Baker McKenzie.

International Trade & Commerce
Tax
Tokyo

Client Alert
15 April 2024

スパイウェア技術の輸出規制に乗り出す新たな動き: ポーランド、ドイツ、韓国、日本の動向

(English follows Japanese)

本アラートに関する
お問い合わせ先：

Weronika Achramowicz
Partner, Warsaw
+48 22 4453429
Weronika.Achramowicz
@bakermckenzie.com

Alexander Ehrle
Associate, Berlin
+49 30 2 20 02 81 626
Alexander.Ehrle
@bakermckenzie.com

Beomsu Kim
Partner, Seoul
+82 2 6137 6801
Beomsu.Kim
@bakermckenziekorea.com

末冨　純子
パートナー
+81 3 6271 9741
Junko.Suetomi
@bakermckenzie.com

米国は最近、多くの国が、スパイウェア技術の輸出規制を実施する共同声明に参加したことを公表した。これは、人権侵害に利用される可能性のあるサイバー関連品目について貿易障壁を設けるという、より広範なイニシアチブの一環である。

3 月 18 日、フィンランド・ドイツ・アイルランド・日本・ポーランド・韓国は、米国・オーストラリア・カナダ・コスタリカ・デンマーク・フランス・ニュージーランド・ノルウェー・スウェーデン・スイス・英国に加わる形で、上記声明に参加した。当初の 11 か国は、昨年のバイデン政権下の第 2 回「民主主義のためのサミット」で初めて声明を発表し、スパイウェア技術の普及と利用に対する国内外での厳格な規制の必要性を強調していた。

3 月にソウルで開催された第 3 回「民主主義のためのサミット」において、上記 17 か国は、情報システムへの不正アクセスを含む有害なサイバー活動のために使用するおそれのある最終使用者に対して、ソフトウェア・技術・機器の輸出防止に努めることを改めて約束した。こうした取り組みは、各国の立法、規制、及び政策における姿勢並びに既存の輸出管理制度に合わせて行われることとなる。

上記約束の新規参加国における具体的な法的影響は今後明らかになっていくが、ポーランド、ドイツ、韓国、日本における今後の動向に関する弊所の専門家の見解は以下の通りである：

1. ポーランド

ポーランドによるスパイウェア規制の約束への署名には、大きな特徴がある。ポーランドの前政権は、商用スパイウェアを購入し、反対勢力への盗聴工作などの違法な目的で使用されていたことが疑われている。その結果、ポーランドは、スパイウェア使用に関する EU 法の違反及び行政における不正な適用の疑いで EU 当局による調査の対象となった。ポーランドでは現在、スパイウェアの使用に関する議論が行われており、将来的にスパイウェアの使用や販売を制限する新たな規制が設けられる可能性がある。

2. ドイツ

当初は躊躇していたドイツも、約 1 年前の協定に参加することを決定した。この決定は、ドイツ政府の連立協定に沿うものである。連立協定が目指すのは、IT セキュリティの格差を是正し、国と民間による監視ソフトウェアの利用に対する介入の基準を引き上げ、ドイツ憲法裁判所の判示したオンライン上の秘密監視の要件を常に遵守することで捜査当局の既存の権限を調整することである。かかる要件には、特に、比例原則の厳格な遵守と、秘密監視によって侵されてはならない私的生活の核となる不可侵な部分の保護が含まれる。


長谷川　匠
シニア・アソシエイト
+81 3 6271 9540
Takumi.Hasegawa
@bakermckenzie.com


戸澤　真偉斗
アソシエイト
+81 3 6271 9725
Maito.Tozawa
@bakermckenzie.com


丸田　郁美
アソシエイト
+81 3 6271 9693
Ikumi.Maruta
@bakermckenzie.com


藤原　総一郎
アソシエイト
+81 3 6271 9707
Soichiro.Fujiwara
@bakermckenzie.com

3. 韓国

韓国政府は、スパイウェア技術の輸出管理に関する上記約束の実現方法の詳細について、検討中のようである。韓国国内においては既に強力な法的枠組みが存在し、スパイウェアの配布が一般的に禁止されている上、データ管理者に対しスパイウェアからの保護が義務付けられている。これに対し、韓国の輸出管理規制においては、主に、戦略物資の輸入を計画している最終使用者や大量破壊兵器の拡散が疑われる最終使用者に焦点が当てられてきた。現段階では、人権的な観点からスパイウェア技術の輸出を制限する明確な法的根拠はない。しかし、2024 年 8 月に予定されている外国貿易法改正においては、韓国が既に参加している国際的な約束にしたがって、技術の輸出を管理する政府の権限を拡大するための明確な基盤がもたらされることが期待されている。韓国政府のアプローチに関する詳細は、今後数か月のうちに発表される見込みである。

4. 日本

日本政府は、スパイウェア技術の管理に関する国際的な約束の枠組みへの参加について、人権保護を含む様々な観点からその意義を認識し、分析及び検討を進めてきた。しかし、現時点では、日本政府はスパイウェア技術の輸出管理に関する約束に署名したことの詳細や背景について、公式に発表していない。この合意をどのように国内法に落とし込むのかについては、まだ検討段階であると思われる。商業的・人権保護的な観点から、規制の対象となる技術の範囲、仕向国による違いの有無、規制の強さの程度等を検討する必要がある。詳細については、今後日本政府から発表されることが見込まれる。

高波　巧
アソシエイト
+81 3 6271 9453
Taku.Takanami
@bakermckenzie.com

廣瀬　詠太郎
アソシエイト
+81 3 6271 9437
Eitaro.Hirose
@bakermckenzie.com

New Countries to Place Export Controls on Spyware Technology: Perspectives on Developments in Poland, Germany, South Korea and Japan

The US recently publicized the fact that a number of countries have joined a pledge to implement export controls on spyware technology as part of a broader initiative to establish trade barriers for cyber-related items that could be used in human rights abuses.

The US, Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland and the UK made the first such pledge during the Biden administration's second annual Summit for Democracy last year by emphasizing the need for stringent domestic and international controls on the spread and use of such technology. On March 18, they were joined by Finland, Germany, Ireland, Japan, Poland and South Korea.

During the third Summit for Democracy held in Seoul in March, all 17 countries pledged to work to prevent the export of software, technology and equipment to end-users who are likely to use them for harmful cyber activities, including unauthorized access to information systems. This will be done in line with the countries' respective legal, regulatory and policy approaches and suitable existing export control regimes.

While the specific legal implications of the commitments made by the newly joined countries have yet to be determined, our experts from Poland, Germany, South Korea and Japan offer high-level insights on these developments below.

1. Poland

Poland's signing of an anti-spyware commitment has a wider dimension. The previous Polish government purchased spyware available on the commercial market which was allegedly used for illegal purposes, such as eavesdropping on the opposition. EU authorities investigated Poland for alleged contraventions and poor administration of EU law with respect to the use of spyware. A debate on the use of spyware is currently underway in Poland which may result in new regulations restricting the use and sale of spyware in the future.

2. Germany

Despite some initial hesitation, Germany decided to sign the nearly one-year-old agreement. This decision aligns with the German government's coalition agreement, which aims to close IT security gaps, raise the intervention thresholds for the use of both state and commercial surveillance software and adjust investigators' existing powers by ensuring compliance with the German Constitutional Court's requirements for secret online searches at all times. The requirements entail, *inter alia*, strict adherence to the principle of proportionality and preservation of an inviolable core area of private life that may not be intruded upon through secret surveillance.

3. South Korea

The details of how these commitments to control the export of spyware technology will be implemented appear to be under review by the government. South Korea already has a robust legal framework to combat spyware within its borders, generally prohibiting its distribution and requiring data controllers to protect against it. In contrast, South Korea's export control regime has focused primarily on end-users who plan to import strategic goods or who are

suspected of contributing to the proliferation of weapons of mass destruction. There is currently no explicit legal basis for restricting the export of spyware technology on human rights grounds. However, it is expected that upcoming amendments to the Foreign Trade Act scheduled in August 2024 will provide a clear foundation for expanding the government's authority to control technology exports following multilateral commitments that South Korea has already made. This could provide the necessary framework for implementing commitments, including controls of spyware exports. More details on South Korea's approach are expected to be announced in the coming months.

4. Japan

The Japanese government has been analyzing and discussing participation in this international spyware tech control framework and recognizes its significance from various perspectives, including that of human rights protection. However, as of this writing, the Japanese government has not officially announced the details of or background to its signing of a commitment to place export controls on spyware technology. It is likely that the details of how this agreement will be reflected in domestic regulations are still under consideration or review. Various issues may need further consideration from a commercial and human rights protection perspective, such as the scope of the technologies to be controlled, the existence of destination country-based differences and the strength of the controls. The Japanese government can be expected to announce further details at a later date.