インシデント報告システム運用事例
~ウイルス調査報告用Webシステム~

OKI-CSIRT
橘　喜胤

www.oki.com/jp/

アジェンダ

- OKI-CSIRTのご紹介
- ウイルス調査報告用Webシステム導入の背景
- ウイルス調査報告用Webシステム
- ウイルス調査報告用Webシステム導入の効果

OKIグループ概要

日本初の電話機を製作以来130年
現在は120カ国で事業展開するグローバル企業へ

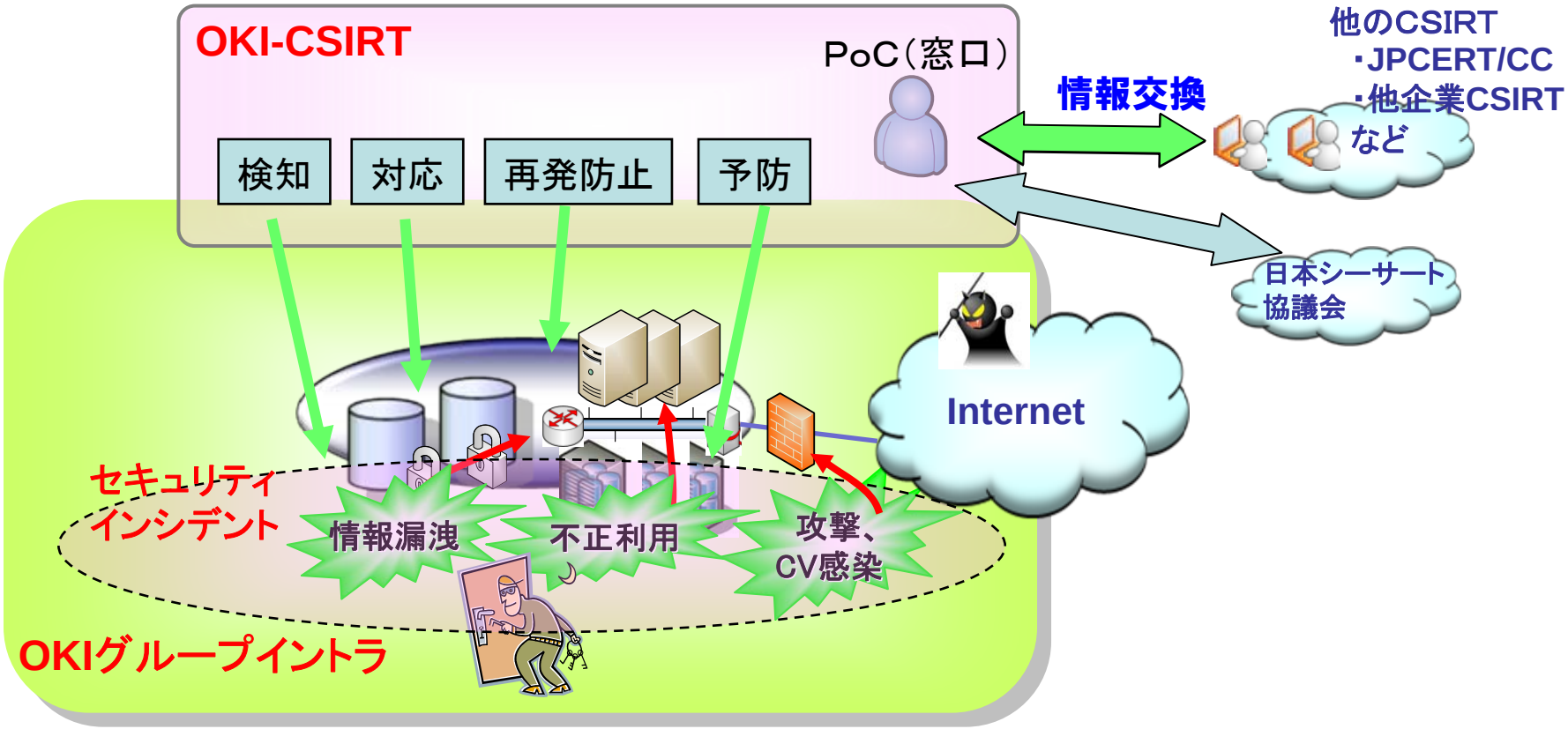
- 創業: 1881年（明治14年）
- 創業者: 沖牙太郎（1848-1906）
- 代表取締役社長執行役員: 川崎 秀一
- 売上高*: 4,327億円
- 従業員数*: 単独：3,103名、連結：16,697名
  （国内10,188名、海外6,509名）
- 子会社* : 68社
- 資本金*: 440億円
- 事業内容: 企業理念の「進取の精神」をもって情報通信システム、プリンタ事業における商品、技術およびソリューションの提供

創業者：沖牙太郎

＊連結ベース　2011年3月31日現在

OKI-CSIRT

2008年5月に、OKIグループで発生するコンピュータセキュリティインシデントの解決を支援する技術支援組織として、OKI-CSIRTを設置



OKI-CSIRTが対応するインシデント

【OKI-CSIRTが対応する主なインシデント】
- ウイルス感染(商品CV※)
- 不正プログラムによる情報
- 情報基盤サービスに対する攻
- 社内規則違反者による不正利

※ OKIグループにおける製品、各種サービ

本日は、商品へのウイルス感染予防についての取り組みのために導入したウイルス調査報告用Webシステムの導入と運用についてお話しします

- OKI-CSIRTのご紹介
- ウイルス調査報告用Webシステム導入の背景
- ウイルス調査報告用Webシステム
- ウイルス調査報告用Webシステム導入の効果

ウイルス感染への取組み 【商品CV】

商品CVとは

OKIグループにおける製品、各種サービスに影響を与えるコンピュータウイルス(不正プログラム)の検知・感染を意味する
(OKIグループ内での呼称)

発足の経緯

- 2007/末頃よりUSBメモリ経由で感染するウイルスが大流行し、OKIにも影響がではじめる
- 従来のルール、体制は、社内IT環境利用におけるウイルス感染対策がターゲット。商品へのウイルス感染予防対策は、不十分
- 2008/3に、商品へのウイルス感染予防の体制を発足
- 体制発足時点から、OKI-CSIRTが重要な役割を担う

従来のウイルス対策運用における課題

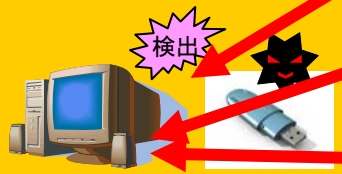
ウイルス対策ソフトは、基本は検知と防御のみ
原因を解決しないと何度も検知し、事故に繋がってしまう

■共有フォルダでウイルス検知

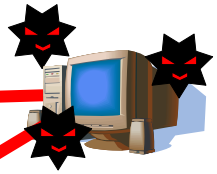
（ファイル感染型ウイルス）

■USBメモリでウイルス検知

（ConfickrやAutorun系ウイルス）



■感染経路



・社内にウイルス対策されていない感染PCが残っている

・感染したUSB媒体の利用

■影響度（お客様に感染させた？）

・顧客のPCに挿入した事があるか
・重要な機器に挿入した事があるか

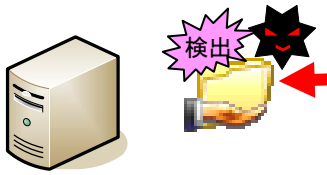
ウイルス対策ソフトがカバーする範囲

従来のウイルス対策運用における課題

ウイルス対策ソフトは、基本は検知と防御のみ
原因を解決しないと何度も検知し、事故に繋がってしまう

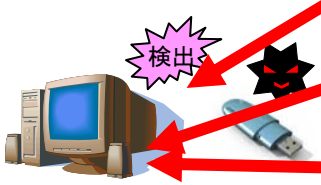
■共有フォルダでウイルス検知

（ファイル感染型ウイルス）

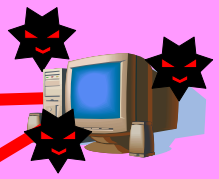


■USBメモリでウイルス検知

（ConfickrやAutorun系ウイルス）



■感染経路



・社内にウイルス対策されていない感染PCが残っている

・感染したUSB媒体の利用

■影響度（お客様に感染させた？）

・顧客のPCに挿入した事があるか
・重要な機器に挿入した事があるか

ウイルス対策ソフトでは分からない部分

従来のウイルス対策運用における課題

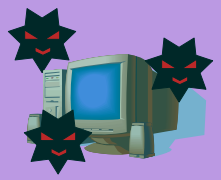
ウイルス対策ソフトは、基本は検知と防御のみ
原因を解決しないと何度も検知し、事故に繋がってしまう

ウイルス検知者へのヒアリングが必要

↓

運用コストが大きいためIT化

■感染経路



・社内にウイルス対策されていない感染PCが残っている

・感染したUSB媒体の利用

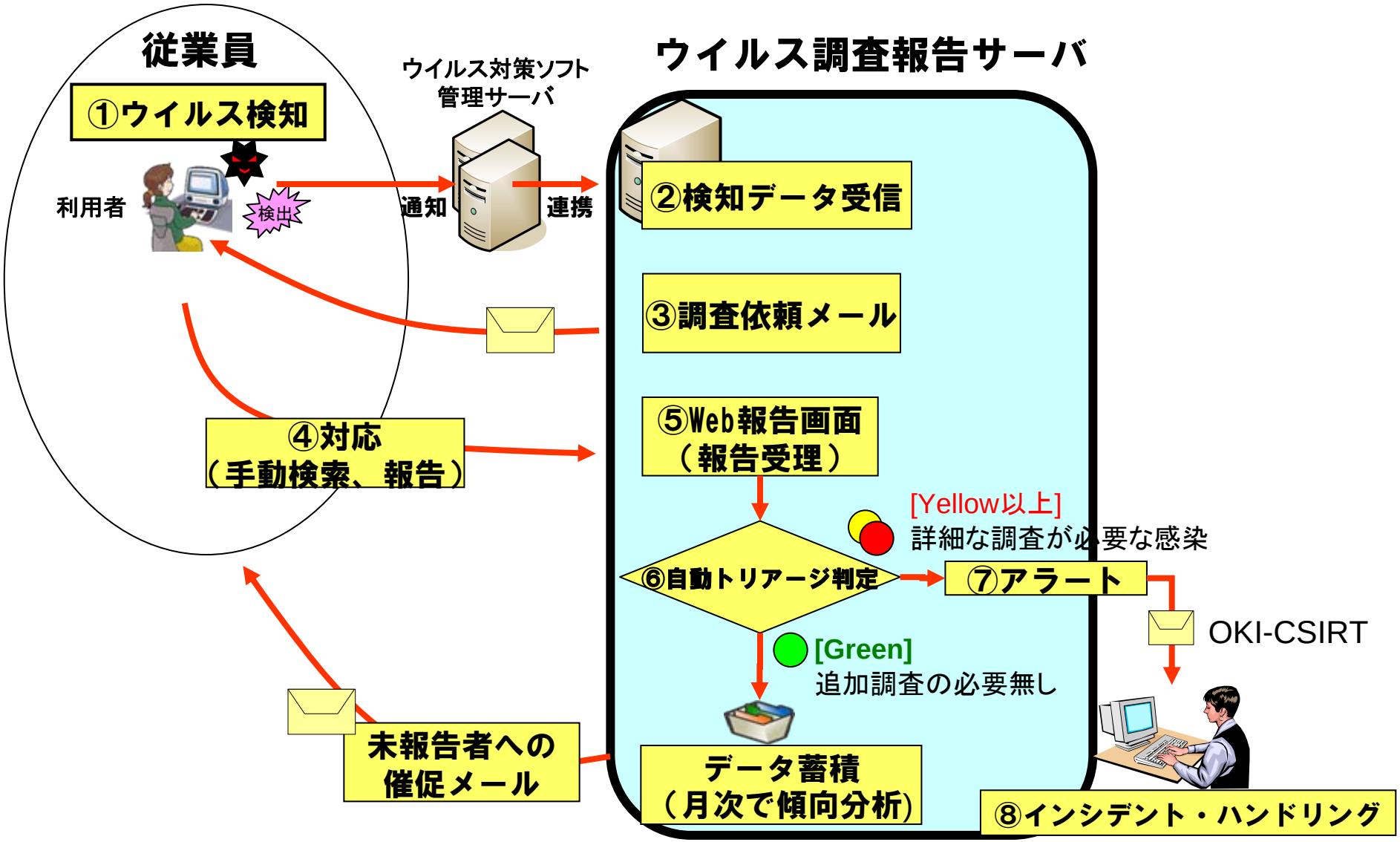
■影響度（お客様に感染させた？）

・顧客のPCに挿入した事があるか
・重要な機器に挿入した事があるか

ウイルス対策ソフトでは分からない部分

- OKI-CSIRTのご紹介
- ウイルス調査報告用Webシステム導入の背景
- ウイルス調査報告用Webシステム
- ウイルス調査報告用Webシステム導入の効果

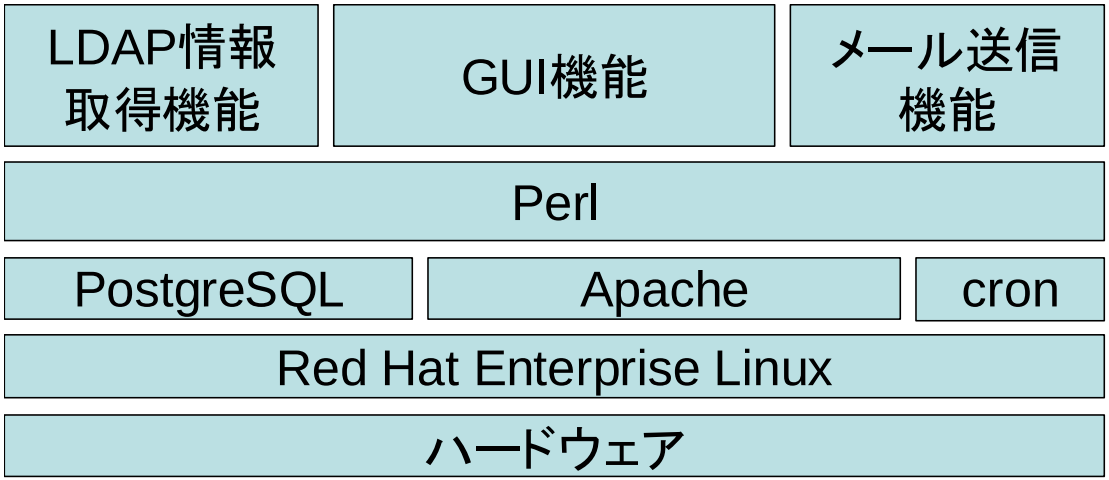
ウイルス調査報告用Webシステム



ウイルス調査報告用Webシステム構成

- ハードは、PCサーバ（余剰機の有効活用）
- OSは、Red Hat Enterprise Linux
- Webアプリケーションは、独自開発
- 社内利用のため、UI、特に管理者用UIは、必要最小限の実装

【ソフトウェア構成】



ウイルス調査報告用Web報告画面

利用者はWeb画面に表示される質問項目に答える

質問項目は、主に以下2点を明確にする事が目的
・影響範囲（顧客や商品に感染していないか）
・感染源

質問項目例:USB媒体で検知した場合

・検出した媒体の所有者は誰ですか？
　　□私物　□会社管理　□顧客

・検出した媒体を利用した場所を全てチェックしてください
　　□自宅　□社内　□顧客先

・検出した媒体を持ち出す前にウイルスチェックしましたか？

私物USB媒体は会社のルールで禁止しているが、利用するケースは残る

- OKI-CSIRTのご紹介
- ウイルス調査報告用Webシステム導入の背景
- ウイルス調査報告用Webシステム
- ウイルス調査報告用Webシステム導入の効果

ウイルス調査報告用Webシステム導入の効果

管理者視点

共通的なウイルス感染経路の見える化

ウイルス検知結果だけでは見えなかった感染経路が明らかになり、対策が可能に
例:「携帯電話を充電しようとしてPCにUSB接続しウイルス検知する例が複数」

自動トリアージ判定により管理者の負荷を軽減

自動トリアージの条件は、運用しながら適時調整を実施

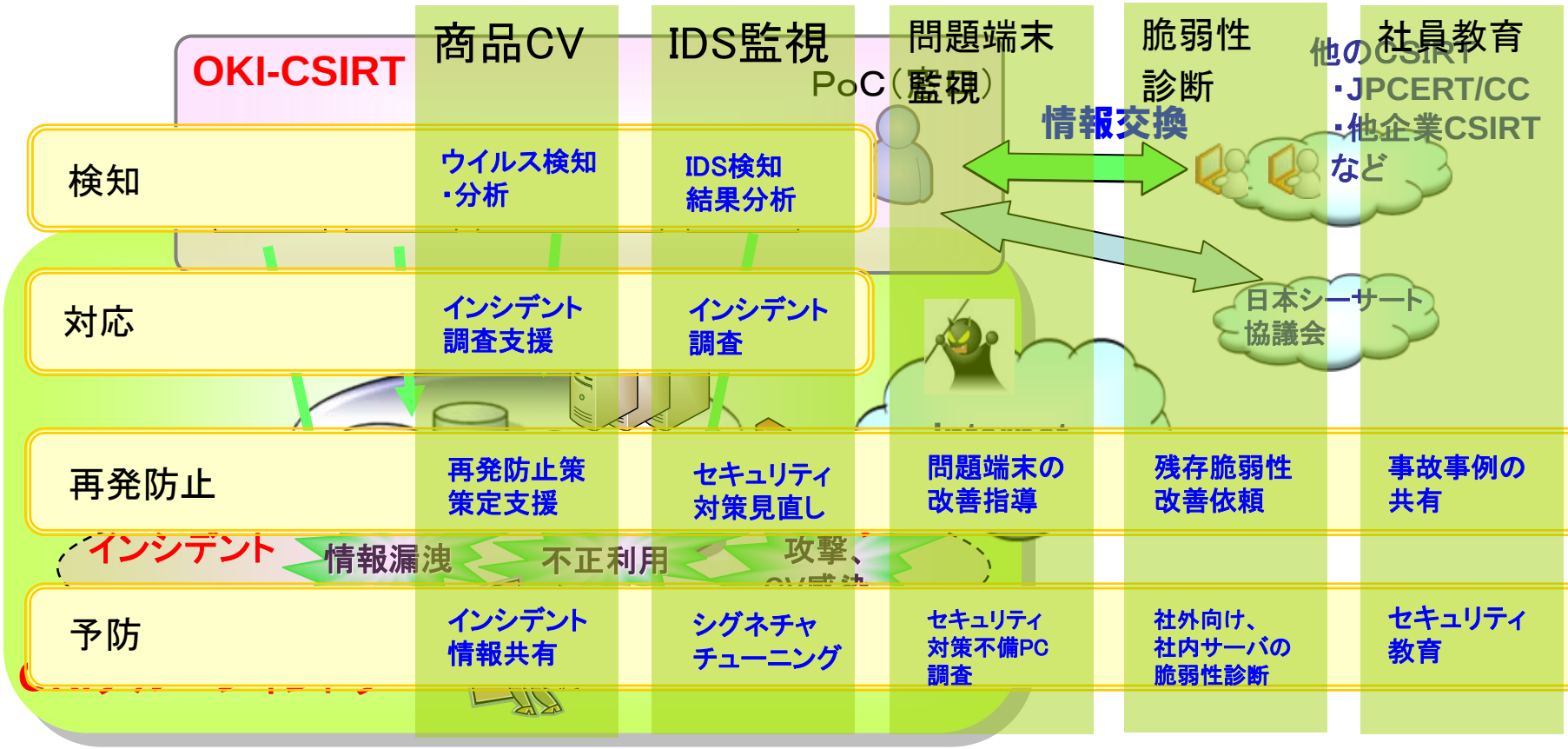
ユーザ視点

ウイルス検知後に行うべき初動と調査が明確かつ簡単に

検知後に届くメールに実施すべき初動が書かれており、調査項目もWeb画面入力で明確化

検知から予防まで各種の取り組み

OKI-CSIRTは、インシデントの検知から予防まで各種の取り組みを行います



社外への活動レポート： CSRレポートに記載

OKI-CSIRTによる セキュリティ事故対応力の強化

OKIは2008年9月にセキュリティ事故対応専門組織としてOKI-CSIRT(オキ・シーサート)を設置し、コンピュータセキュリティ事故への予防対策、事故発生時の対応力を強化しています。OKI-CSIRTは、OKIグループ内で毎月のコンピュータウイルス関連レポートの提供や技術的支援を行っているほか、日本シーサート協議会においても、コンピュータウイルス対策ガイドラインの作成に関与するなど、課題共有と解決に貢献しています。

2010年度は、社内のセキュリティソフトのバージョン状況を監視し、警告する活動を定着化させました。これにより、ウイルスの発生や事故の未然防止を徹底しています。

2010年度の状況 OKI GROUP

情報セキュリティ

OKIグループは情報セキュリティ基本方針のもと、推進組織である情報セキュリティ委員会を中心とした情報セキュリティ体制を整備しています。活動内容のレビュー(年2回)、情報セキュリティに関わるモニタリングなどを行い、個人情報をはじめとするお客様および自社の情報の適正管理・保護に努めています。

お取引先における施策定着度合いの「見える化」

OKIは2008年度より、サプライチェーン全体での情報セキュリティレベルの向上をめざし、重要秘密情報を提示しているお取引先を対象に、情報セキュリティ施策への取り組み状況確認を実施しています。具体的にはOKIが作成したチェックリストに基づいたセルフチェックを実施していただき、回答結果をOKIが独自に点数化することで、取り組み状況や課題の共有化を図っています。

2010年度も、全体として評価ポイントが4ポイント向上した結果が得られています。2010年度の特徴として、パスワードの定期的変更や所属変更に伴うアクセス権の変更などの項目が大きく改善しており、個人単位でのアクセス制御が重要と認識していただけたことがわかりました。

OKI-CSIRTによる セキュリティ事故対応力の強化

OKIは2008年9月にセキュリティ事故対応専門組織としてOKI-CSIRT(オキ・シーサート)を設置し、コンピュータセキュリティ事故への予防対策、事故発生時の対応力を強化しています。OKI-CSIRTは、OKIグループ内で毎月のコンピュータウイルス関連レポートの提供や技術的支援を行っているほか、日本シーサート協議会においても、コンピュータウイルス対策ガイドラインの作成に関与するなど、課題共有と解決に貢献しています。

2010年度は、社内のセキュリティソフトのバージョン状況を監視し、警告する活動を定着化させました。これにより、ウイルスの発生や事故の未然防止を徹底しています。

2010年度は国内と同様に、モバイルPCの盗難および紛失時に情報が漏洩しないようにHDDの暗号化を開始し、同時に、モバイルPCとしての利用が認められた機器に認可シールを貼り付ける運用を開始しました。

ISMS認証の取得を推進

OKIグループは、システム構築や関連サービス提供における信頼性を高めるため、社内情報システム構築・運用部門やシステム設計・開発部門などで情報セキュリティマネジメントシステム(ISMS*)の認証取得に取り組んでいます。

2010年度はグループ企業の再編に伴い、ソフトウェア開発にかかわるグループ企業3社を合併して設立したOKIソフトウェアがISMS認証を取得しました。2011年6月現在、OKIグループの5社7部門がISMS認証を取得しています。

■ OKIグループの ISMS 認証取得状況(2011年6月)

社名・部門名	初回登録日
日本ビジネスオペレーションズ株式会社(運用部、監査指導部)	2004年 1月30日
沖コンサルティングソリューションズ株式会社	2006年 9月20日
株式会社OKIソフトウェア	2007年12月21日
株式会社沖電気カスタマアドテック	2004年 1月31日
沖電気工業株式会社(OKIシステムセンター)	2003年 8月 4日
沖電気工業株式会社(官公事業本部、法人事業本部、官公システム事業部、情報システム事業部(各支通地区))	2004年12月27日
沖電気工業株式会社(情報企画部)	2003年 2月14日

* ISMS : Information Security Management System

個人情報保護の徹底

OKIグループは、2004年に制定した「個人情報保護ポリシー」に基づき、個人情報保護管理責任者のもと、コーポレート・営業部門・事業部門・グループ企業に個人情報保護管理者をおいて、個人情報保護を徹底しています。適切な保護措置を講ずるため、グループ各社においてプライバシーマークの付与認定取得を推進しており、2010年度はグループ再編に伴って設立したOKIソフトウェアおよびOKIプロサーブの2社において認定を取得しまし

（参考）日経NETWORK連載「CSIRT奮闘記」

- 日経NETWORK ‘09/11月号で紹介されました
- 日本シーサート協議会も連載企画に協力
- 各社CSIRTの生い立ちや特徴がわかります！


新米 セキュリティ担当者が行く！
CSIRT奮闘記
現場訪問編

CSIRT
computer security incident response team の略。

OKIとOKINETの「OKI-CSIRT」
権限行使せず技術対応に専念
「品質保証」の考え方で運営

江田 佳領子 日本シーサート協議会 JPCERTコーディネーションセンター
松山 正隼 フリーライター

BP商事のA君は，日本シーサート協議会（NCA）の協力を得て，先月から国内で活動中のCSIRTを訪問して話を聞かせてもらっている。今回の訪問先は，沖電気工業（OKI）と沖電気ネットワークインテグレーション（OKINET）が運営するOKIグループのCSIRT「OKI-CSIRT」である。

OKIは，通信機器や現金自動預け払い機（ATM）などの情報機器メーカーで，システム・インテグレーションをはじめとする情報通信関連の事業も手がけている。OKINETは，OKIのネットワークインテグレーション・サービス事業部門が独立して2005年に設立された会社である。

今回インタビューに応じてくれたのは，OKI-CSIRTの橘 喜嵐さん，原田 融さん，佐藤 正也さんの3人だ（写真1）。橘さんはOKINETのセキュリティセンタ，原田さんと佐藤さんはOKIの情報企画部に所属している。

A君はあいさつを済ませると，早速質問に入った。

A君：OKI-CSIRT設立の背景や経緯を教えてください。

原田さん：きっかけは，Winny経由の情報漏えい事故が世間で騒がれていた2006年にさかのぼります。OKIグループでは当時，同様の事故が発生した場合に備えて技術面でサポートできる部署を作ろうという話になりました。これを受けて，OKINETでセキュリティ製品のサポートやシステム・インテグレーションのコンサルを行っていた部署を「セキュリティセンタ」と名前を変え，OKIグループ内で発生したインシデントに技術面でサポートできるようにしました。これが始まりです。

橘さん：簡単に言えば，それまでお客様向けに行っていたセキュリティ・サービスをグループ内に対しても行うようになったというわけです。

A君：そこから，どのようにしてOKI-CSIRTの構築につながっていったのでしょうか。

橘さん：直接のきっかけは，2007年に発生したUSBメモリーを介して広まるウイルスに感染したという事故です。ここから，グループ全体のインシデント対応体制をしっかりと築こうという機運が高まりました。しかし当初は，グループ全体でのインシデント対応体制を具体的にどう実装すべきか悩んでいました。セキュリティセンタはあくまで技術的なサポートを行う部署にすぎなかったからです。そのころ雑誌の記事でCSIRTの存在を知り，その後た

写真1…OKI-CSIRTに所属する橘 喜嵐さん（左），原田 融さん（中），佐藤 正也さん（右）
橘さんはOKINETセキュリティセンタのセンタ長。原田さんはOKI情報企画部の担当部長，佐藤さんもOKI情報企画部の所属である。

082 • BPNETWORK 2009.11

http://itpro.nikkeibp.co.jp/article/COLUMN/20100723/350594/