

# コロナ禍での被害事例

2020年は新型コロナウイルス感染症の世界的なまん延に伴い、政府機関から日本の組織に対して感染症対策の一環としてニュー

ノーマルな働き方の一つであるテレワークが推奨された。組織のテレワークへの移行に伴いWeb会議サービスやVPN（仮想専用ネットワーク）などの本格的な活用が始まった中、それらを狙った攻撃が観測されている。

内ネットワークに接続したところ社内ネットワークにウイルス感染が拡大した。当時、特定のアクセス方法をを行うことでパスワード施行回数制限を回避できる状況だったため、100万回ほどの試行でログインされる恐れがあると、この状況下において数

約900件がインターネット上で公開されていることが判明した。なお、悪用された脆弱性は19年4月にアドバクにおけるセキュリティ方針を策定し、継続的に対策を実施するよう担当者に指示する。また、対策予算の

を行い、従業員に対してセキュリティ教育を実施する。可能であれば、シンククライアントやVPN、ゼロトラストネットワークなどのセキュリティに強いテレワーク環境の採用に、適切なログの取得と継続的な監視を行うことも重要である。独立行政法人情報処理推進機構（IPA）

## テレワークを狙った攻撃

### ■在宅勤務中にウイルス感染、社内に拡大

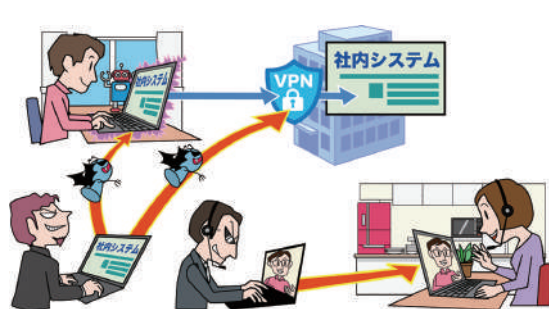
20年4月、在宅勤務中の従業員が社有PCで社内ネットワークを経由せずに外部ネットワークに接続し、SNSを利用した際にウイルスに感染した。その

お、当該脆弱性は、Web会議サービス会社（せいじゃく）性が報告を受けた4月に修正されている。脆弱性の悪用によるVPNの認証情報流出の被害に遭わないために、経営者、セキュ

このようなテレワークなどのニューノーマルな働き方を狙った攻撃のイメージとして、情報リテラシーや個人情報モラル

後、当該従業員が社内の数字であり、パスワードの脆弱性が悪用されて窃取された認証情報

リテラー担当者、従業員や運用ルールの整備を



「テレワークなどのニューノーマルな働き方を狙った攻撃」のイメージとして、情報リテラシーや個人情報モラル

進機構・江島将和

## セキュリティ対策