プライバシーがあぶない！
～「能動的サイバー防御法案」を問う～

日時：２０２５年３月１日（土）午後１時３０分～
場所：愛知県弁護士会５階ホール
主催：愛知県弁護士会

プログラム

司会　四橋　和久（ 愛知県弁護士会 会員 ）

13:30-13:35　**【開会の挨拶】**

尾関　信也（ 愛知県弁護士会 副会長 ）

13:35-15:00　**【講演】**

齋藤　裕 氏（ 新潟県弁護士会所属弁護士 ）

15:00-15:15　**－ 休 憩 －**

15:15-15:55　**【対談】**

齋藤　裕　氏（ 新潟県弁護士会所属弁護士 ）
聞き手　**新海　聡**　（ 愛知県弁護士会所属弁護士 ）
聞き手　**加藤　光宏**（ 愛知県弁護士会所属弁護士 ）

15:55-16:00　**【閉会の挨拶】**

鈴木　典行（ 愛知県弁護士会 秘密保護法・共謀罪法対策本部 本部長代行 ）

以　上

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案（いわゆる「能動的サイバー防御」法案）に関する会長声明

政府は、本年２月７日、①官民連携（情報共有、政府から民間事業者等への対処調整、支援等の取組強化等）、②通信情報の利用（日本に対するサイバー攻撃の実態を把握するため、通信情報を利用し、分析）、③アクセス・無害化措置（サイバー攻撃による重大な危害を防止するための警察・自衛隊による措置等を可能とし、その際の適正性を確保するための手続を新設）等を内容とする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案及びその施行に伴う関係法律の整備等に関する法律案（以下合わせて「本法案」という。）を国会に提出した。

同法案は、基幹インフラ等に対するサイバー攻撃への対処能力を高めることを目的としており、本法案が規定する官民連携等については一定評価し得るところである。

しかし、本法案中、通信情報の利用及びアクセス・無害化措置については、国会における慎重な審議が必要である。

当連合会は、「 》個人が尊重される民主主義社会の実現のため、プライバシー権及び知る権利の保障の充実と情報公開の促進を求める決議」（２０１７年１０月６日人権擁護大会）において、プライバシー尊重の観点から、「公権力が自ら又は民間企業を利用して、あらゆる人々のインターネット上のデータを網羅的に収集・検索する情報監視を禁止すること」を求めている。本法案における通信情報の利用については、不特定の人や回線を対象として行うものであり、「インターネット上のデータを網羅的に収集・検索する情報監視」に該当する可能性がある。また、通信当事者のメールアドレスなど、個人の交流や取引関係を推知し得る情報も選別され、対象となるものであり、通信の秘密の観点から重大な懸念を持たざるを得ない。国会審議においては、通信情報の利用が網羅的な通信情報の利用に該当するのではないか、日本国憲法や自由権規約が保障する通信の秘密やプライバシー権との関係で正当化し得るのか否かという観点からの審議が慎重になされる必要がある。

また、本法案が内容とするアクセス・無害化措置については、主に国外に所在する攻撃サーバ等を対象にすることが想定されており、内閣官房内に設置されていた「サイバー安全保障分野での対応能力の向上に向けた有識者会議」は、当該攻撃サーバが所在する他国の主権との抵触が問題となることを前提に、緊急避難法理により違法性が阻却され得るとしている。この緊急避難が適用されるためには重大かつ急迫した危険や唯一手段性等の要件が必要とされるところである。国会審議においては、アクセス・無害化措置がなされることが想定される事例に即して、本法案がこれらの緊急避難の要件を充足するものとなっているかなどについて慎重な審議を行うことが求められる。

よって、当連合会は、本法案の審議に当たっては、通信情報の利用及びアクセス・無害化措置に関し、上記のとおり指摘した懸念や課題事項について、慎重な検討を行うことを求める。

２０２５年（令和７年）２月１９日

日本弁護士連合会
会長　渕上　玲子

サイバー安全保障分野での対応能力の向上に向けた提言

概　要

令和６年１１月２９日

サイバー安全保障分野での対応能力の向上に向けた有識者会議

サイバー安全保障分野での対応能力の向上に向けた提言 1

サイバー安全保障分野での対応能力を欧米主要国と同等以上に**向上**させるための**新たな取組の実現**のために必要となる**法制度の整備等**について４度の全体会議及び９度のテーマ別会合にて検討し、**提言とりまとめ**。

実現すべき具体的な方向性

（１）官民連携の強化

- **国家をも背景とした高度なサイバー攻撃への懸念の拡大**、デジタルトランスフォーメーションの進展を踏まえると、**官のみ・民のみでのサイバーセキュリティ確保は困難**。インフラ機能など社会全体の強靱性を高めるため、**産業界をサイバー安全保障政策の「顧客」としても位置づけ**、政府が率先して情報提供し、**官民双方向の情報共有を促進**すべき。

- 高度な侵入・潜伏能力を備えた攻撃に対し事業者が具体的行動を取れるよう、専門的なアナリスト向けの技術情報に加え、**経営層が判断を下す際に必要な、攻撃の背景や目的なども共有**されるべき。情報共有枠組みの設置や、クリアランス制度の活用等により、情報管理と共有を両立する仕組みを構築すべき。

- これらの取組を効果的に進めるため、システム開発等を担う**ベンダとの連携を深める**べき。脆弱性情報の提供やサポート期限の明示など、**ベンダが利用者とリスクコミュニケーションを行う**べき旨を法的責務として位置づけるべき。

- 経済安保推進法の**基幹インフラ事業者によるインシデント報告を義務化**するほか、その**保有する重要機器の機種名等の届出**を求め、攻撃関連情報の迅速な提供や、ベンダに対する必要な対応の要請ができる仕組みを整えるべき。基幹インフラ事業者以外についても、インシデント報告を条件に情報共有枠組みへの参画を認めるべき。**被害組織の負担軽減と政府の対応迅速化**を図るため、**報告先や様式の一元化、簡素化**等を進めるべき。

サイバー安全保障分野での対応能力の向上に向けた提言 2

（２）通信情報の利用

- **先進主要国は国家安保の観点からサイバー攻撃対策のため事前に対象を特定せず一定量の通信情報を収集し、分析**。我が国でも、重大なサイバー攻撃対策のため、一定の条件下での**通信情報の利用を検討すべき**。

- **国外が関係する通信**は分析の必要が特に高い。まず、①**外外通信(国内を経由し伝送される国外から国外への通信)**は**先進主要国と同等の方法の分析が必要**。加えて、 ②攻撃は国外からなされ、また、国内から攻撃元への通信が行われるといった状況を踏まえ、**外内通信(国外から国内への通信） 及び内外通信(国内から国外への通信)**についても、被害の未然防止のために必要な分析をできるようにしておくべき。

- **コミュニケーションの本質的内容**に関わる情報は特に**分析する必要があるとは言えない**。**機械的にデータを選別し検索条件等で絞る等の工夫が必要**。

- **通信の秘密**であっても法律により**公共の福祉**のために**必要かつ合理的な制限**を受ける。先進主要国を参考に明確で詳細なルールとなるよう考慮し、緻密な法制度を作るべき。その際、**取得及び情報処理のプロセス**について**独立機関の監督**が重要。

- なお、**通信当事者の有効な同意**がある場合の**通信情報の利用**は、同意がない場合とは**異なる内容の制度により実施することも可能**であると考えられる。その際、制度により、基幹インフラ事業者の協議の義務化等で、必要に応じ、同意を促すことが考えられる。

- 性質上**非公開とすべき範囲はある**が**適切な情報公開**は行われるべき。**公開困難な部分を独立機関の監督で補う**べき。

（３）アクセス・無害化

●サイバー攻撃の特徴（①危険の認知の困難性、②意図次第でいつでも攻撃可能、③被害の瞬時拡散性）を踏まえ、**被害防止を目的**としたアクセス・無害化を行う権限は、**緊急性を意識**し、**事象や状況の変化に応じて臨機応変かつ即時に対処可能な制度にすべき**。こうした措置は、比例原則を遵守し、必要な範囲で実施されるものとする必要。その際、執行のシステム等を含め、従前から機能してきた**警察官職務執行法を参考**としつつ、その**適正な実施を確保するための検討を行うべき**。

●平時と有事の境がなく、事象の原因究明が困難な中で急激なエスカレートが想定されるサイバー攻撃の特性から、**武力攻撃事態に至らない段階から我が国を全方位でシームレスに守るための制度**とすべき。

●アクセス・無害化の措置の性格、既存の法執行システムとの接合性等を踏まえ、**権限の執行主体**は、**警察や防衛省・自衛隊**とし、その能力等を十全に活用すべき。**まずは警察が**、**公共の秩序維持の観点から特に必要がある場合には自衛隊が**これに加わり、共同で実効的に措置を**実施できるような制度とすべき**。

●権限行使の対象は、**国の安全や国民の生命・身体・財産に深く関わる国、重要インフラ、事態発生時等に自衛隊等の活動が依存するインフラ**等へのサイバー攻撃に重点を置く一方、**必要性が認められる場合に適切に権限行使できる仕組み**とすべき。

●国際法との関係では、他国の主権侵害に当たる行為をあらかじめ確定しておくことは困難。他国の主権侵害に当たる場合の違法性阻却事由としては、実務上は対抗措置法理より**緊急状態法理の方が援用**しやすいものと考えられるが、国際法上許容される範囲内でアクセス・無害化が行われるような仕組みを検討すべき。

（４）横断的課題

- 脅威の深刻化に対し、**普段から対策の強化・備えが重要**であり、**サイバーセキュリティ戦略本部の構成等を見直す**とともに、NISCの発展的改組に当たり政府の司令塔として強力な情報収集・分析、対処調整の機能を有する組織とすべき。

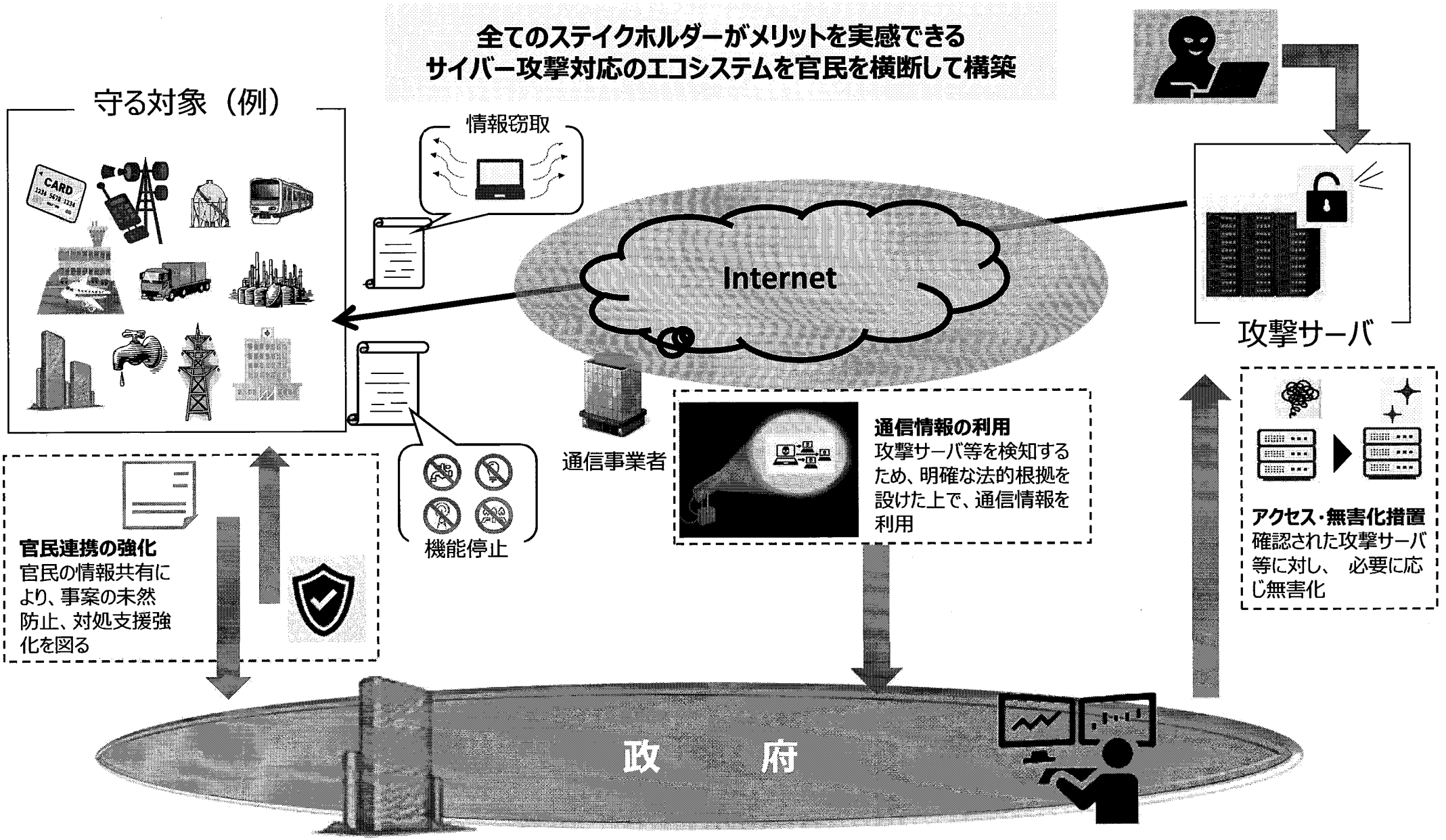
- 重要インフラのレジリエンス強化のため、行政が達成すべきと考える**セキュリティ水準を示し、常に見直しを図る制度**とするとともに、政府機関等についても**国産技術を用いたセキュリティ対策を推進**し、**実効性を確保する仕組み**を設けるべき。

- 政府主導でセキュリティ人材の定義の可視化を行い、関係省庁の人材の在り方の検討を含め、非技術者の巻き込みや人材のインセンティブに資する**人材育成・確保の各種方策を自ら実践**しながら、**官民の人材交流を強化**すべき。

- サプライチェーンを構成する中小企業等のセキュリティについて、意識啓発や支援拡充、対策水準等を検討すべき。

【参考】全体イメージ

「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。



提言で言及された対策	対策（中項目）	対策（細項目）	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案での対応状況	コメント
官民連携の強化	高度な攻撃に対する支援・情報提供			
		専門的なアナリスト向けの技術情報提供	１１条以下、４０条	
		攻撃の背景や目的の情報提供	１１条以下、４０条	
		ダークウェブからの情報提供		
		仮想通貨の移動分析情報提供		
		攻撃者の手法に関する具体的情報提供	１１条以下、４０条	
		サイバーセキュリティ協議会改組	４５条以下	
		緊急性の高い情報発信はワンボイス		
		現場レベルで官民の対応者が集結できる仕組み		
		国産技術の活用		
		友好国との間の相互運用性		
		ISAC間のノウハウ共有を政府が支援		
	ソフトウェア等の脆弱性対応			
		製品ベンダ等が利用者に対し適切にリスクコミュニケーションを行うべき旨の法的責務	サイバーセキュリティ基本法７条２項	
		上記法的責務履行に関し、政府が製品ベンダ等が提供すべき情報を整理		
		政府が、国内で悪用されている脆弱性情報を一元的にわかりやすく発信	４２条	
		特定重要設備に関連する一定の機器について、機種名等の届出を求めた上で、当該機器に対するゼロディ攻撃を含めた攻撃関連情報の迅速な提供や、製品ベンダ等に対する必要な対応の要請ができる仕組み	４条１項	
		SBOMの国際的な相互運用を前提とした活用推進		
		安全性のテスト基準等製品ベンダ等の規律の設定		サイバーセキュリティ基本法７条２項は具体的な規律について定めていない
		脆弱性情報の報告等を求める	４２条	
		ベンダに対するセキュアな製品開発・供給、脆弱性対応にあたっての助言や支援	４２条	
		ユーザーに対する適切な設定・運用の慫慂	４１条、４２条	
		外部からのスキャンによって脆弱性を把握し、注意喚起		注意喚起の対象となった組織の過度な負担に留意とされている
	政府の情報提供・対処を支える制度			
		基幹インフラ事業者に対して、インシデント報告を義務化し、情報共有を促進すべき。その中でもデジタルインフラと電力は、特に重要なインフラとして、より緊密な情報連携を行う	５条	
		重要インフラ事業者、その他の機微技術を持つ者等についても情報共有枠組みへの参画を認める	４５条	
		インシデント報告先の一元化や報告様式の統一化、速報の簡素化、報告基準・内容の明確化		
		インシデント報告での自動化技術活用		

提言で言及された対策	対策（中項目）	対策（細項目）	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案での対応状況	コメント
通信情報の利用			１１条以下、１７条以下、３２条以下	
アクセス・無害化措置			整備法６条の２等	
横断的課題	サイバーセキュリティ戦略本部・NISC・関係省庁が連携した施策の推進	基本的な方針や枠組みを大臣による戦略本部で決定し、それに対して普段から助言をする民の有識者からなる組織が別途存在するという形 NISCについて、政府の司令塔として発展的に改組するにあたり、インデリジェンス能力を高め、技術・法律・外交等の多様な分野の専門家を官民から結集し、強力な情報収集・分析、対処調整の機能を有する組織とする。 その際、NISCや関係する政府機関のほか、重要インフラに位置づけられている地方公共団体を含め、それぞれの役割と責任範囲を明確に整理。 関係省庁のセキュリティ部局が物理的に同じ場所で稼働できるよう、基盤となるインフラの確保	サイバーセキュリティ基本法２６条、３０条の２	
	重要インフラ事業者等の対策強化	実際の攻撃発生時におけるインフラの補完・代替・復旧等の計画 重要インフラ分野の防護範囲を定義するにあたり、重要性の優先順位とともに、新しい分類やデジタル空間の構造を踏まえた検討 優先度のガイドラインを作る サイバーセキュリティ対策の質についての基準、ガイドライン作成 認証、資格の活用や遵守状況の公表 優秀な取り組みの他分野への展開 中小企業へのリソース支援 政府調達要件への採用等		
	政府機関等の強化	戦略本部に全大臣参加 政府機関等の情報システム内で行われる不正活動を監視・制御する技術の導入を進め、今まで以上にサイバー攻撃に関する膨大かつ詳細な状況の観測・分析の積み重ねを行う 政府機関のサイバーセキュリティ水準を強固にする。府省横断的なリスク評価結果や注意喚起等が個々の政府機関に委ねられている点を改める 政府主導で高品質な国産セキュリティ製品、サービス供給の強化を支援。大学等で開発された技術等の社会実装と知見のフィードバックによるさらなる技術開発の促進というエコシステムの構築 政府が公共機関や国民向けに、セキュリティ対策を強化するための多様な支援ｻｰﾋﾞｽを提供	サイバーセキュリティ基本法２８条	

提言で言及された対策	対策（中項目）	対策（細項目）	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案での対応状況	コメント
	サーバーセキュリティ人材の育成・確保	政府が官民の人材育成の取り組みをしっかり把握した上で、技術者に限らず、経営等に関わる者も含めたサーバーセキュリティに関わる人材の定義づけや資格の活用による可視化 雇用する側の視点として、長期的なキャリアパスの明示、待遇の改善、経営層の理解の促進、人材の重要性の周知、企業等の組織への当該分野人材採用のための支援等 サイバーセキュリティを担う人材へのインセンティブ、CISOの重視 若年層から教育 民間とNISC等との人材交流 政府における任期の長期化等のサイバーセキュリティ部局の人材のあり方検討 産学官での人材交流・流動化促進		
	中小企業や地域における対策強化とその他の検討課題等	大企業による下請企業のセキュリティ対策の支援・要請に係る独占禁止法等の明確な整理 サプライチェーン企業の対策水準の検討 サーバーセキュリティの対策・情報共有を実施できる人材育成。政府がそのような中小企業等の活動を支援しつつ情報連携を行う施策検討		

通信情報の利用・無害化措置についての条文に即した検討メモ

弁護士　齋藤裕

第１章　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

第１　機械的情報について

１　２条８項１号

「この法律において「機械的情報」とは、通信情報のうち次に掲げるものをいう。一　電気通信の送信元又は送信先である電気通信設備を識別するアイ・ピー・アドレス・・・通信日時その他の通信履歴に係る情報」

「その他の通信履歴に係る情報」については、２４条において電子メールアドレスが選別後通信情報に含まれることを前提としているため、電子メールアドレス情報が含まれることは明らかである。電子メールアドレスについては、誰と誰が通信をしているかを示すもの、人間関係を示すものであり、要保護性が大きいと考えられる。

「その他の通信履歴に係る情報」については何がそこに含まれるか不明である。プライバシーを侵害につながる情報が入らないよう、対象を具体化する等の方策が必要ではないだろうか。

電気通信事業における個人情報等の保護に関するガイドライン（令和４年３月31日個人情報保護委員会・総務省告示第４号）３８条は、「通信履歴（利用者が電気通信を利用した日時、当該電 気通信の相手方その他の利用者の電気通信に係る情報であって当該電気通信の内容 以外のものをいう。以下同じ。）」との表現を用いているので、本法案においては「通信履歴に係る情報（通信の内容以外のものに限る）」などの表現とすることも考えられよう。

２　２条８項３号

「この法律において「機械的情報」とは、通信情報のうち次に掲げるものをいう。三　前二号に掲げるもののほか、電子計算機の動作の状況を示すために当該電子計算機が自動的に作成した情報その他それによっては通信の当事者が当該通信により伝達しようとする意思の本質的な内容を理解することができないと認められる情報として内閣府令で定める情報」

「それによっては通信の当事者が当該通信により伝達しようとする意思の本質

的な内容を理解することができないと認められる情報」に該当するかどうかの判断は人によって違いうる。どのような情報がここに該当すると想定されるのか国会審議で明らかにされるべきである。

第２　当事者協定について

１　１１条

「内閣総理大臣は、特別社会基盤事業者との間で、内閣総理大臣が、当該特別社会基盤事業者を通信の当事者とする通信情報の提供を受けた上で、当該通信情報のうち外内通信情報・・・に該当するものを用いて、当該特別社会基盤事業者が使用する特定重要電子計算機その他の電子計算機のサイバーセキュリティの確保を図るために必要な分析を行い」

重要電子計算機に対する被害を防止する必要性があるかどうかを問わず、特別社会基盤事業者が協定を締結さえすれば、特別社会基盤事業者と通信をする市民の通信に係る情報を内閣総理大臣に提供することを許容する規定である。

特別社会基盤事業者が協定を結ぼうが、特別社会基盤事業者と通信を行う市民は、通信情報が内閣総理大臣に行くことについて何ら承諾していないのである。

通信の秘密を制限する必要性が何らない場合にも締結できる当事者協定に基づき通信情報の提供を許す制度は憲法２１条の通信の秘密を侵害すると言えるのではないか。

２　１２条

「内閣総理大臣は、事業電気通信役務の利用者・・・との間で、内閣総理大臣が、当該利用者を通信の当事者とする通信情報の提供を受けた上で、当該通信情報のうち外内通信情報に該当するものを用いて、当該利用者が使用する電子計算機のサイバーセキュリティの確保を図るために必要な分析を行い」

１に述べたのとまったく同じことが問題となる。

３　２３条４項

「内閣総理大臣は、次に掲げる場合には、選別後通信情報を、特定被害防止目的以外の目的のために自ら利用し、又は提供することができる　一　第１５条の規定により取得した取得通信情報についての自動選別により得られた選別後通信情報・・・を当該当事者協定の協定当事者の同意を得て、自ら利用し又は

提供する場合」

当事者協定による通信情報の取得は、重要電子計算機に対する被害を防止する必要性があるかどうかを問わず、一方当事者のみの意思のみに基づき実施されるものである。

つまり、協定を締結していない側の通信当事者にとっては、通信情報を取得されなければならない言われがおよそないものである。

さらに、その選別後通信情報まで特定被害防止目的以外の目的に使用されるということになると、その通信の秘密を侵害するものと評価せざるを得ない。

第３　外外通信目的送信措置

１　１７条

「内閣総理大臣は、外外通信・・・であって、重要電子計算機に対する国外通信特定不正行為のうちその実行のために用いられる電子計算機、当該電子計算機に動作をさせるために用いられる指令情報その他の当該国外通信特定不正行為に関する実態が明らかでないために当該国外通信特定不正行為による重要電子計算機の被害を防止することが著しく困難であり、かつ、この項の規定による措置以外の方法によっては当該実態の把握が著しく困難であるものに関係するものが、特定の国外関係電気通信設備・・・を用いて提供される事業電気通信役務が媒介する国外関係通信に含まれると疑うに足りる場合において、必要と認めるときは、当該国外通信特定不正行為に関する第２２条２項に規定する選別の条件を定めるための基準・・・を定め、サイバー通信情報監理委員会の承認を受けて、当該国外関係通信により送受信が行われる媒介中通信情報が複製され、内閣総理大臣の設置する設備・・・に送信されるようにするための措置（以下「外外通信目的送信措置」という。）を講ずることができる。」

「当該国外通信特定不正行為に関する実態が明らかでないために当該国外通信特定不正行為による重要電子計算機の被害を防止することが著しく困難」ということが要件とされている。

しかし、「実態が明らかではない」ことが、ただちに被害防止の困難性につながるものではない。「実態が明らかではない」というだけであれば、行政等において従前実施してきたサイバー防御策によって防御できる可能性もあるだろう。もちろん、「実態が明らかではない」のであれば、従前実施してきたサイバー防御策によっては防御できない可能性も残るが、「実態が明らかではない」というだけであれば、どちらの可能性もあると言わなくてはならない。少

なくとも、積極的に、被害防止が困難であることを疑うに足る事情があるとは言えないだろう。

ところが、法案の書きぶりでは、「実態が明らかではない」という要件が満たされれば、「被害を防止することが著しく困難」という要件を満たすというように解釈されかねないと思われる。

そこで、「被害を防止することが著しく困難」と言えるためには、「実態が明らかではなく、かつ、他の被害の防止策によっては被害を防止することが著しく困難であるものに関係するものが」となるべきである。

そのような規定となった場合には、当然、「実態が明らかではない」ことのみならず、「他の被害の防止策によっては被害を防止することが著しく困難」との要件についても「疑うに足りる」状況がなければならない。

なお、「当該国外通信特定不正行為に関する実態が明らかでないために当該国外通信特定不正行為による重要電子計算機の被害を防止することが著しく困難」の後には、「かつ」という接続詞と「この項の規定による措置以外の方法によっては当該実態の把握が著しく困難であるものに関係するもの」との要件が記載されている。

しかし、本法案が目指すものは被害防止であって、「実態把握」は目的ではない。「実態把握」ができないとしても、被害防止さえできれば良いのである。そうであれば、「この項の規定による措置以外の方法によっては当該実態の把握が著しく困難であるものに関係するもの」との要件は不要であると思われるが、あえて強く削除を求めるほどのものではないだろう。

第４　自動的選別（外外・外内・内外通信目的送信措置）

１　２２条１項

「内閣総理大臣は、第１５条の規定又は外外通信目的送信措置により取得通信情報を取得したときは、当該取得通信情報の中から次に掲げる要件を満たす機械的情報であるもののみを選別して記録する措置であって、その選別が完了する前に当該取得通信情報が何人にも閲覧その他の知得をされない自動的な方法・・・で行われるもの・・・を講じなければならない・・・三　当該取得通信情報に係る対象不正行為に関係があると認めるに足りる状況のものであること」

２　３５条１項

「内閣総理大臣は、特定外内通信目的送信措置又は特定内外通信目的送信措置により取得通信情報を取得したときは、当該取得通信情報の中から次に掲げる

要件を満たす機械的情報であるもののみを選別して記録する措置であって、自動的方法で行われるものを講じなければならない・・・三　当該取得通信情報に係る対象不正行為に関係があると認めるに足りる状況のあるものであること」

3　三号の不明確性

三号の「当該取得通信情報に係る対象不正行為に関係があると認めるに足りる状況のものであること」との要件は不明確であるため、法文等においてどのような状況があれば当該取得通信情報にかかる不正行為に関係があると言えるのか、明確化することが必要である。

第5　選別後通信情報の利用

1　２３条２項

「内閣総理大臣は、第４項の規定による場合を除き、重要電子計算機に対する国外通信特定不正行為・・・による被害を防止する目的・・・以外の目的のために、自動選別により得られた取得通信情報・・・を自ら利用してはならない」

2　３１条３項

「第２３条２項から第４項まで・・・の規定は、通信情報保有機関の長・・・による選別後通信情報の取扱いについて準用する」

3　３６条

「内閣総理大臣が特定外内通信目的送信措置又は特定内外通信目的送信措置により取得通信情報を取得した場合には、特定外内通信目的送信措置又は特定内外通信目的通信措置により取得した取得通信情報を外外通信目的送信措置により取得した取得通信情報と、前条第１項の措置を自動選別と、当該措置により得られた取得通信情報・・・を選別後通信情報とそれぞれみなして、第２３条から第３１条までの規定を適用する」

4　選別後通信情報の捜査利用

都道府県警察が選別後通信情報を取得している場合、３１条２項で準用される２３条２項により、国外通信特定不正行為による被害を防止する目的以外の目的のために選別後通信情報は利用できないことになる。

しかし、国外通信特定不正行為による被害を防止するために捜査、起訴等を

行う必要がある場合に、２３条２項の規定だけでは、警察が選別後通信情報を捜査のために使うことができる余地があるように思われる。

憲法３５条１項は「何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第３３条の場合を除いては、正当な理由に基づいて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない」としている。

よって、捜査のために通信情報の利用を行うのであれば、令状が必要であり、本法案が令状なく通信情報の捜査利用を認めるのであれば憲法３５条１項に違反すると言わなくてはならない。

そうであれば、２３条２項とは別途、選別後通信情報を捜査のために利用できない旨の明文規定が必要だと思われる。

第６　特定内外通信目的送信措置

１　３２条

「内閣総理大臣は、外内通信であって、重要電子計算機に対する国外通信特定不正行為に用いられていると疑うに足りる状況にある特定の国外設備を送信元とし、又は当該国外通信特定不正行為に用いられていると疑うに足りる状況のある特定の機械的情報・・・・が含まれているもの・・・の分析をしなければ当該国外通信特定不正行為による重要電子計算機の被害を防止することが著しく困難であり、かつ、この項の規定による措置以外の方法・・・によっては当該特定外内通信の分析が著しく困難である場合において、必要と認めるときは、この項の規定による措置により取得通信情報を取得した場合のおける第３５条第２項に規定する選別の条件を定めるための基準・・・を定め、サイバー通信情報監理委員会の承認を受けて、国外関係電気通信事業者の設置する特定の国外電気通信設備であって当該国外関係電気通信設備を用いて媒介される国外関係通信に当該外内通信が含まれると疑うに足りるものによる送受信が行われる国外関係通信媒介中通信情報が複製され、受信用設備に送信されるようにするための措置・・・を講ずることができる」

２　３３条

「内閣総理大臣は、内外通信・・・であって、重要電子計算機に対する国外通信特定不正行為に用いられていると疑うに足りる状況のある特定の国外設備を送信先とし、又は当該国外通信特定不正行為に用いられていると疑うに足りる状況のある特定の機械的情報が含まれているもの・・・の分析をしなければ当該国外通信特定不正行為による重要電子計算機の被害を防止することが著しく

困難であり、かつ、この項の規定による措置以外の方法によっては当該特定内外通信の分析が著しく困難である場合において、必要と認めるときは、当該措置により取得通信情報を取得した場合における同条第２項に規定する選別のための基準・・・を定め、サイバー通信情報監理委員会の承認を受けて、国外関係電気通信事業者の設置する特定の国外関係電気通信設備であって当該国外電気通信設備を用いて媒介される国外関係通信に当該特区亭内外通信が含まれると疑うに足りるものにより送受信が行われる国外関係通信媒介中通信情報が複製され、受信用設備に送信されるようにするための措置・・・を講ずることができる。」

３　被害防止の困難性

特定外内通信・特定内外通信の分析をしなければ重要電子計算機の被害を防止することが著
しく困難との要件が設けられている。

この要件は、行政等において従前実施してきたサイバー防御策によって被害防止できる可能性が著しく低い場合にのみ満たされることが国会審議において確認されるべきであろう。

第２章　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の施行に伴う関係法律の整備に関する法律

第１　警察官職務執行法６条の２、２項

１　「サイバー危害防止措置執行官は、サイバーセキュリティ・・・を害することその他情報技術を用いた不正な行為・・・に用いられる電気通信若しくはその疑いがある電気通信・・・又は情報技術利用不正行為用いられる電磁的記録・・・若しくはその疑いがある電磁的記録・・・を認めた場合であって、そのまま放置すれば人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときは、加害関係電気通信の送信元若しくは送信先である電子計算機又は加害関係電磁的記録が記録され電子計算機・・・の管理者その他関係者に対し、加害関係電子計算機に記録されている加害関係電磁的記録の消去その他の危害防止のため通常必要と認められる措置であって電気通信改善を介して行う加害関係電子計算機の動作に係るもの・・・をとることを命じ、又は自らその措置をとることができる」

３　急迫性の要件

海外のサーバーに対する無害化措置が緊急避難法理により違法性が阻却されるためには、加害が「急迫」のものである必要がある。この「急迫」について、緊急避難法理を援用する者は、「時間的な近接性について、一定の合理性をもって説明することができる必要がある」（中村和彦「越境サイバー侵害行動と国際法―国家実行から読み解く規律の行方―」１９６頁）。

ところが、６条の２においては、「そのまま放置すれば人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるとき」との表現を使っている。

「そのまま」であるから、それは１年後かもしれないし、１０年後かもしれない。この条文は、そのうちいつか重大な危害が発生するおそれがあれば「緊急の必要」があるとするものであるが、これでは緊急避難における急迫性については「時間的な近接性について、一定の合理性をもって説明することができる必要がある」との要請を満たすことはできない。つまり、このような条文では、急迫性の要件を満たさず、緊急避難の要件を満たさない無害化措置がなされる危険性を払拭できないことになる。

最低限、「時間的に切迫しており、他の手段をとることができない」との趣旨の要件を盛り込む必要がある。

４　唯一手段性の要件

無害化措置について緊急避難法理が適用されるためには、無害化措置が「唯一の手段」である必要がある（中村和彦「越境サイバー侵害行動と国際法―国家実行から読み解く規律の行方―」１９６頁）。

しかし、６条の２において、そのような要件を踏まえた表現はみられない。

よって、この点からも、６条の２により、緊急避難の要件を満たさない無害化措置が行われるリスクがあると言える。

５　重大な損害をもたらさないとの要件

緊急避難法理が適用されるためには、他国の「不可欠の利益」を「深刻に損なう者ではない」ことが要件である（中村和彦「越境サイバー侵害行動と国際法―国家実行から読み解く規律の行方―」１９８頁）。

しかし、６条の２において、そのような要件を踏まえた表現はみられない。

よって、この点からも、６条の２により、緊急避難の要件を満たさない無害化措置が行われるリスクがあると言える。

第２　自衛隊法９１条の３

１　「警察官職務執行法第６条の２第２項から第１１項までの規定は、第８１条の３第１項の規定により通信防護措置をとるべき旨を命じられた部隊等の自衛官の職務の執行について準用する」

２　自衛隊による無害化措置

第１で述べたところが自衛隊による無害化措置にそのまま当てはまる。

以上