中小企業の情報セキュリティ対策支援
ＷＧ活動報告書

平成２０年１２月

ＮＰＯ日本ネットワークセキュリティ協会
西日本支部情報セキュリティチェックシートＷＧ

目　　次

□資料編

図表番号

【参加メンバー】

情報セキュリティチェックシートＷＧは 2006 年 12 月より活動を開始し、2006 年度で 3 回、2007 年度では 13 回、2008 年度では 10 回。総合しますと 26 回の会議開催を行っております。

井上　陽一	ＪＮＳＡ顧問・西日本支部長	
嶋倉　文裕	富士通関西中部ネットテック（株）	（ＷＧリーダ）
久保　　寧	富士通関西中部ネットテック（株）	
元持　哲郎	アイネット・システムズ（株）	
鮫島　　功	（株）ブロードバンドセキュリティ	
奥村　雅則	（株）ブロードバンドセキュリティ	
斎藤　聖悟	（株）インターネットイニシアティブ	
宇佐川道信	パナソニック電工（株）	
市川　順之	伊藤忠テクノソリューションズ（株）	
西村　　祥	伊藤忠テクノソリューションズ	
辰巳　元昭	凸版印刷（株）	
浅野　二郎		
臼井　義美	ＮＰＯ情報セキュリティ研究所	
宮下　勝彦	ヒューベルサービス（株）	
近畿経済産業局　資源エネルギー環境部		
近畿経済産業局　地域経済部　情報政策課		

１．　はじめに

NPO 日本ネットワークセキュリティ協会（以下、JNSA*1と略す）では活動内容により部会・支部・事業者連絡会と言った活動組織があります。

JNSA 西日本支部（以下、支部と略す）はその活動組織の一つであり、地域の最前線基地として、関西に拠点を置く会員企業が西日本におけるネットワーク社会のセキュリティレベルの維持・向上　並びに　日々高まる情報セキュリティへのニーズに応えるべく、先進性を追求すると共に、質の高いサービスを提供する事を目的として活動しています。

支部では参加企業・団体の有志によってワーキンググループ（以下 WG と略す）活動を行っており、「情報セキュリティチェックシート WG」（以下、本 WG と略す）では、中堅・中小企業の経営者（経営層）の方々が気づきを超えた企業価値向上の視点で、自社のセキュリティ対策の現状を認識し、対応して戴く上でのガイダンスとなる情報セキュリティチェックシートの作成を目的に活動を行っています。

１．１　個人情報保護対策チェックシート WG の発足と成果

個人情報保護法の全面施行に際し、実施四領域（政府機関・地方公共団体、重要インフラ、企業、個人）への対策ガイドラインが政府から明示されました。

しかし、本 WG では、利益・企業価値の最大化を目的とする大手企業とは異なり、量的・質的人材の不足、経済的制約度の高さに加えて、人的信頼関係を基盤としたファミリー色の高い企業継続第一の中小企業に、一律・横断的な対策・措置を明示する事に無理がある。

ましてや、大企業の対策をベストプラクティスとするガイドラインは、中小企業にとっては押し付け以外の何物でもなく、戸惑い・疲弊感を伴うであろうと危惧感を持っていました。

そこで、優秀な技術を持ち、産業の要となっている中小・零細企業が多く存在する関西、とりわけ、昔から「ものづくり」拠点としての存在を全国に示している関西から、中小企業の情報セキュリティ対策は如何にあるべきか！の声を中央省庁に届け、形あるものに仕立てたいとして組織化したのが、本 WG の前身である中小企業向け個人情報保護対策 WG でした。

２年半をかけ、WG メンバーがアンケート活動やヒアリング活動を行いながら、中小企業の実態を吸収できるシートとして精度の向上に努めた中小企業向け個人情報保護対策 WG の成果は「個人情報保護対策チェックシート」として完成し、Ｗｅｂで公開するとともに、平成１８年１０月２６日の第１０回 JNSA 西日本支部主催セキュリティセミナー（ＮＳＦ２００６　Ｉｎ　Ｏｓａｋａ）の来場者に実際に体験を戴きました。

その結果は平成１８年１２月１１日に「個人情報保護対策チェックシート集計結果*2」として、JNSA のホームページに掲載されています。

１．２　情報セキュリティチェックシート WG への進化

しかし、対策し、PDCA サイクルを回す実践フエーズに入った情報セキュリティではありますが、その現状は、情報セキュリティ対策を戦略的に捉えようとする企業は少なく、一部では、危惧された負担感が現れ、対策が形骸化する恐れが現実のも

のとなっていました。
個人情報保護対策における成果を纏め上げた２００６年が終わろうとする頃、米国ではコーポレートガバナンスと内部統制システムを抜本的に改革する企業改革法（SOX 法）の導入により、情報セキュリティを核とした IT ガバナンスに見直しが進められ、我が国においても、米国の企業との取引のある企業を主体に、セキュリティ対策の見直しが急ピッチで始まっていました。(US-SOX は予定より１年遅れて２００６年度に実施となりました。)
財務報告に係る内部統制の評価及び監査基準が確定し、企業が何を行うべきかが明らかになって来るにつれ、IT に係る全般統制・業務処理統制への過度な対応がさらなる混乱に繋がるのではないかとの不安が必然的にメンバーから湧き起こり、取引先からの確認方法としてまた、取引先に対する対策説明としても有効な方法として評価が高まっている*3情報セキュリティ全般を対象としたチェックシートに進化させる事となりました。

２．　情報セキュリティチェックシートの概要

２．１　背景

近年、企業の活動における ICT 利活用の裾野は急速に拡大しており、まず用途という側面においては、経理や販売管理といった会社のいわゆる基幹業務の効率化などの分野から、電子メールやグループウェアなどに代表されるコミュニケーションを中心とした情報系といわれる社員の生産性を向上させる用途への拡大が顕著となっています。また利用者層といった側面では、大企業・中堅企業*4から、中小企業・SOHO そして個人へと、ICT 利活用を行う利用層が急速にかつ大幅に拡大しています。

インターネットと安価なブロードバンド接続の普及がこれら ICT 利活用の用途と利用層を急速かつ大幅に拡大した一つの主要な要因ですが、あまりに急速に普及したことや、また安易に利便性を最優先にしてきたことによって、利用者である企業や個人に認識されずに見過ごされてきた大きな問題点があります。それが情報セキュリティ問題です。

インターネットに接続されたコンピュータを持つ企業・個人は、コンピュータ・ウィルス、スパイウェアやマルウェアなど外部から侵入を試みる悪意のある様々な攻撃を受ける危険性に曝されると共に、ここ数年では日常的に定着した Amazon や楽天に代表されるインターネット環境での商行為に対するクレジット・カードを盗みだすフィッシング詐欺などの犯罪が多発＊５しています。また企業内に目を移せば、全社員へ PC が普及することで、PC の私的利用や不正利用の可能性が拡大し、加えて企業内の情報がデジタル化されたことによって、容易にかつ大量に機密文書が外部に漏れる可能性が明らかになっています。

一方、ICT を利用する環境は日々進化しており、業務ソフトウェアの分野を例にとれば、「パッケージ・ソフトウェアを購入して、自社内のコンピュータに設置して利用するこれまでの利活用形態から、インターネットを通してブラウザさえ動けば、必要なソフトウェアをサービスとして利用し、それに応じて料金を支払う SaaS（Sofrware as a Service）といった「所有」から「利用」への動きが活発化し始めており、中小・零細企業にとっては、多大なコストや導入に準備をかけずとも、容

易に最新のソフトウェア機能を必要に応じて安価に利用できる環境が整いつつあります。

２．２　課題

大手企業はセキュリティを ICT を支える重要な基盤として認識し、その対策に積極的に取り組んでおり、さらにその取引先に対しても自社と同様の情報セキュリティレベルを求め始めています。一定レベル以上の情報セキュリティレベルを有している企業群同士によるビジネス・ネットワークが次第に形成され、情報セキュリティレベルの低い企業はそのビジネス・ネットワークに参加できずにビジネス機会を失っていく方向にあり、まさに情報セキュリティ・デバイドともいえる状況が出現しつつあります。

ICT の利用・活用が遅れている情報セキュリティレベルの低い企業が大企業とのサプライチェーンから外されていく傾向は、優秀な技術を持ち、産業の要となっている中小・零細企業が数多く存在する関西一円、とりわけ、昔から「ものづくり」拠点としての存在を全国に示している一方で、電気業界など世界的な大企業の重要な生産拠点として拡大が見込まれている関西にも顕著に現れてきています。

２．３　情報セキュリティチェックシート開発の目的

情報セキュリティチェックシートは、上述したような背景・課題の中で逡巡している経営者に、現状を踏まえた上で、情報セキュリティ対策にどこから？　どのように取り組むか？　どこまでやらなければいけないか？などを理解し、意思決定する際の指針を提供することを目的としました。

２．４　情報セキュリティチェックシート開発において留意した点

機密性・完全性偏重型から可用性を意識したものに改め、情報を活用する事により企業の活性化・未来の展望が開けると言う視点での安全・安心な仕組みづくりにベースを置いた情報セキュリティ全般を対象としたチェックシートとするため、作成に当たっては次の留意点を元に、開発を進めました。

（１）「関西における情報セキュリティ対策の現状」については、政府、公共機関等の保有する統計・実態調査結果のうち、状況把握に有益な既存のデータの活用を原則とし、IT 成熟度（IT 導入度・浸透度？）を基本情報に、紐付作成する。

（２）西日本支部らしい！関西にマッチしたワークとするため、次の理由から気付きを感じる事で情報セキュリティ対策の実践が期待できる活気ある中小企業の製造業を対象としたワークを展開する。

- 大阪が独自技術を数多く保有する製造事業の集積地である事。
- 製造業は情報資産を網羅出来ると共に、重要情報が比較的絞り易い事。
- 製造業はＪＫ活動、安全活動等を通して、リスク管理を実践している事。
- 製造事業の業態で取り扱う製品・サービスは多岐に分かれており（金型から靴等にまで)、解析結果を業態別に展開する事が可能であること。

（3）対象とする中小企業の規模は中小企業基本法に定義*6される300人未満としつつ、20人未満企業については、次の理由から除く事とする。
『平成１６年度事業所・企業統計調査』（総務省資料）*7によれば、２０人未満が８７％を占めているが、IT活用の四つのステージ*8の第一ステージに近いのが実態と考えられる事から、別途、気づきを目的とした２０人未満の企業でも行える！行わなければならない対策（ex；管理者権限の使い分け、パスワードの設定からログの取得等まで、セキュリティ対策上での基礎的な部分）を簡易版セキュリティチェックシート*9により補完する。

（4）本チェックシートにおける管理策とJISQ２７００１付属書A、システム管理基準については個別にすべての紐付けを行う事を原則とする。尚、JISQ２７００１付属書Aの管理策がチェクシートの複数の管理策に不可分に共通する場合は、重複して紐付ける。

（5）本WGでは可用性を意識したものとするため、SLA視点の対象となるサービスマネジメント領域に属するインシデント管理、問題管理、構成管理、変更管理、リリース管理についてはITLLのガイダンスを参照しつつ、個人情報保護法対策チェックシートで得られた表現・編集方法を組み込んだものとする。』
尚、内部統制への対応をも可能とするが、BCP、BCMは中小企業向けには重過ぎるため、システムに対する災害対策視点に留める事とする。

（6）技術的対策については、複数のセキュリティレイヤを配置する事により、一つのレイヤが侵害されても、残りのレイヤでリソースの保護に必要なセキュリティを確保する縦深防御（マルチレイヤーセキュリティ）のコンセプトを用いる。

（7）マニュアル不在でもチェックシートの活用により対策出来るユーザに理解しやすいチェックシートにするため、設問の求めている背景・主旨を順序立てて具体的に記述する事として、次の記載項目を設けると共に、利用者の負担感を考慮して設問数は４０問程度（その内の60%は技術的対策）に絞り込む。

①管理策を対策内容別にキー情報として記述する。
②対策を”どこまで”行うかについて気づきが得られる様に、想定されるトラブルが機密性・完全性・可用性のいずれに影響するのかを把握出来る様にする。
③何を防御するのか？を明確にするため、システムと言う曖昧な表現は避ける事とし、クライアント防御、ネットワーク防御、サーバ防御、アプリケーション防御、データ防御と具体的に記述する。
④現実に想定されるトラブル事象（例；情報漏えい、不正アクセス、改ざん、なりすまし）を記述し、対策しない場合のリスクを明示する。
⑤チェックシートの作成検討過程では、管理策の脆弱性（トラブル原因）並びに脆弱性への対策についても記述を行い、質問・回答選択肢との紐付けを行う。
なお、本WGで扱う脆弱性には一般的な脆弱性の要素以外に、資産が受ける影

響の度合いや脅威の大きさなどの要素も含める。

（８）その他の留意事項

①管理策　並びに　設問の配列については組織対策・技術対策・物理対策・セキュリティ監査の境界を意識する事無く、共通するキー情報ベースに編集する。
②開発については競争優位性を打ち出す為のみに留め、その他はアプリケーションを活用した効率化が望ましいとする投資の差別化を推奨する事とする。
③暗号、かぎ管理については、対策手法の範疇に入る事から、質問の中で、具体的対策を問う形で記述する事とする。
④無線 LAN については、現状の広がりを考慮し、設問の対象に含める。
⑤Authentication、Authorization、Accountability による分類については、チェックシートをシンプルなものとするため、本 WG では使用しない事とする。

３．　アンケート調査

３．１アンケート調査概要

（１）調査方針

情報セキュリティの確保は、ネットワーク利用者が現在持っているセキュリティ意識、講じられている対策等の現状を的確に把握する事にあるとのコンセプトで、情報セキュリティチェックシートに基づき、関西２府５県（三重県を含む）の未上場会社４３６社を対象にアンケート調査を行った。

（２）調査対象者

これまでの調査活動において、対策意識の向上や実施が進まない理由の最たるものとして次のものが考えられる事から、設問対象者を経営者層と実務層とし、各対策措置においては、インフラ的整備と言う側面と、マネジメント（活用・運用）の側面がある事から、経営層と実務管理者への質問は、経営層・実務管理層ごとに独立する部分と両者に共通に回答戴く部分に分類することとした。

・情報セキュリティ対策に関する経営層の理解が不足。
・組織内における経営層と現場実施部門との意思疎通の不足。
・対策しないことが自らのリスクになる事が認識されていない。

（３）アンケート調査に於いて留意した点

①企業へのアンケートに対する回答要請は実務管理者へのアンケート協力をトップダウンで適切に指示願う事を期待して、経営者とする。
②アンケートの回答者の理解度を高めるために、法律的用語の使用は避け、平易な表現とする。(Ex；識別、洗い出し、アクセス等)
また、可用性を意識して戴くために、フアシリティやリソースを使用禁止すると言う表現は原則使わない事とする。

③回答者の主観的判断により現実とかい離してしまう様な質問、推測を必要とする質問、複数の回答が考えられるような質問等については、極力“よりシンプルに！”を求める。

④管理策　並びに　設問が回答者にとって該当しない場合に、曖昧な回答となる事を避けるため、「該当しない」欄を設け、欄枠内に○印をつけて戴くと共に、該当しない理由については、アンケートの質問票に記載戴く事とする。

（例；無線ＬＡＮ、オンライン取引、インターネット販売、ホームページ）

なお、情報セキュリティ対策上、必須のものについては、該当欄には必須として斜線を引き、選択不可とする。

⑤回答選択肢については実践度・成熟度を確認するため、四段階の質問とする。

ア．対策が全く行われていない。

イ．対策は行われているが、部分的対策（共有）、または偏重。
文書化や周知の徹底が不十分。

ウ．対策が行われている。しかし、定期的な見直しがされていない。

エ．対策を実践すると共に、定期的な見直し実施。PDCA が回っている状態

３．２アンケート調査方法

回答者のアンケート内容への反応を把握し、調査目的に沿った回答が得られるかを確認するために、プレアンケート並びにプレヒアリングを先行実施し、得られた成果を情報セキュリティチェックシートに反映させ、精度を高めたうえで、本実施する事とした。

（１）プレアンケートの実施

近畿経済産業局情報政策課の支援により、平成１６年度～１９年度の近畿圏における IT 化促進補助金交付企業の内の製造業１５社を対象に郵送によりアンケートを送付し、郵送にて回集した。

ア．送付日　　；平成１９年９月１８日

イ．回収期間　　；平成１９年９月１８日～平成１９年１０月１７日

なお、チェックシートは平成１９年１０月２９日の経済産業省主催セミナーで紹介され、更に３社のアンケート協力を得ている。

（２）プレヒアリングの実施

アンケートに於いて、ヒアリングを承諾戴いた企業３社を訪問し、アンケート調査では得られない具体例について、資料を補完する目的で１１月に実施した。

（３）アンケートの実施

東洋経済新報社の集録した未上場企業及び中小企業庁作成の“元気なモノづくり中小企業３００社２００７版“から、近畿２府４県に福井県を加えた地域の製造業３３７社を対象に郵送によりアンケートを送付し、郵送にて回収した。

ア．送付日　　；平成２０年１月１５日

イ．回収期間　　；平成２０年１月１５日～平成２０年１月２８日

（4）ヒアリングの実施

アンケート及びアンケート補完に於いてヒアリングを承諾戴いた企業２社を訪問し、アンケート調査では得られない具体例について、資料を補完する目的で平成２０年３月に実施した。

（5）アンケートの補完

事前アンケートを行い慎重な姿勢で臨んだアンケートではあったが、年初の多忙な時期でもあったためか、アンケートの回収数が予想外に少ないため、次の補完を行い、アンケートの協力並びに活用についての呼びかけを行った。

① 往復ハガキによる上記アンケート発出先企業に再度のお願い。
② 近畿経済産業局情報政策課のホームページに掲載。
③ 協力団体としてのNPO日本システムインテグレーションパートナーズアソシエーション(JASIPA)関西支部や関西情報産業活性化センターに紹介。
④ メディアによるSecurity　NEXTでの紹介。
⑤ （株）クオリティ社のユーザ会（セミナー）での紹介

３．３アンケート調査結果

（1）プレアンケート

アンケートへの回収実績は８０％（１２社/１５社）と高く、近畿経済産業局からの要請である事に加えて、IT化促進補助金交付企業としての協力姿勢の高さによるものと考えられる。(回答戴いた１社は、自社の情報機密度からアンケートへの回答を丁重に固辞されてのものであった。)

●情報セキュリティチェックシートの回答選択肢からの選択結果
（経済産業省主催セミナーでアンケート協力戴いた３社を含む）

経営層には組織的・人的対策について、情報システム部門責任者には技術的対策を中心に回答を求め、更に、経営層との意識の差について確認を行うために、情報システム責任者には文書化された手続き、障害対策、災害対策についての回答を求めた。

その結果、文書化された手続き、障害対策、災害対策については「必要に迫られて」情報セキュリティ対策を実施されている経営者層の場合には情報システム部門責任者に比較してより高い評価がされており、逆に、情報セキュリティ対策の「必要を認識出来ない」経営層の場合には、情報システム部門責任者に比較してより低い評価が行われているとの結果を得た。これは、経営層と情報システム部門責任者の価値観の共有並びに情報の共有が浸透していない事によるものと思われる。

表３－１　情報セキュリティチェックシート　プレアンケート結果

回答企業【業種】　　従業員規模	経営者層				情報シス管理者			
回答選択レベル	1	2	3	4	1	2	3	4
A 金属【金属】　50~100	15				16	6		2
B 印刷【印刷】　50~100	5	1	6	3	2	8	2	11
C 電工【金属】　100~200	9	6			8	13	1	2
D 製紙【紙】　50~100	6	6	3		11	7	5	
E 製作【電気機械】　20~50	2	4	5	4	7	8	5	2
F 精工【同上】　100~200		1	7	7	1	1	10	11
G 作業服製造【繊維工業】　100~200	5	7	2	1	2	12	9	2
H 工業【電子部品】　100~200	8	6	1		6	14	2	1
I 婦人服製造【衣料その他】　20~50	12	3			5	16	3	1
J 器具【輸送用機械器具】　300 人以上					4	15	3	3
K 手袋【繊維工業】　50~100	8	7			10	11	2	
L 繊維【繊維工業】　100~200	5	8	1	1	4	10	4	5
M リース【化学】　20~50		3	8	4		7	11	6
N 機械【情報通信機械器具】100~200-		5	10			11	9	2

＊質問数は経営者層１５、情報システム管理者２５ですが、回答企業にとって、質問が該当しない場合がありますので、回答数と質問数が整合しない場合があります。

表３－２　情報セキュリティチェックシートプレアンケート結果総括

回答企業 / キーワード	回答企業別選択肢レベル														
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	平均
セキュリティ基本方針	1	4	1	1	1	3	2	1	1		1	1	3	3	1.77
責任の明確化	1	4	1	1	2	3	2	1	2		1	2	3	3	2.00
職務の分離	1	1	2	2	4	4	2	1	1		2	2	2	2	2.00
情報資産管理台帳	1	1	1	1	4	4	1	1	1		1	2	4	2	1.85
文書化された手続き	1	3	2	3	2	4	3	2	2	2	2	2	3	3	2.43
ルール	1	4	1	1	1	3	1	1	1		1	1	4	3	1.77
秘密保持	1	2	2	2	3	4	3	1	2		2	2	4	3	2.38
ゾーン管理	1	3	1	2	2	3	2	2	1		2	1	3	3	2.00
入退管理	1	3	1	1	2	2	1	2	1		2	1	3	3	1.77
サービスレベルの確保	1	1	2	2	3	3	2	2	1		1	2	2	3	1.92
ソフトウエアの選別と開発	1	1	1	3	3	3	2	1	1		1	3	2	2	1.85
業務データの管理	1	3	2	2	4	4	1	2	1		2	2	3	?	2.25
障害報告	1	3	2	3	4	4	4	3	3	4	2	4	4	3	3.14
災害対策	1	1	1	2	3	4	2	2	2	1	1	1	3	2	1.86
監査	1	3	1	1	3	3	1	1	1		1	2	3	3	1.85
ＩＤ	1	4	4	1	1	4	4	2	22	2	3	2	4	4	2.71
パスワード	1	4	2	1	1	4	2	2	2	2	2	2	3	3	2.21
アクセス権限	1	4	2	1	1	4	3	2	1	2	1	2	3	3	2.14
ネットワークアクセス制御	1	2	2	1	2	4	3	2	2	2	2	4	2	3	2.29
ネットワークアクセス制御	2	3		1		3	2	2	2	2	1		2		2.00
ネットワークアクセス制御	1	1	1	1	1	3	2	1	2	2	1	1	3	3	1.64
ネットワークアクセス制御	2	2	1	1	1	3	2	1	2	2	1	2	2	2	1.71
ウイルス	4	2	1	1	2	3	2	2	2	3	2	2	3	3	2.29
ウイルス	4	4	3	3	3	3	1	2	2	4	3	4	3	4	3.07
PC・電子媒体・紙の管理	2	4	1	2	2	3	3	2	1	1	1	2	4	2	2.14
電子メール	2	4	2	2	2	3	2	2	2	2	2	2	3	2	2.29
電子メール	1	4	1	1	1	2	1	1	1	1	1	1	2	2	1.43
オンライン取引			2				3		3	2			2		2.40
インターネット販売	1		2				3		3	2		2			2.17
ホームページ	1	2	1	2	3	3	2	1	1	2	2	3	3	3	2.07
監査ログ	1	4	2	1	1	1	2	1	1	1	1	2	2	2	1.57
障害ログ	1	4	4	1	2	4	3	1	4	4	1	4	2	2	2.64
バックアップ	2	4	2	3	3	4	3	4	2	2	2	3	3	3	2.86
性能管理	2	2	2	3	4	4	3	3	2	3	1	3	3	2	2.64
リリース管理	1	2	2	2	4	4	2	2	2	2	2	4	4	2	2.50
変更管理	1	2	1	2	2	4	2	2	2	2	2	2	4	2	2.14
構成管理	1	4	2	2	2	4	2	2	2	3	2	3	4	2	2.50

図３－１　回答企業のキーワードごとの選択肢平均レベル分布図

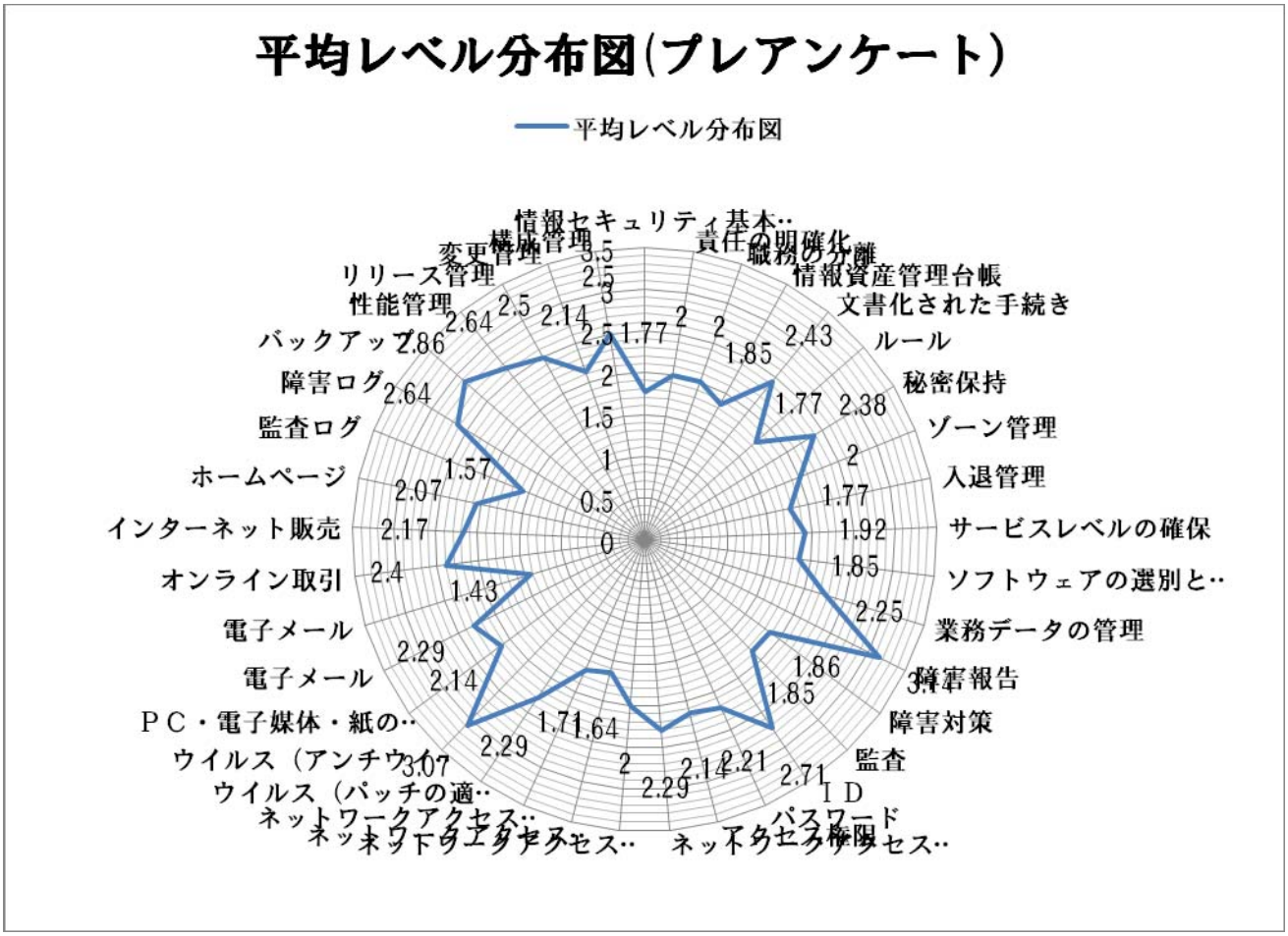


表３－１は実践度・成熟度を確認するための回答選択レベル（四段階）の選択結果を回答企業別にそれぞれ表したものである。表３－２はキーワード別にそれぞれ回答企業の選択レベルを、図１－１は回答企業の平均選択レベルを表したものである。

表３－１からは、規模による差異はあまり見られない。

この事から、「必要に迫られている企業」と「情報セキュリティ対策の必要を感じない企業」間に大きな格差があると考えられ、中小企業にとって、“情報セキュリティ対策の投資効果が見えない“への対応が喫緊の課題であると言える。

また、業種別に見てみると電気機械、機械器具では対策の実施度が進んでいる。

表３－２及び図３－１を見ると、対策が進んでいるのが障害報告とアンチウイルスソフトによるウイルス対策であり、それぞれ選択レベル平均点は３レベル（対策が行われている。しかし、定期的な見直しがされていない。）を超えており、対策を実践すると共に、定期的な見直しも実施し、PDCA が回っている状態の４レベルの企業が４０％を占めている。利用者固有の ID 割り当てによる対策がこれに続いている。

また、障害ログ、バックアップ、変更管理を除く性能管理、構成管理の実施度がそれぞれ高い事から、業務の安定性・効率性に関連する対策が優先事項とされている事が判り、特徴的である。

逆に、セキュリティ基本方針、ルール、入退管理、電子メール（添付フアイル)、監査ログの所謂マネジメント対策が遅れているが､これは人的信頼関係を基盤としたフアミリー色の高い中小企業の一側面を表しているものと言える。

電子メール（添付フアイル）については回答１４社中１０社が１レベル、ルールは同様に１３社中９社、セキュリティ基本方針、情報資産管理台帳の作成、監査ログが同様に８社、監査が同様に７社となっており、対策が全く行われていない企業が多く二極化現象の傾向を如実に物語っていると言えよう。

経営方針の中に情報セキュリティ基本方針を記載･周知徹底している企業にあっては対策がバランスよく行われていることから､経営 TOP 自らの主導性発揮が望まれる。

一方、インフラ的側面としての技術的対策については、上述した電子メール（添付フアイル）及び監査ログを除いて総じて２以上レベルにあり、対策が行われている。

しかし､ネットワークアクセス制御においては外部からのアクセスに対しては２社を除いてその対策は行われているが､社内における重要情報へのアクセスについては､回答企業１４社中、８社が１レベル、サーバへのアクセス制限は同様に１４社中５社と低く､マネジメント対策同様に､人的信頼関係を基盤としたフアミリー色の高い事業継続第一の中小企業の一側面が表れている。

（２）プレヒアリング

ヒアリング調査結果

ヒアリングはＩＳＭＳ等の監査の様に、対策の事実を確認するための経営方針、規定等の文書、情報資産管理台帳等の提示を求めてのものでなかったために、回答に抽象的な説明が多く､回答企業の実態はアンケートの回答結果よりレベルは落ちると推測される。また、プレアンケートの対象が IT 化促進補助金を交付された IT 整備の途上企業である事から、脅威・脆弱性に対する理解が乏しく、このため、情報資産を重要度に応じて整理する域に達していない。

以下にヒアリングで感じた共通点を列記する。

①中小企業の現状は残念ながら自社内で手がいっぱい！
委託先の管理まではとても回らない！

②サービスレベル確保の主体はベンダー等のアウトソース先。
情報システムの運用管理を外部に委託している企業の実態は丸投げにちかいものがあり、サービスレベルの確保については委託先と取り決めをしているとの回答が多いが、ベンダー主導が実態と推測される。このため、アクセス制御やウイルス対策、運用管理については委託先での管理状態を回答されている場合が多く、自社での対策と区別できる工夫が必要と感じた。

③情報資産に占める個人情報のウェイトが高く、情報セキュリティ＝個人情報保護との認識になっており、Ｐマーク取得で情報セキュリティ対策は十分との認識がある。

④自社の生命線である業務用のシステム（FA システム等）に対して基幹系システムに対するリスク認識が低く、品質管理（ＩＳＯ9000)、環境対応（14000)については、積極的に取得しているが、基幹系については事務用管理であるとの認識から切迫感が薄い。また、ＩＳＯ9000, ＩＳＯ14000 取得で、情報セキュリティ基本方針がカバー出来ていると感じている。

⑤文書化の必要は十分認識はしている。昔からの手続き、仕組み、ノウハウの蓄積はあるが、それを”文書化”することが出来ない現実。

⑥大手企業との取引が事業のウェイトの大半を占めている企業にとっては、取引先からの要求事項や確認は”手をこまねいている文書化や性善説信奉により実行し難い責任・権限管理”に良きガイダンスとなるが、中小企業にとっては、いざ実施を求められると”やっかい！で重い！”ものとなり、強要・強制されていると感じるトレードオフの関係。

⑦複数の大手企業と取引を行っている企業では、情報セキュリティ対策の確認事項の共通化を切望されている。

○ヒアリング事例紹介

ア．A 社のヒアリング結果

IT 化には積極的であり、自社の競争力を高めるための改善努力を長年に亘り実践されて来ており、管理手法・手続きは整っているが、すべて、CIO、情報システム課長の頭脳に蓄積されたものであり、両者の阿吽の呼吸によるところが大きい。いずれか一方が何らかの理由で欠ける事があれば機能停止は明らかであり、トラブルに陥った場合には、顧客への説明責任を果たせない危険性が高く、重要な情報資産をその重要性のレベルごとに分類し、レベルに応じた対策措置を行う情報資産管理台帳の整備と共に、情報システムの管理、利用についての正式な文書化が必要であることを指摘した。

イ．B 社のヒアリング結果

取引先に大手企業を持っており、取引先の信用を確保することが一番と意識されており、取引先からの要請・確認＊１０が対策措置の検討にも良きガイダンスとなっている。

但し、本音のところは、大手企業からの詳細な要求事項＊１１にどこまで応えるべきかに悩まれている様子であった。

ウ．C 社のヒアリング結果

経営層と情報システム管理者に共通する質問のすべてで、情報システム管理者の選択レベルが１段階高い回答であった企業。

サーバをハウジング、プロバイダーに全面的に依存されているのが実態であり経営者は自社の能力・体制を記述。一方、情報システム管理者はハウジング先やプロバイダー側の対応を記述されたため、上記の結果となったことが判明。

従業員が１２名と小規模であり、情報システム管理に携わる専任者不在のため業務委託による対策措置が限度の模様。

回答選択肢を業務委託先で対策されている結果なのか？自社で対策の結果なのか？が峻別できるチェックシートとする必要を感じると共に、委託元からの管理についても考察が必要と感じた。

（3）アンケート

プレアンケート並びにプレヒアリングで得た教訓から、プレアンケートで使用した情報セキュリティチェックシートに次の改善を加えた。

①障害報告、災害対策）としていましたが、両者の認識度を比較する領域を広げ、経営層にはこれまで通りとするが、情報システム管理責任者には全問回答戴く事で、マネジメント全般について、両者の認識の整合度を確認する事とした。

②情報セキュリティ対策措置の基盤ともいえる情報資産管理台帳の実用促進への啓発の意味も込め情報資産管理台帳のサンプルを添付した。

③少ない人材を有効に生かす手段として、外部組織に業務、運用管理を委託されるケースが中小企業には多い実態にある事から､｢委託先(アウトソース先)の管理」をキーワード及び質問に加えると共に、サービスレベルの管理についても自社内と委託先（アウトソース先）に区分する事とした。

自社内・委託先のそれぞれでどのようなセキュリティ対応が実施されているのか？の回答を期待して右枠に“質問に該当しない”と同様に、“業務委託の欄”を設けた。

④サービスレベルの確保を組織内部と外部に分離した。

⑤電子フアイルの利用（原則は紙による返信とし、ｅメールでの回答も可）

⑥文言・説明文に次の修正を加えた。

・質問票の最初に、キーワードからトラブル事象例までを参照しての回答を要請する説明文挿入

・文書化された手続きについては、各種マニュアル例示する事とした。

・サービスレベルの確保での例示「専用回線・・・」を情報システム管理責任者に馴染みやすい「サーバ障害」とした。

・中小企業では災害対策は厳しく、回答選択肢の内容も障害を想定しての記述となっている事から災害対策は障害対策に変更した。

・監査は会計監査等との混同を避けるため、情報システム監査とした。

・ネットワークアクセス制御の無線ＬＡＮの質問の回答選択肢に､｢アクセスポイントの管理」の記述を加えた。

・小規模の中小企業では紙依存度が高いことから、PC・電子媒体・紙の管理の質問の回答選択肢に、紙を対象とした記述を加えた。

・オンライン取引､インターネット販売については､ＥＤＩ取引　並びに　自社サイト・楽天ＹＡＨＯＯ等をそれぞれ例示した。

●改善後の情報セキュリティチェックシートの回答選択肢からの選択結果
（アンケートの補完活動で得られた５社を含む）

事前アンケートを行い慎重な姿勢で臨んだアンケートではあったが、年初の多忙な時期でもあったためか？回答数は期待したほど伸びず、アンケートの回収実績は４％弱（１６社/４３７社）と低調な結果に終わった.

回答企業の従業員規模別の内訳は 20 人～50 人規模が５社、50 人～100 人規模が３社、100 人～200 人規模が４社、200 人～300 人規模が１社、300 人以上が２社となっている。また、売上規模別の内訳は 1000 万未満規模が１社、1000 万～5000 万規模が６社, 5000 万～1 億規模が１社、1 億～３億規模が２社、3 億超規模が５社であった。

従業員規模、売上規模、業種による対策の実施度差異はプレアンケートと同様にあまり変化は見られず、定性的な傾向は見られなかった。

しかし、従業員２００人以上の規模の企業では組織的な体制（情報システム責任部門があり、専任者が存在）が取れるとともに、取引先やステークフォルダ等の要請を意識する必要があると想定され、情報セキュリティ対策の実施度は２００人未満の従業員規模企業に比して、一気にその実施度は高くなっている。

マネジメント全般について経営層との認識差を確認するため、情報システム管理責任者には全問回答を求めたが、１社を除いては大きな差異は見られなかった。

図３－２　回答企業のキーワードごとの選択肢平均レベル分布図

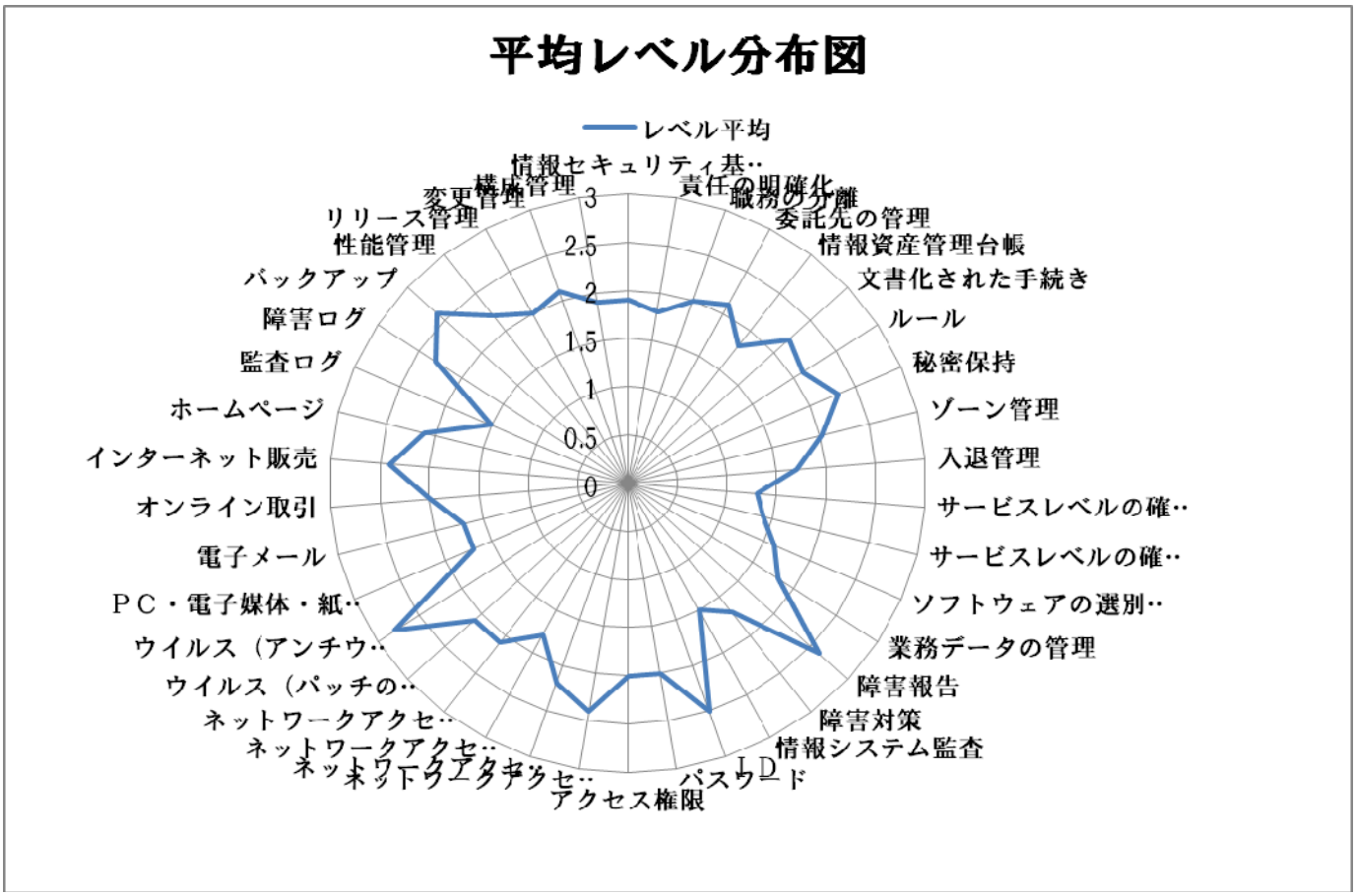


図３－３　　二 極 化 現 象

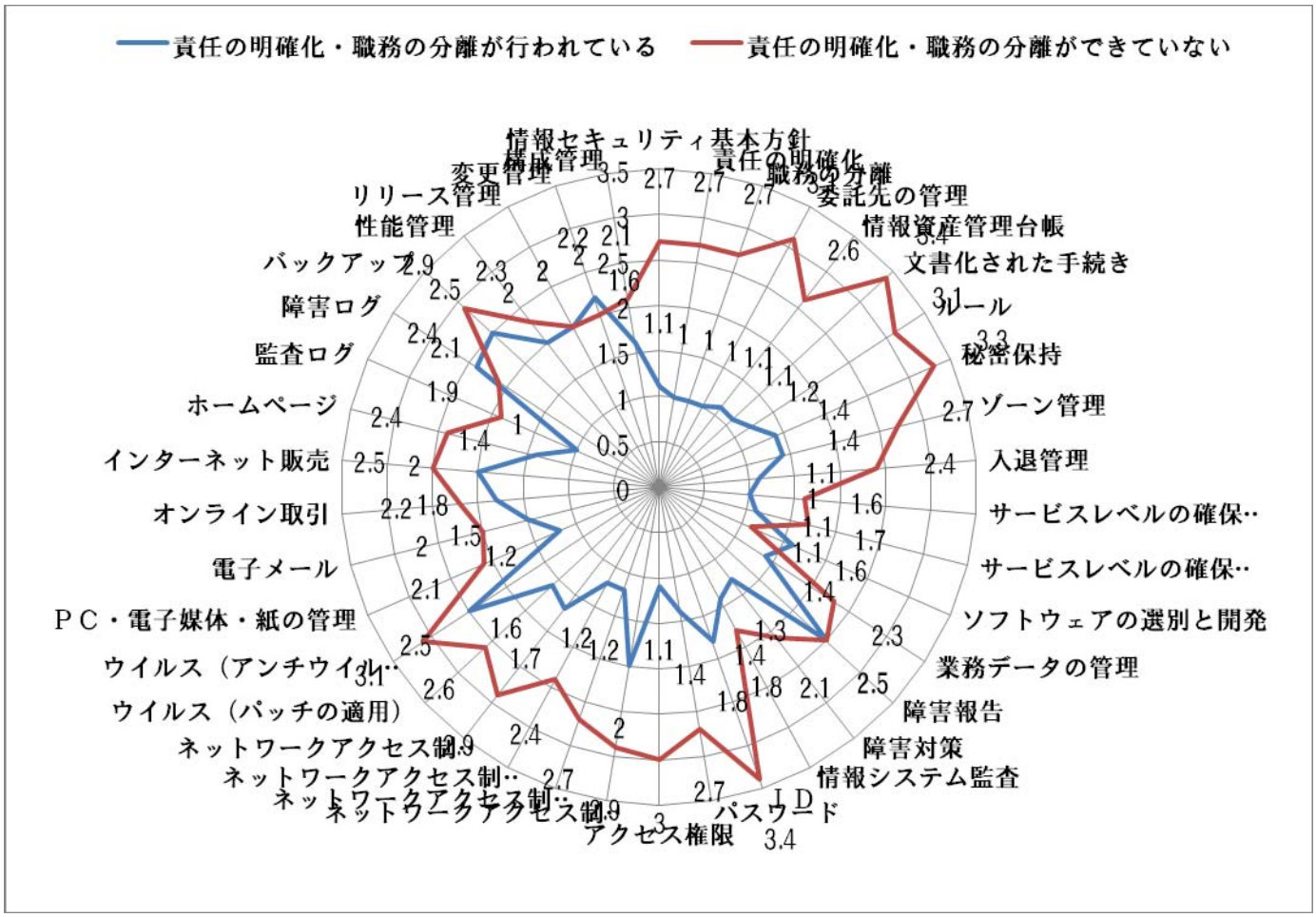


図３－４　従業員規模別対策レベル（組織的対策・技術的対策）

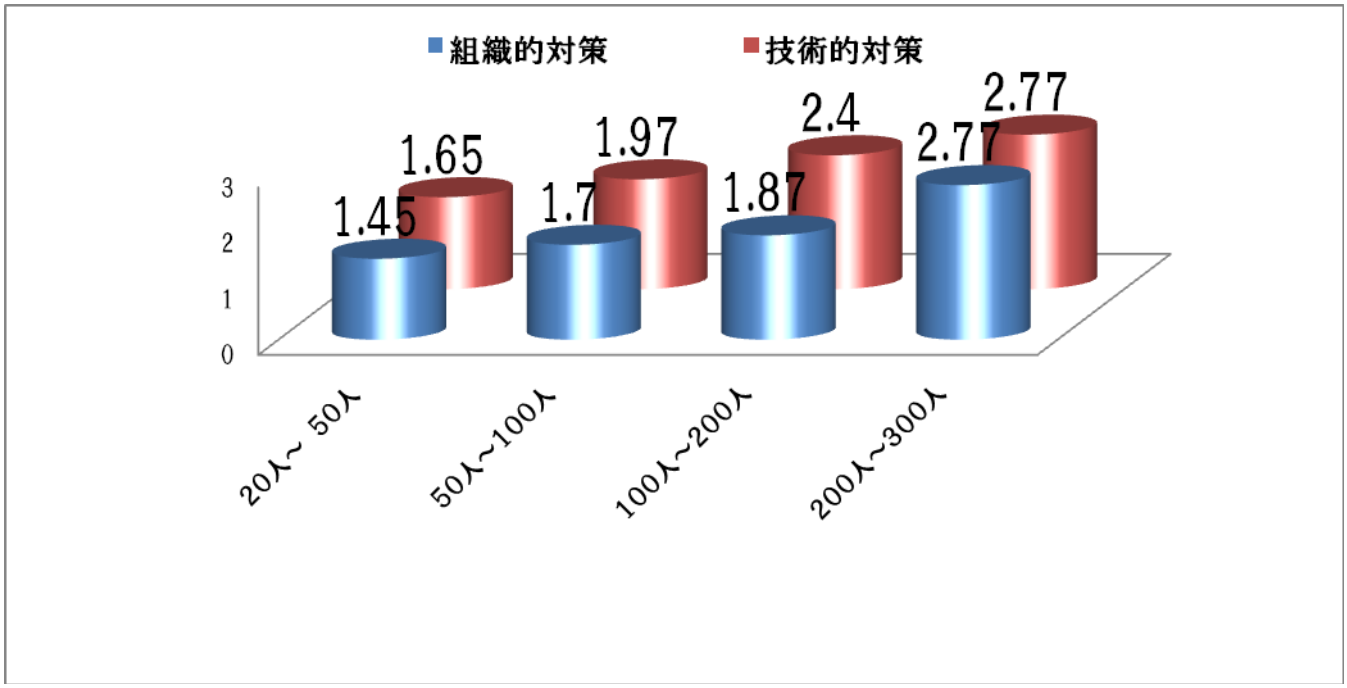


表３－３　情報セキュリティチェックシート　アンケート結果総括

キーワード ＼ 回答企業	回答企業別選択肢レベル														
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
情報セキュリティ基本方針	2	1	1	1	1	1	1	2	1	1	3-2	4	4	4	1
責任の明確化	1	1	1	2	1	2	1	1	1	1	3	4	4	3	1
職務の分離	1	1	1	2	2	1	1	2	1	1	3	4	4	3	1
委託先の管理	1	1	1	4	1	2	無	3	1	1	2-3	4	4	2	1
情報資産管理台帳	1	1	1	1	2	2	1	2	1	1	2-1	4	4	3	1
文書化された手続き	1	1	1	3	2	2	1	3	1	1	2-4	4	4	4	1
ルール	1	1	1	1	3	3	1	3	1	1	3-1	4	4	4	1
秘密保持	1	1	2	2-1	1	3	2	3	1	1	3-4	4	4	3	2
ゾーン管理	1	1	2	1-2	1	2	1	3	1	1	3-2	4	4	1	3
入退管理	1	1	2	1	1	3	1	3	1	1	1	4	4	1	1
サービスレベルの確保（内部）	1	1	1	1	1	2	1	1	1	1	1-2	2	2	1	1
サービスレベルの確保（外部）	1	1	1	1	1	2	無	1	1	1	3	1	3	1	2
ソフトウェアの選別と開発	2	2	2	1	1	2	1	1	1	1	1-4	1	1	1	3
業務データの管理	1	1	1	2	2	2	1	3	1	1	2-4	2	2	1	3
障害報告	2	1-3	2	4-3	3	2	2	2	1	3	3-4	2	2	2	4
障害対策	1	1	1	4-3	1	2	無	2	1	1	2	2	2	1	3
情報システム監査	1	1	1	1	3	1	1	3	1	1	3-4	1	1	1	2
ＩＤ	1	1	1	3	4	3	2	4	1	1	4	3	3	4	3
パスワード	1	1	1	2	3	2	2	①	1	1	3	4	4	3	1
アクセス権限	1	1	1	2	1	2	2	3	1	1	4	4	4	2	1
ネットワークアクセス制御（外部）	1	委2	3	3	2	3	2	2	1	1	2	4	4	2	4
ネットワークアクセス制御（無線）	無	1	?	無	無	2	無	2	2	1	2	4	4	2	無
ネットワークアクセス制御（内部）	1	1	2	1	2	3	1	1	1	1	2	4	4	2	1
ネットワークアクセス制御（サーバ）	1	1	2	2	1	3	2	3	1	1	2	4	4	2	3
ウイルス（パッチの適用）	2	1	?	2	2	3	2	3	1	2	1	2	3	4	1
ウイルス（アンチウイルスソフト）	2	1	3	4	3	3	3	4	2	3	4	1	4	2	3
PC・電子媒体・紙の管理	2	1	2	2	1	3	1	3	1	1	1	1	4	1	1
電子メール	1	2	2	1	1	2	2	3	1	2	1	1	4	2	1
オンライン取引	無	無	2	1	2	3	無	2	1	2	3	無	無	2	無
インターネット販売	無	無	?	1	無	無	無	無	無	2	4	無	2	3	無
ホームページ	委	委	2	2	委4	3	1	委2	1	2	3	1	委	3	1
監査ログ	1	無	?	2	1	2	無	2	1	1	1	1	3	2	1
障害ログ	2	無	?	2	4	2	無	2	1	1	4	1	3	1	4
バックアップ	2	2	2	2	3	2	2	3	2	2	3	3	4	3	4
性能管理	1	無	?	2	3	2	無	2	1	無	2	2	3	3	3
リリース管理	委	無	?	1	2	2	無	2	1	無	3	1	3	2	3
変更管理	2	無	?	2	3	2	無	2	1	無	3	1	2	2	3
構成管理	2	無	?	2	2	2	無	3	1	1	3	1	2	2	2

＊選択肢レベルを複数表示（２－１）しているのは、経営層と情報システム管理責任者の選択肢レベルに差があるため。
（左が経営層、右が情報システム管理責任者）＊委はアウトソース　＊無は回答が無かった。

表３－４　回答者の選択理由（マネジメント系）

キーワード	対策が行われている企業	対策が行われていない企業
情報セキュリティ基本方針	ＣＳＲ、内部統制の必要から制定した。	過去に事故を経験していないため形だけ（情報管理の内部規定程度）のもの。周知徹底が不十分。
責任の明確化	CIO を選任し、経営会議にて報告を徹底	情報システム担当部署以外は不明確 管理者・業務担当者の分離ができていない。
職務の分離	セキュリティ委員会設置し活動	リソース（人員）の関係から分離できていない。
委託先の管理	委託先選定基準があり、基準に沿った相手かどうかの確認のための報告・監査制度あり。	Ｐマーク取得済みの昔からの付き合い先のため安心している。規定は一応ある程度。
情報資産管理台帳	安全対策基準に基づいた障害管理規定やシステムの復旧手順書もある。	ハードウェアの管理台帳はある（固定資産台帳） 情報への関心が低く、情報資産の棚卸は不完全
文書化された手続き	承認された手続きマニュアルあり。 手続きマニュアルはあるが組織内で不統一	手続きマニュアルはあるが組織内で不統一 ビジネスマナーの程度の心得的なものしか無い。
ルール	法令反映、管理者の許可を得て、社内リソース利用 社内規定があり、セキュリティ委員会が見直し	存在するのは情報管理の規定のみ。導入すべき法令を反映したルールの文書化は出来ていない。
秘密保持	内部・外部とも覚書を締結、特に外部については、取引先からの要請もあり、定期的に内容見直し	社外取引の際は機密保持契約を交わしているが、内部は信用している。
ゾーン管理	サーバ等重要情報機器はハウジングまたはアウトソーシング対応。	サーバ室だけは管理している。 建物の構造関係もあり、費用面・運用面から未実施
入退管理	サーバ室は常時施錠。許可されたもののみ許可	お客、メーカーが気軽に出入り出来る社風重視のため消極的。サーバ室だけは管理
サービスレベルの確保（内部）	明確な SLA を策定しているが、システム停止による影響が把握出来ていない。復旧計画あり。	サービスレベルに関しての取り決めがない 生産をコンピュータ化していない。
サービスレベルの確保（外部）	ベンダーより定例会にて報告聴取	同上
ソフトウェアの選別と開発	IT 推進委員会でソフトウェアの選定を決議 開発基準、管理基準はある。パッケージソフトは無い。	都度経営判断
業務データの管理	システム的に入出力データの妥当性のチェック実施 プロセスを整理し、定期的に見直し実施	システム的な入力チェックはあるが形式的なもの
障害報告	毎月報告。緊急連絡体制網作成。	利用者側に影響のない微細な障害は報告せず
障害対策	データセンターは安心。ネットワーク等の足回り心配 大規模災害を想定したリスク管理体制について検討中	障害が発生したらあきらめるしか無いとの考え メーカー・ベンダー頼み。
情報システム監査	社内監査・会計士によるシステム監査を定期的に実施 監査ノウハウを持った人材無し。外部委託は高価	社内ニーズなし。 監査出来る人がいない。外部委託は金食い虫。
ＩＤ	派遣社員・パート社員にも個々に固有ＩＤ発行	共有ＩＤ
パスワード	パスワードポリシーに基づき設定すると共に、ワンタイムパスワードを使用。	規定はあるが、社員が遵守していない。 定規的なパスワード変更を促していない。
アクセス権限	クライアント・サーバ、Ｗｅｂサイト、更には、部署別にフオルダ閲覧制限を設けている。 人事異動の都度、人事部と連携しアクセス権限の変更	業務優先からアクセス制限はしていない アクセスログをチェックする時間がない。

図３－２は回答企業の平均選択レベル、図３－３は責任の明確化・職務の分離が行われている企業（情報システム専任担当がいる）と行われていない企業で対策実施度に大きな差異が生じている二極化現象を表したものである。

表３－３は実践度・成熟度を確認するための回答選択レベル（四段階）の選択結果を回答企業別にそれぞれ表したものであり、表３－４は二極化現象が顕著に表れているマネジメント系について、回答者からの「選択理由」をキーワード別に列記した。

図３－２からはプレアンケートと同様に、障害報告、アンチウイルスソフトによるウイルス対策の実施度が高く、バックアップ対策、利用者固有の ID 割り当てによる対策がこれらと同等の実施度となっている。

図３－３からは組織的対策に加えて、アクセス権限・アクセス制御　監査ログと言ったマネジメント系で上述した二極化現象が顕著である。

逆に、障害報告、アンチウイルスソフトによるウイルス対策については、その実施度には差が無い。また、障害ログ、バックアップ、性能管理、変更管理、リリース管理、構成管理の実施度にも大きな差は無いことから、プレアンケートで得られた業務の安定性・効率性に関連する対策が優先事項とされている事が推定できる。

表３－４からは図３－３の二極化現象が、これまで述べてきた「必要に迫られている企業」と「情報セキュリティ対策の必要を感じない企業」それぞれの事情の一端を垣間見る事が出来る。

（4）ヒアリング

ヒアリング調査結果

ヒアリングはプレヒアリングと同様、ＩＳＭＳ等の監査の様に対策の事実を確認するための経営方針、規定等の文書、委託元からの情報セキュリティチェックシート、情報資産管理台帳等の提示を求めてのものでなかったが、これまでの調査で得た知見をもとに、コンサル的指導を含めてのヒアリングであった。

なお、２社のヒアリング企業の企業ポリシーがそれぞれの置かれた環境・背景から対照的な関係にあることから、ヒアリング事例として紹介する。

ア．　A 社のヒアリング結果

・経営者は体育会系・根性論でシステム投資をしており、資産の取得に関しては社業の好不況に比例させ、業績好調・キャッシュが豊富な時は積極的に投資、無いときには投資を控えるといったスタンスで、IT 投資は便益及びリスクに基づいたものではない。
・ISO9000 を取得していたが手続等が煩雑であるため、認証取得をやめたとのこと（予算との関係もあり）認証を取得する事を第一義とし、基準をガイダンスとして自社に適合したものに改良して、PDCA を回していくとの考えが希薄。
・予算は短期計画はなく中期計画として作成（中期計画には投資額は記載されず）
システム開発はベンダーに依存しており、システムベンダーの経営者とトップ

同士で、要件を伝え提案を受けておられるとの事。
・セキュリティ基本方針とは、ホームページに公開している個人情報保護ポリシーのことで、取引先とリクルートを対象としたもの。経営方針には記載なし。FA、生産管理システムについてはセキュリティ視点が無いため対象外。
・個人情報保護は守る対象がハッキリしているために対策が明示し易く、セキュリティは対策する情報資産が見え難いとの意識が強い。PC、サーバ、プリンタ、ルータ等のハードウェアの管理台帳は固定資産台帳と同一認識。
・重要な情報の洗い出しはしておらず、個人・部署の管理に任せている。
開発部門は開発に関する情報を、営業部は取引先の与信情報を共有フォルダで管理しており、情報の持ち出しはしていない。(事件・事故がおこっていないので)　情報共有の場所としては、ポータルサイト、グループウェア、共有フォルダ。ユーザは主にExplorerを使って共有フォルダを使用。
・「事故を経験していない」ため、承認者を分離する事による業務処理への影響を懸念し、システムの利用者とシステム管理者は分離されているが承認者は分離されていない。
・委託先の管理については、昔から委託しているところであり、選定の基準は無いが、Ｐマーク等を取得している。縛りを強くすると、委託先が身動きできなくなるので、縛りはない。(チェックシートは無いとの事)
・秘密保持については取引先については機密保持契約も覚書程度のものしかない。個人情報は別にして、技術情報が漏えいしても、困るのは自社であり問題ない。技術ノウハウについては特許取得で情報漏えいに備える事としている。(委託元は無く、委託先も一部の仕入れ先を除いては、日本国内に限られている事からグローバル視点は必要ない。)
・ルールについては委託元がないため、強要されるようなセキュリティ基準などはない。役所などの基準はあるが、情報セキュリティに関するものはない。
・IDは全員がローカルのAdmin権限でログイン。ポータルサイト等はアクセス制御をしているが、抜け道はあり。
・win98など古いPCがあり（数台)、最新パッチ、ウイルスパターンの適応外。スタンドアローンで使用。←使用に耐える間は使用するつもり)
ウイルスは管理PCで全端末のウイルス感染状況をチェックしている。
・重要書類は施錠した場所に保管。PC廃棄時にHDDを物理的に破壊。
・保管については紙媒体に関する対応のみ実施。紙の活用が主体？

【ヒアリング機会を戴いた事の御礼と併せてA社TOPに文書にてコンサル】

現在FAを構築されている事から、経営トップはビジネスとITは不可分なものと捉えられ、ITサービスのパフォーマンスや機能の充足の必要性については、理解を持たれていると推察しますが、可用性、キャパシティ、継続性とセキュリティを同一視すべきである事に理解が聊か不足されている様に思われます。

「過去に情報事故が発生していない事から対策の必要性を感じておられない」ため、リスク認識が無いと言うのが御面談の際の説明でしたが、その実態はリスク対策（ヘッジ・低減・移転）を講じずに対策を見送られている（保有）のが現状と思われます。僭越ですが、リスクを保有する結果、どれだけの残留リスクが

あるかを”定量的に見える化”し、経営層が組織の定める基準に照らして受容できる範囲である事を承認戴く必要があります。

また、“リスクに影響を与える”、“リスクの影響を受ける人たち”の間で、リスクに関する情報交換や情報共有を行って戴く必要があります。

このため、情報セキュリティ対策の第一歩として、組織における情報資産を洗い出し、グループ分けを行い、情報資産管理台帳に記載することをお勧めします。その上で、分類と機密性・完全性・可用性の格付けにより、リスクの評価手法とリスクの容認レベルを確立して戴ければ、対策の要・不要を自然に感じとって戴き、IT 投資の計画的・継続的な取り組みが期待出来るものと考えます。

イ．B 社のヒアリング結果

・CSR,内部統制の観点から必要性に迫られ今期制定し、社内イントラネット上に掲載した段階。社員ひとりひとりへの徹底はこれから。
　個人情報保護方針並びにＣＳＲ宣言を昨年から実施。
・J-SOX の影響を受けて、内部統制に対する視点が高まり、CIO も選任されるとともに、情報セキュリティに関する経営陣の職務分掌や責任範囲については明確に決定したが、開始したばかり。
・重要情報についてはある程度管理されているが、経営者の情報資産についての解釈が不十分であり、個人情報・営業情報＝情報資産と考えている。重要資産の定義付けは不明確で、メーカー・取引先からの要請により区別している。
・情報資産管理台帳はそれぞれの部門で管理されており、情報システムに関連するものは、情報システム部門が一括して管理している。
・手続きの文書はあるが、組織内で承認（統一した）されたものがない。
　今回、パソコン設置規定、パソコン利用規程を整備した。また、「情報セキュリティ基本方針」に著作権の保護を提唱、「ソフトウェア利用規程」を作成中。
　※業務に必要なソフトウェアは基本的に情報システムにて一括購入、管理。
・秘密保持については内部については、退職者も含め覚書を交わしている。
　外部については、取引先からの要請もあり、定期的に内容見直しがある。
・サーバなど重要情報機器はデータセンターにハウジング。社内サーバルームは施錠管理しているが、お客、メーカーが気軽に出入できる社風を重視する面もあり、ゾーン管理は進まない状態。
・外部委託しているサーバ監視、回線監視等についてのサービスレベルについては外部委託先に全面的に依存（復旧時間等の取り決めはない)。外部委託先からは、月一度報告会議で実績の報告を受けている。システム的なものに対しては、内部統制上の要請からリスク対応措置が取られているが、企業自らが仕様を作成して SLA レベルに落とし込んだ対応が取れているようには見えない。
・ソフトウェアの選定については「IT 推進委員会」で決議している。
・業務データの管理については、システム的に妥当性の CHECK を行っているが、内部統制の要請から、プロセス視点で定期的に見直す事となったとのこと。
・外部監査、内部監査ともに行っており、情報システム監査については、細かすぎるくらいのチェックあり。
・アクセス制限については人事異動に伴う情報を人事部と連携し対処。

アクセスログ、操作ログ、監査ログについては現在導入検討中。

・リリース管理についてはシステム開発担当と運用担当を分離するとともに、「システム開発規程」「運用規程」を策定した。

・変更管理についてはシステムを変更した際、「単体テスト」→「本番テスト」を行ったうえで、システム運用担当がリリース、書面に残している。

・構成管理についてはEUC統制により、財務諸表に影響を及ぼすスプレットシートも管理統制下に入れ、システム開発と同レベルの手続きを行っている。

【B社ヒアリング総評】

内部統制気運が昨年から高まり、経営TOPの情報セキュリティに対する視点が高まったため、情報システム担当部門としては大変やりやすくなっており、ルール・規定整備が急速に進んでいるが、PDCAはこれから。

セキュリティ最後の砦は人であるとの視点から社員への教育を強化する方向から、インターネット安全教室等の継続した教育支援を要請された。

システムの安全性についてはメーカー（F社）依存。半ば丸投げの形に近い？SLAについての自社からの仕様は無く、復旧時間についても無い。（費用的な責任区分の関連からも不透明にしている模様）

＊　なお、職責の関係もあるが、部長・係長間で評価に差が見られた。

（5）アンケートの補完

回答数は少なかったが、プレアンケート及びアンケートにおける回答、さらにはヒアリング５社で得られた情報から、少なくとも、送付先に対する啓発・啓蒙の役割は果たせたのではないかと考える。

しかし、アンケートの発信・回収結果を事務的に取りまとめることなく、本WGの活動趣旨の原点に立って、何故回答が少なかったのか？についての確認調査を行ない次なる活動に移行すべきとの意見がWGメンバーで大勢を占めたことから「往復ハガキによる再度のお願い」を発信する事となった。

また、再発信することで、情報セキュリティに対する関心度やチェックシート改版に役立てる事が出来ると共に、アンケート未回答者から回答を期待できる副次効果を期待してのものでもあった。（５社のアンケートへの回答が寄せられた。）

●往復ハガキによるアンケート

① 往復はがきに記載する内容

年初の多忙な時期にお願いした事の非礼と併せて、再度の回答をお願いし、回答頂けない方については、以下の質問に答えて戴く（該当する理由を選択）事とした。

Ａ．情報セキュリティ対策は必要なし。

Ｂ.情報セキュリティ対策は必要と考えているが、次の理由で回答できない。

Ⓐアンケートの内容がセンシティブな情報であり、回答は控えたい。

Ⓑ同様のアンケートが多く、回答するメリットに疑問を感じている。

Ⓒ自社の対策レベルが低く、回答できる状態に無い。

Ⓓアンケート内容を理解し、回答できる人材がいない

Ⓔ回答選択肢が複雑で選択が困難。質問数も多すぎる。

② 往復ハガキ採用理由

アンケートの再発信は多忙な業務の中での経営 TOP の労を考え、開封の必要が無く、返信も簡単であるため。

③ はがきによるアンケート実施結果

３月中旬発送・３月末締め切りとして実施した結果は、次の通り。

ハガキの発送件数；３２７件（アンケートによる回答済み企業を除く）

ハガキの返送件数；　４８件（回収率；１５％）

■アンケートに協力出来なかった理由。

A. 情報セキュリティ対策は必要なし；　６件

B. 情報セキュリティ対策は必要と考えているが、次の理由で回答できない。

アンケート内容がセンシティブなため回答は控えたい	９件
同様のアンケートが多く、回答するメリットに疑問	１８件
自社の対策レベルが低く、回答できる状態にない	７件
アンケートの内容を理解し、回答できる人材がいない	３件
回答選択肢が複雑、質問数も多すぎる	５件

図3－5
情報セキュリティ対策意識

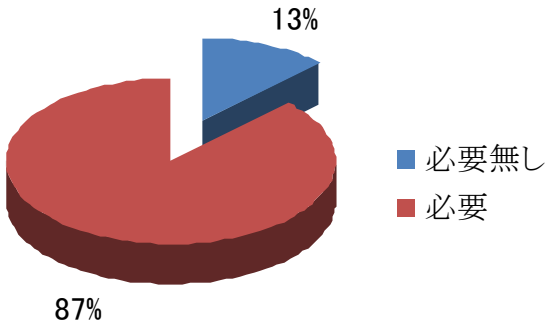


図3－6
アンケートに回答できない理由

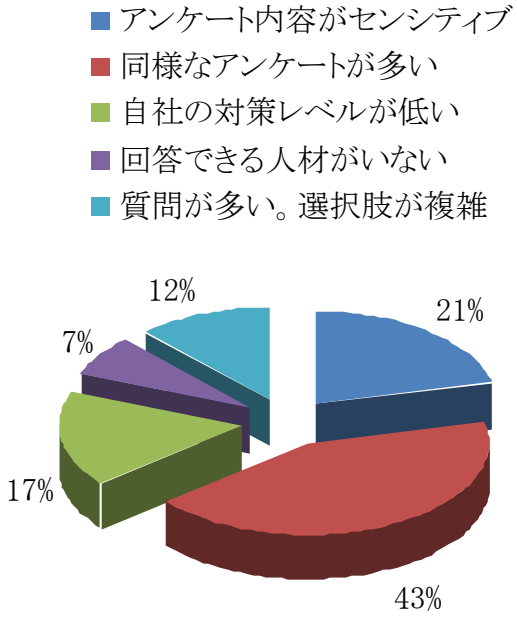


図３－５から、情報セキュリティ対策の必要についての認識度は高く、気づきは進行していると判断できる・しかし、図３－６からは、情報セキュリティ対策上の課題としてのトップ３の内の一つであるセキュリティ対策推進人材の不足が、アンケートに回答できない理由の３６％を占めている。

また、「同様なアンケートが多い」が回答できない理由のトップの４３％となっており、各方面から発信される類似のチェックシートの氾濫傾向が窺え、信頼できるチェックシートの確立が必要になっていると解釈される。

４．BoF の開催

自社の情報セキュリティ対策の実践度を診断する手法として、取引先からの確認方法として、また、取引先に対する対策説明として有効との評価が高まっている情報セキュリティ全般を対象としたチェックシートを開発、気づきも期待し、アンケート及びヒアリング調査を実施したが、中小企業の対応が予想以上に緩慢であることの事実に直面したため、アンケート・ヒアリング結果のまとめの意味で、パネルディスカッション形式での BoF を開催した。また、BoF で提案された「中小企業支援策としてのセキュリティヘルプデスク」について、JNSA 関係者での自由討議を行った。

４．１　BoF の概要

JNSA の年次総会の前に開催される各 WG の成果報告会の１セッションとして、本 WG がアンケート・ヒアリング調査結果で得た見識並びに現在、直面している課題を披露し、来場者も交えた公開討論会の形で、現実的な解についてのアドバイスを求めるコンセプトの下に開催した。

（１）BoF の実施

本 WG リーダをモデリストに、パネリストに経済産業省、IPA、JNSA が登壇し、会場の来場者と公開討論会形式で次のテーマにより実施した。

【テーマ】

①「中小企業における情報セキュリティ対策のトリガーとは」
②「中小企業に共通的に感じられるリスク認識の欠如」
③「中小企業が実際に実践できるアプローチ手法とは」

【パネラーからのコメント】

①「中小企業における情報セキュリティ対策のトリガー」について

・大企業はグローバル化や J-SOX/会社法等コンプライアンスへの要求がセキュリティを施すトリガーになっているが、中小企業にとって情報セキュリティ対策のトリガーは？- 取引先からの要求- 世の中の動向（法律、セキュリティ事故）？
トリガーと感じる企業は良いが、感じない企業はどうすれば良いか？
・外部（大手企業や官庁など）と企業自身が感じているセキュリティ対策への意識のギャップについて議論が出来れば良いのだが、中小企業の場合はなかなかそうはいかない。やはり対策する事の義務化・圧力が必要！
・環境には排出基準があり、品質にも品質基準がある。また、Ｐマークの対象となる個人情報においても保護する対象が明確であり、いずれも外部に与える影響（脅威）が“見える化”“定量的説明”が比較的可能。
・情報セキュリティは明示できる（対策が必要・取引先から強要される）企業と、明示できない企業（対策を必ずしも必要としない・トラブルに見舞われても自社さえ我慢すれば良いとする企業）が混在するため、画一的な定量化が困難。このため、必要とは認識出来ても切迫感に乏しく、いざ実践するとなると、“自分のところは大丈夫だろう”と対策が後回しになる。

・規模の大小に相応するそれぞれのサイズに合った対応が求められるが、対応した企業には“適格マーク”を付与したいもの。

②「中小企業に共通的に感じられるリスク認識の欠如」について

・過去に情報事故が発生していない企業にはリスク観念が希薄。

・情報セキュリティ対策は必要と認識していても、原点とも言える情報資産の洗い出し・分類や情報資産台帳の整理ができていない、抑えきれていないため、情報がどのような形式で格納されているのか？どこにあるのかさえ分からないのが中小企業の実態。このため、リスク度が分からない。リスクアセスメントの仕方が分からないのが現状であり、情報セキュリティ対策をトリガー視点でリスク認識出来ていない。

・分からない企業に、セキュリティ対策を求めても限界が・・・・・・・・むしろ、丸投げしたり、仕様化できない企業にはサポートしている側にサポート責任を求めたり、義務化するほうが良いとも考えられる。
例えば、サポータと一緒になってセキュリティ対策を施す環境を作り上げる。サポータにはサポータとしての適格マークの取得を義務化し、サポータと一緒になって安全な対策を講じた企業には安全事業者の認定を与えるなどの策が、むしろ現実的かもしれない。大胆な発想であるが、サポータへの診断・教育・適格マークの付与は JNSA，サポート先の企業診断はサポーターが実施し、安全事業者の認定は経済産業省？が行うなどの抜本策も必要。

・IT 監査は必要。建築基準法のような届け出制も必要か?
届け出の際にセキュリティ強度証明提出のような仕組みも欲しい。

③「中小企業が実際に実践できるアプローチ手法とは」について

・まだまだ啓蒙・啓発段階にある中小企業には、情報セキュリティ対策の入口に当る情報資産の分類から始め、情報資産の保有状態、利用範囲、管理状況等を情報資産管理台帳に記載して見る。記載された結果から資産価値・脅威・脆弱性を把握し、現状における情報資産の状況をワークシートに記載することで体感してもらうのが近道。
そして、評価段階におけるリスク度の診断・判定は情報セキュリティチェックシートを活用いただく。チェックシートを自社の現況に合わせてアレンジして使用戴く事こそ、チェックシートの求めるところでもある。

【記憶に残った意見・見識】

・トリガーについての共通的な見解。
「情報セキュリティが経営とリンクしている事を明示できない」ジレンマが最大の課題。情報セキュリティ対策がビジネスと連動していない。

・リスク認識は経営者は誰でも感じているが、優先課題と捉えていない。
情報セキュリティ対策が品質基準や環境基準、個人情報保護ガイドラインのように、定量的に明示できない事から、説得感が今一不足。

・リスクは・目的（自身のため、相手先のため、第三者のため）によって異なる。このため、基準も当然異なるべきであり、PCIDSS のような基準が必要である。

・情報セキュリティ対策基準として明示されたガイドラインや ISMS 管理基準に

より、どれだけリスクが排除されたかが見えない。対策する事は“言い訳”のためかもしれない。

・技術対策基準は受け入れられやすいが、技術的対策が定量化されたリスクと紐付け出来ていない。（業務プロセス視点での理解が不足）

・IT の導入の必要が説得できていない。その為、基盤をなす情報セキュリティ対策に説得感がない。このため、CIA が CI 偏重となっている。

・情報セキュリティ対策で最も必要とされるのは組織的対策（マネジメント）経営者の度量の問題。誰がリスクについて経営者を説得できる。経営者に鈴をつけられるのは誰？

・情報セキュリティポリシーを観念的に捉え、そのベースである情報資産管理ができていない。卵と鶏の関係に近いが、リスク認識を引き起こさせるワークが先にあり、組織的対策はその次に行うと言う考え方もありきか・・・・・・

格付けは？適格マークは必要？また付与できるか？

格付けは中小企業には厳しい。大手取引先との委託元・委託先の関係の中では価値がある。適格マークは格付けとは異なり、もっと砕けた低位のもので良いと思われる。安心＝適格マーク、安全＝認証

ウイルス対応、サーバ管理、ボット対策と言った必要最低限の対策を真面目にやっている企業に適格マーク付与することはあっても良いのでは・・・・・・

・ＩＳＭＳ認証のようなものでは無く、出来るところから実施した結果を評価して良いのでは。

４．２　中小企業が求めるセキュリティヘルプデスク

①独自に企業内にセキュリティ担当者を置く事が出来る中小企業（少なくとも質問が出来る担当者が存在する企業）なら、ヘルプデスクも歓迎！

②SI’er やソフトハウスが企業と一体となってセキュリティ対策措置を実現する世界を作り上げる事の方が、中小企業にとっては早道。

情報セキュリティに携わる組織がない中小企業（質問さえできない中小企業；SI’er やソフトハウスに丸投げしている企業）では、サイトを訪れるのは企業ではなく、SI’er やソフトハウスになるだろう」。この場合には、中小企業を対象にしたセキュリティヘルプデスクと言う呼称は中小企業をサポートする SI’er を対象にしたセキュリティヘルプデスクとするのが現実的かもしれない。

③サイトを訪れる人が気楽に訪問可能な状態とするには、企業トップの理解・支援が必要。本アプローチはそういう意味からすると、まずは企業経営陣から進める。

④中小企業の質問はどんな内容だろうか？

テクニカルな部分は相談する相手が存在する。（例えば系列のベンダーとの接触。むしろ、他企業の動向とか、法律的な解釈を求めるケースが多くなるのでは？

そういう事から、情報セキュリティ資格者以外に、弁護士や公認会計士やコンサルの能力が求められよう。

５．　まとめ

５．１　企業分類

情報セキュリティ対策に関するアンケート・ヒアリング、往復ハガキによる補完策、BoF の結果から、中小企業の情報セキュリティ対策に対する行動を３つのパターンとして分類する事が出来る。

表５－１　行動パターンによる企業分類

企業分類	意識	対策の要請
取引先からの要請に応える事が求められる企業（大手企業との取引のウエイトが高い企業）	◎	企業規模に拘わらず委託元と同等の水準を求められている。
責任の明確化・職務の分類が行われている企業（自社の情報セキュリティ対策が必要な企業）	○	企業価値向上・内部統制等目的から対策する事の必要に迫られている。
永遠のビギナー 責任の明確化・職務分類が行われていない企業	△	守るべき情報資産があり、守らねばならない必要意識が漠然とはあるが、費用対効果が見えず躊躇・逡巡し、対策の実践が伴わない。
	×	情報セキュリティ対策の必要を感じない。

５．２　企業分類への具体的なアプローチ策

対象とする中小企業の規模は 300 人未満としつつ，20 人未満企業については、除く事として、アンケート等の活動を行ってきたが、アンケート等で得られた結果は、従業員規模、売上規模による対策の実施度差異はあまり見られず、また業種による差異についても定性的な傾向は見られなかった事から、本 WG が活動対象とする企業分類を次のとおりとする。

表５－２　企業分類への具体的アプローチ策

企業分類		ツール	具体的アプローチ策
受委託関係にある企業		チェックシート	大手企業からの半ば強要・強制に近い要請に応える必要から、主体は大手企業側にある。本 WG は中小企業が実践できるアプローチ手法としてのチェックシートの作成を追求。大手企業の求める対策に対し、中小企業の立場から整合性を求める事を目的としているため、大手企業による要請（格付けワーク等を含む）への提言にとどめる事とする。
自社の対策を迫られている企業		チェックシート	本 WG が開発したチェックシートの活用を促すと共に、IPA の中小企業の情報セキュリティ対策に関する研究会に参画して、標準化を図る。
永遠のビギナー	対策の実践が伴わない企業	チェックシート 情報セキュリティ理解度チェックサイト	中小企業をサポートする SI'er、IT コーディネータへの啓発・教育・サポート（ヘルプデスク等）により、間接的な支援を行うと共に、直接的には情報資産管理台帳への記載を通して、対策の必要の気づきを勧奨する。 （ワークシートでの実践型アプローチ）
	対策の必要を感じない企業	インシデント事例の紹介による啓発・啓蒙	ベストプラクティス型とは真逆の事故事例の積極的紹介による啓蒙・啓発。 セキュリティ読本等による教育やセミナー （気付きを促すアプローチ）

６．情報資産管理台帳ワークシート記載に関連したアンケート調査

アンケート・ヒアリング、往復ハガキによる補完策並びに総括する意味で開催した BoF の結果から、守るべき情報資産があり、守らねばならない必要意識が漠然とはあるが、費用対効果が見えず躊躇・逡巡し、対策の実践が伴わない企業にとっては、『セキュリティ対策はジグソーパズルの様なもの』なのかも知れない。この『ジグソーパズルのピースを作り出すのが情報資産管理台帳』であり、『情報セキュリティ対策の入り口の役割を果たすものである筈！』との認識が得られたので、原点に立ち帰り活動を行う事として、情報資産管理台帳（シート）モデルの作成を次なる活動テーマとした。

なお、情報セキュリティチェックシートについては、往復ハガキで回答できない理由のトップの４３％を「同様なアンケートが多い」が占め、各方面から発信される類似のチェックシートの氾濫傾向が窺えることや同シートに対しては、SE、SI'er の完成版としての評価も高まっている現状から、改編を続けることで逆に混乱を招く恐れも想定されたため、完成版として、自社の対策度診断やサポータの企業支援ツールとして位置付ける事とした。

６．１情報資産管理台帳ワークシートの概要

（１）　背景・課題

情報セキュリティポリシーとは、『どのような情報資産をどのような脅威からどのように守るのかと言った基本的な考え方に立って、情報セキュリティを確保する為の組織、ルール（運用規程、基本方針、対策基準など）を具体的に記載するもの。

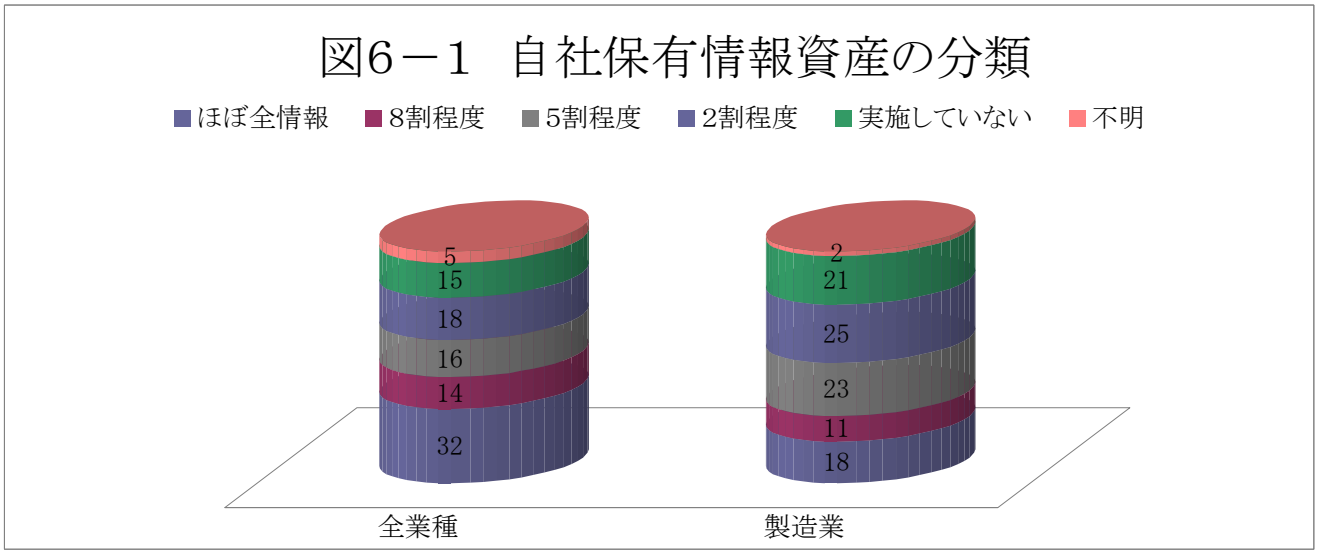
このため、セキュリティポリシーが策定されていれば、対策の実践が伴わないと言う事など起こり得ないわけであるが、対策の実践が伴わない企業に於いては、情報セキュリティ対策の入口とも言われる情報資産管理台帳の未整備が大きく影響し、責任の明確化、職務の分離、ルールにも結果として影響しているのでは無いかと考えられる。

表６－１のアンケート結果により、これらの相関性の存在と共に、マネンジメントの核となる広義の組織体制（責任の明確化、職務の分離、ルール）に於ける二極化現象を見る事が出来る。

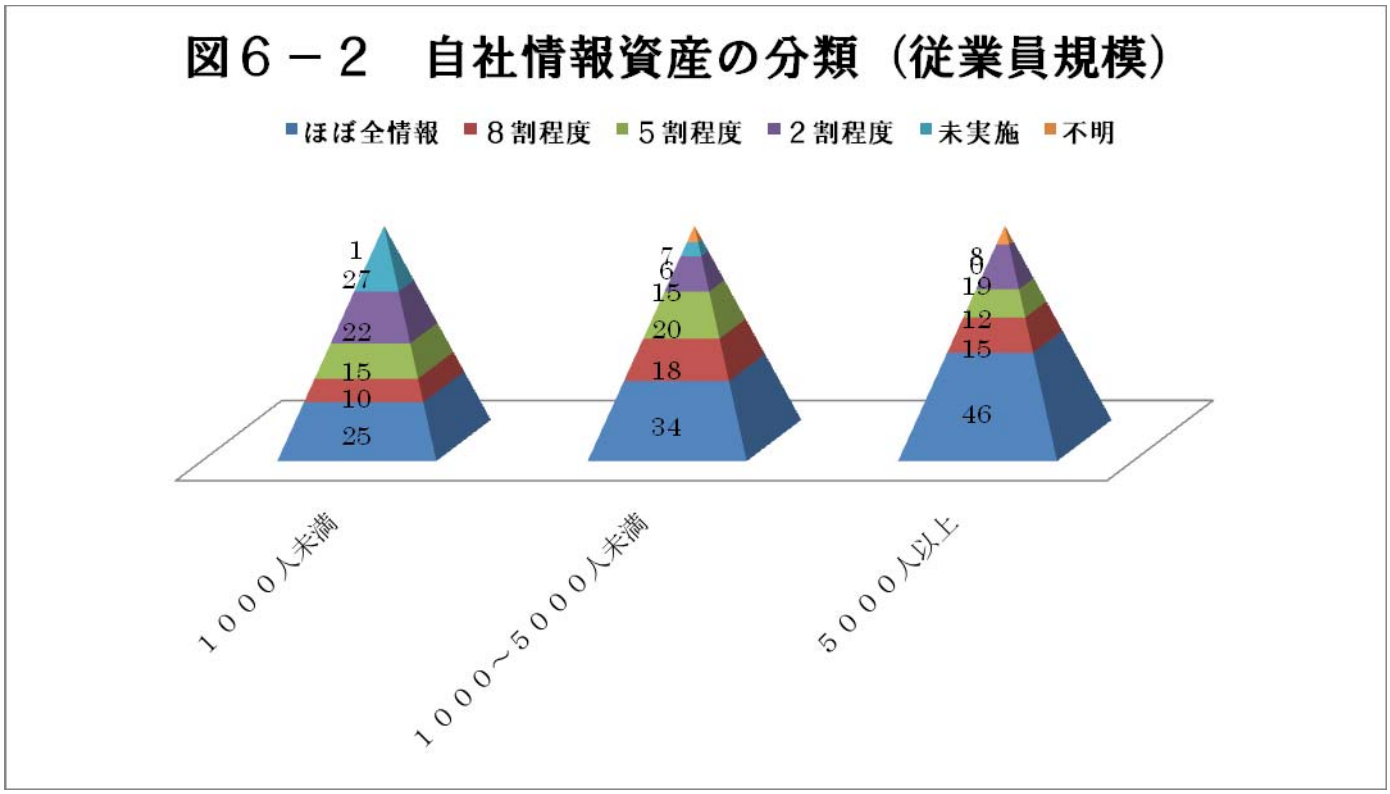
表６－１　　情報セキュリティ基本方針と相関性あるキーワード

選択肢レベル / キーワード	1	2	3	4	回答企業 合　計
情報セキュリティ基本方針	９社	２社	１社	３社	１５社
責任の明確化	９社	２社	２社	２社	１５社
職務の分離	８社	３社	２社	２社	１５社
情報資産管理台帳	８社	４社	１社	２社	１５社
ルール	８社		４社	３社	１５社

情報資産管理台帳が情報セキュリティ対策の入り口のはず！との推論を立てたが、自社保有情報資産の状況は図６－１及び図６－２の IPA 調査資料（取引先の情報セキュリティ対策確認状況に関する実態調査）によれば、作成の実施状況は遅れがちであることが明らか。



全業種で見ると、自社保有情報資産の５割程度以下の分類実施企業が４９％、製造業では６９％、同様に、１０００人未満の従業員規模では６４％を占めており、未実施がそれぞれ１５％、２１％、２７％となっている。



＊３００人未満の企業（１社）の回答は、２割程度の情報について実施しているであった。

（２）情報資産管理台帳作成の目的

取引先と企業自身が感じているセキュリティ対策のギャップについての議論に持ち込むことができる企業にとっては対策を強く求める事が出来るが、それを感じない、自身が我慢さえすればよいと感じる企業が多い中小企業には、対策することへの義務化・切迫感を如何に与えるかが必要となる。過去に情報事故が発生していない企業にはリスクに対する観念が薄く、いざ対策を実践する段階となると、自分のところは大丈夫だろうとなり、対策が後回しにされる。

“IT 活用の知恵比べ”が企業の優劣を決める時代になった今日、情報資産管理台帳ワークシートによるセルフ診断は、内部統制にも、情報セキュリティ対策にも共通する事から、それぞれのサイズにあった対応の必要（リスク認識）を意識づけることを目的として、情報資産管理台帳ワークシートの作成を次期研究テーマとした。

（３）情報資産の洗い出しと情報資産管理台帳

①情報資産が『どこにあり』、『誰が管理し』、『どのような状況で扱われているか』についての情報資産洗い出しの手順の確立が必要。

・範囲の決定

情報資産を初めて洗い出しする場合は、初めから完璧に把握しようとしても、作業負荷が大きすぎて途中で挫折する可能性が大きい。このため段階を踏んでのワークが必要と考えられる。

・『何らかのルールを決定』→『洗い出す対象範囲を決定』

まず、顧客情報を含む個人情報と営業秘密→次回は取引先より提供を受けた機密情報→次々回は・・・。また、特定の部門に限定することも！（EX;開発部門）

・洗い出し作業責任者と実際の作業者の決定。
・情報の管理責任者と情報の利用者を明らかに！

② JIS　Q　27002 参照結果

ア．情報セキュリティを確保するには、保護すべき情報資産を明確にする必要がある。

イ．組織が保有する重要な業務情報とは？
財務情報、人事情報、顧客情報、戦略情報、技術情報

ウ．　情報を処理するコンピュータ、ソフトウェア、記録媒体も情報資産である。

エ．　電子的データだけでは無く、紙媒体、会話、物理的な施設・設備, さらには、人や企業イメージも含まれる。

表６－２　情報資産の分類（ＪＩＳＱ２７００２参照）

分　類	例　　示
情報	データベース及びデータファイル、契約書及び同意書 システムに関する文書、調査情報、利用者マニュアル、訓練資材 運用手順またはサポート手順、事業継続計画、代替手段の取り決め、 監査証跡、保存情報
ソフトウェア資産	業務用ソフトウェア、システムソフトウェア、開発用ツール ユーティリティソフトウェア
物理的資産	コンピュータ装置、通信装置、取り外し可能な媒体、その他の装置
サービス	計算処理、通信サービス、一般ユーティリティ（暖房、証明、電源等）
人、資格等	人、保有する資格・技能・経験
無形資産	組織の評判、イメージ

オ．　記録形態（紙、電子化、人の記憶、製品サンプルに実装）による情報資産の分類。
・情報資産は膨大→個々の情報ごとに洗い出すのでは無く、情報をグループ化。
・自組織の機密情報と他から預かった機密情報に分類
・個人情報、営業機密のような重要な情報のタイプに分類
・資産価値や属性（用途、保管場所、保存期間など）で分類
・用途が同じパソコンやサーバをまとめてグループ化
・情報のライフサイクルが同じものをグループ化

カ．情報資産管理台帳で管理する項目は！
・情報資産の種類、情報資産名
・用途
・影響（CAI）
・業務上の価値（事業継続における重要度）
・管理責任者・管理担当者
・利用者の範囲

・記録形態
・保存場所
・保存期間
・廃棄方法
・その他（他の業務との依存性、バックアップ、ライセンス情報等）

（４）情報資産管理台帳作成における留意点

自社保有情報資産の分類が５割程度以下の企業が大半を占める中小企業、特に６９％を占める製造業にとっては情報がどのような形式で格納されているか？　どこにあるのかさえ分からない実態にあるため、実際に情報資産管理台帳に記載することで、情報資産の存在を感じ、その重要性を識別できるワークシート的な観点でのモデルを作成することとした。

① コンセプトは情報セキュリティ対策の第一歩となる『リスクコントロール』を支援する。
② 最終目標は情報セキュリティチェックシートと紐付けが出来るリスク評価が行える事とするが、その為には、重要な情報資産の存在に気づく段階から、リスク評価を対象とする資産ごとに適切に行える段階にまで、Step By Step で高めていく事とする。
③ 業種単位での情報資産管理台帳モデル作成を通して、その共通性や独立性を考察する。
④ 情報資産管理台帳モデルを参考に、会員企業が実際に情報資産を洗い出し、記載できるかについて、事前に団体事務局を訪問して現状・対象媒体、影響度と共に、業種にあった表現や適切な記載内容、例示等について意見を求めることとした。

●情報資産管理台帳（シート）モデルの作成について留意した点は以下の通り。

ア. 情報資産を洗い出し、簡易に記載できる様に、情報資産管理台帳記入要綱、情報資産管理台帳記入例（サンプル）、情報資産分類例、CIA 影響度レベル例を用意した。

イ. 情報資産管理台帳記入要綱と情報資産管理台帳記入例を組み合わせて表示し、台帳記入へのガイドとした。

ウ. 情報資産管理台帳記入例は、出来るだけ記入例を多く記載すると共に、情報資産分類の情報資産例と紐付けた。
情報資産名欄及び情報資産例欄には製造業にとって重要とされる仕様書、図面、配合データ等から生産管理・販売管理・会計処理等の基幹系システムに至る例示を多く記載。

エ. 情報資産に企業資産に加えて、企業情報資産を処理する社員所有 PC（ネット接続、スタンドアローン）も含める事を推奨した。

オ. 情報資産分類の分類例及び説明には、情報セキュリティチェックシートで使用している用語を使用し、情報資産管理台帳記載と情報セキュリティチェックシートの紐付けを意識させる。

カ. ソフトウェアについては、基本ソフトウェアと応用ソフトウェアの分類に

留め、オフイス用のアプリケーションは管理する単位からは除外した。
リスク管理の点では、最終的には必要な分類であるが、今回のワークの目的が、情報資産管理台帳への記載を第一義としたため、混乱を防ぐ目的から包括した。

キ．CIA 影響度については、情報か情報以外に注意して影響度を評価すること推奨した。リスク評価については、二次、三次 Step でのワークとするため、脅威例、脆弱性例については省略した。

６．２アンケート調査

（１）アンケート調査概要

①調査方針

もう一歩で優良企業に仲間入りできる企業群を見出し、支援すると言う当初の目的達成のためには、アンケート・ヒアリングには元気の良い企業を対象とし、課題を探ると言う行為と WG で得られた成果が実ビジネスの中で活用される結果の双方を満足するアプローチを行うこととした。

②アンケートの対象

これまでの活動の中で、セキュリティ対策に逡巡し、対策に効果を見出す事が出来ないために反応が薄い層に対しては、企業に密接に入り込んでいる中小ソフトハウス等を介して間接的にアプローチする事がリーズナブルとの見識が得られたこともあり、同様の間接的アプローチ視点で、企業の各業種業態で組織化されている元気な「団体・同盟」にアプローチする事とする。

ア．対象業種

これまでと同じく製造業とするが、業種・業態で特性がみられる事から、平成１８年度情報処理実態調査（経済産業省）及び事業所・企業統計調査（総務省資料）を参考に、５業種を抽出後、最終的には３業種に絞り込むこととした。

なお、決定された団体への協力のお願いは、近畿経済産業局にお願いする。

表６－３　キーワード別製造業の中分類業種ベスト５

キーワード	１位	２位	３位	４位	５位
トラブル発生状況	情報通信機械器具	一般機械器具	輸送用機械器具	非鉄金属製品 金属製品	食料品・飲料 たばこ・飼料
対策状況	情報通信機械器具	一般機械器具	化学工業	輸送用機械器具	食料品・飲料 たばこ・飼料
対策費用	情報通信機械器具	一般機械器具	食料品・飲料 たばこ・飼料	電気械器具	輸送用機械器具
対策効果	一般機械器具	食料品・飲料 たばこ・飼料	輸送用機械器具	情報通信機械器具	石油・石炭プラスチック製品
外部への依存度	食料品・飲料 たばこ・飼料	一般機械器具	情報通信機械器具	非鉄金属製品 金属製品	電気械器具

イ．業種絞り込みに於いて留意した検討事項

・統計資料は経済産業省、総務省の全国ベースでのものであり、大手・中堅企業の声が多く集大成されたものと考えられるため、我々が求める中小企業の声にはあらず、参考とするものの、統計値を鵜呑みには出来ない。

・キーワードとして採用した「トラブル発生状況」「対策状況」「対策費用」「対策効果」「外部への依存度」の各統計値＊　を総合的視点（加点方式も考慮）で判断するか？　ワークの方向性に最もフイットするキーワードを採用するか？

・企業規模の機能物数（資本金規模、年間事業収入、従業員規模）を総合的視点で判断するか？　ワークの対象とする業種業態に整合したものを採用するか？

（アンケートに回答している企業の事業収入規模は 10 億～100 億、従業員規模では 100 人～300 人が圧倒的）

・関西における産業構造を反映すべきか。

ウ．検討結果

表６－３から、IT 実践は進んでいるが、効果の認識にまでは至っていない中小企業の対策実態を表す指標としてトラブル発生状況、対策状況、対策費用の回答数が高い上位５業種をピックアップ、関西の産業構造にフイットする以下の３業種を採用することとした。

・一般機械器具製造業に属する「金型」

・食料品・飲料・たばこ・飼料製造業に属する「清酒製造業」

・輸送用機械器具製造業に属する「自転車・同部分品製造業」

なお、情報通信機械器具製造については、委託元・委託先の視点では面白いが、近畿における企業数が少ないこともあり、見送ることとした。

関西における産業構造視点から候補に上がったその他の業種では、靴下製

造業、かばん製造業、繊維工業（＊＊ちりめん等)、産業用ロボットがある。しかし、産業用ロボットについては関西に支部が存在しないため却下となった。

エ．アンケート調査において留意した点

・業界団体事務局との連名によるアプローチ
これまでの企業に直接アプローチするのではなく、近畿経済産業局・JNSA・業界団体事務局連名による協力のお願いとする。

・アンケートへの協力依頼文については、依頼内容の基調は共通とするが、それぞれの団体のおかれた環境や情報資産の状況を考慮して作成する事とする。

・作成された情報資産管理台帳の保存は各団体事務局で保管を原則とし、JNSA では分析・解析のためにデータを活用後、事務局に返還の事としたが、最終的には、JNSA 事務局で責任をもって廃棄する事となった。

・アンケートについては、情報資産を書き出す事、影響度を書く事で、どう役だったかを聞き出す事をポイントとする。
アンケート作成の趣旨は、情報資産管理台帳の作成が自力でどれだけ行えたのか？サンプルシートを活用することにより実施できたのか？作成できたことにより、どう活用したいのか？等の『感度』が作成戴いた情報資産管理台帳から把握し難い事から、これを補完するためである。
＊影響度については具体的な影響を想定できたか？　影響度が想定できない・記入できない理由について問うこととする。

（2）アンケート調査方法

アンケートの対象業種で日常的に使用されている情報資産の名称を情報資産管理台帳記入例（サンプル)、情報資産分類例に記載することで、情報資産管理台帳への記載が「守るべきものは何か？　その重要度は？それを育て、伸ばし、競争相手から如何に守っていくのか？その対策は？」を企業 TOP に気づかせ、企業存続・企業価値向上へのパラダイム変換（ex；利益の追求を「損失回避」から「企業ブランドの向上」）により実現に繋ぐものとの視点で、自社の情報資産管理の現実を見つめて戴くことを目的として、業界団体事務局へのプレヒアリングを実施した。

プレヒアリングで得られた指摘や参考意見は情報資産管理台帳サンプル及び情報資産分類に反映、アンケート協力への“やらされ感”排除に努めた上で、本実施とした。

①プレヒアリングの実施

アンケートの対象としてピックアップした「金型」「自転車・同部分品製造業」「清酒製造業」であったが、このうち、「自転車・同部分品製造業」については、残念ながら海外との競争に疲弊し、完成車・部品メーカーが参加する協会が東京にしか無い事が判明したため、また、「清酒製造業」については、財務省管轄と言う事で、ヒアリングに同意戴けず、残念なが

ら断念する事となった。

そこで、対象業種絞り込み時に、関西における産業構造視点から候補に上がった「かばん製造業」、八尾市を発祥の地として発展して来た「ブラシ製造業」を対象業種にする事とした。

結果として、プレヒアリング先は次の３団体となり、８月下旬から９月初旬に、それぞれの団体事務局を訪問した。

・社団法人　日本金型工業会　西部支部
・兵庫県鞄工業組合
・全日本ブラシ工業協同組合

②アンケートの実施

上記３団体事務局を訪問した結果は調査結果の項で記述することとするが、いざアンケートを発送する段階になり、全日本ブラシ工業協同組合より辞退の申し出があり、アンケートの実施は社団法人日本金型工業会　西部支部、兵庫県鞄工業組合の２団体となった。

それぞれの団体会員（社団法人日本金型工業会　西部支部１３５社、兵庫県鞄工業組合５９社）に郵送によりアンケートを送付し、郵送にて回収した。

ア;送付日　　;平成２０年１０月６日
イ;回収期間　　;平成２０年１０月６日～平成２０年１０月３１日

（3）アンケート調査結果

①プレヒアリング

ヒアリング調査結果

異なる業種選択の趣旨は、アンケートのレスポンスも主要因の一つであるが、中小企業と言えど、それぞれの属する業種によって環境に差異があり、その差異を認識したいと言うのも主要因であった。現実に、組合をヒアリング訪問することで、情報資産の呼称や整理の仕方、課題にも差異がある事や、企業の直面する悩みに直に触れる事が出来た。

以下にヒアリングで感じた共通点を列記する。

・中小企業向けの個人情報保護対策チェックシート、情報セキュリティチェックシートWGの活動（チェックシートの作成・アンケート活動等）と実践して来たが、製造ノウハウの流出*12がユーザからと言う現実を目の当たりにし、まだまだ、大手企業からの目線でのワークであったと痛感した次第である。
・脅威の対象で強く感じたのは製造技術の流出リスク*　であり、その脅威の高さに苦慮されている。（図面・製品仕様・配合データ等）
・一過性の強い単品生産が多く、多額の費用のかかる特許取得は難しく、また、経済産業省の指導（下請適正取引等の推進のためのガイドライン）にも拘わらず、発注側の優位な立場は変わらず、契約書でルール決めされる場合は皆無に近く、発注先コンプライアンス遵守に求めざるを得ない実情。
・製造工程への概念は相似しており、形態もＯＥＭ供給との事。

●ヒアリング事例紹介

○社団法人　日本金型工業会　西部支部

＊金型業界の憂える現実

日本の金型業界は、世界でもいち早くＮＣ加工技術を取り入れ、加工技術で世界トップ集団を走り続けてきた。しかしながら、ＮＣ加工技術の進歩・発展が世界的規模での加工技術の平準化をもたらし、中国・台湾・韓国・タイ・マレーシアなどの東南アジア諸国が工業国として台頭し、現地調達・低賃金国での生産などを背景に、もの作りのグローバル展開の勢いは増加の一途にある。

＊このため、金型業界での情報漏えいはユーザから漏えいするのが多い。

金型の製造委託取引において、発注者の金型仕様要望内容を反映した金型企業作成の金型設計図面を価格見積資料として提出させたり、金型製作後に、金型メンテナンス等を理由に、金型設計図面や金型加工データ等の金型製作用資料の提出を要請し、海外等の他社において同様または類似の金型製造委託に利用している日系企業が増えているとのこと。

＊図面にはねじれ矯正や冷却時の縮小など、金型製作に関するノウハウが盛り込まれ、リスク無しにほぼ同様の金型が製作できるとのこと。

＊金型は基本的に一過性の強い単品生産で、発注側の優位な立場は変わらないため、業界独自の自衛手段としての「金型著作権機構」を始動させたとのこと。（著作権は国内法以外にも国際的にベルヌ条約等で保護されている。）

＊金型業界の取引実態

・従業員１０名以下が８０％、従業員２０名以下では９０％を占めている。

・口約束での受発信→信義則を強要される弱い立場

・団塊の世代到来によるノウハウ伝承が課題→金型設計図面の保存

・情報資産の対象は金型設計図面←情報（ノウハウ・工法等）は図面に集積

・金型設計図面（完成図面）に至るまでの図面の変化

構想図（仕様要望書・仕様打合せ内容を具現化した図面）、承認図、部品図、加工図面、加工コスト

・加工コストと関係の深い会計（経理）・購買管理システム、設計製造システム（CAD・CAM、加工機）、社内 LAN（DNC；ダイレクト NC）も重要資産。

○兵庫県鞄工業組合

＊兵庫県鞄工業組合の抱える課題と製造工程における情報資産の存在

情報資産の最も重要なのは、型紙（デザイン・パターン）であり、同業社への情報封鎖が最重要であるとの事。特許による保護については保護の面で懐疑的；中国における九谷焼の例

＊製造への動機は、一次問屋からのＯＥＭ要求（外注生産）とメーカー自身の開発・生産（工場内一環）に大別されるが、その内、ＯＥＭ供給の場合に、製造技術の流出リスクが高く、その対策に苦慮されている模様。

＊一過性の強い単品生産。経済産業省の指導（下請適正取引等の推進のためのガイドライン）にも拘わらず、発注側の優位な立場は変わらず。

＊「鞄」のＯＥＭにおける受発注の流れ

デザイン仕様書（問屋）→型紙（パターン）→製品サンプル

ユーザからのデザイン仕様書は廃棄する事となっている。

＊一次問屋に保存責任があり、メーカー側としては、感知しないとの事。

＊「鞄」製造それぞれの工程において情報が発生する。

裁断→縫製→仕上げ--------検品

・生産管理システム　　品質基準　　品質基準

デザイン（企画）管理

製造管理

・販売管理システム

＊兵庫県鞄工業組合の取引実態

・生産システムを使用する企業は組合参加企業５９社の内、１０社程度。

・口約束での受発信→信義則を強要される弱い立場

・ノウハウからコスト、資金計画に至るまでの情報は経営 TOP の頭の中。

・型紙は製品として実現可能を前提。

・工業組合はメーカーとしての位置づけであり、ユーザとして卸問屋が存在する。問屋には地場における産地問屋があり、首都圏・名古屋・大阪の大都市に地方問屋と呼ばれる一次問屋が存在するが、一次問屋との直取引が実態。（一次問屋も中小規模企業であり、年収２００億未満の企業との事）

・卸問屋以外に、材料商品組合が存在するが、その数は１２社との事。

○全日本ブラシ工業協同組合

＊ユーザ（サンスター、ライオン、花王）からの発注形式。

＊形態はＯＥＭ供給。

＊製造工程

『デザイン図面→サンプル→金型図面→製造仕様書→製造→検査』

＊製造機械はベルギー製、ドイツ製であり、技術力差は大差なしとの事。

＊口腔衛生の高まりにより業績は堅調。販売はドラッグストアが５０％以上を占め、仲間意識も強く、１３年間で倒産業者無し。ブラシ、本体、パッケージの作成等分業確立。全国で７４社。そのうち８７％を大阪が占めている。（アウトサイダー；３０社程度への警戒感は薄い。）業界内は基本的に世襲が多い。

＊輸出は無く、市場は日本国内のみ

＊組合で毛の硬さなど規格の検査、認証マークを付与。

＊情報資産管理台帳の活用は信頼感や業務効率化視点。

②アンケート

団体事務局の協力を得て慎重に取り組んだが、金融不安の影響から売り上げ減少、事業継続が危ぶまれる事態に陥っている中小企業も見られる世

上不安な中でのアンケートとなってしまい、アンケートの回収実績は３％弱（5 社/194 社）と低調な結果に終わった。

チェックシートでの回答選択方法では、曖昧な理解でも回答は可能であることから、回答する経営 TOP がどれだけ理解しているか？その理解度は？が測れないため、今回のアンケート手法では、ワークシート形式による体感・実感手法（情報資産管理台帳作成を通して、経営 TOP 層に情報資産の管理実態を体感してもらう）を採用したのであるが、情報セキュリティ対策効果に懐疑的である経営 TOP に対しては、記述することへの負担感への配慮も必要であると考えさせられた結果であった。

伝統に裏打ちされた確固たる技術力に企画力・デザイン力を駆使して頑張る　元気な業種ではありますが、従業員規模は１０名以下が８０％、従業員２０名以下では９０％を占めている現状にあり、回答戴いた企業のすべてが２０人以下の規模であった。

表６－４　情報資産管理台帳ワークシート記載に関連したアンケート結果

アンケート質問事項	A 社	B 社	C 社	D 社	E 社	計
情報資産名を書けたか （書けた ○、書けなかった ×）	× 	○ 	× 	○ 	○ 	○ 3 社 × 2 社
書き出せた情報資産は自社の情報資産の何％		60％		60％	60％	
記入例は役に立ったか （役に立った ○、役に立たなかった ×）	× 	○ 	× 	○ 	○ 	○ 3 社 × 2 社
台帳に記載することで対策を行おうと気づかれたか （思った ○、判らない △、思わない ×）	○ 	○ 	△ 	○ 	○ 	○ 4 社 △ 1 社
影響度が具体的に理解出来たか （判った ○、 どう具体的に影響するか判らない △、 影響度とは何かが判らない ×）	△ 	○ 	× 	△ 	△ 	○ 1 社 △ 3 社 × 1 社
影響度の記入例は役に立ったか （役に立った ○、未回答 △、役に立たなかった ×）	△ 	○ 	△ 	△ 	△ 	○ 1 社 △ 4 社

表６－４は回答企業の情報資産の管理実態を表したものであり、少ない回答数ではあるが、中小企業の実態を表す以下の興味深い傾向が見られる。

・情報資産名を書けた企業は記入例が自社と類似しているか否かは関係なく、記入例を参照可能であり、台帳に記載する意義を感じ、情報セキュリティ対策を実践しようとの動機づけになると回答している。
また、自社の情報資産の６０％程度を書き出せたと回答しており、企業規模が小規模の場合（経営 TOP または少数の管理者が情報管理責任者）は比較的洗い

出しが容易にできる可能性を感じる。
情報資産をすべて網羅するのでは無く、自社の事業継続上においてKeyとなる重要資産を管理するのであれば、その可能性は更に広がるものと考えられる。

・情報資産名を書けなかった企業では、当然に記入例を参照する事は出来ず、影響度についても理解できないと回答しているが、興味深いのは、情報セキュリティ対策については、「対策を行おうとは思わない」と言う回答は無く、１社は「対策を行おうと気づかれ」、他の１社は「判らない」と回答しており、情報資産管理台帳の管理は情報セキュリティ対策の入り口の役割を果たすことが出来ると言えよう。

・影響度については、多くの企業がトラブルを経験していないことから、影響そのものが判らないと回答している企業も含め、情報資産を書き出せた企業（１社を除く)、書き出せなかった企業のいずれもが、影響度の記入例が役立ったかの質問に未回答であり、実際にCIAが損なわれた場合に、具体的にどのような影響が発生するかが判らないと言うのが実態と理解することができよう。

・この事から、本アンケートからもチェックシート同様に二極化現象が見られるが、セキュリティチェックシートによるアンケート結果の項では、対策の実践が伴わない企業・対策の必要を感じない企業を『永遠のビギナー』と称したが、『永遠』はあり得ず、セキュリティ対策＝技術的対策と局解しており、情報資産の重要度に応じた対策の必要の理解が不足しているビギナーに、情報資産管理台帳の作成が果たす意義、情報漏えい、情報の改ざん、情報システムが停止した場合に起こり得る取引先や他業務に与える具体的な事象・影響度を積極的に開示、啓蒙・啓発のための教育機会を今以上に拡大・実施していく必要があると考えられる。

７．更なる飛躍に向けて

７．１　中小企業情報セキュリティ対策支援セミナーの開催

情報セキュリティチェックシートの活用を通して、中小企業の情報セキュリティ対策の実情を把握するために実施したアンケート・ヒアリングの結果を総括し、「情報セキュリティ対策を必要とされている企業」にはJNSA西日本支部が作成した情報セキュリティチェックシートを活用戴き、自社の実施状況を診断、さらなる改善・PDCAに役立てて戴く。

一方、「守るべき情報資産があり、守らねばならない必要意識があるが、費用対効果の面が見えず躊躇・逡巡し、対策が伴わない企業」には、対策することへの義務化・切迫感を感じて戴くために、引き続きワークを継続。情報セキュリティ対策の入口と考えられる情報資産管理台帳ワークシートの活用を推奨する事とし、情報資産管理台帳への記載を支援するサンプルモデル等を用意して、アンケート調査を行ったことは、これまで述べてきたとおりである。

その結果は従前同様に回答率は低かったものの、製造業の業種団体の協力

を得て、より現場に近づいたものと評価できる事から、中小企業の IT パートナーとして、システムインテグレーションを支援する団体である JASIPA 関西との共催による「中小企業情報セキュリティ対策支援セミナー」を開催。中小企業に求められる情報セキュリティ対策！中小企業が実際に実践できるアプローチ手法とは？と題して、これまで培ってきた知見をもとにした活動成果の報告を行なうと共に、情報セキュリティ対策のさらなる飛躍に向けての課題を浮き彫りにするために、パネルディスカッション形式での BoF を開催した。

（1）BoF の実施

パネルディスカッション形式による進行は前回同様としたが、パネラーに「情報セキュリティ対策を啓発・支援する側」「対策を実践する上でサポートする側」「ユーザ側の代表者」を配して、それぞれの立場からの知見による議論が期待できるものとした。

・モデレーターとして、情報セキュリティチェックシートモデルの作成者。
・パネラーとして、独立行政法人　情報処理推進機構（IPA）の中小企業の情報セキュリティ対策研究会のリーダ、本 WG リーダ、中小企業製造業向け IT パートナーとして活躍をされている IT 企業社長、中小企業の情報セキュリティ担当者

【テーマ】

① 中小企業における情報セキュリティ対策のトリガーは？
② 中小企業に共通的に感じられる費用対効果への不満
③ 中小企業が実際に実践できるアプローチ手法は？

【パネラーからのコメント及び会場からの意見】

① 中小企業における情報セキュリティ対策のトリガーは？

・トリガーとなるのは取引先等の外部からの評価。
・取引先でウイルス被害が発生し、あらぬ疑いをかけられたが、会社としての予防保全対策で説明する事が出来、逆に、信頼を高める結果となった。
・経営者層で自社のセキュリティについて具体的な話が出来ないと、「脇が甘い企業」と思われるようになってきた。
・中小企業の経営 TOP は情報セキュリティ対策の必要は意識しており、「セキュリティ十戒」では無いが、必ず出るセキュリティ対策は「アクセス制限」（アクティブディレクター・ドメインでのアクセス制限）、「インターネット上での流出対策」（メール添付文書の拒否、管理職がＣＣで見られるように）
・情報セキュリティと言う言葉は説明し難い。品質セキュリティ、知財セキュリティと具体的に守る対象をハッキリさせれば、伝わるのでは・・・・
・セキュリティ対策が常識となれば・・・（銜えタバコがマナー上で敬遠されるように、）←自社・取引先の意識の高い人からのチェックは結構

効き目がある。

② 経営 TOP にトリガーを意識づけるのは誰（鈴つけ役は？）

・取引先が最適。（委託元から委託先への具体的な対策が明示されず、責任だけが押し付けられている現状は反省する必要があるが・・・・・）

・国のガイドラインより業界団体の評価の方がインパクトは高い。 同業者の社長の評価もインパクトは高い。

・中小企業の経営 TOP は品質、知財へのセキュリティ対策は判っている。どうやったら良いかのやり方が判らない。
業界団体標準があれば対策率は進むのでは・・・但し、リスク分析は不要。
最低限の対策を明示し，Step By Step 方式で高めていけば良い。

・しかし、複数の取引先を持つ企業は個別の対策を強いられ、閉口している。

・実践できる対策を明示するのは誰？
業務プロセスを理解できている TOP と何も判っちゃいない TOP ではどうなる。どちらも過剰反応すれば下には押し付け。

・情報セキュリティ対策の必要を主張する人と、情報セキュリティを明示する人との責任の明確化は必要。

③ やっぱり、啓発が必要。

・情報セキュリティには対策が取れていない場合に起こる“痛み”“熱い”の教育のネタが足りない。
「セキュリティ対策をしない」と言う意思決定をしているのではなく、「セキュリティ対策をする」と言う意思決定をしていないだけ。
過去に事故を経験したことが無い。異常状態に直面しても、それを正常の範囲内と捉え、自社は大丈夫と信じてしまう思考パターン（正状化への偏見）への対策として、異状状態（対策しなかったら、こんなトラブルや障害が）の知識をきちんと身につけ、曖昧な判断の入る余地を少なくするための教育・訓練が必要。

・規則はある。しかし、実践となると投げているのが実態のため、「危険予知 トレーニング」が必要。

・セキュリティは元来、双刃の剣と言われているが、「脅し」から「理解」への教育が必要。

・対策レベルを画一的に設定するのではなく、業種別・プロファイリング別に 強度を設定し、対策項目によっては中小企業はレベル１でも良いとか、２で良いとかのガイドラインを考察すべきでは無いのか。（３年前に、経済産業省委託調査でブロードバンドセキュリティに関する調査報告書でセキュリティ対策評価モデルのコンセプトで検討したものはある。）

④　中小企業に共通的に感じられる費用対効果への不満について

・必ず金食い虫と言われる。

・認知確立の問題。人はリスクを引き上げる事を極端に回避しようとする。

・可用性が機密性よりも重要。情報漏えいを起こすと、リスクコミュニケーションでの対応が大変。対応が悪いと顧客からの信用を失ない、売上が落ちる事もある。しかし、情報システムが必要な時に使えないと言うインパクトはもっと大きい。IT 依存度が高ければ高いほど、可用性が求められるのだが・・・。

・しかし、費用対効果を定性的・定量的に説明する事は困難。
地球温暖化とＣＯ２排出との直接の関係を科学的には証明できないが、現段階では温暖化対策にとって必要な事とされている。同じ様に、費用対効果の測定は現時点では困難であるが情報セキュリティ対策を行うことは価値があるとコンセンサスを得るようにする必要がある。

・継続した費用対効果を定性的・定量的に説明できるツール開発へのアプローチの継続は必要。

⑤　中小企業が実際に実践できるアプローチ手法は？

・常識作りが必要！
常識が守れない場合の内部・外部の反応ははっきりしている。
その為には、セキュリティ対策を行ったことで儲かった事例、信頼が営業成約につながった等の事例集を作り、経営とリンクしている事をもっと啓蒙する。
インシデント事例の収集は「内部統制が進んでいる企業には期待できる」が、そうでない企業にとっては信用を低下させ、企業価値を低下させる原因となるから、センシティブな情報を得ることは困難。しかし、企業の価値を高める事ができる成功事例なら、仕組さえ用意すれば可能。

○JNSA 情報セキュリティインシデント被害調査では、人為的インシデントにかかる報告が増加しているとの事。これは「内部統制を迫られている企業」が自主的にインシデントを公開しているため。

○２０１０年４月からセグメント会計基準の運用が予定されていると聞くが、セグメント情報開示は企業の内部管理体制をそのまま外部に公表する事になるため、管理体制に不備がある事は致命的になる。

・費用をかけること無く、こんなセキュリティ対策が出来たと言う事例や提案がもっとあれば・・・・・→これはシステムインテグレータ等の仕事。

・セキュリティ対策の必要を経営 TOP に説明・説得し対策を実現した事例も編纂出来れば・・・・・。

・団体標準をどんどん作り上げていく。

（２）JASIPA 関西による「情報セキュリティチェックシート利活用報告」

SI'er やソフトハウス企業に丸投げに近い中小企業にとっては、サポータ企業が中小企業と一体となってセキュリティ対策措置を実現する世界を作り上げる事の方が早道であるとの知見を得たが、そうなると、中小企業の模範となるサポータ企業のセキュリティに対する認識・実践度が問われる事となる事から、サポータ企業の実態についての調査の一環として、JASIPA 関西のメンバー企業に情報セキュリティチェクシートを実際に使用してもらい、アンケートに協力願う事としたもの。

表７－1 は上述したアンケート結果を取りまとめたものであり、以下の実態が垣間見られる。

① マネジメント系に属するセキュリティ対策の４０％で質問対象外との回答があった。人材支援企業として、派遣先常駐等で管理の必要がないとの見解から
との事であるが、情報資産に対する理解が不足しているものと思慮され、啓発が必要とされる。

② 対策が行われていないレベル１の回答者､質問対象外を選択された上記の企業以外の IT パートナーとして技術支援を行っている企業では、流石にレベル２以上、レベル３の企業が多く、対策の実践度は高い。

③ 同様に、責任の明確化、秘密保持についてもレベル３以上。情報資産管理台帳の作成活用､重要な資産から対策を行うべきとの認識はあると理解される。

④ ネットワークアクセス制御ウイルス、バックアップについては、質問対象外を選択された企業も含めて、すべての企業が対策を行っており、特に、アンチウイルスソフトの導入については、レベル３以上となっている。

⑤ サービスレベルの確保、ソフトウェアの選別と開発、監査ログは対策が出来ていないレベル１と質問対象外の合計が６０％以上となっており、特にサービスレベル（内部）及びソフトウェアの選別と開発は８０％を超える回答となっている。

⑥ 障害対策（地震等の被害を含む)、情報システム監査（第三者監査）の実施
については IT サポータに於いても、これからと言うのが現状。

⑦ 以上の事象から二極化現象は IT サポート企業にも顕著であり、JASIPA 関西の副支部長からも、IT サポート企業全体のレベルアップが必要との認識を強く持つと共に、IT 事業者への警鐘としたいとの説明が補足された。

（３）SI'er からの視点でのセキュリティ対策の必要について

「製造業における情報セキュリティ対策の実情について」と題して、製造業向け IT パートナーとして活躍をされている企業の代表者から、製造業の現場における情報セキュリティ対策の実情と“賢い管理”と共に、「システ

ム管理責任者は絶対必要」と講演戴いた。

また、「製造・生産業務の標準化と過剰在庫の削減成功事例について」と題して、IT パートナーとして活躍されている企業から、IT 活用事例を紹介願うと共に、システム面から見た情報セキュリティ対策の必要について講演を戴いた。

情報セキュリティ対策を可用性の視点に立って、ビジネスと連動している活用事例を紹介戴き、これまでの、CI 偏重のアプローチとは違ったアプローチ策へのヒントになる示唆であった。

表７－１　JASIPA 関西会員による「JNSA チェックシートの活用結果」

キーワード	選択肢レベル				
	1	2	3	4	質問対象外
情報セキュリティ基本方針		○　１０％	○　２０％	○　３０％	○　４０％
責任の明確化			○　４０％	○　２０％	○　４０％
職務の分離		○　２０％	○　２５％	○　１５％	○　４０％
委託先の管理	○　１０％	○　２０％	○　３０％	○　１０％	○　３０％
情報資産管理台帳	○　５％	○　１５％	○　２０％	○　２０％	○　４０％
文書化された手続き	○　１２％	○　２０％	○　１８％	○　１０％	○　４０％
ルール		○　１０％	○　４０％	○　１０％	○　４０％
秘密保持			○　５０％	○　１０％	○　４０％
ゾーン管理		○　３０％	○　１０％	○　２０％	○　４０％
入退管理	○　８％	○　２４％	○　３０％	○　２０％	○　１８％
サービスレベルの確保（内部）	○　４０％	○　１０％	○　１０％		○　４０％
サービスレベルの確保（外部）	○　２０％	○　１０％	○　１０％	○　１０％	○　４０％
ソフトウェアの選別と開発	○　４０％	○　１０％		○　１０％	○　４０％
業務データの管理	○　３０％	○　１０％	○　３０％	○　１０％	○　２０％
障害報告		○　２５％	○　１０％	○　３５％	○　４０％
障害対策	○　４０％	○　３０％	○　１０％	○　１０％	○　１０％
情報システム監査	○　３０％	○　４５％	○　１０％	○　５％	○　５％
ＩＤ	○　１０％	○　１０％	○　６５％		○　１５％
パスワード		○　３０％	○　１０％	○　２０％	○　４０％
アクセス権限	○　１５％	○　２０％	○　１０％	○　４５％	○　１０％
ネットワークアクセス制御（外部）		○　４０％	○　２０％	○　３０％	○　１０％
ネットワークアクセス制御（内部）	○　１５％	○　４０％	○　１０％	○　３５％	
ネットワークアクセス制御（サーバ）	○　１５％	○　３５％	○　２５％	○　２０％	○　５％
ウイルス（パッチの適用）		○　５０％	○　４０％	○　１０％	
ウイルス（アンチウイルスソフト）			○　６０％	○　４０％	
PC・電子媒体・紙の管理		○　１５％	○　３５％	○　３５％	○　１５％
電子メール	○　２０％	○　２０％	○　３０％	○　１０％	○　２０％
ホームページ	○　１０％	○　１０％	○　４０％	○　１０％	○　３０％
監査ログ	○　４０％	○　２０％	○　１０％	○　１０％	○　２０％
障害ログ	○　２０％	○　３０％		○　２０％	○　３０％
バックアップ	○　２０％	○　３０％	○　２０％	○　３０％	
性能管理	○　２０％	○　４０％	○　２０％	○　１０％	○　１０％
リリース管理	○　２０％	○　４０％	○　２０％		○　２０％
変更管理	○　１０％	○　４０％	○　２０％	○　１０％	○　２０％
構成管理	○　１０％	○　４０％	○　２０％	○　１０％	○　２０％

７．２　JNSA 西日本支部が継続して取り組むべき課題・指標

アンケート、ヒアリング、BoF を経て得られた知見　並びに　これまでの活動の最終総括としてのセミナー実施により得られた知見から、本 WG が継続して取り組むべき課題を以下に列挙し、本 WG のモットーである飽くなき探求心発揮への活動指標とする。

① 情報セキュリティチェックシートの活用促進

ア．元気な業界団体への提案・調査を継続し、業界団体のセキュリティ標準化を推進。情報資産管理台帳ワークシート作成を通じて、それぞれの企業特性に合った安全安心な IT 活用のために取り組むべき課題と進むべき方向性の示唆を行うために引き続きワークを継続する。

イ．情報セキュリティチェックシートの対策レベルを画一的に設定するのではなく、業種別・プロファイリング別に　強度の設定を考慮する。

ウ．SI'er やソフトハウスが企業と一体となってセキュリティ対策措置を実現する世界を作り上げる。(中小企業をサポートする SI'er を対象にしたセキュリティヘルプデスクの実現も併せて検討する。)

エ．情報セキュリティチェックシートと実施策としてのソリューションの紐つけは SI'er に求め、現場に適合するシートに改善していく。

オ．中小企業をサポートする SI'er、IT コーディネータへの啓発・教育をチェックシートや情報資産管理台帳への記載を通して行う。

カ．「危険予知　トレーニング」に活用できるチェックシートに高める。

キ．IPA の中小企業の情報セキュリティ対策に関する研究会に参画して、標準化を図る。

② 費用対効果へのチャレンジ。費用対効果を定性的・定量的に説明できるツール開発へのアプローチは必要。

費用対効果の測定が難しい理由として、

（A）測定方法がない。

（B）測定方法が判らない。

（C）測定方法は判るが測定が困難。

（D）測定方法が属人的で客観性がない。

があるが、「容易な測定方法検討する」アプローチをしたい。　費用対効果を明示できて、初めて、実施対策（セキュリティ製品等）との紐付けが実現できると考えており、そこに、真の価値基準（リスク認識）の討議が浮上してくると信じている。

③ セキュリティ対策を行ったことで儲かった事例、信頼が営業成約につながった等の事例集を関西における団体と連携して編纂する。

④ 情報セキュリティ対策の実施度評価・監査について、今回設立された日本セキュリティ監査協会（ＪＡＳＡ）西日本支部と連携して行う。

資　　料　　編

情報セキュリティチェックシート

No.	キーワード	対象					影響			付属書A他	トラブル事象例	質問	回答選択肢	業務委託で対応されている場合は□にチェックをいれて下さい	質問に該当しない場合は□にチェックをいれて下さい
		クライアント	ネットワーク	サーバ	アプリ	データ	機密性	完全性	可用性						
経営者・経営者層の方															
1	情報セキュリティ方針	○	○	○	○	○	○	○	○	システム管理基準 Ⅰ.情報戦略 1.全体最適化(1),(6) A.5.1.1 情報セキュリティ基本方針文書 A.5.1.2 情報セキュリティ基本方針のレビュー	機密性、完全性、可用性のバランスを取ったシステムの利用方針がないと全てのトラブルに発展する可能性がある	情報セキュリティを考慮したシステムの利用・活用方針を明確にしていますか？	①経営方針の中に情報セキュリティに関する記載が無い ②経営方針の中に記載はあるが、周知徹底が不十分である ③経営方針の中に記載をしており、周知徹底もしている ④経営方針の中に記載し、周知徹底しており、定期的に利用方針を見直している		
2	責任の明確化	○	○	○	○	○	○	○	○	システム管理基準 Ⅰ.情報戦略 2.組織体制 2.1(1),2.2(1) A.6.1.1 情報セキュリティに対する経営陣の責任 A.6.1.2 情報セキュリティの調整 A.6.1.3 情報セキュリティ責任の割当て A.6.1.4 情報処理設備の認可プロセス A.6.1.6 関係当局との連絡 A.6.1.7 専門組織との連絡 A.6.1.8 情報セキュリティの独立したレビュー A.8.1.2 選考 A.8.1.3 雇用条件 A.8.2.1 経営陣の責任 A.8.2.3 懲戒手続き A.8.3.1 雇用の終了又は変更に関する責任 A.8.3.2 資産の返却	責任の明確化ができていないとトラブル時の対処が遅れたり、事後の対処が的確に出来ない等の可能性がある	情報システムの利用及び情報セキュリティの推進について，組織における経営陣・各部署の代表者・各自の職務の使命、責任を明確にしていますか？	①情報システムの利用及び情報セキュリティの推進について，経営陣・各部署の代表者・各自の職務の使命、責任は明確ではない ②情報システムの利用については経営陣・各部署の代表者・各自の職務の使命は明確に決まっているが、情報セキュリティの責任については明確ではない ③情報システムの利用及び情報セキュリティの推進について，経営陣・各部署の代表者・各自の職務の使命、責任は明確に決まっている ④情報システムの利用及び情報セキュリティの推進について，経営陣・各部署の代表者・各自の職務の使命、責任は明確に決まっており、定期的に職務の使命、責任を見直している		
3	職務の分離	○	○	○	○	○	○	○	○	システム管理基準 Ⅰ.情報戦略 2.組織体制2.2(2) A.10.13 職務の分割	サーバ、データベース、アプリケーションの管理権限を持つシステム管理者が製造情報を保存した文書管理システムから製造情報を盗み出し、サーバに保存されたデータベース、アプリケーションのアクセスログを消去してしまい、誰が犯人か追跡できない	情報システムに携わる部門は、組織の規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にしていますか？	①システムの利用者とシステム管理者を分離していない（例：経理システムの利用者がシステム管理も兼務している） ②システムの利用者とシステム管理者を分離している ③システムの利用者とシステム管理者の分離しており、さらにそれぞれの業務に対する承認者を分離している ④システムの利用者、システム管理者、承認者を分離しており、責任範囲は権限の乱用や不正使用のリスクを低減するために分離している（例：システム管理者の分離[サーバ管理者、DB管理者、アプリケーション管理者など]）、さらに定期的に職務の分離を見直している		
4	委託先の管理	○	○	○	○	○	○	○	○	A.12.5.5 外部委託によるソフトウエアの開発	①委託先をセキュリティを考慮して選定しなかったため、委託先の社員より情報漏えいが発生してしまう ②システムを管理する基準(ITILなどのフレームワーク)を持っていない委託先にシステム保守を任せたため、小さな障害が大きな障害に発展する	セキュリティを考慮した委託先選定の基準(委託先がシステムの管理方法の基準を持っているか、重要データの管理基準を持っているかなど)がありますか？	①セキュリティを考慮した委託先選定の基準がない ②セキュリティを考慮した委託先選定の基準はあるが、基準にあって いるかを確かめる報告・監査などの手続きがない ③セキュリティを考慮した委託先選定の基準があり、基準にあって いるかを確かめる報告・監査などの手続きがある ④セキュリティを考慮した委託先選定の基準、報告・監査手続き、委託先そのものを定期的に見直している		□
5	情報資産管理台帳	○	○	○	○	○	○	○	○	システム管理基準 Ⅰ.情報戦略 4.情報資産管理の方針 A.7.1.1 資産目録 A.7.1.2 資産の保有者 A.7.1.3 資産利用の許容範囲 A.7.2.1 分類の指針 A.7.2.2 分類の指針	情報資産管理台帳を作成していないため、どの資産が重要であるのか判断できないため、全ての資産に対して過剰なセキュリティ対策をおこなってしまう	情報資産管理台帳を作成していますか?台帳には保有者、利用範囲、重要度、保管場所の記載があり情報資産の利用範囲は機密性・完全性に加え可用性も検討されていますか(不必要に過度な制限を設けていませんか)？	①情報資産管理台帳を作成していない ②情報資産管理台帳を作成しているが、保有者、利用範囲、重要度、保管場所全ての記載があるわけではない ③情報資産管理台帳を作成しており、保有者、利用範囲、重要度、保管場所全ての記載があり、利用範囲は可用性も検討されている ④情報資産管理台帳を作成しており、保有者、利用範囲、重要度、保管場所全ての記載があり、利用範囲は可用性も検討されている。さらに資産内容、記載項目を定期的に見直している		

情報セキュリティチェックシート

No.	キーワード	対象					影響			付属書A他	トラブル事象例	質問	回答選択肢	業務委託で対応されている場合は□にチェックをいれて下さい	質問に該当しない場合は□にチェックをいれて下さい
		クライアント	ネットワーク	サーバ	アプリ	データ	機密性	完全性	可用性						
6	文書化された手続き	○	○	○	○	○	○	○	○	A.8.1.1 役割及び責任 A.9.2.7 装置の移動 A.10.1.1 操作手順書 A.10.1.2 変更管理策 A.10.8.1 情報交換の方針及び手順 A.10.8.2 情報及びソフトウェアの交換契約 A.10.8.5 業務情報システム A.11.1.1 アクセス制御方針 A.11.3.3 クリアデスク・クリアスクリーン方針 A.12.1.1 セキュリティ要求事項の分析及び仕様化 A.12.4.1 運用ソフトウェアの管理 A.15.2.1 セキュリティ方針及び標準の順守 A.15.2.2 技術的コンプライアンスの点検	生産管理システムの管理手続きを文書化していないため、担当者が事故で不在の時、システムが停止してしまう	情報システムの管理、利用に関する組織内で承認された文書化された手続き(ネットワーク管理者マニュアル、サーバ管理者マニュアル、各システムの管理者マニュアル、ユーザマニュアル、データ取り扱いマニュアル等)がありますか？	①情報システムの管理、利用に関する手続きが存在しない ②情報システムの管理、利用に関する手続きは存在するが、文書化されていない ③情報システムの管理、利用に関する組織内で承認された手続きが存在し、文書化されている ④情報システムの管理、利用に関する組織内で承認された手続きが存在し、文書化されており、定期的に手続きを見直している		
7	ルール	○	○	○	○	○	○	○	○	システム管理基準 Ⅰ.情報戦略 6.コンプライアンス A.8.2.2 情報セキュリティの教育及び訓練 A.15.1.1 適用法令の識別 A.15.1.2 知的財産権(IPR) A.15.1.3 組織の記録の保護 A.15.1.4 個人データ及び個人情報の保護	遵守すべき法令が周知徹底(教育を含む)されていないため、ユーザがソフトウエアを違法にコピーし、使用してしまう	情報システム、組織に関する遵守すべき法令を反映したルールを文書化し、関係者に周知徹底(教育を含む)していますか?	①遵守すべき法令を反映したルールを文書化していない ②遵守すべき法令を反映したルールを文書化しているが、関係者に周知徹底していない ③遵守すべき法令を反映したルールを文書化し、関係者に周知徹底している ④遵守すべき法令を反映したルールを文書化し、関係者に周知徹底している。さらに定期的にルールを見直している		
8	秘密保持					○	○	○		A.6.1.5 機密保持契約 A.6.2.1 外部組織に関連したリスクの識別 A.6.2.2 顧客対応におけるセキュリティ A.6.2.3 第三者との契約書におけるセキュリティ	内部又は外部組織が故意に重要な製造情報を漏洩してしまう	組織の内部外部にかかわらず、関係者と、情報保護に対する組織の適切な管理策を反映した覚書または契約を締結していますか？	①組織の内部外部共に秘密保持に関する覚書も契約も締結していない ②組織の外部とのみ秘密保持に関する契約を締結しており、内部とは覚書も契約も締結していない ③組織の内部外部共に秘密保持に関する覚書または契約を締結している ④組織の内部外部共に秘密保持に関する覚書または契約を締結しており、定期的に要求事項を見直しをしている		
9	ゾーン管理	○	○	○	○	○	○			A.9.1.3 オフィス、部屋及び施設のセキュリティ A.9.1.5 セキュリティを保つべき領域での作業 A.9.1.6 一般人の立寄り場所及び受渡し場所 A.9.2.3 ケーブル配線のセキュリティ A.11.6.2 取扱いに慎重を要するシステムの隔離	ゾーン管理をしていないため重要な製品規格をアクセス権限の無い者が作業者の肩越しに見てしまう	アクセスコントロールポリシーに基づいたオフィス、部屋及び建物に対する物理的セキュリティを設計・ゾーン管理(例：サーバルームの設置、重要な情報資産を扱う作業場所の設置やデータセンターなどの利用)していますか？	①セキュリティ設計・ゾーン管理をしていない ②セキュリティ設計・ゾーン管理はしているが、アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理ではない ③アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしている ④アクセスコントロールポリシーに基づいたセキュリティ設計・ゾーン管理をしており、定期的に設計・ゾーン管理を見直している		
10	入退管理	○	○	○	○	○	○			A.9.1.1 物理的セキュリティ境界 A.9.1.2 物理的入退管理策	入退管理をしていないため、部外者が故意あるいは誤って社内に侵入してしまう	情報及び情報処理施設のある領域を保護するために、(社員通用、お客様用、搬入用などそれぞれに)入退管理をしていますか？	①個人を識別した入退管理をしていない ②個人を識別した入退管理をしているが、入退に関するログ・記録は残していない ③個人を識別した入退管理をしており、入退に関するログ・記録も残している ④個人を識別した入退管理をしており、入退に関するログ・記録も残している。さらに定期的に入退管理方法を見直している	□	

情報セキュリティチェックシート

No.	キーワード	対象					影響			付属書A他	トラブル事象例	質問	回答選択肢	業務委託で対応されている場合は□にチェックをいれて下さい	質問に該当しない場合は□にチェックをいれて下さい
		クライアント	ネットワーク	サーバ	アプリ	データ	機密性	完全性	可用性						
11	サービスレベルの確保	○	○	○	○	○	○	○	○	A.9.2.4 装置の保守 A.10.2.1 第三者が提供するサービス A.10.2.2 第三者が提供するサービスの監視及びレビュー A.10.2.3 第三者が提供するサービスの変更に対する管理 A.10.6.2 ネットワークサービスのセキュリティ	①生産ラインでは生産管理システム停止の許容は30分であるが、そのシステムが作動するサーバの運用先とのサービスレベルが存在しない。そのため30分を超えシステムが停止してしまう ②セキュリティパッチがリリースされてからパッチを適応するまでの時間を、セキュリティサービスを提供する会社と取り決めていない。そのためパッチ適応までに時間がかかり、その間にセキュリティホールを悪用され重要情報の破壊と漏えいが発生してしまう	組織の内部(情報システムに携わる部門と利用部門との間)で、情報サービスの提供・利用に関して、重要な要求事項(例：サーバ障害時の復旧時間等)を反映したサービスレベルを取り決めていますか？	①組織の内部でサービスレベルを取り決めていない ②組織の内部でサービスレベルの取り決めはあるが、実績値の報告はしていない ③組織の内部でサービスレベルの取り決めがあり、実績値の報告もしているが、実績値の評価はしていない ④組織の内部でサービスレベルの取り決めがあり、実績値の報告をし、実績値の評価をしており、その評価に基づきサービスレベルを見直している		
12												組織の外部（システムベンダー等）と、システム運用(保守サービス、ヘルプデスクサービス、セキュリティサービス等)に関して重要な要求事項(例：稼働率、障害時復旧時間、システム応答時間、電話応答時間、回答時間等)を反映したサービスレベルの取り決めをしていますか？	①組織の外部とサービスレベルの取り決めをしていない ②組織の外部とサービスレベルの取り決めはしているが、実績値の報告は受けていない ③組織の外部とサービスレベルの取り決めがあり、実績値の報告も受けているが、組織内で実績値の評価はしていない ④組織の外部とサービスレベルの取り決めがあり、実績値の報告を受け、組織内で実績値の評価をしており、その評価に基づきサービスレベルを見直している		□
13	ソフトウエアの選別と開発				○		○	○	○	システム管理基準 Ⅱ.企画業務　1.開発計画　(2),(3)	市販パッケージで代替できる会計ソフトウエアを自社開発してしまう	経営陣はパッケージソフトウエアの採用とソフトウエアの開発に関する明確な基準を定めていますか？(標準化された業務にはパッケージソフトウエアの採用を検討し、差別化されたあるいは競争力のある業務は開発をおこなうなどの基準)	①基準がない ②経営陣に承認されていないが、情報システム部門に基準が存在する ③経営陣に承認された明確な基準が存在する ④経営陣に承認された明確な基準が存在し、定期的に基準を見直している		
14	業務データの管理				○	○	○	○		A.12.2.1 入力データの妥当性確認 A.12.2.2 内部処理の管理 A.12.2.3 メッセージの完全性 A.12.2.4 出力データの妥当性確認 A.12.5.4 情報の漏えい（洩）	各工程で製品規格の入出力データをチェックする手続きがないため、間違ったデータを処理し、次の工程に製品を流し規格外の製品を製造してしまう	入力・出力データの完全性(データの妥当性など)と安全性(情報漏えい対策など)を管理する手続きまたは仕組み(システム的対策)がありますか？	①入力・出力データの完全性も安全性も管理する手続き・仕組みがない ②入力・出力データの完全性のみ管理する手続き・仕組みがある ③入力・出力データの完全性と安全性を管理する手続き・仕組みがある ④入力・出力データの完全性と安全性を管理する手続き・仕組みがあり、 定期的に管理する手続き・仕組みを見直している	□	
15	障害報告	○	○	○	○	○	○	○	○	A.13.1.1 情報セキュリティ事象の報告 A.13.1.2 セキュリティ弱点の報告 A.13.2.1 責任及び手順 A.13.2.2 情報セキュリティインシデントからの学習	障害の報告体制がないため、些細な障害が大きな障害を引き起こし生産ラインを停止してしまう	情報システムの運用において障害・事件・事故は，規模に関わらず、適切な管理者へ，できるだけ速やかに報告していますか？	①障害・事件・事故を報告していない ②大きな障害・事件・事故しか報告していない ③規模に関わらず障害・事件・事故を報告しいる ④規模に関わらず障害・事件・事故を報告しており、報告から運用の見直し改善をおこなっている		
16	障害対策	○	○	○	○	○		○	○	システム管理基準 Ⅵ.共通業務　7.災害対策 A.9.1.4 外部及び環境の脅威からの保護 A.9.2.1 装置の設置及び保護 A.9.2.2 支援ユーティリティ A.14.1.1 事業継続管理への情報セキュリティの組み込み A.14.1.2 事業継続及びリスクアセスメント A.14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施 A.14.1.4 事業継続計画策定の枠組み A.14.1.5 事業継続計画の試験、維持及び再評価	復旧対策が無いため、生産ラインの制御システムの障害時、復旧に時間が掛かってしまい、長時間生産ラインを停止してしまう	地震等の災害を含めた障害時の情報システムに与える影響範囲、被害及びリスクを明確にし、それに基づいた復旧・対応計画を策定していますか？	①障害時の情報システムの復旧計画を策定していない ②障害時の情報システムの復旧計画は策定しているが、障害時の情報システムに与える影響範囲、被害及びリスクに基づいたものではない ③障害時の情報システムに与える影響範囲、被害及びリスクを明確にし、それに基づいた復旧・対応計画を策定している ④障害時の情報システムに与える影響範囲、被害及びリスクを明確にし、それに基づいた復旧・対応計画を策定している、さらに定期的に復旧・対応計画を見直している	□	□
17	情報システム監査	○	○	○	○	○	○	○	○	A.15.3.1 情報システム監査に対する管理策 A.15.3.2 情報システム監査ツールの保護	①独善的な内部監査をしており客観性がない ②監査が日常業務をおこなう妨げになっている	情報システム監査をしていますか？	①内部監査、第三者監査ともにしていない ②内部監査はしているが、第三者監査はしていない ③内部監査、第三者監査ともにしている ④内部監査、第三者監査ともにしており、定期的に日常業務へ与える影響を考慮して監査手続きを見直している	□	

情報セキュリティチェックシート

No.	キーワード	対象					影響			付属書A他	トラブル事象例	質問	回答選択肢	業務委託で対応されている場合は□にチェックをいれて下さい	質問に該当しない場合は□にチェックをいれて下さい
		クライアント	ネットワーク	サーバ	アプリ	データ	機密性	完全性	可用性						

情報セキュリティ責任者・担当者の方

18	ID	○		○	○		○	○		A.8.3.3 アクセス権の削除 A.11.2.1 利用者登録 A.11.5.1 セキュリティに配慮したログオン手順 A.11.5.2 利用者の識別及び認証	利用権限を持たない社員が利用権限を持つ社員に成りすまし不正アクセスにより製造情報を盗み出し、漏洩する	情報システムの利用時に利用者固有のIDを割当てていますか？	①IDを割当てていない ②IDを割当てているが共有IDである ③利用者毎に一意のIDを割当てている ④利用者毎に一意のIDを割当てており、かつIDの割当て状況をチェックしている	□	
19	パスワード	○		○	○		○	○		A.11.2.3 利用者パスワードの管理 A.11.3.1 パスワードの利用 A.11.5.2 利用者の識別及び認証 A.11.5.3 パスワード管理システム		パスワードポリシー（例：パスワードは8文字以上で、英数字混在の類推しにくいものとする、パスワードは6ヶ月毎に変更し、3世代前までと同じものを使うことができない）に基づいてパスワード管理をしていますか？	①パスワードを管理していない ②パスワードを管理しているがポリシーに基づかない ③ポリシーに基づきパスワード管理を行っている ④ポリシーに基づきパスワード管理を行っており、かつ定期的にポリシーを見直している		
20	アクセス権限	○		○	○		○	○		A.8.3.3 アクセス権の削除 A.10.7.4 システム文書のセキュリティ A.11.2.2 特権管理 A.11.2.4 利用者アクセス権のレビュー A.11.3.2 無人状態にある利用者装置 A.11.4.1 ネットワークサービスの利用についての方針 A..11.5.4 システムユーティリティの使用 A.11.6.1 情報へのアクセス制限 A.12.4.2 システム試験データの保護 A.12.4.3 プログラムソースコードへのアクセス制御		管理者、利用者に対しアクセスコントロールポリシーに基づいてアクセス制御を行っていますか？	①アクセス制御はしていない ②アクセス制御を行っているが、ポリシーに基づいていない ③ポリシーに基づいたアクセス制御を行っている ④ポリシーに基づいたアクセス制御を行っており、定期的にポリシーを見直している	□	
21	ネットワークアクセス制御		○				○	○		A.10.6.1 ネットワーク管理策 A.11.4.2 外部から接続する利用者の認証	①外部者に不正アクセスされ製造情報が漏洩する ②外部者に不正アクセスされ製造情報の改ざんが発生する	外部からのアクセスをファイウォールや不正侵入防御装置(IPS)などで制限していますか？	①FWやIPSを導入していない ②外部からのアクセス制限をFWやIPSで実施しているが、アクセスログはチェックしていない ③外部からのアクセス制限をFWやIPSで実施しアクセスログをチェックしている ④外部からのアクセス制限をFWやIPSで実施しアクセスログをチェックし、かつかつアクセス制御の設定の見直しを実施している	□	□
22										A.11.4.3 ネットワークにおける装置の識別 A.11.4.4 遠隔診断用及び環境設定用ポートの保護		無線LANは認証、暗号化を実施し安全に利用していますか？	①アクセスポイントの管理はおこなっているが、認証、暗号化を行っていない ②アクセスポイントの管理に加え、認証、暗号化を行っている ③アクセスポイントの管理に加え、認証、暗号化を行い、アクセスログをチェックしている ④アクセスポイントの管理に加え認証、暗号化を行いアクセスログをチェックし、かつ認証、暗号化を定期的に見直している	□	□
23										A.11.4.5 ネットワークの領域分割 A.11.4.6 ネットワークの接続制御		社内においても重要情報はセグメント分割し他からアクセスできないよう保護していますか？	①アクセス制限していない ②セグメント分割しアクセス制限を実施しているがアクセスログのチェックを行っていない ③セグメント分割しアクセス制限を実施しアクセスログのチェックを行っている ④セグメント分割しアクセス制限を実施しアクセスログのチェックを行い、かつアクセス制御の設定を見直している	□	□
24										A.11.4.7 ネットワークルーティング制御 A.11.5.5 セッションのタイムアウト A.11.5.6 接続時間の制限		サーバのTCP/UDPポート、サービスなどへのアクセスを制御していますか？	①アクセス制限していない ②アクセス制限を実施しているがアクセスログのチェックを行っていない ③アクセス制限を実施しアクセスログのチェックを行っている ④アクセス制限を実施しアクセスログのチェックを行い、かつアクセス制御の設定の見直しを実施している	□	□

情報セキュリティチェックシート

No.	キーワード	対象					影響			付属書A他	トラブル事象例	質問	回答選択肢	業務委託で対応されている場合は□にチェックをいれて下さい	質問に該当しない場合は□にチェックをいれて下さい
		クライアント	ネットワーク	サーバ	アプリ	データ	機密性	完全性	可用性						
25	ウィルス	○	○	○	○		○	○	○	A.10.4.1 悪意あるコードに対する管理策	①ウィルス、ワームに感染し、生産ラインで使用しているPCが目的どおり動作しなくなる ②マルウェアに感染、製造情報が漏洩してしまう	OS、アプリ、ミドルウェアなどにパッチを適用していますか？	①パッチを適用していない ②パッチを適用しているが、その適用は利用者まかせである ③パッチを適用しており、その実施状況も管理している ④パッチ適用の有効性についての評価を行っている	□	□
26										A.10.4.2 モバイルコードに対する管理策 A.12.6.1 技術的ぜい弱性の管理		アンチウィルソフトでウィルス対策を行っていますか？	①アンチウィルスソフトを導入していない ②アンチウィルスソフトを導入しているが定期的なスキャンは実施していない ③アンチウィルスソフトを導入しており、定期的なスキャンおよびパターンファイルの更新を実施している ④アンチウィルスソフトを導入しており、定期的なスキャンおよびパターンファイルの更新を実施し、結果のチェックを行っている	□	□
27	PC・電子媒体・紙の管理					○	○	○	○	A.10.7.1 取り外し可能な媒体の管理 A.10.7.2 媒体の処分 A.10.8.3 配送中の物理的媒体 A.9.2.5 構外にある装置のセキュリティ A.9.2.6 装置の安全な処分または再利用 A.12.3.1 暗号による管理策の利用方針 A.12.3.2 鍵管理 A.11.7.1 モバイルコンピューティング及び通信 A.11.7.2 テレワーキング	①製造情報を含んだ媒体、PCの盗難、紛失により格納していた情報が漏洩する ②媒体に製造情報を格納したまま廃棄してしまい、その情報が漏洩する	媒体・PCの利用時または廃棄時において、媒体やPCに格納された情報に対し漏洩対策を実施していますか？	①何も対策していない ②情報の場合はパスワード設定、暗号化などによる保護、紙の場合は施錠した場所での保管、また廃棄時には消去している ③情報の場合はパスワード設定、暗号化などによる保護、紙の場合は施錠した場所での保管、また廃棄時には消去しており、その実施状況をチェックしている ④情報の場合はパスワード設定、暗号化などによる保護、紙の場合は施錠した場所での保管、また廃棄時には消去し、その実施状況をチェックしており、かつ定期的に保護の方法について見直している		
28	電子メール				○	○	○	○		A.10.8.4 電子的メッセージ通信	①電子メールに重要な製造情報を書いてしまい、盗聴者に情報が漏洩してしまう	電子メール送信に含まれる重要情報は、添付ファイルも含め適切に保護していますか？	①何も対策をおこなっていない ②重要情報はメールでは送信しない、あるいはパスワードで保護したファイルを添付し、パスワードはメール以外の別の手段(例：電話)で相手に伝達している ③重要情報はメールでは送信しない、あるいはデータか通信の暗号化をおこなっている(暗号鍵は適切に管理している) ④重要情報はメールでは送信しない、あるいはデータか通信の暗号化をおこなっている(暗号鍵は適切に管理している)、また定期的に運用・保護方法の見直しをおこなっている		
29	オンライン取引				○	○	○	○	○	A.10.9.2 オンライン取引	①平文で取引情報を通信しているため、取引情報が盗聴者に漏えいしてしまう ②平文で取引情報を通信しているため、盗聴者が情報を盗み、改ざんした情報を取引先に送信する	オンライン取引(EDI=商取引に関する情報を、企業間で電子的に交換する仕組)に含まれる情報は，情報漏洩、改ざん、不正アクセスから保護していますか？	①何も対策をおこなっていない ②ID・パスワードで利用者の認証をおこなっており、通信の暗号化もおこなっている ③通信の暗号化をおこなっており、電子署名も利用している ④通信の暗号化をおこなっており、電子署名も利用している。また定期的に保護方法の見直しをおこなっている	□	□
30	インターネット販売				○	○	○	○	○	A.10.9.1 電子商取引	①平文で販売情報を通信しているため、販売情報が盗聴者に漏えいしてしまう ②ID・パスワードを平文で通信しているため、第三者にID・パスワードが漏えい、そのID・パスワードでサイトにログインされてしまう ③DoS攻撃され、販売サイトが利用できなくなる	インターネットを経由する電子商取引(自社サイトによる消費者への販売、Yahoo, 楽天等を利用した消費者への販売)に含まれる情報は，不正行為，なりすまし，不正アクセス、改ざん及び否認から保護していますか？	①何も対策をおこなっていない ②ID・パスワードで利用者の認証をおこなっており、通信の暗号化もおこなっている ③通信の暗号化をおこなっており、信頼できる認証局で発行された証明書も利用している ④通信の暗号化をおこなっており、信頼できる認証局で発行された証明書も利用している。また定期的に保護方法の見直しをおこなっている	□	□
31	ホームページ				○	○	○	○	○	A.10.9.3 公開されている情報	①不完全なアクセス制御のため、ホームページの内容が改ざんされてしまう ②DoS攻撃され、利用者がホームページにアクセスできなくなる	認可されていない変更を防止するために、ホームページ上の情報は保護していますか？	①何も対策をしていない ②アクセス制御を施しているが、定期的なセキュリティホールへの対策はおこなっていない ③アクセス制御を施し、定期的にセキュリティホールへの対策をおこなっている ④アクセス制御を施し、定期的にセキュリティホールへの対策をおこなっている。また定期的に保護方法の見直しをおこなっている	□	□

情報セキュリティチェックシート

No.	キーワード	対象					影響			付属書A他	トラブル事象例	質問	回答選択肢	業務委託で対応されている場合は□にチェックをいれて下さい	質問に該当しない場合は□にチェックをいれて下さい
		クライアント	ネットワーク	サーバ	アプリ	データ	機密性	完全性	可用性						
32	監査ログ	○	○	○	○	○	○	○		A.10.10.1 監査ログ取得 A.10.10.2 システム使用状況の監視 A.10.10.3 ログ情報の保護 A.10.10.4 実務管理者及び運用担当者の作業ログ A.10.10.6 クロックの同期 A.13.2.3 証拠の収集	①情報漏えい事故発生時、原因の特定ができない、またそのことにより再発防止が打てない ②情報漏えい事故発生時、説明責任が果たせない	管理者、利用者の活動及び情報セキュリテ事象を記録した監査ログを取得・保護していますか？	①監査ログを取得していない ②監査ログを取得・保護しているが、実際に監査していない ③監査ログを取得・保護し実際に監査している ④監査ログを取得・保護し実際に監査しており、監査結果から業務の見直し改善をおこなっている	□	□
33	障害ログ	○	○	○	○				○	A.10.10.5 障害のログ取得	生産管理システムの障害時、障害ログを残していないため根本原因が追求できない	障害ログを取得し、分析すると共に障害に対する適切な処置を取っていますか？	①障害ログを取得していない ②障害ログは取得しているが、分析はおこなっていない ③障害ログを取得し、分析はおこなっているが、障害に対する適切な処置を取っていない ④障害ログを取得し、分析し、障害に対する適切な処置を取っている	□	□
34	バックアップ	○	○	○	○	○			○	A.10.5.1 情報のバックアップ	品質管理システムの障害時、データを破壊してしまい、品質データを復旧できなくなる	クライアント、サーバ、ネットワーク、アプリケーション及びデータのバックアップはバックアップポリシー(バックアップの頻度、バックアップ方法、メディアの保存方法・期間、リカバリ方法、バックアップ内容の確認方法等)に基づきおこなっていますか？	①バックアップをおこなっていない ②バックアップはおこなっているが、バックアップポリシーは無い ③バックアップポリシーに基づいたバックアップをおこなっている ④バックアップポリシーに基づいたバックアップをおこなっており、定期的にバックアップポリシーを見直している	□	□
35	性能管理	○	○	○	○				○	A.10.3.1 容量・能力の管理	生産ラインの増設時、生産管理システムの能力を超えシステムを使用してしまいシステム障害に至る	要求されたシステム性能を満たすために，資源(ディスク容量、CPU、メモリ容量、ネットワーク帯域等)の利用を監視・調整し，システム利用環境に応じた容量・能力を予測・計画をしていますか？	①システムの資源監視・調整をおこなっていない ②システムの資源監視・調整はおこなっているが、それに基づいたシステム利用環境に応じた容量・能力の予想・計画はしていない ③システムの資源監視・調整をおこなっており、それに基づいたシステム利用環境に応じた容量・能力の予想・計画をしている　④システムの資源監視・調整をおこなっており、それに基づいたシステム利用環境に応じた容量・能力の予想・計画をしており、定期的にシステムの監視・調整方法を見直している	□	□
36	リリース管理	○	○	○	○			○	○	A.10.1.4 開発施設、試験施設及び運用施設の分離 A.10.3.2 システムの受入れ	生産管理システムの更新版の受入れ時、テスト無しにシステムを本番稼動させ、その不具合のためシステム障害をおこしてしまう	新しいシステム及びその改訂版・更新版の受入れ基準を確立し，開発中及びその受入れ前に適切なシステム試験を実施していますか？	①システムの受け入れ基準が無く、システムの導入・改定・更新時、適切なシステム試験を実施していない ②システムの受け入れ基準は無いが、システムの導入・改定・更新時、必要に応じてシステム試験を実施している ③システムの受け入れ基準に基づき、システムの導入・改定・更新時、適切なシステム試験を実施している ④システムの受け入れ基準に基づき、システムの導入・改定・更新時、適切なシステム試験を実施しており、定期的に受け入れ基準を見直している	□	□
37	変更管理	○	○	○	○			○	○	A.10.1.2 変更管理 A.12.5.1 変更管理手順 A.12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー A.12.5.3 パッケージソフトウェアの変更に対する制限	変更管理基準が無いため、システム管理者が独断で会計システムのバージョンを期末に上げてしまい、バグのため期末処理が間に合わなくなる	システムの変更の実施は，組織内で承認された変更管理基準の使用によって，管理していますか？	①システムの変更を管理していない ②組織内で承認された変更管理基準はないが、必要に応じシステムの変更管理をおこなっている ③組織内で承認された変更管理基準に基づいて、システムの変更を管理している ④組織内で承認された変更管理基準に基づいて、システムの変更を管理しており、定期的に変更管理基準を見直している	□	□
38	構成管理	○	○	○	○			○	○	システム管理基準 Ⅳ9 構成管理(1)、(2)	構成管理をおこなっていないため、ネットワーク機器の障害時、機器のサポート先が分からず復旧に時間が掛かる	管理すべき、ソフトウエア、ハードウエアの対象範囲を明確にし、構成、調達先、サポート条件等を明確にして組織内で承認された管理基準に基づき管理していますか？	①構成管理をしていない ②組織内で承認された構成管理基準はないが、必要に応じ構成管理をしている ③組織内で承認された構成管理基準に基づいて、構成管理をしている ④組織内で承認された構成管理基準に基づいて、構成管理をしており、定期的に構成管理基準を見直している	□	□

用語解説（参考）

本情報セキュリティチェックシートは情報セキュリティマネジメントについての要求事項を記載した国際規格である ISO27001 を基礎としつつ、企業の所有する情報資産活用のための安全安心な仕組みづくりを推奨する目的から、システム管理基準を加味して作成致しました。

このため、本チェックシートのアンケートにお答え戴く上で、是非ご理解を深めて戴きたいキーワードについて以下に解説することと致します。

1. 情報セキュリティポリシー

セキュリティポリシーとは､「どのような情報資産を､どのような脅威から､どのように守るかと言った基本的な考え方、情報セキュリティを確保するための体制、運用規程、基本方針、対策基準などを具体的に記載するのが一般的であると定義されています

2. 情報セキュリティと情報資産

本チェックシートにおける情報セキュリティの対象は、企業が保有する情報資産の全てが対象となります。

情報セキュリティの役割は情報資産を「安全に守る」こととされています。情報とは企業の場合、お客様、社員の個人情報や、営業情報、経理情報、設計・製造に係る技術情報、システム情報などであり、これらは、企業の業務上において価値を生み出す根源となる事から、情報資産と言われます。

技術ノウハウの様に競合他社が欲しがるものは勿論の事、自社で価値ある情報と思っていなくとも競合他社にとっては価値ある情報である場合や、逆に他社にとって価値ある情報でなくとも、自社の業務において必要不可欠であれば、それは自社にとって、重要な情報資産となります。

情報を保存している情報システム、情報を作成するソフトウェアやメモ、社員の会話や個人の記憶も情報資産となる場合があります。

企業にとって、情報資産の意味するものは幅広く、その価値にも大きな違いがあることから、情報資産の把握と分類を企業の実情にそって適切に管理統制することが大変重要です。

3. 機密性、完全性、可用性について

国際標準では、情報セキュリティを「情報システムに依存するものを機密性、完全性、可用性の欠如に起因する危害から保護すること」と定義しています。機密性、完全性 可用性は、CIA と呼ばれ、情報セキュリティを考える上で重要な概念とされ、情報セキュリティの３要素と呼ばれています。

・機密性（Ｃ：Confidentiality）

情報の利用を許可された人だけが情報を使う事が出来るようにする事。たとえば、情報を見る権限のある人にしか見る事が出来ない様にす

る事です。

・完全性（I:Integrity）

情報および情報の処理方法が正確であり、完全であるようにする事。たとえば、情報が改ざんされたり、情報システムが勝手に変更されない様にする事であり、情報処理方法の正確さとは、情報が誤って削除されたり変更されたりする事が無いようにする事です。

・可用性（A:Availability）

情報の利用を許可された人が、必要なときにはいつでも情報や情報システムを利用出来るようにすること。

たとえば、自然災害やシステムダウンにより、情報を利用する事が出来なくなる事を防ぐ事です。

4. 責任の明確化、職務の分離　並びに情報資産管理台帳について

情報セキュリティの基盤となるのが「責任の分担」「職務の分離」「情報資産管理台帳」です。財務情報だけでなく、すべての情報管理において説明責任を明確にするには、業務プロセスとリスクに応じた「責任の明確化」「職務の分離」、それらに対応した「情報資産管理台帳」の作成・維持が必要となります。

不正行為が行われても、誰もその事実に気が付かず、貴重な情報資産の流出や改ざんといった不利益をまねく事が無い様に、誰がどのような責任を持つべきか、どのようにして責任を果たす為の仕組みを作るべきかが、経営者に求められる大きな責任です。

①　責任の明確化

本チェックシートでは、情報システムの管理及び利用に関して、情報セキュリティの機密性・完全性・可用性の観点から、経営陣、情報システムに携わる部門、利用部門各自の役割を明確に定め責任を割り当てる事を推奨しています。

経営者は情報セキュリティの方向性を定め、情報漏えいなどの事件、事故が 発生した場合の責任を負います。システム管理者は、事件・事故が発生しにくい仕組みを作るために、例えばユーザが簡単なパスワードで情報システムにログインしないための仕組みなどを作る責任があり、利用者は情報システムを正しく使う責任があります。

②　職務の分離

本チェックシートでは、情報システムに携わる部門における管理対象ごとの職務の分離と承認者・実務担当者の分離を推奨しており、チェック機能の最大化と共に、業務の効率性を求めています。

製造業が業務プロセスに応じて、設計担当者、製造担当者、検査担当者の役割を分離するように、情報システムの管理においても、ネットワーク管理者、サーバ管理者、データベース 管理者、アプリケーション

管理者等の役割の分離が必要です。職務を分離することにより、重要な情報資産の不正使用や誤った作業(オペレーション)によるシステム障害のリスク低減が期待できます。

更に、それぞれの職務において、実際に作業を担当する者とその作業を承認する者を分離することが必要です。

実際に職務を分離することが難しい中小企業においても、分離しないことによるリスクが存在することを正しく認識し、そのリスクを低減するために、例えば、業務を兼務する者の作業ログをシステム的に取得するなどの、代替処置が必要になります。

③　情報資産管理台帳

社内の重要な情報資産を洗い出します。ここで言う情報資産とは、

ア.　電子データ、書類などの情報

イ.　業務ソフトウエア、Windows などのソフトウエア

ウ.　サーバ、PC、ネットワーク機器などのハードウエア

エ.　電源、空調などのユーティリティ、サービス

などが対象となります。

また資産管理台帳にはそれぞれの情報資産の重要度、情報資産に対し誰がその資産の管理責任者か、誰がその資産を利用できるか、を記載する必要があります。

情報資産管理台帳サンプルを添付しますのでご参照ください。

情報資産管理台帳を作成することは大変な労力を必要としますが、重要な情報資産を明確にすることにより、セキュリティのための投資・対策にメリハリをつけ、無駄な投資・対策を防ぐことができます。

３．情報セキュリティ対策ベンチマークとの比較

情報セキュリティチェックシート ＶＳ．情報セキュリティ対策ベンチマーク

No	ベンチマーク	No	ＪＮＳＡチェックシート
1 組	情報セキュリティポリシーや情報セキュリティ管理に関する規定を定め、それを実践していますか。	1 組	（情報セキュリティ方針） セキュリティを考慮した情報システムの利用・活用方針を明確にしていますか？
2 組	経営層を含めた情報セキュリティの推進体制やコンプライアンスの推進体制を整備していますか。 ・経営層のリーダシップ ・各部署の活動を調整する組織整備 ・各担当者の権限・責任の明文化 ・遵守すべき法令の正確性・網羅性 ・説明責任を果たす記録整備・保存 ・リソースの分配	2 組	（責任の明確化） 情報システムの利用及び情報セキュリティの推進において、自組織における経営陣・各部署の代表者、各自の職務の使命、責任を明確にしていますか？
		3 組	（職務の分離） 情報システムに携わる部門は、組織の規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にしていますか？
5 組	外部組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか ・委託業務契約書には、業務内容・サービスレベル・安全管理・機密保持責任を明確化 ・委託業務の実施報告・記録確認	4 組	（委託先の管理） セキュリティを考慮した委託先選定の基準（委託先がシステムの管理方法の基準を持っているか、重要データの管理基準を持っているかなど）がありますか？
3 組	重要な情報資産（情報及び情報システム）をその重要性のレベル毎に分類、更にレベルに応じた表示や取扱をする為の方法を定めていますか。 ・ＣＩＡ視点での重要度分類 ・情報資産を利用できる部署・従業者の範囲を定め・明文化 ・情報には紙媒体も含む事。	5 組	（情報資産管理台帳） 情報資産管理台帳を作成していますか。台帳には保有者、利用範囲、重要度、保管場所の記載があり、情報資産の利用範囲は機蜜性・完全性に加えて、可用性も検討されていますか？（不必要に過度な制限を設けていませんか？

No	ベンチマーク	No	ＪＮＳＡチェックシート
4 組	**重要な情報**（例えば、個人データや機密情報など）については、入手・作成・利用・保管・交換・提供・消 去・破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか ・業務プロセス毎の作業責任者や作業手順の明確化、取扱者の限定 ・処理のアクセス記録や確認・保管	6 組	（文書化された手続き） 情報システムの管理、利用に関する組織内で承認された文書化された手続き（ネットワーク管理者マニュアル、サーバ管理者マニュアル、各システムの管理者マニュアル、ユーザマニュアル、データ取り扱いマニュアル等）がありますか？
7 組	経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取り組みや関連規程類について計画的な教育や指導を実施していますか。	7 組	（ルール） 情報システム、組織に関する遵守すべき法令を反映したルールを文書化し、関係者に周知徹底（教育を含む）していますか？
6 組	従業者（派遣を含む）に対し、採用・退職際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。	8 組	（秘密保持） 組織の内部・外部にかかわらず、関係者と、情報保護に対する組織の適切な管理策を反映した覚書または契約を締結していますか？
8 物	特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。 ・特にセキュリティを強化したい物理的区域を定め、この区域の内外において順守すべきセキュリティ上の規定を整備しているか。 ・各種保安設備の設置基準の作成	9 物	（ゾーン管理） アクセスコントロールポリシー（例 情報資産管理台帳の利用範囲に基づく方針）に基づいたオフイス、部屋及び建物に対する物理的セキュリティを設計・ゾーン管理（例；サーバールームの設置、重要な情報資産を扱う作業場所の設置）し、適用していますか？
10 物	重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか		
9 物	顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様な人々についてセキュリティ上のルールを定め、それを実践していますか	10 物	（入退管理） 情報及び情報処理施設のある領域を保護するために、（社員通用、お客様用、搬入用などそれぞれに）入退管理をしていますか？

No	ベンチマーク	No	ＪＮＳＡチェックシート
23 技 障害対応	万が一システムに障害が発生しても必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合を予め想定した適切な対策を実施していますか。 ・システムの可用性要求事項明確化 ・可用性に対応した適切な障害対策 （対応手順・処理実施要領） ・障害部分の切離し、縮退運転機能 ・システムの二重化、バックアップ ・サービスレベルの維持（外部委託先） （最低限の運用時間帯・許容停止時間	11 組	（サービスレベルの確保；内部） 組織の内部（情報システムに携わる部門）・外部（ベンダー、保守業者等）に拘わらず、情報サービスの提供・利用に関して、重要な要求事項（例：専用回線の障害時の復旧時間帯等）を反映したサービスレベルを取り決めていますか？
		12 組	（サービスレベルの確保；外部） 組織の外部（システムベンダー等）と、システム運用（保守サービス、ヘルプデスクサービス、 セキュリティサービス等）に関して重要な要求事項（例：稼働率、障害時復旧時間、システム応答時間、電話応答時間、回答時間等）を反映したサービスレベルの取り決めをしていますか？
		17 組	（情報システム監査） 情報システム監査をしていますか？
		34 技	（バックアップ） クライアント、サーバ、ネットワーク、アプリケーション及びデータのバックアップはバック アップポリシー（バックアップの頻度、バックアップ方法、メディアの保存方法・期間、リカバリー方法、バックアップ内容の確認方法等）に基づき行っていますか？

No	ベンチマーク	No	ＪＮＳＡチェックシート
22 技 ソフトウェア購入・開発	ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセス毎に実施するなど、適切なプロセス管理を実施していますか。 ・ソフトウェア導入・変更手順整備 ・ソフトウェア導入前の評価 ・ソースコードへのアクセス制限 ・構成変更に関する手順書整備 ・不正プログラムのチェック機能 ・外部委託先への管理 （委託契約書へのセキュリティ要件記載・委託先セキュリティ管理実施状況確認）	13 組	（ソフトウェアの選別と開発） 経営陣はパッケージソフトウェアの採用とソフトウェアの開発に関する明確な基準を定めていますか？（標準化された業務にはパッケージソフトウェアの採用を検討し、差別化された、あるいは競争力のある業務は開発を行うなどの基準） ・経営陣の承認
21 技 業務システム開発	業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。 ・セキュリティ要求事項を仕様書化 （利用者・権限区分・複数の業務フロー交差、扱うデータや文書の種類） ・入出力データのチェック機能 （要求・条件に合わない入力の制限） ・情報の保護機能 （利用者毎の読み書き・削除の制限）	14 組	（業務データの管理） 入力・出力データの完全性（データの妥当性など）と安全性（情報漏えい対策など）を管理する手続きまたは仕組み（システム的対策）がありますか？
24 技 事件・事故対応	情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。 ・組織的な対応と体制整備 ・実施要領の存在 ・対応要領（事件・事故の形態ごと） （リスクコミュニケーションなど）	15 組	（障害報告） 情報システムの運用において障害・事件・事故は、規模にかかわらず、適切な管理者へ、できるだけ速やかに報告していますか？

No	ベンチマーク	No	ＪＮＳＡチェックシート
25 技 事業継続	何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できる様になっていますか。（災害を含む情報システム重大事故） ・自組織の業務へのリスクアセスメント実施 ・バックアップセンター確保・運用 ・手作業での業務処理要領整備	16 組	（障害対策） 地震等の災害を含めた障害時の情報システムに与える影響範囲、被害及びリスクを明確にし、それに基づいた復旧・対応計画を策定していますか？
18 技 アクセス制御	情報（データ）や情報システムへのアクセスを制限するために、利用者ＩＤの管理、利用者の識別と認証を適切に実施していますか？ ・利用者ＩＤの管理 （規定の整備、不要なＩＤの削除、共用ＩＤ利用制限、単純なパスワードの設定禁止） ・利用者の識別と認証	18 技	（ＩＤ） 情報システムの利用時に、利用者固有のＩＤを割り当てていますか？ （共有ＩＤの利用制限、不要なＩＤ削除）
		19 技	（パスワード） パスワードポリシー（例；パスワードは８文字以上で、英数字混在の類推しにくいものとする。パスワードは６か月毎に変更し、３世代前までと同じものを使う事ができない。）に基づいてパスワード管理をしていますか？
19 技 アクセス制御	情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。 ・アクセスを管理する方針 ・利用者の限定 （データ・情報システム・業務アプリケーション、サービスの利用者毎の設定） ・利用できる機能の制限 （役職上の権限に合わせた利用権限付与・一度の利用時間の制限） ・定期的なレビュー （職務変更・異動における適切な変更	20 技	（アクセス制限） 管理者、利用者に対し、アクセスコントロールポリシーに基づいてアクセス制御を行っていますか？

No	ベンチマーク	No	ＪＮＳＡチェックシート
16 技 運用管理	通信ネットワークを流れるデータや公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。 ・外部→内部への通信にＶＰＮ使用 ・重要な情報のＳＳＬによる暗号化 ・アクセス制御ポリシーに沿った認証とセグメント管理 ・重要なメールにおける添付ファイル、メッセージの暗号化 ・無線ＬＡＮの傍受対策（暗号化）	21 技	（ネットワークアクセス制御;外部） 外部からのアクセスをファイアウオールや不正侵入防御装置（ＩＰＳ）などで制限していますか？ ・ＦＷ、ＩＰＳによるアクセス制限 ・アクセスログのチェック
		22 技	（ネットワークアクセス制御：無線ＬＡＮ） 無線ＬＡＮは認証、暗号化を実施し、安全に利用していますか？
		23 技	（ネットワークアクセス制御：内部） 社内においても重要情報はセグメント分割し、他からアクセス出来ないように保護していますか？
20 技 ＮＷアクセス制御	ネットワークのアクセス制御を適切に実施していますか。 ・ネットワークの分割 ・外部からの内部への接続時認証 （利用者認証・端末機器認証） ・許可されていないワイヤレスアクセスポイントの設置禁止 ・公衆無線ＬＡＮサービス利用に対するセキュリティ対策 ・検疫	24 技	（ネットワークアクセス制御：サーバ） サーバのＴＣＰ/ＵＤＰポート、サービスなどへのアクセスを制御していますか？
		28 技	（電子メール） 電子メール送信に含まれる重要情報は、添付ファイルも含め、適切に保護していますか？ 本文は適切に保護していますか？ ・不正プログラム対策 ・通信の暗号化 ・パスワードによる保護 ・添付ファイルの暗号化
		29 技	（オンライン取引） オンライン取引(EDI=商取引に関する情報を、企業間で電子的に交換する仕組み)に含まれる情報は、情報漏洩、改ざん、不正アクセスから保護していますか？ ・利用者認証（ＩＤ、パスワード） ・通信の暗号化 ・電子署名

		30 技	（インターネット販売） インターネットを経由する電子商取引（自社サイトによる消費者への販売、Yahoo、楽天等を利用した消費者への販売）に含まれる情報は、不正行為、なりすまし、不正アクセス、改ざん及び否認から保護していますか？ ・利用者認証、通信の暗号化 ・認証局による証明書利用
		31 技	（ホームページ） 認可されていない変更を防止するために、ホームページ上の情報は保護していますか？ ・アクセス制御 ・定期的なセキュリティホール対策
14 技 運用管理	不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウェアなど）への対策を実施しているか。 ・ウイルス対策ソフトの導入 （ゲートウェィ型、フアイル監視型ソフト） ・パターンフアイルの適時更新 ・検疫処理（モバイルＰＣ対策）	25 技	（ウイルス） ＯＳ、アプリ、ミドルウェアなどにパッチを適用していますか？
		26 技	（ウイルス） アンチウイルスソフトでウイルス対策を行っていますか？ ・定期的なスキャンの実施 ・定期的なパターンフアイルの更新
11 物	重要な書類、モバイルＰＣ、記憶媒体などについて適切な管理を行っていますか。 ・行程毎の管理手順・業務実行者の明確化 ・保管キャビネットの施錠 ・プリント出力の放置禁止 ・記憶媒体の粉砕廃棄	27 技	（ＰＣ・電子媒体・紙の管理） 媒体・ＰＣの利用時または廃棄時において、媒体やＰＣに格納された情報に対し、漏洩対策を実施していますか？ ・パスワード設定・暗号化による情報保護 ・廃棄時における消去・実施確認
17 技 運用管理	モバイルＰＣやＵＳＢメモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。 ・データとＰＣの分離（規定化） ・利用者ＩＤ、パスワード、暗号化		

No	ベンチマーク	No	ＪＮＳＡチェックシート
13 技 運用管理	情報システムの運用に際し必要なセキュリティ対策を実施しているか。 ・各種手順書（マニュアル）の作成 ・ルールに従った運用 ・監視、ログの取得と分析 ・安定稼働の為の性能管理 ・時刻同期	32 技	（監査ログ） 管理者、利用者の活動及び情報セキュリティ事象を記録した監査ログを取得・保護していますか？
		33 技	（障害ログ） 障害ログを取得し、分析すると共に、障害に対する適切な処置を取っていますか？
		35 技	（性能管理） 要求されたシステム性能を満たすために、資源（ディスク容量、ＣＰＵ、メモリ容量、ネットワーク帯域等）の利用を監視・調整し、システム利用環境に応じた容量・能力を予測・計画をしていますか？
12 技 運用管理	情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配意していますか。 ・開発・テスト環境と運用環境分離 ・性能管理・変更管理の実施 ・システム受入れ時の十分なテスト ・開発での本番データの使用制限	36 技	（リリース管理） 新しいシステム及びその改訂版の受け入れ基準を確立し、開発中及びその受け入れ前に適切なシステム試験を実施していますか？
15 技 運用管理	導入している情報システムに対して適切な脆弱性対策を実施していますか。 ・脆弱性・脅威情報の定期的収集 ・Ｖｅｒ管理、構成管理、変更管理 （定期的な設定の入れ替え実施） ・不要なサービスの停止 ・組織内標準システムの採用	37 技	（変更管理） システムの変更の実施は、組織内で承認された変更管理基準の使用により、管理していますか？
		38 技	（構成管理） 管理すべきソフトウェア、ハードウェアの対象範囲を明確にし、構成、調達先、サポート条件等を明確にして正式な管理基準に基づき管理していますか?

＊情報セキュリティ対策ベンチマーク　http://www.ipa.go.jp/security/benchmark/

情報資産管理台帳

御社名：

※ 差し支えなければご記載ください。

管理No	情報資産名	対象（媒体）	保管・格納場所	利用範囲	管理部門情報			台帳登録日	廃棄日	保存期間	最終棚卸し日	影響度			備考
					管理責任部門名	管理責任者	連絡先					機密性	完全性	可用性	
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															

◆ ご記入いただいた内容につきましては、ものづくり企業の情報セキュリティ対策推進における現状・課題の分析のための資料とさせていただくためのもので、その統計結果を報告書にまとめる予定です。
個別の内容を公開することは一切ございません。また、報告書完成後は適切に破棄致します。

◆ 「情報資産管理台帳」に書き出す事が出来なかった場合は、お手数ですが、別紙アンケートのみでもご提出いただけると幸いです。

情報資産管理台帳サンプル(金型)

管理No	情報資産名	対象(媒体)	保管・格納場所	利用範囲	管理部門情報			台帳登録日	廃棄日	保存期間	最終棚卸し日	影響度			備考
					管理責任部門名	管理責任者	連絡先					機密性	完全性	可用性	
記入要綱	別紙「情報資産分類」を参考に記入 情報資産例より細かくても、それらを組み合わせたものでも良い、管理する単位で洗い出すこと	情報資産が情報の場合、情報が保存された状態あるいは保存されている媒体を記入 例) ・紙 ・設計製造システム ・CD－R ・ファイルサーバ 等	情報資産が保管・格納される場所を記入 例) 情報の保管場所がサーバ、PCの場合 ・ホスト名を記入、 紙の場合 ・ロッカー ・キャビネット 等	情報資産の利用範囲を記入 ・全社 ・部内 ・課内 ・グループ内 ・XXプロジェクト内 ・幹部社員内 等		情報資産の実際の管理責任部門名、管理責任者、連絡先(内線、外線、ﾒｰﾙｱﾄﾞﾚｽ)を記入		情報資産の本台帳への登録日を記入	情報資産を廃棄する場合、廃棄した日を記入(初回記入時は空白)	登録日に情報資産の保存期間を記入 特に情報の場合、法令や契約を考慮して記入すること	情報資産の棚卸しを最後にした日を記入(初回記入時は現在の日にち)			別紙「CIA影響度」を参考に情報資産が情報か情報以外かに注意して影響度を記入	
記入例															
1	要求仕様書	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
2	構想図面	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		5年	2008/8/26	2	3	3	
3	承認図	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
4	設計図面データ	設計製造システム	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
5	設計図面	紙	鍵つきキャビネット	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
6	部品図	紙	鍵つきキャビネット	設計部門	設計部門	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
7	加工データ	設計製造システム	サーバルーム	製造部門	製造部門	製造部長	内線:4444	2008/8/26		永久	2008/8/26	2	3	3	
8	加工図面	紙	鍵つきキャビネット	製造部門	製造部門	製造部長	内線:4444	2008/8/26		1年	2008/8/26	2	3	3	
9	購買情報 (取引先/コスト/納期情報)	ファイルサーバ	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		1年	2008/8/26	2	3	3	
10	購買情報 (取引先/コスト/納期情報)	紙	鍵つきキャビネット	設計部門	設計部門	設計部長	内線:1111	2008/8/26		1年	2008/8/26	2	3	3	
11	設計製造システム	－	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		－	2008/8/26	2	3	3	
12	製造ネットワーク(DNC)	－	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		－	2008/8/26	2	3	3	
13	ファイルサーバ	－	サーバルーム	設計部門	設計部門	設計部長	内線:1111	2008/8/26		－	2008/8/26	2	1	1	
14	ノートPC	－	オフィス内個人キャビネット	営業部、品質管理部	情報システム部	情報システム部長	内線:3333	2008/8/26		－	2008/8/26	2	1	1	
15	会計情報	ファイルサーバ	MAIN(サーバ名)	経理部	経理部	経理部長	内線:2222	2008/8/26		5年	2008/8/26	2	3	2	
16	営業秘密情報	ファイルサーバ	オフィス内営業部キャビネット	営業部	営業部	営業部長	内線:5555	2008/8/26		10年	2008/8/26	3	3	2	
17	MS Officeライセンス	紙	サーバルーム キャビネット	全社	情報システム部	情報システム部長	内線:3333	2008/8/26		5年	2008/8/26	1	1	1	

情報資産管理台帳サンプル(靴)

管理No	情報資産名	対象(媒体)	保管・格納場所	利用範囲	管理部門情報			台帳登録日	廃棄日	保存期間	最終棚卸し日	影響度			備考
					管理責任部門名	管理責任者	連絡先					機密性	完全性	可用性	
記入要綱	別紙「情報資産分類」を参考に記入 情報資産例より細かくても、それらを組み合わせたものでも良い、管理する単位で洗い出すこと	情報資産が情報の場合、情報が保存された状態あるいは保存されている媒体を記入 例) ・紙 ・生産管理システム ・CD－R ・ファイルサーバ 等	情報資産が保管・格納される場所を記入 例) 情報の保管場所がサーバ、PCの場合 ・ホスト名 を記入、 紙の場合 ・ロッカー ・キャビネット 等	情報資産の利用範囲を記入 ・全社 ・部内 ・課内 ・グループ内 ・XXプロジェクト内 ・幹部社員内 等		情報資産の実際の管理責任部門名、管理責任者、連絡先(内線、外線、ﾒｰﾙｱﾄﾞﾚｽ)を記入		情報資産の本台帳への登録日を記入	情報資産を廃棄する場合、廃棄した日を記入(初回記入時は空白)	登録日に情報資産の保存期間を記入 特に情報の場合、法令や契約を考慮して記入すること	情報資産の棚卸しを最後にした日を記入(初回記入時は現在の日にち)	別紙「CIA影響度」を参考に情報資産が情報か情報以外かに注意して影響度を記入			
記入例															
1	デザイン仕様書	紙	鍵付きキャビネット	設計部	設計部	設計部長	内線:1111	2008/8/26		5年	2008/8/26	2	3	3	
2	生産管理システム (デザイン管理) 型紙	生産管理システム	サーバルーム	設計部	設計部	設計部長	内線:1111	2008/8/26		5年	2008/8/26	2	3	3	
3	生産管理システム (デザイン管理) 型紙	紙	鍵付きキャビネット	設計部	設計部	設計部長	内線:1111	2008/8/26		5年	2008/8/26	2	3	3	
4	生産管理システム (製造管理)製品サンプル	生産管理システム	鍵付きキャビネット	設計部	設計部	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
5	販売管理システム (取引先・コスト等の販売情報)	販売管理システム	サーバールーム	設計部	設計部	設計部長	内線:1111	2008/8/26		永久	2008/8/26	2	3	3	
6	ネットワーク	社内ネットワーク図	サーバルーム	設計部	設計部	設計部長	内線:1111	2008/8/26		－	2008/8/26	2	3	3	
8	ファイルサーバ	社内ネットワーク図	サーバルーム	設計部	設計部	設計部長	内線:1111	2008/8/26		－	2008/8/26	2	1	1	
9	ノートPC	PC管理一覧表	オフィス内個人キャビネット	営業部、 品質管理部	情報システム部	情報システム部長	内線:3333	2008/8/26		－	2008/8/26	2	1	1	
10	会計情報	ファイルサーバ	MAIN(サーバ名)	経理部	経理部	経理部長	内線:2222	2008/8/26		5年	2008/8/26	2	3	2	
11	営業秘密情報	ファイルサーバ	オフィス内営業部 キャビネット	営業部	営業部	営業部長	内線:5555	2008/8/26		10年	2008/8/26	3	3	2	
12	MS Officeライセンス	紙	サーバルーム キャビネット	全社	情報システム部	情報システム部長	内線:3333	2008/8/26		5年	2008/8/26	1	1	1	

CIA影響度

情報

機密性例

影響度	クラス	説明
1	公開	第三者に開示・提供可能
2	社外秘	特定の関係者または部署のみ利用可能
3	関係者外秘	特定の関係者または部署のみに開示・提供可能

完全性例

影響度	クラス	説明
1	低	情報の内容を変更された場合、ビジネスへの影響は少ない
2	中	情報の内容を変更された場合、ビジネスへの影響は大きい
3	高	情報の内容を変更された場合、ビジネスへの影響は深刻かつ重大

可用性例

影響度	クラス	説明
1	低	利用不可能な場合、ビジネスへの影響は少ない
2	中	利用不可能の場合、ビジネスへの影響は大きい
3	高	利用不可能の場合、ビジネスへの影響は深刻かつ重大

情報以外（サーバ、クライアント PC、ネットワーク機器、アプリケーション他）

機密性例

影響度	クラス	説明
1	公開	組織内外で利用可能
2	社外秘	組織内のみ利用可能
3	関係者外秘	特定の関係者または部署のみ利用可能

完全性例

影響度	クラス	説明
1	低	正常に動作しない場合、ビジネスへの影響は少ない
2	中	正常に動作しない場合、ビジネスへの影響は重大
3	高	正常に動作しない場合、ビジネスへの影響は非常に深刻かつ重大

可用性例

影響度	クラス	説明
1	低	1日の情報システムの停止が許容される
2	中	業務時間内の利用は保障する 1時間の情報システムの停止が許容される
3	高	365日24時間のうち99%以上利用できることを保障する

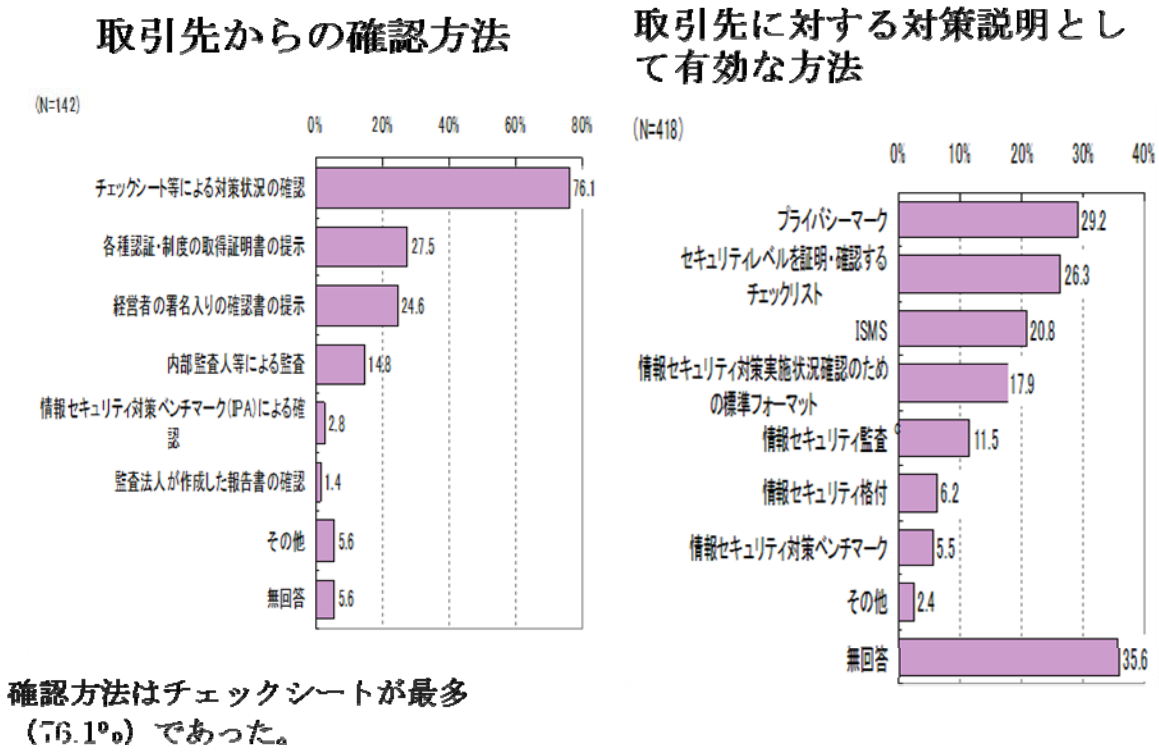
機密性：アクセスを認可された者だけが情報にアクセスできることを確実にすること
　　情報を漏えいや不正アクセスから保護すること
完全性：情報及び処理方法が、正確であること及び完全であることを保護すること
　　情報の改ざんや間違いから保護すること
可用性：認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること
　　情報の紛失・破損やシステムの停止などから保護すること

付録・参考文献

＊１．NPO 日本ネットワークセキュリティ協会（JNSA）
協会公式サイト　http://.jnsa.org/

＊２．中小企業向け個人情報保護対策チェックシート集計結果
協会公式サイト http://.jnsa.org/の成果物２００６年度（2006.12.11）参照

＊３．有効な方法としてのチェックシートの評価
情報セキュリティ対策確認方法
（出典元；ＩＰＡ（中小企業の情報セキュリティ対策に関する研究会報告）



＊４．企業内通信網（LAN）構築率
（出典元；総務省「通信利用動向調査」）

企業規模区分	平成14年	平成15年	平成16年	平成17年
100人～299人	88.4%	90.2%	86.6%	87.6%
300人～499人	93.9%	93.4%	95.3%	90.4%
500人～999人	97.3%	95.2%	98.0%	96.8%
1000人～1999人	98.5%	98.3%	99.0%	97.3%
2000人～2999人	99.3%	97.3%	99.0%	97.7%
3000人～4999人	100.0%	98.2%	98.1%	97.6%
5000人～	100.0%	98.5%	100.0%	96.3%
全体	90.6%	91.6%	89.5%	89.6%

＊５．悪意のある様々な外部からの攻撃やインターネット犯罪の多発
（出典元：警察庁「平成 19 年中のサイバー犯罪の検挙状況」
http://www.npa.go.jp/cyber/statics/h20/pdf39.pdf

＊６．中小企業の規模の定義
●法令上の定義（中小企業基本法第２条第１項）

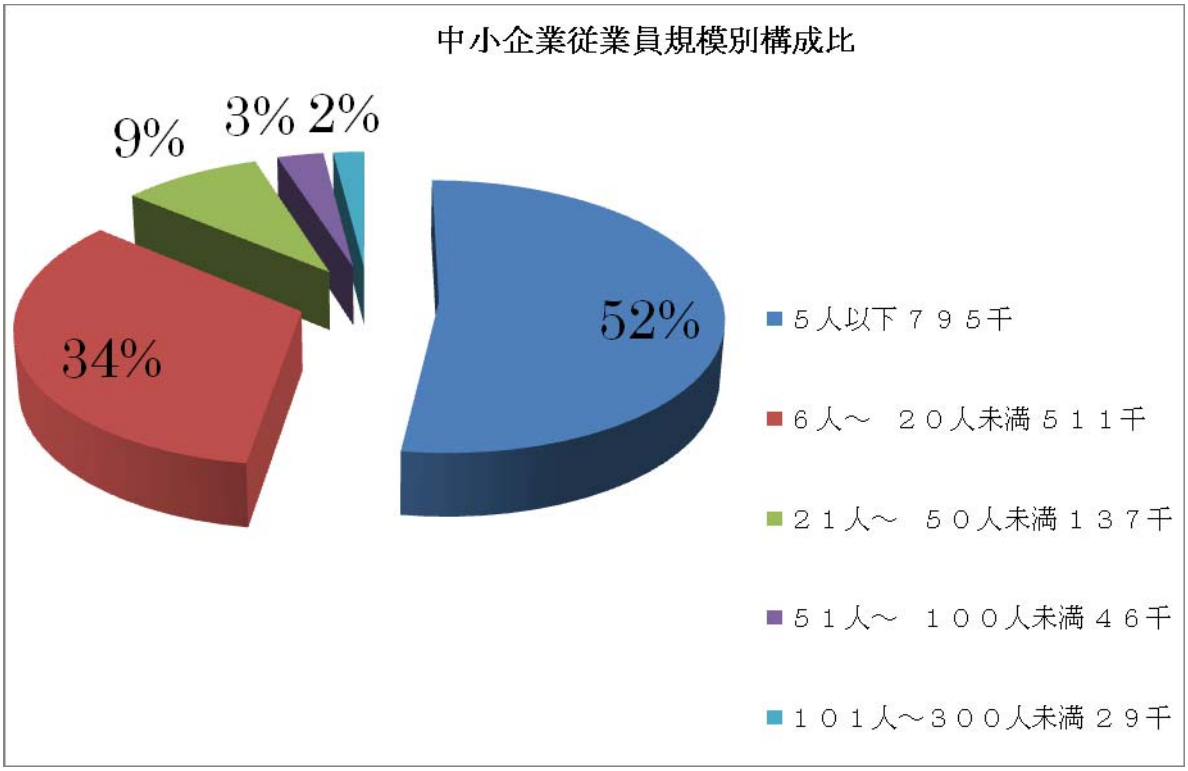
	製造業	卸売業	小売業	サービス業	その他産業
資本金	３億以下	１億以下	５千万以下	５千万以下	３億以下
従業員	３００人以下	１００人以下	５０人以下	１００人以下	３００人以下

＊資本金、従業員のどちらか一方を充足する事が条件。

●政令による定義（中小企業金融公庫法等の中小企業関連立法）
・旅館業　　－－－－－－－－　資本金５千万以下　または　従業員２００人以下
・ソフトウェア業・　　－－　資本金３億円以下　または　従業員３００人以下
　情報処理サービス業

＊７．中小企業規模別構成比
企業の大半を占めるのが中小企業
（出典元；総務省「平成１６年度事業所・企業統計調査」）

・３００人以下事業所の数は全事業所の９９％以上。



＊８．企業版 IT 利活用ステージ評価指標
（出典元；平成１５年度経済産業省発表評価指標）

評価項目	キーワード	ステージ１ IT 初期段階	ステージ２ 部門内最適化	ステージ３ 組織全体最適化	ステージ４ 共同体最適化
組織形態	組織ありきからの脱却	・決算承認に多大な時間を要す	・決済承認のプロセスが簡素化	・組織の階層構造、社内ポストが必要最小限	・企業をまたがったバーチャルな組織がプロジェクトごとに成立
人材 評価制度	企業戦略と整合的な人事制度や評価基準	・過度に固定的人事制度（年功序列、流動性なし等） ・企業戦略と実体的に不整合な人事評価体系、人事システム	部門内での目標管理と実績評価制度	・成果主義に基づく評価基準の明示（スキル標準の策定） ・社内における人材の流動化（スキル転換）	・プロジェクトごとの柔軟な人事政策 ・スキルに応じて外部労働市場を有効活用
教育、構成員のモチベーション	構成員のやる気を引き出す仕組み	・固定的なコミュニケーション ・社員教育制度未実施		・経営者・社員間の垂直方向の円滑・活発なコミュニケーション ・社員スキルの向上を 仕組みで担保（高質の 暗黙知）	
情報共有	オンタイム（即時的）な業績把握と構成員による情報共有	・業績は決算期ごとにしか把握できず ・計画情報（生産、販売）や在庫情報、顧客情報を共有できず	・業績把握は部門内ではオンタイムだが、コーポレートでは決算期ごと ・計画情報、在庫情報は部門内ではオンタイムに把握	・コーポレート全体の業績その他の情報を、経営者まで含めてオンタイムで把握 →経営トップと従業員の情報共有がスムーズに測れる。 →組織階層がフラット化され、顧客ニーズが経営に届きやすい	・バリューチェーンに関わるすべてのプレーヤーと業績その他の情報をオンタイムで共有

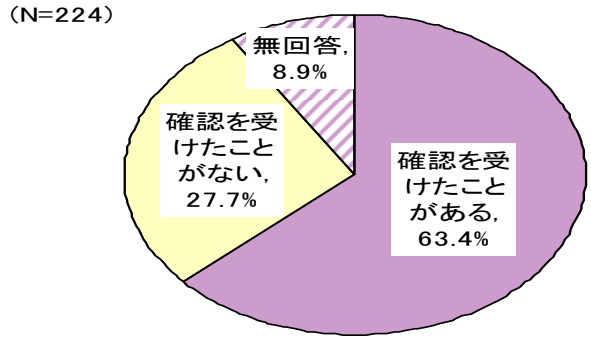
評価項目	キーワード	ステージ１ IT 初期段階	ステージ２ 部門内最適化	ステージ３ 組織全体最適化	ステージ４ 共同体最適化
経営手法 顧客主義	プロダクトアウト（生産主体）からマーケットイン(顧客主体)へ	大量生産型共有体制	ＩＴ活用による需給バランスの調整 多品種少量型供給体制	・ＩＴの活用により顧客ニーズを積極的に経営に反映。 顧客主義に基づくオンデマンド型供給体制	徹底した顧客主義に基づき、企業のフレームを超えた供給体制（コンペティターとの一体供給 複数メーカー製品・サービスのオンデマンドによるバンドル提供
取引関係	バリューチェーンの最適化	取引先が固定化	条件見直しによる取引先の変更	条件見直しによる取引先のダイナミックな変更	バリューチェーンごとの効率化を目指すべく、 企業と取引先との一部融合やシステムの連携を図る。
変化への対応（ＢＰＲ）	変化への対応（柔軟性、迅速性）が 企業成長力への源泉	･変化を受け入れにくい企業体質 ･成功体験や前例への過度の依存 ･従来の業務の単なるシステム化	･部門内においてＩＴによる業務改革の効果（製品としてのＣＲＭ、ＳＣＭ、ＥＲＰの導入） ･他部門とはシステムの流用や共同利用はない	・顧客ニーズの変化（市場の変化）に対し ビジネスプロセスを即時に適応 ・経営の視点からのＩＴ活用（製品としてのＣＲＭ、ＳＣＭ、ＥＲＰの統合化の恩恵） ・業務が独立・モジュール化	・顧客ニーズの変化（市場の変化）に対し、ビジネスプロセスを即時に適応 ・各業務モジュールは独立しており、社内外に関わらずビジネスプロセスに応じ柔軟に組み替え（ウェブサービス・ ＢＰＭ等）
ＩＴ部門の体制（ＣＩＯ）	経営戦略とＩＴ戦略の連携	･社内ユーザー部門のニーズ主導 ･経営戦略とのリンクは薄い ･ベンダー的思考のＣＩＯ		・経営者で能力のあるＣＩＯ ・経営戦略の一環としてのＩＴ投資戦略	

評価項目	キーワード	ステージ１ IT 初期段階	ステージ２ 部門内最適化	ステージ３ 組織全体最適化	ステージ４ 共同体最適化
ＩＴガバナンス	経営戦略に適応したＩＴ投資戦略へ	システムベンダーに 丸投げ	部門単位でのシステム統一	・経営戦略の一環としてのＩＴ投資戦略 ・企業のアイテムを階層化し、システムアーキテクチャーを共通化して管理（統合システムアーキテクチャー）	外部環境の変化に柔軟に適応できるシステム構成
ＩＴ投資効果分析	ビジネスプロセスに基づくＩＴの適用	ＩＴ投資の評価軸がない。	ＩＴ投資に評価がある。（部門ごと）	ＩＴ投資の評価軸がある（エンタープライズアーキテクチャー）	バリューチェーン単位で先行投資（費用）と 再投資の評価軸を設定

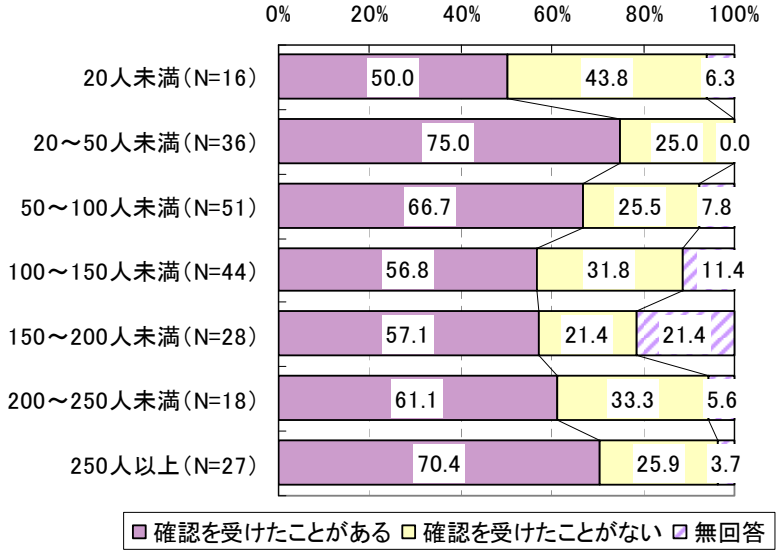
＊９．簡易版セキュリティチェックシート
情報セキュリティ理解度チェック
（出典元：ＪＮＳＡ協会公式サイト「理解度セルフチェック」
http://.jnsa.org/

＊１０．取引先（業務委託元）からの情報セキュリティ対策状況の確認有無

（出典元；ＩＰＡ（中小企業の情報セキュリティ対策に関する研究会報告）



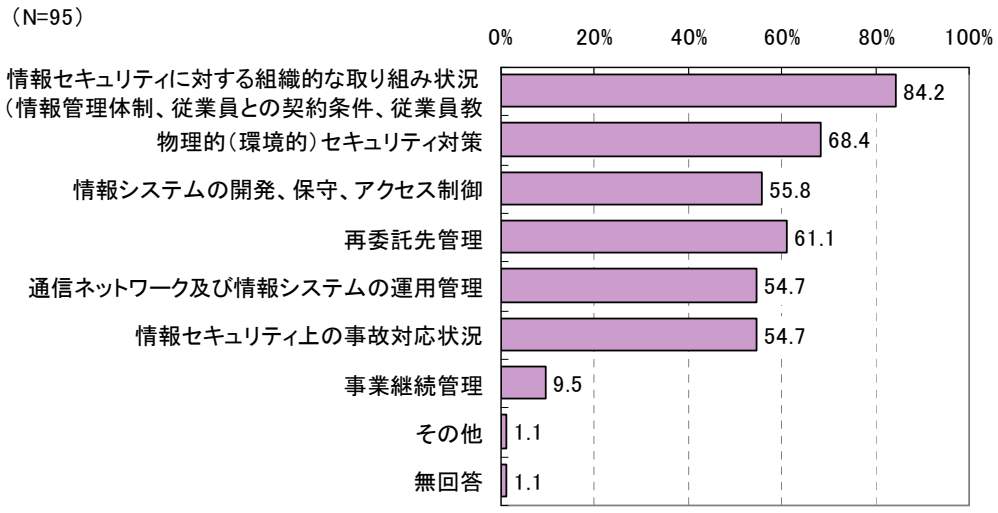
取引先（業務委託元）からの情報セキュリティ対策状況の確認有無



取引先（業務委託元）からの情報セキュリティ対策状況の確認有無（従業員規模別）

＊１１．取引先（業務委託先）に対する大手企業からの要求事項

（出典元；ＩＰＡ（中小企業の情報セキュリティ対策に関する研究会報告）



＊１２．製造ノウハウの流出

（出典元：経済産業省「我が国製造業における技術流出問題に関する実態調査」