ソニーの PSN/SOE での個人情報漏えいについての考察

2011/5/30

株式会社マインド・トゥー・アクション
中島浩光

はじめに：

本考察は、2011 年 4 月~5 月にかけて発覚した、ＰＳＮでの個人情報漏えい事件、SOE での個人情報漏えい事件に関しての情報セキュリティ面からの考察を一般に報道された内容をベースに行った資料であり、文責は株式会社マインド・トゥー・アクションにある。

事件の概要：

一連の事件の概要を時系列に整理する。

日付	概要
2011/4/16~17	米国ソニーオンラインエンターテイメント(SCE)のサイトへ不正アクセスが発生。約 2460 万人分の個人情報が漏えいした可能性。
2011/4/17~19	米国ソニーコンピュータエンターテイメント(SCE)が管理している PlayStationNetwork(PSN)に不正侵入が発生。約 7700 万人分の個人情報が流出
2011/4/20	SOE がシステムに脆弱性があるのを確認し、サービスを一時停止。
2011/4/21	SOE が脆弱性について「問題なし」と判断し、サービスを再開。
2011/4/21	PSN に障害発生。サービス停止
2011/4/27	SCE が PSN から約 7700 万人分の個人情報およびクレジットカード情報が漏えいしたと発表。
2011/5/1	SCE 社長を兼任するソニーの平井一夫副社長が都内のソニー本社で会見して謝罪。脆弱性を突かれたのが原因だと明らかにし、ハッカーが正常な動作として侵入したので検知できなかったと説明。情報開示が遅れたのは「膨大なデータの解析に時間がかかってしまった。なるべく確度の高い情報を届けたかった」と説明。
2011/5/2	SOE システムへの不正侵入と 2460 万件の個人情報流出の可能性が判明
2011/5/3	SOE からの個人情報流出をソニーが公表
2011/5/7	米国ソニー・エレクトロニクスの Web サイト上に人為的ミスにより 10 年前の約 2500 人分の個人情報（名前、住所の一部）が掲載されていたと発表。

2011/5/20	タイのソニーのサイトにフィッシング詐欺サイトが運営されていることが発覚。
2011/5/24	ギリシャのソニー・ミュージックエンターテインメントの Web サイトがサイバー攻撃を受け、約 8500 人分の個人情報（名前、メールアドレス、電話番号、パスワード）が流出したことを公表
2011/5/25	ソニー・エリクソン・モバイルコミュニケーションズのカナダ現地法人運営の Web サイトが不正侵入を受け約 2000 人分の個人情報（氏名、メールアドレス、パスワード）が漏えいしたと発表。

大体の経緯は上記の通り。

PSN から流出したとされる個人情報の内訳は以下の通り。

- 氏名
- 住所
- 電子メールアドレス
- 生年月日
- パスワード（ハッシュ化されている）
- PSN オンライン ID
- 購入履歴
- 請求先住所
- パスワード再設定用の質問への回答などのプロフィールデータ
- クレジットカード番号（暗号化済み）と有効期限
- ユーザーがサブアカウントを作成した場合はサブアカウントのデータ

SOE から流出したとされる個人情報の内訳は以下の通り。

- 氏名
- 住所
- 電話番号
- メールアドレス
- 性別
- 生年月日
- ログインＩＤ
- ハッシュ化されたパスワード
- クレジット/デビットカード番号と有効期限
- デビットカードの購入履歴、口座番号、口座名義、氏名、住所（豪、独、蘭、西ユーザ）

不正侵入の原因はどちらも、既知の脆弱性に対処できておらず、そこを攻撃されたこと。

ソニーはこの件に関して、アメリカの利用者が被害を受けた場合に一人当たり最大100万ドルの補償することを発表している。

また、すでに25件以上の訴訟が発生している。

考察：

一連のソニー関連会社の個人情報漏えい事件において考察するにあたって、押さえておくべき重要なポイントと考えるのは以下の点。

1. 流出した情報の価値について
2. ソニーは被害者なのか？加害者なのか？
3. 「既知の脆弱性」の意味
4. ソニー側のプライバシーポリシー
5. グループ企業において続いた不祥事
6. Pマーク等の審査・監査への影響
7. 事故の原因（運用の不備）

1．流出した情報の価値

今回の事件において流出した個人情報の内容として「クレジットカード番号」が注目されている。確かに、名前とクレジットカード番号と有効期限が分かれば多くのWebサイトでその情報を使って買い物が出来る。

しかし、ここまで騒ぎが大きくなってしまうと、消費者側もカードの利用明細に気を付けるし、カード会社側も気を付け始める。

ただ、今回は、「ID、メールアドレス、パスワード(ハッシュ化)、パスワード再設定用の質問の回答」といったものが流出していて、これが何を意味するか。現在ではいろいろなサービスがインターネット上で提供されており、サイトごとにログインID、パスワードを設定する必要があり、結果として、いくつものID、パスワードを管理しなくてはならない。しかしながら、そんなにたくさんのID、パスワードを覚えておくなんてのはまずできない。その結果、一つのID、パスワードを複数のサイトで使いまわすことになる。サービス提供側も独自のIDのを設定・発行する代わりに、ログインIDを顧客のメールアドレスにしたりする。

また、パスワードもハッシュ（一方向（不可逆）の暗号化）化がされているから、大丈夫という人もいるが、ハッシュのアルゴリズムが古ければ、総当たり攻撃でそれほど時間がかからずにパスワードを推測することが可能。

また、rainbow table と言われるものを使えば、ハッシュのアルゴリズムが新しくても、場合によってはパスワードが推測される。

つまり、今回漏えいした情報というのは、PSN や SOE だけでなく、他のサイトに、それこそ金融機関とか含めて、ログインに利用できる可能性が高い情報である。

実際に yahoo や so-net においてアクセス履歴を見ると、覚えのないところからログインされている、という情報もある。しかも、パスワードを間違えずに一発でログインしているらしい。

http://internet.watch.impress.co.jp/docs/news/20110520_447183.html

http://internet.watch.impress.co.jp/docs/yajiuma/20110520_446951.html

これが PNS 等から漏れた情報を使用したのかどうかは分からないが、関係を疑うべきだと個人的には思う。

２．ソニーは被害者なのか？加害者なのか？

たしかに、外部からの不正攻撃を受けたのだから、ソニー（というか実際に受けたソニー子会社）は被害者ではある。しかし、米国等で起きている訴訟の対象はソニーであり判決で有罪（？）となればソニーは加害者になる。

今回の個人情報漏えい事件については、「外部からの不正アクセス」と「個人情報漏えい」の２つの事件が複合・関連しているため、そのあたりをきちんと整理しておく必要がある。

まず、「外部からの不正アクセス」。これに関して言えば外部の攻撃者が加害者で、ソニーは被害者で間違いない。ただ、ソニー側から FBI に連絡されて捜査もされているが、現時点で攻撃者の特定は出ていないし、「自分が攻撃者である」という声明も出ていない（anonymous から「我々ではない」という声明は出ているが）。

では、「個人情報漏えい」のほう。今回の事件がアメリカの場合どの法律で判断すればよいのか正直よく分からないので、日本の個人情報保護法で解釈してみる。この場合、会員からの個人情報を預かったソニー側には預かった個人情報に対しての安全管理措置を講じる義務があるのだが、実際にこれだけ大規模な事故が起きたのだから、「安全管理措置を講じる義務を怠った」と解釈され、訴えられたわけである。まだ、裁判で判決が出たわけではないので、現時点ではソニーは「加害者扱い」なわけである（まあ、ほぼ黒に近いグレーというところ）。

３．「既知の脆弱性」の意味

PSN、SOE については「既知の脆弱性」を攻撃されている。ソニー側は「高

度な技術を持った侵入」と言っているが、攻撃されているのは「既知の脆弱性」であり、この「既知」という部分が重要である。「既知」であるということは攻撃対象となる製品なりソフトウェアに「こういう攻撃をすれば不正アクセスができるよ」ということが分かっており、また、「セキュリティパッチはこれだよ」と提供されている、もしくは、「回避方法はこうだよ」ということが分かっている、ということであるはず。つまり、不正アクセスを行う人間にとっては、既に知られた攻撃手法であるのだ。確かに「高度な技術」（誰に比べて？）が必要かもしれないが、「既知の脆弱性」を放っておいたということは、ソニー側が前述した「安全管理措置を講じる義務を怠った」と言える。

これが、コンピュータ・ウィルスのゼロデイ・アタックだったり、全く新しい攻撃手法に起因する情報漏えいであれば、ソニー側も「未知の脆弱性」とか「まったく新しい攻撃」と堂々と原因を言えるのだが、「既知の脆弱性」だからなのか「全部、攻撃してきたやつらが悪い！、俺たちは悪くない」というような声明が多いのは気のせいだろうか？

４．ソニー側のプライバシーポリシー

ソニー側のプライバシーポリシーの一部をいくつか以下に抜粋する。

まず、「ソニーグループ・プライバシーポリシー」

http://www.sony.co.jp/privacy/（改定日：2006 年 12 月 1 日）

http://www.scei.co.jp/privacy.html（改定日：2009 年 4 月 1 日）

（うーん、内容ほぼ同じで、文言確かに少し違うけど、名称同じなのに改定日が違うとは・・・まあ、細かいところは一旦おいておこう。）

===

ソニーグループ各社（「ソニー」。以下も同様とします。）では、お客様の個人情報は、ソニーへの信頼のもとお客様が自らの意思により特定の目的での利用のためにソニーに預託したものであり、その個人情報を安全に保管し、お客様の意思を尊重して利用することは、経営上の重要課題であると認識しております。

ソニーは、こうした認識のもと、以下の通り個人情報の取り扱いに関するポリシーを定め、お客様からお預かりした個人情報の適切な取り扱いに取り組んでまいります。

*本ポリシーは、ソニー株式会社およびその日本国内の子会社を対象としたものです。

（中略）

（安全管理措置）

5. ソニーは、お預かりした個人情報を利用目的の範囲内で正確・最新の内容に保つよう努め、不正なアクセス、漏えい、改ざん、滅失、き損等を防止するため、現時点での技術水準に合わせた必要かつ適切な安全管理措置を講じ、必要に応じて是正してまいります。

===

なるほど、「経営上の重要課題だと認識しており」、「現時点での技術水準に合わせた必要かつ適切な安全管理措置を講じ」るわけですね。

まあ、日本国内限定ですが。ただ、この日本国内限定は US や欧州にまで適用しようとすると書かなくてはいけないことが非常に多くなってしまうので日本国内限定にしているのではないかと思うのですね。

では、US の PSN のプライバシーポリシーのセキュリティに関する部分。

http://us.playstation.com/support/privacypolicy/index.htm

Last Revised: April, 2011

==

Accuracy & Security

We take reasonable measures to protect the confidentiality, security, and integrity of the personal information collected from our website visitors. Personal information is stored in secure operating environments that are not available to the public and that are only accessible to authorized employees. We also have security measures in place to protect the loss, misuse, and alteration of the information under our control. Unfortunately, there is no such thing as perfect security. As a result, although we strive to protect personally identifying information, we cannot ensure or warrant the security of any information transmitted to us through or in connection with our websites, that we store on our systems or that is stored on our service providers' systems.

==

“reasonable measure”ですね。で、” Unfortunately, there is no such thing as perfect security.”は、まったくもって同意。なので、” we cannot ensure or warrant the security of any information” の部分についても同意。「保証します」なんて口が裂けても言えない。

問題は、reasonable measure　とはどういうことか、なんですけどね。

日本の PSN のプライバシーポリシー（というか個人情報の取り扱いについ

て）

http://legaldoc.dl.playstation.net/ps3-eula/psn/j/j_privacy_ja.html

===

7. 安全対策

SCE は個人情報の保護のために合理的な安全管理措置を設けています。これには個人情報への不正アクセスや不正公開を最低限にするための仕組と手段が含まれます。しかしながら、SCE は不正アクセスによる個人情報悪用の全てのリスクを排除することを保証できません。PSN／Qriocity のアカウントへの不正アクセス、PSN のアカウントとお客様が PSN のアカウントに保存している決済情報の不正利用を防ぐため、お客様ご自身でパスワードを適切に管理してください。ハードウェア本体を第三者に使用させたり、または第三者に譲渡する（販売店への返品または修理のための返送等を含む）際、自動サインイン機能をご利用の場合は必ずオフにしてください。

===

まあ、米国 PSN と大事なところは変わりません。Reasonable mesure⇒「合理的な安全管理措置」、「SCE は不正アクセスによる個人情報悪用の全てのリスクを排除することを保証できません。」となっています。さあ、で「合理的」ってどういうことでしょうねぇ。

米国ソニー（Sony Corporation of America, SCA）のプライバシーポリシー

http://www.sony.com/terms.shtml

Security

While SCA cannot guarantee that unauthorized access will never occur, rest assured that SCA takes great care in maintaining the security of your personal information and in preventing unauthorized access to it through the use of appropriate technology and internal procedures.

こちらでも、不正アクセスが発生しないことを保証してはいないです。ですが、”great care in maintaining the security…..” セキュリティ対策の維持に「great care」をすると書いてます。”care”というのは注意を払う、予防する、というような意味ですが、「実施する」という宣言とはちょっと違うのでしょうか？

米国 PSN のプライバシーポリシーで出てきた、reasonable、日本語のほうだと「合理的」になると思うのですが、「合理的」ということは「論理」があるわけです。ソニーグループとして個人情報保護は「重要な経営課題」であり、実際今回の事件でかなりの社会的信用・ブランドに傷もつけ、かなりの額の損害賠償が発生しているわけです。そういった中で「既知の脆弱性を放置しておく」というのは「合理的な安全管理措置」と言えるのでしょうか？「想定外でした」ということもないでしょうから。

5．グループ企業において続いた不祥事

今回の事件、最初の PSN の 7700 万件でその件数の多さにびっくりしたが、時期をおかずして SOE の 2460 万件。で、各国の子会社で千件レベルの漏えいとか、フィッシングサイトを仕込まれたとか、ソニーにとっては「弱り目に祟り目」、「泣きっ面に蜂」というレベルを通り越して、あちこちボロが出てきている。

現実としてあちこちボロがあったのは事実なんでしょうが、一つの企業グループでこうも立て続けに事故が発覚するのは、非常に珍しい。今までの個人情報漏えい事件を見ていても、大体単発で終わっている。

このことから言えるのは、企業がグローバルにビジネスを展開し、各国に子会社・関連会社を作って、ネット上にサイトを作ってそこで何らかのビジネスをするということは、確かに市場も顧客も大きくなるかもしれない。ただ、市場や顧客が大きくなると企業にとっての脅威も大きくなる。全体の割合で言えば微々たるものかもしれないが、全体が大きくなるから「微々たるもの」の大きさは大きくなる。

また、多くの子会社・関連会社がある企業グループに結構多いのは、親会社のセキュリティは厳しいが、子会社・関連会社のセキュリティは結構ボロボロ、というもの。親会社は潤沢な資金を背景にセキュリティもきちんとやっているが、子会社・関連会社は予算がなくてセキュリティに回せる予算がない。

今回の事件では、PSN の 7700 万件という件数の大きさから、世界中にニュースが流れた。それが世界各国のソニー子会社・関連会社への不正アクセスを誘発した可能性もあるのではないか。

6．プライバシーマーク等の審査・監査への影響

今回のようにインパクトが大きな事件があると、関連する認定・認証の審査に影響があります。これまでの例でいうと、「外部委託業者から情報漏えい⇒外部委託の管理」、「管理者による情報漏えい⇒管理者権限まわり」というように審査において重点的にチェックされる傾向にありました。

では、今回の事件からどういう傾向になることが考えられるか、であるが、以下の 4 点あたりが怪しいと考えている。

① 脆弱性管理プロセス
② ログの保護
③ 事故対応手順、BCP
④ 改ざん検知

①脆弱性管理プロセス

今回の事件の原因が「既知の脆弱性の放置」というところにある以上、脆弱性管理プロセスは見られる可能性が非常に高い。ただ、今までもこのあたりはふつうにチェックがされているところでもあるが、これまで以上に細かく・厳しく突っ込まれる可能性もある。

特に、インターネット上のサイトでビジネスを行っているようだと、気を付ける必要がある。チェックされると思われるポイントは、脆弱性の検知・把握、脆弱性の評価、脆弱性への対応方針判断、脆弱性への対応・確認といったあたりのプロセス・手順の確立と運用状況の確認といったところか。

②ログの保護について

PSN の今回の事件においては、不正アクセスを行った犯人はアクセスログを消去していったらしい。それがもとで事後対応に時間がかかったりしている。

これまでも、重要情報へのアクセスログの取得については審査等においてチェックされていたと思うのですが、今後はさらに取得したアクセスログの保護がされているかどうかを指摘される可能性がある。ただ、ログの保護と言っても簡単に実装できるのであればいいのだが、なかなかそうもいかないのが現実である。それを審査側/監査側が理解していれば、厳しいことは言わないのでは？とも思うのだが。

③事故対応手順、BCP

今回の事件でソニー側に対して、「対応が遅い！」とか「もっと早く公表すべき！」とかいう批判がある。個人的には、今回のソニーの事故対応のスピードや手順については「悪い」とは思わない（実際の対応内容が結果としてお粗末なものがある、というのは別の話）。ただ、地震や原発事故の関係もあり事故発生時の手順、BCP といった部分についてはあらためてチェックされる可能性が高い。

④改ざん検知・整合性監視

今回の不正アクセスにおいては既知の脆弱性を攻撃され不正プログラムを埋め込まれている。こうしたことから、サーバ上のコンテンツを改ざんされる、不正プログラムを埋め込まれる、コンテンツを消去される、と言ったことへの有効な対応策として改ざん検知やファイル整合性監視というものがある。コンテンツやサーバの設定が改ざんされていないか、整合性が侵されていないかといったことをきちんと確認しているか、ということがチェックされることも考えられる。

7．事故の根本原因

今回の事故の原因が「既知の脆弱性の放置」であるというのは述べてきたとおり。では、そのさらに深い「根本原因」は何か？つまり、「なぜ、既知の脆弱性を放置してしまったのか？」。報道されている記事を見た限り、「SCE の経営陣は今回の脆弱性について把握していなかった」とされている。つまり、現場の担当者が見逃したのか、知らなかったのか、中間管理職が報告を軽視したのか、経営陣に報告しても無視されたのか分からないが、技術的な問題ではなく、「セキュリティの運用がうまくいかなくて発生した」といえると思う。

運用は、手続き・マニュアルがあればよいのではない、それを運用する人間達がいて、その人間に必要な知識・スキルがなければ運用はうまくいかない。

つまり、なんらかのツールを入れれば解決するものではなく、システムセキュリティの知識を持った人間がちゃんといたのか？また、情報セキュリティは技術的な面がフォーカスされがちであるが、組織として考えれば情報セキュリティをビジネス面から判断する能力を組織として持つ必要がある。これは経営陣や管理職がそういう能力を持ってもいいし、それが難しければ、誰かがセキュリティ面とビジネス面をそれぞれ経営陣が判断できるように「翻訳」してもよい。外部の専門家に意見を聞くのもいいだろう。

とにかく、個人としてというよりは、組織としてセキュリティに関する適切な能力がなくてはいけないと思う。

特に今回の案件でいえば、「7700 万件の個人情報」というとてつもなく大きな爆弾を抱えてビジネスをしていたのだから、セキュリティの運用体制が根本原因だったのではないかと思う。

提言：

上記の考察を踏まえて、いくつかの提言。

＜今回の事件で個人情報が漏えいしてしまった個人の方へ＞

今回の件で PSN からもクレジットカードの利用明細の確認、パスワードの変更が推奨されてはいるので、少なくともこれはやっておいた方が良い。また、「秘密の質問」の設定（質問内容と答え）についても変更をしておくことを推奨する。パスワードが分からなくても秘密の質問と答えが分かれば他人がパスワードを再設定することが可能になってしまうかもしれない。

ただ、もっと良いと思うのは、一度退会して、別の ID/メールアドレス/パスワードで入会する（その気があれば）のが良いと思う。

また、漏えいしたメールアドレスの元サイト（例：xxx@yahoo.co.jp であれば www.yahoo.co.jp）や、ID/メールアドレス/パスワードを使いまわしている他サイトのログイン履歴を確認して欲しい。もし、そこで明らかに自分がアクセスしたものでない（通常使っていない場所・プロバイダからログインされている）ものがないかを確認し、もし、怪しいと思ったなら、そのサイトで不正が行われていないかを確認して欲しい。

また、使いまわしていたパスワードは変更したほうがいい。

＜サイト上で大量の個人情報を保有する企業向け＞

まずは、現時点において個人情報を大量に保持していることはそれだけの「爆弾」を抱えているのだということの認識を改めてしてもらいたい。ただ、実在の取引の確保や会員サービス等も必要であるから、個人情報の利活用なしではビジネスが成り立たないというのも事実である。だからといって情報セキュリティ対策にお金をかけてください、と私の商売を考えると言いたくもなるのですが、それよりも、自分たちがビジネスをしようとしている環境が持っているリスクについてもっと勉強というか理解をしてください。インターネット上でどんな人たちが活動しているのか、有名になるということはどういうことか、そこにどんなリスクがあるのか、財務リスク、市場リスク、取引先の信用リスク、カントリーリスクと同じように情報セキュリティリスクも考えてください。そのうえで、予算が十分にあるのであれば情報セキュリティにお金をかけるのもよいでしょう。もし、予算がないのであれば、ないなりにどうすればよいのか考えましょう。インターネット上に役に立つ情報もありますし、専門家に手伝ってもらうのもいいでしょう。

そうやって、組織としての情報セキュリティの能力を高めていってほしいのです。

また、ISMS 認証や P マーク認定を取得している企業の方は、今後の審査においてログの保護、脆弱性管理プロセス、事故対応/BCP といったところを今年の審査の前に見直しておいたほうが良いかもしれません。審査の時に対応が完了していな

くても、現在その部分の対応実施中とか実施予定という状況であれば、乗り切れる可能性も高いと思います。

＜一般の方々へ＞

今回、PSN/SOE 等で情報漏えいが起こり、事故が「検知」されましたが、「検知されていない事故」があるかもしれません。アクセスしているサイトが大企業や有名企業のサイトだからといって安心はしないでください。実際、今回の事件の例や「Gumbler」というコンピュータ・ウィルスは国内の有名企業のサイトに感染していました。したがって、「自分の身は自分で守る」という意識を持ってください。また、自身がどのような情報をサイトに預けているのか？その情報の漏えい・悪用されていないかを定期的に確認しましょう。具体的には、

- クレジットカード番号：利用明細のチェック
- ID/パスワード：ログイン履歴に身に覚えのない時間帯・アドレス等からアクセスされていないか？

といったところです。

また、簡単なパスワードをいろいろなサイトで使いまわすのは危険です。使いまわすのであれば複雑なパスワードを使いましょう。