CLARA ONLINE China Internet Report
2017.7.10

取得が広がるセキュリティ等級認定

株式会社クララオンライン
コンサルティングチーム

<要約と結論>

サイバーセキュリティ法の施行を受け、セキュリティ等級の認定を取得する IT サービスが増えている。阿里巴巴(アリババ)や騰訊(テンセント)が提供するクラウドサービスも 3 級ないしは 4 級の認定を取得済みだ。

セキュリティ等級とは、「情報セキュリティ等級保護管理弁法」で定められているもので、システムが攻撃を受け破壊された場合の損害を想定して 1 級から 5 級の 5 段階に分けられている。等級に応じたセキュリティ対策を取る必要があり、具体的にどのような措置が必要となるかは、国家標準規格で定められている。さらに地域や業界によってガイドラインが出されており、システムの用途に応じて取得すべき等級が決められていることもある。

自社のシステムがどの等級に該当するかは、運営担当者らが規定を参考に決めたのち、届出登録を行い、審査に合格すれば証明書が発行される。以降は定期的にセキュリティ対策の実施状況について検査を行う必要があるほか、保存されている情報や等級によって当局による調査が行われる。

しかし、現行の基準ではクラウドサービスや IoT といった新興分野がカバーできないことから、公安部などは新たな基準の取りまとめを進めている。“セキュリティ等級保護 2.0”と呼ばれる拡張要求は、すでにひな形が完成しておりインターネット上で公開されている。

現行の規定では、セキュリティ対策の責任は当該システムの運営者あるいは使用者が負うことになっている。しかしクラウドサービスの場合、サーバー提供側とサーバー利用者側の双方が責任を負うこととされている。またセキュリティ等級の認定においても、クラウドサービスの等級認定とクラウド上で運用するサービスの等級認定を別々に行うことが定められている。

“セキュリティ等級保護 2.0”が正式に発表されるタイミングは定かでないが、サイバーセキュリティ法など関連する法令との調整が行われている可能性は高い。いずれにせよ、当局が情報セキュリティ等級の認定取得を呼び掛けていることから、年内にも発表される可能性は高いことが予想される。

1. サイバーセキュリティ法の影響か

6 月 1 日から「サイバーセキュリティ法」が施行されたことを受け、IT システムに関するセキュリティ等級の認定が進んでいる。つい先日には、微信(Weixin)等を運営する騰訊(テンセント)のクラウドサービス「騰訊雲」が、金融クラウドプラットフォームで 4 級、パブリッククラウドプラットフォーム、カスタマーサービスシステム、料金計算システム、運用保守管理システムでそれぞれ 3 級の認定を取得したことを発表したばかりだ。サイバーセキュリティ法の施行後、初の認定取得だという。

通信分野のセキュリティ等級制度は 2000 年ごろから整備が始められ、これに関連した国家標準規格(GB 規格)も次々と追加、改訂されている。これまで特に重視されることはなかったが、情報セキュリティの強化を目的としたサイバーセキュリティ法の施行をきっかけに、当局が認定取得の徹底を呼び掛けている。

2. 情報システムのセキュリティ等級とは

2007 年 6 月に発表された「情報セキュリティ等級保護管理弁法(信息安全等级保护管理办法)」では、第 7 条において 5 段階のセキュリティ等級を示している。

1級	情報システムが破壊された場合、公民、法人、その他組織の合法的な利益を損なうが、国家の安全、社会秩序、公共の利益に影響しない。
2級	情報システムが破壊された場合、公民、法人、その他組織の合法的な利益を著しく損う、あるいは社会秩序と公共の利益を損うが、国家の安全に影響しない。
3級	情報システムが破壊された場合、社会秩序と公共の利益を大きく損なう、あるいは国家の安全に損害をもたらす。
4級	情報システムが破壊された場合、社会秩序と公共の利益を著しく損なう、あるいは国家の安全に大きな損害をもたらす。
5級	情報システムが破壊された場合、国家の安全に著しい損害をもたらす。

この等級分けは 2008 年に発表された国家標準規格「情報セキュリティ技術情報システムセキュリティ等級保護基本要求(信息安全技术信息系统安全等级保护基本要求

GB/T22239-2008)」や「情報システムセキュリティ等級保護分類ガイド(信息安全技术信息系统安全等级保护定级指南 GB/T22240-2008)」にも掲載されている。

同ガイドによれば、業務データと情報システムを使ったサービスのセキュリティ等級は、いずれも損害を受ける対象と損害の程度によって次の表のように決まる。判断の優先順位は、まずは国家の安全、次に社会秩序、公共の利益、最後に公民・法人・その他組織の合法的利益となる。

損害を受ける対象	損害の程度		
	普通の損害	大きな損害	著しい損害
公民、法人、その他組織の合法的利益	1級	2級	2級
社会秩序、公共の利益	2級	3級	4級
国家の安全	3級	4級	5級

損害を受ける対象の具体的な例は次の通りとなっている。

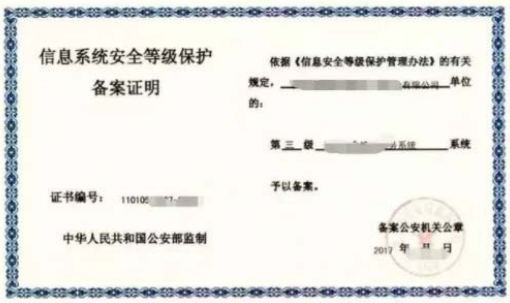
公民、法人、その他組織の合法的利益
法律の保護を受けた公民、法人、その他組織が享受する社会的な権利と利益
社会秩序
・国家機関による社会管理と公共サービス業務の秩序 ・各種経済活動の秩序 ・各産業の科学研究、生産の秩序 ・公衆が法律や道徳のルールの下で正常に生活する秩序 ・その他の社会の秩序
公共の利益
・公共施設の利用 ・公開情報の取得 ・公共サービスの享受 ・その他公共の利益

国家の安全
・政権の安定および国防力 ・国家の統一、民族の団結、社会の安定 ・国家の対外活動中の政治的、経済的利益 ・国家の重要な安全保障作業 ・国家の経済競争力および科学技術力 ・その他国家の安全に影響する事項

また損害の程度に関する定義は次のようになっている。

普通の損害	機能が一部影響を受け、業務能力が低下するが、主要な機能の執行に影響はない。軽微な法的問題が発生し、財産の損失もあるが、社会への悪い影響は限られており、その他組織や個人への損害は少ない。
大きな損害	機能が大きな影響を受け、業務能力が大幅に低下し、主要な機能の執行にも大きな影響がある。深刻な法的問題が発生し、財産の損失も大きく、社会への悪い影響も比較的広い範囲に及び、その他組織や個人への損害も大きい。
著しい損害	機能が特に著しい影響を受けるか、あるいは執行能力を喪失し、業務能力が著しく低下したり、機能が執行できなくなる。特に深刻な法的問題が発生し、財産の損失も莫大で、社会への悪い影響も大きな範囲に及び、その他組織や個人への損害も非常に大きい。

実際にどの等級に該当するのかは、情報システムの運営者や使用者が「情報セキュリティ等級保護管理弁法」と「情報システムセキュリティ等級保護分類ガイド(信息安全技术信息系统安全等级保护定级指南 GB/T22240-2008)」を参考に決めてよい。2 級以上であれば公安に届出登録を行い、審査で認定されれば、証明書が発行される。ただし、省を跨ぐか全国統一で運用されるシステムについては、主管部門が等級を決める。4 級以上に該当すると思われるシステムは、運営者か使用者、あるいは主管部門が当局の専門家委員会に判断を仰ぐとしている(10 条)。


信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，[redacted]单位的：

第三级 [redacted] 系统

予以备案。

证书编号：[redacted]

中华人民共和国公安部监制

备案公安机关公章

[redacted] 年 [redacted] 月 [redacted] 日

セキュリティ等級の届出登録証明書の例

先の 4 級を取得した「騰訊雲」の金融クラウドプラットフォームは、主に金融サービスで利用されることから、サイバー攻撃を受けたり災害などで損害を受ければ、4 級に該当する“社会秩序と公共の利益を著しく損なう、あるいは国家の安全を大きく損なう”可能性があるというわけだ。

なお、ここでいう「情報システム」の定義は、「情報セキュリティ等級保護管理弁法」の上位法である「コンピューター情報システムセキュリティ保護条例(**计算机信息系统安全保护条例**)」で定められており、「コンピューターおよびこれに関連する周辺機器とネットワークを含む設備で構成されたもので、特定のプログラムに従ってデータの収集、加工、保存、送信、検索等の処理を行うマン・マシンシステム」となっている(2 条)。同条例は 1994 年 2 月に施行されたもので、2011 年に条文中の処罰の根拠となる法令の名称を訂正しているが、その他の内容は 20 年以上変わっていない。

3. 必要なセキュリティ保護とは

「情報セキュリティ等級保護管理弁法」の第 8 条において、情報システムの運営者や使用者に対し、当該システムの等級に応じたセキュリティ保護を行うよう求めている。

具体的には、1 級に該当する情報システムの場合、運営者あるいは利用者自身で管理規範や技術標準を元にセキュリティ対策を行えばよいが(自主保護レベル)、2 級の場合は自身でセキュリティ対策を行った上で当局が指導すること(指導保護レベル)、3 級はさらに当局が監督、検査を行うこと(監督保護レベル)、4 級は業務に応じたセキュリティ対策を行い、当局が強制的な監督および検査を行うこと(強制保護レベル)、5 級ではさらに強固なセキュリティ対策を行い、国家が指定した専門部門が監督および検査を行うこと(専門制御保護レベル)、としている。

また、情報システムの稼働中も定期的にセキュリティ等級の見直しと保護対策の実施状況について検査を行う必要があり、3 級に該当するシステムは少なくとも年に 1 回、4 級は少なくとも半年に 1 回、5 級ならば別途定められる基準に沿ったタイミングでの実施が必要となる(14 条)。

さらに 3 級以上の情報システムでは、使用する機器にも次の条件がある(21 条)。

- 製品の研究開発・生産メーカーが、中国公民または中国法人の投資により設立さ

れているか持ち株会社で、中国国内に独立した法人資格を有していること。

- 製品の基幹技術や基幹部品が中国の知的財産権を有していること。
- 製品の研究開発・生産メーカーとその主要事業、技術者に犯罪記録がないこと。
- 製品の研究開発・生産メーカーが、ぜい弱性、バックドア、トロイの木馬等のプログラムや機能を故意に放置または設置していないとの声明を出していること。
- 国家の安全、社会秩序、公共の利益に危害を与えないこと。
- 情報セキュリティ製品認証目録に掲載されている製品については、国家情報セキュリティ製品認証機構の認証証書を取得していること。

具体的にどのようなセキュリティ設計が必要かについては、「情報セキュリティ技術情報システム等級保護セキュリティ設計技術要求(**信息安全技术信息系统等级安全设计技术要求** GB/T25070-2010)」が参考になるだろう。

例えば 4 級のシステムでは、ログインひとつとっても「ユーザーがシステムにログインあるいは再接続するたびにパスワード、生体識別データ、デジタル証明書等セキュリティの高いものを 2 つか 2 つ以上組み合わせて認証を行い、このうち 1 つの識別データは代替不可で、かつ識別データの機密性と完全性が保たれていること」となっている。このほかのシステムやネットワークに関する技術的な要求に加え、セキュリティ管理制度、人員体制、メンテナンスといった管理運用面にも詳細な条件が示されている。

先ほども例を挙げた「騰訊雲」の金融クラウドプラットフォームの場合、上述したような 4 級で求められるセキュリティ対策が取られている。逆に言えば、4 級程度のセキュリティしかないため、ここに 5 級に該当するような重要なデータは保存できないわけだ。実際、PtoP レンディング(ソーシャル融資)の分野では、今まで 2 級の取得で済ませていたところ、個人情報や取引情報を扱うことから、金融機関が運営するものを中心にすでに 150 あまりのサービスが 3 級を取得しているという。

3級取得済みのPtoPレンディングサービスの例
51人品(江西银行)
e路同心(上海银行)
e兴金融(浙商银行)
PP money(厦门银行)
爱贷网(恒丰银行)
爱钱进(华夏银行)
爱投资(新网银行)
大唐普惠(广州大唐普惠互联网金融信息服务有限公司)
为为贷(沈阳尚合电子商务)
中融宝(建设银行)

互金毎日早知道のデータをクララオンライン加工

このほか、地方独自のセキュリティ保護条例や業界・産業ごとのガイドライン等で、対応すべきセキュリティ対策や目標とする等級が決められていることがある。例えば水道関連事業者向けに水利部が発表した「ネットワークと情報セキュリティ体系建設基本技術要求」では、都市部の水資源リアルタイム監測システムについて 2 級または 2 級以上、ダムや灌漑などの水利開発プロジェクトに関する情報システムについて 3 級、水道関連事業者の内部ネットワークおよび日常業務に用いるシステムについて 2 級などと定めている。

4. クラウドにも対応した“セキュリティ等級保護 2.0”

現行の基準ではセキュリティを担保できないクラウド、モバイルインターネット、IoT、産業用コンピューター(IPC) 、ビッグデータといった分野をカバーするため、公安部などは 2014 年ごろから「情報セキュリティ技術情報システムセキュリティ等級保護基本要求(GB/T22239-2008)」の拡張を検討してきた。

阿里巴巴集団(アリババグループ)のクラウドサービス「阿里雲(Alyun)」は、クラウドサービスに関する拡張規格の編集に携わるとともに、2016 年 10 月にクラウドサービスとしては初めてセキュリティ等級の認定を受け、阿里雲電子政務クラウドプラットフォームはクラウド等級保護 3 級、阿里雲金融クラウドは同 4 級が認められている。

この“セキュリティ等級保護 2.0”と呼ばれる拡張規格は、すでにひな形が出来上がっておりインターネット上で公開されている。

——GB/T 22239.1-XXXX 信息安全技术 网络安全等级保护基本要求
第 1 部分 安全通用要求；
——GB/T 22239.2-XXXX 信息安全技术 网络安全等级保护基本要求
第 2 部分 云计算安全扩展要求；
——GB/T 22239.3-XXXX 信息安全技术 网络安全等级保护基本要求
第 3 部分 移动互联安全扩展要求；
——GB/T 22239.4-XXXX 信息安全技术 网络安全等级保护基本要求
第 4 部分 物联网安全扩展要求；
——GB/T 22239.5-XXXX 信息安全技术 网络安全等级保护基本要求
第 5 部分 工业控制安全扩展要求；
——GB/T 22239.6-XXXX 信息安全技术 网络安全等级保护基本要求
第 6 部分 大数据安全扩展要求。

クラウド、モバイルインターネット等への追加規格が記されている

ひな形では、第 2 部分でクラウドサービスに触れている。一部抜粋すると、現行の規定ではセキュリティ対策の責任は情報システムの運営者･使用者が単独で負うことになっているが、クラウドサービスについてはサーバー提供側とサーバー利用者側のそれぞれが責任を負う範囲が明確に示されている。

また、等級認定の対象がこれまでは情報システムと関連するインフラネットワークだけだったのに対し、クラウドプラットフォームとクラウド上で運用するシステムを別々に等級認定することとされた。プラットフォームの等級が、運用するシステムの等級より低くてはならないことから、システムの移行を検討する場合は先にシステムの等級を確認したのち、同じかそれ以上の等級のプラットフォームを探して移行することになる。

さらにクラウドサービスではセキュリティ保護の対象が増えている。例えばネットワークおよび通信について、現行規定の対象は「ネットワーク設備、セキュリティ設備、ネットワークトポロジー、総合ネットワーク管理システム」であるが、これに仮想トポロジー、仮想ネットワーク、仮想化ベースセキュリティ、VMM、クラウド管理プラットフォームが追加される。

この“セキュリティ等級保護 2.0”は、2016 年 10 月に開かれた全国情報セキュリティ等級保護技術大会において、公安部の担当者が近いうちに正式発表すると発言していた。間もなく 1 年が経とうとしているが、先日施行されたサイバーセキュリティ法などとの調整で発表が遅れている可能性もある。いずれにせよ、当局が認定取得を呼び掛けており、どのサービスが何級をとったというニュースが数多く流れるようになったことから、年内にも発表される可能性は高そうだ。

- 本レポートに含まれる情報は一般的なご案内であり、包括的な内容であることを目的としておりません。また法律・条令の適用と影響は、具体的な状況によって大きく変化いたします。具体的な事業展開にあたってはクララオンライン コンサルティングサービスチームより御社の状況に特化したアドバイスをお求めになることをおすすめいたします。また本書の内容は 2017 年 7 月 10 日時点で編集されたものであり、その時点の法律及び情報、為替レートに基づいています。

本書はクララオンライン コンサルティングサービスチームにより作成されたものです。クララオンラインの中国、台湾、韓国、シンガポールなどアジア各国のインターネットコンサルティングサービスに関するお問い合わせは以下の連絡先までお気軽にご連絡ください。

asia@clara.ad.jp または +81(3)6704-0776