



Clearswift SECURE Email Gateway S/MIMEシグネチャゲートウェイとしてのご利用について

2018年8月

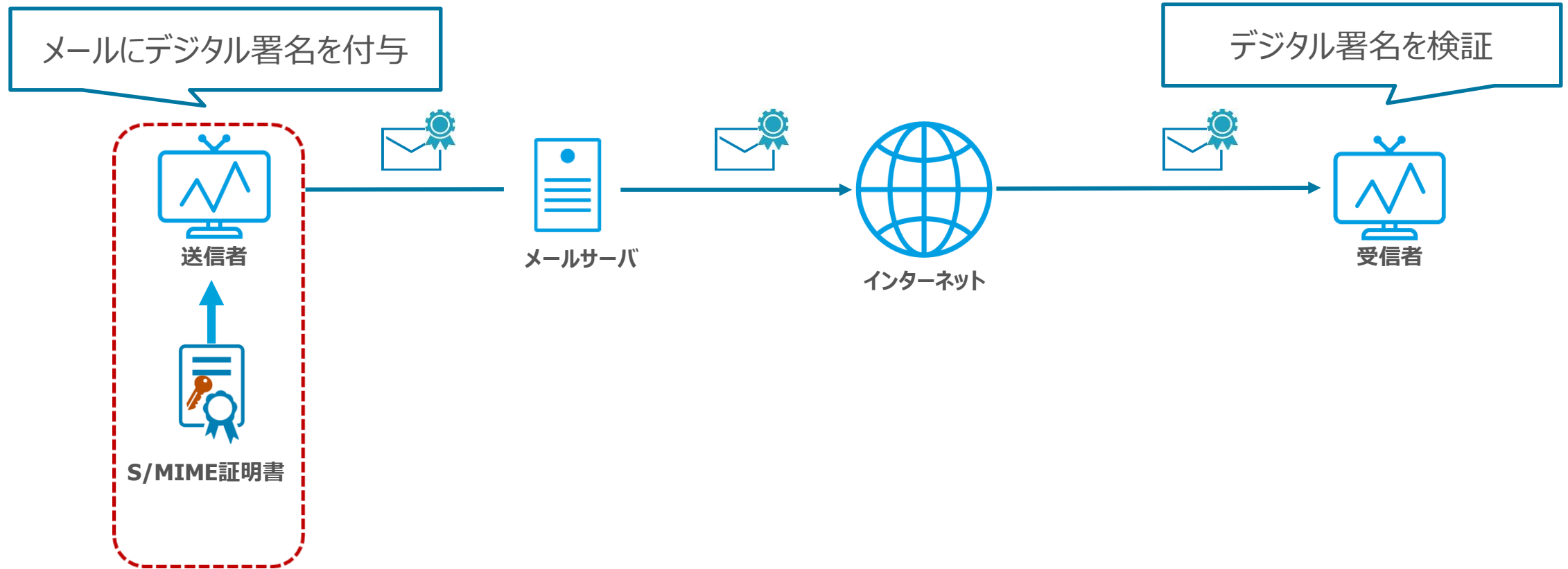
クリアスウィフト リージョナルディレクター 杉山吉寿

S/MIMEについて

- S/MIMEには『**メールの暗号化**』と『**メールへの電子署名の付加**』の2つの役割がある。
- S/MIMEで出来ることは、**メールの盗聴、なりすまし、改ざんの防止**である。
- S/MIMEでは、メールの送信者と受信者の間でPKIを利用し、**送信者が付与したデジタル署名を、受信者で検証することにより**、データの完全性の確保と送信者の確認を可能とする。
- S/MIMEは送信者側にて以下のオプションを選択できる。
 1. 署名のみ
 2. 暗号のみ
 3. 署名 + 暗号

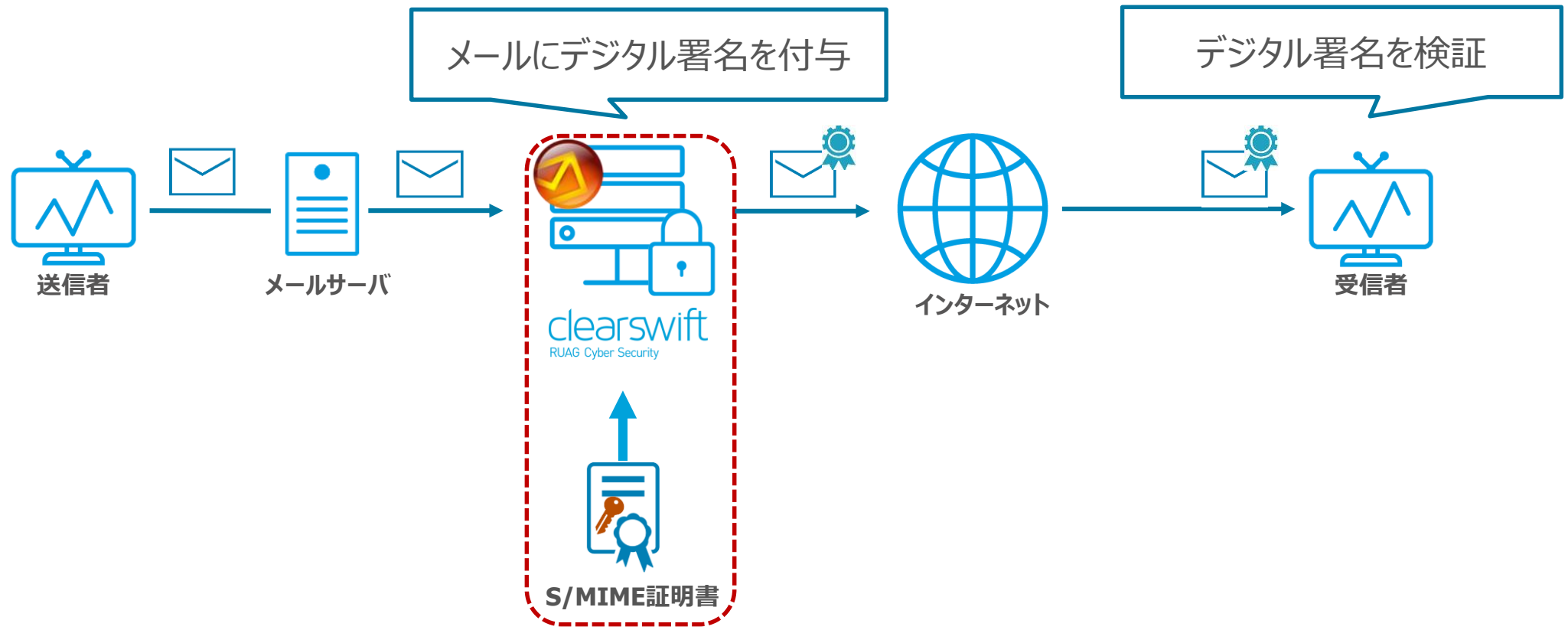
クライアントへS/MIME証明書をインストール

クライアントでメールにデジタル署名を付加して送出する場合、証明書の管理、ユーザの手間が増えるなど運用負担が高くなりがちになります。



SECURE Email GatewayへS/MIME証明書をインストール

Clearswift SECURE Email Gateway(SEG) にS/MIME証明書をインポートすることにより、シグネチャーゲートウェイとして機能させることにより、SEG上で一括してメールにデジタル署名を付加することができるため、運用負荷は軽減されます。



証明書ストアのUI

ホーム ポリシー メッセージ レポート システム 状態 ユーザー

ホーム | キー サーバークエリ | キーサーバークエリの変更 | 証明書ストア

証明書ストア

証明書機関 コーポレート パートナー 設定

検索条件

設定の変更はここをクリックします

インポート フィルターをリセットする

表示: 1 - 20 / 486

タイプ	詳細	電子メール	有効期限
S/MIME	(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim...		2015/03/22
S/MIME	(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim...		2015/03/22
S/MIME	AC Camerfirma S.A., Chambers of Commer...		2038/07/31
S/MIME	AC Camerfirma S.A., Global Chambersign R...		2038/07/31
S/MIME	AC Camerfirma SA CIF A82743287, http://w... chambersroot@chambersi...		2037/09/30
S/MIME	AC Camerfirma SA CIF A82743287, http://w... chambersignroot@chamb...		2037/09/30
S/MIME	AC Camerfirma SA CIF A82743287, http://w... publicnotaryroot@chambe...		2037/09/30
S/MIME	ACCV, PKIACCV, ACCVRAIZ1	accv@accv.es	2030/12/31
S/MIME	ACNLB		2023/05/15
S/MIME	Actalis S.p.A./03358520967, Actalis Authent...		2022/06/25
S/MIME	Actalis S.p.A./03358520967, Actalis Authent...		2030/09/22
S/MIME	AddTrust AB, AddTrust External TTP Networ...		2020/05/30
S/MIME	admin, Services, AdminCA-CD-T01		2016/01/25
S/MIME	admin, Services, Admin-Root-CA		2021/11/10
S/MIME	ADMINISTRACION NACIONAL DE CORREOS,...		2030/12/31
S/MIME	Aerodata CA		2012/08/23
S/MIME	AffirmTrust, AffirmTrust Commercial		2030/12/31
S/MIME	AffirmTrust, AffirmTrust Networking		2030/12/31
S/MIME	AffirmTrust, AffirmTrust Premium		2040/12/31
S/MIME	AffirmTrust, AffirmTrust Premium ECC		2040/12/31

【パートナー】タブ

このエリアには、業務を行う相手や組織に属する S/MIME 証明書と PGP 証明書があります。

パートナー証明書内に含まれているパブリック キーは、以下を行うときに使用します。

- パートナー宛てに送信する電子メール メッセージの暗号化
- パートナーから受信した電子メール メッセージのデジタル署名の検証

【証明書機関】タブ

このエリアには S/MIME 証明書を検証するために使用する証明書機関の証明書/キーを格納します。

署名証明書は、Email Gateway を通過する電子メール メッセージの暗号化、復号化、署名で使用されるその他の証明書を検証するために使用されます。

【コーポレート】タブ

このエリアには、所属組織に属する S/MIME 証明書と PGP 証明書を格納します。

コーポレート証明書に含まれているプライベートキーは、組織内のユーザーの代わりに以下の処理を行うときに使用します。

- 受信メール メッセージの復号化
- 送信メール メッセージへの署名

S/MIME 証明書と PGP 証明書

S/MIME または PGP を使用するには、SEGの適切な暗号化または復号化の証明書ストアエリアにキーを格納する必要があります。既存の証明書をインポートすれば、証明書に含まれているキーを各エリアに格納できます。また、証明書/キージェネレータを使って新しい証明書を作成することも可能です。

暗号化と復号化に使用されるキー

テクノロジー	メール通信の方向	Gateway	受信者のキー	証明書ストア エリア
S/MIME	送信メール	暗号化	パブリック	パートナー
	受信メール	復号化	プライベート	コーポレート デフォルトの復号化キーとして指定
PGP	送信メール	暗号化	パブリック	パートナー
	受信メール	復号化	プライベート	コーポレート

署名と検証に使用されるキー

テクノロジー	メール通信の方向	Gateway	送信者のキー	証明書ストア エリア
S/MIME	送信メール	署名	プライベート	コーポレート
	受信メール	検証	送信者のパブリック キーの CA 証明書 --または-- 自己署名 CA	パートナー
PGP	送信メール	署名	プライベート	コーポレート
	受信メール	検証	パブリック	パートナー

A hand is shown in the upper right, pointing towards a glowing digital interface. The background is a deep blue with a network of white and light blue nodes and lines, suggesting a digital or cyber environment. The overall aesthetic is clean and modern.

clearswift

RUAG Cyber Security

ありがとうございました。