報告書（抜粋）

第三　これまでに採ったセキュリティ関係の措置と今後の対策

これまで、セキュリティ対策については、ファイアウォールやIPS（侵入防御システム）、ウィルス対策ゲートウェイによる通信監視や、複数ベンダーのウィルス対策ソフトを用いた多重検知を行うなど、一般的に想定されるセキュリティ対策を行ってきたところであり、その内容については、セキュリティの専門会社からも一定の評価を得ている。

今回の事態を踏まえ、緊急に措置した対策と今後実施すべき対策を分類し、前項の反省点等に基づいて、セキュリティ対策樹立チームにおける外部有識者の意見を参考にしつつ、なおかつ利用者たる議員事務室の利便性を大きく損なわないよう配慮した上で、以下のとおり取りまとめたところである。

1　緊急に措置した対策

（1）日常監視強化

今回、サーバにおける異常を捕らえたことが事態の発覚につながったことからも明らかなように、サーバの状態を日々詳細に確認することは、異常の早期発見に極めて有用であることが再確認された。そのため、日常点検を含む管理体制において、アクセスを規制している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、監視を強化したところである。

（2）議員用端末の全台緊急点検

中間報告及び調査結果によって、今回のウィルスによる被害の全体像は明らかになったところである。しかしながら、今回の事案に直接関係しない各議員事務室からも現在使用中の端末に対して不安視する声があったことも事実である。これを踏まえ、事務局としては、議員用端末について、各議員事務室及び会派事務室を順次訪問し、不正ファイルの有無を確認するとともに、緊急セキュリティ点検（ウィルスチェック）を行った。その結果、今回問題視された不正なファイルは、他の端末からは発見されず、ウィルスチェックを行った議員用端末の安全性が確認されたところである。

（3）臨時セキュリティ研修

本年１１月２日現在、パスワードの変更状況の調査では、全て若しくは一部のパスワード変更を既に行っていると明確に回答された事務室は概ね４５％

にとどまっていたことからも明らかなように、利用者のセキュリティ意識は必ずしも高いとはいえない。全体としての意識の向上を図るためには、ウィルス感染の危険性やその対処方法等を直接利用者に伝達できるセキュリティ研修の必要性がセキュリティ対策チーム等において指摘されたことから、本年１１月２５日より、議員・秘書等を対象に、ウィルススキャンの手順、不審なメールへの対応、パスワードの定期的変更等を内容としたセキュリティ研修を実施しているところである。

2　短期的に実施すべき対策

（1）利用者への周知方法の確立

利用者に常時、不審メール等の注意喚起を行うには、容易に理解しうる方法で周知を図る必要があると考える。そのため、必要に応じてイントラ等に不審メール情報について告知し、情報共有のためのルール化を図ることとする。

また、非常時においては、院内ＬＡＮが停止する場合をも想定して、館内放送や全議員事務室への個別訪問による説明等、いわゆるアナログ的な手法を活用した連絡周知方法の確立を図ることとする。

（2）ヘルプデスクによる議員用端末の定期検診

今回、緊急の措置として全議員端末に対するセキュリティチェックを行ったところであるが、今後については、ヘルプデスク要員が日頃から定期的に議員事務室を訪問し、ウィルス対策ソフトの動作状況の確認や端末に対するウィルススキャン等を実施することで、潜在的な脅威を早期に発見することが可能となると考える。

現在のヘルプデスクの要員を増員し、巡回訪問、定期健診等の専任者を確保する等のセキュリティチェック体制の強化を図る。

（3）システムの健全性確認

本事案への対処としては、感染した端末（運用管理端末を含む）及びサーバについては切り離し、副次的感染を防止したところである。今後、安心して利用するために、システム全体の健全性について監査等を実施して安全性の裏付けを取ることとする。

（4）アカウント管理体制の強化

管理者権限のＩＤ及びパスワードについては、パスワードの有効期限や強度について一定のルールを定めるなど、厳重に管理することが必要である。また、

管理者権限が必要な作業を精査し、その使用を最小限にとどめるとともに、管理者権限以外でも可能な作業は、権限を細分化することにより、万一被害が生じた場合にもそれを限局することが可能となるよう、必要な権限のみを付与したアカウントを作成することで対応することとする。

（５）不正・不要な通信の排除

今回のような攻撃を未然に防ぐためには、必要のない通信を遮断することが有効であると考えられる。そのため、サーバに対する不要な通信を制限する仕組みを導入するとともに、リモートアクセス端末の不正な接続を遮断する仕組みを導入することで、現在の議員事務室に対するサービスレベルを維持しつつ、更なるセキュリティの強化が可能になると考えられる。

（６）議員用端末の更新及びセキュリティ強化

議員事務室に貸与している端末については、今年度中に更新する予定となっている。その際は、認証証明書についても既存のものを失効させ新たに発行し直すこととするほか、サーバの更新もあわせて行うため、一旦現在の全パスワードは無効化されることとなり、全端末について、より複雑な仮パスワードを発行する。また、利用者に負担をかけないセキュリティ向上策として、新端末については、自動でウィルススキャンを実施する設定とする。

（７）標的型不審メール訓練

不審メールを適切に処理するためには、研修等のみならず、実際に体験することで対応に慣れることも重要である。そのため、政府が行っている標的型不審メール訓練を参考に、本院において実施する場合に配慮すべき事情を勘案しつつ、同様の訓練の実施について早急に検討する。

３　中長期的に検討すべき対策

（１）緊急事態対応訓練

事案に応じた対応マニュアルの早急な策定について先述したが、当該マニュアルの策定をもって対策の完了とするのではなく、いわゆるＰＤＣＡ（Plan（計画）-Do（実施）-Check（評価）-Act（改善））の考え方に基づいて適宜これを見直し、フィードバックを行うことで、より実効性のあるものとして確立していくことが必要である。

このため、政府で実施している大規模サイバー攻撃事態発生時の初動対処に係る訓練のように、対応マニュアルに沿った形で、実環境下において、担当者と保守運用業者での作業手順、事務局内部での情報伝達、さらには議員等への

報告といった手順を確認する。

（２）定期的なセキュリティ研修

前述したとおり、議員及び秘書等を対象に、臨時のセキュリティ研修を実施しているところであるが、利用者のセキュリティ意識を高い状態に保つためには、当該研修を今回限りで終わらせることなく、継続させることが重要である。そこで、議員・秘書・会派に加えて職員も含めた形での利用者のセキュリティ研修を定期的に実施する。

（３）悪性サイトの通信制限及び監視強化

本院における解析結果のみならず、参議院や政府（ＮＩＳＣ）との情報共有によって明らかとなった不正と思われる通信先については、適宜ブロック等の対処をしているところである。今後は、更なる情報共有を進めるだけでなく、通信ブロックの自動化までをも含めた対策を検討する。

またウィルスの活動に特徴的な通信を自動的に検知する仕組みを導入することで、早期発見・対処が可能な環境の構築を検討する。

さらに、外部との通信は現在も２４時間の確認体制で対応しているところであるが、さらなる監視強化の方策として、２４時間の有人監視体制について、その効果等を検証の上、その導入を検討する。