって思って。」

- 講師回答：

暗号化レベルが低いフリーWi-Fi は通信内容を盗み見られるリスクがあるため、テザリングの利用が推奨されました。また、紛失・盗難リスクへの備えとして、Windows 標準の暗号化機能について**「ビットロッカーはオンにしてください」**と強く推奨されました。

⑤ 万が一の際の「ログ」の重要性

被害に遭った際、復旧や原因究明のために何が必要かという点も確認されました。

- **製造業 A 氏：**

「もしランサムウェアとかの被害にあったときにそのログが端末ごとに確認できた方が、あの復旧とかには早いですか？」

- 講師回答：

「絶対にログをログがないと何もできないです。」 操作ログを含めて取得していることを周知するだけでも、内部不正への抑止効果になると強調されました。

---

3. まとめ

本会を通じて、中小企業においては「完璧な対策」を目指すあまり疲弊するのではなく、攻撃のトレンドを理解した上で、以下の 3 点を優先的に実施し、説明責任を果たせる体制を作ることが重要であると結論付けられました。

1. **ネットワーク機器の脆弱性対策**

   （管理者パスワードの変更、ファームウェア更新等）

2. **最新の攻撃手口の共有と教育**

3. **オフラインバックアップとリストアの検証**