日本電通IT Solutions Group

NDK ndis SIC NNG

NDK IT Solutions Group
Customer Conference 2020

アフターコロナで
強化すべきサイバーセキュリティ

日本電通株式会社

秋吉　隆博

情報処理安全確保支援士
第017694号

アフターコロナにおいては、
就業形態としてこれまで少数派だった「テレワーク」の比率が大きくなり、業務によっては常態化することが考えられます。
テレワークで業務を行うことが当然の世の中になりつつある今、本セッションでは強化すべきサイバーセキュリティ対策についてわかりやすくご説明致します。

秋吉 隆博

- 所属　ソリューション営業部
- 得意分野　セキュリティ、ネットワーク
- 出身　大阪生まれ、大阪育ち
- 趣味　料理、犬の散歩、自宅のIT化(IOT化)
- 今注目している技術　量子コンピュータ
- 尊敬する人物　徳川家康
- 資格
  - 情報処理安全確保支援士
  - 情報セキュリティマネジメント
  - 旧情報セキュリティアドミニトレータ
  - Fortinet　NSE4
  - Cisco　CCNP Enterprise

モモ　4歳です

情報通信技術を活用した、場所や時間にとらわれない柔軟な働き方

3種類に分類

自宅利用型テレワーク (在宅勤務)

自宅にいて、
会社とはパソコンとインターネット、電話で連絡

モバイルワーク(社外で仕事)

顧客先や移動中に、
パソコンや携帯電話を使う働き方

施設利用型テレワーク (サテライトオフィス勤務など)

勤務先以外のオフィススペースで
パソコンなどを利用した働き方

＝　会社のネットワークの外で仕事をすること

出典：一般財団法人　日本テレワーク協会Web

現在はデスクワークが主体

妊娠・育児・介護などの理由、身体障がい、あるいはケガなどにより、恒常的または一時的に通勤が困難な人
→常時在宅勤務主体

企画・総務・人事・経理などの管理部門、研究・開発部門の人
→部分在宅勤務主体（週に数日）

営業やSE、サポートサービスなどの顧客対応業務の人
→モバイルワークが主体

働き方改革

少子高齢化による労働力減少にも効果的

労働障壁撤廃

業務効率向上

生活の質向上

建物で例えるなら・・・

社内のネットワークは「城」

情報システム担当者が、ファイアーウォール等のセキュリティ製品を導入し、
社外への通信をルールに基づき、通信の制限/チェック（ウィルス対策、侵入防御）を行っている。
会社貸与PC（セキュリティ対策済み）での業務が原則
→安全なネットワーク、安全な環境

社外のネットワークは「民家」

専門知識を持った情報システム担当者がおらず、家庭用ルータでは、通信の制限/チェックが万全ではない。
個人の端末で作業の可能性（セキュリティアップデート未実施、セキュリティソフト未インストール、
OSのサポート切れ、危険なアプリケーション）

公衆Wifiは誰が接続しているかわからない（情報の傍受など悪意を持った利用者がいる可能性）
→自社のセキュリティ統制から逸脱した環境の可能性

テレワーク中のパソコンを狙う主な脅威

攻撃は無差別に行われます。

フィッシング、標的型攻撃メール

メールを使用した攻撃、情報の窃取、不正侵入、金銭の取得を目的とする。

不正侵入、不正アクセス、踏み台攻撃

通信機器やパソコンの脆弱性を突き、侵入、情報窃取、第三者への攻撃の踏み台にする。

マルウェア（コンピュータウィルス感染）

メールの添付ファイルやWebからのファイルのダウンロードで感染
パソコンの動作の妨げ、データ破壊、情報の窃取、他のパソコンへの拡大を図る。

端末の紛失・盗難

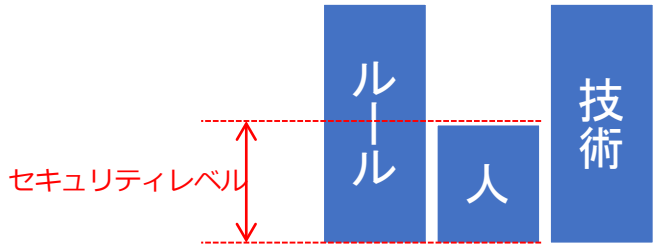
端末の紛失、盗難による、データの消失、情報漏洩

データの消失

マルウェア、ハードウェア故障によるデータ消失

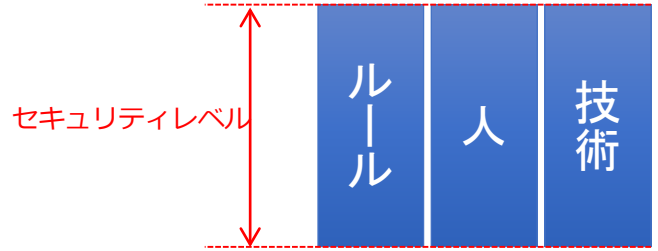
情報セキュリティの考え方

バランスの悪いセキュリティ対策



ルール、人、技術のバランスが悪いと
全体のセキュリティレベルは低下する

バランスがとれたセキュリティ対策



ルール、人、技術がバランスがバランスよく
保たれると高いセキュリティレベルを維持できる

情報セキュリティ対策は「最も弱いところが全体のセキュリティレベルになる」
「ルール」・「人」・「技術」の三位一体のバランスの取れた対策が重要

テレワークに対応した**情報セキュリティガイドライン策定**

基本方針：セキュリティ全体の根幹
対策基準：基本方針をもとに実施すべきことや守るべきことを規定したもの
実施手順：対策基準の事項を具体的に実行するための手順を示したもの

テレワーク実施時にセキュリティガイドラインに追加するルールの観点(例)

- ✓ 自宅における作業環境、PC の保管及び管理方法
- ✓ 自宅における休憩中の PC の取扱い〔ロックだけでいいのか、保管して鍵をかけるのか〕
- ✓ モバイルワークにおける PC の管理方法〔体から離さない、ストラップをつける、のぞき見防止フィルターをつける〕
- ✓ オフィスから持ち出す PC の管理〔暗号化、BIOS パスワードなどを義務付け〕
- ✓ オフィス以外での情報管理〔紙情報の管理、共用スペースでの情報管理〕
- ✓ 社内にVPN接続する頻度(システムからの管理のため、VPN接続させる)

テレワークに対応した**従業員への教育**（セキュリティの啓もう）

セキュリティガイドラインやルールを、テレワーク実施者に遵守するよう求める

研修などを通じて従業員に理解してもらい、浸透させる

例：半年に一度、セキュリティの啓もう教育を行う。

- ✓ 自社のセキュリティガイドラインの説明・強化事項の解説
- ✓ 半期のセキュリティ事故の振り返り
- ✓ セキュリティ脅威の流行の解説と注意喚起
- ✓ IPA発表のセキュリティ10大脅威の説明

テレワークを前提とした**システム、セキュリティの仕組**みづくり①

利用アクセスの管理・制限

① システム及びアプリケーションへのアクセスが従業員本人によるものであることを認証すること（本人認証）
② あらかじめ登録されている端末からのみのアクセスを許可すること（端末認証）

③ 従業員に貸与している PC などの端末情報を一元的に管理すること（端末管理）

例：ソリューション例

① ユーザID、パスワードによる認証システム　シングルサインオン　生体認証など

② Windowsアクティブディレクトリによる、認証

③ IT資産管理ソフトウェアによるPCの一括管理、運用

テレワークを前提としたシステム、セキュリティの仕組みづくり②

暗号による管理

① PC内のデータの暗号化

② 外部記憶媒体(USBメモリ)内のデータの暗号化

<u>例：ソリューション例</u>

① Windows 10 Proに標準搭載されている、BitLockerによる暗号化

② 暗号化機能を持ったUSBメモリ

テレワークを前提としたシステム、セキュリティの仕組みづくり③

運用のセキュリティ

① PC やサーバ等、情報を直接扱っている機器へのウィルス対策

② PCやサーバ等、情報を直接扱っている機器のOSのセキュリティパッチの適用

<u>例：ソリューション例</u>

① 次世代アンチウィルスソフト

② アクティブディレクトリ、WSUS/IT資産管理システムによる更新管理

テレワークを前提としたシステム、セキュリティの仕組みづくり④

ネットワークのセキュリティ

① 公衆Wifiの利用を避ける

② 社内システムと通信するときはVPNやHTTPSで暗号化する

③ インターネットアクセスを保護するサービスの利用

<u>例：ソリューション例</u>

① 会社貸与のモバイルWifi、携帯電話でのテザリング

② リモートアクセス装置による、VPN、HTTPSでの暗号化

③ クラウドセキュリティPROXYサーバ、クラウドセキュリティDNSサーバによる、インターネット通信に対する、ウィルス対策、Webコンテンツフィルタリング、不正通信の防止

- ✓ **企業にとってテレワークに対する取り組みは避けて通れない**

- ✓ **テレワークを導入・運用するうえで情報セキュリティを確保することが重要**
  - ✓ **ルール**：テレワークに対応したセキュリティルールの作成
  - ✓ **人**：セキュリティルールをテレワーク実施者に対し理解してもらう
  - ✓ **技術**：テレワーク時、適切なセキュリティが確保できるセキュリティシステムを導入し、運用する。

日本電通グループがテレワークに必要なIT環境の構築からセキュリティの確保までご支援させていただきます。

参考文献

日本テレワーク協会　Webサイト
総務省　テレワークガイドライン　第四版
厚生労働省　　テレワークの導入・運用ガイドブック

ご視聴ありがとうございました。

本セッションにてご紹介のソリューション、サービスの御相談に関しましては
担当営業、もしくは下記アドレスへご連絡ください。

ご連絡アドレス：日本電通マーケティング事務局
itsol_1@ndknet.co.jp