個人情報漏えいの事例分析と対策についての一検討

原　田　良　雄

A Study of Case Analysis and Countermeasures disclosure of personal information

HARADA Yoshio

目　次

Abstract

When the protection of personal information is neglected and information is leaked through mismanagement, companies are significantly impacted in various ways, including loss of public confidence, suspension of business operations, and the requirement to pay damage compensation.

In this study, through internet news we investigate incidents of personal information leakage, introduce example cases, analyze the causes, and discuss countermeasures. With the spread of the internet and the accumulated storage of large amounts of personal information in databases, incidents of information leakage have become more common, due to unauthorized access obtained, for example, via the internet by exploiting the vulnerability of servers. Moreover, data leakage through mismanagement and deliberate removal of data from the premises also occurs. These issues have become a major threat to firms. We also discuss leakage of personal information resulting from the spread of social media and the increase in use of free software.

キーワード：個人情報漏えい、不正アクセス、個人情報保護対策、ウイルス感染
Key words：Disclosure of personal information, Unauthorized access, Protection of personal information, Virus infection

1．はじめに

個人情報保護を怠り不適正な管理によって情報漏えいした場合、企業は、社会的信用の失墜、業務停止、賠償被害など、大きな影響を受ける。

個人情報保護法[1]（2005年４月１日から施行）では罰則規定も設けられており、「主務大臣」の命令に違反すると６カ月以下の懲役か30万円以下の罰金に処せられ（56条）、報告の徴収に対する報告を怠ったり、虚偽の報告をすると、30万円以下の罰金に処せられる（57条）。また、罰則には「両罰規定」が設けられており、違反行為をした者だけでなく、企業も処罰の対象となっている（58条）。つまり、会社としての管理体制・管理責任を問われるのである。例えば、ある社員が個人情報を持ち出し不正に利用した場合、その社員だけではなく、企業も処罰の対象になる。加えて、漏えいした個人情報の本人から、漏えいによる被害や、実被害が無くても、漏えいしたという事実による損害賠償民事訴訟のリスクが発生する。これらによって、大規模漏えい事件事故の場合は巨額（総額）の賠償金支払いに直面する可能性がある。

本稿では、個人情報漏えいの事件・事故（以降、「インシデント」という）情報をインターネットニュース等で調査し、事例を紹介しつつ原因分析を行い、対策を議論する。個人情報漏えいインシデントは、インターネットが普及し、データベースに大量の個人情報が蓄積されている環境下において、ネット経由からサーバーの脆弱性をついて侵入する等の不正アクセスにより大量の個人情報が漏えいしている。また、個人情報保護法が全面施行されているにもかかわらず、相変わらず、管理ミス、故意によるデータ持ち出し等により個人情報漏えいが発生している。これらは、企業によって大きな脅威となっている。また、ソーシャルメディアの普及やフリーソフトウェアの利用拡大による、個人情報漏えいについても議論する。

2．個人情報漏えい

「個人情報漏えい」は、個人に大して精神的苦痛や経済的損失を及ぼすだけだはなく、企業の信頼を失墜させ、企業に賠償金額や対策費用など予定外の大きな負担を強いることになる。問題を認識し、予め対策を講じることが肝要となる。本章では、まず、個人情報漏えいの具体例を紹介する。次に、個人情報漏えいについて、統計的な情報を紹介する。

[1] http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/030307houan.html

2.1　ヤフー BB の例

ADSL サービス「ヤフー BB」を運営するソフトバンク BB 代表取締役社長兼 CEO 孫正義氏は、ヤフー BB のデータベースから流出した会員の個人情報が451万7,039件であることを確認した、と2004年２月27日発表した。このニュースは当時、テレビ、新聞等で取り上げられ、その漏えい規模と賠償総額の大きさから記憶に新しい。流出した個人情報は申し込み時の住所、氏名、電話番号、電子メールアドレス、ヤフージャパンの電子メールアドレス、申し込み日で、クレジットカード番号などの信用情報は含まれていなかった。事件発生後、ソフトバンク BB は会員に対し、お詫び金として１人当たり500円の金券を送付した。郵送料も含めると、要した総額は約40億円。さらに株価やセキュリティ対策費用なども含めると総額100億円以上の費用が発生したという。また、2006年５月19日には、大阪地方裁判所から民事訴訟を起こした Yahoo! BB 会員ら５人に対して賠償命令が出された。一人当たり5,000円の賠償金であった。これは、当初の全員へのお詫び金500円の10倍にあたる。全員が訴訟を起こせば､大変な金額になったことだろう。この事件の発端は、ソフトバンク BB で働いていた元派遣社員の軽率かつ悪質な行動であった。そもそも在職中に使っていたソフトバンク BB の顧客データベースとリモートメンテナンスサーバーの２つのアクセス用 ID ／パスワードが、本人が退職後、削除もしないで有効状態であったことに起因する。この元派遣社員は、この２つのアクセス用 ID ／パスワードを使い、犯人の前で Yahoo! BB の顧客情報にアクセスできることを自慢した。犯人は、この場で ID とパスワードを記憶し、都内のネットカフェからソフトバンク BB 内のリモートメンテナンスサーバーに侵入。そして、顧客データを盗み出し、それがソフトバンク BB に対する恐喝事件につながった。

2.2　個人情報漏えいインシデントの統計情報

2010年の漏えい人数は約558万人、想定損害賠償総額約1,215億円である。漏えい原因としては「管理ミス」（610件）、「誤操作」（543件）が大半を占めている。2010年は、特定の情報通信業において不正アクセスにより、大規模（約174万人）な事件が１件発生しているため、人数ベースの漏えい業種は「情報通信業」、漏えい原因は「不正アクセス」が突出した結果となっている[2]。

2007年は、インシデント件数は少ないものの、漏えい人数は最大であった（具体的な事例は、３章に記載する）。2010年は、インシデント件数は最大であった。一人あたりの平均想定損害賠償金額は、３万円後半から５万円の範囲に収まっている。

[2] NPO　日本ネットワークセキュリティ協会　2010年情報セキュリティインシデントに関する調査報告書

図表２－１　インシデント・トップ10

No.	漏えい人数	業　　種	原　　因
1	173万5,841人	情報通信業	不正アクセス
2	46万3,360人	情報通信業	内部犯罪・内部不正行為
3	31万人	医療、福祉	不正な情報持ち出し
4	25万4,122人	卸売業、小売業	不正アクセス
5	20万1,414人	学術研究、専門・サービス業	管理ミス
6	19万7,907人	情報通信業	盗難
7	19万7,077人	製造業	設定ミス
8	19万5,132人	サービス業（他に分類されないもの）	不明
9	17万755人	サービス業（他に分類されないもの）	不正アクセス
10	17万325人	金融業、保険業	管理ミス

出所：NPO　日本ネットワークセキュリティ協会
2010年　情報セキュリティインシデントに関する調査報告書（表３－２）

図表２－２　漏えい人数とインシデント件数の経年変化

	インシデント件数	漏えい人数
2005年	1,032件	881万4,735人
2006年	993件	2,223万6,579人
2007年	864件	3,053万1,004人
2008年	1,373件	723万2,763人
2009年	1,539件	572万1,498人
2010年	1,679件	557万9,316人

出所：NPO　日本ネットワークセキュリティ協会
2010年　情報セキュリティインシデントに関する調査報告書（表３－４）よりデータ抽出

文献［情報セキュリティ白書2011］[3]によると、近年の情報漏えいインシデントの特徴は以下の通りである。

2010年度「情報漏えい原因別分類」によると、2009年度では第１位として40％を占めていた「ファイル共有ソフト」は12％に減少し､「不正アクセス･サイバー攻撃」が75％でトップとなった。また､「人的ミス」は22％から11％に減少している。

３．個人情報漏えいインシデント事例

「個人情報漏えい」の件数の大きいものをピックアップして記述する。

[3] 情報セキュリティ白書2011、独立行政法人　情報処理推進機構（IPA）pp. 17

⑴ 2011年の主な事例

ウィキペディア[4]から、2011年４月に発生したソニーが運営するプレイステーションネットワーク（PSN）における過去最悪１億人以上の個人情報流出事件を紹介する。

- （2011/04/27）ソニーおよびSCE（プレイステーションネットワーク） 全世界*7,700万名*の個人情報漏えい。ネットワークサービス「プレイステーションネットワーク」に対し、４月21日に不正アクセス攻撃が始まり、同日よりPSNの全サービスを停止。住所、氏名、メールアドレスなどが流出した不正アクセスがあったと１週間後の４月27日に発表。事件発生から１週間過ぎての公開に国内のみならず世界各国でソニーに対しての聴聞会の任意出頭が要請されている。
- （2011/05/03）SOE（ソニーオンラインエンタテインメント）*2,460万名*、PSN情報漏えいより以前の４月19日にSOEへの不正アクセス攻撃があり、直後の調査では問題なしと判断されていたが、５月１日のPSN謝罪会見より２日後の５月３日にSOEアカウントサービス登録者の住所、氏名、メールアドレスと2007年当時のクレジットカード情報、デビットカード履歴などが流出した可能性があると発表。これによりソニーグループとしての漏えい数は*１億160万件*となり、過去最悪の情報漏えいとなった。
- ５月４日、米下院エネルギー・商業委員会小委員会が行なった公聴会に（招致されていた）ソニー幹部が欠席し、非難を浴びた。公表された回答書によると、すべての利用者7,700万人の個人情報が不正利用者から盗まれたことが明らかになった。
- 経済産業省の行政指導記録から、管理責任者を擁していなかったなどソニーの杜撰な管理体制が明らかとなった。
- ソニーは５月１日に緊急記者会見を行い、サーバーの脆弱性に対処していなかったことが不正侵入の原因であると発表した。ソニーは「サービス停止を我慢しているユーザーへの感謝」（謝罪ではない）として､PSNの有料会員サービス「プレイステーション プラス」（PS+）の30日利用権の付加を実施するとしたものの、個人情報流出に対する一律的な補償に関しては否定した。
- （2011/05/03）SOE（ソニーオンラインエンタテインメント）2,460万名、PSN情報漏えいより以前の４月19日にSOEへの不正アクセス攻撃があり、直後の調査では問題なしと判断されていたが、５月１日のPSN謝罪会見より２日後の５月３日にSOEアカウントサービス登録者の住所、氏名、メールアドレスと2007年当時のクレジット

[4] http://ja.wikipedia.org/wiki/%E5%80%8B%E4%BA%BA%E6%83%85%E5%A0%B1%E6%BC%8F%E6%B4%A9 ［2012.4.10 last visit］

カード情報、デビットカード履歴などが流出した可能性があると発表。

- （2011/06/03）ソニー・ピクチャーズ、約100万件およびミュージックレコード75,000件・ミュージッククーポン350万件、個人情報漏えい。クラッカー集団LulzSecによるもの。グループとして1億261万3,000件の漏えい。

以上のことから、原因は、サーバーの脆弱性[5]に対処していなかったことから不正アクセス攻撃を受けたこと、管理責任者がおらず杜撰な運営であったことであり、対応の遅さや説明責任の意識が薄いことも問題であった。

［YOMIURI ONLINE］[6]によると、プレイステーションネットワークでは、アプリケーションサーバーと呼ばれるプログラムに既知の脆弱性があった。ここを犯人に突かれて侵入されている。ソニーが発表した侵入経路の流れは以下の通り。

①まず犯人はアプリケーションサーバーの脆弱性を突き、通信ツールをプレイステーションネットワーク内に不正に導入（裏口の確保）。

②設置した通信ツールによって、個人情報が保管されているデータベースサーバーへのアクセス情報を入手。

③アクセス情報を使って、外部からデータベースに不正アクセス。個人情報をダウンロード。

ファイアウオールやIPS（侵入防止システム）はあったものの、それを通り抜けている。これについてソニーの業務執行役員・長谷島眞時氏は「正規の通信として、入って出てくる方法で脆弱性を突かれている。そのため不正アクセスとして検知できなかった」と述べている。「最大の問題は、脆弱性に対処していなかったことにある。一般的に対処は難しく、わかっていても直すためのプログラムがなかったり、システムの更新ができなかったりなどの問題で対処できないこともある。しかし、長谷島氏によると「わかっていて更新できなかったのではなく、脆弱性に対処していなかった」とのこと。つまり放置していたことになる。巨大なネットワークを運営しているのにもかかわらず、脆弱性に対処していなかったのはお粗末である。

ユーザー側の対策としては、以下の4ポイントに気をつけたいとしている。

①クレジットカードの利用状況を必ず確認する

---

[5] 脆弱性とは、外部からの不正なアクセスなどによって不正に利用できてしまう問題点・欠陥のこと

[6] http://www.yomiuri.co.jp/net/security/goshinjyutsu/20110502-OYT8T00649.htm［last visit 2012.4.11］

登録したクレジットカードの利用状況・請求書を確認する。身に覚えのない請求があったら、すぐにクレジットカード会社に報告して請求をストップさせること。併せてソニー・コンピュータエンタテインメントの窓口に報告しよう。

②パスワードを必ず変更する

プレイステーションネットワークが再開次第、すぐにアクセスしてパスワードの変更を行うこと。ネットワーク側で変更するように指示が出るので、今までとは異なるパスワード、かつ他のサービスで使っていないパスワードを登録しよう。

③他のサービスで共用しているパスワード・秘密の質問があれば変更

これがもっとも厄介かもしれない。プレイステーションネットワークで使っているパスワードを、他のネットサービスで使っている場合は、そちらも変更する。流出したパスワードでの不正アクセスを防止するためだ。加えて、今回はパスワードを思い出すための「照合質問（秘密の質問）」も流出した可能性がある。「照合質問（秘密の質問）」とは、パスワードを忘れた場合に「母の旧姓」「中学校の名前」などの質問でパスワードを照合するもの。他のサービスで同じ質問を使っている場合は変更しよう。

④便乗した詐欺に注意する

今回の不正アクセス事件に便乗した詐欺に要注意。メールや電話でパスワードを聞かれても一切答えてはいけない。ソニー側から電話やメール、郵便などでユーザーの個人情報を聞くことはない。不正アクセス事件解決のため、と称して個人情報を聞く電話やメールは無視しよう。

賠償金については、「カナダの女性が総額840億円の損害賠償を求め、訴えを起こしていた。弁護士によると、原告側はカナダの利用者約100万人の情報が流出したと主張、集団訴訟を目指しているため、損害賠償額が約840億円になっているという。」[7]

⑵　2010年の主な事例

- （2010/11/10）サミーネットワークス（777town.net）、173万5,841名の個人情報漏えい。オンラインゲームサイト777town.net に10月23日から不正アクセス攻撃がはじまり、11月４日から11月10日までの期間に複数回、外部からの不正アクセスの痕跡を確認、個人情報は、姓のみ、名のみ、郵便番号の一部が漏えいとゲーム用ログイン ID、パスワード、メールアドレスが流出。2010年11月19日午前10時よりサービス再開。（図表２－１の No.１に相当）
- （2010/11/01）ルーク19（サンプル百貨店）、46万3,360名分の氏名、性別、生年月日、

[7] http://raicho.2ch.net/test/read.cgi/newsplus/1304579409/ ［2012.4.10 last visit］

住所、電話番号、メールアドレス、職業、世帯年収、家族構成など。二次被害（架空請求）。従業員が顧客情報を持ち出し複数の名簿業者に売却。（図表２－１のNo.２に相当）

- （2010/09/27）ユニットコム（フェイス／ツートップ）、最大25万4,122名分。2010年９月13日、クレジットカード会社より通販サイトWebサーバーからクレジットカード情報が流出した可能性があるとの指摘を受け判明、９月27日発表。海外からの不正アクセスがあり、顧客情報の一部が流出。フェイスWebサイトにて、2008年６月26日～2010年８月17日の期間に、クレジットカードを利用した顧客７万4,048名分のクレジットカード番号およびクレジットカード有効期限が流出。ツートップにて、1999年６月29日～2008年９月10日の期間に登録された会員個人情報が最大18万74名分流出していた可能性があることが判明した。（図表２－１のNo.４に相当）

⑶　2009年の主な事例

- （2009年04月８日）　三菱UFJ証券株式会社は、同社元社員による顧客情報の不正持ち出しおよび流出の事実が判明したと発表した。情報の内容は、顧客の氏名、住所、電話番号（自宅･携帯電話）、性別、生年月日、職業、年収区分、勤務先名、勤務先住所、勤務先電話番号、勤務先部署名、役職、業種。同社元社員が不正取得し自宅に持ち帰った顧客情報は1,486,651人分で、そのうち、平成20年10月３日から本年１月23日までに新規講座あるいは投信ラップ口座を開設した顧客49,159人の情報を名簿業者へ売却した[8]。

⑷　2008年の主な事例

- （2008/11/03）セガ、アルバイトの応募者合計115名分の個人情報が外部に流出漏えい。氏名、年齢、住所、本籍地、生年月日、電話番号等。Googleマップ経由で流出。Googleマップの「マイマップ」機能で個人情報が相次いで流出した問題で、アイシェアが実施したユーザー意識調査によると、流出は「設定のデフォルトが公開なのが原因」とgoogleに責任があるとする意見が44％と最多だった一方で、「公開設定か確認せずに利用したのが原因」とする自己責任派も37％だった[9]。
- （2008/04/06）サウンドハウス、顧客情報最大９万7,500件。うち２万7,743件はクレジットカード情報含む。中国からのSQLインジェクションによる不正アクセス。SQLインジェクションとは、データベースと連動したWebサイトで、データベースへの問い合わせや操作を行うプログラムにパラメータとしてSQL文の断片を与えることにより、データベースを改ざんしたり不正に情報を入手する攻撃。また、そのような攻

[8] http://www.sc.mufg.jp/［2012.4.9 last visit］

[9] ITmedeiaニュース　http://www.itmedia.co.jp/news/articles/0811/26/news064.html［last visit　2012.4.10］

撃を許してしまうプログラムの脆弱性のこと。SQL インジェクションはパラメータを SQL 文に埋め込む際にきちんとチェックが行われていないために起こる。パラメータ中に SQL 構文や SQL 文で特殊な意味を持つ文字が含まれていないか調べ、含まれていた場合はこれを削除したり別の文字列に変換（エスケープ）するといった処理を組み込む必要がある[10]。

⑸ 2007年の主な事例

- （2007/10/17）富士通エフサス、千葉県職員の個人情報*1万5,000件分*。業務委託先である富士通エフサス社員の私物 PC がウイルスに感染し、Share[11]経由で流出。
  この原因は、仕事上のデータを私物 PC に入れていたことに起因する。公私混同。
- （2007/07/26）アメリカンファミリー生命（アフラック）、顧客情報15万2,758人分、契約情報20万4,716件分。同社代理店の社員が通勤中に顧客情報（住所、氏名、生年月日、性別、契約内容等）の入ったパソコンを置引きされる。保険業界で過去最大規模の個人情報漏えい事故であった。
- （2007年）ドコモ関西の販売代理店であるパナソニック・テレコム株式会社が運営するドコモショップ草津駅前店（滋賀県草津市、平成20年10月19日閉店）のスタッフ（派遣社員）が業務中に不正検索し、顧客の住所・生年月日などの情報を社外（探偵事務所等）に漏らした。顧客より「携帯電話番号しか知らない人が突如自宅を尋ねてきた」とドコモに相談が有り事件が発覚した。ドコモ関西が記者会見にて謝罪（関西地区のみ放映）、新聞に謝罪文掲載、顧客情報管理システム ALADIN のセキュリティー強化を行った。ドコモは本件解決に数億円の経費が掛かった。

⑹ Winny ウイルスによる情報漏えい

Winny ウイルスによる情報漏えいは2004年にも話題になったが、2005年後半からは警察や自衛隊、原子力発電所関連、通信会社など社会インフラを担う官公庁や企業からの漏えいが相次いだ。漏えいの危険はすべての企業にあるといっていい。PtoP ネットワークを使ったファイル共有ソフトウェア「Winny」を悪用するワーム・ウイルス[12]による情報漏えいが、立て続けに起きている。2006年１月から40件以上の情報漏えいが報道された。Winny ウイルスによる情報漏えいで顕著なのは、私用 PC を使っていて Winny ウイルスに感染したケースが多いことだ。「Antinny」などの Winny ウイルスに PC が感染すると、

---

[10] IT 用語辞典　e-Words http://e-words.jp/

[11] Windows2000/XP/vista/7上で動作するファイル共有ソフト、Peer to Peer モデルを用いて通信させる。

[12]それ自身が独立して実行可能なプログラムであるので、あるシステムからあるシステムに感染しようとする時に宿主となるファイルを必要としない。ネットワークを介して、攻撃先のシステムのセキュリティホールを悪用して侵入する事が多い。

PC内のファイルが勝手にWinnyの公開フォルダに入れられてしまう。公開フォルダに入れられたデータはほかのWinnyユーザーが自由にダウンロード可能。時間と共にファイルは拡散する。私用PCに業務データや顧客情報を保存していた場合は、そのデータもWinnyネットワーク上でダウンロード可能になってしまうわけだ。民間企業でも私用PCから情報漏えいするケースが相次いでいる。NTT東日本は約1,400人分の顧客情報を流出させた。NTT東日本栃木支店の社員が業務データを自宅に持ち帰り、作業をしていた。そのPCがWinnyウイルスに感染、漏えいしてしまったようだ。岡山県警や愛媛県警などのケースでも私用PCからデータが漏えいしている。私用PCの利用がWinnyウイルスによる情報漏えいを招いているのは明らかだ。

防衛庁は漏えい発覚後に、私用PCでの重要情報の取り扱いを禁止し、Winnyなどのファイル共有ソフトウェアを私用PCから削除するよう指示した。さらに2006年３月８日には私用PCの業務利用を一切禁止し、業務で使用するPCを公費で支給する方針を打ち出した。陸上自衛隊、海上自衛隊、航空自衛隊には約25万人の職員がいるが、PCの支給は７万台に達する見込みだ。競売事件の裁判資料などが流出した東京地裁も、データを自宅に持ち帰り、漏えいした。最高裁は漏えい発覚後に、業務データを私用PCに保存しないことや、保存してあるデータの削除を指示した。また、あるベンダは業務データの持ち出し禁止を基本に、もし持ち出す場合は利用するPCを登録した上で、業務用PCと同等のセキュリティレベルにすることを規定している。

４．個人情報漏えいの対策

4.1　基本的な対策

⑴　物理的なセキュリティ対策

- 個人情報を扱う部屋の出入り口に入退室管理システムの導入や監視カメラを設置する。
- 個人情報を扱う部屋へのカメラ付き携帯電話や私物のカバンなどの持ち込みを禁止する。
- 個人情報を扱う部屋への個人所有のノートPCやストレージメディア（USBメモリ、SDメモリーカードなど）の持ち込み、使用を禁止する。
- 個人情報が保存してあるサーバーはサーバー・ルームに隔離し、第三者の出入りを制限する。

⑵　アクセス許可者の持ち出し対策

- 正社員の場合は、データ持ち出しに関する規程（順守しなかった場合の罰則も含む）作成と周知をしておく。
- 派遣社員の場合については、派遣契約書において情報漏えいをおこした場合の金銭的損害補償（無制限）条項を入れておく。正社員と同様に個人情報保護について教育を施す。

(3) アクセス制御および不正アクセス調査

- 業務情報へのアクセス権限を明確にし、担当外業務の資料など、業務上不必要な情報にアクセスさせない。データベース・サーバーへのアクセス権を適切に設定して個人情報にアクセスできるユーザーを限定する。離職、あるいは仕事の担当が変わったときは、「速やかにアカウント」を削除することを徹底する。これを行っていれば、2004年におきた「ヤフー BB」の451万以上の個人情報漏えいは、未然に防ぐことができただろう。
- 個人情報を管理しているデータベース・サーバーへのアクセスログを取り、定期的なログ解析・監視体制の構築、および、緊急のログ解析ツールの整備を行っておく。
- ファイアウォールログの調査
- ネットワーク、Web アプリケーションの診断

(4) パソコンや USB 等記憶媒体の盗難、置き忘れ対策

やむを得ず社外に持ち出す際にはパスワードの設定や暗号化や秘密分散[13]を行い、第三者に渡っても参照できなくする。ノート・パソコンに顧客の個人情報などの機密データを保存して持ち歩くとなると、不正利用や情報漏えいなどへの十分な対策が不可欠である。ID とパスワードによるユーザー認証で不正利用を防ぐのが基本だが、端末自体を盗まれたり紛失した場合には、ハードディスクを取り外して別のパソコンにつないでデータを読み取られる恐れもある。データを暗号化すればこのリスクは回避できるが、絶対にパスワードや暗号鍵を解析されないという保証はない。秘密分散を実現するツールは、市販されている。例えば、ノート・パソコンと USB メモリーに分散するソリューション「モバイル割賦」などが市販されている。現在、USB は、データの暗号化機能、ファイルフォルダーのパスワード付機能、モバイル割賦機能等が合理的な価格にて提供されている。

4.2 Winny からの情報漏えい対策

報道によると、漏えいした情報の種類こそ違うが、ほとんどの事件に共通している点は、

[13] 秘密分散とは、機密データをビット単位で複数のパーツに分散させ、パーツがそろったときだけ元のデータに復元できるようにする仕組みである。

職員がファイル共有ソフト Winny を導入（インストール）した私有パソコンに、官公庁や企業等で取り扱う個人情報や機密情報等をコピーし、使用していたところ、ウイルス（W32/Antinny）に感染し、情報漏えいしたという点である。ウイルス（W32/Antinny）に感染すると、パソコン内の送受信メールや Word や Excel 等のデータファイルが、パソコン内の公開フォルダにコピーされてしまう。公開フォルダにコピーされたファイルは、世界中の Winny 利用者が入手できる状態になったということだ。Winny からの情報漏えいを防ぐには、次のような対策が考えられ、それらを組み合わせて実施することが有効と考えられている[14]。（この中で、必要最小限のものを選択して記述する）

⑴　漏えいして困る情報を取り扱うパソコンには、Winny を導入しない。
⑵　職場のパソコンに許可無くソフトウェアを導入しない、または、できないようにする。
⑶　職場のパソコンを外部に持ち出さない。
⑷　職場のネットワークに、私有パソコンを接続しない、または、できないようにする。
⑸　漏えいして困る情報を許可無くメールで送らない、または、送れないようにする。
⑹　ウイルス対策ソフトを導入し、最新のウイルス定義ファイルで常に監視する。
⑺　不審なファイルは開かない。

4.3　Google マップによる情報漏えい対策

グーグルの地図情報サービス「Google　マップ」を使いオリジナルの地図を作成する「マイマップ」機能で、個人情報が閲覧される騒動が2008年11月以降次々に表面化した。企業や学校関係者が登録した個人情報が第三者から閲覧可能になっていた。これは、「マイマップ」の設定を「公開」（デフォルト）にしたまま、ユーザーが地図上にデータを登録していたことが原因だった[15]。これに対する対策は、公開／非公開をしっかり把握した上で設定をおこないサービスを使うことである。もっと堅実な対策は、外部のネットサービスでは、特に、無料のネットサービスでは、個人情報を取り扱わないことである。

4.4　ソーシャルメディアにおける情報漏えい対策

Facebook では、サードパーティの提供する様々なアプリケーションを利用することができる。多くに人気のあるアプリケーションが本人を特定できる情報（Facebook ID）を、広告会社等の外部企業に送信していた。Facebook ID を使うと、利用者の名前を調べるこ

[14] http://www.ipa.go.jp/security/topics/20060310_winny.html［last visit 2012.4.10］
[15] 日経コンピュータ　2009.2.1　pp. 54-55

とが可能になり、利用者がプライバシー設定を「誰にでも公開」している場合は、年齢、性別、住居等の登録情報を調べることができる。プライバシー設定は基本が「公開」であるために、企業が、ソーシャルメディアの組み合わせをおこない、Web サイトとか店舗への集客を行う場合、プライバシー設定に注意を要する[16]。

4.5　マルウェア対策

インシデント種別ごとの報告件数の推移[17]をみると、2009年はマルウェアに起因する件数は9,944中5,311件（53%）、2010年は10,467件中3,367件（32%）であり原因の中で一番多い。マルウェアの生成キットが闇市場で取引されるようになり、構造的には類似しているがコードとしては異なるマルウェアが多数生み出されることになった。

［日経パソコン2010.5.24］によると、ドイツのウイルス検査機関「AV-TEST.org」によれば2008年中には800万近い新種のウイルスが確認されたという。ウイルスはお金儲けのツールになり、ビジネスになっている。ウイルスを使ってパソコンに保存されている個人情報などを盗み、犯罪組織などに販売する。巧妙になるウイルスには古い常識は通用しない。感染経路、感染手法、感染被害の方法と質が変化している。

	以前		現在	例
感染経路	メールに添付されて送られてくる	⇒	メール以外の感染経路が主流に	Web経由やUSBメモリー経由などが脅威に
感染手法	ウイルスファイルを実行すると感染	⇒	実行しなくても感染する恐れあり	ソフトの脆弱性や仕様を悪用
感染被害	感染するとPCを利用できなくなる	⇒	被害は多種多用に	重要情報の盗難やPCの乗っ取りなど

図表４－１　ウイルスの変容

出所：日経パソコン2010.5.24　pp.36（図６）

【対策】複数の対策を組み合わせて守る必要がある。

［日経パソコン2010.5.24 pp.46-49］ウイルス対策７ケ条を以下に記述する。

①信頼できないサイトにはアクセスしない。

②信用できないファイルをダブルクリックしない。

③セキュリティ対策ソフトを使用する。

④ソフトウェアの脆弱性を解消する。

[16] IPA　情報セキュリティ白書2011　pp. 26

[17]「情報化白書2012　激動の時代の情報化」JIPDEC　pp. 105-106

⑤ファイヤーオールやルーターを利用する。

⑥ソフトウェアの設定を変更する。

⑦定期的にバックアップする。

上記①②は、感染の危険性を低減させる。③は既知のウイルスを検出・駆除する。④⑤は脆弱性悪用ウイルスが勝手に動き出さないようにする。⑥使用を悪用されないようにする。⑦感染した場合に復旧しやすい。

【ソフトウェアの脆弱性を解消について】

①ユーザーの負担にならないように、自動的に修正する機能を持つソフトについては、その機能を利用する。例えば、「Windows Update」や「Microsoft Update」の自動更新を有効にしておく。「Windows Update」では、ソフトの修正パッチしか通用しない。「Microsoft Update」に切り替えて office にも対応するように設定しておく。

②自動更新機能がないソフトについては、ユーザーが自分でチェックし、古い場合は、修正パッチや修正版を適用する必要がある。IPA では、そのためのツール「MyJVN バージョンチェッカ」を無料で提供している。

5．おわりに

不正アクセスについては、被害規模が大きくなっている。前述した、ソニーが運営するプレイステーションネットワーク（PSN）における過去最悪１億人以上の個人情報流出事件は。ハッカーによる不正アクセス攻撃を受けたものであり、想定損害賠償総額も大規模になるものと思われる。

他の原因は、盗難、管理ミス、紛失・置き忘れが多い。対策としては、総合的な管理が必要である。本稿では、基本的な対策（アクセス管理、記憶媒体の暗号化、サーバーログ管理等)、ファイル共有ソフ対策、「Google マップ」対策、ソーシャルメディア対策について述べた。

IPA 公開資料「2011年版　10大脅威」[18]では、「狙われ出したスマートホン」が第４位にランキングされている。ソフトウェアの脆弱性を狙うケースと正規のアプリケーションを装ったウイルスをインストールさせる方法がある。利用者が増大していることから、個人情報漏えいの被害が大きくなる。

個人情報と聞くと「実名」「住所」「電話番号」といったワードを連想しがちだが、実は

[18] IPA　2011年版　10大脅威「進化する攻撃…その対策で十分ですか？」 2011年3月　http://www.ipa.go.jp/security/vuln/10threats2011.html

業者がもっとも欲しがっているのは、スマホなどが記録する「位置情報」だという。業者によっては、電話番号なんかよりも乗車履歴やGPSによる位置情報価値がある。例えば、不動産情報や求人情報、飲食店情報など、“場所”が重要になる広告を、特定の個人に向けてピンポイントで出せるわけだ。

今後の課題：

⑴　ソーシャルメディアの組み合わせに関する、情報漏えいに対する検討

⑵　スマートホンの情報漏えいに対する検討

⑶　クラウド・コンピューティングのセキュリティ[19]は、データ保護と暗号については、計算量の問題があり実用化には至っていない。暗号鍵管理、事業者の管理責任範囲など解決すべき問題は多い。このため、今後の検討である。

参考文献

■書籍

- IPA　情報セキュリティ白書2011
- 日経パソコン　2010.5.24
- 日経コンピュータ　2009.2.1
- NPO　日本ネットワークセキュリティ協会　2010年情報セキュリティインシデントに関する調査報告書

■ Webサイト

- IPA　2011年版　10大脅威「進化する攻撃…その対策で十分ですか？」2011年３月　http://www.ipa.go.jp/security/vuln/10threats2011.html［2012.4.10］
- http://www.ipa.go.jp/security/topics/20060310_winny.html［2012.4.10］
- ITmedeia ニュース　http://www.itmedia.co.jp/news/articles/0811/26/news064.html［2012.4.10］
- 「Yomiuri Online」http://www.yomiuri.co.jp/net/security/goshinjyutsu/20110502-OYT8T00649.htm［2012.4.10］
- IT用語辞典　e-Words http://e-words.jp/［2012.4.10］
- http://raicho.2ch.net/test/read.cgi/newsplus/1304579409/［2012.4.10］
- http://www.sc.mufg.jp/［last visit　2012.4.9］
- http://ja.wikipedia.org/wiki/%E5%80%8 B%E4 %BA%BA%E6 %83%85%E5 %A0 %B 1 %E6 %BC% 8F%E6%B 4%A 9［2012.4.10］
- http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/030307houan.html［2012.4.11］

[19]「情報化白書2012　激動の時代の情報化」JIPDEC pp. 93-103