セキュリティ業務を担う人材の現状調査報告書

(2018 年上期調査)

V1.2

特定非営利活動法人　日本ネットワークセキュリティ協会
情報セキュリティ教育事業者連絡会（ISEPA）
2018 年 11 月 2 日

目次

はじめに

NPO 日本ネットワークセキュリティ協会（以下 JNSA）の下部組織にあたる、情報セキュリティ教育事業者連絡会（以下 ISEPA）では、「JTAG（ジェイタッグ）」の活動を 2017 年より開始した。国内の情報セキュリティ事業者やユーザー企業が広く協力して、今後求められるセキュリティ人材の活躍という視点により検討を行っている。

2012 年 4 月に『情報セキュリティ人材の育成に関する基礎調査』[1]の中でセキュリティ人材の不足が発表された。さらに、追加分析[2]も行われ、2014 年に発表されている。そして、2016 年 6 月の『IT 人材の最新動向と将来推計に関する調査結果』[3]により、2020 年には 19.3 万人のセキュリティ人材が不足すると発表された。2018 年に発表された『IT 人材白書 2018』[4]や『情報セキュリティ白書 2018』[5]でも、「人材の不足・確保できていない」という結果が出ており、不足の解消はされていない様相である。

注目すべきは、2020 年に不足すると言われている 19.3 万人を単純に逆算してみると、IT 系企業で 3 万人、ユーザー企業で 16 万人と圧倒的にユーザー企業でセキュリティ人材が不足すると考えられる点である。これは、情報セキュリティ事業者によるサービス提供拡大に伴う不足だけでなく、IT を利用するユーザー系企業のセキュリティ意識や必要性の高まりも起因していると考えられる。

半面、19.3 万人の情報セキュリティ人材の不足を疑問視する声があることも事実である。2018 年 8 月 28 日の日本経済新聞に『セキュリティー人材、消えた「19 万人不足」』[6]という記事が公開された。2016 年の発表から 2 年を迎え、不足すると言われるセキュリティ人材を組織内に確保するよりも、本記事で言われている通り、外部に委託する選択肢を選ぶ企業が出てくることは容易に想像できる。

「JTAG（ジェイタッグ）」の活動では情報セキュリティ事業者だけでなく、ユーザー企業も交えた情報セキュリティ人材を広く調査し、適材適所の人材を検討している。セキュリティの分野がより魅力的な分野となり、長く活躍するキャリア基盤となるよう拡充を推進していく。

最初の調査として、2018 年上期にユーザー企業においてセキュリティ業務に携わる方のヒヤリング調査を実施した。主なヒヤリング対象者は企業のセキュリティ維持向上に関係する業務にあたっている方、企業が提供するサービスのセキュリティ維持向上に関係している方が中心である。本書を通じて、ユーザー企業におけるセキュリティ業務が具体化され、今後のユーザー企業におけるセキュリティ人材の価値向上に寄与できれば幸いである。

※本調査にあたり、社内のセキュリティという観点から、企業名、インタビュー対象者の方々は匿名として発表している。

[1] https://www.ipa.go.jp/files/000014184.pdf
[2] https://www.ipa.go.jp/files/000040646.pdf
[3] http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf
[4] https://www.ipa.go.jp/jinzai/jigyou/about.html
[5] https://www.ipa.go.jp/security/publications/hakusyo/2018.html
[6] https://www.nikkei.com/article/DGXMZO34590330U8A820C1X11000/

1. 調査結果考察

インタビューを依頼するにあたり、『「セキュリティ業務」が何を指すのか』を運営側で定義するのに苦労した。これは、依頼する会社や依頼者の立場により、イメージするセキュリティ業務が違うと想定されたためである。

セキュリティ業務と言っても、CISO・情報システム・総務・人事・法務・リスク管理など多くの部署・担当者がセキュリティに携わっている。最近では CSIRT に代表されるようなセキュリティに特化した部署・チームなども増えているが、「セキュリティと言えば」が全社員で共有できることで、社内セキュリティの業務イメージがつきやすく、キャリアのイメージも描きやすくなると考えられる。

今回の調査にあたり、インタビューをお願いする企業の窓口は社内のセキュリティ事情に精通している方にお願いした。この場合でも、複数の担当者を思い描くことが多く、インタビュー対象者を選ぶにあたり、運営側への趣旨・目的の確認も多かった。社内セキュリティ人材には役割や分担に選択肢があり、キャリア選択の可能性もあると推察できる。

インタビュー対象者は CSIRT 所属を除けば、各部署業務に付随するセキュリティ業務にあたっている方達であった。中には部内でセキュリティ担当を置いているという場合や、部の業務範疇のセキュリティ業務だけ外部へ委託しているといったケースも見られた。また、セキュリティ担当者が研修や勉強会・セミナーへ参加することに寛容な企業が多かった。セキュリティの専門性について一定の理解が得られていると考えられる。（セキュリティ業務について教えられる人材がいない場合も想定できる。）

しかしながら、処遇面で見ると専門性が反映された評価基準にはなっていない企業がほとんどである。CSIRT の場合にはセキュリティ知識・スキルが求められるが、それは各部署が業務を遂行するために求められるノウハウと同等と扱われていると考えられる。逆に、各部署がセキュリティ業務の要素を担う場合では、部署の仕事の範疇とみられていると思われる。CSIRT 自体の地位向上や、『セキュリティ業務』としての認識強化が関係してくることから、JTAG 内「認定 WG」との連携が求められる問題である。

最後に、今回の調査では時代背景や業務命令といった形で、本来業務に加えてセキュリティ業務に携わるきっかけを得ている場合が多かった。現在のセキュリティ需要などを鑑みると、今後はセキュリティ業務につきたいと思い、志すことも増えてくる。しかしセキュリティ業務を志した場合は、セキュリティベンダーでの就業という選択肢があるため、社内セキュリティの業務に取り組む人材の確保は今後ますます難しくなっていくだろう。ユーザー企業として人材確保を考えた場合、採用や育成、キャリア開発などについてキャリアデザインワーキンググループとしても引き続き検討していく事案だと考えている。

今回の調査にはセキュリティサービス事業を提供している会社も含まれており、同じ会社にセキュリティベンダーとしてのセキュリティ人材と、社内セキュリティの人材が存在している。このような企業でも、社内のセキュリティ維持に従事している人材と、セキュリティサービス事業提供に従事している人材の積極的な配置転換は行われていなかった。サンプルが少ないため結論が出せるものではないが、人材の流動化を考えるにあたっては引き続きの調査が必要である。

2. 調査方法

2.1. 調査の目的

セキュリティ業務の担当者や責任者の方の知見やノウハウの共有を行うとともに、セキュリティ業務に携わる方が事前に何を学習および経験しておけば、より円滑にその業務を担うことができるのかを示唆することで、セキュリティ業務に携わる人材の素養を高めるための情報共有を行う。

2.2. 調査期間

2018 年 6 月 ～ 2018 年 10 月

2.3. 調査実施方法

担当者への対面インタビュー
※JTAG賛同メンバーにて実施

2.4. 調査対象企業/調査対象人数

12 社 / 25 名

2.5. ヒヤリング結果のまとめ方

インタビューにてお話いただいた内容を文書化
※インタビュアーの感想、意見は3項ヒヤリング結果には含まれていない。
※発言内容で個人・企業を特定する文言については汎用的な言葉に変更している。

2.6. ヒヤリング対象者分類

グループ 1：自社内のセキュリティ対策の維持・向上を担当している方
(例)・総務をご担当でセキュリティも業務とされている方
・法務をご担当でセキュリティも業務とされている方
・情報システムの管理をご担当されている方
・リスク管理をご担当されている方
・CSIRT ご担当者
・CISO

グループ 2：対外向けサービスのセキュリティ維持・向上を担当している方
(例)・製品/サービス企画でセキュリティも業務とされている方
・製品/サービス構築でセキュリティも業務とされている方
・製品/サービス開発でセキュリティも業務とされている方
・製品/サービス保守でセキュリティも業務とされている方

グループ 3：セキュリティを対象として業務を行っている方
(例)・記者
・トレーナー
・営業
・リサーチ
・法律関係者
・監査関係者
・経営関係者

※今回の調査は、「自社内のセキュリティ対策の維持・向上を担当している方」と「対外向けサービスのセキュリティ維持・向上を担当している方」を中心に行った。

2.7. ヒヤリング項目

1.業務内容の把握
1.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
1.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
1.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無
1.4.「セキュリティ業務」を行う環境（体制）
2.経験談
2.1.「セキュリティ業務」を実施していて苦労した経験
2.2.「セキュリティ業務」をしていてよかった経験
2.3.「セキュリティ業務」をしていて悩んだ経験
2.4.「セキュリティ業務」に着任しての処遇変化
2.5.自社のセキュリティ維持向上に効果が出たという取り組み
3.キャリアパス
3.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)
3.2.「セキュリティ業務」前に行っていた業務内容
3.2.「セキュリティ業務」についたことによるキャリア（観）への影響

※インタビュー対象者の方のご経歴や組織体系により一部変更している場合がある。

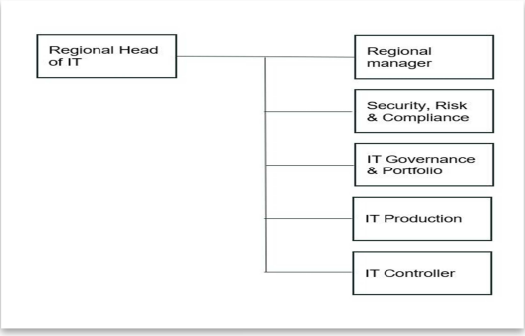
※特にキャリアパスについては、個人に対してのキャリアパスがベースとなるが、複数名でご協力いただいた企業様については、『会社としての考えや方針、または経緯』として記載している場合がある。なお、その際には、項下段に注釈を記載している。

3. ヒヤリング結果

3.1. ケース 1（人材サービス関連：自社内セキュリティ担当）

3.1.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：個人



組織図
業種
人材サービス関連

企業規模

社員数	3000名
システム要員数（内務）	35名
システム要員数（外部委託・派遣）	27名

（インタビュー当時の人数）

3.1.2. 業務内容の把握

3.1.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容

内部統制、監査対応がメインの業務となるが、顧客からくる個人情報保護に関係する質問への対応もしている。主にやっていることとしては、アカウントレビューやログレビューなどになる。部署内にはインシデントレスポンスやバルネラビリティ（脆弱性）チェックを担当している人もいる。さらに、個人情報保護法などに関係する対応は法務部がしている場合もある。

3.1.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容

業務の区切りは明確に分けられない場合が多い。プロジェクトに参加し、要件定義などの際に、セキュリティ観点からのアドバイスを行うなどを現在行っている。

3.1.2.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無

初めてセキュリティ業務についた際には、研修などの教育はなかった。時代的なものもあると思うが、OJT のように業務をしながら覚えていった。ただ、セキュリティ業務を行いながらセキュリティ系の資格（CISSP など）の取得をしていった。現在でも定期的に勉強会やセミナーに参加をしているが費用は自己負担になっている。これは会社の考えなどによるところが大きいと思っている。

海外まで視野を広げるなら、CISSP や CIA の資格は必須と言えるので、上級を目指すなら取得しておくべきだと思っている。これからセキュリティを目指す方やセキュリティに携わって日が浅いと言う方は、色々経験することが大切である。勉強会などに積極的に参加することも大事だと思う。

3.1.2.4.「セキュリティ業務」を行う環境（体制）

基本的にセキュリティ業務は内製化しているので、外注はしていない。社内ではマネージャー1 名とメンバー2 名という体制で行っており、不足を感じている。IT 部門全般としては外注している場合もある。グループ会社では情報システム部門長が責任者を担当していることが多い。グローバル展開する企業なので、CSIRT はグローバルとして存在しており、国内には存在していない。レポートラインも国内で完結しない場合もある。

企業的な特性もあるからか 3 年前後での入れ替わりが多く、入れ替わりの場合には異動というよりも転職による入れ替わりの方が圧倒的に多い。
業務で必要なスキルとしては、監査系のスキルは必要になっている。また、状態を『見える化』するようなツールを導入しており、ツールの見方やその後の対処までわかる必要が出てくる。

3.1.3. 経験談

3.1.3.1.「セキュリティ業務」を実施していて苦労した経験

現職に就く前にしていたセキュリティに関係する業務であるが、人材育成系にかかわることがあった。どういった人材を育てたらよいかを考えるのに苦労したのだが、必要な要素を考えていくと、セキュリティに必要なスキル・技術だけでなく、MBA の内容やファイナンシャル系の内容も必要であると考えられた。経営層には IT 用語を使わずに経営用語と絡めてセキュリティを説明する必要があるとわかると、難しさを感じた。

3.1.3.2.「セキュリティ業務」をしていてよかった経験

一番は面白いことだと思う。世代的なこともあるが、まだセキュリティという言葉が浸透する前から携わってきたことによって、『前任者がいない』『前例がない』という環境での業務を考えながらできたことは良かった。また、セキュリティという業務の性質上、FBI と仕事をする機会もあった。

3.1.3.3.「セキュリティ業務」をしていて悩んだ経験

前例がないので、オフィス新設や事故が発生した場合などに作成するセキュリティポリシーの判断基準をどうすればよいか悩むことがあった。
同僚などとワーキンググループを作り、一緒に作り上げていった。

3.1.3.4.「セキュリティ業務」に着任しての処遇変化

現職にはセキュリティ業務をするために就いているので特にない。セキュリティ業務に携わり始めた当時ではデータセンタ内のインフラを担当していたところから、セキュリティを担当するようになったので『地位』は上がった。

3.1.3.5. 自社のセキュリティ維持向上に効果が出たという取り組み

『見える化』するツールの導入をすることはチェックのしやすさなどを考えたときに効果的であったと思う。
また、社内でネットワークを作ることも有効だった。情報連携がどうしても必要となるので、社内での連携をする必要がある。ただ新規で作ると浸透するまで時間がかかるので、既存のネットワークにセキュリティも交えると連携が早まる。

3.1.4. キャリアパス

3.1.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

自分の意志というよりも、配属されたからという要素が強い。データセンタでのセキュリティ担当になったことからセキュリティのキャリアがスタートした。

3.1.4.2.「セキュリティ業務」前に行っていた業務内容

ネットワーク系のインフラを担当していた。いくつか会社を経験する中で、ヘルプデスクのような業務からネットワーク障害対応、サーバ保守プロジェクトマネジメントなど多く経験したことは役に立っている。学生時代には情報通信工学系の学科にいたが、オーディオ系に関心があったので直接は役に立ったとは感じていないが、独学で PC コンピュータを勉強していたことは役に立ったと思う。

3.1.4.3.「セキュリティ業務」についたことによるキャリア（観）への影響

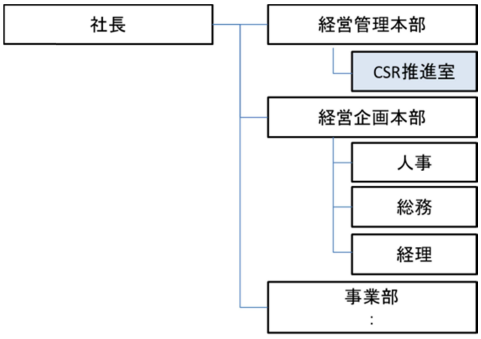
現在の会社でやりたいこととしてはもう少し業務の効率化（外注をうまく使う）など進め

ていきたい。また、プロジェクトに参加することもしていきたいと思っている。個人のキャリアという視点では、今まで満足いくキャリア形成はできていると思っている。今後も自分で決めていきたい。もう少しチャレンジしてもいいと思っている。

3.2. ケース 2（その他金融：自社内セキュリティ担当）
3.2.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：個人

組織図



業種
その他金融

企業規模

社員数	約900名
システム要員数（内務）	約20名
システム要員数（外部委託・派遣）	外部委託（常駐）：約60名

3.2.2. 業務内容の把握
3.2.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
社内の情報セキュリティ施策の推進担当として、社員教育やインシデント対応のほか、情報セキュリティ推進委員会の事務局としてマネジメントレビューの取りまとめなどの業務を行っている。国内外に展開するグループのうちの一企業として、親会社やグループ会社との連携をはかり、グループ全体のガバナンスと自社の独自の施策とのバランスを調整する役割も担っている。

3.2.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
ISO・PMS・EMS・ISMS などの認証維持に関わる業務や、内部監査、リスクマネジメントなどのガバナンス業務、さらには社の CSR 活動全般を担っている。

3.2.2.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無
20 年程前、ISMS と P マークを取得する動きの中で、当時は世間的にもまだ流行りではなかったこともあり進め方がわからず外部のコンサル会社に入ってもらっていた。その外部コンサル会社に内部向けの講習を開いてもらい知識を得た。当時はコンサル料以外の費用をかけて外部に研修に出ることはなかったが、現在は全社的にグループ共通および自社独自の e-learning を年 2 回程度実施している。

3.2.2.4.「セキュリティ業務」を行う環境（体制）
経営企画部配下で CSR 活動を推進する『室』として 3 名。情報セキュリティを業務としているのはそのうち自身を含め正社員 2 名で外部人材の利用はない。事業上の組織とは別に情報セキュリティ推進委員会が存在し、当室がその事務局を担っている。委員会は、営業系の統括部隊・業務系の統括部隊・人事・総務等の約 10 名で構成されており、情報セキュリティマネジメントシステムの運用やマネジメントレビューの答申内容を検討する組織である。委員会の所属要員は決定事項をトップダウンで組織におろせるよう基本的に役員クラスのメンバーで構成されており、テクニカルな企画というよりは業務視点で組織のリスク等を考える場として機能している。
また、個社としての CSIRT は存在していないが、事実上の CSIRT 体制は備えており、情報セキュリティをシステム面でサポートする部隊と当室とで有事の際は対応することになる。その際はもちろんグループの CSIRT とも連携する。

3.2.3. 経験談

3.2.3.1.「セキュリティ業務」を実施していて苦労した経験

事業上致命的なものは発生していないが、現場レベルのインシデントが減らないこと。幸いなことに、インシデントを隠そうとする社風ではなく、仕組みとしてもインシデントが発生すると必ず事務局に情報が回ってくるシステムが構築されている。インシデントの情報は、情報管理責任者だけでなく、発生部門の第一階層にもエスカレーションされ、同様なケース発生が予測される支店や部門などにはもれなく共有される仕組みである。当初は紙での運用だったが、システムで効率化されてきて、原因なども統計的に処理できるようになった。この仕組みの運用は、各種認証取得が他のグループ企業の中でも早かったこともあり、グループ内では例外的に当社独自の運用を許されており、グループの中でも先行している施策である。仕組みは自社独自であるものの、集まったインシデントのサマリー情報はグループ会社内でも共有している。

3.2.3.2.「セキュリティ業務」をしていてよかった経験

社内で専門的にセキュリティ業務に就いている人がごく少数であるため、頼られる存在であること。また、事業をゆるがすような大きなインシデントが発生していないのが自身の業務の成果であると考えると従事してよかったと思える。

3.2.3.3.「セキュリティ業務」をしていて悩んだ経験

当室の業務のひとつである内部監査において、内部監査員として他部署との兼務で監査員を確保しているが、兼務だと時間的に講習等にも行かせることができず、チェックリスト通りの型にはまったやり取りになってしまっていた。そこで監査の質を維持するために、2年程前からは自身を含めたセキュリティ担当の 2 名で対応するようにやり方を変更している。2 名では対応できる範囲が狭まってしまうが、ローテーションについては、独り立ちするまでにかなりサポートしなければならないのでなかなか手が回らないのが現状。また増員については、業務のやり方でなんとかしのげているため、今すぐに当室においてセキュリティ業務担当者を増員する必要性はあまり感じていないが、後進の育成という観点では人材の発掘が必要だと考えている。主にマネジメントシステムの構築や運用というセキュリティ業務にはなるが、セキュリティ人材には、各分野は浅くてもよいので広い知識や業務経験、さらには各所と会話できる人脈があるのが望ましいと考える。また、システムに関する知識や経験があるとかなりのアドバンテージになるだろう。

3.2.3.4.「セキュリティ業務」に着任しての処遇変化

複数業務のうちのひとつという兼務状態ではあるが、社内で情報セキュリティを担当する部署として存在しているので情報セキュリティそのものが特別に処遇されることはない。

3.2.3.5. 自社のセキュリティ維持向上に効果が出たという取り組み

データをイメージ化するシステムの導入だと思う。契約書や与信審査の書類等、業務で大量の書面が発生するので、紙の管理が事業スピードのボトルネックであり、紛失等のリスクも高かったが、イメージ化によって非常に効率的になった。紙がなくなったことで情報セキュリティの観点としても効果があり、業務効率化・情報セキュリティ・紙の利用を減らすことによる環境貢献と一石三鳥になった。書類の場所に依存しない業務が実現でき、今後は働き方改革にも貢献するだろう。

3.2.4. キャリアパス

3.2.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

情報システム部門でシステム開発に約 20 年従事し、ISMS やＰマーク取得の動きの中でマネジメントシステム構築委員会のメンバーとして招集された。構築委員会は人事や営業、業務部隊など全社横断的な要員で構成されていた。認証取得後、構築委員会は一旦解散し、構築したマネジメントシステムを運営する部署が立ち上がり、システム部門出身として引き続き兼務で関わり組織の再編等を経て現在に至る。

3.2.4.2.「セキュリティ業務」前に行っていた業務内容

自社の基幹システムを開発していた。リリース当初はうまく動かず大変な時期もあったが、今となっては、可用性や完全性といった情報セキュリティの三要素について、身をもって重要性を学べた時期ではあった。当時と現在で技術内容は違ってもシステム開発経験がベースにあることで概念が理解しやすく情報セキュリティ業務には入りやすかった。

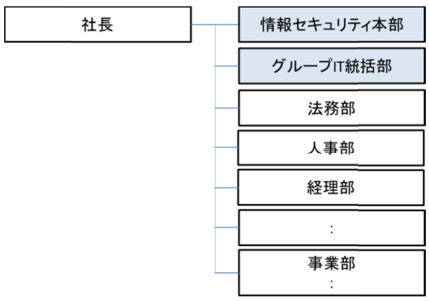
3.2.4.3.「セキュリティ業務」についたことによるキャリア（観）への影響

情報セキュリティは行きつくところは業務品質ではないかと思う。自身の業務品質を向上すれば評価や報酬につながるので積極的な対応をするが、情報セキュリティという視点になると途端にやらされ感になるのが課題だと感じている。また、現場全体のセキュリティレベルを上げるには推進責任者の教育が重要だと感じており、特に新任の責任者の教育は必須である。

3.3. ケース 3（人材サービス関連：自社内セキュリティ担当）
3.3.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：チーム（部署間連携）

組織図



業種
人材サービス関連

企業規模

社員数	約9000名（連結・契約社員含む）

3.3.2. 業務内容の把握
3.3.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
情報セキュリティ本部がグループ全体の情報セキュリティの維持向上をミッションとして活動しており、実質メンバーが 4 名。CISO、室長、自身とメンバー1 名という体制。さらに、IT システムにおける情報セキュリティの実際の運用に当たっては、グループ IT 統括部が連携して行っている。グループ IT 統括部はグループのシェアードサービスの運用保守も行っている部隊で 70 名ほどおり、IT インフラ系だけでなく、セキュリティ分野も一緒に担当する実運用部隊である。

3.3.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
グループ IT 統括部が情報システム部門として、社内業務系システムの運用保守、社内からの問い合わせに対応をしている。部署に所属する人の役割として、セキュリティに特化した人材はいないが、それぞれの担当ごとにセキュリティ対応を行いながら、いわゆる兼業の状態で業務遂行している。

3.3.2.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無
セキュリティに限ったことではないが、部内での教育制度があり、UISS 準拠で IT スキルを向上するための研修の受講をしたり、セキュリティについても e-learning を受講する環境を持ったりしている。UISS 準拠の研修体系化は大変だったが、研修受講を推奨し、受講費用も会社として負担をしている。
エキスパート職制という専門分野に特化した社内制度があり、職制のレベル分けはスキル標準ユーザー協会の示している ISV マップなどを参考にして体系化した。IPA の情報処理技術者資格は一つの基準として取得を推奨している。

また、基本的な IT スキルのレベルチェックを年 1 度実施しており、ポイントの低い分野に対してはスキル向上を促している。
まずは IT の基礎をしっかり学習してもらい、部門ごとに、所属長が上げたい分野やレベルを決めて、受講すべき研修コースを推奨している。
例えば、情報セキュリティ本部は部門特化として、セキュリティの e-learning を推奨している。

3.3.2.4.「セキュリティ業務」を行う環境（体制）

前述したとおり、情報セキュリティ本部とグループ IT 統括部が連携して行っており、基本的に内部の人材だけでの運用を行っている。また、グループ全体のコンプライアンスを担当するコンプライアンス室や、内部監査室との連携はとることになる。

外部人材の活用という面では、新しくセキュリティのためのツールの導入時などは当然外部技術者に依頼するが、平時での運用のための常駐者などは頼んでいない。実際にインシデントが発生し、外部人材に応援を求めることが出てくれば、取引しているセキュリティツールの導入元などに依頼を行うこととなる。

また、フォレンジックは社内人材ではできないので外部に依頼することになるが、手順は内部で作らなければと思っているところである。プロセスとインシデントレスポンスのルール作りは始めており、実際のインシデント発生時は外部と連携して対応する。

他部署とのローテーションなどに関しては、セキュリティの素養がある人材を募集するなどはしておらず、情報セキュリティ本部からグループ IT 統括部に依頼して対応してもらっている。

グループ IT 統括部内でのジョブローテーションなどは、不定期だがインフラやアプリなどでローテーションを行い得意分野の実力をつけてきており、その業務に加えてセキュリティを意識して対応してもらっている。

さらに他部署からグローバル IT 統括部に来て、UISS での研修により実力をつけるなど、徐々に人材育成のサイクルができつつあるので、その仕組みがもっと定期的に回り始め、流動化ができると理想的な組織になるだろう。

3.3.3. 経験談

3.3.3.1.「セキュリティ業務」を実施していて苦労した経験

セキュリティ遵守より、まずは業務優先となる傾向がある。規程などを出すだけでなく、いかに浸透させるかの活動が重要だった。監査の立場で強制力を持たせるなども行ったが、実際に会いに行き、セキュリティの担当と責任者に同席してもらい対面で話をするなどを続けた。継続的に情報発信をして、セキュリティ部門のプレゼンスを上げる工夫が重要だと感じている。

3.3.3.2.「セキュリティ業務」をしていてよかった経験

個人的な嗜好かもしれないが、セキュリティの技術的な勉強が幅広くできるので楽しい。大企業が攻撃される事件が増え始めてから特に意識しだしたが、セキュリティをトリガーとして技術の勉強ができ、知識を広げられるところがよい。

3.3.3.3.「セキュリティ業務」をしていて悩んだ経験

グループ会社では意識の低いところと、高いところの差が大きい。いまだに紙の文化で IT を使っての業務以前のところも多い。逆に固有の運用が確立していて、グループとしての対応というより、個社での対応をきちんと見ていく必要がある会社もある。

また、海外の企業も統制の対象であり対応を進めているが、法の違いなども考える必要がある。今後は海外の法律の勉強などと並行して、共通部分の底上げをはかる必要がある。

3.3.3.4.「セキュリティ業務」に着任しての処遇変化

業務内容による処遇の変化はない。

グループ内に技術職の給与体系は規定されておらず、営業と技術職も同じ給与体系のため、中途の採用含めて苦労している。評価の仕方も難しい状況。

3.3.3.5. 自社のセキュリティ維持向上に効果が出たという取り組み

新しい技術を取り入れる必要があるのではないかということで勉強し、それが結果として効果的なツールを導入してセキュリティ対策向上になってきており、非常に良い流れにつながっている。

3.3.4. キャリアパス

3.3.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

*注)本項は『**チームメンバーがセキュリティ業務についたきっかけ**』という内容で記載*

セキュリティ対応を行うきっかけは、ISMS 認証取得がきっかけで、ISMS の運用を続ける中で徐々にセキュリティの重要性を実感し始めた。他にはグループ IT 統括部に所属し IT 運用を行う中で、情報セキュリティ本部からの依頼によってセキュリティ対応の工数が増えていったという状況。

3.3.4.2.「セキュリティ業務」前に行っていた業務内容

*注)本項は『**チームメンバーがセキュリティ業務前に行っていた業務**』という内容で記載*

理系採用はなく、文系から新卒採用、あるいは中途で入社して IT 運用等を行っている。総合職採用され人材ビジネス部門から異動してきた者もいる。

3.3.4.3.「セキュリティ業務」についたことによるキャリア（観）への影響

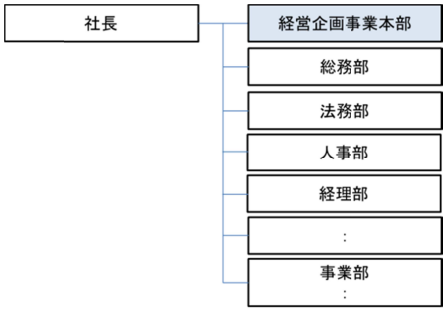
*注)本項は『**会社としてセキュリティ業務に関わる社員の育成やキャリアをどう考えるか**』という内容で記載*

今後は、利用者側がレベルアップできる教育の仕組みが作りたい。今はやらされ感があるので意識が上がりにくいが、利用できる教育のツールや手法などが増えてきているので、そういったものを工夫しながら、教育コースを作り上げて、パッケージのような形で外販できるレベルのものまで引き上げていけたら、自社にとっても社会にとってもハッピーだと思っている。

3.4. ケース 4（卸売業：自社内セキュリティ担当）
3.4.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：個人

組織図：



業種：
卸売業

企業規模：

社員数	約18500名

3.4.2. 業務内容の把握
3.4.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
ISO9001、ISO/IEC27001 の認証維持のための活動、内部監査、教育、リスクアセスメントの運用フロー構築と実施など､セキュリティマネジメントシステムの運用全般を事務局として遂行している。

3.4.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
QMS・EMS・ISMS の統合マニュアルを作成し、それを元に外部審査を受けて事務局として運用にあたっている。また、本社＋全国 50 支社の社員約 3000 名に対してリスクアセスメントに関する教育・勉強会を実施して回っている。

3.4.2.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無
ISO9001、ISO31000、ISO/IEC27001 の内容の理解が必要ではあるが研修体系が存在せず、独学で学んでいるが、他のメンバーにはハードルが高いようである。
事務局が知っておくべき技術系の知識が習得でき、現場との会話もスムーズになるというメリットがあるため､『情報セキュリティマネジメント』の資格取得には力を入れている。今後は事業のアセスメントをする現場側にも取得の推進をする予定である｡取得推進にあたり、特に研修はないが、事務局の場合は、参考書の購入と 1 回目の受験費用を会社で負担している。

3.4.2.4.「セキュリティ業務」を行う環境（体制）
事業の軸が『モノからコト』へ移りゆく中､企業として新しいソリューションを打ち出すにあたっては､新しいリスクにも対応していかなければいけないという考えの元､現社長がマネジメントシステムの維持･運用の重要性を認識し指示を出しているので､現場として推進しやすい体制になっている。
CSIRT は、親会社、グループ会社で体制を整えており、当社が関わるインシデントが発生した場合はテレビ会議等で常時接続を維持し、本部の CSIRT と密に連携を図っている。
当社のマネジメントシステム運用要員としては現状では外部人材はおらず、社員 4 名で担当しており､グループ内の他社よりも統制の効いた質のよい内部監査ができているという自信がある。1 名でも欠けると厳しいと感じている反面、人数が少ない分ガバナンスは効かせやすいとも感じており増員や人材育成の難しさを感じる。
事務局に元 SE で IT に詳しい人に兼務してもらっており、その人にリスクアセスメント

を検討する際に、IT の考えに基づくリスクの意見出しや IT にかかわる説明をしてもらうことで非常に助かっている。一時期はグループ間で人材のローテーションを実施していたが、グループの再編や各社の認証取得状況の相違などにより、今はグループ間異動を行っていない。親会社およびグループ会社間で人材の交流を図り、相互に IT やマネジメントシステムを学ぶというような体制があるとよいと思う。

3.4.3. 経験談

3.4.3.1.「セキュリティ業務」を実施していて苦労した経験

マネジメントシステムの維持・運用業務の遂行にあたっては、経営層にその必要性の理解がなければ現場は非常に苦労すると感じている。

また、自社に IT 部門がないため、IT の問い合わせ先が社内にはなく、親会社やグループのシステム会社にその対応をゆだねている。そのような背景もあり、グループとしては統一したルールを作りガバナンスを効かせたいという思いがあるようだが、一律のルールでは当社の現場においては可用性に欠けて機能しないことが多く、そのギャップを調整するのに苦悩する。そのため、やむをえず自社独自のルールになる場合もある。

3.4.3.2.「セキュリティ業務」をしていてよかった経験

他部署との意見が合わず、理解してもらうのに時間がかかった。しかし、衝突しながらも根気強くコミュニケーションをとることで、プロセスが違うだけで目標が同じであり、双方とも会社をよくしたいという思いがあることがわかり、今では非常に協力的に動いてくれている。

毎年マネジメントシステムを見直し、再構築をすることが『イノベーションをしている』という自負になっているため、苦労はあるが辛くはない。

3.4.3.3.「セキュリティ業務」をしていて悩んだ経験

グループの組織が年に 2 回変わるため、外部審査対象であった部署が無くなるなどの理由でその都度、再構成する必要がある。そのたびに、周りの理解に時間がかかることが多く、そこが悩みとなっている。また、自分より知識を持っている人が少ないのも悩みのひとつである。マネジメントシステムを運用する上で、専門知識を有している方が良いが、転籍者の場合、そこまでに至っていない人もいるため、説明する時間を要することがある。情報セキュリティマネジメントには、ある程度テクニカルな知識も必要となるため、元 SE など IT を知っている人が ISMS の運用業務へ参加してくれるとよい。

3.4.3.4.「セキュリティ業務」に着任しての処遇変化

現状では情報セキュリティに関わる業務へのインセンティブ等はない。

3.4.3.5. 自社のセキュリティ維持向上に効果が出たという取り組み

2015 年度版の QMS と EMS にもリスクという考えが出てきたので、これをきっかけに F コストの削減や、インシデントの予防という観点で QMS・EMS・ISMS の統合運用マニュアルを作成した。リスクアセスメントを実施する現場側には、事務局提供のツールを使って事業上の各業務プロセスにおけるあらゆるリスク（品質・情報セキュリティ・環境）を洗い出してもらい、その中で優先度をつけて対応計画を作成するという教育を全国で実施している。プロセスにおけるリスクの認識が変わるので、効果が出ることを狙っている。

元々、当社では ISMS が先行しており、QMS は『サービス』のみの取得であるため、ISMS から入っているメンバーは QMS に関して知識が浅い傾向があったが、各業務プロセスにおけるリスクが確認できるワークフローを作成し運用するようにしたところ、新人や中途社員はそのワークフローを通してどのプロセスにどのリスクがあるのかを体得することができ、QMS の意識向上に寄与したいと考えている。また、内部監査、認証、リスクアセスメント、教育に関して毎年、改善・改革を行っている結果、インシデントを減らすことに成功している。

3.4.4. キャリアパス

3.4.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

QMS の認証取得、運用をスタートとし、各種マネジメントシステムに関わる中で、ISMS にも携わるようになったことがきっかけである。

3.4.4.2.「セキュリティ業務」前に行っていた業務内容

以前の会社（中小企業）での QMS 取得から始まり、EMS、ISMS と各種マネジメントシステムの取得、運用に 20 年来携わっている。各認証の大改訂も経験しており、マネジメントシステムの構築と運用に関わる知識を長年の業務をとおして体得している。

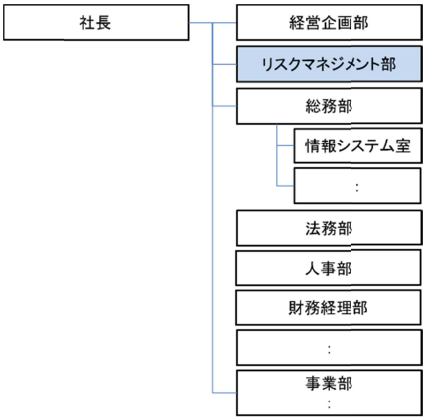
3.4.4.3.「セキュリティ業務」についたことによるキャリア（観）への影響

今後は、後進の育成にも力を入れる必要があり、1，2 名は育成したいと思っている。育成対象として自身の中ではすでに候補を定めており、1 名は、過去に ISMS に関わる部署に所属していた人、もう 1 名は、マネジメントシステムに関わる業務をやりたいという意欲がある人で、後進人材に求めるのは ISO という規格を理解しようとする意欲と素直さである。現状では、これまで地方拠点の ISMS を担当していた人が本社へ異動してきて、本人の前向きな意思で QMS の勉強をしながら業務にあたっている。内部監査の場合は、幹部社員などへ厳しい指摘をする場合もあるため、もの怖じしない性格であるかどうかや、年齢や経験も重要な資質になり、そのような資質を持っている人を探すことが非常に難しいと感じている。

3.5. ケース 5（情報通信業：自社内セキュリティ担当）
3.5.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：ペア（CISO・CISO 補佐）

組織図：



業種：
情報通信業

企業規模：

社員数	約2100名（連結）

3.5.2. 業務内容の把握
3.5.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
ERM を担う部署である。全社のリスク情報の一元管理とリスク対策支援（直接のリスク管理は各部門で実施）をしている。期初にリスクアセスメントをして、各部署に対策を立ててもらい、対策の実施状況を当部がフォローアップして行く役割。情報セキュリティの他、事業継続、コンプライアンスという観点で会社全体として取り組むべきリスクに対し、部門横断で組成されるリスク管理委員会の事務局として対応している。事務局的な仕事の中で、対策や手順の見直し、ルール整備や教育（訓練企画）に関わっている。

加えて、社内で発生するインシデントについて各通報窓口との連携を図り、インシデント報告の取りまとめや分析を行う役割も担っている。必要に応じて、個別インシデントへの対応にもあたっている。

CSIRT は我々 CISO と CISO 補佐の統括の下、組織としてはバーチャルで構築しており、アラートの分析や脅威のトレンド分析などをしている。幸いこれまでは CSIRT としてメンバー全員が関わるようなインシデントは発生していないが、今後はインシデント対応中心の体制だけでなく、CSIRT として平時の体制ももう少し整えていきたい。

3.5.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
情報セキュリティ、サイバーセキュリティとは違う事業継続や人に関わるセキュリティリスクに関わる仕事を担当している。ただ、物理的なセキュリティに関しては総務部門が対応しているし、人に関しては人事部門が担当する場合もあるので、部門横断的に支援する立場が理想だと考えている。

3.5.2.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無
情報セキュリティを担当するときに、技術的なバックボーンが無いが大丈夫かという思いはあった。ただ、情報セキュリティは経営そのものなので、技術以外の点も多く、文系の方が良い点もあると考えている。また、周りに聞ける人はいたので、研修等は特になく、自分で勉強した。ネットワーク、データベースなどインターネットの仕組みのような、技術的な知識はある程度必要だと感じる。また、会社の情報セキュリティを担当する上で ISMS の管理策で何を求められているのか理解できる知識は必要。リスクの捉え方など勉強になる面

が多く、部内でもユーザーガイドを読むように指示している。情報セキュリティマネジメント試験は文系出身でもわかりやすいので、資格としてベースにあるとよい。
過去に、規格取得までは行かないが、マネジメント規格を踏まえた社内体制構築やルール作りに関わった経験があり、その経験に情報セキュリティマネジメント資格などの知識をつけて業務にあたっている。

3.5.2.4.「セキュリティ業務」を行う環境（体制）
現在の体制は 5 名で実施している。全員が社員である。公募をした場合には SI をしている部門や営業から公募があった実績もある。
外部人材をもし使う場合には、担当してもらう業務にもよるが、総じてセキュリティの会話ができるコミュニケーション能力を求める。セキュリティ系の知識を養う為には、研修を受講させる必要などはあると思うが、ルールを作成したり見直ししたりする様な業務は経験させることが必要だと思うので、研修だけでなく OJT と合わせた育成を考えている。外部研修については費用対効果を重視する。

3.5.3. 経験談
3.5.3.1.「セキュリティ業務」を実施していて苦労した経験
何か起きた時に影響度や優先順位の判断に苦労した。部署員にも全てをわかっている人はなかなかいないので、起きていることがどんなことで、すぐにでも対処すべきなのか、会社の状況と照らし合わせた時にリスクの優先順位づけが難しい。社長はあるべき姿、理想の姿をイメージして指示をするが、具体的に実現しようとすると予算などの問題や事業部門との調整などバランスが難しく答えが出しにくい場合がある。また、予算を持つ部署では無いので、最終的には実施部署へのお願いが必要になる。
苦労の一方で、相談できる人はおり、CSIRT も構築しているので、社内の事項については CSIRT メンバーの協力も仰げる。
今、悩んでいることとしては、関係部門間との情報連携や文書化がまだまだ進んでおらず、全体像を把握できる仕組みができていない中でどのように整備すればよいかということである。会社が合併で大きくなったという背景もあり、昔やっていたことを今はやっていなかったり、周りはやっていると思っていたりといったミスコミュニケーションに危機意識を持っている。

3.5.3.2.「セキュリティ業務」をしていてよかった経験
コミュニティに参加するなど関係者が広がったことは良かったと思う。

3.5.3.3.「セキュリティ業務」に着任しての処遇変化
処遇の変化はない。

3.5.3.4. 自社のセキュリティ維持向上に効果が出たという取り組み
グループ会社も増えているので、意識向上のコンテンツなども作成している。普及のためのキャンペーンなどができれば面白いと思う。

3.5.4. キャリアパス
(注)インタビューは 2 名にヒヤリングした為、本項は CISO と CISO 補佐と分けて記載。
3.5.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)
インタビュー対象者：CISO
様々なリスクマネジメントの取り組みがサイロ型でバラバラになっていたため、『全社的なリスクマネジメント（ERM）を導入すべき』との提案をした結果、リスクマネジメントの専任部署が設置され、その責任者として着任した。リスクマネジメント部が当社の重要リスクの１つである情報セキュリティの部門横断的な会議体の事務局となっていたこともあり、CISO という役割を担うこととなった経緯である。

インタビュー対象者：CISO 補佐
2000 年ごろに世の中がセキュリティに動き始めたことで興味を持った。

3.5.4.2.「セキュリティ業務」前に行っていた業務内容

インタビュー対象者：CISO
内部管理（体制）整備など上場準備に関する業務を経験していた。経営企画的な立ち位置で体制やルール作り、内部統制評価などの内部監査業務を経て、現在はリスク管理が業務の中心となっている。これまでの経験はリスクマネジメントに活きていると考えられる。情報セキュリティにも応用が利くものだと感じている。ただ、情報セキュリティという点においては技術的な知識が不足していたので、情報セキュリティに関する勉強のため情報セキュリティマネジメントの試験を受けた。

インタビュー対象者：CISO 補佐
今のキャリアの役に立っているのは、外部組織に常駐しての仕事の進め方の体得や、システム開発の経験である。外部の組織に所属し、様々な事業体の会社の方々とコミュニケーションを重ねることが非常にいい経験になった。

3.5.4.3.「セキュリティ業務」についたことによるキャリア（観）への影響

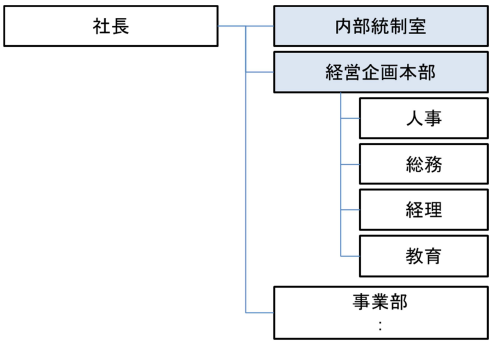
インタビュー対象者：CISO
個人のレベルで言えば特にない。ただ、若手の人の場合にはリスクマネジメントの業務につくことは良いことだと思う。会社に必要なものについて優先順位の考え方は良い経験になる。

インタビュー対象者：CISO 補佐
外部組織での活動をとおして、組織の在り方や企業規模と担当者の配置バランスなどが様々で各企業の悩みも違うということを学んだ。自社に戻り、セキュリティサービス提供をしようにもうまく行かない場合や、ミスマッチを起こす場合もあり、外部組織での経験と照らし合わせることで問題の原因がわかることがある。外部組織での経験で視野が広がったと感じる。社内の若手にもこう行った経験を伝えていければと思っている。

3.6. ケース 6（情報通信業：自社内セキュリティ担当）
3.6.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：チーム（部署間連携）

組織図：



業種：
情報通信業

企業規模：

社員数	約970名
システム要員数（内務）	約700名
システム要員数（外部委託・派遣）	約700名

3.6.2. 業務内容の把握
3.6.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
全社の情報セキュリティ管理に関わる業務全般を事務局として組織を横断的に支援し、円滑な事業活動を促進している。社内の情報セキュリティに関わる責任者をサポートしながら、情報セキュリティインシデント対応や、事象・弱点の是正、予防措置の推進のみならず、情報セキュリティポリシーの維持や手順書の作成の役割も担っている。事務局としては、リスク対応計画の作成および実施や、情報セキュリティへの取り組み度合評価の推進、内部監査支援の機能も有している。

3.6.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
内部統制や総務業務・IT システムを本務とするメンバーが、各専門の業務の分掌範囲にあたる情報セキュリティ業務に対応している。割合として技術職が約 92%、スタッフ職が約 8%で、情報セキュリティ業務を担当する事務局のメンバーはスタッフ職 4 名、現場から 3 名の構成であたる。

3.6.2.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無
グループ会社提供の ISMS 研修基礎教育および、運用組織向け事務局用教材でベースを学ぶ。それらの費用は会社負担。教材等での学習も重要ではあるが、社員に求める一番のポイントは誠実さで、会社の事業を把握し事業部毎の事業特性を考慮するスキルが重要であると考える。情報セキュリティマネジメント系の試験や IPA から提供されている情報セキュリティ普及啓発資料は役に立っている。

3.6.2.4.「セキュリティ業務」を行う環境（体制）
担当役員の直下に事務局が 7 名、各部署長 50 名超を推進責任者として体制化している。その中に外部委託・派遣等の外部人材はいない。事務局は、現場・役員・外部からの情報のハブであり、集まった情報に応じて、各専門の対応担当を振り分けている。情報セキュリティの技術的な内容については、親会社の事業および社内の IT を統括する部署に協力を依頼し、グループとしてガバナンスが効いた状態にある。
また、グループ会社の中でも IT 技術を事業の基盤とする会社であることから、率先して個社としてセキュリティ施策を実践してきており、効果が高かったものはエスカレーションをかけてグループ全体へ展開させている。エスカレーションフローは三年半前に作成され、経験を元に年々改善されている。

3.6.3. 経験談

3.6.3.1.「セキュリティ業務」を実施していて苦労した経験

月に数十万件のアクセスがあるサーバがアタックされ原因究明や対応で 3 ヶ月にわたり徹夜が続いたことや、業務に関わる重要情報が含まれているパソコンを社員が紛失し、部門の 150 人総出で 1 ヶ月間営業活動を縮退して捜索したことなどの苦労経験を現在の推進に役立てている。例えば、当時から事業の利益は顧客からの信頼に基づくものであり、それらを損なわないことが常に最優先されている。情報セキュリティはひとたび起これば、経営問題になることを実際に体験しており、対策の重要性は学習している。

幸いなことに、社員が誠実で適切にエスカレーションしてくれる社風であるが、全国の支社長に対しては、インシデント発生時には叱らずに「他（近隣県）は大丈夫？」と質問するように教育している。言い訳を考えてしまうので報告時に対策は一切求めない。インシデント報告者を叱らないという教育は毎年実施しないといけないと考えている。

3.6.3.2.「セキュリティ業務」をしていてよかった経験

社内の各事業部との連携で、各部署の業務内容について理解を深めることができたり、会社全体の動きを把握できたりすること。情報セキュリティの体制として、平時は各担当領域で業務をしながらも何か起こった時には各領域のエキスパートとチームで動けることが心強い。経験を重ねることで、チームとして適切にスピーディーに対応ができるようになってきている。

3.6.3.3.「セキュリティ業務」をしていて悩んだ経験

情報セキュリティを技術戦略の重要テーマとして対策を打っており、セキュリティ人材が重要であるという認識は経験をとおしてよくわかっているが、数としては増えていないこと。技術系のセキュリティ人材の育成として数十名を研修やミーティングにノミネーションしている。親会社にも人材が少なく、数億をかけて外部委託している状況。技術会社なのだから本来であれば自前でそろえられるはずで、組織と人材本人の意思・士気があれば実現可能であると考えている。

3.6.3.4.「セキュリティ業務」に着任しての処遇変化

情報セキュリティの活動とは直接的な関係はないが、情報セキュリティを取り扱っているからという理由でのインセンティブはないものの、人材の可視化を目的に 800 項目のスキルについて自己申告でチェックする制度を設けている。毎年見直しをしながら 6 年経ち、スキルチェックの結果が報酬と直結することを主管部門が根気強く説いてまわり、ようやく制度として回りはじめた。スタッフ職にも適用を始めている。

IT スキル標準にならった 1~7 のレベルがあり、4 以上の人はプロフェッショナル認定とされ、レベル 4 はリーダー職と同等とみなされる。レベル 5 はエバンジェリストとして部長職と同じ待遇になる。レベル 5～6 にあたるハイレベルな人材の評価は、社内に面談できる人がいないため、外部ベンダーによる「お墨付き」の評価をもらっている。自社の評価のみでは独りよがりで意味がないと考えている。

親会社をはじめ、グループ各社に展開している状況である。

3.6.3.5. 自社のセキュリティ維持向上に効果が出たという取り組み

実際のインシデントの対処によりチームの対応力が上がったことと、備えの重要性を実感し、被害や影響の極小化に貢献する施策を継続できていること。中でも e-learning や標的型攻撃に対する気づきを促すフェイクメール等の施策は、社員のセキュリティリテラシー底上げに効果を奏している。

3.6.4. キャリアパス

3.6.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

注)本項は『セキュリティ業務へのキャリアシフトを会社としてどう考えるか』という内容で記載

社員に対し、年に 1 回異動の希望は聞くが、異動動機がスタッフ職は楽という考えであ

れば受け付けない。ジョブローテーションの希望を聞くだけでは、十分ではないことを認識しており、これを学んだらこうなれるというキャリアパスを会社として明示することが必要であると考えている。現在、組織的にセキュリティに関わる人材に女性もおり、性別の差はないと考えている。

3.6.4.2.「セキュリティ業務」前に行っていた業務内容

*注)本項は『**会社の中でセキュリティ業務が確立した経緯**』という内容で記載*

リスク管理や、P マーク等の認証の維持、内部監査の支援、その他総務業務といった本務に情報セキュリティの要素が加わった。現在では、本務と兼務の業務内容の密接度が高く、常にリンクしている状態である。

3.6.4.3.「セキュリティ業務」についたことによるキャリア（観）への影響

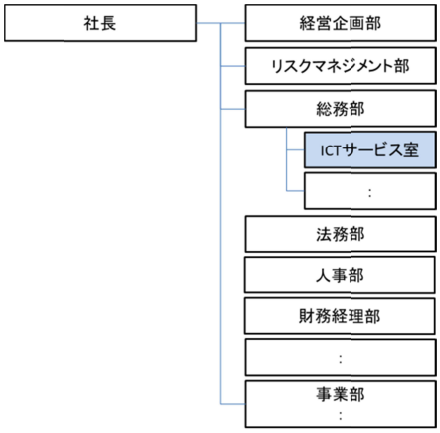
*注)本項は『**会社としてセキュリティ業務に関わる社員の育成やキャリアをどう考えるか**』という内容で記載*

セキュリティ人材の育成は学習時間の確保という点で社員の働き方をどう考えるかにも大きく関連してくると考えている。自己学習の時間（目標：年間 15 時間、推奨：年間 60 時間）は自身のスキル向上のための学習を行うもので、自律的に時間を使うために WLM（ワーク・ライフ・マネジメント）を経営者が率先して呼びかけている。学習時間を確保するために効率性を追求したり自律的な時間の使い方を考えたりすることは、働き方改革の実践要素にもなると考える。

3.7. ケース 7（情報通信業：自社内セキュリティ担当）
3.7.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：個人

組織図：



業種：
情報通信業

企業規模：

社員数	約2100名（連結）

3.7.2. 業務内容の把握
3.7.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
社内向けサービスの運用、インシデント対応をしている。社内情報システムを運用管理する部署の室長として、インシデント時にはシステムやネットワーク停止の判断をしており、権限も有している。夜間にアラートが発砲したような場合には、駆け付けることもある。

3.7.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
情報システム部門の要素もあるため、社内システムの運用保守、社内からの問い合わせに対応をしている。また、社内向けの業務系システムの設計・開発・改修も担当している。部署に所属する人の役割としては、開発系が 5 名、運用系 3 名、稼働に合わせて流動的に活躍する人員が 3 名所属し、業務を遂行している。

3.7.2.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無
研修の受講というよりは OJT や現場業務を進めながら覚えていった。最近では情報処理安全確保支援士を社内で増やすという取り組みがあり、対策講座を受験したり、試験を受験したりしている。費用は会社負担だった。改めて体系的に学ぶことによりセキュリティ知識の振り返りに役立った。
セキュリティ業務で必要な知識を養うためには、自分でセキュリティを試せるような環境を構築して実験してみるのがよいと思う。また、Web サイトをたどりながら知識をつけていくことも役に立つ。

3.7.2.4.「セキュリティ業務」を行う環境（体制）
部署として 12 名体制で行っている。ベテランが多く、40 歳未満はいない。外部の人材は 2 名常駐している。社員では対応が難しい開発において、20 年以上対応をお願いしている。
資産管理やアカウント管理といった業務はグループ会社へ委託しているが、関連会社以外の外部委託はしておらずグループの方針に従っている。外部に委託すると、管理範囲が狭まるというメリットを感じるが、契約の都合上どうしても確認工程が増えるため、スピード感という点ではデメリットと感じてしまうときがある。
一緒に働く人には、コミュニケーションスキル、特に相手の話を理解する力や相手の立場

に応じて説明する能力などを身に着けてほしいと思っている。また、継続して学習する意欲も必要だと思う。PMP・CISSP・情報処理安全確保支援士などの取得は推奨されており、会社負担で研修などが受けられる場合もある。

3.7.3. 経験談

3.7.3.1.「セキュリティ業務」を実施していて苦労した経験

可用性や機密性の確保の間でどこまでを許容範囲とするのか、切り分けが難しいところが苦労している。事業部にセキュリティを専門とする人材による相談窓口が複数あるので、電話やチャット電子メール、訪問などで相談している。

3.7.3.2.「セキュリティ業務」をしていてよかった経験

セキュリティ関連業務をしていることで、セキュリティに関係する部門といろいろ情報交換ができることがよいと思っている。また、情報交換できるという安心感もある。

3.7.3.3.「セキュリティ業務」をしていて悩んだ経験

セキュリティに詳しくない人はインシデントを大ごととしてとらえてしまう。たいしたことでない場合もあるので、説明するのに苦労している。

3.7.3.4.「セキュリティ業務」に着任しての処遇変化

業務内容による処遇の変化はない。

3.7.3.5. 自社のセキュリティ維持向上に効果が出たという取り組み

端末の対策状況を視覚化する製品を導入したところ、アップデートの不備が一目で分かるようになった。効果が出た取り組みの一つだと思っている。

3.7.4. キャリアパス

3.7.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

情報システムの運用に携わる中で必然的にセキュリティ業務も担当していくようになった。したがって、何かをきっかけでセキュリティ業務を担当するといったわけではない。

3.7.4.2.「セキュリティ業務」前に行っていた業務内容

情報システムの運用業務に長年従事している。基本的には情報システムの運用業務の延長にセキュリティ業務があり、現在に至っている。情報システムの運用業務から入っているので、Cisco などのベンダー系資格の取得の勉強で知識を養った。業務全般については OJT を通して覚えていった。今はネットで検索すれば必要な情報が出てくるので、便利になったと思う。Cisco などのベンダー系資格は Cisco 製品を使う上では有用であると考えている。

3.7.4.3.「セキュリティ業務」についたことによるキャリア（観）への影響

特にはない。ただし、今後業務を続けていく上では新しいものに対する興味や関心を持ち続けることは必要だと思っている。部署の同僚ともキャリアについて話をするが、セキュリティ側への異動願望は特になく、現在のキャリアを続けたいという考えのようである。

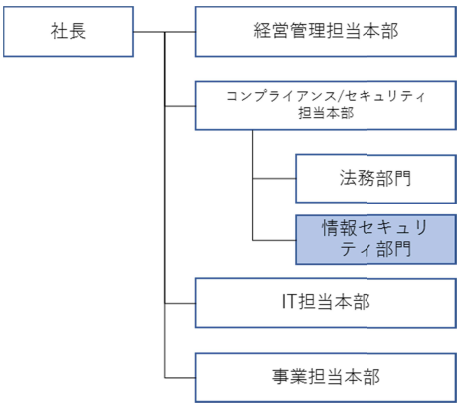
長年の社内情報システム運用業務をとおして感じていることは、世のインフラ管理者は、セキュリティ人材として通用する素養を十分に（あるいはセキュリティ人材以上に）持ち合わせているのではないかということである。サーバやネットワークはもちろんのこと、ミドルウェアやデータベースまで操作することから得る広い IT 知識と経験により、インシデントに対する能力が高いと考えている。既に持っている知識に加えて、セキュリティリスクとなるパターンを学習することで、セキュリティ人材としてのキャリアが開けると考えている。

3.8. ケース 8（教育、福祉、複合サービス業：自社内セキュリティ担当）

3.8.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：ペア（部門内連携）

組織図：



業種：
教育、福祉、複合サービス業

企業規模：

社員数	約20400名（連結）
システム要員数（内務）	約600名

3.8.2. 業務内容の把握

3.8.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容

情報セキュリティ部門にて、ホールディングス全体の情報セキュリティを管理している。部門の成り立ち上、情報セキュリティ部門はコンプライアンス寄りの視点でコーディネーターとしての役割を担い、技術的なところは IT 部門やシステムの運用専門機能を持つグループ会社が担当している。

3.8.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容

セキュリティ業務専任であるが、インシデントに備えた平時の業務として、規模・セキュリティ施策・意識などがそれぞれであるグループ会社内の現状を把握すべく、コミュニケーションを意識的にとるように動いている。各会社の担当と会話する際には何か指標となるものがないと共通化できないため、セキュリティアセスメントチェック表を作成し、運用をしている。チェックの結果が低いとペナルティを課すなどとかいうことではなく、まずは現状を把握して対応範囲や対応方法を検討する材料としている。

3.8.2.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無

基本的には OJT で学んでいる。情報マネジメント試験は会社意向により取得が推奨されたが、教材費や受験料は会社負担ではなかった。技術的な内容については、IT 側の研修制度にゆだねている。

3.8.2.4.「セキュリティ業務」を行う環境（体制）

ホールディングス全体のセキュリティコーディネーターである情報セキュリティ内の担当としては 3 人。IT 関連の技術対応をする要員としては、社内の IT 部門、システムの運用専門機能を持つグループ会社に加え、事業部内の常駐の派遣人材や協力会社のメンバーを含めると 600 人程度の規模になる。（但し、これら 600 人の多くは技術者であり、直接セキュリティ業務に関与するわけではない）関連者という意味では、その他、インシデント対応時の緊急的な体制を外部委託にて備えているので、実質的にはより多い人数が関わっている。IT 関連の技術対応については、自組織外に対応を頼むと依頼にかかる費用も時間もかさむため、状況が共有できた状態ですぐに動けるよう中に人を置く傾向が高い。

3.8.3. 経験談

3.8.3.1.「セキュリティ業務」を実施していて苦労した経験

グループ会社でインシデントが発生した時に連携は取れたものの、どう動かしてよいかに手間取った経験がある。その時は、たまたまその会社の担当者が優秀でうまく回してくれたのでよかったが、そうではないところがあることを考えておかなければならないと感じている。

3.8.3.2.「セキュリティ業務」をしていてよかった経験

ユーザー部門の頃は、社としてきちんとルールを決めて浸透させてくれればいいなと思っていたが、今は自らがそれを実現できる立場にあるということ。

3.8.3.3.「セキュリティ業務」をしていて悩んだ経験

CISO は明文化されていないがセキュリティに関しては部署として意思決定権を持っており、経営会議や、役員に相談できるルートが存在している。意思決定権を持つ一方で、グループ企業数が多く、業態も様々で、すそ野が広いため、ホールディングスとしてどこまでケアできるかが課題になっている。また、組織構成上、事業部門の存在力が強いため、ガバナンスを効かせるために、はっきりと物が言えたり、折れない気持ちを持ったりする強さが必要であると感じる。

また、元々は IT 部門が全事業部を一括して見ていたが、次第にそれぞれの事業部に引き抜かれる形で IT 担当者が散ってしまったので、それらの IT 担当者にホールディングスとしてのガバナンスを効かせるのが難しいと感じる。

3.8.3.4.「セキュリティ業務」に着任しての処遇変化

セキュリティ業務が特別に処遇されることはない。それが主業務であるため、他と比べての特別扱いがないのは理解するものの、何も起きないのがあたり前であり、インシデントが発生しないことへの評価がないことに疑問はある。

また、セキュリティ業務の考え方は、会社の事業やプロダクトに依存するのではないかと思う。IT ベースの企業だとセキュリティ業務への評価やあこがれも出てくるかもしれないが、それ以外が花形の場合はどうしても距離が生じる。

3.8.3.5. 自社のセキュリティ維持向上に効果が出たという取り組み

数年前のインシデント経験が時を経て教訓となり、対応の必要性、重要性について社員の意識に刻まれている。しかし、『会社の対応方針に従います。』というスタンスはある一方で、どういう観点でそういう取り決めになっているかを知ろうとする働きかけがなく、セキュリティ部門が言ったから OK、あるいは NG という転嫁感はいなめない。何がリスクでどうしたらいいのかを現場でも考えてもらいたいという思いはずっとあるが、そこまで成熟できていないのが現状である。

3.8.4. キャリアパス

3.8.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

過去の経歴を踏まえ、CSIRT を立ち上げるので、担当としてという指名だった。

3.8.4.2.「セキュリティ業務」前に行っていた業務内容

注)本項はインタビュイー2 名それぞれを①②に分けて記載。

① 元々は事業部で、顧客データベースにデータ登録する運用業務や当該システムの改訂をしていた時代があり、その時代に技術の勉強をした。その後 5～6 年、個人情報保護担当として P マークや ISMS 認証の検討および取得経験を経て、立候補にて顧客データベースシステム改訂に関わった。非機能要件をまとめる経験をとおしてセキュリティを学んだことが現在の業務に役立っている。法学部出身であるため、法文を読んだり考え方を理解したりする法務的な基礎力は持っていた。

② 同じく元々は事業部で、コールセンターの音声やデータを取り扱う個人情報を取り扱う最前線のシステムをデータ利用者視点で開発・運用していた。セキュリティ部に来て今

度はそれらのシステムを守る側にまわったという感じ。
インターネット創世記（1990 年代）のホームページや ICQ などを触っており、その経験が面白かったのでテレコム業界に入り、音声系の配線・ADSL の認証・なりすましメールの対策などを前職で経験していたのがベーススキルとなっている。

3.8.4.3.「セキュリティ業務」についたことによるキャリア（観）への影響

ユーザー側とは見方が異なり、『(事故を）起こさないためには』ではなく、『起きたらどうするか』を直視できるため、CSIRT 業務、特にインシデントハンドリングの対応を考えることに面白みを感じている。

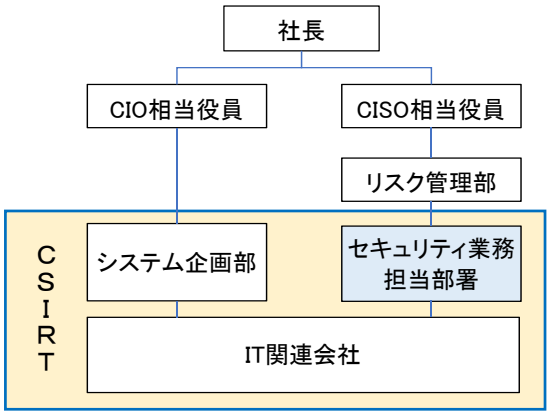
また、セキュリティ人材の育成や、流動化については、一般的なセキュリティ領域であれば外部人材も活用しつつ流動化できるのではないかと思うが、事業重要度が高い領域を任せるには内部できちんとエキスパートを育成しなければならないのでないかと考えている。目下、セキュリティは IT のひとつの領域としてとらえられており、IT 部門の研修体系に依存しているのが現状ではある。

執務エリアや情報については役割と権限でのアクセスコントロールはあるが、仕事についても同様の考え方が適用され、ある一定の資格がないとこれ以上は開発できない・従事できないというような枠組みがあるべきではないかという模索もある。

3.9. ケース 9（金融業：自社内セキュリティ担当）
3.9.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：個人

組織図：



業種：
金融業

企業規模：

社員数	約7,000名
システム要員数（内務）	約250名
システム要員数（外部委託・派遣）	約350名

3.9.2. 業務内容の把握
3.9.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
次のような業務を実施している。
①セキュリティ中期計画の策定・見直し・推進
技術的・人的・組織的対策のそれぞれについて半年ごとに見直しを行い、取締役会に年２回報告している。
②不審メール等の監視・モニタリングとインシデントの未然防止
アラートが出た場合に追跡調査・モニタリングを行っている。有時にはサイバーセキュリティフレームワークに基づいた初動対応を実施。
③（社外向け）セキュリティ関連情報の収集（金融 ISAC 等）
ワーキンググループに積極的に参加している。また、業界他社の動向を把握し、新たな対策や手法を自社でも採用するかどうかの判断に活用している。
④（社内向け）セキュリティ関連情報の共有（CSIRT、グループ企業等）」
社内ＣＳＩＲＴで隔週、グループ内企業で月に１回情報連携を実施。

3.9.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
外部委託リスクの審査のほか、持株会社の IT 全般統制なども兼務している。これにより、委託先の立入検査なども実施する。
社内向け業務としては、CSIRT 人材の育成、マニュアルの策定、訓練の実施などのほか、組織改編に対応したアクセス権の見直し、IT 資産管理に関する申請受付なども行っている。こうした一見泥臭い業務も、円滑な実施には社内での調整能力が必要となるため、兼務にて担当せざるを得ない状況である。

3.9.2.3.「セキュリティ業務」につくにあたって研修などの教育有無
自身ではセキュリティ業務に従事する際に研修等は受講していない。かつてシステムインテグレータに在籍していたときの経験が役立っている。
職場の制度としては、当時はなかったが、現在は「ＣＳＩＲＴ人材育成計画」を策定し、セキュリティ人材の育成対象者に、会社負担で外部研修を受講する制度がある。

3.9.2.4.「セキュリティ業務」を行う環境（体制）

当社では CISO は明示されていないが、CIO とは別の役員が担当し、それぞれシステム企画系部署とリスク管理系の部署を統括することで、相互牽制を機能させる体制となっている。

セキュリティ管理を行う部署はリスク管理系の部署内に 30 名規模（プロパー10 名、IT 関連会社 20 名程度で構成）で設置されているが、いずれも他業務との兼任である。このうち 4 名がいわゆるセキュリティの「橋渡し人材」を担うプロパーの職員であり、実質専任に近い扱いとなっている。橋渡し人材は 1 人では緊急時対応をすべて行うには不足であり、経営への報告とシステム対応の陣頭指揮にそれぞれ 1 名ずつ必要、交代を考えるとそれぞれの役割に 2 名で合計 4 名の確保を目指している。

3.9.3. 経験談

3.9.3.1.「セキュリティ業務」を実施していて苦労した経験

業務の進め方に関して正解が 1 つでないことがある。また、現在は問題ないが、過去にセキュリティ業務についての理解に欠ける人物（*）が上司となったことがあり、業務遂行において多大なる支障が生じるとともに、精神的にも大きなストレスとなった。

（*）営業のみを経験し、システム・セキュリティの経験なし。

3.9.3.2.「セキュリティ業務」をしていてよかった経験

自らが主体となって行ったサイバーセキュリティ対策に関する取り組みが、金融系の業界活動において表彰された。この結果、社長賞を受賞したり、社内報で紹介されたりした。こうした状況を経て、現在は役員から声をかけてもらえるようにもなっている。

3.9.3.3.「セキュリティ業務」をしていて悩んだ経験

現在は、職場環境や金融 ISAC 等のコミュニティ活動に恵まれており、特に悩みはない。ただし、将来的に上述のようなセキュリティ業務への理解に欠ける上司が配属された場合にはそれが悩みとなる可能性もある。

また、最近は優秀な人材を適切に処遇しないと、他社に引き抜かれたり、自分から転職したりすることがあるので、自分の後継者が確保できない場合は困ったことになる。

3.9.3.4.「セキュリティ業務」に着任しての処遇変化

上述の表彰の後、賞与査定の高評価などの変化があった。

3.9.3.5.自社のセキュリティ維持向上に効果が出たという取り組み

3 ヵ年のセキュリティ中期計画の策定・推進において、金融庁からの要請事項（課題のあった事例・標準事例・良好事例のフィードバック）に計画的に対応させることができた。

3.9.4. キャリアパス

3.9.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

積極的にセキュリティ業務を指向したわけではない。人事異動の結果、システムリスク管理部門での勤務を経て、現在のセキュリティ統括部門に移ってきた。ただし、嫌々やっているわけではなく、これまでの社会人経験の中では現在が最も充実している。

3.9.4.2.「セキュリティ業務」前に行っていた業務内容

業務システム・基盤システムの開発・保全（インターネットサービス、コールセンター、有価証券・融資・不動産）、システムリスク管理等の業務を担当した。

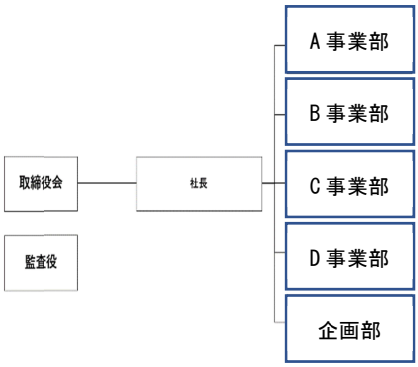
3.9.4.3.「セキュリティ業務」についたことによるキャリア（観）への影響

金融 ISAC での活動を通じて、かなり意識が変わった。現在担当している「橋渡し人材」を短時間で育成することは困難であり、その素養をもった人材を確保するのも簡単ではないが、金融機関におけるシステムリスク管理においては不可欠である。

3.10. ケース 10（情報通信業：自社内セキュリティ担当）
3.10.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：個人

組織図：



業種：
情報通信業

企業規模：

社員数	440名
システム要員数（内務）	100名
システム要員数（外部委託・派遣）	200名

（インタビュー当時の人数）

3.10.2. 業務内容の把握
3.10.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
主にガバナンス（管理/統制）とエンジニアリングの２つの業務がある。
ガバナンスは P マーク認証の更新や、社内のセキュリティ監査の企画、運営、推進などを行っている。自社内に CSIRT を設置していないが、社内横断的にリスク管理を行う委員会を設置している。社内インシデント発生時には、事務局となって全社横断的な対応を行っている。その他には社内業務におけるセキュリティルールの作成、チェック、運用改善業務などがある。
エンジニアリングは、外部からの侵入や攻撃に対して導入している自社内の NW 機器運用や、法人向けに提供しているサーバや WAF 等のサービスにおいて、脆弱性情報の収集や対応のプライオリティ決め等の推進を行っている。

3.10.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
ガバナンス業務は情報セキュリティ担当の課長が責任者となっており、エンジニアリング業務はサービスの開発及び運用部隊、データセンタの保守部門や外部のセキュリティベンダーで対応を行っている。社内にセキュリティエンジニアという専任担当はいない。

3.10.2.3.「セキュリティ業務」につくにあたって研修などの教育有無
セキュリティに特化した研修は用意してはいない、年に 1 度コンプライアンス系の e-learning を行っているが、実際に業務を行いながら修得しているのが現実である。他には自己啓発用として会社が用意しているカリキュラムを各社員が選択して学習する制度がある。

3.10.2.4.「セキュリティ業務」を行う環境（体制）
組織上ではデータセンタの運用をしている事業部が中心となって行っているが、各組織内からもセキュリティ担当を任命し、監査時やセキュリティ発生時には、各組織のセキュリティ担当を中心に組織を牽引し対応を行っている。

3.10.3. 経験談
3.10.3.1.「セキュリティ業務」を実施していて苦労した経験
既にサービスとして提供しているシステム含め、すべてのサービスに WAF や脆弱性検知

システムのパッケージを展開する施策を行っていたが、サイトが複数、多岐に渡るため、計画をたてて適用しないと混乱を招くおそれがあった。入念に計画をたて、サービスの事情や特性等を考慮しながら全社に対して調整する必要があり、社内調整に大変苦労した。
前例がないインシデント発生時は過去のナレッジがないため対応に時間が掛かることがあった。弊社をかたるフィッシングメールの発生が初めて確認された際には、グループ会社や JPCERT/CC に報告しながら対応を行い徐々にルール化していった。

3.10.3.2.「セキュリティ業務」をしていてよかった経験

全サービスの脆弱性対応完了率の数値が大幅に改善した時の達成感、満足感はあった。地味で目立ちにくいし、面倒なことが多い業務だが、やらないといけない業務だということは認識している。セキュリティ対策が少しずつでも進んでいることが感じられた時にやってよかったと思えた。

3.10.3.3.「セキュリティ業務」をしていて悩んだ経験

脆弱性検知システムにより検知された脆弱性への対応依頼をお客様や自社の担当に伝えても、すぐに対応できない場合がある。なかなかモチベーションがあがる業務ではないことや、緊急度に関する意識が合わず後回しにされがちであった。
セキュリティ人材についても、求めるスキルの人材がすぐに見つかるような状況ではない。そのため今ある社内のリソースを活用することになるが、その場合、本来の業務への影響も考慮せざるを得ず、バランスを取るのが難しいと感じた。セキュリティ人材については、社内人材の育成が大切だと思うが、すぐに即戦力にできるものでは無いので大きな課題だと認識している。

3.10.3.4.「セキュリティ業務」に着任しての処遇変化

特にはないと考えている。インシデントは発生しないことが当たり前であり、加点評価と言うよりは減点評価に考えが近いかも知れない。

3.10.3.5. 自社のセキュリティ維持向上に効果が出たという取り組み

脆弱性検知システム導入の例だと、サービス導入時は検知した内容を表示するのみだったが、運用するにしたがってリスク及び優先度の高いものを明示し対応を促すよう工夫した。対応の仕組みを変えたことにより、対応率についても大きく改善することができた。

3.10.4. キャリアパス

3.10.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

全社的にセキュリティ向上施策の重要性が高まる中、セキュリティ担当を有する部門の中で、サービスの開発に携わっている担当であったこともあり、会社から任命された。

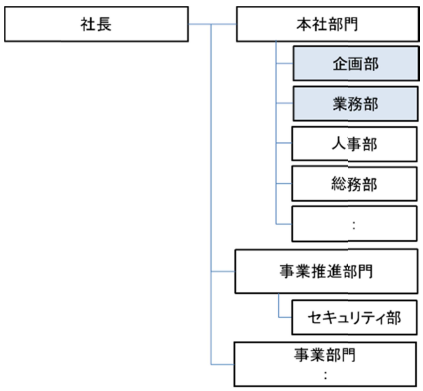
3.10.4.2.「セキュリティ業務」前に行っていた業務内容

サービス開発。IT ベンダー資格の作成及び企画。

3.11. ケース 11（情報通信業：自社内セキュリティ担当）
3.11.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：チーム（部署間連携）

組織図



業種
情報通信業

企業規模

社員数	約2500名

3.11.2. 業務内容の把握
3.11.2.1.「セキュリティ業務」の位置付けとして現在行っている業務内容
社内で発生するセキュリティインシデントの通報窓口。経営に近い部署であることから自社のルールや組織、システム構成など総合的に判断しインシデントをハンドリングする役割も担う。

3.11.2.2.「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
経営企画、計数管理、広報の他、社員が使用する PC やモバイル端末の調達、社内のネットワークの管理といった OA 環境の維持など、全体統括を担う部署としての業務を遂行。

3.11.2.3.「セキュリティ業務」を遂行するにあたっての研修などの教育有無
基本的には独学と経験則。以前はお手本とするものがほとんどなく、オレンジブック（アメリカのセキュリティ評価基準ガイドブック）を参考にしたり、セキュリティに詳しいベンダーに現場で教えてもらったりした。

3.11.2.4.「セキュリティ業務」を行う環境（体制）
3 年ほど前にインシデント対応に係る社内規定を定め各部横断的に分業体制を整備（この 1 年程でようやく分業体制が確立されてきた）。組織を若干ピラミッド型にしており、ガバナンスを効かせやすい体制にしている。技術的な内容に関しては、事業に関わる情報セキュリティを専門的に担う部署が存在するため、同部署やベンダーなどと連携を取りながら対応。
全社的にローテーションを促進する動きはあるが、本社部門では「個別事案の経験や知識」も必要となるため、現状では個別の人選になっている。事務量は増えているが、本社部門の人材は簡単には増やせないのが実情。企画部の要員数は 10 名弱で、全員が社内あるいはグループ会社のメンバーで構成。現状では難しいが、増員がかなう場合に人材の素養として求めるのは、コミュニケーション能力、忍耐力、積極さ。技術は後天的に身に着けられるので重視しないが、ネットワーク技術は持っていると役に立つ。しかしそのような人材はかなりハイスキルであり社内でも数名といった状況である。

3.11.3. 経験談
3.11.3.1.「セキュリティ業務」を実施していて苦労した経験
『セキュリティ業務』といっても、施策を打ちながら自社のセキュリティ体制を整え

る光の部分がある一方で、個別のインシデント対応では、地道な確認作業が必要になることもあり、影で支える業務が存在するのも事実。光と影がリンクすることでチームとして光ることができれば、影の業務であってもその業務にやりがいを持ったり、光の部分を支えているというプライド持ったりすることができる。また、影の部分を通して現場で発生するリアルな事象を経験し、知識を蓄積できたことは非常に大きい。

3.11.3.2.「セキュリティ業務」をしていてよかった経験

金融系のシステム開発を担うため、求められるセキュリティレベルも必然的に高くなっている。その厳しい環境において業務ができているのはいい経験なのかもしれない。きわめて専門的な内容は、セキュリティ専門の部署やベンダーに任せるが、IT ソリューションを事業の１つの柱とする会社であることで、技術的なことに関してもベースの経験や考えがあり、技術論に関するアレルギーがなく、セキュリティ業務に対するアドバンテージになっていると感じている。

また、本社部門は経営に直結している組織なので、『ないルールは作る』という立場にあり、必要な裁量が与えられている。日々発生するインシデントの中には不審メールの着弾等、細かなものもあり、どのレベルまで管理すべきなのかという課題は常にあるが、適宜上層部と意見を交わしつつ、環境やルールを自ら作っていける部分はやりやすいと感じている。

3.11.3.3.「セキュリティ業務」に着任しての処遇変化

現部署ではセキュリティ業務単体でのアサインではないため、他の業務と合わせ総合的に評価される。

3.11.3.4.自社のセキュリティ維持向上に効果が出たという取り組み

インターネット閲覧基盤の導入である。閲覧基盤の導入にともない、各社員の PC ブラウザから直接インターネットを見ることができなくなった。社員にとっては利便性とのトレードオフになったが、外部との分離によりインターネットの閲覧によるウイルス感染の脅威に気を回さなくてもよくなったことは効果として大きい。社員自身がセキュリティインシデントを起こすリスクが減ったという認識で結果的に了承してくれてはいるが、セキュリティと利便性のバランスに悩むところではある。金融に関わる業務の特性上、情報の流出には特に気を配っている。

また、社内の OA 環境を作っている部署が合わせて守りもしているため、自ら作ったものは自分自身が一番理解しているので効率的である。

3.11.4. キャリアパス

3.11.4.1.「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

(注) 本項はインタビュイー3 名それぞれを①②③に分けて記載。

① インターネットからのリクエストに対してリアルタイムにホストコンピューターに問い合わせるカードシステムの構築に携わっていた。システムの品質維持としてセキュリティ対応が不可欠だったことから、外から侵入テストをしてセキュリティホールを見つけるなどしており、『セキュリティ業務』という個別な分離はなかったものの以前から関わっていた。それらの経験をベースにして、社内側へ視点を変えたのが現業務である。

② システム開発部門でインターネット系のシステムを担当していた経験もあり、当時の上司に現在のポジションに招かれて現業務についた。

③ 全体統括部署として総務＋企画業務をする中で社内のあらゆる情報が集まりだし、セキュリティに関する業務が入ってきたという流れだった。

3.11.4.2.「セキュリティ業務」前に行っていた業務内容

(注) 本項はインタビュイー3 名それぞれを①②③に分けて記載

① 元々はシステム開発をしており、自社がインターネットビジネスをはじめる時に立ち上がった部署でインターネット系のシステム企画に携わっていた。その後、クレジットカードの照会等の機能を備えたオンラインシステムの企画・構築を担当していた。

② インターネットバンキングシステムのアプリ開発に従事しており、セキュリティ攻撃の脅威と常に隣り合わせだったため、セキュリティ業務に対する親和性は高かった。学生時代にシステム開発・プログラミングの学習の機会はあったが、セキュリティについては一般的な基礎学習にとどまっている。

③ 金融関連会社の事務集中系の基幹システム開発に携わっていた。基本的には社内システムだったため、外部からの脅威という意味では、インターネットシステム程のセキュリティの考慮は必要なく、業務要件やインフラ周りに専念していた。

3.11.4.3. 「セキュリティ業務」についたことによるキャリア（観）への影響

（注）各インタビュイー個別の将来のキャリア観については①②③に分けて記載

① 現時点では配属されたアサイン先でめいっぱい頑張るという気持ち。ただ、今後はどこにいっても情報セキュリティに関わる要素はついて回るのだとは思う。これまでの経験を通して総合的な力が備わってきていると感じている。

② 継続してセキュリティに特化した仕事をしたいかというとそうではなく、セキュリティ業務の経験をシステム開発の業務に活かしたいと考えている。

③ セキュリティを生業にするには、技術的かつ専門的な内容をより深く学ぶ必要があると感じており、どちらかというとマネジメント側で関わりたいと考えている。セキュリティに携わっていた経験は社内で重宝されるのだろう。

＜共通＞

社内セキュリティインシデントを統括し、事象を俯瞰してみると発生を 100%防ぐのは無理ということがわかった。発生は防ぐことができない代わりに、起こった時に影響がないように出来ればよいのではないか、という観点を持つようになった。

また、以前は『どうやればクラッキングが成立するのか』や、『攻撃をどう防ぐか』いうことに考えがいきがちだったが、最近では『最終的には何を守るべきなのか？』という考えになった。100%のセキュリティ対策は無理で、かつ、やってもきりがないという認識の下、守るべき情報がどこにあってどう守るかを考えるという思考に切り替わっている。セキュリティ対策が必要な業務を担当しているとセキュリティ専門ベンダーにも近いことから色々な情報が入ってきてそのような意識にはなるが、そうでない立場の場合は、なかなかそういう考えにいたらないのが現実と思う。

これまではあえて情報セキュリティとその他リスクを同じ枠で考えていたがもはや、情報セキュリティを独立させて考えないといけなくなっているのが昨今の流れであると感じる。

3.12. ケース 12（情報サービス業：対外向けサービスセキュリティ担当）

3.12.1. 企業プロファイル

インタビュー対象企業グループ：グループ 2
インタビュータイプ：個人

組織図
掲載なし

業種
情報サービス業

企業規模

社員数	10000名以上

3.12.2. 業務内容の把握

3.12.2.1. 「セキュリティ業務」の位置付けとして現在行っている業務内容

SIEM 製品（2003 年頃）がこれからという時代に、海外の先進的な製品を輸入し、プロダクト部門のリーダーを 7~8 年間担当し、公共・金融・医療機関等に機器の納品や利用方法の説明、コンサル的なアドバイスを行っていた。その後、IT 全体統制や海外の SOX 法対応等の上流に携わるようになったが、現在は脆弱性スキャンツールや Web、ネットワークのセキュリティ対策製品を扱うプロダクト部門で管理職に就いている。

3.12.2.2. 「セキュリティ業務」を兼業で実施している場合には兼業の業務内容

現在、兼業はないが過去（2014 年頃）に社内のネットワーク部隊に招集され、インフラ基盤に仮想化の技術を導入するため、ネットワーク構築業務を 2 年ほど行っていたことがある。

3.12.2.3. 「セキュリティ業務」につくにあたって研修などの教育有無

＜過去＞

自身のスキルアップという点では、海外から情報を収集する事が多かった。日本ではまだセキュリティに精通している人が少ない時代からかかわっているため、必然的に情報収集が海外からになった。

また、1998 年頃からセキュリティ事業に携わっており、その頃からセキュリティ人材の育成に関わってきた。現在もそうだが、当時もセキュリティ業務経験や専門知識をもっている人材は希少であった為、ネットワーク、サーバの知見を持った人材を中心に中途採用を行い、入社後に社内のセキュリティエキスパートの下で研鑽を積むという方法をとらざるを得なかった。活用したのは、製品仕入れ先に在籍している高い技術をもった海外のセキュリティ技術者を日本に招き、ペネトレーション等、実際に製品に触れながら行うトレーニングだった。

＜現在＞

現在では様々な機関がセキュリティ技術に関する研修サービスを提供しており、会社の技術者育成プログラムの中にもセキュリティは選択可能な項目になっており、多くの技術者が外部の研修を受講している。また、高度な技術者を育成するために経験豊富な社内セキュリティ技術者が社内研修の講師を担当するセキュリティ人材教育プログラムを立ち上げた。受講者は社内で選抜されたメンバーが対象となっている。初めに基本的な内容について外部研修を受講してもらい、その後社内講師によるオリジナルなプログラムを実施し、最後にテストを受ける内容で、通年実施している。

3.12.2.4. 「セキュリティ業務」を行う環境（体制）

IT セキュリティのコンサル、機器販売、運用保守などサービスとして行っている業務と自社（企業）のセキュリティ業務と 2 つの体制にわかれている。

・社外向けサービス
　ウイルス対策、FW、IPS 等の製品全般を販売する組織と、セキュリティ対策導入のコンサルテーション、脆弱性診断サービス、SOC サービス、SIEM 製品を導入などのサービスを提供する組織がある。

・社内セキュリティ対策
　自社内のセキュリティは情報システム部門が対応しており、自社取り扱いのセキュリティ製品、サービスを活用し、セキュリティサービス部門と連携して行っている。
セキュリティサービス部門と情報システム部門では業務の連携はあるものの人の異動などは発生していない。

3.12.3. 経験談

3.12.3.1.　「セキュリティ業務」を実施していて苦労した経験

＜顧客対応＞
　セキュリティ対策について経営陣になかなか理解されないため、セキュリティ対策にかかる費用が予算化されていないことがある。有事の際も企業によっては、購買プロセスが発生し正式依頼までにリードタイムが発生することがある。有事の際は、至急対応が必要なため、先に対応を行うが対応後の回収（金銭面）をどうするのかという交渉、調整が発生することがある。

＜社内対応＞
　グループ企業、提携先企業含めセキュリティ対策対応レベルを一定水準以上確保するために啓蒙活動から実施する必要があり、顧客対応同様の苦労があった。

3.12.3.2.　「セキュリティ業務」をしていてよかった経験

　業務内容自体が企業継続にかかわってくる場合もあるため、業務に価値があり、やりがいのある仕事だと気づけたこと。また、自分の市場価値があがったこと。

3.12.3.3.　「セキュリティ業務」をしていて悩んだ経験

　日本企業では制度上セキュリティエンジニアに対して人材市場価値同等の地位や待遇を準備することが難しく、せっかく育てても待遇のよい外資系のセキュリティベンダーに一本釣りされるケースが発生する。

3.12.3.4.　「セキュリティ業務」に着任しての処遇変化

　特にない。

3.12.3.5.　自社のセキュリティ維持向上に効果が出たという取り組み

　社内セキュリティ対策を組織横断的に対応できる仕組みとし、結果的に高度なセキュリティ人材が対策、対応可能な体制になっている。また、グループ企業、提携先企業に対しても啓蒙活動を続けた結果、一定水準以上のセキュリティが確保されるようになった。

3.12.4. キャリアパス

3.12.4.1.　「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

　会社が IT セキュリティの事業を発足させることになり、もともと英語を使えたことやネットワーク構築業務を経験していたこともあり任命された。自分が導入したネットワークを守るために必要だと思っていたため前向きに臨むことができた。

3.12.4.2.　「セキュリティ業務」前に行っていた業務内容

　輸出中心の電気メーカーでの商品企画、販売業務に従事していた。

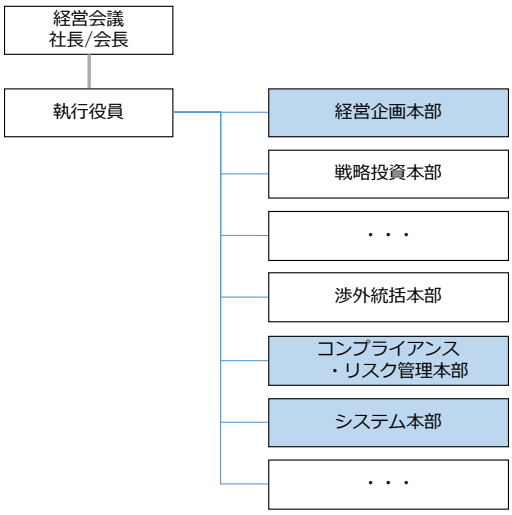
3.12.4.3. 「セキュリティ業務」についたことによるキャリア（観）への影響

英語とセキュリティ業務経験があれば、年齢に関係なく転職の引き合いが多くあり、終身雇用、年功序列のシステムに囚われなくなった。

3.13. ケース 13（インターネット付随サービス業：自社内セキュリティ担当）
3.13.1. 企業プロファイル

インタビュー対象企業グループ：グループ 1
インタビュータイプ：チーム（部署間連携）

組織図



業種：
インターネット付随サービス業

企業規模：

社員数	連結：約2500名

3.13.2. 業務内容の把握
3.13.2.1. 「セキュリティ業務」の位置付けとして現在行っている業務内容
アプリケーション診断を内製化しており、脆弱性診断や脆弱性情報の配信を全社に行っている。SOC も立ち上げており異常検知の強化も行っている。
また、技術アドバイザリーとしてセキュリティポリシーのアドバイスを行ったり、内部監査や e ラーニング研修なども行っている。

3.13.2.2. 「セキュリティ業務」を兼業で実施している場合には兼業の業務内容
セキュリティ部門、情報システム部門、リスクマネジメント部門の 3 部門で CSIRT を形成しており、それぞれの業務を兼務しながら活動を行っている。
セキュリティ部門
・セキュリティ部

情報システム部門
・IT 戦略部
・IT 基盤部

リスクマネジメント部門
・コンプライアンス・リスク管理本部
・法務部
・経営企画本部

3.13.2.3. 「セキュリティ業務」につくにあたって研修などの教育有無
会社から特別にセキュリティに特化した研修を受けたことはない。普段の業務を行っている中で、都度調べつつ知識をつけている。体系的に学習するというより、OJT でスキルを身につける形。ただし、CSIRT メンバーに入る際には、簡単ではあるがオリエンテーション的な形での教育は行っている。
3.13.2.4. 「セキュリティ業務」を行う環境（体制）

セキュリティ部にも技術グループと推進グループに分かれており、それぞれ有事と平時の対応を行っている。技術グループは全員エンジニア。推進グループはエンジニア経験がある人も数名いるが、基本的にはエンジニアではない。IT 戦略部の中には OA サポートやインフラ部隊との橋渡しなどを行っている部隊があり、このあたりが部の中では最もセキュリティに関連する業務に直接携わる。

3.13.3. 経験談

3.13.3.1. 「セキュリティ業務」を実施していて苦労した経験

CSIRT は専任ではおらず、各部門から兼務して行っている仮想組織であるがゆえの共通理解、認識が難しい。また、事業が多角化しており、部署間での共通のポリシーを適用する調整が非常に難しい

また、『セキュリティ部門＝お墨付き部門』と思われがち。各事業部に対し、セキュリティ部門としてアドバイス（暗号化方式等）は行うが、実装運用責任は各部門にあり、実際に実行したかどうかまでは追わない。各部門もセキュリティ部門に言われたからやっているという感覚で対応していることが多く、各部門のセキュリティに対してのモチベーションの部分で苦労している。

セキュリティに関しては、どの企業もあまり内容を外に出したがらないため、他社がどのようにやっているのかという情報を得ることが難しい。これらの情報交換は CSIRT コミュニティを通じて行うことが多い。

3.13.3.2. 「セキュリティ業務」をしていてよかった経験

セキュリティ脅威から会社を守るための活動ができている。対応後の社員からの『ありがとう』という感謝の気持ちが嬉しい。CSIRT に入り横のつながりができたことや、単体の商品の開発に比べ、全体を見なければいけなくなり、視野が広がったことなどが良かったと感じている。4～5 年前と比較するとスペシャリティが高まってきている。

インフラエンジニアとして業務を行ってきた立場からすると、クラウド化の流れにより徐々に業務の幅が狭くなってきている実情がある。セキュリティに携わることで、高い視点から物事を見ることができるようになり、新たなキャリアパスが築けたと感じている。

3.13.3.3. 「セキュリティ業務」をしていて悩んだ経験

インシデントの発生がないことを前提に対策をするため、成果が見えにくい。そのため、モチベーションの維持が難しい。

3.13.3.4. 「セキュリティ業務」に着任しての処遇変化

特別な報酬は無いが、外部視点では市場価値は高まっていると思われる。資格取得支援（還付やインセンティブ）は、セキュリティに興味を持ってもらうという意味も含めて議論しており、制度化までは至っていないが個別に判断している。

3.13.3.5. 自社のセキュリティ維持向上に効果が出たという取り組み

以前は、社内でセキュリティ部は敵だという見られ方をされていたが、会社を守るためにいろんな活動をしていることが社内に浸透していき、今では社内からの見られ方が大きく変わり、色々な方から相談をうけるようになった。

3.13.4. キャリアパス

3.13.4.1. 「セキュリティ業務」についたきっかけ(つきたいと思ったきっかけ)

・上司の指示でセキュリティ業務についた。当時は全く興味がなかったが今となってはやりがいを感じている。

・元々インフラエンジニアだったが、クラウド化が進むにつれ自分の仕事が徐々に減っていくのではないかという危機感のもと、自らの意思でセキュリティ業務にすすんだ。

3.13.4.2. 「セキュリティ業務」前に行っていた業務内容

・理系（国際保健、統計）研究、プロジェクトマネジメント

・理系（生物系　DNA 解析）インフラ運用業務
・文系（法学部国際政治学）IT コンサル

3.13.4.3. 「セキュリティ業務」についたことによるキャリア（観）への影響

セキュリティ業務に携わるまでは、テクニカル寄りでアウトプットも技術ベースだったが、セキュリティ業務を兼務するようになり、論理だけではなく状況判断も必要になることがあり、捉え方や思考が変わった。

また、ここ数年でセキュリティの要素が非常に高まっており、今後、何らかのプロジェクトに携わる際もセキュリティ要件で今の経験が活かせると思う。

あとがき

本書の発行にあたり、多くの方にご協力いただきました。この場を借りまして御礼申し上げます。

発足以来、検討・調査をしてきた JTAG キャリアデザインワーキンググループではセキュリティ人材に関する調査をインタビューという形式で行い、事例集としてまとめました。セキュリティへかかわるきっかけは様々ですが、守るという使命感、業務のやりがい・重要性と、それぞれの思いを伝えていただきました。今回の調査がセキュリティという領域に興味を持つ方の、キャリア形成の一助になれば幸いです。

今回の調査では、まだまだインタビュー対象企業が少ないことも事実です。また、比較的大規模企業が対象になったことから、今後は日本の会社の大多数を占める中堅・中小規模の企業も対象として調査を継続していきます。セキュリティ業務に携わる全ての人材のキャリアデザインを描いていくことで、キャリア形成への貢献に努めてまいります。さらに、JTAG 認定ワーキンググループとも協力をしながら、セキュリティ人材の地位向上に寄与できるよう活動を進めております。引き続きの調査にあたりまして、インタビューへのご協力をお願いいたします。

最後に、多くの企業様に JTAG の活動へご賛同いただければ幸いでございます。JTAG 並びにワーキンググループ活動につきまして、ご質問ありましたらお問い合わせ先までご連絡をお願いいたします。

＜お問合せ先＞

JTAG 事務局（JNSA 内）jtag-sec@jnsa.org

インタビュアー

金田 克彦（株式会社パソナテック、キャリアデザインワーキンググループリーダー）
板倉 恭子（ネットワンシステムズ株式会社）
大槻 晃助（株式会社ラック）
尾方 佑三子（株式会社ラック）
玉川 博之（株式会社 VSN）
冨田 高樹（みずほ情報総研株式会社）
平野 恭祐（株式会社パソナテック）
藤木 将善（株式会社パソナテック）
持田 啓司（株式会社ラック、情報セキュリティ教育事業者連絡会代表）

椎名 司　オブザーバー（株式会社パソナ）

※リーダー以外は五十音順