半径300メートルのIT:

政府がセキュリティ対策に「緊急提言」……えっこのレベル？　と思ったあなたへ

https://www.itmedia.co.jp/enterprise/articles/2002/03/news111.html

国際イベントに向け、サイバー攻撃への警戒が高まっています。先日総務省から発表された「緊急提言」には、各事業者がサイバーセキュリティ強化に向けて速やかに取り組むべき事項が述べられていましたが、その内容に拍子抜けした方もいるのではないでしょうか？

2020年02月04日 07時00分 更新

[宮田健, ITmedia]

2020年以降、日本ではさまざまな国際イベントが控えています。国際イベントの開催に併せてサイバー攻撃が増加するのは世界共通。日本でも同様の被害に備え、政府主導でサイバーセキュリティを見直す動きが進められています。

2020年1月28日、総務省は「わが国のサイバーセキュリティ強化に向け速やかに取り組むべき事項［緊急提言］」を発表しました。今回はこの発表内容と、そこから私たちがなにを考え直すべきかをチェックしてみましょう。

緊急提言！　今、国民が考えるべき総合セキュリティ対策とは？

今回の文書は総務省の「サイバーセキュリティタスクフォース」における成果物で、2020年の夏に**“間に合う”レベルの施策**を含む、5つの提言が行われています。**「その時」まで残り5カ月でも対応できるポイント**がまとめられていますので、ITmediaエンタープライズの読者である、多くの企業にとってもプラスになるはずです。

総務省｜「我が国のサイバーセキュリティ強化に向け速やかに 取り組むべき事項[緊急提言]」の公表

緊急提言の中で示された具体的施策は、以下の5つ。ここからは「つまり何をすれば良いのか」を解説します。

1. IoT 機器のセキュリティ対策の拡充

これは広義の「IoT（モノのインターネット）機器」への対策を意味します。インターネットに接続する機器のセキュリティ対策は、PCやスマートフォンを除けば「機器のベンダーが製造段階からセキュリティを考慮していること」が大原則です。逆に言えば、利用者側でできることは「安全な製品の選定」程度。しかし、IoT機器の見えるところだけを見ても、それが安全かど

うかは分かりません。

そこで政府は今回の文書で、情報通信研究機構（NICT）の取り組み「NOTICE」などの拡大を短期的に採るべき対策としています。NOTICEとは、IoT機器のパスワードが初期パスワードや弱いパスワードなど容易に侵入できるものである場合に、インターネットサービスプロバイダー（ISP）を通して注意喚起するプロジェクトのこと。利用者目線ではNOTICEによって、組織が管理する機器に初期パスワード／弱いパスワードが残っていないかがチェックできます。利用者はNOTICEの注意喚起がISPから来たときにはしっかり対応することと、そして**「ISP以外」からの偽の注意喚起**に気を付けましょう。

政府主導の“対民間”サイバー攻撃？　物議を生む「NOTICE」を実行せざるを得ない、国内の深刻な事情 - ITmedia エンタープライズ

2.地方公共団体向け実践的サイバー防御演習（CYDER）の繰り上げ実施等

緊急提言では「地方公共団体はセキュリティ人材を育成するために、NICTによるサイバー防御演習『CYDER』を受講せよ」と書かれています。もちろんこれまでも、さまざまな方法で人材育成が行われてきましたが、これを「7月までに推し進めよ」と強く推奨しています。

では、一般企業はどうすべきでしょうか。一般向けにも無料で素晴らしい資料がたくさん存在します。中には小学生に向けたまんが本もありますので、ご家族で読んでも良いでしょう。

「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 - ITmedia エンタープライズ

3.サイバーセキュリティに関する情報共有体制の強化

3つ目は「情報共有」です。銀行や情報通信などの業界では、情報を共有する「ISAC（Information Sharing and Analysis Center）」と呼ばれる組織を作り、ビジネスでは競合する企業同士がサイバー攻撃の情報を共有しています。以前お話をうかがった「金融ISAC」では、定期的に合宿形式で実践的な演習を行う「サイバークエスト」を開催し、金融業界以外でも参考になる取り組みを実施しているとのことでした。

社長へのメールを秘書が開いてマルウェアに感染!?　標的型攻撃の実践演習「サイバークエスト」を模擬体験 - ITmedia エンタープライズ

一般企業にできる取り組みとしては、まずは自社の事業に近いISACが存在しないかをチェックすること。もし該当するものがなければ、ぜひ立ち上げを考えてみてください。始めから大きな組織にする必要はありません。「近しい企業、近しい立ち位置の人とチャットで話し合う」といったことでも、立派にISAC的な取り組みになるはずです。

4.公衆無線 LAN のセキュリティ対策

4つ目は「公衆無線LAN」です。国際イベントといえば期待されるのが訪日観光客によるインバウンド需要の高まり。通信環境も訪日客が簡単に利用できる仕組みを採用しつつ、セキュリティ対策を進める必要があります。

今回の提言では、短期的に取り組める内容として「セキュリティを強化したWPA3-Personal、WPA3-Enterprise、Enhanced Openなどの新しい規格が策定されていることを踏まえ、公衆無線LANのセキュリティ対策の状況や利用者が講じるべきセキュリティ対策について、提供サービスの状況について提供者が利用者に対して適切に伝えるとともに、利用者がそのような情報を適切に判断できるよう、リテラシー強化のための周知啓発を強化することが必要である」としています。

この点に関しては、電子フロンティア財団（EEF）が「公衆無線LANは思ったほど危険ではない」と述べています。現在ではほとんどのWebサービスがSSL／TLSに対応しており、かつて危険視されていたほどのリスクはなくなっているという意見です。筆者は個人的にはこれに同意します。リスクマネジメントにおいて必要な方は、VPNなどを活用しましょう。

Why Public Wi-Fi is a Lot Safer Than You Think | Electronic Frontier Foundation

ただし公衆無線LANにおいては暗号化のお話し以外にも、「000000JAPAN」のようにそっくりの偽アクセスポイントを

立ち上げられてしまうなどのリスクはあります。今回の提言に加え、総務省は年度内に公衆無線LANに関するガイドラインを改訂するとのことです。ホテルや観光業、学校などの関係者は、このガイドラインに注目する必要が出てくるでしょう。

5.制度的枠組みの改善

最後の提言は「法令やガイドライン、基準といった制度的な枠組みの定期的見直し」です。電気通信分野や放送分野では、総務省による「情報通信ネットワーク安全・信頼性基準」や電気通信事業者協会の「電気通信分野における情報セキュリティ確保に係る安全基準」、ICT-ISACによる「放送設備サイバー攻撃対策ガイドライン」などが参照されています。各業界にある制度をしっかり見直し、アップデートしましょう。

各企業組織においても、整備されたルールやマニュアルは存在していると思います。ただし、それはサイバー攻撃の最新事情に合っているでしょうか。それは常に見直す必要があるでしょう。ただ「ルールだから、マニュアルに書いてあるから」と従うのではなく、常にルールを疑い、アップデートの必要性をチェックして、関係者全員が組織のあるべき姿を考えることが大切です。

「えっ、そんな程度の話なの？」と思ったあなたへ

緊急提言と題している割にはどれもある意味当たり前の話で、拍子抜けしたかもしれません。もっと実効性のある方法や、決め手となるソリューションを教えてほしい！　と思った方もいるでしょう……おそらくこの緊急提言は、そんな方のために書かれているのです。

緊急提言で述べられた項目は、どれもごく基礎的な「基礎」です。基礎はつまらないことが多いです。そんなことは分かっている、もっと明確なズバリの答えが欲しいという思いはよく分かります。しかし、スポーツだって基礎体力がなければ楽しめません。だからこそ、今さら当たり前のような話が「緊急提言」としてまとめられたのではないでしょうか。「なんだかしっくりこない話だなあ」と思ってしまった方ほど、この5つのポイントをあらためてしっかりと認識していただきたいと思います。

2020年2月1日から、毎年恒例のIPAのサイバーセキュリティ月間がスタートしました。「情報セキュリティ10大脅威2020」も公開されています。実は、これもよく見るとトップ10入りした項目にはそれほど変化がありません。これは基礎、かつ対処が追いついていないため、いまだに攻撃が有効であることを意味します。

基礎をおろそかにしていい分野はどこにもありません。今回の提言の内容をしっかり見直し、さらなる基礎中の基礎「アップデートを行う」「パスワードをしっかり管理」「バックアップを行う」などもお忘れなく。

■「情報セキュリティ10大脅威 2020」　　NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
NEW	スマホ決済の不正利用	1位	標的型攻撃による機密情報の窃取	1位
2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位
1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位
7位	インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃	4位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位
3位	不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位
5位	ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取	7位
6位	偽警告によるインターネット詐欺	9位	IoT機器の不正利用	8位
12位	インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止	6位

2020年の10大脅威は……（出典：情報セキュリティ10大脅威 2020：IPA 独立行政法人 情報処理推進機構）

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

三菱電機の情報漏えい事件から見えること　「守り方」のシフトチェンジを
2019年6月に判明した不正アクセスが、2020年1月にスクープ報道されました。「あれ？」と思われる方も多いでしょう。筆者もその一人です。この違和感をたどって「セキュリティ対策のあるべき姿」を考えてみます。

ゼロデイ攻撃発生、ユーザーにできる「減災」と「防疫」とは
Emotet、Citrix製品へのゼロデイ攻撃、Windows7のサポート終了、IEの脆弱性……、2020年もセキュリティに関する話題は盛りだくさんです。「完璧な安全」は誰にも保証できない時代、ユーザー側でできる最善の備えは何になるのでしょうか。

ユーザー側には対策不可能!?　ECサイトを狙う「Eスキミング」の怖さ
巧妙化が続く、サイバー犯罪。2019年は従来の「セキュリティの常識」がことごとく覆される1年でした。今後さらに問題になりそうなのが、カード決済システムの隙を狙う「Eスキミング」。なんと、利用者にできる対策が「ない」というのです。

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
JPCERTや複数のセキュリティベンダーから、マルウェア「Emotet」の注意喚起が発信されています。ひっそりと広まったマルウェアが他の攻撃の踏み台にされたら、どうなってしまうのでしょう？　辻伸弘氏が危惧する「刈り取り」とは。

ITmedia Inc.