PSIRTと事後対応の取り組み

株式会社アイ・オー・データ機器

情報セキュリティ対策チーム

進化する明日へ
Continue thinking

自己紹介

■名前

島田 康晴(しまだ やすはる)

■所属

事業戦略本部 企画開発部 企画開発6課 課長代理

●当社商品と接続するクラウドサービスの開発を担当

●情報セキュリティ対策チームメンバーで、主にJPCERT/CCとの調整窓口を担当

●当社商品のIPv6対応検討WGのメンバー

会社概要

■社名	株式会社アイ・オー・データ機器
■設立	1976年1月10日
■代表者	代表取締役会長　細野 昭雄 代表取締役社長　濵田 尚則
■所在地	石川県金沢市
■資本金	35億8,807万円
■年商	484億円(2017年6月期 連結)
■従業員数	490人(2017年6月末現在 連結)
■事業内容	デジタル家電周辺機器の製造・販売
■事業所	東京、大阪、札幌、仙台、名古屋、広島、福島

進化する明日へ
Continue thinking

主力商品のご紹介

無線LANルーター

IPカメラ

ネットチューナー

液晶モニタ

NAS

HDD

CDレコ

- 当社はコンピュータ周辺機器から始まって40年以上となりますが、現在の商品ラインナップの多くがネットワーク(インターネット)に接続できるようになっており、これらの商品を広義の意味でIoTデバイスと考えています。

進化する明日へ
Continue thinking

ネットワーク商品と脆弱性

ネットワーク商品を取り扱うようになると、避けて通れないのは「**商品の脆弱性を見つけました！**」報告です。

これまで商品の脆弱性に対応してきた中で、事後対応のポイントを、転んでしまった後に起き上がるための処方箋として、皆様と共有できればと考えています。

進化する明日へ
Continue thinking
I-O DATA

当社の脆弱性情報

- 当社のセキュリティ情報はサポートページに専用の欄を設けて公開しています。
- http://www.iodata.jp/support/information/security/
- 2008年3月に最初の脆弱性を公開してから、インシデントを含めて約30件の情報を公開。
- また、JVNには28件のインシデント情報を公開。

進化する明日へ
Continue thinking
I-O DATA

PSIRTについて

- ここでは商品セキュリティリスクに対応するPSIRTのお話になります。

PSIRTついては、熊白様のお話が参考になるかと思います。

会社の情報セキュリティリスクに対応するCSIRTついては前日のセッションにて解説しています。

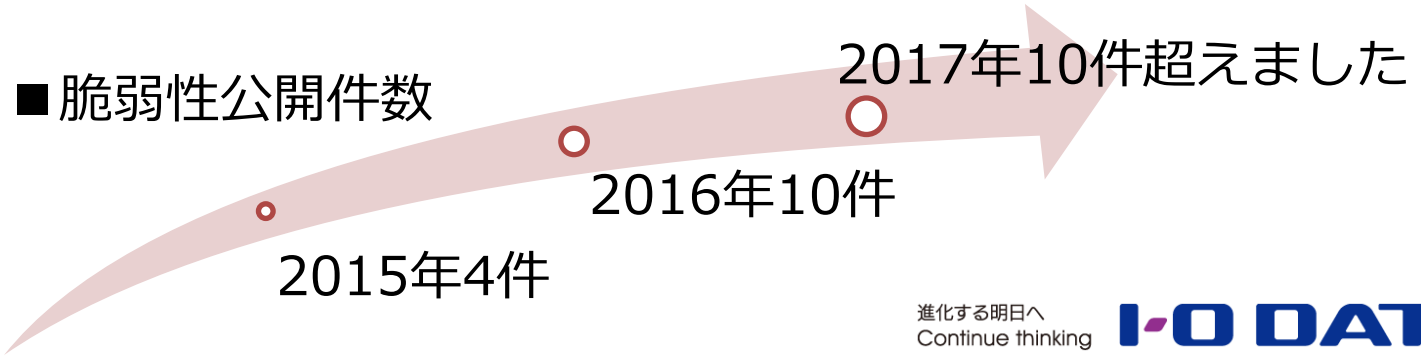
3種類のインシデントとPSIRT

- 当社におけるインシデントには3種類あると考えています。

インシデントの種類	内容	対応
業務インフラに関するインシデント	業務(社内)インフラを利用する上で発生。 ウィルスメールやマルウェアの混入など。	CSIRT
サービスに関するインシデント	当社が管理する外向けのサービスで発生。 ホームページへのDoS攻撃やクラウドサービスからの情報漏洩など。	CSIRT/ PSIRT
商品に関するインシデント	当社が取り扱う商品に発見される脆弱性。 ユーザー環境で被害が発生したり、攻撃の踏み台にされるなど。	PSIRT

情報セキュリティ対策チーム

- 当社においてPSIRTを担っているのが「情報セキュリティ対策チーム」(以降「対策チーム」とします)となります。
- 「ポケドラ」の脆弱性を契機に重大インシデントにも対応できるように、対策チームを立ち上げました。
- 脆弱性に対して広く議論することと、脆弱性対応は全社的な取り組みと考え、人員構成は開発部門だけでなく管理部門、情報システム部門、カスタマサポート部門もメンバーとなっています。
- 対策チーム発足前は、開発部門の数人を中心に商品の脆弱性をハンドリングしてきましたが、脆弱性の公開件数が増えてきたことで業務に支障が出てきていたことも理由としてあります。



進化する明日へ
Continue thinking
I-O DATA

対策チームの取り組み

- 「業務インフラ」「サービス」「商品」に対するインシデントが発生した場合、インシデント情報を基に「顧客対応の可能性」も含めた対応判断を適切かつ速やかに行い、管理することをミッションとしています。

✓ インシデント発生時に対策フローに則ってインシデントハンドリング(判断、対応支援)

✓ 重大インシデント発生時には優先的に対応支援

✓ インシデント判断基準の策定／把握と継続的見直し

✓ 商品セキュリティ仕様の継続的な見直し

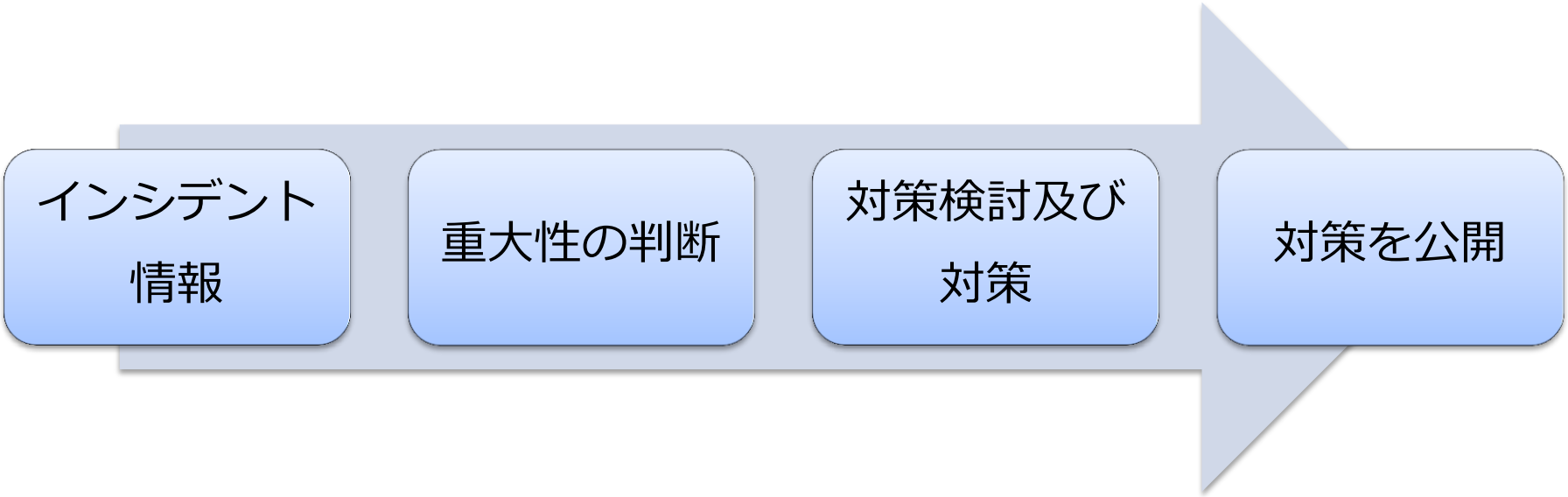
✓ インシデント情報DB作成と管理

✓ 社内システム／社外向けサービス用サーバーの把握

✓ 業界/他社等、情報セキュリティに関する最新状況の把握

※対策チーム自体はCSIRTとPSIRTの機能を兼ねています。

インシデントハンドリング

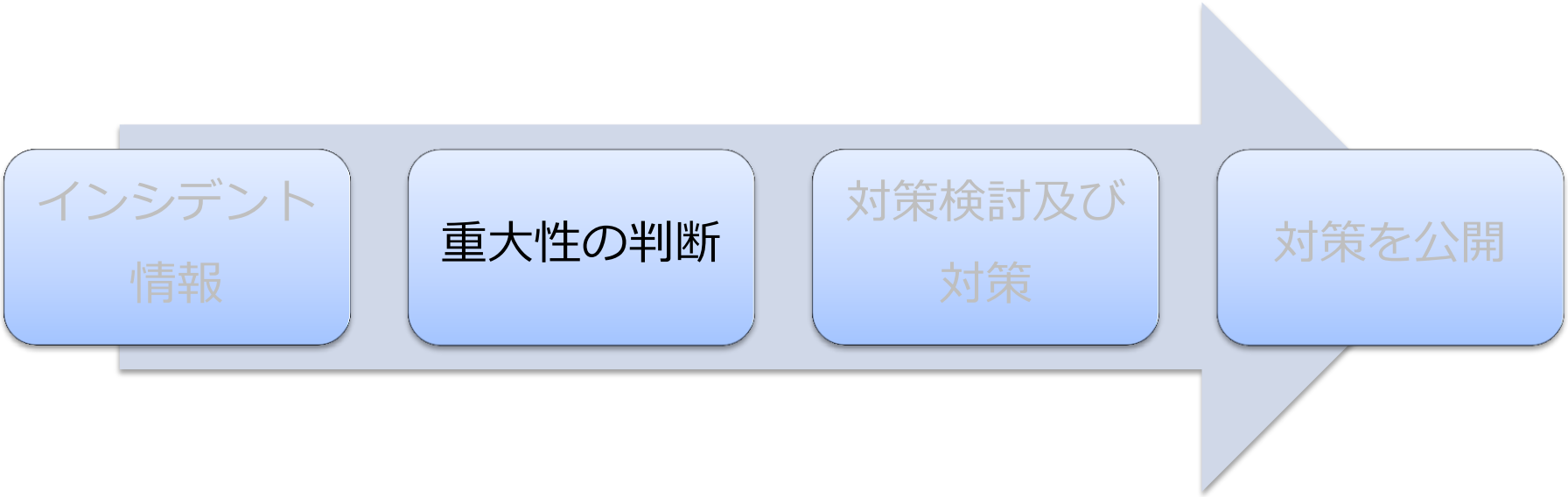


- インシデントに対するハンドリングは上記の手順で行われます。
- 手順としては基本的にIPAの「情報セキュリティ早期警戒パートナーシップガイドライン」に合わせたものになっています。
- 対策チーム立ち上げ前と手順が変わっているわけではありませんが、役割をより明確化しました。

インシデント情報

- JPCERT/CCやユーザー、報道機関などからインシデント情報がもたらされますが、ほとんどはJPCERT/CCからの情報になります。
- JPCERT/CCは開発部門、それ以外はサポート窓口もしくは広報の窓口で受け付けています。
- その情報が、対策チームに上がることになっています。

重大性の判断



- インシデント判断基準を基に開発部門で1次判断、対策チームにて最終判断を行います。
- きわめて重大なインシデントであると判断した場合は、経営陣も参画の上で判断することになっています。

判断基準

- 重大性の判断は、おおよそ以下の項目で判断しています。

✓ インターネット側かLAN側か？
  - インターネットから攻撃を受けるか、LAN側からのみか？

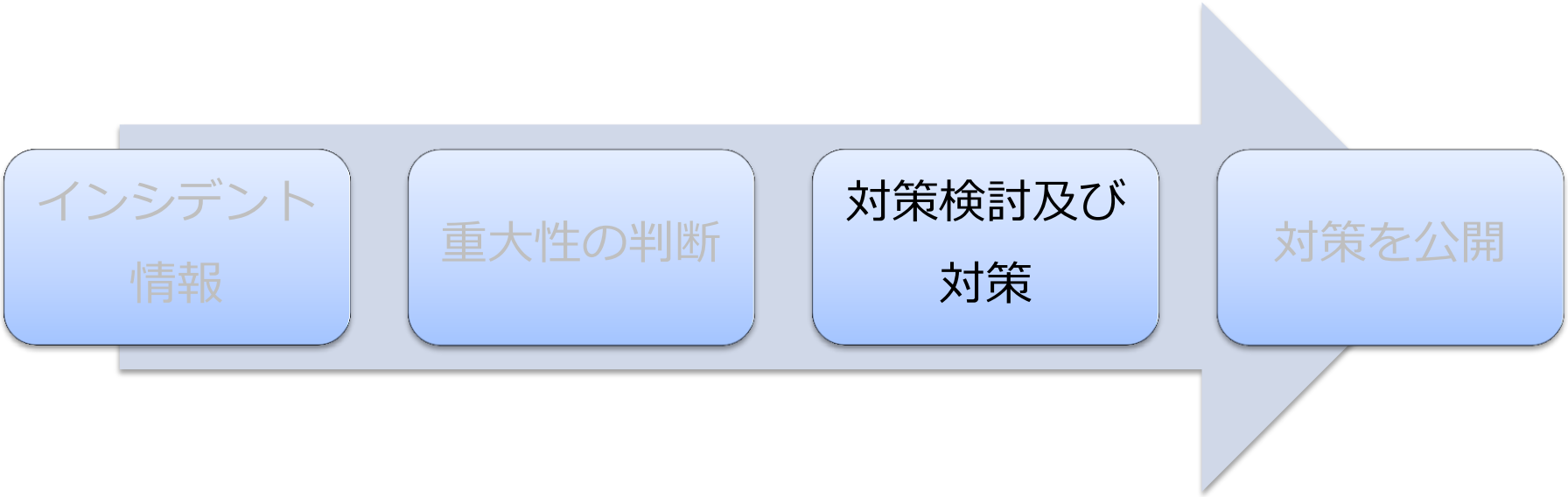
✓ 攻撃の成立度は？
  - 常に成立するか？特定のタイミングか？手順は複雑か？など

✓ ユーザーデータへの影響度は？
  - ユーザーデータが漏洩したり、改竄(消去)されないか？

✓ 周りへの影響度は？
  - 他のシステムに影響を与えないか？

- 重み付けは違いますが、共通脆弱性評価システム(CVSS)と判断するポイントは重なってくると思いますので、スコアは参考になります。

対策検討および対策



- 開発部門にて対策を検討して対策を実施します。
- ワークアラウンドが存在する場合は、この時点で公開を行う場合があります。また、重大インシデントの場合は、対策が完了するまで出荷を停止する場合もあります。

対策を公開

- JPCERT/CCと調整を行った後、当社ホームページ及びJVNで対策を公開します。
- プログラムによる対策の場合は、自動更新機能や通知機能にてプログラムの更新を促します。最近の商品はプログラムの自動更新機能を実装することによりユーザーへの到達を高めています。

公開に必要な情報

- Webで公開するときには以下の情報を公開するようにしています。

✓ 対象となっている商品

✓ 脆弱性が存在するバージョン

例：2.00とそれ以前のバージョン

✓ 対策方法

※ほとんどの場合はソフトウェアのバージョンアップですが、設定変更など運用による回避方法を案内する場合があります。

✓ ソフトウェアで対策する場合は脆弱性を対策したバージョン

例：バージョン2.10で対策しました。

✓ ソフトウェアダウンロード先のリンクと適用方法。

「ポケドラ」の脆弱性とは

- ポケドラ(WFS-SR01)とは、2013年9月販売開始(現行商品)で、スマホ・タブレットやパソコンに保存されている写真や動画をWi-Fi経由でSDカード、USBメモリーに保存・再生できる「Wi-Fiストレージ」商品です。
- 「Wi-Fiルーター」機能を備えており、出張時のホテルで有線LANをWi-Fiで利用することが可能です。

- 当社：http://www.iodata.jp/support/information/2016/wfs-sr01/
- JVN：https://jvn.jp/jp/JVN18228200/index.html

進化する明日へ
Continue thinking
I-O DATA

脆弱性の指摘と協議

外部より、ポケドラに脆弱性があるのではないかと思われる事象を確認との連絡が入りました。

もたらされた情報が事実であれば、重大インシデントとなるため、開発部門で至急調査が行われ、指摘の通りであることが判明しました。

緊急対応の必要性から、経営陣も含めて臨時の会議を開催し、対策の協議を行いました。

脆弱性の判断と対応

協議の結果として、ポケドラの出荷停止、報告者へ一次回答、営業部へ案内、JPCERT/CCへ連絡を行いました。

ワークアラウンドを当社WebページおよびJVNにて公開、販売店など取引先へ案内を実施しました。

対策ファームウェアを公開、合わせて当社WebページおよびJVNにて案内を公開を実施し、出荷も再開しました。

気づかされたこと (その1)

ユーザーの利用実態が我々の想定と違っている部分があった。

→ ユーザー想定を決めつけずに、「かもしれない」という考えが必要。

重大インシデントだが、ファームウェアによる対策まで時間がかかりそうだった。

→ ワークアラウンドがあるのであれば、事前に速やかな公開することが有効です。

気づかされたこと (その2)

今回の脆弱性はインパクトが大きかったため、
数々の取材やヒアリングを受けました。

→ サイバーセキュリティに対する世の中の関心が非常に高くなっていると実感しました。

対策チームの発足など、脆弱性対応に対する取り組みを再点検するきっかけとなりました。

→ 開発部門にて脆弱性対応に対する取り組みの再点検を行っています。

取り組みの再点検 (その1)

商品が使用していないポートがクローズしているか確認しにくい。

- 脆弱性(ポート)スキャナーを導入しました。

担当者によって商品に対するセキュリティの意識に差がある。

- 商品に対するセキュリティ教育の実施。

どの程度セキュアな商品を開発して良いのかわからない。

- セキュリティポリシーの導入・強化。

取り組みの再点検 (その2)

セキュアな商品の開発の仕方がわからない。

- セキュリティ設計基準書の見直し。
- セキュリティ開発ガイドラインの策定。

つながり

ガイドライン等については、金居様と熊白様のお話が参考になるかと思います。

脆弱性を減らす仕様

- 商品の仕様として脆弱性が減るようなアイデアを検討しています。

✓ 商品のサービスやポートの状況を把握し、不要なサービスの停止や、ポートのクローズを行う。

✓ 出荷時のデフォルトパスワードがユニークになるような仕組み作り。

✓ 商品の利用開始時には、出荷時のデフォルトパスワードからの変更を利用者が行うことを促すための仕組み作り。

✓ アプリケーションもしくはクラウドを利用して商品の動作を監視し、異常な動作が観測された場合は通知する仕組み作り。

✓ LAN内利用前提の商品の場合は、プライベートアドレス以外のアドレスでは通信できない仕組み作り。

対応事例紹介

2つの事例を紹介しながら、その他の事後対応のポイントを解説します。

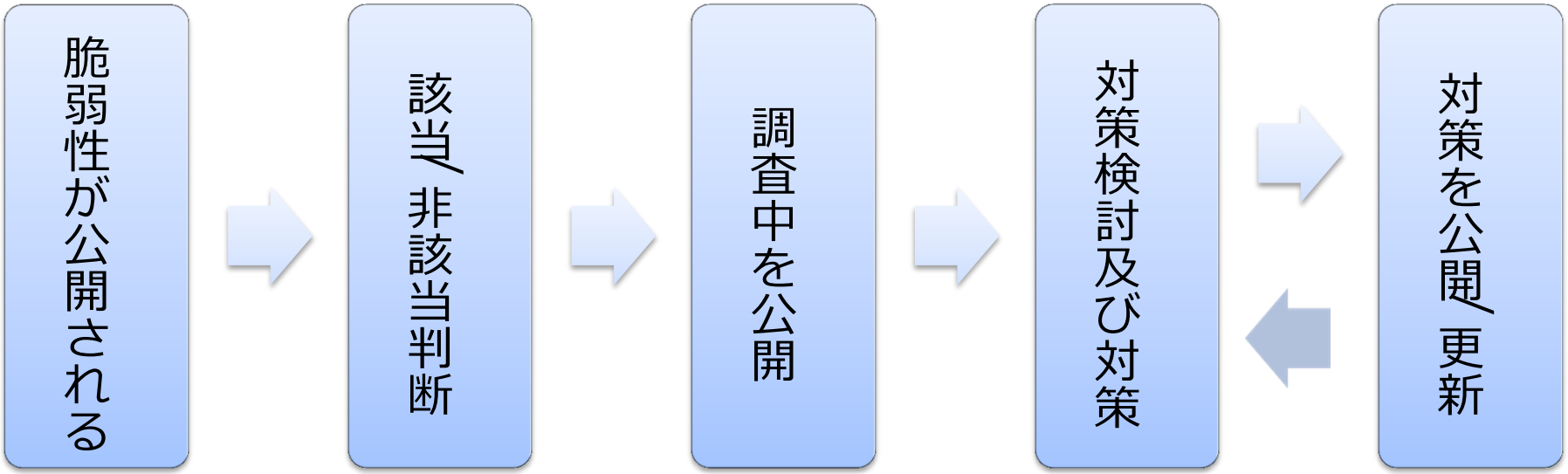
複数商品が該当する事例

- Wi-Fiの通信に利用されているWPA2において、ハンドシェイク中に脆弱性が確認されました。
  - 当社：http://www.iodata.jp/support/information/2017/wpa2/
  - JVN：https://jvn.jp/vu/JVNVU90609033/index.html

- この脆弱性は当社も含めて数多くのWi-Fi商品が該当することになりました。
- 今回の様に脆弱性が先行して公開されて、複数の商品が該当する場合のハンドリングを紹介します。

進化する明日へ
Continue thinking
I-O DATA

複数商品のハンドリング



- 該当/非該当判断で該当商品が無ければ、公開情報なしで終了。(市場の状況に応じて、あえて”該当していません”の公開をしても良いかと思います)
- 該当商品の対策がすべて完了するまで、対策の実施及び対策の公開/更新を繰り返すことになります。

この事例のポイント

- 脆弱性情報が公開されたら、できるだけ速やかに脆弱性の内容を把握して、該当する商品がないかの調査を開始します。
- 調査の段階で該当商品が見つかった場合、速やかに調査中の旨の公開を行うことが望ましいです。
- 市場の脆弱性に対する意識の高まりから、時には顧客などからの問い合わせがすぐに届きます。会社としての対応を明示するためにも情報公開は有効です。
- 該当商品の調査を何処まで遡って調査するかは、商品リストのテンプレート化するなどしてあらかじめ決めておくと、楽になります。

古い商品の対応事例

- 「NP-BBRS」は、2004年販売開始の有線LANルーターで、UPnPに関する脆弱性があり、悪意のある第三者が利用し、任意の他方に対するDoS攻撃に利用される可能性があります。
  - 当社：http://www.iodata.jp/2015/wn-g54r2/
  - JVN：https://jvn.jp/jp/JVN17964918/index.html

- 古い商品に対しての対応判断の事例になります。

利用停止をお願いする

- 10年以上前の商品で、ファームウェアによる対策はすでにできなくなっていました。
- また、設定内容や運用の変更では脆弱性回避ができないことも判明しました。
- ファームウェア修正による対応も、設定内容や運用の変更による対策も不可能な場合であったため、やむなく「商品そのものの利用停止をお願いする」案内としました。
- 商品に対する脆弱性の存在を公開して、もし利用しているユーザーがいれば周知することが目的となります。

EOSという考え方

- ハードウェアの信頼性が向上して長期間問題無く動作するようになることにより、販売完了から時間が経過した商品で脆弱性が見つかることがあります。(古いからこそ狙われるという考え方もあります)
- 古い商品に対する脆弱性対策は様々な理由で困難なことが多いです。しかしながら脆弱性が存在する限り何らかの方法で、その商品の脆弱性が利用されないようにする必要があります。
- EOS(End Of Service)の概念を導入し明示することにより、EOSとなった商品を利用している顧客には、古い商品を使っていることのリスクを説明して、最新機器に買い換えていただくように案内することも必要ではないかと考えています。
- EOSを導入するにしても様々な課題があり、当社でも検討していますが、導入までには至っていません。(現在は商品毎に都度判断となります)

事後対応のリーチ

- 対策ファームウェアを公開しても実際に顧客までリーチしているのかを把握するのは難しい課題です。
- 当社ではWebやJVNでの公開だけでなく、アプリや商品の通知機能を利用して対策を呼びかけています。
- また、現在の商品にはプログラムの自動更新機能を搭載しており、対策が自動的に適用されるようになっています。しかし、どこまで対策が行き届いているのかまでは把握できていません。
- 今後は、更新機能を高度化することにより、プログラムの自動更新だけでなく、商品個々の更新状態の把握やヘルスチェックを行う仕組みを展開することにより事後対応のリーチの見える化を目指しています。

市場に潜む脆弱性

- 実際に市場で商品の脆弱性が問題になっていることを知ることができれば、積極的に重大インシデントを対策できるのではと考えています。
- ダークネット等を利用して、そこに存在する脆弱性を見つけ、そのユーザーへ脆弱性を通知や対応する手段が確立できればと考えています。

つながり　脅威の事例については、金居様のお話が参考になるかと思います。

つながり　というわけで、吉岡先生の取り組みに期待しています。

進化する明日へ
Continue thinking
I-O DATA

最後に

当社は全社的な取り組みとして積極的に脆弱性の対応・公開を行っています。

皆さんは、それぞれの状況にあった事後対応を検討しているかと思いますが、それを実践する上で、少しでも参考になれば幸いです。

ありがとうございました。