「法とシステム監査」研究プロジェクト研究成果報告

サイバー社会における ITのガバナンスとマネジメント ～年金機構事案の教訓～

Governance and management of IT for the organization in cyber-society
- Warning from Japan Pension Service's problem –

成田　和弘

システム監査技術者,CIA,CISA

「法とシステム監査研究プロジェクト」の概要

- 主査　稲垣 隆一、副主査　黒澤 兵夫
- 概要

システム監査は、情報システムの企画、開発、運用、保守に関する現実的な課題の予防、解決に、いかに役立つのか？　レピュテーションリスク、クラウドコンピューティング、ソーシャルネットワーク、ビッグデータの取扱い、マイナンバー制度など現下の課題、**判決例に表れた紛争事例、現下のシステム上の課題を素材**に検討し、その成果を生み出す**システム監査の技法の開発、管理基準の改訂の提案など**に結びつける。

「法とシステム監査研究プロジェクト」メンバー

(原則50音順)

氏名	所属等	備考
荒木 哲郎	弁護士・システム監査技術者	
稲垣 隆一	稲垣隆一法律事務所・弁護士	主査
植野 俊雄	ISU	
黒澤 兵夫	TAKE国際技術士研究所	副主査
瀧澤 和子	早稲田大学	
多和田 肇	システム監査技術者,CIA,CISA	
芳仲 宏	東京地方裁判所	
久山 真宏	東京電機大学	
成田 和弘	システム監査技術者,CIA,CISA	発表

自己紹介

- **銀行員**（営業店は入社直後の1年4ヶ月）
- **システムの企画・開発から監査まで約30年の経験**
  - 勘定系システム、分散システムインフラ構築、セキュリティポリシー策定、システムアライアンス（関連IT会社設立など）、組合委員長、インターネットシステム、CRMシステム、IT投資管理、IT戦略の策定、各開発案件の立ち上げ・推進・プロジェクトマネジメント、合併・システム統合、大規模アウトソーシング契約の締結、BCP／DR体制構築等
  - 監査部でシステム監査を6年
  - 現在はシステム開発会社の品質管理部
- 保有資格・活動
  - CIA、CISA、情報処理技術者（ITストラテジスト、上級システアド、システムアナリスト、プロジェクトマネージャー、システム監査、情報セキュリティアドミニストレータ、データベース）
  - システム監査学会　「法とシステム監査」研究プロジェクト、「IT監査保証の判断基準」研究プロジェクト
  - ISACA　基準委員会委員、COBIT研究会、情報セキュリティ研究会、内部監査におけるシステム監査研究会

発表要旨

- **年金機構事案を境に日本のセキュリティの常識が変わったといわれている。**当該事案については詳細な調査報告書が執拗に侵入を試みるサイバー攻撃の実体を生々しく伝え、整備が遅れた情報システムなど、どこの組織にもありうる検討すべき課題を示唆している。この事案がIT環境の変化を示す重要な警鐘であるとの認識のもと、公開された報告書から、**年金機構にどのようなリスクと課題があったのか**、サイバー空間においてリスクを低減しつつビジネスを展開するため、ガバナンスとマネジメントに何が求められるのかを**システム監査の視点で考察する。**

Agenda

- はじめに
- 攻撃の概要
- 報告書から見えてくる課題
- 年金機構事案の教訓
- システム監査の検証ポイント
- システム管理基準見直しのポイント
- まとめ

はじめに
～年金機構事案とは

- 概要
  - 日本年金機構が**ＡＰＴ（Advanced Persistent Threat）**攻撃を受け、保有する多数の個人情報等が流出した事案。
  - **125万件の個人情報が流出**
  - **被害組織に多数の懲戒者**
    - ✓ 厚労相ら政務三役は1年分の閣僚給与と賞与全額を自主返納
    - ✓ 厚労省担当職員及び担当課長相当職の職員４名を戒告、その他組織管理上の責任を有する幹部職員等９名を訓告
    - ✓ 日本年金機構平成27年6月期役員賞与なし、理事長、副理事長、システム部門担当理事　戒告、月額報酬の2／10を2か月間辞退、　事業管理部門担当理事　　訓告
    - ✓ 日本年金機構システム統括部長、システム統括部　システム管理グループ長　経営企画部長、経営企画部　総務室長　戒告、その他　訓告5名、注意3名

出典：塩崎大臣会見概要　（厚労省）、不正アクセスによる情報流出事案にかかる役職員の制裁等について　（日本年金機構））

はじめに
～APT攻撃とは

- **A**dvanced **P**ersistent **T**hreats
  - Advanced　：**高度な**
  - Persistent　：**いつまでも続く、しつこい**
  - Threat：**脅威**
- ソフトウェアの脆弱性を悪用し、複数の既存攻撃を組合せ、ソーシャルエンジニアリングにより特定企業や個人をねらい、**対応が難しく執拗な**サイバー攻撃 (IPA)

出典：IPAテクニカルウォッチ　『新しいタイプの攻撃』に関するレポート　（ＩＰＡ）

はじめに ～3つの報告書

- 日本年金機構「不正アクセスによる情報流出事案に関する調査委員会」（8月20日）- 年金機構の報告書
  - 「不正アクセスによる情報流出事案に関する調査結果報告について」（67ページ）
    http://www.nenkin.go.jp/n/data/service/press0820.pdf
- サイバーセキュリティ戦略本部（8月20日）
  - 「日本年金機構における個人情報流出事案に関する原因究明調査結果」（28ページ）- NISCの報告書
    http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf
- 厚生労働省「日本年金機構における不正アクセスによる情報流出事案検証委員会」（8月21日）
  - 検証報告書（43ページ）- 第三者委員会報告書
    http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150821-02.pdf

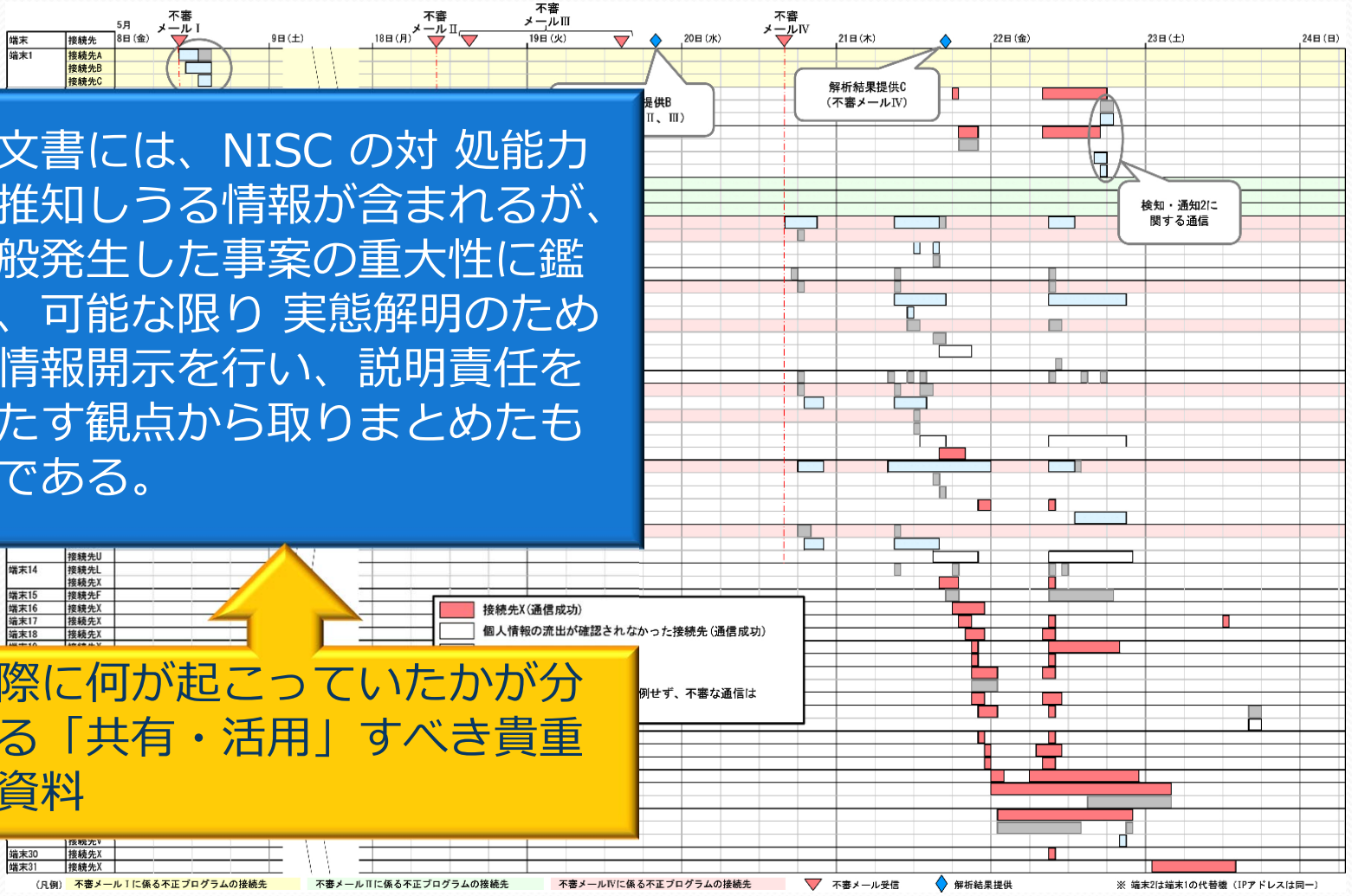
出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」、
サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」、
厚生労働省「日本年金機構における不正アクセスによる情報流出事案検証委員会」検証報告書

はじめに
～サイバーセキュリティ戦略本部の報告書

機構のプロキシログから解析した全感染端末の通信の記録

本文書には、NISC の対 処能力を推知しうる情報が含まれるが、今般発生した事案の重大性に鑑み、可能な限り 実態解明のための情報開示を行い、説明責任を果たす観点から取りまとめたものである。

実際に何が起こっていたかが分かる「共有・活用」すべき貴重な資料



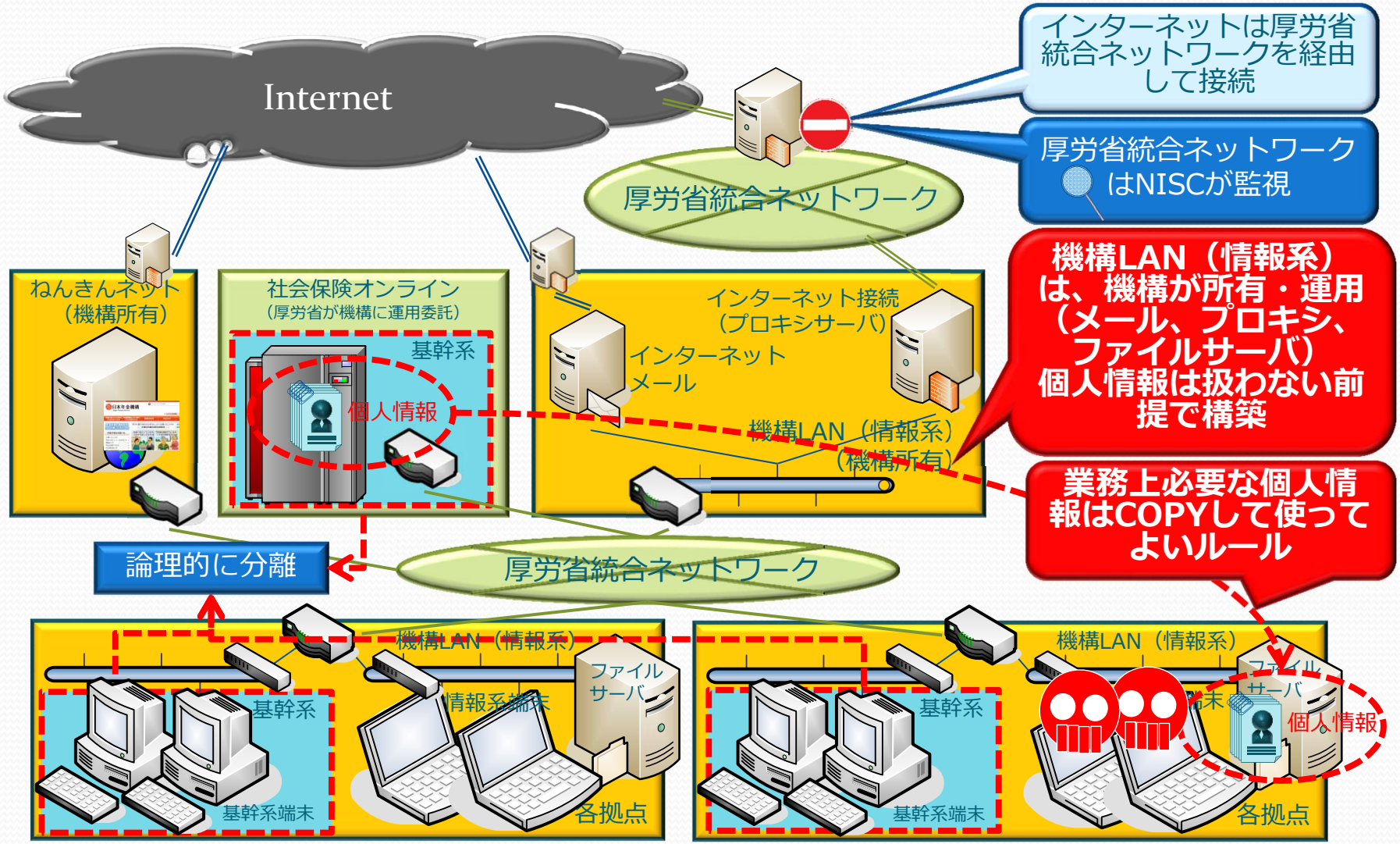
出典：サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」（図 2 感染端末と不審な通信）

攻撃の概要
～三波にわたる不審メール

不審メールの概要	
□	第一波　5月8日(金)
Ⅰ	「厚生年金基金制度の見直しについて(試案)に関する意見」 宛先：**公開メールアドレス(2通)** リンク：商用オンラインストレージ
□	第二波　5月18日(月)～5月19日(火)
Ⅱ	給付研究委員会オープンセミナーのご案内 宛先：**非公開の個人メールアドレス(98通)** ※年金機構の報告書は99通、第三者委員会報告書は101通 添付：給付研究委員会オープンセミナーのご案内.lzh
Ⅲ	厚生年金徴収関係研修資料 宛先：**非公開の個人メールアドレス(20通)** 添付：厚生年金徴収関係研修資料(150331厚生年金徴収支援G).lzh(16通)、リンク：商用オンラインストレージ(4通)
□	第三波　5月20日(水)
Ⅳ	【医療費通知】 宛先：**公開メールアドレス(3通)** ※第三者委員会報告書では5通 添付ファイル：医療費通知のお知らせ.lzh

出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」、
サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」、
厚生労働省「日本年金機構における不正アクセスによる情報流出事案検証委員会」検証報告書

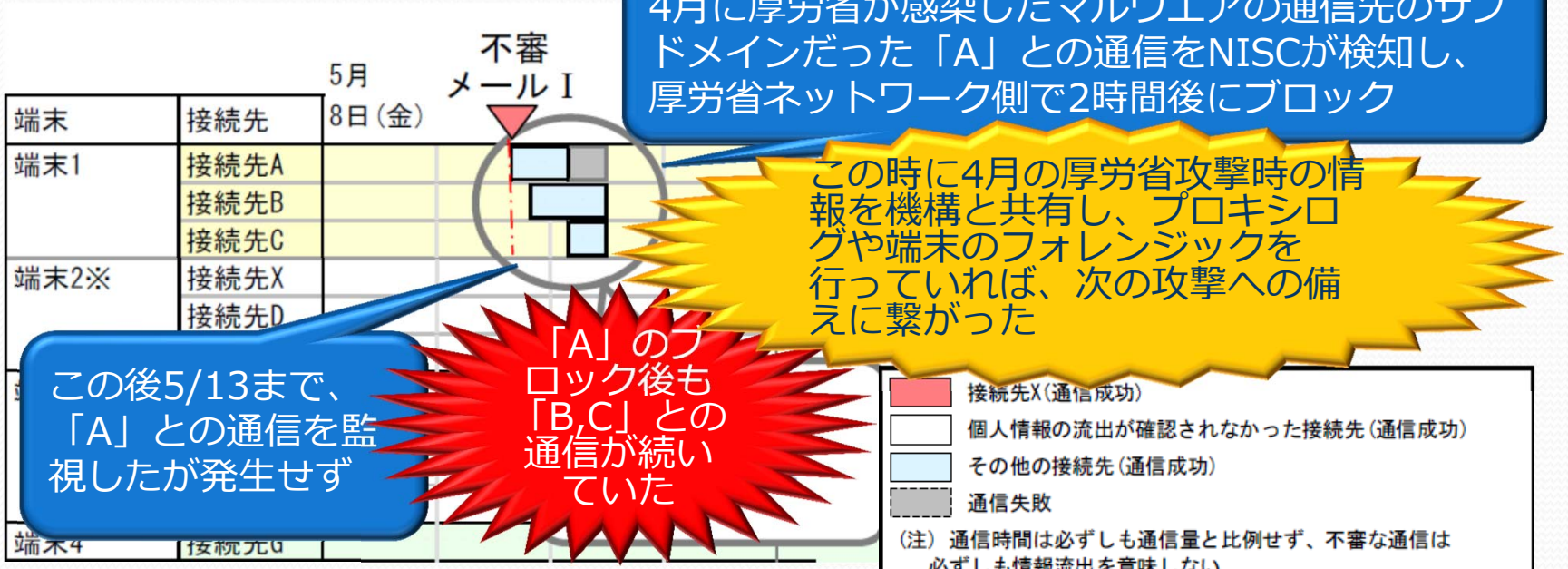
攻撃の概要
～年金機構のシステム



出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」、
サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」、
厚生労働省「日本年金機構における不正アクセスによる情報流出事案検証委員会」検証報告書

攻撃の概要～第一波

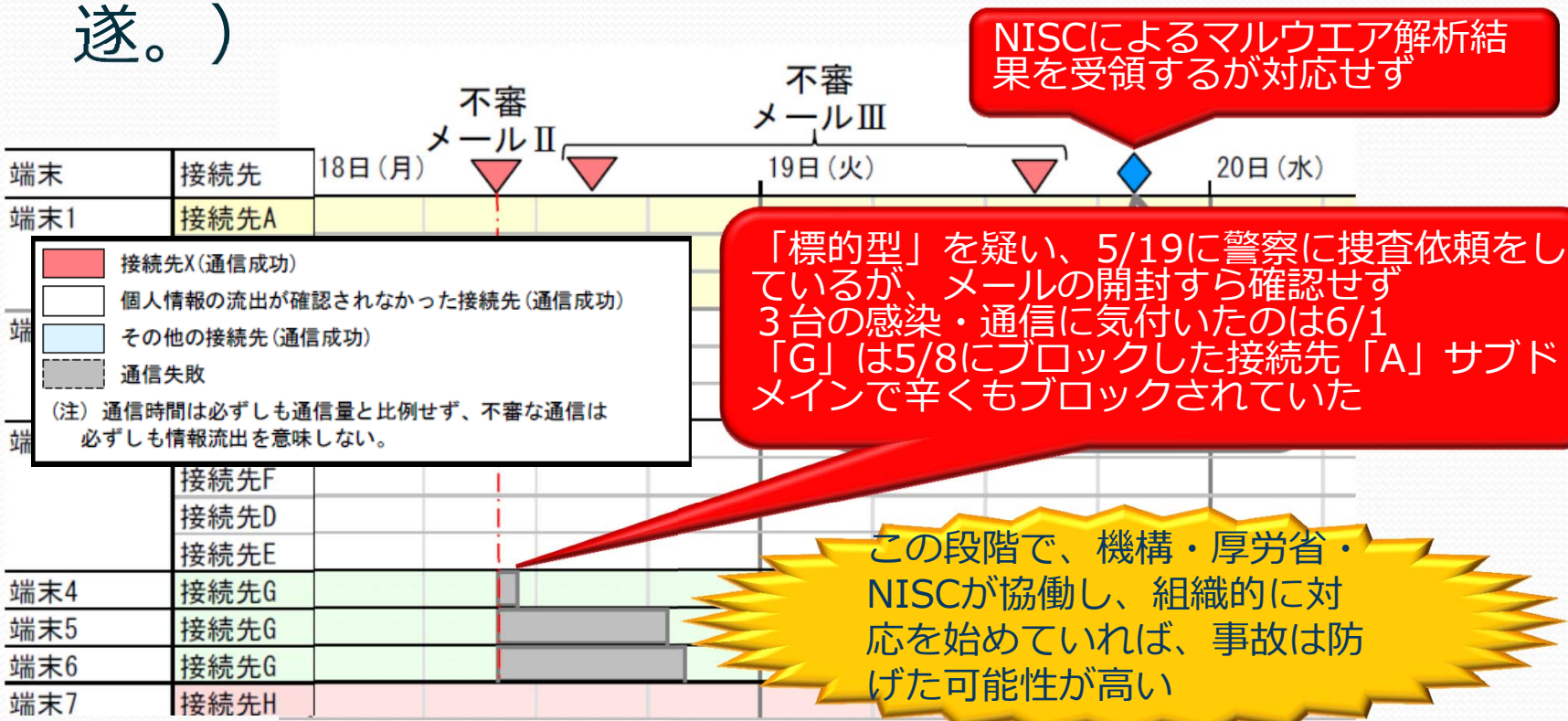
- 5月8 日午前、**2つの公開メールアドレス**に同一の送信元アドレスからメールを受信、**1名がこれを開封**し本文に記載されたリンクからマルウェアに感染。NISCが不審な通信を検知し、指摘により午後にLANケーブルを抜線。



出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」、
サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」、
厚生労働省「日本年金機構における不正アクセスによる情報流出事案検証委員会」検証報告書

攻撃の概要 ～第二波

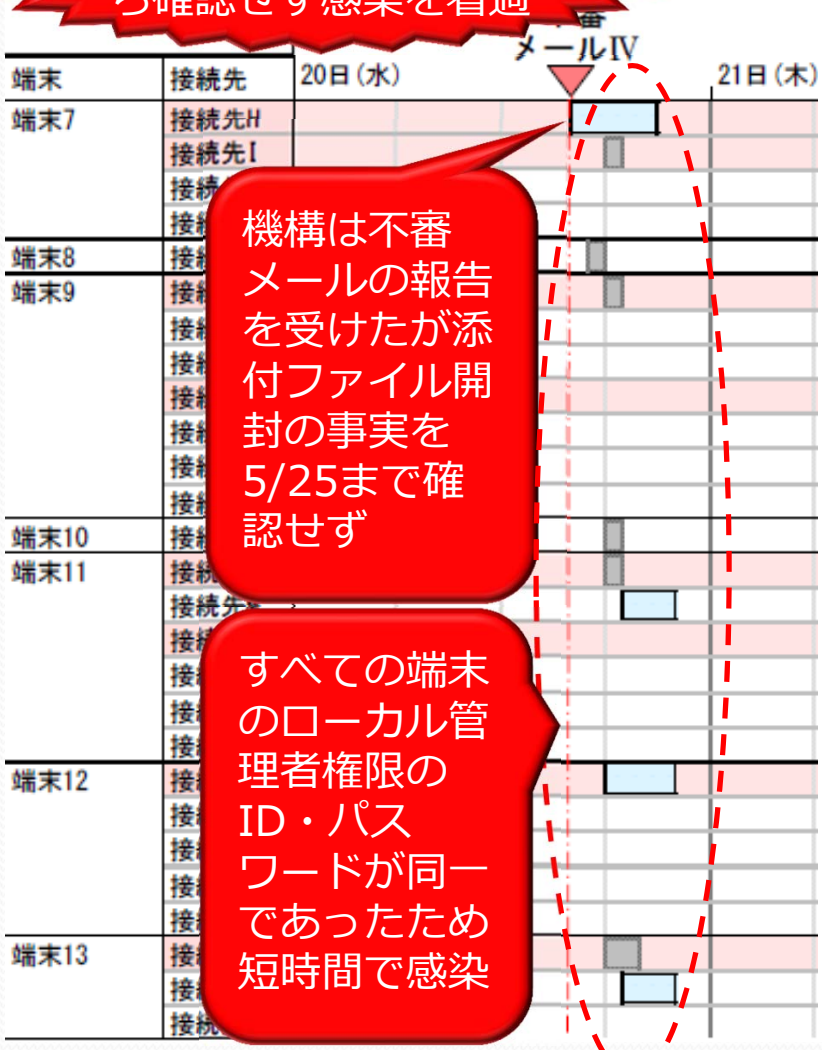
- 5月18日午前から19日午後にかけて、波状的に**121 名の個人メールアドレス**が標的型メールを受信。**3名が開封**しマルウェアに感染（通信は未遂。）



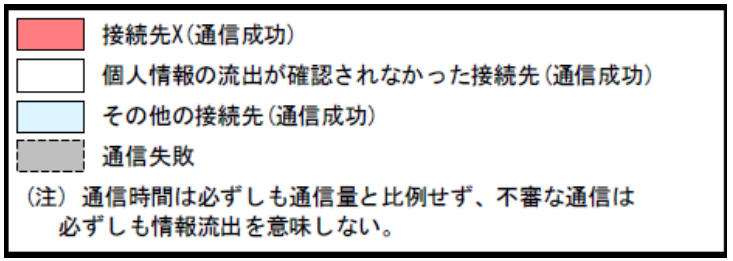
出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」、
サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」、
厚生労働省「日本年金機構における不正アクセスによる情報流出事案検証委員会」検証報告書

攻撃の概要
～第三波（感染当日）

不審メールを認識しているのにメール開封すら確認せず感染を看過



- 5月20日、**公開メールアドレス宛**てに新たな送信元アドレスから標的型メールを3通受信し、**1名が開封し感染。**指令サーバ（H）に接続後、遠隔操作で約30分後にローカル管理者権限を奪取。
- **2時間以内に**他6 台の端末を感染させ**うち4台を遠隔操作下**に。



不審メールIVに係る不正プログラムの接続先

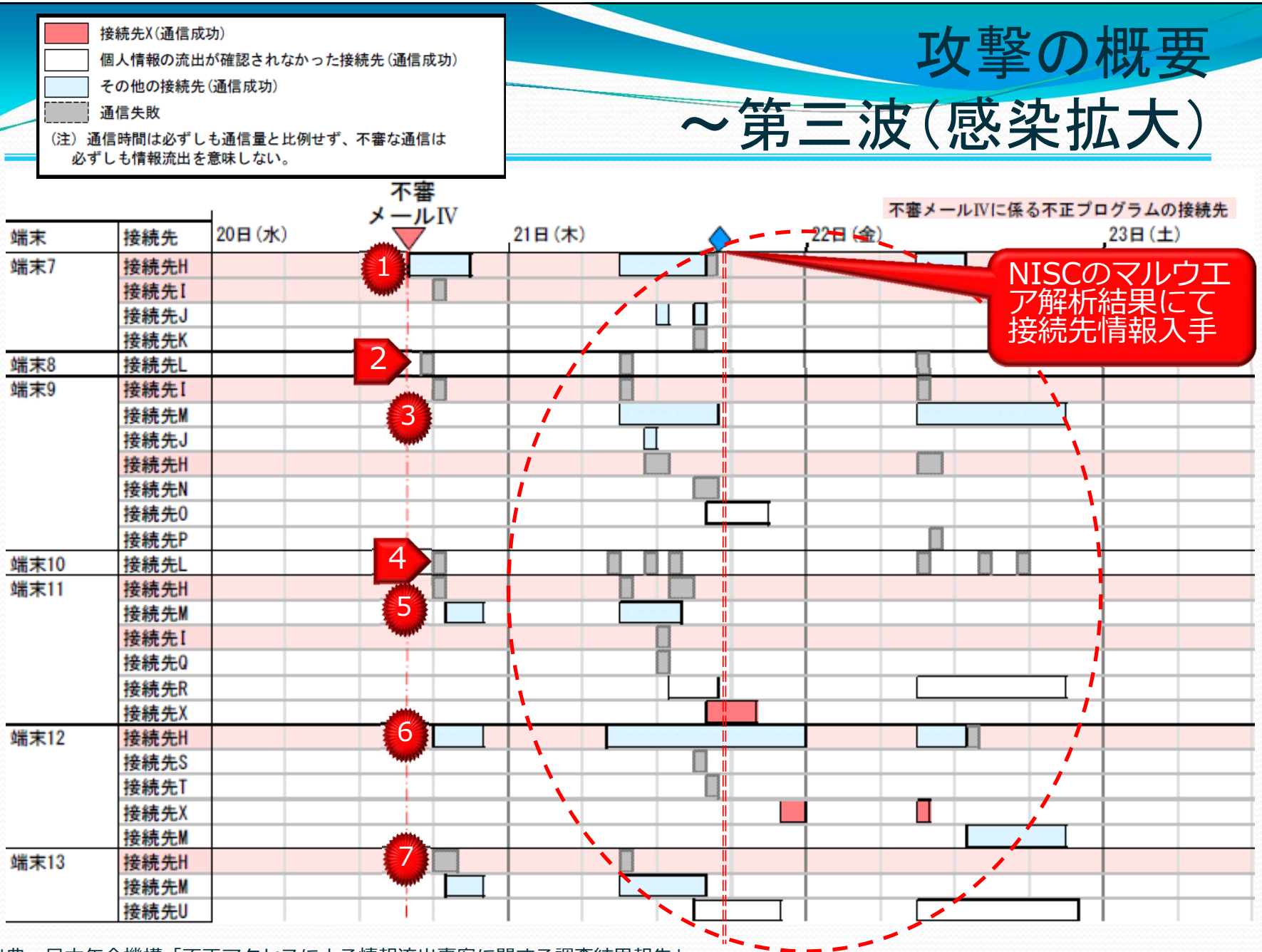
出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」、
サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」、
厚生労働省「日本年金機構における不正アクセスによる情報流出事案検証委員会」検証報告書

攻撃の概要
～年金機構を襲ったマルウエアEmdiviとは

- Emdivi（CloudyOmega/BLUE TERMITE）
  - OSコマンド・プログラム、**管理者ツールを利用した探索行為**、メールアカウントの収集
  - **ドライブ探索→ファイル探索→圧縮コピー→転送→痕跡削除**
  - 脆弱性（MS14-058,MS14-068）を悪用した**管理者権限の奪取**
  - スクリプト探索、パスワードリスト攻撃、**Builtin Administratorパスワード悪用**
    …etc
- 「**見えない悪意の権限者**」が組織内に入り込む
- **ルールや人の眼での管理策の効果は低い**

出典：JPCERT/CC「日本の組織をターゲットにした攻撃キャンペーンの詳細」（2015/11/19）

攻撃の概要
～第三波（感染拡大）



出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」、
サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」、
厚生労働省「日本年金機構における不正アクセスによる情報流出事案検証委員会」検証報告書

攻撃の概要
～第三波（情報漏えい）

接続先X（通信成功）
個人情報の流出が確認されなかった接続先（通信成功）
その他の接続先（通信成功）
通信失敗
（注）通信時間は必ずしも通信量と比例せず、不審な通信は必ずしも情報流出を意味しない。

多数の端末がC&Cサーバと通信するのを放置

NISCのマルウエア解析結果にて接続先情報入手

NISCから異常通信が通知され抜線したが、他の端末の通信に気づきA拠点ネットワークを切り離し

- 5/22遠隔操作23台、「X」と20台通信できたが実際は6台のみ使用

ようやくプロキシログをもとに感染端末を特定して抜線、B拠点のネットワーク切り離しで収束

出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」、
サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」、
厚生労働省「日本年金機構における不正アクセスによる情報流出事案検証委員会」検証報告書

報告書から見えてくる課題 ～致命的だった初動の遅れ

- 初報はトップまで速やかにあがった
  - **5/8 理事長及び副理事長には対応状況の概要について、当日中にそれぞれ報告**（出典：「不正アクセスによる情報流出事案に関する調査結果報告について」（日本年金機構））
  - 機構の担当者には**標的型攻撃の可能性を認識**し、情報発信を行った者もいた
  - 新種ウィルスは**「特定のサイトにファイルを取得しにいくものである」**（出典：「日本年金機構における不正アクセスによる情報流出事案検証委員会　検証報告書」（厚生労働省））
- ここから確り初動対応が始まるべきだったが、**十分な体制整備もモニタリングも行われなかった**
  - **リスク判断の不適切さ**が大きな被害に繋がった

報告書から見えてくる課題
～個人情報保護のコンプライアンスはどこへ

- 事故を起こした機構LANシステム
  - 個人情報など**情報漏洩対策を必要とする情報は保管しないことが原則**
  - しかし、**業務上必要なデータ**については、パスワードやアクセス制限の設定など情報セキュリティ対策を講ずることを前提として**取り扱うことが可能・・・？？？**
    - 「行政機関の保有する個人情報の適切な管理のための措置に関する指針」を忠実に守っていれば…
- **個人情報保護管理者**が行うべきシステム整備を**エンドユーザの責任に転嫁**
  - そもそもパスワードつきでも漏れれば漏えい

出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」

報告書から見えてくる課題
～メールは開けてはいけないのか？

- 本件での攻撃メール開封率はわずか**４％**

内訳	受信件数	開封件数	開封率
業務用（公開）メールアドレス	5通	2通	40.0%
職員個人の業務用メールアドレス	119通	3通	2.5%
合計	124通	5通	**4.0%**

出典：日本年金機構「不正アクセスによる情報流出事案に関する調査結果報告」

- 「メール攻撃訓練」での開封率一般19%、役員31%に比べむしろ優秀（出典：「サイバーセキュリティ傾向分析レポート2015」（ NRIセキュアテクノロジーズ））

✓ しかし**不審メール開封の報告や確認は1度もなかった**

✓ 公開メールは多少怪しくても開けざるをえず、**1通でも開封すれば攻撃は成功している**

➢ 開けないことではなく、**不審メール発見後の初動対応こそが重要**

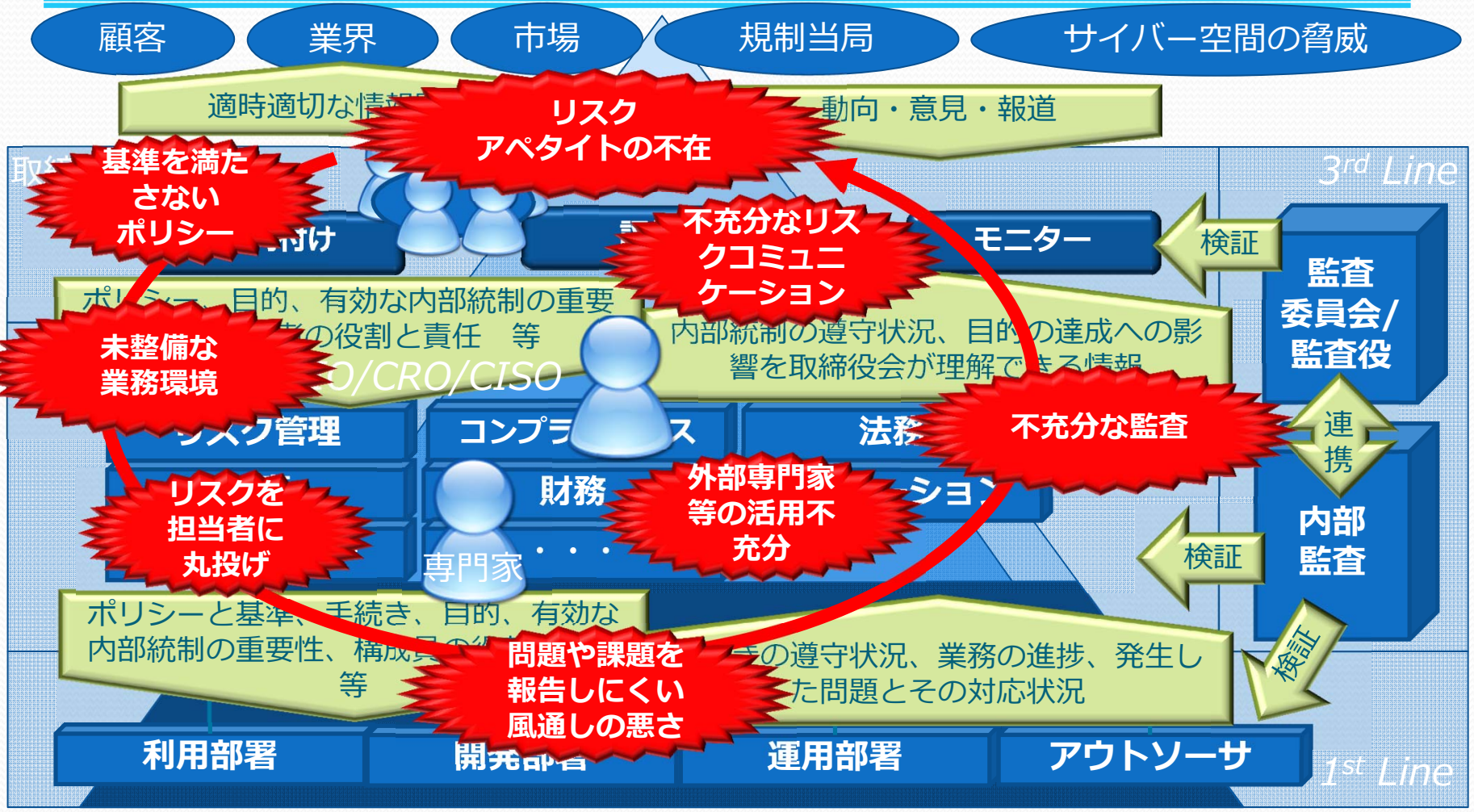
報告書から見えてくる課題
～サイバー攻撃は何がこれまでと違うのか？

- **外部からの組織的な攻撃**
  - ツールにより**内部ネットワーク**から攻撃
  - 権限昇格の脆弱性を利用し**管理権限を奪取**
    - **悪意のある権限者の内部不正と同じ**
  - 内部に侵入したマルウエアは**外部から操作**
    - 犯人は見えず、**牽制効果は働かない**
- 新たな**内部統制上の課題**として組織の**リスクに応じた方針**を定め、**組織全体で対応**していくことが必要
  - **性善説**でつくってきた**業務プロセスも情報システムも見直し**が必要

報告書から見えてくる課題 ～実は年金機構だけではない

- JPCERT/CC
  - 2015年4月～9月でEmdivi関連**93組織**の対応（出典：JPCERT/CC「日本の組織をターゲットにした攻撃キャンペーンの詳細」（2015/11/19）
    - 攻撃者は網羅的に**脆弱な組織とシステム**を探索しており、**必ず攻撃される**と思ったほうが良い
    - サーバーを**C&Cにされ加害者に**なるケースも
- 以下は6月に公表された類似事案のごく一部
  - 「石油連盟パソコンのマルウェア感染による情報流出について」（石油連盟　6/15）http://www.paj.gr.jp/paj_info/press/2015/06/15-001590.html
  - 「当所パソコンのウィルス感染による情報漏えいについて」（東京商工会議所　6/10）http://www.tokyo-cci.or.jp/page.jsp?id=59029
  - 「国際協力機構(JICA)におけるPC及びサーバのウイルス感染について」（国際協力機構 6/17）http://www.jica.go.jp/information/info/2015/20150616_01.html
- **サイバー空間の発展に伴い**リスクの発生確率と影響が大きく変化した**

報告書から見えてくる課題
～「ガバナンス体制＝組織力」の点検の必要性



（参考：COSO. 内部統制の統合的フレームワーク.：日本公認会計士出版局, 2013年　/　ISO/IEC 38500:2015 Governance of IT for the organization.）

報告書から見えてくる課題
～3つの報告書からわかること

- 証拠に基づく点検と第三者検証が重要
  - **証拠に基づく報告**は客観性が高い
  - **当事者の調査報告**の限界は比べると明白
  - **第三者の検証**が管理形骸化の防止に有効
- サイバーリスクの情報共有の重要性
  - 攻撃は高度で執拗だが、**他の組織と同じ攻撃パターン**が繰り返される
  - **サイバーセキュリティ向上を積極的に企図**した報告書の活用

➢ **開示された情報を生かし、自分の組織に同じことが起こらないようにすることが重要**

年金機構事案の教訓 ～足元の管理策の見直し

- 本事案をうけた「独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針」の改定
  - 保護管理者は当該情報システム管理者と連携
  - 権限の内容を業務上必要最小限の範囲に限る
  - **感染端末抜線等の被害拡大防止は直ちに行う**
  - 事案発生のおそれを認識した場合には、時間を要する**事実確認を行う前にまず保護管理者に報告**
    - 具体的で明確な報告ルート等、**報告しやすい環境づくり**が重要
- ➢ 同様の対応の要否等、**基本の見直しが必要**

出典：総務省「独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について」

年金機構事案の教訓
～セキュリティバイデザインの徹底

- 外側の管理策の積み重ねではなく、**セキュリティを組み込んだシステムの設計（セキュリティバイデザイン）**が重要
  - 攻撃された端末から**侵入範囲を拡大させない**ための対策や、ネットワークを管理するような**重要な機器を攻撃させない**ためのシステム設計・構築・運用
  - 組織の業務、取り扱う情報、保有するシステムに応じて、目的に照らし、**業務が円滑に実施できる対策**
- 組織内部から**悪意を持って権限を行使した攻撃が行われることが前提のシステム**を設計・構築・運用すること、必要に応じ**重要な情報はインターネットから遮断**

出典：サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」

年金機構事案の教訓
～基本的な情報セキュリティの徹底と監視強化

- まずは**基本に忠実な対策**が重要
  - 端末のセキュリティ強化
    - **マルウエア起動を抑止/検知するホワイトリスティング**
    - **既知の重要な脆弱性は速やかに修正し、テストする**
    - ゼロデイ攻撃の可能性を踏まえ、使用ソフトを見直し
    - 埋め込みコンテンツを自動的に取り込まないよう設定
  - 検知・拡大防止機能の設計・構築・運用
    - セグメントの分割・システムの分離の徹底
    - **ローカル管理者権限の最小化**
    - 不要な管理アカウントの消去、管理端末の設置場所の分離
- さらに**内部ネットワークの異常検知**の仕組み
  - ファイルサーバのアクセスログやプロキシログ等のログの異常検知、内部ネットワークの不正通信検知システムの導入

出典：サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」

年金機構事案の教訓 ～インシデント対応に係る対策

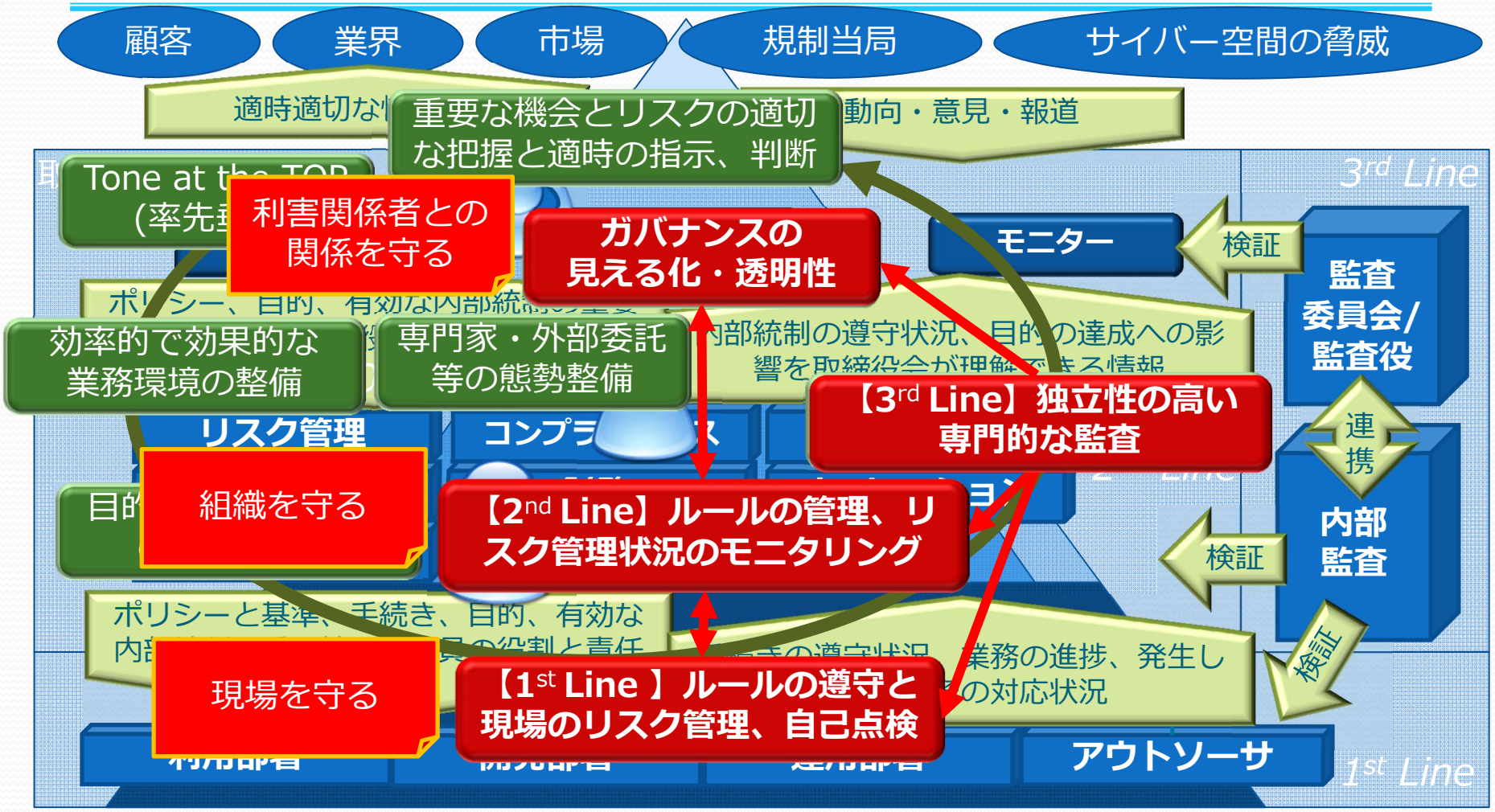
- 不審メール対応が躊躇なく行える環境整備
  - **不審メールの受信は、標的型攻撃の端緒**の可能性があり、繰り返しの攻撃を想定し対応する ～不審メールを必ず報告し、**調査対応を行う体制整備と訓練**
  - **専門性の高い第三者**の事業者（システムの構築・運用事業者とは独立した第三者の事業者）に依頼できるよう**平素から調達の準備**をする
  - インシデント対応は組織のリソースを迅速に投入し、システムや業務を止める判断・指示ができる権限者の下で行う**…権限者の訓練こそ重要**
- 事前にインシデント発生時の対応を**「緊急時対応計画」として定め、**専門性の高い第三者、**発動権限者を入れた訓練を行う**

出典：サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」

年金機構事案の教訓
～内部統制のフレームワークによる組織の強化

（参考：COSO. 内部統制の統合的フレームワーク.：日本公認会計士出版局, 2013年　/　ISO/IEC 38500:2015 Governance of IT for the organization.）

年金機構事案の教訓 ～システム監査の検証ポイント



（参考：COSO. 内部統制の統合的フレームワーク.：日本公認会計士出版局, 2013年　/　ISO/IEC 38500:2015 Governance of IT for the organization.）

システム管理基準見直しのポイント

- **コーポレートガバナンスに対応した拡張**
  - ✓**サイバー社会に適応**したリスクアペタイト
  - 方針の策定、リスクアペタイト、モニタリングと評価などのガバナンスプロセスの明確化
  - 危機管理、インシデント対応体制の明確化（広報、顧客・取引先への通知等含む）
  - リスク管理プロセスの強化等
- **新たなIT環境への対応**
  - ✓**セキュリティ・バイ・デザイン**の対応
  - セキュリティ要件定義の明確化～設計・構築・テスト・運用
  - 検知・防御機能などのセキュリティ基盤整備
  - セルフアセスメントや第三者評価の活用

まとめ

- **３つの報告書を徹底的に生かそう**
  - 技術的な課題、第三者の目線と現場の状況
- 年金機構と同じことはすぐに起こりうる
  - **環境変化を認識し、適切な対応を**
    - 自分の組織が同じ事象に対応できるか確認
    - 足もとはセキュリティの基本の徹底
      - メールとインターネットの重要情報からの分離
      - ホワイトリスティング、脆弱性管理の徹底等
    - 根本はセキュリティバイデザインの徹底
    - 早期発見と速やかな初動体制の事前の整備
      - 発生してからでは間に合わない
- **大きな環境変化への対応こそガバナンスの役割**
  - ガバナンスとは内部統制を適切に機能させること
  - 専門性の高いシステム監査は内部統制上も重要

Thank you

この資料の内容には発表者個人の見解が含まれます。
また、発表者の所属会社とは関係ありません。