情報セキュリティ対策の診断研究プロジェクト　報告

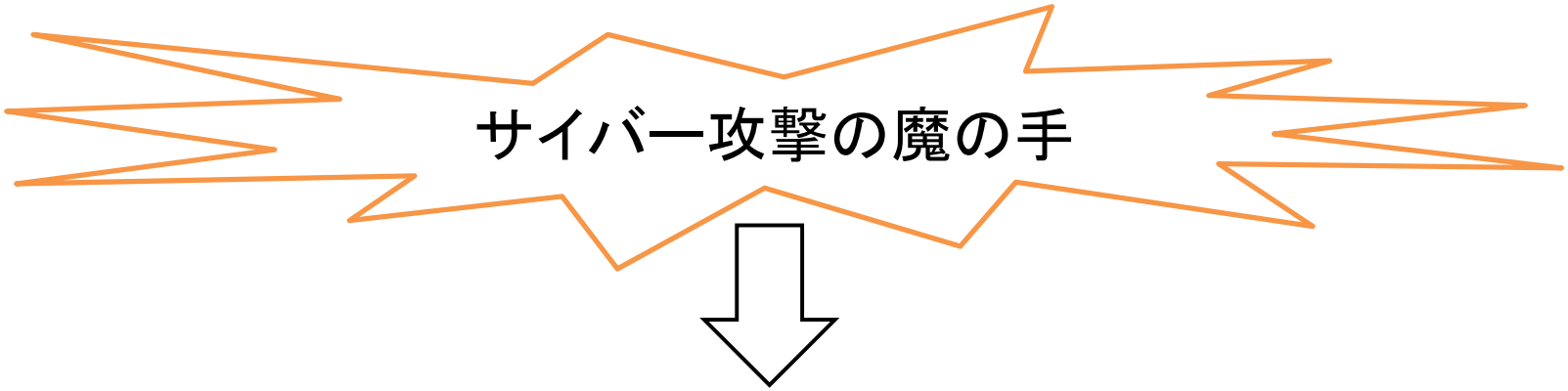
中小企業へのサイバー攻撃を防御するためのCSIRT導入の考察

Study of the CSIRT introduction for the defence of cyber attacks on small and medium enterprises

木村　裕一　　赤尾　嘉治　　久山　真宏
桜井　由美子　　西澤　利治

目次

1. 研究の背景



サイバーセキュリティ基本法

平成27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**

1．研究の背景（現状）

（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）で、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。

1．研究の背景（現状）

「サイバーセキュリティ経営ガイドライン」METI, IPA

<u>サイバーセキュリティ経営の3原則</u>

A）　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

B）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

C）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

1. 研究の背景(現状)

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ベ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. 系列企業やビジネスパ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
7. IT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

1．研究の背景（サイバー攻撃の傾向）

・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、防衛機密等、国の存続を脅かすようなものに変遷。

・単に世の中を混乱させて喜ぶ愉快犯的なもの。

・大口を直接攻撃ではなく、出入り業者等からNW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切り替わってきている。

・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、無名に近い企業・団体（特殊、貴重）
及び脆弱な環境の企業も狙われる傾向にある。

２．研究の目的（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に、備え（未然防止と事後の対応をする必要がある。⇒組織の社会的責任である。

・経営者が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）

・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. 研究の目的

次の3点を考察

①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（訴えかける）にはどのようなしくみが必要か？　【リスク認識】

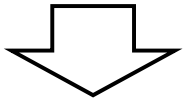
②リスクを認識した後、経営者が、CSIRT導入を決断するためにはさらにどのような情報が必要か？　【現状把握】

③CSIRT導入を決断した後、経営資源の提供可能な範囲内で、組織はまずは何をどこまですればよいか？　【実行計画・実施】

３．考察（リスク認識）

・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。



・そこで、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共有化するための「サイバーセキュリティダッシュボード」の活用を提案する。

（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。

サイバーセキュリティダッシュボード構成要素

Ⅰ　サービス単位の取扱う重要情報の明確化

経営者であれば、おおよそのことは把握しているであろうが、リスクを見直す際には、顧客に提供しているサービス及び企業内活動毎に、取扱う情報の種類、所在、件数等のデータを明確（棚卸）にしておく必要がある。

Ⅱ　サービス単位の利害関係者の明確化

経営者であれば、おおよそのことは把握しているであろうが、被害を被る関係者全体の認識が薄いと、想定外のところで損害賠償を請求され、経営危機に陥る可能性がある。

サイバーセキュリティダッシュボード構成要素

Ⅲ 商用NW環境及び社内システムのNW環境の明確化

影響範囲を明確にするには、商用機・社内システムの所在および
各サーバ内に保管されている情報の重要度と秘匿化対策を明確にする
必要がある。

Ⅳ モバイル端末（スマホ、タブレット、ウェアラブル等）の利用状況の明確化

モバイル端末は、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、SNS、
BYOD等、利用方法も多様化しているので、使いこなせないリスクも含めて、
世の中の流れに取り残されることなくしっかり追随しておく必要がある。
従業者がどのような使い方をしているかを調査し、利用形態毎に保護策を
明確にしておく必要もある。

サイバーセキュリティダッシュボード構成要素

Ⅴ 経営的なリスク（ダメージ）の総括

Ⅰ～Ⅳを判断材料として、最終的には、各サービスが攻撃された場合のダメージを定量・定性の両面から把握しておく必要がある。

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

※「サイバーセキュリティダッシュボード」のアクセスコントロールについて

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になる。

３．考察（現状把握）

～ CSIRT導入推進を必要とする情報～

＜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）

＜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懸念

＜情報集約・情報共有と分析＞

- 経営者が対策必要性を判断（納得しCSIRT導入を決断）
- 経営者から従業者に情報提供
- 当社として実行可能性検討

３．考察（実行計画・実施）

～中小規模企業に必要なCSIRT機能～

経営者はCSIRTの導入を次の要因を考慮して決断する

i. 中小規模企業にとってCSIRTとして何が必要か、組織はまず何をすればよいか

ii. 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

iii. まず、何をするのか

iv. 当社（中小企業）の業務で本当に必要なものか
- 余分な事を求められていないか
- 優先順位の高い（必須の）ものから対応

v. 社内で本当にどこまで可能か
- 対応できなくなったらどうするか

検討結果：次のように見通しを得てすすめる

3．考察（実行計画実施）

～中小規模企業に必要なCSIRT機能～

導入	運用	洗い出した機能	内容	優先順位
○		体制　責任者等を任命	責任者・構成メンバーの任命、役割、責任、活動報告	◎
○		組織　セキュリティ方針の策定	基本事項の確立	◎
○		運用規程　インシデントに備える規定等	インシデント情報集約、管理、情報交換など最低限整備する要素・項目	○
○		組織　情報の報告ルート	情報周知手段等の確立、普段の留意行動等　社内教育	○
○		組織　守るべき情報はどこにあるか	企業内における情報管理の現状把握と必要な対策の確認	○
	○	事故対策システムの導入等	上記の現状に応じた対策システム導入	（○）
	○	組織　セキュリティ対策の策定	事故発生時の対処行動の検討	
○	○	情報取得対外窓口の公表	継続的に担当する者を任命、日本シーサート協議会参加（例）など	

3．考察（実行計画実施）

～中小規模企業に必要なCSIRT機能～

優先度	洗い出した機能	中小企業としての絞り込み	必要経営資源			
			人	技術	工数	金
◎	体制　責任者等を任命	まず責任者を任命	◎	○		
◎	組織　セキュリティ方針の策定	事業範囲での取り組みを確定		○	○	
○	運用規程　インシデントに備える規定等	事業範囲に限定して下記管理対象と関連情報に関するリスク対策を周知する		◎	○	○
	組織　情報の報告ルート	上記規定等の社内教育			○	
○	組織　守るべき情報はどこにあるか明確にする	保有情報、組織の関係情報など管理をするべき対象とそのリスクを分析する	○	◎	○	○
	事故対策システムの導入等	上記の現状に応じた対策システム導入		○		○
	組織　セキュリティ対策の策定	保有情報、関係情報とその連絡先洗出し			○	
	情報取得対外窓口の公表	任命した責任者をあてる			○	

4. 考察の成果

（1）　事業経営リスクの可視化ツール
「サイバーセキュリティダッシュボード」

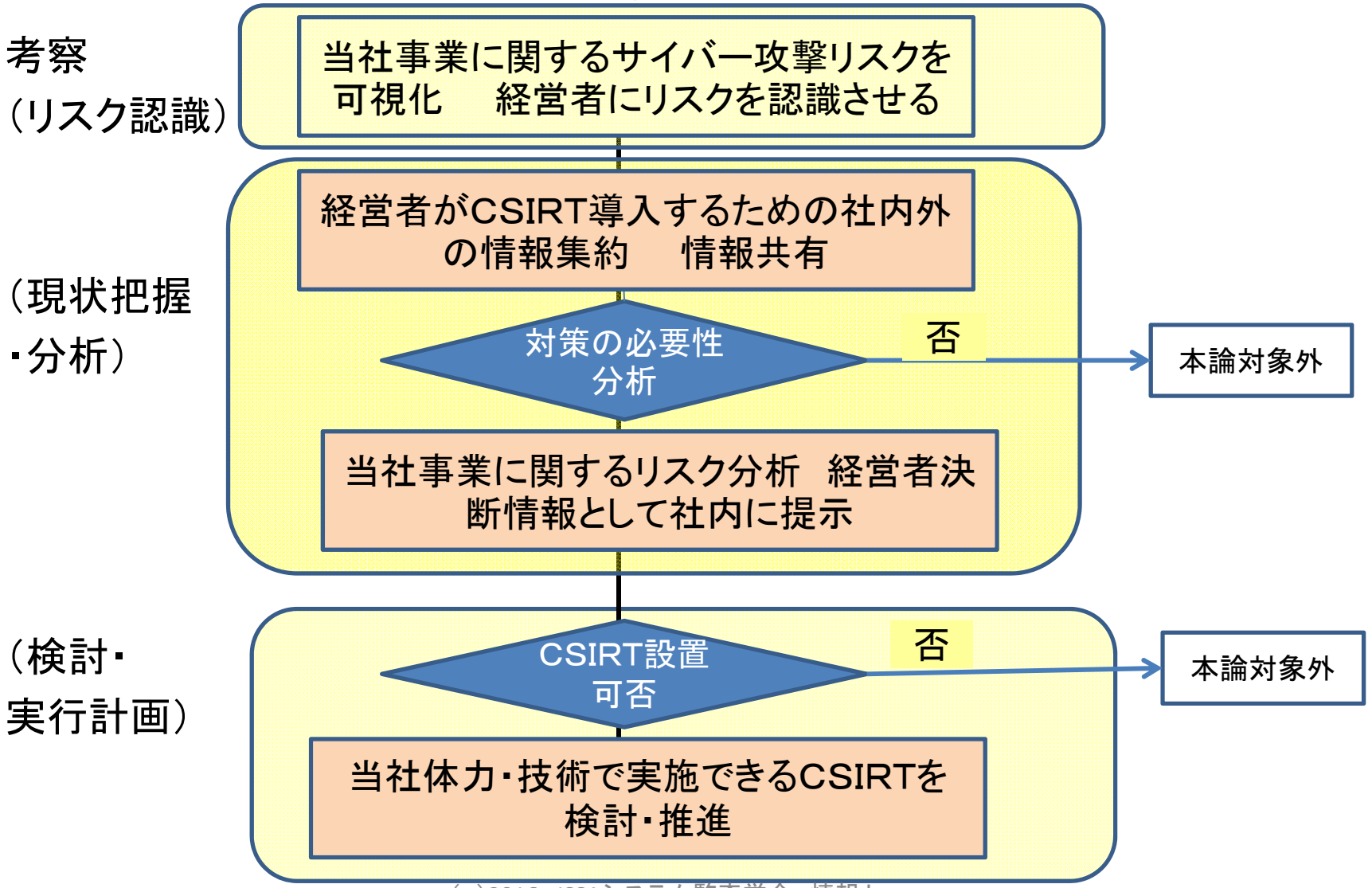
- サイバー攻撃に関して、当社の事業上のリスクを洗い出すリスクを見える化して経営者、関係者が情報共有する

（2）サイバー攻撃のリスクの可視化ツール（2015年研究大会報告）
「模擬戦環境によるサイバー攻撃の解析手法」

- 低価格ワンボードパソコン「Raspberry Pi」上に、脆弱性スキャンを実証する攻撃サーバーと評価対象の標的サーバをハニーポットで構築し、サイバー攻撃を模擬的に再現。
- 実際のサイバー攻撃に使用されるツールは標的サーバーをどのように偵察・調査を行うのか理解することが可能となる。攻撃への対抗手段を評価しながら導入できるなど。

4. 考察の成果

～対策フロー～



5. まとめ

（1）中小規模企業を対象にCSIRT導入方法を容易にする考察

- （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

- 経営者の判断が大きな事に由来する新たな課題の存在も判明

おわりに

- これを参考にして、中小規模企業でサイバー攻撃対策が進むことを期待する。
- 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方法を選択・実施できる。

おわりに

（1）今後の課題
- CSIRTの導入について実証研究
- 目的に対する妥当性確認（方法）
- 実行の可能性（方法）

（2）実証的アプローチ：CSIRTの設置を提案する
（被害の拡大を防止するために、対策の早期実施が必要である）
- サイバー攻撃による侵入検知措置をする。
  サイバー攻撃により万一侵入された場合の様々な対応手順を事前に検討する。
  そのルールを用いてシミュレーションする。

（3）自社の範囲で実施できない部分について、外部の専門企業の協力を得る。その範囲をどのように決定するか

ご清聴有難うございました

当研究は継続しております。一緒に研究する方を募集しています。

当研究プロジェクトでは、ほぼ毎月１回の研究会を開催しています。

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