令和５年４月

国土交通省不動産・建設経済局参事官付

個人データ漏えいに係る対応について
（住宅宿泊管理業者）

個人情報保護法第２６条第１項に基づく個人データの漏えい等の報告のうち、施行規則第７条第３号に規定する「不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態」として、不正アクセスにより個人データが漏えいした場合やランサムウェア等により個人データが暗号化され復元できなくなった場合等のサイバー攻撃・サイバー犯罪によるものの報告を行った場合には、管轄地方整備局等へのご報告（※）に合わせ、警察へ通報・相談いただくとともに、独立行政法人情報処理推進機構のコンピュータウイルス・不正アクセスに関する届出に御協力いただきますようお願い申し上げます。

警察への通報・ご相談窓口及び届出制度の詳細につきましては、個人情報保護委員会にて、別添リーフレット等が作成されておりますので、ご確認ください。（次ページ以降をご覧ください。）

※住宅宿泊管理業者については、個人情報保護委員会の権限が国土交通大臣に委任されています。個人情報保護法の詳細は、個人情報保護委員会のホームページをご覧ください。

以　上

企業の皆様へ サイバー犯罪の被害は警察へ通報を!

社会のデジタル化の進展に伴い、業務に関するデータをオンラインで取り扱う機会が増加する中、企業を標的にしたサイバー犯罪も発生しています。

サイバー犯罪による深刻な被害

ランサムウェア

「ランサムウェア」と呼ばれるコンピュータウイルスに感染すると、パソコンやサーバに保存している**データが暗号化**され使用できなくなり、**データを復元する対価として金銭を要求**される。

さらには、データを盗み取った上、**「対価を支払わなければデータを公開する」などと金銭を要求**するダブルエクストーション(二重恐喝)という手口も発生している。

不正アクセスやコンピュータウイルスによる情報漏えい

パスワード管理の甘さやシステムの脆弱性を悪用して企業のネットワークに侵入するなどの不正アクセス、業務に関連するメールを装って送付されたメールの添付ファイルを開いたことによるコンピュータウイルスへの感染等により、**個人情報や機密情報が盗み取られる。**

テレワーク環境を狙った攻撃も発生している。

サイバー犯罪の実態を明らかにし、被害を拡大させないためには、**被害を潜在化させない**ことが重要です。

このような被害にあわれたら、**最寄りの警察署**または**都道府県警察本部のサイバー犯罪相談窓口**へ

警察では、サイバー犯罪に対する様々な対策を行っています

警察へ寄せられたサイバー犯罪に関する情報を分析し、**事件捜査**を行うほか、**被害企業における対策に必要な情報の提供・助言、他の企業等への被害拡大を防止するための注意喚起**等の被害防止のための取組を行っています。

企業の皆様からの情報提供がサイバー空間の安全につながります

サイバー犯罪に関する情報の分析

サイバー犯罪事件の捜査

被害の拡大防止・再発防止

警察庁 National Police Agency

都道府県警察本部のサイバー犯罪相談窓口はこちら⇒
https://www.npa.go.jp/bureau/cyber/soudan.html

サイバー犯罪被害に遭った場合は警察への通報・相談を！！

警察では、事件捜査に加えて、被害企業等の被害拡大防止や捜査で判明した犯罪の手口等を活用し、さらなる被害の未然防止等の取組を行っています。

サイバー事案が発生した際は、早期の警察への通報・相談をお願いします！！

どんなときに、どこに通報・相談すれば良いですか？

ランサムウェア被害や不正アクセス等による情報漏えい被害等に遭った際に、**最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口に通報・相談**してください。

都道府県警察本部のサイバー犯罪相談窓口はこちら⇒
https://www.npa.go.jp/bureau/cyber/soudan.html

通報・相談したら、どんな対応をしてもらえるのですか？

警察では、通報・相談を受け、全国警察で保有している高度な知見等を基に、事件捜査に加えて、

① 被害企業の**被害拡大防止対策に必要な情報の提供、助言**
② 被害企業の**被害の復旧への貢献**
③ **他の企業等の被害未然防止**のための取組

等を行っています。

捜査をすることで被害復旧に影響はないのですか？

警察では、**被害企業の意向を最大限尊重**し、業務への影響が最小限となるよう**早期の被害復旧等に配慮した捜査**を行っています。例えば、最初はログの保全等の必要最小限の措置をお願いし、ある程度落ち着いてから聴取を行うなどしています。

どんな情報を提供する必要があるのですか？

事案に応じて様々なものが考えられますが、例えば、被疑者の追跡・特定に必要不可欠な**通信ログ・アクセスログ、不正プログラム等の被害サーバ等に記録された情報、システム構成図等**が挙げられます。

警察庁 National Police Agency

ランサムウェア対策、不正アクセス対策等のほか、サイバー事案に関する相談対応等を掲載しています。⇒ https://www.npa.go.jp/ bureau/cyber/index.html

コンピュータウイルス・不正アクセスに関する届出

2023年3月
独立行政法人情報処理推進機構

●届出制度について

◆ 通商産業省（現経済産業省）が告示した「**コンピュータウイルス対策基準**」、「**コンピュータ不正アクセス対策基準**」に基づき、IPAでは国内のコンピュータウイルスの感染被害や不正アクセス被害の届出を受け付けています。

◆ ウイルス感染被害の拡大や再発の防止、不正アクセス被害の実態把握や同様の被害発生の防止に役立てるため、届出にご協力をお願いします。

●届出方法について

◆ 届出をご提出いただくにあたり、被害内容に応じた**届出様式**をウェブページ上にご用意しています。ご記入の上、指定の届出先にメールをご送付ください。

◆ 攻撃等が未遂で**実被害が生じなかった場合も**、被害の拡大や再発の防止に活用させていただきたいため、届出にご協力をお願いします。

◆ 届出する内容が様式にそぐわない場合は**フリーフォーマットによる届出**でも受け付けています。既にIPA以外の組織等へ報告・届出等を行っている場合は、その様式で届出いただいても構いません。

◆ 記入の難しい項目がある場合は、**お分かりになる範囲での記入**に留めていただいても構いません。届出の後に新たに判明した事項などがございましたら、追加でご連絡をお願いします。

●届出内容の公開について

◆ 届出いただいた情報については、ウイルスや不正アクセスによる被害の分析に活用させていただくとともに、国内の被害状況の把握や防止策の啓発を目的とし、届出者が特定されない形で、集計情報や事例情報として公表させていただく場合があります。

どういう時にどの届出を提出すればいいの？

2023年3月
独立行政法人情報処理推進機構

「コンピュータウイルス・不正アクセスに関する届出」については、次のウェブページで、くわしく説明しておりますのでご覧ください。

■コンピュータウイルス・不正アクセスに関する届出
https://www.ipa.go.jp/security/outline/todokede-j.html

●セキュリティソフトがウイルスを発見（検知）した

◆ セキュリティソフトでウイルスを検知したとのアラートが表示された。
パソコンやサーバ内に不審なファイルがあることを発見した。等

「ウイルス発見・感染の届出」をご覧いただき、次の届出先へご提出ください。

届出先：コンピュータウイルス届出窓口
E-Mail： virus@ipa.go.jp

●ファイルが暗号化されて、画面に脅迫文が表示された

◆ パソコンやサーバ等に保存していたファイルが突然開けなくなり、金銭を要求する内容が記載されたメッセージが残されていた。 等

「ランサムウェア被害の届出」をご覧いただき、次の届出先へご提出ください。

届出先：コンピュータウイルス届出窓口
E-Mail： virus@ipa.go.jp

●不正アクセスの被害や疑いがある事態が発生した

◆ 自組織のシステムやネットワークに何者かが不正に侵入した。
または、侵入を試みた形跡を確認した。 等

「不正アクセスの届出」をご覧いただき、次の届出先へご提出ください。

届出先：コンピュータ不正アクセス届出窓口
E-Mail： crack@ipa.go.jp

届出に関して、ご不明な点等ございましたら、上記の各届出先のメールアドレス宛にお問い合わせください。

Copyright © 2023 独立行政法人情報処理推進機構