JPNIC・JPCERT/CC
Security Seminar 2003

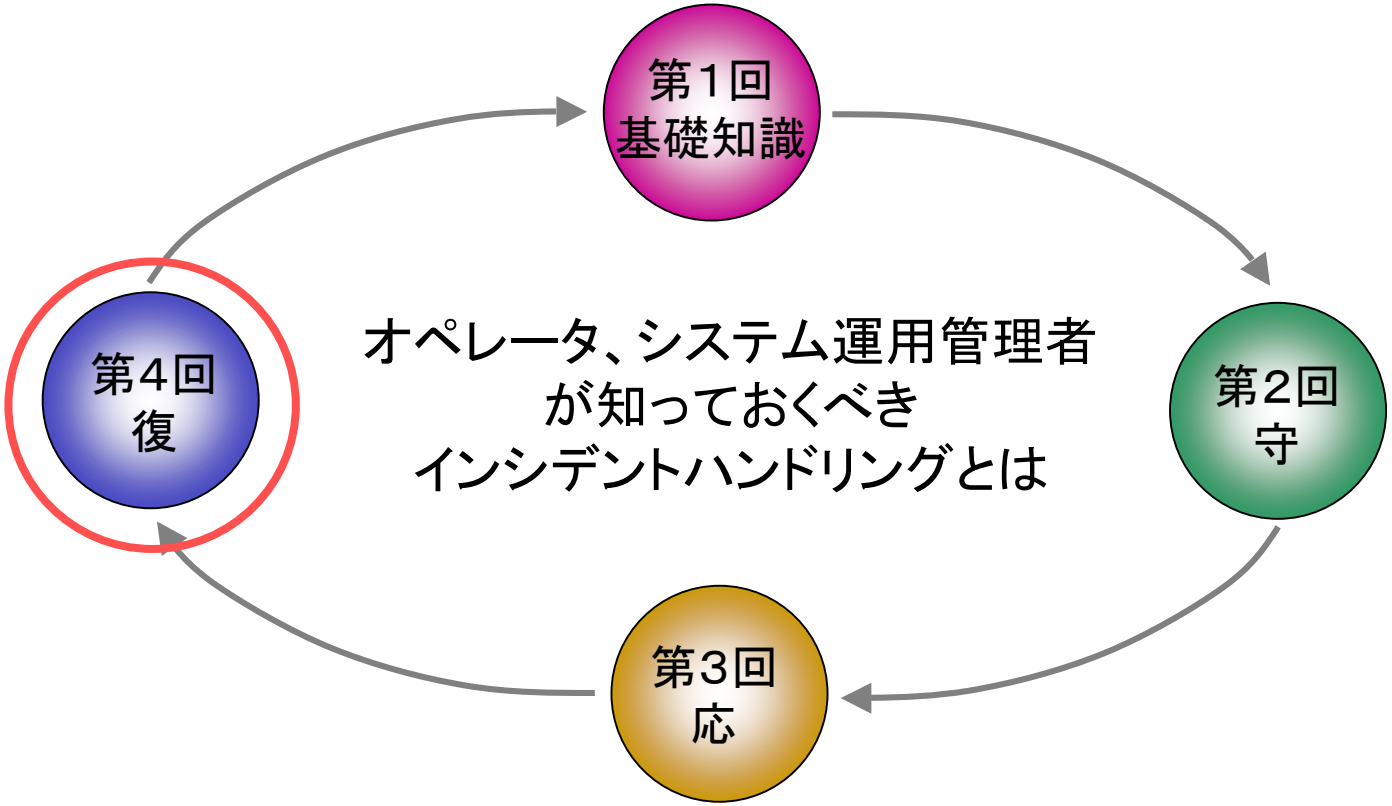
『復：～インシデントから復旧する～』
具体的な復旧方法

2004年2月4日

株式会社 NTTデータ
セキュリティビジネスユニット
西尾　秀一
nishios@nttdata.co.jp

本日の講演

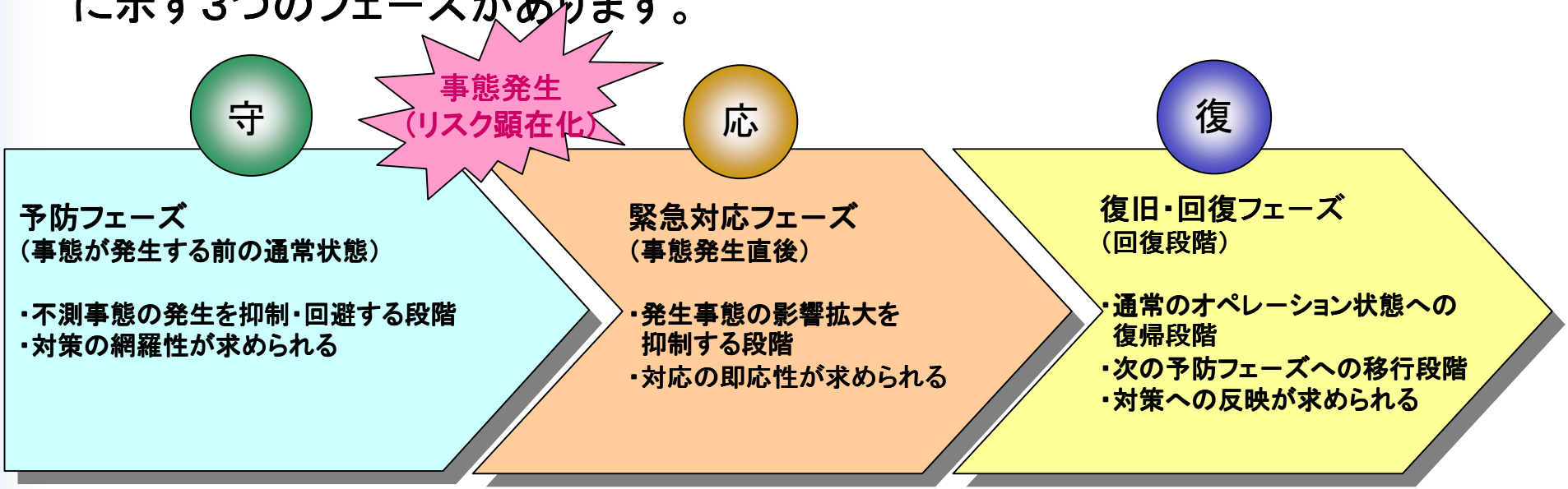
- インシデントを受けたシステム・サービスの復旧のポイント



リスク対応における「復旧フェーズ」の意義

組織リスクへの対処を行うタイミング

●組織リスクへの対処方法では、その方法を実行するタイミングとして、以下に示す3つのフェーズがあります。



組織リスクマネジメントのうちネット関連の安全を図る「情報セキュリティ対策」の場合には、侵入やハッキング等の「事態発生の認知」が非常に難しく、現状、如何に迅速に状況の把握が行なえるかが課題となっています。

（NTTデータ経営研究所「企業におけるリスクマネジメント」より抜粋・編集）

組織が被る被害

●不測事態の発生により被る直接的な被害以上に、企業の機会損失や社会的な信用失墜、さらに株価の暴落などの間接的な被害を如何に抑えるかが企業にとって重要な問題です。

直接的な被害	間接的な被害
・金銭の損失 ・建物や設備等の損害 ・死亡、負傷等の損害	・本来得られたはずの利益（機会損失） ・株価の暴落（社会的な信用失墜） ・組織活動の混乱、イメージ低下

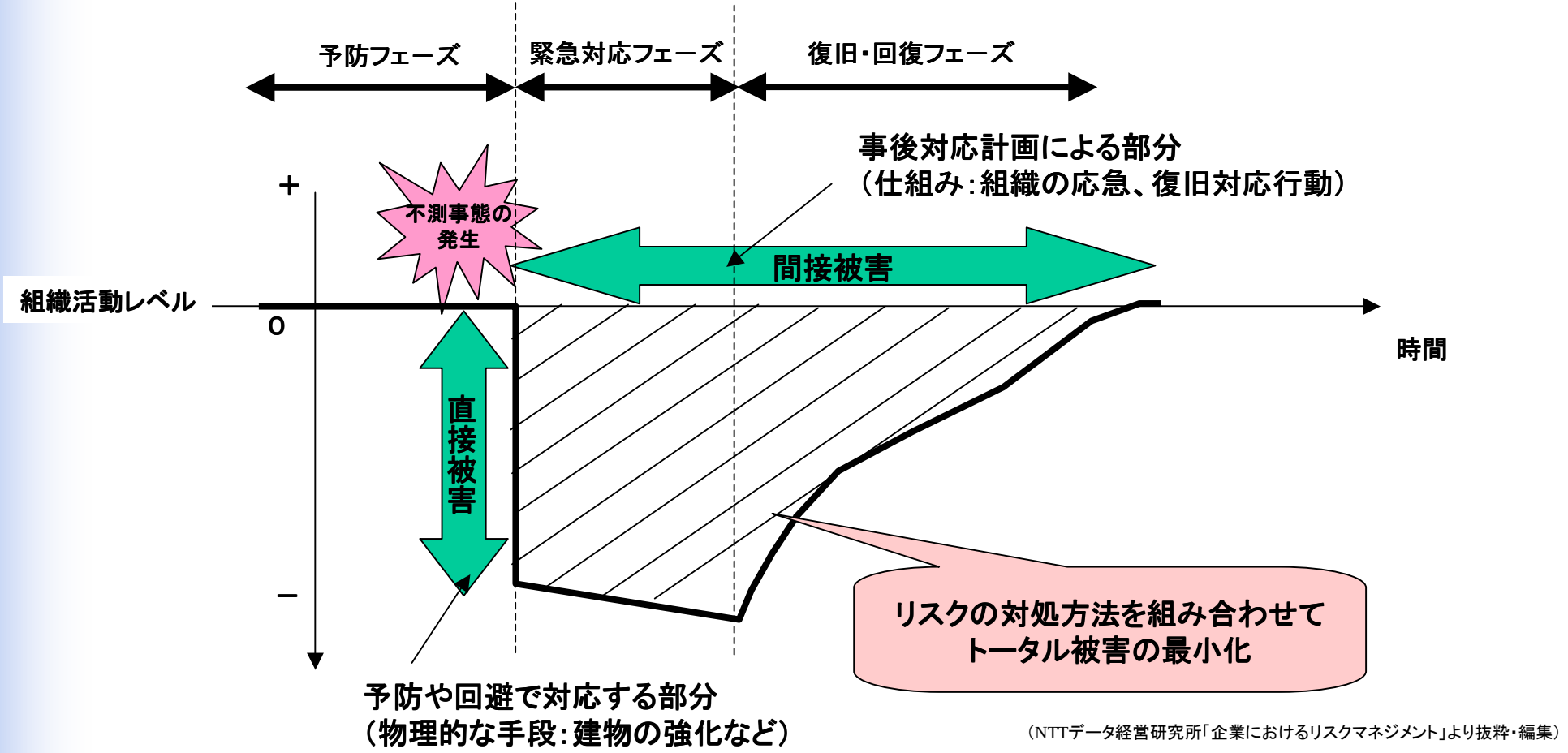
直接被害の大きさだけを見て情報セキュリティ対策の必要性を論じがちだが、
本来は全体的な被害を考慮したセキュリティ対策の検討が必要

情報セキュリティが破られた場合、比較的低額と予測される直接的な被害に比べ、
間接被害は10倍を遥かに超えることが多発するものと想定されます。

（NTTデータ経営研究所「企業におけるリスクマネジメント」より抜粋・編集）

リスクへの対処

●一般的に、物理的な対策（建てる場所の選定や施設の強化）は、主に直接的な被害を軽減するための予防や回避が中心であり、仕組み（組織の復旧対応行動）、人手による対応対策は、主に間接的な被害を軽減するための事後対応が中心です。



（NTTデータ経営研究所「企業におけるリスクマネジメント」より抜粋・編集）

「復旧フェーズ」におけるポイント

復旧フェーズにおける実施事項

1. 残存被害がないかどうかの調査
   - 社内の類似システム・サービスを含め、同様の被害または緊急対応フェーズでは発見できなかった被害がないかどうかを網羅的に調査する必要があります。
2. 通常オペレーションへの復帰
   - 代替サービス、バックアップシステム、縮退運転から、元の状態にシステムやサービスを復旧させる必要があります。
3. 原因分析
   - インシデントの発生原因を分析します。必要に応じて、関係者へのヒアリングや専門家の支援を仰ぐ必要があります。
4. 再発防止策の検討および実施
   - 技術的な防止策および人的・組織的な防止策の両面を検討し、着実に実行します。インシデント対応の顛末について社内（経営陣、オペレータなどの各レベル）で情報共有することも重要です。
5. ユーザへの対応
   - サービスやシステムのユーザに対して、インシデント対応の状況および再発防止策について適切に説明する必要があります。
6. その他社外への対応
   - インシデントの種類や被害状況に応じて、JPCERT/CC、IPA、監督官庁、親会社などの外部機関へ連絡・相談します。また、場合によってはメディア等への対応も必要となります。犯罪行為に関わる場合には、警察（サイバーポリス）への通報も必要です。

1．残存被害がないかの調査

□　残存被害等の網羅的な調査
- ・被害状況の全体的な把握
- ・緊急対応時に発見できなかった残存被害があるかの調査
- ・バックアップへの被害の有無の確認

□　類似システム、サービスの調査
- ・類似システム、サービスの洗い出し（全社網羅的に）
- ・被害状況の調査
- ・インシデント発生の可能性の調査（使用OS、設定等の確認）

□　緊急対処の指示
- ・インシデント発生システムと同等の緊急対策を実施するように指示
- ・緊急対処の実施状況の把握

□　全社対応への注意喚起
- ・全社復旧プログラム（抜本対策、強化策）からの指示待ちを要請
- ・当面の監視体制の強化を指示

2. 通常オペレーションへの復帰（その1）

- □ 復旧責任者・体制の確認
  - ・復旧にあたっての責任者は誰？
  - ・復旧のための費用、要員の手配は誰が行うか？
  - ・関係者の把握
- □ 復旧手順の確認
  - ・復旧手順書の有無
  - ・手順書の内容確認
- □ 復旧レベルの確認
  - ・完全復帰？or部分（段階）復帰？or改善復帰？
  - ・復旧期限の確認
  - ・復旧業務の優先度の確認（通常業務との関係）
- □ 緊急対応策の実施状況の確認（IRTからの引継ぎ）
  - ・バックアップ状況
  - ・代替ハードウェア、ソフトウェア、ネットワーク
  - ・代替サービスや縮退運転の有無の確認
  - ・手作業による代替作業の有無
  - ・被害範囲の状況
  - ・誰が緊急対応を実施したかの確認

2. 通常オペレーションへの復帰(その2)

- □ 復旧計画の策定
  - ・復旧計画書の策定
  - ・必要なリソース(費用、要員)の見積もり
  - ・復旧スケジュールの見積もり
- □ 復旧計画の調整・承認
  - ・社内外関係者との調整(協力体制、スケジュール、費用負担など)
  - ・責任者の承認を得る
- □ 復旧準備作業の実施
  - ・復旧準備(リストア、再構築、再設定等)
  - ・原因となった脆弱性対策の実施
  - ・試験
  - ・復旧の周知、日程調整(ユーザ)
- □ 復旧作業の実施
  - ・復旧作業
  - ・復旧作業終了報告(責任者、ユーザ)
- □ 監視強化
  - ・しばらくは復旧状況の監視を強化する必要あり

3. 原因分析

□ 原因分析、再発防止策実施の責任者・体制の確認
- ・原因分析、再発防止策実施にあたっての責任者は誰？
- ・原因分析、再発防止策実施のための費用、要員の手配は誰が行うか？
- ・関係者の把握

□ 情報収集
- ・当該インシデントに関するセキュリティ専門家等からの情報収集
- ・原因分析に必要な情報の有無の確認
- ・証拠保全状況の確認
- ・関連法規の有無
  （不正競争防止法、個人情報保護法、不正アクセス禁止法など）

□ インシデント発生原因の分析
- ・攻撃元の詳細な分析、特定（社内？or社外？）
- ・システムログ、セキュリティログの詳細な分析
- ・ウィルス感染経路の特定
- ・関係者へのヒアリング（多面的なヒアリング、人権への配慮が必要）
- ・必要に応じて専門家への協力要請

4. 再発防止策の検討および実施（その1）

- □ 再発防止策の検討
  - ・目標レベルの決定
  - ・技術的対策案、運用的対策案、法的対策案の検討
  - ・必要なリソース（費用、要員）の見積もり
  - ・再発防止策実施スケジュールの見積もり
- □ 再発防止策実施計画の調整・承認
  - ・社内外関係者との調整（協力体制、スケジュール、費用負担など）
  - ・責任者の承認を得る
- □ 再発防止策準備作業の実施
  - ・実施準備（調達、再構築、再設定、ポリシー改定、マニュアル改定等）
  - ・試験、レビュー
  - ・日程調整
- □ 再発防止策の実施
  - ・再発防止策の実施（当該システム、サービス）
  - ・再発防止策の実施指示（類似システム、サービス含む全社）
  - ・再発防止策実施状況の確認

4. 再発防止策の検討および実施（その2）

- □ 予備機等への再発防止策の実施
  - ・予備機、バックアップへも同様の対策を実施
- □ 攻撃者等への対抗措置の検討および実施
  - ・社内：解雇、処罰、注意等
  - ・社外：法的措置、損害賠償、委託先の契約解除等
  - ・顧問弁護士への相談

- □ 緊急時対応計画および復旧計画の見直し（事故からの学習）
  - ・一連のインシデント対応各フェーズの反省
  - ・緊急時対応ポリシー、体制、手続き等の見直し
  - ・バックアップ、代替手段の見直し
  - ・復旧ポリシー、体制、手続きの見直し
- □ 情報共有、教育、訓練、監査の実施
  - ・一連のインシデント対応の顛末の関係者（経営陣、オペレータ等）への周知（対応内容、コスト、最終被害等）
  - ・緊急時対応に対する（再）教育の実施
  - ・緊急時対応訓練、復旧訓練の（再）実施
  - ・平常時のセキュリティ監査の実施

5. ユーザ等への対応（その1）

□ ユーザ対応責任者・体制の確認
- ・ユーザ対応にあたっての責任者は誰？
- ・ユーザ対応のための費用、要員の手配は誰が行うか？
- ・関係者の把握（営業、総務部渉外担当、法務部等）

□ 情報収集、準備
- ・対象ユーザの洗い出し
- ・ユーザ被害の把握（範囲、金額）
- ・ユーザとの契約内容、SLAの確認
- ・クレームへの一次対応状況の把握
- ・顧問弁護士への事前相談

□ ユーザ対応策の検討
- ・ユーザ説明方針および方法の検討
- ・損害賠償の検討
- ・ユーザ説明ドキュメントの作成
  （謝罪文、原因究明姿勢、再発防止策、損害賠償）
- ・責任者の承認を得る

5. ユーザ等への対応（その2）

□ ユーザ説明の実施
- ・ユーザ説明ドキュメントの送付
- ・ユーザ説明会の実施、個別訪問の実施

□ クレーム、損害賠償等への対応
- ・顧問弁護士との相談
- ・訴訟対応の検討

6. その他社外への対応

- □ 外部機関等への報告
  - ・報告先の決定（JPCERT/CC、IPA、監督官庁、親会社、グループ会社など）
  - ・報告内容の決定（インシデントの種類、被害、対処方法、再発防止策等）
- □ メディアへの対応
  - ・公表方法、時期の決定（指摘されるまで待つ？or自ら公表する？）
  - ・公表範囲、内容の決定
  - ・社内へのメディア対応方法の周知、徹底（窓口の一本化が基本）
  - ・社内協力体制の構築（広報部）
- □ 株主への対応
  - ・株価の変動、風評の把握
  - ・株主への説明方法、時期の決定
  - ・社内協力体制の構築（総務部）
- □ 犯罪捜査への協力
  - ・証拠提出によるシステム、サービスへの影響検討
  - ・証拠提出範囲の検討
  - ・社内協力体制の構築（法務部、コンプライアンス部）
- □ 脅迫者への対応
  - ・顧問弁護士、警察等と相談の上、断固とした対応が重要

ケーススタディ

情報社会で想定される脅威

情報社会に対する脅威は、機器のシステム故障からサーバーテロによる脅威まで幅広く想定しなければならない

2001年9月11日の米国多発テロで現実のものに・・・

人的エラー

インサイダーによる犯罪

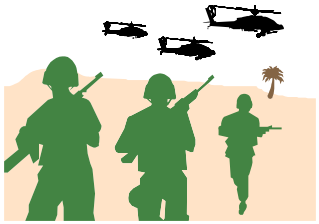
国家諜報戦

産業スパイ

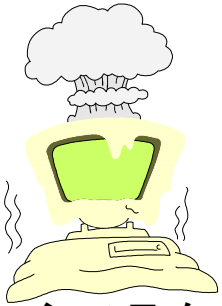
外部からの犯罪

自然災害、火災

テロリズム



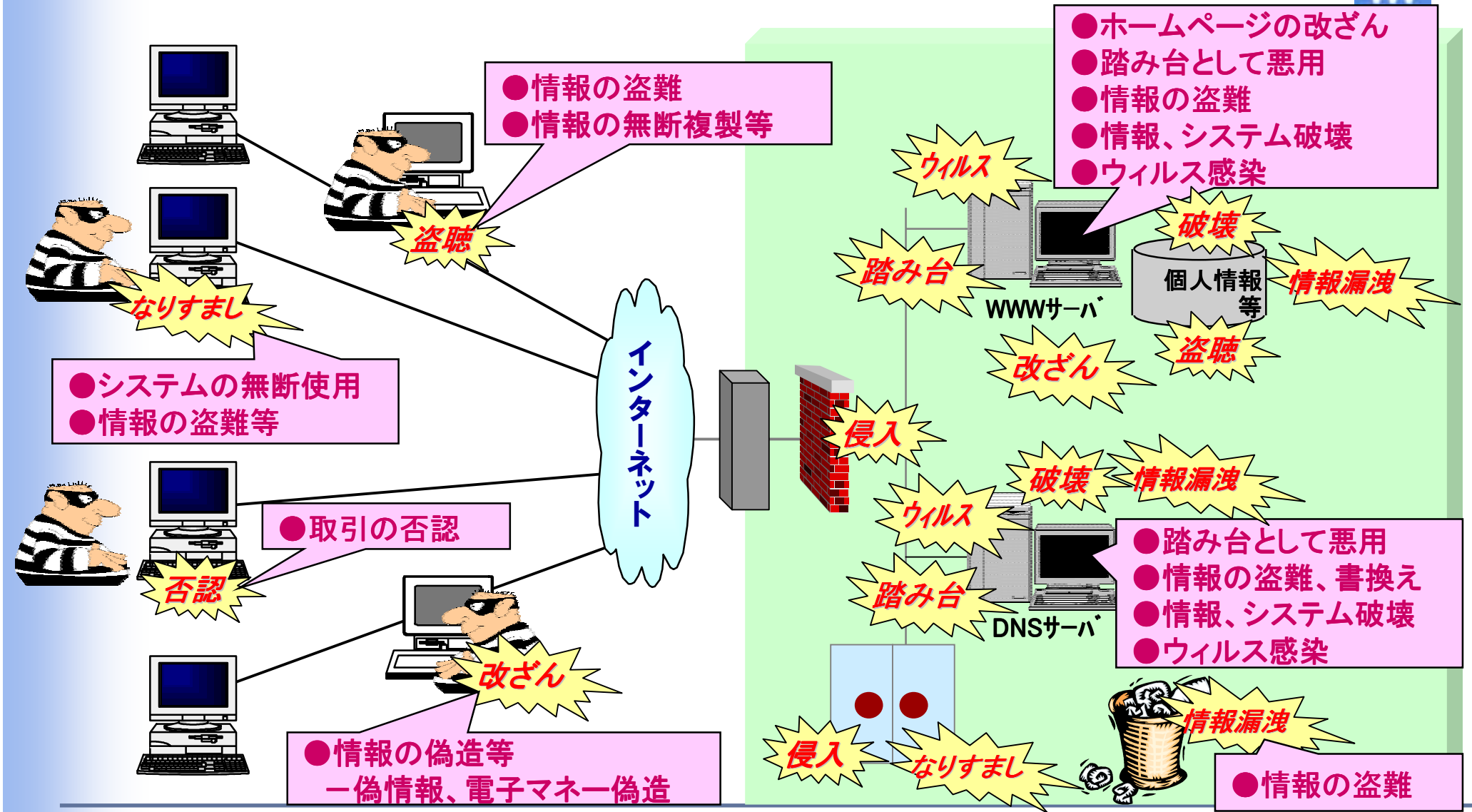
戦争



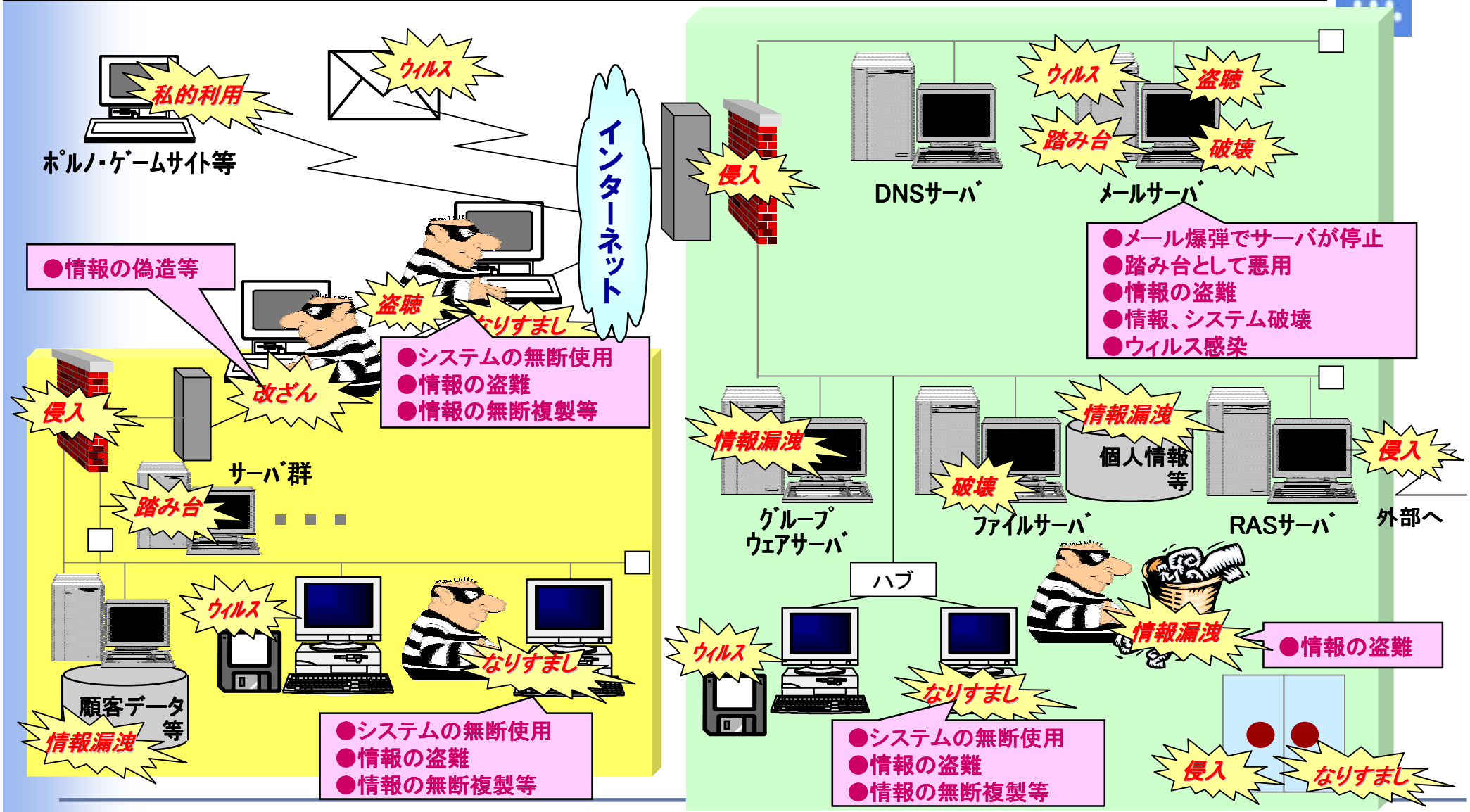
機器、システム故障

いたずら

ネット社会の抱える問題点 ～Weサイト編～



ネット社会の抱える問題点 ～イントラ・エクストラネット編～



Case Study 1 【事例】

社内から他企業に対して不正アクセスが試行され、攻撃先からクレームが・・・

緊急対応

・通報者に対して、原因調査を約束（当日）
・プロキシサーバログ等を解析し、攻撃者A社員を特定（当日）
・社長へ第一報（当日）

復旧対応

・社長を責任者とする対応プロジェクト発足（翌日）
・プロキシサーバログ等を解析し、クレーム先以外への攻撃がないことを確認（翌日）
・A社員からの事情聴取。セキュリティツールの操作ミスであることが判明（翌日）
・社長名による謝罪文の作成および送付（翌日）
・再発防止策、処分の検討（3日間）
　①セキュリティツール使用ネットワークの分離
　②セキュリティツール使用に関するポリシー追加およびマニュアルの作成
　③社長20%減給1ヶ月、A社員およびその上司訓告処分決定
・社長およびA社員による訪問および謝罪（4日後）→謝罪受け入れ
・社長名で、全社員に事件の概要説明をして再発防止を訴える

Case Study 1 【解説】

（1）対応は迅速かつ誠意を示すことが重要

- 通報を受けてから、調査、謝罪までを翌日に行った
- 再発防止策検討を3日間で行った
- 社長が対応の陣頭指揮を執るとともに、謝罪に同行して誠意を見せた
- 調査が長引きそうな場合は、その旨適宜状況報告をする必要あり

（2）クレーム対応窓口の設置が望ましい

- このケースでは、自社のWebサーバの管理アドレスへのメールに通報を受けていた
- たまたまサーバの管理者がメールを読み、かつ、セキュリティに詳しかったため、その後の対応が迅速にとれた
- 通報を受ける窓口体制を設置し、「たまたま」ではなく「確実に」対応が取れるようにすることが望ましい

（3）ログの対象、保存期間も要検討

- このケースのようなインシデントを想定し、社内から社外への不正アクセスが追跡できるようなログの取得を考慮すべき
- 通報が1ヵ月後というケースも珍しくないので、ログの保存期間も考慮する必要あり

【参考】 謝罪文例

2003年10月1日
いろは食品株式会社
鈴木様

ABC情報システム株式会社
代表取締役社長　田中　一郎

貴社Webサーバへの不正アクセスについて

拝啓　初秋の候、時下ますますご清祥の段、お慶び申し上げます。
　さて、2003年9月30日付けの貴信、拝読いたしました。弊社ネットワークより貴社管理のWebサーバへ複数回にわたり通常とは異なるアクセスを試みた形跡があるとのご連絡を受け、事実関係を調査したところ弊社内での不手際と判明いたしました。

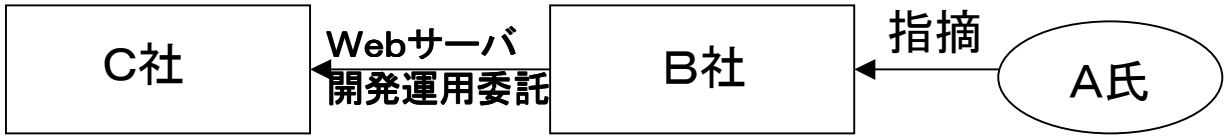
　アクセス先が貴社となった理由といたしましては、決して意図的なものではありません。いずれにせよ弊社の管理不行き届きであり、今回このようなご迷惑をおかけいたしまして心からお詫び申し上げます。
　今後はこのような不手際が再発せぬよう防止策の立案ならびに実施を徹底いたします。なお、経緯と再発防止策のご説明、お詫びにお伺いしたいと思いますので、別途お時間をいただければ幸いです。

　何卒ご理解ご寛容の程宜しくお願い申し上げます。

敬具

Case Study 2 【事例】

管理を委託されているWebサーバの脆弱性を第三者から指摘されたとの連絡が・・・



緊急対応

- C社はB社に対して、調査を約束（当日）
- 調査した結果、クロスサイトスクリプティングの問題があることが判明し、最低限の暫定対処のみ実施（当日）
- C社はB社に対して、プログラム改修の必要がある旨を通知（翌日）

復旧対応

- プログラムの改修費用をB社C社どちらが負担するかで調整難航。結局はB社C社による費用折半ということで決着（2週間後）
- プログラム改修要員の手配がつかず、プログラム改修完了まで4週間を要した（6週間後）
- その間、指摘したA氏へは一切連絡せず放置していたため、B社の誠意が見られないと判断したA氏は、セキュリティコミュニティにB社Webサイトの脆弱性を公表（4週間後）
- 半年後、B社はWebサーバの開発運用委託をC社からD社に切り替えた

Case Study 2 【解説】

（1）復旧にはスピード感と優先順位付けが大切

- 復旧費用の負担について2週間ももめてしまった
- 現場レベルで調整が難航する場合はトップ会談も必要
- 他の業務との優先順位も明確でなかった
- 指摘されるまでの間、情報漏えいなどがなかったの調査も必要であった

（2）通報者への対応は迅速かつ誠意を示すことが重要

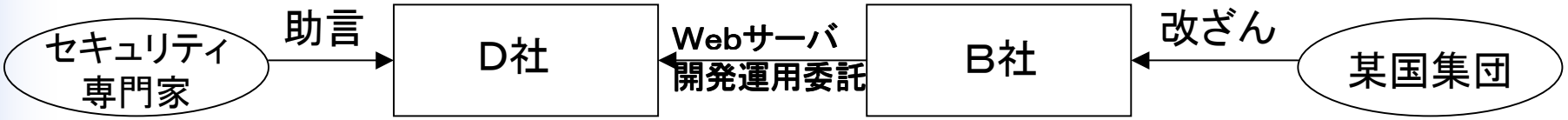
- 善意の報告者が大多数だが、中にはセキュリティコミュニティにおける名誉欲や過剰な使命感を持った第三者もいる
- 彼らはレスポンスが無いことを嫌うことが多い
- 指摘された時点で、指摘への御礼、調査の実施を返答した方がよい場合が多い

（3）あらたな脆弱性が発見された場合の対応費用について

- xSPサービスでは、このケースのようなインシデントを想定し、管理を委託されているシステムにあらたに脆弱性が発見された場合の対応の費用負担について、取引先とあらかじめ合意しておくことも重要

Case Study 3 【事例】

管理を委託されているチケット販売ホームページが改ざんされてしまった・・・



緊急対応

- D社はB社に対して、緊急対応を約束。セキュリティ専門家に支援を仰ぐ（当日）
- あらかじめ定められていた手順に従い、トップページに説明とお詫びを掲載。電話による代替サービスへ誘導（当日）
- D社幹部、B社幹部、セキュリティ専門家から成る対応プロジェクトを発足（当日）
- 暫定のセキュリティ対策を施し、チケット販売を再開（翌日）

復旧対応

- セキュリティ専門家の助言を受け、抜本対策案を立案（3日後）
- サーバ停止期間のB社の被害額を算出（3日後）
- 被害額と対策コストのバランスを考え改善復旧を1ヶ月と定め対策に着手（5日後）
  - ①OS、Webサーバソフトウェアの最新化（D社負担）
  - ②セキュリティ監視サービスの導入（B社負担）
  - ③D社の運用者のスキルアップ施策（教育）の実施（D社負担）
- セキュリティの強化について、ホームページに掲載（1ヵ月後）

Case Study 3 【解説】

（1）セキュリティ侵害発生時の迅速な対応

・ユーザへの告知、代替サービスへの誘導が早かった（あらかじめ手順が決まっていた）
・決定権を持つ幹部が対応プロジェクトに参画した
・ユーザへの説明は事実を隠さず誠意を持って

（2）復旧計画立案には根拠を示すことも重要

・早い段階からセキュリティ専門家の助言を仰いだ
・インシデント発生により被った被害額を算出したことが復旧、再発防止策への経営者の投資につながった

（3）セキュリティ監視サービスの導入

・Webサーバの運用管理者のセキュリティ教育を実施した点は評価できるが、より安心なサービスを提供するためには、セキュリティ専門会社のセキュリティ監視サービスの導入を検討することもお勧め

【参考】 謝罪文掲載例

お客様各位

重要なお知らせ

平素は弊社チケットサービスに格別のご高配を賜り、厚く御礼申し上げます。
7月6日7時20分頃、弊社ウェブサイトが、外部の侵入者によって一部コンテンツが書き換えらえるという被害を受けました。弊社では直ちに対策チームを発足し、11時55分、原因究明と復旧作業のため、弊社ウェブサイトを一旦停止いたします。

これにより現在、お客様におかれましては、本ホームページによる弊社のチケット販売システムをご利用できなくなっています。
誠にご迷惑をおかけいたしますが、システムの復旧まで今しばらくお待ちいただきますよう、お願い申し上げます。
なお、これに伴い、通常の電話予約窓口に加え、緊急電話予約窓口を設置いたしましたので、そちらをご利用いただきますよう、重ねてお願い申し上げます。

弊社では、今回の事態を重大に受け止め、直ちに再発防止の為の対策チームを発足させ、システムの見直し作業に着手しております。

緊急電話予約窓口： 03-xxxx-xxxx

本件に関するお問合せ先:
Bチケットサービス株式会社　広報部
TEL:03-xxxx-xxxx
Email:info@xxx.co.jp

Case Study 4 【事例】

社内でワームが蔓延してしまった・・・

緊急対応

- 感染が確認されたPC、サーバの即時隔離の指示（当日）
- CISOをヘッドとする緊急対応プロジェクトの発足（当日）
- 社外接続停止、全クライアント、サーバの分離と再接続ルールの決定（当日）
- ワーム感染確認手順書作成およびFAX等による配布（～翌日）
- 最新パッチ、パターンファイルの収録されたCD－ROMの作成、配布（～翌日）
- 対策確認されたPC、サーバの再接続（～翌日）

復旧対応

- 全クライアント、サーバの感染確認および対策実施の確認（２日間）
- ほぼ通常状態への復帰（３日後）
- 調査、分析の結果、感染ノートPCの持ち込みが原因であることが判明（３日後）
- また、全社のウィルス対策状況を報告させた結果、パターンファイルを最新化していないPCが多数あることも判明（３日後）
- 再発防止策の検討（３日間）
  - ①ノートPCのセキュリティ対策の強化
  - ②クライアントPC、サーバのパッチ管理策強化、パターンファイルの自動更新の義務化
  - ③定期監査、社員教育の実施

Case Study 4 【解説】

（1）セキュリティインシデント対応組織

・CISOによって、セキュリティ対策優先の方針が示され、ネットワークの停止が決断された

・ネットワーク停止を想定した、対策指示ルートを持つことが重要。このケースでは、FAXによる対策指示を行ったが、インシデント対応組織のFAXが1台しかなく、全組織に送信するのに1昼夜要した

（2）感染原因の徹底究明

・ワームやウィルスの感染源をつきとめることは困難な場合も多いが、再発防止のためには徹底した原因究明が必要

・感染源の追及だけでなく、蔓延してしまった理由を分析することも重要

（3）再発防止策は根気よく実施

・最後はどうしても、利用者のモラルに依存する部分が出てくる。教育を根気よく実施するとともに、監査の実施も有効な場合が多い

情報セキュリティ総合戦略からの視点

※本章の資料は経済産業省情報セキュリティ政策室山崎課長補佐のご好意により
使用させていただいております。

「情報セキュリティ総合戦略」が
2003年10月10日に発表されました

世界最高水準の「高信頼性社会」実現による
経済・文化国家日本の競争力強化と総合的な安全保障向上

http://www.meti.go.jp/policy/netsecurity/strategy.htm

「情報セキュリティ総合戦略」の策定

- 本年５月「産業構造審議会情報セキュリティ部会」を新設し検討。
- １０月１０日 「情報セキュリティ総合戦略」を答申。
- 関係省庁（内閣官房、内閣府、防衛庁、警察庁、総務省）もオブザーバ参加し、我が国で初めてとりまとめた情報セキュリティに関する総合的な戦略。「安全保障」の観点も盛り込み。

産業構造審議会情報経済分科会

情報セキュリティ部会

部会長：寺島実郎 （財）日本総合研究所理事長

（株）三井物産戦略研究所所長

骨格・視点の提示

専門的・実務的観点を付与した戦略案の提示

情報セキュリティ総合戦略策定研究会

委員長：土居範久 中央大学教授

【商務情報政策局長の諮問研究会】

●広い視点からの全体戦略

① 総合安全保障の観点からの情報セキュリティ問題
② 戦略的強化に向けた体制のあり方・官民の役割

＜経済・安保問題有識者、経営者、研究者＞
６月～１０月まで計３回開催

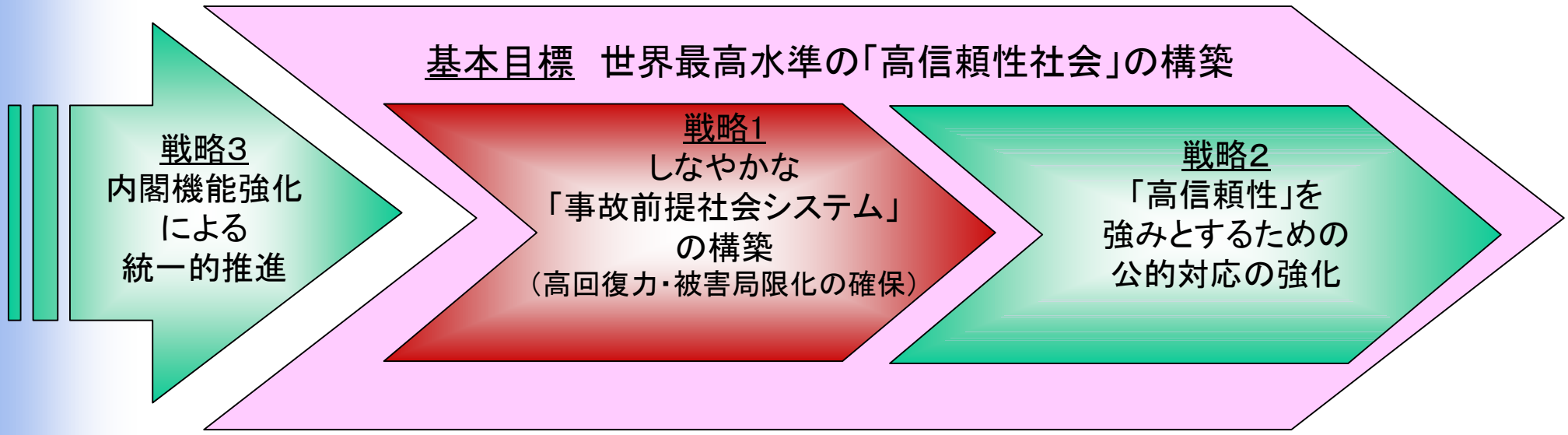
●現場に立脚した技術論・制度論

① 現場が直面している新次元のリスクとは？
② 対応策の現状の実態評価・国際比較
③ 今後の課題 ・ 新しい具体策の提案

＜最前線のセキュリティ技術者、研究者、弁護士、自治体関係者など＞
５月～１０月まで計７回開催

「3つの戦略」

- 「戦略」の基本目標を、経済・文化国家日本の強みを活かした「世界最高水準の『高信頼性社会』の構築」と位置付け。
- その要となる「情報セキュリティ対策」について、**3つの戦略と42の施策項目**を提言。



戦略1：しなやかな「事故前提社会システム」の構築
（高回復力・被害局限化の確保）

- 「情報セキュリティに絶対はなく、事故は起こりうるもの」との前提で、①被害の予防（回避）、②被害の最小化・局限化、③被害からの回復力が最適に組み合わされた対策を講じる社会システム、すなわち、「しなやかな『事故前提社会システム』」を構築。
- こうした観点を踏まえ、事前予防策及び事故対応策の両面に亘る施策を確立・強化。

現状

今回の主な結論

【予防】

現在の対策

- 政府・自治体、重要インフラの対策不足解消
- 脆弱性分析のための中核機関整備
- セキュリティ監査利用促進、格付け
- 一部で暗号・認証技術利用をルール化
- IT製品の安全ガイドライン策定
- 国民の情報セキュリティ意識向上
- 天気予報的セキュリティ警戒警報
- サイバー犯罪対策の法整備

【事故対応（被害を極小化する仕組みづくり）】

現在の対策

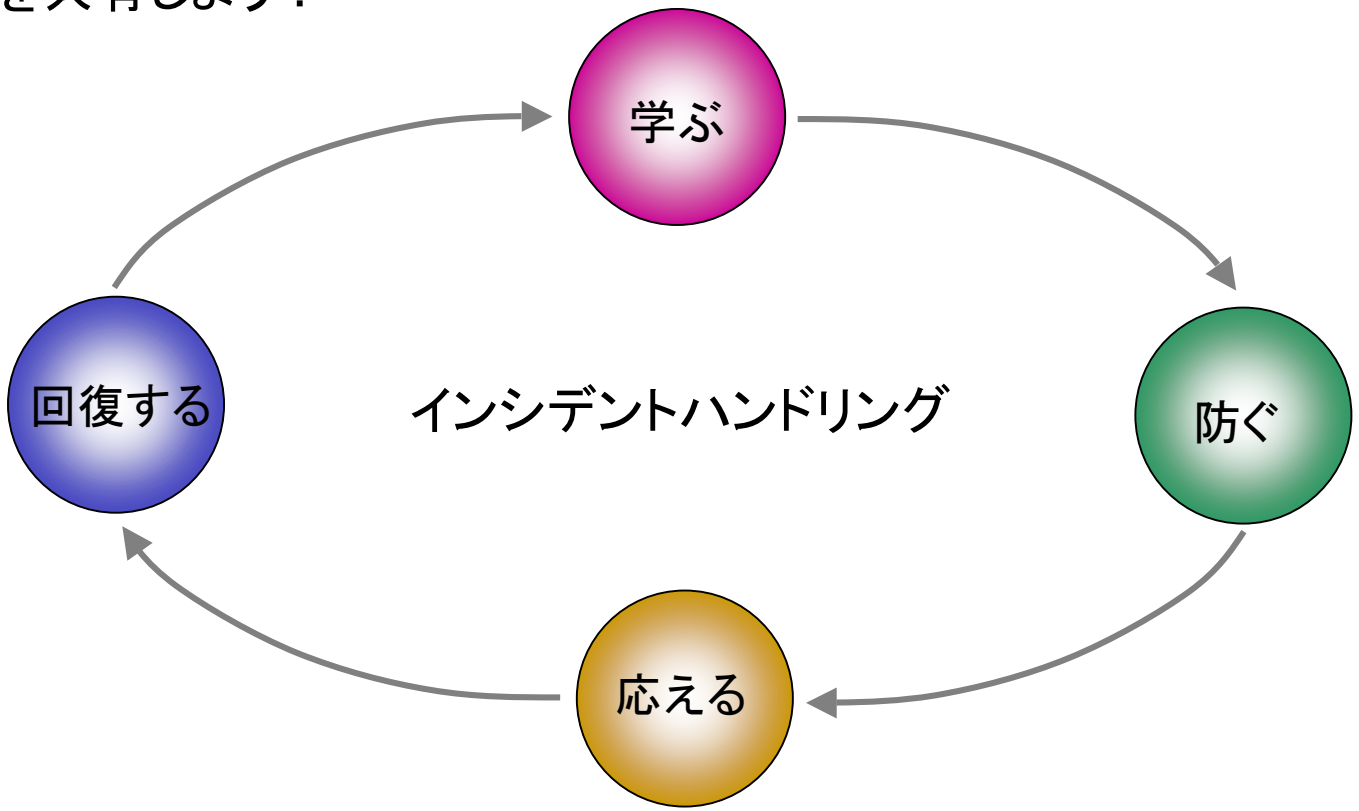
- 政府・重要インフラ共同での**サイバーテロ演習・訓練**の実施
- **重要インフラごとの事故情報共有体制整備**
- **国・自治体における事故情報共有体制整備**
- **サービス継続・復旧ガイドラインの整備**
  政府・自治体・重要インフラ
- **「重要インフラ・システム事故調査委員会」設置**
  ※「航空・鉄道事故調査委員会」のようなもの
- **IT業界における情報共有・協力体制**の立ち上げ
- 損保、技術、契約による**被害軽減モデル案の提示**

セキュリティ人材育成 ： 緊急対応機関での組織的研修、プロフェッショナル資格認定、実務家育成のためのスキル標準整備等

まとめ

まとめ

- 復旧は次の予防への第一歩！
- 事故からの学習こそ大切！
- 事例を共有しよう！



ご静聴ありがとうございました