



内部不正対策 ソリューションガイド



2013年12月26日

特定非営利活動法人
日本ネットワークセキュリティ協会

目 次

1. はじめに.....	3
2. 内部不正対策ソリューションガイド発行に向けて	5
3. 内部不正対策ソリューションガイドの構成と活用方法	7
4. 製品・サービス紹介編	8
5. チェックリスト対応編	76
6. ワーキンググループメンバー.....	89

1. はじめに

昨今、退職の際に技術情報が持ち出され海外に流出する事件や、従業員によって不正に顧客情報が持ち出され個人情報大量漏えいする事件が報道されています。また、悪意はないにしても、USB メモリ等のメディアに格納したデータの紛失や、うっかりミスによるメールの誤送信等を含めると、毎日のように組織の内部者が関係する情報セキュリティ事故が発生しています。

組織の内部者は、何が価値ある情報か、そしてその情報がどこにあるかを把握していません。このため、内部不正では、価値のある情報が大量に盗み出される恐れがあります。日本ネットワークセキュリティ協会 (JNSA) のセキュリティ被害調査 WG の調査では、2005～2011 年の個人情報の漏洩事故のうち、内部犯罪・内部不正行為の件数がわずか 1%程度であるのに対して、内部犯罪・内部不正行為による個人情報の漏洩数は全体の 20%程度に上っています¹。したがって、他の原因の漏洩事故よりも、1 件あたりの被害が多いことがわかります。また、競争力の源泉となる価値ある営業情報が漏洩すれば、競争力低下を招くうえに、内部犯罪・内部不正行為は組織の内部者による犯行であることから、組織自体の信用が失われてしまいます。

このように内部不正は、ひとたび発生すると、事業に大きな影響があることを覚悟しなければなりません。

一方、内部不正に関わる事故は、風評被害が発生する恐れや関係者との調整がつかないなどの理由から、組織内部で処理されてしまう傾向があり、開示義務のあるケースや刑事告発の必要なケースを除いては組織の外部に知られることはめったにありません。また、同業他社などの外部組織との間で情報共有されることは稀であることから、内部不正が発生する要因や効果的な対策の検討を要する場合には、それぞれの組織が自らの経験などをもとに個別に対策を講じているのが実情です。

このような背景から、独立行政法人情報処理推進機構 (IPA) は、2013 年 3 月に、内部不正行為を防止するための環境整備を推進する「組織における内部不正防止ガイドライン」を公開しました。

このガイドラインでは、内部不正の実態をつかみ、実態から得られた事例を極力網羅し

¹ セキュリティ被害調査 WG の原因区分では、「内部犯罪・内部不正行為 (件数率: 約 1%)」の他にも「不正な情報持ち出し (件数率: 約 5%)」などを別に分類しているが、本 WG ではこれらの不正な情報持ち出しも対策の範囲に含めるため、本内部不正対策ソリューションガイドで対策が可能な具体的件数や被害はさらに大きいと考えられる。

た対策を示しています。また、これまで内部不正対策について「考えてこなかった」「何をすればよいかわからなかった」という企業（特に中小企業に重きをおいて）が対策を講じる際の指針として、効果的な環境整備ができることを目指しています。

2. 内部不正対策ソリューションガイド発行に向けて

本冊子は、独立行政法人情報処理推進機構（IPA）によって2013年3月に公開された「組織における内部不正防止ガイドライン」（以下 IPA ガイドライン）に定められた各条項を具現化し、「組織における内部不正」を抑制するための具体的ソリューションを紹介することを目的としたソリューションガイドです。

組織における情報セキュリティでは、人による情報漏洩が話題になり、多くのベンダーから、その対策を行うソリューションが提供されています。本冊子の内容はこれらのソリューションを、IPA ガイドラインをベースにして整理したものであり、同ガイドラインの各条項で示された内容を実際の職場で実現するためには、具体的には何をどうすれば良いかの参考となるように編まれています。

○IPA ガイドラインの内容

一般に、組織が直面する課題を解決する方法としては「制度（組織、社会、ルール）」、「教育（人の啓発）」、「技術（システム）」の3つの方向性があります。「制度を作り、教育によって人を変え、技術で駄目押し」という形です。実際、IPA ガイドラインでは、組織で働く人による情報漏洩に着目し、それを防ぐために、情報システム部門における技術的観点のみならず、総務的観点、人事的な観点も含めて、組織全体で対応しなければならないことについて書かれています。

本ソリューションガイドでは、IPA ガイドラインに則る形で、技術的ソリューションに限らず、働く人の意識や組織文化を変えることによって組織で働く人間が引き起こす情報セキュリティ事故を抑制する手法として、人事的観点、総務的観点からのソリューションについても紹介しています。

○内部不正の影響度

一方、情報漏洩などの「情報セキュリティ事故」を抑制することは、組織運営上の重要な課題には違いありませんが、組織で働く人間が引き起こす事故は、情報セキュリティ分野に限りません。その他にも、違法（脱法）行為、ルール違反に関係する事故としては、使い込み、内部窃盗、不正経理、取引先等との癒着、意図的不作為・隠蔽、組織の私物化（公私混同）などが、組織運営に影響を及ぼす事故としてあげられます。

○内部不正対策ソリューションガイドの意義

組織で働く人間のルール違反（不正）は、組織内部の問題として水面下で処理されること

も少なくなく、社会的に顕在化することは多くありません。しかしながら、これらの事故が、組織や社会に及ぼす影響は決して無視できるものではありません。組織で働く人間が引き起こす違法（脱法）行為、ルール違反への対応は、顕在化はしていないものの、社会的に具体的なソリューションが渴望されている分野ということです。

本冊子で紹介された各種ソリューションは、「組織で働く人間が引き起こす情報漏洩」という情報セキュリティ上の事故に対応するためのベストチョイスを紹介したものです。しかし、これはあくまでも対象を「組織で働く人間が引き起こす情報漏洩」という情報セキュリティ上の事故に限定したうえで、さらに「現時点で、という但し書きが付く範囲で」でしかありません。

組織にとってのそもそもの「セキュリティ」とは、「組織のオペレーションがきちんと回っている状態」を維持することです。その意味で、このソリューションガイドは、「情報漏洩対策」を超えて「組織で働く人間が引き起こす様々な事故」をカバーする形で、また「技術的、システムの対策」を超えて「組織で働く人の意識や組織文化」や「組織の行動が影響を受ける社会文化や規範」にも関わる形で、どんどん成長していくべきものなのではないかと考えています。

JNSA 組織で働く人間が引き起こす不正・事故対応 WG
甘利 康文(セコム IS 研究所)

3. 内部不正対策ソリューションガイドの構成と活用方法

本内部不正対策ソリューションガイドは、「チェックリスト対応編」と「製品・サービス紹介編」から構成しています。IPA ガイドラインの付録Ⅱ：内部不正チェックシートでは、所属する企業や組織の実態をチェックすること、及び所属する部署や部門で何を対策すべきかを調べることができます。

○チェックリスト対応編の内容（A3 横 印刷）

各具体的な対策を検討する際には、はじめにチェックリスト対応編でどのような製品やサービスが提供されているのかを確認してください。このチェックリスト対応編では、各項目の管理策レベルではなく、対策のポイントごとに対応する製品やサービスを紹介しています。

○製品・サービス紹介編の内容（A4 縦 印刷）

チェックリスト対応編で導入検討する製品やサービスを確認した後に、具体的な製品やサービスを知りたい場合は、製品・サービス紹介編を確認してください。製品・サービス紹介編では、一般的な情報セキュリティ対策としては理解しにくい内部不正対策特有のポイントについては、チェックリストの対策のポイント（最左のNo）ごとに、どのような観点で対応しているのかを必要に応じて個別に紹介しています。

IPA ガイドラインとあわせて、内部不正対策の検討にご活用ください。

4. 製品・サービス紹介編

No	製品・サービスの紹介文
1	<p data-bbox="352 477 1050 506">CheckPoint Endpoint Security Full Disk Encryption【メトロ】</p> <p data-bbox="352 524 1378 647">ハードディスク全体の暗号化と OS 起動前の認証により、情報漏洩を強力に防止します。ハードディスクにデータが書き込まれる際に自動で暗号処理を行い、読み込む際に自動で復号処理を行うので、ユーザは暗号化するために特別な操作をする必要がありません。</p> <p data-bbox="352 667 1366 741">専用サーバによる集中管理でソフトウェアのライセンス管理、導入されているバージョンの管理、ログの自動回収など、一元的な管理により大幅に運用コストを削減できます。</p> <p data-bbox="352 813 408 842">[URL]</p> <p data-bbox="352 860 1134 889">http://www.metro.co.jp/products/security/cp_eps_e80/fde.html#tabs</p> <p data-bbox="352 954 520 983"><問い合わせ先></p> <p data-bbox="352 1003 839 1032">株式会社メトロ IT インフラサービス営業部</p> <p data-bbox="352 1052 943 1081">TEL:03-5789-1022 E-mail: sales@tokyo.metro.co.jp</p>
2	<p data-bbox="352 1104 1002 1133">CheckPoint Endpoint Security Media Encryption【メトロ】</p> <p data-bbox="352 1151 1366 1373">メディアのセキュリティ対策に必要な3つの機能（デバイス制御、メディアの丸ごと暗号、操作ログ）を本製品のみで提供可能。面倒なUSBメモリの個体番号を登録せずに、USBメモリを利用制限できる機能は運用負担を軽減、また、低価格な汎用USBメモリやDVDメディアを丸ごと暗号化できるため対策コストを抑えることが可能です。外部メディアへのファイルコピーの際などファイル名のログ収集できるため、証拠証跡として活用できます。</p> <p data-bbox="352 1440 408 1469">[URL]</p> <p data-bbox="352 1487 1062 1516">http://www.metro.co.jp/products/security/cp_eps_e80/me.html</p> <p data-bbox="352 1581 520 1610"><問い合わせ先></p> <p data-bbox="352 1630 839 1659">株式会社メトロ IT インフラサービス営業部</p> <p data-bbox="352 1680 943 1709">TEL:03-5789-1022 E-mail: sales@tokyo.metro.co.jp</p>

3	<p>CheckPoint Appliance【メトロ】</p> <p>Check Point ApplianceはPC、Check Point Go iPad、iPhone などマルチデバイスからのVPN接続に対応し、持ち出しシーンに応じたリモートデスクトップ接続環境を提供します。</p> <p>従来のPCからのVPN接続だけでなく、専用アプリによるiOS、AndroidからのVPN接続や標準搭載の証明書認証を組み合わせれば端末制御としての活用も可能。</p> <p>私物スマートフォンを業務で利用するBYODにも最適です。Check Point Go（USBタイプのデバイス）の活用なら自宅のPCから安全に会社PCにVPN接続することができます。</p> <p>[URL]</p> <p>http://www.metro.co.jp/products/security/cp_utml/remotearchive.html</p> <p><問い合わせ先></p> <p>株式会社メトロ ITインフラサービス営業部</p> <p>TEL:03-5789-1022 E-mail: sales@tokyo.metro.co.jp</p>
4	<p>IBM Guardium【メトロ】</p> <p>Guardiumは、データベース監査ログを一元管理し、ログ収集から、加工、レポート出力、確認までに関わる膨大な工数を削減し、データベース管理者を含む全てのアクセスをリアルタイムに監視しながら、既存環境のパフォーマンスへの影響は最小限に抑えることができます。「ログの記録」、「アラート（警告）」、「集計・レポート」をシンプルな構成で実現しながらも、不正な振る舞いを検知しアラートやセッションの遮断が可能です</p> <p>[URL]</p> <p>http://www.metro.co.jp/products/security/guardium/</p> <p><問い合わせ先></p> <p>株式会社メトロ ITソリューション営業部</p> <p>TEL:03-5789-1022 E-mail: sales@tokyo.metro.co.jp</p>

5	<p>CheckPoint Appliance【メトロ】</p> <p>Check Point Appliance は Web 2.0 のアプリケーションやソーシャル・ネットワーキング・ウィジェットが 24 万件以上登録された、世界最大規模のアプリケーション・ライブラリを利用可能 アプリケーションを識別、検出、分類、制御します。</p> <p>ポートやプロトコルの種類、ネットワークをすり抜ける回避技術が使用されているかどうかに関係なく、アプリケーションのセキュリティ・ポリシーに基づいて、膨大な数のアプリケーションを識別します。</p> <p>[URL]</p> <p>http://www.metro.co.jp/products/security/cp_utml/remoteaccess.html</p> <p><問い合わせ先></p> <p>株式会社メトロ IT インフラサービス営業部</p> <p>TEL:03-5789-1022 E-mail: sales@tokyo.metro.co.jp</p>
6	<p>SHieldWARE【富士通株式会社】</p> <p>SHieldWARE は、汎用の OS 機能では不可能なサーバのセキュリティ強化を実現するソフトウェア製品です。システム管理者も含めた全てのユーザに対するアクセス制御や詳細なログ記録により、不正アクセスやマルウェアの活動などの脅威による改ざんや情報漏えいに対して、強固なサーバセキュリティ対策を実現します。</p> <p>【製品情報詳細】</p> <p>http://jp.fujitsu.com/solutions/safety/secure/products/shieldware/</p>
7	<p>FENCE メール誤送信対策サービス【富士通株式会社】</p> <p>FENCE メール誤送信対策サービスは、メール送信時にメールの内容を自動的に監査し、問題ありと判定したメールを自動的に中断または保留します。問題なしと判定されたメールのみ、メール本文や添付ファイルを自動的にパスワード付き形式に変換します。これにより、簡単・確実にメールからの情報漏えい対策を実現できます。</p> <p>【製品情報詳細】</p> <p>http://jp.fujitsu.com/solutions/safety/secure/products/fence/fence-mail-service/</p>
8	<p>FENCE-PRO【富士通株式会社】</p> <p>社員による情報の持ち出し、PC の盗難・紛失など、企業の重要データは、常に思わぬ危険にさらされています。FENCE-Pro は、強力な AES 暗号アルゴリズムの採用により、それらの脅威から情報資産を守ります。</p>

	<p>【製品情報詳細】</p> <p>http://jp.fujitsu.com/solutions/safety/secure/products/fence/fence-pro/</p>
9	<p>ランブック自動化: 「HP Operations Orchestration」「NetIQ Aegis」 【SCSK】</p> <p>ランブック自動化は IT オペレーションの自動化を実現し、定型業務の効率化と品質を改善します。</p> <p>利用者 ID などのアカウント管理における承認を受け、アクセス権の登録・設定・削除・報告などの各処理の自動化が可能です。</p> <p>また、処理結果のログ管理やその他定型オペレーションの自動化対応も可能です。</p> <p>【製品情報詳細】</p> <p>http://www.scsk.jp/product/common/netiq_aegis/</p> <p>◆お問い合わせ先◆</p> <p>SCSK 株式会社</p> <p>ITエンジニアリング事業本部 ミドルウェア部</p> <p>担当: 奥谷、松井、加藤</p> <p>Tel: 03-5166-1382</p> <p>E-Mail: mw-sales@ml.scsk.jp</p>
10	<p>ネットワーク脅威対策製品: Palo Alto Networks PA シリーズ 【SCSK】</p> <p>「Palo Alto Networks PA シリーズ」はアプリケーション識別機能をコア技術としたアプリケーションファイアウォール製品。コンテンツセキュリティ機能 (Antivirus、IPS、URLFiltering) も兼ね備え、アプリケーション単位、User 単位での細かいアクセス制御が可能です。</p> <p>トラフィック状況、外部脅威状況、ボットネット感染端末等のレポートも充実しています。</p> <p>【製品情報詳細】</p> <p>http://www.scsk.jp/product/common/paloalto/</p> <p>◆お問い合わせ先◆</p> <p>SCSK 株式会社 IT プロダクト&サービス事業本部 ネットワークセキュリティ部</p> <p>担当: 釜井</p> <p>Tel: 03-5859-3037</p> <p>E-Mail: paloalto-info@ml.scsk.jp</p>

11	<p>Web マルウェア対策製品: McAfee Web Gateway 【SCSK】</p> <p>プロキシ、キャッシュ、フィルタの基本的な機能はもちろん、リクエストされた Web ページを介するコンテンツとコードの性質と意図を分析し、マルウェアやブラウザへの攻撃など、隠された脅威からの保護を実現します。</p> <p>【製品情報詳細】 http://www.scsk.jp/product/common/mcafee/</p> <p>◆お問い合わせ先◆ SCSK 株式会社 IT プロダクト&サービス事業本部 ネットワークセキュリティ部 担当：鈴木 Tel：03-5859-3037 E-Mail：mcafee-info@ml.scsk.jp</p>
12	<p>IT データ解析プラットフォーム：Splunk Enterprise 【SCSK】</p> <p>企業内データの大半を占めるマシンデータには、大きな価値と可能性が秘められています。それらを Splunk に投入し、インデックスを付け、解析することにより、ビジネス、IT、セキュリティに役立つ多種多様な情報をリアルタイムで可視化することができます。セキュリティ用途では、収集した各種ログデータの監視はもちろんのこと、時系列に基づいた解析を行うことで、インシデント調査時等にも活用いただけます。</p> <p>【製品情報詳細】 http://www.scsk.jp/product/common/splunk/index.html</p> <p>◆お問い合わせ先◆ SCSK 株式会社 IT エンジニアリング事業本部 ミドルウェア部 担当：根本、手塚 Tel：03-5166-1277 E-Mail：splunk-sales@ml.scsk.jp</p>
13	<p>ログ統合管理システム：Arcsight 【SCSK】</p> <p>ネットワーク上に存在するネットワーク機器、サーバー、アプリケーション等からリアルタイムでログを収集、保管し、多様な分析・レポート機能を提供するログ統合管理ソリューションです。</p> <p>【製品情報詳細】 https://www.scsk.jp/sp/sys/products/arcsight/index.html</p>

	<p>◆お問い合わせ先◆</p> <p>SCSK 株式会社 グローバルセキュリティソリューション部</p> <p>Tel: 03-5166-2815</p> <p>E-Mail: sys-staff@ml.scsk.jp</p>
14	<p>インシデントレスポンスサービス 【SCSK】</p> <p>インシデント発生時にセキュリティプロフェッショナルが、サービス再開までをサポートするサービスです。</p> <p>【サービス情報詳細】</p> <p>https://www.scsk.jp/sp/sys/</p> <p>◆お問い合わせ先◆</p> <p>SCSK 株式会社 グローバルセキュリティソリューション部</p> <p>Tel: 03-5166-2815</p> <p>E-Mail: sys-staff@ml.scsk.jp</p>
15	<p>認証アプライアンスサーバ:RADIUS GUARD (ラディウスガード) 【SCSK】</p> <p>RADIUS GUARD は、スマートデバイスやPCなど、許可した端末や利用者だけに、業務ネットワークへアクセス許可する RADIUS 認証・DHCP アプライアンスサーバです。</p> <p>ネットワーク認証に必要な RADIUS、DHCP、認証局機能、ユーザ管理機能、利用申請ワークフローを1台に集約し、Web 認証、MAC 認証、802.1x 認証に対応。</p> <p>無線 LAN や VPN を安全に、低い運用負荷で利用したいお客様に最適です。</p> <p>【製品情報詳細】</p> <p>http://www.scsk.jp/product/common/radius/</p> <p>◆お問い合わせ先◆</p> <p>SCSK 株式会社</p> <p>IT エンジニアリング事業本部</p> <p>エンジニアリングソリューション第一部</p> <p>E-Mail: RG-info@ml.scsk.jp</p> <p>Tel: 03-5859-3034</p>

16	<p>情報セキュリティ・内部統制コンサルティング【インフォセック】</p> <p>内部不正などの情報セキュリティリスクへの対策及び内部統制整備をご支援します。リスクマネジメント体制の構築、規程/ポリシー/手順の整備、重要情報の区分といった仕組み/ルールづくりから、それらの運用状況のモニタリングまで幅広くご支援致します。</p> <p>まとまった施策単位でのご支援のほかに、情報セキュリティに関するアドバイスを月額の固定費用でご提供する「安心ドクター」サービスもご用意しています。</p> <p>【サービス情報詳細】</p> <p>http://www.infosec.co.jp/service/management/05.html</p> <p>http://www.infosec.co.jp/service/management/11.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社インフォセック</p> <p>Tel : 03-5733-6500</p> <p>Email : contact-info@infosec.co.jp</p>
17	<p>統合ログ管理サービス【インフォセック】</p> <p>内部不正の予防/発見に役立つ様々なログ分析をご提供します。あらゆるデバイス、アプリケーションからの作業内容、作業日時等のログデータを収集し、複数のログからの事象特定/原因調査など、複合的な相関分析を実現します。(例：入退管理ログと社内システム利用ログを複合して分析し、不在者のID不正利用を発見する、等)</p> <p>また、ログ保存期間の安全管理もいたします。</p> <p>【サービス情報詳細】</p> <p>http://www.infosec.co.jp/service/securitysystem/03.html</p> <p>【監視ツール ArcSight についてはこちら】</p> <p>http://www.infosec.co.jp/service/system/09.html#id01</p> <p>◆お問い合わせ先◆</p> <p>株式会社インフォセック</p> <p>Tel : 03-5733-6500</p> <p>Email : contact-info@infosec.co.jp</p>

18	<p>エンドポイントセキュリティ (IBM Tivoli Endpoint Manager) 【インフォセック】</p> <p>わずか1つのプラットフォームにより、資産管理からソフトウェア配布、パッチ管理、節電のための電源管理まで、10種類以上の機能を実現します。</p> <p>分散型アーキテクチャにより、1台の管理サーバで多数・多種のエンドポイントをリアルタイムに一元管理し、設備投資や運用コストを抑制します。</p> <p>【サービス情報詳細】</p> <p>http://www.infosec.co.jp/service/security/06.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社インフォセック</p> <p>Tel : 03-5733-6500</p> <p>Email : contact-info@infosec.co.jp</p>
19	<p>情報セキュリティ教育 【インフォセック】</p> <p>E-ラーニング、集合研修、ハンドブック作成など。</p> <p>内部不正対策に役立つ、情報セキュリティや個人情報保護などのコンテンツを取り揃えて、導入しやすい価格帯で提供しています。</p> <p>お客様固有の規程類・業務内容・利用システムなどに合わせた、コンテンツ内容のカスタマイズもご相談にのります。</p> <p>【ハンドブックのご紹介】</p> <p>http://www.infosec.co.jp/handbook/index.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社インフォセック http://www.infosec.co.jp/</p> <p>Tel : 03-5733-6500</p> <p>Email : contact-info@infosec.co.jp</p>

20	<p>情報セキュリティ監査【インフォセック】</p> <p>独立した専門家の観点から、セキュリティ対策の実施状況や整備状況、セキュリティ事故の発生及び対処の状況を監査し、内部不正等のリスクをより効果的に抑制するための改善案を提示します。また、情報セキュリティ監査に関連し教育、知識トランスファーを行うサービスもご提供します。</p> <p>【サービス情報詳細】</p> <p>http://www.infosec.co.jp/service/management/19.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社インフォセック</p> <p>Tel : 03-5733-6500</p> <p>Email : contact-info@infosec.co.jp</p>
21	<p>ファイル暗号化ソフト「InterSafe IRM」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>InterSafe IRM は、ファイルを閲覧や保存時に自動的に暗号化し、アクセス権限を付与するソフトウェアです。Office 系ドキュメントだけでなく、CAD や動画等、あらゆるデータを暗号化し、アクセス権限付与することで、情報の不正な持ち出しを防止します。万一、持ち出されても、暗号化により解読することができません。また、暗号化ファイルへのアクセス履歴を取得することも可能です。</p> <p>http://www.alsi.co.jp/security/isirm/</p> <p>◆お問い合わせ先◆</p> <p>アルプス システム インテグレーション株式会社</p> <p>セキュリティ営業部</p> <p>Tel : 03-5499-8045</p> <p>E-Mail : ssg@alsi.co.jp</p>

22	<p>デバイス制御ソフト「InterSafe DeviceControl」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>InterSafe DeviceControl は PC から外部デバイスへのアクセス管理とログを取得するソフトウェアです。アプリケーションの起動制御ではなく、ファイルの読み込み・書出しに制御をかけているため、ライティングソフトに依存せず、デバイス制御を行うことが可能です。また、登録した USB メモリや外付け HDD のみ書出しを許可し、個人で持ち込んだデバイスの利用を禁止します。</p> <p>http://www.alsi.co.jp/security/isdc/</p> <p>◆お問い合わせ先◆</p> <p>アルプス システム インテグレーション株式会社 セキュリティ営業部 Tel: 03-5499-8045 E-Mail: ssg@alsi.co.jp</p>
23	<p>セキュリティ USB メモリ作成ソフト「InterSafe SecureDevice」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>InterSafe SecureDevice は市販や今ご利用中の USB メモリを、暗号化しコピーガード付きのセキュリティ USB メモリに変換するソフトウェアです。暗号化と登録されていない PC へのデータコピー、移動の制御により、持ち出し後の情報漏洩等を防止いたします。 また、持ち出し後の操作ログを取得することも可能です。</p> <p>http://www.alsi.co.jp/security/sd/</p> <p>◆お問い合わせ先◆</p> <p>アルプス システム インテグレーション株式会社 セキュリティ営業部 Tel: 03-5499-8045 E-Mail: ssg@alsi.co.jp</p>
24	<p>持出し管理ソフト「InterSafe WorkFlow」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>InterSafe Workflow は、InterSafe DeviceControl により、外部デバイスへの書き込みが規制されている場合でも、書き出し申請・承認経て、デバイス制御の解除、または許可したファイルのみ書出すことが可能です。ファイル単位で書出しを許可した場合、デバイス保存時に自動</p>

	<p>的に暗号化ファイルに変換し、書き出したファイルをサーバー上にアーカイブします。また、「誰が」「いつ」「何を」書出したか、ログも取得可能です。</p> <p>http://www.alsi.co.jp/security/isfl/</p> <p>◆お問い合わせ先◆ アルプス システム インテグレーション株式会社 セキュリティ営業部 Tel: 03-5499-8045 E-Mail: ssg@alsi.co.jp</p>
25	<p>セキュリティ PDF 作成ソフト「InterSafe SecurePDF」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>InterSafe SecurePDF（セキュア PDF）は、Word、Excel 等のファイルから有効期限や印刷制限などを付与したセキュリティ PDF を作成します。</p> <p>スマートフォンやタブレット端末でも、セキュリティを保ったままデータを活用することが可能です。InterSafe IRM 利用時には、既存の暗号化ファイルを直接セキュア PDF 化できます。</p> <p>http://www.alsi.co.jp/security/issp/</p> <p>◆お問い合わせ先◆ アルプス システム インテグレーション株式会社 セキュリティ営業部 Tel: 03-5499-8045 E-Mail: ssg@alsi.co.jp</p>
26	<p>Web フィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>InterSafe WebFilter は、URL データベースに基づいて Web アクセスをコントロールする顧客満足度 No.1 の国産 Web フィルタリングソフトです。SNS や Web メール、オンラインストレージ、掲示板などへのアクセス・書き込み・アップロードを規制します。暗号化された HTTPS 通信にも標準対応しています。また、Google Apps の業務用アカウントのみ利用を許可するなど、柔軟な運用が可能です。</p> <p>http://www.alsi.co.jp/security/is/</p> <p>◆お問い合わせ先◆</p>

	<p>アルプス システム インテグレーション株式会社 セキュリティ営業部 Tel: 03-5499-8045 E-Mail: ssg@alsi.co.jp</p>
27	<p>クラウド型 Web フィルタリングサービス「InterSafe CATS」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>InterSafe CATS は、サーバーレス環境で Web アクセスのコントロールが可能なクラウド型 Web フィルタリングサービスです。管理は全てクラウド上で行なうため、大がかりな設備投資が不要で導入が容易です。また、社内ネットワークに接続していないモバイル PC も一元管理します。SNS やオンラインストレージなどへのアクセス・書き込み・アップロードを規制する他、アプリ規制も可能です (HTTPS 標準対応)。</p> <p>http://www.alsi.co.jp/security/iscats/</p> <p>◆お問い合わせ先◆</p> <p>アルプス システム インテグレーション株式会社 セキュリティ営業部 Tel: 03-5499-8045 E-Mail: ssg@alsi.co.jp</p>
28	<p>ログ分析ソフト「InterSafe LogDirector」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>InterSafe LogDirector は、簡単操作で Web 利用状況を把握できる Web アクセスログ分析ソフトです。内部の誰が、いつ、どんなサイトで、何を行ったのかまで明らかにし、アクセスマネージメントの改善や問題行動の調査に役立てることができます。高速ログ検索で、Web アクセスや Web メールの利用履歴も容易に追跡。さらに、内部の不正アクセスを検知して管理者に知らせるアラート機能も搭載しています。</p> <p>http://www.alsi.co.jp/security/isld/</p> <p>◆お問い合わせ先◆</p> <p>アルプス システム インテグレーション株式会社 セキュリティ営業部 Tel: 03-5499-8045 E-Mail: ssg@alsi.co.jp</p>

29	<p>スマートデバイス向けフィルタリングソフト「InterSafe SecureBrowser」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>InterSafe SecureBrowser は、スマートデバイスの Web アクセスを一括管理する Web フィルタリング機能付きセキュアブラウザです。SNS や Web メール、オンラインストレージ、掲示板などへのアクセスを規制し、情報漏洩や私的利用を防止。Web アクセスログの集計、レポートや検索も可能です。スマートデバイスのセキュアかつ快適な Web アクセスをクラウドによる一括管理で実現します。</p> <p>http://www.alsi.co.jp/security/issb/</p> <p>◆お問い合わせ先◆</p> <p>アルプス システム インテグレーション株式会社 セキュリティ営業部 Tel: 03-5499-8045 E-Mail: ssg@alsi.co.jp</p>
30	<p>スマートデバイス向け統合セキュリティサービス「ビジネススマートセキュリティ」【アルプスシステムインテグレーション】</p> <p>【製品情報詳細】</p> <p>ビジネススマートセキュリティは、スマートデバイスに必要なセキュリティをオールインワンで提供する統合型クラウドサービスです。専用アプリ不要の Web フィルタリングとアプリフィルタリングで、SNS や Web メール、オンラインストレージ、掲示板などへのアクセスやアプリ利用を規制して情報漏洩を防止。さらに、リモートワイプや MDM、拠点間 VPN など、10 の機能で紛失対策やログ管理が可能です。</p> <p>http://www.netstar-inc.com/bssecurity/</p> <p>◆お問い合わせ先◆</p> <p>アルプス システム インテグレーション株式会社 セキュリティ営業部 Tel: 03-5499-8045 E-Mail: ssg@alsi.co.jp</p>
31	<p>i-FILTER 【デジタルアーツ】</p> <p>○Web フィルタリングソフト「i-FILTER」</p> <p>「i-FILTER」 は Web アクセスの制御と可視化(ログ取得など) はもちろん、Web アクセスの入口対策から出口対策までトータルな Web セキュリティソリューションを提供し、情報漏洩対策</p>

	<p>を強かに支援します</p> <p>【製品情報詳細】 http://www.daj.jp/bs/i-filter/</p> <p>◆お問い合わせ先◆ デジタルアーツ株式会社 担当：営業部 Tel：03-5220-3090 問合せフォーム：http://www.daj.jp/bs/inquiry/</p>
32	<p>m-FILTER【デジタルアーツ】</p> <p>○電子メールフィルタリングソフト「m-FILTER」</p> <p>「m-FILTER」はメール誤送信に起因する情報漏洩を効果的に防止するメールセキュリティソフトウェアです。添付ファイルの暗号化、一時保留、本人確認、上長承認等あらゆる誤送信防止機能を単一製品でご提供します。</p> <p>さらに、内部統制や法規制対応に必要なメール保存、メールによる外部からの脅威を排除するアンチスパム機能も搭載しており、電子メール運用における脅威・課題をトータルで解決します。</p> <p>【製品情報詳細】 http://www.daj.jp/bs/mf/</p> <p>◆お問い合わせ先◆ デジタルアーツ株式会社 担当：営業部 Tel：03-5220-3090 問合せフォーム：http://www.daj.jp/bs/inquiry/</p>

33	<p>i-FILTER ブラウザー&クラウド【デジタルアーツ】</p> <p>○法人向けクラウド型 Web フィルタリングサービス「i-FILTER ブラウザー&クラウド」</p> <p>「i-FILTER ブラウザー&クラウド」は、従業員が社外で利用するスマートフォンやノート PC、店頭に置かれたタブレット端末から社内のデスクトップ PC まで、クラウドで一元管理できる Web フィルタリングサービスです。Web アクセスにフォーカスして、業務効率化と同時にさまざまな脅威から、iOS/Android/Windows 端末を守ります。</p> <p>【製品情報詳細】</p> <p>http://www.daj.jp/bs/ifb/</p> <p>◆お問い合わせ先◆</p> <p>デジタルアーツ株式会社</p> <p>担当：営業部</p> <p>Tel：03-5220-3090</p> <p>問合せフォーム：http://www.daj.jp/bs/inquiry/</p>
34	<p>D-SPA【デジタルアーツ】</p> <p>○純国産セキュア・プロキシ・アプライアンス「D-SPA」</p> <p>「D-SPA」は標的型攻撃に対して有効な入口対策・出口対策機能に加え、Web アクセスの一元化・可視化と容易な導入と運用管理を実現する「純国産」アプライアンス製品です。</p> <p>「i-FILTER」で高い実績を有する Web フィルタリングやプロキシ・キャッシュなど、Web アクセスに求められる機能を高速に処理し、国産ならではのサポート体制と合わせ安心してスマートな運用に貢献します。</p> <p>【製品情報詳細】</p> <p>http://www.daj.jp/bs/dspa/</p> <p>◆お問い合わせ先◆</p> <p>デジタルアーツ株式会社</p> <p>担当：営業部</p> <p>Tel：03-5220-3090</p> <p>問合せフォーム：http://www.daj.jp/bs/inquiry/</p>

35	<p>FinalCode【デジタルアーツ】</p> <p>○パスワードレスのファイル暗号化・追跡ソリューション「FinalCode」</p> <p>「FinalCode」は、重要ファイルを暗号化して、利用状況を追跡、遠隔で削除もできるファイル暗号化・追跡ソリューションです。</p> <p>開封ユーザーを限定して重要ファイルを暗号化（AES 256bit 形式）するため、パスワード通知も不要、さらにファイル提供後も動的に権限を変更することで、従来では不可能だったファイルの回収（削除）も簡単に実現します。</p> <p>【製品情報詳細】</p> <p>http://www.finalcode.com/jp/</p> <p>◆お問い合わせ先◆</p> <p>デジタルアーツ株式会社</p> <p>担当：営業部</p> <p>Tel：03-5220-3090</p> <p>問合せフォーム：http://www.daj.jp/bs/inquiry/</p>
36	<p>ISMS 認証取得支援サービス【OSK】</p> <p>「JIS Q 27001：2006（ISO/IEC27001：2005）」の認証を取得するための支援を行います。情報セキュリティ管理のグローバルスタンダードに準拠することで、経営課題である情報セキュリティリスクに対し、技術的な対応だけでなく組織的に対応していくことができます。</p> <p>[製品情報詳細]</p> <p>http://www.kk-osk.co.jp/consult/isms.asp</p> <p>[お問合せ先]</p> <p>株式会社 OSK IT コンサルタント課</p> <p>webmaster@kk-osk.co.jp</p>
37	<p>プライバシーマーク取得支援サービス【OSK】</p> <p>個人情報の取扱いに関するリスク分析結果に基づき、必要な対策を規程化し、従業員への教育・監査・見直しを実施するなど、個人情報に関する適切な保護態勢を構築していきます。プライバシーマークの取得は、情報セキュリティ強化だけでなく、企業の社会的信用の獲得にも役立ちます。</p> <p>[製品情報詳細]</p> <p>http://www.kk-osk.co.jp/consult/pmark.asp</p>

	<p>[お問合せ先] 株式会社 OSK IT コンサルタント課 webmaster@kk-osk.co.jp</p>
38	<p>情報セキュリティポリシー策定支援サービス【OSK】</p> <p>情報資産に対する脅威・脆弱性調査を実施、その結果に基づき情報セキュリティに関する必要な対策を内部規程としてまとめていきます。企業活動を支える情報システムを、適切な情報セキュリティポリシーに沿って運用することで、高度な安全性を確保することができます。</p> <p>[製品情報詳細] http://www.kk-osk.co.jp/consult/spolicy.asp</p> <p>[お問合せ先] 株式会社 OSK IT コンサルタント課 webmaster@kk-osk.co.jp</p>
39	<p>身近な事例で学ぶ情報セキュリティ（eラーニング）【OSK】</p> <p>情報セキュリティ事件・事故の事例から、日常の業務の中で注意しなければならない情報セキュリティ対策について学習できます。標的型攻撃への対策からスマートフォンや SNS 利用時の注意点についても収録しています。</p> <p>[製品情報詳細] http://www.kk-osk.co.jp/product/elearning/elexpress/itsec.asp</p> <p>[お問合せ先] 株式会社 OSK IT コンサルタント課 webmaster@kk-osk.co.jp</p>
40	<p>迫りくる危機！個人情報保護対策（eラーニング）【OSK】</p>

	<p>個人情報の取り扱いを行っている企業の従業員を対象に、日常業務の中に潜む危険性を従業員全員が意識するように、日常的に行わなければならないことを具体的な事例を通じて紹介し、対策を講じる手助けを行います。</p> <p>[製品情報詳細] http://www.kk-osk.co.jp/product/elearning/elexpress/itsec.asp</p> <p>[お問合せ先] 株式会社 OSK IT コンサルタント課 webmaster@kk-osk.co.jp</p>
41	<p>プライバシーマークの基礎知識（eラーニング）【OSK】</p> <p>最新の審査内容と JISQ15001 を基に、プライバシーマークを取得する企業の従業員とプライバシーマークを取得している企業の従業員が、最低限知っておかなければならない知識を紹介します。</p> <p>[製品情報詳細] http://www.kk-osk.co.jp/product/elearning/elexpress/itsec.asp</p> <p>[お問合せ先] 株式会社 OSK IT コンサルタント課 webmaster@kk-osk.co.jp</p>
42	<p>シングルサインオンアプライアンス : Smart eGate 【ソリトンシステムズ】</p> <p>「Smart eGate」は、通信経路上に設置するだけでシングルサインオン環境を実現するための革新的手法を提供します。リバースプロキシ型やエージェント型等の従来型製品のような環境依存はありません。これにより、様々な端末から様々なサイトへ、透過的シングルサインオンを実現します。ユーザは ID/パスワード管理から解放され、管理者はサイトアクセスの一元的な制御/管理が容易になり、「利便性」と「セキュリティ」の両立ができます。</p> <p>【製品情報詳細】 http://www.soliton.co.jp/egate/</p> <p>◆お問い合わせ先◆ 株式会社ソリトンシステムズ IT Security 事業本部 営業本部 Tel: 03-5360-3811 E-Mail: netsales@soliton.co.jp</p>

43	<p>ウェブセキュリティプライアンス : Cisco WSA 【ソリトンシステムズ】</p> <p>「Cisco WSA」は、オールインワンの Web プロキシアプライアンスです。Web レピュテーションフィルタによる Web サイトアクセス制御や、URL フィルタによる Web サイトの分類化に加え、アンチウイルス/マルウェア対策、ユーザごとの Web サイトアクセス制御機能も保持しています。システム全体の統計情報も簡単に取得できます。また Active Directory 等の認証基盤と連携することで、利用者毎のアクセス制御及び、アクセスログの取得が可能になります。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/ironports/</p> <p>◆お問い合わせ先◆</p> <p>株式会社ソリトンシステムズ IT Security 事業本部 営業本部 Tel: 03-5360-3811 E-Mail: netsales@soliton.co.jp</p>
44	<p>メールセキュリティプライアンス : Cisco ESA 【ソリトンシステムズ】</p> <p>「Cisco ESA」は、オールインワンのメールセキュリティアプライアンスです。レピュテーション連携とスパムフィルタでの効率的なスパムメール対策、ウイルスメール対策、メール暗号化および情報漏えい対策等、包括的メールセキュリティを提供します。</p> <p>世界最大級の脅威情報サービス (Cisco SIO) と連携することで、未知の脅威にも対応可能です。また、システム全体の統計情報取得や、メールの送受信の詳細なログも簡単に取得できます。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/ironportc/</p> <p>◆お問い合わせ先◆</p> <p>株式会社ソリトンシステムズ IT Security 事業本部 営業本部 Tel: 03-5360-3811 E-Mail: netsales@soliton.co.jp</p>

・情報資産の重要度分類に基づいて、取扱可能範囲を指定したり、職位・職務、役割、雇用形態などの属性に基づいて、ID やアクセス権限を自動割り当てするなど、ID とアクセス権限の適正管理を実現します。

・発行した ID については、定期的なパスワード変更を強制してセキュリティを高めたり、複数システムのパスワードを1つに統合したり、パスワード忘れ時のリセット処理を自動化するなど、パスワードに関する様々な課題を解決します。

【製品情報詳細】

<http://www.soliton.co.jp/products/management/idmanager/index.html>

◆お問い合わせ先◆

株式会社ソリトンシステムズ

IT Security 事業本部 営業本部

Tel: 03-5360-3811

E-Mail: netsales@soliton.co.jp

※各対策ポイントに関する解説

No. 17 について

「人事異動」もしくは「プロジェクト発足等による利用者による申請」 どちらのトリガーにおいても組織階層責任者及び必要に応じて情報資産管理者の承認を経て、適切なアクセス権付与と剥奪が可能なワークフロー機能を提供。

No. 18 について

別途重要情報として区分された情報資産に対し、部署や役職もしくは情報資産個別にアクセス権設定ルールを定義でき、その設定されたルールに準じてアクセス権の付与&剥奪が可能。

No. 19 について

人事異動に伴う「新規登録・休職・復職・退職」をトリガーに、異動後の部署や役職に応じたアクセス権の自動付与&剥奪が可能。

No. 20: 人事異動や組織改訂などに合わせて、利用者 ID 及びアクセス権の付与ルールを変更することで、一斉に洗い替えする事が可能。洗い替え時には、一定期間、前権限の剥奪に関する猶予期間の設定も可能。

No. 22 について

社員やルールのマスターを共有する単位として「サイト」を複数保持することができ(いわゆるマルチテナント運用が可能)、個々の「サイト」において複数のサイト管理者を個人単位で任意複数の登録が可能。また複数のサイトを束ねる管理者としてシステム管理者を個

	<p>人単位で任意複数の登録が可能。</p> <p>No. 24 について</p> <p>上記 No. 22 と同じ内容で可能。</p> <p>No. 26 について</p> <p>上記 No. 22 で記載したサイト管理者、システム管理者、及び利用者は全員独自のログイン ID とパスワードで認証が要求される。</p> <p>No. 27 について</p> <p>利用者のパスワードは、単純な文字列を使用できないよう独自のパスワードポリシーによる運用が可能。また定期的なパスワード変更期限を設けて、ユーザーにメール通知によりパスワード変更を催促する運用が可能。</p>
46	<p>標的型サイバー攻撃から PC を防御するマルウェア対策ソフトウェア : Zerona 【ソリトンシステムズ】</p> <p>近年の高度なマルウェアによる、プログラムの脆弱性を狙うコード実行型攻撃を徹底ブロックします。新しい攻撃にも対策できるだけでなく、大規模環境の導入・運用に欠かせない管理機能が充実しています。InfoTrace PLUS、NetAttest BigData と併用することで、攻撃検知時の PC 操作までを洗い出すことが可能です。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/zerona/</p> <p>◆お問い合わせ先◆</p> <p>株式会社ソリトンシステムズ</p> <p>IT Security 事業本部 営業本部</p> <p>Tel: 03-5360-3811</p> <p>E-Mail: netsales@soliton.co.jp</p>
47	<p>統合ログ分析アプライアンス:NetAttest BigData 【ソリトンシステムズ】</p> <p>ログ分析の重要性が高まる中、汎用の分析ツールではログ分析が分からない、システムの導入・運用の敷居が高い、といった現状が指摘されています。「NetAttest BigData」は、ソリトン製品のログ分析を標準搭載。設置したその日からログ分析を実施できます。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/bigdata/</p> <p>◆お問い合わせ先◆</p> <p>株式会社ソリトンシステムズ</p>

	<p>IT Security 事業本部 営業本部</p> <p>Tel: 03-5360-3811</p> <p>E-Mail: netsales@soliton.co.jp</p>
48	<p>不正端末検知・遮断アプライアンス : NetAttest LAP 【ソリトンシステムズ】</p> <p>「NetAttest LAP」は、オールインワン認証アプライアンス NetAttest EPS、もしくは検疫+IPS 製品 CounterACT と連携し、ネットワークに接続されたデバイスの検知と、違反デバイスのネットワーク接続をブロックするアプライアンスです。 ネットワーク構成を変更することなく、全社的に、スマートデバイスを含めた持ち込みデバイス・違反デバイスの接続を検知し、ネットワーク利用をブロックできます。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/products/net_security/netattest/lap/index.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社ソリトンシステムズ</p> <p>IT Security 事業本部 営業本部</p> <p>Tel: 03-5360-3811</p> <p>E-Mail: netsales@soliton.co.jp</p>
49	<p>検疫ネットワーク認証アプライアンス : NetAttest Security Filter 【ソリトンシステムズ】</p> <p>NetAttest SecurityFilter (ネットアテスト セキュリティフィルター) は、ネットワークを利用するユーザーの認証と、ネットワークに接続する PC の検疫を行うアプライアンスです。ユーザーと PC 両方のネットワーク利用を制御することで、より安全なネットワーク環境を構築できます。</p> <p>また、L2 ゲートウェイなので、導入箇所を選びません。重要なサーバーファームの手前に設置して、サーバーへのアクセスを一括で制御することもできます。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/sf/</p> <p>◆お問い合わせ先◆</p> <p>株式会社ソリトンシステムズ</p> <p>IT Security 事業本部 営業本部</p> <p>Tel: 03-5360-3811</p> <p>E-Mail: netsales@soliton.co.jp</p>

50	<p>統合 PC セキュリティ管理ソフトウェア : InfoTrace PLUS 【ソリトンシステムズ】</p> <p>InfoTrace PLUS は、誰が、いつ、どの PC から、どのような操作を行ったかを徹底記録します。記録したログは暗号化され、改竄・削除防止措置により、情報漏洩対策だけでなく、PC の私的利用を抑止し業務の効率化にも効果を発揮します。</p> <p>操作ログの記録に加え、「認証」「検疫・資産管理」「ネットワークアクセスと PC 操作制御」「シングルサインオン」まで、組織の IT 運用に必要なセキュリティ対策をオールインワンパッケージで提供します。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/infotraceplus/</p> <p>◆お問い合わせ先◆</p> <p>株式会社ソリトンシステムズ</p> <p>IT Security 事業本部 営業本部</p> <p>Tel: 03-5360-3811</p> <p>E-mail : netsales@soliton.co.jp</p>
51	<p>IC カード認証ソリューション : SmartOn ID 【ソリトンシステムズ】</p> <p>SmartOn ID は、PC 利用時の「本人認証」に IC カードを追加し認証を強化、なりすましや PC 紛失・盗難時の不正利用を防止する PC セキュリティシステムです。</p> <p>社員証や入退室管理などで既に利用している IC カードを有効活用でき、仮想デスクトップやシンクライアントとの混在環境でも利用できます。</p> <p>また、私物 USB メモリやアプリケーションの利用制限やシングルサインオン機能も提供します。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/smarton/</p> <p>◆お問い合わせ先◆</p> <p>株式会社ソリトンシステムズ</p> <p>IT Security 事業本部 営業本部</p> <p>Tel: 03-5360-3811</p> <p>E-mail : netsales@soliton.co.jp</p>

52

セキュアファイル転送アプライアンス : FileZen 【ソリトンシステムズ】

FileZen は、大容量データや機密情報を簡単かつ安全に共有・転送できるファイル転送アプライアンスです。

ファイルの送付・受領を記録に加え、送付時に承認を必須とする運用や、送付したファイルを証跡として保管することができるため、USB メモリなど物理媒体での共有における紛失・盗難のリスクやコストを削減するだけでなく、情報漏洩対策としても効果的です。

【製品情報詳細】

<http://www.soliton.co.jp/filezen/>

◆お問い合わせ先◆

株式会社ソリトンシステムズ

IT Security 事業本部 営業本部

Tel: 03-5360-3811

E-mail : netsales@soliton.co.jp

○マルチ OS 対応セキュアアクセスソリューション : Soliton SecureBrowser /Soliton SecureGateway

「Soliton SecureBrowser(以下、SSB) / Soliton SecureGateway(以下、SSG)」は、強力なセキュリティ機能を備えたブラウザ(SSB)から、ゲートウェイ(SSG)を経由して、企業の社内システム・クラウドシステムを安全に利用するためのソリューションです。SSBは保護された空間で動作し、端末へのデータ保存や外部へのコピーも禁止されています。SSGへの接続認証では、ID・パスワードによる認証の他に、デジタル証明書による認証にも対応しています。SSBとSSG間は暗号化通信を行います。

【製品情報詳細】

<http://www.soliton.co.jp/ssb/>

◆お問い合わせ先◆

株式会社ソリトンシステムズ

IT Security 事業本部 営業本部

Tel: 03-5360-3811

E-Mail: netsales@soliton.co.jp

※各対策ポイントに関する解説

No. 42 について

対象システムの前にSSGを配置することで、認許可された利用者・端末しか接続できない環境を実現します。

No. 60 について

SSBとSSGの通信は暗号化され、組織ネットワークへのセキュアなアクセスを提供します。

54	<p>オールインワン認証アプライアンス : NetAttest EPS 【ソリトンシステムズ】</p> <p>「NetAttest EPS」は、RADIUS や CA 機能を搭載するオールインワン認証アプライアンスです。PC やスマートフォンがネットワークに接続する際、無線アクセスポイントや VPN ゲートウェイと連携し、利用者や端末が正規のものか否かを判断します。1 台で、固定パスワード認証、デジタル証明書認証、ワンタイムパスワード認証に対応できます。システムメンテナンス機能が豊富で、専門技術やコマンドの知識がなくても手軽に導入できるのが特長です。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/eps/</p> <p>◆お問い合わせ先◆</p> <p>株式会社ソリトンシステムズ IT Security 事業本部 営業本部 Tel: 03-5360-3811 E-Mail: netsales@soliton.co.jp</p> <p>※各対策ポイントに関する解説</p> <p>No. 42 について 認証スイッチ、無線アクセスポイント、VPN ゲートウェイ等の機器と連携し、利用者毎にアクセス権限を制御します。</p> <p>No. 44 について 認証スイッチ、無線アクセスポイント、VPN ゲートウェイ等の機器と連携し、未登録ユーザー及びデバイスのネットワーク接続を禁止します。</p> <p>No. 60 について 安全な VPN 環境の実現に必要な、認証システムを提供します。</p> <p>No. 61 について NetAttest EPS のオプション製品「NetAttest EPS-ap」により、遠隔からの情報消去(リモートワイプ)や端末ロック(リモートロック)を行います。</p> <p>No. 66 について 認証の結果(成否や実施日時など)はログに記録されます。</p>
55	<p>入退室管理 : セコム AX 【セコム】</p> <p>暗闇でも画像センサーが鮮明に侵入者の姿をキャッチし、異常信号と画像をセコムへ自動送信する監視システムです。画像センサーはマイクを内蔵しており、現場の状況をセコムが画像と音声で確認し、スピーカーから警告や威嚇することが可能です。犯行が確認できた場合は、セコムが警察に即時通報を行います。また、お客様が身の危険を感じた際に「非常ボタン」を押していただくと、画像と音声でセコムに送信されます。</p>

	<p>【製品情報詳細】</p> <p>http://www.secom.co.jp/business/security/office/ax.html</p> <p>◆お問い合わせ先◆</p> <p>セコム株式会社</p> <p>お問い合わせフォーム: http://www.secom.co.jp/inquiry/contact.html</p>
56	<p>入退室管理：セサモ TRⅡ 【セコム】</p> <p>厳格な出入管理を実現するシステムです。「いつ」「誰が」「どこに」入退室したかをパソコンに自動記録、アンチパスバックや入退室の滞在時間を制限など、さまざまな機能を使った出入管理が可能です。また、出入管理履歴を元に、在室者の有無をカウントし、無人になった場合は、自動的に警戒セットすることなどが可能です。</p> <p>【製品情報詳細】</p> <p>http://www.secom.co.jp/business/security/goods/s_tr2.html</p> <p>◆お問い合わせ先◆</p> <p>セコム株式会社</p> <p>お問い合わせフォーム: http://www.secom.co.jp/inquiry/contact.html</p>
57	<p>入退室管理：セサモ IDs 【セコム】</p> <p>指紋認証による厳正な入退室管理システムです。厳格に入室者を限定したい重要施設や、鍵やカードを持ち帰らせたくない場合に最適です。また、セコムの入退室管理システムとの組み合わせや、セコムの各種オンラインセキュリティシステム、電気錠との接続も可能です。</p> <p>【製品情報詳細】</p> <p>http://www.secom.co.jp/business/security/goods/s_ids.html</p> <p>◆お問い合わせ先◆</p> <p>セコム株式会社</p> <p>お問い合わせフォーム: http://www.secom.co.jp/inquiry/contact.html</p>
58	<p>HVR(監視カメラ)システム【セコム】</p> <p>「カメラの位置や向きが変えられた」「カメラのレンズが覆い隠された」「ケーブルや電源コードが切断された」「撮影するのに十分な明るさがなくなった」などの異常を検知する機能を持った監視カメラシステムです。カメラとしての基本機能にも優れており、照明変動や、明暗の差が大きい場所も監視できることに加え、柔軟なシステムアップも可能となっています。</p>

	<p>【製品情報詳細】</p> <p>http://www.secom.co.jp/business/security/goods/camera_expand.html</p> <p>◆お問い合わせ先◆</p> <p>セコム株式会社</p> <p>お問い合わせフォーム: http://www.secom.co.jp/inquiry/contact.html</p>
59	<p>タグ検知：不正持出し監視システム【セコム】</p> <p>管理対象物に特殊なタグを取り付け、出入口に設置するゲートのセンサーと連動して動作するシステムです。タグの機能を消去せず、あるいはタグを取り付けたままゲートを通過するとシステムが検知してお知らせします。また、持ち出し履歴管理や持ち出し状況の画像記録など、各事業所のニーズにあった多彩なシステム構築も可能です。</p> <p>【製品情報詳細】</p> <p>http://www.secom.co.jp/business/security/goods/kanshi.html</p> <p>◆お問い合わせ先◆</p> <p>セコム株式会社</p> <p>お問い合わせフォーム: http://www.secom.co.jp/inquiry/contact.html</p>
60	<p>金庫：ピタゴラス【セコム】</p> <p>優れた防盜性、耐久性、耐火性を持つセコムオリジナルの金庫です。セコムのオンラインセキュリティシステムと連携することで、こじ開けなどによる異常発生時に、セコムが現場へ急行することなど可能です。サイズ、形状、錠のタイプが異なる豊富な種類をそろえており、錠のタイプや金庫の色を変更したい場合や設置スペースに制約がある場合も、オーダーメイドで対応しています。</p> <p>【製品情報詳細】</p> <p>http://www.secom.co.jp/business/security/goods/kinko.html</p> <p>◆お問い合わせ先◆</p> <p>セコム株式会社</p> <p>お問い合わせフォーム: http://www.secom.co.jp/inquiry/contact.html</p>

61	<p>情報漏洩対策サービス：セコム PC セーフティサービス 【セコムトラストシステムズ】</p> <p>セコム PC セーフティサービスは、インターネット経由で操作ログを収集し、管理者は専用のホームページから情報漏洩対策、IT 資産管理、業務分析の一元管理を行うことができます。IT 資産管理の機能を利用すると、事前に登録された不適切なソフトウェアが PC に導入された場合、管理者に通知されます。</p> <p>【サービス情報詳細】 http://www.secomtrust.net/service/endpoint/pcsafe.html</p> <p>◆お問い合わせ先◆ セコムトラストシステムズ株式会社 Tel : 0120-39-0756</p>
62	<p>セキュリティサービス/マネージドサービス：URL フィルタサービス 【セコムトラストシステムズ】</p> <p>URL フィルタサービスは、インターネットゲートウェイに設置した機器によって、お客様が指定した URL フィルタに基づき、インターネットのアクセスを制限します。フィルタへの指定によって、SNS やアップローダー、掲示板へのアクセスを制限することができます。</p> <p>【サービス情報詳細】 http://www.secomtrust.net/service/datacenter/service/managed_url_filtering.html</p> <p>◆お問い合わせ先◆ セコムトラストシステムズ株式会社 Tel : 0120-39-0756</p>
63	<p>セキュリティサービス：ウイルス対策支援サービス 【セコムトラストシステムズ】</p> <p>セコム監視センターでウイルス感染を 24 時間 365 日監視します。ウイルス感染を検知した場合、セコム監視センターから端末利用者に直接ご連絡し、初動対応を支援して、必要に応じて駆除作業を現地で行うサービスです。</p> <p>【サービス情報詳細】 http://www.secomtrust.net/service/cyber-attack/virus_taiou.html</p> <p>◆お問い合わせ先◆ セコムトラストシステムズ株式会社 Tel : 0120-39-0756</p>

64	<p>セキュリティサービス：データ一時保管サービス 【セコムトラストシステムズ】</p> <p>セコムデータ一時保管サービスは、電子証明書とID/パスワードの組合せにより、送信側、受信側の確実な認証と暗号通信やウイルスチェックなど、万全なセキュリティ対策の標準装備により、なりすまし、盗聴、ウイルス感染、フィッシング詐欺などの不安を抱えることなく、安全・確実・迅速なデータの受渡しが行えます。</p> <p>【サービス情報詳細】</p> <p>http://www.secomtrust.net/service/ekakusin/ichijihokan.html</p> <p>◆お問い合わせ先◆</p> <p>セコムトラストシステムズ株式会社</p> <p>Tel : 0120-39-0756</p>
65	<p>セコム InternetVPN サービス 【セコムトラストシステムズ】</p> <p>セコム InternetVPN サービスは、本社・支社を結ぶネットワーク、もしくはモバイルからのセキュアなアクセスを、既にご契約されているネットワーク環境を変更することなく、容易に構築できます。</p> <p>【サービス情報詳細】</p> <p>http://www.secomtrust.net/service/s_network/internet.html</p> <p>◆お問い合わせ先◆</p> <p>セコムトラストシステムズ株式会社</p> <p>Tel : 0120-39-0756</p>
66	<p>情報漏洩対策サービス：セコム PC セーフティサービス 【セコムトラストシステムズ】</p> <p>セコムPCセーフティサービスは、インターネット経由で操作ログを収集し、管理者は専用のホームページから情報漏えい対策、IT資産管理、業務分析の一元管理を行うことができます。また、利用者がインターネットを通じてプログラムをダウンロードし導入するため、管理者に導入と管理の手間がかかりません。</p> <p>【サービス情報詳細】</p> <p>http://www.secomtrust.net/service/endpoint/pcsafe.html</p> <p>◆お問い合わせ先◆</p> <p>セコムトラストシステムズ株式会社</p> <p>Tel : 0120-39-0756</p>

67	<p>セコムプロフェッショナルサポート：緊急事態サポートサービス（法人様向け）【セコムトラストシステムズ】</p> <p>緊急事態サポートサービスは、ウイルスや不正アクセスの被害を受けた企業に、豊富な経験を持つセキュリティのプロが駆けつけ、初動対応と復旧支援を行います。セキュリティのプロだからできるスピーディーな対応により、お客様の早期業務再開をサポートいたします。</p> <p>【サービス情報詳細】</p> <p>http://www.secomtrust.net/service/prosupport/kinkyujitai.html</p> <p>◆お問い合わせ先◆</p> <p>セコムトラストシステムズ株式会社</p> <p>Tel：0120-39-0756</p>
68	<p>エンプロイモチベーションサーベイ【リンクアンドモチベーション】</p> <p>企業経営における組織状態のモニタリングをすることを目的として、従業員の声を収集することで組織における戦略や方針の徹底度合い及び組織を構成する縦・横の関係性状態及び従業員の意識を可視化します。</p> <p>※尚、本サービスは内部不正に焦点を当てているわけではなく、組織のコミュニケーション状態（方針の浸透、縦・横のつながり）を明確にするためのツールです。</p> <p>【サービス詳細】</p> <p>http://www.lmi.ne.jp/services/morivation_management.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社リンクアンドモチベーション</p> <p>モチベーションマネジメントカンパニー</p> <p>担当：高橋</p> <p>Tel：03-3538-6715</p> <p>E-Mail：lm_jimukyoku@lmi.ne.jp</p>
69	<p>コンプライアンス診断【リンクアンドモチベーション】</p> <p>企業経営における企業存続に向けた目標達成の実現に向けて守るべきルールや決まりごと、果たすべき責任に対して「どのくらい理解が進んでいるか」「どのように実践できているか」を可視化します。</p> <p>※尚、本サービスは内部不正だけに焦点を当てているわけではなく、組織のコンプライアンス遵守の状態を見える化するためのツールです。</p> <p>◆お問い合わせ先◆</p>

	<p>株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋 Tel：03-3538-6715 E-Mail：lm_jimukyoku@lmi.ne.jp</p>
70	<p>経営層向けマネジメント診断【リンクアンドモチベーション】</p> <p>方針伝達や内部統制も含め経営者として果たすべき役割がどの程度発揮されているのか、直接マネジメントを受ける下位者からのアンケートを通じて発揮度合いを可視化します。</p> <p>※尚、本サービスは内部不正だけに焦点を当てているわけではなく、組織のコンプライアンス遵守の状態を見える化するためのツールです。</p> <p>◆お問い合わせ先◆ 株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋 Tel：03-3538-6715 E-Mail：lm_jimukyoku@lmi.ne.jp</p>
71	<p>人材育成コンサルティング【リンクアンドモチベーション】</p> <p>企業の方針や戦略、目指す姿の実現に向けて、階層別・機能別の役割を設定するサポート、及びその役割遂行に向けた行動変容を実現するための研修コンテンツ設計、研修実施サポート（講師アサイン、テキスト準備など）や事前事後のフォローアップ（事前課題、事後アンケートなど）を行います。</p> <p>◆お問い合わせ先◆ 株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋 Tel：03-3538-6715 E-Mail：lm_jimukyoku@lmi.ne.jp</p>
72	<p>人事制度コンサルティング【リンクアンドモチベーション】</p> <p>人事制度を会社の価値観や方針を社員に伝え、社員がそれを体現するためのコミュニケーションツールと置き、等級制度、評価制度、報酬制度などを透明性が感じられ、個々人の納得感高く運用できるような、また個々人の自発的な行動が徹底できるような制度設計をサポートします。</p>

	<p>【サービス詳細】</p> <p>http://www.lmi.ne.jp/services/morivation_management.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋 Tel：03-3538-6715 E-Mail：lm_jimukyoku@lmi.ne.jp</p>
73	<p>評価者研修【リンクアンドモチベーション】</p> <p>企業の方針や戦略、目指す姿の実現に向けたコミュニケーションツールである人事制度を通じて個人に求める行動を徹底するための、評価者に対する目標設定研修、評価者研修及び日常業務におけるフィードバックの強化を目的とした研修の企画設計及び研修実際サポート（講師アサイン、テキスト準備など）を行います。</p> <p>【サービス詳細】</p> <p>http://www.lmi.ne.jp/services/morivation_management.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋 Tel：03-3538-6715 E-Mail：lm_jimukyoku@lmi.ne.jp</p>
74	<p>職場診断【リンクアンドモチベーション】</p> <p>職場のチームワーク向上に向けて職場を構成する個人とのつながり度合い、認識の違い、関係の質を調べることにより、現状の職場の状況及び問題点、課題を明確にします。</p> <p>※尚、本サービスは内部不正に焦点を当てているわけではなく、最小組織である職場のコミュニケーション状態、関係性の質を明確にするためのツールです。</p> <p>◆お問い合わせ先◆</p> <p>株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋</p>

Tel : 03-3538-6715

E-Mail : lm_jimukyoku@lmi.ne.jp

75	<p>関係性マネジメント【リンクアンドモチベーション】</p> <p>システム・コーチングやワークショップを通じて、職場を構成する個々人の認識のズレをすり合わせることで、関係の質の向上、つながりの強化を行う。</p> <p>※尚、本サービスは内部不正に焦点を当てているわけではなく、職場間のコミュニケーション状態、関係性を明確にするためのツールです。</p> <p>◆お問い合わせ先◆ 株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋 Tel：03-3538-6716 E-Mail：lm_jimukyoku@lmi.ne.jp</p>
76	<p>マネジメント診断【リンクアンドモチベーション】</p> <p>管理者とメンバーとの関係性構築に向けて、お互いの関係において何を求めている、何が満たされているのか、どのような認識のズレがあり、どのような観点で信頼関係が構築できていないのか、管理者とメンバー間の関係性を可視化します。</p> <p>※尚、本サービスは内部不正に焦点を当てているわけではなく、管理者とメンバー間のコミュニケーション状態、関係性を明確にするためのツールです。</p> <p>◆お問い合わせ先◆ 株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋 Tel：03-3538-6715 E-Mail：lm_jimukyoku@lmi.ne.jp</p>
77	<p>ヒューマンスキル他者認知サーベイ【リンクアンドモチベーション】</p> <p>「対課題力」「対人力」「対自分力」などのヒューマンスキルが周囲から診ると他者との関係においてどのように発揮できているか、また自身の認識と比較するとどのようなギャップがあるのかを明確にします。</p> <p>※尚、本サービスは内部不正のみに焦点を当てているわけではなく、管理者がメンバーの周囲への能力発揮状況を見極めるためのツールです。</p> <p>◆お問い合わせ先◆ 株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋</p>

	<p>Tel : 03-3538-6715</p> <p>E-Mail : lm_jimukyoku@lmi.ne.jp</p>
78	<p>マネジメント力向上研修【リンクアンドモチベーション】</p> <p>メンバーが担う業務に対する『メンバーのタスク遂行難易度』のメンバー・マネジャー間における認識の違いによって、マネジャーはメンバーへの介入方法を変えるべきであることを理解するとともに、互いの認識状況に合わせたマネジメント手法を理解・習得します。</p> <p>※尚、本サービスは内部不正のみに焦点を当てているわけではなく、管理者のメンバーに対するタスク難易度とメンバーの認識に合わせたマネジメント方法を理解させる研修です。</p> <p>◆お問い合わせ先◆</p> <p>株式会社リンクアンドモチベーション モチベーションマネジメントカンパニー 担当：高橋</p> <p>Tel : 03-3538-6715</p> <p>E-Mail : lm_jimukyoku@lmi.ne.jp</p>
79	<p>NetEvidence【NEC(オーク情報システム)】</p> <p>○ネットワークフォレンジックサーバ：NetEvidence Ax</p> <p>ネットワーク経由で交わされる外部との通信データをパケットレベルで記録し、 「いつ」「どこで」「誰が」「どのような情報を」「どのような手段で」 「どこに漏えいしたか」をすばやく特定し、証拠として保全することができます。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/datanet/netevidence/index.html</p> <p>◆お問い合わせ先◆</p> <p>http://jpn.nec.com/datanet/netevidence/index.html</p> <p>(下方の「資料請求・お問い合わせ」バナーより)</p>

80	UNIVERGE SecureBranch VM 【NEC】
	<p>○VPN 仮想プライアンス : UNIVERGE SecureBranch VM イン트라ネットをそのまま外出先へ広げる、 新しい発想の VPN 仮想プライアンスです。 社内で確立された安全性と利便性を外部へ広げていくことで、 強固なセキュリティと自由なワークスタイルを両立できます。</p> <p>【製品情報詳細】 http://jpn.nec.com/univerge/securebranch_vm/</p> <p>◆お問い合わせ先◆ http://jpn.nec.com/univerge/securebranch_vm/ (下方の「資料請求・お問い合わせ」バナーより)</p>
81	<p>ASA5500 シリーズ 【NEC(CiscoSystems)】</p> <p>○VPN ゲートウェイ : ASA-5500 シリーズ [NEC(CiscoSystems)] 最新のセキュリティサービスを集約する適応型プライアンス。 IPsec、SSL、L2TP/IPsec の 3 種類の VPN により様々なニーズに対応。 また Cisco AnyConnect はアプリケーションストアで配信されているため 入手が容易で、簡単にリモートアクセスを可能にします。</p> <p>【製品情報詳細】 http://jpn.nec.com/datanet/cisco/product/#security</p> <p>◆お問い合わせ先◆ http://jpn.nec.com/datanet/cisco/product/#security (下方の「お問い合わせ」バナーより)</p>

82	PA シリーズ 【NEC(Palo Alto Networks)】
	<p>○次世代ファイアウォール：PA シリーズ</p> <p>アプリケーションを識別し、それに基づいてアプリケーションベースのアクセス制御を行うことができます。</p> <p>それにより、業務に関係のない通信の遮断や、ファイル交換ソフトの使用などによるセキュリティリスクの回避を実現することができます。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/datanet/paloalto/</p> <p>◆お問い合わせ先◆</p> <p>http://jpn.nec.com/datanet/paloalto/</p> <p>(下方の「お問い合わせ」バナーより)</p>
83	<p>MAG シリーズ 【NEC(Juniper Netowrks)】</p> <p>○VPN アプライアンス：MAG シリーズ</p> <p>リモート環境、モバイル環境の正規ユーザー向けに共通のクライアントで高信頼の SSL VPN 接続、ネットワーク・アクセス・コントロール、アプリケーション・アクセラレーションの機能を提供します。</p> <p>【製品情報詳細】</p> <p>http://www.juniper.net/jp/jp/products-services/security/mag-series/</p> <p>(メーカーサイト)</p> <p>◆お問い合わせ先◆</p> <p>日本電気株式会社 企業ネットワーク事業部</p> <p>E-Mail : nwsec@kisl.jp.nec.com</p>

84	<p>ProxySG 【NEC(Blue Coat Systems)】</p> <p>○セキュア Web ゲートウェイ : ProxySG</p> <p>統合セキュリティ・ソリューションとして、すべての Web トラフィックを制御できます。ユーザー認証、Web フィルタリング、データ損失防止、SSL 暗号化トラフィックの調査と検証、コンテンツ・キャッシュ、帯域幅管理、ストリーム・スプリットなどの堅牢な機能を提供します。</p> <p>【製品情報詳細】</p> <p>http://www.bluecoat.com/ja/products/proxysg</p> <p>(メーカーサイト)</p> <p>◆お問い合わせ先◆</p> <p>日本電気株式会社 企業ネットワーク事業部</p> <p>E-Mail : nwsec@kisl.jp.nec.com</p>
85	<p>FortiGate 【NEC(Fortinet)】</p> <p>○統合脅威管理アプライアンス (UTM) : FortiGate</p> <p>豊富な機能と高い性能を実現しながら、コストパフォーマンスに優れた UTM。ファイアウォール、ウイルス/スパイウェア対策、スパム対策、SSL-VPN、IPsec-VPN、アプリケーション可視化と制御、Web フィルタリング等のセキュリティ機能に対応し、操作性に優れた日本語 GUI で導入も管理も容易です。</p> <p>【製品情報詳細】</p> <p>http://www.fortinet.co.jp/products/fortigate/</p> <p>(メーカーサイト)</p> <p>◆お問い合わせ先◆</p> <p>日本電気株式会社 企業ネットワーク事業部</p> <p>E-Mail : nwsec@kisl.jp.nec.com</p>

86	<p>i-FILTER 【NEC(デジタルアーツ)】</p> <p>○Web フィルタリングソフト : i-FILTER</p> <p>通常の URL フィルタリング機能に加え、クライアントからの情報発信も含めたアクセスコントロールを実現し。</p> <p>プロキシサーバとして動作し、詳細な設定が可能。利用環境の規模を問わず、高いパフォーマンスを発揮します。</p> <p>【製品情報詳細】</p> <p>http://www.daj.jp/bs/i-filter/</p> <p>(メーカーサイト)</p> <p>◆お問い合わせ先◆</p> <p>日本電気株式会社 企業ネットワーク事業部</p> <p>E-Mail : nwsec@kisl.jp.nec.com</p>
87	<p>NetScaler MPX 【NEC(CitrixSystems)】</p> <p>○Web アプリケーションデリバリーコントローラ : NetScaler MPX</p> <p>アプライアンスに統合された最先端の SSL 暗号化技術により、毎秒数十万 SSL トランザクション(TPS)をサポートでき、毎秒数ギガビットレベルの安全な Web ページの配信を支援します。</p> <p>【製品情報詳細】</p> <p>http://www.citrix.co.jp/products/netscaler-application-delivery-controller/index.html</p> <p>(メーカーサイト)</p> <p>◆お問い合わせ先◆</p> <p>日本電気株式会社 企業ネットワーク事業部</p> <p>E-Mail : nwsec@kisl.jp.nec.com</p>

88	<p>CounterACT 【NEC(ソリトンシステムズ)】</p> <p>○統合セキュリティプライアンス : CounterACT</p> <p>「エージェントレス検疫」と「ゼロデイ攻撃対応 IPS(不正アクセス防御システム)」の両方を実装した、統合セキュリティプライアンスです。</p> <p>ネットワーク上の端末のあらゆる情報を把握できる検疫機能で持込 PC の検知、排除、セキュリティホールを発見・修正。ウイルス対策ソフト等で対応できないゼロデイアタックなど未知の攻撃は、IPS 機能で防御します。</p> <p>【製品情報詳細】</p> <p>http://www.soliton.co.jp/products/net_security/counteract/index.html</p> <p>(メーカーサイト)</p> <p>◆お問い合わせ先◆</p> <p>日本電気株式会社 企業ネットワーク事業部</p> <p>E-Mail : nwsec@kisl.jp.nec.com</p>
89	<p>UNIVERGE フィジカルセキュリティソリューション 【NEC】</p> <p>NEC UNIVERGE フィジカルセキュリティソリューションは、IC カードによる入退管理を各種システムと連携し、強固なセキュリティと管理の効率化を実現します。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/univerge/solution/index6.html</p> <p>◆お問い合わせ先◆</p> <p>UNIVERGE インフォメーションセンター</p> <p>Tel:0120-75-7400(平日 9:00-12:00、13:00-17:00)</p> <p>E-mail: nivergeinfo@usc.jp.nec.com</p>
90	<p>カスタムメイド研修 【NEC ラーニング】</p> <p>お客様のご要望に合わせてカリキュラムをカスタマイズし、ご提供する研修です。以下のような方にお勧めです。</p> <ul style="list-style-type: none"> ・セキュリティの必要性に対する意識を高めたい ・一般的なセキュリティの注意点を周知したい ・社内で作成したセキュリティポリシーのポイントを周知したい 等 <p>【製品情報詳細】</p> <p>http://www.neclearning.jp/training/custom.html</p>

	<p>◆お問い合わせ先◆</p> <p>http://www.neclearning.jp/contact/index.html</p>
91	<p>研修サービス【NECラーニング】</p> <p>各種研修を取り揃えています。ご要望される研修を選択してください。</p> <ul style="list-style-type: none"> ・ビジネススキル ・IT研修（ITスキル、利用者向けセキュリティ、管理者向けセキュリティ等） ・新入社員研修等 <p>【製品情報詳細】</p> <p>http://www.neclearning.jp/training/index.html</p> <p>◆お問い合わせ先◆</p> <p>http://www.neclearning.jp/contact/index.html</p>
92	<p>情報セキュリティ整備計画策定サービス【NEC】</p> <p>本コンサルティングサービスは情報ではなくITインフラに視点を置くことにより情報セキュリティ整備計画及びセキュリティポリシーの実現性、実効性を高めます。お客様のITインフラと制度成熟度を5段階に数値化して分析を行い、具体的な目標値を定めた上で、実現技術を想定した具体的な施策（プロシージャ）に落としこんでいきます。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/security/im/ps.html</p> <p>◆お問い合わせ先◆</p> <p>http://jpn.nec.com/security/im/ps.html</p> <p>（下方の「資料請求・お問い合わせ」バナーより）</p>
93	<p>InfoCage FileShell【NEC】</p> <p>InfoCage FileShellは、デジタル著作権管理（DRM:Digital Rights Management）により、ファイルに対する認証とアクセス権を一元管理し、アプリケーションに依存せず顧客情報や設計情報などの重要情報を守ります。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/infocage/fileshell/</p> <p>◆お問い合わせ先◆</p>

	<p>NEC プラットフォームビジネス本部</p> <p>http://jpn.nec.com/infocage/contact.html</p>
94	<p>InfoCage PC セキュリティ【NEC】</p> <p>InfoCage PC セキュリティ」は、クライアント総合対策製品で、ユーザ認証、HDD/ファイルの暗号化、プログラムの起動停止/外部メディアへの書き込み制御、周辺機器の利用制限などが可能です。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/infocage/pc_security/</p> <p>◆お問い合わせ先◆</p> <p>NEC プラットフォームビジネス本部</p> <p>http://jpn.nec.com/infocage/contact.html</p>
95	<p>InfoCage ファイル暗号【NEC】</p> <p>InfoCage ファイル暗号は、特別なハードウェアを必要とせず、暗号アルゴリズムでファイル単位で暗号化を行い情報漏えい対策を支援します。パスワード暗号では、パスワードのミス可能回数や期限の設定が可能。</p> <p>【製品情報詳細】</p> <p>http://www.nec.co.jp/cced/infocage/file_a/</p> <p>◆お問い合わせ先◆</p> <p>NEC プラットフォームビジネス本部</p> <p>http://jpn.nec.com/infocage/contact.html</p>
96	<p>InfoCage データ消去【NEC】</p> <p>InfoCage データ消去は、PC 内臓のハードディスク内のデータを完全消去し、データ流出を防止します。</p> <p>【製品情報詳細】</p> <p>http://www.nec.co.jp/cced/infocage/erase/</p> <p>◆お問い合わせ先◆</p> <p>NEC プラットフォームビジネス本部</p> <p>http://jpn.nec.com/infocage/contact.html</p>
97	<p>ALogConVerter【NEC(網屋)】</p>

ユーザーの行動記録をサーバから取得するタイプのアクセスログ監査ツールです。複雑な生ログを解析し、実際にユーザーが行った操作パターンに分析変換することで、「いつ誰がどのような操作を行ったのか」を把握する事ができます。ログの収集対象は Windows、Linux、DB (Oracle、SQLServer)、NAS サーバ (EMC、NetApp、Isilon) です。アクセスログ管理市場でシェア 7 年連続 No1 製品です。

【製品情報詳細】

<http://jpn.nec.com/alog/cv/index.html>

◆お問い合わせ先◆

<http://jpn.nec.com/alog/cv/index.html>

(下方の「お問い合わせ」バナーより)

98 Web フィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】

InterSafeWebFilter は、SNS や掲示板に対して URL フィルタリングにより、アクセスを制限することが可能です。また、POST 行為に対して制限をかけることも可能で、アクセス閲覧は許可するが、書き込みのみを規制するといった運用をすることもできます。

また POST ログから書き込み内容やアップロードファイルを復元し、確認することもできます。日時、利用者 (アカウント)、操作端末 (IP アドレス)、操作内容 (アクセス先 URL)、書き込み内容 (POST リクエスト) 等の情報をアクセスログとして記録します。また、ログ分析ツールも同梱しており、組織全体の利用状況から個々のユーザの利用状況まで、WEB の利用状況を様々な角度から分析することが可能です。

【製品情報詳細】

<http://www.nec.co.jp/middle/InterSafe/>

◆お問い合わせ先◆

<http://www.nec.co.jp/middle/InterSafe/>

(下方の「資料請求・お問い合わせ」バナーより)

※各対策ポイントに関する解説

No. 66、No. 67、No. 68、No. 70、No. 71、No. 104、No. 105、No. 106、No. 111、No. 112、No. 118
について

日時、利用者 (アカウント)、操作端末 (IP アドレス)、操作内容 (アクセス先 URL)、書き込み内容 (POST リクエスト) 等の情報をアクセスログとして記録します。また、ログ分析ツールも同梱しており、組織全体の利用状況から個々のユーザの利用状況まで、WEB の利用

状況を様々な角度から分析することが可能です。

99	<p>InfoTrace PLUS 【NEC(ソリトンシステムズ)】</p> <p>InfoTracePLUS では、PC 上でのファイル操作、印刷、メール送信、アプリケーションの動作等のログを取得することが可能です。取得したログは条件を絞り込んでオンデマンド検索やスケジュール検索をすることができ、誰がいつどのような行為を行ったのかを追跡できます。</p> <p>ログを保存する期間も設定することができ、また、ログの内容は暗号化されます。</p> <p>注意すべき操作が行われた場合に、使用者に警告したり管理者に通報したりすることが可能です。</p> <p>【製品情報詳細】</p> <p>http://www.nec.co.jp/cced/InfoTrace/</p> <p>◆お問い合わせ先◆</p> <p>http://www.nec.co.jp/cced/InfoTrace/</p> <p>(下方の「資料請求・お問い合わせ」バナーより)</p>
100	<p>GUARDIANWALL 【NEC(キヤノン IT ソリューションズ)】</p> <p>メール保存機能によって、外部に送出される電子メールを全て保存、メール監視機能によって内容をチェックし配送の保留、削除、警告等のアクションが可能。電子メールからの機密情報漏えいを効果的に防止できます。</p> <p>【製品情報詳細】</p> <p>http://www.nec.co.jp/cced/GUARDIANWALL/</p> <p>◆お問い合わせ先◆</p> <p>http://www.nec.co.jp/cced/GUARDIANWALL/</p> <p>(下方の「資料請求・お問い合わせ」バナーより)</p>
101	<p>AddPoint/MailWallServer 【NEC(キヤノン IT ソリューションズ)】</p> <p>メール保存機能によって、外部に送出される電子メールを全て保存、メール監視機能によって内容をチェックし配送の保留、削除、警告等のアクションが可能。電子メールからの機密情報漏えいを効果的に防止できます。</p> <p>【製品情報詳細】</p> <p>http://www.nec.co.jp/soft/addpoint/mailwallserver/index.html</p> <p>◆お問い合わせ先◆</p> <p>http://www.nec.co.jp/soft/addpoint/mailwallserver/index.html</p> <p>(下方の「資料請求・お問い合わせ」バナーより)</p>

102	<p>AddPoint/SA 【NEC(キヤノン IT ソリューションズ)】</p> <p>送信するメールを自動的に暗号化し、電子メールの送信経路における盗聴を防止することで、電子メールからの機密情報漏えいを防ぎます。</p> <p>【製品情報詳細】</p> <p>http://www.nec.co.jp/soft/addpoint/sa/index.html</p> <p>◆お問い合わせ先◆</p> <p>http://www.nec.co.jp/soft/addpoint/sa/index.html</p> <p>(下方の「資料請求・お問い合わせ」バナーより)</p>
103	<p>ProofPoint 【NEC(Proofpoint)】</p> <p>外部から送信されてくるメールに対してはスパム対策・ウイルス対策・標的型攻撃メール対策で防御し、内部から送信するメールに対してはフィルタリング・誤送信防止・暗号化により情報漏えいトラブルを防止します。</p> <p>【製品情報詳細】</p> <p>http://www.nec.co.jp/soft/proofpoint/</p> <p>◆お問い合わせ先◆</p> <p>http://www.nec.co.jp/soft/proofpoint/</p> <p>(下方の「お問い合わせ」バナーより)</p>
104	<p>SECUREMASTER 【NEC】</p> <p>人事連携機能により、常に最新の状態で利用者 ID とアクセス権を割り当て管理することができ、ID の棚卸機能により、長く使用されていない ID を提示することができます。パスワードポリシー機能により定期的にパスワードを変更させることを義務付ける運用も可能です。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/websam/securemaster/</p> <p>◆お問い合わせ先◆</p> <p>http://jpn.nec.com/websam/contact.html</p>

105	<p>InfoCage 不正接続防止【NEC】</p> <p>○不正 PC 接続防止ソフトウェア「InfoCage 不正接続防止」</p> <p>「InfoCage 不正接続防止」は社内ネットワークに接続された不正な機器（PC、スマートフォンなど）を検知・遮断し、ウイルス感染や情報漏えいリスクを低減する製品です。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/infocage/prevention/</p> <p>◆お問い合わせ先◆</p> <p>NEC プラットフォームビジネス本部</p> <p>http://jpn.nec.com/infocage/contact.html</p>
106	<p>InfoCage PC 検疫【NEC】</p> <p>○ 検疫ソフトウェア「InfoCage PC 検疫」</p> <p>「InfoCage PC 検疫」は、セキュリティ対策が不十分な PC を基幹ネットワークに接続させずに隔離し、ウイルス感染などの危険性から守ります。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/infocage/pc_quarantine/</p> <p>◆お問い合わせ先◆</p> <p>NEC プラットフォームビジネス本部</p> <p>http://jpn.nec.com/infocage/contact.html</p>
107	<p>Check Point Endpoint Security Full Disk Encryption【NEC(Check Point)】</p> <p>○ ハードディスク暗号化「Check Point Endpoint Security Full Disk Encryption」</p> <p>「Check Point Endpoint Security Full Disk Encryption」はハードディスク全体を暗号化し、PC の置き忘れや盗難などによる情報漏えいを確実に防止します。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/eps/</p> <p>◆お問い合わせ先◆</p> <p>NEC プラットフォームビジネス本部</p> <p>http://jpn.nec.com/infocage/contact.html</p>

108	<p>InfoCage セキュリティリスク管理【NEC】</p> <p>緊急パッチの公開、社内ポリシー変更、新規 PC の接続など日々変化する 社内のセキュリティレベルを可視化。</p> <p>ネットワーク内にある PC のセキュリティ対策状況を把握し、効率的にセキュリティレベルを維持します。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/infocage/srm/</p> <p>◆お問い合わせ先◆</p> <p>NEC プラットフォームビジネス本部</p> <p>http://jpn.nec.com/infocage/contact.html</p>
109	<p>WebSAM AssetSuite【NEC】</p> <p>企業内の IT 機器やソフトウェアのほか、什器や備品、利用者や契約などの資産情報を関連付けて一元管理。コンプライアンス徹底のサポートと運用負担軽減を実現します。</p> <p>情報機器の紛失等を発見できるようにするために、台帳で設置場所や使用者を管理し、定期的に棚卸（資産の有無の確認）の実施を支援します。</p> <p>【製品情報詳細】</p> <p>http://jpn.nec.com/websam/assetsuite/</p> <p>◆お問い合わせ先◆</p> <p>http://jpn.nec.com/websam/contact.html</p>
110	<p>Cyber-Ark PIM Enterprise Suite【ディアイティ】</p> <p>○特権 ID 管理システム「Cyber-Ark PIM Enterprise Suite」</p> <p>お客様組織内に PDCA を構築し維持するための支援を行います。ISO 27001 をベースにした調査表、記録様式、ひな形文書を用いて効率良く作業が行えます。</p> <p>【製品情報詳細】</p> <p>http://www.dit.co.jp/products/cyber-ark/index.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社ディアイティ ネットワークセキュリティ事業部</p> <p>Tel: 03-5634-7651</p> <p>E-Mail: info@dit.co.jp</p>

111	<p>McAfee Web Gateway (Webwasher) 【ディアイティ】</p> <p>○キャッシュ統合型セキュリティプライアンス「McAfee Web Gateway (Webwasher)」 Web2.0の複雑化した脅威を防御するために、一台の筐体にURLフィルタ、アンチマルウェア、アンチウイルス、SSLスキャナ、キャッシュプロキシサーバなどの機能を統合し、インバウンド・アウトバウンド双方の脅威から情報資産を保護するゲートウェイ防御です。</p> <p>【製品情報詳細】 http://www.dit.co.jp/products/mcafee_webgateway/index.html</p> <p>◆お問い合わせ先◆ 株式会社ディアイティ ネットワークセキュリティ事業部 Tel: 03-5634-7651 E-Mail: info@dit.co.jp</p>
112	<p>Tectia シリーズ 【ディアイティ】</p> <p>○セキュリティ通信ソリューション「Tectia シリーズ」 商用SSHをベースにしたエンドツーエンドの通信セキュリティを実現します。運用と管理の一元管理、公開秘密鍵のライフサイクル管理、管理者アクセスの監査証跡取得等の管理機能を提供します。</p> <p>【製品情報詳細】 http://www.dit.co.jp/products/ssh_tectia_series/index.html</p> <p>◆お問い合わせ先◆ 株式会社ディアイティ ネットワークソリューション事業部 Tel: 03-5634-7651 E-Mail: info@dit.co.jp</p>
113	<p>Log Audit Tracker for Ops Manager 【ディアイティ】</p> <p>○SCOM用クライアント監視・監査ソリューション「Log Audit Tracker for Ops Manager」 SCOM (Microsoft System Center Operations Manager) 用の管理パックです。SCOM単体では実現できなかった操作履歴、USBデバイス、ドライブの監視等に加え、クライアント監査に必要な情報をSCOMで収集し、そのレポートを自動作成するためのツールです。</p> <p>【製品情報詳細】 http://www.dit.co.jp/products/lat4scom/index.html</p> <p>◆お問い合わせ先◆</p>

	<p>株式会社ディアイティ 高度ネットワーク開発事業部</p> <p>Tel: 03-5634-7651</p> <p>E-Mail: info@dit.co.jp</p>
114	<p>情報セキュリティマネジメントサービス【ディアイティ】</p> <p>お客様組織内に PDCA を構築し維持するための支援を行います。ISO 27001 をベースにした調査表、記録様式、ひな形文書を用いて効率良く作業が行えます。</p> <p>また、情報セキュリティに関連する教育のカリキュラム策定、テキスト作成、評価テスト作成を支援します。併せて講師育成、講師派遣等の教育実施支援を行います。</p> <p>【製品情報詳細】</p> <p>http://www.dit.co.jp/service/infosec_management/index.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社ディアイティ セキュリティサービス事業部</p> <p>Tel: 03-5634-7654</p> <p>E-Mail: ss-info@dit.co.jp</p>
115	<p>ログ解析サービス【ディアイティ】</p> <p>ファイアウォール、IDS/IPS、proxy 等のログを解析し、インシデントの有無、不審な活動証跡の評価を行いレポートにまとめます。</p> <p>【製品情報詳細】</p> <p>http://www.dit.co.jp/service/infosec_management/index.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社ディアイティ セキュリティサービス事業部</p> <p>Tel: 03-5634-7654</p> <p>E-Mail: ss-info@dit.co.jp</p>

116	<p>フォレンジックサービス【ディアイティ】</p> <p>情報漏えい、ウイルス感染の被害を受けた際に、デジタルフォレンジックにより流出源（感染源）・流出経路（感染経路）・流出範囲（感染範囲）を特定し、証跡を保全するとともに再発防止の支援を行います。</p> <p>【製品情報詳細】</p> <p>http://www.dit.co.jp/service/forensics/index.html</p> <p>◆お問い合わせ先◆</p> <p>株式会社ディアイティ セキュリティサービス事業部</p> <p>Tel: 03-5634-7654</p> <p>E-Mail: ss-info@dit.co.jp</p>
117	<p>情報セキュリティマネジメント支援サービス／IT 統制の整備・改善支援コンサルティング【みずほ情報総研】</p> <p>情報セキュリティマネジメント支援サービスでは、組織にとって一貫性があり、情報セキュリティマネジメント能力をスパイラルアップする仕組みの体制構築を、PDCA サイクルにおける全ての工程でサポートします。</p> <p>また、IT 統制の整備・改善支援コンサルティングでは、システムリスク管理の向上に向けて、各組織の状況に対応した、IT 統制の構築・評価を支援します。</p> <p>【サービス情報詳細】</p> <p>情報セキュリティマネジメント支援サービス</p> <p>http://www.mizuho-ir.co.jp/solution/improvement/riskmanage/security/management/index.html</p> <p>IT 統制の整備・改善支援コンサルティング</p> <p>http://www.mizuho-ir.co.jp/solution/improvement/riskmanage/control/tousei/index.html</p> <p>◆お問い合わせ先◆</p> <p>みずほ情報総研株式会社 経営・ITコンサルティング部</p> <p>Tel: 03-5281-5298</p> <p>E-Mail: sec_manage@mizuho-ir.co.jp</p>

118	<p>セキュリティエリア構築【ドコモ・システムズ】</p> <p>限られたエリアへの限られた人物の入退出を可能としたセキュリティエリアの構築を提供</p> <ul style="list-style-type: none"> ・ 生体認証機器を用いた入退出管理 ・ 監視カメラ導入 <p>ドコモ・システムズ株式会社 セキュリティサービス事業部</p> <p>Mail : sec-sales-ml@docomo-sys.co.jp</p>
119	<p>セキュリティ書庫、鍵管理システムの構築【ドコモ・システムズ】</p> <p>ICカード等による電子的鍵を使った書庫や鍵管理システムの提案・構築</p> <ul style="list-style-type: none"> ・ セキュリティ書庫 ・ 鍵管理システム <p>ドコモ・システムズ株式会社 セキュリティサービス事業部</p> <p>Mail : sec-sales-ml@docomo-sys.co.jp</p>
120	<p>暗号化ソリューションの提案【ドコモ・システムズ】</p> <p>秘文製品を利用しての多様化するセキュリティリスク対策の構築</p> <ul style="list-style-type: none"> ・ メール・Webセキュリティ対策 ・ スマートデバイスセキュリティ対策 ・ エンドポイントセキュリティ対策 ・ コンテンツセキュリティ対策 <p>ドコモ・システムズ株式会社 セキュリティサービス事業部</p> <p>Mail : sec-sales-ml@docomo-sys.co.jp</p>

121	<p>集合型研修、WBT【ドコモ・システムズ】</p> <p>ご要望に応じたカスタムメイドな研修サービスをご提供します。</p> <ul style="list-style-type: none"> ・セキュリティ一般研修 ・セキュリティマインドアップ研修 ・セキュリティ専門研修 (ISMS, 内部監査員研修) <p>ドコモ・システムズ株式会社 セキュリティサービス事業部</p> <p>Mail : sec-sales-ml@docomo-sys.co.jp</p> <hr/> <p>※各対策ポイントに関する解説</p> <p>No. 74 について</p> <p>テスト/アンケートを組み込んだ集合型研修やWBT サービスをご提供します。</p> <p>ご要望に応じて、テスト/アンケートの集計・分析作業を行います。</p>
122	<p>インターネットセキュリティ監視【ドコモ・システムズ】</p> <p>企業内部からの情報漏洩や漏洩の前兆となるような Web サービスへの書き込み等を監視いたします。</p> <p>主な監視先 : Twitter, 2ch, 等</p> <p>ドコモ・システムズ株式会社 セキュリティサービス事業部</p> <p>Mail : sec-sales-ml@docomo-sys.co.jp</p>
123	<p>Trend Micro Professional Service™ (セキュリティポリシー策定支援)【トレンドマイクロ】</p> <p>トレンドマイクロでは、お客さまの情報セキュリティ対策プロセス全体を対象とし、ニーズに合わせたプロフェッショナルサービスにより各ステージを支援いたします。セキュリティ対策の遂行に必要なセキュリティポリシーの作成や見直しの支援も可能です。</p> <p>【製品情報詳細】</p> <p>http://jp.trendmicro.com/jp/products/enterprise/tps/index.html</p> <p>◆お問い合わせ先◆</p> <p>トレンドマイクロ・法人お問合せ窓口 TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p>トレンドマイクロ・直営窓口 TEL : 03-5334-3701</p> <p>お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>

124	Trend Micro Network VirusWall Enforcer 【トレンドマイクロ】
	<p>簡易検疫機能を提供することで、ポリシー違反のPCが組織ネットワークへ直接接続するのを防止できます。</p> <p>【製品情報詳細】 http://jp.trendmicro.com/jp/products/enterprise/nvwe/</p> <p>◆お問い合わせ先◆ トrendマイクロ・法人お問合せ窓口 TEL : 03-5334-3601 FAX : 03-5334-3639 トrendマイクロ・直営窓口 TEL : 03-5334-3701 お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>
125	<p>Trend Micro 情報漏えい対策オプション 【トレンドマイクロ】</p> <p>USBメモリ経由の情報漏えいを防ぎたい、対策にかかるコストを抑えたい企業にとって、情報漏えい対策をオプションで提供することにより、導入管理コスト削減を実現し、対策に必要な機能をシンプルに運用できます。</p> <p>【製品情報詳細】 http://jp.trendmicro.com/jp/products/enterprise/corp_dlp/index.html</p> <p>◆お問い合わせ先◆ トrendマイクロ・法人お問合せ窓口 TEL : 03-5334-3601 FAX : 03-5334-3639 トrendマイクロ・直営窓口 TEL : 03-5334-3701 お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>
126	<p>Trend Micro Safe Lock™ 【トレンドマイクロ】</p> <p>システムの特定期間化（ロックダウン）により、許可されたソフトウェア以外の使用を禁止します。</p> <p>【製品情報詳細】 http://jp.trendmicro.com/jp/products/enterprise/tmsl/index.html</p> <p>◆お問い合わせ先◆ トrendマイクロ・法人お問合せ窓口</p>

	<p>TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p>トレンドマイクロ・直営窓口</p> <p>TEL : 03-5334-3701</p> <p>お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>
127	<p>InterScan WebManager 【トレンドマイクロ】</p> <p>「見せたくないサイトを指定」するだけでなくホワイト系カテゴリを追加し網羅率を向上。例外処理を減らす3次元カテゴリによるきめ細やかな制御と出口対策を加え、有害サイト閲覧リスク軽減と管理性を大幅に向上。</p> <p>【製品情報詳細】</p> <p>http://jp.trendmicro.com/jp/products/enterprise/iswm/index.html</p> <p>◆お問い合わせ先◆</p> <p>トレンドマイクロ・法人お問合せ窓口</p> <p>TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p>トレンドマイクロ・直営窓口</p> <p>TEL : 03-5334-3701</p> <p>お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>
128	<p>InterScan Web Security Suite Plus 【トレンドマイクロ】</p> <p>企業でほぼ必ずアクセス可能とする HTTP 通信において必要とされるネットワーク出入口のセキュリティ対策を総合的に提供。</p> <p>Web 利用時の最新のインターネットの脅威、広範なリスクからユーザを守ります。</p> <p>【製品情報詳細】</p> <p>http://jp.trendmicro.com/jp/products/enterprise/iwsva/index.html</p> <p>◆お問い合わせ先◆</p> <p>トレンドマイクロ・法人お問合せ窓口</p> <p>TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p>トレンドマイクロ・直営窓口</p> <p>TEL : 03-5334-3701</p> <p>お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>

129	<p>TrendMicro Deep Security【トレンドマイクロ】</p> <p>Trend Micro Deep Securityは現在のサーバが抱えているセキュリティ課題を仮想・クラウド・物理環境にまたがって、トータルに解決する統合型サーバセキュリティソリューションです。</p> <p>【製品情報詳細】 http://jp.trendmicro.com/jp/products/enterprise/tmds/index.html</p> <p>◆お問い合わせ先◆ トrendマイクロ・法人お問合せ窓口 TEL : 03-5334-3601 FAX : 03-5334-3639 トrendマイクロ・直営窓口 TEL : 03-5334-3701 お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>
130	<p>ウイルスバスターコーポレートエディション【トレンドマイクロ】</p> <p>高度な相関分析を行うクラウド型サービスと連携して高い防御力を保ち、脆弱性対策やマルチプラットフォーム対応も含む最新のセキュリティを実現。 PC やサーバへの負荷を抑えながら、総合的な対策を支援します。</p> <p>【製品情報詳細】 http://jp.trendmicro.com/jp/products/enterprise/corp10_6/</p> <p>◆お問い合わせ先◆ トrendマイクロ・法人お問合せ窓口 TEL : 03-5334-3601 FAX : 03-5334-3639 トrendマイクロ・直営窓口 TEL : 03-5334-3701 お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>

131	<p data-bbox="347 275 884 304">TrendMicroMobile Security【トレンドマイクロ】</p> <p data-bbox="347 322 1366 400">不正プログラムや不正サイトに対する「セキュリティ対策」と紛失時のデータ保護やセキュリティポリシーを適用する「デバイス管理」を包括的に実現。</p> <p data-bbox="347 418 1082 448">Android や iOS などさまざまなモバイル端末の企業導入を支えます。</p> <p data-bbox="360 515 533 544">【製品情報詳細】</p> <p data-bbox="347 562 1246 591">http://jp.trendmicro.com/jp/products/enterprise/mobile-security/index.html</p> <p data-bbox="347 658 568 687">◆お問い合わせ先◆</p> <p data-bbox="347 705 761 734">トレンドマイクロ・法人お問合せ窓口</p> <p data-bbox="371 752 799 781">TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p data-bbox="347 799 665 828">トレンドマイクロ・直営窓口</p> <p data-bbox="371 846 580 875">TEL : 03-5334-3701</p> <p data-bbox="347 896 1222 925">お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>
132	<p data-bbox="347 958 1161 987">TrendMicro Deep Discovery (ネットワーク挙動監視)【トレンドマイクロ】</p> <p data-bbox="347 1005 1374 1084">Trend Micro Deep Discovery は、ネットワーク内の不審な挙動を可視化し、隠れた脅威を見つけ出す標的型攻撃時代の新・ソリューションです。</p> <p data-bbox="360 1151 533 1180">【製品情報詳細】</p> <p data-bbox="347 1198 970 1227">http://jp.trendmicro.com/jp/products/enterprise/dd/</p> <p data-bbox="347 1294 568 1323">◆お問い合わせ先◆</p> <p data-bbox="347 1341 761 1370">トレンドマイクロ・法人お問合せ窓口</p> <p data-bbox="371 1388 799 1417">TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p data-bbox="347 1435 665 1464">トレンドマイクロ・直営窓口</p> <p data-bbox="371 1482 580 1512">TEL : 03-5334-3701</p> <p data-bbox="347 1532 1222 1561">お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>

133	<p>TrendMicro Deep Security (改ざん検知)【トレンドマイクロ】</p> <p>Trend Micro Deep Securityは現在のサーバが抱えているセキュリティ課題を仮想・クラウド・物理環境にまたがって、トータルに解決する統合型サーバセキュリティソリューションです。</p> <p>【製品情報詳細】</p> <p>http://jp.trendmicro.com/jp/products/enterprise/tmds/index.html</p> <p>◆お問い合わせ先◆</p> <p>トレンドマイクロ・法人お問合せ窓口 TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p>トレンドマイクロ・直営窓口 TEL : 03-5334-3701</p> <p>お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>
134	<p>トレンドマイクロ プレミアムサポート (セキュリティトレーニング)【トレンドマイクロ】</p> <p>トレンドマイクロ プレミアムサポート™ for エンタープライズは、お客さまの「セキュリティ被害ゼロ」を目指した、セキュリティ運用管理支援サービスです。サービスメニューの一環として、セキュリティスペシャリストによるセキュリティトレーニングの提供も受けられます。</p> <p>【製品情報詳細】</p> <p>http://jp.trendmicro.com/jp/products/enterprise/tps/index.html</p> <p>◆お問い合わせ先◆</p> <p>トレンドマイクロ・法人お問合せ窓口 TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p>トレンドマイクロ・直営窓口 TEL : 03-5334-3701</p> <p>お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>

135	<p>Trend Micro 情報漏えい対策オプション (USB 制限)【トレンドマイクロ】</p> <p>USB メモリ経由の情報漏えいを防ぎたい、対策にかかるコストを抑えたい企業にとって、情報漏えい対策をオプションで提供することにより、導入管理コスト削減を実現し、対策に必要な機能をシンプルに運用できます。</p> <p>【製品情報詳細】</p> <p>http://jp.trendmicro.com/jp/products/enterprise/corp_dlp/index.html</p> <p>◆お問い合わせ先◆</p> <p>トレンドマイクロ・法人お問合せ窓口 TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p>トレンドマイクロ・直営窓口 TEL : 03-5334-3701</p> <p>お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>
136	<p>トレンドマイクロ プレミアムサポート (セキュリティポリシー策定支援)【トレンドマイクロ】</p> <p>トレンドマイクロ プレミアムサポート™ for エンタープライズは、お客様の「セキュリティ被害ゼロ」を目指した、セキュリティ運用管理支援サービスです。サービスメニューの一環として、セキュリティスペシャリストによるセキュリティポリシー策定支援も受けられます。</p> <p>【製品情報詳細】</p> <p>http://jp.trendmicro.com/jp/products/enterprise/tps/index.html</p> <p>◆お問い合わせ先◆</p> <p>トレンドマイクロ・法人お問合せ窓口 TEL : 03-5334-3601 FAX : 03-5334-3639</p> <p>トレンドマイクロ・直営窓口 TEL : 03-5334-3701</p> <p>お問い合わせフォーム: https://www.trendmicro.co.jp/contact/salesform.asp</p>

137	<p>セキュリティプリンター / 複合機【大日本印刷】</p> <p>本人を特定し、自分の出力指示した文書のみ印刷、確実に受け取るすることが可能とり、放置プリントや取り間違いを防止します。</p> <p>【製品情報詳細】 http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=11</p> <p>◆お問い合わせ先◆ 大日本印刷株式会社 情報ソリューション事業部 http://www.dnp.co.jp/bf/ss/inquiry.html</p>
138	<p>PKI ドライバ【大日本印刷】</p> <p>IC カードに格納した秘密鍵と X.509 証明書を利用して各種 PKI の機能を実現するためのライブラリ群です。</p> <p>【製品情報詳細】 http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=12</p> <p>◆お問い合わせ先◆ 大日本印刷株式会社 情報ソリューション事業部 http://www.dnp.co.jp/bf/ss/inquiry.html</p>
139	<p>人体通信カード認証 MFP システム【大日本印刷】</p> <p>人体通信によるカード認証 MFP システムは、IC カードを装着した送信機を身に付けることにより、受信アンテナの役割を果たすマットの上に立つだけ、あるいは筐体に設置されたタッチパネルに触れるだけで、使用者の認証が行えます。</p> <p>【製品情報詳細】 http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=28</p> <p>◆お問い合わせ先◆ 大日本印刷株式会社 情報ソリューション事業部 http://www.dnp.co.jp/bf/ss/inquiry.html</p>
140	<p>IC カード発行システム CX-330【大日本印刷】</p> <p>昇華型再転写プリンタ CX-330 の特徴</p> <ul style="list-style-type: none"> ・小型化、軽量化。 ・昇華型再転写による高画質を実現。 ・カード両面に全面印刷可能。

	<ul style="list-style-type: none"> ・USB2.0 接続。100Base-TX/10Base-T Ethernet 接続。 ・接触/非接触 IC カード発行に幅広く対応。 ・インクリボンの情報漏洩防止が可能。 <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=2</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 情報ソリューション事業部</p> <p>http://www.dnp.co.jp/bf/ss/inquiry.html</p>
141	<p>IDカードマネジメントシステム【大日本印刷】</p> <p>人事システムに加え、Active Directory からの人事情報の取得も可能です。取得した人事情報を元に、ID カードを用いた PC 認証システム、入退室管理システム、食堂精算システム、勤怠管理システム、複合機等の ID カード情報を統合管理します。複数のシステムに対して、個別に ID カード情報を登録する必要がなくなり、運用負荷を軽減します。</p> <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=27</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 情報ソリューション事業部</p> <p>http://www.dnp.co.jp/bf/ss/inquiry.html</p>
142	<p>シングルサインオン Evidian Enterprise SS0【大日本印刷】</p> <p>ユーザー/アプリケーション/PC/認証方法/利用時間帯などの組み合わせによるアクセス制限を細かく設定することができます。</p> <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=17</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 情報ソリューション事業部</p> <p>http://www.dnp.co.jp/bf/ss/inquiry.html</p>
143	<p>入退館管理/入退室管理システム【大日本印刷】</p>

	<p>社員、来場者が IC カードを用いて、各扉の電気錠を操作することにより、入場者の制限を図ります。</p> <p>外部不正侵入防止の精度を上げ、セキュリティ性を高めます。</p> <p>【製品情報詳細】 http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=6</p> <p>◆お問い合わせ先◆ 大日本印刷株式会社 情報ソリューション事業部 http://www.dnp.co.jp/bf/ss/inquiry.html</p>
144	<p>SSFC【大日本印刷】</p> <p>SSFCとは、Shared Security Formats Cooperationの略で、ICカードを使った高度な企業内セキュリティシステムの実現を目的に、2005年2月に設立された企業アライアンスです。</p> <p>1枚のICカードで、オフィスビルの入退室から室内機器の利用まで一貫して管理、以下のメリットを提供します。</p> <p>【製品情報詳細】 http://www.ssfc.jp/about/</p> <p>◆お問い合わせ先◆ SSFC アライアンス事務局 https://www.dnp.co.jp/ssfc/inquiry/</p>
145	<p>監視カメラ／レコーダ【大日本印刷】</p> <p>人の出入りや行動を映像として残すことができます。</p> <p>なおかつ、SSFC連携により、入退室／入退館の記録を映像に記録することができ、入退室管理システムとの連携によりセキュリティ性がアップします。</p> <p>【製品情報詳細】 http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=5</p> <p>◆お問い合わせ先◆ 大日本印刷株式会社 情報ソリューション事業部 http://www.dnp.co.jp/bf/ss/inquiry.html</p>

146	<p>オフィスセキュリティ【大日本印刷】</p> <p>『Open&Secure』をコンセプトとした自社ビル構築・運用で培ったノウハウと、カードベンダとしてのセキュリティ環境構築の実績を基に、お客様の業態・特性、ワークスタイルにあったセキュリティの構築、強化を支援します。</p> <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/cio/solution/detail/10011347_5309.html</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 C & I 事業部</p> <p>https://www.dnp.co.jp/CGI/cio/solutions/query/form.cgi?news_seq=299</p>
147	<p>セキュリティロッカー【大日本印刷】</p> <p>ICカード認証機能により、キャビネットの電気錠の解錠/施錠を行い、ログ管理も行います。従来の鍵の管理が不要になり、心理的な不安や、煩雑な作業から開放されます。</p> <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=4</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 情報ソリューション事業部</p> <p>http://www.dnp.co.jp/bf/ss/inquiry.html</p>
148	<p>スマートフォンあんしんパック MDM&セキュアブラウザ【大日本印刷】</p> <p>「リモートロック（遠隔操作によりスマートフォンの全機能をロック）」、「リモートワイプ（遠隔操作によりスマートフォン内のデータを消去）」等の機能により、スマートフォンからの情報漏えいリスクを最小化します。</p> <p>Web フィルタリング機能によって、システム管理者が許可したサイト以外へのアクセスを禁止することが出来ます。</p> <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/bf/ss/anshin/</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 情報ソリューション事業部</p> <p>https://www.dnp.co.jp/CGI/bf/reference.cgi</p>

149	<p>Android アプリ不正改ざん検知ソリューション【大日本印刷】</p> <p>アプリ解析・改ざんを防ぐ、Walnut Detector 第三者からのデコンパイルをシャットアウト！ 改ざんされたアプリを検知し、起動をブロック！</p> <p>【製品情報詳細】 http://www.dnp.co.jp/bf/ss/walnut_detector/</p> <p>◆お問い合わせ先◆ 大日本印刷株式会社 情報ソリューション事業部 https://www.dnp.co.jp/CGI/bf/reference.cgi</p>
150	<p>メール誤送信防止ソフトウェア CipherCraft/Mail【大日本印刷】</p> <p>メール誤送信防止ソフト「CipherCraft/Mail（サイファークラフト/メール）」は、今までお使いのメールソフト（環境）を変えることなく、メールの誤送信防止と自動暗号化を同時に実現、メールからの情報漏えいを防ぎます。 CipherCraft は NTT ソフトウェア株式会社の登録商標です。</p> <p>【製品情報詳細】 http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=29</p> <p>◆お問い合わせ先◆ http://www.dnp.co.jp/bf/ss/inquiry.html</p>
151	<p>Web 脆弱性診断サービス【大日本印刷】</p> <p>DNP の Web 脆弱性診断サービスは、動的診断（外部からの擬似攻撃）と、静的診断（ソースコード診断）を同時に行うハイブリッド型診断です。</p> <p>【製品情報詳細】 http://www.dnp.co.jp/bf/ss/shindan/</p> <p>◆お問い合わせ先◆ https://www.dnp.co.jp/CGI/bf/reference.cgi</p>

152	<p>脆弱性評価 SecureScout (セキュアスカウト) 【大日本印刷】</p> <p>SecureScoutは、システムやネットワークに対して、豊富なテストケースを基に疑似攻撃を行い、IT環境のどこにどのようなセキュリティホールが存在するのかを検出し、その対策用レポートを生成するツールです。</p> <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=18</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 情報ソリューション事業部</p> <p>http://www.dnp.co.jp/bf/ss/inquiry.html</p>
153	<p>データ分散保管 TranC'ert DNA (トランザートディエヌエー) 【大日本印刷】</p> <p>TranC'ertDNA (トランザートディエヌエー)は、デジタルデータ (具体的にはWindowsコンピュータ上のファイル) をバックアップするソフトウェアです。</p> <p>1つのファイルをバラバラに裁断して3つのファイルに分割したうえで、暗号化し、3台の保管サーバに分散保管します。</p> <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=7</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 情報ソリューション事業部</p> <p>http://www.dnp.co.jp/bf/ss/inquiry.html</p>
154	<p>雪見式想起技法活用暗号装具 【大日本印刷】</p> <p>デジタルカメラで撮影した写真や様々な加工を施した任意のJPEG画像の裏側に、暗号化したデータを秘密裏に格納(インプラント)できる機能を有しています。暗号化したデータを隠す為に利用する画像をコンテナ画像と呼び、雪見式では、このコンテナ画像が重要な役割を担っています。</p> <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=24</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 情報ソリューション事業部</p> <p>http://www.dnp.co.jp/bf/ss/inquiry.html</p>

155	<p>覗き見から画面を守る！のぞき見防止フィルター 「アイバリアー」【大日本印刷】</p> <p>○覗き見から画面を守る！のぞき見防止フィルター 「アイバリアー」(弊社OEM製品)</p> <p>【製品情報詳細】</p> <p>http://www2.elecom.co.jp/accessory/filter/ef-pfs/index.asp</p> <p>◆お問い合わせ先◆</p> <p>エレコム株式会社</p> <p>http://www.elecom.co.jp/support/access/</p>
156	<p>静的ソースコード解析ソリューション CxSuite【大日本印刷】</p> <p>ソフトウェアのセキュリティ確保および品質向上を支援するため、ソースコードを技術的・論理的に解析し、そこに潜むセキュリティ上の脆弱性について、「発見」・「原因特定」・「解決策の提供」を行います。</p> <p>【製品情報詳細】</p> <p>http://www.dnp.co.jp/CGI/bf/ss/products/viewer.cgi?mode=detail&current_seq=31</p> <p>◆お問い合わせ先◆</p> <p>大日本印刷株式会社 情報ソリューション事業部</p> <p>http://www.dnp.co.jp/bf/ss/inquiry.html</p>

5. チェックリスト対応編

No				対策のポイント	製品・サービス名【会社名】										
1	4-1.	基本方針	(1)	内部不正の対策が経営者の責任であることを組織内外に示す「基本方針」を策定し、役員に周知徹底していますか？	1. 経営者が内部不正対策の方向づけ、モニタリング、評価に関して組織内外において責任を持ちます。	情報セキュリティ・内部統制コンサルティング【インフォセック】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】							
2					2. 本ガイドライン等を参考にし、基本方針を策定します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	情報セキュリティ整備計画策定サービス【NEC】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	Trend Micro Professional Service™ (セキュリティポリシー策定支援)【トレンドマイクロ】					
3					3. 組織が保護すべき重要な情報(重要情報)を定めます。	情報セキュリティ・内部統制コンサルティング【インフォセック】	情報セキュリティ整備計画策定サービス【NEC】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	Trend Micro Professional Service™ (セキュリティポリシー策定支援)【トレンドマイクロ】					
4					4. 策定した基本方針に照らし合わせ、役員に内部不正対策を教育等によって周知徹底します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	集合型研修、WBT【ドコモ・システムズ】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	Trend Micro Professional Service™ (セキュリティポリシー策定支援)【トレンドマイクロ】	カスタムメイド研修【NECラーニング】				
5					5. モニタリング及び評価の結果をもとに、基本方針を定期的に見直します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ログ分析ソフト「InterSafe LogDirector」【アルプスシステムインテグレーション】	エンployerモチベーションサーベイ【リンクアンドモチベーション】	コンプライアンス診断【リンクアンドモチベーション】	経営層向けマネジメント診断【リンクアンドモチベーション】	情報セキュリティマネジメントサービス【ディアアイティ】	Trend Micro Professional Service™ (セキュリティポリシー策定支援)【トレンドマイクロ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	ALogConVerter【NEC(網屋)】	
6					6. 重要情報とそれ以外の情報を区別します。さらに、重要情報を事業上の重要度等を考慮していくつかに分類することが望まれます。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	情報セキュリティマネジメントサービス【ディアアイティ】	Trend Micro Professional Service™ (セキュリティポリシー策定支援)【トレンドマイクロ】	情報セキュリティ整備計画策定サービス【NEC】				
7					7. 重要情報の区別及び分類は、社会背景や事業環境等とともに変化するため、定期的に見直します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報セキュリティ整備計画策定サービス【NEC】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	情報セキュリティマネジメントサービス【ディアアイティ】	Trend Micro Professional Service™ (セキュリティポリシー策定支援)【トレンドマイクロ】				
8			(2)	①経営者は、内部不正対策の総括責任者の任命及び管理体制と実施策の承認を行っていますか？(ただし、経営者が組織全体に目が届く組織であれば、自ら内部不正対策の実施にあたり、管理体制を必ずしも構築する必要はありません) ②総括責任者は、基本方針に則り組織横断的な管理体制を構築し、実施策を策定していますか？	1. 総括責任者には、事業を考慮した実効的で効果的な内部不正対策を実現するために情報セキュリティと経営を理解できる者を任命します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】							
9					2. 総括責任者は、組織横断的な管理体制や関連部門の役割を具体化、明文化し、その役割を徹底させます。責任部門は統括責任者と共に組織全体での内部不正対策の実施策と実施体制を構築します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】							

10					3.	組織横断的な管理体制の構築では、統括責任者が対策実施の管理・運営の要員として各部門の部門責任者や担当者等を任命します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】										
11	4-2-1.	秘密指定	(3)	重要情報を把握し、重要度に合わせて格付け区分し、取り扱い可能な内部者の範囲を定めていますか？	1.	重要情報の取り扱いを定めます。3つ以上に重要度を格付け区分した場合は、重要度ごとに取り扱いを定めます。定めた重要情報の取り扱いは、定期的に見直します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	情報セキュリティポリシー策定支援サービス【OSK】	情報セキュリティ整備計画策定サービス【NEC】										
12					2.	重要情報の管理者を定めます。例えば、部門責任者又は部門責任者から割り当てられた担当者を管理者とします。また、大規模な組織では、部門ごとに管理者を定めます。	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】											
13			(4)	①重要情報の作成者は、定めた格付け区分を選択し、その選択について上司等に確認を得ていますか？ ②重要情報を含む電子文書には、内部者が分かるように機密マーク等の表示をしていますか？	1.	重要情報の取扱範囲は業務上取り扱う必要のある役職員のみを定めます。取扱範囲は、重要情報の不正使用の危険性を低減するために、職位・職務、役割や責任範囲、雇用形態等を踏まえて定めます。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】									
14					2.	重要情報の作成者が(3)で定めた格付け区分を選択するとともに、その選択については、必ず上司等の重要情報の管理者に確認を得る必要があります。また、既に作成し、保管されている重要情報についても同様に格付けされた区分に適用する必要があります。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	情報セキュリティマネジメントサービス【ディアアイティ】	セキュリティプリンター / 複合機【大日本印刷】								
15					3.	重要情報を含む電子文書には、役職員に分かるように格付け区分を示す機密マーク（秘密等の文字が表示される透かしや秘密を表す図形データ、スタンプ等）の表示を付ける必要があります。重要情報を含む電子文書等には、重要情報の有効期間を指定して上記の機密マークとともに記載することが望まれます。有効期間は定期的に見直します。重要情報の取扱期間が終了したら、廃棄等の取り扱いに従って処理します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	セキュリティ PDF 作成ソフト「InterSafe SecurPDF」【アルプスシステムインテグレーション】								
16					4.	重要情報のレベルにより消去方法のレベルを決めて、PC等の情報機器の媒体から重要情報を消去します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	InfoCage データ消去【NEC】								
17	4-2-2.	アクセス権指定	(5)	①情報システムを管理・運営する担当者は、利用者ID及びアクセス権の登録・変更・削除等の設定手順を定めて運用していますか？ ②情報システムを管理・運営する担当者は、異動又は退職により不要となった利用者ID及びアクセス権を、ただちに削除していますか？	1.	利用者ID及びアクセス権の登録・変更・削除に関する承認手順や設定終了報告等の手続きを定めて運用します。	ISMS 認証取得支援サービス【OSK】	情報セキュリティ・内部統制コンサルティング【インフォセック】											
18					2.	情報システムには、(4)で定めた取扱範囲に基づいて重要情報へのアクセス権が利用者IDに設定されるようにします。もし、(4)で定めた取扱範囲によるアクセス権の設定ができない場合は、(4)の見直し又は情報システムの機能変更を行って対処します。	ランブック自動化：HP Operations Orchestration【SCSK】	ランブック自動化：NetIQ Aegis【SCSK】	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	Cyber-Ark PIM Enterprise Suite【ディアアイティ】	認証アプライアンスサーバ：RADIUS GUARD（ラディウスガード）【SCSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	PKI ドライバ【大日本印刷】	ファイル暗号化ソフト「InterSafe IRM」【アルプスシステムインテグレーション】			
18							情報資産アクセス管理基盤ソフト：Soliton ID Manager【ソリトンシステムズ】	SECUREMASTER【NEC】											
19					3.	利用者ID及びアクセス権の登録・変更・削除の手続きに漏れがないように、人事異動に関連する人事手続き等と連携した運用とすることが望まれます。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	シングルサインオンアプライアンス：Smart eGate【ソリトンシステムズ】	情報資産アクセス管理基盤ソフト：Soliton ID Manager【ソリトンシステムズ】	SECUREMASTER【NEC】	Cyber-Ark PIM Enterprise Suite【ディアアイティ】	人体通信カード認証MFPシステム【大日本印刷】	ICカード発行システム CX-330【大日本印刷】					

20				4.	利用者 ID 及びアクセス権が適切に付与されているかを確認するために、定期的にアクセス権の要件を見直します。例えば、人事異動の時期に一致に見直す等を行うことが望まれます。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報資産アクセス管理基盤ソフト：Soliton ID Manager【ソリトンシステムズ】	SECUREMASTER【NEC】	Cyber-Ark PIM Enterprise Suite【ディアイティ】	IDカードマネジメントシステム【大日本印刷】									
21				5.	特に重要な情報を格納している情報システムでは、時間及びアクセス数等のアクセス条件による制御を行うことが望まれます。例えば、時間であれば夜間に重要情報にアクセスすることを制限します。また、アクセス数であれば重要情報を一括してダウンロードすると上司等に通知されるようにします。	ISMS 認証取得支援サービス【OSK】	プライバシーマークの基礎知識（eラーニング）【OSK】	SECUREMASTER【NEC】	Cyber-Ark PIM Enterprise Suite【ディアイティ】	シングルサインオン Evidian Enterprise SSO【大日本印刷】										
22			(6)	1.	複数のシステム管理者がいる場合は、情報システムの管理者 ID ごとに適切な権限範囲の割り当てを行い、相互に監視できるように設定していますか？ また、システム管理者が一人の場合は、ログ等により監視していますか？	ISMS 認証取得支援サービス【OSK】	情報資産アクセス管理基盤ソフト：Soliton ID Manager【ソリトンシステムズ】	Cyber-Ark PIM Enterprise Suite【ディアイティ】												
23				2.	一人のシステム管理者に権限が集中しないように権限を分散します。	ISMS 認証取得支援サービス【OSK】	Cyber-Ark PIM Enterprise Suite【ディアイティ】													
24				3.	相互に監視するために、作業内容や作業日時等が記載された作業報告を作成して残します。この作業報告を別のシステム管理者が確認することが望まれます。	ISMS 認証取得支援サービス【OSK】	情報資産アクセス管理基盤ソフト：Soliton ID Manager【ソリトンシステムズ】	Cyber-Ark PIM Enterprise Suite【ディアイティ】												
25				4.	システム管理者は、特権を必要とする操作以外では特権を用いて操作を行わないようにします。	ShieldWARE【富士通株式会社】	ISMS 認証取得支援サービス【OSK】	Cyber-Ark PIM Enterprise Suite【ディアイティ】												
26			(7)	1.	情報システムでは、共有 ID や共有パスワード・IC カード等を使用せず、個々の利用者 ID を個別のパスワード・IC カード等で認証していますか？	ISMS 認証取得支援サービス【OSK】	IC カード認証ソリューション：SmartOn ID【ソリトンシステムズ】	情報資産アクセス管理基盤ソフト：Soliton ID Manager【ソリトンシステムズ】	SECUREMASTER【NEC】	Cyber-Ark PIM Enterprise Suite【ディアイティ】										
27				2.	利用者自身の利用者 ID を他の利用者に不正使用されないように、パスワードについては、単純な文字列を設定しないこと及び定期的に変更すること等の管理事項を定めて利用者に実施させます。	ISMS 認証取得支援サービス【OSK】	身近な事例で学ぶ情報セキュリティ（eラーニング）【OSK】	プライバシーマークの基礎知識（eラーニング）【OSK】	IC カード認証ソリューション：SmartOn ID【ソリトンシステムズ】	情報資産アクセス管理基盤ソフト：Soliton ID Manager【ソリトンシステムズ】	SECUREMASTER【NEC】	Cyber-Ark PIM Enterprise Suite【ディアイティ】								
28				3.	他の利用者に ID 及びパスワード・IC カード等を貸与することを禁止します。	ISMS 認証取得支援サービス【OSK】	IC カード認証ソリューション：SmartOn ID【ソリトンシステムズ】	Cyber-Ark PIM Enterprise Suite【ディアイティ】												
29	4-3.	物理的管理	(8)	1.	重要情報の格納場所や取り扱う領域等を物理的に保護するために壁や入退管理策によって保護していますか？	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	迫りくる危機！個人情報保護対策（eラーニング）【OSK】	入退室管理：セコム AX【セコム】	入退室管理：セサモ TR II【セコム】	UNIVERGE フィジカルセキュリティソリューション【NEC】	情報セキュリティマネジメントサービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT 統制の整備・改善支援コンサルティング【みずほ情報総研】	セキュリティエリア構築【ドコモ・システムズ】	入退室管理/入退室管理システム【大日本印刷】					
29						SSFC【大日本印刷】	身近な事例で学ぶ情報セキュリティ（eラーニング）【OSK】													
30				2.	役員や運送業者等の外部者によって、重要情報が不正に持ち出されないように入退可能な領域を決めて領域ごとに入退管理をします。例えば、運送業者はロビーまで、取引先は応接室まで、役員は共用エリアと業務フロアまでというようなセキュリティポリシーを策定します。また、サーバールーム等への入室はシステム管理担当者等の資格のある者だけが可能な場合のみ、サーバールームの管理者（責任者等を含む）の許可を事前にて得て入室するものとします。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	身近な事例で学ぶ情報セキュリティ（eラーニング）【OSK】	迫りくる危機！個人情報保護対策（eラーニング）【OSK】	入退室管理：セコム AX【セコム】	入退室管理：セサモ TR II【セコム】	入退室管理：セサモ IDs【セコム】	UNIVERGE フィジカルセキュリティソリューション【NEC】	セキュリティエリア構築【ドコモ・システムズ】						

31				3.	各入退出管理ポイント（各管理エリアの境界）では、内部不正の防止及び発生後の犯人追跡のために、入退出の記録が取られている必要があります。また、入退出の証跡を残すことを目的とし、顔写真等の「個人を特定するための記録」を取ること、より高い内部不正抑止効果が期待できます。この場合、「入退出の記録」と「個人を特定するための記録」は、定期・不定期に監査を行って照合するようにします。	ISMS 認証取得支援サービス【OSK】	身近な事例で学ぶ情報セキュリティ（eラーニング）【OSK】	迫りくる危機！個人情報保護対策（eラーニング）【OSK】	入退室管理：セサモ TR II 【セコム】	HVR（監視カメラ）システム【セコム】	UNIVERGE フィジカルセキュリティソリューション【NEC】	セキュリティエリア構築【ドコモ・システムズ】	監視カメラ/レコーダ【大日本印刷】		
32				4.	重要情報にアクセス可能な物理的領域については、無人における不正侵入も考慮する必要があります。例えば、機械警備システムや監視カメラを導入し、建物の開錠（最初入場時）・閉錠（最終退出時）における警備システム操作者の記録については、顔写真等の個人を特定するための記録も取られていることが望まれます。	ISMS 認証取得支援サービス【OSK】	身近な事例で学ぶ情報セキュリティ（eラーニング）【OSK】	迫りくる危機！個人情報保護対策（eラーニング）【OSK】	HVR（監視カメラ）システム【セコム】	入退室管理：セサモ TR II 【セコム】	入退室管理：セコム AX 【セコム】	UNIVERGE フィジカルセキュリティソリューション【NEC】	セキュリティエリア構築【ドコモ・システムズ】	オフィスセキュリティ【大日本印刷】	
33				5.	重要情報を格納する装置は、必要に応じてネットワークから隔離された環境を用意する等も考慮する必要があります。	ISMS 認証取得支援サービス【OSK】	金庫：ピタゴラス【セコム】								
34		(9)	①PC等の情報機器やUSBメモリ等の携帯可能な記録媒体は、盗難や不正持ち出し等がないように管理・保護していますか？ ②情報機器や記録媒体を処分する際には重要情報が完全消去されていることを確認していますか？	1.	情報機器の紛失等を発見できるようにするために、台帳等で設置場所や使用者を管理し、定期的な棚卸（資産の有無の確認）を実施します。	デバイス制御ソフト「InterSafe DeviceControl」【アルプスシステムインテグレーション】	ISMS 認証取得支援サービス【OSK】	WebSAM AssetSuite【NEC】	セキュリティ書庫、鍵管理システムの構築【ドコモ・システムズ】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】				
35				2.	盗難や不正持ち出しがないように、情報機器はセキュリティワイヤー等で机等に固定することが望まれます。また、ノートPCやスマートデバイス等の携帯可能なモバイル機器や、USBメモリ等の携帯可能な記録媒体は棚や机等に施錠保管します。	ISMS 認証取得支援サービス【OSK】	セキュリティ書庫、鍵管理システムの構築【ドコモ・システムズ】	セキュリティロッカー【大日本印刷】							
36				3.	重要情報の格納サーバやアクセス管理サーバ等の情報機器は、管理者以外が触れられないように、入退出管理が厳しいサーバールーム等の場所に設置します。	ISMS 認証取得支援サービス【OSK】									
37				4.	情報機器及び記録媒体を処分する際は、HDD や USB メモリ等の記録媒体から重要情報を復元できないように完全消去します。さらに、CD-ROM、DVD-ROM、HDD 等の記録媒体は破砕機等を持って物理的に破壊することが望まれます。	ISMS 認証取得支援サービス【OSK】	InfoCage データ消去【NEC】	身近な事例で学ぶ情報セキュリティ（eラーニング）【OSK】	迫りくる危機！個人情報保護対策（eラーニング）【OSK】						
38		(10)	モバイル機器や携帯可能な記録媒体を外部に持ち出す場合には、持ち出しの承認及び記録等の管理をしていますか？	1.	モバイル機器及び記録媒体を持ち出す際に、部門管理者等の承認を得てから持ち出す必要があります。	持出し管理ソフト「InterSafe Workflow」【アルプスシステムインテグレーション】	ISMS 認証取得支援サービス【OSK】	タグ検知：不正持ち出し監視システム【セコム】							
39				2.	モバイル機器及び記録媒体を持ち出す際に、持ち出した情報資産及び、日時、担当者等を記録して管理する必要があります。	持出し管理ソフト「InterSafe Workflow」【アルプスシステムインテグレーション】	ISMS 認証取得支援サービス【OSK】	タグ検知：不正持ち出し監視システム【セコム】							
40		(11)	個人のモバイル機器及び記録媒体の業務利用及び持ち込みを制限していますか？	1.	個人の情報機器及び記録媒体の業務利用を許可するか検討します。	ISMS 認証取得支援サービス【OSK】	情報セキュリティ整備計画策定サービス【NEC】								
41				2.	業務利用を許可する場合には、利用する業務範囲及び順守事項等のルールを整備する必要があります。利用する業務範囲が広くなれば、扱う重要情報が増えて管理が難しくなることに注意する必要があります。また、業務利用にあたって順守事項等の承諾書をとっておくことが望まれます。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	Trend Micro Professional Service®（セキュリティポリシー策定支援）【トレンドマイクロ】	トレンドマイクロプレミアムサポート（セキュリティポリシー策定支援）【トレンドマイクロ】						
42				3.	個人の情報機器を組織ネットワークへの接続を許可する場合には、許可された業務システム及び業務サービスのみ接続可能とするように制限することが望まれます。	InfoCage 不正接続防止【NEC】	ISMS 認証取得支援サービス【OSK】	統合PCセキュリティ管理ソフトウェア：InfoTrace PLUS【ソリトンシステムズ】	不正端末検知・遮断アプライアンス：NetAttest LAP【ソリトンシステムズ】	CounterACT【NEC（ソリトンシステムズ）】	Soliton SecureBrowser / Soliton SecureGateway【ソリトンシステムズ】	Trend Micro Network VirusWall Enforcer【トレンドマイクロ】	InfoTrace PLUS【NEC（ソリトンシステムズ）】		

43					4.	個人の情報機器において重要度の高い情報を扱う場合には、必要に応じて個人の情報機器上でも重要情報を管理できるソフトウェア等を導入して組織側で重要情報を管理できることが望まれます。	ファイル暗号化ソフト「InterSafe IRM」【アルプスシステムインテグレーション】	ISMS 認証取得支援サービス【OSK】	InfoCage FileShell【NEC】											
44					5.	重要情報の格納サーバやアクセス管理サーバ等が設置されているサーバールームでは、個人所有のノートPC やタブレット端末、スマートフォン等のモバイル機器の持ち込み・利用を厳しく制限します。	認証アプライアンスサーバ:RADIUS GUARD (ラディウスガード)【SGSK】	ISMS 認証取得支援サービス【OSK】	検疫ネットワーク認証アプライアンス:NetAttest Security Filter【ソリトンシステムズ】	不正端末検知・遮断アプライアンス:NetAttest LAP【ソリトンシステムズ】	CounterACT【NEC(ソリトンシステムズ)】	InfoCage 不正接続防止【NEC】	スマートフォンあんしんバックMDM&セキュアブラウザ【大日本印刷】							
45					6.	情報機器の持ち込みを禁止する場所では、持込禁止のポスター等を貼って警告することが望まれます。		ISMS 認証取得支援サービス【OSK】												
46					7.	個人所有のUSB メモリ等の携帯可能な記録媒体等の持ち込みを制限します。記録媒体等の利用は会社貸与品のみとします。	CheckPoint Endpoint Security Media Encryption【メトロ】	デバイス制御ソフト「InterSafe DeviceControl」【アルプスシステムインテグレーション】	ISMS 認証取得支援サービス【OSK】	統合PCセキュリティ管理ソフトウェア:InfoTrace PLUS【ソリトンシステムズ】	InfoCage PCセキュリティ【NEC】	ICカード認証ソリューション:SmartOn ID【ソリトンシステムズ】	Trend Micro 情報漏えい対策オプション【トレンドマイクロ】	InfoTrace PLUS【NEC(ソリトンシステムズ)】						
47	4-4.	技術・運用管理	(12)		1.	組織のネットワークは、重要情報を不正に持ち出し可能なファイル共有ソフトやSNS、外部のオンラインストレージ等の使用を制限していますか？	PG 等の情報機器には、組織内で許可されたソフトウェア以外のもの(例えば、ファイル共有ソフト等)をインストールして利用することを禁止します。利用を許可するソフトウェアは、組織内で決定します。利用者から新たに利用申請があったソフトウェアは、利用させてもよいか判断する必要があります。	エンドポイントセキュリティ (IBM Tivoli Endpoint Manager)【インフォセック】	ISMS 認証取得支援サービス【OSK】	統合PCセキュリティ管理ソフトウェア:InfoTrace PLUS【ソリトンシステムズ】	検疫ネットワーク認証アプライアンス:NetAttest Security Filter【ソリトンシステムズ】	InfoCage PCセキュリティ【NEC】	情報漏洩対策サービス:セコムPCセキュアサービス【セコムトラストシステムズ】	Trend Micro Safe Lock【トレンドマイクロ】	Android アプリ不正改ざん検知ソリューション【大日本印刷】	ProxySG【NEC(Blue Coat Systems)】	PA シリーズ【NEC(Palo Alto Networks)】			
47									InfoTrace PLUS【NEC(ソリトンシステムズ)】											
48					2.	Web アクセスに関しては、コンテンツフィルタを導入して、SNS 及びアップローダー、掲示板等へのアクセスを制限することが望まれます。	CheckPoint Appliance【メトロ】	Web フィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】	i-FILTER【デジタルアーツ】	ISMS 認証取得支援サービス【OSK】	InterScan WebManager【トレンドマイクロ】	InterScan Web Security Suite Plus【トレンドマイクロ】	クラウド型 Web フィルタリングサービス「InterSafe CATS」【アルプスシステムインテグレーション】	i-FILTER【NEC(デジタルアーツ)】	i-FILTER ブラウザー&クラウド【デジタルアーツ】	D-SPA【デジタルアーツ】				
48							ネットワーク脅威対策製品: Palo Alto Networks PA シリーズ【SGSK】	ウェブセキュリティアプライアンス: Cisco WSA【ソリトンシステムズ】	セキュリティサービス/マネージドサービス: URL フィルタサービス【セコムトラストシステムズ】	McAfee Web Gateway (Webwasher)【ディアイティ】	FortiGate【NEC(Fortinet)】	Web マルウェア対策製品: McAfee Web Gateway【SGSK】	スマートデバイス向けフィルタリングソフト「InterSafe SecureBrowser」【アルプスシステムインテグレーション】	スマートデバイス向け統合セキュリティサービス「ビジネススマートセキュリティ」【アルプスシステムインテグレーション】	ProxySG【NEC(Blue Coat Systems)】	PA シリーズ【NEC(Palo Alto Networks)】				
48							InterSafe WebFilter【NEC(アルプスシステムインテグレーション)】													
49					3.	電子メールに関しては、業務のメールを個人のメールアドレスに転送する設定になっていないかを確認することが望まれます。また、外部宛のメール送信を再確認する機能や、添付ファイル等が暗号化されていないと送信できないメールシステム等を導入することで、誤送信による情報漏洩の対策を講じることが望まれます。	FENCE メール誤送信対策サービス【富士通株式会社】	m-FILTER【デジタルアーツ】	ISMS 認証取得支援サービス【OSK】	セキュアファイル転送アプライアンス:FileZen【ソリトンシステムズ】	GUARDIANWALL【NEC(キヤノン IT ソリューションズ)】	メール誤送信防止ソフトウェア CipherCraft/Mail【大日本印刷】	ProofPoint【NEC(Proofpoint)】	暗号化ソリューションの提案【ドコモ・システムズ】	AddPoint/MailWall Server【NEC(キヤノン IT ソリューションズ)】					
50					4.	PC 等の情報機器を守るために、ウイルス対策ソフトの導入やパッチ適用等の一般的なセキュリティ対策を行います。	エンドポイントセキュリティ (IBM Tivoli Endpoint Manager)【インフォセック】	ISMS 認証取得支援サービス【OSK】	身近な事例で学ぶ情報セキュリティ(eラーニング)【OSK】	セキュリティサービス: ウイルス対策支援サービス【セコムトラストシステムズ】	InfoCage セキュリティリスク管理【NEC】	InfoCage PC 検疫【NEC】	TrendMicro Deep Security【トレンドマイクロ】	ウイルスバスターコーポレートエディション【トレンドマイクロ】	Web 脆弱性診断サービス【大日本印刷】					

51		(13)	①委託先等の関係者への重要情報の受渡しは、受渡しから廃棄迄を含めて管理していますか？ ②インターネット等の組織外を介す重要情報の受渡しでは、誤って関係者以外に渡ってしまうことも考慮し、暗号化等で保護していますか？	1.	重要情報の受渡しに関しては、重要度に合わせた組織内部での手順及び承認手続きを定めるとともに、委託先等の関係者にも順守させます。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	迫りくる危機！個人情報保護対策（eラーニング）【OSK】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	情報セキュリティマネジメントサービス【ディアイティ】	データ分散保管 TranC'ert DNA（トランザートディエヌエー）【大日本印刷】				
52				2.	関係者への重要情報の受渡しに関する記録を行います。	セキュリティUSBメモリ作成ソフト「InterSafe SecureDevice」【アルプスシステムインテグレーション】	FinalCode【デジタルアーツ】	ISMS 認証取得支援サービス【OSK】							
53				3.	関係者へのインターネットを用いた送信及び記録媒体を用いた手渡しによる重要情報の受渡しについては暗号化を行います。	FENCE-PRO【富士通株式会社】	セキュリティUSBメモリ作成ソフト「InterSafe SecureDevice」【アルプスシステムインテグレーション】	ファイナル暗号化ソフト「InterSafe IRM」【アルプスシステムインテグレーション】	FinalCode【デジタルアーツ】	暗号化ソリューションの提案【ドコモ・システムズ】	InfoCage FileShell【NEC】	セキュリティサービス：データ一時保管サービス【セコムトラストシステムズ】	InfoCage PCセキュリティ【NEC】	InfoCage ファイル暗号【NEC】	セキュアファイル転送ソリューション：FileZen【ソリトンシステムズ】
53							ISMS 認証取得支援サービス【OSK】								
54				4.	関係者に開示した重要情報の廃棄・消去に関する記録を関係者から取得します。	FinalCode【デジタルアーツ】	ISMS 認証取得支援サービス【OSK】	セキュアファイル転送ソリューション：FileZen【ソリトンシステムズ】							
55				5.	上記の取り決めについては、委託先までではなく、それ以降の再委託先にも順守させる必要があります。		ISMS 認証取得支援サービス【OSK】	迫りくる危機！個人情報保護対策（eラーニング）【OSK】							
56		(14)	組織外部で利用・取り扱い可能な重要情報を限定し、重要情報や情報機器を保護していますか？	1.	情報機器を利用する際に利用者IDとパスワード等による認証をできるように設定をします。また、ノートPCではBIOSパスワード、HDDパスワードを設定することが望まれます。さらに、重要情報を保護するために暗号化ソフトを導入することが望まれます。	Full Disk Encryption【NEC(Check Point Endpoint Security)】	ファイナル暗号化ソフト「InterSafe IRM」【アルプスシステムインテグレーション】	ISMS 認証取得支援サービス【OSK】	ICカード認証ソリューション：SmartOn ID【ソリトンシステムズ】	CheckPoint Endpoint Security Full Disk Encryption【メトロ】	CheckPoint Endpoint Security Media Encryption【メトロ】	暗号化ソリューションの提案【ドコモ・システムズ】	InfoCage PCセキュリティ【NEC】	InfoCage FileShell【NEC】	
57				2.	組織外のネットワークに接続して重要情報を送受信する場合には、重要情報又は通信を暗号化します。	ファイナル暗号化ソフト「InterSafe IRM」【アルプスシステムインテグレーション】	m-FILTER【デジタルアーツ】	FinalCode【デジタルアーツ】	ISMS 認証取得支援サービス【OSK】	NetScaler MPX【NEC(CitrixSystems)】	InfoCage FileShell【NEC】	ASA5500シリーズ【NEC(CiscoSystems)】	雪見式想起技法活用暗号装置【大日本印刷】	Tectiaシリーズ【ディアイティ】	MAGシリーズ【NEC(Juniper Networks)】
57						InfoCage PCセキュリティ【NEC】	InfoCage ファイル暗号【NEC】	Addpoint/SA【NEC(キヤノンITソリューションズ)】	UNIVERGE SecureBranch VM【NEC】	FortiGate【NEC(Fortinet)】					
58		(15)	組織外で重要情報を用いた業務を行う際に、周囲の環境やネットワーク環境等を考慮して保護していますか？	1.	電車の社内やカフェ等では、他面が覗き込まれないように注意します。また、画面に覗き見防止フィルムを貼り、覗き込まれないようにすることが望まれます。	ISMS 認証取得支援サービス【OSK】	身近な事例で学ぶ情報セキュリティ（eラーニング）【OSK】	迫りくる危機！個人情報保護対策（eラーニング）【OSK】	プライバシーマークの基礎知識（eラーニング）【OSK】	覗き見から画面を守る！のぞき見防止フィルター「アイバリアー」【大日本印刷】					
59				2.	ホテルの有線LAN・無線LANや公衆無線LAN等の不特定の利用者が共有するネットワークの接続を許可するかどうかを判断します。		ISMS 認証取得支援サービス【OSK】								

60					3.	許可されたネットワーク環境から組織ネットワークに接続する際には、VPN 等を用いて通信を暗号化する必要があります。	CheckPoint Appliance【メトロ】	スマートデバイス向け統合セキュリティサービス「ビジネススマートセキュリティ」【アルプスシステムインテグレーション】	セコム InternetVPN サービス【セコムトラストシステムズ】	ISMS 認証取得支援サービス【OSK】	UNIVERGE SecureBranch VM【NEC】	ASA5500 シリーズ【NEC(CiscoSystems)】	NetScaler MPX【NEC(CitrixSystems)】	MAG シリーズ【NEC(JuniperNetworks)】	FortiGate【NEC(Fortinet)】	Tectia シリーズ【ディアティ】	
60							Soliton SecureBrowser / Soliton SecureGateway【ソリトンシステムズ】	オールインワン認証アプライアンス：NetAttest EPS【ソリトンシステムズ】									
61					4.	重要情報が記録されている情報機器の紛失を想定し、リモートから情報機器内の重要情報を消去できるツール又はサービスを利用することが望まれます。また、パスワードロックの認証で一定の回数認証に失敗すると重要情報を消去するツールを利用することも望まれます。	InfoCage ファイル暗号【NEC】	セキュリティUSBメモリ作成ソフトウェア「InterSafe SecureDevice」【アルプスシステムインテグレーション】	FinalCode【デジタルアーツ】	ISMS 認証取得支援サービス【OSK】	オールインワン認証アプライアンス：NetAttest EPS【ソリトンシステムズ】	スマートデバイス向け統合セキュリティサービス「ビジネススマートセキュリティ」【アルプスシステムインテグレーション】	TrendMicroMobile Security【トレンドマイクロ】				
62		(16)	第三者が提供するサービスで取り扱い可能である重要情報であるかを判断し、利用前に確認・合意し、利用中にも契約通りのサービス実施内容であることを確認していますか？	1.	第三者が提供するサービスで取り扱ってもよい重要情報であるかを判断します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアティ】	情報セキュリティマネジメント支援サービス/IT 統制の整備・改善支援コンサルティング【みずほ情報総研】	静的ソースコード解析ソリューション CxSuite【大日本印刷】							
63				2.	第三者が提供するサービスにおいてセキュリティ管理策が、重要情報を安全に管理するために十分であるかを確認します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアティ】	情報セキュリティマネジメント支援サービス/IT 統制の整備・改善支援コンサルティング【みずほ情報総研】								
64				3.	第三者が提供するサービスのサービスレベル及び管理上の要求事項が、事業継続において適切であるかを確認します。	情報セキュリティ・内部統制コンサルティング【インフォセック】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアティ】	情報セキュリティマネジメント支援サービス/IT 統制の整備・改善支援コンサルティング【みずほ情報総研】								
65				4.	内部不正が発生した際に、ログが提供されるか確認します。	IBM Guardium【メトロ】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアティ】	情報セキュリティマネジメント支援サービス/IT 統制の整備・改善支援コンサルティング【みずほ情報総研】								
66	4-5.	証拠確保	(17) 重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を定めた期間に従って安全に保護していますか？ (推奨)	1.	ログは、重要情報へのアクセス履歴や、利用者の操作履歴 (Web のアクセスログやメールの送受信履歴等) を取得します。	IBM Guardium【メトロ】	IT データ解析プラットフォーム：Splunk Enterprise【SCSK】	ログ統合管理システム：Aresight【SCSK】	統合ログ管理サービス【インフォセック】	ログ分析ソフトウェア「InterSafe LogDirector」【アルプスシステムインテグレーション】	Log Audit Tracker for Ops Manager【ディアティ】	GUARDIANWALL【NEC(キヤノン IT ソリューションズ)】	i-FILTER【デジタルアーツ】	D-SPA【デジタルアーツ】	Addpoint/MailWall Server【NEC(キヤノン IT ソリューションズ)】		
66						i-FILTER ブラウザー&クラウド【デジタルアーツ】	Web フィルタリングソフトウェア「InterSafe WebFilter」【アルプスシステムインテグレーション】	クラウド型 Web フィルタリングサービス「InterSafe CATS」【アルプスシステムインテグレーション】	スマートデバイス向けフィルタリングソフトウェア「InterSafe SecureBrowser」【アルプスシステムインテグレーション】	スマートデバイス向け統合セキュリティサービス「ビジネススマートセキュリティ」【アルプスシステムインテグレーション】	ファイル暗号化ソフトウェア「InterSafe IRM」【アルプスシステムインテグレーション】	デバイス制御ソフトウェア「InterSafe DeviceControl」【アルプスシステムインテグレーション】	セキュリティ USBメモリ作成ソフトウェア「InterSafe SecureDevice」【アルプスシステムインテグレーション】	Web フィルタリングソフトウェア「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	ISMS 認証取得支援サービス【OSK】		
66						InfoTrace PLUS【NEC(ソリトンシステムズ)】	ウェブセキュリティアプライアンス：Cisco WSA【ソリトンシステムズ】	メールセキュリティアプライアンス：Cisco ESA【ソリトンシステムズ】	オールインワン認証アプライアンス：NetAttest EPS【ソリトンシステムズ】	統合 PC セキュリティ管理ソフトウェア：InfoTrace PLUS【ソリトンシステムズ】	FinalCode【デジタルアーツ】	m-FILTER【デジタルアーツ】	AlogConverter【NEC(網屋)】	情報漏洩対策サービス：セコム PC セーフティサービス【セコムトラストシステムズ】	NetEvidence【NEC(オーク情報システム)】		

67					2.	証跡は、設定したポリシーに応じて、上記のログ以外の日時、利用者、操作端末、操作内容、送受信の内容等の情報を取得します。	i-FILTER ブラウザー&クラウド【デジタルアーツ】	統合ログ管理サービス【インフォセック】	i-FILTER【デジタルアーツ】	D-SPA【デジタルアーツ】	Addpoint/MailWall Server【NEC(キヤノン IT ソリューションズ)】	Log Audit Tracker for Ops Manager【ディアアイティ】	IBM Guardium【メトロ】	GUARDIANWALL【NEC(キヤノン IT ソリューションズ)】	NetEvidence【NEC(オーク情報システム)】	Web フィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】	
67							InfoTrace PLUS【NEC(ソリトンシステムズ)】	m-FILTER【デジタルアーツ】	FinalCode【デジタルアーツ】	ISMS 認証取得支援サービス【OSK】	Web フィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	統合ログ分析アプリケーション:NetAttest BigData【ソリトンシステムズ】	AlogConverter【NEC(網屋)】				
68					3.	ログは定期的に確認します。多量なファイルへのアクセスや業務範囲外のファイルへのアクセス等の通常の業務と異なる事象が発見された者に対して、事象確認又は監視強化等の対策を行うことが望ましい。	IBM Guardium【メトロ】	統合ログ管理サービス【インフォセック】	ISMS 認証取得支援サービス【OSK】	統合 PC セキュリティ管理ソフトウェア: InfoTrace PLUS【ソリトンシステムズ】	ログ解析サービス【ディアアイティ】	AlogConverter【NEC(網屋)】	TrendMicro Deep Discovery (ネットワーク挙動監視)【トレンドマイクロ】	NetEvidence【NEC(オーク情報システム)】	GUARDIANWALL【NEC(キヤノン IT ソリューションズ)】	Web フィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】	
68							InfoTrace PLUS【NEC(ソリトンシステムズ)】	Web フィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	Addpoint/MailWall Server【NEC(キヤノン IT ソリューションズ)】								
69					4.	利用者のプライバシー等を考慮して、ログ・証跡を収集することを労働組合等と合意をとることが望まれます。	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT 統制の整備・改善支援コンサルティング【みずほ情報総研】								
70					5.	ログ・証跡の保存は、リスクとコストのバランスによって期間を決めます。保存期間は、内部不正の抑止の観点から内部者に知らせないことが望まれます。ログ・証跡の確認には、改ざん及び削除防止並びに特定のシステム管理者からのみアクセス可能等の措置が取られていることが望まれます。確認をする際には、統括責任者等のシステム管理者から許可を得ることが望まれます。	i-FILTER ブラウザー&クラウド【デジタルアーツ】	統合ログ管理サービス【インフォセック】	i-FILTER【デジタルアーツ】	m-FILTER【デジタルアーツ】	IBM Guardium【メトロ】	InfoTrace PLUS【NEC(ソリトンシステムズ)】	GUARDIANWALL【NEC(キヤノン IT ソリューションズ)】	D-SPA【デジタルアーツ】	FinalCode【デジタルアーツ】	Web フィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】	
70							ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	AlogConverter【NEC(網屋)】	TrendMicro Deep Security (改ざん検知)【トレンドマイクロ】	NetEvidence【NEC(オーク情報システム)】	Web フィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	Addpoint/MailWall Server【NEC(キヤノン IT ソリューションズ)】	情報セキュリティマネジメント支援サービス/IT 統制の整備・改善支援コンサルティング【みずほ情報総研】			
71			(18)		1.	システム管理者のアクセス履歴や操作履歴等のログ・証跡を記録して保存するだけでなく、そのログ・証跡の内容を定期的にシステム管理者以外が確認していますか？	InfoTrace PLUS【NEC(ソリトンシステムズ)】	統合ログ分析アプリケーション:NetAttest BigData【ソリトンシステムズ】	Web フィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	Addpoint/MailWall Server【NEC(キヤノン IT ソリューションズ)】	統合ログ管理サービス【インフォセック】	NetEvidence【NEC(オーク情報システム)】	GUARDIANWALL【NEC(キヤノン IT ソリューションズ)】	AlogConverter【NEC(網屋)】	ログ解析サービス【ディアアイティ】	Web フィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】	
72					2.	情報システムにおいて、ログ・証跡を収集できない場合には、情報システムの管理者の作業内容をドキュメントに記録し、定期的にその作業内容をシステム管理者の上司や総括管理者が確認します。	統合ログ分析アプリケーション:NetAttest BigData【ソリトンシステムズ】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT 統制の整備・改善支援コンサルティング【みずほ情報総研】								
73	4-6.	人的管理	(19)		1.	①すべての役員に教育を実施し、組織の内部不正対策に関する方針及び重要情報の取り扱い等の手順を周知徹底していますか？ ②教育を定期的に繰り返して実施し、教育内容を定期的に見直しして更新していますか？	情報セキュリティ教育【インフォセック】	人材育成コンサルティング【リンクアンドモチベーション】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT 統制の整備・改善支援コンサルティング【みずほ情報総研】	カスタムメイド研修【NEC ラーニング】	集合型研修、WBT【ドコモ・システムズ】	トレンドマイクロ プレミアムサポート (セキュリティトレーニング)【トレンドマイクロ】				

74				2.	教育を実施した証拠として、受講者の受講状況及び理解度についての記録をとります。	情報セキュリティ教育【インフォセック】	人材育成コンサルティング【リンクアンドモチベーション】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	集合型研修、WBT【ドコモ・システムズ】								
75				3.	教育内容を定期的に見直しで更新し、更新内容を周知徹底します。	情報セキュリティ教育【インフォセック】	集合型研修、WBT【ドコモ・システムズ】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	トレンドマイクロプレミアムサポート（セキュリティトレーニング）【トレンドマイクロ】								
76				4.	教育内容は、職位（管理職、非管理職等）及び契約形態（社員、派遣社員等）等の権限や職務に応じて適切なレベルや内容を実施することが望まれます。特にシステム管理者には規範意識を高める教育を実施することが望まれます。	情報セキュリティ教育【インフォセック】	人材育成コンサルティング【リンクアンドモチベーション】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	集合型研修、WBT【ドコモ・システムズ】	トレンドマイクロプレミアムサポート（セキュリティトレーニング）【トレンドマイクロ】							
77		(20)	雇用の終了時に秘密保持義務を課す誓約書の提出を求めていますか？（推奨）	1.	秘密保持契約には、秘密保持の対象となる重要情報を客観的に特定できる記載が必要です。	ISMS 認証取得支援サービス【OSK】	情報セキュリティポリシー策定支援サービス【OSK】	プライバシーマーク取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】								
78				2.	競争禁止義務を記載する場合には、職業選択の自由を侵害しないように、適切に範囲を設定する必要があります。	ISMS 認証取得支援サービス【OSK】	情報セキュリティポリシー策定支援サービス【OSK】	プライバシーマーク取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】								
79		(21)	従業員の雇用終了時および請負等の契約先との契約終了時に、取り扱いを委託した情報資産のすべてを返却または完全消去し、情報システムの利用者 ID や権限を削除していますか？	1.	誓約書や契約書には、雇用終了時や契約終了時に情報資産の返却及び契約先所有のPC等からの完全消去に関する記載が必要です。	InfoCage データ消去【NEC】	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】									
80				2.	取り扱いを委託した情報資産及び入館証等の権限(Q&A8・P6)	ISMS 認証取得支援サービス【OSK】												
81				3.	情報システムから元従業員の利用者 ID や権限が削除されたことを確認する必要があります。	SECUREMASTER【NEC】	ISMS 認証取得支援サービス【OSK】											
82				4.	契約先所有のPC等に保存されていたすべての重要情報を完全消去した旨の確認を契約先からとることが望まれます。	InfoCage データ消去【NEC】	ISMS 認証取得支援サービス【OSK】	FinalCode【デジタルアーツ】										
83				5.	雇用終了際に情報の持ち出し等の内部不正が発生しやすいことから、雇用終了前の一定期間から、PC等をシステム管理部門等の管理下に置くことが望まれます（例：アクセス範囲の限定、USBメモリの利用制限等）。	InfoCage PCセキュリティ【NEC】	デバイス制御ソフト「InterSafe DeviceControl」【アルプスシステムインテグレーション】	ISMS 認証取得支援サービス【OSK】	ファイル暗号化ソフト「InterSafe IRM」【アルプスシステムインテグレーション】	Trend Micro 情報漏えい対策オプション（USB制限）【トレンドマイクロ】								
84	4-7.	コンプライアンス	(22)	就業規則等の内部規程を整備し、正式な懲戒手続を備えていますか？	1.	内部規程には、懲戒処分の対象となる内部不正（例：営業秘密の侵害、個人情報の目的外利用等）に関する記載が必要です。	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】										
85				2.	内部規程には、秘密保持義務の対象となる重要情報を客観的に特定できる記載が必要です。	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】											

86				3.	解雇等の懲戒処分は、根拠となる内部規程に基づき、かつ労働法制を順守して処分を行なう必要があります。	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】													
87				4.	適切な懲戒処分を決定するために、査問委員会等によって事実関係を明らかにする必要があります。	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】													
88				5.	刑事告発及び刑事訴訟の法的な手続きに関する内部規程を整備する必要があります。	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】													
89		(23)	内部者に対して重要情報を保護する義務があることを理解させるために「秘密保持契約書」等を要請していますか？	1.	「秘密保持誓約書」には、秘密保持の対象となる重要情報を客観的に特定できる記載が必要となります。	ISMS 認証取得支援サービス【OSK】	情報セキュリティポリシー策定支援サービス【OSK】	プライバシーマーク取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】										
90				2.	「秘密保持誓約書」は、役職員に対して重要情報を保護する義務があることを理解させるために、入社時以外にも特定の機会（昇格、配置転換等による業務の変更やプロジェクトの終了時）に誓約書を要請することが望まれます。	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】												
91	4-8.	職場環境	(24)	公平で客観的な人事評価を整備するとともに、業績に対する評価を説明する機会を設ける等、人事評価や業績評価の整備を推進していますか？（推奨）	1.	昇進や昇格及び組織の給与体系については、公平かつ客観的に実施するとともに十分な透明性を保つことが重要です。必要に応じて、上司や部門長が人事評価や業績評価の評価内容を説明することが望まれます。	人事制度コンサルティング【リンクアンドモチベーション】	評価者研修【リンクアンドモチベーション】												
92				2.	評価制度を整備する一環として、業務で必要となる技術や知識に関する教育や研修の受講を推進することが望まれます。	研修サービス【NECラーニング】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】												
93				3.	ある役職員が特定の業務を長期間にわたり担当している場合には、このような状態を避けるために配置転換を検討することが望まれます。															
94			(25)	業務量及び労働時間の適正化等の適切な労働環境を整備するとともに、業務支援を推進する体制や相談しやすい環境を整える等職場内において良好なコミュニケーションを組織全体で推進していますか？（推奨）	1.	特定の役職員が休暇取得できない状態や長時間残業が継続している状態のように、極端に業務負荷が高い場合には、業務量や労働時間を適正な範囲にする必要があります。														
95				2.	業務は肉体的・精神的に健康を損ねない範囲とし、職場環境は安全で衛生的に保つ必要があります。	職場診断【リンクアンドモチベーション】														

105								i-FILTER ブラウザー&クラウド【デジタルーツ】	D-SPA【デジタルーツ】	m-FILTER【デジタルーツ】	NetEvidence【NEC(オーク情報システム)】	Webフィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	InfoTrace PLUS【NEC(ソリトンシステムズ)】						
106				2.	内部不正への対応については、システム管理者、インシデントレスポンス担当者（外部のインシデントレスポンス支援担当者を含む）、デジタル・フォレンジック解析担当者（外部支援担当者を含む）、弁護士、内部監査者等と連携する必要があります。また、サービスを受ける場合には、必要となる情報を迅速に提供できるように事前に伝達内容や方法を取り決めておくことが望まれます。	インシデントレスポンスサービス【OSK】	Webフィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】	統合ログ分析ソリューション:NetAttest BigData【ソリトンシステムズ】	セコムプロフェッショナルサポート:緊急事態サポートサービス(法人様向け)【セコムトラストシステムズ】	Trend Micro Professional Service(セキュリティポリシー策定支援)【トレンドマイクロ】	Addpoint/MailWall Server【NEC(キャノンITソリューションズ)】	NetEvidence【NEC(オーク情報システム)】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	Webフィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	プライバシーマーク取得支援サービス【OSK】				
106								InfoTrace PLUS【NEC(ソリトンシステムズ)】	GUARDIANWALL【NEC(キャノンITソリューションズ)】	AlogConverter【NEC(網屋)】	フォレンジックサービス【ディアイティ】	トレンドマイクロプレミアムサポート(セキュリティポリシー策定支援)【トレンドマイクロ】	ISMS 認証取得支援サービス【OSK】						
107				3.	監督官庁への報告義務がある事案に関して、対応する体制を整えておく必要があります。	ISMS 認証取得支援サービス【OSK】	プライバシーマーク取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】										
108				4.	事業継続計画が存在する場合には、その計画との関係を考慮して内部不正対策の体制を構築する必要があります。	ISMS 認証取得支援サービス【OSK】	情報セキュリティマネジメントサービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】											
109		(28)	内部不正者に対する処罰を検討し、内部不正の事例を内部に告知することを検討していますか？	1.	内部不正による影響を最小限にするために、求められる対応手順や報告手順等事業継続管理手順へ内部不正対策を組込む必要があります。内部不正者に対する処罰を検討するためには、本ガイドラインの(22) 法的手続きの整備で定めた内容を基に、人事担当者及び法務担当者、弁護士等で法的処置に関して検討する必要があります。	情報セキュリティマネジメントサービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】												
110				2.	内部不正の再発防止策を検討し、実施する必要があります。	フォレンジックサービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】												
111				3.	内部不正によるインシデントの具体的な事象から学習し再発を防止するという観点から、発生した内部不正の事例を内部不正者に行われた処分も含めて組織の内部に告知することが望まれます。	InfoTrace PLUS【NEC(ソリトンシステムズ)】	Webフィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	GUARDIANWALL【NEC(キャノンITソリューションズ)】	Addpoint/MailWall Server【NEC(キャノンITソリューションズ)】	Webフィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】	AlogConverter【NEC(網屋)】	NetEvidence【NEC(オーク情報システム)】	情報セキュリティマネジメント支援サービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】					
112	4-10.	組織の管理	(29) 内部不正と思わしき事象が発生した場合についての通報制度を整備し、通報受付を複数設置し、必要に応じて通報者の匿名性を確保していますか？	1.	内部不正の通報に最低限必要となる以下の情報等を示す必要があります。「受付窓口(連絡先と連絡方法)」、「対象となる情報や物理的資産」、「いつ、どのような状態(不正利用、破壊等)になったのか」、「事象をどのように知り得たのか」等。	InfoTrace PLUS【NEC(ソリトンシステムズ)】	GUARDIANWALL【NEC(キャノンITソリューションズ)】	Addpoint/MailWall Server【NEC(キャノンITソリューションズ)】	AlogConverter【NEC(網屋)】	NetEvidence【NEC(オーク情報システム)】	フォレンジックサービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	Webフィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	Webフィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】	Webフィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】				
113				2.	上記の内部不正の通報制度について教育を実施します。	カスタムメイド研修【NEC ラーニング】	情報セキュリティマネジメントサービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】											
114				3.	通報窓口(ホットライン等も含む)には、従業員が所属する部門長以外の窓口を設置することが望まれます。	情報セキュリティマネジメントサービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】												
115				4.	通報者が通報行為により不利益を受けないように匿名性を確保するため、匿名の私書箱や目安箱等を設置することや、第三者機関等の利用も検討することを考えます。	情報セキュリティマネジメントサービス【ディアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】												

11 6		(30)	内部不正対策の項目を抽出し、確認（内部監査等の監査を含む）し、確認した結果は、経営者に報告し、必要に応じて対策の見直しを実施していますか？	1.	内部不正対策として特に実施することが望まれる項目（内部不正事例等で関連すると思われる事項）を参照し、具体的な対策の実施状況や整備状況等を確認し、経営者（経営陣）に報告する必要があります。	InfoCage セキュリティリスク管理【NEC】	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】								
11 7				2.	各部門の業務内容や関係者との取り決めによって、同様の情報についても異なる管理や取扱が行われていないか等を確認する必要があります。	情報セキュリティマネジメントサービス【ディアアイティ】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】									
11 8				3.	内部不正と思われる事象や関連する事件・事故等の記録を確認し、それらの発生後に速やかに報告されているかを確認する必要があります。また、重要情報の管理手順や取扱方法に違反した事例の有無や、その後の対処方法等を確認する必要があります。	InfoTrace PLUS【NEC(ソリトンシステムズ)】	Webフィルタリングソフト「InterSafe WebFilter」【NEC(アルプスシステムインテグレーション)】	Addpoint/MailWall Server【NEC(キャノン IT ソリューションズ)】	情報セキュリティマネジメントサービス【ディアアイティ】	NetEvidence【NEC(オーク情報システム)】	GUARDIANWALL【NEC(キャノン IT ソリューションズ)】	AlogConverter【NEC(網屋)】	情報セキュリティマネジメント支援サービス/IT統制の整備・改善支援コンサルティング【みずほ情報総研】	Webフィルタリングソフト「InterSafe WebFilter」【アルプスシステムインテグレーション】		

6. ワーキンググループメンバー

2013年11月7日時点

氏名	社名
甘利 康文（リーダー）	セコム株式会社 IS 研究所
田中 洋	株式会社インフォセック
岡 憲明	株式会社インフォセック
佐佐木 賢二	グローバルセキュリティエキスパート株式会社
芳賀 政伸	グローバルセキュリティエキスパート株式会社
宮崎 亮	株式会社 JMC
内田 順一	セコム株式会社 IS 研究所
松本 泰	セコム株式会社 IS 研究所
新井 真司	セコム株式会社 IS 研究所
山田 英史	株式会社ディアイティ
遠藤 美貴恵	ドコモ・システムズ株式会社
藤原 隆徳	ドコモ・システムズ株式会社
小屋 晋吾	トレンドマイクロ株式会社
小原 哲也	トレンドマイクロ株式会社
岡本 勝之	トレンドマイクロ株式会社
林 憲明	トレンドマイクロ株式会社
栗津 朱実	トレンドマイクロ株式会社
島 成佳	日本電気株式会社 クラウドシステム研究所
塚田 孝則	株式会社日立ソリューションズ
小川 博久（本ガイド編集担当）	みずほ情報総研株式会社
村上 晃	株式会社ラック
眞田 みずき	フューチャーアーキテクト株式会社
野津 秀穂	大日本印刷株式会社
高橋 潤（オブザーバー）	株式会社リンク アンド モチベーション モチベーションマネジメントカンパニー
益子 るみ子（オブザーバー）	独立行政法人情報処理推進機構 技術本部セキュリティセンター



内部不正対策ソリューションガイド

2013年12月26日

特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）

調査研究部会 組織で働く人間が引き起こす不正・事故対応ワーキンググループ 編著

（お問い合わせ先）

特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）事務局

〒105-0003 東京都港区西新橋1-22-12 JCビル3階

TEL:03-3519-6440 FAX:03-3519-6441 E-Mail:sec@jnsa.org
