新型コロナへの対応による、セキュリティへの影響・対策

JPCERTコーディネーションセンター
早期警戒グループ
石井 泰鷹

アジェンダ

新型コロナウイルスでの環境の変化

在宅勤務社員を狙った攻撃事例

在宅勤務に利用している製品の脆弱性

リモートでの対応体制

アジェンダ(再掲)

新型コロナウイルスでの環境の変化

在宅勤務社員を狙った攻撃事例

在宅勤務に利用している製品の脆弱性

リモートでの対応体制

勤務環境の大きな変化

■今年の新型コロナウイルスの影響

感染対策として人と会わない

生活様式を変える必要が発生

➡ 在宅勤務に移行

もともとあるサイバー上の脅威

脅威

- マルウエア
- 端末の紛失・盗難
- 重要情報の盗聴
- 不正アクセス

影響

- 情報漏えい
- 情報の改ざん
- 業務の中断

在宅勤務によるセキュリティリスク

1. 勤務場所が自宅
   - 社外のネットワークに存在する端末
   - 連絡や連携速度の低下
2. 在宅勤務を可能とする製品の導入
   - Web会議
   - VPN(Virtual Private Network)装置
3. 急遽の設定、構築対応

アジェンダ(再掲)

新型コロナウイルスでの環境の変化

在宅勤務社員を狙った攻撃事例

在宅勤務に利用している製品の脆弱性

リモートでの対応体制

事例1:在宅勤務に利用した端末からの感染

■事象

個人の端末および社内機器のマルウエア感染

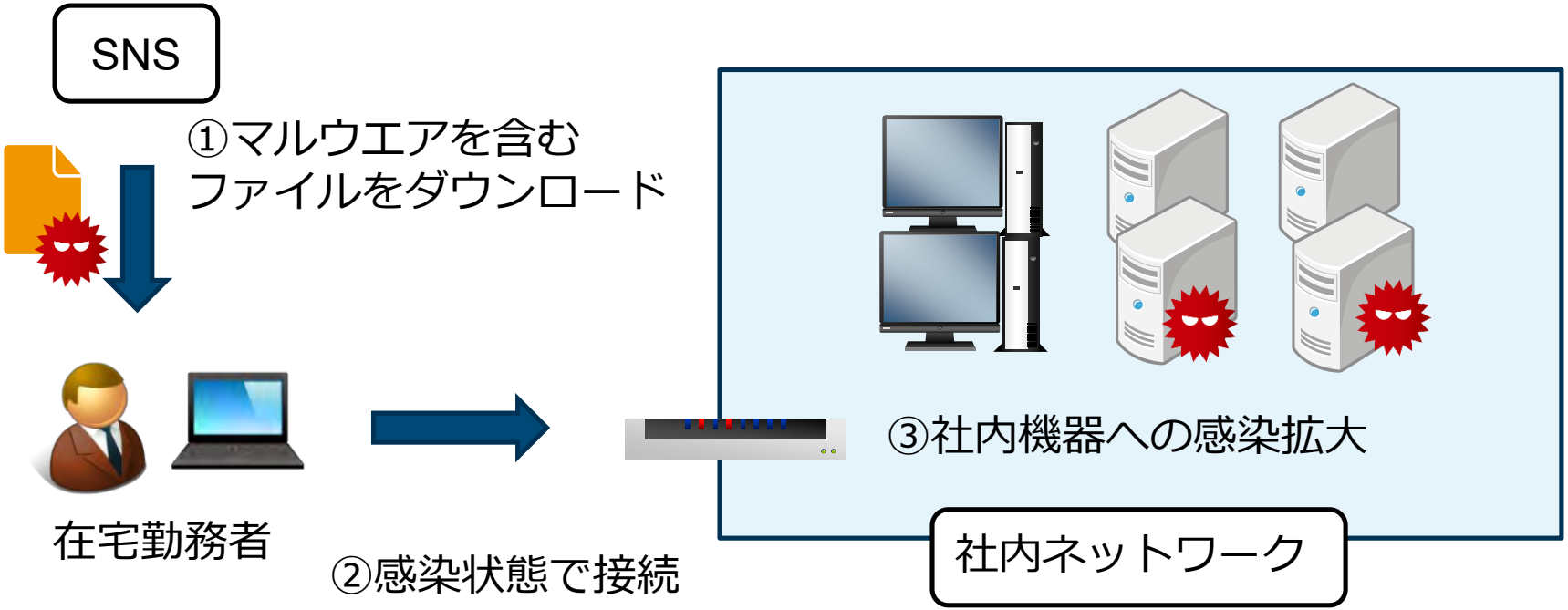
■被害

情報の流出

- ●従業員の個人情報
- ●サーバ設定情報

事例1:在宅勤務に利用した端末からの感染

■在宅勤務者の端末から社内機器へ感染



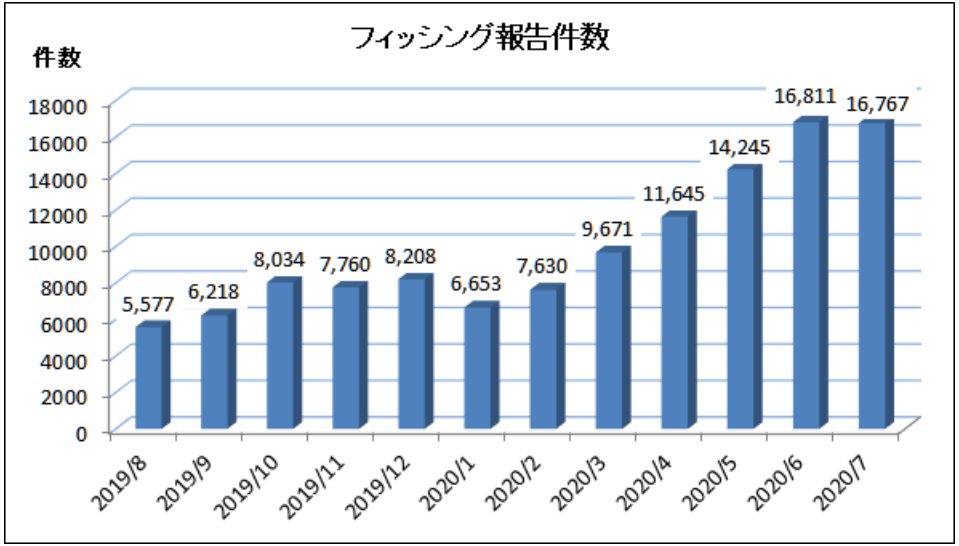
事例1:在宅勤務に利用した端末からの感染

対策

- 外部ネットワーク接続時のVPN接続の強制
- VPN接続前に端末への検疫の実施
- 利用端末へのフィルタリングサービスなどの導入
- 同一パスワードの設定有無の確認
- SNSなど私用利用の勤務者への注意喚起

事例2:新型コロナを題材にしたフィッシング

■2020年３月からフィッシングサイトの報告件数 増加



引用:フィッシング対策協議会:2020/07 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202007.html

事例2:新型コロナを題材にしたフィッシング

- マスク販売や給付金などが題材にされる

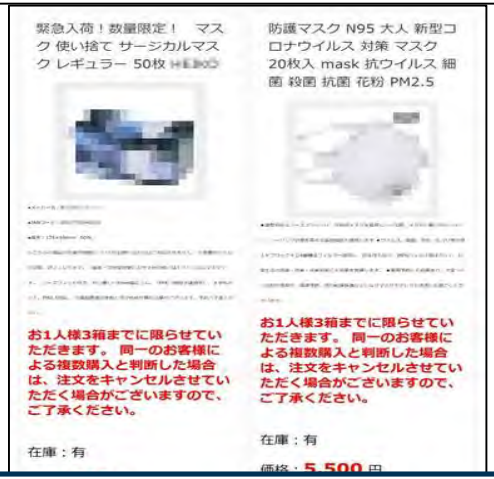
募金の呼びかけ

マスク配布の呼びかけ

マスク配布を装った偽サイトの例

不審なメールの内容

送信元アドレス：”AmazaClub”
件名：<受信者名> 緊急入荷！数量限定！　マスク 使い捨て サージカルマスク レギュラー 50枚
<省略>



マスク販売を装った不審サイトの例

※引用：トレンドマイクロ
https://www.is702.jp/news/3651/

事例2:新型コロナを題材にしたフィッシング

■医療機関を装った誘導メール

To: ●●●
Subject: 新型コロナウイルスの感染予防策について
各位

お世話になっております。

新型コロナウイルス関連肺炎については、中国武漢市を中心に患者が報告され、
国内でも多数患者が報告されています。

つきましては、以下通知をご確認いただき、感染予防策についてよろしくお願いします。

<対策はこちら>　←この部分が不審なURLへのリンクになっています

国立感染症予防センター
This email address is being protected from spambots. You need JavaScript enabled to view it.

引用:国立感染症研究所
https://www.niid.go.jp/niid/ja/others/9432-warning200226.html

事例2:新型コロナを題材にしたフィッシング

- 連絡や体調確認など
  在宅勤務者を狙ったメールが来る可能性

- 対策
  - 会社からの連絡方法の事前通知

アジェンダ(再掲)

新型コロナウイルスでの環境の変化

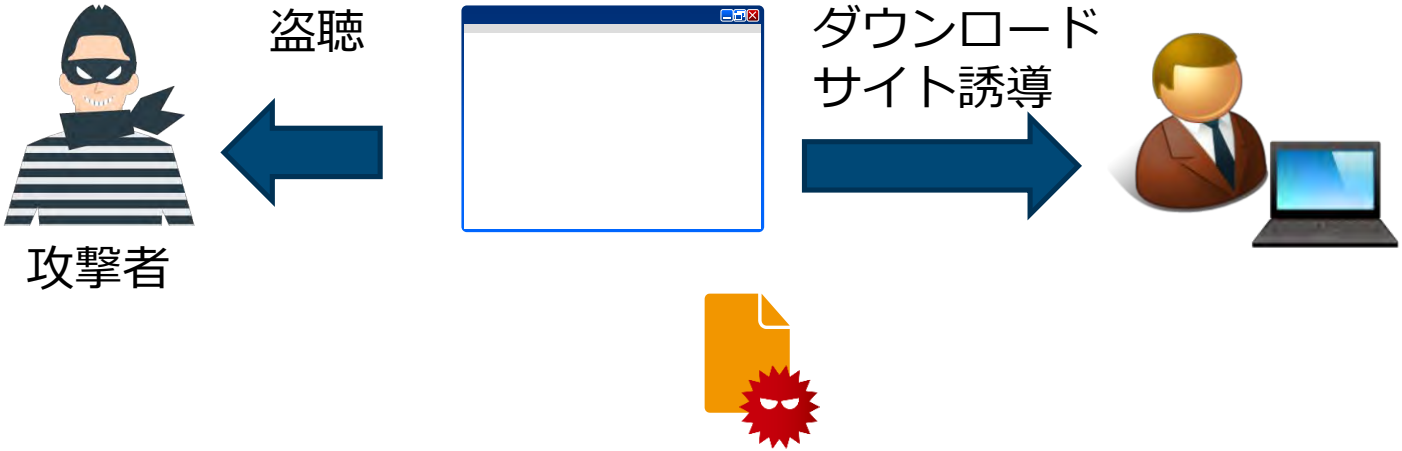
在宅勤務社員を狙った攻撃事例

在宅勤務に利用している製品の脆弱性

リモートでの対応体制

Web会議サービスの脆弱性の被害

- 脆弱性が悪用された場合、
  機微な情報の窃取やマルウエア感染など



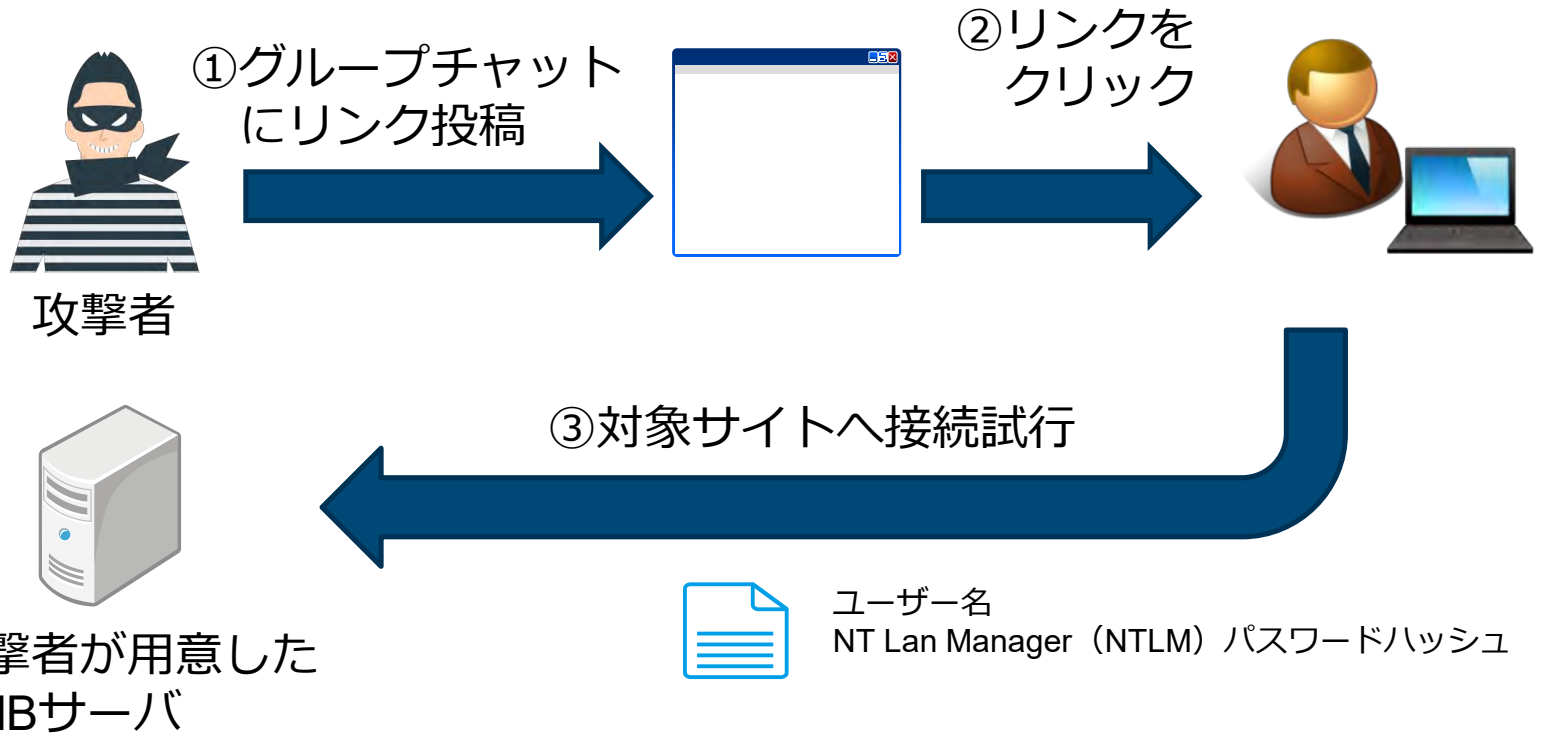
Zoom 認証情報の窃取の脆弱性

- 2020/4 修正された脆弱性
- 影響

  ユーザーのWindowsアカウントの認証情報の窃取
  (ハッシュ化パスワード)

- Universal Naming Convention（UNC）パスが指定されたグループチャットのハイパーリンクをクリックすることで認証情報が奪われる

Zoom 認証情報の窃取の脆弱性



他のWeb会議サービスの脆弱性

CISCO Webex Meetings

- 認証不備による不正アクセス CVE-2020-3361
- 認証トークンの処理が不適切なため
  細工したリクエストでユーザ権限が取得可能

Microsoft teams

- アカウントハイジャック の脆弱性
- 細工したGIFファイルを送付し、 認証トークンを入手

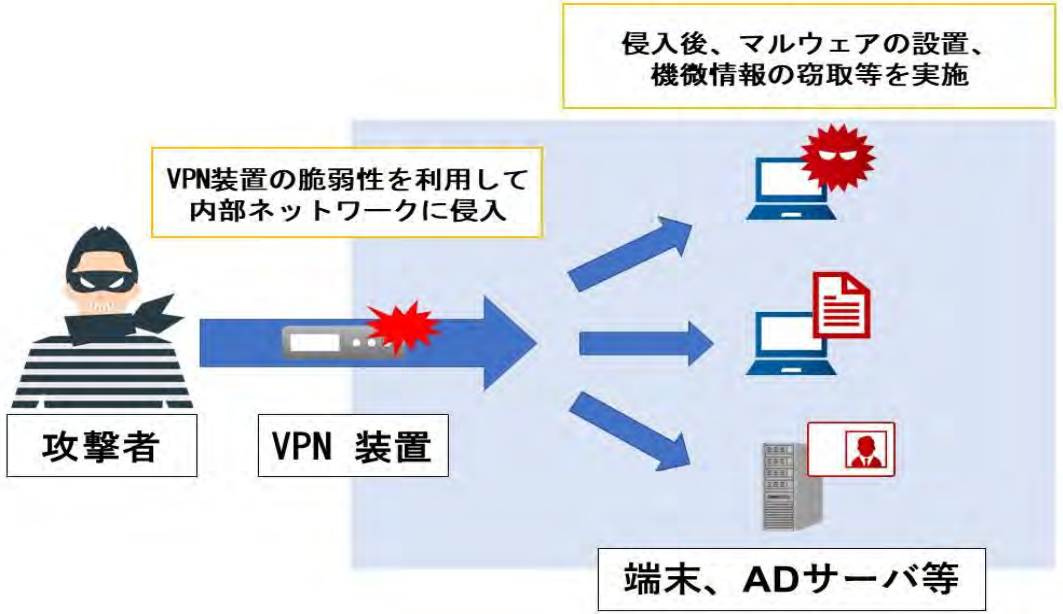
Web会議サービスの脆弱性に対して

- 必ず安全なサービスは存在しない
- 各端末上のアプリが更新されているか確認

- 利用要件を定めて、利用サービスの選定や利用ルールを設定する
  - 会議参加者
  - 取り扱う情報

VPN装置の脆弱性の被害

- 脆弱性が悪用された場合、社内ネットワークへの侵入のため、被害が大きくなることも



複数の Citrix 製品の脆弱性 (CVE-2019-19781)

■影響

遠隔からの任意コードの実行

情報の改ざんや窃取が可能

■国内で本脆弱性を悪用したと思われる攻撃や通信を確認

JPCERT/CC
複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200003.html

複数の BIG-IP 製品の脆弱性 (CVE-2020-5902)

■影響

遠隔からの任意コードの実行

■Traffic Management User Interface (TMUI)※ に細工したHTTPリクエストを送信により悪用可能

➡ インターネット上から、
アクセス可能であることが必要

F5 Networks
K52145254: TMUI RCE vulnerability CVE-2020-5902
https://support.f5.com/csp/article/K52145254

※TMUI : BIG-IP 製品の Web インターフェース

複数の BIG-IP 製品の脆弱性 (CVE-2020-5902)

- 侵害を受けたと思われるシステムや調査活動と思われるスキャンを観測

VPN装置の脆弱性に対して

- セキュリティ情報
  - 脆弱性情報の確認、侵害状況の確認など対応体制の設定
  - 更新スケジュールの設定

- アクセスの制限などセキュアな構築
  - 各製品ベンダの推奨構築との照らし合わせ

アジェンダ(再掲)

新型コロナウイルスでの環境の変化

在宅勤務社員を狙った攻撃事例

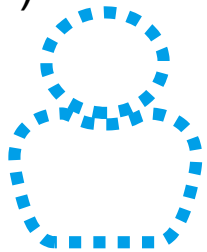
在宅勤務に利用している製品の脆弱性

リモートでの対応体制

リモートでの対応体制

- 対応基準の設定、周知
  - インシデント
  - アップデート
  - 情報の取り扱いレベル

- 連絡チャネルの複数保持(インシデント、アップデート)
  - 管理者、受付窓口
  - メール、電話、サイト



リモートでの対応体制

- リモート上で作業が行えることの確認
  - 機器やソフトウェアの更新
  - インシデント発生時の対応
    - 感染機器の封じ込め
    - ログの取得、調査
- リモート上で作業実施判断
  - 即応性
  - 外部から接続が可能なセキュリティリスク

参考資料

■各機関からガイドラインが発行

総務省
テレワークセキュリティガイドライン第４版 (PDF)
https://www.cloud-for-all.com/hubfs/resources/pdf/000545372.pdf

情報処理推進機構 (IPA)
テレワークを行う際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/telework.html

Web会議サービスを使用する際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/webmeeting.html

終わりに

- 新型コロナウイルスが流行し、半年以上たちます
- 急遽の在宅勤務に対応するため、
  突貫の対応があった
- 今後、在宅勤務が継続する可能性は高いため
  改めて見直し、いただきたい

Thank you!