逆引きで考える
経営と情報セキュリティ

日本マイクロソフト株式会社
チーフセキュリティアドバイザー
高橋　正和

企業における情報セキュリティの現状

- ISMSやプライバシーマークを持っていても、セキュリティ事故が起きる
- 標的型攻撃を防げる気がしない
- XPからの移行が出来ない最大の理由は、「予算が取れない」
  - つまり、経営者を説得できない
- リスク分析、ビジネスインパクト分析なんて、現場にできるわけがない

- 初めて、経営者とIT関係者が真剣に対応を話し合う機会は
  - 残念ながら、セキュリティ事故が発覚した時

- 事故が起きる前に、考えてみてはどうだろうか？

セキュリティ事故シミュレーションの5つのシナリオ

- シナリオ
  1. 「ウィルスに感染し、機密情報が海外に送信」と報道された
  2. 従業員が顧客情報が入ったノートPCを紛失した
  3. インターネット上に取引先の機密情報が掲載されていると連絡が入った
  4. Webサーバーにウィルスが仕込まれて、閲覧者が感染をした
  5. クレジットカード情報を含む大量の顧客情報の流失が判明した

セキュリティ事故シミュレーションの課題

- 課題1
  - CIO側のシナリオ
    - あなたはIT部門の責任者で、事件の発生を金曜日の15:30に知ることとなりました。
    - 他社の事例から、事件を公表する必要があると判断しました。
    - 公表の必要性を経営者に説得する必要がありますが、経営者は17:00には外出し、週末は連絡が付きません。
    1. 17:00までに、事件を公表するためにすべきことをまとめなさい
    2. 経営者を説得するための報告書をA4２枚程度で作成しなさい
  - 経営者側のシナリオ
    - あなたは経営者もしくは経営陣の一員で17:00には外出をしなくてはなりません。（外出の理由を考える必要がある）
    1. 事件を適切に処理するためには、IT部門にどのような対応を求めますか？
    2. 外出をキャンセルして、事故対応にあたるという判断をするためには、どのような情報が必要ですか？
    3. 公表（自社のWebで周知、記者会見、公表しない）をどのように判断するか？
    4. 報告をすべき内部・外部の関係者を上げてください
    5. リーガルチェック
- 課題２
  - 公表を前提とした再発防止策を策定してください
- 課題3
  - 損害額とビジネスへの影響を分析してください

参考資料
東京商工会議所
危機管理対応マニュアルから抜粋

公表についての雛形

- 緊急対策本部の必要性
  - 情報収集の一元化と、方針決定をするための対策本部を設ける必要があるかどうか
  - 以下、設置する場合
  - 本部長はだれか
    - トップまたはナンバーツー
  - 構成メンバーはだれか
    - 必要な部署の管理職７～８人
  - １時間以内に召集できるか
  - 対策本部の場所（フロア、部屋）はどこか
- 対応方針の決定について
  - ただちに回収をするかどうか
  - 製造を中止するかどうか
  - 緊急に記者会見をひらくかどうか
  - 回収告知をするかどうか

企業が連絡を取るべき対象のチェックリスト

□納入先	□関係会社
□仕入れ先	□関連団体
□問屋	□主要株主
□小売店	□弁護士
□輸送会社	□広告会社
□関係当局	□PR会社
□ユーザー	□フリーダイヤル会社
□保険会社	□マスコミ
□社内関係部門	□メインバンク

事件の把握（欠陥商品発生時）

企業がチェックすべき12のポイント

- 判明したきっかけ（症状、現象）はどんなこと？
- 自社および取引先に具体的な損害は出たのか？
- それはどのような状況下で発生したのか？（5W1H）
- 第一報はどこの誰からどこの誰に入ってきたのか？
- それはいつ（○月△日○○時）か？
- それに対し誰が誰にどんな指示（返答）を出したか？
- 第一報を知らせてくれた相手についてわかっていることはなにか？
- お客様に具体的な実害、被害は出ているのか？
- その後、げんざいまで新たな情報は出ているのか？
- 原因は当社製品の不良（欠陥）といえるのかどうか？
- あるとすれば、その原因は何だと推測されるのか？
- 単発で終わるのか、第２、第３の同様の問題が発生する可能性はあるのか？

発生が予想されるクライシスのチェック

- 消費者やユーザーからのクレーム、問い合わせ殺到
- 流通関係からの納入一時ストップ
- 納入先や消費者からの返品
- PL訴訟の発生
- 第三者からのクレーム
- マスコミ報道による社会的信用失墜
- 行政当局からの事情調査
- 行政処分
- 売上ダウン
- 業績悪化

事件の把握（火災などの事故発生時）

すぐにつかんでおくべき16のチェックポイント

- 事故発生の時刻はいつか？
  - ○○時○○分ごろ
- 火災場所はどこか
  - ○○工場△△部門
- どういう状況で発生したのか
- なんらかの兆候はなかったのか
- 想定される原因は何か
- 鎮火はしたのか
- 現在の状況はどうなっているのか
- 消防と警察対応はだれが担当しているのか
- 死亡者はいるのか
- 死亡者の名前・性別・年齢・所属名は
- 負傷者の名前・性別・年齢・所属名は
- 負傷者のケガの具合はどうか
- 入院先はどこか
  - A、B,Cさんは○○病院、D,E,Fさんは△△病院
- 死傷者の家族に連絡はとれたか
- 地域住民に被害はおよんでいないか
- マスコミからの取材状況はどうか

今すぐに準備しておく資料、9つのチェック

- 正式な工場の名称、住所
- 工場長の名前
- 従業員の人数（正社員、パートタイマー）
- 生産品名
- 劇薬、毒物の使用の有無
- 火災による有毒ガス、有毒部室の発生の可能性の有無
- 定期点検体制に関するデータ
- 自衛消防隊の有無と訓練内容
- 防火訓練の有無

最悪の事態を想定した準備は出来ているか（火災などの事故発生時）

- 工場側が事実確認できなうちに、地元マスコミから工場（さらには本社）に電話取材が殺到する恐れはないか
- 現場にロービングしなかったために、現場に記者が踏み込む恐れはないか
- 現場に記者、カメラマンが殺到し、現地での工場対応が間に合わない恐れはないか
  - 119番通報を同時キャッチ、救急車、消防車と同時到着
- 撮影場所をめぐってカメラマンとのトラブルが発生する恐れはないか
- 現場への対置入り取材を巡って、現場責任者や当局とトラブルが発生する恐れはないか
  - 二次災害の防止
- 記者から求められる資料、質問に関する準備の遅れに対するクレームの恐れはないか
- 記者会見の実施時間をめぐりトラブルが発生する恐れはないか
- 速報重視のテレビニュースで未確認情報や誤報が流れる恐れはないか
- 地域住民や関係者からの話をもとにした伝聞情報や事実誤認情報が流れる恐れはないか
  - 情報管理の不徹底

５つの必須メッセージ項目

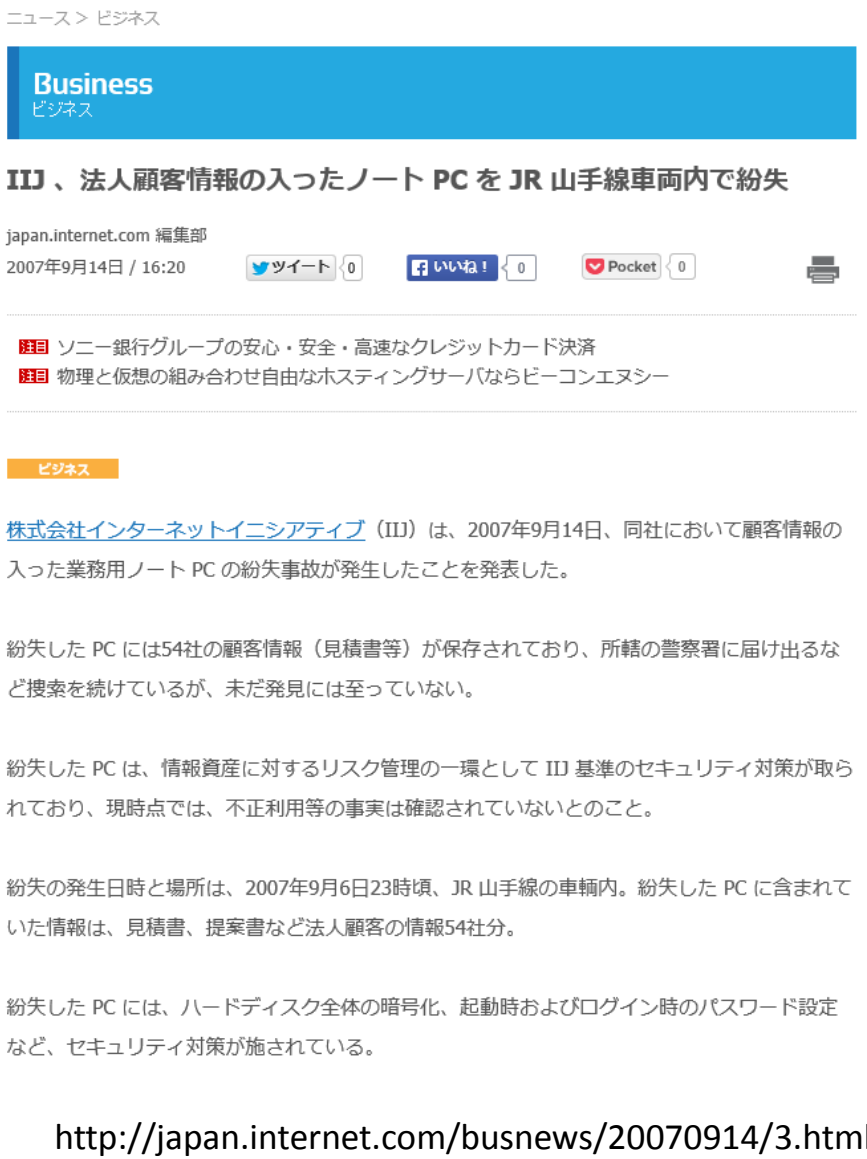
- 謝罪表明
  - 何はともあれ、お詫びする企業姿勢を示すこと
- 原因究明
  - 「なぜ発生したのか」、直ちに原因究明に「取り組んでいる」「究明に着手した」などの企業の意思を表明すること
- 再発防止策（改善など）
  - 「○○検査室を新設した」「○○委員会を発足させることにした」など、再発防止策を具体的な制度、組織で示すこと
- 現状説明（回収広報）
  - 不安感や憶測、疑惑などの発生を防止するために必要な情報を開示すること
- 責任表明
  - 発生したリスクの内容に応じた会社としての責任を表明すること

マスコミからの想定質問と回答13のチェックポイント（欠陥商品発生時）

- いつ不良品（欠陥商品）であることが判明したのか
- 原因は何なのか
- 設計ミスではないのか
- コストダウンが原因ではないのか
- これまでにも同様のケースがあったのではないか
- 会社は事前に気が付いていたのではないか
- 品質管理のミスではないのか
- 品質管理体制はどうなっていたのか
- チェック体制が甘かったのではないのか
- では、なぜ不良品（欠陥商品）が市場に出てしまったのか
- 回収は、今どうなっているのか
- 実害は出ていないのか
- 回収完了までに、どのくらいかかる見通しか

参考事例

IIJ:ノートPCの紛失事例



ニュース > ビジネス

Business
ビジネス

IIJ 、法人顧客情報の入ったノート PC を JR 山手線車両内で紛失

japan.internet.com 編集部
2007年9月14日 / 16:20

ツイート 0　いいね！ 0　Pocket 0

注目 ソニー銀行グループの安心・安全・高速なクレジットカード決済
注目 物理と仮想の組み合わせ自由なホスティングサーバならビーコンエヌシー

ビジネス

株式会社インターネットイニシアティブ（IIJ）は、2007年9月14日、同社において顧客情報の入った業務用ノート PC の紛失事故が発生したことを発表した。

紛失した PC には54社の顧客情報（見積書等）が保存されており、所轄の警察署に届け出るなど捜索を続けているが、未だ発見には至っていない。

紛失した PC は、情報資産に対するリスク管理の一環として IIJ 基準のセキュリティ対策が取られており、現時点では、不正利用等の事実は確認されていないとのこと。

紛失の発生日時と場所は、2007年9月6日23時頃、JR 山手線の車輌内。紛失した PC に含まれていた情報は、見積書、提案書など法人顧客の情報54社分。

紛失した PC には、ハードディスク全体の暗号化、起動時およびログイン時のパスワード設定など、セキュリティ対策が施されている。

http://japan.internet.com/busnews/20070914/3.html

株式会社インターネットイニシアティブ（IIJ）は、2007年9月14日、同社において顧客情報の入った業務用ノート PC の紛失事故が発生したことを発表した。

紛失した PC には54社の顧客情報（見積書等）が保存されており、所轄の警察署に届け出るなど捜索を続けているが、未だ発見には至っていない。

紛失した PC は、情報資産に対するリスク管理の一環として IIJ 基準のセキュリティ対策が取られており、現時点では、不正利用等の事実は確認されていないとのこと。

紛失の発生日時と場所は、2007年9月6日23時頃、JR 山手線の車輌内。紛失した PC に含まれていた情報は、見積書、提案書など法人顧客の情報54社分。

紛失した PC には、ハードディスク全体の暗号化、起動時およびログイン時のパスワード設定など、セキュリティ対策が施されている。

IIJ は、該当する顧客へは個別にお詫びと報告を行っており、PC の所在、情報流出については、今後も監視を継続していく。

IIJ では、「今回の事故を重く受け止め、今後の再発防止に万全を期す」としており、情報セキュリティ担当役員を責任者とした対策本部にて、対策と今後の再発防止策を検討し、速やかに実施していくという。

RSA: APT

RSA SPEAKING OF SECURITY

HOME BLOGS EVENTS NEWS MEDIA

BLOGS

Home » Blogs » Anatomy of an Attack

01 Apr

Anatomy of an Attack

Tags: Advanced Persistent Threats, APTs, Authentication, cyber security, cybercrime, Cybercrime and Fraud, Cyberwarfare
Categories: Fraud Intelligence,FraudAction

I was on a tour in Asia Pacific when I first heard the **news** about the attack. The investigation into this attack continues but I'm eager to share some information with you about it.

Let's first make sure everyone is on the same page. The number of enterprises hit by APTs grows by the month; and the range of APT targets includes just about every industry. Unofficial tallies number dozens of mega corporations attacked; examples are in the press regularly, and some examples are **here**, and **here**.

These companies deploy any imaginable combination of state-of-the-art perimeter and end-point security controls, and use all imaginable combinations of security operations and security controls. Yet still the determined attackers find their way in. What does that tell you?

The first thing actors like those behind the APT do is seek publicly available information about specific employees – social media sites are always a favorite. With that in hand they then send that user a Spear Phishing email. Often the email uses target-relevant content; for instance, if you're in the finance department, it may talk about some advice on regulatory controls.

The attacker in this case sent two different phishing emails over a two-day period. The two emails were sent to two small groups of employees; you wouldn't consider these users particularly high profile or high value targets. The email subject line read "2011 Recruitment Plan."

Follow Us

RSA SILVER TAIL 4.0
Learn More

INTH3WILD
The Current State of Cybercrime
INTH3WILD

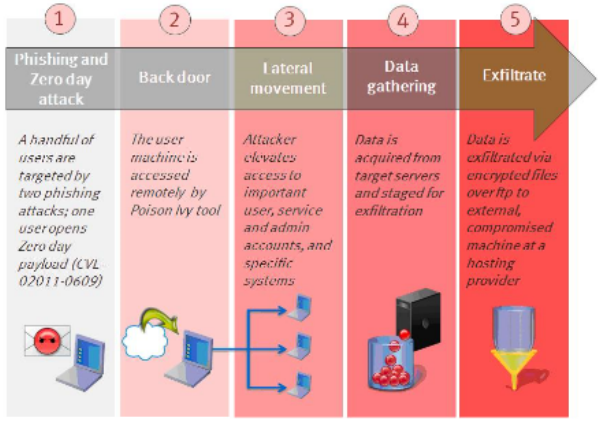
Anatomy of an Attack (Appendix)

Before reading this, you should read the blog entitled 'Anatomy of an Attack', which describes the attack on RSA at a high level. This post is an add-on, a sort of appendix really, that provides some end-to-end visibility into the various stages of the attack.

Advanced Persistent Threat attacks typically have three main phases. The first is the social engineering attack; that's one of the key elements that differentiates an APT from good old hacking. From the very first mention of APTs it's been clear that these attacks will be difficult to defend against, as they use a combination of social engineering with vulnerabilities in the end-point to access users' PCs. Once inside you're already in the network; you just have to find your way to the right users and systems, and carry on with "regular" hacking activities.

End-point security struggles with protecting against more simple form attacks such as data stealing Trojans, which is why you can find so many examples of **ZeusiLeaks**, or employees compromised with a Trojan that grabs the corporate data and sends it to a Trojan mothership halfway across the world. If Trojans available for sale from every digital thug on the cyber block are getting through the perimeter, what should we expect when it comes to the more devious attacks that are currently launched against private sector companies?

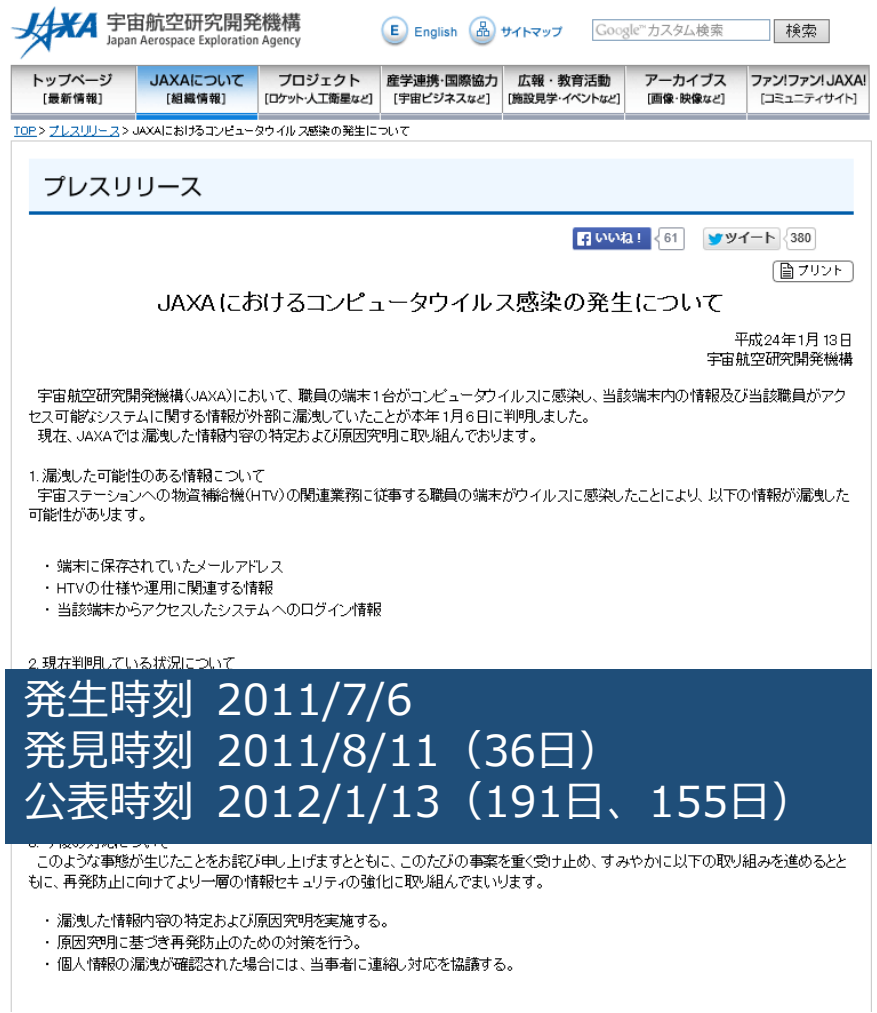
The social engineering part is equally simple. Like I mentioned in a **previous** blog that focused on some long-term defense strategies against APTs, just think of what has changed in the past few decades. In the early 1980s you would have guys like Matthew Broderick in **War Games**, searching for modems connected to sensitive networks. Matthew mapped networks and found weak spots. His attacks had nothing to do with the users; he used weaknesses in the infrastructure. But if Matthew was staging an APT hack today, the first thing he'd do is visit social media sites. He'd collect intelligence on the organizations' people, not infrastructure. Then he'd send a spear phishing email to the employees of interest.



https://blogs.rsa.com/anatomy-of-an-attack/

JAXA:ウィルス感染事例

2012/1/13



JAXA 宇宙航空研究開発機構 Japan Aerospace Exploration Agency

トップページ [最新情報] | JAXAについて [組織情報] | プロジェクト [ロケット・人工衛星など] | 産学連携・国際協力 [宇宙ビジネスなど] | 広報・教育活動 [施設見学・イベントなど] | アーカイブス [画像・映像など] | ファン!ファン!JAXA! [コミュニティサイト]

TOP > プレスリリース > JAXAにおけるコンピュータウイルス感染の発生について

プレスリリース

JAXAにおけるコンピュータウイルス感染の発生について

平成24年1月13日
宇宙航空研究開発機構

宇宙航空研究開発機構(JAXA)において、職員の端末1台がコンピュータウイルスに感染し、当該端末内の情報及び当該職員がアクセス可能なシステムに関する情報が外部に漏洩していたことが本年1月6日に判明しました。
現在、JAXAでは漏洩した情報内容の特定および原因究明に取り組んでおります。

1. 漏洩した可能性のある情報について
宇宙ステーションへの物資補給機(HTV)の関連業務に従事する職員の端末がウイルスに感染したことにより、以下の情報が漏洩した可能性があります。

・端末に保存されていたメールアドレス
・HTVの仕様や運用に関連する情報
・当該端末からアクセスしたシステムへのログイン情報

2. 現在判明している状況について

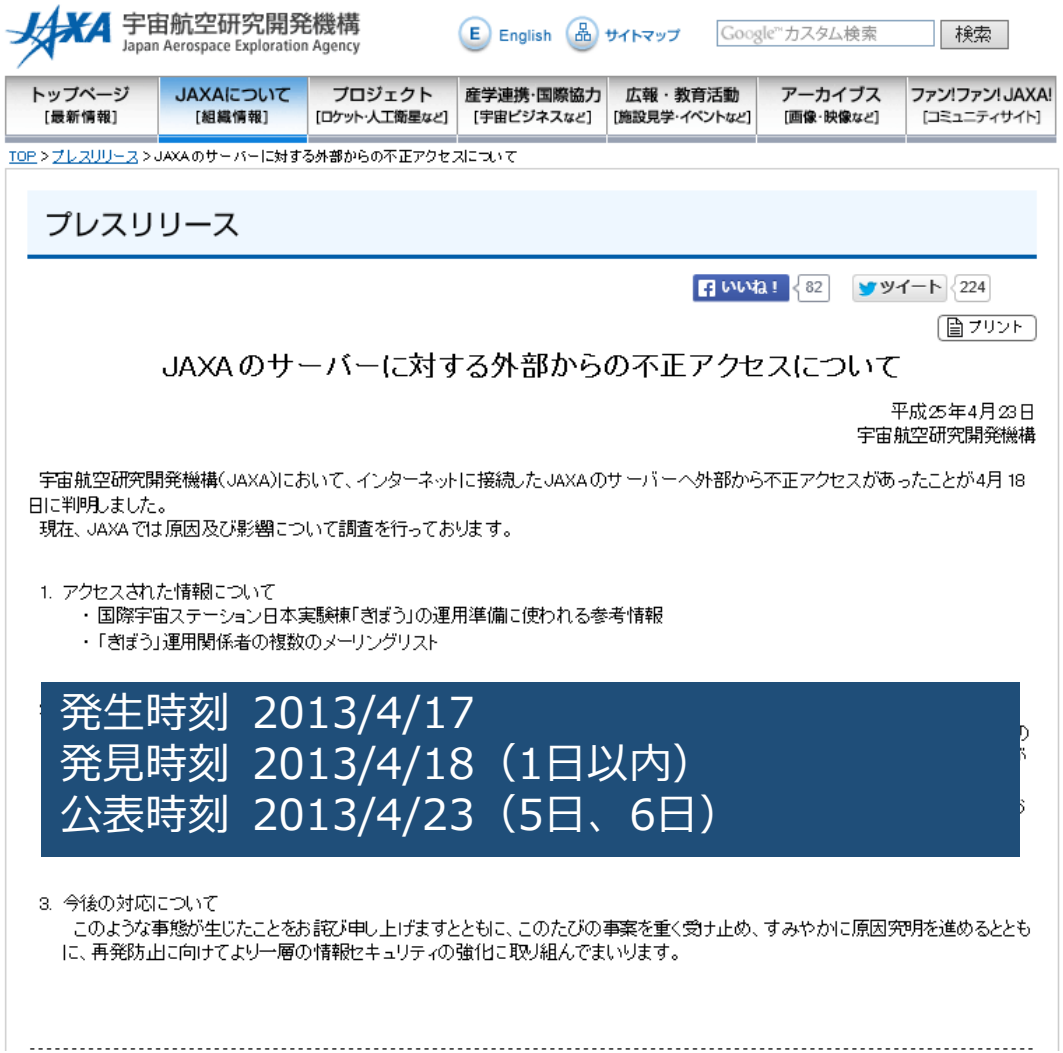
このような事態が生じたことをお詫び申し上げますとともに、このたびの事案を重く受け止め、すみやかに以下の取り組みを進めるとともに、再発防止に向けてより一層の情報セキュリティの強化に取り組んでまいります。

・漏洩した情報内容の特定および原因究明を実施する。
・原因究明に基づき再発防止のための対策を行う。
・個人情報の漏洩が確認された場合には、当事者に連絡し対応を協議する。

発生時刻 2011/7/6
発見時刻 2011/8/11（36日）
公表時刻 2012/1/13（191日、155日）

http://www.jaxa.jp/press/2012/01/20120113_security_j.html

2013/4/23



JAXA 宇宙航空研究開発機構 Japan Aerospace Exploration Agency

トップページ [最新情報] | JAXAについて [組織情報] | プロジェクト [ロケット・人工衛星など] | 産学連携・国際協力 [宇宙ビジネスなど] | 広報・教育活動 [施設見学・イベントなど] | アーカイブス [画像・映像など] | ファン!ファン!JAXA! [コミュニティサイト]

TOP > プレスリリース > JAXAのサーバーに対する外部からの不正アクセスについて

プレスリリース

JAXAのサーバーに対する外部からの不正アクセスについて

平成25年4月23日
宇宙航空研究開発機構

宇宙航空研究開発機構(JAXA)において、インターネットに接続したJAXAのサーバーへ外部から不正アクセスがあったことが4月18日に判明しました。
現在、JAXAでは原因及び影響について調査を行っております。

1. アクセスされた情報について
・国際宇宙ステーション日本実験棟「きぼう」の運用準備に使われる参考情報
・「きぼう」運用関係者の複数のメーリングリスト

3. 今後の対応について
このような事態が生じたことをお詫び申し上げますとともに、このたびの事案を重く受け止め、すみやかに原因究明を進めるとともに、再発防止に向けてより一層の情報セキュリティの強化に取り組んでまいります。

発生時刻 2013/4/17
発見時刻 2013/4/18（1日以内）
公表時刻 2013/4/23（5日、6日）

http://www.jaxa.jp/press/2013/04/20130423_security_j.html

むすび

むすび

- ひな形ありきで考えたセキュリティ対策では、実際の事故に対応できない

- 事故をシミュレーションすることで、以下の項目を明らかにする
  - セキュリティは経営上の問題・戦略課題であること
  - 事件・事故に対応するために必要な体制
  - 事件・事故を把握するために必要な情報
  - 事件・事故を防止するための対策
- この結果を踏まえてひな形を参照する
  - ひな形はゴールではなくツールである