JNSA ワーキンググループ紹介

事業コンプライアンス部会

Japan Digital Design 株式会社
企画 WG リーダー　唐沢　勇輔

■ 事業コンプライアンス部会の設立

本部会は、2018年9月3日に社会活動部会の下に設置した「サイバーセキュリティ事業における適正な事業遂行の在り方に関する検討委員会」での議論が元になっています。同委員会の設立は、セキュリティ事業者として業務に携わっていた方が、その業務内容に関連してウイルス保管容疑で逮捕されるという事案（その後、不起訴が確定）の発生がきっかけです。このままではサイバーセキュリティに関する活動の委縮につながってしまうのではないかという懸念もあり、セキュリティサービスの提供者が自らを守るためにも何らかの手立てが打てないかを議論してきました。委員会での提言として、事業コンプライアンス部会の設置と「サイバーセキュリティ倫理行動宣言」の運用が提案されました。

部会の主な活動は以下の通りです。

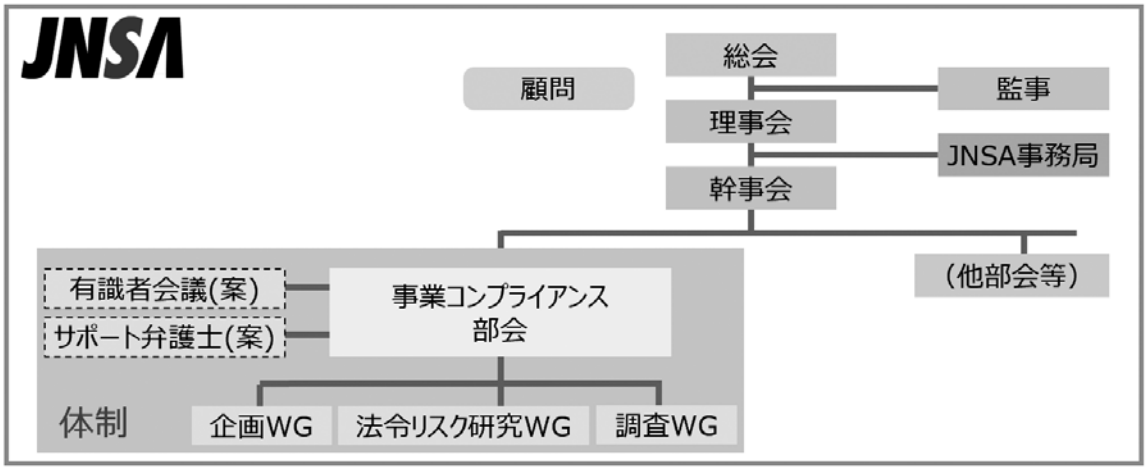
① 業界団体として政府に対し正当なセキュリティ業務が司法捜査の対象とならないよう法整備の働きかけを行っていく。
② JNSA加盟組織が「正当性をもってサーバーセキュリティ事業を行っていることを自己宣言する仕組み」について検討し、業界団体としての健全性を推進していく。

上記②の実現にあたり、「サイバーセキュリティ業務における倫理行動宣言」を2019年8月1日に策定し、自己宣言していただく企業の募集を行いました。2019年12月時点で21社の企業に賛同いただいています。

参考：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/

■ 体制

本部会は以下のような組織体制で運営しています。



図：事業コンプライアンス部会の体制

JNSA ワーキンググループ紹介

部会長:　　西本逸郎（株式会社ラック）
企画WGリーダー:　唐沢勇輔（Japan Digital Design株式会社 / ソースネクスト株式会社）
調査WGリーダー:　小村誠一（エヌ・ティ・ティ・アドバンステクノロジ株式会社）
法令リスク研究WGリーダー:　田原祐介（株式会社ラック）

・企画WG
本部会の企画検討や外部機関とのPoC(Point of Contact)を担います。
賛同企業の募集など、部会全体の取り組みに関する企画運営を行っていく予定です。

図：POC機能

・調査WG
海外の事例や関連法制度に関する調査を実施します。
今年度は英米におけるサイバー犯罪法体系の調査や、海外における事例の調査を行う予定です。

・法令リスク研究WG
サイバーセキュリティ業務の法令リスク一覧を作成したり、国内における事例研究を行います。
どういった業務に、どういったリスクがあるか参照できるような資料の完成を目指します。

・有識者会議（検討中）
検討委員会のメンバーを中心に改組し、本取り組みについてJNSA内外の有識者に議論いただく会議です。

・サポート弁護士（検討中）
サイバー法令に詳しい弁護士の方々に何らかの形で本取り組みをサポートいただくような仕組みです。

サイバーセキュリティ業務における倫理行動宣言

前述した倫理行動宣言の内容を紹介します。「行動規範」と「事業遂行の基本指針」に分かれており、「行動規範」で業務や事業遂行にあたって遵守すべき規範を、「事業遂行の基本指針」でサイバーセキュリティ事業固有のリスクを管理するための指針を示しています。

JNSA会員企業で、上記に則り、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。ご興味ある会員企業の方は、事務局までお問い合わせください。

なお、宣言は、企業名、部署名、サービス名などセキュリティ事業の事業主体の単位で実施可能としています。

■ 行動規範

サイバーセキュリティ事業に携わる者は、情報社会、セキュリティ製品やサービスを利用するお客様、そして事業者自身を守るために、以下の行動規範に則って事業を遂行します。

1. 情報社会の安全を向上させ、安心の醸成に努めます。
2. 法令等の正しい理解に努め、これを遵守します。
3. 高度化する脅威に備え技術の向上に努めます。
4. 自らの製品およびサービスの安全確保に努めます。
5. 倫理観を持ち、正当な目的のために業務を遂行します。

■ 事業遂行の基本指針

1.はじめに：

サイバーセキュリティ事業には、扱い方を誤るとそれ自体が脅威となりうるマルウェアや脆弱性診断ツールなどのソフトウエアや専門技術を事業として取り扱うことから、事業固有のリスクがある。そこで、業界全体として共通的に取り組むべき事業遂行におけるリスク管理の基本指針を定める。

サイバーセキュリティ事業者（以下、事業者）がこの基本指針に則り適切な事業運営体制を構築し、かつ対外的に宣言していくことで、サイバーセキュリティ産業が社会や顧客から信頼を得つつ社会に貢献し、情報社会が健全に発展することを目指す。

2.目的と適用対象

A）目的：事業者が技術的、法的、倫理的なリスクを最小化し、事業に従事する者が安心して事業遂行でき、かつ社会や顧客から信頼されるリスク管理体制の整備を基本指針の目的とする。

B）適用対象：製品製造、販売、サービス提供、教育などのサイバーセキュリティに関わる事業を行う事業者全般を対象とする。たとえ、事業の一部であったとしてもサイバーセキュリティに関わる事業を行うものはこの適用対象とする。

3.リスク管理の考え方

A）サイバーセキュリティ事業の明確化：事業者は、自らが行うサイバーセキュリティ事業を洗い出し、それぞれの業務を具体化するとともに、その目的と分掌を明らかにする。

B）サイバーセキュリティ事業のリスク評価：事業者は洗い出したサイバーセキュリティ事業について、技術的、法的、倫理的なリスクの総合的な評価を実施する。

C）サイバーセキュリティ事業の管理策の策定：事業者は、リスク評価に基づいた管理策を策定し、これに基づいたマネジメントサイクルを実装する。

4.管理策の実施について

事業者は以下の管理策を実施することが望まれる。

A）管理体制の整備：事業者は、管理策に基づき、管理体制を構築する。また、事業内容の変化、社会的通念の変化、法的解釈の変化など時代の変化をとらえるため、定期的に管理策ならびに管理体制を見直すこと。

B）社内教育・指導：事業者は、サイバーセキュリティ事業に関わる従業員を対象に、自らが行うサイバーセキュリティ事業に関するリスクとその管理策の教育を定期的に行うこと。

C）事案（インシデント）対応：事業者は、技術的、法的、倫理的な事案が発生した場合の対応体制および対応計画を整備すること。

D）実施状況の確認：事業者は、管理策が正常に機能していることを定期的に確認し、必要に応じて改善すること。

E）連絡窓口の明確化：事業者は、リスクを早期に発見することを目的として、連絡窓口を明確化すること。

参考記事：https://www.itmedia.co.jp/news/articles/1906/28/news088.html