システム監査学会
2015年6月5日研究大会報告

中小企業へのサイバー攻撃を防御するためのCSIRT導入の研究

（2014年度から引き続き研究中であり、中間報告である）

情報セキュリティ対策診断プロジェクト
木村　裕一(主査)、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

1．1問題提起

1.1.1サイバー攻撃の対象の変化

サイバー攻撃が府省庁、行政機関の重要な情報に狙いをつけて、増加の一方である。当然民間企業にも被害が発生している。

1.1.2民間中小企業も狙われる対象となっている

・価値のある情報を多く保有している。直接お金に結び付かなくとも重要情報を保有し標的となる。

・内部情報を窃取され踏み台として利用される。（取引顧客との信頼関係情報の悪用）

⇒企業・団体の社会的責任として情報の“善管義務”がある。

１．研究の背景

１．２　サイバー攻撃対策の現状と課題

１．２．１　中小規模企業のサイバー攻撃対策の現状

・サイバー攻撃対策は十分ではない。

情報セキュリティ対策自体が脆弱であることが多い。

情報セキュリティ対応者が不足している傾向が強い。「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」状況

１．２．２適切な行動指針の不足

- 「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」（NISC　2104年）

府省庁向けの標準的な対策基準の一つ。

・中小規模企業向けには適切なガイドラインがない。

1．研究の背景

1．3　研究の目的

中小規模企業にとってもサイバー攻撃対策の実施が必要。その現実的な方法を提言

- 経営者が自社のサイバー攻撃のリスクを十分に把握していない（認識していない）
- 中小規模企業でサイバー攻撃対策が進まない原因を探り対応
- 経営資源の制約を考慮した実現しやすい方法

これらに対応するサイバー攻撃対策として
CSIRT組織を設置する方法を基本に提言する

1．研究の背景

1．3　研究の目的

CSIRTとは（一般に）

サイバー攻撃による被害を最小限に抑えることを目的とする。

- 社内インシデント情報をCSIRTに集約し、素早い対処判断を可能にする。
- 侵入以降の事後対応を検討準備し、迅速な対応を可能にする 。
- 世の中のサイバー攻撃に関する情報収集窓口機能を持たせる。

☆「日本シーサート協議会（NCA）」（日本コンピュータセキュリティインシデント対応チーム協議会）

１．研究の背景

１．３　研究の目的（つづき）

＜企業としての課題＞

- 経営者が社外のサイバー攻撃リスクの情報を自社にあてはめて認識していない。
- 経営者はサイバーリスクが自社には無縁であるという認識がある。
- 自社で保有する情報がどのような保護管理の状況にあるか明確に把握していない。
- サイバー攻撃対策の具体的な内容について、どのような事をするか理解していない。

1．研究の背景

1．4 サイバー攻撃対策の方法

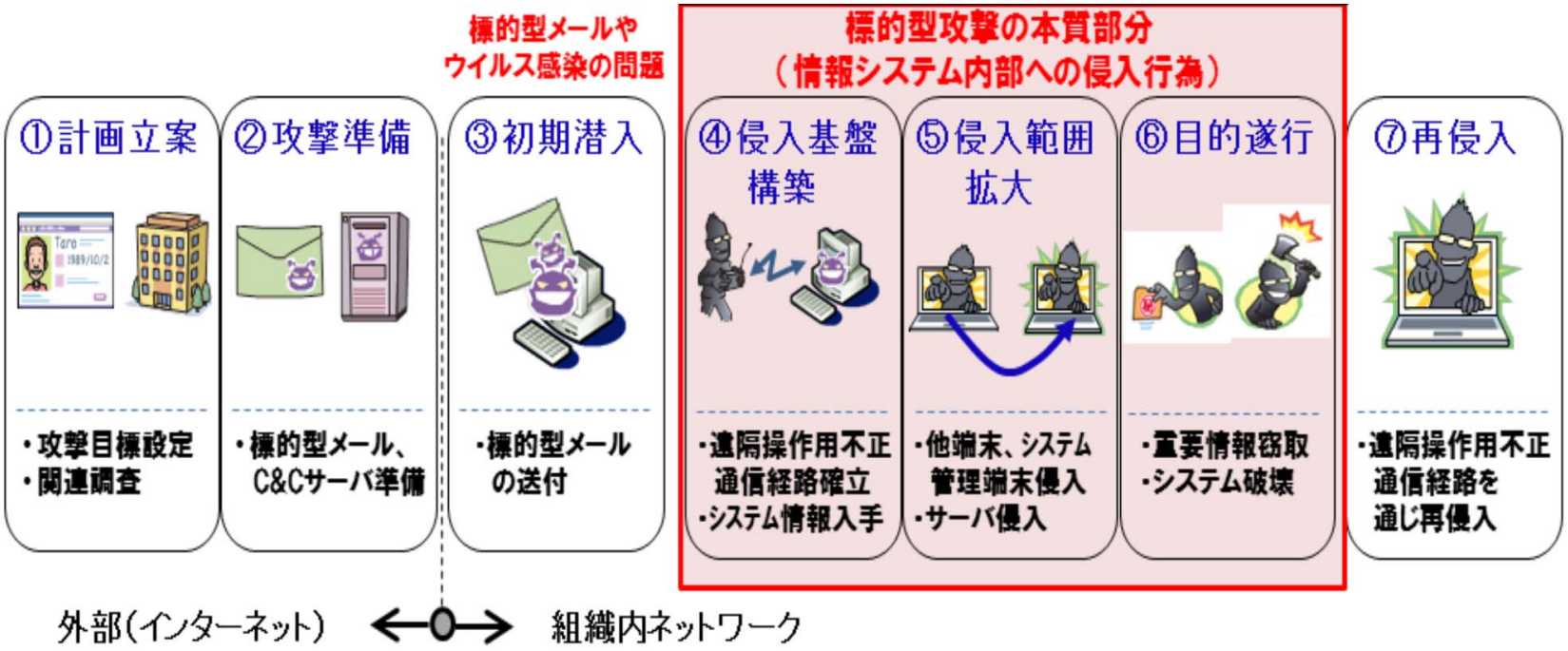
- 経営者が自社のサイバー攻撃リスクを明確に認識できるようにする。リスクを明確に説明する。
- 投入できる経営資源は少ないことを考慮した対策を検討する。
- いくつかの方向からアプローチする。
- 出来るところから、出来る範囲の対策をリスクに応じて実施する方法を検討する。

2. 研究対象と範囲

2.1　サイバー攻撃のリスクの特質

2.1.1　サイバー攻撃の目的、手法など

・攻撃の全体像（NISCガイドラインより）



２．研究対象と範囲

２．１　サイバー攻撃のリスクの特質

２．１．２　サイバー攻撃の特質

- 攻撃者は出来るだけ目立たないよう、攻撃の痕跡を残さないようにする（検知が難しい）。
- 攻撃方法は対象により変化するため対応が難しい。
- 窃取した情報を標的攻撃のなり済ましに利用する。

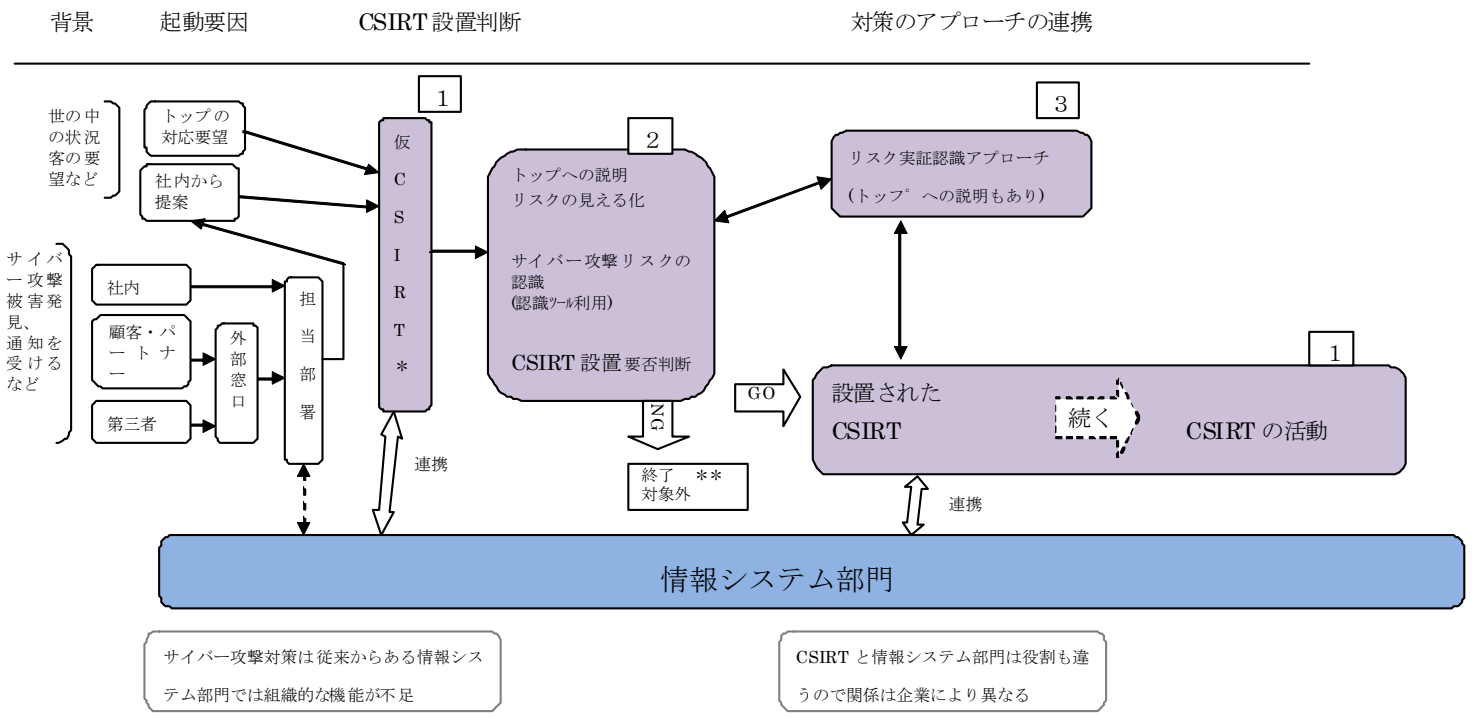
２．２　中小規模企業におけるセキュリティ対策

- （１）中小規模企業としての制限、制約
- （２）想定する中小規模企業のペルソナ
- a)事業などの状況
- b)対策を考える動機

2. 研究対象と範囲
2. 3　サイバー攻撃対策のアプローチ

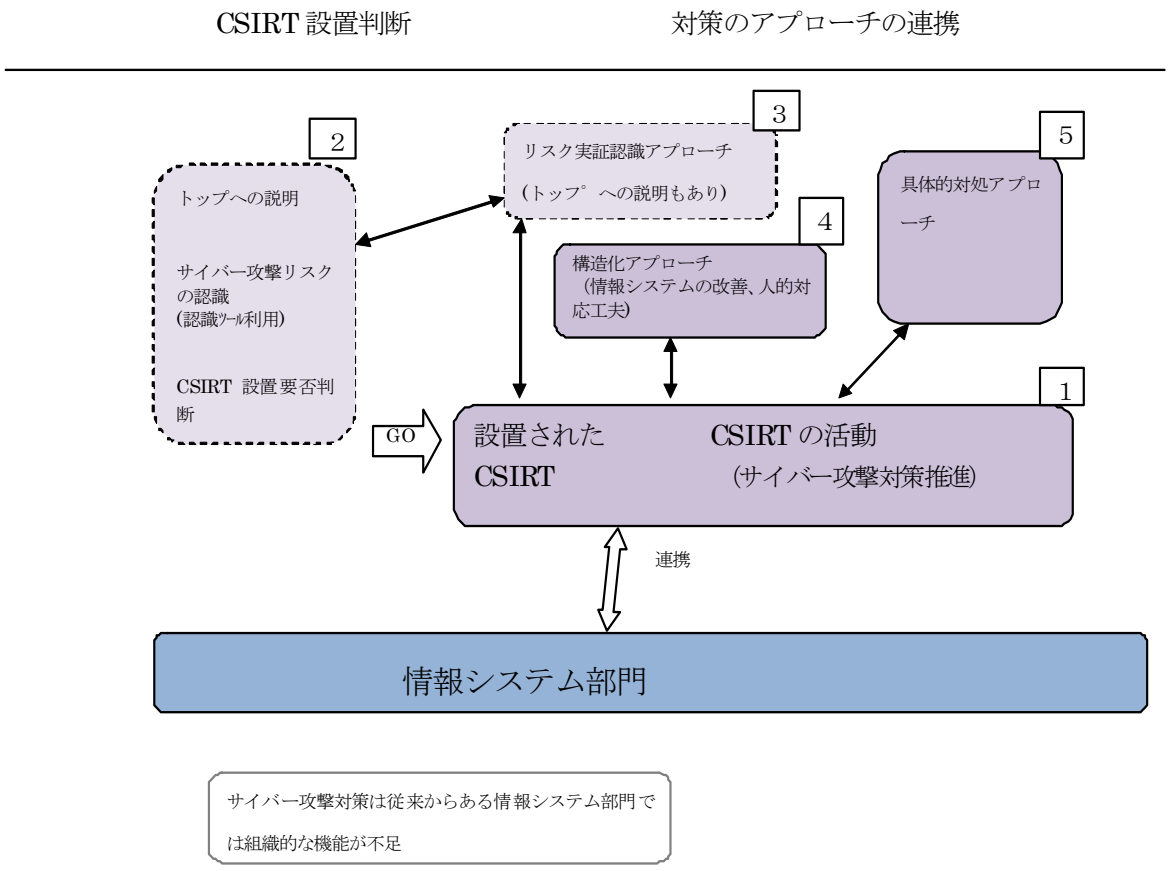
	現状の課題	対策
1	サイバー攻撃対策の必要性を十分に認識していない	CSIRTを設置することを決断（組織的アプローチ）
2	サイバー攻撃リスクを認識していない	経営者にリスクを認識させる（ツールと技法によりリスク認識を図る）
3	経営者はサイバーリスクが自社には無縁のものとの認識である	リスクの見える化によりサイバーリスクへの認識を見直す（実証的アプローチ）
4	自社のセキュリティ対策の実態を把握していない	保護する情報の情報システム上の位置づけを見直すなど（構造的アプローチ）
5	サイバー攻撃対策の具体的内容を理解していない	CSIRTとして行うべき具体的対処

（サイバー攻撃対策のための）CSIRTの設置までのフロー



＊：「仮 CSIRT」として動く“人”は、起動要因を受けて行動する役員、責任者(任命される人など)の役割である。
　誰が担当するか企業ごとに異なる。
＊＊：サイバー攻撃が発見されても、情報システム部門で対応するので、CSIRT は設置しないという判断もある。

(サイバー攻撃対策の)CSIRTの設置と攻撃対処のフロー



３．研究の内容

３．１　サイバー攻撃対策（組織的要素）

３．１．１　企業におけるCSIRTの位置づけ

- 攻撃の被害発生時に全社的な判断、行動を可能にするよう、社内の連携を準備する。
- 社内インシデント情報の集約
- 普段の情報管理ルールを策定
- 侵入被害発生時の対処ルールを策定、全社的な判断、行動が可能にするよう、社内の連携を準備する。
- サイバー攻撃に対処する司令塔的役割で実行部隊ではない。

３．研究の内容

３．１．２中小規模企業におけるCSIRTはどうあるべきか

（１）中小規模企業の制限、制約

- 中小規模企業では、情報システムについて十分な技術力を持つ技術者がいない、専任者を置く余裕もない、または情報システムの技術力が不足、などが一般的状況である。（＊）
- 自社のリスクに相応する対策から実施してゆく。

（＊）勿論中には、自社の扱う業務，情報にふさわしい対応体制を持ち、運用している企業が当然あるが比率は少ない。

3．研究の内容

3．1．2中小規模企業におけるCSIRTはどうあるべきか

CSIRT活動のための情報取得の情報源、活動対象	CSIRTの活動、内部処理	活動結果出力・利用
社内 ・社内情報システムに発生する変化情報（各部署） ・社内のインシデント情報 これらを集約する	・サイバー攻撃対策のルール策定 ・社内への対策情報の発信と情報共有計画と管理 ・企業を代表して情報発信 ・情報システム部門との情報交換・連携 ・経営者への情報提供と判断要請 （CSIRT責任者の任命、社内各部署(総務、人事、営業、各業務部署、研究部門）などからの連携メンバの選定）	・社内への共有情報の発信、対策要請 ・サイバー攻撃対策の運用ルールの策定と周知要請 （運用ルールでバックアップ）
社外 ・当社情報システムに関する社外ユーザ及び取引先からの通知・連絡、障害、不具合、変化の情報 ・世間のサイバー攻撃情報 情報取得に努める		・所定機関への届け出 ・同業者、他社と情報交換 ・CSIRT協議会での情報交換 ・必要時の外部機関への支援要請 ・対外活動をするメンバ選定

3. 研究の内容

3. 1. 3必要な資源

No	施策・機能	必要な経営資源			
		金	人材	工数	技術
1	CSIRTの設置(責任者、構成メンバーの任命、機能、情報取得、報告等役割設定)		◎	○	
2	CSIRT運用ルールの策定（＊）	○		◎	○
3	インシデント情報の集約、管理。サイバー攻撃検知要望、支援		○	◎	○
4	侵入後の社内・社外への対処行動案の事前策定。発生時の対応管理		◎	○	○
5	外部から新しい対策情報の取得		◎		○
6	情報交換　社外		◎		○
7	情報交換・周知　社内		○	◎	○
8	サイバー攻撃緊急対応の措置の社内教育を指示	○		○	
9	日本シーサート協議会参加等		◎		○
記号	◎:主要な資源　○:必要な資源				

３．２　ツールと技法からのアプローチ

- 経営者が、自社が攻撃された場合の事業への影響度をイメージできることにより、合理的な対策を講じるための経営資源の提供を決断できる。

- 社員一人ひとりが、担当業務に直結した現実的なリスクをイメージでき、安全に業務遂行できるようになっているのか否かを検証できる。

【サイバーセキュリティダッシュボード】の設置

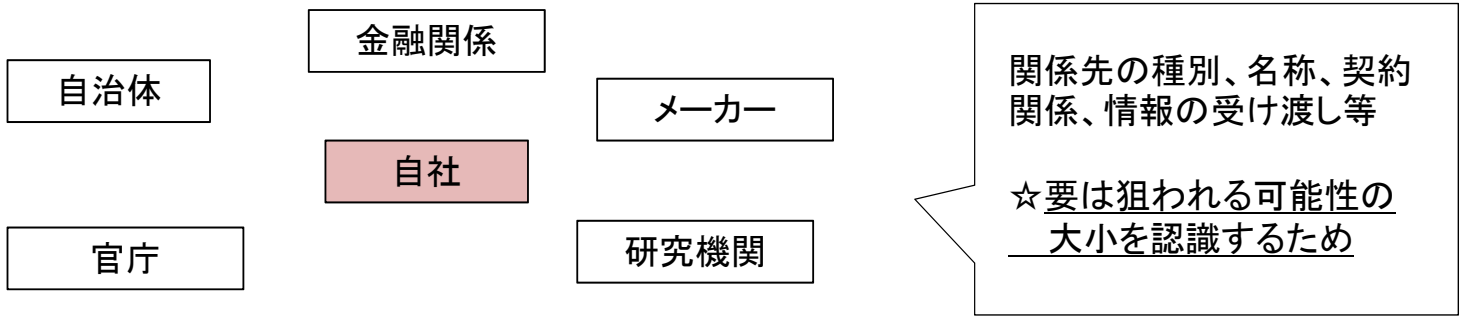
「サイバーセキュリティダッシュボード」の構成

●自社の事業環境の洗い出し

サービス名	売上高	顧客	パートナー
○○サービス	年間売上	利用者、委託元	サプライチェーン

VALUE：権利・ノーハウ	NW・システム環境	重要情報
知財関係の権利、営業秘密、事業上のノーハウ	サービス提供に使用するNW：(インターネット、専用線、無線等) システム：自社内かクラウドか	個人情報（クレジット情報有？、機微情報有？）、具体的な機密情報

●事業展開における利害関係者との関係



「サイバーセキュリティダッシュボード」の構成

●事業展開におけるNW環境詳細

カテゴリ1	カテゴリ2
NW	公衆、無線等
Web	自社HP、サービスサイト
メール	メーラー、ML等
利用・提供しているサービス	オンプレミス、クラウド等
他社とのAP連携	グループ会社等

●自社のネットワーク構成図
●スマートフォン・タブレットの利用状況
●BYOD、SNS利用状況等

「サイバーセキュリティダッシュボード」の構成

●リスク分析結果

- 取扱う情報資産のCIAの喪失
- 知らないうちに加害者になる（踏み台等）
- レピューテーションリスク

●影響度の総括編

カテゴリ	マイナス面評価
財務面	損害賠償額、復旧費用、機会損失による売上減少額
外部利害関係者（業界、顧客、グループ会社、供給者等）	迷惑をかける相手への具体的な影響度
内部利害関係者（従業者）	ボーナス・給与への影響、身売り、倒産

３．研究の内容
その他のアプローチ

- 以降は別途報告、あるいは研究中のサブテーマである

３．３　リスクの実証的アプローチ

- 『「Rsapberry Pi」に構築した模擬選環境によるサイバー攻撃の解析手法の提案』として別途報告

３．４（情報セキュリティ対策への）構造的アプローチ

- 守るものを体系的にセグメント化する（技術的対策）、組織全体の問題として捉え、問題の共有化（人的対策）を確立するなど

３．研究の内容
３．５具体的対策アプローチ

- CSIRTとしてまず整備する事項
  - インシデントを発見する手段の整備
  - エスカレーションルールの整備
- 自社についての情報・知識の集約、情報システムについての把握必須情報
  - 各ネットワーク管理者、責任者
  - ネットワーク構成
  - どこにどういった情報をどのくらい保持しているか

３．研究の内容
３．５具体的対策アプローチ

- ログやイベントの管理
  - 普段よりログ量が増加
  - 業務時間外のログの増減
  - セキュリティアラートの有無
- 外部リソースの活用
  - 外部CSIRT機関やコミュニティとの連携
- CSIRT設置に役に立つ資料の整備
  - CSIRT構築に役立つ参考ドキュメント

３．研究の内容
３．５具体的対策アプローチ

- 各種製品の利用、教育の実施
  - 脆弱性など問題点の事前検査（診断）
    - ペネトレーションテストツール
    - ホワイト/ブラックテスト
    - システム監査
    - 標的型攻撃予防訓練
  - サイバー攻撃を検知・防止するツール（監視）
    - IDS/IPS
    - WAF
    - Firewall
  - インシデント発生後の対応（フォレンジック）
    - フォレンジックツール

４．研究の結果

４．１成果

- 中小規模企業において、サイバー攻撃対策としてCSIRTを設置して行う現実的なアプローチを検討した。
  - ー組織的アプローチ（自社のCSIRT設置必要性の判断）
  - – 経営者にリスクを認識させるツールと技法のアプローチ
  - – リスク見える化の実証的アプローチ

４．２　今後の研究の進め方

- これらはサイバー攻撃対策が進まない事に対する問題解決の提案であり、実証実験を行いこれから検証してゆく。

５．今後の課題

５．１ システム監査が果たす役割（対策状況は妥当か）

- 企業はサイバー攻撃対策を実施する必要があるが、その対策実施状況をどのようにシステム監査するか。
- システム管理基準の中に、直接に該当する項目がない状況である。
- サイバー攻撃対策を考える上でシステム監査をすることも課題ではあるが、当プロジェクトの範囲でなく問題確認に終わっている。
- システム監査学会として、監査基準／管理基準の見直しの問題として取り上げる必要がある。

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　東京都南部労政会館　会議室（山手線大崎駅から5分）　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