日本のサイバーセキュリティを「連携」「学び」「創造」

JNSA活動報告会 事業コンプライアンス部会

サイバーセキュリティ事業における法令リスクとは

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

- サイバーセキュリティサービスの提供者が、社会・お客様・提供者自身を守るための、適正なセキュリティサービス事業遂行の在り方について検討している
- 「サイバーセキュリティ業務における倫理行動宣言」の運用
- 法執行機関との連絡窓口
- 法令リスクや国内外の事例研究

JNSA サイバーセキュリティ業務における倫理行動宣言
Declaration of Ethical Code for Cybersecurity Operations

https://www.jnsa.org/cybersecurity_ethics/

セキュリティ技術は扱いに注意が必要

サイバーセキュリティ事業に関わる技術
脆弱性情報、ペネトレーションテスト技法、マルウェアコード、等

扱い方を誤ると第三者の脅威になりうる
(脆弱性情報が漏えいして攻撃にあう等)

扱い方を誤ると
法令違反になる
＝ **法令リスク**

法令リスクの例

リサーチャの講演やBlog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B氏は、公開の場での研究成果の発表を行っており、カンファレンスやブログなどで多くの成果を公開していた。
- **公開の場やブログ記事でマルウェアの利用を促すような発言や記述があり、一部ではあるが動作可能なマルウェアのコードを公開していた。**

【リスク】

不正指令電磁的記録提供罪（いわゆるウイルス作成・供用罪）に問われる恐れがある。

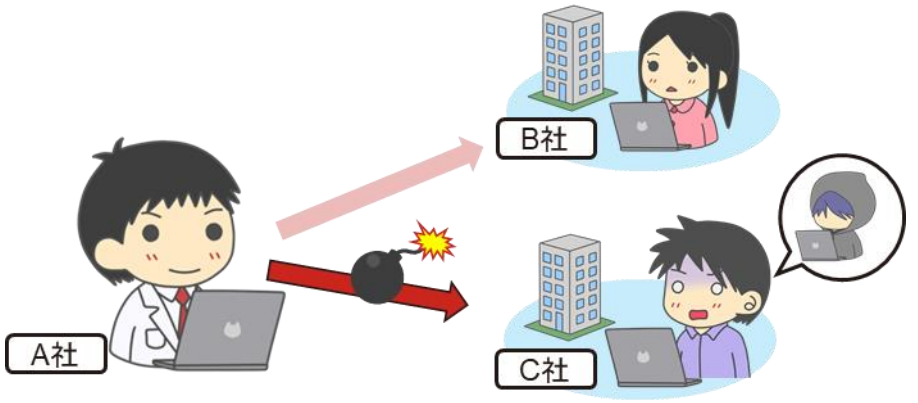
【不正指令電磁的記録に関する罪（不正指令電磁的記録作成等）】

(今回のケースでは) 正当な理由なく、他人のパソコンで実行させる目的で、マルウェアを提供したと司法判断された場合、罪に問われる。

法令リスクの例
契約対象ではない顧客へのセキュリティ診断行為

- 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】
- 第三者に障害等の問題を生じさせてしまう可能性
- 不正アクセス禁止法違反に問われる可能性

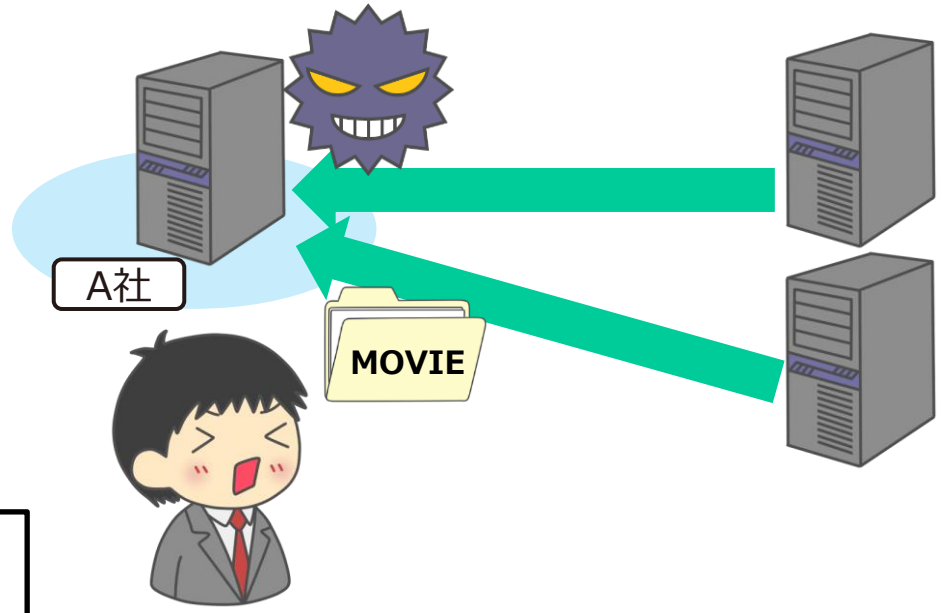


【不正アクセス行為の禁止等に関する法律】
(今回のケースでは) セキュリティ診断によってC社システムのアクセス制御を突破して侵入に成功したとみなされた場合、罪に問われる。（被害の有無は無関係）

法令リスクの例

クローリングによる違法ファイルのダウンロードと保持

- A社はインテリジェンスサービス提供の情報収集のために、様々なWebサイトへのアクセスやクローリングを実施していた。
- **違法な可能性のあるファイルをダウンロード**してしまうこともあったが、そのまま自社内のシステムに保存していた。



【リスク】

児童ポルノ禁止法や不正競争防止法に問われる可能性

【児童ポルノ禁止法】【不正競争防止法】

ダウンロードしたファイルが児童ポルノに該当したり、他社の営業秘密に該当するものだった場合、これらの法令に抵触するとみなされ罪に問われる恐れがあります。

「法令リスク一覧」を会員限定で公開中

【事業コンプライアンス部会｜会員専用「法令リスク一覧」】2023年12月19日

下記URLから法令スク一覧をダウンロードできます。会員企業内限定でご利用ください。

事業コンプライアンス部会　法令リスク一覧＞＞　(PDF1.3MB)　※会員限定

必ず「公開範囲・引用について」をお読みの上、ダウンロード下さい。

2023年12月21日に開催した説明会の資料を公開しています。

2023年12月21日説明会資料　(PDF1.1MB)　※会員限定

■本書の公開背景について

・サイバーセキュリティ事業は、正当な業務を行なっていても抵触する可能性のある法令上のリスクが存在する。それを業務ごとに例示したものです。
・セキュリティ事業や研究を行う事業者が、法令違反を行わないよう対策の参考にしていただくことを意図しています。
・各事業者および所属する技術者が安心して事業を提供できるように支援したいと考えています。

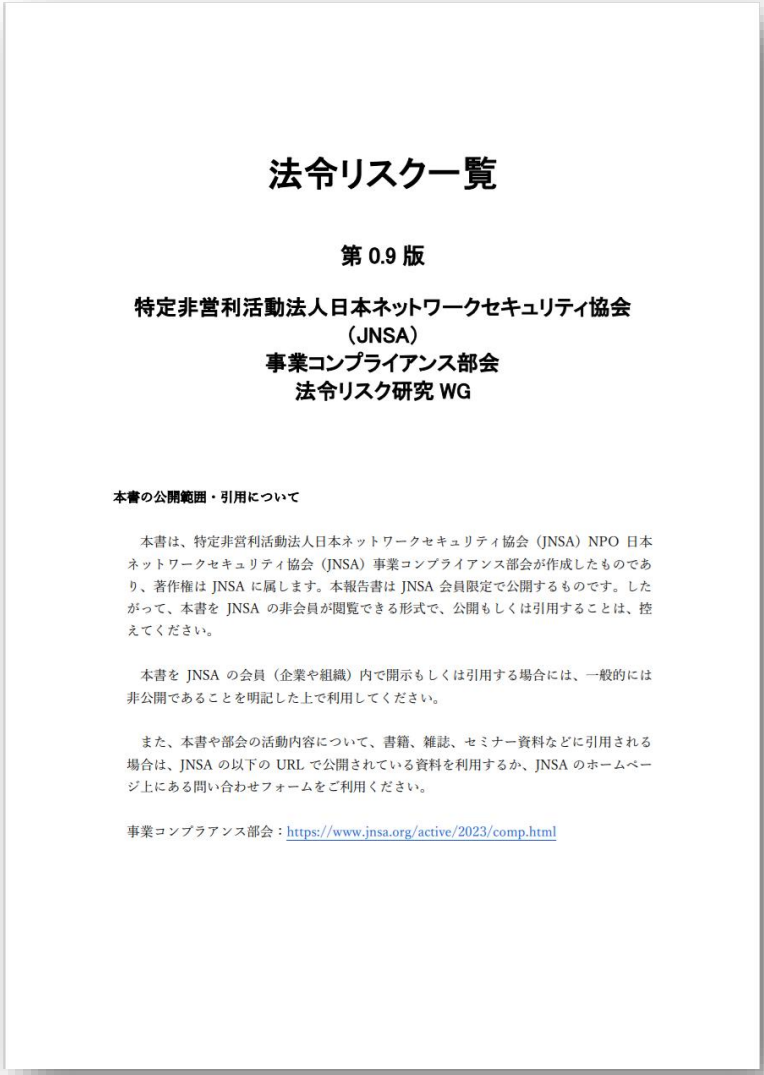
■注意点

・全ての法令リスクを網羅するものではなく、不足は各事業者にて補うことを想定しています。
・対策については各事業者の業務内容にあわせて対策を行ってください。

■公開範囲・引用について

本書は、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（JNSA）NPO日本ネットワークセキュリティ協会（JNSA）事業コンプライアンス部会が作成したものであり、著作権はJNSAに属します。本報告書はJNSA会員限定で公開するものです。したがって、**本書をJNSAの非会員が閲覧できる形式で、公開もしくは引用することは、控えてください。**

本書をJNSAの会員（企業や組織）内で開示もしくは引用する場合には、JNSAのホームページ上にある問い合わせフォーム「報告書の転載・引用連絡」から報告の上、**一般的には非公開であることを明記した上で**利用してください。



法令リスク一覧

第 0.9 版

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
（JNSA）
事業コンプライアンス部会
法令リスク研究 WG

本書の公開範囲・引用について

本書は、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（JNSA）NPO 日本ネットワークセキュリティ協会（JNSA）事業コンプライアンス部会が作成したものであり、著作権は JNSA に属します。本報告書は JNSA 会員限定で公開するものです。したがって、本書を JNSA の非会員が閲覧できる形式で、公開もしくは引用することは、控えてください。

本書を JNSA の会員（企業や組織）内で開示もしくは引用する場合には、一般的には非公開であることを明記した上で利用してください。

また、本書や部会の活動内容について、書籍、雑誌、セミナー資料などに引用される場合は、JNSA の以下の URL で公開されている資料を利用するか、JNSA のホームページ上にある問い合わせフォームをご利用ください。

事業コンプラアンス部会：https://www.jnsa.org/active/2023/comp.html

このような活動にご興味を持たれた方は
ぜひ部会への参加をご検討ください！
（参加方法は事務局までお問い合わせを）
sec@jnsa.org