事　務　連　絡
令和４年１２月８日

各都道府県私立学校主管部課
構造改革特別区域法第１２条第１項の認定を　御中
受けた各地方公共団体の学校設置会社担当課

文部科学省高等教育局私学部私学行政課

「大学等におけるサイバーセキュリティ対策の徹底等について（周知）」の発出について

このたび、大学等の教職員を狙った標的型メール攻撃をはじめとしたサイバー攻撃が頻発していることに鑑み、文部科学大臣所轄学校法人等に対して「大学等におけるサイバーセキュリティ対策の徹底等について（周知）」（令和４年 12 月８日付け事務連絡）を発出し、注意喚起を行いました。

近年のサイバー攻撃は、その手口が従来にも増して巧妙化、多様化しており、被害も大規模になってきています。また、大学等の教職員のみならず、都道府県知事所轄学校法人及び小中高等学校を設置する学校設置会社の教職員も、同様の攻撃の対象となるおそれがあります。

ついては、各都道府県私立学校主管部課及び構造改革特別区域法第１２条第１項の認定を受けた各地方公共団体の学校設置会社担当課におかれては、別添の内容について御了知いただくとともに、必要に応じて所轄の各学校法人及び各会社に対して注意喚起いただくようお願いします。

【別添】
・大学等におけるサイバーセキュリティ対策の徹底等について（周知）（令和４年 12 月８日付け事務連絡）

＜本件連絡先＞
高等教育局私学部私学行政課
連絡先：０３－５２５３－４１１１（内線：２５３３）

別添

個々の教職員を含む大学等を対象としたサイバー攻撃が活発化しつつあり、警察庁及び警視庁からも注意喚起があったことを踏まえ、大学等におけるサイバーセキュリティ対策の徹底等について周知します。各大学等におかれては、学内の教職員にも周知いただくとともに、改めて適切な対策を講じていただくようお願いします。また、万が一被害が発生した場合には、文部科学省及び警察への報告・相談等をお願いします。

事　務　連　絡
令和４年１２月８日

各国公立大学法人担当課
大学を設置する各地方公共団体担当課
各文部科学大臣所轄学校法人担当課
大学を設置する各学校設置会社担当課　御中
放送大学学園担当課
独立行政法人国立高等専門学校機構担当課
高等専門学校を設置する都道府県・指定都市教育委員会担当課

文部科学省高等教育局高等教育企画課

大学等におけるサイバーセキュリティ対策の徹底等について（周知）

各大学及び高等専門学校（以下「大学等」という。）におかれては、日頃からサイバーセキュリティ対策にお取り組みいただくとともに、事案発生時の報告等につき適切に御対応いただき、ありがとうございます。

近年のサイバー攻撃は、その手口が従来にも増して巧妙化、多様化しており、被害も大規模になってきています。各大学等から文部科学省への報告事案を踏まえても、個々の教職員を含む大学等を対象としたサイバー攻撃が活発化しつつあることが見て取れます。

このような状況下、文部科学省としては、「大学等におけるサイバーセキュリティ対策等の強化について（通知）」（令和元年５月 24 日付け元文科高第 59 号）及び「大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて（通知）」（令和４年６月 22 日付け４文科高第 367 号）等において、サイバーセキュリティ対策に係る組織・管理体制の整備や情報セキュリティポリシーの策定などの各大学等における基本的なサイバーセキュリティ対策を徹底いただくとともに、情報セキュリティインシデント等が発生した場合は文部科学省担当部署に御報告をいただくことなどについて周知しております。これを受けて各大学等におかれては適切に御対応をいただいているところですが、依然として、軽微な不注意等に起因する情報漏洩の事例や、個人情報その他の機密情報がネットワーク経由で窃取される事例などが頻発しています。

特に、本年３月頃から、大学等の教職員を狙った標的型メール攻撃が確認されており、

警察庁及び警視庁からも、当該手口によるサイバー攻撃について注意喚起がありました。

ついては、各大学等の設置者におかれては、下記の内容について御了知いただくとともに、各大学等の教職員に対して周知をいただくようお願いします。また、各大学等におかれては、これまでの通知等を参照いただき、学内において適切な対策が講じられているか改めて確認いただき、それを踏まえ更に適切な対策を講じていただくとともに、万が一被害が発生した場合は文部科学省への報告及び警視庁若しくは道府県警察のサイバー犯罪相談窓口又は所轄の警察署への通報・相談を徹底いただくようお願いいたします。

記

１．事案の概要

主に大学等の教職員が個人使用する端末において、標的型メールに添付されたリンクファイルやメール本文に記載された URL へアクセスした結果、マルウェアに感染していることが判明している。

特に、教職員が個人で管理・利用する端末で研究・資料作成などを行っている場合、大学等が管理するネットワーク外であるため、大学等側はマルウェアの感染状況を把握することが困難となっており、被害を受けた教職員もマルウェアに感染していることに気付いていないケースが多発している。

端末がマルウェアに感染すると、当該端末に記録されているデータが窃取される恐れがあり、教職員の研究内容や個人情報を含む資料等が窃取されるなど、場合によっては経済安全保障上、重大な影響を及ぼすおそれがある。

２．本件事案の特徴と対策

(1) 手口

- 実在する組織・人物を騙り、標的となった教職員とメールのやりとりを行う。
- 送信元メールアドレスのドメインが、実在する組織のドメインに類似している。（一文字違い、一文字追加など。）
- メールの内容は極めて精巧であり、大学等の教職員への出講依頼等、正規の依頼であるかのように偽装し、メール本文に記載された URL リンクや関係資料等とされる添付ファイルへ誘導し、当該 URL をクリックしたり添付ファイルを開いたりした端末をマルウェアに感染させる。(URL のリンク先や添付ファイルの内容も巧妙に偽装されており、実際の依頼内容であるかのように誤認させるものとなっている。)
- 最終的に、新型コロナウイルス感染防止等を理由に予定を中止するなどの内容を標的となった教職員に送ることで、正規の組織・人物に依頼内容の確認をさせず、被害の発見を遅らせている。

(2) 有効な対策

- 不審なメールやファイルを不用意に開かない。
- 日常的にやりとりがない組織・人物から来たメールは電話による確認を行う。
- 送信元メールアドレスが過去のメールアドレスと完全に一致するか確認する。

・　教職員の自宅など学外でネットワークを使用する場合は、VPN などを使用し大学のネットワークを使用する。ただし、VPN などは、最新のバージョンにアップデートするなど、対策を徹底する。
・　大学等の関係者、研究室ごとに使用するネットワーク管理が散逸している現状があることから、大学等による一元管理を行う。

（参考）関連通知
・「大学等におけるサイバーセキュリティ対策等の強化について（通知）」（令和元年５月 24 日付け元文科高第 59 号）
・「大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて（通知）」（令和４年６月 22 日付け４文科高第 367 号）

＜本件連絡先＞
（本事務連絡全体について）
文部科学省
高等教育局高等教育企画課
連絡先：０３－５２５３－４１１１（内線：２４７５）

（国立大学法人について）
高等教育局国立大学法人支援課
連絡先：０３－５２５３－４１１１（内線：３７６０）

（公立大学等について）
高等教育局大学教育・入試課
連絡先：０３－５２５３－４１１１（内線：３３７０）

（私立大学等について）
高等教育局私学部私学行政課
連絡先：０３－５２５３－４１１１（内線：２５３３）

（高等専門学校について）
高等教育局専門教育課
連絡先：０３－５２５３－４１１１（内線：３３４７）

（放送大学学園について）
総合教育政策局生涯学習推進課
連絡先：０３－５２５３－４１１１（内線：３４５９）

（その他サイバーセキュリティ等全般について）
大臣官房政策課サイバーセキュリティ・情報化推進室
連絡先：０３－５２５３－４１１１（内線：２２４８）