衆議院サーバ等ウィルス感染防止対策本部
平成２３年１１月２４日現在

これまでに採った措置及び今後の対応について

１．衆議院ＬＡＮのセキュリティ対策関係

（１）事象発生以前からのセキュリティ対策

ファイアウォール

ウィルス対策ソフト（サーバ、端末）……複数ベンダーによる多重検知

ＩＰＳ（攻撃防御システム）、　ウィルス対策ゲートウェイ　　等

（２）８月２９日（サーバの異常検知日）以降

日常点検を含む運用管理体制において、不正サイトへの通信の有無や管理者権限での認証失敗ログの有無等について、監視強化対応を継続中。

- 本事案に関する対応としては、プロキシ、ファイアウォール及びメールサーバ等、各サーバ機器に流出防止対策を設定済み

２．議員室等への周知・啓発関係

１０月２５日　新聞報道への対応状況を案内し、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、会派事務室を訪問し、現在の状況を説明の上、こまめなパスワードの変更等をお願い

１１月　７日～１１月１５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全台の緊急点検（ウィルスチェック）を実施

１１月２５日～１２月　８日（予定）
情報セキュリティ研修の実施（別添ご案内参照）

さらに、ヘルプデスク等を通じ、ウィルス等の相談に対応し、機会あるごとにパスワードの定期的変更をご案内。

３．対策本部としての今後の対応

対策本部において、今回の調査結果を精査し、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。

平成23年11月22日

議　　員　各位
議員秘書　各位
会　　派　各位

情報セキュリティ研修のご案内

衆議院事務局
情報化推進室

情報セキュリティ研修を下記の通り実施いたします。

・日　　時　平成23年11月25日（金）～12月8日（木）【平日のみ　１０日間】
１日５回…①10時～　②11時15分～　③13時30分～
④15時～　⑤16時15分～

・所要時間　１回45分程度

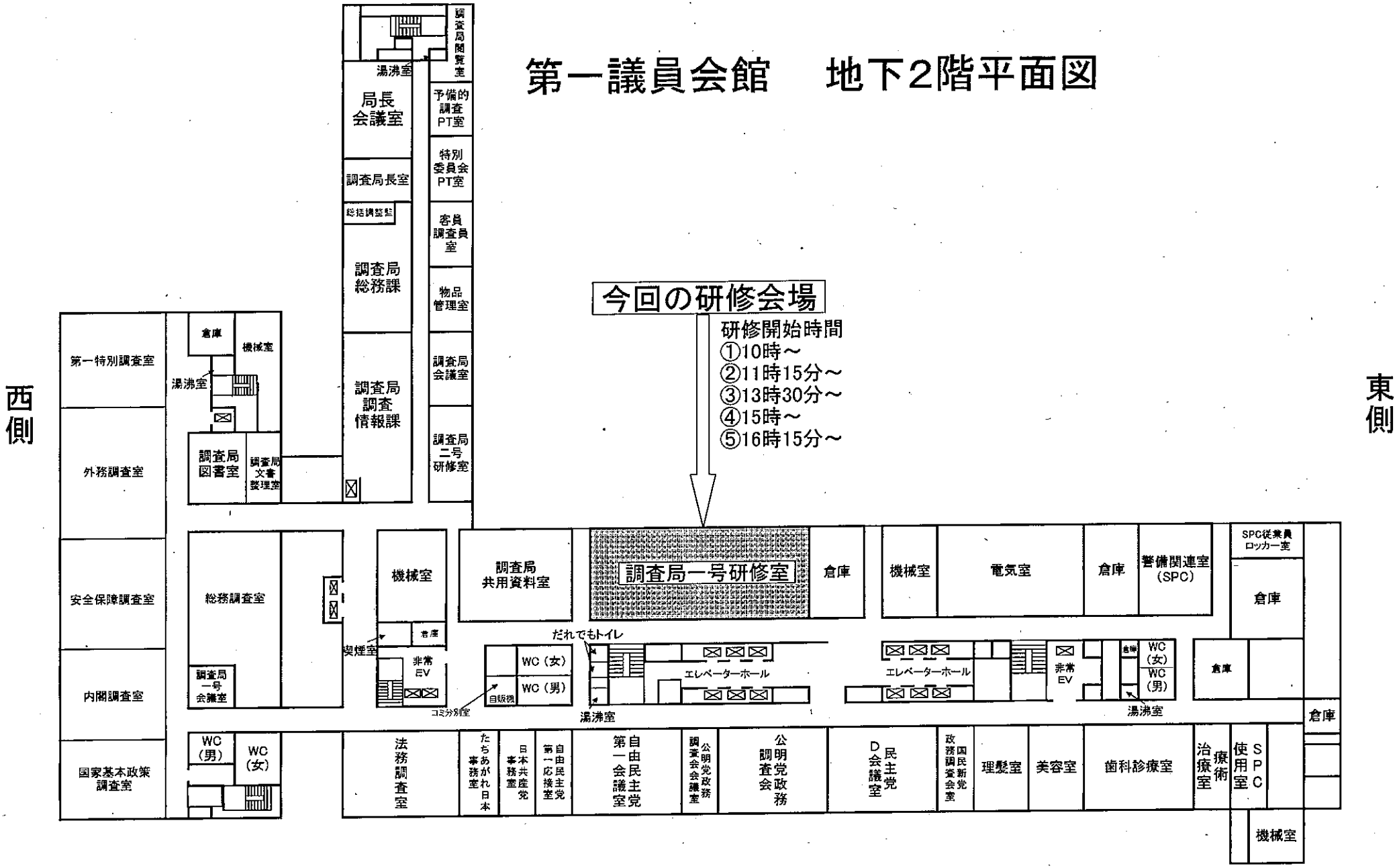
・場　　所　調査局一号研修室（第一議員会館B2）別紙平面図参照

・内　　容　一般的なセキュリティ対策について
（ウィルススキャンの手順、心当たりのないメール対応、
パスワードの定期的変更、外部媒体の使用、
衆議院BBについての注意事項　等）

・そ の 他　　お手数ですが、名刺を１枚ご持参ください。

お問い合わせ先　情報化推進室　内線３４４７０・３４４７５

第一議員会館　地下2階平面図



衆議院サーバ等ウィルス感染防止対策本部の動向

○ 衆議院サーバ等ウィルス感染防止対策本部会合（第１回）
・ 日　　時　　平成 23 年 10 月 26 日（水）
・ 議事要旨　　これまでの経緯等について説明が行われ、質疑応答を行った結果、下記の項目について決定した。
　・ 次回会合は、28 日（金）開催
　・ 事実解明チーム及びセキュリティ対策樹立チームの２チームを設置
　・ 中間報告を次回本部会合で聴取

○ 衆議院サーバ等ウィルス感染防止対策本部　事実解明チーム会合（第１回）
・ 日　　時　　平成 23 年 10 月 27 日（木）
・ 議事要旨　　ＮＴＴ東日本から説明を聴取した後、事実確認を再度行った上で、資料等の時系列整理を行った文書を「中間報告の聴取結果」として、28 日（金）に開催される第２回対策本部会合に提出することを決定した。

○ 衆議院サーバ等ウィルス感染防止対策本部会合（第２回）
・ 日　　時　　平成 23 年 10 月 28 日（金）
・ 議事要旨　　本部長から、ＮＴＴ東日本からの聴取に基づく「中間報告の聴取結果」について対策本部を代表して議院運営委員会庶務小委員会に説明することが提案され、了承された。

○ 衆議院サーバ等ウィルス感染防止対策本部　セキュリティ対策樹立チーム会合（第１回）
・ 日　　時　　平成 23 年 10 月 28 日（金）
・ 議事要旨　　情報化推進室長及びＮＴＴ東日本から、議院運営委員会庶務小委員会に報告された「中間報告の聴取結果」について説明があり、衆議院における今後のセキュリティ対策について議論した。主な議論項目は以下のとおり。
　・ こまめなパスワード変更のお願い
　・ セキュリティ対策について全議員室に協力を求める
　・ ユーザが留意すべきセキュリティについて、秘書等を対象とした研修の実施検討

○ 衆議院サーバ等ウィルス感染防止対策本部会合（第３回）
・ 日　　時　　平成 23 年 11 月 14 日（月）
・ 議事要旨　　本部長から、ＮＴＴ東日本からの調査結果に基づく「衆議院サーバ等ウィルス感染事象について」を対策本部としての調査結果とすること及び本部長報告のとおり対策本部として議院運営委員会庶務小委員会に報告することが提案され、了承された。

○ 衆議院サーバ等ウィルス感染防止対策本部　セキュリティ対策樹立チーム会合（第２回）

・ 日　　時　　平成 23 年 11 月 18 日（金）

・ 議事要旨　　衆議院における今後のセキュリティ対策について議論した。主な議論項目は以下のとおり。

- 早急にとり行うべき対策と中長期的に取り組むべき対策との仕分け
- 関係機関との連携及び情報共有

○ 衆議院サーバ等ウィルス感染防止対策本部　セキュリティ対策樹立チーム会合（第３回）

・ 日　　時　　平成 23 年 11 月 22 日（火）

・ 議事要旨　　衆議院における今後のセキュリティ対策について議論した。
セキュリティ対策樹立チームにおけるこれまでの議論を取りまとめ、対策本部に報告することを決定した。

衆議院

議院運営委員会庶務小委員会

小委員長　松　野　頼　久君（民主）

山　井　和　則君（民主）

笠　　浩　史君（民主）

田名部　匡　代君（民主）

糸　川　正　晃君（民主）

鷲　尾　英一郎君（民主）

佐　藤　　勉君（自民）

髙　木　　毅君（自民）

遠　藤　乙　彦君（公明）

佐々木　憲　昭君（共産）オブザーバー

服　部　良　一君（社民）オブザーバー

衆議院サーバ等ウィルス感染防止対策本部名簿

平成２３年１０月２６日現在

○ 本部長

	小　島　克　美	衆議院事務局庶務部長

○ 構成員

（事）	服　部　　創	衆議院事務局庶務部広報課長
（事）	中　村　　実	衆議院事務局庶務部会計課長
（事）（対）	加　藤　祐　一	衆議院事務局庶務部会計課 情報化推進室長
（対）	能　勢　雄　一	衆議院事務局庶務部電気施設課長
（対）	木　本　裕　司	内閣官房情報セキュリティセンター 内閣参事官
（事）（対）	齋　藤　義　男	東日本電信電話株式会社理事 公共営業部長
（事）（対）	西　本　逸　郎	株式会社ラック取締役
（事）（対）	江　尾　一　郎	株式会社ラックサイバー救急センター センター長
（事）（対）	関　　宏　介	株式会社ラックサイバー救急センター 主席調査員
（事）（対）	大　村　康　晴	株式会社ラックサイバー救急センター 調査員

○ オブザーバー

（対）	若　林　一　広	衆議院事務局ＣＩＯ補佐官
（事）（対）	永　井　達　也	警察庁警備局警備企画課長

（事）：事実解明チーム
（対）：セキュリティ対策樹立チーム

（参考）

「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

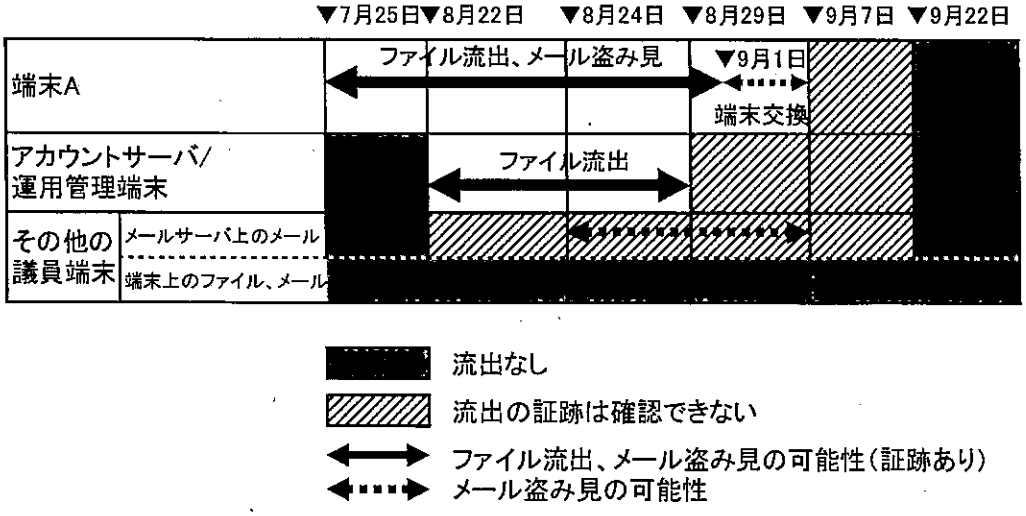
（１）　感染メカニズムの概要

○　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

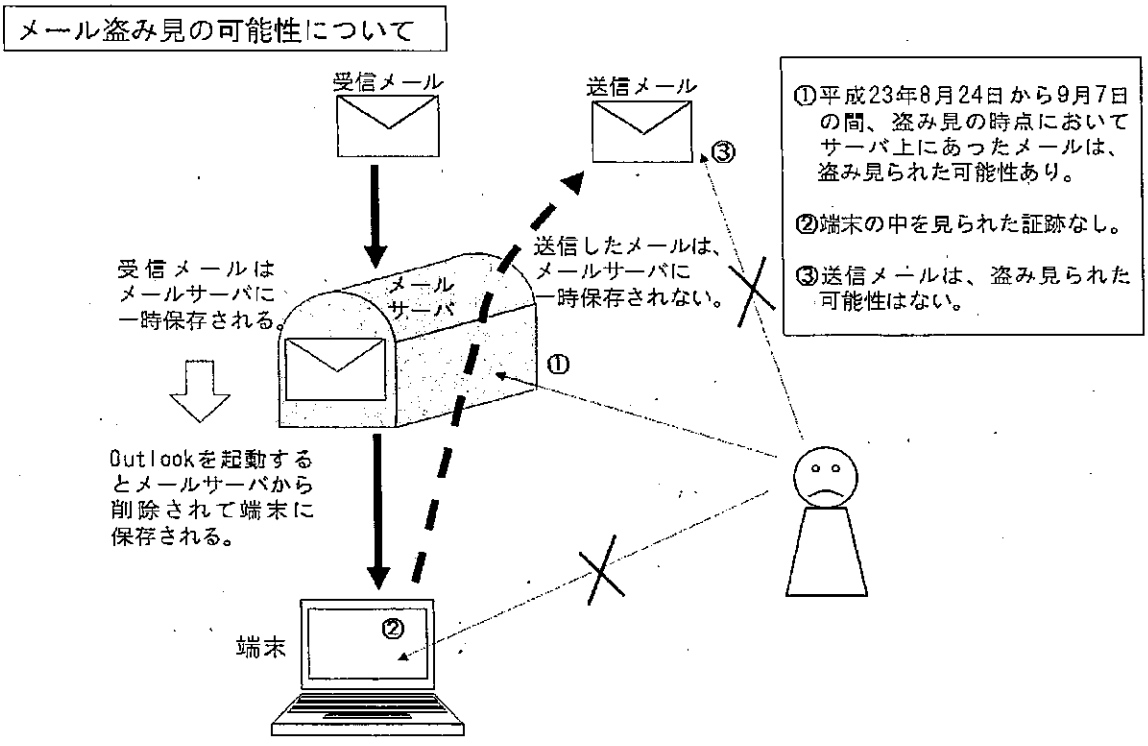
・　管理者権限のＩＤ及びパスワードが流出した８月２２日付の証跡を発見

・　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



平成23年11月24日
情報化推進室

参議院サイバー攻撃に関する報告

1．確認した事象

事象１）本年７月下旬、不審メール（送信者「syoutenn_aguri@aol.jp」、件名「お願い事」）が、議員室のパソコンに到着していた。

事象２）本年８、９月、議員室のパソコンから不正な通信が疑われるメールが、フリーメールアドレスへ発信されていた。

事象３）本年８月から１０月にかけて、衆議院のサイバー攻撃に関する中間報告で不正通信のアクセス先とされた不正サイト（α、β、γ）のうちα、βへ議員室のパソコンからアクセスしていた。
なお、事象２の全てのパソコンに事象３も該当している。

事象４）本年８月から１０月にかけて、事象３の調査中の一部のパソコンから、サーバに不正アクセスしていた。

2．本日までの対応状況

10月25日(火)

○　衆議院へのサイバー攻撃に関する報道（朝日新聞）。

(措置)

・　サーバの調査及びウイルス検査開始。
　　→10月26日（水）感染は確認されなかった。

(議員室対応)

・　議員事務室へ注意喚起のお知らせ。

10月28日(金)

○　衆議院へ送信された不審メールの送信者「syoutenn_aguri@aol.jp」、件名「お願い事」、添付ファイル「Photo.zip」の情報を受領。

(措置)

・　当該不審メールの受信状況等調査開始。

(議員室対応)

・　議員事務室へ注意喚起のお知らせ。
・　議員事務室へ不審メール情報（送信者「syoutenn_aguri@aol.jp」、件名「お願い事」、添付ファイル「Photo.zip」）のお知らせ。

11月1日(火)

○ 不審メール（送信者「syoutenn_aguri@aol.jp」、件名「お願い事」）が、議員室のパソコンに到着していたことを確認（事象１）。

(措置)

・ 当該パソコンについて調査開始。

→11月2日（水）までに、当該パソコンの感染は確認されなかった。

(議員室対応)

・ 事象１についての調査の途中経過等のお知らせ。

11月2日(水)

○ 参議院もフリーメールアドレスへ不正通信があったとの報道（読売新聞）。

○ 議員室のパソコンから不正な通信が疑われるメールが、フリーメールアドレスへ発信されていたことを確認（事象２）。

→11月7日（月）までに当該パソコンをネットワークから切り離し。

(議員室対応)

・ 事象１についての最終調査の結果のお知らせ。

11月4日(金)

○ 不審メール（送信者「syoutenn_aguri@aol.jp」、件名「お願い事」）に関連する不正サイト（α、β、γ）の情報を受領。

(措置)

・ 当該不正サイトへのアクセス状況等調査開始。

(議員室対応)

・ 議員室へ、情報流出防止対策として、重要データの外部メディアへの移動と外部メディア上での使用、パスワードの変更、ウイルス対策ソフトの完全スキャンの実施のお知らせ。

11月7日(月)

○ 不正サイト（α、β）へアクセスしたと思われる議員室のパソコンを検出（事象３）。

→11月10日（木）までに当該パソコンをネットワークから切り離し。

(議員室対応)

・ 議員室へ、「不正サイト等へのアクセス禁止の注意喚起」、「すべてのパソコンへの調査の協力依頼」、「情報セキュリティ研修の開催」、「セキュリティの具体的対策」をお知らせ。

11月21日(月)

○ 事象３の調査中の一部のパソコンから、サーバに不正アクセスしていたことを確認（事象４）。

→当該サーバを直ちにネットワークから切り離し。

（議員室対応）

- 議員室へ、情報流出防止対策として、不正通信発見時のＬＡＮの遮断体制、パスワードの変更、ＯＳ等のアップデートの実施、メールソフトのプレビュー機能の無効化のお知らせ。

３．利用者側の対策

① パソコン本体に保存している重要なデータ、メールは、ＵＳＢメモリ、外付けハードディスク又はＳＤカード等の外部メディアに移してください。
当該データを編集等する場合は、外部メディア上で行ってください。

② ＯＳや次のようなアプリケーションは最新の状態にアップデートしてください。
Microsoft office 製品、Adobe Reader / Acrobat / Flash Player、Oracle Java SE

③ 参議院ネットワークシステムでは常時監視を実施しております。不正な通信を発見した際には、御連絡いたしますので、直ちにLAN ケーブルを抜いてください。

④ 少しでも不審と思われるメールの添付ファイルは開かないでください。また、不審な URL にはアクセスしないでください。もし、不審な点を見い出しましたら、ヘルプデスク（７７２２２）に相談してください。

⑤ 差出人欄が、フリーメールアドレスや普段やりとりのない@ドメインの場合、件名に【至急】、【重要】が付されている場合、差出人メールアドレスと署名のメールアドレスが違う場合は、不審メールの可能性があります。

⑥ 万が一不審なメールの添付ファイル等を開封してしまった場合は、直ちに LAN ケーブルを抜き、ヘルプデスクに御連絡ください。

⑦ メールソフトのプレビュー機能を無効にしてください。

⑧ Windows のパスワードやメールのパスワードを、直ちに、変更してください。

⑨ パスワードは、「他者に知られない」「他者に教えない」「忘れない」「容易に推測可能なものを用いない」「定期的に更新する」ことを徹底してください。

⑩ 私有パソコンについては、所有者において安全対策を徹底してください。御不明な点はヘルプデスクに相談してください。

4．ネットワーク管理者側の対応

以下を実施又は予定しています。

① 全官物・私有パソコンのウィルスチェック等の実施
（実施中～12月5日最終報告（予定））

② 感染が疑われるパソコン等の専門調査会社による調査
（実施中～12月中・下旬最終報告（予定））

③ システム監査の実施
（実施中～12月中・下旬最終報告（予定））

④ 抜本的なセキュリティシステムの設計調査
（実施中～12月中・下旬最終報告（予定））

⑤ 情報セキュリティ研修の実施
（11月21日～29日）

⑥ 私有パソコンに対する最新ウイルスソフトの提供
（11月18日～）

⑦ 不正通信の常時監視の実施
（11月21日～）

以　上

参議院

議院運営委員会 庶務関係小委員会

小委員長　水落敏栄君（自民）

梅村聡君（民主）

川合孝典君（民主）

川崎稔君（民主）

榛葉賀津也君（民主）

中谷智司君（民主）

松浦大悟君（民主）

吉川沙織君（民主）

石井浩郎君（自民）

上野通子君（自民）

大家敏志君（自民）

松山政司君（自民）

義家弘介君（自民）

長沢広明君（公明）

水野賢一君（みんな）