情報セキュリティマネージャー
ISACAカンファレンス 2013 in Tokyo

LAC
安心とともに

新たな脅威に対する 情報セキュリティマネージャーの役割

LAC
Security
Academy

2013年10月26日(土)

株式会社ラック
セキュリティアカデミー
長谷川　長一

株式会社ラック

長谷川　長一（はせがわ　ちょういち）

株式会社ラック　セキュリティアカデミー　プロフェッショナル・フェロー
NPO 日本ネットワークセキュリティ協会(JNSA) 教育部会WGリーダー
同　SNSセキュリティWGメンバー

■ソフトバンク、日本ユニシスを経て、現職。情報セキュリティコンサルティング、情報セキュリティ監査業務を経て、現在は主にセキュリティ教育業務を担当。

■主な担当講師業務
- □(ISC)2 CISSP/SSCPレビューセミナー認定主任講師
- □CompTIA Security+講師
- □東京電機大学 未来科学部 非常勤講師
- □岡山理科大学 総合情報学部 情報科学科 特別講師

■最近の主な活動（2013年10月まで）
- □ 総務省 高度ICT利活用人材育成会議 委員
- □ 経済産業省 情報セキュリティ人材の育成指標等の作成事業 WG委員
- □ 文部科学省 中核的専門人材養成の戦略的推進事業 WG委員
- □ 警察庁 不正アクセス防止対策に関する官民意見集約委員会 WG委員

■主な著書等
「情報セキュリティプロフェッショナル教科書」（アスキーメディアワークス、共著）、「SSCP認定資格公式ガイドブック」（NTT出版、共著）　等。

E-mail : choichi.hasegawa@lac.co.jp
twitter : @ChoichiHasegawa,　　http://www.facebook.com/choichi.hasegawa

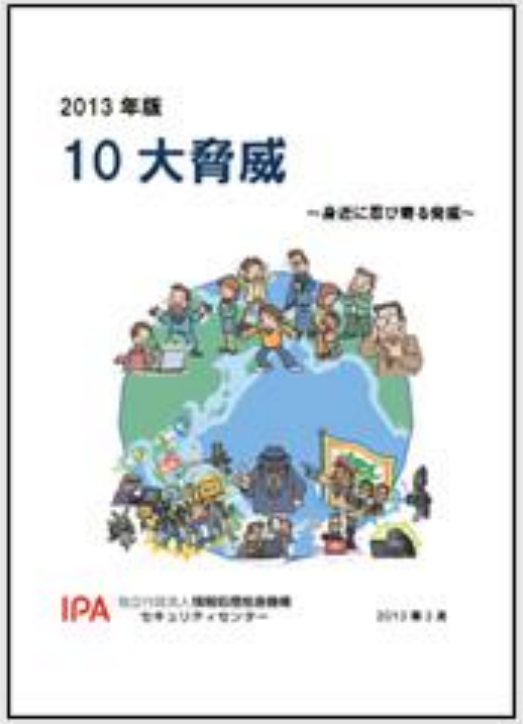
LAC
安心とともに

1.最新の脅威の動向（今、そこにあるリスク）

LAC
Security
Academy

株式会社ラック

<参考>「2013年版 10大脅威～身近に忍び寄る脅威～ 」



1	クライアントソフトの脆弱性を突いた攻撃
2	標的型諜報攻撃の脅威
3	スマートデバイスを狙った悪意あるアプリの横行
4	ウイルスを使った遠隔操作
5	金銭窃取を目的としたウイルスの横行
6	予期せぬ業務停止
7	ウェブサイトを狙った攻撃
8	パスワード流出の脅威
9	内部犯行
10	フィッシング詐欺

脅威は、常に
変化している

～「 2013年版 10大脅威　身近に忍び寄る脅威」
http://www.ipa.go.jp/security/vuln/10threats2013.html

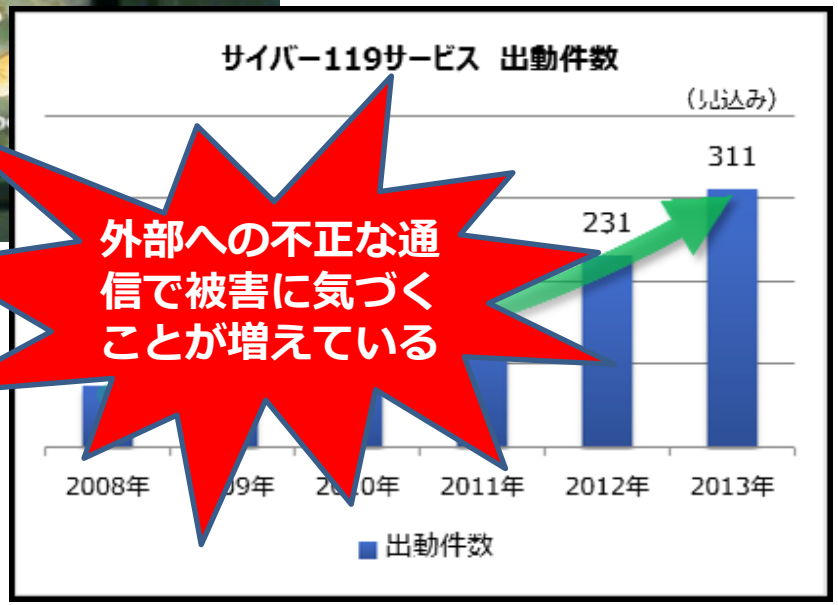
LAC

攻撃はどこから来るのか？

- 365日24時間、世界中から攻撃がやってくる

～LAC監視センター「JSOC」のネットワーク監視の映像

～LACサイバー救急センターの出動実績



相次ぐ、不正ログイン、改ざん

» 2013年06月19日 22時35分 更新

詳細はなお調査中：

[redacted]のWebサイトが改ざん、1週間以上不正プログラムが実行される状態に

トヨタ自動車は2013年6月18日、同社Webサイトが不正アクセスを受け、改ざんされていたこと らかにした。

ツイート 77 B! 39 いいね！ 49 +1 5 投稿 共有 プリント／アラート

[redacted]は2013年6月18日、同社Webサイトが不正アクセスを受け、改ざ ていたことを明らかにした。改ざんされたページにアクセスした場合、マルウ した可能性があることから、同社ではウイルス対策ソフトを最新の状態にアップデ し、感染の確認と駆除を行うよう推奨している。

サイトが改ざんされていたのは、6月5日18時26分から6月14日21時47分までの間。「http://[redacted].jp/jp/news/」以下のコンテンツ、具体的にはニュースやIR情報、CSR情報などに関するコンテンツが改ざんされ、不正なプログラムが自動的に実行される状態になっていた。同社では当該サーバの運用を停止し、セキュリティ対策を た上で7月上旬に復旧させる予定という。

原因は第三者による不正アクセスだが、どういった経路で侵入を受けたか、1週間以 の間改ざんに気付かなかったのはなぜかなど、詳細については調査中という。なお、[redacted]jp」以外のサーバでは、問題は発生していないという。

自動車メーカー大手のトップページ「最新ニュース」からアクセス可能だった。

この間にニュースコンテンツを閲覧した場合、不正プログラムが自動的に実行される状態になっていた。（約78,000人が感染か）

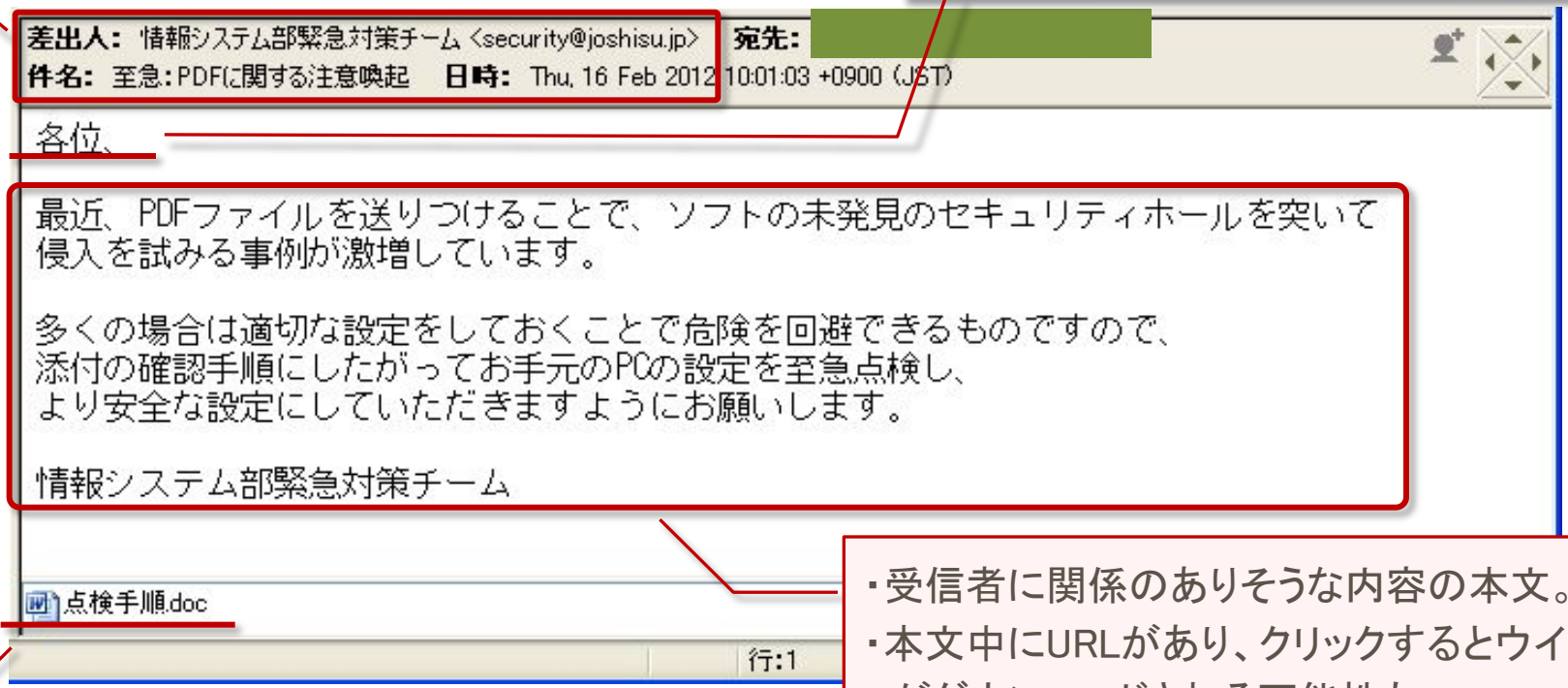
報道されているのは、あくまで「氷山の一角」。組織の種類や規模に関係なく手当たり次第に攻撃。

http://www.atmarkit.co.jp/ait/articles/1306/19/news161.html

標的型攻撃メール

・件名を存在する部署、個人名などに偽装する。
・受信者に関係のありそうな件名。
・「至急」「急ぎ」など、受信者を急がせることも。

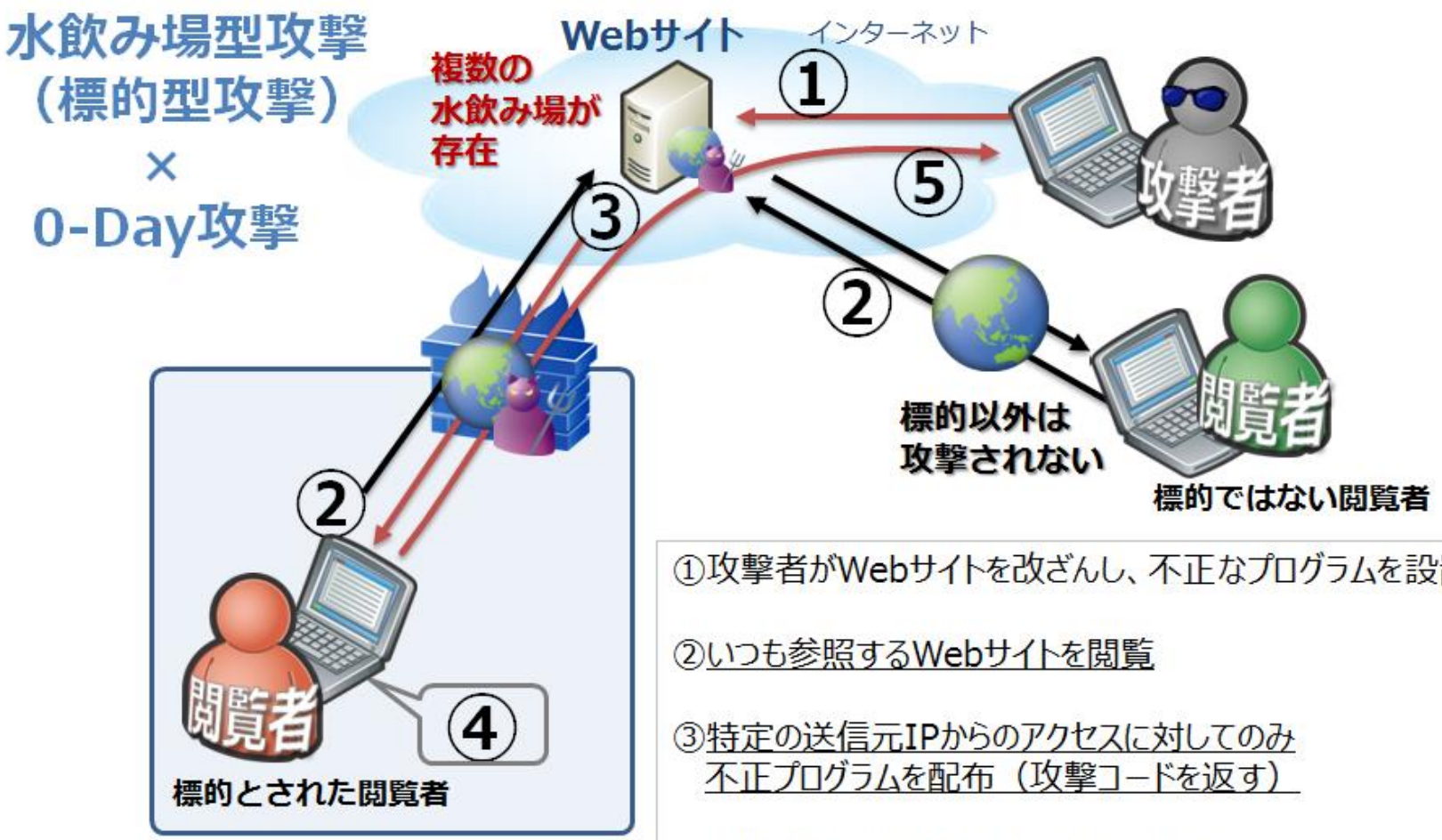
・不特定多数を狙ったものの他、受信者の名前が表記されていることもある。



・受信者に関係のありそうな内容の本文。
・本文中にURLがあり、クリックするとウイルスがダウンロードされる可能性も。

・EXEファイルはもちろん、PDF、Word、一太郎PowerPoint、Excelなどのファイルにも注意。

水飲み場型攻撃（watering hole attack）



①攻撃者がWebサイトを改ざんし、不正なプログラムを設置

②いつも参照するWebサイトを閲覧

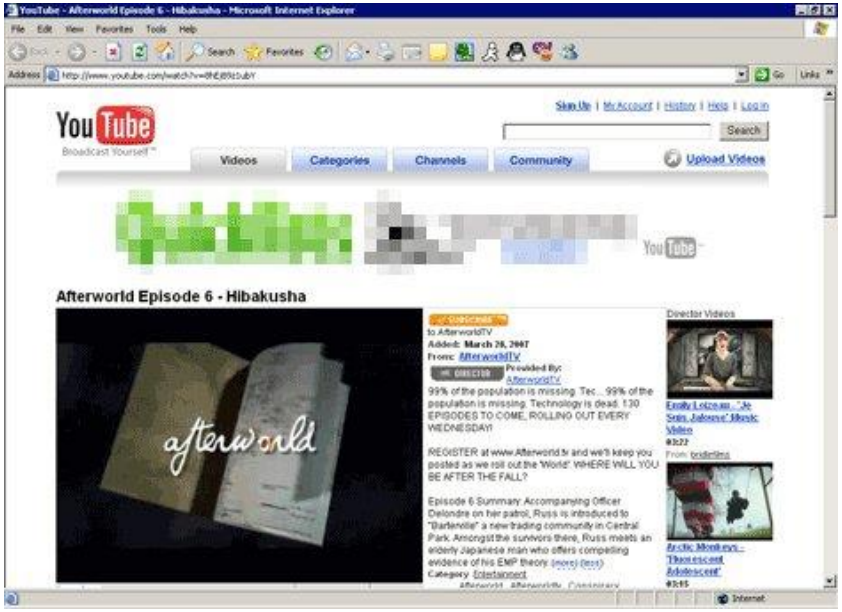
③特定の送信元IPからのアクセスに対してのみ
不正プログラムを配布（攻撃コードを返す）

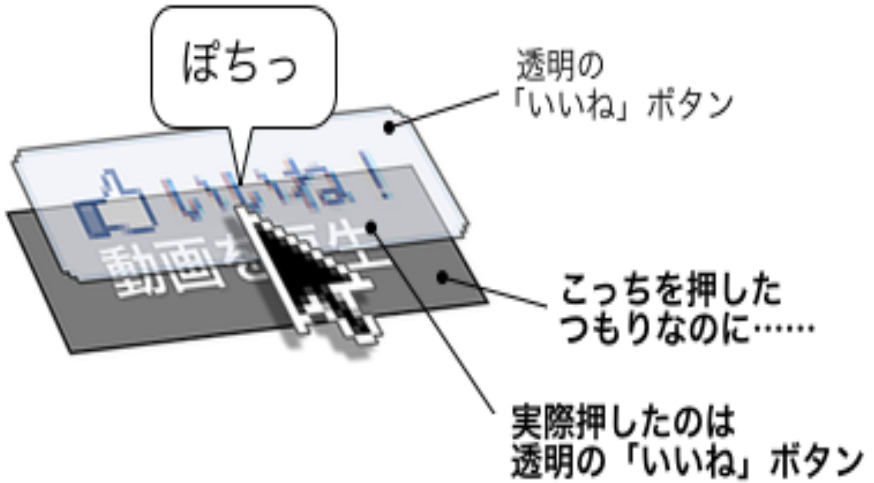
④IE脆弱性を悪用したウイルス感染が成功

⑤攻撃者が用意したサーバへの通信が確立

騙してクリックさせる（クリックジャッキング）

- マルウェアを動作させる、動画のリンクを改ざんする





エロサイトに「いいね」した人がエロサイトを見ていたとは限らない
http://blog.maripo.org/2012/05/like-trap/

動画のリンクが不正なリンクであったり、改ざんされたりした場合、マルウェアサイトに誘導されたりする。動画のリンクそのものを改ざんしたりする。ソーシャルメディアの「いいね！」ボタン等も、要注意。

アカウント乗っ取り（Googleの例）

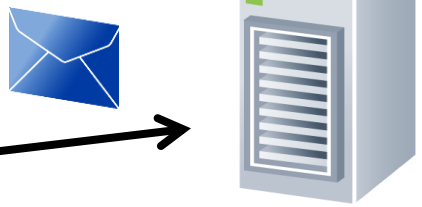
2013年7月22日、Googleアカウントを乗っ取られた方の画面コピー。

多数の不審なアクセス履歴が残っている。

スマートフォンでのマルウェア感染

スマートフォン

スパムメール



メールを送信

ウェブサイト参照

1

ウェブサイト

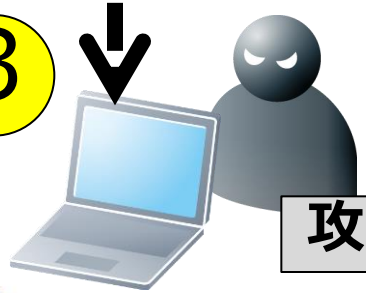
2

メールに添付された
アプリをインストール

・インストールして起動した端末の電話番号や端末識別番号、各種履歴等の窃取
・アドレス帳に登録しているすべてのデータを収集を行い、サーバへアップロードする
・GPSやカメラを起動する

不正操作

3



攻撃者

LAC
安心とともに

2.これからの情報セキュリティマネージャー

LAC
Security
Academy

株式会社ラック

本当にあった話(1)

異動で、情報セキュリティマネージャーになりました。イヤでイヤで仕方ありません。

在任中に重大なインシデントが起こらないことを、毎日ひたすら祈りながら仕事しています。

本当にあった話(2)

会社のWebが改ざんされました。でも、何もできませんでした。

会社に標的型攻撃メールが来ました。でも、何もできませんでした。

というより、正直なところ何が起こったかが未だ理解できません。

本当にあった話(3)

社内ネットワークでマルウェアが蔓延していますが、対応する部署がありません・・・。

重大なインシデントほど、社内をたらい回しになって、対応がどんどん遅れていきます。

ところで、インシデントの原因って？

原因のほとんどは、基本的対策の不備

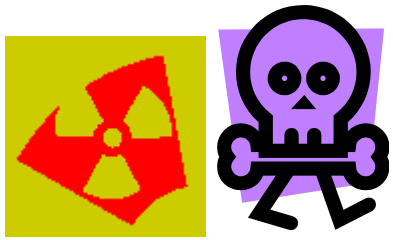
- 標的型攻撃等の脅威の理解が足りなかった（想定なし）
- ファイアウォールの管理者アカウントのパスワードがデフォルトのまま
- ファイアウォール設定の不備（実は”ANY-ANY”だった）
- OS・アプリケーションの最新パッチの未適用
- ウィルス対策システムの定義ファイルの未更新
- Webアプリケーションの脆弱性への未対応
- ID、パスワードの使いまわし
- 不正な外部通信に対しての対応の遅れ（遮断できない）
- インシデント発生時の報告体制や手順の未整備

新しい脅威への対策

- まずは「基本的な対策」をすること。
  - 基本的な対策をできていないのに、応用的な対策などできるはずがない。

- 新たな脅威の理解や想定ができるようにすること。

- （100%防止はできないので）脅威が顕在化した際の対応の仕組みの構築、体制や手順の整備をしておくこと。



経営者とのコミュニケーション

米英IT担当者の64%が脅威を経営陣に報告しないとの調査結果

米TripwireとPonemonは、米英のITセキュリティにかかわる各分野のプロ（担当者）に対して行なったセキュリティマネジメントに関する調査の結果を公開しました。

この調査は、ITセキュリティやIT運用、ITリスク管理、事業運営、コンプライアンス／内部監査、全社的リスいった分野のプロ1320名（米：749名、英：571名）を対象に行われています。

調査結果は以下の通り。

- セキュリティリスクについて経営陣とのコミュニケーションはない、または深刻なセキュリティリスクたときのみ行なっている――64%
- セキュリティリスクの管理と経営との間の連携は乏しいか、全くない、または敵対している――47%
- 関連のあるセキュリティリスクを経営陣に報告・相談しても意味がない――51%

また、「意味がない」理由として以下の4点が挙げられています。

- コミュニケーションがあまりに「サイロ化」している――68%
- コミュニケーションのレベルががあまりに低い――61%
- 情報が技術的過ぎて非技術者であるマネジメント層が理解できない――61%
- ネガティブな事実は上級管理者やCEOに明かされる前にフィルタリングされてしまう――59%

上記に並べた結果だけを見ると、残念な結果としか言えませんが、「現実にはこんなものだろうな」と感じは少なくない、というよりも「ウチと同じだ」と思われている方も多いのではないでしょうか。

・セキュリティリスクについて経営陣とのコミュニケーションはない、または深刻なセキュリティリスクが明らかになったときのみ行なっている　―64%

・セキュリティリスクの管理と経営との間の連携は乏しいか、全くない、または敵対している　―47%

・関連のあるセキュリティリスクを経営陣に報告・相談しても意味がない ―51%

「米英IT担当者の64%が脅威を経営陣に報告しないとの調査結果 」
http://internet.watch.impress.co.jp/docs/column/security/20131004_618137.html

「情報セキュリティマネージャー」の役割

1.情報セキュリティガバナンス

情報セキュリティガバナンスのフレームワークと支持プロセスを確立し維持して、確実に情報セキュリティ戦略が組織の目標と目的と調和し、情報リスクが適切に管理され、プログラム・リソースが責任を持って管理されるようにする。

2.情報リスクの管理とコンプライアンス

情報リスクを許容できるレベルまで管理して、組織の事業要件とコンプライアンス要件を満たす。

3.情報セキュリティプログラムの開発と管理

情報セキュリティ戦略と調和するよう情報セキュリティプログラムを確立し管理する。

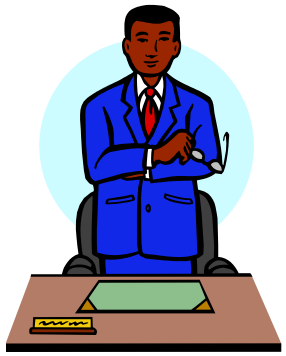
4.情報セキュリティのインシデントの管理

情報セキュリティのインシデントの検知、調査、対応、および復旧を行う能力の計画、確立、および管理を行って、ビジネスへの影響を最小限にとどめる。

~CISM（Certified Information Security Manager） の試験ドメイン

これからは、こうあって欲しい・・・

- 経営陣に、情報セキュリティ活動のビジネスメリットを説明できる。
- ICTの利活用と、情報セキュリティを自ら実践できる。
- 組織の利益や利用者の利便性を優先する。

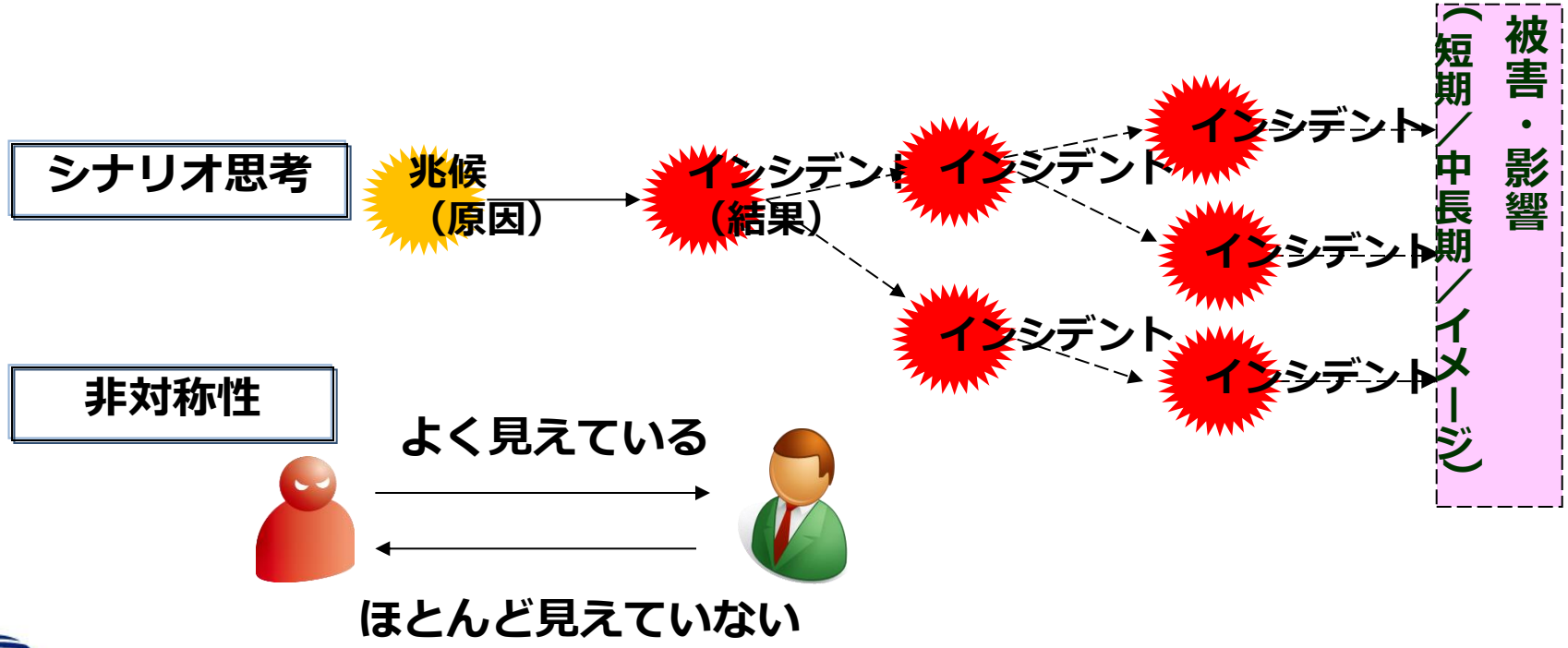


そのためには

- 「実践的」な知識・技術・スキル等を身につけ、維持する。
- 社内外の多くの人と交流し、経験（事例）や情報を共有したり、意見の交換をする。
- 継続的・自律的に研鑽できる
- 常識や慣習にとらわれすぎない

実践的なスキルの例

- 事実を尺度にした思考と判断（特に、緊急時）
- シナリオ思考（多くの不確実性要素のある中でも、予測し、対応する能力）
- 非対称性（不正／攻撃をする側との見え方の違い）への適応



最後に

どんな情報セキュリティマネージャーが必要で、今後も生き残れるのか。

情報セキュリティの「知識」や「技術」だけではなく、組織や市場のニーズと環境の変化に自律的に適応できることが必要。

- 「強い者が生き残ったわけではない。賢い者が生き残ったわけでもない。変化に対応した者が生き残ったのだ」
  ～
  「進化論」、チャールズ・ダーウィン
- 「現状維持では、後退するばかりである」
  ～ ウォルト・ディズニー

Thank you. Any Questions ?

※ この講演における発言、及び資料の内容は、個人の見解であり、所属する企業や団体を代表するものではありません。

LAC