資料2－2

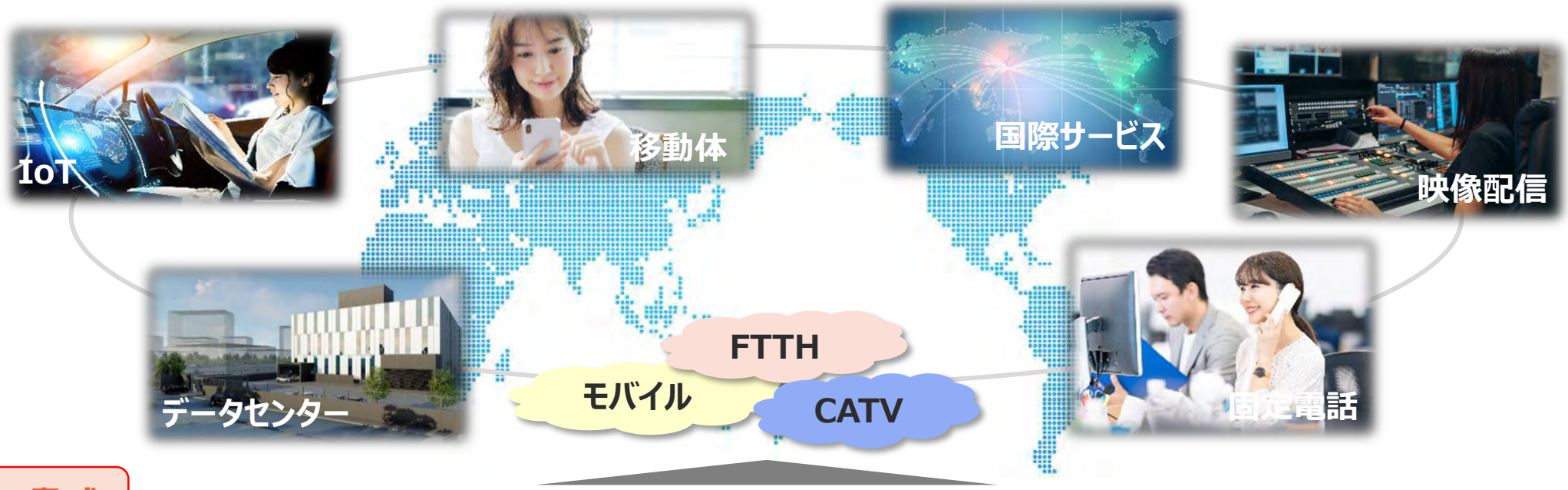
KDDIにおけるサイバーセキュリティ対策の取組み

KDDI株式会社

Tomorrow, Together
KDDI

通信事業者が守るネットワーク

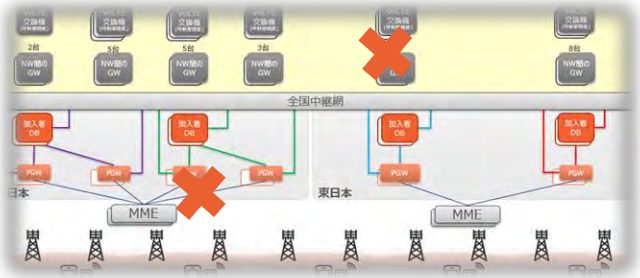
- 自然災害、サイバー攻撃などの脅威から、通信インフラを守るのが通信事業者の使命



通信への脅威

自然災害

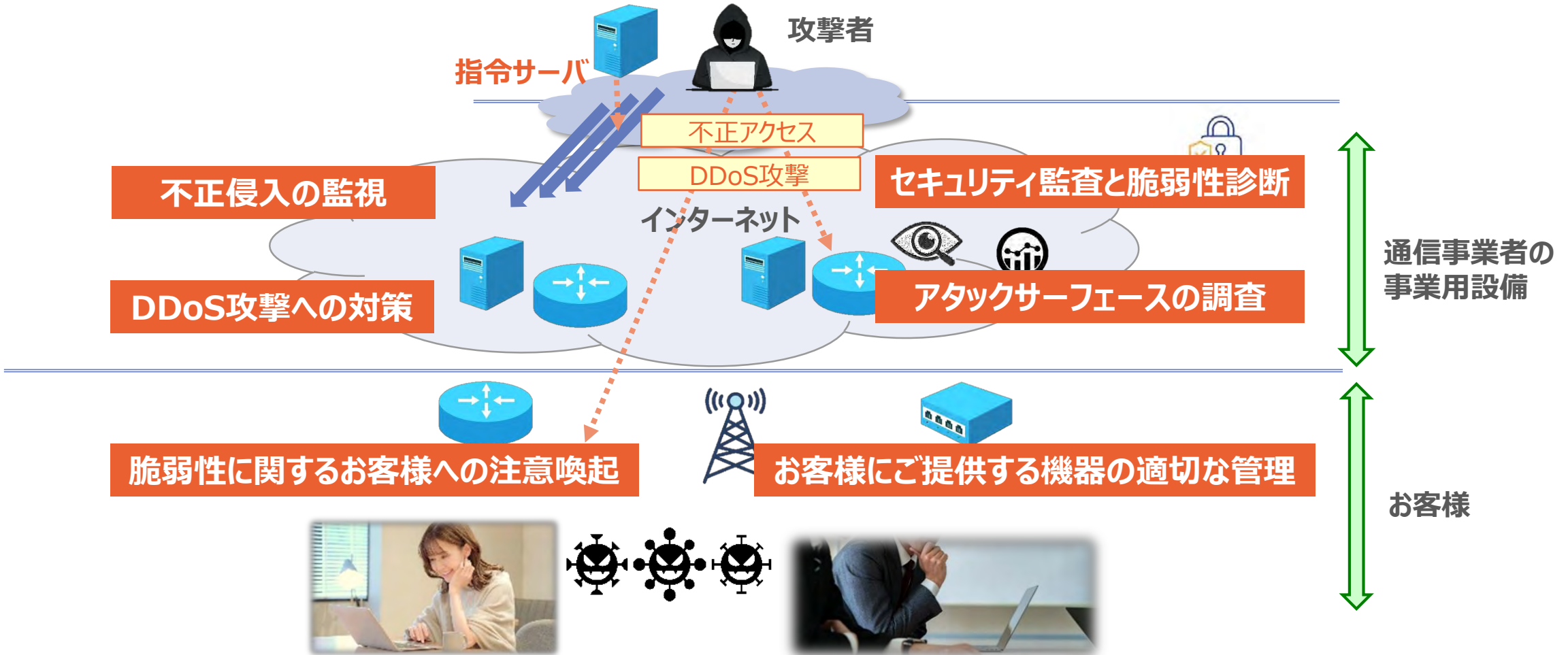
設備障害



サイバー攻撃

KDDIのサイバーセキュリティ対策

- 事業用設備では、不正侵入の監視やDDoS攻撃への対策を実施。
- お客様にはご提供する機器の適切な管理や脆弱性に関する注意喚起を実施。



セキュリティ監視

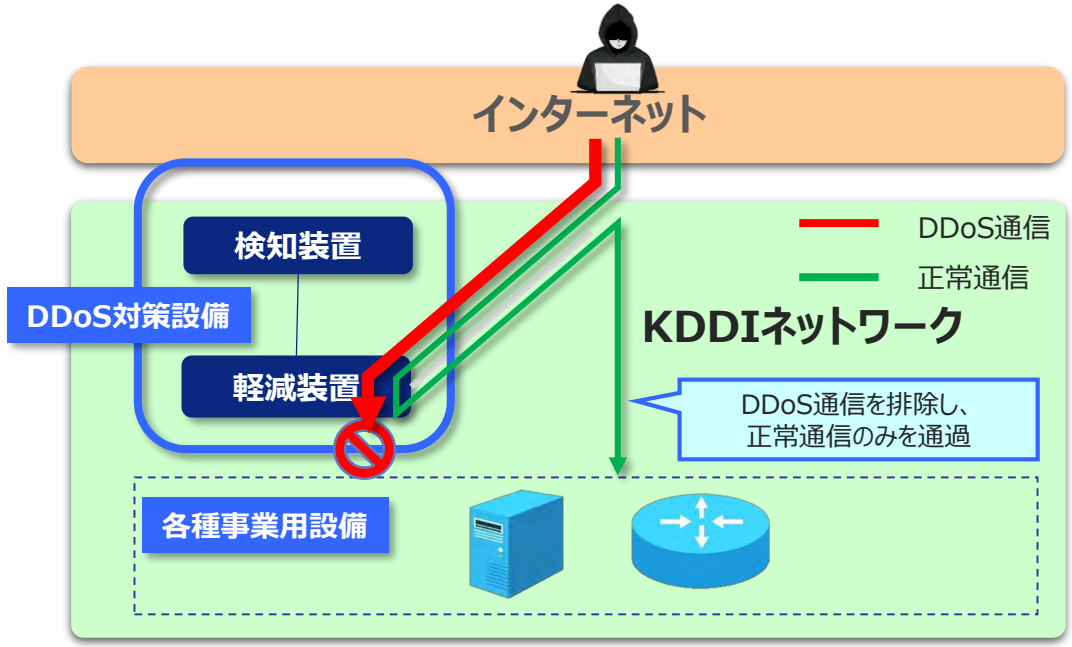
- **事業用設備を守るためにセキュリティオペレーションセンターがサイバー攻撃を監視**
- **DDoS攻撃が発生した際は、DDoS対策設備で攻撃通信を排除**

不正侵入の監視

- 専門的な訓練を受けたセキュリティアナリストが24時間365日の体制で監視。各セキュリティ監視機器から出力されるログを分析し、攻撃の兆候を調査。
- サイバー攻撃を受けた場合は、運用保守部門と連携し、迅速に対処できる体制を構築。

DDoS攻撃への対策

- 事業用設備にDDoS攻撃が発生した場合は、DDoS対策設備で攻撃通信を排除。
- 事業用設備向けのDDoS攻撃の通信元アドレスを調べると、海外と思われるアドレスからの通信が多い。

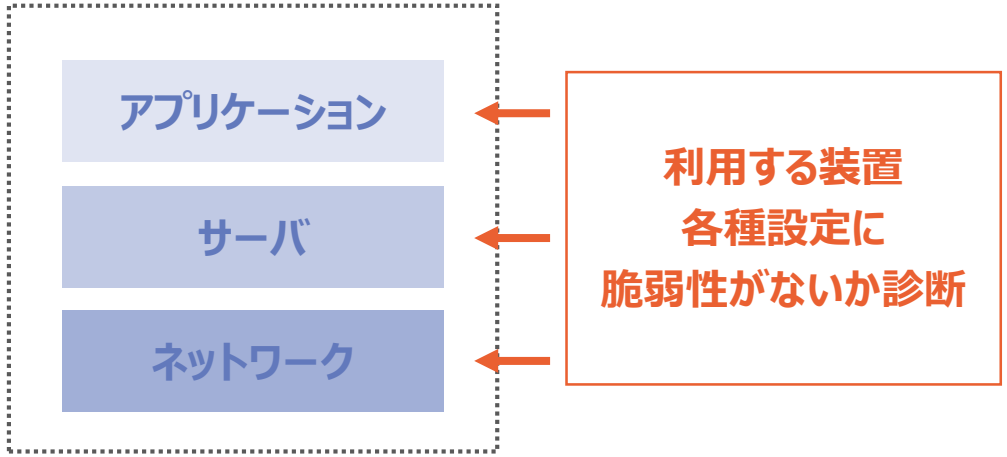


セキュリティ監査と脆弱性の調査

- **社内セキュリティ規範に基づき、事業用設備の監査や脆弱性診断を実施。**
- **OSINT等を活用し、外部公開機器の悪用リスクを調査。**

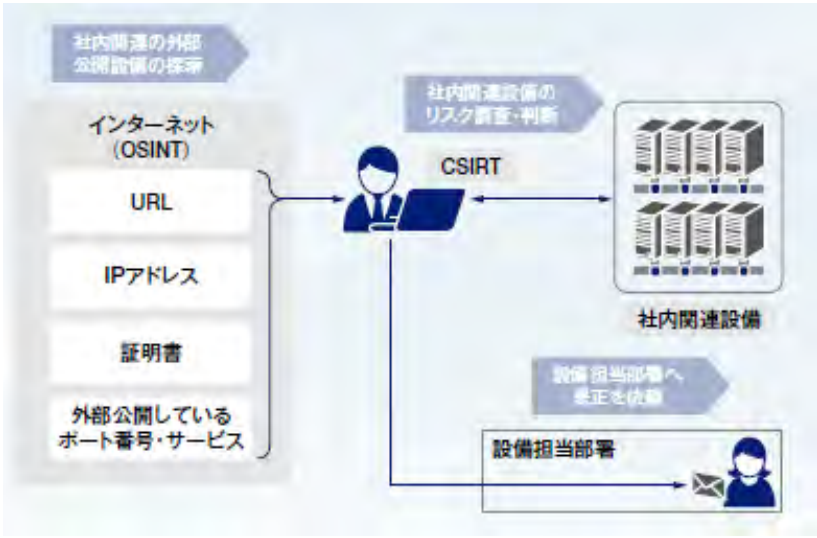
セキュリティ監査と脆弱性診断

- 社内のセキュリティ規範に則り、事業用設備のセキュリティ設計について専門部門が監査を実施。また、運用への移行フェーズと、その後の運用フェーズにてサーバやネットワークに存在する脆弱性を診断。
- 対策の不備や脆弱性が確認された場合は直ちに是正を図る。



アタックサーフェースの調査

- 攻撃者に悪用されるサービスやコンテンツを意図せずに公開していないかなど、OSINT（Open Source Intelligence）などを活用して、外部公開されている社内関連設備を探索し、設備に対する攻撃リスクや管理状況を調査し、速やかに是正。

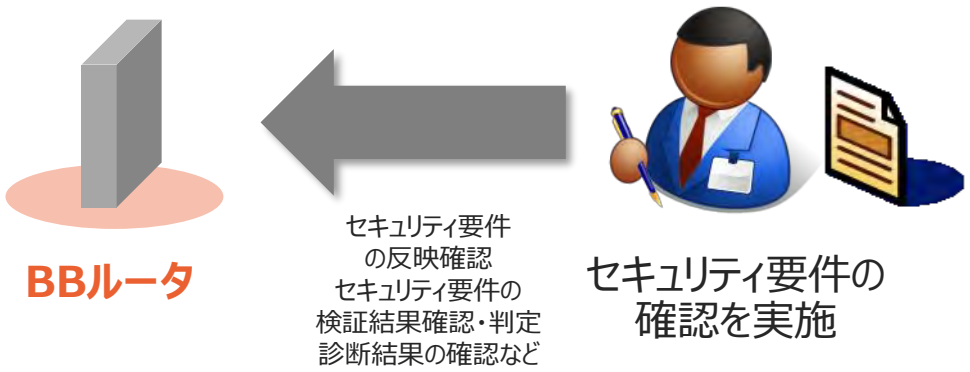


お客様機器の管理

- **お客様回線と併せて提供されるルータについて、セキュリティ観点での確認を実施。**
- **提供後もファームウェア更新など、ソフトウェア状態を管理することで安全性を確保。**

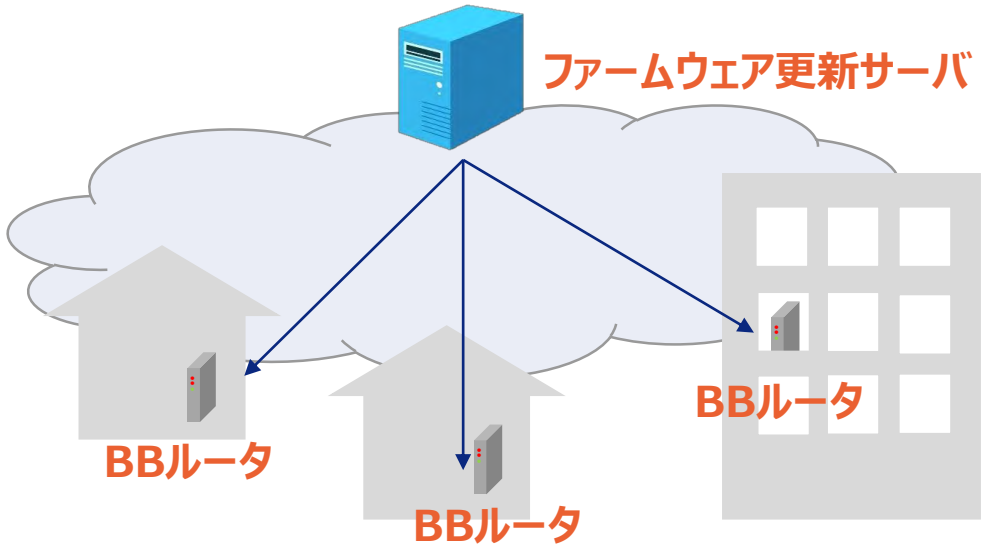
BBルータのセキュリティ

- お客様回線と併せて提供されるBBルータについて、所定のセキュリティ要件を満たしているか確認を実施。
- セキュリティ要件の反映状況や検証及び診断の結果などを確認することで、安全な機器をお客様にご提供する。



提供後のセキュリティ対策

- ファームウェア更新は自社の更新サーバから自動配信され、更新状況を管理。
- 電源断や未接続により未更新となった場合は、回線に接続された時点で更新が開始されるよう待機。

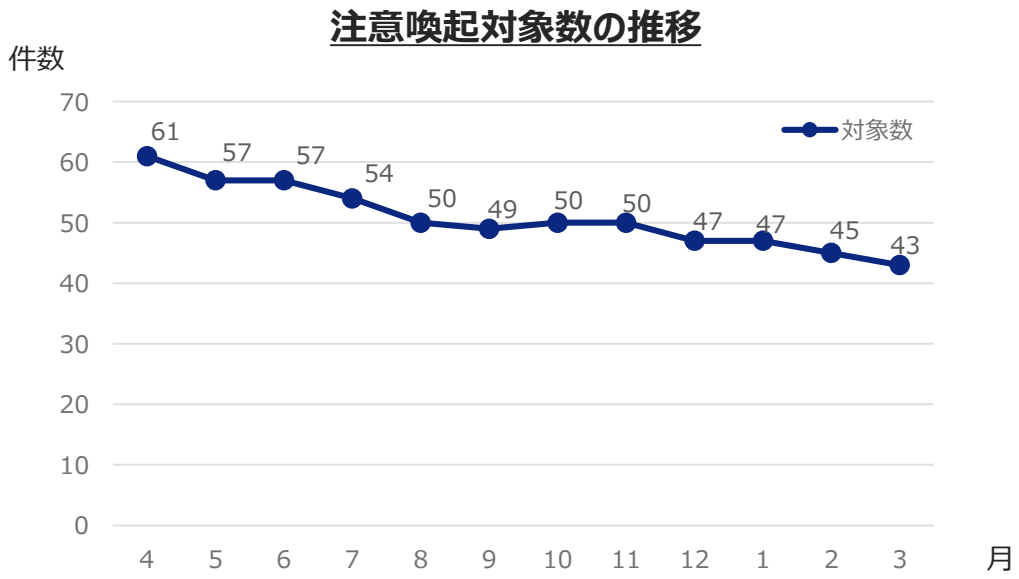


お客様への注意喚起

- **脆弱性を有する機器に関する注意喚起数は、減少傾向。**
- **対象者特定から問合せ対応までの一連の業務に要する負荷が大きい点が課題。**

注意喚起件数の推移

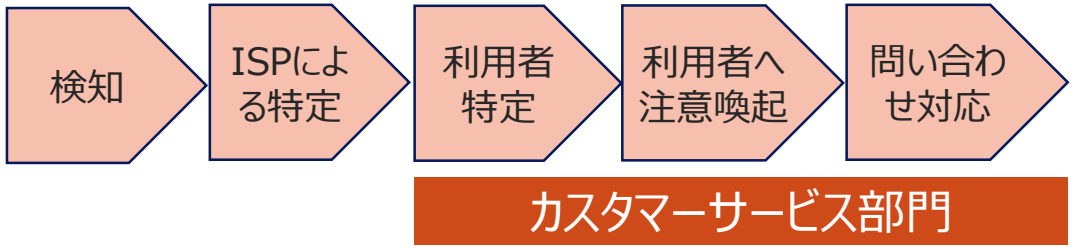
- 令和３年度におけるKDDIの注意喚起対象数567件(主に法人系のサービス)の内、注意喚起実施件数は327件。未実施のIPアドレスは卸先と対象外NW。
- 注意喚起対象数は日々減少している状況。



お客様注意喚起業務と現状の課題

- ICT-ISACから送付されるNOTICE及びNICTERのIPアドレスリストをもとにお客様を特定し、お客様に対してダイレクトメールを発送して注意喚起を実施。
- お客様特定から注意喚起までの業務に、相応の負荷がかかっている状況で、この負荷軽減も課題。

【注意喚起業務フロー】



Emotet注意喚起対応時の事例

- カスタマーサポート部門にて通常業務との輻輳により**リソース不足になり、緊急対応を要するEmotet注意喚起が対応不可**となった。
- 短期的かつスポット対応を分担し、**技術部門にてDM作成・送付などの臨時的な対応を実施**した。

端末の技術的条件、契約約款における規定

- **技術的条件では、端末設備のセキュリティに係る技術的な条件を明確化。**
- **契約約款で禁止行為/利用停止措置を規定しているが、利用停止適用は課題あり。**

技術的条件における記載

- 当社は、端末設備等のインターネット接続時の技術的条件として、サイバー攻撃の禁止と適切なアクセス制御を規定。

【インターネット接続サービス技術的条件】

（送信型対電気通信設備サイバー攻撃の送信の禁止）

第４条　データ伝送用設備端末等の送信型対電気通信設備サイバー攻撃（電気通信事業者がその業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録により送信元の電気通信設備が送信先の**電気通信設備の機能に障害を与える電気通信の送信の送信元であることを合理的に特定できるものに限ります。）の送信を禁止**します。

（識別符号の設定）

第５条　電気通信回線設備を通じて外部から制御可能な状態でデータ伝送用設備端末等を接続する場合は、他者から意図しない制御ができないよう、適切なアクセス制御が設定されていなければなりません。当該適切なアクセス制御とは、ID・パスワードの確認のみによるものの場合、次に掲げる要件のいずれにも該当するパスワードが設定されたものを指します。

一　**８文字以上**であること

二　**過去に不正アクセス行為に用いられたもの、一般的な単語を用いたもの、繰り返し又は連続的なもの**その他の**容易に推測されるもの以外**のものであること

契約約款における記載

- 契約約款の中では、禁止行為を定め、利用者の違反時の利用停止措置についても規定。**一方、脆弱性等を理由とした利用停止措置は、お客様のご理解を頂くことが難しい点が課題。**

【FTTHサービス契約約款】

第 30 条 当社は、基本契約者又は利用契約者が次のいずれかに該当する場合６ヶ月以内で当社が定める期間（そのＦＴＴＨサービスに係る料金その他の債務支払わないときは、その料金その他の債務が支払われるまでの間）、その**ＦＴＴＨサービスの利用を停止することがあります。**

・
・

（基本契約者又は利用契約者の禁止行為）

（１）通信の伝送交換に妨害を与える行為、その他自己以外の者の電気通信設備等の利用 若しくは運営に支障を与える行為又はそのおそれのある行為

・
・

（11）有害なコンピュータープログラム等を送信し、又は掲載する行為

（14）**その他法令又はこの約款等に違反する行為又はそのおそれのある行為**

ICT-ISACにおける情報共有活動

- **ICT-ISACの活動を通して他社のベストプラクティスを共有。**
- **社外組織とのサイバー演習を通じて、関連組織との情報連携体制を確認。**

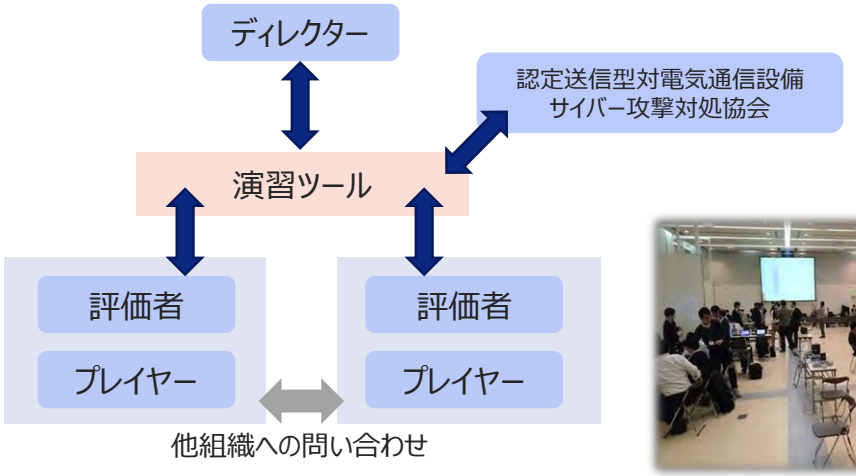
ICT-ISACにおける情報共有

- ICT-ISACの活動を通じて他社のベストプラクティスを共有
- 国内外のISACとの情報共有によりサイバーセキュリティ対策を連携

【インターネット接続サービス技術的条件】

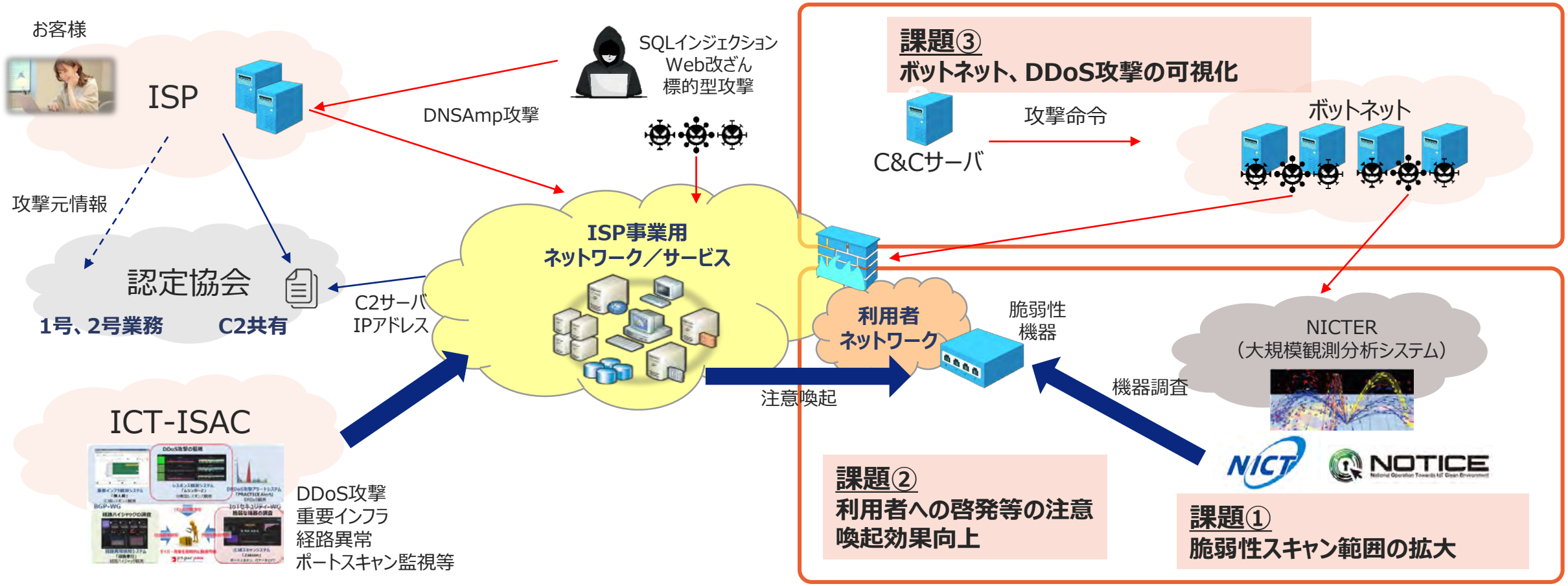
ICT-ISAC、NISCでのサイバー演習

- ICT-ISACやNISC等が主催する横断演習に参加し、社外機関とも連携して対処できる体制を確認。
- 各社との実戦的な演習を通じて情報共有体制を確認。



さらなるサイバー攻撃リスクの低減に向けた課題（1/2）

- **サイバー攻撃にはIoT機器の脆弱性、ボットネット、C2等全体俯瞰した対応が必要**
  - ✓ ランサムウェアなど様々な脅威が顕在化しており、脆弱性スキャン範囲の拡大も必要ではないか。
  - ✓ 加えて、利用者への分かりやすい啓発など注意喚起手法の工夫が必要ではないか
  - ✓ また、施策の効果測定としてボットネット、DDoS攻撃の挙動の可視化が必要ではないか。

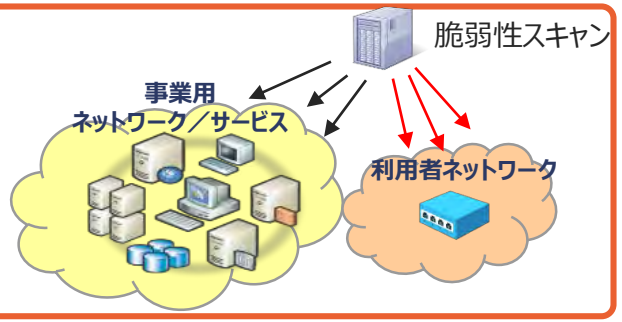


さらなるサイバー攻撃リスクの低減に向けた課題（2/2）

- 各課題については、参加プロバイダーの負荷を考慮しつつ検討を進める必要がある

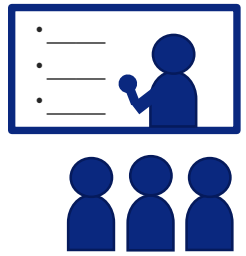
課題①
脆弱性スキャン範囲の拡大

- 事業用設備に対しては定期的に脆弱性スキャンを実施しているが、利用者の設備に対しても同様の脆弱性スキャンを実施することでソフトウェアの脆弱性も検知可能に。



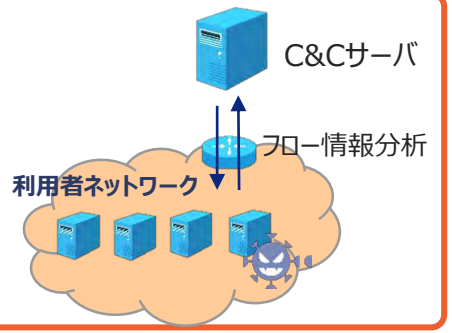
課題②
利用者への啓発等の注意喚起効果向上

- 検知された脆弱性への対応の必要性、手法について理解していただき、利用者の積極的な対応を促すため、利用者への啓発を含む広報面の注意喚起を強化。



課題③
ボットネット、DDoS攻撃の可視化

- 各種活動のPDCAを回していくために効果を測定し、検知できたC2やフロー情報分析により、ボットネットやDDoS攻撃の挙動を可視化。



Tomorrow, Together
KDDI
おもしろいほうの未来へ。
au

「つなぐチカラ」を進化させ、
誰もが思いを実現できる社会をつくる。

KDDI VISION 2030