配布

# テストケースで磨く インシデントハンドリング

## ～既知の脆弱性放置による侵入・改ざんインシデントの場合～

日本シーサート協議会（NTT-CERT）

**林　郁也**

# テストケースについて

【テストケースには、機微な情報が含まれるため、事前資料としての配布は一部分のみとさせて頂いております】

物語は、CSIRTが無い会社のケースを追体験して頂く形になっています。

この追体験を通して、CSIRTに求められる機能がどのようなものか、なぜCSIRTを持つとよいのか？を皆様の胸に感じてください。

ぜひ、あなたが、自分の会社で、このようなインシデントに遭遇したら、どのように対応するかを想像しながら聞いてみて下さい。

# 目次

- インシデント概要
- インシデント詳細（時系列）
- インシデント振り返り
- まとめ

# インシデント概要

この話に登場する固有名詞は、すべて仮名です。実際の人物・団体とは関係ありません。

# 登場人物

AG商事・・・AGグループの企業（CSIRTは未だ無い）

ドット2システムズ・・・SI会社

フューチャーホスティング・・・ホスティング会社

AG-CERT・・・AGグループ（AGホールディングス）のCSIRT

松本・・・AG商事サイト運用責任者。
あまり技術に詳しくない。

瀬川・・・ドット2システムズ若手SE。

渡部・・・AG-CERTのインシデントハンドラー。

# 当該システムの構成と運用形態

AG商事は、㈱ﾌｭｰﾁｬｰﾎｽﾃｨﾝｸﾞのホスティングサービスを利用し、ポータルサイトの運用を行っていた。
サイトの構築はSIerであるﾄﾞｯﾄ2ｼｽﾃﾑｽﾞに依頼していた。

## AG商事：ﾎﾟｰﾀﾙｻｲﾄ構成図

ﾄﾞｯﾄ2：ｼｽﾃﾑ構築

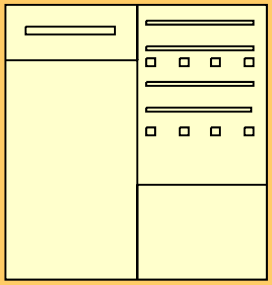
インターネット

公開Webサーバ

＋

環境・ツール類

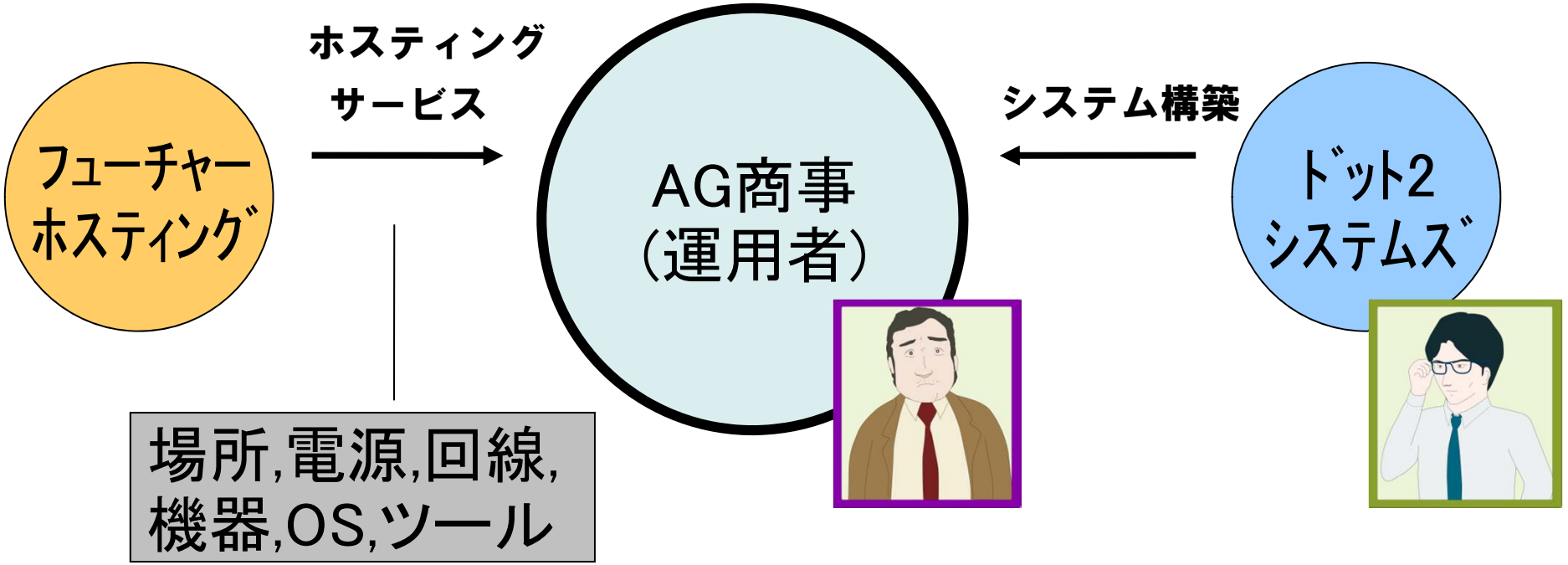
データベースサーバ
（外部から直接アクセスはできない）



ﾌｭｰﾁｬｰﾎｽﾃｨﾝｸﾞ㈱：
ﾎｽﾃｨﾝｸﾞｻｰﾋﾞｽ提供

# 各契約と責任分担

フューチャーホスティングはAG商事に対して、場所・電源・回線・機器・OS・ツールを提供、 ドット2システムズはポータルサイトの構築をAG商事に提供している。
電源と場所以外についてのメンテナンスは、AG商事が管理することとなっていた。

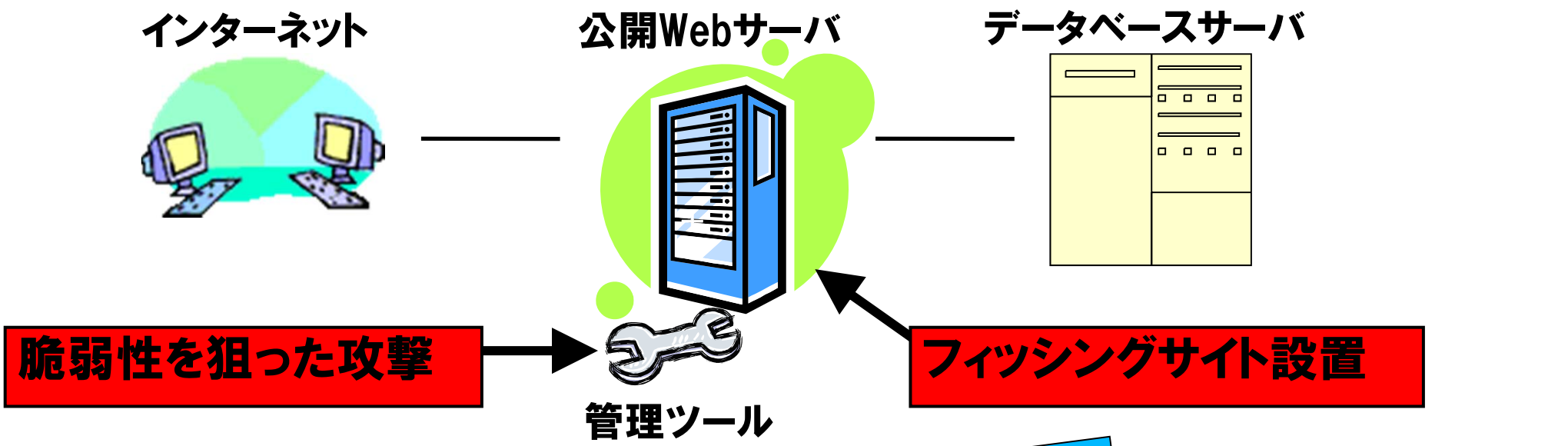


# まとめ

# 振り返りのまとめ

| | 反省点 | 対策例 |
|---|---|---|
| 技術面 | 脆弱性を放置していた | ・最新のセキュリティアップデートやワークアラウンドの適用 |
| | 管理ツールは実際に使用していなかった | ・セキュリティを考慮した適切な作り込み・定期診断の実施 |
| | アクセスが制限されていなかった | |
| | 不要なツールを有効なままにしていた | |
| 運用面 | 長期間にわたり、インシデントの発生に気がつかなかった | ・監視・検知のしくみの整備 |
| | (非常時の)連絡受付窓口がなかった | ・セキュリティ問題に関する外部からの連絡先の設置 |
| | 非常時・緊急時の連絡体制がなかった | ・平時・非常時、それぞれの想定に基づいたステークホルダー(経営～運用、保守ベンダなど)との作業分担、連絡体制の整備<br>・訓練の実施 |
| | 構築ベンダとの保守契約がなかった | |

# もし、AG商事にCSIRTがあったら…




①脆弱性情報を調査・収集する

②外からの通報を受ける窓口

③検知

④いち早いインシデント
レスポンス

CSIRT

⑤設計段階からの関与による防衛
セキュリティ監査による診断

⑥事前対策への反映

⑦テストケース（ベストプラクティス）
による教育・訓練　→　この講座

# 最後に

## ■CSIRTコミュニティの力

今回のケースは、過去にあった教訓的な事例を、CSIRTsで持ち寄り、組み合わせて作成したものです。

このような追体験を通してベストプラクティスを知ることが、いざというときのインシデント対応、インシデントそのものを未然に防ぐ活動につながります。