(ISC)² Secure Events

SECURE TOKYO 2017

いかに280万人の県民資産を守るか？

- ひろしまセキュリティクラウド -

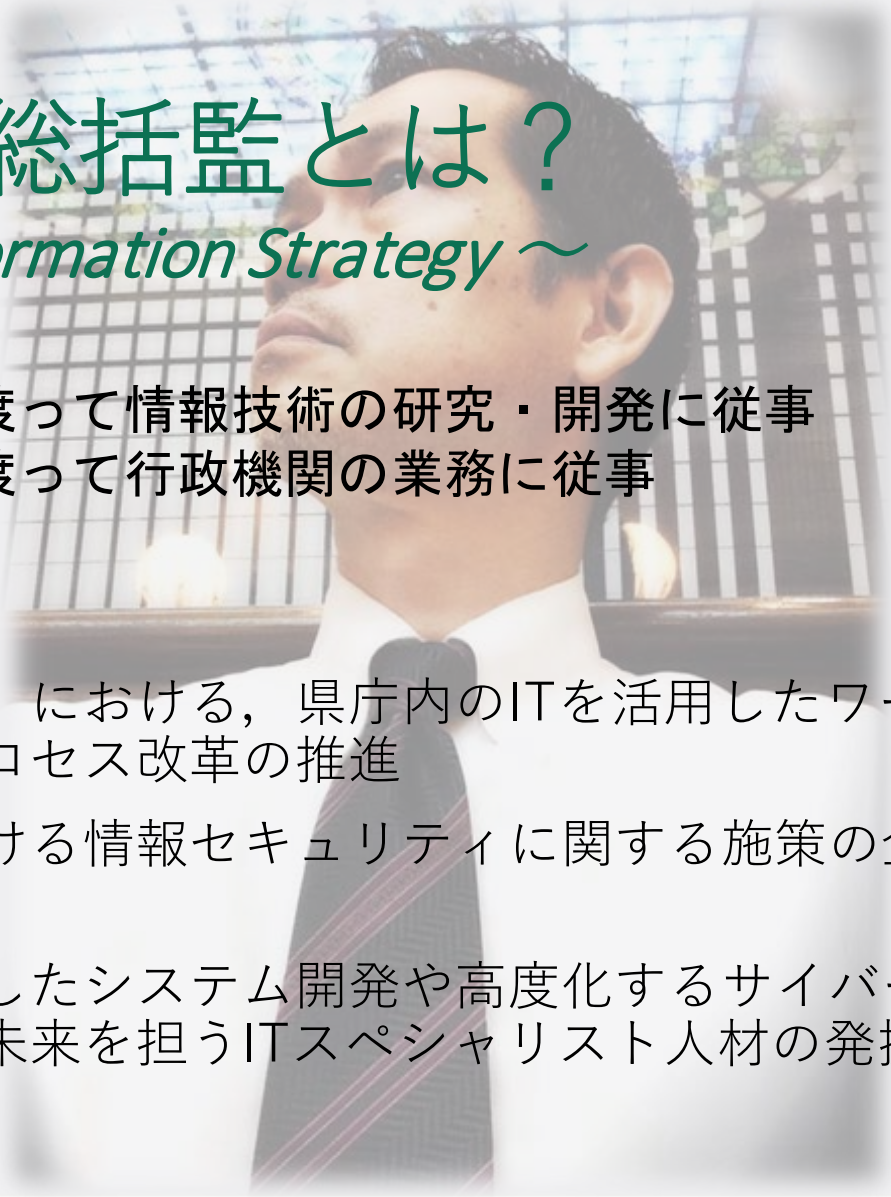
桑原　義幸, CISSP

広島県総務局情報戦略総括監

桑原義幸(くわはらよしゆき)

まずは自己紹介

情報戦略総括監とは？
～ *Chief of Information Strategy* ～

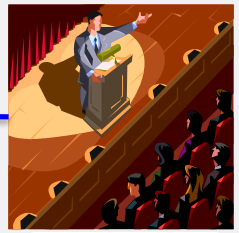


・35年以上に渡って情報技術の研究・開発に従事
・15年以上に渡って行政機関の業務に従事

- 「働き方改革」における，県庁内のITを活用したワークスタイル改革や業務プロセス改革の推進
- 県・市町における情報セキュリティに関する施策の企画、立案および推進
- 新技術を活用したシステム開発や高度化するサイバー攻撃等に対応するための未来を担うITスペシャリスト人材の発掘および育成

組織

湯崎知事



県議会

経営戦略会議

知事部局

情報戦略総括監

総務局

商工労働局

土木局

……

外部機関

県教委，他

県警本部

業務プロセス改革課

PMO

情報担当

情報担当

情報担当

(C) 行政管理担当

(P, D) 業務改革担当

(A) 情報基盤担当

(P, D) 地域情報化担当

庁内横串

23の市町

広島概要

	日本	広島
人口	128,000,000	2,863,000
面積	377,971㎢	8,479㎢

広島サマリ

- 食と文化と2つの世界遺産






昨年も そして今年も！

広島東洋カープ25年振りのリーグ優勝

女子200m平泳ぎ
金メダリスト金藤選手

男子4×100mリレー銀メダリスト山縣選手と湯﨑知事

Hiroshima Year !

現職米国大統領として初の広島訪問

メキシコオリンピック選手団の事前合宿の協定

プロジェクトの背景

サイバーセキュリティを取り巻く日本の状況

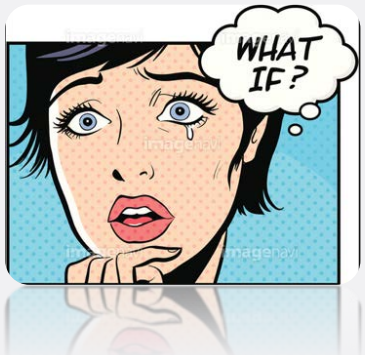
主な出来事

- 2014年11月　　サイバーセキュリティ基本法制定
- 2015年10月　　マイナンバー配布開始
- 2016年1月　　マイナンバー制度開始
- 2020年7月　　東京オリンピック開催

国を挙げた
セキュリティ対策が本格化

セキュリティリスク

- 官公庁におけるサイバーセキュリティリスクが増大
  - 日本年金機構における情報漏えい事件発生
  - 2017年7月よりマイナンバー関連システム情報連携がスタート



国の一つの指針

- 前述の年金機構の事案及び昨今の状況を鑑みて，総務省から示された指針
  - ネットワークの分離
  - CISO設置等体制の強化
  - セキュリティの強靭化
  - セキュリティクラウドの構築
    - 2017年3月末までに実施すること

FYI: 広島県のメール受信状況

攻撃の数 (IPSでブロック)				
	3月	4月	5月	平均
計	604,832	473,768	439,622	506,074

eMail受信状況				
	3月	4月	5月	平均
計	527,075	491,088	364,181	460,781
リジェクト	167,614	173,007	70,341	136,987
タグ付き許可	12,116	14,304	12,501	12,974
許可	347,345	303,777	281,339	310,820
スパム	185	919	1,023	709
(スパム開封)	1	16	7	8

プロジェクトの概要

なぜセキュリティクラウドなのか…？

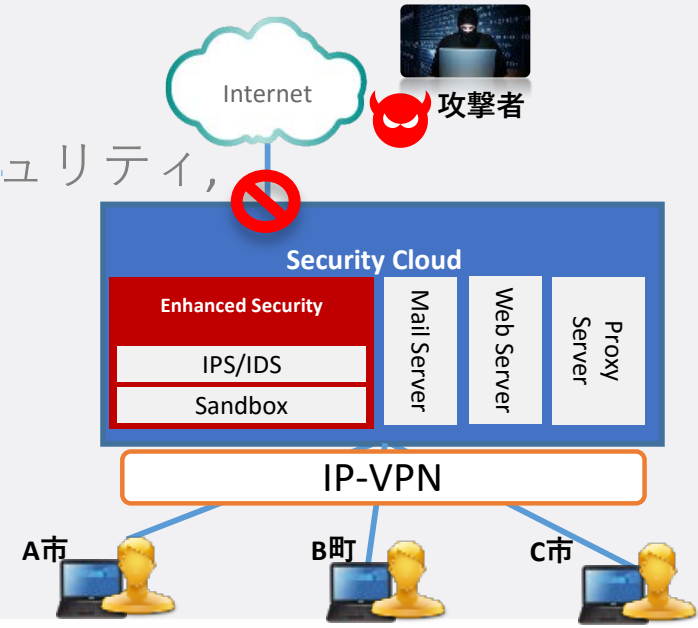
本県の基本方針

- 行政サービスの質を落とすことは絶対に避けるべき
- セキュリティを如何に確保しつつ、柔軟性を高めるべきかに予算を投入すべき
- 侵入される事がリスクではない。侵入後に情報・データを搾取される事がリスクである
- セキュリティを理由に"ワークスタイル変革"等改革を実施しない言い訳にすべきではない

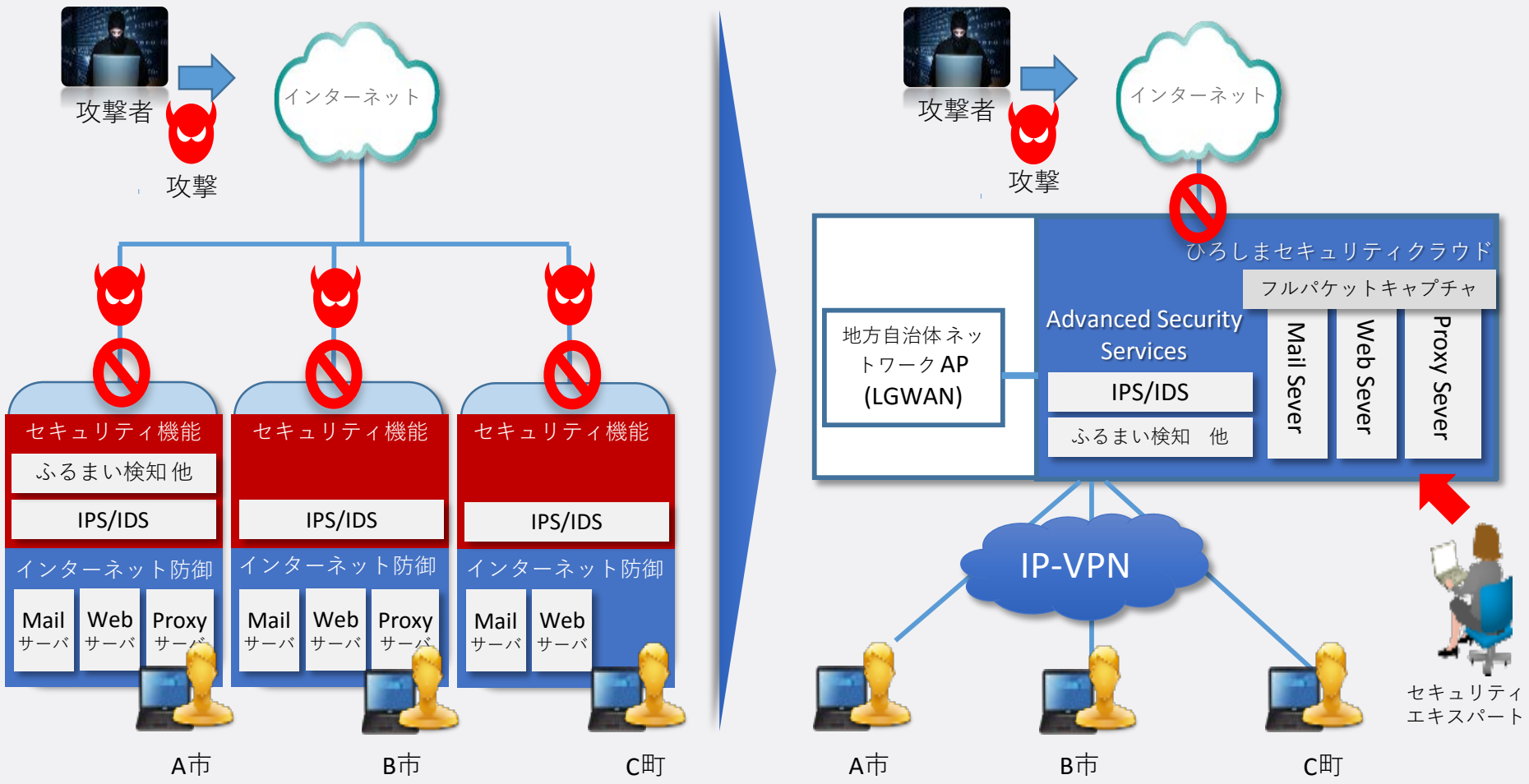
プロジェクト概要

- “セキュリティクラウド“構築プロジェクト
  - 広島県下全ての市町に対して均一のサイバーセキュリティ対策を施せるよう「セキュリティクラウド基盤」を構築する
  - CSIRT及びSOC体制を構築する

- 調達の範囲
  - セキュリティ製品群
    (FW, IPS, メールセキュリティ, Webセキュリティ,
    サンドボックス, 他)
  - SIサービス
  - 運用サービス(SOC業務含む)

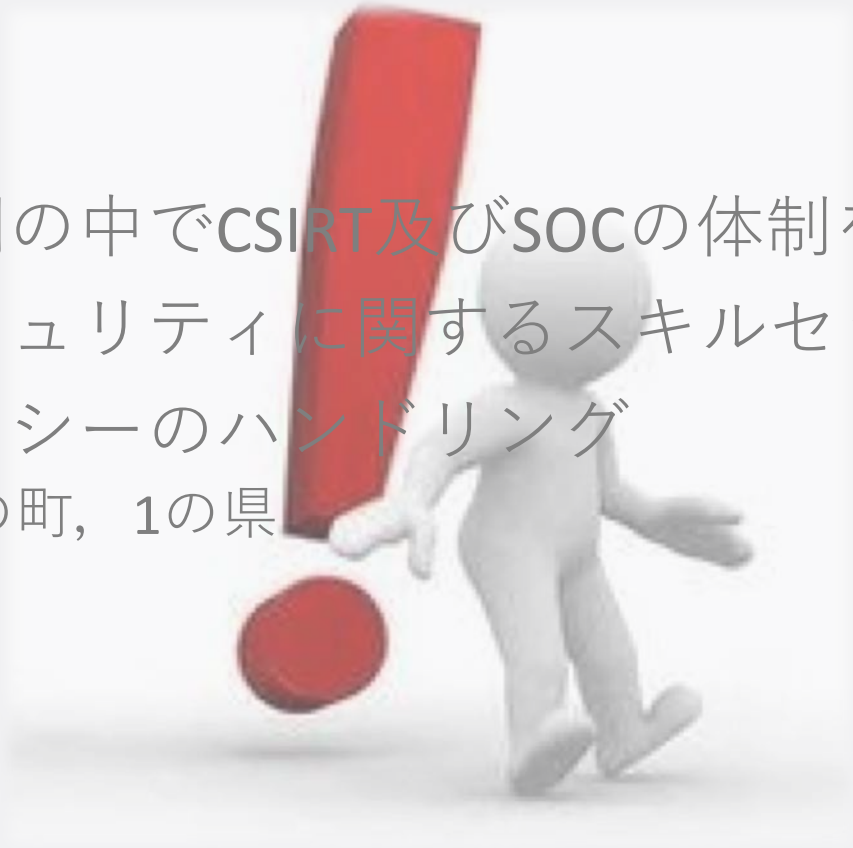


To-Be Model


攻撃者
攻撃
インターネット
セキュリティ機能
ふるまい検知 他
IPS/IDS
インターネット防御
Mail サーバ
Web サーバ
Proxy サーバ
A市
B市
C町
攻撃者
攻撃
インターネット
ひろしまセキュリティクラウド
フルパケットキャプチャ
地方自治体 ネットワーク AP (LGWAN)
Advanced Security Services
IPS/IDS
ふるまい検知 他
Mail Sever
Web Sever
Proxy Sever
IP-VPN
セキュリティ エキスパート
A市
B市
C町

チャレンジ

- 限られた時間の中でCSIRT及びSOCの体制を構築
- サイバーセキュリティに関するスキルセット向上
- マルチテナンシーのハンドリング
  - 14の市，9の町，1の県



フォーカス

- 高速かつ正確に高品質な脅威の検出と分析を実施可能なこと
- セキュリティインテリジェンスの激しい進化への対応を速やかに行えること
- すべての市町に対する一貫したサービス品質を維持すること
- 市町のCSIRTにおけるさらなる努力を最小限に抑える

KSF: 重要成功要因

- プロジェクトマネジメント
  - PMBOK + EVM
- コラボレーション
  - エネコム(エネルギアコミュニケーションズ) + シスコ
- チームワーク
  - 14 市 + 9 町 + 1 県

PMBOK: Project Management Body Of Knowledge
EVM: Earned Value Management

私たちのゴール

- 自治体のベストプラクティスになる

プロジェクト体制

- 広島県
  - 要件定義～調達
  - プロジェクトマネジメント
- エネルギアコミュニケーションズ
  - データセンター及びネットワーク
  - セキュリティデザイン及び構築
- シスコシステムズ
  - SOCデザイン及びインテリジェンス
  - ネットワーク及びセキュリティ機器

メソドロジ

- PMBOK(*1) + EVM(*2)を中心としたプロジェクト管理の徹底
- 進捗管理
  - 実績（人・時） / 計画（人・時）
  - Σ (各団体) / 計23市町+1県

*1: Project Management Body Of Knowledge
*2: Earned Value Management

WBS Dictionary

WBSディクショナリー一覧

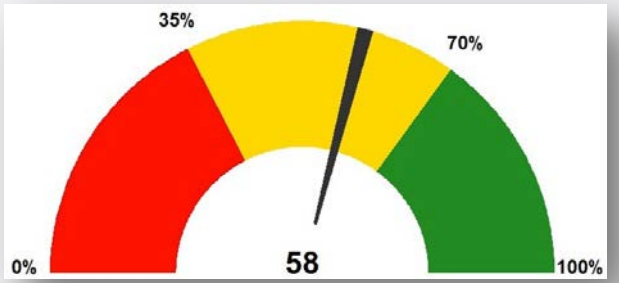
別添1

No	作業項目			成果物	作業内容	関係者	予定スケジュール		コスト見積	進捗率
							開始	終了	工数(人日)	(%)
1	プロジェクト管理	1.1 定例会議(原則毎週木曜日)		ひろしま情報セキュリティクラウド構築工程表 課題管理表、議事録、QA管理表　ほか	各管理項目について、本システムの作業全般にわたっての進捗管理、問題点の解決、状況報告等を行い、プロジェクトを完結する。	広島県／エネコム／シスコ	2016/12/22	2017/3/30	80	
		1.2 概要説明会		概要説明会資料	広島県、市町に対し、情報セキュリティクラウドの全体概要を説明する。	広島県／エネコム	2016/11/8	2016/11/8		
		1.3 キックオフ		プロジェクト実施計画書、WBSディクショナリー一覧 納品物一覧、プロジェクト管理役割分担表 情報セキュリティガイドライン　ほか	広島県とプロジェクトの進め方の情報共有を図るためキックオフを開催する。	広島県／エネコム	2016/12/22	2016/12/22		
		1.4 移行説明会		移行説明会資料	市町に対し、移行説明会を開催し理解を得る。	市町／エネコム	2017/2/3	2017/2/3		
2	参加自治体関係	2.1 詳細ヒアリング	2.1.1 ヒアリングシート記入	ヒアリングシート	市町がヒアリングシートを記入する。	市町	2016/12/22	2016/12/28	100	
			2.1.2 ヒアリングシート回収	ヒアリングシート	市町が作成したヒアリングシートを回収する。	広島県	2017/1/4	2017/1/13		
			2.1.3 構成確認、訪問打ち合わせ	ヒアリングシート	市町を訪問することで、不明点等を確認し、ヒアリングシートを完成させる。	エネコム／市町	2016/12/22	2017/1/20		
		2.2 オプション機能設計	2.2.1 エンドポイントふるまい検知	基本設計書、詳細設計書	エンドポイントふるまい検知機能を設計する。	エネコム	2017/1/10	2017/2/28	10	
			2.2.2 原本メール保管システム	基本設計書、詳細設計書	原本メール保管システム機能を設計する。	エネコム	2017/1/10	2017/2/28		
			2.2.3 Webサーバホスティング機能	基本設計書、詳細設計書	Webサーバホスティング機能を設計する。	エネコム	2017/1/10	2017/2/28		
			2.2.4 コンテンツ改ざん検知	基本設計書、詳細設計書	コンテンツ改ざん検知機能を設計する。	エネコム	2017/1/10	2017/2/28		
		2.3 オプション機能構築	2.3.1 エンドポイントふるまい検知	－	エンドポイントふるまい検知機能を構築する。	エネコム	2017/3/1	2017/6/30	40	
			2.3.2 原本メール保管システム	－	原本メール保管システム機能を構築する。	エネコム	2017/3/1	2017/6/30		
			2.3.3 Webサーバホスティング機能	－	Webサーバホスティング機能を構築する。	エネコム	2017/3/1	2017/6/30		
			2.3.4 コンテンツ改ざん検知	－	コンテンツ改ざん検知機能を構築する。	エネコム	2017/3/1	2017/6/30		
		2.4 移行設計支援		－	市町の環境等の移行設計の支援を行う。	市町／エネコム(支援)	2017/2/13	2017/4/30		
		2.5 本番切替支援		－	市町の環境等の本番切替支援を行う。	市町／エネコム(支援)	2017/4/1	2017/6/30		
3	設計関係	3.1 基本設計	3.1.1 共通機能設計	基本設計書	機器和名、命名規則等共通機能ほかの設計を行う。	エネコム	2016/12/22	2017/1/13	100	
			3.1.2 全体ネットワーク設計	基本設計書	全体ネットワーク設計を行う。	エネコム	2016/12/22	2017/1/13		
			3.1.3 全体セキュリティ機能設計	基本設計書	全体セキュリティ機能設計を行う。	エネコム	2016/12/22	2017/1/13		
			3.1.4 仮想化基盤設計	基本設計書	仮想化基盤の設計を行う。	エネコム	2016/12/22	2017/1/13		
			3.1.5 移行設計	基本設計書	セキュリティクラウド機器の参加団体受入れ設計を行う。	エネコム	2016/12/22	2017/1/13		
			3.1.6 Enewingsクラウド基盤(オプション)	－	Enewingsクラウド設計を行う。	エネコム	2016/12/22	2017/1/13		
			3.1.7 回線	－	回線設計を行う。	エネコム	2016/12/22	2017/1/13		
			3.1.8 お客様レビュー	レビュー議事録、課題管理表	基本設計の客先レビューを行う。	広島県／エネコム	2016/12/22	2017/1/13		
		3.2 詳細設計	3.2.1 共通機能設計	詳細設計書	機器和名、命名規則等共通機能ほかの設計を行う。	エネコム	2017/1/4	2017/2/3	200	
			3.2.2 全体ネットワーク設計	詳細設計書	全体ネットワーク設計を行う。	エネコム	2017/1/4	2017/2/3		
			3.2.3 全体セキュリティ機能設計	詳細設計書	全体セキュリティ機能設計を行う。	エネコム	2017/1/4	2017/2/3		
			3.2.4 仮想化基盤設計	詳細設計書	仮想化基盤の設計を行う。	エネコム	2017/1/4	2017/2/3		
			3.2.5 移行設計	詳細設計書	セキュリティクラウド機器の参加団体受入れ設計を行う。	エネコム	2017/1/4	2017/2/3		
			3.2.6 お客様レビュー	レビュー議事録、課題管理表	詳細設計の客先レビューを行う。	広島県／エネコム	2017/2/2	2017/2/2		
		3.3 運用設計	3.3.1 運用保守設計	運用設計書	システム全体の運用設計を行い、運用設計書・運用手順書を作成する。	エネコム	2017/1/4	2017/2/3	200	
			3.3.2 運用監視設計	運用設計書	運用監視設計書を作成する。	エネコム	2017/1/4	2017/2/3		
			3.3.3 セキュリティ監視設計	運用設計書	セキュリティ監視設計書を作成する。	エネコム／シスコ	2017/1/4	2017/2/3		
			3.3.4 監視パラメータ設計	監視設計書	監視パラメータ設計書を作成する。	エネコム	2017/2/3	2017/2/22		
			3.3.5 お客様レビュー	レビュー議事録、課題管理表	運用設計の客先レビューを行う。	広島県／エネコム	2017/2/23	2017/2/23		
4	構築関係	4.1 セキュリティ機器	4.1.1 構築・試験・チューニング	各機器、装置、構築手順書 サーバ設定書、付帯装置設定書 ラック配線図、物理配線図、論理配線図	セキュリティ関連機器を調達し、試験・チューニングを実施しシステムを構築する。	エネコム	2017/1/16	2017/2/17	200	
			4.1.2 機器設置				2017/2/20	2017/2/24		
		4.2 セキュリティ監視／分析装置	4.2.1 機器設置		セキュリティ監視／分析装置を調達し、試験・チューニングを実施しシステムを構築する。	シスコ	2017/2/20	2017/2/24		
			4.2.3 構築・試験・チューニング				2017/2/27	2017/3/10		
		4.3 システム監視装置	4.3.1 構築・試験・チューニング		システム監視装置の試験・チューニングを実施しシステムを構築する。	エネコム	2017/2/1	2017/3/3		
		4.4 回線	4.4.1 インターネット回線開通	－	インターネット回線を構築する	エネコム	2016/12/25	2016/12/25		
			4.4.2 メイブルネット接続回線開通	－	メイブルネット接続回線を構築する。		2017/1/18	2017/1/18		
			4.4.3 Enewingsクラウド接続回線開通	－	Enewingsクラウド接続回線を構築する。		2017/1/18	2017/1/18		
		4.5 Enewingsクラウド	4.5.1 Enewingsクラウド基盤構築	－	Enewingsクラウド基盤を構築する。		2017/1/16	2017/2/10		
			5.1.1 ネットワークサービス	単体試験設計書	ネットワークサービスの単体試験設計を行う	エネコム	2016/12/22	2017/1/13		

以下省略

WBS毎の進捗管理の考え方(1)

- Design and Documents
  - 0%: 未着手
  - 20%: 着手開始
  - 40%: ドキュメント作業開始
  - 60%: レビュー前ドキュメント完成
  - 80%: 内部レビュー済



WBS毎の進捗管理の考え方(2)

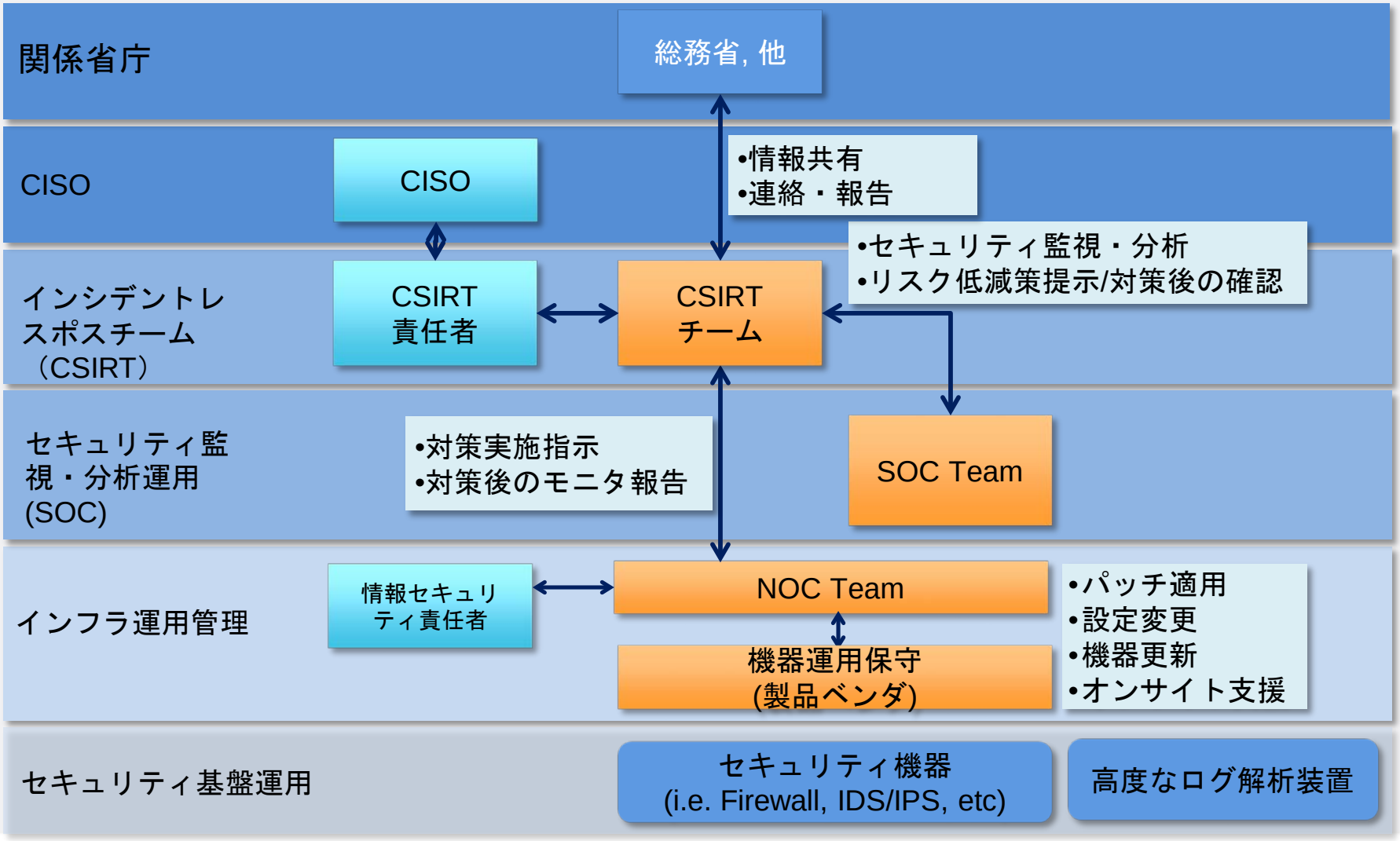
- Deploy
  - 0%: 未着手
  - 30%: セットアップ開始
  - 50%: ソフトウェアインストレーション
  - 51- 100%: パラメータセット及びカスタマイズ
    - 実績パラメータ/計画パラメータ
- Test
  - 0 – 100%: 処理テストケース / 実績テストケース

EVMによる定量化

- SPI: Schedule Performance Index
- CPI: Cost Performance Index
- 各々以下の閾値でマネジメント

SPI	CPI	状況	インパクト	アクション例
1.00 <	1.00 <	計画とおり	無し	無し
0.95 < 0.99	0.95 < 0.99	安全圏	開発チームのみで処理できる範囲	クリティカルパスのタスクでは、次のアクションを起こす - ファストトラッキング(タスクの分割, 並行処理等)
0.90 < 0.94	0.90 < 0.94	注意	**プロジェクトチーム**全体で処理できる範囲	- クラッシング(リソースやコストの追加投入等) - 残業 - 休日返上
< 0.89	< 0.89	危険	マネジメントの判断が必要	- プロジェクトチームにおける役割と権限の見直し - 要件の見直し - カットオーバー日を遅らす

運用体制


関係省庁
総務省, 他
CISO
CISO
•情報共有
•連絡・報告
インシデントレスポスチーム（CSIRT）
CSIRT 責任者
CSIRT チーム
•セキュリティ監視・分析
•リスク低減策提示/対策後の確認
セキュリティ監視・分析運用(SOC)
•対策実施指示
•対策後のモニタ報告
SOC Team
インフラ運用管理
情報セキュリティ責任者
NOC Team
機器運用保守(製品ベンダ)
•パッチ適用
•設定変更
•機器更新
•オンサイト支援
セキュリティ基盤運用
セキュリティ機器(i.e. Firewall, IDS/IPS, etc)
高度なログ解析装置

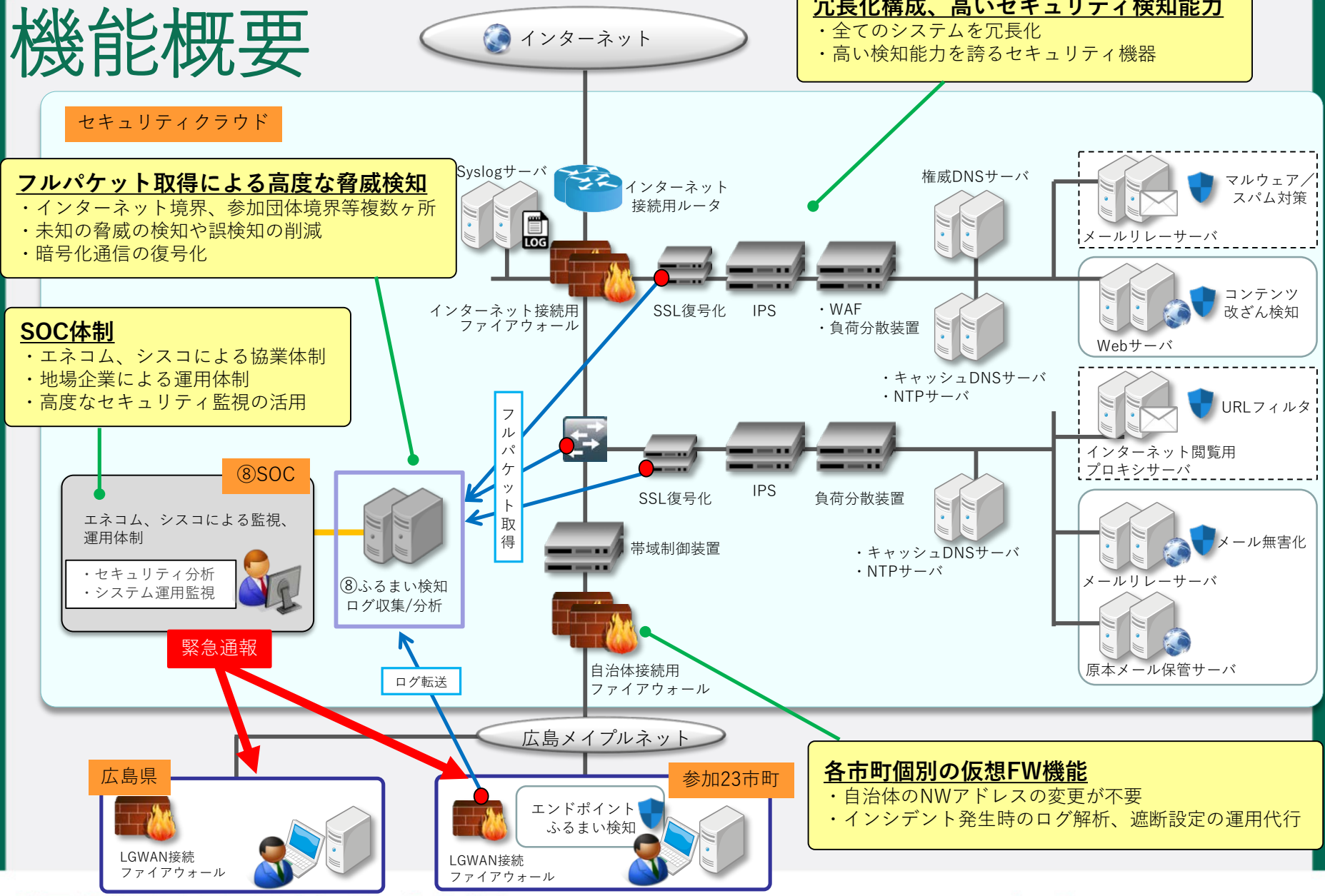
主な機能

- Why Hiroshima Security Cloud ?

求められる機能

主な機能		ポイント
リアルタイム検出	• 各種ログデータをリアルタイムで分析しインシデントを自動検出 • 自社製品以外のログに対応(Syslogプロトコル)	検知スピード
収集データの相関分析	• ログデータ及びテレメトリ、フルパケットキャプチャの相関分析によるFalse Positive の軽減 • アナリストが、原因、感染端末、実施すべき対処を具体的に提示	アラート分析精度 対応工数の軽減
顧客環境を踏まえた運用	• 重要資産や外部接続境界等の配置構成を踏まえた監視ポイントの設定とイベント検出時の優先度設計	情報資産に応じた セキュリティ対策
インテリジェンス活用	• どれくらいのセンサーで全世界のトラフィックを捕捉するか。 • 補足したトラフィックからインテリジェンス強化し既知の脅威の検出精度向上	既知の脅威への 対応
不正トラフィック解析	• テレメトリ、フルパケットを活用した統計分析、ビッグデータ解析により、不正なトラフィックを検出	未知の脅威への 対応

機能概要


インターネット
冗長化構成、高いセキュリティ検知能力
・全てのシステムを冗長化
・高い検知能力を誇るセキュリティ機器
セキュリティクラウド
フルパケット取得による高度な脅威検知
・インターネット境界、参加団体境界等複数ヶ所
・未知の脅威の検知や誤検知の削減
・暗号化通信の復号化
SOC体制
・エネコム、シスコによる協業体制
・地場企業による運用体制
・高度なセキュリティ監視の活用
Syslogサーバ
LOG
インターネット
接続用ルータ
権威DNSサーバ
マルウェア／
スパム対策
メールリレーサーバ
インターネット接続用
ファイアウォール
SSL復号化
IPS
・WAF
・負荷分散装置
コンテンツ
改ざん検知
Webサーバ
・キャッシュDNSサーバ
・NTPサーバ
フルパケット取得
URLフィルタ
インターネット閲覧用
プロキシサーバ
SSL復号化
IPS
負荷分散装置
⑧SOC
エネコム、シスコによる監視、
運用体制
・セキュリティ分析
・システム運用監視
⑧ふるまい検知
ログ収集/分析
帯域制御装置
・キャッシュDNSサーバ
・NTPサーバ
メール無害化
メールリレーサーバ
緊急通報
ログ転送
自治体接続用
ファイアウォール
原本メール保管サーバ
広島メイプルネット
各市町個別の仮想FW機能
・自治体のNWアドレスの変更が不要
・インシデント発生時のログ解析、遮断設定の運用代行
広島県
参加23市町
LGWAN接続
ファイアウォール
エンドポイント
ふるまい検知
LGWAN接続
ファイアウォール

機能一覧

＜基本機能＞

機　能	内　容
①ファイアウォール機能	自治体接続用FW, インターネット接続用FW
②メールセキュリティ機能	マルウェア検知、アンチスパム、メールリレー
③Webセキュリティ機能	URLフィルタ、インターネット閲覧用プロキシ
④侵入防止機能	マルウェア検知、IPS, IDS
⑤WAF機能	WAF, DDoS 対策
⑥DNS機能	権威DNS, キャッシュDNS
⑦時刻同期機能	NTP
⑧SOC機能	ログ収集、フルパケットキャプチャ、セキュリティ分析、ふるまい検知
＜オプション機能＞	
機　能	**内　容**
⑨エンドポイントふるまい検知機能	エンドポイントふるまい検知、遮断
⑩メール無害化機能	メール無害化、原本メール保管（メールスプール）、Webメール
⑪Webサーバホスティング機能	IaaS 提供、OS (Windows, Linux) もオプションとして提供
⑫コンテンツ改ざん検知	Webサーバのコンテンツ改ざん検知、自動修復

	職員数（利用者ＩＤ） 行政部局	ＩＤ数（メールＩＤ） 行政部局	セキュリティクラウド参加端末台数	知事・市長部局	教育委員会（学校等）	端末の種類	回線速度	URLフィルタ運用委託有無
広島市	8,527	8,353	7,500	7,500		物理端末	1Gbps （帯域保証は12Mbps）	有
呉市	2,484	2,484	600	600		仮想端末	100Mbps	無
竹原市	420	330	300	300		仮想化（サスティック） ※メモリの仮想化	100Mbps （ベストエフォート）	無
三原市	914	914	300	300		仮想（SBC）　300台	100Mbps （帯域保証）	有
尾道市	1,400	250	300	300		仮想端末	100Mbps（専用線）	有
福山市	6,769	390	5,450	450	5,000	物理端末	100Mbps （帯域保証，全二重化）	無
府中市	450	350	50	50		物理端末	市長部局：20Mbps	無
三次市	672	900	750	750		物理端末	1Gbps（ベストエフォート， 実測下り80Mbps程度）	無
庄原市	600	200	600	600		仮想環境（サスティック）	10Mbps	無
大竹市	500	35	50	50		物理端末	300Mbps	有
東広島市	994	174	2,000	2,000		仮想端末	1Gbps（ベストエフォート， FTTH4回線）	有
廿日市市	1,280	1,237	1,000	1,000		仮想端末（SBC）	市長部局：100Mbps	有
安芸高田市	555	491	100	100		仮想端末	100Mbps （ベストエフォート）	有
江田島市	504	440	100	100		仮想端末	1Gbps（ベストエフォート）	有
府中町	250	340	105	105		仮想端末（SBC）　75台 物理端末　30台	町長部局：100Mbps	有
海田町	236	330	210	210		仮想　170台 物理　40台	10Mbps（帯域保証）	有
熊野町	132	132	50	50		仮想端末	10Mbps （帯域保証，IP-VPN）	有
坂町	103	160	100	100	（250台追加の可能性あり）	仮想端末（VDI）　100台	30Mbps	有
安芸太田町	155	238	100	100		仮想端末（SBC）　90台 （VDI）　10台	1Gbps （フレッツ光　隼）	有
北広島町	469	500	430	430		物理端末	100Mbps（町長部局と教委等で共用している）	有
大崎上島町	125	55	305	140	165	仮想端末　140台 物理端末　165台	30M （島全体で300Mbps）	有
世羅町	225	44	300	300		物理端末	50Mbps	有
神石高原町	253	305	70	70		物理もしくは仮想端末	47Mbps（ベストエフォート，実測：下り10，上り1）	有
広島県	8,000	8,800	7,150	7,150		物理端末　6,700台 仮想端末 VDI　330台 SBC　120台	100M	有
計	36,017	27,452	27,920	22,755	6,705			

脅威分析のアプローチ

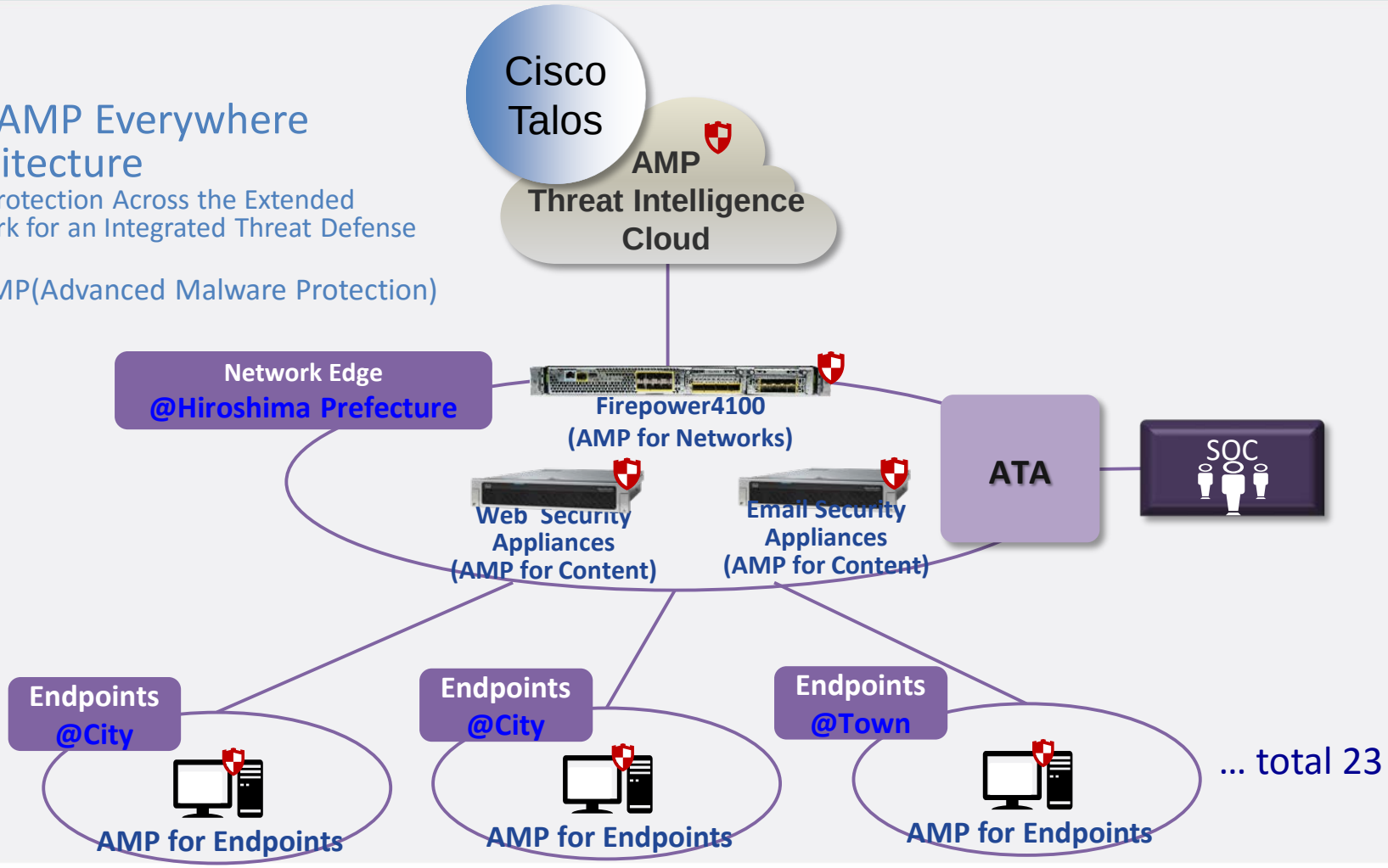
- 膨大な情報源であるメタデータ、テレメトリ、フルパケットを利用した3つの分析手法
- お互いを補完し、検出精度を向上させることが重要
- 受動的に監視するだけではなく能動的な脅威の検出を実地（プロアクティブ・スレットハンティング）

Solution Mapping on Security Cloud

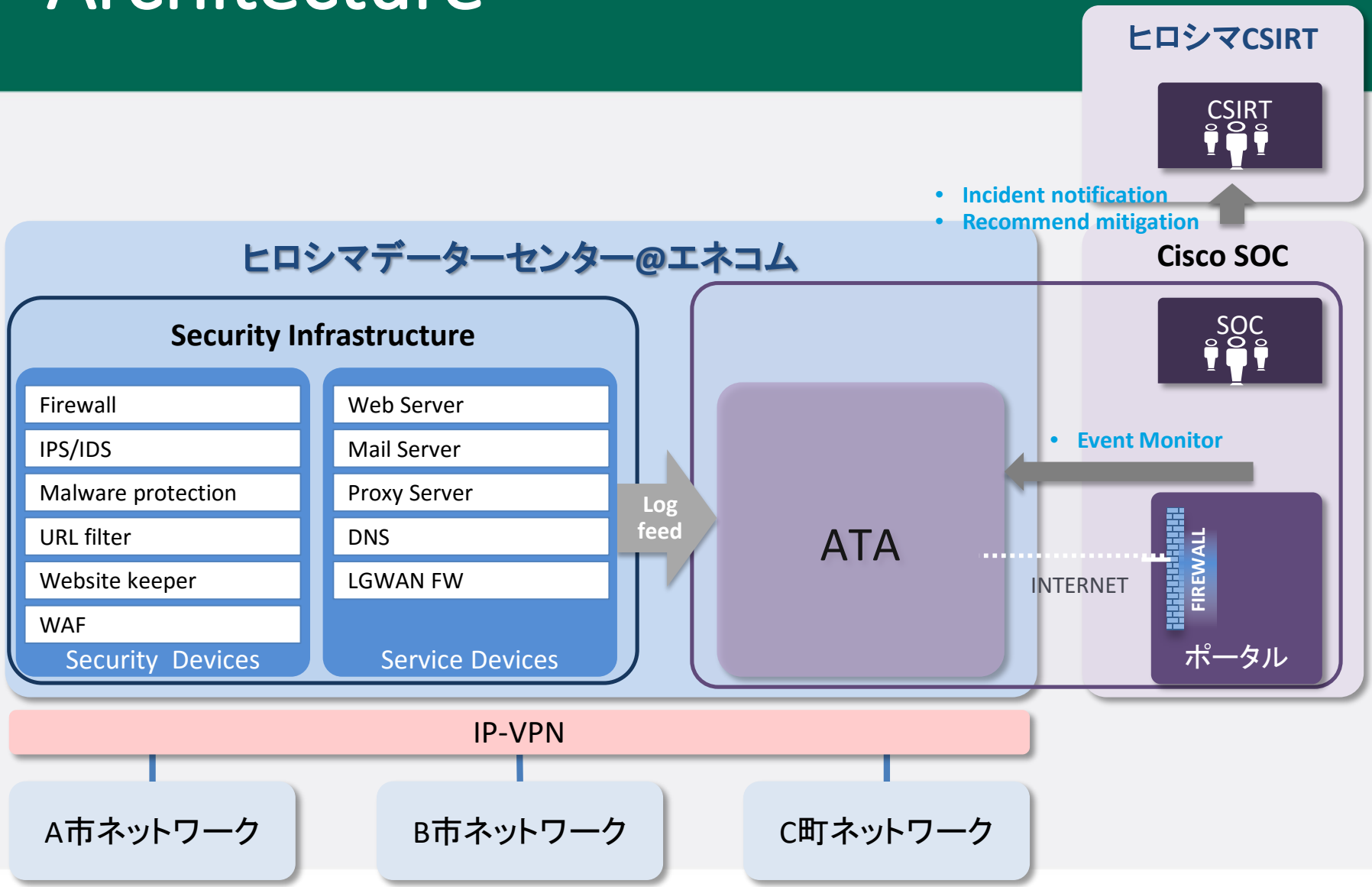
The AMP Everywhere Architecture

AMP Protection Across the Extended Network for an Integrated Threat Defense

= AMP(Advanced Malware Protection)



Architecture



Active Threat Analytics

Finally…

ファシリティ

データセンター

サーバールーム

エントランス

SOC

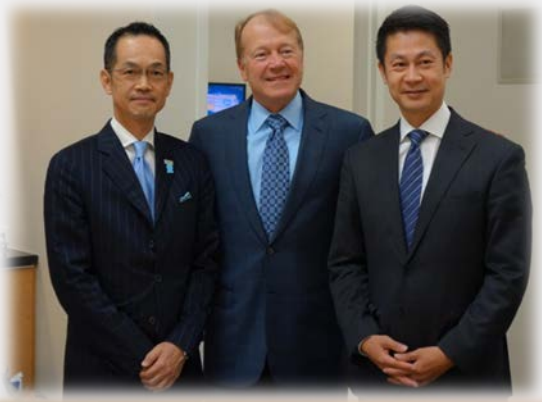
将来の展望

- 単独自治体では限界
- 都道府県単独SOCよりも地域SOCの展開
- 地域教育機関とSOCとのコラボレーション
  - 自治体も投資
- 人員の流動化
  - 産官学の協力体制の強化

謝辞

- 関係各位に深謝！

皆に感謝！



All Project Members

EneCom Team

- Satoshi Kuwagai (President)
- Makoto Ota
- Norimitsu Kawakami
- Masashi Ohkubo
- Kenjirou Komura
- Masakazu Omori
- Takuya Sakimoto
- Masayuki Tsuchie
- Thuguo Yoshiroda
- Shuuji Tahara
- Kazuhiro Tanaka
- Naoya Kadowaki
- Yoichiro Inazawa
- Yusuke Iwaki

Cisco US Team

- John Chambers (Former CEO)
- Scotty Scott (Installation)
- Ryan Morrow (Workshop)
- Dallace Butler (Workshop)
- Peter Savage (Installation)
- Bryan Doerr (PM)

Cisco Japan Team

- Masayuki Asada (AM)
- Ryo Chinen
- Daisuke Naya
- Akifumi Ishikawa (Investigator)
- Setsuko Yagi (PM)
- Yoko Uchida (PM)

Hiroshima Pref. Team

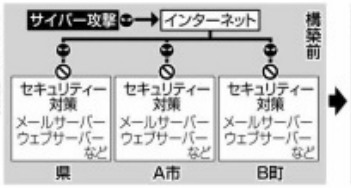
- Hidehiko Yuzaki (Governor)
- Nobuyoshi Sakamoto
- Akitoshi Murakawa
- Teruhiko Sumioka
- Yoshi Kuwahara

中国新聞　2017年（平成29年）7月20日（木曜日）　中国総合（24）

集中管理 ハッカー撃退

広島県 新システム運用開始

米団体、統括者を表彰



ひろしま情報セキュリティクラウド

広島県内の市町が個別に管理していたインターネットの接続環境を集約し、サイバー攻撃を迅速に検知して防御する県のシステム「ひろしま情報セキュリティクラウド」の運用が今月、始まった。システムの先進性や堅固さが高く評価され、プロジェクトを統括した桑原義幸・県情報戦略総括監（59）が、情報セキュリティー分野で世界的に権威がある米国の団体「ISCスクエア」からアジア太平洋地区の功労者として表彰された。（胡子洋）

桑原義幸氏

広島県は、16年9月に地場の情報通信会社を事業者に選定し、桑原氏が統括。構築したシステムはネットワーク上の通信データが可視化できる機能が特徴で、攻撃の迅速な検知や正確な分析が可能になった。未知で高度な脅威に対抗する分析機能も備えるなど独自性も打ち出した。

今月までに県と県内23市町のデータ移行が完了し、運用がスタート。桑原氏は「自治体は個人情報を多く持ち、サイバー攻撃の標的になりやすい。精度の高いセキュリティー対策が欠かせない」と強調する。

桑原氏は大阪府出身。情報通信企業勤務を経て、07年に経営コンサルティング会社を設立。11年4月、県の情報化統括責任者（CIO）として非常勤で採用された。その後も専門家として、他の自治体や企業のIT戦略や政策立案に関わったり、原子力規制委員会の「最高情報セキュリティアドバイザー」を兼務したりしていた。しかし、16年6月、他の役職を全て辞め、常勤の現職に就いた。

ISCスクエアは1989年に設立。情報セキュリティーの専門性に関する国際資格CISSPを創設し、世界160カ国の約10万人を認定している。年1回、米国、欧州など地区ごとに功労者を表彰しており、アジア太平洋地区で自治体職員の受賞は初という。桑原氏もCISSPと職員を含め、県内のプロフェッショナルなIT人材の育成に力を入れたい」と取得しており、「今後は県

(ISC)² Secure Events

SECURETOKYO 2017