標的型メールの攻撃を受けたことについて

当社宛に送信された、お客様を装った標的型メールの添付ファイルを開封したことにより、当社の業務用パソコンが不正な動きをするプログラム(以下、マルウェアと称します)に感染した事実が判明しましたので、お知らせします。

なお、列車の運行に係るシステムに影響はございません。また、現時点でお客様情報等 の個人情報が流出した形跡は認められませんが、引き続き調査を進めます。

当社としましては、原因究明と、再発防止に取り組んでまいります。

1. 概要について

平成27年8月12日、当社から外部の不審なサーバへのアクセスが確認されたとの連絡が外部機関よりありました。調査の結果、これまでに判明した事実は以下のとおりです。

- ○8月11日、当社宛に送信された標的型メールの添付ファイルを開封したことにより、 当該メールを開いた業務用パソコンがマルウェアに感染しました。
- 〇同日以降、上記のパソコンを経由して、他の業務用パソコン6台が感染しました。
- ○感染したマルウェアは、情報の持ち出しを目的とする種類のものでした。

2. これまでの対応について

- ○8月13日、対策本部を設置し、専門機関の助言と協力の下、対応を開始しました。
- ○8月13日以降、感染を確認の都度当該のパソコンをネットワークから切断して感染の拡大と情報の流出を防ぐとともに、専門機関に解析作業を依頼しました。ネットワークから切断し、専門機関に解析作業を依頼したパソコンは合計7台です。
- ○8月18日夕刻より、外部の不審なサーバへの通信を防ぐため、業務用パソコンからの インターネット接続先を必要最小限に限定しました。あわせて外部への通信監視を強 化しておりますが、以降、外部の不審なサーバへのアクセスは発生していません。
- ○8月20日、専門機関の解析により、感染源が標的型メールであると判明しました。
- ○8月18日から27日の間で、標的型メールを受信していた事実や添付ファイル付き メールを開封する際の具体的な手順を全社員に周知するなど、対応を続けてまいりま した。

3. 今後の対応について

- ○全社員に対して、メール開封時の対応や不審メールの取り扱いについて、更に周知を 徹底してまいります。
- ○新種のマルウェアへの対策、ネットワーク監視による攻撃および情報漏えいの検知の 強化など、セキュリティ対策の強化に取り組んでまいります。
- ○今後の調査で新たな事実が判明した場合、速やかにお知らせいたします。