半径300メートルのIT:

2020年は何を信じよう？　サイバーセキュリティのゆく年くる年

https://www.itmedia.co.jp/enterprise/articles/1912/24/news033.html

2019年のサイバーセキュリティを振り返ると、「これまで信じていたものの崩壊」が印象に残っています。来年は、一体何を信じればいいのでしょうか。セキュリティベンダー各社の予想から、2020年の「信用と対策」について考えてみました。

2019年12月24日 07時00分 更新

[宮田健, ITmedia]

　あっという間に1年が終わり、間もなく2020年になります。2019年もサイバーセキュリティの世界にはさまざまな事件がありました。編集部からは「この1年を振り返る何かを」と振られているのですが――過去だけではなく、未来を見てみましょう。セキュリティベンダーが次々に、2020年の予測を発表しています。

本連載でもさまざまな事件を取り上げてきました

各社が「ディープフェイク」「サプライチェーン」への攻撃の激化を予測

　まず、筆者が見かけたセキュリティベンダー発表の「2020年脅威動向予測」を振り返ってみましょう。各社が自社の知見を基に発表した脅威予測を俯瞰（ふかん）し、大まかな傾向を見てみたいと思います。

「ディープフェイク」による詐欺やサプライチェーン攻撃に警戒：2020年の脅威動向を予測 | トレンドマイクロ セキュリティブログ

マカフィー、2020年の脅威動向予測を発表| McAfee Press Release

2019年の振り返りと2020年の脅威予測（パロアルトネットワークス）

Avast Press | アバスト2020年版脅威予測レポートを発表

2020年のビジョン：来年のサイバーセキュリティ予測|チェック・ポイント・ソフトウェア・テクノロジーズ株式会社のプレスリリース

2020 年のサイバーセキュリティトレンド 5 カ条 - News Center Japan

Top 5 Cybersecurity Trends to Prepare for in 2020 | Imperva

ベンダー各社が発表した上記の予測を見ると、多くのベンダーが人間の心を攻撃する「ディープフェイクによる詐欺」と、関連会社や組織内の人間の中で弱い部分を狙う「サプライチェーンに対する攻撃」を指摘しています。特にサプライチェーンに関しては2019年12月、廃棄物処理業者の従業員がHDDを不正に転売していた事件が記憶に新しいでしょう。

防ぎようはあるのか　HDD横領転売事件から見える「サプライチェーン・リスク」(1/2) - ITmedia エンタープライズ

バズワードにとどまらない未来予測――ベンダー独自の視点にも注目を

ここまではセキュリティベンダー各社が共通して述べる注意点といえます。筆者が興味深く感じているのは、特定のベンダーが独自の視点から指摘する脅威です。

McAfeeやCheck Point Software Technologiesは、個人や企業組織を苦しめてきたランサムウェアの被害が「2段階の脅迫攻撃に進化する」と指摘しています。これは、従来の標的型ランサムウェアの攻撃にとどまらず、**まずファイルを暗号化して脅迫し、さらにシステム復元中の被害者に対して機密データの開示を迫る**というもの。ランサムウェアは現在進行形で、しっかりとした対策をしなければならない脅威です（ランサムウェア単体の対策ではなく、バックアップを含む基礎的な対策を！）

悪質ランサムウェアでシステムがダウン！　どうすればいい？　――専門家が語る“意外な対処法” (1/3) - ITmedia エンタープライズ

Palo Alto Networksは、サイバー犯罪の「分業体制」が整い、攻撃者グループ間の協力や連携によって、過去にマルウェアに感染したマシンの二次被害が増える動きを指摘しています。日本においては、2019年末に大きな話題となっている「Emotet」がその代表例といえるでしょう。

猛威を振るうEmotet……これは単なる「種まき」だ？　辻伸弘氏の危惧する近未来 (1/2) - ITmedia エンタープライズ

そして、ImpervaとMicrosoftの脅威予測レポートには「ゼロトラスト」という言葉が出ました。ゼロトラスト、日本においては「2段階認証」同様のバズワードとして耳にした方も多いのではないでしょうか。私自身も最初はバズワードと捉えていたのですが、識者にいろいろと教えていただくうちに、「この考え方はもはや避けられない」と思うようになりました。

ゼロトラストは、特定の製品やソリューションを指すものではなく、セキュリティの概念で、よく「性悪説で考える」と説明されます。通信の安全性を守るために、従来の「壁」だけを信じずに、個別のアクセスがあるたびにその信頼性を最新ポリシーに基づいて判断し、ユーザーやデバイスを常に認証するというもの。**「Trust, but Verify（信じよ、しかし確認せよ）」から「Never Trust, always Verify（信じるな、常に確認せよ）」へ**、考え方をシフトさせることをいいます。

関連会社から納品されるプログラムモジュールや物理的な部品、協力会社の開発思想に、ゼロトラスト――Never Trust, always Verify――という考え方があれば、それこそが最強のサプライチェーンリスク対策になり得るでしょう。ゼロトラストは2020年、私が最も注目するバズワードです。

最後に「2019年に買ったベストガジェット」と言いたいところですが……

そして、2019年もたくさんのガジェットを購入しました。そこで最後に「買って良かったガジェットはこれ！」とご紹介したいところですが……そういったことを書きづらくなる問題が発生しました。「ステマ」騒動です。

「アナ雪2」ステマ騒動、ディズニー声明後に漫画家らが初めての謝罪　「『PR表記必要ない』との説明受けた」(1/2) - ねとらぼ

ステルスマーケティングとは、金銭やサービスの授受を隠して、宣伝と気付かれないように宣伝行為をすること。映画「アナと雪の女王2」にて、ウォルト・ディズニー・ジャパンの宣伝行為が不適切に行われた件で、大きな問題となりました。

この件は実際のステマそのものに加え、インターネット上で発信される情報が疑心暗鬼の対象に――つまり、誰かの感想が「これはステマでは？」という疑念を持たれやすくなってしまったことが、より大きな問題であると思っています。

個人で購入したものを誰に言われることもなく「これはオススメ！」と書いて「ステマだ」と言われてしまっては、本当に良いと思った情報を発信しにくくなってしまいます。これは、冒頭にて指摘した「ディープフェイク」も同様の危うさを持っているかもしれません。**「それ、本当に信じていいんですか？」**という疑念です。

それでもあえて述べれば、筆者の2019年のベストバイは「AirPods Pro」と「iPad」です。2020年はiPadで仕事をしようと思っています！　……ステマではありません、念のため。

[チョコの「GABA for Sleep」ステマ疑惑、グリコがキッパリ否定　「PRツイートにはPR表記を徹底」(1/2) - ねとらぼ]

何を信じればいいのか、どうすれば信じてもらえるのか

2019年はその他にも、信頼をコアコンピタンスとする企業が、その信頼を自ら損なうような事件が多数発生しました。市民を守るべき警察や警備会社による犯罪、通信を守るべき事業者や就職活動を支援する団体による情報の不適切運用、個人情報を保護するデータ保持者によるストレージの不正転売などなど。振り返ると、暗い気持ちになる事件も多かったように思います。

信頼は時間をかけ、少しずつ積み重ねることでしか醸成できません。一方で、失うのは一瞬です。また、どこか一つの企業が信頼を損なえば、水に投げ入れられた毒が広がるように、業界や社会全体が疑心暗鬼に包まれます。これも、2019年に私たちが直面した、大きな脅威といえるでしょう

[7pay事件が“セキュリティよりユーザーの利便性を優先したい”企業に突き付けた教訓 (1/3) - ITmedia エンタープライズ]

[逃げなかった先人たち　過去のインシデントの「後始末」を振り返る (1/3) - ITmedia エンタープライズ]

セキュリティベンダー各社が予測した今後の脅威は、どれもが「何か製品を買ったら守れる」ものでもありません。2019年は、「これさえ守れば大丈夫」という前提が崩れてしまった年といえます。2020年はさまざまな疑念に対し、皆で考えて少しずつ歩み寄る時代にしていかなくてはなりません。

[「お金を払ってセキュリティを学ぶ」のは平成で終わり？　ある無料教本が神レベルで優れている件 (1/3) - ITmedia エンタープライズ]

著者紹介：宮田健（みやた・たけし）

元@ITの編集者としてセキュリティ分野を担当。現在はフリーライターとして、ITやエンターテインメント情報を追いかけている。自分の生活を変える新しいデジタルガジェットを求め、趣味と仕事を公私混同しつつ日々試行錯誤中。

2019年2月1日に2冊目の本『Q&Aで考えるセキュリティ入門　「木曜日のフルット」と学ぼう！〈漫画キャラで学ぶ大人のビジネス教養シリーズ〉』（エムディエヌコーポレーション）が発売。スマートフォンやPCにある大切なデータや個人情報を、インターネット上の「悪意ある攻撃」などから守るための基本知識をQ&Aのクイズ形式で楽しく学べる。

関連記事

「パスワードレス認証」が進行中　FIDOで変わる、セキュリティの常識
IDとパスワードの組み合わせによるセキュリティに、多くの人が限界を感じています。そこで現在、数学的な仕組みを利用してパスワードレス化を実現する、新しいセキュリティアライアンス「FIDO」が広がりつつあります。

セキュリティ意識の陳腐化について　「これなら安心安全！」はすぐに危険になる
情報セキュリティの世界に「絶対」はありません。「この対策さえすれば、絶対安全ですよ！」というフレーズは、大抵間違っています。特に怖いのは、その「絶対安全」の基準がすでに古くなり、むしろ犯罪者の狙い目になっていることで……

不正利用されて感じた、クレジットカードの安心感
決済手法の多様化が進んでいます。現金取引かキャッシュレスか、キャッシュレスならどのサービスを使うか……ポイント還元率やキャンペーンも魅力的ですが、「どうしても発生する被害」としての、不正利用への体制も考えてみませんか？

URLバーの組織名表示を信用できる？ 変化するEV SSLサーバ証明書の取り扱い方
フィッシング詐欺サイトを見抜く方法として何度も紹介してきた「EV SSL証明書」に、大きな変化が起きようとしています。「鍵マークさえあれば安心」「組織名が表示されていれば安全」という先入観に付け入る悪意への対抗策を、皆さんは認識されているでしょうか？

「なんで設計段階で考えなかったの？」と言われるのは、いつだって完成後
エンジニアが困惑し、「どうすればいいの？」と問いたくなってしまうような事態があります。「Coinhive事件」や「無限アラートループ事件」、完成後にプライバシー保護の問題が発覚してリリースが見送られたサービスなどで共通して指摘された、「エンジニアの倫理」とはどのようなものでしょうか？