報道関係者各位

2013 年 8 月 6 日

旅先でのテクノロジー:デジタルの危険は回避できる

（2013 年 7 月 31 日ヘルシンキ発 ー フィンランド本社発表資料抄訳）

夏の休暇にお出かけですか？エフセキュアの調査により、旅先で特に意識すべきデジタル利用の注意点が明らかになりました。

夏休みの季節になりました。人々がスマートフォンにタブレット、日焼け止めにタンクトップをかばんに詰め、気分転換に旅先でのんびりと過ごす季節です。あらゆるデバイスがつながり、目的地を見つけたり、思い出を記録したり、地元の友人と連絡を取り合うことはこれまでにないほど容易になりました。しかしテクノロジーが旅行を快適なものにしてくれる一方で、最近のエフセキュアの調査*により、旅先で特に意識する必要があるデジタルの注意点が浮き彫りになりました。

公衆無線 LAN（Wi-Fi）とインターネットカフェの現実

旅行中は、空港やレストランといった場所での公衆無線 LAN（Wi-Fi）ホットスポットの利用が便利ですが、52%の人々がその安全性とプライバシーについて懸念を抱いていると回答しており、実際それは妥当な懸念と言えます。エフセキュア ラボのセキュリティアドバイザー、**ショーン・サリヴァン**は、公衆無線 LAN は文字通り「公衆」のものとして捉えるべきであると述べています。見知らぬ他人とネットワークを共有しているため、誰かがあなたのしていることをこっそり覗くことのできるソフトウェアを利用しているリスクがあるのです。

「使っているデバイスが自分のものであるためにプライベートであるように感じるかもしれませんが、それは誤りです」とサリヴァンは言います。彼は、パスワードでアカウントにログインすることも含め、他人に知られたくないことは決して公衆無線 LAN の使用中に行うべきではないと忠告し、「私は地下鉄で友人と話すような内容については、喜んで公衆回線の Wi-Fi を使いますが、オンラインバンキングは自宅で行います」と述べています。

図書館やインターネットカフェのような場所にある公共のパソコンについても同じことが言えます。サリヴァンは、パスワードを盗むスパイウェアがコンピュータに常駐している可能性もあるため、公共のパソコンはニュースを読むなどの当たり障りのない目的にのみ使用すべきであると忠告しています。

大切な人と連絡を取るのにどうしても公共の手段を使用しなくてはならない場合の一つの手は、休暇中にのみ使用するアカウントを別途作っておくことです。「そうしておけば、誰かに休暇用の E メールアカウントに侵入されたとしても、その目にさらされるのは母親やキャットシッターとの E メールだけで、メインのアカウントに入っているほかの機密データにはアクセスされずに済みます」とサリヴァンは説明します。

旅先でのバンキング

85%の人が自分のパソコンから、また 24%の人がスマートフォンからオンラインバンキングを利用すると回答しています。では休暇中に、どうしても何らかの手続きを行わざるを得ない状況に置かれたらどうすれば良いのでしょうか？おそらく最善の手段は、多少ローミングが必要になるとしても、取引先である銀行のモバイルアプリを使ってモバイルデータ プランを利用することです。費用はかかりますが、銀行口座をゼロにされてしまうよりは安上がりです。

しかし、「銀行は HTTPS 接続を使っているのだから、公衆無線 LAN を経由しても安全なのではないか」という疑問があります。通常それは事実ですが、その他の要因も認識しておくことが大切です。

39%の人が、利用しているすべてのアカウントで、1 つまたは 2～3 つのパスワードしか使っていないと回答しています。つまり、保護されていないサイトで使うパスワードと、安全な銀行のサイトで使うパスワードが同じであれば、理論上、侵入者はあなたの銀行口座にもアクセスできるということになります。また、侵入者は、入力しているパスワードを肩越しに盗み見るといった、ローテクな手段を用います。

旅先でコンテンツを安全に保護する

67%の人が、デバイスそのものよりもデバイス上にあるコンテンツのほうが重要であると考えていることから、旅行に出る前にバックアップを取っておくことの重要性は明らかです。もしくは、エフセキュアが通信事業者を通じて提供する「F-Secure Content Anywhere（エフセキュア コンテンツ エニウェア）」のようなコンテンツ同期サービスを利用することで、ユーザはデジタルコンテンツを自動的にパーソナルクラウドに同期させることができます。こうしたサービスにより、重いストレージデバイスを持ち歩く必要性がなくなり、休暇中でも手軽に、安全かつプライベートな環境で友人と写真を共有することができます。エフセキュアの個人用コンテンツクラウドで管理されるデータは、データを移行する際もストレージに保管されている間も完全に暗号化されています。

紛失・盗難にあったデバイスの位置特定

電話の紛失や盗難は、休暇を台無しにします。61%の人が自分のデバイスを仕事とプライベートの両方で使用しているという現状を考えると、特に注意深くなる必要があります。電話の紛失はあなたの個人データのみならず、会社や組織のデータにも影響を及ぼす可能性があります。スマートフォンやタブレット向けのエフセキュアの無料の盗難対策アプリ（Anti-Theft**）は、リモートでデバイスをロックしたり、その位置を特定することが可能なほか、必要に応じてデータを完全に消去することもできます。ここで、もうひとつワンポイントアドバイス。パスワード保護されたスクリーンロックは、1 分ほどの短時間の間に作動するように設定しておきましょう。

健全な公衆無線 LAN 利用のためのその他のアドバイス

- デバイスが Wi-Fi スポットに自動的に接続されるように設定しておかないこと
- 自宅に戻ったら、使用した Wi-Fi のアクセスポイントとの接続を切ること
- 旅行中に不要なアプリケーションにログインしないこと
- ログインしているネットワークが、侵入者が仕掛けた罠ではなく、実際に利用している施設のものであることを確認すること
- 周囲に注意を払い、肩越しに盗み見をする人がいないかどうか注意すること
- アカウントごとに異なるパスワードを使用すること
- ノートパソコンは、ファイル共有機能を無効にし、外部からの接続をブロックするようファイアウォールを有効にしておくこと
- 可能な場合は、公衆無線 LAN（Wi-Fi）での接続を保護してくれる VPN（バーチャル プライベート ネットワーク）を使用すること
- 個人の Wi-Fi ネットワークには、プリペイド SIM カード式のトラベル用 Wi-Fi ルータを使用すること
- 個人情報を扱うサイトでは、最低限必ず錠マークやアドレスバーの「https」の存在を確認し、これらがないサイトの使用は避けること
- 覚えておくべき基本ルール：公衆無線 LAN で行うことはすべて、公共の場での会話と同様であると考えること

*エフセキュアの「2013 年デジタルライフスタイル調査」は、15 カ国（ドイツ、イタリア、フランス、英国、オランダ、ベルギー、スウェーデン、フィンランド、ポーランド、米国、ブラジル、チリ、コロンビア、オーストラリア、マレーシア）で 20～60 歳のブロードバンド加入者 6,000 人を対象に Web インタビューを実施しました。同調査は、GfK によって行われ、2013 年 4 月に完了しました。

**Anti-Theft は以下の URL から入手できます。（無償提供でサポート対象外になります。）

http://www.f-secure.com/en/web/home_global/anti-theft

エフセキュア株式会社 会社概要

http://www.f-secure.co.jp/

エフセキュアは、IT 先進国フィンランドで 1988 年に設立されて以来、25 年にわたりセキュリティ製品に取り組んでいる業界の先駆者で、世界規模でセキュリティサービスを提供しています。1999 年に OMX ヘルシンキ証券取引所に上場し、以来、順調に成長を続けている株式公開企業のひとつです。

エフセキュア株式会社は、エフセキュア社 100%出資の現地法人として設立され、以降、増収を続けながら順調に企業規模を拡大しており、2009 年 5 月に日本法人設立満 10 周年を迎えました。

会 社 名:	エフセキュア株式会社
カントリーマネージャ:	アリエン・ヴァン・ブロックランド
所 在 地:	〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F
設 立:	1999 年 5 月
事業内容:	セキュリティ関連製品・サービスの販売およびサポート

本件に関するお問合せ先
エフセキュア株式会社
マーケティング部
Tel: 03-5545-8942 Fax: 03-5545-8945
Email: japan@f-secure.co.jp
〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F
URL: http://www.f-secure.co.jp/
Blog: http://blog.f-secure.jp/