クラウドサービス移行における情報セキュリティ上の留意点

情報処理推進機構(IPA) セキュリティセンター

クラウドサービスのセキュリティ

- クラウドセキュリティには２つあります
  - クラウドコンピューティングセキュリティ
    - クラウドのインフラに関するセキュリティです。ネットワークやハードウェアの仮想化などの技術に対するセキュリティを主に指しています
    - プライベートクラウドなどを構築する際に留意します
  - クラウドサービスセキュリティ
    - クラウドコンピューティングの欠点などを運用によってカバーしているのがクラウドサービスです
    - 多くの場合は、セキュリティ上の問題を解決できるような運用が実施されています

クラウドサービスにおける事故の現状

調査事例の発生年別内訳

発生年	件数
2011年	20
2012年	31
合計	51

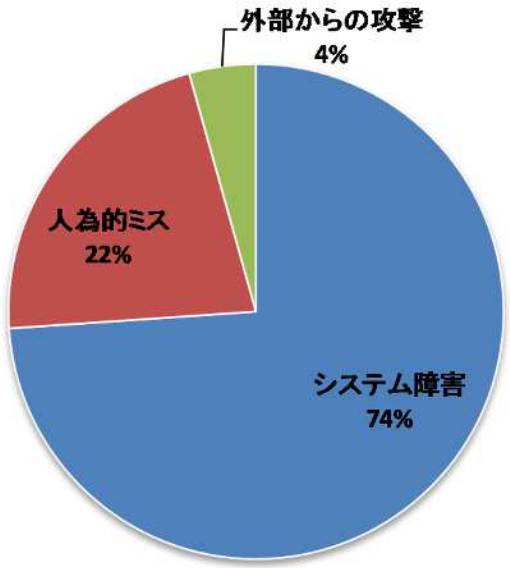
調査事例の発生国・地域の内訳

国または地域	件数
米国	35
日本	12
韓国	2
カナダ	1
欧州	1
合計	51

調査事例の問題別内訳

問題の分類		件数
障害（悪意なし）	①ソフトウェア	12
	②ハードウェア	3
	③設計	3
	④運用・管理	9
	⑤ファシリティ	7
攻撃（悪意あり）	⑥サービス妨害	1
	⑦不正アクセス	9
	⑧その他	1
⑨非公開		6
合計		51

国内における調査結果



トラブル原因分類	件数
システム障害	17
人為的ミス	5
外部からの攻撃	1

- システム障害
  - ハードウェア、ソフトウェアのトラブル
  - ネットワークへの高負荷が最も多く、サービスが停止したり、資産の一部が失われた
- 人為的ミス
  - 作業ミスなどによるデータの滅失など
  - 運用手順が明確で無い為に発生した
  - ネットワークキャリアとのコミュニケーション不足
- 外部からの攻撃
  - DDoS攻撃があるが、実害は少ない

ユーザが行うべきことはなにか

- クラウドサービスはインフラとなっている
  - 電車が遅れてしまった時のために、飛行機が飛ばなかった時のために普段何をしているのかを考えてみる
  - インフラが止まってしまう可能性はゼロではない
- ユーザーが行うべきことはなにか
  - 万が一に備えたバックアップ
    - システムの復旧時に対応できるバックアップデータを用意
    - 復旧にかかる時間の確保を検討する
  - 管理者ID、個人IDのセキュリティ
    - 単純なIDとパスワードの組み合わせではなく、二段階認証や多要素認証ができるかを検討する

経済産業省
Ministry of Economy, Trade and Industry

企業のクラウドサービス利用に際しての最新事例に対応！「クラウドセキュリティガイドライン改訂版」と「活用ガイドブック」を作成しました

本件の概要

経済産業省では、平成23年に公表した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン（以下、ガイドライン）」を改訂いたしました。

初版の公開以来、クラウドサービスの本格的な普及が進む一方、国内外のサービスで 大規模な障害や障害対応過程での情報漏えいの発生等、リスクが顕在化した事例が見受けられるようにもなりました。クラウドサービスを取り巻くこうした環境の変化を踏まえ、 所要の追加等を行いました。

また、本ガイドラインが広く利用されることを期待して、ガイドラインの利用のシーンを具体的に示す「クラウドセキュリティガイドライン活用ガイドブック（以下、活用ガイドブック）」 を新たに作成しました。

本ガイドラインに併せ、活用ガイドブックを利用することで、安心してクラウドサービスを利用できる環境の整備に貢献することを目指します。

1. 検討の背景

経済産業省は、情報セキュリティ確保のためにクラウド利用者自ら行うべきことと、クラウド事業者に対して求めるべきことをまとめたガイドラインを平成23年4月に公表しました。

ガイドライン作成当時に想定されていたリスクにしたがって、クラウドサービス利用者および 事業者が対策すべき事項を整理しましたが、クラウドサービスが多様化し、急速にサービスが普及し、また、国内外で大規模な障害が発生する等情報セキュリティのリスクが顕在化し、 クラウドサービスを取り巻く環境が著しく変化したため、現状に合わせた内容の追加等を行いました。

本ガイドラインは、様々なシーンで活用できる標準的な内容である反面、具体的な対策と事例が欲しいという意見がありました。そこで、新たに「活用ガイドブック」を作成して、クラウド サービス利用におけるそれぞれのリスクに対して解説をするとともに、クラウドセキュリティガイドラインの参照先を示すこととしました。

調査事例の発生年別内訳

発生年	件数
2011年	20
2012年	31
合計	51

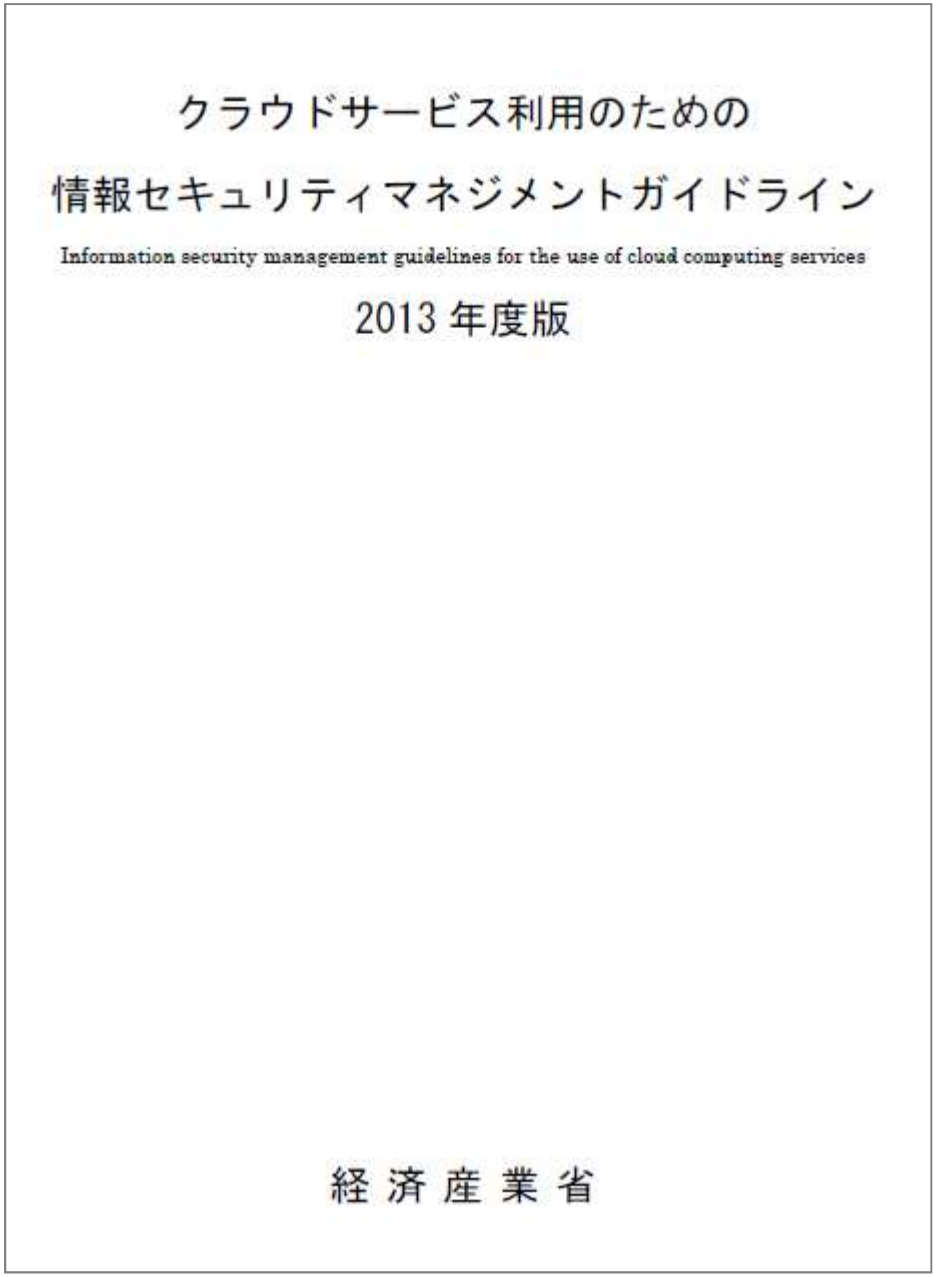
調査事例の発生国・地域の内訳

国または地域	件数
米国	35
日本	12
韓国	2
カナダ	1
欧州	1
合計	51

調査事例の問題別内訳

問題の分類		件数
脆弱（悪意なし）	①ソフトウェア	12
	②ハードウェア	3
	③設計	3
	④運用・管理	9
	⑤ファシリティ	7
攻撃（悪意あり）	⑥サービス妨害	1
	⑦不正アクセス	9
	⑧その他	1
⑨非公開		6
合計		51

http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html


クラウドサービス利用のための
情報セキュリティマネジメントガイドライン
Information security management guidelines for the use of cloud computing services
2013 年度版
経 済 産 業 省


クラウドセキュリティガイドライン
活用ガイドブック
２０１３年度版
経済産業省 商務情報政策局
情報セキュリティ政策室

クラウドセキュリティ活用ガイド

- ガイドラインに触れてもらうために
  - ガイドラインはJIS Q 27002をベースとしたために、慣れていない方には読みにくいものとなってしまった
  - 活用ガイドブックはガイドラインの解説ではなく、ガイドラインの使い方について説明しており、これをきっかけにガイドラインを活用してほしいという思いで作成している
  - 「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」のさらなる活用のために、最新のインシデント事例を前提としたガイドラインの利用を作成しました
- 利用者だけではなく事業者にも
  - 利用者だけではなく、事業者にも利用していただけるように、それぞれの活用シーンを事例として提供し、ガイドラインを様々な用途で利用していただけるように解説しています

http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html

活用ガイドブックの構成

1. はじめに
クラウドサービス利用におけるインシデントの調査をもとに、インシデントの傾向と対策を解説

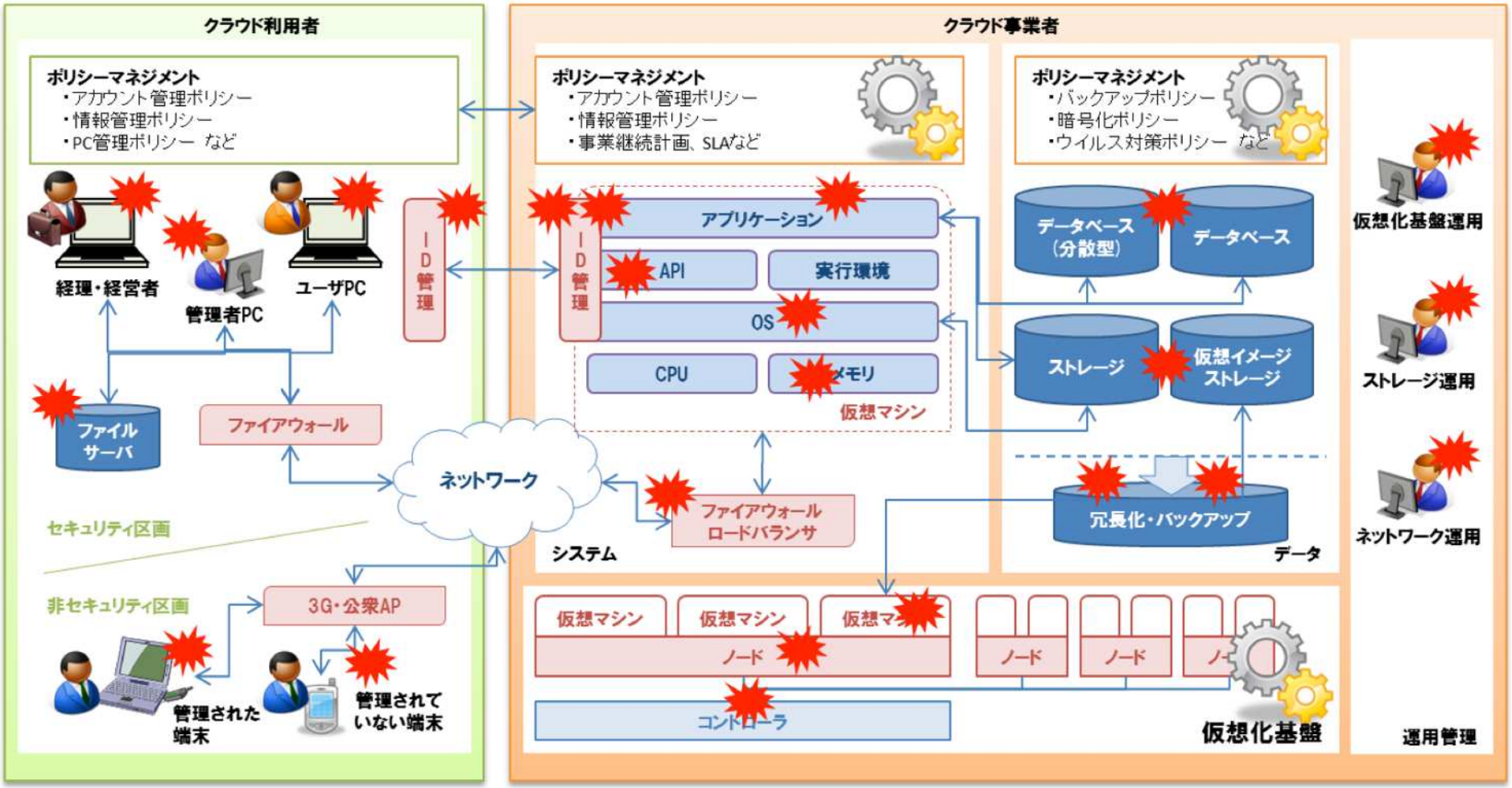
2. クラウドセキュリティとは
クラウドの構造を解説し、構造上の問題点や運用上の問題点などを明確にし、事故が発生する原因や利用者や事業者の責任を明確にする

3. クラウドサービスにおけるリスク
クラウドの構造やインシデントを受けて、クラウドサービスにおける様々なリスクについて解説するとともに、クラウドセキュリティガイドラインの参考となる項番を参照し、重点的な対応ができるようなガイドとしている。
調査結果を前提とした内容としており、ガイドラインの重点項目などがわかるような構成としている

4. クラウド利用者のためのガイドライン活用
クラウドサービスを利用したシステム構築、クラウド事業者の選択、クラウドサービスの契約、インシデントレスポンスの４つのポイントについて、利用者目線での解説を行なっている。巻末には事業者、利用者共に活用できる「契約書のサンプルと解説」、「サービスレベル合意のサンプルと解説」を用意した。

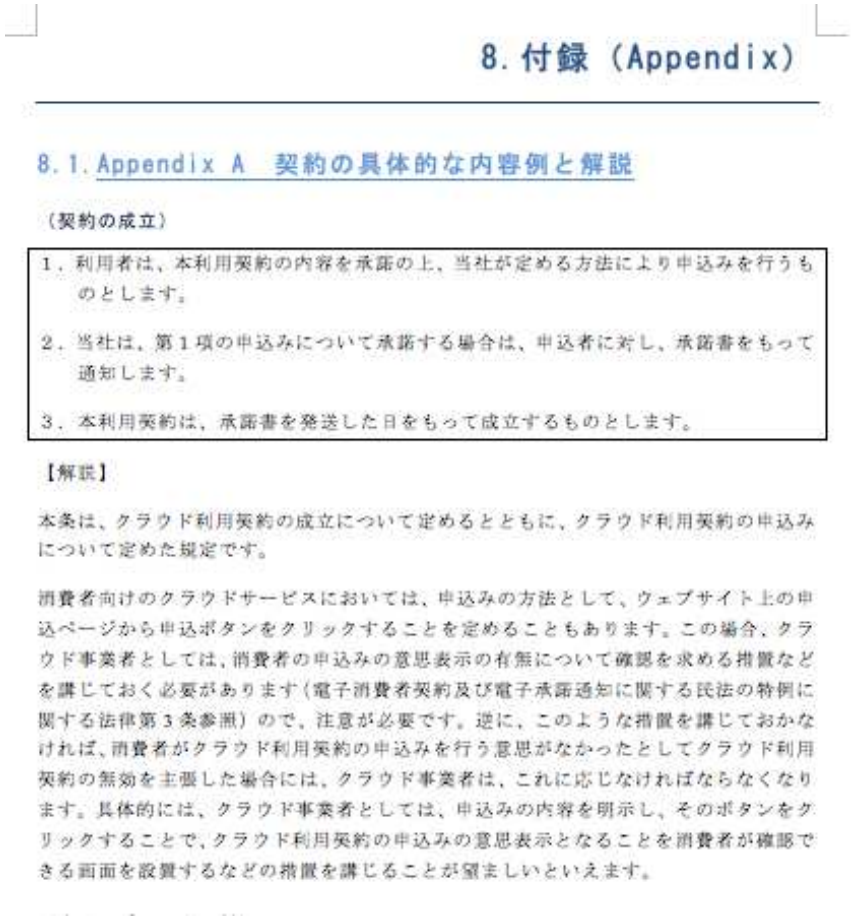
5. クラウド事業者のためのガイドライン活用
クラウドサービスの構築、セキュリティホワイトペーパーの活用、第三者認証の活用、監査の４つのポイントについて、事業者目線での解説を行なっている。利用者に安全にサービスを提供するための情報発信だけではなく、事業者組織の情報セキュリティマネジメントについても解説している。

クラウドサービスにおけるリスク



ガイドラインを活用したリスク分析

契約書のサンプルとSLAのサンプル



8. 付録（Appendix）

8.1. Appendix A　契約の具体的な内容例と解説

（契約の成立）

1．利用者は、本利用契約の内容を承諾の上、当社が定める方法により申込みを行うものとします。

2．当社は、第１項の申込みについて承諾する場合は、申込者に対し、承諾書をもって通知します。

3．本利用契約は、承諾書を発送した日をもって成立するものとします。

【解説】

本条は、クラウド利用契約の成立について定めるとともに、クラウド利用契約の申込みについて定めた規定です。

消費者向けのクラウドサービスにおいては、申込みの方法として、ウェブサイト上の申込ページから申込ボタンをクリックすることを定めることもあります。この場合、クラウド事業者としては、消費者の申込みの意思表示の有無について確認を求める措置などを講じておく必要があります（電子消費者契約及び電子承諾通知に関する民法の特例に関する法律第３条参照）ので、注意が必要です。逆に、このような措置を講じておかなければ、消費者がクラウド利用契約の申込みを行う意思がなかったとしてクラウド利用契約の無効を主張した場合には、クラウド事業者は、これに応じなければならなくなります。具体的には、クラウド事業者としては、申込みの内容を明示し、そのボタンをクリックすることで、クラウド利用契約の申込みの意思表示となることを消費者が確認できる画面を設置するなどの措置を講じることが望ましいといえます。

- 付録に契約書とSLAのサンプルを付けました
  - 契約の具体的な内容例と解説
  - SLAに関する解説と例示
- 事業者が契約や約款を作る際の参考に
  - 小規模事業者などが積極的にサービスを提供できるようにこのようなサンプルを提供している

IPAの資料をご活用ください

そのまま社内研修に使える情報が満載です。

http://www.ipa.go.jp/security/antivirus/shiori.html

動画もたくさんご用意しています

～約10分間のドラマ・アニメ・報道特集等を通して情報セキュリティを学べる

3つのかばん
－新入社員が知るべき情報漏えいの脅威－

＜乗っ取り＞の危険が
あなたのスマートフォンにも！

あなたの書き込みは世界中から
見られてる －適切なSNS利用の心得－

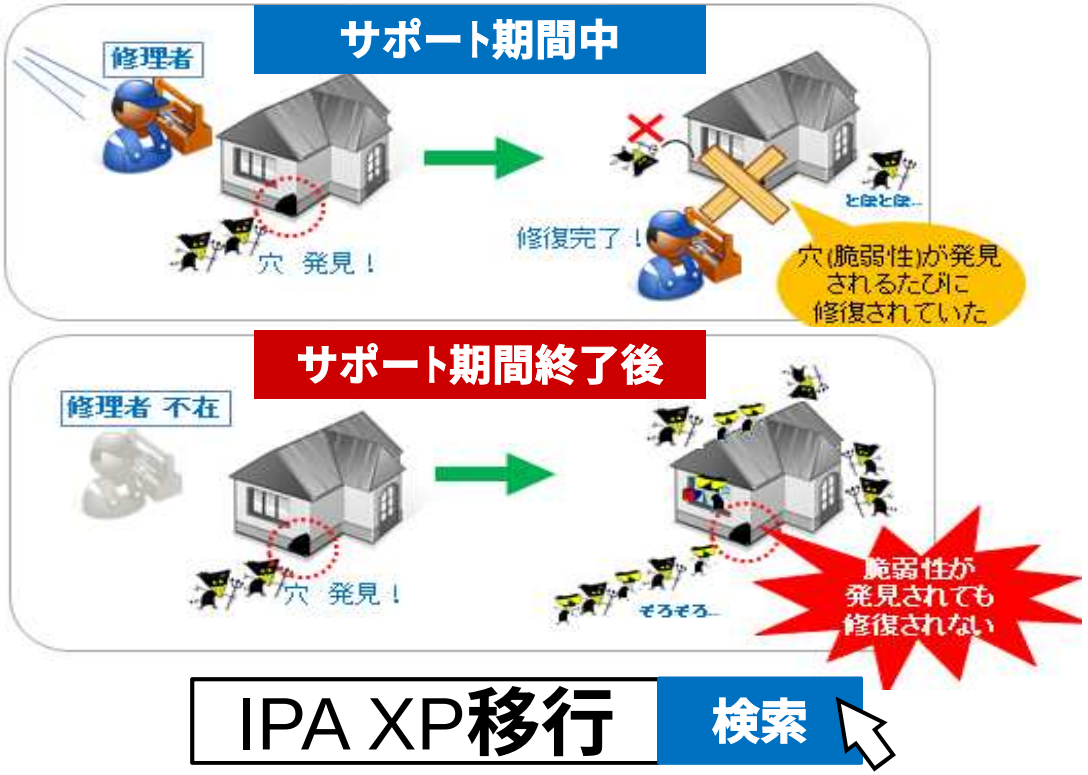
その他のタイトル

- ウイルスはあなたのビジネスもプライベートも狙っている！
- あなたの組織が狙われている！-標的型攻撃 その脅威と対策-
- 大丈夫？あなたのスマートフォン -安心・安全のためのセキュリティ対策-
- あなたのスマートフォン、ウイルスが狙っている！
- ワンクリック請求のワナを知ろう! -巧妙化する手口とその対策-
- 今　制御システムも狙われている！ -情報セキュリティの必要性-
- 東南アジアの情報セキュリティ -現状と対策について-
- 7分で気づく身近にある情報漏えいの脅威
- キミはどっち？ -パソコン・ケータイ・スマートフォン 正しい使い方-
- ほんとにあったセキュリティの話

http://www.ipa.go.jp/security/keihatsu/videos/

IPAからのお願い

Windows XPのサポートが、2014年4月9日に終了しました。
まだ移行していない方は、不正アクセス等を回避するためサポートの継続する後継OS、または代替OSへの移行が望まれます。



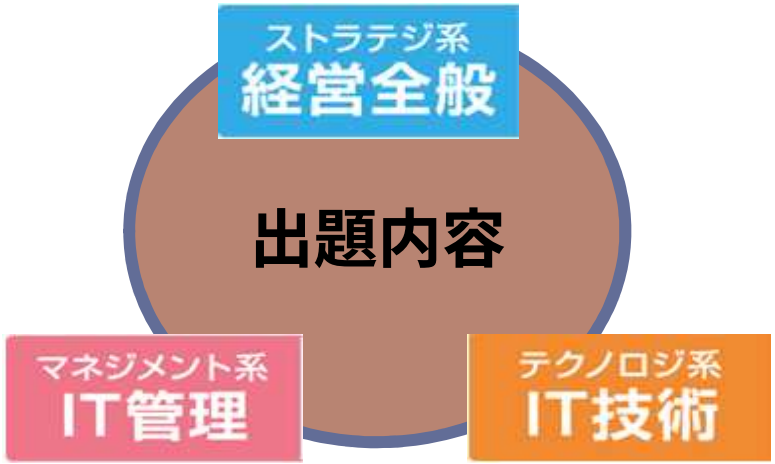
IPA XP移行 検索

企業・社員の情報セキュリティ対策、コンプライアンス向上に！！

ITパスポート試験 （iパス）

IPA

ＩＴを利活用する**すべての社会人・学生**のための**国家試験**



iパス公式キャラクター
上峰　亜衣

情報セキュリティ対策の重要性の高まりを踏まえ、
情報セキュリティの出題を強化！

i パス　検索

本資料に関するお問い合わせは・・・

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
http://www.ipa.go.jp/security

情報セキュリティ安心相談窓口
http://www.ipa.go.jp/security/anshin
anshin@ipa.go.jp