

平成16年度総合セキュリティ対策会議 臨時会議
(平成16年1月28日)
発言要旨

【いわゆる「フィッシング」対策の推進について】

(事務局より説明)

(質疑応答)

- ボットネット対策としては、ウイルス対策ソフトは機能しないのか。
- 事務局 効果がないことはないが、それだけでは対策不足である。

【いわゆる「フィッシング」に対する取組みについて】

(委員よりマイクロソフトの取組みについて説明)

○ 米国では官民の連携の枠組みができつつあり、日本でも、電子署名技術の普及に努めていきたい。一方で、100%安全な技術対策はないので、官民が連携した情報共有や広報啓発が重要と考えている。

(質疑応答)

- フィッシングによる被害は、個人情報を窃取された人だけではなく、なりすましを受けた企業等も被害者ということもあるのではないか。
- SenderID 等電子署名技術は、米国ではどれだけ普及しているのか。
- これからという段階ではあるが、メールサーバソフトに組み込まれる予定になっており、今年はかなり普及が進むと考えている。日本でも、来月からまず送信側について組み込んでいき、徐々に受信側の普及も促進していく予定。
- 複数の電子署名技術が普及すると、受信側は混乱するのではないか。
- 電子署名技術は SenderID 以外にも多くの種類があるが、それぞれにメリット・デメリットがあり、今後改善を図ることにより、共通のものが普及することが望ましいと考えている。

(委員よりヤフーの取組みについて説明)

○ フィッシングページが蔵置されているのが日本のサーバなら、サーバ管理者に連絡をとって対応可能だが、海外のサーバだと連絡しても返事がない。犯罪抑止の観点からも、警察は是非取締りを強化していただきたい。

(質疑応答)

- フィッシングページを発見した際、実際に ID・パスワードを入力したと思われる利用者に通知したということだが、通知をメールで行ったとなると、利用者はどれが偽のメールでどれが本物のメールか区別がつかない状態になるのではないか。
- その可能性も検討したが、緊急性を優先してメールを送り、一定時間内に連絡がなかった人には電話で連絡をした。対象者が少なかったなので、そのような対応

が可能であったが、人数が増えると難しいので、周知徹底に力を注ぎたい。

○ 携帯電話を利用したサービスの場合、フィッシングメールかどうかの判断はより難しくなるのではないか。

(全国銀行協会の取組みについて説明)

○ 昨年末の国家公安委員長要請を受け、各銀行への注意喚起及び当協会ホームページでの広報を実施したほか、当協会で策定しているインターネット・バンキング開設の留意事項にフィッシング対策について盛り込むことを検討している。

(質疑応答)

○ 技術の導入や補償についての約款の規定等、具体的な取組みの予定について教えていただきたい。

○ 注意喚起に努めているのが現状であり、技術の導入については各銀行が判断すべきことと考えている。偽造キャッシュカードの問題でも取りざたされているが、補償・被害救済ということについては、望ましい在り方について検討していきたい。

○ 国内の主要なインターネット・バンキングの本人認証方法について、独自に調べてみたところ、フィッシングに強いと思われるワンタイムパスワード認証(1回ごとに異なるパスワードを入力する認証方式)を取り入れていない企業がまだあるが、固定パスワードによる認証方式はやめていくべきではないか。

○ ワンタイムパスワード認証の採用が、実際にフィッシング対策に有効であるならば、認証方式の見直しについて、インターネット・バンキング開設の留意事項に盛り込むことも検討していきたい。

(委員より全国クレジット産業協会の取組みについて説明)

○ フィッシングにより窃取されたカード番号は、偽造カード作成に利用され、海外で使用とされているようだ。しかしクレジットカードの機能上、実際には使用された例は少なく、また万一使用され被害にあっても、被害額はカード会社で補償している。

(委員よりWEB110の取組みについて説明)

○ フィッシングページかどうかは、URL によって判断することはできないので、認証情報や入力情報の送付先等を確認する必要がある。また他のページのリンク集からフィッシングページに入り込むこともあるので注意が必要。

(総務省の取組みについて説明)

○ 研究会を立ち上げており、電子署名技術の普及に努めたいと考えている。

(経済産業省の取組みについて説明)

○ 連絡会を開催しており、フィッシングに関する広報啓発や技術的対策を推進しているほか、関係業界との協議会設立を検討している。

【いわゆる「フィッシング」対策に係る官民の連携について】

(自由討議)

○ フィッシング対策には、国際連携が欠かせないと考えるが、捜査機関の間での連携は進んでいるのか。

○ 事務局 フィッシング事案の捜査について知見のある米国の捜査機関との情報交換等を進めている。米国の法執行機関も産業界との連携を強化しており、日本でも官民連携した取組みを進めていきたいと考えている。

○ 各企業等がフィッシングページを作られないようなホームページ作りを進めていくことも必要。また、技術の標準化については、いかに上手に普及させるかが重要。さらに、捜査機関の能力向上を図り、是非取締りを強化していただきたい。

○ 広報啓発も重要だが、クレジットカードの被害補償のように、社会システムとしてフィッシング被害にあわないようなスキームを検討しなければならない。フィッシング対策のための法制化・社会的な義務化が必要ではないか。また、取締りの強化のためには追跡性を確保することも重要である。

○ フィッシングは IT 技術の普及の根幹をゆるがす重大事案。今は様々なスキームで対策を進めているようだが、国全体として統一するスキームが必要ではないか。

○ フィッシングに対してどのような罪が適応できるのか検討し、既存の法律で対応できないのであれば、新法制定も視野に入れ検討すべきではないか。IT 分野は、既存の法律で対応できていない部分が多いように思う。

(以上)