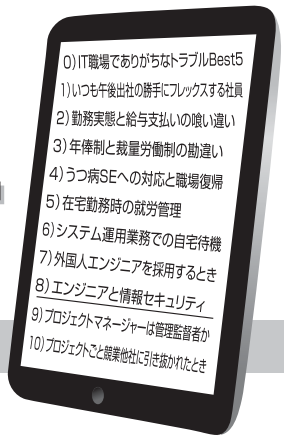
IT職場の問題解決ケーススタディ10

～事件は現場で起きている！～



8 エンジニアと情報セキュリティ

なりさわ社会保険労務士事務所 特定社会保険労務士 **成澤 紀美**

CASE：情報漏洩はヒューマンエラー

- 70ヵ所で３万8,480件の顧客情報を紛失
- 森永ヒ素ミルク事件の裁判関係資料を紛失，被害者455人の個人情報も
- ウェブサイト上に個人情報を誤って掲載
- 顧客情報記載の借入申込関係書類を紛失
- 市営住宅家賃滞納者の名簿を委託職員が紛失
- 元従業員が法人顧客の出荷情報約を不正提供
- 生徒の個人情報入りUSBメモリを紛失，教頭が「発見された」と虚偽報告
- 資格登録者のメールアドレスが流出―建築コンサルタンツ協会
- ……

と，ここ１週間のニュースを拾っただけで，これだけの情報漏洩事故に関する内容が出てきます。公表されていないケースまで想定すると，１日でどれだけの情報漏洩事故が起きているのでしょう。

情報漏洩事故は，すべてヒューマンエラーによるもの。故意に漏洩するもの以外は，ちょっとした情報機器の操作ミスや，単純な確認ミスだったりします。

ヒューマンエラーを「ゼロ」にするのは不可能であり，いくら情報機器を精密なものにしても，これを扱う「人」がミスを起こす以上，情報漏洩事故がなくなることはありません。

上記は普通に情報機器を扱っている方が起こしてしまった事故ですが，エンジニアが関与して起こす情報セキュリティ事故も多くあります。

- サーバに不正アクセス，顧客情報流出の可能性否定できず
- オンラインショップに不正アクセス，カード情報流出の可能性
- 求人サイトでシステム障害，企業担当者や求職者の情報流出
- テスト環境の設定不備でメール誤送信が発生
- ネットショップ14店舗の顧客情報がネット上で閲覧可能に
- ……

と，エンジニアが関与するケースでは，当初から情報取得が目的の悪質なものから，システム上の障害や設定ミスによる事故が目につきます。これらもすべて「人」による行為から起こるものです。

では，これらヒューマンエラーにどう対処していくことで，漏洩事故は防げるのでしょう。

STUDY：企業規模に応じた対応を

大企業では，社内外の様々なインフラやシステムを利用し，情報セキュリティ対策を講じていますが，従業員規模が小さい中小企業では，個人情報保護や情報漏洩対策など企業内でのセキュリティの重要度は高まる一方で，社内に専任のセキュリティ対策担当者や管理者がいないところがまだまだ多く，専門のセキュリティ対策を行っているというケースは多いとはいえないのが実情です。セキュリティ対策を専門としていない他業務と兼業の社員が，セキュリティ管理者として自らの業務の範囲内で努力し，社内の様々なセキュリティ対策を構築しているということもよく見られます。

野村総合研究所の「企業における情報セキュリティ実態調査2012」においても，売上規模にかかわらず８割の企業で人材が不足しているとされています。

東日本大震災以降，企業の情報セキュリティ対策が進んできたというものの，まだまだ人材不足感は否めず，今後もしばらくの間はセキュリティ人材の不足は改善されないと予想されます。

特に海外拠点での情報統制やシ

なりさわきみ：弘前大学人文学部卒業後，大学時代から興味があったコンピュータに関わる仕事を目指し，業務系システム設計に長年，携わる。人事管理システム設計をきっかけに企業人事・労務の道へ。1998年，社労士試験合格。1999年１月，なりさわ社会保険労務士事務所を開業。2003年６月，人事・労務のワンストップサービスを目指し，株式会社スマイング設立に参画。IT関連の顧問先が約８割という業界専門の事務所でもある。 http://www.nari-sr.net
●特定社会保険労務士（東京都社会保険労務士会所属）●AFP（ファイナンシャルプランナー），２級FP技能士　●年金アドバイザー２級（銀行業務検定協会認定）

ステムセキュリティに関する人材の不足感が継続すると思われ，自社でのセキュリティ管理が難しい分野については外部人材の活用がこれまで以上に増えると考えられます。

また同時に,管理コストを抑え，セキュリティ対策の社内推進を図るため，内部人材の育成が進められていくでしょう。

企業規模や事業展開により，かけられるコストに限りがありますので，それぞれに応じた対策を講じていく必要があります。

CHECK：セキュリティスキルを高める

では，エンジニアとして情報セキュリティ対策にどう関与していくべきなのでしょう。

一つは「セキュリティが分かるエンジニア」として，情報セキュリティ対策に関与するというものです。いわゆるセキュリティエンジニアと称されるものです。現時点でこれをやっていればとか，この資格を持っていればという明確なものがあるわけではありませんが，情報セキュリティに関する仕事を専業にしている人が該当します。

経営面でのISMS取得支援から始まり，企業情報の安全を守るためにどのようなシステムにするべきか，データの配置をどうするべきか，認証をどういう方式にするか，といった多岐にわたった知識とスキルが求められます。

またFirewall（ファイアーウォール）の稼動状況を確認したり，セキュリティ問題が発生した場合の対応を行ったりと，テクニカルな作業も発生します。

これら以外にも，実際にシステムに侵入できるかどうかをテストしたり，セキュリティリテラシーを一般社員に教育するための社内教育の講師を務めたりすることも求められるでしょう。セキュリティが分かるエンジニアとしてのフィールドは幅広く，必要なスキルも異なってきます。

- 情報セキュリティに関するマネジメント
- ネットワークインフラ
- Web，電子メール，DNSといったアプリケーションセキュリティ
- Unix，Windows等のOSセキュリティ
- ファイアーウォール
- 侵入検知システム
- ウィルス
- セキュアプログラミング技法
- 認証システム
- 不正アクセスの手法
- 法令，規格　など

労務管理面から見ると，会社がどこまで社員の情報取り扱いに関与するべきなのかを考える必要があります。

例えば，社員が使用しているPC内のメールを監視する権利が会社側にどこまであるでしょうか。社員の不注意により社内情報が外部に流れてしまったり，顧客情報や取引先との営業情報などの企業機密情報が外部に漏れてしまったり，業務には関係ない不適切な内容のやりとりの経緯などがメールを通じて外部に流れてしまうと，企業イメージが損なわれてしまい，関係者が何らかの不利益を被った場合には，会社が訴訟対象になる可能性もあります。

こういった事態にならないよう，モニタリングや監視を行うことも必要になります。ただし，モニタリングや監視を行う際には，社員のプライバシーと職務専念義務との関係が問題になりますので，モニタリングに関するルールを定め，これを周知し理解に努める必要があります。

情報の取り扱いがまずかったために情報漏洩につながってしまった場合，会社側はWebページ上で経緯を説明し，謝罪し，出回った情報を悪用しないように呼びかけるなどの対応が急務であり，より迅速な対応が求められます。

情報の取り扱われ方に大勢の人たちが神経質になっている現状では，情報漏洩事件を起こしたというだけで，かなりの企業イメージダウンになることは避けられません。社員がうっかり失敗をしてしまわないためには，セキュリティチェックに関するしっかりとした社内規程を作成し，これを全社員に通達し，定期的に教育トレーニングを行うなど，決定されたルールに沿ったシステムの運用が必要とされます。