AMT/NEWSLETTER
Crisis Management

2025 年 9 月

民間企業による能動的サイバー防御の主要論点

弁護士 三宅 英貴 / 弁護士 中原 隆雅 / 弁護士 石川 雅人

Contents

Ⅰ．はじめに

2025 年 5 月、「重要電子計算機に対する不正な行為による被害の防止に関する法律」（いわゆるサイバー対処能力強化法）およびその施行に伴う関係法律の整備を目的とする法律（整備法）が成立しました[1]。これらの法律は、公的機関による能動的サイバー防御（Active Cyber Defense）の実施に向けた法的枠組みを整備するものであり、わが国のサイバー・セキュリティ政策における、転換点の一つと位置づけられます。また、同年 7 月には、これらの法律の成立等を踏まえ、内閣サイバーセキュリティセンター（NISC）が改組され、内閣サイバー官を長とする「国家サイバー統括室」（NCO：National Cybersecurity Office）が設置されるなど、2027 年中の施行を見据え、能動的サイバー防御の導入に向けた政府の体制整備も進んでいます[2]。

このような政策的動向を背景に、民間企業においても、従来の受動的な防御策だけでなく、攻撃主体の特定・追跡・妨害を含む能動的対処への関心が急速に高まりつつあります。とりわけ、企業が自社サーバーに仕掛けたプログラム（以下「ICE プログラム」）を通じて、アクセスしてきた攻撃者の端末情報・IP アドレス・位置情報等を取得する技術は、攻撃者特定や二次被害抑止の手段として注目を集めています。

もっとも、こうした手法は、現行の刑法 168 条の 2（不正指令電磁的記録作成等罪）および不正アクセス行為の禁止等に関する法律（以下「不正アクセス禁止法」）との関係で、違法性を問われるリスクがあり、導入にあたっては慎重な法的評価が必要です。

---

[1] https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html

[2] https://www.nisc.go.jp/about/overview/index.html#summary

本稿では、能動的サイバー防御の技術的枠組みとその法的評価の概要を整理し、特に上記 2 法との関係を中心に、企業が検討すべき主要論点を明らかにします。

II. 能動的サイバー防御の概要

能動的サイバー防御とは、サイバー攻撃の兆候を早期に探知し、攻撃主体の特定（Attribution）や妨害措置（Disruption）を通じて、自社システムの安全を能動的に確保するための一連の手法を指します。代表的な技術としては、ハニーポットの設置、逆探知型プログラムの活用、攻撃者が用いる C2（Command and Control）サーバーへの働きかけなどが挙げられます。

本稿で取り上げる「ICE プログラム」（Intrusion Countermeasure Electronics）とは、企業のサーバー上に設置され、外見上は無害なファイル（たとえば PDF）に偽装されたプログラムです。攻撃者がこのファイルを開封・実行した場合に作動し、攻撃者端末から IP アドレス、端末識別情報、OS 情報、位置情報、操作ログ、ディレクトリ構造などを取得し、企業側の管理サーバーに自動送信する仕組みとなっています。いわば「逆探知機能」を備えた情報収集型の能動的サイバー防御技術と位置付けられます。

このような ICE プログラムの活用により、攻撃の出所や挙動を把握することが可能となり、初動対応の高度化が期待されます。しかしその一方で、アクセス者が真に攻撃者であるかを事前に判別する機能は通常備わっておらず、誤検知により無関係な第三者の端末情報を収集するおそれがあります。また、取得される情報の範囲によっては、プライバシーや個人情報保護の観点から問題が生じる可能性もあり、刑法や情報関連法との関係で慎重な検討が必要です。

さらに、ICE プログラムで取得した情報を基に、企業が C2 サーバーの所在を特定し、当該サーバーに対して通信遮断やログ取得、マルウェアの無力化などの能動的措置を講じるケースも想定されます。このような連携的活用においては、ICE プログラムが主として情報収集機能を担い、その後の C2 サーバーに対する措置がより積極的な防御手段と位置付けられます。ただし、C2 サーバーへのアクセスや制御は、刑法 168 条の 2 に加えて不正アクセス禁止法との関係で高い法的リスクを伴うことに留意が必要です。

なお、2025 年 5 月に成立したサイバー対処能力強化法および同整備法では、公的機関である警察・自衛隊が、独立機関の承認を得た上で、限定的に攻撃元サーバー（C2 サーバーを含む）へのアクセスやマルウェアの除去等を実施することが認められています。これに対し、民間企業による ICE プログラムなどの情報収集型の能動的サイバー防御技術の活用や C2 サーバーへのより積極的な対処を合法化・容認する内容は含まれておらず、現時点では民間企業による能動的サイバー防御には引き続き慎重な対応が求められる状況にあります。

III. 刑法 168 条の 2（不正指令電磁的記録作成等罪）との関係

1. 構成要件と判断枠組み

刑法 168 条の 2（不正指令電磁的記録作成等罪）は、「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」の作成・提供・供用等を処罰するものです。本罪につき、2022 年の最高裁判決[3]（いわゆるコインハイブ事件[4]）は、「意図に反する」（反意図性）と「不正な」（不正性）の条文上の 2 つの構成要件について、以下の判断枠組みを示しました。

- 反意図性: 一般の使用者が認識すべき動作と実際の動作が異なること
- 不正性: そのプログラムの動作が社会的に許容されないものであること

ICE プログラムがこれらの構成要件に該当するか否かについて、以下に検討します。

---

[3] 最判令和 4 年（2022 年）1 月 20 日刑集第 76 巻 1 号 1 頁

[4] ウェブサイト運営者が、「Coinhive」（ウェブサイトの閲覧者の同意を得ることなくその電子計算機を使用して暗号資産のマイニングを行わせるウェブサービス）によるマイニングを行わせるためのプログラムコードをサーバコンピュータに保管して不正指令電磁的記録保管罪に問われた事案。

2. 反意図性の検討

ICE プログラムは、多くの場合、外見上は業務ファイルや無害なコンテンツ（例：PDF）に偽装されており、アクセスした利用者（攻撃者を含む）がその機能や挙動を正確に認識することは困難です。コインハイブ事件における最高裁判決では、「反意図性」の判断に際して、プログラムの動作の内容に加え、プログラムに付された名称、動作に関する説明内容、想定される利用方法などを総合的に考慮すべきとされています。

ICE プログラムは基本的に外部の攻撃者を対象とするものであるため、事前にその存在や機能について説明し、同意を得ることは現実的に困難です。このような設計上の性質に照らすと、利用者の意図に反して作動するプログラムと評価されやすく、反意図性が認められる可能性が高いといえます。仮にアクセス時の警告表示を実装していたとしても、これをもって直ちに反意図性が否定されるとは限りません。最高裁は、「反意図性」の判断基準を特定の利用者の主観的意図ではなく、一般の使用者が予期し得る動作と実際の挙動との乖離に置いており、社会通念上その挙動が通常予期されるものであると評価されない限り、反意図性はなお肯定されると解されます。

なお、社内不正対策の目的で ICE プログラムを設置する場合であっても、利用者への十分な説明や警告表示、社内規程等での明示がなければ、従業員にとってもその挙動は意図しないものであると評価される可能性があり、反意図性の要件を満たすおそれがあります。

3. 不正性の検討

不正指令電磁的記録作成等罪における「不正性」とは、当該プログラムの機能や挙動が、社会的に見て相当といえる範囲を逸脱していないかどうかという観点から判断されます[5]。ICE プログラムの不正性については、次の 3 点を中心に検討する必要があります。

第一に、取得対象となる情報の範囲です。ICE プログラムが取得し得る情報には、IP アドレス、端末識別情報、OS 情報、位置情報、操作ログ、ディレクトリ構造などが含まれる可能性があります。中でも位置情報や操作ログといったプライバシー性の高い情報を、利用者の同意なく自動的に取得する設計となっている場合、当該取得が社会的に許容される範囲を超えると評価され、不正性が肯定されるおそれが高まります。とりわけ、防御目的との均衡を欠いた過剰な情報収集は問題視される可能性があります。

第二に、プログラムが作動する対象の限定性が問題となります。ICE プログラムは、アクセスしてきた端末が攻撃者か否かを問わずに作動する設計であることが多く、善意の第三者や偶然アクセスした者の端末情報を取得してしまうリスクがあります。たとえば、設置場所の設定誤りにより外部から容易にアクセス可能な状態になっていた場合や、検索エンジンのクローラーによって ICE プログラムが仕込まれた偽装ファイルがインデックス化された場合には、不特定多数がアクセスし、誤作動を引き起こすおそれがあります。また、セキュリティ研究者やホワイトハッカーが正当な目的でアクセスした場合であっても、ICE プログラムが作動して情報を取得してしまえば、プライバシー侵害等の問題に発展し、プログラム全体に対する社会的評価に重大な影響を及ぼす可能性があります。

第三に、導入目的と手段の相当性の関係が問題となります[6]。ICE プログラムの導入目的がサイバー攻撃に対する初動対応であることには一定の社会的意義が認められますが、その手段が過度に侵襲的である場合には、許容性の限界を超えるおそれがあります。たとえば、C2 サーバーへの妨害措置や、攻撃者端末への一方的な指令送信などが含まれる構成となっている場合には、社会的に相当な対応とは評価されにくく、不正性の要件に該当する可能性が高まります。特に、アクセス者が攻撃者か否かの判断がプログラム作動後にしかなされない構造や、判別困難な状態で一律に情報収集を行う設計は、相当性を著しく損なう要素となり得ます。

---

[5] 正当業務行為等としての違法性阻却を検討する場合も、判断要素は「不正性」の検討枠組みと実質的に重なると思われます。なお、ICE プログラムの設置時点では、通常「急迫不正の侵害」が存在しないため、正当防衛の適用は困難と考えられます。

[6] ICE プログラムによって取得された IP アドレス等の情報は、VPN やプロキシサーバーを経由して偽装されているケースも多く、必ずしも実際の攻撃者の特定に直結するとは限らないという限界も存在します。

過去の事例として、位置情報や通話履歴の取得機能を備えたスマートフォン監視アプリのプログラムが不正指令電磁的記録に該当するとされ、作成等を行った関係者が立件され、有罪判決を受けています[7]。ICE プログラムにおいても、同様に情報収集の範囲が限定されず、防御目的を超えて過剰であると評価される場合には、同種の法的リスクが現実化する可能性があります。

したがって、ICE プログラムについては、取得対象となる情報の範囲や作動対象の限定性、プログラムの具体的な動作内容によるものの、社会的に許容される範囲を逸脱すると評価され、不正性が認められるリスクは高いといえます。このような不正性のリスクを低減するためには、取得情報の範囲を必要最小限に限定した上で、アクセス制御、取得したデータの保持期間の短縮、誤作動防止のためのフィルタリングやアクセス制限等の技術的対策を講じておく必要があります。あわせて、情報取得の目的、手段、合理性を事前に文書化し、第三者に対する説明責任を果たせる体制を整えておくことが、企業にとって重要なリスク管理手段となります。

Ⅳ. 不正アクセス禁止法との関係

不正アクセス禁止法は、アクセス管理者の意思に反して他人の電子計算機に侵入する行為を「不正アクセス行為」として定義し、これを処罰の対象としています。ここでいう「不正アクセス行為」には以下の類型があります（法 2 条 4 項）。

① なりすまし行為（1 号）：他人の ID やパスワードなどの「識別符号」を無断で使用し、アクセスが制限されているコンピュータやサービスにログインする行為。

② セキュリティホール攻撃（2 号・3 号関連）：アクセス制御機能（認証システムなど）の脆弱性や設定不備（セキュリティホール）を悪用したり、それを回避するための特殊な情報やコマンドを入力したりして、制限されているコンピュータやサービスに侵入する行為。

企業が能動的サイバー防御の一環として、攻撃者の C2（Command and Control）サーバー等に対し、脆弱性を突いて侵入したり、ログを取得したり、マルウェアの削除、通信遮断といった措置を講じる場合には、いずれかの方法で攻撃者の意思に反して当該電子計算機にアクセスする必要があると考えられます。そのため、上記の定義に照らすと、不正アクセス行為に該当する可能性が極めて高いといえます[8]。

ここで重要なのは、たとえ当該サーバーがサイバー攻撃の発信元であったとしても、そのサーバーが攻撃者自身により管理され、アクセス制御機能が設定されている限り、その意思に反してアクセス・操作を行うことは、アクセス管理権の侵害として違法と評価され得るという点です。不正アクセス禁止法は、被アクセス側に「加害性」があるか否かにかかわらず、アクセス管理権そのものを法的に保護する趣旨に基づいており、これに反する行為は、法令上原則として違法と評価される可能性が高い点に留意が必要です。

また、このような行為について、刑法上の正当防衛（刑法 36 条）や正当な業務行為（刑法 35 条）により違法性が阻却されるかについては、実務上、極めて否定的に解釈されています。特に、民間企業による能動的サイバー防御が「社会的に相当」と評価されるためには、行為の緊急性、必要性、手段の相当性、代替手段の有無といった非常に厳しい条件をすべて満たす必要があり、これを企業の独自判断に委ねることは現実的とはいえません。

さらに、こうした無断アクセスは、単なる刑事リスクにとどまらず、捜査機関の活動や、国外に設置されたサーバーに対する越境的な侵入との関係で、他国の法制度との衝突や外交上の摩擦を引き起こす可能性も否定できません。国際的にも、サイバー攻撃の巧妙化・深刻化に対し、民間企業が取り得る能動的サイバー防御の是非や法的枠組みについては、活発な議論が行われています。特定の条件下で限定的な対抗措置を認めるべきとの意見がある一方、誤認攻撃のリスク、事態のエスカレーション、法的・倫理的課題、さらには国家主権の侵害といった懸念を理由に、慎重論や反対論が依然と

---

[7] 東京高判令和元年（2019 年）12 月 17 日・高等裁判所刑事裁判速報集（令和元年）362 頁

[8] ICE プログラムが、攻撃者のアクセスを契機として攻撃者端末上で作動し、IP アドレスや OS 情報などの情報を自動送信させる仕組みをとる場合には、通常は企業側から攻撃者端末に対してアクセスする構造にはなっておらず、不正アクセス行為には該当しないと考えられます。ただし、ICE プログラムが企業側から能動的に攻撃者端末に接続し、アクセス制御を突破するような動作を含む場合には、同法の構成要件該当性が問題となる可能性があります。

して根強く存在しています。このような状況を踏まえると、少なくとも現時点では、民間企業が単独で C2 サーバーへの侵入や制御取得、攻撃指令の遮断等を試みることは、極めて慎重に検討すべきであり、原則として回避することが望ましいと考えられます。

V. おわりに

能動的サイバー防御は、サイバー攻撃の高度化・巧妙化に直面する企業にとって、攻撃者の特定や二次被害の抑止といった観点から、極めて魅力的な技術的対応手段となり得ます。特に ICE プログラムのような仕組みは、初動段階での情報収集を可能にするという点で、防御体制の強化に資するものとして注目されています。

しかしながら、現行法の枠組みにおいては、こうした技術が刑法 168 条の 2 や不正アクセス禁止法に抵触するリスクを内包しており、現時点では民間企業が単独で能動的対処を行うことには、法的・技術的・倫理的な観点から慎重な判断が求められます。特に、C2 サーバー等へのアクセスや制御措置は、たとえ相手方が攻撃者であったとしても、アクセス管理権の侵害として違法と評価され得る可能性が高く、また国際的な摩擦を招くおそれもあります。

したがって、企業においては、攻撃の予兆を検知するための監視体制の強化、インシデント発生時の速やかな封じ込め、ログの保全・分析といった初動対応を徹底するとともに、捜査機関との連携を通じて、合法的な手段で攻撃者の特定と対応を図ることが、現実的かつ適法な選択肢となります。

また、能動的サイバー防御の導入を検討する場合には、導入初期段階から法務部門・セキュリティ担当部門・外部の専門家が連携し、プログラムの設計段階から合法性・必要性・正当性を多角的に検討するとともに、誤作動・誤検知・越境アクセス等に関するリスク評価と対策を並行して行うことが重要です。

今後、政府が進める法制度整備の動向や判例の蓄積等を注視しつつ、企業としては現行法の下で許容される範囲において、セキュリティ対策の高度化を図るとともに、必要に応じて専門家の助言を受けながら、慎重かつ計画的な運用を進めることが求められます。

以上

- 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

- 本ニュースレターの執筆者は、以下のとおりです。
弁護士 三宅 英貴（hidetaka.miyake@amt-law.com）
弁護士 中原 隆雅（takamasa.nakahara@amt-law.com）
弁護士 石川 雅人（masato.ishikawa@amt-law.com）

- ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

- ニュースレターのバックナンバーは、こちらにてご覧いただけます。