

頼られる
セキュリティ部門への
道すじ



～もっと頼られるはじめての一步～

はじめに

セキュリティ部門がセキュリティを推進していくには、現場（他部門）の人たちとの協力が不可欠です。

一方で、セキュリティ部門は「面倒な対応を押し付けてくる」などネガティブなイメージを持たれてしまい、協力を得づらいつ感じること多いのではないのでしょうか。

私たちは、セキュリティへの不満や成功事例についての生の声を集めて分析しました。その結果を**”頼られるセキュリティ八か条”**に集約し、現場とセキュリティの距離を縮める**”道すじ”**としてまとめています。

八か条は初級～特級の4段階に分かれていますので、**”はじめの一歩”**として、みなさん一人一人ができそうなものから取り組み、**”もっと頼られるセキュリティ部門”**の実現に活用いただければ幸いです。

頼られるセキュリティ 八か条

初級

まずはお互いを知ろう

- 一、情報発信で存在感をアピールしよう
- 二、わかりやすく丁寧に説明しよう
- 三、現場の人たちと顔見知りになろう

中級

現場のマインドを手に入れよう

- 四、現場と同じ目線をキープしよう

上級

現場とともに成長しよう

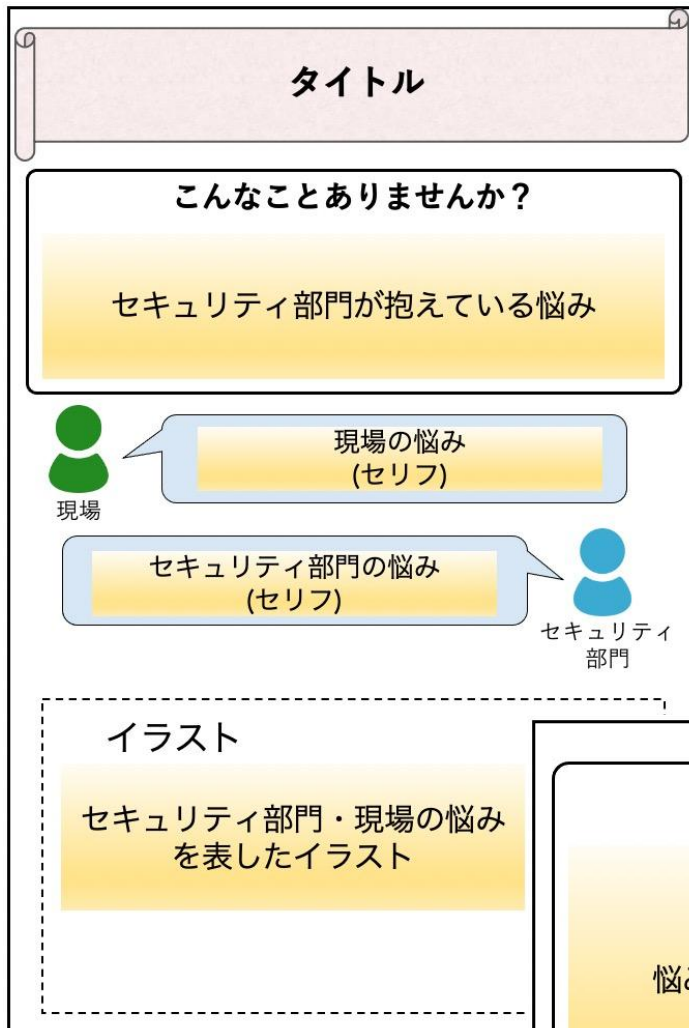
- 五、現場の人たちを巻き込んでいこう
- 六、ルールとポリシーを最適化しよう
- 七、プロフェッショナルな組織を目指そう

特級

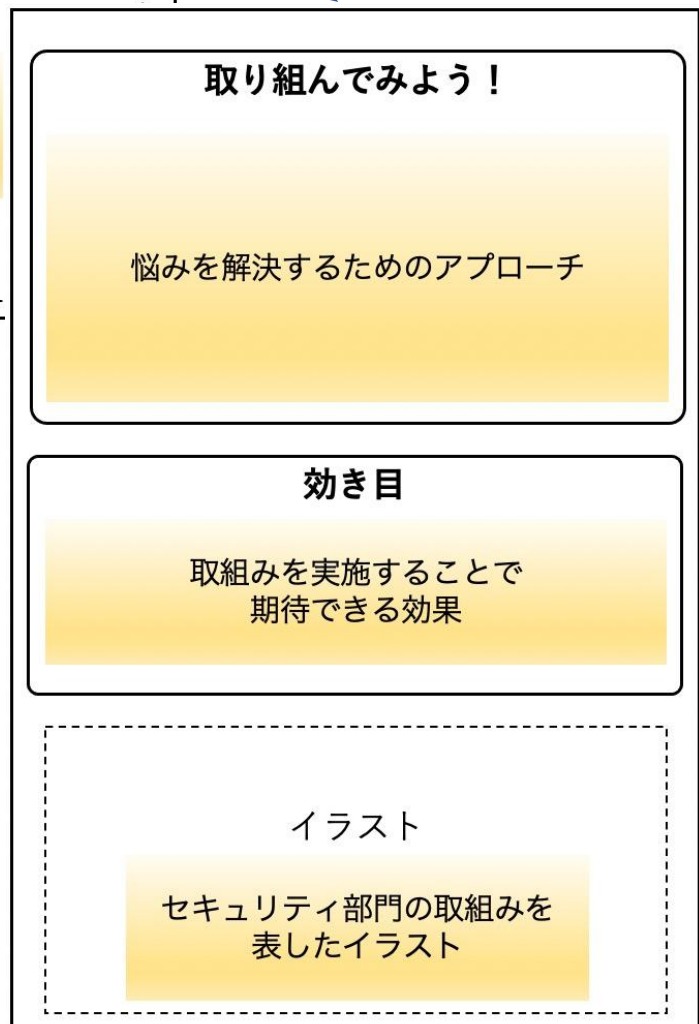
ビジネスとともに推進しよう

- 八、ビジネス×セキュリティのバランス
感覚を鍛えよう

本書の構成



一か条ごとに、
見開き2ページ構成



- 1ページ目
- ・タイトル
 - ・こんなことありませんか？

- 2ページ目
- ・解決のためのアプローチ
 - ・期待できる効果

初級

1.情報発信で存在感をアピールしよう

こんなことありませんか？

- セキュリティ部門の活動が認識されない
- セキュリティの情報発信が不足している
- セキュリティの重要性が浸透していない



現場

セキュリティ部門って何やってるのかよくわからないな

セキュリティの大切さをわかってくれないな...



セキュリティ部門

セキュリティってよくわからない



セキュリティは大切なのに...

取り組んでみよう！

セキュリティに関する最新情報や、社内での取り組みを定期的に社内報などで周知してみましょう。

セキュリティ部門の活動を社内にアピールすることで、セキュリティへの関心が高まり、徐々にセキュリティの重要性が社内に浸透していきます。

話題の事件事故の解説など、経営層が気にする情報を発信することで、より存在感が高まり、必要なリソースが割り当てられる可能性があります。

効き目

- セキュリティ部門の活動が理解される
- セキュリティへの関心が高まる
- セキュリティの重要性が認識される
- リソース不足の解消に繋がる可能性あり



セキュリティは
大切です！



セキュリティ
ちゃんとしないと

初級

2.わかりやすく丁寧に説明しよう

こんなことはありませんか？

- 専門用語ばかりで分かりにくいと言われる
- 必要性がわからないと言われる
- 期限を守ってもらえないことが多い



現場

専門用語が多いし、やる意味もわからない…後回しにしてしまおう

依頼しても理解してもらえないし、期限も守ってもらえない…



セキュリティ部門

専門用語多いし、何言ってるんだろう…



なかなか理解してもらえないな…



取り組んでみよう！

現場への依頼や対応を行う際には、なるべく専門用語を使わず、相手の理解度に合わせて丁寧に説明しましょう。

「社内規程」「セキュリティ上必要」ではなく、必要性やメリット・デメリットを説明すると相手の理解が得られ、スムーズなやり取りが見込めます。

情報開示の問題等で説明できない場合は、説明できない理由を伝えると相手の納得感が高まります。

効き目

- 相手の理解が得られやすくなる
- 納得感をもって対応してもらえる
- 期限を守ってもらえる可能性が高まる

わかりやすく
丁寧に！



なるほど！

初級

3.現場の人たちと顔見知りになろう

こんなことありませんか？

- 現場の人たちの顔が思い浮かばない
- 現場の人たちと直接話す機会が少ない
- セキュリティの相談をしてもらえない



現場

セキュリティについて誰に相談したらいいんだろうか…

現場の人たちとなかなかコミュニケーションが取れないな…



セキュリティ
部門



取り組んでみよう！

現場の人たちと対面でのコミュニケーションを心がけ、顔見知りになってみましょう。

顔見知りが増えると、適切なタイミングで相談ができたり、現場の人たちとの相互理解が進み、風通しがよくなります。

上から目線や一方的にならないように、現場の人たちと良好な関係を築くことで、トラブルや緊急時にも相談しやすくなります。

効き目

- 適切なタイミングで相談できる
- 現場の人たちとの相互理解が深まる
- セキュリティの相談をしてもらいやすくなる



中級

4.現場と同じ目線をキープしよう

こんなことありませんか？

- 現場と同じ方向を向いていない気がする
- 現場のことを理解できていない
- 現場に合わせた説明や提案ができない
- 現場からルールやポリシーの不满がくる



現場

このままのセキュリティルールだと
業務が回らないな…

現場のことをもっと理解しないと不
満ばかり言われてしまうな…



セキュリティ
部門

現場の業務が
回らないよ…



現場に
合わせるのは
ムズカシイ…



取り組んでみよう！

現場の実態に即していないルールやポリシーは現場の協力が得られず、結果的には守ってもらえないことでトラブルに発展する恐れがあります。

現場に合わせたルールやポリシーを策定し、適切なアドバイスをするためには、現場を理解することが大切です。業務内容や現場で使われる専門用語を理解出来るように現場とのコミュニケーションを増やし、現場の目線でセキュリティについて一緒に取り組んでいきましょう。

効き目

- 現場の目指す方向性がわかる
- 現場の業務内容や専門用語への理解が深まる
- 現場に合わせた説明・提案が出来る
- ルールやポリシーを守ってもらえる

現場のことも
わかってくれる！



現場に合わせて
説明できる！



上級

5.現場の人たちを巻き込んでいこう

こんなことありませんか？

- 現場から情報が入ってこない
- いざというときに現場と連携できるか不安
- もっと現場と協力したい



現場

セキュリティに関する報告をしたいのに、いつだれに言えば…

いざというときに現場の人と協力して連携できるだろうか…



セキュリティ部門

報告したいけど、誰に言えばいいのか…



いざというとき、連携できるか不安だ…



取り組んでみよう！

セキュリティの向上には現場からの情報を活用することも重要です。現場の人たちと定期的に報告・連絡できる仕組みを作り上げることで、活発な意見交換が可能になります。セキュリティ部門が現場の定例会に出席するといった方法も効果的です。

また、現場を巻き込んでセキュリティ訓練を定期的に行うことで、現場のセキュリティ意識が向上し、いざというときにも慌てずに対応できるようになります。

効き目

- 現場から情報が入ってくるようになる
- 現場とスムーズに連携がとれる
- 現場と協力しながらトラブルに対応できる



上級

6.ルールとポリシーを最適化しよう

こんなことありませんか？

- ルールやポリシーが複雑で分かりづらい
- ルールやポリシーが増える一方で管理できない
- 古いルールやポリシーが残り形骸化してしまう



現場

パスワードはまだ定期的に変更しないとダメなのかな…

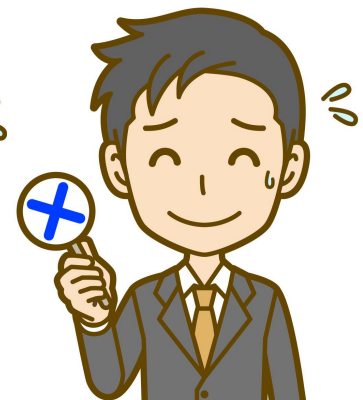
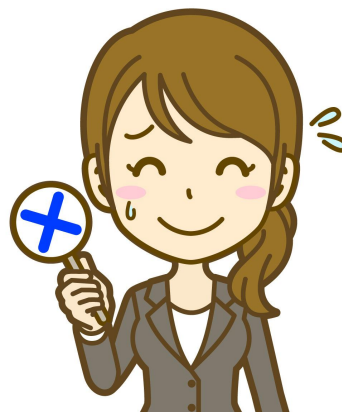
古いルールは見直したいけど、リスクを考えるとなあ…



セキュリティ
部門

定期的に変更するのは
手間がかかるな…

一応ルールなので、
守ってもらわないと…



取り組んでみよう！

複雑で分かりにくいルールやポリシーは現場・セキュリティ部門ともに負荷がかかります。

定期的に不要なルールとポリシーが無いか見直し、複雑なものはわかりやすく簡素化すると現場にもセキュリティ部門にも使い勝手が良いルールとポリシーが維持できます。

見直しの際には、ムダと思えるルールやポリシーを思い切って削除してみましょう。ただし、削除する影響やリスクは注意深く検討が必要です。

効き目

- わかりやすいルールとポリシーにより仕事がかどる。
- 現状に即した最適なルールとポリシーが維持できる。



上級

7. プロフェッショナルな組織を目指そう

こんなことありませんか？

- 相談に対しての回答に時間がかかる
- 対応できる人が固定化・属人化してしまう
- スキルに自信がなく、インシデント対応に不安がある



現場

このあいだ相談した件、なかなか回答が来なくて困るな…

この回答で大丈夫かな…
不安だからもう少し確認しよう



セキュリティ
部門

属人化は困る…



スキルに
自信がない…



取り組んでみよう！

迅速な対応には、セキュリティに精通していることが重要です。スキルマップを定義し、外部講習への参加やセキュリティ資格の取得を積極的に進め、必要なスキルを身につけていきましょう。

セキュリティに関する相談は部門内で情報共有を行うことで属人化を防ぎ、かつ迅速な回答が可能になります。

また、スキルを維持向上するためにも、インシデント対応訓練を定期的に繰り返し実施しましょう。

効き目

- 現場からの相談にすばやく回答できる
- 属人化が解消される
- セキュリティ部門全体のスキルが向上する
- インシデント対応力が向上する

部門全体の
スキルアップ！



すばやく
回答できる！



特級

8. ビジネス×セキュリティの バランス感覚を鍛えよう

こんなことありませんか？

- 現場からセキュリティがビジネスの足かせになっていると言われる
- リスクを取るための判断方法や意思決定のプロセスが決まっていない



現場

セキュリティのせいでビジネスチャンスを逃してしまう…

セキュリティリスクを許容するにも責任を取れないな…



セキュリティ
部門

セキュリティリスク？



ビジネスチャンス？

取り組んでみよう！

セキュリティはビジネスのブレーキだけではなく、時にはアクセルでもあると考え、常にビジネスとセキュリティのバランスを考える癖をつけましょう。

すぐに「NO」と言うのではなく、まずは効果・コスト・リスクを比較し、実現できる方法を提案する勇気と覚悟が求められます。

上位者や経営層にも判断を仰げるように意思決定のプロセスを定義し、組織的なリスクマネジメントを行うことが成功のキーポイントです。

効き目

- ビジネスとセキュリティのバランスを取った提案が出来る
- 組織的にリスクマネジメントが出来る



おわりに

現場の人たちから快く協力が得られれば、セキュリティの向上は今よりもっと進めやすくなるはずです。

そのために、まずは自分たちの行動から変えてみようという熱い思いで、この冊子を作りました。

私たちの目標は、今より**”もっと頼られるセキュリティ部門”**になること、さらに言えば**”愛されるセキュリティ部門”**の実現です。

みなさんも共に、愛されるセキュリティへの道を歩み続けていきましょう。



謝辞

本冊子をまとめるにあたっては、多くの方々のお世話になりました。以下に感謝の意を示します。

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期受講者の皆さまに感謝いたします。皆様から多数のご意見をいただけたことにより、本冊子を作成することができました。心より感謝しております。

阿部 恭一様、鴨志田 昭輝様、茂岩 祐樹様からは、セキュリティ部門運営のノウハウに関する貴重なご意見を賜りました。いただいたご意見は、「頼られるセキュリティ八か条」の検討に大いに参考にさせていただきました。ここに厚く御礼申し上げます。

【監修】

I P A 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講師

満永 拓邦 門林 雄基

【制作】

I P A 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

寺本	翼	清水	慶太
川崎	嗣人	木村	昌雅
酒井	翔悟	酒井	宏尚
松山	幸輝	水田	創



本冊子に記載の内容は (独)情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、制作者の見解に基づきます。



～ Risk少なめTrustマシマシ
Securityバリカタで～



セキュラブ実行委員会 メンバー一同



頼られるセキュリティ部門への道すじ

初版発行 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 (ICSCoE)
セキュラブ実行委員会

「頼られるセキュリティ部門への道すじ」の ご利用について

【著作権】

・「頼られるセキュリティ部門への道すじ」(以下「本冊子」といいます)に関する著作権及びその他すべての知的所有権は、「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“愛されるセキュリティ部署になるには”プロジェクト セキュラブ 実行委員会 (以下、「本プロジェクト」)」及び本冊子中に利用した下記各イラスト制作者等に帰属します。

- ・ イラストAC (<https://www.ac-illustr.com/>)

・ 本作品は、個人、法人組織における非営利目的でのみ、かつ健全な社会通念に反しないことを条件として、本書面の定めに従って事前連絡せずに無償で使用出来るものとします。その他の利用(内容の改変等を含みます)は一切認めませんので、その場合には改めて本プロジェクト及び上記各イラスト制作者等の許諾を得る必要があります。

【免責事項】

・ 本プロジェクトは、本冊子の利用に起因または関連して利用者に生じたトラブルや損失、損害等に対して、一切の責任を負いません。

【注意事項】

・ 本冊子に記載の内容は (独)情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、制作者の見解に基づきます。