2003 年度 JNSA セキュリティポリシーWG 成果物

－　脅威、脆弱性および残存リスク対応表について　－

2004 年 4 月

セキュリティポリシーＷＧ

目次

脅威、脆弱性および残存リスク対応表について

概要

Ｈ１５年度セキュリティポリシーWGの活動では、これまでに作成したポリシーサンプルから５つを選択し、それらの対策を分解した上で、脅威、脆弱性（※１）および残存リスクを結びつけて表形式にまとめています。

通常リスク分析は、「リスクの洗い出し」「洗い出したリスクの評価」の手順を経ます。ただし､ポリシーサンプルでは汎用性を持たせるためにあえて資産を明確にしていないこと、リスクの評価はさまざまな手法があり（※２）統一することが困難なことから、ここではあえてリスクの評価には触れないようにしてあります。実際の評価は、利用者の皆様に最適な手法で実施していただきたいと思います。

利用に際してのポイント

この資料で表現されている脅威、脆弱性および残存リスクは、対策と対応づけるためにかなり具体的に記述されている場合があります。組織全体のリスク分析表をこのレベルで記述しようとすると、膨大な量になる恐れがあります。組織全体の分析は粗く、より重要な部分の分析は細かく、といったメリハリをつけることが、効率的なリスク分析を行うコツです。

今回記述した脅威、脆弱性、残存リスクは、ポリシーサンプルの対策を元に想定例を記述しており、対応するすべての脅威や脆弱性を洗い出している訳ではありません。ＰＤ３００５では、ＢＳ７７９９の１２７項目に対応する「セキュリティ懸念事項」が記述されています。このような網羅性をもった情報を有効に活用しながら作業されることをお勧めいたします。

リスク分析は、分析表そのものを作成するよりも（１）作成する過程で関係者がリスクおよびその程度の共通認識を持つこと（２）残存リスクについて正しく管理すること（３）外部、内部の変化に応じて更新していくこと　の方が重要です。見易さ、維持のしやすさ等にも注意されるとよいと思います。

※１：脅威および脆弱性について

セキュリティポリシーに関係する方は、脅威や脆弱性という言葉をよく耳にすると思いますが、両者の違いを分かりやすく説明すると、以下のようになります。

- 脅威は攻めるものの強さであり、脆弱性は守るものの弱さである。

または、

- 脅威は、自らが管理できない対象が与える影響の大きさであり、脆弱性は自らが管理すべき対象の不備である。

例えば、家の玄関が開きっ放し（脆弱性が高い）が泥棒がいない（脅威がない）場合は問題ありませんが、玄関に二重の鍵をつけても（脆弱性が低い）バールでこじ開けられれば（脅威がより高い）侵入されてしまいます。よって、問題が発生するかどうかは、脅威と脆弱性の相対的な差だと言えます。

※２：さまざまなリスク分析の手法

リスク分析を実施する際、リスクの評価については、実にさまざまなものがあります。（世の中にはリスク分析ツールと呼ばれているものが２００種類以上あると言われています。）リスク評価の方法を複雑にしている例をいくつかご紹介します。

・ リスクの算定式

リスクの算定式として、以下が考えられます。

リスク＝資産の重要性×脅威の程度×脆弱性の程度

リスク＝被害の大きさ×発生確率

これら５つの因子はそれぞれに関連性があるため、リスクを導き出す方式もさまざまな考え方が存在します。

・ 定性リスク分析と定量リスク分析

定性リスク分析は、上記のリスク因子それぞれを、３段階、５段階といった定性的なレベルで分類します。一方、定量リスク分析は、主に定量的な数値（通常は金額）で示します。定性分析実施後に、特定箇所を定量分析するような、組み合わせ方もあります。

・ 資産の分類方法

資産は、タイプと重要度でそれぞれ分類できます。タイプとは、情報、ソフトウェア、ハードウェア、無形財産、人等です。重要度としては、機密レベルに応じて極秘、秘密、社外秘、公開のような分類を行いますが、何種類に分類するのか、といった問題があります。また機密性以外にも、完全性、可用性についても同様の分類をする場合があります。すべてをやりすぎると組み合わせパターンが肥大してしまう問題があります。

・ 定性リスク分析の課題

各リスク因子を何段階に分類するか、そして分類の基準をどのように定義するかを決

める必要があります。また、リスク値を求める場合、定性化されたリスク因子を足す（ＧＭＩＴＳ等）方法、かける方法などがあります。

・ 定量リスク分析の課題

通常は被害の大きさ×発生確率で算出しますが、被害の大きさについて、実際の判例が少ないなかでどれだけ精度の高い数値を出せるのか、といった問題があり、発生確率について、技術の進歩やビジネススタイルの変化が激しい中でどれだけ過去の統計情報が利用できるのか、といった問題もあります。また、ブランドや信頼性、人命といった、金額換算が難しい資産をどのように評価するかも課題です。現実には算定が難しい状況にあります。

対象標準	アカウント管理標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92版）			残存リスク
				項番	項タイトル	内容	
1	・本来、必要でないシステム権限を用いた不正アクセスの試み。	・本来、必要な範囲を超えてシステム権限を付与していること。	⇨	4.1(1)	新規アカウントの発行	新規のアカウントが必要になった場合には、必要な権限と共に人事権を持った管理者に申請する。	・適切な承認ルートを介さずにシステム権限が設定されてしまうこと。 ・人事権を持った管理者からシステム管理者への指示ミス ・システム管理者の設定ミス
2	・本来、必要でないシステム権限を用いた不正アクセスの試み。	・システム管理者が人事面を考慮した権限の妥当性チェックを適切に行なえないこと。 ・申請者はできるだけ広い範囲の権限を望んでいること。	⇨	4.1(2)	新規アカウントの発行	申請を受けた人事権を持った管理者は、必要な権限と必要性を検討し、妥当と判断した場合には、システム管理者に新規アカウントの発行を申請する。	
3	・なりすましによるシステムへの不正アクセスの試み。	・安易で推測可能なパスワードを設定していること。 ・パスワードを複数人が共用していること。 ・同じパスワードを使いつづけていること。	⇨	4.1(3)	新規アカウントの発行	申請を受けたシステム管理者は、申請を受けたアカウントに必要最小限のアクセス権限を設定する。	
4	・ソーシャルエンジニアリング	・人目に付きやすい場所にパスワードを書いたメモを放置・廃棄していること。		4.1(4)	新規アカウントの発行	アカウントに対応したパスワードは、『ユーザー認証標準』に従って慎重に設定しなければならない。	パスワードクラック、スニファリングによるパスワードの盗難
5	・本来、必要でないシステム権限を用いた不正アクセスの試み。	・必要な権限を判断するための一定の基準がなく妥当性の判断が主観で行なわれていること。	⇨	4.1(5)	新規アカウントの発行	メール送受信、ファイル共有、インターネットアクセスなど、基本的なアクセス権限については、別途標準的なアクセス権限の表を作って目安にすることが望ましい。	
6	・本来、必要でないシステム権限を用いた不正アクセスの試み。	・システム管理者が人事面を考慮した権限の妥当性チェックを適切に行なえないこと。	⇨	4.2(1)	アカウントの変更	アカウントに与えられている権限を変更する場合には、新規アカウントの発行と同様に人事権を持つ管理職を通してシステム管理者に申請する。	適切な承認ルートを介さずにシステム権限が変更されてしまうこと。
7	・システム権限を縮小される前に情報資産を駆け込みで取得・持ち出そうとすること。	・人事上の権限の変化が、システムに反映されるタイミングが遅れていること。	⇨	4.2(2)	アカウントの変更	人事権を持つ管理職は、現在部下に与えている権限に変更があった場合には、速やかに申請を行うように担当者に指示しなければならない。特に、権限の縮小が行われた場合には、業務上の不都合とは関係なく、セキュリティ上の理由から、速やかにアクセス権限の変更の申請を行わなければならない。	・異動者とシステム管理者の馴れ合い・共犯 ・人事権を持つ管理者からシステム管理者への指示漏れ ・システム管理者の設定ミス、削除漏れ
8	・システム権限を剥奪される前に情報資産を駆け込みで取得・持ち出そうとすること。	・異動者のアカウントをいつまでも残していること。	⇨	4.3(1)	不要となったアカウントの削除	人事異動などで不要となったアカウントは、速やかに削除・停止にしなければならない。	
9	・本来、利用権限のないアカウントを用いた不正アクセスの試み。	・人事異動の情報をシステム管理者が把握するまでに時間がかかっていること。	⇨	4.3(2)	不要となったアカウントの削除	人事部は、退職や休職などでアカウントが不要になったという情報を得た場合には、速やかにシステム管理者に通知し、アカウントを削除・停止しなければならない。	

対象標準	電子メールサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
1	・社外の第三者からウイルス付メールを送信されたことによるウィルス感染 ・メールが利用できないことによる業務停止	・クライアントが勝手にメールソフトを選択すること ・セキュリティ上脆弱なメールソフトを利用すること ・ヘルプデスクが対応できないこと	⇨	4.1(1)	電子メールサービス利用端末機器のセキュリティ	電子メールの送受信にあたっては、情報セキュリティ委員会が指定した電子メールソフトウェアを用いなければならない。また、情報セキュリティ委員会の指示に従い、当該ソフトウェアのバージョンアップを行わなければならない。	・クライアントＰＣ設定もれ。 ・パターンファイルの更新もれ ・システム管理者設定ミス ・セキュリティパッチの適用漏れ
2	・社外の第三者からウイルス付メールを送信されたことによるウィルス感染	・クライアントが勝手にメールソフトの設定をしていること ・OSのパッチがあたっていない ・指定された機種を使用していない	⇨	4.1(2)	電子メールサービス利用端末機器のセキュリティ	上記ソフトウェアを使用するコンピュータは、『ソフトウェア/ハードウェアの購入および導入標準』に基づいて導入され、『クライアント等におけるセキュリティ対策標準』に基づいたセキュリティ対策を施したものでなければならない。	・指定されていないOSを例外的に使用した場合のサポート不可
3	・管理者による不正アクセス ・ソーシャルエンジニアリング	・初期パスワードをそのまま使っていること ・初期パスワードが漏えいすること	⇨	4.1(3)	電子メールサービス利用端末機器のセキュリティ	電子メールアドレスは初期パスワードとともに発行される。初期パスワードは直ちに変更しなければならない。	・遵守規定が徹底されず、初期パスワードのまま利用されてしまうこと ・システム管理者の不正によるパスワード漏洩
3’	・辞書攻撃、ブルートフォースアタック、ソーシャルエンジニアリングによる不正利用	・長期間同じパスワードを使い続けていること ・安易なパスワード（POP3,IMAP4）設定していること	⇨	4.1(3)	電子メールサービス利用端末機器のセキュリティ	パスワードは最低3ヶ月に1度、定期的に変更しなければならない。設定するパスワードは、『パスワードに関する標準』に則ったものとする。	・遵守規定の徹底されず、パスワードが変更されないまま利用されてしまうこと ・安易なパスワードが使用されてしまうこと ・システム管理者の不正によるパスワード漏洩
4	・第三者による不正利用	・メールソフト起動時にユーザ認証を行わない設定にしていること	⇨	4.1(4)	電子メールサービス利用端末機器のセキュリティ	電子メールソフトウェアの利用にあたっては、パスワードを保存してはならない。電子メールソフトウェア起動時にユーザ認証を必要とする設定にしなければならない。	・遵守規定が徹底されず、利席時などに第三者に不正利用されてしまうこと ・電子メールソフトウェアによってはユーザ認証をしなくても受信トレイに保存されているメールの読み出しができてしまうこと
5	・機密情報の漏えい	・機密情報を勝手に電子メールで送信している状態	⇨	4.2(1)	電子メールで送受される情報の保護	当社の事業に関わる情報や、顧客、従業員のプライバシーに関わる情報などの機密情報は、原則として電子メールを用いて送信してはならない。	・遵守規定が徹底されず、機密情報が電子メールで送信されてしまうこと

対象標準	電子メールサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
6	・機密情報の漏えい ・ネットワーク上での盗聴／改ざん ・メールサーバ管理者による盗聴／改ざん	・暗号化せずに機密情報を送信していること ・業務上改ざんされてはならない情報を電子署名せずに送信していること	⇨	4.2(2)	電子メールで送受される情報の保護	業務上やむを得ず機密情報を送受信する場合は、情報セキュリティ委員会の指示に従い、内容に応じて暗号化、電子署名などの処置を施さなければならない。	・手続きのめんどうさからの対応遅れ、不実行。 ・暗号化ソフト、電子署名の使用法の教育不足 ・機密情報か否かの判断ができないこと
7	・誤送信による電子メール内容の漏洩	・メールの送信先を確認せずに送信していること	⇨	4.2(3)	電子メールで送受される情報の保護	電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。	・遵守規定が徹底されず、確認漏れが発生すること
8	・メールアドレスの漏洩 ・迷惑メールの送信 ・社会的信用の失墜	・Bccを利用せず、ToやCcを利用して、複数人へメールを送信していること（互いにメールアカウントを知らせる必要のない人に漏れてしまう） ・違法に広告メールを送信していること	⇨	4.2(4)	電子メールで送受される情報の保護	当社のセミナー案内や製品ご紹介メールなどのように社外の複数のドメインが混在するメールアドレスに対し、1通の電子メールで同報送信する場合は、送信先メールアドレスが受信者間で閲覧できないよう、設定しなければならない。また、広告メール等の送信にあたっては、法を遵守しなければならない。	・メール作成者の操作ミスによりメールアカウントが漏洩してしまうこと
9	・電子メール内容の漏洩 ⇒プロバイダのサーバ管理者による不正閲覧 ⇒家族による不正閲覧 ⇒ネットワーク上の盗聴 ・不適切な配送先への転送	・ユーザが勝手に個人的なメールアドレスに業務情報を自動転送していること	⇨	4.2(5)	電子メールで送受される情報の保護	電子メールを社外の個人的なメールアドレスに自動転送する場合は、情報セキュリティ委員会に申請を行わなければならない。この場合、転送先メールアドレスは原則として携帯電話のメールアドレスとする。	・手続きのめんどうさからの対応遅れ、不実行。 ・転送許可／非の判断基準が曖昧なことによる不適切な転送許可 ・携帯電話の盗難、紛失 ・携帯メールアドレスの誤入力 ・許可されたメール転送を使って想定を超える機密情報を転送してしまう事 ・携帯電話の管理一般に関する事項

対象標準	電子メールサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
10	・電子メール内容、メールアドレスの漏洩 ・システムリソースの不足	・業務時間中に業務目的以外にメールを送っていること	⇨	4.3(1)	電子メールサービスとネットワーク保護	業務目的以外に電子メールサービスを利用してはならない。	メールサーバ管理者がメールの内容をチェックする場合、以下の残存リスクが存在しうる ・メールサーバ管理者の業務不実行。 ・メールサーバ管理者が不在、技術力不足 ・メールサーバ管理者のﾓﾗﾙの欠如 ・一人の管理者に権限が集中し、相互チェックが働いていない(相互牽制の欠如) ・セミナーなどにメールアドレスを知らせる→スパム
11	・不適切な配送先への転送 ・システムリソースの不足	・スパムメールをユーザ判断で取り扱っていること	⇨	4.3(2)	電子メールサービスとネットワーク保護	スパムメールを受信した場合は、これを転送してはならない。そして、即座に情報セキュリティ委員会に報告しなければならない。	同上 ・情報セキュリティ委員会の対策漏れ
12	・デマウィルスメール、チェーンメール ウィルス、ワーム ・機密情報を引き出そうとする内容のメール ・信頼性のないメーリングリストに入るとメールアドレス流出の可能性がある ・システムリソースの不足 ・企業イメージの低下	・メーリングリストに各自が勝手に加入し、送受信していること ・会社のメールアドレスを用いて、公序良俗に反する発言をすること	⇨	4.3(3)	電子メールサービスとネットワーク保護	当社より発行されたメールアドレスを利用して、社外のメーリングリストに参加する場合は、当該メーリングリストの信頼性、および業務への必要性を充分考慮した上で参加しなければならない。また、参加意義の無くなった場合は、直ちに脱退しなくてはならない。メーリングリストでの発言は、『13．4．2　電子メールで送受信される情報の保護』を遵守しなければならない。それとともに公序良俗に反する発言をしてはならない。	同上 ・規定が遵守されているかどうかチェックできないままメーリングリスト上に発信されること

対象標準	電子メールサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
13	・メール爆弾（受信者に対する迷惑メール） ・メールサーバの可用性	・クライアントＰＣのメール送受信のメールサイズ、送信タイミングをユーザ任せになっていること ・メールサイズを制限する機能がない	⇨	4.3(4)	電子メールサービスとネットワーク保護	電子メールの送信にあたっては、送信するメールサイズを考慮しなければならない。送信可能なメールサイズは、情報セキュリティ委員会にて規定された制限となっている。規定サイズ以上のメールを送信せざるを得ない場合は、分割送信することができる。分割送信時の分割サイズ、送信のタイミングを考慮するものとする。	同上 必要な書類を受け取れない ・分割送信者の集中によるメールサーバーダウン
14	・他のサービスが使用不能 ・送信したメールを受信者が読めない ・システムリソースの不足 ・受動的攻撃を受ける ・HTMLメールは意図しない動作をする	・メールの送受信がユーザ任せになっている	⇨	4.3(5)	電子メールサービスとネットワーク保護	その他、無用な電子メールを送受信することにより、ネットワークに負荷をかけてはならない。また、電子メール送信時にHTMLメールにて送信しないように電子メールソフトウェアを設定しなければならない。	同上 ・HTML形式で作成したドキュメントが受け取れない ・メールソフトによってはHTMLメールのみの機能しかない
15	・添付ファイルによるウイルス感染	・勝手なソフトのインストールやファイルのコピーを行うこと ・経路上でのウィルスチェックを行っていないこと ・パターンファイルが更新されていないこと ・ウイルス添付メールの送信を行うこと	⇨	4.4(1)	電子メールを介してのウイルス被害の防止	メールの受信にあたっては、『ウイルス対策標準』に基づき、電子メール保護機能を有効にしなければならない。	・クライアントＰＣ設定もれ。 ・最新パターンファイルの更新もれ ・システム管理者設定ミス
16	・添付ファイルによるウイルス感染	・添付ファイルを不用意に開示すること	⇨	4.4(2)	電子メールを介してのウイルス被害の防止	送信元不明のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルに対してはこれに操作を加えてはならない。	・感染したＨＴＭＬ形式のメールをあけてしまうこと ・知人からのウィルス付きメールを不審に思わず実行してウィルスに感染してしまうこと
17	・電子メールを介した感染拡大	・各PC上でのｳｨﾙｽ対策不備 ・出所不明なＦＤの不用意な使用	⇨	4.4(3)	電子メールを介してのウイルス被害の防止	ファイルを添付してメールを送信する場合、当該ファイルのウイルス感染が無いことを必ず確認しなければならない。	・クライアントＰＣ設定もれ。 ・最新パターンファイルの更新もれ ・システム管理者設定ミス
18	・対応の遅れによるウイルス感染拡大。	・ｳｨﾙｽ検出時の対応手順や連絡窓口が決められていない ・最新のｳｨﾙｽ情報を収集していない	⇨	4.4(4)	電子メールを介してのウイルス被害の防止	電子メールサービスを利用中に、ウイルスの発見や、ウイルスと思われる症状を発見した場合は、『セキュリティインシデント報告、対応標準』に基づき対応しなければならない。	・手続きのめんどうさからの対応遅れ、不実行によるウィルス感染拡大

対象標準	電子メールサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
19	・機密情報の漏洩。 ・ウィルス感染拡大	・電子メールの利用状況に関してチェック機能がない ・ウイルス感染への対応の遅れ	⇨	4.5(1)	電子メールの監視許可	電子メールの利用状況は、当社メールサーバ管理者の協力のもと、情報セキュリティ委員会によって監視されていることを理解しなければならない。	・メールサーバ管理者の業務不実行（不在や技術不足）。 ・メールサーバ管理者のﾓﾗﾙの欠如 ・権限の集中による(相互牽制の欠如)

対象標準	リモートアクセスサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
1	・第三者によるシステムへの不正アクセス	・障害時の対応がとれない ・迅速な対応がとれない	⇨	4.1(1)	使用機器に関する遵守事項	利用者は、ダイヤルアップによる社内ネットワークへのアクセスにおいて、情報システム部が構築した機器を利用しなければならない。	システム構築時における検証漏れによるシステムの欠陥の発生。
2		・情報システム部がネットワーク機器を管理しきれない	⇨	4.1(2)	使用機器に関する遵守事項	利用者は、ダイヤルアップルータおよびサーバ・モデムなどによる社内ネットワークへの接続手段を、情報システム部の許可を得ることなく設置してはならない。	利用者の設置ミスにより予期しない接続ポイントができている可能性。
3		・セキュリティホールの把握ができない ・情報システム部がネットワーク機器を管理しきれない	⇨	4.1(3)	使用機器に関する遵守事項	その他社内LAN環境への接続にあたり、利用機器は、『LANにおけるPC（サーバ、クライアント等）設置/変更/撤去の標準』に基づいて設定されなければならない。	利用者が許可されていない機器を接続、変更することにより予期しない接続ポイント、セキュリティホールができている可能性。
4	・不正による機密情報の持ち出し ・信頼できない人からのアクセス	・リモートアクセスの使用人数が多くなるとアクセスできなくなること	⇨	4.2(1)	機器の管理に関する遵守事項	リモートアクセスで使用するPCおよび携帯電話は、情報セキュリティ委員会が定める利用者のみ利用することができる。	定めた利用者に悪意があった場合、情報漏えいの恐れがある。利用を許可された人が集中して利用した場合でも、アクセスに支障の出るおそれ。
5	・機器の盗難	・機器が正しく管理されていないこと	⇨	4.2(2)	機器の管理に関する遵守事項	リモートアクセスで使用するPCおよび携帯電話の管理は、所有する利用者が行わなければならない。	利用者の管理が不適切であった場合、機器の盗難等による情報漏えいの可能性。

対象標準	リモートアクセスサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
6	・第三者によるシステムへの不正アクセス	・リモートアクセスの管理がされていないこと	⇨	4.2(3)	機器の管理に関する遵守事項	リモートアクセスの管理は、情報システム部（システム管理者およびオペレータ）が行わなければならない。	管理システムの設定ミスによりリモートアクセスが適切に管理されておらず、予期しない接続ポイントができている可能性。
7		・障害時の対応がとれないこと ・迅速な対応がとれないこと	⇨	4.3(1)	利用環境に関する遵守事項	リモートアクセスで利用できる機器は、情報セキュリティ委員会の定める機器でなければならない。 ・ノート型PC ・PDA ・携帯電話	機器の検証漏れのため定めた機器に不具合があった場合、不正侵入や障害時に迅速な対応ができない可能性。
8		・リモートアクセスの利用場所を把握できないこと	⇨	4.3(2)	利用環境に関する遵守事項	リモートアクセスの利用場所は、情報セキュリティ委員会の定める場所でなければならない。 ・外出先（国内、海外） ・営業所・関連会社等、当社関連施設 ・ユーザ先 ・自宅	・入室を許可されただけの人とアクセスの利用まで許可された人の見分けができない。 ・利用場所が限定されている利用者の他の利用場所からのアクセス。
9		・通信形態が多岐に渡るため、迅速な障害対応ができないこと	⇨	4.3(3)	利用環境に関する遵守事項	リモートアクセスによる接続は、情報セキュリティ委員会の定める通信形態でなければならない。 ・インターネット経由（PC、携帯電話） ・公衆回線（電話回線、INS回線、携帯電話）	通信形態の検証に漏れがあり、定められた通信ではネットワーク容量が不足しており、スループットが低下。 定められた通信にセキュリティ上の不備がある場合、第三者の侵入のおそれ。
10		・意図されていないサービスが利用可能になっていること	⇨	4.3(4)	利用環境に関する遵守事項	リモートアクセスで利用できるサービスは、情報セキュリティ委員会の定めるものでなければならない。 ・http・httpsを利用したサービス ・電子メールサービス ・ファイル転送サービス ・ファイル共有サービス ・業務システムとして導入しているサービス	許可されたサービスを利用した攻撃、不正アクセス。

対象標準	リモートアクセスサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
11	・管理外機材からの機密情報漏えい ・管理外機材からのウイルス感染	・管理外機材のセキュリティ対策不足	⇨	4.4(1)	アカウント管理に関する遵守事項	利用者は、『LANにおけるPC設置/変更/撤去の標準』に準じ、リモートアクセスサービスの利用において、個人所有の機材を利用してはならない。	利用者の許可されていない個人所有機材の接続による、ウイルス感染、不正アクセス等の被害。
12	・ユーザアカウントの不正利用	・情報システム部がアカウントの利用状況を把握していないこと	⇨	4.4(2)	アカウント管理に関する遵守事項	リモートアクセスで利用するPCおよび携帯電話は、利用者（社員）が情報システム部に申請をし、利用者情報（識別番号、パスワード等）を入手しなければならない。 ・利用者名 ・利用場所 ・利用目的 ・利用期間 ・接続機器（機器種別、OS種類） ・接続形態	管理者の改廃手順のミスによりアクセスするための情報が第三者に漏えいする可能性。
13	・退職者や未許可ユーザからのアクセス	・実態と一致しないアカウントを放置すること	⇨	4.4(3)	アカウント管理に関する遵守事項	情報システム部は、利用者情報（利用者、識別番号、パスワード等）の登録・変更・削除を適宜行い、それを管理しなければならない。	管理者の設定ミスにより予期しないアカウントが存在している可能性。
14	・第三者による情報資産への不正アクセス	・全てのサーバおよびサービスのアクセスリストがきちんと管理されていないこと	⇨	4.5(1)	アクセス制御に関する遵守事項	リモートアクセスでは、社内にアクセスできるサーバおよびサービスは必要最低限にしなければならない。	管理者の設定ミスにより許可してはならないサーバ、サービスが利用可能になっている可能性。
15		・ユーザーの権限がきちんと管理されていないこと	⇨	4.5(2)	アクセス制御に関する遵守事項	リモートアクセスでは、利用者毎にアクセスできるサーバおよびサービスを決めることとする。	管理者の設定ミスにより利用者毎のサーバ、サービスのアクセス制限が適切に設定されていない可能性。
16	・インターネット上での不正行為を社内ＬＡＮ経由で行うこと ・リモートアクセス環境を個人用プロバイダーとして利用することによるアクセス過多	・社内ＬＡＮ経由でインターネットへ接続する利用者を把握していないこと。	⇨	4.5(3)	アクセス制御に関する遵守事項	リモートアクセスでは、社内に設置されたサーバのみにアクセスすることができる。ただし、申請により許可された社員についてはインターネットへアクセスすることもできる。	管理者の設定ミスにより許可されたサーバ以外にもアクセスができる可能性。 インターネットへのアクセスを許可された社員が不適切な通信を行う可能性。

対象標準	リモートアクセスサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
17	・機材の故障によるリモートアクセスサービスの停止	・機器管理が十分ではないこと	⇨	4.6(1)	リモートアクセスサーバに関する遵守事項	リモートアクセスサーバは、専用機器（ルータ、サーバ等）または複数のネットワーク機器で構成されなければならない。	専用機器、複数ネットワーク機器が故障する可能性。
18	・第三者による不正アクセス	・アカウント管理をしていないこと	⇨	4.6(2)	リモートアクセスサーバに関する遵守事項	リモートアクセスサーバは、利用者情報を管理することができなければならない。	管理者の管理ミスにより不適切な利用者にアカウントを付与している可能性。
19	・第三者による不正アクセス	・パスワードの強度が弱いこと	⇨	4.6(3)	リモートアクセスサーバに関する遵守事項	リモートアクセスサーバは、利用者認証（発信者識別、ワンタイムパスワード）に対応していなければならない。	
20	・途中経路での盗聴 ・不許可機材からのなりすまし	・保護されていない通信経路を利用すること	⇨	4.6(4)	リモートアクセスサーバに関する遵守事項	リモートアクセスサーバは、通信手段としてコールバックとVPN（暗号化）に対応していなければならない。	
21	・第三者による継続的な不正アクセス ・大量なログデータによるRASの不安定化 ・不正アクセスした者による故意のログ消去	・接続記録が取得・蓄積されていないこと ・接続記録の管理が不徹底なこと	⇨	4.6(5)	リモートアクセスサーバに関する遵守事項	リモートアクセスサーバは、接続記録を蓄積でき各種データを外部媒体（磁気テープ、ＣＤ－Ｒなど）に保管できなければならない。 ・接続成功 ・接続失敗 ・接続の開始時間と終了時間 ・接続時のアカウント名 ・発信者識別 ・障害情報（エラー情報）	・接続記録のチェック不備による異常（不正アクセス等）の検知漏れ ・記憶媒体管理の不徹底による記憶媒体の紛失（ログ紛失、情報漏えい） ・不正コード埋め込みによる記録前のログ改竄・消去（追加） ・ログの大量発生による記録漏れ

対象標準	リモートアクセスサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
22	・正規ユーザ以外のなりすましによる不正アクセス	・クライアント端末がパスワードロックされておらず、かつ、端末が誰でも利用できる環境にある	⇨	4.7(1)	クライアントに関する遵守事項	クライアントは、利用する社員を識別（利用者識別名・パスワード）し該当者以外の利用をできないようにしなければならない。	・クライアント端末への不正侵入、トロイの木馬、キーロガーの埋め込みによるパスワード盗難 ・安易なパスワード設定によるパスワードの推測 ・総当り攻撃によるパスワード盗難 ・ソーシャルエンジニアリング、ショルダーハッキングによるパスワード盗難
23	・意図しない第三者からのシステムへの不正アクセス	・リモートアクセスして認証する際のパスワードが漏洩している、もしくは安易なパスワード設定をしていること ・リモートアクセスして認証する際に入力したパスワードを盗聴される環境にあること	⇨	4.7(2)	クライアントに関する遵守事項	クライアントは、ワンタイムパスワードまたはコールバックに対応していなければならず、それを利用しなければならない。	●OTPの残存リスク ・OTPの生成規則を解析される（リスクとしてはかなり低い） ・パスワード生成器の紛失による不正アクセスのリスク（→トークン利用のOTP） ・パスワード生成ソフトウェアの漏洩、クライアント端末紛失による不正アクセス（→SW型のOTP） ●コールバック機能の残存リスク ・登録したTEL番号の回線を、第三者が不正に利用できる状態にある場合の不正アクセス
24	・第三者からのシステムへの不正アクセス ・盗聴による機密情報の漏洩	・インターネット上に流れる情報が暗号化されておらず盗聴できる状態にあること	⇨	4.7(3)	クライアントに関する遵守事項	クライアントは、通信手段として発信者識別・VPN（暗号化）に対応していなければならず、それを利用しなければならない。	●VPNの残存リスク ・経路上に悪意のあるユーザ管理のルータが設置され、もしくはルータが乗っ取られ、Man-in-the-middle Attackによりセッションハイジャック or なりすまし

対象標準	リモートアクセスサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
25	・クライアント端末経由での社内へのウィルス感染拡大 ・クライアント端末経由での社内への不正アクセス	・正規ユーザ以外がリモートアクセスポイントへアクセス可能であること ・クライアント端末のセキュリティ対策の不備	⇨	4.7(4)	クライアントに関する遵守事項	クライアントは、『クライアント等におけるセキュリティ対策基準』を満たし、かつ『ウィルス対策標準』を満たしていなければならない。	・クライアント端末への不正侵入、トロイの木馬、キーロガーの埋め込みによるパスワード盗難 ・推測され易いパスワード設定によるクライアント端末の不正使用(不正アクセス) ・総当り攻撃によるパスワード盗難 ・ソーシャルエンジニアリング、ショルダーハッキングによるパスワード盗難 ・未知のウィルスによる被害
26	・リモートアクセスサービスの停止	・ユーザが規定外のソフトウェアをインストールしていること ・ユーザのソフトウェア設定に不備があること ・ヘルプデスクが対応できないこと	⇨	4.7(5)	クライアントに関する遵守事項	クライアントは、情報セキュリティ委員会が定めたソフトウェアがイントールされ、正常に動作する状態でなければならない。	・ソフトウェアのバグ（セキュリティホール）、ユーザのアップデート不備によるクライアントPCへの不正侵入
27	・第三者がクライアント端末を入手し、自動接続によりシステムへ不正アクセスすること	・ユーザ自身が識別情報を入力せず、自動接続によりリモートアクセスしていること	⇨	4.8(1)	利用手順に関する遵守事項	利用者は、リモートアクセスを行う場合、クライアントと利用者を識別する情報を入力しリモートアクセスサーバで認証されなければならない。	・クライアント端末への不正侵入、トロイの木馬、キーロガーの埋め込みによるパスワード盗難 ・推測され易いパスワード設定によるパスワードの推測 ・総当り攻撃によるパスワード盗難 ・ソーシャルエンジニアリング、ショルダーハッキングによるパスワード盗難

対象標準	リモートアクセスサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
28	・第三者からのシステムへの不正アクセス ・盗聴による機密情報の漏洩	・リモートアクセスして認証する際のパスワードが漏洩している、もしくは安易なパスワード設定をしていること ・リモートアクセスして認証する際に入力したパスワードを盗聴される環境にあること ・インターネット上に流れる情報が暗号化されておらず盗聴できる状態にあること	⇨	4.8(2)	利用手順に関する遵守事項	利用者は、インターネットを利用してリモートアクセスする場合、ワンタイムパスワードを利用し認証しなければならない。また、VPNを利用する事が望ましい。	●OTPの残存リスク ・OTPの生成規則を解析されるリスク ・パスワード生成器の紛失による不正アクセスのリスク（→トークン利用のOTP） ・パスワード生成ソフトウェアの漏洩、クライアント端末紛失による不正アクセス（→SW型のOTP） ●VPNの残存リスク ・経路上に悪意のあるユーザ管理のルータが設置され、もしくはルータが乗っ取られ、Man-in-the-middle Attackによりセッションハイジャック or なりすまし
29	・第三者からのシステムへの不正アクセス	・リモートアクセスして認証する際のパスワードが漏洩している、もしくは安易なパスワード設定をしていること ・リモートアクセスして認証する際に入力したパスワードを盗聴される環境にあること	⇨	4.8(3)	利用手順に関する遵守事項	利用者は、公衆電話または携帯電話を利用してリモートアクセスする場合、ワンタイムパスワードを使用し認証しなければならない。	●OTPの残存リスク ・OTPの生成規則を解析されるリスク ・パスワード生成器の紛失による不正アクセスのリスク（→トークン利用のOTP） ・パスワード生成ソフトウェアの漏洩、クライアント端末紛失による不正アクセス（→SW型のOTP）
30	・第三者からの不正アクセス	・盗み見、ソーシャルエンジニアリング等リモートアクセスして認証する際のパスワードが漏洩していること ・リモートアクセスして認証する際のパスワードを安易なパスワード設定をしていること	⇨	4.8(4)	利用手順に関する遵守事項	利用者は、上記以外の通信手段を利用してリモートアクセスする場合、コールバック機能を使用し認証しなければならない。	●コールバック機能の残存リスク ・登録したTEL番号の回線を、第三者が不正に利用できる状態にある場合の不正アクセス
31	・離席時の，意図しない第三者によるシステムへの不正アクセス	・離席時のクライアント停止／スクリーンロック等の必要性を認識していないこと，またはスクリーンロック等の機能設定がされていないこと	⇨	4.8(5)	利用手順に関する遵守事項	利用者は、リモートアクセスしている間に利用者がクライアントから離れる場合に、クライアントを停止するか第三者の利用ができないようにしなければならない。	・強制再始動によるクライアントの不正利用

対象標準	リモートアクセスサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
32	・不正なリモートアクセス ・接続失敗	・利用者の操作スキルが不十分であること	⇨	4.8(6)	利用手順に関する遵守事項	利用者は、リモートアクセス利用のための教育を受け一定のレベルになっていることが望ましい。	・利用者の理解不足，モラル低下によるパスワード漏洩 ・悪意の利用者による不正アクセス
33	・クライアントの不適切な利用（業務外の私的利用，不正使用等）	・適切な利用方法が遵守されていないこと	⇨	4.9(1)	検査と監視に関する遵守事項	情報システム部は、定期的（年4回）に外部で使用するPCおよび携帯電話が適切に利用されているか検査しなければならない。	・検査項目の漏れにより不正利用を発見できないこと ・検査で見つかった不正利用に対する対処が行われないことによる不正利用の再発 ・定期検査の間におけるPCの不正利用
34	・不正な接続環境経路での，意図しない第三者によるシステムへの不正アクセス	・不正な接続環境が放置されてしまうこと	⇨	4.9(2)	検査と監視に関する遵守事項	情報システム部は、定期的（年4回）にダイヤルアップルータおよびサーバ、モデムなどによる社内ネットワークへの接続環境が不正に用意されていないか検査しなければならない。	・検査項目の漏れにより不正利用を発見できないこと ・検査で見つかった不正利用に対する対処が行われないことによる不正利用の再発 ・定期検査の間におけるPCの不正利用
35	・意図しない第三者からのシステムへの不正アクセス	・接続記録を解析せずに，不正アクセスに気づかないこと	⇨	4.9(3)	検査と監視に関する遵守事項	リモートアクセスサーバは、接続記録を蓄積・管理し、定期的（毎月）に解析しなければならない。	・不正アクセスの発見遅れ ・未知の攻撃パターンを発見できないこと ・接続記録の改ざんにより不正アクセスが発見できないこと
36	・被害が拡大・再発してしまい，サービスの復旧が遅れること	・緊急時対応の手続きが整っていないこと	⇨	4.10(1)	緊急対応に関する遵守事項	システム管理者は、リモートアクセスサーバに対し、外部から侵害・侵入された場合、リモートアクセスを停止し、原因調査および対策を実施してリモートアクセスを再開始しなければならない。	・緊急対応手順および対応マニュアルの不備によるサービス再開の遅れまたは再開不能
37	・紛失したPCまたは携帯電話を拾得した人が悪用すること	・システム管理者が，PCまたは携帯電話の紛失に気づかないこと	⇨	4.10(2)	緊急対応に関する遵守事項	利用者は、リモートアクセスで使用するPCおよび携帯電話を紛失した場合に、速やかにシステム管理者に報告し具体的な指示を受け、対処しなければならない。	・紛失したことに気づかないこと、システム管理者への報告遅れ、システム管理者の指示遅れによる、盗難されたPCまたは携帯電話から不正アクセス

対象標準	リモートアクセスサービス利用標準

NO	脅威	脆弱性		遵守事項（JNSAポリシーサンプル0．92a版）			残存リスク
				項番	項タイトル	内容	
38	・意図しない第三者のクライアント端末利用による，システムへの不正アクセス	・リモートアクセスで使用するPCまたは携帯電話が放置されること	⇨	4.11(1)	物理セキュリティ遵守事項	リモートアクセスで使用するPCおよび携帯電話は、所有者の周囲に置き管理できるようにし、使用しない時には、定められた場所で保管しなければならない。	・離席時の不正使用、盗難 ・保管場所からの盗難
39	・システム管理者以外の者の不正使用 ・災害によるサーバの障害，停止	・システム管理者以外の者がサーバにアクセスできる環境にあること ・サーバが安全な運用が妨げられるような環境にあること	⇨	4.11(2)	物理セキュリティ遵守事項	リモートアクセスサーバは、システム管理者以外が利用できなく安全・予防対策がなされた場所に設置されなければならない。	・想定外の災害

対象標準	職場環境におけるセキュリティ標準

NO	脅威	脆弱性	遵守事項（JNSAポリシーサンプル0.92版）			残存リスク
			項番	項タイトル	内容	
1	・第三者による書類・媒体等の盗難 ・書類や媒体等の紛失 ・盗み見による情報漏洩	・使用していない書類・媒体等を無造作に机上等へ放置していること	4.1(1)	書類・媒体等の取扱いと保管（クリアデスクポリシー）	従業員は使用していない書類や媒体をキャビネット等へ収納し、机上等に放置してはならない。	・キャビネット等からの書類や媒体の盗難。
2	・重要度の高い書類や媒体等の盗難や火災による焼失	・盗難や火災を考慮して、情報資産(書類や媒体)を重要度に応じた適切な場所（施錠されたキャビネットや耐火金庫など）に保管していないこと	4.1(2)	書類・媒体等の取扱いと保管（クリアデスクポリシー）	従業員は重要度の高い書類や媒体を施錠保管し、特に必要な場合は耐火金庫・耐熱金庫に保管しなければならない。	・キャビネットや金庫等の保管場所の鍵の管理が杜撰な場合、盗難のリスクがある。 ・金庫の盗難・紛失の恐れ。 ・金庫の耐火性能・耐熱時間を超える火災による、焼失の恐れ。
3	・アクセス権のない第三者のなりすましによる、情報資産の盗難・改ざん・消去・破壊	・画面／キーボードロックの未設定及び離席時のログオフやキーボードロックをしていないこと ・重要な情報をデスクトップに置いていること	4.2(1)	画面に表示する情報の管理（クリアスクリーンポリシー）	従業員は不正な操作や盗み見防止するため、離席時にはログオフするか、画面・キーボードロック等の保護機能を使用しなければならない。	・キーボードロックのパスワードの強度がないと、不正に操作される可能性がある。 ・キーボードロックが開始するまでの時間は、不正使用の危険がある。 ・ログインパスワード認証を必要としないOS(Win98等)を利用している場合、強制的にPCを再起動させることで、不正操作が可能になる。 ・キーボードロックの未設定及び離席時のログオフやキーボードロックのし忘れ。 ・離席なくても、背後から画面を盗み見をされる恐れがある。 ・隠しカメラによる盗撮の棄権がある。 ・スパイウェアやキーロガー等による情報収集。
4	・ホワイトボード等に残された情報の漏洩	・書き込み消し忘れのまま放置していること	4.3(1)	事務・通信機器の取り扱い	従業員はホワイトボード等への書き込み内容を使用後に必ず削除し、放置してはならない。	・消し方が十分でないと、記述内容が、わかってしまう。
5	・コピー機、FAX、プリンタ等の入出力書類の放置による、盗難、紛失、盗み見	・コピー機、FAX、プリンタ等の入出力時、立ち会うことを怠っていること ・重要度の高い書類を印刷してもすぐ取りにいかず入出力トレイに放置していること	4.3(2)	事務・通信機器の取り扱い	従業員はコピー機、FAX、プリンタ等の入出力書類を放置してはならない。特に重要度の高い書類は印刷および送受信の間、従業員が常に機器に（FAXの場合は送受信の両側とも）立ち会うようにしなくてはならない。	・印刷ミスや、不必要な文書を何気なくごみ箱に捨ててしまったり、リサイクル用に利用しようとすると、情報漏洩の危険がある。 ・入出力機器のメモリーやハードディスク内に印刷後も、データが残ってしまう。 ・プリンタで印刷された書類を第三者に見られてしまう。
6	・FAXの宛先ミスによる、情報漏洩	・宛先を確認せずFAXを送信していること	4.3(3)	事務・通信機器の取り扱い	従業員はFAX送信時には必ず宛先を確認し、誤送信を防止しなければならない。	・FAXにて正常に送られなかった場合、重要な情報が未送信レポートとして、縮小され排出トレイに置かれたままになる。(重要な書類が確実に送られたかを確認する必要がある) ・未送信レポートを機密文書扱いにせず、そのままゴミ箱に捨ててしまう。 ・送信先のセキュリティレベルが低い場合は、情報漏洩の危険がある。
7	・第三者によるセキュリティ区画への出入りによる、情報資産の盗難、漏洩	・セキュリティ区画が明確でなく受渡し場所があいまいであること ・セキュリティ区画で搬入物の受渡しが行われていること	4.4(1)	搬入物の受渡し	搬入物の受渡しについては受渡し場所を設置し、『サーバルームに関する標準』で定めたサーバルームおよび『物理的対策標準』で定めたセキュリティ区画とは分離しなければならない。	・受渡し場所に不用意に情報資産が放置されている。 ・受け渡し場所からセキュリティ区画へのアクセス制限が実施されていない。
8	・第三者による、情報資産の盗難、漏洩	・アクセス記録の抜け漏れがあること ・従業員以外のスタッフが単独で行動していること	4.4(2)	搬入物の受渡し	受渡し場所への従業員以外のスタッフによるアクセスは、必ず従業員の監視付きで行い、アクセスを記録しなければならない。	・従業員以外のスタッフと従業員の馴れ合いにより、監視やアクセス記録を怠ってしまう。

対象標準	職場環境におけるセキュリティ標準

NO	脅威	脆弱性	遵守事項（JNSAポリシーサンプル0.92版）			残存リスク
			項番	項タイトル	内容	
9	・危険物の持込みによる情報資産の破壊	・搬入物を受け入れる際、不審物のチェックが入念に行われていないこと	4.4(3)	搬入物の受渡し	搬入物の受入れを行う従業員は受入れの際に危険物持込や情報漏洩等のリスクがないかどうか点検しなければならない。	・巧妙に偽装され点検では発見できない不審物による攻撃。
10	・第三者の出入りによる、情報資産の盗難、漏洩	・資産目録等へ登録が速やかに行われない場合があり、機器が盗難・紛失しても、わからないこと	4.4(4)	搬入物の受渡し	搬入物が登録の必要な情報資産である場合、搬入物の受入れを行う従業員は受入れ後速やかに登録作業を行わなければならない。	・資産目録への登録ミス。
11	・郵便物の盗み見、盗難、紛失	・郵便物の抜き取りが可能な、未施錠ポストを利用していること ・重要な郵便物は本人限定受取郵便などにして、盗み見や抜き取られないように、受取本人が受領するようにしていないこと ・郵便物が盗み見られたことに気づかないこ	4.4(5)	搬入物の受渡し	郵便物の受入れ場所には盗み見や抜き取りを防止する対策を行わなければならない。	・郵便物が受け取る係り（メール室等）から宛先本人に渡るまでのルートのリスク対策がされていないと紛失・情報漏洩の危険がある。
12	・第三者による情報の盗み聞き	・場所をわきまえずに重要な情報が会話されていること	4.5(1)	盗み聞きによる情報漏えい防止	従業員は電話や立ち話、オープンな会議スペースでの発言について、盗み聞きを防止するよう配慮しなければならない。	・盗聴器による盗聴。

対象標準	セキュリティインシデント報告・対応標準

NO	脅威	脆弱性	遵守事項（JNSAポリシーサンプル0.92版）			残存リスク
			項番	項タイトル	内容	
1	・ソーシャルエンジニアリングによるパスワード、機密情報の漏洩。 ・テールゲーティングによる物理的不正侵入。 ・メール感染型ワームの蔓延。 ・許可を得ていない接続によるウイルスの蔓延	・社員のセキュリティ意識が低いこと。 ・契約社員、協力会社のセキュリティ意識が低いこと。	4.1（1）	平時の準備	情報セキュリティ委員会は、『セキュリティ教育に関する標準』に基づいて、セキュリティ教育を実施し、従業員のセキュリティ意識の向上に努めなければならない。	・教育を受けていない新入社員に対するソーシャルエンジニアリング、テールゲーティング ・故意による機密情報の漏洩 ・教育内容の漏れ ・教育内容の理解不足
2	・ウィルスによるデータの破壊。 ・ウィルスの蔓延によりシステム資源の使用不能	・ウィルス対策が施されていないコンピュータの存在すること。	4.1（2）	平時の準備	従業員は業務上、利用するすべてのコンピュータについて、『ウィルス対策標準』に基づいて、適切にウィルス対策を実施しなければならない。	・定期的ウィルススキャンの間のウィルス感染 ・新規導入中のコンピュータへのウィルス感染 ・未知のウイルスの感染
3	・セキュリティホールを悪用するウィルスの蔓延。 ・セキュリティホール悪用による不正侵入、機密情報の漏洩、DoS攻撃。	・セキュリティホールが放置されたコンピュータの存在すること。	4.1（3）	平時の準備	情報システム部は、『セキュリティ情報収集および配信標準』に基づいて、当社で使用されている製品のセキュリティ情報を収集し、必要なセキュリティ対策を実施することでセキュリティレベルを維持しなければならない。	・未知のセキュリティホールを悪用した攻撃による不正侵入 ・未知のセキュリティホールを悪用したウィルスの蔓延 ・新たなセキュリティホールが見つかってセキュリティ対策を施すまでの間における不正侵入、ウィルスの蔓延 ・ベンダからのセキュリティ情報発信が不十分なセキュリティホールを悪用した不正侵入、ウイルスの蔓延 ・ベンダのパッチに不備があり、対策が不十分となる可能性。
4	・セキュリティインシデントの再発。	・インシデント対応が行われない状態になること ・インシデント対応(検知・原因究明)の遅れが発生すること	4.1（4）	平時の準備	情報システム部は、インシデントの検知や原因究明に役立てるために『システム監視に関する標準』に基づいて、適切にログを取得しなければならない。	・インシデント発生から対策までの間のインシデントの再発 （・多量のログ解析に時間がかかりインシデントの検知・原因究明が遅れること ・スキル不足による原因究明の遅れ） ・必要なログが取られていなかった場合、原因究明ができない。

対象標準	セキュリティインシデント報告・対応標準

NO	脅威	脆弱性	遵守事項（JNSAポリシーサンプル0.92版）			残存リスク
			項番	項タイトル	内容	
5	・ネットワークを経由した第三者の侵入。 ・社内における認可されていない機器への不正アクセス。 ・トラヒックの増大によるシステム停止（Dos攻撃等も含む）。	・不正侵入があっても検知できないこと。 ・各システム機器への不正なアクセスがあっても検知できないこと。	4.1（5）	平時の準備	情報システム部は、インシデントを検知するため、『システム監視に関する標準』に基づいて、侵入検知システムを利用し、適切にシステムおよびネットワークの監視を行わなければならない。	・ネットワーク監視システムが検知できない手法による攻撃は検知できない。 ・ネットワーク監視システムが監視していないシステムへの不正アクセス、トラヒックの増大等は検知できない。 ・誤検知のため（不正侵入なのに検知されず）、不正侵入を見逃してしまう可能性。 ・検知数が多いため十分に解析できずに侵入を見逃してしまう可能性。
6	・各種インシデントの発生によるサービスの停止。	・各種インシデント発生時に復旧ができないこと。 ・バックアップを取得していても、バックアップ自体を消失、紛失した場合にサービスの復旧ができないこと。	4.1（6）	平時の準備	情報システム部は、インシデント発生後のシステムの復旧作業に役立てるために『システム維持に関する標準』に基づいて、適切にバックアップを取得しなければならない。なお、バックアップは必要に応じて遠隔地にコピーを保管することが望ましい。	・バックアップのコピーまで消失するような地域災害時には復旧できない。 ・バックアップメディアの劣化により必要時に復旧できない。 ・復旧に必要なデータが取得できていなかった場合、復旧できない（バックアップ対象範囲の不備）。 ・リストアの訓練不足により必要時に復旧できない。 ・バックアップ取得後に更新・追加されたデータ消失の可能性がある。 ・遠隔地のバックアップの保管管理方法が適切でない場合、情報漏えいのおそれがある（新規リスク）。
7	・各種インシデントの発生によるサービスの停止。	・各種インシデント発生時に復旧ができない、または復旧が遅れること。	4.1（7）	平時の準備	情報システム部は、インシデント発生後のシステムの復旧作業に必要なリソースを検討し、確保しておかなければならない。	・想定外のリソース不足による復旧の遅れ ・外部リソース損失による復旧不能

対象標準	セキュリティインシデント報告・対応標準

NO	脅威	脆弱性	遵守事項（JNSAポリシーサンプル0.92版）			残存リスク
			項番	項タイトル	内容	
8	・各種インシデントの発生によるサービスの停止。	・インシデント発生時にどのサービスを優先的に復旧させればいいかがわからず、復旧の遅れ等により損失が発生すること。	4.1（8）	平時の準備	情報セキュリティ委員会は、各システムの復旧優先度を決定しなければならない。復旧優先度の決定は、対象システムにおいて運用される業務の停止許容時間を観点において行う。 表1 復旧優先度　業務復旧までの許容時間 3　業務が停止することは許されない 2　24時間以内に復旧しなければならない 1　3日以内に復旧しなければならない 0　インシデント発生時は停止してもよい	・優先度の低いシステムの復旧が遅れることによる損失。 ・復旧優先度の設定ミスによる損失。 ・許容時間内に発生する損失。
9	・ウイルスの感染等、各種インシデント被害の拡大。	・従業員に対する対応手順の周知もれが発生すること。	4.2(1)	セキュリティインシデント発生時	従業員はインシデントの発生と疑われる事象を発見した場合、速やかに情報セキュリティ委員会もしくはセキュリティ担当者に報告しなければならない。またクライアントPCにおいて、ウイルス感染や不正アクセスの疑いがある場合、発見後ただちに該当するクライアントPCをネットワークから切り離した上で報告しなければならない。	・疑わしいと判断するレベルの差による対応の遅れ（パソコンの調子が悪いのでRebootしたが、実はウィルスに感染していた等）。

対象標準	セキュリティインシデント報告・対応標準

NO	脅威	脆弱性	遵守事項（JNSAポリシーサンプル0.92版）			残存リスク
			項番	項タイトル	内容	
10	・ウイルスの感染等、各種インシデント被害の拡大。	・対応方法が未整備の攻撃やウィルスが存在しうること。 ・セキュリティ担当者（対応を指示できる人）の不在であること。 ・インシデントが発生した場合の的確な処置を行っていないこと。	4.2(2)	セキュリティインシデント発生時	（1）の報告を受けた情報セキュリティ委員会およびセキュリティ担当者は、下記の観点で状況把握し、対応方法を報告者に指示しなければならない。セキュリティ担当者が報告を受けた場合は、対応方法を報告者に指示するとともに下記事項を速やかに情報セキュリティ委員会に報告しなければならない。 またセキュリティ担当者のみでの作業が困難である場合は、速やかに情報セキュリティ委員会に申し出て、協力を依頼すること。 ＜観点＞ ・インシデント発生の真偽 ・被害を発見した日時 ・被害の拡大範囲 ・被害内容 ・被害原因 ・対応方法	・ログ等を取得しておらず状況を把握できない。 ・情報セキュリティ委員会でも対応が困難なインシデントが発生した場合、復旧が難しい。 ・インシデントの同時多発による対応の遅れ
11	・新種のウィルスや未知の攻撃手法。 ・各種インシデントの発生。	・インシデント発生時の連絡体制ができていないこと	4.2(3)	セキュリティインシデント発生時	インシデントの発生が確認された場合、情報セキュリティ委員会は速やかに関連する部署（情報システム部、広報担当等）、プロバイダー、外部ベンダー等に連絡し、協力を依頼しなければならない。 また、情報セキュリティ委員会は必要に応じて組織横断的なタスクフォースを設け、状況把握や対応方法の指示にあたることができる。	・代替措置としてサービスの停止やネットワークの切断を実施した場合に機会損失が発生する。
12	・ウィルスや不正侵入によるシステムの破壊。	・バックアップを取得していないこと	4.2(4)	セキュリティインシデント発生時	情報システム部は、インシデントの原因が解消された後、速やかにバックアップテープを用いてシステムを正常な状態に復旧しなければならない。復旧作業にあたっては、4．1（8）で決定した復旧優先度に従って作業すること。	・ウィルス感染やバックドア、トロイの木馬が仕掛けられた状態のバックアップテープの使用による被害の拡大 ・バックアップテープの劣化により復旧ができない可能性がある。 ・バックアップ取得後に更新・追加されたデータ消失の可能性がある。

対象標準	セキュリティインシデント報告・対応標準

NO	脅威	脆弱性	遵守事項（JNSAポリシーサンプル0.92版）			残存リスク
			項番	項タイトル	内容	
13	・二次被害の発生。	・インシデントの影響範囲がわからない等による二次被害を想定していないこと	4.2(5)	セキュリティインシデント発生時	従業員は、インシデントの2次被害防止のため、OS、アプリケーションの入れ替えやクライアントPCの設定変更等の作業が必要になった場合は、情報セキュリティ委員会の指示に従い、速やかに実施しなければならない。	・二次被害の判断ミス。
14	・インシデントの再発。	・再発防止計画の検討されていないこと	4.3(1)	再発防止計画	セキュリティインシデントへの対応が完了した後、情報セキュリティ委員会および情報システム部は、調査結果をもとに再発防止計画を作成しなければならない。再発防止計画作成時には、技術的側面と組織的側面の両方に留意すること。	・時間の経過とともに情報資産が変化し、セキュリティイベントの影響範囲が前例と異なるため、再発防止計画の有効性が低くなるおそれがある。
15	・インシデントのレベルに応じた適切な計画が作成されず、社外への対応不十分により信用失墜	・重大なインシデントに対する、取締役会の認識が不十分であること。 ・社外的なインパクトを考慮したリスクマネジメント全体に基づく判断の、再発防止計画に対して反映していないこと。	4.3(2)	再発防止計画	情報セキュリティ委員会は発生したインシデントのうち、以下の要件を満たすものについては、再発防止計画と共に取締役会に報告しなければならない。 ＜要件＞ ・社外の第三者からのセキュリティ侵害により当社が被害者となる場合。 ・顧客や取引先等の社外に対して当社が加害者となる場合	・偶然重大化しなかったインシデントについて妥当な影響レベルを予測出来ず、関連するセキュリティイベントを軽視する。
16	・再発防止計画に沿った対応の未実施	・従業員に対する再発防止計画の周知もれ、または周知が不十分であること	4.3(3)	再発防止計画	再発防止計画は、すべての従業員に周知され、適切に実施されなければならない。	・社員の異動時に関する周知もれ。 ・再発防止計画の周知・実施までの間のインシデント再発。
17	・過去のインシデント、関連する再発防止計画を速やかに参照できない。 ・計画を見直す際に、不適切な変更が検討される。	・再発防止計画を作成した経緯、各計画に関連するインシデントおよびセキュリティイベントの内容についての管理が不十分であること	4.3(4)	再発防止計画	情報セキュリティ委員会は、セキュリティインシデントの発生から再発防止計画作成までの一連の記録を保管・管理しなければならない。	・過去の事例に基づく再発防止では対応できない、新しい手法による攻撃の被害発生。
18	・インシデント対応の手順通りに作業ができないことによる被害の拡大。	・インシデント対応手順不備の見落とし、及びインシデント対応作業者の手順に対する理解や熟練が不十分であること	4.4(1)	運用の見直し（訓練計画）	本標準の内容の実効性を担保するため、情報セキュリティ委員会は、定期的にセキュリティインシデントの訓練計画を作成し、従業員参加のもと、訓練を実施しなければならない。	・対応手順や訓練計画で想定していなかったタイプのインシデントによる被害発生（対応の不備）。 ・訓練実施が不可能なインシデントの発生。

対象標準	セキュリティインシデント報告・対応標準

NO	脅威	脆弱性	遵守事項（JNSAポリシーサンプル0.92版）			残存リスク
			項番	項タイトル	内容	
19	・インシデント対応訓練で発覚した対応手順の不備と同じ問題でのインシデント対応失敗。	・インシデント対応訓練結果のフィードバックが不十分であること	4.4(2)	運用の見直し（訓練の評価）	・訓練の結果は情報セキュリティ委員会においてレビューし、セキュリティ対策の運用について改善策の審議を実施しなければならない。 ・訓練の結果は、改善策とともにすべての従業員に周知されなければならない。	・インシデント対応の改善策中の不備の存在（いわゆるデグレード）。 ・訓練実施が不可能なインシデントの発生。
20	・発生したインシデントの対応で発覚した対応手順の不備と同じ問題でのインシデント対応失敗。	・発生したインシデントの対応結果のフィードバックが不十分であること	4.4(3)	運用の見直し（インシデント後の見直し）	情報セキュリティ委員会は、セキュリティインシデントの事後に一連の対応を見直し、運用上の改善点を検討しなければならない。検討の結果、運用変更が必要であると認められた場合、速やかに関係する従業員に周知されなければならない。	・インシデント対応の改善策中の不備の存在（いわゆるデグレード）。