平成28年度

北海道開発局における情報セキュリティ対策について
―インシデントの現況と今後の取り組み―

開発監理部　情報管理室　　○佐々木　聖記
松尾　圭司
小林　祐一.

近年、政府機関や企業等を対象としたサイバー攻撃の脅威は増大し、その手法は一層複雑化・巧妙化している。北海道開発局では、「北海道開発局情報セキュリティポリシー実施手順書」を定め、情報セキュリティの確保に取り組んでいるところであるが、依然として外部電磁的記録媒体の使用等に起因するセキュリティインシデントが多く発生している。本稿は、当局におけるインシデント発生状況等を踏まえ、情報セキュリティ対策の課題と今後の取組について報告するものである。

キーワード：情報セキュリティ、セキュリティインシデント、サイバーセキュリティ

1. 情報通信技術とサイバー攻撃の変遷

我が国においては、1990年代以降、パソコンの普及とITインフラの整備・発展により、誰もがインターネットを利用できるようになり、メールの送受信、天気予報・地図・交通情報・動画共有サイトの利用、商品・サービスの購入・取引、オンラインバンキング等、あらゆる分野に普及している。

いまやインターネットとそれを介したサービスは、我々の日常生活や社会経済活動等に重要で必要不可欠な社会基盤となっているが、その反面、ネットワークやシステムを悪用した不正侵入、情報の窃取、改ざん、破壊等のサイバー攻撃の脅威にさらされている。

独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ10大脅威」によると、サイバー攻撃の目的・手法の変遷（図-1）について、インターネットが定着し始めた頃は、強力な感染力を有するウィルスでパソコンやサーバを攻撃する手法が一般的で、その攻撃意図は、いたずらや愉快犯的な意味合いが強かったが、時間の経過とともに、組織化され金銭的又は経済的な攻撃意図を持って「人を騙す」攻撃に推移している。

攻撃意図・目的も政府機関や特定の組織の情報を盗み出す諜報活動や国家の重要インフラの混乱・破壊活動を意図したもの、主義主張又は政治・文化的に対立する国家、組織への抗議・報復といったものが出始め、最近では、国家の関与が疑われるような組織的かつ極めて高度なサイバー攻撃も散見され、悪意ある者による攻撃は一層複雑化・巧妙化し、攻撃対象も政府、民間、個人を問わず拡大し続けているという状況にある。

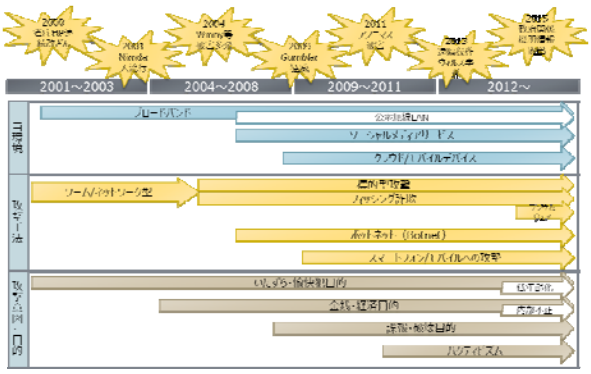

図-1　サイバー攻撃の目的・手法の変遷[1)]

2. 情報セキュリティインシデントの情勢

(1) 情報セキュリティインシデントとは

複雑化・巧妙化するサイバー攻撃等により、最近では、組織的な標的型攻撃や内部不正による情報の持ち出しによって大量の個人情報が流出したり、不正送金を狙ったウィルス感染や政府機関等へのDDoS攻撃によるWebサイトの閲覧障害等が相次ぐなど深刻な被害が絶えず発生している。

このような情報セキュリティを脅かす事件、事故及びセキュリティ上好ましくない事象・事態のことを「情報セキュリティインシデント」（以下「インシデント」という。）といい、ウィルス感染、不正アクセス、アカウント乗っ取り（なりすまし）、情報流出、情報機器や記憶媒体の紛失・盗難等がこれに含まれる。

Satofusa Sasaki, Keiji Matsuo, Yuichi Kobayashi

(2) 政府機関等におけるインシデントの発生状況

「内閣サイバーセキュリティセンター（以下「NISC」という。）」は、政府機関に対するサイバー攻撃の横断的な情報収集・監視活動と政府機関が受信する不審なメール等の情報集約・分析・注意喚起を所掌とし、平成27年5月に政府関係機関で発生した情報流出事案に際し、当該関係機関の情報端末の異常にいち早く気付き、それを通報した組織である。

NISCが発行した「サイバーセキュリティ政策に係る年次報告（2015年度）」によると、平成27年度に政府機関において発生したインシデントの主な要因は、「外部からの攻撃」と「意図せぬ情報流出」に大別され、その傾向として、上半期は、前年度に引き続いて外部からの攻撃、特に標的型攻撃が多く発生し、下半期は、政府機関のWebサイトを閲覧困難にするような攻撃が頻発したこと、また、前年度と同様に職員の過失等による意図せぬ情報流出が散見されたとされている。

「外部からの攻撃」について、平成27年度に政府機関に対するサイバー攻撃の脅威と認知された件数（図-2）は、613万件で、前年度の399万件と比較して約1.5倍に増加している。また、NISCが行った政府機関への通報・注意喚起（図-3）について、不審な通信やWebサイトの障害等（疑いを含む）の検知・通報は、平成27年度が163件で、前年度の264件と比較すると約2/3に減少しているが、政府機関が受信した不審なメール等に関する注意喚起は、平成25年度の381件に対して平成26年度は789件と約2倍に増加し、平成27年度は更に大幅に増加して2,000件に迫る注意喚起を行っている。

これらのことから、平成27年5月に政府関係機関で発生した情報流出事案を契機に各府省庁がセキュリティ対策に取り組んだ結果、一定の効果が得られたと考えられるものの、政府機関に対する攻撃等が減少した訳ではなく、その脅威は増していることがうかがえる。

「意図せぬ情報流出」については、従来から見られる記憶媒体の紛失事案等が発生しているとされている。

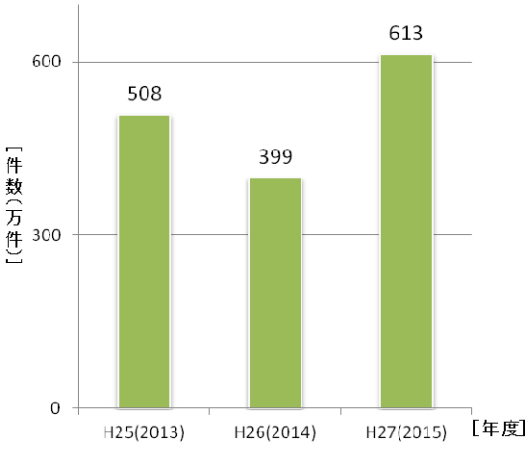

図-2　政府機関に対する脅威件数の推移[2)]

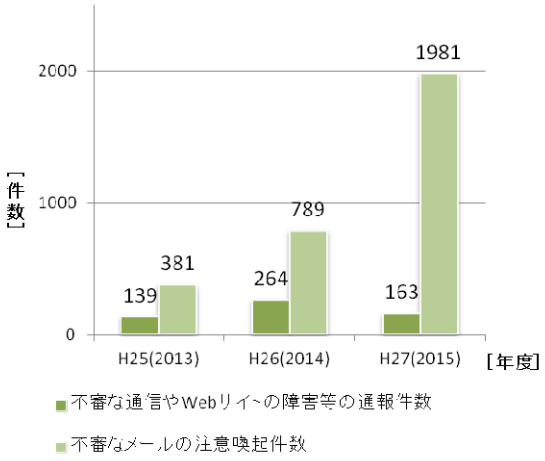

図-3　政府機関への通報・注意喚起件数の推移[2)]

国内においてパソコン、USBメモリ、外付けハードディスクドライブ等の紛失・盗難によって情報が流出した若しくはそのおそれがあるとして新聞、ホームページ等で発表された事案について、情報管理室が独自に調査した結果、平成25年4月から平成28年12月末までの間に292件あり、これを媒体別に集計すると図-4に示すとおり、USBメモリと外付けハードディスクドライブだけで全体の約6割を占めていることが分かった。

特に、平成16年前後から急激にシェアを伸ばしているUSBメモリは、記憶容量が大容量で利便性が高く、コンパクトで可搬性に優れているが、その反面、本人の不注意等による紛失・盗難によって情報流出の危険性が高いという点に注意が必要である。

また、上記独自調査においては、意図せぬ情報流出事案として、書類の誤廃棄やメールの誤送信といった事案も多数確認された。

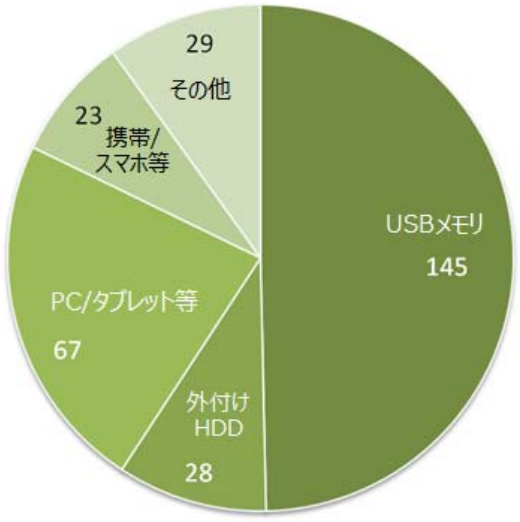

図-4　パソコン、USBメモリ等の紛失・盗難に係る発表件数（媒体別）

3. 政府機関における情報セキュリティ対策

(1) 政府機関の情報セキュリティ対策のための統一基準群とは

平成17年12月に決定された「政府機関の情報セキュリティ対策のための統一基準」は、各府省庁のセキュリティ対策の統一化とセキュリティ水準の底上げを目的とし、平成23年4月に「政府機関の情報セキュリティ対策のための統一基準群」（以下、「統一基準群」という。）として見直された。

統一基準群は、統一規範、運用指針、統一基準及びガイドラインで構成された政府機関の統一的な枠組みであり、各府省庁は、これに準拠した情報セキュリティポリシーを策定し、情報セキュリティ対策を実施するとされている。(図-5)

(2) 統一基準群の改正

統一基準群は、情報通信技術や環境の変化を踏まえて随時見直し・改正が行われてきたが、これまでの度重なる改正によって基準自体が複雑・肥大化したことから、統一基準群の実効性向上を目的として、定義や用語の明瞭・簡潔化、冗長表現の排除、形骸化した規定の見直し等を行い、また、政府機関に対するサイバー攻撃や脅威

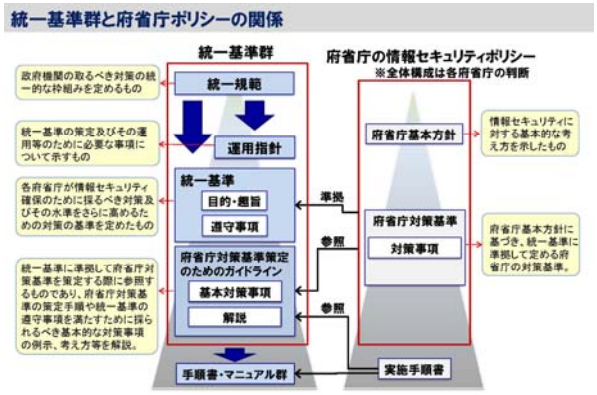

図-5 統一基準群と府省庁ポリシーの関係[3)]

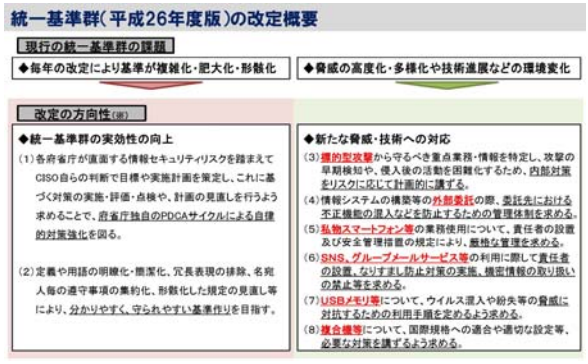

図-6 政府統一基準群の改正概要[3)]

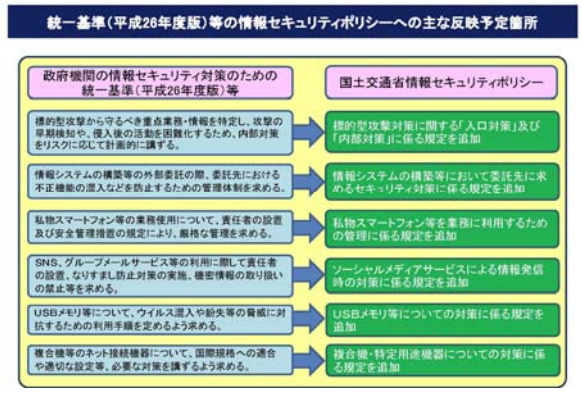

図-7 統一基準群の改正を踏まえた新たな対策事項[4)]

が多様化・巧妙化していることを踏まえ、新たな脅威に対応するため、標的型攻撃の早期検知や侵入後の活動を困難にする内部対策を計画的に講ずることやUSBメモリ等の利用手順を定めることなどが新たに盛り込まれ、平成26年5月に改正された。(図-6)

(3) 国土交通省情報セキュリティポリシーの改正

「国土交通省情報セキュリティポリシー」（以下「ポリシー」という。）は、統一基準群に準拠した国土交通省における対策基準に位置付けられ、国土交通省における情報及び情報システムをあらゆる脅威から守る情報セキュリティ対策の包括的な規程として、平成18年4月に初版が策定された。

ポリシーは、統一基準群の改正を踏まえ、例年、部分改正が行われてきたが、平成26年5月の統一基準群の改正を契機に大幅な見直しが行われ、平成27年4月に全部改正された。

今回の改正においては、これまで3分冊だったポリシーを1文書に統合し、統一基準群の構成変更に合わせてポリシー全体の構成を見直すとともに、職員が遵守すべき事項について、冗長表現の排除、過度に煩雑で形骸化した規定の見直し、具体的な対策の例示を行い、利用者の観点でより理解しやすいよう改善が図られた。

また、統一基準群の改正において、新たな脅威に対応するため盛り込まれた遵守事項については、ポリシーにおける新たな対策事項として反映されている。(図-7)

4. 北海道開発局における状況と取組

(1) 北海道開発局におけるインシデントの発生状況

当局において、不正アクセスやアカウント乗っ取り（なりすまし）といった重大なインシデントは発生していないものの、毎年、ウィルスが検知されている状況にある。

平成25年度から平成28年12月末までに当局においてウ

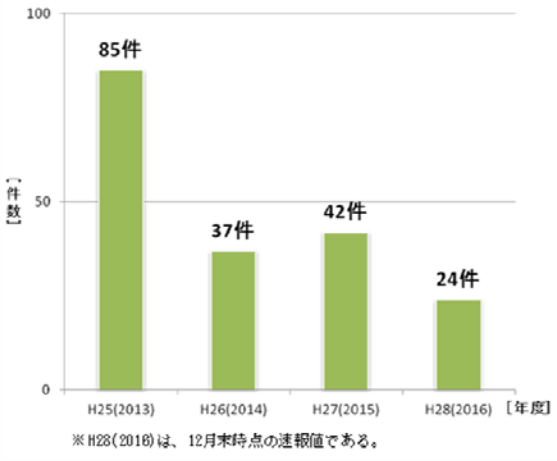

図-8 北海道開発局におけるウィルス検知件数（年度別）

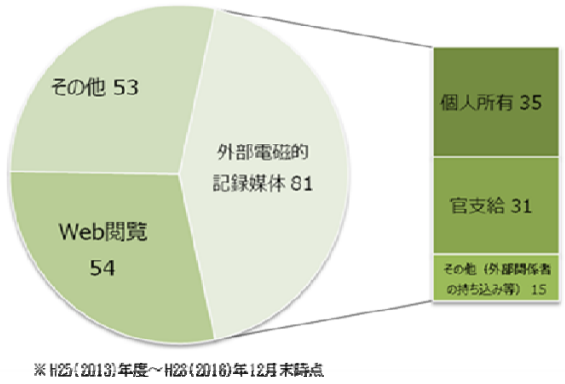

図-9 北海道開発局におけるウィルス検知件数（要因別）

ィルスを検知した件数は、年々減少傾向で推移している。(図-8)

当局におけるウィルス検知の主な要因は、「外部電磁的記録媒体」、「Web閲覧」及び「その他」に大別することができ、要因別の件数は、外部電磁的記録媒体を要因とした検知が81件と最も多い。(図-9)

「Web閲覧」によるウィルス検知については、従来からセキュリティ対策の一環として、職員が閲覧できるWebサイトを制限しており、不審なWebサイトの閲覧はシステム的に防御しているが、近年において、業務上必要なWebサイトを閲覧中に不審なWebサイトに誘導され、ウィルスが検知されたなど、業務上のWeb閲覧でウィルス検知に繋がる事例が発生している。

このことから、業務上必要なWebサイトの閲覧であっても当該サイト内に表示されたリンク等を安易にクリックしないといった職員への教育と周知が重要と考察する。

「その他」のウィルス検知については、不審なファイルが添付されたメールの削除が不完全だったためウィルス検知につながったといった不審なメール受信時における取扱いが不適切だった事案等も含まれる。

これらについては、従来からウィルス検知・駆除ソフトによる対策等が施されているが、新種のウィルスは、当該検知・駆除ソフトをすり抜ける場合があり、また、メール本文に記載されたURLリンクをクリックすることにより不正なサイトへ誘導されるといったことも想定される。

このことから、不審なメールを受信した場合には、安易に当該メールに添付されているファイルを開封しない、本文中のURLリンクはクリックしないといった職員への教育と周知が重要と考察する。

「外部電磁的記録媒体」によるウィルス検知について、要因となった媒体の種類は、USBメモリ、外付けハードディスクドライブ、SDカード等があり、それらを細別すると「個人所有」、「官支給」及び「その他（外部関係者の持ち込み等）」に区分され、特に「個人所有」の媒体から検知されるケースが多くなっている。(図-9)

当局においては、従来から、①個人所有及び出所不明の外部電磁的記録媒体は、本人が知らぬ間にウィルスに感染している可能性があり、これを当局保有のパソコンに接続した場合、ウィルスに感染する等のセキュリティリスクがあるため、これらを使用した業務遂行を禁止していること、②外部電磁的記録媒体を使用する場合は、LANケーブルを抜いた状態で事前にウィルス検疫・駆除を行ってからパソコンに接続すること、③外部関係者等が持ち込む外部電磁的記録媒体については、課所等の長の了解を得た上で、上記と同様、事前にウィルス検疫・駆除を行ってからパソコンに接続することについて、職員に対するセキュリティ教育と注意喚起を行ってきている。

しかし、職員の理解・認知不足等に加えて、パソコンに接続される外部電磁的記録媒体を制御するシステムが構築出来ていないことから、外部電磁的記録媒体を要因とするウィルス検知件数が最も多くなっていると考察する。

(2) 北海道開発局における取組状況

a) 北海道開発局情報セキュリティポリシー実施手順書の改正

「北海道開発局情報セキュリティポリシー実施手順書」（以下「実施手順書」という。）は、ポリシーを遵守する具体的な実施手順として、平成19年11月に初版が策定されており、北海道開発局長を情報セキュリティ責任者とした組織体制と当局職員が遵守する対策事項を定めている。

実施手順書の策定後、ポリシーの改正を反映させるため、随時改正を行ってきたが、平成27年4月のポリシー全部改正を踏まえ、平成28年1月に大幅な見直し・改正を行い、同年4月から施行している。

今回の改正は、①これまで役職別に3分冊されていた実施手順書を1文書に統合した上で全体的に構成見直しを行う、②情報の取扱いに関して、当局が独自に解釈・

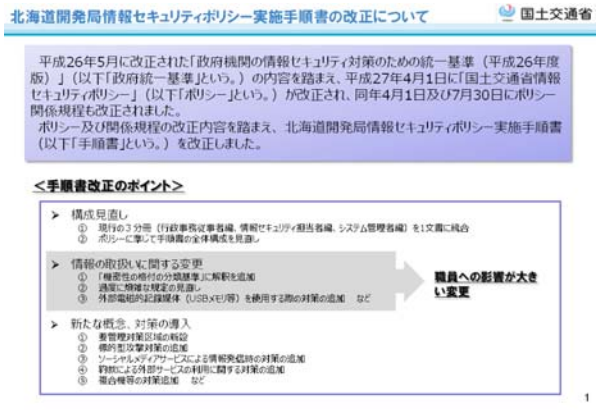

図-10　平成28年1月の実施手順書改正内容

運用していた機密性の格付区分の見直しと手続関係を改正する、③外部電磁的記録媒体の利用手順を新たな遵守事項として実施手順書に規定する、④ポリシーに新たな対策事項として規定されたものを新たな概念・対策として実施手順書に反映させるという内容である。(図-10)

このうち、外部電磁的記録媒体の利用手順については、当面、USBメモリと外付けハードディスクドライブ（以下「USBメモリ等」という。）に限定し、①職員は、USBメモリ等を新規購入した場合は課所等の長へ申し出ること、②課所等の長は、「官給品であること」、「情報漏えい対策機能付きであること」を確認の上、使用を承認すること、③課所等の長は使用を承認したUSBメモリ等の管理台帳を作成すること、④職員は、USBメモリ等を使用する場合は使用承認を受け、管理台帳に登載されているものを使用することと規定した。

今回の改正における情報の取扱いに関する変更とUSBメモリ等の新たな利用手順は、職員への影響が大きく、職員に対する事前の周知や教育等の期間を確保する必要があることから、実施手順書の施行を平成28年4月とし、それまでの間に本局及び各開発建設部において実施手順書改正に係る説明会、開発局イントラネットやコンプライアンス通信を利用した職員周知を実施し、実施手順書施行後には、今回の改正内容に特化したe-ラーニングを実施する等、職員周知・教育の徹底を図った。

b) 標的型攻撃対策

当局においては、従来からパソコンのウィルス感染や外部からのサイバー攻撃に対抗するための対策として、ファイアーウォール、有害サイトのフィルタリングソフト、ウィルス検知・駆除ソフト等によって対応していたが、平成26年5月の統一基準群の改正において、「標的型攻撃に対応するための内部対策をリスクに応じて計画的に講ずる。」と盛り込まれたことを踏まえ、新たな内部監視装置導入の計画・準備を進めていた。

平成27年5月に政府関係機関に対する標的型攻撃によって当該機関から大量の個人情報が流出する事案が発生したことを受けて、国土交通省の最高情報セキュリティ責任者である総合政策局長から、情報の適切な管理徹底と情報システムに対する点検指示があり、当該点検の結果、当局における問題はなかったものの、年々その手法や手口が巧妙化する標的型攻撃に対抗する内部対策を早急に講ずる必要があるとの判断の下、平成28年1月に内部監視装置の導入・稼働に至った。

平成28年7月には、上記内部監視装置によって、当局職員のパソコンが何度も外部への不正な通信を試みていることが確認され、解析・調査の結果、業務遂行上のWeb閲覧によってウィルス検知・対策ソフトでは検知できない新種のウィルスに感染していたことが判明したが、当局が別途実施しているセキュリティ対策によって外部への不正通信は成功しなかったという事案が発生した。

上記事案は、これまでのセキュリティ対策と新たに導入した内部監視装置によって、当局からの情報流失という最悪の事態を回避することが出来たという多重防御の効果が現れた事案である。

c) USBメモリ等に関する対策

a)で記述したとおり、当局においては、新たにUSBメモリ等の利用手順を規定したが、依然として個人所有のUSBメモリ等からウィルスが検知されるケースが発生している状況にある。

平成26年5月の統一基準群改正において、USBメモリ等外部電磁的記録媒体の管理に際しては、これらの接続を制御及び管理するための製品やサービスの導入も有効とされおり、各地方整備局においても、これを導入済み又は導入予定としている実態を踏まえ、当局においても、USBメモリ等を効率的かつ適正に制御・管理するため、デバイス管理システムの導入に向けた計画・準備を進めている。

デバイス管理システムについては、各地方整備局における導入・運用状況を参考に、当局におけるUSBメモリ等の運用実態、管理状況、業務処理状況などを考慮しながら、当該管理システムに求める最低限の要件を洗い出す等検討を進めているところである。(図-11)

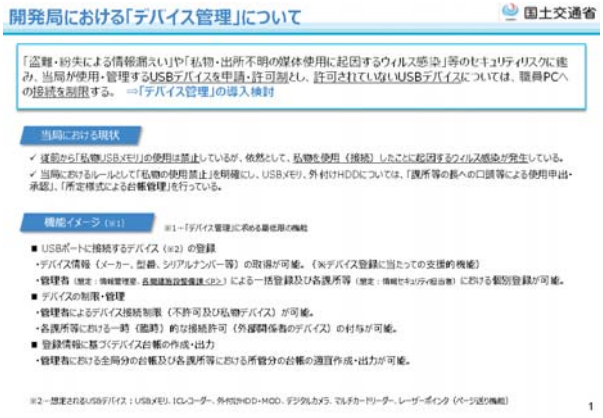

図-11　デバイス管理ソフトの要件定義

5. 今後の取組と課題

(1) 実施手順書の改正と新たな脅威に対抗するための対策

統一基準群及びポリシーの改正を踏まえ、新たな対策や概念を実施手順書に反映させる場合は、冗長的な表現を避け、出来るだけ具体的に対策を例示するなどして分かりやすく、理解しやすい実施手順書を目指すこととする。

職員に対する影響が大きい改正内容が含まれる場合は、今回の改正時における対応と同様、施行開始時期の検討や改正内容に関する説明会の開催、開発局イントラネット等を利用した職員周知など丁寧な対応を考慮する。

また、政府機関等に対する脅威を踏まえ、統一基準群及びポリシーに新たな遵守・対策事項が定められた場合は、当局におけるリスクを勘案の上、実施手順書を改正するとともに、計画的に対策を講ずる必要がある。

(2) 標的型攻撃対策

「標的型メール攻撃」については、平成24年度から、国土交通省総合政策局情報政策課が実施する標的型メール攻撃訓練に参加しているが、標的型攻撃の脅威は、政府機関、民間企業を問わず増大し、不正アクセスや情報の流出などといった直接的な影響だけではなく、組織の信用・信頼の失墜、国民・関係者への謝罪、本人、上司を含めた関係職員の懲戒処分に発展する場合もあり、当局職員の更なる意識定着と冷静・適切な対処方法を習得するためにも、今後も継続して当該訓練に参加していくことが重要となる。

(3) USBメモリ等に関する対策

USBメモリ等の効率的かつ適正な制御・管理を目的としたデバイス管理システムについては、平成30年度内の導入・稼働を目標とする。

当該システムの検討・選定に当たり、現在、本局及び各開発建設部の各課所等において、使用が認められたUSBメモリ等は約1,900個あることから、管理課所等における一括登録や管理台帳出力、外部関係者が持ち込むUSBメモリ等の一時的接続許可の可否に加え、現在、実施手順書においてUSBメモリ等に限定している対象範囲の拡大も併せて検討する等、当局の業務処理上、想定される運用形態を十分考慮する。

また、システム導入・稼働時における混乱を避け、スムーズな導入を目指すため、必要に応じて操作説明会を開催する必要がある。

(4) 職員に対するセキュリティ教育

職員に対するセキュリティ教育については、実施手順書の規定に基づき、e-ラーニングにより年1回実施していることに加え、開発局イントラネットやコンプライアンス通信等を利用して職員周知・注意喚起も行っており、これらにより職員の意識が向上し、「標的型メール攻撃訓練」における開封率低下にも寄与していると考察されることから継続して実施する。

また、職員に対する影響が大きい実施手順書の改正があった場合には、随時、改正内容に特化したe-ラーニングを実施するなどして職員への周知と認知・理解度を高める必要がある。

6. まとめ

政府機関の業務遂行において、パソコン、インターネット、メール等の情報通信技術は必要不可欠な存在であるが、悪意のある者による攻撃は複雑・巧妙化し、ウィルス検知・対策ソフトでは検知できない新種のウィルスも日々報告されている。

ウィルス感染は、不正アクセスや標的型攻撃の糸口となる可能性が高く、その結果、情報システムの停止や情報流出などといった重大なインシデントに発展して、取り返しのつかない事態を招くおそれがあり、ウィルス被害を放置すると逆に加害者となる可能性もある。

ウィルス感染や不正アクセスによる被害を防止するためには、入口対策や内部対策などのシステム的なセキュリティ対策が必要不可欠だが、インシデントを発生させないためには、職員一人ひとりの意識の向上が最も重要であり、もし、事案が発生したときはその初動が重要となる。

そのため、情報管理室は、システム的な対策に加え、情報セキュリティに関する職員周知・注意喚起とセキュリティ教育に関する取組を推進し、職員のセキュリティ意識の向上に努めていきたい。

参考文献

1) IPA：情報セキュリティ10大脅威（2013年版～2016年版）
2) NISC：サイバーセキュリティ政策に係る年次報告（2015年度）
3) NISC：政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）について
4) 国土交通省総合政策局情報政策課：統一基準群の改定に伴う情報セキュリティポリシーの改正について