平成２３年度総合セキュリティ対策会議（第３回）

平成２３年９月８日

発言要旨

１．開会

【生活安全局長交代に伴う挨拶】

○生活安全局長：本日は、前田委員長は始め、各委員の皆様方には大変お忙しい中、お集りいただきまして本当にありがとうございます。

この総合セキュリティ対策会議は、本年度で 11 年目と伺っております。何といいましてもこの会議はこれまでも、毎年御提言をいただき、それが様々な具体的施策として実現するという非常に輝かしい歴史を持った会議だと思っております。そういう意味で本当に国民のためになっている会議ではないかと思っております。

本年度は、サイバー犯罪捜査における事後追跡可能性の確保というテーマで御討議いただいているところでございます。この問題は警察が捜査をして、サイバー犯罪を抑止し、そして安全で平和なサイバー空間をつくるということにおいて、欠くことのできない大前提となる非常に重要な問題であると思います。どうかよろしく御審議をお願いします。

本日は第３回目でありますが、無線ＬＡＮとデータ通信カードについて、いかに事後追跡可能性を確保していくかということについて御議論いただいただきたく思います。どうか、皆様方の御経験、あるいは御見識を踏まえて貴重な御意見を賜りたいと思います。どうぞよろしくお願いいたします。

２．データ通信カードの現状について

【関係２事業者より、データ通信カードの現状について説明】

○説明者１：データ通信カードの契約の際の本人確認の方法について、受付チャンネルごとに大きく２つに分かれており、店頭で購入される場合の受付方法、また、ウェブサイトで通信販売にて購入される場合の受付方法があります。

まず店頭については、こちらは対面での販売になりまして、通常の携帯電話の販売と同様の方法による契約の仕方をしており、「携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律」にのっとった形で実施しております。具体的には法律で定められている免許証等の本人確認書類の原本を御提示いただき、そちらを確認し、契約に至るということになります。また、代理人の方が御

来店されて、契約者の御名義人でない方と手続をする場合においても、代理人の方の本人確認書類原本を確認するといった形で、こちらも法律にのっとった形の役務で受付をしているといった点で、通常の携帯電話の契約と全く遜色のない本人確認方法を実施しております。

続きまして、ウェブサイトでの通信販売についてですが、一番主となります「ドコモオンラインショップ」については、こちらは弊社のホームページから入っていただくと、手続まで行き着くような形の動線になっており、これが一般のお客様が御契約、御購入される際の主たるウェブサイトになっていますが、こちらのウェブサイトにつきましては、音声系の端末とデータ系の端末、モバイルＷｉ-Ｆｉルーター等を含めた一般のお客様向けの商品を御御契約をいただく際においては、通常の携帯電話を購入する際と同等の本人確認を実施しております。

ただし、どうしても対面ではないということで、法律で定められている本人確認書類の原本での確認がどうしても実行できないという点については、店頭での本人確認との差異があります。そういった場合におきましても、契約者御本人様に後日、契約の確認のお手紙を簡易書留等の郵便で、本人限定郵便という形で送らせていただくことで本人の特定をさせていただき、こちらを本人確認に代えさせていただく方法をとっております。

また、現状、当社におきましては把握している範囲では不正取得という事案は特にございませんが、犯罪等悪用された際においては通常の携帯電話契約においても御依頼に基づき、手続にのっとって捜査協力をさせていただいているといったところでございまして、これがデータ通信カードになると変わるというものではありません。

○説明者２：弊社が行っているデータ通信カードの契約時の手続についてです。与信の観点から、支払方法に応じた加入審査という形で実施しています。販売チャンネルによってではなく支払方法に応じて、幾つか加入審査を使い分けているというのが現状です。まずクレジットカードですけれども、これは支払能力の確認ということで、いわゆるオーソリゼーションを実施させていただいており、携帯電話を販売するときのような本人確認書類というのは取得しておりません。それから口座振替と窓口払い、この２つにつきましては、本人確認を実施しており、これは携帯電話の販売時と同等の書類を取得させていただき加入審査をしております。最後に契約成立後、郵送にてサンキューレターで契約内容確認書類というものを郵送しまして、それが不達で戻ってくるといった場合には利用停止や解約を行っているという現状です。

３．データ通信カードに係る論点説明

【事務局より、データ通信カードに係る論点説明】

○事務局：データ通信カード事業者における本人確認実施状況等について、全７社に対してヒアリングを実施し、その状況を取りまとめました。

１点目が料金口座引き落としの際の本人確認方法ですが、結論的には７社中６社が公的書類で御確認をされており、残り１社については、家電量販店等において、期間の決まったデータ通信カードを購入していただくという形の、いわゆるプリペイド販売という形式をとっており、この場合には利用料金の取り損ないという損失の可能性がありませんので、したがって、本人確認の必要性がなく、実施されていないという状況です。

次に２点目は料金クレジットカード払いの際の本人確認方法についてですが、７社中３社は公的書類によって本人確認を実施していますが、残りの４社はクレジットカードの場合には、仮に口座の中の残高がゼロになったとしても、それはクレジットカード会社の負担になるという契約であるということもあり、損失の可能性がないということで、実施されていないという状況です。

３点目は、住居以外での受取でございます。これは犯罪へ悪用を抑止するという観点からは、やはりこうしたデータ通信カードの受取先が住居以外ということですと、どうしても犯罪者グループによって、そのアジト等で受け取られてしまうという問題点があります。

４点目は、これは事業者間で本人確認要領が違うことに関する御意見ということですが、共通の基準のようなものがあればいいという意見が大勢でした。また、共通の基準といったものを作る進め方としまして、やはりその所管省庁の御指導の下で、事業者団体の中での検討を通じ、協議するのがいいのではないかといった意見が大勢でした。

これらの方向性につきましては、携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律の改正によって手当てをするというような方策もありますが、関係事業者数は７社ということで非常に限定的であり、例えば業界内の自主基準を作っていただくとか、申し合わせによる対応という方策も考えられるので、基本的にはそういった自主的な対応でも解決ができない場合については、法律改正も視野に入れて対応を考えるのではないか思っております。

○委員：データ通信カードの加入に当たりまして、他人の本人確認の書類等を用いるなど、何らかの手段で実質的には匿名的に契約をして、そのデータ通信カードを用いて様々な不法行為を行い、それに対してその匿名性から摘発が困難化しているという事案が明らかにされました。業界といたしましても、私どもの利用料金の債権の確保はもとより、

データ通信カードが犯罪に利用されることを少しでも抑止するための本人確認方法の検討につきましては、今後、事案の内容を伺いながら取り組んでいきたいと考えております。

○委員：多分使われているＳＩＭ等は携帯と同じで本人確認がなされていると思いますが、後でそれを契約変更して、データ通信カードの契約にするというような場合も審査といいますか、本人の確認はなされているのでしょうか。

○説明者１：当社では一部特殊な受付方法としてクレジットカードによる受付をしていますが、そういったお客様について通常の一般的な契約、音声もできるような契約に変更する場合においては本人確認を再度実施するような方策をとっております。具体的には、店頭のオペレーターが契約を変更する際においては必ずシステム的にチェックがかかる形になっており、再度の厳密な本人確認をしないと契約の変更ができないということになっております。

○委員：無線ＬＡＮとデータ通信カードどちらが、特に日本で問題が起きているのかということをはっきりさせる必要があると思います。どちらもセキュリティ上の問題があると思いますが、特にどちらが問題なのでしょうか。

○事務局：双方の問題とも現在事後追跡の正に障害になっていると認識しております。

○委員：クレジットカードは、必ずしも本人を証明しているとは言えませんので、本人認証の代わりには使えないと思います。もちろんクレジットカードは本人が使うということは前提です。そのため業界としても、クレジットカードの利用に当たって本人が利用しているということを確認するために、３Ｄセキュアなどの本人認証を導入する努力をしています。カード会社のサービスとして第三者に対して本人であるという証明をするということはやっていないと思います。

○委員：オンラインで即時加入できるサービスということを重視されているような業者もあるようですが、こういうオンラインで即時加入できるサービスは、ユーザーにとっては非常に有効なサービスのように思いますが、これについて通信業者としてどのようにお考えなのでしょうか。

○説明者２：オンラインのところにつきましては、やはりユーザー様にとってワンストップで商品が購入できるという点で、非常にメリットがあると思います。利便性の高いオンラインショップにおける本人確認を実施方法ついてどうするかというところにつきましては、我々としてはできるだけユーザー様にストレスのない形で購入いただく方がいいとは思っていますが、業界全体としてどういうふうなルールができるのか検討してまいりたいと考えています。

○説明者１：ウェブサイトでの販売については、島嶼部に在住していらっしゃるような、なかなか実際に店頭にアクセスが困難なお客様に向けて、利便性を確保するという目的がございます。店頭での販売しかできないといったことになったときに、若干利便性という点でそうしたお客様を救えない、お客様にとってはなかなか購入する際のハードルが高くなってしまうかもしれないというところを加味しながら、組み立てております。

○委員：クレジットカードが与信審査のためのものであるにも関わらず、結局のところ決済方法としてカード番号とか有効期間のみで審査を通ってしまうという部分がそもそも弱点であるという気がして、その部分の有効性を高めることが本人確認にも繋がると思います。

○事務局：この本人確認の考え方ですが、これはやはりそれぞれの段階で本人確認をするということが大事だと思っております。例えばクレジットカードの業界様としては契約時にしっかり確認をするということ、また、それを活用されて事業活動を展開されている事業者におかれましても、クレジットカード会社様が実施した本人確認を利用するのではなく、その事業者自らが段階、段階で本人確認をやっていかないと、本人確認というのはうまく機能しないと思います。

○委員：カード会社の債権保全という意味から、クレジットカード取引において本人認証について力を入れてやっていこうとしております。ただこの件と、各種契約時における本人確認というのはまた別であるということを理解していただきたいと思います。クレジットカードが本人を証明するための手段だということであれば、それだけ厳密な確認作業をやらなければなりませんし、その分のコストを何かいただかなければならないぐらいの話になります。カード会社の本人認証は、あくまでも支払手段における債権者と債務者の債務保全、リスク回避のために実施しているということを御理解いただきたいと思っております。

○委員：確認ですが、データ通信カードが犯罪に使われる場合というのは、契約時に何らかの契約者本人の情報を偽装をして契約しているということが最も多いという理解でよろしいでしょうか。

○事務局：おおむねそういう理解でございます。

４．無線ＬＡＮとセキュリティ

【委員より、「無線ＬＡＮとセキュリティ」について説明】

○委員：一般家庭の中の無線ＬＡＮについては、一般家庭ではパソコンのネットワーク化というよりはインターネット回線を家の中でシェアリングするという形で普及してきて

おりまして、この結果、パソコンだけでなく、ゲーム機であるとかテレビであるとか、

最近ではプリンターに内蔵されて直接プリントできるというようなものへと展開されておりますし、携帯電話であるとか最近はやりのスマートフォンとかタブレットＰＣと呼ばれるものもほとんど無線ＬＡＮを内蔵しておりまして、家の外のいわゆるＷｉ-Ｆｉスポットと呼ばれているところでの接続等、いろいろな場所で使えるようになってきております。

無線ＬＡＮとセキュリティの重要性について御説明しますと、家の中、どこにいても無線接続ができるということは、逆に言いますと無線が届きさえすれば誰でもアクセスできる、誰でもそのデータに接続できるというところが問題になります。これを防ぐために暗号化をするというのが非常に重要になります。

無線ＬＡＮの場合、初期からＷＥＰと呼ばれる暗号方式が提案され、実装されておりますが、セキュリティの強化というのを取り組んできていまして 2004 年にＷＰＡ２と呼ばれている高度セキュリティの標準化をしております。

全くセキュリティの設定のされていないオープンのもの、それからＷＥＰを設定しているもの、そしてＷＰＡ、ＷＰＡ２を設定したものという３段階の状態を比較すると、やはりＷＰＡやＷＰＡ２の設定による対応が重要であるということです。

ステルス機能、Ａｎｙ接続の拒否、登録のないＭＡＣアドレスからの接続要求の拒否等

無線ＬＡＮには、セキュリティを保つための仕組みというものが様々入っておりますが、そもそもそうした機能が設定されなければ全く意味がなく、無線を使う場合にはセキュリティの設定が非常に重要になります。そのために私どもとしてはユーザーが意識しなくても簡単に接続設定ができる、しかも最新の暗号がかかった状態で接続設定ができるということを提案しておりまして、私どものＡＯＳＳと呼ばれているワンボタンでの無線接続設定及びセキュリティ設定というものを 2003 年から提案しており、こういったものをベースにＷｉ-Ｆｉ ＡｌｌｉａｎｃｅのほうでもＷＰＳと呼ばれております接続設定の提案がＷｉ-Ｆｉ Ａｌｌｉａｎｃｅの自主規格として制定され、これが 2007 年に標準的な規格として設定されています。

さらに最近では製品に工場出荷時からセキュリティキーを標準設定した状態で出荷し、何もしないと工場出荷時のセキュリティキーがかかった状態で使うことになるという仕組みも導入されております。

しかし、世の中には簡単に解読できるＷＥＰにしか対応していない機器がありまして、そういったものを接続しようとすると、標準状態のままでは接続ができません。ＷＰＡ２等で、ＡＥＳと呼ばれる強固な暗号化をかけた状態で使っておりますと、例えば、Ｗ

ＥＰにしか対応していない携帯ゲーム機を接続しようと思ったときに、全く接続ができないということになってしまいます。すると、ユーザーは、ゲーム機を接続するため、せっかく設定されたセキュリティを解除してしまいます。そこで、マルチＳＳＩＤという複数のＳＳＩＤを持つ機能を導入し、１つはＡＥＳで接続し、もう一方の口では、ＷＥＰ接続の口を作り、完全にオープンの状態にしてしまうということを防いでおります。

１つＷＥＰの口ができてしまうと、自分のネットワークが危ないのではないかという問題に対しては、ＷＥＰの口からは他のＡＥＳの口へは接続ができないという仕組みになっており、少なくとも自分のネットワークはＷＥＰの口が穴にならないという形になっております。

最後に、公衆無線ＬＡＮ、いわゆるＷｉ-Ｆｉスポットについて御説明しますと、これについては、誰でも自由に接続していくらでも踏み台にできるということにはなっていないと言っていいのではないかと思います。基本的には接続認証を行うというのが原則であり、通信事業者が設置されているＷｉ-Ｆｉスポットに関しては、３Ｇ回線契約のオプションとしてＷｉ-Ｆｉスポットが使用できるということになっており、会員契約をした者のみが認証により接続でき、それ以外の第三者が接続するということがないような仕組みになっています。

一部無料で接続できるフリースポットと呼ばれるサービスについては、ユーザー登録をするようになっており、携帯電話のメールアドレスを登録し、期限付きのキーと会員番号を入手することによって接続ができます。接続手続をすれば、メールアドレスのユーザーが、いつ、どこのスポットで接続をしたかという情報が、履歴としてサーバーに残るようになっております。また、プライバシーセパレータと呼ばれる無線接続端末同士の通信ができないような仕組みも導入しております。

５.無線ＬＡＮに係る論点説明

【事務局より、無線ＬＡＮに係る論点説明】

○委員：データ通信カードについては契約時における本人確認方法の問題、また、３Ｇの無線アクセスポイントについては、本人確認の問題と無線の問題、さらに、先ほどのお話のあった家庭やオフィスに設置された無線ＬＡＮについては、その周辺で不正に利用されるという問題、それから公衆無線ＬＡＮについては、サービスとしてインフラを提供していながら犯罪に使用されるという問題等に分類し、それぞれについて対策を考えなければならないと思います。

一つお聞きしたいのですが、古いＷＥＰしか対応していない機器にＷＰＡなり新しい

セキュリティ設定で対応すると、自動的にＷＥＰが解かれるのでしょうか。

○委員：マルチＳＳＩＤと呼ばれる複数のＳＳＩＤを持つ機能が搭載されていない無線ルーターの場合は、ＳＳＩＤが１つしかないので、ＡＥＳで接続したい、又はＷＥＰで接続したいといったときにどちらかを選択することになります。ＡＥＳの設定ができる機器は通常ＷＥＰの対応ができます。しかしＷＥＰの対応しかできないものはＡＥＳの設定ができません。結果としてＷＥＰの設定しかできない機器を接続するためにはＷＥＰ設定をするしかないのです。

○委員：ＷＥＰを自分でキーを設定して使っているうちに、機器が劣化し、ＷＥＰの設定が解かれた状態に戻るということはあるのでしょうか。

○委員：そういうことはありません。ＷＥＰの設定がされた機器は最後までＷＥＰの状態を維持し続けます。

○委員：一般家庭の使われている無線ルーターは、無線の接続設定をするときに同時に自動的にセキュリティの設定までされるという仕組みを搭載したものになっていると言っていいと思います。さらに工場出荷時のセキュリティ設定というものも導入されており、工場出荷時にそもそもそういう設定がされた機器がかなりの比率で一般家庭に入っていると言っていいと思います。

○委員：例えば我々の会社等は、もともとＰＣに挿入する形の通信カードを数万人という単位で使っていましたが、これが例えばモバイルＷｉ-Ｆｉルーターに変更しつつあります。このセキュリティ設定についてはＷＥＰではなく、ＷＰＡであり、パスワードは 15 桁なのですが、数字だけだと 15 桁ぐらいだったらブルートフォースをかければ数時間でおそらく当てられてしまうかもしれないと思っております。その辺については、業界としては例えば英数交じりにする、工場出荷時において何らかの措置をとる、若しくはユーザーが変更できるとか、そのような対策を検討されているのでしょうか。

○委員：これからスマートフォンの普及に伴い、モバイルＷｉ-Ｆｉルーターの普及も進むと思うので、この辺については危険性があるかもしれません。

６．サイバー犯罪捜査における事後追跡可能性の確保に向けた今後の在り方について

【事務局より、「サイバー犯罪捜査における事後追跡可能性の確保に向けた今後の在り方」について説明】

○委員：無線ＬＡＮについては、悪用されないようにするための暗号化の技術、ＷＰＡ等の技術が普及していく環境があるので、今後事態の改善は期待できると思います。一方、データ通信カードは、現状では、本人確認の手段としてクレジットカードによる決済を

代用しているということで、その結果、クレジットカードが悪用されることによりデータ通信カードが匿名で犯罪に利用されるということがあるのであれば、データ通信カードの販売時においても、携帯電話と同程度の公的書類による本人確認が少なくとも必要であると思います。

○委員：データ通信カード事業者における本人確認の実施状況について、プリペイド販売であるため本人確認を実施していない事業者もいるようでしたが、これは例えば外国人による犯罪に対処するという観点を踏まえた対処が必要かと思います。日本に来て、プリペイドの形態のものを利用する外国人もいると思います。そのような場合に、結局誰がそのデータ通信カードを使ったのか全く分からないという状況になってしまうと困ると思いますので、これは何とか状況を変える必要があるのではないかと思います。

○委員：トレースの部分について、無線ＬＡＮのアクセスポイントの電波の強度等を収集して自分の位置を割り出すようなデータベースがあるのと同様に、逆に移動しているＷｉ-Ｆｉに対する指名手配のようなイメージで、攻撃者が使用したと思われる痕跡のＭＡＣアドレス等の情報を登録しておき、定点観測をして、そこを通過しているＷｉ-Ｆｉの電波の中で一致するようなものがあれば警告を鳴らして追い込んでいくといった方法があってもいいのかもしれません。

○委員：無線ＬＡＮとデータ通信カードの問題については、契約時における入口対策、また、取得後に例えば不正に悪用されるという問題についての対策に切り分けて議論すると良いと思います。

○委員：本人確認が不十分な場合があるという問題に関して、私の疑問は何をもって本人と確認しているのかということについて疑問があります。確認する人の、例えばスキルの問題もあると思いますが、公的書類を使って本人確認をしたとしてもその手法が完成された正確なものでなかった場合には問題解決にならないのではないかと思いました。

以　上