愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信 第７号

令和６年４月

「組織」向け情報セキュリティ10大脅威 4年連続 第1位

ランサムウェア 知ってますか？

ランサムウェアってなに？

身代金要求型の不正プログラム。
感染すると、データが盗まれるうえ、ロックされて開けなくなる。
「元に戻したければお金を払え」と身代金を要求してくる。
さらに「お金を払わなければ盗んだデータを公開するぞ」と脅してくる。

被害に遭わないようにするためには？

・OSやソフトウェアを最新の状態にする
・ウイルス対策ソフトを導入し、パターンファイルを最新にする
・ネットワーク機器のファームウェアを最新にする
・パスワードは推測されにくいものにする
・メールの添付ファイルやリンクはむやみに開かない
・サイバー攻撃の手口について情報共有する

もしものために準備することは？

・データやログのバックアップをとる
・被害にあった場合の復旧マニュアルなどを作っておく
・被害についての報告先などをリスト化する
・サイバー保険の加入を検討する

ランサムウェアに感染してしまったら、**できるだけ早い段階で警察に相談**してほしいニャ

ご協力よろしくお願いします！

愛知県警察
サイバー犯罪対策課

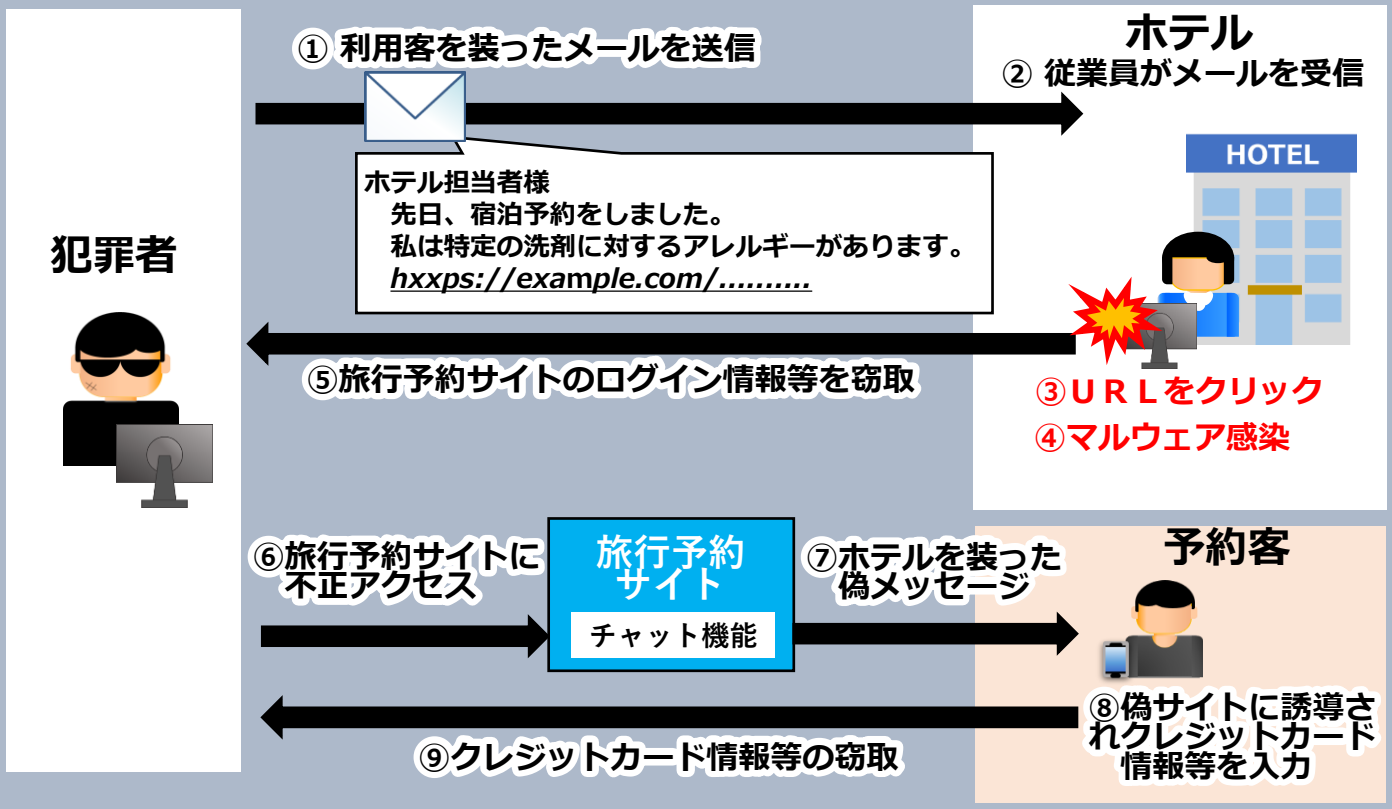
サイバー犯罪対策通信

第８号
令和６年４月

ホテルを狙う事案が発生！

メールのＵＲＬはクリックしないで！

事案の概要



日頃からの備え

- 業務用端末と個人端末を混同しない。（環境を混ぜない。）
- ＯＳやソフトウェア、ウイルス対策ソフトを常に最新の状態にする。
- 各種アカウントのパスワードは複雑なものに設定する。
- アカウントやパスワードをブラウザに保存しない。

愛知県警察サイバー犯罪対策課は、Ｘ（旧ツイッター）や愛知県警察ホームページでサイバー犯罪被害防止に役立つ情報を発信しています！
サイバー犯罪被害防止対策にぜひご活用ください！

愛知県警察
ホームページ

サイバー犯罪対策課
Ｘ（旧ツイッター）

愛知県警察
サイバー犯罪対策課

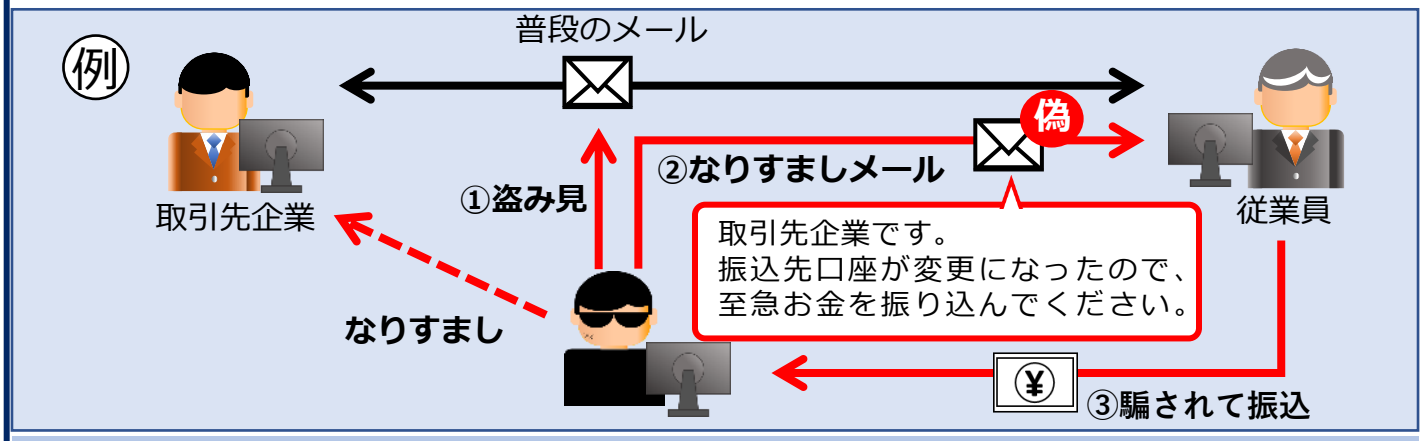
サイバー犯罪対策通信

第９号
令和６年４月

振込先口座の変更？それ本当？

もしかしたら、ビジネスメール詐欺じゃない？

海外の取引先や自社の社員（経営者層等）に**なりすました偽のメールを送り、振込先口座を変更させるなどにより、金銭をだましとる**詐欺（**ビジネスメール詐欺**（BEC：Business Email Compromise）が発生しています。



騙されないようにするには？

1 振込先の変更等は、メール以外の方法（電話等）で確認

2 普段と異なるメールは、メールアドレスや本文をよく確認し、社内で共有・相談

3 メールアカウントのパスワードの複雑化や多要素認証の導入

IPA　ビジネスメール詐欺（BEC）対策サイト
https://www.ipa.go.jp/security/bec/about.html

IPA 独立行政法人 情報処理推進機構

警察庁 National Police Agency

愛知県警察サイバー犯罪対策課は、X（旧ツイッター）や愛知県警察ホームページでサイバー犯罪被害防止に役立つ情報を発信しています！
サイバー犯罪被害防止対策にぜひご活用ください！

愛知県警察ホームページ

サイバー犯罪対策課 X（旧ツイッター）

愛知県警察
サイバー犯罪対策課

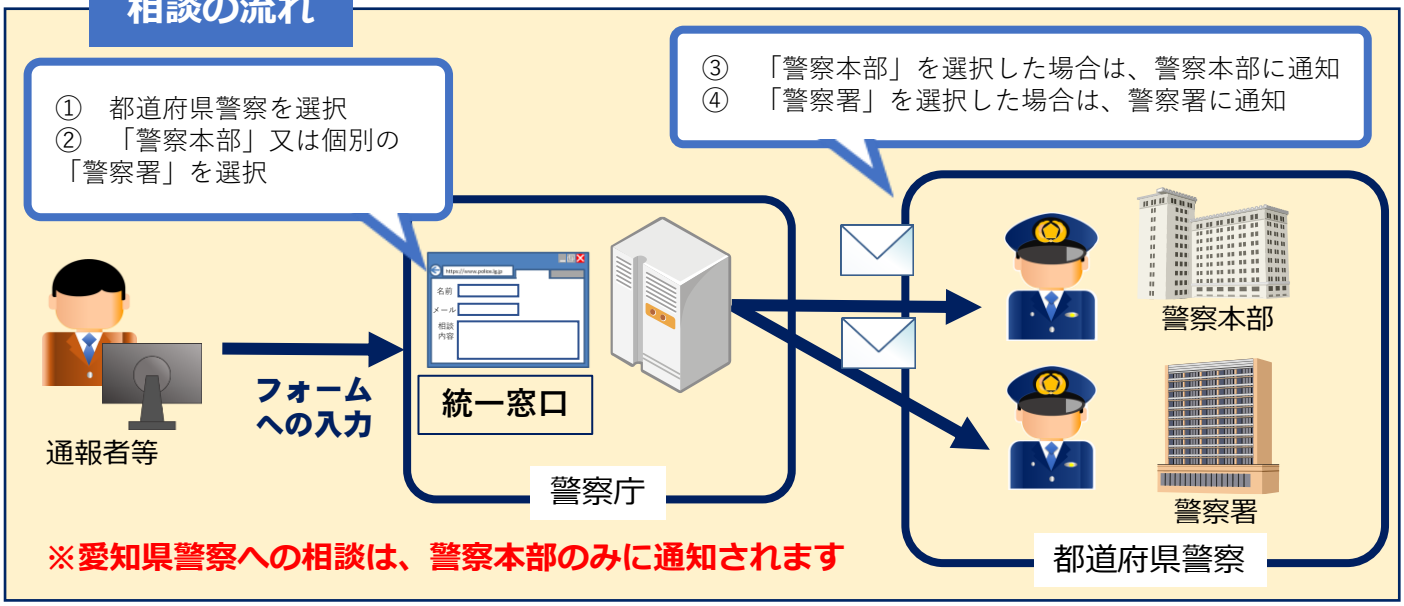
サイバー犯罪対策通信

第10号
令和６年４月

サイバー犯罪等に関する相談の統一窓口が設置されました!

警察庁ウェブサイトにおいて、都道府県警察に対するサイバー事案に関する通報等の統一窓口を設置し、令和6年3月29日から運用を開始しました。

相談の流れ



どうやって通報すればいいの？

① サイトにアクセス

https://www.npa.go.jp/bureau/cyber/soudan.html

緊急を要するものは110番してください。

②よくある相談をチェック

「よくある相談事例とその対処方法」を紹介しています。通報・相談をする前に解決できる場合があるかもしれません。

③ 通報等を選択

「通報」、「相談」、「情報提供」のうち、該当するものを選択してください。

④ 氏名等を入力

「氏名又は名称」、「メールアドレス」を入力してください。

⑤ ワンタイムURLをクリック

ワンタイムURLがメールで送信されます。当該メールに記載されたURLをクリックしてください。

⑥ 本文を記載し送信

「都道府県警察」、「警察署等」の欄から該当するものを選択し、通報等の内容を記載した上で送信してください。

警察庁
National Police Agency

愛知県警察サイバー犯罪対策課は、X（旧ツイッター）や愛知県警察ホームページでサイバー犯罪被害防止に役立つ情報を発信しています！
サイバー犯罪被害防止対策にぜひご活用ください！

愛知県警察ホームページ

サイバー犯罪対策課X（旧ツイッター）

愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R6-11号
組織向け

VPN機器・リモートデスクトップ管理はできてますか？

ランサムウェア対策

VPN機器とリモートデスクトップ

VPNとは、インターネット回線を、あたかも専用線であるかのように利用するサービスのことで、テレワーク等で導入する企業等が増加しています。

リモートデスクトップとは、コンピューター同士をネットワークで接続することで、遠隔操作を可能にするもので、保守管理に使われることが多いWindowsの標準機能です。

こんな会社は危険です！

VPN機器やリモートデスクトップを利用している会社で、次のような場合は非常に危険です。

① VPN機器を使っているが、**ファームウェアのアップデートをしたことがない**
② VPN機器は、委託業者が**たぶんアップデートしてくれていると思う（確認していない）**
③ テレワークでリモートデスクトップを導入したが、今は**使っておらず放置している**
④ **特定しやすいユーザ名**や**単純なパスワード**を使っている
（社員番号や部署名など、類推しやすいものはNG！）

今すぐ確認、見直しをしましょう！

○ VPN機器

① VPN機器のファームウェアを定期的にアップデートする
② 管理を委託している場合は、委託業者がどこまでメンテナンスをしてくれるのか、改めて確認する
③ VPNの認証を強化する
・ユーザ名やパスワードは、特定されにくい複雑なものにする
・多要素認証やワンタイムパスワードなどの導入も検討する

○ リモートデスクトップ

① 使っていなければリモートデスクトップを無効にする
② リモートデスクトップの認証を強化する
・IDやパスワードは、特定されにくい複雑なものにする
・多要素認証やワンタイムパスワードなどの導入も検討する
③ 接続できるIPアドレスを制限する
④ ログイン試行回数を制限する

愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R6-00号
組織向け

VPN機器・リモートデスクトップ管理はできてますか？

VPNとは、インターネット回線を、あたかも専用線であるかのように利用するサービスのことで、テレワーク等で導入する企業等が増加しています。

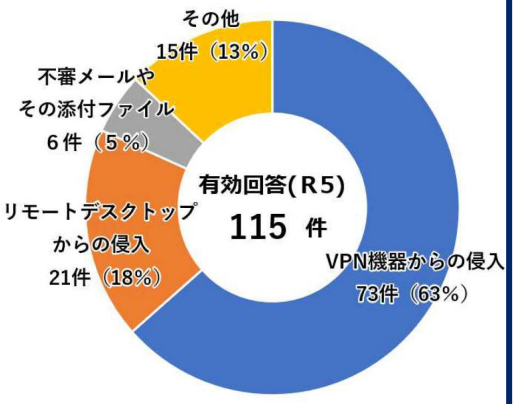
リモートデスクトップとは、コンピューター同士をネットワークで接続することで、遠隔操作を可能にするもので、保守管理に使われることが多いWindowsの標準機能です。。

狙われているVPN機器とリモートデスクトップ

警察庁の統計によると、ランサムウェアの感染経路の約６割がVPN機器、約２割がリモートデスクトップでした。

以上のことから、VPN機器とリモートデスクトップが、攻撃者に標的にされていることがよくわかります。

ランサムウェアの感染経路

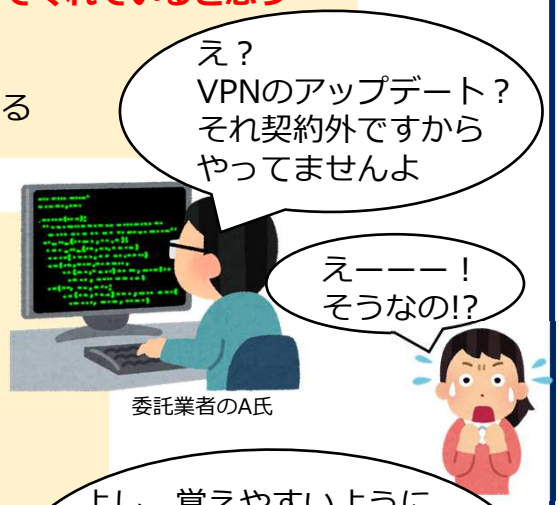


「令和5年におけるサイバー空間をめぐる脅威の情勢等について」より

こんな会社は危険です！

VPN機器やリモートデスクトップを利用している会社で、次のような場合は非常に危険です。

① VPN機器を使っているが、**ファームウェアのアップデートをしたことがない**
② VPN機器の管理は、委託業者が**たぶんアップデートしてくれていると思う**
③ テレワークでリモートデスクトップを導入したが、今は**使っておらず放置している**
④ **特定しやすいユーザ名**や**単純なパスワード**を使っている



今すぐ確認、見直しをしましょう！

○ VPN機器

① VPN機器のファームウェアを定期的にアップデートする
② 管理を委託している場合は、委託業者がどこまでメンテナンスをしてくれるのか、改めて確認する
③ VPNの認証を強化する
・ユーザ名やパスワードは、特定されにくい複雑なものにする
・多要素認証やワンタイムパスワードなどの導入も検討する

○ リモートデスクトップ

① 使っていなければリモートデスクトップを無効にする
② リモートデスクトップの認証を強化する
・IDやパスワードは、特定されにくい複雑なものにする
・多要素認証やワンタイムパスワードなどの導入も検討する
③ 接続できるIPアドレスを制限する
④ ログイン試行回数を制限する

愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R6-12号
組織向け

GW前に必ずやってほしいセキュリティ対策

GW期間中は、いつもと違う体制の勤務が増え、会社でセキュリティインシデントが発生したときに、対応が遅れたり、思わぬ被害が発生するおそれがあります！しっかり対策をとりましょう！

セキュリティ対策責任者・システム担当者向け

□ 対処手順・連絡体制は確認しましたか？ 重要

- 長期休暇期間中の監視体制を確認する。
- セキュリティインシデントの対処手順を確認し、連絡体制を更新する。
  ※長期休暇期間中に認知したインシデントの対応が休暇明けとなり、被害が拡大した事例も！

□ バックアップの対策はできていますか？ 重要

- 重要なデータや機器設定ファイルに対するバックアップ対策を実施する。
- バックアップデータはネットワークから切り離し、変更不可とするなどの対策を検討する。
  ※ランサムウェア攻撃により、大切なバックアップも暗号化されてしまう被害が出ています！

□ アクセス制御の設定は確認しましたか？

- アクセス権限の確認、多要素認証の利用、不要なアカウントの削除等により、本人認証を強化する。
- 利用者にパスワードが単純でないか確認させる。
- 外部ネットワークからアクセス可能な機器へのアクセスは必要なものに限定する。

□ ソフトウェアに脆弱性はありませんか？

- 脆弱性対策の状況を確認し、必要に応じてセキュリティパッチの適用やソフトウェアのバージョンアップを行う。

□ 利用機器に関する対策はできていますか？

- 機器（サーバ、パソコン等、通信回線装置、特定用途機器（防犯カメラなど）等）のファームウェアを最新にアップデートする。
- 不正アクセス等を防止するため、長期休暇期間中に使用しない機器の電源を落とす。

□ 各種ログの確認はしましたか？

- サーバ等の機器に対する不審なアクセスがないか、VPN、ファイアーウォール、監視装置等ログやアラートで確認する。
- 不審なログが記録されていた場合は、早急に詳細な調査等を行う。

情報システム利用職員向け

□ 機器やデータの持ち出しルールを遵守できていますか？

- 端末や外部記録媒体等の持ち出しは、組織内の安全基準等に則った適切な対応を徹底する。

□ 利用機器に関する対策はできてますか？

- 不正アクセスを防止するため、長期休暇期間中に使用しない機器の電源を落とす。

□ 電子メールの対策はできていますか？

- まずは、利用機器のOS・アプリケーションに対する修正プログラムの適用や不正プログラム対策ソフトウェア等の定義ファイルの更新等を実施する。
- 不審な添付ファイルを開いたり、リンク先にアクセスしたりしない。
- 不審な点があれば、電子メールを開封する前に、電話等、別の手段で確認する。

愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R6-12号
組織向け

GW後に必ずやってほしいセキュリティ対策

セキュリティ対策責任者・システム担当者向け

□ バックアップの確認をしましょう

- 重要なデータや機器設定ファイルに対するバックアップ対策を実施する。
- バックアップデータはネットワークから切り離し、変更不可とするなどの対策を検討する。
  ※ランサムウェア攻撃により、大切なバックアップも暗号化されてしまう被害が出ています！

□ アクセス制御の設定確認をしましょう

- アクセス権限の確認、多要素認証の利用、不要なアカウントの削除等により、本人認証を強化する。
- 利用者にパスワードが単純でないか確認させる。
- 外部ネットワークからアクセス可能な機器へのアクセスは必要なものに限定する。

□ 電源を落としていた機器に関する対策をしましょう

- 長期休暇期間中に電源を落としていた機器は、端末起動後、最初に不正プログラム対策ソフトウェア等の定義ファイルを確認する。
- 最新の状態になっていない場合は、更新してから、利用を開始する。

□ ソフトウェアの脆弱性情報を確認しましょう

- 長期休暇期間中における脆弱性情報を確認し、必要に応じてセキュリティパッチの適用やソフトウェアのバージョンアップを行う。
- 直ちに実施することが困難な場合は、リスク緩和策を講じる。

□ 不正プログラム感染の確認をしましょう

- 長期休暇期間中に持ち出しが行われていたパソコン等が不正プログラムに感染していないか、不正プログラム対策ソフトウェア等で確認する。

□ 各種ログの確認をしましょう

- サーバ等の機器に対する不審なアクセスがないか、VPN、ファイアーウォール、監視装置等ログやアラートで確認する。
- 不審なログが記録されていた場合は、早急に詳細な調査等を行う。

情報システム利用職員向け

□ 持ち出した機器や記録媒体の確認をしましょう

- 持ち出した機器の不正プログラム感染や、紛失、盗難による情報漏えい等の被害が発生しないように管理する。

□ 電子メールの対策をしましょう

- 電子メールを確認する前に、利用機器のOS・アプリケーションに対する修正プログラムの適用や不正プログラム対策ソフトウェア等の定義ファイルの更新等を実施する。
- 不審な添付ファイルを開いたり、リンク先にアクセスしたりしない。
- 不審な点があれば、電子メールを開封する前に、電話等、別の手段で確認する。