JNSA ワーキンググループ紹介

事業コンプライアンス部会

部会長：倉持　浩明（株式会社ラック）
副部会長：唐沢　勇輔（Japan Digital Design 株式会社）

事業コンプライアンス部会について

事業コンプライアンス部会は、サイバーセキュリティサービス事業者が社会的責任を果たし、顧客からの信頼を確保し、そして自らを守るために、適正な事業運営の在り方を検討する部会です。具体的には、「サイバーセキュリティ業務における倫理行動宣言」の策定と、自己宣言を行う企業の募集や、宣言内容の更新を行っています。また、法執行機関との連絡窓口としての役割や、国内外の法令リスク事例の調査を実施し、成果物として「法令リスク一覧」を会員企業向けに提供しています。

自社は大丈夫？サイバーセキュリティ事業の法令リスク

サイバーセキュリティ事業では、脆弱性情報やペネトレーションテストの技術など、一般の業務では扱わない高度な技術や情報を取り扱うため、扱い方を誤ると、第三者にとって脅威となる可能性があります。例えば、脆弱性情報が漏洩し、それを攻撃者が利用することが考えられます。そのため、法令違反のリスクが常に存在することを認識し、適切な対策を講じる必要があります。

事例：講演や記事によるマルウェアコードの流出

インテリジェンスサービスを提供しているA社のリサーチャーB氏は、カンファレンスやブログにて多数の調査研究成果を公開していましたが、その中でマルウェアの使用を促すような記述があり、一部で動作可能なマルウェアコードを公開してしまった事例です。この場合、不正指令電磁的記録提供罪に問われる可能性があります。調査研究目的であっても、法的に正当な理由がない限り、このような行為は法令リスクに該当する恐れがあります。

事例：契約対象外の顧客へのセキュリティ診断

セキュリティ診断サービスを提供するA社が、顧客B社から指示されたIPアドレスやドメインに対してペネトレーションテストを実施しようとしたが、指定ミスにより無関係なC社に対してテストを実施してしまった事例です。この行為は意図的でなくても、不正アクセス禁止法に問われるリスクがあります。契約のある顧客に対しては正当な業務目的となる行為も、契約のない顧客に対して行うと法令リスクが生じる恐れがあります。

サイバーセキュリティ事業者が留意すべき法令リスクを一覧で提供

事業コンプライアンス部会では、サイバーセキュリティ事業者が留意すべき「法令リスク一覧」をJNSA会員企業限定で提供しています。この一覧は、正当な業務を行っていても抵触する可能性のある法令上のリスクを整理し、事業者が自らの対策に役立てることを目的としています。社内研修でご利用いただくことを想定したプレゼンテーション版もご用意していますので、是非ご活用ください。

事業の正当性を対外的に示す「サイバーセキュリティ業務における倫理行動宣言」

事業コンプライアンス部会ではサイバーセキュリティ関連業務に特有のコンプライアンスリスクを管理していることを社会や関係省庁に対して明らかにすることを目的として、「サイバーセキュリティ業務における倫理行動宣言」を策定しています。正当なセキュリティ事業を行なっていても抵触する可能性のある業務が違法性を問われないためには、「社内で管理体制や教育を周知していること」「それらの取り扱いが必要となる事業を継続的に行っていること」を裏付け、事業の正当性を対外的に示すことが望ましいと考えられます。

「サイバーセキュリティ業務における倫理行動宣言」に則り、サイバーセキュリティ業務を遂行することを自己宣言していただく企業を募集しています。ご賛同頂ける企業はJNSA事務局までご連絡ください。ご賛同いただいた企業名や事業部名は、JNSAのWebサイトに掲載します。JNSAのWebサイトに貴社名を掲載することで、より信頼性が増すと考えられます。

サイバーセキュリティ業務における倫理行動宣言
https://www.jnsa.org/cybersecurity_ethics/index.html

さいごに

事業コンプライアンス部会は、サイバーセキュリティ事業の法令遵守とコンプライアンス強化を推進し、業界全体の健全な発展を目指しています。部会への参加を希望される方は、事務局までお問い合わせください。皆様と共に、業界全体の健全な発展を目指し、より安全で信頼されるサービス提供に取り組んでいけることを期待しています。