Kaspersky Lab, Inc.に関する事項

米国商務省(以下、商務省)は、Kaspersky Lab, Inc.とその関連会社、子会社、および親会社(Kaspersky)が、特定のサイバーセキュリティおよびアンチウイルス製品およびサービスを米国人に提供する取引を行うことを禁止する最終決定を発表しました。この最終決定に基づき、カスペルスキーのサイバーセキュリティまたはアンチウイルスソフトウェアの再販、カスペルスキーのサイバーセキュリティソフトウェアまたはアンチウイルスソフトウェアの他の製品およびサービスへの統合、または再販または他の製品またはサービスへの統合を目的としたカスペルスキーのサイバーセキュリティまたはアンチウイルスソフトウェアのライセンス供与は、米国または米国人によって禁止されています。

カスペルスキーの製品およびサービスは、米国の国家安全保障および米国人の安全と安全に容認できないリスクをもたらし、米国における情報通信技術およびサービス(ICTS)の完全性と運用を妨害または妨害する過度のリスクをもたらします。特に、米国におけるICTSおよびICTSサプライチェーンの完全性と運用に害を及ぼす重大なリスクがあります。

カスペルスキー製品が禁止されたのはなぜですか?

米国産業安全保障局(BIS)は、大統領令13873および15 C.F.R. Part 791に基づき、カスペルスキーの法的権限に基づくサイバーセキュリティおよびアンチウイルス取引の見直しを実施しました。BIS内の情報通信技術サービス局(OICTS)は、取引が米国に多くのリスクをもたらすと判断し、これらの取引を禁止しました。

カスペルスキー製品がセキュリティリスクと見なされるのはなぜですか?

BISは、カスペルスキーのサイバーセキュリティおよびアンチウイルス製品およびサービス(以下「ICTS製品」)の危険性が、米国の国家安全保障および国民の安全と安全に容認できないリスクをもたらすことを発見しました。考慮されたリスク要因は次のとおりです。

ロシア連邦(ロシア)によってもたらされる脅威。

最終決定では何が禁止されていますか?

BISは、カスペルスキーが米国内または米国人との以下のICTS取引を行うことを禁止する最終決定を発表しました。

- カスペルスキーが設計、開発、製造、または提供したサイバーセキュリティ製品またはサービスの全部または一部を含むICTS取引(最終決定の付録Bに記載されている製品およびサービスを含む)。
- カスペルスキーが設計、開発、製造、または提供したアンチウイルスソフトウェアの全部または一部が関与するICTS取引(最終決定の付録Bに記載されている製品およびサービスを含む)。そして
- カスペルスキーが設計、開発、製造、または供給したソフトウェアの全部または一部をサードパーティの製品またはサービス(「ホワイトラベル」製品またはサービスなど)に統合するICTS取引。

最終決定の対象となる製品およびサービスの非網羅的なリストは、リンク先の付録Bに記載されています。

最終決定は、以下のとおり効力を生じます。

2024年7月20日午前12:00(米国東部夏時間)に、カスペルスキーは、上記の1つ以上のICTS取引に関連する米国人との新たな契約を締結することを禁じられています。

2024年9月29日午前12:00(米国東部夏時間)現在、カスペルスキー、およびその後継者または

カスペルスキーのICTS製品が米国の国家安全保障にもたらす脆弱性。

安全性と、ロシアが提示された脆弱性を悪用した場合の結果。

BISは、カスペルスキーのICTS製品が、米国の国家安全保障および米国人の安全と安全に対して以下のリスクをもたらすことを発見しました。

ロシアは、アメリカ合州国を脅かし続けている外国の敵だ。

カスペルスキーは、ロシア政府の管轄、管理、または指示の対象となります。

カスペルスキーのソフトウェアにより、ロシア政府は米国の顧客の機密情報にアクセスできます。

譲受人は、以下の行為を禁止されます。

- 上記のICTSトランザクションに関連するアンチウイルスシグネチャの更新およびコードベースの更新を提供すること。そして
- Kaspersky Security Network(KSN)を米国内または米国人の情報技術システムで運用する。

2024 年 9 月 29 日午前 12:00 EDT では、以下の行為は禁止されています。

- **転売**Kasperskyのサイバーセキュリティまたはアンチウイルスソフトウェア。
- **統合**カスペルスキーのサイバーセキュリティソフトウェアまたはアンチウイルスソフトウェアを他の製品やサービスに組み込むこと。そして
- **ライセンス**再販または他の製品またはサービスへの統合を目的としたカスペルスキーのサイバーセキュリティソフトウェアまたはアンチウイルスソフトウェア。

米国司法省は、米国の多くの個人や企業が、ウイルスやその他のサイバー脅威からの保護のためにカスペルスキーのソフトウェアに依存していることを認識しています。カスペルスキーソフトウェアのユーザーが代替の製品やサービスを探す時間を確保するため、米国司法省は、カスペルスキーが米国人向けにKSNを引き続き運用することを認めるとともに、付録Bに明記されているように、米国の現在の加入者およびサイバーセキュリティおよびアンチウイルス製品およびサービスのユーザーにアンチウイルスシグネチャのアップデートとコードベースのアップデートを提供できるように、禁止事項を調整しました。 2024年9月29日午前12:00(東部夏時間)まで。

カスペルスキーのソフトウェアでは、悪意のあるソフトウェアをインストールしたり、重要なアップデートを保留したりすることができます。

カスペルスキーのソフトウェアが操作されると、米国の重要インフラなどで、データの盗難、スパイ活動、システムの誤動作などの重大なリスクが発生する可能性があります。また、国の経済安全保障と公衆衛生を危険にさらし、怪我や人命の損失につながる可能性があります。

2024年9月29日午前12:00(米国東部夏時間)以降、カスペルスキーは、上記のICTSトランザクションに関連するアンチウイルスシグネチャのアップデートおよびコードベースのアップデートの提供を禁止されます。米国内または米国人の情報技術システム上で KSN を運用する。

この最終決定は、Kaspersky Threat Intelligenceの製品およびサービス、Kaspersky Security Trainingの製品およびサービス、またはカスペルスキーのコンサルティングまたはアドバイザリーサービス(SOCコンサルティング、セキュリティコンサルティング、アナリストに質問する、インシデントレスポンスを含む)が関与する取引には適用されません。

カスペルスキーのユーザー向けの禁止事項について、詳しくはこちらをご覧ください。

- カスペルスキー個人のお客様
- Kaspersky Businessのお客様
- FAQ
- プレスリリース
- 最終決定
- 付録A - 最終決定において部門が考慮し、対処した情報
- 付録B - 最終決定の対象となるカスペルスキー製品
- DNI公衆脅威評価
- CISA ソフトウェア削除ガイド (個人向け)
- CISA Software Removal Guide for Enterprises

サイバーセキュリティの脅威に関する詳細情報はどこで入手できますか?

国土安全保障省のサイバーセキュリティおよびインフラストラクチャセキュリティ庁(CISA)

CISA は、パートナーと協力して今日のサイバー脅威から防御し、業界と協力して、将来に向けてより安全で回復力のあるインフラストラクチャを構築します。CISA は、利用可能なすべてのリソースを使用して、組織がリスクをより適切に管理し、レジリエンスを高めるのを支援することを目指しており、ここにある無料のサイバーセキュリティ サービスとツールのリストを維持しています。

全米防諜安全保障センター(NCSC)

NCSCは、国家情報長官室の一部であり、米国政府の防諜(CI)および安全保障活動を主導および支援する責任があります。外国の諜報活動が浸透するリスクがある米国の民間部門の組織にCIアウトリーチを提供する。NCSCは、米国政府のサイバーコミュニティおよびICと協力して、外国の諜報活動やその他の脅威アクターのサイバー能力に関する視点を提供し、敵対的なサイバー活動のコンテキストと可能な帰属を提供します。

連邦捜査局(FBI)

FBIは、サイバー攻撃と侵入を調査する主要な連邦機関です。コンピュータへの侵入や攻撃、詐欺、知的財産の盗難、個人情報の盗難、企業秘密の窃盗、犯罪的ハッキング、テロ活動、スパイ活動、妨害行為、その他の外国諜報活動などのサイバー犯罪をFBI現地事務所サイバータスクフォースに報告してください。サイバー犯罪の個々の事例は、サイバー犯罪を報告するための全米の中心的なハブであるFBIのインターネット犯罪苦情センター(IC3)に報告してください。IC3は、被害者と第三者の両方からのインターネット犯罪の苦情を受け付けています。サイバー犯罪の被害に遭ったと思われる場合は、FBIにご連絡ください。

情報通信技術サービス局(OICTS)

BISとOICTSの詳細については、OICTSのメインWebページを参照してください。

の公式ウェブサイト 米国商務省, 産業安全保障局

公開済み *2024年6月20日*
更新 *8月 6, 2024, 06:29 PM EST*