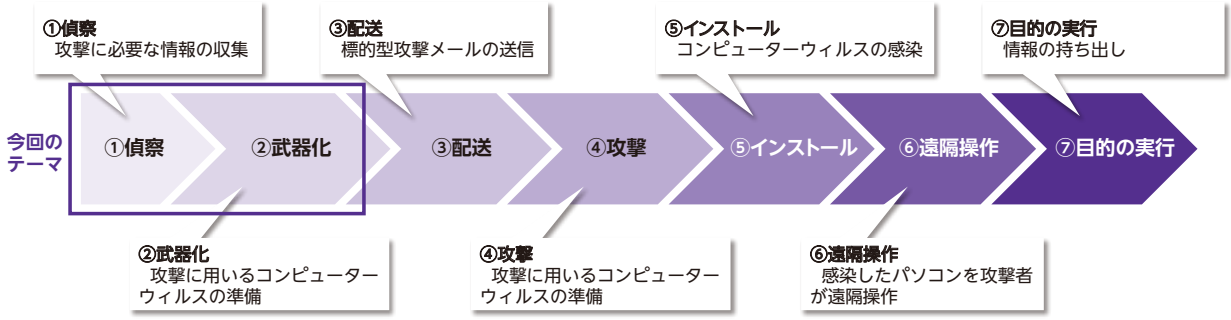
情報セキュリティコラム 第2回

Information Security COLUMN

サイバー攻撃の流れで語る! 今すぐできるサイバー攻撃からの防御方法!

独立行政法人 情報処理推進機構（IPA）様による情報セキュリティコラムの第2回は、「情報資産」をテーマにご紹介いたします。

【サイバーキルチェーン（7段階）】



■攻撃者に隙を与えず情報資産を守る！

今回は、まずみなさんの会社を守るために「情報資産とは何か」を改めて考えていきましょう。

みなさんは標的型サイバー攻撃という言葉を聞いたことはありますか？標的型サイバー攻撃とは企業や組織に所属している従業員を狙って情報を盗み、その情報からコンピューターウィルスを作成し送り込む攻撃手法を指します。

標的型サイバー攻撃としてよく知られる攻撃手法のひとつに「標的型メール攻撃」があります。ご存知の方も多いかと思いますが、日本でも2019年12月から「Emotet（エモテット）」と呼ばれる実在の人物（メールへの返信者）を騙る内容の標的型攻撃メールが多くの企業や組織で確認されています。また2022年４月から、Emotet感染の新たな手口が確認されるなど標的型攻撃メールは日々進化しており、その都度対策が必要となっています。

■「偵察」と「武器化」

では、そのような標的型サイバー攻撃のきっかけはどのようにして私たちの元へとやってくるのでしょうか？また、サイバー攻撃を仕掛けてくる攻撃者は、どのように私たちの組織のネットワークへ侵入してくるのでしょうか？そして、攻撃者から守るべき情報資産とはどこにあるのでしょうか？

ここでキーワードとなるのが、前回のコラムでお伝えした「サイバーキルチェーン」の「偵察」と「武器化」です。

例えば、私たちの生活の一部となりつつあるソーシャルネットワークサービス（SNS）は、使い方を誤ると攻撃者にサイバー攻撃の元となる個人情報を提供することになってしまいます。攻撃者は常にSNS等のインターネット上の情報を「偵察」しながら、サイバー攻撃に活用できそうな隙を狙っています。本名でSNSを利用している場合、投稿の内容や写真、位置情報、そしてみなさんの「本名」から所属企業を特定される危険性があります。また「セキュリティ部門は人手不足でしんどい」や「××というウィルス対策ソフトは操作性が悪い」と投稿しただけで、企業のセキュリティ対応レベルや使用しているウィルス対策ソフトを特定されてしまい、攻撃者にサイバー攻撃を仕掛ける際の情報を与えてしまいます。その情報が、サイバー攻撃で使われるコンピューターウィルス（武器）の作成を手伝ってしまうことになります。実は、みなさんの会社の情報資産は、サーバ上の機密情報だけではなく、こういった所にもあるのです。

■どうやって情報資産を守るのか?

では、情報資産を守るためにはどうしたら良いのでしょうか。ひとつは「SNSに会社の機密情報を書き込まない」等の社員教育です。当たり前じゃないか、もう何年もやってるぞ！そう思った方も少なくないかも知れません。ですが、こういった当たり前の積み重ねがみなさんの会社を守る大きなステップとなっているのです。

次回は、攻撃の侵入を防ぐ対策について紹介します。

（執筆）
IPA産業サイバーセキュリティセンター
中核人材育成プログラム修了生コミュニティー
叶（かなえ）会　飯島 安恵（アクセリア株式会社）