お取引先各位

ウイルス駆除に関するご報告と感染インシデントの終息について

平素は、格別のご高配を賜り誠にありがとうございます。

去る２０２０年9月１４日に感染したコンピュータウイルスの駆除ならびに、社内ネットワークへの拡散防止策の効果確認が終了しましたのでご報告申し上げます。

また、セキュリティ専門企業と協議した「駆除確認観察項目」について２０２０年9月１６日から２週間にわたり検出が認められませんでしたので、社内のコンピュータウイルス感染インシデントの終息を報告させていただきます。

この度は皆様に多大なご迷惑をお掛け致しましたこと深くお詫び申し上げます。

記

１．ウイルス駆除結果

ネットワークの全てのＰＣでウイルス駆除ソフトによる感染確認を行った結果、ウイルスは検知されず安全が確認されました。なお、感染したＰＣはネットワークから切り離し内容調査中です。調査終了後はネットワーク上での再使用は行ないません。

２．社内ネットワークへの拡散防止策の効果確認

セキュリティ専門企業との協議を経てネットワーク全体に関わる挙動監視と通信制限を適用し不正な動きと不当なデータ通信を行わない社内環境を再構築しました。
その結果、その後の経過観測でも効果的な結果が得られていることを確認しました。

３．駆除確認観察項目と観察結果

別紙のとおりです。

４．ウイルス感染インシデントの終息

別紙のとおり、ウイルス感染から約２週間の経過観察期間にて新たな脅威やウイルス活動が見つかっていないこと、ならびに今後採用予定を含むセキュリティ強化策をご報告することで、弊社内で発生したコンピュータウイルスの終息を宣言させていただきます。何卒ご理解賜りますようお願い申し上げます。

５．引き続き取引先様、関係者様へのお願い

成りすましメールはウイルス攻撃者の bot（自動タスク）によるもので、現在もなお届いていることを確認しております。誠に恐縮ではございますが、引き続き弊社社員に成りすましたメールの添付ファイルは開封せず、削除していただきますようお願い致します。

以上

２０２０年１０月１日

株式会社新開トランスポートシステムズ

（ 別 紙 ）

【ウイルス感染対処後の経過観察結果】

以下の表は、9 月 14 日、9 月 15 日に検出したウイルスの対処後に感染拡大の有無を観察した結果です。9 月 16 日以降の 2 週間に渡り、新たなウイルスの検出は認められませんでした。

【　駆除確認観察項目　】		9/14	9/15	9/16	9/17	9/18	9/19
ウイルス/不正プログラム検知の有無		検出	検出	なし	なし	なし	なし
Web レピュテーション警告の有無	9/20	9/21	9/22	9/23	9/24	9/25	9/26
挙動監視異常検知の有無	なし	なし	なし	なし	なし	なし	なし
機械学習型検索検知の有無	9/27	9/28	9/29	9/30			
C&C サーバーへのアクセスの有無	なし	なし	なし	なし			

以下はセキュリティ強化策として施行、または採用予定の取り組みとなります。

攻撃者による防御看破を避ける意図として、具体的な調査結果や設定値などの公表は致しませんのでご理解お願い申し上げます。

【機械的なセキュリティ強化策】

✓　ウイルス対策エンドポイントの設定強化
✓　機械型学習機能によるウイルス/スパイウェア防衛強化
✓　攻撃元 C&C サーバのレピュテーション設定追加
✓　クライアント PC の CUI 実行制限
✓　総合リスクマネジメントサービスの契約

【PC 利用者のセキュリティ教育強化策】

✓　利用者のセキュリティレベル向上に向けた教育の開催数の追加と「徹底」
✓　ウイルスや脆弱性情報など緊急に対処すべき事項の迅速な周知と「徹底」

【実務環境的なセキュリティ改善策】

✓　全メール利用者の認証情報変更
✓　ウイルス感染者が送受信していたメーリングリストアドレスの変更
✓　オンラインストレージサービスによるセキュアな相互情報共有環境の提供
✓　送信メールの添付ファイル自動暗号化＆WEB ダウンロード化を採用

以上