NISC 内閣参事官

報道資料

平成 24 年 1 月 19 日
内閣官房情報セキュリティセンター（NISC）

政府機関における情報セキュリティ対策の取組状況について

－標的型不審メール攻撃訓練結果の概要等について－

本日、開催された「情報セキュリティ対策推進会議」（議長：竹歳誠内閣官房副長官(事務)）において、政府機関における情報セキュリティ対策の取組状況等について報告しました。

その概要は、以下のとおりです。

政府機関における主な取組

・内閣官房等12の政府機関約6万人を対象とした「標的型不審メール攻撃訓練」結果の中間報告 （別紙1）
・11省庁を対象とした「公開ウェブサーバの脆弱性検査」結果の中間報告 （別紙2）
・電子メールの送信元について、なりすましを防止するための対策の一環として「送信ドメイン認証技術の導入」に関する取組状況 （別紙3）

※ これらの資料については、内閣官房情報セキュリティセンターのホームページにおいても公表しております。

（http://www.nisc.go.jp/active/general/torikumi.html）

【本報道発表に関する問い合わせ先】
内閣官房情報セキュリティセンター
内閣参事官　木本　裕司
電話　03-3581-3959（直通）

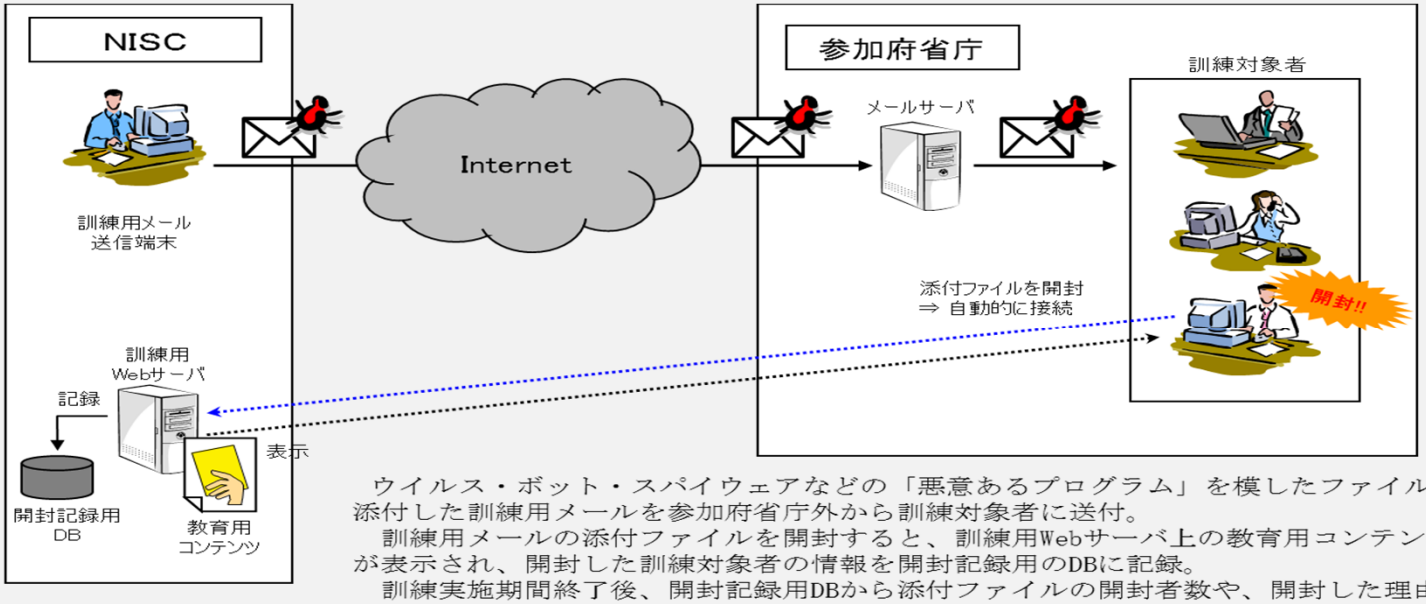
平成23年度　標的型不審メール攻撃訓練結果の概要（中間報告）

標的型不審メール攻撃訓練結果の概要（中間報告）

１．**訓練期間**：平成２３年１０月～１２月

２．**訓練対象**：内閣官房等１２の政府機関約６万名

３．**訓練内容**：①訓練対象者に対して事前教育の実施。
②訓練対象者に対して標的型不審メールを模擬したメールを２回送付。
③模擬メール中の添付ファイルを開封もしくは、ＵＲＬをクリックするなど不適切な扱いをした場合は、教育コンテンツに誘導。
④参加府省庁に個別の訓練結果を通知し、各府省庁内において適切な事後教育指導を実施。



ウイルス・ボット・スパイウェアなどの「悪意あるプログラム」を模したファイルを添付した訓練用メールを参加府省庁外から訓練対象者に送付。
訓練用メールの添付ファイルを開封すると、訓練用Webサーバ上の教育用コンテンツが表示され、開封した訓練対象者の情報を開封記録用のDBに記録。
訓練実施期間終了後、開封記録用DBから添付ファイルの開封者数や、開封した理由等の教育結果を集計。

平成23年度　標的型不審メール攻撃訓練結果の概要（中間報告）

４．**訓練結果**：今回の訓練における不審メールの開封率は以下のとおり。
（**中間報告**）
◆１回目（添付メール）　１０．１%（１．１%～２３．８%）
◆２回目（リンクメール）　３．１%（０．４%～　６．１%）

５．**結果分析**：①１回目の結果と比べ２回目の結果が良くなっていることから、標的型不審メールに対するセキュリティ意識は向上したものと想定される。
（**中間報告**）
②ただし、この効果は一時的なものであり、時間の経過とともに意識レベルは低下するものと想定されるため、今後も訓練を継続していくことが重要である。

６．**課　　題**：不審メールを開封した事例のほか、
（**中間報告**）
①不審メールの送信元に対し、メールを返信する方法で差出人の確認をしているケース
②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、不在通知が自動発信されたケース
がみられた。
これらの事例では、組織で使用している有効なアドレスを攻撃者に通知してしまうことになり、攻撃者に次の攻撃に資する組織内の情報を提供したことになる。
したがって、これらについても対策が必要となる。
対策としては、
①差出人の確認については、電話等により行うこと
②自動返信の範囲を組織内に限定すること
などが考えられる。

※　各府省庁からのリクエストにより、訓練方法をカスタマイズしているケースがある。

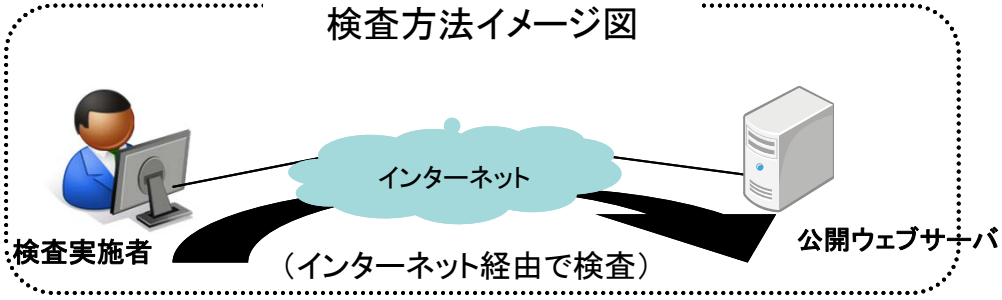
平成23年度　公開ウェブサーバの脆弱性検査結果の概要

別紙2

脆弱性検査状況報告（概要）

1. 検査期間：平成23年9月～12月
2. 検査対象：政府機関における公開ウェブサーバ（検査希望のあった11省庁、約330画面）
3. 検査方法：対象とする公開ウェブサーバにインターネット経由でアクセスし、ツール及び手動により検査を実施
4. 検査内容：プラットフォームに関する検査
   ウェブアプリケーションに関する検査
5. 検査結果：検出された脆弱性のうち緊急性の高いものについては、当該府省庁に対し速報を発出し、対策を実施済み又は実施中
   検査結果については、今後、全府省庁に対して情報共有を行い、政府機関全体の情報セキュリティ対策の向上に活用する予定

検査方法イメージ図

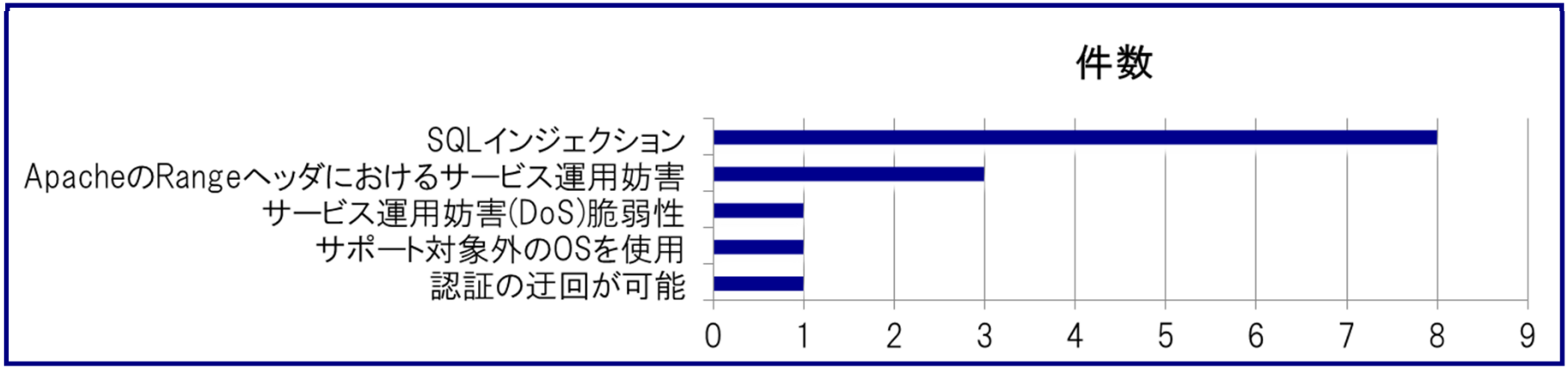


検査工程

	7月	8月	9月	10月	11月	12月	1月
希望調査	→						
検査実施			→	→	→	→	
結果報告					→	→	

「脆弱性検査」結果

危険度「高」の検出結果（延べ14件）



	脆弱性内容	原　因	想定される被害
1	SQLインジェクション	ウェブアプリケーションにおいて、入力値チェックやエスケープ処理が徹底されていない	データベースに格納されている情報の漏えい、改ざん、破壊等の可能性
2	ApacheのRangeヘッダにおけるサービス運用妨害	パッチ未適用	サービス運用妨害(DoS)により、サーバが停止する可能性
3	サービス運用妨害	ハードスペックやソフトウェア設定において、システム導入時に見積もった内容が実運用時のデータ送信量に対し過少である可能性	サービス運用妨害(DoS)により、サーバが停止する可能性
4	サポート対象外のOSを使用	ー	パッチ適用による対策が行えず、セキュリティ侵害が発生する可能性
5	認証の迂回が可能	ウェブアプリケーションにおいて、ログイン処理の成功、不成功にかかわらずアクセス可能なプログラムになっていた可能性	IDとパスワードを入力せずにログイン後のページにアクセスでき、情報漏えい等の可能性

送信ドメイン認証技術の導入に関する取組状況

別紙3

電子メールの送信元について、なりすましを防止するための対策の一環として
DNSサーバへのSPFレコードの記録を推進

これまでの主な取組

- 本省、外局、地方支分部局、独立行政法人等において、送信側SPFの導入を推進
- **本府省庁ドメイン**について、**送信側SPFの設定を完了**（H22年7月）

＊外局等を含むDNSサーバ（送信側）におけるSPF設定状況（率）

H23年7月末現在	→	H23年10月13日現在	→	H24年1月16日現在
37．4%		63．2%		85．1%

（第3レベルドメインについて当センターにて調査）

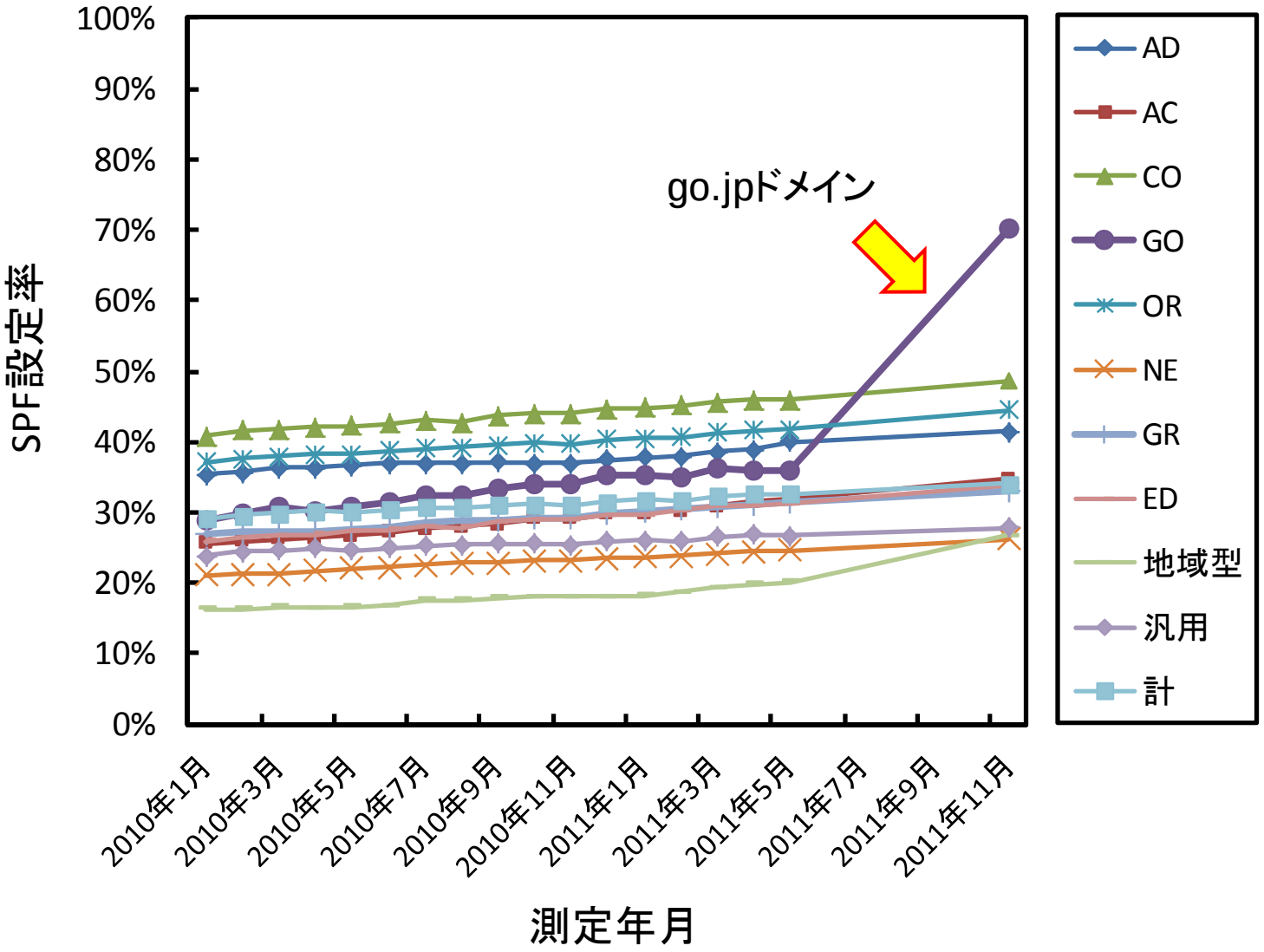
- 受信側においても、送信元を検証する機能を設定することを推進

具体的な取組内容

- DNSサーバにSPFレコードを記載
- 利用していないgo.jp ドメインについては、廃止
- メール送信を行わないgo.jpドメインについては、メール送信を行わない旨をSPFレコードに記述
- SPFレコードの末尾は“~all”ではなく“-all”を記載、サブドメインに対しても同様に対策

＊SPF（Sender Policy Framework）：メールの送信元アドレスの偽装を防止する技術

各ドメイン別における送信側SPF設定率の推移



※ WIDEプロジェクトにおいて調査・公開している送信ドメイン認証技術普及率推移のデータ
http://member.wide.ad.jp/wg/antispam/stats/index.html.ja より当センターでグラフを作成