情報セキュリティ機器調達支援ツール
(SRAS：Security Requirement Aid System)
利用の手引き

2009年7月1日

調達におけるセキュリティ要件研究会

独立行政法人　情報処理推進機構　セキュリティセンター

はじめに

本システムはセキュア・ジャパン２００７に書かれている、政府組織および自治体のセキュリティ要件やセキュリティソリューションを検討を支援するために、平成19年度独立行政法人　情報処理推進機構セキュリティセンター（以下、「IPA」と云う。）に設置された「調達におけるセキュリティ要件研究会」（苗村憲司委員長）が開発したセキュリティ要件の検討のための支援ツールです。

本システムは、IPAセキュリティセンターが提供するセキュリティ情報サービスシステム（「Security　Ipedia」と云う。）の機能の一環で、情報システムのセキュリティ要件を検討する機能を提供します。

目次

1. 本システム利用について

(1) 利用の目的

① 本システムは政府統一基準(NISC)、地方公共団体におけるセキュリティガイド(総務省)を用いて、必要な情報システムのセキュリティ要件を検討するツールとして利用することが出来ます。

② 本システムの利用には、まず情報システムの大まかなネットワーク構成とそのシステム構成要素が必要です。 本システムは、検討対象のネットワーク構成と構成要素から、情報システムの構成要素のセキュリティ要件の候補が導出されますので、それを基に、必要なセキュリティ要件を検討する支援ツールとして利用することが出来ます。

③ 本システムは、構成要素のセキュリティ要件を満足するための、機器毎のソリューションおよび、関係するISO/IEC15408認証製品の候補が表示されます。

本システムを利用することで、必要なセキュリティ要件を満足するIT機器等の情報が入手できますから、調達の際など様々なセキュリティ検討の支援ツールとして利用することが出来ます。

1. 本システム利用について

(2) 利用の内容

本システムを利用して以下の検討ができます。

① 必要なセキュリティ要件の検討

・ネットワーク構成、主要な構成要素を入力することで、必要なセキュリティ要件の検討が行える。

② 関係するセキュリティ技術の検討

・主要な構成要素に関係する必要なセキュリティ要件を満足するセキュリティ技術の検討が行える。

③ システム構成要素に関係する最新のセキュリティ情報の検討

・セキュリティに関係するRSS情報を収集する「セキュリティRSSポータルシステム」と連携することで、検討対象の情報システムに関係する最新の脆弱性情報、セキュリティ事故等の最新のセキュリティ情報を参照することが出来る。

④ 必要なセキュリティ技術を提供するISO/IEC15408認証製品情報の入手

・CC認証製品の情報を掲載した「CCRAポータル」に、必要なセキュリティ要件を満足するソリューションをリンクして、関係するCC認証製品の情報の参照が行える。

2. 利用者に関して

(1) 利用者の検討対象

1) セキュリティ要件の検討　：【設計者】

2) セキュリティ要件を満足する機器の調達の検討　：【調達者】

3) 関係する最新のセキュリティ情報の参照　：【設計者、運用管理者】

(2) 利用者のスキルに関して

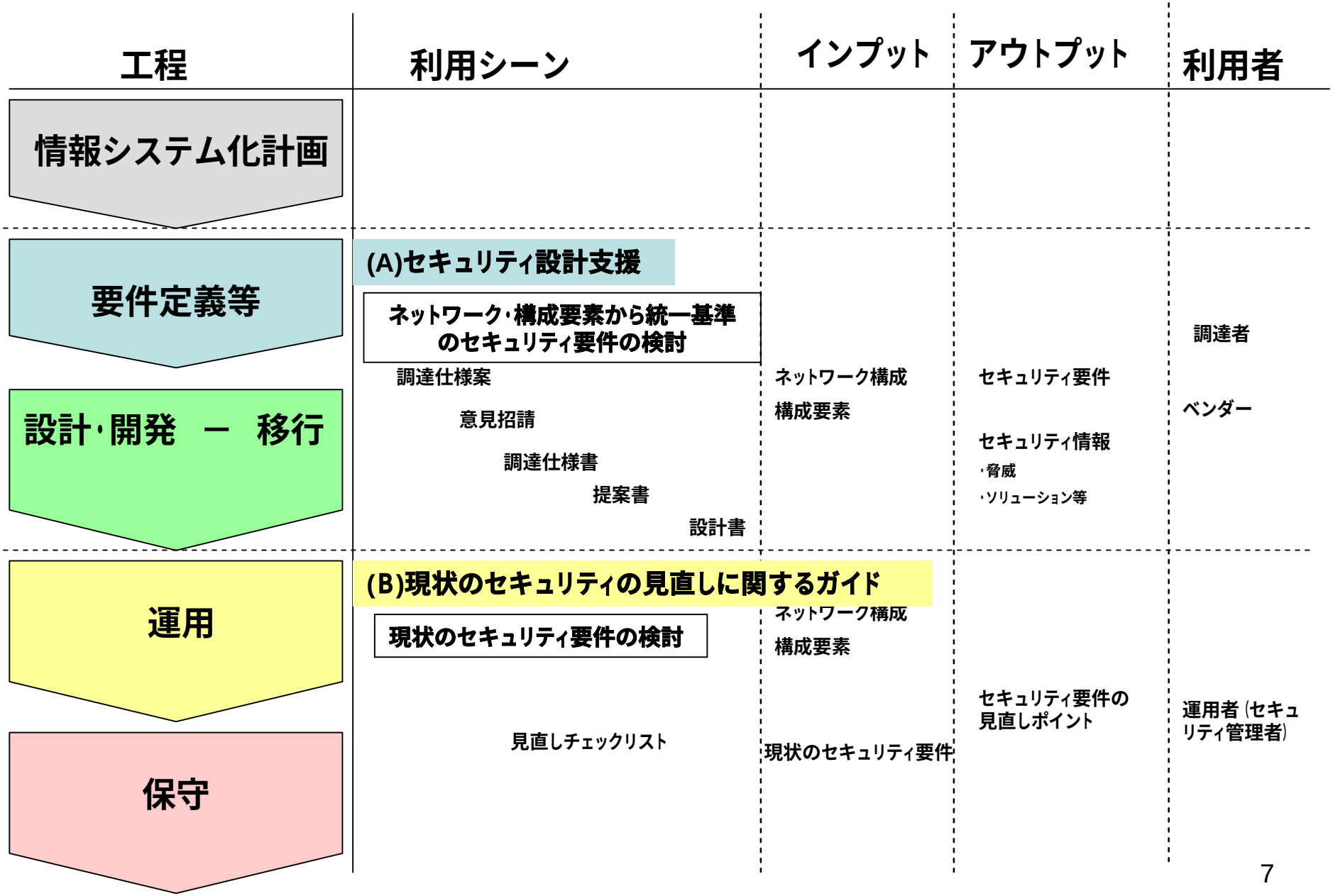
本システムを正しく利用するためには、出力結果の適切な解釈と判断が必要となるので、以下の知識を持つ者が、最終的な解釈と判断を行う必要があります。

1) ITセキュリティマネージメントに関する基礎的な知識。

2) セキュリティソリューションに関する基礎的な知識。

3) ネットワークに関する基礎的な知識。

SRASの利用者について



3. 利用に関しての注意事項

本システムは、セキュリティ要件の自動作成システムではなく、セキュリティ要件に関する情報を提供して、利用者がセキュリティ要件検討を行う際の検討の支援を行うものです。

従って、利用者は、最終的には出力結果を参考に、セキュリティ要件、調達要件を詳細に検討する必要があります。

特に、本システムの利用に関して、利用者が自由に利用していただきIPAでは何ら制約を設けませんが、その利用の責任および対処は、利用者に帰することと致します。

4．SRASシステムの概要について

(1月8日版)

検討は、環境（セキュリティポリシー、対象システム）とライフサイクルの検討フェーズを入力する。

【ライフサイクルの選択】

共通

導入　運用　廃棄/（更新）

【参照するセキュリティポリシーの選択】

政府統一基準

地方セキュリティガイドライン

NIST　SP800-53

ISO/IEC 27001

ローカライズ

【検討対象情報入力システム入力】

（参照するネットワークモデル）

政府機関ネットワークモデル

・構成要素は「統一基準」による

自治体ネットワークモデル

・構成要素は「地域公共ネットワークに係る標準仕様（総務省）」による

保護すべき情報資産

【リスク分析】

（セグメント毎の想定されるリスクを選択）

セキュリティ要件の検討

保存

読込

保存

個別領域

共有領域

検討結果は、機器毎にセキュリティ要件と関連するセキュリティ情報を出力する。

関連するセキュリティ情報の参照

脅威　ソリューション

関連する最新情報（RSS情報）　関連認証製品情報

5．利用ガイド

（1）．利用者登録

IPAセキュリティセンターSecurity　iPedia　SRAS登録画面より、利用者の登録を行い
ユーザIDと仮パスワードを入手します。

（2）．検討対象情報システムの準備

1）検討目的を明確にする。（例えば、セキュリティ要件の検討、改造によるセキュリティ要件の検討等）

2）検討対象の情報システムの主要な構成要素を整理したネットワーク構成図を準備する。

3）検討対象の情報システムの機能の概要を整理する。

4）検討に当たっての前提条件、主要な脅威を整理する。

（3）．検討条件の入力

1）検討するセキュリティポリシーを選択する。

2）（2）で整理した検討対象のネットワーク構成図を基に、SRASに入力を行う。

3）（2）で整理した前提条件、主要な脅威からリスク分析条件を入力する。

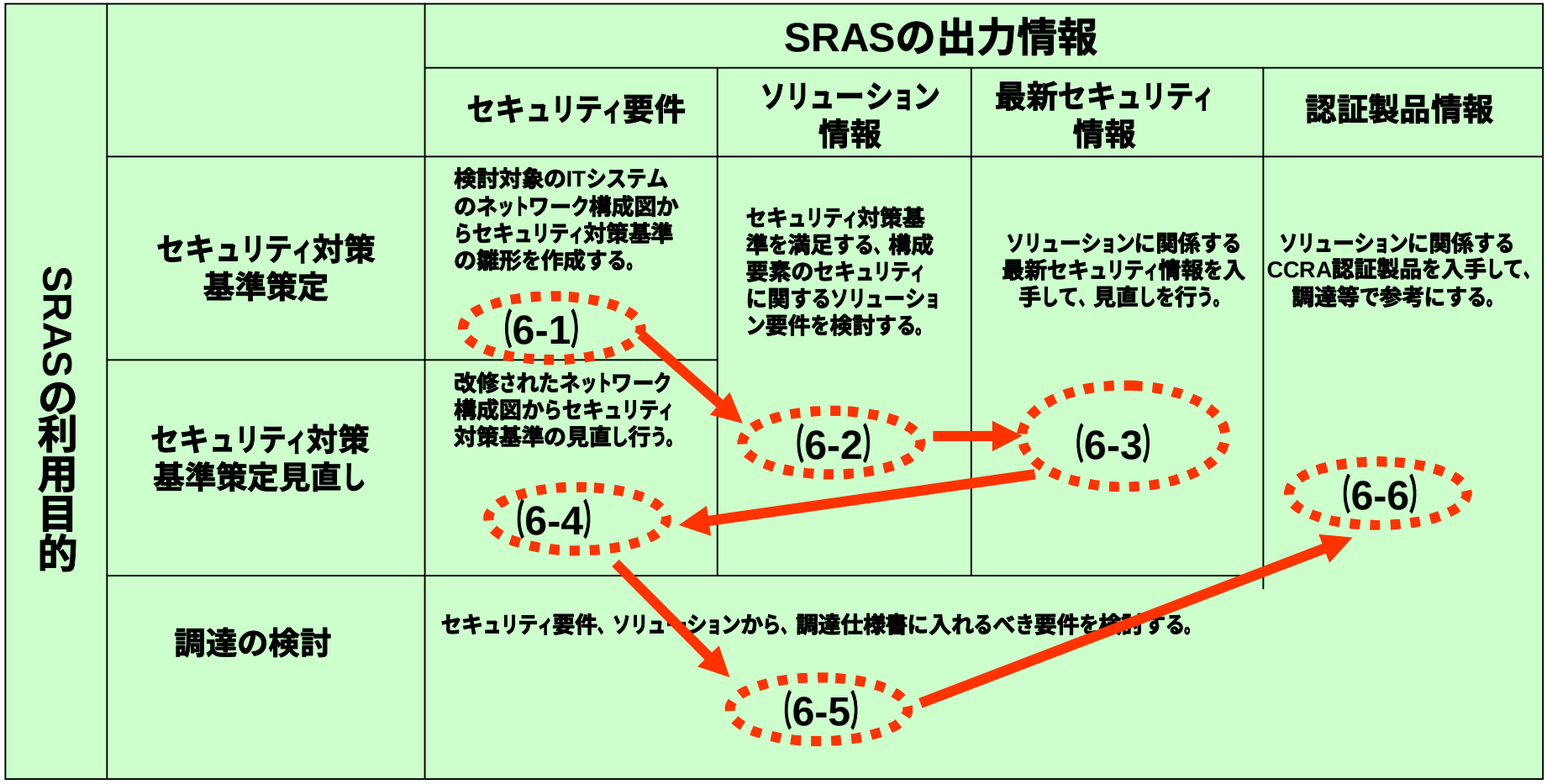
（4）．出力結果の検討と判断

1）セキュリティ要件の出力結果を検討して、対象システムのセキュリティ要件として適切かどうか判断して最終結果をまとめる。

2）ソリューション、脅威、脆弱性及びCCRA認証製品の情報を参照して活用する。

6．利用例

本章ではSRASを利用したセキュリティの検討例を示します。



6-1.　セキュリティ要件の検討を行う場合の例

1）. 目的

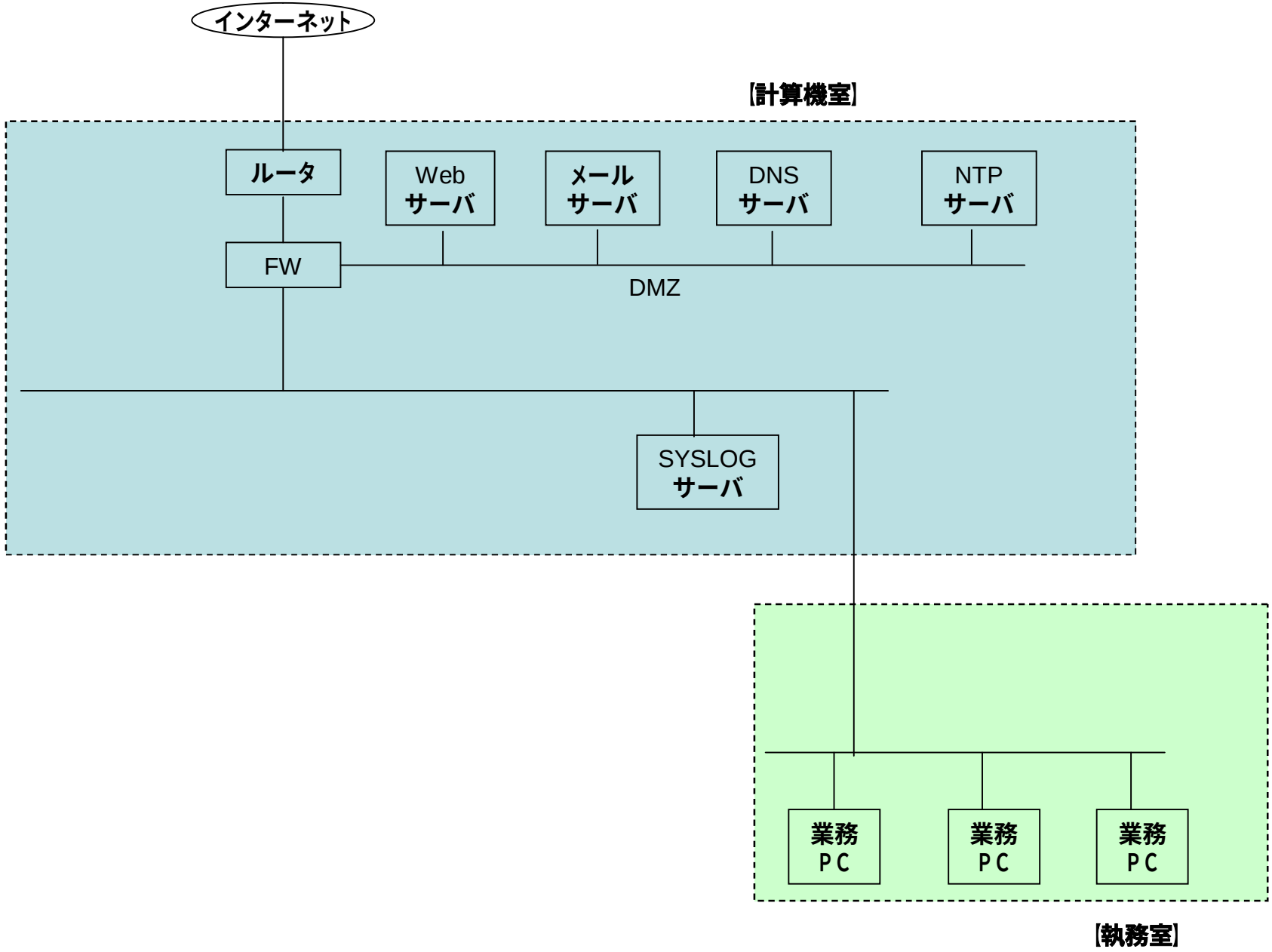
情報システムに必要なセキュリティ対策基準のセキュリティ要件を新たに定めるために、使用する。

2）. 検討に必要な情報

⇒ ネットワーク構成図

検討対象の情報システムの主要な構成要素が記載されたネットワーク構成図を作成する。

検討対象の情報システムのネットワーク構成図



3)．検討対象の情報システム概要の整理

本システムは、○○県庁が、県民にホームページを介して必要な情報提供を行うための、情報提供システムである。

① コンテンツの作成及び公開

広報課の担当職員は情報提供のためのコンテンツを作成するために、ＤＭＺに設置されたWebサーバの公開前コンテンツ作業領域に公開前コンテンツを作成する。

公開前のコンテンツは機密性2（内部情報）として、関係者がメールサーバ上のメーリングリストで審査する。

メーリングリストの情報は機密性2として、非公開とする。

県民や外部からの情報および意見等を収集するために、ホームページに掲載された問合せメールアドレスで受け付ける。

受付けた情報は機密性2として格付けする。

コンテンツの内容の承認は、広報課長が行い、承認後のコンテンツは機密性1、可用性2として、DMZ上に設置されたWebサーバの公開コンテンツ領域にコピーする。

DMZ上の公開Webサーバ、メールサーバ、NTPサーバのアドレス問合せのために、DMZ上にDNSサーバを設置する。アドレス情報は可用性2情報とする。

② 職員へのインターネット利用環境提供

職員は職員間の情報交換をメールサーバで行う。メールの内部情報は機密性2とする。

職員は、コンテンツ作成及び情報収集のために外部のホームページを参照する。

③ セキュリティ対策

ルータ、FWで不要パケットのフィルタリングを行い不正アクセスを防ぐ。ルーティングテーブル、FWのフィルターリングテーブルの情報は可用性2、機密性2であり要保護情報とする。

不正アクセス、システム障害の監視のためにSYSLOGサーバを内部セグメントに設ける。ＬＯＧ情報は可用性2情報とする。

LOGデータの時間的整合を実現するために、NTPサーバをDMZ上に設け、ルータ、FW、Webサーバ、メールサーバ、Proxyサーバの時間同期を行う。

4）. 検討に当たっての前提条件、主要な脅威の抽出例

3）システム概要から前提条件、主要な脅威を抽出する。

①前提条件

ⅰ）ルータ、FW各種サーバは、身分証明書のIDｶｰﾄﾞと入室許可者に知らされたパスワード入力による入室制限が行われた計算機室内に設置される。

ⅱ）サーバへのアクセスは、職員のみとする。

ⅲ）業務ＰＣは、入室制限がない執務室に置かれる。

ⅳ）業務ＰＣの使用は、職員のみとする。

ⅴ）職員は不正行為を行わない。但し誤操作等はあるものとする。

②主要な脅威

ⅰ）外部からの脅威

a） HP公開情報の改ざん　b） 公開前HPコンテンツの改ざん、盗み見

c） 外部の攻撃者によるDos攻撃によるシステム使用障害　（Webサーバ、メールサーバ）

c） メール、Webからのサーバ、業務PCへのウイルス感染

ⅱ）内部からの脅威

a） 職員以外の業務PC使用による公開前HPコンテンツの改ざん、盗み見

b） 職員の誤操作による公開前HP情報の誤消去

c） 職員の誤操作によるルータ、FW、サーバの情報の誤入力、誤消去

d） ＦＤ、ＵＳＢ等を介して業務端末からのウイルス感染

5）. SRAS入力のための条件の整理

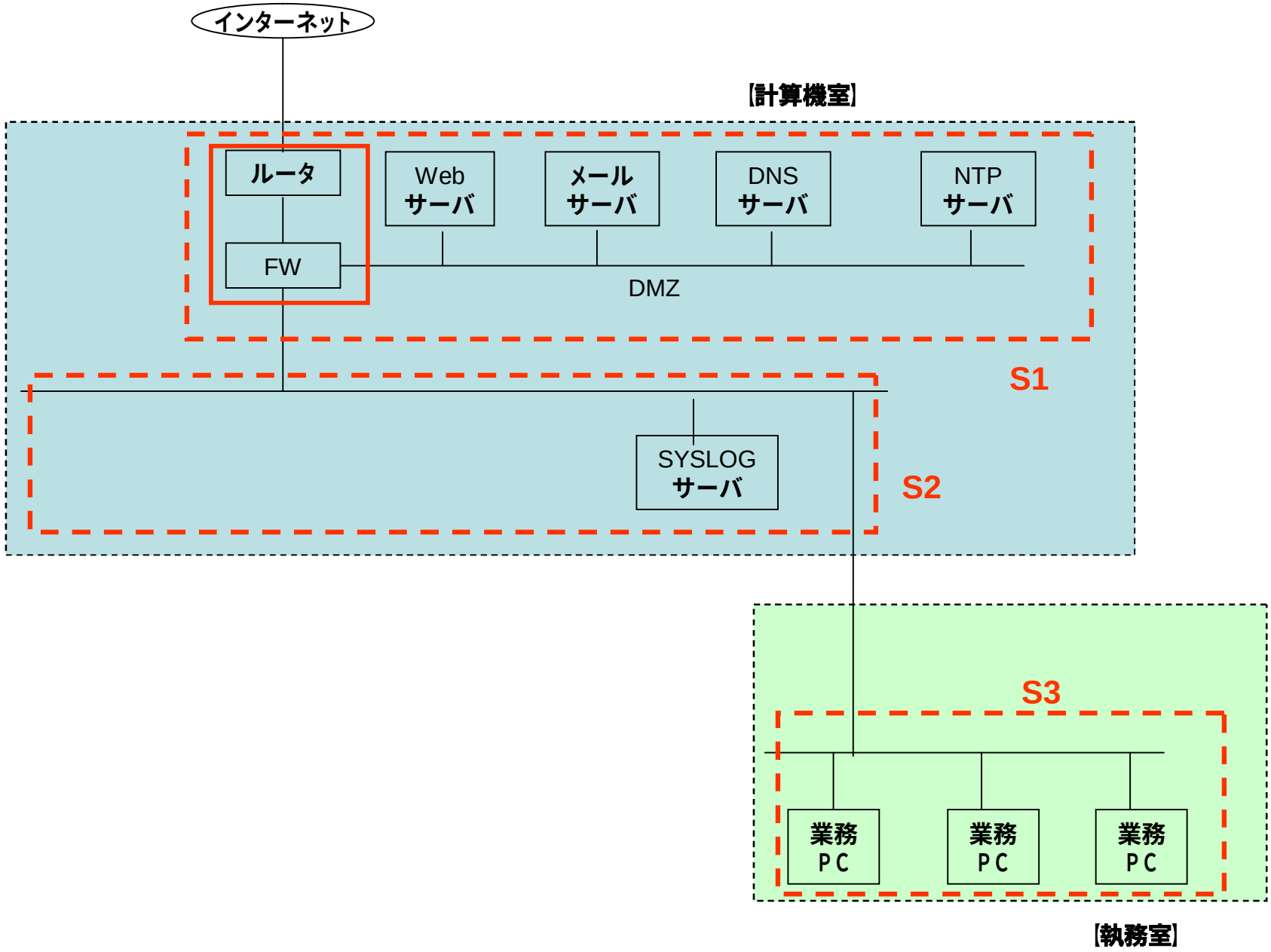
①. セキュリティポリシー　　地方公共団体における情報セキュリティポリシーに関するガイドライン

②. ネットワーク構成　　地方自治体

③. 構成要素

設置箇所	検討対象ITシステム	情報資産	SRAS入力		
	構成要素		選択SG	構成要素	情報格付け
計算機室	通信回線	通信データ	S1	通信回線	要保護情報
	ルータ	ルーティングテーブル		通信回線装置	要保護情報
	FW	フィルタリングテーブル			
	Webサーバ	公開前、公開コンテンツ		Webサーバ	要保護情報
	メールサーバ	メール		メールサーバ	要保護情報
	DNSサーバ	アドレステーブル		DNSサーバ	要保護情報
	NTPサーバ	同期時間データ		各種サーバ	要保護情報
	通信回線（内部LAN）	通信データ	S2	通信回線	要保護情報
	SYSLOGサーバ	LOGデータ		各種サーバ	要保護情報
執務室	通信回線（内部LAN）	通信データ	S3	通信回線	要保護情報
	業務PC			業務用PC	

④SRAS入力のためのセグメント分割



⑤リスク入力に関して

前提条件及び主要な脅威からセグメントに関係ない脅威を除く。

例えば、入室制限のある計算機室内のセグメント（S1，S2）の構成要素は、破壊、盗難等のリスクは存在しない等で以下のリスクを除く。

執務室へは職員以外も入室可能なので破壊、盗難等の脅威は存在する。

	除去リスク
S1，S2	盗聴
	破壊
	盗難
	窃取
	装置・機器等の損傷
	端末等の故障
	アクセスポイントの不正接続
S3	アクセスポイントの不正接続

⑥詳細のセキュリティ要件の選択に関して

システム概要、前提条件及び主要な脅威から必要なセキュリティ要件の選択を行う。

例えば、今回のSRASの利用の視点で不要なセキュリティ要件を外したり、必要なセキュリティ要件の追加を行う。

6-2. ソリューションの検討

詳細検討により選択されたセキュリティ要件に対応するソリューションが表示されるので、機器毎のセキュリティに関係するソリューションの選択を行う。また、追加が必要な要件のソリューションがあれば追加する。

6-1. の選択されたセキュリティ要件を実現するソリューションを以下に示す。

S1の通信回線

アクセス監視･制御
　通信回線利用監視･制御
　　ネットワーク型IDS／IPS
証跡管理
　ログ収集管理
システム動作の保全管理
　システム性能監視
通信回線の保全管理
　トラフィック監視

S1の通信回線装置

アクセス監視･制御
　通信回線利用監視･制御
　　ファイアーウォール
証跡管理
　ログ収集管理
システム動作の保全管理
　システム性能監視
　システム冗長化
　時刻同期
　バックアップ／リストア
　改ざん検知
通信回線の保全管理
　QOS制御
　トラフィック監視

S1のDNSサーバ

主体認証
　ID／パスワード認証
権限管理
　アクセス権管理
　　シングルサインオン（Webシステム）
　　シングルサインオン（非Web系システム）
アクセス監視･制御
　サーバ利用監視･制御
　　サーバ用ファイアーウォール
証跡管理
　ログ収集管理
不正プログラム対策
　アンチウィルスソフト
　アンチウィルスゲートウェイ
　アンチウィルスソフトウェア管理
システム動作の保全管理
　システム性能監視
　システム冗長化
通信回線の保全管理
　トラフィック監視

S1のWebサーバ

主体認証
　ID／パスワード認証
権限管理
　アクセス権管理
　　シングルサインオン（Webシステム）
　　シングルサインオン（非Web系システム）
アクセス監視・制御
　サーバ利用監視・制御
　　サーバ用ファイアーウォール
証跡管理
　ログ収集管理
不正プログラム対策
　アンチウィルスソフト
　アンチウィルスゲートウェイ
　アンチウィルスソフトウェア管理
システム動作の保全管理
　システム性能監視
　システム冗長化
通信回線の保全管理
　トラフィック監視

S1のメールサーバ

主体認証
　ID／パスワード認証
権限管理
　アクセス権管理
　　シングルサインオン（Webシステム）
　　シングルサインオン（非Web系システム）
アクセス監視・制御
　　通信回線利用監視・制御
　　　メール監視（メールフィルタリング）
　　サーバ利用監視・制御
　　　サーバ用ファイアーウォール
証跡管理
　　ログ収集管理
暗号化・電子署名
　　データ暗号化
　　　メール暗号化
　　電子署名
　　　メールへの電子署名
不正プログラム対策
　　アンチウィルスソフト
　　アンチウィルスゲートウェイ
　　アンチウィルスソフトウェア管理
システム動作の保全管理
　　システム性能監視
　　システム冗長化
　　ソフトウェア資産管理
　　　ライセンス、バージョン管理
通信回線の保全管理
　　トラフィック監視

S1の各種サーバ

主体認証
　ID／パスワード認証
権限管理
　アクセス権管理
　　シングルサインオン（Webシステム）
　　シングルサインオン（非Web系システム）
アクセス監視・制御
　　サーバ利用監視・制御
　　　サーバ用ファイアーウォール
証跡管理
　　ログ収集管理
不正プログラム対策
　　アンチウィルスソフト
　　アンチウィルスゲートウェイ
　　アンチウィルスソフトウェア管理
システム動作の保全管理
　　システム性能監視
　　システム冗長化
　　バックアップ／リストア
通信回線の保全管理
　　トラフィック監視

S2の通信回線

証跡管理
　　ログ収集管理
システム動作の保全管理
　　システム性能監視
通信回線の保全管理
　　トラフィック監視

S2の各種サーバ

主体認証
　ID／パスワード認証
権限管理
　アクセス権管理
　　シングルサインオン（Webシステム）
　　シングルサインオン（非Web系システム）
証跡管理
　　ログ収集管理
不正プログラム対策
　　アンチウィルスソフト
　　アンチウィルスゲートウェイ
　　アンチウィルスソフトウェア管理
システム動作の保全管理
　　システム性能監視
　　バックアップ／リストア
通信回線の保全管理
　　トラフィック監視

S3のPC端末

主体認証
　ID／パスワード認証
　生体認証
　　指紋認証
　二要素認証
アクセス監視・制御
　通信回線利用監視・制御
　　メール監視（メールフィルタリング）
　　Web監視（フィルタリング）
端末利用監視・制御
　　端末利用監視システム
　　パーソナルファイアーウォール
証跡管理
　　ログ収集管理
暗号化・電子署名
　　暗号化・署名アルゴリズム
　　共通鍵暗号方式
　　公開鍵暗号方式
　　秘密分散方式
データ暗号化
　　ファイル暗号化
　　ディスク暗号化
　　メール暗号化
電子署名
　　メールへの電子署名
不正プログラム対策
　　アンチウィルスソフト
　　アンチウィルスゲートウェイ
　　アンチウィルスソフトウェア管理
システム動作の保全管理
　　ハードウェア管理
ハードウェア構成管理
ソフトウェア資産管理
　　ライセンス、バージョン管理
物理的対策
　　物理的漏えい対策
　　物品持出管理
　　覗き見防止フィルタ

6-3. 最新セキュリティ情報の参照

構成機器のソリューションに関係する最新セキュリティ情報を参照する。

S1のDNSサーバ

- 主体認証
  - ID／パスワード認証
- 権限管理
  - アクセス権管理
    - シングルサインオン（Webシステム）
    - シングルサインオン（非Web系システム）
- アクセス監視・制御
  - **サーバ利用監視・制御**
- 証跡管理
  - ログ収集管理
- 不正プログラム対策
  - アンチウィルスソフト
  - アンチウィルスゲートウェイ
  - アンチウィルスソフトウェア管理
- システム動作の保全管理
  - システム性能監視
  - システム冗長化
- 通信回線の保全管理
  - トラフィック監視

【RSS検索条件】

サーバ

検索期間：1年

登録RSSサイト全て

【RSS検索結果】

61件中 1－20件目　　1 2 3 4 次へ

サンのWebサーバにXSSの脆弱性

サンのWebサーバにXSSの脆弱性 - ITmedia エンタープライズ ITmedia 総合 | ITmedia News | ITmedia Biz.ID | ITmedia エンタープライズ | TechTargetジャパン | ITmedia エグゼクティブ | ITmedia ＋D PC USER | ITmedia ＋D Mobile | ITmedia ＋D LifeStyle | ITmedia ＋D Games | ITmedia ＋D Shopping | ITmedia ＋D Style | ITmedia キャリアトップ ITニュース W...

2007年12月21日 (580) ep salerts - http://rss.rssad.jp/rss/artclk/N.cTRQmxp4Q/b193876fc31e23854d63395a34743eb7?ul=v2EthxK...

サンのWebサーバにXSSの脆弱性

サンのWebサーバにXSSの脆弱性 - ITmedia エンタープライズ ITmedia 総合 | ITmedia News | ITmedia Biz.ID | ITmedia エンタープライズ | TechTargetジャパン | ITmedia エグゼクティブ | ITmedia ＋D PC USER | ITmedia ＋D Mobile | ITmedia ＋D LifeStyle | ITmedia ＋D Games | ITmedia ＋D Shopping | ITmedia ＋D Style | ITmedia キャリアトップ ITニュース W...

2007年12月21日 (575) ep salerts - http://rss.rssad.jp/rss/artclk/N.cTRQmxp4Q/b193876fc31e23854d63395a34743eb7?ul=v2EthxK...

6-4. システム構成の見直しによるキュリティ対策基準の見直し

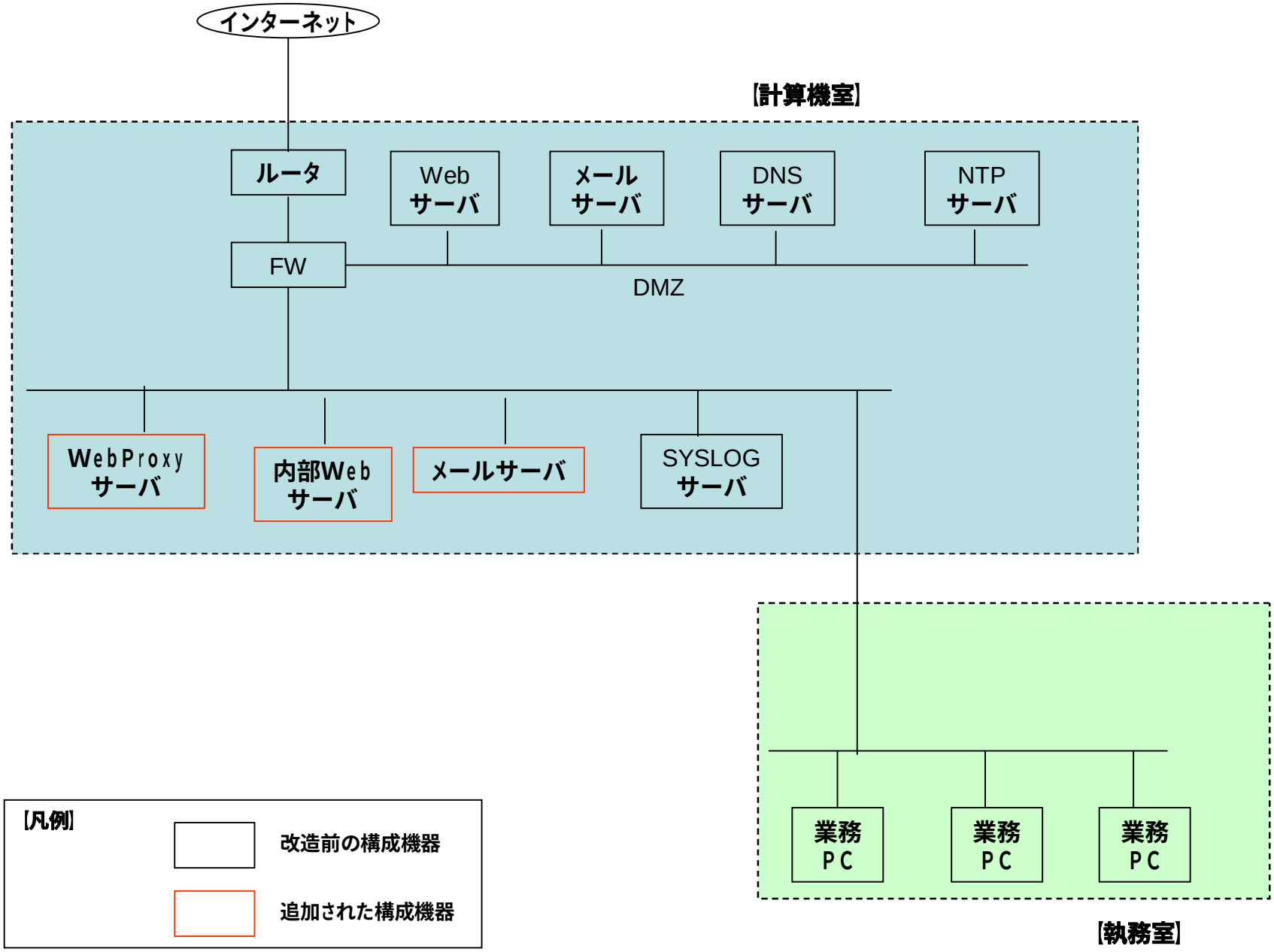
1). 目的

既設の情報システムの改造(6-1.)を行った場合に、新たに検討が必要なセキュリティ要件、見直しが必要なセキュリティ要件を検討する。

2). ネットワーク構成図

検討対象の改造前の情報システム及び改造後の情報システムの主要な構成要素が記載されたネットワーク構成図を作成する。

検討対象の情報システムのネットワーク構成図



3）. 検討対象の情報システム概要の整理

（1）で検討したシステムのセキュリティを強化するために、内部メールサーバ、内部Webサーバ、外部ホームページアクセスのためのProxyサーバを内部セグメントに追加する。

①コンテンツの作成及び公開

広報課の担当職員は情報提供のためのコンテンツを作成するために、内部セグメント上に設置された内部Webサーバ上で公開前コンテンツを作成する。

公開前のコンテンツは機密性2として、関係者が内部メールサーバ上のメーリングリストで審査する。

メーリングリストの情報は機密性2として、非公開とする。

県民や外部からの情報および意見等を収集するために、ホームページに掲載された問合せメールアドレスをDMZ上のメールサーバで受け付ける。

コンテンツの内容の承認は、広報課長が行い、承認後のコンテンツは機密性3（公開）として、DMZ上に設置されたWebサーバにコンテンツをコピーする。

DMZ上の公開Webサーバ、メールサーバ、NTPサーバのURL問合せのために、DMZ上にDNSサーバを設置する。

②職員へのインターネット利用環境提供

職員は職員間の情報交換、外部との情報機密性の高い情報は、内部メールサーバのみ利用（機密性2）扱いとする。

職員は、コンテンツ作成及び情報収集のために外部のホームページを参照するが、ネットワーク負荷軽減と不適切な外部ホームページへの参照が行われないように内部セグメントに設置されたProxyサーバを利用して行う。

③セキュリティ対策

ルータ、FWで不要パケットのフィルタリングを行い不正アクセスを防ぐ。

不正アクセス、システム障害の監視のためにSYSLOGサーバを内部セグメントに設ける。

LOGデータの時間的整合を実現するために、NTPサーバをDMZ上に設け、ルータ、FW、Webサーバ、メールサーバ、Proxyサーバの時間同期を行う。

4)．検討に当たっての前提条件、主要な脅威の抽出例

3) システム概要から前提条件、主要な脅威を抽出する。

①前提条件

ⅰ) ルータ、FW各種サーバは、身分証明書のIDｶｰﾄﾞと入室許可者に知らされたパスワード入力による入室制限が行われた計算機室内に設置される。

ⅱ) サーバへのアクセスは、職員のみとする。

ⅲ) 業務ＰＣは、入室制限がない執務室に置かれる。

ⅳ) 業務ＰＣの使用は、職員のみとする。

ⅴ) 職員は不正行為を行わない。但し誤操作等はあるものとする。

②主要な脅威

ⅰ) 外部からの脅威

a) HP公開情報の改ざん　b) 公開前HPコンテンツの改ざん、盗み見

c) 外部の攻撃者によるDos攻撃によるシステム使用障害　(Webサーバ、メールサーバ)

c) メール、Webからのサーバ、業務PCへのウイルス感染

ⅱ) 内部からの脅威

a) 職員以外の業務PC使用による公開前HPコンテンツの改ざん、盗み見

b) 職員の誤操作による公開前HP情報の誤消去

c) 職員の誤操作によるルータ、FW、サーバの情報の誤入力、誤消去

d) ＦＤ、ＵＳＢ等を介して業務端末からのウイルス感染

5）. SRAS入力のための条件の整理

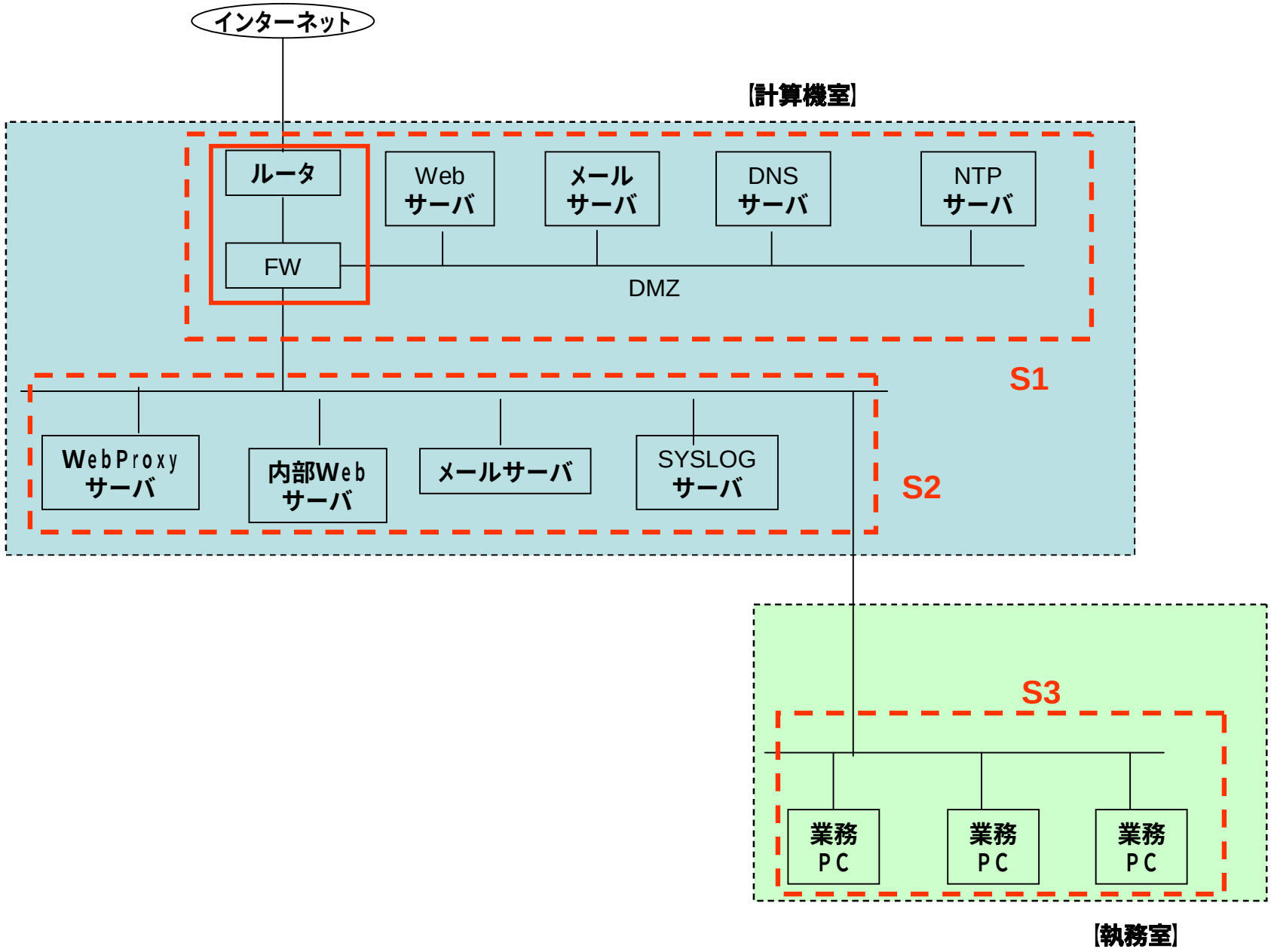
①. セキュリティポリシー　　地方公共団体における情報セキュリティポリシーに関するガイドライン

②. ネットワーク構成　　地方自治体

③. 構成要素

設置箇所	検討対象ITシステム	情報資産	SRAS入力		
	構成要素		選択SG	構成要素	情報格付け
計算機室	通信回線	通信データ	S1	通信回線	要保護情報
	ルータ	ルーティングテーブル		通信回線装置	要保護情報
	FW	フィルタリングテーブル			
	Webサーバ	公開コンテンツ		Webサーバ	要保護情報
	メールサーバ	メール		メールサーバ	要保護情報
	DNSサーバ	アドレステーブル		DNSサーバ	要保護情報
	NTPサーバ	同期時間データ		各種サーバ	要保護情報
	通信回線（内部LAN）	通信データ	S2	通信回線	要保護情報
	WebProxyサーバ			Proxyサーバ	
	内部Webサーバ	公開前コンテンツ		Webサーバ	要保護情報
	メールサーバ	メール		メールサーバ	要保護情報
	SYSLOGサーバ	LOGデータ		各種サーバ	要保護情報
執務室	通信回線（内部LAN）	通信データ	S3	通信回線	要保護情報
	業務PC			業務用PC	

④SRAS入力のためのセグメント分割例



⑤リスク入力に関して

前提条件及び主要な脅威からセグメントに関係ない脅威を除く。

例えば、入室制限のある計算機室内のセグメント（S1，S2）の構成要素は、破壊、盗難等のリスクは存在しない等で以下のリスクを除く。

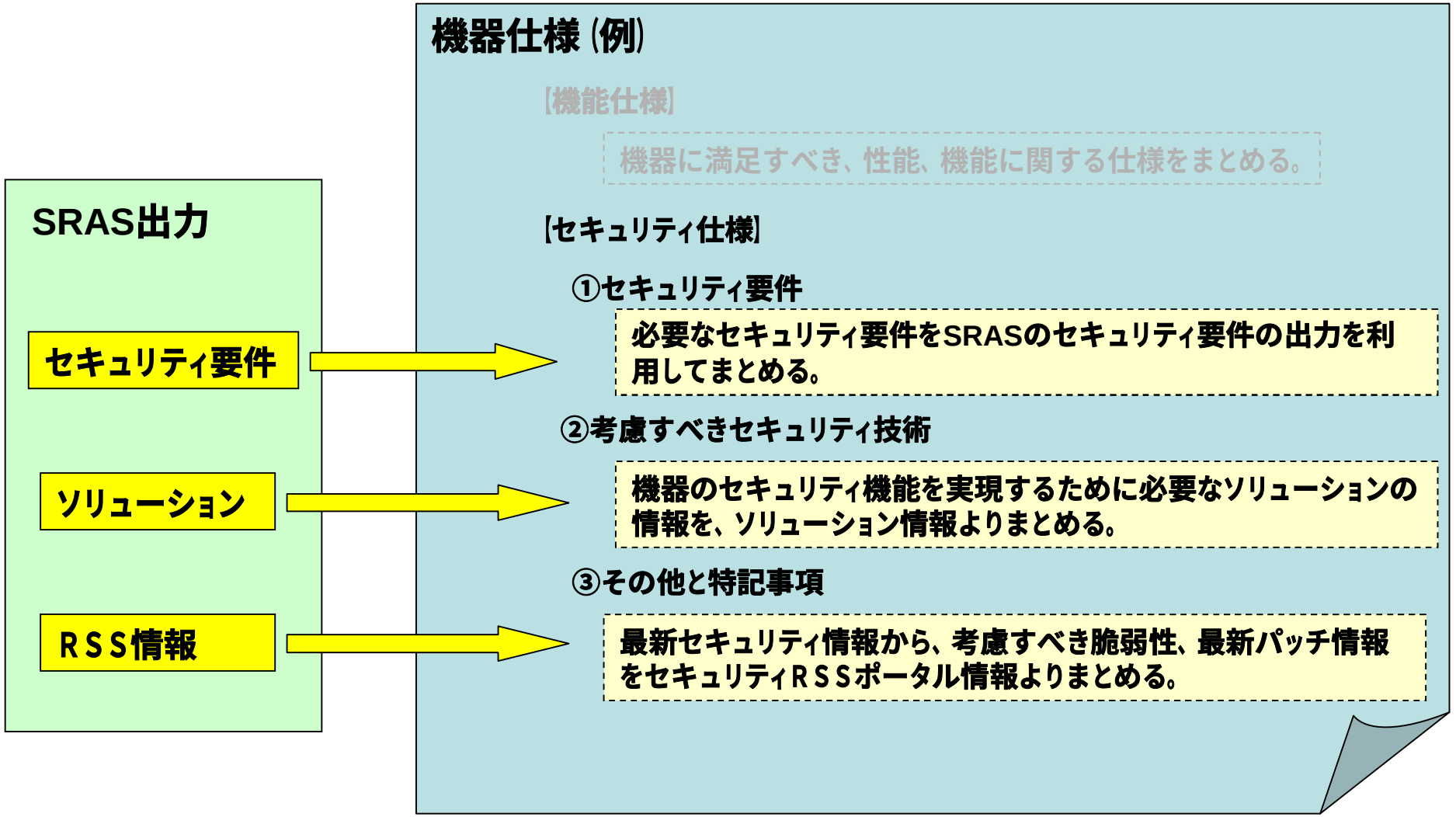
執務室へは職員以外も入室可能なので破壊、盗難等の脅威は存在する。

（S1、S2の脅威は同じ）

	除去リスク
S1，S2	盗聴
	破壊
	盗難
	窃取
	装置・機器等の損傷
	端末等の故障
	アクセスポイントの不正接続
S3	アクセスポイントの不正接続

6-5 調達の検討

構成要素に必要なセキュリティ要件、必要なソリューション、最新の脆弱性情報等のセキュリティ情報を参考にして、調達仕様書の要求仕様として必要な要件をまとめる。



6-7. ＣＣＲＡ製品の検討

詳細検討により選択されたセキュリティ要件に対応するソリューションのカテゴリーに対応するＣＣＲＡ製品の一覧が表示されるので、リストから採用製品の候補を検討する。

主体認証
　ID／パスワード認証
権限管理
　アクセス権管理
　　シングルサインオン（Webシステム）
　　シングルサインオン（非Web系システム）

→ アクセス権

→ ＣＣＲＡポータル　認証製品リスト

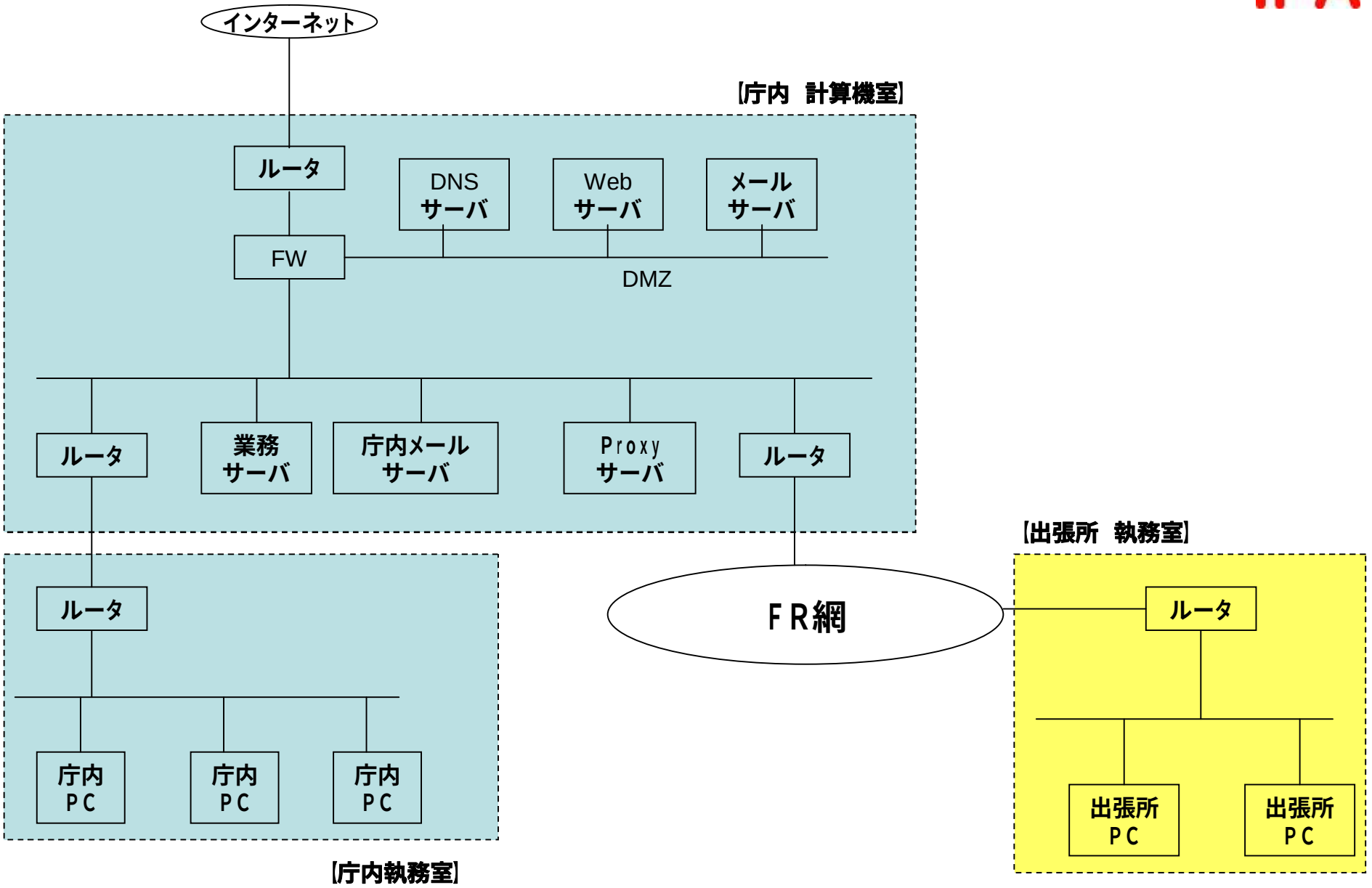
【ＣＣＲＡポータルでＡＣＣＥＳＳ権に関係するもの】

Access Control Devices and Systems

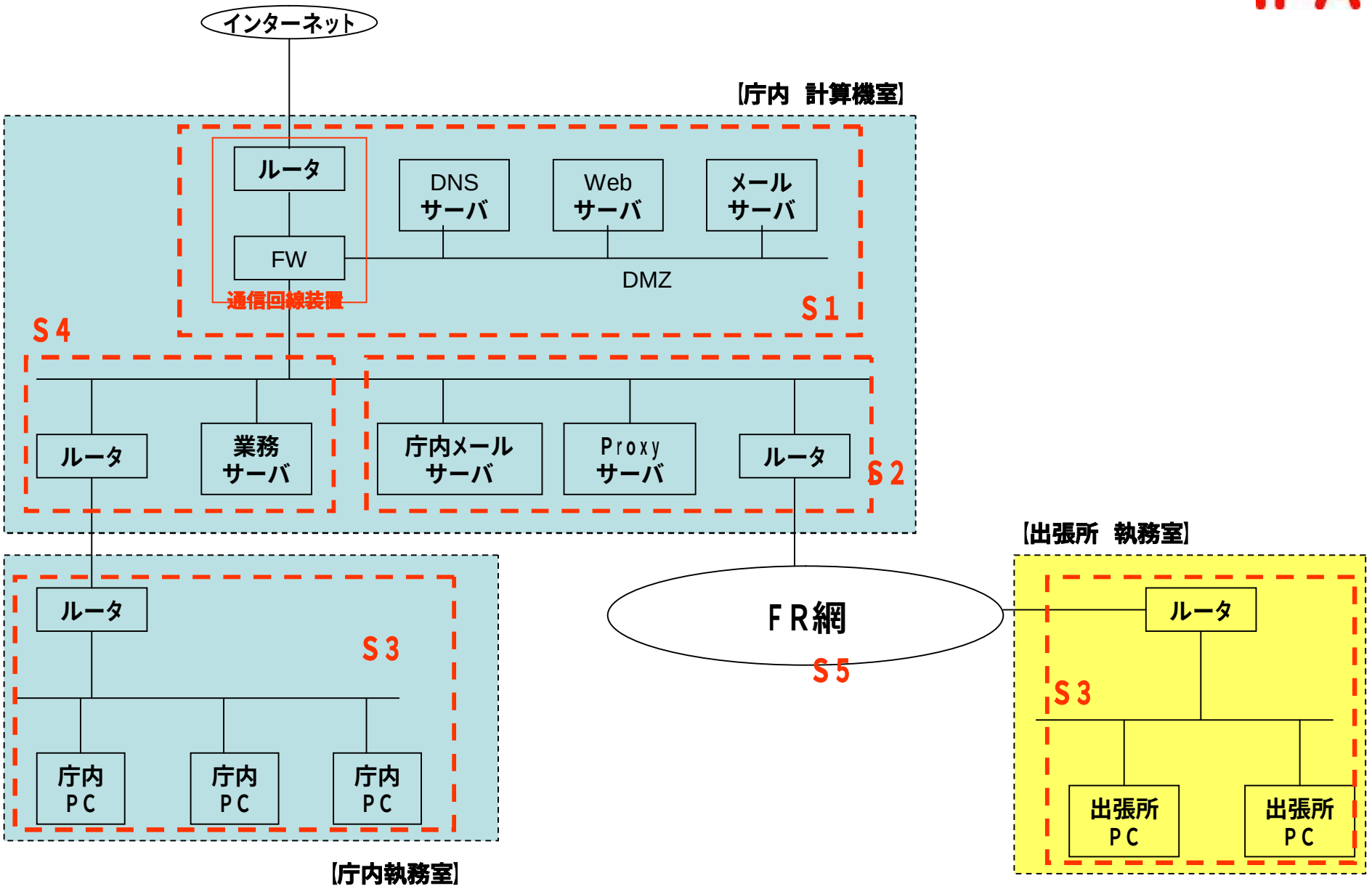
name: **3eTI 3e-525A-3 Access System**		
manufacturer: 3e Technologies International, Inc.	assurance level: EAL2+	certification date: 15 September 2006
certification report: ST_VID3031-VR.pdf	security target: ST_VID3031-ST.pdf	
name: **Boeing Secure Network Server (SNS-3010 and SNS-3210)**		
manufacturer: The Boeing Company	assurance level: EAL4+	certification date: 10 May 2007
certification report: st_vid10127-vr.pdf	security target: st_vid10127-st.pdf	
name: **CA Access Control for Windows r8**		
manufacturer: CA, Inc.	assurance level: EAL3	certification date: 20 June 2007
certification report: st_vid3036-vr.pdf	security target: st_vid3036-st.pdf	

付録．A：ネットワーク図からのセグメント入力例

想定モデル（1）の例


インターネット
【庁内　計算機室】
ルータ
DNS
サーバ
Web
サーバ
メール
サーバ
FW
DMZ
ルータ
業務
サーバ
庁内メール
サーバ
Proxy
サーバ
ルータ
【出張所　執務室】
ルータ
ＦＲ網
ルータ
庁内
ＰＣ
庁内
ＰＣ
庁内
ＰＣ
出張所
ＰＣ
出張所
ＰＣ
【庁内執務室】

想定モデル（1）のセグメントの考え方



想定モデル（1）の検証のための入力について

1．セキュリティポリシー　　地方公共団体における情報セキュリティポリシーに関するガイドライン

2．ネットワーク構成　　地方自治体

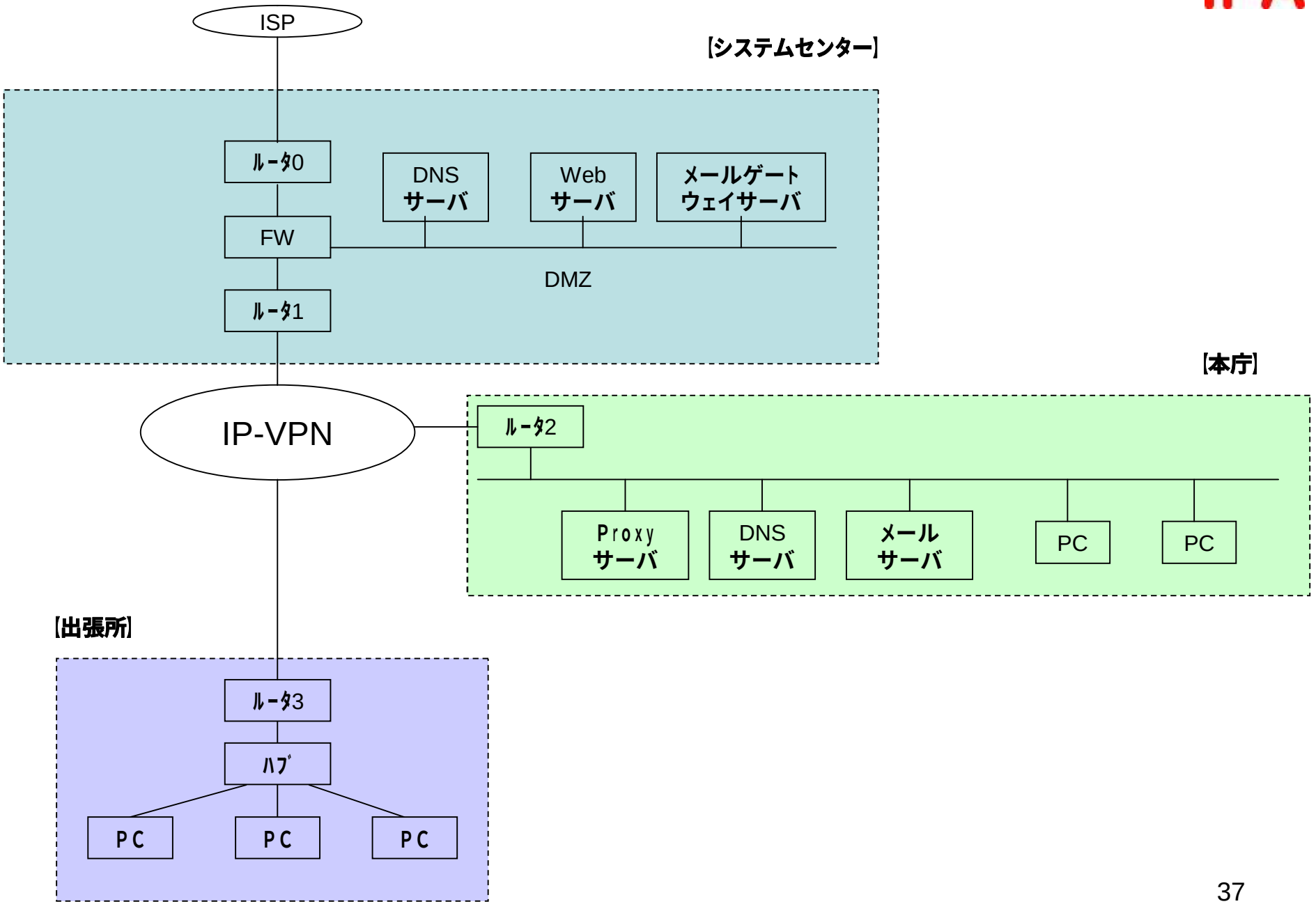
	検討対象ITシステム	SRASの入力		
庁内計算機室	ネットワーク要素	選択SG	構成要素	情報資産
	ルータ	S1	通信回線装置	要保護情報
	FW			
	DNSサーバ		DNSサーバ	要保護情報
	Webサーバ		公開Webサーバ	要保護情報
	メールサーバ		メールサーバ	要保護情報
	ルータ	S2	通信回線装置	要保護情報
	庁内メールサーバ		庁内メールサーバ	要保護情報
	Proxyサーバ		庁内Webサーバ	要保護情報
	ルータ	S4	通信回線装置	要保護情報
	業務サーバ		各種サーバ	要保護情報

	検討対象ITシステム	SRASの入力		
庁内執務室	ネットワーク要素	選択SG	構成要素	情報資産
	ルータ	S3	通信回線装置	要保護情報
	庁内PC		業務用端末	要保護情報

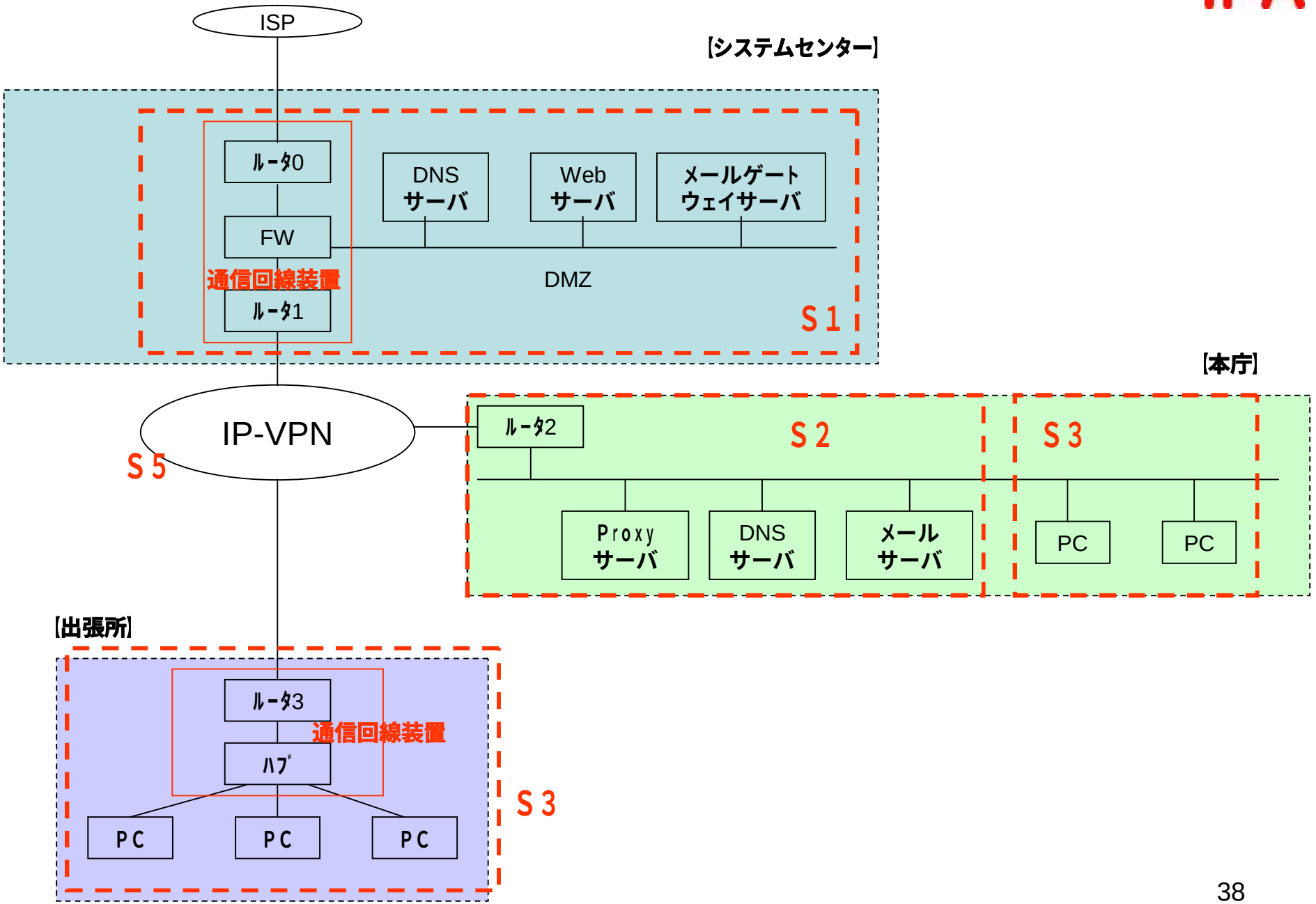
	検討対象ITシステム	SRASの入力		
FR網	ネットワーク要素	選択SG	構成要素	情報資産
	FR網	S5	専用線	要保護情報

	検討対象ITシステム	SRASの入力		
出張先執務室	ネットワーク要素	選択SG	構成要素	情報資産
	ルータ	S3	通信回線装置	要保護情報
	出張所PC		業務用端末	要保護情報

想定モデル（2）の例


ISP
【システムセンター】
ルータ0
DNS
サーバ
Web
サーバ
メールゲート
ウェイサーバ
FW
DMZ
ルータ1
【本庁】
IP-VPN
ルータ2
Proxy
サーバ
DNS
サーバ
メール
サーバ
PC
PC
【出張所】
ルータ3
ハブ
PC
PC
PC

想定モデル（2）のセグメントの考え方



想定モデル（2）の検証のための入力について

1．セキュリティポリシー　　地方公共団体における情報セキュリティポリシーに関するガイドライン

2．ネットワーク構成　　地方自治体

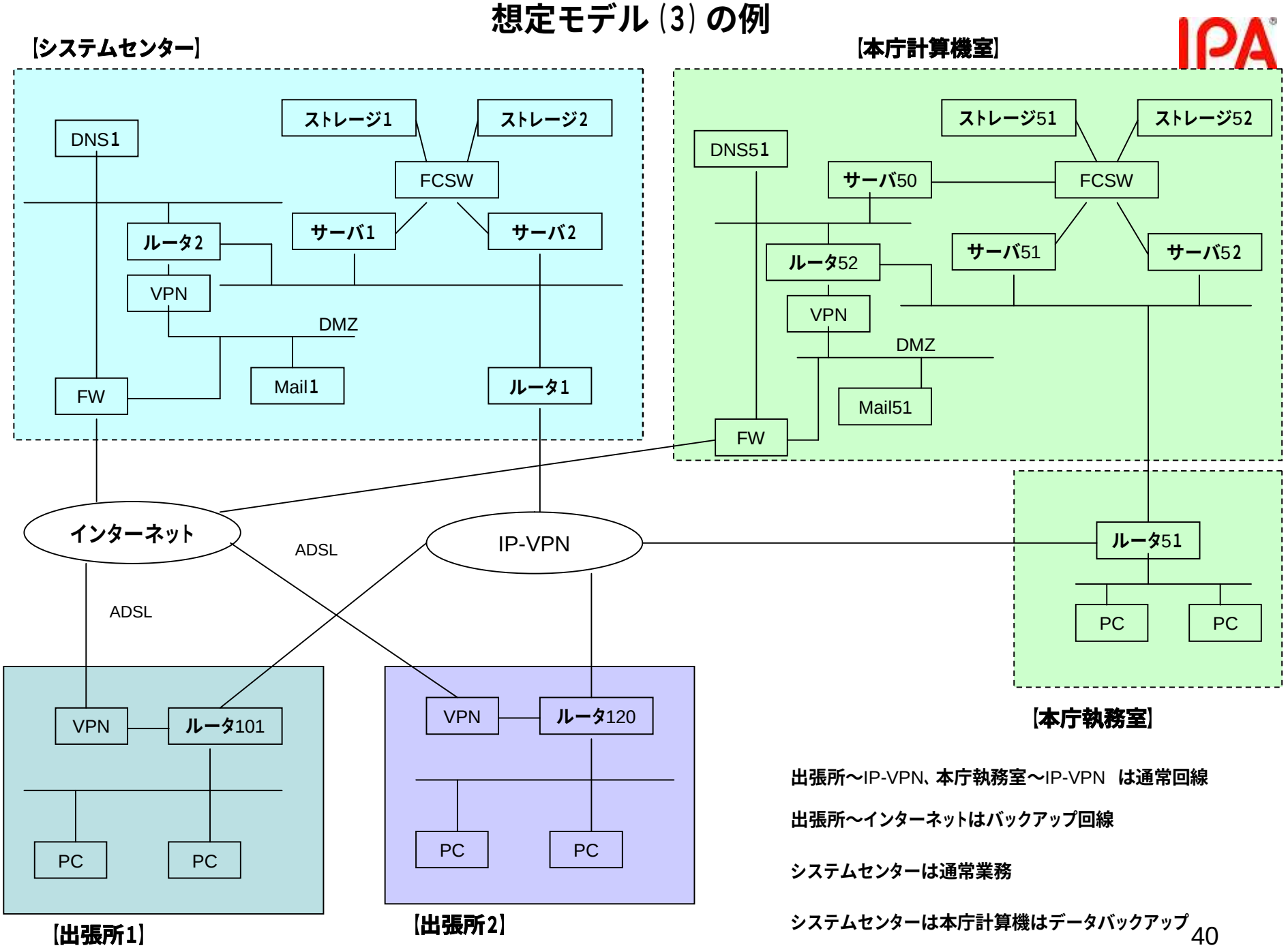
	検討対象ITシステム	SRASの入力		
システムセンター	ネットワーク要素	選択SG	構成要素	情報資産
	ルータ0	S1	通信回線装置	要保護情報
	FW			要保護情報
	ルータ1			要保護情報
	DNSサーバ		サーバ	要保護情報
	Webサーバ		Webサーバ	要保護情報
	メールゲートウェイサーバ		メールサーバ	要保護情報

	検討対象ITシステム	SRASの入力		
本庁	ネットワーク要素	選択SG	構成要素	情報資産
	Proxyサーバ	S2	Webサーバ	要保護情報
	メールサーバ		メールサーバ	要保護情報
	DNSサーバ		サーバ	要保護情報
	庁内PC	S3	端末	要保護情報

	検討対象ITシステム	SRASの入力		
IP－VPN	ネットワーク要素	選択SG	構成要素	情報資産
	IP－VPN	S5	専用線	要保護情報

	検討対象ITシステム	SRASの入力		
出張所	ネットワーク要素	選択SG	構成要素	情報資産
	ルータ3	S3	通信回線装置	要保護情報
	ﾊﾌﾞ			要保護情報
	PC		端末	要保護情報

想定モデル（3）の例



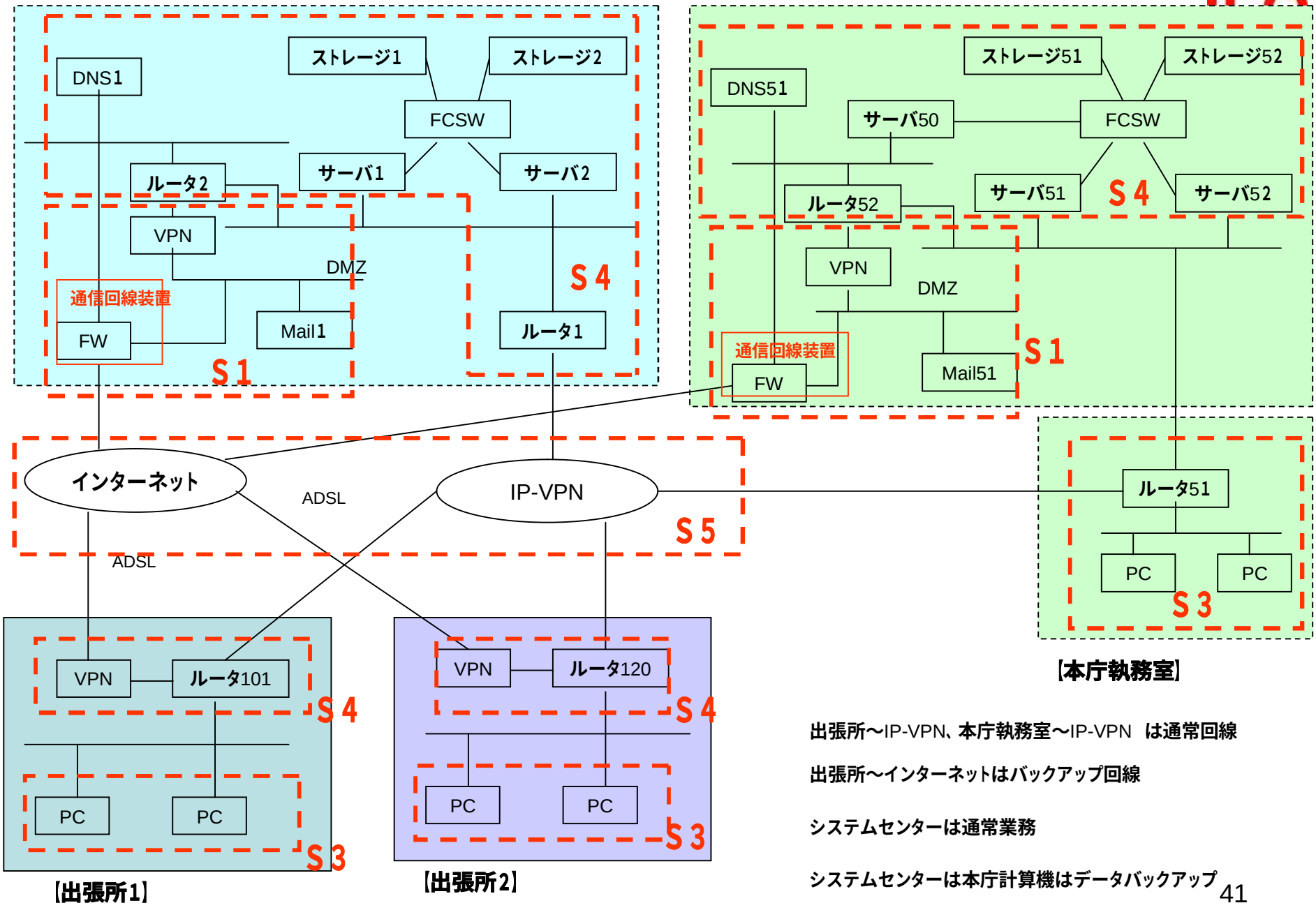
出張所～IP-VPN、本庁執務室～IP-VPN　は通常回線

出張所～インターネットはバックアップ回線

システムセンターは通常業務

システムセンターは本庁計算機はデータバックアップ

想定モデル（3）のセグメントの考え方



出張所～IP-VPN、本庁執務室～IP-VPN　は通常回線

出張所～インターネットはバックアップ回線

システムセンターは通常業務

システムセンターは本庁計算機はデータバックアップ

想定モデル（3）の検証のための入力について

1．セキュリティポリシー

地方公共団体における情報セキュリティポリシーに関するガイドライン

2．ネットワーク構成

地方自治体

システムセンター

検討対象ITシステム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
FW	S1	通信回線装置	要保護情報
Mail1		公開メールサーバ	要保護情報
VPN		VPN	要保護情報
ルータ2	S4	通信回線装置	要保護情報
ルータ1		通信回線装置	要保護情報
サーバ1		サーバ（業務サーバ）	要保護情報
サーバ2		サーバ（業務サーバ）	要保護情報
FCSW		通信回線装置	要保護情報
ストレージ1		サーバ	要保護情報
ストレージ2		サーバ	要保護情報
DNS1		サーバ	要保護情報

出張所1

検討対象ITシステム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
VPN	S4	VPN装置	要保護情報
ルータ1101		通信回線装置	要保護情報
PC	S3	端末	要保護情報

出張所2

検討対象ITシステム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
VPN	S4	VPN装置	要保護情報
ルータ120		通信回線装置	要保護情報
PC	S3	端末	要保護情報

本庁計算機室

検討対象ITシステム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
FW	S1	通信回線装置	要保護情報
Mail51		公開メールサーバ	要保護情報
VPN		VPN	要保護情報
ルータ52	S4	通信回線装置	要保護情報
DNS51		サーバ	要保護情報
サーバ50		サーバ	要保護情報
サーバ51		サーバ	要保護情報
サーバ52		サーバ	要保護情報
FCSW		通信回線装置	要保護情報
ストレージ51		サーバ	要保護情報
ストレージ52		サーバ	要保護情報

本庁執務室

検討対象ITシステム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
ルータ	S3	通信回線装置	要保護情報
PC		端末	要保護情報

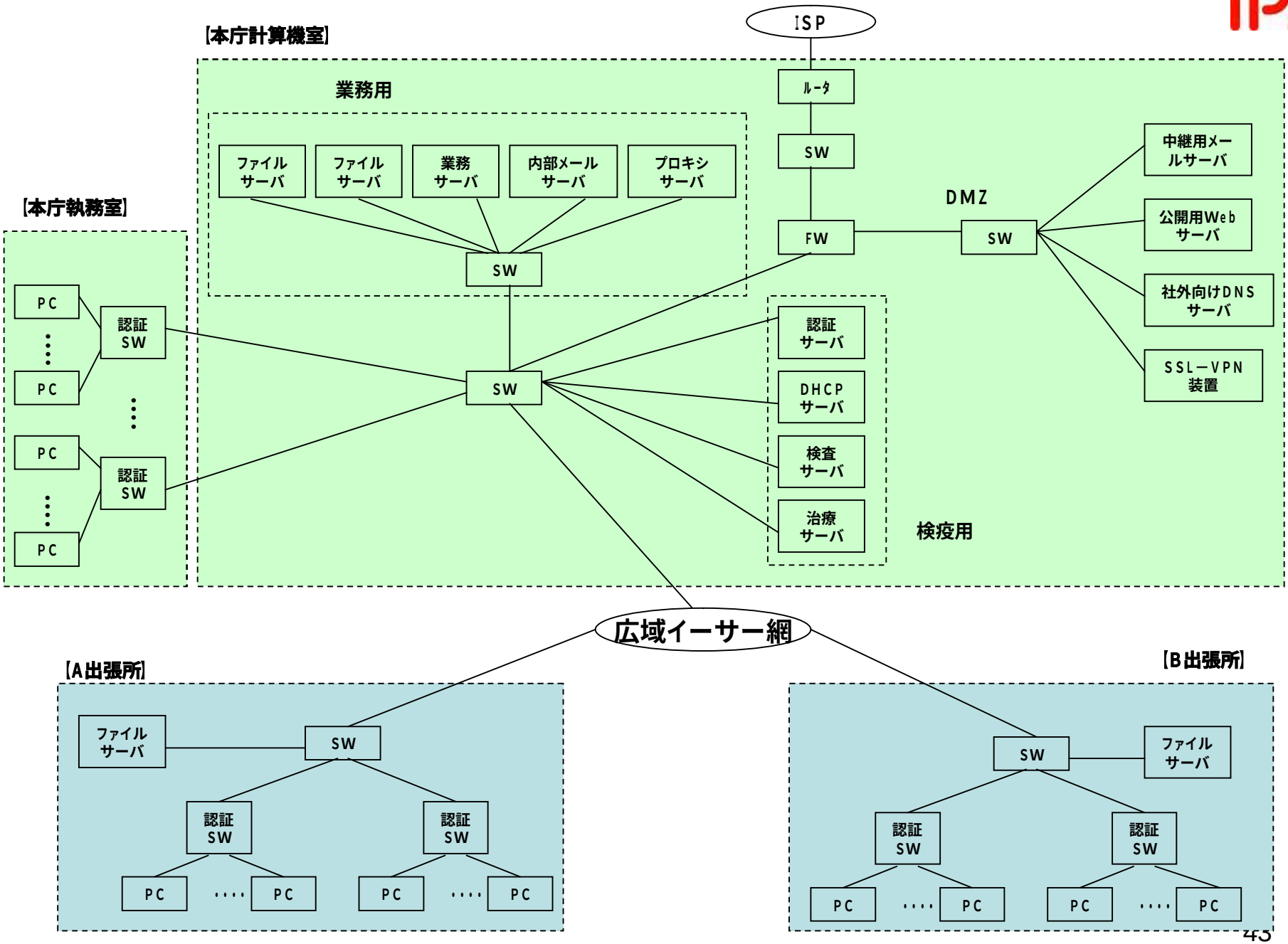
インターネット

検討対象ITシステム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
インターネット	S5	通信回線	要保護情報

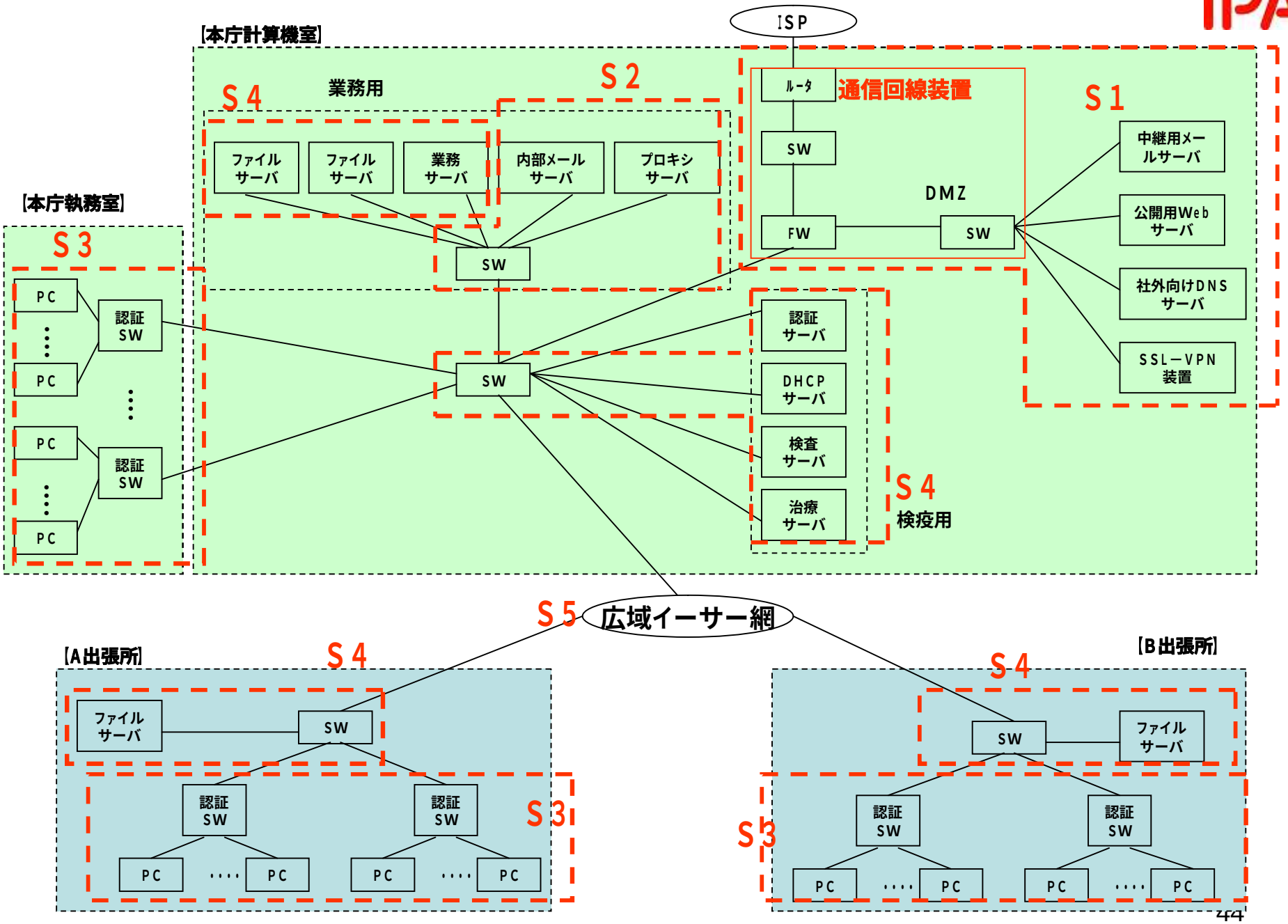
IP-VPN

検討対象ITシステム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
IP-VPN	S5	通信回線	要保護情報

想定モデル（4）の例


【本庁計算機室】
ISP
ルータ
SW
業務用
ファイルサーバ
ファイルサーバ
業務サーバ
内部メールサーバ
プロキシサーバ
SW
FW
DMZ
SW
中継用メールサーバ
公開用Webサーバ
社外向けDNSサーバ
SSL－VPN装置
【本庁執務室】
PC
PC
認証SW
PC
PC
認証SW
SW
認証サーバ
DHCPサーバ
検査サーバ
治療サーバ
検疫用
広域イーサー網
【A出張所】
ファイルサーバ
SW
認証SW
認証SW
PC
PC
PC
PC
【B出張所】
SW
ファイルサーバ
認証SW
認証SW
PC
PC
PC
PC

想定モデル（4）のセグメントの考え方



想定モデル（4）の検証のための入力について

1．セキュリティポリシー　　地方公共団体における情報セキュリティポリシーに関するガイドライン

2．ネットワーク構成　　地方自治体

本庁計算機室

検討対象システム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
ルータ	S1	通信回線装置	要保護情報
SW			要保護情報
FW			要保護情報
SW			要保護情報
中継メールサーバ		メールサーバ	要保護情報
公開Webサーバ		Webサーバ	要保護情報
社外向けDNSサーバ		サーバ	要保護情報
SSL－VPN装置		VPN装置	要保護情報
SW	S2	通信回線装置	要保護情報
内部メールサーバ		メールサーバ	要保護情報
プロキシサーバ		Webサーバ	要保護情報
ファイルサーバ	S4	サーバ	要保護情報
業務サーバ		サーバ	要保護情報
SW	S4	通信回線装置	要保護情報
認証サーバ		サーバ	要保護情報
DHCPサーバ		サーバ	要保護情報
検査サーバ		サーバ	要保護情報
治療サーバ		サーバ	要保護情報

本庁執務室

検討対象システム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
認証SW	S3	通信回線装置	要保護情報
PC		端末	要保護情報

広域イーサー網

検討対象システム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
広域イーサー網	S5	通信回線	要保護情報

A出張所

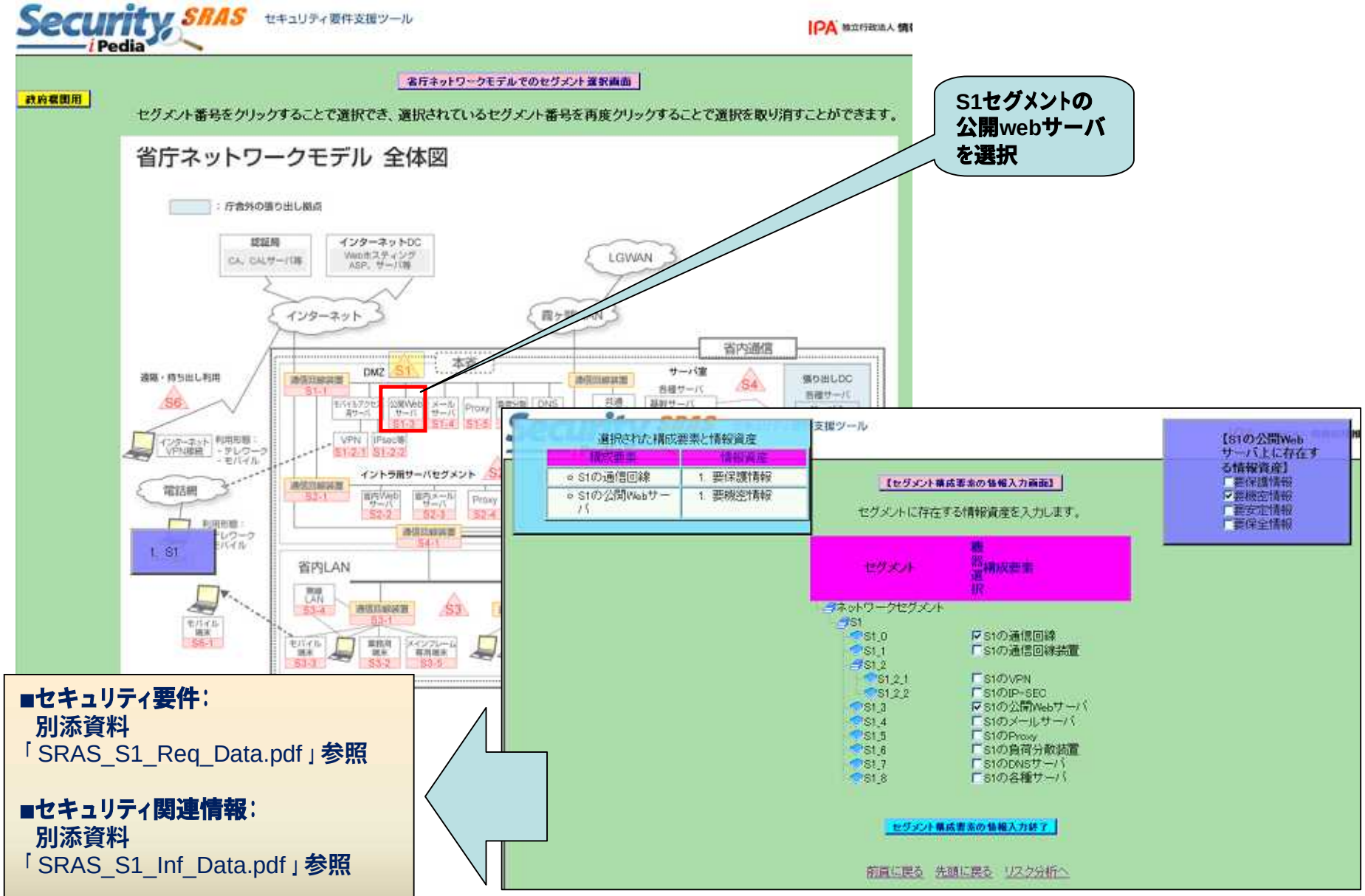
検討対象システム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
SW	S4	通信回線装置	要保護情報
ファイルサーバ		サーバ	要保護情報
認証SW	S3	通信回線装置	要保護情報
PC		端末	要保護情報

B出張所

検討対象システム	SRASの入力		
ネットワーク要素	選択SG	構成要素	情報資産
SW	S4	通信回線装置	要保護情報
ファイルサーバ		サーバ	要保護情報
認証SW	S3	通信回線装置	要保護情報
PC		端末	要保護情報

付録B：事例集

事例：統一基準　S１　公開webサーバ
ライフサイクルごとのセキュリティ要件及びセキュリティ関連情報



■セキュリティ要件：
別添資料
「SRAS_S1_Req_Data.pdf」参照

■セキュリティ関連情報：
別添資料
「SRAS_S1_Inf_Data.pdf」参照