

東京都委託事業
団体向けリスクマネジメント普及啓発事業に係る特別支援
「団体向けサイバーセキュリティ向上支援事業」
支援業務 概要について

2019年2月12日

日本電気株式会社
セキュリティ研究所
主席技術主幹
武智 洋

中小企業のサイバーセキュリティにおける課題と環境

中小企業のサイバーセキュリティにおける課題

1. 人材の不足

- ◆ 情報システム部門の有無：組織的な対応は5割程度
(20人以下では約75%が部門がない、もしくは必要に応じて社員・役員が実施)

2. お金の不足

- ◆ コスト負担が大きい(33%)
- ◆ IT導入の費用対効果がわからない(23%)

3. モチベーションの不足

- ◆ 従業員100人以上の企業では50%を超え意識の高さを伺えるが、5人以下では19%となっており、意識向上の課題があると想定

※2017年3月2日 東京商工会議所生産性向上委員会 発行
「生産性向上・ICT活用状況に関するアンケート調査結果報告書」に基づく

中小企業のサイバーセキュリティにおける環境

1. 今後ますますICT/IoTをビジネスに利活用することが重要になる

- IoTですべてがつながる時代には、そのネットワークに入ることが競争力に直結するため、セキュリティをセットとして考えなければならない

2. サプライチェーンにおけるセキュリティ対策がますます重要となる

- 米国基準のレギュレーションが適用される等、日本のサプライチェーンに対する一層のサイバーセキュリティ対策とマネージメントが求められる方向

4つの要件と3つのソリューション

要件

1. 主な脅威に対応可能なこと
2. 使える／使いやすいこと
3. 進化していくこと
4. 持続可能であること

IPA 情報セキュリティ10大脅威

順位	2017	2018
1位	標的型攻撃による情報流出	標的型攻撃による情報流出
2位	フィッシングウェアによる被害	フィッシングウェアによる被害
3位	ウェブサービスからの個人情報の窃取	ビジネスメール詐欺 NEW
4位	リービズ妨害攻撃によるリービズの停止	脆弱性対策情報の公開に伴い増加する脆弱性の悪用増加
5位	内部不正による情報漏えいとそれに伴う業務停止	セキュリティ人材の不足 NEW
6位	ウェブサイトの改ざん	ウェブサービスからの個人情報の窃取
7位	ウェブサービスへの不正ログイン	IoT機器の脆弱性の顕在化
8位	IoT機器の脆弱性の顕在化	内部不正による情報漏えい
9位	攻撃のビジネス化（アンダーグラウンドサービス）	サービス妨害攻撃によるサービスの停止
10位	インターネットバンキングやクレジットカード情報の不正利用	犯罪のビジネス化（アンダーグラウンドリービズ）

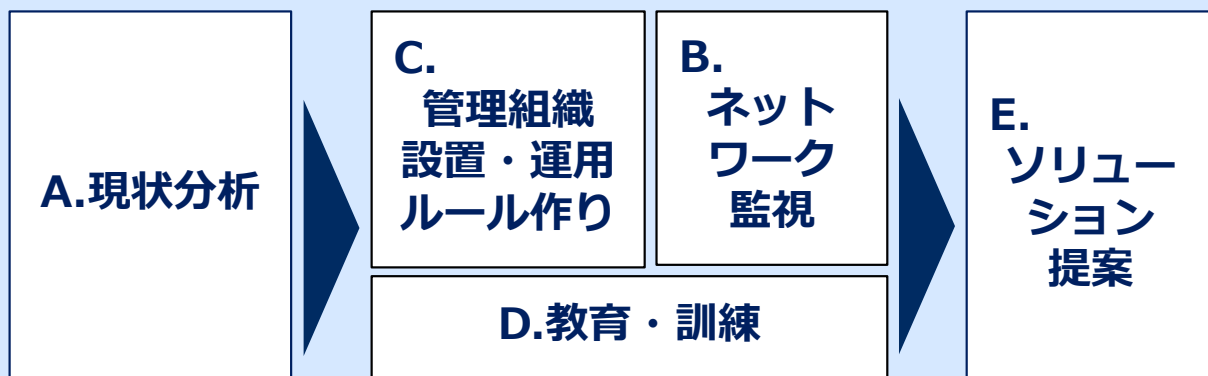
<https://www.ipa.go.jp/security/vuln/10threats2018.html>
<https://www.ipa.go.jp/security/vuln/10threats2017.html>
※年度により項目の表記が異なるが、原文のまま引用

ソリューション

1. 「ゼロコンフィグレーション」、「オペレーションの自動化」、「集中オペレーション」を実現する機器の活用
2. 互助会的組織の設立
3. 持続的なセキュリティ対策コストとビジネスとのバランス

全体の進め方の流れ

大田工連様向け支援モデル事業（本事業）



初年度～3年目まで検証・見直し・改善/発展のサイクルを回していく。

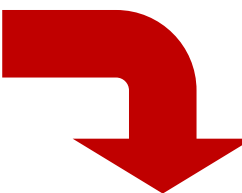
真に有益な
サービス
実現を目指す

視点① 構成管理状況

視点② 脅威／対策へのセキュリティ対応状況

視点③ 組織体制・社規・社内規則等の調査

視点④ 将来意向に関連する調査



事業終了後の
目指す姿

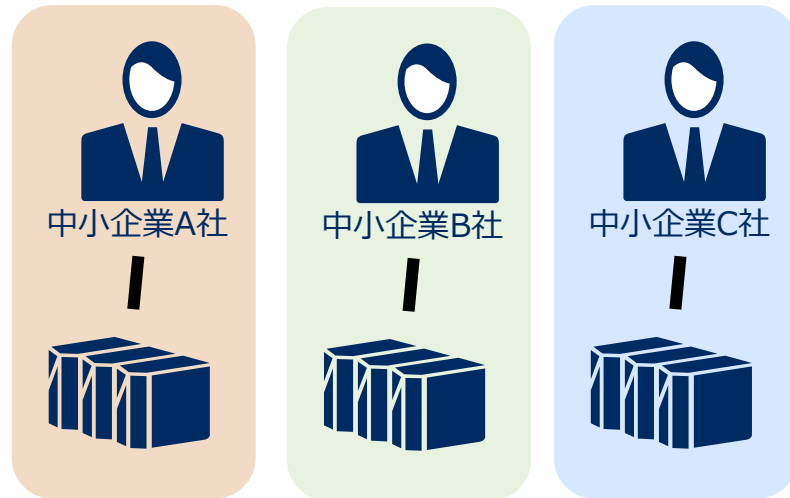
身の丈にあった
機器・サービス
(コスト・手間)

リソースを共有
し、変化に対応
しやすい
相互連携枠組み

持続的なセキュ
リティ対策投資
を生み出す
ビジネス創出

管理組織の目標（個別から共有へ）

従来：各企業様個別のセキュリティ対策



各企業ごとのセキュリティ
リソースへの投資
→規定・ルールもバラバラ

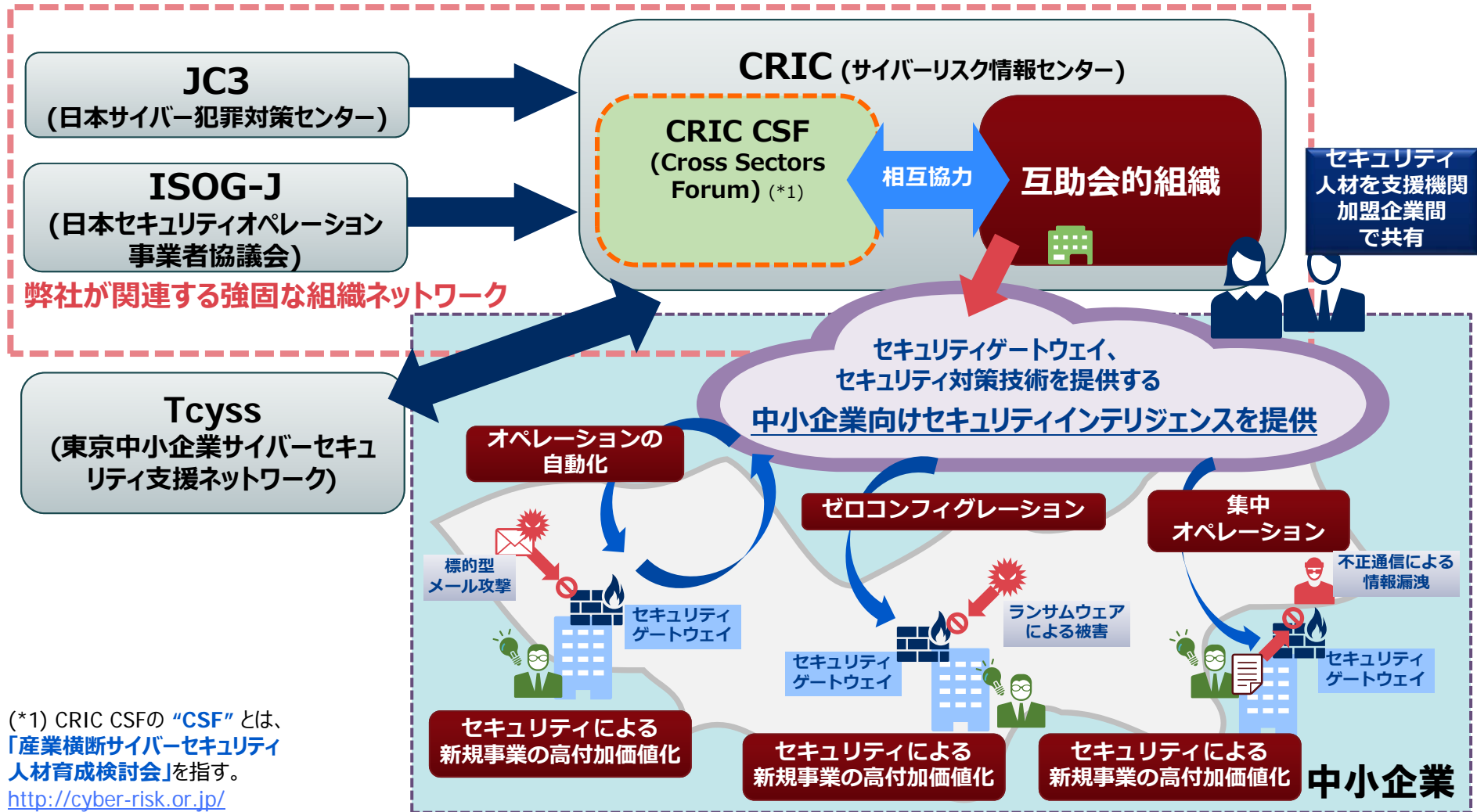


将来：限られたリソースを持ち寄ったセキュリティ対策



規定・ルールの共通化による
セキュリティ対策のリソース
シェアを推進。各企業負荷軽減。

弊社の考える中小企業のサイバーセキュリティのイメージ



いままでの経験からのフィードバック

非常に小さな企業（従業員10名以下）では、セキュリティ人材教育もままならない。

- （極端に言えば）セキュリティ人材なしでも運用可能なセキュリティ対策・施策が必要

クラウドは万能薬ではない

- 中小企業セキュリティでクラウド利用は有効な手段の一つであるが、クラウドにアクセスする部分は、中小企業に残る。
- 工作機械など生産機器も防御する必要がある。

持続できるセキュリティ対策のモデルが必要

- 運用面、コスト面、対策面

管理組織をなくすことはできない

- 各企業が個別にセキュリティ対策するのではなく、可能な限り共通化を行い、共同での対応、リソースのシェアできる体制が必要

共同での対処することのメリット

- コスト面
- Collective Defense の可能性（共同対処、脅威情報の共有【法制度・契約面は要検討】）