情報セキュリティベンダに対する刑事法の萎縮的効果と法律

株式会社ITリサーチ・アート
弁護士 高橋郁夫

調査の背景

- 事件(2017年10月末)
  - 情報セキュリティ提供会社
    - 逮捕(P2Pネットワークの監視に従事していた従業員)
    - 逮捕された従業員-不起訴処分
    - 自らの法令順守の体制の構築・遵守などで不安
    - 法執行機関に対して
      - 法執行が、実際の技術の運用-十分な知識を有さないまま
      - 法の解釈・適用が、明確性を欠くのではないか
- JNSA
  - 2019年8月-「サイバーセキュリティ業務における倫理行動宣言」を公表
  - サイバーセキュリティ事業における適正な事業遂行のあり方に関する検討委員会
    - 企業に対するヒアリング(2018年)
- NICT法改正案
  - 一定の条件のもと不正アクセス禁止法に関して適用の除外となることを明確にした
- 日本学術振興会（JSPS）
  - サイバーセキュリティの研究倫理を考えるWG
    - サイバーセキュリティ研究における倫理的な研究プロセスの普及啓発

法令等遵守の観点からのリスクの分析枠組

- （1） 実体法的なリスク
  - (ア)　　刑事法的なリスク
    - 不正アクセス禁止法に関する罪
    - コンピュータウイルスに関する罪
    - 著作権に関する罪 など
  - (イ)　　民事的なリスク
    - 分析行為-ソフトウエアのライセンス契約違反
    - 脆弱性の公表行為-名誉・信用毀損？
  - (ウ)　　行政的なリスク
    - 個人情報保護等の規定に違反してしまうのではないか？
    - ダークウエブにおいて、犯罪行為によって取得された情報を、対価を支払って取得する行為-反社会的勢力に対する経済的利益の供与の禁止違反？
- （2） 手続法的なリスク
  - フォレンジックスのサービス
    - サービスの法的な効果が否定
    - 証拠力の評価

情報セキュリティベンダの活動と法的リスク

- 取り上げる課題
  - 情報セキュリティに関するツールの取扱いに関する問題
  - コンピュータウイルスの分析活動に関する問題
    - ケーススタディで、事案を作成して国際調査

- その余の課題
  - 脆弱性公開に関する法的問題
    - わが国においては脆弱性早期警戒パートナーシップで詳しく議論されている
    - 法律問題については高橋の分析になる「情報システム等の脆弱性情報の取扱いにおける法律面の調査報告書 改訂版」が公表されている(2019年3月)。
  - 通信の秘密/秘密の保護/ネット中立性とISPのセキュリティ活動の関係
    - 令和2年度調査で総務省からの委託調査を実施中です。

国際調査の枠組

- ドイツ
  - 西貝吉晃准教授（千葉大学法科大学院 ）
- アメリカ
  - 有本真由弁護士（アレシア国際法律事務所-現在）
- イタリア
  - Stefano Mele弁護士（Carnelutti法律事務所）
- イギリス、オーストラリア
  - 高橋郁夫
- 有識者に対するインタビュー
  - アメリカ　Jesse Woo（京都大学　フルブライト）
  - イギリス　Audrey Guinchard（エセックス大学）
  - ドイツ　　Matthias　Lachenmann（弁護士）
  - オーストラリア　Dr. Adrian McCullagh（クイーンズランド大学）

質問1

- 事例1　サイバーセキュリティサービス提供者の従業員Aは、セキュリティ調査のために脆弱性を探知するためのツールを開発し、そのソースコードをGithubで公開していた。ある日、そのツールを利用して、攻撃者側が、実際の攻撃を利用していたことが明らかになった。
- 　Aは、そのソースコードの公開や実際の利用状況について、具体的なモニタリング等を怠っていた。
- (論点)
  - 両用ツールの法的位置づけ
  - 萎縮的効果を回避するための枠組

質問2

- 事例２　サイバーセキュリティサービス提供者の従業員Bは、ファイル共有ソフト・プラットフォームにおいて、拡散するマルウエアの分析と、そのネットワークにおいて流出した情報のモニタリングを担当していた。
- このマルウエアは、上記プラットフォーム利用者のコンピュータの脆弱性を悪用して、デスクトップフォルダーのなかのドキュメントを、その共有プラットフォームに流出するものであった。
- Bは、モニタリングしていた場合に、そのマルウエアが、さらにネットワークで第三者に対して感染してしまう性質をもっているかどうかということについて、一顧だにしなかった。
- (論点)
- コンピュータウイルスの保管をどう考えるのか
- 主観的な意図をどう考えるのか

質問3-5

- 質問3
  - あなたの国において、情報セキュリティベンダもしくは、情報セキュリティの調査員（以下、セキュリティサービス提供者という）が、その業務の遂行に関し、違法行為をしているとして刑事法令が適用された事例（逮捕事例を含む）はありますか？
- 質問4
  - あなたの国において、セキュリティサービス提供者業務の遂行に関し、法の執行が萎縮的効果を有しないようになされている政府や法執行側の努力がありますか？
- 質問5
  - あなたの国において、セキュリティサービス提供者業務の遂行に関し、法の執行が萎縮的効果を有しないように業界側（企業なり、業界団体）が努力をしているということがありますか？　また、オンライン人権団体などの努力があれば、お教えください。

両用ツールと萎縮効果回避の努力(1)

国等	規定	特徴	事例	回避努力
サイバー犯罪条約	6条(装置の濫用)	激しい議論		6条2項で「正当な行為に対する適用禁止」
日本			Winny著作権侵害幇助(最高裁 決定)	
アメリカ	アクセスの構成要件該当性なし(その余の主観要素もない)		US v. Jitesh Thakkar事件/Rubin v. New Jersey事件	
イギリス	コンピュータ不正使用法3A条	提供/提供の申込は、蓋然性を含み・広範すぎる		起訴のガイドラインが公表されている(起訴は、考えにくい)

両用ツールと萎縮効果回避の努力(2)

国等	規定	特徴	事例	回避努力
ドイツ	刑法202条c		違憲審査訴訟がなされた	限定解釈
オーストラリア	刑法478.4条	「意図をもって」の構成要件の該当性なし		一般的な主観的態様についてガイドラインあり
イタリア	刑法615条の5(情報システムを損壊／妨害する機器、デバイス、コンピュータプログラムの拡散)	目的が求められているので、犯罪の成立はない		

注目例

- アメリカ
  - US v. Jitesh Thakkar事件(2019)
    - Thakkarは、ナビンダー・シン・サラオ(「なりすましアルゴリズム」-フラッシュ・クラッシュ（一時的な大幅な価格下落）-違法に儲けた)の求めに応じて、大量の株式の取引注文を出した後、当該取引が実際に実行されないようにするためのコンピュータプログラムを作成し、それをサラオに売却
    - 評決不能陪審（hung jury）-司法省は起訴を取り下げる
- イギリス
  - コンピュータ不正使用法のガイドライン（2008年）
    - 犯罪目的を、主として、故意に、唯一のために、開発されてきているのか
    - コマーシャルベースで、広く利用可能なものか、もしくは、適法な販売チャンネルで売却されているのか。
    - 道具は、適法な目的のために広く利用されるか。
    - 実質的にインストールベースであるのか。
    - もともとの意図された目的と比較して、その道具が、罪を犯すのに使われるにいたった状況は何か。

注目例2

- ドイツ
  - 憲法上の異議申立(セキュリティ研究者等による)-抽象的違憲審査
  - 憲法裁判所
    - 同条に対して一定の限定解釈-訴追されるリスクがない、として申し立てを却下
    - 同裁判所は、同条を、刑法202条a、b等の犯罪行為を遂行するために使用するという意図・目的をもって開発等され、それが客観的に示されているプログラムのみが捕捉される、と解釈
    - セキュリティの専門家は、これを評価

コンピュータウイルス所持-流出被害の刑事責任

国等	規定	特徴	事例	回避努力
日本	不正指令電磁的記録に関する罪	コンピュータ・ウイルスの作成、提供、供用、取得、保管行為が罰せられる		
アメリカ	連邦法1029条	「情を知って、詐欺の意図で」所持する場合		
イギリス	コンピュータ不正使用法の３（1）条	無謀にも（reckless）結果を発生させた場合にも、犯罪が成立-可能性の存在	なし	
ドイツ	マルウェアの保管自体は刑法202条c第1項2号の行為類型には入っていない			
オーストラリア	刑法478．3条	犯罪行為に対する意図が求められており		
イタリア	635条2項以下	故意が必要である		

回答3 業務に対する刑罰法規の適用

国別	事案	備考
アメリカ	US v. Sklyarov事件（2001）、MBTA v. Anderson事件（2008）、David Levin事件（2016）、Justin Shafer事件（2016）、Iowa州誤認逮捕事件（2019）	その他 セキュリティ活動についての事件もある
イギリス	Cuthbert事件 (ツナミハッカー事件, 2005)、Mangham事件(2012)	
ドイツ	特にない	
オーストラリア	Ben Grubb　case　（2011）	AusCERT会議でのハッキングデモのレポートを書いた記者が逮捕された事件(その後、釈放)
イタリア	特にない	

回答4 政府や法執行機関側の努力

国別		具体例
アメリカ	ガイドライン	「刑事捜査におけるコンピュータの捜索・押収と電子的証拠の取得」（2009） 「コンピュータ犯罪の起訴マニュアル」(2010) 知的財産犯罪の起訴マニュアル」（2013） 「コンピュータ犯罪事項の立件および起訴ポリシー」（2014、2016に改訂）
	システム	コンピュータ犯罪と知的財産部（CCIPS）/サイバーセキュリティユニット
イギリス		検察官の行為規範（General Code for Crown Prosecutors）、サイバー犯罪（Cybercrime - prosecution guidance）、コンピュータ不正使用法ガイダンス
ドイツ		憲法訴訟(前述)
オーストラリア		ハイテク犯罪オペレーションセンター（High Tech Crime Operations Centre (HTCOC)）下院通信常任委員会報告(2010)
イタリア		特にない

回答5情報セキュリティベンダ等の活動

国別		具体例
アメリカ	業界団体	SANS Institute
	オンライン人権団体	EFF、CDT(Center for Democracy and Technology)、ACLU(American Civil Liberties Union)
イギリス	セキュリティベンダ	NCC Group
	グループ	CLRNN(The Criminal Law Reform Now Network）、Open Rights Group
ドイツ		The Chaos Computer Club e. V. (CCC)、netzpolitik.org
オーストラリア		Electronic Frontier Australia
イタリア		特にない

推奨事項1 両用ツールについて

- 法執行機関に対して
  - 高度の蓋然性とその認識・認容が必要であるという枠組が確認されるべき
  - ガイドラインが明確にされている国もあることを認識すべき

- ベンダに対して
  - 開発協力者や利用者について、個別にフォロー
  - 悪用の情報をモニタリングし、常にその悪用を困難にするように尽力すること
  - 体制を整えて遵守すること。

推奨事項2 政府や法執行機関の努力

- (調査の結果)逮捕案件は、国際的には2010年以降についてみれば、非常に少ない
- 趣旨を明らかにしたメモが公表されて、法執行の目安とされることが望ましいものといえる
  - 総合的に考慮して判断される
    - ソフトウエアに対して、利用者に対して利用条件が明示されているか
    - 提供者が、利用状況をモニタリングしているか
    - 利用者に対して違法な利用をなさないように確認しているか
    - 可能であれば、利用者に提供される方法について留意をしているか
- (報道)
  - 最高検、サイバー専門班を新設へ…電子データ復元技術も共有(2012/03/10)
    - 東京地検特捜部での捜査経験が豊富な検事や、サイバー事件に精通した検事を集めたチームを新設し、全国の高検・地検にも担当検事を配置。各地の検察庁が担う捜査や公判を支援するほか、特捜事件で活用している「デジタル・フォレンジック（DF）」などの技術の共有も進める

推奨事項3 刑罰法規についての比較情報の収集について

- 我が国においても十分な情報収集がなされるべきである
- 我が国の刑罰法規を、現代社会において、適切なものにするという努力が継続的になされるべきである。