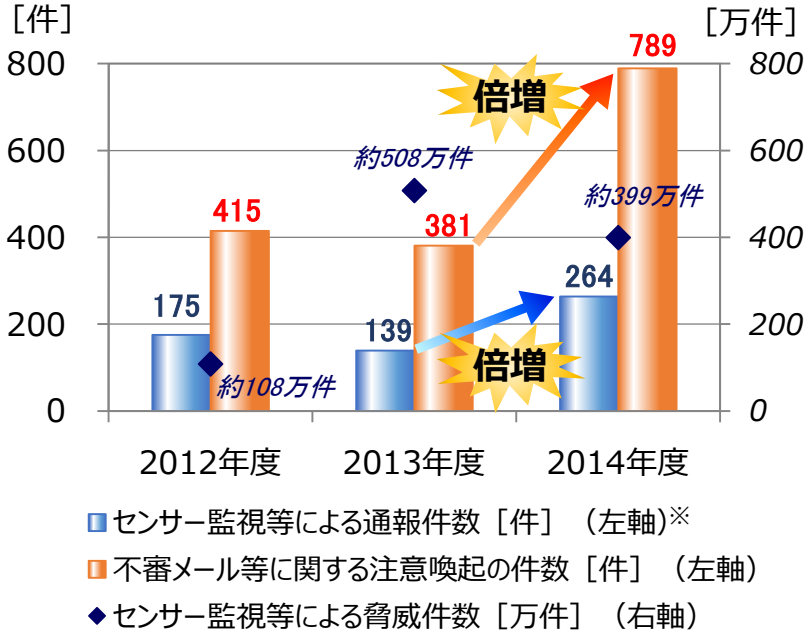
資料１－１

2014年度の政府機関における
サイバーセキュリティ対策に関する
取組と評価等について

政府機関等におけるサイバーセキュリティに関する情勢

- **標的型攻撃の脅威が深刻化**しており、最近では日本年金機構が個人情報の流出を発表（2015年６月）。
- 日本年金機構の原因究明調査結果を踏まえ、情報システムに対する横断監視の対象拡大等、**対策の強化を実施予定**。

【政府機関への脅威件数等】



※ GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）により各府省庁等に置かれたセンサーが検知等したイベントを通知した件数。

【外部からの攻撃に係る2014年度の特徴】

以前にも増して政府機関に大量の不審メール、不正プログラムが送付されており、標的型メールによる脅威が一層深刻化。

- センサー監視等による**通報件数は前年度から倍増**（264件）、そのうち**約４割は標的型メール**（標的型メールの通報件数は前年度比約３倍に増加）。
- 不審メール等の**注意喚起件数**は**前年度から倍増**（789件）。
- センサー監視等による**脅威件数は約399万件**。
  （約８秒毎に１回脅威を認知。前年度より減少したのは、GSOCシステムの能力向上によって、軽微なものの判別対象からの除外を含め、脅威の識別精度が向上したことによるもの。脅威そのものは一層深刻化。）
- 文書作成ソフト等の**未知の脆弱性を利用した攻撃**や、不正通信の接続先にクラウド上のサーバが利用される等、**認知・防御が困難に**。

【2014年度の主なサイバー攻撃事案】

2014.9	［法務省］ サーバに対する外部からの不正アクセスが発覚。
2014.10	［国土地理院］ パソコンがウイルスに感染、情報流出の可能性を発表。
2015.2	［日本貿易振興機構］ 標的型メールによるパソコンのウイルス感染が発覚。
（参考）	
2015.6	［日本年金機構］ パソコンがウイルスに感染、約125万件の情報流出を公表。

政府機関全体の取組と評価①

外部からの攻撃等の情報セキュリティインシデントへの対処等に係る取組

- 各府省庁において、高度化する**標的型攻撃に対応するため**、その標的とされる蓋然性が高い業務・情報に係る**リスク評価に基づく対策の重点化による多重防御の実現に向けた取組を本格実施**。
- NISCにおいて、マニュアルを整備し、**サプライチェーン・リスクに対応するための調達要件を強化**。
- NISCにおいて、府省庁CSIRTやCYMAT※の要員を対象とした研修・訓練に加え、3月18日（サイバーの日）には総務省と共催で競技形式の「**サイバー攻撃対処訓練（NATIONAL３１８（CYBER）EKIDEN）**」を実施し、**サイバー攻撃対処態勢を強化**。
- 各府省庁において、**独立行政法人について、政府統一基準群等を踏まえた対策を講じることによりセキュリティの強化を進める**旨の会議決定（2014年6月）を踏まえて対策を推進。

※ CYber incident Mobile Assistance Team （府省庁横断的な情報セキュリティ緊急支援チーム）

ITの利用動向の変化に伴う新たな課題等への対応に係る取組

- 各府省庁において、政府統一基準群（2014年5月改定）を踏まえ、**セキュリティポリシーの改定を進め、スマートフォンの利用に関する対策やソーシャルメディアサービスの利用に関する対策等を強化**。
- NISCにおいて、政府機関においても利用の拡大が見込まれる**クラウドサービスに関して、調達や運用の観点からセキュリティ対策を検討**。

サイバーセキュリティ基本法の施行等に伴う取組

- **戦略本部による各府省庁等に対する監査について、基本方針を策定**（2015年5月）。マネジメント監査及びペネトレーションテスト（システムへの侵入検査）の実施を決定。
- 監査の前提となる実地調査等を開始。監査制度の早急な立ち上げを図っていく。

政府機関全体の取組と評価②

各府省庁における自己点検等による評価

- 各府省庁が実施する自己による点検の結果からは、一般職員を含む各役割者のポリシー実施率は高水準を維持。
- 一方で、対策が十分には実施されていないとみられる点もあることに加え、点検が形式化し継続的改善の停滞が生じている可能性等も考えられることから、**今後はサイバーセキュリティ戦略本部による第三者的な視点からの監査等を実施し、セキュリティ対策の一層の推進を図っていく**。

○ 行政事務従事者のポリシー実施率※1調査

2012年度	2013年度	2014年度
96.8%	96.8%	97.1%

※1　把握した者のうち、責務が生じた者に占める対策を実施した者の割合

○ 責任者等※2のポリシー実施率調査

2012年度	2013年度	2014年度
99.6%	99.3%	99.7%

※2　最高情報セキュリティ責任者・統括情報セキュリティ責任者・情報セキュリティ責任者・課室情報セキュリティ責任者

重点検査による評価

- 情報システムを対象とした重点検査においては、**インターネットからアクセスされる情報システム（公開ウェブサーバ等）を対象として実施し、検査時点において把握された問題についても対処を完了**。
- SQLインジェクション脆弱性等は情報漏えいや改ざんにつながりかねないため、引き続き対策強化を推進する。

○ ソフトウェアの更新等の確認状況

対象	確認を実施した率
インターネットからアクセスされる情報システム	99%※3

※3　10/1(検査基準日)時点の数値であり、残る１%についてもその後改善を図った

○ SQLインジェクション脆弱性の確認状況

対象	確認を実施した率
公開ウェブサーバ※4	94%※5

※4　インターネット上で公開しているウェブサーバを持つ情報システムのうち、SQLインジェクション脆弱性が技術的に存在し得るもの
※5　10/1(検査基準日)時点の数値であり、残る６%についてもその後改善を図った