第6回最高情報セキュリティアドバイザー等連絡会議における助言

2012 年（平成 24 年）1 月 26 日
最高情報セキュリティアドバイザー等連絡会議

1. 標的型不審メール攻撃訓練結果の概要（中間報告）に関する助言

内閣官房情報セキュリティセンター（NISC）が実施した「標的型不審メール攻撃訓練結果の概要（中間報告）」に基づき、訓練を継続的に実施する必要性や訓練の結果から浮かび上がった課題について、議論を行った。

1） 訓練によってセキュリティ意識は向上したものと思われるが、時間の経過とともに意識レベルは低下するものと考えられるため、今後も訓練を継続していくことが求められる。

2） 訓練を継続するにあたっては、組織としての成熟度向上を意識して行う必要がある。

3） メールの自動返信機能を設定することにより、攻撃者に対して不在通知が自動発信されるケースへの対策については、今後、禁止等も含めた検討が必要である。

2. 公開ウェブサーバの脆弱性検査に関する助言

内閣官房情報セキュリティセンター（NISC）が実施した 11 府省庁の公開ウェブサーバを対象とする脆弱性検査の結果について、議論を行った。

1） 同検査の結果、危険度高（CVSS 基本値 7.0～9.9）に相当する SQL インジェクション及び「Apache の Range ヘッダーにおけるサービス運用妨害（DoS）」の脆弱性が複数の省庁において確認された。各府省庁においては、NISC が発出した平成 24 年 1 月 19 日付けの注意喚起に基づき、管理している公開ウェブサーバについて確認し、脆弱性の存在しないことが確認できない場合には、関係者及び関係事業者と調整の上、適切に措置を講ずることが求められる。

2） 脆弱性の検査を行うツールについても、IPA などが既に開発・公表しており、各府省庁において適宜活用していく必要がある。

3） 公開ウェブサーバの調達にあたっては、検収時等に必ず脆弱性検査を行うとともに、検査の実施も含めた調達のための予算を確保していくことが求められる。特に、各府省庁の広報部門とも連携して、小規模の調達も含めて、検収時等に、外部へ公開するウェブサーバの脆弱性検査を行うことが求められる。

3. 送信ドメイン認証の取組に関する助言

政府機関の送信ドメイン認証の導入に係る取組について報告を受け、今後の取組について、議論を行った。

1） 政府機関における送信側（DNS サーバ）の SPF 設定率は、平成 24 年 1 月 23 日現在で 8 割を越えるものとなった。これは、政府ドメインの安全性・信頼性の向上に繋がるものであり、高く評価される。

2） 政府機関においては、政府ドメインの信頼性確保のため、引き続き送信側SPF対策への取組の徹底を図るとともに、なりすまし電子メール受信時の対策のため、受信側（メールサーバ等）の SPF 対策についても一層推進するべきである。

3） 今後とも、なりすまし電子メールによる情報セキュリティ上の脅威を軽減するために、DKIM や S/MIME のように暗号技術を利用した対策の導入を積極的に検討していくべきである。