NTT-ATの5つのビジョン。

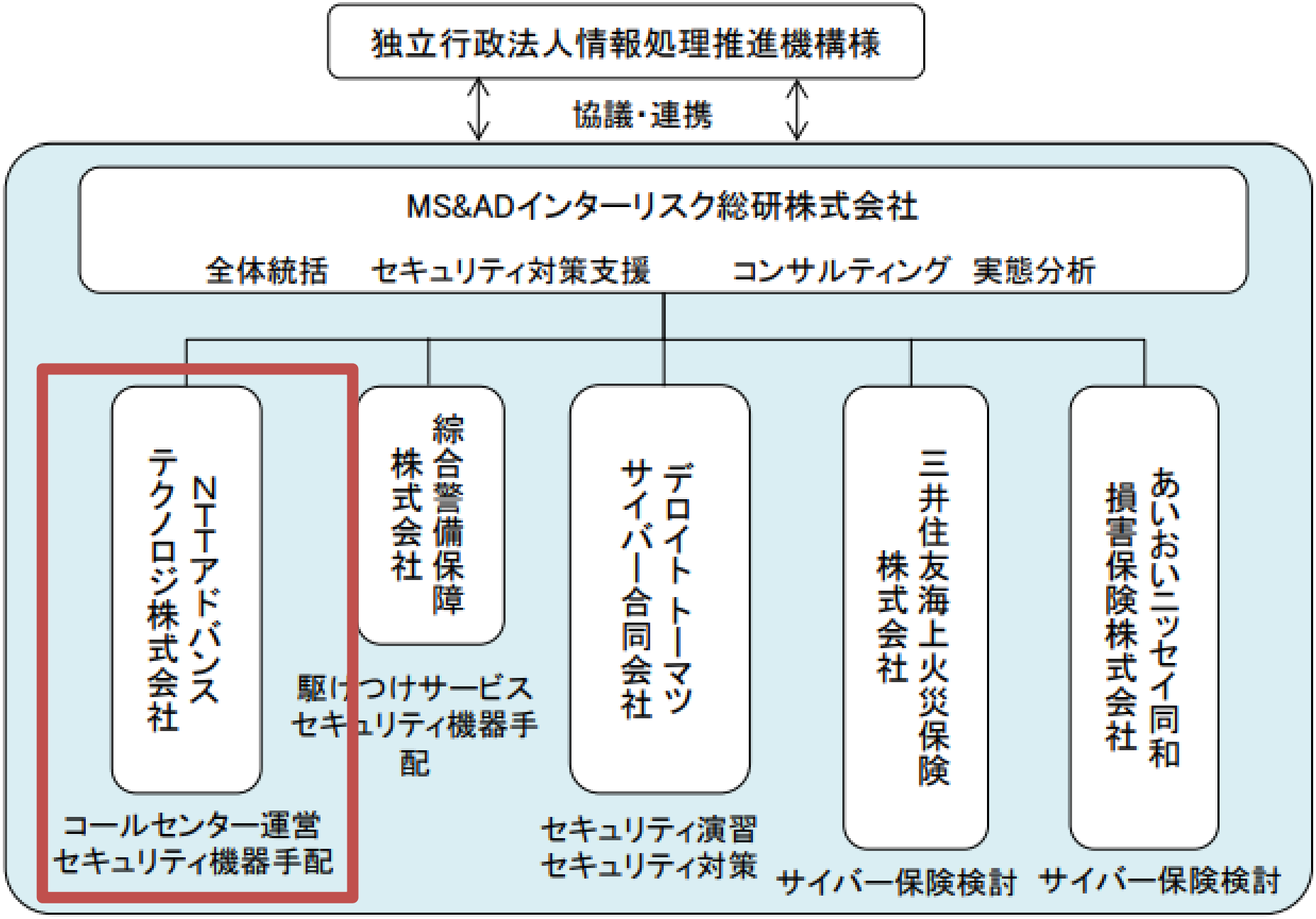
中小企業向けサイバーセキュリティ事後対応支援実証事業（実証地域：愛知県）

中間報告

2019年10月16日

NTTアドバンステクノロジ株式会社

当社の役割（おさらい）



コールセンター対応事例

【事例１】
据置型UTM機器でボットネットとの通信を検知（復数）

■ ボットネットとは…

- サイバー犯罪者に乗っ取られたパソコンが集まってできたネットワーク。
- ボットウイルスに感染したことが原因でパソコンやスマートフォンが知らない間にボットネットに参加させられる。（ゾンビ化）

※ゾンビ化した機器の情報は闇市場で売買されている。

コールセンター対応事例

■ ボットネットに参加させられるとどうなるのか？

- **他社への被害（加害者になる）**

→サイバー攻撃に加担させられる。

  - 他社のサービスを停止させてしまう。
  - 迷惑メールの送信元になってしまう。

- **自社への被害**

→自社の情報を盗まれる。

→攻撃元として被害者から訴訟を起こされるおそれがある。

→会社の信用が失墜し、取引停止などに発展するおそれがある。

コールセンター対応事例

■ 発生事象詳細

・xx月xx日 最初のボットネット通信を検知（1回目の検知）

→発信元のIPアドレスを提示し、以下の初期対応を依頼

- 端末利用者に対し、当該通信が意図して行った通信であるか
- 当該端末のネットワークからの切り離し
- 当該端末のウイルス対策ソフトでのフルスキャン

→以下の状況より一旦様子見

- 通常ネットワークに接続していない端末である
- ウイルス対策ソフトでフルスキャンしても何も検出されない
- 単発の通信であり、手動で行った可能性が否定出来ない

コールセンター対応事例

・xx月xx日（後日） 事象再発（2回目の検知）

17秒で14回の異常通信を検知

→発信元のIPアドレスを提示し、以下の初期対応を依頼

- 端末利用者に対し、当該通信が意図して行った通信であるか
- 当該端末のウイルス対策ソフトの定義ファイル最新化
- 当該端末のネットワークからの切り離し
- 当該端末のウイルス対策ソフトでのフルスキャン
- 検知できない場合は、端末の初期化を推奨

さらに約1時間30分後に別の端末でも25秒で14回の異常通信を検知（3回目の検知）

→上記と同様の初期対応を依頼

2回目、3回目の検知は状況的に明らかに手動ではない。

コールセンター対応事例

■ **対処内容（最後の不正通信の発信元となったIPアドレスの例）**

① マルウェアに感染しているおそれがあるため、発信元のIPアドレスを元に端末の特定を依頼。

② ①と並行して駆けつけ隊を手配。

③ 端末のメーカを特定し、駆けつけ隊へ共有。

④ 駆けつけた時点では該当端末も特定されていたが、駆けつけ隊による現況調査を実施。

⑤ 該当端末は私物の持ち込み端末であったため、端末自体の調査は行わなかった。

コールセンター対応事例

■ 推奨防止策

● 社内ネットワークへの接続制限をかける。

→会社のネットワークに私物のパソコンやスマートフォンをつながせないように制限をかける。
→外出先で利用する業務用端末を支給する。（セキュリティ対策が実施済みであること）

● 私物のパソコンやスマートフォンへのセキュリティ対策を実施、管理する。

→業務上、やむを得ず私物のパソコンやスマートフォンを接続する必要がある場合には、セキュリティ対策を実施した上で定期的なチェックを行うなど管理する。

コールセンター対応事例

【事例２】
据置型UTMでポートスキャン攻撃を検知

■ ポートスキャン攻撃とは…

- サイバー犯罪者が企業を攻撃する前の**偵察活動**。
- 偵察活動により対象企業のネットワークやサーバ、PCの弱点を見つける。

コールセンター対応事例

■ 偵察活動をされるとどうなるのか？

- サイバー攻撃の初期段階。偵察活動自体は悪さをしない。

- 偵察活動がさらに進み、ネットワークやサーバ、パソコン等の弱点（脆弱性）が見つかると、そこを攻撃され、情報を盗まれたり、ウイルスを仕込まれる。

コールセンター対応事例

■ 発生事象詳細

・xx月xx日 ポートスキャン通信を検知

→発信元のIPアドレスを提示し、以下の初期対応を依頼

・端末利用者に対し、該当する時間に不審なサイトを閲覧していないか

・上記の可能性がなければ、当該端末のネットワークからの切り離し

・さらに当該端末のウイルス対策ソフトでのフルスキャン

（継続対応中）

コールセンター対応事例

【事例３】
電話でのお問い合わせ
「Windows Updateについて」

- Windows Updateでは通常、Windowsのセキュリティを修正するプログラム等が定期的(月例)に自動配信され、更新される。

- まれに緊急対応が必要な場合などでMicrosoftから修正プログラムが提供される。
  →これは自動更新のタイミングを待つことなく、手動でインストールする必要がある。

コールセンター対応事例

■ 9月24日にMicrosoftからInternet Explorerの脆弱性を修正するプログラムが提供された。

→これに関するお問い合わせを受け、更新プログラムの手動適用手順をご案内した。

コールセンターより

■ コールセンターへのご相談例

- 「ウイルス対策ソフトで何かを検知した画面が表示された。」
- 「あなたの会社がサイバー攻撃を受けているようだ。と外部から通報があった。（代表例：ホームページの改ざん）」
- 「あなたの会社からサイバー攻撃を受けている。と外部から通報があった。」
- 「怪しいホームページや怪しいメールを開いてしまった。」

など、サイバーセキュリティに関することは**お気軽に**ご相談ください。お待ちしております。

据置型UTM機器の設置状況について

ご協力ありがとうございます！

据置型UTM機器設置状況（2019.10.11時点）		
総数	33	
UTM接続完了	24	73%
都合による対応保留	4	12%
UTM未接続	5	15%

不明点などは
SonicWall**サポートセンターへ！**
・書き方がわからない。
・相談しながら書きたい。
・何をすればいいの？など
0800-800-8529（通話料無料）
044-280-8787（携帯こちら）

引き続き、ご協力をお願いいたします。

据置型UTM機器の回収および継続利用について

■ 据置型UTM機器を継続利用される方

- 新しい機器への入れ替えを行います。
- 設定済みの新しい機器を送付いたしますので、現在ご利用中の機器と入れ替えて同梱の着払い伝票で現在ご利用中の機器を返送してください。
- 価格は本体価格＋遠隔監視費用込みで年間140万円です。
  （実証事業参加企業限定価格。2020年3月31日まで有効。2年目以降は年間124.5万円）
- 提供内容に変更がありますので、詳細は報告会終了後、個別にお問い合わせください。

据置型UTM機器の回収および継続利用について

■ 据置型UTM機器を継続利用されない方

- 機器の回収につきましては、個別にご連絡を差し上げます。

未来を拓くチカラと技術。

NTT AT

〒212-0014 神奈川県川崎市幸区大宮町1310ミューザ川崎セントラルタワーTEL 044-280-8811 FAX 044-520-1530 URL: http://www.ntt-at.co.jp/