D-Case適用事例2
2012年のPC遠隔操作による誤認逮捕

DEOSプロジェクト

2013年7月19日
DEOS研究開発センター

JST-CREST

1. 本事案の概要

1. 遠隔ウィルスによるトラブル発生概要
   - 2012年(平成24年)の初夏から秋にかけて、日本において、犯人がネットの掲示板を介して他者のパソコンを遠隔操作し、これを踏み台としてウェブサイト、インターネット掲示板、メールを通じて襲撃予告や爆破予告などの犯罪予告を行ったサイバー犯罪。その犯人として4人が誤認逮捕された
2. 誤認逮捕が発生した原因
   - 書き込みに使用されたPCのIPアドレスと犯人として誤認逮捕された人のPCのIPアドレスが一致した
   - 複数のウィルス対策ソフトの検査では遠隔操作ウィルス(新種のトロイの木馬)の痕跡の発見は不可能であった
3. 誤認逮捕であることが判明した根拠
   - 逮捕後の押収したPCの解析で、犯人とされていたPCから遠隔操作ウィルスの1つである新種の トロイの木馬を検出した(このトロイの木馬は自分自身を削除する機能を備えているが、ある1人のPCはトロイの木馬が残っていた)
   - 真犯人を名乗る者からの犯行声明文

(出典) Wikipedia 「パソコン遠隔操作事件」
http://ja.wikipedia.org/wiki/%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6

1. 本事案の概要

- PC遠隔操作による犯罪予告一覧(誤認逮捕関連)

事件の内容	罪名
1. 大阪の男性のPC　※大阪府警が誤認逮捕	
・大阪市の商店街での無差別殺人予告メール(注)	偽計業務妨害
・日本航空機への爆破予告メール	ハイジャック防止法違反
2. 福岡の男性のPC　※警視庁が誤認逮捕	
・子役女優への殺害予告メール	脅迫
・東京の幼稚園への無差別殺傷予告メール	威力業務妨害
3. 三重の男性のPC　※三重県警が誤認逮捕	
・東京の携帯電話ショップへの襲撃予告を掲示板に投稿	威力業務妨害
・伊勢神宮への爆破予告を掲示板に投稿	威力業務妨害
4. 東京の男性のPC　※神奈川県警が誤認逮捕	
・小学校への襲撃予告を横浜市のサイトに投稿	威力業務妨害

(出典)　朝日新聞記事「PC遠隔操作、計10件で起訴　誤認逮捕事件の捜査終結」(2013年6月28日)　をもとに作成

(注)大阪府警察の報告書では、大阪市のホームページへの書き込みと記載されている

1. 本事案の概要(大阪府警での捜査の事例)

- 誤認逮捕の事案での捜査事例を大阪府警の例で示す

1. 事件の認知
   - 平成24年7月30日、大阪府南警察署(以下「南警察署」という。)に対する、「市のホームページ内に設けられた「市民の声」という相談窓口に無差別殺人予告が書き込まれた」との大阪市職員からの通報により本件を認知した
   - 書き込み内容から、インターネットを介した威力業務妨害事件と判断した
2. 捜査概要(9月14日、偽計業務妨害罪で起訴された)
   - 本件書き込み時のIPアドレスが判明するとともに、本件書き込みはA氏のモバイルルーターから行われたことが判明し、A氏はルーターにパソコンを接続し、大阪市のホームページへアクセスして本件書き込みを行い、その後アクセス履歴を消去(一部消去漏れ)したと推定された
   - 第三者による犯行可能性の検討がされたが、可能性は低いと判断された(A氏のルーター(無線LAN)やパソコンの無断使用、「CSRF攻撃」での書き込み、遠隔操作での書き込み、時限設定のウイルスの自動実行)
   - 最新ウイルス対策ソフトによるウイルスが検知されなかった
   - 自動実行ファイルの確認で不審点がなかった
   - 本件書き込みに係る履歴の一部が残っていること、また、A氏のパソコン内より、本件書き込みに係る履歴の一部が削除されている事実と、A氏の供述が矛盾することから、証拠隠滅を図ったと認められた

出典:「インターネットを利用した犯行予告ウイルス供用事件の検証結果」(大阪府警察、平成24年12月)

1. 本事案の概要(大阪府警での捜査の事例)

3. A氏の釈放に至る経緯と遠隔操作ウイルス「iesys.exe 」に関する捜査
   - 9月18日、伊勢神宮等に対する犯行予告事件で男性を逮捕していた三重県警察から捜査協力の依頼があった
   - 19日、本件捜査に従事した当府警サイバー対策室員が三重県警察を訪問し、逮捕男性のハードディスク等の不審な状況を確認し、「iesys.exe」という名称のファイルが自動実行していることを確認した
   - 同ファイルは、本件(大阪事件)捜査過程で、8月1日午前5時時点の状態のパソコン内に存在した「iesys.exe 」と同じファイル名であったため、解析を行い、遠隔操作ウイルスである可能性が浮上した
   - 9月21日、A氏は釈放された

- (参考)三重県の男性のPCにトロイプログラムが残っていたことについて
   - 普段からCPUの使用率をチェックしていた男性EはPCの動きが遅くなった際にCPUの使用率が不自然に高くなっていたことを察知し、ダウンロードから約1時間後にトロイプログラムを自分で停止させた
   - 男性Eは三重県警察の尋問に対し、一例として遠隔操作の手法を説明。逮捕から4日後の9月18日頃からより詳細な解析を実施したところ、この男性EのPCについては、他の3人とは異なりトロイプログラムが消去されずに残っていたことから新種のトロイプログラムに感染していたことが判明した

(出典) Wikipedia 「パソコン遠隔操作事件」
http://ja.wikipedia.org/wiki/%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6

1. 本事案の概要(「遠隔操作ウイルス」事件の手口)

1. 2ちゃんねるの掲示板に「無料の便利ツール」と称した実行形式のファイルをダウンロードさせるリンクが書き込まれ、これをダウンロードしたユーザーのPCに不正プログラム(iesys.exe)が送り込まれた
2. ユーザーが「iesys.exe」を実行するとバックドアが作られ、サイバー攻撃者がPCを不正に遠隔操作できる状態になる
3. 不正操作は、攻撃者が掲示板サイトにコマンドを書き込み、iesys.exeに感染したPCがこのコマンドを把握することで行われた。これにより、攻撃者はPCのユーザーになりすまして、犯罪予告を掲示板サイトに書き込むなどの行為をした
4. 不正操作を行う際には、「Tor」と呼ばれるP2Pでの通信経路のデータを改ざんして追跡をできなくさせるツールを利用した
5. ウイルス対策ソフトが「iesys.exe」を定義ファイルで検知できるようになったのは、10月以降であった

出典:「遠隔操作ウイルス」事件に関する「日本ネットワークセキュリティ協会(JNSA)」の記者会見(2012年10月17日)に関する報道
(2012年10月17日 ITmedia Web記事)

2. 本事案の分析

- 利用者がPCを安全に利用（継続利用）する観点から本事案のIT系技術に関連する原因を以下に示す

（誘導）

– ウイルスが仕掛けられた不正プログラムをダウンロードするように誘導された

（検知）

– 新しいウィルス（トロイプログラム）のため、ウイルス対策ソフトウェアの最新の定義ファイルでもこのウイルスを検知できなかった

– ウイルスが自動で動作するため、ウイルスの挙動を利用者が認識することができなかった（三重県の事案を除く）

（痕跡）

– ウイルスの動作による掲示板への書き込みに関する痕跡が残ったままとなった

– ウイルス自体が削除されたため、ウイルス自体の痕跡が残らなかった

3. 本事案の原因に対応するD-Case適用のポイント

＜適用にあたっての基本的な考え方＞

- PC利用にあたって、自身、および、対外的に影響を与えないための継続的な安全利用(注意義務の履行)のケースを明確化する

原因

(誘導)

- ウイルスが仕掛けられた不正プログラムをダウンロードするように誘導された

(検知)

- 新しいウィルス(トロイプログラム)のため、ウイルス対策ソフトウェアの最新の定義ファイルでもこのウイルスを検知できなかった
- ウイルスが自動で動作するため、ウイルスの挙動を利用者が認識することができなかった(三重県の事案を除く)

(痕跡)

- ウイルスの動作による掲示板への書き込みに関する痕跡が残ったままとなった
- ウイルス自体が削除されたため、ウイルス自体の痕跡が残らなかった

D-Case適用ポイント

PCの安全利用に関するD-Caseの適用

1. 安全利用を示すPC利用(動作)のモニタリング
   ・利用者、訪問したURLの履歴、キータイプ情報、ネットワーク上の通信記録などの可視化

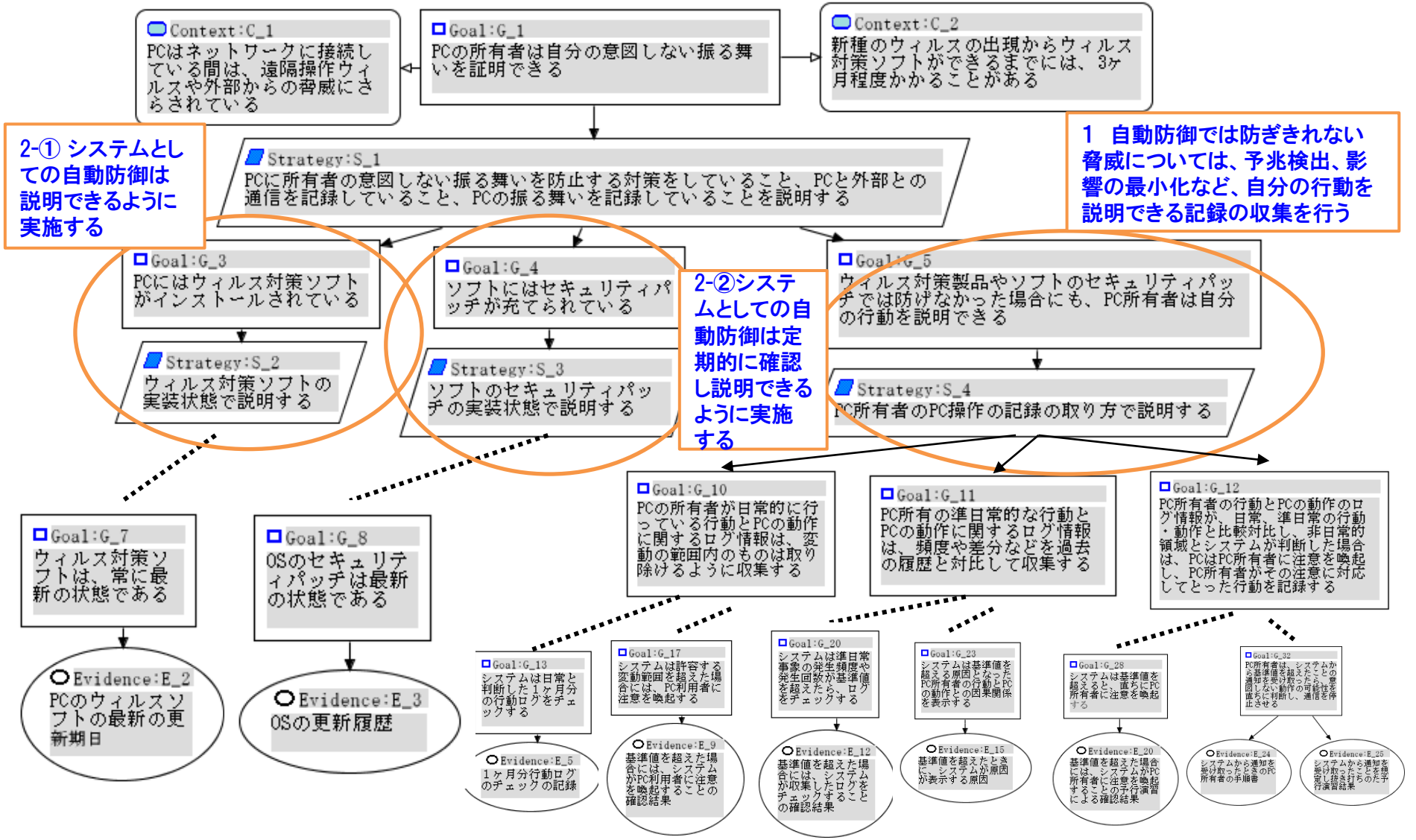
   ⇒ PC利用に関する説明責任

2. PCの安全利用のための対策の明確化
   ①ウイルス対策ソフトウェアの最新化と実行
   - ウイルス対策ソフトウェアの実行履歴
   - ウイルス定義ファイルの最新化の履歴、など(実行記録も含めた記録)

   ②ソフトウェアのセキュリティ対策のための最新化
   - セキュリティパッチの実施履歴

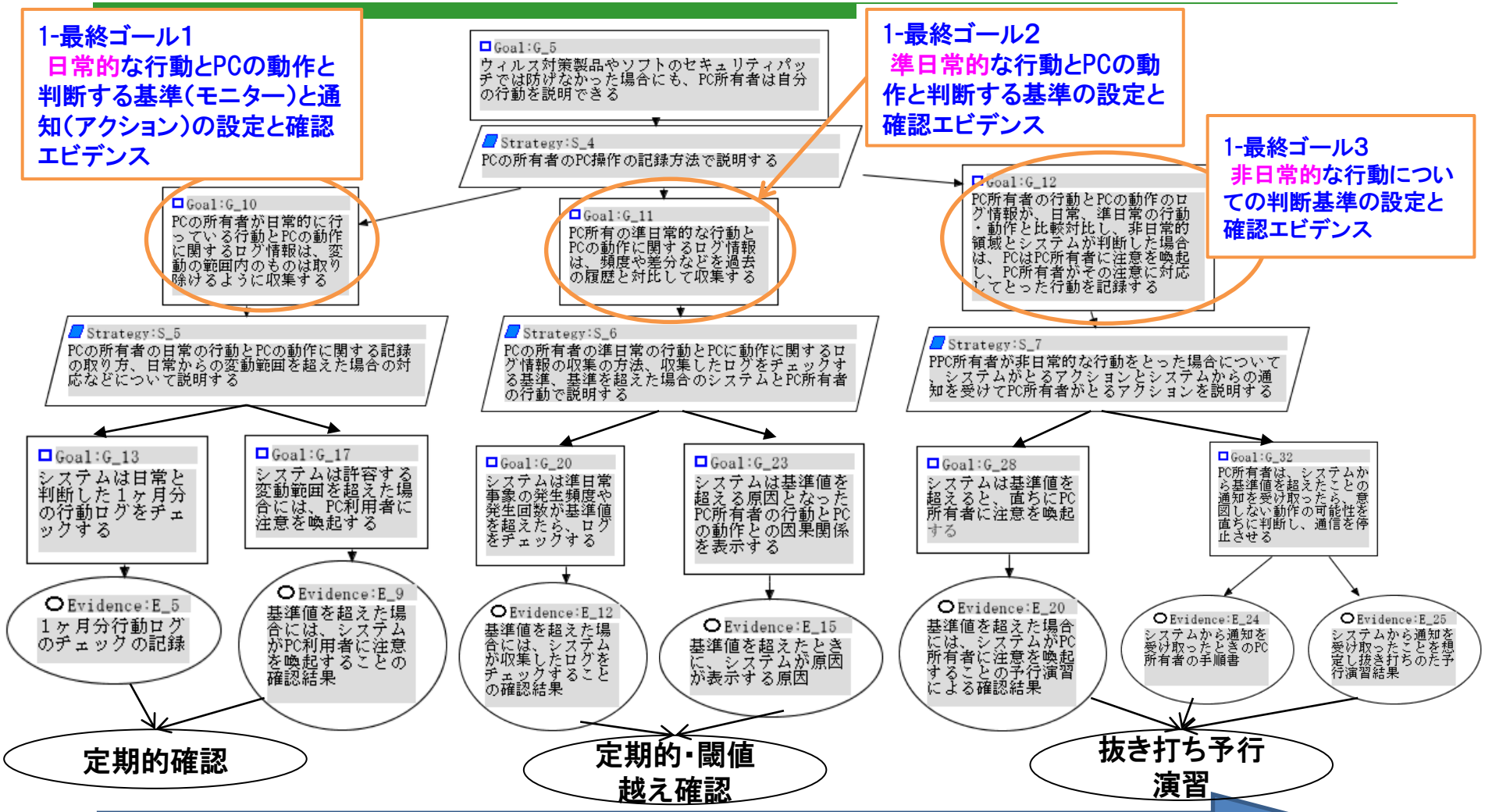
4. D-Case適用時の有効性

（発生事象を100%カバーする場合分けの支援）



4. D-Case適用時の有効性

（システムと人間が連携し、ディペンダビリティを改善できる最終ゴールとエビデンスの展開）



5. D-Case適用時のまとめ

D-Case適用
により

- 網羅性の可視化： システムによる自動防御だけでは対応することができない脅威を含めて、説明責任を果たすためのケースを可視化できる
  - （適用事例での例） PCの所有者は自分の意図しない振る舞いを証明するケースを分析
- 判断基準の設定とエビデンス確認： 日常、準日常、非日常に応じた判断基準の設定と対応するエビデンスによる説明責任の容易化を図ることができる
  - （適用事例での例）行動とPCの動作のログ情報が、日常、準日常の行動・動作と比較対比し、非日常的領域とシステムが判断した場合は、注意喚起。（影響最小化行動）

その結果

- 自分の意図しない振る舞いに対する説明責任の実現
  （PC安全利用支援ツール（説明責任支援）の利用）
- システムによる自動防御では防ぎきれない脅威に対する予兆検出や影響の最小化の実現