

ふくしまPITネットワーク No.42

ふくしま技術情報不正流出防止ネットワーク

Fukushima Prevention Network for **I**llegal Leakage of **T**echnological Information

サイバー攻撃の情勢(令和元年)



警察は、先端技術を有する事業者等との情報共有の枠組みを通じて標的型メール攻撃を把握し、事業者等に対して分析した情報を提供しています。

令和元年中の同ネットワークを通じて把握した標的型メール攻撃の件数は**5,301件**であり、送信元メールアドレスが偽装されていると考えられるものが全体の**92%**と引き続き高い割合となっています。

※ 警察庁では、市販のウイルス対策ソフトでは検知できない不正プログラムを添付して、業務に関連した正当なものであるかのように装った電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させるなどして、情報の窃取を図るものを「標的型メール攻撃」としています。



【サイバー攻撃の事例】

- 国内の大手電機会社は、令和元年6月に同社内の端末で不審な挙動を検知し調査した結果、**第三者による不正アクセス**を受け、外部にデータを送信されていたことが判明したと令和2年1月に公表しました。
一部報道によりますと、同社に対する不正アクセスに中国のサイバー攻撃集団が関与した可能性があると報じられています。

- 警察では、国際的ハッカー集団「アノニマス」を名乗る者が、日本国内の組織に対してサイバー攻撃を実行したとする犯行声明とみられる投稿をSNS上に掲載している状況を把握しています。

日本国内の地方自治体、民間企業等を含む8組織のウェブサイト閲覧障害が発生しました。

そのほかにも、国内外で様々なサイバー攻撃が発生しており、今後も世界規模でのサイバー攻撃の発生等が懸念されています。



※ 警察庁ホームページから抜粋

ふくしまPITネットワーク No.43

ふくしま技術情報不正流出防止ネットワーク

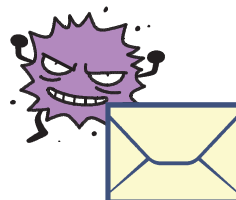
Fukushima Prevention Network for Illegal Leakage of Technological Information

サイバー攻撃の情勢(令和元年)



標的型メール攻撃の特徴

- ・ **「ばらまき型」攻撃の多発傾向が継続**
ばらまき型攻撃が、全体の90%を占め、引き続き高い割合となりました。
- ・ **多数が非公開メールアドレスに対する攻撃**
標的型メールの送信先メールアドレスについては、公開されていないものが全体の82%を占めました。
- ・ **多くの攻撃において送信元メールアドレスを偽装**
標的型メールの送信元メールアドレスについては、偽装されていると考えられるものが全体の92%を占めました。
- ・ **標的型メールに添付されたファイル**
標的型メールに添付されたファイルの形式の割合は圧縮ファイルが全体の87%を占めました。



標的型メール攻撃の事例

- ・ 安全衛生委員会への招待と称して、添付された圧縮ファイルを開くよう誘導するメールが、事業者の非公開メールアドレスに対して送信されました。
- ・ 「賞与支払届」という件名で、メール本文内のリンク先に接続するよう誘導するメールが、事業者の非公開メールアドレスに対して送信されました。

国や自治体、研究機関等を装い、新型コロナウイルスを題材とした標的型メール攻撃も出回っていますので御注意ください。



【標的型メールの例】

差出人： 生産管理課 ●●●●●
送信日時： 2020年●月●日●曜日 ●：●
宛先： ●●●●●
件名： Re:招待:安全衛生委員会-
2020/●/● ●：●～●：●
添付ファイル： ●●●.zip

おはようございます
添付ファイルのご確認、宜しくお願いいたします。
ZIPファイル解凍用パスワード：12345

差出人： ●●●●●
送信日時： 2019年12月●日●曜日 ●：●
宛先： ●●●●●
件名： 賞与支払届

いつも大変お世話になっております。

◆振込データ情報
出金口座： ●●●●●
振込指定日： 2019年12月●日
振込メモ： 2019冬・業績賞与支給

https://.....

できた賞与支払届総括表を
郵送致しますので手続きをお願い致します。
以上、よろしくお願い致します。

ふくしまPITネットワーク No.44

ふくしま技術情報不正流出防止ネットワーク

Fukushima Prevention Network for **I**llegal Leakage of **T**echnological Information

情報漏えい対策(視認性の確保に資する対策)



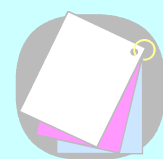
事後的に検知されやすい状況を作り出す対策

○ 秘密情報が記録された媒体の管理等

- ・ 秘密情報が記録された書類、ファイル、記録媒体(USBメモリ等)を、共有して書庫等に保管するとともに、それらの複製を禁止した上で、保管する媒体等に通し番号を付けて管理します。

これによって資料の不足や欠損が生じた場合にすぐに把握できるようにします。

- ・ さらに、共有保管された書類、ファイル、記録媒体を貸し出す場合には、誰にどの記録媒体を貸し出しているかわかるように、貸出時及び返却時に、その日時、氏名、貸し出した資料名等を記録して管理します。



資料の重要性によっては、貸出しを許可制としたり、利用期間を設定して、期間経過後に返却を促す通知を行うことも考えられます。

○ コピー機等における利用者記録・枚数管理機能の導入

従業員等のIDカードとコピー機やプリンター等とを連動させることによって、IDカードによる認証がなければ印刷ができないように設定した上で、コピー機やプリンター等を、誰が、いつ利用したか、どのような資料を何枚印刷したか等を記録します。

