Japan Information Security
Management Systems User Group

新解釈！SCS評価制度が普及した未来とは？

日本ISMSユーザグループ　インプリメンテーション研究会

山口　宏治（富士ソフト株式会社）

皆さん、こんな未来を想像したことはあるでしょうか？

「**もし、日本中の企業が高いセキュリティレベルを当たり前に備える社会になったら・・・。**」

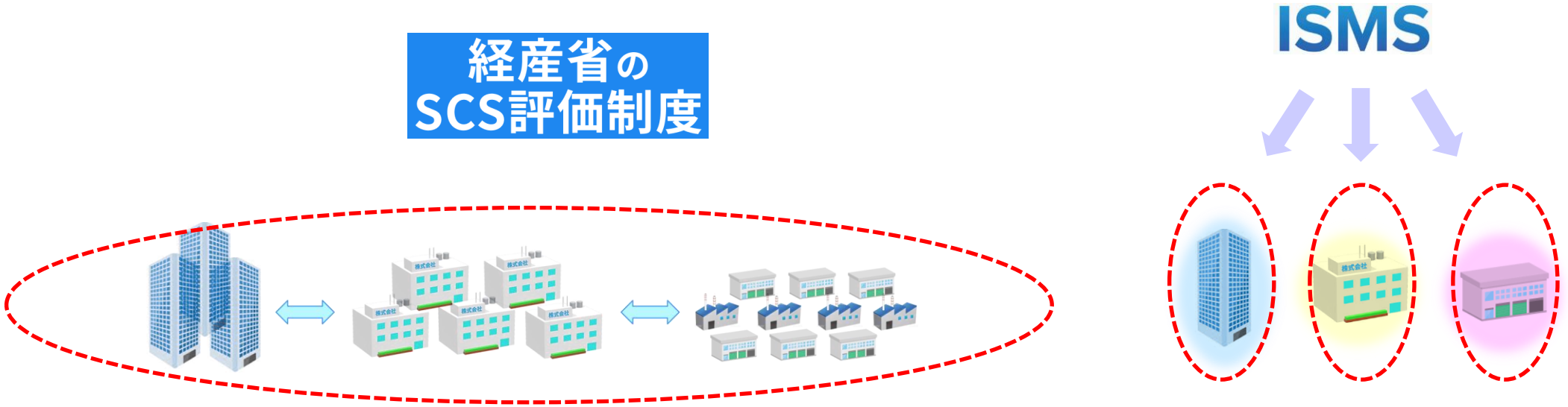
サイバー攻撃は減るのでしょうか。企業間の信頼は高まるのでしょうか。
それとも、新たな課題が生まれるのでしょうか。

今回お話しするテーマは「**SCS評価制度**」です。
しかし、制度の概要や取得方法、要求事項の解説については話しません。

むしろ、この制度が社会に広く浸透し、多くの組織が取り組むようになった未来を想像し、
その先に見えてくる可能性や課題について、皆さんと一緒に考えてみたいと思い、
出来るだけ理解しやすい様に、この資料を作成しました。

是非、皆さんも一緒に考えながら、聞いて頂ければ幸いです。

SCS評価制度の目的は



SCS評価制度は、とても注目度が高く、多くの方が関心を持つ制度と言えるでしょう。

その目的は、サプライチェーンを構成する企業のセキュリティ対策状況を共通の基準で評価・可視化することで、**委託元企業・委託先企業双方の負担を軽減**しつつ、サプライチェーン全体の**セキュリティ水準の底上げを図る**仕組みです。

※経産省HPより引用

経済産業省は、『何を変えたいのか？』を考察

セキュリティ事故を減らしたい

中小企業にもセキュティ対策を浸透させたい

サプライチェーン全体の底上げをしたい

セキュリティを競争力にしたい

CHANGE

評価制度そのものが目的ではなく、
日本企業全体の行動変容が目的

もしも、全国の企業がSCS評価制度を導入したら？

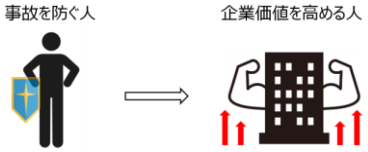
①セキュリティが営業ツールになる

評価が信用になる

②取引条件になる

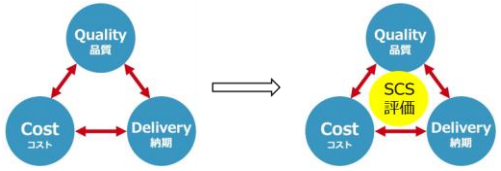
サプライチェーン全体の向上

③セキュリティ担当者の役割が変わる



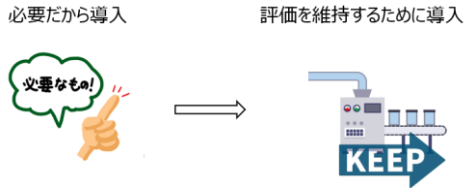
経営への影響が大

④ベンダー選定が変わる



セキュリティが競争力に

⑤中小企業のIT投資が変わる



設備投資の考え方の変化

新たに生まれるビジネス

MENU

SCSコンサル ・・・・・

SCS監査サービス ・・・・・

SCS教育サービス ・・・・・

SCS自動診断ツール ・・・・・

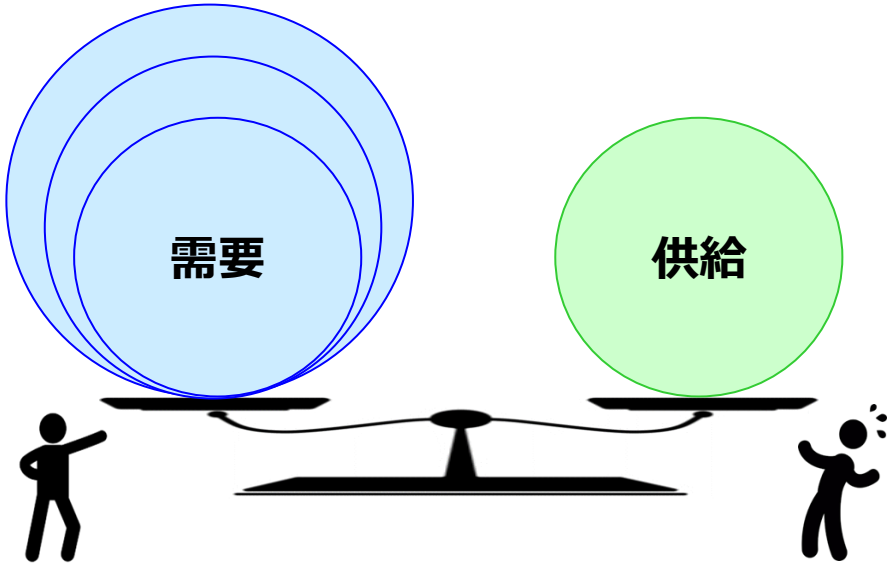
SCS対応クラウド ・・・・・

SCS対応テンプレート販売 ・・・・・

SCS評価制度
スペシャリスト

セキュリティ人材不足について考える

では、セキュリティの仕事が増えたとして、対応出来る人材はいるのでしょうか？

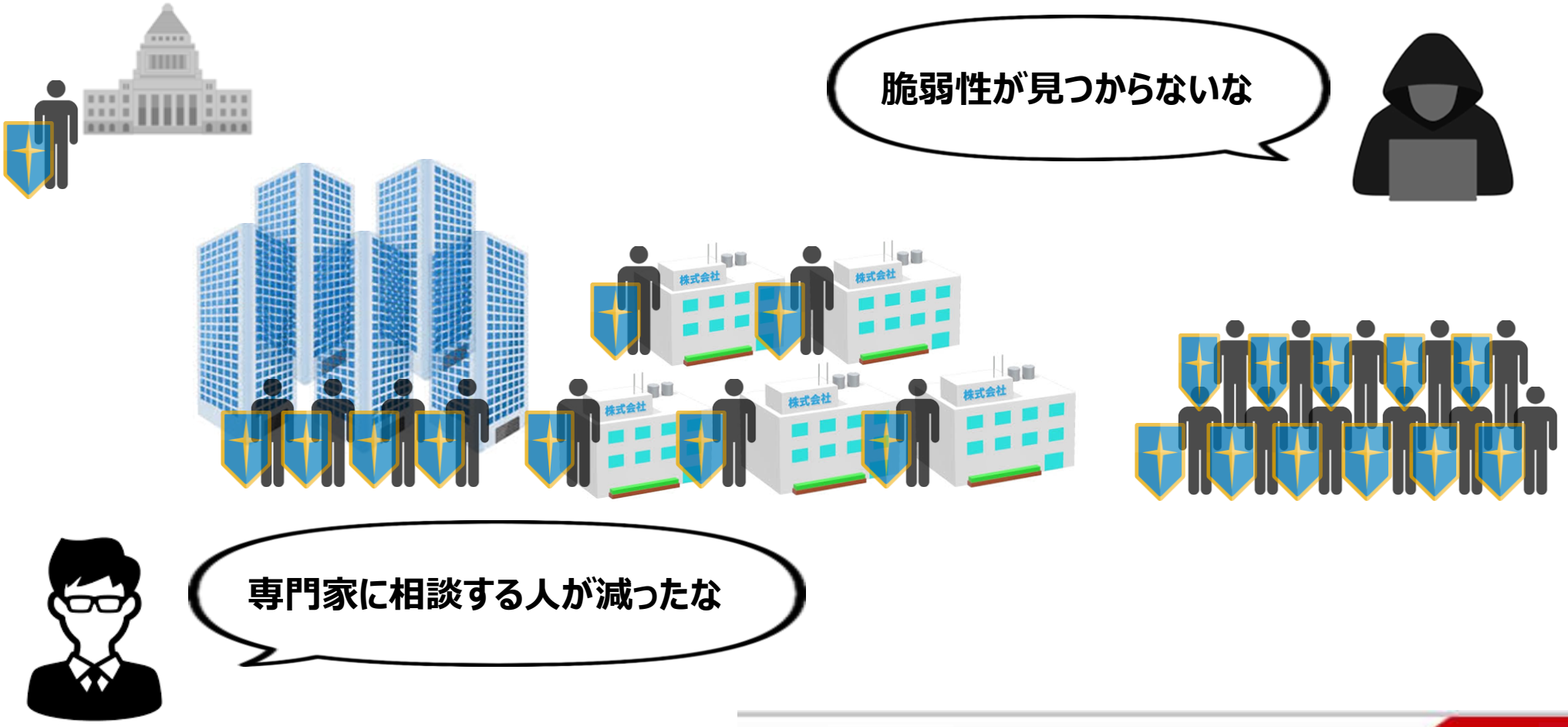


もしも！？

SCS評価制度において、各企業が対策を講じ、社会全体のセキュリティレベルが向上した結果、
セキュリティ人材が増えたとしたらどうなるのでしょうか？皆様も、想像してみてください。

セキュリティ人材が豊富な世界

すべての人がセキュリティ対策を当たり前の様に考え、滞りなく対策を講じているというものです。



セキュリティスペシャリストの育成について考える

もし世界中の人々のセキュリティ意識が極限まで高まり、技術的なミスも脆弱性も、人的ミスも存在しない『**完全に安心な世界**』が実現した場合、その世界は理想郷でしょうか？
更なる問題や課題が発生することも考えられますが、それを目指すという観点で考えてみましょう。

そもそも、今までセキュリティの知識があまりない人が、どうやって**スペシャリストレベル**になるのか？
という課題は残ります。

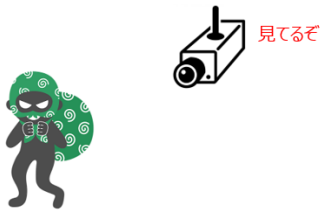
安全な世界は、何もできない世界？

現在の、ITシステムはある程度の利便性とセキュリティのバランスの上に成り立っています。
完全なセキュリティを求めると、以下の様な仕事の効率が著しく落ちる可能性があります。

全て多要素認証 **全通信を厳格に検査** **データ共有は最小限** **持出しは一切禁止**

また、新しい技術は不完全な状態で市場に出てくるということが少なくありません。
もしも、脆弱性がゼロと証明されるまでリリース禁止となれば、新規事業や研究開発の
スピードが大幅に低下するでしょう。結果として、技術進化が鈍化する可能性があります。

完全なセキュリティを実現するには、誰が、いつ、何をしたかを正確に追跡する必要があります。
その結果、常時監視される仕組みが発達するかもしれません。
これは、自由やプライバシーの喪失につながる可能性があります。



つまり、『**安全だが、何もできない世界**』に近づく恐れがあります。

SCS評価制度だけで社会のセキュリティレベルが上がるのか？

最も大きな問題は、『**脆弱性がゼロであることを証明できない**』ことです。
つまり、現実的には、完全なセキュリティは達成できず、100点を目指すではなく、リスクを許容可能なレベルまで下げるという考え方になります。

取引条件としては優秀な制度だと思いますが、日本の企業全体のセキュリティ水準を底上げするには、SCS評価制度だけでは物足りないと考えています。
何故ならば、取引先は変わる、リスクは変化する、インシデントは突発的に起こる。
つまり、セキュリティ対策を1度やって終わりが通用しないからです。

ここで必要になるのが、ISMS（ISO/IEC27001）の考え方です。

ISMSがSCS制度に効果的な5つのポイント

- **①PDCAでやりっぱなしを防ぐ**
- **②リスクベース思考で優先順位がつく**
- **③ルールを組織に定着させる**
- **④経営層を巻き込める**
- **⑤監督・説明責任に耐えられる**

★3の評価基準から見る傾向

ここで、今一度、SCS評価制度の評価基準を見てみましょう。
侵入されない対策を講じるだけでなく、侵入された後の対策が必要と言われてましたが、
AIの進化により、より侵入させない対策に多くの評価基準項目が占めたのかのと思われます。

例：ミュトス

		★3 注
識別	情報資産と脅威の洗い出し、対策すべくリスクを識別する	11
防御	サイバー攻撃などの対策として、適切な防御策を実施する	48
検知	インシデントの発生を検知するための対策を実施する	3
対応	検知したインシデント対応するための対策を実施する	6
復旧	サイバー攻撃などにより失ったデータやサービスを復旧する	1

注：残り12項目はガバナンス領域

SCS評価制度で求められるものと、ISMSにおける運用の比較

課題	SCS評価制度の要求	ISMSにおける運用	
ルールの定着	委託先管理のルール インデント対応のルール セキュリティ基準	文書化 教育 内部監査 マネジメントレビュー	運用を前提とした仕組み
経営層の関与	取引停止の判断が必要 コスト増（セキュリティ対策） リスク受容の意思決定	経営層の関与が必須 リスク承認のプロセスがある	会社の意思決定にする
監督・説明責任	顧客からのセキュリティ要求 監査、チェック インシデント時の説明責任	証跡（エビデンス）が残る 説明ロジックがある	実施していることを証明
意識してないと起こる現実	担当者依存になる ルールがバラバラ 委託先管理が属人化 インシデント時に混乱する	単発対応 → 継続運用 属人対応 → 組織対応 感覚判断 → リスクベースの判断	作業負担・属人化の回避

つまり重要なのは、SCS評価制度の『**何を守るか（対象）**』から、ISMSの『**どうやって回すか（仕組み）**』を考慮することだと考えます。
そして、SCS評価制度を実施することで、ISMSの重要性に気づくのではないか思います。

SCS評価制度を普及させるには？

日本の全ての企業の皆様に、SCS評価制度を普及させるには、「セキュリティの重要性」を説くだけでは、なかなか動いて貰えないと思います。
むしろ必要なのは、「SCS評価制度に対応しなければならない」から検討するのではなく、「対応することで自社にもメリットがある」と感じて貰うことです。

企業にとって、「**必要性**」×「**手間**」×「**費用**」の3つが問題になります。
この問題をしっかり検討して、社会全体のセキュリティの底上げを目指して欲しいと思います。

何をすればいいのか分からないをなくす	**高そう・難しそうというイメージを壊す**	**やる理由を作る**
⇒ 分かりやすい実施手順	⇒ 安価なパッケージを選択	⇒ 取引や経営上のメリット
やったら仕事が増えるを防ぐ	**専門家に支援して貰う仕組みを作る**	**取得したら終わりにしない**
⇒ 外部サービスの活用	⇒ 専門家による伴走	⇒ 継続運用を浸透させる

ISMS認証を形骸化していると、SCS評価制度対応は難しい？

ISMS認証取得済みの企業がSCS評価制度の対応を求められることがあるかと思います。
しっかりと以下の4点に注力していれば、そんなに難しい対応ではないでしょう。

委託先を資産として管理

IT部門だけでなく、調達部門を巻き込んで対応

契約とセキュリティが連動

経営層が関与

①ISMS認証が、認証維持活動になっている。
→監査前だけの年1回だけの活動になっており、審査に通ることをゴールとしている。

②リスク評価が抽象的
→リスクの洗い出しにおいて、情報漏洩リスクやマルウェア感染リスク等とまとめられており、
どの委託先に機密情報があるか、インシデント発生時にどの取引に影響があるかなどの
具体的な問題や対策が洗い出せていない。

③委託先の管理がアンケートをするだけ
→委託先にチェックシートの送付、回収、保管だけで終了し、内容の確認や分析を行っていない。

PDCAでやりっぱなしを防ぐ

ISMSの本質であるPDCAは重要なポイントです。

- **Plan：リスク評価（どの取引先に問題があるか）**
- **Do：対策（契約･監査など）**
- **Check：見直し（問題が起こってないか）**
- **Act：改善（ルールの更新）**

SCS評価制度を単体で考えると、チェックシートを送って終わりになりがちですが、
ISMSを意識していると、**継続的に見直す仕組み**になります。
これこそが、侵入されない為に行うことの第一歩です。

SCS評価制度に取組み、セキュリティ対策の1歩目を歩み出した企業の皆様には、
継続的対策の一環として、ISMS認証取得も目標にして欲しいと考えています。

「制度だからやる」のではなく、「会社を守るために何をすべきか」を考える。
SCS評価制度を、その意識を変えるきっかけにして欲しいと思います。

ご清聴有難う御座いました。