JR東海労新幹線地本　TENKENHANMAR TENKENHANMARTENKENHANM

点検ハンマー

第１１号　発行日　２０１０年１１月０４日　発　責　石尾光春・編　集　地本車技常任委員会

修繕車両所のパソコンがウイルスに感染！

１０月２２日、Ｎ７００系の故障読み出しをするためにパソコンを接続したが読み出しができず、調べてみるとパソコン内に複数のウイルスに感染していることが判明。

急きょ、修繕班とＡＴＣ班の社員が面談され「会社のパソコンに個人のＵＳＢメモリを差し込んだことがあるか？」「ＵＳＢメモリを持ち帰ったことはあるか？」と、恒例の「犯人」探しが行われました。

他の企業でも、ウイルス感染で、社内の機密情報や顧客の個人情報が流失、企業としても信頼を失墜し会社存続の危機に発展しかけない事態が多く報道されています。禁止されている社内情報をＵＳＢメモリに記録し紛失、個人でも社会的制裁をうけています。

最近でも、警視庁などの警察内部資料とみられる文書などのデータがインターネット上に流出、国際テロ捜査情報の可能性もあるとして物議をかもしだしています。

「鉄道会社のパソコンだからウイルスに感染しても問題はない！車両所だから問題はない！」と会社は思っているのでしょうか？なぜ、感染したか原因が分かれば社員に公表すべきです。

社員が感染させたのか？犯人は社員？

感染経路などは不明な中「管理者は感染させていない！」と断言できるのでしょうか？

原因究明を行い、社員に明らかにするのが常識ではないでしょうか。社員からは**「管理者の責任逃れだ！」**との声が出ています。当たり前のことです。

もし、私たち東海労組合員が個人のＵＳＢメモリを会社のパソコンに接続をし、パソコン内のデータをコピーすれば懲戒解雇まで発展する事象であるはずです。

今回は簡単な面談だけで終わったのは何故でしょうか？　不思議でなりません。

もしかして、犯人、原因を探し出すことは都合の悪いことなのか？

今回は、Ｊネットや車両がウイルスに感染したと言われていませんが、今後も感染の危険はない！とは断言できません。ＪＲ東海セキュリティレベルの低さ、常識ある企業では考えられない危機感のなさが現れています。同時にやはり**「ＪＲ東海のセキュリティは社員管理が目的だ！セキュリティと称しながら労務管理が目的！」**と言われて当然の事象であります。