自治体が取り組むべき
新たな情報セキュリティ対策

平成２８年１１月１日
地域情報化セミナー in KUMAMOTO

佐賀県情報監／港区情報政策監　川口　弘行

※本資料は登壇者が所属する機関の意見を代表するものではありません。

本日お話すること

- 番号制度に基づく情報連携開始が目前に迫る中で、行政機関における情報セキュリティに関する課題は、緊急性・重要性ともに高まりつつある状況です。

- 一方、これまでのセキュリティ対策は限られたリスク想定の中で行われたものであり、ソリューション偏重の傾向も見受けられます。

- 今回は佐賀県や他団体における話題を踏まえて、自治体が取り組むべき新たな情報セキュリティ対策について解説します。

自己紹介

川口　弘行（かわぐち・ひろゆき）

博士（工学）　技術経営修士（専門職）
公認情報システム監査人（CISA）
行政書士　ITコーディネータ

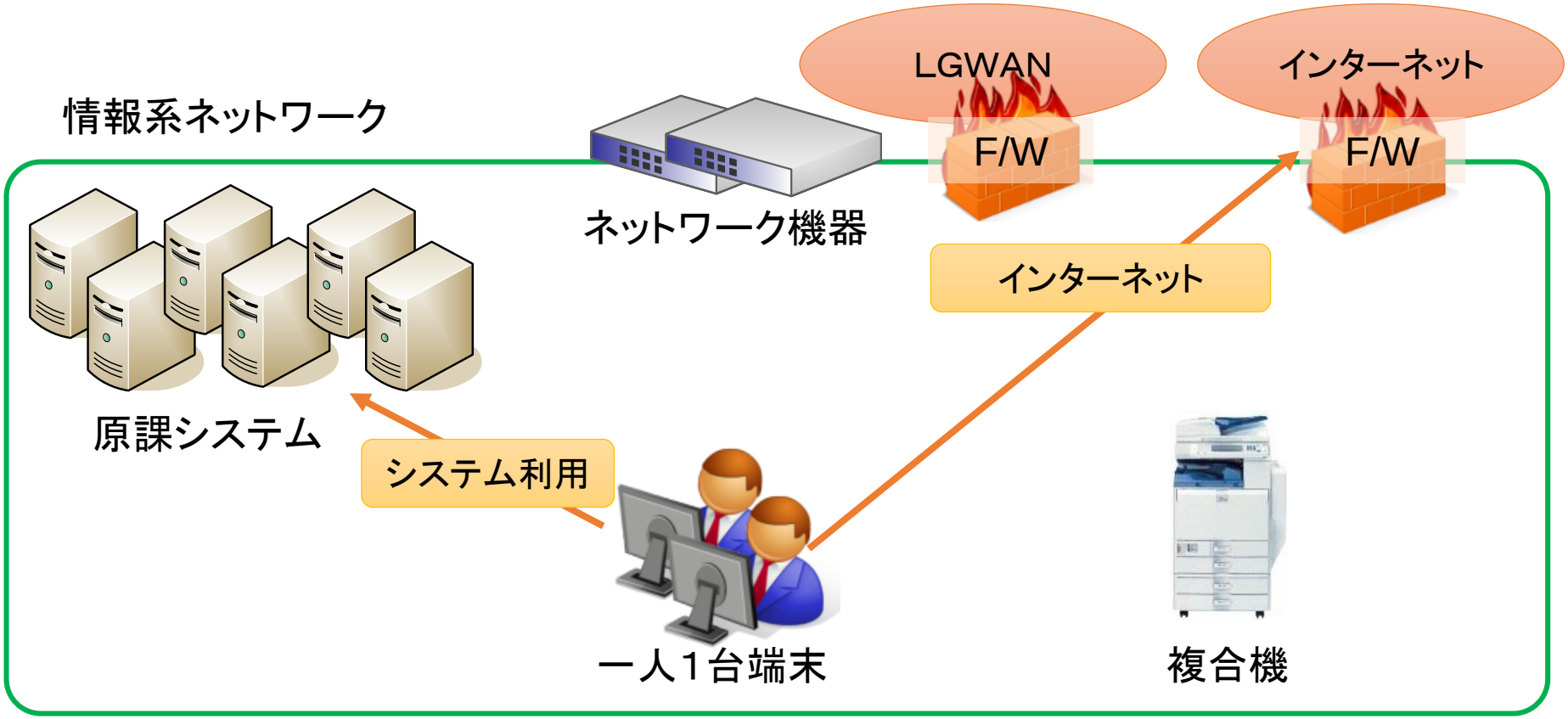
専門分野：電子政府・電子自治体、オントロジ、情報社会学

1996年5月	行政書士登録
2003年8月	電子申請推進コンソーシアム　岐阜県実証実験WG主査
2005年2月	JIPDEC JESAP 電子申請タスクメンバ
2009年4月	高知県庁 専門企画員（CIO補佐官）
2013年4月	港区情報政策監（CIO補佐官）（現職）
2013年4月	経済産業省CIO補佐官・特許庁上級システムアドバイザ
2015年4月	佐賀県庁 情報企画監（情報監）（現職）

自治体における去年までのセキュリティ対策

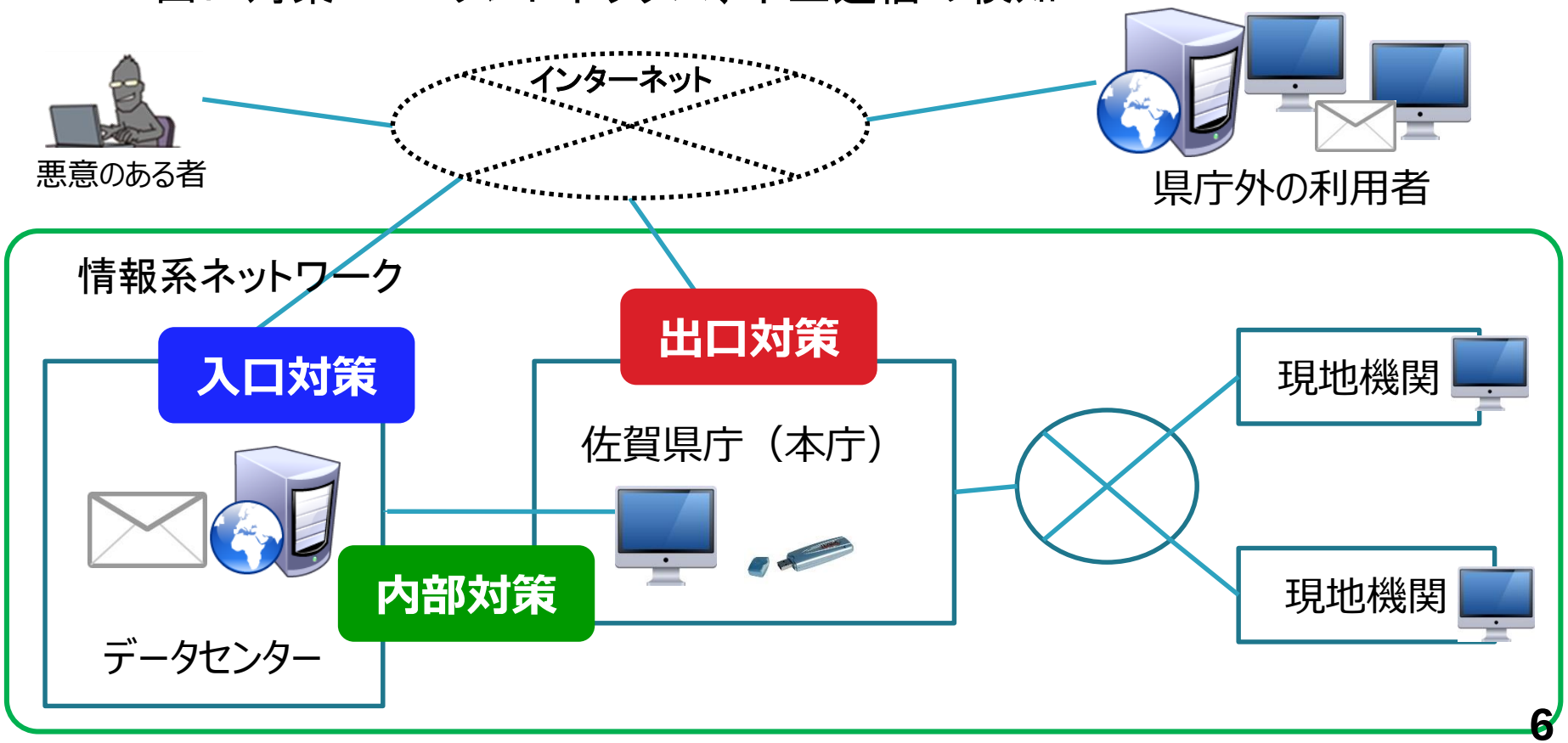
都道府県の場合（ネットワーク構成）

- 全システム及び端末が同一のセキュリティレベル上に配置
- インターネットは、一人1台端末を用いて利用（Web閲覧等）
- 税・福祉に関するシステムも、一人1台端末で業務を実施



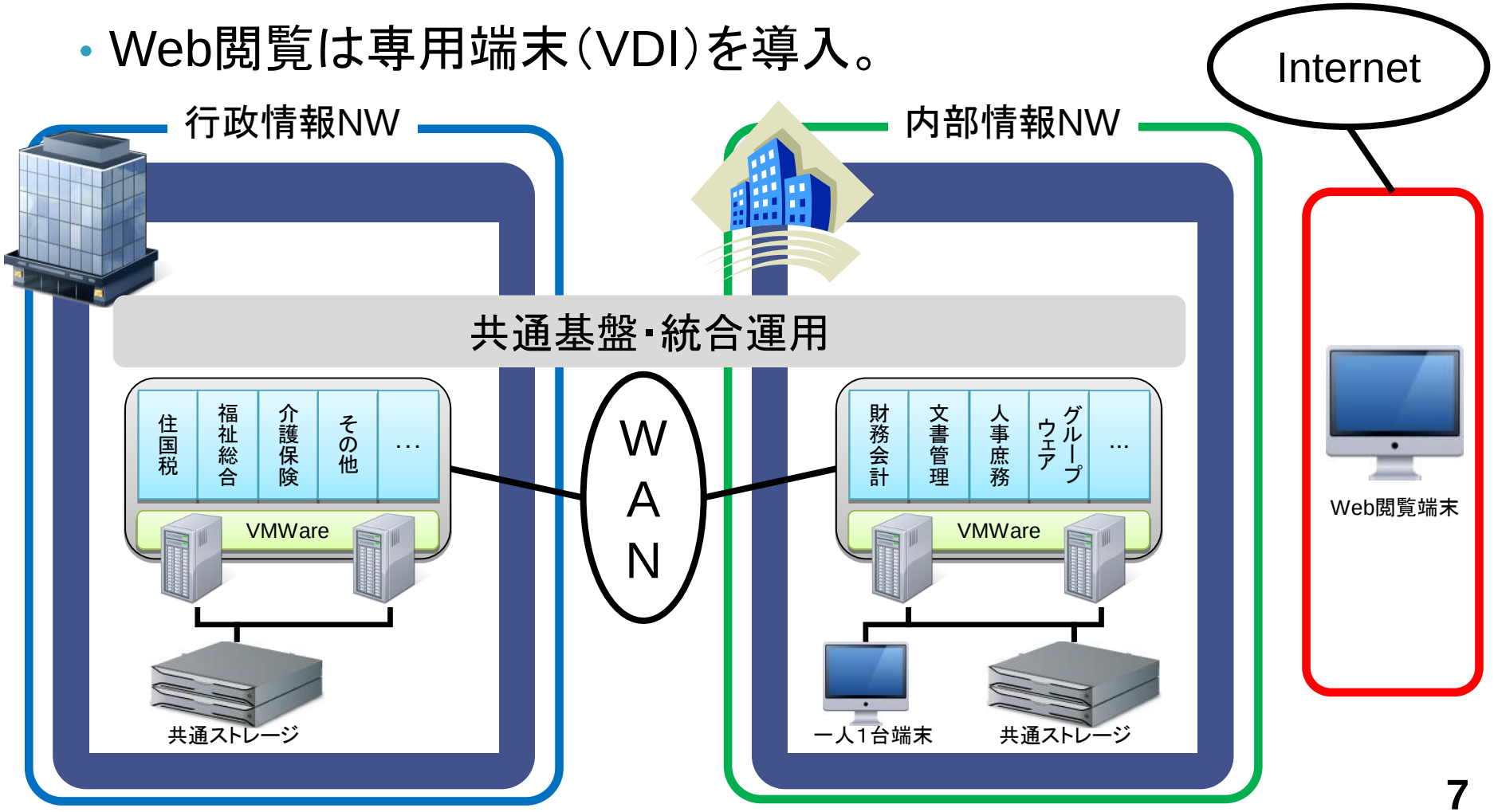
都道府県のセキュリティ対策

- 単一ネットワークを前提とした包括的な対策
  - 入口対策 → IPS/IDS、メール送受信経路の情報漏えい対策
  - 内部対策 → ファイルの暗号化、アンチウイルス
  - 出口対策 → サンドボックス、不正通信の検知



区市町村のセキュリティ対策

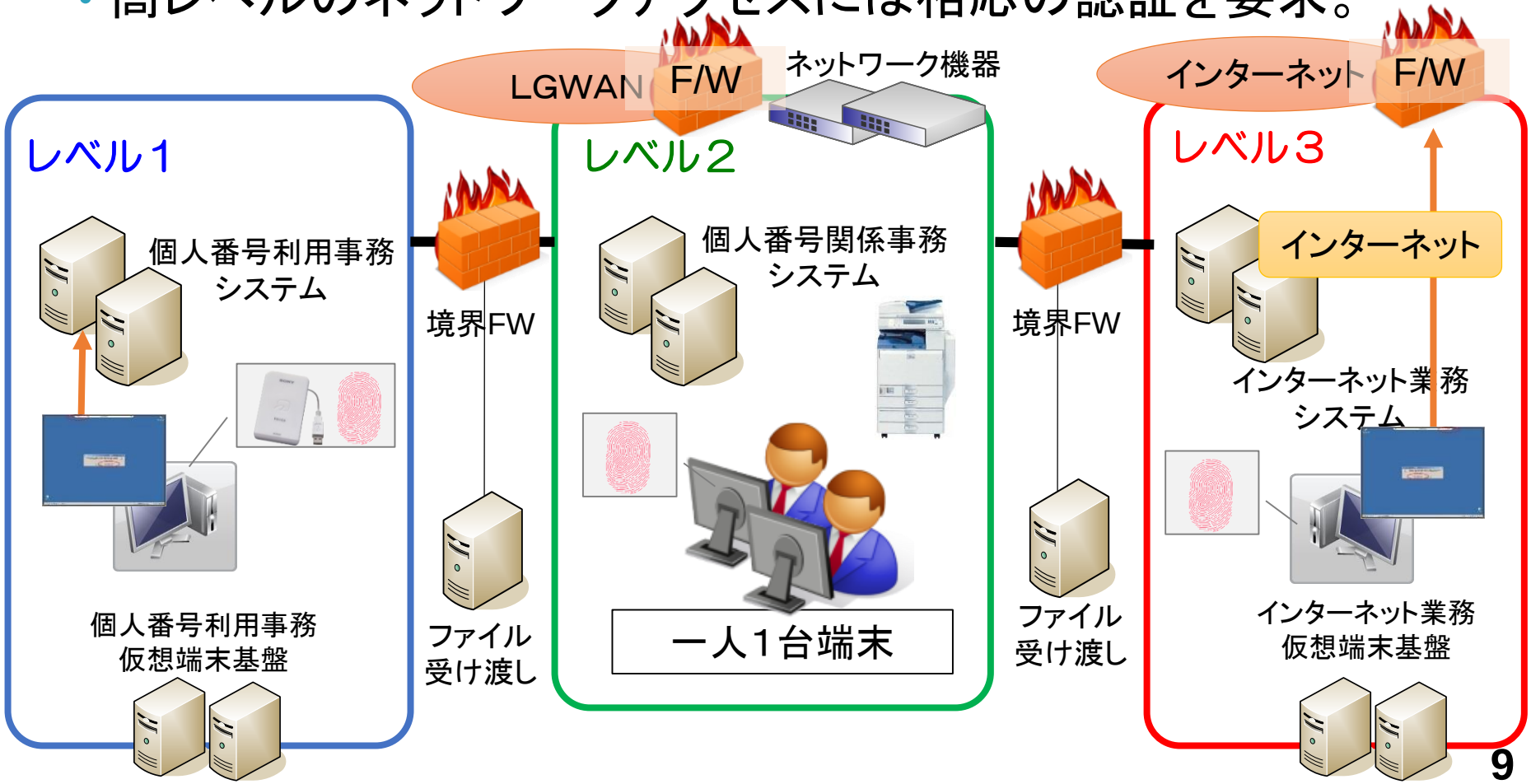
- 行政情報NW、内部情報NW、インターネット接続の
  3つのネットワークで構成されている。
- Web閲覧は専用端末（VDI）を導入。



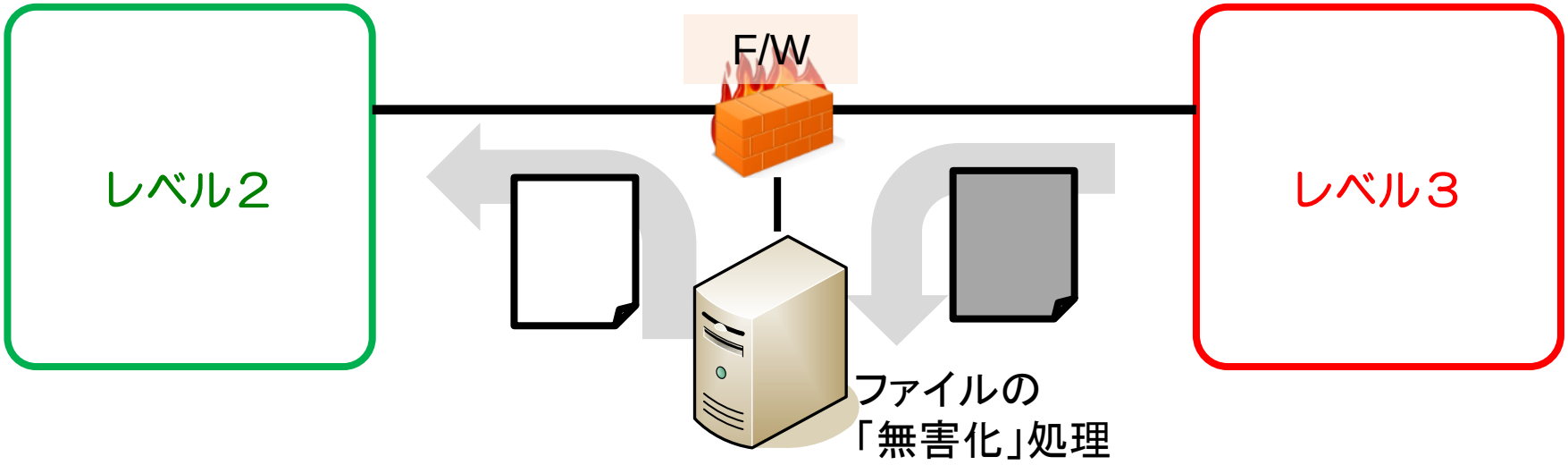
自治体情報セキュリティ強靭化

庁内ネットワーク分離と認証強化

- 庁内ネットワークを3つに分離。
- ネットワーク間のファイル受け渡しを制限。
- 高レベルのネットワークアクセスには相応の認証を要求。



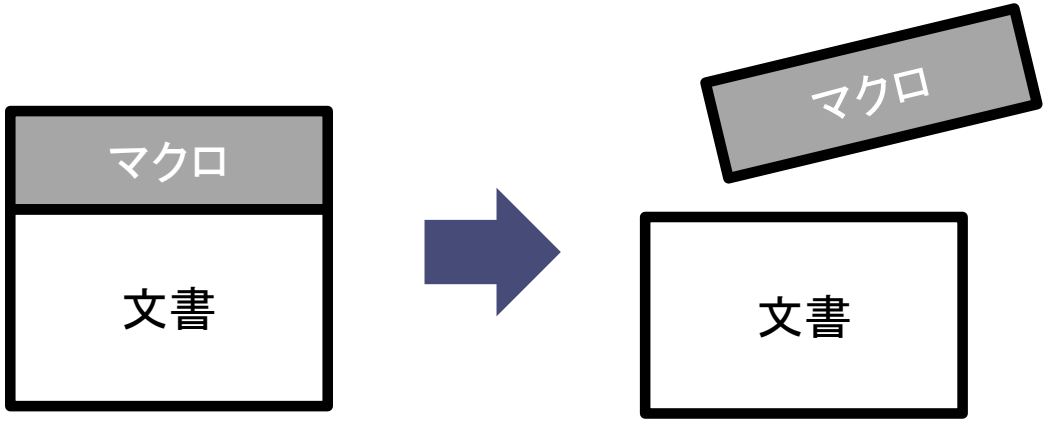
ネットワーク間のファイル受け渡し問題



- 総務省が示す要求事項（要約）
  - ネットワーク間の通信経路を分割すること。
  - 通信する場合には、ウイルス感染のない無害化通信を図ること。
- 自治体側のポリシーにより考慮すべき事項
  - 情報の外部流出のリスクに備え、低レベルネットワークへのファイル受け渡しを制限する。
  - 運用の実態を踏まえ、高レベルネットワークへのファイル受け渡しは管理の上、許容する。

ファイルの「無害化」 → 「サニタイズ」

- 「無害化」の定義を曖昧にした結果、解釈が多様化。
  - アンチウイルス → サンドボックス（振る舞い検知） → ？
  - 「ウイルス感染のない無害化通信」を厳格に実現する手段として、新たに「サニタイズ」という概念が示される。
- サニタイズ
  - 「動作するプログラムがなければマルウェアも機能しない」というシンプルな考えに基づき、文書ファイルの中からプログラム的要素（マクロなど）を削ぎ落とす仕組み。



「サニタイズ」ソリューションの課題

- 製品の選択肢が極端に少ない
- 価格が高い
- サニタイズの精度はよくわからない
- あらゆるファイルをサニタイズできるわけではない

- 国とベンダーの狭間で全国の自治体は困惑している

- サニタイズ製品を自分で開発して、全国の自治体に無償で配布しよう！
  - 先月、「サニタイザー」という製品を発表しました。

サニタイザー　デモ動画　（約4分）

Hiro KAWAGUCHI Laboratory

ファイル無害化アプライアンス

サニタイザー

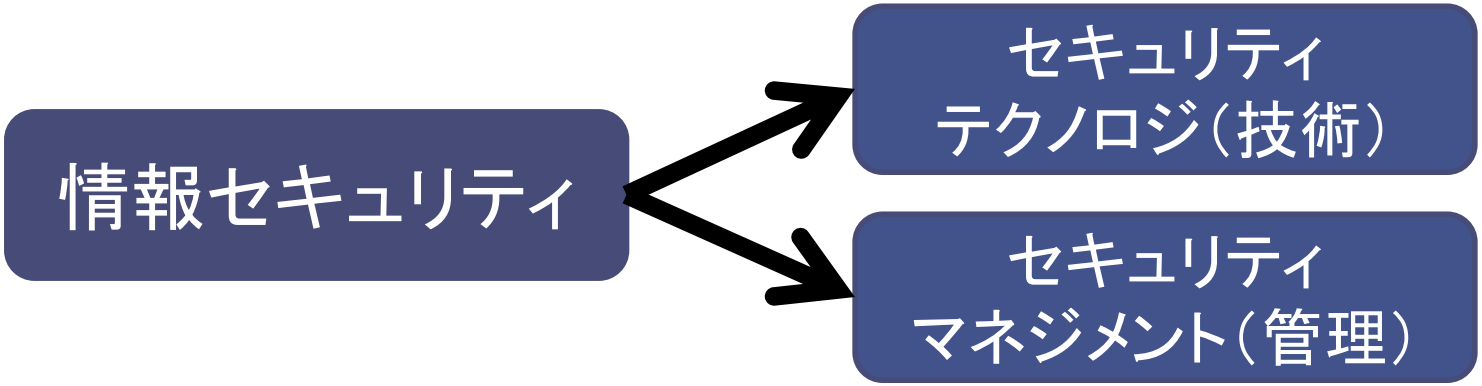
Sanitizer

YouTube　サニタイザーデモ　検索

サニタイザー紹介Webページ　http://www.kawaguchi.com/works/?p=1903

情報セキュリティ業界に対する素朴な疑問

問1：



- セキュリティテクノロジは陳腐化が早い。
  - 常に最新動向をキャッチアップしなければならないため、より多くの資源を投入したものが優位性を発揮しやすい。
  - また、常に自らを大きく見せないと他社と差別化できない。
- セキュリティマネジメントの主体はベンダーではない。
  - マネジメントの領域に参入するためには、顧客の価値観を転換させる必要があるため、現状否定から入る。

問2:

- 「セキュリティ上の脅威をあおり、顧客を不安にさせて、
  高価なセキュリティソリューションを売りつける行為」は、
  企業の論理から見れば正当とも言える。

更問:セキュリティベンダーと顧客との間には、
「情報の非対称性」があるにも関わらず、
後出しジャンケンでしか重要なことを言わないのは
なぜか。

- 最先端技術が詰まった機器は本質的に情報の非対称性を
  内包するもの。
- 一方、そのような人や事業者を「公平な専門家」として
  扱うことの方が問題ではないか。→ 顧客側の問題か？

仮説：情報セキュリティを取り巻く現状は、

- 大多数の人の本音
  - セキュリティ対策として、主体的にセキュリティマネジメントに取り組むことが難しい。（取り組む価値が理解できない）
  - そのため、セキュリティテクノロジの問題にすり替えた上で「モノ」の対策をすることで、手っ取り早く安心したい。
  - 目に見えて効果のあるモノが望ましい。論理的な対策より物理的な対策（ex.ネットワークの分離）を好む。
  - 頼る相手がいないので、多少胡散臭くてもベンダーに依存。一度依存すると、確証バイアスにより常習性が高まる。

→　ただ、この「本音」を責めるべきではない。理由は後ほど。

佐賀県
学校教育ネットワーク
不正アクセス事件

事件の概要

- 何が起こったのか
  - 佐賀県学校教育ネットワークが不正アクセスを受け、生徒の個人情報を含む学校情報が窃取された。
- 被疑者
  - 17歳少年と16歳少年　他数名が犯行事実の一部を共有。
- 被害の内容
  - SEI-Netへの不正アクセスにより、利用者IDを窃取。
  - 校内LANのファイルサーバへの不正アクセスにより、学校情報を窃取。
    - マスコミでは「情報流出」とされているが、正確には「不正アクセス」と「窃取」に留まる。（学校情報は被疑者から不特定多数の外部には拡散していない状況）

教育庁への併任／第三者委員会設置

- 教育庁教育総務課に併任発令（7月13日付）
  - 原因究明、再発防止のための具体的な作業に着手する。

- 佐賀県学校教育ネットワークセキュリティ対策検討委員会（第三者委員会）設置（8月16日）
  - 8月16日　第1回委員会
  - 9月14日　第2回委員会
  - 10月13日　第3回委員会
  - 10月27日　提言内容報告

（写真出典：朝日新聞デジタル　http://www.asahi.com/articles/ASJ8J4RRTJ8JTTHB006.html）

事件発生の要因(私見)

- セキュリティの脆弱性
  - SEI-Netに脆弱性はあったものの、事件との関係は薄い。
  - 内部からの不正を想定しておらず、セキュリティ機器を導入することで、外部からの脅威に対する「安心」を買っていた。
- システムの運用管理
  - 管理者パスワードを窃取されたことが不正アクセスの起点。パスワードの管理が杜撰だった。
  - 特定の個人や組織の責任ではなく、「統制力を維持させる仕組み」が必要だった。
- 不正アクセス後の対応
  - 被疑者特定までは、委託先事業者の犯行という想定。
  - そのため、再発防止策を委託先事業者に依頼することが困難だった。

第三者委員会からの提言（予想）

「必要なのはわかりやすい『模範解答』ではなく、
『自ら考え、行動する力』だ」との提言ならば、
それは新しい教育の在り方と符合するところが多い。

佐賀新聞 LIVE　10月14日（金）　今日の天気予報　電子版会員　紙面を見る　記事データ

トップ　佐賀　全国・世界　文化・芸能　特集・連載・オピニオン　サガン鳥栖　写真館

現在位置：トップ » 佐賀ニュース » 行政・社会 » 不正アクセス検証第三者委　教育、管理強化提言へ

シェア 19　ツイート　G+1 0　B!　印刷

不正アクセス検証第三者委　教育、管理強化提言へ

2016年10月14日 09時06分

佐賀県の県立中学、高校の教育情報システムが不正アクセスされた事件を検証する第三者委員会「県学校教育ネットワークセキュリティ対策検討委員会」（委員長・内田勝也情報セキュリティ大学院大学名誉教授）は１３日、提言書をまとめる最後の会合を開いた。県教委や学校などにセキュリティー文化を醸成する教育の実施などを盛り込む。１０月下旬に正式決定し、公表する。

会合は非公開。終了後に内田委員長は、事件の背景などを踏まえ「技術で全てが解決するものではない」と述べ、改めて管理運用面に問題があったことを強調した。

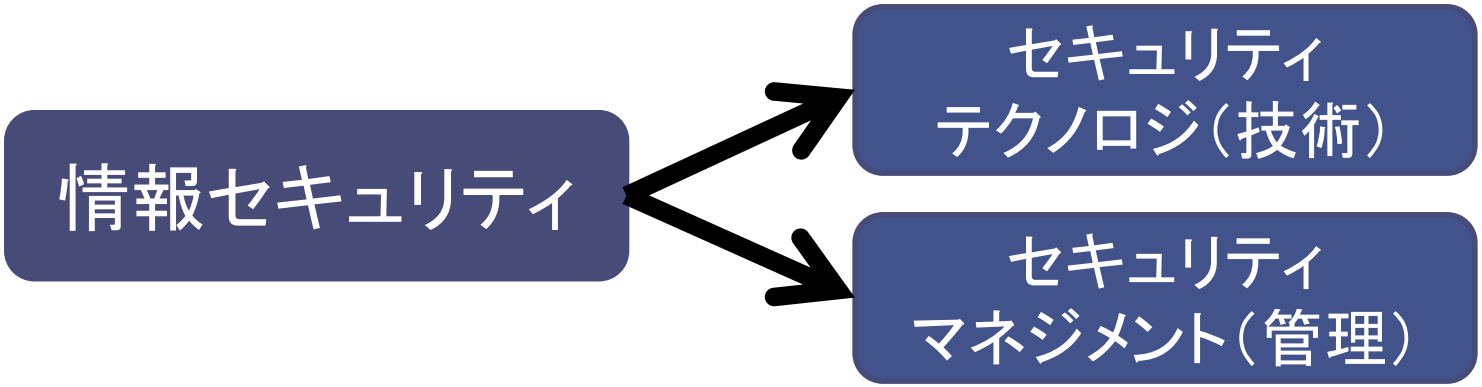
ここ重要！

提言書ではパスワードの管理や重要データの保管、組織体制など、セキュリティーを徹底する方法について一定の方向性を示した上で「県教委に考えてもらうような内容になる」と説明した。

出典：佐賀新聞LIVE http://www.saga-s.co.jp/news/saga/10101/365853 2016.10.14閲覧

新たなセキュリティ対策

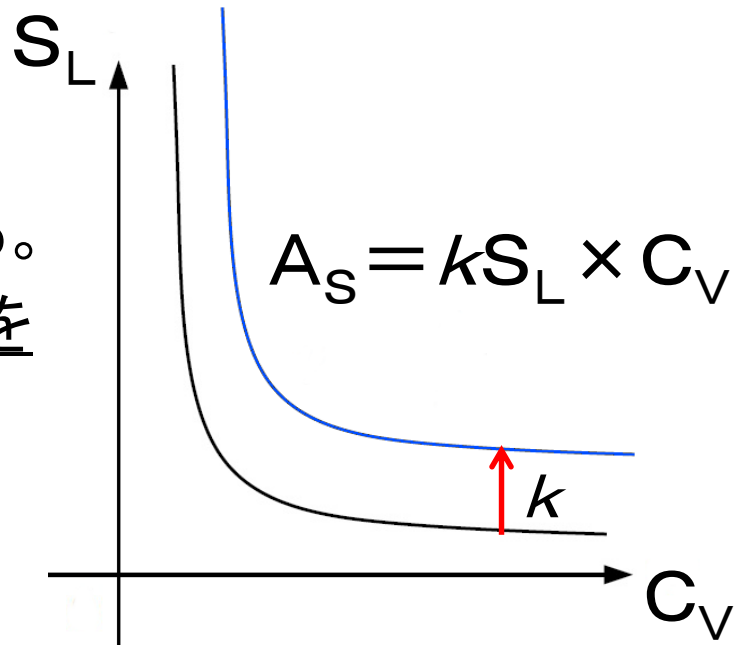
情報セキュリティの要素を思い出してみよう



- 佐賀県学校教育ネットワークの事件は、セキュリティテクノロジ（特にソリューション）に偏重した結果、セキュリティマネジメントが空洞化したことが要因。
- つまり、テクノロジはマネジメントの代替にはならない。
  - と、わかっていても、それを断罪することは、この問題の本質的な解決にはつながらない。
  - そこで、セキュリティをさらに要素分解して考えてみよう。

セキュリティテクノロジを定式化してみよう

- セキュリティの強固さ（S_L）と利便性（C_V）の関係
  - 一般的に相反する。
  - 例えば、ネットワーク分離することは有効だが、一方で分離したネットワーク間の情報の受け渡しに制限を受ける。
  - 総量はセキュリティ施策で保護すべき対象の価値（A_S）と同等であると仮定する。
  - セキュリティソリューションを導入することで、kの分だけセキュリティの強固さが高まる。
  - 保護すべき対象の価値（A_S）をいかに低く抑えられるかで、コスト、強固さ、利便性を両立させることができる。



セキュリティマネジメントを定式化してみよう

- セキュリティマネジメントとは、リスクマネジメントの一種にすぎない。
- 一般的なリスクマネジメントの関係は次のとおり。

保護すべき対象の価値（A_S）≒リスクの規模
＝リスク発生確率（P）×発生した場合の影響（E）

- 発生確率（P）の評価ができず、P=1として悲観するか、P=0に向けた無謀な投資を行おうとしている。
- リスクの規模を一定レベルで受容できるようにするためには、保護すべき対象の価値（A_S）に応じた発生確率（P）を選ぶ（ex.セキュリティソリューションの選定）必要がある。

新たなセキュリティ対策

- 情報資産の分類とゾーニング
  - 情報資産をその重要性に応じて分類する。
  - 物理領域（庁舎や執務室）、論理領域（ネットワーク、情報システム）をゾーニング（レベル分け）する。
  - 分類した情報資産を各ゾーンに配置する。
- ゾーン毎のセキュリティ施策
  - 情報資産の重要性＝ゾーン毎のセキュリティ施策を検討し、適用する。
- 絶対的な情報資産量とその価値の低減を図る
  - 無用な情報は保有しない。

全然新しくない？

ベストプラクティスを疑う

**情報セキュリティはベストプラクティスよりも
セオリーの方が重要**

- 総務省のセキュリティ強靭性モデル
  - 分析の手順が示されていたはず。（分析しましたか？）
  - 佐賀県はこれを忠実にやった上で、県の実態に則した設計を進めていた。
- WHYを示さないで、WHATやHOWを強制するべきではない
  - この場合のWHYとはセオリーに基づいて自らが考えたもの。
  - 「セキュリティ教育」とはこのWHYを考える能力育成のこと。
  - WHAT、HOWを先行させると、テクノロジ偏重を誘発する。

どうもありがとうございました

佐賀県
kawaguchi-hiroyuki@pref.saga.lg.jp

港区
hiroyuki-kawaguchi@city.minato.tokyo.jp