

- ランサムウェアによる被害は、海外において重要インフラサービスが停止する等、引き続き深刻な状況。特に、近年は、データの暗号化と同時に情報の窃取を行い、金銭を支払わなければ当該情報を公開するというより悪質なケースも出現。
- 我が国においても、大手企業等における被害を確認。
- これに対し、G7サミットにおいて声明が出される等、国際的に協力して対処していくこととしており、我が国においても適切に対応していく。

国際社会における対応

G7 [コーンウォールサミット「首脳コミュニケ」\(2021.6.13\)](#)

- ランサムウェアの犯罪ネットワークによる共通の脅威の高まりに緊急に対処すべく協働する

NATO [「首脳コミュニケ」\(2021.6.14\)](#)

- ランサムウェアへの対応を含む[サイバー防衛政策](#)の承認

米国 サイバー事案の予防、検知、評価、修復を推進のための「[国家サイバーセキュリティ向上に関する大統領令](#) (2021.5.12)」

ランサムウェアの脅威に対処するため、早急に措置を講じることを求める「[国家安全保障担当大統領次席補佐官\(サイバー及び新興技術担当\)による企業経営層向け公開メモ](#) (2021.6.2)」

[米露首脳会談](#)においてランサムウェアを含むサイバー攻撃・サイバーについて議論。両国専門家が具体的な理解を深め、両国で発生した事案のフォローアップを行うことに合意(2021.6.16)

英国 [サイバーセキュリティセンター\(NCSC\)長官の年次講演](#)においてランサムウェアを主要なサイバー脅威として警告(2021.6.14)

豪州 国防省アンドリュー・ハスティ副大臣による[ランサムウェア対策に関する声明](#)(2021.6.15)

被害の現状

国外 2021年5月、米国最大の石油パイプラインを運営するColonial Pipeline社がランサムウェアによるサイバー攻撃を受け、5日間操業を停止

2021年6月、食肉加工会社JBS社の米国子会社がランサムウェアによるサイバー攻撃を受け、一部の事業が一時停止

その他、医療機関や自治体においてランサムウェア被害が数多く発生

国内 2020年11月、大手ゲーム会社の一部機器が不正アクセスによりランサムウェアに感染し、顧客や取引先等の約1.6万件の個人情報流出を確認、最大約39万件の個人情報流出した可能性があることが判明

情報処理推進機構(IPA)へのコンピュータウィルス・不正アクセスの届出件数や、民間のサイバー攻撃による被害に関する支援組織への相談件数は増加傾向

政府等における対応

- 我が国においても、内閣サイバーセキュリティセンターにおいて政府関係機関及び重要インフラ事業者等に対して、ランサムウェアによる被害の予防、検知、対応、復旧のための注意喚起を実施する等、関係省庁において、取組を進めている。
- 引き続き、民間分野とも協力しながらランサムウェア被害の防止等に向けた取組を推進する。

内閣サイバーセキュリティセンター

- 重要インフラ事業者等及び一般への注意喚起
(2021.4.30ほか複数回にわたり継続的に実施)
 - ✓ ランサムウェアの感染を防止するための対応策
 - ✓ データの暗号化による被害を軽減するための対応策
 - ✓ 不正アクセスを迅速に検知するための対応策
 - ✓ 迅速にインシデント対応を行うための対応策
- 政府機関等に対する不審な通信の横断的な監視
- 諸外国との情報交換

経済産業省

- ランサムウェアによる被害の急増等を踏まえ、経営者への注意喚起を実施(2020.12.18)
 - ✓ 経営者の関与
 - ✓ 対策におけるリーダーシップ
 - ✓ サイバーセキュリティを踏まえた事業のグローバルガバナンスの構築
 - ✓ 「基本行動指針(共有・報告・公表)」に基づく活動の徹底

警察庁

- ランサムウェア被害における被害相談・注意喚起等を実施
 - ✓ 被害相談への対応・捜査を実施
 - ✓ ウェブサイトにおいて感染防止対策等の情報を発信
 - ✓ 都道府県警察において、一般的な感染手口や感染防止対策等の注意喚起・広報啓発を実施
- 令和4年度からの設置を検討しているサイバー局(仮称)及び実働部隊においてランサムウェア対応を強化
 - ✓ 海外治安機関と連携したランサムウェア被害動向等の情報収集・情報共有の強化
 - ✓ ランサムウェア被害に対する取組の強化
 - ✓ 国際協同捜査への積極的参加