

「電気通信事業におけるサイバー攻撃への適正な対処の 在り方に関する研究会」における法的整理について

2019年4月19日
事務局

- 「通信の秘密」は、通信が人間の社会生活にとって必要不可欠なコミュニケーション手段であることから、表現の自由の保障を実効あらしめるとともに、個人の私生活の自由を保護し、個人生活の安寧を保障する(プライバシーの保護)ため、憲法上の基本的人権の一つとして、憲法第21条第2項において保障されている。
- 日本国憲法の規定を受け、電気通信事業法第4条において、罰則をもって「通信の秘密」を保護する規定が定められており、電気通信事業法上「通信の秘密」は厳格に保護されている。

通信の秘密の範囲

通信の秘密とは、**①個別の通信に係る通信内容**のほか、**②個別の通信に係る通信の日時、場所、通信当事者の氏名、住所、電話番号等の当事者の識別符号、通信回数等**これらの事項を知られることによって**通信の存否や意味内容を推知されるような事項**全てを含む。

通信の秘密の侵害

通信の秘密を侵害する行為は、以下の3類型に大別されている。なお、通信の秘密の保存自体も侵害に該当し得る。

- **知得** = 「積極的に通信の秘密を知ろうとする意思のもとで知り得る状態に置くこと」
- **窃用** = 「発信者又は受信者の意思に反して利用すること」
- **漏えい** = 「他人が知り得る状態に置くこと」

通信の秘密の侵害に当たらない場合

- 通信当事者の有効な同意がある場合
- 通信当事者の有効な同意がない場合であっても以下の場合（違法性阻却事由がある場合）
 - (1) 法令行為に該当する場合
 - (2) 正当業務行為に該当する場合
 - (3) 正当防衛、緊急避難に該当する場合

通信当事者の有効な同意がある場合**○ 通信の秘密の侵害について通信当事者の有効な同意がある場合は、通信の秘密の侵害に当たらない。**

通信当事者が侵害される通信の秘密について個別具体的かつ明確に同意した場合でなければ原則として有効な同意があるとはいえない。

ただし、通常の利用者であれば承諾することが想定される場合であって、利用者が随時不利益なく同意を撤回でき（オプトアウト）、それらが十分に周知されるなどしている場合は、約款等による包括的な同意でも有効な同意といえる場合がある。

違法性阻却事由がある場合**○ 通信当事者の同意がない場合であっても、下記のような違法性阻却事由がある場合には、通信の秘密の侵害が許容される。****(1) 法令行為に該当する場合**

電気通信事業者として、刑事訴訟法第100条に基づく通信履歴の差押えなど、他の法令の規定に基づき正当に行う行為は、法令に基づく行為として違法性が阻却される。

(2) 正当業務行為に該当する場合

電気通信事業者として電気通信役務の提供等の業務を遂行するために必要であって、①目的の正当性、②行為の必要性、③手段の相当性の要件を満たす行為については、正当業務行為として違法性が阻却される。

(3) 正当防衛、緊急避難に該当する場合

通信施設に対する現に生じている攻撃に対応したり人の生命身体に対する危険を避けたりするために通信の秘密を侵す場合等、正当防衛の要件（①急迫不正の侵害、②自己又は他人の権利を防衛するため、③やむを得ずした行為）又は緊急避難の要件（①現在の危難の存在、②法益の権衡、③行為の補充性）を満たす行為については、違法性が阻却される。

1. 日本国憲法

第二十一条

- 2 検閲は、これをしてはならない。通信の秘密はこれを侵してはならない。

2. 電気通信事業法

第三条 電気通信事業者の取扱中に係る通信は、検閲してはならない。

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 電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

第二十九条 総務大臣は次の各号のいずれかに該当すると認めるときは、電気通信事業者に対し、利用者の利益又は公共の利益を確保する為に必要な限度において、業務の方法の改善その他の措置をとるべきことを命ずることができる。

一 電気通信事業者の業務の方法に関し通信の秘密の確保に支障があるとき。

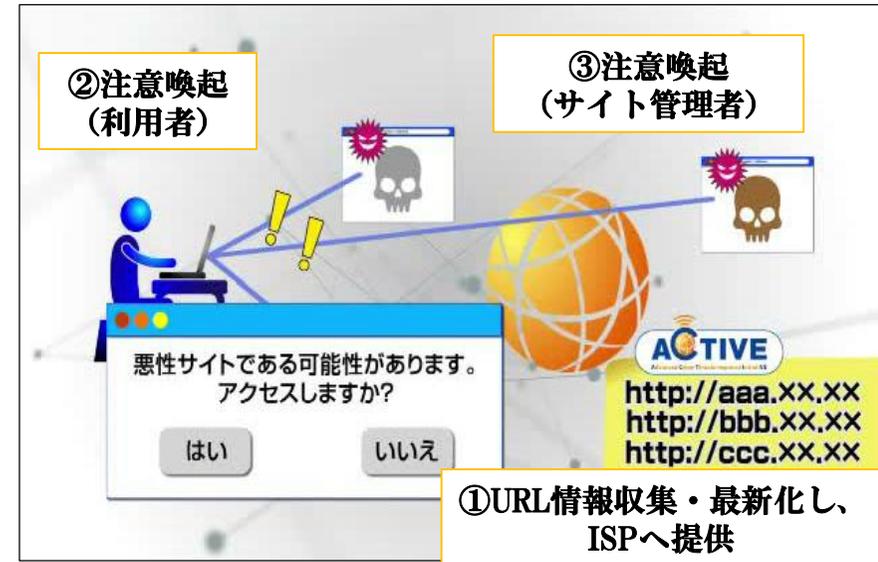
第一百七十九条 電気通信事業者の取扱中に係る通信（括弧内略）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。

- 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。
- 3 前二項の未遂罪は、罰する。

ACTIVE(※)におけるマルウェア感染防止の取組

- ① マルウェア配布サイトのURL情報を収集・最新化し、リスト化してISPへ提供。
- ② マルウェア配布サイトにアクセスしようとする利用者にISPから注意喚起。
- ③ マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

※ 総務省とISP等の協力により、マルウェア配布サイトへのアクセスを未然に防止する等の実証実験を行う官民連携プロジェクト(平成25年度～29年度)。国内主要ISPやウイルス対策ベンダー等が参画。上記①～③のほか、マルウェア駆除の取組も実施。



有効な同意に関する整理(概要)

本取組については、通常の利用者であれば許諾すると想定されることから、次の3要件を満たせば、個別の同意ではなく、契約約款に基づく事前の包括同意であっても、有効な同意といえることができる。

- 1 ユーザが、一旦契約約款等に同意した後も、随時、同意内容を変更できる契約内容であること
- 2 マルウェア配布サイトへのアクセスに対する注意喚起における同意(及びその変更)の有無に関わらず、その他の提供条件が同一であるなど、同意しないユーザの利益が侵害されないようにすること
- 3 当該契約約款等の内容や、事後的に同意内容を変更できること及びその変更方法についてユーザに相応の周知や説明がされていること

有効な同意に関する整理

※「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」第一次とりまとめ19頁参照

○ 前提

通信の秘密についての同意は、一般的には、契約約款等に基づく事前の包括同意のみでは、有効な同意とはいえず、個別の同意でなければならないと解されている。その理由は、次の2つである。

- ① 通信の秘密の利益を放棄させる内容は、当事者の同意が推定可能な事項を定めるという契約約款の性質になじまないこと
- ② 事前の包括同意は、将来の事実に対する予測に基づくため、対象・範囲が不明確となり、ユーザに不測の不利益が生じる危険があること

○ 理由①について

もっとも、マルウェア配布サイトへのアクセスに対する注意喚起を行うために、通信の秘密に当たる情報のうち必要最小限度の事項のみを機械的・自動的に検知した上で、該当するアクセスに対して注意喚起画面等を表示させることについては、安全なインターネットアクセスを確保するためのものであり、通常の利用者であれば許諾すると想定し得ることから、契約約款の性質になじまないとまではいえない。

○ 理由②について

そして、(1)ユーザが一旦契約約款等に同意した後も、随時、同意内容を変更できる契約内容であって、(2)同意(及びその変更)の有無に関わらずその他の提供条件が同一であるなど、同意しないユーザの利益が侵害されないようにされており、(3)事後的に同意内容を変更できること及びその方法等についてユーザに相応の周知や説明がされている場合には、予測できなかった事情が将来生じた場合でも、利用者が不測の不利益を被る危険を回避できる。

○ 結論

したがって、このような場合には、個別の同意ではなく、契約約款に基づく事前の包括同意であっても、有効な同意といえることができると考えられる。