2017.6.2.JSSA大会

中小企業のサイバーセキュリティ経営の枠組みの一考察

「Consideration for Cyber Security Management framework of SME(small and medium enterprises)

2017年06月02日

情報セキュリティ合同研究会

中小企業のサイバーセキュリティ経営の枠組みの一考察

目　　次

0. はじめに：情報セキュリティ研究プロジェクトの活動

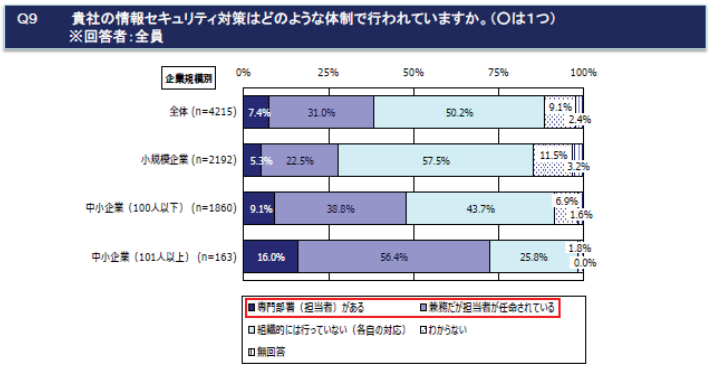
情報セキュリティ専門監査人部会と合同で研究プロジェクトを開催（主査：川辺良和）

研究テーマと概要：　中小組織を対象に、主としてマネジメントの側面に着目して情報セキュリティの諸問題を取り上げ、セキュリティの確立と強化のために有効な考え方や具体的実施策を提案し利用してもらうことを目標にしている。

研究対象となる組織：以下のIPA調査報告で示されるような状況にある中小組織

情報セキュリティ対策担当者がいる小規模企業は27.8%

- “情報セキュリティ対策に係る専門部署または担当者”がいる割合は、小規模企業で27.8%、100人以下の中小企業で47.9%、101人以上の中小企業で72.4%である。



出典：IPA「中小企業における情報セキュリティ対策の実態調査報告書（概要説明資料）」（2017年3月）

1. 研究の背景と狙い （1）

【2015年度】

「情報セキュリティ対策における営業秘密保護」をテーマとした。

【2016年度】

研究の主旨：中小組織のサイバーセキュリティ経営の枠組み

サイバーセキュリティに関するリスクが増大し、中小組織が踏み台とされるケースも報告されている中、「サイバーセキュリティ経営ガイドライン」等、中小企業も対象とする公表資料が多くなっている。

中小組織ではセキュリティ人材が不足している状況を踏まえ、本研究においては、中小組織経営者が理解、把握、実践する上でまさに優先すべき事項をコンパクトにまとめ、考察した。

1．研究の背景と狙い （2）

中小組織のサイバーセキュリティ経営の課題

■中小組織がサイバー攻撃の踏み台に利用される

・中小組織から依頼元（発注元）の担当者情報・やり取りメールを窃盗し、それをなりすましメールの素材として利用し、依頼元組織（大企業など）への攻撃に利用される。

・下請け組織が攻撃されて依頼元が預託していた個人データが窃盗される。

◇外部攻撃ではないが、下請・孫請け運用担当者自らがデータを窃盗し売却なども。

■中小組織がサイバー攻撃に遭った際の特徴

・セキュリティ人材が不足しており、適切な対応がなされない。

・受託業務などで大量の個人データを保管しているケースが多い。

・大企業などと同様に、大量情報の漏えいリスクが高い。

2．公表されている主要な対策ガイドライン（1）

以下の主要なサイバーセキュリティ関係の対策ガイドラインを取りあげ、適用の課題を検討した。

■ISMSの枠組み

■中小企業情報セキュリティガイドライン

■サイバーセキュリティ経営ガイドライン

2．公表されている主要な対策ガイドライン（2）

各ガイドラインの特徴

■ISMSの枠組み　　管理策のベストプラクティスを提示し、リスクアセスメントを基に組織・資産・リスク度合に応じた管理策を自ら選択し、実施し、見直し・改善のPDCAを回すマネジメントシステム。

■中小企業情報セキュリティガイドライン
中小組織をターゲットに厳選した管理策の実施を提示した対策ガイドライン。

■サイバーセキュリティ経営ガイドライン
上記2つの枠組みやガイドラインで提示した予防処置的な管理策を適切に講じていたとしても、攻撃に遭い漏洩してしまうこともありえるので、万一攻撃に遭遇した場合の事後処置が重要であると提言していて、迅速な事後処置の管理策の追加を提示。

2．公表されている主要な対策ガイドライン（3）

■サイバーセキュリティ経営ガイドライン
上記2つの枠組みやガイドラインで提示した予防処置的な管理策を適切に講じていたとしても、攻撃に遭い漏洩してしまうこともありえるので、万一攻撃に遭遇した場合の事後処置が重要であると提言していて、迅速な事後処置の管理策の追加を提示。

＜内容の概要＞
・経営者の認識が必要な3か条、CISOへの指示事項10か条
・サイバー攻撃対策にフォーカス
・CISOに指示する10か条と国際規格ISO/IEC27001及び27002との関係を示している　⇒ISMSとの関係性が明示
・従来の情報セキュリティ対策のうち、内部犯行対策は含んでいない

3. 本研究の背景

○研究の背景

サイバーセキュリティ経営ガイドラインは**大手・中小を含む全体が対象**

したがって、**中小組織向けに厳選されてない。**

⇒中小組織適用のガイドが欲しい！

■ISMSの枠組み　（**対象：大手・中小組織を含む全体**）

■中小企業情報セキュリティ対策ガイドライン
（**対象：中小組織（特に小規模企業向け）**）

■サイバーセキュリティ経営ガイドライン（**対象：大手・中小組織を含む全体**
但し、小規模企業を除く）

→中小企業への厳選した適用を研究

2017.06.02JSSA大会　中小企業のサイバーセキュリティ経営の枠組みの一考察　情報セキュリティ合同研究会　9

4. 本研究の内容

○研究の背景

・サイバーセキュリティ経営ガイドラインは全体の枠組み

→中小企業への厳選した適用を研究の対象としている。

＜基本的な情報セキュリティ対策＞

ISMSの枠組み
（対象：大手・中小組織を含む全体）

中小企業情報セキュリティ対策ガイドライン
（対象：中小組織　特に小規模企業向け）

＜サイバーセキュリティ事後対策＞

サイバーセキュリティ経営ガイドライン
（対象：大手・中小組織を含む全体
但し、小規模企業を除く）

中小組織向け厳選ガイドラインが
必要！　（対象：中小組織、
小規模企業含む）

○研究の方向付け

中小組織向け厳選ガイドライン

・経営者が認識すべき3原則、経営者が実施しなければならない重要7項目

→中小企業情報セキュリティ対策ガイドラインの枠組みを適用し、具体的な取組を選定

2017.06.02JSSA大会　中小企業のサイバーセキュリティ経営の枠組みの一考察　情報セキュリティ合同研究会　10

5. 本研究の結果

○研究の結果

中小組織向け厳選　⇒　ガイドラインの認識すべき3原則及び実施すべき重要7項目

■経営者が認識すべき「3原則」

経営者が認識する必要がある「3原則」	具体的な取組	補足事項
(1) セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。このため、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう。	(5)、(7)、(10)以外	➢ サイバーセキュリティリスクが自社にどのような影響を与えうるのかを認識し、対策を打つべきところへの投資額の決定、対策実施計画の策定、実施、見直しを行い、善管注意義務を果たす責任がある。
(2) 子会社で発生した問題はもちろんのこと、自社から生産の委託先などの外部に提供した情報がサイバー攻撃により流出してしまうことも大きなリスク要因となる。このため、自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要である。	(5)(7)	➢ 善管注意義務の一部である。 ➢ 物理的に目に見えないところについて、確り管理する必要性がある。
(3) ステークホルダー(顧客や株主等)の信頼感を高めるとともに、サイバー攻撃を受けた場合の不信感を抑えるため、平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要である。	(10)	➢ レピュテーショナルリスク対応を考慮する必要があり、企業存続に影響する。

5. 本研究の結果

■経営者が実施しなければならない重要7項目

項番	経営者が実施しなければならない重要7項目	具体的な取組
1	(1)サイバーセキュリティリスクの認識、組織全体での対応の策定	➢ 情報セキュリティポリシー(サンプルは「中小企業情報セキュリティガイドライン」に付属)をもとに、サイバーセキュリティリスクを盛り込む。3原則、取組(3)～(10)の結果をとりまとめて策定する。 ➢ 取引先の重要情報を扱う場合、預ける情報の自組織内での重要度と対策を開示することが必要。 ➢ セキュリティポリシーの冒頭に盛り込む項目 ・社長自身、サイバーセキュリティリスクは自社の経営リスクであると認識していること、 ・自社の重要な保護資産を特定していること ・サイバーセキュリティ対策には自社全員が取り組むこと、 ・セキュリティ対策を定期的・継続的に見直し、セキュリティが保たれた状態を維持すること ➢ サイバーセキュリティリスク管理体制の構築、運用について監査する。

5. 本研究の結果

■経営者が実施しなければならない重要7項目

項番	経営者が実施しなければならない重要7項目	具体的な取組
2	(3)サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定	➢ サイバー攻撃の脅威に対し、経営戦略の観点から、守るべき資産を特定させた上で、社内ネットワークの問題点などのサイバーセキュリティリスクを把握する。 ➢ その上で、多層防御やネットワークの分離などのリスクに応じた対策の目標と計画を策定する。 ➢ 法令違反のリスクや訴訟リスクを予め検討し、法的な要求事項を明確に把握しておくことが望ましいと考えられます。従業員向けの研修等、実施した対策についてのエビデンスだけでなく、できる限りプロセスも含めて記録しておく。 ➢ 守るべき資産とサイバー攻撃の脅威の識別結果を参考にして、自組織でも可能性のあるリスクを検討します。特に、事業継続に関わる重要なシナリオを明らかにする。 ➢ リスク対応(低減、保有、回避、移転)を検討する。 ➢ リスクに応じた対策の目標と対応計画を策定する。

5. 本研究の結果

■経営者が実施しなければならない重要7項目

項番	経営者が実施しなければならない重要7項目	具体的な取組
3	(4)サイバーセキュリティ対策フレームワーク構築(PDCA)と対策の開示	➢ リスクの把握、目標と対応計画策定、予算確保・人材配置及び育成が、計画(Plan)にあたり、この計画に基づき対策を実行(Do)し、実行の結果を確認(Check)し、改善(Act)することで環境の変化に応じたフレームワークを構築する。 ➢ 新たなリスクの発見等(未知のサイバー攻撃への対応などを考慮すると、さらに短いサイクルで見直しを実施することも検討)により、追加的に対応が必要な場合には、速やかに対処方針を修正する。 ➢ 四半期ごとに自組織で何か起こっているのかを報告するために、従業員から報告された様々な内容について、事業への影響度で分類、集計し、件数をまとめた結果をまとめ経営層に報告させる。

5. 本研究の結果

■経営者が実施しなければならない重要7項目

項番	経営者が実施しなければならない重要7項目	具体的な取組
4	(5)系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握 および (7)ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保	➢ 系列企業やサプライチェーンのビジネスパートナーのサイバーセキュリティ対策の内容を契約書等で合意する。 ➢ 系列企業やサプライチェーンのビジネスパートナーのサイバーセキュリティ対策状況(監査を含む)の報告を受け、把握する。 ➢ サプライチェーンの上流に、下流のサイバーセキュリティの対策費用を負担することも含めて、対策レベルの向上を検討してもらう。 - ➢ ウイルス対策ソフトウェアでは検知できないようなマルウェアに感染した疑いのある端末の調査など、自組織では技術的に対応が困難なものについては、外部専門機関やセキュリティベンダに委託することを想定し、自組織で対応できることと外部に依頼が必要なことを予め切り分け。 ➢ 委託元は委託先のサイバーセキュリティ対策を確保するだけではなく、再委託についても同様の対策を求めることを契約書等で合意しておく。

5. 本研究の結果

■経営者が実施しなければならない重要7項目

項番	経営者が実施しなければならない重要7項目	具体的な取組
5	(6)サイバーセキュリティ対策のための資源(予算、人材等)確保	➢ 必要なサイバーセキュリティの対策を明確にし、費用を明らかにする。 ➢ 従業員向け研修等の予算を確保し、継続的にセキュリティ教育を実施する。 ➢ 組織内のIT人材育成の戦略の中で、セキュリティ人材育成、キャリアパス構築する。
6	(8)情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備	➢ 情報の入手と提供という双方向の情報共有を通じて、社会全体でサイバー攻撃の防御につなげることが重要。情報共有を通じたサイバー攻撃の防御につなげていくため、情報を入手するのみならず、積極的な情報提供をする。 ➢ IPAや一般社団法人JPCERTコーディネーションセンター等による注意喚起情報を、自社のサイバーセキュリティ対策に活かす。 ➢ CSIRT間における情報共有や、日本シーサート協議会等のコミュニティ活動への参加による情報収集等を通じて、自社のサイバーセキュリティ対策に活かす。

5. 本研究の結果

■経営者が実施しなければならない重要7項目

項番	経営者が実施しなければならない重要7項目	具体的な取組
7	(9)緊急時の対応体制(緊急連絡先や初動対応マニュアル、CSIRT)の整備、定期的かつ実践的な演習の実施 および (10)被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備	➢ 企業の組織に合わせた緊急時における対応体制を構築する。 ➢ サイバー攻撃による被害を受けた場合、被害原因の特定および解析を速やかに実施するため、関係機関との連携や、ログの調査を速やかにできるようにしておくよう指示する。また、対応担当者にはサイバー攻撃に対応する演習を実施する。なお、インシデント収束後の再発防止策の策定も含めて訓練を行う。 ➢ 緊急連絡網を整備する。その際には、システム運用、Webサイト保守・運用、契約しているセキュリティベンダなどの連絡先も含める。 ➢ 初動対応時にはどのような業務影響が出るか検討し、緊急時に組織内各部署(総務、企画、営業・・・)が速やかに協力できるよう予め取り決めをしておく。 ➢ 訓練においては技術的な対応のみならず、プレスリリースの発出や、所管官庁等への報告手順も含めて想定する。 (続く)

5. 本研究の結果

■経営者が実施しなければならない重要7項目

項番	経営者が実施しなければならない重要7項目	具体的な取組
7	(10)被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備	(続き) ➢ サイバー攻撃の被害が発覚後、速やかに通知や注意喚起が行えるよう、通知先の一覧や通知用のフォーマットを作成し、対応に従事するメンバーに共有しておく。また、情報開示の手段について確認をしておく。 ➢ 関係法令を確認し、法的義務が履行されるよう手続きを確認しておく。 ➢ 経営者が組織の内外への発表を求められた場合に備えて、サイバーセキュリティインシデントに関する被害状況、他社への影響などについて経営者に報告させる。 ➢ インシデントに対するステークホルダーへの影響を考慮し、速やかにこれを公表する。 ➢ 社外への公表は、インシデントや被害の状況に応じて、初期発生時、被害状況把握時、インシデント収束時など、それぞれ適切なタイミングで行う。

6. まとめと今後課題

■まとめ

情報セキュリティ政策は、政府・民間の関係機関で色々と対策が提言されているが、大企業しか対策が取れないケースが多い。

しかし、繰り返しになるが、サイバー攻撃は大企業が対象となっているが、「踏み台」として狙われているのは、中小企業であり、中小企業における情報セキュリティ対策は、避けては通れない。

■今後の課題

・中小企業が実施できるサイバーセキュリティ対策の実践方法を示すこと。
・クラウドサービス、BCPの利用について、検討すること。

ご清聴ありがとうございました。

研究会は、さらに情報セキュリティとシステム監査の有効性と効率性を「深堀り」します。研究会への参画をお待ちしております。

情報セキュリティ合同研究会

＜2016年度　研　究　会　参　加　メ　ン　バ　ー　（敬称略）＞
川辺 良和　【㈲インターギデオン】：主査
山本　孟　【MHOアシストラボ】
植野 俊雄　【ISU】
芳仲　宏　【システム監査技術者】
長野 加代子【㈱ピーアンドアイ】
黒川 信弘　【黒川技術士・行政書士事務所】
田中良治　【発表者】