衆議院サーバ等ウィルス感染事象について

平成23年11月14日
衆議院サーバ等ウィルス感染防止対策本部
（NTT東日本からの調査結果に基づく）

1．発生の原因と経緯

本事案は、悪意のあるメールが3台の議員端末に送信され、うち1台の議員端末（以下端末A）において、添付ファイルを開封・実行したことによる“一次感染”に端を発している。

その後、

①二次感染：議員用アカウントサーバ（4台）及び議員用運用管理端末（2台）への感染

②三次感染：25名の議員の議員端末への感染

へと感染範囲が拡大した事案である。

この事案は、平成23年8月29日にサーバ類の日常点検時において、不正プロセスが発見されたことにより、その後の端末Aのデータ解析及びサーバ等のログ解析により、以下の事実が判明した。

1）一次感染

平成23年7月25日：端末Aにて悪意のあるメールを受信し、添付ファイルを開封・実行したことにより、端末Aがウィルスに感染したと推測される。直後に、端末Aから不審なアドレス宛にメールが送信された証跡が発見された。

平成23年7月26日：端末Aが不正な外部通信（不正サイト（γ））を行った証跡が発見された。

平成23年7月27日：端末Aからキーボード入力情報を不正に記録したファイルが発見された。このことにより、端末Aのキーボード入力情報が窃取されたと推測される。

これらのことから、7月25日～26日の間に、端末AのIDとパスワード、認証証明書（SSL）、同月27日以降に端末Aのキーボード入力情報が窃取されたと推測される。

2）二次感染

平成23年8月22日：端末Aが議員用アカウントサーバに管理者権限で不正ログオンした証跡が発見された。このことにより、管理者権限のIDとパスワードが流出し、端末Aから院内LANへの不正制御が可能となったと推測される。

平成23年8月23日：端末Aから議員用アカウントサーバ等に不正なプログラム（ア）が埋め込まれたことにより、議員用アカウントサーバ・議員用運用管理端末がウィルスに感染し、不正サイト（α）、（β）へのアクセスが発生した。このことにより、ドキュメントが流出したと推測される。

平成23年8月29日：議員用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証跡が発見された。さらに、端末AからIDとパスワードのハッシュ値2676件の証跡が発見された。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される。

2676件の内訳：ユーザID 1142件、コンピュータ個体番号 1534件
＊ハッシュ値：関数を用いて暗号化したデータ

3）三次感染

平成23年8月30日：端末Aにより議員用アカウントサーバに埋め込まれた三次感染源となる不正プログラム（イ）により、議員用アカウントサーバにログオンしたほかの議員端末に不正プログラム（イ）がコピーされ、25台の議員端末がウィルスに感染したと推測される。なお、当該25台の感染端末からのデータ流出の証跡は確認できない。（8月30日にサイトブロックを実施済）

2．対策

1）一次感染対応策

・平成23年9月1日　：端末Aの交換実施
・平成23年9月6日　：不正サイト（γ）へのブロック完了
・平成23年9月14日：端末Aのパスワード変更
・平成23年9月22日：端末Aの認証証明書（SSL）の失効

これらの措置により、端末Aの正常化が完了。

2）二次感染対応策

・平成23年8月29日：感染疑いの運用管理端末2台を院内LANから切り離し
・平成23年8月29日：議員用アカウントサーバ4台の不正プログラム（ア）削除
・平成23年8月29日：不正サイト（α）へのブロック完了
・平成23年8月30日：不正サイト（β）へのブロック完了
・平成23年8月31日：議員用アカウントサーバ1台を院内LANから切り離し
　　9月8日　：議員用アカウントサーバ1台を院内LANから切り離し

これらの措置により、不正サイトへのデータ流出防止完了。

3）三次感染対応策

・平成23年9月2日：議員用アカウントサーバの三次感染源となる不正プログラム（イ）削除
・平成23年11月4日：感染の疑いがあった25台の議員端末の不正プログラム（イ）確認及び削除完了

これらの措置により、三次感染端末の正常化完了

4）その他対応策

・平成 23 年 9 月 14 日：端末 A の ID とパスワードを利用した特定プロバイダ以外からの侵入証跡が発見されたため、リモートアクセスルートを特定プロバイダ経由に限定

（8 月 24 日～9 月 7 日の間に侵入を示す証跡）

この措置により、特定プロバイダ以外を経由した不正サイトへのデータ流出防止および不正サイトからのリモートアクセスルート防止完了。

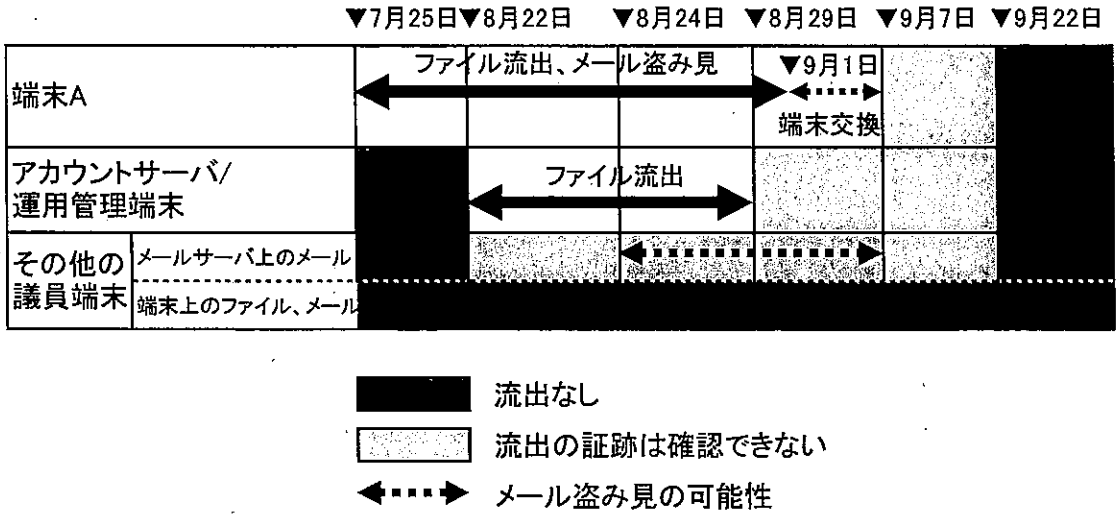
3．感染の影響（推測）

本事案における議員端末および議員用アカウントサーバ等における、ウィルス感染によるメール盗み見およびファイル流出の可能性期間については以下の通りと推測される。

① 端末 A（1 台）：7 月 25 日～9 月 1 日までファイル流出の可能性あり
：7 月 25 日～9 月 7 日までメール盗み見の可能性あり（侵入証跡あり）

② アカウントサーバ/運用管理端末（計 6 台）：8 月 22 日～8 月 29 日までファイル流出の可能性あり

③ その他の議員端末：ファイル流出の証跡は確認できない（可能性はあったが、流出していないと推測）
：8 月 24 日～9 月 7 日までメール盗み見の可能性あり（侵入証跡あり）



感染メカニズムの概要図

【資料1】

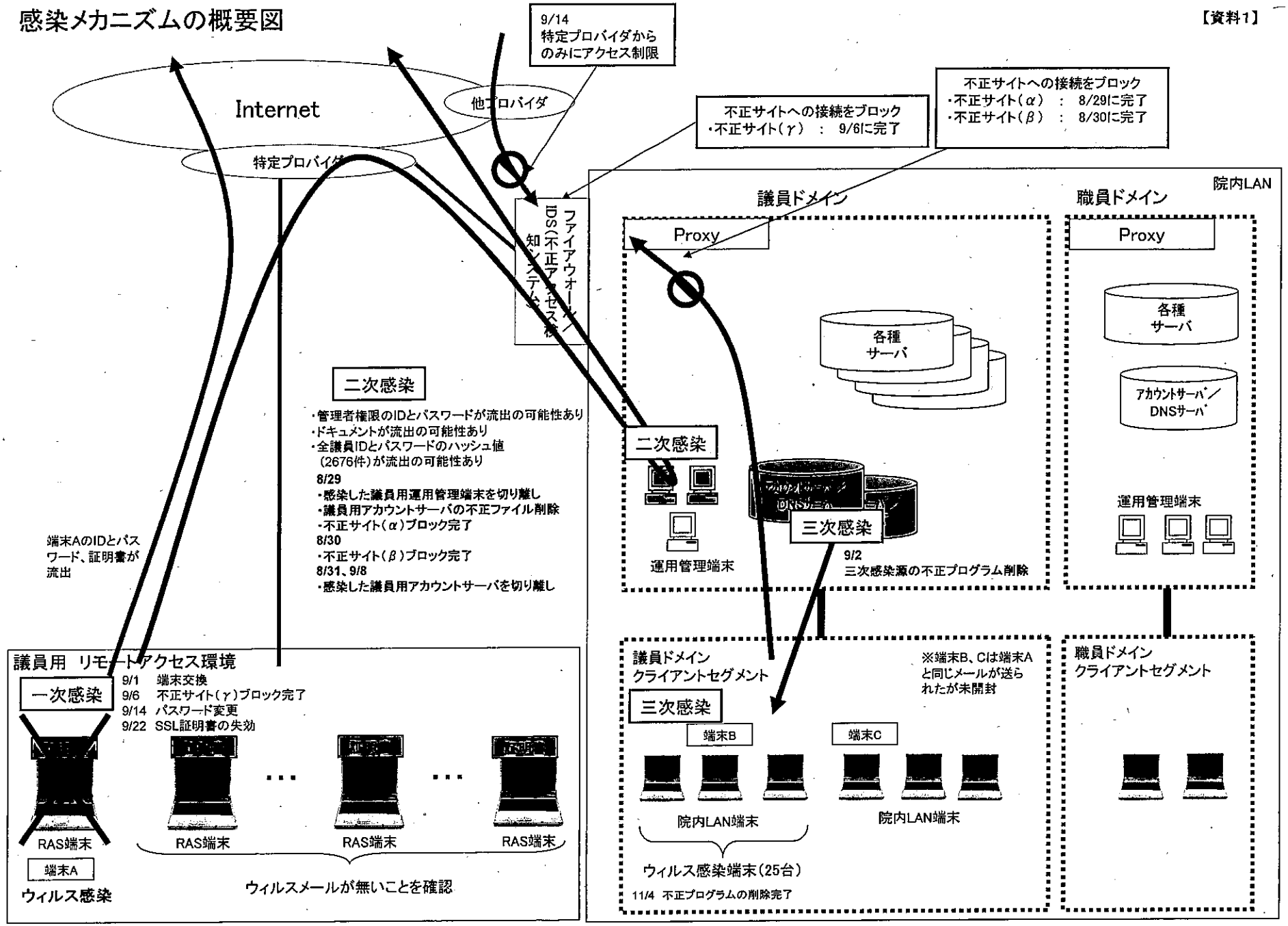


表:ウィルス被害の推測

◎:流出なし
○:流出証跡は確認できない(流出の可能性は極めて低い)
△:端末AのIDとパスワードを利用した特定プロバイダ以外からの侵入の証跡あり
×:流出の可能性あり

状態:
端末A以外の影響がない期間 → 端末A以外に感染が広がった期間 → 不正サイトへのアクセスブロックにて議員端末から情報流出を制限できた期間 → 外部への流出防止がほぼ完了できた期間 → 完了

影響:
- 8/22～9/22 流出および盗み見が技術的に可能な状態であった期間
- 8/22～8/29 サーバ及び端末(計7台)において情報流出の可能性があった期間(議員が利用する端末は1台)
- 8/24～9/7 端末AのIDとパスワードを利用した、特定プロバイダ以外からの侵入の証跡があった期間(メールを盗み見の可能性はあったが判別不可能)

▼7/25 端末Aウィルス感染
7/25 端末Aより不審な宛先へのメールログあり
7/26 FTPコマンド用スクリプトファイル(外部へ通信した可能性を示す)作成の証跡
▼ 8/22 議員用アカウントサーバに管理者権限で不正アクセス開始
▼8/29議員用運用管理端末の院内LANからの切り離し
8/29,30 議員用プロキシにて不正サイトのブロック完了
▼9/1端末A交換
▼9/14 端末Aのパスワード変更 特定プロバイダのみ許可
▼9/22 端末AのSSL証明書の無効化

		7月25日 ～ 8月21日		8月22日 ～ 8月29日		8月30日 ～ 9月14日				9月15日 ～(SSL証明書無効化まで)		9月22日 ～		備考
		メール	ファイル	メール	ファイル	メール		ファイル		メール	ファイル	メール	ファイル	
端末A(1台)		× ・キーボード入力情報流出(情報を取得した証跡あり)	× ・ネットワーク情報流出 ・キーボード入力情報流出(情報を取得した証跡あり)	× ・キーボード入力情報流出(情報を取得した証跡あり)	× ・ネットワーク情報流出 ・キーボード入力情報流出(情報を取得した証跡あり)	× 9/1に端末A交換	△ (9/7 9:05以降SSL侵入なし)	× 9/1に端末A交換	◎	◎ パスワード変更	◎	◎	◎	
議員用運用管理端末(2台) 議員用アカウントサーバ(4台)			◎		× ・ネットワーク情報流出 ・議員用運用管理端末上のドキュメント(情報を取得した証跡あり)			○			○		◎	
その他の議員端末	メールサーバ上のメール	◎		△ (8/24 11:55 初めてSSL侵入)		△ (9/7 9:05以降SSL侵入なし)				○		◎		8/30～9/2 三次感染した議員用端末が25台あったが、議員用プロキシにて不正サイトへのブロック措置を行っていたため、外部への情報流出の証跡は確認できない。
	端末上のファイル、メール	◎	◎	◎	◎	◎		◎		◎	◎	◎	◎	

①8/22～8/29 サーバ及び端末(計7台)において情報流出の可能性あり。(議員が利用する端末は1台)
②ファイルの流出については7台以外に証跡は確認できない。