



# 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。

## 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の一歩～

### 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

初級

### 1.情報発信で存在感をアピールしよう

#### こんなことはありませんか？

- 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…



# 0. 頼られるセキュリティ八か条

**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

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。こちらを意識しながら、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？

**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

セキュリティ部門: セキュリティの大切さをわかってくれないな...

現場: セキュリティってよくわからない

セキュリティ部門: セキュリティは大切なのに...

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？

## 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



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「はじめの一步」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

**初級**  
2.わかりやすく丁寧に説明しよう

**こんなことありませんか？**

- ・ 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** (Green icon): 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

**セキュリティ部門** (Blue icon): 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...

Illustration: A woman at a computer looks frustrated, saying "専門用語多いし、何言ってるんだらう..." (Too many technical terms, what are you saying...). A man stands next to her, looking thoughtful, saying "なかなか理解してもらえないな..." (I can't get it understood...).

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？

**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

Illustration: The same man and woman are now smiling and talking. The man says "わかりやすく丁寧に！" (Clearly and politely!) and the woman says "なるほど！" (I see!).

「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

**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

誰に連絡しよう…

**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

あの人に聞いてみよう！

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步となります。

# 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すか？

**4.現場と同じ目線をキープしよう**

**こんなことはありませんか？**

- 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満がくる

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…

セキュリティ部門: 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…

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！

現場と共通の言葉で話ができる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。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り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すが、現場と協力していますか？

**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…

セキュリティ部門: 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…

いざというとき、連携できるか不安だ…

報告したいけど、誰に言えばいいのか…

**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う方法も効果的です。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

現場から情報がくるとスムーズに対応できる！

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？

**6.ルールとポリシーを最適化しよう**

**こんなことはありませんか？**

- 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…

**セキュリティ部門**

古いルールは見直したいけど、リスクを考えるとなあ…

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。



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くなったり、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

**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…

セキュリティ部門: この回答で大丈夫かな…不安だからもう少し確認しよう

属人化は困る…

スキルに自信がない…

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いませんか？

**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！

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？

**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…

セキュリティ部門: セキュリティリスクを許容するにも責任を取れないな…

**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

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。