通信ネットワーク機器セキュリティ
ユーザーガイドライン　Ver. 1.0

2019年3月29日

一般社団法人　情報通信ネットワーク産業協会

通信ネットワーク機器セキュリティ委員会

【目　次】

第 1 部　共通事項

1.1 適用範囲と目的

1.1.1　背景/前書き

繋がることによる利便性の向上から、インターネットは急速に普及し、IoT 社会へのシフトも加速しています。その結果、従来は通信ネットワーク機器を扱う必要のなかったユーザーが、当該機器の設定/運用を行う状況に直面し、特に、セキュリティ対策に必要な対応の不備によるサイバー攻撃の被害が顕在化してきています。

1.1.2　ガイドラインの適用範囲と目的

こうした状況の中、情報通信ネットワーク産業協会（CIAJ）は、インターネット、IoT を構成する通信ネットワーク機器提供者の業界団体として、適切なセキュリティ対策機能の提供を考察していくと同時に、当該機器ユーザーを対象に、通信ネットワーク機器のセキュリティ対策機能の取り扱いに関して、その必要性をご理解いただき、適切な設定/運用を実施頂くため、本ガイドラインを策定しました。

1.1.3　ガイドラインの構成

本ガイドラインでは、第 1 部で、通信ネットワーク機器共通の事項について、第 2 部以降で、機器個別の事項について説明します。

第 1 部（本部）では、ほとんどの通信ネットワーク機器の設定/運用において必要となる“パスワードの管理（1.2)”、“ファームウェアの最新化（1.3)”、及び“ログ管理（1.4)”の 3 項目について、必要性（考え方）を解説します。

尚、第 2 部以降は、時代の変化に伴い、機器の追加や内容を改版して行くことを想定しています。

1.2 パスワードの管理

通信ネットワーク機器には、機器の設定を変更するための機能が用意されていることが多く、それらの機能を悪用することで、攻撃者が外部ネットワークから機器の設定を変更し利用者の意図しない動作をさせることや、機器によっては OS のコマンド等の実行が行われる可能性があります。

これらの機能の攻撃者からの不正利用を防ぐため、一般的に認証機能を設け正当な利用者以外のアクセスを制限するセキュリティ対策が行われており、認証機能の中でも ID・パスワードによる認証が多く利用されています。ID・パスワードによる認証は、適切に運用管理されていれば、攻撃者からの不正アクセスを防ぐのに有効ですが、近年 ID・パスワー

ド認証機能の運用管理が不十分で、通信ネットワーク機器が攻撃されるケースが増加しています。

攻撃者からの悪用を防ぐため、通信機器の利用者は ID・パスワード認証機能の運用管理について、注意する必要があります。

① 機器の利用開始時に、機器のデフォルトパスワードを変更する。

② 容易に推測できるパスワードは避け、アルファベット数字記号等を含む適切な長さのパスワードを機器ごとに設定する。

③ 他機器・システムと同じ ID・パスワードは利用しない。

④ 設定したパスワードを適切に管理し、他人に教えたり、他人の目に触れる場所にメモ等で残さない。

以前は、定期的にパスワードを変更することが推奨されていましたが、定期的にパスワードを更新することで、安易で規則的なパスワードになってしまう、パスワードの使いまわしが多くなる、といった問題があるため、最近は機器ごとに強固なパスワードを設定し、定期的な更新は行わないということが推奨されています。ただし、異常に気が付いた場合や異常な挙動が疑われる場合は機器の状態確認と合わせ、パスワード変更の必要があります。

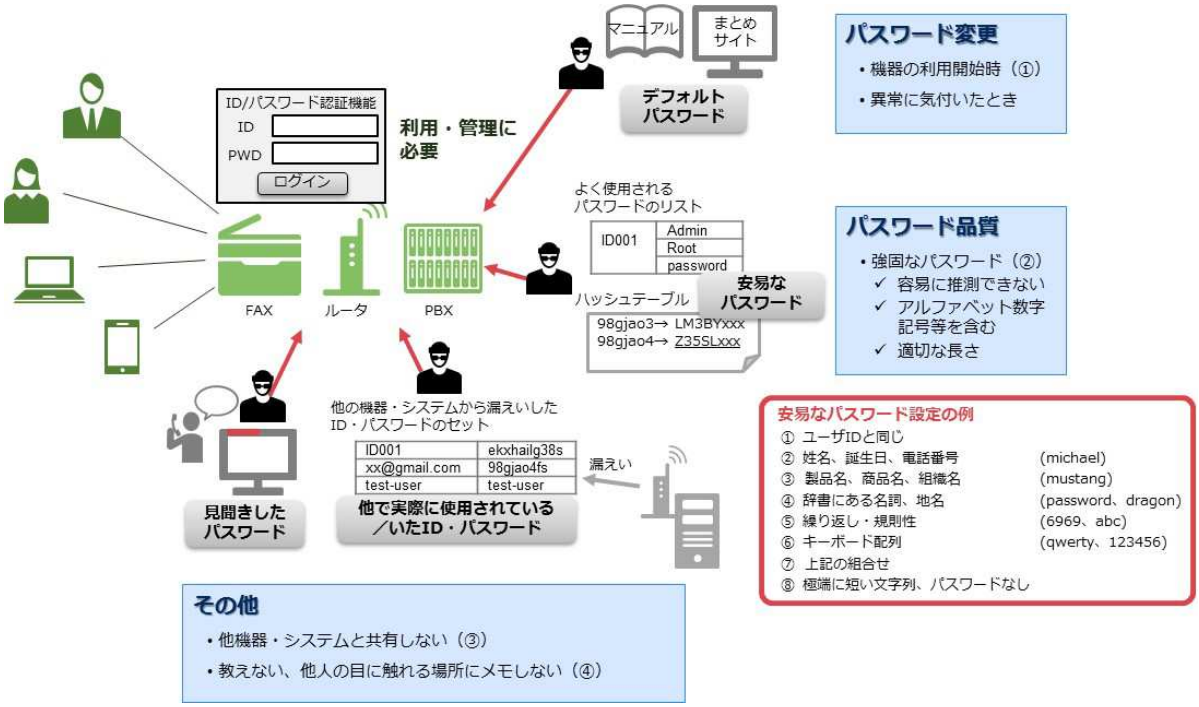


図 1-1 パスワードの管理

1.3 ファームウェアの最新化

IoT に脆弱性が存在すると、攻撃者にとって絶好の標的となり得ます。従って、脆弱性への対応（脆弱性対策）として、ソフトウェア（ファームウェア）を最新化して脆弱性か

ら守ることが重要です。
本節では、運用段階における脆弱性への対応の留意点を示します。

1.3.1 導入段階

機器を運用中に、その機器のソフトウェア（ファームウェア）に脆弱性が発見された場合、アップデート機能がなければ、その機器を継続して使用するとサイバー攻撃をうけるリスクがあります。このため、機器選定においては、ソフトウェア（ファームウェア）のアップデート機能を有する製品から選定することが望まれます。

また、機器を設置する際、ソフトウェア（ファームウェア）が最新かどうかを確認し、古い場合は最新化してから使用開始することが望まれます。

1.3.2 運用段階

機器の設置者や保守者、機器を導入してシステムを運用する運用者や保守者は、用いている機器に対して、ソフトウェア（ファームウェア）を最新化して脆弱性から守ることが重要です。

ソフトウェア（ファームウェア）の最新化に当たっては、以下の対策を事前に組織として定め、定期的に継続して取り組むことが重要です。

① 機器のソフトウェア（ファームウェア）更新手順を定め、その手順に従い実施する。その手順は必要とする関係者に対して、閲覧可能とする仕組みを提供する。

② 各機器へのソフトウェア（ファームウェア）更新は、履歴が閲覧可能な方法にて管理を行う。

③ ソフトウェア（ファームウェア）更新に対しては、事前にバックアップ方法を定めることや、テストで動作確認した後、実働システムへ適用する。

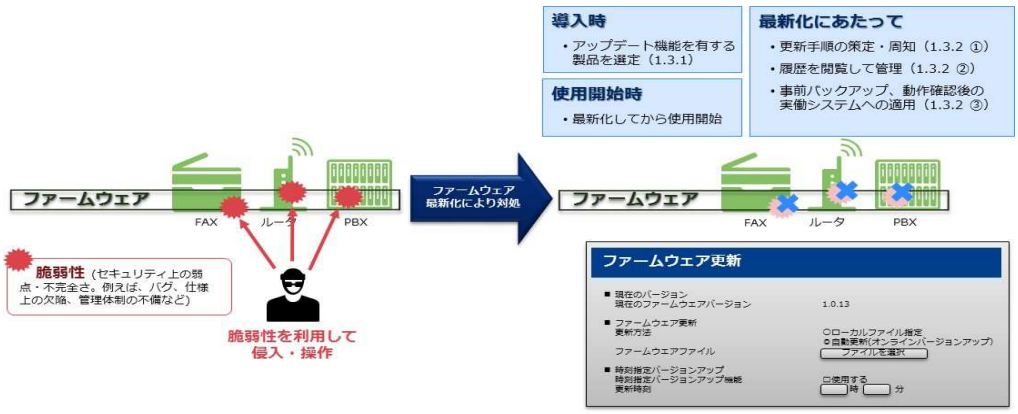


図 1-2 ファームウェアの最新化

1.4 ログ管理

ログにはセキュリティ機能の成功・失敗などを記録するセキュリティログと、それ以外の機器の動作（例えば通信履歴など）を記録する動作ログがあります。

ログ管理とは、システムやサービスを構成する通信ネットワーク機器で発生する事象のうち、特定の事象をログとして記録・保存・保護したり、ログを元に異常な事象・予兆を通知したりするセキュリティ対策です。

適切なログ管理を実施することで、悪意ある第三者等からの不正侵入、不正操作等の情報セキュリティインシデント及びその予兆を検知し、その原因究明を行うことができます。また、組織の利用者による不正行為を抑止する効果も期待できます。

通信ネットワーク機器の管理者（利用者）が適切にログを管理するためには、「1.4.1 導入時」、「1.4.2 運用時」、「1.4.3 廃棄時」、それぞれのタイミングで以下の要件を満たす必要があります。

1.4.1 導入時

通信ネットワーク機器を購入する際、機器の機能としてログ取得や閲覧、保存する機能や時刻同期機能、設定やログデータの削除機能を持つ製品から選択することが望まれます。また、そのような機能を持つ通信ネットワーク機器を設置する際、時刻同期の設定やログ取得、保存に関して設定する必要があります。

保存

① 機器の出荷時設定ではログを取得・保存するよう設定されていない場合があるため、導入時に取得・保存するよう設定する。

② 機器のリソースには限りがあるため、ログのサイズが必要最小限となるよう保存必要な事象のみ保存するよう設定する。

時刻同期

③ 公開 NTP サービス、または組織内の NTP サーバーと当該機器の時刻を同期させるよう設定する。

1.4.2 運用時

通信ネットワーク機器の運用中は定期的に 1.4.1 で設定したログを以下のような観点で確認する必要があります。

① 管理外のインターネット接続がないか。

② 許可なく接続された機器や無線 LAN 機器はないか。

③ 不審な通信が行われていないか。

④ 不正な操作が行われていないか。

定期的な確認で異常を検出した場合、予め決められたインシデント発生時に関する手順に従って対応する必要があります。場合によっては、機器ベンダのサポート窓口や公的セ

キュリティ機関へ連絡することも必要となります。

また、通信ネットワーク機器に保存可能なログのサイズには限りがあるため、消失やログ保存停止を予防するために定期的にバックアップ（別のデバイスに保存、ログサーバーに転送等）する必要があります。

1.4.3 廃棄時

通信ネットワーク機器を廃棄する際、ログ情報などからの情報漏えいを防止するため、機器の設定項目や蓄積されたログ情報を消去または工場出荷時状態に初期化してから廃棄する必要があります。

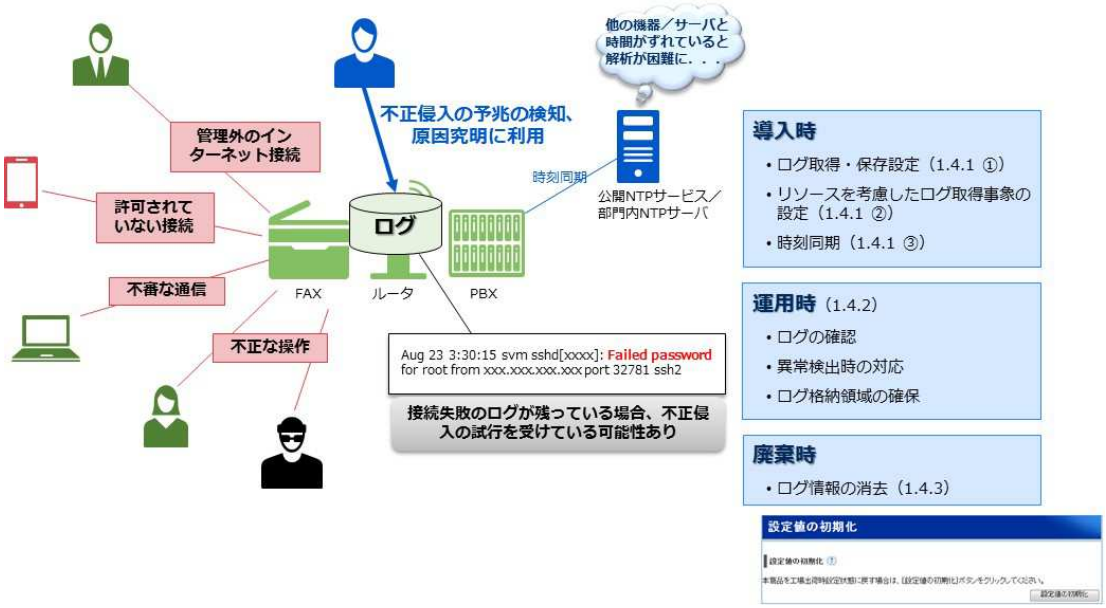


図 1-3 ログ管理

1.5 参照文書

・独立行政法人情報処理推進機構（IPA），「増加するインターネット接続機器の不適切な序情報公開とその対策」 https://www.ipa.go.jp/files/000036921.pdf

・独立行政法人情報処理推進機構（IPA），「つながる世界の開発指針」の実践に向けた手引き　IoT 高信頼化機能編 https://www.ipa.go.jp/files/000059278.pdf

・総務省,国民のための情報セキュリティサイト 「ID とパスワード」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01.html

・独立行政法人情報処理推進機構（IPA），「IoT 開発におけるセキュリティ設計の手引き」 https://www.ipa.go.jp/files/000052459.pdf

・IEC62443-2-1（CSMS 認証基準）

・内閣サイバーセキュリティセンター（NISC），府省庁対策基準策定のためのガイドライン（平成 28 年度版） https://www.nisc.go.jp/active/general/pdf/guide28.pdf

・米国国立標準技術研究所（NIST），SP 800-92 コンピュータセキュリティログ管理ガイド https://www.ipa.go.jp/files/000025363.pdf

・コモンクライテリア承認アレンジメント（CCRA），情報技術セキュリティ評価のためのコモンクライテリア パート 2: セキュリティ機能コンポーネント バージョン 3.1 改訂第 5 版
https://www.ipa.go.jp/security/jisec/cc/documents/CCPART2V3.1R5-J1.0.pdf

第 2 部　PBX

2.1 背景

2015 年頃より、IP（Internet Protocol）電話端末を他社に不正利用され、多額の国際電話料を請求される問題 [1]が発生しています。総務省は 2015 年 6 月 12 日に IP 電話の利用者およびシステムの開発企業、事業者に対して注意喚起 [2]を発表しました。IP ネットワーク上で音声を伝送する VoIP（Voice over Internet Protocol）技術を用いた IP 電話システムや IP 電話サービスは、2000 年初頭頃より実用化されています。2010 年前後より利用者も増え、現在は利用者も 2000 万人を越え、普及期に入ったと言えるでしょう。そのため、IP 電話システムがインターネットでのセキュリティ脅威にさらされるケースが増えてきたと考えられます。IP 電話システムは、ネットワークインタフェースに IP を使用するもののシステムの機能や形態は従来の電話端末や PBX、ボタン電話システムと変わりません。そのため、インターネットシステムでは当たり前のセキュリティ対策や運用上の留意事項が見逃されているため、不正利用などの問題が発生しているケースもあるようです。

2.2 定義

VoIP システムの基本構成を図 2-1 に示します。VoIP システムの多くは、SIP（Session Initiation Protocol）という手順に従っています。SIP では、VoIP システムに接続する IP 電話端末を SIP サーバーに登録します。登録時には、使用する電話番号と IP アドレスを対応付けます。このことにより、電話の発信をする場合に、相手先の電話番号から接続する IP 電話端末の IP アドレスを見つけることが出来ます。

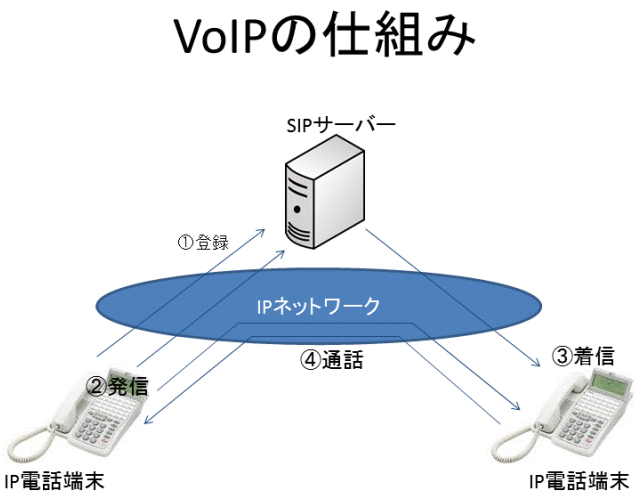


図 2-1 VoIP システムの基本構成

VoIP システムには、製品の特徴によりいくつもの形態があります。基本的な種類を図 2 に示します。

SIP サーバーは、汎用のサーバーに VoIP 機能をソフトウェアで実装したものです。IP 電話端末は、ルーターやスイッチを介して IP ネットワークに直接接続します。アナログ電話端末や公衆電話網への接続は、VoIP ゲートウェイを介します。

IP-PBX や IP ボタン電話は、従来の PBX やボタン電話システムに IP 電話端末を直接収容することが出来る交換システムです。

VoIP ゲートウェイは、アナログ電話端末や公衆電話網などを IP ネットワークに接続するための変換装置です。

IP 電話端末は、見た目は従来の電話機と同じですが、IP ネットワークインタフェースを有する端末です。

VoIPシステムの種類

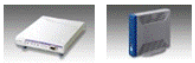
区分	システム	主な機能
VoIPサーバー	SIPサーバー 	IP電話端末の管理、端末間での呼制御を行う
	IP-PBX／ボタン電話 	IP電話端末間および公衆網との間の交換サービスを提供する
VoIP端末	VoIPゲートウェイ 	アナログ電話端末を収容し、IPネットワーク間での音声や信号の変換を行う
	IP電話端末 	IPネットワークに直接接続できる電話端末

図 2-2 VoIP システムの種類

2.3 PBX として具備する機能

一番重要なのは、第 1 部で説明しているパスワードの管理、ファームの最新化です。さらにログ管理、通話履歴管理をすることで、通常時からログや通話履歴を確認することで、日頃使用しない端末からのアクセスや海外発信などを発見することが可能です。

さらに、PBX としては、以下の対策を実施することが、重要です。

① VoIP システムを外部の IP ネットワークと接続する場合は、外部からの不正アクセスを防ぐため、ファイアウォール等でセキュリティの高いネットワーク設計をする。

② 外部より、なりすましにより不正な国際発信を防ぐため、国際発信が不要な場合は、通信キャリアが提供する国際通話発信規制サービスを利用して、国際発信をできないようにする。

③ PBX によっては設定で国際発信をできないようにする機能がある場合は、国際発信をできないようにする。

④ 公衆網から PBX にアクセスし、そこから不正な国際発信（公-公接続）を防ぐため、PBX の設定で、公-公接続をできない設定にする。公-公接続が必要な場合は、公衆網から PBX アクセス時に認証機能を導入する。

⑤ 不正な VoIP 端末（なりすまし）の VoIP サーバーへのアクセスを防ぐため、認証機能がある端末の場合は、認証機能を有効とする。

2.4 PBX の乗っ取り事例と対策

・事例 1：悪意のある第三者が、お客様の PBX を踏み台として、あたかも、お客様の電話が発信しているかのように国際通話等を行う事象。（公ー公接続）

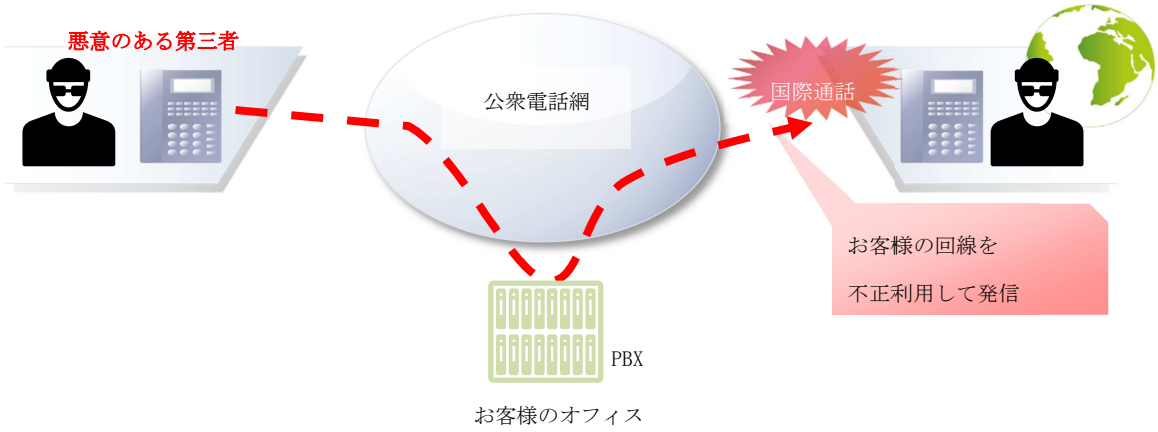


図 2-3 PBX の乗っ取り事例 1

⇒予防策：悪意ある第三者から PBX に着信した際に、PBX にて ID/パスワードを設定する認証機能を導入することにより、第三者からの不正利用を予防できます。

・事例 2：インターネット網の IP 回線から接続し、PBX 配下の VoIP 電話に成りすまし、あたかも、お客様の VoIP 電話から発信しているかのように国際通話等を行う事象。

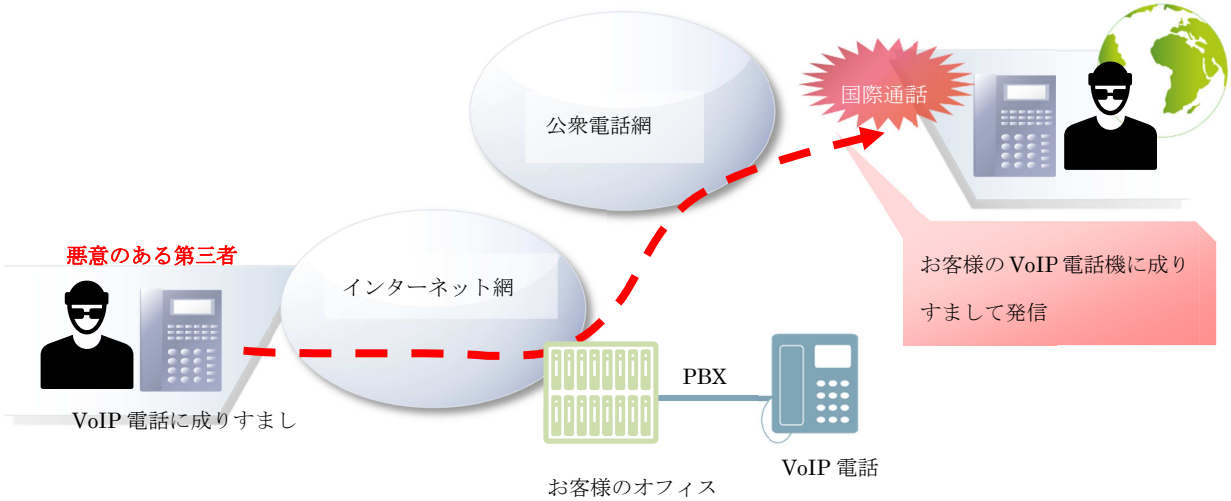


図 2-4 PBX の乗っ取り事例 2

⇒予防策：VoIP 電話を PBX に接続する際、VoIP 電話機からの認証機能により、不正な VoIP 電話の接続を規制することが可能です。

2.5 参照文書

1　総務省研究会資料「なりすましによる IP 電話等の不正利用について」（2015 年 7 月）

2　総務省 IP 電話の不正利用に関する注意喚起（2015 年 6 月 12 日）
http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000191.html

第 3 部　ルーター

3.1 背景

インターネットが普及して約 20 年、今では企業、一般家庭の多くでインターネットを利用できる環境ができてきています。今後、IoT の普及に伴い、さらにインターネットの利用機会、範囲が広がることが予想され、ルーターの利用機会がますます増えています。

そのルーターですが、インターネットからの不正利用が 2010 年ごろから確認され、総務省、警視庁、JEITA さらにルーターベンダー各社からも注意喚起、基本的な対策が発信され、再発防止に向けた活動が行われています。しかし、未だに不正利用の検出が後を絶たず、問題が収束していないのが現状です。

3.2 定義

ルーターは、一般的にインターネットと LAN を接続するための装置になります。LAN は、企業ではイントラネットと呼ばれる社内網を指しますし、家庭においては家庭内ネットワークが該当します。

専門的な言い方をすれば、以下の定義となり、「異なるデータリンクへの中継」がインターネットと LAN の接続に該当します。

ルーターとは、国際標準化機構（ISO）により制定された OSI（Open System Interconnection）に基づいた通信機能を階層構造に分割したモデルのうち第 3 層（ネットワーク層）を利用して、ネットワーク上のデータの中継を行うことを主な目的とする WAN インタフェースを持った製品をいいます。

具体的には IP アドレスを参照し中継動作を行うもので、この中継動作とは IP アドレスヘッダ情報の TTL の減算動作を行い、異なるデータリンクへの中継を行うことをいいます。

3.3 ルーターとして具備する機能と対策

一番重要なのは、第 1 部で説明しているパスワードの管理、ファームの最新化です。さらに、ログ管理をすることで、通常時からログを確認することで、不正なアクセスがないか等を発見することが可能です。

企業においては、イントラネットの管理者が、パスワードの管理、ファームウェアの更新やログの管理を実施しますが、家庭においてはなかなか対応が困難です。

そこで、家庭向けルーターでは、

・使用開始時の設定において、工場出荷時パスワードの強制変更や、工場出荷時にユニークなパスワードを設定

・ファームウェアの自動更新機能の採用
（ただし、機能の開始はユーザー設定による）

といった対策が進められています。

3.4 ルーターの乗っ取り事例

・事例 1：悪意のある第三者が外部から不正アクセスをして、ユーザーが気付かないうちにルーターの設定を変更します。そうすると、ユーザーがあるウェブサイト（例えば銀行）にアクセスしようとすると、本物のウェブサイトに似せた偽ウェブサイトに誘導して、そこで、ID やパスワード、個人情報や重要な情報等を搾取します。これにより、悪意ある第三者がその情報から、ユーザーになりすまして、不正送金等を行う被害にあってしまいます。

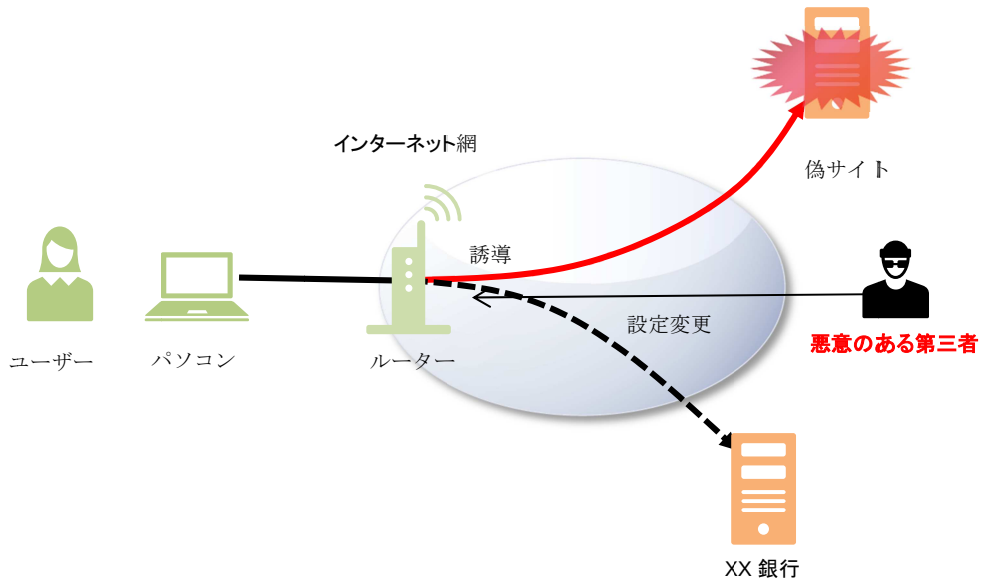


図 3-1 ルーターの乗っ取り事例 1

・事例 2:悪意のある第三者が外部から不正アクセスをして、ユーザーが気付かないうちに、ルーターの設定を変更します。そうすると、インターネットとの通信内容を傍受、また改竄等を行えます。いわゆる「中間者攻撃」による被害が確認されています。これにより、入手した情報を悪用されることで、さらに被害が拡大することになります。

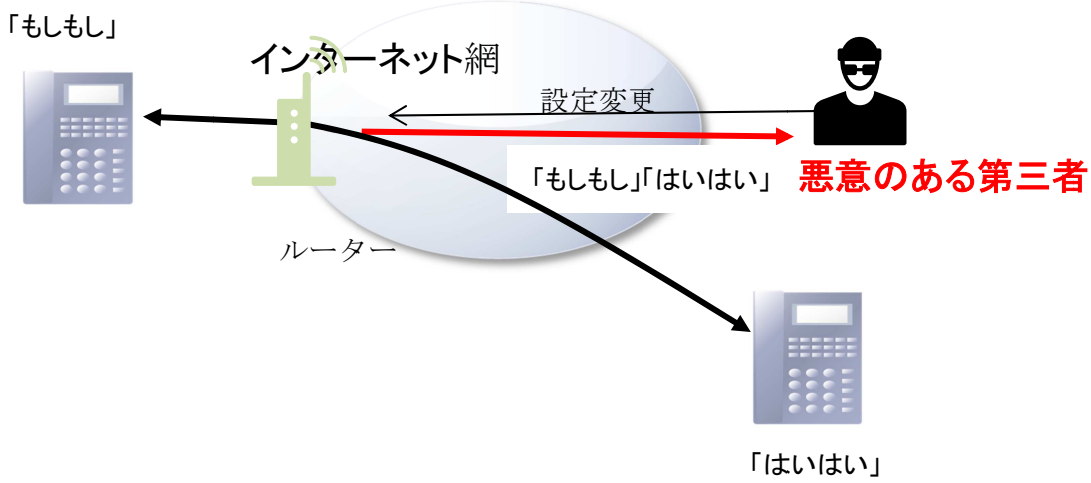


図 3-2 ルーターの乗っ取り事例 2

・事例 3：自宅で使用している無線 LAN ルーターを、他人が無断でアクセスして、インターネット接続する被害が確認されています。無線 LAN の電波は自宅外に漏れており、近所から無線 LAN にアクセスしていました。
また、勝手に接続した他人の端末から、パソコンの共有フォルダなどが見えてしまいます。

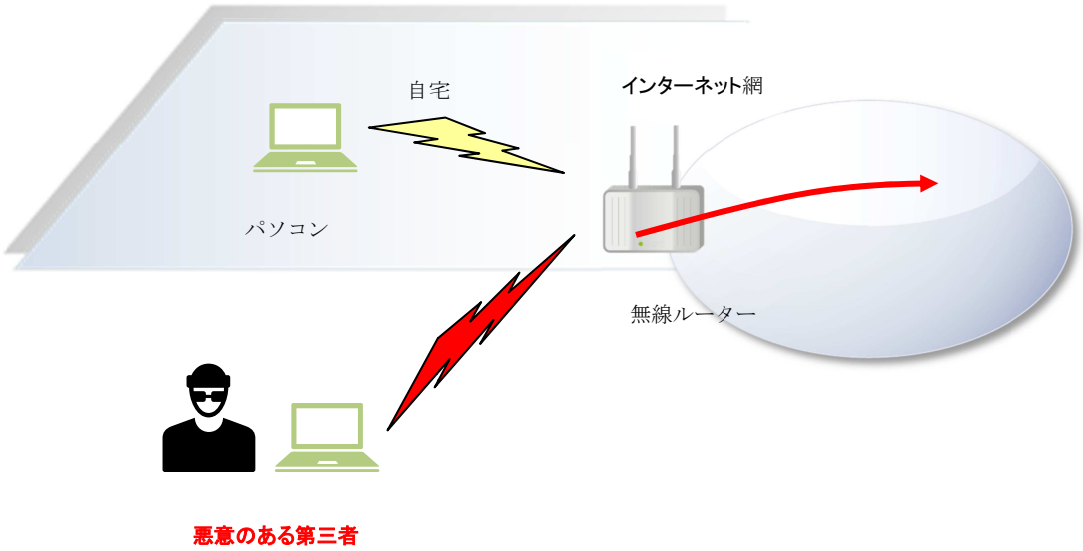


図 3-3 ルーターの乗っ取り事例 3

第 4 部　ファクシミリ

4.1 背景

ファクシミリは操作が簡単で即時に送達が確認できる安心・安全・確実な通信手段として、今でも企業や一般家庭で広く利用されています。　一方で、うっかり「相手先を間違えて送ってしまった」、あるいは「宛先が異なる FAX が来た」など通常使用で誤送信による個人や企業の情報漏洩トラブルの事例がごく稀に見られています。また近年ではイントラネットやインターネットに接続された複合機でファクシミリを使用されるケースや、ファクシミリのクラウドサービス等利用の形態が広がっており、セキュリティに対する利用者の関心も高まっています。

4.2 定義

ファクシミリとは、画像情報を通信回線を通して遠隔地に伝送する機器、あるいは仕組みのことで、ファクシミリ装置やファクシミリ機能を有する複合機だけではなく、形態としては PC 等でファクシミリ機能を実現しているものもあります。　通信回線としては 2000 年代に入り主にオフィス環境においてイントラネットやインターネットなどが利用されるようになりましたが、一般家庭用途および業務用途として公衆電話網が今でも広く利用されています。

4.3 ファクシミリとして具備する機能

意図しない宛先への送信を防止する機能など、下記に挙げたような機能を持つことで、より安心してファクシミリを利用することができます。

■あると望ましい機能

・誤送信を防止するための機能
・誤接続を防止する機能（アナログ回線）
・長時間トレイに受信紙が放置されることを防止する機能
・確実に遅れたことを確認できる機能

*参考：ビジネス用途ファクシミリのセキュリティに関するガイドライン（呼称：FASEC）
https://www.ciaj.or.jp/gazou/guideline/guide_security.pdf

4.4 ファクシミリのセキュリティ事故事例と対策

・事例 1：

宛先指定操作をテンキーにて行った際、無意識の内にキーを押し間違えて意図しない宛先に送信してしまった。

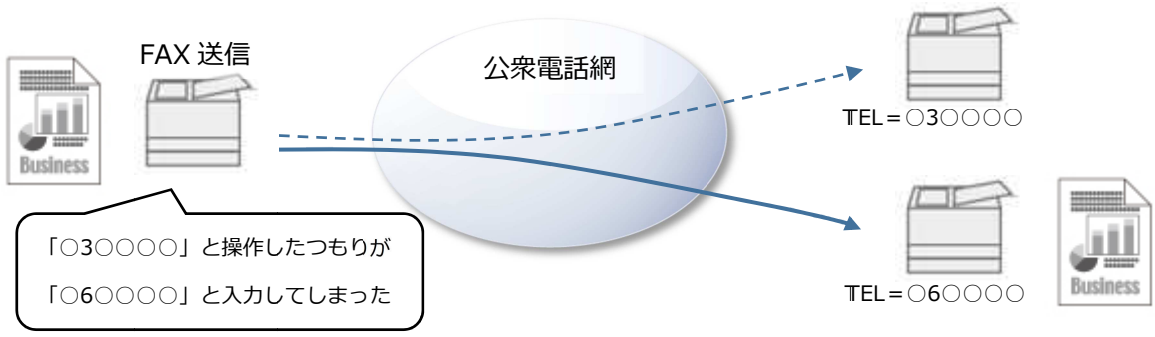


図 4-1 ファクシミリのセキュリティ事故事例 1

対策：

宛先電話番号を 2 回入力し、同じ番号であった場合のみ発信する機能を導入することにより、誤った宛先指定を防止することができます。

・事例 2：

共有しているファクシミリ装置の受信出力用紙を確認したら、送られているはずの受信出力用紙がなくなっていた。(他の利用者が持ち出すことによる情報の紛失、および情報漏洩)

対策：

F コード通信を利用して受信したデータを一旦ファクシミリ装置内のメモリに蓄積させ、利用者の印刷操作により受信したデータの印刷を行うことで、他の利用者が誤って持ち出すことを防止できます。

図 4-2 ファクシミリのセキュリティ事故事例 2

通信ネットワーク機器セキュリティ
ユーザーガイドライン Ver.1.0

一般社団法人　情報通信ネットワーク産業協会
〒105-0013　東京都港区浜松町２−２−12
ＪＥＩ浜松町ビル３階
電　話　03-5403-9357
ＦＡＸ　03-5403-9360