

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。

●大学生・関係者等約35万人分の個人情報、学内イントラネットで4年間閲覧可能状態に

<https://www.yomiuri.co.jp/kyoiku/kyoiku/news/20240604-OYT1T50073/>
<https://www.nikkei.com/article/DGXZQOUE046370U4A600C2000000/>



このニュースをザックリ言うと…

- 6月4日(日本時間)、早稲田大学より、同大学関係者の個人情報が学内イントラネット上で約4年間閲覧可能な状態にあったと発表されました。
- 閲覧可能とされていたのは、同大学の在學生・卒業生を含む大学関係者約35万人分の氏名およびメールアドレスです。
- 2020年4月のシステム設定変更が原因とされ、今年5月3日に指摘を受け、同9日に対策されたとのこと。

AUS便りからの所感等

- 学外への情報漏洩や悪用は確認されていないとのこと。
- 状況についての詳細は不明ですが、一般に考えられるケースとしては、古典的な例である「個人情報が保存されたファイルにWebからアクセスが可能だった」もの、近年であれば「本来アクセスできないデータベースサーバーのポートに直接アクセス可能だった」もの、また「フロントエンドのWebアプリケーションから直接クエリーを送信するデータベース」を利用している場合に「ブラウザから細工したクエリーを送信することにより、本来想定していないテーブルの全件取得が可能だった」もの等様々です。
- Webサービスの構築時や以後の設定変更の際し、情報漏洩が発生するような問題が生じないよう慎重を期すことはもちろん、情報が閲覧可能な状態になっていないか可能な限り確認することが肝要ですが、システムの複雑化が進み、開発側が自前で一通り確認するにも限界があると思われることから、第三者によるセキュリティ診断を受けることを強く推奨致します。

日本経済新聞

早大、個人情報閲覧可能状態に 学内ネットで35万人分

社会・調査

2024年6月4日 14:45

📄 保存

📧 📧 📧 📧 📧 📧

早稲田大の学内イントラネットで2020年4月～今年5月の約4年間、在學生や卒業生ら大学関係者約35万人分の氏名とメールアドレスの一覧が閲覧できる状態で掲載されていたことが4日、大学への取材で分かった。早大によると、システムの設定変更が原因で、学外への情報漏洩や悪用は確認されていない。

学内イントラネットは在學生や教職員らが利用しており、ログインにはIDとパスワードが必要。20年4月にIDを管理するシステムの機能変更が行われ、登録者の氏名とメールアドレスが閲覧できる状態になったが、大学側は気付かなかった。

YOL 読賣新聞 オンライン

早稲田大学の学内イントラネットで4年間、氏名とメールアドレス35万件が閲覧できる状態に

2024/06/04 11:15

📄 この記事をスクラップする 📧 📧 📧 📧

早稲田大学の学内イントラネットで、在學生や一部卒業生などの氏名とメールアドレス約35万件の一覧が約4年間、閲覧できる状態になっていたことが分かった。同大は利用者から指摘を受けた5月に設定を変更し、国の個人情報保護委員会と文部科学省に報告した。学外への情報漏洩は確認されていないとしている。

● Web公開資料PDFに個人情報…マスク下の情報削除されず

<https://xtech.nikkei.com/atcl/nxt/column/18/00598/040500266/>
<http://db.pref.tottori.jp/pressrelease.nsf/webview/O68A5B1B8698392449258B230004418F>



このニュースをザックリ言うと…

- 5月21日(日本時間)、鳥取県より、同県消防防災航空センターがWebサイトで公開していた資料に**個人情報が含まれていた**と発表されました。
- ヘリコプターの「運航の手引き」資料内に**実際の救助事案の報告書が添付**されていましたが、記載されていた**要救助者1名の住所・氏名・電話番号等**について**マスクをしていたものの不十分だった**ため、それらの**情報が確認可能な状態**にあったとしています。
- 当該資料は2023年2月からWebサイトに掲載され、今年3月10日に**消防隊員が気付いたため削除**したとのことです。

AUS便りからの所感

- 掲載時点で、マスクにより画面上では見えないものの、**テキストデータとしてコピー&ペーストが可能**な状態だったとみられ、また掲載直後に**資料を更新した際マスクがずれ、画面上からも閲覧可能な状態**になったとしています。

- Office文書(Word・Excel・PowerPoint)やPDF文書で機密情報部分をマスクしても、マスクの下やテキストデータが閲覧可能だった**事例は過去にも多く報告**されており、**Acrobatの墨消し機能やその他のツールも活用し、マスクされた箇所のその下の部分についてもテキストレベルからの修正・削除を行うこと、資料に貼り付ける画像についても貼り付ける前に画像データの方を修正**することが重要です。

- 加えて、**マスクした状態でデータのコピー&ペーストや検索(機密情報に繋がる入力へのマッチ)ができないかのチェック**を行うことを強く推奨致します(PDF文書内で**検索できない設定**を行う場合、この**設定を解除するツールもある**ことから、**設定する前の状態でチェック**すべきでしょう)。



消防防災航空センターホームページにおける個人情報の漏えい

もどる 2024年05月21日提供 資料提供

提供機関

提供課等：危機管理部消防防災航空センター
電話番号：0857-38-8125 FAX番号：0857-38-8127

内容

消防防災航空センターがインターネットで公開しているヘリコプターの「運航の手引き」の中に、実際の救助事案の報告書を添付していたため、要救助者の個人情報がインターネット上に漏えいしました。該当者には、消防防災航空センターより状況を説明し、謝罪しました。また、インターネット上に残っていた個人情報のデータも削除されていることが確認できました。今後、同様な事案が起きないよう再発防止対策を講じて個人情報の適切な管理に努めます。

1 事案の概要

消防防災航空センターでは、災害発生時に効果的かつ安全に活動するための基本的事項を「運航の手引き」としてまとめ、ホームページで広く一般の方へ公開している。このうち「鳥取県消防防災ヘリコプター運航管理要綱」に実際の緊急運航時の報告書を添付していたため、要救助者の個人情報がインターネット上に漏えいした。

● 月例のセキュリティアップデート、Microsoft・Adobeからリリース

<https://forest.watch.impress.co.jp/docs/news/1599348.html>
<https://msrc.microsoft.com/blog/2024/06/202406-security-update/>
<https://forest.watch.impress.co.jp/docs/news/1599367.html>



このニュースをザックリ言うと…

- 6月12日(日本時間)、**マイクロソフト(以下・MS)**より、**Windows・Office等**同社製品に対する**月例のセキュリティアップデート**がリリースされています。
- **Windowsの最新バージョン**はWindows **10 22H2 KB5039211(ビルド 19045.4529)** および**11 23H2 KB5039212(ビルド 22631.3737)** となります。
- 同日には**Adobe社**からも**Photoshop・Creative Cloud等**に対する**セキュリティアップデート**がリリースされています。

AUS便りからの所感



- MSから今回発表された脆弱性では、**Microsoft Message Queuing(MSMQ)**に関する1件が最も深刻なものとされており、当該サービスが**有効となっている場合(デフォルトでは無効)は**早急なアップデートの適用が推奨されます。

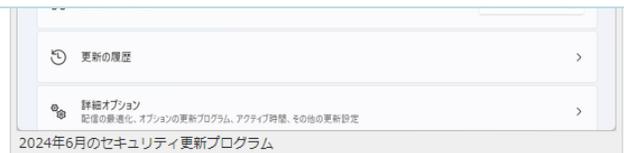
- 日本時間での**第2水曜日(1日が水曜日の場合は第3水曜日)**はMSをはじめとする**各社からのセキュリティアップデート発表が集中**、また**Oracle**からも**4半期毎にJavaやMySQL等のセキュリティアップデートがリリース**される(次回は7/17)ため、**運用している各種プロダクトについて定期的なアップデートのスケジュールが定まっているものを把握**しておくべきなのもありません。

- 今後発生し得る新たな攻撃に備え、**OSや機器のファームウェアあるいは各種アプリケーションに至るまで確実にアップデートを適用**すること、**それまでに発生する攻撃に対しアンチウイルス・UTM等による防壁策をとることが肝要**です。

2024年6月の「Windows Update」がリリース、「Critical」1件を含む49件の脆弱性に対処

「Windows 10 21H2」Enterprise/Educationエディションのサービスは今月が最後

樽井 秀人 2024年6月12日 09:36



米Microsoftは6月11日(現地時間)、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした(パッチチューズデー)。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで49件の脆弱性が新たに対処されている。