11月14日　参議院
庶務関係小委員会報告

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。

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。

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 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。

④ 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。

⑤ 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。

⑥ 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。

⑦ 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21日ダウンロード開始（予定））

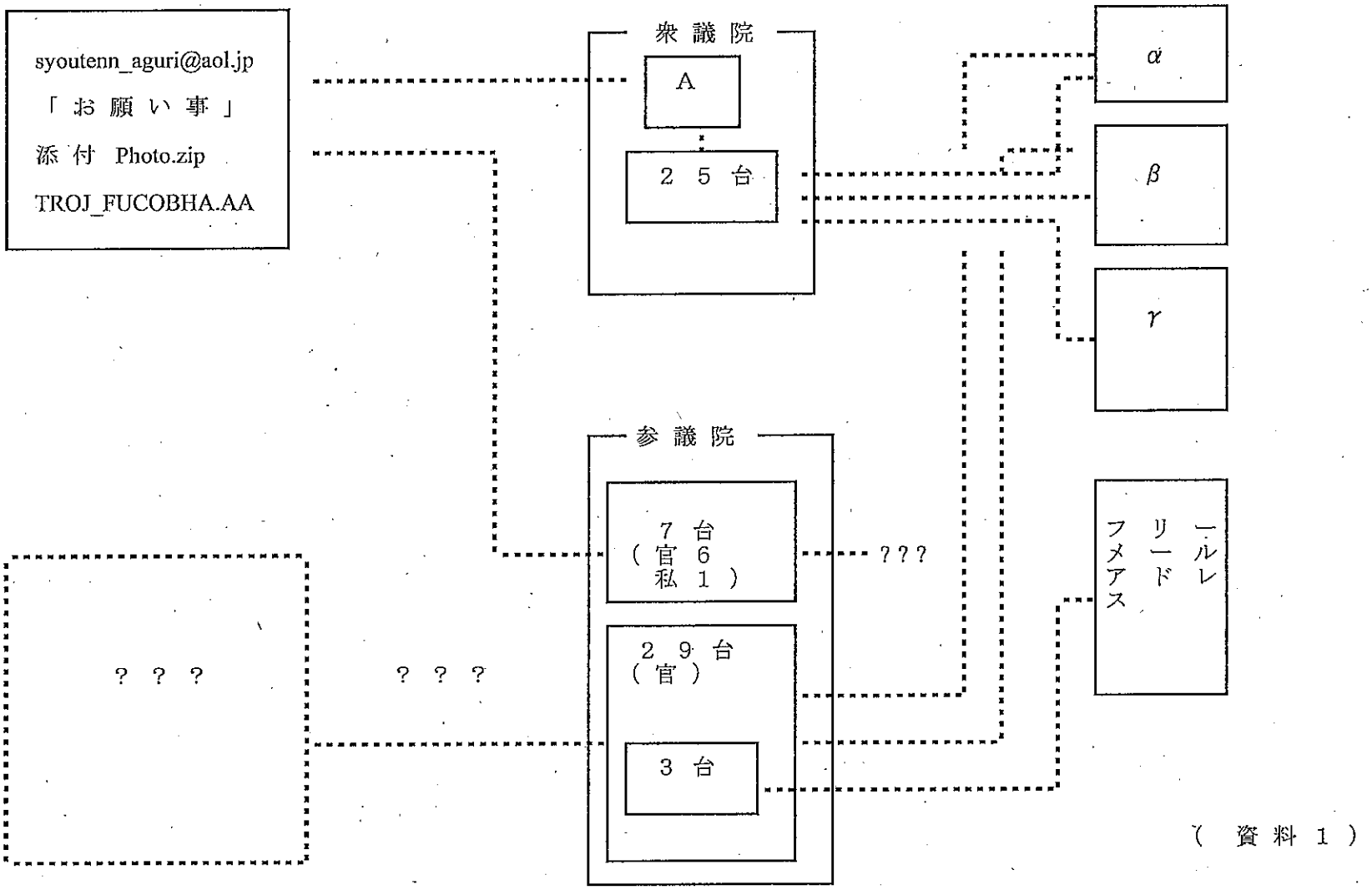
⑦ 不正通信の常時監視の実施
（12月上旬運用開始（予定））

以　上

ネットワークシステム　セキュリティ向上対策工程表（案）

平成23年11月14日
情報化推進室

対策	作業内容	期間	備考
		11月 / 12月	
① 全官物・私有パソコンのウィルスチェック等の実施	議員室に設置している官物・私有パソコンのフルスキャンの実施・支援及びセキュリティ設定の現状調査の実施。調査の結果、不備が確認されたパソコンの設定・支援等を行う。	ウィルスチェック現状調査 → 対策	12／5　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	専門調査会社が、感染が疑われるコンピュータを解析し、コンピュータウィルスによる感染の有無、被害状況、感染経路等の調査を実施する。	解析作業	12月中・下旬最終報告（予定）
③ システム監査の実施	システム監査会社が、現行のネットワークシステムの脆弱性、運用の実態等を調査し、堅牢性の確認結果、改善点等について監査報告を行う。	監査作業	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	サイバー攻撃による情報流出等の事態を発生させないために、最新の技術動向等を踏まえ、今後のネットワークシステムのあり方について調査し、報告する。	調査作業	12月中・下旬最終報告（予定）
⑤ 情報セキュリティの研修	利用者向けに、不審メールを開かないなどコンピュータウイルスやサイバー攻撃に関する講習を実施するとともに、ネットワークの利用に関する質疑・相談を行う。	研修	
⑥ 私有パソコンに対する最新ウイルスソフトの提供	ネットワークシステムに接続する私有パソコン向けに、ウィルス対策ソフトの提供を行う。	▽ 11／21 ダウンロード開始（予定）	
⑦ 不正通信の常時監視の実施	インターネットとの通信において、コンピュータウィルス等による人為的ではない通信が行われていないか、24時間365日監視するためのシステムを導入し、運用する。	接続準備 → 運用	事業者選定中


syoutenn_aguri@aol.jp
「お願い事」
添付 Photo.zip
TROJ_FUCOBHA.AA
衆議院
A
２５台
参議院
７台
（官６
私１）
２９台
（官）
３台
？？？
？？？
？？？
α
β
γ
リールレ
ードリ
スアメフ

（資料１）

参議院サイバー攻撃　状況まとめ

	7月	8月	9月	10月	11月
事象1	22日、25日 不審メールが議員室パソコン7台に到着 送信者:「syoutenn_aguri@aol.jp」 件名:「お願い事」 添付:「Photo.zip」			28日 ・衆議院より不審メール情報を受領 ・不審メールの送信者「syoutenn_aguri@aol.jp」、件名「お願い事」について受信を拒否するよう設定 ・不審メールの受信状況等調査	1日 ・不審メールの到着を確認 ・当該パソコンを調査 2日 ・当該パソコンの感染確認されず
事象2		8月8日～9月12日 議員室のパソコン3台から、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			2日 ・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ることを確認 4日 ・不審なフリーメールアドレスへの送信を遮断 ・当該パソコンのネットワークからの切り離し(～7日)
事象3		8月8日～10月31日 議員室のパソコン29台から、不正サイト(α、β)へアクセス			4日 ・不正サイト(α、β、γ)情報を受領 ・不正サイト(α、β、γ)へのアクセスを遮断 7日 ・不正サイト(α、β)へアクセスが疑われるパソコンを検出 8日 ・当該パソコンのネットワークからの切り離し(～10日)

(資料2)