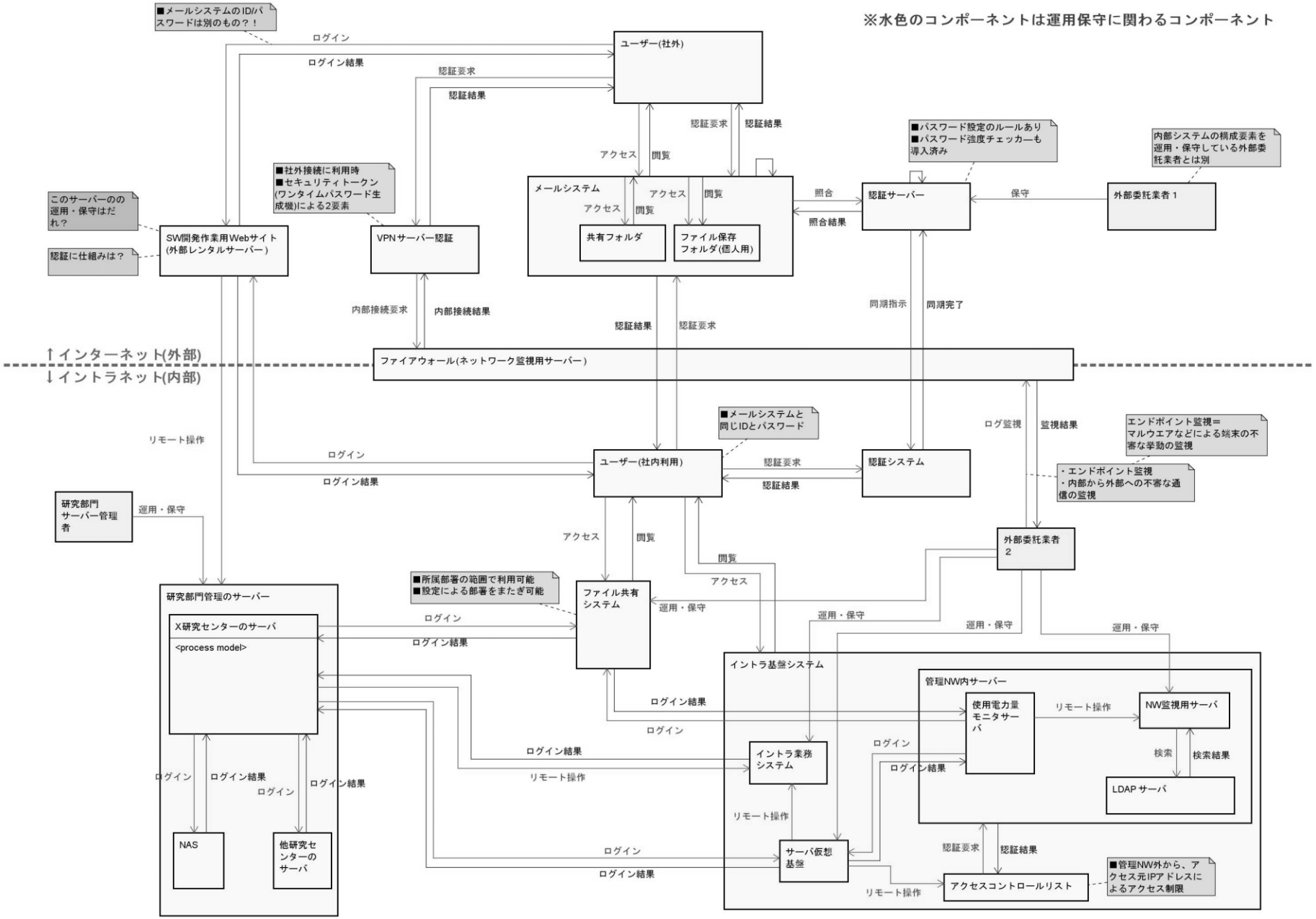
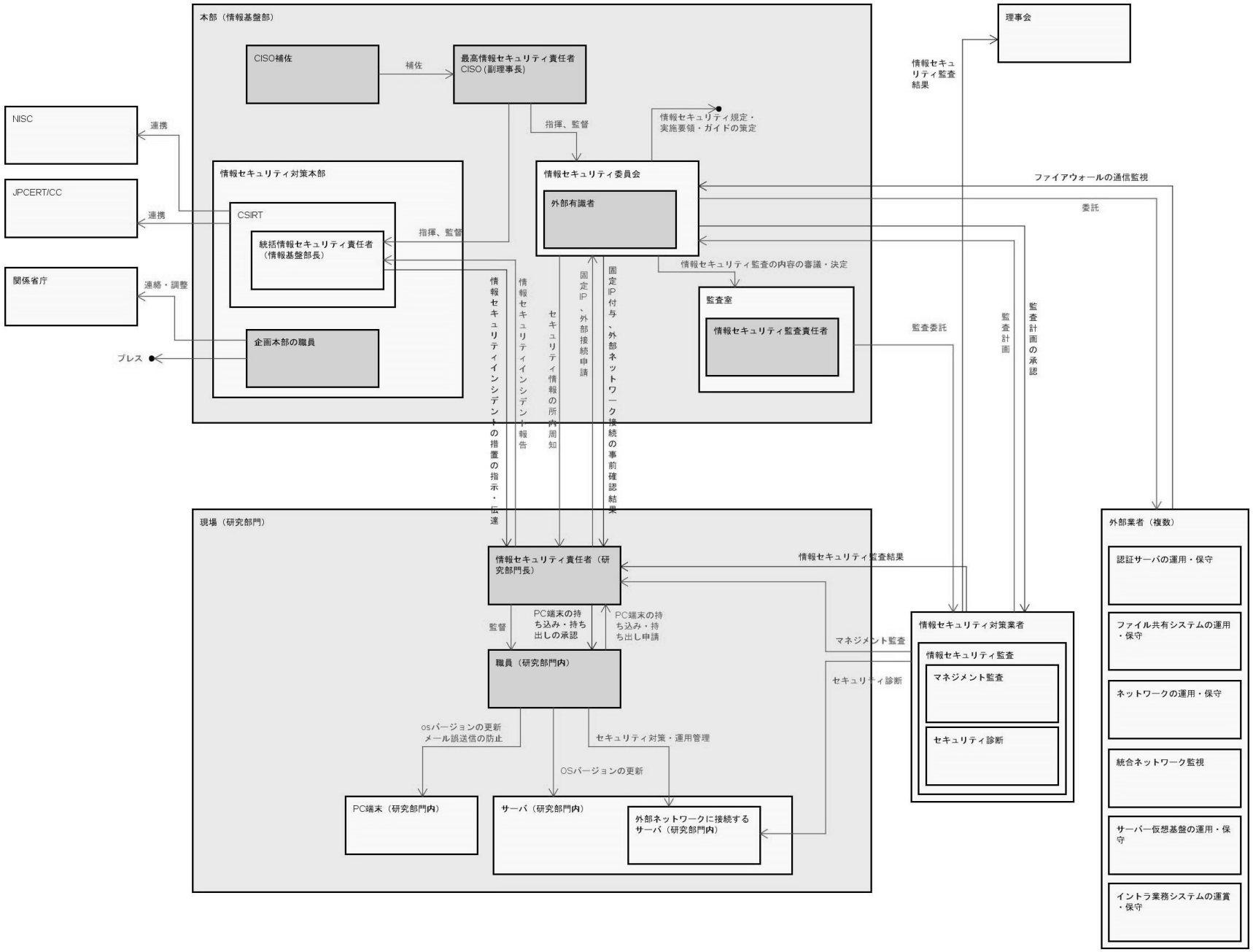
付録1：表4.1.3-1 【CAST3】安全CS（システム・運用保守）



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、回答する必要がありそうな質問を作成 （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、回答する必要がありそうな質問を作成 ※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	<<アクシデント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 月末までの第 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	<<アクシデント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、キーボード配列をなぞっただけ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なものではなかった。	<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「J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「J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	<<アクシデント03-1>> 内部ネットワーク内に設置された仮想マシンP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.「J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	<<アクシデント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 ---ここまでで分析対象のスコープ上に到達	<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れたサーバを使用していた。	<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行われたが、それらのポートスキャンについて、統合ネットワ	<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	<<アクシデント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	<<アクシデント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	<<アクシデント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 【CAST5】具体的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	インシデント発生対象	CAST5-1 安全上の責務(責任)	CAST5-2 非安全なコントロールアクション	CAST5-3 プロセスモデルの欠陥	CAST5-4 意思決定された状況・背景
1	システム(外部)	メールシステム	・認証サーバでユーザIDおよびパスワードの照合を行い、照合結果が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」に耐えられる想定だった	(1)同一ユーザIDのログイン試行失敗に対して何もしなかった (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まのパスワードを許容していた (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しなかった (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)不審なパスワード試行は統合ネットワーク監視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)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 (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材(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かった (5-2)サーバ所有者は攻撃失敗＝被害が出ていないと認識した (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	(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VPN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)は攻撃の重大性とリスク・及ぼす被害について知識がなかった (5-2)サーバ所有者(産総研)の監視体制・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
2		ソフトウェア開発用Webサーバ	・FWの内側と外側を接続する場合はしかるべき機関に申請し、所有者・設定・IPアドレスなどが管理できるようにする	(1)FWの内側と外側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を操作できるような構成のシステムをFWの内部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)手続きの必要性を理解していなかった (1-2)手続きがあることを知らなかった (1-3)無手続きであることを産総研側が気付けなかった (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)公開鍵暗号認証等を用いずに、ID・パスワードによるログインで利用可能にしていた (2-3)攻撃者からのアクセスに気付けなかった (3-1)FW外からFW内のマシンを操作可能にすることに対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	(1-1)知識不足・急いでいた・外部サーバに重要な情報は置かない認識だった・後で検討する予定だった？ (1-2)手続きに対しての知識不足・手続き自体の難易度煩雑さによる断念・手続きの強制力のなさ・手続きが書類だけで効力がない・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を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)逆向き接続以外の解決策がなかった (6-2)逆向き接続が最も容易な解決策だった
3	システム(内部)	使用電力量モニターサーバー	・個別のアクセスコントロールリストによりアクセス元 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)情報基盤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と外のアクセスを監視していていなかった (3)管理者パスワードの回答と「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)パスワードを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)	・アクセスコントロール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、契約における仕様書で定めている ・外部委託者には監査を行う決まりがある	(1)不正ログインされた (2)古いOSを使用しているサーバがあった (3)syslogサーバが当業者が管理している機器の管理パスワードの保管場所として利用されていた (4)syslogサーバに管理パスワードが平文で格納されていることを産総研側は、認識していなかった (5)管理方法・管理会社が異なるサーバがイントラ内部に存在している	(1-1)アクセスコントロールリストによるアクセス制限が行われていなかった (2-1)各サーバのソフトウェア状況の監視・更新が行われていなかった (2-2)ソフトウェア更新勧告を無視していた (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)現場がその運用だと判断していた？ (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)管理用ネットワーク内のLDAPサーバへの検索が行われ、全職員アカウントの記録を窃取された (2)認証サーバのログインIDと暗号化されたパスワードとハッシュ化されたパスワードを窃取された	(1)レコードを記録・持ち出すことができた (2-1)LDAPのログイン情報と認証サーバのログイン情報が同じレコードに保管されていた (2-2)ハッシュ化したパスワードがレコードに保管されていた	(1)持ち出す作業が日常的なので、持ち出せる設定・持ち出す前提の運用になっていた (2-1)LDAPID と 認証IDを同一テーブル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(ハッシュを暗号化パスワードと同じレコードに置いたのはなぜか)

付録5：表4.1.3-5 【CAST6】抽象的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	高位レベルの事象 (抽象的事象)	CAST6-1 安全上の責務(責任)	CAST6-2 非安全なコントロールアクション	CAST6-3 プロセス/メンタルモデルの欠陥	CAST6-4 意思決定された状況・背景
1	システム (外部)	メールシステムへの不正アクセス	・認証サーバでログインIDおよびパスワードの照合を行い、認証結果をユーザに返す。 ・パスワード認証されたログインIDは、メールおよび個人用フォルダ、共有フォルダの閲覧許可をする。 ・照合結果が一致しないユーザにはアクセス許可を与えない	・自動化された複数回のログイン試行に対して、正常に照合結果を返した。 ・不正なログイン情報で不正ログインされた。 ・同一ユーザIDのログイン試行失敗に対してロックアウトなどの処理を行わなかった。 ・システムに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。 ・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 ・サーバ所有者(産総研) は攻撃を受けた事実に対して何も対応をしなかった ・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.認証システム仕様の欠陥 (1-1)2段階認証になっていない。 (1-2)アクセス元に対し本人確認を行う仕組みがない (1-3)ログイン試行に対する制限がない。 (1-4)ログイン画面にてログインが成功した場合と失敗した場合で、結果に違いがない画面設計となっている。 (1-5)安易で推測されやすいパスワードが設定できる。 (1-6)ログインした際に本人への通知がない 2.ユーザのメンタルモデルの欠陥 (2-1)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 3.監視プロセスの欠陥 (3-1)異常検知機能が正常に動作していない。 (3-2)不審なパスワード試行は統合ネットワーク監視の対象に含まれていなかった (3-3)認証の成否をログに出力していない？ (3-4)攻撃の結果をすべて失敗と判断していた(実際は侵入＝ログイン成功している) (3-5)サーバ所有者は攻撃を受けたと報告が上がった調査・対応を指示しなかった	1.認証システム仕様欠陥の背景 (1-1)(1-2)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ことで、「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。 (1-1)(1-2)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VPN接続環境を外した (1-3)(1-4)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、EVSSL証明書の導入によって、認証サーバのログイン画面の真正性を見分けやすくすることで十分と判断した。 (1-5)「安易で推測されやすいパスワード」は設定時にチェックしエラーとていたが、」の「キー配置をなぞっただけのもの」はチェックエラー対象になっていなかった (1-6)正しいリクエスト情報(ID/パスワード)を送信してくるアクセス元は正しいユーザであると判断していた 2.ユーザのメンタルモデルの背景 (2-1)利便性。複雑なパスワードは使用しつらい。覚えにくい。システムがエラーとしないならＯＫという認識 3.監視プロセス欠陥の背景 (3-1)異常検知機能はそもそもあったのか不明 (3-2)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 (3-3)(3-4)運用上のログ解析が要求されるのは失敗(エラー)時であることからエラーログのみ出力(残す) する設計としていた、または大量のデバックログのみが出力されており、認証結果が埋もれていた (3-5)サーバ所有者は攻撃失敗＝ログインされていない＝システムへの被害はないと考えていた
2		内部ネットワークへの侵入	・ログインIDおよびパスワードの照合を行い、ユーザに認証結果を返す。 ・ソフトウェア開発の自動化をサポートするために、X研究サーバ内の仮想マシンを遠隔操作して任意のコマンド実行を行う。 ・FWの内側と外側を接続する場合はしかるべき機関に申請し、所有者・設定・IPアドレスなどを管理する。	・IPアドレスの全域に対してポートスキャンを実施された ・FW外側から内側のマシンを遠隔操作できた ・逆向き接続の設定を想定外の環境下で使用した ・FWの内側と外側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ため、サーバの存在が隠蔽された	1.システム構成の欠陥 (1-1)FW外からFW内のマシンを操作することを前提としたシステムを構築した (1-2)公開鍵暗号認証等を用いずにIDパスワードによるログインで利用可能とした。 (1-3)FW外のサーバに対する攻撃者からのアクセスに気付けなかった (1-4)FW内のサーバ上に配置されたマルウェアを検知する仕組みがなかった (1-5)本来の用途では想定していない環境で逆向き接続という設定を使用したこと 2.システム構築プロセスの欠陥 (2-1)手続きしなくてもシステムを構築することができる	1.システム構成決定の背景 (1-1)研究のために必要だった (1-2)インターネット上とはいえ研究のためだけに建てたサーバなので、研究所員のみがアクセスすると考えセキュリティについては考慮していなかった？ (1-3)インターネット上とはいえ研究のためだけに建てたサーバなので、研究所員のみがアクセスすると考えセキュリティについては考慮していなかった？ (1-4)FW内環境なのでそこまで監視しなくてもよいと考えていた？ (1-5)逆向き接続以外の解決策がなかった/最も容易な解決策だった/過去行ったことがあった 2.システム構築プロセス決定の背景 (2-1)手続きなしでも構築時に必要な情報・資材は全て揃っていたので構築できた
3	システム (内部)	内部システムへの不正ログイン	・アクセスコントロールリストによりアクセス元 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	・アクセス元IPアドレスを制限がされていなかったため、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 ・ID・パスワードを用いて不正ログインされ、リモートデスクトップを用いて遠隔操作。	1.NW構成の欠陥 (1-1)アクセスコントロールリストによる接続元IPアドレスの制限がされていない。 (1-2)研究用のネットワークと業務用ネットワークが切り離されていない。 (1-3)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構成となっている。 2.NW運用監視プロセスの欠陥 (2-1)管理ネットワークの内と外のアクセスを検知・監視していない 3.パスワード運用プロセスの欠陥 (3-1)管理者パスワードの複合に必要な「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.NW構成の欠陥の背景 (1-1)後から設置されたサーバで、その管理が情報基盤部とは別の組織で管理していたため、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。 (1-2)なぜこの構成にしたのか？(現時点では不明) (1-3)なぜこの構成にしたのか？(現時点では不明) 2.NW運用監視プロセス欠陥の背景 (2-1)そこを監視する運用・決まりになっていなかった？ (2-1)FW内なので監視要件が甘かった？ 3.パスワード配布プロセスの欠陥の背景 (3-1)そのやり方に危険性があると思っていなかった (3-2)一番簡単な方法だから (3-3)互いに存在を知っており、送信先さえあっていれば他者に漏れることはないと思っていた
4		内部システムのアクセス権昇格	・アクセスコントロールリストによりアクセス元 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	・外部委託業者のsyslogサーバにLDAP検索用のID/パスワードが平文で格納されていた(攻撃者はそれを読みとった) ・管理用ネットワーク内のLDAPサーバへの検索が行われ、全職員アカウントの記録を窃取された。 ・氏名、所属等の情報がある他、認証サーバのログインIDと暗号化されたパスワードとハッシュ化されたパスワードを窃取された。	1.NW構成の欠陥 (1-1)アクセス制限が施されてない。 (1-2)パスワードが安易なものが使われている。 (1-3)サポート期限切れの古いOSを用いており脆弱性修正パッチが未適用である。 (1-4)既知の脆弱性がある機器(NAS)を使用している 2.パスワード運用プロセスの欠陥 (2-1)LDAPサーバの検索用ID・パスワードが暗号化されずに保管されている。 (2-2)syslogサーバがという別用途のサーバが管理パスワードの保管場所として利用されている (2-3)多くの人は正規の作業用ファイルサーバにて管理されているものと認識していた 3.認証情報データ構成の欠陥 (3-1)ハッシュ化したパスワードがあるのに暗号化したパスワードをレコードに持っていた	1.NW構成の欠陥の背景 (1-1)FW内環境なのでそこまで考慮しなくてよいと考えていた？ (1-2)FW内環境なのでそこまで考慮しなくてよいと考えていた/業務上1ロールに対し複数の人間で使用していたためわかりやすいパスワードにした (1-3)セキュリティリスクが極めて大きいのを把握していたが、対処できていなかった。 (1-3)FW内環境なので、特に急ぎで対応する必要性を感じていなかった (1-4)FW内環境なので、特に急ぎで対応する必要性を感じていなかった 2.パスワード運用プロセス欠陥の背景 (2-1)使用頻度が高いため、アクセスしやすい場所にコピペできる形で保管した？ (2-2)ログ解析のため各機器、サーバへアクセスすることから作業時にアクセスしやすい箇所に保管した？ (2-3)限られた作業者が現場の暗黙の了解で行っていた（本来の運用から外れていることは認識していたことから上長、組織には報告していなかった） 3.認証情報データ構成欠陥の背景 (3-1)当初暗号化で運用されており、仕様変更でハッシュ化を使用するようになったため暗号化カラムが残った？ (3-2)ハッシュ値と暗号化した値を両方使用する処理や機能があるので両方必要だった？ (3-3)ハッシュ化した値があるのに、なぜ暗号化カラムを残したのか不明

付録6：表4.1.3-6【CAST7.8】システムの俯瞰分析 （一部抜粋）

●： 直接的な要因、◎：直接的な要因から影響すると思う要因

							システム/運用					セキュリティマネジメント			CAST7-1				CAST8
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	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	内部システムへのログイン制御	内部システムのアクセス権昇格	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、組織のルール、不測事態の連携不備など	安全な情報システム ＝ルール、学習、リスク検知などの整備不備	安全なマネジメントシステムの設計 ＝ルールの逸脱、教訓活かせない、改善／変更時の不備など	安全な文化 ＝風土、思い込み、軽視など	経時的な変化とダイナミクス ＝ルールの形骸化、長期間にわたる変更による不備など
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が行われた	CAST4	-----	UCA	パスワードポリシー	パスワード連絡の不備			◎	◎	◎	●				●	◎			
3	定常的に通信監視結果を確認/報告する仕組みはあったのか？	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はあったのか？	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、形式的なとアリングや一般的な脆弱性診断に留まっており、	CAST4	-----	UCA	セキュリティ体制	運用の不備		◎				●		●			◎	◎	●
13	定常的にポートスキャンがないか確認/報告する仕組みはあったのか？	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はあったのか？	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リスクチェック、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	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	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カーを導入したが、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	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3の影響を	CAST4	-----	意思決定の背景	ログイン	ログイン認証の強度不足	●		◎			◎		◎		◎		●	
40	当該認証サーバーでは、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	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容していた	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御がなかった	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	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(アクセス権昇格)	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ていない。	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える** **－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》** 産総研のセキュアな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、その処理に必要となる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得る**	**●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

付録8：表4.3-1　報告書とCAST分析から新たな改善案との比較

被害を発生・拡大させた要因（本文と連動）	再発防止のための対策(産総研の報告内容) 7.1. 現時点で措置済の対策	再発防止のための対策(産総研の報告内容) 7.2. 今後取り組む抜本的対策	CAST分析で新たに導きだした改善案	CS図
6.1. システム・機器の問題				
6.1.1 メールシステムのログイン方法	○外部からはVPN 接続を必須とする運用とし、さらに、内部ネットワークから口グインする場合でも、一定期間ごとに二段階認証を求めるよう認証方式を強化した。	(同左)　※高度標的型攻撃	**●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	
6.1.2 内部サーバと連携していた外部サイト	○用途と通信先を精査し、必要性と安全が確認できないサーバ等は全て遮断した。	**7.2.2 運用の見直し強化** ○外部接続に際しては、ネットワーク構成、管理者の知識・能力、管理体制等について専門家による厳格な審査を行い、十分なセキュリティ対策が講じられていることを確認する。	**●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 **●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》 産総研のセキュアな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、その処理に必要となる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	
6.1.3 広域でフラットな内部ネットワーク	○全てのサーバにアクセス権限を設定するとともに、分離用のネットワーク機器を新たに追加し、これによって業務用ネットワークを研究用ネットワークから切り離した。	**7.2.1 システムの強化策** ○多要素認証等の強固な認証技術を、内部システムのうちイントラ基盤システム等の重要なシステムにも導入し、破られにくく、かつ攻撃が検知可能な認証システムを導入する。 ○研究用ネットワークをセグメント分離できるネットワークを構築する。さらに、セグメント間の通信を制御できるようネットワーク構成を抜本的に見直す。	-----	
6.1.4 内部ネットワークの不十分な監視	○既に導入していた統合ネットワーク監視におけるSIEM の自動検知ルールを見直し、不正な通信が内部で発生した場合にもすぐに検知できるよう、内部通信の監視を強化した。	**7.2.1 システムの強化策** ○侵入や拡散の即時検知のため、内外を通過するファイアウォールの監視、セグメント間の内部通信監視を導入する。 ○重要システムにおいては、必要十分なログを蓄積し、不正なアクセスの分析・解析ができるシステムを導入する。また、侵入時にログ等の証跡が消去されないよう、ログの冗長化や遠隔保存等の仕組みを導入する。	-----	
6.1.5 アクセス制限のなかった管理用ネットワークのサーバの存在	(同6.1.3)	(同6.1.3)	●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	
6.1.6 情報機器の脆弱性	○使用を中止し、研究部門から回収した。	**7.2.2 運用の見直し強化** ○エンドポイント監視が効果を上げない機器（研究用の Linux 機器、NAS 等）については、機器の選定方法のガイドライン、監視方法を見直す。 ○情報機器の脆弱性情報の所内徹底を図るとともに、固定IP の運用ルールの見直しを行う。	-----	
6.2. パスワード・暗号鍵の管理と強度の問題	○有効なパスワードの設定方法、管理方法を検討し、情報基盤部で運用開始するとともに、外部委託業者に周知・徹底した。	**7.2.2 運用の見直し強化** ○有効なパスワードの設定方法、管理方法について改めて検討し、産総研の情報セキュリティ実施要領及び情報セキュリティ実施ガイドに反映させるとともに、職員、外部委託業者に周知・徹底する。	● 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	
6.3. 外部委託業者の管理の問題	○老朽サーバは廃止し、最新のOS を載せた新規のサーバに交換した。	**7.2.3 外部委託の運用改善** ○応札業者を限定し、同一業者による長期的・慣行的運用の一因となった可能性 ○一般競争入札について、最低価格落札方式から総合評価落札方式への切り替え ○委託先の選定基準マニュアルと、外部委託業者向けの情報セキュリティ対策チェックリストを作成し、情報セキュリティ対策の履行状況の確認等を定期的に行う。 ○外部委託業者に対して、情報セキュリティ監査を行うことを検討する。	-----	
6.4. マネジメントの課題				
組織・体制上の課題	対策なし	**7.2.2 運用の見直し強化** ○研究活動の実態を踏まえつつ、研究用サーバ管理ルール、重要情報の管理ルールの見直しを行う。 ○全体システムについて、より実効性・継続性のある情報セキュリティ監査を行う。また、ISMS（情報セキュリティマネジメントシステム）の認証取得を検討する。　※具体的な施策がない **7.2.4 組織体制の見直し** ○CISO を長とし、情報セキュリティのリスク認識に基づく情報セキュリティマネジメントシステムを構築し、PDCA サイクルを回すとともに、必要に応じてマネジメント体制の見直しを行う。 ○情報セキュリティ委員会の位置づけを理事長の直下に格上げし、当該委員会を通して、情報セキュリティ対策に関する理事長のトップマネジメントがより強く働くよう体制を見直す。 ○所外の情報セキュリティの専門家を、最高情報セキュリティアドバイザーとして委嘱することを検討する。 ○情報セキュリティ対策部署は、外部の情報セキュリティ機関との連携を一層深め、常に最新の情報を交換するとともに、それらの情報を適時適切に関連部門に提供する。 ○CSIRT 対応のためシステム運用管理部門、部門セキュリティチームから構成する	**●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。 **●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 **●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	
研究部門内での情報セキュリティの徹底	対策なし	**7.2.4 組織体制の見直し** ○システムの調達・管理、情報セキュリティ対策に関する十分な知見を有する者を配置する。 ○情報セキュリティ対策部署の責任者には、所内の各部門長との十分な調整ができるよう、必要な権限を付与する ○部門セキュリティチームを設置する ○外部の情報セキュリティ機関との連携を一層深め、常に最新の情報を交換するとともに、それらの情報を適時適切に関連部門に提供する。 ○研究部門の情報セキュリティ対策状況を、定期的に情報セキュリティ対策部署へ報告する仕組みを 導入する。 ○研究部門長の情報セキュリティ責任者としてのマネジメント向上のため、研究部門長研修（毎年実施）に、情報セキュリティに関する項目を追加する。 ○部門セキュリティチームは、情報セキュリティ対策部署及び CSIRT と連携し、セキュリティ対策に関する最新の情報交換等を行う		
重要情報の管理についてのポリシーと体制	対策なし	対策なし		
研究部門への情報セキュリティ監	対策なし	対策なし		
重大なインシデント事案が発生した際の体制	対策なし	**7.2.4 組織体制の見直し** CISO の下に、情報セキュリティ対策部署を明確に位置づけ、不正なアクセスへの対策の強化を図るとともに、インシデントに対する機動性を確保する。 **7.2.5 事業継続計画（BCP）の見直し** ○情報セキュリティインシデントの深刻度に応じた事業継続計画（Business Continuity Plan）及び緊急時対応計画（Business Contingency Plan）の立案をする。 ○インシデント発生時に十分な対応を行えるように外部委託業者等との契約を見直す。 ○重要なシステムへのサイバー攻撃に対する、継続性（Continuity）と危機対応（Contingency）のための訓練を実施する		

付録9：図4.2.3-1　FRAM手順2（各コンポーネントの抽象化）

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

〇本人認証機能
- ←・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）

〇産業研・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

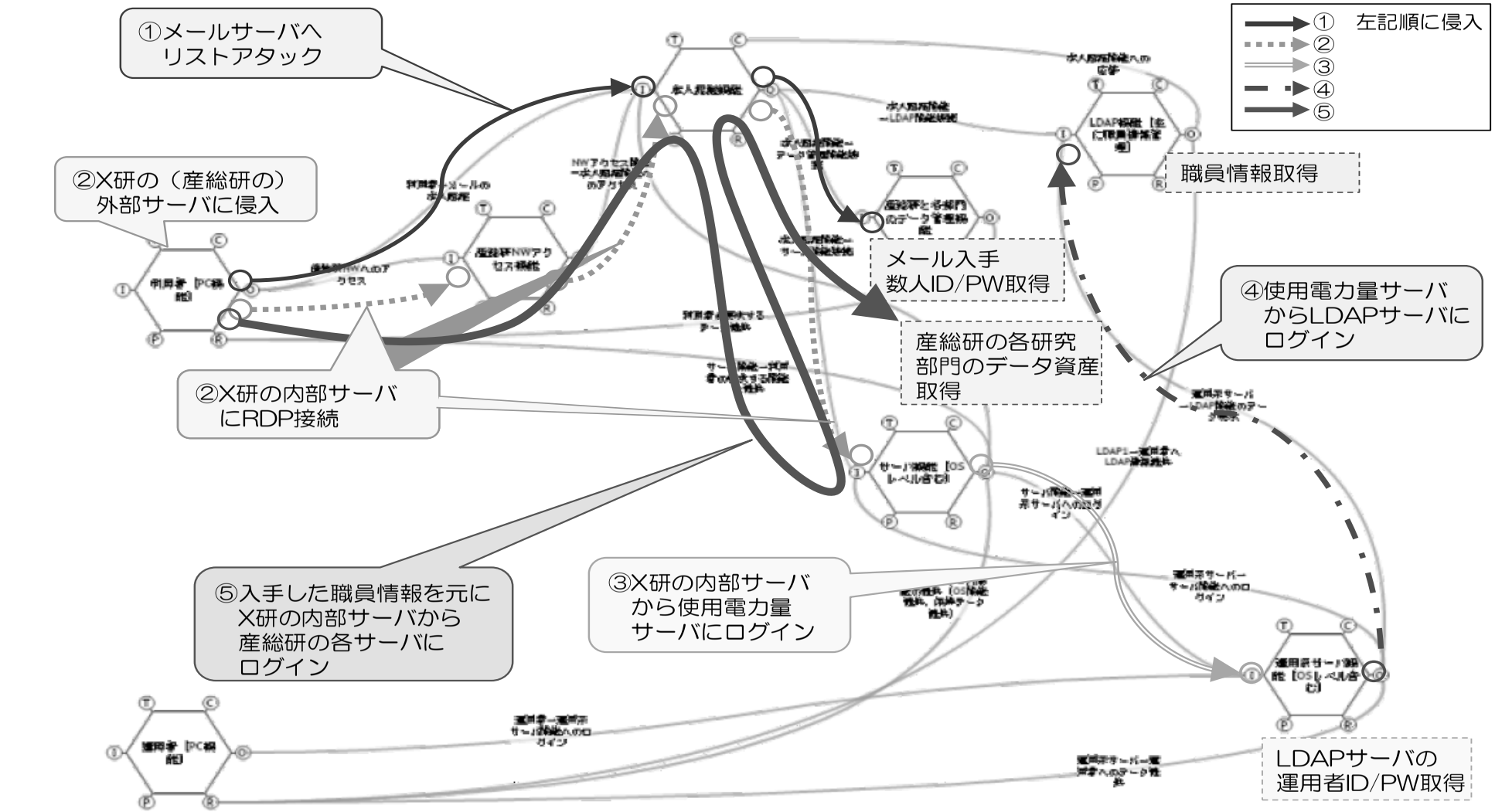
〇産業研NWアクセス機能：　利用者の端末を論理的に業務システムや各研究部門のサーバにアクセス可否を提供
- ←・インタネットからの職員のVPN接続機能：　職員がインタネットからﾘﾓｰﾄｱｸｾｽ（ﾜﾝﾀｲﾌﾟﾑﾊﾟｽﾜｰﾄﾞ）提供
- ・外部サイト～各研究部門サーバ接続間のFW機能：外部接続用FW
- ・産業研内のローカルLANの接続機能：　産業研内のスイッチHUBやWiFi、等

〇サーバ機能（OS含む）：
- ←・各研究部門のサーバ：

〇利用者（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

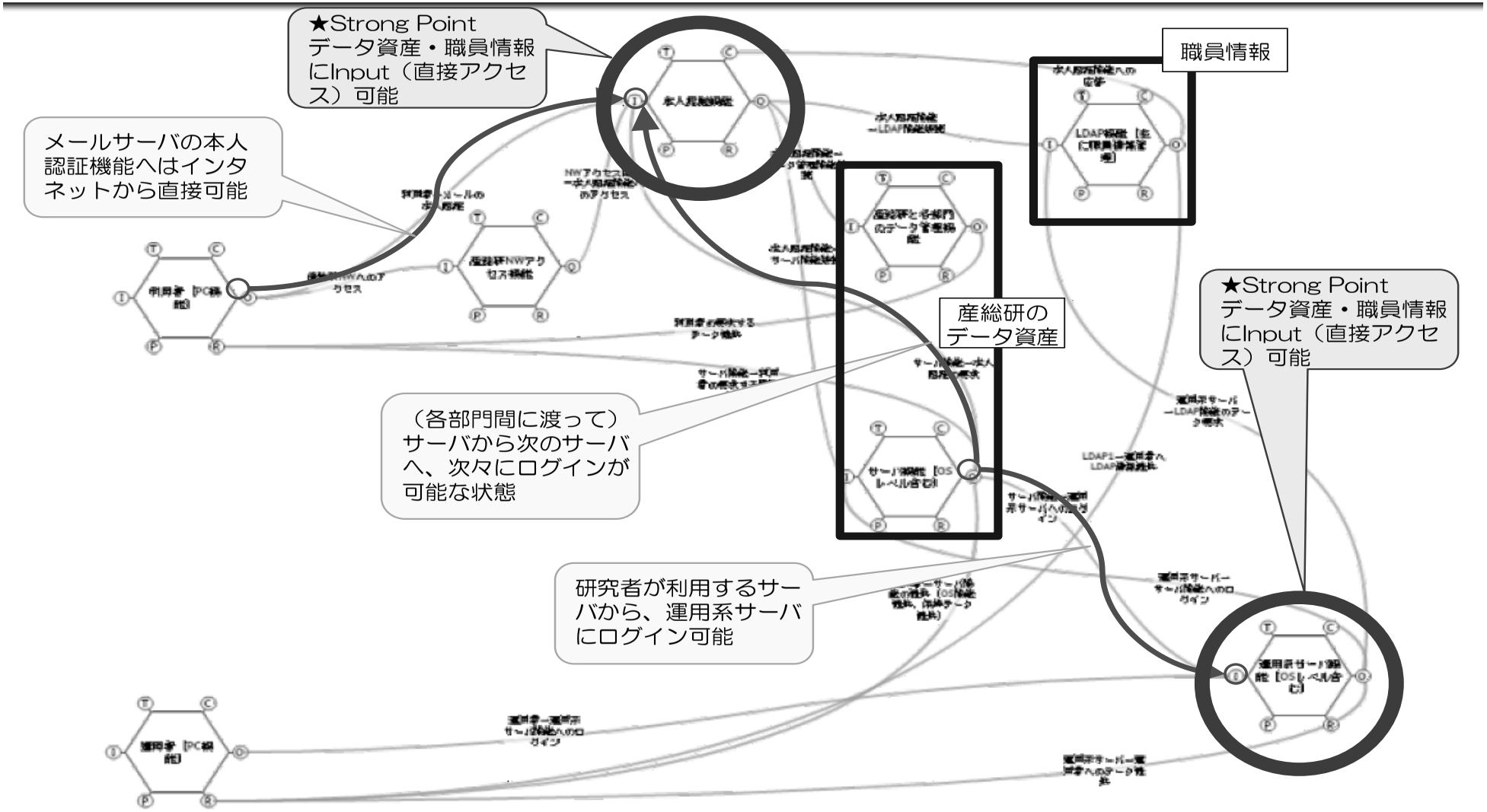
付録10：図4.2.3-2 FRAM手順3（モデルの可視化）と手順4（攻撃経路のシミュレート）

FRAM_手順3（モデルの可視化）と手順４（攻撃経路のシミュレート）



付録11：図4.2.3-3 FRAM手順4（攻撃が成功した要因分析）

FRAM_手順４（攻撃が成功した要因分析）



付録12：図4.2.3-4 FRAM手順5（対策案の創出）

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

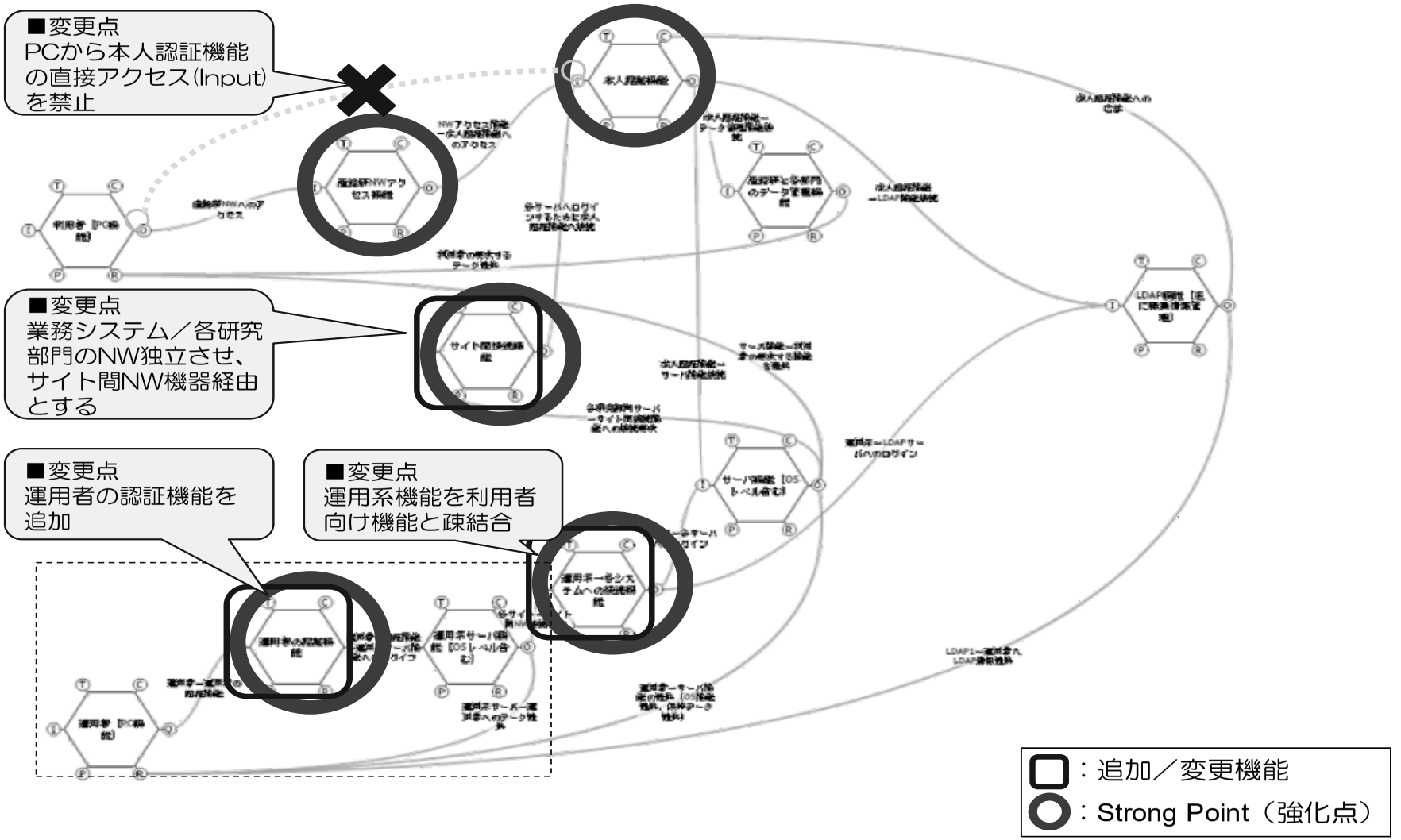
■上記対策でも攻撃を防げないケース
改善を実施しても対応できない場合が存在する
①ID／PWが既に出回っている場合
②職員等の利用者のPCに侵入されている場合
どちらも、産業研の各システム（各研究部門のサーバも含む）は、「本人認証が正しく機能すれば、その人の権限に基づいた情報資産にアクセスできる」というポリシーで設計しているからである。別の表現を用いると、「本人認証が正しいが、不正アクセスされている可能性の検討が抜けている」
⇒①の対策
- PWの全変更。その後の定期的なPW変更　→人系の処理なので、いずれ同じPWに戻る可能性が高い
- 生体認証、ワンタイムトークン、等の多要素認証の導入　→コスト増、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
〇不正アクセスを「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」と結ぶ

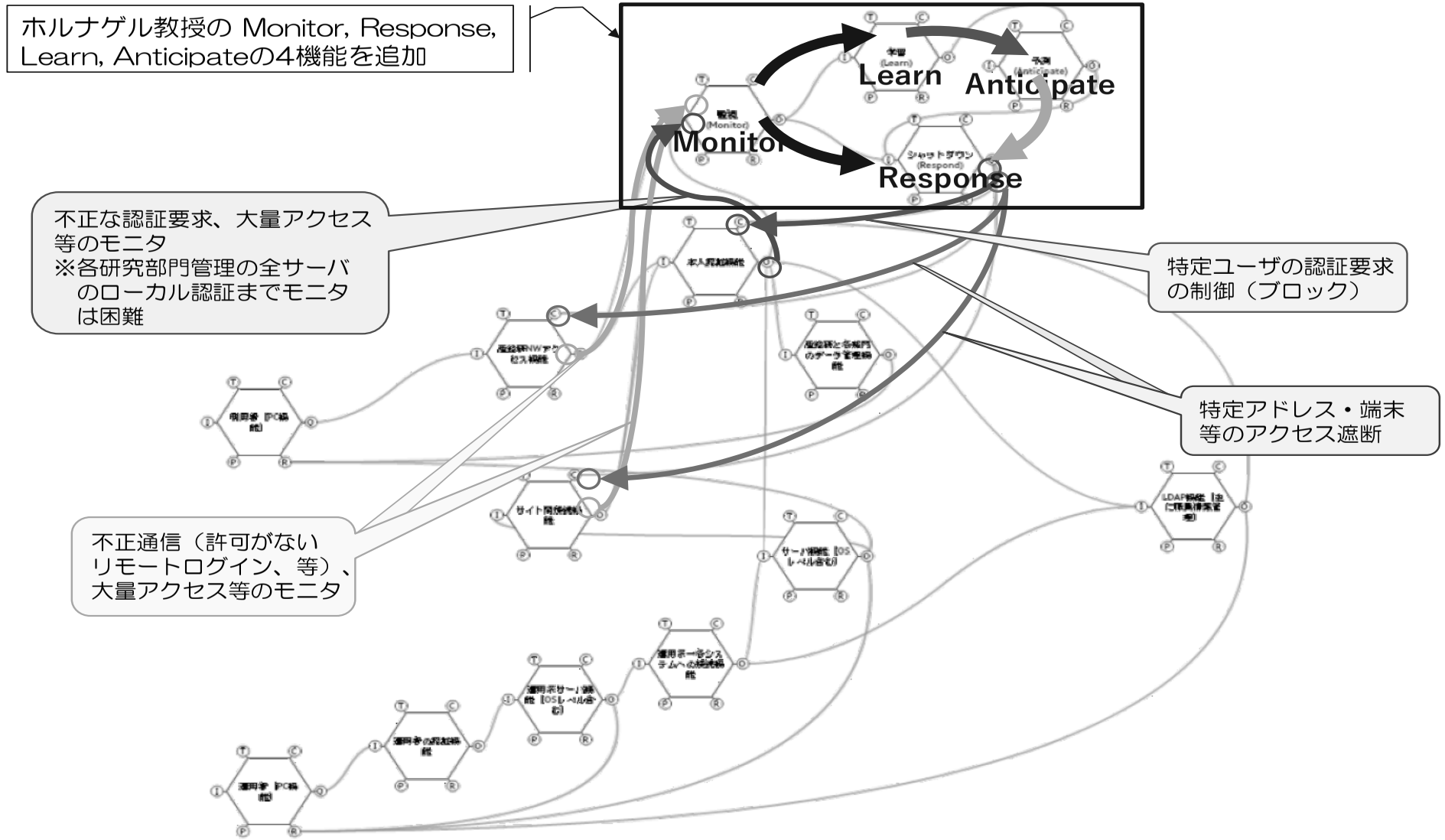
付録13：図4.2.3-5 FRAM手順5（対策案を講じたモデルの再可視化）

FRAM_手順５（対策案を講じたモデルの再可視化）



付録14：図4.2.3-6 FRAM手順5（対策案にHollnagel教授考案の4つの能力の追加）

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変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	-