IoT ネットワーク説明会　（代表的な Q&A 集）

国立研究開発法人物質・材料研究機構
マテリアル先端インフラ事業センターハブ

内容

1．NAT/NAPT にかかる事項

Q:　ネットワーク的に NAT の意味合いは何か.

⇨　IoT セキュリティデバイスの現状の技術的な制約上，デバイス内をパケットが通過する際に，送信先の IP アドレスがダイレクトに見えるようにしなければならないため，プロキシではなく NAT でお願いさせていただいています.

Q:　NAT をつけると外から見えなくなるのではないか

⇨　管理システム側から IoT セキュリティデバイスを見に行くことはしません．IoT セキュリティデバイスから管理システム側へ通信を送る形であり、アプリケーション側でデバイスを識別します.

Q:　NAT，NAPT の利用とあるが，動的でなく静的な NAPT でないといけないのか，それともどちらでもよいのか.

⇨　上記の通り、デバイス内をパケットが通過する際に，送信先（クラウド側）の IP ア

ドレスが分かればよいので，NAT/NAPT については静的でも動的でも構いません．

Q:　NAT は事業専用の NAT が必要か．すでに学内にある NAT をつかってよいか．

⇨　すでにある NAT でかまいません．事業専用である必要はございません．

Q:　大学内の PC（装置）についてはグローバル IP をもたせている．そのような場合は，NAT/NAPT が必要となるか．

⇨　上記の通り、デバイス内をパケットが通過する際に、送信先（クラウド側）の IP アドレスが分かればよいので、そのような場合には NAT，NAPT は必要としません．

2．セキュリティ・設置にかかる事項

Q:　ホワイトリストのブロック性について詳しい技術が知りたい．

⇨　大きく二つのブロック方法があります．一つは公開鍵暗号方式の技術（TLS）を使ったもので，クライアント認証とサーバー認証の両方を行っています．その認証が通らない場合にはブロックします．もう一つがホワイトリスト方式です．これは個別ファイアウォールに近いイメージで，送信元／送信先の IP アドレスやポートの制限をしています．それ以外の通信がきた場合にはアラームがたちあがるようになっています．

Q:　管理システムでのホワイトリストなどの管理は，各機関で行うのか．

⇨　管理システムは NIMS で契約して，ホワイトリストの設定などの管理はセンターハブとして NIMS が管理いたします．各機関には設置する制御 PC の IP アドレスなどのネットワークかかる情報をいただきますが，その設定や監視は NIMS 側で行います．

Q:　測定機器に IP アドレスが割り振られているネットワーク構成になっている．一台の PC に IoT セキュリティデバイスをつけることになると，ネットワーク全体の PC に

IoT セキュリティデバイスを設置する必要があるのか.

⇨ 基本は，同一ネットワーク内でセキュリティが確保されている PC（win10 など）であれば設置していただく必要はありません．セキュリティが確保されていない PC について本 IoT セキュリティデバイスを設置していただき，その IP アドレスをホワイトリストに登録して特定の通信ポートのみを通すことでネットワークにつなげることができるようになります.

Q: 1 台の装置にさえつければよいのか？

⇨ 事業で用いる共用装置 1 台につき 1 個を設置するもので，制御 PC と IoT のネットワーク情報をペアリングさせるものです．複数台の装置を登録する場合はには，それぞれの装置について IoT セキュリティデバイスを設置していただく必要があります．また，IoT セキュリティデバイスは本事業においては NIMS（センターハブ）から配布しますので，各機関からの購入は必要としません.

Q: IDS, IPS は双方向の通信（脅威）に対して動くものであるかであるのか，それとも片方向であるのか

⇨ 通信に関しては双方向です．エンドポイント側（制御 PC)からの拡散に対してもプロテクトするし，外部からのエンドポイントへの侵入も阻止します.

Q: 大学は一般的に FW が入っているが，CYTHEMIS は FW を乗り越えられるのか． IoT セキュリティデバイスのためだけの通信ポートを開ける必要があるか.

⇨ 通信については一般的に開けてあると思われる HTTP（80）と HTTPS（443）のみの利用ですので、特に追加で開けていただく必要はありません。(※)

※説明会では websocket のポートを必要とすることの言及を行いましたが，確認の結果，必要ないとのことで訂正をいたします.

Q: IoT セキュリティデバイスでの人の認証や，またはデータ送信についての制限はあるのか.

⇨ IoT セキュリティデバイスの管理システムそのものは人認証は行っていません．別に構築するデータ構造化システム側に人の認証・認可情報を持たせています.

⇨ データ容量についてはクラウド側（Microsoft Azure を想定）の制限で一回当たりの容量が上限 10GB となっています．それ以上のファイル容量のファイルについては Azure の制限であげることができないため，別の方法による登録を必要とします．それについては，別途，IoT ではない技術的な調整が必要となりますため，個別にご相談をする形となります．

Q: セキュリティアップデートのしくみ、頻度について

⇨ セキュリティアップデートの頻度は半年または年１回が予定されています．ただし、緊急更新については随時行います．アップデート適用は利用者と調整の上実施します。

⇨ IoT セキュリティデバイスから管理システムに定期的に通信が行われており、セキュリティアップデートなどがあった場合に自動的に更新が行われます．

３．レガシーOS への対応

Q: レガシーな OS を前提しているということであるが，最新の OS の PC についても装着しなければならないのか．

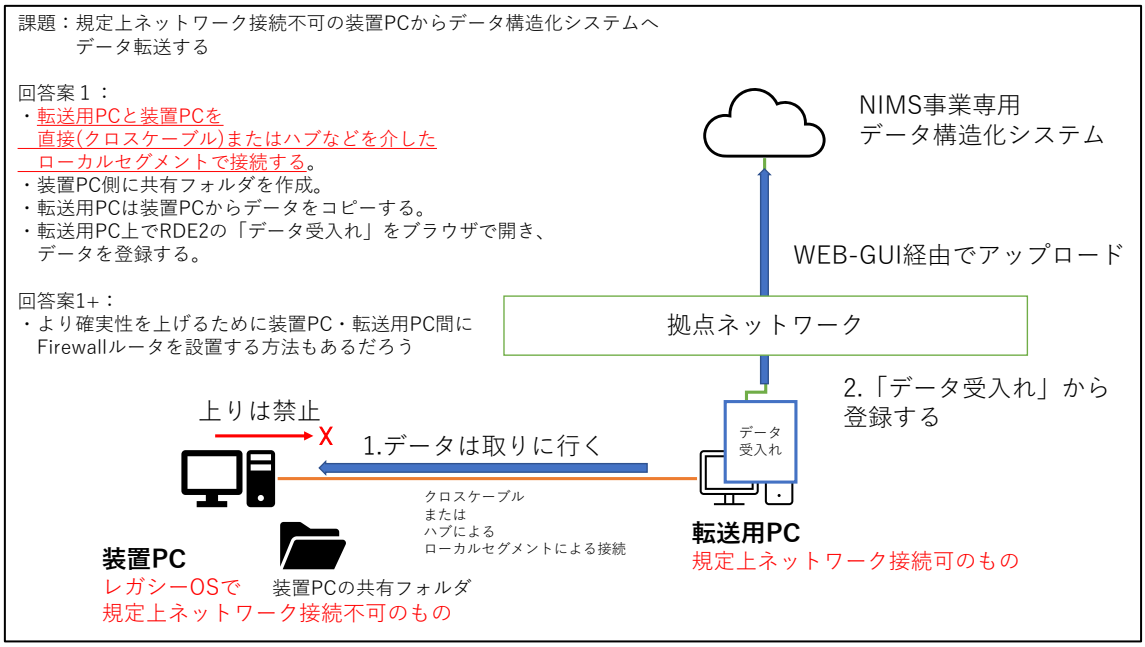
⇨ 最新の OS についても装着していただくことを推奨します．本事業では，登録していない別の PC に接続した場合にはデータがアップロードされないよう，よりセキュアな環境を構築したいと考えています．

Q: 測定装置の制御 PC では OS が XP のものがたくさんある．XP に IoT 設置するときに，クラウドに接続するときにブラウザを立ち上げるのか．

⇨ データを送るときにはブラウザを立ち上げることが前提となっています．次期クラウドデータ構造化システムでは，ブラウザは IE7 までは適正な表示や動作ができることを想定した設計としています．それよりも古いブラウザについては動作保証ができない（もしくは入力制限がかかる）可能性が高くなります．

⇨ このような場合，古い OS の機器から直接接続であげていただくよりも，最新の OS

をもつ中継 PC を設置していただき，その PC にデータを移送してから送っていただくことが確実です．



図： レガシーPC を転送用 PC（中継 PC）を介して構成する例

４．リモートとの併用にかかる案件

Q: 今回の事業においても外部利用を高めるために，遠隔操作（リモート）を活用したい．そのようなケースに対応できるか．

⇨ 事業そのものはリモート事業を要件とはしていませんが，同じ共用装置で他の事業でリモートが行われていることは認識しております．ただし，NIMS では IoT セキュリティデバイスをリモートとしては検証した実績は有していません．また，本事業では，同一の回線でリモートのような外から内の回線と，データ転送のような内から外への通信を同時使用は推奨いたしません．

Q: 遠隔利用の IoT セキュリティデバイスの利用においてはセキュアであるのか．

⇨ NIMS でこの IoT セキュリティデバイスによるリモート事業での検証はおこなっていません．共用装置を他の事業においてリモート事業でも併用している場合には，切り分けて運用をお願いすることになります．

５．その他

Q:　試用はいつから行われるのか

⇨　NIMS のテストは下半期から予定しています.そこで適合テストを行う予定います. その結果をもとに各機関への IoT セキュリティデバイスの配布を行い順次取り付けを進めたいと考えています. もちろん, 各機関で別事業において同様な計画があり,IoT セキュリティデバイスを独自でテストする分は,各機関でも進められます.

Q:　IoT セキュリティデバイスをとりつけた PC の統一ルールなどはあるか. 例えば NIC の２枚差しなどはルールをつくるのか.

⇨　事業としては個別の機関のネットワークポリシーに合致するかを個別に相談して確認をさせていただきながら進めたいと考えています. 各機関が OK であれば設置を進めさせていただきたく考えております.

Q:　IoT セキュリティデバイスの脆弱性が見つかった例があるのか

⇨　脆弱性がみつかった場合は管理システムからアップデートする機能を備えています.

Q:　ネットワークで障害があったとき,IoT セキュリティデバイスは自動復帰するのか. それとも何か操作が必要になるのか.

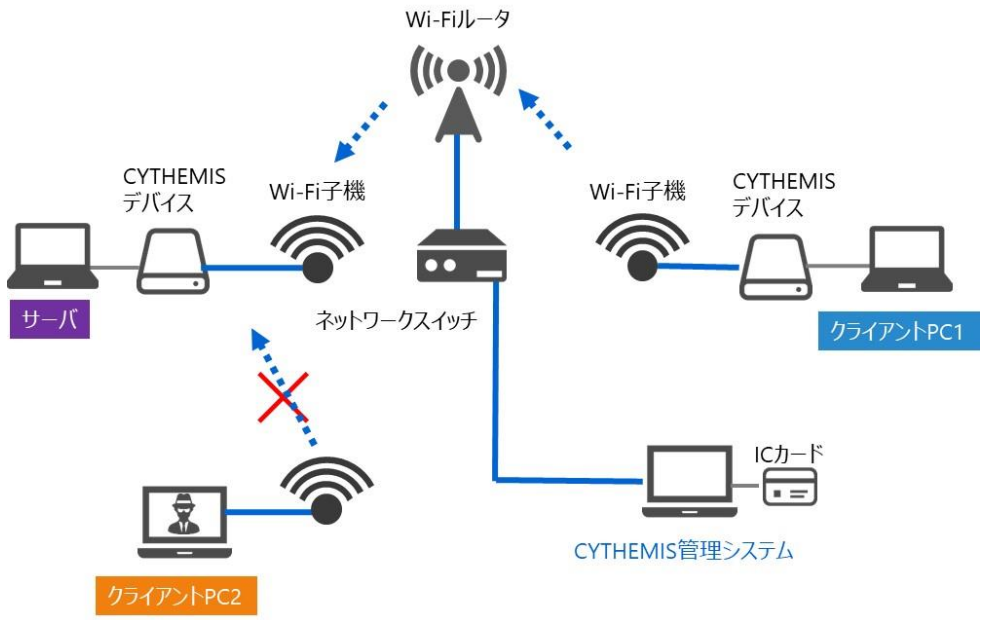
⇨　自動復帰する仕掛けとなっています. 必要に応じては IoT セキュリティデバイスの電源をリセットしていただくことがあります. 一方, ネットワークではなく, クラウドシステムがダウンしたときについては事例がないため, 今後の運用の中で個別対応をさせていただきたいと考えています.

Q:　IoT セキュリティデバイスはルーターなのか？

ルーティングはおこなっていなため, その意味ではルーター機能は備えていません.

Q:　セキュリティデバイスは無線利用可能か？

⇨　セキュリティデバイスそのものは無線通信機能をもっていませんが，LAN ケーブルを介して無線端末を接続させれば無線通信を構成できます.



図：　無線通信による構成例

Q:　CYTHEMIS から外部への通信は無線 LAN を通じても良いか？

⇨　外部への通信に無線 LAN を経由することは可能です. 上記の配線図を参照ください.

Q:　NIC を交換した場合利用可能か？

⇨　NIC 交換後に装置 PC の IP アドレスを同じに設定することで設定を変えずに継続利用可能です. ただし、ホワイトリストでソース側の指定を MAC ADDRESS にしている場合はホワイトリストの変更が必要となります.

Q:　転送速度（伝達速度）の 70 Mbps について

⇨ 現状はデバイスの仕様により 70 Mbps（実測値ベース）となっております．巨大ファイルなどの転送が見込まれる場合には，転送させる時間帯をずらすなどのタイムシフトの運用もご一考ください．

（参考：NIMS 内部では 10GB を超えるファイルの場合には業務規程の時間外，もしくは週末にご対応をいただくように運用側でルールを設けております）

発行：2021 年 7 月 30 日
改訂：2021 年 10 月 8 日

文責：国立研究開発法人物質・材料研究機構
マテリアル先端インフラ事業センターハブ　（担当：松波、登坂）