JETRO
日本貿易振興機構（ジェトロ）

「サイバーセキュリティ法（2025 年改正）」および「国家サイバーセキュリティインシデント報告管理弁法」の要点整理と対応策

～中国のデータ三法に関する制度情報 専門家による政策解説～

2026 年 2 月

日本貿易振興機構（ジェトロ）
北京事務所
調査部

【免責条項】

本レポートは、北京金誠同達法律事務所に委託し、作成したものです。
本レポートで提供している情報は、ご利用される方のご判断・責任においてご使用下さい。ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用される方が不利益等を被る事態が生じたとしても、ジェトロおよび執筆者は一切の責任を負いかねますので、ご了承下さい。

1. 背景

2025 年 10 月 28 日、第十四期全国人民代表大会常務委員会第 18 回会議において、改正後の「中華人民共和国サイバーセキュリティ法」（中華人民共和国主席令第 61 号、以下「**サイバーセキュリティ法**」という。）が可決され、2026 年 1 月 1 日より施行された[1]。本回改正は、「サイバーセキュリティ法」が 2017 年 6 月 1 日に正式に施行されて以降、初の全面的な改正となる。改正内容は、主として「サイバーセキュリティ法」と他の関連法令との整合性の強化およびサイバーセキュリティに関する違法行為に対する責任の強化に重点が置かれている。

また、「サイバーセキュリティ法」「データセキュリティ法」および「個人情報保護法」等の法令においてサイバーセキュリティインシデント発生時の報告義務を具体化するため、国家インターネット情報弁公室は 2025 年 9 月に「国家サイバーセキュリティインシデント報告管理弁法」（以下「**弁法**」という。）を公布し、同弁法は 2025 年 11 月 1 日より施行されている[2]。「弁法」は、サイバーセキュリティインシデントの報告主体、報告手続、報告期限、報告内容および監督管理上の責務等について、いずれも詳細な規定を設けている。

本レポートでは、「サイバーセキュリティ法」および「弁法」の関連情報を整理・解説する。これを踏まえ、実務上の対応経験と照らして、日系企業に対する今後の対応方法について解説する。

2.「サイバーセキュリティ法」の要点解説

2.1 AI の発展に伴う需要への対応

「サイバーセキュリティ法」第 20 条に「人工知能（AI）条項」が新たに設けられ、法律上で初めて AI の安全および発展に関する原則的な規定が明確化された。同条項では、国家は AI の基礎理論研究およびアルゴリズム等の重要技術の開発を支援し、データ資源や計算能力等の基盤施設の整備を推進し、AI の倫理規範を整備し、リスクの監視評価および安全監督を強化し、AI の応用および健全な発展を促進すると明確に規定している。本規定は法律上の原則的な規定であり、日系企業を含む多くの企業にとって、直接的な法的義務を構成するものではないが、今後の AI 産業の発展に対しては顕著な指導的意義を有し、立法者が AI 産業を重視していることを示している。

2.2 関連法令との整合性強化

「サイバーセキュリティ法」第 4 章では「ネットワーク情報のセキュリティ」に関する内容が規定されており、ネットワーク情報の内容の管理だけでなく、個人情報の保護も含まれる。個人情報保護に関する法定義務について、第 42 条は次のように規定している。「ネットワーク運営者が個人情報を取り扱う場合、本法および『中華人民共和国民法典』、『中華人民共和国個人情報保護法』等の法律・行政法規を遵守しなければならない。」個人情報保護に関する法的責任について、第 71 条は次のように規定している。「次の各号のいずれかの行為があった場合、関連法律・行政法規の規定に基づき処理・処罰する：（二）本法第 24 条第 3 項、第 43 条から第 45 条の規定に違反し、個人情報の権益を侵害した場合」これらの条項を通じて、企業は「サイバーセキュリティ法」を遵守するだけでなく、

[1] 全国人大網： http://www.npc.gov.cn/npc/c2/c30834/202510/t20251028_449048.html
[2] 国家インターネット情報弁公室：https://www.cac.gov.cn/2025-09/15/c_1759583017717009.htm

「個人情報保護法」や「ネットワークデータセキュリティ管理条例」等の法律・法規に従って個人情報の取り扱いを行うことが明確化されている。

そのため、「サイバーセキュリティ法」の規定を適用する際には、同法と他の法律との整合性にも注意する必要がある。例えば、ネットワーク運営者が個人情報を収集・利用する場合、「サイバーセキュリティ法」第 43 条に規定される「合法、正当、必要という原則を遵守し、収集・使用規則を公開し、情報を収集・使用する目的・方式と範囲を明示し、被収集者の同意を得なければならない」という原則的規定を遵守するとともに、「個人情報保護法」や「ネットワークデータセキュリティ管理条例」等の法律・法規と照らし合わせ、例外規定の有無等を確認する必要がある。

2.3 法的責任の整備および強化

「サイバーセキュリティ法」の今回改正の特徴は、法的責任制度の整備および強化にあり、罰則の種類が新たに追加され（例えば通報、アプリケーションの停止等）、過料額が引き上げられた点である。さらに、「他の直接の責任者」を処罰対象者の範囲に含め、「個人情報保護法」および「データセキュリティ法」と整合させ、いわゆる「両罰制」を採用しており、直接の責任を負う主管者および他の直接の責任者（以下「**関連責任者**」という。）は、規定に基づき過料を科される可能性がある。

注目すべき点は、今回の改正が「寛厳併済（寛大な措置と厳格な措置の併用）」の方式を採用しており、行政処罰責任を一方的に重くするものではなく、明らかに軽微な行為については減免措置も規定されていることである。「サイバーセキュリティ法」第 73 条では、「行政処罰法」に規定される情状により軽減、減刑または処罰しない場合には、当該規定に従い軽減、減刑または処罰しないと定められ、同規定は「行政処罰法」第 32 条、第 33 条[3]の規定と一致している。法的責任に関する重点的な新設条項および変更点は以下の通りである。

2.3.1 サイバーセキュリティ保護義務の不履行

「サイバーセキュリティ法」第 61 条は、サイバーセキュリティ保護義務に関する法的責任を強化しており、ネットワーク運営者の一般義務および重要情報インフラ運営者（以下「CIIO」という）の特別義務を含む。一般義務は、「サイバーセキュリティ法」第 23 条に規定されるネットワークセキュリティ等級保護制度および第 27 条に規定されるサイバーセキュリティインシデントの緊急対応計画・報告制度に対応している。特別義務は、「サイバーセキュリティ法」第 35 条、第 36 条、第 38 条および第 40 条に対応する。

同時に、同条は「三段階の階梯型罰則」を採用しており、改正前は、是正を拒否した場合やサイバーセキュリティに危害を及ぼす結果を招いた場合にのみ、過料が科されてい

---

[3] 全国人大網：http://www.npc.gov.cn/c2/c30834/202101/t20210122_309857.html
「行政処罰法」第 32 条 当事者に以下に記載する情状の 1 つがある場合、行政処罰をできるだけ軽くするかまたは軽減しなければならない。
（一）自発的に違法行為による危害結果を除去し、または軽減させた場合
（二）他人の脅迫を受け、または騙されて違法行為をした場合
（三）行政機関がまだ把握していない違法行為を自発的に供述した場合
（四）行政機関の違法行為取締に協力し、功績を上げた場合
（五）法律、法規、規則において、その他の行政処罰を軽くしまたは軽減すべき旨の規定がある場合
「行政処罰法」第 33 条　違法行為の情状が軽くかつ直ちに是正された結果、危害を生じさせなかった場合、行政処罰を与えない。初回の違法行為であり、かつその結果としての危害が軽いものであり、直ちに是正された場合、行政処罰を与えないことができる。
当事者に主観的な過失がないことを証明する十分な証拠がある場合、行政処罰を与えない。法律、行政法規に別途規定がある場合はその規定に従う。

た。改正後は、違法行為がある場合はいずれも過料が科され、是正を拒否した場合やサイバーセキュリティに危害を及ぼす結果を招いた場合には、過料が倍増される。同時に、第3 項で規定される「サイバーセキュリティに深刻な危害を及ぼす結果」（主に大量のデータ漏えい、重要情報基盤の一部機能喪失等の状況を指す）を引き起こした場合、関連責任者は最高 100 万元、企業は最高 1,000 万元の処罰を受ける可能性がある。

2.3.2 安全なネットワーク製品およびサービスの提供義務の不履行

「サイバーセキュリティ法」第 62 条は、安全なネットワーク製品・サービスおよび電子情報並びにアプリケーションソフトウェアの提供義務の不履行に関する法的責任を規定しており、第 24 条に規定されるネットワーク製品・サービス提供者の義務および第 50 条に規定される電子情報・アプリケーションソフトウェア運営者の情報セキュリティ要件を含む。注目すべき点は、同条に新たな法的責任項目が追加され、第 2 項として「前項の第 1 号、第 2 号の行為により、本法第 61 条第 3 項で規定される結果を招いた場合は、当該項の規定に従い処罰する」と規定されている。従来の規定と比較して、過料の上限が大幅に引き上げられ、処罰対象者の範囲も拡大された。すなわち、安全なネットワーク製品およびサービスの提供義務を履行しなかった場合、直接の責任を負っていた主管者だけでなく、関連責任者も処罰対象となり得る。

2.3.3 ネットワーク重要設備およびサイバーセキュリティ専用製品の認証義務の不履行

「サイバーセキュリティ法」第 25 条は、ネットワーク重要設備やネットワーク専用製品等の安全認証および安全検査制度を規定しており、改正後の「サイバーセキュリティ法」は第 63 条で相応の法的責任を追加し、「違法所得を没収する」および「過料を併科する」と規定するとともに、「関連業務の一時停止、操業停止、関連の業務許可証または営業許可証を取り消すこと」といった処罰手段も追加された。

2.3.4 セキュリティホールの管理義務の不履行

「サイバーセキュリティ法」第 28 条は、サイバーセキュリティの管理義務を規定しており、今回の改正では第 65 条において従来の法的責任が強化された。同条もまた「三段階の階梯型罰則」を採用しており、関連責任者を処罰対象に含めている。違法行為があれば過料が科され、「是正を拒否した場合または情状が深刻である場合」の過料額も引き上げられ、最高で企業に対して 100 万元、関係する個人に対して 10 万元の過料が科される。同時に、「ウェブサイトの閉鎖」という処罰を「ウェブサイトまたはアプリケーションの閉鎖」に調整し、第 61 条第 3 項に規定される「サイバーセキュリティに深刻な危害を及ぼす結果」を過料倍増の対象事例とした。

2.4 海外適用効力の拡大

「サイバーセキュリティ法」第 77 条の規定によれば、中国のサイバーセキュリティに危害を及ぼす場合、関連主管部門は海外の機関・組織・個人に対して法に基づき法的責任を追及する権限を有し、深刻な結果を生じた場合には、関連部門は財産の凍結や他の必要な制裁措置を同時に取ることができる。本改正後は、従前のように海外機関が中国の重要情報インフラに危害を及ぼすことや「深刻な結果」を生じさせることを要件としておらず、海外適用の効力範囲が拡大されている。

3.「国家サイバーセキュリティインシデント報告管理弁法」の要点解説

3.1 適用範囲

「弁法」第 1 条および第 12 条は、適用主体を規定しており、中華人民共和国国内でネットワークを構築・運営する、またはネットワークを通じてサービスを提供するネットワーク運営者を含む。「サイバーセキュリティ法」第 78 条第 3 項によれば、ネットワーク運営者とは、ネットワークの所有者、管理者およびネットワークサービス提供者を指す。

「弁法」第 12 条は同時にサイバーセキュリティインシデントの定義を規定しており、人為的要因、ネットワークへの攻撃、ネットワークの不備や欠陥、ソフトウェア・ハードウェアの欠陥や故障、不可抗力等の要因により、ネットワークおよび情報システム、またはそのデータ・業務アプリケーションに危害を及ぼし、国家・社会・経済に負の影響を与えるインシデントを指す。サイバーセキュリティインシデントの識別方法については、下記のサイバーセキュリティインシデント報告フローにおける階層別解説を参照することができる。

3.2 報告のフロー

3.2.1 等級別判断

サイバーセキュリティインシデントが発生した後、関係主管部門へ報告すべきかとうかを判断するに先立ち、まず当該サイバーセキュリティインシデントのレベルを判定し、「特別重大サイバーセキュリティインシデント」「重大なサイバーセキュリティインシデント」「比較的重大なサイバーセキュリティインシデント」または「一般的なサイバーセキュリティインシデント」のいずれに該当するかを確定する必要がある。「弁法」第 4 条によれば、報告が求められるのは「比較的重大」およびそれ以上のレベルに該当するサイバーセキュリティインシデントに限られ、「一般サイバーセキュリティインシデント」は報告対象外とされている。「弁法」の別紙である「ネットワークセキュリティインシデント等級分類ガイドライン」の規定に基づき、企業に関連する「比較的重大」およびそれ以上のサイバーセキュリティインシデントの判定基準は以下のとおりである。

判定の要素	特に重大	重大	比較的重大
重要情報インフラの動作	全体が 6 時間以上、または主要機能が 24 時間以上停止する	全体が 1 時間以上、または主要機能が 3 時間以上停止する	全体が 30 分以上、または主要機能が 2 時間以上停止する
コアデータ、重要データが窃取、改ざん、偽造されること	国家安全保障および社会の安定に特に深刻な脅威をもたらした場合	国家安全保障および社会の安定に深刻な脅威を与えた場合	国家安全保障および社会の安定に比較的深刻な脅威を与えた場合
個人情報の漏洩	1 億人以上	1,000 万人以上	100 万人以上
ポータルサイト、重点ニュースサイト、超大型ネットワークプラットフォームなどに	省級以上の党・政府機関ポータルサイト、中央重点ニュースサイト、超大型ネットワークプラットフォームなどが攻撃・改ざんされ、	地方自治体以上の党・政府機関、企業・団体のポータルサイト、省級以上の重点ニュースサイト、大規模以上のネットワークプラットフォーム	党・政府機関、企業・団体のポータルサイト、主要ニュースサイト、ネットワークプラットフォーム等が攻撃・改ざんされ、違法

おいて違法有害情報が拡散した場合	違法有害情報が特大範囲で拡散した場合。以下のいずれかに該当する場合、「特大範囲」と認定される： （1）ホームページに表示され 6 時間以上継続、または他のページに表示され 24 時間以上継続した場合； （2）ソーシャルプラットフォームで 10 万回以上転送された場合； （3）閲覧またはクリック数が 100 万回を超えた場合； （4）省級以上のネット情報部門・公安機関が「特に広範囲な拡散」と認定した場合。	等が攻撃・改ざんされ、違法有害情報が広範囲に拡散した場合。以下のいずれかに該当する場合、「広範囲」と認定される： （1）ホームページに表示され 2 時間以上継続、または他のページに表示され 12 時間以上継続した場合； （2）ソーシャルプラットフォームで 1 万回以上転送された場合； （3）閲覧またはクリック数が 10 万回以上の場合； （4）省級以上のネット情報部門・公安機関が「広範囲に拡散」と認定した場合。	有害情報が広範囲に拡散した場合。以下のいずれかに該当する場合、「広範囲」と認定される：（1）ホームページに表示され 30 分以上継続、または他のページに表示され 2 時間以上継続した場合； （2）ソーシャルプラットフォームで 1,000 回以上転送された場合； （3）閲覧またはクリック数が 1 万回以上の場合； （4）省級以上のネット情報部門・公安機関が「広範囲に拡散」と認定した場合。
直接的経済損失	1 億元以上	2,000 万元以上	500 万元以上

3.2.2 報告主管部門および報告期限

主体	報告先の部門	報告の期限
重要情報インフラ運営者	【比較的重大なサイバーセキュリティインシデント】 ・自社の保護業務部門[4] ・公安機関	直ちに、遅くとも 1 時間以内
	【重大および特に重大なサイバーセキュリティインシデント】 ・自社の保護業務部門 ・国家サイバーセキュリティ部門 ・国務院公安部門	直ちに、遅くとも 30 分以内
中央および国家機関の各部門およびその直属機関	【比較的重大なサイバーセキュリティインシデント】 ・当該部門のネット情報管理機関	速やかに、遅くとも 2 時間以内
	【重大および特に重大なサイバーセキュリティインシデント】 ・当該部門のネット情報管理機関	速やかに、遅くとも 1 時間以内

[4] 保護業務部門は、重要情報インフラ運営者の所属する業界・分野の主管部門を指す。

	・国家ネット情報部門	
他のネットワーク運営者	【比較的重大なサイバーセキュリティインシデント】 ・管轄の省級サイバーセキュリティ部門	速やかに、遅くとも 4 時間以内
	【重大および特に重大なサイバーセキュリティインシデント】 ・管轄の省級サイバーセキュリティ部門 ・省級サイバーセキュリティ部門は、ただちに国家サイバーセキュリティ部門に報告し、同時に同レベルの関連部門に通報する	遅くとも 1 時間以内

「弁法」第 4 条第 5 項の規定によると、当該業界分野に別途規定がある場合、ネットワーク運営者は業界主管監督部門の要求に従い報告しなければならない。違法犯罪の疑いがある場合、ネットワーク運営者は速やかに公安機関に通報しなければならない。

3.2.3 報告経路

サイバーセキュリティ部門は、以下の 6 種類のサイバーセキュリティインシデント報告経路を開設している。

- 12387 サイバーセキュリティインシデント報告ホットラインに電話し、音声案内に従って報告する。
- サイバーセキュリティインシデント報告公式サイト 12387.cert.org.cn にアクセスして報告する。
- WeChat で「12387」ミニプログラムを検索し、ホーム画面から「事件報告」をクリックする。
- 「国家インターネット緊急対応センターCNCERT」公式 WeChat アカウントをフォローし、「事件報告」をクリックする。
- 電子メールで 12387@cert.org.cn に報告する。
- ファックス（010-82992387）で報告する。

3.2.4 報告内容

ネットワークセキュリティインシデントを報告する際には、以下の内容を含めるものとする。

（一）関係機関の名称および関係システムまたは施設の基本状況。

（二）ネットワークセキュリティインシデントの発見または発生日時、場所、種類、レベル、既に生じた影響と危害、既に講じた措置およびその効果。ランサムウェア攻撃事件については、身代金支払いの要求金額、方法、日付等も含むものとする。

（三）事態の進展傾向および引き起こす可能性のあるさらなる影響と危害。

（四）サイバーセキュリティインシデントの原因に関する予備的分析意見。

（五）攻撃源調査の手がかり（可能性のある攻撃者情報、攻撃経路、存在する脆弱性等を含むがこれらに限定されない）。

（六）今後講じる予定の対応措置および支援要請事項。

（七）サイバーセキュリティインシデント現場の保護状況。

（八）その他報告すべき状況。

規定時間内に発生原因、影響、発展傾向等を判定できないサイバーセキュリティインシデントについては、まず第一項（関係機関の名称および関係システムまたは施設の基本状況）および第二項（ネットワークセキュリティインシデントの発見または発生日時、場所、種類、レベル、既に生じた影響と危害、既に講じた措置およびその効果。ランサムウェア攻撃事件については、身代金支払いの要求金額、方法、日付等も含むものとする）の内容を報告し、その他の状況は 72 時間以内に追加報告する。具体的な報告内容は、本レポートの別紙 1「サイバーセキュリティインシデント報告書」を参照できる。

上記（二）の「種類」については、国家標準「情報セキュリティ技術 サイバーセキュリティインシデントの等級分類ガイドライン（GB/T 20986-2023）」に基づき判定することができる。

3.2.5 インシデント対応総括報告書

「弁法」第 8 条によると、インシデントの対応作業終了後、ネットワーク運営者は 30 日以内に、インシデントについて包括的な分析・総括を行い、インシデント対応総括報告書を作成し、元の報告経路を通じて提出しなければならない。

3.3 法的責任

国家インターネット情報弁公室が開催した記者会見によれば[5]，今回公布された「弁法」は、サイバーセキュリティインシデント報告フローの要件を明確化する規定として、「サイバーセキュリティ法」等関連法に規定されるサイバーセキュリティインシデント報告義務を補完する下位法として位置付けられる。具体的には、改正後の「サイバーセキュリティ法」第 27 条[6]、「データセキュリティ法」第 29 条[7]、「個人情報保護法」第 57 条[8]等の法令を参照できる。

また、サイバーセキュリティインシデント報告義務に関する違法責任について、 「両罰制」を採用しており、違法企業、直接の責任を負っていた主管者および関連責任者に対して処罰を行う。

注目すべき点は、「弁法」が「寛厳併済（寛大な措置と厳格な措置の併用）」の方式を採用しており、法的責任の軽減事由を規定している。第 11 条によると、ネットワーク運営者が合理的かつ必要な防護措置を講じ、緊急対応計画に基づき処理を行い、インシデントの影響および危害を効果的に軽減し、かつ本弁法に基づき適時に報告した場合、状況に応じて関連機関および関係者の責任を軽減または免除することができる。

4. 日系企業への対応策の提言

前述の「サイバーセキュリティ法」および「国家サイバーセキュリティインシデント報告管理弁法」の要点整理に基づき、かつ実務上の具体的な状況を踏まえ、以下の対応策をまとめる。

---

[5] 国家インターネット情報弁公室：「国家サイバーセキュリティインシデント報告管理弁法」に関する記者会見：https://www.cac.gov.cn/2025-09/15/c_1759583021718167.htm。

[6] 「サイバーセキュリティ法」第 27 条　ネットワーク運営者は、サイバーセキュリティを侵害するインシデントが発生した場合、規定に従い関係主管部門に報告する必要がある。

[7] 「データセキュリティ法」第 29 条　データセキュリティインシデントが発生した場合、規定に基づいて適時にユーザーに告知し、かつ関連主管部門に報告しなければならない。

[8] 「個人情報保護法」第 57 条　個人情報の漏えい・改ざん・紛失が既に発生しており、または今後発生するおそれのあるときは、個人情報の取扱者は、救済措置を直ちに実施し、個人情報保護の職責を履行する政府機関および個人に通知しなければならない。

4.1「サイバーセキュリティ法」に基づく未履行義務のリストの整理と速やかな是正

2026 年 1 月 1 日に改正された「サイバーセキュリティ法」は、法的責任の面で大幅に強化されており、特に処罰の適用場面の拡大、過料上限の引き上げ、および関連責任者への処罰の強化が行われている。これを踏まえ、日系企業には、新改正「サイバーセキュリティ法」の関連規定に従い、現時点で未履行または未完了の法的義務のリストを整理し、当該リストに基づき企業が直面する法的リスクを速やかに評価し、対応すべき是正措置を早急に完了することを強く推奨する。

4.2 サイバーセキュリティ等級保護制度の早急な整備

「サイバーセキュリティ法」で規定されたサイバーセキュリティ等級保護制度は、今回の改正により変更されておらず、むしろ、同法に定められた義務を履行していない場合の法的責任は強化されている。現時点の実務状況を見ると、日系企業を含む多くの企業は、「サイバーセキュリティ法」の規定に従い、サイバーセキュリティ等級保護制度を実施・運用しておらず、相応の法的リスクが存在する。新法の正式施行に伴い、未履行の法的義務に対する行政執行はさらに厳格化されると考えられる。したがって、社内の関連情報システムに対してサイバーセキュリティ等級保護制度をまだ整備していない日系企業は、高額な処罰を回避するため、早急にサイバーセキュリティ等級保護等のサイバーセキュリティ関連義務を履行し、主要システムの等級保護のレベルの判定および届出を完了することを推奨する。

4.3 サイバーセキュリティインシデントの緊急対応体制の構築および定期的演習

「弁法」における各レベルのサイバーセキュリティインシデントの認定基準を見ると、日系企業は、取り扱う重要データや個人情報の範囲が限られているため、「比較的重大」およびその以上のサイバーセキュリティインシデントが発生し、関係主管部門への報告が必要となる可能性は高くないものと考えられる。しかし一方で、「サイバーセキュリティ法」第 27 条[9]、「データセキュリティ法」第 29 条[10]および「個人情報保護法」第 57 条[11]では、企業は突発的なサイバーセキュリティインシデントに対応するため、事前にサイバーセキュリティインシデントの緊急対応計画を策定し、当該計画に基づき定期的に演

---

[9] 「サイバーセキュリティ法」第 27 条　通信事業者はサイバーセキュリティインシデントの緊急対策案を制定し、システムの脆弱性、コンピュータウイルス、サイバー攻撃、ネットワーク侵入などのセキュリティリスクを速やかに処理しなければならない。サイバーセキュリティに危害を加える事件の発生時には、即座に緊急対策案を始動し、相応の救済措置を講じ、規定に基づいて関連主管部門に報告しなければならない。

[10] 「データセキュリティ法」第 29 条 データ取扱活動を行うときにはリスクのモニタリングを強化しなければならず、データセキュリティ上の欠陥や不備等のリスクを発見した場合には直ちに補完措置を講じなければならず、データセキュリティインシデントが発生した場合には直ちに補完措置を講じ、規定に基づいて適時にユーザーに告知し、かつ関連主管部門に報告しなければならない。

[11] 「個人情報保護法」第 57 条 個人情報の漏えい・改ざん・紛失が既に発生しており、または今後発生するおそれのあるときは、個人情報の取扱者は、救済措置を直ちに採択し、個人情報保護の職責を履行する政府機関および個人に通知しなければならない。通知には、次の各号に掲げる事項が含まれていなければならない。

（一）個人情報の漏えい・改ざん・紛失が既に発生しており、または今後発生するおそれのある情報の種類・原因、およびもたらされるおそれのある危険

（二）個人情報の取扱者が実施した救済措置、および個人が実施することのできる危険軽減措置

（三）個人情報の取扱者の連絡方法

個人情報取扱者による措置の実施によって、情報の漏えい・改ざん・紛失によりもたらされる危険を有効に回避することができたときは、個人情報の取扱者は、個人への通知を行わないことができる。個人情報保護職責履行部門は、危険がもたらされるおそれのあるものと考えたときは、個人への通知を個人情報の取扱者に要求することができる。

習を実施することが求められており、インシデント発生時の対応能力の向上を図る必要がある。これを踏まえ、在中国日系企業は、自社の実情に応じて社内のサイバーセキュリティインシデント緊急対応計画を適時更新・整備し、定期的（少なくとも年 1 回）に緊急対応演習を実施するとともに、主管部門による随時の確認に備えて、当該演習に関する関連資料や記録を保存することを推奨する。

4.4 社内における関連管理制度の整備、従業員への教育の強化、サイバーセキュリティおよびデータコンプライアンス意識の浸透

このほか、以下の措置を取ることを推奨する。

- 「サイバーセキュリティ法」および「弁法」等関連法規の要件に照らし、社内の関連管理制度を整備する。
- サイバーセキュリティおよびデータコンプライアンスに関する従業員への教育を強化する。
- 従業員に対して関連管理制度、サイバーセキュリティインシデント緊急対応計画および報告フローを学習させるとともに、日常的かつ実践的な演習を実施し、形式的にならないようにし、セキュリティインシデント発生時に効果的に対応できることを確保する。
- 従業員への教育の際には、サイバーセキュリティおよびデータコンプライアンスの理念を浸透させることに重点を置き、企業のサイバーセキュリティおよびデータコンプライアンス水準の根本的な向上を図る。

別紙 1[12]

サイバーセキュリティインシデント報告書

<table>
<tr><td colspan="2">*[13]会社名</td><td></td><td>*インシデント
発生場所</td><td></td></tr>
<tr><td colspan="2">*サイバーセキュリティ
担当者および電話番号</td><td></td><td>会社の FAX 番号</td><td></td></tr>
<tr><td rowspan="6">*サイバーセキュリティインシデント初期判定状況</td><td>*初期判定インシデントタイプ</td><td colspan="3">□悪意のあるプログラム　□サイバー攻撃
□データセキュリティ　□設備・施設の故障
□規則違反操作　□セキュリティ上の潜在リスク
□異常インシデント　□不可抗力インシデント
□他のインシデント</td></tr>
<tr><td>*初期判定インシデントレベル</td><td colspan="3">□特に重大　□重大　□比較的重大　□一般　□その他</td></tr>
<tr><td>判定根拠</td><td colspan="3">（具体的には、「サイバーセキュリティインシデント報告管理弁法」別紙「サイバーセキュリティインシデント等級分類ガイドライン」の条項内容を列挙）</td></tr>
<tr><td>*インシデント発生組織およびインシデント発生施設の基本状況</td><td colspan="3">（インシデント発生組織のネットワークおよび情報システムの機能、ならびに関連するネットワーク構成状況等を記入すること）</td></tr>
<tr><td>*発生日時・場所および事態の経過概要</td><td colspan="3"></td></tr>
<tr><td>*インシデントによる影響および被害</td><td colspan="3">（インシデントによって既に生じた影響および被害を記入すること。影響の程度、影響を受けた人数、経済的損失等を含む。ランサムウェア攻撃インシデントの場合は、要求された身代金の金額、支払い方法、日付等も記入すること）</td></tr>
<tr><td>既に講じた措置およびその効果</td><td colspan="3"></td></tr>
</table>

[12] この表は、WeChat ミニプログラム「12387」内の「我要報告（報告する）」コーナーにある「サイバーセキュリティインシデント報告表」を参照して作成。

[13] 「*」の付いた項目は記入必須。

サイバーセキュリティインシデントのさらなる判定状況[14]	インシデント発生の初期判定原因	
	事態の進展傾向および今後生じ得る影響・被害	（インシデントによって既に生じた影響および被害を記入すること。影響の程度、影響を受けた人数、経済的損失等を含む）
	その他補足内容	（1. 原因究明調査の手がかり、攻撃者の可能性情報、攻撃経路、存在する脆弱性等を含むがこれに限らない；2. 今後予定している対応措置および支援要請事項；3. サイバーセキュリティインシデント現場の保全状況；4. その他報告すべき事項）
	別紙	

[14] 発生から 4 時間以内に判定できない場合、初回報告後 72 時間以内に追加報告する必要がある。

レポートをご覧いただいた後、アンケート（所要時間：約 1 分）にご協力ください。
https://www.jetro.go.jp/form5/pub/ora2/20250045

本レポートに関するお問い合わせ先：
日本貿易振興機構（ジェトロ）
調査部 中国北アジア課
〒107-6006 東京都港区赤坂 1－12－32
TEL：03-3582-5181
E-mail：ORG@jetro.go.jp