特集／米中の規制等を巡る諸動向

〈1〉中国ネットワーク製品のセキュリティ脆弱性管理規定を読む

～日本の脆弱性関連情報の取扱制度との比較から～

一般社団法人 JPCERT コーディネーションセンター[1]
早期警戒グループ マネージャ　脅威アナリスト
佐々木　勇人

国際部　脅威アナリスト
米澤　詩歩乃

１．はじめに

2021 年 12 月 9 日（日本時間 10 日未明）に Java ベースのオープンソースのロギングライブラリ[2] である、Apache Log4j に深刻な脆弱性が見つかったことが公表され、世界各国の IT／セキュリティ業界関係者が対応に追われた。このライブラリが多くのソフトウェア製品やオンラインサービスに使われていることや、悪用した攻撃が非常に容易であることから、世界的に大きな衝撃を与えた。JPCERT コーディネーションセンターからも 11 日土曜日に緊急の注意喚起を発行し、対応にあたった次第である。

この脆弱性を発見したのは中国アリババのグループ企業である、Alibaba Cloud のセキュリティチームであった。彼らは 2021 年 11 月 24 日に、このライブラリを管理している Apache Software Foundation[3] にこの脆弱性の報告を行っている。その後、経緯は不明ながら、12 月 9 日に海外のリサーチャーによる本脆弱性に関する Twitter 上の投稿が行われ、Alibaba Cloud のセキュリティチームも本脆弱性について公表するに至った。以上のような経緯から、影響範囲の広さもさることながら、修正版が公表される前に、脆弱性の存在が明らかになったことで大きな混乱が発生してしまった事象であった。

その後、South China Morning Post[4] やロイターが報じたものとして、中国工業情報化部が、アリババクラウドが本件脆弱性情報を速やかに報告しなかったとして、提携関係を 6 か月間停止する処分を発表したとする情報が流れた。これは、ネットワーク製品の脆弱性に関する報告等を定めた「ネットワーク製品のセキュリティ脆弱性管理規定[5]」（中国名：网络产品

[1] 本稿は筆者の所属元での活動知見を踏まえて執筆しているが、ここで述べる見解等は必ずしも組織を代表するものではない。また、本稿で取り上げる中国側法令の用語の翻訳については、執筆者による仮訳である点をご了承いただきたい。
[2] システムの様々なログ（動作履歴やアクセス履歴など）を記録（ロギング）するためのプログラムの集まりのこと
[3] 世界中の IT システムでオープンソースソフトウェアが広く活用されているところ、オープンソースソフトウェアの開発・管理はボランタリーなコミュニティ活動等が担っていることが多くその中でも大規模に活動しているオープンソースソフトウェア・コミュニティの一つ。元々は Web サーバソフトウェアの Apache HTTP Server の開発・管理のために発足したが、その後活動が拡大し、Log4j などの他のソフトウェアプロジェクトも担当している。
[4] 海外メディアが最初に参照したのは、香港の 21 世紀経済報道（中国名：21 世纪经济报道）の速報と思われる。ちなみに、これを引用して報じた、South China Morning Post 紙は香港の英字紙であるが、2015 年からアリババグループ傘下にある。
[5] 中华人民共和国国家互联网信息办公室「网络产品安全漏洞管理规定」http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm

安全漏洞管理規定)が 2021 年 9 月から施行されたことが念頭にあったものと思われる[6]。

しかし、その後、この報道に関する続報はなく、また、当局からの処分内容を示す公表資料も見つかっていない。また、これらの報道の根拠が不正確であったり、あるいは憶測記事なのではないか、とする指摘の声[7]も上がっている。果たして、アリババクラウドはどのような理由で処分を受けたのか、現時点では詳細は不明である。

近年、中国のベンダー、研究者による脆弱性発見の数が増えており、今回の Log4j 脆弱性発見に係る経緯は不明ながら、世界的に大きな影響を及ぼす可能性のある脆弱性を中国の研究者等が見つけた際の当局の動向に世界中から大きな注目が集まっていることを象徴する事案であったと言える。

本稿では、「ネットワーク製品のセキュリティ脆弱性管理規定」について、同じくソフトウェアの脆弱性情報の取り扱いについて定め、既に 10 年以上の制度運用がなされている日本国内の制度との比較を行い、どのような点が国内制度と異なるのかを中心に解説していきたい。

2．日本国内における脆弱性情報の取り扱い制度

日本国内においては、2004 年に経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」（以下、「脆弱性取扱告示」と記す）に基づく、「情報セキュリティ早期警戒パートナーシップ」という制度が運用されており、脆弱性発見者、報告先・調整機関、製品開発者の 3 者間における調整や脆弱性情報の公表に向けた取り組みが行われている。

ソフトウェアは製造物責任法（いわゆる PL 法）における製造物の対象にはなっておらず[8]、ソフトウェアの脆弱性についてメーカーに対して何らかの強制力を持つ法制度はなく、基本的には前述の通り経済産業省告示に基づく制度の下、発見者、調整機関、製品開発者との連携により対応が行われている。

当該告示では、脆弱性情報の公表に向けた、発見者、受付機関（IPA）、調整機関（JPCERT/CC）、製品開発者の間における脆弱性情報の取り扱いが示されている。具体的な手続きなどの運用に関する詳細は「情報セキュリティ早期警戒パートナーシップガイドライン」[9]が定められており、脆弱性情報のハンドリングにおいて何らかの新しい問題が出て来た場合などは、IPA に設置された「情報システム等の脆弱性情報の取扱いに関する研究会[10]」で有識者や経済産業省、JPCERT/CC とともに検討がなされ、ガイドラインの更新が行われている。

前述の通り、この制度においては、国の告示に基づくものとはいえ、何らかの法的な義務や罰則を定めたものではなく、ガイドラインに沿わない対応を行った脆弱性発見者や製品開発者に対してなんらペナルティが発生するものではない。各プレイヤーに求められる「役割」、脆弱性情報の公表という「目標」、脆弱性情報という「情報の取扱い方」がそれぞれ示されており、各プレイヤー間で共通して参照で

---

[6] 一部国内メディアでは、中国当局への報告の根拠として「サイバーセキュリティ法」第 25 条を示しているものが見受けられたが、同条はネットワーク運営者に対するものであり、主にインシデント発生時の報告に関する事項である。「ネットワーク製品のセキュリティ脆弱性管理規定」の根拠となっている、脆弱性発見時の当局への報告は同法 22 条による。

[7] https://note.com/note_s/n/n21ddfc5e91c2

[8] 製造物責任法における「製造物」は「製造又は加工された動産」（第二条 1 項）と定義されているところ、ソフトウェアは無体物であり法の対象外となっている。一方で、「ソフトウェアの不具合が原因で、ソフトウェアを組み込んだ製造物による事故が発生した場合、ソフトウェアの不具合がその製造物自体の欠陥と解されることがあり、この場合、その欠陥と損害との間に因果関係が認められるときには、その製造物の製造業者等にこの法律による損害賠償責任が生じる場合がある」、とされている。
参考：消費者庁「製造物責任法の概要 Q & A」
https://www.caa.go.jp/policies/policy/consumer_safety/other/pl_qa.html

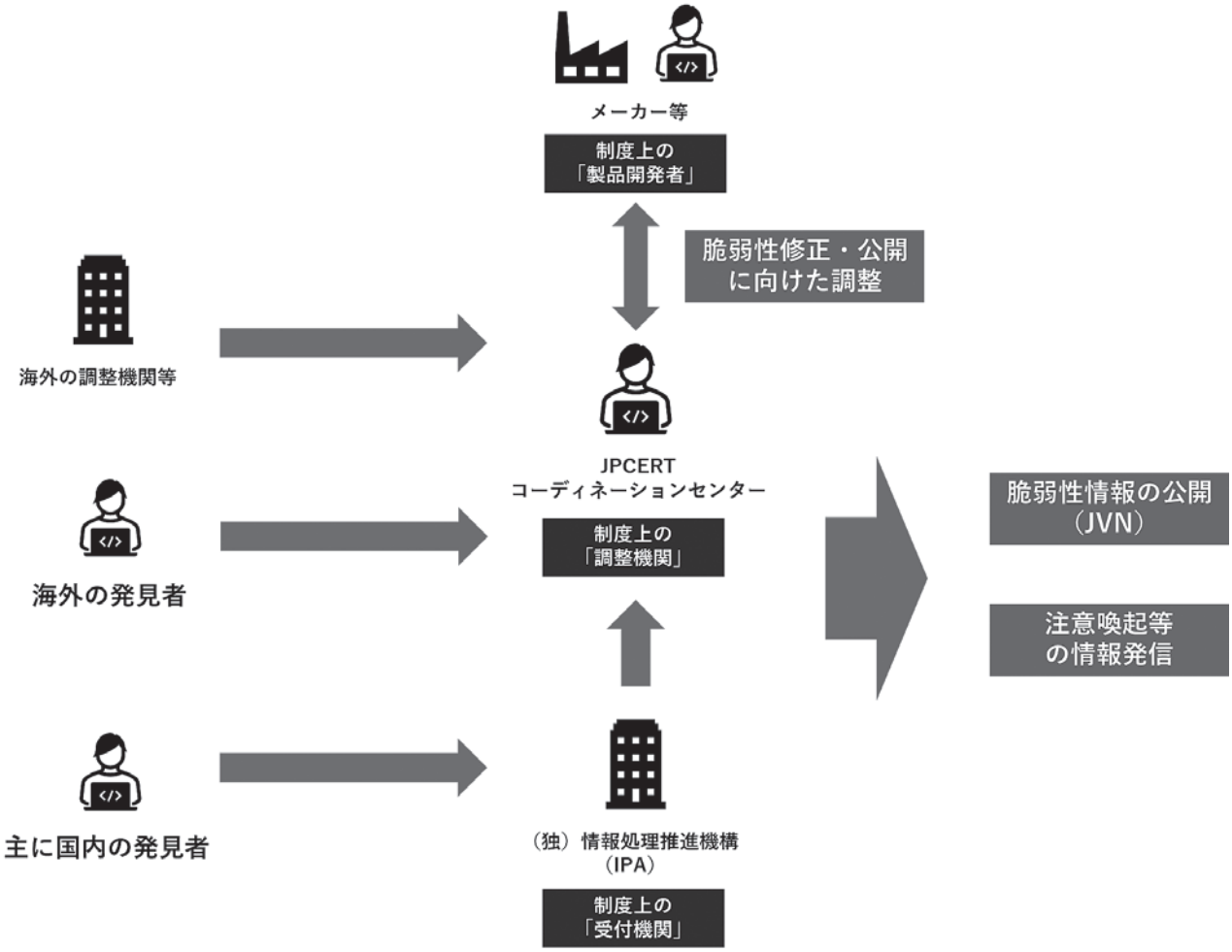
[9] IPA、JPCERT/CC 情報セキュリティ早期警戒パートナーシップガイドライン
https://www.jpcert.or.jp/vh/top.html#guideline
https://www.ipa.go.jp/security/ciadr/partnership_guide.html

[10] 毎年度開催されるところ、以下は 2021 年度研究会に関する報告である
2021 年度情報システム等の脆弱性情報の取扱いに関する研究会 https://www.ipa.go.jp/security/fy2021/reports/vuln_handling/research_2021.html

きる、ガイダンスの機能を有していると言える。特に、初めて脆弱性を見つけた発見者や、初めて自社製品の脆弱性公表を行う製品開発者が「何をしたらいいかわからない」場合のガイダンスとして使われている。

海外においては、同様の脆弱性情報の取扱いを定めた制度が運用されてこなかったところ、日本においては各プレイヤーの任意の協力に基づく制度運用が長年行われてきているのである。

図：告示制度における関係者間の役割について



３．中国における関連法令の概要・経緯

中国政府はここ数年、国の安全保障を目的としてサイバー空間にかかる法体制を急速に整えている。その初めとして、2017 年 6 月 1 日にサイバーセキュリティに関する基本法となる「中国サイバーセキュリティ法[11]」が施行され、2021 年には、「中国個人情報保護法」と「中国データセキュリティ法」が成立し、中国のネットワークとデータのセキュリティに関連する重要な 3 つの柱となる基本法が揃った。

サイバーセキュリティ法では、サイバー空間における主権の保護や国家安全保障、社会の公共利益の保護などを目的として、ネットワーク運用におけるセキュリティの保護、個人情報の保護、重要情報インフラの保護、緊急時の対応などについて、政府の監督機関やネットワーク運営者などの主要な責務とされる事項がまとめられている。また、違反した場合の罰則も定められているため、強制力をもつ法律

[11] 中华人民共和国国家互联网信息办公室「中华人民共和国网络安全法」
http://www.cac.gov.cn/2016-11/07/c_1119867116.htm