「衆議院サーバ等ウィルス感染事象について」要旨（11月14日庶務小委員会に報告）

衆議院サーバ等ウィルス感染防止対策本部

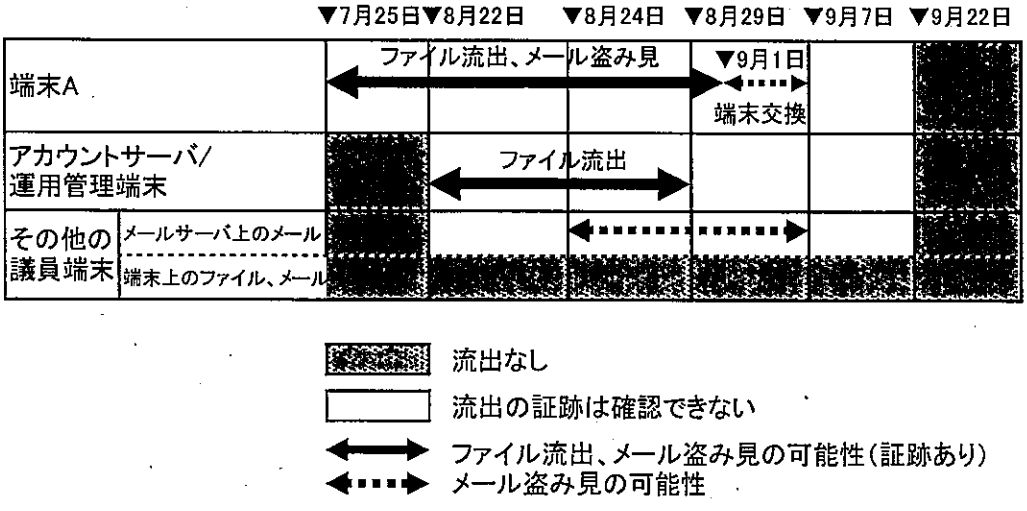
（１）　感染メカニズムの概要

○　本事案は、端末Ａに対する標的型メールの送信及び端末Ａでのメールの開封を発端とした「一次感染」に始まり、議員用アカウントサーバからの「管理者権限のＩＤ及びパスワードの流出」を経て、議員用アカウントサーバ・運用管理端末上での不正プログラムの動作による「二次感染」、そして議員用アカウントサーバから議員用端末を標的とした不正プログラム拡散による「三次感染」と進行していったものと推測

・一次感染：端末Ａ
・二次感染：議員アカウントサーバ４台及び運用管理端末２台
・三次感染：議員端末２５台

なお、悪意のあるメールを送信された３台の端末のうち、２台についてはメールの添付ファイルは開かれずに削除されたため、一次感染とならず

（２）　流出した可能性のあるデータと期間について



○　端末Ａについて

・　７月２５日から２６日の間のいずれかの時点において、端末ＡのＩＤ及びパスワード、衆議院にアクセスするための証明書が窃取されたと推測
・　７月２５日から９月１日の間までファイル流出の可能性あり
・　７月２５日から９月７日までメールを盗み見られた可能性あり

○　サーバと運用管理端末について

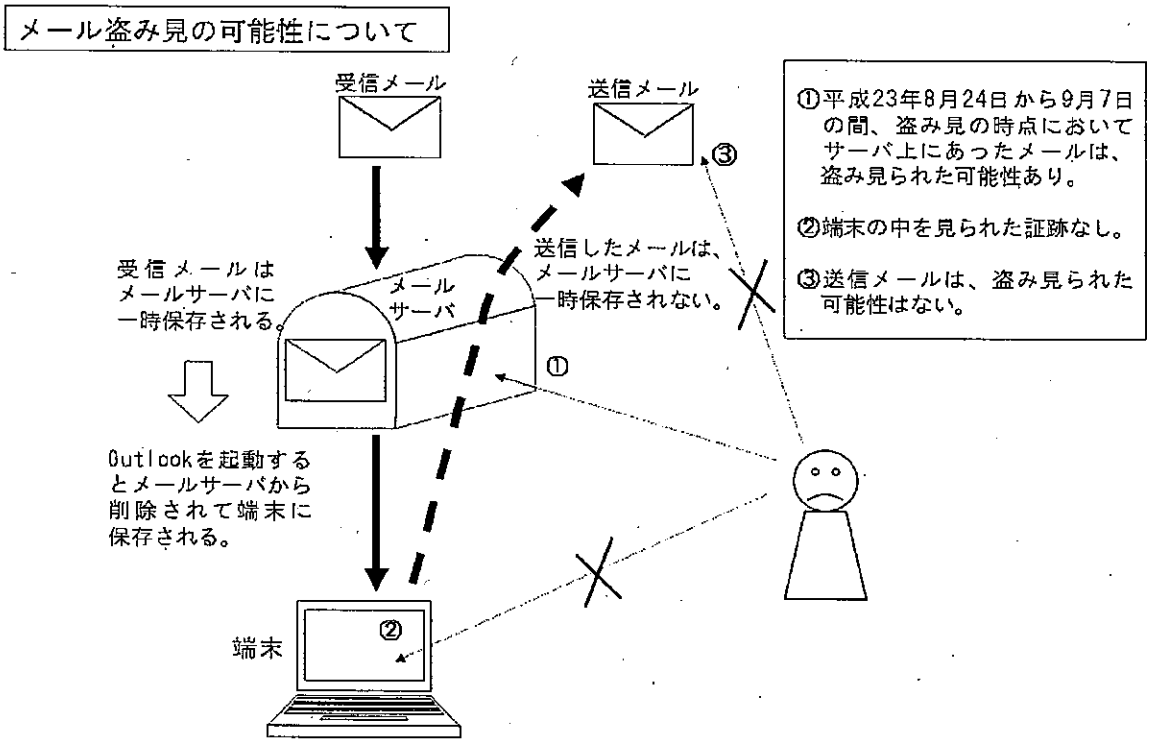
・　管理者権限のＩＤ及びパスワードが流出した８月２２日付の証跡を発見

・　端末Ａから議員アカウントサーバ等に不正なプログラムが埋め込まれ、不正サイトへのアクセスが発生した同月２３日付の証跡を発見。これにより、運用管理端末からドキュメントが流出したと推測

・　運用管理端末から全議員のＩＤとパスワードのハッシュ値を出力するツールの同月２９日付の証跡を発見。このことにより、全議員のＩＤとパスワードのデータが流出したと推測

○　三次感染した２５台を含むその他すべての議員端末について

・　ファイル流出についての証跡は確認されず。ただし、メールサーバ上に保存されていたメールについては、８月２４日から９月７日までの間、盗み見られた可能性あり



これまでに採った措置及び今後の対応について

1　これまでに採った措置等について

１０月２５日：パスワードの定期的な変更をお願い

１０月２７日：「パソコンのセキュリティ対策について」を案内し、速やかなパスワードの変更をお願い

１１月　２日：全議員事務室、会派事務室を訪問。現在の状況を説明して、こまめなパスワードの変更等をお願い

１１月　７日：全議員事務室・会派事務室を順次訪問し、衆議院貸与パソコンのウィルスチェックを実施

2　今後の対応について

対策本部において、今回の調査結果を精査した上で、事務局における対応の問題点等について、反省すべき点、改善すべき点を真摯に検証を行った上で体制の見直しも含めた今後のセキュリティ向上のための対策を検討する