Microsoft セキュリティ アセスメント ツール

中規模企業向け
Aisen
完了 05-10-05 0:15

このレポートは以下のセクションで構成されています。

- エグゼクティブ サマリ
  - はじめに
  - 背景：アセスメントのプロセスおよび範囲
  - 状況分析
  - 採点表
  - セキュリティ イニシアチブ
- アセスメントの詳細
  - 分析の対象領域
    - インフラストラクチャ
    - アプリケーション
    - 運用
    - 人的要素
- 優先順位付きの対応リスト
- 付録
  - 質問と回答
  - 用語集
  - グラフの解釈

Microsoft パートナーが、このレポートを検証し、提案を実装するための詳細な実施計画の開発をお手伝いします。Microsoft パートナーとの取引がまだない場合は、http://directory.microsoft.com/mprd/ でセキュリティ ソリューション関連の Microsoft パートナーのリストを表示できます。

エグゼクティブ サマリ

はじめに

この Microsoft セキュリティ アセスメント ツールは、自社のコンピュータ環境におけるセキュリティ リスクの特定と対処を支援するために設計されています。このツールでは、総合的なアプローチを使用し、人的要素、プロセス、および技術にわたるトピックを対象とすることによってセキュリティ戦略を測定します。所見には、推奨のリスク低減策が併記されています。必要に応じて参照できる詳細情報へのリンクなども記載されています。このリソースは、よりセキュアな環境を作るツールや方法を理解する上で有用となるでしょう。

このまとめセクションでは、IT マネージャおよび上級マネージャに自社の全体的なセキュリティ状況の概要を提供します。詳細な所見および提案は、以下の詳細なレポートに記載されています。

背景：アセスメントのプロセスおよび範囲

このアセスメントは、組織のビジネス リスクと、リスクを低減するために導入されているセキュリティ対策を特定するために設計されています。この市場区分に共通する問題に注目し、ビジネスを支える技術、プロセス、人的な観点から上位レベルのアセスメントを提示するためにアンケートが開発されました。

自社のビジネス モデルに関するアンケートで始まるこのツールでは、選択した業界およびビジネス モデルに応じて、注目する必要のあるビジネス上のリスクを測定し、ビジネス リスク プロファイル (BRP) を構築できます。2 つ目のアンケートは、時間の経過に伴って導入されたセキュリティ対策のリストをまとめるためのものです。これらのセキュリティ対策は連動して複数の防御層を形成し、セキュリティ リスクや特定の脆弱性に対する防御を強化します。各層が、1 つに組み合わされた多層防御戦略に貢献します。各層の合計を多層防御のインデックス (DiDI) といいます。次に BRP と DiDI を比較して、インフラストラクチャ、アプリケーション、運用、人的要素の分析領域 (AoAs) におけるリスク分布が測定されます。

セキュリティ リスク対防御の測定に加え、このツールでは、自社のセキュリティの成熟度も測定できます。セキュリティの成熟度とは、強力なセキュリティと維持可能な施策の展開度を指します。最低レベルでは、セキュリティ防御がほとんど導入されておらず、対応も受身です。最高レベルでは、確立された検証済みのプロセスによって、より予防的な措置を取ることができ、必要に応じて効率よく一貫した対応ができます。

提示されるリスク管理提案は、導入済みの技術、現在のセキュリティ状況、および多層防御施策が反映され、回答企業にカスタマイズされたものとなります。この提案を、業界で認知されているベスト プラクティスに進むための手引きとして活用してください。

アンケート、測定、提案で構成されているこのアセスメントは、自社環境に 50 ～ 500 台のデスクトップを持つ中規模企業を対象としています。このアセスメントでは、特定の技術またはプロセスの詳細な分析ではなく、企業環境全体におけるリスクの可能性を幅広く対象領域としています。したがって、このツールでは導入されているセキュリティ対策の実効性は測定できません。そのため、このレポートは、より厳しい配慮を必要とする特定の領域に焦点を当てる際の準備的な手引きとして使用してください。このレポートは、アセスメントを専門とする第三者による評価の代わりとなるものではありません。

状況分析

このセクションでは、お客様の回答に基づいて、前述の概念を図式的に示します。メモ：

- BRP は、業界および企業のビジネス モデルに関連するリスクを測定したものです。
- DiDI は、ビジネスについて特定されたリスクを低減するために、人的要素、プロセス、技術にわたって使用されているセキュリティ防御を測定したものです。
- セキュリティの成熟度は、多くの部門にわたって維持可能なセキュリティ レベルを作成するために利用できるツールを効果的に使用する能力を測定したものです。

[これらの用語の詳細およびグラフの解釈方法については、「付録」を参照してください。]

結果：

分析の対象領域	リスク対防御の分布	セキュリティの成熟度
インフラストラクチャ		
アプリケーション		
運用		

人的要素	●	●

リスク対防御の分布

この図は、分析領域ごとの多層防御の評価の違いを示しています。リスク アセスメントに対する回答によると、以下のチャートに表示されているように、防御策で対処するリスクが多すぎますが、改善の余地があります。これは、環境全体の保護を少数の防御策に依存している可能性があることを示しています。

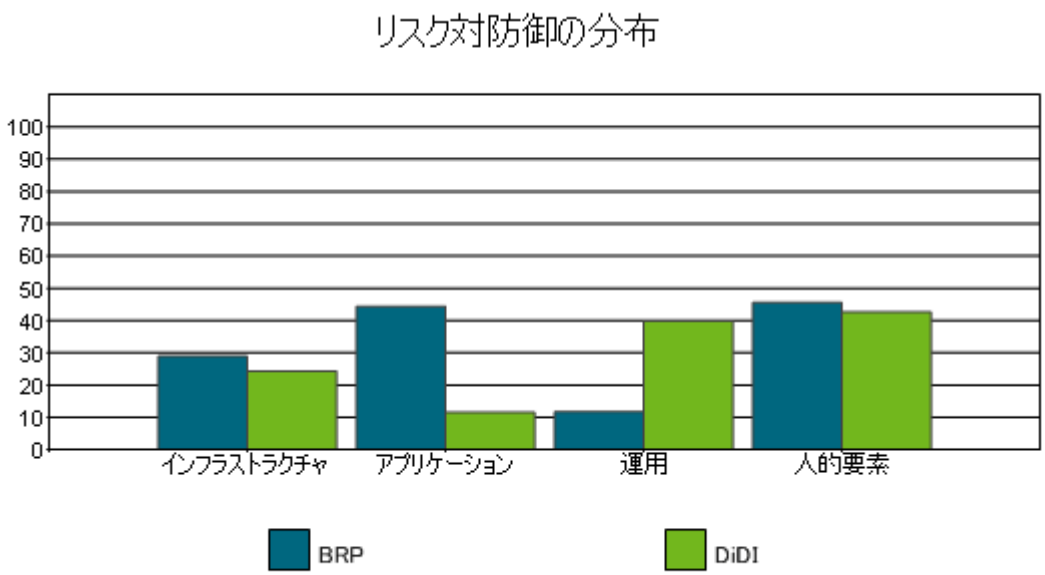

図 1 : BRP と DiDI の比較

一般に、同じカテゴリの DiDI の点数と BRP の点数が同等であることがベストです。カテゴリ内またはカテゴリ間での不均衡は、どちらの点数が高くても、IT 投資の見直しが必要であることを示します。

セキュリティの成熟度

セキュリティの成熟度では、制御 (物理的なものおよび技術的なもの)、IT リソースに対する技術的な洞察力、ポリシー、プロセス、維持可能な施策などが考慮されます。利用可能なあらゆるツールを効果的に使用して、いかなる制限にも対応できるセキュリティ レベルを作成できるかどうかが、組織のセキュリティの成熟度の判断基準となります。セキュリティの成熟度のベースラインを確立し、それを使用して組織のセキュリティ プログラムで重点を置くべき領域を定義する必要があります。すべての組織のセキュリティ レベルを最適レベルにする必要はありませんが、現在直面しているビジネス リスクを考慮し、現状を把握して目標を設定する必要があります。例えば、セキュリティ リスクが低い IT 環境を持つ企業では、ベースライン レベルの上限または標準レベルの下限を変更してセキュリティの強化を図る必要はないかもしれません。一方、セキュリティ リスクが高い IT 環境を持つ企業は、最適レベルのセキュリティを導入しようとするでしょう。セキュリティ リスクの評価には、ビジネス リスク プロファイルの点数を参考にします。

- セキュリティの成熟度 — 維持可能なセキュリティについて、企業の施策を業界で認知されているベスト プラクティスと比較した値。各企業は、ビジネスを推進する中で生じるリスクに対して、関連するセキュリティ戦略と成熟度レベルが見合うように努力する必要があります。
- ベースライン — 防衛の最前線として予防的なセキュリティ対策が導入されていますが、運用および事故への対応はまだ非常に受身です。
- 標準 — 定義されている戦略を支える複数の防御層が導入されています。
- 最適 — 適切な対象を適切な方法で効果的に保護しています。ベスト プラクティスが確実に使用されています。

リスク アセスメントに対する回答によると、以下のチャートに表示されているように、セキュリティの多層アプローチの開発と、運用および事故への対応により主体的なアプローチを取ることにさらに重点を置く必要があります。まず、包括的な社内セキュリティ ポリシーを作成し、それを IT インフラストラクチャのポリシーおよび手順を開発する手引きとして使用します。ポリシーおよび手順のフレームワークが固まったら、それらを使用して、業界で認知されているベスト プラクティスに従った、必要なだけの防御を資産に適用するセキュリティの多層アプローチを定義できます。

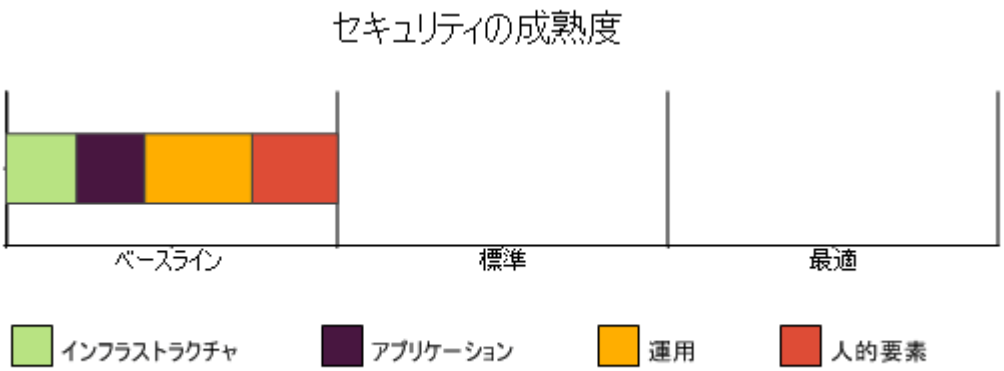

図 2 : セキュリティの成熟度

採点表

リスク アセスメントに対する回答によると、防御策の点数は以下ようになります。このレポートの「アセスメントの詳細」および「優先順位付きの対応リスト」セクションには、それぞれについて所見、ベスト プラクティス、提案を含むさらに詳細な情報が記載されています。

凡例 : ● ベスト プラクティスに適合 ● 改善が必要 ● 著しく不足

インフラストラクチャ ●
防衛線内での防御 ●
- ファイアウォール規則とフィルタ ●
- ウイルス対策 ●
- ウイルス対策 - デスクトップ ●
- ウイルス対策 - サーバー ●
- リモート アクセス ●
- セグメンテーション ●
- リモート アクセス ユーザー ●
- 侵入検知システム (IDS) ●
- ワイヤレス ●

認証 ●
- 管理者 ●
- 内部ユーザー ●
- リモート アクセス ユーザー ●
- パスワード ポリシー ●
- パスワード ポリシー - 管理者アカウント ●
- パスワード ポリシー - ユーザー アカウント ●
- パスワード ポリシー - リモート アクセスのアカウント ●

管理とモニタリング ●
- 構築 ●
- セキュアな構築 ●
- 第三者との関係 ●
- 物理的セキュリティ ●

アプリケーション ●
アプリケーション ●
- ロードバランシング ●
- クラスタリング ●
- アプリケーションとデータ復旧 ●

運用 ●
環境 ●
- ファイアウォール規則とフィルタ ●
- 管理者 ●
- 管理ホスト ●
- 管理ホスト - サーバー ●
- 管理ホスト - ネットワーク デバイス ●
- 第三者との関係 ●

セキュリティ ポリシー ●
- セキュアな構築 ●
- プロトコルとサービス ●
- 利用規定 (AUP) ●
- ユーザー アカウント管理 ●
- セキュリティ要件 ●
- ガバナンス ●
- セキュリティ ポリシー ●

修正プログラムと更新プログラムの管理 ●
- ネットワーク ドキュメンテーション ●
- アプリケーション データ フロー ●
- パッチ管理 ●
- ウイルス データ ファイル ●
- 変更と構成の管理 ●

バックアップと復旧 ●
- ログ ファイル ●
- バックアップ ●
- バックアップ メディア ●
- バックアップと復元 ●

人的要素 ●
要件と評価 ●
- セキュリティ要件 ●
- セキュリティ評価 ●
- セキュリティ意識 ●

サードパーティ独立系ソフトウェア ベンダ (ISV)	🔴
内部開発	🔴
脆弱性	🔴
アプリケーション設計	🔴
認証	🔴
パスワード ポリシー	🟡
認証とアクセス制御	🟢
ロギング	🟡
入力の検証	🟢
データ ストレージと通信	🔴
暗号化	🔴
暗号化 - アルゴリズム	🔴
ポリシーと手順	🔴
経歴調査	🟢
人事管理規定	🔴
第三者との関係	🟡
研修と意識	🔴
セキュリティ意識	🟡

セキュリティ イニシアチブ

以下の領域でベスト プラクティスが不足しているため、自社環境のセキュリティを強化するために対処する必要があります。このレポートの「アセスメントの詳細」および「優先順位付きの対応リスト」セクションには、それぞれについて所見、ベスト プラクティス、提案を含むさらに詳細な情報が記載されています。

高 (優先順位)	中 (優先順位)	低 (優先順位)
暗号化 - アルゴリズム	ウイルス データ ファイル	ファイアウォール規則とフィルタ
管理ホスト - ネットワーク デバイス	プロトコルとサービス	バックアップ
ログ ファイル	アプリケーション データ フロー	変更と構成の管理
暗号化	ユーザー アカウント管理	利用規定 (AUP)
セキュリティ評価	セキュリティ ポリシー	構築

アセスメントの詳細

レポートのこのセクションには、各カテゴリの詳細な所見、ベスト プラクティス、提案、および詳細情報の参照先が記載されています。次のセクションには、優先順位付きの提案が記載されています。

分析の対象領域

以下の表は、セキュリティ リスク アセスメントの上位レベル分析で使用した対象領域を示し、各領域のセキュリティに対する関連性を説明したものです。このドキュメントの「アセスメントの詳細」セクションに、アセスメントの回答から明らかとなった各領域についての自社のセキュリティ状況と、業界で広く認知されているベスト プラクティスと、そのプラクティスを実行するための提案をまとめています。

カテゴリ	セキュリティの重要性
ビジネス リスク プロファイル	
ビジネス リスク プロファイル	リスク低減を効率よく進めるには、自社のビジネスの特性がリスクに与える影響を理解して、リソースを適用すべき箇所を特定しなければなりません。ビジネス リスクのクリティカルとなる部位を知ることで、セキュリティ関連予算を適切に配分することができます。
インフラストラクチャ	
境界での防衛	境界での防衛では、自社の内部ネットワークが外部の世界と接続されるネットワーク境界部分のセキュリティを扱います。侵入者に対する最初の防衛線となります。
認証	ユーザー、管理者、リモート ユーザーの認証手順を厳しくすることで、部外者がローカル アカウントまたはリモート アカウントを介して攻撃した場合でも、ネットワークへの不正アクセスを防止することができます。
管理とモニタリング	IT 環境を維持し、分析するには、管理、モニタリング、および適切なロギングが不可欠です。攻撃を受けてセキュリティ事象を解析しなければならない場合に、これらのツールはより重要となります。
ワークステーション	どのような環境であっても、個々のワークステーションのセキュリティは防衛上不可欠な要素であり、とくにリモート アクセスを許可している場合は一層重要となります。一般的な攻撃に対抗できる安全措置をワークステーションに講じておかなければなりません。
アプリケーション	
導入と使用	ビジネス推進に不可欠なアプリケーションを本稼動として導入する場合、それらアプリケーションとサーバーに対しセキュリティと可用性を確保しなければなりません。継続的なメンテナンスを行って、セキュリティ バグに修正プログラムを適用するとともに、新しい脆弱性を環境内に取り込まないように努めることが不可欠です。
アプリケーション設計	アプリケーション設計では、認証、承認、データ検証のようなセキュリティ メカニズムを適切に実装しないと、攻撃を仕掛ける者にセキュリティ脆弱性の利用を許してしまうことになり、機密情報にアクセスを与えてしまいます。
データ ストレージと通信	あらゆる経営においてデータの完全性と秘匿性は重要な課題です。データ喪失やデータ盗難は、企業の収益に影響を与えるだけではなく企業の評判をも傷つけます。ビジネスの重要なデータが、アプリケーションによってどのように処理され、どのように保護されているかを理解することが重要です。
運用	
環境	企業のセキュリティは、適用されている業務手順、プロセス、ガイドラインに依存します。それらを改善することで、企業のセキュリティを、技術面での防御にとどまらずさらに高めることができます。業務部門が企業環境のセキュリティを支え、維持していくには、環境の正確な文書化とガイドライン化が不可欠です。
セキュリティ ポリシー	企業のセキュリティ ポリシーとは、技術と手順のセキュアかつ適切な利用方法を規定した、社内で適用されている種々のポリシーとガイドラインを指します。この分析領域では、ユーザー、システム、データなど、さまざまなセキュリティに対応するポリシーを取り上げます。
バックアップと復旧	災害やハードウェア/ソフトウェア障害が発生した場合でもビジネスの継続性 (コンティニュイティ) を維持するには、データのバックアップと復旧が不可欠です。バックアップと復旧の手順が適切に定められていないと、データと生産性の多大な損失を招きます。
修正プログラムと更新プログラムの管理	企業内の IT 環境のセキュリティを維持する上で、適切な修正プログラムと更新プログラムの管理が重要です。修正プログラムと更新プログラムは、既知で利用可能な脆弱性をふさぐために、随時適用しなければなりません。
人的要素	

要件とアセスメント	意思決定者全員にセキュリティ要件を理解させ、技術的な意思決定と事業的な意思決定が互いに衝突するのではなく、セキュリティを高める方向に働くようにしなければなりません。第三者に定期的なアセスメントを委託することで、自社のセキュリティの調査、評価、および改善すべき領域の特定が可能になります。
ポリシーと手順	明確かつ現実的な規定によって第三者との関係を管理すれば、企業がさらされるリスクの範囲が限定されます。また、従業員の雇用と退職に関する規定によって、従業員が持つ悪意や不満から組織を防衛しなければなりません。
教育と意識	従業員には研修を実施し、たとえ意図しなくても自社を多大なリスクに露呈させることを防ぐために、日々の業務がどのようにセキュリティに関係しているか認識させなければなりません。

アセスメントの分析

このセクションは、インフラストラクチャ、アプリケーション、オペレーション、人的要素の 4 つの主な領域に分かれています。

インフラストラクチャ

インフラストラクチャのセキュリティでは、あるべきネットワークの機能、ビジネス プロセスとしてサポートすべき事項(外部または内部)、ホスト コンピュータの構築と展開の方法、ネットワークの効果的な運用と保守の方法にそれぞれ焦点をあてています。効果的なインフラストラクチャ セキュリティは、ネットワーク防御、事案への対応、ネットワークの可用性、障害分析といったさまざまな領域に著しい改善をもたらす手段となります。中身が完全に把握され、かつ継続的な維持が図られる強固なインフラストラクチャ設計を確立することで、リスクの識別と脅威の緩和が可能になります。アセスメントでは、以下のインフラストラクチャ セキュリティ領域に焦点を当て、企業のインフラストラクチャ リスクの低減の支援を目的とした上位レベルの手順を検証します。

- 境界での防御—ファイアウォール、ウイルス対策、リモート アクセス、セグメンテーション
- 認証—パスワード ポリシー
- 管理とモニタリング—管理ホスト、ログ ファイル
- ワークステーション—構築の構成設定

防衛線内での防御		
サブカテゴリ	ベスト プラクティス	
ファイアウォール規則とフィルタ	ファイアウォールは防衛の最前線の役割を持ち、すべてのネットワーク境界に配置しなければなりません。ファイアウォールに実装する規則は高度に限定的なものとし、ホストごと、およびサービスごとに設定しなければなりません。 ファイアウォールの規則やルーターの ALC (アクセス制御リスト) を作成する場合は、まず第一に、アクセス制御デバイスとネットワークを外部の攻撃から防御することに焦点を置きます。 + ネットワークの ALC とファイアウォールの規則を使用してデータフローを強化します。 + 現行の規則が DoS (サービス拒否) 攻撃に効果があるかを確認するため、ファイアウォールの規則とルーターの ALC の検証を行ってください。 + 体系的かつ正式なファイアウォール整備の一環として 1 つ以上の DMZ を導入してください。 + インターネットからアクセスできるサーバーはすべて DMZ 内に配置します。DMZ へのアクセスおよび DMZ からのアクセスは制限してください。	
	所見	提案
ファイアウォール規則とフィルタ	回答によれば、ファイアウォールがオフィスごとに導入されています。	ファイアウォールまたは他のネットワークレベルのアクセス制御の各オフィスでの導入を継続してください。また、すべてのファイアウォールが正常に機能しているかどうかを頻繁にテストして確認してください。
	所見	提案
ファイアウォール規則とフィルタ	回答によれば、サーバーを保護するホストベース ファイアウォール ソフトウェアを使用しています。	すべてのサーバーへのホストベースのファイアウォールのインストールを継続してください。また、このソフトウェアを社内のすべてのデスクトップ PC とノート PC に導入することを検討してください。

リソース

インターネット ファイアウォールに対するFAQ

このFAQは、ファイアウォールの導入について理解を深めたい、ITプロフェッショナルではないユーザーに適しています。

http://www.microsoft.com/japan/security/protect/firewall.asp

Deploying Firewalls: By Fithen,William, et al. Software Engineering Institute, Carnegie Mellon University, 1999.

この文書中にある実施事項は、システム、セキュリティおよびネットワーク管理者向けのものです。著者が提供しているのは、ファイアウォールを展開する全段階におけるシステムの設計から、必要な仕様に対してファイアウォールのシステムをテストするセキュリティ ポリシーを反映するための設定、そして最終的なロール アウトのための推奨策です。

http://www.cert.org/security-improvement/modules/m08.html

ネットワークをセキュリティ保護する

これはネットワーク管理者と IT 専門家向けに書かれたものです。ネットワーク レベルの最大の脅威とその対策方法について説明されています。 セキュリティ問題とルーター、ファイアウォール、そしてスイッチに適用する設定を検証しています。

http://www.microsoft.com/japan/msdn/security/guidance/secmod88.mspx

サブカテゴリ	ベスト プラクティス	
ウイルス対策	サーバーからデスクトップに至る環境全体にウイルス対策を適用してください。ファイル サーバー スキャナ、コンテンツ スクリーニング ツール、データ アップロード/ダウンロード スキャナなど、特定の処理には専用のウイルス対策を導入してください。 ウイルス対策ソフトウェアは、自社に入ってくるウイルスと、自社から出ていくウイルスの両方についてスキャンするように設定してください。 ウイルス対策は、最初に重要なファイル サーバーに対して行い、次にメール サーバー、データベース サーバー、Web サーバーの順に適用してください。 デスクトップ PC およびノート PC の環境を構築する際は、ウイルス対策クライアントをデフォルトで導入してください。 Microsoft Exchange を使用している場合は、Microsoft Exchange が提供しているウイルス対策およびコンテンツフィルタ機能をメールボックス レベルで追加してください。	
	所見	**提案**
ウイルス対策	回答によれば、境界ホストにウイルス対策ソフトウェアがインストールされています。	
	所見	**提案**
ウイルス対策	回答によれば、電子メールサーバーにウイルス対策ソフトウェアがインストールされています。	

リソース

ウイルス対策ソフトウェアに関するFAQ

このFAQは、ウイルス対策ソフトウェアの理解を深めたい、ITプロフェッショナルではないユーザーに適しています。

http://www.microsoft.com/japan/security/protect/antivirus.asp

サブカテゴリ	ベスト プラクティス	
ウイルス対策 - デスクトップ		
	所見	**提案**
ウイルス対策 - デスクトップ	回答によれば、ウイルス対策がデスクトップ レベルに適用されています。	現状の施策を継続してください。ユーザーに、ウイルス データ ファイルを定期的に更新するポリシーを適用してください。 ワークステーション環境の構築では、ウイルス対策クライアントをデフォルトで追加してください。

サブカテゴリ	ベスト プラクティス	
ウイルス対策 - サーバー		
	所見	**提案**
ウイルス対策 - サーバー	回答によれば、ウイルス対策がサーバー レベルに適用されています。	現状の施策を継続してください。サーバーに接続されているウイルス対策クライアントに対して、集中管理コンソールから設定とウイルス データ ファイルを配備するアクティブな管理方法を検討してください。 Microsoft Exchange を使用している場合、メール ボックス レベルでウイルス対策やコンテンツ フィルタ機能の追加を検討してください。

サブカテゴリ	ベスト プラクティス	
リモート アクセス	あらゆる環境においてワークステーションは防御のボトルネックであり、特に、リモート ユーザーやローミング ユーザーに社内環境への接続を許しているときに顕著となります。 パーソナル ファイアウォールやウイルス対策などのツールやリモート アクセス ソフトウェアをすべてのワークステーションに導入し、適切に構成してください。 これらツール類には定期的な見直しが必要なポリシーを実装して、使用中のアプリケーションやサービスの変更がツールの構成に反映されるようにし、同時に、ワークステーションが攻撃に対して耐性を常に維持できるようにしてください。	
	所見	**提案**
リモート アクセス	回答によれば、内部ネットワークにリモート アクセスできます。	
	所見	**提案**
リモート アクセス	回答によれば、パートナやベンダといった第三者、または従業員はリモートから内部ネットワークに接続でき、また、VPN テクノロジの実装という重要な判断が下されています。しかし、さらなる防衛手段として求められる多元的な認証は導入されていません。	インターネットを経由した会社のリソースへのリモート ユーザー接続に多元的な認証方法の導入を検討してください。VPN デバイス上のアクセス一覧をすべてのユーザーに対して定期的に監査してください。
	所見	**提案**
リモート アクセス	回答によれば、この質問の回答を知りません。	IT 部門の担当者またはセキュリティ関係のパートナとともにこの保留項目を見直してください。詳細について、MSAT のこの質問に最もふさわしい回答を入力してください。

サブカテゴリ	ベスト プラクティス	
セグメンテーション	ベンダ、パートナー、および顧客のアクセスから特定のエクストラネットを分離するために、セグメンテーションを使用してください。 顧客にサービスを提供する場合は、その際に使用する特定のアプリケーション ホストとポートに特定のアプリケーション トラフィックのみがルーティングされるように、外部に向けられているそれぞれのネットワーク セグメントを設定してください。 第三者からの接続については、それぞれが必要なものにしかアクセスできないように、ネットワーク制御でアクセスを確実に制限してください。 提供しているネットワーク サービスへのアクセス、またはネットワーク サービスからのアクセスを制限してください。また、ネットワーク セグメント間のアクセスも制限してください。	
	所見	**提案**
セグメンテーション	回答によれば、ネットワークが複数のセグメントで構成されています。	ネットワーク トラフィックを適切に管理し、ユーザーの要件に応じてリソースへのアクセスを制限するために、ネットワーク セグメントの使用を継続してください。
	所見	**提案**

セグメンテーション	回答によれば、外部顧客からのアクセスやエクストラネット サービスと会社のリソースとを分離するネットワーク セグメントは実装されていません。顧客/パートナ固有のエクストラ ネットサービスは、個別のネットワーク セグメント上に置くことが重要です。	エクストラネット アクセス サーバーを物理的に異なるネットワーク セグメントに分離してください。 第三者からのアクセスに対して、特定のホストのみ接続を許可し、社内インフラストラクチャへのアクセスは必要なもののみに制限し、リモート ネットワークへの接続は遮断するよう制限をかけてください。

リソース

中小規模、リモートオフィスネットワークのためのセキュリティ

このシスコの SAFE SMR は、ネットワーク セキュリティの設計に多層防御のアプローチを取り入れたものです。セキュリティを多層で防御することで、一つのセキュリティ システムの不具合によりネットワーク リソース全体を危険にさらさないためのものです。組織にセキュアなネットワークを設計、構築するために、この最善策をご使用ください。

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8a0.shtml

サブカテゴリ	ベスト プラクティス	
リモート アクセス ユーザー	アクセス方法がダイヤルアップ経由または VPN 経由に関わらず、すべてのリモート アクセス ユーザーに複雑なパスワードを必要とするポリシーを適用してください。下記の条件を満たすものを複雑なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 8 文字以上 リモート アクセス アカウントに追加的な認証手段の実装を検討してください。また、アカウント管理 (アカウント共有不可) やアカウント アクセス ログに、高度な統制を採用してください。 リモート アクセスで重要なことは、強力なアカウント管理の実践、完全なログ取得の実践、および問題の検知機能を駆使して、会社のリソースを保護することです。さらに、リモート アクセス サービスを介してブルート フォース方式を用いたパスワード攻撃が行われるリスクを低減するために、下記の制御の実装を検討してください + 期限付きパスワード + ログインに 7 ～ 10 回失敗した場合にアカウントをロックアウト + システムでのログ取得 リモート アクセスでは、ネットワークおよびホストへのアクセスに使用するシステム上のリモート アクセス サービスも考慮に入れなければなりません。また、リモート アクセス経由でネットワークへのアクセスが許可されているホストには、アクセス制御の実装を検討してください。	
	所見	**提案**
リモート アクセス ユーザー	回答によれば、従業員がネットワークにリモート アクセスできます。	リモート アクセスに対して多元的な認証システムをまだ使用していない場合は、その使用を検討してください。また、リモート アクセスを業務上必要な従業員のみに制限してください。
	所見	**提案**
リモート アクセス ユーザー	回答によれば、契約社員がネットワークにリモート アクセスできます。	従業員からのリモート アクセスに関するベスト プラクティスに従うほかに、契約社員からの接続を、リモート アクセスが必要なシステムのみに制限することを検討してください。また、契約社員からの接続をより容易に制御および制限するために、契約社員用に別のエントリ ポイントを使用することを検討してください。

サブカテゴリ	ベスト プラクティス	
侵入検知システム (IDS)	企業システムに対する攻撃を検知して通知するため、ネットワーク ベースおよびホスト ベースの侵入検知システムを導入する必要があります。	

	所見	提案
侵入検知システム (IDS)	回答によれば、侵入検知用ハードウェアまたはソフトウェアを使用していません。	ホストベースまたはネットワークベースの侵入検知システムの導入を検討してください。
	所見	**提案**
侵入検知システム (IDS)	回答によれば、ホストベースの侵入検知システム (HIDS) を使用していません。	ホストベースの侵入検知システムの導入を検討してください。ホストに対する攻撃が発生すると管理者に通知されるので、管理者は随時対応することができます。
	所見	**提案**
侵入検知システム (IDS)	回答によれば、ネットワークベースの侵入検知システム (NIDS) を使用していません。	ネットワークベースの侵入検知システムの導入を検討してください。ネットワークに対する攻撃が発生すると管理者に通知されるので、管理者は随時対応することができます。

リソース

監査と侵入検出

このドキュメントが提供するのは、記録する必要のあるイベントの種類と、侵入者を検出することの重要性に関する高レベルな概要です。さまざまなモニター技術および検出方法を取り上げています。

http://www.microsoft.com/japan/technet/security/prodtech/win2000/secwin2k/09detect.asp

サブカテゴリ	ベスト プラクティス	
ワイヤレス	ワイヤレス ネットワークの実装に関するベスト プラクティスの 1 つは、ネットワーク自体の SSID をブロードキャストしないということです。WPA 暗号化機能を使用し、基本的にネットワークは信頼性が低いものとして扱ってください。	
	所見	**提案**
ワイヤレス	回答によれば、ネットワークにワイヤレス接続できません。	ワイヤレス アクセスを許可しないことで、リスクにさらされる可能性は低減します。ただし、将来ワイヤレス アクセスを計画または実装する場合は、実装時に SSID のブロードキャストを無効にし、WPA 暗号化 を採用してネットワークを信頼できないものとして扱ってください。
	所見	**提案**
ワイヤレス	回答によれば、ワイヤレス ネットワークを信用できないものとして扱っていません。	データの完全性を保持するために、ワイヤレス ネットワークを信頼できないネットワーク セグメントに移行し、VPN または類似のテクノロジを使用することを検討してください。
	所見	**提案**
ワイヤレス	回答によれば、ワイヤレス環境で WEP 暗号化を使用していません。	現在暗号化を使用していない場合は、ワイヤレス ネットワーク トラフィックの傍受および平文の読み取りを防止するために、WPA の使用を検討してください。
	所見	**提案**
ワイヤレス	回答によれば、ワイヤレス環境で WPA 暗号化を使用していません。	現在暗号化を使用していない場合は、ワイヤレス ネットワーク トラフィックの傍受および平文の読み取りを防止するために、WPA の使用を検討してください。
	所見	**提案**
ワイヤレス	回答によれば、アクセス ポイントの SSID のブロードキャストをディスエーブルにしていません。	一時的なユーザーがワイヤレス ネットワークに接続しにくくなるように、SSID のブロードキャストの無効化を検討してください。
	所見	**提案**
ワイヤレス	回答によれば、ワイヤレス環境で MAC 制限を使用していません。	MAC フィルタに加えて、WPA 認証の使用を検討してください。許可されていないコンピュータからネットワークに接続できなくなります。
	所見	**提案**
ワイヤレス	回答によれば、アクセス ポイントの SSID をデフォ	アクセス ポイントやワイヤレス ネットワークの悪用

	ルト値から変更していません。	を防止するために、SSID を、会社とは簡単に結び付かない値に速やかに変更してください。

認証		
サブカテゴリ	ベスト プラクティス	
管理者	管理アカウントについては、複雑なパスワードを必要とする制限の厳しいポリシーを適用してください。下記の条件を満たすものを複雑なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 14 文字以上 さらに、パスワード攻撃が行われた場合のリスクを低減するために、下記の制御を実装してください。 + 期限付きのパスワード + ログインに 7 ～ 10 回失敗した場合にアカウントをロックアウト + システムでのログ取得 複雑なパスワードの実装に加えて、多元的な認証手段の実装を検討してください。アカウント管理 (アカウント共有不可) やアカウント アクセス ログに高度な制御を採用してください。	
	所見	提案
管理者	回答によれば、デバイスやホストへの管理アクセスの認証には単純なパスワードしか用いられていません。または、パスワードは使用されていません。	すべての管理アカウントとサービス アカウントに複雑なパスワード制御の実装を検討してください。下記の条件を満たすものを複雑なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 8 文字以上

サブカテゴリ	ベスト プラクティス	
内部ユーザー	ユーザー アカウントに、複雑なパスワードを必要とするポリシーを適用してください。下記の条件を満たすものを複雑なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 8 文字以上 さらに、パスワード攻撃が行われた場合のリスクを低減するために、下記の制御を実装してください。 + 期限付きパスワード + ログインに 10 回以上失敗した場合にアカウントをロックアウト + システムでのログ取得 複雑なパスワードの実装に加えて、多元的な認証手段の実装を検討してください。 アカウント管理 (アカウント共有不可) やアカウント アクセス ログに、高度な制御を採用してください。	
	所見	提案
内部ユーザー	回答によれば、社内のネットワークとホストへのユーザー アクセスの認証には単純なパスワードしか用いられていません。または、パスワードは使用されていません。	アクセス レベルにかかかわらず、すべてのユーザーに複雑なパスワード制御の実装を検討してください。下記の条件を満たすものを複雑なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 8 文字以上

サブカテゴリ	ベスト プラクティス	
リモート アクセス ユーザー	アクセス方法がダイヤルアップ経由または VPN 経由に関わらず、すべてのリモート アクセス ユーザーに複雑なパスワードを必要とするポリシーを適用してください。下記の条件を満たすものを複雑なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 8 文字以上 リモート アクセス アカウントに追加的な認証手段の実装を検討してください。また、アカウント管理 (アカウント共有不可) やアカウント アクセス ログに、高度な統制を採用してください。 リモート アクセスで重要なことは、強力なアカウント管理の実践、完全なログ取得の実践、および問題の検知機能を駆使して、会社のリソースを保護することです。さらに、リモート アクセス サービスを介してブルート フォース方式を用いたパスワード攻撃が行われるリスクを低減するために、下記の制御の実装を検討してください + 期限付きパスワード + ログインに 7 ～ 10 回失敗した場合にアカウントをロックアウト + システムでのログ取得 リモート アクセスでは、ネットワークおよびホストへのアクセスに使用するシステム上のリモート アクセス サービスも考慮に入れなければなりません。また、リモート アクセス経由でネットワークへのアクセスが許可されているホストには、アクセス制御の実装を検討してください。	
	所見	**提案**
リモート アクセス ユーザー	回答によれば、内部ネットワークやホストへのリモート アクセスの認証には単純なパスワードしか用いられていません。または、パスワードが使用されていません。	許可されたアクセスがダイヤルアップ経由か VPN 経由かにかかわらず、すべてのリモート アクセス ユーザーに複雑なパスワード制御の実装を検討してください。下記の条件を満たすものを複雑なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 8 文字以上

サブカテゴリ	ベスト プラクティス
パスワード ポリシー	一般に、管理者用パスワードの作成に適用される制限は、一般ユーザー アカウントのパスワードに適用される制限よりも厳格である必要があります。 Windows システムの場合、管理者アカウント (およびサービスアカウント) のパスワードは、英数字と特殊文字が混在した 14 文字の長さでなければなりません。

リソース

White paper on Password Recovery for Web-based Applications

この文書は、開発者とアプリケーションのビジネス所有者の両者を対象にしており、システムのユーザーが企業の顧客またはクライアントである Web アプリケーションに焦点が当てられています。パスワードの復旧についての異なるテクニックが、それぞれの利点を交えて説明されています。

http://fishbowl.pastiche.org/archives/docs/PasswordRecovery.pdf

サブカテゴリ	ベスト プラクティス	
パスワード ポリシー - 管理者アカウント		

	所見	提案
パスワード ポリシー - 管理者アカウント	回答によれば、管理者アカウントにパスワード ポリシーが適用されています。	管理アカウントに対して、成功と失敗のすべての認証のロギングやモニタリングなどの追加保護措置の実装を検討してください。 平文のテキスト プロトコルは避けてください。

サブカテゴリ	ベスト プラクティス	
パスワード ポリシー - ユーザー アカウント		
	所見	提案
パスワード ポリシー - ユーザー アカウント	回答によれば、ユーザー アカウントにはパスワード ポリシーが適用されています。	認証の失敗回数がしきい値を超えたときに、通知をシステム管理者に送るようなロギング方法の実装を検討してください。 パスワード ポリシーのテストの実施を検討してください。

サブカテゴリ	ベスト プラクティス	
パスワード ポリシー - リモート アクセスのアカウント		
	所見	提案
パスワード ポリシー - リモート アクセスのアカウント	回答によれば、リモート アクセス アカウントにはパスワード ポリシーは適用されていません。	示されたベスト プラクティスに従って、リモート アクセスのアカウントにパスワード ポリシーの実装を検討してください。

管理とモニタリング		
サブカテゴリ	ベスト プラクティス	
構築	ベンダから提供されているすべてのセキュリティ更新プログラムと推奨ロックダウン構成を使用して構築プロセスを維持してください。このプロセスは定期的に検証してください。 各ホストでハードニング手順を使用して、セキュリティ更新プログラムを適用し、サービスおよびアプリケーションを正しく構成してください。不必要なサービスとアプリケーションは無効にしてください。 ワークステーションは、推奨セキュリティ更新プログラムの適用、不必要なパッケージやサービスの削除、ファイル許可の監査を行って、ハードニングしてください。 ワークステーションの標準構築手順にハードニングを組み入れてください。	
	所見	提案
構築	回答によれば、ワークステーションの構築にインストール イメージまたは正式な文書は使用されていません。	各ワークステーションに対するセキュアなシステム構築手順を作成してください。最新のサービス パック、ホット フィックス、その他のハードニング テクニックを使用して、構築方法を定期的に更新してください。

サブカテゴリ	ベスト プラクティス	
セキュアな構築		
	所見	提案
セキュアな構築	回答によれば、システム構築にホストのハードニング手順が含まれていません。	SANS、NIST、NSA、またはその他の標準的なホストのハードニング手順に従って、すべてのシステムを構築してください。
	所見	提案
セキュアな構築		

	回答によれば、リモート制御/管理ソフトウェアを社内環境で使用していません。	リモート制御/管理ソフトウェアを使用しないという現状の施策を継続してください。
	所見	**提案**
セキュアな構築	回答によれば、ディスク暗号化ソフトウェアを社内環境で使用していません。	マシンの盗難時のデータ障害を防止するために、ディスク暗号化ソフトウェアの使用を検討してください。
	所見	**提案**
セキュアな構築	回答によれば、パスワードで保護されたスクリーン セーバーを社内環境で使用していません。	短時間の休憩時にもパスワードで保護されたスクリーン セーバーの使用をすべてのユーザーに義務付けることを検討してください。
	所見	**提案**
セキュアな構築	回答によれば、すべてのワークステーションにはパーソナル ファイアウォールはインストールされていません。	使用中のアプリケーションやサービスの変更に対応して、デフォルトのファイアウォール設定を定期的に見直すポリシーを実装してください。
	所見	**提案**
セキュアな構築	回答によれば、ワークステーションには、内部ネットワークに接続するリモート クライアント ソフトウェアはインストールされていません。	リモート アクセスが必要な場合は、リモート アクセスのクライアント ソフトウェアを個々のワークステーションに導入することを検討してください。また、そのソフトウェアは、リモート アクセス サーバーのポリシーに適合するように構成してください。
	所見	**提案**
セキュアな構築	回答によれば、モデムを社内環境で使用していません。	マシンに直接ダイヤル インされるリスクを低減するために、モデムとダイヤルアップ アクセスの無効化を継続してください。

リソース

Securing Public Web Servers

このコラムでは、一般向けの Web サイトの運営に関連する危険性を緩和する方法を説明しています。Web サーバー ソフトウェアおよび基礎となるホスト オペレーティング システムの構成、Web サーバーの完全性の保持などのトピックが取り扱われています。

http://www.cert.org/security-improvement/modules/m11.html

passfilt.dll

Passfilt.dll とは Microsoft® Windows NT® 4.0 オペレーティング システムの代替の .dll です。passfilt を使用して、オペレーティング システムの既定のパラメータを変更し、強力なパスワードのサポートおよび管理者のアカウント ロックアウト (ネットワーク レベルで) を提供することができます。

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/strong_password_enforcement_and_passfilt_dll.asp

The Twenty Most Critical Internet Security Vulnerabilities

このリストは、SANS (SysAdmin, 監査, ネットワーク, セキュリティ) インスティチュートおよび FBI の国家インフラ防護センター (NIIPC) によって編集されました。Microsoft® Windows® のオペレーティング システム で悪用されることの多い 10 のサービスと、Linux および Unix で最も一般的に悪用される 10 のサービスについて説明しています。ご使用の環境で悪用される可能性のある脆弱性の特定、そして推奨されている対策方法の確認にご使用ください。

http://www.sans.org/top20/#threats

NSA Security Recommendation Guides

このガイドは米国家安全保障局 (NSA) が提供しているネットワーク セキュリティの改善に関する技術的なアドバイスです。IP ルーター (特にシスコ システムズのルーターの詳細な取り扱い方法を掲載) 設定の原則とガイダンスが含まれています。この情報はアクセス管理、攻撃防御、ネットワーク コンポーネントのシールド、そしてネットワーク トラフィックの整合性と機密保持に対処するものです。

http://www.nsa.gov/snac/cisco/index.html

Microsoft Gold Certified Partners

セキュリティ ソリューションに関するマイクロソフト認定ゴールド パートナープログラムは、ユーザーのセキュリティ向上を支援する IT ソリューションの構築、展開を提供する専門企業を見つけることをお手伝いします。マイクロソフトは、パートナー企業にマイクロソフトの技術やソリューションに関して高いレベルの専門知識を取得してもらえるよう、密に連携をとっています。

http://directory.microsoft.com/resourcedirectory/Services.aspx

Windows Server 2003 セキュリティ ガイド

このガイドは、さまざまな環境に対応するセキュアなWindows Server 2003の構築方法を記載した、分かりやすいアドバイス、ツール、テンプレート集です。サーバーのインストールと構築に責任を負っているネットワーク管理者とITプロフェッショナルにとって有用な情報が書かれています。

http://www.microsoft.com/japan/technet/security/prodtech/win2003/w2003hg/sgch00.asp

Microsoft Baseline Security Analyzer (MBSA)

MBSAは、Windowsシステムをスキャンしてセキュリティ パッチの適用有無などを調べるアプリケーションで、ダウンロードによって入手可能です。スキャンするコンピュータのアカウント設定やパスワード強度を調べる簡単なツールも付属します。MBSAはWindows 2000、Windows XP、Windows Server 2003で動作します。

http://www.microsoft.com/japan/technet/security/tools/tools/mbsahome.asp

データベース サーバーをセキュリティ保護する

このガイドは、データベース設計者およびデータベース管理者を対象に書かれています。このガイドはデータベース サーバー (特に Microsoft® SQL Server™) をセキュアにするための効果的な手順を提供しています。このガイドはデータベース サーバーに影響を及ぼす最も一般的な脅威について検討し、セキュアな構成を適用するプロセスを紹介しています。

http://www.microsoft.com/japan/msdn/security/guidance/secmod91.mspx

UNIX & インターネットセキュリティ 第2版 Simson Garfinkel, Gene Spafford 著

この本はユーザーおよび管理者を対象としており、Unix ホストとネットワーク セキュリティに関する実用的な情報を掲載しています。Unix のセキュリティ対策の実施に関する問題、アプローチとその方法を取り上げています。

http://www.amazon.co.jp/exec/obidos/ASIN/4900900389/qid=1116995480/

サブカテゴリ	ベスト プラクティス	
第三者との関係	企業がさらされるリスクを低減するため、第三者との関係を定めた正式な規定と手続きが必要です。規定と手続きによって、セキュリティの問題と各法人の責任分担が明らかとなります。 第三者との規定には、下記のような事項を定めてください。 + 接続とアクセスのレベル + データの提供と操作 + それぞれの法人の役割と責任 (権限を含む) + パートナシップの管理—立ち上げ、進行中、終了	
	所見	提案
第三者との関係	回答によれば、社内スタッフがシステムを設定しています。	システムの構成は、社内スタッフがテスト済みの構築イメージに従って行ってください。

サブカテゴリ	ベスト プラクティス	
物理的セキュリティ	盗難を防ぐため、すべてのコンピュータ システムに細心の注意を払ってください。サーバーとネットワーク機器は、施錠したキャビネットに保管して部屋の鍵を締め、入室を制限する必要があります。	
	所見	提案

物理的セキュリティ	回答によれば、企業の資産を守るための、物理的なセキュリティ制御が導入されていません。	重要なシステムおよびネットワーク コンポーネントへのアクセスをセキュアなものにするために、物理的な制御の使用を速やかに計画してください。また、将来的にはすべてのコンピュータ機器に対して物理的なセキュリティ制御を行うことを検討してください。
	所見	**提案**
物理的セキュリティ	回答によれば、サーバーを施錠可能なキャビネットか棚に入れていません。	サーバーを施錠可能なキャビネットや棚に保管すると、不正な改ざんからの保護を強化できます。可能な場合は、サーバーを施錠可能な場所に移動することを検討してください。
	所見	**提案**
物理的セキュリティ	回答によれば、侵入を検知して報告するアラームシステムがインストールされていません。	侵入の検知および報告を行うために、警報システムの導入を検討してください。
	所見	**提案**
物理的セキュリティ	回答によれば、ネットワーク機器を、入室が制限されている鍵のかかった部屋に保管していません。	ネットワーク機器を施錠した部屋やクローゼットに保管してください。ネットワーク機器をよりセキュアな場所に移動することを計画してください。
	所見	**提案**
物理的セキュリティ	回答によれば、ワークステーションをワイヤーロック鍵で固定していません。	盗難を防ぐために、ワイヤーロックを使用してワークステーションをセキュアに維持することを検討してください。
	所見	**提案**
物理的セキュリティ	回答によれば、ノート PC をワイヤーロック鍵で固定していません。	盗難を防ぐために、ワイヤーロックを使用してノート PC をセキュアに維持することを検討してください。
	所見	**提案**
物理的セキュリティ	回答によれば、機密データの印刷物を、施錠されたファイル キャビネットに保管していません。	機密情報の盗難や公開を防ぐために、機密文書は、施錠したキャビネットに保管してください。
	所見	**提案**
物理的セキュリティ	回答によれば、ネットワーク機器を施錠可能なキャビネットか棚に入れていません。	ネットワーク機器を施錠可能なキャビネットや棚に保管すると、不正な改ざんからの保護を強化できます。可能な場合は、ネットワーク機器を施錠可能な場所に移動することを検討してください。
	所見	**提案**
物理的セキュリティ	回答によれば、サーバーを、入室が制限されている鍵のかかった部屋に保管していません。	サーバーを施錠した部屋やクローゼットに保管してください。サーバーをよりセキュアな場所に移動することを計画してください。

リソース

Basic Physical Security

このリソースが提供するのは、物理セキュリティにおける 3 つの基本原則である、人を近づけない、遮断する、そしてネットワーク接続の保護についてです。

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-203.asp

アプリケーション

アプリケーション セキュリティを完全に理解するには、アプリケーションのユーザー ベースだけでなく、根底にある基本的なアプリケーション アーキテクチャについて十分に理解している必要があります。潜在的な脅威の大きさと性質の特定を開始できるのはその後です。

この自己アセスメントは範囲が限定されているため、アプリケーション アーキテクチャの完全な分析やユーザー ベースの完全な理解はできません。このアセスメントでは、自社内のアプリケーションを確認し、セキュリティと可用性の観点からそれらを評価することを目的としています。また、多層防御 (DID) を強化するために社内環境で使用されている技術を検証します。アセスメントでは、以下のアプリケーション セキュリティ領域に焦点を当て、企業のアプリケーション リスクの低減の支援を目的とした上位レベルの手順を検証します。

- 導入と使用—可用性を高めるメカニズム

- アプリケーション設計—認証、アクセス制御、更新プログラムの管理、入力の検証、ログと監査
- データ ストレージと通信—暗号化、データ転送、アクセス制限

アプリケーション		
サブカテゴリ	ベスト プラクティス	
ロードバランシング		
	所見	提案
ロードバランシング	回答によれば、ロード バランサーは導入されていません。	Web サーバーの可用性を高めるため、Web サーバーの前段にハードウェア ロード バランサーの導入を検討してください。 ロード バランサーは外部には仮想的に単一の IP アドレスを提供し、クラスタ化された各 Web サーバーのアドレスにマッピングします。

サブカテゴリ	ベスト プラクティス	
クラスタリング		
	所見	提案
クラスタリング	回答によれば、クラスタリングは導入されていません。	重要なデータベースとファイル共有の可用性を向上させるために、クラスタリング方式の導入を検討してください。

サブカテゴリ	ベスト プラクティス	
アプリケーションとデータ復旧		
	所見	提案
アプリケーションとデータ復旧	回答によれば、あなたの会社は基幹業務アプリケーションを導入しています。	基幹業務 (LOB) アプリケーションがある場合は、セキュリティを定期的に評価し、バックアップを定期的に行い、完全に文書化し、障害に備えて代替手段を用意してください。
	所見	提案
アプリケーションとデータ復旧	回答によれば、アプリケーション復旧とデータ復旧のテストは行われていません。	フル バックアップを定期的に行ってください。アプリケーションを正常状態に復帰させるバックアップと復旧のテストを定期的に行ってください。

サブカテゴリ	ベスト プラクティス	
サードパーティ独立系ソフトウェア ベンダ (ISV)	サードパーティ独立系ソフトウェア ベンダ (ISV) は、アプリケーションのセキュリティ更新プログラムとアップグレードを定期的に提供し、セキュリティ更新プログラムの目的や、適用後のアプリケーションの機能、構成、セキュリティなどへの影響について説明する必要があります。 サードパーティ (ISV) は、重要なセキュリティ更新プログラムを明確に区別して、そのプログラムが迅速に適用されるようにしなければなりません。 サードパーティ (ISV) は、アプリケーションのセキュリティ メカニズムのすべてを説明し、最新のドキュメントを提供しなければなりません。 アプリケーションを導入している部門は、最高レベルのセキュリティの実現に必要な設定要件を理解しなければなりません。	
	所見	提案
サードパーティ独立系ソフトウェア ベンダ (ISV)	回答によれば、サードパーティ ベンダは、社内の重要なアプリケーションをまったく開発していません。	重要アプリケーションの社内開発を継続してください。ただし、将来サード パーティからの調達が決定した場合は、重要アプリケーションを開発したサードパーティが該当アプリケーションのサポートを継続し、適宜更新プログラムを提供し、万が一アプリケーションのサポートを終了する場合にはソース コー

		ドを提供する用意があることを確認してください。

サブカテゴリ	ベスト プラクティス	
内部開発	社内開発部門は、アプリケーションのセキュリティ更新プログラムとアップグレードを定期的に提供し、セキュリティ更新プログラムの目的や、適用後のアプリケーションの機能、構成、セキュリティなどへの影響ついて説明する必要があります。 社内開発部門は、重要なセキュリティ更新プログラムを明確に区別して、企業がそのプログラムを迅速に適用できるようにしなければなりません。 開発部門は、アプリケーションのセキュリティ メカニズムのすべてを説明し、最新のドキュメントを提供しなければなりません。 アプリケーションを導入している部門は、最高レベルのセキュリティの実現に必要な設定要件を理解しなければなりません。 アプリケーション アーキテクチャや導入の見直し、および懸念されるセキュリティ問題の特定のために、第三者への業務委託を検討してください。	
	所見	**提案**
内部開発	回答によれば、あなたの会社はオフィス アプリケーションにカスタム マクロを使用しています。	カスタム マクロを使用するには、Office のセキュリティ設定をダウングレードして、アプリケーションを悪意のあるドキュメント類に対して公開する必要があります。カスタム マクロを開発および実行できるのは、業務上必要な従業員のみに制限することを検討してください。
	所見	**提案**
内部開発	回答によれば、社内でアプリケーション開発に携わっている開発部門は、開発したアプリケーション向けに、ソフトウェア更新プログラム、セキュリティ修正プログラムを定期的に提供してくれません。	社内開発部門と連携を試み、導入済みアプリケーションのソフトウェア アップグレードと更新プログラムを定期的に入手できるように努めてください。 更新プログラムが提供された場合、運用システムに適用する前に開発環境で完全なテストを行ってください。 社内開発部門と協業し、最高のセキュリティを維持できるようアプリケーションの設定を精査してください。 アプリケーション アーキテクチャや導入の見直し、および懸念されるセキュリティ問題の特定のために、第三者への業務委託を検討してください。

サブカテゴリ	ベスト プラクティス	
脆弱性	すべての既知のセキュリティ脆弱性を特定して、セキュリティ更新プログラムを適用しなければなりません。ベンダの Web サイトや他のセキュリティ サイトを定期的に監視して、導入済みアプリケーションの脆弱性に関する情報や入手可能なセキュリティ更新プログラムについて確認してください。 セキュリティ脆弱性が既知であるにも関わらずセキュリティ更新プログラムがない場合は、プログラムの提供時期を特定し、該当の脆弱性に対して暫定的なリスク軽減策を策定してください。 アプリケーションのセキュリティ設計を評価するために、第三者による定期的な監査の実施を検討してください。第三者によって、追加のセキュリティ対策が必要となる領域が判明することもあります。	
	所見	**提案**
脆弱性	回答によれば、セキュリティ上の既知の脆弱性に対応する手順は決められていません。	アプリケーション ベンダ (ISV または社内開発部門) と連携し、セキュリティの脆弱性への取り組み計画を策定してください。 更新プログラムが提供された場合、運用システムに適用する前に開発環境で完全なテストを行ってください。 さらに、更新プログラム適用後に各アプリケーションのテストを行い、更新プログラムのロールバックを

		必要とするアプリケーション固有の障害を検証してください。

リソース

Advanced SQL Injection in SQL Server Applications by Chris Anley

この文書では、Microsoft® Internet Information Services Server および SQL Server™ の攻撃に使われる一般的な SQL インジェクションの手法について説明しています。SQL インジェクションとは、普通のテキスト入力フィールドを介し有害である可能性のある文字を渡すことによりデータベースを攻撃する方法です。

http://www.nextgenss.com/papers/advanced_sql_injection.pdf

アプリケーション設計		
サブカテゴリ	**ベスト プラクティス**	
認証	アプリケーションには、データや機能のアクセスを制御するセキュリティ要件と同程度の認証機能を実装しなければなりません。パスワードに依存するアプリケーションには、文字の混在 (アルファベット/数字/記号)、最小文字数、履歴管理、有効期限の強制、有効期限の前倒し、辞書チェックといった、複雑なパスワードの制約を適用しなければなりません。 アプリケーションは、認証に失敗したログインの試行について、パスワード情報以外をログに記録しなければなりません。データや機能にアクセスするすべて要素が適切な認証資格情報を備えているか確認する必要があります。 システムへの管理者アクセスは、利用可能な最も強力な認証形式で保護する必要があります。一般に、管理者用パスワードの作成に適用される制限は、一般ユーザー アカウントの制限よりも厳格でなければなりません。 適正なパスワード ポリシーが適用された強力なパスワードに加え、他の認証手段によるセキュリティ強化を検討してください。	
	所見	**提案**
認証	回答によれば、重要アプリケーションには簡単なパスワード認証が適用されています。	重要アプリケーションのすべてのアカウントに複雑なパスワード制御の実装を検討してください。 下記の条件を満たすものを強力なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 8 文字以上

サブカテゴリ	**ベスト プラクティス**
パスワード ポリシー	強力なパスワードの使用は「多層防御」を得る基本的な要素です。強力なパスワードとは、8 ～ 14 文字で構成された、英数字と特殊文字を含む文字列です。パスワードに対する、最小文字数の規定、メンテナンス履歴、有効期限、有効期限の前倒しなど、防御を高めるすべての施策を設定してください。一般に、パスワードの有効期限は下記の条件で設定します。 + 最長 90 日 + 新規アカウントはログイン時にパスワード変更が必要 + 8 個のパスワード履歴を保存 (最低 8 日) システムへの管理者アクセスは、利用可能な最も強力な認証形式で保護する必要があります。一般に、管理者用パスワードの作成に適用される制限は、一般ユーザー アカウントの制限よりも厳格でなければなりません。一般ユーザー アカウントのパスワードの長さが 8 文字に規定されている場合は、管理者アカウントのパスワードの長さは 14 文字にする必要があります。 すべてのユーザー アカウントに対して、ログイン認証を 10 回失敗した場合にはアカウント ロックアウトを適用してください。アカウント ロックアウトの制御方法は、ブルート フォースによるパスワード攻撃を防ぐための単純なブロックから、管理者介入によってアンロックする複雑な方法までさまざまです。アカウント ロックアウト制御を実装する場合は、下記のガイドラインについて検討してください。

	+ ユーザー アカウントは 10 回以上のログイン失敗でロックアウト + 重要なアプリケーションに対するアカウントのアンロックには管理者のアクセスを必要とし、他のアプリケーションに対する一般ユーザー アカウントのアンロックは 5 分後に自動的に実行する + 一般ユーザー アカウントのキャッシュ問題は 30 分後に自動的復旧	
	所見	**提案**
パスワード ポリシー	回答によれば、重要アプリケーションには強力なパスワード制御は適用されていません。	すべてのアプリケーションに強力なパスワード制御の実装を検討してください。 下記の条件を満たすものを強力なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 8 文字以上
	所見	**提案**
パスワード ポリシー	回答によれば、重要アプリケーションにはアカウント ロックアウト制御は適用されていません。	外部に提供されているすべての重要なアプリケーションには、まず初めに、アカウント ロックアウト (10 回のログイン失敗後) の適用を考慮してください。アカウント ロックアウトの制御方法は、ブルート フォース式によるパスワード攻撃を防ぐための単純なブロックから、管理者の介入によってアンロックする複雑な方法などさまざまです。アカウント ロックアウト制御を実装する場合は下記のガイドラインを検討してください。 + 10 回以上のログイン失敗でロックアウト + カウントのアンロックには管理者アクセスが必要 + 一般ユーザー アカウントは 30 分後に自動的に復元
	所見	**提案**
パスワード ポリシー	回答によれば、重要アプリケーションには期限付きパスワード制御が適用されています。	期限付きパスワードの導入を、外部に提供されているすべてのアプリケーション、および、機密データを操作する重要な内部アプリケーションに拡大することを検討してください。

サブカテゴリ	**ベスト プラクティス**	
認証とアクセス制御	アプリケーションには、機密データや機能へのアクセスを特定の許可されたユーザーまたはクライアントのみに提供する、承認機能を実装しなければなりません。 ロールに基づくアクセス制御を、データベース レベルとアプリケーション インターフェースに適用してください。 このような制御を行うことで、クライアント アプリケーションが悪用された場合でもデータベースを保護できます。 認証が成功する前に、認可を確認する必要があります。 適切な認可を受けずにアクセスしようとしたすべての試みをログに記録する必要があります。 機密データを処理する重要なアプリケーションと、ユーザーがインターネット経由で利用できるインターフェイスに対して、定期的なアプリケーション テストを実施してください。アプリケーション テストでは「ブラック ボックス」と「ホワイト ボックス」の両方を行ってください。他のアカウントからデータへのアクセス権を取得できるか確認してください。	
	所見	**提案**
認証とアクセス制御	回答によれば、重要アプリケーションには、アカウントの特権レベルに基づいた機密データや機能へのアクセス制限が適用されています。	機密データを処理する重要アプリケーションと、ユーザーがインターネット経由で利用できるインターフェイスに対して、集中的なアプリケーション テストの実施を検討してください。 アプリケーションに対して「ブラック ボックス」と「ホワイト ボックス」の両方のテストを行い、併せて特権エスカレーション テストも行ってください。

サブカテゴリ	ベスト プラクティス	
ロギング	企業環境内のすべてのアプリケーションで、ログを有効にしてください。ログ ファイル データは、問題の発生、傾向の分析、および監査目的において重要です。 アプリケーションは、認証に失敗したログインと成功したログイン、ユーザー アカウントを含むアプリケーション データの変更、重度のアプリケーション エラー、リソースに対するアクセスの失敗と成功などの情報をログとして取得しなければなりません。 ログ データへの書き込みでは、機密データを書き込まないようにしなければなりません。	
	所見	**提案**
ロギング	回答によれば、アプリケーションはさまざまなイベントをログ ファイルに記録しています。ベスト プラクティスに示されたすべてのイベントを記録します。	ログ ファイルの管理と分析を楽にするため、集中ロギング方式によるログの統合を検討してください。このロギング方式では、企業データの保持ポリシーに従い、ログの保管とアーカイブが行わなければなりません。
	所見	**提案**
ロギング	回答によれば、ユーザー アカウントの変更をログに記録していません。	特権エスカレーションおよび新規アカウントの不正作成を検出するために、ユーザー アカウントの変更のロギングを検討してください。
	所見	**提案**
ロギング	回答によれば、リソースに対するアクセスの成功をログに記録していません。	悪意のある動作を事後に追跡するために、リソースに対するアクセス成功のロギングを検討してください。
	所見	**提案**
ロギング	回答によれば、リソースに対するアクセスの拒否をログに記録していません。	特権エスカレーションでの試行を検出できるように、リソースに対するアクセス拒否のロギングを検討してください。
	所見	**提案**
ロギング	回答によれば、データの変更をログに記録していません。	悪意のある動作を追跡するために、データの変更のロギングを検討してください。
	所見	**提案**
ロギング	回答によれば、アプリケーション エラーをログに記録しています。	アプリケーション エラーのロギングを継続してください。
	所見	**提案**
ロギング	回答によれば、認証成功をログに記録していません。	ユーザーの動作を追跡するために、認証成功のロギングを検討してください。
	所見	**提案**
ロギング	回答によれば、認証失敗をログに記録していません。	ブルート フォース攻撃を検知するために、認証失敗のロギングを検討してください。

サブカテゴリ	ベスト プラクティス	
入力の検証	アプリケーションは、ユーザー、クライアント アプリケーション、提供データなどの外部ソースからの、複数のポイントでの入力を受け取ります。よって、入力データが文法的にも意味的にも正しいことを確認する検証を実行する必要があります。また、入力データが文字列の長さや文字セットなどの規定されている制限や依存関係のあるコンポーネントに違反していないか検証が必要です。 ユーザーのすべての入力は、サーバー側でチェックします。	
	所見	**提案**
入力の検証	回答によれば、提供データからのすべての入力が検証されています。	ユーザー入力の整合性と適切な検証を維持するため、各アプリケーションで入力の精査を継続してください。 入力データの検証では、文法的および意味的に正しいデータは許容し、また、無効な文字のスクリーニングだけに頼ってはなりません。
	所見	**提案**
入力の検証	回答によれば、エンドユーザーのすべての入力が検証されています。	ユーザー入力の整合性と適切な検証を維持するため、各アプリケーションで入力の精査を継続してくだ

		さい。 入力データの検証では、文法的および意味的に正しいデータは許容し、また、無効な文字のスクリーニングだけに頼ってはなりません。
	所見	**提案**
入力の検証	回答によれば、クライアント アプリケーションからのすべての入力が検証されています。	ユーザー入力の整合性と適切な検証を維持するため、各アプリケーションで入力の精査を継続してください。 入力データの検証では、文法的および意味的に正しいデータは許容し、また、無効な文字のスクリーニングだけに頼ってはなりません。

データ ストレージと通信		
サブカテゴリ	**ベスト プラクティス**	
暗号化	機密データは、暗号化またはハッシュ化してデータベースまたはファイル システムに格納してください。アプリケーションでは、暗号化して一般開示に制限を要するデータ、鍵付きハッシュ値 (HMAC) を生成して単に改竄を防止したデータ、パスワードなど機能性自体の低下なしで非可逆変換 (ハッシュ) を適用したデータを区別しなければなりません。アプリケーションは、復号キーを暗号化されたデータとは別に格納しなければなりません。 機密データは、他のコンポーネントに送信する前に暗号化する必要があります。平文テキストを扱い、データを脅威にさらす中間コンポーネントが送信前または受信後の段階に存在しないことを確認してください。トランスポートのセキュリティ メカニズムが備える認証機能を利用してください。 広く認知されている高強度の暗号には、3DES、AES、RSA、Blowfish などがあります。最低でも 128 ビットのキー サイズを持つ暗号を使用してください (RSA は 1024 ビット)。	
	所見	**提案**
暗号化	回答によれば、現在のアプリケーションは、ストレージにおいても送信においてもデータの暗号化を行っていません。	機密データの処理を行うアプリケーションには、データの送信と格納の両方に、業界標準暗号アルゴリズムの採用を検討してください。

サブカテゴリ	**ベスト プラクティス**
暗号化 - アルゴリズム	最適なキーのサイズと要件に応じた最適な暗号化モードを備えた業界標準の暗号アルゴリズムをアプリケーションで採用してください。 業界で広く認知されている高強度の暗号には、3DES、AES、RSA、Blowfish などがあります。 最低でも 128 ビットのキー のサイズを持つ暗号を使用してください (RSA は 1024 ビット)。

運用

この分析領域では、多層防御を強化するために組織が従う業務上の施策、手順、およびガイドラインを評価します。このアセスメントでは、企業環境内でシステム構築、ネットワーク ドキュメンテーション、および技術の使用を既定するポリシーと手順を検証します。これには、管理者および業務スタッフが使用する情報および手順の管理に必要なサポート業務も含まれます。業務上の施策、手順、およびガイドラインを確立して理解し、それらに従うことによって、多層防御を強化できます。アセスメントでは、以下の業務上のセキュリティ領域に焦点を当て、企業の業務リスクの低減の支援を目的とした上位レベルの手順を検証します。

- E環境—システム構築、ネットワーク ドキュメンテーション、アプリケーション データ フロー、アプリケーション アーキテクチャ
- セキュリティ ポリシー—プロトコルとサービス、利用規定、ユーザー アカウント管理
- 修正プログラムと更新プログラムの管理—パッチ管理、ウイルス データ ファイル
- バックアップと復旧—バックアップ、保存、テスト

環境		
サブカテゴリ	ベスト プラクティス	
ファイアウォール規則とフィルタ	ファイアウォールは防衛の最前線の役割を持ち、すべてのネットワーク境界に配置しなければなりません。ファイアウォールに実装する規則は高度に限定的なものとし、ホストごと、およびサービスごとに設定しなければなりません。 ファイアウォールの規則やルーターの ALC (アクセス制御リスト) を作成する場合は、まず第一に、アクセス制御デバイスとネットワークを外部の攻撃から防御することに焦点を置きます。 + ネットワークの ALC とファイアウォールの規則を使用してデータフローを強化します。 + 現行の規則が DoS (サービス拒否) 攻撃に効果があるかを確認するため、ファイアウォールの規則とルーターの ALC の検証を行ってください。 + 体系的かつ正式なファイアウォール整備の一環として 1 つ以上の DMZ を導入してください。 + インターネットからアクセスできるサーバーはすべて DMZ 内に配置します。DMZ へのアクセスおよび DMZ からのアクセスは制限してください。	
	所見	提案
ファイアウォール規則とフィルタ	回答によれば、ファイアウォールを正しく機能させるためのテストを定期的に実施していません。	ファイアウォールの定期的なテストを実施してください。ファイアウォールが、外部トラフィックに対してだけでなく内部トラフィックに対しても正しく機能することを確認してください。

リソース

インターネット ファイアウォールに対するFAQ

このFAQは、ファイアウォールの導入について理解を深めたい、ITプロフェッショナルではないユーザーに適しています。

http://www.microsoft.com/japan/security/protect/firewall.asp

Deploying Firewalls: By Fithen,William, et al. Software Engineering Institute, Carnegie Mellon University, 1999.

この文書中にある実施事項は、システム、セキュリティおよびネットワーク管理者向けのものです。著者が提供しているのは、ファイアウォールを展開する全段階におけるシステムの設計から、必要な仕様に対してファイアウォールのシステムをテストするセキュリティ ポリシーを反映するための設定、そして最終的なロール アウトのための推奨策です。

http://www.cert.org/security-improvement/modules/m08.html

ネットワークをセキュリティ保護する

これはネットワーク管理者と IT 専門家向けに書かれたものです。ネットワーク レベルの最大の脅威とその対策方法について説明されています。 セキュリティ問題とルーター、ファイアウォール、そしてスイッチに適用する設定を検証しています。

http://www.microsoft.com/japan/msdn/security/guidance/secmod88.mspx

サブカテゴリ	ベスト プラクティス
管理者	管理アカウントについては、複雑なパスワードを必要とする制限の厳しいポリシーを適用してください。下記の条件を満たすものを複雑なパスワードと見なします。 + アルファベットと数字の混在 + 大文字と小文字の混在 + 少なくとも 1 つの特殊文字 + 14 文字以上 さらに、パスワード攻撃が行われた場合のリスクを低減するために、下記の制御を実装してください。 + 期限付きのパスワード + ログインに 7 ～ 10 回失敗した場合にアカウントをロックアウト + システムでのログ取得

	複雑なパスワードの実装に加えて、多元的な認証手段の実装を検討してください。アカウント管理 (アカウント共有不可) やアカウント アクセス ログに高度な制御を採用してください。

	所見	提案
管理者	回答によれば、環境内のシステムやデバイスでセキュアな管理を維持するための個別ログインを採用していません。	管理業務に別のアカウントを要求することを検討してください。また、管理者資格情報が頻繁に変更されることを確認してください。

	所見	提案
管理者	回答によれば、ネットワークに対する管理者アクセスをユーザーに与えています。	セキュアな構築の変更機能を制限するために、ユーザーの管理者アクセスの削除を検討してください。

サブカテゴリ	ベスト プラクティス
管理ホスト	管理パッケージを使用する場合は、管理コンソールがハードニングされ、物理的にもセキュアでなければなりません。 ネットワーク サービスとデバイスの管理に使用する管理ワークステーションをハードニングしてください。 SSH 接続または VPN 接続を使用して、平文テキスト プロトコルを保護してください。 管理ワークステーションは、特定のネットワークとホスト管理者の専用としてください。 SNMP を採用しているすべての管理システムについて、最新バージョンのセキュリティ更新プログラムが適用されていて、既定のコミュニティ文字列が使用されていないことを確認してください。 共有システムには、いかなる管理専用データも保存しないでください。共有ワークステーションを、ネットワーク デバイスやホストの管理に使用しないでください。

サブカテゴリ	ベスト プラクティス
管理ホスト - サーバー	

	所見	提案
管理ホスト - サーバー	回答によれば、サーバー管理専用のコンピュータが導入されています。	平文のテキスト プロトコルを安全なものにする SSH や VPN の使用を検討してください。

サブカテゴリ	ベスト プラクティス
管理ホスト - ネットワーク デバイス	

	所見	提案
管理ホスト - ネットワーク デバイス	回答によれば、ネットワーク管理専用のコンピュータは導入されていません。	ネットワーク デバイスをセキュアな管理プロトコルを介して管理する独立した管理用ホストの導入を検討してください。

サブカテゴリ	ベスト プラクティス
第三者との関係	企業がさらされるリスクを低減するため、第三者との関係を定めた正式な規定と手続きが必要です。規定と手続きによって、セキュリティの問題と各法人の責任分担が明らかとなります。 第三者との規定には、下記のような事項を定めてください。 + 接続とアクセスのレベル + データの提供と操作 + それぞれの法人の役割と責任 (権限を含む) + パートナシップの管理—立ち上げ、進行中、終了

	所見	提案
第三者との関係	回答によれば、あなたの会社は、社内でコンピュータ環境を管理しています。	ビジネス ニーズに基づいて、自社管理またはアウトソーシングのいずれかを実行可能な対策にすること

		ができます。管理をアウトソーシングする場合は、契約書、およびセキュリティ要件の順守を実施する際に使用する SLA (Service Level Agreement) でセキュリティ要件に対処してください。

セキュリティ ポリシー		
サブカテゴリ	ベスト プラクティス	
セキュアな構築		
	所見	提案
セキュアな構築	回答によれば、インフラストラクチャ デバイスの構築プロセスを文書化しています。	文書化された、インフラストラクチャ デバイスの構築プロセスを実装してください。また、新しい更新プログラムのリリース時にビルドが最新の状態に更新されていることを確認してください。
	所見	提案
セキュアな構築	回答によれば、サーバーの構築プロセスを文書化しています。	文書化された、サーバーの構築プロセスの使用を継続してください。また、新しい更新プログラムのリリース時にビルドが最新の状態に更新されていることを確認してください。
	所見	提案
セキュアな構築	回答によれば、ワークステーションおよびノート PC の構築プロセスを文書化しています。	文書化された、ワークステーションおよびノート PC の構築プロセスを実装してください。また、新しい更新プログラムのリリース時にビルドが最新の状態に更新されていることを確認してください。

リソース

Securing Public Web Servers

このコラムでは、一般向けの Web サイトの運営に関連する危険性を緩和する方法を説明しています。Web サーバー ソフトウェアおよび基礎となるホスト オペレーティング システムの構成、Web サーバーの完全性の保持などのトピックが取り扱われています。

http://www.cert.org/security-improvement/modules/m11.html

passfilt.dll

Passfilt.dll とは Microsoft® Windows NT® 4.0 オペレーティング システムの代替の .dll です。passfilt を使用して、オペレーティング システムの既定のパラメータを変更し、強力なパスワードのサポートおよび管理者のアカウント ロックアウト (ネットワーク レベルで) を提供することができます。

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/strong_password_enforcement_and_passfilt_dll.asp

The Twenty Most Critical Internet Security Vulnerabilities

このリストは、SANS (SysAdmin, 監査, ネットワーク, セキュリティ) インスティチュートおよび FBI の国家インフラ防護センター (NIIPC) によって編集されました。Microsoft® Windows® のオペレーティング システム で悪用されることの多い 10 のサービスと、Linux および Unix で最も一般的に悪用される 10 のサービスについて説明しています。ご使用の環境で悪用される可能性のある脆弱性の特定、そして推奨されている対策方法の確認にご使用ください。

http://www.sans.org/top20/#threats

NSA Security Recommendation Guides

このガイドは米国家安全保障局 (NSA) が提供しているネットワーク セキュリティの改善に関する技術的なアドバイスです。IP ルーター (特にシスコ システムズのルーターの詳細な取り扱い方法を掲載) 設定の原則とガイダンスが含まれています。この情報はアクセス管理、攻撃防御、ネットワーク コンポーネントのシールド、そしてネットワーク トラフィックの整合性と機密保持に対処するものです。

http://www.nsa.gov/snac/cisco/index.html

Microsoft Gold Certified Partners

セキュリティ ソリューションに関するマイクロソフト認定ゴールド パートナープログラムは、ユーザーのセキュリティ向上を支援する IT ソリューションの構築、展開を提供する専門企業を見つけることをお手伝いします。マイクロソフトは、パートナー企業にマイクロソフトの技術やソリューションに関して高いレベルの専門知識を取得してもらえるよう、密に連携をとっています。

http://directory.microsoft.com/resourcedirectory/Services.aspx

Windows Server 2003 セキュリティ ガイド

このガイドは、さまざまな環境に対応するセキュアなWindows Server 2003の構築方法を記載した、分かりやすいアドバイス、ツール、テンプレート集です。サーバーのインストールと構築に責任を負っているネットワーク管理者とITプロフェッショナルにとって有用な情報が書かれています。

http://www.microsoft.com/japan/technet/security/prodtech/win2003/w2003hg/sgch00.asp

Microsoft Baseline Security Analyzer (MBSA)

MBSAは、Windowsシステムをスキャンしてセキュリティ パッチの適用有無などを調べるアプリケーションで、ダウンロードによって入手可能です。スキャンするコンピュータのアカウント設定やパスワード強度を調べる簡単なツールも付属します。MBSAはWindows 2000、Windows XP、Windows Server 2003で動作します。

http://www.microsoft.com/japan/technet/security/tools/tools/mbsahome.asp

データベース サーバーをセキュリティ保護する

このガイドは、データベース設計者およびデータベース管理者を対象に書かれています。このガイドはデータベース サーバー (特に Microsoft® SQL Server™) をセキュアにするための効果的な手順を提供しています。このガイドはデータベース サーバーに影響を及ぼす最も一般的な脅威について検討し、セキュアな構成を適用するプロセスを紹介しています。

http://www.microsoft.com/japan/msdn/security/guidance/secmod91.mspx

UNIX & インターネットセキュリティ 第2版 Simson Garfinkel, Gene Spafford 著

この本はユーザーおよび管理者を対象としており、Unix ホストとネットワーク セキュリティに関する実用的な情報を掲載しています。Unix のセキュリティ対策の実施に関する問題、アプローチとその方法を取り上げています。

http://www.amazon.co.jp/exec/obidos/ASIN/4900900389/qid=1116995480/

サブカテゴリ	ベスト プラクティス	
プロトコルとサービス	社内ネットワークで利用が許されているプロトコルとサービスに関する標準や事例を明確に文書化してください。許可されているすべてのサービスが、そのアクセス権を持つ業務レベルの事業ニーズを確実に満たせるように、アクセス制御リストを検証する必要があります。特定の IP アドレスまたは範囲を可能な限り特定してください。サーバーで稼動させるサービスは事業上のニーズを満たすサービスのみに限定してください。指定のプロトコル バージョンおよび最低の暗号化の強度についても、このガイドラインに明記してください。境界デバイス (ルーター、ゲートウェイ、ファイアウォールなど) の使用、認証の強化、通信の暗号化など、社内認定済みのプロトコルの使用を推進してください。	
	所見	提案
プロトコルとサービス	回答によれば、内部ネットワークで利用が許されているプロトコルとサービスを規定したガイドラインが存在します。	利用が許されているプロトコルとサービスのドキュメントを監査し、各デバイスの設定済み ACL とファイアウォール規則がドキュメントに準拠しているかどうかを確認してください。 ドキュメントをイントラネットで公開し、併せて変更ポリシーを適用してください。

サブカテゴリ	ベスト プラクティス	
利用規定 (AUP)	企業内のネットワーク、アプリケーション、データ、およびシステムの利用を規定した利用規定 (AUP) が存在します。その利用規定では、デジタル メディア、印刷媒体、および、その他の知的財産権についても規定しています。	
	所見	**提案**
利用規定 (AUP)	回答によれば、内部ネットワークの利用規定 (AUP) が存在します。	会社のリソースを利用するすべての従業員と顧客は利用規定を熟知していなくてはなりません。イントラネットで利用規定を公開し、また、新入社員研修での紹介を検討してください。

サブカテゴリ	ベスト プラクティス	
ユーザー アカウント管理	IT リソースへのアクセスを必要とする全従業員に、個別のユーザー アカウントを作成してください。ユーザー間でアカウントを共有させてはなりません。デフォルトでは必要最低限の特権のみを付与します。ネットワーク管理者とサーバー管理者には、非特権アカウントと特権 (アドミニストレータ) アカウントの両方を発行してください。強いパスワードの利用を強制し定期的に監査するとともに、すべてのアカウントの変更をログに記録してください。従業員の職務の変更があった場合、必要に応じてアカウント特権の見直しと変更を行ってください。従業員が退職した場合、当人が利用していたすべてのアカウントを削除してください。	
	所見	**提案**
ユーザー アカウント管理	回答によれば、社員のアカウント管理に関するポリシーが存在します。	個人のユーザー アカウントはベスト プラクティス セクションで述べているポリシーのリストに従って管理することが重要です。 Windows 環境では Active Directory によるユーザー アカウント管理の導入と、アカウントに対してパスワードの強度のテストを定期的に行うことを検討してください。このような機能に対応したシェアウェア、ファイアウォール、サードパーティ製ツールなどを使用してください。 Windows 2000 を搭載したサーバーでは、Microsoft Operations Manager (MOM) に対応した監査手法と通知機能を開発し、アカウントの特権変更を追跡してください。
	所見	**提案**
ユーザー アカウント管理	回答によれば、ユーザー アカウントを共有していません。	
	所見	**提案**
ユーザー アカウント管理	回答によれば、管理者が特権アカウントと非特権アカウントの両方を持っています。	
	所見	**提案**
ユーザー アカウント管理	回答によれば、従業員が退社する際にアカウントが削除されません。	悪意のある元従業員から保護するために、すべてのアカウントを退職時に速やかに削除してください。
	所見	**提案**
ユーザー アカウント管理	回答によれば、パスワードの強度を強制していません。	ポリシーで最低限のパスワードの強度を定義する必要があります。パスワードの強度は認証機能によって強制されます。

サブカテゴリ	ベスト プラクティス	
セキュリティ要件	セキュリティに関するすべての打ち合わせと意思決定には、セキュリティの専門知識を持つ従業員を任命して従事させてください。資産の価値から保護を必要とするリソースを特定するとともに、保護に必要なセキュリティ レベルを見極めてください。すべての脅威の大きさと性質は分析を行うことで明らかになります。コストと保護によって得られる利益とのトレードオフを勘案してセキュリティ戦略を定め、場合によっては他者へのリスクの移転やテクノロジー導入によるリスクの発生と受諾を選択肢として取り入れます。事業的な観点と技術的な観点の両面から定められたセキュリティ要件は文書化し、精査と将来の設計への取り組みを目的としてすべての部門に公開します。各部門で扱うアプリケーションとデータの違いによって、正反対の要件が規定されることがあります。	
	所見	**提案**
セキュリティ要件	回答によれば、あなたの会社には、コンピュータ環	コンポーネントへの重要度レベルの割り当てを継続

	境の各コンポーネントに重要度レベルを割り当てるためのモデルがあります。	してください。また、新しい機器の追加時にはモデルを更新してください。

サブカテゴリ	ベスト プラクティス	
ガバナンス	第三者による監査を定期的に実施して、医療に関する HIPAA、SEC の規定に準拠した企業に対する Sarbanes-Oxley など、現在の法律上および民政上の要件を順守していることを確認してください。	
	所見	**提案**
ガバナンス	回答によれば、あなたの会社にはコンピュータ環境を規定するためのポリシーがあります。	適用可能な標準 (ISO17799、CoBIT、HIPAA、SOX など) に従って、コンピュータ環境の管理ポリシーの策定と実装を継続してください。

サブカテゴリ	ベスト プラクティス	
セキュリティ ポリシー	セキュリティ ポリシーは、企業経営幹部から権限を与えられた管理部門、IT 部門、および人事部門の情報提供をもとに定義し、CoBIT などの最新のベスト プラクティスを反映するように定期的に更新してください。	
	所見	**提案**
セキュリティ ポリシー	回答によれば、会社のセキュリティ関連の処理を規定する情報セキュリティ ポリシーがあります。	情報に関するセキュリティ ポリシーの使用を継続してください。ただし、技術および環境の現時点での変化に応じてポリシーを定期的に見直し、更新してください。
	所見	**提案**
セキュリティ ポリシー	回答によると、IT 部門のみでポリシーを策定しました。	ポリシーの策定は、法的要件、技術的要件、およびビジネス要件を考慮するために、IT 部門代表者と企業代表者の両者が行ってください。

リソース

Sample Security Policy Templates セキュリティ ポリシー サンプル テンプレート (JNSA)

これらのポリシー テンプレートのサンプルは商用団体などセキュリティの専門家グループにより作成されたものです。これらのテンプレートを使用し容易にお使いの環境にあったポリシーを展開することが可能です。

http://www.securityunit.com/docs/

Microsoft Operations Framework (MOF) ーチーム モデル ー

このホワイト ペーパーはIT部門が優れた効率とシナジーを生み出すためのガイダンスを提供します。このドキュメントは、組織構成とプロセス責任元に対するベスト プラクティスの概要として、ITマネージャおよび運用マネージャに向けて書かれています。

http://www.microsoft.com/japan/technet/itsolutions/tandp/opex/mofrl/mofeo.asp

運用に関するMicrosoft Operations Framework (MOF) プロセス モデル

このホワイト ペーパーは、企業内ITソリューションに対する信頼性、可用性、サポート性、管理性の実現に努めている企業向けに、MOFプロセスモデルの技術的な手引きを記載しています。このペーパーは、企業内で一貫したポリシ、手順、標準、ベストプラクティスの適用に責任を負っているITマネージャ向けです。

http://www.microsoft.com/japan/technet/itsolutions/tandp/opex/mofrl/mofpm.asp

修正プログラムと更新プログラムの管理	
サブカテゴリ	ベスト プラクティス
ネットワーク ドキュメンテーション	外部ネットワークと内部ネットワークの、最新かつ正確な物理的および論理的なダイアグラムを常に用意してください。

	環境内のすべての変更は、対応するダイアグラムに随時反映してください。 最新のダイアグラムへのアクセスは IT 部門に限定してください。	
	所見	提案
ネットワーク ドキュメンテーション	回答によれば、ネットワークの論理ダイアグラムは存在し、最新の状態に更新されています。	ネットワーク ダイアグラムを更新するポリシーを見直してください。 環境の変更管理ポリシーが存在するのであれば、ダイアグラムの変更作業を正式な手順として変更管理ポリシーに加えてください。 最新のダイアグラムは、主として、IT 部門かセキュリティ部門に所属する限定した担当者だけに参照を許可してください。

サブカテゴリ	ベスト プラクティス	
アプリケーション データ フロー	アプリケーションのアーキテクチャ ダイアグラムには、主要なコンポーネントとデータ フローを記載する必要があります。データフローには、システムがどのデータを通すか、データをどのように処理するかなどを含めた、環境内の主要データの流れを記載してください。 アプリケーション自体やアプリケーションの稼動環境に変更があった場合は、対応するダイアグラムを随時更新してください。	
	所見	提案
アプリケーション データ フロー	回答によれば、内部接続アプリケーションの正確なアーキテクチャ図とデータフロー図のみが存在します。外部アプリケーションはありません。	アプリケーション アーキテクチャ部門およびそれぞれのビジネス オーナーと連携して、外部接続アプリケーションの正確なアーキテクチャ図とデータ フロー図を作成してください。アプリケーションの優先順位を決める過程では、そのアプリケーションが処理するデータが重要かつ機密であるかどうかで判断し、その優先順位に従ってアーキテクチャ図とデータ フロー図を作成してください。環境やアプリケーション自体が変更された場合、適宜ダイアグラムを更新してください。

リソース

Web アプリケーション セキュリティ強化: 脅威とその対策

このガイドは、セキュアな Microsoft® ASP.NET Web アプリケーションの設計、構築および構成のための強固な基礎を提供します。アプリケーションを保持していている場合も、新しいアプリケーションを構築している場合も、ここで説明されている原理はハッキングに強い Web アプリケーションを構築するための手助けになります。

http://www.microsoft.com/japan/msdn/security/guidance/secmod71.mspx

The Open Web Application Security Project Guide (OWASP)

OWASP は情報および知識の共有により、Web アプリケーションおよび Web サービスを向上させることに専念しているオープンソース コミュニティです。OWASP の世界中のメンバーは Web アプリケーションのセキュリティに関連する情報および技術を交換しています。また、このサイトは商業的な品質を持つ無償のオープンソースのドキュメンテーションおよびソフトウェアも提供しています。IT 組織は OWASP を使用し、IT グループが求めている Web アプリケーションのセキュリティ レベルに見合うアプリケーション ベンダーを特定することも可能です。

http://www.owasp.org/documentation/guide/1.1/index

セキュアなASP.NETアプリケーションを構築する:認証、認可、セキュア通信

このガイドには、Windows 2000用および.NETフレームワークversion 1.0に対応する、セキュアなASP .NETアプリケーションの設計および構築方法がまとめられています。複数の.NETアプリケーションをわたったアプリケーション レベルでの認証と認可の通信メカニズム構築において、セキュリティを高める各機能の使用方法を説明しています。

http://www.microsoft.com/japan/msdn/net/security/secnetlpMSDN.asp

Writing secure code—プログラマのためのセキュリティ対策テクニック (上) (下) Michael Howard, David C. LeBlanc 著

本書はアプリケーション ソフトウェアの設計、構築、テストのためのセキュアなコーディング技術を概説しています。危険なアプリケーション プログラミング インターフェース (API) についての説明、セキュリティ チェックリストが付録として提供されています。本書では主に Microsoft® Windows® オペレーティング システムおよび C/C++ を取り扱っており、また Microsoft .NET Framework へのいくつかのリファレンスもあります。

http://www.amazon.co.jp/exec/obidos/ASIN/4891004460/qid=1116913493/

サブカテゴリ	ベスト プラクティス	
パッチ管理	セキュリティ更新プログラムと構成設定の変更は、有効になった時点で随時 (社内セキュリティ ポリシーで定義された時点で) 展開してください。セキュリティ更新プログラムの提供元が社内かサードパーティに関わらず、セキュリティ更新プログラムおよび更新プログラムは、本番系システムに適用する前に運用環境で完全なテストを行ってください。さらに、セキュリティ更新プログラム適用後に各システムのテストを行い、プログラムのロールバックを必要とするシステム固有の障害を検証してください。 システムをグルーピングに従って分類し、セキュリティ更新プログラムを適用するスケジュールを決めてください。重要なシステム、およびトラフィックが高いシステムから先にプログラムを適用します。	
	所見	**提案**
パッチ管理	回答によれば、オペレーティング システムとアプリケーションに対する修正プログラムおよび更新プログラムの管理を規定したポリシーが存在します。	現状の施策を継続するとともに、ベスト プラクティス セクションの情報を調べ、現在のポリシーを変更する必要があるかどうかを判断してください。 Windows を搭載したサーバーの管理と更新プログラム展開を自動化するために、SMS (System Management Server) と WSUS (Windows Server Update Services) の評価を検討してください。
	所見	**提案**
パッチ管理	回答によれば、修正プログラムや更新プログラムを全システムに適用する前にテストしています。	運用環境への導入前の、すべての修正プログラムと更新プログラムのテストを継続してください。
	所見	**提案**
パッチ管理		サーバーに自動パッチ管理を導入して、更新プログラムが適宜適用されるようにしてください。
	所見	**提案**
パッチ管理		ワークステーションおよびノート PC に自動パッチ管理を導入して、更新プログラムが適宜適用されるようにしてください。

リソース

セキュリティ パッチ管理に対するMicrosoftガイド

このガイドは企業内で複数台のWindowsコンピュータの管理に責任を負っているシステム管理者向けに書かれています。セキュリティ パッチ管理の方法と、推奨されるプロセス、ツール、導入手法について述べています。

http://www.microsoft.com/japan/technet/security/topics/patch/default.asp

サブカテゴリ	ベスト プラクティス
ウイルス データ ファイル	ウイルス対策の関連ベンダの Web サイトを定期的に監視し、更新プログラムがリリースされていたら、隔離したラボ環境にダウンロードしてテストを行ってください。更新プログラムが、その時点で導入しているオペレーティング システムやアプリケーションと不整合を起こさないか社内リリースの前に確認してください。 ウイルス対策ソフトウェアが備えている自動更新機能により、テスト前の更新プログラム ファイルが自動的に導入されてしまい、ファイル破壊を招くおそれがあるので、すべてのシステムでその機能を無効にしてください。 ウイルス対策ソフトウェアに対して、どのシステムが古いウイルス データ ファイルを使用し、どのシステム

	がウイルス チェックを無効にしているかを通知する、集中コンソールの導入を検討してください。 社内ネットワークに接続する頻度の低いリモート ユーザーには、自動更新機能の適用を検討してください。	
	所見	**提案**
ウイルス データ ファイル	回答によれば、ウイルス対策でウイルス データ ファイルを更新するポリシーが存在します。	関連ベンダやセキュリティ サイトを定期的に巡回し、最近の攻撃やウイルスの拡大に関する情報を収集してください。リモート ユーザーが定期的にシステムを更新しているかどうかを監査してください。 ベスト プラクティスに示されている施策を継続してください。

サブカテゴリ	**ベスト プラクティス**	
変更と構成の管理	本番系システムに対する変更は、導入する前に、セキュリティと互換性をテストしてください。また、すべての生産システムの構成について、完全に文書化して保管しておいてください。	
	所見	**提案**
変更と構成の管理	回答によると、あなたの会社には、変更および構成設定の管理プロセスがあります。	導入前にすべての更新プログラムのテストと文書化を行うときは、正式な変更と構成設定の管理プロセスの使用を継続してください。
	所見	**提案**
変更と構成の管理	回答によると、参照できるように構成設定が文書化されています。	システムのトラブルシューティングおよび復旧を容易に行うために、すべての構成設定の文書化を継続してください。
	所見	**提案**
変更と構成の管理	回答によると、構成の変更を運用コンピュータに展開する前にテストしています。	運用コンピュータへの導入前に、すべての構成の変更をテストするという現状の施策を継続してください。
	所見	**提案**
変更と構成の管理	回答によれば、構成設定の順守について、チェックと施行を集中管理しています。	順守のチェックおよび実施を集中管理システムから行うという現状の施策を継続してください。

バックアップと復旧		
サブカテゴリ	**ベスト プラクティス**	
ログ ファイル	ログ ファイルは、計画されたすべての行為を上書きしないで記録するように設定してください。自動プロセスは、ログ ファイルを日単位で交換して、それを管理ネットワーク内のセキュアなサーバーにオフロードするように設定してください。 ログ ファイルと構成設定が変更および削除されないように、アクセスを制限してください。 疑わしい動作または異常な動作を見つけるために、ログ ファイルを定期的に検査する必要があります。検査すべき事項は、システム操作、メンテナンス、セキュリティです。イベント関連付けソフトウェアと傾向分析を使用して、検査の確度を高めてください。	
	所見	**提案**
ログ ファイル	回答によれば、ログの取得が設定されていません。	まず最初に、DMZ に配置されたサーバーとデバイス、および重要な基幹ネットワークに配置されたサーバーに対して、ロギングを有効にしてください。 同様のシステムにも同一のロギング設定を行い、また、ログ ファイルの変更や削除が行われないようにアクセスを制限してください。 重要なログが生成された場合に通知が送付されるよう、Microsoft Operations Manager (MOM) の導入を検討してください。
	所見	**提案**
ログ ファイル	回答によれば、ログが、集中管理されているログ サーバーに書き込まれません。	運用サーバーで障害が発生した場合にデータを保持するために、集中管理ログ サーバーへのロギングを検討してください。

	所見	提案
ログ ファイル	回答によれば、ログ ファイルのローテーションは行われていません。	ログファイルは毎日ローテーションし、管理ネットワーク内のセキュアなサーバーにログ ファイルをオフロードするよう自動プロセスを設定してください。セキュリティ部門がログ ファイルの傾向分析を行えるように、また問題が発生ときに保護されたログにアクセスできるように、ログ ファイルをデータベースに保存することを検討してください。

	所見	提案
ログ ファイル	回答によれば、ログ ファイルへのアクセスは保護されていません。	DMZ 上と基幹ネットワーク上のサーバーで取得したオペレーティング システムのすべてのログ ファイルとアプリケーションのすべてのログ ファイルには、ファイル アクセスの制限を与えてください。

	所見	提案
ログ ファイル	回答によれば、ログ ファイルの定期的な確認は行われていません。	疑わしい動作または異常な動作を見つけるために、セキュリティ部門はログ ファイルを毎日検査しなければなりません。DMZ 上と基幹ネットワーク上のサーバーを MOM (Microsoft Operations Manager) によって監視し、ログを取得してください。重要なログが生成された場合、MOM は管理チーム内のメンバに通知を送信します。

サブカテゴリ	ベスト プラクティス	
バックアップ	フル バックアップは定期的に行ってください。可能であれば、フル バックアップとフル バックアップの間に差分バックアップを取ってください。バックアップ戦略は、システムとアプリケーションを完全に復元しなければならないワーストケースにも対処しなければなりません。重要なアプリケーションを最短時間で機能的に完全に復元しなければなりません。	
	所見	提案
バックアップ	回答によれば、社内環境にある重要なデータの定期的なバックアップが行われています。	バックアップ手順を監査して、重要なすべての資産が定期的にバックアップされているか確認してください。バックアップ メディアからの復元性を確認するために、定期的に復元機能のテストを行ってください。

サブカテゴリ	ベスト プラクティス	
バックアップ メディア	バックアップ メディアの保管と取扱いを規定する詳細なポリシーが必要です。ポリシーは、次の項目について言及する必要があります。 + 社内/社外での保管 + メディア ローテーション + セキュリティ制御 + アクセス対象者コントロール リムーバブル バックアップ メディアは施錠した耐火性キャビネットに保管し、認可を受けた担当者のみがキャビネットを開閉するように制限してください。 災害発生時の復旧性を高めるため、社外の保管場所を利用してください。	
	所見	提案
バックアップ メディア	回答によれば、バックアップ メディアの保管と取り扱いに関するポリシーが存在します。	バックアップ メディアの取り扱いと保管を規定したポリシーの策定は重要な第一歩であり、さらに、より良いものに完成させていくことが重要です。ベスト プラクティス セクションで述べているすべての基準を満たすよう、ポリシーを定期的に監査してください。

	所見	提案
バックアップ メディア	回答によれば、パックアップを社外に保管していません。	バックアップ メディアは社外にある施錠した耐火性キャビネットに保管してください。キャビネットへのアクセスは必要な担当者のみに制限してください。また、バックアップメディアは、製造元の指示に従って交換してください。

	所見	提案
バックアップ メディア	回答によれば、バックアップを耐火性の施錠キャビ	バックアップ メディアは社外にある施錠した耐火性

	ネットに保管していません。	キャビネットに保管してください。キャビネットへのアクセスは必要な担当者のみに制限してください。また、バックアップメディアは、製造元の指示に従って交換してください。
	所見	**提案**
バックアップ メディア	回答によれば、バックアップ メディアへのアクセスが制限されていません。	バックアップ メディアは社外にある施錠した耐火性キャビネットに保管してください。キャビネットへのアクセスは必要な担当者のみに制限してください。また、バックアップメディアは、製造元の指示に従って交換してください。
	所見	**提案**
バックアップ メディア	回答によれば、バックアップ メディアのローテーションと交換について、ポリシーで規定されていません。	バックアップ メディアは社外にある施錠した耐火性キャビネットに保管してください。キャビネットへのアクセスは必要な担当者のみに制限してください。また、バックアップメディアは、製造元の指示に従って交換してください。

サブカテゴリ	**ベスト プラクティス**	
バックアップと復元	バックアップと復元手順は、メディアの欠陥を特定し、機能停止後の復元の成功率を向上させるという意味から、定期的にテストを行ってください。 別のシステムに対するデータの復元については、アプリケーションの復元と合わせ、手順を詳細に適切に文書化しなければなりません。 バックアップと復元の手順を規定したすべてのドキュメントが、ビジネスの継続に必要なすべての重要なシステムを対象としていることを監査してください。	
	所見	**提案**
バックアップと復元	回答によれば、バックアップと復元手順の定期的なテストに関するポリシーは存在しますが、文書化されていません。	バックアップと復元のテスト手順は、まず初めに、ビジネスの継続に必要なクリティカルなシステムを対象として策定し、次に、すべてのシステムに拡張してください。バックアップと復元手順のテストを定期的に行い、ハードウェアおよびソフトウェアのすべてのコンポーネントが正しく機能するか確認してください。

リソース

Backup and Restore Solution

このリソースでは、Microsoft® Windows® 2000 Server 環境における設計、展開そしてシステムのバックアップと復旧方法が提供されています。

http://www.microsoft.com/technet/ittasks/maintain/backuprest/Default.asp

人的要素

企業におけるセキュリティ対策では、企業がセキュリティ全体を維持するために重要な組織面が見落とされがちです。アセスメントのこのセクションでは、企業のセキュリティ ポリシー、人事プロセス、および従業員のセキュリティ意識と教育を規定する企業内のプロセスについて検証します。また、人的要素の分析領域では、日常業務および職務の定義に関連するセキュリティの扱いにも焦点を当てます。アセスメントでは、以下の人的要素に関するセキュリティの領域に焦点を当て、企業の人的要素によるリスクの低減の支援を目的とした上位レベルの手順を検証します。

- 要件とアセスメント—計画、第三者による評価
- ポリシーと手順—人事管理規定、第三者との関係
- 教育と意識—セキュリティ意識

要件と評価	
サブカテゴリ	**ベスト プラクティス**

セキュリティ要件	セキュリティに関するすべての打ち合わせと意思決定には、セキュリティの専門知識を持つ従業員を任命して従事させてください。資産の価値から保護を必要とするリソースを特定するとともに、保護に必要なセキュリティ レベルを見極めてください。すべての脅威の大きさと性質は分析を行うことで明らかになります。コストと保護によって得られる利益とのトレードオフを勘案してセキュリティ戦略を定め、場合によっては他者へのリスクの移転やテクノロジー導入によるリスクの発生と受諾を選択肢として取り入れます。事業的な観点と技術的な観点の両面から定められたセキュリティ要件は文書化し、精査と将来の設計への取り組みを目的としてすべての部門に公開します。各部門で扱うアプリケーションとデータの違いによって、正反対の要件が規定されることがあります。	
	所見	**提案**
セキュリティ要件	回答によれば、セキュリティ部門と事業部門がセキュリティ要件定義に関与しています。	セキュリティ部門は、テクノロジの要件定義から、設計、展開に至るまで、すべての局面に参加してください。セキュリティ要件はわかりやすく規定し、機能仕様の一部として文書化してください。
	所見	**提案**
セキュリティ要件	回答によれば、セキュリティ部門は、テクノロジのライフサイクルの導入段階に関与していません。	セキュリティ部門は、すべてのプロジェクトについて、テクノロジのライフサイクルの全段階に関与する必要があります。
	所見	**提案**
セキュリティ要件	回答によれば、セキュリティ部門は、テクノロジのライフサイクルの計画および設計段階に関与しています。	
	所見	**提案**
セキュリティ要件	回答によれば、セキュリティ部門は、テクノロジのライフサイクルのテスト段階に関与していません。	セキュリティ部門は、すべてのプロジェクトについて、テクノロジのライフサイクルの全段階に関与する必要があります。
	所見	**提案**
セキュリティ要件	回答によれば、セキュリティ部門は、テクノロジのライフサイクルの実装段階に関与していません。	セキュリティ部門は、すべてのプロジェクトについて、テクノロジのライフサイクルの全段階に関与する必要があります。
	所見	**提案**
セキュリティ要件	回答によれば、情報セキュリティに関与する各担当者に役割と責任が割り当てられています。	

サブカテゴリ	**ベスト プラクティス**	
セキュリティ評価	第三者による評価は、セキュリティに対する自社の姿勢を客観的に見る上で重要です。 また、第三者による評価によって、顧客、パートナー、あるいはベンダ側のセキュリティ要件に自社が適合しているかどうかが分かり、法規への順守も証明されます。 評価では、インフラストラクチャ、アプリケーション、ポリシー、監査手順を対象とします。これら評価では、脆弱性の特定のみに焦点を当てるのではなく、セキュアではない構成設定や無関係なアクセス特権についても監査を行わなければなりません。セキュリティ ポリシーと手続きの精査を行い、実際の状況との差異を評価してください。	
	所見	**提案**
セキュリティ評価	回答によれば、第三者による独立したセキュリティ評価は行われていません。	重要なネットワークおよびアプリケーション インフラストラクチャから自己評価を開始してください。 重要なネットワークおよびアプリケーション インフラストラクチャに対し、第三者による評価を定期的に要求するような計画の策定を検討してください。 評価結果を改善プロジェクトに組み入れてください。
	所見	**提案**
セキュリティ評価		セキュリティ評価では、インフラストラクチャ、アプリケーション、ポリシー、監査を対象とします。
	所見	**提案**
セキュリティ評価		セキュリティ評価では、インフラストラクチャ、アプリケーション、ポリシー、監査を対象とします。
	所見	**提案**
セキュリティ評価		セキュリティ評価では、インフラストラクチャ、アプリ

		ケーション、ポリシー、監査を対象とします。
	所見	提案
セキュリティ評価		セキュリティ評価では、インフラストラクチャ、アプリケーション、ポリシー、監査を対象とします。
	所見	提案
セキュリティ評価	回答によれば、あなたの会社のセキュリティ評価を行っているのは、社内スタッフではありません。	社内スタッフがセキュリティ監査を頻繁に実施することを検討してください。ただし、これらの監査に信頼できるサード パーティからの意見を補足して、強化してください。
	所見	提案
セキュリティ評価		セキュリティ評価では、インフラストラクチャ、アプリケーション、ポリシー、監査を対象とします。
	所見	提案
セキュリティ評価		セキュリティ評価では、インフラストラクチャ、アプリケーション、ポリシー、監査を対象とします。
	所見	提案
セキュリティ評価		セキュリティ評価では、インフラストラクチャ、アプリケーション、ポリシー、監査を対象とします。
	所見	提案
セキュリティ評価		セキュリティ評価では、インフラストラクチャ、アプリケーション、ポリシー、監査を対象とします。

サブカテゴリ	ベスト プラクティス	
セキュリティ意識	セキュリティ意識研修を実施し、従業員に最新のセキュリティ状況を把握させることで、自社のセキュリティ方針への貢献が期待できるようになります。知識豊かな従業員はセキュリティ問題を報告してくれる良い情報源になるでしょう。 セキュリティ意識研修を効果的なものにするには、アプリケーション、ネットワーク、ハードウェアなど、あらゆる観点のセキュリティを対象にするとともに、それら構成要素がセキュリティの危険にさらされたと認識したときに取るべき行動について、従業員に明確なガイドラインを示す必要があります。 会社のリソースの利用を統制する規定を従業員に適用してください。 新入社員研修にセキュリティ意識研修を加えてください。また、上級コースや補習コースの研修を定期的に実施し、最新の事例とリスクに対してすべての従業員の意識を高めるよう施策を進めてください。 従業員の教材に対する理解度を確認するため、定期的に試験を実施してください。	
	所見	提案
セキュリティ意識	回答によれば、会社のセキュリティを担当する個人またはグループが存在します。	会社のセキュリティを担当する個人または部門を存続させてください。また、コンピュータ環境を変更する前に、この部門に問い合わせることを義務付けてください。
	所見	提案
セキュリティ意識	回答によれば、社内のセキュリティ部門が、新規テクノロジおよび導入済みテクノロジの要件定義に関与しています。	コンピュータ環境を変更する前に、セキュリティ部門に問い合わせることを継続してください。セキュリティ部門は、計画の初期段階のすべての打ち合わせに参加する必要があります。

リソース

Computer Security Incident Response (CSIRT)

このハンドブックでは、コンピュータ のセキュリティ インシデント レスポンス チーム (CSIRT) の発足と運営に関するガイダンスが提供されています。ここでは、極秘情報の取り扱い、運営および技術的な問題に対するほかの組織との連携について述べられています。CSIRT の設立は将来的なインシデントの予防に役立つだけでなく、迅速な対応能力を備えるための優れた方法です。

http://www.cert.org/archive/pdf/csirt-handbook.pdf

Building an Information Technology Security Awareness and Training Program

このドキュメントは米国連邦標準技術局により作成されました。IT ユーザーのためのセキュリティ啓発プログラムの整備に関するガイドをセキュリティ管理者に提供します。

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Steps for recovering from a UNIX or NT System compromise

この文書では、Unix および Microsoft® Windows NT® 4.0 システムでセキュリティが侵害された場合の対応方法が提案されています。ここで提供されている情報は、IT 環境のシステム管理者およびセキュリティの専門家向けのものです。

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

セキュリティ ガイダンス センター

このサイトでは、実践に役立つセキュリティのヒントや、HowTo 記事、最新のセキュリティ ガイダンスを提供しています。

http://www.microsoft.com/japan/security/guidance/default.mspx

ポリシーと手順		
サブカテゴリ	ベスト プラクティス	
経歴調査	経歴調査とは、潜在的な問題の特定を目的として実施されるもので、その結果として企業組織および他の従業員のリスク エクスポージャが低減されます。また、この調査によって、潜在的な問題の特定に加えて、候補者の履歴書との相違が明らかになります。 雇用手続きの過程で、候補者の職歴と犯罪歴を確認してください。 候補者のスキルについては、詳細に記述した職務内容 (ジョブディスクリプション) によって長所と短所を評価してください。	
	所見	提案
経歴調査	回答によれば、すべての従業員の経歴調査が行われます。	申し分ありません。この施策を継続してください。経歴調査には候補者の職歴、学歴、犯罪歴も対象となります。

サブカテゴリ	ベスト プラクティス	
人事管理規定	正式な退職規定によって、雇用契約終了時に必要なすべての手続きが行われることが保証されます。 自己都合と会社都合の両方の退職を取り扱えるように規定を定めてください。 退職規定には、下記のような事項を定めてください。 + 各部門への通知&—人事、IT、警備、ヘルプデスク、経理など + 従業員付き添いによる会社施設外への誘導 + すべてのアカウントとネットワークアクセスの停止 + 企業所有物の回収—ノート PC、PDA、電子メディア、機密書類など	
	所見	提案
人事管理規定	回答によれば、従業員の退職規定は正式には定められていません。	人事部門と連携して正式な退職規定を速やかに策定してください。 自己都合退職と会社都合退職を別々の規定として定めてください。 この規定において重要となる項目は、退職者のあらゆる物理的なアクセスおよび IT 権限を完全に遮断することです。
	所見	提案
人事管理規定	回答によれば、自己都合の退職規定は定められていません。	人事部門と連携して自己都合の退職規定を速やかに策定してください。
	所見	提案

人事管理規定	回答によれば、会社都合の退職規定は定められていません。	人事部門と連携して会社都合の退職規定を速やかに策定してください。

サブカテゴリ	ベスト プラクティス	
第三者との関係	企業がさらされるリスクを低減するため、第三者との関係を定めた正式な規定と手続きが必要です。規定と手続きによって、セキュリティの問題と各法人の責任分担が明らかとなります。 第三者との規定には、下記のような事項を定めてください。 + 接続とアクセスのレベル + データの提供と操作 + それぞれの法人の役割と責任 (権限を含む) + パートナシップの管理—立ち上げ、進行中、終了	
	所見	提案
第三者との関係	回答によれば、第三者との関係に関する正式な規定が定められています。	第三者との関係を定めた既存の規定と手続きを監査してください。ビジネスの発展に合わせて、規定が整合していること、および自社の立場が適正に表現されていることを確認してください。

研修と意識		
サブカテゴリ	ベスト プラクティス	
セキュリティ意識	セキュリティ意識研修を実施し、従業員に最新のセキュリティ状況を把握させることで、自社のセキュリティ方針への貢献が期待できるようになります。知識豊かな従業員はセキュリティ問題を報告してくれる良い情報源になるでしょう。 セキュリティ意識研修を効果的なものにするには、アプリケーション、ネットワーク、ハードウェアなど、あらゆる観点のセキュリティを対象にするとともに、それら構成要素がセキュリティの危険にさらされたと認識したときに取るべき行動について、従業員に明確なガイドラインを示す必要があります。 会社のリソースの利用を統制する規定を従業員に適用してください。 新入社員研修にセキュリティ意識研修を加えてください。また、上級コースや補習コースの研修を定期的に実施し、最新の事例とリスクに対してすべての従業員の意識を高めるよう施策を進めてください。 従業員の教材に対する理解度を確認するため、定期的に試験を実施してください。	
	所見	提案
セキュリティ意識	回答によれば、セキュリティ意識研修があります。	全従業員はセキュリティ意識研修に参加しなければなりません。セキュリティ意識研修を新入社員研修の必須項目としてください。 知識豊かな従業員はセキュリティ問題を報告してくれる良い情報源になるでしょう。
	所見	提案
セキュリティ意識	回答によれば、セキュリティ意識研修に参加しているのは従業員の 25% 未満です。	全従業員はセキュリティ意識研修に参加しなければなりません。セキュリティ意識研修を新入社員研修の必須項目としてください。 知識豊かな従業員はセキュリティ問題を報告してくれる良い情報源になるでしょう。
	所見	提案
セキュリティ意識	回答によれば、意識研修で、パーソナル ファイアウォールや暗号化の使用など、コンピュータ セキュリティについて取り上げていません。	セキュリティ意識研修では、セキュリティ ポリシーとセキュリティ制御、疑わしい動作の報告、電子メール セキュリティ、インターネット セキュリティ、コンピュータ セキュリティなど、セキュリティのすべての局面を対象とします。
	所見	提案
セキュリティ意識	回答によれば、意識研修で、Web の閲覧やダウンロードなど、インターネット セキュリティについて取り上げています。	
	所見	提案
セキュリティ意識	回答によれば、意識研修で、プライバシー問題につ	セキュリティ意識研修では、セキュリティ ポリシーと

	いて取り上げていません。	セキュリティ制御、疑わしい動作の報告、電子メール セキュリティ、インターネット セキュリティ、コンピュータ セキュリティなど、セキュリティのすべての局面を対象とします。
	所見	**提案**
セキュリティ意識	回答によれば、意識研修で、疑わしい動作の報告について取り上げていません。	セキュリティ意識研修では、セキュリティ ポリシーとセキュリティ制御、疑わしい動作の報告、電子メール セキュリティ、インターネット セキュリティ、コンピュータ セキュリティなど、セキュリティのすべての局面を対象とします。
	所見	**提案**
セキュリティ意識	回答によれば、意識研修で、会社のセキュリティ ポリシーとコントロールについて取り上げています。	
	所見	**提案**
セキュリティ意識	回答によれば、意識研修で、スパムと添付ファイルの管理方法など、電子メールのセキュリティについて取り上げています。	
	所見	**提案**
セキュリティ意識	回答によれば、研修は、2 年ごとまたはそれ以上経過してから実施しています。	全従業員に対してセキュリティ研修を 3 か月ごとに実施してください。
	所見	**提案**
セキュリティ意識	回答によれば、表題に関する研修が職務に応じた内容で従業員に対して行われています。	すべての従業員に自己に期待されている役割とその期待に応える方法を確実に理解してもらうには、職務に対応した研修と継続的な教育が欠かせません。社内のあらゆる職位の従業員に対して、職務ごとに必要となるセキュリティの研修を継続的に行ってください。
	所見	**提案**
セキュリティ意識	回答によれば、アプリケーションのセキュリティ研修は、組織における従業員の職務に基づいて実施されています。	
	所見	**提案**
セキュリティ意識	回答によれば、事故への準備と対応の研修は、組織における従業員の職務に基づいて実施されていません。	全従業員に対して、役割に応じた、表題に関する研修を行ってください。この研修は一般従業員に対する研修よりも詳細な内容にし、頻繁に内容を更新してください。
	所見	**提案**
セキュリティ意識	回答によれば、インフラストラクチャのセキュリティ研修は、組織における従業員の職務に基づいて実施されていません。	全従業員に対して、役割に応じた、表題に関する研修を行ってください。この研修は一般従業員に対する研修よりも詳細な内容にし、頻繁に内容を更新してください。
	所見	**提案**
セキュリティ意識	回答によれば、業務上のセキュリティ研修は、組織における従業員の職務に基づいて実施されていません。	全従業員に対して、役割に応じた、表題に関する研修を行ってください。この研修は一般従業員に対する研修よりも詳細な内容にし、頻繁に内容を更新してください。

リソース

Computer Security Incident Response (CSIRT)

このハンドブックでは、コンピュータ のセキュリティ インシデント レスポンス チーム (CSIRT) の発足と運営に関するガイダンスが提供されています。ここでは、極秘情報の取り扱い、運営および技術的な問題に対するほかの組織との連携について述べられています。CSIRT の設立は将来的なインシデントの予防に役立つだけでなく、迅速な対応能力を備えるための優れた方法です。

http://www.cert.org/archive/pdf/csirt-handbook.pdf

Building an Information Technology Security Awareness and Training Program

このドキュメントは米国連邦標準技術局により作成されました。IT ユーザーのためのセキュリティ啓発プログラムの整備

に関するガイドをセキュリティ管理者に提供します。

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Steps for recovering from a UNIX or NT System compromise

この文書では、Unix および Microsoft® Windows NT® 4.0 システムでセキュリティが侵害された場合の対応方法が提案されています。ここで提供されている情報は、IT 環境のシステム管理者およびセキュリティの専門家向けのものです。

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

セキュリティ ガイダンス センター

このサイトでは、実践に役立つセキュリティのヒントや、HowTo 記事、最新のセキュリティ ガイダンスを提供しています。

http://www.microsoft.com/japan/security/guidance/default.mspx

優先順位付きの対応リスト

以下のリストは、「アセスメントの詳細」セクションで前述した提案に優先順位を付けたものです。これらの各項目の詳細については、「アセスメントの詳細」セクションの該当する箇所を参照してください。

Microsoft セキュリティ パートナーがこれらの対応を網羅するセキュリティ プログラムの構築をお手伝いします。

推奨される対応リスト	
分析トピック	**提案**
高 (優先順位)	
領域: アプリケーション カテゴリ: データ ストレージと通信 サブカテゴリ: 暗号化 - アルゴリズム	
領域: 運用 カテゴリ: 環境 サブカテゴリ: 管理ホスト - ネットワーク デバイス	ネットワーク デバイスをセキュアな管理プロトコルを介して管理する独立した管理用ホストの導入を検討してください。
領域: 運用 カテゴリ: バックアップと復旧 サブカテゴリ: ログ ファイル	ログファイルは毎日ローテーションし、管理ネットワーク内のセキュアなサーバーにログファイルをオフロードするよう自動プロセスを設定してください。セキュリティ部門がログファイルの傾向分析を行えるように、また問題が発生ときに保護されたログにアクセスできるように、ログ ファイルをデータベースに保存することを検討してください。
領域: アプリケーション カテゴリ: データ ストレージと通信 サブカテゴリ: 暗号化	機密データの処理を行うアプリケーションには、データの送信と格納の両方に、業界標準暗号アルゴリズムの採用を検討してください。
領域: 人的要素 カテゴリ: 要件と評価 サブカテゴリ: セキュリティ評価	セキュリティ評価では、インフラストラクチャ、アプリケーション、ポリシー、監査を対象とします。
中 (優先順位)	
領域: 運用 カテゴリ: 修正プログラムと更新プログラムの管理 サブカテゴリ: ウイルス データ ファイル	関連ベンダやセキュリティ サイトを定期的に巡回し、最近の攻撃やウイルスの拡大に関する情報を収集してください。リモート ユーザーが定期的にシステムを更新しているかどうかを監査してください。 ベスト プラクティスに示されている施策を継続してください。
領域: 運用 カテゴリ: セキュリティ ポリシー サブカテゴリ: プロトコルとサービス	利用が許されているプロトコルとサービスのドキュメントを監査し、各デバイスの設定済み ACL とファイアウォール規則がドキュメントに準拠しているかどうかを確認してください。 ドキュメントをイントラネットで公開し、併せて変更ポリシーを適用してください。
領域: 運用 カテゴリ: 修正プログラムと更新プログラムの管理 サブカテゴリ: アプリケーション データ フロー	詳細： このガイドは、セキュアな Microsoft® ASP.NET Web アプリケーションの設計、構築および構成のための強固な基礎を提供します。アプリケーションを保持していている場合も、新しいアプリケーションを構築している場合も、ここで説明されている原理はハッキングに強い Web アプリケーションを構築するための手助けになります。 http://www.microsoft.com/japan/msdn/security/guidance/secmod71.mspx

	OWASP は情報および知識の共有により、Web アプリケーションおよび Web サービスを向上させることに専念しているオープンソース コミュニティです。OWASP の世界中のメンバーは Web アプリケーションのセキュリティに関連する情報および技術を交換しています。また、このサイトは商業的な品質を持つ無償のオープンソースのドキュメンテーションおよびソフトウェアも提供しています。IT 組織は OWASP を使用し、IT グループが求めている Web アプリケーションのセキュリティ レベルに見合うアプリケーション ベンダーを特定することも可能です。 http://www.owasp.org/documentation/guide/1.1/index このガイドには、Windows 2000用および.NETフレームワークversion 1.0に対応する、セキュアなASP .NETアプリケーションの設計および構築方法がまとめられています。複数の.NETアプリケーションをわたったアプリケーション レベルでの認証と認可の通信メカニズム構築において、セキュリティを高める各機能の使用方法を説明しています。 http://www.microsoft.com/japan/msdn/net/security/secnetlpMSDN.asp 本書はアプリケーション ソフトウェアの設計、構築、テストのためのセキュアなコーディング技術を概説しています。危険なアプリケーション プログラミング インターフェース (API) についての説明、セキュリティ チェックリストが付録として提供されています。本書では主に Microsoft® Windows® オペレーティング システムおよび C/C++ を取り扱っており、また Microsoft .NET Framework へのいくつかのリファレンスもあります。 http://www.amazon.co.jp/exec/obidos/ASIN/4891004460/qid=1116913493/
領域: 運用 カテゴリ: セキュリティ ポリシー サブカテゴリ: ユーザー アカウント管理	
領域: 運用 カテゴリ: セキュリティ ポリシー サブカテゴリ: セキュリティ ポリシー	ポリシーの策定は、法的要件、技術的要件、およびビジネス要件を考慮するために、IT 部門代表者と企業代表者の両者が行ってください。 詳細： これらのポリシー テンプレートのサンプルは商用団体などセキュリティの専門家グループにより作成されたものです。これらのテンプレートを使用し容易にお使いの環境にあったポリシーを展開することが可能です。 http://www.securityunit.com/docs/ このホワイト ペーパーはIT部門が優れた効率とシナジーを生み出すためのガイダンスを提供します。このドキュメントは、組織構成とプロセス責任元に対するベスト プラクティスの概要として、ITマネージャおよび運用マネージャに向けて書かれています。 http://www.microsoft.com/japan/technet/itsolutions/tandp/opex/mofrl/mofeo.asp このホワイト ペーパーは、企業内ITソリューションに対する信頼性、可用性、サポート性、管理性の実現に努めている企業向けに、MOFプロセスモデルの技術的な手引きを記載しています。このペーパーは、企業内で一貫したポリシ、手順、標準、ベストプラクティスの適用に責任を負っているITマネージャ向けです。 http://www.microsoft.com/japan/technet/itsolutions/tandp/opex/mofrl/mofpm.asp
低 (優先順位)	
領域: インフラストラクチャ カテゴリ: 防衛線内での防御 サブカテゴリ: ファイアウォール規則とフィルタ	詳細： このFAQは、ファイアウォールの導入について理解を深めたい、ITプロフェッショナルではないユーザーに適しています。 http://www.microsoft.com/japan/security/protect/firewall.asp この文書中にある実施事項は、システム、セキュリティおよびネットワーク管理者向けのものです。著者が提供しているのは、ファイアウォールを展開する全段階におけるシステムの設計から、必要な仕様に対してファイアウォールのシステムをテストするセキュリティ ポリシーを反映するための設定、そして最終的なロール アウトのための推奨策です。 http://www.cert.org/security-improvement/modules/m08.html これはネットワーク管理者と IT 専門家向けに書かれたものです。ネットワーク レベルの最大の脅威とその対策方法について説明されています。 セキュリティ問題とルーター、ファイアウォール、そしてスイッチに適用する設定を検証しています。 http://www.microsoft.com/japan/msdn/security/guidance/secmod88.mspx

領域: 運用 カテゴリ: バックアップと復旧 サブカテゴリ: バックアップ	バックアップ手順を監査して、重要なすべての資産が定期的にバックアップされているか確認してください。バックアップ メディアからの復元性を確認するために、定期的に復元機能のテストを行ってください。
領域: 運用 カテゴリ: 修正プログラムと更新プログラムの管理 サブカテゴリ: 変更と構成の管理	導入前にすべての更新プログラムのテストと文書化を行うときは、正式な変更と構成設定の管理プロセスの使用を継続してください。
領域: 運用 カテゴリ: セキュリティ ポリシー サブカテゴリ: 利用規定 (AUP)	会社のリソースを利用するすべての従業員と顧客は利用規定を熟知していなくてはなりません。イントラネットで利用規定を公開し、また、新入社員研修での紹介を検討してください。
領域: インフラストラクチャ カテゴリ: 管理とモニタリング サブカテゴリ: 構築	各ワークステーションに対するセキュアなシステム構築手順を作成してください。最新のサービス パック、ホット フィックス、その他のハードニング テクニックを使用して、構築方法を定期的に更新してください。

付録

質問と回答

このアセスメントに対して以下の回答が入力されました。

アセスメントの質問	回答
ビジネス リスク プロファイル	
企業内で使用しているデスクトップ PC とノート PC の台数:	50 ～ 149 台
企業内で使用しているサーバーの台数:	1 ～ 5 台
インターネットに常時接続していますか?	はい
顧客やベンダは、インターネット経由で社内ネットワークや内部システムにアクセスできますか?	不明
外部顧客やパートナー向けに、ポータルや Web サイトのようなアプリケーション サーバーを社内に構築しサービスを提供していますか?	はい
社外と社内両方のクライアントが同一のネットワーク セグメントで使用するサービスを導入していますか?	いいえ
外部パートナーまたは顧客に、データアクセス、記録の更新、またはその他の情報操作を目的として、社内バックエンド システムへの直接接続を許可していますか?	いいえ
社外向けサービスと社内向け業務サービスに、データベース アプリケーションなど、同一のバックエンド インフラストラクチャ構成要素を導入していますか?	いいえ
従業員または契約社員に社内ネットワークへのリモート アクセスを許可していますか?	はい
個人的な Web サーバーや長い間温めているプロジェクトを格納しているコンピュータなど本番系以外のシステムを、汎用の社内ネットワークに接続することを従業員に許可していますか?	はい
データ処理を目的として、バックアップ テープやメディアのほかに、社外への機密データや社外秘データの持ち出しを許していますか?	いいえ
社内でシステム セキュリティの問題が発生すると事業の推進に大きな影響が及びますか?	いいえ
事務所スペースを他社と共有していますか?	いいえ
アプリケーションを開発していますか?	はい
ソフトウェア開発者に、企業の開発リソースへのリモート アクセスまたはアプリケーション コードのリモートでの開発を許していますか?	いいえ
顧客、パートナー、または一般市場向けに、ソフトウェア製品の開発と販売を行っていますか?	はい
開発者に、リモート アクセスによって、または分離保護していないマシン上で、システム開発またはテストを行うことを許可していますか?	はい
社内の IT 担当者は (開発者とは別に) 基幹業務 (LOB) アプリケーションを管理していますか?	はい
サードパーティによって保存、処理、または配布されたデータを業務上必要としていますか?	はい
顧客データの保存と処理を行う環境を社内用リソースと共有していますか?	はい
提供するビジネス サービスを外部のソフトウェア開発パートナーに委託していますか?	はい
データ処理またはデータ マイニングを必要とするサービスから利益を得ていますか?	いいえ
あなたの会社が提供するアプリケーションサービスを利用してデータ処理を行っている顧客にとって、そのサービスは顧客の事業推進にクリティカルですか?	はい
クリティカルな業務アプリケーションをインターネットを通じて利用できるようにしていますか?	いいえ
自社環境の重要なアプリケーションの対象ユーザーは誰ですか?	内部従業員
重要なアプリケーションに対して、ユーザーにどのようなアクセス方法を許可していますか?	内部ネットワークからのアクセスのみ
社内ネットワークは、プライベートまたはパブリックを問わずネットワーク リンクを介して、顧客、パートナー、またはサードパーティのネットワークに接続していますか?	いいえ
メディア ファイルやドキュメンテーションなどのデータの保管または電子的な配布によるサービスから収益を得ていますか?	いいえ
ここ半年以内に主要な技術コンポーネントの一部を「丸ごと交換」しましたか?	いいえ
パートナー、ベンダ、その他のサードパーティから得る提供データや処理データに依存していますか?	はい
サイトの停電、あるいはハードウェアやアプリケーションの障害などによって、顧客が利用しているアプリケーションやインフラストラクチャに問題が生じた場合、自社の収入に影響が及びますか?	いいえ
取扱いに注意を要する重要な顧客のデータを保管していますか?	はい

顧客が持つインフラストラクチャ コンポーネントまたはアプリケーションは、あなたの会社が持つリソースへのアクセスに依存していると思われますか?	いいえ
自社のインフラストラクチャやアプリケーション コンポーネントを複数の顧客と共有していますか?	いいえ
情報技術 (IT) を会社の必要条件と考えていますか?	はい
全従業員が業務にコンピュータを使用していますか?	はい
インフラストラクチャの全部または一部の保守または所有を外部に委託していますか?	はい
新しい技術コンポーネントに関して、中期または長期にわたる選定と導入の計画を策定していますか。	不明
あなたの会社は新しい技術をいち早く採用する傾向がありますか?	はい
新しい技術の選定と導入を、現時点でのベンダとのパートナシップやライセンス契約に基づいて行っていますか?	はい
技術の選定は、現在の IT 部門の担当者が持つ技術的な知見に制限されていますか?	いいえ
新しい企業や他社の既存の環境の買収によってネットワークを拡張していますか?	いいえ
従業員に、取扱いに注意を要する顧客情報や自社のデータをワークステーションにダウンロードすることを許可していますか?	はい
ユーザーによる情報へのアクセスを職務に基づいて制限していますか?	はい
発生の可能性があるセキュリティ問題に対する新しいサービスやアプリケーションを評価せずに導入していますか?	いいえ
特権アカウントの資格情報を定期的に変更していますか?	いいえ
アクセス特権を持つ従業員の退職後に特権アカウントの資格情報を変更していますか?	はい
最もあてはまる業種を選択してください:	IT サービス
従業員数を選択してください:	501 人以上
会社の所在地は複数ありますか?	はい
厳しい競争にさらされている業界または研究開発を主体とする業界にあって、知的財産の盗難や産業スパイに多大な憂慮を抱いていますか?	はい
自社の技術部門担当者には高い離職率が見られますか、または人員削減が行われていますか?	いいえ
自社の製品またはブランドの知名度は高いと思いますか?	はい
下位のバージョンや古いソフトウェア (ベンダによって現在サポートされていないソフトウェア) を使用していますか?	はい
ソフトウェアを信頼できるベンダやソースから入手していますか?	はい
インフラストラクチャ	
企業リソースを保護するために、ファイアウォールやその他のネットワーク レベルでのアクセス制御をネットワーク境界上に適用していますか?	はい
それぞれの事務所所在地でそうしたアクセス制御を適用していますか?	はい
ホストベースのファイアウォール ソフトウェアを使用して、サーバーを保護していますか?	はい
企業環境にウイルス対策を実装していますか?	はい
ウイルス対策を導入しているシステムを選択してください:	境界ホスト (ゲートウェイ、プロキシ、中継など)
ウイルス対策を導入しているシステムを選択してください:	電子メール サーバー
ウイルス対策を導入しているシステムを選択してください:	デスクトップ
ウイルス対策を導入しているシステムを選択してください:	サーバー
社内ネットワークへのリモート アクセスは可能ですか?	はい
多元的な認証方法 (トークン、スマート カードなど) をリモート ユーザーに採用していますか?	いいえ
会社のリソースに対するリモート ユーザーからの接続に、セキュリティを維持するために、仮想プライベート ネットワーク (VPN) を採用していますか?	はい
クライアントが必要なすべてのセキュリティ チェックに合格するまで、VPN によって検疫ネットワークへの接続を制限できますか?	不明
ネットワークに複数のセグメントが存在していますか?	はい
外部顧客のアクセスやエクストラネット サービスを会社のリソースと分離するために、ネットワーク セグメントを使用していますか?	いいえ
ネットワークへのリモート アクセスが可能なユーザーを選択してください:	従業員
ネットワークへのリモート アクセスが可能なユーザーを選択してください:	契約社員

侵入検知ハードウェアまたはソフトウェアを使用して、攻撃を特定していますか?	いいえ
ネットワークへのワイヤレス接続は可能ですか?	いいえ
デバイスやホストの管理を行うために管理者アクセスに適用している認証オプションを挙げてください:	簡単なパスワード
内部ネットワークや社内ホストにアクセスするために、内部ユーザーに適用している認証オプションを挙げてください:	簡単なパスワード
リモートユーザーに適用している認証オプションを挙げてください:	簡単なパスワード
パスワード ポリシーの強制にあたって、アカウントの種類別に統制を行っていますか?	はい
ログイン失敗が一定の回数繰り返された後でアカウントへのアクセスを遮断するために、アカウント ロックアウトを有効にしていますか?	いいえ
パスワード ポリシーを強制しているアカウントを選択してください:	管理者
パスワード ポリシーを強制しているアカウントを選択してください:	ユーザー
インストールイメージや正式に文書化された構成設定に基づいて構築されているものを以下から選択してください。	ワークステーションとノート PC
インストールイメージや正式に文書化された構成設定に基づいて構築されているものを以下から選択してください。	サーバー
構成設定にはハードニング対策が含まれていますか?	いいえ
従業員のワークステーションおよびノート PC にインストールしている対策を選択してください。	パーソナル ファイアウォール ソフトウェア
社内システムの構成は、自社とハードウェア供給業者/再販業者のどちらが行っていますか?	社内スタッフによる設定
会社の資産を保護するために、物理セキュリティ コントロールを導入していますか?	いいえ
アプリケーション	
基幹業務 (LOB) アプリケーションを使用していますか?	はい
企業内環境に導入している重要アプリケーションはサードパーティが開発したものですか?	いいえ
Office アプリケーション (Word、Excel、Access など) にカスタム マクロを使用していますか?	はい
企業内環境に導入している重要アプリケーションは社内の開発部門が開発したものですか?	はい
社内開発部門は、ソフトウェア アップデート、セキュリティ更新プログラム、およびセキュリティ メカニズムに関するドキュメントを定期的に提供していますか?	いいえ
社内環境で現在使用しているアプリケーションのいずれかは、セキュリティに関して既知の脆弱性を持っていますか?	はい
そのセキュリティ上の脆弱性に対応する手順は決められていますか?	いいえ
重要アプリケーションに使用されている最も一般的な認証方法を下記のリストから選択してください。	簡単なパスワード
重要アプリケーションにパスワード ポリシーの適用を強制していますか?	はい
重要アプリケーションに適用しているパスワード制御を選択してください:	パスワードの有効期限
社内環境で使用している重要アプリケーションは、機密データや機能へのアクセスを制限するメカニズムを持っていますか。	はい
社内環境で使用している重要アプリケーションは、分析と監査目的のために、メッセージをログファイルとして記録する機能を持っていますか?	はい
ログを取得しているイベントを選択してください:	アプリケーション エラー
導入しているアプリケーションは、入力データをチェックする機能を持っていますか?	はい
アプリケーションの検証機能が適用される入力データを下記のリストから選択してください。	データ提供
アプリケーションの検証機能が適用される入力データを下記のリストから選択してください。	エンド ユーザー
アプリケーションの検証機能が適用される入力データを下記のリストから選択してください。	クライアント アプリケーション
重要アプリケーションは取扱いに注意を要する重要なデータを処理する時に暗号化を行っていますか?	いいえ
運用	
ファイアウォールのテストを定期的に行って、正しく機能するか確認していますか?	いいえ
通常業務と 管理業務で使用するログイン アカウントを区別していますか?	いいえ
ユーザーに自分が使用するワークステーションおよびノート PC に対する管理者アクセスを付与していますか?	はい
システムやデバイスにセキュアな管理を維持するために、専用管理ホストを使用していますか。	はい
現在使用している専用管理ホストを選択してください:	サーバー
環境の管理は、自社と外部委託のどちらで行っていますか?	会社が環境を管理します。

ホストの構築手順は文書化されていますか? 文書化されている場合は、その種類 (構築手順が文書化されているホストの種類) を挙げてください。	サーバー
社内ネットワークで利用が許されているプロトコルとサービスを規定したガイドラインは文書化されていますか? 該当するオプションを選択してください。	ガイドラインは存在し、文書化されています。
社内ネットワークの利用規定 (AUP) はありますか?	はい
社員のアカウント管理に関するポリシーはありますか?	はい
社員のアカウント管理に適用しているポリシーを以下から選択してください:	個人別のユーザー アカウント (アカウントは共有していない)
社員のアカウント管理に適用しているポリシーを以下から選択してください:	管理者に対する特権アカウントと非特権アカウント
コンピューティング環境の各構成要素に重大度レベルを割り当てる際のモデルはありますか?	はい
コンピューティング環境を規定するポリシーはありますか?	はい
組織のセキュリティ関連の活動を規定する、情報に関するセキュリティ ポリシーはありますか?	はい
そのポリシーの策定者を選択してください:	IT 部門のみ
ネットワーク インフラストラクチャおよびホストの正確な論理ダイアグラムや構成の関係書類は文書化されていますか?	はい
重要アプリケーションの正確なアーキテクチャ ダイアグラムとデータフロー ダイアグラムはありますか?	はい
ダイアグラムが存在するアプリケーションはどれですか:	内部接続アプリケーションのみ
セキュリティ更新プログラムと更新プログラムのポリシーおよび手順は確立されていますか?	はい
それらが存在する構成要素を選択してください:	オペレーティング システムとアプリケーションの両方
セキュリティ更新プログラムと更新プログラムのテストを導入前に行っていますか?	はい
セキュリティ更新プログラムの導入および管理に使用するものを挙げてください:	Windows Server Update Services (WSUS)
ウイルス データ ファイル ベースの検出製品を更新するポリシーは確立されていますか?	ウイルス対策
変更と構成の管理手順はありますか?	はい
構成は参照用に文書化されていますか?	はい
構成の変更のテストを運用コンピュータへの導入前に行っていますか?	はい
構成の順守は (例えば、Active Directory のグループ ポリシーを使用して) 一元的にチェックされ強制されていますか?	はい
ホストとデバイスのイベントを記録するようログを設定していますか?	いいえ
重要なデータや機密データを定期的にバックアップしていますか?	はい
バックアップ メディアの保管と取扱いに関するポリシーと手順は策定されていますか?	はい
バックアップと復元手順の定期的なテストに関するポリシーはありますか? そのポリシーは文書化されていますか。	はい、ただし文書化されていません。
人的要素	
この個人またはグループはセキュリティの専門知識を有していますか?	はい
テクノロジーのライフサイクルにおいて、このセキュリティ部門または担当者が関与するのはどの段階ですか?	計画と設計
役割と責任は、情報セキュリティに関与する個人ごとに定義されていますか?	はい
第三者に社内環境のセキュリティ評価を依頼していますか?	いいえ
社内環境のセキュリティ評価を社内で行っていますか?	いいえ
セキュリティを担当する個人またはグループが社内に存在していますか?	はい
この個人またはグループは、新しい技術および既存の技術のセキュリティ要件定義に関与していますか?	はい
雇用手続きの一環として経歴調査を行いますか?	はい
最も該当する項目を選択してください:	すべての候補者に対して経歴調査を行います。
従業員の退職規定はありますか?	いいえ
第三者との関係に関する正式な規定はありますか?	はい
セキュリティ意識研修はありますか?	はい
セキュリティ意識研修に参加する従業員の割合はどのくらいですか?	25% 未満

意識研修で取り上げるトピックを選択してください。	Web の閲覧やダウンロードを含む、インターネット セキュリティ
意識研修で取り上げるトピックを選択してください。	会社のセキュリティ ポリシーとコントロール
意識研修で取り上げるトピックを選択してください。	スパムや添付ファイルの処理を含む、電子メール セキュリティ
研修はどのくらいの頻度で実施されますか?	2 年ごとまたはそれ以上
組織の職務にもとづいて従業員にセキュリティに関する研修を行っていますか?	はい
下記から該当するものすべてを選択してください:	業務上のセキュリティ

用語集

用語集では、このレポートに含まれている標準的なセキュリティ業界用語および概念を取り上げています。このレポートに含まれていない用語も記載されています。

用語	定義
アプリケーション	エンド ユーザーに機能を提供するソフトウェア プログラム。実行するには、オペレーティング システムが必要です。たとえば、ワープロ、スプレッドシート、データベースなどのプログラムがあります。
ウイルス対策 (AV)	コンピュータ環境を有害なソフトウェアから保護するソフトウェアおよびハードウェア技術。
ビジネス リスク プロファイル (BRP)	組織がさらされているリスクを、ビジネス環境および企業活動を行う業界に基づいて測定したもの。
多層防御のインデックス (DiDI)	ビジネスについて特定されたリスクを低減するために、人的要素、プロセス、技術にわたって使用されているセキュリティ防御を測定したもの。
非武装地帯 (DMZ)	ファイアウォールによって内部ネットワークから分離され、別のファイアウォールを介してインターネットに接続されている、ネットワークの一部。
ファイアウォール	ネットワーク経由の不正アクセスからホストを保護するハードウェアまたはソフトウェア デバイス。
多元的な認証	ユーザーが知っている情報、ユーザーが持っているもの、ユーザー自身の一部のうち 2 種類以上の併用を必要とする認証。たとえば、銀行のデビット カードは、ユーザーが持っているもの (カード自体) とユーザーが知っている情報 (PIN 番号) の 2 つの要素を必要とする認証です。複数のパスワードの入力をユーザーに要求する認証は、「ユーザーが知っている情報」だけなので、1 要素の認証にすぎません。一般に、要素が多いほどよりセキュアな認証になります。したがって、ID カード (ユーザーが持っているもの)、PIN (ユーザーが知っている情報)、および指紋スキャナ (ユーザー自身の一部) を要求するシステムは、ユーザー名/パスワード (1 要素) のみまたは ID カードと PIN を要求するシステムよりもセキュアです。
運用	組織の保護および維持に関連するポリシー、プロセス、手順、および施策。
人的要素	組織のメンバ。さらに、組織のメンバと組織の保護に関連するポリシー、プロセス、手順、施策。
公開鍵基盤 (PKI)	公開鍵暗号および電子署名に必要な技術一式を統合したもの。公開鍵と秘密鍵を組み合わせた暗号化を使用して、鍵の管理、データの完全性、およびデータの機密性を提供します。
プロセス	職務の遂行に使用する、文書化された一連の作業手順。
セキュリティの成熟度	セキュリティの成熟度では、制御 (物理的なものおよび技術的なもの)、IT リソースに対する技術的な洞察力、ポリシー、プロセス、維持可能な施策などが考慮されます。利用可能なあらゆるツールを効果的に使用して、いかなる制限にも対応できるセキュリティ レベルを作成できるかどうかが、組織のセキュリティの成熟度の判断基準となります。セキュリティの成熟度のベースラインを確立し、それを使用して組織のセキュリティ プログラムで重点を置くべき領域を定義する必要があります。すべての組織のセキュリティ レベルを最適レベルにする必要はありませんが、現在直面しているビジネス リスクを考慮し、現状を把握して目標を設定する必要があります。例えば、セキュリティ リスクが低い IT 環境を持つ企業では、ベースライン レベルの上限または標準レベルの下限を変更してセキュリティの強化を図る必要はないかもしれません。一方、セキュリティ リスクが高い IT 環境を持つ企業は、最適レベルのセキュリティを導入しようとするでしょう。セキュリティ リスクの評価には、ビジネス リスク プロファイルの点数を参考にします。

グラフの解釈

BRP 対 DiDI

- BRP の点数は 0 ～ 100 点で、点数が高いほどその AoA に大きなビジネスリスクが潜在していることを示しています。ビジネスにはある程度のリスクが必ずついて回るため、この採点が 0 点になることはありません。また、直接的なリスク低減戦略を持ち得ないビジネスが存在することも理解してください。
- DiDI の点数も 0 ～ 100 点です。点数が高いほど、DiD 戦略によって、その AoA に多大なセキュリティ対策がとられていることを示します。DiDI の点数は環境の防御に使用されている全体的な戦略を反映したものであって、環境全体のセキュリティの有効性やセキュリティ維持に費やしたリソースを反映したものではありません。
- 直感的には、BPR の点数が低くて DiDI が高いほうが結果として優れているように感じられるかもしれませんが、一概にそうとも限りません。その理由は、すべてのセキュリティ要素を、この自己アセスメントの対象範囲として考慮することは不可能だからです。BRP の点数と DiDI の点数が大きく乖離した AoA が存在する場合は、その AoA について詳細に検証する必要があることを示しています。結果の分析では、それぞれの AoA で、BRP と DiDI の相関関係を考察してください。環境が安定していれば、すべての AoA で、相対的に均一な点数が得られると考えられます。DiDI の点数が AoA 全体で均一にない場合は、採用しているセキュリティ戦略が単一のリスク低減手段に依存していることを強く示唆しています。人的要素、プロセス、技術のすべてでバランスが取れたセキュリティ戦略を採用しない限り、環境は攻撃に対してより脆弱になると考えられます。

セキュリティの成熟度

- 各 AOA (分析領域) についてのセキュリティの成熟度の点数は 0 ～ 100 点で、点数が高いほど社内のセキュリティの成熟度レベルが高いことを示します。しかしセキュリティの成熟度の概念は総合的なものなので、採点ではすべての領域の点数を加算して総合的な評価 (ベースライン、標準、最適) を決定します。この総合点は 0 ～ 400 点です。どの領域でも、点数が 0 または 100 になることはまずありません。ほとんどの企業ではある程度の保護策を採用しているので、最低でもベースライン レベルになると考えられます。セキュリティ戦略およびプログラムに巨額の投資が必要なほど深刻なリスク レベルの企業はほとんどありません。
- セキュリティの成熟度は、制御 (物理的なものおよび技術的なものの両方)、IT リソースに対する技術的な洞察力、ポリシー、プロセス、維持可能な施策で構成されます。セキュリティの成熟度は、多くの部門にわたって維持可能なセキュリティ レベルを作成するために利用できるツールを効果的に使用する能力を通じてのみ測定できます。セキュリティの成熟度のベースラインを確立および使用して、組織のセキュリティ プログラムで重点を置く領域を定義する必要があります。すべての組織が最適レベルに到達しようと奮闘する必要はありませんが、ビジネス リスクと比較した現状の評価と目標の決定は必要です。
- 積み重ねグラフには、インフラストラクチャ、アプリケーション、運用、人的要素の 4 つの領域に基づく成熟度の総合点が表示されます。これらの各領域の点数の合計によって、ランク (ベースライン、標準、最適) が決定します。最高点を取るには、多層による予防的なセキュリティ対応を達成する、バランスの取れたアプローチがセキュリティ プログラムに必要です。4 つの分析領域の相対的なサイズを比較することによって、自社のセキュリティ制御について他の領域に比べてより成熟している領域があるかどうかの判断や、適切なリスク低減計画ができます。