2024.3.1

中国風険消息〈中国関連リスクニュース〉 <2024 No.4>

中国「情報セキュリティ等級保護」制度と当社における対応事例の紹介

【要点】
- ◆ 「情報セキュリティ等級保護」制度の概要、導入までの背景、認証取得の対応フロー、セキュリティ要件、処罰事例について説明する。
- ◆ 当社が準備を開始してから、認証を取得するまでの経緯を紹介する。
- ◆ 当社における対応事例をもとに、当事者の視点からみた等級保護対応のポイントを説明する。

1.「情報セキュリティ等級保護」制度の概要

(1)制度の概念

中国政府が推進する情報セキュリティ等級保護制度(以降、「等級保護」)は、国家秘密情報、国民・法人・その他組織に関連する固有情報や公開情報、これらの情報を保管・伝送・処理する情報システムについて等級分類を行い、その程度に応じて企業等にセキュリティ対応を促すものである。企業は、自社が該当する等級をふまえたセキュリティ管理を徹底し、情報セキュリティインシデント（情報セキュリティに関する事故・事件）にも適切に対応できるよう各種の準備を行うことが求められる。

(2)導入までの背景

等級保護に関する重要政策の推移は図表 1 のとおりである。2016 年にサイバーセキュリティ法が発布されて以降、等級保護に関する政府部門の検査・監督は大幅に強化されている。

図表 1　重要政策の推移（等級保護）

1994 年 等級保護（概念）導入	「中華人民共和国コンピュータ情報システムセキュリティ保護条例」にて、「システム・データの等級保護」という概念が提起された。
1999 年 対応基準公表	「コンピュータ情報システムセキュリティ保護等級分類ガイドライン」にて、等級分類の原則・基準が整備された。また、セキュリティ保護の技術的対策・管理的対策が規定された。
2007 年 管理方法公表	「情報セキュリティ等級保護管理弁法」にて、等級保護実施の具体的方案・管理機構が規定された。また、政府や企業の責任・義務が明確化された。
2016 年 等級保護関連法律成立	サイバー空間の安全性、情報セキュリティの確保を目的として、「サイバーセキュリティ法」が制定され、情報インフラ保護が強化された。
2019 年 等級保護 2.0 基準公表	「基本要件、設計要件、評価要件」の枠組みを統一した規格が公表され、クラウドコンピューティング、IoT にまで対象範囲が拡大された。

(3)等級分類の考え方

企業が有する各種情報・システムの等級は、万が一システムがハッカーに改ざんされるなどした場合の「損害対象（誰が損害を受けるか）」「損害程度（どの程度損害を受けるか）」の 2 つの要素より決定される。等級分類の判断指標は、図表 2 のとおりである。

図表 2　等級分類の判断指標

損害対象＼損害程度	一般的な損害	重大な損害	特に重大な損害
公民、法人およびその他の組織の合法的な権益	1 級	2 級	2 級
社会秩序/公共利益	2 級	3 級	4 級
国家安全保障	3 級	4 級	5 級

出典：GB/T 22240-2020　信息安全技术　网络安全等级保护定级指南

なお、等級分類を行う際の「損害程度」については、定量的な要件は定められておらず、正確に自社の等級を把握することが難しいといえる。自社の等級を判断する場合は、図表 3 が参考になる。金融やインフラ系の業種を除けば、一般的な企業は 2 級（3 級）に該当するケースがほとんどである。

図表 3　等級保護の判断基準

等級	保護レベル	評価頻度	主な対象
1 級	自主保護	外部審査不要	小型私営、個人企業、小中学校、郷鎮所属の情報システム、県級単位の一般的な情報システム
2 級	指導保護	2 年に 1 回	県級のその他部門における重要な情報システム、地市級以上の国家機関・企業事業体内の一般的な情報システム(公開されているページ)
3 級	監督保護	年 1 回以上	地方市級以上の国家機関・企業・病院・大学内の重要な情報システム、大量の会員情報(10 万以上)を有するプラットフォーム等
4 級	強制保護	半年に 1 回	電力、電信、ラジオ、鉄道、民間航空、銀行、税務などの重要なシステム
5 級	制御保護	必要に応じて自主検査	軍需産業、重要な科学研究分野などの極めて重要な情報システム

出典：GB 17859-1999　计算机信息系统 安全保护等级划分准则

(4)対応フロー

国家標準（GB）では、実施主体・対象に基づき、等級保護（認証取得）の対応フロー（5 ステップ）が定められている。各ステップにおける対応は図表 4 のとおりである。

図表 4　等級保護の対応フロー

ステップ		内容
1	等級分類	自主的に情報システムのセキュリティ保護等級を確認の上、専門家・主管部門による審査を実施する。
2	届出	2 級以上の情報システムについて、公安局へ届出を行う。公安局は届出資料、等級の正確性について審査し、審査合格後に届出証明を発行する。
3	構築	セキュリティ保護等級に基づき、国家標準で定めるセキュリティの構築・是正、セキュリティ管理制度の確立・実施を徹底する。
4	評価測定	国家要求に適合する評価測定機関による等級審査を実施する（初回審査、再審査の計 2 回が必要)。
5	検査	公安局による情報システム（2 級）への指導を行う。また、3 級、4 級の場合は、定期的に監督・検査を展開する。

(5)セキュリティ要求

セキュリティ要求は、主に技術面と管理面に区分される。等級が上がるにつれて、要求項目が増え、要求レベルが高くなる。1～3 級の情報システムに求められる要求は図表 5 のとおりである。

図表 5　セキュリティ要求（技術面・管理面）

大分類	中分類	小分類
技術要求	管理センター	システム管理、監査管理、安全管理、集中管理制御
	システム環境	認証、アクセス制御、セキュリティ監査、不正コード防止 信頼性のある検証、データ整合性、侵入防止 データバックアップ回復、残留情報保護、個人情報保護 データプライバシー
	ファイアウォール	境界保護、アクセス制御、侵入防止、信頼性のある検証 不正コードおよびスパム対策、セキュリティ監査
	通信ネットワーク	ネットワークアーキテクチャ、通信転送、信頼性検証
	物理的環境	物理的な場所の選択、物理的なアクセス制御 盗難防止と破壊防止、落雷防止、防火、防湿、静電気防止 温度・湿度制御、電力供給、電磁保護
管理要求	管理制度	セキュリティポリシー、管理ルール整備・周知、レビューと改訂
	管理組織	部署設置、人員配置、授権・審査許可 コミュニケーション・協力、審査・検査
	管理者	社員の採用・退職、安全意識教育・訓練、外部人員の訪問管理
	設計監理	等級分類・届出、セキュリティルール整備、製品購買・使用 自社ソフトウェア開発、アウトソーシングソフトウェア開発 工程実施、テスト検収、システム交付、等級測定評価 ベンダー選定
	運転・保守管理	環境管理、資産管理、メディア管理、デバイス保守管理 脆弱性およびリスク管理 ネットワークおよびシステムセキュリティ管理 不正コード防止管理、構成管理、パスワード管理 バックアップ・リカバリ管理、変更管理 セキュリティインシデント処理、緊急対策管理 アウトソーシング運用管理

(6)処罰事例

サイバーセキュリティ法の施行以降、各地の公安機関による定期的な取り締まりも強化されており、図表 6 のような処罰事例も発生している。

図表 6　サイバーセキュリティ法に基づく処罰事例

事例 1	2022 年 7 月、広州警察は某企業が使用するシステムが 2 級情報システムに該当すると判断した。本件は 2021 年 7 月に公安機関へ等級保護の届出が行われていたが、届出以降も規定に基づくシステムのセキュリティ等級保護測定評価を実施しておらず、等級保護制度を十分に遵守していなかった。広東省コンピュータ情報システムセキュリティ保護条例に基づき、広州警察は同社への行政処罰を課し、期限内での是正を命じた。
事例 2	2023 年 3 月、北京市公安局は某企業が使用する OA システムがサイバー攻撃を受けていることを確認した。同社がネットワークセキュリティ保護義務を履行していなかったため、OA システムがハッキング・改ざんされたものである。サイバーセキュリティ法に基づき、当局は同社に対して警告および罰金 5 万元、ネットワークセキュリティの管理者に対して 5 千元の罰金を科し、期限内での是正を命じた。

２．当社における認証取得体験レポート（等級保護２級）

以下は、当社自身が等級保護への対応が必要であることを認識してから、2 級の認証を取得するまでの体験レポートである。全体を 4 つのステップに分け、各ステップでどういう対応を実施したか、外部業者のサポートを要したか、どの程度の費用が発生したかについても併せて説明する。

＜ステップ１＞　事前準備

実施事項	自社システムの特性に基づいて等級を自主判断し、公安局へ届出を行う。
実施主体	自社のみで対応
外注コスト	ゼロ
所要期間	1 ヶ月
具体的な対応	説明
①自社の情報システムの特性を自主評価し、等級を自主判断（1 級）	当社の社内システムは主に、財務システム、ファイルサーバ、OA システム、メールシステム、ウェブサイトである。ウェブサイトを除けばすべて内部システムである。ウェブサイトは一般公開しているが、閲覧者と双方向でやり取りする機能（掲示板機能、ネット取引等）はなく、顧客データも取扱っていない。この時点では、公安局指定の評価機関による審査を必要としない「1 級」と自己判断した。（後に誤りであることが判明）
②公安局指導を受けて等級判断を修正（1 級⇒2 級）	ほどなくして、会社所在地を管轄する公安局からサイバーセキュリティの研修会に参加するよう通知を受ける。公安局より、ウェブサイトを有する場合は、掲載内容に関わらず 2 級に該当するため、認証取得の対応を行う必要があるとの指摘を受けた。万が一、ウェブサイトがハッカーに改ざんされた場合、国家の安全や公衆の利益が侵害される可能性があることが 2 級の根拠であるらしい。研修の最後に、公安局より当社を含む研修参加各社へ、期限内に是正対応を実施せよとの通知書が発行された。
③可能な限り、自社独力での認証取得にチャレンジすることを決定	コンサル業者へ情報収集をおこない、以下情報を得た。 ・認証取得には、政府の認可を受けた測定会社への発注が必要である。 ・評価費用は等級やシステムにより異なるが 2 級の場合は 80～160 万円。 ・測定審査で不備が認められれば、評価費用とは別にネットワークファイヤーフォール等のセキュリティ製品を購入する必要があり、全体の費用は 400 万円を超えることもあり得る。 ・測定会社へ照会したところ、審査のプロセスは専門的であるため、コンサル業者の支援を受けながら進めたほうがよいとの助言を受けた。当社は、コストを最小限に抑えつつ、関連の知見を得たいと考え、まずは独力で進めることとした。（後に独力では困難であることが判明）
④公安局申請の資料を作成・提出	公安局指定の様式を用いて「信息系统安全等级保护备案表、信息系统安全等级保护定级报告（情報システム安全等級保護申請表および報告書）」を作成し、公安局窓口へ持参して提出した。書類上の不備により何度も書類を修正する必要があったこと、窓口の受付時間が午前・午後で各 2 時間しかないこともあり、正式に受理されるまで手間がかかった。受理されてから 2 週間後、公安局より認証取得に必要な登録番号が発行され、正式に評価機関への発注が可能となった。

＜ステップ２＞評価機関による審査

実施事項	評価機関による審査
実施主体	・自社 ・政府の認可を受けた測定機関（←発注が必須） ※コンサル業者の支援を受けたほうがスムーズと感じた。 （当社はこの時点では独力で対応）
外注コスト	約 40 万円（←評価機関による審査費用として必須）

所要期間	審査から審査結果レポート受領まで約 2 週間 ※審査自体は 1 日で完了
具体的な対応	説明
審査基準	当社の場合、ウェブサイトは比較的シンプル（掲示板機能やネット取引の機能はない）であることもあり、評価機関による審査は 1 日で完了した（評価機関より 2 名が来社、各々技術面と管理面を審査）。審査は減点方式であり、等級保護 2 級の合格点は 100 点満点中 70 点である。70 点未満の場合は不合格となり、是正措置を講じたのちに再審査を受けなければならない。また、審査項目はリスクに応じて高・中・低に区分されており、「高リスク」項目の不備が一つでもあれば、仮に総点数が 70 点以上でも不合格となる。
審査項目（技術面）	技術面の審査は関連する国家標準に基づいて実施される。審査項目は約 130 に及び、項目毎に具体的な証明を求められる。例えば、ウェブサイトサーバのリモートログインパスワードは 8 桁以上、大文字、小文字、数字、記号を含み、最大有効期間は 90 日であることが求められる。また、サイトでデータベースを使用する場合は、ログのバックアップ、監査、データベースのバックアップと復元対策、パスワード設定が求められる。当社のウェブサイトは自社内でなく、IT ベンダーのクラウドサーバ上に置かれているため、サーバルーム関連の審査項目の確認では、IT ベンダーへの照会も必要となった。このほか、サーバにリモートアクセスする場合のＰＣのセキュリティ対策として、パスワード設定、権限の分離、ログの記録、ウイルス対策、ウェブサイトの脆弱性スキャン等も必須要件だった。
審査項目（管理面）	管理項目の審査は国家標準をもとに実施される。審査項目毎に、該当する文書の提出が求められる。例えば、自社内におけるセキュリティ部門の設置、役割設定、文書の審査・公布、情報システムの安全設計基準の設定、ソフトウェア開発管理、システムリリース時のチェックなどに関する文書の提出が求められた。これらに対して知見のない会社にとっては、対応難易度は高いと感じられ、当社の場合は、約 60 項目の不備を指摘された。
審査結果	審査から 1 週間ほどで評価機関から審査結果の通知を受けた。約 80 の不備の指摘を受けて不合格となった。なお、評価機関からは「どのように改善すればよいか」の説明はないため、個々の項目に対して、どの程度の労力やコストをかけて改善するかの判断が難しく、等級保護に知見を有するコンサル業者の支援を受けたほうがスムーズであることがわかった。

＜ステップ３＞　不備の是正

実施事項	測定審査で指摘された不備の是正
実施主体	・自社 ・コンサル業者（←自社独力での対応に限界を感じ、支援を依頼）
外注コスト	・140 万円（セキュリティ製品の購入） ・100 万円（コンサル業者への委託料。ステップ 4 の対応を含む）
所要期間	約 2 ヵ月
具体的な対応	説明
コンサル業者への委託	この時点で、コンサル業者を選定し、支援を求めることとした。コンサル業者を起用することにより「（不合格となった）どの項目にどの程度対策を講じれば合格できるか」が明確化できたほか、ハードやソフトの改善が必要な場合に、コンサル会社が有するサーバ・セキュリティ製品を利用することができるといった利便性も感じられた。
不備の是正	「（不合格となった）どの項目にどの程度対策を講じるか」をコンサル会社と協議しながら不備の是正対応を進めた。ポイントは、合格点である 70 点をクリアするためには、必ずしも全ての不備を解消する必要はないということである。当社は、不備項目全体の中から、高リスク・中リスクに該当

	する項目、低リスクでも比較的簡単な改善で合格できそうな項目に重点的に取り組む方針で進めた。 技術面の是正対応としては、HTTPS への強制ジャンプ、ウェブサイトのデータとログのバックアップ、権限の分離、強力なパスワードの設定、クラウド・ウェブアプリケーションへのファイアウォール設定、セキュリティ監査、セキュリティ監視等の対応を実施した。 ここでセキュリティ製品の購入が必要となり、約 140 万円のコスト負担が発生した。管理面の是正対応は、コンサル会社が提供する文書テンプレートを参考に、不備を指摘された文書の整備を行った。
再審査の手配	再審査で新たな指摘を受けるのを回避するため、初回審査と再審査は同一の担当者である方がよいが、多忙のため評価機関の予定が取りづらい状態となっていた。そこで当社では、不備の是正対応にかかる時間を見越して、1 カ月前に予約を入れた。

＜ステップ４＞再審査～認証取得

実施事項	評価機関による再審査～認証取得
実施主体	・自社 ・政府の認可を受けた評価機関（←発注が必須） ・コンサル業者（ステップ３より継続して支援を受けた）
外注コスト	約 40 万円（評価機関による審査費用として必須）
所要期間	約 2 ヵ月　※再審査自体は 1 日
具体的な対応	説明
再審査の条件	再審査の確認項目は初回審査と同様である。初回に不合格だった項目を中心に確認が行われる（サーバの移転など大きな環境変化があれば審査のやり直しもあり得る）。再審査で不合格となった場合には、審査後に追加で是正対応を講じることも可能である。最終的な審査結果は、評価機関が公安局に報告を行った後に確定される。その時点で採点基準に調整が加わることもあり得るため、合格点より少し高めの点数を取れるよう準備した方が良い。
再審査項目 （技術面・管理面）	再審査では、評価機関から様々な質問・確認が行われる。当社の場合は、自社の担当者（筆者）が主に回答し、適宜同席したコンサル業者にもサポートしてもらった。評価機関とコンサル業者の担当者に面識があったこともあり、やり取りをスムーズに進めることができた。 技術面では、評価機関は前回不備だった項目について、各種システム、ウェブサイトのサーバ、ファイアウォール等の状況に対して逐一確認が実施された。審査用に専用端末を 1 台用意し、関連するファイルを保存しておくことで、当社の日常業務に支障が出ないよう審査をスムーズに進めることができた。 管理面では、ルールを整備するのみならず個々の文書の内容について細かな確認が行われた。また、個々の文書は 1 年以内に更新された最新版でなければならない。あらかじめ各種の文書や検査表を印刷しておくとスムーズである。 再審査が終わった時点で評価機関より大まかな点数を教えてもらうことができ、合格できそうな感触を得ることができた。
再審査の結果	再審査の 1 週間後、評価機関から結果の通知を受けた。当社は合格ラインの 81 点であった。この段階で、異議申し立てを行うことも認められているが、点数の高低で等級保護認証の取得可否に影響が及ぶことはない。この後、評価機関から公安局へ再審査結果が報告される。さらにその約 1 ヶ月後に、正式な等級保護認証取得の証明書が発行される。

３．当事者の視点からみた等級保護対応のポイント

本章では、当社における等級保護２級の認証取得体験を通じ、企業が等級保護対応を進める際に注意すべきと感じたポイントを整理する。

(1) 実施目的を明確にする

等級保護対応と同時に「ネットワークセキュリティレベルの向上を図りたい」「既存システムを統合したい」と考える企業も少なくないと思われる。しかし、等級保護対応を実施する際に、複数の目的を同時に達成しようとすると、対応すべき事柄が複雑になり、認証取得のハードルが過度に高くなるおそれがある。したがって、「等級保護の認証取得」にフォーカスして取り組む必要があると感じた。

(2) すべての情報・システムを評価の対象とする

企業が取り扱う情報・システムの等級に応じ、個別評価を行うことが国家標準で求められている。等級保護対応の最初のステップとして、自社が有する情報・システムをすべて洗い出し、等級分類の自社判断を進める必要があるといえる。万が一、対象とする情報・システムに抜け漏れがあると、せっかく等級保護対応を進めているにもかかわらず、認証取得に向けた各種対応が無効となるおそれもあるため、注意が必要である。

(3) コンサル業者を活用する

当社は当初、自社で等級保護対応を進めていたが「不適合項目をどう改善すればいいか（どの程度まで対策すれば合格できるか）分からない」といった課題に直面した。やみくもに対応を進めると、時間や費用が積み重なり、必要以上のリソースを消費してしまう可能性も考えられる。したがって、初めて等級保護対応を行う際は、早い段階より豊富な知見を有するコンサル業者を活用することが望ましい。なお、起用するコンサル業者により、対応に要する費用（改善対策として購入する製品なども含む）も異なるため、複数社の提案内容を事前に確認する必要がある。

(4) 自社にて対応可能な範囲を広げる

等級保護対応は一度認証を取得すれば、それ以降の対応が不要となるというものではない。2 級の情報・システムであれば、2 年に 1 回評価を実施することが国家標準で求められている（要求事項は初回評価時と同様)。今後の対応まですべてコンサル業者に委託すると、外注コストが中長期的に発生することとなる。そこで、このような状況を回避するため、自社の担当者を等級保護対応に関与させて、社内に等級保護対応のノウハウを蓄積することにより、2 回目以降の対応を想定し、自分たちで対応可能な範囲を広げることが重要であると感じた。これにより、外注に係る費用を最小限に抑えることが可能となる。

執筆:インターリスク上海　高級経理　張若亭

＜参考資料＞

- 《信息安全等级保护管理办法》 https://www.gov.cn/gzdt/2007-07/24/content_694380.htm
- 国家标准清单：

GB/T 22240-2020	信息安全技术　网络安全等级保护定级指南
GB/T 25058-2019	信息安全技术　网络安全等级保护实施指南
GB/T 25070-2019	信息安全技术　网络安全等级保护安全设计技术要求
GB/T 22239-2019	信息安全技术　网络安全等级保护基本要求
GB/T 28448-2019	信息安全技术　网络安全等级保护测评要求
GB/T 28449-2018	信息安全技术　网络安全等级保护测评过程指南
GB/T 36958-2018	信息安全技术　网络安全等级保护安全管理中心技术要求
GB/T 36959-2018	信息安全技术　网络安全等级保护测评机构能力要求和评估规范
GB/T 36627-2018	信息安全技术　网络安全等级保护测试评估技术指南
GB　17859-1999	计算机信息系统　安全保护等级划分准则

- 测评公司目录：网络安全等级保护网　https://www.djbh.net/agency?q=agencyIn&tab=2
- 处罚案例：广州市人民政府公共服务、腾讯网北京市昌平区委宣传部官方账号

  https://www.gz.gov.cn/zwfw/zxfw/ggfw/content/post_9129540.html

  https://new.qq.com/rain/a/20230913A05GBX00

ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランス　グループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティング及び広範な分野での調査研究を行っています。
中国進出企業さま向けのコンサルティング・セミナー等についてのお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先　　ＭＳ＆ＡＤインターリスク総研　リスクコンサルティング本部　国際業務室
TEL.03-5296-8920　　https：//www.irric.co.jp/

インターリスク上海は、中国　上海に設立されたＭＳ＆ＡＤインシュアランスグループに属するリスクマネジメント会社であり、お客様の工場・倉庫等へのリスク調査や、ＢＣＰ策定等の各種リスクコンサルティングサービスをご提供しております。
お問い合わせ・お申し込み等は、下記の弊社お問合せ先までお気軽にお寄せ下さい。

お問い合わせ先　　瑛得管理諮詢（上海）有限公司　（日本語表記：インターリスク上海）
上海市浦東新区世紀大道 100 号　環球金融中心 34 层 T10 室-2
TEL：+86-(0)21-6841-0611（代表）