関係各位

自治体情報セキュリティ対策における、秘密分散技術（電子割符）の適切な現場利活用に向けた予算折衝の際のポイント

―ネットワーク分離等実施後にも残る情報資産の適切な管理に対する現場対処現実解具体化に向けて―

（初版）

秘密分散法コンソーシアム
事務局　幹事　保倉　豊

拝啓

時下ますます御健勝のこととお慶び申し上げます。平素は当コンソーシアムの活動にご理解をいただき厚く御礼申し上げます。

当コンソーシアムでは秘密分散技術（電子割符）を適切に用いることで、万が一不正アクセスやサイバー攻撃等を受けた際にも被害を最小化できる具体策として、複数自治体様での現場導入を実施いただいております。本資料は、そうした導入事例の存在を知った他の自治体情報セキュリティご担当者様より、秘密分散技術（電子割符）を適切に現場導入することに関し、組織内調整を円滑にするための資料のご要望があり、複数自治体様等のアドバイス等を受け取り急ぎ関係者向け暫定版資料を作成したものです。

昨今の量子コンピュータを含めた計算機能力の向上に加え、AIの一般化は既存情報セキュリティ技術のコアである暗号技術の短命化を加速していることは周知の事実で、電子政府推奨暗号も例外ではありません。先日の GDPR 施行も大きなインパクトを世界中に与えています。そうした状況下で、原理的にも安全性根拠の異なる秘密分散技術（電子割符）の技術標準化推進活動及び、健全な市場啓発活動等を強化している我々コンソーシアムとしては、最大限全国の自治体における情報セキュリティへの貢献ができるよう、
現場ご要望に応えたいと考えております。

本資料は、そうした際の予算確保の説明等で参考となるよう工夫したものです。ご活用いただけましたら幸いです。但し、上記のとおり急なご要望に対処した資料の為、不備な箇所も多いと存じますので、ご不明な点や修正すべき点等は、遠慮なく知らせいただけますようお願い申し上げます。

敬具

自治体情報セキュリティ対策における、秘密分散技術（電子割符）の適切な現場利活用に向けた予算折衝のポイント

―ネットワーク分離等実施後にも残る情報資産の適切な管理に対する現場対処現実解具体化に向けて―

（初版）

平成30年09月11日

秘密分散法コンソーシアム

序文

我々秘密分散法コンソーシアムは２００２年の発足時より、当該技術の健全な市場普及と技術標準化を推進すべく活動をしてきた。そうした中で、個人情報保護法や番号法の本格施行、サイバーセキュリティ基本法等の国内法に加え、EU データ保護指令等に関連する情報資産の厳格な安全管理措置が官民問わず要求されている。こうした背景には、高度化・巧妙化・広域組織化する攻撃者の存在、更に量子コンピュータを含めた計算機能力の飛躍的向上や AI をはじめとしたイノベーションの結果、既存暗号技術の短命化が回避できない状況となっていることの影響も排除できない。

本資料は、攻撃者の恰好の標的となる公共組織、特に自治体におけるネットワーク分離等の情報セキュリティ対策後も実在するセキュリティ課題に対し、現場における現実解の一つである秘密分散技術（電子割符）の適切な現場導入に向けた予算確保の説明のポイントを示し、安全安心な自治体の実現に貢献することを目的としている。

注：秘密分散技術（電子割符）や IT セキュリティの技術的説明と言うよりも、実際の予算折衝での参考となるような内容を心掛けた。

目次

事務局連絡先：　秘密分散法コンソーシアム
所属・担当者名：事務局・保倉　豊
所在地：東京都渋谷区笹塚 1-32-2 ソネット笹塚 102
メールアドレス　：http://www.sss-c.org/又は、
gfi-info@gfi.co.jp

第１章　予算確保のポイント

１．１　費用対効果と事故発生時の責任の所在

血税を用いた情報セキュリティ対策は、当然ながらその費用対効果が求められる。一般論として、費用と効果に関しては下記のような図式が成立する。

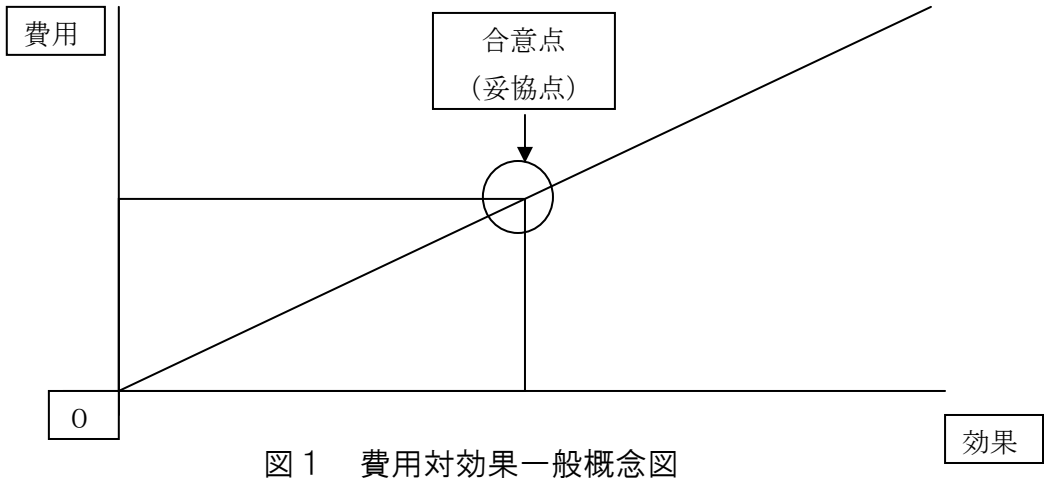

図１　費用対効果一般概念図

何らコストをかけずして効果は得られないという誰にでも分かる単純な図式であるが、予算折衝の際に往々にして軽んじられる傾向がある。この際、何に対する費用（予算）の確保を行うかを明確にすることが大事である。

自治体における情報セキュリティ対策となれば、最悪の情報漏えい等の事故発生時の損害全てを前提とした対策予算となる。同時に、予算は無限にあるわけではなく、情報セキュリティにも限界があることも事実であるから、現場の実態に即した合意点を見出す必要がある。

では、合意点（妥協点）をどの程度に設定すべきであろうか。

情報セキュリティ対策予算を考えるには、年金機構や原発事故等の教訓から、すでに想定外という逃げ道は無く最悪の事態を前提とした損害額をベースとしなければならない。その一方、予算額もセキュリティ対策も限界があるので、対策の内容を吟味して極力「残存リスク」を最小化できるセキュリティ対策を導入の際の設定としなければならない。

POINT：

① 最悪の事態を想定した被害額を知ること
② 残存リスクを最小化できる対策を具体化すること
③ 現実的合意点（妥協点）を見出すこと

コラム１　全体意識底上げの重要性

昨今の高度化するサイバー攻撃は、実は無差別型攻撃が端緒となっていることが多い。広く感染先を求め、実際に感染した端末等から様々な組織内情報を入手し、更なる標的型攻撃等を実行する。

公共機関等では首長や情報関連の CSIRT に関連した部署が参画する訓練等が実施されるが、組織全体が参加する情報セキュリティ訓練が実施されることは少ないという。

情報セクションがどれだけ意識レベルが高くても、上記のように CSIRT に関係しない部門職員の意識レベルはどうなるであろうか。先般の日本航空の標的型攻撃で約４億円の損害が発生したことは、そうしたセキュリティ意識の問題とも言える。

予算決定する部署の意識レベルが低ければ、情報セクションが実施すべきと考える予算案の真意を理解できず、予算化実現が困難なものになる。

以前お話しをお聞きした神奈川県藤沢市担当者意見では、小さなトライでも良いので、全庁職員の参加する情報セキュリティ意識の改革等に資する取り組みを実施していくことが、結果として全体の情報セキュリティ意識の向上につながり、結果として必要な情報セキュリティ対策予算への理解度も高まることとなるとし、小さな取り組み成果を、目に見える形で（良い結果でも悪い結果でも大して効果が無くても）首長も含め全体に情報共有すると、情報セクションへの協力姿勢が高まっていくとのことである。

やはりセキュリティとは、不断の努力による組織全体のセキュリティ意識レベルの底上げが必要なのである。

第２章　自ら考え守る

２．１　総務省ガイドライン等

自治体における情報セキュリティ対策で、基本的な資料となっているのは、総務省公開の「地方公共団体における情報セキュリティポリシーに関するガイドライン(平成27 年3 月版)」であるが、その冒頭部の第1章 総則1.1. 本ガイドラインの目的の中に、以下の記述がある。

> 地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産に自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。
> （中略）
> また、社会保障・税番号制度（以下、「番号制度」という。）におけるセキュリティ対策の状況を踏まえ、本ガイドラインについても必要に応じて更なる改定を実施する予定である。

これは、総務省としてガイドラインを出すものの、最終判断と責任は自治体（現場）にある。ということを言っている。更に、公開するガイドライン自体も完全無欠のものではないことを、あらかじめ宣言している。という構図になっている。このことから、最低限の参考例等として利活用することはできても、実際に事故発生してしまった場合には、何らこのガイドライン記載の対処例を実施していたとしても、重大事態の報告時や実際の法廷の場等に立つこと考えれば事故発生と言う事実に対して情状酌量の余地は無い。ということになる。

この基本的な構図は、総務省指導で実施されたネットワーク分離等の対策や、LG-WANを行政組織が利活用することに関しても、全く同様であると考えなければならない。今回のインタビューで直接ご担当者様と意見交換をした自治体職員様によると、漏えい事故で住民からの訴訟に敗訴した宇治市職員様は、「自治体としての対策が甘かったと見做された瞬間敗訴になるのである。」とのこと。その時点で入手可能な対策の内から、既存事故事例に該当しないもので、且つ説明責任を果たせる最善の策を講じる必要がある。

POINT：
① ガイドラインは最低限の例示でしかない
② 自治体自らが適切な安全管理措置を実施しなければならない
③ 事故発生した際の最終的な責任は、自治体（現場）に来る

コラム２　LG-WAN も芋づる式

目を背けたい事実であるが、業務系や基幹系（住基）に接続している LG-WAN は、J-LIS（地方公共団体情報システム機構）が管理しているのであるが、その安全性を保証しているわけではない。（総務省自体も然り）

その構造上、各自治体が連携しており上位には番号法関係の重要なネットワークがつながっている。しかし、LG-WAN には民間事業者とのデータ交換等が可能な ASP（インターフェース）が存在し、すでに利活用されている。

インターネットとは簡単に言えばコンピューターネットワークのネットワークであり、基本的には誰にも何も保証しないのである。上記 J-LIS の管理する LG-WAN だけがその安全性を保証できる状況にあるだろうか。攻撃者からすればゼロデイのウイルスを、そのネットワーク内のどの端末でも、IOT 機器でも感染させることができれば良いのである。ゼロデイウイルスのソースも、ゼロデイであることの確認も、攻撃者にとっては大した先行投資は必要ないのであり、そこに実在する現実の脅威への危機意識の持ち方が問われる。

第３章　攻撃者から見た自治体の姿等

３．１　自治体情報セキュリティの特異性

自治体情報セキュリティの特異性とは何であろうか。法律解釈における自治行政の考え方や、民事訴訟や国家賠償請求といった手続きの話しであろうか。そうではない。自治体の存在そのものや、自治体の保有する情報自体が、攻撃者にとって付加価値の高いターゲットである。ということ。この認識を再度肝に銘じて欲しい。参考までに少し古いが、以下東京海上日動リスクコンサルティング株式会社の公表資料の一部を引用する。

―引用部開始―

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。

―引用部終了―

上記レポート作成時点では、番号法が存在しない為、マイナンバー等の情報は対象として記載されていないが、現在は存在する。

先般日本航空が標的型攻撃により、実際に約４億円の被害に遭っている。危機意識が薄い組織ではどこでも発生しうる事件である。担当者が一定期間で異動する自治体組織は攻撃者から見て手玉に取りやすい相手と見えている。

POINT:

① 多様化する攻撃者にとって自治体は恰好の攻撃対象である

② 攻撃者が圧倒的有利であり、事故発生時の信用失墜は免れない

③ 不利な現場でも事故発生時の現場関係者の処分は厳しくなる一方

コラム３　JR 新幹線の台車亀裂問題

先日わが国の誇る新幹線の台車にヒビが入り、名古屋駅で緊急停車し事なきを得たことが報道された。まだ最終的な国土交通省運輸安全委員会の調査結果は出ていないが、ここには大事な問題が潜んでいると考える。

「日常業務における慣性の法則である」別な表現をすれば、「惰性」である。

この博多発東京行きの「のぞみ」は、名古屋で運転を取りやめる以前にすでに、異臭や煙等の異常を確認していながら具体策を行わず名古屋まで来てしまったのである。台車の状況から、その後の区間で台車が破断したであろうことが報道されている。当然、恐ろしい被害が発生することになったであろう。

筆者は、新幹線がダイヤ通りに運行される世界に冠たる日本の鉄道であることも含め、現場職員に巨大なプレッシャーがかかっていたものと考えている。つまり、少々の異常で新幹線を止めるとなれば、当然ダイヤは乱れる。するとどのような評価が自らに及ぶか。その板挟みになったのではないか。そこで働いたのが、前述の「日常業務における慣性の法則」であり、「自らが関与している間に事故さえ発生しなければよい」との考えではなかったか。「安全に関し、現場の声を軽視した」判断をしていないか。最終的には、乗客からの強い要望を受け緊急停車したのではないか。

―複数メディア報道内容抜粋―

岡山駅から乗車したＪＲ西日本の保守担当の社員が、「次の駅で停車し検査した方がいい」という趣旨の進言をしたにもかかわらず、東京の指令所が「支障はない」と判断し、走行を続けていたことがわかった。

―抜粋終了―

今後、新幹線ではじめての重大インシデントの調査報告がどのようなものになるか、注目したい。

第４章　説明で参考とすべき事故等

４．１　日本年金機構や宇治市の事件

自治体情報セキュリティを考えるうえで重大な事件として真っ先に対象となるのは、年金機構からの情報漏洩と京都府宇治市の訴訟事例であろう。

２０１５年に発生した年金機構の約１２５万人分の個人情報漏洩事件に関しては３つの公的報告書が公開されているので詳細はここに記載しないが、機構内のシステムとしてはすでに当時事実上ネットワーク分離を実施していたのだが、現場実務上の理由から情報共有のファイルサーバーを利活用していたことが発端となっている。勿論、標的型攻撃に引っかかってしまったことやパスワード等その他の問題点もあるが、根幹は現場実務においてネットワーク分離は現実解とはならない。ということであり、その後も同様な事故は発生し続けることになる。なお、当時の NEWS 記事によると表面化しているだけでも約１１億円の対処費用が費やされていることが会計検査院の調査で判明しており、本事件に関しては当時サイバーセキュリティ戦略本部長から厚生労働大臣に対して、サイバーセキュリティ基本法第 27 条第３項に基づく勧告が出されているが、技術的対策に関しては、「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）資料等を参考とする旨明記されている。

自治体事例では、１９９９年に発生した京都府宇治市役所の住民基本台帳データ２１万人分の外部漏洩事件は民事訴訟に発展したが、機微度合いが低いものとされ一人当たり１万円の慰謝料＋弁護士費用５千円の支払いの判決となった。因みに機微度が高い事件の事例としては、エステティック TBC の事件がある。この場合には慰謝料３万円＋５千円弁護士費用となった。これは外部委託先のミスであったが、裁判では委託元の責任が問われたのである。またベネッセ事件の場合には、「被害者の会」による集団訴訟となった。更に、ベネッセ事件では、株主が約 2895 万人分の個人情報を漏えいさせて 260 億円もの特別損失を計上して赤字にしてしまうような情報管理体制しか構築していなかった点について、取締役が注意義務を怠っていたなどとして、260 億円の代表訴訟を提起した。今後、経済状況の悪化もあり情報漏洩によるわずかな慰謝料でも入手したいということで集団訴訟化が容易になると考えられ、賠償額の高騰は避けられない。因みに、２０１６年 JNSA 報告の一人当たり平均想定損害賠償額は３万１６４６円である。

POINT:

①情報漏洩による民事訴訟で説明責任を果たせる対策が必要

②対処費用は賠償額に加え関係部署の緊急稼働やシステム対処、報告等々

③信用失墜、人事考課等々

コラム４　本当の強靭化の問題点

これまでコンソーシアムでは、自治体業務の実情調査や本資料作成も含め複数自治体職員に対し複数回のインタビューを重ねてきた。そこから言えることは、ネットワーク分離等の対処を伴う自治体情報システム強靭性向上モデル対処と自治体情報セキュリティクラウドの実施によって、異口同音に現場実務上の支障が生じており、情報部門が管理すべき対象が増えた為（事実上ネットワークが２倍以上になっている)、情報システム部門の負荷が増大したとの結果が出ている。

一般論であるが人間の特性を考えると、先のコラム３に記載したように人間の行動には大きく心理的要因が作用すると考えられ、この分野だけで一つの学問になるくらいの世界であるが、筆者の実体験から要約すると、

A:ことなかれ主義
B:楽をしたい
C:多数派でいたい
D:自分だけは・・・

が、人間の行動原理の本質を示すわかり表現であろうと考える。これは裁判官であろうと政治家であろうと、官公庁職員であろうと人間に通底する基本的な行動原則で、善人や悪人の違いも関係なく、あるのはその強弱のみ。

この原則から、ネットワーク分離等の後の業務環境を見たとき、何が今後表面化してくるかは、言わずもがなである。すでに各自治体インタビューで前兆現象は顕在化してきており、事件発生へのカウントダウンとも言える状況と我々コンソーシアムは認識している。事件化への基本的な流れは、

1st, 手間のかかる状態が嫌になる
2nd, 抜け道を探す
3rd, 抜け道を見つけ試す
4th, 使える抜け道を常用化
5th, 保身の為に抜け道を使う際に余計なことをする
6th, 深く静かに組織に浸透する
7th, 問題表面化した際には所属する組織全体が危機的状況となる

上記は決して単なる想像上の話しではなく、我々コンソーシアムが重ねた自治体等インタビュー結果を基にした、容易に想定できる今後の姿である。

更に付け加えるべきは、一定レベルの権限者は例えば業務系とインターネット接続系とのファイル移動等が事実上無制限にできる場合も往々にしてあるので、仮にこうした権限者のセキュリティ意識が欠如していた場合、当事者の自治体のみならずLG-WAN全体にも及ぶ重大事態発生の可能性が否定できず、そうなれば惨憺たる事態となり国民・住民からの信用はゼロになる。

第５章　説明モデル

５．１　例えばの説明シナリオ

以下予算折衝等の際の説明の流れの一例を示す。（あくまで一例）

①高度化するサイバー攻撃の概要
②総務省ガイドライン等に依存するだけでは被害発生を抑止不能
③不正アクセス等による情報漏えい等事故発生時の損害額提示
④秘密分散技術（電子割符）を適切に用いた際の効能と予算案提示
⑤予算不承認の場合の責任の所在の明確化

①高度化するサイバー攻撃の概要等は、別添資料の P4～14 参照のこと。
（別添資料は現時点非公開ですが公開に向け調整中です）

②次に、総務省ガイドライン等に依存するだけでは被害発生を抑止できない現実を示します。特に非定型ファイルやデータが実務上必ず発生しており、それら一時情報は要機密であったり機微情報であったりすることが多いことも説明。

③更に、不正アクセス等による最悪の情報漏えい等事故発生時の損害額として、例えばですが、某市市民１０万人の情報が漏えいしたとして、更にそのうちの２０％が訴訟を起こしたとします。上記 JASA 賠償額平均より１人あたり３万円の損害賠償とすると、約６億円の賠償費用となります。仮に８０％の住民が集団訴訟に応じれば、約２４億円の賠償費用となります。更に、関係者の緊急稼働や関係各所への報告準備や報告、緊急のシステム改善対処費用、市民への情報開示等々に加え、最終的には関係職員等への懲罰等も一種の損害額とみるべきでしょう。少なく見積もっても１０億円規模。

④そして、秘密分散技術（電子割符）を適切に用いた際の効能と予算案提示は、万が一の不正アクセス等の場合にも、日常的には安全管理措置対象情報が割符化されており、職員が復元して利活用している間のみに対象情報が漏えい等する可能性が限定されることから、職員に大きな負荷をかけずに被害を最小化できることを説明。更に、復元に至らない数の割符ファイルの流出等は重大事態に至らないという、複数法律家の意見や、秘密分散法コンソーシアムによる個人情報保護委員会への確認概要も説明。

⑤最後に、情報管理部門としては、昨今のサイバー攻撃等と自治体がそうした攻撃者にとって狙われやすい組織であること、更に総務省ガイドライン等を守るだけでは、自治体自身の安全管理の姿勢として不十分である事実を踏まえ、具体策とその予算を提示したので、仮にこれが承認されない場

合には、③で示す対処費用を予備費として情報管理部門に付けていただきたい旨交渉する。念押しとして、実際に情報漏えい等が発生した場合には、承認しなかった部署で責任を取っていただきたい旨、宣言する。

コラム５　予算が無いからは通用しない

これまで、自治体組織内で予算取りに苦労する方々に向けた論調で記載してきたが、自治体インタビューでは次のようなコメントも頂戴している。

「想定外だった。時間が無かった。予算が無かった。」

これでは住民はもとより裁判官も納得しない。

本章では、情報セクションからは真っ当な予算要求をした事実を宣言し、想定した事故等が発生した際に予算承認をしなかったセクションに責任論を展開するストーリーを記載してきたが、（実は、本コメントを頂戴した自治体職員様のアドバイスでもあった）それは組織内の話しで、且つ必ずしもそのような効能が確約される性質のものではない。実際に情報漏えい等の事故等が発生したら、結局のところ専門部署に対し「何故適切な対処を前もって行わなかったのか」、「然るべき説明をして予算確保しなかったのか」等々というロジックで追いつめられることになる。

前述宇治市事件関係職員コメントにもあるように、「自治体としての対策が甘かったと見做された瞬間敗訴になるのである。」ということから、情報セクションの皆さんは、必要な対策を講じさせるよう説明し説得する責任が事実上生じている状況となっており、その責の重さを周囲が理解するよう、前述のように小さな取り組みでも良いので今すぐにでも全庁レベルで情報セキュリティの取り組みを実施することをお勧めする。勿論、現時点で最善と考えられるリスク最小化の予算案提出と説明を早急に行うことは不可欠である。

第６章　引用・出典等

６．１　出典等一覧

①「地方公共団体における情報セキュリティポリシーに関するガイドライン(平成27 年3 月版)」
http://www.soumu.go.jp/main_content/000348656.pdf

②TOKIO MARINE NICHIDO　リスクマネジメント最前線　東京海上日動リスクコンサルティング株式会社
2015｜No.12　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～
http://www.tokiorisk.co.jp/risk_info/up_file/201507091.pdf

③朝日新聞デジタル　年金機構の情報流出問題、対処費に１１億円　検査院調べ
https://www.asahi.com/articles/ASJDJ45S3JDJUTILOOX.html?jumpUrl=http%253A%252F%252Fdigital.asahi.com%252Farticles%252FASJDJ45S3JDJUTILOOX.html%253F_requesturl%253Darticles%252FASJDJ45S3JDJUTILOOX.html%2526amp%253Brm%253D437

④日本年金機構における不正アクセスによる情報流出事案について　報告書・勧告等
https://www.kantei.go.jp/jp/pages/nenkin_fusei_access.html

- 情報セキュリティ強化等に向けた組織・業務改革（平成 27 年 9 月 18 日　厚生労働省）
  概要（PDF / 176KB）　本文（PDF / 297KB）
- サイバーセキュリティ基本法第 27 条第 3 項に基づく勧告（平成 27 年 9 月 11 日　内閣サイバーセキュリティセンター）（PDF / 289 KB）
- 日本年金機構における不正アクセスによる情報流出事案検証委員会検証報告書（平成 27 年 8 月 21 日　厚生労働省）
  要約版（PDF / 1.0MB）　報告書（PDF / 1.5MB）
- 不正アクセスによる情報流出事案に関する調査結果報告（平成 27 年 8 月 20 日　日本年金機構）（PDF / 10.3MB）
- 日本年金機構における個人情報流出事案に関する原因究明調査結果（平成 27 年 8 月 20 日　サイバーセキュリティ戦略本部）（PDF / 758KB）

⑤ 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年度版）
平成26年５月19日 情報セキュリティ政策会議
http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf

⑥府省庁対策基準策定のためのガイドライン 平成26年５月19日 内閣官房情報セキュリティセンター
http://www.nisc.go.jp/active/general/pdf/guide26.pdf

⑦2015 年 08 月 27 日　株式会社ラック　よくぞ出した、NISC の調査報告！西本 逸郎
https://www.lac.co.jp/lacwatch/people/20150827_000241.html

⑧インターネットセキュリティの歴史 第３回 「京都府宇治市住民基本台帳データ漏えい事件」
https://www.jpcert.or.jp/tips/2007/wr071501.html

⑨サイバー攻撃で情報漏えいが発生した際に負う法的責任とは
https://business.bengo4.com/category3/practice312

⑩2016 年 情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編～
（セキュリティ被害調査ワーキンググループ）
http://www.jnsa.org/result/incident/

⑪堺市　元市職員による個人情報の流出事案について
http://www.city.sakai.lg.jp/shisei/gyosei/kokai/kojinjoho/index.html

⑫記者の眼できる人に任せ過ぎ？ 堺市 68 万個人情報流出事件、最大の問題
清嶋 直樹＝日経コンピュータ 2016/02/23
http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/021900491/

⑬堺市　調査結果の報告（平成27年12月14日掲載）
http://www.city.sakai.lg.jp/shisei/gyosei/kokai/kojinjoho/kojinjoho1214/index.html

⑭堺市報道提供資料　平成２７年１２月１４日　担当課総務局人事部人事課 職員の不祥事案について
http://www.city.sakai.lg.jp/shisei/koho/hodo/hodoteikyoshiryo/kakohodo/teikyoshiryo_h27/teikyoshiryo_h2712/1214_02.files/1214_02.pdf

⑮堺市個人情報流出被害者の会　設立
http://sakai-johoryusyutsu.com/

⑯元堺市職員、不起訴処分に　全有権者の個人情報流出　2017 年 3 月 24 日 19 時 15 分
https://www.asahi.com/articles/ASK3S5Q3NK3SPTIL03J.html

⑰報道関係者各位　2014年9月10日　データベース・セキュリティ・コンソーシアム（DBSC）
データベースのセキュリティ対策およびデータベース管理者の意識調査報告書を公開
～管理者の 10 人に 1 人は「情報を売却するかも知れない」～
http://www.db-security.org/20140910news.pdf

コラム６　大阪府堺市事件

この事件も社会と自治体等に大きなショックを与えた事件で、全有権者約６８万人の分の住所・氏名・生年月日、市外の有権者異動先情報等がインターネット上に流出した事件で、京都府宇治市の２２万人を遥かに超える。

事前の内部通報に同市が真っ当に対処しなかったことは、前述コラム記載に関係するのでここでは触れない。一方、同職員が IT スキルがあり、自治体の為にシステム開発しようとしたとも考えられるが、筆者が注目したいのは、「確信犯」である。という一点である。

少々長くなるが、情報セキュリティに関連する者としてお許し願いたい。

前コラムで、自治体情報システム強靭性向上モデル対処に触れたが、建前として情報持ち出しはできない筈であるが、その実はある。その際、正当な業務として持ち出すのか、何らかの犯罪行為を前提とした「確信犯」としての行為なのかの区別が情報システム的につかない。人系のセキュリティをかけたとしても「確信犯」は潜り抜けるであろう。同市は対象職員を懲戒処分とし市として告訴していたが証拠が集まらず嫌疑不十分で不起訴。つまり発生する損害等を全額同市が負担することとなり、住民の集団訴訟に発展した。同元職員は、作成したシステムを無償で提供しようと売り込みをしていたようであるが、これは IT 業界のビジネスモデルで良くある話しで、後には金銭を得ようとしていたと考えるのが正しいであろう。

同市開示情報では、

「流出した個人情報を保全する試み（平成２７年１２月１４日）個人情報の流出による 2 次被害の発生は現在確認されていませんが、流出した個人情報を保全し 2 次被害の発生を防止するため、これまでに判明している市等への通報者や個人情報を含むファイルに外部からアクセスした者に対して、本事案に関する情報の提供や、流出した個人情報の返却、消去を求めるべく接触を試みています。現時点では、通報者やアクセス者に対して直接接触するまでには至っていませんが、情報提供や個人情報の返却、消去に協力が得られるよう、引き続き誠実に対応してまいります。また、万が一、2 次被害の発生が確認された場合には、あらゆる法的措置を講じて対応してまいります。」

とあるが、流出した情報による 2 次被害が発生していないことが確認できていない。や、流出した情報の返却や消去に協力が得られるよう誠実に対処してまいります。とは何であろうか。確認できていないのと 2 次被害が実は密かに発生している可能性が否定できないこととは大きな隔たりがある。犯罪者がわざわざ堺市の事件で流出した情報を利用して強盗やストーカ行為、

特殊詐欺（オレオレ詐欺）をしています。等と宣言することはまず無い。更に、流出した情報の返却や消去が事実上不可能であることを踏まえると、同市の対処は一般市民から見ると何ら流出した個人情報の保全や２次被害の発生防止措置とはならず、そもそも根本的解決策にもなっていない。

過去に情報公開されている資料で興味深いものがある。我々コンソーシアムも連絡を取ったことがあるデータベース・セキュリティ・コンソーシアム（DBSC）公開データベース管理者１０００人へのアンケート調査報告である。
―DBSC 調査報告書一部引用抜粋―
①”30.4%のデータベース管理者が「管理者でない人に管理者権限が付与されている」と回答”しており、データベースに対するセキュリティ対策は、その進捗は見られるもののまだ十分ではない。特に管理者権限を持つユーザに対する制御や監視、牽制などには課題が多い。

②”データベース管理者の約10%が「情報を売却するかも知れない」と回答”としており、
一定の割合のデータベース管理者が、状況によっては不正に手を染めてしまうかも知れないという漠然とした不安を持っている。また給与や職務環境については、必ずしも満足していない人が多く、このことが不正を起こしやすい状況を生んでいる。
―一部引用抜粋終了―
同調査報告書の公開が２０１４年であり、経年で増加傾向であることや、前述のようなネットワーク分離等の実施後の労働環境、更に社会全体の経済状況の失速等も踏まえると、管理権限を有する者の内部犯行が生じる可能性は以前よりも増加していると認識すべきである。特に労働環境や条件面の改善に向けては首長等も含めた本件理解が必須と考える。

機微な情報の持ち出しやローカル保存に関しては、複数合意での実行許可を付与する構造にするといった職員の理解と対策の実施や、秘密分散技術（電子割符）の復元条件設定機能を利活用することで、完全とは言えないまでも、そのリスクを最小化することも可能であろうと考えるが、根本的な解決には前述の不断の情報セキュリティ意識の向上や労働環境の改善が不可欠。

―以下、その他参考―
説明案
総務省指導ネットワーク分離等実施後にも個人情報等の情報資産が存在し、その適切な管理が必要である。また、外部接続系は元よりLGWANにも

民間とのデータ交換等が可能なインターフェースが存在し、ゼロデイ攻撃等の危険性は全く否定できない。特に昨今の高度化巧妙化したサイバー攻撃の実状を踏まえると、ステルス化して検知されないように静かに深く長く自治体ネットワーク内に侵入している可能性もあり、総務省ガイドライン冒頭部記載のように自治体自ら最善の対策を具体化しなければならない。

国際的にも大きな話題となったネットワークから分離されていたイラン核関連施設に対する稼働停止攻撃は記憶にも新しい。なお、総務省ガイドライン記載事項に従うことや、ネットワーク分離等は最低限の対策等の例示に過ぎず、それらを実施していたとしても、実際に漏洩等の事故が発生すれば、それは自治体が責任を負う構造であることは、先の総務省ガイドライン冒頭部記載事項を再度説明する間でもない。

相次ぐ行政機関等からの情報漏洩等を受け、昨年人事院の懲戒処分等の方針発表があったが、総務省ガイドライン記載事項や指導等に漫然と従っていて事故発生したと見なされてしまうことは避けなければならない。その為には、総務省ガイドライン冒頭部記載のように自治体自ら最善の対策を具体化しなければならないことは、一般論として最低限実施されていなければならない取り組みと考えられる。

また個人情報保護委員会公表の行政機関向けガイドラインでは、不正アクセス等があっても被害を最小化するための対策を求めている。そこには、ネットワーク分離等との例示があるが、問題点はネットワーク分離した後にも個人情報等の情報資産が存在していることである。
完全に業務アプリケーション内で閉じている場合にはまだしも、特にワード、エクセルや、PDF等の作業中ファイル等の非定型ファイルやデータは、内部資料作成や外部とのやり取り等、実務上その発生や管理をゼロにできない。また、作業中ファイルやデータ等という性質上明確な情報管理がしにくく職員個々の管理意識に依存する傾向が強い。

埼玉県小鹿野町役場様の採用事例や成田市役所様が新年度導入予定の秘密分散技術（電子割符）の全庁採用は、そうした非定型ファイルやデータを業務系又は外部接続系ネットワーク上のファイルサーバーに集約して管理するが、同時に日常的には自動的に割符化して管理することにより、安全管理措置の対象となるファイルやデータが現実には存在しない状態を実現する仕組みである。

法令解釈等の観点からは、理論上組織内に存在するが、復元しない限り対象ファイルやデータ実在しないという適切な安全管理措置を実施している状態となる。なお、対象ファイル等を利活用する際には通常のエクスプローラによる情報利活用が可能であり、且つ対象ファイル等のみをＲＡＭ上に復元して利活用し、HDDには記録しない仕組みで、ファイル等利活用終了時には自動的に再度割符化して管理される。

このことにより、職員に本システムを利用することに特段意識させる必要も無く業務上大きな負荷となっている重大事態の発生リスクを日常的に最小化すると同時に、総務省ガイドライン記載の自治体自ら最善の対策を実現し、更に個人情報保護委員会ガイドライン記載の、万が一の不正アクセス等があったとしても被害を最小化することを実現している。予算案(導入費用や保守費用等)を示す。

なお、このような要機密情報や要安定情報の管理手法は、内閣サイバーセキュリティセンター公開の、政府機関のセキュリティ対策資料にも記載されているものであり、現政府が推奨するセキュリティバイデザインの方向性にも合致する。

- ネットワーク分離後のセキュリティ
  - 制度面

    最終的には自治体が自主的に情報セキュリティ対策を策定し、その最終責任も自治体が負うもの。

    > 地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産に自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。
    >
    > 地方公共団体における情報セキュリティポリシーに関するガイドライン(平成 27 年 3 月版)

  - セキュリティリスク

    完璧なセキュリティ対策は存在しない。突破されることを前提にし、受けた被害の極限化を図る対策をとるべき。

電力・ガス等の重要インフラを含む産業用の制御システムは、常時ネットワークにつながっていないことから、サイバー攻撃の影響を受けづらいと言われてきた。
しかしながら、メンテナンスを行う際に、ウイルスに感染したＰＣやＵＳＢを介して、感染するウイルスが発見されるなど、制御システムに対する脅威が現実化してきた。

経産省：サイバーセキュリティに関する今後の課題

イランでは核施設の制御システムへ攻撃がなされ、クローズしたシステムでも安全ではないと証明することとなった。

経団連：「日本を取り巻くサイバー攻撃の現状－安心・安全な企業活動のためのヒント」

- LG-WAN 接続系の安全性
  - 多くは論理分離のため、完全に遮断されているわけではない。
  - 完全に分離されていても、異なるネットワーク系の PC 同士を一時的に直結するようなデータ移送ケースも垣間見られるようになってきている模様。
  - USB やインターネット接続系からのメール転送などによりマルウェア等が侵入する可能性がある。
  - その他業務システム連携上、他ネットワークとの壁に穴が開いている場合がある。
  - 自組織ではインターネット接続系と完全分離していても、他組織で感染した場合、LG-WAN 経由で侵入される可能性がある。
  - 現在は安全だといわれているネットワークで対策を怠ると、侵入された場合、無防備。
  - 業者、職員等のメンテナンス時のＰＣやＵＳＢの利用によるデータ持ち出し、マルウェアの侵入等の人為的ミスも考慮すべき。

※特にゼロデイ攻撃については、新種のマルウェアの発生件数は激増。既存のウィルスソフトでは対応しきれない。

2011 年に 2000 万件未満→2014 年以降は 1 億件以上

- 守るべきデータ

個人情報、特定個人情報等が記載された、ワード、エクセルや、ＰＤＦファイル等の非定型ファイル

  - 非定型文書は、専用の業務システムに比べ管理が難しく、容易に外に出やすい。
  - 某市様では、各端末の個人情報ファイルを調査、収集したと聞いている。
  - これらをファイルサーバで集中管理し、各端末からの不用意な流出を防ぐ。
  - 一方でサーバに集約すると、攻撃者からは攻撃対象が明確になり、また一度に丸ごと盗まれるリスクがあるため、秘密分散技術で適切に守ることが必要。

- 現在利用している秘密分散技術利活用システムの拡張
  現在 PC で、口座振替データの一時保管用として使っている。各課から USB で生データを持ち込み、PC へコピーすると、自動的に割符化する仕組みであるが、庁内であっても生データを USB で持ち運ぶリスクがある。各課の端末から直接割符化し、ネットワーク上のファイルサーバへ保管し、そこからネットワークを介して金融機関への転送用 PC で直接復元することで、USB 紛失リスクを無くすことができる。

- 他のネットワークへの対応
  教育系など総務省管轄以外のネットワークについて、ネットワーク分離されていない場合の対策も必要。
  災害監監視等を行う防災系ネットワークの監視カメラやルータ等 IOT 機器に関するケアも重要と考える。

自治体情報セキュリティ対策における、秘密分散技術（電子割符）の適切な現場利活用について
―ネットワーク分離等を実施後に残る情報資産の適切な管理に対する現場対処現実解資料―
秘密分散法コンソーシアム（SSS-C）

平成３０年０９月１１日　初版公開
発　行：秘密分散法コンソーシアム
事務局：〒151-0073　東京都渋谷区笹塚 1-32-2 ソネット笹塚 102
秘密分散法コンソーシアム事務局（グローバルフレンドシップ株式会社内）
gfi-info@gfi.co.jp　秘密分散法コンソーシアム WEB（http://www.sss-c.org/）