自治体等サイバー・セキュリティの脅威と セキュリティ・ガバナンスの動向について （調査研究レポート）

目　次

自治体等サイバー・セキュリティの脅威とセキュリティ・ガバナンスの動向

1．はじめに

本資料は政令指定都市の副最高情報統括責任者（いわゆるCIO補佐官）、その後、大学研究機関にて電子自治体（CIO 制度設計研究、サイバー・セキュリティ研究）と地域活性化の実践的な研究活動を行ってきた筆者（研究員）の研究レポートである。

冒頭、本研究レポートでの用語の定義等を行う。

⑴「自治体等」：基礎自治体、中核市、政令指定都市、特別区、都道府県並びに、教育委員会、小中高等学校、自治体に関連する外部機関（財団法人、一般社団法人）大学・大学院などを指す。

⑵「サイバー・セキュリティの脅威」：庁内の情報システム（基幹系システム、情報系システム）のみならず、自治体等に関連した外部機関とのデータ連携や、スマートフォン、タブレット端末、IOT,M２M 等を通じて庁内のシステムと何らかの形でデータの授受が行われる範囲での脅威を指す。

⑶「セキュリティ・ガバナンス」：自治体等により体制や運用に差異があるが、ここで言うセキュリティ・ガバナンスとは自治体等が条例や規則、要項等で定めたところの、「最高情報統括責任者（いわゆるCIO）」「最高情報セキュリティ統括責任者（いわゆるCISO）」体制を指す。
その任に当たる責任者のもとで「情報セキュリティポリシー」の実効性と組織体制の適切性、リスク管理、インシデント対応などが適切に遂行されているかを指す。

2. サイバー・セキュリティの脅威

平成２８年 ２ 月 ７ 日に放送された「NHK スペシャル サイバーショック（CYBER SHOCK）狙われる日本の機密情報」では平成２７年５月の日本年金機構の標的型攻撃で約１２５万件の年金情報が流出した以外にも、同時に約１０００以上の企業、行政機関、病院などがサイバー攻撃を受けたと報道された。

日本年金機構に届いた不審メールの一覧の中には非公開の職員のメールアドレスに届いた「件名：年金規制制度の見直しについて」というメールがあり、公開アドレスに届いたメールは「件名：年金制度見直し（試案）に関する意見」であり、職員が不審を抱かず開いてしまう巧妙な手口のものであった。（「年金情報流出問題」に関する調査報告書より）

そして、さらに脅威なのは、約１，０００件の中に公的機関や大学付属病院、自治体、防衛関連産業など国家の安全保障を脅かすようなインシデントが数多く発生していることである。

そのインシデントの中には新たな開業を間近に控えた交通機関(防犯体制、安全対策等交通の安全に関わる情報)、国の安全保障（政治家の行動予定など）に関する情報、医療の最新研究に携わる機関、企業の知財等が攻撃対象となった。

また、自治体等では小規模な自治体もその攻撃の対象となった。その自治体（日本海側の町役場)は職員が海難事故防止のホームページに仕掛けられたマルウェア（水飲み場型攻撃という）に感染したことが明らかになっている。

これらのインシデント事例からも分かる通り、数年前とは状況が大きく異なり、規模の大小問わず、あらゆる行政機関・自治体等はこれらの脅威に対処することが喫緊の課題となり、またセキュリティ・ガバナンス体制の構築は一部門（例えば情報システム課）だけの問題ではなく自治体トップ（首長）の問題となっており地域住民に対する説明責任が今後厳しく問われると想定される。

次項以降にこれらのサイバー・セキュリティの脅威の現状を踏まえ、自治体等の取るべき手段や対策の動向を技術面・体制面で提言する。

3. 自治体等のサイバー・セキュリティ要件（システム面）

情報漏洩とサイバー攻撃・標的型攻撃から自治体の情報資産を守るためには、

１） 外部からの攻撃（ウィルス・マルウェア・標的型攻撃）

２） 内部からの情報流出（過失・故意による情報流出）

の２つの側面からの安全を担保する必要がある。

１）２）を同時に確保するためには運用や規則や罰則規定といった規律による管理では不十分である。また、企業のように情報資産を厳重な入館・退館管理で行うことは「市民に広く開かれた市役所」である基礎自治体にとって非現実的である。

そこで、筆者はシステムとしての必要機能要件は以下４点と考える。

ア 持ち出しはすべて自動暗号化

基幹系・情報系問わずシステムの外に持ち出す操作をすべて検知し、自動的に暗号化すること。USB メモリ、外付け HDD,CD-R,スマートフォン、メール等ネットワーク経由も自動暗号処理。

イ 書き出し制限機能（Write 制限機能）。

インターネットなどの通信やあらゆるアプリケーション、すべてのファイルに対して「書き込み・通信(Write)」を完全にシャットアウト。

ウ すべての PC 操作の履歴取得。

すべての PC の全操作・プログラムの動きの記録。全業務のトレーサビリティと耐監査性を担保する。

エ サイバー攻撃に対するディフェンス機能。

ウィルス、マルウェア、標的型攻撃、未知のウィルス、フィッシングまであらゆるサイバー攻撃から防御策を打つこと。

以上４つのシステム要件を満たすためには、従来のウィルスソフトによる対策では不十分であり、OS サイドのセキュリティミドルウェアとして API の動きを監視し、すべてのアプリケーション命令をコントロールする必要がある。

4. 従来方式のどこが問題か

では従来から自治体等がとってきた対策やシステムのどこが問題なのか幾つかの具体例で説明する。

⑴ ウィルス対策ソフトによるセキュリティ対策
これまでのウィルス対策ソフトでは未知の脅威は防げない。
それは、既知のウィルスの検知競争でありゼロデイ攻撃を例に挙げればブラックリスト方式では未知のサイバー攻撃を防ぐことはできない。
これから重要な機関等のセキュリティ対策はホワイトリスト方式が主流になるであろう。

⑵ 基幹系と情報系の物理的な分離運用
基幹系システムと情報系システムの物理的分離は多くの自治体で既に実施しているが、調査統計でも明らかなようにインシデントの８割が過失による情報漏洩であり、物理的に分離したとしても情報の持ち出しは完全には防げない。（日本年金機構のインシデント事例）

⑶ 仮想化ソフト・シンクライアント等による対策
これは VM(Virtual Machine)と言う古くからある技術やレガシーシステムの端末の技術を応用したものであり、幾つかの自治体で実施しているが、同じく人間系による故意・過失によるインシデントは完全には防げない。

⑷ セキュリティポリシーで厳しく運用を規定して、職員の研修を定期的に行う
これも人間系の対策であり、インシデントの８割に当たる、過失・故意の情報漏洩を防ぐことはできない。国が定める番号制度の罰則規定もこれにあたり、悪意を持った故意の情報漏洩を未然に防ぐことはできない。

⑸ ２４時間 365 日の監視体制を外部に委託する
これはかなりの抑止効果があるが、監視範囲はネットワーク経由のサイバー攻撃であり、先程来の悪意・故意・過失による情報漏洩を防ぐことは出来ない。
情報漏洩の多くは、退職者や外部委託先などで起きており、ネットワーク監視ではこれらを完全に防ぐことはできない。

5. それでは、どうすれば良いのか？

それは実社会のセキュリティを考えてみれば良い。
実社会のセキュリティ（物理セキュリティ）はすべてホワイトリスト方式なのである。
例：＊ビルの入館管理（ID カード）
ID カードを持っている人のみ入館できる。ゲスト ID は決められた部屋のみ入室できる。

＊空港のゲート
２重３重物理的なセキュリティチェックを行い、パスした人のみゲートをくぐることが出来る。

あるべきサイバー・セキュリティ　システムの要件定義：

１）　自動暗号化（あらゆる持ち出しに対し）
２）　書き出し制限（Write 制限機能）
３）　PC 履歴の完全取得（Auditability）
４）　ホワイトリスト方式のディフェンス機能（未知の Cyber 攻撃からの防御）
５）　人間系・運用・規則等に頼らないシステム（８割は過失による情報漏えい）

以上５つのシステム要件を満たすサイバー・セキュリティ製品を喫緊の経営課題として各自治体や行政機関は検討する必要がある。

次項にシステム面だけでなく、自治体等の体制面での提言を行う。

６．サイバー・セキュリティのあるべきガバナンス体制

サイバー・セキュリティシステムの要件と同時にガバナンス体制が重要となる。

<u>あるべきサイバー・セキュリティガバナンス体制の提言</u>

１．　情報システム部門から独立した庁内全体を統括できる立場の最高サイバー・セキュリティ統括監の設置。

行政機関では台風・地震・ゲリラ豪雨と言った防災面での「危機管理室」や局部長級の「危機管理監」といった体制を構築しつつある。同様にサイバー・セキュリティに関しても「最高サイバー・セキュリティ統括監」等の設置が喫緊の課題であり、サイバー・セキュリティに関して全ての権限と責任を持ち万一、セキュリティ・インシデントが起きた場合のリスク管理等のコントロールタワーとなる必要がある。

２．　番号制度（いわゆるマイナンバー制度）の本格的な運用を間近に控え、特にバックオフィスのデータ連携とセキュリティ対策を一体化して見直す。

マイナンバー制度は本来的には国の事務（法定事務）であり、自治事務ではないが、セキュリティ・インシデントの責任は自治体にもある。現場のシステムの改修に終始するだけではなく、運用体制・業務フローの見直し、セキュリティ・インシデント防御対策の一体化した取り組みが必要である。

３．　最高サイバー・セキュリティ統括監は副市長や市長直属とし、管下に複数のサイバー・セキュリティ専門家（任期付職員含む）を配置する。

サイバー・セキュリティのリスクを可能な限り低減させるためには、以上の様なガバナンス体制が必要であるが、庁内の権限や専権事項を超えた対応をスピーディに取る必要が出てくることもある。緊急事態に備えできるだけ上位の特別職といった庁内横断の決定ができる体制をとる必要がある。

7. まとめ

これまで述べてきたにことを簡潔に以下に纏める。

- **昨今のサイバー・セキュリティの脅威は、これまでとは全く異なり国家や自治体の安全保障を脅かすものであること。**
- **旧来型のウィルス対策ソフトや規則・運用では未知の脅威に対処できないこと。**
- **そのためには自動暗号化とホワイトリスト方式の対策が必須であること。**
- **部局の権限を超えて庁内全体を統括するガバナンス体制の確立が必要であること。**

これらのことは、マイナンバー制度の本格的な運用と、利用範囲の拡大を目前に控え、各自治体等の喫緊の経営課題であると考えている。

本研究レポートについてのお問い合わせ・具体的なご相談等はメールにて下記研究員までお願いいたします。
慶應義塾大学 SFC 研究所　研究員（自治体サイバー・セキュリティ研究）　植 松 正 博
電子メール：masa007japan@icloud.com
注：当研究レポートは研究員の見解を述べたもので慶應義塾大学 SFC 研究所の見解を述べたものではありません。

