秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文

【趣旨・目的】

サイバー攻撃の全容解明やサイバー攻撃による被害拡大の防止の観点から、専門組織を通じたサイバー攻撃に関する情報共有を促進することは重要である。

以下に示すモデル条文は、専門組織を通じた情報共有を促進し、被害組織の被害に対する迅速な調査や被害拡大防止等を目的として、あらかじめ被害組織（ユーザー組織。甲）と専門組織（乙）間で合意しておく攻撃技術情報等の取扱いや円滑な情報共有のための関連事項（保有情報に対する安全管理措置や免責事項など）を示すものである。

【モデル条文】

１．乙は、本サービスの遂行過程において、乙の知見により得られたサイバー攻撃に関する通信先、マルウェア、脆弱性その他の情報（以下この条において「攻撃技術情報」という。）について、甲の被害に対する迅速な調査、被害拡大の防止及び甲乙以外の組織に対するサイバー攻撃の未然防止を目的としてこれを保有又は利用し、また、甲を識別及び特定できないように加工した攻撃技術情報（以下この条において「攻撃技術情報」及び「甲を識別及び特定できないように加工した攻撃技術情報」を合わせて「攻撃技術情報等」という。）を作成、保有、利用又はサイバーセキュリティに関する専門組織に対して開示することができる。 ２．乙は、保有する攻撃技術情報等について、必要かつ適切な安全管理措置を講じなければならず、前項の目的を達成するために必要な範囲を超えて攻撃技術情報等を開示してはならない。 ３．乙は、第１項及び第２項の攻撃技術情報等の利用又は開示に関連して、甲に生じた損害については一切の法的責任を負わないこととする。ただし、乙に故意又は重過失がある場合は、この限りでない。

【解説】

・対象となる情報

「サイバー攻撃に関する」情報が対象であり、通信先、マルウェア、脆弱性に関する情報を含み、それ以外のものも含むとしている。具体的には、IP アドレス、ドメイン(FQDN)、URL、ポート番号、マルウェアの種類（検知名）、脆弱性の呼称、CVE 番号、ソフトウェア名、影響を受けるバージョン、攻撃者が用いた特徴的な正規ツールや設定情報等が含まれる。

・目的

甲の被害に対する迅速な調査、甲の被害拡大を防止すること、他の組織における将来の

サイバー攻撃の未然防止としている。例として他の組織においても同様の被害が発生している場合に、当該組織における有用な情報を取得すべく、甲の情報を提供し、甲の被害に対する迅速な調査を行う目的など。

・攻撃技術情報に対する行為

乙は、上記目的のために攻撃技術情報を保持、利用することができるが、利用範囲は乙の裁量に委ねられている。例えば、乙が提供するサービスにおいて、他社に提供するサービスにも利用できることになる。他方、利用に開示が含まれるかは明確ではないが、開示を明確に除外する場合には、「保持又は利用（開示は除く。）」と記載することが考えられる。

・非特定化加工攻撃技術情報に対する行為

乙は、上記目的のために甲を識別及び特定できないように加工した攻撃技術情報（以下、「非特定化加工攻撃技術情報」とする）を作成、保持、利用することができる。

非特定化加工攻撃技術情報に関するユースケース等については、「攻撃技術情報の取扱い・活用手引き」に例示する。

開示の対象者については、「サイバーセキュリティに関する専門組織」としている。専門組織を明確にする場合、例えば、IPA や ISAC など具体的な組織名を列挙することが考えられる。

・安全管理措置

乙は、攻撃技術情報に対しては保持や利用する場合、非特定化加工攻撃技術情報に対しては保持、利用又は開示する場合に、必要かつ適切な安全管理措置を講じる義務を負うようにしている。漏えい等させないための技術的安全管理措置に加え、開示の際には適切な開示範囲を限定する措置などが求められる。

・免責

乙は、攻撃技術情報等の利用又は開示に関して裁量権があるが、これによって生じた損害については、故意又は重過失を除いては一切法的責任を負わないこととしている。免責の対象は当該情報の利用又は開示に関してであり、作成又は保持に関しては免責されないこととしている。

その理由として、サイバー攻撃が高度化する中、単独組織による攻撃の全容解明は困難であり、攻撃の全容の把握や被害の拡大を防止する等の観点からサイバー攻撃に関する情報共有は極めて重要であるところ、乙の故意や重過失によらない事由により、作成した非特定化加工攻撃技術情報を開示したことにより被害組織が推測されてしまった場合であっても免責としている。