マネジメント講座

情報漏洩を防ぐ ①　ヒューマンエラーの本質

業務でのＩＴ（情報技術）利用が増えるにつれて顕著になってきているリスクが情報漏洩だ。一般に情報漏洩といえば、不正アクセスやウイルス感染など外部からのサイバー攻撃を想像する人が多いと思われる。

しかしＮＰＯ法人・日本ネットワークセキュリティ協会がまとめた２０１７年の「情報セキュリティインシデントに関する調査報告書」によると、誤操作や紛失・置き忘れ、管理ミスなどのインシデント（セキュリティーを脅かす事象）が全体の６割を占める。

人為的ミス（ヒューマンエラー）による情報漏洩が後を絶たない状況がうかがえる。

こうしたヒューマンエラーは、守るべきルールを知らなかった、何らかの理由でルールを守らなかった、ルールを守る気がなかった、などの背景から引き起こされる。

このためヒューマンエラーの発生確率をゼロにすることは難しい。だがヒューマンエラーを減らし、たとえエラーが起こっても情報漏洩を発生させない仕組みをつくることは可能だ。

ヒューマンエラーによる情報漏洩を減らすにはセキュリティーに関するルールをしっかりと整備し、「どのような行動をとるべきか」「行ってはいけない行動は何か」を明確にする必要がある。

さらに「情報漏洩につながるミスやトラブルが起きるかもしれない」という前提で定期的にルールをチェックし、自社の身の丈に合った運用にブラッシュアップしていくことが重要だろう。

ヒューマンエラーはインシデントの原因ではなく結果といわれる。「絶対に情報漏洩しない」と考えるのではなく「するかもしれない」という当事者意識を持たせ続けることが、組織の運営上、重要になってくる。

（ＳＯＭＰＯリスクマネジメント取締役　宮崎義久）

ヒューマンエラーの発生要因と対応のポイント

主な発生要因

- 守るべきルールを知らなかった
- ルールを守るつもりだったが、実践できなかった
- ルールを守る気がなかった

↓

主な対応

- 情報を取り扱うためのルールを整備
- ルールを守りやすい環境を整備
- なぜルールが必要なのかを教える

（注）SOMPOリスクマネジメント作成

2019年6月4日
日経産業新聞

マネジメント講座

メール誤送信に２重の対策

情報漏洩を防ぐ ②

メールは情報伝達を効率化し、今や企業間のコミュニケーションツールとして欠かせない手段となっている。一方で「メールの宛先をうっかり間違えて送ってしまった」「添付ファイルを間違えて送ってしまった」などのミスは、仕事をする上で誰もが体験、もしくはひやっとしたことがあるのではないだろうか。

一般財団法人・日本情報経済社会推進協会の「２０１７年個人情報の取扱いにおける事故報告にみる傾向と注意点」によると、最も多い情報漏洩の原因に「メールの誤送信」が挙げられている。

メールの誤送信は大きく３つに類型化することができる。「メールの宛先を誤って送信した（宛先間違い）」「同報メールの際に本来ＢＣＣで送信すべきところＴＯやＣＣで送信した（ＢＣＣとＴＯ／ＣＣの誤り）」「本来とは誤ったファイルを添付して送信した（ファイルの添付ミス）」といった具合だ。

これらの対策の基本はメール送信者一人ひとりが送信前にメール内容（宛先・本文・添付ファイル）が正しいか確認する行為を徹底することである。そのほか「宛先のオートコンプリート機能を無効にする」「送信メールを一時保留する」「添付ファイルを暗号化する」なども効果的な運用ルールである。

だがどんなに注意しても、すべてを担当者任せにしていては１００％守られることは不可能である。一方で誤送信を防ぐためのチェック作業が担当者の大きな負担となっているケースも多い。

誤送信による情報漏洩リスクの回避と担当者の負荷の軽減という両面の解消が必要だ。運用ルールによる対策だけでなく、それらを補完する「システムによる対策」との両輪で対策を講じていくことが有効だろう。

（ＳＯＭＰＯリスクマネジメント取締役　宮崎義久）

メール誤送信の発生要因と対応のポイント

主な発生要因
- 宛先間違い
- BCCとTO／CCの誤り
- ファイルの添付ミス

主な対応
- 宛先は必ずアドレス帳に登録し、手入力をしない
- メーラーの自動補完機能をOFFに
- 送信前に宛先が正しいかをチェック
- 添付ファイルを暗号化
- 同報送信時はBCCを使う

（注）SOMPOリスクマネジメント作成

2019年6月11日
日経産業新聞

マネジメント講座

情報漏洩を防ぐ ③　USBメモリー対策

USBメモリーは大容量のデータ保存や受け渡しに便利であり、社外に持ち出すことも多い媒体だ。そのためカバンに入れて電車の網棚に……といった移動時の乗り物内や路上、公園、飲食店などでの置き忘れが多い。うっかり落としたり、転んでなくしたりするケースもある。

社内でも、机の上に置きっぱなしにしたり、会議などで席を外した際に所在不明になってしまうケースが見受けられる。

こうした事象は手荷物が多い時や疲れている時、飲酒・飲食時、睡眠不足、何か急いでいる時などに起きやすい。USBメモリーは携帯しやすく、手軽に利用しやすいがゆえに、後から考えれば「なぜ持ち出したのか」と思えるような状況で紛失するケースもある。

業務上、どのような情報をUSBメモリーで持ち出す必要があるのかを確認し、運用ルールを見直すことが必要だ。

利用を許可する場合は、社外に持ち出すUSBメモリーにタグ・ストラップを付けたり、セキュリティー機能付きの製品を使用したりすることが対策上、有効である。

利用申請・承認の手続きを定め、利用後の初期化とともに定期的な棚卸しで所在を確認。長期間使われていないUSBメモリーは回収するなど、利用者の情報セキュリティー意識を継続的に高めていくことも重要だ。

USBメモリーを介したウイルス感染にも注意が欠かせない。社外のパソコンや社外で預かったUSBメモリーを社内環境に接続してネットワークに感染を広げないよう自動再生機能を停止させ、ファイルを開く前にウイルスチェックを行うことが重要になる。

（SOMPOリスクマネジメント取締役　宮崎義久）

USBメモリーを扱う際のリスクと対応のポイント

主なリスク

- 移動時の乗り物内、飲食店、路上などでの置き忘れ
- 落下、転倒による紛失
- ウイルス感染

↓

主な対応

- セキュリティー機能付きのUSBメモリーを使う
- 持ち運ぶ必要のない個人情報などを保存しない
- ファイルは暗号化して保存する
- USBメモリーにタグやストラップ、鈴を付ける
- 自動再生機能を停止する
- ファイルを開く前に必ずウイルスチェックを行う

(注)SOMPOリスクマネジメント作成

2019年6月18日
日経産業新聞

マネジメント講座

外出先でも油断なく

情報漏洩を防ぐ ④

高速の通信回線や無線を利用したネットワーク環境の普及により、外出先や交通機関での移動中に、ノートパソコンやタブレット、スマートフォンなどの端末を使って業務を行うケースが増えている。それに伴い、端末の置き忘れや盗難、ショルダーハッキング（端末画面ののぞき見）などのリスクも増している。

中でも置き忘れなどの紛失や盗難は、持ち物から意識が薄れたときや持ち物から遠ざかったとき、夜間の外出、海外出張時などに頻繁に発生している。

端末は電車の網棚などに置かず、常時目の届くところで保管することを徹底すべきである。外出先で端末を利用する場合には、画面が見える範囲に人がいないことを確認し、端末にのぞき見防止フィルターを貼るなどの対応が必要になる。

やむを得ず離席する場合には端末のロックなどの対策を行うことを徹底すべきだろう（パスワードを書いた紙を貼り付けるなどは論外である）。

最近はフリーＷｉ－Ｆｉのアクセススポットが充実し、誰でも簡単に利用できるようになった。しかしフリーＷｉ－Ｆｉはまだ暗号化されていないセキュリティーの甘いものが多く存在する。

安易に接続すると無防備なネットワークにつながってしまい、盗聴や情報漏洩の危険性が高まる。無線ＬＡＮを使う場合には、信頼できるアクセスポイントを選び、適切な暗号化などの設定を行うことが必要である。

交通機関での移動中や商談前に立ち寄った飲食店などで、ついこれからの商談について話しているケースもみられる。誰が居合わせているか分からない。公共の場での会話や電話の内容に注意を払う必要がある。

（ＳＯＭＰＯリスクマネジメント取締役　宮崎義久）

外出先で業務用端末を使う リスクと対応のポイント

主なリスク

- 置き忘れや紛失、盗難
- 端末画面ののぞき見
- ウイルス感染
- 電話・会話の声漏れ

主な対応

- 端末が入ったカバンから目を離さない
- 端末にパスワードを書いた紙を貼り付けない
- 信頼できるアクセスポイントを選ぶ
- 適切な暗号化などの設定を行う
- 公の場で機密情報を話さない

(注)SOMPOリスクマネジメント作成

2019年6月25日
日経産業新聞

マネジメント講座

情報漏洩を防ぐ ⑤　社有車でもリスク認識を

個人情報や機密情報が入ったノートパソコンやUSBメモリー、書類などが車上荒らしで盗まれるケースがある。盗難ではなくても、駐車場から車を出す際に書類などを屋根に置いてそのまま発進させてなくしたり、車庫の中や路上に機密情報の入ったカバンなどを置き忘れたりといったケースもみられる。

警察庁の統計によると、2018年度に発生した車上荒らしは5万4千件あまり。そのうち「施錠あり」のケースは半数の約2万7千件を占めた。これはあくまで警察庁が認知した犯罪の統計だが、施錠をしていても決して安心はできないことがわかる。

ビジネスシーンの中で使われることの多い移動手段である「社有車」についても、機密情報をどのように扱うかが大きな課題になっている。

社外へ機密情報を持ち出すことは情報セキュリティーの側面からは大きなリスクを伴うが、それなしで業務を行うことは非現実的である。実際に持ち出している情報を「本当に持ち出す必要があるのか」「すべて持ち出さなければならないのか」という観点でみると、本来は必要のない情報まで外部に持ち出していることに気づくだろう。

機密情報を持ち出す場合には、最低でも「いつ」「どこで」「誰が」「どのような目的で」「どのように」「どのような情報を」利用するのかを把握しておく必要がある。その上で個人情報を持ち出す際には、上司の許可を条件にするといった対処も有効である。

さらに社有車で機密情報を持ち出す場合には、ちょっとした休憩であっても、助手席に物を置いて車を離れてはいけない。盗難や紛失は誰もが巻き込まれる可能性があることを常に認識させ続ける必要がある。

（SOMPOリスクマネジメント取締役　宮崎義久）

社有車での移動中のリスクと対応のポイント

主なリスク

- 盗難（車上荒らし）
- 車屋根への置き忘れ
- 車庫や路上での置き忘れ

主な対応

- 個人情報を持ち出す際は、上司の許可を必要にする
- 車の助手席に物を置いて、車を離れない

（注）SOMPOリスクマネジメント作成

2019年7月2日
日経産業新聞

マネジメント講座

情報漏洩を防ぐ ⑥　在宅勤務にもリスク

総務省の２０１８年版「情報通信白書」は、在宅勤務を実施する企業が緩やかに増加していると指摘した。働き方改革の進展やＩＣＴ（情報通信技術）の発達に伴い、更なる増加が見込まれる。ただ業務上、社外に情報を持ち出すため、様々なリスクが考えられる。

その一つが、場所のリスクだ。テレワークの利用により、自宅だけでなく公共エリアでも業務をこなせるようになる半面、部外者が重要情報を不正に閲覧・入手するリスクが想定される。

対策としては、在宅勤務を実施できる場所の限定や、情報の取り扱いルールを社内で決めておくことが重要である。

二つ目は媒体のリスクだ。在宅勤務で使うパソコンや書類などについては電子媒体ならばウイルス感染などのリスク、紙媒体であれば紛失などのリスクが考えられる。

在宅勤務に当たっては、電子媒体は情報セキュリティー対策が施された自社の媒体を貸与することが望ましい。紙媒体については、個人情報・機密情報の持ち出しルールを順守した上で、在宅勤務終了後に会社へ返却させ、書類などの紛失がないかも確認すべきだ。

三つ目が通信のリスクだ。在宅勤務やテレワークでは、リモート接続でウェブを閲覧しながらの作業も考えられる。無料のＷｉ－Ｆｉなどを利用すれば、ウイルス感染のリスクが高まる。

通信については会社が契約するＷｉ－Ｆｉ機材を利用させ、自宅のＷｉ－Ｆｉや無料Ｗｉ－Ｆｉの利用は禁止するなどの対策が有効になる。

在宅勤務をする従業員本人が、そのリスクを認識することも重要だ。リスクと対策に関する教育を定期的に実施することが欠かせない。

（ＳＯＭＰＯリスクマネジメント取締役　宮崎義久）

在宅勤務のリスクと対応のポイント

主なリスク
- 場所のリスク
- 媒体のリスク
- 通信のリスク

主な対応
- 在宅勤務実施場所の限定
- 情報の取り扱いルールの制定
- 必要な機材を会社から貸与
- 紙などは持ち出し枚数の制限など
- 安全な通信手段の選択
- 従業員教育

(注)SOMPOリスクマネジメント作成

2019年7月9日
日経産業新聞

マネジメント講座

酒席は特に用心を

情報漏洩を防ぐ ⑦

歓送迎会などの宴席、社員同士の飲食や取引先との酒席など、仕事にかかわる社外での会合は日常的な光景だ。このような席を通じて相手との円滑なコミュニケーションが期待できる一方、情報セキュリティーの観点からはリスクも多い。組織として、適切なルール作りを含めて対策を実施すべきである。

お酒を飲むと緊張感が緩み、つい、会社の内部情報や社内外の人間関係などを愚痴と一緒に話してしまいがちだ。だが、それは情報漏洩になる可能性がある。会話の内容から具体的な状況などが類推可能となるケースも考えられる。機密情報や顧客情報などについて酒席で口外することを厳しく禁じ、定期的に従業員へ周知する必要がある。

飲酒で注意力が低下し、所持品の紛失や置き忘れをしたり、車内や駅のホームで居眠りをしたすきに所持品が盗難にあったりといった事態が起きることもあり得る。

カバンに顧客から預かった資料や社用パソコンが入っていれば、情報漏洩の事故となり、顧客への謝罪などの対応に追われることになる。重要情報を所持した状態での酒席参加の禁止などといった対策をとる必要もあるだろう。

酒席の状況をＳＮＳ（交流サイト）に流すといったケースも増えている。ただ書き込む内容によっては情報漏洩になったり、会社の信用を傷つけたりする事態になりかねない。ＳＮＳの使用におけるルールを設け、従業員に徹底すべきだ。

情報漏洩の事故は、業務時間中にだけ発生するわけではない。業務時間外であっても従業員に実施してもらいたい情報セキュリティー対策を明確にし、周知し続ける活動が欠かせない。

（ＳＯＭＰＯリスクマネジメント取締役　宮崎義久）

酒席におけるリスクと対応のポイント

主なリスク

- 会話内容に重要情報が含まれる
- 所持品の紛失・盗難
- SNSへの不適切な投稿

主な対応

- 社外での重要情報の口外を禁止するルールを制定、周知
- 酒席参加における所持品の限定
- SNSへの書き込みルールの制定、周知
- 上記対応の継続的な実施

(注)SOMPOリスクマネジメント作成

2019年7月23日
日経産業新聞

マネジメント講座

クラウド利用の落とし穴

情報漏洩を防ぐ ⑧

総務省が発表した2018年の通信利用動向調査によると、クラウドサービスを利用していると回答した企業の割合は約6割に達した。16年の調査では5割未満だった。今後も利用率は高まり続けるとみられる。

確かにクラウドサービスは便利だが、一定のリスクがあることを認識したうえで従業員に利用させることが重要だ。

クラウドサービスでは、IDとパスワードを組み合わせた情報を使って個人を認証する仕組みが多く用いられている。

しかし従業員が個人や会社で利用するクラウドサービスに認証情報を使い回した場合、1つのサイトの認証情報が漏れてしまえば、悪意のある者によって他のサービスにアクセスされ、情報窃取や不正利用の被害に巻き込まれる恐れがある。

IDとパスワードの使い回しが不可で、二段階認証であるなど、より高度な認証を実装しているクラウドサービスを利用することが重要だ。

クラウドサービスには、自社が貸与するパソコン以外のデバイスからでもアクセスできる機能もある。だが自社管理外のデバイスで同サービスにアクセスした際、認証情報や履歴が残ったり、ダウンロードした情報がデバイス内に残ったりし、社外に重要な情報が漏れる恐れもある。利用するサービスは慎重に選定する必要がある。

クラウドサービスは業務効率の向上など、事業競争力をつけるうえで重要なツールになり得る。半面、デジタル依存度が高まることで情報セキュリティーのリスクも大きくなり、事業に影響をおよぼす可能性がある。

クラウドサービスを採用する際は、デジタル変革と併せて、企業の情報セキュリティーマインドの変革対応を実施すべきである。

（SOMPOリスクマネジメント取締役　宮崎義久）

クラウドサービスのリスクと対応のポイント

主なリスク

- 個人認証情報の使い回しによるリスク
- 自社管理以外のパソコンでも利用可能なリスク

主な対応

- 認証情報の使い回しの禁止
- より高度な個人認証方法を採用したサービス利用
- 自社管理以外のパソコンによるサービス利用の禁止
- 社外のデバイスからアクセスできない仕様の採用
- サービス利用後にデータを残さない方法の採用

(注)SOMPOリスクマネジメント作成

2019年7月30日
日経産業新聞

マネジメント講座

情報漏洩を防ぐ ⑨

事故対応への備え

情報の紛失、誤送信、サイバー攻撃など情報セキュリティーの事故につながる事態を予防することは重要だが、リスクをゼロにすることはできない。そのため万一の備えとして事故発生時の対処について準備しておくことが重要になる。

企業が準備すべきポイントは以下の通りだ。まず事故に素早く対応するため、事故発生の事実を迅速に責任者へ報告できる仕組みが必要である。

その際、どのような事態が事故に当たるのかをあらかじめ定義し、従業員に周知することが重要だ。事故を起こした従業員が報告しやすくなるよう「悪意ではない事故で速やかな報告であれば、厳罰を与えない」ことも周知すべきである。

事故報告を受けた後、社内の情報統制に配慮しつつ常に状況を正確に捉えて適切に対処しなければいけない。事実確認や原因特定の調査はもちろん、自社や顧客らにどのような悪影響が想定されるかの整理が必要だ。

調査結果と影響の大きさによっては、顧客への謝罪や事故の説明が必要になる。謝罪対応の準備も重要である。

謝罪対応については、事実関係の報告だけでなく、今まで実施してきた予防策、事故発覚から謝罪までの対応内容、今後の再発防止策や補償などについて説明できるように準備しなければ、顧客への説明責任を果たせない恐れがある。

監督官庁やその他の利害関係者への対応、従業員への指示、苦情相談への対応など、実施すべき事項は多くある。

一連の事故対応では、状況の変化を把握するため、広く情報を収集し続けることが重要だ。平時から事故対応における役割分担や手順を定め、実際にそのとおり動けるかを訓練するといった対応準備も欠かせない。

（SOMPOリスクマネジメント取締役　宮崎義久）

事故発生時の対処のポイント

主なポイント
事故発生の事実を迅速に責任者へ連絡
状況を正確に捉える活動
謝罪対応など利害関係者への説明

▼

主な対応
■事故内容の定義と社内周知
■事実確認と原因特定調査
■説明に必要となる事項の準備
■社内外に対して広く情報収集
■上記の対応を適切に実施するための平時からの手順作成や訓練

（注）SOMPOリスクマネジメント作成

2019年8月6日
日経産業新聞

マネジメント講座

従業員の意識改革が大事

情報漏洩を防ぐ ⑩

情報漏洩事故を継続して防ぐには、これまで紹介してきた対策を実施するほか、従業員の情報セキュリティーマインドの向上が不可欠だ。連載の最終回にあたり、マインド面からのアドバイスを幾つか紹介していこう。

まず従業員に対して定期的に情報セキュリティー対策の内容と、実施する理由をセットで教育することを勧めたい。

従業員は禁止事項や対策内容を聞いても、その理由に納得がいかなければ、そのセキュリティー対策が単に非効率な活動に見えてしまい、対策を軽視する恐れがある。

情報セキュリティーの研修では、その対策の実施を決めた経緯や、実施しないことで起きる恐れのあるリスクについても丁寧に伝えたい。従業員が事故の具体的なシーンを思い浮かべ、影響の大きさを認識し、適切な対処が欠かせないことを実感することが重要だ。

日常から周囲への声かけや意識付けを行うことも勧めたい。情報セキュリティー対策は仮に実施しなくても業務を遂行できてしまうことがある。だが個人の注意力や記憶力に頼りすぎてはヌケやモレが起きかねない。

朝礼や会議などで情報セキュリティー活動の重要性を周知するのはもちろん、社内の壁面などに注意事項を張り出すのも有効だ。従業員同士の声かけを通じて、誰もが情報セキュリティー対策を意識し、組織が一体となって対策のヌケ・モレを防ぐことが欠かせない。

これらの活動を組織が継続的にやり続ける、言い続けることにより、情報セキュリティー活動を『当たり前』の文化にしたい。これが社内風土として根付き、マインドを持った従業員が適切に業務とセキュリティー対策を実施することで、事故を起こしにくい組織をつくることが期待できる。

（SOMPOリスクマネジメント取締役　宮崎義久）

＝この項おわり

情報漏洩を起こさないためのポイント

主なポイント

- 情報セキュリティー対策の実施だけを伝えても形骸化する恐れがある
- 個人の能力に頼るには限界がある

↓

主な対応

- 情報セキュリティー対策の内容と実施する理由をセットで教育
- 情報セキュリティーが常に意識できる環境を用意
- 上記の活動を継続的にやり続け、言い続けて社内風土とする

（注）SOMPOリスクマネジメント作成

2019年8月20日
日経産業新聞