仮想モデル企業

ECサイト企業

ECサイト企業概要

【会社のビジネス概要】
・健康食品の開発・製造、販売まで行う。
・店舗は持たず、Webでネット販売を行っている。

従業員	300名
売上	100億

企業IT活用方針	・IT活用に積極的でクラウド利用
情報セキュリティポリシー	・Pマークを取得しているが、PCIDSSは未対応
体制	・情報システム部は存在する ・組織横通しの情報セキュリティ委員会、SOC、CERT機能はない ・個人情報管理委員会はある ・危機管理体制はあるが、製品問題、特許、従業員の就労問題、災害対策が主
役割	・CIO、CISOが不在、個人情報管理責任者は情報システム部長
経営者	・IT投資は行う ・情報セキュリティ対策の必要性は理解、現状および何から、どこまで着手すべきか把握できていない ・他社の対策状況を気にする
情報システム部門	・主業務はアプリ開発、それに伴うサーバ、DB構築も行うが、主に委託者が実施 ・担当社員は5名 ・ネットワーク技術者はいない（知識が少ない）

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

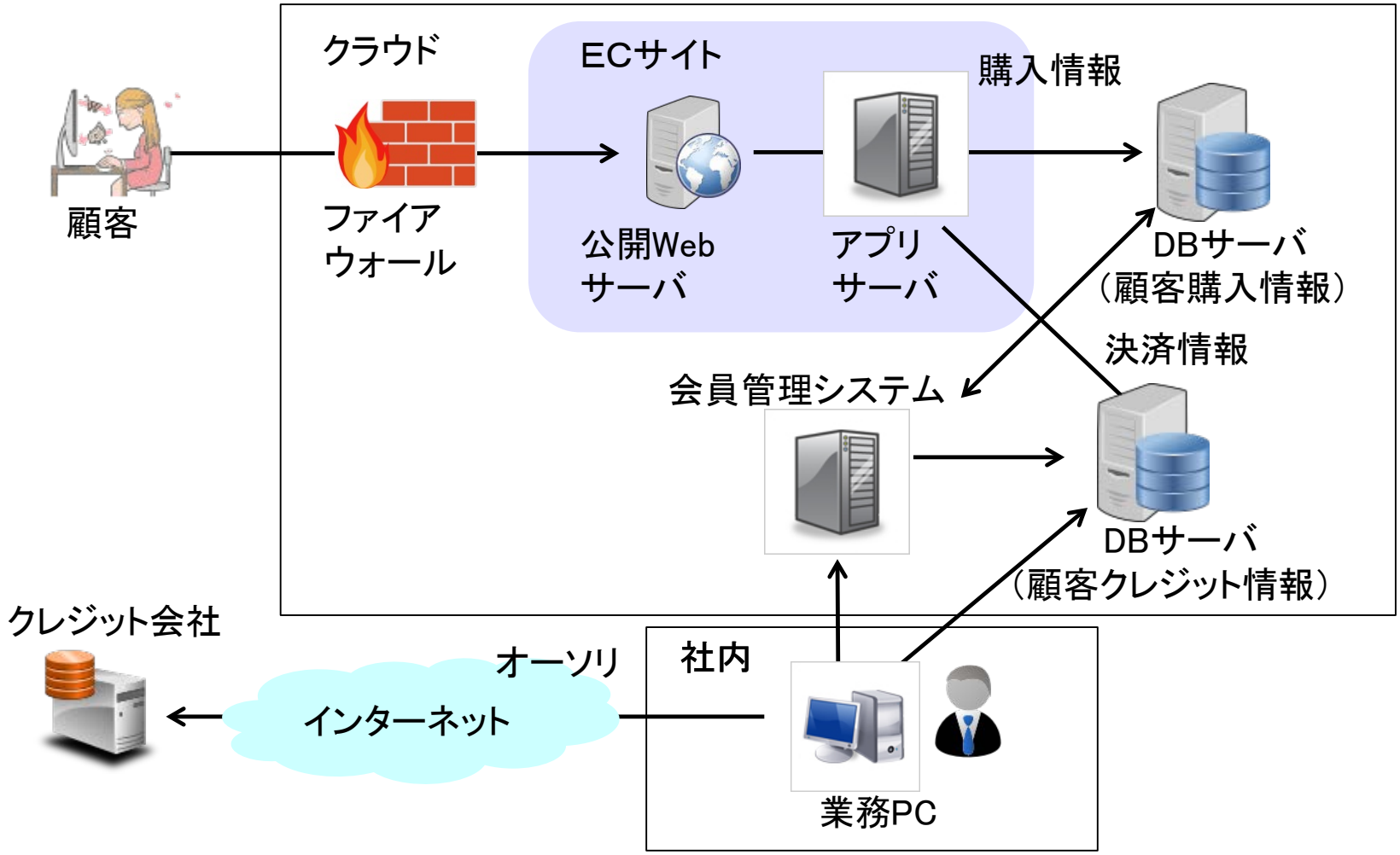
ECサイト企業のIT関連の詳細

【会社のビジネス、システム詳細】

・クラウドでECサイトを構築
・FWはクラウド事業者提供のものを利用、設定はユーザ毎に可能だがログはなく、設定の見直しをしていない
・オープンソースを利用しWebサイトを構築
・ECサイトでのクレジット決済を提供、顧客が入力したクレジット情報、セキュリティコードを保存
・電話注文でもクレジット決済が可能
・会員管理のシステムを保有、会員管理システムもクラウドに構築、インターネットからはアクセス不可
・クレジット情報は、会員情報とは別のDBに保管
・担当社員は、会員情報、クレジット情報に会員システム経由にアクセス
・会員情報、クレジット情報にアクセス可能な業務PCはインターネットには接続しない
・電話注文でのクレジット決済は上記業務PCによりインターネット経由でクレジット会社にオーソリのため接続する
・上記PCのインターネットによるシステム的な接続制限は、クレジット会社以外無し
・脆弱性検査、ペネトレを実施したことはない
・ECサイト、会員管理システム、DBサーバ、業務PCにパッチは適用しないが、ウィルス対策ソフトは導入、手動アップデート
・ ECサイト、会員管理システム、DBサーバへの社員や管理者のアクセスログは取得しているがチェックしていない
・ログをsyslogサーバなどで保全しておらず、保存期間も各サーバのHDD容量に依存
・開発システムは運用システムとは別であるが同じネットワークに設置、テスト用データを利用

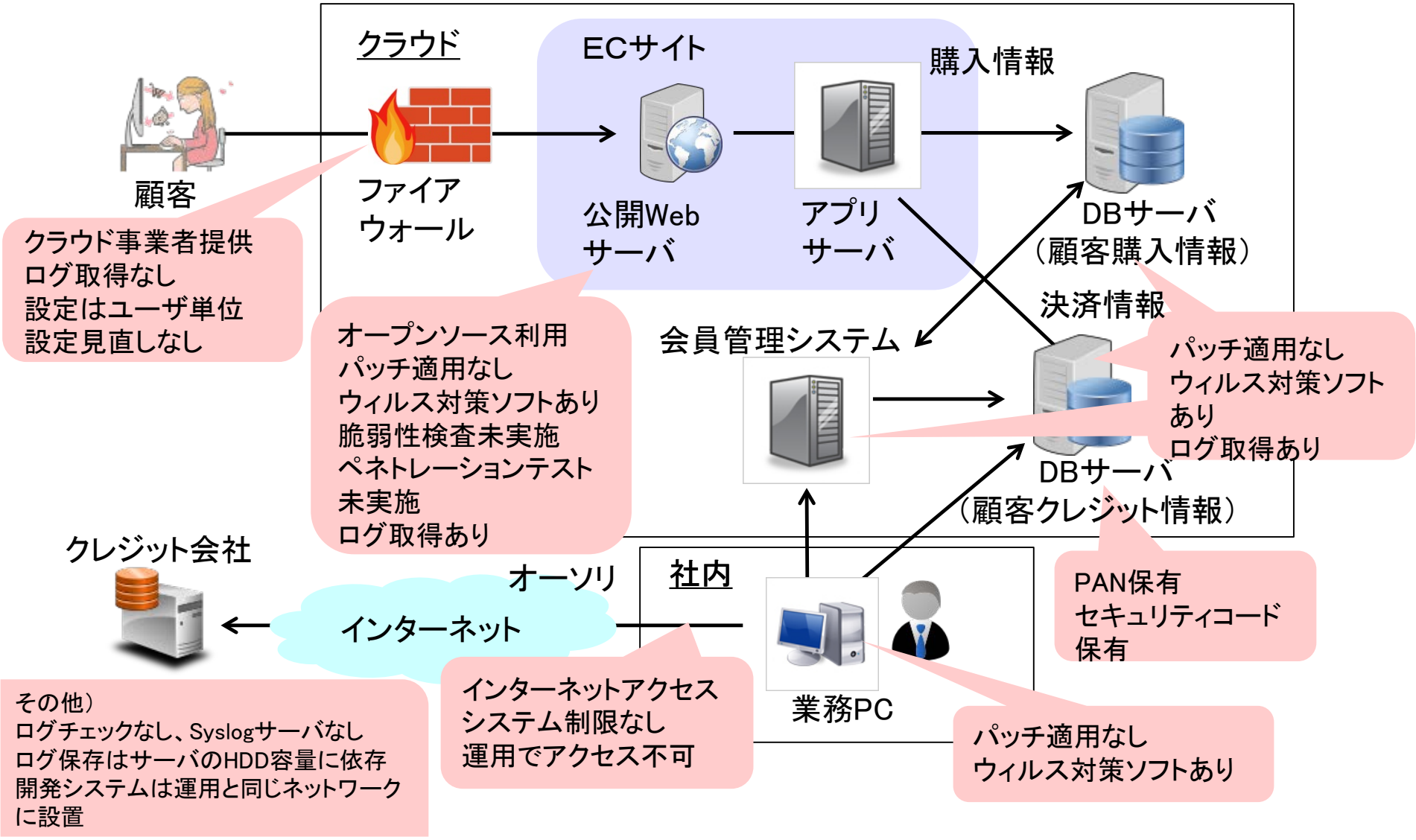
Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

ECサイト企業のシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

ECサイト企業のシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

ECサイト企業の外部状況

影響元	状況		セキュリティ目的・範囲・レベル
マクロ環境	社会・文化	・実店舗に出向かない買い物の要望の拡大 ・働き方の変化により時間を気にしない買物の要望の拡大	・顧客が安心して製品の購入が可能なWebサイトの提供 ・サイバー攻撃や内部犯行によるクレジット情報、個人情報の流出は顧客離れ、損害賠償や、Webサイトの停止につながり、売上/利益が減るため、Webサイト、DBの保護が最優先 ・クレジット情報漏洩リスクを軽減する非保持化などのPCIDSS準拠が必須
	政治	・キャッシュレスの推進	
	技術	・クラウド活用によるECサイト構築のハードル低下	
	法律・規制	・割賦販売法の改正（カード会社の加盟店での取り合扱い状況確認義務）	
ミクロ環境	競争環境	・店舗を必要としないため多くの同業他社の参入（製造とインターネット販売の一体化）	
	市場	・健康志向により地域に関係なく市場の拡大	
外部との関係	クレジット業界	・PCIDSS準拠への要求	
	顧客	・インターネットでのカード決済への不安 ・個人情報漏洩時は損害賠償訴訟	

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

ECサイト企業の内部状況

影響元	状況	
組織体制 方針・戦略	方針	・IT活用に積極的でクラウド利用
	情報セキュリティ ポリシー	・Pマークを取得
	体制	・情報システム部は存在する ・組織横通しの情報セキュリティ委員会はない ・SOC、CERT機能はない ・個人情報管理委員会はある ・危機管理体制はあるが、製品問題、特許、従業員の就労問題、災害対策が主
	役割	・CIO、CISOが不在、個人情報管理責任者は情報システム部長
内部影響 因子	経営者	・IT投資は行う ・情報セキュリティ対策の必要性は理解、現状および何から、どこまで着手すべきか把握できていない ・他社の対策状況を気にする
	情報システム部門	・主業務はアプリ開発、それに伴うサーバ、DB構築も行うが、主に委託者が実施 ・ネットワーク技術者はいない（知識が少ない）
リソース	人員	・明確な情報セキュリティ担当者はいない ・情報システム部門の人材のみではECサイトの構築、運用人員が不足するため、外部委託している
	技術	・リスク評価、必要な対策を決定し、運用する技術力はない

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

ECサイト企業　評価

現状

・店舗を持たないECサイトでの販売による、店舗費や人件費を抑えたビジネスの展開
・顧客情報の流出のリスクが残る現在のECサイト、業務 システム
（業界標準を達成せず、改正割賦販売法に対応不十分）
・ECサイト、業務システムの維持、運用に対し脆弱な体制

目指す姿

顧客情報を安全に活用したビジネス、売上/ 利益の拡大
・店舗費や人件費を抑えたECサイト活用のビジネスの展開
・顧客が安心して製品の購入可能なECサイトの提供
・顧客情報を保護するECサイトや業務システムの維持（業界標準に準拠）
・改正割賦販売法の順守
・上記を支えるための社内、協力会社との体制の維持とその運用

差異

・業界標準、改正割賦販売法に対応不十分なECサイト、業務 システム
・ECサイト、業務 システムの維持、運用に支障をきたす脆弱な体制

起こりうる被害

顧客情報（個人情報、クレジット情報）の漏洩に伴う企業価値の毀損、機会損失による売上/利益の減少

損金の発生	顧客の損害賠償請求（裁判対応、損害賠償の支払い）、クレジット不正利用の補償 クレジット再発行費用の補償、臨時コールセンターの設置　など 裁判費用 aaa万円 損害賠償 bbb万円/人 会員数減少 ccc万人 max ddd万円　他 eee万円
売上/利益の減少	信頼喪失による顧客離れ、購入の減少、ECサイト停止（営業停止）により機会損失

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

改善

企業価値毀損、機会損失を招かないECサイト、業務 システムと運用体制強化

現状売上　mmm万円/年　　現状利益　nnn万円/年
改修費用回収予想　q年後
増加ランニング費用　ooo万円/年
現状利益確保に必要な売上　　ppp万円/年(+rrr%増)

改善策

ECサイト、業務システムの安全性の確保
①～②を1年で対応、③をその次年に対応

① 業界標準、改正割賦販売法への初期対応	<今年度　xxx万円の改修 >
② 業界標準、改正割賦販売法への完全移行	<今年度　yyy万円の改修 >
③ 安全性の定期的な確認、見直しの実施	<次年度以降　zzz万円/年>
①、②に伴う保守費、委託費	<次年度以降　sss万円/年>

通常時と事故などの異常時における、自社と協力会社との役割分担の見直し、責任の明確化、及び自社ビジネスを支えるECサイト、業務システムの運用体制の再構築

① 業界標準、改正割賦販売対応、事故発生時における社内、協力会社の役割の見直し
　<今年度　aaa万円で検討>
② 社内、協力会社の推進体制の構築・運用
　<今年度　bbb万円、次年度以降 ccc万円/年>

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

技術対策

ECサイト、業務システムの安全性の確保

具体策

ECサイト、業務システムについては、セキュリティコード以外も含むクレジット情報の安全な取扱いやシステムの安全性の確保、定期的な安全性の確認など、PCIDSSに対応する。

①～②を1年で対応、③をその次年に対応

① 保存非許可データの保持停止、消去
クレジット情報の非通過化（非保持）

② Webサイト、会員システム、DB、ネットワーク等、PCIDSSに準拠したシステム移行
開発システムと運用システムの分離
ログ管理システムの構築
WAFの導入　など

③ PCIDSSに準拠する定期的な試験、見直しの実施
脆弱性検査の実施(1Q単位、4回/年)
ペネトレーションテストの実施(1回/年)
脆弱性の把握、評価とパッチ適用
ログの確認　など

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

その他の改善

ECサイトの廃止、販路の見直し

現状売上　mmm万円/年　　現状利益　nnn万円/年
増加ランニング費用　ooo万円/年
現状利益確保に必要な売上　　ppp万円/年(+rrr%増)

改善策

ECサイトの廃止、販路の見直し
①～②を1年で対応、③をその次年に対応
① ECサイトを廃止 〈今年度　xxx万円の改修 〉
② 販路の開拓(ショッピングサイトへの出店)　　〈今年度　xxx万円の委託 〉
〈次年度以降　zzz万円/年の委託 〉

自社ビジネスの構造変更に伴う運用体制の再構築
① ショッピングサイトへの対応体制の構築　　〈今年度　aaa万円で検討〉
② ショッピングサイトの商品情報のメンテナンス運用
〈今年度　bbb万円、次年度以降 ccc万円/年〉

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

地域密着
スーパーマーケット

スーパー企業概要

【会社のビジネス概要】
・取扱のメインは食品。
・店舗本店含め10店舗有している。
・増加する高齢者のため、移動スーパーにも着手した。

従業員	800名 （パート込み）
売上	100億

企業IT活用方針	・IT活用はあまり積極的に利用していない
情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ	・無し
体制	・情報システムは総務部配下の一部門 ・組織横通しの情報ｾｷｭﾘﾃｨ委員会、SOC、CERT機能はない ・危機管理体制はあるが、食品衛生、従業員・パート／アルバイトの就労問題、災害対策が主
役割	・CIO、CISOは不在、個人情報管理責任者は総務部長
経営者	・IT投資は積極的ではない ・情報ｾｷｭﾘﾃｨは自社にとって無縁の世界だと思っている ・地域に根差し、地域のお客様満足度向上を経営方針としている
情報ｼｽﾃﾑ部門	・主業務は在庫管理、受発注システムの運用 ・担当社員は5名 ・ﾈｯﾄﾜｰｸ技術者はいないため外注にて構築（知識が少ない）

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

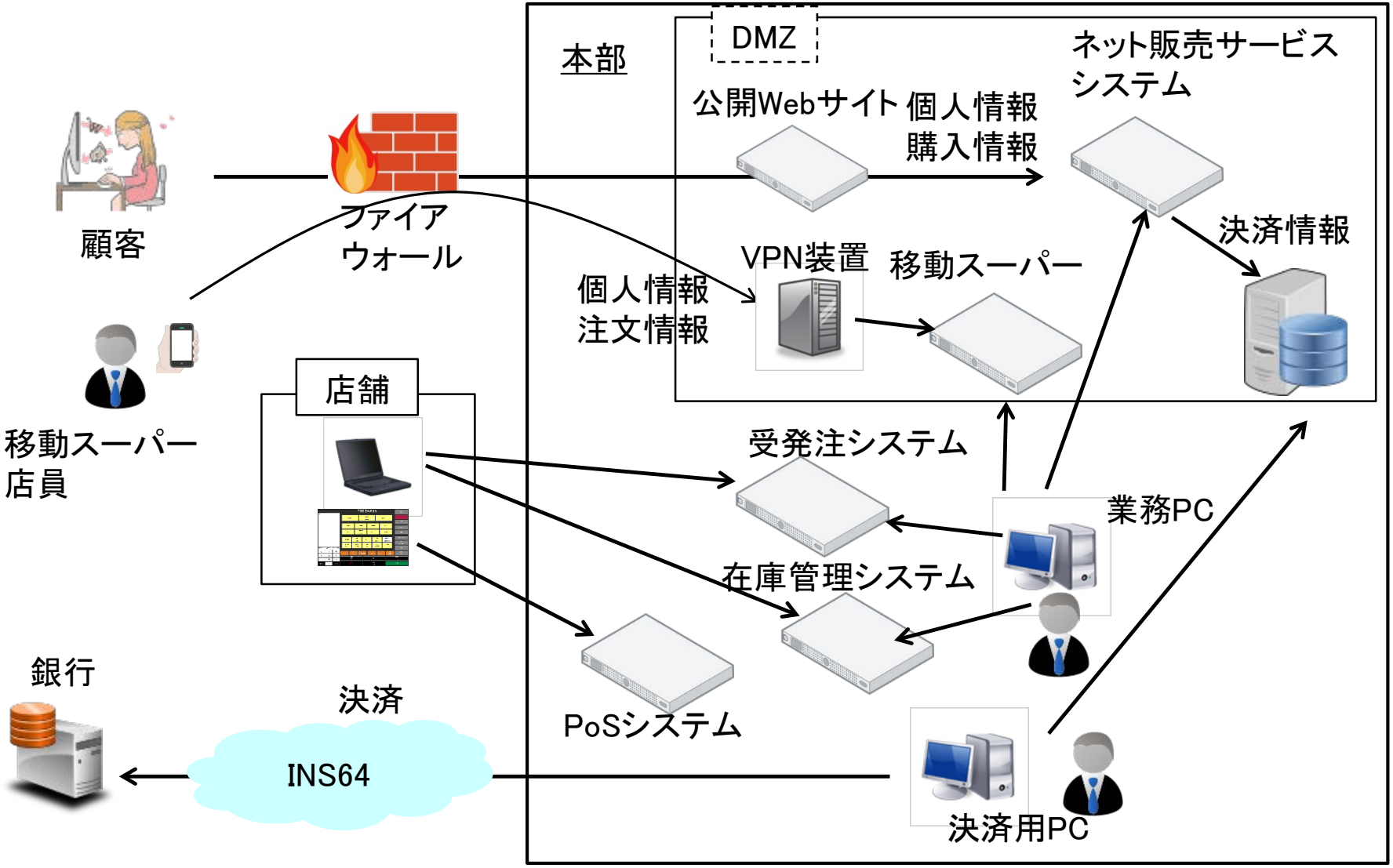
スーパー企業のIT関連の詳細

【会社のビジネス、システム詳細】

・クラウドは利用していない
・サーバー及びFWは社内のサーバールームに設置
・FWの設定は外注に依頼しパラメータシートは残っていない
・公開Webサイトを保有し、店舗情報、チラシ情報の発信、およびオンライン注文受付と配達をセットにしたネット販売サービスを展開している
・ネット販売サービスは、都度の現金、または月1回の銀行引き落としで決済を行う
・買い物に店舗に出向けず、PCやスマートフォンによるネット販売サービス活用ができない高齢者向けに移動スーパーを展開しており、決済が現金のみだが、品切れの商品の注文を受け付けるため、注文者の個人情報および注文品をリモート端末から入力するシステムを構築している
・WordPressを利用しWebサイトを構築している
・レジでのクレジット決済はない
・ネット販売サービス、移動スーパーのシステムはそれぞれで個人情報を保有し、各システムは、本部の特定PCにアクセスを制限し、品物の手配と配送車に指示を出す
・公開Webサイトに脆弱性検査、ペネトレーションテストを実施したことはない
・PCは本部と、各店舗に1台あるが、ウィルス対策ソフトは導入しており、手動アップデートを行っている、ただしWindowsアップデートは行っていない
・ネット販売サービス、移動スーパーの各システムに対し社員や管理者のアクセスログは取得しているが保存期間及びチェックのルールは定義されていない
・ログをsyslogサーバなどで保全しておらず、保存期間も各サーバのHDD容量に依存
・テストシステムは用意していない

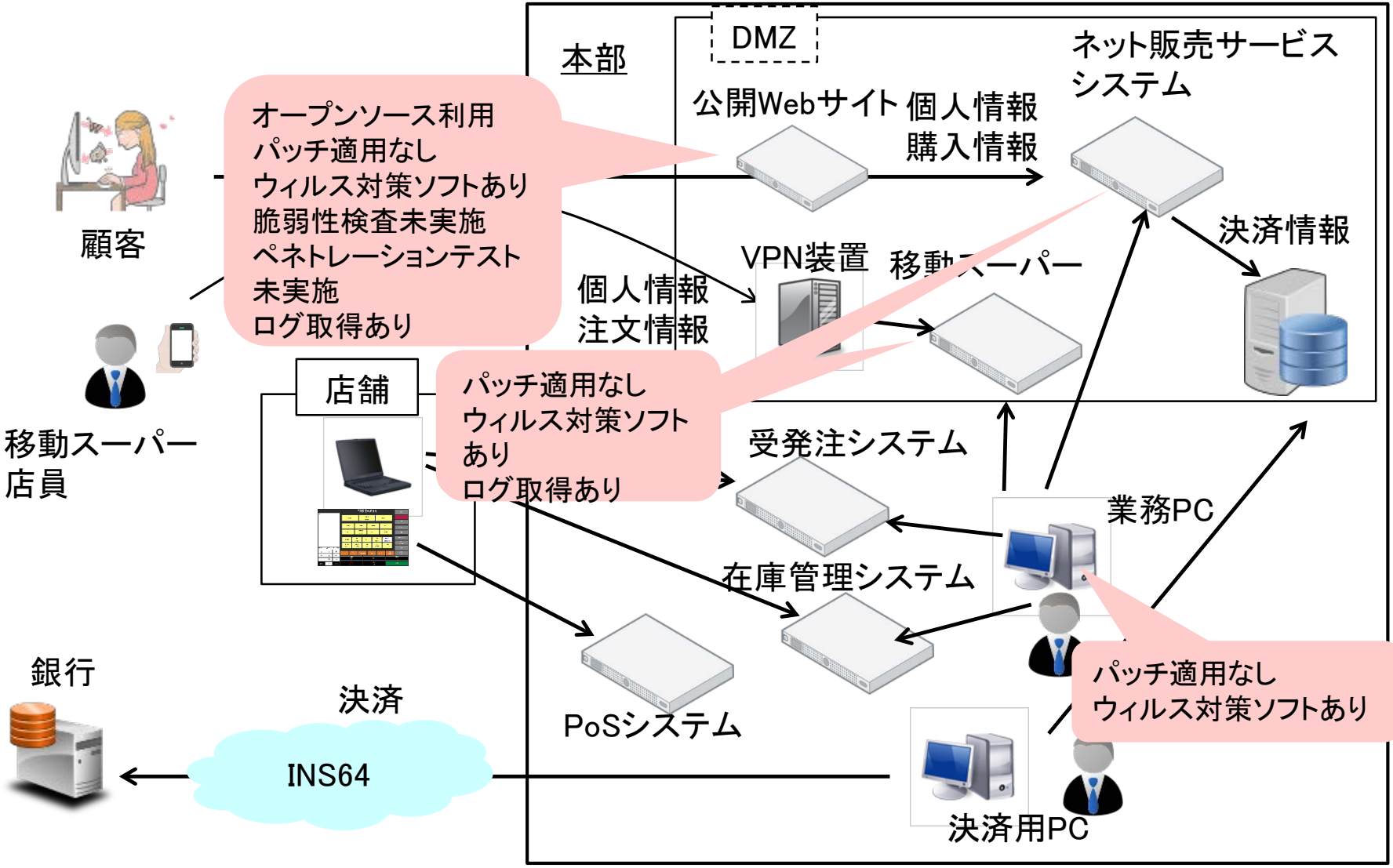
Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

スーパーのシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

スーパーのシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

スーパーの外部状況

影響元	状況		セキュリティ目的・範囲・レベル
マクロ環境	社会・文化	・実店舗に出向くことが困難な高齢者の増加 ・買い物以外にも高齢者向けの介護、旅客運送、その他サービスの要望	・サイバー攻撃や内部犯行による顧客情報、特に高齢者の情報流出は、高齢者を狙う犯罪者による被害の拡大となる可能性があり、その結果、地域住民の信用失墜、連携の破綻により売上が減少につながるため、個人情報の保護、適正な取り扱いが最優先
	政治	・移動販売の規制緩和	
	技術	・クラウド活用によるWebサイト構築のハードル低下	
	法律・規制	・個人情報保護法の改正	
ミクロ環境	競争環境	・地域密着のため、他業種、他企業の参入は困難	
	市場	・地域密着のため市場の拡大はないが、高齢化に伴う提供サービスの拡大の可能性	
外部との関係	顧客	・地域住民との信頼関係に基づく連携が、店舗、移動スーパーの売り上げ、利益確保に結び付く	

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

スーパーの内部状況

影響元	状況	
組織体制 方針・戦略	方針	・ITは業務関連でオンプレミスがメイン、クラウドの利用は考えていない
	情報セキュリティ ポリシー	・Pマークの取得を検討中
	体制	・情報システム部門は存在する ・組織横通しの情報セキュリティ委員会はない ・SOC、CERT機能はない ・個人情報管理委員会はある ・危機管理体制はあるが、衛生関連、従業員の就労問題、災害対策が主 ・パートを含む社員に情報セキュリティ教育は実施していない
	役割	・CIO、CISOは不在、個人情報管理責任者は情報システム部長
内部影響 因子	経営者	・IT投資は積極的に行わない ・情報セキュリティは自社にとって無縁の世界だと思っている ・地域に根差し、地域のお客様満足度向上を経営方針としている
	情報システム部門	・主業務は在庫管理、受発注システムの運用 ・ネットワーク技術者はいないため外注にて構築（知識が少ない）
リソース	人員	・明確な情報セキュリティ担当者はいない ・情報システム部門の人材のみではWebサイトの構築、運用人員が不足するため、外部委託している
	技術	・リスク評価、必要な対策を決定、運用する技術力はない

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

スーパー　評価

現状

・Pマークは取得していないが、これから取得予定
・地域に密着し、地元住民と信頼関係を構築することで、地元住民と連携し、高齢者向けの移動スーパーの場所の確保と展開や、ネット販売と店舗以外でも売上を上げている
・顧客情報の流出リスクを把握できていない現在のネット販売、移動スーパーの両システム
・Webサイト、業務システムの維持、運用に対し脆弱な体制

目指す姿

地域住民との信頼関係に基づくビジネスの確立、売上 / 利益の拡大
・顧客と顔が見えることによる信頼関係の構築
・サイバー攻撃や内部犯行による顧客情報、特に高齢者の情報流出は、高齢者を狙う犯罪者による被害の拡大となる可能性があり、その結果、地域住民の信用失墜、連携の破綻により売上が減少につながるため、個人情報の保護、適正な取り扱いが最優先

差異

・Webシステム、ネット販売、移動スーパーシステムにリスクの見逃し
・Webサイト、業務 システムの維持、運用に支障をきたす脆弱な体制
・個人情報の保護および管理体制の希薄

起こりうる被害

顧客情報の漏洩に伴う企業価値の毀損、機会損失による売上/利益の減少

損金の発生	顧客の損害賠償請求（裁判対応、損害賠償の支払い） 臨時コールセンターの設置　など 裁判費用 aaa万円 損害賠償 bbb万円/人 顧客数減少 ccc人 max ddd万円　他 eee万円
売上/利益の減少	信頼喪失による顧客離れ、販売の減少、Webサイト停止（営業停止）による機会損失

Copyright (c) 2000-2017　NPO日本ネットワークセキュリティ協会

改善

企業価値毀損、機会損失を招かないWebサイト、業務 システムと運用体制強化

現状売上　mmm万円/年　　現状利益　nnn万円/年
改修費用回収予想　q年後
増加ランニング費用　ooo万円/年
現状利益確保に必要な売上　　ppp万円/年(+rrr%増)

改善策

Webサイト、業務システムの安全性の確保
①～②を今年度で対応、③をその次年度に対応

① 現状システムの脆弱性の把握	<今年度　xxx万円>
② 把握した脆弱性の改修	<①に基づく改修費用算出 今年度予算　yyy万円>
③ 安全性の定期的な確認、見直しの実施	<次年度以降　xxx万円/年>
②に伴う保守費、委託費	<次年度以降　sss万円/年>

通常時と事故などの異常時における、自社と協力会社の役割分担の見直し、責任の明確化、及び自社ビジネスを支えるWebサイト、業務システムの運用体制再構築

① 改正個人情報保護法対応、事故発生時における社内、協力会社の役割の見直し
　<今年度　aaa万円で検討>
② 社内、協力会社の推進体制の構築・運用、および社内教育の確立
　<今年度　bbb万円、次年度以降 ccc万円/年>

Copyright (c) 2000-2017　NPO日本ネットワークセキュリティ協会

技術対策

Webサイト、業務システムの安全性の確保

具体策

Webサイト、業務システムにおいて、個人情報の安全な取扱いやシステムの安全性の確保、定期的な安全性の確認などを行う
①を今年度で対応、②をその次年度に対応

①定期的な試験、見直しの確立
- 脆弱性検査の実施(1Q単位、4回/年)
- ペネトレーションテストの実施(1回/年)
- 脆弱性の把握、評価とパッチ適用
- 脆弱性の改修施策検討、費用確保の仕組み確立

② Webサイト、業務システム、ネットワーク機器でのインシデント検知のためのログ管理
- 想定するサイバー攻撃、内部不正検知のためのログ設計
- 各システムでのログ取得設定
- ログ管理システムの構築
- ログ分析システムの構築

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

医療機関

医療機関概要

【組織のビジネス概要】
・一般病床　50床　療養病床　100床
・糖尿病治療に特化し、透析センターを持つ

組織のIT活用方針	・IT活用による業務効率の向上
情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ	・個人情報保護対策は実施
体制	・システム管理を行う情報管理課が存在するが、医療機器を管理する部署は存在しない ・組織横通しの個人情報保護委員会は存在する ・危機管理体制はあるが、医療関連が主で情報セキュリティに対する体制は無い
役割	・個人情報管理責任者は事務局長、CIO、CISOは不在
経営者 （医院長）	・情報セキュリティ対策の必要性は理解しているが、セキュリティ対策は医療従事者の負担になることが多いので、医療の質に関わらない限り積極的に行いたくない ・社会保障費圧縮による診療報酬の低減化が進んで行きそうなので、積極的にITを活用し効率を上げて行きたいと考えている
情報ｼｽﾃﾑ部門	・情報システム（電子メール、Web）、病院情報システム(HIS)、放射線科情報システム(RIS)に関連するネットワーク機器、サーバ、クライアントの管理が主業務 ・HIS、RIS、各種医療機器の管理は業者に任せている

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

医療機関のIT関連の詳細

【組織のビジネス、システム詳細】

・　一般病床　50床　療養病床　100床

・診療科は糖尿病内科、内科、腎臓内科、泌尿器科、外科、整形外科、放射線科、リハビリテーション科、小児科、循環器内科、循環器外科、消化器内科、消化器外科

・糖尿病治療に特化し、人工透析センターも保有する。

・病院情報システム(HIS)、放射線科情報システム(RIS)、各検査システムと情報システム(電子メール利用、Web閲覧)とはファイアウォールで論理的に分離

・システム管理を行う情報管理課が存在するが、情報システムの管理が主で、HIS、RIS、各種医療機器の管理は、実質的に各ベンダーが実施している。

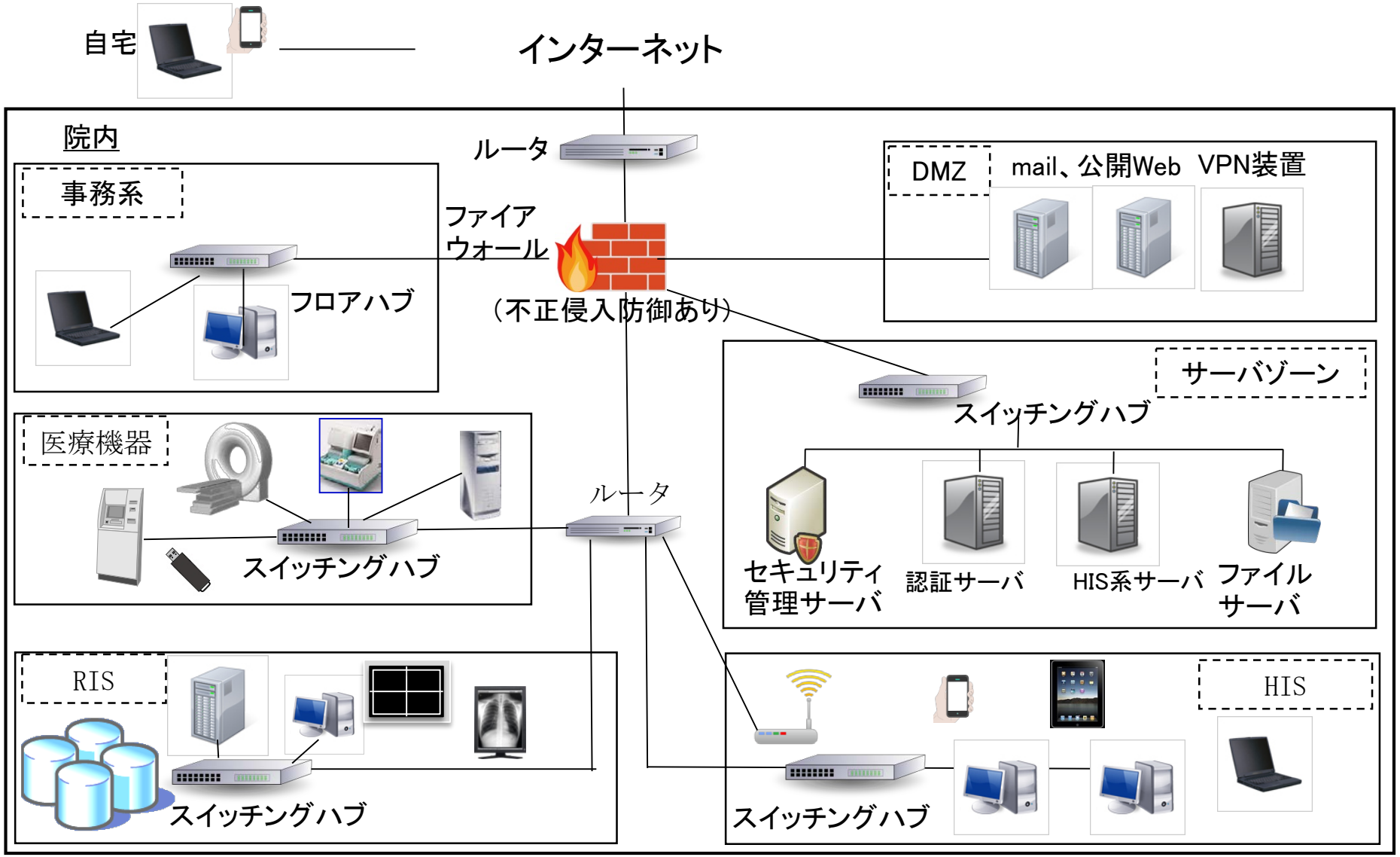
・セキュリティ対策は事務局長を責任者とする個人情報保護対策が主で、PCの操作ログの取得、USB記憶媒体の管理、情報システムのセキュリティパッチの適用、不正端末検知、ウイルス対策を実施している。

・事務系とHIS、RIS、医療機器はファイアウォールで論理的に分離しているが、ウイルス対策、PC操作ログ取得、不正端末検知用サーバは各セグメントを跨って利用している。

・HIS系では無線LANを使用しているがデバイス認証は行っていない。院内ではID、パスワードで認証を実施しており、パスワードは6文字。一部共通IDも使用。

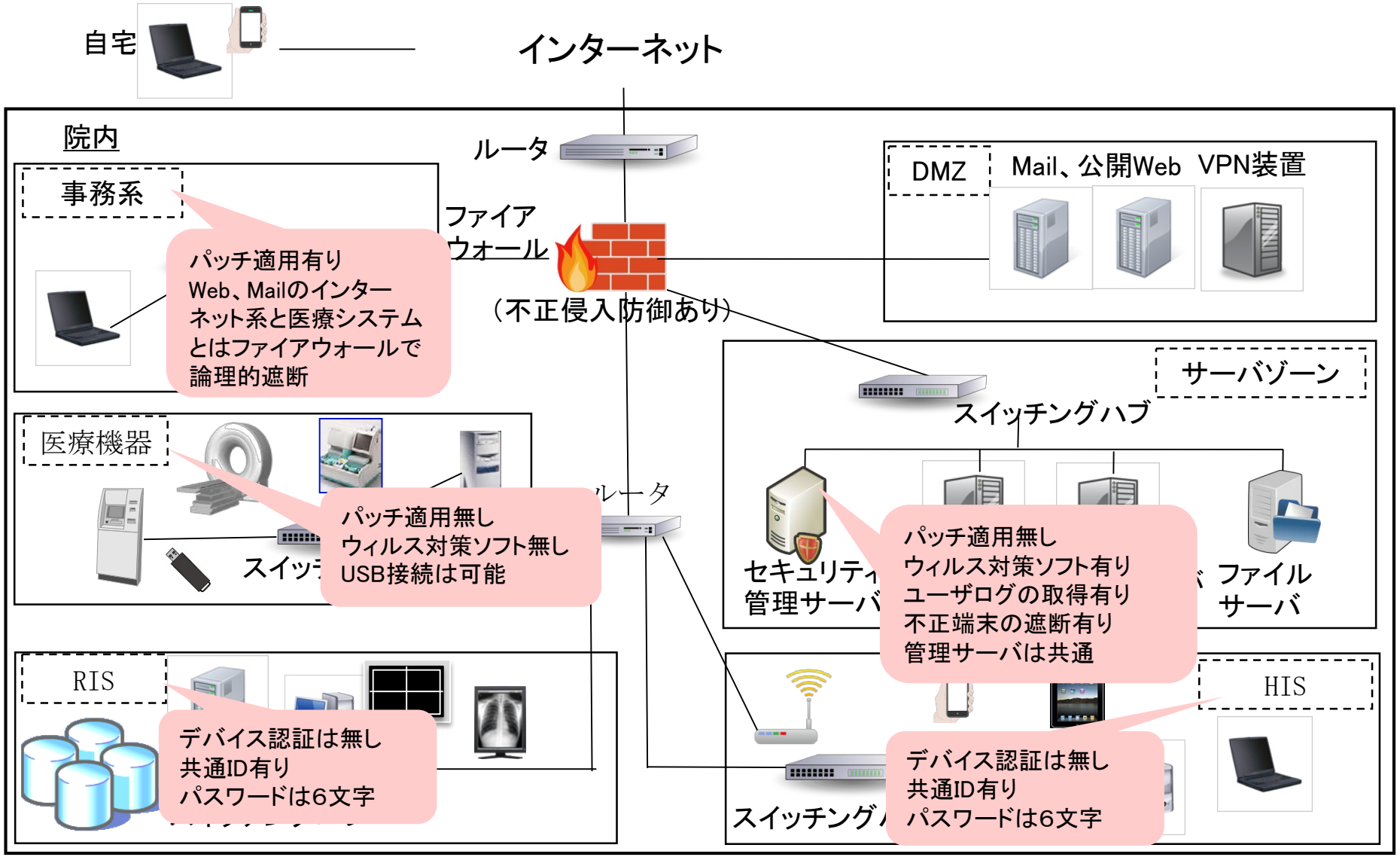
Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

医療機関のシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

医療機関のシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

医療機関の外部状況

影響元	状況		セキュリティ目的・範囲・レベル
マクロ環境	社会・文化	・高齢化社会の到来 ・高齢化社会による患者数増大による、医師看護師等医療従事者の不足 ・ランサムウェアによる海外医療機関の被害増 ・(医療)情報技術者の不足	・患者の個人情報の保護 ・病院情報システム(HIS)、放射線科情報システム(RIS)、医療機器の可用性、完全性の確保
	政治	・高齢化社会に伴う社会保障費圧縮による診療報酬の低減化	
	技術	・医療へのAI技術、ビッグデータの活用 ・IoT、ロボット技術の医療介護への活用	
	法律・規制	・医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律 ・個人情報保護法	
ミクロ環境	競争環境	・地域で3番目の病床数を持つ病院 ・高齢化の進展で急性疾患から慢性疾患へと変化	
	市場	・高齢化に伴い、医療機関を利用する人口は増加し市場は拡大しているが、国の社会保障費圧縮による診療報酬の低減化により現実は厳しい	
外部との関係	医療業界	・CT、MRI、PET等と常に最新技術が導入される傾向がある	
	顧客	・地域の入院患者及び外来患者	

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

医療機関の内部状況

影響元	状況	
組織体制 方針・戦略	方針	・IT活用による業務効率の向上
	情報セキュリティ ポリシー	・個人情報保護方針は存在するがセキュリティ方針は無い ・医療機器に関する完全性、可用性観点からのセキュリティの認識が無い
	体制	・システム管理を行う情報管理課が存在する ・組織横通しの個人情報保護委員会は存在する ・危機管理体制はあるが、医療関連が主で情報セキュリティに対する体制は無い ・対象は情報系で医療機器は範囲外である
	役割	・CIO、CISOが不在、個人情報管理責任者は事務局長
内部影響 因子	経営者 （医院長）	・情報セキュリティ対策の必要性は理解しているが、セキュリティ対策は医療従事者の負担になることが多いので、医療の質に関わらない限り積極的に行いたくない ・社会保障費圧縮による診療報酬の低減化が進んで行きそうなので、積極的にITを活用し効率を上げて行きたいと考えている ・医療機器に関する管理責任者が存在しないことを問題だと認識している
	情報システム 部門	・情報システム（電子メール、Web）、病院情報システム(HIS)、放射線科情報システム(RIS)に関連するネットワーク機器、サーバ、クライアントの管理が主業務 ・HIS、RIS、各種医療機器の管理は業者に任せている
リソース	人員	・システム管理が主で明確には情報セキュリティ管理は行っていない ・HIS、RIS、各種医療機器の管理は業者に委託
	技術	・HIS、RISに関連する個人情報保護対策は実施している ・HIS、RIS、院内の医療機器をセキュリティ管理する技術力は無い

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

医療機関　評価

現状

・患者の個人情報保護を主としたセキュリティ対策
・病院情報システム(HIS)、放射線科情報システム(RIS)、医療機器の可用性、完全性の確保に課題
・医療機器のセキュリティ確保に関しては、院内に担当者がおらず、完全にベンダー任せ
・医療機器に関しては薬事法の対象となり、ウイルス対策ソフト、セキュリティパッチの適用は改造と見なされ、法に抵触するためセキュリティを確保できていない

目指す姿

院内にあるすべてのコンピュータに関わるセキュリティの確保
・病院情報システム(HIS)、放射線科情報システム(RIS)の可用性、完全性の確保
・薬事法の対象となる医療機器の運用方法の見直し及び対策の決定
・上記を支えるための院内、ベンダーとの体制の維持とその運用

差異

・病院情報システム(HIS)、放射線科情報シス テム(RIS)の可用性、完全性の欠如
・薬事法の対象となる医療機器のセキュリティ対策が無い

起こりうる被害

医療機器の停止による医療行為の混乱や停止、または医療過誤の発生と医療報酬の減少

停止した医療機器の復旧費用	停止した医療機器復旧のための費用 復旧費用 aaa万円
医療報酬の減額	bbb万円
誤診	誤診による医療事故の発生、患者への保障費用の負担、行政指導への対応

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

改善

医療情報システムと医療機器のセキュリティリスク低減

現状売上　mmm万円/年　　現状利益　nnn万円/年
改修費用回収予想　q年後
増加ランニング費用　ooo万円/年
現状利益確保に必要な売上　　ppp万円/年(+rrr%増)

改善策

院内セキュリティの強化

① 国内外の病院で発生しているインシデントの収集と分析及び対策の検討
〈今年度　xxx万円〉

医療情報システムのセキュリティ強化 〈今年度　yyy万円 次年度以降　sss万円/年〉
① 医療情報システムと情報システム間のアクセス制御の強化
② 医療情報システムと情報システムにウイルス対策、PC操作ログ取得、不正端末検知用サーバをそれぞれ設置
③ ベンダーと協力したランサムウェア対策
④PCのOS・アンチウイルス等に対するパッチを適用し、常に最新状態を更新・維持

薬事法の対象となる医療機器のセキュリティ強化 〈今年度　zz万円 次年度以降　aa万円/年〉
① 医療機器のリスト化と院内担当者の決定、ベンダー緊急連絡先の記載
② 医療機器へのUSB/PC接続時のウイルス検索駆除ツールの使用
③ ベンダー協力による医療機器への定期なウイルス検索駆除ツールの適用

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

参考資料

IPA　医療機器における情報セキュリティに関する調査
https://www.ipa.go.jp/files/000038223.pdf

トレンドマイクロ株式会社　導入事例：国立大学法人　金沢大学附属病院
http://www.trendmicro.co.jp/cloud-content/jp/pdfs/business/case-study/kanazawa-hospital/pdf-casestudy-kanazawa-hospital-new-20130827.pdf

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

卸売業（商社）

卸売業（商社）企業概要

【会社のビジネス概要】
・数社のアパレルメーカー、ブランドの販売を行う。
・主に百貨店や総合スーパーなどの実店舗向けに、販売を行っている。

従業員	70名
売上	20億

企業IT活用方針	・受発注業務、WebEDI、営業業務においてタブレットを用いて製品紹介
情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ	・企業ホームページに掲載している程度
体制	・情報システム部は存在する ・組織横通しの情報ｾｷｭﾘﾃｨ委員会、SOC、CSIRT機能はない ・危機管理体制はあるが、従業員の就労問題、災害対策が主
役割	・CIO、CISOは不在、情報管理責任者は情報システム部長
経営者	・IT投資は基幹業務がメインであり、消極的 ・情報ｾｷｭﾘﾃｨ対策の必要性は殆ど理解できておらず、現状および何から、どこまで着手すべきか把握できていない ・他社の対策状況を気にもせず、重要情報は持っていないという認識
情報ｼｽﾃﾑ部門	・主業務は基幹業務の安定稼働、それに伴うサーバ構築も行うが、主に委託者が実施 ・担当社員は2名 ・ﾈｯﾄﾜｰｸ技術者はいない（知識が少ない）

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

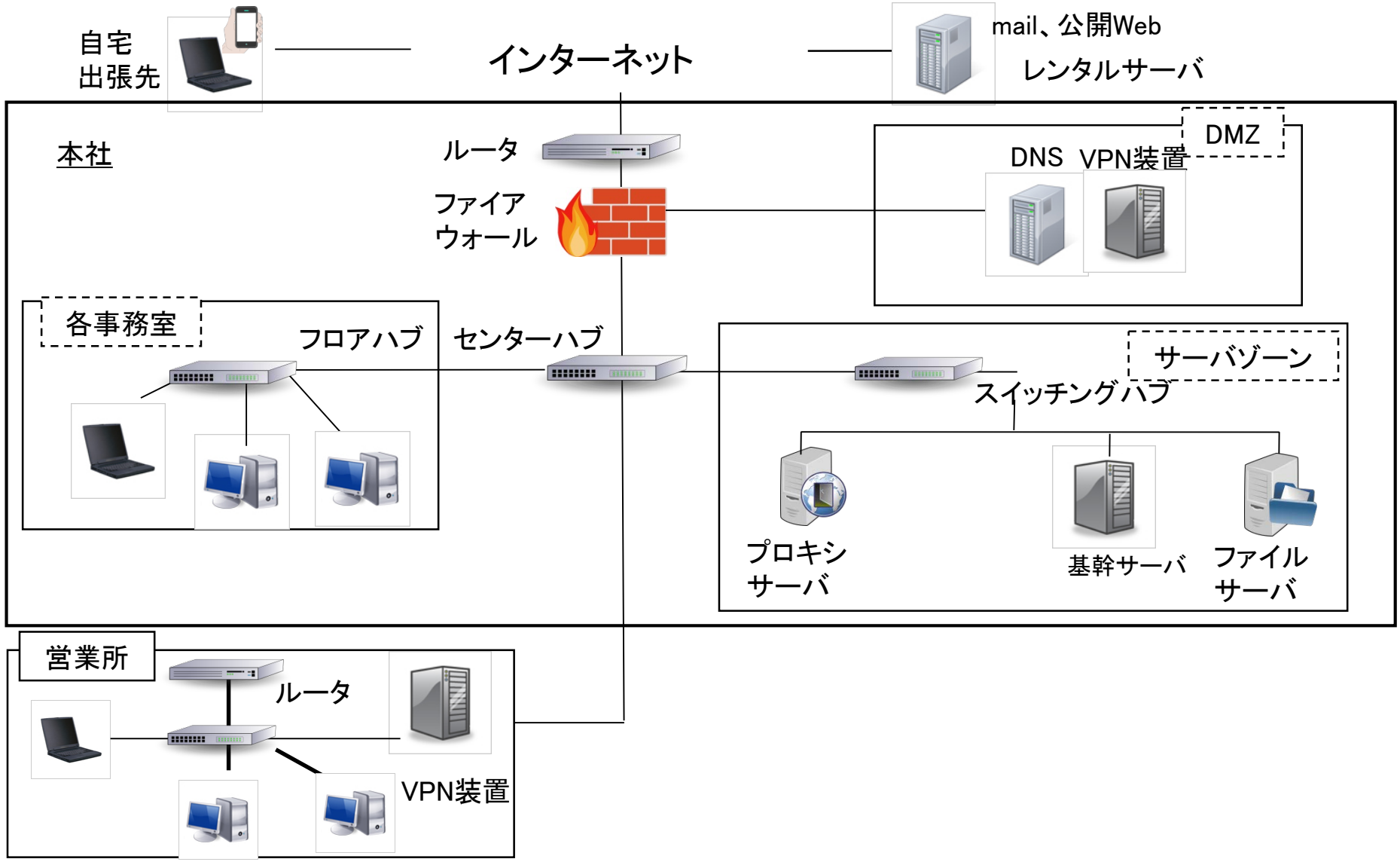
卸売業（商社）のIT関連の詳細

【会社のビジネス、システム詳細】

・アパレル・繊維メーカーが多い地域でもあり、長年繊維原料やアパレルを取り扱ってきた
・拠点は、東京と大阪の二か所
・基幹サーバや社内インフラをオンプレミスで構築
・FWは利用しているが、5年毎の更新
・ログは保存せず、設定の見直しをしていない
・基幹サーバーは、メインフレームを15年以上継続して利用
・受発注業務は、基幹サーバーで管理しており、メインフレームメーカーに依存している体質
・WebEDIは取引先要望で利用しているが、一度紙に印刷して、基幹サーバーに手入力
・昔からの商習慣ということもあり、取引先も変化は殆どないが、一部アパレルメーカーが大きくなり、アパレルメーカーから取引条件として、セキュリティ向上の依頼が増え始めている
・インターネットは配布しているPCからは接続でき、本社FWからのみのアクセスしかできない
・社員の個人情報及びマイナンバーは、人事部が人事DBに保管
・上記PCはクレジット会社以外のインターネットへのシステム的な接続制限はない
・Webサイトは、会社紹介などの為にホームページを立ち上げてはいるが、更新頻度は少ない
・社内ファイルサーバーなど含め、脆弱性検査、ペネトレーションテストを実施したことはない
・DBサーバ、業務PCにパッチは適用していないが、ウィルス対策ソフトは導入し、インターネット経由で、定義ファイルのアップデートを行っている
・各個人PCの資産管理は、Excelにて管理しており、USBデバイスやSDカードの接続制限やPC操作ログ取得などはしていない

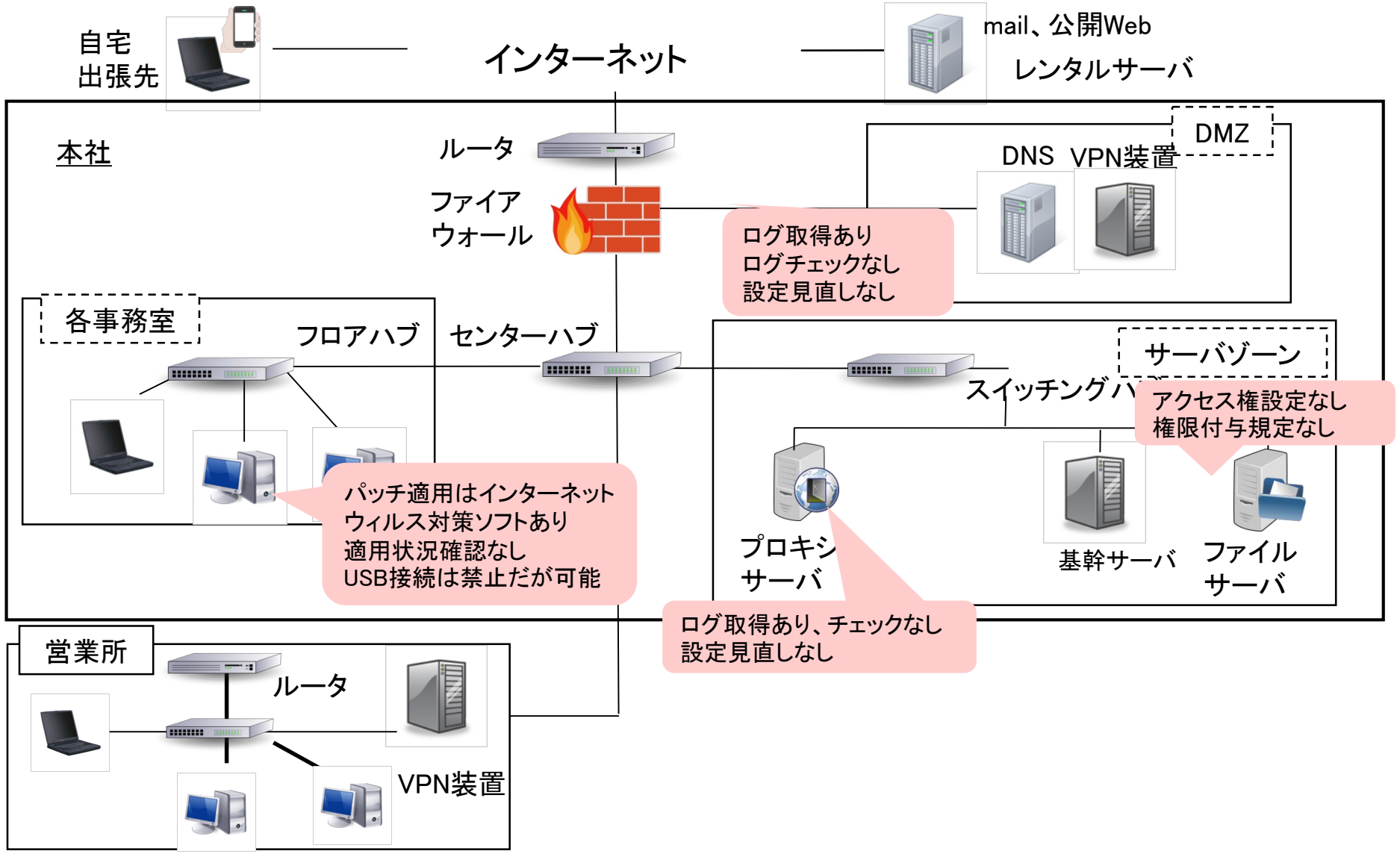
Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

卸売業（商社）のシステム構成



Copyright (c) 2000-2018 NPO日本ネットワークセキュリティ協会

卸売業（商社）のシステム構成



Copyright (c) 2000-2018 NPO日本ネットワークセキュリティ協会

卸売業（商社）の外部状況

影響元	状況		セキュリティ目的・範囲・レベル
マクロ環境	社会・文化	・アパレルメーカー数、ブランドの増大 ・インターネットで買物する顧客の拡大により、実店舗での販売が低迷	・BtoBビジネスであり、メーカーの価格情報やデザインなどの情報漏洩を防ぐ必要性はあるとは思っているが、対策まではしていない。 ・サイバー攻撃や内部犯行によるメーカーの価格情報、デザイン情報の流出により、顧客からの信用をなくしてしまい、取引がなくなる可能性がある。
	政治・経済	・国内市場は人口減少の影響により、縮小 ・海外市場は、ASEAN諸国やインドなどの市場も大きくなり、各国に拡大を検討中	
	技術	・EDI取引の活発化により、商社機能の必要性も減り始めている	
	法律・規制	・不正競争防止法の改正により、取引先の情報の保護を強化 ・サイバーセキュリティ経営ガイドラインに沿った経営が求められている	
ミクロ環境	競争環境	・海外アパレルブランドの日本参入やメーカー直販のECサイトの増加	
	市場	・ファストファッション市場の拡大	
外部との関係	顧客	・百貨店や大手スーパーなどの実店舗での取引減少	

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

卸売業（商社）の内部状況

影響元	状況	
組織体制 方針・戦略	方針	・メインフレームベンダー依存からの脱却し、自主的なセキュリティ対策が必要
	情報セキュリティ ポリシー	・取引先の要求もあり、形だけでも作成し、企業ホームページには掲載
	体制	・情報システム部は存在するが実質2人 ・組織横通しの情報セキュリティ委員会はない ・SOC、SIRT機能はない ・危機管理体制はあるが、従業員の就労問題、災害対策が主
	役割	・CIO、CISOは不在
内部影響 因子	経営者	・IT投資はメインフレームの更新が主で、営業活動におけるPC利用は積極的 ・取引先から要求はあるものの、情報セキュリティ対策の必要性は理解できておらず、現状および何から、どこまで着手すべきか把握できていない ・他社の対策状況を気にもせず、重要情報は持っていないという認識
	情報システム部門	・主業務は各ユーザーのPCのメンテナンスや入れ替え業務などを実施 ・ネットワーク技術者はいない（知識が少ない）
リソース	人員	・明確な情報セキュリティ担当者はいない ・情報システム部門の人材のみでは対応できないため、メインフレームの作業については外部に委託している
	技術	・リスク評価、必要な対策を決定、運用する技術力はない

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

卸売業（商社） 評価

現状

スピード経営ができておらず生産性が低く、また全社的に情報セキュリティに対して体制面、運用面も不足

・情報システム部門は実質2人しかいない
・今までと同じ業務の仕方であり、生産性が低い
・最新ITの利活用ができていない
・自然災害などを考慮したBCPなどが無い
・全社的なマルウェア蔓延時には、情報システム部門が徹夜で対応し、復旧させたが、収束したかは不明

目指す姿

ITを利活用し生産性向上させ、売上・利益を確保する

・クラウドを活用し海外展開なども迅速な経営を行う
・情報セキュリティ体制面、運用面を整備
・取引先の情報を保護する体制、運用、ITを整備
・自然災害やマルウェア感染等、事業継続困難となった場合の回復力を付ける為、BCPを整備し運用
・サイバーセキュリティ経営ガイドラインに沿った運用を行う

差異

・マルウェア感染や取引先情報の漏えい等のインシデント発生時のルールや体制がなく、可用性、回復力がない
・IT全般において、ベンダー依存から脱却できておらず、不十分な対策、運用となっている

起こりうる被害

社内マルウェア拡散や取引先への飛び火などによる機会損失による売上/利益の減少、競争力の低下

業務、取引停止	社内でのマルウェア拡散や取引先に飛び火することにより業務の停止、取引停止による売上減少 aaaa万円
売上/利益の減少、損金の発生	回復力不足により、復旧に時間がかかるため、それに伴う契約の打ち切り 裁判費用 bbb万円　損害賠償 ccc万円
売上/利益の減少	業務継続できないことよる取引の停止 入荷、出荷停止による売上損 aaaa万円

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

改善

取引先情報の保護と機会損失を招かない事業継続体制整備や運用

現状売上　mmm万/年　　現状利益　nnn万円/年
改修費用回収予想　q年後
増加ランニング費用　ooo万円/年
現状利益確保に必要な売上　　ppp万円/年(+rrr%増)

改善策

情報セキュリティ全般の強化
①～②を今年度で対応、③をその次年度に対応

① マルウェア感染させない為の社員教育を行う　〈今年度　yyy万円の教育 〉
② ネットワークや端末の現状把握　〈今年度　xxx万円の改修 〉
③ ネットワークの見直しや最新技術の導入　〈今年度　yyy万円の改修 〉

①、②、③に伴う保守費、委託費　〈次年度以降　sss万円/年〉

通常時と事故などの異常時における、取引先との情報交換体制構築、責任の明確化、及びシステムの運用体制の再構築

① 事故発生時、体制の構築とルール化　〈今年度　aaa万円で検討〉
② 通常時と事故発生時に情報の収集、分析と対策が行える体制の構築　〈今年度　bbb万円で検討〉

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

技術対策

自社の安全性の確保とセキュリティリスクの低減

具体策

自社の安全性の確保とセキュリティリスクの低減
①～②を今年度に対応

① 端末などの資産の把握と管理
FWの見直しと最新マルウェア対策ソフトの導入
パッチ配信システム、PC操作ログ取得、外部接続デバイスの制御システムの導入

② USB、PCなど、未許可端末の社内NW接続を制限
BYOD時のセキュリティ確保
クラウド化の推進によるセキュリティ向上
マルウェア感染を外部専門家が監視する仕組みの導入　など

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業 装置系

製造業(装置系)企業概要

【会社のビジネス概要】
・電気機器製造メーカ
・自社製品の開発製造の他、他社からのOEM、ODMを行う。
・少量生産は国内工場、大量生産は中国の提携工場で行う。

従業員	80名
売上	25億

企業IT活用方針	・現状は生産管理や購買、販売の個別のシステムのみであるが、今後は統合したシステム等、IT活用による業績向上を目指す
情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ	・利用者を対象にした主にPC利用の規定のみ
体制	・情報システム部は存在する ・組織横通しの情報ｾｷｭﾘﾃｨ委員会、SOC、CERT機能はない ・危機管理体制はあるが、製品問題、災害対策が主 ・QMS,EMS事務局あり(総務が担当)、ISO9001,ISO14001取得済
役割	・CIO、CISOが不在、情報管理責任者は情報システム部長
経営者	・IT投資は積極的に行う ・情報ｾｷｭﾘﾃｨ対策の必要性は理解、現状および何から、どこまで着手すべきか把握できていない ・働き方改革や育児介護との両立のため、テレワークの導入を考えている。
情報ｼｽﾃﾑ部門	・主業務は3人、主に各社員のPCやデータ保存用のサーバを担当 ・工場は生産管理部門の管轄、ITに強い社員が担当している ・業務システムやネットワーク構築などはベンダーまかせ

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

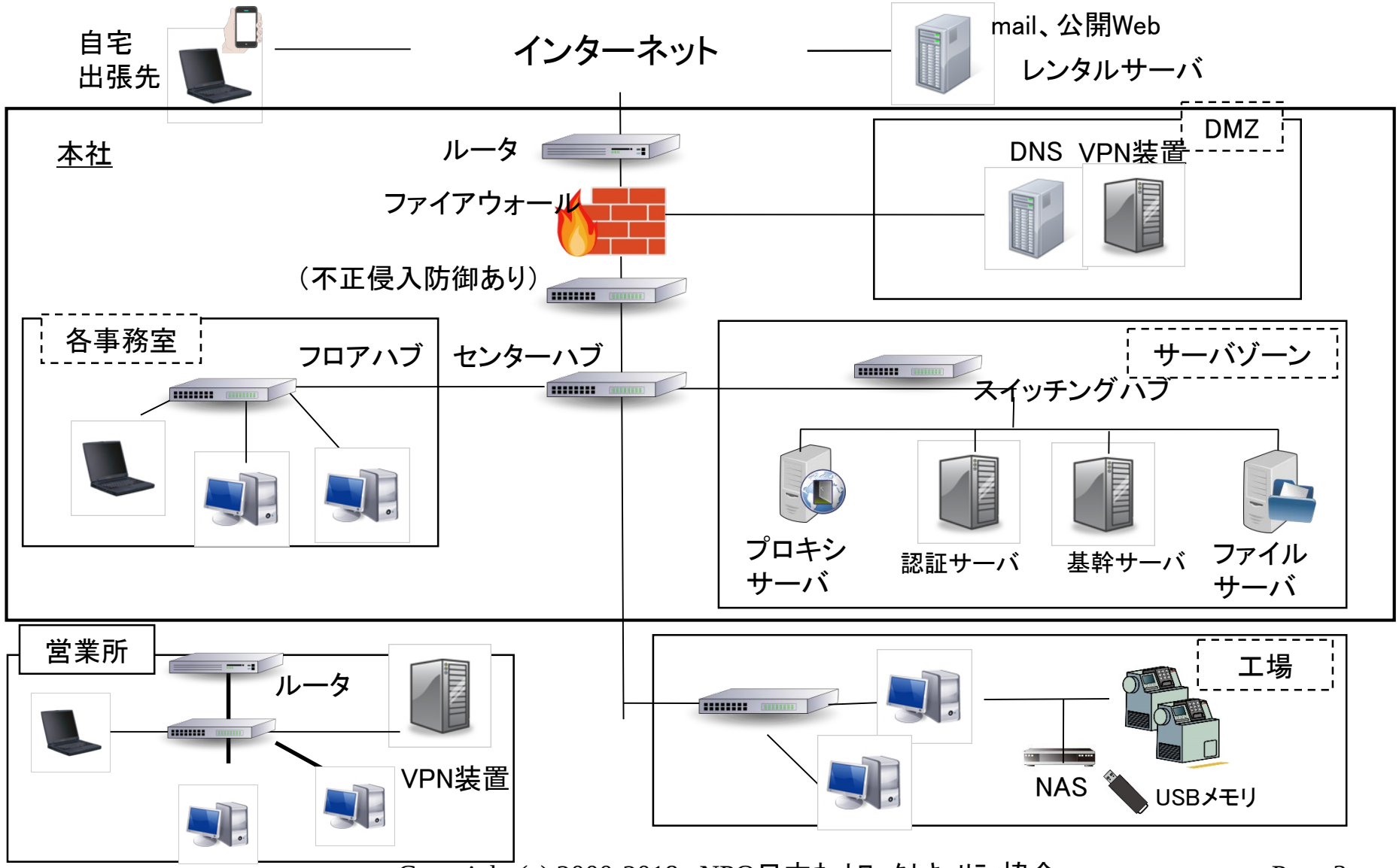
製造業（装置系）のIT関連の詳細

【会社のビジネス・システム詳細】

・従来小型家電を開発製造していたが、新たにヘルスケア向けの自社製品を開発中である
・国内メーカーからOEM生産を受託している
・開発から受託するODM生産もある
・大量生産時はコスト削減のため、中国の提携先工場へ生産を委託
・生産効率を上げるためIT投資、受発注や生産管理の統合システムの導入を検討中
・顧客企業より、生産データの中国工場への提供に対し、営業秘密漏洩の懸念が出ていたり、中国の為替や人件費増で委託費が大きくなっていることから、国内での生産を強化したい
・購買管理、販売管理、生産管理、各々のシステムを導入している
・設計開発はPCを利用、設計者の個人PCと兼用している。データ保管はサーバを利用
・公開Webサーバ、メールサーバーは、法人向けのレンタルサーバーを利用
・ファイアウォール設置など工場以外のネットワーク環境はベンダーの勧めで構築
・働き方改革や育児介護との両立支援のため、テレワークの導入を考えている
・開発データなどを保存するファイルサーバはアクセス権の認証は行っているが、アクセス権の付与には明確な規定なし（上司承認でOK）。開発データは担当者のPC上にも保存可能
・USBメモリの使用は営業・事務職は禁止しているが、物理的に接続は可能
・工場や開発部門ではネットワーク非接続の機器とのデータ交換にUSBメモリ、SDカード使用。
・何が営業秘密情報となるか明確化されていないが、QMSにより営業情報の取扱い、管理の仕方には手順やフォーマットの取り決めがある
・PCにアンチウイルスソフトは導入し、最新化とパッチも適用することになっているが、実態を把握できていない
・サーババックアップは情報システム部が定期的に実施

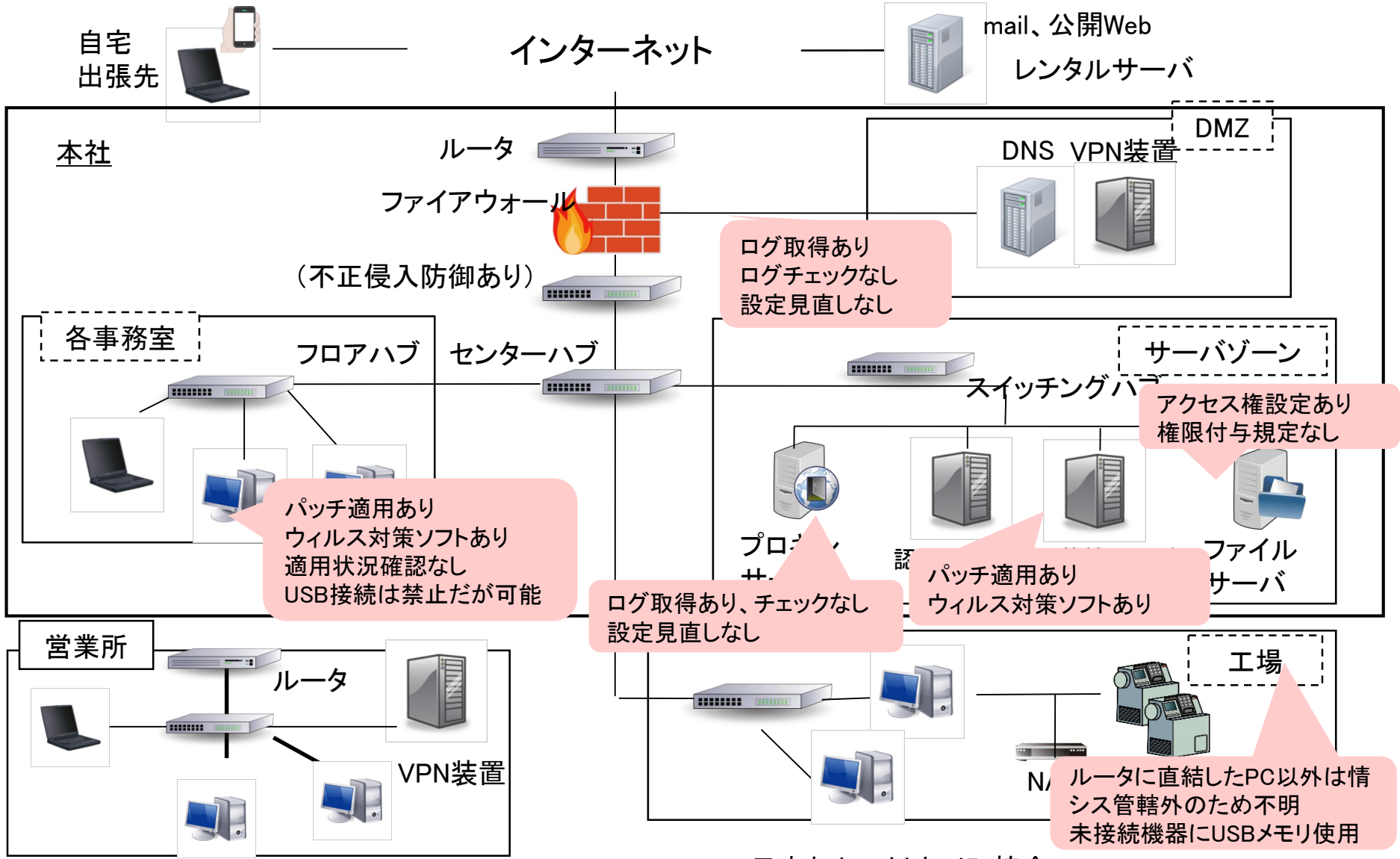
Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業のシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業のシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業(装置系)の外部状況

影響元	状況		セキュリティ目的・範囲・レベル
マクロ環境	社会・文化	・働き方改革や育児介護との両立のための施策が求められている ・高齢化に伴いヘルスケア製品が注目される	・自社ビジネスの維持、拡大のため、開発技術情報の保護 ・顧客への自社ビジネスの維持、拡大のため、顧客仕様、顧客技術情報の保護
	政治・経済	・国内市場は縮小傾向、ASEANなどアジア新興国の市場が拡大 ・為替と人件費高で中国生産のコストが増大	
	技術	・IoT,AIの生産現場への応用が進んでいる	
	法律・規制	・改正不正競争防止法による営業秘密保護強化 ・サイバーセキュリティに対し経営ガイドラインで経営層への要求	
ミクロ環境	競争環境	・モジュール化が進み新興国でも新製品開発が容易になり、差別化を図ることが必須	
	市場	・安い量産品と高付加価値の個別製品に二分化	
外部との関係	顧客	・顧客の情報セキュリティ要求 （中国への設計情報開示、新製品の開発情報漏洩防止）	

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業(装置系)の内部状況

影響元	状況	
組織体制 方針・戦略	方針	・IT活用により、受発注・生産管理の効率向上を目指す
	情報ｾｷｭﾘﾃｨ ﾎﾟﾘｼｰ	・利用者を対象にした主にPC利用の規定のみ ・開発情報保護、営業情報保護の対策方針の欠落 ・海外工場との間のデータ授受やデータ管理の取り決め不足
	体制	・情報システム部は存在する ・組織横通しの情報ｾｷｭﾘﾃｨ委員会、SOC、CERT機能はない ・危機管理体制はあるが、製品問題、特許、従業員の就労問題、災害対策が主 ・工場のネットワークは生産管理部門まかせで情報システムは関与しない ・ISO9001とISO14001の認証取得しており、開発情報や営業情報の手続きはQMSの手順書で定められており、運用のチェックも行われている
	役割	・CIO、CISOが不在、情報管理責任者は情報システム部長 ・QMS、EMS関連はISO事務局(総務の兼任者)が取りまとめている
内部影響 因子	経営者	・IT投資により業績向上を図りたいと考えている ・働き方改革や育児介護との両立支援のため、テレワークの導入に前向き ・情報ｾｷｭﾘﾃｨ対策の必要性は理解、現状とやるべき事は把握できていない ・セキュリティ事故の影響に気が付いていない
	情報ｼｽﾃﾑ部門	・社員のPCとサーバの管理、システムの不具合対応など2人＋兼務部長1人 ・サーバのバックアップは行うが、セキュリティ観点の運用はない
	その他の部門	・QMSの手順や決まりに従って業務を進める文化が定着している
リソース	人員	・明確な情報セキュリティ担当者はいない ・社内システムの構築は外部に委託している
	技術	・リスク評価、必要な対策を決定、運用する技術力はない

Copyright (c) 2000-2018 NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

製造企業(装置系)　評価

現状

・全社的な情報セキュリティ体制、取組み不足
・ISO9001を取得しており、QMSに基づいて仕事を行っているが、情報セキュリティの観点が抜けている
・事故対応に支障の恐れ
・セキュリティ推進体制、インシデント対応体制がない
・開発情報、営業情報の管理はQMSのルールに則って完全性や可用性が重視され、機密性の観点において情報システムとの連携や、インシデント対策が不足
・工場のネットワークが管理されていないため、トラブル発生時の対応が遅れる恐れ

あるべき姿

・自社開発技術力の優位性を確保し、IT活用で生産性を向上させ、売上・利益拡大
・テレワーク導入など働き方整備で人材確保
・開発技術情報、製造情報の保護
・顧客仕様、顧客技術情報の保護
・工場ネットワークとの統合、管理体制の構築
・社外から社内ネットワークへの安全な接続を実現
・IT、セキュリティ事故時の早期復元を可能とする体制の確立、そのための準備

差異

・情報管理上、機密性確保の観点が不足
・技術情報の保護、事故対応に支障をきたす脆弱な体制、ルール
・工場や社外とネットワークが安全に接続できるシステムになっていない

起こりうる被害

自社の技術情報、顧客技術情報の毀損、漏洩、およびそれに伴う競争力の低下、契約の停止による売上の減少
生産効率化遅れによる費用増加で利益減少、育児介護により社員が離職し生産性低下、採用費用の増加

売上/利益の減少、損金の発生	顧客の技術情報の毀損、漏洩による契約の打ち切り、損害賠償 裁判費用 bbb万円　損害賠償 ccc万円
売上/利益の減少	受注情報、生産技術情報の毀損により製品出荷の停止 生産管理システム、受発注システムの停止による製品出荷の停止 出荷停止による売上損 aaaa万円
費用の増加	工場とのネットワーク統合遅れで生産効率低下、生産能力不足による失注 社員離職にともなう人材採用費用　ddd万円

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

改善

技術情報、受注情報を含む顧客情報の保護の徹底とインシデント時における早期復旧体制、準備

現状売上　mmm万円/年　　現状利益　nnn万円/年
改修費用回収予想　q年後
増加ランニング費用　ooo万円/年
現状利益確保に必要な売上　　ppp万円/年(+rrr%増)

改善策

技術情報、受注情報を含む顧客情報の安全性の確保
①～②を今年度で対応、③を次年度に対応

① 情報セキュリティ侵害時の被害の最小化	<今年度　xxx万円の改修 >
② 営業秘密情報へのアクセス管理の徹底	<今年度　yyy万円の改修 >
③ 安全性の定期的な確認、見直しの実施	<次年度以降　zzz万円/年>
①、②に伴う保守費、委託費	<次年度以降　sss万円/年>

通常時と事故などの異常時における、自社と協力会社との役割分担の見直し、責任の明確化、及び自社ビジネスを支えるシステムの運用体制の再構築

① 営業秘密情報の明確化と不正競争防止法対応のルール化　<今年度　aaa万円で検討>
② 事故発生時における社内、協力会社の役割の見直し、ルール化
　< 今年度　bbb万円で検討>
③ 社内、協力会社の推進体制の構築・運用
　<今年度　bbb万円、次年度以降 ccc万円/年>

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

技術対策

自社の技術情報、生産技術、受注情報などの安全性の確保
工場ネットワークとの統合、社外から社内ネットワークへの安全なアクセス方法の確立

具体策

自社の技術情報、生産技術、受注情報などの保護、安全な取り扱いのため、PCを含む社内システムでの情報セキュリティ対策を強化する
①～②を今年度で対応、③以降を次年度に対応

① 技術情報を格納するファイルサーバのアクセス管理
　技術情報へのアクセス権の明確化と設定
② PCのセキュリティ対策の強化
　パッチ適用、ウィルス対策ソフトの最新化状況の把握とフォローアップ
　USBなど外部媒体の接続制限と許可したUSBのみ利用可能とするなど
③ 本社ネットワークのセグメント分割
　サーバ、部門でのネットワークセグメント分割とセグメント間のアクセス管理
④ ログ管理の強化
　取得ログの見直しとログ保全、ログ確認のシステム化　　など

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業　情報系

製造業企業概要

【会社のビジネス概要】
・化学工業メーカ、他製造業を顧客とし、触媒、セラミックなどを提供。
・自社の保有する技術を生かし、新しい分野にも進出。

従業員	300名
売上	200億

企業IT活用方針	・IT活用は生産管理が主、研究、開発用にPC、サーバを利用 ・工場におけるIoT活用（製造機械の稼働状態、製造過程の状態をセンサーで収集、将来は完全自動化まで）を目指す
情報セキュリティポリシー	・利用者を対象にした主にPC利用の規定のみ
体制	・情報システム部は存在する ・組織横通しの情報セキュリティ委員会、SOC、CERT機能はない ・危機管理体制はあるが、製品問題、特許、従業員の就労問題、災害対策が主
役割	・CIO、CISOが不在、情報管理責任者は情報システム部長
経営者	・IT投資は行う ・情報セキュリティ対策の必要性は理解、現状および何から、どこまで着手すべきか把握できていない ・他社の対策状況を気にする
情報システム部門	・主業務は基盤整備、5人 ・工場は生産管理部門の管轄、情報システム部門は関与しない

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

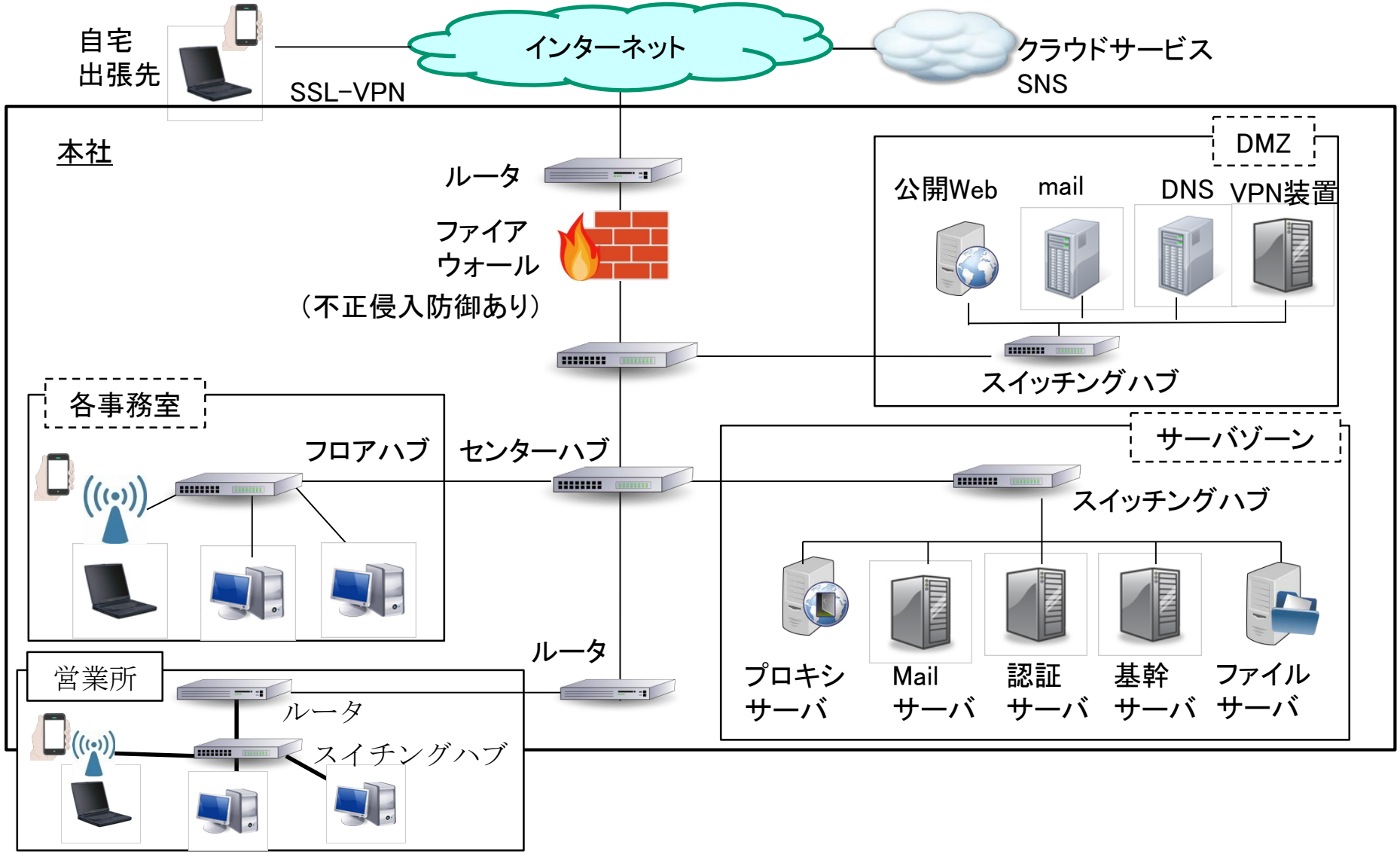
製造業のIT関連の詳細

【会社のビジネス、システム詳細】

・IT活用は生産管理が主、研究、開発用にPC、サーバを利用
・オンプレに公開Webサーバ、メール環境を構築
・オンプレのDMZは、FW(IPS機能あり)を設置、ログは取得するがチェックはしていない
・proxyあり、ログは取得するがチェックはしていない
・人事給与、生産管理、受発注管理、経理などの基幹サーバ、研究開発用のファイルサーバはサーバ室に設置、事務所のネットワークはL2で接続し、同じセグメントにある
・ DMZ、社内のサーバへのアクセスログは取得するが、チェックはしていない
・研究開発用のファイルサーバは認証は行っているが、アクセス管理はない
・PCにUSB接続は自由
・何が営業秘密情報となるか、明確化されていない
・PCにAVを導入し最新化とパッチも適用することになっているが、実態は把握できていない
・サーバはDMZ、社内ともパッチ未適用、AVの導入のみ、バックアップは情報システム部が管理

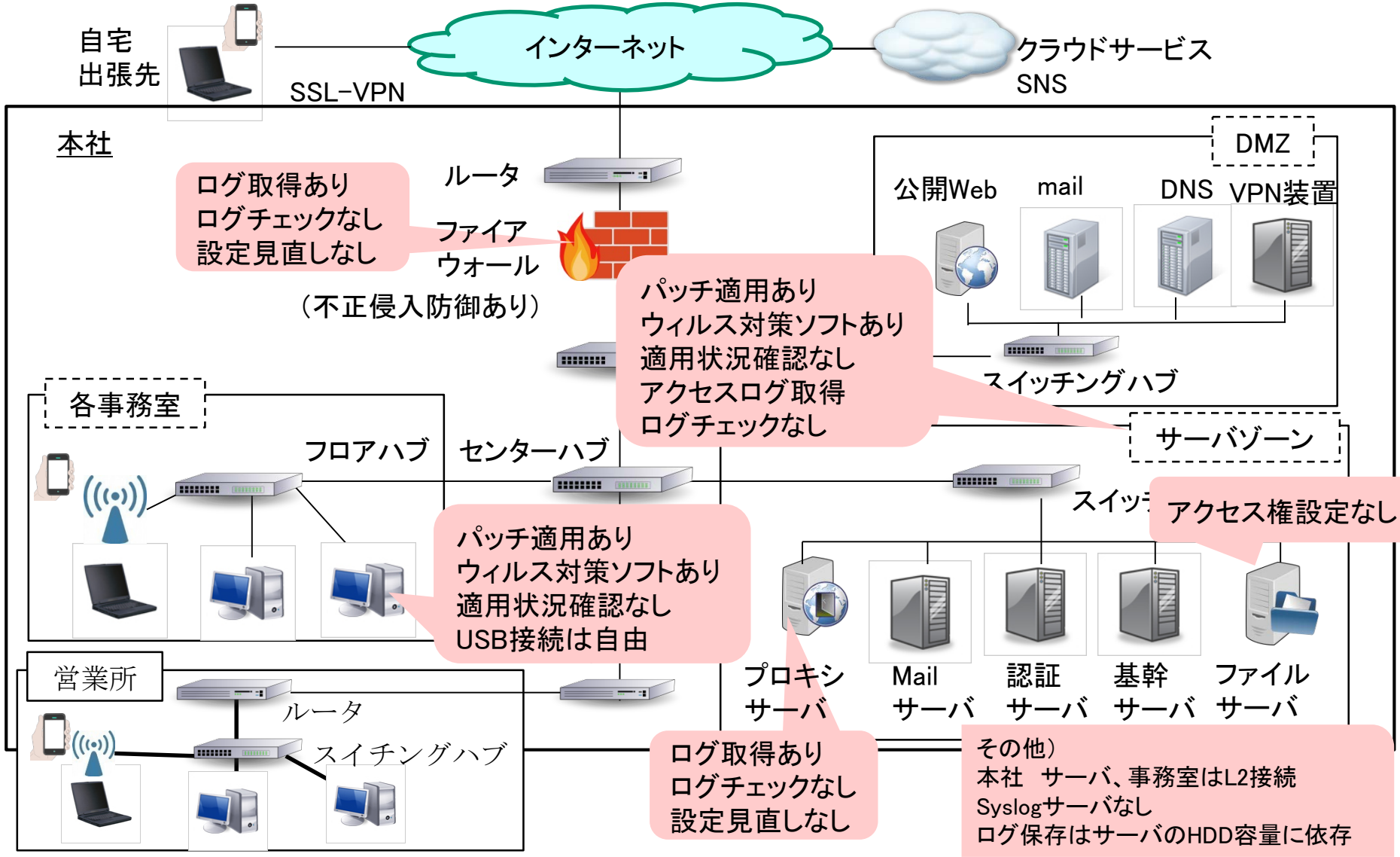
Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業のシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業のシステム構成



Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業の外部状況

影響元	状況		セキュリティ目的・範囲・レベル
マクロ環境	社会・文化	・環境保護、省エネルギーへの関心の高まりにより、それを支える素材分野が注目されている	・自社ビジネスの維持、拡大のため研究開発技術情報の保護 ・顧客への自社ビジネスの維持、拡大のため、顧客仕様、顧客技術情報の保護
	政治	・海外子会社とのコミュニケーションを阻害する外国政府の政策	
	技術	・早い技術革新	
	法律・規制	・改正不正競争防止法による営業秘密保護強化 ・サイバーセキュリティ経営ガイドラインでの経営層への要求	
ミクロ環境	競争環境	・他社との技術開発競争の動向次第で、自社の技術が陳腐化	
外部との関係	顧客	・顧客の情報セキュリティ要求 （セキュリティレベルと契約のリンク） ・厳しいコスト削減要求	

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

製造業の内部状況

影響元	状況	
組織体制 方針・戦略	方針	・IT活用は生産管理が主、研究、開発用にPC、サーバを利用
	情報ｾｷｭﾘﾃｨ ﾎﾟﾘｼｰ	・利用者を対象にした主にPC利用の規定のみ ・技術情報保護の観点による対策方針の欠落
	体制	・情報システム部は存在する ・組織横通しの情報ｾｷｭﾘﾃｨ委員会、SOC、CERT機能はない ・危機管理体制はあるが、製品問題、特許、従業員の就労問題、災害対策が主
	役割	・CIO、CISOが不在、情報管理責任者は情報システム部長
内部影響 因子	経営者	・IT投資は行う ・情報ｾｷｭﾘﾃｨ対策の必要性は理解、現状および何から、どこまで着手すべきか把握できていない ・セキュリティ事故の影響に気が付いていない ・他社の対策状況を気にする
	情報ｼｽﾃﾑ部門	・主業務は基盤整備、5人 ・サーバのバックアップは行うが、セキュリティ観点の運用はない
リソース	人員	・明確な情報セキュリティ担当者はいない ・情報システム部門の人材のみでは社内システムの構築、運用人員が不足するため、外部委託している
	技術	・リスク評価、必要な対策を決定し、運用する技術力はない

Copyright (c) 2000-2018　NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

製造企業　評価

現状

・全社的な情報セキュリティ体制及び取組み不足
・セキュリティ推進、事故対応に支障の恐れ
・インシデント対応体制がない、準備がない
・人の権限管理不足やUSB管理不足により、技術情報の持ち出し、漏洩のリスクがある
・営業秘密情報の定義が不明確

目指す姿

自社技術情報の優位性を確保したビジネス
・研究開発技術情報や優位性を持つ技術情報の保護
・顧客仕様、顧客技術情報の保護
・IT、セキュリティ事故時の早期復元を可能とする体制の確立、そのための準備
・不正競争防止法による営業秘密保護強化

差異

・自社、顧客の技術情報や受注情報の保護に不十分であり基本的な情報セキュリティ対策
・技術情報の保護、事故対応に支障をきたす脆弱な体制、ルール

起こりうる被害

自社の技術情報、顧客技術情報の毀損、漏洩、およびそれに伴う競争力の低下、契約の停止による売上の減少

開発への投資費用の回収不可	自社の技術情報の毀損、漏洩により他社との競争に負ける
売上計画の損失	営業秘密としての扱い不足により法的に保護されない 投資費用未回収　xxxx万円　売上計画の損失　yyyy万円
売上/利益の減少、損金の発生	顧客の技術情報の毀損、漏洩による契約の打ち切り、損害賠償 裁判費用 bbb万円　　損害賠償 ccc万円
売上/利益の減少	受注情報、生産技術情報の毀損により製品出荷の停止 生産管理システム、受発注システムの停止による製品出荷の停止 出荷停止のよる売上損 aaaa万円

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

改善

技術情報、受注情報を含む顧客情報の保護の徹底とインシデント時における早期復旧体制、準備

現状売上　mmm万円/年　　現状利益　nnn万円/年
改修費用回収予想　q年後
増加ランニング費用　ooo万円/年
現状利益確保に必要な売上　　ppp万円/年(+rrr%増)

改善策

技術情報、受注情報を含む顧客情報の安全性の確保
①～②を1年で対応、③をその次年に対応

① 情報セキュリティ侵害時の被害の最小化	<今年度　xxx万円の改修 >
② 営業秘密情報へのアクセス管理の徹底	<今年度　yyy万円の改修 >
③ 安全性の定期的な確認、見直しの実施	<次年度以降　zzz万円/年>
①、②に伴う保守費、委託費	<次年度以降　sss万円/年>

通常時と事故などの異常時における、自社と協力会社との役割分担の見直し、責任の明確化、及び自社ビジネスを支えるシステムの運用体制の再構築

① 営業秘密情報の明確化と不正競争防止法対応のルール化　<今年度　aaa万円で検討>
② 事故発生時における社内、協力会社の役割の見直し、ルール化
　< 今年度　bbb万円で検討>
③ 社内、協力会社の推進体制の構築・運用
　<今年度　bbb万円、次年度以降 ccc万円/年>

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会

技術対策

自社の技術情報、生産技術、受注情報などの安全性の確保

具体策

自社の技術情報、生産技術、受注情報などの保護、安全な取り扱いのため、PCを含む社内システムでの情報セキュリティ対策を強化する
①～②を1年で対応、③以降をその次年に対応

① 技術情報を格納するファイルサーバのアクセス管理
　技術情報へのアクセス権の明確化と設定
② PCのセキュリティ対策の強化
　パッチ適用、ウィルス対策ソフトの最新化状況の把握とフォローアップ
　USBなどの外部媒体の接続制限と許可したUSBのみに利用制限　　など
③ 本社ネットワークのセグメント分割
　サーバ、部門でのネットワークセグメント分割とセグメント間のアクセス管理
④ ログ管理の強化
　取得ログの見直しとログ保全、ログ確認のシステム化　　など

Copyright (c) 2000-2018　NPO日本ネットワークセキュリティ協会