セキュリティ業務を担う人材の現状調査報告書

（2018 年下期調査）

Ｖ１．０

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）
2019 年 6 月 19 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のための検討を行っている。

平成を振り返ると、『インターネットの普及』・『「ガラケー」から「スマートフォン」への変化』・『クラウドの登場』・『SNS の浸透』と、テクノロジーが大きく進化した。ハードからソフトへの変化、オンプレミスのようなプラットフォーム専有から、クラウド環境におけるプラットフォーム共有への変化は特に著しい。テクノロジーの変化に合わせるように社会も大きく変わった。パソコンが貴重な時代の平成前期から、現在では一人複数台のデバイスを使い在宅ワークやリモート業務を可能にし、ウェブ会議は当たり前のように行われている。これらの変化により、一層の情報リテラシーやセキュリティ意識が求められる時代になったといえるであろう。

社会構造の変化に伴い、社会を構成する我々にも変化が求められるようになったのではないか。大企業では数千人規模での早期退職制度による人員削減を発表[1]し、大企業だから継続した雇用という時代ではなくなった。さらに、経済協力開発機構（OECD）の調査によると「既存の職業の約 14%は自動化の結果消滅し、約 32%は根本から変化する可能性[2]」があると伝えている。少子高齢化による労働人口の減衰、仕事自体の減少と変化は、テクノロジーの利用をさらに活性化させることだろう。すでに不足していると言われているセキュリティ人材が、さらに多岐多様な業界で求められ、より影響を受けるのではないだろうか。なお、2018 年上期の JTAG キャリアデザイン WG の調査報告書[3]の「はじめに」では人材不足を取り上げている。

セキュリティに限った話ではないが、変化が多い時代だからこそ、組織内の人事異動・OJT による受動的な学びだけではなく、組織を超えたコミュニティでの能動的な学びも必要だと思われる。そして、学んだ成果を発揮する場、能力を評価する場を用意していくことも継続学習には必要であろう。内閣府の年次経済財政報告[4]では「4 割程度の企業については自己啓発を実施しても処遇を変化させないと回答」と記載がある。人生 100 年時代とも言われる今日、一人ひとりが何を学びどう変化に活かすかを考える意識や、学びの先に何があるのかを示す指標、さらには学びの成果を評価する仕組みづくりが必要ではないだろうか。

JTAG では、セキュリティが多くの人のキャリアに影響を与える事を想定し、キャリアデザインワーキンググループではキャリアの指標作成を、認定ワーキンググループではスキルの可視化を目指して活動している。働き方改革に代表されるように、これからの時代は組織に合わせた働き方から、個人にあった働き方へと変化をしていくことだろう。JTAG の活動が、令和時代を生きるセキュリティ人材の長期活躍を支援し、納得いくキャリア形成の一助になれば幸いである。

---

[1] https://www.nikkei.com/theme/?dw=19021901
[2] https://community.oecd.org/docs/DOC-132202
[3] https://www.jnsa.org/isepa/images/outputs/JTAGreport2018_1H_1.2.pdf
[4] https://www5.cao.go.jp/j-j/wp/wp-je18/index.html

調査結果考察

2018 年度の調査は上期 12 社、下期 5 社と計 17 の企業からヒヤリングを行った。セキュリティ人材のインタビュー調査にお答えいただくだけあって、どの企業もセキュリティについて一定の理解が進んでいる企業であった。各社の特長はあれ、企業の規模や業種など違いが見える結果となっている。今回の調査結果の考察では、下期だけの考察でなく、上期調査との比較や、他団体の資料なども参考にしながら考察を行なっていく。今回ヒヤリングを行った対象のうち 1 つは個別レポートを省略し、共通の課題を抽出した総合的な記載としている。

1、下期インタビューのまとめ

2018 年度の調査はインタビューが 5 社と上期と比べると少ない結果となった。しかしながら、企業規模が 10 名程度の企業や 300 名程度の企業と、上期と比べても特徴がある企業にインタビューをすることができた。社員数の違いはセキュリティ人材のあり方の違いも見えてくる結果となっている。

1 つ目の違いとしては、そもそものセキュリティ人材のあり方である。社員数が数 100 名規模の企業では、「ひとり情シス」という言葉に代表されるような、事実上一人でセキュリティを含めた IT 全般の業務を担当するというケース事例が見受けられた。ただし、逆のケース例として、組織的な対応をしているという事例も聞けた。これらの違いは、業界や業種といった会社を取り巻く事情などが影響を与えていることが想定される。ギャップや温度差の違いなどが業界により違うこと、さらには業界内でも違いが存在する可能性が高いのではないだろうか。

また、社員数が数 10 名規模の企業では、事業部門の担当者が必要なセキュリティを担当しているという事例を聞くことができた。セキュリティ業務を兼業で行うという事例は他企業でも話を聞けたが、総務部門や IT 部門のような間接部門が多かったため、事業部門の担当者が兼業するケースは初めての事例であった。ただ、事業部門の担当者がセキュリティも担当しているといった事例は、社員数 10 名規模の企業においては多い事例ではないだろうか。セキュリティ人材の側面を持った事業部門の担当者という立場は、セキュリティ人材という枠に収まらないことだろう。プラス・セキュリティの要素など多角的な考察が必要な事案だと考えられる。

2 つ目の違いとして、キャリアや評価、育成における違いである。主にセキュリティに関係する業務を 1 人で担当していると答えた企業は、技術スキルの習得に自身で行動し、必要なツールなどの内製化・導入を進める傾向があるようだ。逆に組織的に対応をしていると答えた企業は、勉強会などをする機会を設けていた。どちらが正解という性質のものではない。しかし、自組織の性質や成熟度、課題などを見定めた対応が求められるであろう。現状からの変化のタイミングでのセキュリティ人材の行動は、セキュリティ人材がステップアップをするチャンスと言えるのではないだろうか。

そして、事業部門の担当者が必要なセキュリティを担当している事例であるが、必要であればセキュリティトレーニングを受講するなどの対応をしていた。すなわち、事業に必要なセキュリティを学びながら事業運営を行なっているという事になる。こういった経験がビジネス感覚を持ったセキュリティにつながるのではないだろうか。トレーニング機会

と合わせて、ISAC のような同業界の事業者同士の情報交換の場の活用も望まれるところである。セキュリティがビジネスと密接に関係し、多くの人に求められている現在においては、事業運営とセキュリティという組み合わせは、キャリアアップに求められる必要な要素の一つと感じることもできた。セキュリティ人材のキャリアを考えるにあたって、興味深い事例であった。

今回のインタビューの結果は、サンプル量と事例の特殊性から、本報告書が目的とする「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」に当てはまらない部分があることは否めない。しかし、キャリアデザインを描く上では非常に興味深い結果と考えている。

2、上期・下期のインタビュー比較のまとめ

2018 年度の上期（調査期間：2018 年 4 月～2018 年 9 月）と下期（調査期間：2018 年 10 月～2019 年 4 月）を比較し、傾向を分析する。下期インタビューのまとめでも記載した、社員数による違いは上期と下期を比べるとより顕著に見ることができる。逆に社員数に関わらず共通する事項も見ることができた。

はじめに、上期と下期での大きな違いで顕著に現れたのが、「セキュリティを担う組織」という点である。上期は組織としてセキュリティ業務を担う場合が多く、インタビューをするにあたって、どの担当にインタビューをすれば良いかなど、セキュリティ業務の関係者が多岐に渡る事例があった。下期においては、組織でという企業もあったが、実質 1 人で担当しているという企業の例が多かった。

次に、上期と下期で共通する課題も見て取れた。「育成」という点である。上期調査では、組織の取り組みの中に育成人数や育成計画を盛り込んでいる企業があった。組織の規模に対しての人数不足や、業務の偏りを改善するための育成のように、各社による目的の違いはあるが、育成を考えていない企業はなかったように感じている。組織としてセキュリティを対応するには、構成員それぞれの成長を考える必要が求められるのではないだろうか。逆に、下期のインタビューでは実質 1 人で行っているという特性上、自身の成長がそのまま組織の成長につながる場合が存在する。しかし、万が一担当者が不在になるような場合、セキュリティレベルを維持しながら事業運営を行なうことができるのであろうか。

また、組織によっては数年サイクルでのジョブローテーションが仕組み化されており、人事発令後に慌ただしく新しい役割を担うケースもあるいう。組織形態や事業規模による人的リソースの考慮は必要であるが、個人の努力のみに依存せず、セキュリティ人材が不在になったり、総替わりしたりすることを想定して各社各担当が育成の仕組みを考えることは、現セキュリティ担当のキャリアアップと、次のセキュリティ人材のキャリアスタートのきっかけになるのではないだろうか。

さらに、「育成の方法」という点においても上期と下期で共通する部分が見てとれた。基礎となる最低限の知識を、資格やセミナーで得るということである。一部、上期調査の企業で、社内独自にカリキュラムを作成し教育しているという企業もあったが、インタビューにお答えいただいた人の多くは、資格の勉強やセミナーを通して知識のインプットをしていた。セキュリティのキャリア形成において、セミナーや勉強会への参加といった能動的な学習は、キャリアアップの必要な要素と感じる事例であった。共通する部分が見られた半面、より深く調査すれば、研修受講費や教材費の補助に代表されるようなサポート面で違いが出てくる可能性が存在する。キャリアアップのしやすさという点に違いがある

のかは、継続した調査が必要な事案である。

最後に、「評価」という点である。資格手当などで差別化される企業はあったが、特別にセキュリティ担当だからと処遇が高まるという企業は調査期間全体を通して見受けられなかった。評価においては各社の特徴が出やすいところであるが、専門性を高め、専門家としてステップアップをする方が評価される場合もあれば、多くの部署を経験し、異動をしながらステップアップをすることで評価される場合もあることだろう。社会人生活が 40 年を超える中で、セキュリティ業務を経験した場合と、経験していない場合の処遇の差などは今回の調査だけで判断できるものではない。しかし、業界によっては、長い実績を鑑みると、部署異動を重ねた人が昇進の機会を得やすいといった傾向を、今回のインタビューを通して垣間見ることができた。

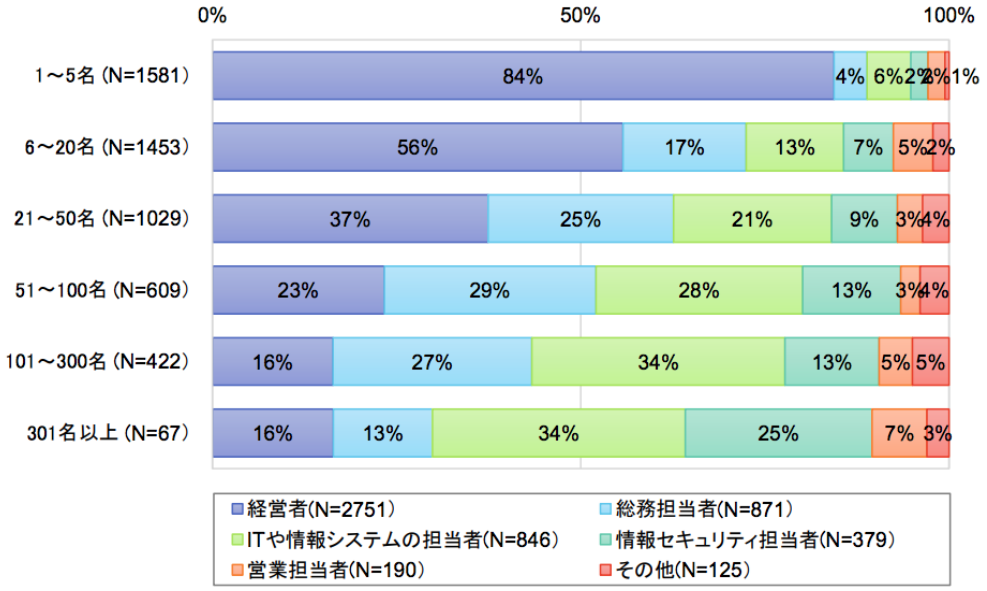
上期、下期を通してみると、上期調査の対象となった社員数が多い企業の方が計画的に実施されているように感じた。そのためキャリアパスも描きやすく、成長がしやすいのではないだろうか。逆に下期調査では、自分で考え判断することがより求められる環境であるように感じた。自社内で相談できる人がいない、自分の判断が事業運営を左右する状況はより人を成長させることだろう。そしてこの環境は、上期調査の中で語られた『前例がないことを、調べ・考え・判断しながら進めた経験が成長のきっかけになった』ということに共通する要素を持っているのではないだろうか。

3、他団体の資料とヒヤリング結果の考察

2018 年度のインタビューについて、業界・業種・企業規模と違いがある中でも、セキュリティ意識を持ち取り組んでいることが見て取れた。しかしながら、サプライチェーンという言葉がセキュリティを考えるキーワードとなっている今日において、自社のセキュリティが万全だからという事で安心ができない時代である。今回の調査を踏まえ、ほか団体の資料も参考にしながら、考察を行う。

はじめに、『2018 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策　の実態調査- 調査報告書 -』[5]をもとに考察していく。
注目する点として、『SECURITY ACTION 自己宣言の主導者（役割）』の分布である。

図 1：SECURITY ACTION 自己宣言の主導者（役割）



『2018 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策　の実態調査- 調査報告書 -』P26 より引用

注目の 1 つ目として、社員数 20 名以下の企業では SECURITY ACTION 自己宣言の主導者が、経営者と回答をしている点である。ただし、SECURITY ACTION 自己宣言の主導者だから実務担当者ということは直結しないだろう。しかし、今回の JTAG インタビューでも社員数 10 名規模の企業では役員層がインタビューを答えている。セキュリティ関係の取り組みを進めるに当たって、企業規模が小さい企業ほど経営者（経営層）の影響が大きいと言えるのではないだろうか。単純にセキュリティ人材のキャリアを考えるだけならば、社員数の多い企業の方が、兼務を含め業務経験を積みやすい環境が整っているように見て取れる。しかし、本来のセキュリティの意味からすれば、セキュリティ対策の有無が事業継続や経営に大きく関わる社員数 20 名以下の企業に対してこそ、セキュリティ人材のあり方についてなど、より議論されていく必要があると感じる。社員数 20 名以下の企業でのセ

[5] https://www.ipa.go.jp/security/fy30/reports/sme/index.html

キュリティ業務経験が、キャリアのプラスに繋がることが大切であろう。

2 つ目の注目点としては、社員数が 20 名を超えてくるタイミングで、総務担当者・IT や情報システム担当者が SECURITY ACTION 自己宣言の主導をしたという点、社員数が 300 名を超えると情報システム担当者が主導したという 2 点である。こちらも主導と業務担当者が異なることはあるだろうが、インタビューの結果と合わせると、総務部門・IT 部門はセキュリティ業務に関係している割合は高かった。社員数が 30 名を超えるタイミングは、より組織的な対応として、総務・IT 部門等の複数の部門が関わりだす転換点と見ることができるのではないだろうか。そして、300 名を超えるタイミングでは情報セキュリティ担当者が SECURITY ACTION 自己宣言の主導をしている。情報セキュリティ担当者なので、実際にセキュリティ業務に従事しているはずである。これらの結果から、社員数が増えるタイミング、特に 20 名を迎えようとする時期と 300 名を迎える時期は、キャリア形成のきっかけや変換点になるタイミングと見ることができるのではないだろうか。変化を迎えるタイミングまでに何を学び、どのような経験を積めば良いのかを定めていくことは、円滑なキャリア形成を支援するものになるだろう。

最後に、企業を取り巻くセキュリティとして、サプライチェーンの問題をよく耳にする。一企業だけでビジネスが完結する時代ではないため、複数の企業が関係したビジネス展開をすることは珍しくない。プライバシーマーク制度[6]や ISMS 認証制度[7]などを取得することは、企業のセキュリティレベルや意識を対外的に示すことができるであろう。しかしながら、企業間での取引となると『IT サプライチェーンにおける 情報セキュリティの責任範囲に関する調査』[8]にまとめられているように、『委託元と委託先の意識のギャップ』や『責任範囲を明確にできない』といった課題があるようである。セキュリティ人材は今後、自社内を超えたセキュリティ対応を求められるのだろうか。必要とあれば取引先と協議をしながらセキュリティ対応に臨む場合もあると思われる。一部では、すでに取引先やサードパーティベンダを監査・調査するような場合が存在している。業界・業種・業務特性による対策や対応の違いを理解し、セキュリティの相乗効果が狙えるような議論ができる環境は、セキュリティ人材が活躍できる場につながっていくのではないだろうか。そして、これからのセキュリティ人材のキャリアアップには、自社だけで完結しない、他社（他者）を巻き込んだ経験が必要なのかもしれない。

4、今後の調査に当たって

2018 年度の調査は上期、下期に渡って、共通の質問を首都圏中心で行った。業界・業種の違い、会社規模の違いを見いだすことができた。しかしながら、以下の点においては今後の調査が必要だと考えている。

- 同業界の中での企業規模の違いによるキャリア形成の課題
- 首都圏と地方圏の違いによるキャリア形成の課題
- 年代別に見るキャリア形成の課題
- 組織をまたがってのセキュリティ体制

---

[6] https://privacymark.jp/index.html

[7] https://isms.jp/isms.html

[8] https://www.ipa.go.jp/security/fy30/reports/scrm/index.html

これらに関しては、WG 内でも、それぞれ違いが出るのではないかと議論している。地方圏だから、小規模だからといったことがセキュリティを考えない・対策を講じないという理由にならないようにしなくてはいけない。さらに、企業規模や地域に関係なくキャリア形成ができるようにする必要もあるだろう。キャリア形成の中で、環境や育成方法の選択肢を示しつつ、キャリア形成に必要な要素を考察して行きたい。

また、ヒヤリングを中心に行ってきた 2018 年度の調査であるが、セキュリティ人材のより具体的なキャリア形成を考えるに当たっては、より多くの意見を収集する必要があると感じている。WG 活動を通じて調査方法の検討も行っていく予定である。

2019 年度の活動を通じて、今回の考察を検証しつつ、より多くの方の指標になるように、継続した活動を予定している。

調査方法

1.1. 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人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。

1.2. 調査期間

2019 年 3 月 ～ 2019 年 4 月

1.3. 調査実施方法

担当者への対面インタビュー
※JTAG賛同メンバにて実施

1.4. 調査対象企業

5 社

1.5. ヒヤリング結果のまとめ方

インタビューにてヒヤリングした内容を文書化
※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。

1.6. 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担当されている方
・リスク管理を担当されている方
・CSIRT 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。

1.7. 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。
※本質問をベースにインタビューを行ったが、インタビューを受けた関係者様の実態と合わないこともあり、一部質問をまとめるなどを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。

2. ヒヤリング結果

2.1. ケース 1

2.1.1. 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：サービス業

社長―――情報セキュリティ戦略推進室
　　システム部
　　総務
　　人事
　　事業部 A
　　事業部 B

企業規模：社員数　約 300 名（連結）

情報セキュリティ戦略推進室	9 名(社員 3 名、外部人材 6 名)
システム部	25 名程度（社員のみ）

※外部人材はベンダ等で、常駐ではなく週に 1-2 日程度役割に応じてきてもらっている。

2.1.2. 業務内容の把握

2.1.2.1.「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

情報セキュリティ戦略推進室のメンバとしてセキュリティ全般を担当している。ポリシー策定や新システム導入時のセキュリティ対策、社内のリテラシー教育および CSIRT 活動など。室内での役割としては主に IT 技術に関わる内容をメインで担当している。

2.1.2.2.「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

情報セキュリティ戦略推進室へ入室する前は IT 戦略室で今後のシステム導入を検討する業務を兼業していた。過去に事故があったことをきっかけに情報セキュリティ戦略推進室が新設され、現在は情報セキュリティ戦略推進室でセキュリティ業務のみを行っている。

2.1.2.3.「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

会社として用意している体系的な教育は無い。
学生のころから IT に関わる機会があった。社会人になってからは、第 1 種情報処理試験を取得し、アセンブラを使ったファームウェアの開発、小規模組織における「ひとり情シス」の経験があったことが、セキュリティ技術の習得の素地となっており、自己学習で現在のセキュリティ業務をできるレベルへ達することができた。
同部署のもう 1 名のメンバは IT 技術のキャッチアップが必要なため、一緒に展示会やセミナーへ参加し、その内容について自身が追加の説明をすることで知識をつけられるように工夫している。

2.1.2.4.「セキュリティ業務」を行う環境（体制）

室長とメンバ 2 名の体制。室長は管理職として全般を管理している。自身は IT 技術に関して全般を主に担当している。同部署のもう 1 名のメンバは社内のセキュリティリテラシー向上のための教育や事業とセキュリティのバランスをとるための社内調整などを主に担当している。
ただ、メンバ間での業務はお互いに遂行できるよう日々情報共有や知識の習得を行っている。

なお、特に CSIRT という組織を作ってはないため、必要に応じて情報セキュリティ戦略推進室のメンバと社内関係部署のメンバで実質の CSIRT 活動を行っている。

2.1.3. 経験談

2.1.3.1.「セキュリティ業務」を実施していて苦労した経験

会社として最初に CSIRT 活動を行った時が、苦労した。理由としては、社内や顧客、取引先、関係官庁への連絡を含め全部を一人で仕切ったが、関係者が多く、未経験の業務をどう進めるのかという試行錯誤が多くあり苦労したことにある。
今ではこの経験をもとに、どのように活動すると良いのか等をアドバイスする立場となり社内の CSIRT 活動を推進している。

2.1.3.2.「セキュリティ業務」をしていてよかった経験

技術が好きなので、色々調べたりすることは楽しい。
また、現在の業務を通じて、情報システムの正常系だけではなく異常系＝セキュリティの視点がついたことで視野が広がった。

2.1.3.3.「セキュリティ業務」をしていて悩んだ経験

技術的な側面で最終的な判断時に悩むことがある。自身で情報を様々収集できるスキルは持っており収集を行えるがデマ等も含まれるリスクがある点が懸念される。
情報収集する中で、原文を必ず確認する、協力ベンダのサポートチケットが使える場合は活用する、という方法で懸念点をクリアしている。
もちろん部署内での相談・判断も行っており、特に業務や社内事情に関連する判断は情報セキュリティ戦略推進室での判断となる。

2.1.3.4.「セキュリティ業務」に着任しての処遇変化

セキュリティ業務そのものが特別に処遇されることはない。

2.1.3.5.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

セキュリティを強化することで社内的にはビジネスストッパーとなることもあり、また、利用個人としては多少の不便は出るが業務上は便利になる部分もあり、そこを代わりに担保するなど意識して社内説明や調整を行っている。この点が、自社のセキュリティ維持向上だけではなく事業への貢献としても実感出来ている。

2.1.4. キャリアパス

2.1.4.1.「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)

元々は社内システム担当部署にいたが、セキュリティ関連で人手が必要な時に手伝ったことがきっかけでセキュリティ業務がメインとなった。

2.1.4.2.「セキュリティ業務」前に行っていた業務内容

ファームウェア開発や、社内システムの導入から運用を行っていた。

2.1.4.3.「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

ネットワークは欠かせない世の中において、セキュリティの業務に携わることで技術者としても 1 歩リードしている実感があり、どんな仕事についても役立つ業務だと思っている。
さらに、事業サイドとの調整を通じて事業とのバランスを取りつつセキュリティ業務を様々整えている経験から、何かを形にしていくことの大切さを実感しつつ、実行・説明できるようになった。今後は大規模過ぎない環境であればセキュリティを全部見るような CISO 的な立場を目指してみたい。

2.2. ケース 2
2.2.1. 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

企業規模：社員数　約 10 名
（アルバイト、パートナー含む）

業種：サービス業

2.2.2. 業務内容の把握
2.2.2.1. 「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
現在行っている業務としてセキュリティと位置づくものは、『個人情報管理』が一番関係している。地域おこしや街づくりコンテストといったイベントを行うような事業をしており、関係者には学生がいたりと個人情報の管理は注意して行っている。また、外部のパートナーと協力する機会も多く、NDA などを取り交わすなども関連する業務と言える。
技術的にも VPN などの環境を整えるなども社員で行っている。

2.2.2.2. 「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
兼業という考え方もあまりなく、事業執行としてセキュリティを行っていくことが多い。企業の特性として、新規事業の立ち上げ支援、地方自治体と企業の橋渡しなどを行う企画事業を中心にしている。そのため、初期の段階では関係者も少なく相手企業や地方自治体のセキュリティポリシーに遵守する事がある。

2.2.2.3.「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
特別に何か教育を受けたという事はない。OJT などで進めていくことが多い。過去には、一緒に事業を行う企業様の研修を受講したこともあった。

2.2.2.4.「セキュリティ業務」を行う環境（体制）
専任でのセキュリティ担当という事はなく、3 名（役員 2 名と社員 1 名）が主に対応している。事業執行にあたっての対応でセキュリティが関係してくることが多い。

2.2.3. 経験談
2.2.3.1.「セキュリティ業務」を実施した経験談
※苦労した経験、よかった経験、悩んだ経験については、セキュリティ業務が専門の方へのインタビューではないので、経験談として包括

各企業様のセキュリティポリシーに遵守する事があると、各企業様の特徴が出ることがある。場合によっては手間をかけなければいけないこともあるためコミュニケーションの方法などを変えなければいけない経験をした。
また、外部の人材の活用を考えたことはないが、今後もないとは言えない。ただ、自社内でできないと判断するような場合には、間にベンダを交えた 3 社契約を取り交わすなどしてきた経験がある。
現在では運用系の業務が少ないためこのやり方が自社にあっていると考えている。

2.2.3.2.「セキュリティ業務」に着任しての処遇変化
基本的には事業執行に関係する業務が主業務であり、特別な処遇変化はない。

2.2.3.3. 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

社内のセキュリティ対策として一番大きい取り組みは『持たない』という事だと考えている。規模や要件を見て参画を判断する事もあるし、場合によっては間にベンダを入れるなどの取り組みをし、社内で情報を持つことを少なくしている。自分たちが情報を持たないようにすることが、セキュリティインシデントを防ぐ対策となっている。

2.2.4. キャリアパス

※「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)、「セキュリティ業務」前に行っていた業務内容、「セキュリティ業務」についたことによるキャリア（観）への影響を包括して記載。個人としてのキャリアではなく、組織としての観点で記載。

現状では P マークの取得などは考えていない。企業の特性として新規事業の立ち上げなどをするとなると『スピード感』を考えないといけない。スピード感を意識すると、『セキュリティ』の観点で物事を見た場合に鈍ってしまう場合がある。そのため現在の事業を続けている間は現状のままのやり方で考えている。

現在の主な事業では指示を出してくれる人はおらず、受動的な人はいないような環境での業務となっている。そのため価値観を共有したコミュニティでの業務ができており、今後は雇用の仕方なども変わってくると思っている。そのため現在は『セキュリティ』だからと言って特別な報酬は検討していない。

今後はプロジェクトベースでの雇用などを行っていく。イベントからのつながりや、コミュニティ活動を通じたつながりを雇用に活かしていく。地方では医療系の課題、金融系の課題なども出ているため、セキュリティが必要な場面も出てくると想定している。その場合にも『つながり』を活かしてプロジェクトに Join するというような方法をしていきたい。こういった活動に参加する事は、セキュリティ人材に関わらず『人のキャリア』によい影響を与えると考えている。

2.3. ケース 3
2.3.1. 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：個人

企業規模：社員数　約 250 名　　業種：旅行業

2.3.2. 業務内容の把握
2.3.2.1.「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
日本から欧州への旅行を中心としたツアー手配を主な事業とする企業であり、自身は国内拠点の情報システム管理業務を実施している。海外拠点のシステム管理業務は別の担当が受け持つ。欧州が主要拠点であることで GDPR への対応がセキュリティ業務にあたるとは認識しているが、システム管理業務とセキュリティ業務の境界は明確でなく、複合的な業務となっている。

2.3.2.2.「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
情報システムのサービスデスク業務として、エンドポイントの OS の管理や、セキュリティソフトの検知ログの監視、定義ファイルの最新バージョン適用状況を管理しており、目下、Windows10 へのマイグレーション対応が迫る状況にある。社内の半数以上がノート PC であり、業務形態上社外に持ち出して業務をする社員が多いため、エンドポイントの管理が非常に重要であると認識している。注力するのがゲートウェイか、エンドポイントかは業態によって比重が変わるのだと思う。

2.3.2.3.「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
体系的研修は受けていないが、セミナーや同業他社の担当との会話から自主的に吸収している。申し出れば試験料の補助は出るが、旅行業に関連する試験を重要視する傾向にあり、IT 系の資格は業界的に縁遠いこともあって体系的には存在しない。ただし、会社として積極的な学習を後押ししてくれる雰囲気はある。クラウドの活用を進めるにあたって、セキュリティも含めて有効なサービスにはどのようなものがあるかを自主的に勉強している状況である。

2.3.2.4.「セキュリティ業務」を行う環境（体制）
情報システム管理業務の構成人数は正社員として 4 名で、内訳としては、上長・サービスデスク（自身）・基幹業務アプリケーションの管理プログラマーが 2 名となっている。そこに、サービスデスク（自身）のアシスタントとして派遣社員が 1 名入っている。ジョブローテーションの期間は特に定められておらず、要員補充は突発的に起こる。

オフィスの IT 機器全般・ネットワーク・機器監視といった要素を含めたセキュリティの構成は上長と 2 名体制で考えており、体系的な専門の知識は有していないが、業務に必要な個別の知識は有しているという状況である。

組織としてセキュリティの体制を構築したいという思いはあるが、現状としてセキュリティ専任の要員はいない。旅客リストの処分などのセキュリティ業務に対して、副社長・総務部長が運用責任者ではあるが、実運用に対しては不十分であるととらえている。

2.3.3. 経験談
2.3.3.1.「セキュリティ業務」を実施していて苦労した経験
予防策と緊急対応の方針についてはマニュアルになっているものの、社内でマルウェアの感染が発覚した際に、原因の特定に苦労した経験がある。感染の検知に端を発し、LAN ケーブルの抜線、業務を止めないための PC 交換、中身の確認など初動は速やかに実施できた

が、マルウェアであると断定した以降の調査をどのレベルまで実施するかに悩んだ。上層部と相談したところ、費用対効果の面から、侵入ルートの特定までは実施せず、今後どのように防ぐのかにフォーカスした対応となった。セキュリティインシデントが発生しても、ユーザー（＝現場スタッフ）は可及的速やかに業務に戻らねばならないので、データの復旧、特に安全なファイルをどのラインで復旧させるかなどを瞬時に決断する必要があり、マニュアルに定めた通り動きを体にしみこませる重要さを痛感した。経験をしないことには身につかない感覚でもあると感じている。

2.3.3.2.「セキュリティ業務」をしていてよかった経験

全拠点内において特にアジア（国外）は、セキュリティ主導で施策を講じるため、現場との意見の食い違いが生じがちであるが、これまでの営業アシスタントなどの業務経験を活かして旅行業としての事業背景を説明し、それぞれの立場の考えを伝えるリージョン間の架け橋になっている。セキュリティをきっかけとして社全体の重要な役割を担えるようになったことはよかったと感じている。

2.3.3.3.「セキュリティ業務」をしていて悩んだ経験

ユーザーの利便性とセキュリティレベルの維持のバランスに苦心している。以前 USB メモリを差しても読み込みができないようにしたことがあるが、現場に事前に周知していなかったため混乱があった。

その他、セキュリティに関する社員教育も並行して実施しているが、日常業務の比重が重かったり、年次があがるとわからないことを聞けなくなったりする人間的な要因がセキュリティホールになることを危惧しており、新しいメンバへの教育を起点として、社員全体の意識を変えるのが重要だと感じている。

2.3.3.4.「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業務そのものが特別に処遇されることはない。専門職としての採用もした方がよいのではないかという提言をしつつも事業主体が旅行業ということもありなかなか難しい状況である。

2.3.3.5.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

外部のセミナー講師などのコンテンツは必ず社員がチェックして用意したものを差す決まりにしている。社外の人が社内の PC に直接 USB メモリを差すことを制限したことでセキュリティ向上に一定の成果をみた。

また、GDPR で事故が起きたときの対応は未済ではあるが、情報を取り扱いする人への意識づけのため、個人情報が含まれているのを検知するプログラムは作成している。どこが発信源なのか、どこが罰則の対象になるのか、どこに責任があるのかを切り分ける為には、何が GDPR に関係する情報なのかを意識することからであるという認識のもと対応を進めている。

さらには、予防策はなるべく計画的に立てるという指針のもと、機器の入れ替え、イメージマスターの更新などは計画的に実施している。なるべく物理的な機器は持たず、信頼性の高いクラウドサービスを利用する方針で、全ての持ち出し PC ではローカルに情報を持たないようにしており、BIOS ロック、ネットワークパスワードによって情報へのアクセスを制限することで、情報の流出元を極力縮小している。

2.3.4. キャリアパス

2.3.4.1.「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)

営業アシスタント業務についた際、それまでの業務経験から手配と営業双方の業務を理解できたため、間に存在するアシスタント業務の負荷が非常に高くなり疲弊してしまった。上層部に相談したところ、情報システムに関わるという働き方もあるという教示を受け、旅行業の総合職として就職したので当初は想定していなかったが、そのような働き方もあるのか

と意識の変革があった。

2.3.4.2.「セキュリティ業務」前に行っていた業務内容

総合職で入社し、現在は 9 年目になる。現在の業務の前には、ホテル手配業を 2 年、総合手配を 2 年、営業アシスタントを 2 年半経験した。現在の業務につくまでは、IT の経験は全くなかった。

2.3.4.3.「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

旅行業を目指して入ったが、ジョブローテーションで IT に関わるようになり、IT 目線でどうビジネスを手助けできるか、セキュリティの専門家というよりは旅行会社として IT にどう携わるかという視点になった。ツアーの手配業務をやらずにいきなり営業をやると業務が分からない、管理部門は現場を把握し切れていないという状況の中で、自社の業務を理解し、現場の IT リテラシーレベルに応じた説明能力が必要と考えている。技術的にどこか専門の領域を持ちたいとは思っているがまだ経験が足りない状態ではある。昨今多様化する社員の働き方も踏まえ、全ての部門を経験した人材として、事業とシステム運用の関わり方を経営にどう提言していくかがこれからのミッションであると考えている。

2.4. ケース 4
2.4.1. 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

企業規模：社員数　約 500 名　　業種：情報サービス業

2.4.2. 業務内容の把握
2.4.2.1.「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
社内システムおよびサービスの監視基盤作成や、新しいサービスを企画する時のセキュリティ設計、さらにはインシデント疑いのあるものの調査、ISMS の審査対応のとりまとめなど、セキュリティ関連の仕事を全般的に行っている。

2.4.2.2.「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
社内システムのセキュリティ対応業務だけではなく、サービス商品としての自社開発アプリにセキュリティ上の問題が無いかという相談やチェックなど、セキュリティに関連する業務は全般的に対応している。

2.4.2.3.「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
IPA の第二種情報処理技術者試験(現在の基本情報処理試験に相当)を高校生の時に取得、大学 1 年から研究室に属して専門知識を深め、博士課程（研究テーマは情報セキュリティ）まで履修し、大手 IT ベンダの基礎研究所に就職した。
学生時代から培った高い専門スキルと、常に作業の効率化を考えて行動をするという資質も持ち合わせており、自身の情報収集力とスキルで十分に業務遂行が可能であるため、現時点では研修などの教育が必要ない状況である。

2.4.2.4.「セキュリティ業務」を行う環境（体制）
技術部セキュリティグループの所属にて、顧客に提供しているアプリや各種サービス等の技術に関するとりまとめを 2 名体制で行っている。
いわゆる情報システム部にあたる社内 IT の担当部門は、セキュリティグループとは別に存在しており、セキュリティグループでは、社内外からのセキュリティ関連の問い合わせや、ISMS のリスク管理等に日々対応している。
何か困った時、技術的アドバイスを求めたい時は、社内業務に精通していることも勘案し、入社時に直属の上司だった技術本部のマネージャーへ相談をしている。
技術に関しての相談も、個別の技術詳細というよりは概念的なセキュリティアーキテクチャについてなどが主な相談事項となる。

2.4.3. 経験談
2.4.3.1.「セキュリティ業務」を実施していて苦労した経験
大手 IT ベンダの SOC 時代には、多忙かつ顧客ありき対応という職場環境のため、現状の業務の仕方が効率的には良くないと思いつつ、やり方を変えずに対応せざるを得ないことが多々あった。疑問を感じていながらも、業務が忙しくなると、こなすべき定例業務のサイクルにはまってしまい、そこから抜け出せなくなっていた。
また、新しい目で効率化を目指そうと思っても、周りが忙しすぎて思考停止に陥ってしまっ

ており、効率化を行えず、変わらず忙しいままの悪循環となってしまっていたことに苦心した。

2.4.3.2.「セキュリティ業務」をしていてよかった経験

学生時代から培ってきた自身のスキルを活かし、セキュリティ関連の業務委託は特に行わなくても対応できている。セキュリティ監視基盤の 7 割～8 割は自作の自動化ツールを利用しており、効率化が図れている。

2.4.3.3.「セキュリティ業務」をしていて悩んだ経験

現在、やりたいことが色々あるが、人手不足でできていない。人が増えてくれることに越したことはないが、現状は、優先順位の高いものから対応するしかない状況。
また、事業推進とセキュリティのバランスをどうやってとるか、という点は日々頭を悩ませているポイントである。
セキュリティにより過ぎると事業スピードを鈍らせることもあるが、セキュリティが蔑ろにされないようにしなければならず、うまい落とし所を探すことについて、まだ難しいと思うことがある。
だが、最近はうまく新しい技術を当てはめて導入することで、事業推進とセキュリティを両立することもできるようになってきており、そういった部分も含めて常に考えながら業務をしている。

2.4.3.4.「セキュリティ業務」に着任しての処遇変化

グループとして、スキルの高いエンジニアが多く就業しており、専門性も尊重され、エンジニアの地位は確立されている。また、エンジニアとしての評価基準（リーダーシップ、技術領域への専門知識）についても適正な評価を受けていると感じている。
社内の規定として、外部に対してアウトプットしていくことが評価されたり、従業員は自分の良識に基づいて、業務時間中に開発したソフトウェアを OSS として公開できたりという自由な風土が、エンジニアのスキルアップやモチベーション向上に良い影響を及ぼしている。

2.4.3.5.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

元々セキュリティに対する意識は強い社風だが、ISMS についてのオリエンテーションや社内セキュリティ教育用テストの作成などで、社員のセキュリティモラルやスキルアップの向上に貢献したと感じている。
また、もう一人のセキュリティグループメンバの育成にも積極的で、Slack のチャネルでセキュリティや技術関連の Web ニュースを展開したり、イベントやセミナーは可能なかぎり一緒に参加し、重要ポイント等を事前共有したりと、知識の共有を図っている。
さらに技術本部としては、共通認識を得るために、GitHub のレビューリクエストをグループ内で行うという取り組みを行い、お互いに情報共有や確認をしてからアプライするということを実施している。

2.4.4. キャリアパス

2.4.4.1.「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)

学生時代からの興味関心をきっかけに、スキルアップを行い、自然な流れで現在の職務についた。

2.4.4.2.「セキュリティ業務」前に行っていた業務内容

学生時代からの専攻も情報セキュリティであり、新卒就職先も現職もセキュリティ関連業務のため、IT セキュリティ関連以外の業務はしていない。

2.4.4.3.「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

セキュリティに限らず、ものづくりが好きで、常に“どうすると更に良くなるか”ということを考えて前をみており、ソフトウェアであれば自分で作っていくという姿勢がある。当面は現業に邁進しながら、将来的には CISO を視野に経験を積んでいきたいと思っている。

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。

2018 年上期に引き続き 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形式で行い、報告書としてまとめました。年間を通した比較を行うなど、キャリアの在り方の検討を行っています。セキュリティへかかわるきっかけは様々でしたが、使命感・やりがい・重要性と、それぞれの思いが伝わるインタビューでした。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。

2018 年度の調査では、インタビュー対象企業が少ないことも事実ですが、リアルな声を聴けたインタビューになったと感じています。JTAG キャリアデザインワーキンググループでは、セキュリティ業務に携わる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。また、JTAG 認定ワーキンググループとも協力をし、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。引き続きの活動にあたりまして、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

現状調査報告書作成委員会

玉川 博之（株式会社 VSN、キャリアデザインワーキンググループリーダー）
新井 是昭（ヤマト運輸株式会社）
伊井 あすみ（株式会社ラック）
板倉 恭子（ネットワンシステムズ株式会社）
井田 潤（トレノケート株式会社）
伊藤 良孝（株式会社インターネットイニシアティブ）
上田 健吾（NRI セキュアテクノロジーズ株式会社）
大槻 晃助（株式会社ラック）
尾方 佑三子（株式会社ラック）
柏谷 知美（ネットワンシステムズ株式会社）
金田 克彦（株式会社パソナテック）
砂田 浩行（株式会社日本総合研究所）
槌井 恵子（ネットワンシステムズ株式会社）
三浦 順子（トレノケート株式会社）
渡邉　真裕子（トレノケート株式会社）
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）

※リーダー以外は五十音順