サイバーセキュリティー等級保護条例
（意見募集稿）

（仮訳）

（2018 年 7 月）

日本貿易振興機構（ジェトロ）北京事務所

本資料は、JEITA/JLMC 北京事務所のご厚意により、ジェトロが同事務所から許諾を得てウェブサイトに掲載しています。本資料は仮訳であり、原本は中華人民共和国公安部のウェブサイト（www.mps.gov.cn/n2254536/n4904355/c6159136/content.html）でご覧いただけます。

JEITA/JLMC 北京事務所（仮訳）

目次

第一章　総　則

第1条【立法の主旨と依拠】サイバーセキュリティー等級保護業務を強化し、サイバーセキュリティー対策能力および水準を高め、ネットワーク空間における主権と国の安全、公共の利益を保護し、公民、法人およびその他の組織の合法的な権利・利益を保護し、経済社会における情報化の健全な発展を促進するため、「中華人民共和国サイバーセキュリティー法」、「中華人民共和国国家機密保護法」等の法律に依拠し、この条例を定める。

第2条【適用範囲】中華人民共和国国内において、ネットワークを構築、運営、保守、利用し、サイバーセキュリティー等級保護業務および管理監督を実施する場合にこの条例を適用する。個人および家庭内で構築され、使用されているネットワークは除く。

第3条【制度の確立】国はサイバーセキュリティー等級保護制度を実施し、ネットワークに対して等級別の保護、管理監督を行う。

前項にいう「ネットワーク」とは、コンピューターまたは、その他の情報端末および関連のデバイスで構成され、一定の規則およびプログラムにより情報を収集、保存、伝送、交換、処理するシステムである。

第4条【業務の原則】サイバーセキュリティー等級保護業務は、重点を強調し、主動的防御、総合的防止・制御の原則に基づき、サイバーセキュリティー防護体系を構築し、完全なものにし、国の安全、国の経済と人民の生活、公共の利益に及ぶネットワークインフラの運用の安全、データの安全を重点的に保護するものである。

ネットワーク運営者は、ネットワークの構築過程において、サイバーセキュリティーの保護、秘密保持、暗号化による保護の措置を同時並行して計画、確立、実施する。

機密ネットワークでは、国の秘密保護に関する規定および標準に基づき、システムの実情に結び付けて機密保護および機密の管理監督を行う。

第5条【職責分担】中央サイバーセキュリティーおよび情報化指導機関が、サイバーセキュリティー等級保護業務を統一し、指導する。国のインターネット情報部門は、サイバーセキュリティー等級保護業務の統制・調整に責任を負う。

国務院公安部門は、サイバーセキュリティー等級保護業務を主管し、その管理監督に責任を負い、法に基づきサイバーセキュリティーの保護を計画、実施する。

国の機密保護行政管理部門は、機密ネットワークの等級別保護業務を主管し、サイバーセキュリティー等級保護業務における秘密保護の関連業務の管理監督に責任を負う。

国の暗号管理部門は、サイバーセキュリティー等級保護業務における暗号管理の関連業務の管理監督に責任を負う。

国務院またはその他の関係部門は、関連法令の規定に基づき、各自の職務範囲内でサイバーセキュリティー等級保護に関する業務を行う。

県級以上の地方人民政府は、この条例および関連法令の規定に基づき、サイバーセキュリティー等級保護業務を行う。

第6条【ネットワーク運営者の責任と義務】ネットワーク運営者は、法に基づきネットワークの等級付け・登録、セキュリティーの構築・改善、等級評価、自主検査等の業務を実施し、管理および技術的措置を講じて、ネットワークインフラ、ネットワーク運営、データの安全、情報の安全を保障し、サイバーセキュリティー・インシデントに効果的に対応し、ネットワークの違法・犯罪活動を防止する。

第7条【業界に対する要求】業界主管部門は、当業界・分野におけるサイバーセキュリティー等級保護制度の確実な実施を計画、指導する。

第二章　支援と保障

第8条【総合的保障】国はサイバーセキュリティー等級保護制度における組織の指導体系と技術支援体系および保障体系を構築、整備する。

各級人民政府および業界主管部門は、サイバーセキュリティー等級保護制度の実施を情報化業務の全体計画に盛り込み、統一的に計画手配し推進する。

第9条【規格の制定】国は整ったサイバーセキュリティー等級保護規格体系を構築、整備する。国務院の標準化行政主管部門と国務院公安部門、国の機密保護行政管理部門、国の暗号管理部門は各自の職責に基づき、サイバーセキュリティー等級保護の国家規格と業界規格を制定する。

国は企業、研究機関、高等教育機関、ネットワーク関連業界の、サイバーセキュリティー等級保護の国家規格、業界規格の制定への関与を支援する。

第10条【投入と保障】各級人民政府は、サイバーセキュリティー等級保護重点事業およびプロジェクトを奨励、援助し、サイバーセキュリティー等級保護技術の研究開発および応用を支援し、安全な信頼できるネットワーク製品とサービスを推し広める。

第11条【技術支援】国は、サイバーセキュリティー等級保護の専門家チームと等級評価、セキュリティー構築、緊急対応措置等の技術支援体系を構築し、サイバーセキュリティー等級保護制度を支える。

第12条【成果に対する審査】業界主管部門、各級人民政府は、サイバーセキュリティー等級保護業務を、成果審査評価、社会治安の総合管理審査等に組み入れる。

第13条【周知・教育と研修】各級人民政府およびその関係部門は、サイバーセキュリティー等級保護制度の周知・教育を強化し、社会大衆のサイバーセキュリティー保護の意識を高める。

国は企業・政府系事業組織、大学、研究機関等がサイバーセキュリティー等級保護制度についての教育と研修の実施を奨励、支援し、サイバーセキュリティー等級保護の管理および技術人材の育成を強化する。

第14条【イノベーションの奨励】国は新たな技術、アプリケーションを利用して、サイバーセキュリティー等級保護管理および技術的対策を行うことを奨励し、主動的防御、信頼できるコンピューティング、AI（人工知能）等の技術を用いて、サイバーセキュリティー技術保護措置を刷新し、サイバーセキュリティー対策の能力と水準を高める。

国はネットワークの新たな技術・アプリケーションを普及させるにあたり、サイバーセキュリティーのリスク評価を計画、実施し、新たな技術・アプリケーションにおけるセキュリティーリスクを防止する。

第三章　ネットワークのセキュリティー保護

第15条【ネットワーク等級】国の安全、経済構築、社会生活におけるネットワークの重要度、および、いったん破壊され、機能を失い、またはデータの改ざん、漏えい、滅失、毀損が発生した後の、国の安全、社会秩序、公共の利益および関係する公民、法人、その他の組織の合法的な権利・利益に与える危害の程度などの要素に基づき、ネットワークを五つのセキュリティー保護等級に分ける。

（一）第1級、いったん破壊されると、関係する公民、法人およびその他の組織の合法的な権利・利益が損なわれるが、国の安全、社会秩序、公共の利益には危害が及ばない一般ネットワーク。

（二）第2級、いったん破壊されると、関係する公民、法人およびその他の組織の合法的な権利・利益に重大な損害が生じ、または社会秩序および公共の利益に危害がもたらされるが、国の安全には危害が及ばない一般ネットワーク。

（三）第3級、いったん破壊されると、関係する公民、法人およびその他の組織の合法的な権利・利益に非常に重大な損害が生じ、または社会秩序および公共の利益に重大な危害がもたらされ、または国の安全にも危害が及ぶ重要ネットワーク。

（四）第4級、いったん破壊されると、社会秩序および公共の利益に非常に重大な危害がもたらされ、または国の安全に深刻な危害をもたらす特に重要なネットワーク。

（五）第5級、いったん破壊されると、国の安全に非常に重大な危害をもたらす極めて重要なネットワーク。

第16条【ネットワークの等級付け】ネットワーク運営者は、その計画・設計段階において、ネットワークのセキュリティー保護等級を決定する。

ネットワークの機能、サービス範囲、サービス対象、処理データ等に大きな変化が生じる場合、ネットワーク運営者は、法に基づきネットワークのセキュリティー保護等級を変更しなければならない。

第17条【等級付けに対する評価・審査】第2級以上のネットワークとするものについて、その運営者は専門家による評価・審査を行わなければならない。業界主管部門がある場合は、評価・審査の後主管部門に報告して承認を得なければならない。

省をまたぎ、または全国統一のネットワークを形成して運営されているネットワークは、業界主管部門が統一して暫定的なセキュリティー保護等級を制定し、評価・審査を行って等級を決定する。

業界主管部門は、国家規格・規範に基づき、当業界ネットワークの特徴を踏まえ、業界サイバーセキュリティー等級保護の等級付けに関する指導意見を制定することができる。

第18条【等級付け・登録】第2級以上のネットワーク運営者は、そのネットワークのセキュリティー保護等級が確定された後、10業務日以内に県級以上の公安機関で登録手続きを行わなければならない。

ネットワークの廃止または変更によって、セキュリティー保護等級を調整する場合は、原登録を受理した公安機関で10業務日以内に登録の取り消し、または変更手続きを行わなければならない。

登録手続きの具体的な方法は、国務院公安部門が策定する。

第19条【登録審査】公安機関は、ネットワーク運営者が提出した登録資料に対する審査を行わなければならない。等級付けが正しく、登録資料が要件を満たしているものについては、10業務日以内にサイバーセキュリティー保護等級の登録証明書を発行しなければならない。

第20条【一般セキュリティ保護義務】ネットワーク運営者は、法に基づき以下のセキュリティー保護義務を履行し、ネットワークと情報の安全を保障しなければならない。

（一）サイバーセキュリティー等級保護業務の責任者を決定し、サイバーセキュリティー等級保護業務責任制を確立して、責任追及制度を実行する。

（二）安全管理および技術保護制度は、人員管理、教育・研修、システムセキュリティー構築、維持管理等の制度を確立する。

（三）機械室の安全管理、設備、媒体の安全管理、サイバーセキュリティー管理等の制度を実行し、作業規範および作業工程を定める。

（四）身分識別、悪意のあるコードによる感染の拡散防止、サイバー攻撃防止に対する管理、技術的措置を講じる。

（五）モニタリング、ネットワークの運用状態の記録、サイバーセキュリティー・インシデント、違法・犯罪活動に対する管理および技術的措置を実行し､規定に基づき6カ月以上遡ることのできるネットワーク違法・犯罪に関するログを保存する。

（六）データ分類、重要データのバックアップ、暗号化等の措置を実行する。

（七）法に基づき個人情報を収集、利用、処理し、個人情報に対する保護措置を実行し、個人情報の漏えい、毀損、改ざん、窃取、滅失、濫用を防止する。

（八）違法情報の発見、遮断、削除等の措置を実行し、違法情報の大量拡散、違法・犯罪の証拠隠滅等を防止する措置を実行する。

（九）ネットワーク接続の登録およびユーザーの本人確認等の責任を適切に果たす。

（十）ネットワークで発生した案件・事件に対しては、24時間以内に当地の公安機関に報告しなければならない。国家機密を漏えいした場合は、併せてその地の秘密保護行政管理部門に報告しなければならない。

（十一）法律、行政法規で定めるその他のサイバーセキュリティー保護義務

第21条【特殊なセキュリティ保護義務】第3級以上のネットワーク運営者は、本条例第20条に規定するサイバーセキュリティー保護義務を履行するほか、以下の各号に掲げるセキュリティー保護義務をさらに履行しなければならない。

（一）サイバーセキュリティー管理機関を決定し、サイバーセキュリティー等級保護業務における職務責任を明確にし、ネットワークの変更、ネットワーク接続、維持管理、技術保障組織の変更等の事項に対する段階的な審査承認制度を制定する。

（二）サイバーセキュリティーの全体計画と総合的なセキュリティー対策を制定、実行し、セキュリティー構築案を策定し、専門技術者による評価・審査を経る。

（三）サイバーセキュリティー管理責任者と重要職務に就く人員に対する身上調査を行い、証明書取得後着任の制度を実行する。

（四）ネットワークの設計、構築、維持管理、技術サービスを提供す

る機関、人員に対する安全管理を行う。

（五）サイバーセキュリティーに関する情勢の感知モニタリング警報措置を実行し、サイバーセキュリティー対策管理プラットフォームを構築して、ネットワークの運用状態、トラフィック、ユーザー行動、サイバーセキュリティー案件・事件等に対する動的モニタリング分析を行い、同級の公安機関と連携する。

（六）重要ネットワーク設備、通信リンク、システムの冗長性、バックアップおよび復旧に関する措置を実行する。

（七）サイバーセキュリティー等級評価制度を構築し、定期的に等級の評価を行い、評価状況およびセキュリティーの改善措置、改善結果を公安機関と関係部門に報告する。

（八）法律および行政法規に定めるその他のサイバーセキュリティー保護義務。

第22条【オンラインの検査・測定】新たに構築された第2級ネットワークをオンライン運用する前に、サイバーセキュリティー等級保護の関連規格・規範に基づきネットワークの安全性に対する試験を行わなければならない。

新たに構築された第3級以上のネットワークをオンライン運用する前に、サイバーセキュリティー等級評価機関に委託して、サイバーセキュリティー等級保護の関連規格・規範に基づき評価を行わなければならず、等級評価を通過した後に運用可能となる。

第23条【等級評価】第3級以上のネットワーク運営者は、毎年1度サイバーセキュリティー等級評価を行い、セキュリティー上の潜在的なリスクを発見、改善し、毎年サイバーセキュリティー等級評価の作業状況および評価結果を登録している公安機関に報告しなければならない。

第24条【セキュリティーの改善】ネットワーク運営者は、等級評価において見つかったセキュリティー上の潜在的なリスクに対する改善案

を策定し、改善措置を実施し、潜在的なリスクを除去しなければならない。

第25条【自主検査業務】ネットワーク運営者は、当組織のサイバーセキュリティー等級保護制度の実施状況とサイバーセキュリティー状況に対し、毎年少なくとも1度自主検査を実施し、セキュリティー上の潜在的なリスクを発見した場合には速やかに改善し、登録している公安機関に報告しなければならない。

第26条【評価活動におけるセキュリティー管理】サイバーセキュリティー等級評価機関は、ネットワーク運営者に安全で客観的かつ公正な等級評価サービスを提供しなければならない。

サイバーセキュリティー等級評価機関は、ネットワーク運営者とサービス契約を締結し、評価担当者に対してセキュリティー上の秘密保護教育を実施し、その者とセキュリティー上の秘密保護責任に関する契約書を締結して、評価担当者のセキュリティー上の秘密保護義務と法律責任を明確にし、その者を専門の研修に参加させなければならない。

第27条【ネットワークサービス機関の要件】ネットワークサービス提供者が、第3級以上のネットワークにネットワークの構築、運用・保守、安全モニタリング、データ分析等のネットワークサービスを提供する場合、国の関連法令および技術規格の要件を満たしていなければならない。

サイバーセキュリティー等級評価機関等のネットワークサービス提供者は、そのサービスの過程で知り得た国家機密、個人情報、重要データを守らなければならない。サービスを提供する中で収集、掌握したデータ情報、システムの不具合、悪意のあるコード、サイバー攻撃等のサイバーセキュリティー情報を不正に利用、または無断で公表してはならない。

第28条【製品およびサービスの購入、利用におけるセキュリティー要求事項】ネットワーク運営者は、国の法令および関連規格・規範の要求

事項を満たすネットワーク製品およびサービスを購入、利用する。

第3級以上のネットワーク運営者は、セキュリティー保護等級に適応したネットワーク製品およびサービスを取り入れ、重要箇所に使用するネットワーク製品については、専門の評価機関に委託して特定項目の試験を行い、その結果に基づき要件を満たしたネットワーク製品を選択し、購入したネットワーク製品およびサービスが国の安全に影響を及ぼす可能性がある場合は、国のネットワーク情報部門が国務院の関係部門と共同で実施する国家安全審査を通過しなければならない。

第29条【保守点検の要求事項】第3級以上のネットワークは国内において保守点検を行わなければならず、国外からの遠隔地操作による保守点検を実施してはならない。業務上の必要性から、やむを得ず国外からの遠隔操作による保守点検が必要な場合は、サイバーセキュリティー評価を行い、リスク管理制御措置を講じなければならない。保守点検を実施する時には、その日誌をつけ、それを保存し、公安機関の検査時に事実どおりに提供しなければならない。

第30条【モニタリング警報と情報の通報】地市級以上の人民政府は、サイバーセキュリティー・モニタリング警報および情報通報制度を確立し、セキュリティーモニタリング、情勢感知、警報の通報等の業務を行わなければならない。

第3級以上のネットワーク運営者は、サイバーセキュリティー・モニタリング警報および情報通報制度を確立、整備し、規定に従って同級の公安機関にサイバーセキュリティー・モニタリング警報情報を提出し、サイバーセキュリティー・インシデントを報告しなければならない。業界主管部門がある場合には、業界主管部門へも申告と報告を行わなければならない。

業界主管部門は、当業界・分野におけるサイバーセキュリティー・モ

ニタリング警報および情報通報制度を確立、整備し、規定に従って同級のネットワーク情報部門と公安機関にサイバーセキュリティー・モニタリング警報情報を提出し、サイバーセキュリティー・インシデントを報告しなければならない。

第31条【データおよび情報のセキュリティ保護】ネットワーク運営者は、重要データおよび個人情報のセキュリティー保護制度を構築し、実行に移し、保護措置を講じて、データおよび情報の収集、保管、伝送、利用、提供、廃棄の過程における安全を保障し、遠隔地でのバックアップ・復旧等の技術的措置を確立して、重要データの完全性、機密性および可用性を保障しなければならない。

ネットワーク運営者は、許可または授権を経ずに、その提供するサービスと関係のないデータおよび個人情報を収集してはならない。法律、行政法規の規定および双方の取り決めに違反して、データおよび個人情報を収集、利用、処理してはならない。収集したデータおよび個人情報を漏えい、改ざん、毀損してはならない。授権を受けずにデータおよび個人情報へのアクセス、利用、提供を行ってはならない。

第32条【緊急対応処理に対する要求】第3級以上のネットワーク運営者は、国の関連規定に従って、サイバーセキュリティー緊急対応マニュアルを制定し、定期的にサイバーセキュリティー緊急対応訓練を実施しなければならない。

ネットワーク運営者がサイバーセキュリティー・インシデントを処理するにあたり、現場を保護し、関連データ情報を記録、保存し、併せて、ただちに公安機関と業界主管部門に報告しなければならない。

公安機関と業界主管部門は、同級のインターネット情報部門に重大なサイバーセキュリティー・インシデントの処理状況を報告しなければならない。

重大なサイバーセキュリティー・インシデントが発生した場合、関係

部門はサイバーセキュリティー緊急対応マニュアルの要求に基づき、共同で緊急対応処置を実施する。電信業務経営者、ネットワークサービス・プロバイダーは、重大なサイバーセキュリティー・インシデントの処理と復旧に協力し、サポートしなければならない。

第33条【監査、審査要求】ネットワーク運営者が、ネットワークを構築、運営、保守、利用して、社会に行政許可を取得する必要のある経営活動を提供する場合、関係主管部門は、サイバーセキュリティー等級保護制度の実施状況を監査および審査の範囲に組み入れなければならない。

第34条【新しい技術とアプリケーションのリスク管理制御】ネットワーク運営者は、サイバーセキュリティー等級保護制度の要求に基づき、措置を講じて、クラウドコンピューティング、ビッグデータ、AI（人工知能）、IoT（モノのインターネット）、産業用制御システムおよびモバイルインターネット等の新たな技術、アプリケーションがもたらすセキュリティーリスクを管理、制御し、潜在的なリスクを除去しなければならない。

第四章　機密ネットワークのセキュリティー保護

第35条【等級別保護】機密ネットワークは、保管、処理、伝送される国家機密の最高機密等級によって、極秘級、機密級、秘密級に分けられる。

第36条【ネットワークの等級付け】機密ネットワークの運営者は、法に基づき機密ネットワークの機密等級を確定し、当組織の秘密保護委員会（指導グループ）の審査決定を経て、同級の秘密保護行政管理部門に登録する。

第37条【プランの審査と論証】機密ネットワークの運営者が機密ネッ

トワークを計画、構築するにあたり、国の秘密保護規定と標準要求に基づき等級別保護案を制定し、身分の識別、アクセス制御、安全の監査、境界のセキュリティー保護、情報の流れ管理・制御、電磁波の漏えい・輻射防護、ウイルス対策、暗号化による保護ならびに秘密保護の管理監督等の技術および管理措置を取らなければならない。

第38条【構築管理】機密ネットワークの運営者が、その他の組織に機密ネットワークの構築を委託する場合、相応する機密情報システム総合インテグレーターの認定を受けた組織を選び、構築組織と秘密保護契約を結び、秘密保護責任を明確にして、秘密保護措置を講じなければならない。

第39条【情報設備とセキュリティーの保護製品の管理】機密ネットワーク中に使用する情報設備は、国の関係主管部門が公表している機密専用情報設備目録から選び、目録にない場合は、政府調達の一覧表から製品を選び、やむを得ず輸入製品を使用する必要がある場合は、セキュリティー・秘密保護検査を実施しなければならない。

機密ネットワークの運営者は、国家機密保護行政管理部門が使用を禁じ、または政府調達主管部門が調達を禁止している製品を使用してはならない。

機密ネットワークに使用するセキュリティー・秘密保護製品は、国家機密保護行政管理部門が設けた検査機関の検査を経なければならない。コンピューターウイルス対策製品には、コンピューター情報システムセキュリティー専用の製品販売許可証を取得している信頼できる製品を使用し、暗号化製品には、国家暗号管理部門が承認している製品を使用しなければならない。

第40条【評価・審査とリスク評価】機密ネットワークは国の機密保護行政管理部門が設け、または授権した秘密保護評価機関が検査、評価し、市轄区が設置された市級以上の秘密保護の行政管理部門の審査に合格

した後に利用しなければならない。

機密ネットワークの運営者は、その利用を開始した後、定期的にセキュリティー・秘密保護検査とリスクに対する自己評価を実施し、秘密保護行政管理部門が計画したセキュリティー・秘密保護リスク評価を受けなければならない。極秘級ネットワークは毎年少なくとも1度、機密級と秘密級ネットワークは少なくとも2年に1度実施する。

公安機関と国家安全機関の機密ネットワークの利用に対する管理は、国家機密保護行政管理部門が公安機関、国家安全機関と共に定めた関連規定に基づいて行う。

第41条【機密ネットワークの利用管理に対する一般的要求】機密ネットワークの運営者は、セキュリティー・秘密保護管理制度を制定し、相応の管理機関を設定し、セキュリティー・秘密保護管理人員を配置して、そのセキュリティー・秘密保護責任を確実に果たさなければならない。

第42条【機密ネットワークの警報通報に対する要求】機密ネットワークの運営者は、当組織の機密ネットワークセキュリティー・秘密保護モニタリング警報および情報通報制度を確立、整備し、セキュリティー上の潜在的なリスクを発見した場合には、速やかに緊急対応措置を講じ、秘密保護行政管理部門に報告しなければならない。

第43条【機密ネットワークに重大な変化が生じた場合の処理】以下の各号のいずれかに該当する場合は、機密ネットワークの運営者は、国家機密保護規定に従い速やかに秘密保護行政管理部門に報告し、相応の措置を講じなければならない。

（一）機密等級に変化が生じた場合。

（二）接続範囲、端末の数量が審査に通った範囲、数量を超えた場合。

（三）所在場所の物理的環境またはセキュリティー・秘密保護施設に変更が生じ、新たなセキュリティー・秘密保護リスクをもたらす可能性がある場合。

（四）新たにアプリケーション・システムを増やし、またはアプリケーション・システムを変更もしくは削減したことで、新たなセキュリティー・秘密保護にリスクがもたらされる可能性がある場合。

前項で列挙した状況に対し、秘密保護行政管理部門は、速やかに機密ネットワークに対して改めて評価と審査を行うか否かの決定を下さなければならない。

第44条【機密ネットワーク廃止時の処理】機密ネットワークの利用を終了する場合、機密ネットワークの運営者は、速やかに秘密保護行政管理部門に報告し、国の秘密保護規定および標準に基づき、機密情報設備、製品、機密媒体等を処理する。

第五章　暗号管理

第45条【暗号に関する要求事項の確定】国家暗号管理部門は、ネットワークのセキュリティー保護等級、機密ネットワークの機密等級および保護等級に基づき、暗号の設定、利用、管理、適用における安全性評価要求を定め、サイバーセキュリティー等級保護暗号標準規範を制定する。

第46条【機密ネットワークの暗号化による保護】機密ネットワークおよび伝送する国家機密情報は、法に基づき暗号化により保護しなければならない。

暗号化製品は暗号管理部門の承認を得なければならず、暗号化技術を用いたソフトウェアシステム、ハードウェア設備等の製品は、暗号の検査を通過しなければならない。

暗号の検査、設置、調達、利用等は、暗号管理部門が統括管理する。システム設計、運用保守、日常管理および暗号評価は、国の暗号管理関連法規および標準に従って行われなければならない。

第47条【非機密ネットワークの暗号化による保護】非機密ネットワークは、国の暗号管理に関する法令および標準の要求に従って、暗号化技術、製品、サービスを利用しなければならない。第3級以上のネットワークは、暗号化による保護を取り入れ、国家暗号管理部門が認可した暗号化技術、製品、サービスを利用しなければならない。

第3級以上のネットワーク運営者は、ネットワークの計画、構築、運用段階において、暗号適用の安全性評価管理弁法と関連標準に基づき、暗号適用の安全性評価機関に委託してその評価を行わなければならない。ネットワークは評価を通過した後にオンライン運用が可能となり、運用後は毎年少なくとも1度評価を実施する。暗号適用の安全性評価結果は、登録を受理した公安機関と所在地の市轄区が設置された市の暗号管理部門に届け出らなければならない。

第48条【暗号の安全管理責任】ネットワーク運営者は、国の暗号管理法規および関連管理要求に基づき、暗号の安全管理職責を果たし、暗号安全制度の構築を強化し、暗号安全管理措置を完全なものとし、暗号の利用行為を規範化しなければならない。

いかなる組織および個人も暗号を利用して国の安全、公共の利益を損なう活動に従事し、またはその他の違法・犯罪活動に従事してはならない。

第六章　管理監督

第49条【安全管理監督】県級以上の公安機関は、ネットワーク運営者が国の法令の規定および関連規格・規範要求に基づき、サイバーセキュリティー等級保護制度を実行し、サイバーセキュリティー対策、サイバーセキュリティー・インシデントへの緊急対応処置、重大な活動におけるサイバーセキュリティー保護等の業務を行うことに対し管理監督す

る。

第3級以上のネットワーク運営者が、サイバーセキュリティー等級保護制度に基づきネットワークインフラ、ネットワーク運用の安全とデータの安全保護責任および義務を適切に果たすことに対し、重点的に管理監督する。

県級以上の公安機関は、同級の業界主管部門が国の法令の規定および関連規格・規範の要求に基づいて実施する、当業界・分野に対するサイバーセキュリティー等級保護制度の実行、サイバーセキュリティー対策・サイバーセキュリティー・インシデントへの緊急対応措置・重大な活動におけるサイバーセキュリティー保護等の監督業務に対し、その状況を監督、検査、指導する。

地・市級以上の公安機関は、毎年サイバーセキュリティー等級保護に関する業務情報を同級のインターネット情報部門へ通報する。

第50条【セキュリティ検査】県級以上の公安機関は、ネットワーク運営者が以下のサイバーセキュリティー業務を実施する状況を監督、検査する。

（一）日常的なサイバーセキュリティー対策業務

（二）重大なサイバーセキュリティーの潜在的なリスクに対する改善状況

（三）重大なサイバーセキュリティー・インシデントに対する緊急対応措置および復旧業務

（四）重大な活動におけるサイバーセキュリティー保護業務の実施状況

（五）その他のサイバーセキュリティー保護業務状況

公安機関は、第3級以上のネットワーク運営者に対し、毎年少なくとも1度セキュリティー検査を実施する。関連業界にかかわる場合は、その業界主管部門と共にセキュリティー検査を実施することができる。必

要がある場合は、公安機関は民間に委託して技術支援を受けることができる。

公安機関は法に基づき監督・検査を行い、ネットワーク運営者はそれに協力し、公安機関の要求に従い、事実どおりに関連データ情報を提供しなければならない。

第51条【検査・処分】公安機関は、その監督・検査においてサイバーセキュリティーの潜在的なリスクを発見した場合には、ネットワーク運営者にただちに措置を講じて除去するよう命じ、ただちに除去できない場合は、期間を定めて改善を命じなければならない。

公安機関が、第3級以上のネットワークに重大なセキュリティー上の潜在的なリスクがあることを発見した場合は、速やかに業界主管部門に通報するとともに、同級のインターネット情報部門に通報しなければならない。

第52条【重大な潜在的なリスクの処理】公安機関は、その監督・検査において重要な業界または当地区に国、公共の安全、公共の利益を著しく脅かす重大なサイバーセキュリティーの潜在的なリスクを発見した場合には、同級の人民政府、インターネット情報部門および上級の公安機関に報告しなければならない。

第53条【評価機関とセキュリティー構築機関に対する管理監督】国は、サイバーセキュリティー等級評価機関とセキュリティー構築機関に対し、推薦リストの管理を行い、サイバーセキュリティー等級評価機関とセキュリティー構築機関が、業界の自主規制組織を設立し、業界自主規制規範を制定し、自主規制を強化するよう指導する。

非機密サイバーセキュリティー等級評価機関とセキュリティー構築機関に対する具体的な管理規則は、国務院公安部門が定める。秘密保護の科学技術評価機関管理規則は、国家機密保護行政管理部門が定める。

第54条【重要人員の管理】第3級以上のネットワーク運営者の重要職

務を担う人員、および第3級以上のネットワークにセキュリティサービスを提供する人員は、国外で組織されるネットワークの攻防活動に、無断で参加してはならない。

第55条【事件の調査】公安機関は、関連規定に基づきサイバーセキュリティー・インシデントを処理し、事件に対する調査を実施して、事件の責任を認定し、法に基づきサイバーセキュリティーを損ねる違法・犯罪活動を調査、処分しなければならない。必要がある場合は、ネットワーク運営者に情報の転送遮断、ネットワーク運用の一時停止、関連データのバックアップ等の緊急措置を講じるよう命じることができる。

ネットワーク運営者は、公安機関および関係部門が行う事件の調査および処分業務に協力し、それをサポートしなければならない。

第56条【緊急事態時におけるネットワークの遮断措置】ネットワークに存在するセキュリティー面での潜在的なリスクが国の安全、社会の秩序および公共の利益を著しく脅かす場合は、緊急事態下において公安機関がネットワーク接続の停止、シャットダウン・改善を命じることができる。

第57条【秘密保護に対する管理監督】秘密保護行政管理部門は、機密ネットワークのセキュリティー保護業務に対する管理監督に責任を負い、非機密ネットワークの機密漏えい行為に対する管理監督に責任を負う。潜在的なリスクを発見し、または秘密保護法令に違反し、もしくは秘密保護規格に合わない秘密保護に対しては、「中華人民共和国保守国家秘密法」および国の秘密保護関連規定に従って処理、処分する。

第58条【暗号に対する管理監督】暗号管理部門は、サイバーセキュリティー等級保護業務における暗号管理に対する管理監督に責任を負い、ネットワーク運営者のネットワークに対する暗号の設定、利用、管理および暗号評価状況を監督、検査する。そのうちの重要機密情報システムについては、少なくとも2年に1度監督、検査を行う。監督・検査におい

て潜在的なリスクを発見し、または暗号管理の関連規定に違反し、もしくは暗号関連規格・規範の要求を満たしていない場合は、国の暗号管理関連規定に従って処理、処分する。

第59条【業界に対する管理監督】業界主管部門は、当業界・分野におけるサイバーセキュリティー等級保護業務計画と規格・規範を制定し、ネットワークの基本状況、等級付け登録状況、セキュリティー保護状況を把握し、当業界・分野におけるネットワーク運営者が行うネットワーク等級付け登録、等級評価、セキュリティーの構築・改善、セキュリティーの自主検査等を管理監督しなければならない。

業界主管部門は、当業界・分野におけるネットワーク運営者がサイバーセキュリティー等級保護制度と関連規格・規範の要求に基づき講じるサイバーセキュリティー管理、および技術的保護措置、実施するサイバーセキュリティー対策、サイバーセキュリティー・インシデント緊急対応処理、重大な活動におけるサイバーセキュリティー保護等の業務を、管理監督しなければならない。

第60条【管理監督責任】サイバーセキュリティー等級保護管理監督部門およびその業務担当者は、職務の遂行において知り得た国家機密、個人情報および重要データを厳格に秘密保護しなければならず、漏えいし、販売し、または違法に第三者に提供してはならない。

第61条【法の執行への協力】ネットワーク運営者および技術支援組織は、公安機関、国家安全機関の法に基づく国家の安全保護、犯罪捜査活動を支援し、協力しなければならない。

第62条【サイバーセキュリティ事情聴取制度】省級以上の人民政府公安部門、秘密保護行政管理部門、暗号管理部門は、サイバーセキュリティー等級保護管理監督の職務の遂行において、ネットワークに比較的大きなセキュリティー上の潜在的なリスクがあることを発見し、またはセキュリティーインシデントが発生した場合は、ネットワーク運営者の法

定代表人、主要責任者およびその業界主管部門に対し、事情を聴取することができる。

第七章　法律責任

第63条【セキュリティー保護義務違反】ネットワーク運営者が、本条例第16条、第17条第1項、第18条第1項と第2項、第20条、第22条第1項、第24条、第25条、第28条第1項、第31条第1項、第32条第2項に定められたサイバーセキュリティー保護義務を履行しなかった場合において、公安機関はその履行を命じ、「中華人民共和国サイバーセキュリティー法」第59条第1項の規定により処罰する。

第3級以上のネットワーク運営者が、本条例第21条、第22条第2項、第23条、第28条第2項、第30条第2項、第32条第1項の規定に違反した場合は、前項の規定に従って厳重に処罰する。

第64条【技術保守要求違反】ネットワーク運営者が本条例第29条の規定に違反し、第3級以上のネットワークに対して国外からの遠隔での技術保守を行い、サイバーセキュリティー評価を行わず、リスク管理・制御措置を講じず、技術保守日誌を記録、保存しなかった場合は、公安機関と関連業界主管部門が各自の職責に基づき是正を命じ、「中華人民共和国サイバーセキュリティー法」第59条第1項の規定により処罰する。

第65条【データの安全および個人情報保護要求違反】ネットワーク運営者が本条例第31条第2項の規定に違反して、データおよび個人情報を無断で収集、利用、提供した場合は、ネットワーク情報部門と公安機関が各自の職責に基づき是正を命じ、「中華人民共和国サイバーセキュリティー法」第64条第1項の規定により処罰する。

第66条【サイバーセキュリティー・サービスの責任】本条例第26条第3項、第27条第2項の規定に違反した場合は、公安機関が是正を命じ、情

状に基づき、警告、違法所得の没収、違法所得の倍以上10倍以下の過料という処分を単独または併用して科し、違法所得がない場合は、100万元以下の過料を科し、直接的な責任を負う主管担当者とそのほかの直接責任者に1万元以上10万元以下の過料を科す。情状が重い場合には、併せて許可証発行機関に通知して、関連業務の許可証の取り消しまたは営業許可証の取り消しとなるまで、関連業務の一時停止、営業を停止しての是正を命じることができる。

本条例第27条第2項の規定に違反して、個人情報の漏えい、違法販売または第三者への提供を行った場合は、「中華人民共和国サイバーセキュリティー法」第64条第2項の規定により処罰する。

第67条【法の執行への協力義務違反】ネットワーク運営者が本条例の規定に違反して、以下の行為に該当する場合、公安機関、秘密保護行政管理部門、暗号管理部門、業界主管部門および関係部門は、各自の職責に基づき是正を命じる。是正に応じないまたは情状が重大な場合には、「中華人民共和国サイバーセキュリティー法」第69条の規定により処罰する。

（一）関係部門が、法に基づき実施する監督・検査を拒絶、妨害した場合。

（二）サイバーセキュリティーの保護に関するデータ情報を、事実どおりに提供することを拒んだ場合。

（三）緊急対応処理において、関連主管部門の統一した指示・指導に従わなかった場合。

（四）公安機関、国家安全機関への技術支援、協力を拒んだ場合。

（五）電信業務経営者、ネットワークサービス・プロバイダーが、重大なサイバーセキュリティー・インシデントの処理および復旧において、本条例の規定に基づきサポート、協力を行わなかった場合。

第68条【秘密保護および暗号管理責任違反】本条例の秘密保護管理、暗号管理に関する規定に違反した場合、秘密保護行政管理部門または暗号管理部門が各自の職責に基づき役割分担をして是正するよう命じる。是正に応じない場合は警告を発し、その上級主管部門に通報し、その主管者、そのほかの直接責任者、を法に基づき処分するよう提案する。

第69条【管理監督部門の汚職の責任】ネットワーク情報部門、公安機関、国家機密保護行政管理部門、暗号管理部門、関係業界主管部門およびその業務担当者に以下の各号のいずれかに該当する行為がある場合は、直接責任を負う主管者、そのほかの直接責任者、または関連業務担当者を、法に基づき処分する。

（一）職務怠慢、職権濫用、私情による不正を働いた場合

（二）サイバーセキュリティー等級保護に対する監視監督の職務の遂行において知り得た国家機密、個人情報および重要データの漏えい、販売、違法な提供を行い、または取得したその他の情報を別の用途に利用した場合。

第70条【法条競合】本条例に違反し、治安管理の違反行為を構成する場合は、公安機関が法に基づき治安管理処罰を科し、犯罪を構成する場合には、法に基づき刑事責任を追及する。

第八章　附　則

第71条【用語の解釈】この条例にいう「内」、「以上」にはその数が含まれ、“業界主管部門”には業界管理監督部門が含まれる。

第72条【軍隊】軍隊におけるサイバーセキュリティー等級保護業務は、軍隊の関連法規に従って実施する。

第73条【発効時期】この条例は　　年　月　日から施行する。