セキュリティアウェアネスとは何か

日本電気株式会社
宮崎　駿

はじめに

コロナ禍でフィッシングや標的型攻撃など、メールを利用して、受信者を起点に侵害をしようとする攻撃が増えています。攻撃が比較的容易なうえ、セキュリティ対策が疎かになりがちな「人」を対象とした攻撃であるため、組織はこれを大きな脅威として認識する必要があると思います。

このような、人を狙った攻撃への対策としてセキュリティアウェアネス（Security Awareness）というものがあります。

ここでは、セキュリティアウェアネスとは何かをNIST SP 800-16 Information Technology Security Training Requirements: a Role- and Performance-Based Model（以下、NIST SP 800-16）[1]とNIST SP 800-50 Building an Information Technology Security Awareness and Training Program（以下、NIST SP 800-50）[2][3]から考えていきたいと思います。

セキュリティアウェアネスとトレーニング

セキュリティアウェアネスの定義をNIST SP 800-16より引用します。

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.

理解のために、IPAが公開しているセキュリティ関連NIST文書の日本語訳の中でSP 800-16と関連の深いNIST SP800-50より引用します。

意識向上はトレーニングではない。意識向上を掲げる目的は、単純にセキュリティへ意識を向けることである。意識向上は、各自がIT セキュリティの問題を認識し、適切な対応を行うことを意図したものである。

引用にある通り、セキュリティアウェアネスとは人がなんらかのITシステムを利用するときに、セキュリティ上のリスクの理解や問題が発生したときの正しい対処を"意識"させるものだと解釈できます。

※NIST SP 800-16の内容・文脈から引用にあるAwarenessはSecurity Awarenessと同義だと解釈しています。

※以後、単にアウェアネスとしている場合はセキュリティアウェアネスも指していることとします。

言葉のニュアンスが難しいところではありますが、あくまで“意識”させるものであり、“できるようにすること”を主眼とするものではないというところがポイントだと考えています。アウェアネスは日本語訳では意識向上と訳されており、具体的なアウェアネスの取り組みとしてはポスターやチラシなどが挙げられています。このことからもあくまで意識付けの意味合いだということがわかるかと思います。

アウェアネスについて「意識付けだけでは対策として不十分ではないか」という意見があるかと思います。実際に“できる”ようにすることにはトレーニングが当てはまります。
NIST SP 800-16、およびNIST SP 800-50ではアウェアネスとトレーニング、教育の関係性について示されています。

トレーニングの定義をより簡潔にまとめているNIST SP 800-50より引用します。

Training strives to produce relevant and needed security skills and competencies.
トレーニングでは、関連性のある必要なセキュリティスキルおよび能力を生み出すように努める。

引用にある通り、トレーニングとは人に必要なスキルを習得させるように仕向けるものだと解釈できます。そのため、例えば従業員が標的型攻撃メール等に適切に対処できるようになってほしい場合はそのためのトレーニングを受けさせれば良いということになります。

アウェアネスとITセキュリティリテラシー

ここで、アウェアネスとITセキュリティリテラシーは何が違うのかという疑問があるかと思います。
ITセキュリティリテラシーについて、NIST SP800-16より引用します。

IT Security literacy refers to an individual's familiarity with—and ability to apply—a core knowledge set (i.e., "IT security basics ") needed to protect electronic information and systems.
（筆者訳）：ITセキュリティリテラシーとは情報とシステムを守るのに必要となるコアな知識体系（つまりITセキュリティの基本）を理解していて、それを実践できること。

アウェアネスはセキュリティの体系的な知識の理解と実践ができることを目指しているわけではなく、業務上のどういう場面でセキュリティのリスクの問題があり、そこでどういう対処が適切なのかを意識させることだと考えています。

ITセキュリティリテラシーは基本的な情報セキュリティの体系的な知識の習得ということなので、ITセキュリティリテラシーができているイメージとしては「基本的なセキュリティの教科書をやったから基本はおさえているよ」というのが近いと思います。

セキュリティアウェアネストレーニング

アウェアネスとトレーニングは異なるという話をしました。しかし、セキュリティアウェアネスというキーワードでWeb検索すると、様々な企業がセキュリティアウェアネストレーニングという名前で有償のトレーニングを提供していることがわかります。アウェアネスとトレーニングは違うもののはずですが、セキュリティアウェアネストレーニングとは何でしょうか。。

ここで、2019年に撤回されている資料（Retired Draft）のため参考情報となりますがNIST SP 800-16 Rev.1 A Role-Based Model for Federal Information Technology/Cybersecurity Training(3rd Draft)（以下、NIST SP 800-16RD）[4]よりアウェアネストレーニング（Awareness Training）の定義を引用します。なお、NIST SP 800-16RDではAwareness Trainingとは別にAwarenessとTrainingが定義されているため、AwarenessとTrainingという2つの用語を並べているというよりは、Awareness Trainingで一つの用語だと考えたほうが良いと思います。

Awareness Training – consists of instructor led, on-line courses, exercises or other methods that inform users of acceptable use of and risk to the organization's organizations systems.
（筆者訳）：意識向上トレーニング -インストラクター付きのオンラインのコースやエクササイズなどの方法で行われるトレーニングです、トレーニングでは組織のシステムで許容される操作とリスクについて示されます。

NIST SP 800-16RDはNIST SP 800-16を置き換える予定だった文書です。NIST SP 800-16は発行日が1998年であり今から20年以上前のものです。このことから一時はNIST SP 800-16の内容は現在の社会の状態に照らし合わせるとそぐわないと考えられていたと思います。

NIST SP 800-16が公開された当時としてはそれほどITシステムの利用者全員にセキュリティのトレーニングを強制するほどの社会状況ではなく、意識向上の取

り組みだけで済んでいたのだと思います。しかし、昨今のフィッシングや標的型攻撃メール、ソーシャルエンジニアリングなど、当時に比べて社会の状況は劇的に変化しています。これまでは意識付けだけで済ませていた内容について、スキルとして習得してもらう必要性が出てきたのだと考えています。そのため、それを表すための用語としてアウェアネストレーニングが定義されたのだと思います。

そして、このアウェアネストレーニングがセキュリティアウェアネストレーニングという名前で、有償で企業から提供されているということではないかと思います。

アウェアネスを向上させるにはどうすればいいのか

組織において、従業員のアウェアネスを向上させるにはどうすればいいのでしょうか。

その場の状況に応じてセキュリティに注意を向けることを人にさせるというのは、人の意識関わることであるため一朝一夕でできることではありません。
当人にセキュリティの関心があるのであれば、日常的にセキュリティに注意を向けることも考えられます。
しかし、セキュリティに関心がない人の方が多いのが現実だと思います。

関心の有無にかかわらず人のアウェアネスを向上させるためのポイントとしては「当たり前にする」ということだと考えています。
当たり前のことは関心があるかどうかに関わらず、当たり前のこととして意識すると思います。

では、当たり前のことにするためにはどうすればいいのでしょうか。

結論としては、ターゲットとする人にとって受け入れられやすい形で繰り返し伝えていくことだと思います。
例えば、NISC（内閣サイバーセキュリティセンター）はサイバーセキュリティ月間というキャンペーン[5]を行い、国民全体のアウェアネス向上に取り組んでいます。

このキャンペーンの中で取り扱われているポスターとバナーにアニメ作品が使われています。

これは、ターゲットとする人の多くがこのアニメ作品に関心があり、受け入れられやすいという想定の元、このアニメ作品を使ったのだと考えています。

このように、ターゲットとする人にとって受け入れられやすい形でメッセージを伝えていくことで、それが当たり前のことだと刷り込まれていき、アウェアネスの向上につながると思います。

そして、繰り返しになりますが、それを確実に身に着けさせる取り組みがセキュリティアウェアネストレーニングになります。

まとめ

ここで、アウェアネスとITセキュリティリテラシーとトレーニングについて、交差点を渡るということを例にそれぞれがどう機能するかを示して、違いをまとめます。

アウェアネス：青信号の交差点を渡っていても、右折してくる車はあるかもしれないという事を知っていて、「気を付けなきゃ」と思える　（そういうセンスをトレーニングするのがアウェアネストレーニング）

ITセキュリティリテラシー：具体的な確認の仕方、右見て左見て、もう一度右を見るという事を知っている

トレーニング：実際に交差点を渡る場面で、右見て左見て右を見ることができる（セキュリティ）スキルを習得させる。

このように自分なりに例に当てはめてみると違いが理解しやすくなると思います。

最後に、巧妙な手口と呼ばれるサイバー攻撃は人を起点にしているケースが多いのではないかと感じています。人はどうしてもミスをする可能性があるため、組織の最も脆弱な部分になってしまうことが多いです。

現状、人を起点にしたサイバー攻撃は増加しており、今後セキュリティアウェアネストレーニングがより求められることになるのではないかと感じています。技術で組織を守れる範囲は今後より広がるだろうとも考えられますが、どうしても人がケアしなければならない領域は残ると思います。ITの発展に合わせて技術だけでなく、人もセキュリティのレベルを上げていくことができれば社会はより安定して発展するだろうと思います。

本記事が少しでもみなさんの役に立ち、安全・安心な社会に少しでも寄与することを願っています。

【参考文献】

[1] https://csrc.nist.gov/publications/detail/sp/800-16/final
[2] https://csrc.nist.gov/publications/detail/sp/800-50/final
[3] https://www.ipa.go.jp/files/000025333.pdf
[4] https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/archive/2014-03-14
[5] https://www.nisc.go.jp/security-site/month/index.html