資料8

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

2019年度　重要インフラにおける補完調査について

2020年７月13日

内閣官房　内閣サイバーセキュリティセンター(NISC)

補完調査とは

調査の目的

補完調査とは、行動計画※の取組の評価に当たって、個別施策の結果・成果だけでは把握しきれない状況についても適切に把握することが重要であることから、個別施策の指標では捉えられない側面を補完的に調査することを目的として毎年度実施する調査です。

※重要インフラの情報セキュリティ対策に係る第４次行動計画
（平成29年４月18日サイバーセキュリティ戦略本部決定、令和２年１月30日サイバーセキュリティ戦略本部改定）

調査の運営

重要インフラサービス障害等の事例について、重要インフラ事業者等の協力を得て、現地調査（ヒアリング等）を実施します。重要インフラ事業者等における今後の取組にも資するよう、原因、対応、得られた気付き・教訓等をとりまとめ、可能な範囲で調査結果を公表します。

調査対象事例の選定基準

本報告書の調査対象事例は、2019年1月1日～2019年12月31日の間に、重要インフラ事業者等から内閣サイバーセキュリティセンターに提出された情報連絡の事例の中から、主に以下の選定基準により選定しました。

- 重要インフラサービス及びその周辺サービスへの実害の有無
- 事案の重大さ・社会的影響（関心）の大きさ
- 類似事例の発生状況や今後発生する可能性
- 攻撃手口や被害の目新しさ
- 世の中のトレンド
- 他分野への波及の可能性
- 得られる気付き・教訓の有用性等

※その他、事案の対応の優劣、地域性や分野のバランスも考慮

2019年度　調査対象事例　概要

- **“重要インフラ事業者が利用するサーバやメール環境への不正アクセス”**が複数分野の重要インフラ事業者等で発生したことから、各事業者における対応事例を調査。
- **”外部からのサイバー攻撃”**や**”重要インフラ事業者内でのインシデント”**等、例年発生頻度の高い脅威は2019年も一定数発生しているが、対応を実際に経験したことで重要インフラ事業者が新たに気づいた課題や教訓等について調査。

No.	事例	影響	原因
システム故障に起因した重要インフラサービス障害			
1	改元に伴うシステム変更トラブルへの対応	利用者が、改元後に処理されるサービスの予約手続きを改元前に行ったところ、サービスの提供日が誤って表示されるトラブルが発生。	日付形式の切り替え日に関する認識が、店舗端末接続ネットワーク側との間で異なっていたため。
2	重要インフラサービスの一部業務の停止	重要インフラサービスで利用するデータベースのシステムファイルが破損したことにより、顧客がサービスを利用できなくなった。	不具合を改修する修正パッチを未適用であったため。
3	委託先のシステムトラブルに伴うサービス障害	複数の重要インフラ事業者が共同利用する業務システムにおいて障害が発生し、利用する複数の事業者において同時にサービス障害が発生。	大量データの処理が一時的に集中し、ホストコンピュータ上の通信制御ソフトウェアのリソースが枯渇したため。
4	重要インフラサービスの業務遅延	重要インフラサービスに遅延が生じたことから、業務スケジュール管理システム経由で業務スケジュールの組み換え処理を試みたが、システムが正常に動作せず、重要インフラサービスの業務遅延が拡大。	システムの処理タイミングの一部ずれが生じ、排他制御が適切に実施されなくなったため。
外部からのサイバー攻撃			
5	不審メールによるマルウェア「Emotet」への感染	重要インフラ事業者の職員が不審メールの添付ファイルを開封し、マクロを有効化したことで、端末がマルウェア「Emotet」に感染。感染後、感染端末を使用していた職員を騙るメールが、外部組織に送信。	重要インフラ事業者の職員が、外部から送信された不審メールの添付ファイルを開封してしまったため。
6	重要インフラ事業者が利用するサーバへの不正アクセス	重要インフラ事業者が利用するサーバが不正アクセスされ、同サーバから外部に不審なメールが送信。	コンテンツ管理システム(CMS)のプラグインの脆弱性を悪用され、サーバが不正アクセスされた可能性が高い。
7	クラウド型メールサービスに対する不正ログイン	重要インフラ事業者が利用するクラウド型メールサービスに対し、攻撃者が不正アクセスを実行し、重要インフラ事業者のメールアカウント経由で、当該事業者とは無関係なメールが大量に外部へ送信。	クラウド型メールサービスのログイン画面について、アクセス制御が十分でなかったため。

得られた気付き・教訓　概要（各事案に共通する事項）

システム故障に起因した重要インフラサービス障害事例（No. 1, 2, 3, 4）から

- システム故障への対応方針を迅速に決定できるようにするために、重要インフラサービスにおける判断権者を事前に明確にしたうえで、**実効的な権限委譲について検討**することが重要。
- 重要インフラサービスの機能保証の考え方を踏まえ、**サービスの優先度に応じた段階的な復旧対応方針の策定**や**代替手段を用いた事業継続計画の整備**を事前に検討することが重要。
- システム故障発生時に、重要インフラサービスの関係者等に迅速に連絡できるよう、組織内だけでなく、**外部委託先や**当該サービスに関わる**システムを共同利用する他の事業者等を含めた緊急連絡体制の整備、連絡手段の確保**、訓練の実施が重要。

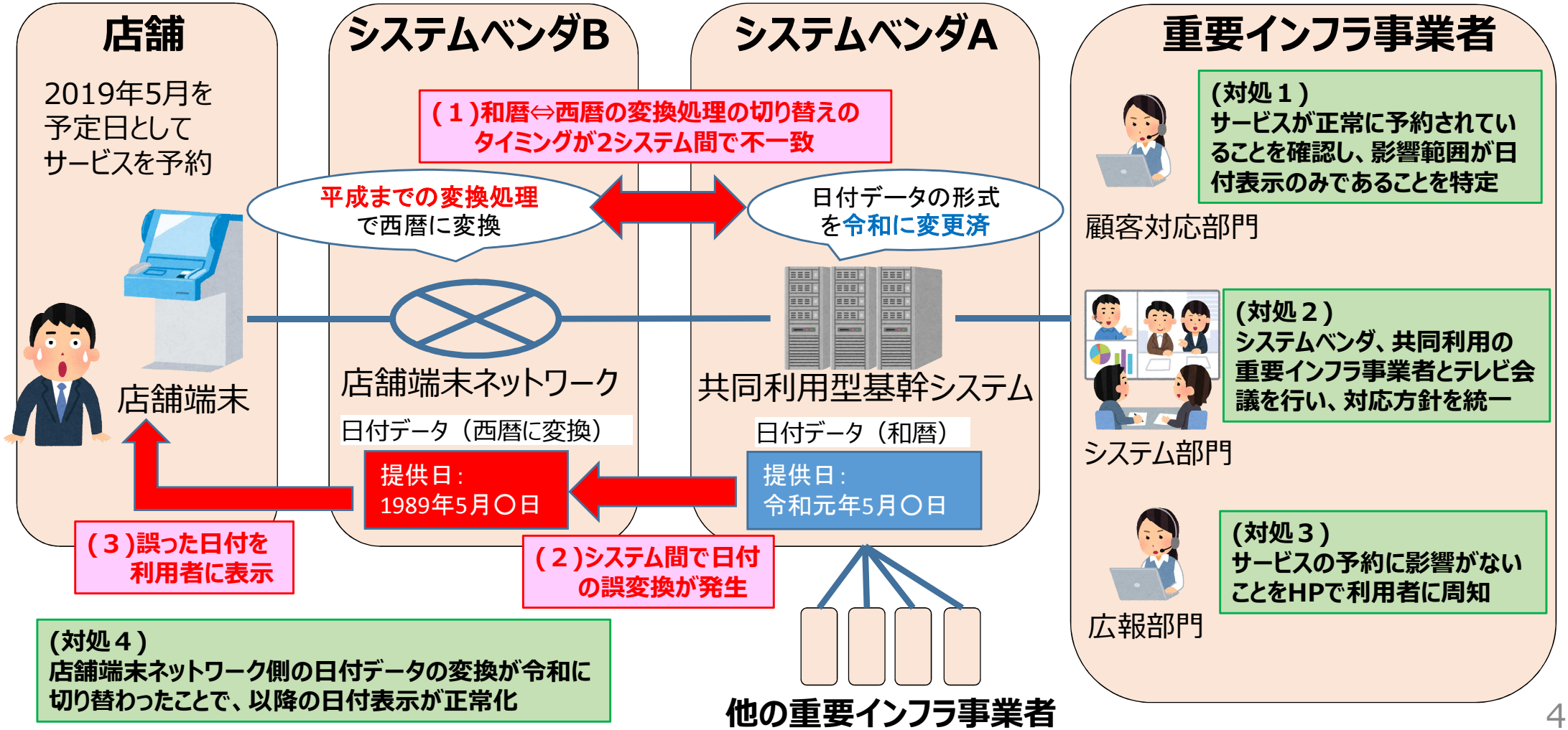
外部からのサイバー攻撃への対応事例（No. 5, 6, 7）から

- 他の重要インフラ事業者における類似のサイバー攻撃の被害を防止するため、事業者は**迅速にサービスに対する影響を公表**し、その後も適時、**続報の公表を検討**することが重要。
- クラウドサービス利用時は、クラウドサービスの仕様やサービスの提供条件を十分確認したうえで、サービスに**適切な設定を行い、仕様を考慮した運用**を実施することが重要。
- 有識者に**技術的見解を確認できる体制の構築やベンダとの委託契約の締結**等を通じて、セキュリティインシデント発生時の技術的対応を迅速に実施できるようにすることが重要。

※　個々の事例ごとの他の気付き・教訓については、各事例の項を参照。

事例1　改元に伴うシステム変更トラブルへの対応　1／2

- 利用者が、2019年5月（改元後）に処理されるサービス（重要インフラサービスに該当）の予約手続きを同年4月（改元前）に行ったところ、サービスの提供日が「1989年5月○日」と表示されるトラブルが発生
- 重要インフラ事業者は、当該トラブルが予約に影響しないことを特定し、サービスを継続する対応を意思決定
- システムベンダや他の重要インフラ事業者と連携し、利用者への対応を統一して迅速にHP等で周知し、問い合わせ対応を行ったことで、分野全体で大きな混乱なく事態を収拾



事例1　改元に伴うシステム変更トラブルへの対応　2／2

【1　背景】

- 共同利用型の基幹システムは、店舗端末接続ネットワークを通じて、重要インフラサービスを店舗に提供する。
- 改元対応に向け、約２年前から、システムベンダとも連携し、影響調査や改修等を進めてきた。
- 処理が5月以降となるサービス予約の日付の形式（和暦）を、連休前の2019年（平成31年）4月26日に切り替え、令和の年号に対応した。

【2　検知】

- 4月26日、店舗端末の利用者から、サービス予約日の日付表示が1989年（平成１年）となる旨の問い合わせが、システムベンダBのコールセンター経由で重要インフラ事業者のシステム部門に寄せられた。
- システム部門の職員が店舗に出向き再現性を確認

【3　対処】

- 基幹システムでのサービス予約のステータス確認により、影響はサービス予約の日付表示のみのトラブルであることを特定すると共に、該当する利用者数を正確に把握
- システムベンダ及び共同利用の重要インフラ事業者と連携して、影響範囲と対応の選択肢を精査し、当該トラブルへの対応方針を統一
- 調査結果と対応方針を顧客対応部門に展開し、顧客からの問い合わせへの態勢を用意
- トラブル認識から3時間後に、ホームページ等を通じて、サービス予約に影響がないことを利用者に提供し、混乱が大きくなる前に事態を収拾

【4　原因】

- 日付形式の切り替え日に関する認識が、店舗端末接続ネットワーク側との間で異なっていたため。（２つのシステムの切り替えタイミングに関する試験項目の不足）

【5　再発に備えた対策】

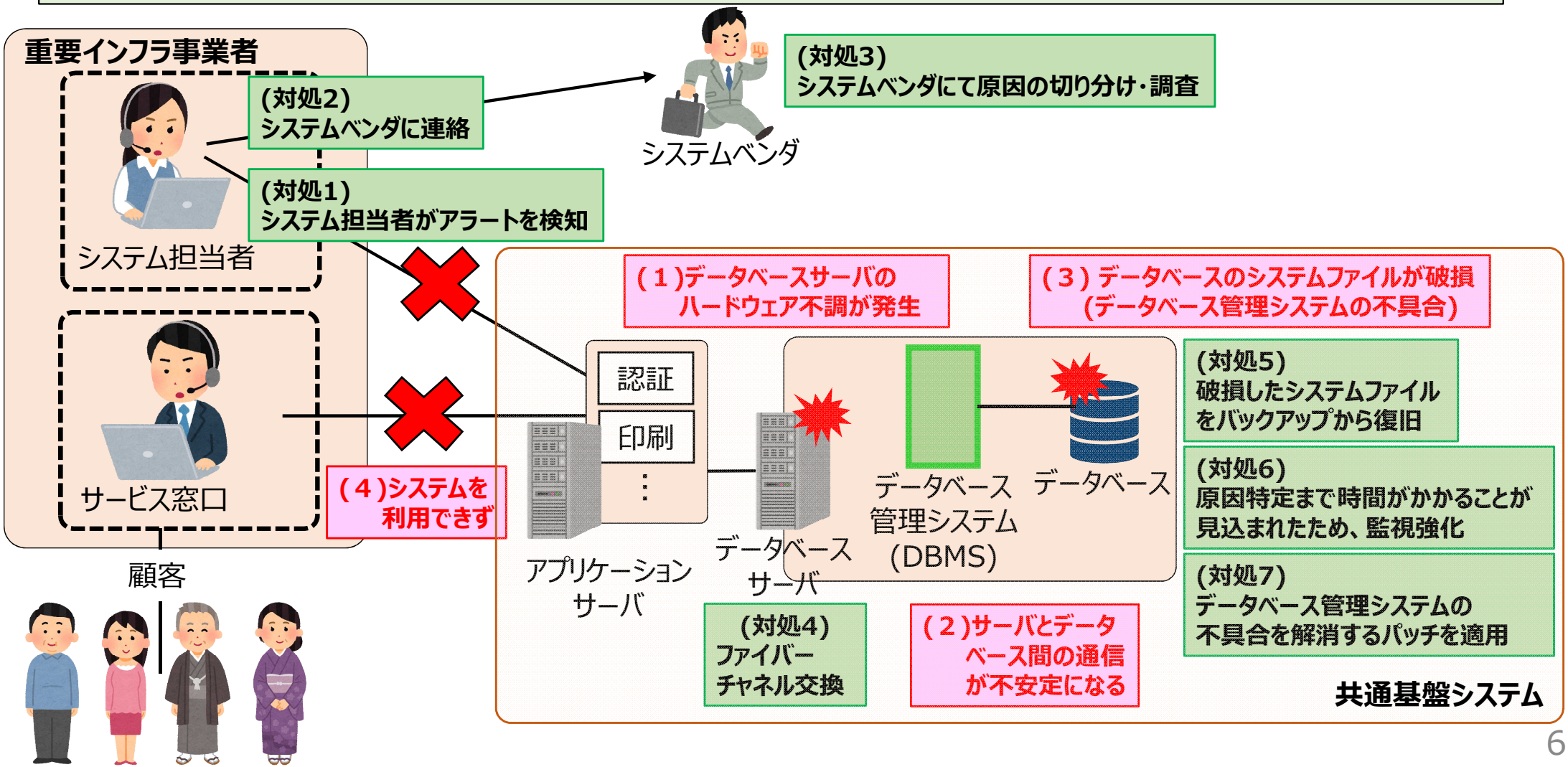
- システムの移行計画に関するプロジェクト管理方法（要件定義、試験観点抽出、コミュニケーションプロセス等）の見直し

【6　得られた気付き・教訓】

- **利用者への影響を抑えるため、敢えてサービスを止めない選択**
  システムベンダが提案した「サービス停止を伴うプログラム改修」等の選択肢もあった状況で、改修を実施する場合のリスクと、現状のままサービス継続することのリスクを正確に見極め、最も利用者に影響がない対応を選択した。
- **非常時に備えた権限移譲**
  重要インフラサービスに影響するシステム障害への対応方針の意思決定や公式HPへの案内掲載等の権限がシステム部門に委ねられていたため、一貫した対応を迅速に行うことができた。
- **顧客対応、広報と一体となった対応態勢**
  システム障害発生時に顧客対応、広報、システムの部門が密に連携して動くプロセスが、過去の経験から事業者内全体に定着しており、各部門が役割を迷いなく果たすことができた。
- **同分野の事業者と有事に協力できる関係**
  システムを共同利用する重要インフラ事業者同士が情報を共有できる関係が平時から構築されていたことが、利用者への統一的な対応に繋がり、分野全体で混乱を回避できた。

事例2　重要インフラサービスの一部業務の停止　1／2

- 重要インフラサービスで利用するデータベースのシステムファイルが破損したことにより、顧客がサービスを利用できなくなった。
- データベースサーバとデータベース間の通信が不安定になった際に発生するデータベースソフトの不具合により、データベースのシステムファイルが破損したことが原因。
- 恒久対策として、データベースソフトの不具合を解消するパッチを適用。



事例2　重要インフラサービスの一部業務の停止　2／2

【1　背景】

- 複数の業務において利用する、認証、印刷等の複数の機能を統合した、共通基盤システムを運用している。
- システムは、各機能が利用するデータを格納したデータベースサーバと接続している。
- システムにおいて、インシデント発生の1週間前から、業務に支障がないレベルの通信エラーが頻発していた。

【2　検知】

- システムを監視するシステム担当者がアラートの発生を確認し、障害を覚知した。
- システムを利用する複数の拠点から、印刷処理ができない旨の連絡が寄せられた。

【3　対処】

- インシデント発生前から通信エラーが頻発していたため、ハードウェア故障を疑い、ファイバーチャネルを交換した。
- 機器交換後、システムを再起動するも障害が復旧せず、データベースのシステムファイルの破損が判明した。
- サービスの優先度が高い業務から再開すべく、対応方針を決めた。また、バックアップファイルからシステムファイルを復元することで復旧し、業務を再開した。

【4　原因】

- データベースサーバのハードウェア不調により、サーバとデータベース間の通信が不安定になった。
- サーバとデータベース間の通信が不安定になった場合に発生するデータベースソフトの不具合により、データベースのシステムファイルが破損した。
- 不具合を改修する修正パッチを未適用であった。

【5　再発に備えた対策】

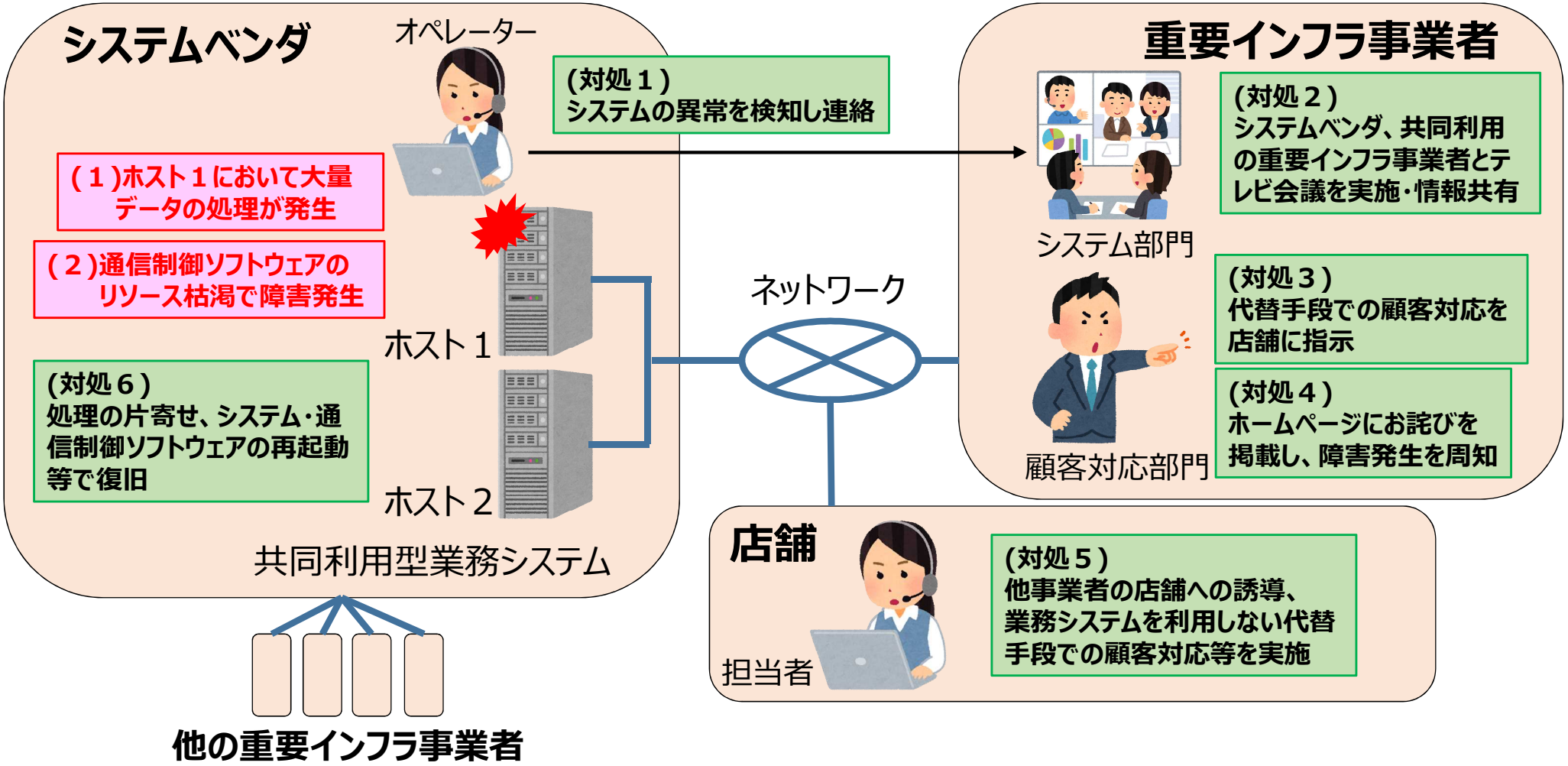
- データベース管理システムの修正パッチを適用した。
- データベースのシステムファイルを三重化した。
- ハードウェアが不調の場合に速やかに交換できるよう、システムの監視体制を強化した。

【6　得られた気付き・教訓】

- **サービスの優先度に応じた復旧対応方針の検討**
  障害発生時、サービスの優先度に応じて順次復旧できるよう、対応方針を決めた。
- **適時・的確な情報発信**
  事前に報道発表の基準・手順を策定していたことで、障害の発生や復旧見込みを適時・的確に公表できた。
- **インシデント対応体制の整備**
  複数の拠点に人員が配置され、距離が離れていたが、テレビ会議の利用により、円滑に連携できた。
- **平常時における対応の見直し**
  共通基盤システムでは、パッチ適用検証工数や適用することによる想定外の影響を鑑み、無条件に適用しない方がよいと考えていた。影響度の大きいパッチは検証の上、迅速な適用を検討するように対応方針を見直した。また、1週間前からインシデントの兆候(通信エラー)があり、対応について検討していたさなか、本事例が発生したことを踏まえ、今後障害につながる可能性が高い事象は早期に予防交換を含め対応することとした。

事例3　委託先のシステムトラブルに伴うサービス障害　1／2

- 複数の重要インフラ事業者が共同利用する業務システムにおいて障害が発生し、利用する複数の事業者において同時にサービス障害が発生。
- 重要インフラ事業者は、テレビ会議によりシステムベンダからの報告及び他事業者からの情報共有を受け、状況を把握。早期に代替手段での対応を店舗に指示、ホームページにお詫びを掲載するなどして、混乱を回避。
- 再発に備えた対策として、通信制御ソフトウェアのリソース監視強化、リソース枯渇時の対応マニュアルの策定、共同利用事業者の処理方法変更、他に同様の不備がないかを確認。



事例3　委託先のシステムトラブルに伴うサービス障害　2／2

【1　背景】

- 業務システムの開発・運用・保守は、システムベンダに委託していた。
- 当該システムは、汎用機ホストコンピュータ2台の2系統によるロードシェア構成としており、複数の事業者で共同利用していた。

【2　検知】

- システムベンダのオペレーターがシステム障害発生を検知。
- 職員が障害の再現性を確認。

【3　対処】

- ホームページ上へのお詫びの掲載、他事業者の店舗への誘導、当該システムを利用しない代替手段での顧客対応等を実施。
- システムを共同利用する複数の事業者間で、テレビ会議システムを利用して情報共有。
- 2系統のうち、障害が発生していないホストコンピュータへ片寄せ。
- ホストコンピュータ、通信制御ソフトウェアを再起動。

【4　原因】

- 大量データの処理が一時的に集中し、ホストコンピュータ上の通信制御ソフトウェアのリソースが枯渇。

【5　再発に備えた対策】

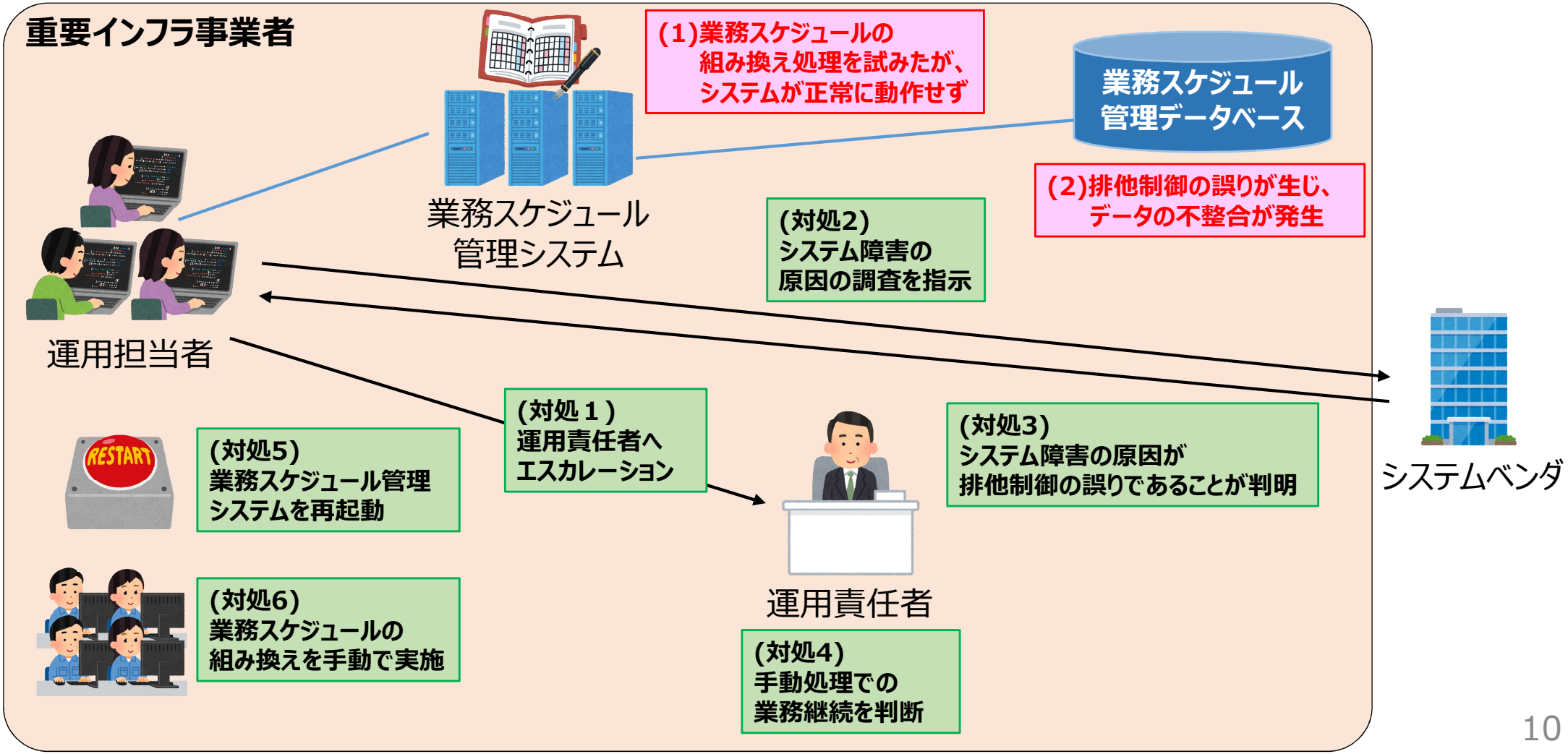
- 通信制御ソフトウェアのリソース監視強化。使用率がしきい値を超えた場合に警告メッセージを通知するようプログラムを変更。
- リソース枯渇時の対応マニュアルを策定。
- データ処理が集中しないよう、共同利用の事業者を順番に処理するように変更。
- 障害発生時、システムベンダから重要インフラ事業者の担当者への第一報がより迅速に伝えられるよう、初動対応を見直し。
- 業務システムの再点検(本件同様の不備の有無等)。

【6　得られた気付き・教訓】

- **緊急時の連絡体制整備**
  サービス提供支障発生時は、原因がシステム障害でも災害と同様の体制としていたことから、連絡体制が明確になっており、迅速な意思決定が行われた。また、権限移譲により、緊急時には、経営層へ情報共有するも、現場の判断に委ねられていたことが奏功した。
- **代替手段の準備**
  店舗では、システム障害が発生した場合に備えて、代替手段を確保していた。定期的に訓練していたため、大きな混乱もなく代替手段で顧客対応等を実施でき、事態の収拾につながった。
- **テレビ会議システムを利用した遠隔地との情報共有**
  システムベンダやシステムを共同利用する他の事業者とテレビ会議システムを利用して連携し、システムベンダからの障害状況・復旧目標等の情報、各事業者の対応状況等を情報共有したことが、全体として統一的・迅速な対応につながった。

事例4　重要インフラサービスの業務遅延　1／2

- 重要インフラサービスに遅延が生じたことから、業務スケジュール管理システム経由で業務スケジュールの組み換え処理を試みたが、システムが正常に動作せず、重要インフラサービスの業務遅延が拡大。
- 業務スケジュール管理システムにおいて、排他制御の誤りが発生し、データの不整合が生じたことが原因。
- 再発防止として、データベースから取得したデータが最新であるか否か確認する等、排他制御が確実に実施されるようにシステムを改修。



事例4　重要インフラサービスの業務遅延　2／2

【1　背景】

- 重要インフラ事業者では、事象発生当日、重要インフラサービスの一部業務に遅延が生じていた。
- 本重要インフラサービスでは、業務に遅延が生じた場合、業務スケジュール管理システムを操作することで、業務スケジュールの組み換えが自動で実施されるようになっていた。
- 業務スケジュール管理システムでは、複数の運用担当者からの業務スケジュール組み換え操作を誤りなく処理するため、排他制御処理（データベースへの同時アクセスによりデータの不整合が生じないよう、データの読み書きを一時的に制限する処理）を行っていた。

【2　検知】

- 運用担当者が業務スケジュール管理システムで、業務スケジュールの組み換え処理を実行したが、変更が反映されなかったことで、事象を把握。

【3　対処】

- システムベンダに原因の調査を指示
- 業務スケジュール管理システムの再起動。
- 重要インフラサービスの進行状況の更なる遅延を防止するため、業務スケジュールの組み換えを手動で実施。

【4　原因】

- 関連システムの一部更改や通信回線速度の高速化の影響で業務スケジュールの組み換え処理の実行速度が向上し、一部処理のタイミングずれが生じたため、排他制御が適切に実施されなくなった。
- 排他制御の誤りにより、古いデータを基に業務スケジュールの組み換えが実施され、業務スケジュールデータに不整合が発生。

【5　再発に備えた対策】

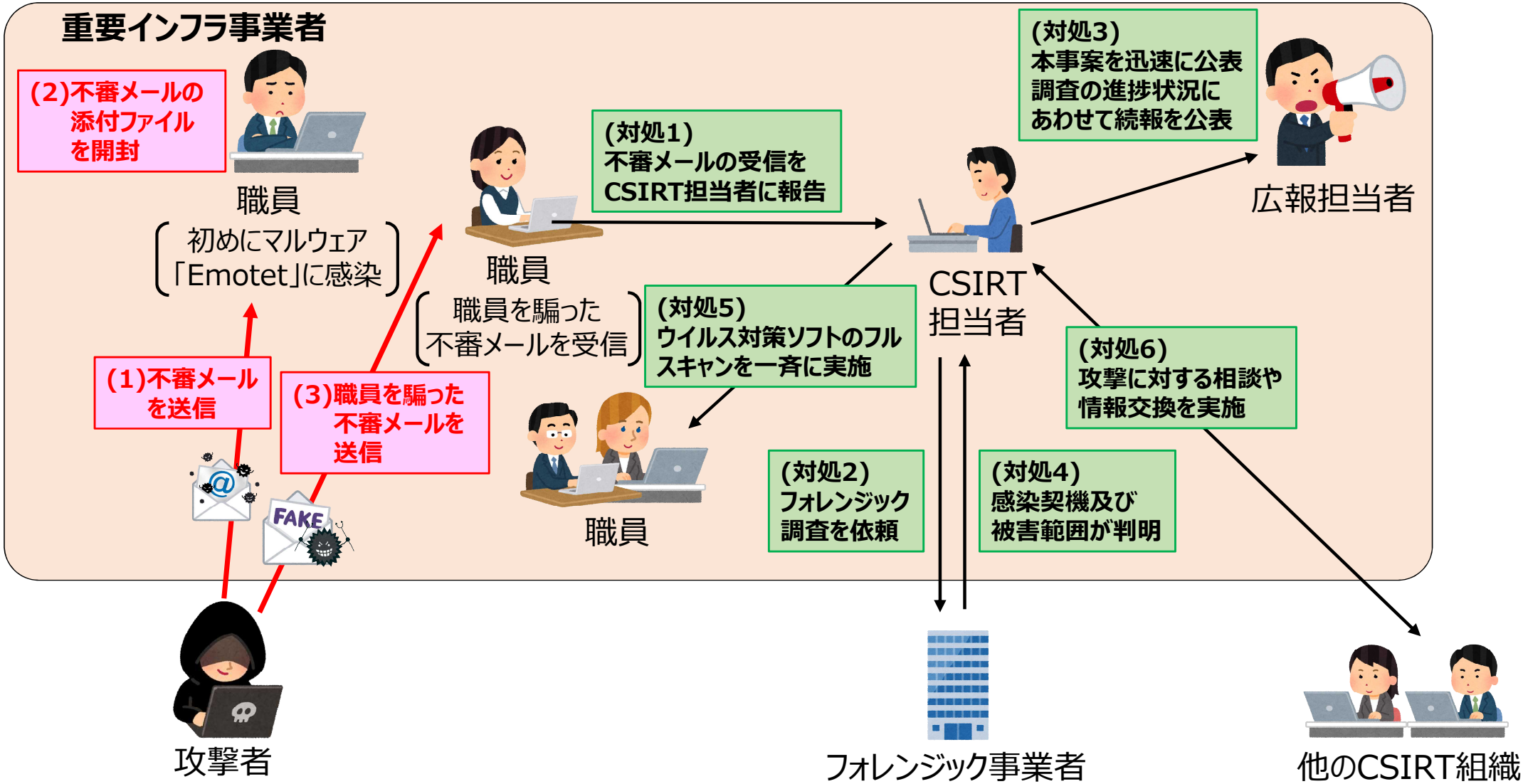
- 排他制御の誤りを防止するため、業務スケジュール管理システムにデータを取得、反映する際に、取得したデータが最新か否か確認する処理をシステムに追加。
- 排他制御の誤りを防止するため、業務スケジュールデータの参照時や更新時に同データにアクセスしている端末が存在するか否か迅速に確認できるよう、システムを改修。

【6　得られた気付き・教訓】

- **運用担当者を育成する取り組みの重要性**
  平時から、重要インフラ事業者では、有識者から運用担当者への業務ノウハウのレクチャや運用担当者間での勉強会の開催等、担当者のスキルを向上するための取り組みを定期的に実施していたため、障害発生時も、複雑な業務スケジュールの組み換え作業を手動で誤りなく実施できた。
- **障害発生時の迅速な判断**
  障害発生時における業務継続方針の決定権者が重要インフラ事業者内で明確になっており、本事案においても、手動での業務継続を迅速に判断できた。
- **排他制御の確実な実施**
  データの不整合が生じないようにするため、データベースから取得したデータが最新であるか否かの確認等、排他制御の仕組みが確実に実施されるようにシステムを設計することが重要。

事例5　不審メールによるマルウェア「Emotet」への感染　1／2

- 実在の組織や人物になりすます手口で、マルウェア「Emotet」に感染させる不審メールが流行。
- 重要インフラ事業者の職員が不審メールの添付ファイルを開封し、マクロを有効化したことで、端末がマルウェア「Emotet」に感染。感染後、感染端末を使用していた職員を騙るメールが、外部組織に送信。
- 再発防止策として、クラウド型メールサンドボックスの導入や職員に対する継続的なセキュリティ教育を実施。



事例5　不審メールによるマルウェア「Emotet」への感染　2／2

【1　背景】

- 実在の組織や人物になりすます手口で、マルウェア「Emotet」に感染させる不審メールが流行していた。
  添付ファイル(Word形式)を開き、マクロを有効化することで、端末がマルウェア「Emotet」に感染した。
- 重要インフラ事業者では、スパムメールフィルタを導入済。
- 重要インフラ事業者は、CSIRT間の情報共有コミュニティに参加しており、他のCSIRTに相談しやすい状況にあった。

【2　検知】

- 重要インフラ事業者（発生組織）の職員になりすましたメールを別部署の職員が受信、発生組織へ連絡したことで、担当者が事象を把握。

【3　対処】

- マルウェア感染が疑われる端末について、フォレンジック事業者にフォレンジック調査を依頼。
- 重要インフラ事業者が管理する全ての端末に対して、ウイルス対策ソフトのフルスキャンを一斉に実施。
- 迅速に第一報を公表した後、詳細な調査結果が判明する度に、続報を公表。

【4　原因】

- 重要インフラ事業者の職員が、外部から送信された不審メールの添付ファイルを開封してしまった。

【5　再発に備えた対策】

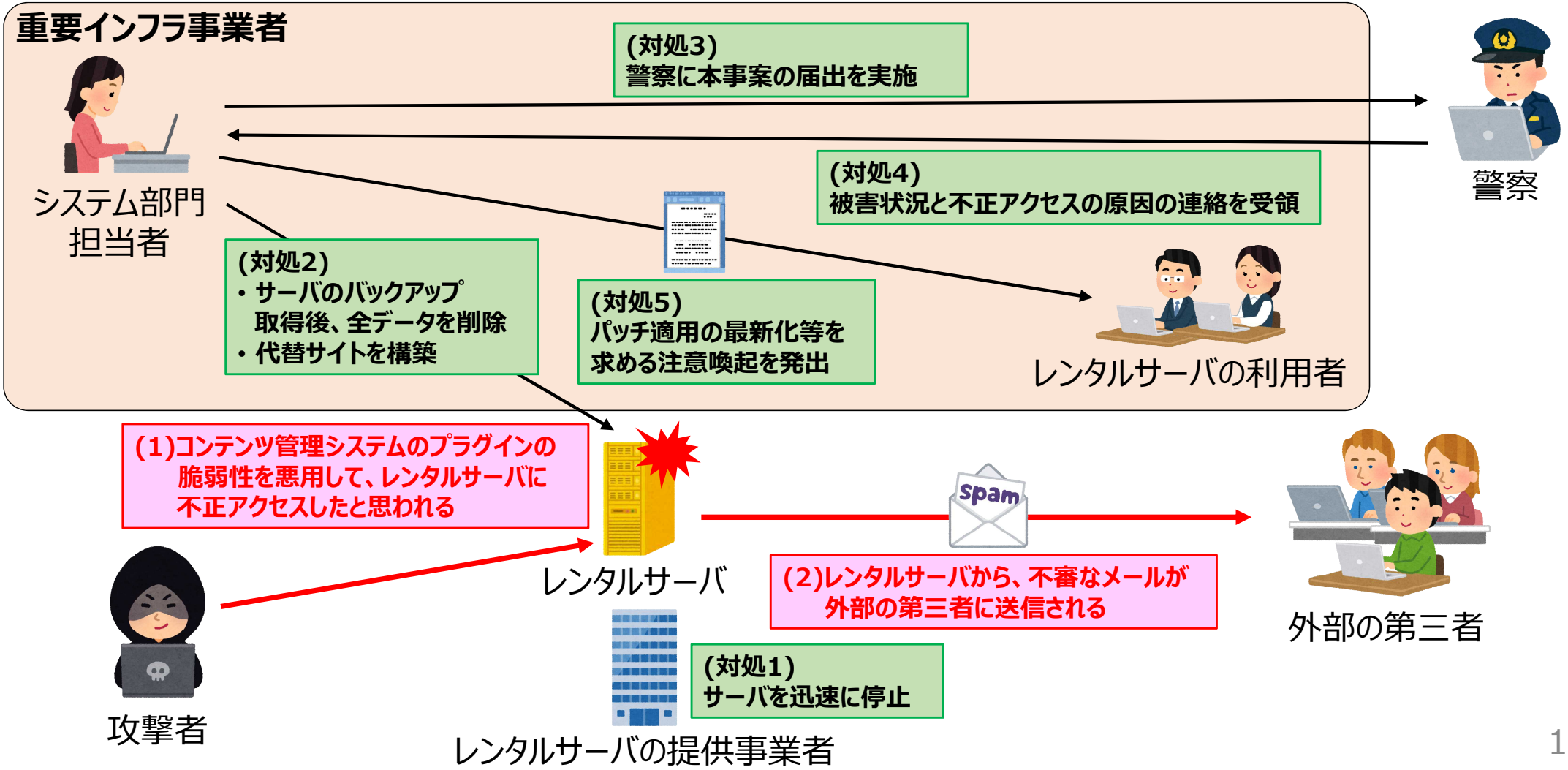
- 組織内のメールセキュリティ対策を強化し、比較的導入が容易なクラウド型のメールサンドボックスソリューションを導入。
- 攻撃の特徴や対策をまとめたリーフレットを全職員に配布。さらに、職員のセキュリティ知識の定着状況を確認するテストを実施。

【6　得られた気付き・教訓】

- **適時・的確な情報発信**
  緊急時対処マニュアルに基づき、迅速に第一報を公表し、その後も適宜必要なタイミングで情報を公表したことで、漏えいした情報を悪用した攻撃の二次被害を防止した。また、情報を公開したことで、他の重要インフラ事業者の対応にも貢献した。
- **情報共有コミュニティへの継続的な参加**
  日頃から情報共有コミュニティに継続的に参加していたことで、他のCSIRT組織と、本攻撃に対する相談や情報交換をしながら、対応を進めることができた。
- **不審メール受信時の報告体制の整備**
  重要インフラ事業者及び関連組織で、不審メール受信時の報告フローを定め、報告ツールを各端末にインストールしていたことで、本事案発生時にも、不審メールの受信がCSIRT組織に迅速にエスカレーションされた。
- **職員に対する継続的なセキュリティ教育**
  全職員に対し、不審メールの特徴をまとめた小型のリーフレットやマルウェア「Emotet」の概要を記載した文書を配布したり、セキュリティ知識の定着状況を確認するテストを実施したりすることで、職員のセキュリティ知識の底上げを図った。

事例6　重要インフラ事業者が利用するサーバへの不正アクセス　1／2

- 重要インフラ事業者が利用するサーバが不正アクセスされ、同サーバから外部に不審なメールが送信。
- サーバに導入していたコンテンツ管理システム(CMS)のプラグインの脆弱性を悪用し、攻撃者がサーバに不正アクセスした可能性が高いと考えられる。
- 重要インフラ事業者は、新たにサーバの運用契約をベンダと締結し、サーバのパッチ適用やインシデント発生時のログ調査をベンダに迅速に依頼できるようにした。



事例6　重要インフラ事業者が利用するサーバへの不正アクセス　2／2

【1　背景】

- 重要インフラ事業者のシステム部門がレンタルサーバを契約し、複数部署でサーバを共同利用していた。
- 重要インフラ事業者自身がサーバへのパッチ適用を実施していた。
- インシデント発生以前から、同レンタルサーバ上で構築されたWebサイトのレイアウトが崩れるといった事象が発生していた。

【2　検知】

- レンタルサーバの提供事業者が「当該重要インフラ事業者が利用するサーバから不審なメールが送信されている」と連絡したことで重要インフラ事業者は事象を把握。

【3　対処】

- レンタルサーバの提供事業者が、当該サーバを迅速に停止。
- バックアップ取得後、サーバの全データを削除し、別環境にて代替サイトを構築。
- システム部門が、レンタルサーバの利用者に対し、パッチ適用の最新化等を求める注意喚起を発出。
- 警察に本事案の届出を実施。

【4　原因】

- コンテンツ管理システム(CMS)のプラグインの脆弱性を悪用され、サーバが不正アクセスされた可能性が高い。

【5　再発に備えた対策】

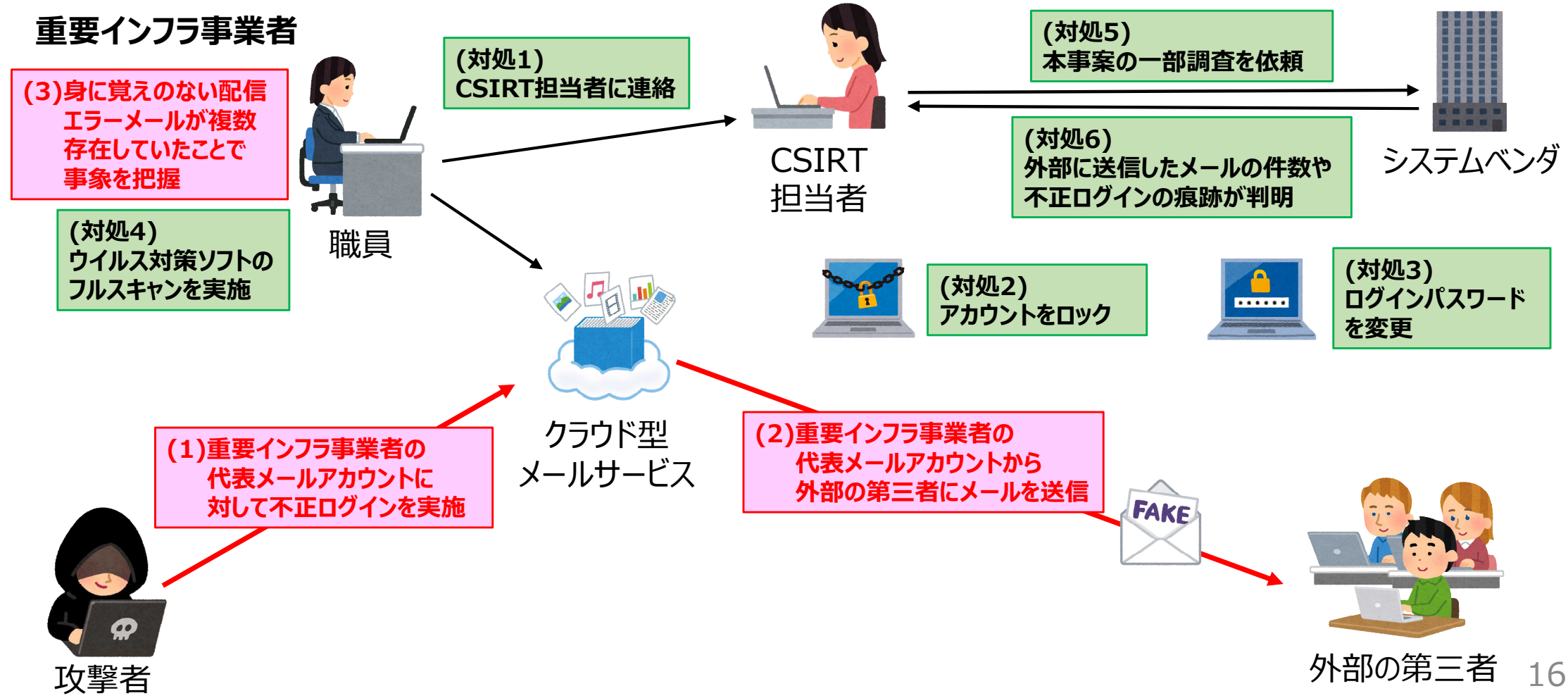
- 新たにベンダとサーバの運用契約を締結し、パッチ適用やインシデント発生時のログ調査をベンダに迅速に依頼できるようにした。

【6　得られた気付き・教訓】

- **セキュリティインシデント及び障害発生時の対応体制の整備**
  有識者に技術的見解を確認できる体制の構築やベンダとの委託契約の締結等を通じて、セキュリティインシデントや障害発生時に、ログの確認やサーバの設定変更等の技術的対応について円滑に実施できる体制を整備することが重要。
- **サーバの資産管理の徹底**
  コンテンツ管理システムのプラグインの脆弱性は、攻撃の対象になり易いため、パッチが公開され次第、できる限り迅速にパッチを適用する等の管理策を講じる。また、自組織の端末やサーバの資産管理を徹底し、インストールしているソフトウェアの一覧やバージョン情報を正確に把握できるようにする。
- **初動対応マニュアル策定の重要性**
  複数部署が関わる複雑なサービス提供体制であったが、初動対応マニュアルを策定し、レンタルサーバの利用者に配布していたことで、被害極小化に向けた対応が迅速に実施できた。
- **迅速な予兆の検知**
  Webサイトのレイアウトが崩れている、身に覚えのないアカウントが作成されている、突然アカウントロックがかかっている等、通常と異なる挙動が確認された場合は、些細なことでもシステム管理者に報告するように、各システム担当者に対し意識づけを行う。

事例7　クラウド型メールサービスに対する不正ログイン　1／2

- 重要インフラ事業者が利用するクラウド型メールサービスに対し、攻撃者が不正アクセスを実行し、重要インフラ事業者のメールアカウント経由で、当該事業者とは無関係なメールが大量に外部へ送信。
- 重要インフラ事業者の職員が受信メールボックスを確認した際、身に覚えのない配信エラーメールが複数存在していることに気付き、本事象を把握。
- 再発防止として、クラウド型メールサービスのログイン画面へのアクセス制限や取得可能なログの整理と設定の見直しを実施。



事例7　クラウド型メールサービスに対する不正ログイン　2／2

【1　背景】

- 重要インフラ事業者では、クラウド型メールサービスを利用しており、同サービス上に、重要インフラ事業者配下の各組織の代表メールアカウントを作成していた。
- ログイン画面で、ID(メールアドレス)とパスワードを入力することで、メールサービスを利用可能であった。

【2　検知】

- 職員が自組織の代表メールアドレスを確認した際、身に覚えのない配信エラーメールが受信メールボックス内に複数存在していることに気付き、事象を把握。

【3　対処】

- 不正アクセスされたメールアカウントのロックを実施。
- 同メールアカウントを使用していた職員の端末全てに対し、ウイルス対策ソフトのフルスキャンを実施。
- 重要インフラ事業者配下の全ての組織のメールアカウントに対して、ログインパスワードを変更。
- クラウド型メールサービスのログ等をもとに、攻撃者が不正ログインしたアカウント経由で外部に送信したメールの件数や不正ログインの痕跡を特定。

【4　原因】

- クラウド型メールサービスのログイン画面について、どこからでもアクセスできるようになっていた。
- クラウド型メールサービスに対して、IDとパスワードのみでログインできるようになっていた。

【5　再発に備えた対策】

- クラウド型メールサービスのログイン画面にアクセス可能なIPアドレスを制限。
- クラウド型メールサービスのアクセスログ保存期間を見直し。
- Webフィルタリングソフトを用いて、過去に職員がアクセスしたフィッシングサイトをブロック。
- 職員に対するeラーニングやセキュリティ勉強会を実施。

【6　得られた気付き・教訓】

- **クラウド型メールサービスへのログイン強化**
  クラウド型メールサービスについては、業務要件を踏まえ、アクセス元IPアドレスを制限する若しくは、多要素認証を導入する等の不正ログイン対策を講じることが重要。
- **クラウド型メールサービスのログ保存期間の検討**
  クラウド型メールサービスを利用する前に、同サービスのアクセスログやメール送信ログ、メール受信ログ等のログデータの保存期間を十分検討し、万一のセキュリティインシデント発生時に、不正アクセスの原因や被害状況を調査できるようにする。
- **迅速な不正ログインの兆候の把握**
  クラウド型メールサービスの利用者が、身に覚えのない配信不能メールが受信メールボックスに存在する、メールの自動転送設定が追加されている等の異常を把握した場合は、迅速にシステム管理者に報告する旨、職員に教育することが重要である。また、コストは掛かるが、サービスのログを監視するサービスを契約することも選択肢としては考えられる。