【ブロードバンドルーターの安全分析】概要説明

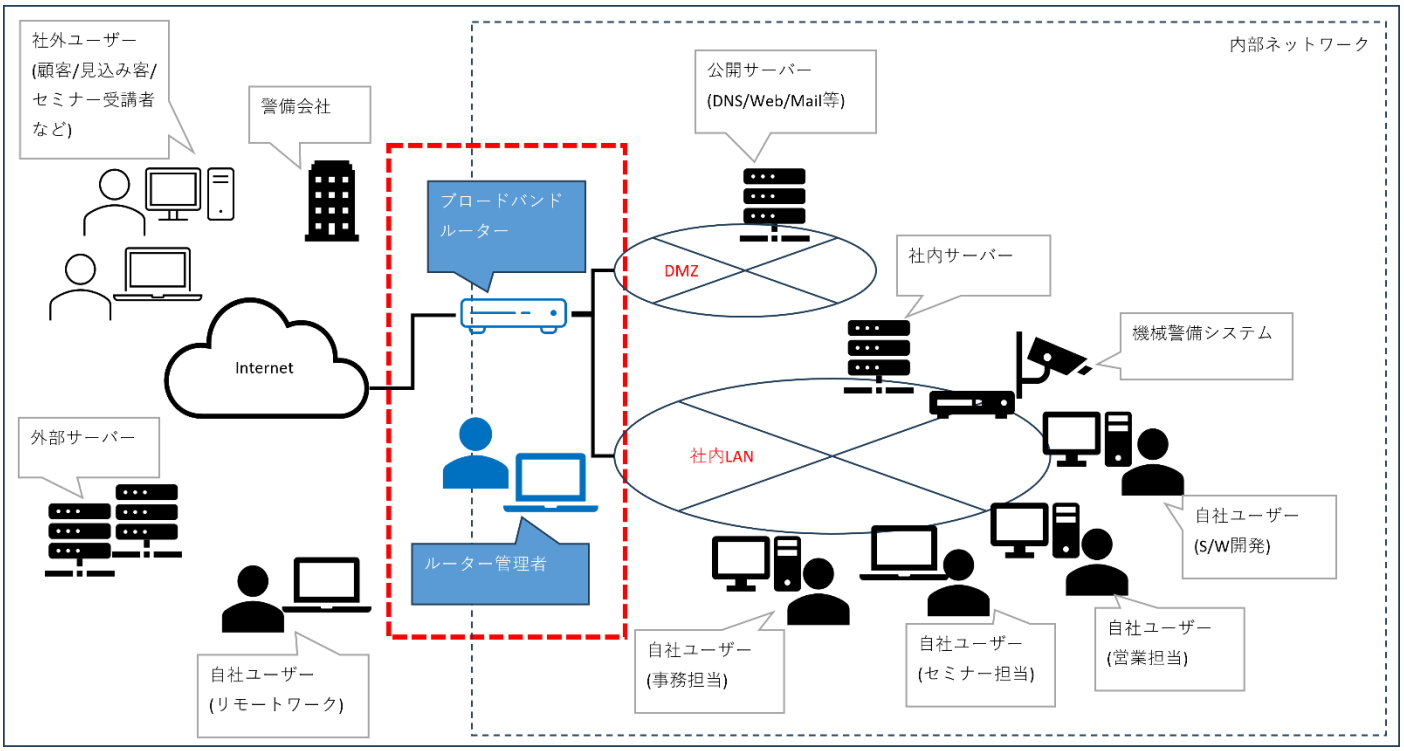
2025/7/22 作成

企業のネットワークに設置したブロードバンドルーターを対象として STAMP/STPA による安全分析を行うために想定したネットワークの概要を説明します。STAMP/STPA の学習を行い、その実践をトライするという位置づけで実施するものです。(有識者とのレビューにより、当初の分析をやり直したものになります。)

■分析対象とするネットワークの概要

一般的な企業の小規模ネットワーク構成を想定しました。このうちインターネットと内部ネットワークを接続する**ブロードバンドルーターとその管理者(下図の赤の点線で囲まれた部分)について**の安全分析を行います。

概要図：



・内部ネットワーク

DMZ には外部に公開するサーバーを接続して運用している想定としました。

社内 LAN には、社内向けの各種サーバー、自社内で業務を行うユーザー(例:ソフトウェア開発担当、営業担当、セミナー担当、事務担当等)の PC、機械警備用の装置といったものを接続して運用している想定としました。

社内のユーザーは、インターネット及び内部ネットワークを利用して日々の業務を行っている想定としました。業務の実施に際して、インターネットの利用が事実上不可欠となっています。

・外部(インターネット)

外部の関係者として、社外ユーザー(例:顧客、見込み客、セミナー受講者等)、リモートワークする自社ユーザー、社外の各種サーバー、警備会社(のサーバー)といった存在がある想定としています。

■概要図に登場する関係者の説明

1. ブロードバンドルーター

   インターネットと内部のネットワークを接続するブロードバンドルーターです。プロバイダとの接続を行ってインターネットを利用可能にします。また DMZ と社内ネットワークを異なるインタフェースで分離します。ファイアウォール機能で外部の攻撃から内部ネットワークを保護します。

   DNS、DHCP はブロードバンドルーターでは担当しないものとしました。インターネットからの VPN アクセス機能はブロードバンドルーターで実現するものとしました。

2. ルーター管理者

   ブロードバンドルーターの設置、保守・管理を行う担当者を想定しています。

3. 公開サーバー

   内部ネットワークの DMZ に配置してインターネット及び社内 LAN からのアクセスが可能なオンプレミスのサーバーです。提供するサービスとして Web、Mail、DNS 等を想定しました。

4. 社内サーバー

   社内 LAN からアクセス可能な各種サービスを提供する社内向けサーバーです。提供するサービスは、Active Directory サービス、DNS、DHCP、NAS、ソースコード管理、バグトラッキングシステム等を想定しました。社外からは直接アクセスできません。リモートワークする自社ユーザーは VPN 接続によりアクセス可能になる想定としています。

5. 外部サーバー

   レンタルサーバー事業者が貸し出しているサーバー上に構築したオンプレミスの代替となるサーバー(Web、Mail、DNS、NAS)を想定しました。クラウド上にあり、一定のセキュリティ対策が行われている想定です。

   また、グループウェア(例:Microsoft 365、Google Workspace 等)のサーバーもここに含みます。アプリケーション、Mail、オンラインストレージ等のサービス利用では一定のセキュリティ対策が行われている想定です。

6. 自社ユーザー

   自社ユーザーは、インターネット及び内部ネットワークを利用して業務を遂行する想定です。ソフトウェア開発担当、営業担当、セミナー担当(セミナーはオンラインで行う)、事務担当など各業務担当者があり、その業務実施に際してグループウェア、ファイル共有、ソースコード共有、調査・学習、AI サービス、Chat サービス、IP 電話等を利用することを想定しています。外部サーバーの設定管理を行う自社の担当者はここに含まれます。

   内部ネットワーク以外でリモートワークする社員も存在し、ブロードバンドルーターが提供する VPN サービスを利用して社内サーバーを利用することを想定しています。

7. 社外ユーザー

   社外ユーザーには、現在の顧客、今後商談を行い顧客となる可能性がある見込み客、開催するセミナーへの参加者といった関係者を想定しています。

8. 警備会社

   社内に機械警備システムを設置していた場合に通報する先の警備会社を想定しています。これは社外に存在する関係者の例として挙げたものです。

■要求仕様

ブロードバンドルーターとルーター管理者における管理作業に関する要求事項を以下に示します。

※ブロードバンドルーターとルーター管理者の責任範囲に

1. ルーター管理者はブロードバンドルーターがインターネット接続を維持するよう、日々その適切な管理に努めること。
2. ブロードバンドルーターへの管理者ログイン(WebUI、VTY 接続)は、社内 LAN(VPN 接続した端末を含む)の端末に制限すること。また、適切なセキュリティ強度を確保すること。
3. ブロードバンドルーターはファイアウォール機能を用いて DMZ 及び社内 LAN の各セグメントに対して保護を行うこと。
4. ブロードバンドルーターは DMZ 及び社内 LAN の各セグメントに属するサーバーや PC 等の機器がインターネットと通信できる環境を提供すること。
5. ブロードバンドルーターは事前に登録した自社ユーザーに対して適切なセキュリティ強度を確保した VPN 接続サービスを提供し、社内 LAN へのアクセスを可能にすること。
6. ブロードバンドルーターは動作ログを保持し、必要に応じて適切に保存する設定とすること。
7. ブロードバンドルーターは異常を検知した時は、設定に従いメール送信や WebUI による表示等の手段を用いてルーター管理者に通知すること。
8. ブロードバンドルーターは長期の連続稼働に適した環境に設置して運用すること。(予め温度・湿度、無停電電源、サージ防止、安定して設置できる施錠可能なラック内などの条件を設定する。)

※ブロードバンドルーターとルーター管理者の範囲に分析範囲を制限する前提のため、それ以外のステークホルダーに関係する要求は記しません。

■前提条件

安全分析をブロードバンドルーターとルーター管理者の範囲に制限して行うため、以下の前提条件を追加します。

1. ネットワーク回線(インターネットに接続するための光回線、内部 LAN 回線)と関連する機器(ONU やネットワーク HUB)については不具合が発生しないものとする。インターネット回線は 1 経路のみとする。
2. ブロードバンドルーターのメーカーは脆弱性や不具合に対応したファームウェアを適切に提供しているものとする。
3. ブロードバンドルーターを含む設置機器の自然故障や EOL については検討の対象外とする。
4. 地震、水害、火災、電力会社の停電事故、放射能汚染、などの災害のために機器の破損・故障の発生、インターネット接続の長時間停止の発生は、検討の対象外とする。

【補足】

1 については、インターネット回線側の問題によりインターネット接続が切断した場合は自社で回復することが困難な問題であり、対策としてはインターネット回線の多重化となりますが、前提としてインターネット回線は 1 経路のみとしているため、検討の範囲外とします。

2、3 については、ブロードバンドルーターや周辺の機器が自然に故障しないこと、メーカーサポートが有効であること、脆弱性や不具合に対する対応が継続していることを前提として安全分析を行います。

4 については、自社の責任の範囲外である天災・人災が発生した場合は要求仕様を満たせなくとも問題ないという判断です。

■分析対象について

最初はネットワーク管理の安全分析として組織全体の安全分析を行うことを考えていましたが、全てのステークホルダーについての損失・アクシデントを定義して安全分析を実施するのは STAMP/STPA の実践のトライとするには分析の規模がかなり大きくなることが考えられたため、**ブロードバンドルーターの損失・アクシデントに制限**する方針としました。

セキュリティとセーフティの観点から以下の損失・アクシデントを想定しました(レビューの経過に従い当初の分析とは異なる損失・アクシデントになっています)。

【損失・アクシデント表】

番号	損失・アクシデント
1	**インターネット接続が長時間停止する。(停止時間は T.B.D)**
2	**ブロードバンドルーターが起動不能になる。**
3	**ブロードバンドルーターより火災の危険が発生する。**
4	**ブロードバンドルーターの設定情報が漏洩する。**
5	**内部ネットワークへの不正アクセスを許す。**
6	**外部への攻撃の踏み台として利用される。**

インターネット接続が失われた際の損失基準となる停止時間は”長時間”としましたが、組織により許容できる時間は異なる考え、定量化せず”T.B.D”と表現しました。

この損失・アクシデントよりハザード、制御構造の定義、UCA(Unsafe Control Action)、安全制約を抽出します。そして HCF(Hazard Causal Factors)を特定し、対策を立案します。

【ご注意】

上記全ての損失・アクシデントに対して対策まで分析しておりません。

STAMP/STPA 安全分析のトライの一例として、損失・アクシデントの一部に対して対策まで実施しております。

複雑システムにおいて、各コンポーネント間の安全維持制御の乱れが、想定外の事象によるシステム全体の安全制約の逸脱になるとされており、これを分析する手法が STAMP/STPA です。本来はネットワークシステム全体の安全分析を行う必要があります。コンポーネント間の安全維持制御を含んだ全体の安全分析は今後の課題とします。

■STAMP/STPA とセキュリティについて

前述した損失・アクシデントにはセーフティの問題だけではなくセキュリティの問題が含まれています。セーフティで発生した問題（設定ミス）がセキュリティの問題（攻撃者による攻撃を受けてしまう）に発展することを検討したためです。

本来、STAMP/STPA は安全性分析のために開発された手法のため、セキュリティ分野への適用は可能ではあるが、工夫が必要であるなど課題があるとされています。

セキュリティ分野へ適用するために STPA を拡張した「STPA-Sec」、「STPA-SafeSec」が提唱されており、本来であれば前述したブロードバンドルーターとルーター管理者の安全分析のセキュリティ分野のアクシデントもそのような手法で分析すべきと考えられます。

有識者とのレビューでは、「STPA 教材としてはセキュリティ問題を除外すべき」とのご指摘をいただいておりました。

有識者とのレビュー時に、分析を行って得られる対策は従来から言われているような一般的なものしか導出できないのではないか、と指摘されていました。確かにブロードバンドルーター単体のセキュリティの問題については STAMP/STPA 分析をするまでもなく一般的なセキュリティ対策を行うことで十分となると思われます。

しかしながらセーフティの問題（設定の不備を含む設定ミス）がセキュリティの問題に発展することはルーター管理者にとっては大きな問題となるのが現実だと考えます。その文脈を踏まえ、当たり前のことであっても敢えてそのまま損失・アクシデントとして記載するものです。

参考文献：

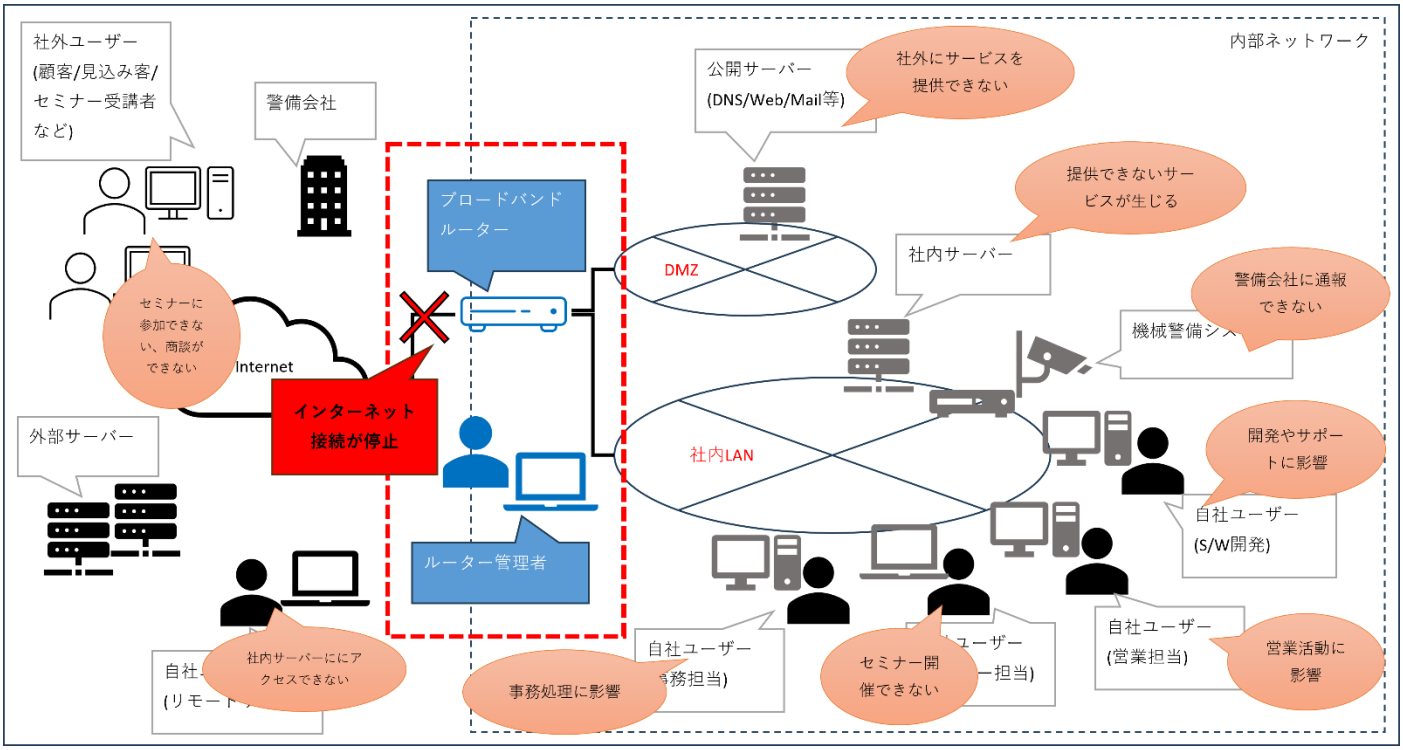
STAMP 海外事例の紹介： STPA-SafeSec（岡本 圭史先生 岡野 浩三先生）
https://www.ipa.go.jp/archive/files/000064390.pdf

■「インターネット接続が長時間停止する」を損失・アクシデントとする考えについて

STAMP/STPA の安全分析では、避けるべき望ましくない結果を**損失・アクシデント**とします。有識者とのレビューのやりとりでは「インターネット接続が長時間停止する」では具体的な損失・アクシデントとなっていないとの御指摘をいただきました。

そこで、ブロードバンドルーターが原因で「インターネット接続が長時間停止する」とステークホルダーに生じる損失・アクシデントを検討してみました。

【ステークホルダーに生じる損失・アクシデントの例】



公開サーバー：インターネットにサービス(DNS/Web/Mail 等)を提供できなくなる。

社内サーバー：インターネットを利用して提供する社内向けサービスが利用できなくなる。

外部サーバー：社内ネットワークからグループウェア、Mail、ファイル共有等のサービスを利用できなくなる。

自社ユーザー(ソフトウェア開発担当)：開発作業、サポート作業等に影響が出る。

自社ユーザー(営業担当)：顧客、見込み客への連絡や商談といった営業活動に影響が出る。

自社ユーザー(セミナー担当)：開催予定のオンラインセミナーが開催延期や開催中止になる。

自社ユーザー(事務担当)：インターネットを利用した受発注業務、連絡業務、会計業務等に影響が出る。

自社ユーザー(リモートワーク)：社内サーバーにアクセスする必要がある業務を実施できない。

社外ユーザー：自社とのオンラインセミナー参加、商談、の連絡・依頼ができなくなる等の影響が出る。

機械警備システム：異常が発生した場合の通報処理ができず、損害が発生・拡大する場合がある。

警備会社：機械警備システムからの通報を受けられなくなり、異常が合った場合に対応できない、対応が遅れる等の影響が出る。

会社全体：業務を予定通りに行えないなどの影響が出て会社全体の信用毀損を招き、経営不振を招く。

上記のように自社の業務に影響が発生し、金銭的な損失が発生する場合があり、最終的には会社としての信用が毀損・喪失へと繋がっていくことが考えられます。

STAMP/STPA 分析では、損失・アクシデントを具体的に想定することが具体的な対策を引き出すために重要になります。会社全体を分析範囲とすると「インターネット接続が長時間停止する」だけではなく、各ステークホルダーの損失・アクシデントを想定する必要があります。

しかし今回は STAMP/STPA の実践のトライという位置づけのため、ブロードバンドルーターとルーター管理者の責任の範囲で想定される損失・アクシデントに制限した分析とする方針でした。

ブロードバンドルーターとルーター管理者にとっては「インターネット接続が長時間停止する」ことが損失・アクシデントであるとして分析します。

また、各ステークホルダーに生じる損失・アクシデントはステークホルダー毎の安全分析、また会社全体の安全分析で論ずることとして今回の分析からは除外します。これらは今後の課題とします。

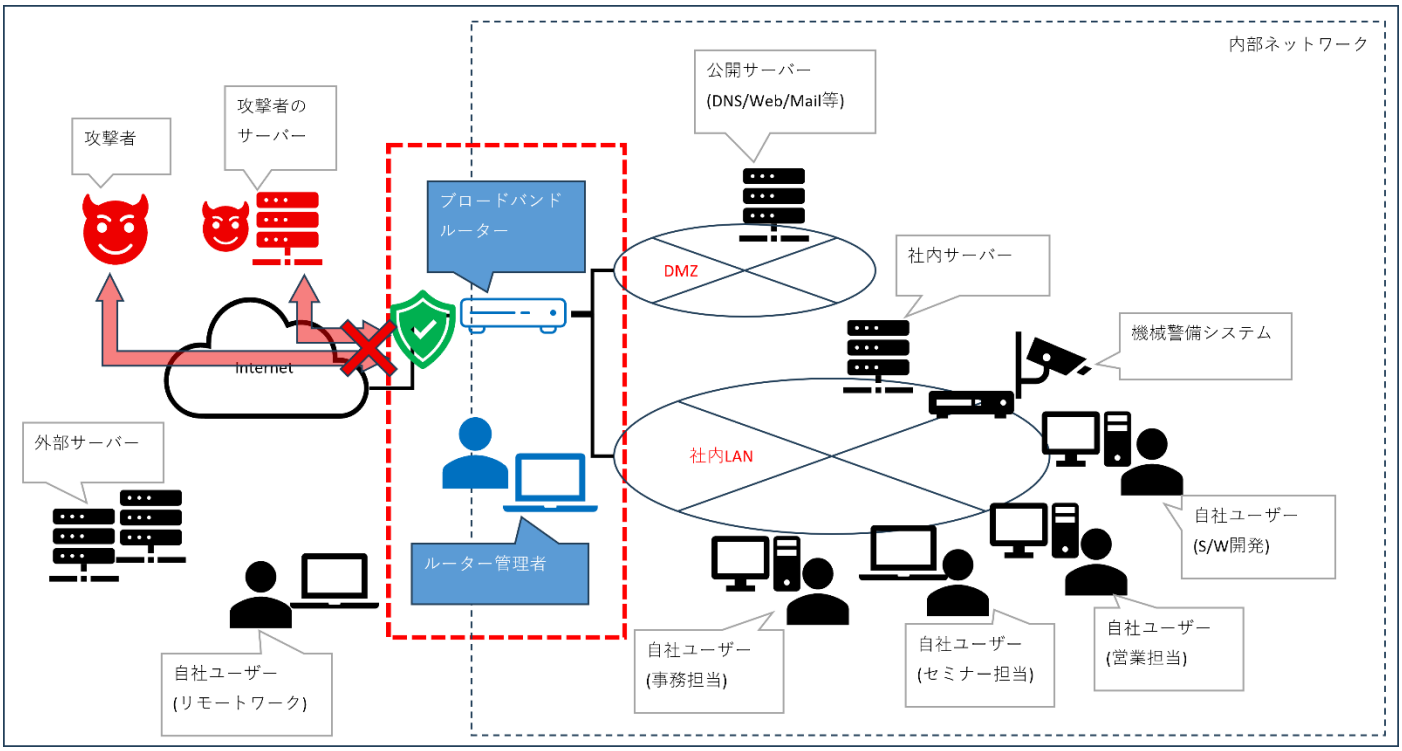
■「内部ネットワークへの不正アクセスを許す」場合の損失・アクシデントについて

前述の『「インターネット接続が長時間停止する」を損失・アクシデントとする考えについて』で、各ステークホルダーに生じる損失・アクシデントを検討しました。

同様にブロードバンドルーターが「内部ネットワークへの不正アクセスを許す」場合に、ブロードバンドルーターで発生したアクシデントの影響を受けて各ステークホルダーに生じる損失・アクシデントを検討してみます。

※セキュリティ問題であるため、本来であれば STAMP/STPA の適用には課題があります。

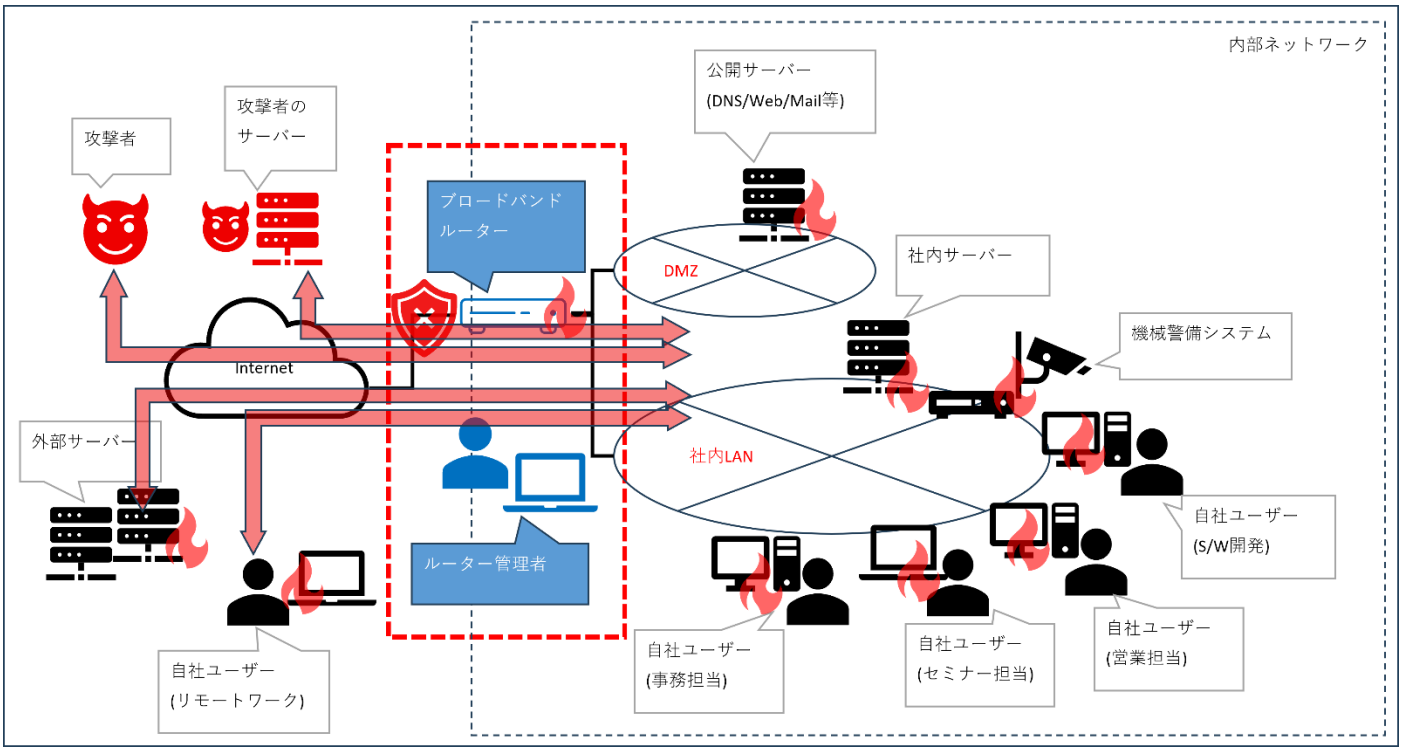
【ブロードバンドルーターが内部ネットワークへの不正アクセスを許していない状態】



ブロードバンドルーターは、一般的に言われるファイアウォール機能を用いて外部から内部ネットワークへのトラフィックをルールに従って制限を行います。

ファイアウォール機能が意図した設定のとおりに働いている場合、内部ネットワークは外部の攻撃者、攻撃者のサーバーから直接の攻撃を受けないようになっています。

【ブロードバンドルーターが内部ネットワークへの不正アクセスを許す状態】



ブロードバンドルーターの、ファイアウォール機能が有効に働いていない場合、内部ネットワークへのトラフィックが制限されず内部ネットワークの機器（ブロードバンドルーターの内部ネットワーク側インタフェース、公開サーバー、社内サーバー、自社ユーザーPC）に到達した場合、外部からの不正アクセスや攻撃を受ける可能性が高まります。また、外部から不正アクセスや攻撃を受けた機器が踏み台となって内部・外部への不正アクセスや攻撃に利用されることにより被害が拡大する可能性があります。ゼロトラスト環境ではない場合、内部からの不正アクセス・攻撃に対して脆弱であることがあり、組織全体への被害拡大につながる可能性が推測できます。

各機器への不正アクセス・攻撃により発生する損失・アクシデントを検討してみます。

1. 機器にマルウェアが感染する。
2. 機器にランサムウェアが感染し、ファイルを暗号化され身代金を要求される。
3. 機器から機密情報・個人情報が漏洩する。
4. 攻撃の踏み台になる。
5. 業務への影響が出る。

上記により、具体的な損失・アクシデント(業務への影響、金銭的損失、会社の信用毀損・損失)に繋がる可能性があります。

但し、損失・アクシデントが発生するのは不正アクセス・攻撃を受けた機器側にセキュリティ対策の不備や脆弱性が存在し、**不正アクセス・攻撃が成功した場合に限ります**。

前述の通り、今回は STAMP/STPA の実践のトライという位置づけであり、ブロードバンドルーターとルーター管理者の責任の範囲で想定される損失・アクシデントに制限した分析とするため、各ステークホルダーに生じる損失・アクシデントはステークホルダー毎の安全分析、また会社全体の安全分析で論ずることとし、今回の分析からは除外します。

具体的な損失ではない「ブロードバンドルーターが内部ネットワークへの不正アクセスを許す」が、ブロードバンドルーターとルーター管理者にとっては損失・アクシデントであるとして分析します。