CLARA ONLINE China Business Report
2019.9.10

サイバーセキュリティ法の執行事例

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>

中国でサイバーセキュリティ法が施行されて 2 年余りが経った。しかし日本においては、EU 一般データ保護規則(GDPR)などに比べて内容に対する意識はまだ高くないようだ。実際に執行されているのか疑う声も聞こえるが、施行からわずか 3 カ月で大手 IT 企業が処分されており、現在まで積極的な取り締まりが続いている。

全ての事例が公表されているわけではないが、関連規定が定まらない現時点では、主にセキュリティ対策、有害情報の扱い、個人情報保護で処分を受けるケースが多い。違反が発覚するきっかけとなるのは、サイバー犯罪の捜査中、あるいは当局の定期検査や集中取り締まりなどが多い。政府はインターネットユーザーに違反行為の通報を奨励しており、これがきっかけとなることもある。

大企業を中心に多くの企業が対策を済ませているが、目下検討が進められている関連法規が正式発表されれば、本格的に指導や取り締まりが始まる可能性は高い。まだ対策が十分でない場合、必要に応じて専門家の判断を仰ぎ、現時点でできる限りの措置を行って備えることが望まれる。

1. サイバーセキュリティ法の施行から 2 年

サイバーセキュリティ法が 2017 年 6 月 1 日に施行されて、はやくも 2 年余りが経った。いまだに決定していないガイドラインや細則も多く、意見募集稿の段階で 2 年近く時間が経ったものもある。

そのような状況であっても、中国でビジネスを行う事業者は法令順守を求められるが、日本側とりわけ日本の本社や親会社の中で、サイバーセキュリティ法についての認識はまだ十分とは言えないようだ。中国でサイバーセキュリティ法違反の大事件が起きて日本でも報道されれば別だが、関連法規がまだ整備されていないためなのか、実際にこれで取り締まりを受けることがあるのか、そもそもきちんと執行されているのか、といった声も聞かれる。

結論から言えば、施行から 3 カ月で複数の大手 IT 企業が処分を受けており、その後も管轄当局や各地の公安局が積極的な取り締まりを行っている。差し当たっては明らかにサイバーセキュリティ法の規定に背いているケースが警告や過料の対象だ。また以前であれば他の法令に基づいて処罰されていたケースでも、現在は IT 領域で最も上位として扱われる法令がサイバーセキュリティ法であることから、サイバーセキュリティ法違反として処分されることもある。

2. 違反事例

これまでにサイバーセキュリティ法違反を理由として処分が行われた事件をいくつか紹介しよう。なお日本でもそうであるように、全ての事例の詳細が公表されているわけではないため、実際にはかなりの数の指導や処分が行われている可能性がある。

- セキュリティ対策の未実施：2017 年 6 月

山西省忻州市政府の直属事業法人の WEB サイトに対し SQL インジェクション攻撃が行われているとして、国家ネットワーク情報セキュリティ通報センターに複数の通報があり発覚した。忻州市公安局は当該サイトの運営者に対し、サイバーセキュリティ法 11 条、59 条に違反しているとして、現場調査を行い、改善命令を出すとともに行政警告処分とした。

- 有害情報の流布：2017 年 8 月

騰訊(テンセント)、新浪微博、百度貼吧の 3 社は、サイバーセキュリティ法 47 条で流布を禁じているわいせつ、民族的な恨み、テロリズムに関する情報や評論といった有害情報を書き込んだユーザーアカウントに適切な対処をしなかったため、これらの情報が広く流布したとして、各社の所在地のネットワーク情報弁公室は 3 社にそれぞれ最高額の過料を科した。

騰訊のサイバーセキュリティ法違反を報じる微信の記事

● ログの保存義務違反：2017 年 8 月

重慶市に拠点を置くデータセンター運営会社が、サイバーセキュリティ法で求められているログインに関するログを保存していなかったため、重慶市公安局ネットワークセキュリティチームから警告を受け、15 日以内の改善を命じられた。重慶市で初の摘発となった。

運営会社側は公安局から行政処罰通知書を受け取った後、直ちに改善方案を作成した。作業の完了後には公安局が改善状況の検収を行った。

● セキュリティ等級保護制度の未実施：2017 年 8 月

四川省公安局は、宜賓市教師トレーニング教育研究センターが運営する WEB サイト「教師発展プラットフォーム」について、サイバーセキュリティ法に定められたネットワークセキュリティ等級保護制度の届出登録や等級評価作業等を実施しておらず、セキュリティ保護義務を怠ったとして、法人に対して過料 1 万元、法人の代表者個人に対して過料 5,000 元を科した。

● セキュリティ等級保護制度の未実施：2017 年 8 月

安徽省蚌埠市公安局は、懐遠県教師進修学校の WEB サイトがハッカーに攻撃されたため調査を行ったところ、被害にあった WEB サイトはサイバーセキュリティ法で定められたネットワークセキュリティ等級保護制度の届出登録や等級評価作業を実施しておらず、セキュリティ保護義務を怠ったとして、学校に対して過料 1 万 5,000 元、直接の責任者である副校長に過料 5,000 元を科した。

その後もセキュリティ等級保護制度が実施されなかったため、学校に対してさらに過料 1 万 5,000 元、副校長に過料 5,000 元を科し、地元政府の担当者である副県長にも改善を約束させた。

● セキュリティ対策の未実施：2017 年 8 月

黒竜江省ハルピン市公安局は、方正県政府農業技術推広センターが運営する「方正農

業社会科サービスプラットフォーム」がハッカーの攻撃を受けたことについて調査を行った結果、プラットフォームの開設以来メンテナンスが行われておらず、セキュリティ対策も実施されていなかったことが明らかになった。公安局はサイバーセキュリティ法の規定に違反したとして、同センターに改善を求めるとともに、過料 2 万元を科した。

- 実名登録の徹底義務違反：2017 年 9 月

広東省通信管理局は、阿里雲計算有限公司(Aliyun)がサイバーセキュリティ法 24 条に違反しているとして、改善命令を出した。同社はインターネット接続サービスを提供する際に、ユーザーに真実の身分情報の登録を求めなければならないが、これを徹底していなかった。

同じく、三人網絡科技有限公司もサイバーセキュリティ法 24 条、61 条、および電話ユーザーの真実の身分情報登記規定 17 条に違反しているとして、改善命令を出すとともに、過料 5 万元、7 日間以下の営業停止およびサイトの閉鎖を命じた。同社は、ユーザーに真実の身分情報の登録を求めないまま IP 電話サービスを提供した。

- 有害情報の流布：2017 年 9 月

広東省通信管理局は、広州荔支網絡技術有限公司が、サイバーセキュリティ法 47 条、68 条およびインターネット情報サービス管理弁法 16 条、23 条に違反しているとして、改善命令を出すとともに処罰を警告した。同社は、運営するサービスプラットフォームを利用してユーザーが流布した有害情報を放置し、情報の拡散を防止しなかった上、関連する記録を保存して主管部門に報告しなかった。

- セキュリティ対策義務違反：2017 年 9 月

広東省通信管理局は、動景計算機科技有限公司が、サイバーセキュリティ法 22 条に違反しているとして、改善命令を出すとともに、セキュリティ評価を実施し、他の運営サービスについても全面的なセキュリティ検査を実施するよう求めた。同社は運営するブラウザー関連サービスにセキュリティホールが見つかったが、これを速やかに修正しなかったため、有害情報の流布に利用された。

● セキュリティ対策義務違反：2017 年 9 月

安徽省淮南市公安局は、淮南職業技術学院のシステムにあるセキュリティホールが原因で、システムに保存している学生 4,000 人余りの個人情報が漏洩したとして、現場検査を行った。その結果、同校がセキュリティ管理制度を設けておらず、必要なセキュリティ対策をとっていなかった上、ログの保存期間が規定の 6 カ月に満たず、データのバックアップや暗号化を行っていなかったことが判明した。公安局は同行がサイバーセキュリティ法の規定に違反したとして、改善命令と行政警告を行った。

● 個人情報の違法な売買：2018 年 3 月

湖南省株洲市公安局は、2017 年 11 月に湖南工貿技師学院が運営する公式サイトについて、重大なセキュリティ上の欠陥があることを発見した。サイトの制作とメンテナンスを請け負っている市内の IT 企業を検査したところ、サイバーセキュリティ法に定められたセキュリティ対策を実施していないことが発覚したため、2018 年 2 月までに改善するよう求めた。

しかし 3 月末に公安局が再度検査を行ったところ、サイトの修正やセキュリティ対策が行われないままだったことが明らかになったため、サイバーセキュリティ法 21 条、25 条、59 条に違反しているとして行政警告の処分とし、改善が確認されるまではサイトを閉鎖するよう求めた。

● セキュリティ保護義務違反：2018 年 5 月

雲南省大理ペー族自治州に拠点を置くある企業の WEB サイトが、ハッカーの攻撃を受け改ざんされた。公安局はハッカーの捜査をする一方で、被害企業のセキュリティ対策実施状況についても調査を行ったところ、必要な対策が全く取られていなかったことが発覚した。

被害企業はサイバーセキュリティ法 21 条、59 条およびコンピューター情報ネットワーク国際聯網セキュリティ保護管理弁法の 12 条、21 条、23 条に違反していたとして、警告および過料を科すとともに、同社のセキュリティ責任者個人に対しても過料を科し、速やかな改善を求めた。

● 個人情報の違法な売買：2018 年 7 月

四川省内江市威遠県公安局が、県内に拠点を置く内装会社が個人情報を違法に購入していることを発見し調査を行ったところ、県内のマンションの販売担当者から住民およそ 5,000 人分の個人情報を購入していたことが明らかになった。内装工事の電話セールスを行うためだったという。公安局はサイバーセキュリティ法の個人情報に関する規定に違反するとして、内装会社の責任者に刑事責任を追及するとしている。

● セキュリティ対策の未実施：2018 年 12 月

江西省徳興市公安局は、市内に拠点を置く江西福聖元生物化学技術有限公司が適切に ICP 登録を行っていないことを発見した。調査を行ったところ、同社の公式サイトは ICP 登録だけでなく、セキュリティ管理も実施されていなかったためにハッカーにサイトを乗っ取られ、違法賭博サイトに書き換えられていたことが明らかになった。公安局はサイバーセキュリティ法 59 条に違反しているとして、同社に警告を行い、改善を要求した。現在同社のサイトは運営を停止している。

● 有害情報の流布：2018 年 12 月

陝西省延安市甘泉県公安局は、市内に住む女性が微信(WeChat)を通じて違法行為を行っていることを発見し調査を行ったところ、タバコや賭博ゲーム、医薬品等を複数回にわたって違法に販売していたことが発覚した。公安局はサイバーセキュリティ法 46 条に違反しているとして、犯人の女性を 5 日間の行政拘留に処した。

● プライバシーポリシーの表示義務違反：2019 年 7 月

全国情報セキュリティ標準化技術委員会などが組織する違反アプリの摘発専門チームは、次の 10 件のアプリがサイバーセキュリティ法 41 条で定められたプライバシーポリシーを表示していないとして、アプリとその運営会社を公表し、30 日以内の改善を求めた。違反が認められたのは、中国銀行手機銀行、春雨医生、魔漫相機、淘粉吧、当当雲閲読、我愛我家、愛鮮蜂、北京預約掛号、韻達快逓、北京交通のアプリ。

あわせて、同じく 41 条に違反して、一度に複数の個人情報収集許可を求め、同意し

なければインストールできない仕様にしているとして 20 件のアプリの名称と運営会社を公表した。

- セキュリティ対策義務違反：2019 年 7 月

湖南省衡陽市衡山県公安局は、県内のある企業が運営する FTP サーバーがウイルスに感染し、ハッカーによって改ざんされたことが発覚したことから、サイバーセキュリティ法違反として期限付きの改善命令をだした。しかし 3 週間後に同社のサーバールームを検査したところ、セキュリティ対策を実施しておらず、セキュリティホールが放置されたままになっていたことから、サイバーセキュリティ法の規定に違反したとして、再度改善命令を出すとともに過料 1 万元を科した。

3. 現時点でできる限りの対策を

サイバーセキュリティ法の関連規定が定まらない現時点では、主にセキュリティ対策、書き込みや流布が禁止されている有害情報の扱い、個人情報保護で行政処分を受けるケースが多いようだ。

処罰を受けたすべての事案が公開されているわけではないが、サイバー犯罪やセキュリティインシデントが発生して捜査が行われたり、あるいは公安局の定期検査や集中取り締まりで発覚したりするケースが多いことが伺える。近年は、政府が一般消費者やユーザーに違反行為の通報を奨励しており、これをきっかけに調査が行われるケースもある。とりわけ日本企業を含む外資系企業は、政治的に関係が悪化すれば、容易にターゲットにされてしまう可能性も忘れてはいけない。中国でビジネスを行っている企業だけでなく、日本に拠点を置いたまま中国向けにビジネスを行っている場合でも、サイバーセキュリティ法の適用対象となる可能性があるため注意が必要だ。

サイバーセキュリティ法では、違法行為が認められた場合、まずは是正を命じる警告が行われる。すみやかに是正しないか情状が深刻な場合は、過料又は業務停止や営業許可の取り消し処分が行われる。加えて、企業や個人の信用情報に不良記録が記載され、公示されることになる。他人に損害を与えた場合には、民事責任や刑事責任も追及される。

現時点では、セキュリティ対策、禁止情報の扱い、個人情報保護に関する対策を軸に、業種や業態に応じて必要なその他の対応を行うことが必須となる。検討が進められている関連法規のうち、意見募集が済んだものだけで 10 近くある。近い将来これらが正式発表されれば、本格的に指導や取り締まりが行われるようになることは想像に難くない。

施行から 2 年以上が経ち、すでに多くの企業が対策を済ませて、より具体的な対応のために関連法規の動向を注視している状況だ。対策がまだ十分でない企業は、自社が規定の対象に該当するのか慎重に判断し、必要に応じて専門家の判断を仰いで現時点でできうる限りの措置を行っておくことが望ましい。

- 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 2019 年 9 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ビジネス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。

sales@clara.ad.jp または +81(3)6704-0777(代表)