＜研究論文＞

中小企業へのサイバー攻撃を防御するための CSIRT 導入の考察

Study of the CSIRT introduction to defend the cyber attack to the small and medium enterprises

木村　裕一　Yuuiti kimura　木村システム企画
赤尾　嘉治　Yoshiharu Akao　NPO 法人 OCP 研究所
桜井　由美子　Yumiko Sakurai　EyeBeyond

概　要

高度サイバー攻撃対策として、府省庁や行政機関などに向けては、NISC（内閣サイバーセキュリティセンター）の「サイバーセキュリティ戦略」等で、CSIRT（Computer Security Incident Response Team）の導入を施策化している。民間企業（特に中小企業）については、「サイバーセキュリティ経営ガイドライン」が公表され CSIRT の整備を推奨しているが、対策は一部の企業を除き普及していない。

セキュリティの対策が進まない要因として中小企業の経営者が自社における現実的な高度サイバー攻撃の脅威や影響の大きさを十分に認識することが難しく、また、リスクを認識できたとしても、その後、CSIRT 導入にむけて何をなすべきかの具体的な手順が明確になっていないことが挙げられる。そこで、筆者らは、経営者がサイバー攻撃リスクを明確に認識する方法、CSIRT 導入を決断するまでの手順および CSIRT 導入のための社内対応について研究した。その研究過程においては、CSIRT 導入を、事業の必要性に合わせて進めることが出来るように考慮した。

キーワード：サイバー攻撃、中小企業、CSIRT 導入、経営者のリスク認識

1．はじめに

1.1 サイバー攻撃の状況

サイバー攻撃の魔の手が、日本に襲いかかっていることは、連日のマスコミの報道や、各団体の調査等で明らかである。特に最近は、官庁や大手企業だけでなく、意外に思えるような、名も知られていない企業（以降、各種団体、組織体についても企業と言う）も狙われる傾向にある。

攻撃者の狙い目も次第に変わってきており、最近は、単に世の中を混乱させて喜ぶ愉快犯的なもの、個人情報、企業秘密のように、窃取することによって大金を手にすることができるものから、国家機密、防衛機密のように、国の存続を脅かすようなものにまで変遷してきている。また、その手口も年々巧妙になり、府省庁、産業界、研究機関等で多くの重要情報を取り扱う組織を直接攻撃するのではなく、出入り業者等からネットワーク経由やソーシャルエンジニアリング等を通して目標にたどり着く方式（いわば外堀を埋めてから本丸を攻める戦法）に切り替わってきている。さらに、企業内から情報等を窃取するだけでなく、脆弱なサーバを踏み台にして、追跡捜査を妨害することも常套手段になっている。

そのような状況からすると、企業は、規模の大小や、扱っている情報の価値に関わらず、自社をとりまくリスクを十分に認識し、無意識のうちに犯罪に加担することのないように備えて、未然防止と有事の場合の適切な行動をする必要がある。もはや、自社をとりまくリスクを十分に認識し、備えをすることは、「企業の社会的責任である」と言える。

1.2 政府機関、民間への対応

サイバーセキュリティ基本法（平成 26 年法律

2016/10/13 提出 /2017/3/22 受理

第 104 号、最終改訂平成 28 年 4 月）に基づき，政府機関に関しては「高度サイバー攻撃対処のためのリスク評価等のガイドライン」[1] をベースに「サイバーセキュリティ戦略」[2] の中で、CSIRT 導入に取り組むことを施策として明記している。民間に関しては、「サイバーセキュリティ経営ガイドライン」[3]（経済産業省、独立行政法人　情報処理推進機構 (以降 IPA という)）において、緊急時の対応体制として、サイバーインシデント対応の専門チーム CSIRT の整備を推奨している。本経営ガイドラインの対象は、大企業と、小規模事業者を除く中小企業のうち IT システムや IT を活用したサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業である。ここで中小企業は中小企業基本法による定義の規模の企業を対象にしており、例えば小売業では資本金５千万円以下、従業員 50 人以下 (どちらかを満たす) の企業で、ある程度の体制を持つ企業を対象にしている。また、推奨であるので特段の拘束力はなく、企業の裁量に任されているのが現状である。

2．サイバー攻撃に関する先行研究と中小企業の状況

2.1 先行研究および参考文献

サイバー攻撃、CSIRT に関する研究には多くの先行研究論文があるが、中小企業の CSIRT 導入を扱ったものは少ない。また、情報セキュリティの専門企業からは、中小企業の CSIRT 導入について各種サービスや製品に関連して啓蒙する記事が掲載されるようになった。

参考文献は研究論文や製品等情報以外にも大学・学会の研究論文、国・機関の施策、国・機関や情報セキュリティの専門企業の調査資料、事例報告に関する情報も多く公表されている。これらをこの論文作成の討議と考察のベースとして参考にした。

2.2 中小企業のセキュリティ対策状況

情報セキュリティ及び CSIRT に関しての調査として「「企業 IT 利活用調査 2016」に見る IT 化の現状」[4] があるが、この中で情報セキュリティインシデントの認識状況は、サイバー攻撃、DDoS 攻撃、成りすましメール受信などの発生率は大企業や中小企業でもあまり変わらないとされている。（調査は従業員数 50 人以上の企業対象）

さらに中小企業に関しては情報セキュリティ対策が遅れているという調査結果がある。中小企業においては、その企業が取り扱う情報が重要なものであるにも関わらず、情報セキュリティ対策は脆弱であることが多い。例えば、大企業と比べ中小企業では情報セキュリティに関する業務に従事する人員が不足している傾向が強く、その原因として「情報セキュリティにまで人材が割けない」「経営層の理解や認識が足りない」が半数を超えている。[5] [6] [7]

このように中小企業では一般的にサイバー攻撃に対する経営者の認識が十分でない。これは前掲の調査のほか、筆者らがシステム監査業務等の経験から得られた情報や Web の資料 [8] などもあり実態が伺えた。

民間企業の経営者に対する国の指導としては前記の「サイバーセキュリティ経営ガイドライン」が出されており、そこでは以下の視点が示されている。

1．サイバーセキュリティは経営問題
2．経営者が認識する必要がある「3 原則」
(1) 経営者は、IT 活用を推進する中で、サイバーセキュリティリスクを認識し、リーダシップによって対策を進めることが必要
(2) 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、IT システム管理の委託先を含めたセキュリティ対策が必要
(3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要
3．情報セキュリティ対策を実施する上での責任者となる担当幹部 (CISO 等) に指示すべき「重要 10 項目」として、キュリティポリシーの策定など、リーダシップの表明と体制の構築、リスク管理の枠組み決定、防御のための事前対策などの具体的な項目が挙げられている。

本経営ガイドラインが出された背景にあるのは、サイバー攻撃対策の重要性に気づいていない経営者が多いことである。

また、中小企業のうち本経営ガイドラインの対象から除かれた小規模事業者であっても、業務委託を受けるなどにより社会的に重要な情報を取り扱う企業も多く、これらの企業ではサイバー攻撃

対応のための機能を持つことが必要になる。しかし、情報セキュリティ専門の部署もなく、情報セキュリティ担当者もいない小規模事業者については、本経営ガイドラインにより示される対応が必要であると促されても対応が難しい。本論文ではこのような小規模事業者 (4．1　考察の対象としている想定企業) も対象に考察する。

3．本論文の目的

3.1 サイバー攻撃の対象となる企業

「1．はじめに」において、企業にとってサイバー攻撃に対する備えをすることは、「企業の社会的責任である。」と述べた。先行研究においては、大規模企業、中小企業における対応や社会インフラを担う企業への対応面は多く研究されている。しかし、情報セキュリティを考える専門組織を持たず、担当者もいないような中小企業における対策などについては、理論面でも研究が少なく、前記のように調査でサイバー攻撃に対する備えが十分でない結果が報告されている。[5][6]

対策が十分でない一方、

・世の中の変化、特に IT 技術応用面の拡充によって、サイバーセキュリティ対策が必要な範囲が広がった
・重要な情報を取り扱い、重要なサービスを提供して経営をしている企業では、中小企業でもその経営資源が持つリスク相応のリスク対策を必要とする。その実施のカギは経営者のリスク認識に大きく左右される

という状況がある。

3.2 考察事項

本論文ではサイバー攻撃に対する CSIRT の導入をテーマとし、“導入の考察” は、中小企業に「サイバー攻撃対策の組織」CSIRT を作ることを目的とし、その方法を考察する。

ここで CSIRT は次の機能を持つ組織と考える。サイバーインシデントに対し、企業として統一的な対応ができること、すなわち、経営者を含め社内各部署が連携し意思決定がなされる、対外的な対応窓口を一元化し明確にする、インシデント対策、対応が統一して行われる、対応責任者が明確であることである。また、サイバー攻撃に対する予防的対処も範囲とする。

本論文では、次の 3 点を考察することを目的とした。

①経営者がサイバー攻撃リスクを明確に認識する方法
②経営者がリスクを認識した後、CSIRT 導入を決断するためのトリガーとなる情報を得て決断に至るまでの手順
③決断後の CSIRT 導入のための社内対応

なお、考察結果の実証研究については、今後の課題と考えている。

4．サイバー攻撃リスクの認識と対処

4.1 考察の対象としている想定企業

筆者らの考察の対象は以下のような企業とする。

①社内に要件を満たす情報セキュリティの専門家集団を設置することが困難な企業
・組織図上はシステム部門なるものが設置されていても、サイバーセキュリティに対する力量確保が十分にできていない。
・兼務等で日常業務に忙殺されて担当者が力量を確保する余裕がない。
②信頼のおける外部専門家を調達することが困難な企業
・自力解決できない部分を、企業の事業展開上のリスクを当事者意識を持って分析し、解決策を分かり易く提案してくれる外部専門家に巡り会えない。
・巡り会ったとしても、高額で依頼できない。
③経営者にとって事業環境、受注業務内容、顧客ニーズ、自社の業務能力を把握している信頼のおける者達（以降「企業ブレイン」という。）がまだ存在していない企業
・サイバー攻撃に対するリスク分析および対策立案を一般論でなく、自社の実態に合わせて、分析・説明できるキーマン（管理職、または役員）がまだ存在しない。
・それなりに進言する者がいても、先行投資をすることを決断するに至らない。

4.2 経営者がサイバー攻撃リスクを明確に認識する方法

4.2.1 リスクの整理の仕方

経営者にとって重視すべきリスクとは、事業継続に影響を及ぼすリスクであり、常に、実感として認識しておく必要がある。具体的にどのような

リスクが存在し、リスクが顕在化した場合に、自社および利害関係者へどの程度の影響があるのかを、理解し、その認識を継続的に持ち続ける必要がある。経営者は決断すべきことが多く多忙であり、リスク認識の必要性は頭では理解できていても、現実的には以下のような「壁」が立ちはだかっている。

・リスク分析という言葉はよく聞くが、具体的にどのようにすれば良いか分からず手が出ない。
・リスク分析の資料は膨大な量であることが多い。
・リスク分析の表現形式が、情報資産に対する脅威・脆弱性の度合いの評価に留まり、経営者の判断にとって重要な、事業内容と利害関係者との関係性が希薄な場合が多い。

そこで、筆者らは、上記の壁を乗り越えて、経営者がサイバー攻撃に由来する事業継続に影響を及ぼすリスクを認識して、リーダシップを発揮して、対策の実現を牽引するためには、リスクを経営者の目線で分析評価し「見える化」して、「サイバーセキュリティダッシュボード」で情報を共有化し、リスク認識の維持管理ができるようにすることが、先決であると考えた。

「見える化」を主体的に実施するのは自社の事業に精通している「企業ブレイン」が望ましい。しかし、そのような能力を持ち合わせている者がいない場合、当面は社内で出来るだけ適任の者を「企業ブレイン」として任命し、業務管理者、また必要により経営者の協力を得ながら実施するのが妥当であると考える。

(注)(NISC のリスク評価等のガイドライン[1] の中で、「リスク評価ダッシュボード」という類似の提案がある。「リスク評価ダッシュボード」は対策の導入計画と進捗状況の把握に特化しているが、本論文で検討するダッシュボードは、「事業継続に影響を及ぼすリスクの見える化」を目的とする。

4.2.2「事業継続に影響を及ぼすリスク」分析のアプローチ

経営者目線のリスクの認識のためには、まずは、自社の事業環境に密着した纏め方をし、かつ、ポイントを押さえて全体を見通し鳥瞰できることが重要である。詳細に整然とまとめるやり方を超えて、経営会議等で戦略を検討する際の資料として、経営者が自ら使いこなせるものにすることが肝要である。経営者であれば、おおよそのリスクは把握しているであろうが、セキュリティリスクは大小に関わらず脆弱性を突かれて顕在化するので、全てを鳥瞰して理解できていることが重要である。

自社の事業環境に密着したリスク分析の実施のためには、まずは事業環境全般を洗い出してからリスクの洗い出しを行うという２ステップを踏むことが必要である。以下に説明する。

4.2.2.1 事業環境全般の洗い出し

サイバー攻撃のリスクの影響度を認識するためには、次の４つの側面から事業環境全般を認識する必要がある。４つの側面と各側面の洗い出しの狙いを図表 - １に示す。

側面	洗い出しの狙い
事業環境全般	・迷惑を被る関係者および不正使用されうる情報の種類や件数等を把握することで、金銭的ダメージ、事業継続上のダメージ等を具体的にイメージするため。サービスまたは業務単位に、年間売上高、顧客、利用システム、重要データ、保管サーバ、保管場所、サプライチェーンの状況等をまとめる。
企業秘密情報	・不正使用されうる情報の種類を具体的にイメージするため。企業秘密に関わる各種データの種類、利害関係者、保管サーバ、保管場所等をまとめる。
IT 環境	・アタックされた場合に機密性、完全性、及び可用性を喪失する可能性のある情報の所在や他組織との関係性をトレースできるようにするため。商用機環境と社内システム環境について、概要が把握できるようにまとめる。
モバイル端末の利用状況	・直接アタックされた場合とアタックされたサーバ等にアクセスして感染し、他のサーバ等に影響を拡大する可能性もあるので、想定リスクをイメージできるようにするため。ノート PC、スマートフォン、タブレット、ウェアラブル、ハンディターミナル等がどこでどのような目的で利用されているかをまとめる。

図表 - １　事業環境全般の認識

（1）事業環境の洗い出し

企業を事業継続するためには、契約締結済の業務を守ることは当然であるが、さらに、中期経営計画等で明確にしている戦略・戦術の実現も視野にいれてリスクを分析する必要がある。そのためには、各業務やサービス単位に、年間売上高（今期および中期経営計画上の目標）、顧客、エンドユーザ、供給者に分類されるサプライチェーンも意識した利害関係者、利用システムと重要データ（顧客から預かるデータを含む）、保管場所等の情報等、サーバ攻撃を受けた場合の事業継続上のダメージを評価する上で、最低限必要な情報を鳥瞰できるようにする。

図表 - 2 に事業環境の洗い出しの例示を示すが、例示した項目以外にも、契約上の義務、市場での評価（強み、弱み、顧客満足度）、競合状況も合わせて整理しておくと、当該業務やサービスの置かれている状況を理解する上で有効である。

業務やサービス	年間売上高	利害関係者 （法人名も特定）	利用システムと重要データ	保管場所 （自社管理、第三者サービスの利用）
○○通販サービス	100 億円	購入者 出店企業（者） 決済関係企業 保管・梱包・配送会社 サイト運営会社	○○通販システムの購入者情報 （連絡先、クレジットカード、銀行口座） (20 万件) 出店者情報 (500 件) 管理者 ID	・自社設置サーバ ・契約 IDC ・○○クラウドサービス

図表 - 2　事業環境の洗い出し結果の例示

（2）企業秘密情報の洗い出し

企業秘密に関わる情報を図表 - 3 に例示するが、不正使用されると、事業継続上困難な状況になり得る情報である。企業秘密情報のカテゴリ毎に、情報の種類、利害関係者、保管場所等のデータの他、攻撃を受けた場合の、事業継続上のダメージを評価する上で、最低限必要な情報を鳥瞰できるようにする。

企業秘密カテゴリ	情報の種類	利害関係者（法人名も特定）	保管場所
知財	AA 特許（出願前・中・後） BB 商標（出願前・中・後）	特許事務所 共同出願者	経営企画室個人 PC 本社サーバ
経営戦略 顧客情報 営業情報 技術情報	中長期経営計画 新サービス企画 顧客分析	顧客 グループ会社 共同研究者 アライアンス企業	研究所室内個人 PC 研究所サーバ 管理本部サーバ 本社サーバ
個人情報	従業者情報 特定個人情報	従業者 委託先	本社キャビネット 本社サーバ パッケージベンダのサーバ 契約 IDC

図表 - 3　企業秘密の洗い出し結果の例示

（3）IT 環境の洗い出し

サービス提供で利用しているサーバ、内部管理で利用しているサーバを洗い出し、それぞれのサーバがどのサービスと紐づいており、どのような情報が保管されているのかを明確にする。これにより、各サーバが攻撃された場合の影響範囲を把握できる。

サービス名	サーバ名	管理の主体（自社／他社）	保管情報	概算件数
○○通販サービス	受注管理サーバー	○○クラウドサービス	注文者名、連絡先、クレジットカード情報等	300 万件
	商品種別サーバー	自社管理	商品番号、商品名、価格等	5 千件

図表 - 4　IT 環境の洗い出しの対象の例示

（4）モバイル端末の利用状況の洗い出し

モバイル端末（ノートPC、スマートフォン、タブレット、ウェアラブル、ハンディターミナル等）は、一括管理しにくい面があり、技術の進歩が速い。また、連絡用に利用するだけでなく、システム検証、リモートアクセス端末、SNS(Social Networking Service)、BYOD(Bring Your Own Device) 等、利用方法も多様化しており、リスクを認識しておかないと、セキュリティホールになる危険性が高い。ネットワークに接続されているあらゆる機器を洗い出し、従業者がどのような使い方をしているかを調査し、利用形態毎に合理的な保護策が講じられているか否かを明確にしておく必要がある。

利用形態	区分	管理者、端末	合理的な保護策の例示（番号は表の下を参照）
連絡用	会社支給	○○、ﾉｰﾄPC	① ② ③ ④ ⑤
	BYOD	○○、ｽﾏｰﾄﾌｫﾝ	① ④ ⑥
サービスを利用する場合の端末	会社支給	○○、ﾀﾌﾞﾚｯﾄ	① ② ③ ④ ⑤
	BYOD	○○、ｽﾏｰﾄﾌｫﾝ	① ④ ⑥
システム検証用	会社支給	○○、ﾉｰﾄPC	①② ③ ④ ⑤
	BYOD	○○、ｽﾏｰﾄﾌｫﾝ	① ④ ⑥

図表 - 5　モバイル端末利用状況の洗い出し対象の例示

（合理的な保護策の例示）
①ナンバーロック／②遠隔消去契約／③ MDM（Master Data Management）導入／④アプリケーションダウンロード制限／⑤ハードディスク暗号化／⑥ BYOD 誓約書締結

4.2.2.2「事業継続に影響を及ぼすリスク」の分析

事業環境全般の洗い出し、自社の置かれている状況を把握した後に利害関係者のダメージも含め事業継続に影響を及ぼすリスクを分析する。これにはサービスの中断等による直接的な影響の他、サイバー攻撃を受けたことが知れ渡ることによるレピュテーションリスクが及ぼす影響もある。自社が提供するサービス（業務）毎にリスクを分析する。

サービス（業務名）			顧客への保証レベル			
○○通販サービス			24 時間 365 日稼働			
想定事象	深刻度	利害関係者への影響	ダメージ			
			金銭的	人的	物理的	経営計画上
通販サイトが改ざんされて利用不能になる。	代替不可なので、回復までサービス停止	購入希望者はサービスが利用できない。出店者は販売できない。	出店者からのサービス停止期間分について損害賠償を求められる。	復旧作業に追われる。事業撤退の場合は雇用に影響あり。	出店者と契約していた自社の倉庫に売れ残り商品が滞留し、回転率が悪くなる	中期経営計画の見直しを迫られる。

図表 - 6 - 1　事業継続に影響を及ぼすリスク洗出しの例示

カテゴリ	事象	許容範囲	ダメージ		経営的影響
○○通販サービス	サービス中断又は機能不全	回復 1 時間以内	復旧費用（インシデント対応担当者労務費、システム復旧費用等）	経費 売上減少	信用失墜 ボーナス減額 給与遅配 営業権譲渡 倒産
			損害賠償額（弁護士費用、担当者労務費、損害賠償費用、謝罪広報費用等）		
			機会損失による売り上げ減少		
			機会損失による事業撤退		
	データ窃取		損害賠償額（弁護士費用、担当者労務費、損害賠償費用、謝罪広報費用等）　機会損失による売り上げ減少　機会損失による事業撤退		

図表 - 6 - 2　サービスが攻撃された場合のダメージの例示

カテゴリ	利害関係者	リスク	ダメージ
○○通販サービス	一般消費者	サイトからの注文ができない 窃取されたデータの悪用	購買意欲の衰退や不満 データの悪用による直接被害
	通販サイト構築担当Ａ社	管理者権限で当該社データセンターにアクセスして感染	通販サイト撤退による売上額の減少
	販売データ保管Ｂデータセンター	顧客データの漏えい	通販サイト撤退による売上額の減少
	商品保管、梱包、発送	当該者からの発送指示がなくなり業務中断	通販サイト中断により注文の減少による梱包・出荷品の減少
	問合せ対応（コールセンター）	業務中断	通販サイト撤退による売上額の減少

図表 - 6 - 3　利害関係者のダメージの例示

4.2.3「セキュリティダッシュボード」の維持管理

４．２．２．１及び４．２．２．２の成果物は、事業環境全般の洗い出し結果、および「事業継続に影響を及ぼすリスク」の分析結果を記載したセキュリティダッシュボードである。これらを共有環境（イントラネット、グループウェア、ファイルサーバ等）に保管し、共有情報とする。

本ボードで情報を共有化することにより、事業運営のかじ取りを任されている経営陣および管理責任者のリスクコミュニケーションを円滑にすることを想定する。その一方、分析結果は機密情報でもあるので、部門、役職等組織と役割を考慮したアクセスコントロールが必要になる。また、契約締結前等で法人名を特定するまでに至っていないケースもあり、重要情報の粒度をどの程度にするかは、サービスの複雑性、リスクの大小によって異なるが、冗長なもの及び端折り過ぎたものは有効でない。

また、リスクは、定期的および事業環境の変化に応じて随時見直しをする必要があることは言うまでもない。

4.3 CSIRT 導入を決断するためのトリガーとなる情報を得て決断に至るまでの手順

経営者は事業全体に責任を持って判断をしなければならないため、サイバー攻撃リスクがあるからという理由で CSIRT 導入を優先することはできない。他の多くの経営課題とリスクを視野に判断することが必要で、その対比をした上で行動を決定することになる。現状把握と、それに基づく決断は４．３．１および４．３．２のように行う。また、現状把握とそのリスク分析結果は CSIRT 導入を決断するためのトリガー情報であり経営者から社内への説明情報[9]でもある。

4.3.1 CSIRT 導入判断のための現状把握

インシデントの発覚の約７割は外部からの指摘による[3]など、サイバー攻撃を受けたことの自社での検知は困難で社外からの情報は重要である。次のような情報についても、リスク対策の緊急度、優先度を検討する。

- 顧客・パートナーなどからの“サイバー攻撃されているのではないか”という指摘または問い合わせ情報
- 過去にインシデントが発生して対応した経験 (及びインシデントの再発生)
- 社内からあがる「当社は○○業務情報が狙われる恐れがある。サイバー攻撃に対策しなければならないのではないか」という声
- 経営者自身からの、サイバー攻撃対策が必要かどうかの検討要請（「うちの会社は大丈夫なのか」に応えること）

緊急度、優先度としては、上記の情報のリスクが顕在化した場合について、「図表 - ６－１」、「図表 - ６－２」、「図表 - ６－３」の分析と同様の深刻度、ダメージ、及び想定発生確率、対策の緊急性を洗い出す。この洗い出しは「企業ブレイン」あるいはそれに近い適任者により行う。この際、必要に応じて経営者と連携を取り、また現場の管理者の協力を得て行う。

4.3.2 経営者による決断

経営者は４．２のリスク分析結果と、上記情報のリスク対策の緊急度、優先度情報を CSIRT 導入のトリガーとなる情報として、現時点で経営的に CSIRT 導入対策が必要であるかどうか判断する。

（１）導入を採用する場合

経営者は CSIRT 導入のトリガー情報により、

対策が現時点で必要であり、また情報システム部門等の部分的対応では不可である、企業全体で統一的対応を図る事項であると判断した場合に、CSIRT 導入を施策とすることを決断する。まず CSIRT 導入の担当者として「推進責任者」を決め、任命する。

（2）導入を採用しない場合

経営者は“当社は現在のインシデント対応、情報セキュリティ対策で十分”などと判断し、導入を採用しないこともありうる。導入しない場合でも、経営者には上記リスクに対して次のような責任が伴う。

・利害関係者が納得する説明責任を果たせること。
・法制度に抵触していないこと。

加えて上記リスクを残存リスクとして自覚して発生するリスクを許容することが必要である。また、他に経営案件があるので本件採用のデシジョンを先送りするという場合もある。その場合でも、上記が残存リスクとして残る。

4.4 CSIRT 導入のための社内対応

中小企業に必要な CSIRT が何か、企業はまず何をすればよいか、CSIRT 導入について、推進責任者が進める内容と条件、必要な資源を考察する。

4.4.1 導入に必要な活動

情報セキュリティ対策のために企業が必要な事項、CSIRT に要求される機能、中小企業の経営者の決断行動、また CSIRT 導入の参考文献 [10] [11] [12] などを元に検討した。考察の結果、CSIRT 導入段階は次のようになる。

① CSIRT 推進責任者の任命
導入活動のキーマンを任命し、活動環境を整備する。

② CSIRT の構成メンバーの任命、組織の基本機能（設置、運営、報告）確認
CSIRT を組織させる。

③情報セキュリティ対策方針の策定・公表
社内外に方針を公表する。

④ CSIRT の機能の洗い出し
具体的な CSIRT の機能を明らかにする。

⑤ CSIRT 運用ルールの策定
運用ルールを整備し、周知する。

⑥インシデント情報の集約、管理。社内各部署へサイバー攻撃検知依頼、支援（実施）
(発生の想定を含む) インシデント対応活動を実施する。

⑦サイバー攻撃検知時の緊急対応
具体的な緊急対応内容を明らかにする。

⑧情報交換・周知の手段確立 （社内）
社内における情報連携を実施する。

⑨情報交換の手段確立 （社外）
社外との情報交換等を実施する。

⑩導入後の見直し
リスクの見直しと必要なフィードバックを行う。

この各段階の活動内容を、図表 - 7 に示す。

CSIRT 導入活動
1．CSIRT 推進責任者の任命
a）経営者が CSIRT「推進責任者」を任命し社内に周知する。推進責任者は必ずしも専任でなく、兼任であっても良いが、実際に活動できる者が必要である。推進責任者は組織の目的、メンバー権限、責任、予算の概要などについて経営者に確認し、承認を得る。 b）推進責任者の役割 推進責任者は社内に CSIRT の導入を推進すると共に、サイバー攻撃が事業経営に及ぼす影響を考え、全社的立場で調整を図る役割を持つ。また、対外的に企業を代表することがある。 ただ、最初からこの役割を果たせる者が存在しない場合は、経営者はまずはそれに近い者を任命して経営者と連携させながら育ててゆくことが必要になる。 c）技術要件：推進責任者はある程度の技術知識、能力要件を必要とする。最初から満たすことは困難な場合、CSIRT の構成メンバーの情報セキュリティ担当者のサポートを受け、順次育成するなどの方法を考える。外部に支援を求めることが可能である。社内で可能な範囲を見極め、社外の支援を求める範囲を想定し、情報セキュリティ専門企業の支援を求める。

2．CSIRT の構成メンバーの任命、組織の基本機能（設置、運営、報告）確認
a）CSIRT 構成メンバーの任命：各部署に情報取得と管理の担当者を任命 (構成メンバーは基本的に兼務）し、メンバーを社内で正式に任命する。この中に情報セキュリティ担当者の任命も必要である。 b）CSIRT 組織の基本機能の確認　　CSIRT 設置、インシデント情報集約、その管理、サイバー攻撃対策情報の扱い、報告など運用ルールの策定 構成メンバーの役割、情報連携、報告ルート確立 c）情報セキュリティ担当者はサイバー攻撃に対しての技術的対応を継続的に担当できる者であることが必要（複数でサポートも可能)。また外部の支援を受ける場合、窓口となる。
3．情報セキュリティ対策方針の策定・公表
a）情報セキュリティ対策方針：事業で自社が講ずる対策を策定し経営者名で HP 等に公表する。 b）方針内容：サイバー攻撃検討の動機に関するリスクへの対処や、情報セキュリティ対策の考え方、また、社内関係部署に対する支援機能などを反映する。 (可視化したリスク、及び導入動機への対策、インシデント経験をリスク対策方針に反映)
4．CSIRT の機能の洗い出し
a）守るべき情報等の明確化：リスクの洗い出しの結果、損害、影響の大きさなどをもとに判断し決定する。 b）現在実施している情報セキュリティ対策の状況確認 守るべき対象を考慮して情報セキュリティの基本的対策の現在の実施状況（見直し状況を含む）の確認。情報セキュリティ対策体制の現状をこの段階で確認する。 基本対策項目（例：ID・アカウント管理、ウイルス対策ソフトの適用、ログ取得とチェック、暗号化、私用機器接続・利用制御等の確実な適用、見直し状況等）　基本対策確認方法（例：IPA「5 分で出来る！情報セキュリティ自社診断」[13 の付録］を利用するなど IPA 資料利用が可能） c）実施する情報セキュリティ対策内容（機能、役割等）を明確化する。ツール利用の検討、対策の実施部署を決める。 ・サイバー攻撃検知、異常事項の周知とインシデント報告方法の検討 機能：情報連携に関してメンバーの役割の明確化、インシデント報告、情報取得。
5．CSIRT 運用ルールの策定
a）運用ルール (通常時の基本ルール、緊急時ルール）の策定 インシデント報告ルール、任命されたメンバーの役割と権限、報告ルートの確立、情報の共有、報告の方法、及びこれらルールの正式な社内規程化 b）社内関係者全員の認識・啓発活動と社内整備（自社で対応可能な体制、仕組みを作る） 社内関係部署教育、サイバー攻撃等に関連する諸規定策定とその規定等の社内周知など インシデント対応ルールや関連活動の啓発活動、対応訓練などの実施 c）外部からの支援 自社で侵入検知が不可の部分、侵入後の対応可能でない部分については、推進責任者から外部の情報セキュリティ専門企業へ支援を求めるなどをルール化する
6．インシデント情報の集約、管理。社内各部署へサイバー攻撃検知依頼、支援（実施）
a）CSIRT によるインシデント対応実施（既存組織の機能拡充または新規設置） インシデント発生時の情報収集と管理の仕組みの実施 CSIRT 運用は一般社員（社内関係者）の協力がないと実施できない。情報セキュリティ対策方針に沿って一般社員も情報セキュリティ活動に参加させる諸活動を進める b) 通常時の情報収集の仕組み（検討と構築、運用）(同上) ログ収集・分析、異常値検出の実施 c）仕組みの見直し、改善　　ツール利用の検討
7．サイバー攻撃検知時の緊急対応
a）緊急時対応措置：インシデント対応、状況分析、原因究明、対策対応検討、顧客や社外への対応、社外への支援依頼 体制の起動、社外への支援依頼のルール確認 b）侵入後の社内・社外への対処行動案の事前策定。発生時の情報収集から侵入検知、社外対応訓練　（インシデント発生、その他異常検知、客からのクレーム、通知対応)
8．情報交換・周知の手段確立　（社内）
a）情報交換機能確立、社内各部署との連携、運用

9．情報交換の手段確立 （社外）
a）窓口責任者の機能設定、外部から新しい対策情報の取得（方法確立） （例：日本シーサート協議会 [10] [11] への参加と、活動、同業者との情報交換）
10. 導入後の見直し
a）サイバー攻撃が経営に与えるリスク、サイバーセキュリティリスクの再確認、周知 b）運用後間を置かずに見直しを実施する

図表 - 7　CSIRT 導入活動

4.4.2 導入時の経営者の留意点

経営者は 4.3.2 で CSIRT 導入の要否を判断する。CSIRT 導入を決定する場合、次が経営者の関心事項になる。

①事業継続の目的達成に実際に有効か
②必要な人・物・金が投資に引き合うものか
③予算通りに進む見通しがあるか
④設定した目標レベルがリスク対策として有効かどうか
⑤どのような手順で進めるか

また、経営者は次の社内向け活動、社外向け活動の見通しをつけながら進める。

①資源、技術が不足する場合の対処方法はどうか
②社内のみで対応できない場合、外部にどのように依存するか

経営者はこれを企業ブレインと意思疎通を図り解決することが必要である。なお、CSIRT 組織を基本的には次のように考える。

①既存組織の機能を活用 (拡充) する
②全く新たに必要とする機能のみ新規に設定する
③ CSIRT 推進責任者の下に可能なら専任担当者を置く
④各部署におくセキュリティ担当者は基本的に兼務体制とする

4.4.3 運用開始時の活動

（1）運用準備の完了

CSIRT の運用準備の完了時期は、導入に必要で活動に伴う設置・始動、組織、ルールや、セキュリティ方針など、具体的な成果物が完成した時である。ここでの課題として、社内で対応できる範囲を見極めて、出来ない範囲（特に技術的な対応）については社外の支援を求める、その考え方などを整理しておく。

「図表 - 7　CSIRT 導入活動」(5. CSIRT 運用ルールの策定）を参照

（2）CSIRT 導入に関わる社外向け活動

CSIRT が企業として行う活動は、まず情報セキュリティ対策方針を公表すると共に、サイバー攻撃対策組織 CSIRT を設けたことを HP 等により公にすることである。

次に窓口担当者 (推進責任者が兼務も可) が行うべき対外的活動は具体的にはつぎのような事項がある。

① CSIRT 設置とその窓口責任者の公表（障害、問題の受付窓口一本化や機能の明確化など）
②サイバー攻撃に関する最新情報収集（日本 CSIRT 協議会などへの参加等）
③緊急時対応など、情報集約、判断、社外への情報発信等の関連ルールの策定、発生時報告

5. まとめ

考察結果をまとめると次のようになる。

（1）経営者がサイバー攻撃リスクを明確に認識する方法

経営者がサイバー攻撃を受けた際の現実的なリスクを認識する（経営者が対策の必要性を認識する）ために、サイバー攻撃による自社の「事業継続に影響を及ぼすリスク」を可視化する方法、および「サイバーセキュリティダッシュボード」にて情報を共有化することを提案した。しかし、経営者が自社のサイバー攻撃リスクを認識できたとしても、実際に CSIRT 導入を決断する（経営者の背中を押す）ためには、自社のインシデント情報等、他の業務リスクの現状把握が必要である。

（2）経営者がリスクを認識した後、決断するための情報と処置

可視化したサイバー攻撃リスク情報、社内外からの情報にかかわるリスクと対策情報、インシデントからの経験値情報を総合的に考慮して、企業が対応・判断するための情報とする方法を提供した。

中小企業における経営判断は、経営者意向が大きいため、対策を進めるためには経営者の理解と

決断が欠かせない。本論文では経営者がサイバー攻撃リスクを認識すること、CSIRT 導入決断と対応の手順を考察しているので、本稿の対策により中小企業にも導入が図れる方法と考える。小規模より体力的、技術的に優位な経営状況にある中規模企業においても、この導入の方法は適用が可能である。また、経営者がCSIRT導入を決断しなかった場合の留意点も明確にした。

（3）決断後の CSIRT 導入のための社内対応

決断した後、CSIRT を導入し、運用、維持するための対応活動を「図表 - 7　CSIRT 導入活動」に明確にした。各活動の順番や深度は企業特性や企業環境によりカスタマイズして行い、これら活動情報の社内共有化も併せて実施する。

6．おわりに

本論文のおわりに当たって、今後に更なる考証を試みる必要がある 3 点について述べる。

（1）考察結果の活用

経営者がリスクを認識し、CSIRT 導入を決断し、決断した後の社内対応までの一連の流れを順に提示することができた。この考え方、手順は社内にセキュリティ組織を持たないような企業に関しても「CSIRT 導入の手引き」になると考える。これを参考にして、中小企業でもサイバー攻撃対策が確実に進むことを願っている。

（2）実証研究について

考察結果の活用として、具体的に企業に導入する実証研究の必要性を認識している。実証研究は、自社の業務環境を考えて、サイバー攻撃対策の有無確認が必要と考える、あるいはその関心がある経営者の企業を対象にする。これにより筆者らが考察した結果の有効性の検証と更なる改善ができるものと考える。

（3）企業特性への対応

事業継続に影響を及ぼすリスクの影響の大小、及び対策の緊急性等は個々の企業によって異なる。また、攻撃の方法も年々高度化している。筆者らの考察結果は企業の特性や新たな脅威の出現に応じて、具体的には個々の企業の経営環境に基づきケースバイケースで現場対応し、カスタマイズするノーハウを附加する必要性もある。

本論文は、情報セキュリティ対策診断プロジェクトのメンバーの討議によってまとめたものである。討議には西澤利治氏、久山真宏氏に参加していただいた。ここに感謝の意を表したい。

参考文献

[1] 内閣官房情報セキュリティセンター「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（平成 26 年 6 月）
[2] 内閣官房情報セキュリティセンター（平成 27 年 1 月改組し、現在内閣サイバーセキュリティセンター（NISC））「サイバーセキュリティ戦略」（平成 27 年 9 月）
[3] 経済産業省、独立行政法人情報処理推進機構 (IPA)「サイバーセキュリティ経営ガイドライン」V1.0　（平成 27 年 12 月）
[4] 日本情報経済社会推進協会（JIPDEC）「JIPDEC IT － Report 2016 Spring「企業 IT 利活用調査 2016」に見る IT 化の現状」（2016 年 5 月）
[5] IPA「2015 年度中小企業における情報セキュリティ対策に関する実態調査報告書」（2016 年 3 月）
[6] 日本情報システム・ユーザー協会（JUAS）「企業 IT 動向調査　2016 年」（2016 年 4 月）
[7] IPA「情報セキュリティ人材の育成に関する基礎調査」（2012 年 4 月）
[8] TechTerget ジャパン　Web 掲載情報「「中小企業はサイバー攻撃に狙われない」と思い込んでいる上司をどう説得する？」(2016年4月) http://techtarget.itmedia.co.jp/tt/news/1603/22/news06.html
[9] 赤尾嘉治　経営情報学会秋全国研究発表大会要旨集　2016「サイバーセキュリティ対応を躊躇する経営陣の意思決定行動に関する考察」（2016 年 9 月）
[10] 日本コンピュータインシデント対応チーム協議会（日本シーサート協議会）「活動内容、入会案内、運営規約等」www.nca.gr.jp/
[11] 日本コンピュータインシデント対応チーム協議会「CSIRT スターターキット」(2011 年 8 月)
[12] 日経コンピュータ特集記事「CSIRT について　被害最小化の切り札」(2014 年 7 月 16 日)
[13] IPA「組織の情報セキュリティ対策自己診断テスト」情報セキュリティ対策ベンチマーク V4.4　（2015 年 10 月）

以上