事　務　連　絡
平成28年２月２日

各府省庁情報セキュリティ担当課室長 殿

内閣官房 内閣サイバーセキュリティセンター
内閣参事官（政府機関総合対策担当）
内閣参事官（情報統括担当）
内閣参事官（事案対処分析担当）

分散型サービス不能攻撃への対処について（注意再喚起）

平成 27 年 11 月 25 日付文書でも注意喚起をしましたが、政府機関や重要インフラ関係事業者（以下「政府機関等」という。）を標的とした分散型サービス不能（ＤＤｏＳ）攻撃とみられる攻撃により、ホームページの閲覧が不能となる事案が多発しています。ＮＩＳＣで把握している限りにおいても、回線容量を超過させる手法や、異常な通信によりサーバの処理容量を超過させる手法など、様々な手法が用いられていることが判明しています。また分散型サービス不能攻撃は昨今では、インターネット上に存在する地下組織が安価に提供しており、大規模な攻撃を試みることがより容易となっている背景事情も影響しているものと考えられます。

各府省庁におかれましては、「政府機関の情報セキュリティ対策のための統一基準」（平成 26 年 5 月 19 日情報セキュリティ政策会議決定）に基づき、分散型を含むサービス不能攻撃への対策を講じていることと存じます。他方で、本年は伊勢志摩サミット及び関連大臣会合の開催を控え、我が国への国際的な関心が高まることから、この種の攻撃がさらに活発化することも予想されます。

こうした最近の分散型サービス不能攻撃を回避する対策は、以下を例とするいくつかの手法が回線事業者やウェブホスティング事業者等により提供されており、比較的短期間で導入が可能とのことです。

- 攻撃元となっているＩＰアドレスからの通信を遮断する
- 攻撃と判断される異常なパケットの通信を破棄する
- ウェブサーバを仮想的に多数配置し、攻撃による大量の通信を分散させて処理する

各府省庁におかれましては、以上の状況も踏まえつつ、引き続き攻撃動向に注意するとともに、開設しているウェブサイトの重要度等にも鑑み、分散型サービス不能攻撃対策の強化について速やかに御検討をお願いします。

また、攻撃を受けた府省庁にあっては、『我が国におけるサイバー攻撃に係る情報収集・集約体制等の整備について』（平成 22 年 12 月 27 日情報セキュリティ対策推進会議申合せ）３（１）に基づき、関係機器のログ等の情報をＮＩＳＣに提供いただきますようお願いします。具体的には、攻撃と思われる通信を認知した際は、初動にて実施した対策等を記入し、インシデント連絡様式を初報として速やかにご提出ください。加えて、府省庁にて把握されているログ情報、フロー情報、トラフィック情報等についても併せてご提出をお願いします。