平成１５年度　セキュリティ研究部会　報告書

セキュリティポリシーの定着化に向けて

～課題と解決のヒント集～

社団法人　日本情報システム・ユーザー協会

［セキュリティ研究部会報告書・目次］

はじめに

JUAS のセキュリティ研究部会は今期で 5 年目を迎えました。発足当初より会員企業の情報セキュリティに対する関心は大変高く、毎年の参加メンバーは常に 20 社以上を数えています。国際規格の研究や、リスクアセスメント、汎用セキュリティポリシーの作成など、数多くのテーマで活発な活動を続けてきました。

一方、わが国の情報セキュリティマネジメントの現状は、ここ 1～2 年の間に個人情報保護法の施行、ISMS 適合性評価制度の正式発足など、急速に基盤整備が進みました。各企業もこれに対応し、本格的なセキュリティ対策に取り組むところが増え、ウイルス対策だけにとどまらない、全社的なセキュリティポリシーの制定など、大企業を中心にセキュリティ管理のレベルは着実に上がってきています。

しかし、実際にこうした管理ルールを制定しても、現実にこれを順守し実を上げていくこと、すなわち、これらの制度がうたう PDCA（Plan Do Check Act）サイクルを企業内で実践していくことは並大抵のことでできることではありません。国際基準の認証を取得した企業が、個人情報漏洩事故を起こすなど、単にポリシーを制定しただけでは安閑としていられない、待ったなしの厳しい現実もあります。

そこでセキュリティ研究部会では、今年度はこうしたセキュリティポリシーの定着をテーマにメンバーを募集したところ、例年の 2 倍近い 50 社を上回る応募がありました。いかに各企業が定着に苦労しているかを物語っています。

研究部会の議論は、会員企業限りという約束で建前ではなく現実の率直な実情と、経験、体験を報告してもらい、問題点を共有することに力点をおきました。その結果、各社から合わせて 100 以上の課題、問題が提起され、課題の整理とその対処法の提起など活発な意見交換が行われました。

こうして、ポリシー、ルールの定着を妨げる材料には事欠きませんでしたが、その対処法、解決法はそう簡単に出てくるものではなく、正直言って難しい問題が続出しました。論理では片付かない企業風土、人間性などに起因する問題は経営トップのよほどの強い意志と理解が得られないと、単に規制を強化するだけでは実質的な効果を上げることができないからです。

また、現実の問題点は、現象面で整理してもつきつめていくと複数の問題に共通した原因であることも多く、問題点からアプローチした我々の方法では全体がうまく整理されず、明確な答が得られていないまま残された課題も多々ある結果となりました。

しかし、当報告書の内容は一読されればわかるように、会員企業の皆さんが現実に直面して苦悩している状況が整理されたものになっており、身につまされること請け合いの内容であると確信しています。そういう意味では貴重な情報が集まっているといえるのではないでしょうか。

最終的に執筆に参加したメンバーは 30 名以下となりましたが、当報告書は参加メンバーのこれまでの貴重な経験が生かされた、いわば TIPS 集（ヒント集、知恵袋集）ということで皆さんのお役に立てるのではないかと考えています。
悩みを共有することで有効な解決方法の模索の参考にしていただき、これをお読みになった読者の企業のセキュリティレベルが少しでも向上することを希望してやみません。

最後になりましたが、この報告書を作成するにあたって、全体のためにこれまでの経験を忌憚なく披露していただいた参加メンバー全員に感謝するとともに、会の運営にあたり、種々お世話になった JUAS ならびに研究部会事務局の石川継雄氏、小川 あつし氏にメンバーを代表して心から感謝の意を表させていただきたいと思います。ありがとうございました。

平成 16 年 3 月 31 日
セキュリティ研究部会長　永田靖人

第１章　セキュリティ定着に関する企業の悩み

本章では、セキュリティポリシーを作成し制定したが、社内に上手く定着しなくて困っているという、多くのユーザー企業の声について論じます。

１．１　困っている企業を論じる前提条件

ユーザー企業の困っている状況を論じるに当たって、当研究会では次のような条件を想定しました。

・報告書の読者は、JUAS の研究会参加企業を想定しました。
・議論の対象は、既にセキュリティポリシーが制定はされているが、定着されているとは言いがたいという認識で論じました。
・企業内のセキュリティ遵守状態の把握は、企業の中のいろいろな視点が考えられますが、認識はセキュリティ研究部会に参加している参加者の視点で捉えました。
・論じている問題点は、JUAS に加盟している企業が潜在的に持っているであろう内容を想定しました。
・ニュースソース（情報源）は各ユーザー企業からの自己申告をまとめました。
・セキュリティ対策の規模や程度は企業規模によって異なりますが、2002 年度 JUAS 版セキュリティポリシーを制定したときと同様に、日本の中堅企業のいわゆるよくある会社を想定しました。
・困っている項目の相互関係は、1.3 節で詳細に説明しました。

１．２　ユーザー企業の困っている内容

ユーザー企業の困っている項目は多岐にわたり、一概に表現することは真意を歪めてしまうし、すべてを網羅的に表現することは極めて困難が多い。しかし、ある程度の共通点も見られ、それらの項目を大括りにグループ別にまとめ表現することは価値があるし、読者の参考になるとも考え、列挙してみました。

①基本方針に関する項目
・取締役会承認など、改訂作業が重過ぎて改定に踏み切れない。
・記載内容が多すぎたり、理想に走りすぎていて、実行レベルに落とせない項目がある。
・既存の規定類（機密管理規程など）との整合性がないため、どちらも実施されない。

②組織・体制に関する項目
・セキュリティ委員会はあるが活動が低調だったり、管理・統括部門が複数にわたり、

責任部門がはっきりしないので、当事者意識が薄く、定着しない。
・一部の体制で意思決定を行っていて、現場を巻き込んだ体制になっていない。
・担当者がローテーションで変わってしまって、引き継ぎ・継続されない。
・規程が多すぎて覚えきれず、なかなか遵守できない。

③制度・運用に関する項目（管理側の問題点）
・リスクアセスメントが行われないので、問題意識が生まれない。
・懲戒事項に連動していないので、遵守意識が生まれにくい。
・管理文書がわかりにくい。わからせようとする努力がみられない。
・セキュリティ運用計画が効果的に実施されない、状況報告がなされない。
・インシデントのケーススタディやインシデント発生時のエスカレーションフロー（定義・訓練）がない。
・ログ（アカウント、ファイアウォールなど）の棚卸管理と対策をしていない。
・遠隔営業地、グループ会社のセキュリティ運用の管理までは手が回らない。
・契約社員、外部業者、外注委託先のセキュリティ管理がチェックされていない。
・外注委託先のセキュリティ管理と自社のセキュリティ管理水準の乖離が大きく、水準を保てる保証がない。

④管理に関する項目（利用者側の問題点）
・PC に情報を入れて持ち歩いて盗難にあう。モバイル機器が盗難にあう。
・セキュリティホール（個人 PC の無断接続、自宅へコピーなど）が発生する。
・クリアスクリーン、クリアディスクが徹底されていない。
・パスワードが安直、パスワードの貸し借りが公然と行われている。
・禁止サイトへのアクセスがなくならない。
・機密に関する社外での不用意発言（インサイダー情報など）がある。
・重要情報管理の施錠ルールが守られていない。
・印刷された重要情報の廃棄に注意が払われていない。

⑤技術に関する項目（施策不足の問題点）
・標準化が進んでおらず、対策が後手に回る（統一したアクションが取れない）。
・セキュリティホール（ユーザーID の管理、独自ソフトの導入、メールの添付ファイル管理など）が管理されていない。
・バージョンアップ・機能改善が後手に回りセキュリティホールを作ってしまう。外部の攻撃に対して適切な処置が取れない。
・ネットワークガバナンスがない（脆弱な会社とつながってしまう）。
・ネットワークインシデント発生時（DOS 攻撃時、侵入時、ウイルス感染など）のエス

カレーションフロー（定義・訓練）がない。
・セキュリティライフサイクル管理（PC・電子媒体の廃棄など）に差がある。
・ネットワークの監視が行われていない、侵入検知機能が組み込まれていない。
・Web サイトのフィルタリングが行われていない。
・自動化（ウイルスパターンの導入、PC のパッチ適用）対策が遅れている。
・情報制約（ファイルのダウンロード、印刷の制限等）が行われていない。
・情報の完全性（バックアップ／リストア）の定期的機能検証が行われていない。
・バックアップメディアの保管ルール（外部保管、搬送ルートのトレースなど）が行われていない。

⑥資産の分類及び仕方に関する項目
・重要情報の管理台帳が作成されていない（インシデント発生時に差し止め請求権、原状復帰請求権、損害賠償請求権が行使できない)。
・情報資産の台帳管理がされていない、更新されていない（紛失を検出できない)。

⑦企業風土・文化に関する項目
・経営者、管理者がリスクのパラダイムシフトに気がついていない。
・経営者自身の意識を変えることが難しい（経営指標に載ってこない)。
・セキュリティ関連の業務の優先順位を下げられて、なかなか実施されない。
・総論では賛成しているが、自分の問題とは捉えない。
・ペナルティがないので、軌道修正されない。

⑧監査に関する項目
・監査する部門がない。
・内部監査では、形式的チェックのみで効果的な監査にならない。
・監査の視点が、有効性・可用性を向いておらず、効果的な結果を出せない。
・監査結果をフィードバックする仕組みがない。
・実施レベルを確認・評価できる管理指標を設定できない。

⑨教育・訓練に関する項目
・教育内容が具体的行動に結びつくようになっていない。
・受講しっぱなしで、教育の受講確認が取られていない。
・インシデント、ウイルス感染被害などへの教育・指導が行われていない。
・派遣社員など、入れ替わりがある社員へ教育する仕組みがない。
・セキュリティ管理がなぜ重要なのかを教育する体系が整備されていない。
・ユーザー向けのガイドが作成されていない。

１．３　セキュリティポリシーの定着における「困っている内容」のまとめ方

1.2 節で上げられた、セキュリティポリシーの定着における困っている内容（問題・課題）の洗い出しと整理について、様々なアプローチを試みました。ここでは、そのうちの「ひとつの事例」を紹介します。このアプローチにおける検討プロセスは以下の通りです。

①セキュリティポリシーが定着していない状態についての企業の事例を抽出
②困っていること（問題・課題）の洗い出し
③問題・課題のカテゴリーを作成
④カテゴリー同士の関連性、相互作用などを分析
⑤最終的な検討対象の大カテゴリーと体系を作成

①および②の活動により、研究会メンバーから様々な情報が集まりました。しかし、これらの情報は各メンバーがそれぞれ問題・課題の洗い出しをするにあたって、各々想定する「前提」が異なっているために、集まった情報は統一されたものではありませんでした。そのため、これらの情報をまとめ上げ、体系化して整理することを試みました。

まず、「セキュリティポリシーの定着における問題・課題を洗い出す」という命題で、各メンバーが抽出にあたり想定した前提について、表１－１の４つに分類しました。セキュリティポリシーの定着における問題・課題にあたっては、主に「阻害要因」に区分される情報を優先的に取り上げるのが適切と考えられますが、他の区分であっても、ヒントになる事項は多く含まれる可能性がありますので、後からでも参照しやすいようにまとめることを心がけました。

表１－１　＜４つの問題領域＞

各々が想定した前提の区分	説明
阻害要因	セキュリティポリシーの定着にあたって、阻害となっている事項の原因を抽出している。（命題どおり） ・経営者、管理者の意識が低い ・規定、標準改訂手続きが適切でない ・組織の末端までの周知がされてない　　等
施策	セキュリティポリシーの定着の問題・課題の抽出ではなく、具体的な施策や対策を述べている。 ・罰則を適用する ・同意書・宣誓書を提出させる ・e-Learning などを活用した教育をする　等
事象／影響	セキュリティポリシーの定着の問題・課題の抽出ではなく、発生した事実などを述べている。 ・不注意による情報紛失・漏洩 ・不注意やリテラシー不足によるウイルス感染 ・施錠管理をしていない　　等
注目分野	セキュリティポリシーの定着の問題・課題の抽出ではなく、興味分野などを述べている。 ・個人情報取り扱いの基準制定の方法 ・セキュリティインシデントへの対応手順と体制 ・人的脆弱性の克服法　　等

さらに、セキュリティポリシーの定着を考える上では、PDCA サイクルを意識する必要があると考え、抽出された各事項は、PDCA サイクルではどの位置に属するかについても分類することとしました。

また、③のプロセスとして各メンバーから抽出された項目ごとにその内容から「組織／体制」「文化／風土」「意識」などのカテゴリーを付しました。各メンバーから抽出されたすべての項目について、このカテゴリーを付すと、全部で表１－２のようなカテゴリーが作成できました。

表１－２　＜問題・課題のカテゴリー＞

大項目	中項目	説明
人的要因	意識	必要性を感じていない等の問題
	心理	理解していても受け入れられない等の問題
	手間	作業的に面倒でやらない等の問題
	優先事項	セキュリティへの対応は優先度が低く扱われる等の問題
	知識	知らないためにできない等の問題
	リテラシー	やりたくてもできない等の問題
	ミス	操作間違い等による漏洩等の問題
	文化／風土	組織の風潮による阻害等の問題
管理要因（維持/運営）	組織／体制	体制の形骸化、要員不測等の問題
	分担／責任	体制があっても個々の責任などが不明確等の問題
	監査／状況把握	ルールの定着状況の把握ができない等の問題
	教育	教育カリキュラムが悪い等の問題
	ドキュメント	記載内容が難しい等の問題
	罰則	処罰が明確でない等の問題
	手順／展開	進め方が悪い等の問題
	手続き	運用できるレベルの手続きになっていない等の問題
	制度整備	ルール自身がない等の問題
環境要因(インフラ・技術)	システム／技術	設定が不適切等の問題
	負担軽減	作業がシステム化されていない等の問題
	費用	セキュリティの予算が確保できない等の問題

こうして作成された表は表１－３のようなイメージのものになりました。

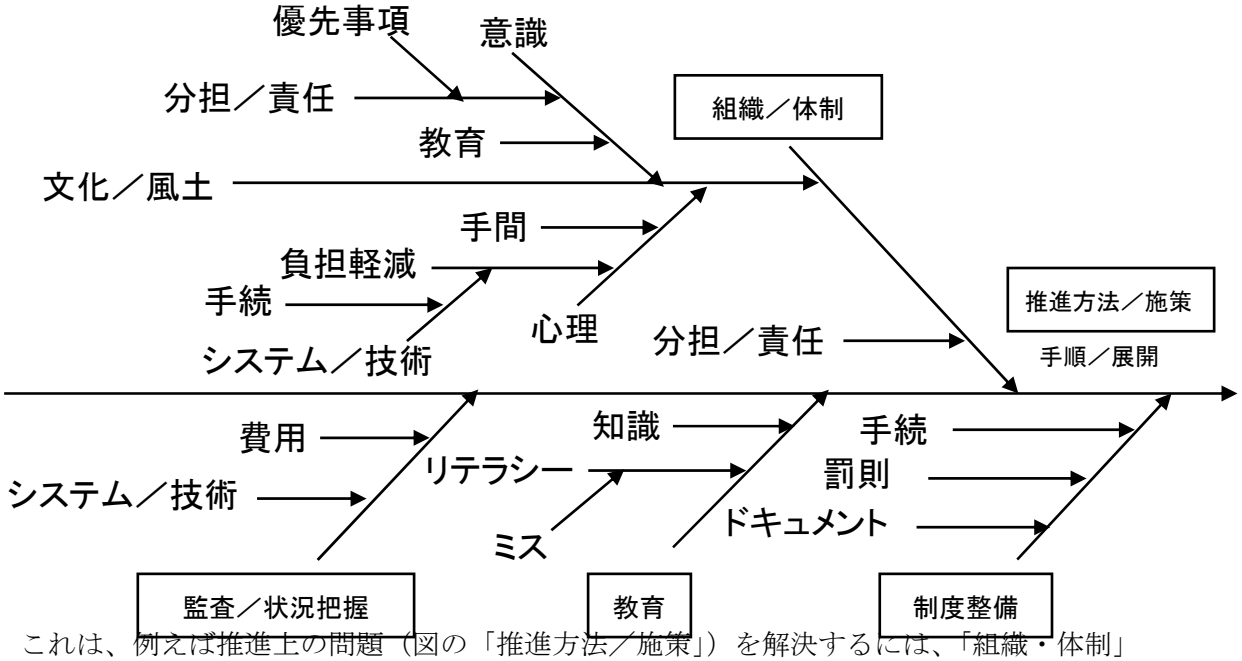
表１－３

提案者	問題・課題（例）	阻害要因	施策	事象影響	注目分野	P	D	C	A	人的要因	管理要因	環境要因
A 氏	・経営者の意識	●				●				●		
B 氏	・罰則を適用する		●				●				●	
C 氏	・情報紛失・漏洩			●		－	－	－	－	●	●	●
・												
・												
・												
・												

※紙面の都合上、「中項目」のカテゴリーは省略しています。

次に、④の検討プロセスとして、問題・課題の中項目について関連性、相互作用などを分析しました（図１－１参照）。

図１－１



これは、例えば推進上の問題（図の「推進方法／施策」）を解決するには、「組織・体制」「制度整備」「教育」「監査／状況把握」の問題を解決する必要があり、さらに、組織・体制の問題を解決するには、「分担／責任」「風土／文化」の問題を解決する必要があるとい

うように解釈します。

四角で囲った部分は、特に根幹となるカテゴリーで、これらを解決するということは、全体も解決されることにつながるため、これを重点検討項目としました。さらに、「組織・体制」「制度整備」「推進」については、「主要プロセス」。「教育」「監査」については、「支援プロセス」と分類しました。これが、最後の⑤の検討プロセスです。結果として表１－４のようになります。

表１－４　＜重点検討項目＞

プロセス	項目
主要プロセス	組織・体制
	制度整備
	推進
支援プロセス	教育
	監査

このように、ある程度、体系的に整理した上で問題・課題に対する対策について検討することにより、各対策間の統一性をとることに役立ったと考えています。

１．４　情報セキュリティ対策の困っている状態（定着の状態）と測定指標の議論

前節までで、セキュリティポリシーが上手く定着しなくて困っているという、会員の声とそのまとめ方について述べました。ここで、いきなり「それでは対策は？」と進まず、当研究会では次の問題提起があり、それに対し討議を行いました。

「『定着しない』というが、どんな状態を指して『定着しない』というのか。それぞれが『定着していない状態』の認識に幅があるのではないか。この認識を擦り合わせないまま、具体的な対策を論じるのは、拙速ではないだろうか。」

ということから、各会員の認識していることを自由に発言しあいました。

①「定着していない状態」の各会員の認識

会員 A :「教科書的に言えば、管理のサイクル PDCA が効果的に回っているか、ということだろう。セキュリティポリシーはこの場合、P に相当する。」

会員 B :「ポリシーが定着されている状況とは、すべての従業員間でポリシー・規定類が要求しているような行動が行われている、つまりポリシー・規定類で守るべき基準（Criterion）が明示されていることじゃないかな。」

会員 C :「『定着していない』事例のひとつとして、教育を受けてくれない、セキュリティ管理者を置いてくれないなど、指示に従ってくれないことがある。」

会員 D:「ポリシーにいくら従っていても、そのポリシーが不備、あるいは不十分のため、セキュリティ上のインシデントが発生しては、結局それは『定着していない』ことにならないか。ということは、どれだけそういったインシデントが発生しにくいか、というセキュリティ上の安定性とか信頼性などが、定着しているかいないかを左右する、重大な要件ではないか。」

会員 E:「ISMS のコンサルタントをやっている経験から、『同僚がいかがわしいサイトを会社で見ていたら、あなたはどう行動しますか？』という質問が、その会社の教育、文化（風土）、体制（escalation system）を知る上で有効だ。また、どこまで投資をすれば十分か、という質問をよく受ける。さらにセキュリティとリスクマネジメントを混同している人がいる。」

などなど、多様な意見が出されました。次に、それならば PDCA の C として、「定着している状態」をどのように評価できるか、定量的な方法はあるか、という議論に移りました。

②定着度の測定方法

会員 A:「管理のサイクル PDCA が効果的に回っているのが、『定着している状態』だとしても、C が機能しないと A に繋がらないね。皆さんは、社員がセキュリティポリシーに従っていることを、どうやって把握しているのだろう。」

会員 C:「実施度をアンケート形式で調査し、それを点数化するのも一法ではないか。」

会員 A:「セキュリティ問題は安全問題と同じで、いかに問題が起きにくいかの指標が必要（①での会員 D さんと同じ）。ただ、セキュリティ事故は災害ほど件数はなく、同じ管理はしにくい。セキュリティ上のヒヤリとした、あるいはハッとした事例（実際のトラブルには至っていないが）をカウントし、それを削減するのも一法だと思う。」

など、こちらも多くの意見が出されました。ただ、時間的な制約があり、これを具体的に受けて次のステップに移ったりしていませんし、項目の深掘りをして結論が出たわけでもありません。

しかし、冒頭に述べたように「セキュリティポリシーが上手く定着しなくて困っている」という問題意識から、その対策を検討するときに、「情報セキュリティ対策が定着している状態とは何か」、また、その「定着度の測定方法はどうすべきか」について考えてみることは、有効な手段であると思われます。

１．５　困っている状況の打開策検討へのアプローチ

以上の議論を経て、ユーザー企業の困っている項目を解決策に導くアプローチとして、

以下に示すような手順を経てまとめ作業が行われました。解決策をまとめる方向付けの視点としては、「ユーザー企業でそのまま役に立つ【知恵袋】を提供しよう」ということで、研究会参加者自体が大いに張り切って汗を流して取り組みました。

1.3 節の分類でも議論したように、広範囲な項目を対象にしているため一括作業はできず、分類された項目をそれぞれがメールにてグループ内メンバーに送信し合い、適時内容を確認し、意見交換し、最終的に定期的に集まって討議しながら進めました。

各自、自分の業務をこなしながらの対応で、検討に参加された方には敬意を表します。

①情報セキュリティは範囲が広く、取り組むテーマが大きいので、議論が成果に結びつくよう大まかに 2 つのグループに分かれて議論しました。

②取り組みの初期の段階で、各ユーザー企業の概況を報告してもらい、各企業の状況の違いを認識しつつ、共通の議論の土台としました。

③まとめの方向性は、ユーザー企業が自主的に発案しましたが、成果物をにらんでの客観的な視点については、ユーザー企業ではあるがコンサルタントを生業にしている参加者に参考意見を求めました。

④読み手のことを考えて、まとめの表現を統一することとしました。まとめは表形式にし、必要な項目を関連付けて参照できるよう考慮しました。

⑤表への記入は各ユーザー企業が分担してあたりました。解決策の記入にあたっては、それぞれが「あるべき姿」を思い浮かべながら検討しました。それを統合し、全体の整合性が取れるように考慮しました。

第２章　対応策から見たセキュリティ定着への考え方

前章では、セキュリティが定着しない事象に関して当部会で行った要因側から分析・整理・対応策導出のプロセスの解説を紹介しました。本章では、その結果得られた「定着へ向けた対応策」について取り上げます。

２．１　セキュリティ定着のための対応策の基本

セキュリティ定着のための対応策の基本は、ISMS などの中で指摘されているように、情報セキュリティに対するリスクを洗い出し、情報セキュリティポリシーを定め、そのポリシーを確実に運用し、運用などの評価結果から見直しを実施するという、セキュリティマネジメントシステムにおける PDCA サイクルを回して継続的改善を図っていくことです。しかしながら、当部会の中で行われた討議からは、このような理想的な形でセキュリティマネジメントシステムが運営されていることは、まだ一部に留まっているという現状が、浮かび上がってきました。その原因は前章で指摘された阻害要因として集約されていますが、その中でも実行される対応策自身とその運用に関わる要因は、企業の業種、規模、取り組みの経緯などによって変化する部分もあるものの、参加企業の共通の問題であるものが多数存在するとの感触が得られました。

そこで、本章では「情報セキュリティ定着のための対応策」について、各企業で共通する部分を次項の３つの問題にまとめて整理し、解説を行います。

２．２　セキュリティ定着のための対応策の重要ポイント

当部会で討議・検討された対応策（TIPS 集）は、第 3 章・課題と解決のヒント集にまとめられていますが、この対応策を概括し、各企業で共通する部分をまとめると、

（１）セキュリティマネジメントシステム（ルール・仕組み・体制など）を、いかに守りやすく、実行しやすく設計するかという事項
（２）セキュリティマネジメントシステムを、いかに徹底していくかという事項
（３）セキュリティマネジメントシステムを、いかに的確に評価し改善していくかという事項

の３つに大別されます。以下、この３つの事項について詳述いたします。

（１）セキュリティマネジメントシステム（ルール・仕組み・体制など）を、いかに守りやすく、実行しやすく設計するかという事項

本事項に関しては、情報セキュリティを支える３要素である人的・管理的・技術（環境）的側面から考えて、対応策の設計に関し次のような配慮を行うことが重要と思われます。

①人的要素の対応策として、セキュリティマネジメントシステムを設計・構築する際に、いかに実業務を行われる利用者の方々やキーマンを巻き込んでいくかということが重要です。「定着しない」ということは、「関係者がルール・仕組みを守ろうとしない／守れない」ということでありますが、この背景を検討していくと、実業務を行われる利用者の方々に当事者意識が欠けている（自分の問題として考えていない）ケースが多いことがよく見受けられます。これは、専門家だけでルールを設定してしまい、現場の状況・レベルと合致していないルール・仕組み・体制を作ってしまったような場合がその典型的な例です。このような場合、無理に当事者意識を持たせようにも、敵対的な心理状態になってしまうこともままあります。

こういった事態を避けるためにも、セキュリティマネジメントシステムを設計・構築する際から、実業務を行われる利用者の方々やキーマンを参加させ、「リスクアセスメント」等で洗い出されたリスクや課題を、自らの問題として認識してもらい、専門家やセキュリティの担当者だけではなく、利用者の方々が容易に実施できる身の丈にあった、ルール・仕組み・体制とすることが重要です。

このようにして作られたルール・仕組み・体制は他人から押し付けられたものではなく、自分自身で考えたものなので守らざるを得ないものとなっていきます。このやり方はセキュリティマネジメントシステム完成後に陳腐化してきた際にも有効であると考えられます。

②管理的要素の対応策として、セキュリティマネジメントシステムを実行するに当たり、通常業務の中にうまく入れ込み、現場の負荷が大きく増加しないような、普段実施している作業が情報セキュリティを守ることに直接繋がっているようなルール・仕組み・体制の設計や、情報セキュリティの遵守状況が容易にわかる仕組みの構築が重要です。具体的には、複数のマネジメントシステムに必要なタスクを共通化するとか、セキュリティ要件を満たしたPCでないと購買できない仕組みとなっていて、普通に業務をやっていればよいとか、フリーアドレス化によりクリアデスク、クリアスクリーンポリシーが遵守されていることが一目でわかるといったようなことがあげられます。

③技術（環境）要素の対応策として、情報セキュリティを守るために技術や設備を積極的に採用し、自動化・フールプルーフ化を推進していくということが重要です。ルールや体制だけで、情報セキュリティを担保しようとしても、通常業務に追われている現場の利用者は、通常業務を優先し、情報セキュリティは二の次三の次となってしまいがちです。さらにルールや体制自体が日常業務への制約になってしまうような事態になれば、むしろ積極的に守られない事態をも生じてしまいます。最新技術の導入や他社の運用方法を学習し、特に意識しなくても自動的に対応できるような仕組みを用意していくことが必要です。典型的な例は、ネットワークに繋がっているPC等を立ち上げる際に、PC内にインストールされているソフトウエアを確認するユーティリティや、新たなウイルス対策パターンを自動的に更新するシステムなどを用意し、利用者が意識的に対応しな

くても情報セキュリティ上の問題を減少させる仕掛け、仕組みがそれに当たります。

（２）セキュリティマネジメントシステムを、いかに徹底していくかという事項

情報セキュリティに限らず、マネジメントシステム全般に共通の事項ですが、マネジメントシステムを徹底するという対応策は、当然重要です。適切なマネジメントシステムが設定されているならば、これを愚直に運営し、個々の責任を明らかにして地道に運用をしていくことが必要です。

実際に運営されている会社においては、「最初は十分に納得されていなかったようなところでも、手を抜かずに着実に執行していると、利用者等も多数が従うようになる」という意見も数多く出てきています。逆に、設定されたルールを破っていても、対応策などを行わず、放置しているような組織では、「守らなくても構わない」という風土を醸成してしまい、様々な部分で破綻を起こしてしまうことに陥りがちです。

（３）セキュリティマネジメントシステムを、いかに的確に評価し改善していくかという事項

この部分も情報セキュリティに限らず、マネジメントシステム全般に共通の事項ですが、実施されているセキュリティマネジメントシステムをいかに的確に評価し改善していくかという事項の対応策も重要です。これは、セキュリティ監査や各種のチェック・検査を定期的に実施し、構築されたセキュリティマネジメントシステムが、有効に機能しているか、組織内外のリスク変化に伴って、セキュリティマネジメントシステム自体を見直す必要はないのかなどを確認することです。本事項はかなり専門的な力量が必要とされますので、適切に外部の力を使うことも必要となる場合があります。

第３章　課題と解決のヒント集

- 目次 -

- 目次 -

- 目次 -

項番	大分類	小分類	問題・課題事項	対処方法	備考
1	組織・体制	監査要員	◆（監査者の要員の不足） ・情報セキュリティに関する内部監査の要員がいない。	◇外部専門機関の支援を受ける。 ◇内部監査人にセキュリティ監査の専門教育を実施しスキル育成を行う。 ◇セキュリティ監査要員の採用を行う。	☆経営としてセキュリティをどう捉えるかの判断が重要である。
2	組織・体制	管理要員	◆（管理者の要員の絶対的不足） ・必要な要員がおらず、セキュリティを守るための体制が組めない。 ・セキュリティを推進する母体の事務局の業務が忙しすぎて,セキュリティ対策推進が後回しになっている。	◇リスク評価に基づき実施することを絞り込む。 ◇セキュリティの専門教育を実施しスキル育成を行う ◇セキュリティ要員の採用を行う。 ◇必要に応じ外部要員の使用を行う。	☆セキュリティを何処まで自社で守るかの判断が重要。
3	組織・体制	管理要員	◆（管理者の要員の不足） ・セキュリティの専門要員がおらず、兼務で対応しているため特定要員の負荷が高い。	◇セキュリティ管理者をある程度専任化して負荷低減を図る。 ◇リスク評価に基づき自社で実施すべきことを明確化し絞り込む。 ◇外部専門機関の支援を受ける。 ◇業務やシステム等を出来るだけ標準化する。 ◇セキュリティの専門教育を実施しスキル育成を行う ◇セキュリティ要員の採用を行う。	☆経営としてセキュリティをどう捉えるかの判断が重要である。
4	組織・体制	管理要員	◆（管理者の要員の質と量の不足） ・脆弱性対策等、考慮すべき事項が複雑多岐に亘るため適切な対策を適切な方法で実施することが難しい。	◇リスク評価に基づき自社で実施すべきことを明確化し絞り込む。 ◇外部専門機関の支援を受ける。 ◇ISMS認証を受ける等して、PDCAサイクルを確立する。 ◇長期計画を策定しセキュリティレベルを向上させる。	☆経営としてセキュリティをどう捉えるかの判断が重要である。
5	組織・体制	利用者	◆（利用者の質） ・ポリシー・ルールが末端まで浸透しない。（理解されない） ・推進する側と、ルールを守る側の意識・知識ギャップが存在する。	◇覚えてもらうポリシー・ルールを最小限に絞り込む。 ◇図入り・理解度テスト付のような資料（手引書）を作る。 ◇標語集・ポスターなどで啓発をはかる。 ◇仕組み（設備）でカバーできる部分は積極的に仕組み（設備）を採用する。 ◇キーマンを取り込み推進を図る。	☆最後の砦は人間であるとの認識に立った地道なリテラシーアップが必要。
6	組織・体制	意識・風土	◆（部署・組織間の差） ・部門によって取り組み方の温度差が出ている。 ・事業部門が6拠点に分かれており、かつ客先での業務が多い部門もあり、緊急連絡等での懸念がある。→業務により意識・風土が異なり統一的に推進することが難しい。 ・営業所など、SOHOオフィスのセキュリティ意識が低い。	◇キーマンを取り込み推進を図る。 ◇ポリシー・ルールの構成を原則的に守らなければいけないことと、現場である程度モディファイできることに分ける。 ◇現場である程度モディファイできる部分では現場の自主性を尊重する体制とする。 ◇ポリシー・ルールは文書でしっかり体系として構築する（最終的な判断はその文書で行う必要があるため）がそのダイジェストを図入りで分かりやすく要約した手引書を作る。 ◇ポリシー・ルールに関する小テストを定期的に実施理解度を確認する。 ◇システムログインやアプリケーション使用の際にポリシー・ルールの関係する部分を示し、その後ログインやアプリケーションの使用を実施させる。	☆セキュリティは経営課題であるとの認識が重要。

項番	大分類	小分類	問題・課題事項	対処方法	備考
7	制度	ポリシー	◆（ポリシーの構成・作り方） ・ポリシー・ルールを一から作るには荷が重いが、さりとて良い雛形はない。（特にプロシジャーの部分）	◇稚拙でも、まず作って、運用して見る。 ◇現場に任せられる部分は現場で作成する。 ◇共通に使うOS等の標準的な環境でデフォルトで守るべきポリシー・ルールの採用（ツール等への組込み） ◇業務分掌や職務規程へセキュリティ事項を盛り込む。（業務の一環として認知する）	☆汎用的に使用されている基盤についての汎用的なポリシーは流用を考える。
8	制度	マネジメントシステム	◆（システムがない） ・全社としての災害対策が出来ていない。→災害（セキュリティ対策の仕組みがない）	◇マネジメントシステムを構築する。 ◇リスク評価に基づいた優先順位に従いポリシー・ルールを策定する。	☆誰かが監視してマネジメントサイクル（PDCA）を回すのでなく自然に回るような仕組みが理想である。
9	制度	マネジメントシステム	◆（活用されない） ・インシデントを会社として管理する（災害事例として活用する）仕組みがない。	◇他社の仕組みを参考にして仕組みを作る。 ◇活用することに評価を与える。（活用を賞する。）	☆誰かが監視してマネジメントサイクル（PDCA）を回すのでなく自然に回るような仕組みが理想である。
10	制度	マネジメントシステム	◆（うまく動かない） ・セキュリティ管理委員会は開催してはいるが，ウィルス対策しか話題にならない。→セキュリティの仕組みがうまく動かない	◇セキュリティインシデントに賞罰を適用する。（問題を起こさないことにも正の評価を与える　無災害表彰） ◇ポリシー・ルールが実業務の手順になるようにする。 ◇ポリシー・ルールを守らないと損になるような仕組みを構築する。 ◇外部セキュリティ監査を受審し注意を喚起し、意識の向上を図る。 ◇他社事例等により注意を喚起する。 ◇過去のインシデントを整理（分類）して、重大な事例を全社員へ紹介する。（掲示板、メール、Newsなどを活用）	☆誰かが監視してマネジメントサイクル（PDCA）を回すのでなく自然に回るような仕組みが理想である。
11	制度	意識（モラル）	◆（個人の感覚） ・セキュリティは原則として守りであるという意識であり、ちゃんとやっても評価はされないが、問題が一度発生すると直ぐに罰せられる。このため後ろ向きにしか対応がされない。	◇セキュリティインシデントに賞罰を適用する。（問題を起こさないことにも正の評価を与える　無災害表彰） ◇セキュリティ対応を業務としてきちんと位置づける。（費用・人・時間を配分） ◇意識向上、啓発のためにQC的活動を推進する。（例えば、機密文書を机上に置きっぱなしにしない月間運動など） ◇目安箱を設けて、社内での指摘が簡単にできる仕組みを導入する。	☆最後の砦は人間であるとの認識に立った地道なモラルアップが必要。
12	推進	運用	◆（変更管理） ・異動や退職によるアクセス権限の変更が遅れる。 ・台帳上のPCの使用者と実際の使用者が異なるケースがある。	◇変更管理を強化する。 ◇定期的にU-IDの棚卸を実施する。 ◇人事システムと連動した仕組みを作る。 ◇変更管理の自動化を進める。	☆地道な努力が重要である。
13	推進	運用	◆（グローバル運用） ・海外グループ会社からの社内メールからウィルス感染してしまった。	◇海外との接続口にファイアウォールを設置する。 ◇ウイルスチェックを強化する。 ◇グローバルとしてウイルス対策の標準化を図る。	☆地道な努力が重要である。
14	推進	運用	◆（NotePCの運用） ・顧客からの要望で、NotePCにデータを入れて歩かざるを得ない。	◇使用するデータ・設備をなるべく絞る。 ◇ファイルにパスワードを設定する。 ◇PC上にデータを置かずに、必要時にサーバーからとる。 ◇生体認証・暗号化ツール等によるデータのセキュリティ強化を行う。	☆地道な努力が重要である。

項番	大分類	小分類	問題・課題事項	対処方法	備考
15	情報持ち出し		ゴミ箱に顧客に関する情報が捨てられている。	(1)全社員を対象とした啓蒙活動(説明会、WBTの義務化等) 秘密情報の管理ルールを作成する。 従業員にルールを周知徹底する。 委託業者と秘密保持契約を結ぶ。 個人情報保護のルールを作成して、従業員に周知する。 (2)チェック体制の構築 内部監査のルールと体制を作る。 懲戒のルールと体制を作る。 事件・事故報告のルールと体制を作る。	(1)顧客に関する情報 顧客に関する情報は、取引の信用上から秘密情報として保護する必要があります。また、その情報が顧客の個人情報である場合には、個人情報保護法によって保護され、その情報の本来の目的以外に使用されないよう保護する必要があります。更に、その情報が、顧客との秘密保持契約に該当する場合は、漏洩した場合には、契約違反になります。 (2)漏洩ルート ゴミ箱に捨てられた情報は、ゴミ収集業者に渡ることになり、どのように処理するかについて、業者と秘密保持契約を結んでおくことが必要です。また、ゴミ箱に捨てることは第三者(外部作業者)の目に触れることになり、会社に出入りしている外部作業者との秘密保持契約や誓約書を結んでおくことが必要です。
16	情報持ち出し		モバイルマシンの紛失、盗難が時々発生する。	(1)管理ルールの策定(紛失時の届け出、対応、機密情報の取り扱いを含む) モバイルマシンの管理ルールを作成し、従業員に周知する。 事件・事故報告ルールと体制を作る。 警察に紛失、盗難届を出す。 ルールを見直して再発防止策を打つ。 紛失、盗難保険に入る。 (2)場合によっては、機密情報の暗号化を行う。 個人認証の仕組みを組み込む。 ディスクを暗号化等により保護する。	モバイルマシンの社内外での紛失、盗難は年々増加しています。以前は盗難PCを中古市場に売却するケースが多かったのですが、最近ではディスク内のデータを売却するケースも出ています。このデータの漏洩から保護するために、ディスクのアクセスにパスワードを設けたり、暗号化して保護するなどの方法が用いられます。
17	情報持ち出し		重要な情報が電子データという形で簡単に持ち出せるようになった。	(1)社規、ルールの整備、教育。 情報の区分及び保護のルールを作成する。 責任者を決めて、組織的に運用する。 ルールを従業員に周知徹底する。 ルールが守られているかの監査を定期的に行う。 (2)電子メール添付、FTPの制限、監視。 電子メール添付のルールを作り、監視を行う。 FTPのルールを作り、監視を行う。 (3)アクセス権管理 アクセス権管理のルールを作成する。 システム管理者、従業員に周知徹底する。 アクセス権に変更があった場合の更新、及び定期的なチェックを行う。 (4)ログ収集 ログ収集の手順と責任者を決める。 重要なシステムについては定期的なログの監視を行う。	電子データの持ち出し方法は、電子メールへの添付やFTPなどの通信媒体による方法が容易に出来ます。このため、電子メールへの添付やFTPを禁止し、通信装置で制限しているケースもあります。その他、ノートPCや可搬型媒体を持ち込み、コピーして持ち出す場合もあり、社員あるいは外部作業者に対して、ノートPCや可搬型媒体の持ち込みを制限することも必要です。
18	情報持ち出し		顧客に機密情報が流出している。	(1)ラベルの周知徹底。 情報の分類、ラベル付け、取り扱いのルールを作る。 秘密情報を保護する組織、責任者を作る。 (2)啓蒙教育の実施。 従業員に教育し、周知徹底する。 (3)セキュリティ事故のルール セキュリティ事件・事故報告のルールと体制を作る。	機密情報の社内漏洩を防ぐには、ルールと表示と組織の3つの活動が必要です。第1は、機密情報保護のルールを作成し、社内に周知することです。第2は社内の情報のどれが機密であるかラベル付けをし、鍵付き書庫などに保管することです。第3は管理体制や責任者を決めて、組織的に運用することです。この一連の活動を行わずに漏洩した場合には、企業としての管理責任が問われます。

項番	大分類	小分類	問題・課題事項	対処方法	備考
19	情報持ち出し		機密ファイルなどの転送流出など	(1)運用の整備 機密ファイル等の保護のルールと管理組織を作る。 従業員に周知徹底する。 適切に運用されているか監査する。 (3)アクセス権管理 アクセス権のルールを作成する。 管理者にアクセス権を設定させる。 アクセス権に変更があった場合に設定を更新する。 (3)システム側での制限 電子ファイル転送のルールを作成し、システム側で制限する。 DRM(Digital Right Management)システムの導入。デジタル署名の導入。	DRMの導入により、認証された個人のみに情報の閲覧や承認処理を許可することができ、コンテンツが無断で使用されるのを防ぐことができます。また、誰がいつ何回コンテンツをアクセスしたかを管理することができます。 デジタル署名の導入により、正当な発信者から発信され、途中で改ざんなどが行われていないことを保証することができます。発信者は秘密キーで暗号化し、受信者は公開キーで復号化するとデジタル署名になります。
20	情報持ち出し		インターネットなどを介した情報の流出	(1)運用の整備 Web情報発信のルールを作り、周知する。 外部からのアクセスの認証を行う。 セキュリティ事件・事故の報告のルール、体制を作り、従業員に周知する。 (2)システム側の整備 アクセスログを取る仕組みを組み込んで、不正アクセスを調べる。 アクセスログ、パケットキャプチャーにより通過内容を保管する。 侵入検知システムを入れて、外部からの攻撃を検知して防ぐ。	内部者による不正送信の他に、インターネット上に無防備に情報を送信したことによる流出、外部からのハッキングによる不正アクセス、隠れチャネルやトロイの木馬による情報の流出などの危険から保護しなければなりません。 また、社員がホテルやインターネットカフェなどで会社のサーバーをアクセスすると、URL、ID、パスワードが残り、あるいはスパイウェアが仕組まれていて、後から不正アクセスされる危険性があり、ホテルやインターネットカフェからアクセスすることを禁止するなどの防御が必要です。
21	情報持ち出し		FD,CD-Rによる社内秘密情報の持ち出し	(1)運用の整備 秘密情報のルールを作成し周知する。 電子メール添付、FTPを禁止する。 秘密保持契約を従業員と結ぶ。 秘密情報の個人PCへの複製を禁止する。 (2)システム側での整備 PCバイオスレベル、またはユーティリティによるFD,CD-Rの無効化。 秘密情報をサーバーに置き、アクセス制御をしてコピーできないようにする。	社員あるいは外部作業者が、ノートPCや可搬型媒体を社内に持ち込み、持ち出すことにより、社内情報が漏洩する危険性があります。これを防ぐために、無登録のPCの社内ネットワークへの接続を検知する、可搬型媒体へのコピーを禁止する、アクセス権管理を徹底する、秘密保持契約を結ぶなどの対策が必要です。
22	情報持ち出し		自宅でインターネットを利用したりすることによるクライアントPCへの被害	(1)会社のモバイルPC 会社のモバイルPCの社外での私的利用の禁止。 会社のモバイルPCにウイルスチェック、パーソナルファイアウォールを入れて不正アクセス、攻撃、侵入から保護する。 会社の秘密情報をモバイルPCに保存して持ち歩くことを禁止。 (2)個人PCの会社への持ち込み 個人PCを会社のネットワークへ接続することを禁止。 個人のPCにウイルスチェック、パーソナルファイアウォールを入れて不正アクセス、攻撃、侵入から保護する。 (3)自宅PC 会社の秘密情報を自宅のPCへダウンロードすることを禁止。 パーソナルファイアウォールの導入。	クライアントPCを自宅など社外に持ち出し、インターネットをアクセスすると、ウイルスに感染することがあります。これを会社に持ち帰ると、社内のサーバーやクライアントPCに感染します。この危険性を防ぐには、クライアントPCに、OSのパッチ、ウイルス対応ソフト、パーソナルファイアウォールを入れて、かつ最新のバージョンに更新することが必要であり、対応が遅れると感染することがあります。

項番	大分類	小分類	問題・課題事項	対処方法	備考
23	会社間のルール		システム運用・保守を全面的アウトソースしている場合、アウトソース先のセキュリティポリシーと自社セキュリティポリシーに相違が発生する。	①契約事項に、自社セキュリティポリシー準拠を追加する。 ②契約後は、ヒヤリングやセキュリティ監査を実施し、セキュリティポリシー準拠を検証する。	◇セキュリティポリシー準拠状況は完全でないことが往々にして発生するため、ヒヤリング・監査の実施ならびに、実施後の対応策検討が重要である。（PDCA）
24	会社間のルール		部分的なハードウェアメンテナンスをアウトソースしている場合、アウトソース先のセキュリティポリシーと自社セキュリティポリシーに相違が発生する。	①契約事項に、自社セキュリティポリシー準拠を追加する ②回線経由での監視業務の場合、アクセス権を「読み込みのみ」とする。	◇回線経由によるハードウェア遠隔監視（サーバ稼動状況、ディスクアレイ稼動状況、PBX稼動状況など）等を想定している。
25	会社間のルール		開発業務をアウトソースしている場合、アウトソース先からのアクセス（セキュアな接続）を許可しているがアウトソース先のセキュリティーポリシー及び運用が不透明である。	①契約事項に、自社セキュリティポリシー準拠を追加する ②アウトソース先チームのネットワークと、アウトソース先企業ネットワークとを分離する。	
26	会社間のルール		資本関係のない企業に対し、限定業務をアウトソースしている場合、アウトソース先でのセキュリティレベルと自社セキュリティレベルに相違が発生する。	①契約事項に、自社セキュリティポリシー準拠を追加する ②キーマン間におけるヒヤリング、ならびに、ヒヤリング結果をに基づいた対応策の検討・実施	教育、情報セキュリティ委員会、内部監査、認証範囲の拡大。
27	会社間のルール		系列企業に対し、限定業務をアウトソースしている場合、アウトソース先でのセキュリティレベルと自社セキュリティレベルに相違が発生する。	①契約事項に、自社セキュリティポリシー準拠を追加する ②（資本関係の強弱を利用した）系列間セキュリティポリシーの統一化 ③キーマン間におけるヒヤリング、ならびに、ヒヤリング結果をに基づいた対応策の検討・実施	教育、情報セキュリティ委員会、内部監査、認証範囲の拡大。
28	会社間のルール		各事業部門間でのセキュリティレベルに相違が発生する。	①各事業部門キーマン間におけるヒヤリング、ならびに、ヒヤリング結果に基づいた対応策の検討・実施	教育、情報セキュリティ委員会、内部監査、認証範囲の拡大。
29	会社間のルール		派遣社員へのセキュリティ教育が徹底されない。	①雇用開始時に、自社セキュリティポリシーに関する教育を実施する。	◇契約更新あるいは一定期間ごとにセキュリティポリシー教育を実施することが望ましい。 ◇長期にわたる派遣社員に対しては、正社員と同等のセキュリティ教育を実施する例も見受けられる。
30	会社間のルール		委託契約先へのセキュリティ教育が徹底されない。	①契約事項に、自社セキュリティポリシー準拠を追加する	◇セキュリティポリシー準拠状況は完全でないことが往々にして発生するため、ヒヤリング・監査の実施ならびに、実施後の対応策検討が重要である。（PDCA）
31	メール処理		◆SMTPメールによる、内部からの情報漏洩 ・ある社員が社外者に送った電子メールに、誹謗・中傷の内容が書かれていた。 ・ある社員が電子メールを利用して、社員の電子メールアドレス帳などの個人情報を外部の人間に販売していた。	◇メールサーバーにフィルタリングソフトを導入し、誹謗・中傷にあたる言葉が電子メール本文中にあった場合ならびに添付ファイル名が機密情報名にあたる場合、電子メールが発信出来ないようにすると同時にセキュリティ管理部門へ通知する仕組みを設ける。◇セキュリティ事故発生時の追跡調査ができるように、メールサーバーならびにSMTPゲートウェイのログを記録管理し、ログをチェックできるようにする。	社員へ電子メール内容ならびに送信記録について全て記録されていることとシステム管理部門にてチェックしていることを事前に周知した上で、ツールを導入する必要があります。
32	メール処理		◆Webメールによる、内部からの情報漏洩 ・ある社員が社外者に送った電子メールに、誹謗・中傷の内容が書かれていた。 ・ある社員が電子メールを利用して、社員の電子メールアドレス帳などの個人情報を外部の人間に販売していた。	◇Webメールサイトへのアクセスを禁止する。	

項番	大分類	小分類	問題・課題事項	対処方法	備考
			セキュリティポリシーは策定したが、遵守状況が把握できないため、ポリシーの問題や運用の実態が把握できない。	【人的セキュリティ対策における遵守状況の把握】 （1）情報セキュリティに関係する社員、社員外含む利用者の一人でもポリシーを遵守しなければ、セキュリティはその人のレベルに落ち込んでしまう。まずは全利用者の情報セキュリティに関する認識及び行動を知るために、定期的な”自己分析（テスト形式）評価”を実施し利用者のレベルを把握すること。 例： 定期的なバックアップは出来ているか？ 例： 業務目的外の利用をしていないか？ 例： 許可のないPCをLANに接続していないか？ 例： 外部契約時に個人情報取扱特記事項はどう明記しているか？ 等 （2）定期的な訓練を抜き打ちで実施し、個人の情報セキュリティに関するレベルがどの程度向上しているのか？ 部署単位及び全社でどの位レベルが向上しているのか？ 訓練結果のデータ収集の記録 例： 不明な添付ファイル付きメール送信し、どう対処するか？ 例： 訓練用メールを受け取った際の行動ログ（クリック履歴）の記録 等 （3）システム構築時の設計段階から情報セキュリティ担当者の参加と内容の把握が必要である。システム検討会を開きシステム構築するにあたって、情報セキュリティポリシーに準拠した設計になっているのか確認。及び、システム公開後の変更時にも情報セキュリティ委員会への連絡と承認許可取得ルートを確立する。システム構築外部委託業者及びシステム維持保守担当（外部委託業者含む）への情報セキュリティポリシーの開示と徹底は事前に必須。契約時に情報セキュリティ規定に準拠した開発、運用の記述を盛り込むこと。	原因：利用者の認識レベルを把握する手段がない。 阻害要因：情報セキュリティに関する利用者の個人のレベルが低い。業務範囲外として注視しない。覚えるのが面倒くさい。IT/コンピュータへの毛嫌い。 システム構築にあたっては、構築外部委託業者によって、ポリシー外のHW、SWやプログラム言語が得意な業者もいる。納期優先でポリシー外の選択をする場合もある。特例が発生する。
33	記録の作成			【技術的セキュリティ対策における遵守状況の把握】 （1）セキュリティ対策ツールによる各種ログの記録 例： セキュリティホールの検知・確認・パッチ適用情報記録 例： ファイル単位のアクセス権限からサーバー単位のアクセス権限の不正アクセス情報の記録 例： ネットワーク機器（FireWall/ルータ/IDS/ウィルス対策ソフト等）のログ記録 例： ID/PSWD管理情報の記録 等 （2）各対策ツール/機器（FireWall/ルータ/IDS/ウィルス対策ソフト等）のログを集計し分析できるツールの導入により、状況把握が容易になる。	原因：対策ツールがなく、状況が把握できない。 阻害要因：費用対効果が見え難いし、ツール導入/維持費が高い。担当者のITスキルが乏しく、世の中技術動向が分からず、どのツールを選択すべきか分からない。
				【運用面の対策における遵守状況の把握】 （1）ユーザーヘルプデスクのユーザー対応記録によって、ユーザーの遵守状況の把握 （2）各グループ/部単位での情報セキュリティ担当者（その組織の長が相応しい）による、定期的な組織員の遵守状況を記録し報告を徹底する。怠った場合や管理下で規定違反が発覚した場合は連帯責任で人事的罰則や経済的罰則を与える。 例： 離席時には画面ロックがかかっているか？ 例： プリンタに印刷した書類を残していないか？ 例： 退社時にはPCに施錠を掛けているか？ 例： ID/PSWDを無闇に口外したり付箋に書いて置いてないか？ 等 （3）定期的な内部/外部監査における状況収集と記録 （4）ポリシー規定外を実施する際の、情報セキュリティ委員会への承認ルートの確立と記録	原因：運用体制が確立できていない。 阻害要因：全社的に優先順位が低く、かつ、経営層の情報セキュリティ知識が乏しいため。運用体制を整備することによる業務の増加及び人員確保などによる費用発生。

項番	大分類	小分類	問題・課題事項	対処方法	備考
34	記録の作成		ポリシー・規定類はできたが、PDCAが回らない。取組が長続きしないため、投資が無駄になる。	『計画』=>『実行』=>『チェック』=>『行動』のサイクルを円滑に循環させセキュリティレベルの維持/向上を図るには、全社一丸となって情報セキュリティ対策に真剣に取り組む必要がある。 『計画』 目的、目標、プロセスの確立(ポリシー策定)をするための人員の確保が必要。 1. 社の業務形態を熟知している人材 2. 経営戦略/経営層判断を熟知している人材 3. ITに精通している人材 4. 社内規定に精通している人材 (遵守事項を違反した際の罰則規定) 5. 確立した計画を理解し指導できる経営層 『実行』 策定したプロセスを実行できるように、利用者レベルを向上させポリシーを遵守させること。 1. 定期的なIT関連の教育・啓蒙活動 (セキュリティとは？から始まる) 2. 各種情報セキュリティ関連の記録・保管の徹底 3. 規定を遵守しなかった場合の人事系罰則と経済系罰則の実行 4. 技術的対策への費用投資 (ツール) 『チェック』 プロセス、製品、規定の遵守に関する監視/測定及び監査については、監督権限の拡大や経営層からのトップダウン的な指導が不可欠。 1. グループ/部の長が責任者となり、組織単位で規定を遵守しているかチェック 2. 内部/外部監査を実施。監査権限の拡大によって強制力を持たす。 3. 利用ユーザーの情報セキュリティに関連するレベルチェック 4. ツールやネットワーク機器によるチェック 『行動』 プロセスパフォーマンスの継続的改善のための処置を定期的に実施し再度『計画』を修正する 1. 技術的対応による各種ログと教育結果や監査結果記録などから、個人レベル、組織レベル、 全社レベルでの統計データを分析 2. 分析した結果をもとにポリシーの修正などを計画、実施する	原因:人員の確保が難しく、運用体制が脆弱に成り易かったり、規定違反時の全社的な罰則規定がない。 阻害要因:経営層の積極的な参加がない。費用対効果が見難く全社で取組難い。監査権限の拡大など、権限の拡大が会社的にスムーズに通らない。担当者の組織移動等にて業務の引継ぎが煩雑になり取組が長続きしない。担当者レベルの関心レベルも低いのが事実。
35	記録の作成		監査、監督権限が強固でないため、内部監査、監督が疎んじられる。	(1)監査、監督権限を拡大し絶対的な強制力を持たせる。 (2)監査に関しての妨害/不正については罰則の規定を設ける。	原因:社内の権限変更は容易でない。内部監査の場合、監査人と監査される側の上下関係/人間関係などが複雑。

項番	大分類	小分類	問題・課題事項	対処方法	備考
36	アクセス権限		アクセス権限に関するセキュリティ規定が厳格に実施され、情報を利用するためには、規定に沿った届けを行わないとアクセス権限が付与されず、情報利用ができなくなった。そのため、これを煩雑と考える利用者が、アクセスの申込みを行わなくなったため、結果として情報利用が減少した。	◇セキュリティ規定を厳格に運用することは必要である。ただ、セキュリティ管理者にとっては当たり前のことでも、利用者にとっては煩雑で、耐え難い運用であってはならない。利用者側の立場に立ってアクセス権限付与に関する運用を工夫する必要がある。例えば、情報資産のレベルに応じて、デフォルトで利用可能な部署等を規定し、予め権限を付与する。それ以上の高度なレベルの情報へのアクセスについては利用者がWebからの簡易な設定で利用申請し、セキュリティ管理者が審査し、権限を付与するような運用が考えられる。	◇阻害要因 ・セキュリティ規定が一般的なレベルよりも煩雑 ・アクセス者のセキュリティに対する意識が低く、少しの煩雑にも耐えられない。
37	アクセス権限		情報資産に対する、情報セキュリティのレベルが明確になっていないため、情報資産に対するアクセス権限が適切に付与されず、本来、権限を与えられるべきではない者が、レベルの高い情報資産にアクセスし、情報漏洩するといった問題が発生した。	◇情報資産に対するセキュリティレベルの明確化は最低限実施すべき事項である。その後、これに基づいてアクセス権限を付与するが、間違いはあり得るため、その後のモニタリングを実施する必要がある。セキュリティのレベルに応じて、情報資産へのアクセス状況をログ等により監査し、適切な利用者のみがアクセスしているかどうかをチェックし、本来、権限のない利用者がアクセスしている場合、直ちに、アクセスを制限し、権限の見直しを図る。	
38	アクセス権限		情報システム個々のアプリケーションに重要度の設定がなされていないため、アプリケーション毎に重要度がバラバラになっており、整合性がとれていない。このため、重要度の高いシステム例えば、経営者レベルのみがアクセスすべきシステムに対しても、一般の利用者がアクセスし、情報漏洩する問題が発生した。	◇アプリケーションと、そのアプリケーションがアクセスする情報資産とのリンク付けを行い、情報資産に対する情報セキュリティレベルに応じて、アプリケーションの重要度を設定する。	
39	アクセス権限		情報システム部門内でもセキュリティに関する意識の統一が出来てないため、アクセス権限を実現する仕組みが統一されず、バラバラの状態となり、アクセス権限設定時のミスが多発し、情報漏洩事故が頻発した。また、システム個々にアクセス権限の設定を行うため、コスト増の問題が発生した。	◇セキュリティポリシーに基づいたアクセス権限を実現するプラットフォームを構築し、全てのシステムがそのプラットフォーム上で構築されるようにする。	
40	アクセス権限		情報資産のセキュリティレベルは整理され適切なアクセス権限付与ルールも決められているが、実際にアクセス権限を付与する際に、付与者によって偏りが発生し、混乱している。	◇アクセス権限の付与については、1名で実施せず、管理責任者が確認を実施し、全体との整合性を取る。 ◇アクセス権限付与ルールは曖昧さを排除し、自動的に付与できる仕組みとする。	
41	アクセス権限		情報資産に対する適切なアクセス権限付与ルールが決められていないため、誤ったアクセス権限を付与し、情報漏洩が発生した。	◇利用者を部署、職位によりカテゴライズする。情報資産についてもその内容とセキュリティレベルでカテゴライズし、利用者と情報資産のマトリックスを作成し、誰に、どの情報資産へのアクセスを付与するか設定する。付与基準としては、セキュリティレベルの低い情報資産は、広範囲な利用者へ権限を付与し、レベルの高い情報資産に対しては、リスクと業務上の必要性、管理責任を総合的に判断し、決定する。	
42	アクセス権限		一人の社員に対し、複数のシステムアカウントが存在するため、退職時の抹消手続きが複雑になっている。そのため、退職者のシステムアカウント抹消手続きが遅延し、退職者による情報アクセスが発生し、情報漏洩が発生した。	◇システム毎にアカウントが別々になっている件に対しては、認証を1箇所で行う仕組みの導入で対応可能。 ◇アカウント抹消手続きの遅延は人事システムとの連携により、退職と同時に抹消することで対応可能。 ◇退職時の事務処理ルートを確立し、各システム管理者へ確実に情報が行き渡るようにし、即、システムアカウントの抹消を行う。	
43	アクセス権限		ライバル企業への退職予定者が、退職の1ヶ月前から、営業情報を密かに漏洩し、退職後、ライバル企業に持ち込んだ。	◇退職の意思が判明後は、退職予定者の上長は、システム管理者と連携し、退職予定者のアクセス状況をモニタリングし、不正を発見した場合は、法的処置を講じる。	

項番	大分類	小分類	問題・課題事項	対処方法	備考
44	ウィルス対策		【企業（組織）としてウィルス対策の認識が低い】 ◆問題が発生し被害が出ないと対策を実施しない傾向にある ◆被害の大きさが想定できず、問題発生時は企業として社会的責任を受けることとなる	①事象発生時のリスクを想定し危機管理の課題として経営に進言し経営層の意識改革を図る ②危機管理およびコンプライアンスの観点からウィルス対策業務を位置づけ、恒常的に運用できる体制を確立する	◇実施には相応のコストが発生するが投資対効果が明確にできないため、経営判断が困難 ◇対象システムによってはウィルス対策による障害発生などのリスクも発生する可能性がある
45	ウィルス対策		【個人としてウィルス対策の認識が低い】 ◆ウィルス駆除ソフトのインストール、日々のウィルスチェックを義務付けているが実施しない社員がいる ◆対策のアンバランスによりセキュリティホールが存在し、そこから被害の拡大が予想される	①実施しない場合には罰則を課すなどルールとして定める、また、人事考課にも含めるなどリスクが各自へフィードバックするような仕組みとする ②対策実施状況を公開することによる各自の意識の向上を図る ③e-ラーニングシステムなど、一般利用者でも理解しやすい環境整備を行い継続的な啓蒙活動を推進する	◇各種更新が手動になっている場合、更新の手間が掛かる ◇被害にあった経験がないとリスクに対する認識が薄い ◇二次感染による被害の実例（例えば、顧客へのウィルスメール送信等）を認識させることにより、ウィルスに対するリスクを認識させるのも有効である。
46	ウィルス対策		【ウィルスに対するシステム的な対策の仕組みの不備】 ◆情報消失による情報資産の消失 ◆情報漏洩によるビジネスチャンス・信頼の消失	①インベントリ管理システムの導入による管理の自動化・省力化を図る ②ソフトウェア配布、アンチウィルスソフトのエンジンやDATファイルの自動更新環境を整備し、環境維持の自動化・省力化を図る ③アンチウィルスゲートウェイの導入	◇各種更新が手動になっている場合、更新の手間が掛かる ◇ウィルス対策ソフトやセキュリティパッチの適用によって稼動中システムへ影響を及ぼす可能性がある
47	ウィルス対策		【すべての事業所に対し、ウィルス対策を実施できない、またはウィルス対策要員を配置できない（特に、遠隔地の事業所の場合）】 ◆情報消失による情報資産の消失 ◆情報漏洩によるビジネスチャンス・信頼の消失	①ウィルス感染時対応を制定し、徹底を図る ②Webベースドトレーニング（WBT）ツールによるウィルス教育実施 ③既存の業務フロー・ツール（たとえば、朝礼やWeb掲示板）にウィルス教育コンテンツを組み込む。 ④ウィルス感染する恐れがある経路（たとえば、インターネット接続）を集約し、集約した経路に対しアンチウィルスゲートウェイ機器を導入する。	◇ウィルス感染時対応として、「感染が発見された場合、LANケーブルを抜く」といった最小限の対応をするだけでも、二次感染を防ぐことが可能です。 ◇既存の業務フロー・ツールに、ウィルス情報・対策を組み込むことにより、個々の従業員が違和感なくウィルス情報・対策を目にすることが可能です。 （新規ツールとしてWBTツール導入した場合、「新規」ツールに対して使用者の抵抗感が強く、導入効果が薄れる場合が多々存在します。）
48	ウィルス対策		【ウィルス感染時のプロシージャが存在しない】 ◆情報消失による情報資産の消失 ◆情報漏洩によるビジネスチャンス・信頼の消失	①ウィルス感染時の報告経路を制定し、徹底を図る。 ②ウィルス感染時対応を制定し、徹底を図る。	◇可能であれば、全社的なウィルスヘルプデスク要員を配置することが望ましい。（要員は社内外を問わず）
49	専門人材育成		『個人情報保護法』、『不正アクセス防止法』などの法令遵守が徹底しない。	教育プログラムの中にコンプライアンスの項目を盛り込む。 -管理職教育 -昇格時研修 -新人研修 等。	法務部や弁護士、セキュリティコンサルタントなど法律問題に詳しくかつ事例、判例に詳しい専門家の助力を借りることが有効です。 また日常業務でやってはいけないことをできるだけ具体的に示すことが理解につながります。
50	専門人材育成		法令遵守（コンプライアンス）に関し、守らなくてはいけない事項、遵守を阻害する要因が明確になっていない。 また社員に対する教育が徹底されていない。	(1)遵守すべき法律をリストアップし、それぞれについて業部に基づいた対策を立案する。 (2)対策に基づいた教育を、現場マネージャの義務とする。 (3)当事者を集めてリスクマップ等を作成させる。	(1)具体的な業務フローにおける対策が明確になります。やってはいけないことが明確となります。 (2)具体的な業務を遂行する社員への周知徹底が期待できます。 (3)リスクマップ作成については、経営コンサルタントなど専門家の助力を得ることも有効です。
51	専門人材育成		セキュリティ全般を評価できる人材がいない。	(1)外部の専門家や同じ立場の人たちが集まった、セキュリティマネジメントの研究会などに、社員を参加させる。（外部交流） (2)社内でのシステム監査やセキュリティ監査に、社員を参加させて経験を積ませる。	(1)例えばJUASの研究部会に参加するなど。営利を目的としない中立的な活動が望ましいです。 (2)ISMSの取得により経験を積んだり、資格の取得をさせたりすることで自ら学習できる機会を与えるのも有効です。（システム監査、情報セキュリティアドミニストレータ、ISMS審査員資格など）
52	専門人材育成		問題点を発見できる監査能力を持った人材がいない。	(1)社内でのシステム監査やセキュリティ監査に、社員を参加させて経験を積ませる。 (2)教育プログラムを作り、養成する。	ISMSの取得により経験を積んだり、資格の取得をさせたりすることで自ら学習できる機会を与えるのも有効です。（システム監査、情報セキュリティアドミニストレータ、ISMS審査員資格など）

項番	大分類	小分類	問題・課題事項	対処方法	備考
53	専門人材育成		現実のセキュリティをマネジメントできる人材がいない。	(1)セキュリティマネジメントの教育プログラムを作り、各職場に提供する。 (2)セキュリティマネジメントのヘルプデスク(問い合わせ窓口)を設置する。	(1)具体的な手順などを、わかりやすくまとめた資料を提供したり、あるいはWebを使ったトレーニングプログラムを用意するなど。
54	専門人材育成		セキュリティ技術を理解して使いこなせる人材がいない。	(1)職場のネットワーク管理をWGを作って実施させ、経験を積ませる。 (2)社内ネットワーク構築など具体的な作業が発生するプロジェクトに参加させる。	全社で組織される情報セキュリティ委員会や、技術系の委員会などに参加させることも有効です。
55	専門人材育成		具体的なセキュリティ対策を個人として実施できない人がいる。	(1)ヘルプデスクを設置し、問い合わせ窓口を広報、周知させる。 (2)対策に関するTIPSをスキルがないひとでも理解できるようにわかりやすくする。	
56	本人認証		パスワードの定期変更が徹底されない。	(1)定期的変更の必要性を理解させる。 (2)OSのパスワードポリシーの設定。 ・最低文字数 ・有効期限 などセキュリティポリシーに従って設定しパスワードの変更を促す仕組みを作ります。 (3)リボーク機能の設定 ・パスワードの誤入力が続いた場合、アカウントを一時的に無効化します。 (4)管理台帳を作成し、更新を管理職に義務づけ、内容を社内に公開する。	(1)ユーザーにパスワードの変更が必要な理由を理解させることにポイントをおきます。 例えばランダムな文字を使ったパスワードの、ツールでのクラッキングに必要な時間を説明し、クラッキングの所要時間以内に変更を行うことで危険性を低下させることを理解させる。 (2)セキュリティポリシーのパスワード運用規程に則って設定します。 (3)万が一、システムが不正アクセスを受けたときクラックされる確率を低減させるための設定です。一般ユーザーのアカウントに設定します。Windows系では、管理者アカウントでは使えません。 (4)パスワードの変更状況をイントラネットで公開します。またパスワードの期限切れが近くなった場合、上司経由で催促を行い、上司に対応を報告させるような仕組みを作ります。更新の入力は、イントラネットで各自ができるような仕組みが必要です。
57	本人認証		ソーシャルエンジニアリング対策をどこまで実施すべきか適度な基準が明確でない。	(1)社内電話帳をもとにコールバックして、本人であることを確認する。また上司などの第3者に連絡し申請者本人であることを確認する。 (2)社員証(写真)による本人確認をおこなった上で、パスワードを再発行して、直接本人へ通知する。 (3)社内システムの認証方式にあわせて、認証情報の再設定ルールを決めます。管理者に対してルールの教育を行います。	(3)社内システムの特性に合わせて、認証情報の再設定ルールを決めます。例えば、オフィス内ではID、パスワードの認証を使い、RASではTokenカードによるワンタイムパスワード認証をおこなっているような場合は、 ・パスワード再設定ルール:内線電話によるコールバック確認、申請書の上司へのCC送付など。 ・Tokenカード紛失ルール:紛失手続きを行ったのち、新規申請を行う。(上司の承認が必要。) また経営者も含めて運用ルールを周知させます。
58	本人認証		認証に必要なパスワードなどを複雑にすることが難しい	(1)Tokenベースの認証、ワンタイムパスワードなど (2)パスワード診断ツールを利用する。 (3)シングルサインオンの仕組みを導入する。 (4)安易なパスワードの危険性をデモや実際のデータを示して社員に理解させる。	(1)特にRASからのアクセスは脅威が大きいので、これらの方式を利用することが一般的です。このとき、紛失、盗難に備え下記のような対策もあわせて取る必要があります。 ・PIN番号はメモしない。 ・紛失時に、当該Tokenカードを無効化するためのルールを決める。 ・紛失時のペナルティ(実費を負担させるとか) (3)複数のサーバーを利用する環境の場合、一回の認証で済ませるような仕組みを構築します。複数のID、パスワードの運用は煩雑性が増し安易なパスワードの割り付けを助長します。 (4)ユーザーに安易なパスワードが如何に危険かを認識させることにポイントをおきます。 例えばツールでのクラッキングに必要な時間を説明したり、パスワード辞書の内容を説明する。などが考えられます。

項番	大分類	小分類	問題･課題事項	対処方法	備考
59	規程見直し		機密区分がしっかり運用されていない。当社では、技術情報の漏洩を嫌い、頻繁に使用されるマニュアルの殆どが極秘情報になっている。極秘資料は使用後、直ちに返却しなければならないにも係わらず、次の使用を見越して自己保存している。	■紙媒体の場合 ・貸し出し記録ノートによる所在管理（期間・氏名など） ・資料管理者の設定（書類キャビネット鍵管理・貸し出し管理） ・極秘資料の明示（機密＋取り扱い事項など押印） ■デジタルデータの場合 ・システム設定の見直し（複製及び印刷は不可、閲覧のみ可能）	
60	規程見直し		情報量が爆発的に増加し、重要なのか、正しい情報なのかなど、評価・確認が分からない。管理対策をきめ細かく行うため、詳細分析を採用し、総合的判断も必要なのでセキュリティ標準委員会で情報区分（ラベル）付けを行うこととした。しかし、業務の拡大により、判別しなければならない情報量が爆発的に増加し、各委員も業務が多忙で欠席が多く評価されないまま、実施されている。	■情報管理策定アプローチの見直し ・現在の企業内情報ではなく、金銭的被害の大きい企業情報による分類策定 ・上記優先順位順に１つずつ管理対策策定と実施 （デジタルデータ、紙媒体の管理方法）	
61	規程見直し		セキュリティ規定の変更が実施されない。当社では、商品販売に伴いユーザーカスタマイズのための技術情報を提供する。（範囲は情報機密区分の程度により提供）この為、当商品は販売実績が良い。当商品群は商品寿命が短く、それにつれ機密度が低下するが、機密度はイントラネット上で行う。しかし、営業員はイントラネットの利用が少なく、その変更を知らないことが多い。そのため、販売機会を失っている。	■営業員が利用するイントラへの変更 営業員の販売機会損失を防ぐためにイントラのコンソリゼーションを行い変更情報を一元化した企業ポータルにて提供する。	
62	規程見直し		情報開示ポリシーが設定されていない。当企業は先端技術の開発をコアとしている。学会での発表は企業イメージを高めるとして推奨されている。しかし、極秘情報とされるものまで発表されたため、競合企業に新商品開発で負けてしまった。研究員は、経営者の情報開示ポリシーとセキュリティ尊重の板ばさみになっている。	■情報開示ポリシーの見直し ・項番60（金銭的被害レベル）での対処法などをベースに情報開示ランクを設定する。 ※顧客プレゼン、学会、NDA時など ・項番61（企業ポータル）などでの情報開示 ・情報開示前の監査策定	
63	規程見直し		全社的なセキュリティポリシーを現場での運用にマッピングできない。当社は2大営業所と多数の地方営業所を持つ販売会社である。セキュリティーポリシは本社担当役員と2大営業所所長をメンバーとしたセキュリティ委員会で策定した。しかし、多くの地方営業所は人数が少なく、専門知識を有するスタッフもいないので、現場での実施にまでセキュリティポリシーを落とし込めない。	■セキュリティポリシー実施方法の見直し ポリシーとしての目的は変えずに実現するための方法を見直す。 例えば ※現場スタッフの職務を圧迫せず実施するには ・専門スタッフを確保する。 ・人に依存せずシステム側（技術）でサポートする	

項番	大分類	小分類	問題・課題事項	対処方法	備考
64	不正アクセス		社員のセキュリティ意識が低い ・自分は大丈夫だと思っている。 ・セキュリティパッチ適用、WinNT、フリーウェア等	(1)デモを交えたセキュリティ教育を行う。 　－ハッキングデモ 　－パッチを適用していないために発生したセキュリティ事故の事例を説明 　－ポリシーに違反して、事故を起したときの懲戒処分を具体的に説明する。 (2)ポリシー遵守の誓約書へのサインを求める。	(1)の教育では、具体的な事例や発生する脅威をできるだけわかりやすく説明することにポイントをおきます。 ハッキングのデモなど社内で対応できない場合は、専門家に依頼することを検討します。 また懲戒処分に関しては、(2)の誓約書を根拠として厳正に実施すること、また中身についてできるだけ具体的に理解させます。
65	不正アクセス		インシデント発生時において、インシデントの発生自体に気がつかない	(1)監視体制の整備（人員含む） 　－Firewall、IDS、認証サーバーなどのログの定期的な監査を管理者の職務の一つとして実施する。 　－職務の週報などに解析結果の報告を義務づける。 　－ログ解析ツールを導入する。 　－職務定義書などに明確に記述する。 (2)インシデント情報データベースの整備 　－社内で発生したセキュリティ事故の記録をセキュリティ委員会などで収集し、社内に広報する。	(1)ISO9000などの対応で職務分担や職務定義書などがあれば、これらに明確に記述します。 また担当者の負荷を低減するための処置として、ログ解析ツール等の導入も必要です。 また人的リソース不足などで社内で対応できない場合は、社外のサービスの利用も検討します。
66	不正アクセス		インシデントの報告がされない。	(1)インシデント対応ルールを社員に周知する。 －パンフレット、イントラネットでの広報 －報告された内容の利用について広報 (2)インシデント情報データベースの整備 　－社内で発生したセキュリティ事故の記録をセキュリティ委員会などで収集し、社内に広報する。	インシデント報告については、報告先、報告内容などを緊急時対応計画などであらかじめ定めておきます。 また報告された内容が、インシデント情報データベースなどに蓄積され再発防止のために利用されることを周知させることで、その重要性が認識されると思います。
67	不正アクセス		外部の人間が会社内の情報倉庫に潜り込むことが容易にできるようになり、企業のコアコンピタンスを脅かすようになった。	(1)セキュリティマネジメントの取り組みを行う。 　・リスク分析を実施し、脅威と脆弱性を明確にした上で結果として発生する可能性のあるリスクの大きさを評価する。 　・リスクの大きさに応じて相応の対策を取る。 　・ISMSの認定を受け、継続的な取り組みを行える体制を社内に構築する。	基本的には、ISMSの仕組みを構築して、継続的なセキュリティへの取り組みを行うことが必要です。
68	不正アクセス		社員のセキュリティ意識が低く、社内で義務付けているWindows Updateを行わず、またフリーウェアなど出所の不明なソフトウェアをインストールして利用している。	①意識を改革させるために、実際にセキュリティパッチを適用していないために発生する危険性を実際のデモを交えて見せる。 ②社内のルールとして違反をした場合の処分などを明示的にし、社としてもセキュリティに対する取り組みの重用性を示す。 ③その内容に同意する署名をしてもらい心理的効果を狙う。	習慣的に意識付けさせるための工夫が1番必要。
69	不正アクセス		社内で運用しているシステムに関して何か問題が発生していてもそのことに気づかない。	①ファイアウォール、IDS、認証サーバーのログを定期的にチェックする管理体制を作る。 ②管理者は何が正常なログであるかをベンダーに確認するとともに、その製品に対して理解する必要がある。見たことのない、また不正だと思われるログに関してはベンダーに問い合わせできる体制を整えておき、セキュリティに対する事故や対策の記録をとる。 ③②の記録を社内に公開して社員に対して意識付けもおこなう。	
70	不正アクセス		社内で運用しているシステムに関して何か問題が発生しているにも関わらず、報告されず、放置されている。	①インシデント対応に関しての方法やルールをイントラネットやパンフレットなどで周知させる。 ②対応方法をルール化しそれに則った対応がなされていない場合は処分を与えるようにセキュリティに対する意識付けを行う。	

項番	大分類	小分類	問題・課題事項	対処方法	備考
71	不正アクセス		不正侵入検知システム（IDS）を導入したがアラートが大量にで、どのアラートが不正によるものかわからない。最終的にはIDSを止めて運用する。	①社内ネットワークの構成を確認して各サーバー、クライアントで利用しているサービス、プロトコル、ポートは何かを把握する。 ②IDS製品について理解する。IDS検知システムの適切なポリシー設定方法、（どのプロトコルのポートが現ネットワークでは不正かを決める）構成方法を理解検討する。（どの場所に機器をおくかなど。） ③導入後にはネットワーク内で稼動しているサービスの全てにアクセスし、ログがでるか出ないかなどのチェックを行う必要がある。また不正アクセスを擬似的に起こしログのフォーマットを理解することも大切である。	日頃、ネットワークの管理として、どのサーバーで何を利用しているのか、常に管理することが大切である。 また稼動している製品についての運用知識は最低限必要である。
72	不正アクセス		ある社員がヘルプデスクにノートPCを修理依頼した時、サポートスタッフが会社で配布しているソフト以外のソフトが多くインストールされていることを発見した。そこでPCをチェックしてみると、スパイウェアなどがインストールされていた。またインターネットの履歴をみるとURLフィルタリングで禁止されているはずのURL履歴が残っていた。このユーザーは自宅でインターネットを利用してソフトウェアをダウンロードしたことを認めた。	①部署内に管理者を設け、定期的にユーザーのPCをチェックする環境を構築する ②会社でサポートしていないソフトウェアをインストールする場合、申請を必要とする。 ③会社外のインターネットアクセスは常に会社を経由するような仕組みを構築する。ブラウザにプロキシサーバーの設定を固定するなど ④スパイウェアを発見するソフトを定期的に動作するように各クライアントにデプロイする。	PCの中をチェックされるかもしれないという、心理的なものをユーザーに与えることにより、不正な利用を控えようという気持ちにさせる。
73	不正アクセス		サーバーのログを調査していると休日にサーバーにログインを試みようとした形跡が発見される。管理者に聞いたところ休日は出勤しておらずサーバーにはアクセスしていない。サーバーは物理的には誰でもアクセスできる場所にあるため、誰がアクセスしたのか把握できない。	①サーバーを鍵のある場所に設置し、入出管理記録ができるようにする。 ②サーバーをデータセンターに預け、常にセキュリティが確保された状態にしておく。	常に、サーバーへのアクセス記録がとれるような体制にする必要がある。リモートからアクセスする場合はサーバー内のログを記録することはもちろん、物理的なアクセスの場合にも記録が残るような設備、手順を整える。
74	不正アクセス		社内の一般ユーザーよりビルの共有部分から無線LANにアクセスできると知らされ、セキュリティが確保されていないのではないかと心配になる。そこで外部のセキュリティ調査を依頼しセキュリティに関して改善すべき点を相談した。その中にエクストラネットへのアクセスもあげられ現状のID制御だけでなく、認証情報とデータの暗号化が必要であると指摘を受けた。	①IPSec、HTTPSなどのVPN導入を検討。 ②2要素認証など、より強固な認証を利用して本人であることを証明する。 （What you know, What you haveなど ）	①、②を構成する中で、どのサーバーをVPNで外部にアクセスさせるか、またはどのサーバーは外部には完全に隔離するかなどポリシーを定める必要がある。
75	不正アクセス		社内のセキュリティを強化するため、ファイアウォール以外に不正侵入検知して防御するIDPを導入した。しかしこの機器を導入してからユーザーからあるアクセスが利用できなくなったと苦情が多発。IDPのログを調査してみると、複数のサービスが利用できないようなログが残っている。これでは他のサービスも利用できなくなっている可能性があるのでIDPの運用を見送る。	①社内ネットワークの構成を確認して各サーバー、クライアントで利用しているサービス、プロトコル、ポートは何かを把握する。 ②IDS製品について理解する。IDS検知システムの適切なポリシー設定方法、（どのプロトコルのポートが現ネットワークでは不正かを決める）構成方法を理解検討する。（どの場所に機器をおくかなど。） ③導入後にはネットワーク内で稼動しているサービスの全てにアクセスし、ログがでるか出ないかなどのチェックを行う必要がある。また不正アクセスを擬似的に起こしログのフォーマットを理解することも大切である。	

項番	大分類	小分類	問題・課題事項	対処方法	備考
76	一般社員の認識	ITリテラシー教育	新規導入またはサービスを社員に徹底する仕組みが不足しているため、オペレーションにあたって認識すべき注意事項等を理解しないまま使用している。	新規のアプリケーション及びシステム等の導入については、 1）導入担当者を明確に決め、社内調整のもと、ユーザーへの教育を行う仕組みを作る。 2）マニュアル等の整備も導入担当者の業務とする 3）マニュアル参照だけで済むものと教育が必要なものとのレベル分けをし、効率よく進める 4）導入した社員の理解度を測る仕組みを作り、必要に応じて再教育または定期的な更新教育を行う	
77	一般社員の認識	ポリシー浸透の壁	社内掲示板にセキュリティポリシーや情報セキュリティマニュアルを公開したが、社員が読んでおらず、浸透しない。	【社内掲示板が読まれない原因】 1)社員にITを利用した業務の体制が浸透していない 2)他の業務に優先順位が置かれているおり、掲示板を見に行くことやポリシー、マニュアルを読むことの優先度が低い 【対応策】 1）ITを否応なく利用させる Webベースのトレーニングシステム導入、ならびにトレーニング結果を鑑みた業績評価制度構築。 ・部門ごとに参加率や浸透率を評価し成績順に公表することで競わせる。 ・受講状況を事務局で把握・管理する（業務の一部として） 2）全員参加を条件とする（義務化） ・参加全社員を対象とした啓蒙活動（説明会、WBTの義務化等）を継続的に行う ・業務の一部であることを明示して参加しやすい雰囲気を作る ・社員が自らの問題として認識できるような工夫（社員全体を巻き込む） ・読むことを仕事の一部として組込み、全員で読む時間を持つ →会議の場で毎回数項目ずつ読み合わせ、話し合いをもつ、等 ・入社時の研修に組み込む ・経営トップからのメッセージ発信、続いて幹部役員、部門長、リーダークラスへと同じメッセージを共有し、確実に社員に訴えかける仕組みと役割分担を構築する（＝全社的な動きにする）。特に部門長の認識が重要。	
78	一般社員の認識	教育への不参加	業務多忙を理由にセキュリティ教育に参加しないため、本人が気づかないうちにセキュリティポリシー違反を犯す恐れがある。	部門長とのコミュニケーション。 ・まず部門長から率先して参加する姿勢をもつ。 ・仕事の一部であり、組織の構成員としての義務であることを認識させる ・全員が参加することの意味を明確に伝える（セキュリティはたった一人の脆弱性により崩れる） ・部全体の会議などで全員で少しずつ読みあわせを行う（一度で終わらせる必要はなく、毎回少しずつ行う） →継続することにより、意識を根付かせる	
79	一般社員の認識	内容の不理解	・セキュリティポリシーを社員に浸透させる仕組みができていない	・社員自身が、自分にとって身近な問題だと理解できるような伝え方の工夫 ・効率よく社員にセキュリティの必要性及びポリシーを教育する仕組みの構築 ・自社の情報がどの程度重要性をもち、漏れるとどんな被害があるのかを理解させる	
80	一般社員の認識	意識の低さ	・社内で起こる可能性のあるセキュリティ事故に対する、被害が実感できていない。 ・セキュリティの必要性が社員に理解されていない	・具体的な自社のインシデント事例を作成して、シミュレーション体験させる（インシデント発生時の想定被害金額含む）	

項番	大分類	小分類	問題・課題事項	対処方法	備考
81	一般社員の認識	技術／非技術の違い	技術部門（技術者）はセキュリティの重要性を認識しているが非技術者部門ではあまり重要と考えていない。インシデント阻止は重要と認識しているが技術的対策が良く分からない。 また、技術系の人間がセキュリティの重要性について理解せず、利便性を追求するあまりセキュリティを無視する。	・インシデント事例の公開（金額含む） ・継続的な社内教育の実施 ・技術系部門と非技術系部門とでは知っておくべき知識が違うことを認識した上、双方が知るべき内容を分類する（非技術系には理解できないことも多い） ・上記知識をもとに、有事の対応（役割り分担）を具体的に定め、手順として社内に定着させる。 ・インプットは繰り返し行う	
82	その他		・セキュリティレベルの強化が操作性、利便性を阻害する。～「セキュリティを強化することが、操作性、利便性が一方的に低下する」と考えられており、セキュリティマネジメントへの協力が低下してしまう可能性がある。セキュリティを守るためには、際限なくコストがかかると思われており、限度範囲が不明確になっている。 ・業務オペレーション時において、これまでの業務オペレーションに、セキュリティレベルを向上するために、後からプロセスを追加すると現場から反発（煩わしい）が発生する。 ・業務優先でセキュリティ規定が守られない。	・セキュリティレベルの強化を行う際に、「コストバランス」「可用性」を重視したリスク分析を行い、無理なレベル強化がされないようにする ・反発される可能性が高い「キーメンバー」とのインタビューを行い、「会社として総合的に良い方向性」を一緒に話し合うようにする ・投資可能予算総額を明確にし、運用コストを「成り行き管理」と比べて評価する ・オペレーションプロセスに影響がでないような仕組みの実装 ・【一般社員向け社内ルール】情報漏洩時責任の一部を、一般社員にも負わす。	今後の作業として、理想のセキュリティレベルと現状とのギャップを埋めるフェーズがある。（PDCA） ISMS導入現場を見ると、「煩わしい」の意見は必ず表面化するが、時間と共に「面倒だがルールの一部」と認識されることが多い。ルールの一部であるとの認識までの所要時間は、ルールチェックをする立場の人材選びに大きく依存する。 セキュリティ規定が業務の一部であることを認識させることが、重要。
83	その他		社員のセキュリティ意識が低いため、自組織、自担当の利便性のため、社内システムの脆弱性を探し、ローカルルールを作ろうとする。	・罰則の明確化をすることと、マネジメントの管理責任徹底を図ることで、未然防止が進むようにする ・ローカルルールを作って対応しようとする「キーメンバー」とのインタビューを行い、「会社として総合的に良い方向性」を一緒に話し合うようにする	現状は、「セキュリティを高める」という作業のみがクローズアップされているが、セキュリティを高める本来の意義とは、質の高い企業活動をさせる手段の一つである。
84	その他		システム開発時において、インフラ部分に関するセキュリティ要求は明確であるが、アプリケーション（社内システムなど）に関しては、顧客からの機能要求仕様（利便性がある）自体がセキュリティホール（情報漏洩）になっている。	・このままのやり方で開発を行うと、どのような問題が起きるのか、「成り行き予測」を誰にでもわかる形で相手に示す。利便性を保ちつつセキュリティレベルを向上するための代替案提示を行う。 ・IPAのセキュアプログラミングガイドラインを元に、アプリケーションを実装する。アプリケーション要求定義のひとつに、セキュリティ要件を設ける ・既存のアプリケーションに対するセキュリティテスト（ツール使用）を実施し、修正を必要とする箇所を洗い出す。 ・要求に対するセキュリティホール一覧表の提示やインシデント例の提示を行い、説得をする ・書面による記録の保管（続行時）を行い、罰則等の適用の証拠とする。	顧客からの要求仕様がセキュリティホールになっている場合は、プロトタイプアプリケーションに、セキュリティチェックツールによるテストを実施し、セキュリティホールであることを認識させる。
85	その他		セキュリティは非常に幅が広く、専門用語など理解しにくい（非技術者）部分がある。また、それを理由に協力が得られないことがある。	・わかりやすい用語集、ハンドブックを作成し、「間違い」が起きないように、注意を喚起する ・【一般社員向け施策】（専門用語理解に対しては、「学習する」ことが必要なため） 全社員が閲覧する、本社部門からの社内コミュニケーションツール （例えば、全社員向けメールやWeb掲示板） にセキュリティ用語説明を組み込む。（普段使用している社内コミュニケーションツールに、学習コンテンツを組み込むことにより、学習側に運用負荷を感じさせないことを目的としています。） ・幅広い情報の収集や専門家の育成を継続的に行い、利便性のあるソリューションの検討が行われるようにしていく。	「セキュリティ」の文字で表される新しい仕組みを業務フローに組み込むためには、既存インフラを利用することにより、比較的ではありますが、理解ならびに導入を促しやすい。
86	その他		情報インフラが経営の動脈となり、故意や過失で停止すると、企業の多くの活動が停止する。	・インフラ停止の可能性を「リスク分析方式」で確認を行い、個別に対応策を決めていく。 ・発生の蓋然性が高い部署・機能に対しては、マネジメントレベルの方に「リスク発生時の責任」を明示して伝える。 ・教育し、できているかどうか内部監査を行う。クリティカルな職種は複数アサインして相互牽制を行う。 ・【経営陣向け】上記記載の「個別の対応策」の実施費用、すなわちリスク発生回避費用を算出し、マネジメントレベルのほうに、リスク発生時の責任に加えて、「リスク発生回避費用」を明示する。可能ならば、「リスク発生時の責任」と「リスク発生回避費用」を認識させ、リスク発生回避施策を実施するか否かを決定する場を持たせる。（追記：この項目に限る対処方法でなく、全てに当てはまってしまいますが…）	

項番	大分類	小分類	問題・課題事項	対処方法	備考
87	その他		個人情報の漏洩や社員による外部への不正アクセスがあると、会社が厳しく糾弾されるようになった。	・自社の業態に近い形で発生したトラブル／その損害を伝えるようにすることで、「自分の問題」として理解させるように仕向ける ・【一般社員向け施策】（内部に限った情報漏洩抑止の目的で）メールフィルタリング、フォレンジック等の導入、ならびに導入施策の機能を周知し、抑止効果を狙う。 ・ルールの整備、教育による周知、相互牽制、懲戒制度を設けて抑止する。アクセス制御を強化する。アクセスログを取って監視する。	今後は、個人情報保護法への対応についても考慮する必要がある。
88	その他		火災対策、地震対策が十分にできていない。	・地震／火災が起きた時のリスク分析をしっかり行う。分析結果から導き出される責任分掌を個別部署に割り当て、計画化する。また、分析結果をマネジメントレベルに認識させ、経営課題に組み込むことが望ましい。 ・現象的には、防火性、耐震性を高める。ハード、ソフト、データのバックアップを整備する～マシンルームを分散するなどの施策を計画する。	ディザスタリカバリ（DR）サイト構築がベストだが、膨大な投資が必要となる。コストを抑えるためには、情報資産ごとに資産価値ならびにセキュリティレベルを算出し、算出結果に応じたDR方式を適用するとコストが抑えられる場合がある。 （DR方式を細分化しすぎると、逆にコスト高を招く） アウトソーシングサービスを利用すると、比較的安価にDRサイトを構築可能
89	その他		機密情報の管理が不十分で、情報の管理分類がされていない	・情報を管理するためのシステムの統一化を行う。 ・管理分類が誰にでもわかるようにし、分類者による差異が起きないようにする。 ・「情報漏洩時のリスク」を「成り行き分析」で定量化し、経営者の危機感を誘う ・これらを浸透させるために、教育の徹底、管理の徹底、内部監査を行う。	
90	その他		・ポリシーが具体的な形にならず、結果的に情報セキュリティが守られない～セキュリティポリシーに対し消極的態度で、意見が出ない。	・「情報漏洩時のリスク」を「成り行き分析」で定量化し、経営者／関係者の危機感を誘う ・セキュリティ教育の徹底～セキュリティ事例等の広報活動の充実。	インセンティブを導入して、意見に対し対価を支払う企業の例はあるが、効果は未知数
91	その他		・セキュリティに関して投資対効果が評価できる基準や情報がない～利用部門の思い込みが激しく、コストと効果のバランスが取れていない ・システムセキュリティ対策費用をどこまで掛けるべきか？そのよりどころとなる基準は？	・「情報漏洩時のリスク」を「成り行き分析」で定量化し、経営者の危機感を誘う ・「投資対効果」の分析方法を伝える／「情報セキュリティのチェーン」をリスク分析として行い、無駄な投資が起きないように誘導する ・セキュリティレベルの強化を行う際に、「コストバランス」を重視したリスク分析を行い、無理なレベル強化がされないようにする ・【経営向け】リスク分析により明確化したリスクに対し、対処費用を算出する。 ・継続的な啓蒙活動、eラーニング等による学習／管理のしやすい仕組みの提供	

おわりに

企業における情報セキュリティに関わるものは、負託された責任の大きさ重さを感ずる一方、企業の情報セキュリティに関する文化・体質の変革者として孤独を感ずるときがあります。

この孤独を感ずるのは、

・抵抗感

情報セキュリティへの取り組みが経営管理面でのトップダウンの要請としても、セキュリティを守る側の従業員にとっては何も便利になるわけではなく、逆に不便になることに対して抵抗がある。

・疎外感

今まで情報システムの導入により、利用者に利便性を供与し感謝されてきた情報システム構築部門の人間にとって、管理統制というまったく異なった作業が強いられ、社内に相談相手もいない。

・不安感

情報セキュリティに携わるものは、セキュリティレベルの向上というプラス面の一方で、情報セキュリティ対策に要するコストおよび対策運用による従業員の業務能率の阻害といったマイナス面への責務も負う。このため、情報セキュリティ担当者は、企業における情報化の段階を理解したうえで、セキュリティリスクの度合いを測り、バランスの取れた対策を講じていく必要がある。これでいいのかという自問が常にある。すなわち、これで合格という共通の尺度、目標がない。

などなど、悩みの理由は深い。

今年の部会活動への応募者は、当初 50 名にもなり例年に倍する応募をいただきました。これは、情報セキュリティに関わる社会的関心の高さはもちろんですが、当部会の昨年度報告「JUAS が作るセキュリティポリシー（国際規格に準拠したセキュリティ管理汎用規定集)」への会員企業からの反響の大きさを感ずるとともに、部会活動へのさらなる期待を感ずるものでありました。

同時に、先に述べた孤独感を分かち合う人々が集いお互いに経験と知恵を出し合い、また事例の研究を通じ、「企業における情報セキュリティの一層の定着」に取り組みたいという意欲を感ずるものでありました。

部会活動は、情報セキュリティに関わる「他社事情の相互聴取」、「定着に向けての問題・課題整理」、途中２人の講師を招き、情報セキュリティ定着に関する TIPS をいただきながら「問題解決の提案」と作業を進め、全 10 回部会を開催しました。

情報セキュリティ担当者の悩みは深いが、大きな経営課題であることも確かです。この経営課題に応える担当者は、企業において初めての経験であることから、日夜相談する相手もなく苦労されていると思います。今回まとめた「セキュリティポリシー定着化に向けて～課題と解決のヒント集」は、そうしたセキュリティ担当者の毎日の活動を心から支援するものであり、必ずしも網羅的な資料ではありませんが、セキュリティの定着に行き悩んだ際には、一度は開いていただき、問題解決の糸口を感じ取っていただければ幸いです。

また参加メンバーにとっては、この１年間、同じように現場で抱える課題や悩みを出し合い真剣に議論しあうことにより、今後の日常業務の中で発生する様々な問題や悩みについて気軽に相談できるネットワークが構築できたことは、「報告書」以外のもう一つの大きな収穫であったと考えます。

最後に、本研究会の活動をまとめるにあたって、研究部会での講演を快く引き受けていただいた浅井講師（長岡技術科学大学教授）、向山講師（社会経済生産性本部）に感謝の意を表します。浅井講師からは、大手企業において情報セキュリティの定着に尽力された実践を踏まえた視点から、また向山講師からは、情報セキュリティの展開について多くの企業の事例を見てこられた視点から、それぞれの経験に裏打ちされた大変貴重な示唆をいただきました。

また、この研究部会事務局として大所帯の部会活動をお世話いただいた石川継雄氏、小川あつし氏にあらためて感謝の意を表します。

セキュリティ研究部会副部会長　大友俊夫／宮木宏尚