西村高等法務研究所「CLOUD Act 研究会」報告書
【参考資料】 引用条文集

Ⅰ. CLOUD Act[1](→第 3.、第 4.、第 6.)

SEC. 103. PRESERVATION OF RECORDS; COMITY ANALYSIS OF LEGAL PROCESS.

(a) REQUIRED PRESERVATION AND DISCLOSURE OF COMMUNICATIONS AND RECORDS.—

(1) AMENDMENT.—Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

"§2713. Required preservation and disclosure of communications and records

"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.".

(2) (略)

(b) COMITY ANALYSIS OF LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—Section 2703 of title 18, United States Code, is amended by adding at the end the following:

"(h) COMITY ANALYSIS AND DISCLOSURE OF INFORMATION REGARDING LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—

"(1) (略)

"(2) Motions to quash or modify.—

(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes—

"(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

"(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government. (略)

---

[1] Clarifying Lawful Overseas Use of Data Act, *available at* https://www.justice.gov/dag/page/file/1152896/download)

"(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that—

"(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

"(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

"(iii) the customer or subscriber is not a United States person and does not reside in the United States.

"(3)~(5) (略)"

(c) RULE OF CONSTRUCTION.—Nothing in this section, or an amendment made by this section, shall be construed to modify or otherwise affect the common law standards governing the availability or application of comity analysis to other types of compulsory process or to in stances of compulsory process issued under section 2703 of title 18, United States Code, as amended by this section, and not covered under subsection (h)(2) of such section 2703.

SEC. 104. ADDITIONAL AMENDMENTS TO CURRENT COMMUNICATIONS LAWS.

Title 18, United States Code, is amended—

(1) in chapter 119—

(A) in section 2511(2), by adding at the end the following:

"(j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523." and;

(B) (略)

(2)~(3) (略)

SEC. 105. EXECUTIVE AGREEMENTS ON ACCESS TO DATA BY FOREIGN GOVERNMENTS.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

" § 2523. Executive agreements on access to data by foreign governments

"(a) (略)

"(b) Executive Agreement Requirements.—For purposes of this chapter, chapter 121, and chapter

206, an executive agreement governing access by a foreign government to data subject to this chapter, chapter 121, or chapter 206 shall be considered to satisfy the requirements of this section if the Attorney General, with the concurrence of the Secretary of State, determines, and submits a written certification of such determination to Congress, including a written certification and explanation of each consideration in paragraphs (1), (2), (3), and (4), that—

"(1) the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement, if—

"(A)~(B) (略)

"(2) the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement;

"(3) the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data; and

"(4) the agreement requires that, with respect to any order that is subject to the agreement—

"(A) the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement;

"(B)~(C) (略)

"(D) an order issued by the foreign government—

"(i) shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

"(ii)~(vi) (略)

"(E)~(K) (略)

"(c) (略)

"(d) EFFECTIVE DATE OF CERTIFICATION.—

"(1) NOTICE.—Not later than 7 days after the date on which the Attorney General certifies an executive agreement under subsection (b), the Attorney General shall provide notice of the determination under subsection (b) and a copy of the executive agreement to Congress, including—

"(A)~(B) (略)

"(2) ENTRY INTO FORCE.—An executive agreement that is determined and certified by the Attorney General to satisfy the requirements of this section shall enter into force not earlier than the date that is 180 days after the date on which notice is provided under paragraph (1), unless Congress enacts a joint resolution of disapproval in accordance with paragraph (4).

"(3) (略)

“(4) CONGRESSIONAL REVIEW.—

“(A) (略)

“(B) JOINT RESOLUTION ENACTED.—Notwithstanding any other provision of this section, if not later than 180 days after the date on which notice is provided to Congress under paragraph (1), there is enacted into law a joint resolution disapproving of an executive agreement under this section, the executive agreement shall not enter into force.

“(C) (略)

“(5)~(8) (略)

“(e)~(h) (略)”

(b) (略)

II. 日本法

① 日本国憲法[2](→第 4.、第 6.)

〔生命及び自由の保障と科刑の制約〕

第三十一条　何人も、法律の定める手続によらなければ、その生命若しくは自由を奪はれ、又はその他の刑罰を科せられない。

〔侵入、捜索及び押収の制約〕

第三十五条　何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第三十三条の場合を除いては、正当な理由に基いて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない。

２　捜索又は押収は、権限を有する司法官憲が発する各別の令状により、これを行ふ。

〔自白強要の禁止と自白の証拠能力の限界〕

第三十八条　何人も、自己に不利益な供述を強要されない。

２～３　(略)

② 刑事訴訟法[3](→第 4.)

〔情報公開法等の適用除外〕

第五十三条の二　(略)

---

2 昭和 21 年憲法。日本国憲法の条文の題名は、衆議院ホームページ(http://www.shugiin.go.jp/internet/itdb_annai.nsf/html/statics/shiryo/dl-constitution.htm#3sho)に従っている。

3 昭和 23 年法律第 131 号。条文の題名は、宇賀克也ほか編『六法全書　平成 31 年版』(有斐閣、2019 年)に従っている。

２　訴訟に関する書類及び押収物に記録されている個人情報については、行政機関の保有する個人情報の保護に関する法律（平成十五年法律第五十八号）第四章及び独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号）第四章の規定は、適用しない。

３～４　(略)

〔差押え、提出命令〕

第九十九条　(略)

２　差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であつて、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる。

３　(略)

〔記録命令付差押え〕

第九十九条の二　裁判所は、必要があるときは、記録命令付差押え(電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえることをいう。以下同じ。)をすることができる。

〔郵便物等の押収〕

第百条　裁判所は、被告人から発し、又は被告人に対して発した郵便物、信書便物又は電信に関する書類で法令の規定に基づき通信事務を取り扱う者が保管し、又は所持するものを差し押え、又は提出させることができる。

２　前項の規定に該当しない郵便物、信書便物又は電信に関する書類で法令の規定に基づき通信事務を取り扱う者が保管し、又は所持するものは、被告事件に関係があると認めるに足りる状況のあるものに限り、これを差し押え、又は提出させることができる。

３　前二項の規定による処分をしたときは、その旨を発信人又は受信人に通知しなければならない。但し、通知によつて審理が妨げられる虞がある場合は、この限りでない。

〔執行の方式〕

第百十条　差押状、記録命令付差押状又は捜索状は、処分を受ける者にこれを示さなければならない。

〔電磁的記録に係る記録媒体の差押えの執行方法〕

第百十条の二　差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状の執行をする者は、その差押えに代えて次に掲げる処分をすることができる。公判廷で差押えをする場合も、同様である。

一　差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し、印刷し、又は移転した上、当該他の記録媒体を差し押さえること。

二　差押えを受ける者に差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写させ、印刷させ、又は移転させた上、当該他の記録媒体を差し押さえること。

〔責任者の立ち会い〕

第百十四条　公務所内で差押状、記録命令付差押状又は捜索状の執行をするときは、その長又はこれに代わるべき者に通知してその処分に立ち会わせなければならない。

２　前項の規定による場合を除いて、人の住居又は人の看守する邸宅、建造物若しくは船舶内で差押状、記録命令付差押状又は捜索状の執行をするときは、住居主若しくは看守者又はこれらの者に代わるべき者をこれに立ち会わせなければならない。これらの者を立ち会わせることができないときは、隣人又は地方公共団体の職員を立ち会わせなければならない。

〔捜査に必要な取調べ〕

第百九十七条　捜査については、その目的を達するため必要な取調をすることができる。但し、強制の処分は、この法律に特別の定のある場合でなければ、これをすることができない。

２　捜査については、公務所又は公私の団体に照会して必要な事項の報告を求めることができる。

３　検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至つたときは、当該求めを取り消さなければならない。

４　前項の規定により消去しないよう求める期間については、特に必要があるときは、三十日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて六十日を超えることができない。

５　第二項又は第三項の規定による求めを行う場合において、必要があるときは、みだり

にこれらに関する事項を漏らさないよう求めることができる。

〔令状による差押え・記録命令付差押え・捜索・検証〕

第二百十八条　検察官、検察事務官又は司法警察職員は、犯罪の捜査をするについて必要があるときは、裁判官の発する令状により、差押え、記録命令付差押え、捜索又は検証をすることができる。この場合において、身体の検査は、身体検査令状によらなければならない。

２　差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であつて、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる。

３～６　(略)

〔差押え等の令状の方式〕

第二百十九条　前条の令状には、被疑者若しくは被告人の氏名、罪名、差し押さえるべき物、記録させ若しくは印刷させるべき電磁的記録及びこれを記録させ若しくは印刷させるべき者、捜索すべき場所、身体若しくは物、検証すべき場所若しくは物又は検査すべき身体及び身体の検査に関する条件、有効期間及びその期間経過後は差押え、記録命令付差押え、捜索又は検証に着手することができず令状はこれを返還しなければならない旨並びに発付の年月日その他裁判所の規則で定める事項を記載し、裁判官が、これに記名押印しなければならない。

２　前条第二項の場合には、同条の令状に、前項に規定する事項のほか、差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であつて、その電磁的記録を複写すべきものの範囲を記載しなければならない。

３　(略)

〔押収・捜索・検証に関する準用規定、検証の時刻の制限、被疑者の立会い、身体検査を拒否した者に対する制裁〕

第二百二十二条　第九十九条第一項、第百条、第百二条から第百五条まで、第百十条から第百十二条まで、第百十四条、第百十五条及び第百十八条から第百二十四条までの規定は、検察官、検察事務官又は司法警察職員が第二百十八条、第二百二十条及び前条の規定によつてする押収又は捜索について、(略)これを準用する。ただし、司法巡査は、第百二十二条から第百二十四条までに規定する処分をすることができない。

２～７　(略)

③　刑事訴訟規則[4]（→第 4.）

(令状請求の方式)
第百三十九条　令状の請求は、書面でこれをしなければならない。

④　犯罪捜査規範[5]（→第 4.）

（人の住居等の任意の捜索の禁止）
第百八条　人の住居又は人の看守する邸宅、建造物若しくは船舶につき捜索をする必要があるときは、住居主又は看守者の任意の承諾が得られると認められる場合においても、捜索許可状の発付を受けて捜索をしなければならない。

⑤　犯罪捜査のための通信傍受に関する法律[6]（→第 4.）

(傍受令状の提示)
第十条　傍受令状は、通信管理者等に示さなければならない。ただし、被疑事実の要旨については、この限りでない。

(該当性判断のための傍受)
第十四条　検察官又は司法警察員は、傍受の実施をしている間に行われた通信であって、傍受令状に記載された傍受すべき通信(以下単に「傍受すべき通信」という。)に該当するかどうか明らかでないものについては、傍受すべき通信に該当するかどうかを判断するため、これに必要な最小限度の範囲に限り、当該通信の傍受をすることができる。
２　(略)

（傍受記録の作成）
第二十九条　検察官又は司法警察員は、傍受の実施（第二十条第一項又は第二十三条第一項第二号の規定によるものを除く。以下この項において同じ。）を中断し又は終了したときは、その都度、速やかに、傍受をした通信の内容を刑事手続において使用するための記録一通を作成しなければならない。傍受の実施をしている間に記録媒体の交換をしたときその他記録媒体に対する記録が終了したときも、同様とする。
２　検察官又は司法警察員は、再生の実施を中断し又は終了したときは、その都度、速や

4　昭和 23 年 12 月 1 日最高裁判所規則第 32 号。

5　昭和 32 年国家公安委員会規則第 2 号

6　平成 11 年法律第 137 号。

かに、再生をした通信の内容を刑事手続において使用するための記録一通を作成しなければならない。再生の実施をしている間に記録媒体の交換をしたときその他記録媒体に対する記録が終了したときも、同様とする。

3　第一項に規定する記録は、第二十四条第一項後段若しくは第二十六条第二項の規定により記録をした記録媒体又は第二十五条第三項の規定により作成した同条第一項の記録媒体の複製から、次に掲げる通信以外の通信の記録を消去して作成するものとする。

一　傍受すべき通信に該当する通信

二　第十四条第二項の規定により傍受をした通信であって、なおその内容を復元するための措置を要するもの

三　第十五条の規定により傍受をした通信及び第十四条第二項の規定により傍受をした通信であって第十五条に規定する通信に該当すると認められるに至ったもの

四　前三号に掲げる通信と同一の通話の機会に行われた通信

4　第二項に規定する記録は、第二十四条第一項後段若しくは第二十六条第二項の規定により記録をした記録媒体又は第二十五条第三項の規定により作成した同条第二項の記録媒体の複製から、次に掲げる通信以外の通信の記録を消去して作成するものとする。

一　傍受すべき通信に該当する通信

二　第二十一条第四項（第二十三条第四項においてその例による場合を含む。次号において同じ。）の規定により再生をした通信であって、なおその内容を復元するための措置を要するもの

三　第二十一条第五項（第二十三条第四項においてその例による場合を含む。）の規定により再生をした通信及び第二十一条第四項の規定により再生をした通信であって第十五条に規定する通信に該当すると認められるに至ったもの

四　前三号に掲げる通信と同一の通話の機会に行われた通信

5～7　(略)

(通信の当事者に対する通知)

第三十条　検察官又は司法警察員は、傍受記録に記録されている通信の当事者に対し、傍受記録を作成した旨及び次に掲げる事項を書面で通知しなければならない。

一　当該通信の開始及び終了の年月日時並びに相手方の氏名(判明している場合に限る。)

二　傍受令状の発付の年月日

三　傍受の実施の開始及び終了の年月日

四　傍受の実施の対象とした通信手段

五　傍受令状に記載された罪名及び罰条

六　第十五条に規定する通信については、その旨並びに当該通信に係る犯罪の罪名及

び罰条

七　次条の規定による傍受記録の聴取等(聴取若しくは閲覧又は複製の作成をいう。以下この号において同じ。)及び第三十二条第一項の規定による傍受の原記録の聴取等の許可の請求並びに第三十三条第一項又は第二項の規定による不服申立てをすることができる旨

２　前項の通知は、通信の当事者が特定できない場合又はその所在が明らかでない場合を除き、傍受の実施が終了した後三十日以内にこれを発しなければならない。ただし、地方裁判所の裁判官は、捜査が妨げられるおそれがあると認めるときは、検察官又は司法警察員の請求により、六十日以内の期間を定めて、この項の規定により通知を発しなければならない期間を延長することができる。

３　(略)

⑥　行政手続等における情報通信の技術の利用に関する法律[7]（→第 4.）

(定義)

第二条　この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一～三　(略)

四　署名等　署名、記名、自署、連署、押印その他氏名又は名称を書面等に記載することをいう。

五　(略)

六　申請等　申請、届出その他の法令の規定に基づき行政機関等に対して行われる通知(訴訟手続その他の裁判所における手続並びに刑事事件及び政令で定める犯則事件に関する法令の規定に基づく手続(次号から第九号までにおいて「裁判手続等」という。)において行われるものを除く。)をいう。

(電子情報処理組織による申請等)

第三条　(略)

２～３　(略)

４　第一項の場合において、行政機関等は、当該申請等に関する他の法令の規定により署名等をすることとしているものについては、当該法令の規定にかかわらず、氏名又は名称を明らかにする措置であって主務省令で定めるものをもって当該署名等に代えさせることができる。

7　平成 14 年法律第 151 号。

⑦　電気通信事業法[8]（→第 4.、第 6.）

(秘密の保護)

第四条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

２　(略)

第百七十九条　電気通信事業者の取扱中に係る通信（第百六十四条第三項に規定する通信並びに同条第四項及び第五項の規定により電気通信事業者の取扱中に係る通信とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号ロの通知及び認定送信型対電気通信設備サイバー攻撃対処協会が取り扱う同項第二号ロの通信履歴の電磁的記録を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。

２　電気通信事業に従事する者（第百六十四条第四項及び第五項の規定により電気通信事業に従事する者とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号又は第二号に掲げる業務に従事する者を含む。）が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。

⑧　刑法[9]（→第 4.、第 6.）

（正当行為）

第三十五条　法令又は正当な業務による行為は、罰しない。

（緊急避難）

第三十七条　自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。ただし、その程度を超えた行為は、情状により、その刑を減軽し、又は免除することができる。

２　前項の規定は、業務上特別の義務がある者には、適用しない。

⑨　電気通信事業における個人情報保護に関するガイドライン[10]（→第 4.）

(第三者提供の制限)

第十五条　電気通信事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

8　昭和 59 年法律第 86 号。

9　明治 40 年法律第 45 号

10　平成 29 年 4 月 18 日総務省告示第 152 号。

一　法令に基づく場合

二～四　(略)

２～１１　(略)

⑩　個人情報の保護に関する法律[11](→第 2.、第 4.、第 6.)

(定義)

第二条　この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

一～二　(略)

２～７　(略)

８　この法律において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。

９～１０　(略)

(第三者提供の制限)

第二十三条　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一　法令に基づく場合

二～三　(略)

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

２～６　(略)

⑪　行政機関の保有する個人情報の保護に関する法律[12](→第 4.)

(開示請求権)

第十二条　何人も、この法律の定めるところにより、行政機関の長に対し、当該行政機関の保有する自己を本人とする保有個人情報の開示を請求することができる。

２　(略)

(訂正請求権)

第二十七条　何人も、自己を本人とする保有個人情報(次に掲げるものに限る。第三十六条

11　平成 15 年法律第 57 号。

12　平成 15 年法律第 58 号。

第一項において同じ。)の内容が事実でないと思料するときは、この法律の定めるところにより、当該保有個人情報を保有する行政機関の長に対し、当該保有個人情報の訂正(追加又は削除を含む。以下同じ。)を請求することができる。ただし、当該保有個人情報の訂正に関して他の法律又はこれに基づく命令の規定により特別の手続が定められているときは、この限りでない。

一～三　(略)

２～３　(略)

(利用停止請求権)

第三十六条　何人も、自己を本人とする保有個人情報が次の各号のいずれかに該当すると思料するときは、この法律の定めるところにより、当該保有個人情報を保有する行政機関の長に対し、当該各号に定める措置を請求することができる。ただし、当該保有個人情報の利用の停止、消去又は提供の停止(以下「利用停止」という。)に関して他の法律又はこれに基づく命令の規定により特別の手続が定められているときは、この限りでない。

一～二　(略)

２～３　(略)

(適用除外等)

第四十五条　第四章の規定は、刑事事件若しくは少年の保護事件に係る裁判、検察官、検察事務官若しくは司法警察職員が行う処分、刑若しくは保護処分の執行、更生緊急保護又は恩赦に係る保有個人情報(当該裁判、処分若しくは執行を受けた者、更生緊急保護の申出をした者又は恩赦の上申があった者に係るものに限る。)については、適用しない。

２　(略)

III. その他の外国法

①　米国憲法[13](→第 4.)

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

13　The Constitution of the United States of America, *available at* https://www.law.cornell.edu/constitution

② 米国連邦刑事訴訟規則[14]（→第 4.、第 5.）

Rule 4.1. Complaint, Warrant, or Summons by Telephone or Other Reliable Electronic Means

Primary tabs

(a) In General. A magistrate judge may consider information communicated by telephone or other reliable electronic means when reviewing a complaint or deciding whether to issue a warrant or summons.

(b) Procedures. If a magistrate judge decides to proceed under this rule, the following procedures apply:

(1) Taking Testimony Under Oath. The judge must place under oath — and may examine — the applicant and any person on whose testimony the application is based.

(2) Creating a Record of the Testimony and Exhibits.

(A)~(B) (略)

(3) Preparing a Proposed Duplicate Original of a Complaint, Warrant, or Summons. The applicant must prepare a proposed duplicate original of a complaint, warrant, or summons, and must read or otherwise transmit its contents verbatim to the judge.

(4) Preparing an Original Complaint, Warrant, or Summons. If the applicant reads the contents of the proposed duplicate original, the judge must enter those contents into an original complaint, warrant, or summons. If the applicant transmits the contents by reliable electronic means, the transmission received by the judge may serve as the original.

(5) Modification. The judge may modify the complaint, warrant, or summons. The judge must then:

(A) transmit the modified version to the applicant by reliable electronic means; or

(B) file the modified original and direct the applicant to modify the proposed duplicate original accordingly.

(6) Issuance. To issue the warrant or summons, the judge must:

(A) sign the original documents;

(B) enter the date and time of issuance on the warrant or summons; and

(C) transmit the warrant or summons by reliable electronic means to the applicant or direct the applicant to sign the judge's name and enter the date and time on the duplicate original.

(c) Suppression Limited. Absent a finding of bad faith, evidence obtained from a warrant issued under this rule is not subject to suppression on the ground that issuing the warrant in this manner was unreasonable under the circumstances.

---

14 Federal Rules of Criminal Procedure, *available at* https://www.law.cornell.edu/rules/frcrmp

Rule 41. Search and Seizure

(a) Scope and Definitions.

(1) (略)

(2) Definitions. The following definitions apply under this rule:

(A) “Property” includes documents, books, papers, any other tangible objects, and information.

(B)~(E) (略)

(b) Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

(1)~(5) (略)

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

(c)~(f) (略)

③ Stored Communications Act (SCA、CLOUD Actによって改正された部分以外)[15](→第4.)

18 U.S. Code § 2705. Delayed notice

(a) (略)

(b) Preclusion of Notice to Subject of Governmental Access.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will

15 18 U.S. Code CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TR ANSACTIONAL RECORDS ACCESS, *available at* https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

result in—

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

④ ドイツ刑事訴訟法（英訳）[16]（→第 4.）

Section 110 Examination of Papers

(1)～(2) (略)

(3) The examination of an electronic storage medium at the premises of the person affected by the search may be extended to cover also physically separate storage media insofar as they are accessible from the storage medium if there is a concern that the data sought would otherwise be lost. Data which may be of significance for the investigation may be secured; Section 98 subsection (2) shall apply mutatis mutandis.

⑤ 英国捜査権限規制法（RIPA）[17]（→第 4.）

49 Notices requiring disclosure.

(1) This section applies where any protected information—

(a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;

(b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications or obtain secondary data from communications, or is likely to do so;

(c) has come into the possession of any person by means of the exercise of any power conferred by an authorisation under section 22(3) or (3B) or under Part II Part 3 of the Investigatory Powers Act 2016 or Part 2 of this Act, or as a result of the giving of a notice under section 22(4) in pursuance of an authorisation under Part 3 of the Act of 2016 or as the result of the issue of a warrant under Chapter 2 of Part 6 of the Act of 2016, or is likely to do so;

(d) has come into the possession of any person as a result of having been provided or disclosed

---

16 THE GERMAN CODE OF CRIMINAL PROCEDURE, *available at* https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

17 Regulation of Investigatory Powers Act 2000, *available at* http://www.legislation.gov.uk/ukpga/2000/23/contents

in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or

(e) has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police, the National Crime Agency or Her Majesty's Revenue and Customs, or is likely so to come into the possession of any of those services, the police, the National Crime Agency or Her Majesty's Revenue and Customs.

(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds—

(a) that a key to the protected information is in the possession of any person,

(b) that the imposition of a disclosure requirement in respect of the protected information is—

(i) necessary on grounds falling within subsection (3), or

(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,

(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and

(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime; or

(c) in the interests of the economic well-being of the United Kingdom.

(4)~(11) (略)

50 Effect of notice imposing disclosure requirement.

(1) Subject to the following provisions of this section, the effect of a section 49 notice imposing a disclosure requirement in respect of any protected information on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form is that he—

(a) shall be entitled to use any key in his possession to obtain access to the information or to put it into an intelligible form; and

(b) shall be required, in accordance with the notice imposing the requirement, to make a disclosure of the information in an intelligible form.

(2)~(10)　(略)

⑥　オーストラリア電気通信その他の法令の改正法(援助及びアクセス提供法)[18]（→第 4.）

317B　Definitions

electronic protection includes:

(a)　authentication; and

(b)　encryption.

317E　Listed acts or things

(1)　For the purposes of the application of this Part to a designated communications provider, listed act or thing means:

(a)　removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider; or

(b)　providing technical information; or

(c)　installing, maintaining, testing or using software or equipment; or

(d)　ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format; or

(da)　an act or thing done to assist in, or facilitate:

(i)　giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(ii)　the effective receipt of information in connection with a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(e)　facilitating or assisting access to whichever of the following are the subject of eligible activities of the provider:

(i)　a facility;

(ii)　customer equipment;

(iii)　a data processing device;

(iv)　a listed carriage service;

(v)　a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service;

(vi)　an electronic service;

(vii)　a service that facilitates, or is ancillary or incidental to, the provision of an electronic service;

18　Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195

(viii) software used, for use, or likely to be used, in connection with a listed carriage service;

(ix) software used, for use, or likely to be used, in connection with an electronic service;

(x) software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network; or

(f) assisting with the testing, modification, development or maintenance of a technology or capability; or

(g) notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation; or

(h) modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider; or

(i) substituting, or facilitating the substitution of, a service provided by the designated communications provider for:

(i) another service provided by the provider; or

(ii) a service provided by another designated communications provider; or

(j) an act or thing done to conceal the fact that any thing has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

(i) enforcing the criminal law, so far as it relates to serious Australian offences; or

(ii) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or

(iii) the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

317L Technical assistance notices

(1) The Director-General of Security or the chief officer of an interception agency may give a designated communications provider a notice, to be known as a technical assistance notice, that requires the provider to do one or more specified acts or things that:

(a) are in connection with any or all of the eligible activities of 34 the provider; and

(b) are covered by subsection (2).

Note: Section 317ZK deals with the terms and conditions on which such a 3 requirement is to be complied with.

(2) The specified acts or things must be by way of giving help to:

(a) in a case where the technical assistance notice is given by the Director-General of Security—ASIO; or

(b) in a case where the technical assistance notice is given by the chief officer of an interception agency—the agency;

in relation to:

(c) the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

(i) enforcing the criminal law, so far as it relates to serious Australian offences; or

(ii) assisting the enforcement of the criminal laws in force 16 in a foreign country, so far as those laws relate to serious foreign offences; or

(iii) safeguarding national security; or

(d) a matter that facilitates, or is ancillary or incidental to, a matter covered by paragraph (c).

(2A) The specified acts or things must not be directed towards ensuring that a designated communications provider is capable of giving help to ASIO or an interception agency.

Listed acts or things

(3) The acts or things specified in a technical assistance notice given to a designated communications provider must be listed acts or things, so long as those acts or things:

(a) are in connection with any or all of the eligible activities of the provider; and

(b) are covered by subsection (2).

Note: For listed acts or things, see section 317E.

⑦ EU データ一般保護規則(GDPR)[19](→第 5.)

Article 4 Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

IV. 条約及び行政協定

① デジタル貿易に関する日本国とアメリカ合衆国との間の協定[20](→第 5.)

第二十一条　暗号法を使用する情報通信技術産品

１～２　(略)

３　いずれの締約国も、暗号法を使用し、及び商業上の目的のために設計された情報通信

19 General Data Protection Regulation, *available at* https://gdpr-info.eu/

20 デジタル貿易に関する日本国とアメリカ合衆国との間の協定, available at https://www.mofa.go.jp/mofaj/ila/et/page3_002912.html

技術産品に関し、当該情報通信技術産品の製造、販売、流通、輸入又は使用の条件として、当該情報通信技術産品の製造者又は供給者に対して次のいずれかのことを要求してはならない。

(a) 当該締約国又は当該締約国の領域に所在する者に対し、暗号法に関連する財産的価値を有する情報を移転し、又は当該情報へのアクセスを提供すること（特定の技術、生産工程その他の情報（例えば、非公開の暗号鍵その他の秘密のパラメーター、アルゴリズムの仕様その他設計の詳細）の開示によるものを含む。）。

(b) 情報通信技術産品の開発、製造、販売、流通、輸入又は使用について、当該締約国の領域に所在する者と提携し、又は協力すること。

(c) 特定の暗号化アルゴリズム又は暗号を使用し、又は統合すること。

② サイバー犯罪条約[21]（→第 5.）

Article 18 Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Article 32 Trans-border access to stored computer data with consent or where publicly available

---

21 Convention on Cybercrime, *available at* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

③ 刑事に関する共助に関する日本国とアメリカ合衆国との間の条約[22]（→第 5.）

第二条

1 (略)

2 この条約に基づく共助の請求は、請求国の中央当局から被請求国の中央当局に対して行われる。

3 両締約国の中央当局は、この条約の実施に当たって、相互に直接連絡する。

④ 米英行政協定（→第 5.、第 6.）[23]

Article 1: Definitions

For the purposes of this Agreement:

1~13. (略)

14. Serious Crime means an offense that is punishable by a maximum term of imprisonment of at least three years.

15~16. (略)

Article 2: Purpose of the Agreement

l. The purpose of this Agreement is to advance public safety and security, and to protect privacy, civil liberties, and an open Internet, by resolving potential conflicts of "legal obligations when communications service providers are served with Legal Process from one Party for the production or preservation of electronic data, where those providers may also be subject to the

---

22 刑事に関する共助に関する日本国とアメリカ合衆国との間の条約, *available at* https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_3.html

23 Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, *available at* https://www.justice.gov/ag/page/file/1207496/download#Agreement%20between%20the%20Government%20of%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes)

laws of the other Party. The Agreement provides an efficient, effective, data protection-compatible and privacy-protective means for each. Party to obtain, subject to appropriate targeting limitations, electronic data relating to the prevention, detection, investigation, or prosecution of Serious Crime, in a manner consistent with its law and the law of the other Party.

2.-3. (略)

Article 4: Targeting Restrictions

1~2. (略)

3. Orders subject to this Agreement may not intentionally target a Receiving-Party Person, and each Party shall adopt targeting procedures designed to implement this requirement as described in Article 7.1.

4~5. (略)

Article 5: Issuance and Transmission of Orders

1. Orders subject to this Agreement shall be issued. in compliance with the domestic law of the Issuing Party, and shall be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation.
2. Orders subject to this Agreement shall be subject to review or oversight under the domestic law of the Issuing Party by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the Order.
3. Orders subject to this Agreement for the interception of wire or electronic communications, and any extensions thereof, shall be for a fixed, limited duration; may not last longer than is reasonably necessary to accomplish the approved purposes of the Order; and shall be issued only if the same information could riot reasonably be obtained by another less intrusive method.
4. The Issuing Party may not issue an Order subject to this Agreement at the request of or to obtain information to provide to the Receiving Party or a third-party government.
5. The Issuing Party may issue . Orders subject to this Agreement directly to a Covered Provider. Such Orders shall. be transmitted by the Issuing Party's Designated Authority. The Designated Authorities of the Parties may mutually agree that the functions each carries out under Articles 5.5 through and inclusive of 5.9, 6.1, and 6.2 may be performed by additional authorities in whole or in part. The Designated Authorities of the Parties may, by mutual agreement, prescribe rules and conditions for any such authorities.
6. Prior to transmission, the Issuing Party's Designated Authority shall review the Orders for compliance with this Agreement.
7. Each Order subject to this Agreement must include a written certification by the Issuing Party's Designated Authority that the Order is lawful and complies with the Agreement, including the

Issuing Party's substantive standards for Orders subject to this Agreement.

8. The Issuing Party's Designated Authority shall notify the Covered Provider that it invokes this Agreement with respect to the Order.
9. The Issuing Party's Designated Authority shall notify the Covered Provider of a point of contact at the Issuing Party's Designated Authority who can provide information on legal or practical issues relating to the Order.
10. In cases where an Order subject to this Agreement is issued for data in respect of an individual who is reasonably believed to be located outside the territory of the Issuing Party and is not a national of the Issuing Party, the Issuing Party's Designated Authority shall notify the appropriate authorities in the third country where the person is located, except in cases where the Issuing Party considers that notification would be detrimental to operational or national security, impede the conduct of an investigation, or imperil human rights.
11. The Parties agree that a Covered Provider that receives an Order subject to this Agreement may raise specific objections when it has reasonable belief that the Agreement may not properly be invoked with regard to the Order. Such objections should generally be raised in the first instance to the. Issuing Party's Designated Authority and in a reasonable time after receiving the Order. Upon receipt of objections to an Order from a Covered Provider, the Issuing Party's Designated Authority shall respond to the objections. If the objections are not resolved, the Parties agree that the Covered Provider may raise the objections to the Receiving Party's Designated Authority. The Parties' Designated Authorities may confer in an effort to resolve any such objections and may meet periodically and as necessary to discuss and address any issues raised under this Agreement.
12. If the Receiving Party's Designated Authority concludes that the Agreement may not properly be invoked with respect to any . Order, it shall notify the Issuing Party's Designated Authority and the relevant Covered Provider of that conclusion, and this Agreement shall not apply to that Order.

Article 8: Limitations on Use and Transfer

1~2. (略)

4. Where an Issuing Party has received data pursuant to Legal Process from a Covered Provider, and
    a. the United Kingdom has declared that its essential interests may be implicated by the introduction of such data as evidence in the prosecution's case in the United States for an offense for which the death penalty is sought; or
    b. the United States has declared that its essential interests may be implicated by the introduction ofsuch data as evidence in the prosecution's case in the United Kingdom in a manner that raises freedom of speech concerns for the United States;

prior to use of the data in a manner that is or could be contrary to those essential interests, the Issuing Party shall, via the Receiving Party's Designated Authority, obtain permission to do so. The Receiving Party's Designated Authority may grant permission, subject to such conditions as it deems necessary, and if it does so, the Issuing Party may only introduce this data in compliance with those conditions. If the Receiving Party does not grant approval, the Issuing Party shall not use the data it has received pursuant to the Legal Process in that manner.

5. (略)

以　　上