ＢＳＫ第２８－５号

セキュリティより始めよ

START WITH SECURITY　A GUIDE FOR BUSINESS
Federal Trade Commission

平成２８年９月

公益財団法人　防衛基盤整備協会

はしがき

本小冊子は、２０１５年６月に米国の連邦取引委員会（Federal Trade Commission：以下、FTC）が、企業に対して、企業の保有する機微な情報を保護するためにどのようなセキュリティ対策を実施すべきかについて公表したビジネスガイドで、FTCがこれまでに公表した５０件以上に上る法執行事案から得られた教訓を１０項目にまとめたものを翻訳したものです。

高まるセキュリティ脅威、大企業も中小企業もサイバーセキュリティの確保を経営問題としてとらえ、対策を講じる必要性が生じています。セキュリティ事故を起こした企業は顧客や取引先の信頼を失うだけでなく、膨大な損害を被る危険性があります。

本ビジネスガイドでは、企業のセキュリティ対策の意識向上のために１０項目にまとめた基礎的、基本的なセキュリティ対策についてその概要と関連する法執行事例について述べており、企業がセキュリティリスクを軽減、回避するのに役立つ資料であると思われます。

平成２８年９月

公益財団法人　防衛基盤整備協会

理事長　宇田川新一

セキュリティより始めよ

1. 先ずセキュリティより始めよ　・・・・・・・・・・・・・・・・・・・・・・・２

2. データへのアクセスは賢明にコントロールせよ　・・・・・・・・・・・・３

3. 安全なパスワードと認証手続きを要求せよ　・・・・・・・・・・・・・・４

4. 機微な個人情報は安全に保管せよ、そして、伝送の際にも保護せよ　・・・６

5. ネットワークを細分化せよ。侵入しようとする動きをモニターせよ　・・・７

6. ネットワークへの遠隔アクセスを防護せよ　・・・・・・・・・・・・・・８

7. 新製品開発にあたっては十分なセキュリティ対策を適用させよ　・・・・９

8. サービスプロバイダが合理的なセキュリティ対策を実行しているか確認せよ
・・・１１

9. セキュリティを最新にして、将来の脆弱性に備えることができるような
手続きを導入せよ　・・・・・・・・・・・・・・・・・・・・・・・・・１２

10. 書類、メディア、デバイスも防護せよ　・・・・・・・・・・・・・・・１３

ネットワーク管理やアプリ開発、さらには紙ファイル整理にいたる様々な場面において、健全なセキュリティが確保できているということは、決して偶然の産物といったものではありません。事の初めからセキュリティを考慮する会社は、選択肢を比較考量し、業務の特性と情報の機微の程度に応じて、合理的な選択をします。データを襲う脅威は時の流れとともに姿・形を変えることがあります。しかし、健全なセキュリティの基本は不変です。連邦取引委員会（Federal Trade Commission：以下、FTC）が、「個人情報を保護する：ビジネスのためのガイド（*Protecting Personal Information: A Guide for Business*）」において強調したように、どのような個人情報がファイルやコンピュータにあるかどうかを知っておくべきであり、業務に必要な情報だけを保管すべきです。保管する情報は、保護しなければなりません。もう必要のない情報は、適切に破棄すべきです。そして、勿論、セキュリティ事故対処計画をあらかじめ作成しておくべきです。

FTCには、「個人情報を保護する」の他、上記の原則を個々のビジネスに適用するやり方を熟考する上で手助けとなる情報資源があります。従業員訓練支援のためのオンライン教材、データ保護上の個々の課題に対応する諸刊行物、さらにはニュースリリース、ブログ、ガイダンスといったものですが、これらは、思いがけない落とし穴を探知し回避することができるよう手助けすることを目的としています。

もう一つ、機微なデータを保全することについての情報資源があります。それは、FTCがこれまでに公表した50件以上にのぼる法執行事案から得られる教訓です。これらは、当事者の同意により紛争を終了させる和解事案であって ― 事実認定は裁判所で確定されたものではありません ― 個々の行政決定は、当然のことながら、当該会社に対してだけ適用されるに過ぎません。しかしながら、各社が犯したとされ、法執行事案にまで発展したセキュリティ問題は、他社にとっては自らの業務を改善する手掛かりとなるものなのです。そして、これらの逸脱は、たいていの場合、セキュリティの基礎的、基本的な手違いを伴っています。以下に掲げる教訓十則は、こうした事案の本質を抽出したものですが、さらに、将来、襲ってくるかもしれない脆弱性と、その実用的なリスク減少策にも触れています。

１．先ずセキュリティより始めよ

入社志願書に記載されている個人情報から始まって、ネットワークファイルに収録されている顧客のクレジット番号に至るまで、機微な情報は、多くの会社の隅から隅にまで充満しています。企業の管理職からは、よく、秘密情報をどのようにして管理したら良いのかという質問を受けますが、専門家たちが一致している大事な第一歩があります。それは、セキュリティから始めよ、ということです。人事、営業、会計、情報テクノロジー等々、会社の全部門における意思決定において、セキュリティを計算に入れよということです。「ただ何となく」情報を集めて、取って置くなどということは、今やまともなビジネス戦略たりえません。賢明な会社ならば、結果を予想してデータに関する意思決定を考え抜きます。いかなる種類の情報を収集するのか、保存期間はいつまでとするのか、情報にアクセスできるのは誰にするのかといったことを意識的に選択することにより、将来におけるデータ漏洩のリスクを減少させることができるのです。無論、このような意思決定は、事業の性格により違いが出てくるものです。データ収集・保存・利用に際して、無駄がなく、効果的な方策を採用することにより、セキュリティを当初から組み込んでおくことの効用については、以下に述べるFTCの各事案からの教訓例が証明するでしょう。

（１）必要のない個人情報は集めないこと

当初の意思決定に影響を与えるべき一つの基本原則があります。それは、持ってないものは盗まれっこないという原則です。会社が人々から機微な情報を求めるのはどういう時かといえば、人々にオンライン上で登録してもらったり新規アカウントを設定してもらったりする時でしょう。ところで、このような手続きを見つめ直して、人々に入力を求めているものの全てが本当に必須なものなのかどうか確認したのは、直近ではいつだったのでしょうか。言えますか。多くのFTC事案から得られる教訓がこれです。例えば、RockYou社に対するFTCの苦情申し立てによれば、同社はサイト登録プロセスの中で大量の情報を収集していたところ、Eメールのアドレスのほか、Eメールのパスワードをも ― ビジネス上必要ではないにも関わらず ― 収集した上、これを暗号がかかっていないテキストとして保管していたのです。RockYou社は人々のEメール・アカウントに対するリスクを不必要に作り出した、というのがFTCの主張です。そもそも、単に、そのような機微な情報を集めなければ、このようなリスクは回避できたはずなのです。

（２）情報の保管は、ビジネス上の正当な理由がある場合に限ること

商取引きにおいては、その一環として、個人情報を収集する必要が生じるということは時にあることです。しかし、その取引が完了した後ともなれば、個人情報を保管し続けることは賢明ではなくなっているかも知れないのです。FTCが取り扱ったBJ’s Whokesale Club社事案についてみると、同社は、顧客の有するク

レジットカードやデビットカードの情報を収集して、個々の店舗での取引を処理していました。FTCの苦情申し立ては、会社側が、その個人情報データを販売完了後最大３０日間も保管していたというものでした。これ自体、銀行規制に違反することですが、そればかりでなく、ビジネス上の正当な必要性なしに情報を保管することにより、BJ’s Whokesale Club社は、過度のリスクを作り出してしまったと、FTCは主張しました。同社のセキュリティ慣行には他にも弱点があったのですが、ハッカーたちがこの弱点をついて顧客データを盗み出し、クレジットカードやデビットカードを偽造するのに悪用したのです。顧客の金融情報は、正当な必要性がなくなれば、直ちに安全に破棄する、このことさえ実行していれば、リスクを限定することが出来たはずなのです。

（３）個人情報の不必要な使用は避けること

ジャグリングをするとしても、明朝時代の磁器の花瓶を空中高く投げる人はいないでしょう。ビジネスにおいてもまた、不必要なリスクを惹起するような個人情報の使い方をすべきではありません。金融サービス業のAccretive社事案においてFTCは、同社が、実在する人々の個人情報を従業員訓練プログラムで使用し、かつ、プログラム終了後においても、これを従業員のコンピューターから削除しようとしなかったと主張しました。同じく、Foru International社事案において、FTCは、同社が、ソフトウェア開発依頼先の業者に対し、顧客の機微データにアクセスさせたと非難しました。教育訓練なりソフトウェア開発なりの目的のためには仮想の情報を使用すればよく、そうすれば、どちらの案件においても余計なリスクを避けることが出来たはずだったのです。

２．データへのアクセスは賢明にコントロールせよ。

ビジネス上、機微な情報を保管し続ける正当な理由があると判断した以上、これを保全する適切な手段を講じましょう。外部から詮索する目線を避けようとするのはもっともなことでしょう。しかし、従業員についてはどうでしょうか。貴社に勤める誰も彼もが、社のネットワークやその中の情報に対し無制限にアクセスすることを必要とするということはないのです。制御の仕組みを付加することによって、従業員がアクセスできるのは「知る必要（need to know)」がある時のみに限定できるようにしましょう。ネットワークについて言えば、個人情報が保管されている場所へのアクセスを制限したり、特定のデータベースを使用する個人を限定したりするために、別個のユーザーアカウントを設けるなどの手段を検討してください。紙のファイルや外部ドライブ、ディスクなどについて言えば、鍵のかかるファイルキャビネットに保管するといった実に簡単なやり方もあります。保有しておられる機微な情報へのアクセスをコントロールする方法を検討するにあたっては、FTCが取り扱った事案から得られる次のような教訓に配慮されるとよいでしょう。

（１）機微情報へのアクセスを制限すること

従業員がその職務を行うにあたって個人情報を扱う必要がなければ、個人情報にアクセスする必要はありません。例えば、Goal Financial社事案におけるFTC側の主張では、同社は、紙ファイルやネットワークに保管されていた個人情報への従業員のアクセスをコントロールすることが出来ていませんでした。その結果、従業員のグループが、許可なく、消費者7000人分の機微情報を含む個人情報を紙ファイルやネットワークから第三者に転送したのです。アクセス権限を設定し、業務上の必要性を有する、許可を得た従業員のみが個人情報にアクセスできるようにしておけば、このような手違いを同社が事前に防止できていたはずなのです。

（２）管理者アクセス権限を限定すること

管理者アクセスとは、システムの管理者がシステム全体にわたる変更を行うことができるようにするものですが、このようなアクセス権限は、システム管理の仕事を行う従業員にのみ限定すべきです。例えば、FTCは、Twitter社事案において、同社が、ユーザーパスワードのリセット、非公開のつぶやきの閲覧、ユーザーの代理としてのつぶやき発信といった管理者としてのコントロール権をほとんど全ての従業員に対し付与していたと主張しました。管理者アクセス権限を社内の事実上、全員に 付与したことにより、Twitter社は、従業員の誰か一人が信頼を裏切った場合、深刻な違反を引き起こすというリスクを増大させていたのです。そのようなリスクを減少させるには、どのようにすればよかったのでしょうか？　それは、従業員にシステム管理コントロールにアクセスさせるにあたり、当該従業員の業務上の必要性に合わせて行えばよかったのです。

３．安全なパスワードと認証手続きを要求せよ

個人情報をネットワークに保存する際には、推測されにくいパスワードの設定を含め、強固な認証手続きがあれば、データにアクセスできるのは権限のある個人だけということを確実にする上で役に立ちます。貴社の方針の検討にあたって、FTC事案から得られる助言は以下の通りです。

（１）複雑かつユニークなパスワードを強く要求すること

「121212」とか「qwerty」といった「パスワード」は、パスワードがないのとほとんど等しいと言えます。パスワードに求める強さの基準を検討することが賢明である所以です。Twitter社事案では、同社の従業員が管理者権限用のパスワードとして、辞書にある普通の単語を使用したり、既に他のアカウントで使用されているパスワードを使用したりすることを容認していました。FTCとして、ツイッター社の緩すぎる実務慣行が同社のシステムを脆弱なものとしたと主張するのは、ハッカーたちが、パスワード推測プログラムを走らせたり、Twitter社従業員が会社のシステムで同じパスワードを使っていたら儲け物という考えで、

他のシステムから盗んだパスワードを試してみたり、ということがあり得るからなのです。従業員に対し、複雑なパスワードを選ばせたり、公用私用に同じパスワードを使わないよう教育したりすることにより、より安全なパスワードシステムを導入していれば、Twitter社としては、このようなリスクを限定することができたはずなのです。

（2）パスワードを厳重に管理すること

パスワードは、システム侵入者が簡単に見つけることができないようにしておきましょう。Guidance Software社事案におけるFTCの主張は、同社がネットワーク・ユーザー資格情報を平文の理解し易いテキスト文書として保存しておいたため、一人のハッカーがネットワーク上でクレジットカード情報にアクセスすることを許したというものでした。同じく、Reed Elsevier社事案におけるFTCの主張によれば、同社は、顧客がユーザー資格情報を脆弱なフォーマットでクッキーとして自分のコンピュータ内に保存することを許しました。Twitter社事案に戻ると、同社は、従業員が管理者パスワードを平文のテキスト文書として個人の e-メイルアカウント内に保存することを禁止する方針を確立していなかったと、FTCは主張しました。いずれの事案においても、当該各社が、ユーザー資格情報の安全保管のための方針と手続きを定めてさえおけば、リスクを減少させることができたはずでした。その他、パスワード侵害から保護するのに役立つ、例えば二要素認証といった他の保全策も検討してみてはいかがでしょうか。

（3）ブルートフォース攻撃に備えること

無限の数の猿たちが無限の数のタイプライターを叩いていれば、大傑作がいつかは出来上がるだろう、ということわざを思い出していただきたい。ハッカーたちが使う自動プログラムは、同じように機能します。これらの総当り攻撃は、文字の無数の組み合わせをタイプしていくうちに、誰かのパスワードを突き止めることができるという原理で機能します。Lookout Services 、Twitter、Reed、Elsevier各社に関する事案において、FTCは、ログインの試みが一定回数、失敗すれば、ユーザー資格情報を一時停止ないし無効にするということが行われていなかったとしています。ログインの試みの回数を適切に制限しなかったことにより、各社は、自社のネットワークにリスクをもたらしたのです。何度もログインの試みがなされるアカウントは、一時停止し又は無効にするという方針を実施していれば、このようなリスクを除去するのに役立ったはずです。

（4）認証手続きのバイパスに備えること

表玄関に鍵をかけても、裏口が空いていれば、まともな備えにはなりません。FTCは、Lookout Services社事案においては、同社がそのウェブ・アプリケーション制作にあたり、「推測可能なリソースの位置」と呼ばれるものやその他のよく知られたセキュリティ上の欠陥について、その有無を十分に事前テストするこ

とを怠ったと主張しました。その結果、一人のハッカーが容易にパターンを推測し、URLを不正操作することで、ウェブアップの認証スクリーンをバイパスし、同社のデータベースに不正アクセスしたのです。同社は、よくある脆弱性の有無をテストしておけば、その認証メカニズムの安全性を向上させることができたはずでした。

４．機微な個人情報は安全に保管せよ。そして、伝送の際にも保護せよ

多くの会社にとって、機微な情報を保管することはビジネス上、必須です。そこで、社のネットワークを保全するために適切な手段を講じても、更に、データを他の場所に伝送しなければならないことが生じます。保管と伝送の際において秘密事項を保全するためには、強力な暗号を使用しましょう。どのような暗号方式を採用するかは、収集する情報の種類、収集方法、処理方法によって変わりますが、可能性としては、TLS/SSL暗号、保存データ暗号、反復的暗号学的ハッシュ関数などがあります。しかし、どのような方法を選定するとしても、その強力さの程度は、選定作業をする人々の質に左右されます。このような作業を行うべく指名された人々に対しては、機微情報を貴社がどのように使用するのかを理解させるとともに、個々の場面で何が適切かを判断できるノウハウを有していることを確認すべきでしょう。以上を念頭に置きつつ、以下、FTCの関わった事案から得られる若干の教訓を紹介します。それは、保管と伝送の段階で機微な情報を保全する際に考慮すべき教訓なのです。

（１）機微な情報の保全は、そのライフサイクル全体について行うこと

データというものは一箇所に止まってはいません。だからこそ、そして情報を伝送することが貴社のビジネス上必要である以上、全ての段階で保全を考慮する必要があります。Superior Morgage Corporation事案におけるFTCの主張によれば、顧客のウェブ・ブラウザーと同社のウェブサイト・サーバーとの間の通信はSSL暗号によって保護されていたところ、情報がサーバーに到着した後は、同社のサービスプロバイダが暗号を解き、平文に直して同社の本社や支店に転送していました。このようなリスクは、最初の伝送段階についてだけでなく、そのライフサイクル全体にわたってデータを保全すれば、防ぐことができたはずです。

（２）業界で実証済みかつ受容されている方式を使用すること

従うべき技術標準を検討するにあたっては、既に効果的な標準が専門家たちによって開発済みで、貴社の事業にそのまま応用できるかも知れないということを考慮しておく必要があります。機転のきく会社であれば、ゼロから出発する無駄を省き、みんなの知恵を活用しようとするものでしょう。この原則を実例で明らかにするのは、ValueClick社事案です。FTCの調査によれば、同社は、電子商取引サイトを通じて収集した顧客の機微情報をデータベースとして保管していま

したが、そこで使用していた暗号は、非標準の自社開発方式のものでした。FTCの指摘した問題点は、その方式が、広く受け入れられ詳細にテストされている方式とは異なり、単純なアルファベット置換方式を採用していて重大な脆弱性にさらされているということでした。同社としては、業界でテストされ受容されてきた実証済みのデータ処理方法を使用しておきさえすれば、このような弱点を抱えることにはならなったはずなのです。

（3）適切な設定を確保すること

どれほど強力な暗号であっても、設定を適切に行わなければ、ユーザーを保護してはくれません。これが、Fondango社とCredit Karma社に対する FTC の法執行から事業者が得ることのできる一つのメッセージです。二社とも、自社のアプリにSSL暗号を使用していたのですが、FTCの調査によれば、SSL証明書有効性確認として知られる重大なプロセスをオフにして、しかも代替保全策を講じることがなかったのです。このため、両社のアプリは中間者攻撃に対して脆弱になり、ハッカーが行おうとすれば、アプリが伝送する機微情報の暗号を解ける状況を惹起したのです。このようなリスクは、SSL実装にあたり設定を適切にしておけば阻止することができたはずです。

5．ネットワークを細分化せよ。侵入しようとする動きをモニターせよ

ネットワーク設計にあたっては、ファイアウォールなどの仕組みを使ってネットワークをセグメントに分割することにより、ネットワーク上のコンピュータ同士のアクセスやコンピュータとインターネットとのアクセスを制限することを考えましょう。有益な防護手段をもう一つ。それは、侵入検知システムを使って貴社のネットワークへの不正アクセスの活動の有無をモニターすることです。ネットワーク設計上、考慮すべき教訓は以下の通りですが、いずれもFTC事案から得られています。

（1）ネットワークをセグメントに分割すること

ネットワークに繋がっているからといって、全てのコンピュータが他の全てのコンピュータと通信する必要があるわけではありません。特に機微な情報を保護するためには、ネットワーク上の別個、安全な場所に保管するという方法があります。これが、DSW社事案から得られる教訓です。FTCの主張によれば、同社は、その一店舗のネットワーク上のコンピュータが、他の店舗のネットワークや会社全体のネットワーク上のコンピュータと連接してしまうことを充分には制限していませんでした。その結果、ハッカーたちが、一店舗の一台のコンピュータを使って、他の店舗や会社全体のネットワーク上の個人情報に連接し、アクセスしようと思えば、できる状態になっていました。そのようなリスクを減少させるには、同社がネットワークをきちんとセグメントに分割しておけばよかったのです。

（2）ネットワーク上の動きをモニターすること

効果的な侵入検知システムは、ネットワーク上の不正な動きを検知した際には、（映画の題名ではありませんが）「ドアをノックするのは誰？」という問いを発するものなのです。Dave & Busters社事案におけるFTCの主張によれば、同社は侵入検知システムを利用せず、また、ネットワークのシステムログをモニターして疑わしい動きがないかどうかを調べることもしていませんでした。同じようなことが、Cardsystem Solutions社でも起こっていた、とFTCは言明しています。同社は、そのネットワークに対する権限なきアクセスを探知する充分な措置を講じてはいませんでした。ハッカーたちはこの弱点を突き、同社のネットワーク上にプログラムをインストールして、保存してある機微な情報を収集し、これを４日毎に外部に送信させていたのでした。両社とも、各々のネットワーク上の動きをモニターしていれば、データ漏洩の発生のリスクやその規模を減少させることができたはずなのです。

６．ネットワークへの遠隔アクセスを防護せよ

ビジネスというものは、会社の事務所の中でだけ行われるものではありません。社外で働く従業員たちは生産性を高める可能性をもたらしますが、同時に、セキュリティ上、新たな課題をもたらし得るものでもあります。従業員、顧客、サービス提供事業者に対し、貴社がネットワークへの遠隔アクセスを許可するとして、そのアクセスポイントの安全性を確保する対策は採っておられますか？ FTCの諸事案は、貴社の遠隔アクセス方針を創り出す上で考慮すべきいくつかの要素があることを示唆しています。

（1）エンドポイントのセキュリティを確保すること

ことわざで「鎖の強さは最も弱い輪によって決まる」と言われているように、ネットワークのセキュリティの強度も、そこに遠隔アクセスするコンピューターのうち最もセキュリティの弱いものによって決まります。これこそ、自社のネットワークに遠隔アクセスするコンピューターがエンドポイントとしての充分なセキュリティを有しているかどうか確認を怠った事業者たちに関するFTC諸事案からもたらされるメッセージなのです。例えば、Premier Capital Lending社は，消費者に関する報告を受け取るため、自社ネットワークへの遠隔ログイン・アカウントを、報告元に対しアクティブにしたのですが、その際、相手の保全状況の評価を怠っていたとされています。やがて、ハッカーが報告元のシステムに侵入したのですが、その際、ログイン認証情報を盗み出し、これを使って、消費者の個人情報を横取りしたとされています。Settlement One社事案における苦情申し立てによれば、同社は、ファイアウォールや最新版のウィルス対策ソフトといった基礎的なセキュリティ対策すら講じていないような顧客に対して、ポータルサ

イトを経由して消費者レポートにアクセスすることを許可していました。

LifeLock社は、FTCの告発によれば、そのネットワークに遠隔アクセスするために従業員が使用するコンピュータにウィルス対策ソフトをインストールすることを怠っていました。各社とも、自社のネットワークに遠隔アクセスをするコンピュータを防護しておけば、このようなリスクを減少させることができていたでしょう。

（2）アクセスに適切な制限を設けること

貴社のネットワークに時に応じてアクセスする必要がある人々がいるからといって、その全員が内密なフリーパスを持っていなければならないということにはなりません。だからこそ、仕事を遂行するのに必要な範囲にアクセスを限定することが賢明なのです。例えば、Dave & Buster’s社事案では、FTCは、同社がネットワークへの第三者のアクセスを適切に制限することを怠ったと告発しました。侵入者が、第三者である企業のセキュリティの弱さを突いて、Dave & Buster’s社のネットワークに多数回、接続し個人情報を窃取していたのです。Dave & Buster’sは、どうすればリスクを減少させることが出来たのでしょうか。それは、例えば、接続を特定のIPアドレスに限定するとか、一時的な限定的アクセス権のみを付与するとかによって、第三者によるネットワーク・アクセスに制限を課すことができたはずなのです。

7．新製品開発にあたっては十分なセキュリティ対策を適用させよ

ところで、貴社では、最高の新アプリや革新的ソフトウェアを設計中だったとしましょう。開発の初期段階でこそ、製品を顧客がどのように使うだろうかということをとことん考え抜いて下さい。顧客に機微な情報を保存させたり送信させたりするのだとして、そのような情報を安全に処理できるような新製品になっているでしょうか。市場に参画する前に、FTC 事案に見られる、製品の開発、設計、試験、発表にかかわる教訓を熟考して下さい。

（1）技術者に対して安全なコード化の訓練をおこなうこと

貴社では、開発担当者に対してセキュリティを正面に据えるべきことを説明していますか。MTC社、HTC America社、TRENDnet社といった事案において、各社は、従業員に対し安全なコード化実施の訓練を施すことを怠っていたと、FTCは主張しました。その結果は、疑問の多い設計決定であり、その中には、ソフトウェアに脆弱性を持ち込むといったことも含まれていました。例えば、HTC America社事案における苦情申し立てによれば、同社のモバイル機器にプリインストールされたログ・アプリケーションについて、入手が簡単な通信保全の仕組みを導入することを怠りました。その結果、悪意ある第三者のアプリが当該ログ・アプリケーションと通信できるようになり、消費者のテキスト・メッセージや位置データ

その他の機微な情報が危険にさらされたのです。同社としては、技術者たちに対し安全なコード化の実践の訓練を施すことにより、このような脆弱性のリスクを減少させることができたはずなのです。

（2）プラットフォームのセキュリティに関するガイドラインを遵守すること

「車輪の再発明」というのは、既に確立されている技術があるにもかかわらず同じものを再び作ることを言いますが、セキュリティに関する限り、「車輪の再発明」は不必要なのかも知れません。時には、専門家の意見に従うことが最も賢明です。HTC America社, Fandango社, 及びCredit Karma社の事案において、FTCは、プラットフォーム側のセキュリティに関する明確なガイドラインを遵守することを三社が怠ったと主張しました。例えば、Fandango社とCredit Karma社は、その開発したスマホアプリにおいて、SSL証明書有効性確認と呼ばれる最も大切なプロセスを無効化した結果、消費者がアプリを通じて送るメッセージについて、第三者攻撃を使った傍受の危険にさらすことになったのです。

iOSやアンドロイドの開発者ガイドラインは、SSL証明書有効性確認を無効化してはならないと明確に警告していますが、各社がこのガイドラインを守っていれば、このような脆弱性を予防できたはずです。

（3）売り物とするプライバシーやセキュリティの特徴が作動するかどうか確かめること

貴社のソフトウェアがプライバシーやセキュリティを売り物としているならば、それが宣伝通りに機能するかどうかを確かめることです。TRENDnet社の場合、カメラの画像を非公開にするというオプションが実際に画像へのアクセスを制限するのかどうか、テストを怠っていたとFTCは主張しました。その結果、何百もの「非公開」画像が外部で入手できてしまったのです。同様に、Snapchat社は、メッセージが「永遠になくなる」と宣伝していましたが、この主張が正確であることの裏付けを怠っていたというのが、FTCの言明するところです。すなわち、当該アプリは、サンドボックスの外にビデオファィルを保存しており、他の問題点と相まって、よくあるファイル閲覧ツールを使えば、ビデオファイルを容易に回復することが可能となっていたのです。他社にとっての教訓とは、プライバシーやセキュリティをアプリの特徴とするならば、宣伝通りの製品となっているかどうかきちんと確認すべきだということです。

（4）よくある脆弱性の有無をテストすること

ありとあらゆる脅威をあらかじめ予想することはできませんが、しかし、いくつかの脆弱性はよく知られており、かなり予見可能です。FTC法執行事案においては、事業者がそのアプリに関し、よく知られている脆弱性の有無を適切に確認することを怠っていたケースが十数件ありました。例えば、Guess社事案においては、SQLインジェクション攻撃に対して脆弱か否かの確認を怠りました。その

結果、ハッカーたちが、SQLインジェクション攻撃を使用して、消費者のクレジットカード情報のあるデータベースにアクセスすることができたのです。このようなリスクは、オープン・ウェブ・アプリケーション・セキュリティ・プロジェクト（Open Web Application Security Project ： OWASP）が特定しているような、よく知られている脆弱性の有無をテストしていれば回避できたはずなのです。

※オープン・ウェブ・アプリケーション・セキュリティ・プロジェクト
（Open Web Application Security Project ： OWASP）
ウェブアプリケーションをはじめとするソフトウェアのセキュリティ環境の現状、またセキュアなソフトウェア開発を促進する技術・プロセスに関する情報共有と普及啓発を目的として活動

８．サービスプロバイダが合理的なセキュリティ対策を実行しているか確認せよ

セキュリティのこととなると、貴社にサービスを提供する業者（サービスプロバイダ）に対して、すなわち、例えば消費者から収集した個人情報を処理させたり、アプリを開発させるなどの相手の下請け業者に対して、監視の目を緩めることがあってはなりません。雇う前の候補者に対しては、セキュリティへの期待度を明確に伝えることです。適切なセキュリティ対策を実行できるような業者を選ぶよう、妥当な方策を講じることです。そして、業者が貴社の要求水準を満たしているかどうかモニターすることです。FTCの諸案件は、業者の選定と監督に関し考慮すべき事項について助言しています。

（１）文書化すること

適切なセキュリティ規準を守るべきことを契約の一部とすることを強く主張することです。GMR Transcription社は、機微な音声ファイルの文書化業務を下請けに出していたのですが、サービスプロバイダに対し適切なセキュリティ対策をとるように契約で要求していませんでした。その結果、高度に秘匿すべき健康関連情報を含む大量のファイルがインターネット上で広範に暴露されたのです。先ず第一に、同社は契約条項の一部として、例えば暗号化などの合理的なセキュリティ対策を下請け業社に義務づけることができたはずなのです。

（２）契約遵守を確認すること

セキュリティというものは、「私たちの言うことを信じて下さい」で済むようなものではありません。セキュリティに関する要求をサービスプロバイダー契約事項とすることは大事な第一歩ですが、一連の工程の中に監督という要素を盛り込むことも同じように大事なことです。Upromise社事案は、このことを証明する良い例です。同社は、サービスプロバイダを使って、消費者の閲覧情報を収集し、

個々人に最適な購入呼びかけができるようなブラウザー・ツールバーを開発させたのですが、それは「個人を同定するような情報を除去する」フィルタを使用してから送信するようになっていると請け負っていました。しかしながら、同社は、サービスプロバイダが、消費者情報を保護するためのプライバシー保護やセキュリティに関する自社の方針なり契約条項なりに合致するように、当該情報収集プログラムを実行したかどうか確証することを怠っていました。その結果、くだんのツールバーは、金融機関口座番号やセキュリティ番号を含む機微な個人情報を保護が本来かかっているウェブ・ページから収集し、これを暗号のかかっていないテキストとして送信したのです。Upromise社としては、どうすればリスクを軽減させることができたのでしょうか。それは、開発工程を通じてサービスプロバイダに質問を投げかけ、そのフォローアップを続行していくことだったのです。

９．セキュリティを最新にして、将来の脆弱性に備えることができるような手続きを導入せよ

ソフトウェアとネットワークを安全にすることは、一回こっきりで済むことではなく、継続的なプロセスであって、警戒を怠らないようにする必要があります。貴社ネットワークで第三者製ソフトウェアを使用していたり、貴社のアプリに第三者製ソフトウェアライブラリーを含めている場合には、出る度にアップデートを実行してください。貴社開発のソフトウェアを使用している場合、ソフトの脆弱性に気づいた人はどのようにして貴社に連絡すればよいのでしょうか。貴社はどのようにして直すのでしょうか。FTCの諸事案は、脆弱性の管理について考える上で必要な論点を提供してくれます。

（１）第三者のソフトウェアをアップデートすること、パッチを施すこと

時代遅れのソフトは、セキュリティを徐々に蝕んでいきます。解決策は、定期的にアップデートを行うことと、第三者パッチをあてることです。例えば TJX 社事案では、ウィルス対策ソフトをアップデートしなかったため、ハッカーたちが既知の脆弱性に付け入ったり会社側の防御策を圧倒したりするリスクを増加させたと、FTCは主張しています。ネットワークやソフトの複雑性によっては、パッチを当てる際には深刻な方を優先する必要が出てきますが、いずれにせよ、第三者のソフトをアップデートしパッチを当てる合理的なプロセスを導入しておくことは、漏洩のリスクを減少させる重大なステップなのです。

（２）信頼できるセキュリティ警告に注意を払い、迅速に対処すること

脆弱性の問題が目に入ってきたら、注意深く耳を傾け、迅速に行動しましょう。HTC America社事案において、FTCは、同社がセキュリティの脆弱性に関する報告を受け取り、対処するプロセスを有していなかったと主張しました。HTCの警告

への反応は遅かったとされていますが、そのことは、問題の脆弱性が他のOS版にまで拡大してしまったことを意味していたのです。時には、セキュリティ警告を受けても、会社の忙しさの中で忘れ去られてしまうことがあります。例えば、Fandango社では、セキュリティ・リスクに関する警報は一般的な消費者サービスの一環として扱っていました。FTCの苦情申し立てによれば、一人の研究者が脆弱性のことで会社に連絡を取ったのですが、システムの手違いで、この連絡をパスワード・リセットの依頼として間違って分類して自動応答をした上、解決済みとしたため、この連絡をあとから再度チェックすべしという警報を残すことにはならなかったというのです。その結果、Fandango社としては、FTCの職員が連絡して初めて脆弱性を知ることになったのです。他者にとっての教訓は何でしょうか。それは、セキュリティ上の脆弱性に関するレポートを受け取り、対処する効果的なプロセスを設置せよということです。明確に公表され（例えば、security@yourcompany.com といった専用のアドレスをもった）効果的なルートを設置し、レポートを受け取り、貴社のセキュリティ担当部門に警報を伝えるようにすることを検討してはどうでしょうか。

10. 書類、メディア、デバイスも防護せよ

ネットワークのセキュリティこそ考慮すべき緊要な事項ですが、同じような教訓は、紙の書類とかハードドライブ、ラップトップコンピュータ、フラッシュメモリー、ディスクといった物理的メディアとかにも応用されるのです。FTCの事案は、貴社における物理的セキュリティを考慮する上で参考となる事項を提供します。

（1）機微な情報は安全に管理すること

重要な紙の書類を残す必要がある場合には、これを安全に管理する手段を講じて下さい。不動産仲介業者Gregory Navone事案において、FTCは、被告が過去の顧客の機微な情報を箱詰めにして車庫に保存していたと主張しました。Lifelock社に対する苦情申し立て事案では、同社が、消費者の個人情報を記載するファックス受信紙を鍵のかかっていない、誰でも入れる場所に放置していたとされています。いずれの場合も、事業者が書類の保存に関する方針を定め、実行に移していれば、顧客に対するリスクを軽減することが出来たはずなのです。

（2）個人情報を処理するデバイスを保護すること

ネットワーク上に保存されている情報を保全しても、もし当該情報が、これを収集するデバイスを通じて事前に盗まれていたとしたら、顧客を保護したことにはなりません。2007年のDollar Tree社に対する調査事案において、同社の個人識別番号入力デバイスが不正操作や窃盗に脆弱だったとFTCのスタッフは言明しています。その結果、権限のない個人が、「PEDスキミング」として知られる攻撃方法で、磁気ストライブデータや個人識別番号などの支払いカード情報を盗み取

ることができるという状態に置かれていました。FTCスタッフは、この種の攻撃が当時は真新しかったこともあり、他の諸事情もあって、調査を終了させました。しかしながら、POSシステムを標的とする攻撃は今日ではありふれていて、よく知られるようになっています。事業者としては、このようなデバイスから情報漏洩が起こらないよう、合理的な対応を行うべきです。

（３）データが移動途上の場合の安全基準を定めること

賢明な事業者であれば、機微な情報を事務所外でも保全することの重要性を理解することでしょう。例えば、Accretive社事案では、一人の従業員が、600個のファイルを含み、２万３千人の患者に関する２千万件の情報の入ったラップトップコンピュータを鍵のかかった車の座席に放置していたところ、これが盗まれてしまいました。CBR Systems社事案は、暗号化されていないバックアップテープ、ラップトップコンピュータ１台、外部ハードディスク１台に関わるものであって、いずれも機微な情報を入れていたのですが、従業員の車から盗まれてしまったのです。いずれのケースでも、事業者は、データが移動途上の場合の合理的なセキュリティ対策を実施していれば、消費者の個人情報に対するリスクを減少させることができたはずです。例えば、ファイル、ドライブ、ディスクなどを送付するにあたっては、送付途上の現在位置がわかるような輸送手段を使用することです。従業員が機微な情報を抱えながら飛び回る機会を限定することです。しかし、機密の情報を持って出張しなければならないビジネス上の正当な理由がある場合には、従業員は、可能な限り、これを外部の眼の届かない場所に置き、鍵をかけておくべきです。

（４）機微な情報の破棄を安全に行うこと

もはや必要のない紙の書類や装置は、ごみの山のように見えるかもしれませんが、これに消費者や従業員の個人情報が含まれていれば、なりすまし窃盗犯にとっては宝の山なのです。例えば、FTCの苦情申し立てによれば、Rite Aid社やCVS Caremark社は、調剤処方箋のような機微な個人情報を含む紙書類を大型ゴミ収集容器に投げ捨てていました。Goal Finantial社事案においては、一人の従業員が不要になったハードドライブを売却したのですが、それには、およそ３万４千人の顧客の機微な個人情報が平文で入っていたと、FTCは主張しました。ここに掲げた各社としては、シェレッダーにかけ、焼却し、粉砕して書類が読めなくなるようにし、現存の技術を駆使して使われなくなったデバイスを消去することにより、消費者の個人情報へのリスクを回避することが出来たはずなのです。

より情報を求めている人のためにFTCのビジネスセンター（business.ftc.gov）にはデータ・セキュリティのセクションがあり、そこには、関連する事案の最新リストなど無料の情報資源が掲載されています。

FTCは、消費者のために行動し、市場における欺瞞、詐欺、不公正取引を防止します。FTCのビジネスセンターは、事業者や会社が法制度を理解し遵守するためのツールを提供しています。所属しておられる組織や産業の規模のいかんにかかわらず、遵守の責任について知ることは、そして履行することは、スマートで健全なビジネスなのです。ビジネスセンター（business.ftc.gov）をご訪問ください。

連邦小企業オンブズマン（National Small Business Ombudsman）及び10カ所の地域公正局（Regional Fairness Boards）は、連邦政府による法令遵守行為及び法執行行為に関する小企業からのコメントを募集しています。オンブズマンは、毎年、これらの行為のあり方を評価し、各行政庁の小企業への対応に評点をつけます。小企業は、オンブズマンにコメントしたために報復を受けることはありません。フリーダイアル1-888-REGFAIR（1-888-734-3247）または sba.gov/ombudsman あてにコメントをお願いします。

平成２８年発刊資料

ＢＳＫ 第２８－４号『企業が国際共同開発に参加する場合の契約制度上の課題等(その３)』
（平成２７年度）
ＢＳＫ 第２８－３号『データ抜き取りの探知及び防止（平成２７年度)』
本報告書の中で意見にわたるものは、委託研究先の見解であることをお断りしておきます。

セキュリティより始めよ（平成２８年度）
平成２８年９月発行 非売品　　禁無断転載・複製 発　行　：　公益財団法人　防衛基盤整備協会 編　集　：　防衛基盤研究センター刊行物等編集委員会 〒160-0003　東京都新宿区本塩町２１番 電　話　：　０３－３３５８－８７５４　　ＦＡＸ　：　０３－３３５８－８７３５ メール　：　koueki@bsk-z.or.jp ホームページ　：　https://ssl.bsk-z.or.jp

平成27年度情報セキュリティ川柳入選作品

主催　公益財団法人 防衛基盤整備協会

最優秀賞

友好が
写真アップで
絶交に

ペンネーム　友情報

佳作

そのサイト
白雪姫も
実は魔女

ペンネーム　三郎

佳作

「同意する」
規約長すぎ
ついボタン

ペンネーム　楓すず

佳作

四季問わず
国境超えて
サギの群れ

ペンネーム　三郎

佳作

『重要』の
疑似餌が踊る
詐欺メール

ペンネーム　ばいなりい

ヤング奨励賞

詐欺かもよ
そのワンタッチ
考えて

ペンネーム　頭川成葉