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。

●大学病院、メール誤送信により患者情報3,275人分流出の可能性

https://www.asahi.com/articles/ASM8561RKM85ULOB017.html
https://www.tokyo-np.co.jp/article/kanagawa/list/201908/CK2019080602000150.html

このニュースをザックリ言うと･･･

- 8月5日（日本時間）、横浜市立大学附属病院より、臨床研究に用いる膀胱がん患者3,275人分の個人情報について、メールの誤送信により流出した可能性があると発表されました。

- 個人情報は、同病院を含む神奈川県内20病院で2010～2014年に膀胱がんの手術を受けた患者の氏名・生年月日・性別・初回手術日・手術後の治療および再発の有無等、センシティブな情報を含む約70項目が含まれていたとのことです。

- 同病院の医師が7月24日に協力病院等の医師22人に対し症例データをメールで送信した際、13人分のメールアドレスを間違え、うち11人分はエラーで戻ってきたものの、残る2人分に対し送信された可能性があるとのことです。

AUS便りからの所感等

- 同病院による研究計画書では、症例のデータは匿名とし、協力病院とデータをやり取りする際は直接届けるか郵送することになっていましたが、遵守されておらず、やはりルール違反であるメール（かつフリーメールサービス）を用いてやり取りする体制が常態化していたとのことです。

- 照合作業が煩雑になるという理由で患者データの匿名化を行わないようになったこと、あるいはデータの暗号化を行っていなかったことを含め、様々な運用上の問題が重なって発生した事例と言える一方、データの共有手段が不便なものに限定されたことにより、逆に安全でない手段が密かに導入された可能性も見過ごせないものがあります。

- 一般的なデータ共有についての話とはなりますが、多数のメールアドレスをメーラーに入力して送信するやり方に代えてメーリングリストを用意する、その他メールの暗号化や誤送信防止等を自動的に行うソリューションを採用する、場合によってはデータ共有のためにオンラインストレージを用意する等、安全性を最優先としつつも利便性も確保し得る手段を検討し、それらが十分な説明・周知のもとに正式に採用されることが最も望ましいと言えるでしょう。

朝日新聞 DIGITAL

匿名化せず病歴をメールで…横浜市大病院、ずさんな扱い

有料記事
2019年8月6日14時01分

記者会見する二見良之・横浜市立大学理事長（左から２人目）、相原道子・同大学付属病院長（左）ら＝横浜市役所

横浜市立大学 付属病院が５日、臨床研究に用いる膀胱（ぼうこう）がんの患者３２７５人の個人情報をメールの誤送信で漏洩（ろうえい）させたと発表した。市立大病院を含む 神奈川県 内の２０病院で手術を受けた患者のデータで、個人情報をずさんに扱っていた実態が浮かんだ。

がん患者３２７５人の個人情報を誤送信　横浜市大病院

市立大病院によると、泌尿器科の４０代の男性医師が７月２４日、市立大病院と、臨床研究に協力する県内１９病院の医師ら２２人に送信しようとしたが、１３人分のアドレスが間違っていた。うち１１のアドレスに送ったメールは届かずに戻ったが、二つのアドレスに送ったメールは戻らず、病院側は返信を依頼したものの５日時点で反応はないという。

東京新聞

横浜市大病院　患者情報流出　協力医師、全員が同じ医局出身

ツイート　B! 5　シェア 84　　2019年8月6日

横浜市立大病院の医師が日頃からデータの受け渡し究計画違反だが、取材で研だったことが分かった。内

市立大病院によると、個十五人、性別不明が二人だ

研究は効果的な手術と治療を明らかにするため二〇一二年に始まった。研究グループは二十病院から、一〇～一四年にぼうこうがんの手術をした患者の氏名、性別、生年月日、がんの深刻度、生活習慣、手術後の治療など七十一項目のデータを取得。その後も毎年、術後の経過を更新するためデータを受けとっていた。

同病院の研究倫理委員会が国の倫理指針に基づき承認した研究計画では、データは匿名にし、更新時の受け渡しは手渡しか郵送と定めていた。しかし、研究グループは当初からデータの受け渡しにメールを使用。さらに研究グループが一五年ごろ、患者の氏名を記載したデータを送るよう依頼して全ての病院が応じ、匿名にする運用も途絶えた。

国の倫理指針では、他の病院に患者データを送る際は匿名化するか、各病院の倫理委の許可などを得る必要がある。協力した多くの病院はこの手続きを取らず、指針に違反していた。医師がフリーメールで情報の送信をしたため、協力していることすら知らなかった病院も複数あった。

メールを誤送信した四十代男性医師は市立大病院の聞き取りに「匿名だとデータの照合に時間がかかるため氏名の記載を依頼した」と話したという。百七十五件のデータを提供した藤沢市民病院の担当者は「医師同士が知り合いだとしてもルールとしてダメだと断るべきだった」と語った。

各病院は五日、対象の患者に謝罪文を送付するなどの対応を取った。厚生労働省は六日以降、市立大病院の情報管理を調査し、具体的な問題が見つかれば指導する。相原道子院長は「再発防止に向けて取り組む」と話した。

●Microsoft、「BlueKeep同様に危険」なリモートデスクトップサービスの脆弱性修正の早期適用を呼び掛け

https://www.itmedia.co.jp/news/articles/1908/14/news059.html

このニュースをザックリ言うと･･･

- 8月14日（日本時間）、マイクロソフト（以下MS）より、8月度の月例セキュリティパッチが公開されました。
- 例によって影響するプロダクトはWindows・IE・Edge・Office等広範囲に及びますが、特にWindows 7（およびWindows Server 2008 R2）以降のリモートデスクトップサービス（RDS）の脆弱性（CVE-2019-1181, CVE-2019-1182）について、これを悪用する攻撃が今後大規模に行われる恐れがあるとして、早急なパッチの適用を呼びかけています。

AUS便りからの所感等

- RDSについては、5月にもWindows7以前において「BlueKeep」と呼ばれる脆弱性が発見され、大規模な攻撃につながることが懸念されたことから、サポートが終了したXPに対してもパッチが提供される事態となっています（AUS便り 2019/05/20号参照）。
- 脆弱性の悪用以外にも、外部からRDSにログインし、マルウェアを送り込もうとする等の攻撃のため、RDSのサービスポート（TCP/UDPポート3389番）へのアクセスが頻繁に確認されています。
- MSでは根本的対策として、全てのケースにおいてパッチの適用を強く推奨している一方、他の攻撃の可能性も含めた回避策として、RDSが必要でない場合は無効にすること、サービスポートへのアクセスをファイアウォールやUTMでブロックすること等を回避策として挙げています。

●WebサーバへのDoS攻撃の可能性…Apache、Nginx等修正パッチ公開

http://jvn.jp/vu/JVNVU98433488/index.html

このニュースをザックリ言うと･･･

- 8月14日（日本時間）、大手動画サービスNetflixの技術者より、WebサーバのHTTP/2プロトコルの処理においてDoS攻撃の可能性がある脆弱性（CVE-2019-9511～CVE-2019-9518）が存在すると発表されました。
- 脆弱性の悪用により、HTTP/2をサポートするWebサーバが応答不能状態に陥る可能性があるとされています。
- 米CERT/CCおよびIPA・JPCERT/CC等からも相次いで同様の発表があり、同時に関連するプロダクトについて、各ベンダーから脆弱性を修正するパッチがリリースされています（Apache 2.4.41、Nginx 1.16.1・1.17.3およびマイクロソフト8月度月例パッチ等）。

AUS便りからの所感等

- HTTP/2は、従来のHTTP/1.1における問題点を解決し、モバイル環境等でも最適な通信を行えるよう設計されたプロトコルで、比較的新しいWebブラウザ（Chrome・Edge・Firefoxは対応、IE11は非対応）とサーバが対応しています。
- 脆弱性そのものは必ずしも致命的なものとは限らないようですが、攻撃手法が確立し、HTTP/2をサポートするWebサーバの数次第では見過ごせない影響が出ることも十分考えられます。
- WebサーバにおいてHTTP/2が有効になっているかは、Webブラウザ（同様にHTTP/2に対応している必要があります）の開発者コンソールを開いた状態でサーバにアクセスすることにより確認できますので、その上でパッチが適用されるまでは、設定により一時無効にすることも検討に値するでしょう。