



中国のサイバーセキュリティ法におけるプライバシー

著者： クリス・カオ、 ネイサン・スナイダー、 北川恵子

2017年3月

国際ビジネスの世界は、中国(中華人民共和国)での新しいサイバーセキュリティ法（下記“同法律”とする）の2017年6月1日の施行を前にして、慎重かつ警戒の体制となっています。同法律では、企業に対し、サイバーセキュリティの観点からプライバシーを保護するためのシステムを構築することを要求しています。しかしながら、この種のシステムがどの位徹底されるべきか、そしてどのような措置が適切であるとみなされるかについての多くの未解決の問題が残されています。

企業が彼らのサイバーインフラストラクチャーを変更するための時間枠はわずか数ヶ月しか残されていません。そしてさまざまな多国籍企業が同法律の規定する要件を満たすために、彼らの事業のさまざまな側面において行動を起こしています。

弁護士は法律で事業を行っています

サイバーセキュリティ、特に個人情報保護に関してクライアントにアドバイスを行っている弁護士にとって、同法律への遵守とデータの使用においては三重苦（三つの困難）があります。企業は、データの移動性、データ保



Photo courtesy of Alessio Lin

護の厳格な基準、データの価値の向上の3つの目標のうちの2つのみを選択できます。

コンサルタントがクライアントに対してバランスの取れたソリューション（解決策）をセットアップする手助けをすることは本当の難題となるでしょう。

コンサルタントにとっての良いニュースは、サイバーセキュリティ市場が巨大であるということです。同法律はイントラネットであってもウェブサイトや通信インフラストラクチャーを持つほぼすべての企業にサイバーセキュリティの責任を課しているため、ほとんどの事業は、同法律の要件を満たすためにITセキュリティシステムをセットアップする必要があるでしょう。あらゆる“ネットワーク事業者”（基本的にはインターネットへのアクセス権を持つすべての機関を意味する）が

自分のシステムの責任を負うようにし、そのため、違法な目的をもった詐欺を企む当事者に利用されないようにすることが倫理としてまとめられます。サイバーセキュリティに対する基本的要求は、ウェブサイトの「インターネットコンテンツプロバイダ」規則へのコンプライアンスから、プライバシー問題からデータ保護と利用のバランスまで含む包括的なサイバーセキュリティメカニズムにまで進化しました。

悪いニュースとは、いくつかの重要な規則がまだ定められていない状態にあるということです。まず最初に、既に使用されているコンピュータやその他のサイバー設備を整備する必要があるかまたはそれが義務化されていますか？同法律では、このような機器がサイバーセキュリティまたは「インターネット重大インフラ」に影響を及ぼす場合、州の強制検証命令の要件を満たさなければならないと述べています。しかし、現時点では、検証基準やプロセスに関する拘束力のある規則は存在しません。

第二に、この法律では複数層のITセキュリティメカニズムを規定しており「ネットワーク事業者」は、そのような仕組みのなかでの彼らの位置づけに沿ったサイバーセキュリティ計画を立てなければなりません。しかしメカニズムがどのようになるのかはまだ決定されていません。

第三に、データのローカリゼーション要件とデータのクロスボーダー（国境を越えた）取引との間の矛盾は辛いものです。

これらの質問に関しては、コンサルタントは待つこと以外ほとんどできることはありませんが、役人関係者は、詳細な条例、規則、カタログが検討されていることを示唆しており、それらは同法律が執行される前に公布される予定であります。

弁護士が今後目指すべき役割は何ですか？

多くの重要な規則がまだ整備されていないことを考えれば、弁護士は依然としてなすべきことが沢山あります。同法律では、サイバーオペレーションセキュリティ、個人情報保護、電信通信当局とのやりとりという3つの主要な側面に大まかに分類できる要件を規定しています。それぞれの面において、弁護士は役割を担います。

サイバーオペレーションセキュリティ

サイバーオペレーションのセキュリティに関しては、弁護士はストレージ、ハッキング、ウィルス、ソート、暗号化、バックアップの問題に触れるデータ保護について顧客に対してアドバイスを提供するものとします。

この作業は単にIT部門の仕事ではありません。弁護士は、そのような技術的プロセスが、法律（または一般的なプラクティスおよび法律が存在しないところでの慣行およびガイドライン）に準拠していることを確認して、例えばデータ漏洩などの場合にクライアントがより安全な位置に置かれるようにする必要があります。その上、弁護士はその当初から介入すべきです。

データのライフサイクルは大まかに以下の6つの段階に分けられます。

- 1) 生成/調達
- 2) 保管
- 3) 使用
- 4) 共有
- 5) ファイリング、および
- 6) 破棄

コンプライアンスの面では、各段階は比較的にそれぞれ別々のルールになっています。法律の顧問は、外部からの攻撃だけでなく、機

関の内部での悪意または不注意による不正行為からも保護するデータ保護システムを構築する際にアドバイスをする必要があります。多層の機密データアクセスシステムが慎重に確立され、異なる従業員に対して異なるアクセス権が与えられるべきであります。このプロジェクトは、ITチームや弁護士によって実施されるビジネス秘密の保護と重複しています。望ましくない状況のなかでの悪化を避けるために、「ネットワーク事業者」は、弁護士を使って緊急時計画を立案するとともに行政当局とのやり取りに関して支援する必要があります。

個人情報保護

個人情報保護は同法律の重要な一部分です。個人情報保護とプライバシーに関する規則は、有名なAPECプライバシーフレームワークと非常によく似ています。このフレームワークは、9つの原則を定めています。

- 1) 被害の防止
- 2) 通知
- 3) 情報集めの限界
- 4) 選択肢
- 5) 個人情報の保護または正確性
- 6) 安全保障措置
- 7) アクセスと安全対策
- 8) アクセスと修正、および

9) 説明責任。

それぞれの原則において、法律顧問がプライバシーコンプライアンスにおいて大きな役割を果たし、それぞれの同法律の対応を見ることができます。個人情報保護は一般的なデータ保護と似ています。なぜなら個人情報はデータの一種であるためです。しかし、個人情報の方が消費者の権利を含む様々な視点か

ら法律によって規制されているため、もっと注意を要します。

法律顧問は、請負業者との契約を合理化・改善するためにクライアントを支援することもできます。個人は、ネットワーク事業者が収集した彼らの個人情報の削除または修正を要求する権利があります。個人に正当な事由がある場合、ネットワーク事業者は要求された通りに行動しなければなりません。個人は、またネットワーク事業者からの個人データを取得するネットワーク事業者の請負業者が削除を実行することを保証するよう求めるかもしれません。請負業者が個人データの削除および訂正ポリシーに正式に従うことを確認するために、顧客と彼らの請負業者との契約交渉は重要です。

行政当局とのやりとり

最後にはなりましたが、これも重要なことですが、法律顧問は、行政当局とのやりとりについて顧客に助言をすべきであります。この法律は、ネットワーク事業者と当局との間の協力を規定しています。サイバーセキュリティの不規則性が発生した場合、当局に対して早期報告することで、通常、結果として生じたいかなる責任をも緩和することができます。当局と日ごろの緊密な関係を持つことで、当局の監督が緩和されますが、サイバーセキュリティの施行と執行のあらゆる問題に関与する当局の数は10を超えるかもしれません。したがって、顧問は、今後、サイバーセキュリティに関するアドバイスにおいて、重大な任務があることが予想できます。

著者：



Chris CAO, associate
クリス・カオ、アソシエート
chris.cao@eiger.law



Nathan SNYDER, trainee
ネイサン・スナイダー 研修生
nathan.snyder@eiger.law



Keiko KITAGAWA, Japanese Account Representative
北川恵子日本顧客部門代表者
keiko.b.kitagawa@eiger.law

DISCLAIMER

This publication is not intended to provide accurate information in regard to the subject matter covered. Readers entering into transaction on the basis of such information should seek additional, in-depth services of a competent professional advisor. Eiger, the author, consultant or general editor of this publication expressly disclaim all and any liability and responsibility to any person, whether a future client or mere reader of this publication or not, in respect of anything and of the consequences of anything, done or omitted to be done by any such person in reliance, whether wholly or partially, upon the whole or any part of the contents of this publication. This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license,

please visit <http://creativecommons.org/licenses/by-sa/3.0/>.