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。

●中央省庁の職員2000人分の公用メールアドレス流出…ネットで売買

https://www.nikkei.com/article/DGXMZO28965850T00C18A4CC1000/
https://web.archive.org/web/20180409030150/http://www3.nhk.or.jp/news/html/20180403/k10011389481000.html

このニュースをザックリ言うと･･･

- 4月3日（日本時間）、内閣サイバーセキュリティセンター（NISC）より、中央省庁の職員延べ2111人のメールアドレス等が流出したとして、全府省庁に注意喚起が出されたことが分かりました。

- 2月に闇サイトにアップロード・売買されていた大量のアカウント情報をイスラエルのセキュリティ会社KELA社が調査した結果判明したもので、外務省や総務省等の職員の公用メールアドレスや、ネット通販サイトなどにログインするためのパスワードが含まれていたとされています。

- NISCでは、公用アドレスは業務以外では使わないことや、同じパスワードを使い回さないことなどのルールの徹底を改めて促したとのことです。

AUS便りからの所感等

- 省庁自体へのサイバー攻撃による流出は確認されていないとのことで、公用メールアドレスで登録していた外部サービスからの間接的な流出と考えるのが自然でしょう。

- 省庁に限らず、会社などの組織で発行されたメールアドレスでサービス登録を行うことは、こういった流出の発生時に標的型攻撃に繋がる可能性があり、組織メンバーとしての登録を要するものでなければ、可能な限り個人のメールアドレスやGMail等のフリーメールサービスでの登録を推奨することがある種のリスクの分散となると考えられます。

- パスワードを使い回さないことは、他のサービスへ芋づる式に不正ログインされる事件が多発したことから、ここ数年セキュリティ対策として重要視されています。

- 奇しくも総務省では「パスワードの定期的変更は不要」と呼びかけるようになりました（「AUS便り2018/04/09号」参照）が、こういった流出が発生した時、あるいはその疑いが生じたときこそがパスワードを変更しなければならないタイミングであることに注意が必要です。

日本経済新聞

中央省庁でメアド流出　職員延べ２千人、パスワードも

社会
2018/4/3 23:11

保存 共有 印刷 その他

政府の内閣サイバーセキュリティセンターは３日、中央省庁の職員延べ約２千人のメールアドレスが外部に登録したログイン用のパスワードとともに流出していたとして、全府省庁に緊急の注意喚起を行った。インターネット上の複数のサイトで同じパスワードを使い回すことを禁止し、必要に応じて変更を呼び掛ける内容。政府関係者が明らかにした。

日本政府の関係機関を狙ったサイバー攻撃では、2015年に日本年金機構の個人情報約125万件が流出している。

サイバー攻撃の形態が複雑化する中、政府は18年度のサイバーセキュリティーの関連予算として621億円（17年度比22億円増）を計上し、中央省庁の防御態勢強化に取り組んでいる。20年東京五輪・パラリンピックに向け、今年７月にはサイバーセキュリティ戦略を３年ぶりに改定する予定だ。〔共同〕

画像の拡大

霞が関の官庁街

NHK NEWS WEB

中央省庁2000人余のメールアドレス流出 ネット上で売買

4月3日 16時12分　IT・ネット

サイバー攻撃の新たな危険が明らかになりました。中央省庁の職員延べ２０００人余りのメールアドレスが、外部に登録したパスワードとともに流出してインターネット上で売買されていることがわかり、「内閣サイバーセキュリティセンター」はすべての省庁に対して緊急の注意喚起を行いました。

情報流出は、ことし２月に何
に判明しました。

イスラエルにある情報セキュ
果、外務省、経済産業省、総
のメールアドレスと、会員制
れ、すでに何者かによってこ
確認されました。

これらの情報は、業務中にア
公用のメールアドレスを使っ
か、過去に流出した古い情報

”標的型攻撃で被害拡大のおそれも”

今回、流出が明らかになった情報が悪用された場合のリスクについて、情報セキュリティーに詳しい社会情報大学院大学の白井邦芳教授は、特定の省庁の職員を狙って偽のメールを送りつけ、ウイルスに感染させて機密情報を盗み取る「標的型」と呼ばれるサイバー攻撃のほか、中央省庁の職員を装った詐欺やサイバー攻撃の危険性を指摘しています。

さらに、外部のシステムなどで同じパスワードを使い回していると認証を突破されてしまうほか、違うパスワードを使っていても似たような特徴がないか類推されるおそれがあるとしています。

白井教授は「犯罪者が情報を手に入れるとどのような立場の人のメールアドレスかを調べて標的型攻撃などを仕掛けるおそれがあり、被害が大きくなることは十分に考えられる」と指摘しています。

一方、今回、流出が明らかになった情報の中には中央省庁のほか大手企業や大学、それに個人のものも含まれ、日本人とみられるメールアドレスとパスワードは２００万件にのぼっています。

●大学のWebメールシステムに不正アクセス…36万通の迷惑メール送信

https://www.nikkei.com/article/DGXMZO29194310100420180000000/

このニュースをザックリ言うと・・・

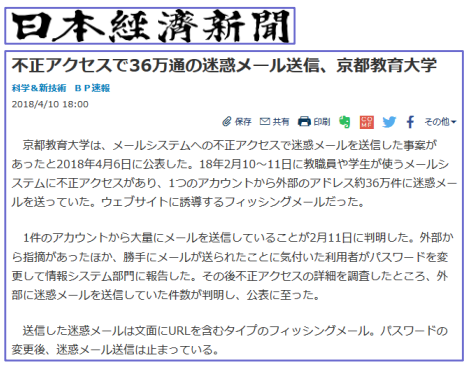
- 4月6日（日本時間）、京都教育大学より、同大学のWebメールシステムが不正アクセスを受け、外部への迷惑メール送信に悪用されていたことが発表されました。

- 不正アクセスは2月10日～同11日に発生しており、1件のアカウントが乗っ取られ、学外の約36万件のメールアドレスに対しフィッシングメールが送信されたとのことです。

- なお、Webメールサービスおよび学内の他のサービスからは個人情報の流出の痕跡はなかったとしています。

AUS便りからの所感等

- 組織内部ネットワークのサービスへ、任意の外部ネットワークからID・パスワードだけでログイン可能になっていたところをフィッシングメール等でアカウント情報を抜き取られたか、推測されて侵入されたものとみられており、今後学外からの利用時に多要素認証を求めるシステムの導入も検討するとしています。


日本経済新聞

不正アクセスで36万通の迷惑メール送信、京都教育大学

科学&新技術 ＢＰ速報

2018/4/10 18:00

保存 共有 印刷 その他

京都教育大学は、メールシステムへの不正アクセスで迷惑メールを送信した事案があったと2018年4月6日に公表した。18年2月10～11日に教職員や学生が使うメールシステムに不正アクセスがあり、1つのアカウントから外部のアドレス約36万件に迷惑メールを送っていた。ウェブサイトに誘導するフィッシングメールだった。

1件のアカウントから大量にメールを送信していることが2月11日に判明した。外部から指摘があったほか、勝手にメールが送られたことに気付いた利用者がパスワードを変更して情報システム部門に報告した。その後不正アクセスの詳細を調査したところ、外部に迷惑メールを送信していた件数が判明し、公表に至った。

送信した迷惑メールは文面にURLを含むタイプのフィッシングメール。パスワードの変更後、迷惑メール送信は止まっている。

- たった1件のアカウントの乗っ取りでも、そこを踏み台としての更なる内部への不正アクセスや、外部への大規模の迷惑行為という悪用に繋がり得ますが、今回メール送信以外の被害が発生しなかったのが救いだったものの、これについても不審な外部への通信を遮断するといった出口対策を行う余地はあったと言えます。

- こういった不正アクセス事件を単に批判するのではなく、自組織においてとるべき対策、例えば外部からのアクセスに対する認証の追加や、UTMの導入等による不正行為を自由に行わせない安全なネットワーク構成等を検討する材料とすることが重要です。

●仮想通貨を採掘する「Chrome」拡張機能、全て禁止に

https://japan.zdnet.com/article/35117084/

このニュースをザックリ言うと・・・

- 4月2日（米国時間）、Googleより、同社のWebブラウザ「Google Chrome」の拡張機能を公開する「Chrome Web Store」において、仮想通貨のマイニング（採掘）を行う拡張機能を排除する方針を明らかにしました。

- 仮想通貨をマイニングする拡張機能の承認は今後行わず、また6月下旬には、既存の拡張機能についてもマイニングを行うものは全て削除するとしています。

- 同社では、これまでマイニングを唯一の目的とするとユーザに十分に説明している拡張機能を承認していましたが、マイニングスクリプトを含む拡張の約90%がこのポリシーに従っておらず、却下されていたとのことです。

AUS便りからの所感等

- 昨年ランサムウェアに取って代わってマイニングを行うマルウェアが増加し（「AUS便り2018/02/13号」参照）、今年に入りわずか3ヶ月間でGoogle・FacebookおよびTwitterが関連する広告の掲載を禁止する方針とする等、仮想通貨をめぐる状況は劇的に変化しています。


ZDNet Japan

仮想通貨を採掘する「Chrome」拡張機能、全て禁止に

Stephanie Condon（ZDNet.com） 翻訳校正：編集部 2018年04月03日 08時32分

いいね！19 G+ B! 5 Pocket 10

印刷 メール ダウンロード クリップ

Googleは、ユーザーの同意なく仮想通貨マイニングスクリプトを埋め込む拡張機能が増えていることを受け、そうしたスクリプトを実行する「Chrome」拡張機能を取り締まろうとしている。

Googleは米国時間4月2日から、仮想通貨マイニングを実行する拡張機能について、その意図が明示されているか否かに関わらず「Chrome Web Store」では承認しないことをブログ記事で明らかにした。続いて6月下旬には、仮想通貨をマイニングする既存の拡張機能をすべて削除するという。

- SNS等ネット上の評判に注視しつつ、可能な限り公式の拡張機能サイトからインストールするよう心がけること、加えてアンチウイルス・UTMによるプロセスや通信の監視・適宜遮断を行うことが内部で不正行為が行われるリスクを少しでも軽減する一助となるでしょう。