

東日本大震災から考える情報セキュリティ

| | |
|----------|---|
| その他のタイトル | The Great East Japan Earthquake and Information Security |
| 著者 | 河野 和宏 |
| 雑誌名 | 社会安全学研究 = Safety science review |
| 巻 | 2 |
| ページ | 42-43 |
| 発行年 | 2012-03-31 |
| URL | http://hdl.handle.net/10112/00018552 |

東日本大震災から考える情報セキュリティ

The Great East Japan Earthquake and Information Security

関西大学 社会安全学部

河野 和宏

Faculty of Safety Science, Kansai University

Kazuhiro KONO

情報がデジタル化され、多くの人々がインターネットの恩恵を受けている近代の情報化社会において、災害と情報セキュリティは実は密接な関係がある。今回の東日本大震災でも、震災・津波によるデータの消失やネットワークの不通・電力不足による提供サービスの質の低下、さらに事業継続計画（BCP）の見直しなど、多くの課題が露呈した。しかしながら、これらは組織に対する課題であり、一般の人々にはあまり現実味がないかもしれない。そこで以下では、今回の災害で問題となった迷惑メールに焦点を当て、人々が情報セキュリティをどのようにとらえているか考察する。

東日本大震災の発生から数日後、多くの迷惑メールが出回っていたのはご存じだろうか。実は、筆者にも東日本大震災に関連した迷惑メールが送られてきており、その内容は節電に関するものであった。具体的には、東北地方の電力不足を補うために関西電力が電力供給を始めており、少しでも多くの電力を送電するため節電に協力してほしいという内容であった。上記は節電に関する迷惑メールの例であるが、他にも有害物質や放射性物質が雨と一緒に降ってくる・関西でも大地震が起きるといった人々の不安を煽る内容のメール、募金・寄付を装った出会

い系サイトの宣伝メール等、多種多様の迷惑メールが確認されている。

迷惑メールの目的は、主にユーザの個人情報や金銭の詐取であり、詐取する方法としては、ウイルスを使って個人情報を盗もうとする方法（具体的には、メール中にウイルスを仕込むといった方法やメール中にウイルスが置かれたURLを画像等に隠しておき、クリックされると画像や動画等にみせかけたウイルスがダウンロードされ感染するといった方法等）、ユーザが興味を引くようなサイトを装い利用者をサイトに誘導させた後、ユーザに個人情報を入力させ盗もうとする方法（いわゆるフィッシング）が代表的である。今回の震災でも、例えば、募金のお願いと称してメール中にあるURLをクリックすると募金を装ったフィッシングサイトにアクセスされ個人情報や金銭を取られるという迷惑メールが確認されている。

今回の震災で問題となった迷惑メールの多くは、上記の代表的なものではなく、チェーンメールと呼ばれるものである。チェーンメールの目的は個人情報や金銭の詐取ではなく、誤った情報、つまりデマの流布である。チェーンメールは、いわゆる不幸の手紙の電子メール版であり、今回の場合、節電への協力のお願いという

いかにも本当らしい内容を送り、他人にメールを転送するよう誘導する。転送されたメールを受け取った人も同様に転送していくため、転送する人はねずみ算式に増加していくことになり、瞬く間にデマが拡散していくことになる。今回、チェーンメールが流行してしまった理由は、通常の迷惑メールと異なりチェーンメールは知り合いから送られてくるという点、メールの内容自体が節電や募金・寄付の呼びかけという今回の震災で被災した人々を助けたいという人の善意を利用する内容であった点¹⁾があげられる。

しかしながら、チェーンメール自体は昔から存在するものであり、今回は東日本大震災という特殊な状況であったが、このようなチェーンメールが流行することを考えると、一般の人々のインターネットに対するセキュリティの意識が未だに低く、大量に流れてくる情報を正しく判別できていないことがうかがえる。例えば節電に関しては、少しでも電力の仕組みを知っていれば、東日本と西日本の周波数の違い等の問題から大電力を供給するのはできないと判断できるため、チェーンメールであることを見抜くことが可能である。また電力の仕組みを知らなくても、このような重大な内容が政府や電力会社の公式会見もなくメールで送られてくること自体おかしいと感じなくてはならない。

節電や募金・寄付は良いことであると考え、メールの転送をした、もしくは受け取った内容の行動をしたという話もよく耳にするが、大いに問題である。大量のチェーンメールが転送されるとネットワークに負荷がかかるという問題が発生するだけでなく、デマの拡散により情報

の判断が難しくなり、いたずらに人々の不安感を煽ることにつながる。また、場合によっては、寄付等の善意でした行動により、行動を受け取った相手側の本来の活動を逆に阻害することにもなりえる。

さらに、チェーンメールを信じて行動するという事は、「私は騙されやすい」と周りに公言しているようなものである。節電や募金・寄付自体は良いことであるのだが、このようなチェーンメールを自身の行動の判断材料にしてしまうと、悪意ある第三者は人の心理を逆手にとって行動するため、後々大きな被害を受ける可能性が高くなるということを考えるべきである。

今回のチェーンメールの拡散に代表されるように、一般の人々はまだ情報セキュリティに対する意識が低いと感じられる場面がよく見受けられる。特に、近年はパソコンだけでなくスマートフォンの急速な普及もあり、より利用者側に高いセキュリティ意識を持つことが要求されているにもかかわらず、「インターネットは便利なもの」「プロバイダ側の対応やソフトの導入によりセキュリティ対策は万全」等のイメージが先行し、セキュリティに対する人々の意識はなかなか向上していない。情報モラルの観点からもセキュリティは重要であるため、非常時であろうとも高いセキュリティを保つことができるよう、日ごろからセキュリティを意識しておく必要がある。

注

- 1) 人の心理や善意を利用する方法をソーシャルエンジニアリングと呼ぶ。