Ksisnetだより

発行:Ksisnet事務局
令和 3年 3月31日
Vol.91

「情報セキュリティ10大脅威2021」（組織） 3位 NEW

テレワーク等のニューノーマルな働き方を狙った攻撃

IPA（情報処理推進機構）が公開している「情報セキュリティ10大脅威2021」にて、
「テレワーク等のニューノーマルな働き方を狙った攻撃」
が新たにランクインし、**3位**に選出されています。今回はその手口や対策などについてご紹介します。

2020年は、組織の積極的なテレワークへの移行に伴い、自宅等からVPN経由で社内システムにアクセスしたり、ウェブ会議サービスを利用して会議を行ったりする機会が増えました。また、テレワークのために**私物PC**や**自宅ネットワーク**を利用したり、VPN等のために**初めて使うソフトウェアを導入**したり、以前までは**緊急用として使っていた仕組みを恒常的に使う**必要が出てきました。
このような**業務環境の急激な変化**を狙った攻撃が行われています

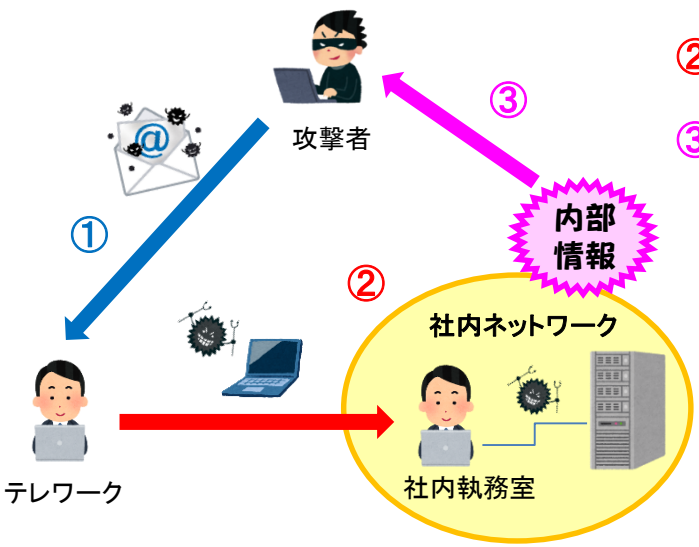
攻撃手口

①テレワーク用ソフトウェアの脆弱性の悪用
VPN等のテレワーク用に導入している製品の脆弱性を悪用し、社内システムに不正アクセスしたり、PC内の業務情報を窃取したりする。

②急なテレワーク移行による管理体制の不備
テレワークで利用しているPC内のOSやソフトウェアのセキュリティ管理を組織側から行うのは難しく、ルール整備やセキュリティ対策のノウハウが不十分なまま利用を開始している。

③私物PCや自宅ネットワークの利用
私物PCをテレワークで利用している場合、ウェブサイトにアクセスしたり私物のソフトウェアをインストールしたりして、ウイルスに感染したり、情報を抜き取られる被害に遭うおそれがある。
また、組織支給のPCを利用している場合でも、適切なセキュリティ対策が行われていない自宅ネットワークを利用することで、PCがウイルスに感染する等のおそれがある。

個人情報漏えい事例



① 社員がテレワーク中にSNSで知り合った第三者（攻撃者）から、ウイルスが添付されたメールを受け取った。
② 社員が、ウイルス感染したPCを、出勤時に社内ネットワークに接続し、社内に感染を拡げた。
③ ウイルス活動により、内部情報が攻撃者に漏えいした。

【対 策】
- テレワーク環境ではVPN機器へ接続しない限りインターネットを利用できない仕組みを導入することで、社内と同等のセキュリティ対策を適用する。
- 少しでも不審に感じたメールに添付されているファイルやリンクは絶対にクリックしない。
- セキュリティ確保の為の組織のルールや相談体制を整備する。

テレワークを行う際のセキュリティ上の注意事項

勤務先からテレワーク環境が提供されている方も、提供されずご自身のパソコンをお使いの方も、セキュリティ対策が充分なものかどうか、「 日常における情報セキュリティ対策 」を確認してみて下さい。

「 日常における情報セキュリティ対策 ～組織の利用者向け～」

1 修正プログラムの適用
利用するパソコン、スマートフォン等のOSや各種ソフトウェアを最新のバージョンに更新する。

2 セキュリティソフトの導入および定義ファイルの最新化
利用するパソコン、スマートフォン等にセキュリティソフトを導入し、セキュリティソフトの定義ファイルを常に最新の状態に設定する。

3 パスワードの適切な設定と管理
パスワードは可能な範囲で長い文字列、少なくとも大小英字、数字および記号を混在させて8文字以上に設定し、使い回しをしない。また、パスワードを初期設定のまま利用しない。

4 不審なメールに注意
ウィルスを組み込んだファイルが添付されているメールを開いてしまい、被害に遭う場合があることから、少しでも不審に思ったメールの添付ファイルやURLは不用意にクリックせずに、システム管理者に相談する。

5 USBメモリ等の取り扱いの注意
自身が管理していないUSBメモリ等の外部記録媒体をパソコンに接続したり、自身が管理していないパソコンに自身の外部記録媒体を接続しない。

6 社内ネットワークへの機器接続ルールの遵守
ウイルス感染している可能性も考え、個人所有のパソコンや外部記録媒体を不用意に社内ネットワークに接続しない。

7 ソフトウェアをインストールする際の注意
ソフトウェアをインターネットからダウンロードしたり、自身のパソコンにインストールしたりする場合は、事前にシステム管理者の許可をとる。

8 パソコン等の画面ロック機能の設定
第三者に見られたり、操作されたりしないようパソコンやスマートフォン等には画面ロックを設定する。
席を離れる際は、パソコンには画面ロックをかけ、スマートフォンは放置しない。

「 日常における情報セキュリティ対策 ～組織のシステム管理者向け～」

システム管理者の方は、上記組織の利用者向け情報セキュリティ対策を各利用者に周知徹底することはもちろん、下記の対策も徹底して下さい。

1 情報持ち出しルールの徹底
業務用パソコン等の機器やデータを組織外に持ち出す場合のルール（紛失した場合に備えて持ち出す機器やUSBメモリ等の外部記録媒体に適切な暗号化を施す等）を明確にし、関係者に周知徹底する。

2 社内ネットワークへの機器接続ルール
普段は社内ネットワークに接続していないパソコン等の機器を社内ネットワークに接続する場合のルールを明確にし、関係者に周知徹底する。接続する機器の脆弱性対策やウイルスチェックなどが適切に実施されているかを確認する。

3 定期的なバックアップの実施
システムの不具合やランサムウェア等のウイルスによるデータ破壊に備えて、定期的に外部記録媒体等へバックアップを行う。

4 不要なサービスやアカウントの停止または削除
外部から接続できるサーバで稼働している不要なサービスや、管理する機器やシステムに存在する不要なユーザアカウントは、停止または削除する。

【参　考】
IPA「情報セキュリティ10大脅威2021」「テレワークを行う際のセキュリティ上の注意事項」「日常における情報セキュリティ対策」
個人情報保護委員会「テレワークに伴う個人情報漏えい事案に関する注意事項」

「情報セキュリティ10大脅威 2021」の詳細については、下記ウェブサイトで公開されています。
https://www.ipa.go.jp/security/vuln/10threats2021.html