情報セキュリティ対策診断の研究プロジェクト　報告

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

2017年研究大会報告

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

木村　裕一　　赤尾　嘉治　　桜井　由美子

目次

- 当研究は、2016年報告テーマの継続である。
- 2017年報告での研究内容の主な追加・変更点
  リスクの「見える化」の検討
  CSIRT導入の社内活動の検討
  コンサル向け「手引書」の検討
  これらの結果を研究論文としてまとめた

1．研究の背景
1．1 サイバー攻撃の傾向

・世の中を混乱させて喜ぶ愉快犯的なものから、
国家機密、防衛機密等、国の存続を脅かすようなものに変化

・大口を直接攻撃ではなく、出入り業者等からﾈｯﾄﾜｰｸ経由や
ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞを通してたどり着く方式に替わってきている。

・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。

・官公庁や大手企業だけでなく、重要情報、価値ある情報を扱う
企業・団体及び脆弱な環境の企業も狙われる傾向にある。

1．2 問題意識

企業は、規模の大小や、扱っている情報の価値に関わらず、自組織をとりまくリスクを認識し、無意識のうちに犯罪に加担することのないよう、未然防止と事後対応に備える必要がある。

⇒組織の社会的責任である。

1．3　対策

サイバーセキュリティ基本法（2015年1月9日　全面施行）

第13条：**国の行政機関**等におけるサイバーセキュリティ**確保**

第14条：**重要社会基盤事業者**等におけるサイバーセキュリティ**確保の推進**

第15条：**民間事業者及び教育研究機関**等の**自発的な取組みの推進**

（行政機関）

「**高度サイバー攻撃対処のためのリスク評価のガイドライン**」(2014/6/25)

防衛及び対応の実現手法をガイド。

府省庁CSIRTおよび府省庁の壁を越えたCYMAT(*)が稼働。

(*)(Cyber　Incident Mobile Assistance Team)

（民間）

「**サイバーセキュリティ経営ガイドライン**」(2015/12)

サイバーセキュリティ経営の3原則

サイバーセキュリティ経営の重要10項目（CSIRT含む）

事実上は、組織の裁量に任されている。

2．研究の目的（問題意識）
2．1　中小企業の状況

- 中小企業では経営者が情報リスクを認識しリーダーシップを発揮して対策を進める必要があるが、現実的には、経営者の情報セキュリティへの関与の度合いは、企業規模の大小に逆比例している。（IPA調査）
- サイバー攻撃の対象となる中小企業も多い。
- 中小企業では対策が十分でない。
- サイバー攻撃に対する備えをすることは重要情報を取り扱う企業の社会的責任である。
- 中小規模の経営者が容易にリスクを認識でき、リーダシップを発揮して対策を進めることができるようにすることが重要であると考えた。

２．２ 中小企業の対策ガイドライン（１）

「サイバーセキュリティ経営ガイドライン」 METI, IPA

●サイバーセキュリティは経営上の問題である

●経営者が認識する必要がある「３原則」

①経営者がリスクを認識しリーダーシップをとって対策を進める。
②自社のみならず、系列企業やﾋﾞｼﾞﾈｽﾊﾟｰﾄﾅｰ等も意識する。
③平時・緊急時、何れも関係者と適切なﾘｽｸｺﾐｭﾆｹｰｼｮﾝを図る。

２．２ 中小企業の対策ガイドライン（２）

サイバーセキュリティ経営の重要10項目

①リスク認識と対応方針策定
②リスク管理体制の構築
③リスクの把握と実現ｾｷｭﾘﾃｨﾚﾍﾞﾙを踏まえた目標と計画
④セキュリティ対策ﾌﾚｰﾑﾜｰｸ構築(PDCA)と対策の開示
⑤系列企業やﾋﾞｼﾞﾈｽﾊﾟｰﾄﾅｰを含めた対策の実施と状況把握
⑥セキュリティ対策のための資源の確保
⑦ITシステム管理の委託先のセキュリティ確保
⑧攻撃情報共有と有効活用のための環境整備
⑨緊急時対応体制（マニュアル、CSIRT整備、演習）
⑩被害発覚時の通知先、開示情報の把握、経営者による説明のための準備

２．３ 問題意識と当研究の目的

- サイバーセキュリティ対策として中小企業へのCSIRTの導入の方法
- 次の3つの目的を考察する

目的A 経営者がサイバー攻撃リスクを明確に認識する方法

目的B 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

目的C 決断後のCSIRT導入のための社内対応

２．４ 考察の対象企業

情報セキュリティに関して

① 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があっても、サイバーセキュリティ対策が十分でない。
- 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
- 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「企業ブレイン」がまだ育っていない企業
- 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「企業ブレイン」（管理職又は役員等キーパーソン）がまだ育っていない。
- 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。

3．考察1（目的Aについて）
3．1　サイバー攻撃対策の課題と対策方法

・経営者に、サイバー攻撃による事業上のリスクの認識を深めてもらうには、一般論ではなく、実際の事業に直結したリスク評価を行う必要がある。

・また、事業環境の変化に応じてリスクの見直しが必要になるので、常時、キーパーソンと情報共有をできるようにしておく必要がある。

⇩

・サイバー攻撃を受けた場合の影響範囲と影響度を認識するため情報を「**見える化**」し、社内のキーパーソンと情報共有化するための「**サイバーセキリティダッシュボード**」として活用する。

（NISCのガイドラインの中で、「リスク評価ダッシュボード」という類似の提案があるが、「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、本ダッシュボードは、「自社の事業上のリスクの可視化」が主である。

3．2　経営者がサイバー攻撃リスクを明確に認識する方法

「事業継続に影響を及ぼすリスク」分析のアプローチ（リスクの整理の仕方）

事業環境全般
- 事業のサービスまたは業務単位に、金銭的、事業継続上のダメージ等を具体的にするため。

企業秘密情報
- 不正使用されるとダメージを受ける情報の種類・属性を具体的にイメージするため。

IT環境
- アタックされた場合に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。

モバイル端末の利用状況
- 他の業務システム等に影響が拡大するリスクをイメージするため。

3．3　事業環境に影響を及ぼすリスクとダメージの把握（1）

サービスが攻撃された場合のダメージを定性・定量の両面から把握しておく必要がある。

- ・利害関係者への影響度
- ・従業者への影響度
- ・損害賠償額
- ・復旧費用
- ・機会損失による売上減少額

事業継続に影響を及ぼす経営リスク（ダメージ）洗出しの例示

サービス（業務名）		○○通販サービス					
顧客への保証レベル		24時間365日稼働	ダメージ				
想定事象	深刻度	利害関係者への影響	定性的				定量的
			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。	

3．3　事業環境に影響を及ぼすリスクとダメージの把握（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	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		

3．3　事業環境に影響を及ぼすリスクとダメージの把握（3）

利害関係者のダメージの例示

カテゴリ	利害関係者	リスク	ダメージ	ダメージ額
○○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	
□□サービス				

3．4　セキュリティダッシュボード

作成資料

前項の作成資料をセキュリティダッシュボードと呼ぶ。

サイバー攻撃に関して、当社の事業上のリスクを洗い出し、リスクを「見える化」して経営者、関係者が情報共有する

※情報共有：　経営者（経営陣）、企業ブレイン

- 機密情報

  「サイバーセキリティダッシュボード」はアクセスコントロールが必要

  自社のリスクの全体像は明確になったが、これらの中には必ずしも社内全てにオープンにすることが妥当でないものも存在するので、部門、役職等組織内の構造に起因するアクセスコントロールが必要

- 見直し

  事業環境は変化するので、適宜見直しが必要

4．考察（目的Bについて）
4．1CSIRT導入推進を必要とする情報

目的B 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

経営者が決断するために考慮する事項

①社外からの情報
- 顧客から当社への情報（クレーム、事故情報など）
- 同業者・業界からの情報（事故情報、ガイドラインなど）

②社内からのサイバー攻撃対策の必要性情報
- 社内（現業/営業/情報部門など）からの要望
- 社内からのセキュリティへの懸念

③情報集約・情報共有と分析
- 経営者が対策必要性を判断し、納得してCSIRT導入を決断
- 経営者から従業者に情報提供・共有

4．2 中小規模企業に必要なCSIRT機能

経営者は当社として実行可能性を検討

①中小規模企業に必要なCSIRTとは何か、企業はまず何をすればよいか

②経営資源（人、モノ、金）がどれだけ必要か、当社の資源で出来るのか

③当社の業務で本当に必要不可欠なものか
本当に優先順位の高いものから対応

④社内で本当にどこまで実行可能か
対応できなくなったらどうするか

⇒ 検討結果：CSIRTの導入するか否か決断する

5. 考察3（目的Cについて）
5．1　導入活動段階

決断後のCSIRT導入のための社内活動

	CSIRT導入段階	活動項目
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・実施	運用ルールを整備し、周知し、実施する。
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 発生の想定を含むインシデント対応
7	サイバー攻撃の監視と検知時の緊急対応	具体的な緊急対応内容を明らかにする。監視活動を実施し、検知時に緊急対応をする。
8	**情報交換・意思疎通、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。

5．2　CSIRT導入活動

CSIRT推進責任者の任命　（中小企業としての工夫例）

① **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。
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。

② **推進責任者の役割**
推進責任者は組織（CSIRT委員会）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、同意を得る。
推進責任者は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。

③ **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。

５．３ 運用開始確認

運用準備の完了確認（経営者の留意事項）

- CSIRTの運用準備の完了確認は重要である。
  完了時期は、導入に必要で活動に伴う設置・始動事項、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、追加管理策の完了と運用実績を確認した時である。
- ここでの課題として、社内で対応できる範囲と出来ない範囲を見極めておき、特に技術的な対応については社外の支援を求めることなど方策を整理しておく。

６．まとめ
６．１ 成果

研究の成果

（1）中小規模企業がCSIRTを確実に導入できる方法を考察

- 攻撃者は組織が持つ情報の価値に着目する。企業規模で考えることではない
- 攻撃者は社会の中でその組織が果たす役割に着目する
- 中小規模企業であっても、サイバー攻撃対策の対象と考える必要がある。しかし中小規模企業に関する検討が少なく、導入の手引きも少ないため、それを対象に考察することの意味がある

（2）中小規模企業にサイバー攻撃対策の組織を導入するまでを考察

（3）中小規模企業でサイバー攻撃対策がなぜ進まないのか

- 経営者の判断のウエイトが大きな事に由来する新たな課題の存在も判明した

6．2　考察結果の活用

（1）結果の活用

- 経営者がリスクを認識し、CSIRT導入を決断し、社内対応までの流れを提示することができた。この考え方、手順に基づき「CSIRT導入の手引書」及び「関連帳票」を作成する。
- これにより、経営環境に則してカスタマイズすることができ、セキュリティ組織を持たないような企業にも適用できるものと考える。

（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。
- この結果により考察した内容の有効性の検証と更なる改善ができるものと考える。
- 実証研究へ関心がある参加企業を募集しています。
  チャレンジする企業と共同して研究を更に深めたいと思います。

おわりに

- 提案した方法は中小規模企業がリスク状況を確認した上で段階的に選択・実施できる。
- これを参考にして、中小規模企業でサイバー攻撃対策が確実に進むことを期待する。

本論文ではプロジェクトのメンバーの西澤利治氏、久山真宏氏に討議に参加していただいた。

ご清聴有難うございました

当研究プロジェクトは継続して、一緒に研究する方を募集しています。

研究会は、ほぼ毎月１回　開催しています。

場　所　メンバー企業　会議室　他

時期・時間　毎月中旬、水曜（原則）の１８：３０から約2時間

研究結果については、HPに公表します。

連絡は、「情報セキュリティ対策の診断」研究プロジェクトまで

＜問い合わせの窓口アドレス＞（学会事務局経由）

http://www.sysaudit.gr.jp/toiawase/index.html

25