不正アクセスによる被害事例

株式会社サンエイ

不正アクセスによる被害状況

不正アクセスによる 被害事例 一覧

2022年にサイバー攻撃被害を公表した企業のうち、従業員数400名未満の企業

企業名	種別	漏洩件数	従業員数
株式会社スタイリッシュ・エイチ・アンド・エイ	通販	18,000件	120名
株式会社フルノシステムズ	業務	1,068件	140名
ジェントス株式会社	通販	5,521件	88名
株式会社akaran	通販	8,483件	17名
山陽SC開発株式会社	業務	7,950件	54名
株式会社ランドマーク	通販	63,565件	20名
株式会社テツコーポレーション	業務	1,525件	35名
株式会社世界堂	通販	約18万件	287名
株式会社アットキャド	業務	21,751件	312名
クリーンテックス・ジャパン株式会社	業務	40,600件	86名
カメイ・プロアクト株式会社	通販	5,172件	63名
株式会社SODA	通販	約275万件	300名
株式会社誠和	通販	5,548件	183名
井上商事株式会社	通販	7,645件	230名
月桂冠株式会社	業務	約2.7万件	365名

企業名	種別	漏洩件数	従業員数
中央教育研究所株式会社	通販	2,270件	63名
株式会社ほくせん	通販	44,559件	119名
宇都宮ケーブルテレビ株式会社	通販	1,053件	49名
京都駅ビル開発株式会社	業務	4,650件	45名
株式会社FLYWAY	通販	2,763件	11名
株式会社デジタ	通販	21,042件	155名
ビーズ株式会社	業務	23,435件	65名
オカ株式会社	通販	7,086件	93名
株式会社日能研	会員	約28万件	346名
ビバリーグレンラボラトリーズ株式会社	通販	46,702件	66名
株式会社ジェック	業務	約2万件	80名
株式会社マルカン	通販	1,152件	367名
株式会社石橋楽器店	通販	98,635件	334名

出典：過去の個人情報漏洩事件まとめ／サイバーセキュリティ.com より対象企業を抜粋

不正アクセスによる 被害事例１

学校・学習塾向け教材の開発・販売を行う企業（広島市／従業員数：63名）

不正アクセス調査のため、70日間のサイト停止

学校・学習塾向け教材の開発・販売を行う企業（広島市／従業員数：63名）が運営する、進学塾・教師用教材 販売サイトが第三者による不正アクセスを受け、クレジットカード決済を行った利用者 2,270名のクレジットカード情報（カード名義人名、クレジットカード番号、有効期限、セキュリティコード）2,930件が漏洩した可能性があることを公表しました。

【クレジットカードの再発行手数料負担（試算）】

約2,000円/件×2,930件＝**約586万円**

- 漏洩したクレジットカードの差替えに掛かる手数料について、90%以上の事業者が費用を負担
- 差替えに伴う費用は、1件あたり約2,000円との回答が60%を占める

（ECサイトへの不正アクセスに関する実態調査／IPA）

https://www.chuoh-kyouiku.com/news/security.html

https://security.sanei-fcg.com/?post_type=casestudy&p=578

すべての既存会員へお詫びクーポンを配布

通販サイトの一時閉鎖に伴うお詫びとして、すべての既存会員へ500円割引クーポン（総額 113万円以上）の配布を公表しました。

【支出試算】

500円/名×2,270名＝**113万円以上**

通販システムの脆弱性が狙われた事例

公表内容には「弊社が運営する当該サイトのシステムの一部の脆弱性を突いたことによる第三者の不正アクセスにより、ペイメントアプリケーションの改ざんが行われたため」とあり、通販システムに内在する脆弱性が狙われたものと推測されます。

不正アクセスによる 被害事例２

公立大学法人（富山県／職員数：211名）

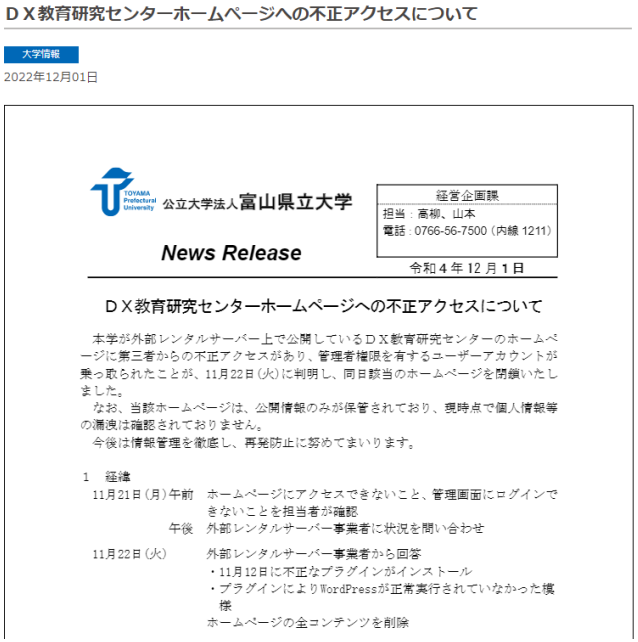
不正アクセスによる乗っ取り、全データ削除＆Webサイト閉鎖

公立大学法人（富山県／職員数：211名）が運営する施設案内サイトが不正アクセスにより管理者権限を乗っ取られ、Webサイトを閉鎖したことを公表しました。

迷惑メールの送信サーバーとして利用された痕跡

公表内容には「迷惑行為としてメール送信の痕跡を確認」「現時点で個人情報の漏洩は確認されておりません。」とあり、迷惑メールの送信サーバーとして利用された模様です。

迷惑メールの送信サーバーとして利用された場合、サーバーがブラックリストに指定されてしまい、正規のメールを相手先が受信できなくなる可能性があります。



ＤＸ教育研究センターホームページへの不正アクセスについて

大学情報

2022年12月01日

公立大学法人富山県立大学

経営企画課
担当：高柳、山本
電話：0766-56-7500（内線 1211）

News Release

令和４年 12 月１日

ＤＸ教育研究センターホームページへの不正アクセスについて

本学が外部レンタルサーバー上で公開しているＤＸ教育研究センターのホームページに第三者からの不正アクセスがあり、管理者権限を有するユーザーアカウントが乗っ取られたことが、11月22日(火)に判明し、同日該当のホームページを閉鎖いたしました。
なお、当該ホームページは、公開情報のみが保管されており、現時点で個人情報等の漏洩は確認されておりません。
今後は情報管理を徹底し、再発防止に努めてまいります。

1　経緯
11月21日(月)午前　ホームページにアクセスできないこと、管理画面にログインできないことを担当者が確認
午後　外部レンタルサーバー事業者に状況を問い合わせ
11月22日(火)　外部レンタルサーバー事業者から回答
・11月12日に不正なプラグインがインストール
・プラグインによりWordPressが正常実行されていなかった模様
ホームページの全コンテンツを削除

https://www.pu-toyama.ac.jp/news/news_outline/2022/12/01/15392/
https://security.sanei-fcg.com/?post_type=casestudy&p=767

ワードプレスの被害事例

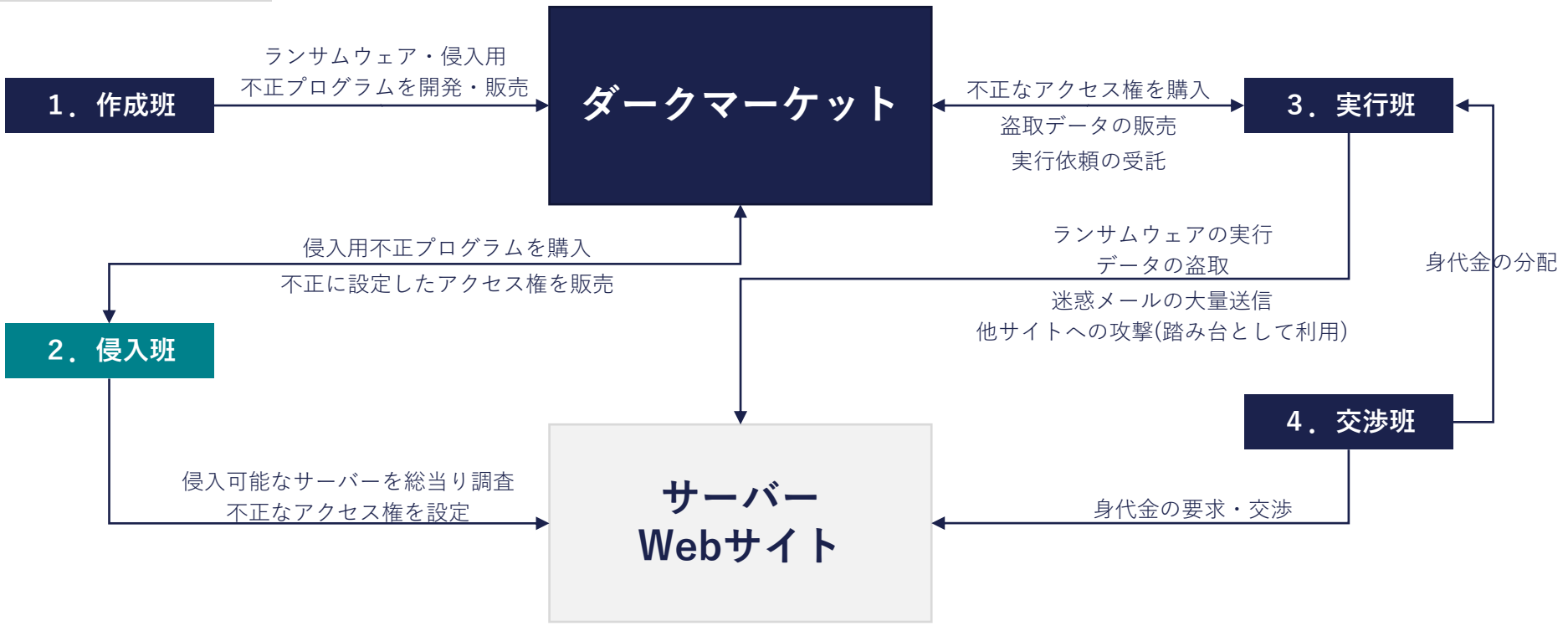
公表内容には「11月12日に不正なプラグインがインストール」「プラグインにより WordPressが正常実行されていなかった模様」とあり、更新管理システムにWordPress（ワードプレス）が使われていたことが確認できます。導入のしやすさ、扱いやすさの面から世界的に広く普及（シェア：約40%）している更新管理システムである反面、攻撃の標的になりやすく、特にセキュリティ対策が欠かせないシステムです。

組織の規模に関わらず被害発生、なぜか？

組織の規模に関わらず、被害が生じる背景

サイバー攻撃は、分業化されている

サイバー攻撃 分業モデル



出典：サイバー攻撃、進む分業　「侵入口」100ドルで闇取引／日本経済新聞
マルウェア、ランサムウェア、ダークウェブ　驚異のサイバー犯罪最前線／Forbes JAPAN

侵入班は、侵入可能なサーバーを無作為に調査するため、**攻撃の実施に組織の規模は無関係**

組織の規模に関わらず、被害が生じる背景

各グループの役割

1．作成班
- シェアの高いソフトウェア（ワードプレス、php、Apache等）の脆弱性を悪用して侵入する不正なプログラムを開発
- 不正プログラムをダークマーケット上で販売し利益を得る
- 脆弱性を調査する自動プログラム（ボット）を開発、ダークマーケット上で販売利益を得る

2．侵入班
- インターネット上で稼働するサーバー/Webサイトを対象に、**自動プログラム等により無作為に脆弱性を調査**
- 調査に必要な自動プログラムはダークマーケット上で調達
- 脆弱性のあるサーバー/Webサイトに不正アクセスを行い、外部から制御可能な状態を設定
- **制御可能なアクセス権をダークマーケット上で販売**し利益を得る

▶ 侵入できれば
標的はどこでもよい

3．実行班
- 侵入班から購入したアクセス権を利用して不正アクセスを行う
- サーバー内に格納されているデータの盗取、ランサムウェアによる暗号化等の侵害行為を実施
- 同時に、接続されているネットワーク内を水平移動し、さらなる感染拡大を試みる
- 交渉班が獲得した身代金の分配金、ダークマーケット上での依頼報酬により利益を得る
- 盗取したデータに価値があれば、ダークマーケット上で販売し利益を得る

4．交渉班
- 実行班が攻撃した被害者組織と身代金支払いの交渉を行う
- 獲得した身代金の一部は侵害実行班の分配金に充当される

ご相談 受付中

お問い合わせ

https://sanei-fcg.hubspotpagebuilder.com/cloudflare/

- 自社ホームページのセキュリティが気になる方
- 自社ホームページに脆弱性が無いか確認したい方
- 自社ホームページの表示速度が遅いので改善したい方
- サイバー保険について知りたい方

通販サイト、Webサイトのセキュリティについて、ご相談承っております。
お気軽にお問い合わせ、ご相談ください。