RFC3013　推奨されるISPセキュリティサービスと手順

参照資料	管理策	医療機関		ルータ製造・販売事業者		ISP/NW事業者	
		機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール
	ISP は、ネットワークセキュリティに関する論点用に SECURITY、不適切な公共での行為に関する論点用に ABUSE、それからネットワークインフラストラクチャに関する論点用に NOC のメールボックスを割り当てている [RFC2142] を遵守する必要があります（SHOULD）。						○
	さらに ISP は、その連絡先情報が、Whois の中であれ、ルーティングレジストリ [RFC1786] の中であれ、他のいかなるリポジトリの中であれ、完全で、正確で、そして連絡可能であることを確保にする義務があります。					○	○
	ISP は、対顧客、対他の ISP、対 IRT、対法執行機関、もしくは対プレスや一般公衆に、セキュリティインシデントについての情報の共有上の明確なポリシーと手順をもつことが**必要です（SHOULD）**。						○
	ISP は、自身と他の ISP の間の境界をまたぐセキュリティインシデントを取り扱うためのプロセスを実際にもつ必要があります。						○
	ISP は、このようなコミュニケーションをセキュアチャネル越しに行うことができる**必要があります（SHOULD）**。しかし、司法管轄圏によっては、セキュアチャネルが許されていないこともあることを銘記しておいてください。					○	○
	ISP は、その提供しているサービスにおけるセキュリティ脆弱性情報を顧客に通知することにおいて、積極的である**必要があります（SHOULD）**。さらに、新しい脆弱性がシステムやソフトウェアに発見され次第、そのサービスがそれらのリスクによって脅かされているか否かを示す必要があります。						○
	ある ISP のインフラストラクチャのコンポーネントに影響を与えるセキュリティインシデントがおきた場合、その ISP は、その顧客に（下記の事項を）報告する必要があります。 - 当該インシデントへの対応を誰がコーディネートしているか - 該当の脆弱性 - どのようにサービスが影響を受けたか - 当該インシデントに対応するために何がなされているか - 顧客データが侵された可能性があるか否か - 該当の脆弱性を根絶するために何が行われているか - 予測可能と仮定し、対応のためのスケジュール						○
	多くの ISP は、顧客に停電やサービス停止について通知する手続きを確立しています。ISP が、これらのチャネルをセキュリティ関連のインシデントを報告することのために利用することは、妥当といえます。このような場合、その顧客のセキュリティ 連絡窓口は、通知される担当者ではないかもしれません。むしろ、通常の連絡窓口がその報告を受け取るでしょう。顧客は、このことを知っておく必要があり、 そのような通知を適切に転送するようにしなければなりません。		○				
	ISP が CSIRT をもっているか否かにかかわらず、ISP は、その顧客から報告されたインシデントを受け取り扱うための、よく宣伝されたやり方をもつ必要があります。						○
	さらに ISP は、報告されたインシデントに対応する能力主体を明確に文書化する必要があり、CSIRT がある場合には、どの（ CSIRT の）構成員がその顧客を含むかと、誰にインシデントを報告することができるかを表示する必要 があります。						○

参照資料	管理策	医療機関		ルータ製造・販売事業者		ISP/NW事業者	
		機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール
	それゆえ ISP にとって、その顧客がインシデントが起きる「事前」に、そのインシデント対応の一連の段階を規定できるようにするために、どのインシデント対応／セキュリティ資源を顧客に入手可能にしているかを公表することは重要です。						○
	各 ISP は、適切な利用法に関するポリシー(AUP)をもつ**必要があります(SHOULD)**。						○
	ISP が顧客と、インターネットへの接続性を提供することの契約をする際には常に、その契約は AUP の配下におかれる必要があります。						○
	AUP は、契約が更新されるたびにレヴューされる必要があり、さらに、ISP は、積極的にポリシーが更新されるたびに顧客に通知する必要があります。						○
	AUP は、システムもしくはネットワークの様々なコンポーネントにおいて、顧客がすべきことと、すべからざることを明確に識別する必要があり、そのネットワーク上で許容されるトラフィックの種類が含まれます。						○
	ISP は、自身の AUP をその顧客に対して伝えることに加えて、そのコミュニティが、その ISP が何を適切と考えているかを認識できるように、そして、不適切な行為が起きた場合において、どんなアクションを期待するかを知ることができるように、自身のポリシーを、その Web サイトのような公的な場で公表する必要があります。						○
	AUP は、不適切な行為が行われた場合において、いかなる制裁が執行されることになるか、表明において明確である必要があります。						○
	多くの司法管轄単位はデータ保護の法規制をもっています。このような法規制が適用されるところでは、ISP は、保持する個人データを考慮する必要があり、必須とあらば、自身をデータコントローラーとして登録し、そのデータを法規制の文言に従ってのみ使用するように備える必要があります。インターネットのグローバルな性格によって、このような法規制が存在しないところに位置する ISP は、少なくとも典型的なデータ保護法(例: [DPR1998])を読むことによってデータ保護の発想に慣れておく必要があります。						○
	ISP は、このようなやり方で、インターネットのネットワークインフラストラクチャを管理することに責任を負います。 - 十分に既知のセキュリティ脆弱性に対抗しているようにする - 簡単には、攻撃者によってハイジャックされて以降の攻撃に使用されることがないようにする						○
	ISP は通常、IRR(Internet Routing Registry)や APNIC、ARIN、RIPE データベースのようなグローバルなリポジトリに蓄積されたデータを保守することに責任を負います。このデータへの更新は、強い認証を使用することによってのみ可能である必要があります。					○	○
	ISP は、その顧客に割り当てるアドレス空間を、その代表者欄により詳細な連絡先情報があるように、公的に登録する必要があります。						○
	ISP のトラフィックを正しい宛先に経路制御する能力は、ルーティングレジス トリ [RFC1786] 中で設定されるルーティングポリシーに依存することがあり ます。その場合で、かつそのレジストリがサポートしているならば、ISP は、保守しているレジストリ情報が強い認証を使用しているときにのみ更新できるようにし、更新を行う権限者が適切に制限されるようにする必要があります。					○	○

参照資料	管理策	医療機関		ルータ製造・販売事業者		ISP/NW事業者	
		機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール
	善良なる管理者の注意義務はまた、宛先にとって経路の選択肢がある場合に、誰のルーティング告知により大きな信頼をおくかを決定する際にも払われる必要があります。						○
	BGP 認証 [RFC2385] が、ルーティング ピアに使用される必要があります（SHOULD）。					○	
	ISP の各顧客との境界ルーターにおいて ISP は、顧客から来る、その顧客に割り当てたアドレス以外のソースアドレスを もつ、すべてのトラフィックを積極的にフィルタする必要があります。					○	
	顧客と ISP 間のインターフェイスにおける入方向フィルタリングが不可能である、これらの希な場合においては、その顧客には、彼らのネットワーク中に入方 向フィルタリングを実装することが強く薦められる必要があります。一般に、フィルタリングは、できる限り実際のホストの近くで行われる必要があります。					○	
	ISP の顧客が、偽のソースアドレスに依拠する攻撃にさらされることを低減するために、ISP は下記の事項を行う必要があります。各顧客との境界ルーターにおいて、ISP は、顧客宛ての、その顧客に割り当てたことのあるあらゆるアドレスに該当するソースアドレスをもつすべてのトラフィックを積極的にフィルタする必要があります。					○	
	ISP は、例えば、プライベートなイントラネットのために割り当てられたアドレスへの経路を無視するため、偽の経路を避けるため、"BGP Route Flap Dampening" [RFC2439] とアグリゲーション（集合）ポリシーを実装するために、ISP が聞くルーティング告知をフィルタする必要があります。					○	
	ISP は、そのネットワークの他の部分におけるルーティングについて過剰な負荷にさらすことのリスクを低減させるテクニックを実装する必要があります。					○	
	それゆえ、ブロードキャストメディアに接続されているルーターは、そのメディアへの指図されるブロードキャスト [RFC2644] を許容するように設定されてはなりません（MUST NOT）。					○	
	メール、News や Web ホスティングのような極めて重要な ISP 機能を行っているすべてのシステムは、それらへのアクセスが、それらのサービスの管理者にのみ可能であるように制約される必要があります。そのアクセス は、強い認証に従ってのみ許可される必要があり、暗号化されたリンク越しである必要があります。それらのサービスがリッスンしているポートだけが、ISP のシステムネットワークの外部から到達可能である必要があります。					○	
	ISP は、サービスを提供することにおいて、よりセキュアな手法が利用可能となり次第、その手法について最新であることを保つ必要があります。						○
	システムは、トランジットネットワークセグメントに設置されるべきではありません。						○
	ISP は、そのメールインフラストラクチャが、送信者の身元を隠しながら UBE （ Unsolicited Bulk E-mail ）を投入する「スパマー」によって利用されることを防ぐために、積極的な手順をふむ必要があります。						○
	ISP はまた、その顧客に、自身のシステム上で、この活動を防ぐのに必須の手順をふむことを強く薦める必要があります。						○
	メッセージ送信は、"SMTP Service Extension for Authentication"[RFC2554] に記述されている AUTH SMTP サービス拡張を使用して、認証される必要があります。					○	

参照資料	管理策	医療機関		ルータ製造・販売事業者		ISP/NW事業者	
		機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール
	この理由は、入り方向ローカル配信と中継（つまり、顧客に ISP の SMTP サー ビス経由でメールをインターネット上の任意の受信者宛てに送信することができ ること）を区別できるようにすることにあります。認証されていない SMTP は、ローカル配信用にのみ許可される必要があります。					○	