ABeam Consulting®

Build Beyond As One™

中国における個人情報保護および サイバーセキュリティ関連法動向と対応

Trends and Responses in Personal Information Protection and Cybersecurity-Related Laws in China

2025.08

はじめに

現代のデジタル社会において、サイバーセキュリティと個人情報保護は極めて重要な課題となっている。インターネットの普及とともに、私たちの生活はますますオンラインに依存するようになり、個人情報の取り扱いも増加している。このような状況下で、サイバー攻撃やデータ漏洩のリスクは高まり続けており、各国政府はこれに対処するための法規制を強化している。

中国においても例外ではなく、サイバーセキュリティ法をはじめ法整備が段階的に進んでおり、中国でビジネスを行う企業は法規制への対応が求められている。

本レポートでは、まず主要国・地域におけるサイバーセキュリティおよび個人情報保護に関する法規制の現状とその特徴について概述する。特に、欧州連合(EU)、アメリカ合衆国、および日本に焦点を当て、それぞれの法規制がどのようにして個人情報を保護し、サイバーセキュリティを強化しているかを解説する。

次に、主要国・地域との類似点や相違点を踏まえて、中国におけるサイバーセキュリティおよび個人情報保護に関する法規制の現状とその特徴について概述する。

最後に、中国において法規制に対応するために各企業が実施すべきプロセスを当社の知見を踏まえて解説し、グローバルな視点からの対応策を提案する。

本レポートが、サイバーセキュリティおよび個人情報保護に関する理解を深め、中国における企業や個人が適切な対策を講じるための一助となることを願う。

目次

第一章

主要国・地域の個人情報保護および サイバーセキュリティ関連法規制概要

1.1 主要国・地域の規制動向

近年、グローバルな個人情報保護やサイバーセキュリティに関する法規制は急速に進展している。特に、デジタル化の進展とともに、個人情報の保護とサイバーセキュリティの重要性が増している。

欧州連合(EU)の一般データ保護規則(GDPR)は、2018年に施行されて以来、世界的なデータ保護の基準となっている。

アメリカでは、州ごとに異なるプライバシー法が存在する。カリフォルニア州の消費者プライバシー法(CCPA)やその改正版であるカリフォルニア州プライバシー権法(CPRA)は、GDPRに類似した規制を設けており、消費者に対するデータの透明性と管理権を強化している。

アジア地域でも、個人情報保護に関する法規制が強化されている。日本の個人情報保護法は2022年に改正され、データ漏洩時の報告義務や個人の権利強化が図られた。

中国においても2017年のサイバーセキュリティ法の施行を皮切りに、データセキュリティ法や個人情報保護法など、関連法やガイドラインが相次いで施行されている。

以降でこれら主要国・地域の法制度のポイントについて解説する。

EU[1]
● 2016年：ネットワークおよび情報システムのセキュリティに関する指令(NIS指令)
● 2018年： 一般データ保護規則(GDPR)
● 2023年：NIS2指令

アメリカ[2]
● 2018年：カリフォルニア州消費者プライバシー法(CCPA)
● 2022年： 重要インフラ向けサイバーインシデント報告法(CIRCIA)
● 2023年：カリフォルニア州プライバシー権法(CPRA)

日本[3]
● 2005年：個人情報保護法
● 2015年：サイバーセキュリティ基本法

[1]. 出典：https://eur-lex.europa.eu/ より抜粋

[2]. 出典：https://oag.ca.gov/およびhttps://www.federalregister.gov/より抜粋

[3]. 出典：https://laws.e-gov.go.jp/ より抜粋

1.2 EUの関連法概要

個人情報保護

欧州連合(EU)では、デジタル時代における個人情報保護とサイバーセキュリティの強化を目的として、数々の法規制を導入してきた。その中でも特に重要なのが、2018年に施行された「一般データ保護規則(General Data Protection Regulation，通称GDPR)」である。個人の権利が強化されるとともに、事業者に対しては広範な適用範囲と違反時の厳しい罰則が規定されている。

GDPRは他国の法制度へも強い影響を与えている。

【GDPRの主要ポイント[1]】

適用範囲	• EU域内に拠点を持つ企業だけでなく、EU域内の個人データを処理する全ての企業に適用される。これにより、EU域外の企業もGDPRの規制対象となる。
個人データの定義	• 識別された又は識別され得る個人に関するあらゆる情報。Cookieなどのデジタルデータも多くの場合該当すると考えられる。
個人の権利	• データ主体(個人)の権利を強化し、データアクセス権、訂正権、消去権(「忘れられる権利」)、データポータビリティ権などを明確に規定している。
データ越境	• 原則的にEU域外への個人データの持ち出し(移転)を認めていない。移転には「越境移転規制」というルールをクリアする必要がある。
罰則	• GDPR違反に対する制裁金は非常に高額で、最大で年間売上高の4%または2000万ユーロのいずれか高い方が課される可能性がある。

[1]. 出典: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1743906443998 より当社にて抜粋・要約して記載

1.2 EUの関連法概要

サイバーセキュリティ

EUはサイバーセキュリティの強化にも力を入れており、重要インフラのセキュリティを強化し、サイバー攻撃に対する耐性を高めることを目的として2016年には「ネットワークおよび情報システムのセキュリティに関する指令(The Directive on Security of Network and Information Systems、通称NIS指令)」を制定した。NIS指令はEU各国のセキュリティ強化に貢献したものの、デジタル化の急速な進化や各国間の対策のレベル感の差異により、一部の加盟国がサイバー脅威に対して脆弱になりEU全体に波及するリスクに直面している。こうしたリスクの解消を目的として、改正版として2023年にNIS2指令が発効され、EU加盟国は2024年10月までにこの指令を国内法に組み込むことが求められた。

対象企業は高いセキュリティ態勢の整備が必要であり、違反時の罰金は高額である。

【NIS2指令の主要ポイント[1]】

対象	• EU内でサービスを提供する必須事業体および重要事業体。 • 必須事業体：エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、デジタルインフラ、など。 • 重要事業体：郵便、宅配、化学品、食品 、 製造業など。
必要な セキュリティ対策	• 全方位的な災害アプローチ対応が必要。 • システムセキュリティポリシー、インシデント対応計画、事業継続計画、サプライチェーンのセキュリティ対策、トレーニング、アクセス管理手順、など。
報告義務	• 重大なインシデント発生時に、24 時間以内の早期警告や1ヶ月以内の最終報告書の当局提出などが必要。 • 当局は必須事業体への抜き打ち検査などの監査や書面調査権限を有する。
罰則	• 必須事業体：最高1,000万ユーロ、または事業体の全世界年間総売上高の2%のいずれか高い方の額の罰金。 • 重要事業体：最高700万ユーロ、または事業体の全世界の年間総売上高の1.4%のいずれかの高い方の額の罰金。

[1]. 出典: https://www.nis-2-directive.com/NIS_2_Directive_Articles.html より当社にて抜粋・要約して記載

1.3 アメリカの関連法概要

個人情報保護

アメリカ初の包括的な個人情報保護法として、2018年にカリフォルニア州で「カリフォルニア州消費者プライバシー法(California Consumer Privacy Act， 通称CCPA)」が制定された。2020年には、CCPAを強化する形で「カリフォルニア州プライバシー権法(California Privacy Rights Act，通称CPRA)」が成立し、2023年に施行された。

その他の州においても、CCPAやEUのGDPRの要素を取り入れつつ、各州の特性に合わせた規制を行っている。

連邦レベルでは2022年に「アメリカデータプライバシー保護法(American Data Privacy and Protection Act，通称ADPPA)」の法案が初めて委員会で可決され、包括的な個人情報保護法の成立が期待されている。

【CPRAの主要ポイント[1]】

適用範囲	• カリフォルニア州で事業を行う営利企業・団体で、年間総収入が2,500万ドルを超えるなどの条件に当てはまる企業。これにより、カリフォルニア州外の企業もCPRAの規制対象となる。
個人情報の定義	• 特定の消費者又は世帯を、識別したり直接的または間接的に合理的にリンクさせることのできる情報。Cookieなどのデジタルデータも多くの場合該当すると考えられる。
個人の権利	• 消費者の権利として、知る権利、削除する権利、個人情報の販売または共有に関するオプトアウトの権利、未成年者のためのオプトインの権利、訂正する権利、等を規定。
データ越境	• 海外へのデータ移転自体について直接かつ個別に規制する規定はない。
罰則	• 違反1件あたり2,500ドル(16歳未満個人情報に関する故意/違反は7,500ドル)以下の制裁金が科される。また、消費者は1事故あたり最大750ドルの損害賠償請求権があり、賠償額が高額となる可能性がある。

[1]. 出典: https://www.caprivacy.org/cpra-text/ より当社にて抜粋・要約して記載

1.3 アメリカの関連法概要

サイバーセキュリティ

サイバーセキュリティに関しては、政府と民間企業間でのサイバー脅威情報の共有を促進し、レジリエンスを強化することを目的に、2022年に「重要インフラ向けサイバーインシデント報告法(Cyber Incident Reporting for Critical Infrastructure Act of 2022，通称CIRCIA)」が制定された。その後、2024年に米国サイバーセキュリティ・インフラストラクチャセキュリティ庁(Cybersecurity and Infrastructure Security Agency，通称CISA)がCIRCIAの具体的な施行規則案(意見募集稿)を発表した。この規則案が採択されれば、化学、防衛、通信、金融、食料、原子力、情報技術、医療など、16の重要インフラ分野に属する多数の企業が対応必要となる。なお、本規制案の最終稿は現在策定中。

【CIRCIA規則案の主要ポイント[1]】 ※未施行

対象	• 重要インフラ部門に属する小規模企業の基準を超える米国内の事業体。 • 重要インフラ：化学、防衛、通信、金融、食料、原子力、情報技術、医療など。
必要な セキュリティ対策	• インシデント発生時の報告に必要なデータの記録が必要。 (一)脅威行為者とのやりとり(メール、チャットなど)。 (二)不審なNWトラフィック、ファイル、ログインなど。 (三)OSバージョン、パッチレベル、構成設定など。
報告義務	• 報告対象となるインシデントが発生したと認識してから72時間以内、ランサムウェア攻撃に対する身代金の支払いが支払われてから24時間以内に当局への報告が必要。
罰則	• 当局は対象事業体に情報提供の要求や召喚状を執行する権限を有する。 虚偽の報告に対しては、罰金や最長5年の懲役(テロに関係する場合は最長8年)が科される。

[1]. 出典: https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements より当社にて抜粋・要約して記載

1.4 日本の関連法概要

個人情報保護

日本の個人情報保護法(Act on the Protection of Personal Information，通称APPI)は、個人の権利や利益を保護しつつ、個人情報の適正な取り扱いを確保することを目的としています。この法律は、2003年に制定され、2005年に全面施行された。その後、デジタル技術の進展やグローバル化に対応するため、数回の改正が行われている。現在は3年ごとに施行状況についての検討を行い、必要があるときは見直しすることが定められている。

【個人情報保護法(APPI)の主要ポイント[1]】

適用範囲	• 日本国内の個人に対する物品又は役務の提供に関連して、個人情報、個人関連情報又は仮名加工情報、匿名加工情報を利用する事業者。外国において取扱う場合も適用。
個人情報の定義	• 生存する個人に関する情報で、氏名、生年月日その他の記述などで特定の個人を識別できる情報。指紋、マイナンバーなどの個人を特定できる符合も含む。Cookieなどのデジタルデータも個人情報と紐づけ管理されている場合に該当。
個人の権利	• 個人情報の開示、訂正、利用停止、消去に関する請求権を規定している。
データ越境	• 外国にある第三者への提供を認める旨の本人の同意を得た上で移転可能。ただしEUなど、個人情報保護制度が日本と同などの水準にあると認定された国・地域とは自由に移転可能。
罰則	• 違反時に、個人には1年以下の懲役または100万円以下の罰金が科される。法人には1億円以下の罰金が科される。

[1]. 出典:https://laws.e-gov.go.jp/law/415AC0000000057より当社にて抜粋・要約して記載

1.4 日本の関連法概要

サイバーセキュリティ

サイバー攻撃の増加とその高度化に対応するため、日本においても2015年に「サイバーセキュリティ基本法」が施行された。本法においては、政府によるサイバーセキュリティ戦略本部の設置やサイバーセキュリティ戦略の立案を義務付け、政府、地方公共団体、重要インフラ事業者などがサイバーセキュリティ対策に努めることを求めている。

しかし、EUやアメリカと比べ、重要インフラ事業者に対する具体的なセキュリティ対策の義務付けや、違反時の罰則がまだ十分に整備されていない面もあり、関連法制の強化は引き続き検討が必要な段階である。

【サイバーセキュリティ基本法の主要ポイント[1]】

対象	• 国、地方公共団体、重要社会基盤(インフラ)事業者、サイバー関連事業者など。 • 重要インフラ：電力、ガス、化学、航空、鉄道、情報通信、金融、医療など。
必要な セキュリティ対策	• 重要インフラ事業者にて、サイバーセキュリティに関する基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進が必要となる。
報告義務	• 本法自体に重要インフラ事業者やその他事業者への報告義務の規定はない。各分野個別のガイドラインなどに沿った報告を行う。
罰則	• サイバーセキュリティ協議会の事務従事者が秘密を漏らした場合は一年以下の懲役又は五十万円以下の罰金が科される。事業者のサイバーセキュリティ対策不備に対する罰則規定はない。

[1]. 出典:https://laws.e-gov.go.jp/law/426AC1000000104 より当社にて抜粋・要約して記載

1.5 まとめ

近年のサイバー攻撃のリスク増大やデータ保護意識の高まりを受けて、主要国・地域では法制度の整備・改正が取り組まれており、当該エリアでビジネスを行う企業は対応が必要である。特にEUは厳格なルールと高額な罰金が特徴であり、他の法動向にも影響を与えている。

こうした主要国・地域の動向を踏まえた上で、中国における個人情報保護やサイバーセキュリティ対策の主要法について次章で解説する。

個人情報保護関連法の主要ポイントサマリー

	EU (GDPR)	アメリカ (CPRA)	日本 (APPI)
データ越境	原則禁止 (ルールをクリアすれば可能)	規定なし	本人の同意の上で可能 (個人情報保護制度が日本と同等以上の水準にあると認定された国・地域とは自由に移転可能)
罰則	高額の罰金	高額の罰金	EU、アメリカに比べ低額の罰金や懲役刑

サイバーセキュリティ関連法の主要ポイントサマリー

	EU (NIS2指令)	アメリカ (CIRCIA規則案) ※未施行	日本 (サイバーセキュリティ基本法)
報告義務	重大インシデント発生時 24時間以内の早期警告 など	重大インシデント発生時 72時間以内の報告 など	報告義務の規定はない
罰則	高額の罰金	罰金 又は5年以下の懲役刑 など	低額の罰金 又は1年以下の懲役刑 など

第二章

中国における個人情報保護および
サイバーセキュリティ関連法規制概要

2.1 中国の法整備動向

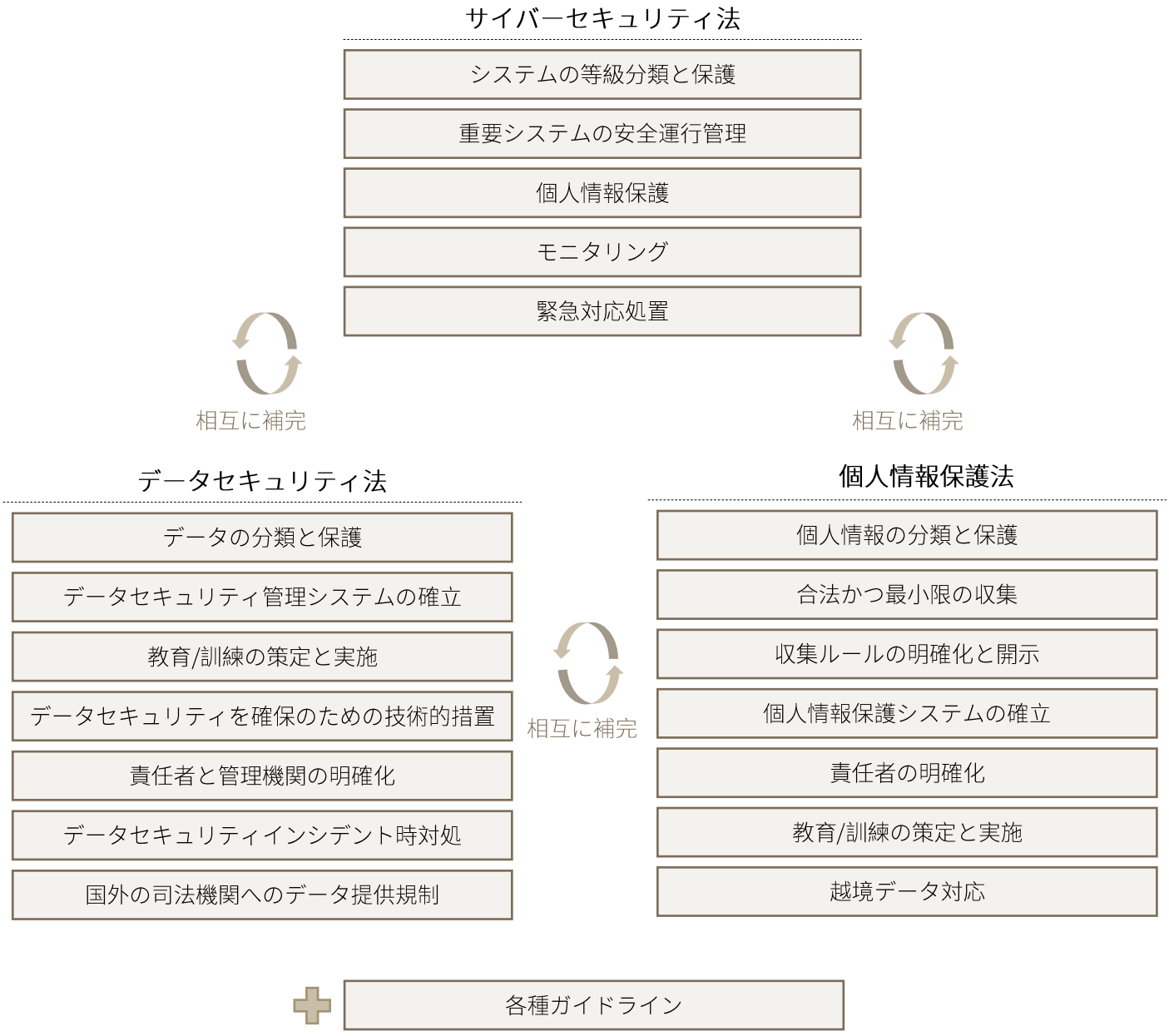
中国においても、デジタル社会の進展やそれに伴うリスクの増大を受けて、サイバーセキュリティや個人情報保護に関する法整備に早くから着手している。具体的には、2017年の「サイバーセキュリティ法」を皮切りに、「データセキュリティ法」、「個人情報保護法」というデータ関連主要三法が施行された。また、関連するガイドラインなども順次施行されており、在中国企業はこれらの法規にのっとった対応が求められている。

主要な法整備動向

2017年6月1日	《サイバーセキュリティ法》 サイバーセキュリティガバナンスへの道筋をつける
2020年1月1日	《暗号法》 暗号技術の応用と管理の規範化
2021年9月1日	《データセキュリティ法》 国のデータセキュリティと安全性の能力を強化する
2021年11月1日	《個人情報保護法》 個人情報の法制化を加速する
2022年9月1日	《データ越境安全管理弁法》 個人情報及び重要データの処理取扱いを規制する
2023年6月1日	《個人情報越境の標準契約弁法》 個人情報越境時に提出すべきの標準契約書の提供
2024年3月22日	《データの越境流動の規範化及び促進に係る規定》 個人情報越境時の手続き要件の緩和
2024年9月14日	《センシティブ個人情報識別ガイドライン》 センシティブ個人情報を識別するための具体例を提示
2025年1月1日	《ネットワークデータセキュリティ管理条例》 データ三法に基づいて遵守すべき規定を具体化

2.2 主要な法の概要

データ三法ではそれぞれ重要データや個人情報の保護、セキュリティ管理体制の確立などが規定されているが、各法の内容はある程度重なる領域がありそれぞれが補完しあう関係となっている。また、各法に基づいた個別ガイドラインも順次施行されている。したがって、各企業は各データ三法やガイドラインなどの内容を理解した上で総合的な対応を行う必要がある。



2.3 サイバーセキュリティ法概要

サイバー攻撃の増加と、それに伴うネットワークおよびシステムの管理の堅確化・高度化の必要性を受けて、2017年6月1日にサイバーセキュリティ法がされた。この法律は、サイバー空間の安全を確保し、国家の安全と公共の利益を守ることを目的としている。サイバーセキュリティ法は、企業にとってシステムの重要性に応じた管理面/技術面双方での包括的な対応をを課す一方で、サイバー空間の安全を確保し、国家の安全と公共の利益を守るための重要な法律である。

中国の企業は、本法の規定を遵守し、適切な対策を講じることで、サイバーセキュリティの強化を図る必要がある。

【サイバーセキュリティ法の主要ポイント】

対象	• 中国内のネットワーク運営者、重要インフラ施設運営者、インターネット製品およびサービス提供者などの企業や個人を対象とする。
必要な セキュリティ対策	• 等級保護制度に基づき、等級に報じた管理面、技術面双方でのセキュリティ対策が必要となる。
報告義務	• ネットワーク 製品及びサービスに安全上の欠陥などのリスクが存在することを発見した際には、セキュリティインシデント規定に従い関係各所に報告が必要。 • 重要インフラについては最低年一回の検査報告が必要。　など
罰則	• 違反時は深刻度に応じた罰則が科される。 重大な場合は高額の制裁金が科される。また、関連事業の停止の可能性もある。

2.4 等級保護制度

中国のサイバーセキュリティ法に基づき、サイバーセキュリティ攻撃の損害を受けた場合に影響を及ぼす対象とその影響度に応じて、一級から五級に等級付けされ各等級に応じたセキュリティ対策が求められる。

【等級の判定基準[1]】

損害を受ける対象	被害を受けた場合の影響度		
	一般的な損害	深刻な損害	特に深刻な損害
国民・法人・その他組織の利益	第一級	第二級	第三級
社会秩序と公共利益	第二級	第三級	第四級
国家安全にかかわる内容	第三級	第四級	第五級

【等級保護の対応プロセス[1]】

[1]. 出典:「GB/T 22240—2020 ネットワークセキュリティ等級保護定級ガイドライン」および「GB/T 28449-2018 ネットワークセキュリティ等級保護評価測定プロセスガイドライン」より当社にて抜粋・要約して記載

2.5 個人情報保護法概要

中国での個人情報保護について包括的に規定した法律として、2021年に「個人情報保護法」が施行された。中国としての個人情報の収集、使用、保存、提供に関する規定を設け、個人の権利を保護している。

【個人情報保護法の主要ポイント】

適用範囲	• 中華人民共和国の域内において自然人の個人情報を処理する活動に対して、本法を適用する。 • 中華人民共和国の域外において、中華人民共和国域内の自然人の個人情報を処理する活動が、以下に掲げる事由のいずれか一に該当する場合も、本法を適用する。 (一)域内の自然人に向けて商品又はサービスを提供することを目的としている場合。 (二)域内の自然人の行為を分析し、評価する場合。 (三)法律、行政法規が規定するその他の事由。
個人情報の定義	• 匿名化された情報を除き、電子的又はその他の方法で記録された、識別された又は識別可能な自然人に関連するあらゆる種類の情報。
個人の権利	• データ主体(個人)の権利を強化し、知る権利、閲覧権、複製権、訂正権、削除権などの各種権利などを規定している。 • 企業は個人情報の処理に関して本人の明確な同意を得る必要がある。
データ越境	• 特定の条件に当てはまる場合は、データ管理態勢の自己評価や当局の評価に合格した上で個人情報の越境が可能となる。
罰則	• 違反時は深刻度に応じて罰則がある。深刻な場合は5000万元以下又は前年の売上高の5%未満の罰金を科される。また、関連事業の停止の可能性もある。

2.6 データ越境規制

個人情報保護法の重要な規定の一つとして個人情報を中国国外へデータ越境転送する場合の規制がある。データ越境規制については2022年の「データ越境安全管理弁法」などを経て順次手続きが具体化・改正されている。越境するデータの内容と量に応じて必要な手続きが異なっており、 特に外資系企業は自社への影響を確認し適切な対応をする必要がある。

【データ越境のパターン[1]】

越境パターンごとの必要な手続き		
越境パターン		必要な手続き
1	• 重要データ(※)を越境する ※一度改ざん、破壊、漏洩または違法な取得・利用が行 われると、国家の安全、公共の利益を脅かす恐れのあるデータ	国家ネットワーク安全弁公室の安全評価
2	• 当年1月1日から累積して越境する一般個人情報が100万人以上または敏感個人情報が1万人以上となることが見込まれる場合	国家ネットワーク安全弁公室の安全評価
3	• 当年1月1日から累積して越境する一般個人情報が10万人以上100万人未満となることが見込まれる場合または1万人未満の敏感個人情報を越境する場合	標準契約の締結または個人情報保護認証の取得
4	• 当年1月1日から累積して重要インフラ運営者以外のデータ処理者が海外に一般個人情報を提供した件数(敏感個人情報を含まない)が10万人未満の場合 • 個人を一方当事者として契約を締結、履行するために域外に個人情報を提供する場合(例、越境ショッピング、航空券・ホテルの予約、ビザの手続きなど) • 法に基づいて制定された労働規則制度及び集団契約に基づいて国境を越えた人的資源管理を行い、海外に従業員の個人情報を提供する必要がある場合　　など	データ越境にあたって当局への届け出は不要 (ただし、「個人情報保護法」第55条の規定により、件数に関わらず個人情報保護のセルフアセスメントは必要となる)

[1]. 出典:「越境データセキュリティ管理弁法」、「データの越境流動の規範化及び促進に係る規定」より当社にて抜粋・要約して記載

2.7 セキュリティ関連法に基づく処罰・裁判事例

セキュリティ関連法に違反した場合は行政処罰や裁判による賠償を命じられる場合がある。以下にサイバーセキュリティ法違反の事例と、個人情報保護法の域外適用によりフランス企業に賠償命令がでた判例について例示する。グローバル企業が中国の個人情報を取り扱う場合は、GDPRなどの自地域の法令に則るだけでなく中国の関連法に適用したローカライズも必要となる。

サイバーセキュリティ法に基づく行政処罰事例(2024年8月) [1]

2023年11月から2024年7月にかけて、通辺市公安機関は通辺の某热电公司に対して複数回のネットワーク安全監督検査を実施し、高リスクのセキュリティ脆弱性に対して行政警告を行った。しかし、同社は有効な是正措置を講じず、システムは長期間高リスク状態を放置したまま稼動していた。そのため、公安機関は同社の法人代表Aとネットワーク安全責任者Bに対して、それぞれ1万元と5千元の行政罰金を科した。

個人情報保護法の域外適用による賠償判例(2023年9月) [2]

中国人の原告Cは、フランスの某会社が運営するホテルの会員カードを購入し、同社のアプリでミャンマーのホテルを予約した。その後、原告は個人情報が同社グループの複数の域外地域と事業者に共有されたことを発見した。原告はアプリ上で個人情報が複数の国に共有されることが記載された同社ポリシーに同意していたものの、ポリシー上では提供する事業者と地域の範囲が不明確であり不適切な個人情報の共有がなされたと認識し、個人情報保護法に違反として同社を提訴した。裁判所は、被告が適切な情報提供を行わず、個人情報を不適切に共有したと認定し、原告への書面での謝罪と個人情報の削除、および2万元の賠償を命じた。

[1]. 出典:https://baijiahao.baidu.com/s?id=1810625493255242736&wfr=spider&for=pcより当社にて抜粋・要約して記載

[2]. 出典: https://www.meritsandtree.com/UpLoadFile/Files/2024/9/2/18249331e6e8f0be-b.pdf より「(2022)粤0192民出6486号」の判決内容を当社にて抜粋・要約して記載

2.8 在中国の日系企業が取り組むべきこと

中国では、システムセキュリティや個人情報保護に関して、世界的に見てもいち早く包括的な整備が進められている。セキュリティリスクやビジネスの動向を考慮し、関連法の具体化や補足も進んでいる。中国の法律はGDPRと類似する点も多いが、中国独自の具体的な規定も存在する。したがって、例えばEU内では適法でも中国では違法となる場合があるため、セキュリティ管理態勢の適切なローカライズが必要である。

関連法への対応必要事項は多岐にわたるが、初期段階からすべてを実行することは困難である。まずは、しっかりと自社の現状を適切に把握し、その上で現実的な対応策・スケジュールを策定し、段階的かつ確実に実行することが肝要である。

現状の把握や対応計画の立案が自社リソースで困難な場合は、専門のコンサルティング会社を活用することが有用である。アビームコンサルティングは、当該分野での多数の実績を有しており、次章ではその一例を紹介する。

【中国のサイバーセキュリティ関連法への主要な対応事項】

システムセキュリティの観点
1) 中国国内で利用する情報システムのセルフアセスメント 2) 等級に応じたセキュリティ対策

個人情報保護の観点
1) 利用する個人情報の適切な把握 2) 個人情報の収集や管理について、中国の関連法・ガイドラインに則した対応の実施 3) 国外へ越境する個人情報の種類・量に応じた適切な手続き

第三章

中国の法制度への対応方法

3.1 中国の法制度への対応プロセス

中国のサイバーセキュリティ関連法への対応に当たっては、まず現状のシステムや保有データの重要度(等級、個人情報有無、越境データ有無など)を適切に把握した上で、あるべき姿とのギャップを明らかにすることが必要である。また、それらの課題に対する対応ロードマップを整備し、対策の実行とその後の継続的評価/改善のPDCAサイクルを回していくことが肝要である。

①現状調査	• 情報システムの管理面/技術面での態勢について、各種法律やガイドラインに従って自己アセスメントを行う • 個人情報などのデータの保有/管理状況について自己アセスメントを行う
②あるべき姿とのギャップの抽出	• 中国の各種法制度に違反する可能性のあるギャップ(課題)をリストアップする
③ロードマップ策定	• 課題について対策と対応時期を検討しロードマップを策定する
④対策の実行	• ロードマップに従って対応策を実施する • 情報システムの等級届け出や個人情報のデータ越境に関する当局への届け出を行う
⑤継続的な評価・改善	• 定期的なアセスメントの実施や従業員へのトレーニングなど継続的な評価・改善活動を行う

3.2 事例1 - 情報システムの自己アセスメント支援

法対応の必要性は理解しているものの、社内リソースが不足していて現状の把握が不十分な在中国の外資系企業は多く存在する。当社はそうした企業の自己アセスメントを支援し、等級保護の要求事項に対する現状の充足状況と課題を明確化した。

背景と課題	中国でビジネスを展開する日系製造業A社は、オンプレミスやパブリッククラウド上に複数の業務システムを保有していた。しかし、IT部門や法務部門のリソースが潤沢でないことから、それらのシステムの管理状況が法対応として適切かどうか未評価であった。
当社が提供したソリューション	A社が保有する主要システムについて、等級保護の管理面および技術面の両面の要求事項に適合しているかどうかのアセスメントを実施した。要求に達していない部分については具体的にリスト化し、優先的に対応すべき事項を明確にした。

アセスメント観点(大分類)[1]

管理面要求	セキュリティ管理制度	技術面要求	物理環境
	セキュリティ管理機構		通信ネットワーク
	セキュリティ人員管理		セキュリティ区域境界
	セキュリティ建設管理		コンピューティング環境
	セキュリティ運用管理		セキュリティ管理センター

[1]. 出典:「GB/T 22239-2019 情報セキュリティ技術 ネットワークセキュリティ等級保護基本要求」より当社にて抜粋・要約して記載

3.2 事例2 - 越境個人情報アセスメント支援

個人情報保護について、近年その定義や情報取得・管理要件が段階的に規定・具体化されている。特に個人情報を中国国外に越境転送する場合は情報の内容や量によって手続きが異なるため、各企業は自社の保有状況を正確に把握した上で適切な対応をとる必要がある。当社は保有するテンプレートや評価基準などを活用して越境する個人情報のアセスメントを実施した。

背景と課題

日系サービス業B社は、中国拠点において従業員や顧客の個人情報を保有し、業務上一部のデータを日本本社にも転送している。それらの情報の棚卸や管理状況が法要件に適しているかについて未評価であり、早急に確認する必要があった。

当社が提供したソリューション

当社の個人情報の棚卸や管理状況に関するテンプレートなどを活用してB社の個人情報管理の現状アセスメントを実施した。アセスメントを通してデータ越境関して実施すべき手続きや管理上の課題について明らかにし、今後の対応ロードマップを作成した。

個人情報例[1]

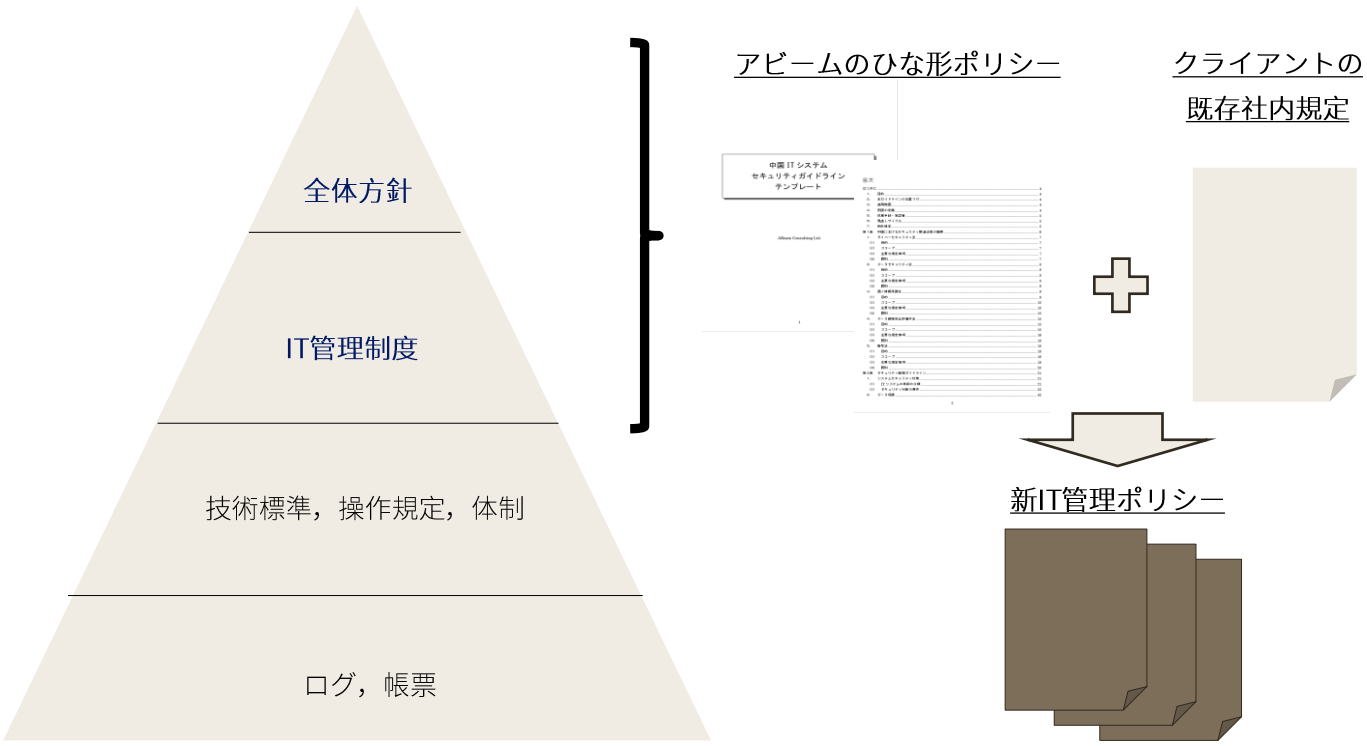
個人情報(例)	種類例
個人の基本データ	個人の氏名、生年月日、性別、民族、国籍、家族関係、住所、個人の電話番号、電子メールアドレスなど
個人の身分情報	身分証、士官証、パスポート、運転免許証、従業者証、出入許可証、社会保険カード、居住証など
個人の生体認証情報	個人の遺伝子、指紋、声紋、手相、耳介、虹彩、顔の特徴など
ネットワークIDの識別情報	システムアカウント、IPアドレス、ユーザー個人のデジタル証明書など
個人の健康及び生理的情報	個人の発病治療などにより生じる関連記録。例えば、疾病、入院記録、医師指示票、検査報告、手術及び麻酔記録、看護記録、投薬記録、薬品食品アレルギー情報、出産情報、既往歴、治療状況、家族の病歴、現病歴、伝染病歴など、並びに、個人の身体的健康状況について生じる関連情報
個人の教育及び勤務情報	個人の職業、職位、勤務先、学歴、学位、教育を受けた経歴、職歴、育成訓練記録、成績票など
個人の財産情報	銀行口座、識別情報(パスワード)、預金情報(資金額、金銭支払受取記録などを含む)、不動産情報、貸付記録、信用情報、取引及び消費記録、出納記録など、並びに仮想通貨、仮想取引、ゲーム類のリディームコードなどの仮想財産情報
個人の通信情報	個人情報主体の通信記録及び内容、ショートメッセージ、マルチメディアメッセージ、電子メール、並びに個人の通信を記述したデータなど
連絡先の情報	アドレス帳、友達リスト、グループリスト、電子メールアドレスリストなど
個人のネットワーク接続記録	ログに記録されたユーザーの操作記録をいう。ウェブサイト閲覧記録、ソフトウェア使用記録、クリック記録、お気に入りリストなどを含む
個人の常用装置情報	ハードウェアのシリアル番号、装置のMACアドレス、ソフトウェアリスト、一意の装置識別コードなどを含めた、個人が常用する装置の基本的状況を記述した情報をいう
個人の位置情報	行動の軌跡、正確な位置情報、宿泊情報、緯度経度などを含む
その他の情報	婚姻歴、宗教の信仰、性的指向、公開されていない違法犯罪記録など

[1]. 出典:「GB/T 35273-202_信息安全技术个人信息安全规范」より当社にて抜粋・要約して記載

3.2 事例3 - IT管理ポリシー策定支援

等級保護の要求に対応するためには、まず社内のIT管理ポリシーを適切に整備してそれに則った管理面/技術面の具体策を実行していく必要がある。等級保護の要求は多岐にわたるため、当社は要求に対応したひな形ポリシーを基に各企業に適したIT管理ポリシー策定を支援している。

背景と課題	日系製薬業C社は、社内情報システムの自己アセスメントの結果、IT管理ポリシーの充足度が等級保護の要件に対して不足していることが判明した。同社は中国国内に複数の支社を有しており、国内全社共通で利用可能なIT管理ポリシーを整備する必要があった。
当社が提供したソリューション	当社の等級保護要求に対するひな形IT管理ポリシーを基に、クライアントの既存の社内規定の内容も加味して、等級保護の要求事項に対応したC社中国全社共通のIT管理ポリシーを策定した。

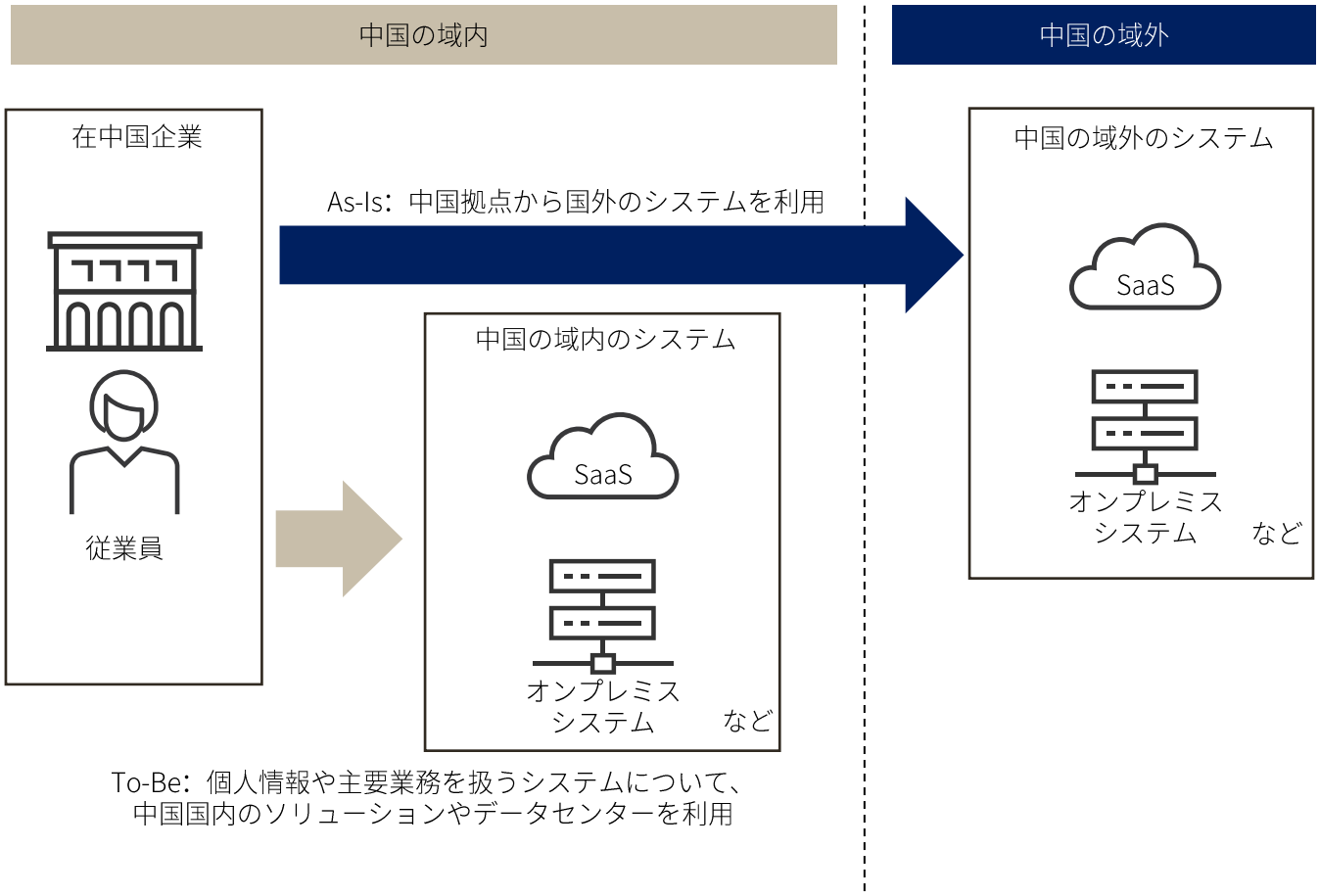


3.2 事例4 - 中国ITソリューション活用の構想策定

中国において国外の本社などのシステムを利用する外資系企業は多い。

しかし、国外システムの利用は個人情報保護やAI、半導体規制などのリスクも伴う。当社は、主要な業務システムについて中国国内のソリューションへの切り替えを検討するクライアントに対して、構想策定を実施した。

背景と課題	中国に複数の工場や事務所を持つ日系製造業D社は、日本本社や国外のSaaSを利用して主要業務や一部個人情報の管理を行っていた。現時点では中国のセキュリティ関連法に抵触はしていないものの、将来的なリスクや利便性を勘案し中国国内のシステム利用を検討していた。
当社が提供したソリューション	当社のABeam Global Development Centre(Shanghai)(略称：GDC)での豊富な知見や人員を活用し、国外システムを中国に移管する場合の一連の構想策定(アーキテクチャの検討、中国国内ソリューションの選定、実現のための費用・期間の見積やロードマップの作成、など)を実施した。



第四章

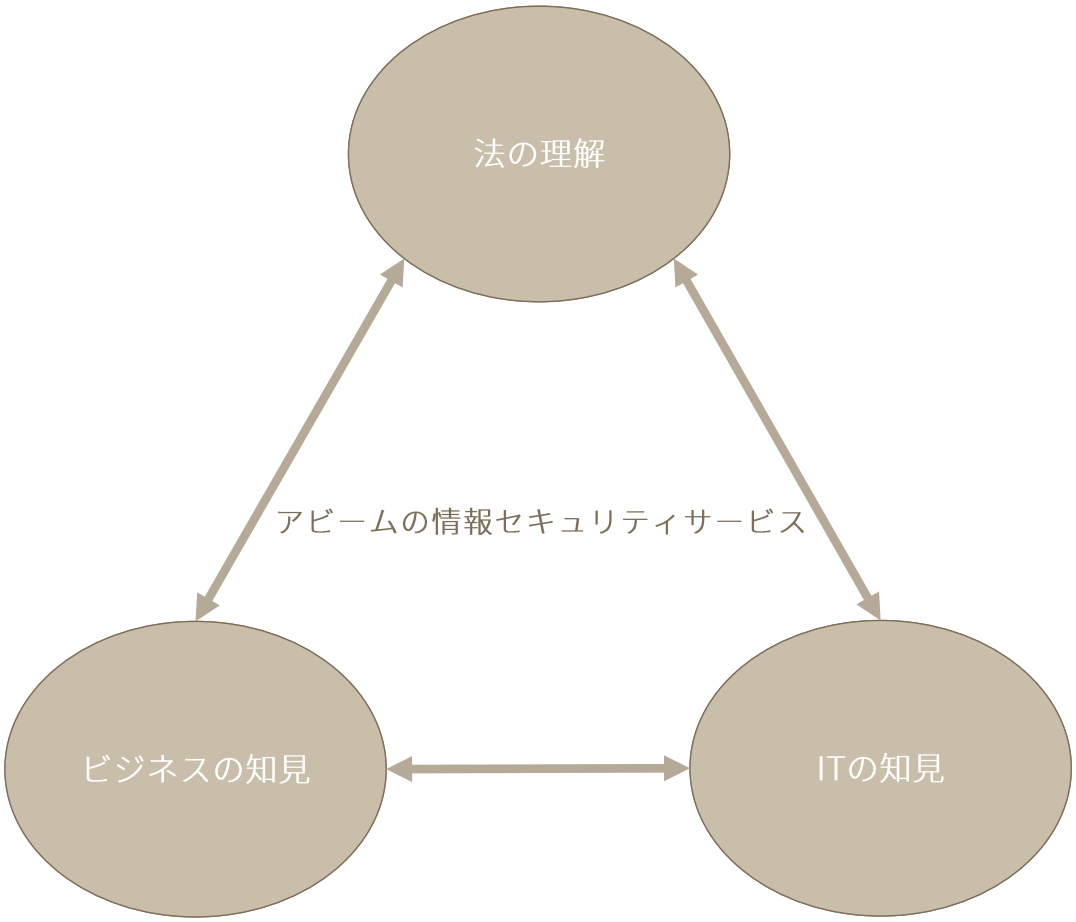
デジタル社会でのリスク管理：アビームコンサルティングの役割とソリューション

現代のデジタル社会において、サイバーセキュリティと個人情報保護は極めて重要な課題となっている。インターネットの普及とともに、私たちの生活はますますオンラインに依存するようになり、個人情報の取り扱いも増加している。このような状況下で、サイバー攻撃やデータ漏洩のリスクは高まり続けており、各国政府はこれに対処するための法規制を強化している。

中国も例外ではなく、在中国企業は関連法への適切な対応が必要である。しかし、法律やガイドラインは随時補足、具体化されており、一企業の内部リソースのみで適切に追随していくことは難しい。

当社はグローバル総合コンサルティングファームとして、各国の法要件の理解はもとより、それを企業に実装するためのビジネス・ITについても豊富な知見を有している。これらのケイパビリティを活かして、当社は在中国日系企業に対してクラインとの中国サイバーセキュリティ法対応における「現状調査」「あるべき姿の検討」「法対応の実行」「継続サポート」の支援ソリューションを提供している。当局への届け出申請や当局との連携、専門家への連携など、複雑なコミュニケーションもワンストップで対応可能である。

サイバーセキュリティや個人情報保護の法対応についても、当社は引き続き在中国企業の成長を支援していく。



アビームコンサルティングについて

アビームコンサルティングは、アジアを中心とした海外ネットワークを通じ、それぞれの国や地域に即したグローバル・サービスを提供している総合マネジメントコンサルティングファームです。戦略、BPR、IT、組織・人事、アウトソーシングなどの専門知識と、豊富な経験を持つ約8,800名のプロフェッショナルを有し、金融、製造、流通、エネルギー、情報通信、パブリックなどの分野を担う企業、組織に対し幅広いコンサルティングサービスを提供しています。アビームコンサルティングは、企業や組織とともに新たな未来を共創し、確かな変革に導く創造的パートナーとして、企業や社会の変革に貢献します。

中国市場においては、2003年の初進出以来、20年以上にわたり実績を積み重ねてまいりました。現在では、上海、深セン、西安、大連、中国香港、中国台湾などに拠点を展開しており、2024年7月時点で中国国内の従業員数は1,100名を超えています。

本レポートにご関心をお持ちの企業様は、ぜひお気軽にご相談ください。貴社のビジネストランスフォーメーションを、私たちが全力でご支援いたします。

ABeam Consulting China

地址：上海市浦東新区陸家嘴環路479号71階

TEL：+86-21-3303-9510

著者

小澤 繁樹　　Ozawa　Shigeki

本レポートの利用についての注意・免責事項

本レポートは、2025 年3月に入手した情報に基づくものであり、その後の法律改正などにより、記載内容が古くなっている可能性があります。また、本レポートは法律専門家ではない立場で当社が作成したものです。入手した情報の制限、解釈の相違、またはその他の客観的な制約により、内容的な欠落または誤りが生じる可能性があります。したがって、本レポートはあくまで参考情報としてご活用ください。当社はその完全性・正確性について一切の責任を負いません。また、本レポートはいかなる法的助言を構成するものでもなく、法的助言の根拠となるものでもありません。本レポートに記載された情報に基づいて何らかの行動を取られる場合は、必ず実際の状況を踏まえ、専門の法律事務所等にご相談ください。

本レポートまたはその内容に起因し、またはそれに関連して生じたあらゆる損害(直接的、間接的、付随的、懲罰的損害および逸失利益その他を含むがこれに限らない)について、契約責任、制定法責任、不法行為責任(過失責任を含む)のいずれに基づく責任であっても、また、予見できた、または予見できたか否かを問わず、当社は一切の責任を負わないものとします。


ABeam Consulting®
Build Beyond As One.