身を守るには
知ることから！

社内回覧用

情報セキュリティ被害の最新事例
2025年5月版

【大切なお願い】
会社を守るため、社長様、幹部様、従業員様、
パソコンやスマホを利用する**皆さまに回覧ください。**
自分事で実態を知ることが対策の第一歩です。

【この冊子の活用の仕方】
この冊子では、セキュリティの最新情報を月刊で
お伝えしています。被害事例を**自社に置き換えて、**
対策と意識向上にお役立てください。

BASIC Confertas Office

■PR TIMESが不正アクセス被害　最大90万件以上の個人情報流出の可能性

2025年5月8日

- PR TIMESがサーバ侵害を受け、最大90万件以上の個人情報流出の可能性を明らかにした
- IP制限や多要素認証をすり抜ける高度な手口による攻撃であり偵察・侵入・バックドア設置など計画的なサイバー攻撃だった
- 流出した情報には氏名や企業名、部署名、電話番号、メールアドレスのほか、利用者に関してはハッシュ化されたパスワードなども含まれる。

■画像：株式会社PR TIMESのホームページ

■出典：
https://scan.netsecurity.ne.jp/article/2025/04/30/52775.html

多要素認証やIP制限を突破された点からも、従来の防御策だけでは不十分であることが明らかです。システムやパスワード管理の定期見直しも怠らないよう徹底しましょう。

■偽警告にだまされ個人情報流出か やまがた農業支援センターで3万件超

2025年5月13日

- 職員が「ウイルス感染」の偽警告に騙され、遠隔操作アプリをインストールしたことが原因
- データが消去され、約3万2,000件分の個人情報が流出した可能性あり
- 対象は契約者の氏名・住所・口座情報など、正確な内容把握は依然困難な状況である

同様の被害を防ぐためには、職員への定期的なセキュリティ教育と訓練を実施し、正規サポートの見極め方や不審な画面の対処法を周知徹底することが必要です。また、業務端末へのアプリインストールを制限し、不審な挙動を検知できる仕組みの導入も検討してみてはいかがでしょうか。

■画像：やまがた農業支援センターのホームページ

■出典： https://www.yamagata-nogyo-sc.or.jp/

■日邦バルブがランサム攻撃で個人情報流出　防げたはずの“脆弱性”

2025年5月15日

- 2025年3月18日、ランサムウェアによりサーバーが暗号化され、メールや財務システムが一時使用不能に
- 原因はファイアウォールとウイルス対策ソフトの更新不備、従業員343名の個人情報が流出した
- お客様・取引先情報には被害なし、生産販売業務も通常通り

セキュリティ対策の“抜け穴”は狙われます。今後は更新漏れをなくす仕組みが重要となってきます。従業員情報も企業の責任範囲なので再度、履歴書や健診結果の保管ルールを見直しましょう。

■画像：ScanNetSecurityの該当ページ

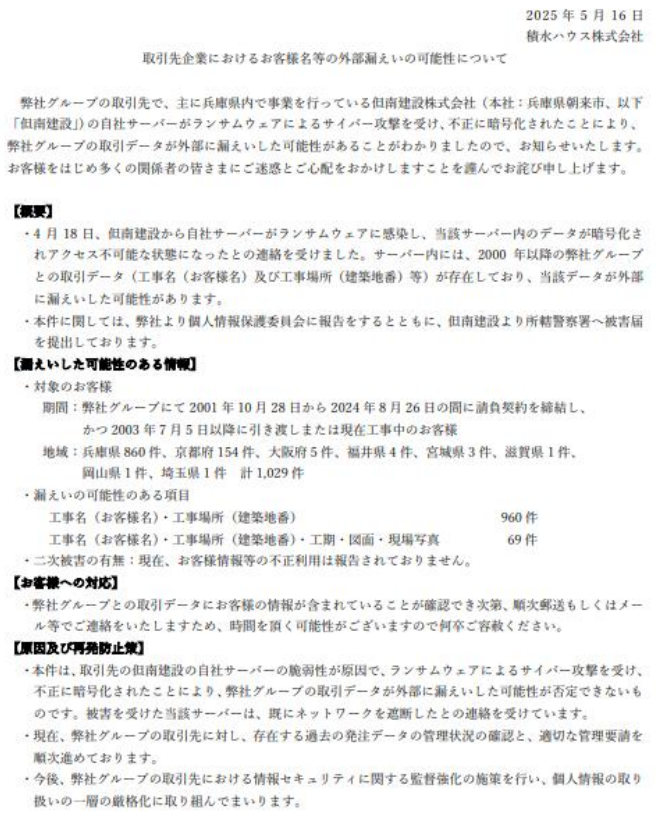
■出典： https://scan.netsecurity.ne.jp/article/2025/05/29/52944.html

■取引先から情報漏えい 積水ハウス関連で1,000件超 原因はランサム攻撃

2025年5月16日

- 但南建設のサーバーがランサムウェアに感染、積水ハウスグループの取引データが漏えいの可能性があると明らかにした
- 漏えい対象にはお客様名・建築地番など計1,029件、一部は図面や現場写真も含まれる
- 原因は取引先サーバーの脆弱性、積水ハウス側は再発防止策として取引先への管理強化を表明している

自社のセキュリティだけでなく、取引先の情報管理体制もリスク管理対象と考えましょう。委託先や協力会社に対しても、情報の暗号化やアクセス制限を明確に求めることが重要となります。万が一の漏えい時に備えて、情報の分類・最小化と迅速な連絡体制の整備を進めていきましょう。



2025 年 5 月 16 日
積水ハウス株式会社

取引先企業におけるお客様名等の外部漏えいの可能性について

弊社グループの取引先で、主に兵庫県内で事業を行っている但南建設株式会社（本社：兵庫県朝来市、以下「但南建設」）の自社サーバーがランサムウェアによるサイバー攻撃を受け、不正に暗号化されたことにより、弊社グループの取引データが外部に漏えいした可能性があることがわかりましたので、お知らせいたします。お客様をはじめ多くの関係者の皆さまにご迷惑とご心配をおかけしますことを謹んでお詫び申し上げます。

【概要】
・4 月 18 日、但南建設から自社サーバーがランサムウェアに感染し、当該サーバー内のデータが暗号化されアクセス不可能な状態になったとの連絡を受けました。サーバー内には、2000 年以降の弊社グループとの取引データ（工事名（お客様名）及び工事場所（建築地番）等）が存在しており、当該データが外部に漏えいした可能性があります。
・本件に関しては、弊社より個人情報保護委員会に報告をするとともに、但南建設より所轄警察署へ被害届を提出しております。

【漏えいした可能性のある情報】
・対象のお客様
期間：弊社グループにて 2001 年 10 月 28 日から 2024 年 8 月 26 日の間に請負契約を締結し、かつ 2003 年 7 月 5 日以降に引き渡しまたは現在工事中のお客様
地域：兵庫県 860 件、京都府 154 件、大阪府 5 件、福井県 4 件、宮城県 3 件、滋賀県 1 件、岡山県 1 件、埼玉県 1 件　計 1,029 件
・漏えいの可能性のある項目
工事名（お客様名）・工事場所（建築地番）　960 件
工事名（お客様名）・工事場所（建築地番）・工期・図面・現場写真　69 件
・二次被害の有無：現在、お客様情報等の不正利用は報告されておりません。

【お客様への対応】
・弊社グループとの取引データにお客様の情報が含まれていることが確認でき次第、順次郵送もしくはメール等でご連絡をいたしますため、時間を頂く可能性がございますので何卒ご容赦ください。

【原因及び再発防止策】
・本件は、取引先の但南建設の自社サーバーの脆弱性が原因で、ランサムウェアによるサイバー攻撃を受け、不正に暗号化されたことにより、弊社グループの取引データが外部に漏えいした可能性が否定できないものです。被害を受けた当該サーバーは、既にネットワークを遮断したとの連絡を受けています。
・現在、弊社グループの取引先に対し、存在する過去の発注データの管理状況の確認と、適切な管理要請を順次進めております。
・今後、弊社グループの取引先における情報セキュリティに関する監督強化の施策を行い、個人情報の取り扱いの一層の厳格化に取り組んでまいります。

■画像：積水ハウス株式会社のホームページ

■出典：https://www.sumirin-crest.co.jp/

■レゾナックがランサムウェア被害　被害拡大防止に着手中

2025年5月20日

- 2025年5月20日、レゾナックの一部サーバが外部からの攻撃を受けランサムウェアへ感染したことが明らかになった
- これに対し緊急対策本部を設置し、ネットワーク遮断など被害拡大防止に着手している
- 業績への影響を含め、調査と復旧作業が現在も進行中である

ランサムウェアは大企業だけの問題ではなく、中小企業も標的になります。定期的なバックアップとネットワーク分離の見直しが重要です。万一に備えて、緊急時の対応手順を整えておきましょう。

RESONAC
Chemistry for Change

Global

HOME > ニュースリリース > 2025 > 弊社にて発生したセキュリティインシデントについて（第一報）

弊社にて発生したセキュリティインシデントについて（第一報）

その他

2025年05月20日
株式会社レゾナック・ホールディングス

本日5月20日、株式会社レゾナックの一部サーバー等に対して、外部から攻撃を受けたセキュリティインシデントが発生したことをお知らせします。
本件について、緊急対策本部を設置し、影響範囲等の調査と復旧への対応を進めております。
被害の全容を把握するには、今しばらく時間を要する見込みですが、現時点で判明している内容について、下記の通りご報告いたします。
お取引様、関係先の皆様に多大なるご心配とご迷惑をおかけすることになり、深くお詫び申し上げます

記

１．　経緯
5月20日（火）に、当社の一部サーバーに対して、外部からの攻撃が確認され、ランサムウェアの感染が確認されました。直ちに、外部専門家の協力のもと調査を開始し、迅速に対応を進めるべく緊急対策本部を立ち上げました。

２．　現在の状況と今後の対応
15時30分現在、被害の拡大を防ぐための対応を進めており、ネットワークの遮断等の措置を行っております。システムの保護と復旧に向けて作業を進め、皆様へのご迷惑を最小限に止めるべく取り組んでまいります。
なお、本件による業績への影響については精査中であり、今後の業績に重大な影響が認められる場合には速やかに公表いたします。

■画像：レゾナック株式会社のホームページ上のお知らせ

■出典： https://www.resonac.com/jp/news/2025/05/20/3510.html

■OS更新時のミスで個人情報公開 茨城県で発覚

2025年5月30日

- サーバOS更新中にテスト出力された個人情報ファイルが外部公開状態に
- 最大264回の閲覧ログあり、氏名・住所・電話番号など150件程度が含まれる
- 原因は委託先の確認漏れであるとし、再発防止策として定期点検と報告体制を強化している

この事例は、委託先管理の不備により個人情報が漏えいした典型例です。再発防止には、外部委託先への明確な管理基準の徹底と、定期的な情報公開状況の点検が不可欠です。

Security NEXT

Security NEXTでは、最新の情報セキュリティに関するニュースを日刊でお届けしています。

ニュース | 政府・業界動向 | 脆弱性 | 製品・サービス | コラム

OS更新作業中にテスト出力した個人情報ファイルを外部公開 - 茨城県

茨城県は、広聴情報共有化システムにおいて、一時的に作成した個人情報を含むテストファイルが、サーバ上で外部に公開されていたことを明らかにした。

同県によれば、同県に寄せられた意見を記録し、データベースとして活用するための「広聴情報共有化システム」において、出力テストにより個人情報を含むファイルを一時的に作成したが、誤ってそのまま外部に公開されていた。

5月8日に外部からメールで指摘があり問題が発覚。2022年7月に受け付けた県民相談など、氏名86件、住所53件、電話番号4件、メールアドレス2件が含まれる。

同日、同県では公開サーバから対象ファイルを削除した。同サーバにおける

■画像：SecurityNextの該当ページ

■出典： https://www.security-next.com/170478

情報セキュリティ対策は、実績豊富で信頼できる企業をお選びください。

最近は、ランサムウェアや情報漏えいなど、経営に関わるサイバー攻撃の被害も増加し、ひとつの社会問題となっています。私たちは、「サイバー攻撃の脅威からお客様を守りたい」そして、「今後もお客様と一緒に永く成長していきたい」と強く思っています。

情報セキュリティは、社内ネットワークに関わる重要な部分であり、信頼できる会社と付き合うことが大切です。私たちは、お客様に正確な情報と知識、安心の技術サポートを提供できる体制を整えていますので、ぜひご安心ください。