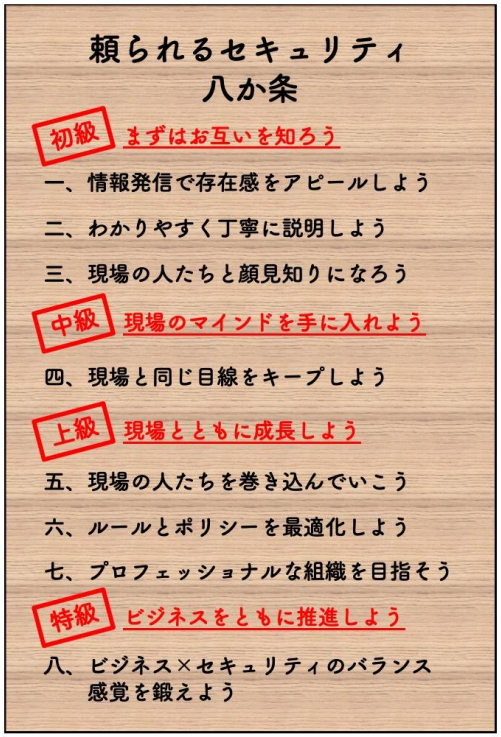
愛されるセキュリティ部門への道すじ
【解説文書】

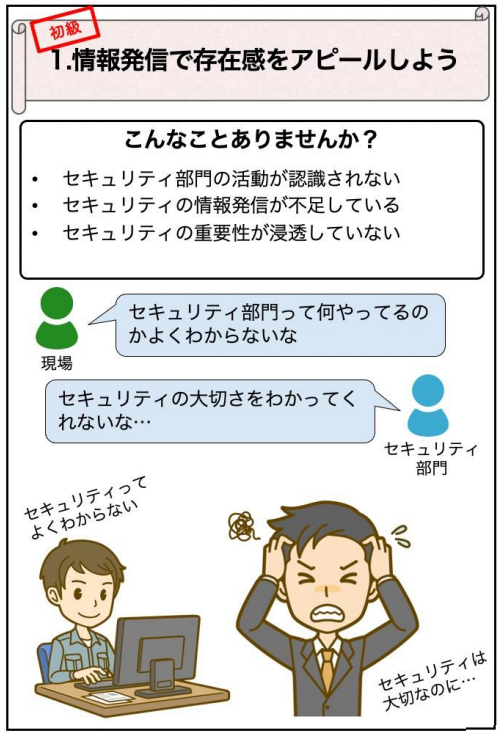
2021年6月

独立行政法人 情報処理推進機構
産業サイバーセキュリティセンター
中核人材育成プログラム第4期受講者
セキュラブ実行委員会

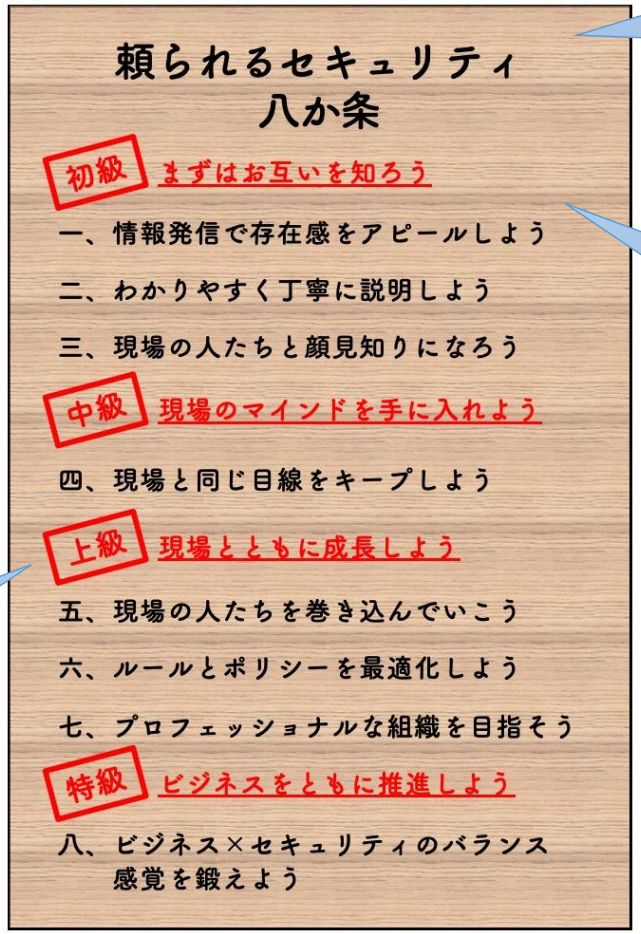
本解説文書について

- 本解説文書は、冊子「頼られるセキュリティ部門への道すじ」に記載の「頼られるセキュリティ八か条」の内容について、それぞれの取り組みの背景となる問題意識と、取り組みの狙いについて解説するものとなります。
- 冊子と合わせて読んでいただき、自社での取り組みにぜひご活用ください。





0. 頼られるセキュリティ八か条



実践したい内容を八か条に集約しています。

初級から順に、実施できているか確認していきましょう！

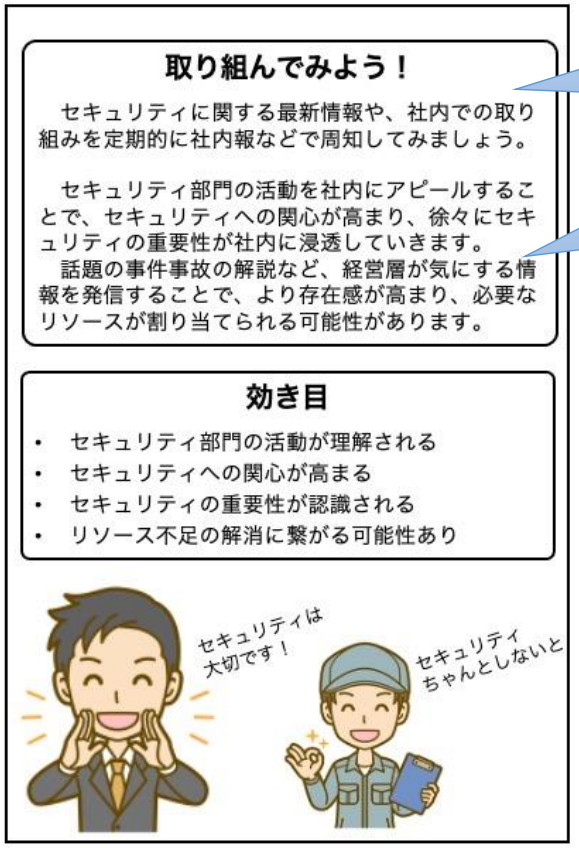
上級以上は時間をかけてゆっくり目指していきましょう。

セキュリティ部門への不満や成功事例についての生の声を集め、そこから絞り込んだ8つの対策を、「頼られるセキュリティ八か条」として表現しました。
対応の難易度順に上から並んでいるので、自部門で実施できていないものから、順番に対策していってみてください。
また初級から特級の4段階のレベルで分けており、各級で共通する目的を一言で表しています。こちらも意識しながら、一つ上の級を目指して取り組んでいきましょう。

1.情報発信で存在感をアピールしよう

セキュリティ部門って何やってるのと言われたことありませんか？

わからないからやらなかったと言われたことありませんか？



社内報などで広く定期的に周知するのがPOINT!

話題の事件事故の解説は関心度が高く効果的！業務に関する内容なら◎

【問題意識】
　現場はセキュリティ部門が何をしているかわからず、セキュリティの取組みを何のために、何を行えばよいかが伝わらないことがある。
　その結果、セキュリティ部門からの依頼は理解されず、セキュリティの取組みが会社内へ浸透していかないという問題が見られる。

【取り組みの狙い】
　セキュリティ情報やセキュリティ部門の活動を発信することで、セキュリティ部門の存在を知ってもらうとともに、セキュリティを身近に感じてもらうことを目指しましょう。
　会社内へセキュリティを浸透させる「はじめの一歩」として、自部門で実施できる情報発信を本書における最初の取組みとしました。

2.わかりやすく丁寧に説明しよう

他部署の人にとっては本業ではないので後回しにされがちと感じたことはありませんか？

「わかりやすく丁寧に」の秘訣は、相手の理解度に合わせること！

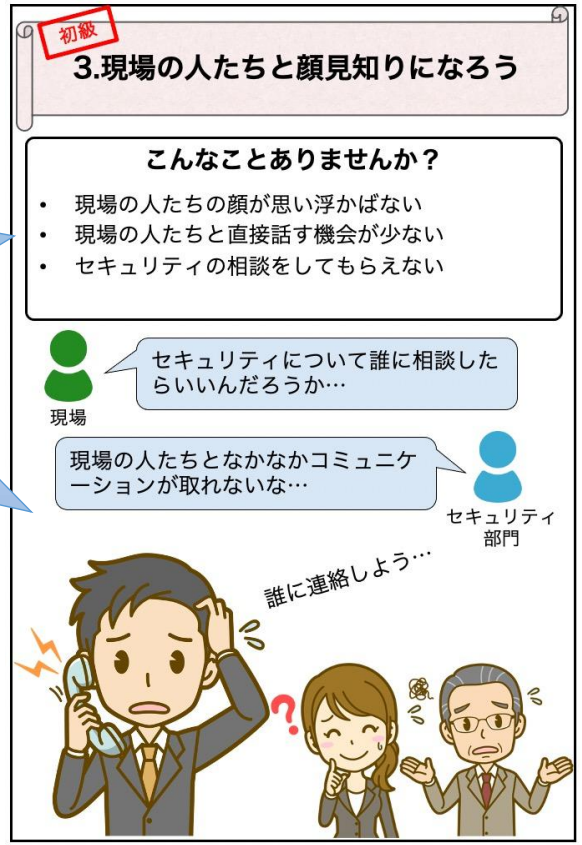
【問題意識】
セキュリティ部門の業務は専門知識を要するためか、自然と専門知識が前提となる話しぶりであったり、専門用語が混ざってしまいがち。結果として説明の労力を省く形になることも多く、後回しにされがちな本業以外の業務の中でもさらに後回しにされがちとなっている。

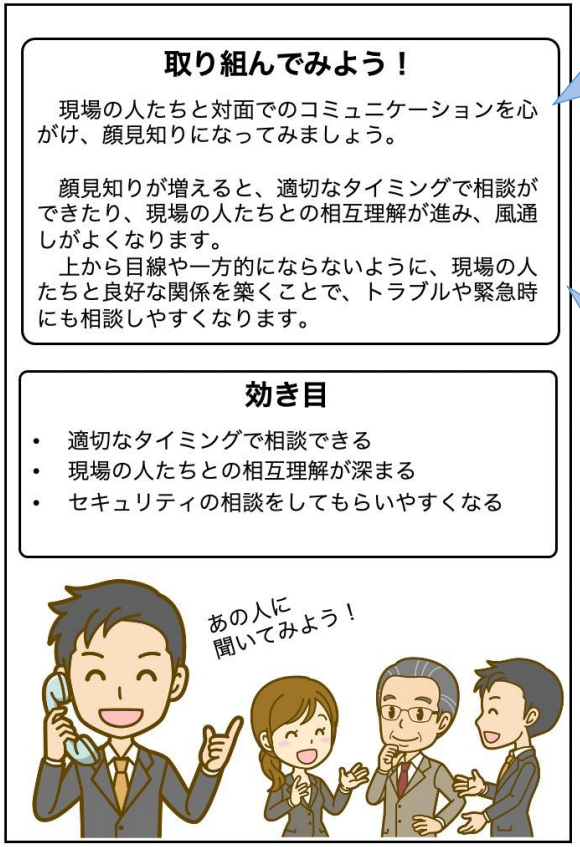
【取り組みの狙い】
普段面倒で省略しがちであっても、都度都度説明する、会話する経験を積んでいくことで多少なりとも論理的思考力や説明力、コミュニケーション能力が上がっていきます。
以降の八か条を実践する上での基礎的な部分でもあるため、初級編として位置づけました。

3.現場の人たちと顔見知りになろう

現場に顔見知りの人がどれだけいますか？相談はしやすい雰囲気が作れていますか？

連絡したいときにすぐに連絡出来ないことが、セキュリティ向上の障壁になっていませんか？





可能であれば対面でのコミュニケーションが◎お互いの顔を知り、相互理解が進みます！

ときには無理な相談をされ、ついつい上から目線や一方的になることもあるので要注意！

【問題意識】
現場とのコミュニケーションが不足しているために、セキュリティ部門が現場の連絡先を把握していない。
現場もセキュリティ部門への連絡手段がわからず、セキュリティに関する相談を気軽に出来ない。また、顔のわからない相手からの依頼に対応するのは面倒という気持ちも生まれる。

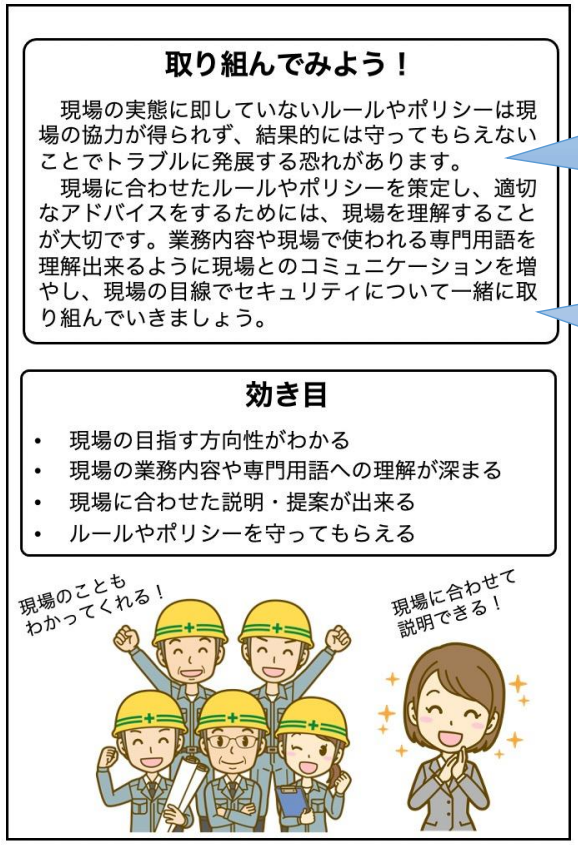
【取り組みの狙い】
セキュリティ部門と現場とのコミュニケーションを活発に行うことで、お互いの顔を知り、相互理解を徐々に深めていける良好な関係性を築くことが出来ます。コミュニケーションの継続こそが現場理解力を高めていくための入り口であり、気軽にセキュリティ部門に相談できることが、セキュリティ向上の一歩となります。

4.現場と同じ目線をキープしよう

現場の事業の目的とセキュリティの目的の目線がずれていると感じたことはありませんか？

現場の経験がなく、何をやっているのかわからないと思うことなはないですか？

ガイドラインやフレームワークを自社にそのまま当てはめてしまってませんか？



現場と共通の言葉で話ができるとコミュニケーションがしやすくなります！

現場の理解が進むとルールやポリシーの問題点が見えてくるかも

【問題意識】
現場の業務を理解していないまま、ルールやポリシーにあるからと一律の説明をしたり、杓子定規な対応をしてしまっている。
現場での業務経験がなく、現場が何をしているかわかっていない。現場からルールやポリシーについて、自分たちの実態にあってないと不満を言われる。

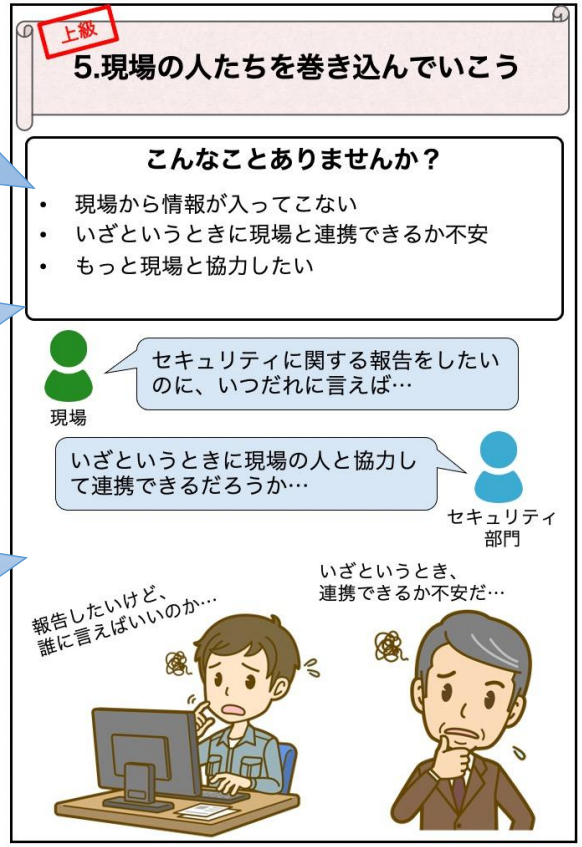
【取り組みの狙い】
現場の実態に即していないルールやポリシーは、結果的に守ってもらえなくなります。
現場に合わせたルールやポリシーを策定するためには、まず現場の理解が重要となってきます。
現場を理解し、現場の目線で考える取組みを進めることで、お互いにとってWin-Winとなるような提案などができるようになります。

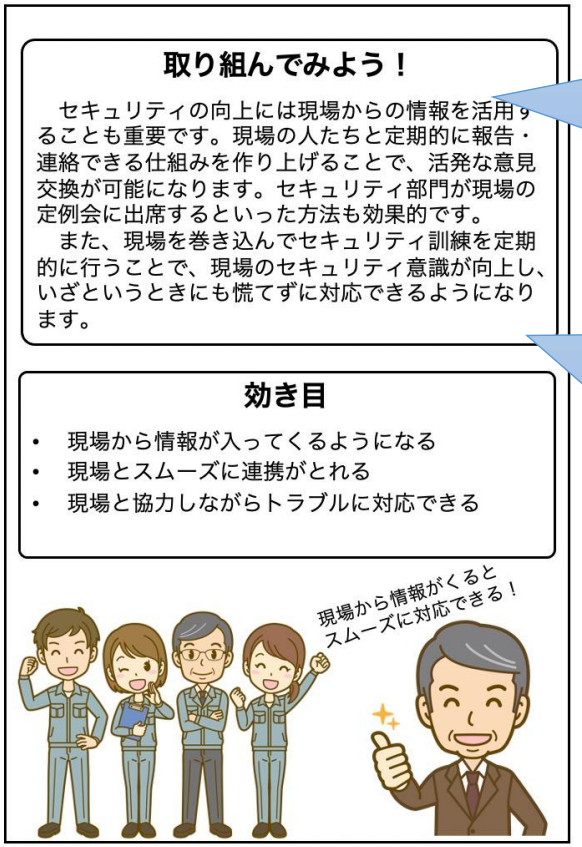
5.現場の人たちを巻き込んでいこう

現場で何に困っているか知っていますか？

問題が発生した時には円滑に対処できる自信がありますか？

単独でセキュリティ対応をしていませんか？現場と協力していますか？





やみくもに製品導入やルール追加するのはNG！現場の声を聞き、必要なこと、できることを実施することが大切です。

セキュリティ事象は初動が重要です。いざという時に慌てず対応できるよう定期的なセキュリティ訓練を実施しましょう。

【問題意識】
現場からの情報連携がないため、セキュリティ上の課題・問題を把握できていない。
現場も報告・相談したくても誰にすれば良いかわからない。
ルールや運用は存在するが、セキュリティ事象が発生することはあまりないため、いざという時に円滑に対処できるか不安。

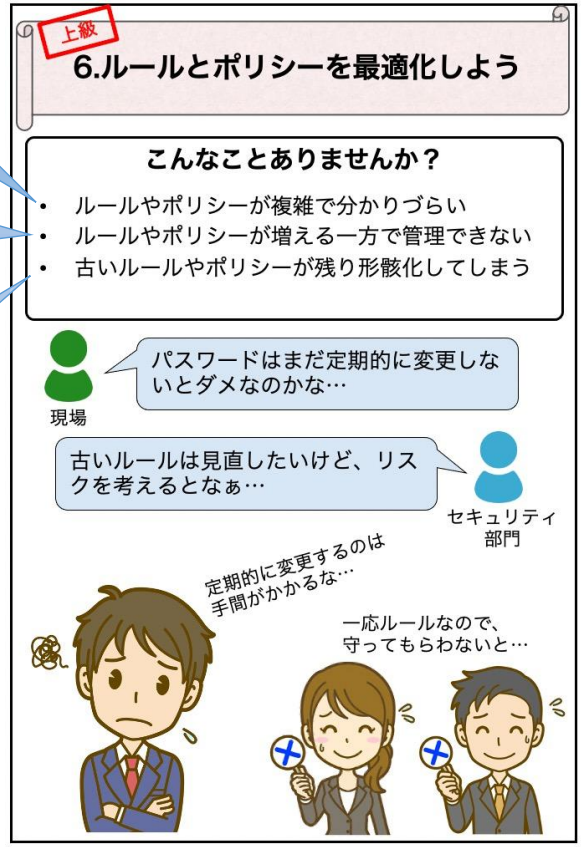
【取り組みの狙い】
セキュリティはセキュリティ部署だけで作るものではなく、現場と協力しながら作り上げていくものです。
世間のセキュリティ状況だけではなく現場の情勢も刻々と変化します。柔軟・円滑なセキュリティ対応をするために定期的な情報連携の場を設けたり訓練をすることが重要です。

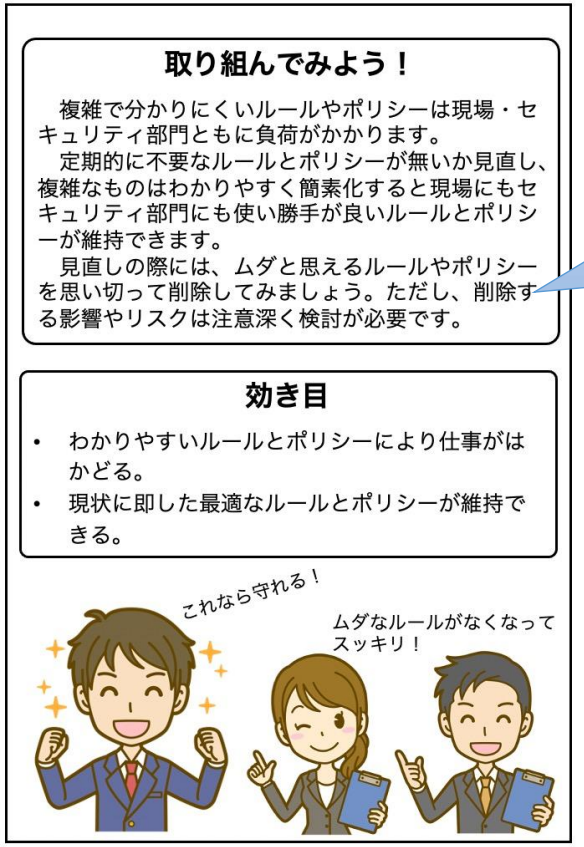
6.ルールとポリシーを最適化しよう

ルールが複雑だと思ったり、言われたことはありませんか？

ルールが多くて管理が煩雑と思ったことはありませんか？

ルールを廃止したことがありますか？





経営はまず無駄を省くところから。
ルールにおいても同じことが言えます。

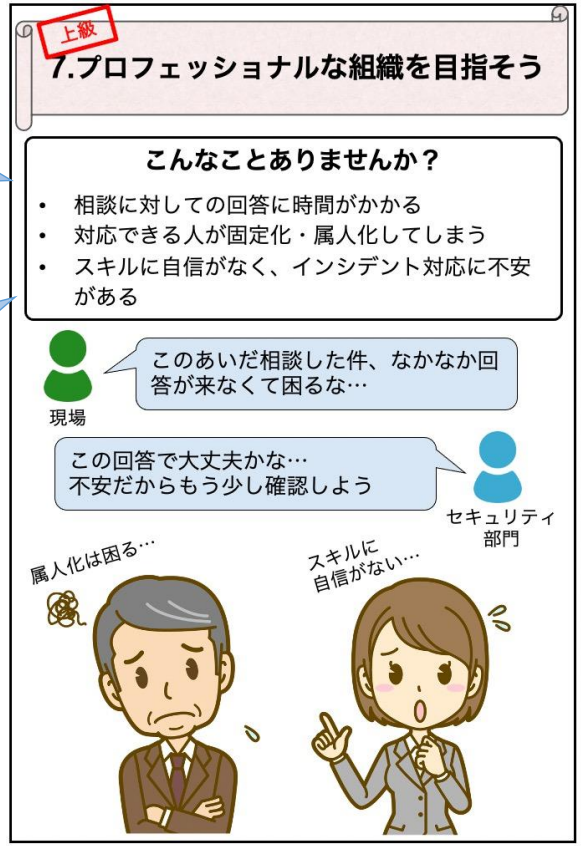
【問題意識】
形骸化したポリシーや複雑なポリシーが多く存在しており、現場ではポリシーを守る必要性を感じれなかったり、対応のスピード感が落ちてしまったりする。セキュリティ部門でも、守ってもらうための説明がつかなかったり、判断に時間がかかったりと、運用において手間がかかる一方となっている。

【取り組みの狙い】
ルールが整理されないことによるデメリットを考慮し、まずは「減らす必要がある」という意識を持つことが重要です。
最適化されたルール・ポリシーはセキュリティ部門・現場の双方にメリットがあります。
必要なルールは残しつつ、定期的に見直す機会を作るようにしましょう。

7.プロフェッショナルな組織を目指そう

現場からの相談に慎重になりすぎることはないですか？

知識のある人に対応が集中してしまってませんか？



部門全体のレベルアップを行い、チームでの対応を目指しましょう！

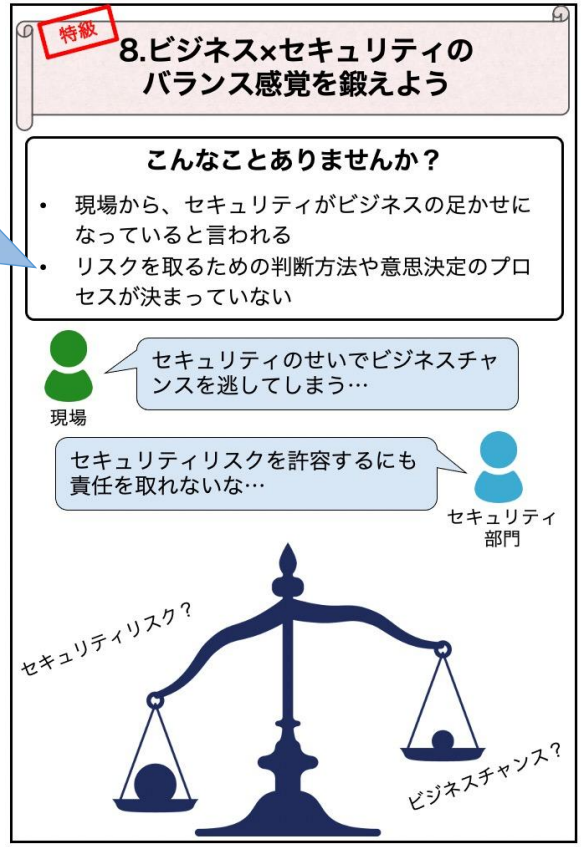
スキルの成熟には時間がかかります。外部講習への参加やインシデント対応訓練を繰り返しながら、少しずつ進めましょう。

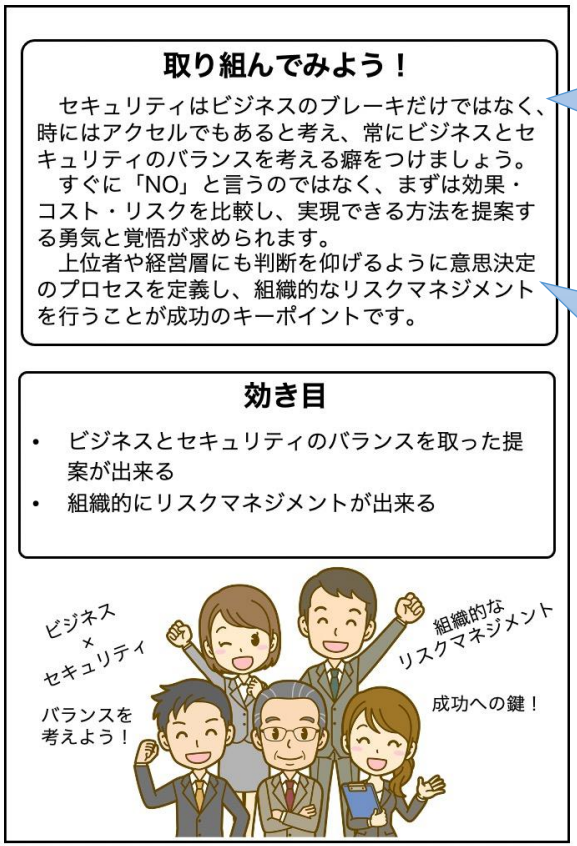
【問題意識】
キーワードは「スキルへの不安」と「属人化」。セキュリティは確実な正解が無い分野のため、判断に自信が持てず慎重になりすぎたり、知識・スキルのある人に対応を任せてしまったりする。それらは現場目線では「対応の遅さ」や「たらい回し感」に繋がり、セキュリティ部門への不満や不審感として表れてしまう。

【取り組みの狙い】
個人のスキルアップももちろん重要ですが、ここでは部門全体として必要なスキルを身につけることに主眼を置いています。チームで対応・解決を目指しましょう。
プロフェッショナルな部門となることは、次の「ビジネスとセキュリティのバランスを取る」ことにも繋がります。

8.ビジネス×セキュリティのバランス感覚を鍛えよう

セキュリティ部門がルールを守るためだけに活動する組織になってませんか？





セキュリティとビジネスのバランスを取る意識が重要！

経営層を説得するために他社事例を集めておくのもポイントです！

【問題意識】
現場業務の効率化や、新しいビジネスを始めるためのシステム導入について相談を受けた際に、セキュリティを理由にストップをかけることが多い。
インシデントが発生したときの会社への被害やセキュリティ部門としての責任を想像すると、部門としてリスクを取ることにためらう。

【取り組みの狙い】
セキュリティとビジネスは両輪のようなバランスが求められるため、時にはリスクの許容も含めてセキュリティマネジメントを推進する必要があります。
リスクマネジメントのためには経営層も巻き込み、組織全体で意思決定できる状態を目指しましょう。