WG2：なりすましログインの痕跡探し

2013年10月21日開催
ISOG-J 技術ワーキンググループ（WG2）

© 2013 ISOG-J

技術ワーキンググループ（通称 WG2）

- 最新の技術動向を調査し、最適なセキュリティオペレーション技術を探究、技術者の交流を図ることを目的としています。
- 各社持ち回りで担当

- 最近のテーマ
  - インシデント対応の現場の悩み
  - ペネトレーションテストについて考えること
  - 某社社内用CTFに挑戦
  - 某社IPS製品の紹介
  - 某社標的型攻撃対策サービスの紹介
  - 某社ログ解析ツールの紹介

© 2013 ISOG-J

前提：会員制ウェブサイトで発生する不正アクセス事件

「GREE」への不正ログインに関するご報告

2013/08/08
グリー株式会社

じゃらんnetへの「なりすましログイン」検知のご報告とパスワード変更のお願い

【重要】不正ログイン発生に関するご利用再開について（詳報）

いつもGREEをご利用いただきありがとうございます。
8月6日（火）にご報告いたしました不正アクセス発生に関しまして、GREEアカウントを一時停止させていただいております対象のお客さまへ、サービスのご利用再開に関するお知らせとなります。

三越オンラインショップ・不正アクセスについて

この度、株式会社三越伊勢丹のショッピングサイト「三越オンラインショッピング」におきまして、外部からの不正アクセスを受け、ユーザーのお客様にご登録いただいている会員情報が不正に閲覧され、情報が漏洩していたことを確認いたしました。ユーザーのお客さまをはじめとする皆様には、大変なご迷惑、ご心配をおかけいたしましたことを深くお詫び申し上げます。
今後、お知らせすべき新たな情報が判明した場合は、引き続き公表をしてまいります。何卒、ご理解を賜りますようお願い申し上げます。

「OCN」で不正ログイン、パスワード変更被害 - 乗っ取りアカウントで不正アクセス

NTTコミュニケーションズは、同社のインターネット接続サービス「OCN」において、利用者以外の第三者による不正ログインが発生したことを明らかにした。今回の攻撃には、乗っ取ったアカウントが利用されたという。

【重要】不正アクセスとアカウント管理に関するご注意

現在、弊社のオンラインサービス（「弊社サービス」）で流出したと思われるアカウント名およびパスワードを使用しスクウェア・エニックス アカウントへの不正アクセスを試みる第三者による攻撃を確認しております。

お知らせ

「バンダイナムコIDポータルサイト」への不正ログイン発生のご報告と パスワード変更のお願い

2013/09/27 15:00

お客様各位
2013年9月27日
株式会社バンダイナムコゲームス

2013年7月9日
株式会社コナミデジタルエンタテインメント

「KONAMI IDポータルサイト」への不正ログイン発生のご報告とパスワード変更のお願い

2013年7月5日
（2013年7月9日 更新）

お客様各位

任天堂株式会社

「クラブニンテンドー」サイトへの不正ログイン発生のご報告とパスワード変更のお願い

「Mobage」への不正ログインに関するご報告と
パスワード変更のお願い

ヘルプ > eoからのお知らせ > 不正ログイン被害のご報告とパスワード再設定のお願い

サービス別ヘルプページ
▸ 表行

不正ログイン被害のご報告とパスワード再設定のお願い

eBookJapan

• 閉じる

2013年08月12日 14時30分 更新

個人情報流出や仮想通貨の不正利用などの被害報告は確認されていない：

Amebaで第三者による不正ログイン～24万3266件のアカウントに影響

【重要なお知らせ】不正ログインに関する最終報告

（2013年7月23日 16時00分 追記）

不正アクセスによる「なりすまし」ログインついての調査結果ご報告（最終報告）

© 2013 ISOG-J

いわゆる「なりすましログイン／リスト型攻撃」の課題

- ユーザの課題
  - 複数の会員制ウェブサイトで同じIDとパスワードを使い回している
  - 根本的にはここが課題
- サービス提供者の課題
  - コスト
    - 二要素認証、二段階認証、ログインアラート機能等の技術的対策はある
    - サービスコストは最終的にはユーザの使用料金に転嫁される（かもしれない）
  - 技術的な課題
    - 止めること
      - 誤検知、見逃し、コストの問題
    - 見つけること
      - ユーザに迷惑をかけない
      - すぐにできる
      - 本当に見つけられる？

今回はここに注目！！

© 2013 ISOG-J

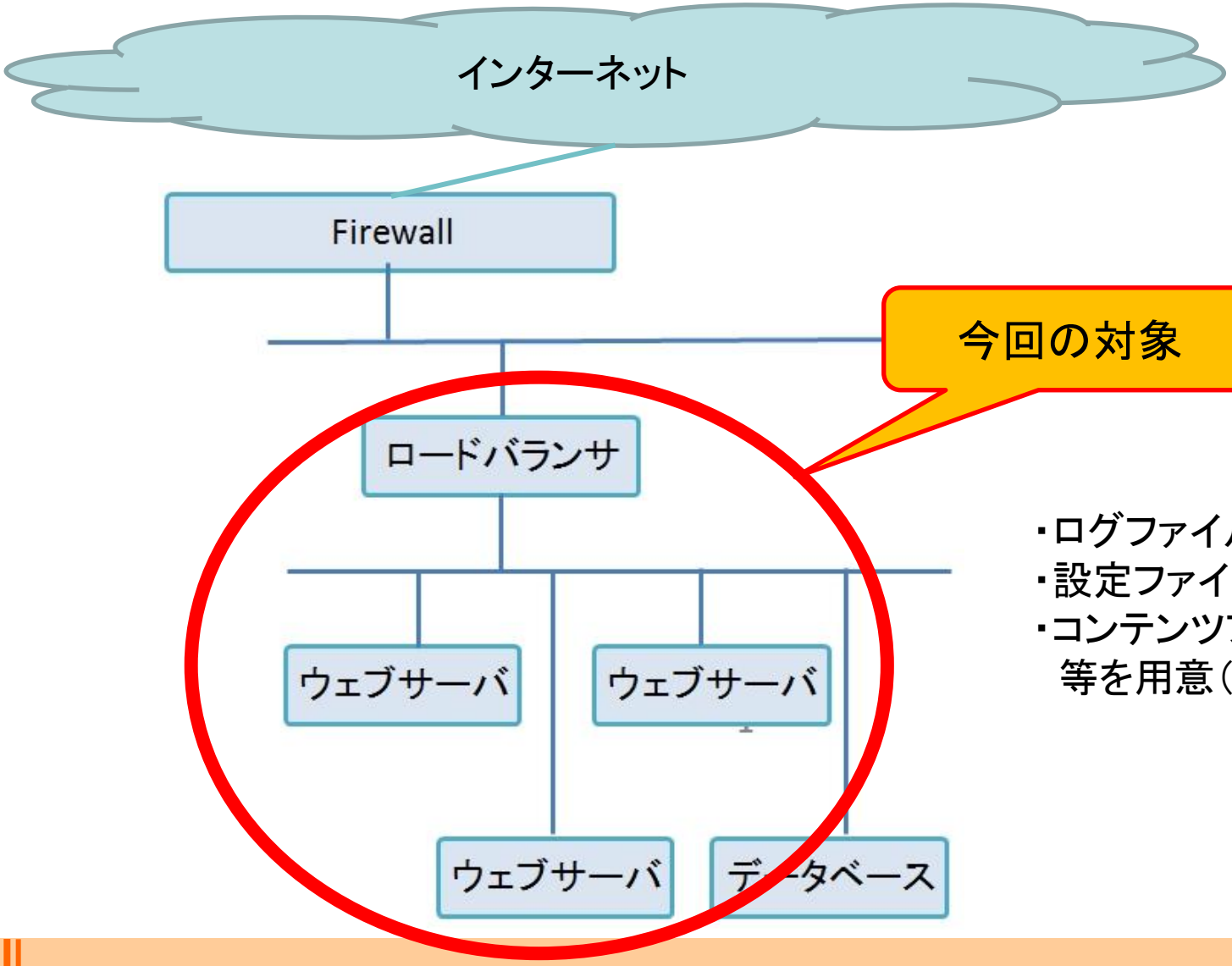
WG2開催概要

- 開催日：2013年10月21日（月）15時～18時
- 開催場所：カスペルスキー様セミナールーム
- 参加人数：17社42人
- 担当：（株）ラック 川口

- 課題：担当が用意した課題ファイルに含まれる「なりすましログイン」の痕跡を発見し、以下の情報を突き止める
  - なりすましログインを行ったIPアドレス
  - なりすましログインが成功した時刻
  - なりすましログインが成功したユーザID
  - なりすましログインを行ったUser-Agent

© 2013 ISOG-J

ログ解析対象の環境



・ログファイル
・設定ファイル
・コンテンツファイル
　等を用意（約3GB）

© 2013 ISOG-J

参加者のアプローチ

- ログインに関するログを探した
- エラーコードに注目した
- 認証系のログを探した
- 多数のアクセスがあるものに注目した
- リクエストメソッドに注目した
- 攻撃ツールのような動きについて注目した
- レポート用ツールを使用してビジュアル化した
- Excelを使用した
- grep一本で頑張った

- 詳細についてはISOG-J内における共有とする

© 2013 ISOG-J

宣伝：技術ワーキンググループ参加者募集




懇親会もセットでもお待ちしています







2013 ISOG-J

© 2013 ISOG-J