Advanced Technology, Secu Japan co.ltd.

ReceiveGUARD

Cooperate, Creative & Customizing
= 3C Rules

『 APT、BEC(ビジネスメール詐欺)攻撃に対する唯一の対応可能なソリューション』

ReceiveGUARD

Contents

ReceiveGUARD

Ⅰ. メールセキュリティの重要性

1.メール攻撃の現状

2.メール攻撃事例

3.保安管理政府の予防ガイド

4. Receive GUARD

1.メール攻撃の現状

インターネットインフラの増加によるハッカーのメール攻撃270%急増

ランサムウェア被害増加率

2015年被害金額約1,090億円
2016年被害金額約3,000億円

出典:KISA 2017ランサムウェアの動向報告書

APT攻撃メール申告現況

2014年、申告841件
2015年、申告1,305件

出典:KISA 2016サイバー脅威動向報告書

ハッキングの流入ルートメール

ランサムウェア/APT攻撃の流入ルート
メール87%

出典:パロアルトネットワークスの報告書

2.メール攻撃類型別事例

Ⅰ.従来の同一メールアドレス攻撃

HACKER

使用者の同一のメールアドレスを使用して
相手に詐欺メールを発送

普段からメールのやり取りをしたアカウントから来た
メールだから何の疑いもなくメールを確認して被害発生

USER

Ⅱ.類似ドメインアドレス攻撃

HACKER

使用者が目で確認することが不可能なように正常のアカウント
と 同様にアカウントを生成して詐欺メールを送信

普段からメールのやり取りをしたアカウントから来た
メールだから何の疑いもなくメールを確認して被害発生

USER

Case 1 2017. 12

J社、ハッキングメール詐欺で3.8億円の被害

ⅰ.取引先偽装ハッキングメール受信
ⅱ.ウイルスない正常なメールで攻撃
ⅲ.取引代金3.8億円のハッカーに送金

JALの3.8億円振り込め詐欺に見られるBEC
(ビジネスメール詐欺)

“日本航空は２０日、約３億８千万円の「振り込め詐欺」の被害に遭ったと発表した。取引先になりすましたメールで航空機リース料などの支払いを要求され、応じてしまったという。
日航の説明では、取引のある金融会社の担当者を装うメールが９月２５日に届き、支払口座を香港の銀行に変更したと伝えてきた。送信元のアドレスは画面表示上、担当者のものと同じだったため、日航側は信じて同月２９日に約３億６千万円を送金した。翌１０月、本物の金融会社から督促があり、だまされたことがわかったという。香港の銀行からはすでに金は引き出されていた。

出典：ＪＡＬが振り込め詐欺被害　「航空機リース料」信じる

Case 2

L社、ハッキングメール詐欺で24億円の被害

ⅰ.取引先偽装ハッキングメール受信
ⅱ.ウイルスない正常なメールで攻撃
ⅲ.取引代金3.8億円のハッカーに送金

2.メール攻撃類型別事例

Ⅲ.ヘッダの偽造•変造攻撃

HACKER

使用者と実際の送受信しているドメインを使用して
悪性ファイルを添付して、メール送信

取引会社のドメインから受信されたメールなので疑いもなく
メールの閲覧および添付ファイルダウンロードして被害発生

USER

Case 3

D社 A部長、本社ドメインとして偽装されているメールで・ランサムウェア襲撃される

ⅰ。会社のメールアカウントと同じドメインから送信されたメール何通を発見
ⅱ。疑われることなく、添付ファイル実行
ⅲ。変種・ランサムウェアで会社ネットワークに拡大

Ⅳ. 本文悪性URL攻撃

HACKER

税金報告のソフトウェア会社に見せかけて、税金報告代行者に
悪性コードが植えつけられたウェブサイトリンク添付して、メール送信

税金報告用ソフトウェア会社だと思って本文に込められたリンククリックしてpcに悪性コードが植えられて会社の情報流出

USER

Case 4

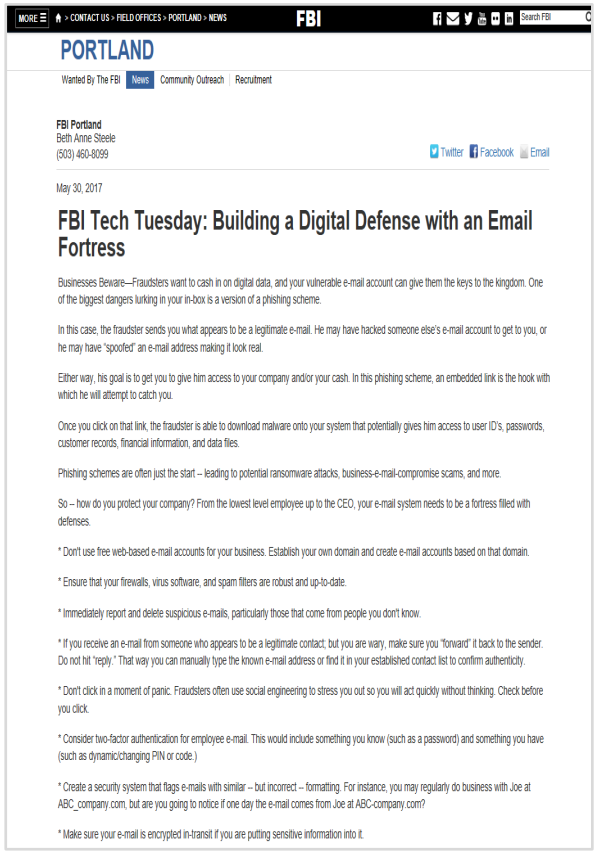
会計士、税理士ターゲット新型メール、フィッシング詐欺

ⅰ。税金報告代行者ターゲット新型メール、フィッシング詐欺登場
ⅱ。税金報告の会社を装ってウェブサイトリンクかかったメールでソフトウェアアップデート設置するように誘引
ⅲ。会社の情報、金融情報を疑いなく流出する事故

3.保安管理政府の予防ガイド

セキュリティの一般的な勧告事項の提示!

FBI



MORE ☰ > CONTACT US > FIELD OFFICES > PORTLAND > NEWS FBI Search FBI

PORTLAND

Wanted By The FBI | News | Community Outreach | Recruitment

FBI Portland
Beth Anne Steele
(503) 460-8099

Twitter Facebook Email

May 30, 2017

FBI Tech Tuesday: Building a Digital Defense with an Email Fortress

Businesses Beware—Fraudsters want to cash in on digital data, and your vulnerable e-mail account can give them the keys to the kingdom. One of the biggest dangers lurking in your in-box is a version of a phishing scheme.

In this case, the fraudster sends you what appears to be a legitimate e-mail. He may have hacked someone else's e-mail account to get to you, or he may have "spoofed" an e-mail address making it look real.

Either way, his goal is to get you to give him access to your company and/or your cash. In this phishing scheme, an embedded link is the hook with which he will attempt to catch you.

Once you click on that link, the fraudster is able to download malware onto your system that potentially gives him access to user ID's, passwords, customer records, financial information, and data files.

Phishing schemes are often just the start -- leading to potential ransomware attacks, business-e-mail-compromise scams, and more.

So – how do you protect your company? From the lowest level employee up to the CEO, your e-mail system needs to be a fortress filled with defenses.

* Don't use free web-based e-mail accounts for your business. Establish your own domain and create e-mail accounts based on that domain.

* Ensure that your firewalls, virus software, and spam filters are robust and up-to-date.

* Immediately report and delete suspicious e-mails, particularly those that come from people you don't know.

* If you receive an e-mail from someone who appears to be a legitimate contact, but you are wary, make sure you "forward" it back to the sender. Do not hit "reply." That way you can manually type the known e-mail address or find it in your established contact list to confirm authenticity.

* Don't click in a moment of panic. Fraudsters often use social engineering to stress you out so you will act quickly without thinking. Check before you click.

* Consider two-factor authentication for employee e-mail. This would include something you know (such as a password) and something you have (such as dynamic/changing PIN or code.)

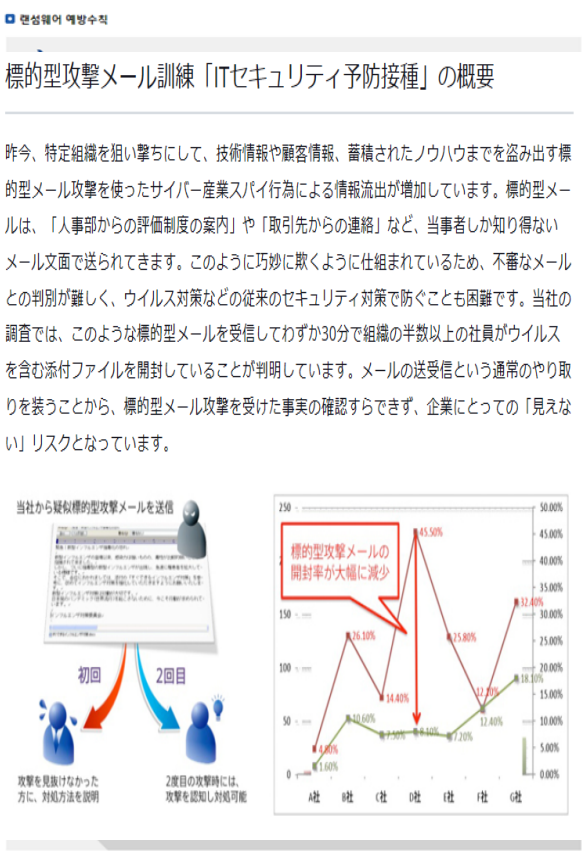
* Create a security system that flags e-mails with similar -- but incorrect -- formatting. For instance, you may regularly do business with Joe at ABC_company.com, but are you going to notice if one day the e-mail comes from Joe at ABC-company.com?

* Make sure your e-mail is encrypted in-transit if you are putting sensitive information into it.

2017. 05. 30

- 事業用メールは無料のウェブメールがなく、独自ドメインサーバを構築し、アカウントを生成する
- ファイアウォール、ウイルスソフトウェアおよびスパムフィルターが常に最新の状態で正常に作動したか どうかを確認する
- 知らない人が送信した不審なメールは直ちに 報告して削除すること
- 正常に見えるの口座でもらったメールが疑わらしば、回答がない伝送を押して当該メール 住所の真偽を確認すること
- 何も考えずに受けたメールを考えず開いて見ないこと
- メールログインの2段階の認証を考慮する
- 規則的にやり取りする電子メール住所はフラグを利用して区分すること
- 重要情報は伝送時に暗号化になって送信されるか確認すること

日本政府



랜섬웨어 예방수칙

標的型攻撃メール訓練「ITセキュリティ予防接種」の概要

昨今、特定組織を狙い撃ちにして、技術情報や顧客情報、蓄積されたノウハウまでを盗み出す標的型メール攻撃を使ったサイバー産業スパイ行為による情報流出が増加しています。標的型メールは、「人事部からの評価制度の案内」や「取引先からの連絡」など、当事者しか知り得ないメール文面で送られてきます。このように巧妙に欺くように仕組まれているため、不審なメールとの判別が難しく、ウイルス対策などの従来のセキュリティ対策で防ぐことも困難です。当社の調査では、このような標的型メールを受信してわずか30分で組織の半数以上の社員がウイルスを含む添付ファイルを開封していることが判明しています。メールの送受信という通常のやり取りを装うことから、標的型メール攻撃を受けた事実の確認すらできず、企業にとっての「見えない」リスクとなっています。

勧告事項

1。すべてのソフトウェアは最新バージョンにアップデートして 使用する。

2.ワクチン・ソフトを設置して、最新バージョンにアップデートする。

3.疑わしいメールとURLリンクは実行しない事

4.ファイル共有サイトなどでファイルのダウンロードや実行に 注意しなければならない。

5.重要資料は定期的にバックアップしなければならない。

企業の対応策

6.バックアップ体制構築や運営を通じたセキュリティー強化

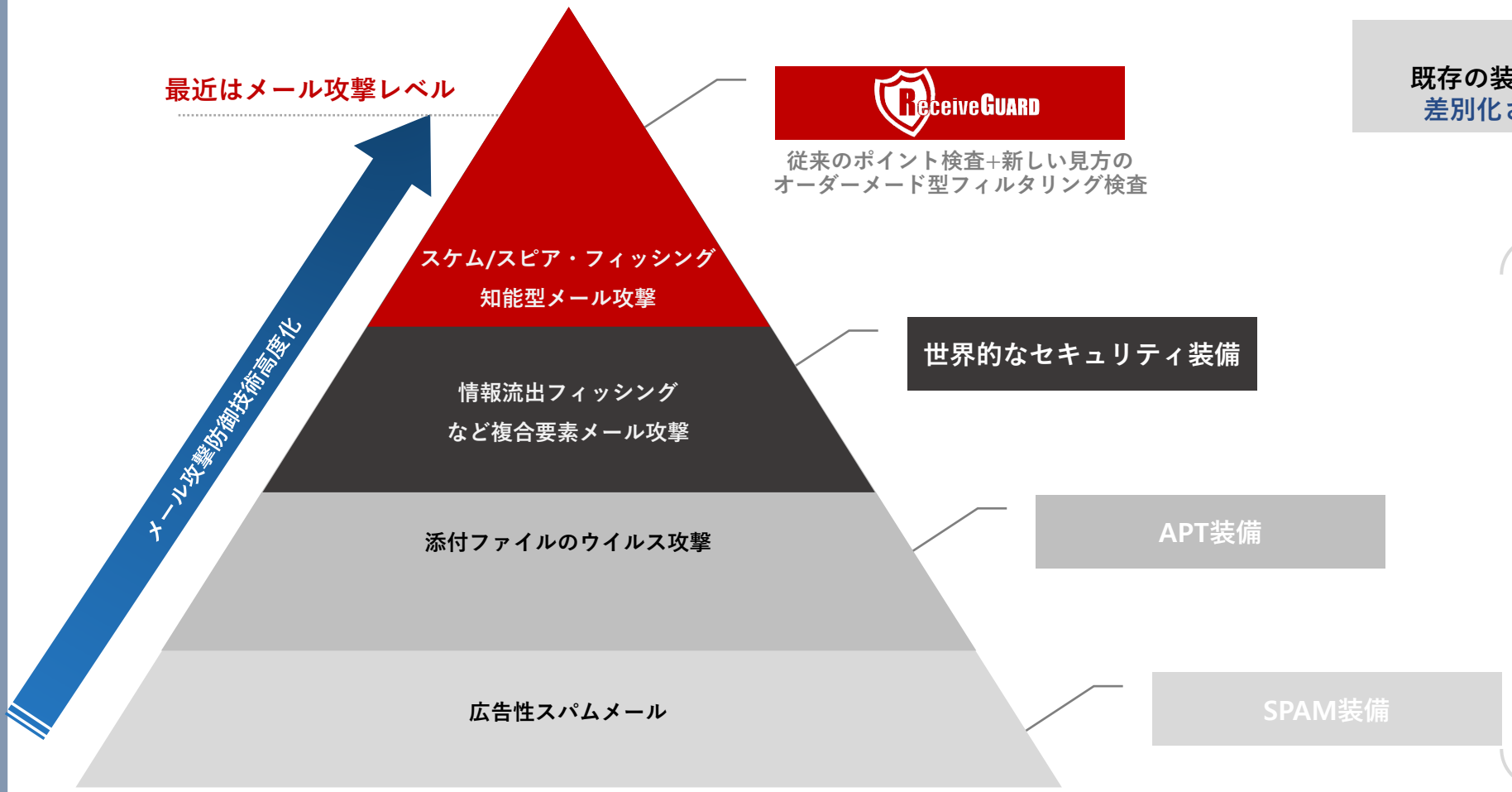
7.迷惑メールセキュリティソリューションを通じた迷惑メール遮断すること

8.パッチの管理システムなどのセキュリティ装備を利用した役員 PCセキュリティアップデート

9.周期的な役職員や一般社員に対するセキュリティ教育実施

3. Receive GUARD

特定対象を狙うメール攻撃!オーダーメード型フィルタリングに安全なメールの環境構築



Receive GUARDは
既存の装備が検査しないポイントまで検査する
差別化された次世代メールセキュリティ製品

既存の装備の検査では進化した
社会工学的/知能型メール
攻撃に無策!

3. Receive GUARD

社会工学的なハッキング攻撃, ReceiveGUARD だけが唯一の先制対応ソリューション!

Gartnerで技術力を認めたe-mailセキュリティ

詐欺メール唯一対応ソリューション

APT攻撃及び金融詐欺などBEC(Business e-mail Compromise)攻撃にメールエンジンの開発及びe-mail

サービスのノウハウに、体系的かつ適当なフィルタリングシステムで、世界唯一の先制対応可能

AIとメールセキュリティの結合

2017のガートナーIT 10代トレンドであるAIとセキュリティ技術の融合!Receive GUARDが先導!

マシンラーニングを通じたデータの蓄積から信頼度プログラムを適用、危険有無を自ら判断

ランサムウェア(新型悪性コード)の遮断

行為の基盤動的解析を通じて添付ファイルの危険性を判断、新型ランサムウェア危険を事前に遮断

既存のアンチウイルス製品の短所である
パターンアップデートの静的解析の限界を克服

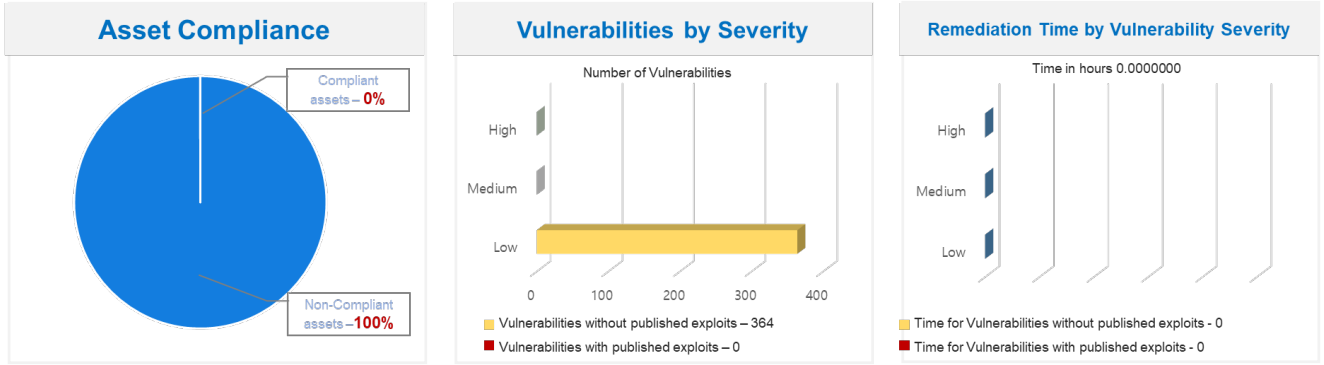
4. Receive GUARD

世界が認めた**革新的な次世代**メールセキュリティ製品 ReceiveGUARD

Gartner®

"Receive GUARDは他のe-mailセキュリティ製品の弱点だったTargeting攻撃とパターン化されていない
ハッキング攻撃を**AIとMachine learningを通じて補完する必ず必要な次世代革新e-mailセキュリティ製品**"
2017-03

RAPID7
国際セキュリティ製品の認証テスト



シンガポール政府調達登録に向けた計364つの脆弱点分析、テスト結果'**ホール0個**'の'**完全性製品**'判定
2017-09

3. Receive GUARD

独自のメールエンジンの保有企業が作った
メール専用セキュリティソリューション!!

2004
- メールエンジンの開発
- 技術の商用化及びサービスの開始

2014
- メールファイアウォール装備 Receive GUARD発売
- セキュリティe-mailエンジン SECU MAIL開発

2015
- SECU MAILサービスの商用 (使用者のメールセキュリティ強化)
- e-mailのセキュリティエンジン特許出願
- 世界初詐欺メール専用セキュリティソリューション発売

2017
- Receive GUARDの高度化
- 使用者専用のセキュリティ機能の適用
- 送信セキュリティメール高度化
- 国内初の自社開発e-mail セキュリティOne Stop Serviceの SCM GUARD Platform発売
- 日本の商用化サービス
- グローバルサービス (米国、欧州、東南アジア、中東)

ReceiveGUARD

Ⅱ. 製品紹介

1.主要機能

2.悪性メール検出例

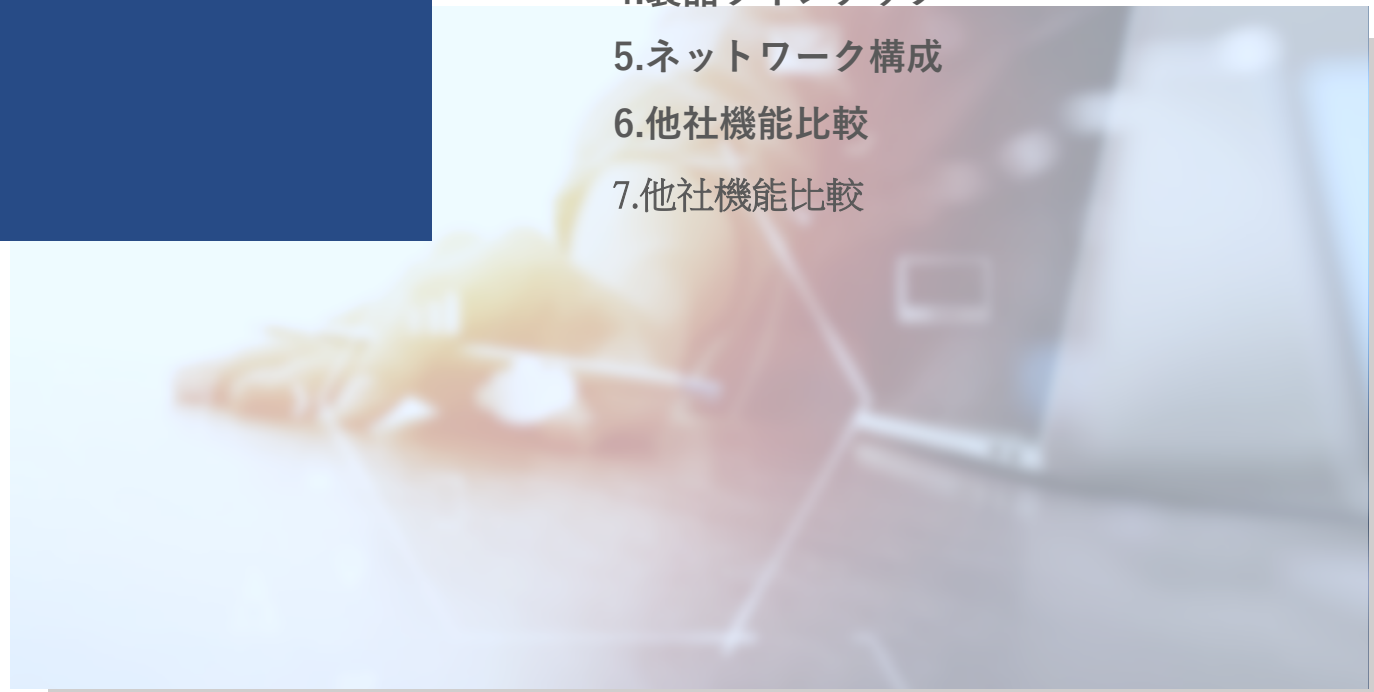
3.詳細機能

4.製品ラインナップ

5.ネットワーク構成

6.他社機能比較

7.他社機能比較



1.主要機能(1)

悪性メールの原因分析、オーダーメード型フィルタリング対応

仮想空間

- メール1件当たり必要な数だけVA投入し、リアルタイムでメールの確認
- 少なくとも1,000個以上のVA検査待機中
- メール速度向上及び検査の精度確保
- URL分析および偽造・変造ファイル分析、ウイルス探知、Malware探知

メールの信頼度表示

- VAで分析して学習した結果をもとに信頼度生成
- 受信する各メールごとに個別の信頼も構築
- 信頼度をもとに危険性を付与して使用者転送の有無を決定

知能型学習

- 遮断されたメールを使用者が許可した場合、当該メール原文全体分析
- 原文分析時の各例外事項に合うように自動でパターン生成
- パターンの変造を防ぐために流動暗号化方式で保管

ランサムウェアの遮断

- 基本添付ファイルに対して、ウィルスやMalware検査を進行
- 本文にリンクされたURLをVAで直接開いてみた後、ダウンロードできる
- ファイルがある場合VAであらかじめダウンロードして危険性検査
- Malwareのチェック機能を通じてファイル拡張子が変調された悪性コード
- 検出

リアルタイムURL分析

- 本文にリンクがつながっている住所はVAであらかじめ開けてみて
- 悪性コード検査
- 本文にリンクしたURLの確認結果、該当サイト内部に
- 追加リンクがあるなら、End-Pointまで追跡、追加の危険性の遮断

最初の送信経路追跡

- 各アカウント別に初メール送信経路情報保存
- メール再受信時保存された経路と比較
- 送信経路変更時に、警告メッセージ挿入

送信先アドレス偽造・変造を検査

- メール送信先アドレスの有効性をチェックして偽造・変造検査
- サーバは有効かは別に発信者アドレスの偽造・変造跡検出
- スヌピン攻撃の予防

危険性メールIMAGE変換

- フィルターされたメール送信の際、危険性メールIMAGE変換機能
- 遮断メールの中でメールの内部にURLリンクがある場合のメール
- 内容そのものをイメージに変換させて伝送
- 原文の再送信の要請時e-mail、パスワード入力後、勘定認証サーバと
- 通信を通じ確認した後、伝送

類似ドメイン検査

- 既存のドメインと類似性比較分析
- 危険のアカウントである場合、比較分析してから、警告表示

1.主要機能(2)

悪性メールの原因分析、オーダーメード型フィルタリング対応

レポート機能

- 管理者にレポート設定権限を付与
  (報告書は除外対象者および機能)
- レポート確認後、別途リンク接続後メール遮断/許可設定
- 使用者に遮断の内訳などに対する報告書、メール転送
- メール管理機能を通じて受信内訳の照会、メール遮断、メール許容機能を提供

業務/広告メール区分管理

- メール本文とメールヘッダなどの一定のパターンを通じてメール区分管理
- 別の統計を通じて簡単にメール管理

ロードバランシング

- メールサーバトラフィックの状態を確認後使用量を分配して伝送
- 大容量メール受信時の迅速な処理

偽造・変造ファイル分析

- PDF、HWP、DOC、PPTなど、一般的に使用する文書ファイルに偽装した 悪性コードとウイルスプログラム検出
- VAであらかじめ確認して、危険性の遮断

添付文書内の危険リンク検出

- メール内の添付された文書の本文を分析してリンク検出
- リンクの危険性をすでに累積された信頼度データを基に分析
- 自体データが累積されるほど、より明確な検出可能

メールのタイトルに警告文表示

- 遮断メールを容認する際、[BLOCK][WARNING]などの警告文章の掲載されて使用者に伝送
- 警告の文句の確認にメールの安全性確認
- 警告の文句は管理者が変更可能

アーカイブ

- 管理者が設定した周期的に個人バックアップ可能
- 失策で削除されたメールも復元可能
- Applianceだが、ウェブメールシステムと同一に保管適用
- 情報とファイルを取り外すことで実際のメール・システムと同一
- 原文保管

個人使用者フィルタリング構築

- メール遮断の際、個人使用者に周期的に報告書伝送
- 個人使用者専用ウェブページを通じてデータ管理
- 別途の中央の管理者がいないシステムに適用可能
- 多様な使用者の検証でより明確なフィルタリング確保

多様な支援

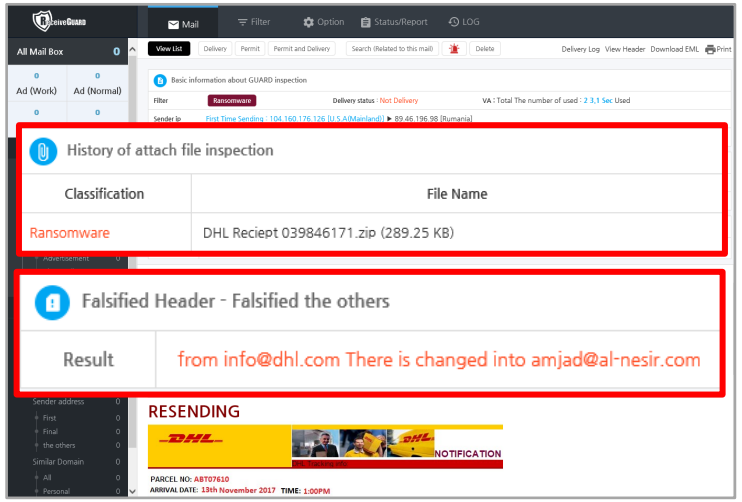
- 連結されたメールサーバと通信チェックが可能なウェブ管理者機能を提供
- RCPTの照会、メール転送結果に対するログ記録の照会可能
- 全体システムの運営に対するリアルタイム情報提供
- 内部施設網への流動設定提供

2.悪性メール検出例

Case 1

類似ドメイン利用・ランサムウェア攻撃

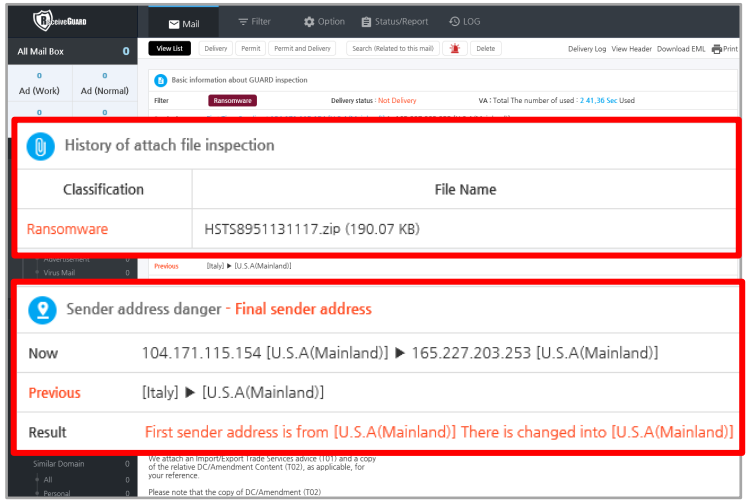
ⅰ。海外配送サービス会社(dhl>dlhl)に偽装
ⅱ。配送に情報確認要請文書伝達
ⅲ。・ランサムウェア添付攻撃を試み
ⅳ。Receive GUARDリアルタイム危険事前検出/遮断



Case 2

銀行アカウントのハッキング詐欺メール送信

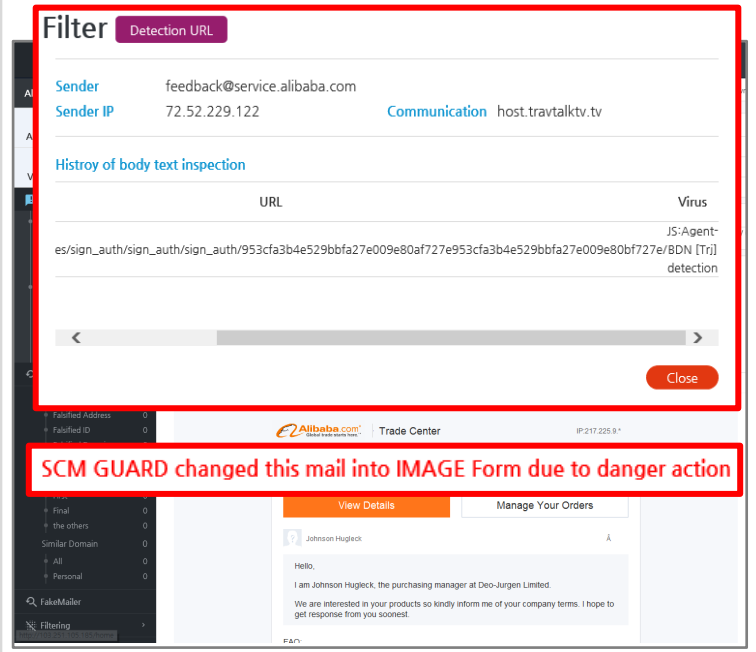
ⅰ。海外銀行(HSBC)メールアカウントのハッキング
ⅱ。秘密文書を装ったフィッシング攻撃を試み
ⅲ。詐欺を通じて企業の重要情報流出の試み
ⅳ。Receive GUARD送信経路探知/遮断



Case 3

ホスティング詐称本文URL攻撃

ⅰ。メールホスティング企業を装ったハッキングの試み
ⅱ。本文URLに・ランサムウェア実行リンク攻撃
ⅲ。URL検査の結果、悪性コード検出/遮断
ⅳ。使用者イメージでリンク無害化配信



3.詳細機能

世界唯一のAIのメールの分析システムVA

他社製品

他社の分析システム(VM)限界

-既存のVM方式は資源を固定型として配分して相互Shareがなることができない検査処理する方式で負荷が発生してキューが積もる問題発生

-固定されたリソース使用の方式でH/W、耐久性持続及びリソースの可用性に対する問題

-分析装備拡張時、過度な追加費用の発生

VS

ReceiveGUARD

独自開発Virtual Area(VA)のSolution

- Receive GUARDの独自のメールの分析技術人Virtual Areaを開発
- VAは資源に対するフリーの配分方式として検査に該当する難易度だけの資源を配分するように設計
- Core Resource Share方式でPerformance可用率を最大限活用
- 単一方式の既存製品問題点に対する解決策として多重方式のリソース共有のソリューションであるVA適用
  Core Resource Shareで最高の可用性の確保

VAの運営方式

- VAは、受信したe-mail検査項目に合わせてリアルタイム配分後の運営
- 受信時の割り当てをするコントロールエンジンで検査に必要なVA数と割当がなるVAに検査項目をOrderして運営される
- 検査が終わったVAは共有された資源がリセットされて検査中または始めなければならない部分に再配分

3.新型・ランサムウェア検出

TOTAL - 174　送信　削除

差出人	メール受信者	タイトル	フィルター	状態	受信日
indore.depot@hindware.c…		PURCHASE ORDER	検知	未転送	18-04-09 12:16
purchase@westcoastin.com		PURCHASE ORDER	ランサムウェア	未転送	18-04-06 11:49
purchase@westcoastin.com		PURCHASE ORDER	ランサムウェア	未転送	18-04-06 11:40
ah02a_cs@infiniumtoyota…		URGENT ORDER	検知	未転送	18-04-06 11:39
info@huayfenghang.com.sg		PROFOMA INVOICE	検知	未転送	18-04-06 11:38
Caleb@imaginefilms.tv		coupon_30_835410778	ランサムウェア	未転送	18-04-04 18:18
Caleb@imaginefilms.tv		coupon_30_835410778	ランサムウェア	未転送	18-04-04 18:17
Caleb@imaginefilms.tv		coupon_30_835410778	ランサムウェア	未転送	18-04-04 18:16
Caleb@imaginefilms.tv		coupon_30_835410778	ランサムウェア	未転送	18-04-04 18:15
Caleb@imaginefilms.tv		coupon_30_835410778	ランサムウェア	未転送	18-04-04 18:13
Caleb@imaginefilms.tv		coupon_30_835410778	ランサムウェア	未転送	18-04-04 18:10
Caleb@imaginefilms.tv		coupon_30_835410778	ランサムウェア	未転送	18-04-04 18:10
Caleb@imaginefilms.tv		coupon_30_835410778	ランサムウェア	未転送	18-04-04 18:06
admin@benaros.ml		DHL GLOBAL FORWARDING ARRIVAL NOTICE	ランサムウェア	未転送	18-04-04 18:02
admin@benaros.ml		DHL GLOBAL FORWARDING ARRIVAL NOTICE	ランサムウェア	未転送	18-04-04 17:56
admin@benaros.ml		DHL GLOBAL FORWARDING ARRIVAL NOTICE	ランサムウェア	未転送	18-04-04 17:53

添付ファイル検査の内訳

ファイル名	分類	内容
ZA77848787587785878989895 87.R21	ウイルス	Behavior Detection : Create file, Run process

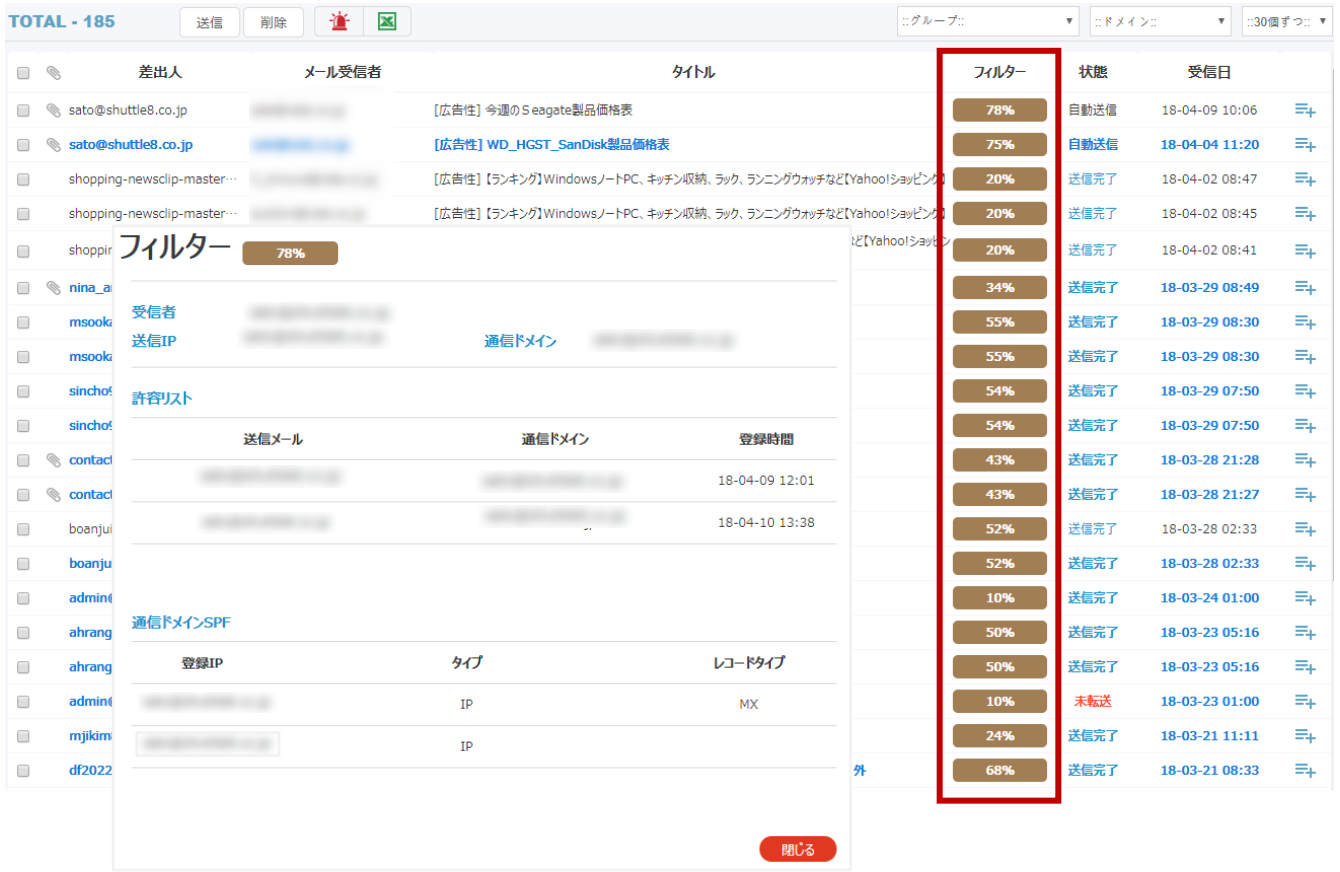
1次ワクチン検査　パターンのウィルス検査

- ウイルスパターン検査の実施
- 従来の更新された悪性コード検出

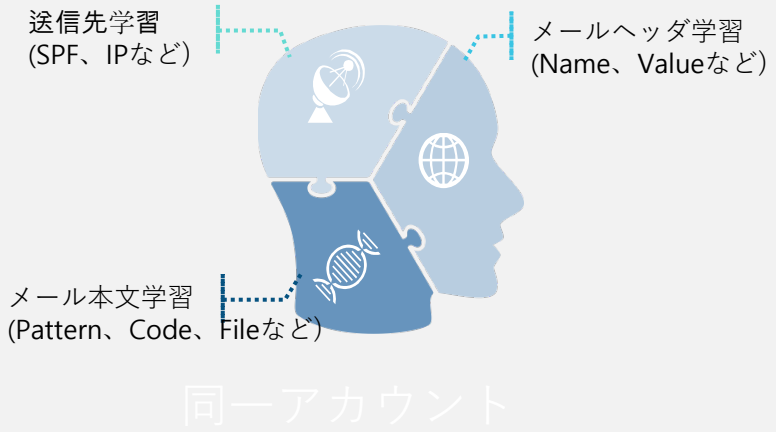
2次CUBE検査　ウィンドウ環境システムの変更感知検査

- 1次検査通過したファイルについて別途検査
- アップデートされていないファイルを、別途の安全な空間で実行
- ウインドウズシステムの変更が感知されれば、直ちに遮断

3.信頼度(ハッカー送信検出)

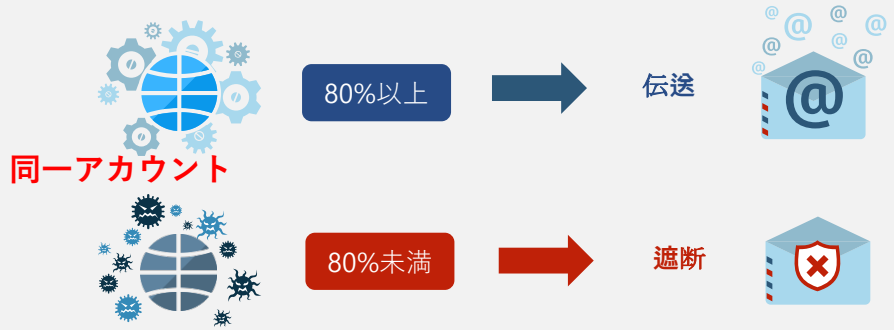


1. ID別の受信メールの情報分析・学習



同一アカウント

2.学習情報利用、受信メールの信頼度適用



3.送信先の追跡

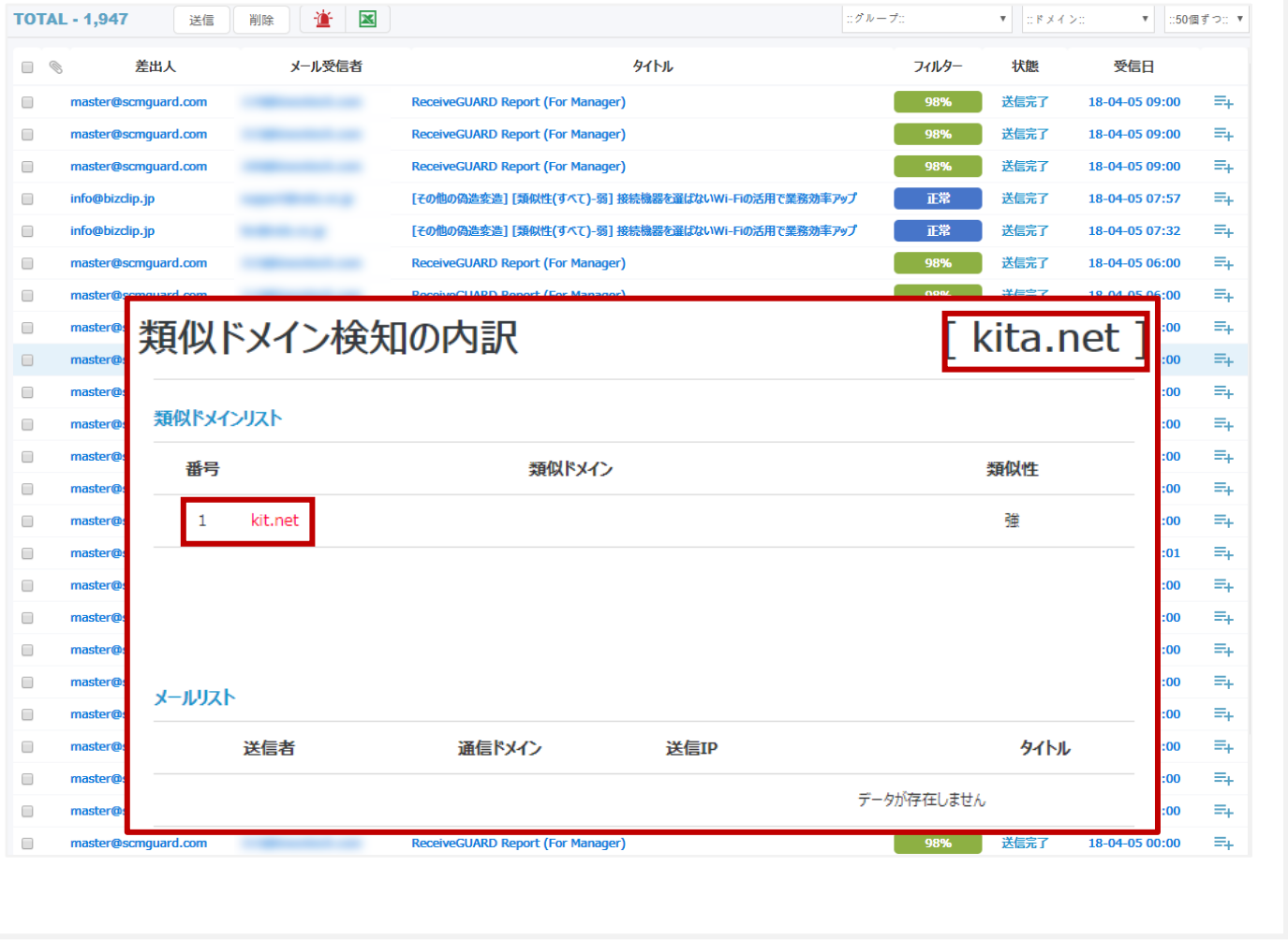
TOTAL - 1,050　送信　削除　::グループ::　::ドメイン::　::100個ずつ::

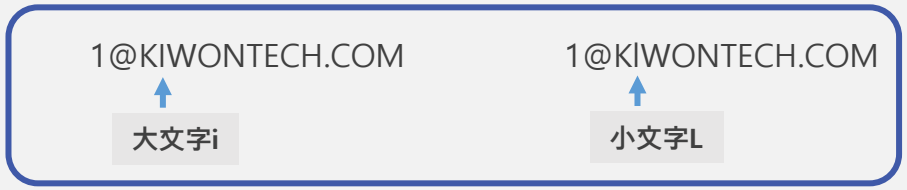
差出人	メール受信者	タイトル	フィルター	状態	受信日
info@transmarine.co.th		ETA NOTICE (6 DAYS) FOR LOADING ONE GRADE OF PHENOL IN BULK CLOSE TO 2,000MT AT THAI TANK TERMINAL MAPTAPHUT ,THAILAND - MT ORIENT PINE - V.18004	追跡	未転送	18-03-13 20:36
James.McNally@clarksons···		ExxonMobil - ONSAN CHEMI - 1, 3 or 5 Year Time Charter	追跡	未転送	18-03-13 20:36
st@odinsp.com.sg		Odin Marine: 1000MT Exxal9S, Singapore - Durban, 10 - 15 April	追跡	未転送	18-03-13 20:35
st@odinsp.com.sg		[ODIN MARINE] PALMS / OLEO CHEMS CARGOES TO AG / CHINA / INDIA / INTRA SEA / PAKISTAN	追跡	未転送	18-03-13 20:35
wss.thailand@wilhelmsen···		MT.SUNRISE ECO / V.18004 / NOMINATION MESSAGE / KOHSICHANG	追跡	未転送	18-03-13 20:33
wss.thailand@wilhelmsen···		RE: MT.SUNRISE ECO / V.18004 / NOMINATION MESSAGE / KOHSICHANG	追跡	未転送	18-03-13 20:33
WSS.ISTANBUL.SHIPSAG···		TRANSITING THROUGH TURKISH STRAITS 26.02.2018	追跡	未転送	18-03-13 20:33
st@odinsp.com.sg		[TrackingETC]RE: Eastern Chemi - Bunge/Sunwoo, CP 23 Feb 18, Laycan 08 - 16 Mar 18 (TBN), Lift #017-18	追跡	未転送	18-03-13 20:33
st@odinsp.com.sg		Odin Marine Transhipment Requirement - Ulsan to Mid China	追跡	未転送	18-03-13 20:31
st@odinsp.com.sg		[ODIN MARINE] PALMS / OLEO CHEMS CARGOES TO AG / CHINA / INDIA / INTRA SEA / PAKISTAN	追跡	未転送	18-03-13 20:31
YT.Lee@wilhelmsen.com		Daily #PortNews update//Port Moresby, Papua New Guinea - earthquake//	98%	未転送	18-03-13 20:29
James.McNally@clarksons···		RE: RE: ExxonMobil - ONSAN CHEMI - 1, 3 or 5 Year Time Charter	追跡	未転送	18-03-13 20:28
wss.thailand@wilhelmsen···		RE: MT.SUNRISE ECO / V.18004 / TENTATIVE ITINERARY / KOHSICHANG	98%	未転送	18-03-13 20:27

送信先が危険 - 最終的な送信先

現在	119.73.177.131 [シンガポール] ▶ 52.133.138.12 [米国] ▶ 104.47.126.125 [大韓民国]
移転	[香港] ▶ [米国] ▶ [シンガポール]
結果	最初の送信先が [シンガポール] から [大韓民国] に変更されました。

3. 類似ドメイン検出





類似性検出後の使用者に危険性のお知らせ

[類似性-危険]不審なメールアドレスとのやり取りをした場合、警告のお知らせ

[類似性-上] 1@KIWONTECH.com ->1@KIWONTECH.com (一つ検出)

[類似性-中] 1@KIWONTECH.com -> 1@KIW0NTECH.com (二つ検出)

[類似性-下] 1@KIWONTECH.com -> 1@KIW0MTECH.com (三つ検出)

正確な判断のため、個人別DB化索引分析

人の視線に区分すること大変な類似したドメイン検出

3.ヘッダの偽造変造

TOTAL - 409　送信　削除

差出人	メール受信者	タイトル	フィルター	状態	受信日
admin@benaros.ml		DHL GLOBAL FORWARDING ARRIVAL NOTICE	ランサムウェア	未転送	18-04-04 18:02
admin@benaros.ml		DHL GLOBAL FORWARDING ARRIVAL NOTICE	ランサムウェア	未転送	18-04-04 17:56
admin@benaros.ml		DHL GLOBAL FORWARDING ARRIVAL NOTICE	ランサムウェア	未転送	18-04-04 17:53
support@sys.jpdirect.jp		[業務性] [その他の偽造変造] 【重要】ドメイン名登録更新料のご請求	遮断	未転送	18-04-01 06:19
support@sys.jpdirect.jp		[業務性] [その他の偽造変造] 来月ご請求に関する事前のご連絡	遮断	未転送	18-04-01 05:04
kiatchuan.sbs-asia.com@···		[広告性] [アドレス偽造変造] Re: MV. CHANDRA KIRANA _ PO for supply SAACKE Boiler / Burner	遮断	未転送	18-03-29 16:13
contact.manwesa@gmail.···		New Quotation CIF Saudi Arabia	ウイルス	未転送	18-03-28 21:52
contact.manwesa@gmail.···		New Quotation CIF Saudi Arabia	ウイルス	未転送	18-03-28 21:51
contact.manwesa@gmail.···		New Quotation CIF Saudi Arabia	ウイルス	未転送	18-03-28 21:50
contact.manwesa@gmail.···		New Quotation CIF Saudi Arabia	ウイルス	未転送	18-03-28 21:47
contact.manwesa@gmail.···		New Quotation CIF Saudi Arabia	ウイルス	未転送	18-03-28 21:46
contact.manwesa@					18-03-28 21:44
contact.manwesa@					18-03-28 21:42
contact.manwesa@					18-03-28 21:40
contact.manwesa@					18-03-28 21:37
contact.manwesa@					18-03-28 21:34
zandretradingltd@					18-03-27 11:03
admin@bedisk.tk					18-03-21 01:05
naito@hship.co.jp					18-03-13 20:41
ops@sinoleadmarir					18-03-13 20:41

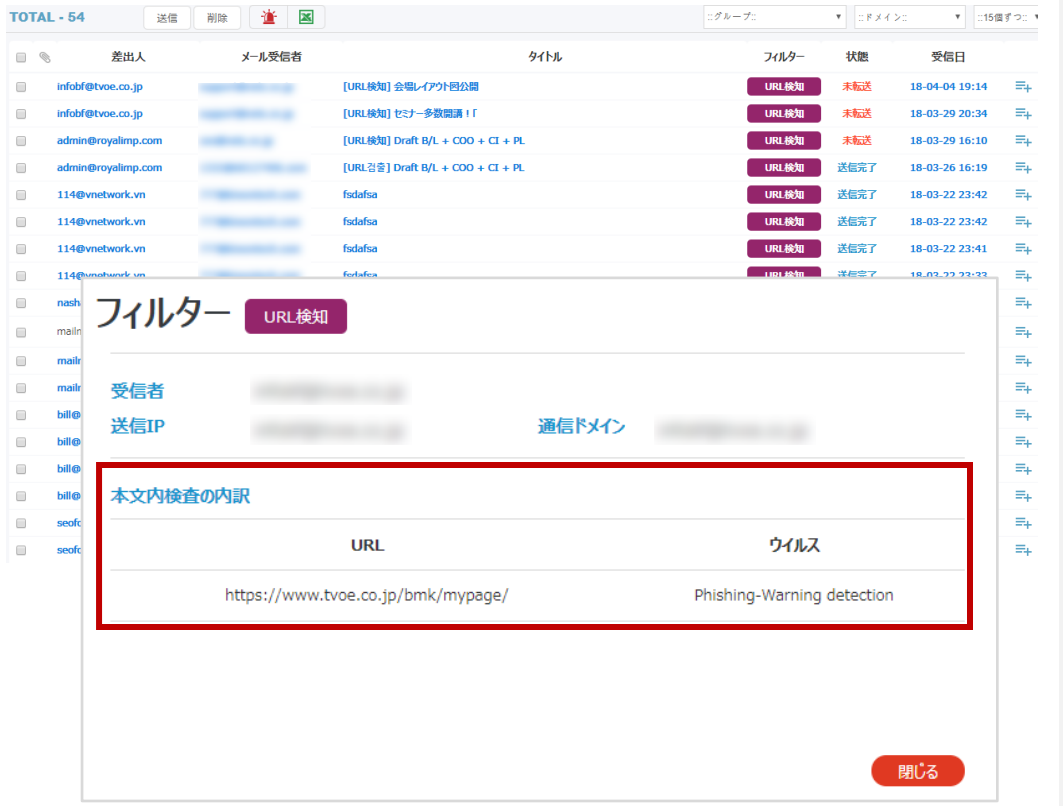
添付ファイル検出の内訳

分類	ファイル名
ランサムウェア	dhl_tracking_document.ace (1019.95 KB)

ヘッダ偽造変造 - その他の偽造変造

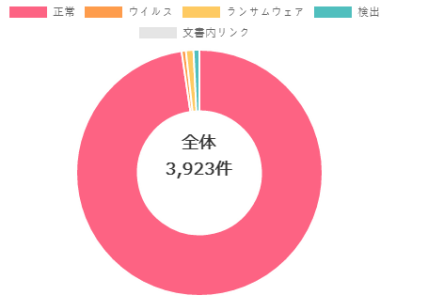
結果	hawks3399@gmail.com から admin@bedisk.tk に変更されました。

3.本文URL検出/イメージ化



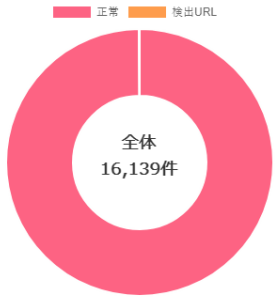
4.統計レポート_フィルタリング/装備

▸ 添付ファイル検査の内訳の現状



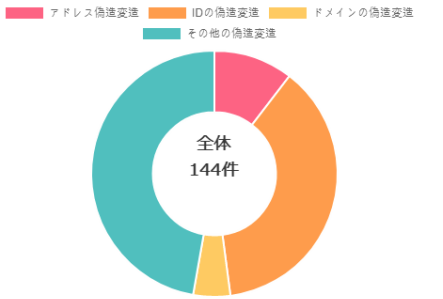
全体	正常	ウイルス	ランサムウェア	検出	文書内リンク
3,923 件	3,832 件	22 件	39 件	30 件	0 件

▸ URL検事の内訳の現状



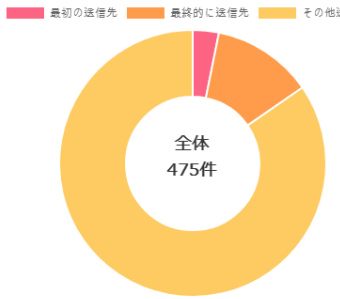
全体	正常	検出URL
16,139 件	16,122 件	17 件

▸ ヘッダの偽造変造の状況



全体	アドレス偽造変造	IDの偽造変造	ドメインの偽造変造	その他の偽造変造
144 件	15 件	54 件	7 件	68 件

▸ 送信先の危険の状況



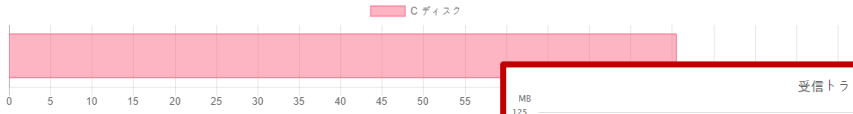
全体	最初の送信先	最終的に送信先	その他送信先
475 件	15 件	58 件	402 件

▸ リソース情報

- CPU&メモリ使用率

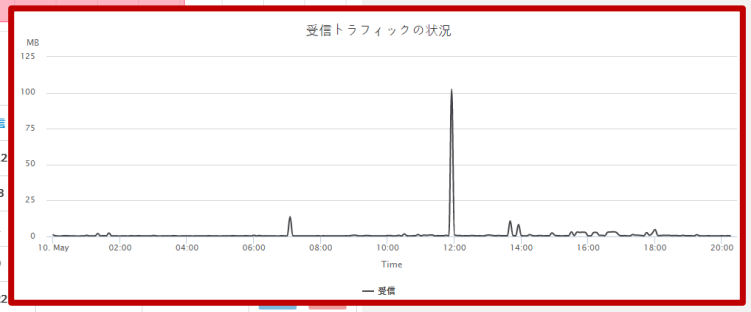
日付	日付	CPU最大	CPU、少なくとも	CPU平均	メモリー最大	メモリー最小	平均メモリー
2018-4-10	3%	1%	0%	87%	59%	55%	見本
2018-4-9	4%	0%	0%	74%	57%	54%	見本
2018-4-8	3%	0%	0%	74%	56%	55%	見本
2018-4-7	4%	0%	0%	74%	56%	54%	見本
2018-4-6	16%	1%	0%	65%	57%	54%	見本
2018-4-5	12%	1%	0%	68%	53%	51%	見本
2018-4-4	11%	1%	0%	72%	52%	52%	見本

- グラフ



- ディスク使用率

日付	SCMGuardの受信/発信トラフィックの状況	最大受信	最小受信	平均受信			
2018-4-10	26.7635	0.0463	1.2827	102.5112			
2018-4-9	13.8474	0.0461	0.8537	14.1998			
2018-4-8	1.6782	0.0621	0.1624	1.2961			
2018-4-7	11.2162	0.0636	0.2681	1.1019			
2018-4-6	39.4338	0.0678	1.4053	102.7422			
2018-4-5	53.6825	0.0670	0.9294	83.5489	0.2924	1.0057	受信 | 送信
2018-4-4	21.4181	0.0556	1.1752	86.6509	0.2196	1.7805	受信 | 送信

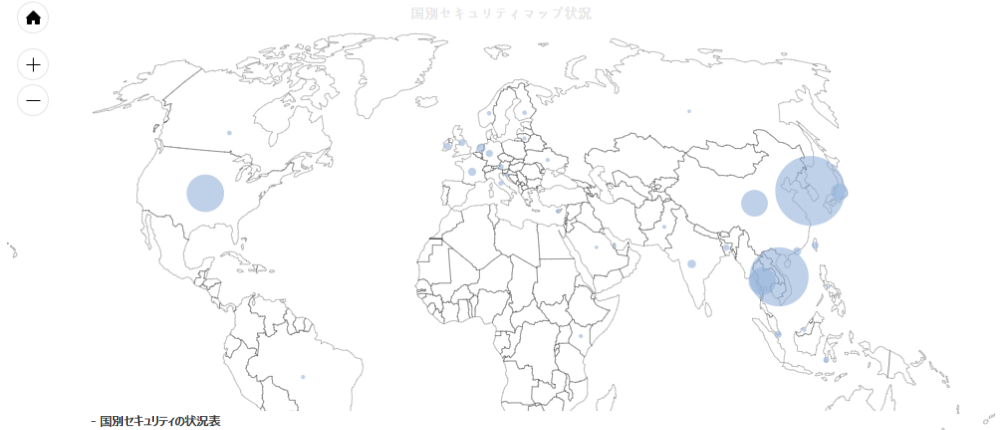


フィルタリング統計資料の提供

- 期間設定して統計データ検索可能
- 各フィルタリングは別に統計結果照会
- 装備の状態・ヒストリー検索
- ワンクリック印刷機能を提供

4.統計レポート-国別/勘定別/装備

- 国別セキュリティマップ状況



- 国別セキュリティの状況表

国名	危険メール				変調メール				総計
	業務性	広告性	悪性メール	ランサムウェア	ランサムウェア	ヘッダの偽造変造	類似ドメイン(全て)	類似ドメイン(個人)	
大韓民国	9	277	5	0	0	0	968	0	1,259
ベトナム	442	84	4	4	0	0	369	0	903
米国	8	329	12	9	0	0	4	0	362
タイ	0	191	0	0	0	0	0	0	191
中国	52	131	0	0	0	0	0	0	183
オーストラリア	0	72	0	0	0	0	0	0	72
日本	19	42	5	0	0	0	6	0	72
オランダ	1	6	0	0	0	0	11	0	18
インド	6	10	0	0	0	0	0	0	16
フランス	4	10	0	1	0	0	0	0	15
香港	3	11	0	0	0	0	1	0	15

現況/レポート - アカウント別に攻撃の状況

グループ | ドメイン | 直接入力 | 2017-06-01 | 2018-04-10 | 適用

形式別攻撃照会 | 国別攻撃照会

Top 100

順位	メールアカウント	件数
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

11位~40位

順位	メールアカウント	件数
11		102
12		99

41位~70

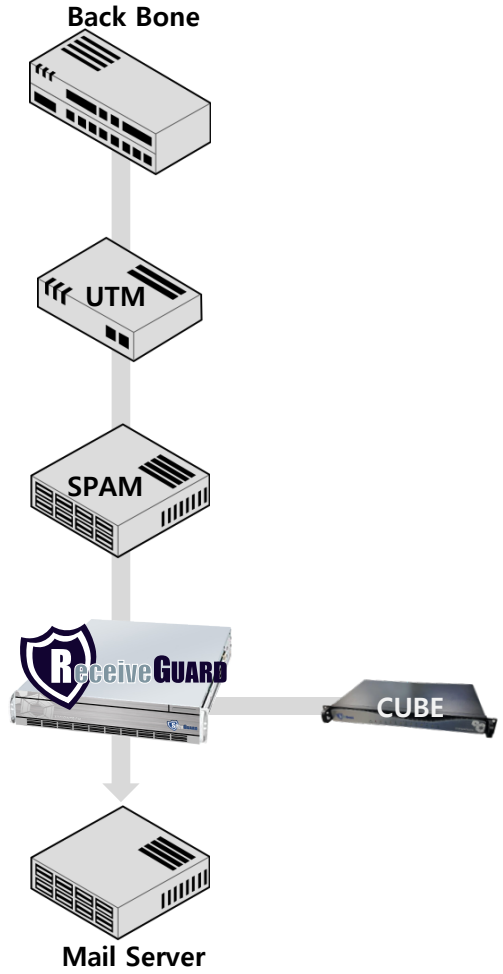
順位
41
42

4.製品ラインナップ

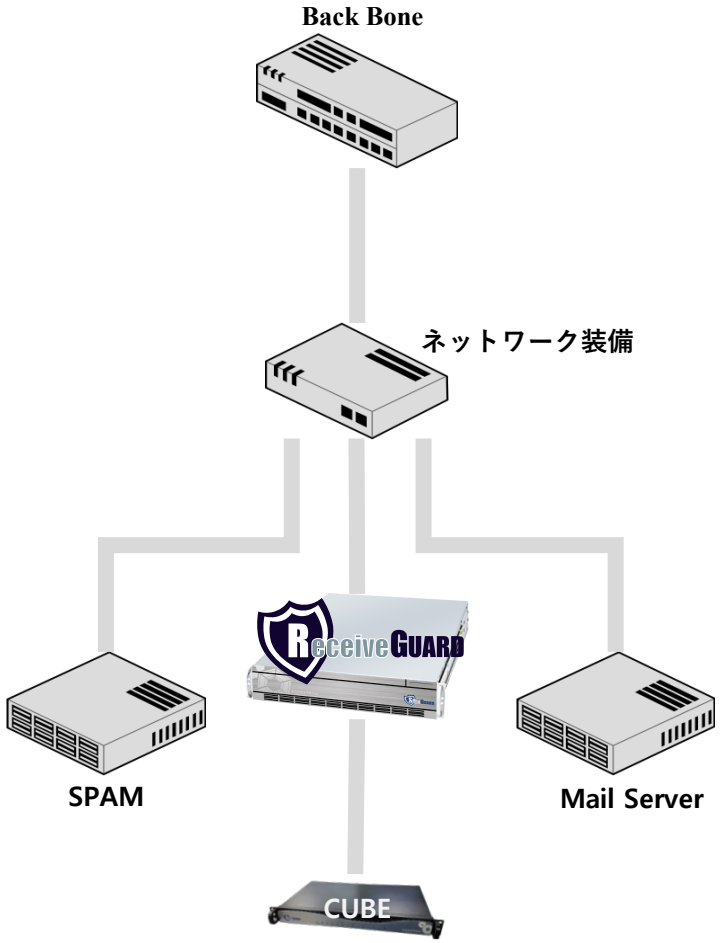
	Standard	Enterprise		
	SCM 147	SCM 113	SCM 115	SCM 117
Model			 ※ 4Coreでの増設も可能	 ※6Coreで12Core変更不可能
Spec.	• CPU : Intel® i5-3570アイビーブリッジ 3.4GHz * 1EA • Cache : 6MB (1 x 6MB) • Memory : 16GB (2 x 8GB) DDR3-12800 • HDD 0 : SSD 250GB HDD * 1EA • HDD 1 : SATA 1TB HDD * 1EA • Power Supply 250W Power Supply	• CPU : Intel® Xeon® E3-1231V3 3.40GHz * 1EA (4 Core) • Cache : 8MB (1 x 8MB) Level 3 cache • Memory : 16GB (2 x 8GB) • DDR4-2133R DIMMs • NIC : Ethernet (4*1GbE) Adapter • SSD 240GB * 2EA : RAID 1 • SSD 240GB * 2EA : RAID 1 • SATA 1TB * 2EA : RAID 1 • Power Supply 740W Power Supply *2	• CPU : Intel® Xeon® E5-2620V3 2.40GHz * 1EA (6 Core) • Cache : 15MB (1 x15MB) Level 3 cache • Memory : 32GB (2 x 16GB) • DDR4-2133R DIMMs • NIC : Ethernet (4*1GbE) Adapter • SSD 240GB * 2EA : RAID 1 • SSD 240GB * 2EA : RAID 1 • SATA 2TB * 2EA : RAID 1 • Power Supply 740W Power Supply *2	• CPU : Intel® Xeon® E5-2620V3 2.40GHz * 2EA (12 Core) • Cache : 15MB (1 x15MB) Level 3 cache • Memory : 64GB (8 x 8GB) • DDR4-2133R DIMMs • NIC : Ethernet (4*1GbE) Adapter • SSD 240GB * 2EA : RAID 1 • SSD 240GB * 2EA : RAID 1 • SATA 4TB * 2EA : RAID 1 • Power Supply 740W Power Supply *2
비고	• ユーザ単位:100人、200人、300人 • ネットワーク・ポート全てギガビット支援 • ソーホー型、最少仕様でパフォーマンス運営可能 • 基本仕様で、中央CUBE使用可能 • 別途CUBE導入の内部接続可能	• Core単位:4Core、6Core、12Core構成 • 運営体制、米DB運用構成を分離して相互干渉が発生しない • 全体ハードをRAID 1で構成し、資料の流失を最大に防止 • VA数を最大限に増やすためのH/W仕様 • データ保存がなるハードを除いて全てSSDの形で既存のIn Memory方式にCore単位別に最高のパフォーマンス運営		

5.ネットワーク構成

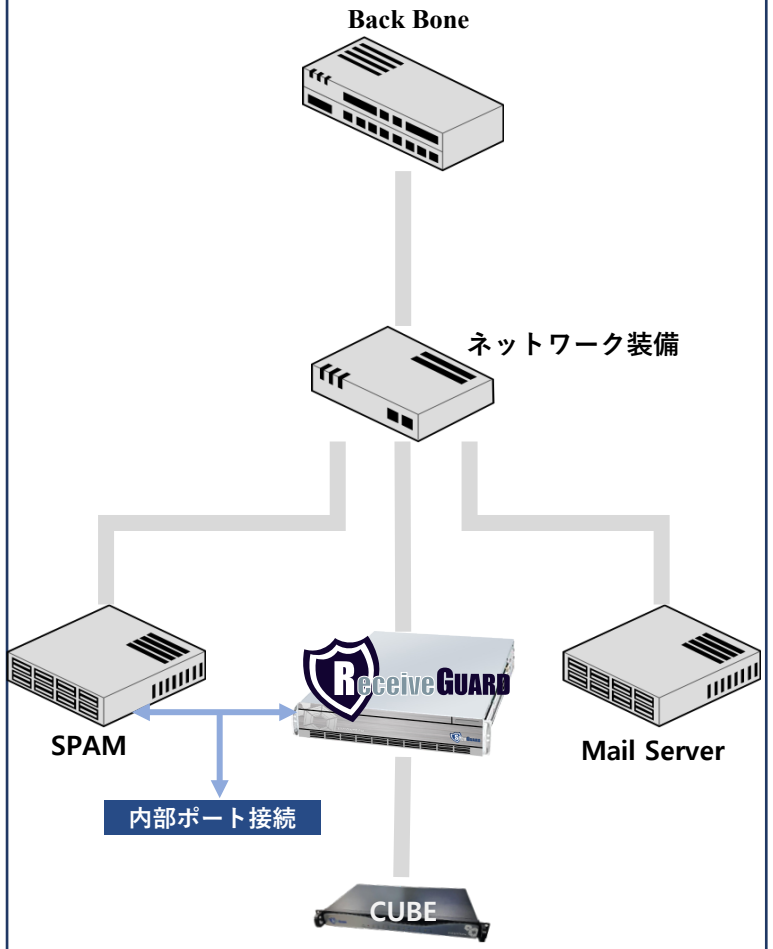
基本構成



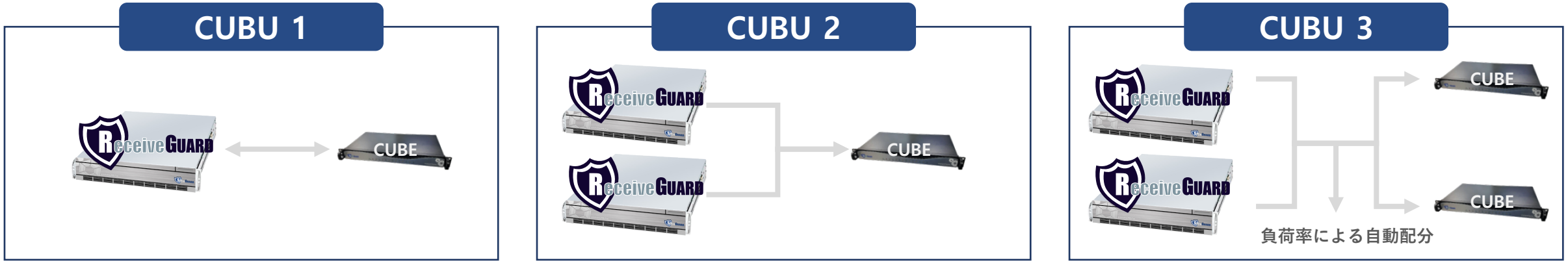
プロキシ方式



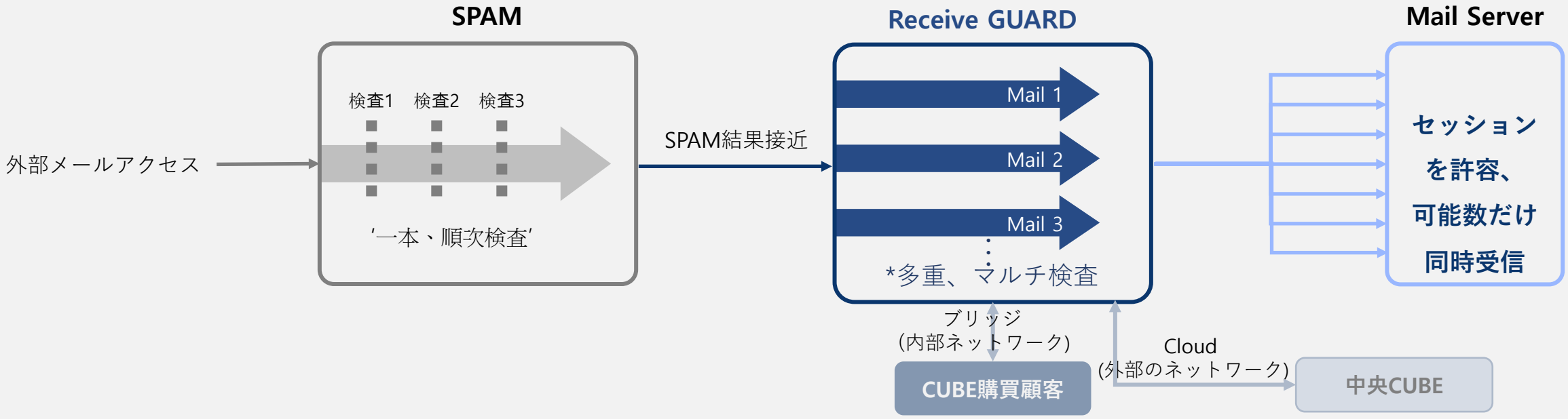
ブリッジ方式



5.ネットワーク構成



parsing方法



6.他社との機能比較

Receive GUARDだけがスケム、スピア・フィッシングなど詐欺メール先制対応可能

機能比較	ReceiveGUARD	他社製品(APT)
メール原文を分析してから、信頼度表示	O	X
URL END POINTまで追跡後の検査	仮想空間を利用して、直接開いてみる方法で検査	URLデータベースを利用して検査
ウィンドウシステム変更ファイル感知	メール受信時に添付されたファイルリアルタイム検査	データベースを利用してアップロード方式
類似性ドメイン検査	O	X
危険性メールのイメージ化させて伝送	O	X
遮断メール転送時に認証手続き	O	X
メールサーバトラフィックの状態自体確認後自動配信	O	X
メールIP追跡で送信先国家情報確認	O	O

6.他社との機能比較

機能比較	ReceiveGUARD	F社	S社	J社	D社
大容量添付ファイルリアルタイム処理可能	O	X	X	X	X
URL END POINTまで追跡後検知	O	本文URLだけが検知可能	O	本文URLだけが検知可能	本文URLだけが検知可能
ウィンドウシステム変更ファイル感知	O	X	X	X	X
メール1件当たりVA最小3つ以上投入可能、(最小1,000個以上運営)	O	全体VAが96個	投入数未記入	多数だけ表現	X
危険性メールのイメージ化させて伝送	O	X	X	X	メール原文リンクの形で暗号化
遮断メール転送時に認証手続き	O	X	X	X	X
メールサーバトラフィックの状態自体確認後自動配信	O	X	X	X	X
メールIP追跡で送信先国家情報確認	O	X	X	X	O

Ⅲ. 事業進行状況

1.海外の構築の現況

2.使用客の現況

3. SCM GUARD Platform

4.会社紹介

1.海外事業現況

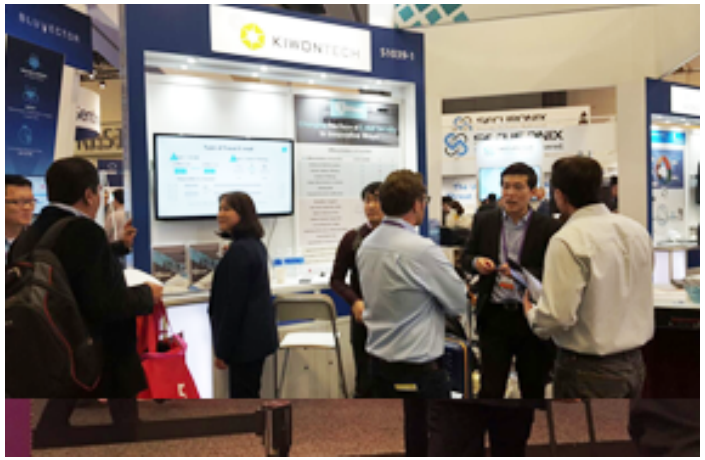
- 米国– OPSWAT
- 英国-T Global
- ドイツ- Intermundien-Lemon Europe GmbH
- イスラエル- Resec
- オマーン- OZONE United
- インドネシア- Telindo
- オーストラリア- Jasus
- シンガポール- Sin yun
- ベトナム- VNETWORK
- 日本- Taiyo

世界が選択したメールセキュリティ装備, Receive GUARD

1.海外事業現況

米国/ワシントン
韓米ICT情報セキュリティ使節団ビジネス発表会

- 韓米情報セキュリティe-mailセキュリティ部門**韓国代表参加**
- e-mail犯罪動向及び**対応策発表**



米国/サンフランシスコ
世界最大のセキュリティの展示会**RSA 2017**

- **米政府機関の要請**セキュリティ展示会RSA参加
- **米政府調達企業**のビジネス**パートナーシップ採決**

世界が選択したメールセキュリティ製品,

2.使用客の現況

ベトナム国防部の導入決定

LG 化学

HYUNDAI HEAVY INDUSTRIES CO.,LTD.

for a better future KEP

AJU銀行

DINTEC

現代ケミカル

OCI Company Ltd.

韓国政策研究院

Hyundai Oilbank

KOLON

KMA 大韓医師協会

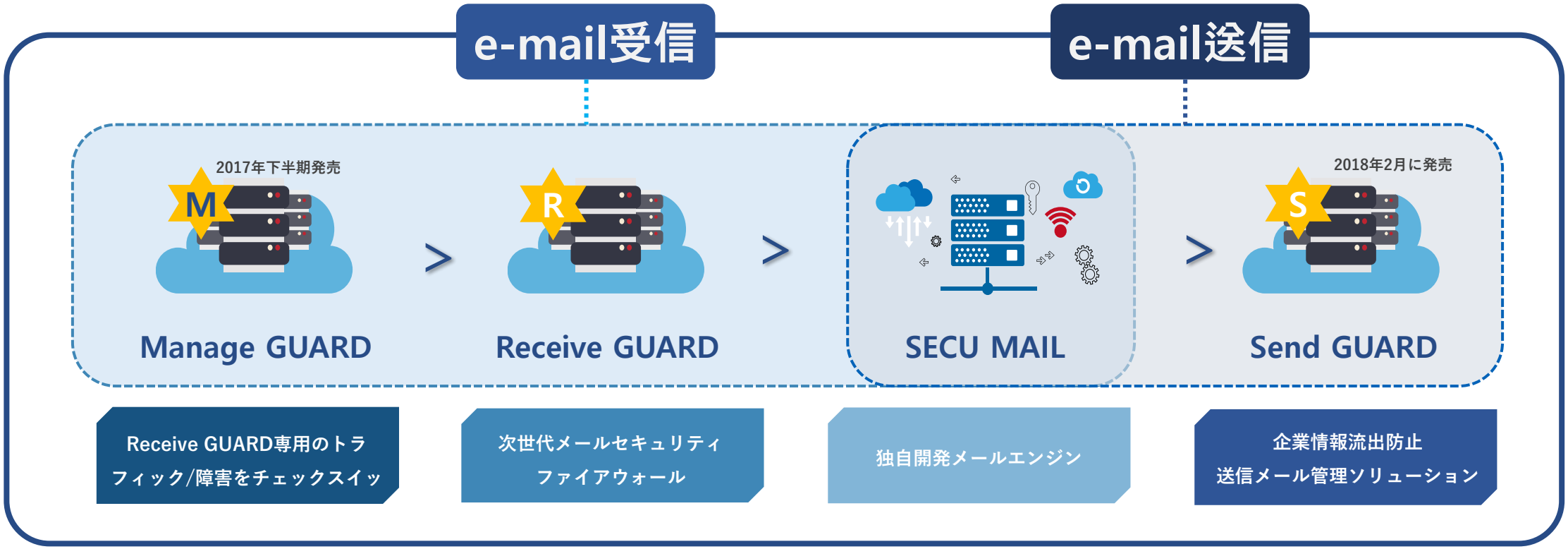
ソウル大学校 SEOUL NATIONAL UNIVERSITY

現代オイルターミナル

COSMO OIL

HYUNDAI and SHELL Base Oil

3. SCM GUARD Platform



メールの最初から最後まで! 唯一の独自開発 e-mail, One Stop Service!

4.会社紹介

Secu Japan

会社名	セキュ．ジャパン株式会社〒
住所	〒615-0036 京都市右京区西院太田町23番地
代表取締役	金 容基
設立日	2018年
ホームページ	www.scmguard.jp
代表番号	075-321-1881
FAX	075-316-6122

Advanced Technology, Secu Japan co.ltd.

THANK YOU

Cooperate, Creative & Customizing
= 3C Rules