寄稿論文

中小企業における情報セキュリティ管理者の必要性とその役割に関する考察

A Study on the necessity of information security administrator and its role for small and medium-sized enterprises

是永逸郎　Itsurou KORENAGA

要　約

情報通信ネットワークが急速に進展し、ネットショッピング等、情報処理技術を活用したビジネスはさらに拡大している。一方、情報漏えい、インターネット上の不祥事など経営上のリスクは増大している。情報セキュリティ対策は中小企業の重要な経営課題の一つとなっている。本稿では、情報セキュリティ対策の中心となる人材、情報セキュリティ管理者の必要性とその役割について考察する。

Abstract

Information and communications network has grown rapidly and business using information technology is expanding, while management risk (information leak, deplorable incident on the internet etc.) is increasing. IT security measures has been one of the most important management issue. This report describes the necessity of information security administrator (human resources to be a center of IT security measures) and its role.

Ⅰ．はじめに

情報通信ネットワークが急速に進展し、ネットショッピング等、情報処理技術を活用したビジネスはさらに拡大を続けている。中小企業においてもビジネスを展開していく上で情報処理技術を活用する場面はますます増加している。一方、情報漏えい、サイバー攻撃、インターネット上の不祥事など、情報処理に係る分野での経営上のリスクは増大しており、情報セキュリティ対策の必要性は高まっている。しかしながら情報セキュリティを維持する、あるいは、向上させるためには様々な費用が発生する。こうしたコストは中小企業にとって大きな問題である。

本稿では中小企業における「情報セキュリティ管理者」の必要性・重要性について論じ、さらには、その役割や求められる技能を定義したい。

企業における情報セキュリティ体制に関する先行研究としては、田中〔2005〕がある。田中は情報セキュリティ体制を構成する人材モデルとして、情報セキュリティ最高責任者(CISO)、情報セキュリティ委員会、情報セキュリティ責任者、情報セキュリティ推進担当者、個人情報管理責任者、個人情報保護責任者、内部監査人、情報システム部門セキュリティ担当の八つに分類している。ここで述べられている人材モデルは明らかに大企業を意識したものであり、中小企業における情報セキュリティ管理を考える場合には、現実的ではない。中小企業においては、これらの人材モデルを担当する人をそれぞれ確保するのは困難であり、一人の担当者がこれら複数の人材モデル、あるいはその一部の役割を兼任することになる。本稿では、中小企業の実態に合った形で、現実的な「情報セキュリティ管理者」の有りようについて論考したい。

中小企業の定義としては、中小企業基本法による中小企業者の範囲[1)]が一般的であるが、本稿では便宜的に従業員数300人以下の企業を中小企業、300人を超える企業を大企業としている。

Ⅱ．中小企業における情報セキュリティ対策の現状

表１は、2014年４月から2016年１月までの間に発生した、中小企業の情報セキュリティ対策にとって重要な出来事を挙げてみたものであ

る。これらの出来事は全て外部要因によるもので、企業は好むと好まざるとに関わらず、対処せざるをえない。

表1．2014年4月以降の中小企業の情報セキュリティ対策にとって重要な出来事

2014年4月1日	消費税8％へ引き上げ
2014年4月8日	暗号通信ライブラリ OpenSSL に情報漏えいの脆弱性が発見
2014年4月9日	Windows XP サポート終了
2014年8月7日	Internet Exlorer の最新版以外のセキュリティサポートを終了と発表
2015年7月15日	Windows Server2003サポート終了
2016年1月1日	マイナンバー制度開始
2016年1月12日	Internet Explorer の最新版以外のセキュリティサポート終了
2016年1月13日	Windows 8 のセキュリティサポート終了（Windows8.1は継続）

出所：筆者作成

2014年4月9日、マイクロソフト社は自社のオペレーティングシステム（以下 OS という）Windows XP のサポートを終了した。マイクロソフト社はサポート終了の1年前から移行支援強化期間として最新 OS への移行を呼びかける啓発活動を行っており、多くの企業では OS の入れ替え、パソコンの入れ替え作業に追われた。

しかしながら、サポート終了後に Windows XP を使い続けている企業も多く存在するとの報告もある。「一般社団法人日本コンピュータシステム販売店協会が発表した IT 利活用動向調査によると、Windows XP を使い続けている企業は、中規模一般企業では19%、小規模一般企業では15%」との調査結果[2]がある。また、アメリカの調査会社 NetMarketShare が公開しているデータによると、サポート終了から約1年8カ月経過した2015年12月時点においても、Windows XP のシェアは10.93%（Net Market Share〔2016〕）となっており、Windows8.1（10.3%）や Windows10（9.96%）を上まわっている。

サポートが終了した OS は、新たな脆弱性が見つかった場合にもソフトウェアの更新がされない。つまり、その脆弱性はいつまでも解消されずに残ったままになるということであり、悪意を持った人間からすれば、恰好のターゲットになる。このようにセキュリティ面での大きな問題があることは明らかであるにも関わらず、新しい OS への移行が進まないのには理由がある。主に以下の3つの理由によるものと考えられる。

（1）人材の問題

新しい OS への移行を計画し、推進・実行することのできる人材がいない。業務でパソコンを使用することはできても、OS を入れ替える、新しいパソコンを購入してデータや環境を移行するとなると、簡単ではない。外部に相談しようにも誰に何を相談すればよいのかわからない。

（2）費用の問題

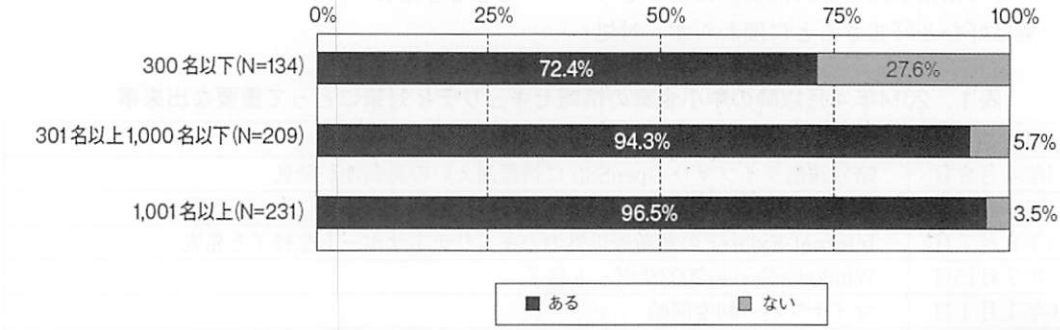
OS を入れ替えるためには新しい OS を購入する必要がある。また、対象のパソコンが古く、新しい OS に対応できない場合、パソコンそのものを買い替える必要がある。企業では複数台のパソコンが使われているため、全てのパソコンを新しい OS にするには多額の費用がかかる。資金力が乏しい中小企業にとっては容易ではない。

（3）ソフトウェアの問題

Windows XP は、2001年の登場以来、世界中の企業で10年以上という長期に渡って幅広く使われてきた OS である。そのため、この OS の上で動作することを前提に作られたソフトウェア資産が多く存在する。これらのソフトウェアが、新しい OS では正しく動作しない、あるいは正しく動作するかどうかわからない、動作保証されないというようなケースがでてくる。そのため、新しい OS に移行しない、移行できない。

この中でも一番の問題は、人材の問題である。中小企業では専任の部署がないところも少なくない。図1は IT 関連の業務を担当する専任の部署（以下、IT 部門という）の有無を尋ねた結果を表している。301名以上の企業では9割以上の企業に IT 部門があるのに対し、300名以下の中小企業では72.4%に留まる。

IT 部門を設置する余力が無い中小企業であっても、業務でパソコンやタブレット、スマートフォン等を利用しているのであれば、情報セキュリティに関する対応から逃れることはできない。中小企業においても情報セキュリティに関する対応を行う責任者・担当者（以下、「情報セキュリティ管理者」という）を選任す



出所：独立行政法人情報処理推進機構 IT人材育成本部〔2015〕pp. 172

図 1ユーザー企業におけるIT部門の有無【従業員規模別】　従業員数不明を除く[3)]

ることが必要になってくる。

筆者が実際に訪問したある中小企業では、情報セキュリティ管理者にあたる人はおらず、強いて言えば経営者がその役割を果たしていた。過日、情報セキュリティ対策について相談を受け、経営者から話を伺った。コピー機を納入している会社からファイアウォールとウィルス対策ソフトウェアのセットの導入を勧められ、リース契約を結んだが、その有効性について教えてほしいとの相談であった。ファイアウォールやウィルス対策ソフトウェアは、定評のある製品のOEM製品であり有効なものと認めることができたが、問題はその金額であった。リース契約なので、月々の支払額はそれほど大きな金額ではないように見えるが、リース期間の満了まで支払うとなるとかなり大きな金額となる。その機能と比べて、あまりにも高額な契約であった。また守るべきパソコンやデータの価値と比べても、とても見合う金額ではない。事業者間の契約なのでクーリングオフも効かず、リース契約なので中途解約することもできないというものであった。情報セキュリティについて不安や危機感を持っていたために、契約した訳であるが、情報セキュリティに関する十分な知識を持っていなかったために、随分と余計な投資をしてしまった例である。正しい知識を持った情報セキュリティ管理者がいれば、このような事態は避けられたのではないかと考える。

Ⅲ．情報セキュリティ対策の必要性

この章では、情報セキュリティ対策がなぜ必要なのかについて、情報セキュリティの脅威そのものや法律上の要請、企業倫理などの観点から考察を行う。

1．企業を脅かす情報セキュリティの脅威

インターネットバンキングの不正送金被害、パスワードリスト攻撃による不正ログイン、内部不正による情報漏えい、標的型攻撃など、企業を脅かす情報セキュリティの脅威は高度化・巧妙化してきている。

経済産業省が実施した「平成26年情報処理実態調査」[4)]によると、5,210社へのアンケートの結果、1,180社（22.6%）が情報セキュリティ上のトラブルがあったと回答している。トラブルの多くはシステムトラブルやシステム停止であるが、コンピュータウイルスや重要情報の漏えいも多く発生している（表2）。

表2．情報セキュリティトラブルの発生情報

トラブルの種類		発生したことがある件数（社）	集計企業数に対する割合
システムトラブル	システムトラブル	758	14.9%
システムの停止	内部要因によるシステムの停止	594	11.7%
	外部要因（地震、火災等の問題）によるシステムの停止	145	2.9%
その他のシステムトラブル	DoS攻撃	84	1.7%
	スパムメールやDoS攻撃の中継利用等	83	1.6%
	ホームページやファイル、データの改ざん	32	0.6%
コンピュータウイルス	USB経由によるウィルスなどの感染	240	4.7%
	スパムメールによるウィルスなどの感染	232	4.6%
	外部ホームページへのアクセスによるウィルスなどの感染	286	5.6%

	標的型サイバー攻撃によるウィルスなどの感染	33	0.6%
	その他の経路によるウィルスなどの感染	130	2.6%
不正アクセス	IP・メールアドレス詐称	47	0.9%
	リソースの不正使用	10	0.2%
	内部関係者による不正アクセス	16	0.3%
重要情報の漏えい	コンピュータウィルス、ファイル共有ソフトに起因する情報漏えい	4	0.1%
	不正アクセスによる情報漏えい	7	0.1%
	標的型サイバー攻撃による情報漏えい	3	0.1%
	内部者による情報漏えい	23	0.5%
	委託先による情報漏えい	17	0.3%
	ノートパソコン及び携帯記憶媒体等の盗難・紛失	239	4.7%

出所：経済産業省　平成26年情報処理実態調査の集計結果のデータに基づき筆者作成

2．情報セキュリティに対する法律上の要請

2015年９月３日、個人情報保護法を改正する法律が衆議院本会議において可決・成立され、同月９日に公布された。この改正により、これまで適用除外となっていた、取り扱う個人情報に係る個人の数が5,000件以下であった事業者においても、改正後は個人情報取扱事業者となることになった。

また、2016年１月からはマイナンバー制度（社会保障・税番号制度）が実施された。これにより企業は従業員などの個人番号を収集し、漏えいすることがないよう安全に保管・管理した上で、必要が無くなった場合にはデータを速やかに破棄・削除しなければならない[5)]という難しい対応を迫られることとなった。

3．情報セキュリティと企業倫理

情報セキュリティの確保を図ることには、単に自社のリスクを防衛するだけではなく、企業倫理の面からも必要かつ重要である。北原〔2012〕は、①「情報技術には『欠陥』が含まれている」、②「『絶対的安全性』を求めることは現実的ではない。」、③「情報事故の存否は、まさに、利用者自身のその利用方法によるのである。」とした上で、情報技術と倫理の関係について次のように述べている。「情報事故の発生に配慮しながら、情報技術を利用することが情報技術の倫理的利用法である。情報事故は、情報技術の利用によって、利用者自身の、あるいは、他の情報利用者の、『権利や利益を侵害』するという結果を惹起する。利用者が、欠陥のある情報技術を、そのまま、何の配慮もなく利用すれば、他の同じネットワーク利用者に迷惑がかかる」。「そのためには、利用する情報技術にどんな欠陥が含まれているかを認識していなければならない。」（北原〔2012〕pp.17－18）

言い換えれば、情報技術にどんな欠陥があるのかを認識せずして利用することは、倫理的に問題があり、そのことで他の利用者に迷惑をかけたとすれば、倫理的に責任があるということである。企業にコンプライアンスが強く求められるようになった現在、単に法令順守ということだけでなく、高い倫理観を持つことが求められる。情報事故により他者に迷惑をかけることは、情報事故そのものが与える実害やそれに対しての補償ということだけでなく、社会的な信用を失い、会社の存亡に関わるような事態になることさえある。

Ⅳ．中小企業における情報セキュリティ管理者の必要性・重要性

1．中小企業における情報セキュリティ対策の現状

中小企業における情報セキュリティ対策の実施状況は大企業に比べると遅れている。経済産業省が実施した「平成26年情報処理実態調査」によると、総従業員数300人を超える大企業では、91.6%の企業が「既に対策を実施している」のに対し、300人以下の中小企業では、76.7%に留まっている。100人以下の企業においては、既に対策を実施している企業は69.9%であり、9.8%は「対策も検討もしていない」という結果となっている（表３）。

情報セキュリティ教育の実施においても中小企業と大企業では大きな開きがある。大企業では、55.4%の企業が実施しているのに対し、中小企業では、32.9%である。100人以下の企業においては、27.3%しか実施していない（表４）。

中小企業の情報セキュリティ対策が遅れている原因を探るため、情報セキュリティ対策の阻害要因（表５）について見てみると①「手間・コストがかかる」、②「対策をどこまでやるべ

表３．情報セキュリティの対策状況（総従業者規模別）

分　類	総従業者規模別	既に対策を実施している	トラブルがあったので対策を講じた	対策は実施していないが検討している	対策も検討もしていない
中小企業	～100人	69.9%	4.5%	7.5%	9.8%
	101人～200人	76.5%	7.3%	7.2%	6.9%
	201人～250人以下	84.4%	8.2%	4.9%	3.3%
	251人～300人	85.1%	4.5%	4.9%	4.5%
	中小企業計	76.7%	6.3%	6.7%	6.9%
大企業	301人～1,000人	89.1%	10.1%	3.2%	2.4%
	1,001人～5,000人	95.0%	12.2%	1.0%	1.2%
	5,001人～	99.4%	17.3%	0.0%	0.0%
	大企業計	91.6%	11.2%	2.3%	1.9%
	合計	84.2%	8.8%	4.5%	4.4%

出所：経済産業省　平成26年情報処理実態調査の集計結果のデータに基づき筆者作成

表４．一般社員向けの情報セキュリティ教育の実施状況（総従業者規模別）

分　類	総従業者規模別	集計企業数(社)	実施している件数（社）	集計企業数に対する割合
中小企業	～100人	732	200	27.3%
	101人～200人	1,207	389	32.2%
	201人～250人以下	366	147	40.2%
	251人～300人	288	117	40.6%
	中小企業計	2,593	853	32.9%
大企業	301人～1,000人	1,630	790	48.5%
	1,001人～5,000人	825	523	63.4%
	5,001人～	162	136	84.0%
	大企業計	2,617	1,449	55.4%
	合計	5,210	2,302	44.2%

出所：経済産業省　平成26年情報処理実態調査の集計結果のデータに基づき筆者作成

きかがわからない」、③「実施する知識・ノウハウがない」のが主な要因である。①②については、総従業員規模が大きい企業にとっても大きな阻害要因であり、むしろ大企業の方が阻害要因としてのポイントが高い。中小企業特有の阻害要因としては、③「実施する知識・ノウハウがない」、④「専門家（CIO、CISO、セキュリティ担当管理職）がいない」などの人材面での問題が浮かび上がってくる。

このような状況からすると、中小企業が情報セキュリティ対策を進めるにあたっての一番の課題は、対策を実施するための知識やノウハウを持つ人材がいないことであると考えられる。今後、中小企業においてもそのような人材、情報セキュリティ管理者となる人が必要となるものと考える。

表５．情報セキュリティ対策の阻害要因（総従業者規模別）

総従業者規模別	情報セキュリティ対策の阻害要因（複数回答）				
	手間・コストがかかる	対策をどこまでやるべきかがわからない	実施する知識・ノウハウがない	専門家(CIO、CISO、セキュリティ担当管理職)がいない	企業のセキュリティ体制が整っていない(情報セキュリティガバナンスが確立されていない、セキュリティ対策方針が明確でない等)
～100人	41.7%	37.8%	31.8%	23.5%	18.0%
101人～200人	48.7%	36.9%	29.2%	26.3%	19.7%
201人～250人以下	57.1%	42.9%	33.9%	24.3%	17.8%
251人～300人	54.2%	36.8%	30.9%	25.0%	21.5%
301人～1,000人	56.7%	41.5%	26.8%	22.0%	19.6%
1,001人～5,000人	66.7%	45.7%	20.4%	19.5%	14.5%
5,001人～	71.0%	54.3%	17.3%	11.7%	7.4%
合計	54.7%	40.8%	27.5%	22.8%	18.2%

出所：経済産業省　平成26年情報処理実態調査の集計結果のデータに基づき筆者作成

2．情報セキュリティ管理者の役割・求められる技能

情報セキュリティ管理者のイメージとしては、情報セキュリティマネジメント試験[6]の対象者が近いと思われる。試験要綱[7]では、試験の対象者像を「情報システムの利用部門にあって，情報セキュリティリーダーとして，部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシーを含む組織内諸規程）の目的・内容を適切に理解し，情報及び情報システムを安全に活用するために，情報セキュリティが確保された状況を実現し，維持・改善する者」と定義している。要求される技能としては12の大項目と35の小項目が挙げられており（表6）、情報セキュリティ管理者に求められる技能が網羅されている。

情報セキュリティ対策はここまでやれば万全ということはない。一方、情報セキュリティ対策にかけることができるコストは有限であるため、コストパフォーマンスが高い対策を選んで実施することになる。

表6．情報セキュリティマネジメント試験において要求される技能

大項目	小項目
1 情報資産管理の計画	1−1 情報資産の特定及び価値の明確化
	1−2 管理責任及び利用の許容範囲の明確化
	1−3 情報資産台帳の作成
2 情報セキュリティリスクアセスメント及びリスク対応	2−1 リスクの特定・分析・評価
	2−2 リスク対応策の検討
	2−3 リスク対応計画の策定
3 情報資産に関する情報セキュリティ要求事項の提示	3−1 物理的及び環境的セキュリティ
	3−2 部門の情報システムに関する技術的及び運用のセキュリティ
4 情報セキュリティを継続的に確保するための情報セキュリティ要求事項の提示	4−1 情報セキュリティを継続的に確保するための情報セキュリティ要求事項の提示
5 情報資産の管理	5−1 情報資産台帳の維持管理
	5−2 媒体の管理
	5−3 利用状況の記録
6 部門の情報システム利用時の情報セキュリティの確保	6−1 マルウェアからの保護
	6−2 バックアップ
	6−3 ログ取得及び監視
	6−4 情報の転送における情報セキュリティの維持
	6−5 脆弱性管理
	6−6 利用者アクセスの管理
	6−7 運用状況の点検
7 業務の外部委託における情報セキュリティの確保	7−1 外部委託先の情報セキュリティの調査
	7−2 外部委託先の情報セキュリティ管理の実施
	7−3 外部委託の終了
8 情報セキュリティインシデントの管理	8−1 発見
	8−2 初動処理
	8−3 分析及び復旧
	8−4 再発防止策の提案・実施
	8−5 証拠の収集
9 情報セキュリティの意識向上	9−1 情報セキュリティの教育・訓練
	9−2 情報セキュリティに関するアドバイス
	9−3 内部不正による情報漏えいの防止
10 コンプライアンスの運用	10−1 順守指導
	10−2 順守状況の評価と改善
11 情報セキュリティマネジメントの継続的改善	11−1 問題点整理と分析
	11−2 情報セキュリティ諸規程の見直し
12 情報セキュリティに関する動向・事例情報の収集と評価	12−1 情報セキュリティに関する動向・事例情報の収集と評価

出所：「情報処理技術者試験情報セキュリティマネジメント試験（レベル２）シラバス−情報処理技術者試験における知識・技能の細目−Ver1.0」

平成26年情報処理実態調査のデータを元に、情報セキュリティ向上に寄与したと答えた企業数が多いものから順に14の対策を挙げてみた（表7）。「外部接続へのファイアウォールの配置」、「重要なシステムへの内部でのアクセス管理」、「重要なコンピュータ室への入退室管理」など技術的対策が上位を占めているが、4位に「従業員に対するセキュリティ教育」が入っている。個人情報漏えいの原因の80%以上が誤操作、管理ミス、紛失・置忘れなどの人的要因により発生しており[8]、セキュリティ教育を行うことは、情報セキュリティ管理者の重要な役割の一つと考えられる。

表7．情報セキュリティ対策状況

No.	項目	集計企業数(社)	セキュリティ向上に寄与した(社)	集計企業数に対する割合
1	外部接続へのファイアウォールの配置	5,210	2,670	51.2%
2	重要なシステムへの内部でのアクセス管理		2,559	49.1%
3	重要なコンピュータ室への入退室管理		2,153	41.3%
4	従業員に対する情報セキュリティ教育		2,138	41.0%
5	セキュリティ監視ソフトの導入		2,019	38.8%
6	セキュリティポリシーの策定		2,006	38.5%
7	セキュリティポリシーに基づいた具体的な対策の検討		1,966	37.7%
8	全社的なセキュリティ管理者の配置		1,963	37.7%
9	内部統制の整備強化		1,803	34.6%
10	リスク分析		1,628	31.2%
11	部門ごとのセキュリティ管理者の配置		1,441	27.7%
12	内部による定期的なシステム監査		1,436	27.6%
13	内部による定期的な情報セキュリティ監査		1,415	27.2%
14	定期的なアクセスログの分析		1,351	25.9%

出所：経済産業省平成26年情報処理実態調査の集計結果のデータに基づき筆者作成

大企業に比べて、人材育成に時間やコストを多く割くことができない中小企業にとって、情報セキュリティマネジメント試験において要求されるような技能を持つ人材を育成することは非常に困難である。このような人材を育成するための教育・研修機関もでてきているが、現時点ではまだ十分には普及していない。情報セキュリティに対する関心の高まりとともに、教育・研修機関がさらに充実するのを待つ必要がある。

これらを踏まえた上で、中小企業の情報セキュリティ管理者として、筆者が最低限必要と考える役割を定義してみたものが次にあげる3つの役割である。

（1）守るべきものを把握し、どのように守るかを決める

パソコン、サーバー、プリンタ複合機、ソフトウェア、電子媒体などの情報資産の管理台帳を作成する。それぞれがどのようなリスクを有しているか、どのような被害が考えられるかを分析し、セキュリティポリシーを策定する。ファイアウォールの設置、セキュリティ監視ソフトの導入、アクセス管理、入退室管理などの具体的な対策の検討・導入を行う。

（2）一般社員に対する情報セキュリティ教育

無知によるトラブルの予防、情報セキュリティに対する意識の向上、うっかりミスの予防、SNSの利用方法などについて教育を行う。情報処理推進機構（IPA）やNPO日本ネットワークセキュリティ協会（JNSA）のサイトに豊富な教材があるので、これらを利用するとよい。

（3）定期的なチェック

定期的にシステム監査、セキュリティ監査、アクセスログの分析などのチェックを行う。あるいは外部の専門家に依頼する。いわば企業の情報セキュリティについて定期健康診断を行う。

V．おわりに

2014年11月6日、衆議院においてサイバーセキュリティ基本法が可決され、翌年1月9日に全面施行された。同法は国のサイバーセキュリティに関する基本理念を定めたものであり[9]、今後、より具体的な法制化や行政のための指針が定められることが予想される。近い将来、情報セキュリティ管理者の選任が法的に義務付け

られることも考えられる。

労働安全の分野では、「労働安全衛生法」により、事業場を一つの適用単位として、各事業場の業種、規模等に応じて、安全管理者の選任を義務づけている[10]。「消防法」では、「一定規模の防火対象物の管理権原者は、有資格者の中から防火管理者を選任して、防火管理業務を行わせなければならない」とされている[11]。安全管理者、防火管理者には資格が必要とされ、講習を受け、修了試験に合格するなどして資格を取得することが求められる。情報セキュリティ管理者も同様な位置づけとなるのではないだろうか。

サイバーセキュリティ基本法の第二十一条には「人材の確保」について以下の通り定められている。

「国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る人材の確保、養成及び資質の向上のため、資格制度の活用、若年技術者の養成その他の必要な施策を講ずるものとする。」

このことからも、サイバーセキュリティに係る人材は、今後、間違いなく非常に重要となってくるものと思われる。情報セキュリティ管理者もまたしかりである。

本稿では、中小企業における情報セキュリティ管理者の必要性とその役割について考察を行った。情報セキュリティ管理者が行う具体的な対策やそれにかかるコスト、そのコストをどのように捉えるかなどについては非常に興味深いテーマであるが、本稿では言及することができなかった。今後の研究課題としたい。

1）中小企業基本法では、第二条で「中小企業者の範囲」を次のように定義している。この定義にあてはまらないものが大企業ということになる。
一　資本金の額又は出資の総額が三億円以下の会社並びに常時使用する従業員の数が三百人以下の会社及び個人であつて、製造業、建設業、運輸業その他の業種（次号から第四号までに掲げる業種を除く。）に属する事業を主たる事業として営むもの
二　資本金の額又は出資の総額が一億円以下の会社並びに常時使用する従業員の数が百人以下の会社及び個人であつて、卸売業に属する事業を主たる事業として営むもの
三　資本金の額又は出資の総額が五千万円以下の会社並びに常時使用する従業員の数が百人以下の会社及び個人であつて、サービス業に属する事業を主たる事業として営むもの
四　資本金の額又は出資の総額が五千万円以下の会社並びに常時使用する従業員の数が五十人以下の会社及び個人であつて、小売業に属する事業を主たる事業として営むもの

2）「同調査は、同協会サポートサービス委員会が、ジーエフケー・カスタムリサーチ・ジャパンの協力を得て、2015年９月～10月にかけて、従業員350人以下の中堅企業および中小企業764社と、同協会会員会社のうち、従業員１万人以下の中堅・中小企業の132社を対象に回答を得ており、合計896社の結果をまとめている。」(ASCII.jp〔2015〕の記事による)。

3）ユーザー企業587社を対象として郵送アンケート／ウェブアンケートにより実施した2014年度調査

4）情報処理実態調査は民間企業における情報処理の実態を把握し、情報政策の基礎資料とするため、経済産業省が昭和44年から毎年実施している。

5）「それらの事務を処理する必要がなくなった場合で、所管法令において定められている保存期間を経過した場合には、個人番号をできるだけ速やかに廃棄又は削除しなければならない。」（内閣府の外局の一つである個人情報保護員会が示している「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」p31)。

6）2016年春季から開始される情報処理技術者試験の新たな試験区分である。

7）独立行政法人情報処理推進機構「情報処理技術者試験　試験要綱 Ver2. 1」

8）NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ情報セキュリティ大学院大学原田研究室　廣松研究室〔2015〕「2013年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」、NPO 日本ネットワークセキュリティ協会 p12

9）サイバーセキュリティ基本法第一条、第三条

10）労働安全衛生法　第十一条

11）消防法　第八条

参考文献

・ASCII.jp〔2015〕、'ASCII.jp:Windows XP を使い続けている企業は、IT 業界に多い（１／２）｜マイクロソフト・トゥディ'、http://ascii.jp/elem/000/001/080/1080840/（2016年１月12日閲覧）
・Net Market Share〔2016〕、'Desktop Operating System Market Share December、2015'、https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0（2016年１月12日閲覧）
・NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ情報セキュリティ大学院大学原田研究室　廣松研究室〔2015〕「2013年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」、NPO 日本ネットワークセキュリティ協会
・井海宏通〔2012〕「初めてでもよくわかる小さな会社の IT 担当者になったら読む本」、日本実業出版社
・北原宗律〔2012〕「情報社会の法律」、創成社
・久保木孝明著・山本喜一監修〔2011〕「情報社会と情報倫理」、近代科学社
・総務省〔2015〕「平成27年版情報通信白書」（総務省ウェブ・サイトから本白書をダウンロード）（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27／pdf/index.html）
・田中信也〔2005〕「情報セキュリティにおける教育の重要性と人材の育成」、UNISYS TECHONOLOGY REVIEW 第86号、AUG, 2005
・中小企業庁〔2015〕「中小企業白書〈2015年版〉地域発、中小企業イノベーション宣言！」、日経印刷
・独立行政法人情報処理推進機構〔2015〕「情報セキュリティ白書2015」、独立行政法人情報処理推進機構
・独立行政法人情報処理推進機構 IT 人材育成本部〔2015〕「IT 人材白書」、独立行政法人情報処理推進機構
・独立行政法人情報処理推進機構 IT 人材育成本部情報処理技術者センター〔2015〕「情報処理技術者試験　試験要綱 Ver2. 1」、独立行政法人情報処理推進機構
・独立行政法人情報処理推進機構 IT 人材育成本部情報処理技術者センター〔2015〕「情報処理技術者試験　情報セキュリティマネジメント試験（レベル２）シラバス-情報処理技術者試験における知識・技能の細目-Ver1. 0」、独立行政法人情報処理推進機構
・中村行宏・横田翔〔2015〕「事例から学ぶ情報セキュリティ―基礎と対策と脅威のしくみ」、技術評論社