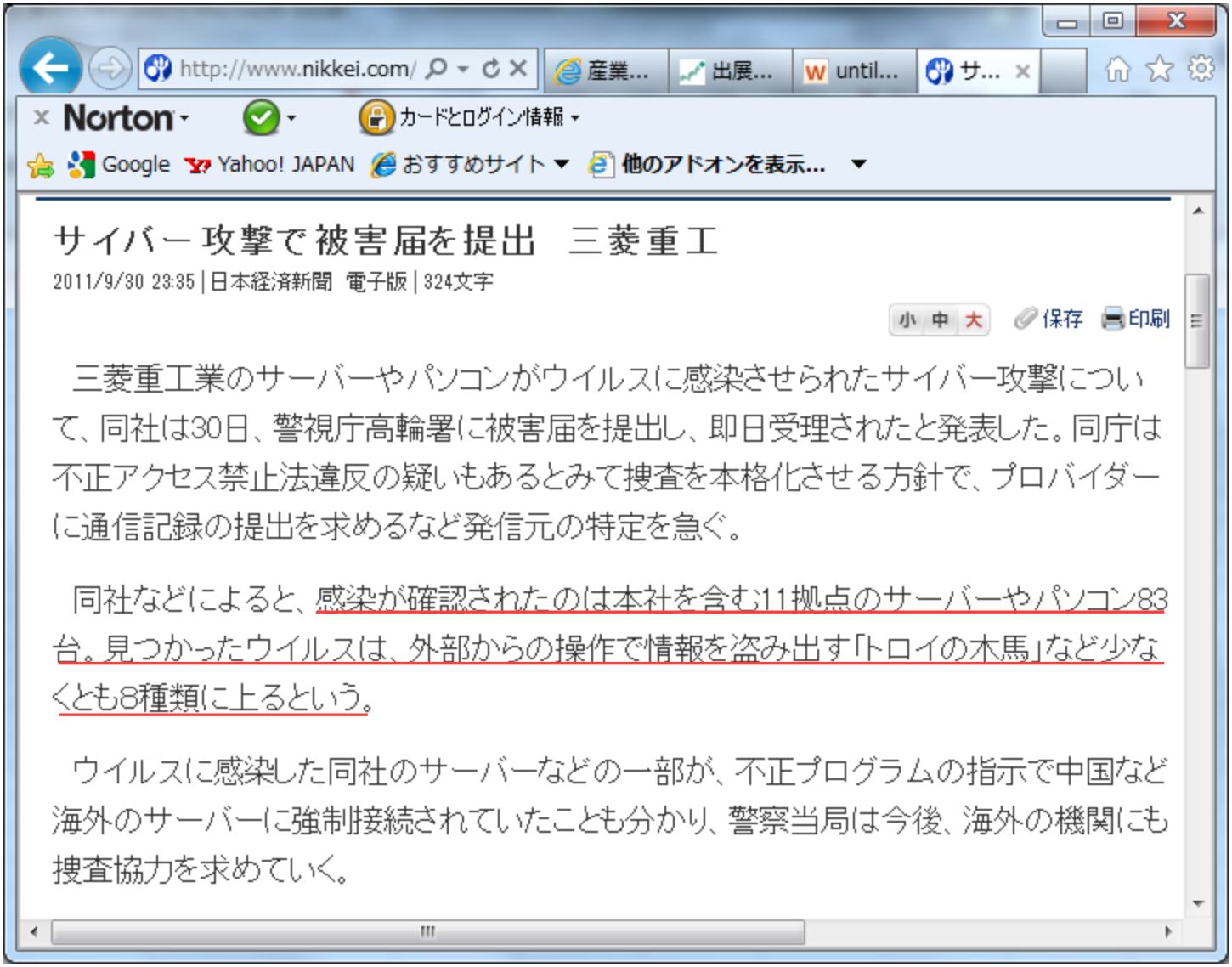
侵入されてないと
みなさんお思いなのです・・・

が

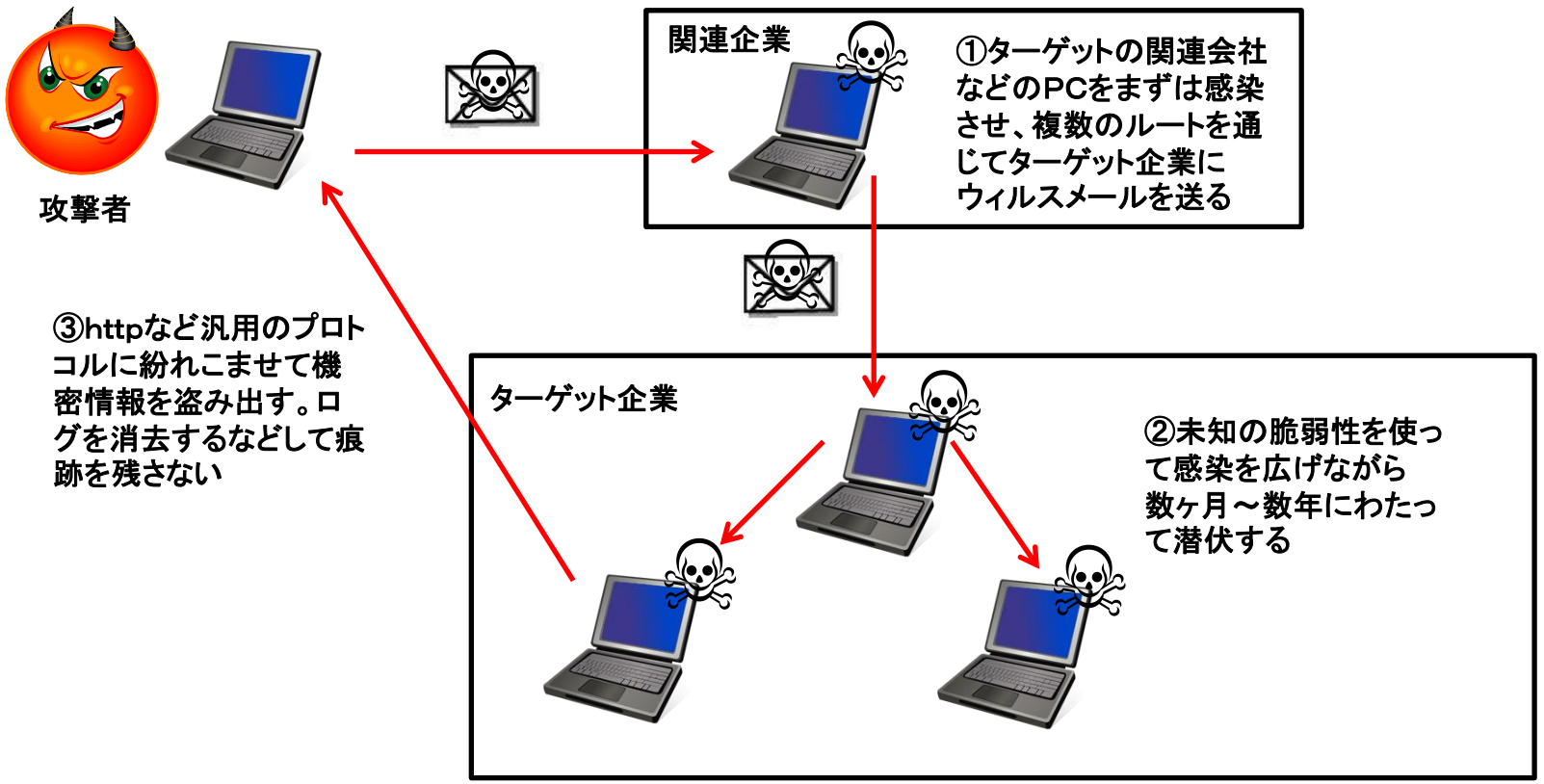
1 三菱重工がサイバー攻撃で被害届（2011/9/30）



三菱重工を襲った「標的型サイバー攻撃」（APT）

新たな脅威となっているのは、特定の企業や団体を狙い撃ちにして機密情報を盗み取る高度なサイバー攻撃、すなわち「APT（Advanced Persistent Threat）攻撃」。

APT攻撃の特徴は、狙った標的に対し、数ヶ月から数年にわたって執拗に攻撃を続けること。



3 「わが社は問題ない」とお思いですか？

1.「ウィルス対策ソフトを全パソコンに導入し、パターンファイルの更新と定期スキャンを全社員に実施させている。これまでに問題は発生していない。わが社にはウィルスは侵入していない。」

➡ APT攻撃はウィルス対策ソフトでは検出できないのです。

2.「わが社には価値の高い情報はないよ。わが社に侵入したってなにも得るものはない。不正侵入の心配なんかいらないよ。」

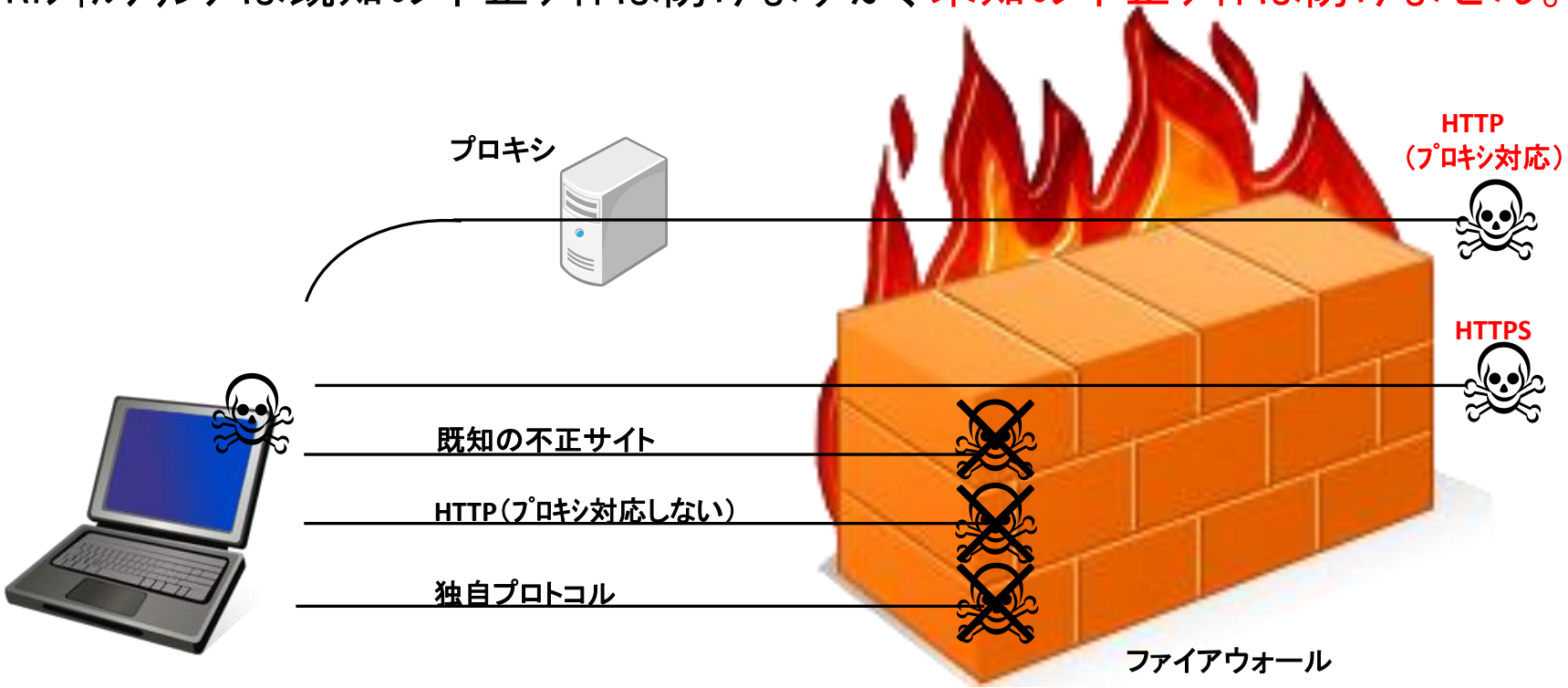
➡ APT攻撃ではターゲット企業の関連企業が最初に狙われるのです。

ファイアウォールとプロキシとURIフィルタリングで遮断している・・・？

ファイアウォールでプロキシ経由以外の通信を遮断して防げるバックドア通信（*1）は、TCPベースの独自プロトコル通信とHTTP（Proxy対応しない）通信のみで、バックドア通信全体の約50%。

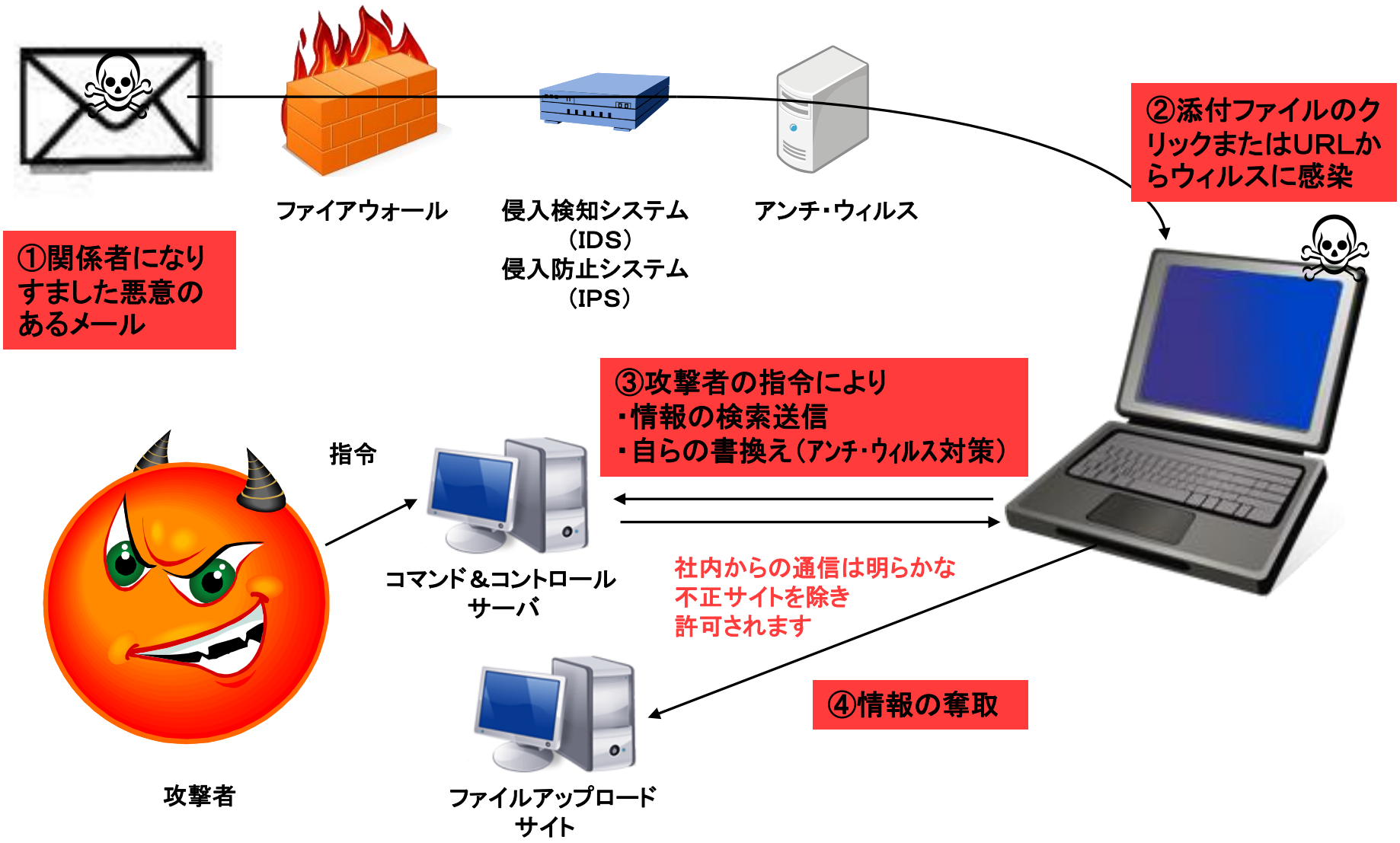
残りの50%（HTTP（Proxy対応）とHTTPS）は防ぐことができません。

URIフィルタリングは既知の不正サイトは防げますが、未知の不正サイトは防げません。



*1：ウィルスによる組織内部からインターネットへの不正通信

標的型サイバー攻撃の典型的手法



なぜ攻撃は成功するのか？

初期攻撃が成功してしまう要因

- ウィルスの種類の多様化
  - ウィルスの件数や亜種の増大
  - 標的型メールのように検知されないウィルスの増加
    （標的にしか送られない，そして動的に姿を変える）
  - 従来のパターンマッチングをベースとしたウィルス対策ソフトの限界
- 多種のソフトウェアの脆弱性が狙われる
  - 標的型メールは一般ユーザが普通に利用するクライアントソフトの脆弱性を狙う
  - 一般ユーザにクライアントソフトのパッチ適用の習慣が薄い
    （たとえば Adobe Acrobat ）
- ゼロデイの脆弱性が狙われる
  - パッチ運用を行っていても攻撃が成立してしまう
- バックドアと外部との通信を遮断できない設計思想
  - 内部から外部への通信は安全と考える従来のネットワークセキュリティ設計を逆手に取った攻撃

防御の第一段階（入口）を突破された場合、二段三段の対策が存在せず、攻撃が成功する

最初の悪意のあるメールをクリックしなければいい？

標的型メールの例

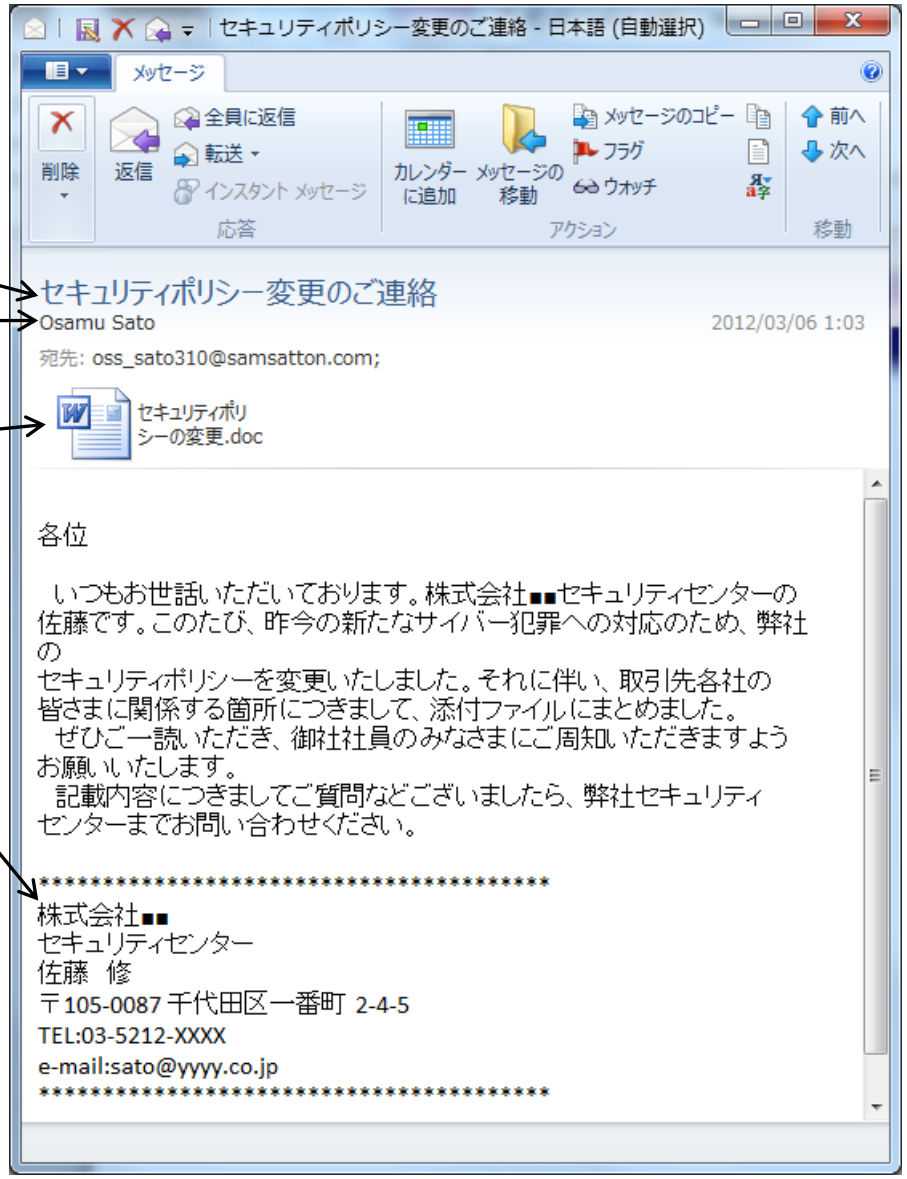
もっともらしいタイトル

実在する送信者
（実在するアドレス）

本文内容に沿った添付ファイル

業務メールと見間違う本文

実在する会社名，住所，電話番号

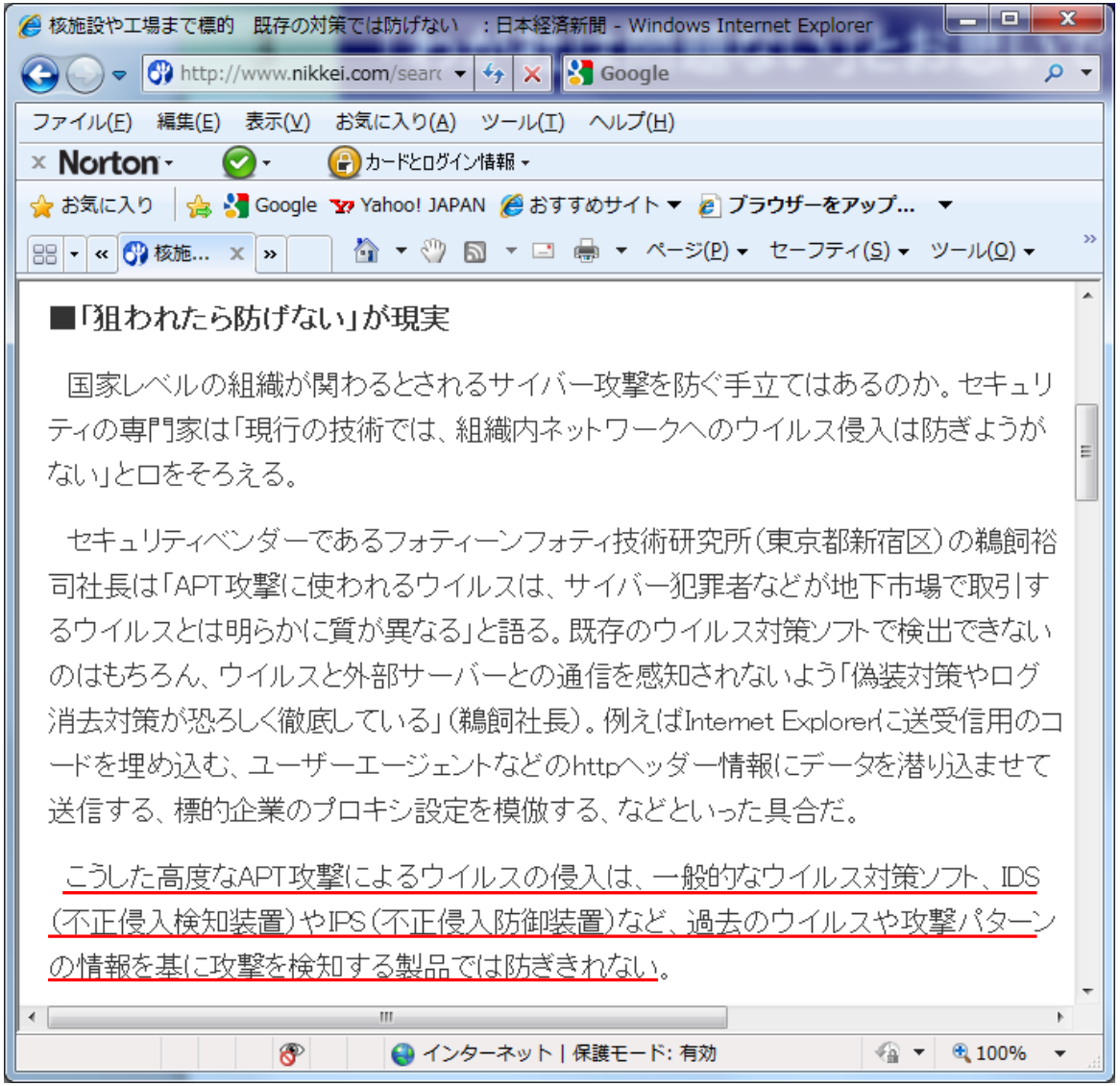


このメールを受信して、ファイルをクリックしない自信はありますか？
社員の誰もクリックしないと言い切れますか？　　し　か　し、

添付ファイルをクリックするだけで（またはハイパーリンクをクリックするだけで）、ウィルスに感染してしまうのです

8 「狙われたら防げない」が現実なのです

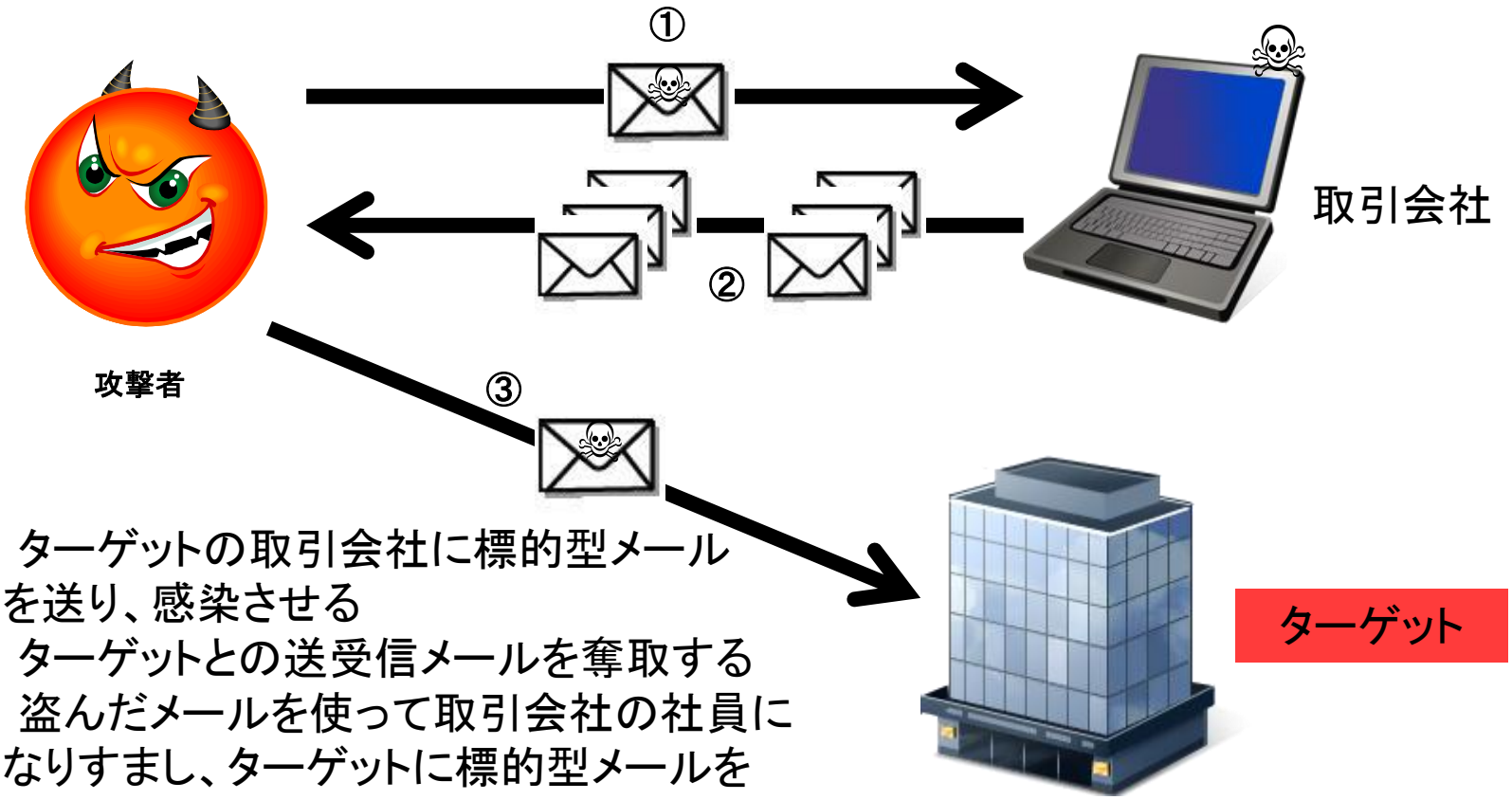
日経コンピュータ
2011年11月24日号
「APT攻撃の脅威」より



「わが社にはそんな貴重な情報はないから心配ない」

いえ、対岸の火事ではないのです

攻撃者はいきなりターゲットを狙わず、関連組織を経由して攻撃することが多い



① ターゲットの取引会社に標的型メールを送り、感染させる
② ターゲットとの送受信メールを奪取する
③ 盗んだメールを使って取引会社の社員になりすまし、ターゲットに標的型メールを送信する

情報の盗み出しだけが目的でもないのです

BOTとは

コンピュータを悪用することを目的に作られたプログラムで、感染するとインターネットを通じて悪意を持った第三者に遠隔操作される悪性プログラムです。

➡ 情報を盗み出すプログラムもBOTのひとつですが、それだけではありません。

ボットに感染したコンピュータは、攻撃者が用意した指令サーバに自動的に接続され数十～数百万台のボット感染コンピュータを従えた「ボットネットワーク」と言われる巨大ネットワークを形成します。

感染したコンピュータは、攻撃者からの命令を待ち続け、攻撃者から命令が下されると、このボットネットワークに接続された感染コンピュータは、攻撃者の意のままにフィッシング目的などのスパムメールの大量送信や、特定サイトへのDDoS攻撃などに利用され、とても大きな脅威となります。

メール添付感染型だけでなく、最近では**Web閲覧感染型**も増えています。

ボットネットを構築し、それを第三者へ売るビジネスもあるといわれています。

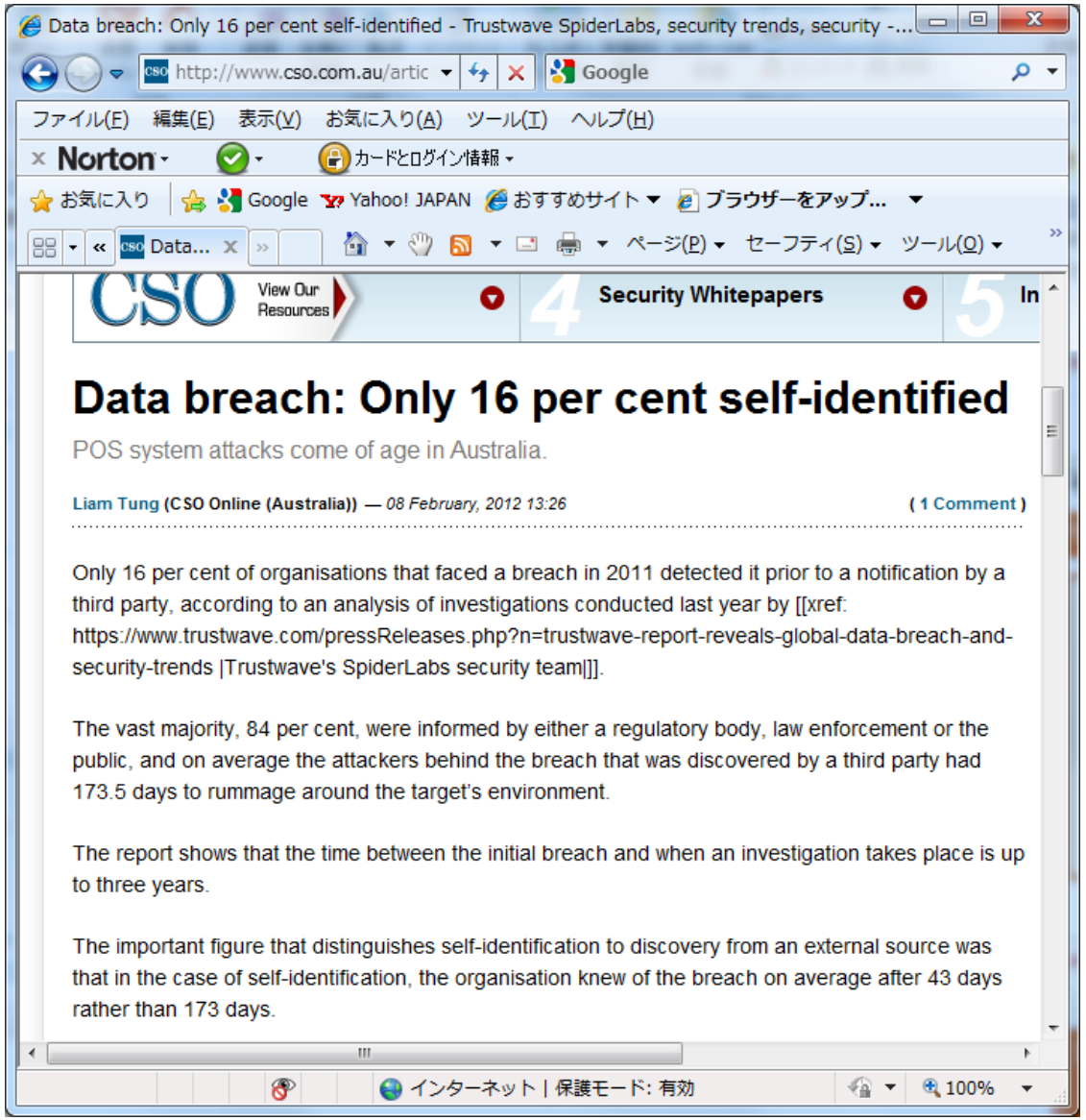
「それでも、わが社は大丈夫だと思うのだが・・・」

Trustwave 社の調査報告

2011年にAPT攻撃を受けた企業の中で、第三者からの指摘を受ける前に自ら攻撃を検知した企業はわずか16%にすぎない。残りの84%は第三者からの指摘によって初めて気づいている。

また、自ら検知した16%の企業が最初のデータ漏洩から漏洩に気づくまでの期間は平均43日だが、第三者の指摘で気づいた84%の企業は173日もかかっている。

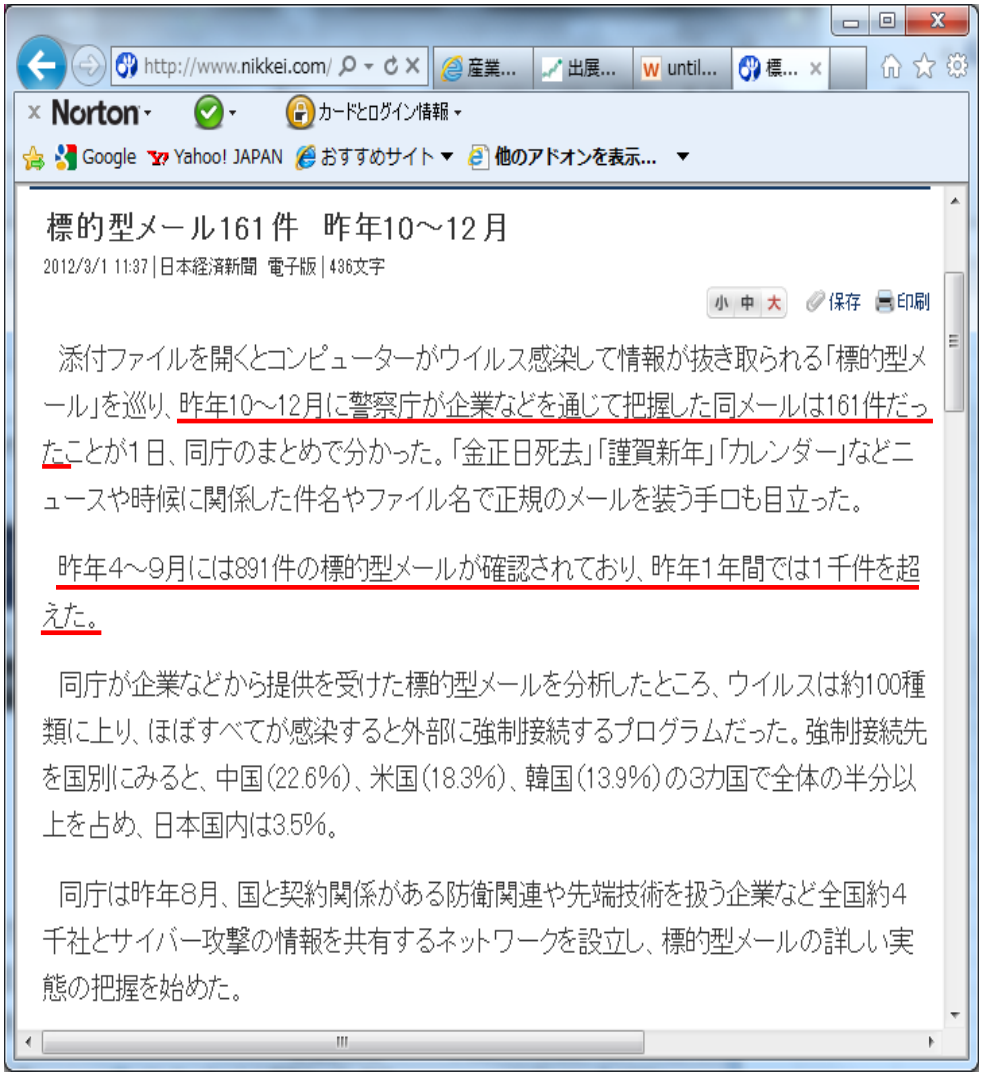
これは気づいた企業だけの話！
気づいてない企業は？？？



12 もちろん日本でも

昨年10月～12月に警察庁が把握した「標的型メール」は161件。昨年１年間では１千件を超えた。

ウィルスは約100種類に上り、ほぼすべてが感染すると外部に強制接続するプログラムだった。強制接続先を国別にみると、中国（22.6%）、米国（18.3%）、韓国（13.9%）の3ヵ国で全体の半分以上を占め、日本国内は3.5%。



標的型メール161件　昨年10～12月

2012/3/1 11:37 | 日本経済新聞 電子版 | 436文字

小 中 大　保存　印刷

添付ファイルを開くとコンピューターがウイルス感染して情報が抜き取られる「標的型メール」を巡り、昨年10～12月に警察庁が企業などを通じて把握した同メールは161件だったことが1日、同庁のまとめで分かった。「金正日死去」「謹賀新年」「カレンダー」などニュースや時候に関係した件名やファイル名で正規のメールを装う手口も目立った。

昨年4～9月には891件の標的型メールが確認されており、昨年1年間では1千件を超えた。

同庁が企業などから提供を受けた標的型メールを分析したところ、ウイルスは約100種類に上り、ほぼすべてが感染すると外部に強制接続するプログラムだった。強制接続先を国別にみると、中国（22.6%）、米国（18.3%）、韓国（13.9%）の3カ国で全体の半分以上を占め、日本国内は3.5%。

同庁は昨年8月、国と契約関係がある防衛関連や先端技術を扱う企業など全国約4千社とサイバー攻撃の情報を共有するネットワークを設立し、標的型メールの詳しい実態の把握を始めた。

まだ安心していられますか？

いま、この瞬間に、みなさまの会社のパソコンやサーバが操作され、漏洩してはいけない顧客データや、会社の機密情報が盗み出されているかもしれません。

盗み出されていないと証明できる根拠がないのです。

攻撃によって受ける
組織の損失を想像してみてください

では、どうすればよいのでしょう

残念ながら、現時点で100%標的型攻撃を防ぐ対策は存在しません

- 入口対策、出口対策にまずは注力
- ネットワーク設計の見直し、再構築も視野に
- 社員教育、情報収集も忘れない

さまざまな効果的な対策を組み合わせて防御力を上げるしかありません

しかし、無限に費用はかけられません

効果的な対策のご提案

標的型メール，ウィルスは、時々刻々姿を変え、新たな脆弱性を突いてきます。これらの攻撃を事前に検知することは実質的に不可能です

だから感染する、これは現時点では仕方ない。
問題なのは、**気づかないこと**

幸いにも、標的型ウィルスには共通の振る舞いがあります。

- **不自然な通信量の増大**
- **侵入路を探すポートスキャン**
- **パスワード取得のための　Brute force attack　（総当たり攻撃）**
- **外部C&Cサーバとの不正通信**

などです。

これらの不自然な通信、つまり、業務と無関係な通信を捕捉する。

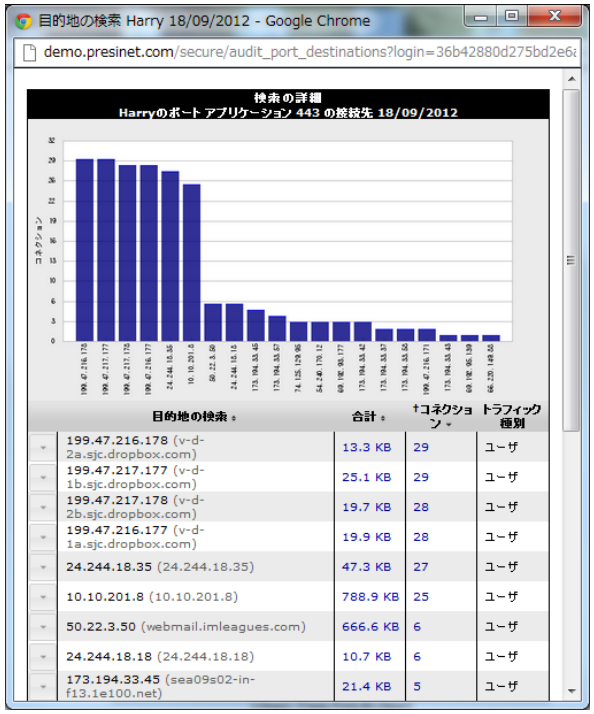
もしあやしい通信が見つかったなら、発信元のパソコンやサーバの感染，侵入を疑い、調査すべきです。

TVO の Full Connection Tracking

TVO は異常な状態のコネクションも含め、全てのコネクションを記録します。ポートスキャンや　Brute force attack により無応答となったり、拒否応答されたコネクションが全て記録され、適切に設定することによりアラート通知を受けることができます。また、外部C&Cサーバとの不正通信の痕跡もすべて記録します。

TVO によりネットワークの状況を観察することにより、ウィルスの侵入を早期に発見する可能性が高まるのです。

エラーコネクションの表示

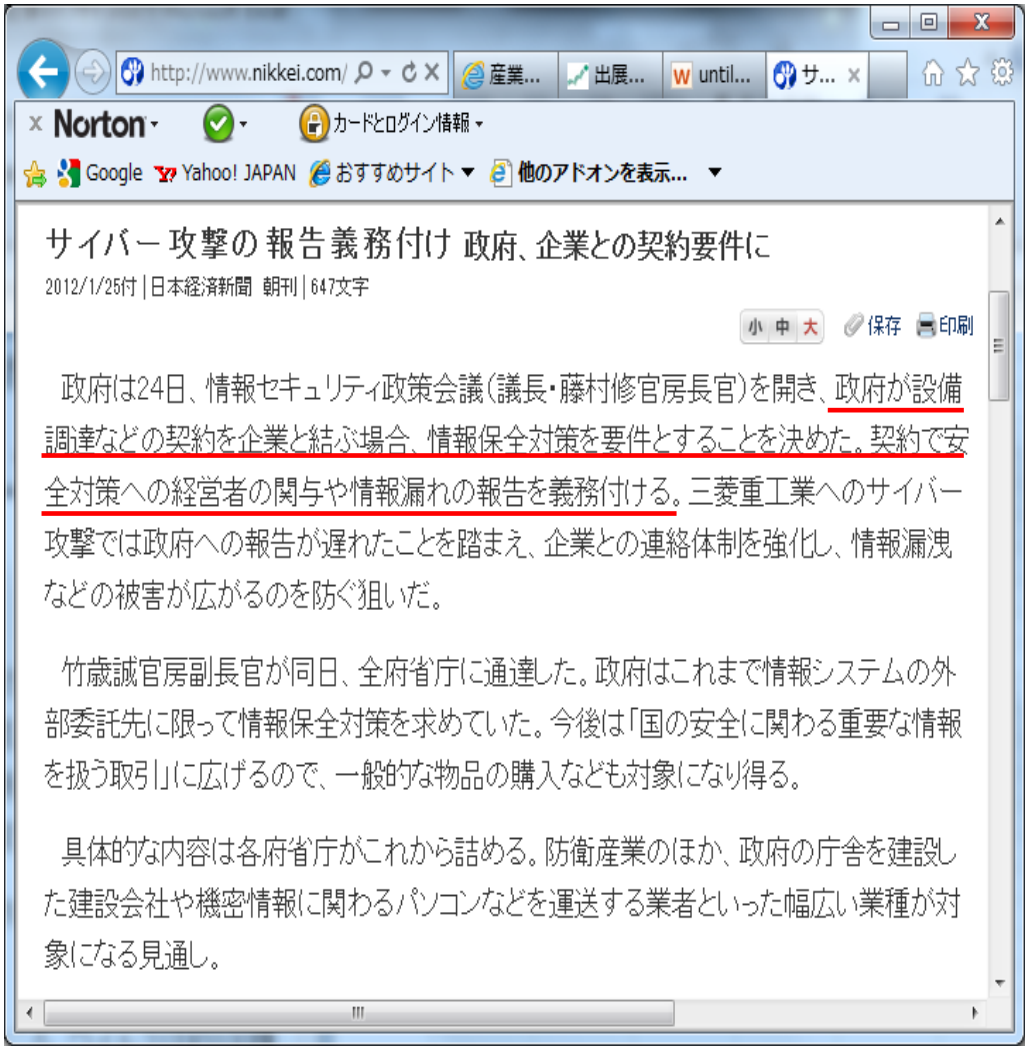


感染が疑われるPCの全接続先の表示

サイバー攻撃の把握が契約要件に？

近い将来、政府，自治体や大企業との契約要件として、サイバー攻撃をチェックしているかどうかを問われることになりそうです。

問われてから始めたのでは過去の証明ができません。いますぐに、始めるべきだとお思いになりませんか。



サイバー攻撃の報告義務付け 政府、企業との契約要件に

2012/1/25付 | 日本経済新聞 朝刊 | 647文字

小 中 大 保存 印刷

政府は24日、情報セキュリティ政策会議（議長・藤村修官房長官）を開き、政府が設備調達などの契約を企業と結ぶ場合、情報保全対策を要件とすることを決めた。契約で安全対策への経営者の関与や情報漏れの報告を義務付ける。三菱重工業へのサイバー攻撃では政府への報告が遅れたことを踏まえ、企業との連絡体制を強化し、情報漏洩などの被害が広がるのを防ぐ狙いだ。

竹歳誠官房副長官が同日、全府省庁に通達した。政府はこれまで情報システムの外部委託先に限って情報保全対策を求めていた。今後は「国の安全に関わる重要な情報を扱う取引」に広げるので、一般的な物品の購入なども対象になり得る。

具体的な内容は各府省庁がこれから詰める。防衛産業のほか、政府の庁舎を建設した建設会社や機密情報に関わるパソコンなどを運送する業者といった幅広い業種が対象になる見通し。

期待できる投資効果

①情報漏えいの不安を払拭した積極的ビジネス展開
②不正通信をチェックしていることをアピールすることによる、取引先様からの信用維持拡大、競業他社との差別化、新規顧客の開拓
③従業員のみなさんのインターネット業務外利用を抑止することによる、生産性の向上、従業員のセキュリティ意識の向上、残業代や電気代の節約によるコスト削減
④ウィルス被害やネットワーク監視不在などに起因して現実に多く発生しているネットワークトラブルを未然に防ぐことによる、組織運営の円滑化、生産性の維持拡大

ARTflow

www.artflowjapan.com

for human happiness

お問い合わせは

inquiry@artflowjapan.com