資料１

攻撃の予兆や被害に関する情報収集・分析に係る基本方針について（案）

平成16年７月26日
情報セキュリティ対策推進会議幹事会

１　情報収集・分析の必要性

コンピュータウイルスやいわゆるサイバー攻撃などにより情報通信ネットワークを通じて情報システムを攻撃し、あるいはこれに侵入する事案や標準化が進む情報通信技術の欠陥を悪用して情報システムの安全性を脅かす事案は、一度これが発生するとその被害が拡散し、あるいは同種の事案が多発するという特徴を有している。このような事案に政府として緊急かつ的確に対処し、被害の拡大を防止するためには、ソフトウェアの脆弱性やコンピュータウイルスの特性に関する情報及びこれらを踏まえた対応要領に関する情報、さらにはいわゆるハッカー組織の動向等に関する情報等を幅広く収集し、これを集約、分析して、被害を受けた府省庁に適切な対処策を提示するとともに、被害を受けていない府省庁に対しても予防策等を速やかに示すことが不可欠である。

また、情報システムに対する脅威は、こうした外部からの攻撃や不正な侵入に限られるわけではなく、府省庁の内部から行政上重要な情報が漏えいし、改ざんされ、又は破壊される可能性（最近民間企業等において個人情報が漏えいする事案が多発していることは、情報セキュリティを確保する上で、職員の管理が極めて重要であることを如実に示している。）や、情報システムの設計や設定の誤り等の運用上の過失によって情報システムに障害が発生し、又は情報システムが損壊するという可能性についても軽視すべきではない。このように、情報セキュリティが侵害され、又は損なわれる事案（以下「情報セキュリティ関係事案」という。）は多種多様であることから、これらの事案による被害の発生や拡大を防止するためには、平素から、実際に被害が発生した事案について、その原因、手口等に関する情報を収集し、これを分析して対処策を検討しておくことが必要である。

２　現状における問題点

(1)　内閣官房の体制に係る問題点

政府においては、情報セキュリティ関係事案が発生し、又は発生するおそれがある場合に、各府省庁が連携して緊急にこれに対処するため、「政府機関の情報システムに係る緊急時の連絡等について」（平成12年４月17日各府省庁申合せ、平成14年４月１日一部改定）において、情報セキュリティ関係事案による被害を認知した府省庁は内閣官房情報セキュリティ対策推進室（以下「内閣官房」という。）に通報すること、及び内閣官房は各府省庁に対し、各府省庁が執るべき対処策に関する情報を提供すること等を内容とする連絡連携体制を定めたところである。このように、内閣官房は、政府機関における情報セキュリティ関係事案に係る情報を収集・分析すべき役割を担っているところであるが、その体制は十分ではなく、いわゆるシステムベンダー、情報セキュリティベンダー、民間の情報セキュリティ関係事案対応機関等、幅広い情報源から継続的に情報の収集を行い、これらの情報を分析することは困難な状況にある。

なお、平成14年には、内閣官房内に緊急対応支援チームを設置し、情報収集・分析能力の向上を図ったところであるが、同チームは、ほとんど常駐していないことから、集中的かつ恒常的に情報の集約及び分析を実施することは難しい状況にある。また、同チームの人員構成は、インターネット関連技術の専門家が中心であるため、コンピュータウイルスやソフトウェアの脆弱性に関する情報の収集には多大な成果を収めたものの、ますます増加し、多様化しつつある情報セキュリティ関係事案の全てに対処することは必ずしも容易でない現状にある。

(2) 各府省庁から内閣官房への連絡事項等に係る問題点

前述した「政府機関の情報システムに係る緊急時の連絡等について」においては、各府省庁は、その情報システムに被害が発生した場合には、内閣官房へ速やかに連絡することとされているが、同文書においては、

ア 各府省庁は、被害に係る第一報のみを内閣官房に報告すれば足りることとされており、その原因、今後執ろうとする対策の内容等について続報することとは明示されていない。このため、被害の原因の分析等に必要となる情報が内閣官房に集約されない状況となっている。

イ 通報の対象となる被害として、「不正アクセス」、「サービス不能攻撃」、「情報の窃盗、漏えい」等が掲げられている一方、情報システムの設計や設定の誤り、ハードウェアの故障等による障害による情報システムのサービス停止については、内閣官房への通報を求めていない。しかしながら、これらの原因による情報システムのサービス停止についても、情報セキュリティの確保という観点においては、その結果の重大性は同じであるため、必要な情報の収集・分析を行い、政府としての対処策を検討する必要がある。

ウ イで述べたように各府省庁から内閣官房への通報の対象となる被害が限定されているため、原因が不明である情報セキュリティ関係事案については、その原因が判明するまでの間、内閣官房への通報を求めていない。しかし、原因が判明した段階で初めて内閣官房に情報が集約されたとしても、それ以前に他の府省庁で同様の被害が既に発生している可能性があるため、被害の発生を未然に防止することはできない。

という問題が顕在化している。

(3) 関係機関との連携に係る問題点

各府省庁の情報システムへの攻撃の予兆等に関する情報については、内閣官房や各府省庁だけでなく、民間の情報セキュリティ関係事案対応機関においても往々にして関係する情報を有していることがあり、内閣官房として当該情報を早期に把握することができれば、各府省庁に対して必要な対処に関する情報を速やかに提供することが可能となるはずである。しかしながら、現状では、内閣官房とこれらの民間機関との間での連絡連携体制が十分に整備されていないため、各機関が有する情報が有効に活用されていない状況にある。

3 基本方針

２を踏まえ、政府における攻撃の予兆及び被害に関する情報収集・分析を次の方策に

より一層充実することとする。

(1)　内閣官房の体制強化

緊急対応支援チーム員については、多種多様な情報セキュリティ事案に対応することができ、分析能力を有する者を確保するとともに、可能な限り、その常駐化を図り、情報の収集・集約・分析を集中的かつ効率的に実施し、また、速やかに各府省庁に対して執るべき対処策等に関する情報を提供できる体制を整備する。

(2)　各府省庁から内閣官房への通報事項等の見直し

「政府機関の情報システムに係る緊急時の連絡等について」について、

ア　通報の対象とすべき情報セキュリティ関係事案の範囲の拡大

イ　被害が発生し、又はその発生のおそれがあった場合における通報すべき事項の見直し並びに速報及び続報の徹底

ウ　情報セキュリティ関係事案への対処状況のフォローアップ

等を内容とする見直しを行う。

(3)　関係機関との連携体制の整備

内閣官房が中心となって、関係府省庁の協力を得て、情報セキュリティ関係事案対応機関等と連携するための体制を整備し、情報セキュリティ関係事案に係る情報の早期共有を行える環境を整備する。