TOKIO MARINE NICHIDO

公共機関等におけるサイバー攻撃
～マイナンバー制度の導入により高まるリスク～

近年、組織に対するサイバー攻撃が増加傾向にあることは周知の事実である。中でも、政府等の関連機関や公共性の高い組織に対するサイバー攻撃は特に多発している。そこで本稿では、2016 年 1 月に開始される「マイナンバー制度」がサイバー攻撃のリスクを更に高めると言われる理由や、公共機関等サイバー攻撃の標的になりやすい組織における対策の見直しの必要性について解説する。

1. 公共機関等に対するサイバー攻撃

公共機関等がサイバー攻撃を受けた事例は枚挙にいとまがない。日本年金機構からの個人情報漏えいが明らかとなった 2015 年 6 月 1 日以降にも、サイバー攻撃の被害が公共機関等から報告されている（表 1）。

■表 1　2015 年 6 月に公共機関等で発生した主なサイバー攻撃

公表日	組織	概要
6 月 10 日	東京商工会議所	事務局員が使用しているパソコンが標的型メールによるウイルスに感染し、個人情報が流出した可能性があることが明らかとなった。
6 月 15 日	石油連盟	職員のパソコンが標的型メールによるウイルスに感染し、石油政策上の要望事項とその関連資料に関する情報が流出した。また個人情報が流出した可能性も否定できないとされる。
6 月 17 日	長野県上田市役所	庁内ネットワークが標的型サイバー攻撃を受け、ウイルスに感染していたことが外部機関からの通報で発覚した。
6 月 17 日	全国健康保険協会	4台の職員端末が外部との不審な通信を行っていたことが明らかとなった。
6 月 22 日	早稲田大学	職員が標的型メールの添付ファイルを開封したことにより、事務用のパソコンがマルウェアに感染していたことが外部機関からの通報により明らかとなった。また、同大学が所有するスケジュール管理ウェブサイトが、学外からの不正侵入により改ざんされていたことも公表された。

出典：各公式発表をもとに弊社作成

公共機関等がサイバー攻撃の標的となりやすい背景には、3 つの理由があると考えられる。

1つ目は、社会的なインパクトの大きさである。サイバー攻撃の中には、政治的な意図をもった攻撃や愉快犯的な攻撃が見受けられるが、公共機関等がサイバー攻撃を受けた場合、一般的な企業に比べ報道等で大きく取り上げられる可能性が高く、これらの意図が達成されやすいものと考えられる。

2 つ目は、情報盗取を目的とした標的先へのサイバー攻撃の踏み台としての利用価値が高いことである。例えば中央省庁等に対して標的型メールを送付する手段として、関連する公共機関等のメールを乗っ取り、乗っ取った組織のメールアドレスから中央省庁等へ標的型メールを送信することで、受信者にメールを開封させる可能性を高めることができる。またその踏み台とされた組織と中央省庁等が業務上の必要性等でネットワーク接続している場合には、その組織が中央省庁等への侵入の入口とされてしまう可能性もある。

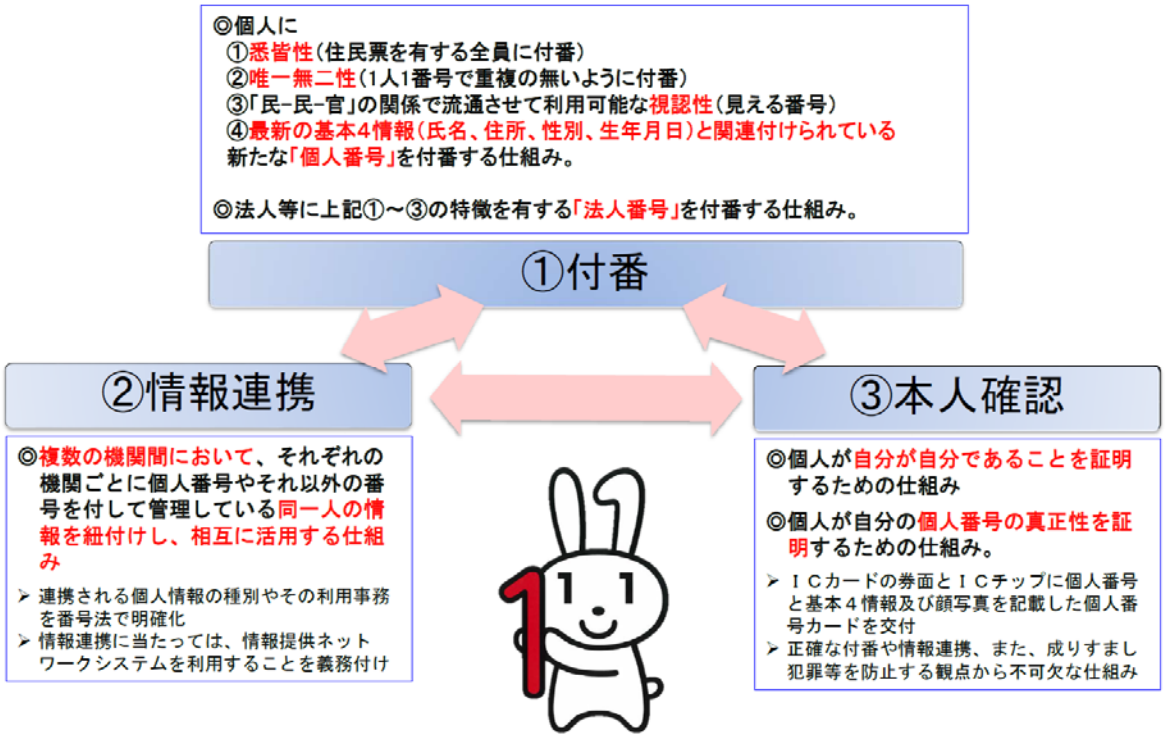
3 つ目は、質の高い個人情報を保有している可能性が高いことである。例えば市区町村役場では、居住する住民の住所や生年月日、家族構成等の情報が管理されているが、これらは民間企業が会員登録等の目的で保有する情報よりも正確であることは言うまでもない。

個人情報盗取を目的とした攻撃者にとって、公共機関は高いインセンティブ（誘因）を有する。この誘因は次章で説明するマイナンバーの導入により、今後、更に高まることが想定される。

2. マイナンバー制度の導入とリスク

2015 年 10 月に施行され、2016 年 1 月に利用開始予定の社会保障と税の共通番号制度――通称「マイナンバー制度」は、社会保障、税等の分野で効率的に情報を管理・活用することを目的とした制度である。各利用分野の情報を国民一人ひとりがもつ 12 桁のマイナンバーに紐づけることで、各機関が他機関の管理する情報を照会できるようになり、国民の手続きの負担も軽減することが期待されている。またマイナンバーが記載された IC カードは、身分証明書としての役割も担うことになる。

■図１　マイナンバー制度の仕組み



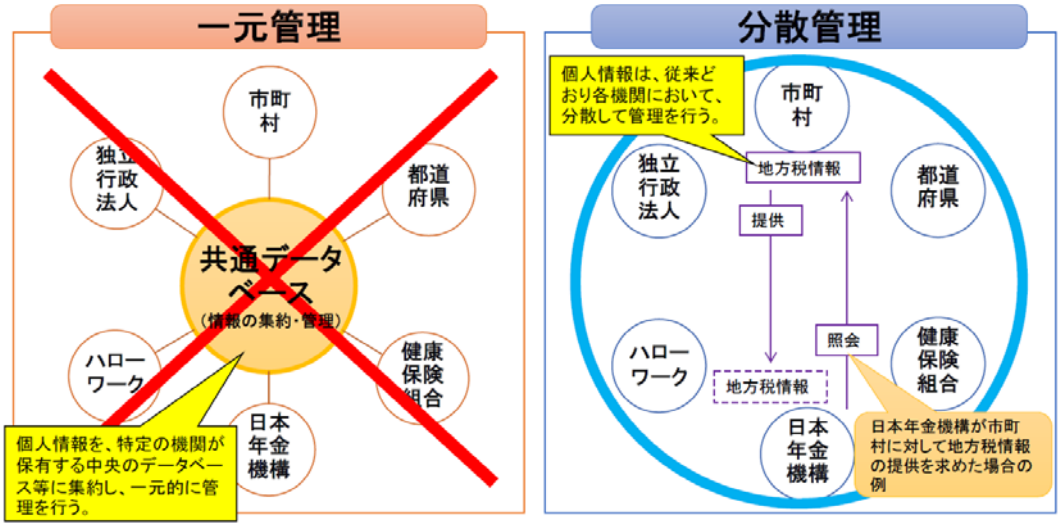
出典：内閣官房ホームページ

このように、マイナンバー制度は関係機関・国民ともにメリットの大きな制度である一方、一部の専門家からは、マイナンバーに関連したサイバー攻撃の発生を懸念する声が挙げられている。マイナンバー制度と似た制度として、1999 年に導入された住民基本台帳ネットワークシステム（以下「住基ネット」）があるが、マイナンバーは住基ネットよりも更に広範囲での利用が想定されている。

具体的には、住基ネットに登録された情報は氏名や性別、生年月日、住所に限られたが、マイナンバー制度では、社会保障や税金にかかわる情報が紐づけられる。2016 年 1 月に利用が開始されるのは、社会保障、税、災害対策の 3 分野であるが、将来的には年金や銀行口座との連動も想定されている。また住基ネットは利用する機関が行政機関に限られていたが、マイナンバー制度は当然のことながら、紐づけられる情報を扱う機関全てが利用対象となる。

内閣府はこれに対し、「マイナンバー制度に紐づけられる情報は共通データベース等で一元管理されるわけではなく、各機関において分散管理されるため、全ての情報が一度に漏えいすることはない」と説明している（図2参照）。しかし、ある機関のアカウントがサイバー攻撃者に乗っ取られ、他の機関が所有する情報を不正に照会されてしまう等、一つの機関のシステムへの侵入により、他の機関が持つ情報にアクセスされてしまう可能性がないとは言えない。またどこかの機関でマイナンバーが流出すると、当該マイナンバーを手掛かりに他の機関が持つ情報にアクセスされるリスクも考えられる。

■図２　マイナンバー制度における情報管理のイメージ



出典：内閣官房ホームページ

物事が便利になるときには、それに伴う弊害が生じることも少なくない。リスクが高まる懸念があるからといって、マイナンバー制度の利用範囲を限定すべきという意見もまた短絡的すぎるかもしれない。マイナンバー制度を安全に運用していくためには、マイナンバー制度にかかわる機関、またマイナンバーを扱う各企業等が適切な対策を講じていくことが前提となる。

万一自分の組織がマイナンバーにかかわる個人情報漏えいの原因となってしまった場合には、組織の社会的信用は大きく失墜し、莫大な賠償責任を負担する可能性がある。サイバー攻撃への対策を決してなおざりにしてはいけない。

3. 公共機関等におけるサイバーリスク対策見直しの必要性

ことにマイナンバー制度にかかわる個人情報を扱う公共機関等においては、従来からサイバーリスクに対する対策が講じられてきているものと思われる。しかし、対策が不十分だったり、導入された対策が形骸化しているケースも多々あるのではないだろうか。

日本年金機構の個人情報漏えい事件の直接的な原因は、職員が送られてきた標的型メールを開封したこととされている。しかし事件の背景を詳しくみてみると、事件を拡大させた原因が他にもあることがわかる。

1つは、運用上の不備である。本来、年金データが保存されている基幹システムはネットワークから物理的に切り離された設計となっており、そこからのデータ漏えいの可能性は極めて低かった。しかし通知業務等、一部の作業をするうえで必要なデータは、職員のパソコンともつながる「LAN システム(ファイル共有サーバー)」に外部記憶装置により適宜移される手順となっていたために、このLANシステムに保存されたデータが今回のサイバー攻撃の対象となってしまった。また、パスワードをかけるという内部の運用ルールが徹底されていなかったことも問題である。

問題発覚後の対応の遅れも、被害を拡大させた原因の 1 つである。職員が事件の発端となった標的型メールを受信し URL をクリックしたのは、2015 年 5 月 8 日であった。サイバー攻撃を確認した場合、すぐにネットワークを遮断して、関係者に注意を呼びかけることは対応の基本である。しかし同機構がネットワークを遮断したのは攻撃が確認されたパソコンのみで、同機構全体のインターネットへのアクセスが遮断されるまでにはいくつかの段階が踏まれている。実際この間に、同機構の端末から外部に対する不審な通信がたびたび確認されている[1]。

情報処理推進機構(IPA)は 6 月 2 日、「ウイルス感染を想定したセキュリティ対策と運用管理を」と題した注意喚起を行っている。ウイルス感染対策はもちろん重要であるが、攻撃手法は年々巧妙化しているため、「重要な業務や機密情報にはウイルス感染を想定した『多層防御』を行う必要がある」としている。

多層防御のポイント(管理・運用の見直し例)

1. **ウイルス感染リスクの低減**
   - ソフトウェアの更新の習慣化および徹底
   - セキュリティソフトウェア(ウイルス対策ソフト)の導入
   - メールの添付ファイルのブロック
   - ウェブフィルタリング
   - 教育や訓練
2. **重要業務を行う端末やネットワークの分離**
   - 一般の端末と重要業務システムとの分離
   - 部署など業務単位でのネットワークの分離
3. **重要情報が保存されているサーバーでの制限**
   - 共有フォルダのアクセス権の設定
   - データの暗号化やパスワードによる保護
4. **事後対応の準備**
   - 体制の整備
   - 手順書や外部の連絡先の準備

出典:情報処理推進機構ホームページ「【注意喚起】ウイルス感染を想定したセキュリティ対策と運用管理を」
(http://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html)

[1] 日本年金機構の情報漏えい事件に関する情報は、2015 年 6 月 1 日に行われた同機構による記者会見をもとにしている。

公共機関等やその他の個人情報等、重要な情報を扱う機関においては、自分の組織のサイバー攻撃への対策が適切であるか、改めて見直しを行うことが重要である。特に、ウイルス感染を完全に防ぐことが今や不可能と言われている中、「ウイルスに感染しないこと」を前提に置いた体制は極めて危険と言える。

顕在化していないリスクに対する対策は、どのような組織においても形骸化しがちである。対策の見直しをPDCA（計画・実行・評価・改善）サイクルにあてはめて定期的に行うことが求められるのは、サイバー攻撃への対策も同じであることは言うまでもない。

4. おわりに

民間調査会社が日本と米国の企業を対象に実施した複数の調査において、日本企業のセキュリティ投資が米国企業よりも低いことが明らかとなっており、対策の遅れが指摘されている。これは民間企業を対象とした調査であるが、公共機関等においてもその状況に差がない可能性は高い。

サイバー攻撃に関するリスクが高まる昨今、日本の企業や公共機関等も、扱う情報の重要性に見合ったセキュリティ投資や従業員教育等の拡大が必要であると考えられる。マイナンバーはもちろん、個人情報等重要な情報を扱う組織においては、一般的なセキュリティ対策や他組織の取組みを基準にするのではなく、自組織として本当に必要な対策を検討し、講じていくことが強く求められている。

[2015年7月9日発行]

東京海上日動リスクコンサルティング株式会社
ビジネスリスク本部
〒100-0005 東京都千代田区丸の内1-2-1 東京海上日動ビル新館8階
Tel.03-5288-6712 Fax.03-5288-6626
http://www.tokiorisk.co.jp/