【機密性2情報】（有識者会議終了時まで）

資料5

民間の情報保全システムの現状について

対　　策	概要説明
ガバナンス強化、サイバーアタック防御システム	・CodeRed,NIMDA等のワームの特性を分析し、被害の局所化を目指した統合システム 表の顔はウイルス対策システムであるが、本当の顔はガバナンス強化システムであり、社内のセキュリティ情報の把握(数の管理)を実現するコアシステム ・社内のPCとネットワークの情報を統合的に監視し、サイバー攻撃への対応や施策展開の見える化が可能 ・PCのセキュリティ対策としては、PCのシステム状況、パッチ適用状況、検疫、使用禁止ソフトの検出機能をもつ ・ネットワークのセキュリティ対策としては、攻撃監視(IDP)とネットワーク遮断システムから構成されている
情報漏洩防御システム	・過去に発生した情報漏洩事件を分析し、PCの盗難・紛失、媒体を利用したデータ持ち出し、メール誤送信、外注先からの情報漏洩などに対応可能なように設計 ・PCの全ドライブの暗号化機能(PCの盗難紛失対策) ・リムーバブルメディアの使用制限 ・ファイルの暗号化(メール誤送信対策,アクセス制御) ・ログ採取(内部犯罪の抑止) ・スクリーンロック、時刻変更禁止等
シンクライアント	・利用端末を問わないため、いつでもどこでも、情報に安全にアクセス可能 ・USBストレージの利用が不可能な特別USBポートのみを実装したPC USBフラッシュメモリなどへの持ち出しによる、外部記憶媒体経由の情報漏えいを防止 ・リモートデスクトップ接続経由のブレードサーバ利用 管理対象外プリンタからの印刷による、印刷物経由の情報漏えいを防止 ・ハードディスクレスの専用端末、データは全て社内サーバに集約 PC盗難・紛失時のハードディスク残存データの漏えいを防止 ・USBトークンを利用したPC利用者認証 なりすましによる、社内インフラへの不正アクセスを防止 ・情報漏洩対策(データの持ち出し対策)、社外でのPC盗難・紛失対策として導入 ・ID及びパスワード認証に加え、証明書(トークン、ICカード等)を利用した認証が可能 ・OTP(ワンタイムパスワード)等の様々な認証方式に対応可能
入退管理システム	・フラッパーゲートを利用した入退場管理 ・ICカード、指紋等を利用した入退室管理、監視カメラによる入出者監視
統合ログ解析/フォレンジック解析	・各種サーバ、PC、ネットワーク等のログを統合的に解析し、発生した事象の詳細を特定 ・PCやサーバの情報を解析し、発生した事象の詳細を特定
フィジカルセキュリティ	・手のひら静脈認証を用いたセキュリティネットワーク ・手のひら静脈認証を用いたPCログオン用ソフトウェア
統合ID管理基盤の構築による、グループ会社ID管理の一元化	・200社以上のグループ会社社員IDを統合管理。 ・統一ID管理基盤を利用し、グループ内でのWebインフラ、メールインフラの共同利用・効率化を実現
対社外通信におけるセキュリティ対策	・Webフィルタリングの実施 掲示板書き込み、フリーメール利用などによるWeb経由の情報漏えいを防止 ・メールフィルタリングの実施 上長への同報による社外メール送信許可(不正メール送信の抑止) 情報漏えいキーワードの有無によるメール送信制御
社内Webシステムのセキュリティ	・統合ID管理システムと連動したWebシングルサインオンによる、社内Webシステムへのアクセス制御 ・Webコンテンツ(Webファイル)閲覧権限設定によるアクセス制御 通常のアクセス制御に加え、コピー＆ペースト、印刷可否も制御
業務ドキュメントのDRM保護の推進	・メール送信操作に統合された添付ファイルの利用権管理を実施 誤送信先の第三者による添付ファイルの閲覧を防止 ・グループでのネットワークインフラ共用により、効率的なDRMシステムの利用を実現
資産管理ツールによる、クライアントPC環境のセキュリティ維持	・Windowsセキュリティパッチ、ウイルスパターンファイル自動アップデートの統合管理 ・セキュリティ対策状況のレポートの提出
情報漏えい防止ソフトの早期からの導入と定期的な監査	・内部関係者からの漏えいを防止するソフト ・PCの操作や機能を禁止・制御するだけではなく、必要に応じて許可する事が可能 ・ログ取得や不正操作に対する警告などの監視機能 ・外部デバイス及びネットワーク上へ出力したファイルの本体を複製保存 ・無線通信、PDA、USBリンクケーブルなど多様なデバイスからの漏えいを防止可能 ・クライアント側でのアンインストール不可能 ・ハードウェア、ソフトウェアに変更があった場合、即座に管理者へアラート通知 ・柔軟なファイル出力権限とアクティブディレクトリの組織単位、グループ及びユーザーごとに対応したポリシー設定が可能 ・当該情報漏えい防止ソフトがインストールされていないPCからのネットワークアクセスを禁止 ・行動制御、行動監視、資産管理、リモート管理を一つのコンソール画面で管理 ・情報の出力制限、暗号化、通信機能やソフトウェアの制御、ネットワーク利用の制限、監査ログ取得・分析の対応により 情報漏洩防止を徹底しながら効率良い運用が可能 ・社内の従業員、協力会社社員のPCへの導入と定期的な持ち出し監査を実施
Webコンテンツフィルタリングの導入と定期的な監査	・情報漏洩を防止する強力なフィルタリング機能、Webメール、ファイル共有サイト等にファイルがアップされる際に、 ファイルの中身を検知し、制御。 ・豊富なWebセキュリティ機能として、コンテンツフィルタリングの他にアンチウイルス、アンチマルウェア機能、URLフィルタリングを提供。 ・レポーティング機能として、フィルタリングにて禁止されたリスト等を提供
電子メールセキュリティ	・情報漏洩を防止する強力なフィルタリング機能 ・暗号化機能：暗号化ソフトとの連携 ・メール保管機能 ・内部統制にも有効なモニタリング機能 ・レポーティング機能、送受信メールをリアルタイムに分析 違反や傾向を迅速に把握可能
端末の不正接続防止 検疫ネットワーク	・PC検疫 許可されていないPCのネットワーク接続を防止 ポリシーに従っていないPCは検疫ネットワークにて検疫、治療されるまで基幹ネットワークへの接続を防止する仕組みを提供
RFID 電子透かし 電子割符	・暗号化、電子割符によるデータ保護、公開ドキュメントへのアクセス制御、RFIDによる持出し管理、電子透かし印刷 ・重要書類にRFIDタグを付与して、持ち出し管理やトレーサビリティを実現、情報管理の徹底や棚卸作業の効率化が図れる書類管理システム ・書類を格納したボックスとひも付けて格納場所の検索や管理も可能 ・担当者による書類の持出しに際して、当該作業を行う担当者と、取り扱われる書類の種別、管理番号等を特定し、作業記録として蓄積、また権限を超過した作業に対して警告 ・書類の搬出入の履歴をもとに、万一の紛失や情報漏洩が発生した際の最終貸出先の特定や、漏洩元捜索(トレーサビリティ)を実現 ・センター内に格納されている書類の一覧、それぞれの書類の保管年数などを把握し、棚卸の際の固定資産等の確認や使用されている書類の交換指示、不正持出しの早期検出 ・搬入時に、書類と格納するボックスを紐付け、検索や格納場所の管理、書類の格納されたボックスの把握や誤って格納された書類を棚卸時に自動判別
認証局の構築運用	電子署名法に対応した電子認証局からイントラネット向け電子認証局まで、目的や規模に応じた認証局の企画およびから構築・運用をトータルサポート
セキュリティ強化カーネル	・Linuxサーバー向けのセキュリティ強化カーネル ・アクセス制御機能を強化することで、システムへの不正侵入を防止 ・システム管理者が許可したい操作を一通り行うだけで、その操作のみを許可し、それ以外の操作を禁止できるポリシーを自動生成し、セキュリティポリシー作成の労力を大幅に削減 ・アプリケーションレベルでのアクセス制御を行うシステム(Webサーバ、データベースサーバ等)に存在する未知のセキュリティホールを攻撃してシステムに侵入されるという脅威に対する保険として利用 ・システム管理者が作成したポリシー(管理者権限を与えるけれども、必要なコマンドのみを操作可能とする等)に基づきファイルの読み書きやプログラムの実行を制限することで、セキュリティホールに起因する不正侵入に対する耐性を向上 ・セキュリティ修正プログラムの適用頻度を減らすことができるようになるため、動作確認試験のための稼動を削減可能 ・ログイン認証の強化や管理者業務の分担も実現