NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

サイバーセキュリティ事業者としての コンプライアンスリスクとその保護

2019年6月12日

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

アジェンダ

- 活動背景
- 検討委員会 委員名簿
- 検討委員会の活動内容
- 提案の全体像
- サイバーセキュリティ事業者行動規範(案)
- サイバーセキュリティ事業の基本指針(案)
- 事業コンプライアンス部会の設置
- まとめ

活動背景

2017年、セキュリティサービスを提供している組織において、不正指令電磁的記録（ウイルス）保管容疑で逮捕される事案が発生した。サービスや研究等を実施するにあたって、ウイルス保管の取り扱い、何が不正に相当するのかなどが不明瞭。業界としての基準や指針等がなく、企業活動や研究の萎縮につながっている可能性がある。

↓

事業者・研究者が安心して活動できる指針を策定し、日本のセキュリティ業界の維持、発展を期する。

活動背景 – 事案の例

投影のみ

活動背景

サイバーセキュリティ事業に関わる技術

攻撃コード、マルウェア、ペネトレーション
テスト技法　など

扱い方を誤ると脅威になりうる
＝ 留意が必要

今までは各事業者、各コミュニティ、
各個人が個別に留意してきた

サイバーセキュリティへの注目度の向上
新規参入する事業者・技術者の増加

検討委員会 委員名簿

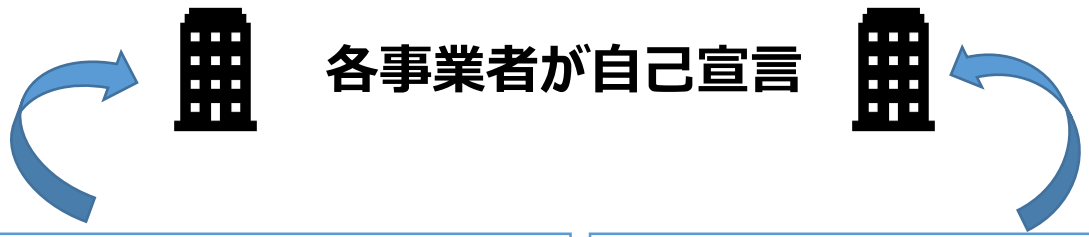
- サイバーセキュリティ事業における適正な事業遂行の在り方に関する検討委員会
  委員名簿　（敬称略）
  - 委員長
    田中 英彦　（JNSA会長／情報セキュリティ大学院大学）

  - 委員（五十音順）
    新井　悠　　（トレンドマイクロ株式会社）
    鵜飼 裕司　　（株式会社FFRI）
    佐々木 良一　（東京電機大学）
    菅谷 光啓　　（NRIセキュアテクノロジーズ株式会社）
    武智　洋　　（日本セキュリティオペレーション事業者協議会
    　　／日本電気株式会社）
    西本 逸郎　　（株式会社ラック）
    北條 孝佳　　（西村あさひ法律事務所）
    丸山 司郎　　（JNSA社会活動部会／株式会社ベネッセインフォシェル）
    湯浅 墾道　　（情報セキュリティ大学院大学）

検討委員会の活動内容

- JNSA会員企業へのアンケート（25社）
- JNSA会員企業への聞き取り調査（9社）
- 検討委員会の開催・議論（4回）
- 関係省庁、学会等への説明
- 4/1～15　JNSA内パブコメ
- 4/12　幹事会での説明
- 5/10　部会設置について理事会で承認

提案の全体像



「サイバーセキュリティ事業者行動規範」
各事業者が「社会」「顧客」「従業員と企業自身」を守るために遵守すべき規範

「サイバーセキュリティ事業遂行の基本指針」
各事業者が、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

事業コンプライアンス部会の設置

- 「行動規範」「基本指針」の普及、自己宣言企業の募集とJNSA HP掲載
- 海外の事例や関連法制度に関する調査の実施
- PoC（Point of Contact）機能による、関係省庁との円滑なコミュニケーションの実現、関連法制度の立法・改正時の提言活動（ロビー活動）
- 有識者会議の運営、サポート弁護士との連携

サイバーセキュリティ事業者行動規範(案)

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。

サイバーセキュリティ事業遂行の基本指針(案)

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. リスク管理の基本的な考え方
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
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が望ましい
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が望ましい。
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が望ましい。
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が望ましい。
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が望ましい。

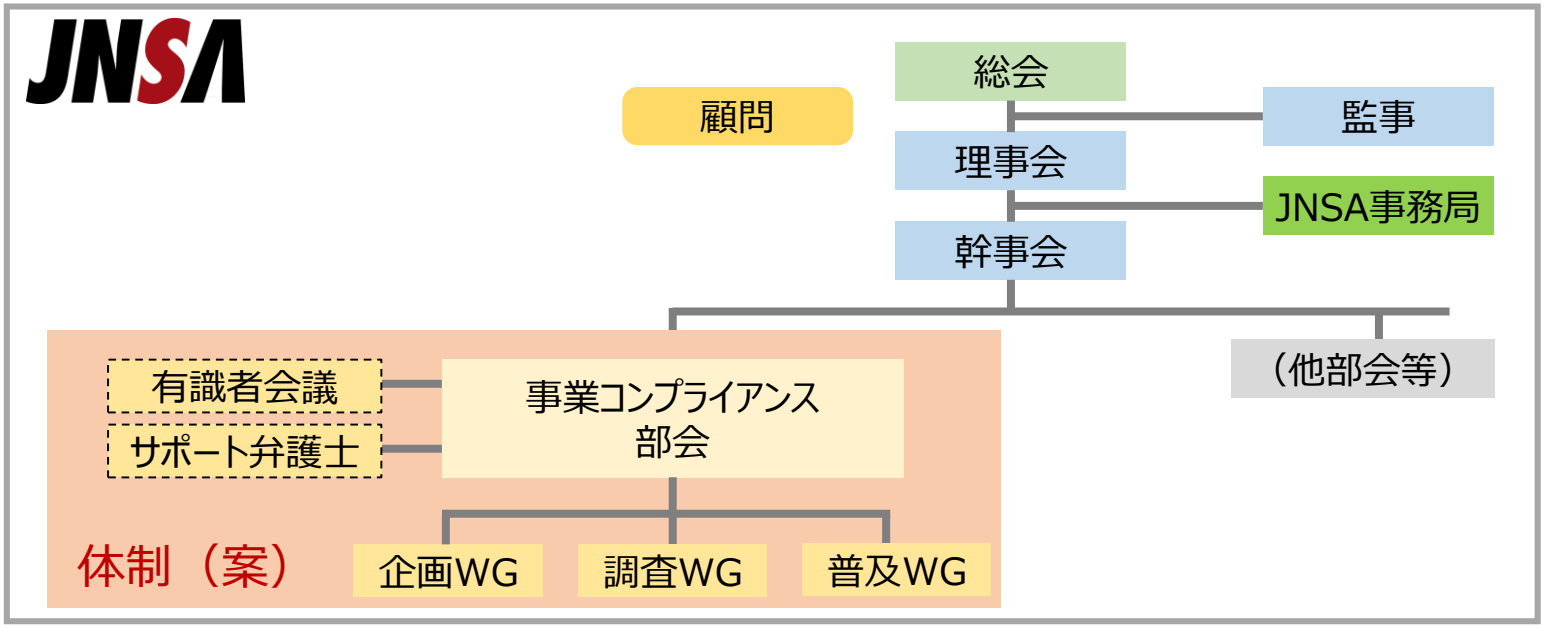
事業コンプライアンス部会の設置

■ 事業コンプライアンス部会を設置する（体制図は次ページ）

- 部会が中心となって「行動規範」「基本指針」を広めていく活動を行い、関係省庁や社会全般に対するサイバーセキュリティ事業者の信頼性を向上させる。
- 次のような機能を継続的に提供
  - 「行動規範」「基本指針」の策定や今後の改訂および普及（自己宣言の募集や一定のプロセスを経てJNSAホームページ掲載）
  - 海外の事例や関連法制度に関する調査の実施
  - PoC（Point of Contact）機能による、業界と関係省庁の円滑なコミュニケーションの実現
  - 有識者会議の運営、サポート弁護士との連携
  - 関連法制度の立法・改正時の提言活動（ロビー活動）

事業コンプライアンス部会の設置

（前ページからの続き）



有識者会議	本検討委員会を持続的運用を前提に改組
サポート弁護士	サイバー関連法に詳しい弁護士の一覧を作成し、会員企業からの依頼に迅速に対応
企画WG	本活動の企画検討や外部機関とのPoCを担う
調査WG	海外の事例や関連法制度に関する調査を実施
普及WG	セキュリティ事業者の自己宣言を募集し、普及啓発を進める