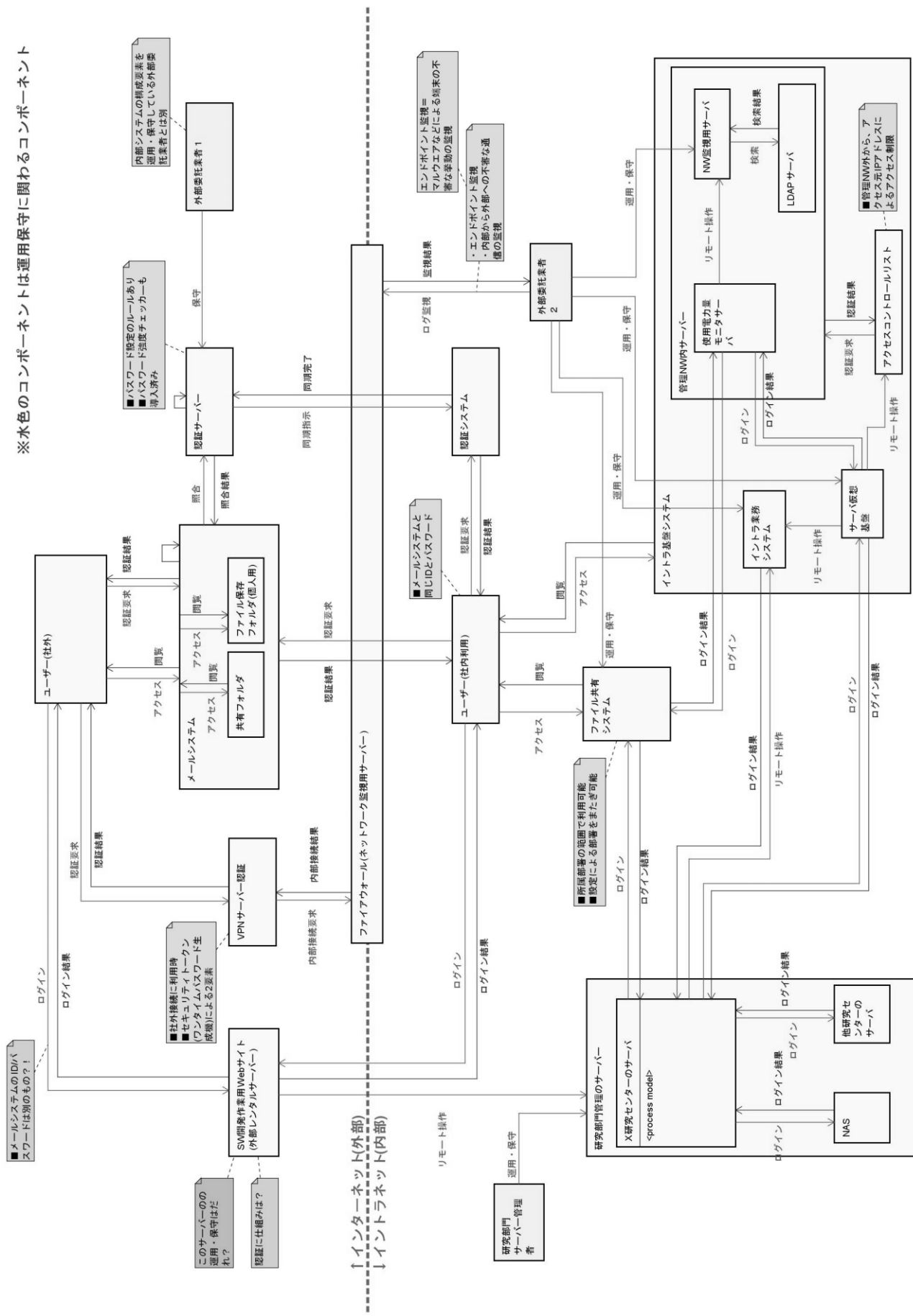
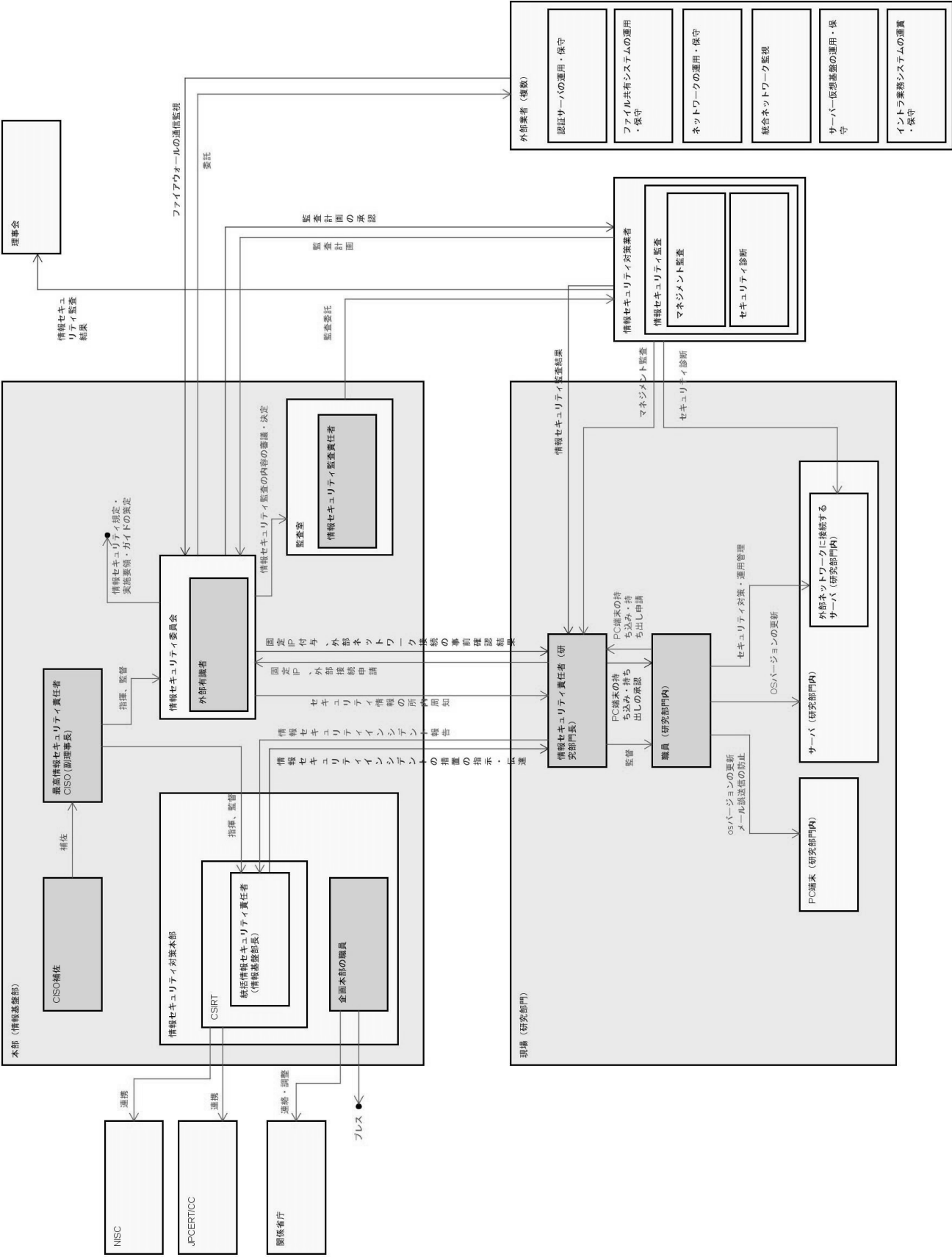


※水色のコンポーネントは運用保守に関わるコンポーネント



付録2：表4.1.3-2 [CAST3]安全CS (セキュリティマネジメント)



付録3：表4.1.3-3 【CAST4】イベントチェーンと質問生成（システム・運用保守）

ID	損失に近接する「システム、運用保守」上の発生イベント (What? : 何が起きたのか) ※産総研（損失を被った側）の視点から記述	各イベントが発生した理由の説明に対して、回答する必要があるような質問を作成 (Why? : 原因究明のため明らかにしたいこと)	調査報告書による説明	各イベントが発生した理由の説明に対して、回答する必要があるような質問を作成 ※調査報告書による説明に対して追加
0	何らかの手法により職員のアカウントへ不正ログインされた	<検知・分析> Q0-1. なぜ、不正ログインを検知できなかったか？	A0-1. 詳細の記述無し	<準備> Q.A0-1. 情報基盤部によるセキュリティ診断がうまく機能していなかった？
1	<<アクション01>> 外部ネットワークに構築した認証サーバーに対して、パスワード試行攻撃（ブルートフォース攻撃）が行われた	<検知・分析> Q1-1. なぜ、パスワード試行攻撃を検知できなかったか？ <準備> Q1-2. なぜ、認証サーバーは外部ネットワークに構築されていたのか？リスクは考慮されていたか？ Q1-3. なぜ、認証サーバーのアドレスが特定されたのか？	A1-1. ID/パスワードを探り当てようとするパスワード試行攻撃の兆候があったが、それを察知はしていた。しかし、察知した際に有効な対策が打てなかった (侵入者はパスワード試行攻撃等により、10月27日から12月未までの第1次攻撃で100名の職員アカウントに不正ログインしたと推測される) A1-2. メールシステムはクラウドサービスであり、クラウドサービスの導入時、VPNによるアクセス制限を解除して利便性を向上させた。し	<封じ込め> Q.A1-1. なぜ、察知した時点で対策を打つように動けなかったか？ <準備> Q.A1-2. なぜ、VPNアクセス制限解除によるリスク評価が行われなかったか？ Q.A1-3. ログインが外部から可能であったことが起因している？
2	<<アクション02>> 特定したパスワードを用いて、外部ネットワーク上のメールシステムへ不正ログインが行われた	<準備> Q2-1. なぜ、簡単に特定できるパスワードが含まれていたのか？ Q2-2. パスワード運用ルールは存在したか？存在した場合、ルールは守られていたか？	A2-1. 職員に対するパスワードの設定ルールは定めていたものの、キーボード配列をそのままの安易なパスワードを設定していた例があった（このため、100アカウントのパスワードを特定され、メールシステム等に侵入された）。また、管理者パスワードについても安易な設定が少なからずあった。 A2-2. 2017年11月に新たなパスワードの設定ルールを設けるとともにパスワードの強度チェッカーを導入したが、キーボード配列をなぞっただけのようなパスワードを排除するようものではなかった。	<準備> Q.A2-2. なぜ、パスワード設定ルールや強度チェッカーは効果的に運用されなかったのか？
3	産総研が保有するIPアドレスの全域に対してポートスキャンが行われ、外部から利用の際に用いるVPNの接続口を発見された	<検知・分析> Q3-1. なぜ、ポートスキャンを検知できなかったのか？	A3-1. 詳細の記述無し	<準備> Q.A3-1. 情報基盤部によるセキュリティ診断がうまく機能していなかった？
4	メールシステムへの不正ログインで利用されたアカウントを用いて不正接続が試みられたが、VPNサーバーで二要素認証を実施していたため、侵入を防いだ	<検知・分析> Q4-1. なぜ、不正接続の痕跡を検知できなかったのか？	A4-1. ある時点で検知はしていたが、すべて失敗と判断していた	<準備> Q.A4-1. 情報基盤部によるセキュリティ診断がうまく機能していなかった？ <検知> Q.A4-1. なぜ、すべて失敗と判断したのか？
5	何らかの手法で外部レンタルサーバーの「サイト」のID/パスワードを特定され、不正ログインされた	<準備> Q5-1. なぜ、ファイアウォールの外に「サイト」を公開していたのか？ Q5-2. なぜ、外部レンタルサーバーの存在やアドレスを特定されたのか？	A5-1. 詳細の記述無し A5-2. 詳細の記述無し	-----
6	<<アクション03-1>> 内部ネットワーク内に設置された仮想マシンとQを遠隔操作された	<準備> Q6-1. なぜ、遠隔操作できたのか？	A6-1. 「サイト」には、内部サーバと連携して、外部から容易に内部サーバ上のOSをコントロールできる機能（外部からの遠隔操作）があった。 この機能の危険性について、X研究センターの認識が不足していた。	<準備> Q.A6-1. なぜ、X研究センターは機能のセキュリティ上の危険性について認識が不足していたのか？
7	<<アクション03-2>> 仮想マシンPに通信中継ソフトウェアを設置され、イントラ業務システムへのアクセスが行われた。 研究部門管理の仮想環境の仮想マシン4台やNASにマルウェアが設置された	<準備> Q7-1. なぜ、イントラ業務システムのURLが特定されたのか？ Q7-2. なぜ、マルウェアが設置されてしまう脆弱性が認識されていなかったのか？	A7-1. イントラシステムのURLは、それまでにメールシステムへの不正ログインで閲覧していた被害アカウントのメールの内容から見つけ出していたものと推定できる A7-2. 以前より脆弱性の懸念が指摘されていたNASが、安価であること等を理由に、十分なリスク評価をせずに多くの研究部門で使用されていた。一部の外部委託業者は、保守サポート期限が切	<準備> Q.A7-2. なぜ、NASの脆弱性に対するリスク評価が十分されなかったか？ 外部委託業者へのガバナンスが弱かった？
8	---ここからは更なる被害の拡大--- 仮想マシンPを踏み台として、内部システムへのポートスキャンが行われた	<検知・分析> Q8-1. なぜ、内部システムへのポートスキャンを検知できなかったのか？	A8-1. 統合ネットワーク監視を外部委託業者に委託し、ファイアウォールその他のログを自動検知ルールにより監視していたものの、内部システムへ侵入された後のポートスキャンを検知することができなかった。 (2017年12月21日、12月22日、12月27日、2018年1月15日、1月19日、1月23日にポートスキャンが実施された。また、1月23日にポートスキャンが実施された。)	<封じ込め> Q.A8-2. 内部システムへ侵入された際の被害の最小化が考慮されていなかった？
9	メールシステムのアカウントを用いて、ファイル共有システムへの不正アクセスが行われた	<準備> Q9-1. なぜ、メールシステムとファイル共有システムのアカウントは同じだったのか？リスクは考慮されていたか？	A9-1. 詳細の記述無し	<準備> Q.A9-1. 利便性を重視し、セキュリティリスクが評価されていなかった？
10	<<アクション04>> リモートデスクトップにより使用電力量モニターサーバーへ不正侵入された	<準備> Q10-1. なぜ、アクセス制限していなかったのか？ Q10-2. なぜ、IDやパスワードが特定できたのか？ Q10-3. なぜ、内部ネットワーク内を自由にアクセスできたのか？	A10-1. 一部の外部委託業者のサーバについては、十分なセキュリティ対策が講じられていなかった。 情報基盤部とは別の組織が管理していて、アクセス元IPアドレスを制限する必要性の認識が共有されていなかった。 A10-2. 要機密情報の送信方法についての具体的なルールはなく、多くの場合、パスワードをメールで送信していた（メール内に書かれていた管理者パスワードや暗号鍵を侵入者に窃取され、それを用いてメールの添付ファイルの閲覧やサーバへの侵入等が行われた） A10-3. 内部ネットワークが広域でフラットな構成であり、研究用ネットワークと、業務用ネットワークとが切り離されていなかった。このため、内部ネットワーク内であれば、どのサーバへも到達可能な状態に	-----
11	<<アクション05>> LDAPサーバーで不正検索し、職員のアカウントを窃取された	-----	-----	-----
12	LDAPサーバーの不正検索で特定した情報を用いて、メールシステムへの第二次攻撃が行われた	-----	-----	-----
13	<<アクション06>> ファイル共有システムへ管理者権限で接続されたり、サーバー仮想基盤の管理コンソールへ不正ログインされた	<準備> Q13-1. なぜ、管理用ID/パスワードを暗号化せず保管していたのか？	A13-1. 詳細の記載なし	<準備> Q.A13-1. 外部委託業者に対するガバナンスの弱さが起因している？

付録4：表4.1.3-4 [CASTS] 具体的なコンポーネントレベルでの分析（システム・運用保守）

No	カテゴリ	CASTS-1 安全上の置換(責任)	CASTS-2 非安全なコンポーネントロケーション	CASTS-3 脆弱なコンポーネントロケーション	CASTS-4 脆弱なコンポーネントロケーション	CASTS-5 脆弱なコンポーネントロケーション
1	システム (外部)	・認証サーバにユーザIDおよびパスワードの照合を行い、照合結果が一一致したユーザのみアクセス許可を与える ・照合結果が一一致しないユーザにはアクセス許可を与えない ・ログイン用のIDを各職員が独自に決める任意の文字列であるパスワードが二つあるのに近い設計となっていたことから、リスト型攻撃」に陥えられた	(1)同一ユーザIDのログイン試行失敗に対して何もなかった (2)アクセスしているのが正規ユーザが攻撃者か判別できなかった (3)キーボード配列のまのみのパスワードを判別していた (4)攻撃者からの攻撃に対し、監視者は「攻撃は失敗している」と判断した (5)サーバ所有者(産総研)は攻撃を受けたことに対して何もなかった (6)正規ユーザが不正ログインされていることに気付かなかった	(1)不審なパスワードは行はるネットワーク上の対象に含まれていなかった (2)アクセス元に対し本人確認する制御がなかった (3-1)変更で推察されたり弱いパスワードを設定する(パスワードポリシー)であった (3-2)弱いパスワードを設定する一部の職員は、定期的に弱いパスワードに変更し続けていた (4-1)監視者の攻撃の結果を判断する過程・方法が誤っていた (4-2)監視者は攻撃の結果を理解する資料(ここではログ)を持っていなかった (5-1)サーバ所有者は攻撃の重大性を理解していないかった (5-2)サーバ所有者は攻撃失敗＝被害が出ていると認識した (6)他者にログインされていることに対しての通知・制御がなかった	CASTS-5-4 脆弱なコンポーネントロケーション (1)認証サーバは、別の保守委託先業者が管理しており、産総研ネットワークの外に置かれていたため (2)認証サーバ(を外部からログインできる設計に変更した際に、ユーザの利便性を考慮してPIN接続環境を外した (3-1)ログインIDが任意の文字列のためパスワード本体に対するセキュリティが下がっていた (3-2)不明 (4)不明 (5-1)サーバ所有者(産総研)は攻撃の重大性やリスク、および被害について知識がなかった (5-2)サーバ所有者(産総研)が監視体制、監視基準などに攻撃に対する事象が盛り込まれていなかった (6)不明	(1-1)知識不足・急いでいた・外部サーバに重要な情報は漏れない認識だった・後で検討する予定だった？ (1-2)手続に対する知識不足・手続自体の集約度・煩雑さによる断念・手続の強制力のため・手続が書類にだけ有効かない・形骸化？ (2-1)メール上にログイン情報を記載していた (2-2)インターネット上に設置することのリスクを認識していなかった (2-3)不明 (3)利便性/研究に必要であることも優先する状況だった？ (4)インターネット上に設置することのリスクを認識していなかった (5-1)X研究所サーバ管理者は知識が不足していた (5-2)産総研は (6-1)逆向接続以外の解決策がなかった (6-2)逆向接続が最も容易な解決策だった
2		ソフトウェア開発用Webサーバ	(1)FWの内側と外部とを接続するサーバを構築した際、所定の手続きを行っていなかった (2)ソフトウェア開発用Webサーバに攻撃者の侵入を許した (3)ソフトウェア開発用WebサーバからX研究所内の仮想マシンを遠隔操作された (4)ソフトウェア開発用WebサーバにはX研究所内の仮想マシンにマルウェアを置かれた (5)外部から内部マシンのOSを操作できるように構成のシステムをFWの内側と外部にまたがって設置した (6)想定していない環境下で逆向き接続の設定を使用した	(1-1)手続の必要性を理解していなかった (1-2)手続があることを知らなかった (1-3)無手続であることを産総研側が気付かなかった (2-1)ソフトウェア開発用Webサーバのログイン情報が攻撃者に流出していた (2-2)公開電話番号認証番号を用いて、ID・パスワードによるログインで利用可能になっていた (2-3)攻撃者からのアクセスに気付かなかった (3-1)FWが5FW内のマシンを操作可能にするに對する重大性を認識していなかった (3-2)X研究所内の仮想マシンのアクセス状態を監視していなかった (4-1)X研究所内の仮想マシンの状態を監視していなかった (4-2)X研究所内の仮想マシンにマルウェアを検知する仕組みがなかった (5-1)システム構成の危険性を認識していなかった (5-2)システム構成の危険性を検知・指摘されなかった (6)逆向き接続を採用したこと	(1)サーバ管理元が別組織だったため情報の共有がなされていなかった (2)FW内のためセキュリティ設計・認識が甘くなっていた (3-1)そういう運用手順になっていた (3-2)パスワードと連絡する際の運用ルールがなかった/周知されていなかった/運用ルールが存在したが守られていなかった	
3	システム (内部)	・個別のアクセスコンポーネント・リストにより個別にアクセス元IPアドレスを制限し、管理用ネットワーク外からは直接アクセスできないようにするルールを設けていた	(1)管理用ネットワーク外から直接アクセスできる状態となっていた (2)管理ネットワーク外から直接アクセスできることを産総研内で検知できなかった (3)サーバに管理者アカウントで侵入された	(1)情報基準部とは別の組織が管理していたが、アクセス元IPアドレスを制限する必要性の認識が共有されていなかった (2)管理ネットワークの中でのアクセスを監視していなかった (3)管理者(パスワード)の回答でパスワードルールを本文に記載したメールを送受信していた	(1)サーバ管理元が別組織だったため情報の共有がなされていなかった (2)FW内のためセキュリティ設計・認識が甘くなっていた (3-1)そういう運用手順になっていた (3-2)パスワードと連絡する際の運用ルールがなかった/周知されていなかった/運用ルールが存在したが守られていなかった	
4		NW監視用サーバ (外部委託者管理)	・アクセスコンポーネント・リストにより個別にアクセス元IPアドレスを制限し、管理用ネットワーク外からは直接アクセスできないようにする ・産総研の情報はセキュリティポリシーを遵守するよう、契約における仕様で定めている ・外部委託者には監査を行う決まりがある	(1-1)アクセスコンポーネント・リストによるアクセス制御が行われていなかった (2-1)各サーバのソフトウェア状態の監視・更新が行われていなかった (2-2)ソフトウェア更新動向を監視していた (3-1)syslogサーバを管理(パスワード保管場所として勝手に決めていた (3-2)管理(パスワード)保管場所が他になかった (3-3)管理(パスワード)の保管方法が決まっていなかった (4-1)管理(パスワード)の管理方法を決めていなかった/決めていたが守っていなかった (4-2)管理(パスワード)を平文で置くことの危険性がわかっていなかった (5)産総研の管理基準と異なる基準で管理が行われている	(1)不明、イントラ内のNWなので必要ないと判断していた？ (2)不明、必要ないと判断していた？ (3-1)現場がその運用を判断していた？ (3-2)syslogサーバに置くのが正規の運用だった？ (3-3)正規の格納場所がアクセスしにくい場所にあった？ (4)管理対象のサーバにログインする頻度が多いため参照しやすい平文で格納した？ (5)管理基準は外部委託者側で決めてよく、産総研との合意・協議は必要ないと思っていた？	
5		LDAPサーバ	----	(1)パスワード記録・持ち出すことができた (2-1)LDAPのログイン情報は認証サーバのログイン情報が同じユーザに保管されていた (2-2)ハッシュ化したパスワードがユーザのアカウントに保管されていた	(1)持ち出す作業が日常的なもので、持ち出す設定・持ち出す前提の運用になっていた (2-1)LDAPと認証サーバに同一ユーザに格納する設計の認証システムだった(なぜそのような設計に？) (2-2)ハッシュ化したパスワードが処理に必要な前提の認証システムだった(パスワードを暗号化(パスワードと同じユーザに置いたのはなぜか)	

[illegible]

●：直接的な要因、○：直接的な要因から影響すると思う要因

No	欠陥	CAST手順	コンポーネント	欠陥分類	キーワード1	キーワード2	システム/運用					セキュリティマネジメント			CAST7-1				CAST8
							ログイン認証機能	不正監視機能	内部ネットワークへの侵入	外部システムへのログイン制御	内部システム間のアクセス権限格	マネジメント体制（本部）	マネジメント体制（各研究部門）	情報セキュリティ監査体制	情報交換と相互連携 ＝周知徹底不備、暗黙のルール、不測事態の連携不備など	安全な情報システム ＝ルール、手順、リスク未知などの監護不備	安全なマネジメントシステムの設計 ＝ルール、手順、更新話かせない、改善/変更時の不備など	安全な文化 ＝風土、思い込み、意識など	
1	要機密情報の送信方法についての具体的なルールはなく、多くの場合、パスワードをメールで送信していた	CAST4	-----	UCA	パスワードポリシー	パスワード連絡の不備	●		○			●				●	○		
2	メール内に書かれていた管理者パスワードや暗号鍵を侵入者に窃取され、メールの添付ファイルの閲覧やサーバへの侵入等に成功した	CAST4	-----	UCA	パスワードポリシー	パスワード連絡の不備			○	○	○	●				●	○		
3	定期的に通信監視結果を確認/報告する仕組みがあったのか？	CAST4	-----	UCA	セキュリティ体制	組織間の連携不足		○				●	○		●				
4	セキュリティ診断結果を報告し、その内容をフィードバックする仕組みがあったのか？	CAST4	-----	UCA	セキュリティ体制	組織間の連携不足		○				○	○	●	●				
10	報告を受けた情報基盤部は詳細な調査を行わなかったのか？	CAST4	-----	UCA	セキュリティ体制	組織間の連携不足		○				●	○	○	○		●		
11	マネジメント監査やセキュリティ診断は定期的に実施していたが、形式的なアタリや一般的な脆弱性診断に留まっていたのか？	CAST4	-----	UCA	セキュリティ体制	運用の不備		○				●		●			○	○	●
13	定期的にポートスキャンがないか確認/報告する仕組みがあったのか？	CAST4	-----	UCA	セキュリティ体制	組織間の連携不足			○			●			●				
14	セキュリティ診断結果を報告し、その内容をフィードバックする仕組みがあったのか？	CAST4	-----	UCA	セキュリティ体制	組織間の連携不足						●		○	○		●		
15	定期的なセキュリティ診断結果がインシデント対応に活かされる仕組みがあったのか？	CAST4	-----	UCA	セキュリティ体制	組織間の連携不足			○			●		○	○		●		
21	一部の外部委託業者のサーバについては、十分なセキュリティ対策が講じられていなかった。	CAST4	-----	UCA	セキュリティ体制	運用の不備					○		●	○	○	●			
23	日常的な情報機器のチェック、インシデントに関する監視とその報告等が適切に行われないケースもあり、また、リスクに認識がなかった	CAST4	-----	UCA	セキュリティ体制	組織間の連携不足			○		○	●			●				●
25	メールシステムとファイル共有システムのログインIDは同じであったがリスクは考慮されていたか？	CAST4	-----	プロセスモデル	ログイン	ログイン認証の強度不足	●		○			○				○	●		
27	職員、管理者に対するパスワードの設定ルールは定めていたが、キーボード配列をなぞっただけの安易なパスワードを設定された	CAST4	-----	プロセスモデル	パスワードポリシー	パスワードの強度不足	○		○			●		○		○			●
28	新たなパスワードの設定ルールを設け、パスワードの強度チェックを導入したが、安易なパスワードを排除できなかった	CAST4	-----	プロセスモデル	パスワードポリシー	パスワードの強度不足	○					●		○		○	○		●
29	ルールを変えたが、強度を満たすパスワードが適用されるのは次のパスワード有効期限切れのときであり、今回のパスワード変更時に適用されなかった	CAST4	-----	プロセスモデル	パスワードポリシー	パスワード運用の不備						○		●		○	○		●
38	脆弱性がある状態を、研究部門や情報基盤部は認識していたのか？	CAST4	-----	プロセスモデル	セキュリティ体制	組織間の連携不足					○	●	○	○	○		●		
39	ログインIDをメールアドレスではなく、職員が独自に決める任意の文字列としていることから、いわゆるリスト型攻撃の影響を受ける	CAST4	-----	意思決定の背景	ログイン	ログイン認証の強度不足	●		○			○		○		○		●	
40	当該認証サーバでは、ログインIDをメールアドレスではなく、職員が独自に決める任意の文字列としていることから、いわゆるリスト型攻撃の影響を受ける	CAST4	-----	意思決定の背景	ログイン	ログイン認証の強度不足	○			○		●		○		○		●	
42	定期的なセキュリティ診断結果がインシデント対応に活かされる仕組みがあったのか？	CAST4	-----	意思決定の背景	セキュリティ体制	組織間の連携不足		○					●	○			●		
62	管理ネットワーク外から不正ログインされた	CAST5	NW監視用サーバ(外部委託者管理)	UCA	ログイン	ログイン認証の強度不足	○			●			○			●	○		
84	ソフトウェア開発用Webサーバに攻撃者の侵入を許した	CAST5	ソフトウェア開発用Webサーバ	UCA	ログイン	不正ログイン						●	○			○			
93	ソフトウェア開発用Webサーバのログインに公開鍵暗号認証等を用いずに、ログインID・パスワードによるログインで利用可能に	CAST5	ソフトウェア開発用Webサーバ	プロセスモデル	ログイン	ログイン認証の強度不足	●		○			○		○		●	○		
112	ログインしているのが正規ユーザか攻撃者か判別できなかった	CAST5	メールシステム	UCA	ログイン	不正ログイン		●	○					○		●			
113	キーボード配列のままのパスワードを許可していた	CAST5	メールシステム	UCA	パスワードポリシー	パスワードの強度不足	○		○			●		○		●	○		
116	正規ユーザのログインIDで不正ログインされていることに気付かなかった	CAST5	メールシステム	UCA	ログイン	不正ログイン		●	○					○		●			
118	アクセス元IPアドレスに対し本人確認する制制がなかった	CAST5	メールシステム	プロセスモデル	ログイン	不正ログイン	●		○					○		●			
119	安易で推測されやすいパスワードが設定できるパスワードポリシーとなっていた	CAST5	メールシステム	プロセスモデル	パスワードポリシー	パスワードの強度不足	○		○			●			○	○	●		
120	弱いパスワードを設定する一部の職員は、定期的に弱いパスワードに変更し続けていた	CAST5	メールシステム	プロセスモデル	パスワードポリシー	パスワードの強度不足	○		○			●		○		○	○		●
128	ログインIDが任意の文字列のためパスワード本体に対するセキュリティが下がっていた	CAST5	メールシステム	意思決定の背景	パスワードポリシー	パスワードの強度不足	○		○			●		○		●	○		
149	不正なログインIDにも関わらず不正ログインされた	CAST6	外部システム(不正アクセス)	UCA	ログイン	不正ログイン	●		○			○				●			
151	ログイン試行に対する制限がない	CAST6	外部システム(不正アクセス)	プロセスモデル	ログイン	ログイン認証の強度不足	●	○				○				●	○		
153	ログイン認証が安易で推測されやすいパスワードが設定できる	CAST6	外部システム(不正アクセス)	プロセスモデル	パスワードポリシー	パスワードの強度不足	○		○			●		○		●	○		
154	ログイン認証が2段階認証になっていない	CAST6	外部システム(不正アクセス)	プロセスモデル	ログイン	ログイン認証の強度不足	●					○				●	○		
156	ログインIDを各職員が独自に決める任意の文字列としていた	CAST6	外部システム(不正アクセス)	意思決定の背景	ログイン	ログイン認証の強度不足	●					○				●	○		
157	パスワードが二つあるのに近い設計になっていたことから、リスト型攻撃に耐えられると想定していた	CAST6	外部システム(不正アクセス)	意思決定の背景	パスワードポリシー	パスワードの強度不足	○					●		○		○		●	
158	認証サーバを外部ネットワークからログインできる設計に変更した際に、EVSSL証明書の導入によって、認証サーバのログインIDが変更された	CAST6	外部システム(不正アクセス)	意思決定の背景	ログイン	不正ログイン	●					○				●	○		●
163	パスワードが安易なものが使われている	CAST6	内部システム(アクセス権限格)	プロセスモデル	パスワードポリシー	パスワードの強度不足	○		○			●	○	○		○		●	
181	セキュリティマネジメントに関する人が足りない	CAST6	マネジメント体制(本部：情報基盤部)	UCA	セキュリティ体制	体制の不備			○		○	●	○	○	●				
183	CISOと情報セキュリティ責任者間での意思疎通の迅速性に欠けている	CAST6	マネジメント体制(本部：情報基盤部)	プロセスモデル	セキュリティ体制	組織間の連携不足			○		○	●		○	●				
184	情報セキュリティ対策に組織的に取り組めていない	CAST6	マネジメント体制(本部：情報基盤部)	プロセスモデル	セキュリティ体制	組織間の連携不足				○		●		○	●		○		
185	情報技術に関する専門家の人数が不足しており、研究部門へのサポートが十分にできていない	CAST6	マネジメント体制(本部：情報基盤部)	プロセスモデル	セキュリティ体制	体制の不備		○		○		●		○	●				
186	重大なインシデントが発生した際に参照する事業継続計画が用意されていない	CAST6	マネジメント体制(本部：情報基盤部)	プロセスモデル	セキュリティ体制	危機管理の不備			○		○	●		○	●				

付録7：表4.1.3-7 【CAST7,8】事例の特徴と分析から見える弱点とその改善案

項	特徴	分析から見える弱点	改善勧告案
1	侵入に関するもの	アクセス元の信頼性の欠如 VPNや二段階認証の導入を対策としているが、固定のID、パスワードでは下記手段により解読の可能性があると考えられる - 盗み見 - キーロガー - 総当たり攻撃 など	●正規ユーザー認証の強化 認証要求元が、産総研が認めた正式なユーザであることを証明できるデータを認証要求データに組み込む。 例： ワンタイムパスワードの導入 電子証明書によるアクセス元の信頼性の向上
		アクセス内容の監視の欠如 不正アクセスと思われる攻撃があったときに、即時に検知、制御できる仕組みがなく、専門家である外部委託業者の対応に依存しすぎたと考えられる	●不正アクセスの検出・制御力の強化 常時監視・常時検知・常時追従の仕組みを検討し、アクセス監視の結果を外部委託業者から産総研に常時公開し、異常値のアラート検知時に即緊急通知が出るようにする 例： 回数制限などにより自動的にIDの無効化(ロック、失効など) 電子証明書が不一致の不正アクセス パスワードミス など ●アクセス内容の監視強化・監視精度向上 外部委託業者から監視プランを提出させ、産総研の有識者が監視プラン(監視対象、異常判定条件、測定方法)に対し、妥当性確認を行った上で運用を実施するようにする
2	アクセス権限に関するもの	ユーザー毎の権限の分離の欠如 管理用ネットワーク内のサーバにアクセス制限の設定がネットワーク内のいずれかのサーバで管理者のID、パスワードハッキングされると他のサーバにアクセス可能になると考えられる	●ユーザーに応じたセキュア情報の分離を強化 サーバー管理に対して、サーバー毎に管理者アカウントを設定し、他サーバーへのアクセスを制限できるようにする 例： サーバ毎に管理者のID、パスワードをユニークする サーバ毎の管理者を分離する
		業務毎の権限の分離の欠如 外部委託業者が利用するパスワード情報を厳格にルール化しても再発する可能性がある。 社内ユーザーが危険性があるところに安易にシステム構築ができる、してしまう前提の考慮が必要と考えられる	●カテゴリ毎にセキュア情報の公開範囲を限定する 《外部委託業者》 産総研のセキュア情報を渡さず監視業務が可能な運用を検討し作成する 例： システム・機器に直接アクセスせずとも業務可能にする仕組み 事前に開示はIDのみ、パスワードは必要時に産総研内で発行、一定期間経過後、自動で無効化 《社内ユーザー》 ユーザに実行されて困る処理を洗い出し、その処理に必要な情報はセキュア情報として公開しない。ユーザが実行できる処理を事実上不可能にする 上記を可能にしたのちは、前述の「●不正アクセスの検出・制御力の強化」で挙げた常時監視・常時検知・常時追従で、実行してしまった場合を摘出できるようにする
3	マネジメントに関するもの	有識者の助言の欠如 有識者の不足や担当者の意識不足の対策としてインシデントの訓練とあるが、意識改革やスキルアップの対策を講じる必要があると考えられる	●意識改革・スキルアップ インシデント訓練に加え、ワークショップやマイスター認定制度など導入などの対策を組み込む。
		セキュリティ監査の形骸化 監査頻度が年1～2回と少なく、前回からの差分が大きくなり、組織やユーザーがまだ追従しきれず、形骸化する可能性がまだ残っていると考えられる	●常時監視・常時検知・常時追従が行える仕組みの検討 アクションの頻度を上げ、セキュリティ監査1回のアクションでの差分追従が可能な状況にする 例： ・監視情報をデイリーで取得・検知条件を設定値化し、照合を行う ・監査対象の変更の登録箇所を制定し、変更発生時は必要関係部署へ通知する ・監査側のセキュリティ監査内容見直しも週次で行う
		責任者/担当者の責務の形骸化 ITの専門家の外部委託業者に任せている甘えから当事者意識を醸成する、というゴールから逆算して、必要な育成プランが必要であると考えられる	●当事者意識の醸成 ゼロトラストネットワークの前提に基づいた設計を行い、その理念を共有することで、責任者に対する当事者意識を育てる ●セキュリティマネジメントに対する専門家を調達 極力システム設定・プログラミングで対策させるための方策を立案してもらう ●損害発生時のロールプレイ 実際の受ける損害の試算、各方面への対応、謝罪、など責め立てられる状況をロールプレイする

[illegible]

FRAM_手順2（各コンポーネントの抽象化）

■抽象化の考え方

- ・今回の情報漏洩は本人認証におけるアタックがスタートであるため、「本人認証機能」と「産業研・各研究部門のデータ管理機能」を中心に考える
- ・産業研の内部NW（業務システムと各研究部門の各サーバ／NAS）へアクセスは、今回の情報漏洩元がX研の外部サーバであることから、「産業研NWアクセス機能」として1機能として着目する

■抽象化の単位

○本人認証機能

- ←・メールサーバ利用の認証
- ・業務システムを利用するときの本人認証
- ・各研究所が管理しているサーバにログインするときの認証（サーバローカルでの認証含む）

○産業研・各研究部門のデータ管理機能

- ←・メールサーバ：
メール情報を参照／送信／受信
- ・業務システム：
業務システムのアプリ機能
- ・各研究部門が管理しているサーバ／NAS： 各研究部門毎に管理している保存／参照

○産業研NWアクセス機能： 利用者の端末を論理的に業務システムや各研究部門のサーバにアクセス可否を提供

- ←・インターネットからの職員のVPN接続機能： 職員がインターネットからリモートアクセス（クラウドのアプリ）提供
- ・外部サイトへ各研究部門サーバ接続間のFW機能： 外部接続用FW
- ・産業研内のローカルLANの接続機能： 産業研内のスイッチHUBやWiFi、等

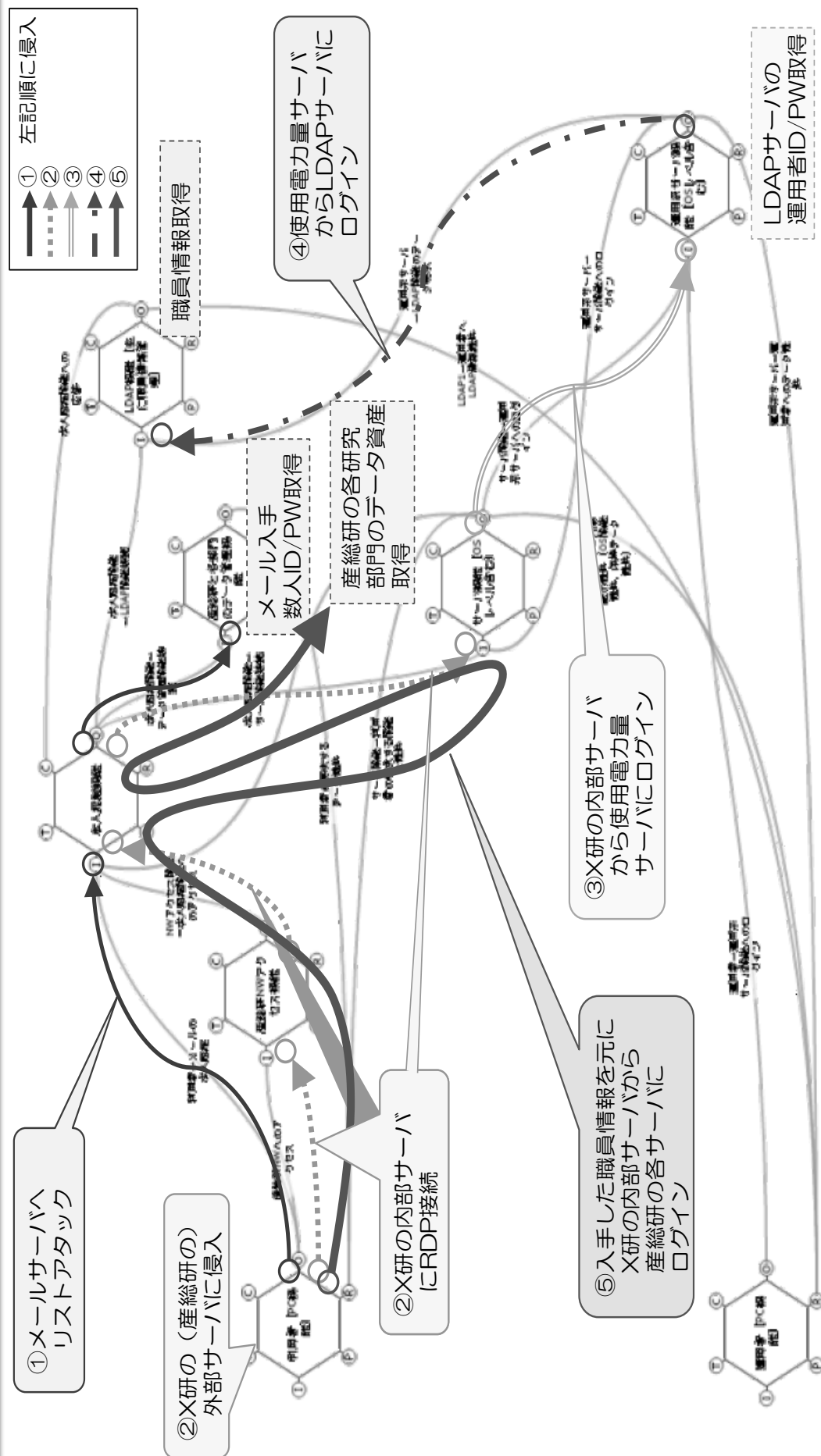
○サーバ機能（OS含む）：

- ←・各研究部門のサーバ：

○利用者（PC含む）： 本人認証がOKなら自分自身が利用可能な情報／データを利用できる

- ←・職員等、正当な利用者
- ・産業研の外部に設置しているサーバから内部NWにアクセスする利用者
- ・不正侵入者

FRAM_手順3（モデルの可視化）と手順4（攻撃経路のシミュレート）





FRAM_手順5（対策案の創出）

■改善の考え方

- ・運用系は、職員など利用者が直接利用するサーバやノード関連と疎結合の状態にするため、運用系の機能と利用者が関係する機能との間に、「運用系→各システムの接続機能」（具体的には、運用系サーバと業務システム／各研究部門のサーバ間にFWもしくはNW機器）を導入。各研究部門のサーバから運用系サーバ／NW機器へのログインを禁止する。併せて、「運用者用の認証機能」を導入する。
- ・職員等の利用者が「本人認証機能」に接続する前に、「産総研NWアクセス機能」経由とする。産総研NWアクセス機能としてどこまで機能強化（例、ワンタイムパスワードや端末認証）を具備するかは、言及しない。
- ・業務システムと研究部門それぞれ間の機能を疎結合とするために、「サイト間接続機能」を導入する。具体的には、業務システムと研究部門それぞれNWを分離し、ある研究部門から、他の研究部門のサーバや業務システムに接続するためのFWもしくはNW機器を導入する。

■改善に含めていない内容

- ・本人認証機能の強化（例、パスワードの複雑性強化、パスワードロック、多要素認証、等）については、「本人認証機能」そのものに閉じる仕様（他の機能に影響しない）のため、ここでは言及しない

■上記対策でも攻撃を防げないケース

改善を実施しても対応できない場合が存在する

- ①ID／PWが既に出回っている場合
- ②職員等の利用者のPCに侵入されている場合

どちらも、産業研の各システム（各研究部門のサーバも含む）は、「本人認証が正しく機能すれば、その人の権限に基づいた情報資産にアクセスできる」というポリシーで設計しているからである。別の表現を用いると、「本人認証が正しいが、不正アクセスされている可能性の検討が抜けている」

⇒①の対策

- ・PWの全変更。その後の定期的なPW変更 →人系の処理なので、いずれ同じPWに戻る可能性が高い
- ・生体認証、ワンタイムトークン、等の多要素認証の導入 →コスト増、利用者の作業負担など出る。

⇒②の対策

- ・ウィルス対策ソフトの導入
- ・利用者のPCは産業研情報システム部で管理し、個人が好きなソフトや勝手な利用方法を制限する

■上記ケースへの対策

○不正アクセスを「Monitor」「Learn」「Anticipate」「Response」機能を追加により、遮断する機能を設ける

Learnの例：

“利用者毎に利用している時間帯利用”、“利用者が普段利用しているデバイス”

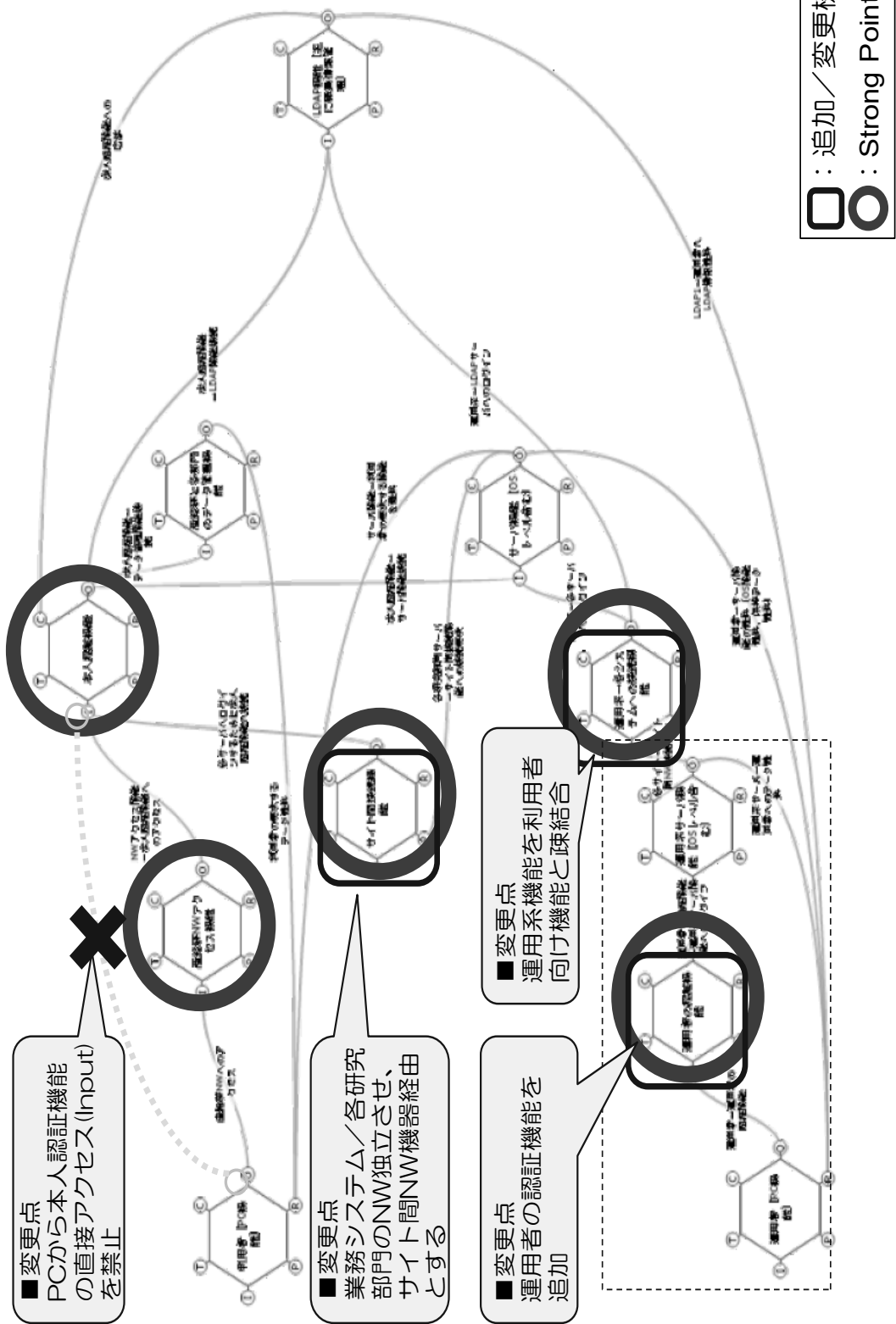
Anticipateの例：“特定のIPアドレスから複数IDでアクセスは不正の可能性大”、

“普段存在しない第三国のIPアドレスからアクセスは不正の可能性有”、等

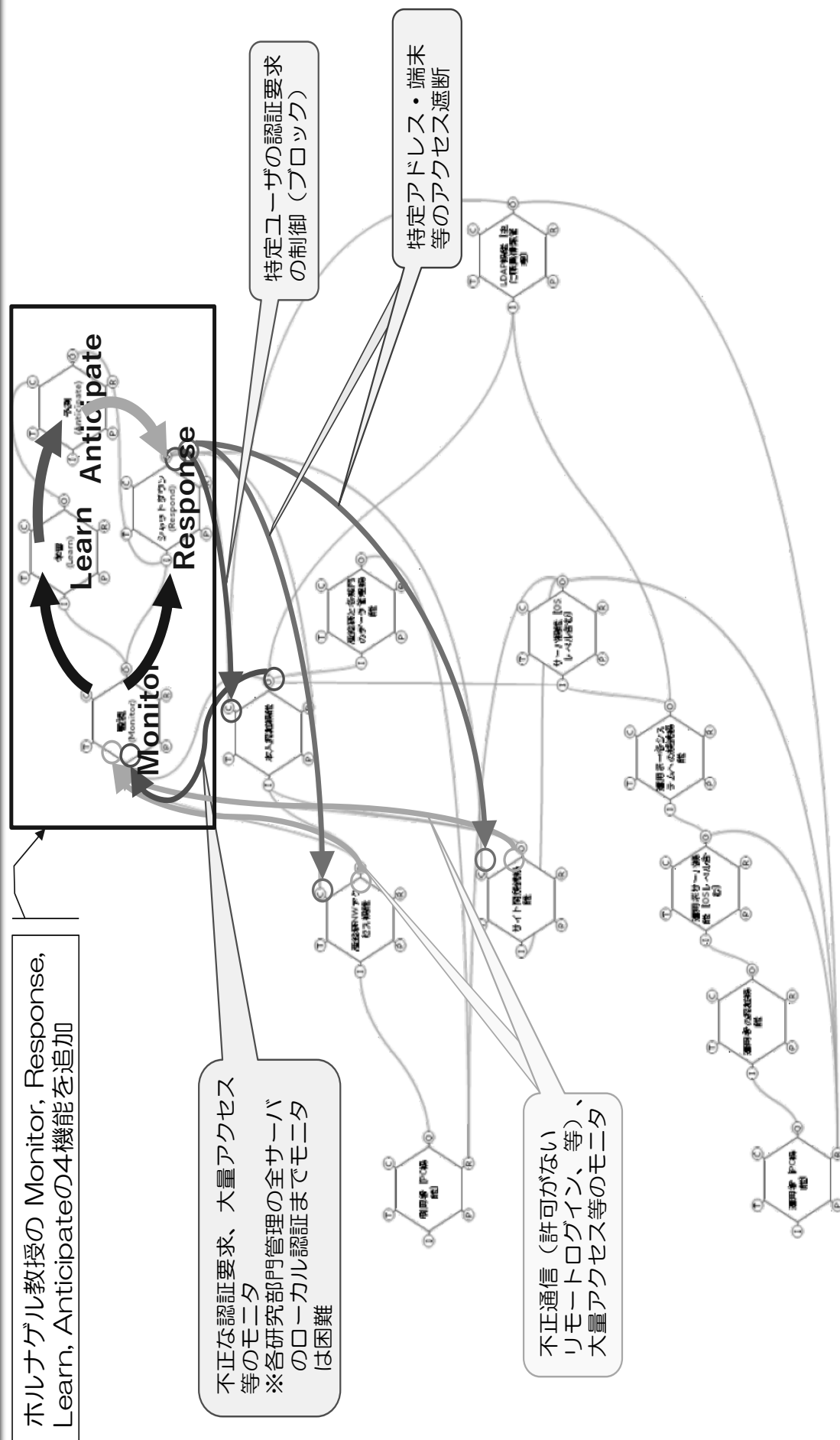
→ホルナゲル教授の4機能を追加することにおいて、

「Monitor」「Response」機能を、「本人認証」「NWアクセス機能」「サイト接続間機能」と結び

FRAM_手順5（対策案を講じたモデルの再可視化）



FRAM_手順5（対策案にHollnagel教授考案の4つの能力の追加）



付録15：表4.3-2 考察に対する各分析手法の評価

No	観点	CAST	FRAM	共通
1	分析過程に課題があったか？	-	-	・別々にモデルを作成すると、三者三様のものが出来上がる ・一つのベースモデルを最初に作成して分析を進めることで解消できる。 ・コンポーネント二つからスタートしてもいい ・時系列の情報が掴みづらいため、別途補う手法が必要（状態遷移など） （例えばCASTだと、コントロールストラクチャーの経時的变化を表現する手順は用意されていない）
2	分析成果物に対する認識に課題があったか？	・コントロールストラクチャーの解釈について、人ごとの違いは見られなかった	・まず図表を読み解くことが難しく、読み解いても解釈の違いが出る傾向があった	-
3	実務で使える事故分析手法か？	・サポートに入ってくるレベルのインシデント情報でも、カジュアルに実施できた実績あり。発想を膨らませるフレームワークとして使える ・コントロールストラクチャーは情報共有するのに良い ・悪かったところを把握し、次に設計に活かすときにはSTPAに反映する。初期設計として取り込むことで同様の事故を繰り返さないようにできる	・想定シナリオを用意してから適用するのが良いと思われる ・産総研事例では、FRAMの6機能を全部使いきれなかった。同期処理・非同期処理が組み合わさったようなシステムだと効果が発揮できるのでは ・事故分析よりも、設計段階から活用したほうがいい手法という所感 ・現状を把握し、理想はどうあるべきか示し、現状から理想に向かうためにどうすればできるか考える	-