NESCO

「自治体情報システム強靭化向上モデル」と暗号化対策

機密ファイル保護・管理システム
DataClasys（データクレシス）のご紹介

株式会社ネスコ
ITシステム事業部

20160422

概要

総務省は2017年7月から開始されるマイナンバー連携業務開始時までに自治体情報システム強靭化向上モデルと情報セキュリティクラウドを各自治体に実現するよう求めています。

今回の総務省の求めの背景には「日本年金機構への標的攻撃による個人情報125万件の漏洩事件」があります。

事件の概要と指摘は下記の通りです。

2015年5月に日本年金機構が標的攻撃を受け、125万件の個人情報流事件が発生しました。

この事件では日本年金機構の職員がメールに添付されたファイルを開封したところ「EMVIDI」と言われるRAT（RemoteAccessTooL）が動作し外部の港区の民間企業のサーバを経由して個人情報記載ファイルが外部に漏洩したと言われています。

この事件では下記の3点が各方面から指摘されています。

1）標的攻撃は異なる部門に複数回にわたって巧妙に行われ全てを防ぐのは厳しい。
2）侵入が検知された後の初期対応が甘く感染を広げてしまいました。
3）個人情報ファイルのパスワード設定により暗号化対策はルール化されていたが、実際に暗号化されていたファイルは70万件で、55万件は暗号化されておらず機構内の運用が徹底していませんでした。

また、同時期に長野県上田市、東京商工会議所などでも標的攻撃を受けました。

特に上田市では感染PCを特定するまで住基ネット、LGWAN、インターネットとの回線の接続を一時的に切り離しました。そのため行政業務、住民サービスに多大な影響を与えたと言われています。

この事件を受け総務省は急遽「自治体情報セキュリティ検討チーム」を専門家、自治体担当者なども含むメンバーで結成しました。

1.「自治体情報セキュリティ検討チーム」の活動結果

1.「自治体情報セキュリティ検討チーム」の活動結果

総務省ではマイナンバーの施行を控えこの「標的攻撃に対応するためのセキュリティ検討チーム」を7月に発足させました。

8月に中間報告、11月には報告書をまとめ各自治体にセキュリティ対策の強化を求めました。2015年度の補正予算で総額260億円の対策費を計上しました。

2．対策の概要

2．対策の概要

中間報告

年金機構の標的攻撃発生時の初動体制のまずさから感染を広げたことから緊急に中間報告がまとめられました。同報告書では事故発生時の初動マニュアルの策定、緊急時対応の計画と訓練などが中間報告としてまとめられました。

主な論点

1．組織体制の再検討、職員の訓練等の徹底
- （1）CISO・CSIRTの設置等
- （2）インシデント連絡ルートの再構築（多重化）
- （3）緊急時対応計画の見直しと緊急時対応訓練の逐次実施
- （4）特に標的型攻撃に対する対策の徹底

2．インシデント即応体制の整備
- （1）インシデント連絡ルートに沿って、都道府県による支援体制を再確認
- （2）不正通信の監視機能の強化
- （3）自治体情報セキュリティ支援プラットフォーム（仮称）の創設

3．インターネットのリスクへの対応
- （1）安全性の確認
- （2）システム全体の強靱性の向上
- （3）自治体情報セキュリティクラウドの検討

4．総務省の役割

総務省、自治体情報セキュリティ検討チーム
「自治体情報セキュリティ緊急強化対策について」中間報告
(http://www.soumu.go.jp/main_content/000372668.pdf)から抜粋

2．対策の概要

更に2015年11月に「新たな自治体情報セキュリティ対策の抜本的な強化に向けて」という最終報告書がまとめられました。

総務省報告書掲載サイト

http://www.soumu.go.jp/main_content/000387560.pdf

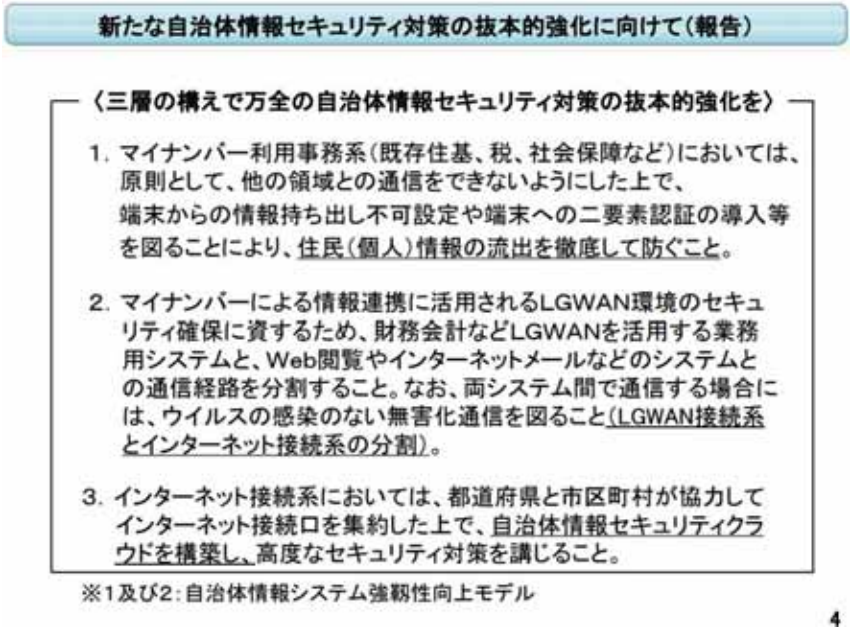
この報告書ではマイナンバーの情報連携が始まる2017年7月までに自治体情報セキュリティの抜本的対策を行う必要があるとされています。

具体的には自治体情報システム強靭化向上モデルと自治体情報セキュリティクラウドの構築が求められています。

3．自治体情報システム強靭化向上モデル

3．自治体情報システム強靭化向上モデル

自治体強靭化向上モデルではマイナンバー利用事務などの①番号系業務の情報システムと財務会計などの②自治体業務用情報システム、ホームページなどを活用した情報発信や市民とのメールによる連絡などの③インターネット活用業務の3つを原則的に分離すること。特にインターネット関連業務系とLGWAN接続系の分離が求められています。更に、情報の持ち出し制御、端末のニ因子認証の導入が求められています。



注）出口対策としての自治体セキュリティクラウド
年金機構や上田市の標的攻撃ではいずれも内閣セキュリティセンターやJPCERTコーディネーションセンターなどの外部からの指摘で標的攻撃が発覚しています。標的攻撃の際の外部との不正な通信を監視、発見するのは専門家、専門機関が必要であり、各自治体で対応するには無理があり都道府県単位でインターネットの出入り口をまとめ監視する対策を自治体情報セキュリティクラウドと称しています。

総務省報告書
「新たな自治体情報セキュリティ対策の抜本的な強化に向けて」
(http://www.soumu.go.jp/main_content/000387560.pdf)から抜粋0

4．今後の課題

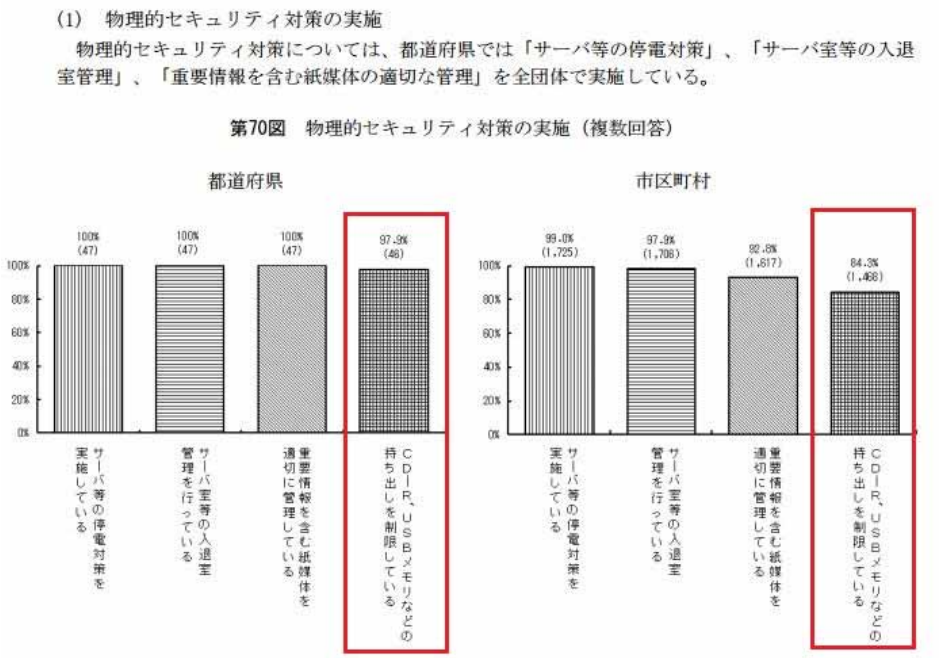
4．今後の課題

今回の総務省の情報セキュリティ強靭化向上モデルは年金機構での標的攻撃による情報漏洩事件を背景としているため主にネットワーク構成上の対策が主となっています。持ち出し制御や二因子認証などのPC管理の強化も加えられています。

すでに持ち出し制御については2016年3月に総務省自治行政局地域情報政策室がまとめた「地方自治情報管理概要」によれば大半の自治体で実施済みです。

（http://www.soumu.go.jp/main_content/000405300.pdf）

この概要によればすでに大半の自治体でCD-R、USBメモリーなどの持ち出し制御を実施しています。（都道府県で97.9%、市町村で87.2%）



総務省「地方自治情報管理概要」
（http://www.soumu.go.jp/main_content/000405300.pdf）
47ページより抜粋

4．今後の課題

しかし、これらの対策をしている民間企業や自治体でも漏洩事件は発生しています。

20014年7月に発覚したベネッセでのスマートフォン経由での漏洩事件や2015年12月に報道された大阪府堺市での職員による有権者名簿持ち出しネット上に公開してしまった漏洩事件などが発生しています。

また、今回初めて二因子認証が求められています。従来はパスワード管理を厳格に実施するように求められていたが、定期的にパスワードを変更することは逆に類推しやすいパスワードを設定することにつながりかねず効果が疑わしいとの指摘もされ始めています。そのため一般的なID、パスワードに加えて生体情報などによるユーザ認証が求められています。しかし、EMDIVなどのRATを利用したリモートアクセスは正規のユーザがログインしているPCにバックドアから侵入しますので、二因子認証は標的攻撃には有効とは言えません。

5．それでもファイルは持ち出される！

5．それでもファイルは持ち出される！

もともと自治体業務では下記のようなファイルの持ち込み、持ち出しが行われています。

・関係団体、関係者との情報共有
・国、県、他の市町村などとの通知・連絡、調査報告などの業務
・市民、関連団体との連絡、情報発信など
・庁外でのファイルの利用
・戸別訪問、庁外における各種調査業務、投票所における選挙事務、健診会場における事務、施設管理等庁外での業務執行

また、マイナンバーについてもLGWAN経由での情報連携が行われます。

従ってネットワークを分離すればファイルの外部への持ち出しはなくなることにはなりません。持ち出しできないのでは業務は回らないので一定の運用ルールのもとにファイルの持ち出しを許可せざるを得ない現状を考慮する必要があります。

さらに、電子政府、電子自治体の推進、各業務・台帳の電子化、行政事務の効率化の推進に伴い電子ファイルの庁外への持ち出しや関係団体・市民との電子ファイルでの情報共有や情報発信は今後むしろ増えていくものと予想されます。

6．ファイルは持ち出しされるとの前提での対策とは！

6．ファイルは持ち出しされるとの前提での対策とは！

ファイルがどこにあろうがファイルの管理者が許可した利用者が許可された操作範囲でのみ利用できるのであればファイル内に記載された情報をどこでもいつでも保護することができます。

このコンセプトが実現できれば、庁内で利用されるファイルも庁外の人と共有ファイルもあるいは何らかの理由で本来の利用者でない人の手に渡ったファイルも保護される。電子ファイルの共有、情報発信と保護の両立が可能となります。

このようなコンセプトの製品は実は比較的古くからあります。

典型的な製品としてAdobe社のAdobeReaderがあります。この製品はPDFに変換したファイルにパスワードを付与する、印刷を禁止するなどの設定ができます。パスワードを通知された利用者のみがファイルを開くことができ、場合によっては印刷も禁止可能です。

また、マイクロソフト社のWord、Excel、PowerPointにも同様な設定が可能であります。これらの仕組みはファイルを暗号化し、暗号化したまま閲覧や更新などの利用が可能です。したがって、ファイルが持ち出しされるという前提に対して有効な対策となります。しかし、今までは、これらの製品はアプリケーションや用途･使い方が限定されており、またパスワードの管理が煩わしいなど必ずしも自治体の業務に適用しづらい面があり普及してきていません。

6．ファイルは持ち出しされるとの前提での対策とは！

当社の開発、販売しているDataClasys（データクレシス）もこのような製品のひとつです。

「アプリを問わずに暗号化！」と「操作は変わらず漏洩防止！」をコンセプトに自社内で開発されてきた製品です。各業界のお客様のご要望に応じて開発、改良を重ねてきています。幅広いアプリケーションへの対応、金融、製造業、自治体、サービス業など幅広い業種での利用実績を誇る製品です。

今回の総務省の強靭化向上モデルで利用が想定されているSBC（Server Based Computing）方式のシンクライアントにもこの4月1日のバージョンアップで対応しました。

DataClasys の特長まとめ

■すべての段階で暗号化したまま編集、閲覧

暗号化されたファイルは機密性を保ったまま、平文ファイル（暗号化されていないファイル）と同じ操作で利用できます。
マクロ、リンクも権限があればそのまま利用可能、もちろんファイル名、拡張子もそのままです。

■暗号化されたファイルを異なるアプリケーションで共有

異なるアプリケーション間で暗号化されたファイルなどを共有、同じ権限で操作可能です。
動画や画像などのマルチメディア系のファイルも暗号化、異なるビューアやアプリケーションで利用できます。

■極秘、社外秘など機密度、重要度別の管理が可能

機密区分で暗号化されたファイルは、所属組織（グループ）職位（ポスト）によって権限管理されます。
例えば社外秘で暗号化されたファイルは部長職以上は全ての権限、課長職は印刷、更新、閲覧、一般社員は閲覧のみの権限が付与されその権限範囲で暗号ファイルを利用できます。

■オフライン利用時も、利用期限、利用端末の制限により安全に利用可能

特定の区分で暗号化された暗号ファイルのみ社内のPCをそのまま社外に持ち出してもそのまま利用できます。
ファイルが流出しても権利のない第三者は開くことができません。
IDファイル利用PC制限の利用で、暗号化ファイルを操作できるPCを特定することも可能です。

■電子政府推奨の暗号アルゴリズム、特許取得した鍵配信技術により高信頼のシステム

公開鍵暗号方式と共通鍵暗号方式のハイブリット方式を採用しています。
※公開鍵:RSA（鍵長2048ビット）、共通鍵:AES（鍵長256ビット）

■国内開発のため、ユーザニーズに細かく対応

高品質かつ日本で求められる細やかな機能をバージョンアップで実現。

■DataClasys開発Kit（オプション）により既存のシステムへの組込み、連携が可能

コマンドラインインターフェイスにより、DataClasysの優れた暗号化エンジンを文書管理システムやファイル転送、ファイル共有システムなどに組込むことが可能です。

7．DataClasysによる柔軟な運用方法

7．DataClasysによる柔軟な運用方法

DataClasysではファイルサーバ、PCローカルなどのファイルの保存領域別や特定個人情報記載ファイルにターゲットを絞った暗号化など業務に合わせたポリシーに従った暗号化管理が可能です。アプリケーションや拡張子などによる硬直的な管理ではなく、ファイルの運用に応じた柔軟な暗号化管理ができます。

1）ファイルサーバに個人情報記載ファイルを集中させて暗号化し保護する運用

ファイルサーバ上の特定のフォルダを個人情報記載ファイルの保存フォルダなどとして利用者に個人情報記載ファイルの保存を徹底させる。

DataClasysで対象フォルダを自動暗号化設定し、ファイルの新規保存、更新、名前を付けて保存時に自動的に暗号化する。リアルタイムに監視し暗号化します。（ただし、大容量、多量のファイルが保存される場合は暗号化に時間を要する場合があります。）サブフォルダも階層に制限なく暗号化します。また、暗号ファイルを開いて名前を付けて保存する場合は暗号化フォルダ内にしか保存できず暗号化属性を引き継ぎます。一度、暗号化されると暗号を解除できる権限者が復号という操作をしないかぎり暗号の解除はできません。（他の暗号システムの中には権限者が暗号化サーバ･フォルダから持ち出した場合は復号されたファイルとして持ち出されてしまう場合もあり注意が必要です。）

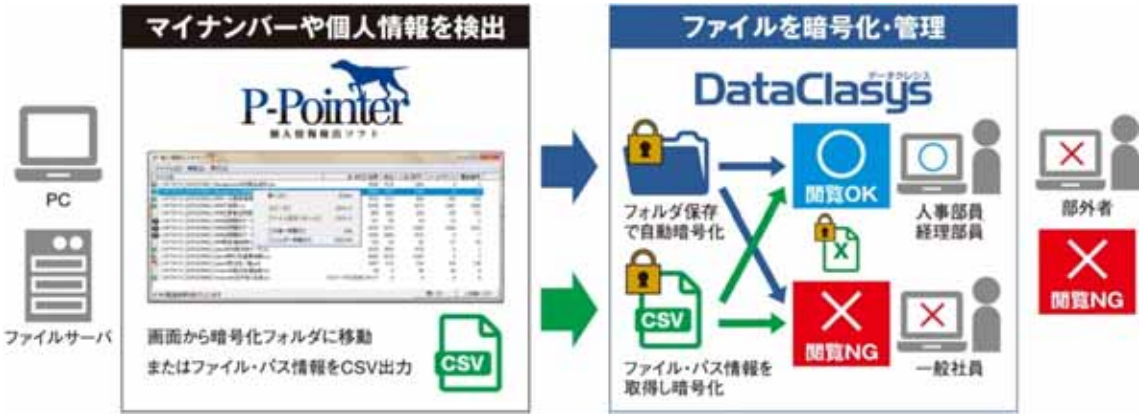
さらに個人情報探索ツールと連携することにより個人情報記載ファイルを探索して自動暗号化することができます。

PC、サーバにある個人情報記載ファイルを探索し特定のファイルサーバ領域のフォルダに自動移動しかつ自動暗号化します。

さらに暗号化された個人情報ファイルがPCなどにダウンロードされて放置された場合も定期的に探索して所定のファイルサーバに移動させて番号法に則った管理ができます。

7．DataClasysによる柔軟な運用方法

個人情報探索ツール　P-Pointerとの連携イメージ



この方式のメリットは個人情報に特化して集中的に管理し他の業務用のファイルの暗号化が避けられる。外部と共有する前提のファイルなどの暗号化を解除するなどの作業が不要になる。他の類似システムではアプリケーションと拡張子の組み合わせで暗号化されてしまうので、暗号化が不要なファイルも暗号化されてしまう。結果的に例外処理の設定が多くなりセキュリティホールとなる場合もありますが、この運用ではどうしても情報漏洩をさせたくないファイルに絞って管理できます。

7．DataClasysによる柔軟な運用方法

2）全ファイル暗号化し保護する運用

利用者がファイルを保存するファイルサーバ、PCローカルの領域を自動暗号化し、全ファイルを暗号化管理する。

全ファイルを暗号化するため、漏れなく保護することが可能です。金融機関や自治体での実績があります。ほとんどのファイルが個人情報記載ファイルである市町村では全ファイル暗号化の運用を目指す自治体が多くあります。

全ファイルを暗号化する場合は、庁外でのオフライン環境下で利用する文書、国、県への回答書や報告書やWebサイト用の文書なども漏れなく暗号化します。

・庁外でも暗号化のまま利用

DataClasysでは庁外に持ち出して利用する場合は、オフライン機能を設定することにより暗号化状態のまま一定期間のみ利用可能です。

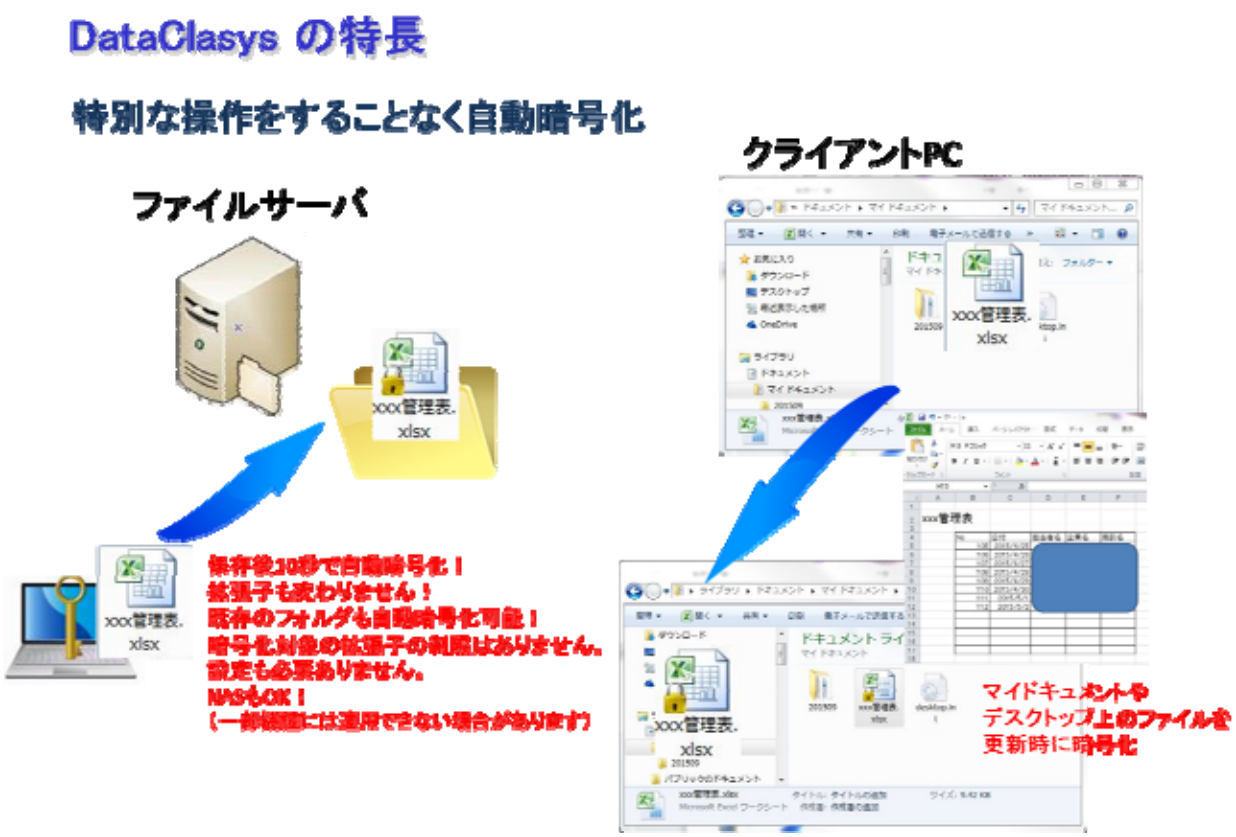
・パスワード付ZIPファイルへの自動変換

国、県、他の団体へのメールに添付するファイルはメール作成時には暗号ファイルをそのまま添付して自動的にパスワード付ZIPファイルに変換することが可能です。

全ファイルを暗号化した場合に暗号を解除する権限を利用者や管理者にできるだけ付与せずに運用する設定が可能です。

7．DataClasysによる柔軟な運用方法

DataClasysの自動暗号化



8．まとめ

8．まとめ

ファイルは持ち出しされるとの前提でファイルを暗号化管理すれば、標的攻撃対策にとどまらず電子政府、電子自治体の推進による行政サービスの向上、効率化と情報漏洩対策の両立を図ることができます。

今までのセキュリティ対策は「侵入させない」、「持ち出しさせない」というコンセプトで導入させてきました。しかし、攻撃手段の多様化･進化、例えばスマートフォンや通信機器などのポータブルな通信手段の多様化などにより、「侵入させない」･「持ち出しさせない」では対応しきれないことが明白になってきています。

ファイルの流出による情報漏洩を防ぎ、自治体情報システムの強靭化向上には「ファイルは持ち出しされる」との前提での対策が必要です。

DataClasysでは一度、暗号化されると暗号化されたまま編集、更新が可能です。編集、更新ができる利用者もファイル自体をコピーや別名保存しても暗号化のままのファイルしか扱えません。また、利用者がログインしているPCに不正プログラム（EMDIVのようなRATなど）でリモートログインされてファイルを社外に送信されても暗号ファイルのまま送信され、ファイルの中身を解読することができません。不正アクセス者はごみファイルを盗んだだけとなります。

「ファイルは持ち出しされる」との前提での対策
＝DataClasysでの暗号化で情報漏洩対策を！！

8．まとめ

自治体様の調達時に必要な暗号システムの調達仕様書のひな形を用意しています。必要な方はご連絡いただければ送付させていただきますので、下記までご連絡下さい。

株式会社ネスコ
ITシステム事業部ITソリューション
担当　板倉まで
E-MAIL：y-itakura@notes.nesco.co.jp
電話：03-3861-2348

お問い合わせは下記まで

〒101-0032
東京都千代田区岩本町1-10-5　TMMビル7F

株式会社ネスコ
ITシステム事業部
ITソリューション

Tel　03-3861-2348
Fax　03-3861-2347
URL　http://www.nesco.co.jp
E-Mail　dataclasys@notes.nesco.co.jp