JNSA 2025年度活動報告会

サイバーセキュリティ事業における法令リスク
事業コンプライアンス部会の活動紹介

July, 2025

JNSA 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）

サイバーセキュリティ事業における法令リスク

高度な技術や情報を取り扱うサイバーセキュリティ事業では、
正当な業務として行なっていても、
法令やコンプライアンスに抵触してしまうリスクがある。

事例：セキュリティ企業従業員の逮捕(ウイルス保管容疑)

- ✓ 2017年10月、ウイルスを業務用PCに保管したとして**セキュリティ企業の従業員が逮捕**された。
- ✓ 同社は「この取得と保管は**ファイル流出監視サービス**を行うという 正当な理由に基づくもので、取得・保管したファイルを他人のコン ピュータにおいて実行の用に供する目的はありません。したがいま して、不正指令電磁的記録（ウイルス）保管では無いと考えており ます」と反論
- ✓ 結果として、**不起訴処分**となったが、日本国内において**セキュリティ企業従業員が逮捕**された事例

事業コンプライアンス部会成果物（法令リスク一覧）より抜粋

法令リスク一覧：リスク11より

想定されるリスクの例

契約対象ではない顧客への診断行為

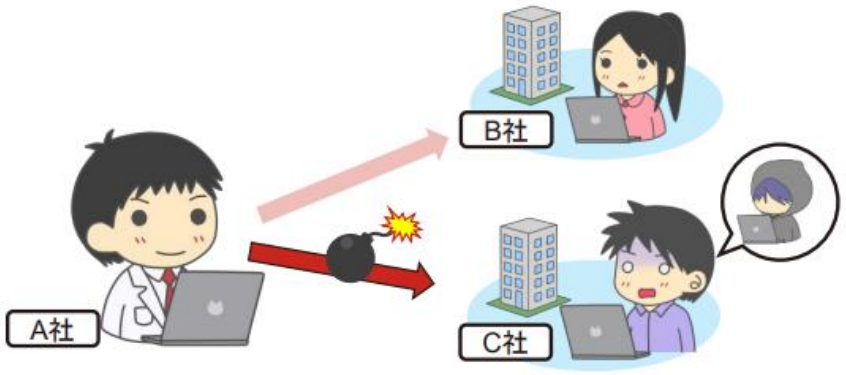
- A社は顧客B社から指示のあったIPアドレス/ドメインに対して、ペネトレーションテストを実施しようとした
- しかし、IPアドレス/ドメインの入力ミスにより無関係のC社に誤ってテストを実施してしまった
- 当初は誤りに気が付かなかったが、テストを進めるうちに気が付いて、すぐにテストを中止してC社に報告し、謝罪を行った

リスク：

✓不正アクセスの意図があると判断される

✓第三者が被害を受ける

【不正アクセス禁止法】承諾の無い脆弱性の調査や脆弱性への攻撃は、不正アクセスとみなされる可能性がある



26

事業コンプライアンス部会成果物（法令リスク一覧）より抜粋

法令リスク一覧：リスク17より

想定されるリスクの例

発見した脆弱性の不適切な公開

- A社は脆弱性診断とペネトレーションテストを提供していた
- A社がテストで発見した脆弱性や、検証で確認した脆弱性を、適切な届出先に報告する前に、A社のブログで公開してしまった
- 脆弱性の詳細は隠されていたが、公開された情報から脆弱性の内容が暴露されてしまい、修正が行われる前に悪用されてしまった

リスク：

✓不正アクセスが可能な情報を提供したと判断される
✓第三者が被害を受ける

【不正アクセス禁止法における不正アクセス罪の幇助犯】【威力業務妨害罪の幇助犯】
【電子計算機損壊等業務妨害罪の幇助犯】
不正アクセス行為を助長する意図がなくても第三者が不正アクセスに用いることを知って脆弱性情報を提供したとみなされる可能性があります。また、当該脆弱性情報を悪用されることでシステムが停止したり、データの改ざん等が発生したりした場合には、意図的に第三者の業務を妨害しようとしたとみなされる可能性があります。

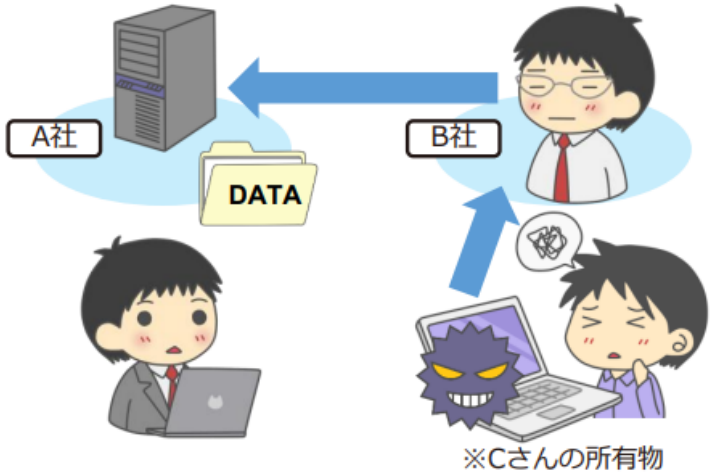
32

事業コンプライアンス部会成果物（法令リスク一覧）より抜粋

法令リスク一覧：リスク38より

想定されるリスクの例
所有者のプライバシー侵害、民事訴訟

- A社はフォレンジックサービスを提供していた。
- 端末やディスク等の証拠保全や調査は、契約したB社と契約を行い、B社の承認の上で実施していた。
- ところが、**実際にはB社の従業員であるCの所有物**であり、B社はCの所有物であることを知りながら、**Cの承諾を得ずにA社に証拠保全の許可**を行っていた。



※Cさんの所有物

リスク：
✓契約の問題により作業が阻害される可能性がある。

国内の犯罪には該当しませんが、民事訴訟となる可能性があります。

59

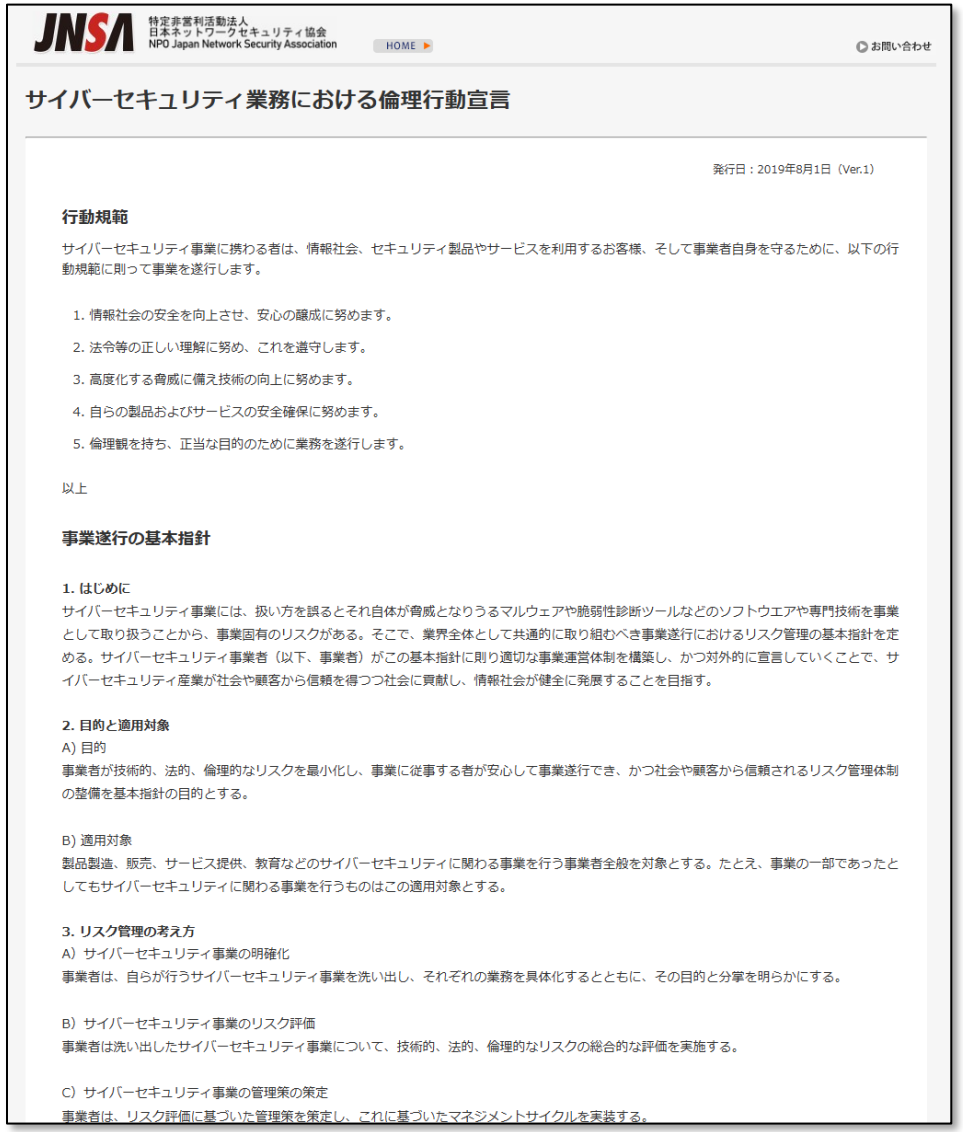
事業コンプライアンス部会

事業コンプライアンス部会では、**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、適正なサイバーセキュリティ事業遂行の在り方を検討**しています。

- **「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・更新
- 法令リスクに関連する、**法執行機関との連絡**窓口
- 法令リスク事例を調査し、**「法令リスク一覧」**を会員企業に公開

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/



JNSA 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 NPO Japan Network Security Association　HOME　お問い合わせ

サイバーセキュリティ業務における倫理行動宣言

発行日：2019年8月1日（Ver.1）

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。

以上

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

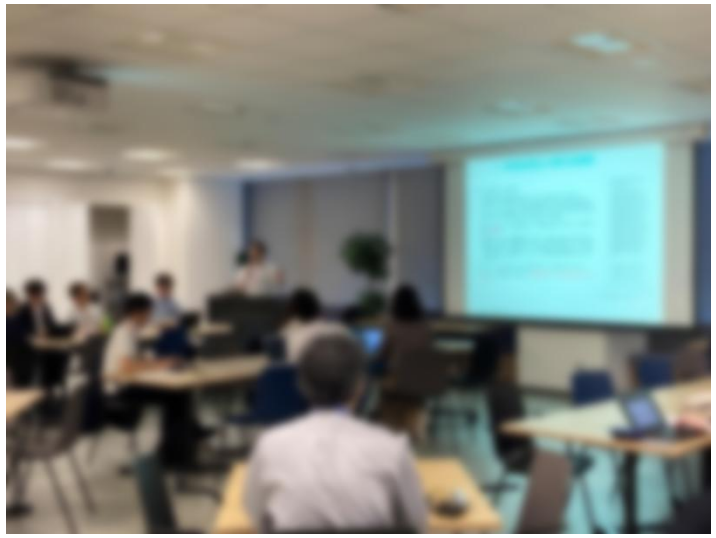
事業者は、リスク評価に基づいた管理策を策定し、これに基づいたマネジメントサイクルを実装する。

各社の事業が正当に実施されており、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。**

- ✓ 自社のセキュリティ事業が違法性を問われないために
- ✓ 継続的な事業として行っているとして事業の正当性を宣言
- ✓ 安心してセキュリティ事業を提供していくために

倫理行動宣言に御賛同いただいた企業名や事業部名をJNSAのWebサイトに掲載します。JNSA事務局までお問い合わせください。

法令リスクや事業コンプライアンスをテーマにした勉強会を開催



2025年6月開催／会員限定勉強会
【ランサムウェアとセキュリティサービスに潜む“法的リスク”】

- ランサムウェアの身代金支払いに関する法的論点
- SOC/MSSサービスの情報漏洩インシデントから考える法令リスク

勉強会参加者の声

- 顧客からの相談事項に関してヒントになった
- 経営層の責任が具体的に良く理解できた
- ランサムウェアの支払いに関しての考え方が整理して理解できた

Join our team!

事業コンプライアンス部会への参加をご検討ください！

sec@jnsa.org