— AUS（アルテミス・ユーザ・サポート）便り 2015/12/21号 —

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●IEのサポートポリシー変更、各OSでの最新バージョンを･･･IPAも警告

https://www.ipa.go.jp/security/ciadr/vul/20151215-IEsupport.html
https://www.microsoft.com/japan/msbc/Express/ie_support/

このニュースをザックリ言うと･･･

- 12月15日（日本時間）、独立行政法人情報処理推進機構（IPA）より、マイクロソフトが2016年1月12日をもってInternet Explorer（IE）のサポートポリシーを変更することに伴い、各Windows OSでの最新バージョンへのアップグレードを呼びかける発表がありました。

- サポートポリシーの変更は2014年8月に発表されていたものであり、例えば、Windows VistaはIE9、Windows7はIE11より前のバージョンのIEについてパッチがリリースされなくなります。

- IPAでは、ユーザのPCにインストールされているIEのバージョンが最新か確認すること、組織内のシステムが最新版のIEで動作するか、表示に問題がある場合互換表示モード等で対策できるか、について確認すること等を推奨しています。

AUS便りからの所感等

- 2016年1月12日にリリースされる定例のセキュリティパッチを最後に、古いバージョンのIEへのパッチの提供は終了となるとみられます。

- Windows VistaにおいてIE7・8、Windows 7においてIE8～10を利用している場合は、それぞれIE9および11へのアップグレードを行ってください（Windows 8.1・10は、いずれもIEのバージョンが11に固定されています）。

- Windows 8については1月12日にOSそのものがサポート終了となるため、Windows 8.1以降へのアップグレードが必要となることにも注意してください。

- 古いバージョンのIEからアップグレードできない場合に攻撃を受ける可能性を考慮し、UTMやアンチウイルスによる防御も怠りなく行うようにしましょう。

図1：IE のバージョンごとの影響（イメージ）

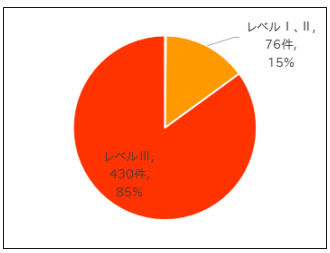


図2：IE 7 から 10 の深刻度別脆弱性登録件数
（2013 年 1 月～2015 年 11 月）

MSBC Microsoft Business Connection

IE7	IE8	IE9	IE10	IE11	OSサポート終了期間
Windows Vista					2017年4月
	Windows 7				2020年1月
				Windows 8.1	2023年1月

2016 年 1 月 12 日（米国時間）を過ぎると
各 OS の最新版の IE のみのサポートとなります

ご利用の OS	サポート対象となる最新版 IE
Windows Vista	IE9
Windows 7	IE11
Windows 8.1	IE11

●大阪府堺市、有権者68万人分の個人情報流出が判明

http://www.itmedia.co.jp/news/articles/1512/14/news104.html

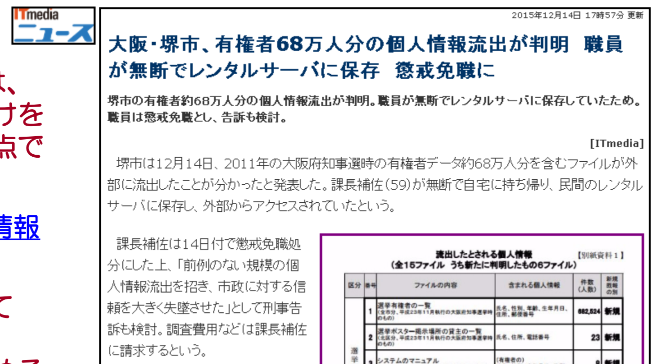
このニュースをザックリ言うと・・・

- 12月14日（日本時間）、大阪府堺市より、2011年の大阪府知事選時の有権者682,524人分の個人情報等のデータが同市課長補佐によって不正に持ち出され、外部に流出していたとの発表がありました。

- 堺市では、6月に「インターネット上に不審な情報がある」との通報を受けて調査を行い、9月7日の時点で課長補佐個人が契約していたレンタルサーバ上に外郭団体職員の名簿など約1,000件の個人情報が保存されていたのを確認したこと、また9月13日には前述の有権者約68万人分の個人情報を課長補佐が持ち出し、自宅のパソコンに保存していたことを発表しており、そして今回、約68万人分の個人情報を含めたデータもレンタルサーバ上に保存され、外部からアクセスがあったことが判明した模様です。

- 課長補佐は市選管事務局で開発していた選挙管理システムを独自に改良して民間企業等に売り込もうとしていたとされており、それら各種行為によって懲戒免職処分とされています。

AUS便りからの所感等



ITmedia ニュース

2015年12月14日 17時57分 更新

大阪・堺市、有権者68万人分の個人情報流出が判明　職員が無断でレンタルサーバに保存　懲戒免職に

堺市の有権者約68万人分の個人情報流出が判明。職員が無断でレンタルサーバに保存していたため。職員は懲戒免職とし、告訴も検討。

[ITmedia]

堺市は12月14日、2011年の大阪府知事選時の有権者データ約68万人分を含むファイルが外部に流出したことが分かったと発表した。課長補佐（59）が無断で自宅に持ち帰り、民間のレンタルサーバに保存し、外部からアクセスされていたという。

課長補佐は14日付で懲戒免職処分にした上、「前例のない規模の個人情報流出を招き、市政に対する信頼を大きく失墜させた」として刑事告訴も検討。調査費用などは課長補佐に請求するという。

流出したとされる個人情報　【別紙資料１】
（全15ファイル　うち新たに判明したもの6ファイル）

区分	番号	ファイルの内容	含まれる個人情報	件数（人数）	新規既報の別
選挙	1	選挙有権者の一覧	氏名、性別、年齢、生年月日、住所、郵便番号	682,524	新規
	2	選挙ポスター掲示場所の貸主の一覧	氏名、住所、電話番号	23	新規
	3	システムのマニュアル	（有権者の）	8	新規

- 昨年7月に発覚したベネッセからの個人情報流出事件とは、（今回は個人情報自体が主体ではなかったとは言え）金儲けを目的とした行動の過程で内部から個人情報が持ち出された点で似通っていると言えます。

- また、課長補佐に対し適切な手続きを経ることなく個人情報データを提供した別の職員等も処分を受けています。

- 不正アクセスやマルウェアによる内部からの流出についてアンチウイルス・UTMによる防御を確実に行う一方、ポリシーに反した内部からの人為的持ち出し行為を食い止めるためには、個人情報を取り扱うシステム・ネットワークの構成を見直すことが肝要でしょう。

●DNSサーバソフト「BIND」に2件の脆弱性

http://internet.watch.impress.co.jp/docs/news/20151217_735953.html

このニュースをザックリ言うと・・・

- 12月15日（米国時間）、DNSサーバソフト「BIND」について2件の脆弱性（CVE-2015-8000, CVE-2015-8461）が発表され、開発元の米ISCより修正バージョン（BIND 9.10.3-P2/9.9.8-P2）がリリースされており、JPRS等もこれをうけて警告を出しています。

- 脆弱性はいずれもDNSサーバプロセスを不正に落とされる可能性があるもので、特に1件（CVE-2015-8000）について、BIND 9.0.0以降全てのバージョンに影響するため、BINDをDNSキャッシュサーバとして利用しているあらゆる組織について早急なアップデートが推奨されています。

AUS便りからの所感等

INTERNET Watch

ニュース

「BIND 9」に深刻な脆弱性、パッチバージョン公開

（2015/12/17 19:11）

Internet Systems Consortium（ISC）が開発・提供するDNSソフト「BIND 9」において、DoS攻撃が可能になる脆弱性（CVE-2015-8000）が見つかったとして、株式会社日本レジストリサービス（JPRS）などが16日、注意喚起を出した。BIND 9の運用者に対して、修正パッチの適用など適切な対応をとるよう強く推奨している。

JPRSによれば、不正なDNS応答を拒否する処理に不具合があり、不正なクラスを持つ応答がキャッシュされることでnamedが異常終了を起こすという。キャッシュDNSサーバーの機能が有効に設定されているBIND 9の全バージョンが影響を受けることから、対象が広範囲にわたるとしている。一方、権威DNSサーバーではリスクは限定的だという。

ISCでは、この脆弱性の深刻度を"重大（Critical）"とレーティング。これを修正したパッチバージョンとして、9.10系列の「9.10.3-P2」、9.9系列の「9.9.8-P2」を15日に公開している。

同バージョンでは、これとは別の深刻度が"中（Medium）"の脆弱性（CVE-2015-8461）も修正している。

- 組織内でBINDによるDNSキャッシュサーバを立てている（そして各クライアントPCでそれを参照するよう設定している）場合、これらの脆弱性によりDNSキャッシュサーバがダウンし、名前を引くことができなくなる可能性があります。

- 脆弱性を突くシナリオとしては、メールサーバやWebサーバの名前解決のため、ターゲットとなるDNSキャッシュサーバが悪意のあるDNSサーバへ問合せを行うよう誘導することが考えられます。

- DNSキャッシュサーバが外部から第三者のドメインについての問合せを受け付ける設定になっている場合、やはり脆弱性を突くよう誘導される他、別の攻撃を受ける可能性もありますので、自組織のネットワーク以外からそういった問合せを受けないよう設定を確認することを推奨致します。

- この他、不正なDNS応答に関しては、UTMの設置によって防御できる可能性もあります。