中小企業における
情報セキュリティ対策の実態調査
- 事例集 -

2017 年 7 月 7 日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目　次

【事故事例】

事例 1　栃木県／製造業 1
事例 2　東京都／製造業 2
事例 3　神奈川県／製造業 3
事例 4　新潟県／製造業 4
事例 5　静岡県／製造業 5
事例 6　兵庫県／製造業 6
事例 7　鳥取県／製造業 7
事例 8　東京都／情報通信業 8
事例 9　東京都／情報通信業 9
事例 10　東京都／情報通信業 10
事例 11　京都府／情報通信業 11
事例 12　奈良県／情報通信業 12
事例 13　秋田県／運輸業 13
事例 14　宮崎県／運輸業 14
事例 15　富山県／卸売業 15
事例 16　山形県／卸売業 16
事例 17　滋賀県／卸売業 17
事例 18　福岡県／卸売業 18
事例 19　福島県／小売業 19
事例 20　福井県／小売業 20
事例 21　滋賀県／小売業 21
事例 22　東京都／金融業 22
事例 23　埼玉県／不動産業 23
事例 24　東京都／不動産業 24
事例 25　京都府／不動産業 25
事例 26　高知県／不動産業 26
事例 27　福岡県／不動産業 27
事例 28　栃木県／サービス業 28
事例 29　東京都／サービス業 29
事例 30　神奈川県／サービス業 30
事例 31　福岡県／サービス業 31
事例 32　福岡県／サービス業 32

【事故以外事例】

事例 33　新潟県／農林水産業 33
事例 34　石川県／農林水産業 34
事例 35　島根県／農林水産業 35
事例 36　徳島県／農林水産業 36
事例 37　鹿児島県／建設業 37
事例 38　千葉県／製造業 38
事例 39　岩手県／情報通信業 39
事例 40　群馬県／情報通信業 40
事例 41　富山県／情報通信業 41
事例 42　和歌山県／情報通信業 42
事例 43　香川県／情報通信業 43
事例 44　佐賀県／情報通信業 44
事例 45　沖縄県／情報通信業 45
事例 46　愛知県／運輸業 46
事例 47　広島県／運輸業 47
事例 48　山形県／小売業 48
事例 49　山口県／小売業 49
事例 50　北海道／金融業 50
事例 51　青森県／金融業 51
事例 52　岡山県／金融業 52
事例 53　福岡県／金融業 53
事例 54　熊本県／金融業 54
事例 55　三重県／不動産業 55
事例 56　大阪府／不動産業 56
事例 57　大分県／物品賃貸業 57
事例 58　宮城県／サービス業 58
事例 59　茨城県／サービス業 59
事例 60　東京都／サービス業 60
事例 61　長野県／サービス業 61
事例 62　岐阜県／サービス業 62
事例 63　大阪府／サービス業 63
事例 64　大阪府／サービス業 64
事例 65　兵庫県／サービス業 65
事例 66　岡山県／サービス業 66
事例 67　愛媛／サービス業 67
事例 68　長崎県／サービス業 68

事例一覧

No.	所在地	業種											企業規模					事故ケース						頁
		農林水産業	建設業	製造業	情報通信業	運輸業	卸売業	小売業	金融業	不動産業	物品賃貸業	サービス業	５名以下	６～２０名	２１～５０名	５１～１００名	１０１～３００名	ウイルス感染	ランサムウェア	標的型攻撃	不正アクセス	内部不正	パソコン紛失	
1	栃木県			○												○		○						1
2	東京都			○												○			○					2
3	神奈川県			○										○					○					3
4	新潟県			○											○				○					4
5	静岡県			○												○		○						5
6	兵庫県			○													○	○	○					6
7	鳥取県			○											○			○						7
8	東京都				○								○								○			8
9	東京都				○												○	○						9
10	東京都				○												○						○	10
11	京都府				○												○	○		○				11
12	奈良県				○								○								○			12
13	秋田県					○									○					○				13
14	宮崎県					○											○				○			14
15	富山県						○									○		○						15
16	山梨県						○							○				○						16
17	滋賀県						○							○					○					17
18	福岡県						○							○				○						18
19	福島県							○						○				○						19
20	福井県							○									○			○				20
21	滋賀県							○							○			○						21
22	東京都								○								○				○			22
23	埼玉県									○				○					○					23
24	東京都									○			○					○						24
25	京都府									○					○				○					25
26	高知県									○						○		○						26
27	福岡県									○					○				○					27
28	栃木県											○		○								○		28
29	東京都											○			○			○						29
30	神奈川県											○			○			○				○		30
31	福岡県											○		○				○						31
32	福岡県											○		○								○		32
33	新潟県	○														○								33
34	石川県	○											○											34

No.	所在地	業種											企業規模					事故ケース						頁
		農林水産業	建設業	製造業	情報通信業	運輸業	卸売業	小売業	金融業	不動産業	物品賃貸業	サービス業	5名以下	6～20名	21～50名	51～100名	101～300名	ウイルス感染	ランサムウェア	標的型攻撃	不正アクセス	内部不正	パソコン紛失	
35	島根県	○												○										35
36	徳島県	○												○										36
37	鹿児島県		○														○							37
38	千葉県			○													○							38
39	岩手県				○									○										39
40	群馬県				○											○								40
41	富山県				○									○										41
42	和歌山県				○									○		○								42
43	香川県				○																			43
44	佐賀県				○								○											44
45	沖縄県				○										○									45
46	愛知県					○									○									46
47	広島県					○											○							47
48	山形県							○							○									48
49	山口県							○					○											49
50	北海道								○								○							50
51	青森県								○						○									51
52	岡山県								○						○									52
53	福岡県								○								○							53
54	熊本県								○							○								54
55	三重県									○				○										55
56	大阪府									○				○										56
57	大分県										○				○									57
58	宮城県											○		○										58
59	茨城県											○			○									59
60	東京都											○	○											60
61	長野県											○		○										61
62	岐阜県											○				○								62
63	大阪府											○			○									63
64	大阪府											○				○								64
65	兵庫県											○			○									65
66	岡山県											○			○									66
67	愛媛県											○		○										67
68	長崎県											○		○										68

事例 1

所在地	栃木県
業種	製造業
従業員規模	51～100 名
事故の有無	有(2013 年)
ケース	ウイルス感染

ウイルス対策ソフトの運用不備で情報漏えい事故が発生 取引先からの信用回復と対策強化に力を注ぐ

■ 発生した事故と影響

当社は、栃木県南部で加工食品の製造及び卸売業を営んでいる。近年は、インターネットによる一般消費者向けの通信販売も開始した。2013 年、役員のパソコンがウイルス感染し、保存されていた過去の電子メールが勝手に大量発信され、自社及び取引先の重要な情報が漏えいする事態となった。取引先からはクレームが寄せられ、謝罪はしたものの信用が失墜してしまった。

■ 事故の要因

- 感染したパソコンにはウイルス対策ソフトはインストールされていたが、アップデートが実施されていなかった。十数台ある他のパソコンも使用者任せの状況であり、再発の危険は非常に高かった。
- IT ベンダでの勤務経験がある従業員から、出入口の施錠等の物理的なセキュリティの問題を指摘されていたが、当時は従業員以外の個人情報の取り扱いは少なく、セキュリティ対策よりも売上を伸ばし経営を維持することが優先と考えていたため特別な対策は行われていなかった。

■ 事故後の取り組み

組織的	人的	物理的	技術的

- 組織としてのセキュリティ体制の確立と従業員のセキュリティ意識の醸成を優先的に行った。具体的には、社長を情報セキュリティ責任者、IT 担当者をセキュリティ対策推進担当者とし、組織としてセキュリティ対策に取り組むことを全従業員に宣言した。
- 従業員に対する啓蒙・教育として、定期的にセキュリティ対策に関する動画を視聴し、社長からのコメントや取り組みの報告を行った。
- また、事故の再発を防ぐためにシステム面でのリスク調査を行い、緊急性が高いリスクから順次対策を行った。具体的には、USB メモリによるデータの持ち出し制限、Wi-Fi のセキュリティ強化、パソコンへの重要情報の保存禁止、ノートパソコンのワイヤーロック、ビジネス型ウイルス対策ソフトによる集中管理などである。

■ 取り組みによる効果

以前のセキュリティ事故により失った取引先からの信頼はまだ回復していないものの、当社の取り組み内容を説明することで徐々に理解を得られるようになってきた。社内では、「今までやってなかったのになぜやるのか」「業務効率が下がる」などの否定的な意見が多いのが現状である。しかし、一部の従業員からは、セキュリティに対する心配や対応方法の相談なども寄せられるようになっており、意識向上につながってきている。

■ 情報セキュリティ担当者の視点

インターネット通販事業を開始し、取り扱う個人情報も増えていることから、一層のセキュリティ対策強化が必要と考えている。まずは実態に沿った対応を進め、全従業員に個人情報を守ることを根付かせたい。時間はかかるだろうが、社長及び情報セキュリティ担当者が中心となり、しっかりとした仕組み作りと企業風土の醸成に努めていく。将来的にはプライバシーマークの取得を目指して、積極的に取り組んでいきたい。

事例 2

所在地	東京都
業種	製造業
従業員規模	51～100 名
事故の有無	有(2016 年)
ケース	ランサムウェア

製品納入先の高い情報セキュリティレベルに合わせることで、安心して業務を実施

■ 発生した事故と影響

当社は、東京都で自動車部品を加工製造している。完成車メーカーから提供される受注データや見込みデータは、自動車部品組合のサーバから当社へ直接送信されるため、情報セキュリティ対策は完成車メーカーの指示に従う必要がある。しかし、これまで完成車メーカーから、当社のウイルス感染したパソコンからのメール送信を注意されたことがある。また、2016 年、海外から来たメールに添付されていたファイルを開封して「ランサムウェア」と思われるマルウェアに感染し、パソコンが使用不能になり、パソコンを入れ替えた。

■ 事故の要因

従業員の情報セキュリティに関する意識が不十分であったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 情報セキュリティ対策は、すべてのパソコンにウイルス対策ソフトを導入するなど、完成車メーカー指定の仕様に合わせることを原則としている。完成車メーカー指定のシステム会社に業務委託し、当社のシステム環境を整備しているため、当社内には IT 専門の担当者を置いていない。システム会社は、自動車業界・自動車部品業界など業界標準に精通しているため、安心して業務委託を任せることができている。
- 従業員に対して、社外から届く電子メールに添付されているファイルを開封する時は、発信元の会社名を確認するように注意をしている。
- 完成車メーカーから来るデータは、社内の重要なデータで、完成車メーカーからの受注、作業指示、出荷、請求に利用している。会計業務は会計事務所に接続されたパソコンを利用し、社内のネットワークからは分離している。
- システムが止まると出荷ができなくなるため、毎日異常なく利用できることを前提としているが、情報漏えい防止のためにあえてバックアップは取得していない。発注データが消失した場合は、発注元にある控えのデータをマスターとして再送してもらう運用にしている。

■ 取り組みによる効果

システムが安定的に運用され利用できることと、完成車メーカーの高い情報セキュリティレベルに合わせることで、安心して業務を実施できている。

■ 情報セキュリティ担当者の視点

現状では IT システムが社内インフラとして十分機能し、活用されていると考えている。IT 専門の担当者は不在ではあるが、特定のシステム会社を活用できている状況である。情報セキュリティ対策が重要であることは理解しており、今後は優先順位付けや予算措置について検討していきたい。

事例 3

所在地	神奈川県
業種	製造業
従業員規模	6～20 名
事故の有無	有(2015 年)
ケース	ランサムウェア

自社の IT リテラシーのレベルに見合った情報漏えい対策 従業員の意識変革と仕組みによる防御の二本立て

■ 発生した事故と影響

当社は、神奈川県で真空ポンプなど真空機器装置の設計・改造・製造・メンテナンス事業を展開している。2015 年、ある日届いた経営者宛のメールに添付されているファイルを安易に開いてしまった結果、「ランサムウェア」に感染し、「ファイルをロックしたので、解除して欲しければ連絡をするように」と電話番号を含む警告画面がパソコンのスクリーン上に表示され消えなくなった。社内の重要データは共有サーバで管理されており、バックアップ等を行っていたため会社としての被害はなかったが、個人の写真などのデータは参照できなくなっていた。

■ 事故の要因

事故に遭うまで、当社の経営層を含む従業員の IT リテラシーや情報セキュリティに対する意識は、決して高いものではなかった。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 「内部の人間が意識せずに被害にあう」ことを防ぐために、勉強会などを開催して従業員の意識を変えることに取組んでいる。また、メールサーバのフィルタリング機能を利用して、必要のないメールは従業員に届かないようにすることに取組んでいる。従業員の意識変革と仕組みによる防御の二本立てで取り組みを行っていく必要があると考えている。
- 情報漏えいによって企業の存続を揺るがすような情報の多くは紙で管理している。電子化されたデータは漏えいすれば問題はあるものの、決定的なダメージを受けることはない。こうした現状を変化させないことは、IT リテラシーの高くない当社にとっては一つの考え方だと感じている。

■ 取り組みによる効果

これまで言葉は聞いたことがあっても、どんなものかイメージできていなかったランサムウェアの被害が実際に社内で発生したことで、情報セキュリティは自分達にも関係があるものだということが意識付けされたと思っている。しかしながら、情報セキュリティが自分達の実際の業務に直接関係することが少ないせいか、意識が十分に高まったとは言えない。また、仕組みとしてメールサーバのフィルタリング機能を利用し、受信する迷惑メールの数を減らしているが、フィルタリングを強力にすることで本来必要なメールが届かなくなったり、反対にフィルタリング機能を弱くすると、フィルタリングの効果が出なかったりと試行錯誤しながら対応しているのが現実で、利便性とセキュリティのバランスの重要さと難しさを認識している。

■ 情報セキュリティ担当者の視点

中小企業にとっては、情報セキュリティにどれだけの予算を計上するのかは非常にシビアな問題であり、大がかりな投資を行うことが難しいと考えている。そのような状況の中で、自社の状況や外部からの評価を意識し、外部からの信頼を落とさないための取り組みとして、情報セキュリティに関しても考えていく必要があると思っている。従業員のセキュリティ対策に対する意識についても、従業員が無意識に情報セキュリティの被害にあわない仕組みについても、一朝一夕でできるものではないので、時間をかけて取り組みを継続していきたい。

事例 4

所在地	新潟県
業種	製造業
従業員規模	21～50 名
事故の有無	有(2015 年)
ケース	ランサムウェア

ランサムウェア感染をきっかけにセキュリティ対策を強化 コスト最適化と従業員の意識改革に取り組む

■ 発生した事故と影響

当社は、新潟県北東部に本社を置く住宅関連機器メーカーである。2015 年、ウェブサイトの閲覧を通じて「ランサムウェア」に感染し、ローカルファイルとネットワーク上の共有フォルダが暗号化された。バックアップファイルからデータを復元できたため被害は最小限で済んだが、この経験により組織的な情報セキュリティ対策の必要性を再認識することとなった。

■ 事故の要因

感染したパソコンの OS はサポートが終了した Windows XP だった。通常は、リスク回避のためオフライン運用をしていたが、不注意でネットワークに接続したことからランサムウェアに感染した。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 運用面の対策は、本社業務部門の部門長を責任者とし、当社として取り組むべき情報セキュリティ対策の方針・社内ルールを定め、社内通達や連絡会議等の場を通じて周知徹底を図っている。また、毎年情報セキュリティセミナーに参加し、最新動向の把握と社内への普及啓発に努めている。
- 技術的な対策は、既知のマルウェアを確実に検出できるよう OS の更新やウイルス対策ソフトの定義ファイルを自動更新設定にするなど、常に最新の状態にしておくように徹底している。また、万が一マルウェアに感染した場合でも、復元できるよう重要な情報資産は定期的に外付け HDD へバックアップをとっている。現在は、標的型攻撃メールに備えたプロバイダーの迷惑メールフィルタオプションの採用を検討中である。

■ 取り組みによる効果

- 情報セキュリティに対する取り組み方針を明確にできた。具体的には、社内の情報資産の分類及びリスク分析を行った結果、当社としては「ソフトウェアの最新化」と「バックアップの徹底」の 2 点を重点対策として定めている。
- ウイルス対策ソフトのコスト最適化ができた。定義ファイルを自動更新することで既知の脅威に備えている。未知の脅威については完全には防げないと考えており、「感染した場合はバックアップから復元できればよい」という考え方で OS 標準搭載のセキュリティ保護機能を主体とする運用にしたことで、年間 30 数万円のコスト削減につながった。
- 従業員の情報セキュリティに対する意識も高まっている。基本動作（漏えいして困る情報は社外に持ち出さない、怪しいメールは開かずに削除する、感染に気付いたら直ちにネットワークから切り離す等）が身に付いたことで、判断を任せられるようになった。ランサムウェアの被害経験以降、セキュリティ事故は発生していない。

■ 情報セキュリティ担当者の視点

仕事にストレスのかかるようなセキュリティ対策はとるべきではなく、過剰な投資にならないよう配慮している。当社の規模や事業内容において、情報セキュリティ対策にどこまで投資すべきか、また投資対効果をどのように判断するかといった点に適切な基準を持つことが望まれるため、公的機関や IT ベンダ主催の情報セキュリティセミナー等を通じて、最新情報の収集やリスク、課題等の把握に努め、限りある経営資源を有効活用できるよう推進していきたい。

事例 5

所在地	静岡県
業種	製造業
従業員規模	51～100 名
事故の有無	有(2008 年)
ケース	ウイルス感染

UTM の導入や情報セキュリティ対策の実践により取引先から高い評価と信頼を得ている

■ 発生した事故と影響

当社は、静岡県で薄板鋼板の板金製作を多品種少量生産で行っている製造業である。2008 年頃、従業員がメールに添付されていたファイルを不用意に開き、ウイルス感染により当社の基幹システムの設定が書き換わる障害が発生した。システムベンダの協力を得て障害の調査を行い、復旧するまでの 1 週間ほど、基幹システムの一部が使用できなくなった。幸い、他には被害はなかったが、セキュリティ対策の重要性を痛感した。また、当社では取引の約 8 割を EDI で行っており、また、図面や CAD ファイルなどの取引先の重要なファイルを預かって製造を行うため、安定稼働と情報流出防止の観点で、セキュリティ対策はますます重要になっている。

■ 事故の要因

メールフィルタリングツールを導入していないことに加え、不審メールを受信した際の対処方法を詳しく知らなかったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- セキュリティ対策に関するベンダからの紹介や提案などを受け、ランサムウェアの対策に UTM を導入し、UTM の出力レポートのチェックを毎日行っている。メールフィルタリングツールにより、添付ファイルと全文検索を行っている。また、2014 年に本社・工場間に VPN を導入し、セキュリティの強化を図り、ウイルス対策は、ウイルスチェッカーを USB メモリに入れて定期的に全パソコンのチェックを行っている。パソコンの廃棄は、ハードディスクを取り出して廃棄し、取り出したハードディスクは粉砕して廃棄することとしている。
- 朝礼等を利用して従業員に情報セキュリティ対策の重要性についての啓発も行っている。

■ 取り組みによる効果

取引の 8 割を占める EDI 等、インターネット環境を支障なく、安全に利用できている。UTM を導入している企業は少なく、情報セキュリティ対策を実践していることで、取引先等からの評価は高く、信頼されている。VPN の導入により社内システムを安全に使用しており、サーバや工作機械のリモートメンテナンスも行っている。大量のスパムメールをはじいているので、業務の効率化に寄与していると考えられる。また、地域の企業からも頼りにされて、情報セキュリティ対策等で相談を受け、サポートを行うこともある。

■ 経営者の視点

業務を行う上でインターネットの利用は不可避である。セキュリティ対策を重ね、2008 年頃の障害以降、幸い被害は発生していないが、UTM 等でも防ぐことのできない脅威があると考えられ、これまでの対策で十分とは考えてはいない。今後は人材を育成し、セキュリティ関連業務を分担していきたいと考えている。現在、本社事務所にサーバを設置しているが、サーバ室の分離、サーバのクラウド化についても考えている。従業員の情報セキュリティ意識はまだまだ十分とは言えず、従業員の何気ないパソコン操作が脅威となるおそれがあり、さらなる教育を行い、意識の向上が必要と考えている。従業員教育では、IPA が公開している情報セキュリティの普及啓発資料を利用して教育を行うことを考えている。

事例 6

所在地	兵庫県
業種	製造業
従業員規模	101～300 名
事故の有無	有(2015 年)
ケース	ウイルス感染 ランサムウェア

技術的な対策だけでは万全ではない、従業員の意識の高さが組織を守る

■ 発生した事故と影響

当社は、兵庫県で自動車タイヤ用チューブ、配管機材等のゴム製品、加速度センサ等の製造・販売を行っている。
2005 年頃、社内のパソコンやサーバがマクロウイルスに感染した。数名の担当者が深夜まで復旧作業を行ったが、知識不足のためウイルス駆除の方法を間違えて拡散させてしまい、収束に 1 週間ほど費やした。幸い、会社として業務停止に陥ることはなかった。また、2015 年、総務系パソコン 2 台が「ランサムウェア」に感染し、すべてのデータが暗号化されて元に戻すことができなかった。当社は差分バックアップを行っていたため、データ滅失は一部で済んだが、再作成に時間がとられ、その間、社内の支援業務が遅延しないよう残業等で対応せざるを得なかった。発見が早かったため、社内の他部門及び取引先への感染拡大がなかったことは不幸中の幸いであった。

■ 事故の要因

2005 年頃のウイルス感染時にはウイルス対策を実施していなかった。その後、ウイルス対策ソフトを導入しており特段の問題もなく推移していた。しかし、2015 年、公的機関になりすました偽メールに従業員がだまされてメールに記載されている URL をクリックしたためにランサムウェアに感染した。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 電子メールによるウイルス感染防止のための従業員教育を行った。
- 情報資産管理の充実を図った。対象はパソコン、サーバ等の IT 資産の台帳管理だけでなく、ウイルス感染や故障等のトラブル防止、ソフトウェアライセンスの適正使用等多岐にわたる。
- 現在の重点的な取り組みは、情報漏えいの防止である。内部犯行による情報漏えい対策は、大手企業だけではなく、当社にとっても喫緊の経営課題である。プロジェクトチームを結成し、情報漏えいに関するインシデントタイプを分析し、考えられる経路毎にデータアクセス制御に関する対策方法、ハード・ソフトの守備範囲等、技術面の検討をしている。文書・情報管理規程の見直し、モラルアップ等組織面からの対策も重視している。

■ 取り組みによる効果

- 情報の適正な管理については就業規則で規定しているだけであるが、ウイルス対策ソフト、USB メモリのパスワード設定等について説明することにより従業員の意識は高くなっている。
- 取引先の大手企業が適宜実施する情報セキュリティ対策調査にも真摯に回答しており特段の要請等はなく、取引を継続できている。これまでに内部からの情報漏えいが起きていないこともその効果だと考えている。

■ 情報セキュリティ担当者の視点

情報資産管理では推進者と経営幹部がリスク評価を共有し、セキュリティ対策の優先順位付けをして、情報漏えいの経路を断つことが重要である。また、どんなに優れた対策をしていても一人でも意識の低い従業員がいれば、インシデントが発生してしまうので、組織と個人を守るためには、“ONE FOR ALL, ALL FOR ONE”の精神が不可欠である。情報セキュリティ対策を全社的な運動として推進することが喫緊の課題である。今後は、情報漏えいや紛失、盗難等が発生した場合の対応手順の整備、各部署へのセキュリティ担当者の配備、内部監査の制度化等を検討していく予定である。

事例 7

所在地	鳥取県
業種	製造業
従業員規模	21～50 名
事故の有無	有(数年前)
ケース	ウイルス感染

低コストでできるセキュリティ対策を実施しながら妥当なレベルを模索

■ 発生した事故と影響

当社は、鳥取県で FA 機器の設計・製造を行う企業である。取引先とは日常的に CAD データをメールでやり取りしており、CAD データは会社の重要な資産であると認識している。数年前、ウイルスに感染したことがあったが、幸い被害は確認されていない。

■ 事故の要因

事故が発生するまで、ウイルス対策を何も行っていなかった。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | **技術的**

- 社外にウイルス感染で迷惑をかけることのないよう、ウイルス対策としてインターネットサービスプロバイダーのメール監視サービスに加入し、迷惑メールのフィルタリングやウイルスチェックを行っている。また最近、取引があるシステムベンダの営業担当者から、ウイルス対策ソフトの導入を提案された。その必要性を感じたので、近日中に導入する予定である。
- 業務用のデータは NAS で共有しており、それをミラーリングしてバックアップしている。
- 古い CAD ソフトを使い続ける都合上、サポートが終了した Windows XP のパソコンが 3 台残っており、この点はリスクを懸念している。
- 特別な従業員教育はしていないが、怪しいウェブサイトを会社で見るようなことはなく、それなりのモラルは保たれていると思う。また、個人のパソコンを業務に使うことはないが、USB メモリなどは個人の持ち物を利用することはある。パスワードなどのセキュリティ管理は弱く、パソコンが誰でも使える状態であることが多い。

■ 取り組みによる効果

以前はウイルス感染や迷惑メールが多い状態にあったが、現在では迷惑メールはほとんどがフィルタリングされ、最近になってウイルス感染被害は出ておらず、その他にも直接的なセキュリティ問題は発生していない。従業員について、最低限のモラルは保たれているとはいえ、セキュリティ意識はまだ高くはない。パソコンや業務ソフトがパスワードなしで使えたり、メールでファイル送信するとき暗号化されていなかったりすることがある。

■ 情報セキュリティ担当者の視点

セキュリティ対策は高いレベルを目指すときりがないので、当社の規模の場合にどの程度が妥当か、見極めが重要である。メールでデータを送るときに暗号化したり、個人所有の USB メモリの使用を禁止したりするなど、低コストでできるセキュリティ対策は実施したい。また、紙ファイルも机上に放置することをやめさせるなど、パソコンに限らずセキュリティ意識を高めたい。また、古い CAD を入れ替えて、Windows XP を使わない状態を早く実現したい。将来的には Windows 7 についても同様の問題が予想され、投資が必要となるのは経営者として困ることではあるが、毎年少しずつ新しい機種に更新しておくなど、負担を分散するようにしたい。いずれにせよ、システム活用は当社にとって重要な要素なので、社会的に見て妥当なセキュリティ状態が保たれるよう、努力を続けたい。

事例 8

所在地	東京都
業種	情報通信業
従業員規模	5 名以下
事故の有無	有(2010 年)
ケース	不正アクセス

利便性向上のためのセキュリティ強度の緩和により不正アクセスの影響を受けた。その後のセキュリティ対策の継続的な実施が顧客から評価されている。

■ 発生した事故と影響

当社は、東京都でキャリアの公式サイトの開発と運用を手掛け、ホスティングサービスを提供している。2010 年頃からスマートフォンの普及により、多様な端末からの公式サイトへのアクセスを可能にし、当社が手掛けるサービスも幅広い端末で利用できるようするために、アクセス制御を緩め、パソコンからのアクセスも許可する必要があった。同時にパソコンによる SQL インジェクション、DoS・DDoS 攻撃など不正アクセスが目立つようになってきた。これらの攻撃により、ネットワークや CPU やメモリなどの資源が占有され、サービスに支障をきたし始めた。

■ 事故の要因

利便性向上を推進する中で、アクセス制御などセキュリティ強度を意図的に緩めたことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | **技術的**

- 運用環境（インターネットサーバサービス）に関しては、①メールサーバや DNS サービスなどサービス毎の設定やパラメータの見直し、②サービスやプロトコル毎、国や地域別 IP アドレスブロック毎のアクセス制御や URI フィルタリング、③コンソールログの常時監視、④アクセスログの保存と解析を行っている。通常と異なる挙動を見つけた場合は、個別にフィルタリングルールを設定している。過剰にフィルタリングしてしまうことで、必要な通信が行えなくなりサービスが提供できない副作用が生じているが、都度調整しながら対応している。
- 開発環境（デスクトップ）に関しては、開発するアプリケーションの仕様などの制限のため、Java 等のソフトウェア製品を最新のバージョンにすることができない事情がある。そこでエンドポイントセキュリティ製品を導入し、ウイルスの侵入や意図しない外部との通信などを監視することで安全を確保している。

■ 取り組みによる効果

インターネットに常時接続されているサーバについては、常時攻撃を受けている状態にあるもの、フィルタリング等の対策により過負荷に陥ることなく安定的に運用できている。これまでのところ、外部からの攻撃に起因する、運用中のサービスの停止や、預かっている機密情報の漏えいなど、重大事故は発生していない。こうした取り組みが、携帯電話キャリア各社から評価され継続的な取引につながっている。

■ 経営者の視点

情報セキュリティ対策を継続的に行っていることが企業の信用につながると考える。当社はごく小規模な企業のため大がかりな設備投資は難しい。運用環境には、現状のネットワーク構成や機器配置を変更することなく導入できる透過型のファイアウォールを設置する。ログなどの稼働情報から動的にフィルタリングルールを作成し適用するプログラムを開発し、セキュリティ管理の負担を軽くしたい。また、サーバは長期使用する固定資産であり、稼働させる OS はセキュリティを維持しながら長期（10 年以上）運用が可能なプロダクトを選ぶ必要があることを痛感している。セキュリティも考慮しながら IT の導入・活用を進めていきたい。

事例 9

所在地	東京都
業種	情報通信業
従業員規模	101～300 名
事故の有無	有(2000 年)
ケース	ウイルス感染

ウイルス感染で数日間、業務が停止
全社的な情報セキュリティレベルの向上と均一化に取り組む

■ 発生した事故と影響

当社は、東京都に本社を置く医療情報システムの導入・開発業務を中心とした SI サービス企業である。2000 年頃、社内のパソコンやサーバがコンピュータウイルス「Nimda」に感染する被害に遭遇した。復旧のために徹夜で対応したが、数日間の業務停止状態に陥った。その間の会社としての被害額は、推計で数千万円に上る。

■ 事故の要因

被害が発生するまで、セキュリティ対策ソフトを全く導入していなかった。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 情報セキュリティ対策の必要性を認識し、現在に至るまで、順次対策を導入していった。具体的には、ウイルス対策、暗号化ソフト、インベントリ収集ツールの導入などの技術的な対策と、情報セキュリティに関する社内規則の制定、プライバシーマークや ISMS の取得など、運用面での対策に取り組んだ。
- 事業拠点の増加に伴い、会社全体として情報セキュリティ対策の水準を維持することが難しくなったため、各拠点で情報セキュリティ担当者を育成した。IT 関連の教育は社内で実施し、情報セキュリティ関連のスキル取得推進のため、受験料補助や合格祝い金の支給を行っている。また、3ヶ月毎に各拠点の担当者が集まって情報セキュリティ委員会を開催し、現状や悩み、好事例を共有することで、会社としての情報セキュリティ対策の均一化、向上を図っている。また、ISMS の内部監査では、ある拠点の情報セキュリティ担当者が別の拠点を見ることで、監査する側・される側の視点を養い、情報セキュリティに関する意識を高めている。
- 情報セキュリティ関連の知識や活動指針、内容をまとめた「情報セキュリティハンドブック」を作成し、従業員全員と協力会社に配付している。この内容をもとに毎年テストを実施し、基準点に満たない場合、補講への出席や再受験が義務付けられている。

■ 取り組みによる効果

- 以前は、規則により従業員の業務活動を強制的に縛っていた。従業員からは、作業がしにくいといった反発もあったが、従業員の情報セキュリティに対する意識が高まり、現在では従業員にある程度判断を任せられるようになった。
- 顧客や取引先からの要請もあり、情報セキュリティ対策に取り組んでいる面もある。顧客や取引先の情報セキュリティに関する要求水準を満たすことができており、現在も案件を受注することができている。

■ 情報セキュリティ担当者の視点

情報セキュリティ対策を進めるには、経営層の理解が一番重要である。当社の経営層は理解を示す一方、取り組みの費用対効果を意識し、情報セキュリティに関する作業の効率化や費用の圧縮を求める。そのため、担当者には会社の身の丈に合った対策とはどのようなものかの見極めが求められる。また、情報セキュリティは従業員一人ひとりの意識にかかっているため、従業員のリスク意識やモラルのさらなる向上のための継続的教育が必要である。特に、ウイルス被害の経験がない従業員のリスク意識向上のための教育をどのように行っていくかが課題である。

事例 10

所在地	東京都
業種	情報通信業
従業員規模	101～300 名
事故の有無	有(2011 年)
ケース	パソコン紛失

セキュリティ規程の整備や従業員教育により、ビジネスの品質やレベルが向上し、新たな仕事の受注につながる

■ 発生した事故と影響

当社は、東京都で顧客のアフターメンテナンスサービスを受託して、ハードウェア・ソフトウェアの保守・運用サービスの提供のほか、情報系のコンサルティングやネットワーク構築・設計サービスを提供している。2011 年、顧客情報の入ったパソコンの紛失事故が発生した。情報漏えいなどの実害はなかったが、顧客に紛失の事実を伝え、その後信用を失うこととなった。

■ 事故の要因

利便性を重視し、持ち出しに関する明確なルールや手続き等がなく、また会社として情報セキュリティに対する意識が高くなかったため、パソコンを自由に持ち出せる環境であった。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- パソコンなどのデバイスの持ち出し規程や取扱規程、暗号化などの対策を進めた。また、会社支給の携帯電話については、遠隔操作により利用を制限することができるような取り組みを実施した。規程の策定やツールの導入だけでは不十分であるため、全社教育を実施し、従業員の情報セキュリティ意識の向上にも取り組んだ。
- セキュリティ規程には、基本方針や詳細手順の他に、責任者の任命、アクセス制限の明確化、守秘義務、機器・メール・インターネットの私的利用制限、機器等の取扱、破損、紛失に関する事項、紛失した際の届け出義務等を規定した。また、就業規則には、社内の情報セキュリティに関するルールから逸脱した場合の措置や具体的なケースについて規定している。

■ 取り組みによる効果

利便性が低くなったという声はあるが、従業員の情報セキュリティに対する意識が高まったことは実感している。また、顧客情報の取り扱い範囲の拡大や量の増大に伴い、規程の再整理や教育などの取り組みによって、ビジネスの品質やレベルが一段向上し、安心感が他社との差別化となり、新たな仕事の受注につながっている。

■ 情報セキュリティ担当者の視点

顧客から受託してサービスを行っている以上、顧客からの「信頼」は何物にも代え難いので、情報セキュリティ対策に対する最低限の投資は必要と考えている。過去の事故経験から、経営層も同様の考え方を持っている。また、情報セキュリティは、従業員一人ひとりの意識にかかっているため、従業員のリスク意識やモラルのさらなる向上のために継続した教育を実施し、意識レベルを維持し、情報漏えいを発生させないようにしたい。予算やリソースに限りがあるため、万全な対策ができているとは言えないが、ある程度の対策は実施していると認識している。他社がどの位対策されているのか、当社は本来求められる情報セキュリティ対策レベルを満たせているのか、どこまでやれば十分なのか留意し、対策を進めていきたい。

事例 11

所在地	京都府
業種	情報通信業
従業員規模	101～300 名
事故の有無	有(2003 年)
ケース	ウイルス感染 標的型攻撃

グループ企業内で複数回のセキュリティ事故を経験
その後、グループ全社で様々な取り組みを実施

■ 発生した事故と影響

当社は、京都府に本社を置き情報システム企業の子会社としてグループ企業全体の SI サービスを展開している。2003 年頃、親会社でメールの添付ファイルからウイルスに感染し、復旧に多くの時間がかかった。また、標的型攻撃によりこれまで 6 回ほどデータ改ざんなどの被害に遭っている。こうした被害をきっかけに、全国の拠点にウイルス対策ソフトを導入したが、2010 年頃にある会社からセキュリティ対策ソフトのライセンス購入に関して不正があると指摘され、セキュリティ対策ソフトのライセンス数の確認と導入の徹底を行った。

■ 事故の要因

当時はウイルス対策ソフトを導入していなかったほか、従業員の情報セキュリティ対策に関する意識も十分ではなかった。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- グループ全社のセキュリティポリシーを設定し、ISMS の認証を取得した。
- オンプレミスのメールやスケジュール管理をクラウド上に移行して、よりセキュリティ対策の強化を図りつつある。
- スマートフォンやタブレットがグループ全体で約 2,000 台あるため、MDM（Mobile Device Management）ツールを導入して、リモートワイプ（遠隔消去）できる環境を整えている。
- USB メモリの運用規程を作成した。親会社のサービスマンによる USB メモリの社外持ち出し時及び返却時に必ずウイルススキャンチェックを実施しノートに記録する。
- 脆弱性診断ソフトを導入してセキュリティホール対策を行っている。また、添付ファイル付き標的型攻撃メールテストをグループ従業員向けに過去 9 回実施している。
- グループ全社から代表が集まり、1 回／半年セキュリティ対策実績と今後の方向性について会議を持っている。さらに国内グループでは e ラーニング教育を 2 ～ 3 回／年行っている。海外は自主性に任せている。

■ 取り組みによる効果

- 国内のセキュリティ管理で精一杯のため海外のセキュリティ管理までなかなか手が回らないが、クラウドへの移行に伴うウェブサイトの集約によって、標的型攻撃対策などの成果が出るものと思われる。
- グループ全社のセキュリティ会議や e ラーニングの徹底により、グループ従業員のセキュリティ意識は高まっている。
- ヘルプデスクがグループ全社のウイルス対策ソフトの導入展開、インシデント時の対応を行っており、現場からは感謝の声がある。

■ 情報セキュリティ担当者の視点

クラウドシステムを活用することで、全世界レベルで情報セキュリティ対策のレベル向上を図りたい。また製造業の技術情報などを狙った標的型攻撃などが考えられるため、セキュリティホールのチェックなどを徹底したい。取引先からのセキュリティ対策に関する各種アンケートでは今のところ問題は指摘されていないが、引き続き対策強化を図っていく。

事例 12

所在地	奈良県
業種	情報通信業
従業員規模	5 名以下
事故の有無	有(発生年不明)
ケース	不正アクセス

セキュリティ対策は、お金をかけなくてもできることをやること、人の教育が重要

■ 発生した事故と影響

当社は、奈良県でソフト開発・販売やパソコンを用いた職業訓練サービスの提供などを行っている。かつて電子メールの不正送信の踏み台にされたことがあり、自社の実害は生じていないものの、知らない間に攻撃の一端を担うこととなった。

■ 事故の要因

ウイルス対策ソフトの導入や OS・アプリケーションの定期的なアップデートが十分でない等、自社のメールサーバのセキュリティ管理が十分でなかったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 社外に設置している法人向けサービス用のサーバ等の情報セキュリティには細心の注意を払っており、陳腐化の影響を避けるため数年から 5 年毎に入れ替えを行っているほか、情報セキュリティ対応をしっかり行えるようにしている。社内のコンピュータネットワークについては、各パソコンにウイルス対策・不正使用対策ソフトを導入するとともに、全メールの内容を一定期間、サーバに保管している。
- 当社では、パソコンの利用者を経営者、経理事務担当、正従業員、生徒・一般利用者の各グループに分類し、アカウント毎に権限を設定している。また事務所内の机とパソコンの物理的な配置についても、意図せずにパソコンモニタの内容が部外者の目に入ることを避けるため、十分な配慮を行っている。

■ 取り組みによる効果

情報セキュリティ対策は、それをすることで目に見えて利益率が向上するものでも、生産性が向上するものでもないことは重々承知しており、保険的な必要経費と捉えているが、情報セキュリティ対策を積極的に行っていることが顧客の心情にプラスに働いている。当社の事業の特徴は「口コミ」であり、既存顧客のリピート注文や、既存顧客からの口コミによる新規顧客からの注文により成り立っている。そのため当社にとって最も大事なのは「信頼」であり、情報セキュリティ対策をしっかり行っていることを顧客に知っていただくことは大きなメリットとなっている。

■ 情報セキュリティ担当者の視点

情報セキュリティについて当社が重要であると考えていることは、第一に「お金をかけなくてもできることはやっておく」ということである。従業員へは「メールのリンクは踏むな・・・いつもの手順でたどれ」「たとえ銀行や有名な企業らしきところからのメールであっても安易に開くな」と伝えてあり、「何か困った時、トラブルが発生した時には焦るな」と伝えている。不測のトラブルは人で回避できることも多いため、情報セキュリティ対策は「教育」が最も大事と考えている。クラウドサービス・シンクライアントなどが普及していくにつれ、ネットワーク全体の監視が重要になってくる。将来的には、ネットワーク全体を集中監視する専用機器を導入した情報セキュリティ対策に切り替えていきたい。

事例 13

所在地	秋田県
業種	運輸業
従業員規模	21～50 名
事故の有無	有(発生年不明)
ケース	標的型攻撃

中小企業も標的型攻撃の対象となることを認識し、セキュリティ対策の取り組みを開始

■ 発生した事故と影響

当社は、秋田県で引越しに伴う運送のほか、米・建材などを中心とした輸送を生業としている物流企業である。取引先とのやり取りが紙・FAX から電子データを利用するようになり、電子メールでやり取りをする量が多くなってきた。そうした中、業務に関係のないメールの添付ファイルを社長が開けてしまったことがある。明確なセキュリティ被害はなかったが、中小企業でも標的型攻撃の対象になることを認識し、対策に取り組むこととなった。特に取引先との情報が外部に漏えいすることが一番の危機と感じている。

■ 事故の要因

メールフィルタリングツールを導入していないことに加え、不審メールを受信した際の対処方法を詳しく知らなかったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | **技術的**

- 使用しているパソコン 7 台、サーバ 1 台のすべてに対して、ファイアウォール、不正侵入防御対策、ウイルス対策ソフト、スパムメール対策、Web 閲覧制限などのセキュリティ対策を行った。
- 教育や規程などの IT 以外のセキュリティ対策は一般的なもの（書類の保管等）のみであり、セキュリティ対策に関する計画的な取り組みは行われていない。
- IT 関係のセキュリティ対策は、取引しているベンダに相談し、アドバイスを受けて導入している。

■ 取り組みによる効果

被害に直面したことがないので普段はセキュリティリスクを意識することがないが、たまにインターネットを閲覧している時に、ウェブフィルタリングで規制されている旨の表示を見ることがあり、そのような時に身の回りにセキュリティリスクが存在することに気付く。こうしたことが、セキュリティ対策の取り組みの効果であると感じている。

■ 情報セキュリティ担当者の視点

セキュリティ対策は取引している IT ベンダに任せており、導入している対策で十分と思っていたが、IPA から提供されている「新・5 分でできる！情報セキュリティ自社診断シート」の結果を見ると、まだまだ不十分と感じた。また、セキュリティに関して直接被害を受けたことがないので、セキュリティ対策に関する従業員の意識が低いと感じられる。現在取引しているベンダに相談し、セキュリティ対策や従業員の情報セキュリティに対する意識の向上に向けた取り組みを検討したい。しかし、本業でないところに、コストがかかることがセキュリティ対策への一つの障壁と考えている。

事例 14

所在地	宮崎県
業種	運輸業
従業員規模	101～300 名
事故の有無	有(発生年不明)
ケース	不正アクセス

自社のウェブサイト改ざんをきっかけにセキュリティ被害を身近に感じ、セキュリティ対策を強化

■ 発生した事故と影響

当社は、宮崎県でバス・タクシー事業を中心とした運輸業を営んでいる。ウェブサイトや電子メールのサーバを社内に置いているが、ウェブサイトの一部が改ざんされ、意図しない有害サイトへ誘導される事案が発生した。機密情報などを扱うサーバではなかったため、実害はなかったが、自社内で実際に発生したため、セキュリティ被害は身近なものであると感じた。また、ウイルス添付メールも日常的に捕捉されているが、ウイルス対策ソフトが機能しており事故にはつながっていない。今後、これらをきっかけとして、ハード面、ソフト面、そして従業員のさらなるリテラシーの向上の取り組みを進めていく予定である。

■ 事故の要因

CMS（Contents Management System）の脆弱性を攻撃されたことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 業務上、メール送受信やインターネット利用の頻度が高いため、定期的に従業員に対して、IT だけではなく、セキュリティ全般についての啓蒙をしている。
- 現在、ファイアウォールの強化を優先的に取り組んでいる。外部の業者に管理を委託しているサーバや、自社内にあるサーバに対して、本社、拠点、グループ会社がアクセスするため、VPN 等の適切なアクセス手段を用意しており、メールの監視、ウェブアクセスのフィルタリングなども一元的に管理できるファイアウォールの導入により、日々の監視業務の効率化も図ることを推進している。

■ 取り組みによる効果

普段から、情報セキュリティ対策に関する啓蒙を行うなどして、従業員のセキュリティに対する意識は高まっていると感じている。ハード、ソフト面での取り組みは未着手の状態なので、効果を評価することはできないが、今後、優先順位をつけて対策をする予定としている。

■ 情報セキュリティ担当者の視点

現在のところ、具体的な対策はこれからの状態であるが、監視業務をできるだけ自動化することで精度向上と省力化を図っていきたいと考えている。省力化できた分は、他の業務に振り向けることで、これまで対策ができていなかった部分の強化を図っていきたいと考えている。そのためには、リスクの大きさを及び費用対効果を見極めた上で、経営層への理解を促していくことが、これからの情報セキュリティ担当者としての役割だと考えている。また、従業員に対しては、ウイルスメールの取り扱い、インターネットの適正利用、情報漏えい防止についての意識向上を図り、インシデント発生時の手順などもマニュアル化し、徹底させることで、人的要因による事故発生のリスクを軽減させていきたい。グループ会社間で意識の差があるが、情報セキュリティ担当者として、属人的でない、グループ全体としてのセキュリティへの意識向上を促していきたいと考えている。

事例 15

所在地	富山県
業種	卸売業
従業員規模	51～100 名
事故の有無	有(2016 年)
ケース	ウイルス感染

安心して業務に取り組める環境を目指す従業員の意識向上のため継続的な従業員教育の実施と理解度を繰り返し確認

■ 発生した事故と影響

当社は、富山県で工業用ゴム製品の販売やきめ細かなサービスを顧客に提供する専門商社として事業を展開している。業務でパソコンを使うのが当たり前であり、ニュースなどで情報セキュリティに関する事故なども目にしており、関心を持っていた。2016 年、ランサムウェアに関する記事が新聞に掲載されていて、ますます関心度を深めていた中、パソコン 1 台がウイルス感染して使えなくなり、初期化し、再設定をせざるを得ない状況が発生した。被害が拡大しなかったのが不幸中の幸いであったが、これまで以上に情報セキュリティの必要性を認識した。

■ 事故の要因

従業員の情報セキュリティに関する意識が不十分であったことが原因と考えられる。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 業務システムを委託しているベンダに、メールなどのセキュリティ対策を依頼し、ウイルス対策ソフトの活用や、ファイアウォールの導入など、ハード面からの対応を順次とっていた。また、事故の例や、注視すべき事項（メールの扱い方や、事故があった時の連絡体制など）を、適宜、従業員へ周知している。
- 今回、新たに別のベンダに依頼し、メールのテスト・サービスを実施した。その結果、安易にメールを開いてしまう従業員が想定以上に多く、ソフト面での対応の重要性が認識できた。また、これに合わせて、現在のセキュリティレベルも再確認でき、高いレベルであることが認識できた。ただし、メールについては、本来は届くべきものが届かないという場合もあり、引き続き運用条件を検討していく。

■ 取り組みによる効果

事故があった場合の連絡方法・ルートなどについて、繰り返し、従業員に周知してきたことで、事故（パソコン 1 台のウイルス感染）の時も拡散を防ぐことができ、慌てずにベンダの協力のもと対応できた。一定のレベルで従業員における意識付けができていると感じている。

■ 情報セキュリティ担当者の視点

メール・テストサービスを利用したことで、新たに課題や経営と現場とのリスクに対する認識の違いが大きいことが明確になった。顧客情報等の情報資産に対する従業員の意識をより一層高めるため従業員教育を継続的に実施し、適宜、理解度の確認を繰り返しながら、安心して業務に取り組んでいけるようにしていきたい。また、ウェブサービスの利用という観点では、インターネットバンキングのリスクを認識し、それぞれの金融機関のサービスレベルに合わせて、ワンタイムパスワードの利用、総合振込のみでの利用などの対応をとっていきたい。

今後もベンダ等から、随時、セキュリティに関する情報・提案を受け、順次対応をとっていく。また、自社内の取り組みを発信し、顧客へもセキュリティ意識の浸透を図っていくことで、相互に安心できる環境を作っていきたい。

事例 16

所在地	山梨県
業種	卸売業
従業員規模	6～20 名
事故の有無	有(2016 年)
ケース	ウイルス感染

顧客への影響を考慮して外部要因に対するセキュリティ対策を強化、外部接続システムの対策を優先

■ 発生した事故と影響

当社は、山梨県で建築金物などの卸売業を営む企業である。2016 年中頃、業務で使用しているパソコンがウイルスに感染した。顧客への被害はなく、復旧作業にもそれほど時間を要しなかったが、顧客への連絡や社内対策などの作業負荷、ネットワークの遅延、システムの性能低下などの影響があった。

■ 事故の要因

ウイルス感染を意図した外部からのメール等を誤って開封してしまったことによるものと推測される。

■ 事故後の取り組み

組織的 | 人的 | **物理的** | **技術的**

- 対策の実施にあたっては、ウイルス感染被害があった場合の顧客への影響度を中心に、外部要因に対するセキュリティ機能の強化を実施した。当社では従来 2 つのシステムを運用しており、財務・販売・給与関係のシステムは外部と接続していないことから、外部の脅威の影響を受けないため事故後も対策を変更していない。
- インターネットを活用したシステムに力点を置きセキュリティに関する設備投資を実施した。具体的には、数年前から使用しているインターネットとの接続機器を、現状より機能を強化した新規機器に交換し、ウェブ閲覧・電子メールに対するフィルタリング機能を強化した。
- 自社ウェブサイトには取扱商品、顧客からの相談窓口、アクセスマップなどの機能を持たせており、不正アクセス監視機能を強化した。また、ウイルス対策ソフトを当社で使用している各パソコンにインストールした。その他、パソコンのユーザ管理を実施しており、一般ユーザは新規ソフトウェアのインストールはできない。

■ 取り組みによる効果

現在まで、ウイルス感染やシステムの性能低下を原因とする顧客からの苦情や業務上の被害は発生していない。不審な添付ファイル付き SPAM メールは依然として受信しており、正しいメールとの区別に難儀している。しかし、取り組みにより脅威が顕在化していないものとみなし、対策の効果ありと判断している。

■ 経営者の視点

現状の情報セキュリティ対策はまだ不十分と考えているが、リスクに対して何をどこまで対策するのかの判断が難しい。脅威や直接的なリスクを感じた場合に、費用と効果のバランスで判断することになる。当社では情報システムの運用・管理を経営者が担当している。今後、社会がさらなる IT 化へと変化する中で、当社従業員に対しても、IT リテラシー教育を行う必要を感じている。社会の趨勢もあり、当社でもタブレット等を使用し始めているため、MDM(Mobile Device Management)の導入を検討する時期が来ていると考える。
自社ウェブサイトに対する不正なアクセスについては、今後の技術の向上に伴い、さらなるセキュアなプログラミングにより自社への脅威を可能な限り排除する対策が必要になると予想している。

事例 17

所在地	滋賀県
業種	卸売業
従業員規模	6～20 名
事故の有無	有(2015 年)
ケース	ランサムウェア

個人任せの対応から組織的な情報管理へ転換
クラウドシステムの導入で運用面の改善に取り組む

■ 発生した事故と影響

当社は、滋賀県に本社を置く汎用ガソリンエンジンや同搭載製品等の輸入・販売・アフターサービスを行う卸売業者である。2004 年の創業以来、ウイルス対策ソフトやファイアウォールなどのセキュリティ対策を行なってきた。しかし 2015 年末頃、「ランサムウェア」に感染し、共有フォルダ内のいくつかの PDF ファイルが暗号化されてしまった。結局、そのファイルを削除し、紙ベースで管理していた情報をスキャナーで読み込んで復元した。販売店との契約書や従業員情報等があったが情報量としてはあまり多くないので、何とか復元でき、事なきを得た。

■ 事故の要因

ランサムウェアが仕組まれたメールの添付ファイルを、従業員が不注意で開封してしまったことによる感染。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 全従業員向け e ラーニングによるセキュリティ教育を親会社からの共通の施策として実施した。
- 従来、重要データのバックアップは定期的に行っている。今後、BCP の観点からバックアップデータの遠隔地での管理を考えたい。
- 共有フォルダにアクセス可能な ID とパスワードを設定するなどのアクセス権限を設けた。
- 全国各地の営業マンが、パソコンや固定ディスクに名刺等の顧客情報を入れて持ち歩いている。ログイン時の ID、パスワードは管理されているが、それ以外は個人任せとなっており、顧客情報である名刺管理が課題となっていた。
  2016 年にクラウドの名刺管理システムを導入したことにより、営業マンは名刺をスキャナーやスマートフォンからアップロードできるようになり、どこからでもアクセスできてセキュリティ上も安全なシステムとなっている。

■ 取り組みによる効果

- セキュリティトラブル以降、e ラーニングによる教育などにより従業員のセキュリティ対策意識は向上している。
- 名刺管理のクラウドシステム導入は、営業マンからは便利で安全になったと評判が良く、効果を感じている。

■ 情報セキュリティ担当者の視点

経営者もセキュリティ対策には関心を持っており、営業、スタッフも任されているという意識は高い。名刺管理のほか、今後もクラウドシステムなどいろいろな形でのセキュリティ運用の改善を講じたい。ただ、どこまでセキュリティ対策をやれば良いか、専門家がいないので分からない。適切な専門家がいれば指導を受けたいと思っている。

事例 18

所在地	福岡県
業種	卸売業
従業員規模	6～20 名
事故の有無	有(2010 年)
ケース	ウイルス感染

ウイルス対策ソフトの更新手続きミスでトロイの木馬に感染
安心して働ける職場環境作りに積極投資

■ 発生した事故と影響

当社は、福岡県北部で菓子・パン類等の食料品を取り扱う商社である。2010 年、1 台のパソコンが突然動かなくなった。調査したところ、「トロイの木馬」に感染していることが判明し、急きょアプリケーションの停止とネットワークからの切り離しを行った。自社で OS の再インストールを行うなどリカバリーを行ったが、完全な復旧までに 2 ヶ月を要した。

■ 事故の要因

ウイルス対策ソフトの契約更新期間中に入金手続きが行えず、数日間サポートが切れた状態にあった。そのわずかの間にインターネットにつながっていたパソコンがウイルスに感染した。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 情報セキュリティに関するマニュアル（セキュリティポリシー、パスワードの設定、メールの送受信、バックアップ、ハードディスクの破棄ルールなど）を作成し、社内で定期的に勉強会を実施している。
- サーバとパソコンは社内 LAN でつなぎ、パソコン毎に役割を決め、アクセス制限をかけてリスク分散を図っている。販売管理システムは機密性が高いデータを保有していることからインターネット、社内 LAN から完全に切り離し、情報漏えいが起きないようできる限りのセキュリティ対策に取り組んでいる。そのほか、USB メモリの暗号化、パスワード保護の徹底、ウイルス対策ソフトによるウイルス侵入・感染防止などを行っている。インターネットバンキングについても、取引先の各銀行から指導を受け、さらなるセキュリティ対策レベルの向上に努めている。

■ 取り組みによる効果

幹部会では、常にセキュリティ関連情報を共有し、経営陣の理解を得ている。経営者自身が情報セキュリティの重要性を十分に認識することで、投資も進めてきた。そのため、従業員が安心して仕事に取り組める環境ができている。企業経営において、取引先に迷惑をかけないことは当然の責務であり、システムがスムーズに動き、トラブルを起こさないことが重要である。これまで大きな被害にあうことなく、顧客対応ができていることで、取引先との強い信頼関係構築につながっていると考えている。

■ 情報セキュリティ担当者の視点

日本は海外からのウイルス攻撃に常にさらされ、目に見えない恐怖がある。日本国中がインターネットでつながっており、社会全体で対策を打たなければ、被害は連鎖していくだろう。そのような中で最も重要なことは、経営者の意識を変えていくことだと考えている。「自社だけは大丈夫」という楽観的な考え方は危険であり、ウイルスに感染してからでは手遅れとなり、取引先に迷惑をかけ、社会的信用をなくす。最悪の場合は、倒産にもなりかねない。セキュリティ対策のためには、ある程度の金銭的投資が必要だが、決裁権を持つ経営者がリーダーシップを発揮し、対策を推進するべきだろう。
当社では、過去に従業員の USB メモリからもウイルスが見つかっている。侵入経路を断つためにも、従業員の情報セキュリティ教育をもっと強化していくつもりである。今後は、机の上の整理や書庫への保管、パソコンのロック機能の利用などにも徹底して取り組んでいく予定である。

事例 19

所在地	福島県
業種	小売業
従業員規模	6～20 名
事故の有無	有(2015 年)
ケース	ウイルス感染

ウェブサイトの閲覧でウイルス感染
信用を守るためにセキュリティ対策の強化を図る

■ 発生した事故と影響

当社は、福島県内に 4 店舗を展開する和洋菓子店である。2015 年中頃、普段使用しているパソコン画面が突然動かなくなるなど、これまでに経験したことのない妙な動作をするようになった。ウイルス対策ソフトを入れているのでウイルスに感染したなどとは思っていなかったが、日頃からパソコンや FAX 等の管理を依頼している地元のシステム会社にメンテナンスを依頼し確認をしてもらったところ、ウイルスに感染していることがわかった。

■ 事故の要因

通常、社内でパソコンを操作する担当者は 1 名のみであり、オフィスアプリケーションの操作と電子メールの送受信の利用がほとんどであった。また、社外のウェブサイトを閲覧することはあまりないため、ウイルス対策ソフトだけで十分と考えていたが、今回の侵入経路はウェブサイト経由の可能性があるとアドバイスを受けた。

■ 事故後の取り組み

組織的 | 人的 | **物理的** | **技術的**

- 顧客に電子メールを出す際にウイルス感染したもの送ることは許されないので、パソコン等のエンドポイントから電子メールサーバまで監視できるソリューションを採用した。月額 9,000 円の負担となり、小規模事業者にとっては決して安くはないが、信用には代えられないと考えた。
- 顧客の情報が入ったパソコンからは電子メールの送受信ができないように設定している。
- USB メモリの使用についても、使用者は一人に限っており、紛失しないように留意している。

■ 取り組みによる効果

- 新しいソリューションを採用した後から現在に至るまでは、新たにウイルスに感染することなくパソコンを使用することができている。
- 対策として必要なことを実施したことで一定の効果も得られたと考えており、今のところ安堵している。

■ 経営者の視点

今やコンピュータやインターネットの利活用は会社経営において必要なものであることは間違いない。そして安全に使うためにも、ランサムウェアの被害などの情報もあることから今後も最新の情報を収集するように努めたい。
社内の運用としては、万が一またランサムウェアなどによる被害にあった時のために、定期的なデータのバックアップを行うことを習慣化するようにしていきたい。情報セキュリティを確保するための対策は中小企業の経営者一人での対応には限界がある。そのためにもすぐに駆けつけてきてくれる地元の信頼できるパートナーとの連携が重要であると考える。

事例 20

所在地	福井県
業種	小売業
従業員規模	101～300 名
事故の有無	有(2016 年)
ケース	標的型攻撃

個人情報漏えい対策費用が数千万円に上ることが予想され、セキュリティ対策を強化

■ 発生した事故と影響

当社は、福井県で印刷やノベルティ品、オフィスサプライ品のネット通販を行っている。プライバシーマークを取得し、情報セキュリティ対策を推進していたにも関わらず、2016 年中頃、標的型攻撃メールによってコンピュータウイルスに感染する事案が発生した。情報漏えい等の実害はなかったが、当社で個人情報の漏えいが起きた場合、その対策費用は数千万円に上るおそれがあることが分かったため、情報セキュリティ対策のさらなる強化を図った。

■ 事故の要因

メールフィルタリングツールを導入していないことに加え、不審メールを受信した際の対処方法を詳しく知らなかったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- ウイルス対策ソフトの強化として、これまで使っていたウイルス対策ソフトより強固な機能を持つソフトに変更した。これにより、ウイルス付きの添付ファイルだけでなく、怪しいと思われる添付ファイルも駆除することが可能になった。
- 個人情報を扱っているパソコンの使用制限を強化するために、静脈認証装置を取り付け、静脈認証情報をあらかじめ登録した従業員だけがパソコンを操作できるように変更した。
- セキュリティに関するテストを実施するなど、セキュリティ教育を継続的に実施している。また、標的型攻撃メールへの対応として、ダミーメールによるテストを実施した。

■ 取り組みによる効果

プライバシーマーク取得による効果として、取引先の信頼が高まり、受注増につながっている。また、ウイルス対策ソフトの強化による効果として、怪しいメールの駆除が毎日のように発生しており、水際でブロックしている。ただし、取引先からの正常なメールもブロックしてしまい迷惑をかけることもあったが、説明して理解をいただき、ブロックされない形でメールを送っていただくように変更してもらった。また、従業員教育による効果として、情報セキュリティに対する従業員の意識が向上している。しかし、標的型攻撃メールのダミーテストでは、90%の従業員が開封しており、教育のさらなる徹底が必要である。

■ 情報セキュリティ担当者の視点

ソフトウェアのバージョン管理や USB メモリの使用制限、操作ログの管理など、セキュリティ対策をさらに強化するために IT 資産管理ソフトの導入を検討している。こうしたソフトを導入することで、従業員に対するけん制も働くのではと期待している。一方、技術的な対策には限界もあるため、情報セキュリティに対する従業員教育をさらに徹底することが課題である。現在は年に一度しか行っていない教育の回数を増やして意識の低下を防ぐことや、情報システム担当者だけで教育を実施するのは負担が大きいため、情報セキュリティ委員会を設置して各部署に委員を配置し、日頃から情報セキュリティの啓発活動を行えるような仕組みも検討している。

事例 21

所在地	滋賀県
業種	小売業
従業員規模	21～50 名
事故の有無	有(2003 年)
ケース	ウイルス感染

自動車メーカー提供のディーラー向けウェブクラウドシステムの利用、セキュリティポリシーの徹底により、高い情報セキュリティレベルのビジネス環境を実現

■ 発生した事故と影響

当社は、滋賀県の地場の自動車ディーラーであり、自動車メーカーとの資本関係はない。従来は自社のシステムを利用していたが、2003 年以降は全面的に自動車メーカーのディーラー向けウェブクラウドシステムを利用するよう切り替えた。電子メールもセキュリティ関連ソフトも全面的にそのシステムが提供するものを利用している。2003 年までは、電子メールの添付ファイルによるウイルス感染が発生したことはあったが、ウェブクラウドシステムを利用してからは生じていない。

■ 事故の要因

自社でシステム全般を管理していた際、ウイルス対策ソフトやメールのフィルタリングソフトの導入が不十分であったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 取引の関係上、自動車メーカーが求めるセキュリティポリシーが徹底されており、また顧客情報を扱うこともあって従業員の情報セキュリティに関する意識は高くなった。自動車メーカーの掲示板等で情報セキュリティ対策に関する指示がなされると、それをもとに当社のセキュリティ責任者が自社の店舗に対策の指示と徹底を伝えている。社内では紙媒体の顧客情報も管理しているが、夜間には店舗の警備体制が機能しており、防犯カメラも設置されているなど、情報管理に関する情報セキュリティ対策のレベルは高いと考えている。
- ディーラー向けウェブクラウドシステムを利用するとパソコンにはデータが残らないが、パソコンや USB メモリの社外への持ち出しを禁止することで情報漏えい対策を徹底している。ウェブクラウドシステムで電子メールを参照する場合、システムが不審メールと判定した電子メールの添付ファイルを開くことはできない。
- 情報システムの運用に関しては、IT ベンダと保守契約を結んでおり、IT 運用上の不都合が生じた場合に対応してもらっている。また、自動車メーカー指定の各種セキュリティ保険にも加入している。

■ 取り組みによる効果

顧客と常に接し、顧客情報を扱うため従業員のセキュリティ意識は高く、社内指示も徹底しているためこれまでセキュリティに関するトラブルは生じていない。また、ウェブクラウドシステム導入によるセキュリティ上の効果も大きいと体感している。営業マンはタブレットを持っているが、個人情報はウェブクラウドシステム上にあり、セキュリティを保ちやすい。IT 面で課題があれば、保守契約会社の支援があり、安心してシステム運用を行うことができている。

■ 経営者の視点

地元県内のディーラーの会議（1 回／月）において、経営者間でセキュリティインシデントなどの情報交換を行っている。メーカーのセキュリティポリシーを共有しており、また各種情報機器の持ち出しを禁止しているため、セキュリティ対策はそれなりにできていると思う。今後は不用意に電子メールの添付ファイルを開かないなどの従業員教育を徹底していきたい。また、メーカーの情報部門や運用をお願いしている IT ベンダとも、定期的にセキュリティ関連の情報交換を行うことで、セキュリティ被害の未然防止に努めたいと考えている。

事例 22

所在地	東京都
業種	金融業
従業員規模	101～300 名
事故の有無	有(2014 年)
ケース	不正アクセス

ウェブサーバへの不正アクセス検出後、セキュリティ対策を一層強化し、その後のインシデントにおいて被害なし

■ 発生した事故と影響

当社は、東京都でグループ企業の資産運用を行っている。金融庁を監督官庁とする業態であり、発足当初よりグループのセキュリティ指針に則り対策を講じていた。2014 年 2 月に公開された IPA のセキュリティ情報に基づき、外部委託先の調査結果を踏まえ、ファイアウォールの脆弱性対策を講じる計画を進めていた折、ウェブサーバへの侵入が検出された。現象は負荷監視で検知し、対外遮断の仕組みが機能したことで実被害はなかったが、このインシデント発生以降、経営層も含めより一層の情報セキュリティ対策の取り組みを進めている。

■ 事故の要因

ウェブサーバ、ネットワークのセキュリティ対策が不十分であったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- ハード面の対策として、メールフィルタリング（ホワイトリスト併用）、誤送信対策、標的型攻撃対策、WAF（Web Application Firewall）、改ざん検知、プロセス監視やプリンタ操作ログ監視のほか、他社の事件を参考にスマートフォンの接続監視（禁止）なども追加実施し、社内外両面に対して技術的に想定される対策は講じている。
- ソフト面の対策として、半年毎の抜き打ち訓練実施、情報セキュリティ研修の開催（１回／年）、新入従業員・中途採用時の研修を実施してきたが、2014 年のインシデント発生以降は、情報セキュリティ研修の開催頻度を倍増（２回／年）し、特にインシデント発生時の緊急対応力の向上と徹底を図っている。
- 運用面での取り組みとして、電子媒体の持ち出し管理、社内保管物の棚卸し、USB メモリの使用禁止等を実施している。
- インフラ面の取り組みとして、社内システム毎のネットワーク系分離、個人／共有端末の分離を実施してきたが、徐々に追加対策をしたことでネットワークの系が複雑になっていた。事務所移転時にネットワークの再構築を行うことができ、これを機に最新方式によるモニタリング環境を構築し、管理面の効率も向上できた。

■ 取り組みによる効果

2015 年度に当社への脆弱性を狙った不正アクセスや SQL インジェクション、DoS 攻撃が仕掛けられたが、情報セキュリティ対策の効果により、被害は発生していない。対策導入効果として経営層にも報告しており、投資対効果の理解を得ている。

■ 情報セキュリティ担当者の視点

今後の追加対策として、従業員教育・研修を通じた、インシデント対応ほか情報セキュリティ対策ルールの確実な実施・定着化、サンドボックス運用による開封確認の導入、バナー対策（Java や Flash のバージョン管理）、ウイルス検知のほか社内モニタリング監視の実施、退社予定者に対する３ヶ月間のメール監査等を検討している。また様々な規約・ルール改定に関して、社内の情報セキュリティハンドブックへの反映を確実に実施したい。情報セキュリティ人材（社内・外部）の育成やノウハウ蓄積など、本業以外の体制の維持や必要リソース割り当てについて、身の丈にあった取組の評価・判定を継続的に検討していきたい。

事例 23

所在地	埼玉県
業種	不動産業
従業員規模	6～20 名
事故の有無	有(2017 年)
ケース	ランサムウェア

情報セキュリティ対策の取り組みにより従業員の意識向上、業務の効率化を実現

■ 発生した事故と影響

当社は、埼玉県でショッピングセンターの統合的な運営管理を展開している。顧客の個人情報、取引先との契約に係る情報などの重要情報を保持しており、顧客情報の漏えいによるブランドイメージの失墜や情報システムの停止による損失などの情報セキュリティ上のリスクは、当社にとって大きな被害や影響をもたらすと認識している。多くの場合、その被害や影響は取引先や顧客などの関係者へも波及することから、情報セキュリティ対策の必要性を認識し、現在に至るまで、順次対策を進めてきた。しかし、2017 年 1 月、社内のノートパソコンが「ランサムウェア」に感染した。ノートパソコンから感染していないデータのみをウイルスチェック可能なハードディスクにデータ 1 個ずつ確認しながら移行した。感染したノートパソコンは初期化してから廃棄（リース会社へ返却）する予定にしている。

■ 事故の要因

従業員の情報セキュリティに関する意識が不十分であったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- コスト的に可能な限りの物理的な対策、人的な対策、技術的な対策をおこなっている。具体的には、フロアや施設への入退出管理、書類などの施錠管理、情報機器や記録媒体の持ち込み・持ち出しの制限、ハードディスク等の廃棄時の破砕・溶融、ウイルス対策ソフト・サービスの導入である。
- 警備担当者に情報セキュリティ関連のスキルを習得させるほか、新人に対して入社当日に警備担当者が教育を行っている。

■ 取り組みによる効果

- 従業員の情報セキュリティに対する意識が向上した。日々の職務の中で情報セキュリティを意識した行動が定着している。
- 従業員のリスク管理の重要性に対する理解・認識が向上した。リスク管理の考え方が定着するにつれ、業務経験が浅い従業員も職場の潜在的なリスクを感じることができるようになった。
- 情報資産の見直しを図ることができた。情報資産を特定する過程で業務内容を精査することができ、業務の効率化が実現したことによる効果は大きい。

■ 情報セキュリティ担当者の視点

情報セキュリティを取り巻く環境は日々複雑化、高度化していることから、情報セキュリティ対策を定期的に見直せるような体制作りが重要であると感じている。情報セキュリティに対する意識は従業員個々にみると温度差があるので、今後は従業員への情報セキュリティ対策の実践教育に取り組んでいきたい。そのためには、情報セキュリティに関するリスクを分析して、当社にあったセキュリティのルールやガイドライン作りがかかせないと感じている。システム的には、重要なシステム・データのバックアップを講じていく予定である。

事例 24

所在地	東京都
業種	不動産業
従業員規模	5 名以下
事故の有無	有(2013 年)
ケース	ウイルス感染

ウイルス対策ソフトを導入しただけでは安心ではない紙ベースの業務形態を維持する方針

■ 発生した事故と影響

当社は、東京都で不動産賃貸・売買を中心に、分譲住宅や増改築・リフォームなどの事業を展開している。まだ Windows XP を使用していた頃、当時のプロバイダーからウイルスに感染しているおそれがあり、至急アップグレードするように連絡があった。ウイルス対策ソフトは導入していたが、状況が全くつかめず、急いで OS を入れ替えた。

■ 事故の要因

サポートの終了した OS を使っていたことが原因である。ウイルス対策ソフトを導入したからといって安心ではないということを実感した。

■ 事故後の取り組み

組織的 | 人的 | **物理的** | 技術的

- 不動産業として情報の取り扱いにはセンシティブであり、重要データはパソコンには一切保存せず、すべて紙媒体で施錠管理している。完了した案件については、スキャンデータとして CD や外付けハードディスクに記録・保管し、同様に施錠管理しており、外部に持ち出すことはない。外付けハードディスクを廃棄する場合は、社内で破壊した上で廃棄処理に回している。
- パソコンには個人情報を含む取引に関する情報は保管しない。また、機密情報の管理については社長が行っており、パソコンに保管してよい情報についても社長の判断としている。
- インターネットバンキングは利用していない。メールでの添付ファイルのやり取りも基本的には控えている。ノートパソコンには最低限の情報しか格納せず、基本的に持ち出しも行わないようにしている。

■ 取り組みによる効果

- 現状では、特にセキュリティ事故につながるような事象は起こっておらず、また外部からも十分ではないかという意見もあるため、効果は出ているのではないかと思われる。
- 1 分 1 秒を争うような業務ではないため、紙ベースの業務形態で十分と判断しており、情報セキュリティへの投資を増加させても、効果はないと考えている。

■ 経営者の視点

従業員 2 名の小規模企業であり、また、不動産業という、さほど緊急性を伴わない業務の性格から、情報セキュリティ対策については現状で十分だとの外部の意見がある。この規模と業態に見合った対策としてどこまで実施すべきなのかが投資対効果も含めて判断できないため、今後何をしてよいかは分からない。ただし、インターネットや電子メールの取り扱いについては、基本的に、「信じない」という考えで、「絶対大丈夫」という保証がない限り利用を促進しないため、今後も、今以上に利用していくことは考えておらず、また業務的にも必要ではないと考えている。

事例 25

所在地	京都府
業種	不動産業
従業員規模	21～50 名
事故の有無	有(2016 年)
ケース	ランサムウェア

ランサムウェア感染をきっかけに情報セキュリティへの取り組みの方向性が明確化、まず業務現場の社内ルールの整備から開始

■ 発生した事故と影響

当社は、京都府に本社を置きオフィスビルやマンションの管理をしている。2016 年、役員が宛先不明のメールの添付ファイルを不用意に開封し、1 台の社内 LAN 端末パソコンが「ランサムウェア」に感染した。その結果、共有サーバ内のファイルにアクセスできなくなった。幸いにも経理サーバは、別セグメントで運用しており、経理サーバのデータは被害を免れた。経理サーバを納入したベンダに相談した結果、共有サーバのデータを捨てても事業継続に大きな支障はないので、身代金支払い要求を無視して共有システムを初期化する対応を実施した。共有サーバの再稼働には 1 週間以上の時間を要した。

■ 事故の要因

メールフィルタリングツールを導入していないことに加え、不審メールを受信した際の対処方法を詳しく知らなかったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

事故発生当時、当社には情報システムを管理する体制がなく、社内の情報システムを一括して管理するベンダも存在しなかった。さらに情報リテラシーが低く、守るべき情報が組織として明確になっていないほか、情報を管理するための組織的なルールが明確になっていない、情報セキュリティ教育が実施されていないなどの問題があった。ランサムウェア被害の後、情報セキュリティに取り組む必要性が社内に認識されつつあり、社内で IT リテラシーが高いと目される管理部の 1 名及び経理部の 1 名にて、まずは業務現場で守るべき社内ルールを明確化するための取り組みを始めたところである。

■ 取り組みによる効果

効果面では、まだこれからのことと言えるが、当社が情報セキュリティに取り組むための方向付けは担当者レベルで明確になりつつある。具体的には、前項に挙げた状況を解消するために、当社としての今後の情報利活用の在り方を明確にして、それに対応する情報セキュリティの要件を洗い出し、内部規程をはじめとするルール及びインフラ面の整備を推進することになる。仕組みができれば、続いて組織内への浸透策として、継続的な教育の実施を行いたい。

■ 情報セキュリティ担当者の視点

情報セキュリティへの取り組みの必要性は、経営者にも認識されつつある。この方向性を正しく推進していくには、社内担当者だけではなく、経営者に対する外部からのさらなる啓蒙活動が望まれる。担当者が正当な認識のもとに社内の情報セキュリティレベルの向上を推進したいと思っても、経営者からの強力なコミットメントがなければ成功しない。

当社としては、理論どおりに方針を明確にし、内部規程やインフラを整備して、その後に組織に定着させる手法よりも、業務現場の実務的な情報セキュリティの日常的かつ具体的な運用ルールの明確化とその実施から対策を進めていきたいと考えている。

事例 26

所在地	高知県
業種	不動産業
従業員規模	51～100 名
事故の有無	有(発生年不明)
ケース	ウイルス感染

従業員の情報管理意識の高さにより大きな事故はない
組織的な取り組みはこれから

■ 発生した事故と影響

当社は、高知県で賃貸不動産管理を事業としており、現在は大手の不動産賃貸借ネットワークチェーンに加盟している。ビジネスとして顧客への情報提供に重点を置いており、全職員がネットワークを利用し、パソコンやタブレットを活用して日々の業務を行っている。業務上入手する顧客の個人情報等の重要情報があり、管理すべき情報の量は多い。そのような中で、社内のパソコンが電子メールを通じてウイルスに感染し、対応に苦労した。何が起きているかが理解できず、外部の専門家に対処してもらった。

■ 事故の要因

パソコン等の利用ルールが定められておらず、従業員が意図せずに危険な操作をしてしまった可能性がある。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 上記の経験を踏まえて、外部の専門家に相談し、社内におけるパソコンの利用ルールを作成するとともに対策ツールを導入した。現状において、セキュリティ対策は業務上の役割としてではなく、２名の従業員による自主的な取り組みとして行われている。
- 情報管理の観点では、利用者アカウント毎のアクセス制御、情報資産の保管場所の施錠管理を実施しているほか、データとシステムのバックアップの確実な運用を行っている。総務と経理部門のシステムは営業系とはネットワークが切り離され、単独で運用されている。また、すべてのパソコンにウイルス対策ソフトを導入しているほか、外部へファイルを送信する際はパスワード設定による保護も実施している。こうしたルールの遵守状況は、個々の従業員との対話を中心に確認されている。

■ 取り組みによる効果

上述のように、組織的な情報セキュリティ対策に関する取り組みは現状において実施されていないが、全従業員が情報機器を業務で活用し、顧客向けにウェブサイト等を通じてビジネス展開していることから、従業員の情報管理に対する意識や倫理レベルは高く、担当者は日々の管理に対し、責任感と危機感をもって取り組んでいる。この結果、今日まで大きなセキュリティ事故は発生していない。

■ 情報セキュリティ担当者の視点

セキュリティ対策は当社にとって非常に重要であり、取り組むべき内容や範囲等については十分に認識しているが、対策のための費用の確保が一番大きな問題である。大がかりな対策を導入する前に、短期間で対応できるようなルールの整備や、個々のセキュリティ対策機能の設定など、できるところから取り組みを進めていく意向であり、現在こうした対策に関する情報を収集している。当社の業務は情報システムに依存している部分が大きな比重を占めており、万が一事故が発生した場合の影響は大きい。セキュリティ対策が重要であり、組織としてセキュリティ運用を行うことが必須であると経営者に理解してもらうことが、今後の事業継続のためにかかせないと考えている。

事例 27

所在地	福岡県
業種	不動産業
従業員規模	21～50 名
事故の有無	有(発生年不明)
ケース	ランサムウェア

経営者の情報セキュリティに対する理解の下で対策を推進
セキュリティ事故発生時の素早い対応が感染拡大を防止

■ 発生した事故と影響

当社は、福岡県で地元を中心に不動産業を営んでおり、多くの顧客を抱えている。2010 年頃、当時情報セキュリティについて特に問題があった訳ではないが、個人情報保護の重要性と「個人情報保護マネジメントシステム実施のためのガイドライン第 2 版」の発表等から、経営者が個人情報保護を中心とした情報セキュリティの必要性を強く感じ、取り組むようになっていた。しかし、従業員のパソコンで業務中に「ランサムウェア」に感染した。メールを開封して間もなくパソコンが暗号化されてしまい、その従業員はすぐにネットから切り離し、責任者の総務部係長へ報告を行った。緊急で IT ベンダに連絡をとり対処したため、その後の広がりを防ぐことができた。

■ 事故の要因

従業員の情報セキュリティに関する意識が不十分であったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 当社のセキュリティ対策は、個人情報保護監査責任者も兼ねている総務部係長が中心となり、セキュリティ企画や関係者を巻き込んで運用にあたっている。ランサムウェアに感染した経験から、総務部係長は不定期的ではあるがログを確認するようになっている。
- プライバシーマークを取得しており、プライバシーマークで必要とされているマニュアル類に従って個人情報保護の仕組みを運用している。オフィスへの入退室管理、書類等紙媒体及びモバイルメディアの施錠管理、システム及び重要なデータの定期的バックアップ、アカウント毎のアクセス可能範囲及び 3 段階のアクセス権限レベルの制定、ハードディスク等の廃棄時の破砕、VPN、サーバ及び全パソコンのウイルス対策ソフトの導入等物理面、論理面を含めて取り組んでいる。サーバは IT ベンダにアウトソーシングしており、運用にも万全を期している。
- 不動産業界は重要な個人情報を扱っており、同業者との横のつながりを持ち、同業者間の情報セキュリティに関する情報交換を行っている。

■ 取り組みによる効果

- プライバシーマーク取得の効果は大きかった。取引先からの評価が高く、営業面でも自信をもって行っている。
- もともと経営者の情報セキュリティに対する理解があったので情報セキュリティ対策は行いやすかった。また、情報セキュリティ事故を起こした時の関係者の対応が素早く行え、普段からの心構えがいかに重要であるかが認識でき、情報セキュリティに関する意識が大きく変わり、従業員の意識がより高まった。

■ 情報セキュリティ担当者の視点

システム的な対応はほぼできていると思っているが、人に関わる運用面には改善の余地がある。例えば、情報セキュリティ専任者がいない環境での最新のセキュリティ関連情報の入手や従業員教育など、対応を進める上で悩ましい部分がある。また、情報セキュリティには終わりがないという不安があり、どこまでやればいいのか妥当な判断ができない。これらの課題がある中で、情報セキュリティ専任者のいない小さな企業で重要情報を守りきるには従業員全員が同じ価値観を持って対応しなければ効果が上がらないので、やらされる情報セキュリティから従業員自ら行う攻めの情報セキュリティが行える人材として育てる方針である。

事例 28

所在地	栃木県
業種	サービス業
従業員規模	6～20 名
事故の有無	有(2015 年)
ケース	内部不正

内部不正の再発防止策に取り組み、リスク低下と従業員の安心感を実現

■ 発生した事故と影響

当社は、栃木県で自治体等からの委託により、し尿、浄化槽汚泥、生ごみ等の浄化処理を行っている。2015 年頃、関係者しか立ち入ることのできない設備の写真が、業務と直接関係がない非公式な文書に掲載されて委託元に送付される事案が発生した。調査の結果、退職した従業員によるものと判明し、委託元からは信用回復のため再発防止策を求められることとなった。当社では従業員以外の個人情報を取り扱うことはほとんどなく、情報を外部に持ち出すことも少ないため、従業員との間で機密保持契約を締結している以外は特別な対策を実施してこなかった。しかし、今回の件を受けて、新たな取り組みの必要性を感じた。

■ 事故の要因

情報漏えいに関するリスクの見極め、従業員に対する情報セキュリティ関連の教育、就業規則や守秘義務などのルール・規則面の整備が不十分であったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 再発防止策として、スマートフォン等を含むカメラの持込制限等も検討したが、内部犯行に対しての効果は限定的であり、逆に利便性の低下が大きいため、機密保持契約と啓発・教育を徹底することにとどまった。また、定期的なアンケートによるセキュリティ対策状況の報告とセキュリティ担当者に対する集合研修を行っている。
- 業務上の電子ファイルについては、クライアントパソコンに保存せず、社内に設置した NAS に保存するルールとしている。NAS はミラーリングを行っており、災害時などに備え、持ち出し可能なハードディスクに定期的にバックアップしている。また、USB メモリについては、暗号化機能を備えたものを使用している。
- 社外へは VPN で親会社のネットワークに接続し、そこから外部に接続されている。外部と接続する際にはパスワードを求められ、アクセスログが取得される。メールサーバも親会社が提供し、フィルタリングが行われている。
- 建物内には当社の他に業務委託先企業 1 社が入居しており、機密保持契約を締結している。

■ 取り組みによる効果

当社は特定の委託先から長期に業務を受託していることもあり、事業を通じた効果を知ることはできない。一度失った信用はすぐには回復できず、相手側は守って当たり前との意識があるため、評価されることは少ないが、再度セキュリティ事故が発生した場合、必要以上にコストがかかる対策を求められることに加え、経営に対しても大きなインパクトが発生することになるので、リスクを低下できたことが最大の効果だと感じている。また、従業員がセキュリティの脅威をあまり意識することなく、日常の業務に安心して取り組めることで作業効率が上がっていると感じている。

■ 情報セキュリティ担当者の視点

企業の情報セキュリティ向上には経営者のコミットメントが必須であるが、中小企業においては、さらに経営者自らがリーダーとなって牽引していく姿勢が重要だと感じている。今後はクラウドの利活用も視野に入れた情報セキュリティ対策を進めていく必要があると考えている。また、ネットワーク障害に備えた自社 NAS との併用も検討しているが、ディスクの盗難などのリスクは残存するため対策を検討中である。

事例 29

所在地	東京都
業種	サービス業
従業員規模	21～50 名
事故の有無	有(2000 年)
ケース	ウイルス感染

顧客への納品物にウイルス感染防止対策を実施し、顧客からの評価と信頼が高まり、業務拡大につながった

■ 発生した事故と影響

当社は、東京都で一般廃棄物・産業廃棄物の中間処理を行っている。2000 年頃、専用の基幹システムの開発に着手し、パソコン等を導入して運用を続けていたところ、社内のすべてのパソコンの動きが非常に遅くなった。システム導入を依頼した会社に相談したところ、ウイルス感染によるものと診断された。機密情報の漏えいや基幹システムの停止の被害を受けたが、ウイルスの感染経緯や原因を解明することはできなかった。その後、被害範囲の限定や、対策の検討、再発防止など、被害後の対応に多大の工数を要した。ウイルス感染を経験したことで、データの保護とシステムの可用性の重要性に気付いた。

■ 事故の要因

パソコンを利用し、外部と接続している状況にも関わらず、ウイルス対策ソフトを導入していなかったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 自社用ファイアウォールを運用するとともに、すべてのパソコンにウイルス対策ソフトを導入した。また、基幹システムは社内の有線 LAN からのみアクセスできるようにしており、従業員が出先で使用するタブレットやスマートフォンからのアクセスは許可していない。常務が自ら先頭に立ち、情報セキュリティに関する企画・導入・監視・運用をしている。また、年に 1 回の従業員教育を行うとともに、毎週の週礼にて社外で業務する運転手にも情報セキュリティの重要性を伝えている。
- 産業廃棄物の破棄証明を希望する顧客には、納品する CD-R のウイルス・スキャンを実施し、そのスキャンプログラム名と更新レベルを明記して納品するなど、顧客に CD-R を介してウイルス感染がないように配慮している。

■ 取り組みによる効果

対策導入以降、情報漏えい等セキュリティ事故は起きていない。CD-R に関する上述の対策を行うことで、情報セキュリティに対する意識が高いと経営姿勢が評価され、顧客の信頼も高まった。さらに、顧客から情報機器のデータ消去業務も依頼され、新たな仕事の獲得に結びついた。基幹システムを安心して活用できるようになり、各種多様な帳票が柔軟に出力できるようになった結果、監督官庁に正確かつ迅速に報告書等を提出でき、業務エリアの拡大にも結びついている。

■ 経営者の視点

現行の社内システムは機能中心で、セキュリティ管理は外側で対応する考え方である。この考え方は、経営陣の計画や要望に追随できず、情報セキュリティリスクと対策が残ることになる。今後、社内システムをリニューアルして情報セキュリティを組み込んだシステムに移行する必要がある。情報システム全体を俯瞰して、情報セキュリティ全体のバランスを見て、急いで対策を打たなければならない部分から対策を打っていく。物理的対策としては、監視カメラを出入口だけではなく、敷地全体が監視できるように追加設置していきたい。また、現在廃棄依頼される情報機器の多くにデータが残っているが、これを消去してから廃棄する業者はほとんどない。今後はデータを消去して廃棄する分野に進出し、ワンストップ産業廃棄物処理業者を目指したい。

事例 30

所在地	神奈川県	**複数の IT ベンダから情報収集し、情報セキュリティの重要性の理解が深まった**
業種	サービス業	
従業員規模	21～50 名	
事故の有無	有(2015 年)	
ケース	ウイルス感染 内部不正	

■ 発生した事故と影響

当社は、神奈川県で木材及びプラスチック材を主に扱う産業廃棄物業者である。2015 年頃、2 件のトラブルに見舞われた。一つは、「トロイの木馬」への感染により、基幹システムのスローダウンやレスポンス低下などが慢性化していたことである。データの喪失などの被害はなかったものの、業務効率の低下が定常的に発生していたと考えられる。もう一つは派遣従業員が退職する際、顧客情報データを持ち出したことである。退職後にパソコンの操作履歴を分析した結果発覚した。幸い実害は出ていない。

■ 事故の要因

産業廃棄物処理業という業種から、従業員の IT に対する知識は十分と言えず、パソコンがウイルスに感染しているかどうかも確認できなかったり、システムのレスポンスが悪くてもそういうものだと思ったりしていた。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | **技術的**

- 資産管理ソフトウェアを導入し、約 30 台ある社内のパソコンすべてのセキュリティ対策ソフトのパターンファイルやセキュリティパッチを最新に維持すること、パソコンでの操作履歴の把握を行えるようにした。
- サーバの統廃合やセキュリティ強化を実施する中で、IT ベンダの選定を実施した。これまでの業者だけでなく、門戸を広げ業者選定するようにした。

■ 取り組みによる効果

- 大きな効果として、IT ベンダとの関係性を変化させたことにより、より柔軟で効果的な IT システムの構築ができ、同時に情報セキュリティ対策の効果を高め、リスクを削減したことが挙げられる。複数業者からの提案を受け入れ評価することで、より広く情報収集することができ、自社の IT システムや情報セキュリティの在り方を自ら考えることができるようになった。また、こうした取り組みを通じて、経営層や従業員にも少しずつ情報セキュリティの重要性を理解してもらえるようになったと感じている。
- 当社の場合、情報セキュリティに関する問題が発生したことが直接の情報セキュリティ対策に取り組むきっかけになった訳ではなく、新任の担当者の情報セキュリティに対する意識の高さから、取り組みの重要性を強く感じ、その取り組みを実行に移していく中で問題の検出やその問題の解決を平行して行っていった。

■ 情報セキュリティ担当者の視点

当社は創立以来順調に事業を拡大してきたが、今後さらなる事業の成長に向け、自社の事業方針を対外アピールしていく必要があり、情報セキュリティリスクへの対応も重要な課題になるものと感じている。技術的な面においては、スマートフォンの取り扱いによる情報セキュリティリスクが懸念される。当社においては多くの従業員に社給のスマートフォンを貸与しているが、アプリの管理など早急に対策を実施する必要があると考えている。経営層に直接の事業成果に結びつかない情報セキュリティへの投資を理解してもらうことに苦労したり、情報セキュリティに対する業務への評価が十分に得られなかったりすることが悩みである。

事例 31

所在地	福岡県
業種	サービス業
従業員規模	6～20 名
事故の有無	有(2009 年)
ケース	ウイルス感染

事故を経験し、従業員が一致団結して情報セキュリティ対策に取り組む効果を認識

■ 発生した事故と影響

当社は、福岡県で自動券売機等の機器の納入や納入した機器の保守サービスを展開している。2009 年頃、顧客に納入した機器のトラブル時にログを取るために使用した USB メモリがウイルス(WORM_DOWNAD.AD)感染事故を起こした。幸いにも納入機器にはウイルス対策ソフトが導入されていたため、すぐに発見できウイルスによる被害はなかったが、ウイルスを持ち込んだことが大問題であり、顧客からの強い要請のもと、情報セキュリティリテラシーの向上と徹底を図ることが企業存続に必須の要件と認識し、改善に取り組むこととなった。

■ 事故の要因

USB メモリの取り扱い手順やウイルスチェックに関するルールが明確に規定されていなかったことに加えて、情報セキュリティリテラシーの徹底が従業員に浸透していなかったことが原因である。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 納入先企業の指導も受け、「情報セキュリティ事故防止のための遵守事項及び作業手順」を経営者、セキュリティ担当者を中心に制定した。この目的はウイルスや作業ミスによる顧客や自社システムの損壊、及び顧客情報、個人情報流出等の事故を未然に防ぐために定めたもので、業務を行う上で最低限遵守すべき事項とした。また、従業員に支給したパソコンやデータサーバ及び経理システムの取り扱い、パソコンや USB メモリ等の記録媒体を持ち出す場合の手順、移動・運搬における注意事項、顧客施設内や帰社後の作業手順を定め、徹底して情報セキュリティリテラシーの向上に努めている。
- 作業時における遵守事項補則も定めており、修理に不要なデータは顧客に依頼して移動または削除してもらう、ハードディスク等記録媒体を交換した場合は顧客に廃棄を依頼する、自社で記録媒体を破棄する場合は破壊することを定めた。
- 自社内で重要な位置付けのパソコンにはセキュリティワイヤーでの機器の固定、書類等の紙媒体での情報は施錠管理を徹底するよう再確認した。

■ 取り組みによる効果

情報セキュリティに対する従業員の意識が大きく変わった。情報セキュリティの事故を起こせば企業存亡の危機にもつながるという体験から従業員が率先して制定した作業手順を遵守している。また、従業員個人に 1 台ずつ支給しているパソコンの管理レベルが大きく上がった。現在は無事故でサービスを展開できている。また、訪問先顧客の情報セキュリティリテラシーが目につくようになり、場合によっては指導する状況も出てきた。

■ 情報セキュリティ担当者の視点

自社内・企業間における情報資産の価値が企業活動の成否を左右する現在、それを支えるリスク管理の一環としての情報セキュリティ対策こそ、正面から対峙しなければならない経営課題であることをさらに認識し徹底する必要がある。従業員が一致団結して情報セキュリティ対策に取り組めば効果が大きいことが認識できたので、今後もセキュリティ担当者を中心に継続して定期的にスキルアップを図りたい。

事例 32

所在地	福岡県
業種	サービス業
従業員規模	6～20 名
事故の有無	有(2015 年)
ケース	内部不正

内部不正をきっかけにユーザ ID とパスワードの管理強化を徹底

■ 発生した事故と影響

当社は、福岡県で家電量販店の保守サービス部門へサービス提供している。2015 年頃、ある担当者が業績を上げたい一心で別担当者のシステム上の保守情報にアクセスした。幸い目的が個人情報ではなく、業務処理件数、保守ノウハウ等の取得にあったため大事には至らなかった。

■ 事故の要因

パスワードが推測可能なほど弱かったのが原因である。ユーザ ID とパスワードの強化を徹底するなど、情報セキュリティの重要性が再認識され、自社システムの情報セキュリティ対策についても改善に取り組むこととなった。

■ 事故後の取り組み

組織的 | 人的 | 物理的 | 技術的

- 事故が発生したシステムに接続しているパソコンの ID とパスワードに関するポリシーを明確化した。ユーザ ID とパスワードは 6 ヶ月毎に変更している。特徴的なことはユーザ ID も変更することである。ID の権限には 3 段階あり、管理職、一般従業員等、最小権限の原則に基づき権限を割り当てている。
- 自社システムにウイルス対策ソフトを導入しているほか、ランサムウェア対策としてシステム及び重要データのバックアップを USB メモリに毎月定期的に取得し、USB メモリを金庫に保管している。電子メールの取り扱いについても知らない発信者からのメールや表題の怪しいメールは開封しない等を徹底している。事業拠点の増加に伴い、情報セキュリティ対策の水準を維持することが難しくなったため、各拠点に情報セキュリティ担当者を育成・配置した。
- IT 関連の教育は社内で実施しているが、情報セキュリティ関連のスキル向上を促すため、従業員に対して関連資格の取得を推進しており、受験料の補助や合格祝い金が支給される。また、3 ヶ月毎に各拠点の担当者が集まり、情報セキュリティ委員会を開催している。現状や悩みを共有し、好事例があれば取り上げたりすることで、会社としての情報セキュリティ対策の均一化、向上を図っている。ISMS の内部監査では、ある拠点の情報セキュリティ担当者が別の拠点を見るようにしており、監査する側、される側の視点を養い、情報セキュリティに関する意識の向上を図っている。

■ 取り組みによる効果

情報セキュリティに対する従業員の意識変化が起こっていると感じる。情報セキュリティに関するルールを守らなければリスクが顕在化するということを従業員全員が認識するようになった。また、部外者がオフィスへ無断で侵入してきたことがあったが、冷静に声がけして退去させることができた。これをきっかけに物理的なセキュリティ対策の必要性も感じ、施錠管理と入退室管理を強化した。

■ 情報セキュリティ担当者の視点

情報セキュリティ対策を推進していく上で、経営者の理解は必要不可欠であるため、経営者の判断にとって必要な情報を集めたいと思っている。その上で、インターネットニュースや TV ニュース等で知った情報セキュリティに関する最新情報を朝礼等で従業員に指導するなどの啓発活動を通じて、リスクに備えたい。

事例 33

所在地	新潟県
業種	農林水産業
従業員規模	51～100 名
事故の有無	無

組織内研修の効果：不審なメールへの関心の高まり、OS やセキュリティソフトを常に最新の状態にするのは当たり前

■ 情報セキュリティ対策に取り組むきっかけ

当組織は、新潟県で農業従事者によって構成され、給排水・区画整備・農道整備等の農地改良を行っている。近年、職員のメールアドレス宛の迷惑メール・詐欺メールが多くなり、選別作業が業務に支障をきたす上、実在の組織を名乗る巧妙な詐欺メールもあり、危険性を感じるようになった。特に、国家資格者を名乗るメールは、普段から国家資格者への依頼が多い当組織では正規のメールと紛らわしく、内容を信用してしまうおそれもある。機械的なウイルスチェックだけでなく平文のメールであっても注意する必要があり、職員の意識向上の必要性を感じた。また、過去にはドメイン名の末尾が「go.jp」であったこともあり、政府組織と間違えられることによるサイバー攻撃にも警戒する必要があった。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 組織内のネットワーク管理者がセキュリティセミナーを受講し、そこで学んだことを基に、システム会社の協力を得て組織内研修を開催した。組織内研修は複数回に分けて実施し、全職員が受講することを義務付けた。
- セキュリティソフトを常に最新版にしておくようセキュリティポリシーに記載し、研修でもそのことを全職員に伝えた。また、ソフトウェアのアップデートが必要な場合は社内報で周知するようにした。セキュリティソフトは、パソコンとサーバとで異なるメーカーのものを採用し、万一片方で対応できない問題があった場合でも相互補完できるようにした。
- 組織内サーバへの社外からのアクセスは、VPN 経由を必須とし、また、社内から社外へのアクセスにはプロキシを必須として、出入口を集約させることで設定・監視をしやすいようにした。

■ 取り組みによる効果

- 組織内研修の主な目的は職員の意識向上であり、受講後に「こんなメールが来たけれども本物かどうか」「大丈夫かどうか」といった質問が出るようになり、一定の効果が現れている。従来、情報セキュリティは担当者が気をつければよいという意識があったが、全職員が他人事ではなく自ら気をつけるべきことであるという意識を持てるようになってきた。
- OS やセキュリティソフト等のアップデートについても、常に最新版にしておくのが当たり前の状況になりつつある。以前はアップデート時間などが業務上負担になる場合にはアップデートしなかったり後回しになったりすることがあったが、研修後はそのようなことはなくなった。

■ 情報セキュリティ担当者の視点

組織内研修は今後も定期的に続けていく。受講直後は皆が関心を持っているが、「喉元過ぎれば熱さ忘れる」となる可能性もある。組織内の IT スキル・知識レベルがバラバラなため、内容が難しくなりすぎないように気をつける必要がある。一方で研修が惰性化しないよう、新しい要素や実際に起きたセキュリティ事故の話等も盛り込みたい。また、USB メモリやメモリカードを用いた外部とのデータのやり取りが多いため、ルールの整備と実施を徹底したい。将来はデータをサーバに直接送信するなど USB メモリやメモリカードを使わない方法で同業務ができるようにしていきたい。

事例 34

所在地	石川県
業種	農林水産業
従業員規模	5 名以下
事故の有無	無

当たり前の対策が顧客及び自社内の安心感につながる

■ 情報セキュリティ対策に取り組むきっかけ

当社は、石川県の農業従事者である。米穀の直接販売を目的にネットショップを構築し、運営している。1990 年代後半、会社のパソコンで訳の分からない内容の不審な電子メールを受信したことで、ウイルスに感染したのではないかと疑った。この時はウイルスに感染していなかったが、知人からウイルスに感染すると怖いと聞いたこともあって、ウイルス被害を未然に防ぐため、ウイルス対策ソフトウェアを導入したのが、情報セキュリティ対策に取り組んだきっかけである。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | **技術的**

- 社内のすべてのパソコンにウイルス対策ソフトを導入するようにした。
- その後、ネットショップを構築するとともに、バックヤード業務としての販売管理、給与・経理、従業員との情報共有の目的でサーバを導入した。この時、システムを導入した業者に委託して、Web 関係の対策（Web、ファイアウォール）、ファイル等の暗号化、ネットワーク接続監視などの情報セキュリティ対策を導入した。
- 情報セキュリティ対策を委託するにあたり、業者の見積もりの妥当性が分からず苦労した。そのため、10 数年前からウェブサイト作成等で支援を受け、信頼している IT コーディネータに相談し、アドバイスをもらった。

■ 取り組みによる効果

- 当社のセキュリティ対策は社外から見ると当たり前のことかもしれないが、最近は顧客のマイナンバーを扱うこともあり、顧客情報が外部に漏れるリスクが小さくなっていることの安心感がある。
- 対策に使っている費用の妥当性が分からないので、費用対効果は答えようがない。お米販売のネットショップにおいて、カード決済を望む顧客が多いため、購入の時の安心感にはつながっていると思う。

■ 情報セキュリティ担当者の視点

今後予想される悪質なウイルスへの対策は必要と思っているが、情報セキュリティについての知識があまりないので、どのように対策を向上させればよいかは分からないというのが正直なところである。情報セキュリティ全般についての現在の課題は、スマートフォンの情報セキュリティ対策である。直近に受けた情報セキュリティ被害はない。しかし、セキュリティの取り組みの導入を検討している他社、経営者に向けて、情報セキュリティ対策は、農業で言えば農機具のようなもので、米作りには必要なものであり、同時にまさかの備えとしての保険のようなものであるとアドバイスしたい。

事例 35

所在地	島根県
業種	農林水産業
従業員規模	6～20 名
事故の有無	無

鳥インフルエンザ対策の基本理念「予防と隔離」を情報セキュリティ対策にも応用

■ 情報セキュリティ対策に取り組むきっかけ

当社は、島根県で養鶏場を経営し、日々卵の出荷を行っている。当社の IT 利用は、電子メールとインターネットの他に基本的な販売、仕入れ、会計、給与業務を既成のパッケージソフトにて行い、鶏舎の温度管理を Excel にて記録するなど必要最低限のものである。それでもコンピュータウイルスに感染してしまえば、鳥インフルエンザ同様、事業そのものが停止してしまう。当社では情報の脅威も事業の脅威と同等であると捉え、情報セキュリティ対策に取り組むこととした。セキュリティの一般的知識は有していたものの、専門知識には自信がなかったことから、まずパッケージソフトの導入時に支援を受けているベンダに相談した。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 鳥インフルエンザ対策として「予防と隔離」を基本理念として、普段の作業にも徹底している。IT にも同じ理念を取り入れた。まずは基本的な予防策として市販のウイルス対策ソフトを導入した。この他、インターネットバンキングでは取引銀行からの指示でブラウザのセキュリティ設定を行った。
- 人的な対策として、日頃から配送や機器の保守業者以外に対して会社敷地内への立ち入りを認めていないのと同様、面識がない、または通常の交流がない人物からのメールは、一切開かないことを社内のルールとした。一方で、従業員には積極的に電子メールやインターネットを利用して欲しいので、初心者にはインターネットの閲覧に関して特に規制をしていない。ある程度使い慣れた段階で社長が利用範囲を監督するようにしている。社内に IT に強い若手従業員が少ないこともあり、こうした対策は社長自ら主導している。現状では IT 利用時にこれ以外のルールは定めていないが、将来は必要であると認識している。

■ 取り組みによる効果

取り組み以前から IT に関する被害は生じていなかったが、情報セキュリティ対策を整備することで利用時の安心感を得ることができた。利用時のやや放任的な姿勢も、対策を整備しているから可能であると認識している。従業員に対しては、日常の業務において、現場の業務と同様に IT 利用時にもリスクを意識することを強調しており、従業員の中でも利用頻度の高い者に対し、セキュリティについて指導を行う環境を整えることができている。どこまで浸透しているかは分からないが、意識付けの良いきっかけになった。

■ 経営者の視点

今後は従業員による IT 利用に関して明確な指針を示し、ルールを整備する必要があると考えるが、現状で常識的な使い方の範囲内ということもあり、暫く様子をみる予定である。ルールに縛られて使えないようになるよりは、積極的に使い慣れてからルールを明確にする方針は続ける。もちろんセキュリティの重要さは認識しているので、自社にとってどの程度のレベルのセキュリティ対策をすべきか、今後もベンダと相談しながら進めていきたい。近年農業関連では多くの IT 利活用事例があり、今後様々なシステムやアプリケーションが出てくることが見込まれるので、当社でも利用価値のあるものは積極的に利用していく。この際、セキュリティについても最優先で考えていきたい。

事例 36

所在地	徳島県
業種	農林水産業
従業員規模	6～20 名
事故の有無	無

セキュリティ対策を含めた管理体制が取引先から評価
地震の被災経験から BCP を考慮したシステム構築を目指す

■ 情報セキュリティ対策に取り組むきっかけ

当社は、徳島県で野菜苗、接木苗を生産している法人である。当社はパソコンが珍しい時代から積極的に活用を進め、多拠点を結び、生産管理、販売管理、会計等に活用している。インターネットを活用する頃からセキュリティ対策の必要性を感じ、対策に取り組んできた。また、2016 年の熊本地震では拠点農場の被災によりネットワーク回線がダウンし、情報システムが使えなくなった。苗への被害は軽く、地元農家等への販売は継続したが、情報システムが使えないため現場では混乱が見られた。この経験から、セキュリティに加え BCP の観点を組み入れた情報システムの構築を進めている。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | **技術的**

- 2015 年に多拠点を結ぶ VPN 回線をリニューアルした際にセキュリティの強化を図った。ファイアウォールの設置、ウイルス監視の導入、ネットワーク監視の導入を行った。併せて従来認めていた個人所有パソコン等の社内ネットワークへの接続禁止など運用ルールの強化を図った。
- 情報システムの管理担当者は、現場作業と兼業のため、繁忙期には管理業務に割ける時間が限られる。そこで、ネットワーク監視、ウイルス監視、ファイアウォール運用管理等について、外部サービスを活用し運用の負荷を下げている。
- 帳票の作成は、生産管理システムでは最低限とし、ユーザが個々のパソコンにデータをダウンロードして加工するエンドユーザコンピューティングにて対応している。これはセキュリティ上のリスクとなり得るため、データ活用の必要性と外部に流失した影響を勘案して、利用できるデータへのアクセス制限とログ管理で可用性と機密性の両立を図っている。

■ 取り組みによる効果

- 大手種苗メーカーや、コンプライアンス意識の高い農協等と取引を行っている。これら企業等と取引を行う場合、当社の情報システムを含めた、社内の管理体制についての情報提供を求められることがある。当社のセキュリティ対策を含めた管理体制は、これら企業等から評価され、安定した取引につながっている。また、外部のサービスを活用することで現場業務との兼任をしながら、高いセキュリティ品質を保てることに満足している。
- ネットワーク回線のリニューアルの結果、セキュリティを強化した一方で回線速度が速くなったこともあり、情報システムの運用の安定化と操作性の向上等の効果が出ており、従業員からの評判も良い。

■ 情報セキュリティ担当者の視点

外部からの攻撃で被害を受けることよりも、内部の人材の過失による情報流出の可能性が高く、社内への教育が重要と考えている。当社の業務の関係上、従業員の IT リテラシーは高いとは言えない。入社時に就業規則の説明の中でセキュリティについて教育を行い、その後はグループウェアで周知を図っている。しかし、現在はセキュリティに関する暗黙のルールはあるが明文化されていないため、今後はセキュリティポリシーや各種規程の策定とともに、計画的な教育を行う必要があると考えている。また、県外拠点の成長に合わせて、情報システムの見直しを考えている。特に災害時の事業継続と物理セキュリティの強化を目指し、クラウド環境での運用の検討を進めている。費用対効果を見極めて進める方針である。

事例 37

所在地	鹿児島県
業種	建設業
従業員規模	101～300 名
事故の有無	無

情報漏えいに対する従業員の意識向上において現場監査の有効性を実感

■ 情報セキュリティ対策に取り組むきっかけ

当社は、鹿児島県の住宅メーカーで、県内の複数箇所に事業所を構えている。グループウェア、メール、ウェブサイトなど ICT の活用をいち早く取り入れ、現在では ICT なしには仕事ができない存在となっている。現在、個人情報を含む 6 万件以上の機密情報を所有しており、万が一情報漏えいが起こった際の会社への影響は計り知れないものが想定されることから、情報セキュリティ対策に取り組み始めた。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- ウイルス対策ソフトは、コーポレートエディションを導入し、Windows Update も含めて常に最新に保っている。加えて Microsoft 社／ウイルス対策ソフト会社／その他セキュリティ関連サイトを毎日チェックし、ウイルスメールの実際例をグループウェア上で公開し従業員が参照している。参照状況も確認でき、ほぼ全員が参照している状況である。
- 自社提供に加え BYOD（パソコンやスマホ）を利用可能としているが、申請／監査制度を採用している。四半期に一回は現場訪問による実機監査を実施しており、パソコンではアップデート確認や不要アプリの確認／USB メモリ利用禁止（ソフト購入済）の確認、スマホでは保存画像の確認／メールアプリの利用禁止確認などを実施している。規則違反を発見した際には、その場で是正をしている。パソコンは、固定 IP の利用を前提にしているが、他の機器に差し替えて社内 LAN に接続する危険もあったことから、固定 IP＋MAC アドレス認証で不正に接続ができない状況にした。
- 万が一の災害／障害／セキュリティ被害に備え、毎日バックアップを取得し、本社と事業所間でバックアップの相互保管を行っている。さらに、月に一回は外付け媒体にバックアップを取り、耐火金庫に保管している。

■ 取り組みによる効果

- ランサムウェア／標的型攻撃などのメールが従業員に到達することはあるが、従業員全員が事例を参照していることもあり被害はない。従業員からも「この前、ウイルスメールがきましたが、削除／駆除しました」と日常会話に出る状況である。従業員の情報セキュリティに関する意識は高まっている。
- 現場監査は非常に有効で、本人だけでなく、その周辺の従業員の意識を向上させることにもつながる。
- 「（意識的に）不正を行えないように『いつも監視されている』ということを意識させること」と、「ふとした気の緩みで漏えいを起こさないように『常に情報提供を続ける』ことで啓蒙を継続する」などで対策の効果は出ている。

■ 情報セキュリティ担当者の視点

現在、実際に情報漏えいを起こした他県の同業会社を訪問し、被害実態、対処方法、被害額などをヒアリングし、情報漏えい時の必要な対策を整理している。一方で、経営者は情報漏えい対策の意識は高いものの、対策費用が高額であると二の足を踏んでしまう。当社では年間の ICT 総費用を抑えつつ、情報セキュリティ費用を捻出する取り組みを従来行ってきた。トレードオフの関係である利便性や効率化とセキュリティについて、バランスを見極めることが必要である。今後は、万が一情報漏えい事故が発生した場合も想定し、情報セキュリティ対策について前向きに進めていきたい。

事例 38

所在地	千葉県
業種	製造業
従業員規模	101～300 名
事故の有無	無

基幹システムの刷新を機に体系的なセキュリティ対策を強化

■ 情報セキュリティ対策に取り組むきっかけ

当社は、千葉県でスマートフォンなどの精密電子機器の中の伝導体・絶縁体材料として使用される金属を製造している。仕事量が増加してきた 2010 年頃、社内にある営業情報（取引先や取引条件）や製造原価などの社内情報が競合他社等に漏えいするリスクに対して、明確な方針のもとで対策をとってこなかったことに気付き、当時事務所にあった時約 20 台のパソコンにウイルス対策ソフトを導入した。またマイナンバーの取り扱いが求められることになったのを機会に情報漏えい防止対策として、ファイアウォールを当初の予算外であったが前倒しで導入した。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | **技術的**

- すべてのパソコン（約 100 台）にウイルス対策ソフトを導入した。工場にある作業実績収集用のパソコンはアプリケーションの関係で Windows 7 だが、事務所のパソコンはすべて Windows10 に統一している。
- ネットワーク関連の対策としては、ファイアウォールを導入し、運用を開始した。併せて、運用ルールの整備も進み、他県にある自社工場と一つのネットワークとして管理し、不正に外部のウェブサイトをアクセスしないように管理している。
- 国内・海外ともに受注データの受信は FAX が中心であり、電子メールの添付を通じたウイルス感染のおそれはない。
- 業務データのバックアップは、定期的にとり、社外の保管倉庫に保管している。
- 業務量拡大や従業員増員に対応し、情報セキュリティを強化する必要があり、基幹システムを刷新する計画である。これまで、体系的に情報セキュリティ対策をしてこなかったので、新基幹システムは構築時から情報セキュリティを意識したものにしたいと考えている。

■ 取り組みによる効果

これまで情報セキュリティ関連で事故は起こしていない。当初の心配事に対する対策の効果は得られたと認識している。こうした成果を踏まえて、経営方針に沿って基幹システムの刷新が進んでいる。

■ 情報セキュリティ担当者の視点

情報セキュリティ対策の観点から現行システムの見直しのための改善計画を作成し、対策に着手したい。具体的には ID/パスワードの管理などを検討している。さらに、全従業員に対して情報セキュリティ研修を実施し、情報セキュリティの重要さ・大切さを根付かせたい。併せて、業務の中に情報セキュリティ対策を組み入れていくことを考えている。
時代の変化が早いので、情報システム担当として、必要な情報セキュリティ対策については適宜経営陣に提案し、実施していく必要があると感じている。そのため、こうした対策は他社の事例を参考にして、良いものを積極的に取り入れたい。必要であれば、年度計画予算を追加してでも実施することを考えている。

事例 39

所在地	岩手県
業種	情報通信業
従業員規模	6～20 名
事故の有無	無

取引先からの要請に応じてセキュリティポリシーを整備
従業員の役割・責任の明確化、意識の向上

■ 情報セキュリティ対策に取り組むきっかけ

当社は、岩手県でパッケージ開発・販売、受託システム開発、システム運用業務を核とした事業展開を行っている。運用をしているシステムには個人情報が含まれることから、以前から情報セキュリティには配慮していた。当社パッケージの販売代理店から、情報セキュリティに対する対応とそのエビデンスを求められることが増えたのを機会に、2015 年 8 月頃、社内規程の見直し及びセキュリティポリシーの策定を行った。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- セキュリティポリシー及び社内規程に沿って、業務運用・ハードウェア・ソフトウェアの取り扱いを明確にし、業務を遂行している。外部接続サーバにはファイアウォールを導入し、メールサーバにはフィルタリングソフトを導入して、外部からの脅威に対応している。また、サーバ室への入退出は、入退出記録を取り、鍵の取り扱い等も規程に従い運用している。
- セキュリティポリシーに関しては、年 1 回の見直しを行い、時間経過とともに形骸化しがちな作業手順等の見直しを実施している。

■ 取り組みによる効果

- セキュリティポリシー及び社内規程に、従業員のとるべき行動及び責任の所在を明確化することで、従業員の情報セキュリティに対する認識が向上し、セキュリティインシデントは発生していない。業務手順にセキュリティ項目を付加したことで手順が多くなり、全体的な作業効率は若干低下した部分があるが、想定の範囲内と捉えている。
- 標的型攻撃メールの受信例はあるが、被害は発生していない。
- 現在の情報セキュリティ対策が、業績向上には直接結びついていないが、対外的には、情報セキュリティ対策のエビデンスを明確に提示できるようになった。

■ 情報セキュリティ担当者の視点

現状ではシステム運用時のログ管理は OS と通信機器等のみにとどまっているが、情報セキュリティの向上のため、操作ログの収集も行うことを検討しており、来年度には導入したいと考えている。また、執務室・サーバ室の入退室に関して、物理的な鍵を使用した運用を行っているが、できれば静脈認証等のシステムを導入して管理していきたい。本件も、具体的な運用に向けて検討を行っており、来年度に対応したいと考えているが、入口の物理的な工事を必要とするため費用面の点で停滞している。

マイナンバー向けのソフトウェアは今後もリリースされることが予想されるため、現在導入している情報漏えい対策ソフトを随時置き換えたいと考えている。

事例 40

所在地	群馬県
業種	情報通信業
従業員規模	51～100 名
事故の有無	無

情報セキュリティ対策に取り組むことは企業として当然のこと
セキュリティ事故事例の共有により従業員の意識向上

■ 情報セキュリティ対策に取り組むきっかけ

当社は、群馬県でシステムの受託開発及び客先常駐による運用保守の業務と自社開発商品として、医療向けソフトの開発・販売を行っている。外部監査人から「情報セキュリティ対策に取り組むことは企業として当然である」とのアドバイスもあり、情報セキュリティ対策に積極的に取り組むことになった。またシステムの発注元が毎月発行している生々しいセキュリティ事故の事例を社内で共有したり、開発現場において情報セキュリティ対策について確認が行われたりする環境も情報セキュリティ対策に取り組むきっかけとなっている。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 発注元が公開している情報セキュリティ等のガイドラインを参考にして自社の情報セキュリティガイドラインを作成している。特に管理業務を行っている本社はできる限りガイドラインの遵守に努力し、客先常駐の現場においては顧客の情報セキュリティガイドラインに柔軟に対応するよう心掛けている。
- プライバシーマーク取得に向けて社内プロジェクトを発足し、取り組み中である。プライバシーマーク取得の取り組みを機会に情報セキュリティ対策にさらに意欲的に取り組むようになり、リスク分析や内部監査、入退室者の管理などを行うようになった。
- 作業現場が本社と離れているため、パソコン紛失等による情報漏えいに備え、パソコンの持ち出しを台帳管理している。現在は Excel を用いているが、今後は持出場所、パソコンのセキュリティ状態等を一元管理するため資産管理システムの導入も検討している。
- 発注元から毎月発行されるセキュリティ事故事例を社内で共有し、情報セキュリティへの意識を保っている。また、「新５分でできる！情報セキュリティ自社診断シート」を委託先選定のチェックツールとして利用している。

■ 取り組みによる効果

- セキュリティ事故ゼロを継続できており、発注元からの評価を下げることなく受注の増加につながっている。
- 現場の従業員においては、作業量が増加したことに対して当初は不満もあったが、情報セキュリティ事故事例の共有やプライバシーマーク取得に向けた一連の取り組みの効果もあり、従業員の情報セキュリティへの意識は高まってきている。また副次的な効果として、現場のリーダーに情報セキュリティ対策を任せることによるリーダースキルの向上もみられた。

■ 経営者の視点

これまでは代表者に権限等が集中していたが、情報セキュリティ管理の階層化等を手始めに組織体制を整備し、権限委譲を含め人依存から仕組みへと組織改革に取り組んでいきたい。また現在行っている年１回の情報セキュリティ教育だけでなく、毎月送られてくる発注元からの情報セキュリティ事故の事例をグループウェアで共有し、さらに従業員の意識の向上を図りたい。一方で、当社のもう一つの事業である医療向けソフトの開発・販売において、顧客である医療機関の情報セキュリティ意識が低いことが課題となっている。今後は顧客の情報セキュリティ意識の向上も含めたサービス提供について検討していきたい。

事例 41

所在地	富山県
業種	情報通信業
従業員規模	6～20 名
事故の有無	無

できることから初めて安心してサービスを提供できる環境へ
他社の有志による勉強会でセキュリティ情報を共有

■ 情報セキュリティ対策に取り組むきっかけ

当社は、富山県でスマートフォン等の販売や顧客のサポート事業を展開している。そのため、常日頃からセキュリティに関しては関心を持っていたこと、取引先のキャリアからより安全な環境の要請があったこと、またスマートフォン等を販売した顧客からの問合せや相談に的確に対応し、より良いサービスと安心感の提供につなげたいという思いもあり、自社においても何らかの対応が必要であると認識していた。当社において、セキュリティ事故は発生していないように見えるが、実際のところは分からないと認識している。外部セミナーの受講等を通じて得た情報を活用し、まずできることから始めるとともに、より積極的に情報収集に取り組まなければならないと考えた。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- できることから始めるという観点で、ネットワークに極力接続しない、電子メールに個人情報関連のドキュメントを添付しないようにするなど、運用ルールを決め、従業員に周知することから始めた。拠点間の情報の受け渡しは、特定の媒体（USB メモリ）のみを使用し、その媒体自体は鍵のかかる金庫に保管し、使用する場合は社長の許可を得ることとした。これにより、経営（社長）と現場の間での情報セキュリティに関する意識の違いを小さくするようにもしている。
- 20 社あまりの有志による勉強会（NPO 法人化している）を実施しており、その中で、セミナーで学んだ内容などを共有し、当社以外にも情報セキュリティの重要性を認識してもらうようにしている。ただ、当社自身の知識や情報が少なく、今後さらに情報収集に努めるようにしたい。

■ 取り組みによる効果

- セキュリティ事故は起こっていないようであり、また、物理的対応なども含め、リスク対策を講じることで、社内全体の意識付けもできてきており、経営として安心感も少しずつ生まれている。
- スマートフォンを代表とする通信機器について、顧客からの問合せにも答えられる幅が広がりつつある。

■ 経営者の視点

継続的な情報収集と、各種団体（商工会議所、県警サイバー対策室）や、情報関連企業への情報提供等を打診し、費用面も含めた具体的な対策を考えていきたい。また、それを通じて、従業員への意識付けをより強くすることで、安心してサービスの提供ができる環境を作っていく。現在、この点については、経営者の思いのもとで対応を進めているが、経営者だけでなく、経営者を補助できる従業員の育成にも努めていきたい。

また、当社の取り組みや現状を、勉強会で共有し、相互に理解を深めるように進めていくことで、中小零細企業の対応の在り方を探っていきたい。

事例 42

所在地	和歌山県
業種	情報通信業
従業員規模	6～20 名
事故の有無	無

ISMS 認証取得により対外的な信用獲得
情報セキュリティ対策は企業戦略として捉えることが必要

■ 情報セキュリティ対策に取り組むきっかけ

当社は、和歌山県でシステム開発やクラウドサービス等の IT 運用サービスを提供している。情報セキュリティに関しては、当初から関心を持っていたが、昨今の DoS 攻撃や標的型攻撃などにより、小規模企業でも情報セキュリティ対策が必要不可欠と感じられるようになった。そのような中、クラウド等のオンデマンド型 IT サービスを提供する当社の事業形態について、官公庁などの顧客から情報セキュリティの認証取得の要望が高まったことを踏まえ、2015 年から ISMS 認証取得に向けた取り組みを開始し、情報セキュリティ対策を整備した上で、2016 年 8 月に ISMS 認証を取得することができた。自社による取り組みだけでは、スキル不足や人員不足から ISMS 導入は困難であると判断し、外部からコンサルタントを入れて対応したことで、比較的短期間で ISMS 認証を得ることができた。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 小規模企業ながら、ISMS 認証に基づき PDCA サイクルのもとで情報セキュリティ対策を実施している。まず情報資産の洗い出しを行い、リスクを分析し、情報セキュリティポリーを策定し、対策手順を策定している。情報セキュリティ対策としては、適用宣言書に基づき、技術的対策、物理的対策や管理的対策を実施している。特に、サーバに関しては、東南海地震も考慮し、データセンターに移行し、当社施設内には 1 サーバのみ設置している。
- 当社の IT 運用サービス業務を振り返り、運用手順を明確化し、運用マニュアルを策定した。その際に当社における情報セキュリティの脆弱性を発見し、是正もしくは予防処置を実施することができた。さらに情報セキュリティ教育を全従業員に実施し、情報セキュリティの重要性を認識させている。

■ 取り組みによる効果

ISMS 認証により、全社として情報セキュリティ対策が一通り対応できているという効果は当然ある。対外的には、顧客である官公庁等からの信頼を得られただけでなく、業界内でも情報セキュリティの対応ができている企業として信頼を得られている。社内的には、従業員全員の教育により、情報セキュリティに対する知識が深まり、情報セキュリティの意識が高まった。また、副次的な効果であるが、運用マニュアルが整備されたことで、業務について誰でも理解できるようになった。

■ 経営者の視点

小規模企業のため、経営者自身が情報セキュリティの責任者となって対応している。ISMS 認証取得は、従業員全員で取り組んだことで成功したと感じている。情報セキュリティについては、情報セキュリティ対策費用のみで捉えるのではなく、経営計画の時点から企業全体の方針や戦略として捉え、情報セキュリティ投資を進めることを考えている。
DoS 攻撃や標的型攻撃は、常に、あるものであり、さらに、新しい手口で攻撃されてくるので、「これで万全」と考えず、リスクがあると考えて対応する必要がある。ISMS 認証取得がゴールではなく、今後もさらに、情報セキュリティ対策を実施し、より強固な情報セキュリティ体制を確立していきたい。

事例 43

所在地	香川県
業種	情報通信業
従業員規模	51～100 名
事故の有無	無

プライバシーマーク取得の効果は個人情報のセキュリティ確保だけではなく業務の効率化につながった

■ 情報セキュリティ対策に取り組むきっかけ

当社は、香川県で官公庁、病院、介護施設、給食会社、食品会社、学校、幼稚園等向けの栄養管理、給食管理のパッケージソフトウェアを開発販売している。かつて官公庁の入札に参加するには当社の代理店がプライバシーマークを取得していればよかったが、2012 年から自社での取得が必須となり、これをきっかけに当社もプライバシーマークを取得した。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- プライバシーマークの取得に取り組む過程でセキュリティ体制の構築を進めた。執務フロアや施設への入退出制限や情報の保管場所の施錠、機器や記録媒体の持込・持出制限、ログやファイル情報に基づく監視等の設備、運用体制の構築を図るとともに、情報セキュリティに関する定期的な内部監査を行っている。これらの対策は、入退出設備の改修やウイルス対策ソフトの導入への投資を除き、Windows Server 等の基本的なセキュリティ機能を用いて実現している。またソフトウェア会社である強みを活かし、当社独自のツールを開発することでも業務の効率化を進めた。
- プライバシーマークの運用状況の確認は通常 1 ヶ月単位で十分であるが、当社は 1 週間単位で実施し、日報とともに、管理票を PDF 形式にて本社にメールで送信することを義務付けている。従業員の負担は大きくなるが、セキュリティへの意識向上が運用のポイントと考え、あえて報告頻度を高くしている。従業員は導入当初、慣れない作業に相当な苦労もあったかと思うが、入札資格を満たしセキュリティを強化するために必要なことと自覚し、プライバシーマークの取得と運用に協力してくれた。管理すべき項目は増えたが、継続的な業務の見直しと、必要な記録を作業記録から自動生成させるなどの効率化の工夫と組み合わせて積極的に取り組んだ結果、現在はこれらの活動が習慣化している。
- IPA 等から公表される情報や教育資料を社内に周知さることで、セキュリティに関する継続的な学習を促している。こうした教育の効果については、年に 1 度テストを実施して確認している。

■ 取り組みによる効果

プライバシーマーク取得が業務を見直すきっかけとなった。業務が全体的に効率化されたことで、以前と比べて残業時間が減り退社時間が早くなるなどの効果も出ている。クリアデスクポリシーの徹底、書類等の置き場所のルール化等により、社内の整理整頓が行われたことも業務の効率化につながっている。また、以前は開発現場で作成した記録や報告書に必要事項の記入漏れや内容の不足が見受けられた。プライバシーマーク取得後は開発現場で行う作業の意義、予想されるリスク、必要な記録は何かを従業員が考える習慣がついたことで、訪問記録や報告書の品質向上に結びついているように感じる。

■ 経営者の視点

セキュリティ対策のための設備やソフトウェア等の導入よりも、従業員一人ひとりの意識が大事である。この考えを徹底して従業員に教えていくことが、情報セキュリティ対策を導入し、運営していく上でのポイントと考えている。定期的な見直しが必要とはいえ、現状において個人情報のセキュリティ確保を目的とする体制の運用は順調である。しかし、今後従業員の増加等により管理が行き届かなくなる可能性はある。従業員が一定数を超えた段階で、全体的な視点でセキュリティを見直し、ISO27000 等の管理システムの導入が必要と考えている。

事例 44

所在地	佐賀県
業種	情報通信業
従業員規模	5 名以下
事故の有無	無

インターネット上のリスクや最新技術の動向を常に把握 セキュリティ強度を高めることで外部評価を獲得

■ 情報セキュリティ対策に取り組むきっかけ

当社は、佐賀県でインターネットサービス事業を基盤として、ホスティングサービスの提供、コンテンツ制作やネット通販事業を展開している。顧客の情報コンテンツやシステムを預かるため、情報漏えいを起こさないための仕組みや、数多くのアクセスに対応できる安全なネットワーク及び情報セキュリティシステムを構築する必要性を認識している。具体的には、インターネットデータセンターとの連携による 365 日 24 時間体制でのセキュリティチェックや、各種セキュリティソフトやネットワークツールの導入等、また、情報セキュリティに関する社内規程等の制定・遵守等も実施し始めた。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 情報セキュリティに関する社内規程等を遵守し、チェック体制等が曖昧にならないような従業員教育を行い、情報セキュリティに対する意識の向上を図っている。
- 自社ウェブサイト運営に関しては、ウェブサーバに対するハッキング等の不正アクセスが多いため、顧客でもある関係機関（官公庁）と連携した情報共有体制を構築しており、サイバー攻撃等の情報交換を逐次実施している。
- 一般顧客へのウイルス対策として、スキャン等による発見と通知を実施しており、改善率も上がっている。
- また、サポートデスクを設置してセキュリティ等に対する相談窓口を開設している。セキュリティトラブルが発生した場合は、駆けつけ支援等も対応している。

■ 取り組みによる効果

- セキュリティ強度の高いサーバを提供しており、官公庁から高い評価を得ている。特にサイバー攻撃に対する取り組みが評価されており、この管理体制、信頼性が当社の強みとなっている。
- 1 回のトラブルが顧客からの信頼を損ねる結果となるので、高度な暗号化やセキュリティ度が高いチェックシステムを導入している。使いづらさ等の指摘もあったが、現在は、安心・安全を提供しているとの評価を得ている。

■ 経営者の視点

どんなにセキュリティ対策を実施していても、ネットワークにつながっている以上、あらゆる問題が出る可能性があると認識しており、アンテナを高く張り、最新技術や動向等の情報を収集している。また、メーカーから様々なソリューション提案等を受けており、プライバシーマーク等の費用がかかるものには、体力的に可能な範囲で対応していく予定である。ただし、ハードウェア・ソフトウェア等のバージョンアップ等には逐次対応しており、監視についても継続して実施する。顧客である一般の企業では、セキュリティソフトの更新忘れ、アカウント名やパスワードの不備が多く見受けられ、情報リテラシーに関する情報収集や教育の場をもっと活用していく必要があると考えている。セキュリティに関するレベルアップは、単なる知識習得ではなく判断する部分のレベル向上が今後の課題だと思っている。リーダー的な従業員を講習会等に極力参加させ、他の従業員へフィードバックさせるようにしていきたい。

事例 45

所在地	沖縄県
業種	情報通信業
従業員規模	21～50 名
事故の有無	無

万が一の事故やトラブルを具体的に想定し、対応策を検討
ISMS 取得後も従業員の知識習得と意識醸成を強化

■ 情報セキュリティ対策に取り組むきっかけ

当社は、沖縄県で IT 関連機器や情報通信システム、ネットワークシステムの設計・構築・保守を幅広い業態・業種向けに行っている。世間の情報セキュリティ事故やサイバー攻撃の脅威、ビジネスニーズを背景に情報セキュリティ対策に力を入れて取り組むようになった。ビジネスニーズにおいては、公的機関のシステム調達案件仕様で求められている情報セキュリティ要件を満たすため、ISMS やプライバシーマーク認証取得に取り組むようになった。また、取引先からの業務委託を受ける際に、取引先と同等の情報セキュリティ要件を満たすよう要求があり、作業者の情報セキュリティ教育の実施・教育結果報告が必要になっている。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 情報セキュリティ対策を取り組むにあたり、検討する範囲が広く、どこからどうやって対策を講じたらよいか悩みがあった。そのため ISMS の考え方を基準に当社が、どのように情報セキュリティ対策を行うべきかを整理していった。ISMS の内容理解や、対策の方向性に誤りがないかコンサルタントに相談し、順次対策に取り組んだ。
- 新しいリスクの発生や対策範囲の広さから、情報セキュリティ対策に万全はないと認識しており、自社の事業規模に応じた対応の優先順位をつけ順次取り組みを行っている。技術的対応として 2016 年に UTM を導入し、不正侵入対策を行っている。人的対応としては、従業員に対し情報セキュリティテストを実施し合格点に達するまで、何度でもテストを実施し情報セキュリティ知識や意識を高めるようにしている。

■ 取り組みによる効果

- 情報セキュリティ対策の効果については、経営的な数値で表すことは難しいと考えている。情報セキュリティ対策を実施し、万が一情報セキュリティ事故が起こった時の事業損失を最小限に抑える必要があることを経営層や従業員に認識してもらえた。一般的に中小企業においての各種取り組みは、費用や人的リソースの制約があり性善説で行われることが多いが、情報セキュリティ対策への取り組みを行うようになってからは、会社がチェックする仕組みができ上がり、不正に対しての抑止効果、教育により事故を起こさせない効果があった。
- 社外からの評価として、ISMS 及びプライバシーマーク両方の認証取得がされている安心感の声があった。

■ 情報セキュリティ担当者の視点

情報セキュリティ対策のソリューションを導入するだけでは、報セキュリティ事故は防げない。従業員の情報セキュリティに関する知識・意識が重要であると考えており、今後は情報セキュリティ対策に関する社内人材育成に力を入れていきたい。情報セキュリティ対策意識の高い従業員はまだ一部である。規程に書かれていること以外にも、高い情報セキュリティ対策意識をもって判断・行動できる従業員や情報セキュリティに関する内部監査が相互にできるレベルの従業員を多く育成していきたい。また、退職者の情報セキュリティリスクについて、検討を開始している。悪意を持っていれば情報セキュリティ対策を潜り抜けるため、きりのない対策となる。予想されるシナリオと対応策を経営層と話し合っており、必要な対策を見極めていきたい。

事例 46

所在地	愛知県
業種	運輸業
従業員規模	21～50 名
事故の有無	無

セキュリティ対策が取引先から評価され好条件で受注
業界全体のイメージアップを目指して対策に取り組む

■ 情報セキュリティ対策に取り組むきっかけ

当社は、愛知県で積載車を持たない自走陸送会社で、登録代行業務、ディーラー整備工場回送業務、駐車代行業務等を BtoB、BtoC で行っている。当社が管理する情報は、顧客情報、従業員の個人情報、取引先から提供される個人情報、業務上の機密情報などが数千件に及び、日々増えている。これまで当社においては情報漏えい等のセキュリティ事故は起きていないが、毎日のように情報漏えいの事故・事件のニュースに接し、また大手取引先（リース会社）から、情報漏えい対策を喚起されたことあり、企業イメージアップを兼ねて何らかの情報セキュリティ対策をしなければならないと認識し、対策に取り組むこととした。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 情報関連業務で 20 年以上の経験を有する役員が IT 担当者となり、自身でインターネットによる情報収集を行うとともに社労士の支援を得て、就業規則等に企業情報の扱いを規定し、社内研修において従業員に周知している。研修は本社内で行っているが、本社に出向くことが困難な遠方の営業所の従業員には、当社所有の大型バスを改造し、車内にパソコン等を設置して研修ができる環境を整備した上で、営業所での「出前研修」を実施するなどにより、従業員全員への意識徹底を図っている。
- 当社が保有する情報については当初、業務担当者のそれぞれのパソコン内で運用保管していたが、データサーバに集約し、情報の共有と安全対策を図るようにした。しかし、自社サーバに対するサイバー攻撃が懸念されるため、社内システム内のデータも含めてクラウドへの移行を検討中である。

■ 取り組みによる効果

当社で実施している情報セキュリティ対策が大手取引先（リース会社）から評価されつつあり、以前は委託料の安さが一番の条件であったが、現在は他社より割高なケースにおいても受注できるようになっている。
また、社内においてこれまで情報セキュリティに関する事故は発生していない。

■ 情報セキュリティ管理者の視点

当社の事業アピールとして、「日本一の品質、顧客の安心」を掲げている。これを実現するにはコンピュータにおける対策を外すことができず、安心は情報セキュリティ対策を行うことであると認識している。
自社ウェブサイトの作成は外部委託であるが、社内システムは市販のパッケージとオフィスアプリケーションをもとに IT 担当者の内製により構築している。今後の事業展開を考えると、IT 関連の情報提供を求めることができ、開発を依頼できるような業者とともに連携していきたい。
情報セキュリティ対策が当社の評価・信頼アップにつながり、いずれは業界全体のイメージアップになれば、ドライバーが若手のあこがれの職業となり、現状の人手不足を解消できるのではと期待し、今後も情報セキュリティ対策に取り組みたいと考えている。

事例 47

所在地	広島県
業種	運輸業
従業員規模	101～300 名
事故の有無	無

内部統制の一環として情報セキュリティ対策を強化
従業員のリスク意識向上のための啓発活動も重要

■ 情報セキュリティ対策に取り組むきっかけ

当社は、広島県を中心に法人向けの運送・倉庫業務と個人の引越し業務など物流業務全般を行っており、全国に営業所を展開している。社内情報システムは本社にサーバを置き各拠点から VPN によりアクセスを行えるようにしている。情報セキュリティに関しては以前から行っていたつもりだったが 2010 年頃、当時在籍していた従業員が P2P の技術を利用したファイル共有ソフトである Winny を社内のパソコンで利用していたことが発覚した。幸いそのことによる被害はなかったが、同時期に親会社が内部統制の見直しを行うこととなり、その一環として社内のパソコンなど IT 機器の管理や監視が強化されることとなった。そして情報セキュリティに関する社内規則の制定を行い資産管理やアクセス制限、ウイルス対策など情報セキュリティ対策に投資を行った。また、2011 年の東日本大震災による営業所の被害をきっかけにデータバックアップの重要度を認識し、本社サーバへ各拠点のデータバックアップを行う仕組みを導入するなど物理的な BCP 対策を行い始めた。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 法人だけでなく個人の情報を扱っていることや事業拠点の増加がある中、内部統制の一環として策定された情報セキュリティに関する社内規則をもとに IT 資産管理を徹底している。インターネット回線には UTM を導入して不正侵入防御を行い、各パソコンにはウイルス対策ソフトを導入し、それらの状況は委託している管理会社からレポートが届き確認している。また従業員にはスマートフォンを除く IT 機器の持ち込みを原則として禁止するとともに社内での Wi-Fi 利用を行わないなど、無線での接続はできないようにしている。サーバへのアクセス権は一部の責任者のみとしており、ネットワークを物理的に分けている。サーバルーム入口とサーバラックの両方に鍵を掛け、容易にサーバへアクセスができないような仕組みとしている。さらに各拠点から集めたデータをストレージに定期的にバックアップし耐火金庫に保管するなどセキュリティ対策とともに BCP 対策を行っている。
- ウェブサーバは外部業者が運用するレンタルサーバを利用しており、社内ネットワークには一切関係がない。またウェブサイトは全ページ SSL 化により問合せデータの通信経路途中での流出防止などのセキュリティ対策も行っている。
- マイナンバーの取り扱いは限られた者だけが行えるようにしており、専用の耐火金庫で管理保管している。

■ 取り組みによる効果

可能な限り物理的な対策を行っていることもあり、今までウイルス感染やネットワーク攻撃などの被害や情報漏えいは確認されていない。また、内部統制の一環として親会社からの監査が入るため、その時に指摘された点は改善している。企業だけでなく個人の情報も扱っているため、情報漏えいを起こさないように今後もできる部分から対応をしていく考えである。

■ 情報セキュリティ担当者の視点

経営層の理解は得られているが、一方で情報セキュリティに関する費用の圧縮を行いたいという要求もある。可能であれば各パソコンからのインターネットの利用制限をしたいが業務効率の観点から行う訳にはいかない状況である。情報セキュリティをより高めるためには物理的な対策だけでなく従業員一人ひとりの意識にかかっている。そのため従業員のリスク意識向上のための啓発など教育について検討していきたい。

事例 48

所在地	山形県
業種	小売業
従業員規模	21～50 名
事故の有無	無

事業環境の変化、社会的要請に応えるため取り組みを開始
従業員の意識が向上し、さらにレベルアップを目指す

■ 情報セキュリティ対策に取り組むきっかけ

当社は、山形県で個人情報を取り扱う必要のある医療機器を販売している。昨今の社会的要求に沿って、情報セキュリティ対策に取り組んできており、これまで直接的な被害に遭遇したことはないが、これまでの対策で十分とは言えず、従業員の IT リテラシーも決して高いとは言えない状況にあった。当社で扱っている医療情報などが記載された個人情報は万が一にも流出してはならないので、これまで紙媒体で交換していた。しかしながら、IT 化の広がりのもと、電子媒体での交換を見据えた情報セキュリティが必要不可欠として、対策を講じることとなった。

■ 主な取り組み内容

組織的 | 人的 | **物理的** | **技術的**

- 情報セキュリティ対応の機器、インフラ、ソフトを導入し、企業として必要な対策を行っている。十分なものとは言えないが、過度な投資はできず、企業体力とのバランスを取りつつ、従業員の IT リテラシー向上に合わせ、順次対策を充実させようとしている。
- 社内での情報共有のために顧客管理システムを導入しており、同システムにおいて情報へのアクセス可能者の限定、格納データの暗号化、通信路の暗号化、USB 媒体の接続禁止等の対策を行っている。
- 一部の個人情報においては、社内の安全管理措置が十分と認められないことから、信頼でき、かつ適切な情報セキュリティサービスを提供している専門業者に管理を移管している。

■ 取り組みによる効果

- 以前はパスワードをメモに残すなど、セキュリティ意識の低い従業員も見受けられたが、会社として情報セキュリティ対策に取り組んでいる姿を見せることで、従業員の情報セキュリティに対する意識が確実に向上している。
- 対外的には、情報セキュリティ対策は行っているのが当然のことであり、アピールすることでかえって不信感を与えることも懸念される。ビジネスを継続させる上で当然のこととして取り組んでいることもあり、これらの活動によって、取引が増えるなどの効果は生じていない。ただし、対策を行わないことで失われるものはあると考えている。

■ 情報セキュリティ担当者の視点

企業の特性によって IT の活用内容も様々であり、情報セキュリティ対策をどこまで行えば十分といった指針が見えにくく、必要な費用の想定が難しい。相談できる企業を見極めながら、企業体力や保有スキルに合ったバランスの取れた情報セキュリティ対策を導入したいと考えている。また、スマートフォン、タブレットなど情報端末が多様化しており、その利用シーンもますます拡大すると見込まれる。今後は、それらの活用と制限をどのようにバランスさせるかを課題とし、取り組んでいきたいと考えている。

事例 49

所在地	山口県
業種	小売業
従業員規模	5 名以下
事故の有無	無

事故の発生経験はないが油断せずに対策に取り組む
従業員に対する情報セキュリティ教育の実施が課題

■ 情報セキュリティ対策に取り組むきっかけ

当社は、山口県で刃物・錠前や鍵・厨房用品・工具の販売、取り付け、メンテナンスを行っている。今までウイルス感染等の直接的な被害を受けたことはないが、メディアや関連機関から情報漏えいやウイルス感染被害等のニュースや、情報セキュリティ対策の必要性の喚起が頻繁にされており、当社においても重要情報（顧客情報、営業・技術情報）を漏えいさせないためには、無防備・無対策ではあってはならないことを認識し、必要な対策を実施し始めた。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- ウイルス対策ソフトの導入や電子メールソフトの選定などの技術的な対策、ならびに重要情報の管理方法など運用面での対策の 2 種類が挙げられる。
- パソコンにはウイルス対策ソフトの導入や、フィルタリング機能が強化された電子メールソフトの使用などの対策をしている。さらには外部からの攻撃によって被害を受ける可能性を最小限にするために、インターネットに接続できるパソコンの限定と、最重要情報はパソコン内には保管せず、紙ベースで取り扱い、施錠管理を原則とする運用を行っている。
- 社内における情報セキュリティ責任者を明確にし、情報セキュリティに関する相談や情報収集の窓口を一本化することで、情報セキュリティ対策の実施状況の一元的な把握と情報の共有化を図っている。
- 日常から情報セキュリティ関連の話題を取り上げることで、従業員の情報セキュリティに関する意識の向上を図っている。

■ 取り組みによる効果

- ウイルスへの感染はもとより、顧客情報をはじめとした重要情報の漏えいも発生したことがなく、顧客からの信用を得ることができている。
- 小人数の組織であるが、情報セキュリティ責任者を中心に、情報セキュリティ対策の共有化ができており、従業員の情報セキュリティに関する意識も着実に向上している。

■ 経営者の視点

情報セキュリティ関連の取り組みを徹底するには、情報セキュリティ責任者だけではなく、従業員全員が情報セキュリティに関するスキルやリスク意識を向上する必要があり、情報セキュリティ教育をどう実施していくかが課題と考えている。
今までウイルス感染等の被害が発生したことはないが、油断することなく、自社の身の丈にあった情報セキュリティ対策を実施していきたい。

事例 50

所在地	北海道
業種	金融業
従業員規模	101～300 名
事故の有無	無

積極的なセキュリティ投資と IT 人材育成に注力
行政、金融機関、取引先からの信頼獲得を実感

■ 情報セキュリティ対策に取り組むきっかけ

当社は、クレジットカードに関する事業を営んでいる関係で、個人情報の取り扱いを最重要課題と捉え、2009 年にはプライバシーマークを取得している。また、2020 年の東京オリンピック・パラリンピックに向け、インバウンド需要を取り込むことに資するため、行政の指導のもとに、より一層、安全・安心なクレジットカード利用環境を整える準備を進めてきた。そのような中、2014 年に同業他社における情報漏えい事件をきっかけとして、第三者委員会による評価のもと、当社の個人情報保護体制を再度見直す必要に迫られた。具体的には、情報セキュリティに対する組織的な取り組み、物理的セキュリティ、情報システム及び通信ネットワークの運用管理、情報システムのアクセス制御及び情報システムの開発、保守におけるセキュリティ対策といった観点から、十分な体制を構築する諸施策を推進していくこととなった。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- プライバシーマークを取得後、ISMS の取得も検討してきたが、現在はクレジットカード業界における情報セキュリティ対策のデファクト標準である PCIDSS の取得に向けて準備を進めている。同標準は要件として、「ネットワークやアプリケーションのペネトレーション・テストの回数や実施時期」「パッチリリース後 1 ヶ月以内の適用」「6 回ログオンに失敗した場合のロックアウト」「クライアントパソコンへのパーソナル・ファイアウォールのインストール」等といったかなり厳しい内容であり、取得に向けて専門のコンサルタントに依頼して取り組んでいる。
- 物理的セキュリティ対策としてはこれまでのセキュリティカードによる入室から、入退出のチェックまで行うようにし、さらに、バイオメトリクス認証（生体認証）の一つである静脈認証まで行うようにした。
- 情報ネットワークの見直し、運用体制の見直しを行い、また、組織的な取り組みの一環として情報セキュリティマネジメント試験の受験を会社として推奨し、現在 4 名の合格に至っている。また、毎年、社内の研修で情報セキュリティに関する教育も継続的に実施している。

■ 取り組みによる効果

上記取り組みを全社的に行ってきたため、従業員のセキュリティに対する意識が確実に高まってきている。従業員のモチベーションも上がり、IT 人材、セキュリティ人材も育成されてきた。物理的対策としての入退出チェックの強化により、導入直後に多少の混乱はあったものの、これまでの経験により想定していた内容で従業員も運用に対する理解を示してくれた。対外的には PCIDSS の取得準備を進めていることで、行政、金融機関、取引先から評価され信頼を築くことができ、間接的ではあるが、投資に対する費用対効果は十分あったものと実感している。

■ 経営者の視点

今後は運用監視のシステムを導入し、ログの監視及び改ざん防止、ファイアウォールの強化、暗号化ソフトの導入等、技術的な側面からの強化を図っていく予定である。また、人材育成にも力を入れ、兼務ではあるが、自社で運用できるための環境を整えていきたい。さらには、BCP の観点からも対策を行い、より一層、顧客の信頼を得ていきたいと考えている。

事例 51

所在地	青森県
業種	金融業
従業員規模	21～50 名
事故の有無	無

内部と外部、双方の視点で実施状況を点検
情報セキュリティレベル向上のために人的ミスの防止を図る

■ 情報セキュリティ対策に取り組むきっかけ

当社は、青森県で保険代理業を営んでおり、保険加入者の情報を多数取り扱っているため、契約保険会社（生命保険、損害保険）からの強い指導で情報セキュリティに関する社内規程を整備し、セキュリティを考慮した情報システムを使用している。社内に、保険代理店専用サーバ、総務用サーバ、社内イントラ（ファイル共有、コミュニケーション）サーバを保有し、複数店を VPN で接続している。また、ベネッセ事件をきっかけとして USB 管理、ファイル共有ソフト、メールの取り扱い等のセキュリティ対策を強化した。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

2014 年に市内の IT ベンダに依頼し、セキュリティを考慮した VPN ネットワークシステムを構築した。その際、インターネット接続部分にファイアウォール、ウイルス対策ソフト、メールチェックシステム、1 年分のシステムログ保有など基本的なセキュリティ対策を取り入れた。また、保険会社のシステムへの接続時は OS、ソフトウェア等のバージョンチェックが自動的に動作するようになっている。ファイルへのアクセスは、権限設定を実施し、機密性を保っている。保険会社の指導により、保険取り扱い社内研修等でコンプライアンス、情報セキュリティ教育を実施している。また、対策の実施状況の自主点検を行うほかに、保険会社からの定期的な点検も行っている。営業用に使用する外部持ち出しパソコンは、情報の記録を禁止しシンクライアント使用とし 2 重パスワード設定、持ち出し記録管理を徹底している。情報システムの導入、セキュリティ対策対応では、社内に詳しい従業員がおらず、市内の IT ベンダからアドバイスを受けながら構築した。

■ 取り組みによる効果

- 目に見える効果は感じていないが、ベネッセ事件等の影響後保険会社からの強い指導、社内での取り組みにより、セキュリティ対策は当たり前の意識が定着しており、セキュリティ事故、事象はない。
- セキュリティ対策は当たり前の意識が定着しているため、対策実施による社内からの不満などもなかった。
- 業界としてセキュリティ対策は当然のこととなっておりビジネス的なメリットは特ににない。

■ 経営者の視点

当社は、保険関連の顧客情報が重要な情報資産であるが、現状では保険会社が要求するセキュリティ対策はできている。しかし、人のミスによる漏えい、標的型攻撃メールへの対応に不安がある。対策向上のために必要なこととして、従業員のさらなる情報セキュリティ意識の向上、企業内の体制整備がある。情報システムでのセキュリティ事故はないが、紙媒体の誤廃棄（シュレッダー）などのケアレスミス等があり、人的ミスの防止が課題である。たとえ、システムに対する情報セキュリティ対策が万全でも、システムを使う人の情報セキュリティ対策に対する意識が低ければ、意味をなさないため、今後はセキュリティ関連ツールとセキュリティ関連ルールのバランスを取った展開をしていきたい。

事例 52

所在地	岡山県
業種	金融業
従業員規模	21～50 名
事故の有無	無

情報セキュリティにおいてキーとなるのは「人」社内のすべての人がその重要性を認識することが第一

■ 情報セキュリティ対策に取り組むきっかけ

当社は、岡山県で投資信託運用を中心とした事業を実施している。個人情報を直接扱うことはないが、金融という性質上グループ内の情報セキュリティに対する要求はもともと厳しく、いち早く業務規程の整備やウイルス対策、ファイアウォールの設置など基本的なレベルのセキュリティ対策を行っていた。そのような中、2013 年頃に監督官庁の監督指針が改正され、より高度な情報セキュリティ対策が求められることとなった。そこで、指針に準拠する形で対策レベルを高度化することとなり、事務所の移転に合わせて ID ドアの設置やセキュリティツールの導入等の対策を充実させるようになった。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- セキュアな運用が要求される基幹業務系ネットワークとインターネット接続が必要な情報系ネットワークを分割しており、基幹業務系はインターネットに接続しないことでセキュリティを確保している。また、サーバへのアクセスに関しては情報をレベル分けして担当者毎にアクセス権限を設定し、管理している。
- 業務上、可用性、完全性が特に重視されるシステムでは、BCP サイトとしてバックアップシステムを維持した上で、毎年業務実行訓練を実施している。
- 昨年、初めての試みとして情報セキュリティを専門とするコンサルタント会社に委託して社内の情報セキュリティ対策の診断を実施した。その結果、いくつかの脆弱性、改善すべき点の指摘も受けたので、対応を行っていく。
- 情報セキュリティ対策を行っていく上で、従業員への意識付けは大きな課題と認識している。各種規程や IPA の映像教材を共有フォルダに置いて参照や視聴を促している。

■ 取り組みによる効果

- 以前は技術的対策面等で専門業者に任せきりの部分があったが、社内での取組のレベルアップによって、業者とディスカッションしながらより良い仕組みの構築が行えるようになった。
- 規程の整備や教育などで従業員の意識が高まり、日々の業務運用の中での情報セキュリティ対策が普通のこととして認知されつつある。その結果、ヒヤリ・ハットレベルの事象も見逃されることなく責任者に報告されるようになった。
- コンサルタントの指摘により、今後、セキュリティレベル向上のために実施すべきことが明確になった。

■ 情報セキュリティ担当者の視点

地方企業にあってはスキルを持つ人材の確保も難しい。そこで、社内に複数のキーマンを育成すべく、情報セキュリティマネジメント試験へのチャレンジを推奨している。また、昨今のサイバー攻撃の高度化に対し、今後は侵入検知や異常発見、影響を最小限に止める封じ込め等の対策にも注力していきたい。

やはり情報セキュリティにおいてキーとなるのは「人」であり、経営者から従業員一人ひとりに至るまですべての人がその重要性を認識することが第一である。さらに最新の情報をキャッチする仕組みを持つことも重要である。IPA のサイトや各種ソースを活用して新たな脅威や対策の情報を敏感に収集することを心掛けたい。

事例 53

所在地	福岡県
業種	金融業
従業員規模	101～300 名
事故の有無	無

セキュリティ対策は企業を守るツールへの投資
情報漏えい事故は会社の存亡に関わる脅威

■ 情報セキュリティ対策に取り組むきっかけ

当社は、福岡県で不良債権の買取・管理・回収及び担保不動産の処分の受託業務を展開している。設立当時はインターネットが一般に浸透し始めた頃で、セキュリティについての関心はあまり高くなく、ファイアウォール、ウイルス対策ソフトによる自己防衛程度であった。2005 年頃に大幅な組織統合があり、取扱商品の幅が広がったことから、情報インフラの再整備を図ることになった。その際、ハッカーによる侵入や個人情報の保護などが今後重大なテーマになってくると考え、独自のセキュリティポリシーを策定し、大規模なセキュリティ投資を行った。入退室管理システムの導入、盗難防止・自社サーバ保護のために鉄製ドアへ交換するなどオフィス環境を整備し、堅牢なファイアウォールによるネットワーク構築、高度なセキュリティソフトを導入するなど、ハード、ソフト両面でできる限りの対策を講じていった。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 初期のシステム構築から携わっている IT 責任者 2 名がセキュリティポリシーに則り、システムの運営・管理をしている。部署毎にコンプライアンスの勉強会を月 1 回定期的に開催し、個人におけるセキュリティ対策についてもこの中で取り上げている。2016 年には標的型サイバー攻撃の模擬訓練を実施した。
- パソコンには入退室 IC カードによるロック／アンロック機能を導入しており、退出時にカードを抜くと、自動的にロックがかかる仕組みになっている。またパソコン毎にインターネットの閲覧制限やシステムへのアクセス制限をかけているほか、文書やメールの暗号化、CD、DVD への書き込み制限ができるソフトを導入し、情報漏えいを防止している。さらに USB メモリをパソコンに差し込んだ時点で日時や操作が記録され、IT 責任者が 1 ヶ月毎にログの内容を報告している。
- 毎日のデータをストレージサーバにバックアップ、また毎週金曜日には支店が入居している系列銀行内のサーバへその情報を転送し、二重のバックアップ体制をとっている。これによって火災等、万が一の事態にあってもデータの消失を免れ、拠点間でもデータが共有できるようになっている。

■ 取り組みによる効果

- IT 責任者がリーダーシップをとってセキュリティ対策を推進することにより、トレンドにあったセキュリティ対策を講じており、現状、十分な対策ができていると思っている。
- 定期的なコンプライアンス勉強会やサイバーセキュリティ演習会などを通じて、従業員一人ひとりが高いセキュリティ意識を保持している。一方で標的型サイバー攻撃の模擬訓練メールを、対象従業員に送信したところ、ファイルをクリックした従業員が数名いたため、再度注意喚起を促した。

■ 情報セキュリティ担当者の視点

いくら業績を伸ばしても、一度の情報漏えいで会社がひっくり返る可能性は十分にある。セキュリティ対策は企業を守るツールであるため、経営者は「利益を生まないソフトやシステムは買わない」と考えるのではなく、セキュリティ対策は投資と考えるべきである。そのためには、信頼できる業者を選び、自社にあった投資をしていくのが良いと思う。今後、Windows10 に対応したシステム移行が課題として残っており、必要な投資に対する経営者の理解を促進する予定である。

事例 54

所在地	熊本県
業種	金融業
従業員規模	51～100 名
事故の有無	無

経営トップの判断で情報セキュリティ対策を実施
金融業界では情報セキュリティ対策はやって当たり前

■ 情報セキュリティ対策に取り組むきっかけ

当社は、熊本県でクレジットカードの発行から代金回収、及び銀行・住宅ローンの信用保証事業を中心に業務を行っている。個人情報保護法の制定と自社で扱う情報の増加をきっかけとして、経営トップの判断で情報セキュリティ対策を行うこととなり、コンサルティング会社に調査を依頼したところ、パソコンを共有のパスワードで運用している例など 100 以上の指摘を受けた。その改善を行うと同時に 2010 年に ISMS とプライバシーマークを続けて取得した。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- セキュリティに関して「内部管理室」という部署を作り、常務取締役を管理責任者にし、トップが常にチェックできる体制を構築した。また、各部の部長及び課長を集めて「情報セキュリティ運営委員会」を作り、毎月集まって社内の情報セキュリティについて議論を交わすようにした。
- 全社的な定例教育において年 1 回 10 問程度のテストを実施し、理解度を確認している。回答率 8 割以上を合格とし、不合格の場合は再試験を受けるよう求めている。テストの問題は、プライバシーマーク取得事業者向けの研修から抜粋し独自に作成している。
- USB メモリの利用は許可制で、取締役でも承認を受けなければならない。USB メモリが利用できる機器は特定されているので、インシデントが発生した際も追跡しやすい。USB メモリの媒体管理簿は監査対象になっている。
- 以前は従業員に電子メールの使用を許可していなかった。現在も電子メールの使用者は限定されているので、従業員にとってはあまり制限がかかっているという認識はなく、それが当たり前のように進められている。

■ 取り組みによる効果

- 従業員に個人情報の重要性を認識する文化が根付いているため、トラブル等はなく自然と取り組んでいった。
- 取引先などから時々情報セキュリティへの取り組みについて問合せがある。業界の特性上、「やって当たり前」という状況であるが、一定の評価を得ている。

■ 経営者の視点

経営トップは現状に満足している。ただし、現場の業務負担が大きいところがあり、可能なものは簡素化して従業員の負担減を目指している。経産省の方針で 2018 年 3 月までに PCIDSS に準拠するよう求められており、重荷ではあるが 2020 年のオリンピックに向けて安心、安全なキャッシュレス社会を迎えることができるように全社をあげて取り組むことを検討している。従業員の作業負担、高額な導入・運用費用の捻出が大きな課題である。
グループウェアで Flash Player を使っており、その脆弱性をついてくるウイルスに困っている。IPA のサイトで情報を収集しながら対策を検討、実施している。また業務システムは OS に依存しているので、OS のバージョンアップもできない。
PCIDSS に準拠するために、この辺りをベンダと一緒に今後見直す予定である。

事例 55

所在地	三重県
業種	不動産業
従業員規模	6～20 名
事故の有無	無

朝礼を活用して従業員に呼びかけ「個人情報はお金と同じ価値がある」として情報管理を徹底

■ 情報セキュリティ対策に取り組むきっかけ

当社は、三重県北部で住宅建築や不動産賃貸、エネルギー設備工事などの事業を展開している。近年、個人情報の漏えいに関する事故のニュースを見る機会が多くなり、また近隣では、「ランサムウェア」の被害にあったという企業の話も聞いている。当社は、大家さんのマイナンバーや入居者の個人情報などを管理しており、マイナンバー法や個人情報保護法への対応が必要となっている。こうしたことからも、情報セキュリティ対策の重要性を認識し、順次対策を進めてきた。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- ウイルス対策ソフト及びセキュリティ管理システムを導入し、機器やソフトウェア資産の一元管理をしている。運用管理を支援し、より安全な情報漏えい対策の実現を目指している。従業員教育では、朝礼を利用して、他社の情報漏えい事件などを取り上げ、注意喚起を行っている。
- 情報セキュリティ管理システムは、個人情報を取り扱う業務が多いことから、顧問 SE と相談し導入を決めた。このシステムは、個人情報（データ）の操作履歴等の証跡を記録・保存している。収集した証跡は、役員が確認を行っており、情報管理の状況を把握できる体制となっている。
- マイナンバーは、インターネットを介した漏えいや電子データによる大量流出などのリスクを最小限に抑えることが必要と考え、基本的には紙媒体での運用と耐火金庫での保管を徹底している。
- パソコン上のＣドライブからのデータ漏えい、紛失を防ぐ目的で重要情報はサーバ上に保存することとしている。サーバのバックアップは、外部バックアップセンターを利用し、３段階のサイクルで実施するとともに、フォルダへアクセス権限を設定し、情報の共有範囲を必要最小限にとどめている。

■ 取り組みによる効果

- システムの導入や環境整備などを進めることで、従業員には個人情報がお金と同じように価値のあるもの、重要なものであるとの意識が根付き、情報管理を徹底することができている。また、証跡の取得・監視により、管理者から適切な注意・監督が行うことができるため、従業員の規範意識も高まり、責任ある行動をとるようになった。
- セキュリティ管理ソフトの導入にはコストがかかるが、インターネット社会では自社の信用力が重要であるため、今後はこの強みを営業活動などに活かしていく。

■ 経営者の視点

個人情報など当社にとって重要な情報の受け渡しには、FAX や郵送などの通信手段も用いるため、今後も情報漏えい事故が発生しないよう取り組んでいきたい。そのためにも従業員教育がさらに必要と考えているが、県内では情報セキュリティ関連の研修会が少ないため、人材育成が課題である。朝礼での呼びかけのほかにも、外部講師による勉強会の検討や他社の取り組み事例なども参考にしていきたい。

事例 56

所在地	大阪府
業種	不動産業
従業員規模	6～20 名
事故の有無	無

セキュリティ対策が取引条件となったのを契機に情報セキュリティ・マネジメントシステムを構築

■ 情報セキュリティ対策に取り組むきっかけ

当社は、大阪府で不動産業とマンション管理業を営み、顧客の福利厚生施設である借り上げ住宅の管理業務等を行っている。顧客から発注上の必須条件として、情報セキュリティ及び個人情報の管理について要求されたことが情報セキュリティ対策に取り組む直接のきっかけである。これを機に他の顧客にも同様のニーズがあると判断し、情報セキュリティ・マネジメントシステムの構築を開始した。

■ 主な取り組み内容

組織的	人的	物理的	技術的

- 2012 年秋から情報セキュリティ管理規程、個人情報管理規程に基づいた運用を開始した。取り扱う情報も、顧客の個人情報を始めとして、営業機密情報、従業員関係情報、取引先情報、2016 年よりマイナンバー等時代に合わせて広げ、全社で全従業員が情報セキュリティの確保に取り組んでいる。
- 技術的対策、物理的対策、人的対策他セキュリティ責任者の任命、実際の運用上で気付いた改善案への対応等などを社長がリーダーシップを取り実施している。社内にはパソコン数台が LAN 接続されており、ファイアウォールを設置し、全パソコンにはウイルス対策ソフトを導入し、パターンファイルは自動更新して運用している。
- コンサルティング会社と報セキュリティ・マネジメントシステムの構築についてコンサルティング契約を結び、指導を受けながら情報資産の洗い出し、リスク分析等を実施し ISMS を構築し、半年後に全従業員に教育し運用に入った。報セキュリティ・マネジメントシステムの構築にあたっては、IPA の 5 分でできる！情報セキュリティ自社診断シートで自社の現状を評価し運用規程を作成するのに役立てた。
- 毎年全従業員の教育を自社教育テキストと IPA のウェブサイトの各種情報を活用して実施し、従業員全員が受講し最新知識を習得しながら情報セキュリティマネジメントに取り組んでいる。中小企業向け情報セキュリティガイドライン等も役立てている。朝礼で必要に応じて情報セキュリティの徹底を説いている。

■ 取り組みによる効果

全従業員が情報セキュリティについて正しい理解ができ、日常の業務の中で、情報セキュリティに関して正しい運用が可能になった。具体的には、最新ソフトウェアの利用、ウイルス対策ソフト（パターンファイルを含め）の正しい活用、パスワードの正しい取り扱い、怪しいメール受信時の対策、情報の社外持ち出し時の注意、情報の正しい保管と廃棄、共有設定などの正しい運用、セキュリティ事故などの新しい情報・知識の習得等が適切に行われるようになった。その結果、ウイルス感染や情報漏えい事故などがない状況となり、顧客との良好なビジネス上の信頼関係の構築とその維持ができている。

■ 経営者の視点

当社では、顧客の個人情報について複雑な取り扱いはなく、情報システムへの依存度も特に高い訳ではないので緊急の課題はないが、情報セキュリティは変化するので、時代に合わせて経営者、従業員が常に情報セキュリティに関心を持ち続け、必要に応じてレベルアップしていく方針である。ウイルス感染、情報漏えい、内部不正、サイバー攻撃、標的型攻撃等の事故や、いわゆるヒヤリハット経験もこれまでは特にないので、これからも情報セキュリティ規程に沿って情報の正しい取り扱いを実施し、情報セキュリティを確保していきたいと考えている。

事例 57

所在地	大分県
業種	物品賃貸業
従業員規模	21～50 名
事故の有無	無

ウイルス対策ソフトの導入は最低限必要な対策
情報セキュリティ体制の整備と社内教育が今後の課題

■ 情報セキュリティ対策に取り組むきっかけ

当社は、大分県で重機や車両のレンタル・リース・修理・販売や中古建設機械輸出を主な事業として行っている。社内では外部のシステム会社に委託開発した基幹システムを社内ネットワーク経由で利用しており、業務で十数台のパソコンが稼働している。また、自社ウェブサイトは社内で作成・更新するなど、業務での IT 活用には力を入れてきた。これまでのところ、情報セキュリティ対策についての取引先等外部からの要求は特にないものの、テレビやインターネットを通じて情報セキュリティに関する事件・事故のニュースをいくつも見かけるようになったことから、自社でも情報セキュリティ対策が必要だと感じ、2005 年頃から取り組みを開始した。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | **技術的**

- 業務で使用するパソコンすべてにウイルス対策ソフトを導入し、常に最新版に更新して使うようにしている。
- 情報セキュリティ関連被害防止の組織面・運用面での対策は特に実施していないが、外部とのメールについては海外との取引で使用することもあって役員 1 名に限定して運用している。
- 情報セキュリティ業務の外部委託はおこなっていないが、システムを委託している業者に必要に応じて情報セキュリティに関しても相談している。

■ 取り組みによる効果

- ウイルス対策ソフトによって週に数件程度のウイルスが受信メールから検出されるが感染には至っていない。
- 防犯対策としてネットワークカメラで敷地内を監視し、これを自社サイトで公開している。海外の取引先からはよく見られているようでビジネスにプラスに働いているが、公開することによるリスクもあるということなので、見直したい。

■ 情報セキュリティ担当者の視点

これまでのところ情報セキュリティに関する実害は発生していないが、受信した電子メールから週に数件のウイルスが検出されている。ウイルス対策ソフトの導入は最低限必須であると認識している。また、ネットバンキングの取り扱いに不安を覚えている。金融機関が提供する対策に加えて、ネットバンキングを操作できる担当者を限定することで事故発生防止に努めているが、それだけでは不十分ではないかと感じている。

現状では情報セキュリティの体制が整備されておらず、責任者が明確になっていない状態であり、総じて対策は不十分だと感じている。特に、従業員の情報セキュリティに関する意識向上は大きな課題であると認識しており、これからは情報セキュリティに関する責任者を明確にし、月 1 回開催している全体会議で情報セキュリティに関する話題や事例を取り上げる等、社内の教育や意識向上に取り組みたいと考えている。

事例 58

所在地	宮城県
業種	サービス業
従業員規模	6～20 名
事故の有無	無

ベンダ任せにしない主体的な取り組みを維持
情報管理の徹底を通じて、業務効率がアップ

■ 情報セキュリティ対策に取り組むきっかけ

当社は、宮城県で建設関連の設計、コンサルティング、物販事業等を行っている。1995 年頃から、継続的にパソコン導入とセキュリティ対策を実施してきたが、最近は、特にスパムと思われるメールが多くなり、件名、内容とも巧妙化してきているため、ウイルス感染の危険が増していると感じていた。また、インターネットの閲覧などの際に、不要なソフトを意識せずにインストールしてしまうことや、取引先から USB メモリ経由で資料を受け取った際、ウイルスと思われるファイルが格納されていたことなどもあり、統一的に管理、統制する仕組みがなければ、情報漏えいやデータ破壊などの事故を防ぐことが難しいと考えるようになった。

■ 主な取り組み内容

組織的 | 人的 | **物理的** | **技術的**

- 業務で利用するパソコンは、管理者用アカウントと従業員用アカウントを分け、ソフトウェアのインストール、設定変更等は管理用アカウントでのみ行うようにしている。データは、NAS を導入して集中的に管理し、アカウントやデータの種類によりフォルダを分けて担当外の情報へのアクセスを制限し、ログの採取を行っている。
- 従業員のパソコンについては、レジストリの設定により USB メモリへの書き出しを制限している。また、原則として USB メモリの利用を禁止し、データの受け渡しは後述する統一メールアカウントによる送受信により行っている。
- 業務で利用するメールアドレスを統一し従業員共通で利用している。受信はアドレス帳に登録されているアドレスのみを許可しており、新規取引先、問合せなどのメールは、管理者が確認後にアドレス帳に登録している。
- インターネットで閲覧できるサイトを明示的に登録して、必要なサイトは都度、管理者が確認し追加している。SNS サイトへのアクセスは、原則禁止している。

これらの取り組みは、ベンダ任せにせず、自ら情報収集し検証して採用したものであったので、試行錯誤の面はあったが、当社規模の情報セキュリティ対策として一定の機能を果たせていると考えている。USB メモリが使えない、メールアドレスが共通になるなど仕事のやり方が変わるものであったため、情報セキュリティの必要性について、従業員、取引先等の理解を得る必要があり、現在も継続して説明等行っている。

■ 取り組みによる効果

データ破壊、情報漏えい防止等の情報セキュリティ面での効果に加え、個々のパソコンの設定が共通化され、データも集中管理できたため、パソコンの管理、更新時等に個別の設定やデータを考慮する必要がなくなり、作業効率が上がった。また、業務のメールの送受信を統一アカウントにより実施しているため、問合せや受け渡しデータ等が一元管理できるようになり、CC:による添付データの重複などもなくなり、作業、管理効率も向上している。

■ 情報セキュリティ担当者の視点

業態、規模により可能な対策は異なると思われるが、どのような場合でも、社内に担当者を設けてシステムや情報セキュリティ対策について、ベンダに任せきりにしない姿勢が重要と考えている。今後も、新しい OS やデバイス、サービスなどが登場することが予想されるので、その特徴や脆弱性に関する情報などを収集し、当社にあった情報セキュリティ対策を講じる必要があると考えている。また、従業員への教育や説明なども繰り返し実施し理解を得ていきたい。

事例 59

所在地	茨城県
業種	サービス業
従業員規模	21～50 名
事故の有無	無

大切なことは「無事故」を継続すること
自社にあった情報セキュリティ対策を見出し始めた企業

■ 情報セキュリティ対策に取り組むきっかけ

当社は、茨城県の事務用機器・複合機・IT 機器の販売店である。クライアントパソコン 30 台前後、サーバ 3 台前後の規模のシステムを保有しており、顧客に販売する製品を社内で率先して利活用することで、より良いサービスを提供できるようにすることを狙いとしてシステム部を設置し、IT システムの運用にあたっている。2010 年頃になって、取扱商品の一つである複合機のメーカーから、情報セキュリティ対策を促されたことが対策に取り組んだきっかけである。また、地域の入札において、プライバシーマークなどが求められる場合があり、現状はまだ取得はしていないものの、情報セキュリティ関係の認定に関しても、関心をもって注視している。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- セキュリティ対策としての基本的なことを、きっちりやるという方針を掲げて取り組んできた。具体的には、クライアントパソコンへのウイルス対策ソフトのインストール、ウェブアクセスのフィルタリング、ファイアウォールの設置、ウェブサーバを社外のクラウドに移管するなどの対策を実施している。
- まだ試行段階ではあるものの、クライアントパソコンでの利用履歴管理、パソコン等の資産管理、USB メモリの接続管理なども、順次実施の予定としている。
- この半年ほどウイルス付きメールなど、システム運営上の新たな脅威が増えてきた印象があり、さらに注意を喚起しつつ対策を行っていく予定である。

■ 取り組みによる効果

幸いなことに、これまで社内では情報セキュリティの事故は起きていない。ただ、当社商圏一帯で 1000 台弱の複合機を管理する中では、ウイルス感染などのトラブルをしばしば耳にする。複合機や IT サービスを提供する立場にある当社が、情報セキュリティの事故を起こすことなく営業すること自体が、顧客の安心のために重要なことであると考えており、無事故が最大の効果であるという自己評価をしている。

■ 情報セキュリティ担当者の視点

基本的な情報セキュリティについては実施できていると認識している。担当者として、情報セキュリティについて重要なことは、ウイルス対策やセキュアなネットワーク、クライアントパソコンの管理など基本的なことにまず取り組むことであると感じている。その上で、情報セキュリティ全般のリスク管理が必要になってくるのではないかと思う。今後、プライバシーマークの認証取得などによりマネジメントを強化すべきか、あるいは、クライアントパソコンの紛失対策、バックアップ対策など、より深い領域に進むべきなのか、指針を定めていきたい。また、情報セキュリティの展示会や、セミナーなどにも積極的に参加して、知見をさらに深めていくような活動も実施していきたい。

事例 60

所在地	東京都
業種	サービス業
従業員規模	5 名以下
事故の有無	無

他社在籍時の事故経験からセキュリティ対策ソフトを慎重に選定、できるだけ閉じた環境で業務を実施

■ 情報セキュリティ対策に取り組むきっかけ

当社は、東京都で画像データ解析による建物などの構造物の欠損部位を調査（非破壊検査）する研究開発・機器製作・販売を行っている。担当者が以前在籍していた会社で、USB メモリから MAC 及び Windows95 にウイルスが感染し、すべてのデータがクラッシュしてしまった経験があることを聞き、当社では、運用面での対策周知及びいろいろなセキュリティ対策ソフトを試し、定義ファイルの更新の頻度が高く、なおかつ動作が軽い最適なセキュリティソフトを選定するなどの対策を講じている。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | **技術的**

- 事業拠点は本社と研究所の 2 カ所であるが、拠点間通信は行っておらず、機密情報（技術）及び調査したデータ等は研究所内に閉じており、NAS を 1 台設置し、社内のパソコン 2 台で共有している。
- セキュリティ対策ソフトの定義ファイルは常に自動で最新状態になるようにし、メール及びファイルのやり取りがあった場合でも常にスキャンするようにしている。
- 顧客はセキュリティに対して非常に厳しい会社が多いことと、業務の性質上、画像等の大容量のデータを扱うため、顧客及び外部との情報のやり取りについては、電子メールでは機密性のない情報のやり取りに限るようにしており、重要なデータについては CD-ROM や DVD 等に焼き、直接納品している。
- インターネットの閲覧も業務に関係のあるサイトのみにするなど、運用面でセキュリティが確保されるよう心掛けている。

■ 取り組みによる効果

研究所そのものが研究機関関連の会社のみが入居できるビルに立地していることから入退出管理が確実に行われており、不審者の侵入による情報漏えいの可能性は極めて少ない状態であること、2 名のセキュリティに対する意識の高い研究者により業務が遂行されていること、さらに運用面、セキュリティ対策ソフトの最新管理の周知徹底により、これまで被害は発生していない。

■ 経営者の視点

納品等で外部に持ち出す媒体を万が一紛失した場合、パスワードや暗号化等により内容を見ることができない状態にする等、今後対策強化が必要であると考えている。また、海外では社内のメールサーバ経由による配信遅延が多く、海外出張時に限りフリーメールを使用している。フリーメールでは内容を見られても仕方がないという認識のもと、内容には気を付けるようにしているが、今後海外に出ることが多くなると予想されるため、対処方法を検討していきたい。
現在は少人数で、外部とのやり取りも限定された状態での研究・開発を行っているため、セキュリティは保たれている。今後業務が拡大し、従業員も増えた場合に、セキュリティルールの規程等の明文化と日常のセキュリティに対する運用監視をどのようにするか、将来を見据えて検討したいと考えている。

事例 61

所在地	長野県
業種	サービス業
従業員規模	6～20 名
事故の有無	無

早くから業務を IT 化し従業員のセキュリティ意識が高い クラウドサービスの利用により適切な情報管理体制を維持

■ 情報セキュリティ対策に取り組むきっかけ

当社は、長野県で自動車の販売、車検・整備、修理、板金塗装、自動車保険と、車に関わる業務全般を営んでいる。車検・整備や修理状況を顧客毎に管理する必要があり、早くからコンピュータと自動車業界シェア No.1 のパッケージソフトを導入し、顧客管理と車両管理を行ってきた。個人情報保護法が制定された時には、個人情報取扱事業者の対象となるため、自社のプライバシーポリシーを作成した。それを機に情報管理とセキュリティ対策を実施することは企業責任と考え、前向きに取り組んでいる。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | **技術的**

- 顧客管理ソフトはパッケージソフトを利用していたが、クラウドサービスを利用することとなり、1 台のパソコンを専用端末として事務所内に設置した。担当従業員だけがアカウントとパスワードで端末とシステムにログインすることができ、顧客管理を行っている。月々の使用料がかかるものの、①常に最新バージョンのシステムが使用できる　②データを安全に保管できる　③セキュリティ対策もサービスに含まれている等のメリットがある。
- 工場内にはデスクトップパソコンを 1 台設置し、整備担当従業員が車検・整備情報を確認したり、整備情報を追加入力したりできる環境を整えている。顧客を特定できる個人情報はないが、車両や整備の情報は会社にとって財産となる情報であるため、端末にアカウントとパスワードを設定し整備担当従業員のみが使用できるように管理している。
- クラウドサービスを活用することにより、自社サーバを持たず、パソコンも業務毎に使用者を切り分け、ネットワークもシンプルな設計としている。セキュリティ関連の被害を防止するために、①パソコンやシステムのアカウントとパスワードの管理②ウイルス対策ソフトの導入と更新③OS・ソフトウェアの最新バージョンへの更新等ができている。

■ 取り組みによる効果

- 早くから顧客情報や車両情報を IT 化したことにより、従業員の IT スキルが高い。また、IT 化により、事務作業の効率化が図れ、整備担当従業員間の情報共有も円滑となり、従業員が情報を安全に管理し活用することの意義を理解している。このことから、従業員の情報セキュリティに対する意識は高まってきている。
- 社内の基幹業務でクラウドサービスを利用していることにより、タイムリーに必要な情報セキュリティ対策や法令遵守対応が可能であり、社内の情報管理体制を自然と構築することができた。

■ 経営者の視点

今後は従業員に専用のパソコンやモバイル機器を導入することも想定され、状況に合わせて従業員に対するセキュリティ教育や研修を充実する必要がある。また、担当者が経営者に対して、時代に即した IT 投資を提案するにあたり、直接売上にはつながらなくても、IT 化の規模にあった情報セキュリティ対策も一緒に講じなければならないことを提案し、さらなる理解を求める必要がある。

事例 62

所在地	岐阜県
業種	サービス業
従業員規模	51～100 名
事故の有無	無

業界慣例の紙媒体の管理にはルールの徹底で対応
所属団体・市町村の実地検査への対応を通じて「情報セキュリティ対策はできていて当たり前」という考えが社内に浸透

■ 情報セキュリティ対策に取り組むきっかけ

当社は、岐阜県を中心に介護福祉用具のレンタル・販売などを行っている。介護保険を扱う際、通常以上に大量の個人情報（銀行口座、身体・家族情報等）を扱う必要があり、所属団体や市町村による情報セキュリティの実地検査が、最低年 1 回はある。また、厚生労働省の情報公開のため、当社の基本情報やセキュリティでやるべきことを自己採点して提出（年 1 回）する必要がある。このような状況にあることから、情報セキュリティの重要性を認識し、対策に取り組むようになった。さらに当社においては、当初、情報管理は本部 1 拠点のみで行っていたが、営業拠点が増えることによりネットワーク化が必要となり、ハード面での情報セキュリティ対策の強化が求められたこともきっかけとなっている。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- 当業界では、紙媒体による情報のやり取りが主流であるため、従業員には紙に記録された情報の管理に関するルールの徹底をしている。まず、顧客情報は顧客単位でクリアファイルにファイリングし、鍵のかかるキャビネットに保管する。契約のなくなった顧客情報についても 5 年間は保管義務があるため、異なる倉庫内の鍵のかかるキャビネットに入れて保管し、保管期間を過ぎた情報は、溶解処理して破棄している。顧客情報をケアマネージャに渡す場合は、コンピュータより出力し、1 部を当社で保管、1 部を相手に手渡しするようにし、コピーはしないように指導している。
- コンピュータ上での情報セキュリティ確保の取り組みとしては、ハードウェア、ソフトウェア、ネットワーク、サーバ等の管理を一括して同一の IT ベンダに委託し、責任の所在を明確にしている。また、ウイルス対策ソフトを常に最新の状態とすることを求めている。サーバ等のシステムログについては、次回のシステム更新を契機に管理に活用することを計画している。
- 情報セキュリティに関する従業員教育を 1 ヶ月に 1 回、会議の場にて行い、従業員全員へ通達するようにしている。

■ 取り組みによる効果

情報公開のためのチェックに対応したり、所属団体・市町村による情報セキュリティ対策の実地検査などに対応したりする中で、「情報セキュリティ対策はできていて当たり前」という考えが社内に浸透してきている。この結果、新規の介護施設との商談に際して、セキュリティに対する考え方を尋ねられた場合も、担当者が情報セキュリティに関する当社の考え方を明確に答えることができるため、案件獲得につながっている。

■ 情報セキュリティ担当者の視点

業界としてみた場合、運用面での情報セキュリティ対策を今後強化する必要を感じている。当社の取引先である大手企業の系列企業では、個人の持ち物に至るまで厳格な管理を行っている。業界全体で将来的に同様の方向に進んでいくことが見込まれるため、他社の情報セキュリティ対策手法を参考にして、当社の対策を改善していきたいと考えている。

事例 63

所在地	大阪府
業種	サービス業
従業員規模	21～50 名
事故の有無	無

経営者が率先してセキュリティ対策に取り組むことにより、従業員の意識改革セキュリティ対策の実施が迅速化

■ 情報セキュリティ対策に取り組むきっかけ

当社は、大都市を拠点に、システム開発の受託や情報技術者の派遣等を中心に行っている。大手 SIer が ISMS やプライバシーマークを取得し、情報セキュリティに対して本格的に取り組んできており、大手 SIer からの受注に際して情報セキュリティに対する要求が厳しくなっている。また、直接受託開発を行うに際にも、情報セキュリティは重要な項目となってきている。さらに、当社は、顧客へ技術者の派遣も行っており、顧客からは情報セキュリティに対して理解のある人材の要望も高くなってきている。当社の規模では、情報セキュリティ事故が発生すれば、大きな痛手を被ることになる。当社は、設立時から情報セキュリティ対策の重要性を認識し取り組んでいる。

■ 主な取り組み内容

組織的 | 人的 | 物理的 | 技術的

- ウイルス対策ソフトによる最新のウイルスチェックや Windows Update などのソフトウェアの脆弱性への対応などの技術的対策は、基本として実施している。
- 従業員の情報セキュリティへの意識付けをしっかりと行うことが大切であるため、入社時に情報セキュリティの研修を実施するだけでなく、数ヶ月に 1 回、情報セキュリティの基本施策を全員で読み直し、継続的に意識付けを行っている。また、他社で発生した情報セキュリティ事故を対岸の火事とするのではなく、当社としての注意事項として通達を行い、情報セキュリティ対策に対する意識の向上を図っている。

■ 取り組みによる効果

- 対外的には、情報セキュリティに前向きに取り組んでいる企業として信頼を得られていると感じている。また、情報セキュリティに対する新しい投資は、顧客からのより高い信頼につながり、ビジネス機会の拡大となる。
- 内部的には、当初は情報セキュリティに対して「やらされている感」がある従業員も見られたが、現在では、これが当たり前という雰囲気が醸成されて、従業員の情報セキュリティに対するリテラシーの全体的な底上げにつながった。

■ 経営者の視点

当社の規模の企業では、経営者自らが情報セキュリティ責任者として率先して活動することが大切である。自ら、情報セキュリティ責任者として対応することで、従業員の意識改革や情報セキュリティ対策が迅速に実施できていると認識している。また、情報セキュリティ対策に対しては、その投資により企業の業績が赤字にならない範囲で、実質的な効果だけではなく取引先からの信頼確保などを総合的に判断して、対応していくことも必要である。さらに、経営者が、同規模の企業会合において、情報セキュリティの重要性と情報セキュリティ対策の必要性を話している。対策の必要性を認識しつつも、何をやったら良いか分からない経営者も多く、当社の対策内容を伝えることは重要なことである。今後も経営者として、当社の情報セキュリティ責任者として対応するとともに、身の丈に合ったセキュリティ対策を推進していきたい。

事例 64

所在地	大阪府
業種	サービス業
従業員規模	51～100 名
事故の有無	無

利便性やコストを考慮しつつセキュリティ重視の対策を実施
全社で ISMS の取得を目指す

■ 情報セキュリティ対策に取り組むきっかけ

当社は、大阪府に本社を置き医療情報システムに特化したシステム提案・構築・保守を提供している。医療機関は、患者の診療情報を含めて個人情報の適切な取得・保管・利用などについての管理上の義務を負っている。それに関わる医療情報システムに携わっている企業として情報セキュリティ対策に取り組むことはビジネス戦略上必要不可欠であり、会社設立以来、他社のセキュリティ事故を他山の石として、現在に至るまで順次対策を導入してきた。

■ 主な取り組み内容

組織的	人的	物理的	技術的

- ウイルス対策、ファイアウォール、VPN、アクセス制御など技術的なものだけでなく、プライバシーポリシー策定、情報セキュリティに関する社内への啓蒙教育の徹底、ISMS 取得など組織的・人的な対策を実施してきた。情報セキュリティ対策は、利便性とのトレードオフ関係にある。これまでどちらかと言えばセキュリティを重視してきたが、利便性に関するアンケートによると、従業員には特段の不便さはないようである。今後もこれまでどおり、利便性よりもセキュリティ重視の対策を継続する。現在の代表的な取り組みとしては、外向けポートを業務上必要なものに絞るなどの制限を強化している。また、機密情報を保護するためセキュリティゾーニングも徹底している。これらの取り組みは、従業員を信用していないということではなく、従業員・組織・顧客を守るための措置であることを周知している。
- 支店では ISMS を取得している。セキュリティポリシーが文章化されており、クリアデスク・クリアスクリーン、フロアや施設への入退室管理などのガイドブックが整備されている。重要なデータのバックアップは本社で行っている。本社は ISMS の取得はしていないが、運用面では支店と同様に行っており、時機を見て ISMS を取得する予定である。ただし、データのバックアップは不十分であり、東京支店で実施するか、クラウドなどへ外部委託をするか検討中である。外部に委託する場合は基準に則り選定する。

■ 取り組みによる効果

- 支店で ISMS を取得していることもあり社外から相応に評価されている。本社でも同様の運用をしていることから情報の適正管理が徐々に浸透してきており、従業員の意識は年々高くなっている。
- 会社設立以来、内部者の不正による被害は起きていない。また、メールにウイルスが添付されているケースはあるが、適切に処理しており被害はない。これも効果だと考えている。

■ 情報セキュリティ担当者の視点

情報セキュリティ対策に万全はない。常に利便性やコストとのバランスを考えながら、セキュリティ重視の対策を継続したい。そのためには、さらなる従業員のセキュリティ意識の向上、従業員への情報セキュリティ対策の実践教育は不可欠であり、社外教育、資格取得などを含め対策支援費等の補助制度の充実を図りたい。現在、少人数でセキュリティ対策の検討を推進しているが、今後は、「SSL/TLS 暗号設定ガイドライン」、「組織における内部不正防止ガイドライン」、「中小企業の情報セキュリティ対策ガイドライン」など IPA の様々なガイドラインを活用しながらセキュリティ対策の強化を図りたい。

事例 65

所在地	兵庫県
業種	サービス業
従業員規模	21～50 名
事故の有無	無

個人情報保護は社会的使命
従業員のセキュリティ意識の向上を継続的に目指す

■ 情報セキュリティ対策に取り組むきっかけ

当社は、兵庫県で賃貸居住者への家賃保証サービスを行っている。住居のオーナー、入居者、オーナーと入居者の橋渡しをする不動産会社などの膨大な量の顧客情報を取り扱っており、個人情報の権利・利益を保護することは社会的使命であり、情報セキュリティ対策は不可欠であるという認識のもと、現在に至るまで順次対策を導入してきている。

■ 主な取り組み内容

組織的	人的	物理的	技術的

- ウイルス対策、ファイアウォール、VPN など技術的な対策に加え、就業規則における情報取扱規程、罰則規程の制定、プライバシーポリシーの制定など、組織的な対策を実施してきた。
- ビジネスの進展に伴い、取り扱う個人情報の量、事業拠点数、従業員数が増加しており、多重債務、家賃滞納等の機微情報も含まれるため、取り扱いには慎重を期す必要がある。ログのチェック、アクセス制御等の対策が求められ、これらは今後の基幹システム入替時に導入を予定しており、具体的対策の検討を進めているところである。
- セキュリティ対策として、仕組みや啓蒙・教育など組織風土の強化を進めている。業務上、膨大な量の個人情報にアクセスする必要があることから、入退室管理、施錠管理、磁気媒体の持ち出し禁止などルール厳守の徹底を図っている。また、セキュリティ対策もリスクマネジメントの一環として、就業規則における情報の取り扱いやプライバシーポリシーについての再教育を図るとともに、外部教育の受講を促進している。

■ 取り組みによる効果

- 会社全体としてのセキュリティ対策の導入や教育による効果としては、個人情報の重要性について従業員の意識が年々向上していることが挙げられる。個人情報漏えい事故・事件から学ぶことも多く、手を変え、品を変え粘り強く実施していくことが重要である。また、罰則規程も明確になっておりプライバシーポリシーの遵守にもつながっている。
- これまでセキュリティ事件・事故の発生がないことで従業員の自信につながるだけではなく、顧客から評価されることも増えている。しかし、セキュリティに完全はないので、気を引き締めていくことが重要であると認識している。

■ 情報セキュリティ担当者の視点

今後、特に重要なセキュリティ対策として挙げられるのは、内部不正の抑制である。近年、組織内部からの情報漏えいインシデントに関する報道が相次いでいる。情報漏えいの 60%はうっかりミスに起因しており、今まで以上にルールや規則を明確にし、従業員への徹底を図ることが大切である。内部不正の手口としては USB メモリ等による情報持ち出しであり、ルールや規則に依存するだけではなく、これらの痕跡が残る対策の導入をし、周知することで抑制につながると考えている。いずれにせよ、継続して進めなければならないのは、従業員のセキュリティ意識向上のため、従業員への情報セキュリティ対策実践教育である。また、頃合を見て、プライバシーマークを取得したい。

事例 66

所在地	岡山県
業種	サービス業
従業員規模	21～50 名
事故の有無	無

情報の可用性と完全性の確保を重視
情報共有や標準化により従業員のセキュリティ意識向上

■ 情報セキュリティ対策に取り組むきっかけ

当社は、岡山県で古くなった工作機械に最新の制御機能を付加してリニューアルする事業を行っている。個人情報を扱う業種ではないが、経営者はコンプライアンスに対する意識が高く、大手企業との取引もあるため、企業として情報セキュリティにも対応していこうという思いがあった。少人数の企業でもあり当初は社内のパソコンが数台、請求書なども手書きの状態ではあったが、2009 年に ICT に詳しい従業員が入社したことをきっかけに、ICT 利活用の推進と合わせて情報セキュリティ対策にも注力することとなった。当社の情報は、様々な業務に関わるノウハウや営業に関する情報が中心となるため、情報の消失を防止し、適切に保管して業務に活用できることが必要で、可用性、完全性の維持を重視している。

■ 主な取り組み内容

組織的 | 人的 | **物理的** | **技術的**

- 意識しなくてもセキュアな情報管理ができる仕組みを心掛けており、ウイルス対策ソフトの導入やパターンファイルの更新など個別パソコンの基本的な対応を実施した上で、業務上の情報は NAS に保管するようにしている。NAS は現用系とバックアップ系の 2 系統に分け、現用系はレプリケーション機能を用いて可用性を高めている。現用系の NAS はフォルダ毎にアクセス権を設定して利用者の所属や役職、担当業務によってアクセスレベルを分けており、バックアップ系はシステム管理者以外のアクセスを禁止している。また、社外からのアクセスも受け付けない。
- ソフトウェアのサポート情報にも気を配っており、以前使用していたメーラーのサポートが停止したため、全パソコンのメーラーを変更した。また、ランサムウェアや標的型攻撃メール等のリスクはレポートを社内で回覧し、注意を促している。
- マイナンバー関連もガイドラインに沿った運用を実施しており、専用のパソコンを導入してネットワークから切り離し、情報を暗号化するなどの対応を行っている。

■ 取り組みによる効果

情報セキュリティ関連の注意喚起の情報発信や標準化等で、社内の情報セキュリティに対する意識が徐々にではあるが向上しつつあり、現場での勝手な設定変更等がなくなり、疑問点や不明点も積極的にシステム管理者に相談、報告する習慣が根付いた。また、ウイルスが仕込まれた攻撃メールの添付ファイルを従業員がうっかり開いてしまうことがあったが、ウイルス対策ソフトのパターンファイル更新を確実に実施していたため感染は免れた。念のために、その後パソコンのリカバリーやメールアドレスの変更等の対応を行った。この件は、従業員に情報セキュリティ対策の必要性を身近に感じさせることとなった。また、システム担当者は、スキルアップのため情報セキュリティスペシャリスト試験にチャレンジし、合格を果たしている。

■ 情報セキュリティ担当者の視点

地方の少人数の企業ではあるが、大手企業との取引もあり、コンプライアンス面も重視している。しかしながら、情報セキュリティ対策に大きな費用を投じることは経営上難しい。そこで、従業員の意識付けが最も重要と考えており、折を見てまめに情報発信を行うこと等で意識レベルを向上させていきたい。社内の情報管理については段階的にレベルアップしてきているが、業務上、ノートパソコンや USB メモリによる情報の持ち出しが不可避である。対象となる従業員は限られているため個別に注意を喚起して対応しているが、今後は仕組みとして情報セキュリティを維持するよう対応を検討している。

事例 67

所在地	愛媛県
業種	サービス業
従業員規模	6～20 名
事故の有無	無

徹底してコストをかけない対策を採用
組織内部からの情報漏えいのリスク低減策は今後の課題

■ 情報セキュリティ対策に取り組むきっかけ

当社は、愛媛県で浄化槽管理を事業としている。当社の経営者は大手情報通信会社に勤務していたが、数年前に家業を継ぐこととなった。いざ継いでみると、数多くの個人情報を保有しているにも関わらず、事務所内はすべてが手作業・紙媒体であり、パソコンが 1 台もないことに驚いた。そこで、まずはパソコンを導入し、効率化を図るため、紙媒体では探すことにも時間を要している顧客台帳を電子化することを検討した。しかしながら、大手情報通信会社勤務経験から、情報管理の重要性と難しさを十二分に認識しており、限られた予算の中、安易（情報セキュリティ対策無し）に行う訳にはいかなかった。

■ 主な取り組み内容

組織的 | 人的 | **物理的** | 技術的

- 従業員の IT スキルや情報管理コスト等を検討した結果、外部とは遮断（インターネット・ネットワーク接続無し）し、スタンドアロン運用することとした。言わば最も原始的な情報セキュリティ対策である。
- パソコンに対しては、USB メモリなどの外部記憶装置の接続を禁止し（当社で使用するバックアップ用は除く）、ウイルス感染のリスクを回避している。また、業務書類（紙媒体）については、社外への持ち出し禁止、シュレッダー、溶解処理のルール化を図り、従業員に徹底している。なお、外部との連絡に電子メールを使用することも必要となり、それに対しては、業務で使用しない別のパソコンをインターネット接続し、対応している。
- パソコンの故障や災害時の対策として、パソコン予備機（メインパソコン故障時に使用）の設置と USB メモリへのデータバックアップを週 1 回行っている。その USB メモリは、当社敷地外に置いてある耐火金庫内に保管している。

■ 取り組みによる効果

当社のような小規模事業所において、情報漏えいは致命傷であり、身の丈に合わない情報化をしてしまえば、それに伴い情報セキュリティ対策コストも大きな負担となる。よって身の丈に合った現状のスタイルにしたことで、コスト負荷がかからずに済んでいる。また、パソコンを外部と遮断し、ウイルス感染・情報漏えいのリスクを回避していることで、経営者としての心理負担（情報漏えいの心配・不安）の軽減ともなっている。さらには、パソコンをインターネットに接続した場合、一般的に、常駐するウイルス対策ソフトや、知らず知らずのうちに行われたアプリケーションソフトのインストール及び設定変更等が、パソコンの処理速度低下の要因ともなっており、その要因を排除できていることから、パソコンの処理速度は、購入時の速度を維持できている。

■ 経営者の視点

今後、新事業を展開する場合は別として、現時点において、当事業の今後の大きな変化はないものと予想し、現状のスタイルで対応が可能と考えている。しかしながら、パソコンを外部と遮断しても、組織内部から情報が漏えいするリスクがあることを認識する必要がある。これについては非常に難しい課題であるが、操作履歴のログ管理ソフトなどを利用し、技術的に監視できる仕組みの構築や、普段における従業員とのコミュニケーション・待遇改善への取り組みなど、従業員との良好な関係を築くことも重要であると考えている。そして最後に、万一にでも、顧客台帳等の個人情報が流出した場合には、当社の存続はないものと覚悟し、今後も情報セキュリティに向き合っていくつもりである。

事例 68

所在地	長崎県
業種	サービス業
従業員規模	6～20 名
事故の有無	無

重要情報を守るためのセキュリティ対策を実施

専用線利用、社内規程策定、ウェブシステムの遠隔監視

■ 情報セキュリティ対策に取り組むきっかけ

当社は、長崎県で保険代理店として、各種保険や備品、業務改善などを請け負う管理システムサービスの提供を行っている。顧客等の重要情報については、本部からの要請もありセキュリティ対策に取り組むようになった。本部から提供される最新のセキュリティ情報を把握したり、公的機関が開催する情報セキュリティセミナー等を担当従業員に受講させたりするなどの対応をしながら、セキュリティシステムや関連ソフトウェア等の導入を、コストを考えながら行っている。

■ 主な取り組み内容

組織的 | 人的 | **物理的** | **技術的**

- 重要情報を保管している機器は、インターネットにつながず専用線を利用している。汎用性がなくデメリットもあるが、必要な対策であると考えている。しかし、ウェブを活用したシステムも存在するので、セキュリティソフト等の更新には注意を払っている。
- 現在、社内規程を作成しており、それに則った情報システム（主にパソコン）の運用を行っている。例えば、電子決済の承認個人 ID を活用、サーバにカギをかけた状態での運用・管理、個別ではパスワードの定期的変更の徹底、更にモバイル端末にも規定を設けている。また、これらを円滑に運営するための社内教育も実施している。
- 現在、本部とつながっているウェブシステムについては、IT ベンダと監視システムの契約をしており、遠隔でチェックしている。他のウェブシステムについても、契約ベンダの監視システムによるチェックを行っている。

■ 取り組みによる効果

数年前に会社体制を変更した際に、情報端末機器の更新及びセキュリティシステムの導入をしたことが効果を発揮し、これまでに何も問題が起きなかったと考えられる。

■ 情報セキュリティ担当者の視点

安全性をユーザ側で判断できないのが少々不安であるが、今後はクラウドシステムの活用も検討している。また、最新の情報システムでも必ず安全という訳ではないので、セキュリティ対策に関する予算（安全なハードウェア、ソフトウェアの購入、各種セミナー等の費用等）の確保は必要と考えている。さらに、自社ウェブサイトを活用した情報発信・各種サービス提供等も今後行う予定なので、現在のセキュリティ対策をより一層強化していく必要があると考えている。