『ネットワーク安全法』施行後の4年を振り返って （一）

弁護士法人大江橋法律事務所
弁護士 竹田 昌史
PROFILE

上海翰凌法律事務所
律師 張 鵬程
PROFILE

今年の6月末に中国の配車サービス最大手である滴滴出行（DiDi）が米ニューヨーク証券取引所に上場した直後の7月2日に、突如、インターネット規制当局[1]による安全審査の実施とDiDiアプリの新規登録の一時停止が発表されました。更にその数日後、個人情報の違法な収集使用を理由として、中国で配信されるアプリストアから合計25個のDiDi関連アプリの撤去命令が下されたことは、日本の新聞等でも大きく報じられました。これら一連の審査の実施や撤去命令の根拠とされたのが、『ネットワーク安全法』[2]（以下「ネット安全法」といいます。）です。

ネット安全法は、2017年6月1日の施行からすでに4年近くが過ぎました。当初はその適用範囲の広さゆえ不明な点が多かったものの、この4年間で、多くのネットワーク安全に関連する法規、規則制度、基準等が相次いで公布され、また多くの処罰事例も積み重なり、少しずつ同法の運用状況が明らかになってきました。

本ニュースレターでは、全3回に分けて、ネット安全法の施行から4年間を振り返ってみたいと考えています。本稿はシリーズの第1回目として、先ず企業の立場に立って、ネット安全法の基本的な構造についてご説明いたします。

一　ネット安全法が想定するネットワークと安全

ネット安全法は合計7章（79条）からなり、主に第3章の「ネットワーク運行上の安全」と第4章の「ネットワーク情報の安全」が企業の様々な義務を定めており、重要な内容となります。この「ネットワーク運行上の安全」や「ネットワーク情報の安全」を理解するためには、まず「ネットワーク」と「安全」という言葉の意味を十分に理解することが非常に重要です。

[1] DiDi への審査の実施等に関する公告によれば、安全審査についてはネットワーク安全審査弁公室が行い、DiDi 関連アプリに対する各アプリストアからの撤去命令については国家インターネット情報弁公室が行っています。ネットワーク安全審査弁公室は国家インターネット情報弁公室の内部組織の一つであることから、本稿では、特に区別の必要がある場合を除き、両者を「インターネット規制当局」と総称します。

[2]中華人民共和国主席令第 53 号、2016 年 11 月 7 日公布、2017 年 6 月 1 日施行

ネット安全法において、「ネットワーク」とは、「コンピュータその他の情報端末及び関連設備により構成され、一定の規則及びプログラムに従い情報について収集、保存、伝送、交換及び処理をするシステム」をいいます。そのため、「ネットワーク」には、不特定多数の者の間でのインターネット以外に、個々の企業内でのローカルエリアネットワークやイントラネットも含まれることになります。

またネットワークの「安全」とは、「必要な措置を講じることを通じて、ネットワークに対する攻撃、侵入、妨害、破壊及び不法使用並びに突発的事故を防止し、ネットワークが安定かつ信頼可能な運行状態にあるようにし、並びにネットワークデータの完全性、秘密保持性及びユーザビリティを保障する能力」をいいます。そのため、ネットワークの安定性や運行の安全のみならず、ネットワーク上のデータや情報も保護の対象とされます。

二　ネット安全法の適用を受ける主体

ネット安全法が適用される主体（適用主体）は、大きく4種類に分けられます。1つ目は「ネットワーク運営者」、2つ目は「重要情報インフラ運営者（CIIO）」、3つ目は「特定業務の運営者 」[3]、4つ目は「すべての個人と組織」です。

4つの分類は必ずしも明確に区別できるわけではありませんが、各分類に応じて様々な義務と責任を負うため、企業としては、自社がどの分類に該当するのかを判断する必要があります。実務上、しばしば問題になるのはネットワーク運営者とCIIOです。そのため、以下では、ネットワーク運営者とCIIOを中心に解説いたします。

1　ネットワーク運営者

ネット安全法上、ネットワーク運営者は、ネットワークの所有者、管理者及びネットワークサービスの提供者をいいます（第76条）。そして、「ネットワーク」には個々の企業内でのローカルエリアネットワークやイントラネットも含まれ、同法は、中国国内におけるネットワークの「使用」についても適用されます（同法第2条）。そのため、例えば、中国の現地法人間や各法人内をLANで繋ぎ、またイントラネットを通じて情報を共有する場合、それらの現地法人は「ネットワーク運営者」であると判断される可能性があります。

2　重要情報インフラ運営者（CIIO）

（1）CIIOとは

企業は、自社がネットワーク運営者に該当すると判断した場合、更にCIIOに該当するか否かを判断しなければなりません。

[3]具体的には、ネットワーク製品/ネットワークサービスのプロバイダ、デジタル情報の発送/アプリケーションソフトウェアのダウンロードサービスプロバイダ等が含まれます。

ネット安全法では、ネットワーク運営者に該当することを前提として、以下の条件を満たすインフラ施設（CII）のネットワーク運営者を、特にCIIOと位置づけ、厳しい義務と責任を負わせています（同法第31条）。

①　公共通信及び情報サービス、エネルギー、交通、水利、金融、公共サービス、電子行政サービス等の重要な業界及び分野に該当すること

②　ネットワークの機能の破壊や喪失又はデータ漏洩にひとたび遭遇すれば、国の安全、国民の経済・生活及び公共の利益に重大な危害を及ぼす恐れのある重要情報インフラ施設であること

CIIOに関しては、今年の7月30日に国務院から「重要情報インフラ施設安全保護条例」（以下「CII安全保護条例」といいます）が公布され、9月1日から施行されますが、同条例で定めるCIIの定義では、上記（1）①の重要な業界及び分野に加えて「国防科学技術工業」を明記しています。また②の重要インフラ施設についても「重要なネットワーク施設、情報システム」と明記し、規制を強める分野や対象を少しずつ明確にしていることが伺えます。

（2）CIIOの認定

CII安全保護条例では、CIIOの認定にあたって、以下の2つのポイントを定めています。

①　CIIの認定ルールの策定

上記業界及び分野の主管部門と監督管理部門（いわゆる、CIIの安全保護業務に責任を負う機関であり、以下「保護担当部門」といいます）は、当該業界、分野の実状を踏まえ、以下の3つの要素を考慮してCIIの認定ルールを策定するものとされています。

ⅰ）ネットワーク施設、情報システムの当該業界、分野の重要な中核業務に対する重要度

ⅱ）ネットワーク施設、情報システムが破壊、機能不全又はデータ漏洩に遭遇すれば発生しうる被害の程度

ⅲ）その他の業種及び分野への関連性の影響

②　認定主体と事後の企業による報告義務

ネット安全法上、誰がCIIの認定を行うのか明らかではありませんでした。これに対し、CII安全保護条例では、保護担当部門がCIIの認定を行うことを明記し、速やかに認定結果を当事者に通知し、かつ国務院公安部門に報告するものとされました。

ただし、事後に認定結果に影響を及ぼす比較的大きな変化が生じたときには、CIIO自らが速やかに状況を保護担当部門に報告する義務が新設され、報告義務を怠った場合には行政罰を課すことが規定されました。

上記（2）①の「CIIOの認定ルール」に関して、2016年6月に中央網信弁ネットワーク安全協調局が行政部門

の内部向けに制定した『重要情報インフラ確定ガイドライン（試行）』（以下「確定ガイドライン」といいます。）で定める以下の3つのステップの判断基準は、CIIの判断プロセスを理解するうえで参考になります。

第一ステップ：ネット安全法で定める重要な業種や分野を参考に、当該地区、部門、業界の実状に基づき重要業務を確定。

第二ステップ：重要業務に関係する情報システム又は産業用制御システムを確定。

第三ステップ：第二ステップで確定された重要情報インフラに関するシステムについて、以下の3つの分類に区別し、各分類で定める一定の量的基準に照らして、最終的にCIIを確定。

a）　ウェブサイト類

e.g. 一日平均のウェブサイト閲覧数が延べ100万人を超えるウェブサイト

b）　プラットフォーム類

e.g.一日平均の成約発注額又は取引額が1000万人民元を超える場合

c）　生産業務類

e.g.一旦安全事故が発生すると、直接5000万人民元以上の経済損失を生じる場合

また確定ガイドラインは、あくまで行政機関内部向けのガイドラインですが、特に第三ステップでは具体的な定量基準を定めており、各企業が、自社の重要情報インフラ運営者に該当するリスクを判断するために有益といえます。そのため、今後新たに制定される予定の認定ルールでも、確定ガイドラインと同様の手法が踏襲されるのかが注目されます。

三　ネット安全法の重要な制度

ネット安全法上、企業にとって重要な制度は「ネットワーク運行上の安全」及び「ネットワーク情報の安全（個人情報の保護がメイン）」に関する制度です。また同法では、一定の事由がある場合には、各運営者の関係部門に対する報告や必要な協力を義務付けており、それらをまとめると、以下のとおりとなります。

1　ネットワーク運行上の安全制度

ネットワーク運行上の安全を担う重要な当事者はネットワーク運営者とCIIOであり、その制度上、主に両者を念頭に置いて規定されています。

（ネットワーク運営者を対象とする制度）

適用主体	制度及び義務の概要	関連条文
ネットワーク運営者	安全のレベル別保護制度 ●国で定める等級レベルに応じた安全保護義務を負う。	第 21 条
	実名登録制 ●ネットワーク接続等のサービスを利用するユーザーに対し実名登録を要求しなければならない。	第 24 条
	緊急対応策、リスク処置制度 ●ネットワーク攻撃、ウイルス侵入時の緊急対応策の策定、緊急時の対処義務を負う。	第 25 条

CIIOは、ネットワーク運営者の上記義務以外に、更に以下の義務も負います。

（CIIOを対象とする制度）

適用主体	制度及び義務の概要	関連条文
CIIO	より厳格な安全のレベル別保護制度 ●専門的な安全管理組織の設置、重要職務の担当者への審査、従業員への定期的な教育などの義務を負う。	第 34 条
	調達行為に関する安全審査義務 ●ネットワーク製品やサービスの調達が国家の安全に影響を与える恐れがある場合、国家安全審査に合格しなければならない。	第 35 条
	調達時の安全秘密保持契約の締結義務 ●ネットワーク製品やサービスの調達時に、安全秘密保持契約を締結しなければならない。	第 36 条
	データの越境移転にかかる制限 ●中国国内で取得した個人情報及び重要データの中国国内保存義務、並びに当該情報を国外に越境する場合の安全評価の実施義務を負う。	第 37 条
	安全性の検査評価制度 ●自らまたは第三者機関を通じて、少なくとも年一回、安全性に関する検査評価を行い、保護担当部門に報告する義務を負う。	第 38 条

2　ネットワーク情報の管理制度

ネットワーク情報の管理制度の重点は、やはり個人情報の保護におかれています。そして、ネットワークの運行の安全制度と異なり、CIIOに対する特別な義務はなく、主にネットワーク運営者に対する以下のような義務を定めています。

適用主体	制度及び義務の概要	関連条文
ネットワーク運営者	個人情報の安全保護 ●ユーザーの情報の秘密の保持、及び保護制度の確立義務を負う。	第 40 条 第 42 条
	個人情報の収集方針の告知、及び同意の取得 ●収集のルール、目的、方法、範囲を告知し、被収集者の同意を得る必要がある。	第 41 条 第 42 条
	収集、使用の制限	第 41 条

	●提供するサービスと無関係な情報、違法又は契約違反となる個人情報の収集、使用は禁止される。	
	個人情報の毀損の禁止 ●収集した情報を漏洩、改ざん、毀損してはならず、被収集者の同意のない第三者への提供も禁止される。漏洩等が発生した場合には救済措置を採らなければならない。	第 42 条
	個人からの要求に基づく情報の削除及び訂正 ●違法な情報収集使用を理由とする個人からの削除要求又は情報の誤りを理由とする修正要求がある場合、当該個人の情報の削除、修正義務を負う。	第 43 条

更に、情報管理と違法な情報の取り締まりという観点から、以下のような制度も設けています。

適用主体	制度及び義務の概要	関連条文
ネットワーク運営者	ユーザーが公表する情報の管理 ●ユーザーが公表する情報内容が法令に違反する場合、直ちに公表の停止、削除等の措置を採らなければならない。	第 47 条
	ネットワーク情報に関する苦情申立て・通報 ●ネットワーク情報に関する苦情申立の制度を設けなければならない。	第 49 条

3　協力と報告制度

適用主体	制度及び義務の概要	関連条文
ネットワーク運営者	ネットワーク安全事件の報告 【三,1.の緊急対応策、リスク処置制度に対応】 ●ネットワーク攻撃、ウイルス侵入等のネットワーク運行上の安全に危害を及ぼす事態が生じた場合、救済措置を採ると共に、主管部門へ報告しなければならない。	第 25 条
	公安機関、国家安全機関への協力 ●各機関による国の安全の維持活動及び犯罪捜査活動に対する技術支援及び協力をしなければならない。	第 28 条
	個人情報の漏洩、毀損、紛失の報告 【三,2.の個人情報の毀損の禁止に対応】 ●個人情報の漏洩、毀損、紛失又はその可能性が発生した場合、ユーザーへの告知及び主管部門への報告義務を負う。	第 42 条
	ユーザーの違法情報の報告 【三,2.のユーザーが公表する情報の管理に対応】 ●ユーザーが公表した違法情報を削除すると共に、記録を保存して主管部門に報告しなければならない。	第 47 条
	監督検査への協力 ●ネットワーク情報部門が実施する監督検査に対して協力しなければならない。	第 49 条

4．CII安全保護条例で新設された主な義務

CII安全保護条例では、ネット安全法では規定されていないCIIOに対する新たな義務も新設されており、各企業が注意すべき主なものは以下の通りです。

適用主体	制度及び義務の概要	関連条文
CIIO	ネットワーク安全に対する重大事件が発生した場合の保護担当部門及び公安部門への報告 ● ネット安全法では、「ネットワーク運営者」の義務としてネットワーク安全事件発生時の主管部門への報告が義務付けられた。これに対し、今回、「CIIO」に関しては、「重大な」ネットワーク安全事件発生時に、「公安部門」への報告も追加された。違反の場合、「ネットワーク運営者」の義務に比べて重い行政処罰が課される。	第 18 条（CII 安全保護条例、以下同様）
	合併、分割、解散等の状況が発生した場合の保護担当部門への報告義務 ● 報告に基づき保護担当部門の要求がある場合、安全確保のための措置を講じなければならない。	第 21 条

組織再編時の報告義務に関しては、合併、分割、解散以外に、CIIOが他社を買収する場合や他社に買収される場合まで適用されるかは明らかではありません。また「審査」ではなく「報告」であり、当該報告を怠った場合には一定金額の行政罰が課せられますが、独占禁止法の事業者集中のように審査完了まで行為の実施を禁止する内容にはなっていません。もっとも、実務上、中国での組織再編やM&Aにおいて行政部門への報告や審査制度はプロジェクトのスケジュールに大きく影響するため、今後の運用が注目されます。

最後に、中国の個人情報保護法がいよいよ2021年8月20日に公布され、11月1日から施行されることになりました。そこで、次回は、日本企業にも大きな影響を及ぼす、ネット安全法や個人情報保護法等で定める情報の越境に関する規制の現状についてご説明いたします。

以上

具体的な事案に関するお問い合わせ／配信申込・停止申込✉メールアドレス： info_china@ohebashi.com

back to contents