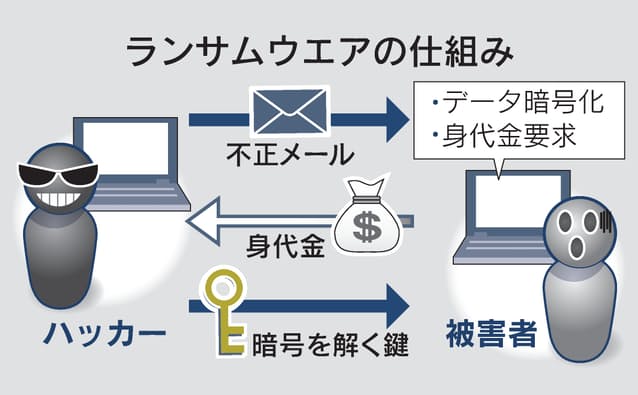
**ランサムウエアとは　システム復元へ身代金要求**

**Techワード**

[ビジュアル用語解説](https://www.nikkei.com/theme?dw=21042000)

2021年6月4日 2:00 [有料会員限定]



パソコンなどのデータを暗号化し、元に戻すために身代金を要求するランサムウエア（身代金要求ウイルス）が近年、猛威を振るっている。米サイバー対策企業の調査では過半数の企業や組織が過去1年以内に攻撃を受け、5月7日には米国の石油パイプラインに被害が出た。攻撃を検知する仕組みを導入するなど防御体制の強化が急務だ。

「おまえが支払わなかったら、漏洩データは自動的に公開される。公開後は少なくとも6カ月、我々のコンテンツ配信サーバー上でさらされることになる」――。サイバー攻撃を受けたある日本企業のパソコン画面に残されたメッセージだ。

2021年5月、米石油パイプライン最大手コロニアル・パイプラインが、犯罪集団「ダークサイド」のランサムウエア攻撃により一時操業停止を余儀なくされた。ダークサイドも身代金を要求する脅迫文を企業に容赦なく突き付けてくる。

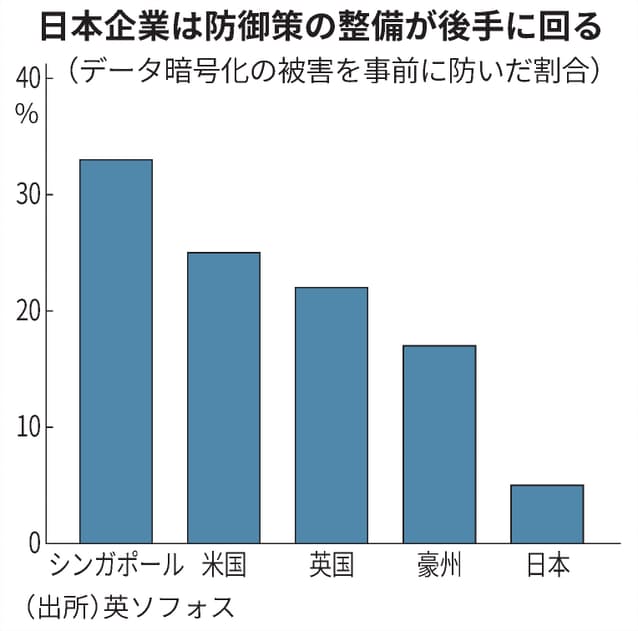
ランサムウエアは17年に世界に拡散した「ワナクライ」によって存在を広く知られるようになった。[ホンダ](https://www.nikkei.com/nkd/company/?scode=7267)や[日立製作所](https://www.nikkei.com/nkd/company/?scode=6501)などの日本企業もシステムに影響を受けた。

その後も攻撃は止まらない。この4～5月には鹿島や[東芝テック](https://www.nikkei.com/nkd/company/?scode=6588)などの海外子会社の被害が判明した。米サイバー対策企業クラウドストライクが日本や米国など世界12カ国・地域で実施した20年夏の調査によれば、過去1年以内に攻撃を受けた企業は56%に達した。

特に19年末からは「二重の脅迫」と呼ぶ手口が横行する。標的企業の社内に侵入すると、まずは大量のデータを盗み出す。続いて元のファイルを暗号化し、その暗号を解くために身代金を要求する。支払いを拒否すれば「盗んだ情報を暴露する」と二重に脅してくる。

犯罪者の脅迫に屈する企業もある。クラウドストライクの同じ調査では身代金を支払ったと回答した日本企業は32%に上り、平均支払額は117万ドル（約1億2700万円）だった。

一方、拒否した企業は実際にデータを闇サイトに暴露されることが多い。ゲーム大手[カプコン](https://www.nikkei.com/nkd/company/?scode=9697)を攻撃した犯罪者集団「RAGNAR LOCKER（ラグナロッカー）」は、従業員のパスポートや社内メールなどとみられるデータを20年11月に公開した。



データを暗号化される前に気づいて防御する必要がある。だが、英サイバー対策企業ソフォスの20年調査によれば、データを暗号化される被害を事前に防いだ日本の企業や組織は5%だけだった。同じ調査で米国は25%が防いでいた。

サイバーディフェンス研究所の名和利男専務理事は「企業はセキュリティーの状態を可視化する対象を大幅に広げるべきだ」と指摘。多くのシステムを監視し、迅速に対処できる体制構築が急務だ。

すべての記事が読み放題　まずは無料体験（初回１カ月）