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。

●「Googleグループ」アクセス制限設定に不備、個人情報10,307件が閲覧可能状態に

https://www.itmedia.co.jp/news/articles/2506/18/news086.html
https://www.daiso-sangyo.co.jp/wp-content/uploads/2025/06/42c327021022154ac3ee5aa42ac101b5.pdf
https://www3.nhk.or.jp/news/html/20250417/k10014781801000.html
https://www.lac.co.jp/archive/20130710_000166.html

このニュースをザックリ言うと･･･

- 6月18日(日本時間)、100円ショップ「ダイソー」運営元の大創産業社より、同社が内外でやり取りしたメールの一部情報が外部から閲覧可能な状態にあったと発表されました。

- 対象となるのは、同社ECサイト利用者4,498件、取引先4,578件、中途採用応募者698件および従業員533件、併せて10,307件の氏名・住所・電話番号・メールアドレス等となっています。

- メールのやり取りや管理を行っていた「Googleグループ」が2019年12月9日以降公開設定となっており、外部から指摘を受け今年4月26日に非公開設定を行ったとしています。

AUS便りからの所感等

- Googleグループにおける会話の閲覧・グループの検索への公開設定について、以前は「(ウェブ上の)すべてのユーザー」に公開される設定が作成時のデフォルトであった模様で、2013年にラック社が注意喚起を行った経緯があります。

- 現在、作成時のデフォルト設定は「メンバーのみ可能」とされているもの、最近でも4月17日にNHKのニュースにおいて公開設定となっているグループが多くみられることが取り上げられており、今回の事例もニュースを見た第三者が公開されているグループの検索を行ったことで発見された可能性も考えられます。

- 同じくGoogleが提供するGoogleドライブ等、およびその他が提供するクラウドサービスを利用している場面において、公開設定の点検を行い、第三者からの閲覧を意図していない領域については必ず非公開ないし検索されない設定とするよう心掛けてください(加えて同社が行ったような、公開状態で作成できないようにする等の設定も可能な限り実施しましょう)。

ITmedia NEWS

ダイソー、1万件超の個人情報漏えいか　約5年間外部から閲覧可能に　「Googleグループ」の閲覧権限に不備

2025年06月18日 13時35分 公開　[ITmedia]

100円ショップ「ダイソー」を運営する大創産業（広島県東広島市）は6月18日、顧客や取引先、従業員などの個人情報計1万307件に漏えいの可能性があると発表した。同社が利用していた掲示板／メーリングリストサービス「Googleグループ」の設定不備により、2019年12月9日から5年超もの間、外部から閲覧可能となっていた。

閲覧権限に不備があったのは、同社が管理していた57グループ。いずれも登録された関係者限定で利用すべき情報だったが、外部からもアクセスできる設定となっていた。

閲覧可能だった情報は氏名、住所、電話番号、メールアドレスなど。内訳は、同社ECサイトの利用者4498件（うち口座情報49件）、取引先4578件、中途採用の応募者698件（うち履歴書・職務経歴書など615件）、従業員533件（うち健康保険証149件、要配慮個人情報4件を含む）。

●損保ジャパン、個人情報等最大1,750万件流出の可能性…4月の不正アクセスで

https://www3.nhk.or.jp/news/html/20250611/k10014832171000.html
https://www.sompo-hd.com/-/media/hd/files/news/2025/20250611_1.pdf

このニュースをザックリ言うと･･･

－6月11日(日本時間)、損害保険ジャパン社より、社内システムが外部から不正アクセスを受け、大規模な情報流出が発生した可能性があると発表されました。

－対象となるのは、同社顧客関連のデータ(氏名・連絡先・証券番号等)約726万件、代理店関連のデータ約178万件、その他証券番号・事故番号のみのデータ(同社データベースと照合しなければ個人を特定できないとのこと)約844万件、合わせて約1,748万件とされています。

－4月17日～21日にかけて、同社Webシステムに不正アクセスがあったことが原因としており、被害を受けた情報の不正利用の事実は現在確認されていないとのことです。

AUS便りからの所感

－4月25日に不正アクセスの初報があり、今回の続報で被害状況の詳細が発表されたもので、これまでの不正アクセスによる情報流出事案の中でも突出した規模の被害となっています。

－侵入経路については未発表であり、今後の続報待ちとみられますが、再発防止策において「他システムに同様の脆弱性がないこと」の確認等を挙げており、何らかの脆弱性を突かれて不正アクセスに至った可能性が考えられます。

－外部公開システムから、社内ネットワークからのみアクセス可能なサーバー・ネットワーク機器、およびクライアントPCに至るまで全てのシステムにおいてOS等を最新に保ち、アンチウイルス・UTM等による防御、また不正アクセスやその兆候を早々に検知するシステムの導入等、情報流出を食い止める各種ソリューションの導入を強く推奨致します。

●5月度フィッシング報告件数は229,536件、3か月連続の20万件超

https://www.antiphishing.jp/report/monthly/202505.html

このニュースをザックリ言うと･･･

－6月20日(日本時間)、フィッシング対策協議会より、5月に寄せられたフィッシング報告状況が発表されました。

－5月度の報告件数は229,536件で、4月度(https://www.antiphishing.jp/report/monthly/202504.html)の246,580件から17,044件減少しています。

－フィッシングサイトのURL件数は55,940件で4月度(48,373件)から7,567件増加、使用されるTLD(トップレベルドメイン名)の割合が多かったのは .com(約25.5%)、.goog(約24.8%)、.asia(約23.1%)、.cn(約8.0%) .net(約4.4%)、.jp(約4.4%)で、この6つで約90.1%を占めています。

－悪用されたブランド件数は91件で4月度(100件)から9件減少、割合が多かったのはSBI証券(約23.3%)、Apple(約13.3%)、Amazon(約6.8%)で、次いで1万件以上報告されたANA、野村證券、VISAと合わせて約59.3%、さらに1,000件以上報告された31ブランドまで含めると約95.4%を占めたとのことです。

AUS便りからの所感

－過去最多の報告件数となった3月度以降、減少は続いているものの緩やかで、3か月連続で20万件超を記録しています。

－フィッシングサイトのTLDは長らく.comと並んで多数を占めていた.cnが急減し、代わりに.googと.asiaが急増しています。

－同協議会からは6月3日に2024年におけるフィッシングの被害状況、フィッシングの攻撃技術・手法などをとりまとめた「フィッシングレポート2025」および「フィッシング対策ガイドライン」の改訂版が発表されており、2024年に大手メールサービスからの推奨に伴い導入が進んだ各種対策について適切に運用されているか等の確認を推奨致します。